ipexpert

IPexpert's Detailed Solution Guide

for the Cisco® CCIE™ Security Volume 1

Complete DSG Labs 1-5

Table of Contents

Section 1: ASA Solutions

Lab-1: ASA Initialization – This lab is intended to familiarize you with the initialization of the ASA and the new features associated with it. This section contains two ASAs. One of the ASAs is loaded with 8.2 code and the other is loaded with 8.6 code. It is very important to understand the new features in the 8.6 version of software. This lab focuses on IPv4 routed mode only. Further ASA labs are built on this lab topology (Network Topology 1.1) therefore, it is important to understand this topology.

We highly recommend creating your own diagram at the beginning of each lab so you are able to draw on your own diagram, making it much easier when you step into the real lab. Multiple topology drawings are available for this section.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- Make it a common practice to verify the pre-configurations loaded on the devices.

Estimated Time to Complete: 1 Hour

Pre-setup

Load the initial configurations for the routers and switches. Note that routers and switches are pre-configured with these initial configurations.

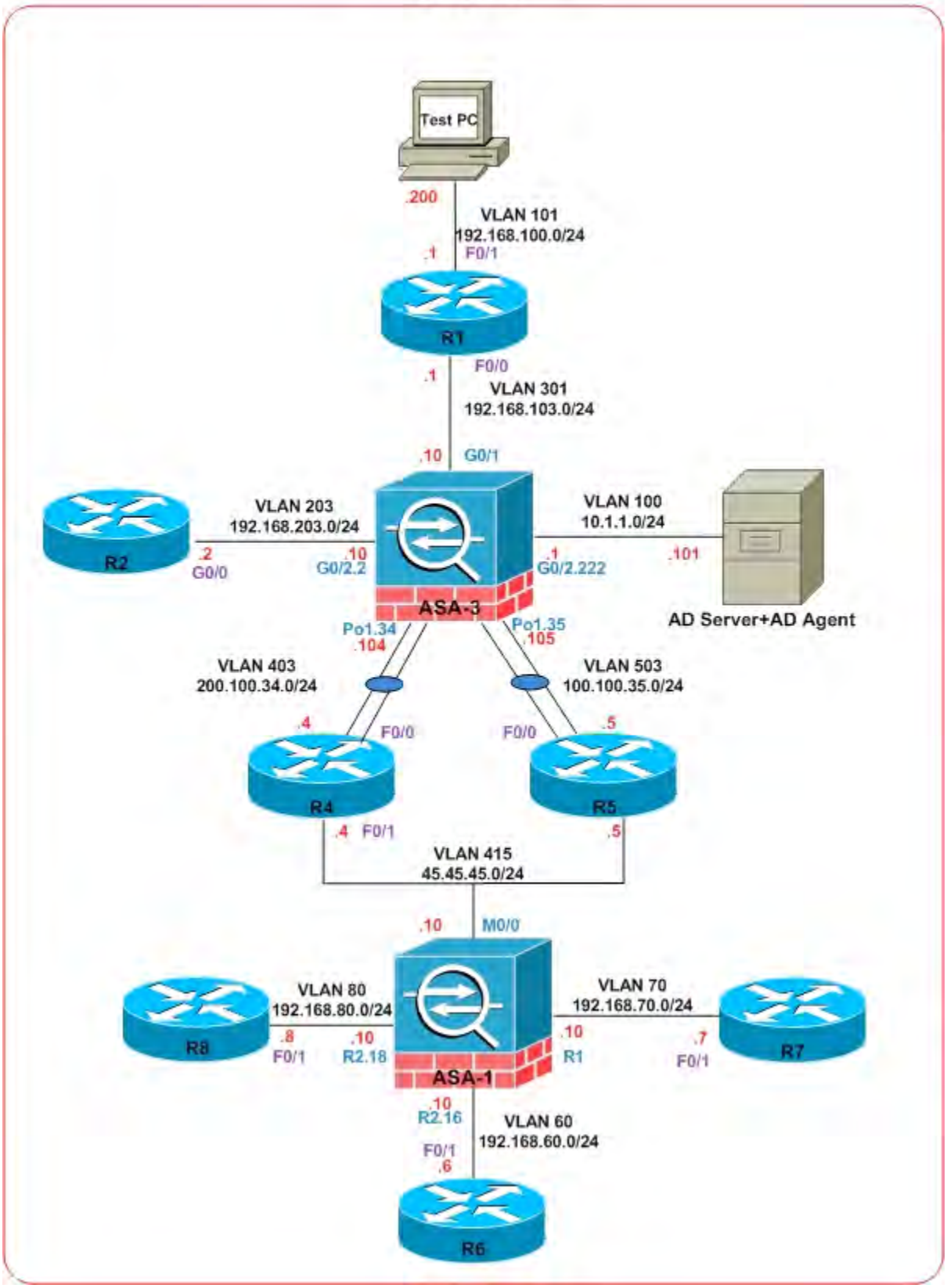
NOTE: *Do not make additional configuration on the routers, unless explicitly asked for in the*

task; some switching configuration must be performed as per the task requirements.

Use the logical topology drawing – Network Topology 1.1 and refer to the general physical connectivity.

Ensure that your ASA is in single context routed mode before you start the configuration. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.1 (Logical)



Lab 1: Configuration Tasks

Task 1: Initialization ASA-3

- Configure a hostname of "ASA-003fw" on ASA-3
- ASA-003fw should have a domain name of ipexpert.com
- Configure ASA-003fw interfaces and the appropriate switchports on the Catalyst with the specifications below. After you perform this task, ensure that you can ping your directly connected neighbors R2 and the AD Server.

ASA Interface	VLAN Tag	Security Level	Name	IP Address
G0/1	----------	100	INSIDE	192.168.103.10/24
G0/2.2	203	50	dmz1	192.168.203.10/24
G0/2.222	100	50	dmzserver	10.1.1.1/24

- Configure ASA-003fw the interfaces with EtherChannel and the appropriate switchport configurations on the Catalyst switch with the specifications below. All the devices should actively send LACP packets to setup the EtherChannel. After you perform this task, ensure that you can ping your neighbors R4 and R5.

ASA Interface	Member Interfaces on ASA	ASA System priority	Max Bundle	Load Distribution Algorithm
Port-Channel1	G0/0 and G0/3	10	2	Vlan-Src-Dst-ip-Port
ASA Interface	**VLAN Tag**	**Security Level**	**Name**	**IP Address & V-MAC**
Po1.34	403	0	Outside-1	200.100.34.104/24 0044.0044.0044
Po1.35	503	0	Outside-2	100.100.35.105/24 0055.0055.0055

Detailed Solution: Lab-1

Task-1

Summary Guidelines

1. Make sure you know the physical and logical topology well
2. Do not start configuring tasks linerarly. Read the entire lab to identity any dependency with other tasks and then proceed to configure.
3. Pre- load the configurations and check if the loaded configuration is correct
4. Before you begin with configuring the ASA. Configure the Layer-2 i.e. switch with VLAN's/Trunks
5. Once Layer 2 is in order. You may begin configuring the ASA.
6. Pay very close attention to the names, interfaces and IP address.
7. After you configure them, make it a point to verify your configs and save them.

Step 1: Layer 2 configuration

Network Topology 1.1 is a logical topology. Physically all the Ethernet interfaces of routers and ASA's are connected to switches. Hence we need to first build the layer 2 and then proceed to the layer 3 part of the configuration. Please refer the physical connection topology.

If the appropriate VLAN's are not created then you may create them. However if you do create them make sure the VLAN number matches with the topology.

** NOTE – switch configuration is already part of the Initial configurations (but it does not have to be in the real lab) – configuration is shown here for your reference **

SW3

```
interface GigabitEthernet1/0/20
 description ASA_Inside_G0/1
 switchport access vlan 301
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/21
 description ASA_DMZ_INTERFACES
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,203
 switchport mode trunk

interface GigabitEthernet1/0/22
 description ASA_OUTSIDE_PORTCHANNEL_INTERFACE
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 403,503
 switchport mode trunk
 channel-group 1 mode active


interface GigabitEthernet1/0/19
 description ASA_OUTSIDE_PORTCHANNEL_INTERFACE
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 403,503
 switchport mode trunk
 channel-group 1 mode active
```

Step 2: ASA Configuration

Now we shall configure the hostname, domain name, and all the interface related parameters. Make sure the interface numbers match as stated in the task.Make sure the interface names match as stated in the task albeit they are case-insensitive.

ASA3

```
domain-name ipexpert.com

interface GigabitEthernet0/1
 no shutdown
 nameif INSIDE
 security-level 100
 ip address 192.168.103.10 255.255.255.0
 no shutdown

interface GigabitEthernet0/2
 no nameif
 no security-level
 no ip address
 no shutdown

interface GigabitEthernet0/2.2
 vlan 203
 nameif dmz1
 security-level 50
 ip address 192.168.203.10 255.255.255.0
 no shutdown

interface GigabitEthernet0/2.222
 vlan 100
 nameif dmzserver
 security-level 50
 ip address 10.1.1.1 255.255.255.0
 no shutdown
```

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
 no shutdown

interface GigabitEthernet0/3
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
 no shutdown

interface Port-channel1
 lacp max-bundle 2
 port-channel load-balance vlan-src-dst-ip-port
 no nameif
 no security-level
 no ip address

interface Port-channel1.34
 mac-address 0044.0044.0044
 vlan 403
 nameif Outside-1
 security-level 0
 ip address 200.100.34.104 255.255.255.0

interface Port-channel1.35
 mac-address 0055.0055.0055
 vlan 503
 nameif Outside-2
 security-level 0
 ip address 100.100.35.105 255.255.255.0
```

Verification

Step 1: Verify layer 2 connectivity.

We should make sure the layer 2 is proper. This includes VLAN assignment and trunking configuration.

On SW3

```
sw3#sh vlan brief |  exclude unsup

VLAN  Name                             Status      Ports
---------------------------------------------------------------------------
<SNIP>
301   VLAN0301                         active      Gi1/0/20
```

Interfaces G1/0/15 – 18 and G1/0/23 – 24 are inter-switch trunk links.

```
sw3#show interface trunk

Port        Mode         Encapsulation  Status      Native vlan
Gi1/0/15    on                802.1q         trunking  1
Gi1/0/16    on                802.1q         trunking  1
Gi1/0/17    on                802.1q         trunking  1
Gi1/0/18    on                802.1q         trunking  1
Gi1/0/21    on                802.1q         trunking  1
Gi1/0/23    on                802.1q         trunking  1
Gi1/0/24    on                802.1q         trunking  1
Po1                 on               802.1q         trunking 1

Port        Vlans allowed on trunk
Gi1/0/15    1,70,100-101,203,300-301,403,503
Gi1/0/16    1,70,100-101,203,300-301,403,503
Gi1/0/17    1,70,100-101,203,300-301,403,503
Gi1/0/18    1,70,100-101,203,300-301,403,503
Gi1/0/21    100,203
Gi1/0/23    1,70,100-101,203,300-301,403,503
Gi1/0/24    1,70,100-101,203,300-301,403,503
Po1                 403,503

Port        Vlans allowed and active in management domain
Gi1/0/8     none
Gi1/0/9     none
Gi1/0/15    1,70,100-101,203,300-301,403,503
Gi1/0/16    1,70,100-101,203,300-301,403,503
Gi1/0/17    1,70,100-101,203,300-301,403,503
Gi1/0/18    1,70,100-101,203,300-301,403,503
Gi1/0/21    100,203
Gi1/0/23    1,70,100-101,203,300-301,403,503
Gi1/0/24    1,70,100-101,203,300-301,403,503
Po1                 403,503

Port  Vlans in spanning tree forwarding state and     not pruned
Gi1/0/8     none
Gi1/0/9     none
Gi1/0/15    1,70,100-101,203,300-301,403,503
Gi1/0/16    none
```

```
Gi1/0/17    none
Gi1/0/18    none
Gi1/0/21    100,203
Gi1/0/23    1,70,100-101,203,300-301,403,503
Gi1/0/24    1,70,100-101,203,300-301,403,503
Po1                 403,503
```

On ASA3

```
ASA-003fw# sh port-channel 1
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 2
Load balance: vlan-src-dst-ip-port
```

Layer-2 Etherchannel verification on ASA3

```
ASA-003fw# sh port-channel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use      N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
---
1      Po1(U)             LACP    Gi0/0(P)    Gi0/3(P)
```

Layer-2 Etherchannel verification on Switch3

```
sw3#sh etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
---
1      Po1(SU)          LACP      Gi1/0/19(P) Gi1/0/22(P)
```

Step 2: Verify layer 3 connectivity on the ASA3

```
ASA-003fw# show interface ip brief
Interface                  IP-Address      OK?    Method     Status          Protocol
GigabitEthernet0/0         unassigned      YES    unset      up              up
GigabitEthernet0/1         192.168.103.10  YES    manual     up              up
GigabitEthernet0/2         unassigned      YES    unset      up              up
GigabitEthernet0/2.2       192.168.203.10  YES    manual     up              up
GigabitEthernet0/2.222     10.1.1.1        YES    manual     up              up
GigabitEthernet0/3         unassigned      YES    unset      up              up
<SNIP>
Port-channel1              unassigned      YES    unset      up              up
Port-channel1.34           200.100.34.104  YES    manual     up              up
Port-channel1.35           100.100.35.105  YES    manual     up              up
```

```
ASA-003fw# show nameif
Interface                  Name            Security
GigabitEthernet0/1         INSIDE               100
GigabitEthernet0/2.2       dmz1                  50
GigabitEthernet0/2.222     dmzserver             50
Management0/0              management           100
Port-channel1.34           Outside-1              0
Port-channel1.35           Outside-2              0
```

We can test connectivity with simple ping tests. Keep in mind here that you don't have any routing enabled, so keep it simple and just test to what is directly connected.

```
ASA-003fw# ping 200.100.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.4, timeout is 2 seconds:
!!!!!

ASA-003fw# ping 100.100.35.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.35.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-003fw# ping 192.168.103.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.103.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-003fw# ping 192.168.203.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-003fw# ping 10.1.1.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Notes

This task focuses on basic initialization of the ASA3 such that traffic can pass through the ASA. Interfaces can be physical or logical. For an interface to pass traffic, 3 main parameters should be configured. These are the interface name, IP address and mask and finally security level. Interface names are case-insensitive. However for the sake of the exam it is required to configure the exact names/case given in the task. Any name other than inside has a security level of zero. Do not forget to un shut the interface using “no shutdown” since they are in shutdown state.

ASA’s interfaces can be slpit into multiple logical interfaces i.e. sub-interfaces or VLAN interfaces. Here each sub-interface is associated with a VLAN tag. Since the ASA does not support DTP, you should statically configure the switches to trunk. It is a best practice to filter or send specific VLAN’s from the switch to the ASA using switchport trunk allowed vlan command. VLAN interfaces or sub-interfaces increase the number of available interfaces which is very useful for multi-context.

Etherchanel feature was introduced from 8.4 code of the ASA. Etherchannel interfaces allow the ASA to bundle similar physical interfaces (Same type,speed and duplex) into a single logical port-channel interface. This provides fault taulerance and high-speed links between devices. An ether-channel can be created from 1 to 8 active ports with an additional of upto 8 inactive ports using LACP protocol for link negotiation or 16 active members using static/no-negotiation "on" port channel configuration. It uses a propritery hash algorithm based on source/destionation IP, port or VLAN numbers and aggrigates traffic. All security related configurations will be done on the port channel interface and not the actual channel member/physical interface. Even the port channel interface can be split into multiple logical VLAN interfaces. You may refer the documentation for details related to other LACP parameters like system priority, port priority etc. Etherchannel feature can be utilized in both single context and multi-context mode of the ASA. The ASA supports upto 48 etherchannel interfaces. Make sure both the switch and the ASA is properly configured for ether-channel.

Port channel interface can be used for failover, however they need to be manually created on both the units and certain port-channel or LACP commands are not sync'd between the failover pair and may need to be individually configured.

Task 2: Initialization of ASA-1

- Configure a hostname of "ASA-001fw" on ASA-1
- ASA-001fw should have a domain name of ipexpert.com
- Configure the ASA-001fw outside interface and the appropriate switchports on the Catalyst with the specifications below. The management interface should be made a normal routed interface. After you perform this task, ensure that you can ping your directly connected neighbors R4 and R5.

ASA Interface	VLAN Tag	Security Level	Name	IP Address
M0/0	----------	0	OUTSIDE	45.45.45.10/24

- Configure ASA-001fw with redundant interfaces and the appropriate switchports on the Catalyst with the specifications below. After you perform this task, ensure that you can ping your neighbor R7.

ASA Interface	Member Interfaces	V-MAC	Active Interface
Redundant1	E0/0 and E0/1	0077.0077.0077	E0/1
ASA Interface	IP Address	Security Level	Name
Redundant1	192.168.70.10/24	70	DMZ1

- Configure ASA-001fw with redundant interfaces and the appropriate switchport configurations on the Catalyst switch with the specifications below. After you perform this task, ensure that you can ping your neighbors R6 and R8.
- Make sure during the configuration the redundant interfaces, E0/2 is added as the first member interface.

ASA Interface	Member Interfaces on ASA	V-MAC	Active Interface
Redundant2	E0/2 and E0/3		E0/3
ASA Interface	VLAN & IP Address & V-MAC	Security Level	Name
Redundant2.18	VLAN- 80 192.168.80.10/24 0088.0088.0088	80	Dmz2
Redundant2.16	VLAN- 60 192.168.60.10/24 0066.0066.0066	100	inside

Detailed Solution: Lab-1

Task-2

Step 1: Layer 2 configuration

Network Topology 1.1 is a logical topology. Physically all the Ethernet interfaces of routers and ASA's are connected to switches. Hence we need to first build the layer 2 and then proceed to the layer 3 part of the configuration. Please refer the physical connection topology.

If the appropriate VLAN's are not created then you may create them. However if you do create them make sure the VLAN number matches with the topology.

** NOTE – switch configuration is already part of the Initial configurations (but it does not have to be in the real lab) – configuration is shown here for your reference **

SW1

```
interface F0/14
 switchport access vlan 45
 switchport mode access
 spanning-tree portfast
```

SW3

```
interface GigabitEthernet1/0/6
 switchport access vlan 70
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/7
 switchport access vlan 70
```

```
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/8
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 60,80,415
 switchport mode trunk

interface GigabitEthernet1/0/9
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 60,80,415
 switchport mode trunk
```

Step 2: ASA Configuration

Now we shall configure the hostname, domain name, and all the interface related parameters. Make sure the interface numbers match as stated in the task.

ASA1

```
domain-name ipexpert.com

interface Ethernet0/0
 no nameif
 no security-level
 no ip address
 no shutdown

interface Ethernet0/1
 no nameif
 no security-level
 no ip address
 no shutdown

interface Ethernet0/2
 no nameif
 no security-level
 no ip address
 no shutdown

interface Ethernet0/3
 no nameif
 no security-level
 no ip address
 no shutdown

interface Management0/0
 no shutdown
```

```
 no management-only
 nameif OUTSIDE
 security-level 0
 ip address 45.45.45.10 255.255.255.0

interface Redundant1
 member-interface Ethernet0/1
 member-interface Ethernet0/0
 mac-address 0077.0077.0077
 nameif DMZ1
 security-level 70
 ip address 192.168.70.10 255.255.255.0

interface Redundant2
 member-interface Ethernet0/2
 member-interface Ethernet0/3

interface Redundant2.16
 mac-address 0066.0066.0066
 vlan 60
 nameif inside
 security-level 100
 ip address 192.168.60.10 255.255.255.0

interface Redundant2.18
 mac-address 0088.0088.0088
 vlan 80
 nameif Dmz2
 security-level 80
 ip address 192.168.80.10 255.255.255.0

redundant-interface redundant 1 active-member ethernet 0/1
redundant-interface redundant 2 active-member ethernet 0/3
```

Verification

Step 1: Verify layer 2 connectivity.

We should make sure the layer 2 is proper. This includes VLAN assignment and trunking configuration.

ASA-1 M0/0 interface connection to SW2

```
sw2#sh vlan brief | exclude unsup
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
--
<SNIP>
45   VLAN0045                          active    Fa0/4, Fa0/5, Fa0/14
<SNIP>
```

ASA1 E0/0 and E0/1 interface

```
sw3#sh vlan brief | exclude unsup
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
--
<SNIP>
70   VLAN0070                          active    Gi1/0/6, Gi1/0/7
<SNIP>
```

ASA1 E0/2 and E0/3 interface

```
sw3#sh interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/8     on               802.1q         trunking      1
Gi1/0/9     on               802.1q         trunking      1
<SNIP>
Port        Vlans allowed on trunk
Gi1/0/8     60,80,415
Gi1/0/9     60,80,415
<SNIP>
Port        Vlans allowed and active in management domain
Gi1/0/8     60,80
Gi1/0/9     60,80
<SNIP>
Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/8     60,80
Gi1/0/9     60,80
<SNIP
```

Step 2: Verify layer 3 connectivity on the ASA1

```
ASA-001fw# sh interface ip  brief
Interface                  IP-Address     OK?     Method  Status  Protocol
Ethernet0/0                unassigned     YES     unset   up      up
Ethernet0/1                unassigned     YES     unset   up      up
Ethernet0/2                unassigned     YES     unset   up      up
Ethernet0/3                unassigned     YES     unset   up      up
Management0/0              45.45.45.10    YES     manual  up      up
Redundant1                 192.168.70.10  YES     manual  up      up
Redundant2                 unassigned     YES     unset   up      up
Redundant2.16              192.168.60.10  YES     manual  up      up
Redundant2.18              192.168.80.10  YES     manual  up      up
```

```
ASA-001fw# show nameif
Interface           Name      Security
Management0/0       OUTSIDE   0
Redundant1          DMZ1      70
Redundant2.16       inside    100
Redundant2.18       Dmz2      80
```

```
ASA-001fw# show interface redundant 1
Interface Redundant1 "DMZ1", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        MAC address 0011.0011.0011, MTU 1500
        IP address 192.168.70.10, subnet mask 255.255.255.0
<SNIP>
  Redundancy Information:
        Member Ethernet0/0(Active), Ethernet0/1


ASA-001fw# sh interface redundant 2
Interface Redundant2 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 100 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 001b.2ac2.6572, MTU not set
        IP address unassigned
<SNIP>
  Redundancy Information:
        Member Ethernet0/3(Active), Ethernet0/2
```

```
ASA-001fw# sh interface redundant 2.16
Interface Redundant2.16 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 100 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 0066.0066.0066, MTU 1500
        IP address 192.168.60.10, subnet mask 255.255.255.0
<SNIP>
ASA-001fw# sh interface redundant 2.18
Interface Redundant2.18 "Dmz2", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 100 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 0088.0088.0088, MTU 1500
        IP address 192.168.80.10, subnet mask 255.255.255.0
<SNIP>
```

We can test connectivity with simple ping tests. Keep in mind here that you don't have any routing enabled, so keep it simple and just test to what is directly connected.

```
ASA-001fw# ping 192.168.60.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.60.6, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-001fw# ping 192.168.70.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-001fw# ping 192.168.80.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.80.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-001fw# ping 45.45.45.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-001fw# ping 45.45.45.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Notes

This task focuses on basic initialization of the ASA1 such that traffic can pass through the ASA. Interfaces can be physical or logical. Here we have used redundant interface. This is a logical grouping of a pair of similar interfaces to provide interface redundancy. Each interface in a redundant interface is known as member interface. When one member interface goes down the other member interface takes over. However note that there is no pre-emption for the member interface. Hence always one interface is active and the other in standby state. When we create the redundant interface, the first configured member interface becomes the active interface and hence even the MAC address is derived from that interface. We can use any virtual mac-address for the redundant interface. Using a privilege exec command we can change the state of an interface from standby to active. (redundant-interface redundant <> active-member Ethernet <>). However this will not survive a reboot. Redundant interface can be split into multiple logical VLAN interfaces.

Management interface can be converted to a data interface by using “no-management only” command. However this is not the best practice. Any interface can be converted to a management interface by using “Management-only” command. Hence any traffic that needs to pass through the firewall gets dropped automatically. You can have upto 8 redundant interfaces. Redundant interface configuration must be configured manually on the ASA’s when used as a failover interface.

Lab 2: ASA IPv4 Unicast Routing Overview

Lab 2: ASA IPv4 Unicast Routing– This lab is intended to let you be familiar with IPv4 unicast routing on the ASA in routed mode. Lab 2 focuses on configuring dynamic routing protocols on the ASA like OSPFv2, RIPv2, and EIGRP. Static routing with route tracking will also be part of the configuration tasks along with route manipulations.

General Rules

- By now you should have understood the physical and logical topology.
- Double-check and save your configurations before you perform Lab 2.
- Read tasks very carefully to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 2 Hours

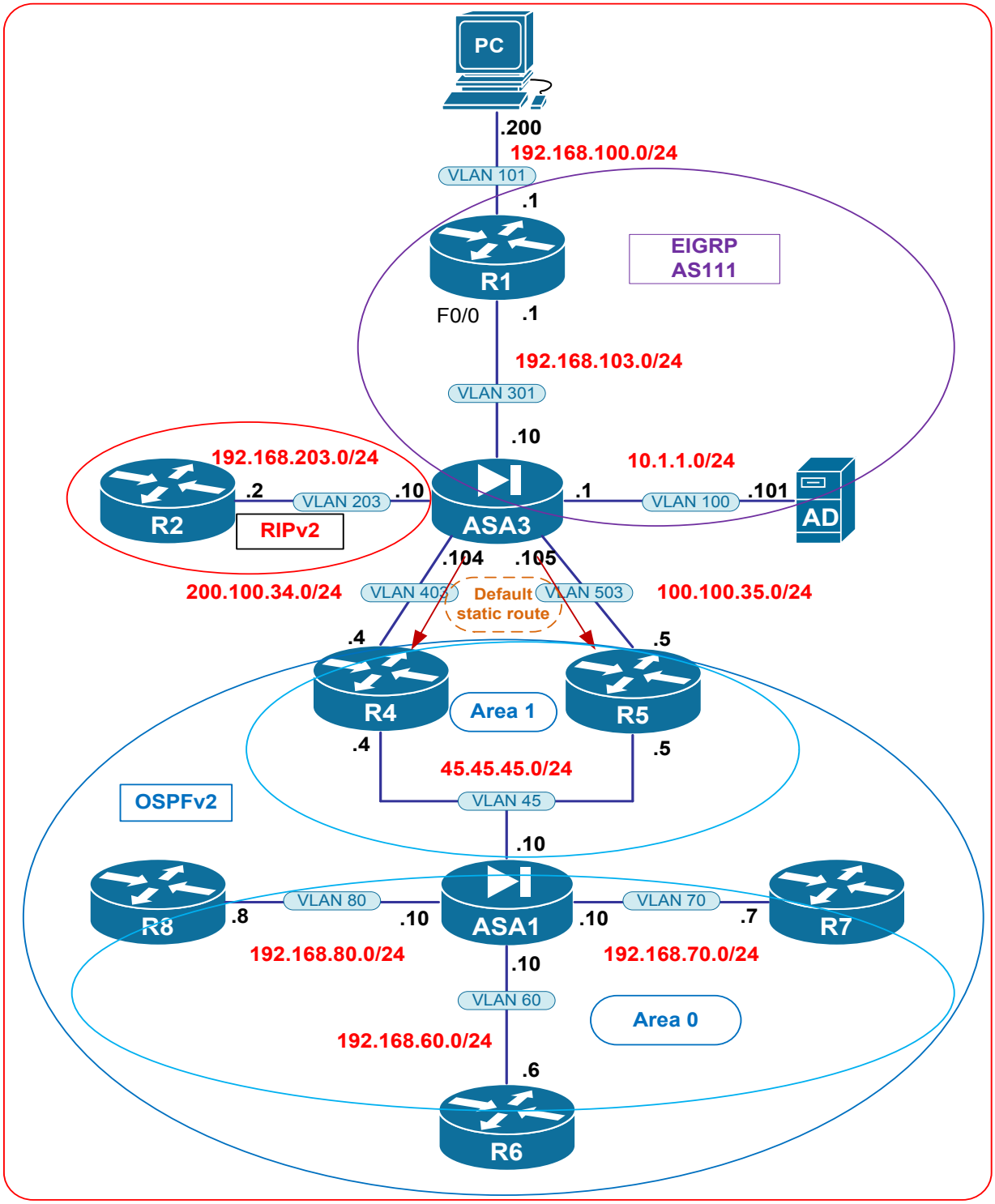
Pre-setup

This lab builds on the previous Lab 1. You must complete Lab 1 prior to starting this lab.

NOTE: Routing has been pre-configured on the routers

Use the logical topology drawing – Network Topology to understand how routing should occur and also refer to the general physical connectivity. Ensure that Lab 1 was successfully completed and verified using DSG. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below. Study the IP address table of routers and the routing topology diagram carefully.

Network Topology 1.1 (Logical)



LAB 2: IP Address Table of Routers

Router	Interface	IP Address
R1	F0/0	192.168.103.1/24
R1	F0/1	192.168.100.1/24
R1	Lo0	1.1.1.1/24
R1	Lo1	11.11.11.11/32
R2	G0/0	192.168.203.2/24
R2	Lo0	2.2.2.2/24
R2	Lo1	22.22.22.22/32
R4	F0/0	200.100.34.4/24
R4	F0/1	45.45.45.4/24
R4	Lo0	4.4.4.4/24
R4	Lo1	44.44.44.44/32
R5	F0/0	100.100.35.5/24
R5	F0/1	45.45.45.5/24
R5	Lo0	5.5.5.5/24
R5	Lo1	55.55.55.55/32
R6	F0/0	192.168.60.6/24
R6	Lo0	6.6.6.6/24
R6	Lo1	66.66.66.66/32
R7	F0/0	192.168.70.7/24
R7	Lo0	7.7.7.7/24
R7	Lo1	77.77.77.77/32
R8	F0/0	192.168.80.8/24
R8	Lo0	8.8.8.8/24
R8	Lo1	88.88.88.88/32

Detailed Solution:Lab-2

Task 1: Static Routes on ASA-3 for internal networks

- Configure appropriate static routes on ASA-003fw for all the internal networks (i.e. the inside and DMZs). Ensure you create static routes to the IP's of Loopback 0 and Loopback 1 configured on R1 and R2. Ensure that you can ping the Test PC and all the internal IPs.

Task-1:Solutions

Step 1: Configure static routes in the global config mode. Check the IP address table and verify the pre-loaded configurations on the routers.

```
route INSIDE 192.168.100.0 255.255.255.0 192.168.103.1
route INSIDE 1.1.1.0 255.255.255.0 192.168.103.1
route INSIDE 11.11.11.11 255.255.255.255 192.168.103.1
route dmz1 2.2.2.0 255.255.255.0 192.168.203.2
route dmz1 22.22.22.22 255.255.255.255 192.168.203.2
```

Verification

Step 1: Verify the static routes in the routing table

```
SA-003fw(config)# sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

S     1.1.1.0 255.255.255.0 [1/0] via 192.168.103.1, INSIDE
S     2.2.2.0 255.255.255.0 [1/0] via 192.168.203.2, dmz1
C     100.100.35.0 255.255.255.0 is directly connected, Outside-2
C     200.100.34.0 255.255.255.0 is directly connected, Outside-1
S     22.22.22.22 255.255.255.255 [1/0] via 192.168.203.2, dmz1
C     10.1.1.0 255.255.255.0 is directly connected, dmzserver
C     192.168.203.0 255.255.255.0 is directly connected, dmz1
S     11.11.11.11 255.255.255.255 [1/0] via 192.168.103.1, INSIDE
C     192.168.1.0 255.255.255.0 is directly connected, management
C     192.168.103.0 255.255.255.0 is directly connected, INSIDE
S     192.168.100.0 255.255.255.0 [1/0] via 192.168.103.1, INSIDE
```

Step 2: Ping the remote network to verify connectivity

```
ASA-003fw(config)# ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-003fw(config)# ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-003fw(config)# ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-003fw(config)# ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-003fw(config)# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Notes

Configuring IPv4 static route is very straight forward. Below is the command syntax for configuring static route

route interface *ip_address netmask gateway_ip* [distance]

Although we have not yet started with NAT configuration, it is however good to know how routing works on the ASA and its interaction with NAT.

By default the ASA uses both routing table and the XLATE table for routing decision. As we know routing is based on the destination IP.

There are 2 steps involved for forwarding IP packets – 1) Select egress interface and then 2) select the appropriate next hop

Step-1: Egress interface selection process summary –

- If the destination IP is present in the XLATE table or a static entry exists, the egress interface is selected based on XLATE entry and not the routing table.
- If no translations exist then the routing table is used for egress interface determination.

Step-2: Next Hop Selection Process

- Only after egress interface is determined, the ASA performs additional route lookup to find out the best next hop. Not all the configured static routes are used for next hop determination. But only a sub-set of routes associated to that particular egress interface are used for next hop determination.
- Packet will be forwarded after the next-hop determination for that destination IP, else ASA will drop the packet and generate a syslog message (id-110001)
- Example - Suppose the XLATE process determined DMZ1 interface as egress and the route configured for the next hop for the destination IP belongs to a different interface, assume DMZ2. In this case ASA drops the packet since no routes were present for that particular destination IP in routes associated with DMZ1. Hence loadsharing can only happen only on multiple next hops belonging to routes on the same egress interface and it can never load sharing cannot occur across multiple egress interfaces.

Task 2: Floating static default routes with object tracking

- Configure floating static default routes towards R4 and R5 on ASA-003fw. The ASA should pick R4 as the primary default gateway and R5 as the backup default gateway. Use SLA with object tracking to accomplish this task.
- The ASA should send 3 ICMP SLA packets on every 5 seconds interval/SLA operation. Set the timeout value and the threshold to 1000 milliseconds for the ICMP Echo reply. The ASA should track R4's Fa0/1 interface address for reachability.
- SLA monitor scheduling should start immediately. Use an SLA monitor ID of 111 and a track-id of 11.

Task-2: Solutions

Step 1: Configure SLA process and start the SLA process

```
sla monitor 111
 type echo protocol ipIcmpEcho 45.45.45.4 interface Outside-1
 num-packets 3
 timeout 1000
 threshold 1000
 frequency 5

sla monitor schedule 111 life forever start-time now
```

Step 2: Associate the SLA monitoring process with a route tracking ID/object.

```
track 11 rtr 111 reachability
```

Step 3: Configure primary static default route and associate with the tacking ID.

```
route Outside-1 0.0.0.0 0.0.0.0 200.100.34.4 1 track 11
```

Step 4: Configure backup/floating static default route with a higher admin distance.

```
route Outside-2 0.0.0.0 0.0.0.0 100.100.35.5 222
```

Verification

Step 1: Verify the static routes in the routing table

```
ASA-003fw(config)# sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 200.100.34.4 to network 0.0.0.0

S    1.1.1.0 255.255.255.0 [1/0] via 192.168.103.1, INSIDE
S    2.2.2.0 255.255.255.0 [1/0] via 192.168.203.2, dmz1
C    100.100.35.0 255.255.255.0 is directly connected, Outside-2
C    200.100.34.0 255.255.255.0 is directly connected, Outside-1
S    22.22.22.22 255.255.255.255 [1/0] via 192.168.203.2, dmz1
C    10.1.1.0 255.255.255.0 is directly connected, dmzserver
C    192.168.203.0 255.255.255.0 is directly connected, dmz1
S    11.11.11.11 255.255.255.255 [1/0] via 192.168.103.1, INSIDE
C    192.168.1.0 255.255.255.0 is directly connected, management
C    192.168.103.0 255.255.255.0 is directly connected, INSIDE
S    192.168.100.0 255.255.255.0 [1/0] via 192.168.103.1, INSIDE
S*   0.0.0.0 0.0.0.0 [1/0] via 200.100.34.4, Outside-1
```

Step 2: Verify SLA monitor configuration

```
ASA-003fw(config)# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 111
Owner:
Tag:
Type of operation to perform: echo
Target address: 45.45.45.4
Interface: Outside-1
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 5
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
ASA-003fw(config)# show sla monitor operational-state
Entry number: 111
Modification time: 08:13:00.103 UTC Tue Feb 5 2013
Number of Octets Used by this Entry: 2056
Number of operations attempted: 33
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 08:15:40.103 UTC Tue Feb 5 2013
Latest operation return code: OK
RTT Values:
RTTAvg: 1   RTTMin: 1   RTTMax: 1
NumOfRTT: 3 RTTSum: 3   RTTSum2: 3
```

Step 3: Verify Object Tracking

```
ASA-003fw(config)# sh track 11
Track 11
  Response Time Reporter 111 reachability
  Reachability is Up
  1 change, last change 00:02:27
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

Step 4: Verify if backup route works. Shutdown F0/1 on R4 and verify. Make sure to unshut the interface after verification.

```
R4(config)#interface f0/1
R4(config-if)#shutdown
```

```
ASA-003fw(config)# show track 11
Track 11
  Response Time Reporter 111 reachability
  Reachability is Down
  3 changes, last change 00:00:37
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

```
ASA-003fw(config)# sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 100.100.35.5 to network 0.0.0.0

S    1.1.1.0 255.255.255.0 [1/0] via 192.168.103.1, INSIDE
S    2.2.2.0 255.255.255.0 [1/0] via 192.168.203.2, dmz1
C    100.100.35.0 255.255.255.0 is directly connected, Outside-2
C    200.100.34.0 255.255.255.0 is directly connected, Outside-1
S    22.22.22.22 255.255.255.255 [1/0] via 192.168.203.2, dmz1
C    10.1.1.0 255.255.255.0 is directly connected, dmzserver
C    192.168.203.0 255.255.255.0 is directly connected, dmz1
S    11.11.11.11 255.255.255.255 [1/0] via 192.168.103.1, INSIDE
C    192.168.103.0 255.255.255.0 is directly connected, INSIDE
S    192.168.100.0 255.255.255.0 [1/0] via 192.168.103.1, INSIDE
S*   0.0.0.0 0.0.0.0 [222/0] via 100.100.35.5, Outside-2
```

Notes

The configuration seen here uses the Static Route Tracking, Service Level Agreement (SLA) monitor process. The ASA associates a static route with a target that you define and then it monitors it using ICMP. If an echo reply is not received, the object is considered down, and the associated route is removed from the routing table. Then the previously configured “backup” route is used in place of the route that is removed. While the backup route is in use, the SLA monitor operation continues to try to reach the monitoring target. Once the target is available again, the first route is replaced in the routing table, and the backup route is removed. This doesn’t require any special configuration to replace the primary route because its chosen based

on its metric, which is why the secondary route uses a metric that is higher. If they were the same you would load balance rather than chose a primary.

When you access the sla monitor you configure the timeout and frequency before you schedule it. Once its scheduled you have to stop it to change the timers. Refer to the ASA documentation for more information.

Task 3: OSPFv2 on the ASA

- Configure OSPFv2 on ASA-001fw. The Router-ID should be configured as 11.45.45.11. The outside interface should be in Area 1 and the internal interfaces (i.e. DMZs and inside interfaces) should be in Area 0.
- Authenticate all the adjacencies with MD5 authentication. They key number should be 1 and the pre-shared secret key should be "C1SC0I23".
- Network statements should be as specific as possible.
- Do not advertise the R6 Loopback1 interface into OSPF area 1.
- Routers have been pre-configured. No additional configurations are required on the routers. Do not modify any configurations on the routers.
- Ensure you are able to ping the Loopbacks on R6, R7, R8, R4, R5, and the outside interfaces of ASA-003fw.

Task-3

Step 1: Configure OSPF on ASA1

```
router ospf 1
 router-id 11.45.45.11
 network 45.45.45.10 255.255.255.255 area 1
 network 192.168.60.10 255.255.255.255 area 0
 network 192.168.70.10 255.255.255.255 area 0
 network 192.168.80.10 255.255.255.255 area 0
 area 0 range 66.66.66.66 255.255.255.255 not-advertise

interface Management0/0
  ospf message-digest-key 1 md5 C1SC0I23
  ospf authentication message-digest

interface Redundant1
 ospf message-digest-key 1 md5 C1SC0I23
 ospf authentication message-digest

interface Redundant2.16
 ospf message-digest-key 1 md5 C1SC0I23
 ospf authentication message-digest

interface Redundant2.18
 ospf message-digest-key 1 md5 C1SC0I23
 ospf authentication message-digest
```

Verification

Step 1: Verify the OSPF neighbor state.

```
ASA-001fw(config)# show ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
7.7.7.7           1   FULL/BDR        0:00:36     192.168.70.7    DMZ1
6.6.6.6           1   FULL/BDR        0:00:30     192.168.60.6    inside
8.8.8.8           1   FULL/BDR        0:00:31     192.168.80.8    Dmz2
4.4.4.4           1   FULL/BDR        0:00:36     45.45.45.4      OUTSIDE
5.5.5.5           1   FULL/DROTHER    0:00:33     45.45.45.5      OUTSIDE
```

Step 2: Verify the routes on ASA1. Routers have been pre-configured.

```
ASA-001fw(config)# sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O E1 1.1.1.0 255.255.255.0 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O E1 2.2.2.0 255.255.255.0 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O    100.100.35.0 255.255.255.0 [110/11] via 45.45.45.5, 0:02:13, OUTSIDE
C    192.168.60.0 255.255.255.0 is directly connected, inside
O    4.4.4.0 255.255.255.0 [110/11] via 45.45.45.4, 0:02:13, OUTSIDE
O    55.55.55.55 255.255.255.255 [110/11] via 45.45.45.5, 0:02:13, OUTSIDE
O    200.100.34.0 255.255.255.0 [110/11] via 45.45.45.4, 0:02:13, OUTSIDE
O    5.5.5.0 255.255.255.0 [110/11] via 45.45.45.5, 0:02:13, OUTSIDE
O    66.66.66.66 255.255.255.255 [110/11] via 192.168.60.6, 0:05:42, inside
O    6.6.6.0 255.255.255.0 [110/11] via 192.168.60.6, 0:05:42, inside
O E1 22.22.22.22 255.255.255.255 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O    7.7.7.0 255.255.255.0 [110/11] via 192.168.70.7, 0:05:42, DMZ1
O    8.8.8.0 255.255.255.0 [110/11] via 192.168.80.8, 0:05:42, Dmz2
C    192.168.80.0 255.255.255.0 is directly connected, Dmz2
O    77.77.77.77 255.255.255.255 [110/11] via 192.168.70.7, 0:05:42, DMZ1
O E1 10.1.1.0 255.255.255.0 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O E1 192.168.203.0 255.255.255.0 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O E1 11.11.11.11 255.255.255.255 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O    88.88.88.88 255.255.255.255 [110/11] via 192.168.80.8, 0:05:42, Dmz2
O E1 192.168.103.0 255.255.255.0 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
O    44.44.44.44 255.255.255.255 [110/11] via 45.45.45.4, 0:02:13, OUTSIDE
C    192.168.70.0 255.255.255.0 is directly connected, DMZ1
O E1 192.168.100.0 255.255.255.0 [110/12] via 45.45.45.4, 0:02:13, OUTSIDE
C    45.45.45.0 255.255.255.0 is directly connected, OUTSIDE
```

Notes

In this task type-3 LSA filter is done by “area range” with “not-advertise” keywork since 66.66.66.66/32 is considered a loopback network. In order to use filter-lists you may have to change the network type on R6 Lo1 to point-point.

Authentication can be done on per interface or area level.

ASA supports upto 2 OSPF processes and can keep the routes separate between the two processes. We can redistribute between the processes to send routes across.

The ASA supports many of protocol features similar to the IOS. You may refer the documentation for more information.

Task 4: EIGRP on ASA

- Remove all the static routes pointing to the internal networks (i.e. DMZs and inside on ASA-003fw). Do not remove the default floating static routes and the SLA configurations.
- Configure EIGRP AS 111 between R1 and ASA-003fw. Advertise the dmzserver interface into EIGRP but a neighbour relationship should not be formed on that interface if a router is attached to that segment.
- Network statements should be as specific as possible and you should disable automatic summarization behaviour.
- The EIGRP adjacency between R1 and ASA should be authenticated using an MD5 password. R1 is already configured with the appropriate key-chain and password. Configure the same authentication parameters on ASA-003fw.
- The ASA should send only a default route to R1. Change the admin distance of the Null route to 250.
- Do not modify any configuration on R1.
- Ensure ASA can ping all of the inside networks including the test PC.

Task-4: Solutions

Step 1: Remove the static routes and configure EIGRP on ASA3.

```
no route INSIDE 192.168.100.0 255.255.255.0 192.168.103.1
no route INSIDE 1.1.1.0 255.255.255.0 192.168.103.1
no route INSIDE 11.11.11.11 255.255.255.255 192.168.103.1
no route dmz1 2.2.2.0 255.255.255.0 192.168.203.2
no route dmz1 22.22.22.22 255.255.255.255 192.168.203.2

router eigrp 111
 no auto-summary
 eigrp router-id 133.133.133.133
 network 10.1.1.1 255.255.255.255
 network 192.168.103.10 255.255.255.255
 passive-interface dmzserver

interface GigabitEthernet0/1
 authentication key eigrp 111 CISC0I123 key-id 10
 authentication mode eigrp 111 md5
 summary-address eigrp 111 0.0.0.0 0.0.0.0 250
```

Verification

Step 1: Verify the EIGRP neighbor state.

```
ASA-003fw(config)# sh eigrp 111 neighbors
EIGRP-IPv4 neighbors for process 111
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.103.1           Gi0/1            10  00:15:28 2    200  0   14
```

Step 2: Verify the EIGRP topology table and routing table.

```
ASA-003fw(config)# sh eigrp 111 topology

EIGRP-IPv4 Topology Table for AS(111)/ID(133.133.133.133)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 11.11.11.11 255.255.255.255, 1 successors, FD is 130816
        via 192.168.103.1 (130816/128256), GigabitEthernet0/1
P 0.0.0.0 0.0.0.0, 1 successors, FD is 2816
        via Summary (2816/0), Null0
P 1.1.1.0 255.255.255.0, 1 successors, FD is 130816
        via 192.168.103.1 (130816/128256), GigabitEthernet0/1
P 10.1.1.0 255.255.255.0, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/2.222
P 192.168.100.0 255.255.255.0, 1 successors, FD is 28416
        via 192.168.103.1 (28416/28160), GigabitEthernet0/1
```

```
P 192.168.103.0 255.255.255.0, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/1
```

```
ASA-003fw(config)# sh route INSIDE
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 200.100.34.4 to network 0.0.0.0
D    1.1.1.0 255.255.255.0 [90/130816] via 192.168.103.1, 0:15:46, INSIDE
D    11.11.11.11 255.255.255.255
           [90/130816] via 192.168.103.1, 0:15:46, INSIDE
C    192.168.103.0 255.255.255.0 is directly connected, INSIDE
D    192.168.100.0 255.255.255.0 [90/28416] via 192.168.103.1, 0:15:46,INSIDE
```

Step 3: Ping the INSIDE networks to ensure reachability.

```
ASA-003fw(config)# ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-003fw(config)# ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-003fw(config)# ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Task 5: RIPv2 on the ASA

- Configure RIPv2 between the ASA3 and R2.
- Ensure that RIPv2 update packets are sent only over the DMZ1 interface and disable automatic summarization.
- The RIPv2 adjacency should be authenticated using MD5. R1 is preconfigured with the appropriate keychain and MD5 password. Configure the same authentication parameters on ASA-003fw.
- Redistribute EIGRP AS 111 into RIPv2.
- ASA-003fw should advertise a default route to R2.
- Do not modify any configuration on R2.
- Ensure the ASA can ping all the Loopback networks on R2.

Task-5: Solutions

Step 1: Configure RIPv2 on ASA3

```
router rip
 network 192.168.203.0
 passive-interface default
 no passive-interface dmz1
 redistribute eigrp 111 metric 2
 default-information originate
 version 2
 no auto-summary


interface GigabitEthernet0/2.2
 rip authentication mode md5
 rip authentication key C1SC0123 key_id 1
```

Verification

Step 1: Verify the routing table for DMZ1 interface.

```
ASA-003fw(config)# sh route dmz1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 200.100.34.4 to network 0.0.0.0

R     2.2.2.0 255.255.255.0 [120/1] via 192.168.203.2, 0:00:20, dmz1
R     22.22.22.22 255.255.255.255 [120/1] via 192.168.203.2, 0:00:20, dmz1
C     192.168.203.0 255.255.255.0 is directly connected, dmz1
```

Step 2: Verify the RIP database to check the received routes and also to check if redistribution and summarization is working.

```
ASA-003fw(config)# sh rip database

0.0.0.0 0.0.0.0    auto-summary
0.0.0.0 0.0.0.0    redistributed
```

```
    [0] via 0.0.0.0,
1.0.0.0 255.0.0.0    auto-summary
1.1.1.0 255.255.255.0    redistributed
    [2] via 192.168.103.1,
2.0.0.0 255.0.0.0    auto-summary
2.2.2.0 255.255.255.0
    [1] via 192.168.203.2, 0:00:17, GigabitEthernet0/2.2
10.0.0.0 255.0.0.0    auto-summary
10.1.1.0 255.255.255.0    redistributed
    [1] via 0.0.0.0,
11.0.0.0 255.0.0.0    auto-summary
11.11.11.11 255.255.255.255    redistributed
    [2] via 192.168.103.1,
22.0.0.0 255.0.0.0    auto-summary
22.22.22.22 255.255.255.255
    [1] via 192.168.203.2, 0:00:17, GigabitEthernet0/2.2
192.168.100.0 255.255.255.0    auto-summary
192.168.100.0 255.255.255.0    redistributed
    [2] via 192.168.103.1,
192.168.103.0 255.255.255.0    auto-summary
192.168.103.0 255.255.255.0    redistributed
    [1] via 0.0.0.0,
192.168.203.0 255.255.255.0    auto-summary
192.168.203.0 255.255.255.0    directly connected, GigabitEthernet0/2.2
```

Step 3: Ping the DMZ1 networks to ensure reachability.

```
ASA-003fw(config)# ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms

ASA-003fw(config)# ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Task 6: DMZ Communication

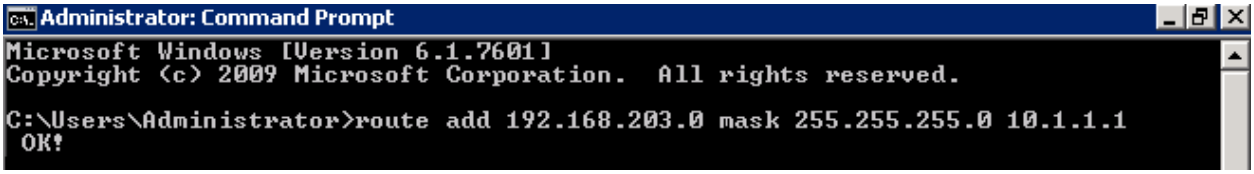
- Configure ASA-003fw such that the R2 Fa0/0 interface can ping the AD server.
- Do not use ACLs to accomplish this task.
- You can add a single static route on the AD Server to accomplish this

Task-6: Solutions

Step 1: Configure same-security-level configuration on ASA3

```
same-security-traffic permit inter-interface
```

Step 2: Configure a static route on the AD for DMZ1 network. You will lose your RDP access if you set the default gateway.

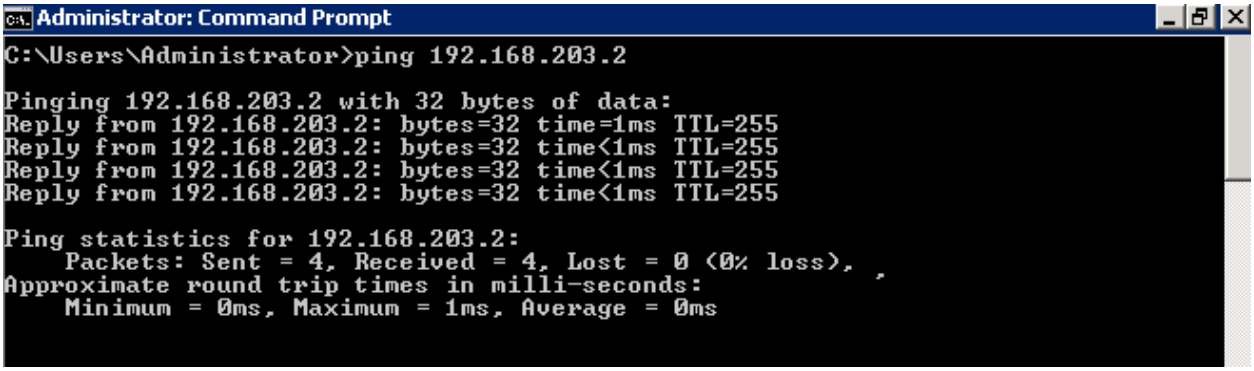


Verification

Step 1: Ping from R2 to the AD.

```
R2#ping 10.1.1.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Step 2: Ping from the AD to R2



Notes

In this lab if you had not changed the admin distance of summary null route generated by EIGRP to 250 or above 222, then the route tracking and the floating static default route would not work correctly because EIGRP summary null route has an admin distance of 5.

The "passive-interface <nameif/int>"command is used in many dynamic routing protocols to disable sending updates or neighbor hello packets out from a specific interface or all interfaces. The behavior of this command is protocol specific.

In RIPv2 this command will disable sending multicast updates on a specific interface. When this command is used in conjunction with "default" keyword then RIP process disables sending multicast updates on all the interfaces. You can use "no passive-interface <Interface>" to send multicast updates out of a specific interface.

However the router can receive incoming updates from other RIP speaking neighbors and install in the routing table when "passive-interface" command is used. You can use "passive-interface default" and in conjunction with neighbor command to send updates to a particular neighbor as unicast.

In EIGRP the "passive-interface" command stops sending filters out hello packets. Hence neighbor relationship is not formed. Hence no routes are sent or received. You may use the neighbor command to send unicast update to a specific neighbor.

The "passive-interface" command in OSPF stops sending the OSPF hello packets. Hence no neighbor relation is formed. Without a neighbor relationship, routes cannot be received and installed in the routing table. This behavior is similar to EIGRP.

Remember the authentication key and key ID must match for RIP and EIGRP between neighbors.

Lab 3 ASA System Management and IP Services

Lab 3: ASA System Management and IP Services – This lab is intended to let you be familiar with configuring necessary system management and IP services on the ASA. This lab scenario will focus on configuring NTP, DNS, DHCP Server, DHCP Relay, Logging services, SNMPv3, SNMPv2c, and Management Access.

General Rules

- By now you should have understood the logical topology well and established routing.
- Double-check and save your configurations before you perform Lab 3.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 2 Hours

Pre-setup

This lab builds on the previous Lab 2. If you have skipped lab 2, load Initial Configuration for lab 1 (called “labs 1-4”) and then download final configurations for Lab 2. Copy them to the ASA1 and ASA3.

Use the logical topology drawing – Network Topology 1.1. Ensure that Lab 2 was successfully completed and verified using DSG. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below. Ensure that routes are present on the ASAs in the routing table based on Lab 2.

Detailed Solution: Lab-3

Task 1: NTP server and client configuration on ASA-3 and R4

- Configure R4 as the NTP server and ASA-003fw as the NTP client.
- R4 and ASA-003fw should be in the same time zone of PST -8.
- The NTP protocol should use MD5 authentication with a key-id of 1 and password of 1PXP3RT.

Task-1:Solutions

Step 1: On R4 configure the timezone and change the clock settings.

```
clock timezone PST -8    → (Global Config)

clock set (hh:mm:ss)(DAY<1-31>)(MONTH)(YEAR)   → (privilege exec mode)
```

Step 2: Configure R4 as the NTP server

```
ntp authentication-key 1 md5 1PXP3RT
ntp authenticate
ntp trusted-key 1
ntp master
```

Step 3: Configure ASA3 as the NTP client

```
ntp authentication-key 1 md5 1PXP3RT
ntp authenticate
ntp trusted-key 1
ntp server 200.100.34.4 key 1 prefer

clock timezone PST -8
```

Verification

Step 1: Verify NTP status and association on ASA3

```
ASA-003fw(config)# show ntp status
Clock is synchronized, stratum 9, reference is 200.100.34.4
nominal freq is 99.9984 Hz, actual freq is 100.0050 Hz, precision is 2**6
reference time is  d4fd4f90.a0e0f2a7 (15:10:13.628 PST Wed Feb 6 2013)
<SNIP>

ASA-003fw(config)# show ntp associations detail
200.100.34.4 configured, authenticated, our_master, sane, valid, stratum 8
ref ID 127.127.1.1, time d4fd4fc7.6e779150 (15:10:14.431 PST Wed Feb 6 2013)
```

```
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
<SNIP>
```

Task 2: NTP server and client configuration on ASA-1 and R5

- Configure R5 as the NTP server and ASA-001fw as the NTP client.
- R4 and ASA-001fw should be in the same time zone of IST 5:30.
- The NTP protocol should use MD5 authentication with a key-id of 1 and password of 1PXP3RT.

Task-2:Solutions

Step 1: On R5 configure the timezone and change the clock settings.

```
clock timezone IST 5 30    → (Global Config)

clock set (hh:mm:ss)(DAY<1-31>)(MONTH)(YEAR)   → (privilege exec mode)
```

Step 2: Configure R5 as the NTP server

```
ntp authentication-key 1 md5 1PXP3RT
ntp authenticate
ntp trusted-key 1
ntp master
```

Step 3: Configure ASA1 as the NTP client

```
ntp authentication-key 1 md5 1PXP3RT
ntp authenticate
ntp trusted-key 1
ntp server 45.45.45.5 key 1 prefer

clock timezone IST 5 30
```

Verification

Step 1: Verify NTP status and association on ASA1

ASA-001fw(config)# sh ntp status
Clock is synchronized, stratum 9, reference is 45.45.45.5
nominal freq is 99.9984 Hz, actual freq is 99.9969 Hz, precision is 2**6
reference time is d4bca4a9.ba638b47 (15:15:13.728 IST Wed Feb 6 2013)
<SNIP>

ASA-001fw(config)# sh ntp associations detail

45.45.45.5 configured, authenticated, our_master, sane, valid, stratum 8
ref ID 127.127.1.1, time d4bca4a0.cec9b5aa (15:15:04.807 IST Wed Feb 6 2013)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
<SNIP>

Task 3: DNS configuration on ASA-3

- Configure ASA-003fw to perform DNS lookups. The DNS server IP address is 10.1.1.101.

Task-3:Solutions

Step 1: Configure DNS lookup on ASA3

```
dns domain-lookup dmzserver
DNS server-group DefaultDNS
    name-server 10.1.1.101
    domain-name ipexpert.com
```

Verification

Step 1: Ping using host names and verify using show dns-host command

```
ASA-003fw# ping www.ipexpert.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA-003fw# ping www.google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms


ASA-003fw# sh dns-host

Host                      Flags       Age Type   Address(es)
www.google.com            (temp, OK)  0    IP    10.1.1.101
www.ipexpert.com          (temp, OK)  0    IP    10.1.1.101
```

Task 4: DHCP server configuration on ASA-3

- Configure ASA-003fw as a DHCP server to provide IP addresses on the dmz1 interface.
- The DHCP scope should be 192.168.203.100 – 192.168.203.200.
- DNS, WINS, and the TFTP server IP address should be 10.1.1.101.
- The domain name should be ipexpert.com.
- The default gateway should be the IP address of the dmz1 interface.
- The lease should be set to 2 hours.
- ASA-003fw should send ICMP packets before IP address assignment to clients. The timeout value should be 60 milliseconds.

Task-4:Solutions

Step 1: Configure DHCP server on ASA3

```
dhcpd ping_timeout 60
dhcpd domain ipexpert.com
dhcpd option 3 ip 192.168.203.10
dhcpd option 150 ip 10.1.1.101
!
dhcpd address 192.168.203.100-192.168.203.200 dmz1
dhcpd dns 10.1.1.101 interface dmz1
dhcpd wins 10.1.1.101 interface dmz1
dhcpd enable dmz1
```

Verification

Step 1: Configure R2 G0/0 to obtain an ip address using DHCP and after verification re-configure back the IP address of R2 (192.168.203.2)

```
R2(config)#int g0/0
R2(config-if)#ip address dhcp
*Feb  2  12:00:44.191:  %DHCP-6-ADDRESS_ASSIGN:  Interface  GigabitEthernet0/0
assigned DHCP address 192.168.203.100, mask 255.255.255.0, hostname R2
```

```
ASA-003fw(config)# show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

192.168.203.100  0063.6973.636f.2d30.           3123 seconds    Automatic
                 3031.622e.6434.6139.
                 2e65.6336.302d.4769.
                 302f.30
```

```
ASA-003fw(config)# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools         2
Automatic bindings    1
Expired bindings      2
Malformed messages    0
Message               Received
BOOTREQUEST           0
DHCPDISCOVER          387
DHCPREQUEST           393
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             387
DHCPACK               383
DHCPNAK               10
```

```
ASA-003fw(config)# sh dhcpd state
Context  Configured as DHCP Server
Interface INSIDE, Not Configured for DHCP
Interface dmz1, Configured for DHCP SERVER
Interface dmzserver, Not Configured for DHCP
Interface management, Not Configured for DHCP
Interface Outside-1, Not Configured for DHCP
Interface Outside-2, Not Configured for DHCP
```

Task 5: DHCP relay services configuration on ASA-1

- Configure ASA-001fw as the DHCP relay agent for clients on the DMZ2 interface.
- The DHCP server IP address is 45.45.45.45 (TBC-10.1.1.101). Make sure the ASA changes the default gateway info to the DMZ2 interface IP address.
- Set the address negotiation timeout to 60 seconds

Task-5:Solutions

Step 1: Configure DHCP relay on ASA1

```
dhcprelay server 45.45.45.45 OUTSIDE
dhcprelay enable Dmz2
dhcprelay setroute Dmz2
dhcprelay timeout 60
```

Verification : This is a config only question. Hence make sure your configuration matches the solution.

```
ASA-001fw# sh dhcprelay state
Context  Configured as DHCP Relay
Interface OUTSIDE, Not Configured for DHCP
Interface DMZ1, Not Configured for DHCP
Interface inside, Not Configured for DHCP
Interface Dmz2, Configured for DHCP RELAY SERVER
```

Task 6: Logging configuration on ASA-3

- Create a log filter list to send all IKE, IPSec, and VPN client warning messages to a syslog server at 10.1.1.101.
- Send only critical EIGRP and RIP messages to the buffer and change the buffer size to 32768. Messages should be saved to the flash when the buffer gets full.
- Create a log filter list to send all failover related error messages to an email address of halogs@ipexpert.com from asa003fw@ipexpert.com. The SMTP server IP address is 10.1.1.101.
- Send debug messages to the ASDM. The ASA should buffer 300 messages.

Task-6:Solutions

Step 1: Enable logging

```
logging enable
```

Step 2: Create Logging lists

```
logging list IPSEC level warnings class vpn
logging list IPSEC level warnings class vpnc
logging list FAILOVER level errors class ha
```

Step 3: Send logs to syslog server.

```
logging host dmzserver 10.1.1.101
logging trap IPSEC
```

Step 4: Send logs buffer and change the buffer logging parameters

```
logging class rip buffered critical
logging class eigrp buffered critical
logging buffer-size 32768
logging flash-bufferwrap
```

Step 5: Send logs to ASDM

```
logging asdm debugging
logging asdm-buffer-size 300
```

Step 6: Send logs to email

```
logging mail FAILOVER
logging from-address asa003fw@ipexpert.com
logging recipient-address halogs@ipexpert.com level errors
smtp-server 10.1.1.101
```

Verification: This is a config only question. Hence make sure your configuration matches the solution.

```
ASA-003fw(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging:  class rip eigrp, 0 messages logged
    Trap logging: list IPSEC, facility 20, 0 messages logged
        Logging to dmzserver 10.1.1.101
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: list FAILOVER, 0 messages logged
    ASDM logging: level debugging, 36106 messages logged
```

Task 7: Logging configuration on ASA-1

- Configure ASA1 to send all warning messages to an internal syslog server. The IP address of the server is 192.168.60.100.
- The ASA should include timestamps and the hostname in the syslog messages.

Task-7:Solutions

Step 1: Enable logging

```
logging enable
```

Step 2: Configure syslog and other parameters and send the logs.

```
logging timestamp
logging trap warnings
logging device-id hostname
logging host inside 192.168.60.100
```

Verification : This is a config only question. Hence make sure your configuration matches the solution.

```
ASA-001fw(config)# sh logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level warnings, facility 20, 23 messages logged
        Logging to inside 192.168.60.100
    History logging: disabled
    Device ID: hostname "ASA-001fw"
    Mail logging: disabled
    ASDM logging: disabled
```

Task 8: SNMPv3 configuration on ASA-3

- Configure SNMPv3 to send all IKEv2, IPSec, and remote access traps to the SNMP server at 10.1.1.101.
- SNMPv3 messages should be authenticated with a password of C1SCO using the SHA algorithm.
- The SNMPv3 group is “IPXGROUP1”.
- Associate the SNMPv3 user “ADMIN” with the above referenced group.
- Set the location to SanJose.

Task-8:Solutions

Step 1: Enable SNMP server

```
snmp-server enable
```

Step 2: Configure SNMPv3 Group

```
snmp-server group IPXGROUP1 v3 auth
```

Step 3: Configure SNMPv3 user

```
snmp-server user ADMIN IPXGROUP1 v3 auth sha C1SCO
```

Step 4: Configure SNMPv3 server

```
snmp-server host dmzserver 10.1.1.101 version 3 ADMIN
```

Step 5: Configure location for SNMP

```
snmp-server location SanJose
```

Step 6: Configure SNMP traps

```
snmp-server enable traps ipsec start stop
snmp-server enable traps remote-access session-threshold-exceeded
snmp-server enable traps ikev2 start stop
```

Verification : This is a config only question. Hence make sure your configuration matches the solution.

```
ASA-003fw(config)# show snmp-server group

groupname : IPXGROUP1                          security model:v3 auth
readview   : def_read_view                            writeview : <no writeview
specified>
notifyview: def_notify_view
row status: active


ASA-003fw(config)# show snmp-server user
User name: ADMIN
Engine ID: 80000009fef5a095bb1eeb7a78140a71973c20da3583fa1c0e
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: IPXGROUP1
```

Task 9: SNMPv2c configuration on ASA-1

- Configure a global community string of "5ECURITY" and set the location to Moon.
- Only the NMS server IP of 192.168.60.100 can poll the ASA. Use a community string of "5ECUR1TY".
- Send all traps except syslog to 192.168.60.101. Use a community string of "5ECUR1TY".

Task-9:Solutions

Step 1: Enable SNMP server

```
snmp-server enable
```

Step 2: Configure global community string

```
snmp-server community 5ECURITY
```

Step 4: Configure SNMPv2c servers

```
snmp-server host inside 192.168.60.100 poll community 5ECUR1TY version 2c
snmp-server host inside 192.168.60.101 trap community 5ECUR1TY version 2c
```

Step 5: Configure location for SNMP

```
snmp-server location Moon
```

Step 6: Configure SNMP traps

```
snmp-server enable traps snmp authentication linkup linkdown coldstart
snmp-server enable traps ipsec start stop
snmp-server enable traps entity config-change fru-insert fru-remove
```

```
snmp-server enable traps remote-access session-threshold-exceeded
```

Verification : This is a config only question. Hence make sure your configuration matches the solution.

```
ASA-001fw(config)# show snmp-server statistics
0 SNMP packets input
<SNIP>
18 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    18 Trap PDUs
```

Task 10: Management access configuration on ASA-1 and ASA-3

- Configure ASDM and Telnet access on the inside interface from any hosts.
- Configure SSH access on the outside interface from any hosts for ASA-3.
- Configure SSH access on the outside interface to allow only 200.100.34.111 and 100.100.35.111 for ASA-1. (This will work after LAB 4 Translations/NAT).
- Change the Telnet password to "CC1EI23" on both the ASAs.
- Use SSH version 2 only.
- Configure the above tasks on both of the ASAs. You are allowed to modify the VLAN on the switch to test ASDM access. The test PC should be in VLAN 101 only.
- You may create any local user account using local AAA authentication to test on ASA-1. You may test this after the NAT and ACL configuration given in LAB 4.
- Test the ASDM access to ASA-3 from the test PC.

Task-10:Solutions

Step 1: Configure ASDM access and telnet for both ASA1 and ASA3

```
ASA1
asdm image disk0:/asdm-66114.bin
http server enable
http 0.0.0.0 0.0.0.0 inside
telnet 0.0.0.0 0.0.0.0 inside
```

ASA3

```
asdm image disk0:/asdm-66114.bin
http server enable
http 0.0.0.0 0.0.0.0 INSIDE
```

```
telnet 0.0.0.0 0.0.0.0 INSIDE
```

Step 2: Configure SSHv2 on ASA1 and ASA3

ASA1 and ASA3

```
crypto key generate rsa modulus 1024
ssh version 2
passwd CC1EI23


ASA3
ssh 0.0.0.0 0.0.0.0 Outside-1
ssh 0.0.0.0 0.0.0.0 Outside-2

ASA1
ssh 200.100.34.111 255.255.255.255 OUTSIDE
ssh 100.100.35.111 255.255.255.255 OUTSIDE
```

Step 3: Configure any local user and AAA local authentication on ASA1

```
username cisco password cisco
aaa authentication ssh console LOCAL
```

Verification

Step 1: Test telnet access on ASA3 from R1 (Inside)

```
R1#telnet 192.168.103.10
Trying 192.168.103.10 ... Open

User Access Verification

Password:
Type help or '?' for a list of available commands.
ASA-003fw> exit

Logoff

[Connection to 192.168.103.10 closed by foreign host]
```

Step 2: Test telnet access on ASA1 from R6 (Inside)

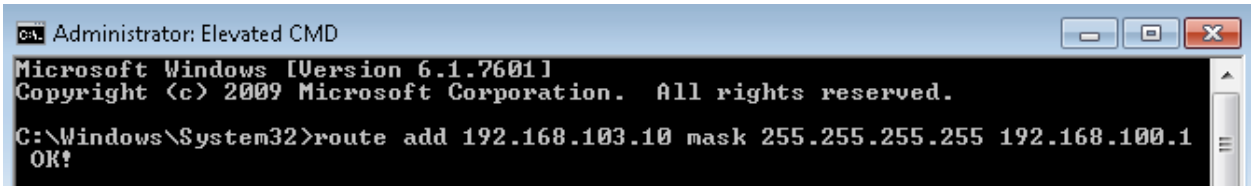
```
R6#telnet 192.168.60.10
Trying 192.168.60.10 ... Open

User Access Verification

Password:
```

```
Type help or '?' for a list of available commands.
ASA-001fw> exit

Logoff

[Connection to 192.168.60.10 closed by foreign host]
```

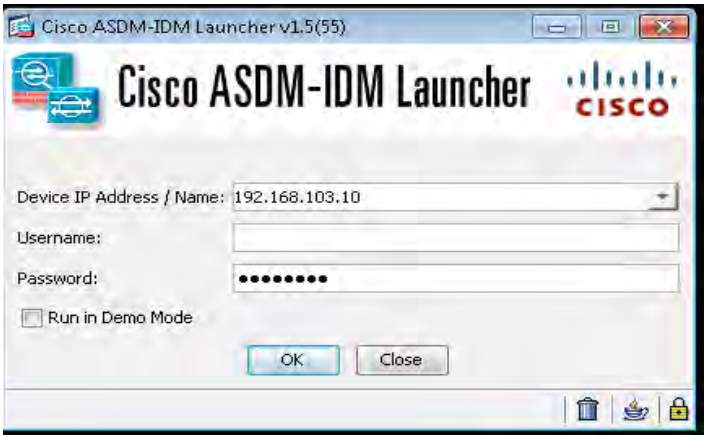
Step 3: Test ASDM and SSH access on ASA3. Configure Test-PC1 in VLAN 101. This PC is connectd to SW3 G1/0/2. Use any IP address for the Test-PC from VLAN101 range. Do not set the default gateway. Make sure you add static routes on the test PC.

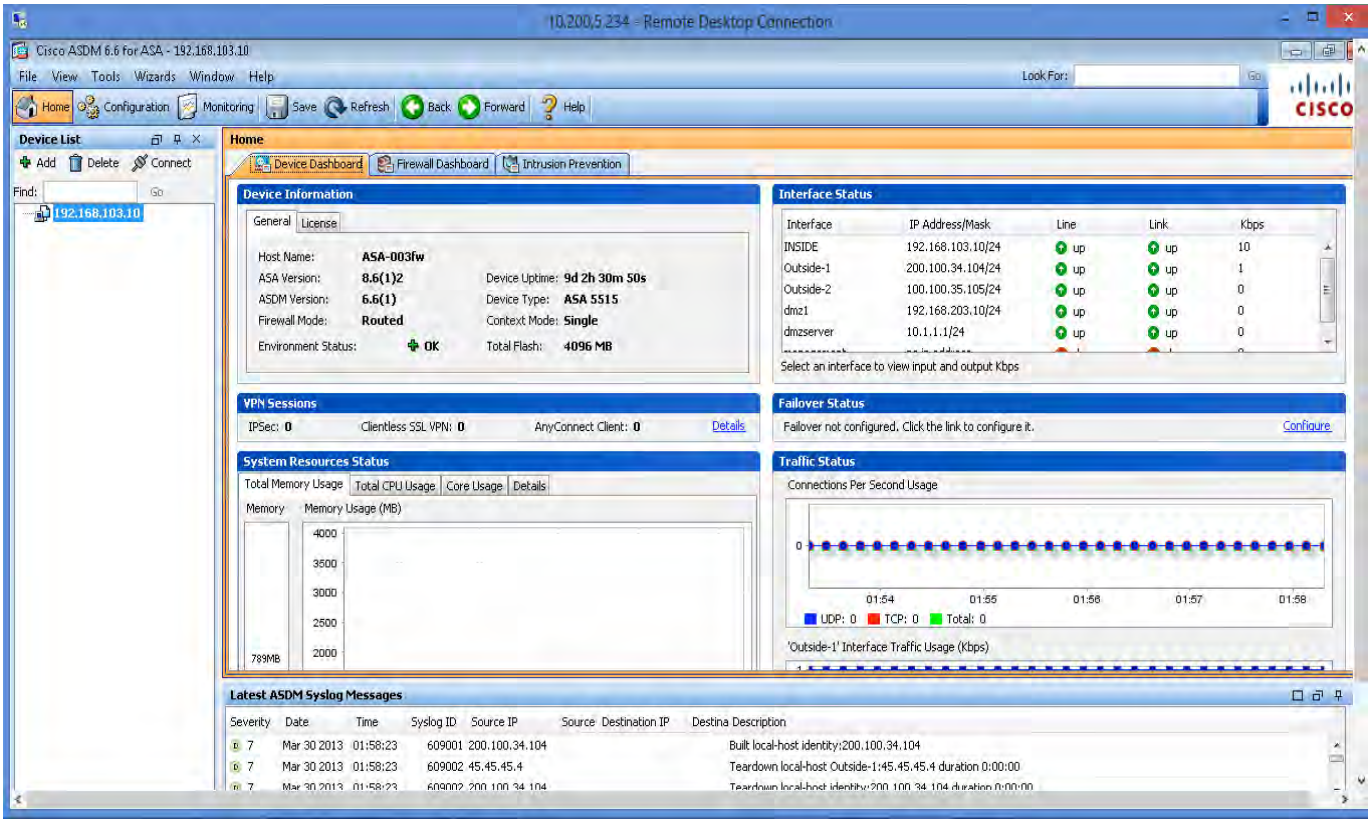
```
SW3
sw3(config)#int g1/0/2
sw3(config-if)#switchport host
sw3(config-if)#switchport access vlan 101
```

RDP into Test PC and add the route



Launch the ASDM using the





Lab 4: Address translations and access control on the ASA

Lab 4: Address translations and access control on the ASA – This lab is intended to let you be familiar with configuring the necessary system configurations to perform NAT/PAT on 8.2 code and 8.4/8.6 code on the ASA. It is very important to understand and configure NAT for both the OS versions since the lab blueprint states both versions are present. NAT has been completely re-engineered in ASA 8.4 software and higher. Apart from translation, this lab also covers access control for traffic passing through the ASA and traffic destined to the ASA. Even in ACLs, there are major differences between 8.2 code and 8.4/8.6 codes. It is very important to understand these differences in order to configure them effectively.

General Rules

- By now you should understand the logical topology very well, and have established routing and other services on the ASA.
- Double-check and save your configurations before you perform Lab 4.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 4 Hours

Pre-setup

This lab builds on the previous Lab 3. If you have skipped lab 3, load Initial Configuration for lab 1 (called “labs 1-4”) and then download final configurations for Lab 3. Copy them to R4, R5 and both ASAs - ASA1 and ASA3.

Use the logical topology drawing – Network Topology 1.1. Ensure that Lab 2 was successfully completed and verified using DSG. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below. Ensure that routes are present on the ASAs in the routing table based on Lab 2.

Detailed Solution:Lab-4

Task 1: Static auto NAT for dmz1 on ASA-3

- Configure static auto NAT using objects as per the table below. Use any object name of your choice. Use global ACLs to allow anyone to send ICMP and Telnet traffic to these IPs. Use object-groups in the ACLs wherever possible.

Real IP	Mapped IP	Real Interface	Mapped Interface
192.168.203.2	200.100.34.2	Dmz1	Outside-1
192.168.203.2	100.100.35.2	Dmz1	Outside-2
22.22.22.22	22.22.22.22	Dmz1	Outside-1
22.22.22.22	22.22.22.22	Dmz1	Outside-2
2.2.2.2	2.2.2.2	Dmz1	any

Task-1:Solutions

Step 1: Configure static Auto NAT/Object NAT for Dmz1 on ASA3.

```
//Static Auto NAT configuration for 192.168.203.2 (Outside-1)
object network dmz1-R2-G00-Out1
 host 192.168.203.2
 nat (dmz1,Outside-1) static 200.100.34.2

//Static Auto NAT configuration for 192.168.203.2 subnet (Outside-2)
object network dmz1-R2-G00-Out2
 host 192.168.203.2
 nat (dmz1,Outside-2) static 100.100.35.2

//Static Identity Auto NAT configuration for 22.22.22.22(Outside-1)
object network dmz1-R2-lo1-Out-1
 host 22.22.22.22
 nat (dmz1,Outside-1) static 22.22.22.22

//Static Identity Auto NAT configuration for 22.22.22.22(Outside-2)
object network dmz1-R2-lo1-Out-2
 host 22.22.22.22
 nat (dmz1,Outside-2) static 22.22.22.22

//Static Identity Auto NAT configuration for 2.2.2.2
object network dmz1-R2-lo0
 host 2.2.2.2
 nat (dmz1,any) static 2.2.2.2
```

Step 2: Configure Global ACL's and apply

```
object-group network PING_TELNET_DMZ1_Static_IP
 network-object host 192.168.203.2
 network-object host 22.22.22.22
 network-object host 2.2.2.2

access-list GLOBAL extended permit tcp any object-group
PING_TELNET_DMZ1_Static_IP eq telnet

access-list GLOBAL extended permit icmp any object-group
PING_TELNET_DMZ1_Static_IP

access-group GLOBAL global
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table.

"Show nat interface () detail" displays the NAT rules configured for that particular interface including hit count, real IP and the mapped IP address.

```
ASA-003fw(config)# sh nat interface dmz1 detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
3 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
4 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
5 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 100.100.35.2/32
```

"Show nat detail" displays the NAT rules globally including hit count, real IP and the mapped IP address.

```
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
```

```
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
3 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
4 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
5 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 100.100.35.2/32
```

Step 2: Verify NAT configuration. Telnet from R5 to R2

```
R5#telnet 100.100.35.2
Trying 100.100.35.2 ... Open

R2#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:09:13
*578 vty 0                 idle                 00:00:00 100.100.35.5

  Interface    User               Mode         Idle     Peer Address

R2#exit
[Connection to 100.100.35.2 closed by foreign host]
R5#
```

"Show nat interface ()" displays the NAT rules configured for that interface including hit count but does not show more details related to real IP and the mapped IP address. The same applied to "show nat" without the "detail" keyword.

```
ASA-003fw(config)# sh nat interface dmz1

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 0
2 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 0
3 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 0
4 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 0
5 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
    translate_hits = 0, untranslate_hits = 1
```

```
ASA-003fw(config)# sh access-list GLOBAL
access-list GLOBAL; 6 elements; name hash: 0xbaf7cf02
access-list GLOBAL line 1 extended permit tcp any object-group
PING_TELNET_DMZ1_Static_IP eq telnet 0x630e43dd
  access-list GLOBAL line 1 extended permit tcp any host 192.168.203.2 eq
telnet (hitcnt=2) 0x0f057ac7
```

```
  access-list GLOBAL line 1 extended permit tcp any host 22.22.22.22 eq
telnet (hitcnt=0) 0x7a22bf04
  access-list GLOBAL line 1 extended permit tcp any host 2.2.2.2 eq telnet
(hitcnt=0) 0xb64f30ad
access-list GLOBAL line 2 extended permit icmp any object-group
PING_TELNET_DMZ1_Static_IP 0xa46651ca
  access-list GLOBAL line 2 extended permit icmp any host 192.168.203.2
(hitcnt=0) 0xefe51814
  access-list GLOBAL line 2 extended permit icmp any host 22.22.22.22
(hitcnt=0) 0x0a94e47a
  access-list GLOBAL line 2 extended permit icmp any host 2.2.2.2 (hitcnt=0)
0xc0ac4bc5
```

```
R5#telnet 22.22.22.22
Trying 22.22.22.22 ... Open

R2#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:13:10
*578 vty 0                 idle                 00:00:00 100.100.35.5

  Interface    User               Mode         Idle     Peer Address

R2#exit

[Connection to 22.22.22.22 closed by foreign host]

R5#telnet 2.2.2.2
Trying 2.2.2.2 ... Open

R2#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:13:37
*578 vty 0                 idle                 00:00:00 100.100.35.5

  Interface    User               Mode         Idle     Peer Address

R2#exit

[Connection to 2.2.2.2 closed by foreign host]
R5#
```

```
ASA-003fw(config)# sh nat interface dmz1 detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
3 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
```

```
4 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
5 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.203.2/32, Translated: 100.100.35.2/32
```

Step 2: Verify NAT configuration. Telnet from R4 to R2

```
R4#telnet 200.100.34.2
Trying 200.100.34.2 ... Open

R2#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:22:13
*578 vty 0                 idle                 00:00:00 200.100.34.4

  Interface    User               Mode         Idle     Peer Address

R2#exit

[Connection to 200.100.34.2 closed by foreign host]

R4#telnet 22.22.22.22
Trying 22.22.22.22 ... Open

R2#who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:24:48
*578 vty 0                 idle                 00:00:00 200.100.34.4

  Interface    User               Mode         Idle     Peer Address

R2#exit

[Connection to 22.22.22.22 closed by foreign host]
R4#
```

```
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
3 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
4 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
5 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
```

```
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.203.2/32, Translated: 100.100.35.2/32
```

Task 2: Dynamic auto NAT/PAT for dmz1 on ASA-3

- Configure dynamic NAT/PAT using objects as per the table below. You must use objects and object-groups. Use any names for objects and object-groups.

Real IP/ Subnet	Mapped IP / Subnet	Real Interface	Mapped Interface
192.168.203.0/24	200.100.34.203	Dmz1	Outside-1
192.168.203.0/24	100.100.35.203	Dmz1	Outside-2
Range 192.168.203.60 to 192.168.203.70	NAT Pool Range - 200.100.34.60 200.100.34.70 Backup PAT - 200.100.34.71	Dmz1	Outside-1
Real IP/ Subnet	**Mapped IP / Subnet**	**Real Interface**	**Mapped Interface**
Range 192.168.203.60 to 192.168.203.70	NAT Pool Range - 100.100.35.60 100.100.35.70 Backup PAT - 100.100.35.71	Dmz1	Outside-2
2.2.2.0/24	PAT Pool Range 200.100.34.80 to 200.100.34.85 Use round robin method	Dmz1	Outside-1
2.2.2.0/24	PAT Pool Range 100.100.35.80 to 100.100.35.85 Use round robin method	Dmz1	Outside-2

Task-2:Solutions

Step 1: Configure dynamic Auto NAT/PAT on ASA-3

```
//Dynamic Auto PAT configuration for 192.168.203.0/24 subnet
object network R2-Subnet-Out-1
 subnet 192.168.203.0 255.255.255.0
 nat (dmz1,Outside-1) dynamic 200.100.34.203

//Dynamic Auto PAT configuration for 192.168.203.0/24 subnet
object network R2-Subnet-Out-2
 subnet 192.168.203.0 255.255.255.0
 nat (dmz1,Outside-2) dynamic 100.100.35.203
```

```
//Dynamic Auto NAT/PAT configuration for range 192.168.203.60 to
192.168.203.70 for Outside-1

//Define the translated IP range (NAT pool)
object network R2-60-70-out1-range
 range 200.100.34.60 200.100.34.70

//Define the PAT IP
object network R2-60-70-out1-pat
 host 200.100.34.71

//Combine the translated NAT pool and PAT IP in the object-group
object-group network R2-NAT-PAT-OUT-1
 network-object object R2-60-70-out1-range
 network-object object R2-60-70-out1-pat

//Dynamic NAT/PAT configuration for range 192.168.203.60 to 192.168.203.70
object network R2-Range-Out-1
 range 192.168.203.60 192.168.203.70
 nat (dmz1,Outside-1) dynamic R2-NAT-PAT-OUT-1
```

```
//Dynamic Auto NAT/PAT configuration for range 192.168.203.60 to
192.168.203.70 for Outside-2

//Define the translated IP range (NAT pool)
object network R2-60-70-out2-range
 range 100.100.35.60 100.100.35.70

//Define the PAT IP
object network R2-60-70-out2-pat
 host 100.100.35.71

//Combine the translated NAT pool and PAT IP in the object-group
object-group network R2-NAT-PAT-OUT-2
 network-object object R2-60-70-out2-range
 network-object object R2-60-70-out2-pat

//Dynamic NAT/PAT configuration for range 192.168.203.60 to 192.168.203.70
object network R2-Range-Out-2
 range 192.168.203.60 192.168.203.70
 nat (dmz1,Outside-2) dynamic R2-NAT-PAT-OUT-2
```

```
//Dynamic Auto PAT using PAT pool configuration for range 2.2.2.0/24 for
Outside-1
```

```
//Define the translated PAT pool for Outside-1
object network PAT_POOL_DMZ1_OUT1
 range 200.100.34.80 200.100.34.85

//Dynamic Auto PAT using PAT pool configuration for range 2.2.2.0/24 for
Outside-1
object network dmz1-R2-lo0-Subnet-Out-1
 subnet 2.2.2.0 255.255.255.0
 nat (dmz1,Outside-1) dynamic pat-pool PAT_POOL_DMZ1_OUT1 round-robin
```

```
//Dynamic Auto PAT using PAT pool configuration for range 2.2.2.0/24 for
Outside-2

//Define the translated PAT pool for Outside-2
object network PAT_POOL_DMZ1_OUT2
 range 100.100.35.80 100.100.35.85

//Dynamic Auto PAT using PAT pool configuration for range 2.2.2.0/24 for
Outside-2
object network dmz1-R2-lo0-Subnet-Out-2
 subnet 2.2.2.0 255.255.255.0
 nat (dmz1,Outside-2) dynamic pat-pool PAT_POOL_DMZ1_OUT2 round-robin
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table.

ASA automatically orders NAT/PAT the rules in section-2 i.e Auto NAT. If you observe dynamic NAT/PAT is placed after static NAT

```
ASA-003fw(config)# show nat detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
3 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
4 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
5 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
    translate_hits = 0, untranslate_hits = 2
```

```
    Source - Origin: 192.168.203.2/32, Translated: 100.100.35.2/32
6 (dmz1) to (Outside-1) source dynamic R2-Range-Out-1 R2-NAT-PAT-OUT-1
    translate_hits = 0, untranslate_hits = 0
    Source    -    Origin:    192.168.203.60-192.168.203.70,    Translated:
200.100.34.60/30, 200.100.34.64/30, 200.100.34.68/31, 200.100.34.70/32
    200.100.34.71/32
7 (dmz1) to (Outside-2) source dynamic R2-Range-Out-2 R2-NAT-PAT-OUT-2
    translate_hits = 0, untranslate_hits = 0
    Source    -    Origin:    192.168.203.60-192.168.203.70,    Translated:
100.100.35.71/32, 100.100.35.60/30, 100.100.35.64/30, 100.100.35.68/31
    100.100.35.70/32
8 (dmz1) to (Outside-1) source dynamic dmz1-R2-lo0-Subnet-Out-1 pat-pool
PAT_POOL_DMZ1_OUT1 round-robin
    translate_hits = 0, untranslate_hits = 0
    Source   -   Origin:   2.2.2.0/24,   Translated   (PAT):   200.100.34.80-
200.100.34.85
9 (dmz1) to (Outside-2) source dynamic dmz1-R2-lo0-Subnet-Out-2 pat-pool
PAT_POOL_DMZ1_OUT2 round-robin
    translate_hits = 0, untranslate_hits = 0
    Source   -   Origin:   2.2.2.0/24,   Translated   (PAT):   100.100.35.80-
100.100.35.85
10 (dmz1) to (Outside-1) source dynamic R2-Subnet-Out-1 200.100.34.203
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.0/24, Translated: 200.100.34.203/32
11 (dmz1) to (Outside-2) source dynamic R2-Subnet-Out-2 100.100.35.203
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.0/24, Translated: 100.100.35.203/32
```

Step 2: Verify NAT configuration. Telnet from R2 to R4 and R5 We need to reconfigure the IP address of R2 G0/0 and then change it back after testing. Reason of change the IP address is that there is a Static Auto NAT for 192.168.203.2

Since Global ACL's have been configured we may need to create a temporary ACL since the connection from R2 G0/0 will be denied by the global ACL. Remember the task does not ask you to create ACL's.

```
ASA3

access-list GLOBAL extended permit tcp host 192.168.203.60 host 200.100.34.4
eq telnet
access-list GLOBAL extended permit tcp host 192.168.203.60 host 100.100.35.5
eq telnet
```

```
R2

R2(config)#int g0/0
```

```
R2(config-if)#ip address 192.168.203.60 255.255.255.0

R2#telnet 200.100.34.4
Trying 200.100.34.4 ... Open

R4#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:07:57
*514 vty 0                 idle                 00:00:00 200.100.34.68
```

```
ASA
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
<SNIP
6 (dmz1) to (Outside-1) source dynamic R2-Range-Out-1 R2-NAT-PAT-OUT-1
    translate_hits = 2, untranslate_hits = 0
    Source     -     Origin:     192.168.203.60-192.168.203.70,     Translated:
200.100.34.60/30, 200.100.34.64/30, 200.100.34.68/31, 200.100.34.70/32
    200.100.34.71/32
<SNIP>

ASA-003fw(config)# sh xlate
6 in use, 30 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
<SNIP>
NAT from dmz1:192.168.203.60 to Outside-1:200.100.34.68 flags i idle 0:02:25
timeout 3:00:00
```

```
R2#telnet 100.100.35.5
Trying 100.100.35.5 ... Open

R5#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:54
*514 vty 0                 idle                 00:00:00 100.100.35.66
```

```
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
<SNIP>
7 (dmz1) to (Outside-2) source dynamic R2-Range-Out-2 R2-NAT-PAT-OUT-2
    translate_hits = 2, untranslate_hits = 0
    Source     -     Origin:     192.168.203.60-192.168.203.70,     Translated:
100.100.35.71/32, 100.100.35.60/30, 100.100.35.64/30, 100.100.35.68/31
    100.100.35.70/32
<SNIP>
```

```
ASA-003fw(config)# sh xlate
7 in use, 30 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
<SNIP>
NAT from dmz1:192.168.203.60 to Outside-2:100.100.35.66 flags i idle 0:01:53
timeout 3:00:00
```

Task 3: Static auto NAT for the dmzserver interface on ASA-3

- Configure static auto NAT using objects as per the table below. Use any object name of your choice. Configure ACLs to allow any traffic to the AD server. Do not use global ACLs. Use only objects in the ACL configuration.

Real IP	Mapped IP	Real Interface	Mapped Interface
10.1.1.101	200.100.34.101	Dmzserver	Outside-1
10.1.1.101	100.100.35.101	Dmzserver	Outside-2

Task-3:Solutions

Step 1: Configure static auto NAT for AD server

```
//Static Auto NAT configuration for AD  (Outside-1)
object network ADServer-OUT-1
 host 10.1.1.101
 nat (dmzserver,Outside-1) static 200.100.34.101

//Static Auto NAT configuration for AD  (Outside-2)
object network ADServer-OUT-2
 host 10.1.1.101
 nat (dmzserver,Outside-2) static 100.100.35.101
```

Step 2: Configure ACL's to allow access to the AD server.

```
object network ANY
 subnet 0 0

access-list OUT-1 extended permit ip object ANY object ADServer-OUT-1
access-list OUT-2 extended permit ip object ANY object ADServer-OUT-2

access-group OUT-2 in interface outside-2
access-group OUT-1 in interface outside-1
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries.

```
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
<SNIP>
2 (dmzserver) to (Outside-1) source static ADServer-OUT-1 200.100.34.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 200.100.34.101/32
3 (dmzserver) to (Outside-2) source static ADServer-OUT-2 100.100.35.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 100.100.35.101/32
<SNIP>
```

Step 2: Ping from the outside to the AD.

Task 4: Static object NAT between dmz1 and dmzserver on ASA-3

- Configure static object NAT such that R2 can ping the AD server using an IP address of 192.168.203.101 from Gi0/0. The AD server should see R2 Gi0/0 as 10.1.1.2.

Task-4:Solutions

Step 1: This configuration is similar to twice NAT. However the task specifies to use Auto/Object NAT. Hence 2 rules need to be created.

```
//Static Auto NAT configuration for R2 when communicating with AD using
192.168.203.101.In other words AD appears as 192.168.203.101 in VLAN 203
(dmz1)

object network AD_DMZ
 host 10.1.1.101
 nat (dmzserver,dmz1) static 192.168.203.101


//Static Auto NAT configuration for AD when communicating with the R2 using
10.1.1.2. In other words R2 G0/0 appears as 10.1.1.2 in VLAN 100 (dmzserver)

object network DMZ_AD
 host 192.168.203.2
 nat (dmz1,dmzserver) static 10.1.1.2
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries.

```
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmzserver) to (Outside-1) source static ADServer-OUT-1 200.100.34.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 200.100.34.101/32
3 (dmzserver) to (Outside-2) source static ADServer-OUT-2 100.100.35.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 100.100.35.101/32
4 (dmzserver) to (dmz1) source static AD_DMZ 192.168.203.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 192.168.203.101/32
5 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
6 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
7 (dmz1) to (dmzserver) source static DMZ_AD 10.1.1.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 10.1.1.2/32
<SNIP>
```

Step 2: Allow ICMP in the GLOBAL ACL and remove after testing. Ping from R2 and the AD server.

```
access-list GLOBAL permit icmp any any
```

```
R2#ping 192.168.203.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Task 5: DNS rewrite using static auto NAT for the inside interface on ASA-3

- Inside subnet users are unable to connect to an internal web server (192.168.103.80) that is mapped to 200.100.34.40 and 100.100.35.40 due to a DNS resolution error. Assume that those users are configured with an external DNS server that returns public addresses – fix this. Also use global ACL's to allow HTTP and HTTPS access to these servers from anyone from the outside. Use objects and object-groups in the ACL to minimize the number of ACEs.

Task-5:Solutions

Step 1: Configure DNS rewrite using Auto NAT

```
//Static Auto NAT configuration with DNS re-write
 object network INSIDE_WEB_out-1
  host 192.168.103.80
  nat (INSIDE,outside-1) static 200.100.34.40 dns

//Static Auto NAT configuration with DNS re-write
object network INSIDE_WEB_out-2
  host 192.168.103.80
  nat (INSIDE,outside-2) static 100.100.35.40 dns
```

Step 1: Configure ACL's to allow access to these webservers.

```
object-group service WEB tcp
 port-object eq 443
 port-object eq 80

access-list GLOBAL extended permit tcp any object INSIDE_WEB_out-1 object-
group WEB
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries again.

```
ASA-003fw(config)# sh nat detail

Auto NAT Policies (Section 2)
<SNIP>
7 (INSIDE) to (Outside-1) source static INSIDE_WEB_out-1 200.100.34.40   dns
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.80/32, Translated: 200.100.34.40/32
8 (INSIDE) to (Outside-2) source static INSIDE_WEB_out-2 100.100.35.40   dns
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.80/32, Translated: 100.100.35.40/32
<SNIP>
```

Step 2: R1 F0/0 is pre-configured with a secondary address of 192.168.103.80 and HTTP server has been enabled. Test from R4 and R5.

```
R4#telnet 200.100.34.40 80
Trying 200.100.34.40, 80 ... Open
GET
HTTP/1.1 400 Bad Request
Date: Thu, 28 Mar 2013 09:19:55 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 200.100.34.40 closed by foreign host]



R5#100.100.35.40 80
Trying 100.100.35.40, 80 ... Open
GET 1.1
HTTP/1.1 400 Bad Request
Date: Thu, 28 Mar 2013 09:21:11 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 100.100.35.40 closed by foreign host]
```

Task 6: Static auto NAT for INSIDE on ASA-3

- Configure static auto NAT using objects as per the table below. Use any object name of your choice. Use global ACLs such that anyone can send ICMP, SSH, Telnet, FTP, SMTP, HTTP, and HTTPS traffic to these servers/PC. Use object-groups in the ACL to minimize the number of ACEs.

Real IP	Mapped IP	Real Interface	Mapped Interface
1.1.1.0/24	1.1.1.0/24	INSIDE	any
192.168.103.1	200.100.34.1	INSIDE	Outside-1
192.168.103.1	100.100.35.1	INSIDE	Outside-2
192.168.100.200	200.100.34.111	INSIDE	Outside-1
192.168.100.200	100.100.35.111	INSIDE	Outside-2

Task-6:Solutions

Step 1: Configure Static auto NAT for INSIDE on ASA-3

```
//Static identity Auto NAT (R1 Lo0 Subnet)
object network R1-LO-Subnet
 subnet 1.1.1.0 255.255.255.0
 nat (INSIDE,any) static  R1-LO-Subnet

//Static Auto NAT for for R1 F0/0 (Outside-1)
object network R1_f00_out-1
 host 192.168.103.1
 nat (INSIDE,outside-1) static 200.100.34.1

//Static Auto NAT for for R1 F0/0 (Outside-2)
object network R1_f00_out-2
 host 192.168.103.1
 nat (INSIDE,outside-2) static 100.100.35.1

//Static Auto NAT for for Test-PC (Outside-1)
object net TEST_PC_OUT_1
 host 192.168.100.200
 nat (INSIDE,Outside-1) static 200.100.34.111

//Static Auto NAT for for Test-PC (Outside-2)
object network TEST_PC_OUT_2
 host 192.168.100.200
 nat (INSIDE,Outside-2) static 100.100.35.111
```

Step 2: Configure ACL's to allow access.

```
object-group network INSIDE_NET_IP
 network-object 1.1.1.0 255.255.255.0
 network-object host 192.168.103.1
 network-object host 192.168.100.200

object-group service INSIDE_SERVER tcp
 port-object eq 80
 port-object eq 443
 port-object eq 23
 port-object eq 22
 port-object eq 25
 port-object eq 21

access-list GLOBAL extended permit tcp any object-group INSIDE_NET_IP object-
group INSIDE_SERVER
access-list GLOBAL extended permit icmp any object-group INSIDE_NET_IP
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries again.

```
ASA-003fw(config)# sh nat interface INSIDE  detail

Auto NAT Policies (Section 2)
7 (INSIDE) to (Outside-1) source static TEST_PC_OUT_1 200.100.34.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 200.100.34.111/32
8 (INSIDE) to (Outside-2) source static TEST_PC_OUT_2 100.100.35.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 100.100.35.111/32
9 (INSIDE) to (Outside-1) source static R1_f00_out-1 200.100.34.1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.1/32
10 (INSIDE) to (Outside-2) source static R1_f00_out-2 100.100.35.1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.1/32, Translated: 100.100.35.1/32
11 (INSIDE) to (Outside-1) source static INSIDE_WEB_out-1 200.100.34.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 200.100.34.40/32
12 (INSIDE) to (Outside-2) source static INSIDE_WEB_out-2 100.100.35.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 100.100.35.40/32
16 (INSIDE) to (any) source static R1-LO-Subnet R1-LO-Subnet
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 1.1.1.0/24, Translated: 1.1.1.0/24
```

Step 2: Ping from R4 and R5 to R1 F0/0 and Lo0. Basic ping test would be sufficient.

```
R5#ping 100.100.35.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.35.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R5#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
R4#ping 200.100.34.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 7: Static PAT/port redirection using auto NAT for INSIDE on ASA-3

- 11.11.11.11 is a Telnet and an FTP server. Any outside users should be able to FTP to 11.11.11.11 using an IP address of 200.100.34.21 and a TCP port of 2121 and Telnet using an IP address of 200.100.34.23 and a TCP port of 3001. Use any object names of your choice for NAT. ACLs should be interface specific to allow access to these servers. Do not use objects or object-groups in the ACEs.

Task-7:Solutions

Step 1: Configure Static PAT for 11.11.11.11 for Outside-1.

```
//Static PAT for FTP
object network R1_FTP_Out-1
 host 11.11.11.11
 nat (INSIDE,Outside-1) static 200.100.34.21 service tcp ftp 2121

//Static PAT for telnet
object network R1_Telnet_Out-1
 host 11.11.11.11
 nat (INSIDE,Outside-1) static 200.100.34.23 service tcp 23 3001
```

Step 2: Allow access to 11.11.11.11 from the outside.

```
access-list OUT-1 permit tcp any host 11.11.11.11 eq 23
access-list OUT-1 permit tcp any host 11.11.11.11 eq 21
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries again.

```
ASA-003fw(config)# sh nat interface INSIDE detail

Auto NAT Policies (Section 2)
5 (INSIDE) to (Outside-1) source static R1_FTP_Out-1 200.100.34.21    service
tcp ftp 2121
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.21/32
    Service - Protocol: tcp Real: ftp Mapped: 2121
6  (INSIDE)  to  (Outside-1)  source  static  R1_Telnet_Out-1  200.100.34.23
service tcp telnet 3001
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.23/32
    Service - Protocol: tcp Real: telnet Mapped: 3001
9 (INSIDE) to (Outside-1) source static TEST_PC_OUT_1 200.100.34.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 200.100.34.111/32
10 (INSIDE) to (Outside-2) source static TEST_PC_OUT_2 100.100.35.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 100.100.35.111/32
11 (INSIDE) to (Outside-1) source static R1_f00_out-1 200.100.34.1
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.1/32
12 (INSIDE) to (Outside-2) source static R1_f00_out-2 100.100.35.1
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 192.168.103.1/32, Translated: 100.100.35.1/32
13 (INSIDE) to (Outside-1) source static INSIDE_WEB_out-1 200.100.34.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 200.100.34.40/32
14 (INSIDE) to (Outside-2) source static INSIDE_WEB_out-2 100.100.35.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 100.100.35.40/32
18 (INSIDE) to (any) source static R1-LO-Subnet R1-LO-Subnet
    translate_hits = 0, untranslate_hits = 10
    Source - Origin: 1.1.1.0/24, Translated: 1.1.1.0/24
```

Step 2: Test from R4. Basic telnet test would be sufficient.

```
R4#200.100.34.23 3001
Trying 200.100.34.23, 3001 ... Open

R1#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:03
*514 vty 0                 idle                 00:00:00 200.100.34.4

  Interface    User               Mode         Idle     Peer Address

R1#exit

[Connection to 200.100.34.23 closed by foreign host]
```

Task 8: Static PAT/port redirection using auto NAT for INSIDE on ASA-3

- There are multiple internal servers on the INSIDE interface. The ISP (R5) has only provided a single IP address. Configure Static PAT using objects as per the table below. ACLs should be interface specific to allow access to these servers. Re-use the existing objects when creating the ACEs for the server IPs.

Real IP and Port	Mapped IP and Port	Real Interface	Mapped Interface
11.11.11.25 TCP 25	100.100.35.222 TCP 2525	INSIDE	Outside-2
11.11.11.80 TCP 80	100.100.35.222 TCP 8080	INSIDE	Outside-2
11.11.11.88 TCP 443	100.100.35.222 TCP 4343	INSIDE	Outside-2
11.11.11.22 TCP 22	100.100.35.222 TCP 2222	INSIDE	Outside-2
11.11.11.23 TCP 23	100.100.35.222 TCP 2323	INSIDE	Outside-2

Task-8:Solutions

Step 1: Configure Static PAT for various servers using the same Translated IP but different ports for Outside-2.

```
//Static PAT for SMTP
object network R1_Server1_SMTP
```

```
 host 11.11.11.25
 nat (INSIDE,Outside-2) static 100.100.35.222 service tcp 25 2525

//Static PAT for HTTP
object network R1_Server2_HTTP
 host 11.11.11.80
 nat (INSIDE,Outside-2) static 100.100.35.222 service tcp 80 8080

//Static PAT for HTTPS
object network R1_Server3_HTTPS
 host 11.11.11.88
 nat (INSIDE,Outside-2) static 100.100.35.222 service tcp 443 4343

//Static PAT for SSH
object network R1_Server4_SSH
 host 11.11.11.22
 nat (INSIDE,Outside-2) static 100.100.35.222 service tcp 22 2222

//Static PAT for Telnet
object network R1_Server5_telnet
 host 11.11.11.23
 nat (INSIDE,Outside-2) static 100.100.35.222 service tcp 23 2323
```

Step 2: Allow access these servers from outside-2

```
access-list OUT-2 extended permit tcp any object R1_Server1_SMTP eq smtp
access-list OUT-2 extended permit tcp any object R1_Server2_HTTP eq www
access-list OUT-2 extended permit tcp any object R1_Server3_HTTPS eq https
access-list OUT-2 extended permit tcp any object R1_Server4_SSH eq ssh
access-list OUT-2 extended permit tcp any object R1_Server5_telnet eq telnet
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries again.

```
ASA-003fw(config)# show nat interface INSIDE detail

Auto NAT Policies (Section 2)
5 (INSIDE) to (Outside-1) source static R1_FTP_Out-1 200.100.34.21   service
tcp ftp 2121
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.21/32
    Service - Protocol: tcp Real: ftp Mapped: 2121
6  (INSIDE)  to  (Outside-1)  source  static  R1_Telnet_Out-1  200.100.34.23
service tcp telnet 3001
    translate_hits = 0, untranslate_hits = 6
```

```
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.23/32
    Service - Protocol: tcp Real: telnet Mapped: 3001
7  (INSIDE)  to  (Outside-2)  source  static  R1_Server4_SSH  100.100.35.222
service tcp ssh 2222
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.22/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: ssh Mapped: 2222
8  (INSIDE)  to  (Outside-2)  source  static  R1_Server5_telnet  100.100.35.222
service tcp telnet 2323
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.23/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: telnet Mapped: 2323
9  (INSIDE)  to  (Outside-2)  source  static  R1_Server1_SMTP  100.100.35.222
service tcp smtp 2525
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.25/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: smtp Mapped: 2525
10  (INSIDE)  to  (Outside-2)  source  static  R1_Server2_HTTP  100.100.35.222
service tcp www 8080
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.80/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: www Mapped: 8080
11  (INSIDE)  to  (Outside-2)  source  static  R1_Server3_HTTPS  100.100.35.222
service tcp https 4343
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.88/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: https Mapped: 4343
14 (INSIDE) to (Outside-1) source static TEST_PC_OUT_1 200.100.34.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 200.100.34.111/32
15 (INSIDE) to (Outside-2) source static TEST_PC_OUT_2 100.100.35.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 100.100.35.111/32
16 (INSIDE) to (Outside-1) source static R1_f00_out-1 200.100.34.1
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.1/32
17 (INSIDE) to (Outside-2) source static R1_f00_out-2 100.100.35.1
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 192.168.103.1/32, Translated: 100.100.35.1/32
18 (INSIDE) to (Outside-1) source static INSIDE_WEB_out-1 200.100.34.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 200.100.34.40/32
19 (INSIDE) to (Outside-2) source static INSIDE_WEB_out-2 100.100.35.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 100.100.35.40/32
23 (INSIDE) to (any) source static R1-LO-Subnet R1-LO-Subnet
    translate_hits = 0, untranslate_hits = 10
    Source - Origin: 1.1.1.0/24, Translated: 1.1.1.0/24
```

Step 2: R1 Lo1 is pre-configured with a many secondary addresses. Test from R5. Create a temporary route on ASA for these servers.

ASA

```
route INSIDE 11.0.0.0 255.0.0.0 192.168.103.1
```

```
R5#100.100.35.222 2323
Trying 100.100.35.222, 2323 ... Open

R1#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:03:52
*514 vty 0                 idle                 00:00:00 100.100.35.5

  Interface    User               Mode         Idle     Peer Address

R1#exit

[Connection to 100.100.35.222 closed by foreign host]



R5#100.100.35.222 8080
Trying 100.100.35.222, 8080 ... Open
GET
HTTP/1.1 400 Bad Request
Date: Thu, 28 Mar 2013 10:18:31 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 100.100.35.222 closed by foreign host]


R5#100.100.35.222 2222
Trying 100.100.35.222, 2222 ... Open
SSH-1.5-Cisco-1.25
                  c
[Connection to 100.100.35.222 closed by foreign host]


R5#100.100.35.222 4343
Trying 100.100.35.222, 4343 ... Open
GET
^Z

[Connection to 100.100.35.222 closed by foreign host]
```

Task 9: Dynamic PAT and DNS rewrite on ASA-3

- Make sure that any outbound connection from DMZ's and Inside subnets going out of Outside-1 and Outside-2 is PAT'd to the appropriate ASA outside interface and also performs DNS re-write.

Task-9:Solutions

Step 1: Dynamic PAT for all outbound connections for both the outside interfaces with DNS re-write.

```
object network ALL_out-1
 subnet 0 0
 nat (any,outside-1) dynamic interface dns

object network ALL_out-2
subnet 0 0
nat (any,outside-2) dynamic interface dns
```

Verification

Step 1: Verify Auto NAT policies (Section-2) entries in NAT table. If you observe the ASA has re-ordered the entries again.
Review all your NAT rules now. Entry 30 and 31 correspond to the outbound PAT with DNS re-write.

```
ASA-003fw(config)# show nat detail

Auto NAT Policies (Section 2)
1 (dmz1) to (any) source static dmz1-R2-lo0 2.2.2.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (dmzserver) to (Outside-1) source static ADServer-OUT-1 200.100.34.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 200.100.34.101/32
3 (dmzserver) to (Outside-2) source static ADServer-OUT-2 100.100.35.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 100.100.35.101/32
4 (dmzserver) to (dmz1) source static AD_DMZ 192.168.203.101
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.101/32, Translated: 192.168.203.101/32
5 (INSIDE) to (Outside-1) source static R1_FTP_Out-1 200.100.34.21    service
tcp ftp 2121
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.21/32
    Service - Protocol: tcp Real: ftp Mapped: 2121
```

```
6  (INSIDE)  to  (Outside-1)  source  static  R1_Telnet_Out-1  200.100.34.23
service tcp telnet 3001
    translate_hits = 0, untranslate_hits = 6
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.23/32
    Service - Protocol: tcp Real: telnet Mapped: 3001
7  (INSIDE)  to  (Outside-2)  source  static  R1_Server4_SSH  100.100.35.222
service tcp ssh 2222
    translate_hits = 0, untranslate_hits = 12
    Source - Origin: 11.11.11.22/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: ssh Mapped: 2222
8  (INSIDE)  to  (Outside-2)  source  static  R1_Server5_telnet  100.100.35.222
service tcp telnet 2323
    translate_hits = 0, untranslate_hits = 4
    Source - Origin: 11.11.11.23/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: telnet Mapped: 2323
9  (INSIDE)  to  (Outside-2)  source  static  R1_Server1_SMTP  100.100.35.222
service tcp smtp 2525
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.25/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: smtp Mapped: 2525
10  (INSIDE)  to  (Outside-2)  source  static  R1_Server2_HTTP  100.100.35.222
service tcp www 8080
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 11.11.11.80/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: www Mapped: 8080
11  (INSIDE)  to  (Outside-2)  source  static  R1_Server3_HTTPS  100.100.35.222
service tcp https 4343
    translate_hits = 0, untranslate_hits = 2
    Source - Origin: 11.11.11.88/32, Translated: 100.100.35.222/32
    Service - Protocol: tcp Real: https Mapped: 4343
12 (dmz1) to (Outside-1) source static dmz1-R2-lo1-Out-1 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
13 (dmz1) to (Outside-2) source static dmz1-R2-lo1-Out-2 22.22.22.22
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 22.22.22.22/32, Translated: 22.22.22.22/32
14 (INSIDE) to (Outside-1) source static TEST_PC_OUT_1 200.100.34.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 200.100.34.111/32
15 (INSIDE) to (Outside-2) source static TEST_PC_OUT_2 100.100.35.111
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.100.200/32, Translated: 100.100.35.111/32
16 (INSIDE) to (Outside-1) source static R1_f00_out-1 200.100.34.1
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.1/32
17 (INSIDE) to (Outside-2) source static R1_f00_out-2 100.100.35.1
    translate_hits = 0, untranslate_hits = 9
    Source - Origin: 192.168.103.1/32, Translated: 100.100.35.1/32
18 (INSIDE) to (Outside-1) source static INSIDE_WEB_out-1 200.100.34.40   dns
```

```
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 200.100.34.40/32
19 (INSIDE) to (Outside-2) source static INSIDE_WEB_out-2 100.100.35.40   dns
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.103.80/32, Translated: 100.100.35.40/32
20 (dmz1) to (dmzserver) source static DMZ_AD 10.1.1.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 10.1.1.2/32
21 (dmz1) to (Outside-1) source static dmz1-R2-G00-Out1 200.100.34.2
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
22 (dmz1) to (Outside-2) source static dmz1-R2-G00-Out2 100.100.35.2
    translate_hits = 0, untranslate_hits = 2
    Source - Origin: 192.168.203.2/32, Translated: 100.100.35.2/32
23 (INSIDE) to (any) source static R1-LO-Subnet R1-LO-Subnet
    translate_hits = 0, untranslate_hits = 10
    Source - Origin: 1.1.1.0/24, Translated: 1.1.1.0/24
24 (dmz1) to (Outside-1) source dynamic R2-Range-Out-1 R2-NAT-PAT-OUT-1
    translate_hits = 2, untranslate_hits = 0
    Source     -     Origin:     192.168.203.60-192.168.203.70,     Translated:
200.100.34.60/30, 200.100.34.64/30, 200.100.34.68/31, 200.100.34.70/32
    200.100.34.71/32
25 (dmz1) to (Outside-2) source dynamic R2-Range-Out-2 R2-NAT-PAT-OUT-2
    translate_hits = 2, untranslate_hits = 0
    Source     -     Origin:     192.168.203.60-192.168.203.70,     Translated:
100.100.35.71/32, 100.100.35.60/30, 100.100.35.64/30, 100.100.35.68/31
    100.100.35.70/32
26 (dmz1) to (Outside-1) source dynamic dmz1-R2-lo0-Subnet-Out-1 pat-pool
PAT_POOL_DMZ1_OUT1 round-robin
    translate_hits = 6, untranslate_hits = 0
    Source   -   Origin:   2.2.2.0/24,   Translated   (PAT):   200.100.34.80-
200.100.34.85
27 (dmz1) to (Outside-2) source dynamic dmz1-R2-lo0-Subnet-Out-2 pat-pool
PAT_POOL_DMZ1_OUT2 round-robin
    translate_hits = 2, untranslate_hits = 0
    Source   -   Origin:   2.2.2.0/24,   Translated   (PAT):   100.100.35.80-
100.100.35.85
28 (dmz1) to (Outside-1) source dynamic R2-Subnet-Out-1 200.100.34.203
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.0/24, Translated: 200.100.34.203/32
29 (dmz1) to (Outside-2) source dynamic R2-Subnet-Out-2 100.100.35.203
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.0/24, Translated: 100.100.35.203/32
30 (any) to (Outside-1) source dynamic ALL_out-1 interface   dns
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 200.100.34.104/24
31 (any) to (Outside-2) source dynamic ALL_out-2 interface   dns
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 100.100.35.105/24
```

Task 10: Manual dynamic NAT on ASA-3

- Configure ASA-3 such that when IP address ranges of 192.168.100.230 and 192.168.100.240 connects to VLAN 45, they are NATed to a pool of 200.100.34.230,-200.100.34.240 and 100.100.35.230-100.100.35.240. Configure ACLs to allow any traffic between them. Re-use objects when creating global ACEs.

Task-10:Solutions

Step 1: Configure objects.

```
object network R1_Range
 range 192.168.100.230 192.168.100.240

object network VLAN415
 subnet 45.45.45.0 255.255.255.0

object network Pool1
 range 200.100.34.230 200.100.34.240

object network Pool2
 range 100.100.35.230 100.100.35.240
```

Step 2: Configure manual NAT. (Policy NAT)

```
nat (INSIDE,Outside-1) source dynamic R1_Range Pool1 destination static VLAN415 VLAN415

nat (INSIDE,Outside-2) source dynamic R1_Range Pool2 destination static VLAN415 VLAN415
```

Step 3: Configure ACL'S to allow access.

```
access-list GLOBAL permit ip object R1_Range object VLAN415
access-list GLOBAL permit ip object VLAN415 object R1_Range
```

Verification

Step 1: Verify Manual NAT entries (Section-1).

```
ASA-003fw(config)# show nat detail

Manual NAT Policies (Section 1)
```

```
1 (INSIDE) to (Outside-1) source dynamic R1_Range Pool1    destination static
VLAN415 VLAN415
    translate_hits = 0, untranslate_hits = 0
    Source    -    Origin:    192.168.100.230-192.168.100.240,    Translated:
200.100.34.230-200.100.34.240
    Destination - Origin: 45.45.45.0/24, Translated: 45.45.45.0/24
2 (INSIDE) to (Outside-2) source dynamic R1_Range Pool2    destination static
VLAN415 VLAN415
    translate_hits = 0, untranslate_hits = 0
    Source    -    Origin:    192.168.100.230-192.168.100.240,    Translated:
100.100.35.230-100.100.35.240
    Destination - Origin: 45.45.45.0/24, Translated: 45.45.45.0/24

Auto NAT Policies (Section 2)
<SNIP>
```

```
R1#ping 45.45.45.23 source 192.168.100.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.23, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.230
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#ping 45.45.45.5 so 192.168.100.230
```

```
Show Xlate
ASA-003fw(config)# sh xlate
24 in use, 30 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
<SNIP>
NAT  from  INSIDE:192.168.100.230  to  Outside-1:200.100.34.240  flags  i  idle
0:00:00 timeout 3:00:00

ASA-003fw(config)# sh conn all
7 in use, 11 most used
ICMP Outside-1 45.45.45.23:0 INSIDE 192.168.100.230:1, idle 0:00:00, bytes 72
<SNIP>
```

Task 11: Manual dynamic PAT on ASA-3

- Users on VLAN 203 should be PATed to 200.100.34.115 and 100.100.35.115 when they try to connect to 45.45.45.23 on port 23 (Telnet). Manual NAT statements should be very specific. Use global ACLs to allow traffic to flow. You can re-use the existing objects.

Task-11:Solutions

Step 1: Configure objects.

```
object network R2-Subnet
 subnet 192.168.203.0 255.255.255.0

object network TELNET115_403
 host 200.100.34.115

object network TELNET115_503
 host 100.100.35.115

object network VLAN415_TELNET_SERVER
 host 45.45.45.23
object service telnet
 service tcp destination eq telnet
```

Step 2: Configure manual PAT. (Policy PAT)

```
nat (dmz1,Outside-1) source dynamic R2-Subnet TELNET115_403 destination
static VLAN415_TELNET_SERVER VLAN415_TELNET_SERVER service telnet telnet

nat (dmz1,Outside-2) source dynamic R2-Subnet TELNET115_503 destination
static VLAN415_TELNET_SERVER VLAN415_TELNET_SERVER service telnet telnet
```

Step 3: Configure ACL's to allow the flow from VLAN 203 to 45.45.45.23.

access-list GLOBAL extended permit tcp object R2-Subnet object VLAN415_TELNET_SERVER eq telnet

Verification

Step 1: Verify Manual NAT entries (Section-1).

```
ASA-003fw(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (INSIDE) to (Outside-1) source dynamic R1_Range Pool1   destination static
VLAN415 VLAN415
    translate_hits = 26328, untranslate_hits = 6
    Source    -    Origin:    192.168.100.230-192.168.100.240,    Translated:
200.100.34.230-200.100.34.240
    Destination - Origin: 45.45.45.0/24, Translated: 45.45.45.0/24
2 (INSIDE) to (Outside-2) source dynamic R1_Range Pool2   destination static
VLAN415 VLAN415
    translate_hits = 0, untranslate_hits = 0
    Source    -    Origin:    192.168.100.230-192.168.100.240,    Translated:
100.100.35.230-100.100.35.240
    Destination - Origin: 45.45.45.0/24, Translated: 45.45.45.0/24
```

```
3 (dmz1) to (Outside-1) source dynamic R2-Subnet TELNET115_403    destination
static VLAN415_TELNET_SERVER VLAN415_TELNET_SERVER service telnet telnet
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.0/24, Translated: 200.100.34.115/32
    Destination - Origin: 45.45.45.23/32, Translated: 45.45.45.23/32
    Service - Origin: tcp destination eq telnet , Translated: tcp destination
eq telnet
4 (dmz1) to (Outside-2) source dynamic R2-Subnet TELNET115_503    destination
static VLAN415_TELNET_SERVER VLAN415_TELNET_SERVER service telnet telnet
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.0/24, Translated: 100.100.35.115/32
    Destination - Origin: 45.45.45.23/32, Translated: 45.45.45.23/32
    Service - Origin: tcp destination eq telnet , Translated: tcp destination
eq telnet

Auto NAT Policies (Section 2)
<SNIP>
```

```
R2#telnet 45.45.45.23
Trying 45.45.45.23 ... Open

R4#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:49:30
*514 vty 0                 idle                 00:00:00 200.100.34.115


///ASA (Make sure to unshut after testing)
ASA-003fw(config)# int port-channel 1.34
ASA-003fw(config-subif)# shut
R2#telnet 45.45.45.23
Trying 45.45.45.23 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:52:54
*514 vty 0                 idle                 00:00:00 100.100.35.115
```

Task 12: Manual static identity NAT on ASA-3

- Create a loopback on R2 with an IP address of 222.222.222.222/32. Configure static identity NAT such that only outside users can ping that IP address. Use global ACLs to allow access.
- Advertise the new loopback into RIPv2 on R2 and create appropriate static routes on R4 and R5.

Task-12:Solutions

Step 1: Configure Loopback on R2 and advertise into RIP.

```
int lo222
 ip add 222.222.222.222 255.255.255.255

router rip
 network 222.222.222.0
```

Step 2: Configure Static routes on R4 and R5.

```
R5
ip route 222.222.222.222 255.255.255.255 100.100.35.105

R4
ip route 222.222.222.222 255.255.255.255 200.100.34.104
```

Step 3: Configure objects on ASA3

```
object network R2_Loop222
 host 222.222.222.222
```

Step 4: Configure Manual identity NAT on ASA3

```
nat (dmz1,outside-1) source static R2_Loop222 R2_Loop222
nat (dmz1,outside-2) source static R2_Loop222 R2_Loop222
```

Step 5: Configure global ACL's

```
access-list GLOBAL permit icmp any object R2_Loop222 echo
access-list GLOBAL permit icmp object R2_Loop222 any echo-reply
```

Verification

Step 1: Verify Manual NAT entries (Section-1). Entry 5 and 6 of section 1.

```
Manual NAT Policies (Section 1)
<SNIP>
5 (dmz1) to (Outside-1) source static R2_Loop222 R2_Loop222
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 222.222.222.222/32, Translated: 222.222.222.222/32
6 (dmz1) to (Outside-2) source static R2_Loop222 R2_Loop222
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 222.222.222.222/32, Translated: 222.222.222.222/32
<SNIP>
```

Step 2: Telnet from Lo222 to R4 and R5 and perform basic ping tests.

```
R2#telnet 45.45.45.4 /source-interface lo222
Trying 45.45.45.4 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:04:58
*514 vty 0                 idle                 00:00:00 222.222.222.222

  Interface    User               Mode         Idle     Peer Address

R4#exit

[Connection to 45.45.45.4 closed by foreign host]
R2#ping 4.4.4.4 so lo 222

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 222.222.222.222
!!!!!

R2#ping 45.45.45.5 so lo 222

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.5, timeout is 2 seconds:
Packet sent with a source address of 222.222.222.222
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms




R2#telnet 100.100.35.5 /source-interface lo222
Trying 100.100.35.5 ... Open


R5#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:04:00
*514 vty 0                 idle                 00:00:00 222.222.222.222

  Interface    User               Mode         Idle     Peer Address

R5#ping 222.222.222.222

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 222.222.222.222, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#exit

[Connection to 100.100.35.5 closed by foreign host]
R2#
```

Task 13: Manual static identity NAT on ASA-3

- A VPN tunnel exists between VLAN301 and VLAN60. Configure a NAT exception using manual NAT. Both the outside interfaces on ASA-3 are tunnel endpoints.

Task-13:Solutions

Step 1: Configure objects

```
object network VLAN301
 subnet 192.168.103.0 255.255.255.0

object network VLAN60
 subnet 192.168.60.0 255.255.255.0
```

Step 2: Configure NAT exemption using Manual NAT.

```
nat (INSIDE,Outside-1) source static VLAN301 VLAN301 destination static
VLAN60 VLAN60

nat (INSIDE,Outside-2) source static VLAN301 VLAN301 destination static
VLAN60 VLAN60
```

Verification

Step 1: Verify Manual NAT entries (Section-1). Entry 7 and 8 of section 1.

```
ASA-003fw(config)# sh nat detail
Manual NAT Policies (Section 1)
<SNIP>
7 (INSIDE) to (Outside-1) source static VLAN301 VLAN301   destination static
VLAN60 VLAN60
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.0/24, Translated: 192.168.103.0/24
    Destination - Origin: 192.168.60.0/24, Translated: 192.168.60.0/24
8 (INSIDE) to (Outside-2) source static VLAN301 VLAN301   destination static
VLAN60 VLAN60
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.0/24, Translated: 192.168.103.0/24
```

```
    Destination - Origin: 192.168.60.0/24, Translated: 192.168.60.0/24

Auto NAT Policies (Section 2)
<SNIP>
```

Task 14: Twice NAT on ASA-3

- R1's Fa0/0 should be able to connect to R4's Loopback0 using an IP address of 192.168.103.4 and R4 should see R1's Fa0/0 as 200.100.34.117. Use global ACLs to allow ICMP and Telnet access.

Task-14:Solutions

Step 1: Configure objects

```
object net DOUBLE_NAT_R1_real
 host 192.168.103.1

object net DOUBLE_NAT_R1_map
 host 200.100.34.117

object network DOUBLE_NAT_R4_real
 host 4.4.4.4

object network DOUBLE_NAT_R4_map
 host 192.168.103.4
```

Step 2: Configure Twice NAT on ASA3

```
nat (INSIDE,Outside-1) source static DOUBLE_NAT_R1_real DOUBLE_NAT_R1_map
destination static DOUBLE_NAT_R4_map DOUBLE_NAT_R4_real
```

Step 3: Configure ACL to allow R1 to telnet and ping R4 Lo0 using 192.168.103.4

```
access-list GLOBAL extended permit tcp object DOUBLE_NAT_R1_real object
DOUBLE_NAT_R4_real eq 23
access-list GLOBAL extended permit icmp object DOUBLE_NAT_R1_real object
DOUBLE_NAT_R4_real
```

Verification

Step 1: Verify Manual NAT entries (Section-1). Entry 9 of section 1.

```
ASA-003fw(config)# sh nat detail
Manual NAT Policies (Section 1)
```

```
<SNIP>
9 (INSIDE) to (Outside-1) source static DOUBLE_NAT_R1_real DOUBLE_NAT_R1_map
destination static DOUBLE_NAT_R4_map DOUBLE_NAT_R4_real
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.117/32
    Destination - Origin: 192.168.103.4/32, Translated: 4.4.4.4/32
<SNIP>
```

Step 2: Ping and telnet from R1. Use 192.168.103.4 to connect to R4 Lo0.

```
R1#telnet 192.168.103.4
Trying 192.168.103.4 ... Open

R4#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:53:15
*514 vty 0                 idle                 00:00:00 200.100.34.117


R1#ping 192.168.103.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.103.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Task 15: NAT control on ASA-1

- Enable NAT-Control to ensure that a translation rule exists for any outbound connections on ASA-1.

Task-15:Solutions

Step 1: Enable NAT-CONTROL on ASA-1

```
nat-control
```

Verification

Step 1: Verify NAT rules to check for implicit deny due to nat-control.

```
ASA-001fw(config)# sh nat

NAT policies on Interface DMZ1:
  match ip DMZ1 any OUTSIDE any
    no translation group, implicit deny
```

```
    policy_hits = 0

NAT policies on Interface inside:
  match ip inside any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
  match ip inside any DMZ1 any
    no translation group, implicit deny
    policy_hits = 0
  match ip inside any Dmz2 any
    no translation group, implicit deny
    policy_hits = 0

NAT policies on Interface Dmz2:
  match ip Dmz2 any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
  match ip Dmz2 any DMZ1 any
    no translation group, implicit deny
    policy_hits = 0
```

Task 16: Dynamic NAT/PAT on ASA-1

- Translate all outbound connections from any internal and dmz zones to a global pool of 45.45.45.200 to 45.45.45.250. Back this pool with a PAT. The PAT IP address is 45.45.45.251. If this PAT pool is exhausted, the ASAs outside interface should be used as the next backup PAT address.

Task-16:Solutions

Step 1: Configure dynamic NAT/PAT on ASA-1

```
nat (DMZ1) 1 0.0.0.0 0.0.0.0
nat (inside) 1 0.0.0.0 0.0.0.0
nat (Dmz2) 1 0.0.0.0 0.0.0.0

global (OUTSIDE) 1 45.45.45.200-45.45.45.250
global (OUTSIDE) 1 45.45.45.251
global (OUTSIDE) 1 interface
```

Verification

Step 1: Verify NAT rule table

```
ASA-001fw(config)# sh nat

NAT policies on Interface DMZ1:
  match ip DMZ1 any OUTSIDE any
```

```
    dynamic translation to pool 1 (45.45.45.200 - 45.45.45.250)
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any DMZ1 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0

NAT policies on Interface inside:
  match ip inside any OUTSIDE any
    dynamic translation to pool 1 (45.45.45.200 - 45.45.45.250)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any DMZ1 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any inside any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any Dmz2 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
  match ip inside any DMZ1 any
    no translation group, implicit deny
    policy_hits = 0
  match ip inside any Dmz2 any
    no translation group, implicit deny
    policy_hits = 0

NAT policies on Interface Dmz2:
  match ip Dmz2 any OUTSIDE any
    dynamic translation to pool 1 (45.45.45.200 - 45.45.45.250)
    translate_hits = 0, untranslate_hits = 0
  match ip Dmz2 any DMZ1 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip Dmz2 any Dmz2 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip Dmz2 any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
  match ip Dmz2 any DMZ1 any
    no translation group, implicit deny
    policy_hits = 0
```

Step 2: Telnet from R6 to R4. This should get translated to one the IP address of global pool. Also check the XLATE table if the entry has been created on the ASA.

```
R6#45.45.45.4
Trying 45.45.45.4 ... Open
```

```
R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 01:18:33
*514 vty 0                 idle                 00:00:00 45.45.45.223

ASA-001fw(config)# sh xlate
1 in use, 20 most used
Global 45.45.45.223 Local 192.168.60.6
```

Task 17: Policy Dynamic PAT on ASA-1

- All outbound HTTP traffic from R8 Loopback1 (88.88.88.88) should be PATed to 45.45.45.101.

Task-17:Solutions

Step 1: Configure ACL for policy NAT

```
access-list r8weblo1 extended permit tcp host 88.88.88.88 any eq www
```

Step 2: Configure policy dynamic NAT

```
nat (Dmz2) 2 access-list r8weblo1
global (OUTSIDE) 2 45.45.45.101
```

Verification

Step 1: Verify NAT rule table

```
ASA-001fw(config)# sh nat dmz2
  match tcp Dmz2 host 88.88.88.88 OUTSIDE any eq 80
    dynamic translation to pool 2 (45.45.45.101)
    translate_hits = 1, untranslate_hits = 0
<SNIP>
```

Step 2: Telnet from R8 to R4 on port 80 using loopback 1 as the source.

```
R8#telnet 45.45.45.4 80 /source-interface lo1
Trying 45.45.45.4, 80 ... Open
GET
HTTP/1.1 400 Bad Request
Date: Fri, 22 Feb 201308:23:49 GMT
Server: cisco-IOS
Accept-Ranges: none
```

```
400 Bad Request

[Connection to 45.45.45.4 closed by foreign host]
```

Task 18: Static NAT on ASA-1

- Configure Static NAT as per the table below. Allow HTTP, FTP, HTTPS, Telnet, TACACS+, SSH, and ICMP Echo traffic from anyone on the outside to the translated IPs. Use a minimum number of ACEs. Do not use enhanced service object groups.

Real IP	Mapped IP	Real Interface	Mapped Interface
192.168.60.6	45.45.45.6	inside	OUTSIDE
192.168.70.7	45.45.45.7	DMZ1	OUTSIDE
192.168.80.8	45.45.45.8	Dmz2	OUTSIDE

Task-18:Solutions

Step 1: Configure static NAT

```
static (inside,OUTSIDE) 45.45.45.6 192.168.60.6 netmask 255.255.255.255
static (DMZ1,OUTSIDE) 45.45.45.7 192.168.70.7 netmask 255.255.255.255
static (Dmz2,OUTSIDE) 45.45.45.8 192.168.80.8 netmask 255.255.255.255
```

Step 2: Configure Object groups

```
object-group network N1
 network-object host 45.45.45.6
 network-object host 45.45.45.7
 network-object host 45.45.45.8


object-group service S1 tcp
 port-object eq tacacs
 port-object eq telnet
 port-object eq ssh
 port-object eq www
 port-object eq https
 port-object eq ftp
```

Step 3: Configure ACL's

```
access-list out extended permit tcp any object-group N1 object-group S1
access-list out extended permit icmp any object-group N1 echo
access-group out in interface OUTSIDE
```

Verification

Step 1: Verify NAT rule table

```
ASA-001fw(config)# sh nat inside
  match ip inside host 192.168.60.6 OUTSIDE any
    static translation to 45.45.45.6
    translate_hits = 1, untranslate_hits = 14

ASA-001fw(config)# sh nat dmz1
  match ip DMZ1 host 192.168.70.7 OUTSIDE any
    static translation to 45.45.45.7
    translate_hits = 0, untranslate_hits = 14

ASA-001fw(config)# sh nat dmz2
  match ip Dmz2 host 192.168.80.8 OUTSIDE any
    static translation to 45.45.45.8
    translate_hits = 0, untranslate_hits = 9
```

Step 2: Perform basic ping test from R4 to the translated IP's

```
R4#ping 45.45.45.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 45.45.45.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 45.45.45.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 19: Static Identity NAT on ASA-1

- Configure Static Identity NAT as per the table below. Allow Outside users to be able to ping and Telnet to these IPs. Use a minimum number of ACEs. Do not use enhanced service object groups.

Real IP	Mapped IP	Real Interface	Mapped Interface
6.6.6.6	6.6.6.6	inside	OUTSIDE
7.7.7.7	7.7.7.7	DMZ1	OUTSIDE
8.8.8.8	8.8.8.8	Dmz2	OUTSIDE

Task-19:Solutions

Step 1: Configure static identity NAT

```
static (inside,OUTSIDE) 6.6.6.6 6.6.6.6 netmask 255.255.255.255
static (DMZ1,OUTSIDE) 7.7.7.7 7.7.7.7 netmask 255.255.255.255
static (Dmz2,OUTSIDE) 8.8.8.8 8.8.8.8 netmask 255.255.255.255
```

Step 2: Configure Object groups

```
object-group network N2
 network-object host 6.6.6.6
 network-object host 7.7.7.7
 network-object host 8.8.8.8
```

Step 3: Configure ACL

```
access-list out extended permit icmp any object-group N2
access-list out extended permit tcp any object-group N2 eq telnet
```

Verification

Step 1: Verify NAT rule table

If you observe static commands are populated as rules in the NAT table based on the order in which they have been entered unlike NAT command which is re-ordered automatically where more specific/best match is ordered first irrespective of the order of entry.

```
ASA-001fw(config)# sh nat inside
  match ip inside host 192.168.60.6 OUTSIDE any
    static translation to 45.45.45.6
    translate_hits = 1, untranslate_hits = 14
  match ip inside host 6.6.6.6 OUTSIDE any
    static translation to 6.6.6.6
    translate_hits = 0, untranslate_hits = 5
```

```
<SNIP>

ASA-001fw(config)# sh nat dmz1
  match ip DMZ1 host 192.168.70.7 OUTSIDE any
    static translation to 45.45.45.7
    translate_hits = 0, untranslate_hits = 14
  match ip DMZ1 host 7.7.7.7 OUTSIDE any
    static translation to 7.7.7.7
    translate_hits = 0, untranslate_hits = 5
<SNIP>

ASA-001fw(config)# sh nat dmz2
  match ip Dmz2 host 192.168.80.8 OUTSIDE any
    static translation to 45.45.45.8
    translate_hits = 0, untranslate_hits = 9
  match ip Dmz2 host 8.8.8.8 OUTSIDE any
    static translation to 8.8.8.8
    translate_hits = 0, untranslate_hits = 5
<SNIP>
```

Step 2: Perform basic ping test from R4.

```
R4#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 7.7.7.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 20: Static PAT on ASA-1

- Create a new loopback on R7 with an IP address of 177.177.177.177/32 and advertise that into OSPF.
- Any Telnet request that is sent to the ASA's outside interface should be redirected to 177.177.177.177.

- Create a new loopback on R8 with an IP address of 188.188.188.188/32 and advertise that into OSPF.
- Redirect all HTTP requests sent to 45.45.45.80 to 188.188.188.188.
- Redirect all Telnet requests sent to 45.45.45.81 to 188.188.188.188.
- Redirect all SSH requests sent to 45.45.45.82 to 188.188.188.188.
- Redirect all DNS requests sent to 45.45.45.83 to 188.188.188.188.
- Configure appropriate ACLs to allow access.

Task-20:Solutions

Step 1: Configure Loopbacks on R7 and R8 and advertise into OSPF

```
R7
interface Loopback177
 ip address 177.177.177.177 255.255.255.255
 ip ospf 1 area 0

R8
interface Loopback188
 ip address 188.188.188.188 255.255.255.255
 ip ospf 1 area 0
```

Step 2: Configure static PAT

```
static (DMZ1,OUTSIDE) tcp interface telnet 177.177.177.177 telnet
static (Dmz2,OUTSIDE) tcp 45.45.45.80 www 188.188.188.188 www
static (Dmz2,OUTSIDE) tcp 45.45.45.81 telnet 188.188.188.188 telnet
static (Dmz2,OUTSIDE) tcp 45.45.45.82 ssh 188.188.188.188 ssh
static (Dmz2,OUTSIDE) udp 45.45.45.83 domain 188.188.188.188 domain
```

Step 3: Configure ACL's to allow access to these servers

```
access-list out extended permit tcp any host 45.45.45.80 eq www
access-list out extended permit tcp any host 45.45.45.81 eq telnet
access-list out extended permit tcp any host 45.45.45.82 eq ssh
access-list out extended permit udp any host 45.45.45.83 eq domain
access-list out extended permit tcp interface OUTSIDE eq telnet
```

Verification

Step 1: Use telnet from R4 to the translated IP's and port to simulate the connection.

```
R4#telnet 45.45.45.10
```

```
Trying 45.45.45.10 ... Open

R7#exit

[Connection to 45.45.45.10 closed by foreign host]


R4#telnet 45.45.45.80 80
Trying 45.45.45.80, 80 ... Open
GET
HTTP/1.1 400 Bad Request
Date: Fri, 22 Feb 201308:54:30 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 45.45.45.80 closed by foreign host]


R4#telnet 45.45.45.81
Trying 45.45.45.81 ... Open

R8#exit

[Connection to 45.45.45.81 closed by foreign host]
```

Step 2: Verify NAT rule table

```
ASA-001fw(config)# sh nat dmz1
  match ip DMZ1 host 192.168.70.7 OUTSIDE any
    static translation to 45.45.45.7
    translate_hits = 0, untranslate_hits = 14
  match ip DMZ1 host 7.7.7.7 OUTSIDE any
    static translation to 7.7.7.7
    translate_hits = 0, untranslate_hits = 5
  match tcp DMZ1 host 177.177.177.177 eq 23 OUTSIDE any
    static translation to 45.45.45.10/23
    translate_hits = 0, untranslate_hits = 2
  match ip DMZ1 any OUTSIDE any
    dynamic translation to pool 1 (45.45.45.200 - 45.45.45.250)
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any DMZ1 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
```

```
ASA-001fw(config)# sh nat dmz2
  match ip Dmz2 host 192.168.80.8 OUTSIDE any
    static translation to 45.45.45.8
    translate_hits = 0, untranslate_hits = 9
  match ip Dmz2 host 8.8.8.8 OUTSIDE any
    static translation to 8.8.8.8
    translate_hits = 0, untranslate_hits = 5
  match tcp Dmz2 host 188.188.188.188 eq 80 OUTSIDE any
    static translation to 45.45.45.80/80
    translate_hits = 0, untranslate_hits = 1
  match tcp Dmz2 host 188.188.188.188 eq 23 OUTSIDE any
    static translation to 45.45.45.81/23
    translate_hits = 1, untranslate_hits = 2
  match tcp Dmz2 host 188.188.188.188 eq 22 OUTSIDE any
    static translation to 45.45.45.82/22
    translate_hits = 0, untranslate_hits = 0
  match udp Dmz2 host 188.188.188.188 eq 53 OUTSIDE any
    static translation to 45.45.45.83/53
    translate_hits = 0, untranslate_hits = 0
<SNIP>
```

Task 21: Static Policy NAT on ASA-1

- Create a new loopback on R6 with an IP address of 166.166.166.166/32 and advertise that into OSPF.
- When 166.166.166.166 communicates with 4.4.4.4, it should be translated to 45.45.45.50.
- When 166.166.166.166 communicates with 5.5.5.5, it should be translated to 45.45.45.51.

Task-21:Solutions

Step 1: Configure Loobacks on R6 and advertise into OSPF

```
R6
interface Loopback166
 ip address 166.166.166.166 255.255.255.255
 ip ospf 1 area 0
```

Step 2: Configure ACL's for policy static NAT

```
access-list r4lo166 extended permit ip host 166.166.166.166 host 4.4.4.4
access-list r5lo166 extended permit ip host 166.166.166.166 host 5.5.5.5
```

Step 3: Configure policy static NAT

```
static (inside,OUTSIDE) 45.45.45.50  access-list r4lo166
static (inside,OUTSIDE) 45.45.45.51  access-list r5lo166
```

Verification

Step 1: Telnet from R6 lo166 to 4.4.4.4 and 5.5.5.5

```
R6#telnet 4.4.4.4 /source-interface lo166
Trying 4.4.4.4 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:06:01
*514 vty 0                 idle                 00:00:00 45.45.45.50



R6#telnet 5.5.5.5 /source-interface lo166
Trying 5.5.5.5 ... Open

R5#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:46:52
*514 vty 0                 idle                 00:00:00 45.45.45.51
```

Step 2: Verify NAT table rule

```
ASA-001fw(config)# sh nat inside
  match ip inside host 192.168.60.6 OUTSIDE any
    static translation to 45.45.45.6
    translate_hits = 1, untranslate_hits = 14
  match ip inside host 6.6.6.6 OUTSIDE any
    static translation to 6.6.6.6
    translate_hits = 0, untranslate_hits = 5
  match ip inside host 166.166.166.166 OUTSIDE host 4.4.4.4
    static translation to 45.45.45.50
    translate_hits = 1, untranslate_hits = 0
  match ip inside host 166.166.166.166 OUTSIDE host 5.5.5.5
    static translation to 45.45.45.51
    translate_hits = 1, untranslate_hits = 0
  match ip inside any OUTSIDE any
    dynamic translation to pool 1 (45.45.45.200 - 45.45.45.250)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any DMZ1 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
```

```
  match ip inside any inside any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any Dmz2 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
  match ip inside any DMZ1 any
    no translation group, implicit deny
    policy_hits = 0
  match ip inside any Dmz2 any
    no translation group, implicit deny
    policy_hits = 0
```

Task 22: Identity NAT on ASA-1

- Configure Identity NAT for 77.77.77.77 for outbound connections only.

Task-22:Solutions

Step 1: Configure identity NAT

```
nat (DMZ1) 0 77.77.77.77 255.255.255.255
```

Verification

Step 1: Telnet from R4 lo166 to 4.4.4.4 and 5.5.5.5

```
R7#telnet 4.4.4.4 /source-interface lo1
Trying 4.4.4.4 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:10:01
*514 vty 0                 idle                 00:00:00 77.77.77.77
```

Step 2: Verify NAT table rules

If you observe identity NAT always takes low priority over other rules hence it is automatically added to lower part of the NAT rule table (after Exemptions, static NAT etc.). It is valid only for outbound connections.

```
ASA-001fw(config)# sh nat dmz1
  match ip DMZ1 host 192.168.70.7 OUTSIDE any
```

```
    static translation to 45.45.45.7
    translate_hits = 0, untranslate_hits = 14
  match ip DMZ1 host 7.7.7.7 OUTSIDE any
    static translation to 7.7.7.7
    translate_hits = 0, untranslate_hits = 5
  match tcp DMZ1 host 177.177.177.177 eq 23 OUTSIDE any
    static translation to 45.45.45.10/23
    translate_hits = 0, untranslate_hits = 2
  match ip DMZ1 host 77.77.77.77 OUTSIDE any
    identity NAT translation, pool 0
    translate_hits = 1, untranslate_hits = 0
  match ip DMZ1 host 77.77.77.77 DMZ1 any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any OUTSIDE any
    dynamic translation to pool 1 (45.45.45.200 - 45.45.45.250)
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any DMZ1 any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip DMZ1 any OUTSIDE any
    no translation group, implicit deny
    policy_hits = 0
```

Task 23: NAT Exception on ASA-1

- Configure NAT exception traffic for VPN traffic between VLAN60 and VLAN301.

Task-23:Solutions

Step 1: Configure ACL's for NAT exemption

```
access-list NONAT extended permit ip 192.168.60.0 255.255.255.0 192.168.103.0
255.255.255.0
```

Step 2: Configure NAT exemption

```
nat (inside) 0 access-list NONAT
```

Verification

Step 1: Verify NAT table rules

```
If you observe NAT exemption always takes precedence over any other rule
hence it is automatically added to the top of the NAT rule table. It is valid
for both inbound and outbound connections.
```

```
ASA-001fw(config)# sh nat inside
  match   ip   inside   192.168.60.0   255.255.255.0   OUTSIDE   192.168.103.0
255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip inside 192.168.60.0 255.255.255.0 DMZ1 192.168.103.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match   ip   inside   192.168.60.0   255.255.255.0   inside   192.168.103.0
255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip inside 192.168.60.0 255.255.255.0 Dmz2 192.168.103.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip inside host 192.168.60.6 OUTSIDE any
    static translation to 45.45.45.6
    translate_hits = 1, untranslate_hits = 14
  match ip inside host 6.6.6.6 OUTSIDE any
    static translation to 6.6.6.6
    translate_hits = 0, untranslate_hits = 5
  match ip inside host 166.166.166.166 OUTSIDE host 4.4.4.4
    static translation to 45.45.45.50
    translate_hits = 2, untranslate_hits = 0
  match ip inside host 166.166.166.166 OUTSIDE host 5.5.5.5
    static translation to 45.45.45.51
    translate_hits = 1, untranslate_hits = 0
```

Task 24: Outside/Destination Static NAT on ASA-1

- Configure Destination Static NAT such that inside users can communicate with R4's Fa0/1 (45.45.45.4) interface using an IP address of 192.168.60.45.

Task-24:Solutions

Step 1: Configure Destination NAT (similar to twice NAT)

```
static (OUTSIDE,inside) 192.168.60.45 45.45.45.4
```

Verification

Step 1: Telnet from R6 to 192.168.60.45

```
R6#telnet 192.168.60.45
```

```
Trying 192.168.60.45 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:59
*514 vty 0                 idle                 00:00:00 45.45.45.6
```

Step 2: Verify NAT table rules

```
ASA-001fw(config)# sh nat OUTSIDE
  match ip OUTSIDE host 45.45.45.4 inside any
    static translation to 192.168.60.45
    translate_hits = 0, untranslate_hits = 1
```

Task 25: DNS doctoring using NAT

- Configure a static translation for a server located on an inside subnet with an IP address of 192.168.60.100 to 45.45.45.100 on the outside.
- Internal users are unable to connect to this server due to a DNS resolution problem. Perform DNS rewrite using static NAT.
- Allow HTTP access to this server on weekdays from 9 AM to 5 PM from 1st June 2013 onwards. Log all permits that match this ACE. The logging level should be set to the default of informational.

Task-25: Solutions

Step 1: Configure Static NAT with DNS re-write

```
static (inside,OUTSIDE) 45.45.45.100 192.168.60.100 dns
```

Step 2: Configure time range needed for the ACL's

```
time-range WEEKDAYS_9_5
 absolute start 09:00 01 June 2013
 periodic weekdays 9:00 to 17:00
```

Step 3: Configure time range ACL's to allow access to this web server with log option.

```
access-list out extended permit tcp any host 45.45.45.100 eq www log 6 time-
range WEEKDAYS_9_5
```

Verification

Step 1: Check the current clock and the access list to check if it is inactive.

```
ASA-001fw(config)# sh clock
15:01:40.730 IST Fri Feb 28 2013

Show access-list
<SNIP>
access-list out line 10 extended permit tcp any host 45.45.45.100 eq www log
debugging interval 300 time-range WEEKDAYS_9_5 (hitcnt=0) (inactive)
<SNIP>
```

Step 2: Change the clock settings to make the ACL active. Remember ASA has been configured as NTP client.

```
ASA-001fw(config)# clock set 15:00:00 3 june 2013

Show access-list
<SNIP>
access-list out line 10 extended permit tcp any host 45.45.45.100 eq www log
debugging interval 300 time-range WEEKDAYS_9_5 (hitcnt=0)
<SNIP>
```

Step 3: Telnet from R4 to 45.45.45.100 on port 80 to simulate the connection.

```
R4#telnet 45.45.45.100 80
Trying 45.45.45.100, 80 ... Open
GET
HTTP/1.1 400 Bad Request
Date: Fri, 22 Feb 201309:42:24 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 45.45.45.100 closed by foreign host]
```

Step 4: Verify NAT table rules

```
ASA-001fw(config)# sh nat inside
<SNIP>
  match ip inside host 192.168.60.100 OUTSIDE any
    static translation to 45.45.45.100
    translate_hits = 0, untranslate_hits = 12
<SNIP>
```

Task 26: Enhanced Service Object-Groups

- DMZ1 contains the following servers given below. Configure Static NAT for these servers. Allow HTTP, HTTPS, FTP, DNS, RADIUS, TACACS+, SMTP, TFTP, ICMP, and IPSec traffic to these servers from the outside. Use a single ACL to accomplish this task.

Real IP Address	Mapped IP Address	Mapped Interface
192.168.70.60	45.45.45.60	OUTSIDE
192.168.70.61	45.45.45.61	OUTSIDE
192.168.70.62	45.45.45.62	OUTSIDE
192.168.70.63	45.45.45.63	OUTSIDE
192.168.70.64	45.45.45.64	OUTSIDE

Task-26:Solutions

Step 1: Configure static NAT for the servers.

```
static (dmz1,OUTSIDE) 45.45.45.60 192.168.70.60
static (dmz1,OUTSIDE) 45.45.45.61 192.168.70.61
static (dmz1,OUTSIDE) 45.45.45.62 192.168.70.62
static (dmz1,OUTSIDE) 45.45.45.63 192.168.70.63
static (dmz1,OUTSIDE) 45.45.45.64 192.168.70.64
```

Step 2: Configure object groups

```
object-group network N3
 network-object host 45.45.45.60
 network-object host 45.45.45.61
 network-object host 45.45.45.62
 network-object host 45.45.45.63
 network-object host 45.45.45.64

object-group service ES
 service-object icmp
 service-object udp eq isakmp
 service-object udp eq 4500
 service-object esp
  service-object tcp eq smtp
 service-object tcp eq www
 service-object tcp eq https
 service-object tcp eq ftp
 service-object tcp eq tacacs
 service-object udp eq domain
 service-object udp eq radius
 service-object udp eq radius-acct
 service-object udp eq tftp
```

Step 3: Configure ACL's using enhanced service object groups

```
access-list out extended permit object-group ES any object-group N3
```

Verification

Step 1: Perform basic ping test from R4 to the translated IP's.

```
R4#ping 45.45.45.60

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.60, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 45.45.45.61

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.61, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 45.45.45.62

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.62, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 45.45.45.63

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.63, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 45.45.45.64

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.64, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Step 2: Verify NAT rule table

```
ASA-001fw(config)# sh nat dmz1
  <SNIP>
  match ip DMZ1 host 192.168.70.60 OUTSIDE any
    static translation to 45.45.45.60
    translate_hits = 0, untranslate_hits = 5
```

```
  match ip DMZ1 host 192.168.70.61 OUTSIDE any
    static translation to 45.45.45.61
    translate_hits = 0, untranslate_hits = 5
  match ip DMZ1 host 192.168.70.62 OUTSIDE any
    static translation to 45.45.45.62
    translate_hits = 0, untranslate_hits = 5
  match ip DMZ1 host 192.168.70.63 OUTSIDE any
    static translation to 45.45.45.63
    translate_hits = 0, untranslate_hits = 5
  match ip DMZ1 host 192.168.70.64 OUTSIDE any
    static translation to 45.45.45.64
    translate_hits = 0, untranslate_hits = 5
  <SNIP>
```

Task 27: ICMP Filters on ASA-1

- Configure the ASA such that no device on the outside can ping its outside interface while the ASA can ping any outside device. Use a single command to accomplish this task and do not use ACLs.

Task-27:Solutions

Step 1: Configure ICMP filters

```
icmp permit any echo-reply OUTSIDE
```

Verification

Step 1: Perform basic ping test from R4 to the ASA interface and from ASA to other devices.

```
R4#ping 45.45.45.10 (before ICMP filter)

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R4#ping 45.45.45.10 (after ICMP filter)

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ASA can still ping any device.

ASA-001fw(config)# ping 4.4.4.4
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA-001fw(config)# ping 45.45.45.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 45.45.45.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Task 28: uRPF and fragmented packets on ASA-1

- Enable an uRPF check on the outside interface of ASA-1 and the firewall should not allow any fragmented packets passing through from the outside interface.

Task-28:Solutions

Step 1: Deny fragments on the outside interface and enable uRPF check on the outside.

```
fragment chain 1 OUTSIDE
ip verify reverse-path interface OUTSIDE
```

Verification

Step 1: Ping from R4 with a size greater than 1500 bytes fragment ICMP packets.

```
R4#ping 6.6.6.6 size 1500
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R4#ping 6.6.6.6 size 1501
Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ASA
ASA-001fw : %ASA-4-209005: Discard IP fragment set with more than 1 elements:
src = 45.45.45.4, dest = 6.6.6.6, proto = ICMP, id = 193
```

Step 2: Use show command to verify uRPF drops

```
show ip verify statistics interface OUTSIDE
interface OUTSIDE: 0 unicast rpf drops
```

Task 29: ACL Logging on ASA-1

- Configure ASA-1 to generate warning syslog messages of 106100 for all the denied packets.
- Change the maximum number of denied flows that generate syslog messages to 2000 and set the interval between the maximum denied flow syslog message generations to 3600 seconds.

Task-29:Solutions

Step 1:

```
access-list deny-flow-max 2000
access-list alert-interval 3600

access-list out deny ip any any log
```

Verification

Step 1: Simulate a connection from R4 such that the ASA generates syslog 106100 for the denied packets.

```
ASA-001fw : %ASA-6-106100: access-list out denied tcp
OUTSIDE/45.45.45.4(52784) -> inside/6.6.6.6(9999) hit-cnt 1 first hit
```

Task 30: Control Plane ACL on ASA-1

- Configure the control plane ACL on ASA-1 to allow only OSPF packets on the outside interface.

Task-30:Solutions

Step 1: Configure a set of ACL's to permit OSPF packets and deny remaining.

```
access-list OSPF_CP permit ospf any any
access-list OSPF_CP deny ip any any

access-group OSPF_CP in interface OUTSIDE control-plane
```

Task 31: Management access for ASA-1

- Configure appropriate global ACLs on ASA-3 such that the Test PC can manage the ASA-1 from VLAN 101 (SSH). You have already configured the management access in LAB 3.
- Test the ASDM access to ASA-1 from the Test PC located in VLAN 100.

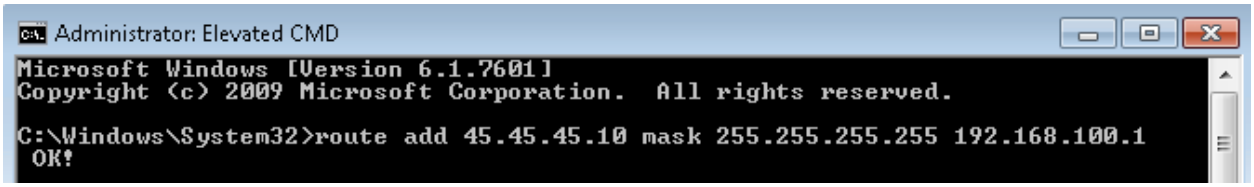
Task-31:Solutions

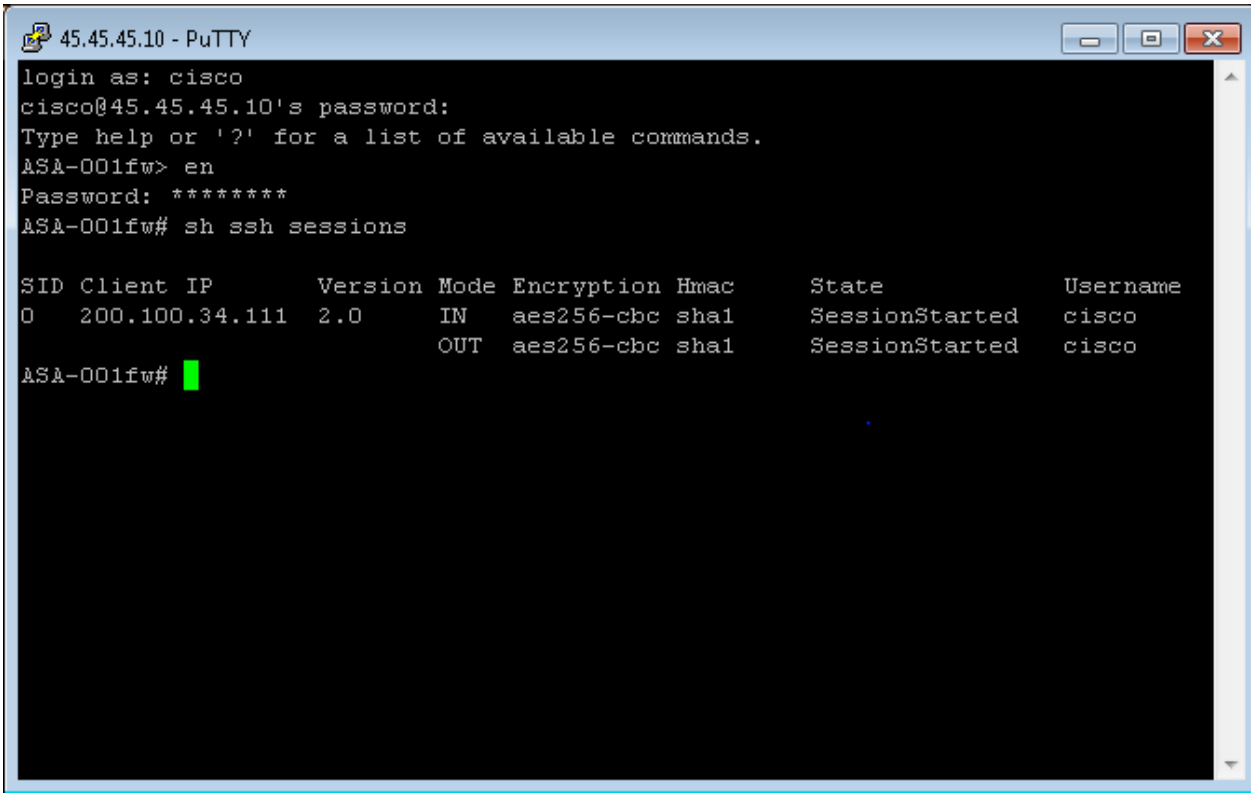
Step 1: Create ACL's to allow access on ASA3

```
access-list GLOBAL extended permit tcp host 192.168.100.200 host 45.45.45.10
eq ssh
```

Verification

Step 1: Configure static route on the test PC and use putty to SSH into ASA1





NOTES

Global ACL's – One of the main motivation to create global ACL feature was to minimize the number of ACL's created during checkpoint to ASA migration and to create flow based policy. These provide interface independent policies. Global ACL's provides access control to traffic on all interfaces except for internal interfaces such as Loopback, identity, Internal-Control, Internal-Data, etc only in the ingress/input direction. They do not support control-plane or per-user-override features. The order of processing ACL's is given below.

Order:

1. interface ACL's
2. global ACL's
3. default glabal ACL rule *(deny ip any any)*

Interface ACL rules has a priority of 13 in the ASP table.

Global ACLs has a priority of 12. (Higher the value more the priority and higher the priority is processed first, hence interface ACL's are processed before Global ACL entries).

It is very important to understand that the implicit deny ip any any of the global ACL has a priority of 11. This means that once a global ACL is applied, the implicit *deny ip any any* rule is removed from the interface rule and added to the end of the global rule.

NAT Simplification in 8.4/8.6 - NAT has been simplified in configuration where all the NAT rules recide in a single global table which is divided into 3 sections, ability to insert NAT rule in any arbiratary manner, independt of security level, interfaces, ACL, ability to use objects instead of inline IP's

NAT rules globally recide in a single table and rules are applied on first match basis. The Global NAT rule table is divided into 3 sections –

- Section 1 (Manual NAT and Twice NAT) – NAT rules instered by the user in any order. Similar to policy NAT where source and destination can be specified. Can translate both source and destination in a single rule. NAT command can contain the objects/object-groups or IP's. You must specify the source and destination. Manual NAT has higher precedence over auto nat (section 2) by default unless it is placed in section 3.
- Section 2 (Auto NAT or Object NAT) – Rules are automatically placed by the ASA when NAT command is used inside the object. Does not support policy NAT (i.e. destination based). Only one NAT command can be used inside the object hence either the source or destination IP/port can be translated in one rule. Order is done by the ASA automatically – Static over dynamic, longest prefix, lower numeric from the 1st octect etc
- Section 3 (Manual NAT) – Same command syntax and logic as rules in section 1 i.e. Manual NAT but "after-auto" keyword is used so that this NAT rule takes lower precedence and is matched after section 2.

You may refer the documentation for more information.

Lab 5: High Availability and Modular Policy Framework on the ASA

Lab-5: High Availability and Modular Policy Framework on ASA – This lab is intended to let you be familiar with configuring stateful failover, which provides device level HA and modular policy framework (MPF). Using MPF we can configure the ASA for application inspection, set connection limits, QOS, TCP normalization and diverting traffic to IPS modules.

General Rules

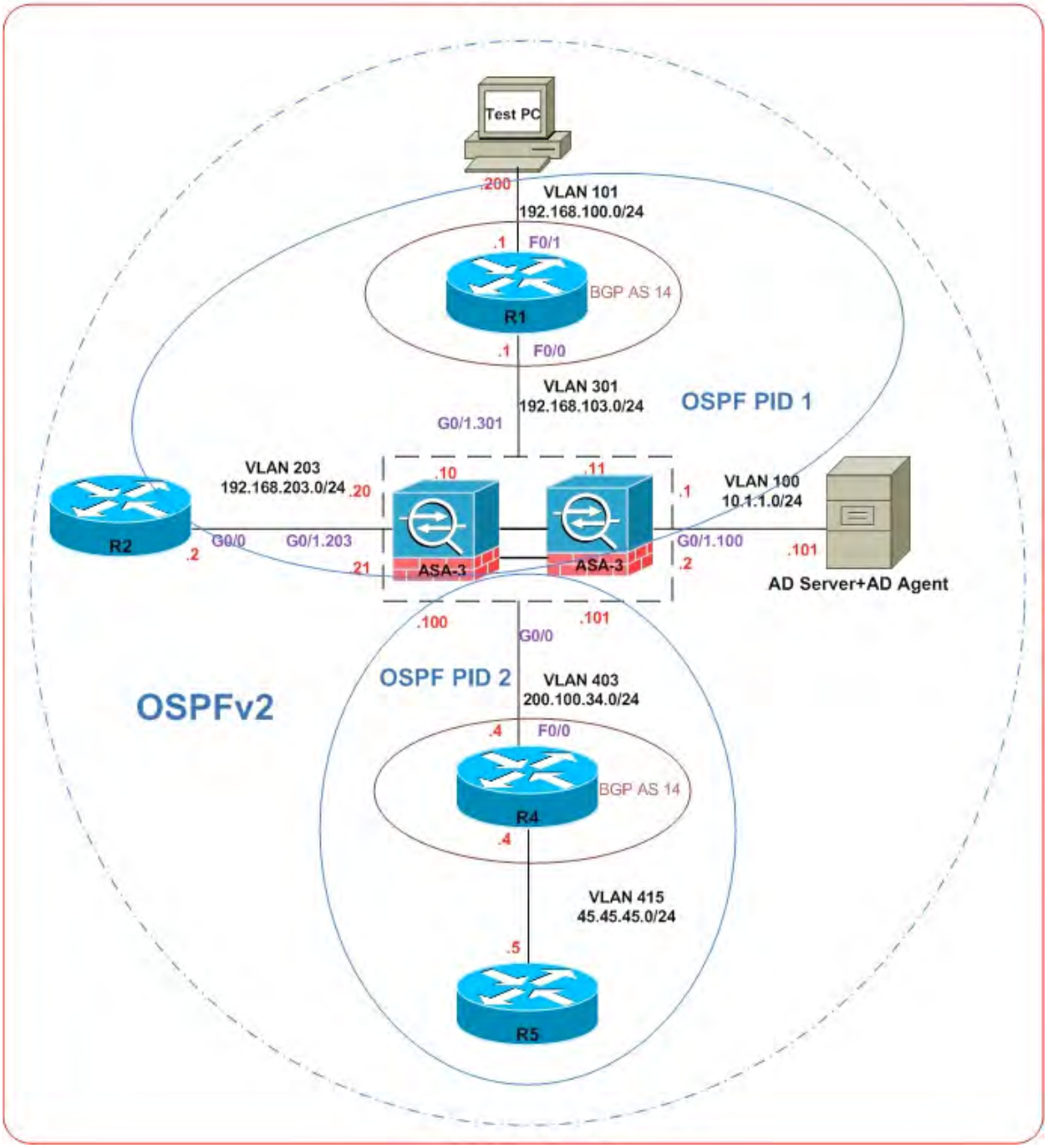
- By now you should understand how NAT works in 8.6/8.4 and 8.2 versions and how ACLs work on the ASA.
- You should understand the new logical topology (Network Topology 1.3).
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 3 Hours

Pre-setup

Load the initial configurations for Lab 5. Use the logical topology drawing – Network Topology 1.3. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.3
(Logical)



Detailed Solution:Lab-5

Task 1: Basic Initialization ASA-3

- Configure a hostname of "ASA003" on ASA-3.
- ASA003 should have a domain name of ipexpert.com.
- Configure ASA003 interfaces and the appropriate switchports on the Catalyst with the specifications below. After you perform this task, ensure that you can ping your directly connected neighbors R2, R1, R4, and the AD Server.

ASA Interface	VLAN Tag	Security Level	Name	Active IP Address	Standby IP Address
G0/0	----------	0	outside	200.100.34.100/24	200.100.34.101/24
G0/1.100	100	90	dmz1	10.1.1.1/24	10.1.1.2/24
G0/1.203	203	50	dmz2	192.168.203.20/24	192.168.203.21/24
G0/1.103	103	100	inside	192.168.103.10/24	192.168.103.11/24

Task-2:Solutions

Step 1: Check VLANs and trunks on the switches :

SW3 & SW4

```
interface GigabitEthernet1/0/19
 switchport access vlan 403
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,103,203
 switchport mode trunk
```

Step 2: ASA3 initialization

```
domain-name ipexpert.com
hostname ASA003

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 200.100.34.100 255.255.255.0 standby 200.100.34.101
 no shutdown

interface GigabitEthernet0/1
 no nameif
```

```
 no security-level
 no ip address
 no shutdown

interface GigabitEthernet0/1.100
 vlan 100
 nameif dmz1
 security-level 90
 ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2

interface GigabitEthernet0/1.203
 vlan 203
 nameif dmz2
 security-level 50
 ip address 192.168.203.20 255.255.255.0 standby 192.168.203.21

interface GigabitEthernet0/1.103
 vlan 103
 nameif inside
 security-level 100
 ip address 192.168.103.10 255.255.255.0 standby 192.168.103.11
```

Verification

Step 1: Verify interface configurations and perform ping test to the directly connected neighbors on ASA3

```
ASA003(config)# show interface ip brief
Interface                              IP-Address          OK?  Method  Status
Protocol
GigabitEthernet0/0                        200.100.34.100      YES   manual   up
up
GigabitEthernet0/1                     unassigned             YES  unset    up
up
GigabitEthernet0/1.100             10.1.1.1                    YES   manual   up
up
GigabitEthernet0/1.103                 192.168.103.10       YES   manual   up
up
GigabitEthernet0/1.203                 192.168.203.20       YES   manual   up
up
GigabitEthernet0/2                    30.1.1.1                YES  unset    up
up
GigabitEthernet0/3                    40.1.1.1                YES  unset    up
up
<SNAP>
```

```
ASA003(config)# ping 200.100.34.4
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA003(config)# ping 192.168.103.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.103.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA003(config)# ping 192.168.203.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA003(config)# ping 10.1.1.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Task 2: Configure Active/Standby Failover

- Configure ASA-3 and ASA-4 for device level HA using the failover feature on the ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the parameters below for the failover configuration. Configure the switch such that the Gi0/2 interface of the firewall should be in VLAN 300. Make sure the failover key is encrypted using AES with a password of 1P3X93RT.

Failover interface – Gi0/2
Primary IP – 30.1.1.1/24
Standby IP – 30.1.1.2/24
Interface Name - FA1LOVER
Key - C1SCO

- Monitor all of the dmzs and outside interfaces and change the failed interface policy to 2.
- Enable stateful failover on the Gi0/3 interface with the parameters below. Configure the switch such that the Gi0/3 interface of the firewall should be in VLAN 400.

Stateful Link – Gi0/3
Primary IP – 40.1.1.1/24
Standby IP – 40.1.1.2/24
Interface Name - 5TATE

- Enable replication of HTTP sessions.
- Configure the ASA to allow ICMP traffic from the outside. Do not use Global ACLs.

Task-1:Solutions

Step 1: Make sure CAT3 and CAT4 interfaces connected to the ASAs are properly configured :

```
interface GigabitEthernet1/0/21
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/22
 switchport access vlan 400
 switchport mode access
 spanning-tree portfast
```

Step 2: Configure failover on ASA3 (Primary Unit)

```
interface GigabitEthernet0/2
 no shut
interface GigabitEthernet0/3
 no shut

failover lan unit primary
failover lan interface FA1LOVER GigabitEthernet0/2
failover interface-policy 2
failover key C1SCO
failover replication http
failover link 5TATE GigabitEthernet0/3
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
failover interface ip 5TATE 40.1.1.1 255.255.255.0 standby 40.1.1.2
monitor-interface dmz1
monitor-interface dmz2
failover
```

Step 3: Configure failover on ASA4 (Secondary Unit)

```
interface GigabitEthernet0/2
no shut
interface GigabitEthernet0/3
no shut

failover lan unit secondary
failover lan interface FA1LOVER GigabitEthernet0/2
failover key C1SCO
```

```
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
failover
```

Step 4: Configure AES password encryption.

```
key config-key password-encryption 1P3X93RT
password encryption aes
```

Step 5: Configure ACL's to allow outside access

```
access-list out extended permit icmp any any
access-group out in interface outside
```

Verification

Step 1: Verify Failover on primary and secondary units.

```
ASA003(config)# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FA1LOVER GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 2
Monitored Interfaces 3 of 114 maximum
failover replication http
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 05:10:56 UTC Feb 10 2013
      This host: Primary - Active
            Active time: 2857 (sec)
            slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
              Interface outside (200.100.34.100): Normal (Monitored)
              Interface dmz1 (10.1.1.1): Normal (Monitored)
              Interface dmz2 (192.168.203.20): Normal (Monitored)
              Interface inside (192.168.103.10): Normal (Not-Monitored)
            slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
              IPS, 7.1(4)E4, Up
      Other host: Secondary - Standby Ready
            Active time: 121 (sec)
            slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
              Interface outside (200.100.34.101): Normal (Monitored)
              Interface dmz1 (10.1.1.2): Normal (Monitored)
              Interface dmz2 (192.168.203.21): Normal (Monitored)
              Interface inside (192.168.103.11): Normal (Not-Monitored)
            slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
              IPS, 7.1(4)E4, Up
```

```
Stateful Failover Logical Update Statistics
      Link : 5TATE GigabitEthernet0/3 (up)
      Stateful Obj      xmit       xerr       rcv        rerr
      General           395        0          347        1
      sys cmd           347        0          347        1
      up time           0          0          0          0
      RPC services      0          0          0          0
      TCP conn          0          0          0          0
      UDP conn          0          0          0          0
      ARP tbl           3          0          0          0
      Xlate_Timeout     0          0          0          0
      IPv6 ND tbl       0          0          0          0
      VPN IKEv1 SA      0          0          0          0
      VPN IKEv1 P2      0          0          0          0
      VPN IKEv2 SA      0          0          0          0
      VPN IKEv2 P2      0          0          0          0
      VPN CTCP upd      0          0          0          0
      VPN SDI upd       0          0          0          0
      VPN DHCP upd      0          0          0          0
      SIP Session       0          0          0          0
      Route Session     42         0          0          0
      User-Identity     3          0          0          0

      Logical Update Queue Information
                  Cur   Max   Total
      Recv Q:     0     5     3012
      Xmit Q:     0     30    3290
```

ASA4

```
ASA003(config)# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: FA1LOVER GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 2
Monitored Interfaces 3 of 114 maximum
failover replication http
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 07:38:29 UTC Feb 9 2013
      This host: Secondary - Standby Ready
            Active time: 121 (sec)
            slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
              Interface outside (200.100.34.101): Normal (Monitored)
              Interface dmz1 (10.1.1.2): Normal (Monitored)
              Interface dmz2 (192.168.203.21): Normal (Monitored)
              Interface inside (192.168.103.11): Normal (Not-Monitored)
```

```
            slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
              IPS, 7.1(4)E4, Up
      Other host: Primary - Active
            Active time: 2911 (sec)
            slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
              Interface outside (200.100.34.100): Normal (Monitored)
              Interface dmz1 (10.1.1.1): Normal (Monitored)
              Interface dmz2 (192.168.203.20): Normal (Monitored)
              Interface inside (192.168.103.10): Normal (Not-Monitored)
            slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
              IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
      Link : 5TATE GigabitEthernet0/3 (up)
      Stateful Obj      xmit       xerr       rcv        rerr
      General           356        0          402        0
      sys cmd           356        0          354        0
      up time           0          0          0          0
      RPC services      0          0          0          0
      TCP conn          0          0          0          0
      UDP conn          0          0          0          0
      ARP tbl           0          0          3          0
      Xlate_Timeout     0          0          0          0
      IPv6 ND tbl       0          0          0          0
      VPN IKEv1 SA      0          0          0          0
      VPN IKEv1 P2      0          0          0          0
      VPN IKEv2 SA      0          0          0          0
      VPN IKEv2 P2      0          0          0          0
      VPN CTCP upd      0          0          0          0
      VPN SDI upd       0          0          0          0
      VPN DHCP upd      0          0          0          0
      SIP Session       0          0          0          0
      Route Session     0          0          42         0
      User-Identity     0          0          3          0

      Logical Update Queue Information
                  Cur   Max   Total
      Recv Q:     0     7     6057
      Xmit Q:     0     1     356
```

Task 3: Routing ASA-3

- Configure OSPF area 0 with a process-id of 1 on all of the dmzs and inside interfaces and generate a default route in OSPF.
- Configure OSPF area 0 with a process-id of 2 on the outside interface.
- Ensure that Inside and DMZ routes are not present on R4 and R5 routing tables.
- Routers are pre-configured for routing.

Task-3:Solutions

Step 1: Configure OSPF on the primary unit

```
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 192.168.103.0 255.255.255.0 area 0
 network 192.168.203.0 255.255.255.0 area 0
 default-information originate always

router ospf 2
 network 200.100.34.0 255.255.255.0 area 0
 log-adj-changes
```

Verification

Step 1: Verify routes on ASA3 and the OSPF neighbor relation state

```
ASA003(config)# sh route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    1.1.1.0 255.255.255.0 [110/11] via 192.168.103.1, 0:14:36, inside
O    2.2.2.0 255.255.255.0 [110/11] via 192.168.203.2, 0:14:36, dmz2
O    4.4.4.0 255.255.255.0 [110/11] via 200.100.34.4, 0:14:36, outside
O    55.55.55.55 255.255.255.255 [110/12] via 200.100.34.4, 0:14:36, outside
C    200.100.34.0 255.255.255.0 is directly connected, outside
O    5.5.5.0 255.255.255.0 [110/12] via 200.100.34.4, 0:14:36, outside
O    22.22.22.22 255.255.255.255 [110/11] via 192.168.203.2, 0:14:36, dmz2
C    40.1.1.0 255.255.255.0 is directly connected, 5TATE
C    10.1.1.0 255.255.255.0 is directly connected, dmz1
C    192.168.203.0 255.255.255.0 is directly connected, dmz2
O    11.11.11.11 255.255.255.255 [110/11] via 192.168.103.1, 0:14:36, inside
C    192.168.103.0 255.255.255.0 is directly connected, inside
O    44.44.44.44 255.255.255.255 [110/11] via 200.100.34.4, 0:14:36, outside
O    192.168.100.0 255.255.255.0 [110/11] via 192.168.103.1, 0:14:36, inside
O    45.45.45.0 255.255.255.0 [110/11] via 200.100.34.4, 0:14:36, outside
C    30.1.1.0 255.255.255.0 is directly connected, FA1LOVER
```

```
ASA003(config)# sh ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/DR         0:00:31     200.100.34.4    outside
1.1.1.1           1   FULL/DR         0:00:32     192.168.103.1   inside
2.2.2.2           1   FULL/DR         0:00:35     192.168.203.2   dmz2
```

Step 2: Ping from R1 Lo0 to R5 Lo0 and verify if the R has received the OSPF route from ASA3

```
R1#ping 5.5.5.5 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.103.10 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.103.10, 00:08:56, FastEthernet0/0
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, Loopback0
L        1.1.1.1/32 is directly connected, Loopback0
      2.0.0.0/24 is subnetted, 1 subnets
O        2.2.2.0 [110/12] via 192.168.103.10, 00:08:56, FastEthernet0/0
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/11] via 192.168.103.10, 00:08:56, FastEthernet0/0
      11.0.0.0/32 is subnetted, 1 subnets
C        11.11.11.11 is directly connected, Loopback1
      22.0.0.0/32 is subnetted, 1 subnets
O        22.22.22.22 [110/12] via 192.168.103.10, 00:08:56, FastEthernet0/0
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, FastEthernet0/1
L        192.168.100.1/32 is directly connected, FastEthernet0/1
      192.168.103.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.103.0/24 is directly connected, FastEthernet0/0
L        192.168.103.1/32 is directly connected, FastEthernet0/0
```

```
O     192.168.203.0/24 [110/11] via 192.168.103.10, 00:08:56, FastEthernet0/0
```

Task 4: Static Auto-NAT for INSIDE on ASA-3

- Configure Static Auto NAT using objects as per the table below.

Real IP	Mapped IP	Real Interface	Mapped Interface
1.1.1.1	1.1.1.1	inside	outside
192.168.103.1	200.100.34.1	inside	outside
192.168.203.53	200.100.34.53	dmz2	outside
192.168.203.2	200.100.34.2	dmz2	outside
11.11.11.11	200.100.34.80	inside	outside
22.22.22.22	200.100.34.81	dmz2	outside
10.1.1.25	200.100.34.25	dmz1	outside
10.1.1.1	200.100.34.50	dmz1	outside
10.1.1.21	200.100.34.21	dmz1	outside

Task-4:Solutions

Step 1: Configure objects on the primary unit i.e. ASA3

```
object network R1_lo0
 host 1.1.1.1
object network R1_f0
 host 192.168.103.1
object network D2_DNS
 host 192.168.203.53
object network R2_f0
 host 192.168.203.2
object network IN_WEB
 host 11.11.11.11
object network D2_WEB
 host 22.22.22.22
object network D1_SMTP
 host 10.1.1.25
object network D1_AD
 host 10.1.1.1
object network D1_FTP
 host 10.1.1.21
```

Step 2: Configure static auto NAT on the primary unit i.e. ASA3

```
object network R1_lo0
 nat (inside,outside) static 1.1.1.1
```

```
object network R1_f0
 nat (inside,outside) static 200.100.34.1

object network D2_DNS
 nat (dmz2,outside) static 200.100.34.53

object network R2_f0
 nat (dmz2,outside) static 200.100.34.2

object network IN_WEB
 nat (inside,outside) static 200.100.34.80

object network D2_WEB
 nat (dmz2,outside) static 200.100.34.81

object network D1_SMTP
 nat (dmz1,outside) static 200.100.34.25

object network D1_AD
 nat (dmz1,outside) static 200.100.34.50

object network D1_FTP
 nat (dmz1,outside) static 200.100.34.21
```

Verification

Step 1: Verify from the NAT table and perform basic ping test from R4

```
ASA003(config)# sh nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_lo0 1.1.1.1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 1.1.1.1/32
2 (dmz1) to (outside) source static D1_AD 200.100.34.50
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.1/32, Translated: 200.100.34.50/32
3 (dmz1) to (outside) source static D1_FTP 200.100.34.21
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.21/32, Translated: 200.100.34.21/32
4 (dmz1) to (outside) source static D1_SMTP 200.100.34.25
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.25/32, Translated: 200.100.34.25/32
5 (inside) to (outside) source static IN_WEB 200.100.34.80
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.80/32
6 (dmz2) to (outside) source static D2_WEB 200.100.34.82
    translate_hits = 0, untranslate_hits = 0
```

```
    Source - Origin: 22.22.22.22/32, Translated: 200.100.34.81/32
7 (inside) to (outside) source static R1_f0 200.100.34.1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.1/32
8 (dmz2) to (outside) source static R2_f0 200.100.34.2
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
9 (dmz2) to (outside) source static D2_DNS 200.100.34.53
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.53/32, Translated: 200.100.34.53/32
```

```
R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 200.100.34.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 200.100.34.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
R4#ping 200.100.34.80

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.80, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R4#ping 200.100.34.81

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.100.34.81, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Task 5: Dynamic PAT for INSIDE on ASA-3

- Configure dynamic PAT such that all outbound connections from DMZs and Inside interfaces are PATed to the ASA's outside interface.

```
object network ALL
 subnet 0.0.0.0 0.0.0.0
```

```
 nat (any,outside) dynamic interface
```

Verification

Step 1: Verify NAT table

```
show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_lo0 1.1.1.1
    translate_hits = 2, untranslate_hits = 2
    Source - Origin: 1.1.1.1/32, Translated: 1.1.1.1/32
2 (dmz1) to (outside) source static D1_AD 200.100.34.50
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.1/32, Translated: 200.100.34.50/32
3 (dmz1) to (outside) source static D1_FTP 200.100.34.21
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.21/32, Translated: 200.100.34.21/32
4 (dmz1) to (outside) source static D1_SMTP 200.100.34.25
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.25/32, Translated: 200.100.34.25/32
5 (inside) to (outside) source static IN_WEB 200.100.34.80
    translate_hits = 2, untranslate_hits = 2
    Source - Origin: 11.11.11.11/32, Translated: 200.100.34.80/32
6 (dmz2) to (outside) source static D2_WEB 200.100.34.81
    translate_hits = 2, untranslate_hits = 2
    Source - Origin: 22.22.22.22/32, Translated: 200.100.34.81/32
7 (inside) to (outside) source static R1_f0 200.100.34.1
    translate_hits = 2, untranslate_hits = 2
    Source - Origin: 192.168.103.1/32, Translated: 200.100.34.1/32
8 (dmz2) to (outside) source static R2_f0 200.100.34.2
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.203.2/32, Translated: 200.100.34.2/32
9 (dmz2) to (outside) source static D2_DNS 200.100.34.53
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.203.53/32, Translated: 200.100.34.53/32
10 (any) to (outside) source dynamic ALL interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 200.100.34.100/24
```

Task 6: IPS Software module traffic diversion on ASA-3

- Divert all traffic to the IPS software module with an inline fail-open policy. Apply this policy to the outside interface.

Task-6:Solutions

Step 1: Configure class map to match all traffic

```
class-map ALL
 match any
```

Step 2: Configure policy map to divert traffic to the IPS with fail-open option and apply to the outside interface

```
policy-map OUT
 class ALL
  ips inline fail-open

service-policy OUT interface outside
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show service-policy ips

Interface outside:
  Service-policy: OUT
    Class-map: ALL
      IPS: card status Up, license status Enabled, mode inline fail-open
        packet input 10, packet output 10, drop 0, reset-drop 0
```

Task 7: ICMP inspection on ASA-3

- Enable ICMP and ICMP error inspection globally and police all incoming ICMP traffic at 8000 bits/sec with a burst size of 1000 bytes/second.

Task-7:Solutions

Step 1: Configure ACL to match ICMP traffic and classify ICMP traffic using class map.

```
access-list icmp extended permit icmp any any

class-map ICMP
 match access-list icmp
```

Step 2: Configure ICMP inspection in the global policy map with policing option

```
policy-map global_policy
 class ICMP
  police input 8000 1000
  inspect icmp
```

```
policy-map global_policy
 class inspection_default
  inspect icmp error
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# sh service-policy global

<SNIP>
    Class-map: ICMP
      Input police Interface outside:
        cir 8000 bps, bc 1000 bytes
        conformed 0 packets, 0 bytes; actions:  transmit
        exceeded 0 packets, 0 bytes; actions:  drop
        conformed 0 bps, exceed 0 bps
      Input police Interface dmz1:
        cir 8000 bps, bc 1000 bytes
        conformed 0 packets, 0 bytes; actions:  transmit
        exceeded 0 packets, 0 bytes; actions:  drop
        conformed 0 bps, exceed 0 bps
      Input police Interface dmz2:
        cir 8000 bps, bc 1000 bytes
        conformed 0 packets, 0 bytes; actions:  transmit
        exceeded 0 packets, 0 bytes; actions:  drop
        conformed 0 bps, exceed 0 bps
      Input police Interface inside:
        cir 8000 bps, bc 1000 bytes
        conformed 0 packets, 0 bytes; actions:  transmit
        exceeded 0 packets, 0 bytes; actions:  drop
        conformed 0 bps, exceed 0 bps
      Inspect: icmp, packet 0, lock fail 0, drop 0, reset-drop 0
```

Task 8: DNS inspection on ASA-3

- 200.100.34.53 is a DNS server. To prevent DNS cache poisoning, configure DNS ID randomization. Only DNS queries related to the ipexpert.com domain should be allowed. Mask the RD bit for more enhanced protection. Apply this policy globally. Allow DNS access to this server. Do not use global ACLs to allow access to this server.
- Report any DNS spoofing attacks towards 200.100.34.53 by generating a syslog message.

Task-8:Solutions

Step 1: Configure ACL's to match DNS traffic towards 200.100.34.53 and create the appropriate class-map. D2_DNS object can be re-used.

```
access-list D2_DNS extended permit udp any object D2_DNS eq domain

class-map R2_DNS
 match access-list D2_DNS
```

Step 2: regex to match ipexpert.com domain

```
regex IPX "ipexpert\.com"
```

Step 3: Configure Layer 7 DNS policy map to specify action

```
policy-map type inspect dns D2_DNS
 parameters
  id-randomization
  id-mismatch count 1 duration 1 action log
 match header-flag RD
  mask
 match not domain-name regex IPX
  drop
```

Step 4: Apply Layer 7 policy map in the Layer3/4 Global policy map for the specific DNS traffic.

```
policy-map global_policy
 class R2_DNS
  inspect dns D2_DNS
```

Step 5: Allow ACL's to permit DNS traffic to 200.100.34.53.

```
access-list out extended permit udp any object D2_DNS eq domain
```

Verification

Step 1: This is a configuration only question.

```
 show service-policy inspect dns
<SNIP>
    Class-map: R2_DNS
      Inspect: dns D2_DNS, packet 0, lock fail 0, drop 0, reset-drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        id-randomization, count 0
        id-mismatch count 1 duration 1, log 0
        match header-flag RD
```

```
          mask, packet 0
        match not domain-name regex IPX
          drop, packet 0
<SNIP>
```

Task 9: FTP inspection on ASA-3

- Configure a policy to prevent web browsers from sending embedded commands in FTP requests. Configure this policy globally.
- 200.100.34.21 is an FTP server running on port 2121. Do not allow users to delete or rename any files on this server. Mask banner and syst command replies. Users should not be able to download any file starting with a string of "confidential". Configure this policy and apply this globally. Allow outside access to this server. Do not use Global ACLs.
- Drop all file executable file types. Apply this globally.

Task-9:Solutions

Step 1: Configure regex to match string starting with confidential

```
regex FILE "^confidential.*"
```

Step 2: Configure Layer 7 FTP policy map to specify the actions

```
policy-map type inspect ftp D1_FTP
 parameters
  mask-banner
  mask-syst-reply
 match request-command rnfr rnto dele
  reset
 match filename regex FILE
  reset log
```

Step 3: Configure ACL's to match traffic towards 200.100.34.21 on TCP port2121 and create appropriate Layer 3/4 class map to match that traffoc

```
access-list D1_FTP permit tcp any obj D1_FTP eq 2121
class-map D01_FTP
 match access-list D1_FTP
```

Step 4: Configure FTP inspection in the global policy for traffic towards 200.100.34.21 and apply L7 FTP policy map for that inspection.

```
policy-map global_policy
```

```
 class D01_FTP
  inspect ftp strict D1_FTP
```

Step 5: Configure ACL's to allow access to this FTP server.

```
access-list out extended permit tcp any object D1_FTP eq 2121
```

Step 6: Configure Regex to match exe files

```
regex EXE_FILES "*.[Ee][Xx][Ee]"
```

Step 7: Configure FTP Layer 7 policy map to match executable files and drop files

```
policy-map type inspect ftp  EXE_FILES
 match filetype regex EXE_FILES
  reset
```

Step 8: Configure FTP inspection in the global policy under inspection_default class map.

```
policy-map global_policy
 class inspection_default
  inspect ftp strict EXE_FILES
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config-pmap-c)# show service-policy inspect ftp

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ftp strict EXE_FILES, packet 0, lock fail 0, drop 0, reset-
drop 0
        match filetype regex EXE_FILES
          reset, packet 0
<SNIP>
    Class-map: D01_FTP
      Inspect: ftp strict D1_FTP, packet 0, lock fail 0, drop 0, reset-drop 0
        mask-banner enabled
        mask-syst-reply enabled
        match request-command rnfr rnto dele
          reset, packet 0
        match filename regex FILE
          reset log, packet 0
```

Task 10: HTTP inspection and content filtering on ASA-3

- Globally enable HTTP inspection and also enable HTTP inspection on port 8888 globally.
- Filter all outbound active-x and java contents on HTTP port 8888 from the VLAN101 to any destination.
- A Websense server is located in dmz1. The IP address of the server is 10.1.1.16. Configure URL (HTTP-80,8888 and HTTPS) filtering from VLAN 101 on port HTTP port 80. Use fail open options if the Websense server is down. Users should not be allowed to use a proxy server.
- 200.100.34.80 is a webserver running on a non-standard port of 8080. Create an HTTP deep packet inspection policy to match all the parameters below and reset the connection. Log all protocol violations. Apply this policy globally. Create an interface specific ACL to allow access to this server from the outside.

Request Header Host should contain “200.100.34.80”
Request URI containing “exec” string
Request Method GET

- 200.100.34.81 is a webserver. Create an HTTP deep packet inspection policy to match any of the parameters below and reset and log the connection. Set the maximum number of simultaneous connections to 3000, half opened embryonic connections to 300, and idle timeout to 30 minutes. Apply this policy globally. Create an interface specific ACL to allow access to this server from the outside.

Content Type Mismatch
Header length greater than 500 bytes
Via count greater than 0
Users should not be able to upload any files to this server
Users should not be able to use Mozilla browsers when accessing this server

- Do not allow any Active-X/ Java applets in the HTTP response from 200.111.111.80. Apply this policy on the outside interface. Use the MPF only.

Task-10:Solutions

Step 1: Configure HTTP inspection on pot 80 and 8888

```
policy-map global_policy
 class inspection_default
 inspect http
```

```
class-map http8888
 match port tcp eq 8888
policy-map global_policy
 class http8888
  inspect http
```

Step 2: Configure Active-X and Java filters for VLAN 101 on ASA3

```
filter activex 8888 192.168.100.0 255.255.255.0 0.0.0.0 0.0.0.0
filter java 8888 192.168.100.0 255.255.255.0 0.0.0.0 0.0.0.0
```

Step 3: URL filtering for VLAN101 using Websense.

```
url-server (dmz1) vendor websense host 10.1.1.16 timeout 30 protocol TCP
version 1 connections 5
filter https 443 192.168.100.0 255.255.255.0 0.0.0.0 0.0.0.0 allow
filter url http 192.168.100.0 255.255.255.0 0.0.0.0 0.0.0.0 allow proxy-block
filter url 8888 192.168.100.0 255.255.255.0 0.0.0.0 0.0.0.0 allow proxy-block
```

Step 4: Configure regex to match 200.100.34.80 and “exec”

```
regex R1_WEB "200\.100\.34\.80"
regex exec "exec"
```

Step 5: Configure Layer 7 Class map to match the required HTTP parameters

```
class-map type inspect http match-all IN_WEB
 match request uri regex exec
 match request method get
 match request header host regex R1_WEB
```

Step 6: Configure Layer 3/4 Class map to match HTTP 8080 traffic to match traffic towards 200.100.34.80 and create appropriate class map

```
access-list IN_WEB extended permit tcp any object IN_WEB eq 8080
class-map R1_WEB
 match access-list IN_WEB
```

Step 7: Configure layer 7 HTTP policy map to specify action

```
policy-map type inspect http IN_WEB
 parameters
  protocol-violation action log
 class IN_WEB
  reset
```

Step 8: Apply HTTP inspection in the global policy using Layer 3 /4 policy map. Make sure you apply the Layer 7 Policy map inside the L3/4 policy map.

```
policy-map global_policy
 class inspection_default
```

```
 class R1_WEB
  inspect http IN_WEB
```

Step 9: Configure ACL's to allow HTTP access to that server

```
access-list out extended permit tcp any object IN_WEB eq 8080
```

Step 10: Create Regex to match Mozilla user agent

```
regex MOZILLA ".* [Mm][Oo][Zz][Ii][Ll][Ll][Aa]*"
```

Step 11: Configure Layer 3/4 Class map and ACL's to match traffic destined to 200.100.34.81

```
access-list D2_WEB extended permit tcp any object D2_WEB eq www
class-map R2_WEB
 match access-list D2_WEB
```

Step 11: Configure Layer 7 Class map with match any option to match various HTTP parameters as specified in the task

```
class-map type inspect http match-any D2_WEB
 match req-resp content-type mismatch
 match request header length gt 500
 match request header via count gt 0
 match request method post
 match request header user-agent regex MOZILLA
```

Step 12: Configure Layer 7 HTTP policy map specify the action

```
policy-map type inspect http D2_WEB
 parameters
 class D2_WEB
  reset log
```

Step 13: Apply HTTP inspection on the Layer 3/4 policy map. Use the default global policy. Make sure you also apply the L7-HTTP policy map in the HTTP inspection and also set the connection limits.

```
policy-map global_policy
 class R2_WEB
  inspect http D2_WEB
  set connection conn-max 3000 embryonic-conn-max 300
  set connection timeout idle 0:30:00
```

Step 14: Configure ACL's to allow access to this server

```
access-list out extended permit tcp any object D2_WEB eq www
```

Step 15: Configure Layer 3/4 Class map and ACL's to match traffic from to 200.111.111.80

```
access-list Web_Server_Filter extended permit tcp host 200.111.111.80 eq www
any

class-map Web_Server_Filter
 match access-list Web_Server_Filter
```

Step 16: Configure Layer 7 Class map with match any option to match various HTTP parameters as specified in the task

```
policy-map type inspect http Web_Server_Filter
 parameters
 match response body active-x
  mask
 match response body java-applet
  mask
```

Step 17: Apply HTTP inspection on the Layer 3/4 policy map on the outside interface. Make sure you also apply the L7-HTTP policy map in the HTTP inspection.

```
policy-map OUT
  class Web_Server_Filter
   inspect http Web_Server_Filter
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config-pmap-c)# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http, packet 0, lock fail 0, drop 0, reset-drop 0
<SNIP>
    Class-map: http8888
      Inspect: http, packet 0, lock fail 0, drop 0, reset-drop 0
    Class-map: R1_WEB
      Inspect: http IN_WEB, packet 0, lock fail 0, drop 0, reset-drop 0
        protocol violations
          log, packet 0
        class IN_WEB
          reset, packet 0

Interface outside:
  Service-policy: OUT
```

```
    Class-map: Web_Server_Filter
      Inspect: http Web_Server_Filter, packet 0, lock fail 0, drop 0, reset-
drop 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
        protocol violations
          packet 0
        match response body active-x
          mask, packet 0
        match response body java-applet
          mask, packet 0
```

Task 11: ESMTP inspection on ASA-3

- 200.100.34.25 is an SMTP server. Drop all emails with a size greater than 9 MB. Also drop any emails which have a recipient count greater than 1000. Only allow internal emails that contain domain names of "@ipexpert.com", "@ipexpert.in" and "@proctorlabs.com". Apply this policy globally in the "inspection_default" class-map.

Task11: Solutions

Step 1: Create Regex and Regex type class map to match internal domains.

```
regex ipexpert1 "@ipexpert.com"
regex ipexpert2 "@ipexpert.in"
regex ipexpert3 "@proctorlabs.com"

class-map type regex match-any INTERNAL_EMAIL
 match regex ipexpert1
 match regex ipexpert2
 match regex ipexpert3
```

Step 2: Create layer 7 ESMTP policy map to specify parameters given in the task

```
policy-map type inspect esmtp D1_SMTP
 parameters
 match header to-fields count gt 1000
  reset
 match body length gt 9000000
  reset
 match not sender-address regex class INTERNAL_EMAIL
  reset
```

Step 3: Apply Layer 7 policy map to the existing ESMPT inspection in the global policy

```
policy-map global_policy
 class inspection_default
  no inspect esmtp
```

```
  inspect esmtp D1_SMTP
```

Step 4: Allow access from the outside to this mail server.

```
access-list out permit tcp any object D1_SMTP eq 25
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show service-policy inspect esmtp

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: esmtp D1_SMTP, packet 0, lock fail 0, drop 0, reset-drop 0
        mask-banner, count 0
        match header to-fields count gt 1000
          reset, packet 0
        match body length gt 9000000
          reset, packet 0
        match not sender-address regex class INTERNAL_EMAIL
          reset, packet 0
<SNIP>
```

Task 12: IM inspection on ASA-3

- Only allow MSN and Yahoo IM chat. Drop all other services in MSN and Yahoo IM. Apply this policy globally. VLAN 101 should be exempted from this policy.

Task-12:Solutions

Step 1: Configure ACL's to match all traffic except from VLAN 101 and create appropriate Layer 3 / 4 class map.

```
access-list vlan101 deny ip 192.168.100.0 255.255.255.0 any
access-list vlan101  permit ip any any
class-map IM
 match access-list vlan101
```

Step 2: Configure Layer 7 IM class & policy map with parameters as per the task

```
class-map type inspect im match-all IMCLASS7
 match protocol msn-im yahoo-im
 match not service chat
```

```
policy-map type inspect im IM
 parameters
 class IMCLASS7
  drop-connection
```

Step 3: Apply the IM inspection in the global policy

```
policy-map global_policy
 class IM
  inspect im IM
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show service-policy inspect im

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: IM
      Inspect: im IM, packet 0, lock fail 0, drop 0, reset-drop 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
        class IMCLASS7
          drop-connection, packet 0
```

Task 13: IP Options inspection on ASA-3

- Configure a global policy to ensure ASA does not conform to RFC 2113.

Task-13:Solutions

Step 1: Configure Layer 7 IP Options policy map with parameters as per the task

```
policy-map type inspect ip-options IPO
 parameters
  router-alert action clear
```

Step 2: Apply the IP options inspection in the global policy

```
policy-map global_policy
 class inspection_default
  no inspect ip-options
  inspect ip-options IPO
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show service-policy inspect ip-options

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ip-options IPO, packet 0, lock fail 0, drop 0, reset-drop 0
        Router Alert:  allow 0, clear 0
<SNIP>
```

Task 14: IPSec passthrough inspection on ASA-3

- Configure a global policy to limit the number of simultaneous ESP tunnels from the same host to 10 tunnels with an idle time of 30 minutes.

Task-14:Solutions

Step 1: Configure IPSec Layer 7 Policy map and specify the parameters as per the task

```
policy-map type inspect ipsec-pass-thru IPSEC
 parameters
  esp per-client-max 10
  esp timeout 00:30:00
```

Step 2: Configure IPSec Pass through policy in the default inspection class under the global policy.

```
 policy-map global_policy
  class inspection_default
  inspect ipsec-pass-thru IPSEC
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show service-policy inspect ipsec-pass-thru
```

```
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ipsec-pass-thru IPSEC, packet 0, lock fail 0, drop 0, reset-
drop 0
```

Task 15: BGP through ASA-3

- Configure the appropriate policy and ACLs to ensure the BGP adjacency between R4 and R1 is established successfully.

Task-15:Solutions

Step 1: Configure TCP map to allow options 19 to pass through.

```
TCP-map BGP
 TCP-options range 19 19 allow
```

Step 2: Create L3/4 class map to match BGP traffic

```
class-map BGP
 match port tcp eq 179
```

Step 3: Disable random sequence number generation for the TCP packets and allow option 19 to pass through in the global policy for the BGP traffic

```
policy-map global_policy
 class BGP
   set connection random-sequence-number disable
   set connection advanced-options BGP
```

Step 4: Optional step. Allow ACL's if R4 initiates the connection first.

```
access-list out extended permit tcp host 4.4.4.4 host 1.1.1.1 eq bgp
```

Verification

Step 1: Verify if the BGP connection is in "UP" on R1

```
R1#sh ip bgp summary
BGP router identifier 11.11.11.11, local AS number 14
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
4.4.4.4         4           14      15      17        1    0    0 00:12:40        0
```

ASA3

```
sh service-policy global
<SNIP>
  Class-map: BGP
      Set connection policy: random-sequence-number disable
        drop 0
      Set connection advanced-options: BGP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

Task 16: TCP normalization on ASA-3

- 200.100.34.1 is a Telnet and SSH server. Configure ASA to either drop, or allow, or normalize TCP packets using the TCP normalizer feature destined to that server from the outside as per the parameters below :

Check-retransmission	Enforce
Checksum-Verification	Enforce
Exceed-mss	drop
Invalid-ack	Drop
Reserve-bits	clear
Synack-data	Allow
Syn-data	Allow (Default)
Tcp-options timestamp	clear

- Set TCP idle timeout to 60 seconds. Enable DCD for connections to this server. Probes should be sent every 5 seconds.
- Maximum number of simultaneous connections per host should be set to 1 and maximum number of simultaneous connection should be set to 2.
- Configure appropriate interface ACLs to allow access to this server. Apply the policy on the outside interface.

Task-16:Solutions

Step 1: Configure to match telnet and SSH traffic towards R1 F0/0 and create appropriate class map.

```
access-list R1_f0 extended permit tcp any object R1_f0 eq ssh
access-list R1_f0 extended permit tcp any object R1_f0 eq telnet

class-map TCP_MAP
 match access-list R1_f0
```

Step 2: Configure TCP map as per the parameter specified in the task

```
tcp-map TCP_MAP
  check-retransmission
  checksum-verification
  exceed-mss drop
  reserved-bits clear
  synack-data allow
  tcp-options timestamp clear
```

Step 3: Apply the TCP map to the SSH and telnet traffic in the OUT policy map along with other connection settings as stated in the task

```
policy-map OUT
 class TCP_MAP
  set connection advanced-options TCP_MAP
  set connection timeout idle 0:01:00 dcd 0:00:05
  set connection conn-max 2 per-client-max 1
```

Step 4: Configure ACL's to allow access.

```
access-list out extended permit tcp any object R1_f0 eq ssh
access-list out extended permit tcp any object R1_f0 eq telnet
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config-pmap-c)# sh service-policy interface outside

Interface outside:
  Service-policy: OUT
    <SNIP>
    Class-map: TCP_MAP
      Set connection policy: conn-max 2 per-client-max 1
        current conns 0, drop 0
      Set connection timeout policy:
        idle 0:01:00
        DCD: enabled, retry-interval 0:00:05, max-retries 5
        DCD: client-probe 0, server-probe 0, conn-expiration 0
      Set connection advanced-options: TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

Task 17: Traceroute through ASA-3

- Configure ACLs such that R5's Loopback0 can traceroute to R1 loopback0. Ensure R1 is able to see the ASA in the traceroute output. Apply this policy globally. Do not create any new class map to accomplish this task.

Step 1: Configure ACL's to allow R5 Loopback0 to traceroute to R1 loopback0.

```
access-list out extended permit udp host 5.5.5.5 host 1.1.1.1 range 33434
33464
```

Step 2: Configure the ASA to decrement TTL for all packets passing through it

```
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

Verification

Step 1: Verify the configuration on ASA

```
ASA003(config)# sh service-policy global

Global policy:
  Service-policy: global_policy
<SNIP>
    Class-map: class-default

      Default Queueing      Set connection policy:         drop 0
      Set connection decrement-ttl
```

Step 2: Trace from R1 Lo0 to R5 Lo0

```
R1#traceroute 5.5.5.5 so lo0

Type escape sequence to abort.
Tracing the route to 5.5.5.5

  1 192.168.103.10 0 msec 0 msec *
  2 200.100.34.4 0 msec 0 msec 4 msec
  3 45.45.45.5 0 msec 0 msec *
```

Task 18: Netflow/NSEL on ASA-3

- Configure the ASA such that all events related to any BGP traffic is sent to a NSEL collector. The Collector is located in the dmz1 interface with an IP address of 10.1.1.100 running on UDP port 10000. Disable all syslog messages that have become redundant due to the NSEL configuration.

Task-18:Solutions

Step 1: Configure Class-Map and ACL's to match BGP traffic

```
access-list BGP extended permit tcp any any eq bgp
access-list BGP extended permit tcp any eq bgp any

class-map BGP_NEWFLOW
 match access-list BGP
```

Step 2: Configure Netflow to export BGP events and disable redundant syslog messages.

```
flow-export destination dmz1 10.1.1.100 10000

policy-map global_policy
 class BGP_NEWFLOW
  flow-export event-type all destination 10.1.1.100

logging flow-export-syslogs disable
```

Verification

Step 1: Verify on ASA to check if events are being exported to the NSEL collector.

```
ASA003(config)# show flow-export counters

destination: dmz1 10.1.1.100 10000
  Statistics:
    packets sent                                                1
  Errors:
    block allocation failure                                    0
    invalid interface                                           0
    template send failure                                       0
    no route to collector                                       0
```

Task 19: LLQ on ASA-3

- Enable LLQ for VoIP traffic marked with a DSCP value of af31 (Signal) and ef (Voice-RTP) on the outside interface. Set the allowed number of packets queued at the tx-ring for the priority-queues to 300 and the depth of the software priority queue to 800 (i.e. number of packets queued at the priority-queues). Apply this policy for the outside interface.

Task-19:Solutions

Step 1: Change the priority queue parameters for the outside interface

```
priority-queue outside
  queue-limit   800
  tx-ring-limit 300
```

Step 2: Configure class map to match VOIP traffic including signal traffic

```
class-map VOIP
 match dscp af31 ef
```

Step 3: Configure priority queue for VOIP traffic in the OUT policy-map.

```
policy-map OUT
 class VOIP
  priority
```

Verification

Step 1: This is a configuration only question

```
ASA003(config)# show service-policy priority

Interface outside:
  Service-policy: OUT
    Class-map: VOIP
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 0

ASA003(config)# show priority-queue config

Priority-Queue Config interface outside
                current         default          range
queue-limit     800             2048             0 - 2048
tx-ring-limit   300             512              3 - 512

ASA003(config)# show priority-queue  statistics

Priority-Queue Statistics interface outside

Queue Type          = BE
Tail Drops          = 0
Reset Drops         = 0
Packets Transmit    = 218
Packets Enqueued    = 0
Current Q Length    = 0
Max Q Length        = 0

Queue Type          = LLQ
Tail Drops          = 0
Reset Drops         = 0
Packets Transmit    = 0
Packets Enqueued    = 0
Current Q Length    = 0
Max Q Length        = 0
```

Task 20: Management Traffic Connection Limits on ASA-3

- Enable ASDM access on the outside interface such that anyone can connect to the ASA.

- Set the simultaneous maximum number of ASDM connections on the outside interface to 2 and maximum embryonic connections to 8. Apply this policy on the outside interface.

Task-20:Solutions

Step 0: Configure ASDM access with local authentication

```
http server enable
http 0.0.0.0 0.0.0.0 outside

asdm image disk0:/asdm-66114.bin
aaa authentication http console LOCAL
username cisco pass cisco
```

Step 1: Configure management type class map to match HTTPS/ASDM sessions

```
class-map type management ASDM
 match port tcp eq https
```

Step 2: Set the connection limits for ASDM sessions in the OUT policy-map

```
policy-map OUT
 class ASDM
  set connection conn-max 2 embryonic-conn-max 8
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show service-policy interface outside
<SNIP>
    Class-map: ASDM
      Set connection policy: conn-max 2 embryonic-conn-max 8
        current embryonic conns 0, current conns 0, drop 0
<SNIP>
```

Task 21: Threat Detection on ASA-3

- Enable advanced threat detection to gather statistics about suspicious activity based on access-list denies and host scanning (8 hours interval).
- Ensure ASA shuns any network scan or sweeps. Make sure ASA does not shun the AD server. Shun duration should be half of the default value.

Task-21:Solutions

Step 1: Configure threat detection as per the task

```
threat-detection basic-threat
threat-detection statistics host number-of-rate 2
threat-detection statistics access-list
threat-detection statistics tcp-intercept
threat-detection   scanning-threat   shun   except   ip-address   10.1.1.101
255.255.255.255
threat-detection scanning-threat shun duration 1800
```

Verification

Step 1: This is a configuration only question.

```
ASA003(config)# show threat-detection statistics
Current monitored hosts:0  Total not monitored hosts:0
                        Average(eps)    Current(eps) Trigger      Total events
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour ACL  hits:
01  icmp/1                          0               0       0               43
02  vlan101/2                       0               0       0               36
03  out/1                           0               0       0               12
04  out/8                           0               0       0                8
  8-hour ACL  hits:
01  icmp/1                          0               0       0               77
02  vlan101/2                       0               0       0               47
03  out/1                           0               0       0               33
04  out/8                           0               0       0                8
 24-hour ACL  hits:
01  icmp/1                          0               0       0               77
02  vlan101/2                       0               0       0               47
03  out/1                           0               0       0               33
04  out/8                           0               0       0                8
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

ASA003(config)# show threat-detection scanning-threat
Latest Target Host & Subnet List:
Latest Attacker Host & Subnet List:

ASA003(config)# show threat-detection rate
                        Average(eps)    Current(eps) Trigger      Total events
  1-hour ACL  drop:                 0               0       0               19
  1-hour SYN attck:                 0               0       0               18
  10-min  Scanning:                 0               0       0                1
  1-hour  Scanning:                 0               0       0               42
  10-min  Firewall:                 0               0       0                1
  1-hour  Firewall:                 0               0       0               24
  10-min DoS attck:                 0               0       0                1
```

```
  1-hour DoS attck:                0              0         0                5
  10-min Interface:                0              0         0               12
  1-hour Interface:                0              0         0               51
```

NOTES

You may refer the documentation for more information on MPF and application inspection.

Lab 6: Transparent Firewall

Lab 6: Transparent Firewall– This lab is intended to let you be familiar with the transparent firewall feature on the ASA. This lab consists of two ASAs. One of the ASA is loaded with 8.6 code and other is loaded with 8.2 version. There are several changes in configuring the transparent firewall between different software versions.

General Rules

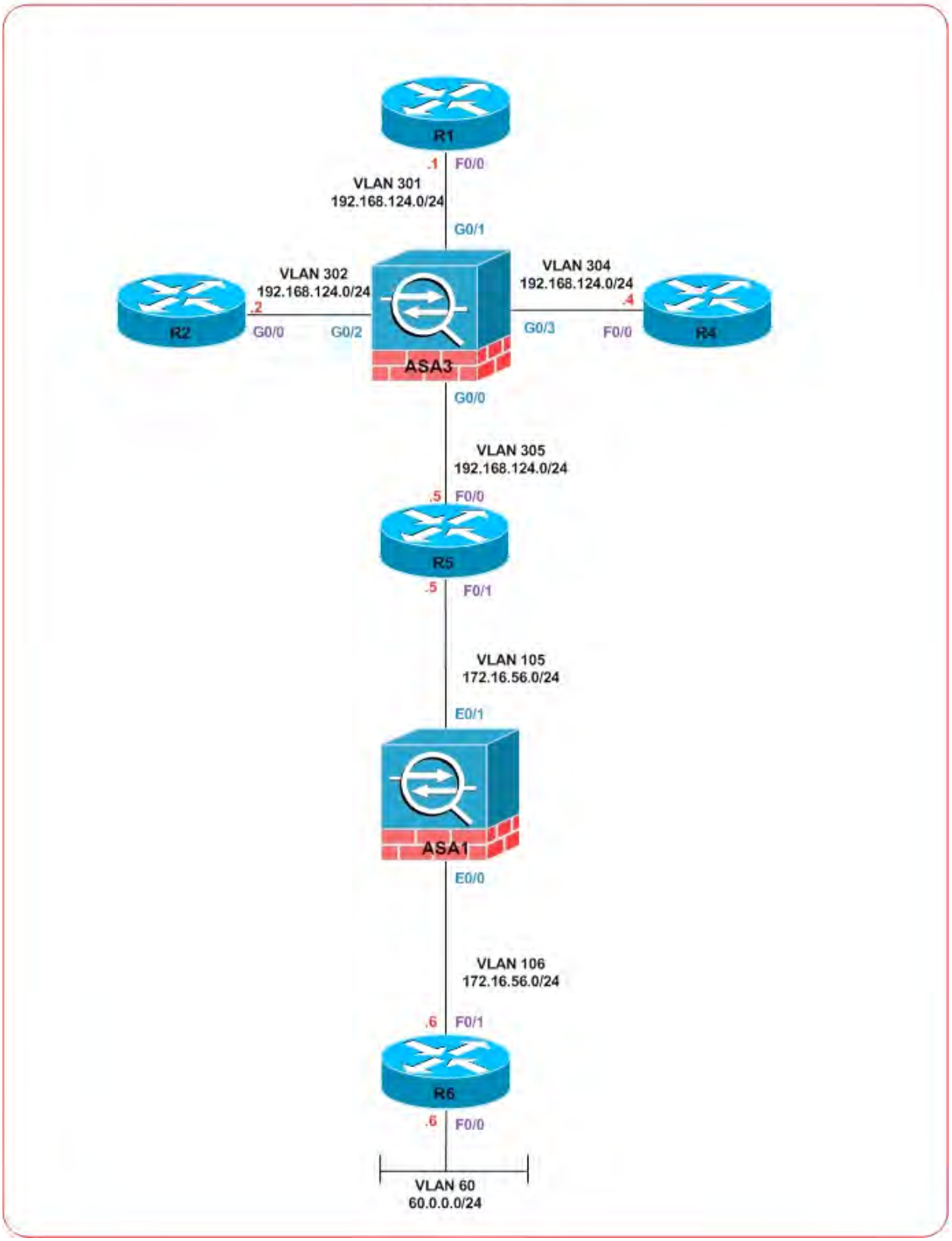
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 3 Hours

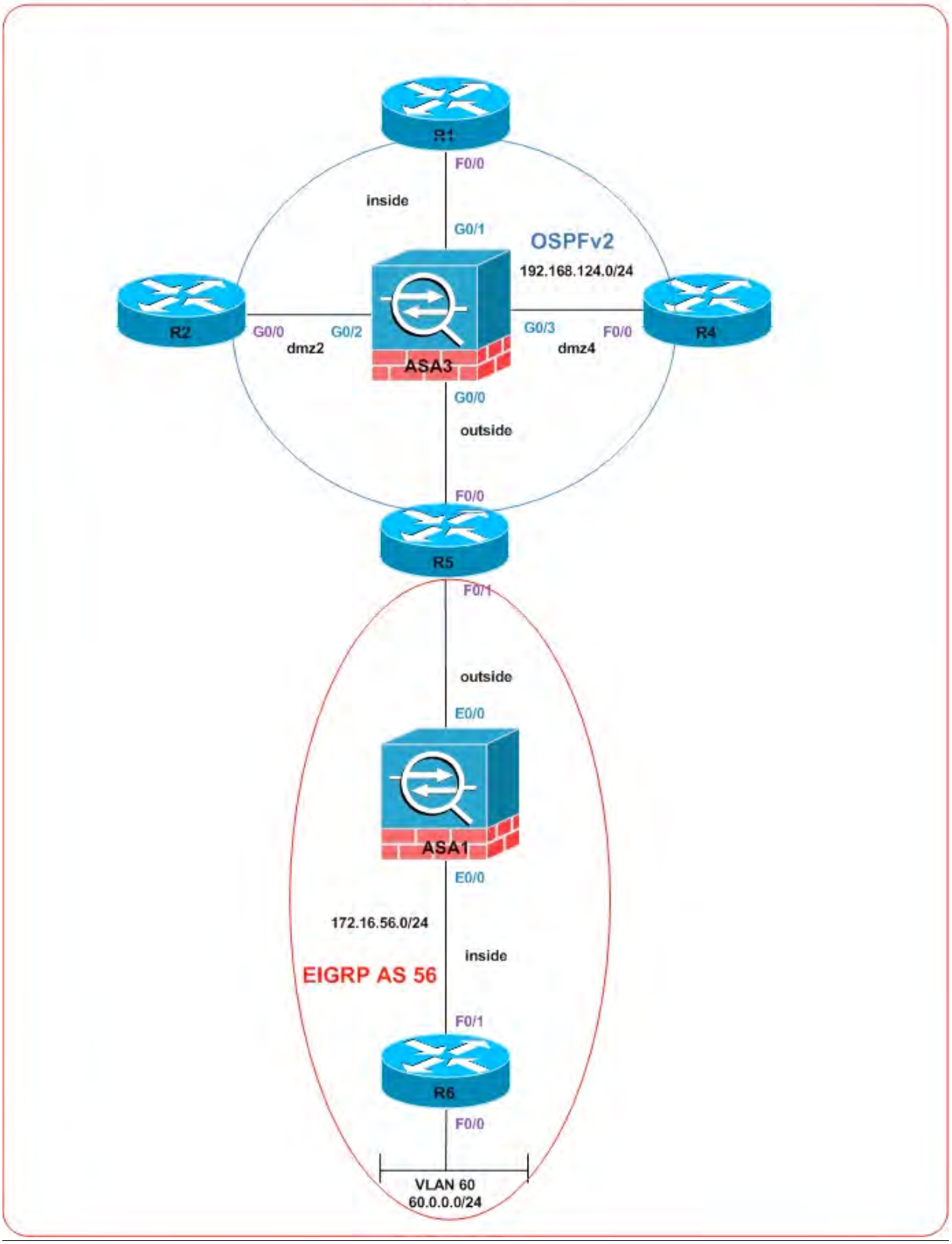
Pre-setup

Load the initial configuration for Lab 6. Routers are pre-configured. Use the logical topology drawing - Network Topology 1.4 and 1.5 to understand the logical topology and routing when transparent firewall is introduced. Double-check the loaded pre-configuration before starting the Lab. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.4
(Logical)



Network Topology 1.5
(Logical)



Detailed Solution:Lab-1

Task 1: Basic Initialization ASA-3

- Change the mode to Transparent. Configure a hostname of “FwtASA3” on ASA-3.
- FwtASA3 should have a domain name of ipexpert.com.
- Configure the FwtASA3 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	Bridge Group	VLAN	Security Level	Name
G0/0	100	305	0	outside
G0/1	100	301	100	inside
G0/2	100	302	50	dmz2
G0/3	100	304	60	dmz4
M0/0	None	444	100	mgt

- Configure a BVI address of 192.168.124.100 and management IP of 192.168.1.100.

Task-1:Solutions

Step 1: Double-check switchport configuration :

SW3

```
interface GigabitEthernet1/0/19
 switchport access vlan 305
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/20
 switchport access vlan 301
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/21
 switchport access vlan 302
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/22
 switchport access vlan 304
 switchport mode access
 spanning-tree portfast
```

Step 2: Change the mode to transparent and initialize the ASA as per parameters in the task

ASA3

```
firewall transparent

hostname FwtASA3
domain-name ipexpert.com

interface BVI100
 ip address 192.168.124.100 255.255.255.0

interface GigabitEthernet0/0
 nameif outside
 bridge-group 100
 security-level 0
 no sh

interface GigabitEthernet0/1
 nameif inside
 bridge-group 100
 security-level 100
 no sh

interface GigabitEthernet0/2
 nameif dmz2
 bridge-group 100
 security-level 50
 no sh

interface GigabitEthernet0/3
 nameif dmz4
 bridge-group 100
 security-level 60
 no sh

interface Management0/0
 nameif mgt
 security-level 100
 ip address 192.168.1.100 255.255.255.0
 management-only
 no sh
```

Verification

Step 1: Verify the interface configs

```
FwtASA3(config)# show nameif
Interface                Name                        Security
```

```
GigabitEthernet0/0       outside                 0
GigabitEthernet0/1       inside                100
GigabitEthernet0/2       dmz2                   50
GigabitEthernet0/3       dmz4                   60
Management0/0            mgt                   100
```

```
FwtASA3(config)# show interface ip brief
Interface                              IP-Address          OK?  Method  Status
Protocol
GigabitEthernet0/0                        192.168.124.100   YES   unset     up
up
GigabitEthernet0/1                        192.168.124.100   YES   unset     up
up
GigabitEthernet0/2                        192.168.124.100   YES   unset     up
up
GigabitEthernet0/3                        192.168.124.100   YES   unset     up
up
GigabitEthernet0/4          unassigned       YES unset   administratively down
down
GigabitEthernet0/5          unassigned       YES unset   administratively down
down
Internal-Control0/0                  127.0.1.1               YES  unset    up
up
Internal-Data0/0                        unassigned            YES  unset    up
up
Internal-Data0/1                        unassigned            YES  unset    up
up
Internal-Data0/2                        unassigned            YES  unset    up
up
Management0/0                              192.168.1.100      YES  unset    up
up
BVI100                                        192.168.124.100  YES  unset    up
up
```

Step 2: Verify the bridge group

```
FwtASA3(config)# show bridge-group
Static mac-address entries:  0 (in use), 65535 (max)
Dynamic mac-address entries: 8 (in use), 65535 (max)

 Bridge Group: 100
 Interfaces:
 GigabitEthernet0/0
 GigabitEthernet0/1
 GigabitEthernet0/2
 GigabitEthernet0/3
```

```
 Management System IP Address:  192.168.124.100 255.255.255.0
 Management Current IP Address: 192.168.124.100 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 8
```

Task 2: ACLs on ASA-3

- The 192.168.124.0/24 subnet has been configured for OSPF. Configure Global ACLs to permit any OSPF traffic from R1, R2, R4, R5.
- Allow all SSH, Telnet, GRE, SMTP, FTP, TFTP, IPSEC, HTTP, DNS, HTTPS, ICMP, ISAKMP (UDP - Src 500 and Dst 500) traffic from 192.168.124.0/24 subnet. Use a single ACL to accomplish this task.
- Allow HTTP, HTTPS, Telnet, SSH, and ICMP access from VLAN 60 to the 192.168.124.0/24 subnet. Apply this ACL on the outside interface.
- Globally inspect ICMP traffic.

Task-2:Solutions

Step 1: Configure objects-groups for ACL related to permitting OSPF traffic

```
object-group network OSPF
 network-object host 192.168.124.1
 network-object host 192.168.124.2
 network-object host 192.168.124.4
 network-object host 192.168.124.5
```

Step 2: Configure global ACL's to allow any OSPF traffic sourced from R1, R2, R4 and R5 and apply the ACL.

```
access-list GLOBAL extended permit ospf object-group OSPF any
access-group GLOBAL global
```

Step 3: Configure enhanced service objects-group and network object for ACL various services stated in the task for 192.168.124.0/24 network

```
object network 192
 subnet 192.168.124.0 255.255.255.0

object-group service S1
 service-object esp
 service-object gre
 service-object icmp
 service-object tcp eq ftp
```

```
 service-object tcp eq http
 service-object tcp eq https
 service-object tcp eq ssh
 service-object tcp eq telnet
 service-object tcp eq smtp
 service-object udp eq domain
 service-object udp eq tftp
 service-object udp eq isakmp
 service-object udp source eq isakmp
```

Step 4: Configure global ACL's to allow traffic from 192.168.124.0/24 network using enhanced service object group in the ACL.

```
access-list GLOBAL extended permit object-group S1 object 192 any
```

Step 5: Configure interface ACL's for inbound traffic on the outside interface.

```
access-list OUT extended permit tcp 60.0.0.0 255.255.255.0 object 192 eq www
access-list OUT extended permit tcp 60.0.0.0 255.255.255.0 object 192 eq
https
access-list OUT extended permit tcp 60.0.0.0 255.255.255.0 object 192 eq ssh
access-list OUT extended permit tcp 60.0.0.0 255.255.255.0 object 192 eq
telnet
access-list OUT extended permit icmp 60.0.0.0 255.255.255.0 object 192
access-group OUT in interface outside
```

Step 6: Configure ASA3 to inspect ICMP globally

```
policy-map global_policy
 class inspection_default
  inspect icmp
```

Verification

Step 1: Verify if OSPF adjacency and routes is established on the routers. Verify from R4

```
R4#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DROTHER    00:00:38    192.168.124.1   FastEthernet0/0
2.2.2.2           1   FULL/DROTHER    00:00:30    192.168.124.2   FastEthernet0/0
5.5.5.5           1   FULL/DR         00:00:35    192.168.124.5   FastEthernet0/0

R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.124.5 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 192.168.124.1, 00:09:23, FastEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 192.168.124.2, 00:09:23, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Loopback0
     55.0.0.0/32 is subnetted, 1 subnets
O       55.55.55.55 [110/2] via 192.168.124.5, 00:09:23, FastEthernet0/0
     5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       5.5.5.5/32 [110/2] via 192.168.124.5, 00:09:25, FastEthernet0/0
O E2    5.0.0.0/8 [110/20] via 192.168.124.5, 00:09:25, FastEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2    172.16.56.0/24 [110/20] via 192.168.124.5, 00:09:25, FastEthernet0/0
O E2    172.16.0.0/16 [110/20] via 192.168.124.5, 00:09:26, FastEthernet0/0
     22.0.0.0/32 is subnetted, 1 subnets
O       22.22.22.22 [110/2] via 192.168.124.2, 00:09:26, FastEthernet0/0
C    192.168.124.0/24 is directly connected, FastEthernet0/0
     11.0.0.0/32 is subnetted, 1 subnets
O       11.11.11.11 [110/2] via 192.168.124.1, 00:09:26, FastEthernet0/0
     44.0.0.0/32 is subnetted, 1 subnets
C       44.44.44.44 is directly connected, Loopback1
O*E2 0.0.0.0/0 [110/1] via 192.168.124.5, 00:09:26, FastEthernet0/0
```

Step 2: Perform basic ping test from R5

```
R5#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 3: Basic Initialization the ASA-1

- Configure a hostname of “FwtASA1” on ASA-1.
- Telnet password should be set to “ipexpert”.
- FwtASA1 should have a domain name of ipexpert.com.
- Configure the FwtASA1 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	VLAN	Security Level	Name
E0/0	106	100	inside
E0/1	105	0	outside

- Configure a Global IP address of 172.16.56.100.

Task-2:Solutions

Step 1: Check L2 configuration :

SW3

```
interface GigabitEthernet1/0/6
 switchport access vlan 106
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/7
 switchport access vlan 105
 switchport mode access
 spanning-tree portfast
```

Step 2: Change the mode to transparent and initialize the ASA as per parameters in the task

ASA1

```
firewall transparent

hostname FwtASA1
domain-name ipexpert.com
passwd ipexpert

interface Ethernet0/0
 nameif inside
```

```
 security-level 100
 no shutdown

interface Ethernet0/1
 nameif outside
 security-level 0
 no shutdown

ip address 172.16.56.100 255.255.255.0
```

Verification

Step 1: Verify the interface configs

```
FwtASA1(config)# show nameif
Interface                 Name                      Security
Ethernet0/0               inside                    100
Ethernet0/1               outside                     0

FwtASA1(config)# sh interface ip brief
Interface                                IP-Address          OK?  Method  Status
Protocol
Ethernet0/0                                 172.16.56.100      YES  unset    up
up
Ethernet0/1                                 172.16.56.100      YES  unset    up
up
Ethernet0/2                  unassigned       YES unset  administratively down
up
Ethernet0/3                  unassigned       YES unset  administratively down
up
Management0/0                unassigned       YES unset  administratively down
up




FwtASA1(config)# sh ip address
Management System IP Address:
        ip address 172.16.56.100 255.255.255.0
Management Current IP Address:
        ip address 172.16.56.100 255.255.255.0
```

Task 4: ACLs on ASA-1

- Configure ACLs to allow EIGRP traffic between R6 and R5.
- Allow all inbound SSH, Telnet, GRE, SMTP, FTP, TFTP, IPSEC, HTTP, DNS, HTTPS, ICMP, ISAKMP (UDP - Src 500 and Dst 500) traffic from 192.168.124.0/24 to the VLAN60 subnet. Use a single ACL to accomplish this task.

- Allow all outbound ICMP, Telnet, SSH, HTTP and HTTPS traffic from VLAN60 to 192.168.124.0/24.

Task-4:Solutions

Step 1: Configure ACL's to allow EIGRP traffic through ASA1 between R5 and R6

```
access-list IN extended permit eigrp host 172.16.56.6 host 172.16.56.5
access-list IN extended permit eigrp host 172.16.56.6 host 224.0.0.10
access-list OUT extended permit eigrp host 172.16.56.5 host 172.16.56.6
access-list OUT extended permit eigrp host 172.16.56.5 host 224.0.0.10

access-group IN in interface inside
access-group OUT in interface outside
```

Step 2: Configure enhanced service object groups needed for the inbound ACL

```
object-group service S1
 service-object esp
 service-object gre
 service-object icmp
 service-object udp source eq isakmp
 service-object tcp eq ftp
 service-object tcp eq ssh
 service-object tcp eq telnet
 service-object tcp eq smtp
 service-object tcp eq www
 service-object tcp eq https
 service-object udp eq tftp
 service-object udp eq isakmp
 service-object udp eq domain
```

Step 3: Configure inbound ACL's

```
access-list OUT extended permit object-group S1 192.168.124.0 255.255.255.0
60.0.0.0 255.255.255.0
```

Step 4: Configure outbound ACL's for VLAN 60 to 192.168.124.0/24

```
access-list IN extended permit icmp 60.0.0.0 255.255.255.0 192.168.124.0
255.255.255.0
access-list IN extended permit tcp 60.0.0.0 255.255.255.0 192.168.124.0
255.255.255.0 eq ssh
access-list IN extended permit tcp 60.0.0.0 255.255.255.0 192.168.124.0
255.255.255.0 eq telnet
access-list IN extended permit tcp 60.0.0.0 255.255.255.0 192.168.124.0
255.255.255.0 eq www
```

```
access-list IN extended permit tcp 60.0.0.0 255.255.255.0 192.168.124.0
255.255.255.0 eq https
```

Verification - Check the mode of the firewall using " show firewall" command on the ASA to check if the ASA is in routed or transparent mode.

Step 1: Verify if EIGRP neighbourship has been established between R5 and R6 and verify routes. Verify from R5.

```
R5#sh ip eigrp neighbors
IP-EIGRP neighbors for process 56
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   172.16.56.6             Fa0/1             10 01:02:11   10   200  0  3


R5#sh ip route eigrp

     60.0.0.0/24 is subnetted, 1 subnets

D       60.0.0.0 [90/30720] via 172.16.56.6, 00:01:18, FastEthernet0/1
```

Step 2: Test the inbound ACL's. Ping and telnet from R1 to VLAN 60 (R6 F0/0)

```
R1#ping 60.0.0.6 so f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.0.6, timeout is 2 seconds:
Packet sent with a source address of 192.168.124.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms


R1#telnet 60.0.0.6
Trying 60.0.0.6 ... Open

R6#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:53
*514 vty 0                 idle                 00:00:00 192.168.124.1
```

Step 3: Test the Outbound ACL's. Ping from R6 VLAN 60 (R6 F0/0) to R1, R2 and R4.

```
R6#ping 192.168.124.1 so f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.124.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 60.0.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R6#ping 192.168.124.2 so f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.124.2, timeout is 2 seconds:
Packet sent with a source address of 60.0.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R6#ping 192.168.124.4 so f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.124.4, timeout is 2 seconds:
Packet sent with a source address of 60.0.0.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
R6#telnet 192.168.124.4 /source-interface f0/0
Trying 192.168.124.4 ... Open

R4#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:04:56
*514 vty 0                 idle                 00:00:00 60.0.0.6
```

Task 5: Transparent Firewall NAT/PAT on ASA-1

- Configure static NAT for R6 Lo16 (16.16.16.16). It should be translated to 60.0.0.16.
- Configure PAT for R6 Lo0 (6.6.6.6) to 160.0.0.6.
- Configure appropriate static routes on ASA and R5.
- Configure appropriate ACLs to allow R6 Lo0 to Telnet to R1 Lo0
- Ensure 192.168.124.0/24 can ping 60.0.0.16. Use an ACL to accomplish this task. Do not use MPF to accomplish this task.

Task-5:Solutions

Step 1: Configure Static NAT and PAT on ASA1 with appruprate routes

```
ASA1

static (inside,outside) 60.0.0.16 16.16.16.16 netmask 255.255.255.255

nat (inside) 1 6.6.6.6 255.255.255.255
global (outside) 1 160.0.0.6
```

```
route inside 6.6.6.6 255.255.255.255 172.16.56.6 1
route inside 16.16.16.16 255.255.255.255 172.16.56.6 1
```

Step 2: Configure static route for 160.0.0.6 on R5

```
R5
ip route 160.0.0.6 255.255.255.255 172.16.56.6
```

Step 3: Configure ACL such that R6 Lo0 can telnet to R1 Lo0 on ASAs 1 &3

ASA1

```
access-list IN extended permit tcp host 6.6.6.6 host 1.1.1.1 eq telnet
```

ASA3

```
access-list OUT permit tcp host  160.0.0.6 host 1.1.1.1 eq 23
```

Step 4: Configure ACL on ASA1 such that 192.168.124.0/24 can ping 60.0.0.16

```
access-list OUT extended permit icmp host 192.168.124.0 255.255.255.0 host
60.0.0.16 echo
access-list IN extended permit icmp host 16.16.16.16 192.168.124.0
255.255.255.0 echo-reply
```

Verification

Step 1: Verify NAT table on ASA1

```
FwtASA1(config)# show nat

NAT policies on Interface inside:
  match ip inside host 16.16.16.16 outside any
    static translation to 60.0.0.16
    translate_hits = 2, untranslate_hits = 2
  match ip inside host 6.6.6.6 inside any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside host 6.6.6.6 outside any
    dynamic translation to pool 1 (160.0.0.6)
    translate_hits = 6, untranslate_hits = 0
```

Step 2: Telnet to R1 Lo0 from R6 Lo0

```
R6#telnet 1.1.1.1 /source-interface lo0
Trying 1.1.1.1 ... Open

R1#show users
```

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:02:35
*514 vty 0                 idle                 00:00:00 160.0.0.6
```

Step 3: Ping from R1 to 60.0.0.16

```
R1#ping 60.0.0.16 so f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.0.16, timeout is 2 seconds:
Packet sent with a source address of 192.168.124.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 6: Ethertype ACLs on ASA-1

- Configure Ethertype ACLs to allow TRILL (TRILL TE) and MPLS unicast and MPLS multicast
- frames to pass through ASA-1.

Task-6:Solutions

Step 1: Configure ethertype ACL's and apply on both inside and outside interface

```
access-list ETHER ethertype permit 22f3
access-list ETHER ethertype permit mpls-unicast
access-list ETHER ethertype permit mpls-multicast

access-group ETHER in interface outside
access-group ETHER in interface inside
```

Verification

Step 1: This is a configuration only question.

```
FwtASA1(config)# show access-list
<SNIP>
access-list ETHER; 3 elements
access-list ETHER ethertype permit 22f3 (hitcount=0)
access-list ETHER ethertype permit mpls-unicast (hitcount=0)
access-list ETHER ethertype permit mpls-multicast (hitcount=0)
```

Task 7: Dynamic ARP inspection on ASA-1

- Configure DAI on ASA-1 such that no ARP traffic passes through the firewall without

checking the static MAC to IP binding table. If none of the ARP packets match an entry then the ASA should drop that packet. Create the appropriate MAC to IP bindings.

Task-7:Solutions

Step 1: Configure ARP inspection with no-flood option. Also create static ARP entrie for R5 and R6 F0/1 interface's on ASA1

```
arp outside 172.16.56.5 001b.d515.a0b9 //(check the MAC of R5 F0/1)
arp inside 172.16.56.6 001b.d515.a1f1  //(check the MAC of R6 F0/1)

arp-inspection outside enable no-flood
arp-inspection inside enable no-flood
```

Verification

Step 1: Shutdown R6 F0/1 interface and make sure there is no ARP entry. Unshut the interface and make sure EIGRP neigbour with R5 comes up

```
R6(config)#int f0/1
R6(config-if)#shut

R6(config-if)#do sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  60.0.0.6               -   001b.d515.a1f0  ARPA   FastEthernet0/0

R6(config)#int f0/1
R6(config-if)#no shut

*Apr  1 17:16:49.158: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 56: Neighbor 172.16.56.5
(FastEthernet0/1) is up: new adjacency
R6#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  60.0.0.6               -   001b.d515.a1f0  ARPA   FastEthernet0/0
Internet  172.16.56.5            0   001b.d515.a0b9  ARPA   FastEthernet0/1
Internet  172.16.56.6            -   001b.d515.a1f1  ARPA   FastEthernet0/1
```

Step 2: Check the ARP statistics on ASA1

```
FwtASA1(config)# sh arp statistics
        Number of ARP entries in ASA: 2

        Dropped blocks in ARP: 40
        Maximum Queued blocks: 21
```

```
        Queued blocks: 0
        Interface collision ARPs Received: 0
        ARP-defense Gratuitous ARPS sent: 0
        Total ARP retries: 17
        Unresolved hosts: 0
        Maximum Unresolved hosts: 3
```

Task 8: Prevent MAC Spoof attacks on ASA-1

- Disable MAC learning on the outside and inside interfaces and create static bindings for R5 and R6.

Task-8:Solutions

Step 1: Disable MAC learning on both the interfaces and create static MAC binding for R5 and R6 F0/1 interface

```
mac-learn inside disable
mac-learn outside disable

mac-address-table static outside 001b.d515.a0b9
mac-address-table static inside 001b.d515.a1f1
```

Verification

Step 1: Verify if the MAC address is changed to static entry type on ASA1. NOTE: MAC address will be different for each rack. Please log into R5 and R6 and find out the BIA MAC-Address.

```
FwtASA1(config)# sh mac-address-table
interface                   mac  address          type       Age(min)
------------------------------------------------------------------
inside                     001b.d515.a1f1          static
outside                    001b.d515.a0b9          static
```

NOTES

Bridge Group feature provides a mechanism to group upto 4 interfaces (pyhsical or logical interfaces) under a logical group and manage multiple such groups through a single context.

Each Bridge Group will have an ip address associated with it, this is a mandatory configuration to pass traffic through the ASA. An interface named BVI (Bridge Virtual Interface) needs to be created corresponding to each Bridge Group. The primary purpose of this interface is to allocate IP to the Bridge Group. The global ip which was supported in transparent firewall till

8.3 version is no longer supported. However the IP on the BVI interface is similar in functionality to the global IP, albeit it pertains to the corresponding Bridge Group only.

Bridge Group – Bridge Group is an interface submode command. To put an interface into or to remove it from a bridge group, the user can use the following command:

[no] bridge-group <id>

Each bridge groups is associated with a bridge-group id, which is nothing but an identifier for the bridge group.

Valid range for the id being <1-100>, which must be unique within the context.

BVI Interface - BVI stands for Bridge Virtual Interface. Each bridge group is associated with a BVI interface. To create or delete the BVI interface the user can give the following command from the config mode :

[no] interface BVI <id>

Here id is same as the Bridge Group id of the corresponding Bridge Group.

Need for a BVI interface : For a bridge group to allow through the box traffic an ip configuration is mandatory. This ip is configured on the BVI interface corresponding to the bridge-group.

BVI interface can be created in the single, user or admin context. It can't be configured on in the system context.It can be seen using the show interface, show run interface within the context. It won't be visible in the system context.

Use the below command to configure BVI IP address under the interface BVI <ID>

[no] ip address <ip_address> [<mask>] [standby <sby_ip_addr>]

1. The BVI IP should belong to the same subnet as that of it's member interfaces.

2. The BVI IP of different bridge group should not belong to overlapping subnets, i.e. they should belong to unique subnets.

Bridge Groups are isolated from each other. That means that traffic can't flow from one bridge group to other.For example if a host from one vlan belonging to Bridge Group 1 tries to send traffic to another host belonging to another vlan which is a part of Bridge Group 2, they won't be able to do so. To enable the same you will have to get routed through an external router/Layer 3 device.

Interfaces can’t be shared across the bridge groups.

Mandatory Configuration - To allow traffic to pass on an interface it has to be associated with a bridge group. If an interface is not associated with any bridge group, there won't be any mac-learning on that interface and the packets from that interface are going to be dropped. Thus bridge group is going to be a mandatory configuration.

Change in Global IP Handling in TFW mode - In TFW mode, per context global ip assignment is no more supported, instead the ip configuration will be limited only to the BVI interface and management only interface.

While displaying the ip using the "show ip" command, this ip should be displayed as the management ip of the bridge group.

In transparent firewall one management only interface can be configured per context. A management ip can be configured for this interface, which can be used for to/from the box traffic.

Lab 7: Active/Standby Transparent Firewall

Lab 7: Active/Standby Transparent Firewall – This lab is intended to let you be familiar with the transparent firewall feature on ASA on 8.6 using multiple bridge groups in single context mode with stateful failover.

General Rules

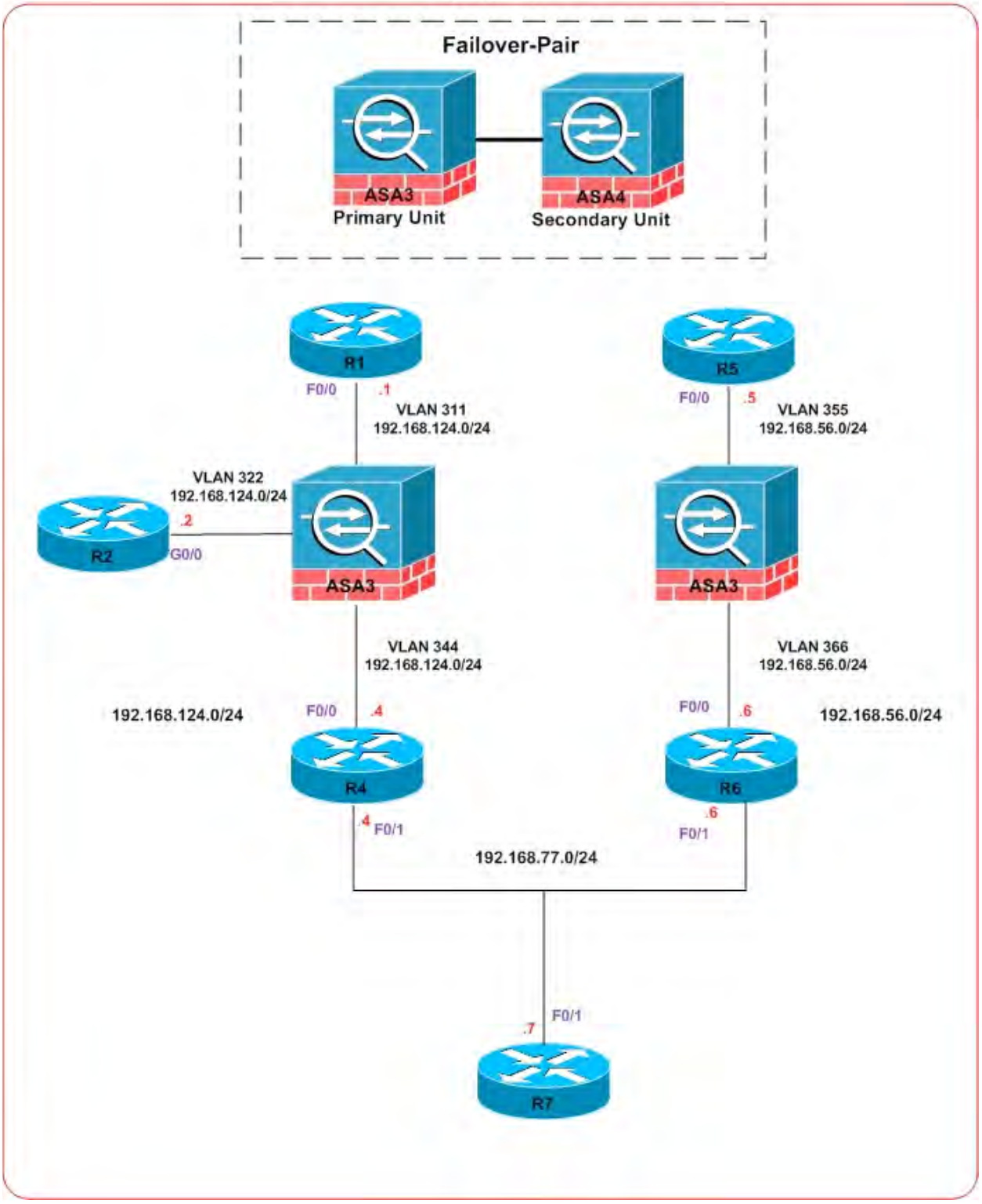
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular chapter.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 2.5 Hours

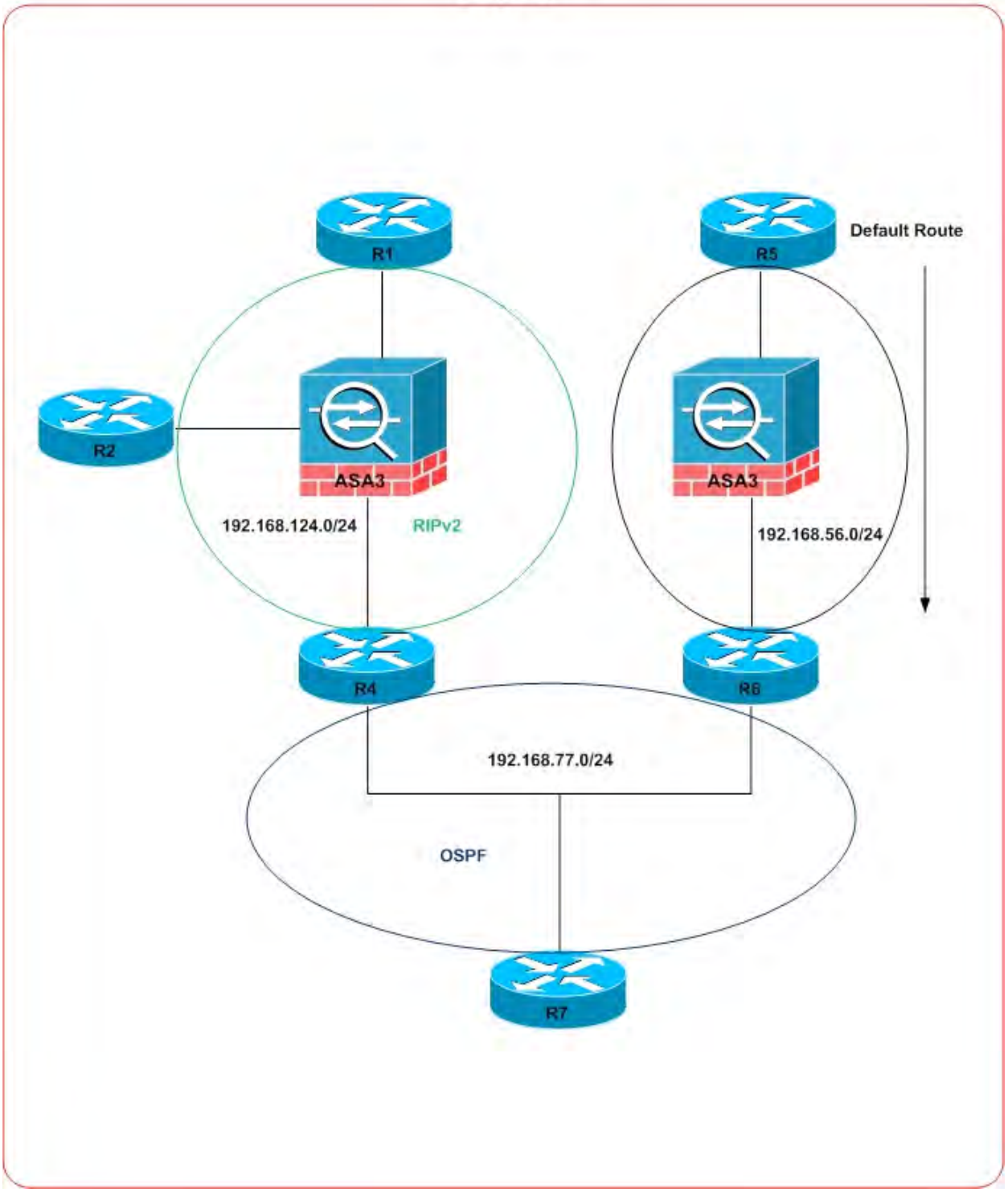
Pre-setup

Load the initial configuration for Lab 7. Routers are pre-configured. Use the logical topology drawing (Network Topology 1.6 and 1.7) to understand the logical topology and routing when Transparent firewall is introduced. Double-check the loaded pre-configuration before starting the Lab. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.6
(Logical)



Network Topology 1.7
(Logical)



Task 1: Basic VLAN Setup

- Configure the Catalyst switch with the appropriate VLANs for ports and trunks for the firewall as per topology diagram 1.6.

(Please read the entire Lab-7 before performing this task)

Detailed Solution:Lab-1

Task-1:Solutions

Step 1: Configure SW3 and SW4 with the appropriate VLAN/Trunks.

```
interface GigabitEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 311,322,344
 switchport mode trunk

interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 355,366
 switchport mode trunk
```

Verification

Step 1: Check the trunk status on SW3 and SW4. You will require to unshut G0/0, G0/1 interfaces of the ASA's for this verification.

```
show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/15    auto             n-802.1q       trunking      1
Gi1/0/16    auto             n-802.1q       trunking      1
Gi1/0/17    auto             n-802.1q       trunking      1
Gi1/0/18    auto             n-802.1q       trunking      1
Gi1/0/19    on               802.1q         trunking      1
Gi1/0/20    on               802.1q         trunking      1
Gi1/0/23    auto             802.1q         trunking      1
Gi1/0/24    auto             802.1q         trunking      1



Port        Vlans allowed on trunk
Gi1/0/15    1-4094
Gi1/0/16    1-4094
Gi1/0/17    1-4094
Gi1/0/18    1-4094
Gi1/0/19    311,322,344
```

```
Gi1/0/20     355,366
Gi1/0/23     1-4094
Gi1/0/24     1-4094

Port         Vlans allowed and active in management domain
Gi1/0/15     1,77,200,311,322,333,344,355,366
Gi1/0/16     1,77,200,311,322,333,344,355,366
Gi1/0/17     1,77,200,311,322,333,344,355,366
Gi1/0/18     1,77,200,311,322,333,344,355,366
Gi1/0/19     311,322,344
Gi1/0/20     355,366
Gi1/0/23     1,77,200,311,322,333,344,355,366
Gi1/0/24     1,77,200,311,322,333,344,355,366

Port         Vlans in spanning tree forwarding state and not pruned
Gi1/0/15     none
Gi1/0/16     none
Gi1/0/17     1,77,200,311,322,333,344,355,366
Gi1/0/18     none
Gi1/0/19     311,322,344
Gi1/0/20     355,366
Gi1/0/23     none
Gi1/0/24     none
```

Task 2: Failover Configuration

- Change the firewall mode to transparent.
- Configure ASA-3 and ASA-4 for device level HA using the failover feature on the ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the parameters below for the failover configuration. Configure the switch such that the Gi0/2 interface of the firewall (failover port) should be in VLAN 300. Share the Gi0/2 interface for stateful link failover.

Failover interface – Gi0/2
Primary IP – 30.1.1.1/24
Standby IP – 30.1.1.2/24
Interface Name - FA1LOVER
Key - C1SCO

Task-2:Solutions

Step 1: Create VLAN 300 and assign G1/0/21 on SW3 and SW4 to that VLAN.

SW4 (VTP Server)

```
vlan 300
```

SW3, SW4

```
default int g1/0/21

interface GigabitEthernet1/0/21
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast
```

Step 2: Configure stateful failover on SW3 and SW4. The primary unit is SW3.

ASA3

```
firewall transparent

interface gigabitEthernet 0/2
 no shutdown

failover lan unit primary
failover lan interface FA1LOVER GigabitEthernet0/2
failover key C1SCO
failover link FA1LOVER GigabitEthernet0/2
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
failover
```

ASA4

```
firewall transparent

interface gigabitEthernet 0/2
 no shutdown

failover lan unit secondary
failover lan interface FA1LOVER GigabitEthernet0/2
failover key C1SCO
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
failover
```

Verification

Step 1: Verify the failover configuration

ASA3

```
ciscoasa(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FA1LOVER GigabitEthernet0/2 (up)
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 05:01:08 UTC Feb 28 2013
        This host: Primary - Active
                Active time: 20321 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up
        Other host: Secondary - Standby Ready
                Active time: 40 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         2969       0          2682       0
        sys cmd         2682       0          2682       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        155        0          0          0
        UDP conn        51         0          0          0
        ARP tbl         59         0          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   19         0          0          0
        User-Identity   3          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       6       22743
        Xmit Q:         0       30      26561
```

ASA4

```
ciscoasa(config)# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: FA1LOVER GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 114 maximum
```

```
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 02:34:58 UTC Apr 1 2013
        This host: Secondary - Standby Ready
                Active time: 40 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up
        Other host: Primary - Active
                Active time: 20591 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         2718       0          2986       0
        sys cmd         2718       0          2718       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          153        0
        UDP conn        0          0          51         0
        ARP tbl         0          0          51         0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          10         0
        User-Identity   0          0          3          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       9       46949
        Xmit Q:         0       1       2718
```

Task 3: Basic Initialization ASA-3

- Configure a hostname of "ASA3TFW" on ASA-3.
- ASA3 should have a domain name of ipexpert.com.
- Configure the ASA3 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	Bridge Group	VLAN	Security Level	Name
G0/0.311	10	311	100	inside
G0/0.322	10	322	50	dmz
G0/0.344	10	344	0	outside
G0/1.355	20	355	100	in
G0/1.366	20	366	0	out

- Configure a BVI 10 address of 192.168.124.100 and a standby IP of 192.168.124.101.
- Configure a BVI 20 address of 192.168.56.100 and a standby IP of 192.168.56.101.
- Ensure all interfaces are monitored.

Task-3:Solutions

Step 1: Configure basic initialization on the primary unit/Active i.e. ASA3

```
hostname ASA3TFW
domain-name ipexpert.com
```

Step 2: Create subinterfaces and bridge group. Assign the subinterfaces to appropriate bridge group and configure interface related parameters.

```
interface BVI10
 ip address 192.168.124.100 255.255.255.0 standby 192.168.124.101

interface BVI20
 ip address 192.168.56.100 255.255.255.0 standby 192.168.56.101

interface GigabitEthernet0/0
 no nameif
 no security-level
 no shutdown

interface GigabitEthernet0/1
 no nameif
 no security-level
 no shutdown
```

```
interface GigabitEthernet0/0.311
 vlan 311
 nameif inside
 bridge-group 10
 security-level 100

interface GigabitEthernet0/0.322
 vlan 322
 nameif dmz
 bridge-group 10
 security-level 50

interface GigabitEthernet0/0.344
 vlan 344
 nameif outside
 bridge-group 10
 security-level 0

interface GigabitEthernet0/1.355
 vlan 355
 nameif in
 bridge-group 20
 security-level 100


interface GigabitEthernet0/1.366
 vlan 366
 nameif out
 bridge-group 20
 security-level 0

monitor-interface inside
monitor-interface dmz
monitor-interface outside
monitor-interface in
monitor-interface out
```

Verification

Step 1: Verify bridge group configuration

ASA3

```
ASA3TFW(config)# show bridge-group
Static mac-address entries:  0 (in use), 65535 (max)
Dynamic mac-address entries: 0 (in use), 65535 (max)

 Bridge Group: 20
 Interfaces:
```

```
 GigabitEthernet0/1.355
 GigabitEthernet0/1.366

 Management System IP Address:  192.168.56.100 255.255.255.0
 Management Current IP Address: 192.168.56.100 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 0

 Bridge Group: 10
 Interfaces:
 GigabitEthernet0/0.311
 GigabitEthernet0/0.322
 GigabitEthernet0/0.344

 Management System IP Address:  192.168.124.100 255.255.255.0
 Management Current IP Address: 192.168.124.100 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 0
```

ASA4

```
ASA3TFW(config)# show bridge-group
Static mac-address entries:  0 (in use), 65535 (max)
Dynamic mac-address entries: 3 (in use), 65535 (max)

 Bridge Group: 20
 Interfaces:
 GigabitEthernet0/1.355
 GigabitEthernet0/1.366

 Management System IP Address:  192.168.56.100 255.255.255.0
 Management Current IP Address: 192.168.56.101 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 0

 Bridge Group: 10
 Interfaces:
 GigabitEthernet0/0.311
 GigabitEthernet0/0.322
 GigabitEthernet0/0.344

 Management System IP Address:  192.168.124.100 255.255.255.0
 Management Current IP Address: 192.168.124.101 255.255.255.0
```

```
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 3
```

```
ASA3TFW(config)# sh nameif
Interface                  Name                       Security
GigabitEthernet0/0.311     inside                     100
GigabitEthernet0/0.322     dmz                         50
GigabitEthernet0/0.344     outside                      0
GigabitEthernet0/1.355     in                         100
GigabitEthernet0/1.366     out                          0
```

ASA3

```
ASA3TFW(config)# sh interface ip brief
Interface                                IP-Address           OK?  Method  Status
Protocol
GigabitEthernet0/0          unassigned      YES unset  up                    up
GigabitEthernet0/0.311      192.168.124.100 YES unset  up                    up
GigabitEthernet0/0.322      192.168.124.100 YES unset  up                    up
GigabitEthernet0/0.344      192.168.124.100 YES unset  up                    up
GigabitEthernet0/1          unassigned      YES unset  up                    up
GigabitEthernet0/1.355      192.168.56.100  YES unset  up                    up
GigabitEthernet0/1.366      192.168.56.100  YES unset  up                    up
GigabitEthernet0/2          30.1.1.1        YES unset  up                    up
<SNIP>
BVI10                       192.168.124.100 YES unset  up                    up
BVI20                       192.168.56.100  YES unset  up                    up

ASA3TFW(config)# sh monitor-interface
        This host: Primary - Active
                Interface inside (192.168.124.100): Normal (Monitored)
                Interface dmz (192.168.124.100): Normal (Monitored)
                Interface outside (192.168.124.100): Normal (Monitored)
                Interface in (192.168.56.100): Normal (Monitored)
                Interface out (192.168.56.100): Normal (Monitored)
        Other host: Secondary - Standby Ready
                Interface inside (192.168.124.101): Normal (Monitored)
                Interface dmz (192.168.124.101): Normal (Monitored)
                Interface outside (192.168.124.101): Normal (Monitored)
                Interface in (192.168.56.101): Normal (Monitored)
                Interface out (192.168.56.101): Normal (Monitored)

ASA3TFW(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FA1LOVER GigabitEthernet0/2 (up)
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 23:35:43 UTC Jan 23 2014
        This host: Primary - Active
                Active time: 3074 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface inside (192.168.124.100): Normal (Monitored)
                  Interface dmz (192.168.124.100): Normal (Monitored)
                  Interface outside (192.168.124.100): Normal (Monitored)
                  Interface in (192.168.56.100): Normal (Monitored)
                  Interface out (192.168.56.100): Normal (Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up
        Other host: Secondary - Standby Ready
                Active time: 9 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface inside (192.168.124.101): Normal (Monitored)
                  Interface dmz (192.168.124.101): Normal (Monitored)
                  Interface outside (192.168.124.101): Normal (Monitored)
                  Interface in (192.168.56.101): Normal (Monitored)
                  Interface out (192.168.56.101): Normal (Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         505        0          397        0
        sys cmd         397        0          397        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        1          0          0          0
        ARP tbl         79         0          0          0
        L2BRIDGE Tbl    5          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   19         0          0          0
        User-Identity   4          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       7       3049
        Xmit Q:         0       44      4157
```

ASA4

```
ASA3TFW(config)# sh interface ip brief
Interface                              IP-Address           OK?  Method  Status
Protocol
GigabitEthernet0/0          unassigned      YES unset  up                    up
GigabitEthernet0/0.311      192.168.124.101 YES unset  up                    up
GigabitEthernet0/0.322      192.168.124.101 YES unset  up                    up
GigabitEthernet0/0.344      192.168.124.101 YES unset  up                    up
GigabitEthernet0/1          unassigned      YES unset  up                    up
GigabitEthernet0/1.355      192.168.56.101  YES unset  up                    up
GigabitEthernet0/1.366      192.168.56.101  YES unset  up                    up
GigabitEthernet0/2          30.1.1.2        YES unset  up                    up
<SNIP>
BVI10                       192.168.124.100 YES unset  up                    up
BVI20                       192.168.56.100  YES unset  up                    up
```

Task 4: ACLs on ASA-3

- Configure interface specific ACL's to allow RIPv2 traffic between R1,R2 and R4.
- Allow all outbound HTTP, HTTPS, FTP, telnet and DNS traffic on BVI 10 group for all dmz and inside hosts.
- Do not configure any ACL's for BVI 20 group. Do not use Global ACL's.

Task-4:Solutions

Step 1: Configure interface specific ACL's to allow RIP packets to pass through and apply on the interface of the correct bridge group interface (inside,outside,dmz). Configure this on ASA3 which is the Active unit.

```
access-list DMZ extended permit udp host 192.168.124.2 host 224.0.0.9
access-list OUT extended permit udp host 192.168.124.4 host 224.0.0.9
access-list IN extended permit udp host 192.168.124.1 host 224.0.0.9

access-group DMZ in interface dmz
access-group IN in interface inside
access-group OUT in interface outside
```

Step 2: Configure appropriate outbound ACL's as per the task.

```
access-list IN extended permit tcp any any eq www
access-list IN extended permit tcp any any eq ftp
access-list IN extended permit tcp any any eq https
```

```
access-list IN extended permit tcp any any eq telnet
access-list IN extended permit udp any any eq domain

access-list DMZ extended permit tcp any any eq www
access-list DMZ extended permit tcp any any eq ftp
access-list DMZ extended permit tcp any any eq https
access-list DMZ extended permit tcp any any eq telnet
access-list DMZ extended permit udp any any eq domain
```

Verification

Step 1: Verify if RIP routes are present on R1, R2 and R4.

R1

```
R1#sh ip route rip
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.124.4 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
R        2.2.2.0 [120/1] via 192.168.124.2, 00:00:12, FastEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
R        4.4.4.0 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
      6.0.0.0/32 is subnetted, 1 subnets
R        6.6.6.6 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
      7.0.0.0/32 is subnetted, 1 subnets
R        7.7.7.7 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
      22.0.0.0/24 is subnetted, 1 subnets
R        22.22.22.0 [120/1] via 192.168.124.2, 00:00:12, FastEthernet0/0
      44.0.0.0/32 is subnetted, 1 subnets
R        44.44.44.44 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
      66.0.0.0/32 is subnetted, 1 subnets
R        66.66.66.66 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
      77.0.0.0/32 is subnetted, 1 subnets
R        77.77.77.77 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
R     192.168.56.0/24 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
R     192.168.77.0/24 [120/1] via 192.168.124.4, 00:00:06, FastEthernet0/0
```

R2

```
R2#sh ip route rip
     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 192.168.124.1, 00:00:15, GigabitEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
R       4.4.4.0 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
R    192.168.77.0/24 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
     66.0.0.0/32 is subnetted, 1 subnets
R       66.66.66.66 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
     6.0.0.0/32 is subnetted, 1 subnets
R       6.6.6.6 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
R    192.168.56.0/24 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
     7.0.0.0/32 is subnetted, 1 subnets
R       7.7.7.7 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
     77.0.0.0/32 is subnetted, 1 subnets
R       77.77.77.77 [120/1] via 192.168.124.4, 00:00:20, GigabitEthernet0/0
     11.0.0.0/32 is subnetted, 1 subnets
R       11.11.11.11 [120/1] via 192.168.124.1, 00:00:15, GigabitEthernet0/0
     44.0.0.0/32 is subnetted, 1 subnets
R       44.44.44.44 [120/1] via 192.168.124.4, 00:00:21, GigabitEthernet0/0
R*   0.0.0.0/0 [120/1] via 192.168.124.4, 00:00:21, GigabitEthernet0/0
```

R4

```
R4#sh ip route rip
     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 192.168.124.1, 00:00:24, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
R       2.2.2.0 [120/1] via 192.168.124.2, 00:00:04, FastEthernet0/0
     22.0.0.0/24 is subnetted, 1 subnets
R       22.22.22.0 [120/1] via 192.168.124.2, 00:00:04, FastEthernet0/0
     11.0.0.0/32 is subnetted, 1 subnets
R       11.11.11.11 [120/1] via 192.168.124.1, 00:00:24, FastEthernet0/0
```

ASA3

```
Show access-list
<SNIP>
access-list DMZ line 1 extended permit udp host 192.168.124.2 host 224.0.0.9
(hitcnt=2)
access-list OUT line 1 extended permit udp host 192.168.124.4 host 224.0.0.9
(hitcnt=2)
access-list IN line 1 extended permit udp host 192.168.124.1 host 224.0.0.9
(hitcnt=2)
<SNIP>
```

Step 2: Telnet from R1 and R2 to R4 loobkack0.

```
R1#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:16
*514 vty 0                 idle                 00:00:00 192.168.124.1
```

```
R2#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:14
*514 vty 0                 idle                 00:00:00 192.168.124.2
```

ASA3

```
ASA3TFW(config)# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list DMZ; 6 elements; name hash: 0x55d29ba9
access-list DMZ line 1 extended permit udp host 192.168.124.2 host 224.0.0.9
(hitcnt=2) 0x809dcc09
access-list DMZ line 2 extended permit tcp any any eq www (hitcnt=0)
0x9fbee591
access-list DMZ line 3 extended permit tcp any any eq ftp (hitcnt=0)
0xadb6b6ef
access-list DMZ line 4 extended permit tcp any any eq https (hitcnt=0)
0x1613d92a
access-list DMZ line 5 extended permit tcp any any eq telnet (hitcnt=1)
0xdce165bd
access-list DMZ line 6 extended permit udp any any eq domain (hitcnt=0)
0x28728588
access-list OUT; 1 elements; name hash: 0xcd7d0798
access-list OUT line 1 extended permit udp host 192.168.124.4 host 224.0.0.9
(hitcnt=2) 0x485692d1
access-list IN; 6 elements; name hash: 0x9f2434aa
access-list IN line 1 extended permit udp host 192.168.124.1 host 224.0.0.9
(hitcnt=2) 0xce7207e2
access-list IN line 2 extended permit tcp any any eq www (hitcnt=0)
0x13f8d01c
access-list IN line 3 extended permit tcp any any eq ftp (hitcnt=0)
0xf2508d85
access-list IN line 4 extended permit tcp any any eq https (hitcnt=0)
0x73ce9627
```

```
access-list IN line 5 extended permit tcp any any eq telnet (hitcnt=2)
0x6367dd84
access-list IN line 6 extended permit udp any any eq domain (hitcnt=0)
0xbb228a88
```

Task 5: Transparent firewall NAT on ASA-3

- Configure Object Static NAT for R5 Lo0 to 192.168.56.55.
- You are allowed to create one static route to accomplish this task.
- R5 Lo0 should be able to telnet and ping R1 Lo0. Ensure that you match the below output.

```
R5#ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#telnet 1.1.1.1 /source-interface lo0
Trying 1.1.1.1 ... Open

R1#who
    Line       User       Host(s)              Idle       Location
*514 vty 0                 idle                 00:00:00 192.168.56.55

  Interface    User               Mode         Idle     Peer Address

R1#exi

[Connection to 1.1.1.1 closed by foreign host]
R5#
```

- You are allowed to configure ACL's to allow access on BVI 10 outside interface only.
- No ACL's should be configured on any BVI 20 group of interfaces. Do not use Global ACL.

Task-1:Solutions

Step 1: Configure Static Object NAT for 5.5.5.5 and add configure a static route on ASA3

```
object network R5lo0
 host 5.5.5.5
 nat (in,out) static 192.168.56.55

route in 5.5.5.5 255.255.255.255 192.168.56.5
```

Step 2: Allow telnet and ICMP Echo on the "outside" interface of BVI 10. This is the traffic from R5 to R1 loopback0's.

```
access-list OUT extended permit tcp host 192.168.56.55 host 1.1.1.1 eq telnet
access-list OUT extended permit icmp host 192.168.56.55 host 1.1.1.1 echo
```

Step 3: Inspect ICMP globall since the task states not to configure ACL's for BVI20. Hence the echo-reply from R1 Lo0 will be allowed back only if ICMP is inspected.

```
policy-map global_policy
 class inspection_default
   inspect icmp
```

Verification

Step 1: Telnet and Ping from R5 as per the task

R5

```
R5#telnet 1.1.1.1 /source-interface lo0
Trying 1.1.1.1 ... Open

R1#show users
    Line       User       Host(s)              Idle       Location
*514 vty 0                 idle                 00:00:00 192.168.56.55


R5#ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Step 2: Verify NAT table on ASA3.

```
ASA3TFW(config)# show nat detail

Auto NAT Policies (Section 2)
1 (in) to (out) source static R5lo0 192.168.56.55
    translate_hits = 15, untranslate_hits = 0
    Source - Origin: 5.5.5.5/32, Translated: 192.168.56.55/32
```

Notes

ASA 8.4 version supports automatic stateful failover for dynamic routing protocols (EIGRP and OSPF) to minimize traffic disruption during re-convergance of the routing protocols. No

additional configuration is required except enabling stateful failover. Here the routes learnt from OSPF or EIGRP is synced in the RIB on the standby unit. During a failover event the traffic passes normally over the newly active secondary unit since it has the routes. Immediately after a failover the routes epoch number in the RIB increments and re-convergance timer starts on the active unit. During this timer the active unit will re-establish OSPF or EIGRP adjacency with the peer router and install routes in the routing table with an updated epoch number and replace the old ones. Use “show route failover” for more info on the sequence number, re-convergance timer etc.

Lab 8: Routed Mode Multi-Context and Active/Active Failover

Lab 8: Routed Mode Multi-Context and Active/Active Failover – This lab is intended to let you be familiar with configuring ASA in multi-context routed mode with failover. Using multicontext you can configure Active/Active failover or Active/Standby failover. If both the device loadshare traffic, then it's called Active/Active. This is a very key topic and you will understand how order of operation is important when configuring Active/Active failover. Hence to begin with we shall start with just configuring one ASA 5515-X series with Multi-context and then advance to Active/Active failover.

General Rules

- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

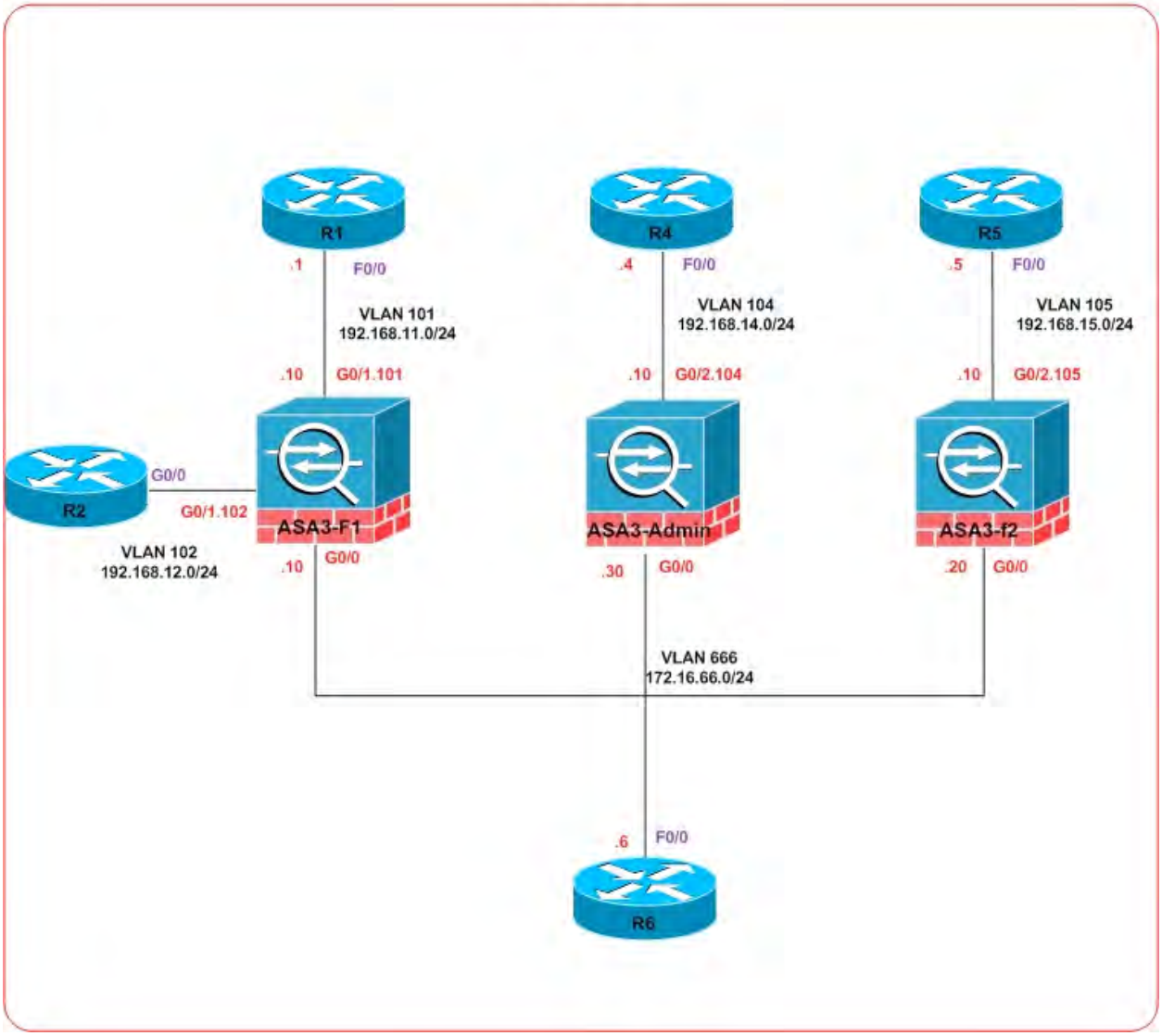
Estimated Time to Complete: 3 Hours

Pre-setup

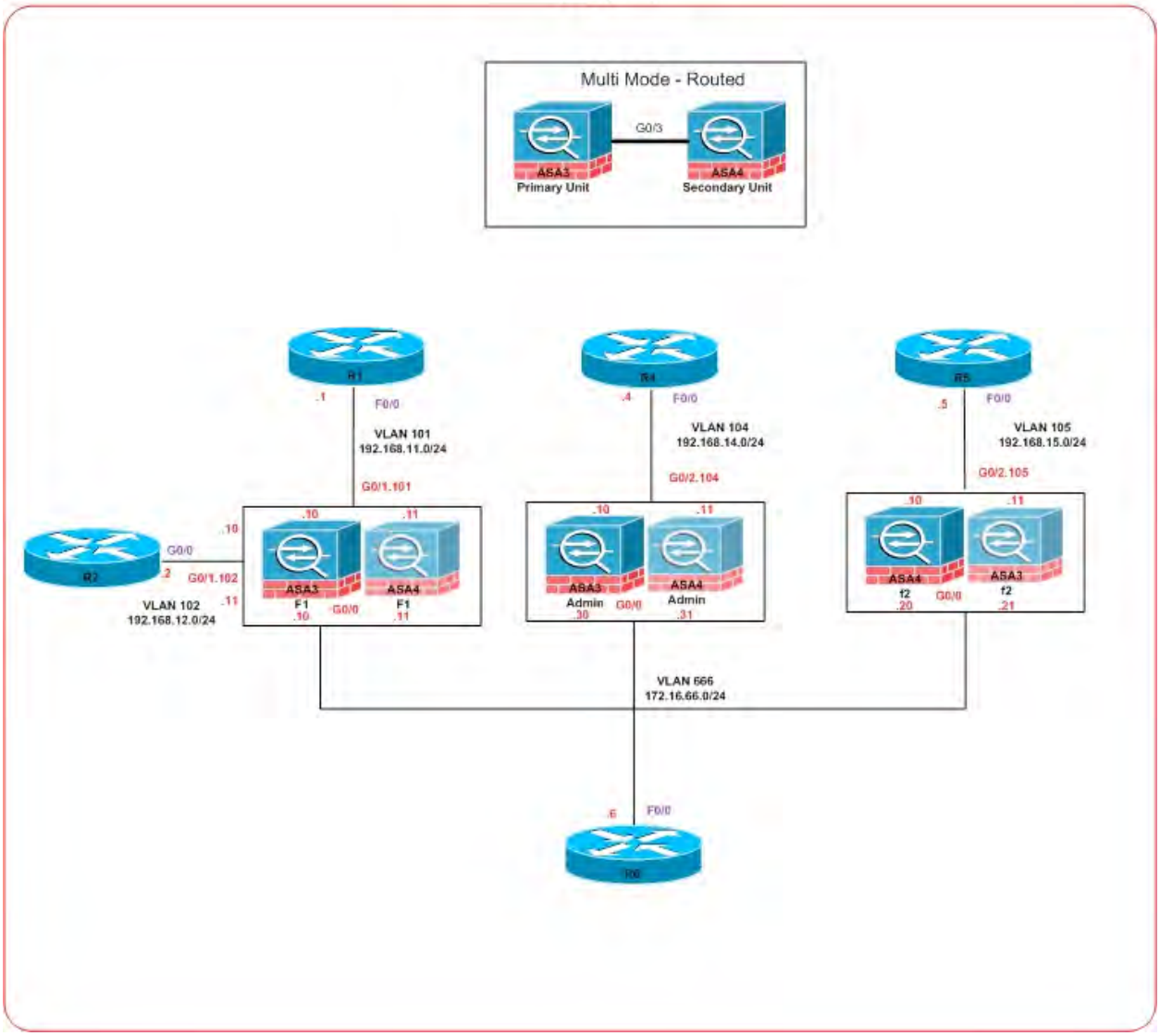
Load the initial configuration for Lab 8. Routers are pre-configured. Use the logical topology drawing - Network Topology 1.8 - to understand the logical topology when Multi-Context firewall is introduced. Use the logical topology drawing - Network Topology 1.9 - to understand the logical topology when Multi-Context firewall with Active/Active failover is introduced. Double-check the loaded pre-configuration before starting the Lab.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.8
(Logical)



Network Topology 1.9
(Logical)



Detailed Solution:Lab-8

Task 1: Basic VLAN Setup

- Configure the Catalyst switch with the appropriate VLANs for ports and trunks for the firewall as per topology diagram 1.8.

Task-1:Solutions

Step 1: Configure CAT3 switchports connected to ASA3 :

```
interface GigabitEthernet1/0/19
 switchport access vlan 666
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101,102
 switchport mode trunk

interface GigabitEthernet1/0/21
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 104,105
 switchport mode trunk
```

Verification

This task can only ve verified when ASA interfaces have been initialized. Use “show interface trunk” command after the interfaces have been initialized.

Task 2: Firewall Mode on ASA-3

- Change the firewall mode on ASA-3 to multi-mode to support multi-context.
- Configure a hostname of “ASA003” on ASA-3.
- ASA003 should have a domain name of ipexpert.com.
- Administratively enable all interfaces.

Task-2:Solutions

Step 1: Change the mode to multiple. This will reboot the device.

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
```

Step 2: Configure hostname, domain name, and unshut the interfaces.

```
hostname ASA003
domain-name ipexpert.com

interface GigabitEthernet0/0
no shutdown

interface GigabitEthernet0/1
no shutdown

interface GigabitEthernet0/2
no shutdown

interface GigabitEthernet0/3
no shutdown
```

Verification

Step 1: Verify the trunk configuration on SW3

```
SW3#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/15    on               802.1q         trunking      1
Gi1/0/16    on               802.1q         trunking      1
Gi1/0/17    on               802.1q         trunking      1
Gi1/0/18    on               802.1q         trunking      1
Gi1/0/20    on               802.1q         trunking      1
Gi1/0/21    on               802.1q         trunking      1
Gi1/0/23    on               802.1q         trunking      1
Gi1/0/24    on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/0/15    1-4094
Gi1/0/16    1-4094
Gi1/0/17    1-4094
Gi1/0/18    1-4094
Gi1/0/20    101-102
Gi1/0/21    104-105
Gi1/0/23    1-4094
Gi1/0/24    1-4094

Port        Vlans allowed and active in management domain
Gi1/0/15    1,101-102,104-105,333,666
Gi1/0/16    1,101-102,104-105,333,666
Gi1/0/17    1,101-102,104-105,333,666
Gi1/0/18    1,101-102,104-105,333,666
Gi1/0/20    101-102
Gi1/0/21    104-105
```

```
Gi1/0/23    1,101-102,104-105,333,666
Gi1/0/24    1,101-102,104-105,333,666

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/15    1,101-102,104-105,333,666
Gi1/0/16    none
Gi1/0/17    none
Gi1/0/18    none
Gi1/0/20    101-102
Gi1/0/21    104-105
Gi1/0/23    1,101-102,104-105,333,666
Gi1/0/24    1,101-102,104-105,333,666
```

Task 3: VLAN Sub-interface creation on ASA-3

- Configure VLAN sub-interfaces on ASA3 as per the parameters below:

ASA Interface	VLAN
G0/1.101	101
G0/1.102	102
G0/2.104	104
G0/2.105	105

Task-3:Solutions

Step 1: Create sub-interfaces on ASA3

```
interface GigabitEthernet0/1.101
 vlan 101

interface GigabitEthernet0/1.102
 vlan 102

interface GigabitEthernet0/2.104
 vlan 104

interface GigabitEthernet0/2.105
 vlan 105
```

Verification

Make sure your configuration matched the solution

Task 4: Context creation on ASA-3

- Remove any existing context configuration and delete any .cfg files from flash.
- Configure contexts as per the table below. Designate “Admin” to be the admin context.
- Gi0/0 will be shared between all the contexts.
- Allocate the default virtual sensor to the Admin context.
- Use the “mac-address auto” with any prefix of your choice for auto generation of MAC address.

Context	Interface Allocation	Interface name	Configuration file (Flash/Disk0)
Admin	G0/0	A_OUT	Admin.cfg
Admin	G0/2.104	A_IN	
f1	G0/0	----------	F1.cfg
f1	G0/1.101	----------	
f1	G0/1.102	----------	
f2	G0/0	F2_OUT	F2.cfg
f2	G0/2.105	F2_IN	

- Limit the resource allocation for the f2 context as per the parameters below:

Resource	Limits
Connections	2000
Xlate	200
Telnet,SSH,ASDM	2 each

Task-4:Solutions

Step 1: Configure context resource class to limit resources as per the task.

```
class f2
  limit-resource Conns 2000
  limit-resource Telnet 2
  limit-resource ASDM 2
  limit-resource SSH 2
  limit-resource Xlates 200
```

Step 2: Context as per the parameters specified in the task. Delete any existing .cfg files in the flash.

```
ASA003# delete flash://*.cfg

context Admin
  allocate-interface GigabitEthernet0/0 A_OUT
  allocate-interface GigabitEthernet0/2.104 A_IN
  allocate-ips vs0
  config-url disk0:/Admin.cfg

context f1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1.101-GigabitEthernet0/1.102
  config-url disk0:/F1.cfg

context f2
  member f2
  allocate-interface GigabitEthernet0/0 F2_OUT
  allocate-interface GigabitEthernet0/2.105 F2_IN
  config-url disk0:/F2.cfg

admin-context Admin
no context admin
```

Step 3: Configure MAC-Address Auto with any prefix.

```
mac-address auto prefix 77
```

```
ASA003# sh context
Context Name      Class      Interfaces           URL
*Admin            default    GigabitEthernet0/0,  disk0:/Admin.cfg
                             GigabitEthernet0/2.104
 f1               default    GigabitEthernet0/0,  disk0:/F1.cfg
                             GigabitEthernet0/1.101-102
 f2               f2         GigabitEthernet0/0,  disk0:/F2.cfg
                             GigabitEthernet0/2.105

Total active Security Contexts: 3
```

```
ASA003# sh context detail
Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/1,
     GigabitEthernet0/1.101-102, GigabitEthernet0/2,
     GigabitEthernet0/2.104-105, GigabitEthernet0/3,
     GigabitEthernet0/4, GigabitEthernet0/5, Internal-Control0/0,
     Internal-Data0/0, Internal-Data0/1, Internal-Data0/2,
     Management0/0, Virtual254
  Class: default, Flags: 0x00000819, ID: 0
```

```
Context "Admin", has been created
  Config URL: disk0:/Admin.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/2.104
  Mapped Interfaces: A_IN, A_OUT
  Real IPS Sensors: vs0
  Mapped IPS Sensors: vs0
  Class: default, Flags: 0x00000813, ID: 2

Context "f1", has been created
  Config URL: disk0:/F1.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/1.101-102
  Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/1.101-102
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: default, Flags: 0x00000811, ID: 3

Context "f2", has been created
  Config URL: disk0:/F2.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/2.105
  Mapped Interfaces: F2_IN, F2_OUT
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: f2, Flags: 0x00000811, ID: 4

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: default, Flags: 0x00000809, ID: 257
```

Task 5: Admin context configuration on ASA-3

- The Admin context should have a domain name of ipexpert.com.
- Configure interfaces with the parameters below. After you perform this task, ensure that you can ping your directly connected neighbors.

ASA Interface	IP Address	Security Level	Name
A_OUT	172.16.66.30/24	0	outside
A_IN	192.168.14.10/24	100	inside

- Configure a static default route toward R6 and a static route for R4 Lo0 (4.4.4.4).
- Enable Telnet on the inside interface from anyone.
- Enable SSH and ASDM access on the outside interface from anyone.

- Create username cisco password cisco123 and enable SSH, Telnet, and ASDM authentication locally.
- Create an inter-context static route to R5 Lo0 (5.5.5.5).
- Configure an ACL to allow all traffic between R4 Lo0 and R5 Lo0. Apply this on the outside interface.

Task-5:Solutions

Step 1: Change context to "Admin" and initialize the interfaces and configure hostname, domain name

```
changeto context Admin

hostname Admin
domain-name ipexpert.com

interface A_OUT
 nameif outside
 security-level 0
 ip address 172.16.66.30 255.255.255.0

interface A_IN
 nameif inside
 security-level 100
 ip address 192.168.14.10 255.255.255.0
```

Step 2: Configure static default toute towards R6 and a static route for R4Lo0

```
route outside 0.0.0.0 0.0.0.0 172.16.66.6
route inside 4.4.4.4 255.255.255.255 192.168.14.4
```

Step 3: Configure management access for Admin context

```
changeto system
asdm image disk0:/asdm-66114.bin

changeto context Admin

crypto key generate rsa

http server enable
http 0.0.0.0 0.0.0.0 outside
telnet 0.0.0.0 0.0.0.0 inside
ssh 0.0.0.0 0.0.0.0 outside

username cisco password cisco123
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
```

```
aaa authentication telnet console LOCAL
```

Step 4: Configure intercontext routing for R5 Lo0

```
route outside 5.5.5.5 255.255.255.255 172.16.66.20
```

Step 5: Configure ACL's to allow traffic between all R4Lo0 and R5Lo0. Apply this on the outside interface.

```
access-list OUT extended permit ip host 5.5.5.5 host 4.4.4.4
access-group OUT in interface outside
```

Verification

Step 1: Verify the interface configuration and the MAC address

```
ASA003/Admin(config)# sh interface detail

Interface A_OUT "Outside", is up, line protocol is up
        MAC address a24d.0000.0002, MTU 1500
        IP address 172.16.66.30, subnet mask 255.255.255.0
  Traffic Statistics for "Outside":
        0 packets input, 0 bytes
        3 packets output, 84 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface A_IN "inside", is up, line protocol is up
        MAC address a24d.0000.0004, MTU 1500
        IP address 192.168.14.10, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        3 packets output, 84 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
  Control Point Vlan104 States:
        Interface vlan config status is active
        Interface vlan state is UP
```

Step 2: Verify the static routes

```
ASA003/Admin(config)# sh route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.66.6 to network 0.0.0.0

C    192.168.14.0 255.255.255.0 is directly connected, inside
S    4.4.4.4 255.255.255.255 [1/0] via 192.168.14.4, inside
S    5.5.5.5 255.255.255.255 [1/0] via 172.16.66.20, Outside
C    172.16.66.0 255.255.255.0 is directly connected, Outside
S*   0.0.0.0 0.0.0.0 [1/0] via 172.16.66.6, Outside
```

Step 3: Telnet into Admin context from R4

```
R4#telnet 192.168.14.10
Trying 192.168.14.10 ... Open


User Access Verification

Username: cisco
Password: ********
Type help or '?' for a list of available commands.
ASA003/Admin> en
Password: ********
ASA003/Admin# exit

Logoff


[Connection to 192.168.14.10 closed by foreign host]
```

Step 4: Ping R6 Lo0 and R4Lo0 from Admin context. Intercontext routing can be verified after "f2" context has been initialized.

```
ASA003/Admin(config)# ping 6.6.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
ASA003/Admin(config)# ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Task 6: f2 context configuration on ASA-3

- Configure interfaces with the parameters below. After you perform this task, ensure that you can ping your directly connected neighbors.

ASA Interface	IP Address	Security Level	Name
F2_OUT	172.16.66.20/24	0	OUT
F2_IN	192.168.15.10/24	100	IN

- Configure a static default route toward R6 and a static route for R5 Lo0 (5.5.5.5).
- Create an inter-context static route to R4 Lo0 (4.4.4.4).
- Configure an ACL to allow all traffic between R4 Lo0 and R5Lo0. Configure Global ACLs.
- Configure Static Identity NAT using Manual NAT for R5 Lo0 when it communicates with R4 Lo0.
- All other outbound traffic should be PATed to the interface IP using Auto NAT.
- Allow all outbound telnet traffic from VLAN 105. Configure Global ACLs.

Task-6:Solutions

Step 1: Change context to "f2" and initialize the interfaces and configure hostname

```
Changeto context f2
hostname f2

interface F2_OUT
 nameif OUT
 security-level 0
 ip address 172.16.66.20 255.255.255.0

interface F2_IN
 nameif IN
 security-level 100
 ip address 192.168.15.10 255.255.255.0
```

Step 2: Configure static default toute towards R6 and a static route for R4Lo0

```
route OUT 0.0.0.0 0.0.0.0 172.16.66.6
route IN 5.5.5.5 255.255.255.255 192.168.15.5
```

Step 3: Configure Manual NAT (policy NAT). Create objects and then the NAT configuration.

```
object network R5
 host 5.5.5.5
object network R4
 host 4.4.4.4

nat (IN,OUT) source static R5 R5 destination static R4 R4
```

Step 4: Configure intercontext routing between R4 and R5 Lo0

```
route OUT 4.4.4.4 255.255.255.255 172.16.66.30
```

Step 5: Configure outbound PAT to the OUT interface

```
object network ALL
 subnet 0.0.0.0 0.0.0.0

object network ALL
 nat (IN,OUT) dynamic interface
```

Step 6: Configure ACL's to allow traffic between R4 and R5 Lo0 and aoutbout telnet traffic from VLAN 105 using Global ACL's.

```
access-list GLOBAL extended permit ip host 4.4.4.4 host 5.5.5.5
access-list GLOBAL extended permit ip host 5.5.5.5 host 4.4.4.4
access-list GLOBAL extended permit tcp 192.168.15.0 255.255.255.0 any eq
telnet

access-group GLOBAL global
```

Verification

Step 1: Verify the interface configuration and the MAC address

```
ASA003/f2(config)# sh interface detail
Interface F2_OUT "OUT", is up, line protocol is up
        MAC address a24d.0000.0006, MTU 1500
        IP address 172.16.66.20, subnet mask 255.255.255.0
  Traffic Statistics for "OUT":
        1 packets input, 28 bytes
        1 packets output, 28 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface F2_IN "IN", is up, line protocol is up
```

```
        MAC address a24d.0000.0008, MTU 1500
        IP address 192.168.15.10, subnet mask 255.255.255.0
  Traffic Statistics for "IN":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
  Control Point Vlan105 States:
        Interface vlan config status is active
        Interface vlan state is UP
```

Step 2: Verify the static routes

```
ASA003/f2(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.66.6 to network 0.0.0.0

C    192.168.15.0 255.255.255.0 is directly connected, IN
S    4.4.4.4 255.255.255.255 [1/0] via 172.16.66.30, OUT
S    5.5.5.5 255.255.255.255 [1/0] via 192.168.15.5, IN
C    172.16.66.0 255.255.255.0 is directly connected, OUT
S*   0.0.0.0 0.0.0.0 [1/0] via 172.16.66.6, OUT
```

Step 3: Verify NAT table

```
ASA003/f2(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (IN) to (OUT) source static R5 R5   destination static R4 R4
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 5.5.5.5/32, Translated: 5.5.5.5/32
    Destination - Origin: 4.4.4.4/32, Translated: 4.4.4.4/32

Auto NAT Policies (Section 2)
1 (IN) to (OUT) source dynamic ALL interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 172.16.66.20/24
```

Step 4: Telnet between R5 Lo0 and R4 Lo0. Also telnet from R5 to R6

```
R5#telnet 4.4.4.4 /source-interface lo0
Trying 4.4.4.4 ... Open

R4#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:25
*514 vty 0                 idle                 00:00:00 5.5.5.5

R5#telnet 6.6.6.6
Trying 6.6.6.6 ... Open



R6#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:21
*514 vty 0                 idle                 00:00:00 172.16.66.20
```

Task 7: f1 context configuration on ASA-3

- Configure interfaces with the parameters below. After you perform this task ensure that you can ping your directly connected neighbors.

ASA Interface	IP Address	Security Level	Name
G0/0	172.16.66.10/24	0	outside
G0/1.101	192.168.11.10/24	100	inside
G0/1.102	192.168.12.10/24	50	dmz

- Configure static default route towards R6 and a static route for R2 (2.2.2.2) and R1 Lo0 (1.1.1.1)
- Configure Static Auto NAT and translate 1.1.1.1 to 172.16.66.80 on the outside and 2.2.2.2 to 172.16.66.23.
- Allow all ICMP traffic to pass through from the outside
- Allow HTTP access to 172.16.66.80 and telnet access to 172.16.66.23 anyone from the outside. Telnet from R5 and R4 f0/0 to 172.16.66.23 should be successful.
- Do not use global ACL's

Task-7:Solutions

Step 1: Change context to "f1" and initialize the interfaces and configure hostname

```
Changeto context f1
hostname f1

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.66.10 255.255.255.0

interface GigabitEthernet0/1.101
 nameif inside
 security-level 100
 ip address 192.168.11.10 255.255.255.0

interface GigabitEthernet0/1.102
 nameif dmz
 security-level 50
 ip address 192.168.12.10 255.255.255.0
```

Step 2: Configure a default toute towards R6 and static routes for R1Lo0 and R2Lo0 on "F1" context

```
route outside 0.0.0.0 0.0.0.0 172.16.66.6
route inside 1.1.1.1 255.255.255.255 192.168.11.1
route dmz 2.2.2.2 255.255.255.255 192.168.12.2
```

Step 3: Configure static Auto NAT

```
object network R1
 host 1.1.1.1
 nat (inside,outside) static 172.16.66.80
object network R2
 host 2.2.2.2
 nat (dmz,outside) static 172.16.66.23
```

Step 4: Configure ACL's as per the task and apply on the outside interface

```
access-list OUT extended permit icmp any any
access-list OUT extended permit tcp any host 1.1.1.1 eq www
access-list OUT extended permit tcp any host 2.2.2.2 eq telnet

access-group OUT in interface outside
```

Verification

Step 1: Verify the interface configuration and the MAC address

```
ASA003/F1(config)# sh interface detail
```

```
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
        MAC address a24d.0000.000a, MTU 1500
        IP address 172.16.66.10, subnet mask 255.255.255.0
  Traffic Statistics for "outside":
        3 packets input, 102 bytes
        8 packets output, 986 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface GigabitEthernet0/1.101 "inside", is up, line protocol is up
        MAC address a24d.0000.000c, MTU 1500
        IP address 192.168.11.10, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
        7 packets input, 976 bytes
        2 packets output, 56 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
  Control Point Vlan101 States:
        Interface vlan config status is active
        Interface vlan state is UP
Interface GigabitEthernet0/1.102 "dmz", is up, line protocol is up
        MAC address a24d.0000.000e, MTU 1500
        IP address 192.168.12.10, subnet mask 255.255.255.0
  Traffic Statistics for "dmz":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
  Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
  Control Point Vlan102 States:
        Interface vlan config status is active
        Interface vlan state is UP
```

Step 2: Verify the static routes

```
ASA003/F1(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.66.6 to network 0.0.0.0

C    192.168.12.0 255.255.255.0 is directly connected, dmz
S    1.1.1.1 255.255.255.255 [1/0] via 192.168.11.1, inside
S    2.2.2.2 255.255.255.255 [1/0] via 192.168.12.2, dmz
C    172.16.66.0 255.255.255.0 is directly connected, outside
C    192.168.11.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 172.16.66.6, outside
```

Step 2: Ping from R2 to R6 Lo0

```
R2#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Step 3: Telnet R5/R4 to R2

```
R4#telnet 172.16.66.23
Trying 172.16.66.23 ... Open


R2#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:39
*578 vty 0                 idle                 00:00:00 192.168.14.4

R5#telnet 172.16.66.23
Trying 172.16.66.23 ... Open

R2#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:02:17
*578 vty 0                 idle                 00:00:09 172.16.66.20
```

Task 8: Basic VLAN Setup

- Configure the catalyst switch with the appropriate VLAN's for ports and trunks for the firewall to support topology diagram 1.9.

NOTE: *Refer Network Topology Diagram 1.9*

Task-1:Solutions

Step 1: Configure appropriate access VLAN and trunks on SW4 for ASA4

```
interface GigabitEthernet1/0/19
 switchport access vlan 666
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101,102
 switchport mode trunk

interface GigabitEthernet1/0/21
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 104,105
 switchport mode trunk
```

Verification

This task can only ve verified when ASA interfaces have been initialized. Use "show interface trunk" command after the interfaces have been initialized.

Task 9: Failover Configuration

- Change the mode to routed multi-mode on ASA-4
- Configure ASA-3 and ASA-4 for device level HA using failover feature on ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the below parameters for the failover configuration. Configure Switch such that G0/3 interface of the firewall should be in VLAN 333. Share G0/3 for stateful link failover. **DO NOT ENABLE FAILOVER IN THIS TASK.**

Failover interface – G0/3
Primary IP – 30.1.1.1/24
Standby IP – 30.1.1.2/24
Interface Name - FA1LOVER
Key - C1SCO

Task-9:Solutions

Step 1: Configure SW3 and SW4 G1/0/22 with access VLAN 333. You may create the VLAN on CAT4 if it does not exist.

CAT4

```
vlan 333
```

CAT3, CAT4

```
interface GigabitEthernet1/0/22
 switchport access vlan 333
 switchport mode access
 spanning-tree portfast
```

Step 2: Configure stateful Failover on ASA3 and ASA 4. Do not enable failover.

```
ASA3
changeto system
failover lan unit primary
failover lan interface FA1LOVER GigabitEthernet0/3
failover key C1SCO
failover link FA1LOVER GigabitEthernet0/3
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2

ASA4
Change the mode to Multiple

mode multi

After a reboot

interface GigabitEthernet0/3
no shut

failover lan unit secondary
failover lan interface FA1LOVER GigabitEthernet0/3
failover key C1SCO
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
```

Verification This task can be verified after task 10. Make sure the configs and the order of entering the configs match the solution.

Task 10: Active/Active Failover Configuration on ASA-3

- Admin and F1 context should be active on ASA-3 and f2 context should be active on ASA-4. Configure failover groups with pre-empt option.
- Configure failover accordingly and now enable failover.

Step 1: Configure failover groups with preempt option

ASA3 (System context)

```
failover group 1
  preempt
failover group 2
  secondary
  preempt
```

Step 2: Configure contexts to join failover groups (ASA3)

```
context Admin
  join-failover-group 1

context F1
  join-failover-group 1

context f2
  join-failover-group 2
```

Step 3: Enable Failover on ASA3

```
failover
```

Step 4: Enable Failover on ASA4

```
failover
```

Verification

Step 1: Verify the failover configuration on ASA3 and ASA4

ASA3

```
ASA003(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FA1LOVER GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Group 1 last failover at: 10:32:00 UTC Feb 28 2013
Group 2 last failover at: 10:31:58 UTC Feb 28 2013

  This host:    Primary
  Group 1       State:          Active
                Active time:    395 (sec)
  Group 2       State:          Standby Ready
                Active time:    146 (sec)
```

```
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Admin Interface Outside (172.16.66.30): Unknown (Waiting)
                  Admin   Interface   inside   (192.168.14.10):   Normal   (Not-
Monitored)
                  F1 Interface outside (172.16.66.10): Unknown (Waiting)
                  F1 Interface inside (192.168.11.10): Normal (Not-Monitored)
                  F1 Interface dmz (192.168.12.10): Normal (Not-Monitored)
                  f2 Interface OUT (0.0.0.0): Unknown (Waiting)
                  f2 Interface IN (0.0.0.0): Normal (Not-Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    247 (sec)

                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Admin Interface Outside (0.0.0.0): Unknown (Waiting)
                  Admin Interface inside (0.0.0.0): Normal (Not-Monitored)
                  F1 Interface outside (0.0.0.0): Unknown (Waiting)
                  F1 Interface inside (0.0.0.0): Normal (Not-Monitored)
                  F1 Interface dmz (0.0.0.0): Normal (Not-Monitored)
                  f2 Interface OUT (172.16.66.20): Unknown (Waiting)
                  f2 Interface IN (192.168.15.10): Normal (Not-Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         55         0          35         0
        sys cmd         33         0          33         0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        14         0          0          0
        ARP tbl         4          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          0          0
        User-Identity   4          0          2          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       35
```

```
        Xmit Q:          0        1        55
```

ASA3

```
ASA003(config)# sh context detail
Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/1,
     GigabitEthernet0/1.101-102, GigabitEthernet0/2,
     GigabitEthernet0/2.104-105, GigabitEthernet0/3,
     GigabitEthernet0/4, GigabitEthernet0/5, Internal-Control0/0,
     Internal-Data0/0, Internal-Data0/1, Internal-Data0/2,
     Management0/0, Virtual254
  Class: default, Flags: 0x00000819, ID: 0

Context "Admin", has been created
  Config URL: disk0:/ADmin.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/2.104
  Mapped Interfaces: A_IN, A_OUT
  Real IPS Sensors: vs0
  Mapped IPS Sensors: vs0
  Class: default, Flags: 0x00000813, ID: 2
  Failover group: 1

Context "F1", has been created
  Config URL: disk0:/F1.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/1.101-102
  Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/1.101-102
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: default, Flags: 0x00000811, ID: 3
  Failover group: 1

Context "f2", has been created
  Config URL: disk0:/F2.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/2.105
  Mapped Interfaces: F2_IN, F2_OUT
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: f2, Flags: 0x00000811, ID: 4
  Failover group: 2

<SNIP>
```

ASA4

```
ASA003(config)# sh failover
Failover On
Failover unit Secondary
Failover LAN Interface: FA1LOVER GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Group 1 last failover at: 10:35:51 UTC Apr 3 2013
Group 2 last failover at: 10:35:51 UTC Apr 3 2013

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    569 (sec)

                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Admin Interface Outside (0.0.0.0): Unknown (Waiting)
                  Admin Interface inside (0.0.0.0): Normal (Not-Monitored)
                  F1 Interface outside (0.0.0.0): Unknown (Waiting)
                  F1 Interface inside (0.0.0.0): Normal (Not-Monitored)
                  F1 Interface dmz (0.0.0.0): Normal (Not-Monitored)
                  f2 Interface OUT (172.16.66.20): Unknown (Waiting)
                  f2 Interface IN (192.168.15.10): Normal (Not-Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

  Other host:   Primary
  Group 1       State:          Active
                Active time:    717 (sec)
  Group 2       State:          Standby Ready
                Active time:    146 (sec)

                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Admin Interface Outside (172.16.66.30): Unknown (Waiting)
                  Admin   Interface   inside   (192.168.14.10):   Normal   (Not-
Monitored)
                  F1 Interface outside (172.16.66.10): Unknown (Waiting)
                  F1 Interface inside (192.168.11.10): Normal (Not-Monitored)
                  F1 Interface dmz (192.168.12.10): Normal (Not-Monitored)
                  f2 Interface OUT (0.0.0.0): Unknown (Waiting)
                  f2 Interface IN (0.0.0.0): Normal (Not-Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/3 (up)
```

```
        Stateful Obj    xmit       xerr       rcv        rerr
        General         78         0          110        0
        sys cmd         76         0          76         0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          26         0
        ARP tbl         0          0          4          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          0          0
        User-Identity   2          0          4          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       110
        Xmit Q:         0       1       78
```

Task 11: Re-configure Active and Standby IP address.

- Since failover is enabled. Re-configure each context with standby IP Address as per the network diagram 1.9 on the appropriate active ASA.
- Configure a static MAC address for A_OUT interface of Admin context. 0011.0011.0011 should be the active and 0022.0022.0022 should be the standby MAC address.

ASA3 (Active for Admin and F1 context)

```
changeto context Admin
interface A_OUT
 mac-address 0011.0011.0011 standby 0022.0022.0022
 ip address 172.16.66.30 255.255.255.0 standby 172.16.66.31

interface A_IN
  ip address 192.168.14.30 255.255.255.0 standby 192.168.14.31

changeto context f1

interface GigabitEthernet0/0
  ip address 172.16.66.10 255.255.255.0 standby 172.16.66.11

interface GigabitEthernet0/1.101
 ip address 192.168.11.10 255.255.255.0 standby 192.168.11.11

interface GigabitEthernet0/1.102
 ip address 192.168.12.10 255.255.255.0 standby 192.168.12.11
```

ASA4 (Active for f2 context)

```
changeto context f2

interface F2_OUT
 ip address 172.16.66.20 255.255.255.0 standby 172.16.66.21

interface F2_IN
 ip address 192.168.15.10 255.255.255.0 standby 192.168.15.11
```

Verification

Step 1: Verify the MAC address for Admin Context on ASA3

```
ASA003/Admin(config)# sh interface detail
Interface A_OUT "Outside", is up, line protocol is up
        MAC address 0011.0011.0011, MTU 1500
        IP address 172.16.66.30, subnet mask 255.255.255.0
<SNIP>
```

Step 3: Verify the IP address configuration on ASA3 for all the contexts

```
ASA003/Admin(config)# sh ip address
System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
A_OUT                    Outside                172.16.66.30    255.255.255.0   manual
A_IN                     inside                 192.168.14.30   255.255.255.0   manual
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
A_OUT                    Outside                172.16.66.30    255.255.255.0   manual
A_IN                     inside                 192.168.14.30   255.255.255.0   manual

ASA003/Admin(config)# changeto context F1
ASA003/F1(config)# sh ip address
System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       outside                172.16.66.10    255.255.255.0   manual
GigabitEthernet0/1.101   inside                 192.168.11.10   255.255.255.0   manual
GigabitEthernet0/1.102   dmz                    192.168.12.10   255.255.255.0   manual
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       outside                172.16.66.10    255.255.255.0   manual
GigabitEthernet0/1.101   inside                 192.168.11.10   255.255.255.0   manual
GigabitEthernet0/1.102   dmz                    192.168.12.10   255.255.255.0   manual



ASA003/F1(config)# changeto context f2
ASA003/f2(config)# sh ip address
System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
F2_OUT                   OUT                    172.16.66.20    255.255.255.0   manual
F2_IN                    IN                     192.168.15.10   255.255.255.0   manual
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
F2_OUT                   OUT                    172.16.66.21    255.255.255.0   manual
```

```
F2_IN                     IN                     192.168.15.11   255.255.255.0   manual
```

Step 4: Verify the IP address configuration on ASA4 for all the contexts

```
ASA003/Admin(config)# sh ip address
System IP Addresses:
Interface                 Name                   IP address      Subnet mask     Method
A_OUT                     Outside                172.16.66.30    255.255.255.0   manual
A_IN                      inside                 192.168.14.30   255.255.255.0   manual
Current IP Addresses:
Interface                 Name                   IP address      Subnet mask     Method
A_OUT                     Outside                172.16.66.31    255.255.255.0   manual
A_IN                      inside                 192.168.14.31   255.255.255.0   manual


ASA003/Admin(config)# changeto context F1
ASA003/F1(config)#  sh ip address
System IP Addresses:
Interface                 Name                   IP address      Subnet mask     Method
GigabitEthernet0/0        outside                172.16.66.10    255.255.255.0   manual
GigabitEthernet0/1.101    inside                 192.168.11.10   255.255.255.0   manual
GigabitEthernet0/1.102    dmz                    192.168.12.10   255.255.255.0   manual
Current IP Addresses:
Interface                 Name                   IP address      Subnet mask     Method
GigabitEthernet0/0        outside                172.16.66.11    255.255.255.0   manual
GigabitEthernet0/1.101    inside                 192.168.11.11   255.255.255.0   manual
GigabitEthernet0/1.102    dmz                    192.168.12.11   255.255.255.0   manual




ASA003/F1(config)# changeto context f2
ASA003/f2(config)# sh ip address
System IP Addresses:
Interface                 Name                   IP address      Subnet mask     Method
F2_OUT                    OUT                    172.16.66.20    255.255.255.0   manual
F2_IN                     IN                     192.168.15.10   255.255.255.0   manual
Current IP Addresses:
Interface                 Name                   IP address      Subnet mask     Method
F2_OUT                    OUT                    172.16.66.20    255.255.255.0   manual
F2_IN                     IN                     192.168.15.10   255.255.255.0   manual
```

Lab 9: Multi-Mode Transparent Firewall with Active/Active Failover

Lab 9: Transparent Mode Multi-Context – This lab is intended to let you be familiar with configuring ASA in multi-context transparent mode since there is a significant difference in configuring transparent firewall in Multi-context between 8.2 and 8.4/8.6 code of the ASA. This lab focuses on 8.6 version of the ASA. In version 8.2 only two unique interfaces can be added per context. This is, however, not the same in 8.6 version

General Rules

- By now you should have understood how to configure Failover and the order of operation when configuring Active/Active failover.
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

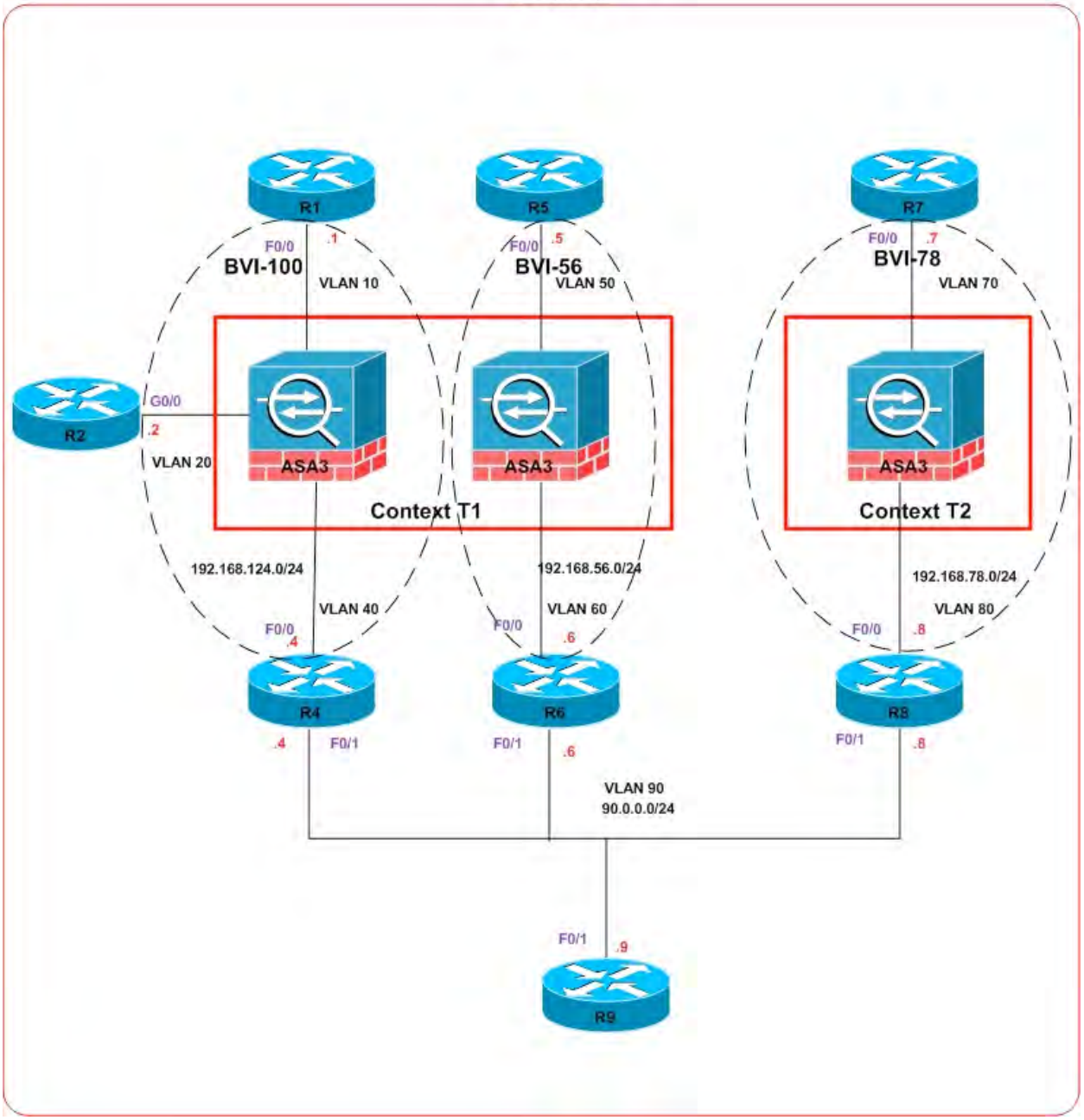
Estimated Time to Complete: 3 Hours

Pre-setup

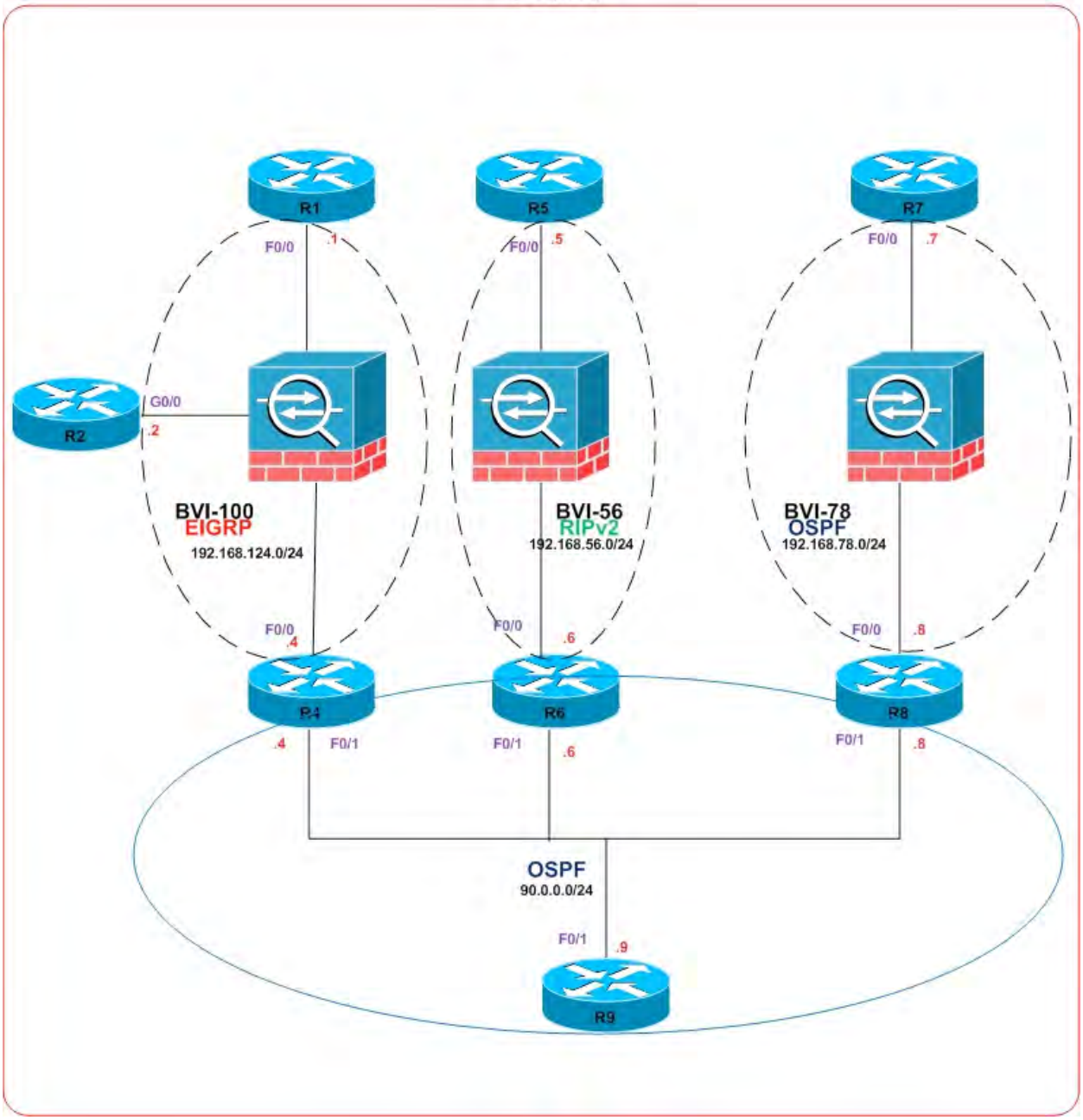
Load the initial configuration for Lab-9. Routers are pre-configured with routing. Use the logical topology drawing - Network Topology 1.10, 1.11 and 1.12 to understand the logical topology and routing topology when Multi-Context transparent firewall is introduced with Active/Active failover. Double check the loaded pre-configuration before starting the Lab.

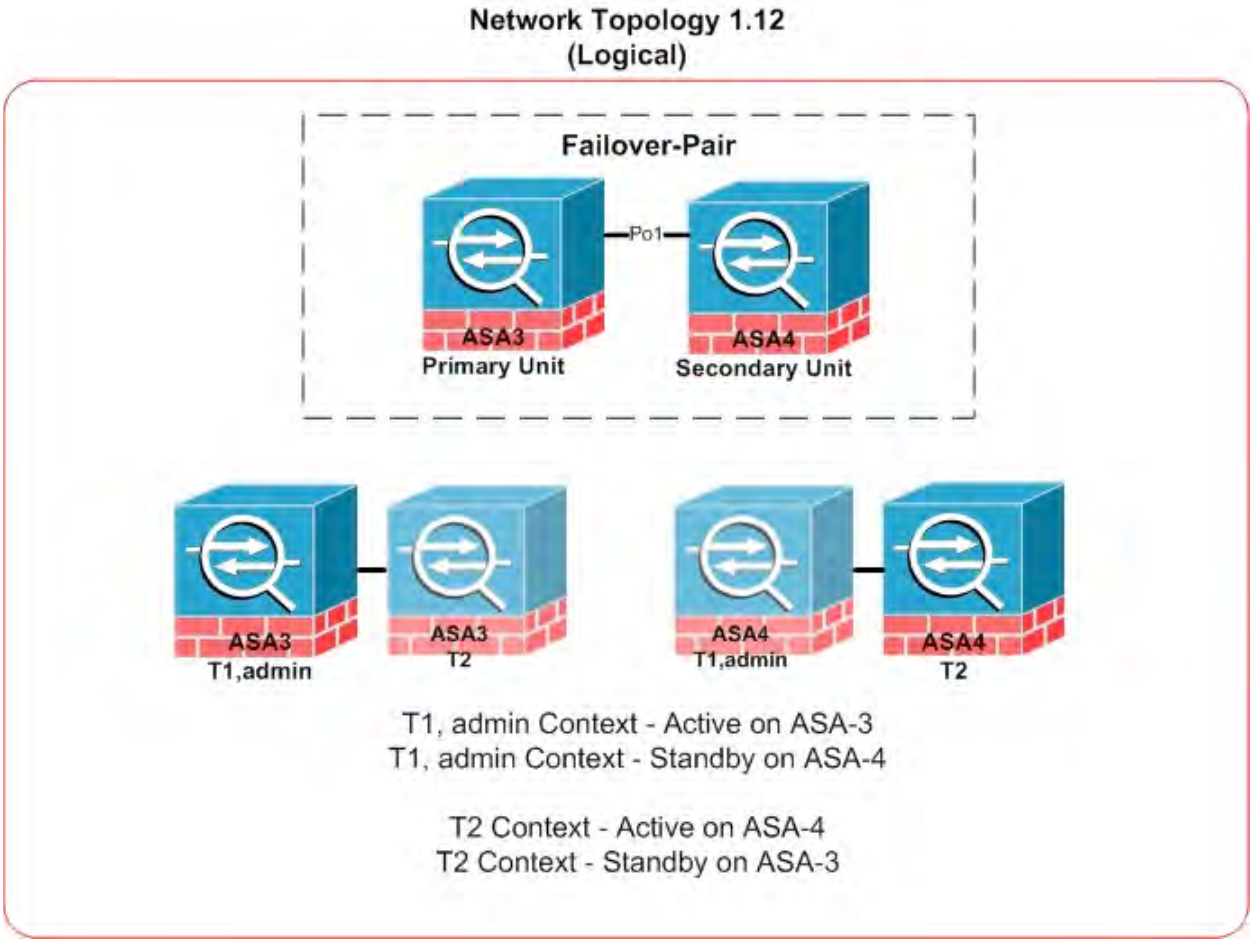
This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.10
(Logical)



Network Topology 1.11
(Logical)





NOTE: *The lighter color/transparent icon of the ASA indicate on that particular ASA the mentioned context is in standby state.*

Detailed Solution:Lab-9

Task 1: Basic VLAN Setup

- Configure the catalyst switches with the appropriate VLAN's for ports and trunks for the firewall as per topology diagram 1.10 and 1.11.

```
(Read the even Task 3 before you configure this)
```

Task-1:Solutions

Step 1: Configure trunk on SW3 & SW4

```
interface GigabitEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,40,50,60,70,80
 switchport mode trunk
```

Verification This can be verified after the ASA has been initialized

Task 2: Firewall Mode on ASA-3

- Change the mode to Multi context transparent mode on ASA-3
- Configure a hostname of "ASA003" on ASA-3
- ASA003 should have a domain name of ipexpert.com
- Un shut all the interfaces

Task-2:Solutions

Step 1: change the mode to multiple and then change the transparent mode and initialize the ASA3. Unshut all the interfaces.

```
mode multi

firewall transparent
hostname ASA003
domain-name ipexpert.com

interface GigabitEthernet0/0
no shut

interface GigabitEthernet0/1
no shut

interface GigabitEthernet0/2
no sh
```

```
interface GigabitEthernet0/3
no sh
```

Task 3: VLAN Sub-interface creation on ASA-3

- Configure VLAN sub-interfaces on ASA3 as per the below parameters

ASA Interface	VLAN
G0/0.10	10
G0/0.20	20
G0/0.40	40
G0/0.50	50
G0/0.60	60
G0/0.70	70
G0/0.80	80

Task-3:Solutions

Step 1: Configure VLAN subniterfaces on ASA3

```
interface GigabitEthernet0/0.10
 vlan 10

interface GigabitEthernet0/0.20
 vlan 20

interface GigabitEthernet0/0.40
 vlan 40

interface GigabitEthernet0/0.50
 vlan 50

interface GigabitEthernet0/0.60
 vlan 60

interface GigabitEthernet0/0.70
 vlan 70

interface GigabitEthernet0/0.80
 vlan 80
```

Verification

Step 1: Verify using show interface command

```
ASA003(config-subif)# sh interface
Interface GigabitEthernet0/0 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
<SNIP>
Interface GigabitEthernet0/0.10 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 10
        Available for allocation to a context
Interface GigabitEthernet0/0.20 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 20
        Available for allocation to a context
Interface GigabitEthernet0/0.40 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 40
        Available for allocation to a context
Interface GigabitEthernet0/0.50 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 50
        Available for allocation to a context
Interface GigabitEthernet0/0.60 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 60
        Available for allocation to a context
Interface GigabitEthernet0/0.70 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 70
        Available for allocation to a context
Interface GigabitEthernet0/0.80 "", is up, line protocol is up
  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 80
        Available for allocation to a context
```

Task 4: Context and failover group creation on ASA-3

- Create contexts as per the below table

Context	Interface Allocation	Configuration file (Flash/Disk0)	Failover Group
admin	M0/0	admin.cfg	1
T1	G0/0.10	T1.cfg	1
	G0/0.20		
	G0/0.40		
	G0/0.50		
	G0/0.60		
T2	G0/0.70	T2.cfg	2
	G0/0.80		

- The failover groups should be configured with pre-emption option. Failover group 2 should be secondary mode on ASA-3. Configure ASA-3 accordingly.
- Limit the resource allocation for T2 context as per the below parameters

Resource	Limits
Connections	5000
Mac-address	500

Task-4:Solutions

Step 1: Configure resource limiting class for the context

```
class T2
  limit-resource mac-addresses 500
  limit-resource Conns 5000
```

Step 2: Configure failover groups with preempt option.

```
failover group 1
  preempt
failover group 2
  secondary
  preempt
```

Step 3: Configure contexts as per the task requirements. Delete any existing .cfg files. “admin” will be the admin context.

```
 delete *.cfg  (on ASA3 and ASA4)

Delete filename [*.cfg]?

Delete disk0:/F1.cfg? [confirm]

Delete disk0:/ADmin.cfg? [confirm]

Delete disk0:/F2.cfg? [confirm]


admin-context admin
context admin
  allocate-interface Management0/0
  config-url disk0:/admin.cfg
  join-failover-group 1
```

```
context T1
  allocate-interface GigabitEthernet0/0.10
  allocate-interface GigabitEthernet0/0.20
  allocate-interface GigabitEthernet0/0.40
  allocate-interface GigabitEthernet0/0.50
  allocate-interface GigabitEthernet0/0.60
  config-url disk0:/T1.cfg
  join-failover-group 1


context T2
  member T2
  allocate-interface GigabitEthernet0/0.70
  allocate-interface GigabitEthernet0/0.80
  config-url disk0:/T2.cfg
  join-failover-group 2
```

Verification

Step 1: Verify context configurations

```
ASA003(config)# sh context detail
Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/0.10,
     GigabitEthernet0/0.20, GigabitEthernet0/0.40,
     GigabitEthernet0/0.50, GigabitEthernet0/0.60,
     GigabitEthernet0/0.70, GigabitEthernet0/0.80, GigabitEthernet0/1,
     GigabitEthernet0/2, GigabitEthernet0/3, GigabitEthernet0/4,
     GigabitEthernet0/5, Internal-Control0/0, Internal-Data0/0,
     Internal-Data0/1, Internal-Data0/2, Management0/0, Virtual254
  Class: default, Flags: 0x00000819, ID: 0

Context "admin", has been created
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: default, Flags: 0x00000813, ID: 1
  Failover group: 1

Context "T1", has been created
  Config URL: disk0:/T1.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/0.20,
     GigabitEthernet0/0.40, GigabitEthernet0/0.50,
     GigabitEthernet0/0.60
  Mapped Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/0.20,
     GigabitEthernet0/0.40, GigabitEthernet0/0.50,
     GigabitEthernet0/0.60
```

```
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: default, Flags: 0x00000811, ID: 2
  Failover group: 1


Context "T2", has been created
  Config URL: disk0:/T2.cfg
  Real Interfaces: GigabitEthernet0/0.70, GigabitEthernet0/0.80
  Mapped Interfaces: GigabitEthernet0/0.70, GigabitEthernet0/0.80
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: T2, Flags: 0x00000811, ID: 3
  Failover group: 2

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Real IPS Sensors:
  Mapped IPS Sensors:
  Class: default, Flags: 0x00000809, ID: 257
```

Task 5: T1 context configuration

- Configure BVI interface 100 with a primary IP address of 192.168.124.100 and standby IP address of 192.168.124.101.
- Configure BVI interface 56 with a primary IP address of 192.168.56.56 and standby IP address of 192.168.56.57.
- Configure T1 context as per the below parameters

ASA Interface	BVI	Security Level	Name
G0/0.40	100	0	outside
G0/0.10	100	100	inside
G0/0.20	100	50	dmz
G0/0.50	56	50	IN
G0/0.60	56	0	OUT

- Configure global ACL to permit any EIGRP traffic
- Configure global ACL to allow RIP traffic between R5 and R6. The ACL should be host specific and should not have 224.0.0.9 in the destination.
- Allow all ICMP traffic in the global ACL
- Ensure routing adjacency is established as per the network diagram

Task-5:Solutions

Step 1: Configure Bridgegroup 100 on ASA3 and all the interface parameters assoctaied with that bridge group

```
changeto context T1
interface BVI100
 ip address 192.168.124.100 255.255.255.0 standby 192.168.124.101

interface GigabitEthernet0/0.20
 nameif dmz
 bridge-group 100
 security-level 50

interface GigabitEthernet0/0.40
 nameif outside
 bridge-group 100
 security-level 0

interface GigabitEthernet0/0.10
 nameif inside
 bridge-group 100
 security-level 100
```

Step 2: Configure Bridgegroup 56 on ASA3 and all the interface parameters assoctaied with that bridge group

```
interface BVI56
 ip address 192.168.56.56 255.255.255.0 standby 192.168.56.57

interface GigabitEthernet0/0.50
 nameif IN
 bridge-group 56
 security-level 100

interface GigabitEthernet0/0.60
 nameif OUT
 bridge-group 56
 security-level 0
```

Step 3: Configure ACL's as per the task

```
access-list GLOBAL extended permit eigrp any any
```

```
access-list GLOBAL extended permit udp host 192.168.56.6 host 192.168.56.5 eq
rip
access-list GLOBAL extended permit udp host 192.168.56.5 host 192.168.56.6 eq
rip
access-list GLOBAL extended permit icmp any any

access-group GLOBAL global
```

Verification

Step 1: Verify Bridge group 100 settings

```
ASA003/T1(config)# sh bridge-group 100
 Interfaces:
 GigabitEthernet0/0.20
 GigabitEthernet0/0.40
 GigabitEthernet0/0.10

 Management System IP Address:  192.168.124.100 255.255.255.0
 Management Current IP Address: 192.168.124.100 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 2
```

Step 2: Verify bridge group 56 configuration

```
ASA003/T1(config-if)# show bridge-group 56
 Interfaces:
 GigabitEthernet0/0.50
 GigabitEthernet0/0.60

 Management System IP Address:  192.168.56.56 255.255.255.0
 Management Current IP Address: 192.168.56.56 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 0
```

Step 3: Verify EIGRP adjacency on R1 and ping to R9 Lo0

```
R1#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(124)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.124.4           Fa0/0             13 00:06:50   12   200  0  145
0   192.168.124.2           Fa0/0             10 00:06:50    4   200  0  146
```

```
R1#ping 9.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Step 4: Verify RIP routes R6 and R6 and ping from R5 and ping to R9 Lo0

```
R5#sh ip ro rip
     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
R       2.2.2.0 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
R       4.4.4.0 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
R    192.168.78.0/24 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
     6.0.0.0/24 is subnetted, 1 subnets
R       6.6.6.0 [120/1] via 192.168.56.6, 00:00:19, FastEthernet0/0
R    192.168.124.0/24 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
     8.0.0.0/32 is subnetted, 1 subnets
R       8.8.8.8 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
     9.0.0.0/32 is subnetted, 1 subnets
R       9.9.9.9 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
     90.0.0.0/24 is subnetted, 1 subnets
R       90.0.0.0 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
R*   0.0.0.0/0 [120/6] via 192.168.56.6, 00:00:19, FastEthernet0/0
R5#ping 9.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Task 6: T2 context configuration

- Configure BVI interface 78 with a primary IP address of 192.168.78.78 and standby IP address of 192.168.78.79.
- Configure T2 context as per the below parameters

ASA Interface	BVI	Security Level	Name
G0/0.80	78	0	outside
G0/0.70	78	100	inside

- Configure interface specific ACL's to allow OSPF traffic. ACL's should be as specific as possible. Do not use any global ACL's.
- Allow ICMP traffic to pass through in the ACL's. Do not use global ACL's.
- Ensure routing adjacency is established as per the network diagram
- Ensure you are able to accomplish the below from R7.

```
R7#ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 5.5.5.5 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 2.2.2.2 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task-6:Solutions

Step 1: Configure BVI 78 bridge group and the appropriate interface specific parameters on ASA4 which is active for T2 context as per task.

```
changeto context T2
hostname T2

interface BVI78
 ip address 192.168.78.78 255.255.255.0 standby 192.168.78.79

interface GigabitEthernet0/0.70
 nameif inside
 bridge-group 78
```

```
 security-level 100

interface GigabitEthernet0/0.80
 nameif outside
 bridge-group 78
 security-level 0
```

Step 2: ACL's to allow OSPF and ICMP traffic as stated in the task

```
access-list IN extended permit ospf host 192.168.78.7 host 224.0.0.5
access-list IN extended permit ospf host 192.168.78.7 host 192.168.78.8
access-list IN extended permit icmp any any

access-list OUT extended permit ospf host 192.168.78.8 host 224.0.0.5
access-list OUT extended permit ospf host 192.168.78.8 host 192.168.78.7
access-list OUT extended permit icmp any any
access-group IN in interface inside
access-group OUT in interface outside
```

Verification

Step 1: Verify the bridge group configuration on ASA4

```
ASA003/T2(config)# sh bridge-group
Static mac-address entries:  0 (in use), 500 (max)
Dynamic mac-address entries: 2 (in use), 500 (max)

 Bridge Group: 78
 Interfaces:
 GigabitEthernet0/0.70
 GigabitEthernet0/0.80

 Management System IP Address:  192.168.78.78 255.255.255.0
 Management Current IP Address: 192.168.78.78 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 2
```

Step 2: Verify OSPF routes and adjacency on R7

```
R7#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.78.8 to network 0.0.0.0

     1.0.0.0/24 is subnetted, 1 subnets
O E2    1.1.1.0 [110/20] via 192.168.78.8, 00:03:01, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
O E2    2.2.2.0 [110/20] via 192.168.78.8, 00:03:01, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
O E2    4.4.4.0 [110/20] via 192.168.78.8, 00:03:01, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
O E2    5.5.5.0 [110/20] via 192.168.78.8, 00:03:01, FastEthernet0/0
C    192.168.78.0/24 is directly connected, FastEthernet0/0
     6.0.0.0/24 is subnetted, 1 subnets
O E2    6.6.6.0 [110/20] via 192.168.78.8, 00:03:02, FastEthernet0/0
O E2 192.168.56.0/24 [110/20] via 192.168.78.8, 00:03:02, FastEthernet0/0
O E2 192.168.124.0/24 [110/20] via 192.168.78.8, 00:03:02, FastEthernet0/0
     7.0.0.0/24 is subnetted, 1 subnets
C       7.7.7.0 is directly connected, Loopback0
     8.0.0.0/32 is subnetted, 1 subnets
O       8.8.8.8 [110/2] via 192.168.78.8, 00:03:02, FastEthernet0/0
     9.0.0.0/32 is subnetted, 1 subnets
O       9.9.9.9 [110/3] via 192.168.78.8, 00:03:02, FastEthernet0/0
     90.0.0.0/24 is subnetted, 1 subnets
O       90.0.0.0 [110/2] via 192.168.78.8, 00:03:02, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.78.8, 00:01:32, FastEthernet0/0
```

```
R7#sh ip ospf ne

Neighbor ID     Pri   State           Dead Time   Address         Interface
8.8.8.8           0   FULL/  -        00:00:36    192.168.78.8    FastEthernet0/0
```

Step 3: Perform ping test as per task from R7 Lo0

```
R7# ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 5.5.5.5 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 2.2.2.2 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 7: Failover Configuration

- Configure Failover – use G0/1 as a failover link. Use VLAN 100
- Change the mode to Transparent Multi-mode on ASA-4
- Configure ASA-3 and ASA-4 for Active/Active failover. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the below parameters for the failover configuration. Share G0/1 for stateful link failover.

Failover interface – G0/1
Primary IP – 30.1.1.1/24
Standby IP – 30.1.1.2/24
Interface Name - FA1LOVER
Key - C1SCO

Task-7:Solutions

Step 1: Bring the failover pot up on ASA3 and ASA4

ASA3 and ASA4

```
interface GigabitEthernet0/1
 no sh
```

Step 2: Configure the switches

SW3 and SW4

```
interface GigabitEthernet1/0/20
 switchport access vlan 100
 switchport mode access
```

Step 3: Configure failover as per task.

ASA3

```
failover lan unit primary
```

```
failover lan interface FA1LOVER G0/1
failover key C1SCO
failover link FA1LOVER G0/1
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
failover
```

ASA4

```
failover lan unit secondary
failover lan interface FA1LOVER G0/1
failover key C1SCO
failover interface ip FA1LOVER 30.1.1.1 255.255.255.0 standby 30.1.1.2
failover
```

Verification

Step 1: Verify failover on ASA3

```
ASA003(config)#  sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FA1LOVER GigabitEthernet0/1 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Group 1 last failover at: 14:30:13 UTC Jan 24 2014
Group 2 last failover at: 14:30:11 UTC Jan 24 2014

  This host:    Primary
  Group 1       State:          Active
                Active time:    493 (sec)
  Group 2       State:          Standby Ready
                Active time:    242 (sec)

                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  T1   Interface   inside   (192.168.124.100):   Normal   (Not-
Monitored)
                  T1 Interface dmz (192.168.124.100): Normal (Not-Monitored)
                  T1   Interface   outside   (192.168.124.100):   Normal   (Not-
Monitored)
                  T1 Interface IN (192.168.56.56): Normal (Not-Monitored)
                  T1 Interface OUT (192.168.56.56): Normal (Not-Monitored)
                  T2 Interface inside (192.168.78.79): Normal (Not-Monitored)
                  T2   Interface   outside   (192.168.78.79):   Normal   (Not-
Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up
```

```
  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    371 (sec)
  Group 2       State:          Active
                Active time:    639 (sec)

                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  T1   Interface   inside   (192.168.124.101):   Normal   (Not-
Monitored)
                  T1 Interface dmz (192.168.124.101): Normal (Not-Monitored)
                  T1   Interface   outside   (192.168.124.101):   Normal   (Not-
Monitored)
                  T1 Interface IN (192.168.56.57): Normal (Not-Monitored)
                  T1 Interface OUT (192.168.56.57): Normal (Not-Monitored)
                  T2 Interface inside (192.168.78.78): Normal (Not-Monitored)
                  T2   Interface   outside   (192.168.78.78):   Normal   (Not-
Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/1 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         49         0          30         0
        sys cmd         27         0          27         0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        14         0          0          0
        ARP tbl         1          0          0          0
        L2BRIDGE Tbl    5          0          2          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          0          0
        User-Identity   2          0          1          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       30
        Xmit Q:         0       1       49

ASA003(config)# sh failover group ?

exec mode commands/options:
  <1-2>  Failover group number
ASA003(config)# sh failover group 1
```

```
  Last Failover at: 14:30:13 UTC Jan 24 2014

  This host:    Primary
                State:          Active
                Active time:    540 (sec)

                T1 Interface inside (192.168.124.100): Normal (Not-Monitored)
                T1 Interface dmz (192.168.124.100): Normal (Not-Monitored)
                T1   Interface   outside   (192.168.124.100):   Normal   (Not-
Monitored)
                T1 Interface IN (192.168.56.56): Normal (Not-Monitored)
                T1 Interface OUT (192.168.56.56): Normal (Not-Monitored)


  Other host:   Secondary
                State:          Standby Ready
                Active time:    371 (sec)

                T1 Interface inside (192.168.124.101): Normal (Not-Monitored)
                T1 Interface dmz (192.168.124.101): Normal (Not-Monitored)
                T1   Interface   outside   (192.168.124.101):   Normal   (Not-
Monitored)
                T1 Interface IN (192.168.56.57): Normal (Not-Monitored)
                T1 Interface OUT (192.168.56.57): Normal (Not-Monitored)

  Stateful Failover Logical Update Statistics
        Status: Configured.
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        17         0          0          0
        ARP tbl         1          0          0          0
        L2BRIDGE Tbl    5          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          0          0
        User-Identity   2          0          0          0
```

Lab 10: Routed Mode IPv6 on ASA

Lab 10: Routed Mode IPv6 on ASA – This lab is intended to let you be familiar with configuring ASA using IPv6 and IPv4 dual stack. Although 8.6 has limited featured when compared with Version 9.0 of the ASA, it is necessary to be familiar with configuring ASA using IPv6 protocol. This section will focus on interface addressing, ACL's, Filters, Failover and MPF.

General Rules

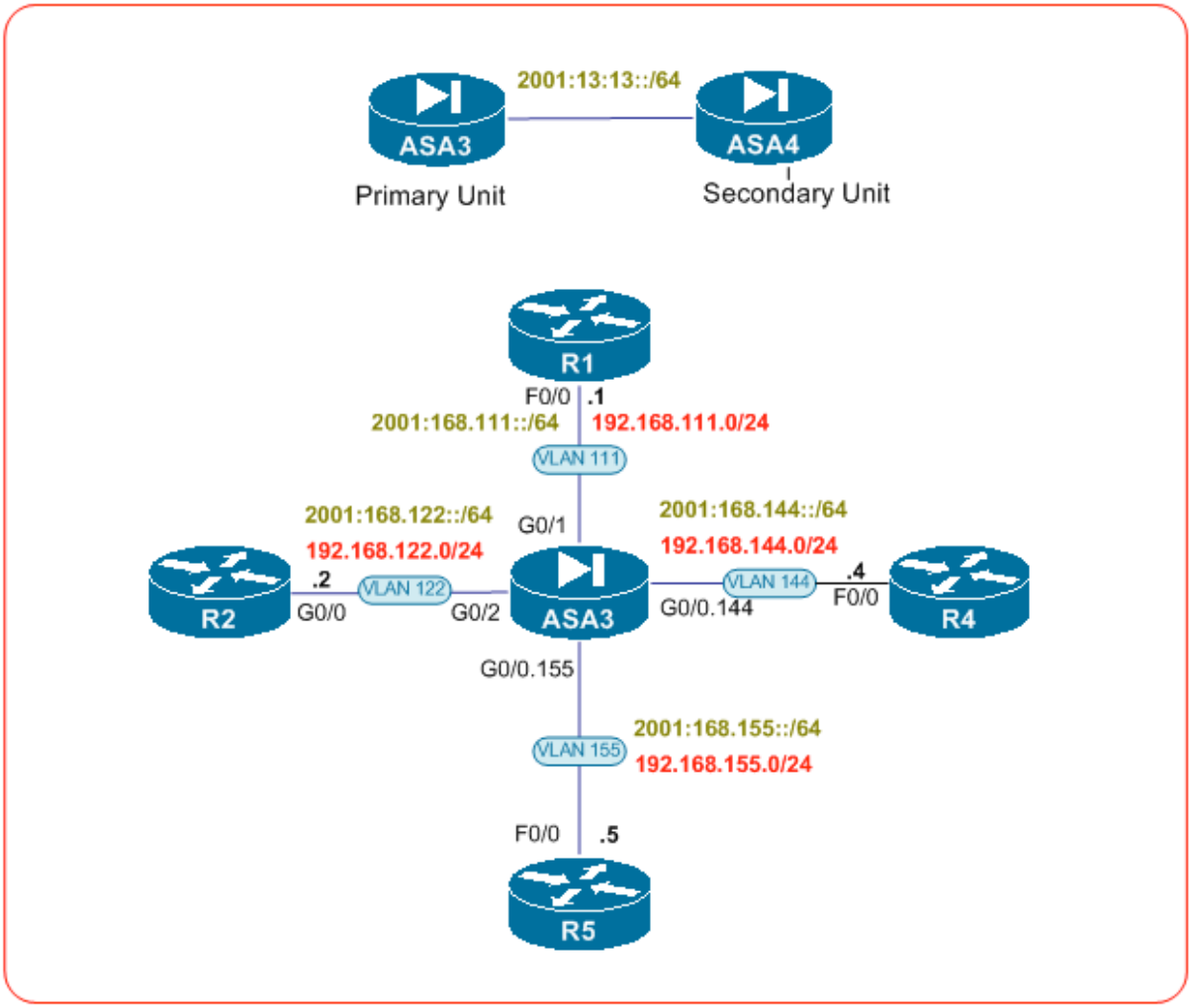
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 2 Hours

Pre-setup

Load the initial configuration for Lab 10. Routers are pre-configured with routing. Use the logical topology drawing - Network Topology 1.13. Double-check the loaded pre-configuration before starting the Lab. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.13 (Logical)



Detailed Solution:Lab-10

Task 1: Initialization of ASA-3

- Configure a hostname of "ASA-003fw" on ASA-3.
- ASA-003fw should have a domain name of ipexpert.com.
- Configure ASA-003fw interfaces. Ensure that you can ping your directly connected neighbors.
- Suppress IPv6 router advertisements on the outside interface.

ASA Interface	VLAN Tag	Security Level	Name	IPv4 Address Active and Standby IP	IPv6 Address Active and Standby IP
G0/1	-------	100	Inside	192.168.111.10 192.168.111.11	2001:168:111::10/64 2001:168:111::11/64
G0/2	------	20	dmz2	192.168.122.10 192.168.122.11	2001:168:122::10/64 2001:168:122::11/64
G0/0.144	144	40	dmz4	192.168.144.10 192.168.144.11	2001:168:144::10/64 2001:168:144::11/64
G0/0.155	155	0	outside	192.168.155.10 192.168.155.11	2001:168:155::10/64 2001:168:155::11/64

Task-1:Solutions

Step 1: Initialize ASA3 and configure interfaces as per task

```
hostname ASA-3
domain-name ipexpert.com

interface GigabitEthernet0/0
 no nameif
 no security-level
 no ip address
 no shutdown

interface GigabitEthernet0/0.144
 vlan 144
 nameif dmz4
 security-level 50
 ip address 192.168.144.10 255.255.255.0 standby 192.168.144.1
 ipv6 address 2001:168:144::10/64 standby 2001:168:144::11

interface GigabitEthernet0/0.155
 vlan 155
 nameif outside
```

```
 security-level 0
 ip address 192.168.155.10 255.255.255.0 standby 192.168.155.11
 ipv6 address 2001:168:155::10/64 standby 2001:168:155::11
 ipv6 nd suppress-ra

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.111.10 255.255.255.0 standby 192.168.111.11
 ipv6 address 2001:168:111::10/64 standby 2001:168:111::11
 no shutdown

interface GigabitEthernet0/2
 nameif dmz2
 security-level 20
 ip address 192.168.122.10 255.255.255.0 standby 192.168.122.11
 ipv6 address 2001:168:122::10/64 standby 2001:168:122::11
 no shutdown
```

Verification

Step 1: Verify VLAN assignment and trunks on SW3

```
SW3#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
--
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/22
111  VLAN0111                         active    Gi1/0/20
122  VLAN0122                         active    Gi1/0/21
<SNIP>
```

```
SW3#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/15    on               802.1q         trunking      1
Gi1/0/16    on               802.1q         trunking      1
Gi1/0/17    on               802.1q         trunking      1
Gi1/0/18    on               802.1q         trunking      1
Gi1/0/19    on               802.1q         trunking      1
Gi1/0/23    on               802.1q         trunking      1
Gi1/0/24    on               802.1q         trunking      1

Port        Vlans allowed on trunk
```

```
<SNIP>
Gi1/0/19    144,155
<SNIP>

Port        Vlans allowed and active in management domain
<SNIP>
Gi1/0/19    144,155
<SNIP>

Port        Vlans in spanning tree forwarding state and not pruned
<SNIP>
Gi1/0/19    144,155
<SNIP>
```

Step 2: Verify interface configurations

```
ASA-3(config)# sh int ip br | e una
Interface                              IP-Address      OK? Method  Status
Protocol
GigabitEthernet0/0.144                 192.168.144.10  YES    manual    up
up
GigabitEthernet0/0.155                 192.168.155.10  YES    manual    up
up
GigabitEthernet0/1                        192.168.111.10      YES   manual   up
up
GigabitEthernet0/2                        192.168.122.10      YES   manual   up
up
Internal-Control0/0        127.0.1.1       YES unset  up


ASA-3(config)# sh ipv6 interface brief
GigabitEthernet0/0 [up/up]
    unassigned
dmz4 [up/up]
    fe80::e22f:6dff:febb:fcb7
    2001:168:144::10
outside [up/up]
    fe80::e22f:6dff:febb:fcb7
    2001:168:155::10
inside [up/up]
    fe80::e22f:6dff:febb:fcb4
    2001:168:111::10
dmz2 [up/up]
    fe80::e22f:6dff:febb:fcb8
    2001:168:122::10
GigabitEthernet0/3 [administratively down/down]
    unassigned
GigabitEthernet0/4 [administratively down/down]
    unassigned
```

```
GigabitEthernet0/5 [administratively down/down]
    unassigned
Management0/0 [administratively down/down]
    unassigned

ASA-3(config)# ping 192.168.144.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.144.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA-3(config)# ping 192.168.155.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.155.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA-3(config)# ping 192.168.122.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASA-3(config)# ping 2001:168:111::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:168:111::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA-3(config)# ping 2001:168:122::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:168:122::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Task 2: Routing on ASA-3

- Configure OSPF on all the interfaces using a single network statement.
- Configure an IPv6 static default route towards R5.
- Configure IPv6 static routes for all the loopback in dmzs and inside networks.

Task-2:Solutions

Step 1: Configure IPv6 routes as per task

```
ipv6 route inside 2001:1:1::/64 2001:168:111::1
ipv6 route dmz2 2001:2:2::2/128 2001:168:122::2
ipv6 route dmz4 2001:4:4::4/128 2001:168:144::4
ipv6 route outside ::/0 2001:168:155::5
```

Step 2: Configure OSPF as per task

```
router ospf 1
 network 0.0.0.0 0.0.0.0 area 0
```

Verification

Step 1: Verify OSPF adjacency and routes on ASA3

```
ASA-3(config)# sh ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/DR         0:00:39     192.168.144.4   dmz4
5.5.5.5           1   FULL/DR         0:00:39     192.168.155.5   outside
1.1.1.1           1   FULL/DR         0:00:39     192.168.111.1   inside
2.2.2.2           1   FULL/DR         0:00:39     192.168.122.2   dmz2
```

```
ASA-3(config)# sh ipv6 route

IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static
S   2001:1:1::/64 [0/0]
     via 2001:168:111::1, inside
S   2001:2:2::2/128 [0/0]
     via 2001:168:122::2, dmz2
S   2001:4:4::4/128 [0/0]
     via 2001:168:144::4, dmz4
L   2001:168:111::10/128 [0/0]
     via ::, inside
C   2001:168:111::/64 [0/0]
     via ::, inside
L   2001:168:122::10/128 [0/0]
     via ::, dmz2
C   2001:168:122::/64 [0/0]
     via ::, dmz2
L   2001:168:144::10/128 [0/0]
     via ::, dmz4
C   2001:168:144::/64 [0/0]
     via ::, dmz4
L   2001:168:155::10/128 [0/0]
     via ::, outside
C   2001:168:155::/64 [0/0]
     via ::, outside
L   fe80::/10 [0/0]
     via ::, dmz4
     via ::, outside
     via ::, inside
     via ::, dmz2
L   ff00::/8 [0/0]
```

```
     via ::, dmz4
     via ::, outside
     via ::, inside
     via ::, dmz2
S    ::/0 [0/0]
     via 2001:168:155::5, outside
```

```
ASA-3(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.122.0 255.255.255.0 is directly connected, dmz2
O    1.1.1.1 255.255.255.255 [110/11] via 192.168.111.1, 0:09:22, inside
O    2.2.2.2 255.255.255.255 [110/11] via 192.168.122.2, 0:09:22, dmz2
O    4.4.4.4 255.255.255.255 [110/11] via 192.168.144.4, 0:09:22, dmz4
O    5.5.5.5 255.255.255.255 [110/11] via 192.168.155.5, 0:09:22, outside
C    192.168.111.0 255.255.255.0 is directly connected, inside
C    192.168.144.0 255.255.255.0 is directly connected, dmz4
C    192.168.155.0 255.255.255.0 is directly connected, outside
```

Task 3: IPv6 and IPv4 filters on ASA-3

- Configure global ACLs to allow all ICMP traffic for IPv4 and IPv6 traffic.
- Configure interface specific ACLs on the outside to allow Telnet traffic to R2 Lo0, SSH traffic to R4 Lo0, and HTTP traffic to R1 Lo0. This should apply both for IPv4 and IPv6 traffic.
- No one should be able to ping the outside interface using IPv6

Task-3:Solutions

Step 1: Configure Global IPv6 and IPv4 ACL's to allow ICMP and apply them.

```
ipv6 access-list GLOBAL6 permit icmp6 any any
access-list GLOBAL4 extended permit icmp any any

access-group GLOBAL4 global
access-group GLOBAL6 global
```

Step 2: Configure IPv6 ACL's as per task and apply them to the outside interface

```
ipv6 access-list outv6 permit tcp any host 2001:1:1::1 eq www
ipv6 access-list outv6 permit tcp any host 2001:2:2::2 eq telnet
ipv6 access-list outv6 permit tcp any host 2001:4:4::4 eq ssh
access-group outv6 in interface outside
```

Step 3: Configure IPv4 ACL's as per task and apply them to the outside interface

```
access-list out extended permit tcp any host 1.1.1.1 eq www
access-list out extended permit tcp any host 2.2.2.2 eq telnet
access-list out extended permit tcp any host 4.4.4.4 eq ssh
access-group out in interface outside
```

Verification

Step 1: Ping from R5 and telnet to R2 lo0.

```
R5#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms



R5#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R5#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#ping 2001:1:1::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R5#ping 2001:2:2::2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:2:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms

R5#ping 2001:4:4::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4:4::4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms


R5#ping 2001:4:4::4 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4:4::4, timeout is 2 seconds:
Packet sent with a source address of 2001:5:5::5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

```
R5#telnet 2001:2:2::2
Trying 2001:2:2::2 ... Open

R2#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:16
*578 vty 0                 idle                 00:00:00 2001:168:155::5

R5#telnet 2.2.2.2
Trying 2.2.2.2 ... Open

R2#show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:27
*578 vty 0                 idle                 00:00:00 192.168.155.5
```

Task 4: IPv6 Management access to ASA-3

- Configure a username of cisco and password of cisco123.
- Allow SSH access from IPv6 outside subnet. Authenticate using local AAA
- Allow telnet access from IPv6 inside subnet. Authenticate using local AAA

Task-4:Solutions

Step 1: Configure local Username and password also configure telnet and SSH authentication using the local user database

```
username cisco password cisco123
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
```

Step 2: Allow telnet and SSH access

```
crypto key generate rsa
telnet 2001:1:1::1/128 inside
ssh 2001:5:5::5/128 outside
```

Verification

Step 1: Telnet from R1 to ASA3

```
R1#telnet 2001:168:111::10 /source-interface lo0
Trying 2001:168:111::10 ... Open

User Access Verification

Username: cisco
Password: ********
Type help or '?' for a list of available commands.
ASA-3> en
Password: ********
ASA-3# exit

Logoff

[Connection to 2001:168:111::10 closed by foreign host]
```

Task 5: Configure IPv6 Active/Standby Failover

- Configure ASA-3 and ASA-4 for device level HA using failover feature on ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the parameters below for the failover configuration. Configure Switch such that G0/3 interface of the firewall should be in VLAN 999. Enable stateful failover on the same interface G0/3.

Failover interface – G0/3
Primary IP – 2001:13:13::10/64
Standby IP – 2001:13:13::11/64
Interface Name - FA1LOVER
Key - C1SCO

Task-5:Solutions

Step 1: Configure the switches

CAT4

```
vlan 999

interface GigabitEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 144,155
 switchport mode trunk
!
interface GigabitEthernet1/0/20
 switchport access vlan 111
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/21
 switchport access vlan 122
 switchport mode access
 spanning-tree portfast
```

CAT3, CAT4

```
interface GigabitEthernet1/0/22
 switchport access vlan 999
 switchport mode access
 spanning-tree portfast
```

Step 2: Configure Failover

```
ASA3 (Primary Unit)

int GigabitEthernet 0/3
 no shut

failover lan unit primary
failover lan interface FA1LOVER GigabitEthernet0/3
failover key C1SCO
failover link FA1LOVER GigabitEthernet0/3
failover interface ip FA1LOVER 2001:13:13::10/64 standby 2001:13:13::11
failover

ASA4 (Secondary  Unit)

int GigabitEthernet 0/3
 no shut

failover lan unit secondary
failover lan interface FA1LOVER GigabitEthernet0/3
```

```
failover key C1SCO
failover interface ip FA1LOVER 2001:13:13::10/64 standby 2001:13:13::11
failover
```

Verification

Step 1: Verify failover

```
ASA-3(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FA1LOVER GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 10:17:18 UTC Apr 6 2013
        This host: Primary - Active
                Active time: 105 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface   dmz4   (192.168.144.10/fe80::e22f:6dff:febb:fcb7):  Normal
(Not-Monitored)
                  Interface outside  (192.168.155.10/fe80::e22f:6dff:febb:fcb7): Normal
(Not-Monitored)
                  Interface  inside  (192.168.111.10/fe80::e22f:6dff:febb:fcb4):  Normal
(Waiting)
                  Interface   dmz2   (192.168.122.10/fe80::e22f:6dff:febb:fcb8):  Normal
(Waiting)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface   dmz4   (192.168.144.1/fe80::e22f:6dff:febb:f76e):   Normal
(Not-Monitored)
                  Interface outside  (192.168.155.11/fe80::e22f:6dff:febb:f76e): Normal
(Not-Monitored)
                  Interface  inside  (192.168.111.11/fe80::e22f:6dff:febb:f76b):  Normal
(Waiting)
                  Interface   dmz2   (192.168.122.11/fe80::e22f:6dff:febb:f76f):  Normal
(Waiting)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         15         0          6          0
        sys cmd         6          0          6          0
        up time         0          0          0          0
        RPC services    0          0          0          0
```

```
        TCP conn          0          0          0          0
        UDP conn          0          0          0          0
        ARP tbl           4          0          0          0
        Xlate_Timeout     0          0          0          0
        IPv6 ND tbl       0          0          0          0
        VPN IKEv1 SA      0          0          0          0
        VPN IKEv1 P2      0          0          0          0
        VPN IKEv2 SA      0          0          0          0
        VPN IKEv2 P2      0          0          0          0
        VPN CTCP upd      0          0          0          0
        VPN SDI upd       0          0          0          0
        VPN DHCP upd      0          0          0          0
        SIP Session       0          0          0          0
        Route Session     4          0          0          0
        User-Identity     1          0          0          0

        Logical Update Queue Information
                          Cur     Max     Total
        Recv Q:           0       6       6
        Xmit Q:           0       30      88
```

ASA4

```
ASA-3# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: FA1LOVER GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 07:42:05 UTC Apr 4 2013
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface   dmz4   (192.168.144.1/fe80::e22f:6dff:febb:f76e):   Normal
(Not-Monitored)
                  Interface outside  (192.168.155.11/fe80::e22f:6dff:febb:f76e): Normal
(Not-Monitored)
                  Interface  inside  (192.168.111.11/fe80::e22f:6dff:febb:f76b):  Normal
(Waiting)
                  Interface   dmz2   (192.168.122.11/fe80::e22f:6dff:febb:f76f):   Normal
(Waiting)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Other host: Primary - Active
                Active time: 301 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface   dmz4   (192.168.144.10/fe80::e22f:6dff:febb:fcb7):   Normal
(Not-Monitored)
                  Interface outside  (192.168.155.10/fe80::e22f:6dff:febb:fcb7): Normal
(Not-Monitored)
```

```
                  Interface  inside  (192.168.111.10/fe80::e22f:6dff:febb:fcb4):  Normal
(Waiting)
                  Interface   dmz2   (192.168.122.10/fe80::e22f:6dff:febb:fcb8):   Normal
(Waiting)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : FA1LOVER GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         32         0          72         0
        sys cmd         32         0          32         0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          35         0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0
        Route Session   0          0          4          0
        User-Identity   0          0          1          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       7       378
        Xmit Q:         0       1       32
```

Task 6: IPv6 inspection using MPF

- Drop all fragments in the header extension using MPF. Apply this in the default policy map under the inspection_default class.

Task-6:Solutions

Step 1: Configure IPv6 Inspection policy map and apply in the global policy

```
policy-map type inspect ipv6 IPV6
 parameters
 match header fragment
  drop log
```

```
policy-map global_policy
 class inspection_default
  inspect ipv6 IPV6
```

Verification

Step 1: Verify IPv6 Inspection

```
ASA-3(config)# show service-policy inspect ipv6

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ipv6 IPV6, packet 0, lock fail 0, drop 0, reset-drop 0
        params verify-header type fails 0
        params verify-header order fails 0
        match header fragment
          drop log, packet 0
        match header routing-type
          drop, packet 0
          log, packet 0
```

Lab 11: Transparent Mode using IPv6

Lab-11: Transparent Mode IPv6 on ASA– This lab is intended to let you be familiar with configuring ASA using IPv6 and IPv4 dual stack. Although 8.6 has limited featured when compared with Version 9.0 of the ASA, it is necessary to be familiar with configuring ASA using IPv6 protocol for transparent mode on 8.6 version of the ASA.

General Rules

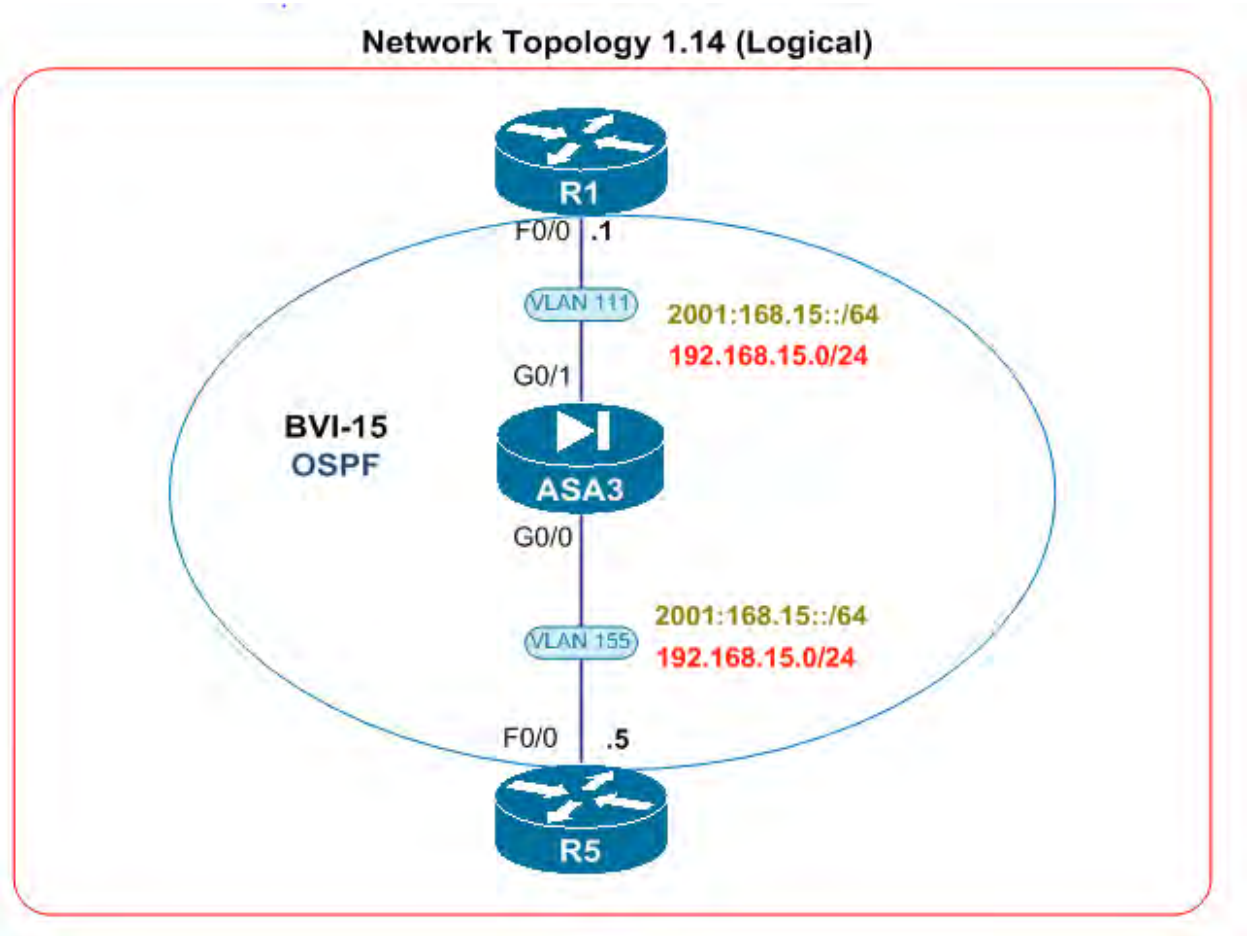
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 1 Hour

Pre-setup

Load the initial configuration for Lab 11. Routers are pre-configured with routing. Use the logical topology drawing - Network Topology 1.14. Double-check the loaded pre-configuration before starting the Lab.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.



Detailed Solution:Lab-11

Task 1: Basic Initialization ASA-3

- Configure a hostname of "FwtASA3" on ASA-3.
- FwtASA3 should have a domain name of ipexpert.com.
- Configure FwtASA3 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	Bridge Group	VLAN	Security Level	Name
G0/0	15	115	100	inside
G0/1	15	111	0	outside

- Configure a BVI 15 address of 192.168.15.10/24 and 2001:168:15::10/64.

Task-1:Solutions

Step 1: Initialize ASA3 as per task. Change the mode to transparent on ASA3 and configure bridge groups.

```
firewall transparent
hostname ASA3

interface BVI15
 ip address 192.168.15.10 255.255.255.0
 ipv6 address 2001:168:15::10/64

interface GigabitEthernet0/0
 nameif outside
 bridge-group 15
 security-level 0
 no sh

interface GigabitEthernet0/1
 nameif inside
 bridge-group 15
 security-level 100
 no sh
```

Verification

Step 1: Verify bridge group configuration

```
ASA3(config)# show bridge-group
Static mac-address entries:  0 (in use), 65535 (max)
Dynamic mac-address entries: 4 (in use), 65535 (max)

 Bridge Group: 15
 Interfaces:
 GigabitEthernet0/0
 GigabitEthernet0/1

 Management System IP Address:  192.168.15.10 255.255.255.0
 Management Current IP Address: 192.168.15.10 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2001:168:15::10/64
 Static mac-address entries:  0
 Dynamic mac-address entries: 4
```

Task 2: IPv4 and IPv6 ACLs

- Configure global ACLs to allow OSPF adjacency to occur between R1 and R5.

Task-2:Solutions

Step 1: Configure IPv4 and IPv6 ACL's as per task and make sure R4 and R5 establish OSPFv2 and OSPFv3 adjacency.

```
ipv6 access-list GLOBAL_6 permit ospf any any
ipv6 access-list GLOBAL_6 permit icmp6 any any

access-list GLOBAL_4 extended permit ospf any any

access-group GLOBAL_4 global
access-group GLOBAL_6 global
```

Verification

Step 1: Verify OSPFv2 and OSPFv3 adjacency on R4/R5

```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.155.5     1   FULL/DR         00:00:39    192.168.15.5    FastEthernet0/0

R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
5.5.5.5           1   FULL/DR         00:00:35    4               FastEthernet0/0



R5#sh ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           1   FULL/BDR        00:00:30    3               FastEthernet0/0

R5#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:33    192.168.15.1    FastEthernet0/0
```

Section 2
IOS Firewall

Section 2: IOS Firewall is intended to let you be familiar with the NAT & firewall technologies that are available on IOS. You will be configuring Network Address Translations, Access-Lists, Zone Based Firewall and other filtering technologies along with some advanced features related to those.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on the IOS Firewall feature set. You will need to pre-configure the network with the base configuration files

NOTE: *Static/default routes are NOT allowed unless otherwise stated in the task*

NOTE: *ICMP and ICMPv6 traffic can be allowed everywhere unless otherwise stated*

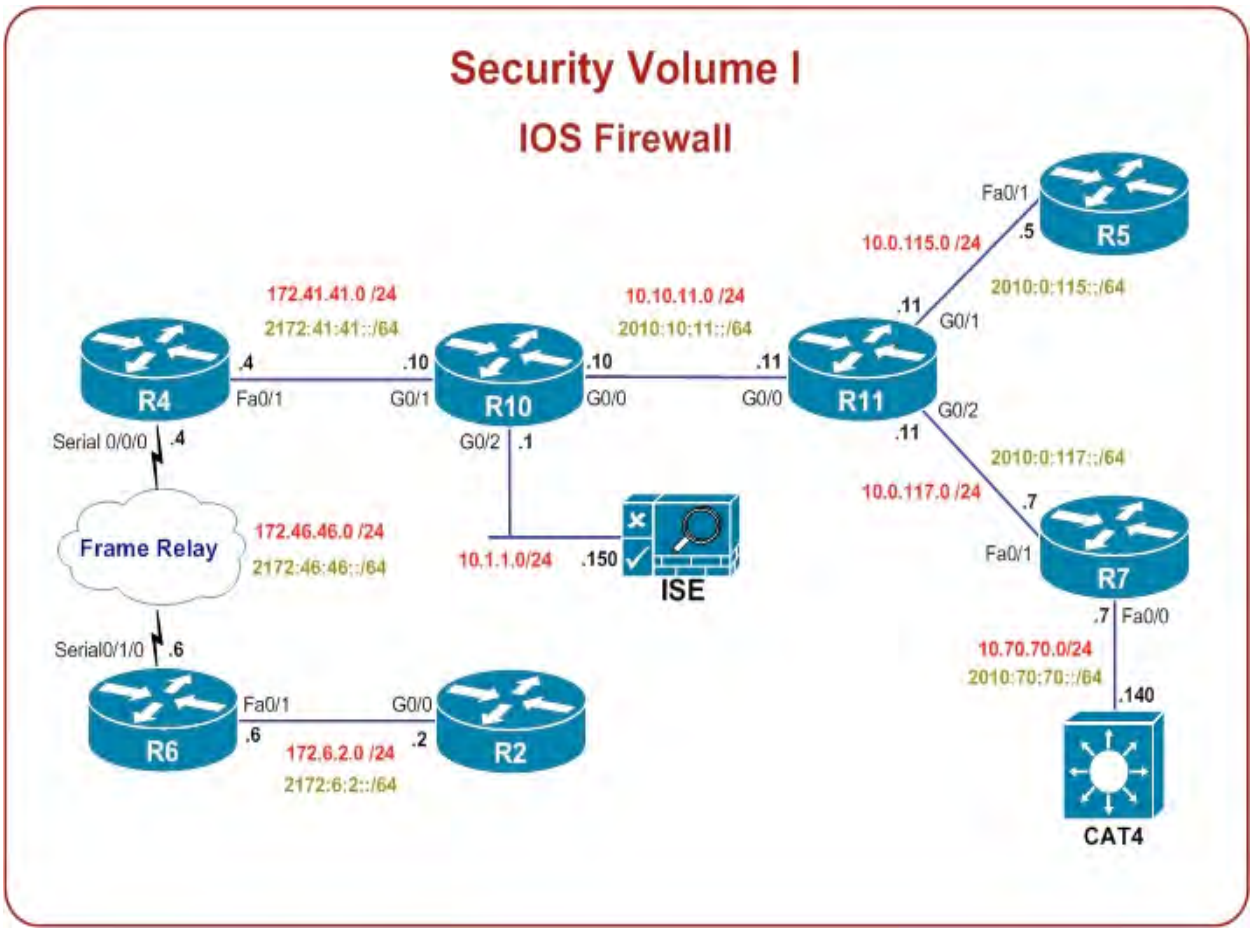
Estimated Time to Complete: **5 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R2	G0/0	62	172.6.2.2/24 2172:6:2::2/64
	Loop0		2.2.2.2/24 2::2/64
R4	F0/1	41	172.41.41.4/24 2172:41:41::4/64
	S0/0/0		172.46.46.0/24 2172:46:46::4/64
	Loop0		4.4.4.4/24 4::4/64
R5	F0/1	115	10.0.115.5/24 2010:0:115::5/64
	Loop0		5.5.5.5/24 5::5/64
R6	F0/1	62	172.6.2.6/24 2172:6:2::6/64
	S0/1/0		172.46.46.6/24 2172:46:46::6/64
	Loop0		6.6.6.6/24 6::6/64
R7	F0/0	70	10.70.70.7/24
	F0/1	117	10.0.117.7/24 2010:0:117::7/64
	Loop0		7.7.7.7/24 7::7/64
R10	G0/2	100	10.1.1.1/24
	G0/1	41	172.41.41.10/24 2172:41:41::10/64
	G0/0	101	10.10.11.10/24 2010:10:11::10/64
	Loop0		100.100.100.10/24 10::10/64
R11	G0/0	101	10.10.11.11/24 2010:10:11::11/64

	G0/1	115	10.0.115.11/24 2010:0:115::11/64
	G0/2	117	10.0.117.11/24 2010:0:117::11/64
	Loop0		11.11.11.11/24 11::11/64



Solutions

Task 1: IOS NAT

- Configure R11 to NAT R7's F0/1 to 10.10.11.7
- Configure a pool using 10.10.11.60 – 10.10.11.80 for the rest of the devices in VLAN 117
- R5's F0/1 should be translated to 10.10.11.50 if attempting to connect to R10's loop0
- For any other destinations the translated address should be 10.10.11.5
- Outside to Inside traffic should be allowed but only to the respective addresses
- Allow the rest of the IPs in VLAN 115 to be translated to R11's G0/0
- Configure R11 to keep these translations for ICMP traffic for 3 seconds, UDP for 60 seconds and TCP for 40 seconds
- If a TCP packet does not complete communication for either FIN or SYN state R11 should remove the translation after 20 seconds
- Enable NAT on R10. Don't specify "inside" or "outside" domains
- Configure R10 to translate all VLAN 101 addresses to a pool 172.99.99.60 – 172.99.99.80
- If the addresses are exhausted allow for PAT
- As a result VLAN 101 devices should be able to communicate with public networks
- Limit the maximum number of NAT translations for any given host on R10 to 25
- Log R11's translations to the Syslog server 10.10.11.100

Detailed Solution

R11

```
ip access-list extended R5_TO_R10LOOP
 permit ip host 10.0.115.5 host 100.100.100.10

ip access-list extended R5_TO_REST
 deny   ip host 10.0.115.5 host 100.100.100.10
 permit ip host 10.0.115.5 any

ip access-list extended VLAN115
 deny   ip host 10.0.115.5 any
 permit ip 10.0.115.0 0.0.0.255 any

ip access-list extended VLAN117
 deny   ip host 10.0.117.7 any
 permit ip 10.0.117.0 0.0.0.255 any

route-map R5_TO_REST_RMAP permit 10
 match ip address R5_TO_REST

route-map R5_TO_R10LOOP_RMAP permit 10
 match ip address R5_TO_R10LOOP
```

```
ip nat translation tcp-timeout 40
ip nat translation udp-timeout 60
ip nat translation finrst-timeout 20
ip nat translation syn-timeout 20
ip nat translation icmp-timeout 3

ip nat pool NPOOL1 10.10.11.60 10.10.11.80 prefix-length 25

ip nat in source stat 10.0.115.5 10.10.11.5 route- R5_TO_REST_RMAP reversible
ip nat in sou sta 10.0.115.5 10.10.11.50 route- R5_TO_R10LOOP_RMAP reversible
ip nat inside source list VLAN115 interface GigabitEthernet0/0 overload

ip nat inside source list VLAN117 pool NPOOL1
ip nat inside source static 10.0.117.7 10.10.11.7

ip nat log translations syslog

logging trap debugging
logging 10.10.11.100
logging on

int g0/0
 ip nat outside

int g0/1
 ip nat inside

int g0/2
 ip nat inside
```

R10

```
ip access-list extended VLAN101
 permit ip 10.10.11.0 0.0.0.255 any

ip nat translation max-entries all-host 25

ip nat pool NPOOL99 172.99.99.60 172.99.99.80 prefix-length 24 add-route

ip nat source list VLAN101 pool NPOOL99 overload

router ospf 1
 redistribute static subnets

int g0/0
 ip nat enable

int g0/1
 ip nat enable
```

NAT Configuration Guide and Command Reference are the best resources for NAT configuration options. NAT is definitely a very useful tool for both real world implementations and for getting around requirements in the lab.

When configuring route-map support on static translations with multi-direction NAT rules it is important to add the `reversible` keyword to allow initiate inbound connection from external networks.

Be sure to be familiar with the global settings with NAT. What protocols can be tuned for translations, etc. On R10 we limited the max NAT entries permitted per host, which can be useful in a network attack scenario.

Timeout parameters for NAT are configured globally under the "`ip nat translation`" options.

On R10 the task states to not define an inside or outside network. This is accomplished using the command `ip nat enable`. This is a good way to do NAT on routers as it doesn't matter for direction any more. Traffic is translated based on rules you define in your NAT entries.

The shortcoming to this method is that you cannot generate traffic on the router and test NAT translations. Traffic needs to be generated by a device beyond the router. Also, this method should be used when configuring VRF aware NAT. But VRF NAT is beyond the scope of the Security lab at this time.

In the beginning of this lab there were restrictions on creating manual static routes to fix routing. By creating a pool with the "`add-route`" option a static route is created automatically without to the NVI0 interface allowing for redistribution into the routing protocols.

IPv6 Considerations

NAT Protocol-Translation (NAT-PT) was moved to Historic Status. There are numerous reasons NAT-PT was a bad idea and deserved to be shot. If you want to know all of them, read the RFC 4966.

Verification

Start with telnet from R7 to verify translation and log generation:

```
R7#telnet 4.4.4.4
Trying 4.4.4.4 ... Open


Password required, but none set
```

```
[Connection to 4.4.4.4 closed by foreign host]

*Mar 21 23:16:25.646: %IPNAT-6-CREATED: tcp 10.0.117.7:63034 10.10.11.7:63034
4.4.4.4:23 4.4.4.4:23

R11#sh ip nat tran
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.10.11.7:63034   10.0.117.7:63034   4.4.4.4:23         4.4.4.4:23
--- 10.10.11.7         10.0.117.7         ---                ---
--- 10.10.11.5         10.0.115.5         ---                ---
--- 10.10.11.50        10.0.115.5         ---                ---

R7(config)#int f0/1
R7(config-if)#ip add 10.0.117.70 255.255.255.0

R11#sh ip nat t
Pro Inside global      Inside local       Outside local      Outside global
--- 10.10.11.7         10.0.117.7         ---                ---
tcp 10.10.11.60:39232  10.0.117.70:39232  4.4.4.4:23         4.4.4.4:23
--- 10.10.11.60        10.0.117.70        ---                ---
--- 10.10.11.5         10.0.115.5         ---                ---
--- 10.10.11.50        10.0.115.5         ---                ---
```

Don't forget to put the original address on F0/1 after testing. Now R5:

```
R10(config)#line vty 0 4
R10(config-line)#no logi

R4(config)#line vty 0 4
R4(config-line)#no login

R5#telnet 100.100.100.10
Trying 100.100.100.10 ... Open

R10>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:34
*388 vty 0                 idle                 00:00:00 10.10.11.50

  Interface    User               Mode         Idle     Peer Address

R10>

R11#sh ip nat tran tcp ver
Pro Inside global      Inside local       Outside local      Outside global
tcp    10.10.11.50:48772        10.0.115.5:48772           100.100.100.10:23
100.100.100.10:23
    create 00:00:23, use 00:00:20 timeout:40000, left 00:00:19, Map-Id(In):
0,
```

```
    flags:
extended, use_count: 0, entry-id: 12, lc_entries: 0

R5#telnet 10.10.11.10
Trying 10.10.11.10 ... Open
R10>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:02:47
*388 vty 0                 idle                 00:00:00 10.10.11.5

R11#sh ip nat tra tcp
Pro Inside global      Inside local       Outside local      Outside global
tcp     10.10.11.5:63951            10.0.115.5:63951           10.10.11.10:23
10.10.11.10:23Interface     User                  Mode           Idle      Peer
Address

R10>
```

Now the other way round. Since the "`reversible`" option was added and the translation is static, R10's loopback should be only able to reach 10.10.11.50. Any other address will not be able to reach 10.10.11.50 but 10.10.11.5 instead:

```
R10#telnet 10.10.11.50
Trying 10.10.11.50 ...
% Connection refused by remote host

R10#telnet 10.10.11.50 /source-interface l0
Trying 10.10.11.50 ... Open


Password required, but none set

[Connection to 10.10.11.50 closed by foreign host]

R11#sh ip nat tran tcp
Pro Inside global      Inside local       Outside local      Outside global
tcp  10.10.11.50:23           10.0.115.5:23              100.100.100.10:22018
100.100.100.10:22018


R10#telnet 10.10.11.5 /source-interface l0
Trying 10.10.11.5 ...
% Connection refused by remote host

R10#telnet 10.10.11.5
Trying 10.10.11.5 ... Open
```

```
Password required, but none set

[Connection to 10.10.11.5 closed by foreign host]

R11#sh ip nat t tcp
Pro Inside global      Inside local       Outside local      Outside global
tcp  10.10.11.5:23              10.0.115.5:23              10.10.11.10:60611
10.10.11.10:60611

R11#clear ip nat tran *
R11#telnet 10.10.11.10 /source-interface g0/1
Trying 10.10.11.10 ... Open
R10>
```

This is a TCP translation so it should timeout in 40 seconds. Press CTRL+SHIFT+6+X:

```
R11#sh ip nat tran tcp ver
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.10.11.11:63753  10.0.115.11:63753  10.10.11.10:23     10.10.11.10:23
    create 00:00:03, use 00:00:01 timeout:40000, left 00:00:38, Map-Id(In):
2,
    flags:
extended, use_count: 0, entry-id: 29, lc_entries: 0
```

Configured ICMP timeout is 3 seconds (3000 msecs):

```
R11#ping 10.10.11.10 source g0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.11.10, timeout is 2 seconds:
Packet sent with a source address of 10.0.115.11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R11#sh ip nat tran icmp ver
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.10.11.11:4     10.0.115.11:4      10.10.11.10:4      10.10.11.10:4
    create 00:00:00, use 00:00:00 timeout:3000, left 00:00:02, Map-Id(In): 2,
    flags:
extended, use_count: 0, entry-id: 33, lc_entries: 0
```

All looks good. Let's now verify NAT config on R10:

```
R10#sh ip nat nvi statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
NAT Enabled interfaces:
  GigabitEthernet0/0, GigabitEthernet0/1
Hits: 0  Misses: 0
CEF Translated packets: 146, CEF Punted packets: 0
```

```
Expired translations: 4
Dynamic mappings:
-- Source [Id: 1] access-list VLAN101 pool NPOOL99 refcount 0
 pool NPOOL99: netmask 255.255.255.0
        start 172.99.99.60 end 172.99.99.80
        type generic, total addresses 21, allocated 0 (0%), misses 0
```

Telnet, disconnect from the session and telnet second time:

```
R11#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:26:01
*514 vty 0                 idle                 00:00:00 172.99.99.60

  Interface    User               Mode         Idle     Peer Address

R4>

R10#sh ip nat nvi translations
Pro Source global      Source local       Destin  local      Destin  global
tcp 172.99.99.60:20138 10.10.11.11:20138  4.4.4.4:23         4.4.4.4:23
tcp 172.99.99.60:54526 10.10.11.11:54526  4.4.4.4:23         4.4.4.4:23


R10#sh ip nat sta
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
Inside interfaces:
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Outside Destination
[Id: 1] access-list VLAN101 pool NPOOL99 refcount 2
 pool NPOOL99: netmask 255.255.255.0
        start 172.99.99.60 end 172.99.99.80
        type generic, total addresses 21, allocated 1 (4%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
nat-limit statistics:
 All Host Max allowed: 25
 host 10.10.11.11: max allowed 25, used 2, missed 0
Queued Packets: 0
```

```
R7#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:44:18
*514 vty 0                 idle                 00:00:00 172.99.99.60
 515 vty 1                 idle                 00:01:37 172.99.99.60
 516 vty 0/0/0             idle                 00:00:28 172.99.99.60

  Interface    User               Mode         Idle     Peer Address

R4>

R10#sh ip nat sta
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
Inside interfaces:
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Outside Destination
[Id: 1] access-list VLAN101 pool NPOOL99 refcount 2
 pool NPOOL99: netmask 255.255.255.0
        start 172.99.99.60 end 172.99.99.80
        type generic, total addresses 21, allocated 1 (4%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
nat-limit statistics:
 All Host Max allowed: 25
 host 10.10.11.11: max allowed 25, used 2, missed 0
 host 10.10.11.7: max allowed 25, used 1, missed 0
Queued Packets: 0
```

Now let's limit number of translations to 1 just to test the limits:

```
R10(config)#ip nat translation max-entries all-host 1
R10#clear ip nat nvi tra *
R10#deb ip nat detailed
IP NAT detailed debugging is on


R7#telnet 4.4.4.4
Trying 4.4.4.4 ... Open
```

```
R4>
R7#telnet 4.4.4.4
Trying 4.4.4.4 ...
% Destination unreachable; gateway or host down

R7#

*Mar 21 23:14:33.407: NAT: [0] Allocated Port for 10.10.11.7 -> 172.99.99.60:
wanted 41096 got 41096
*Mar 21 23:14:33.407: NAT: administratively-defined entry limit reached (1)
*Mar 21 23:14:33.407: NAT-SymDB: DB is either not enabled or not initiated.
*Mar 21 23:14:33.407: NAT*: Can't create new inside entry -
forced_punt_flags: 0
*Mar 21 23:14:33.407: NAT: [0] Allocated Port for 10.10.11.7 -> 172.99.99.60:
wanted 41096 got 41096
*Mar 21 23:14:33.407: NAT: administratively-defined entry limit reached (1)
*Mar 21 23:14:33.407: NAT-SymDB: DB is either not enabled or not initiated.
*Mar 21 23:14:33.407: NAT-NVI: translation failed (A), dropping packet
s=10.10.11.7 d=4.4.4.4
```

Task 2: IOS Access-Lists

- On R2 allow HTTP and HTTPs destined to a webserver located at 2.2.2.2
- The above mentioned webserver will be taken down for maintenance and backups
- Every Wednesday between 1am and 3am traffic to this device should be blocked
- The maintenance schedule will come into effect March 1st 2013 and will last for the next 2 months
- New TCP sessions should not be allowed to/through R2. Log all attempts
- Devices from behind R2 including the router must be able to establish new TCP sessions.
- There should be an explicit entry in the ACL allowing it. Also permit all other traffic
- There are multiple servers located in VLAN 70 behind R7:
    - 10.70.70.22 & 2010:70:70::22 (SSH, Syslog, HTTPs)
    - 10.70.70.53 & 2010:70:70::53 (DNS, Kerberos, LDAP SSL)
    - 10.70.70.153 & 2010:70:70::153 (DNS, Kerberos, LDAP SSL)
- Create access-lists that will allow for communication to those servers from any source
- IPv4 ACL should only have three “permit” entries
- All other unnecessary traffic should be explicitly blocked but not logged
- You should be as specific as possible in both ACLs. Apply them inbound on R7’s F0/1

Detailed Solution

R2

```
time-range WEB_TRANGE
 absolute start 00:00 01 March 2013 end 23:59 30 April 2013
 periodic Wednesday 13:00 to 14:59
```

```
ip access-list extended FILTER
 permit icmp any any
 deny   tcp any host 2.2.2.2 eq www time-range WEB_TRANGE
 deny   tcp any host 2.2.2.2 eq 443 time-range WEB_TRANGE
 permit tcp any host 2.2.2.2 eq www
 permit tcp any host 2.2.2.2 eq 443
 permit tcp any any established
 deny   tcp any any syn log
 permit ip any any

int g0/0
 ip access-group FILTER in
```

R7

```
object-group network R7
 host 10.0.117.7
 host 224.0.0.5
 host 224.0.0.6

object-group service R7_SERVICES
 ospf
 icmp echo
 icmp echo-reply

object-group service S1_SERVICES
 tcp eq 22
 udp eq syslog
 tcp eq 443

object-group service S2_SERVICES
 tcp eq domain
 udp eq domain
 tcp eq 750
 udp eq 750
 tcp eq 636

object-group network SERVERS2
 host 10.70.70.53
 host 10.70.70.153

ip access-list extended OUTSIDE_IN
 permit object-group R7_SERVICES any object-group R7
 permit object-group S1_SERVICES any host 10.70.70.22
 permit object-group S2_SERVICES any object-group SERVERS2
 deny   ip any any

ipv6 access-list OUTSIDE6_IN
 permit 89 any host FF02::5
 permit 89 any host FF02::6
```

```
 permit 89 any host FE80::7
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit icmp any host FF02::1 router-advertisement
 permit icmp any host FF02::1 router-solicitation
 permit icmp any host 2010:0:117::7
 permit tcp any host 2010:70:70::22 eq 22
 permit tcp any host 2010:70:70::22 eq 443
 permit udp any host 2010:70:70::22 eq syslog
 permit tcp any host 2010:70:70::53 eq domain
 permit udp any host 2010:70:70::53 eq domain
 permit tcp any host 2010:70:70::53 eq 750
 permit udp any host 2010:70:70::53 eq 750
 permit tcp any host 2010:70:70::53 eq 636
 permit tcp any host 2010:70:70::153 eq domain
 permit udp any host 2010:70:70::153 eq domain
 permit tcp any host 2010:70:70::153 eq 750
 permit udp any host 2010:70:70::153 eq 750
 permit tcp any host 2010:70:70::153 eq 636
 deny ipv6 any any

int f0/1
 ip access-group OUTSIDE_IN in
 ipv address fe80::7 link-local
 ipv6 traffic-filter OUTSIDE6_IN in
```

In the task we were told that we need to allow TCP connections coming back in from external that have already been allowed out (source from behind R2). This is accomplished using the keyword "`established`".

Time Ranges allow the application of ACL rules based on date and time. This is an advantage when you don't want access list entries always in effect or in effect as soon as they are applied.

The Object Groups for ACLs feature lets you classify devices or protocols into groups and apply those groups to access control lists to create policies for those groups. Same concept as on the ASA.

As a real-world advice if you want to modify the content of an ACL without removing it (e.g. you want to put an entry between sequence 6 and 7) you can accomplish this by using resequencing (`ip access-list resequence`).

If you don't know/remember what is the port number corresponding to a particular protocol you can use the ASA's Configuration Guide. Navigate to "Reference" -> "Addresses, Protocols, and Ports". In this task, if you used 88 for Kerberos, that is acceptable as well since the question does not specify what version we are talking about (v4 is 88).

It would be a good question to the proctor how "specific" you should be with the ACL entries. In this particular case we are definitely OK with "any" as the source; for ICMPv6 destination of "any" is also acceptable since otherwise it would be a real pain to account for all possible Neighbor Discovery destinations – Link Local, Solicited Node Multicast, Global and All IPv6 Nodes.

IPv6 Considerations

The ACL functionality in IPv6 is similar to the ACLs in IPv4. Access lists determine the type of traffic that is blocked or forwarded at device interfaces. Access lists allow the filtering of inbound and outbound traffic at specific interfaces based on source and destination addresses. At the end of each access list is an implicit deny statement.

Key thing to remember about IPv6 ACLs is that they contain implicit permit rules to enable IPv6 Neighbor Discovery. These rules, however, will get overridden by placing an explicit "`deny ipv6 any any`" statement within an ACL. This is why for that type of situations exceptions must be made "earlier" in the ACL.

Also note the difference in applying an IPv6 ACL – this is accomplished by using the "`ipv6 traffic-filter`" command.

Object Groups are not supported for IPv6 addresses.

Verification

Start with telnet from R6 to verify SYN logging:

```
R6#telnet 2.2.2.2
Trying 2.2.2.2 ...
% Destination unreachable; gateway or host down

R2#sh access-l
Extended IP access list FILTER
    10 permit icmp any any
    20 deny tcp any host 2.2.2.2 eq www time-range WEB_TRANGE (inactive)
    30 deny tcp any host 2.2.2.2 eq 443 time-range WEB_TRANGE (inactive)
    40 permit tcp any host 2.2.2.2 eq www
    50 permit tcp any host 2.2.2.2 eq 443
    60 permit tcp any any established
    70 deny tcp any any syn log (2 matches)
    80 permit ip any any (5 matches)
```

What about sessions initiated from R2?:

```
R2#telnet 6.6.6.6
Trying 6.6.6.6 ... Open


Password required, but none set

[Connection to 6.6.6.6 closed by foreign host]

R2#sh access-list
Extended IP access list FILTER
    10 permit icmp any any
    20 deny tcp any host 2.2.2.2 eq www time-range WEB_TRANGE (inactive)
    30 deny tcp any host 2.2.2.2 eq 443 time-range WEB_TRANGE (inactive)
    40 permit tcp any host 2.2.2.2 eq www
    50 permit tcp any host 2.2.2.2 eq 443
    60 permit tcp any any established (18 matches)
    70 deny tcp any any syn log (2 matches)
    80 permit ip any any (18 matches)
```

Also verify HTTP & HTTPs (or at least one):

```
R2(config)#ip http ser

R2#sh clock
*11:25:14.499 UTC Fri Mar 22 2013

R6#telnet 2.2.2.2 80
Trying 2.2.2.2, 80 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Fri, 22 Mar 2013 11:15:28 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

R2#sh access-l
Extended IP access list FILTER
    10 permit icmp any any
    20 deny tcp any host 2.2.2.2 eq www time-range WEB_TRANGE (inactive)
    30 deny tcp any host 2.2.2.2 eq 443 time-range WEB_TRANGE (inactive)
    40 permit tcp any host 2.2.2.2 eq www (12 matches)
    50 permit tcp any host 2.2.2.2 eq 443
    60 permit tcp any any established (19 matches)
    70 deny tcp any any syn log (2 matches)
    80 permit ip any any (23 matches)

R2#clock set 13:21:11 20 March 2013
```

```
R6#telnet 2.2.2.2 80
Trying 2.2.2.2, 80 ...
% Destination unreachable; gateway or host down

R2#sh access-l
Extended IP access list FILTER
 10 permit icmp any any
 20 deny tcp any host 2.2.2.2 eq www time-range WEB_TRANGE (active) (1 match)
 30 deny tcp any host 2.2.2.2 eq 443 time-range WEB_TRANGE (active)
 40 permit tcp any host 2.2.2.2 eq www (23 matches)
 50 permit tcp any host 2.2.2.2 eq 443
 60 permit tcp any any established (19 matches)
 70 deny tcp any any syn log (2 matches)
 80 permit ip any any (104 matches)
```

Now Router 7. We will not any replies back since there is no device with 10.70.70.22 in VLAN 70. You could re-configure CAT4 but we can test without it:

```
R11#telnet 10.70.70.22 22
Trying 10.70.70.22, 22 ...
% Connection timed out; remote host not responding

R11#telnet 10.70.70.22 443
Trying 10.70.70.22, 443 ...
% Connection timed out; remote host not responding

R11#telnet 10.70.70.53 750
Trying 10.70.70.53, 750 ...
% Connection timed out; remote host not responding

R11#telnet 10.70.70.153 750
Trying 10.70.70.153, 750 ...
% Connection timed out; remote host not responding

R11#telnet 10.70.70.153 636
Trying 10.70.70.153, 636 ...
% Connection timed out; remote host not responding
R7#sh access-l
Extended IP access list OUTSIDE_IN
    10 permit object-group R7_SERVICES any object-group R7 (499 matches)
    20 permit object-group S1_SERVICES any host 10.70.70.22 (4 matches)
    30 permit object-group S2_SERVICES any object-group SERVERS2 (6 matches)
    40 deny ip any any
```

To test IPv6 part we will need to configure CAT4 for IPv6:

```
CAT4(config)#sdm pref dual-ipv4-and-ipv6 default
```

```
CAT4#reload

CAT4(config)#int vlan 70
CAT4(config-if)#ipv add 2010:70:70::22/64

CAT4(config)#ipv route ::/0 2010:70:70::7
CAT4(config)#ip http secure-server
```

If you did not put entries for Neighbor Discovery, R7 loses connectivity:

```
R7#ping 2010:0:117::7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:0:117::7, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

After adding entries for OSPF and Neighbor Discovery you should be able to keep the adjacencies and ping between the directly connected routers:

```
R7#clear ipv ospf proc
Reset ALL OSPF processes? [no]: yes

*Mar  22  13:31:21.146:  %OSPFv3-5-ADJCHG:  Process  1,  Nbr  11.11.11.11  on
FastEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
*Mar  22  13:31:21.162:  %OSPFv3-5-ADJCHG:  Process  1,  Nbr  11.11.11.11  on
FastEthernet0/1 from LOADING to FULL, Loading Done

R11#clear ipv ne
R11#ping 2010:0:117::7 rep 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 2010:0:117::7, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 8/8/8 ms

R7#clear ipv ne
R7#ping 2010:0:117::11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:0:117::11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

R7#sh ipv access-l
IPv6 access list OUTSIDE6_IN
    permit 89 any host FF02::5 (8 matches) sequence 10
    permit 89 any host FF02::6 sequence 20
```

```
    permit 89 any host FE80::7 (6 matches) sequence 30
    permit icmp any any nd-ns (4 matches) sequence 40
    permit icmp any any nd-na (4 matches) sequence 50
    permit icmp any host FF02::1 router-advertisement (2 matches) sequence 60
    permit icmp any host FF02::1 router-solicitation sequence 70
    permit icmp any host 2010:0:117::7 (12 matches) sequence 80
    permit tcp any host 2010:70:70::22 eq 22 sequence 90
    permit tcp any host 2010:70:70::22 eq 443 sequence 100
    permit udp any host 2010:70:70::22 eq syslog sequence 110
    permit tcp any host 2010:70:70::53 eq domain sequence 120
    permit udp any host 2010:70:70::53 eq domain sequence 130
    permit tcp any host 2010:70:70::53 eq 750 sequence 140
    permit udp any host 2010:70:70::53 eq 750 sequence 150
    permit tcp any host 2010:70:70::53 eq 636 sequence 160
    permit tcp any host 2010:70:70::153 eq domain sequence 170
    permit udp any host 2010:70:70::153 eq domain sequence 180
    permit tcp any host 2010:70:70::153 eq 750 sequence 190
    permit udp any host 2010:70:70::153 eq 750 sequence 200
    permit tcp any host 2010:70:70::153 eq 636 sequence 210
    deny ipv6 any any sequence 220
```

All right, few final tests for the server part:

```
R11#telnet 2010:70:70::22 443
Trying 2010:70:70::22, 443 ... Open

 [Connection to 2010:70:70::22 closed by foreign host]

R11#telnet 2010:70:70::22 636
Trying 2010:70:70::22, 636 ...
% Destination unreachable; gateway or host down

R11#telnet 2010:70:70::22 22
Trying 2010:70:70::22, 22 ... Open
SSH-1.99-Cisco-1.25

[Connection to 2010:70:70::22 closed by foreign host]

R11(config)#ip name-server 2010:70:70::53
R11(config)#ip domain-lookup

R11#MiamiVice
Translating "MiamiVice"...domain server (2010:70:70::53)

Translating "MiamiVice"...domain server (2010:70:70::53)

Translating "MiamiVice"...domain server (2010:70:70::53) % Name lookup
aborted
```

```
R11#telnet 2010:70:70::153 750
Trying 2010:70:70::153, 750 ...
% Destination unreachable; gateway or host down

R7#sh ipv access-l
IPv6 access list OUTSIDE6_IN
   permit 89 any host FF02::5 (207 matches) sequence 10
   permit 89 any host FF02::6 sequence 20
   permit 89 any host FE80::7 (6 matches) sequence 30
   permit icmp any any nd-ns (6 matches) sequence 40
   permit icmp any any nd-na (18 matches) sequence 50
   permit icmp any host FF02::1 router-advertisement (22 matches) sequence 60
   permit icmp any host FF02::1 router-solicitation sequence 70
   permit icmp any host 2010:0:117::7 (12 matches) sequence 80
   permit tcp any host 2010:70:70::22 eq 22 (7 matches) sequence 90
   permit tcp any host 2010:70:70::22 eq 443 (12 matches) sequence 100
   permit udp any host 2010:70:70::22 eq syslog sequence 110
   permit tcp any host 2010:70:70::53 eq domain sequence 120
   permit udp any host 2010:70:70::53 eq domain (12 matches) sequence 130
   permit tcp any host 2010:70:70::53 eq 750 sequence 140
   permit udp any host 2010:70:70::53 eq 750 sequence 150
   permit tcp any host 2010:70:70::53 eq 636 sequence 160
   permit tcp any host 2010:70:70::153 eq domain sequence 170
   permit udp any host 2010:70:70::153 eq domain sequence 180
   permit tcp any host 2010:70:70::153 eq 750 (2 matches) sequence 190
   permit udp any host 2010:70:70::153 eq 750 sequence 200
   permit tcp any host 2010:70:70::153 eq 636 sequence 210
   deny ipv6 any any (21 matches) sequence 220
```

Task 3: Reflexive Access-Lists

- On R6 allow uses from VLAN 62 to reach external networks. Allow the following :
  - SSH to routers R4 and R10
  - SMTP
  - DNS
  - HTTP and HTTPs
- The return entries should be automatically created for the above mentioned traffic
- These entries should expire after 3 minutes for TCP-based protocols
- DNS entries (TCP & UDP) should expire after 1 minute
- Global Reflexive Timeout should be set to 100 seconds
- You are allowed to make any other necessary permissions and permit ICMP but all other traffic should be dropped
- Configure the same policy for IPv6 traffic
- Don’t use CBAC or ZFW to accomplish this task

Detailed Solution

R6

```
ip access-list extended RACL
 permit tcp any host 4.4.4.4 eq 22 reflect MIRROR timeout 180
 permit tcp any host 100.100.100.10 eq 22 reflect MIRROR timeout 180
 permit tcp any any eq smtp reflect MIRROR timeout 180
 permit tcp any any eq www reflect MIRROR timeout 180
 permit tcp any any eq 443 reflect MIRROR timeout 180
 permit udp any any eq domain reflect MIRROR timeout 60
 permit tcp any any eq domain reflect MIRROR timeout 60
 permit tcp any any eq 81 reflect MIRROR timeout 300
 permit ip any any

ip access-list extended OUTSIDE_IN
 permit ospf any any
 permit icmp any any
 evaluate MIRROR
 deny   ip any any log

ipv6 access-list RACL6
 permit tcp any host 4::4 eq 22 reflect MIRROR6 timeout 180
 permit tcp any host 10::10 eq 22 reflect MIRROR6 timeout 180
 permit tcp any any eq smtp reflect MIRROR6 timeout 180
 permit tcp any any eq www reflect MIRROR6 timeout 180
 permit tcp any any eq 443 reflect MIRROR6 timeout 180
 permit tcp any any eq domain reflect MIRROR6 timeout 60
 permit udp any any eq domain reflect MIRROR6 timeout 60
 permit ipv6 any any

ipv6 access-list OUTSIDE6_IN
 permit 89 any any
 permit icmp any any
 evaluate MIRROR6
 deny ipv6 any any log

ip reflexive-list timeout 100

int s0/1/0
 ip access-group OUTSIDE_IN in
 ip access-group RACL out
 ipv6 traffic-filter OUTSIDE6_IN in
 ipv6 traffic-filter RACL6 out
```

Reflexive Access Lists allow IP packets to be filtered based on upper-layer session information. You can use this feature to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network. This is accomplished

by combining an interface ACL with the Reflexive Filtering, a kind of session filtering. Note RACLs don't reflect router-generated traffic (see Verification).

A Reflexive ACL is triggered when a new IP upper-layer session (such as TCP or UDP) is initiated from "inside" of the network, with a packet traveling to the external ("outside") network. When triggered, the Reflexive Access List generates a new, temporary entry. This entry will permit traffic to enter our network only if the traffic is part of the session - but it will not permit packets that do not match any of the existing sessions.

Reflexive ACLs are somewhat similar to the method seen in the previous task –the "`established`" keyword, but "`established`" only works for the TCP protocol. For the other upper-layer protocols (such as UDP, ICMP, and so forth), you would have to either permit all incoming traffic or define all possible permissible source/destination host/port address pairs for each protocol. Unmanageable.

Another advantage of using RACLs is a truer form of session filtering, which is much harder to spoof. Not only the ACK/RST bit is checked (as with "`established`") but also the addresses and port number. The disadvantage of this feature is inability of tracking secondary channels used by some protocols, like for example FTP. RACLs are not able to properly handle such protocols.

Temporary reflexive access list entries are removed at the end of the session. For TCP sessions, the entry is removed 5 seconds after two set FIN bits are detected, or immediately after matching a TCP packet with the RST bit set. Also if no packets are seen for the session for the "`timeout`" period, an entry is removed.

For UDP and other protocols, since these are considered to be connectionless, there is no session tracking information embedded in packets. Therefore the end of a session for those is when no packets are seen for the flow for the `timeout` period.

Reflexive ACLs are not supported with numbered ACLs on the ISR routers. If you had attempted to create a Reflexive ACL with a numbered ACL you would not have found the option available.

Once you create an ACL that specifies what traffic should be "reflected" you must apply it to the interface in the direction of the user traffic. So there will be two interface ACLs involved – one that is blocking the traffic from the "outside" and one that creates "reflected" entries. Return packets will be allowed based on that "reflected" ACEs.

By adding the `timeout` option to the ACLs above we have defined the absolute length of time, in seconds that the reflexive ACL list entry can remain in a dynamic access list. 180 seconds for the TCP sessions and 60 seconds for DNS.

IPv6 Considerations

Reflexive Access Lists are supported for IPv6 as shown in this task.

Verification

Start with telnet to test TCP traffic using IPv4 for transport:

```
R4(config)#ip domain-name ipexpert.com
R4(config)#cry key gen rsa mod 768

R2#telnet 4.4.4.4 22
Trying 4.4.4.4, 22 ... Open
SSH-1.99-Cisco-1.25

R2#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... Open

R6#sh access-l MIRROR
Reflexive IP access list MIRROR
     permit tcp host 4.4.4.4 eq 22 host 172.6.2.2 eq 49164 (6 matches) (time
left 176)
     permit tcp host 4.4.4.4 eq www host 172.6.2.2 eq 60960 (6 matches) (time
left 174)

R2#telnet 11.11.11.11 25
Trying 11.11.11.11, 25 ...
% Connection refused by remote host

R6#sh access-l RACL
Extended IP access list RACL
    10 permit tcp any host 4.4.4.4 eq 22 reflect MIRROR (16 matches)
    20 permit tcp any host 100.100.100.10 eq 22 reflect MIRROR (1 match)
    30 permit tcp any any eq smtp reflect MIRROR (2 matches)
    40 permit tcp any any eq www reflect MIRROR (15 matches)
    50 permit tcp any any eq 443 reflect MIRROR
    60 permit udp any any eq domain reflect MIRROR
    70 permit tcp any any eq domain reflect MIRROR
    80 permit tcp any any eq 81 reflect MIRROR
    90 permit ip any any

R2(config)#ip domain lookup
R2(config)#ip name-server 11.11.11.11

R2#ValVerde
Translating "ValVerde"...domain server (11.11.11.11)
 (11.11.11.11)

R6#sh access-l MIRROR
Reflexive IP access list MIRROR
```

```
     permit udp host 11.11.11.11 eq domain host 172.6.2.2 eq 59187 (1 match)
(time left 58)
     permit udp host 11.11.11.11 eq domain host 172.6.2.2 eq 49497 (2
matches) (time left 58)
     permit udp host 11.11.11.11 eq domain host 172.6.2.2 eq 61989 (2
matches) (time left 55)
     permit udp host 11.11.11.11 eq domain host 172.6.2.2 eq 54682 (1 match)
(time left 52)

R4#telnet 2.2.2.2
Trying 2.2.2.2 ...
% Destination unreachable; gateway or host down

*Mar  22  18:32:14.297:  %SEC-6-IPACCESSLOGP:  list  OUTSIDE_IN  denied  tcp
172.46.46.4(54109) -> 2.2.2.2(23), 1 packet
```

All right, all looks good. Now IPv6 :

```
R2#telnet 4::4 22
Trying 4::4, 22 ... Open
SSH-1.99-Cisco-1.25

R2#telnet 4::4 80
Trying 4::4, 80 ... Open

R6#sh access-l MIRROR6
IPv6 access list MIRROR6 (reflexive) (per-user)
    permit tcp host 4::4 eq 22 host 2172:6:2::2 eq 59546 timeout 180 (2
matches) (time left 169) sequence 1
    permit tcp host 4::4 eq www host 2172:6:2::2 eq 43393 timeout 180 (2
matches) (time left 171) sequence 2

R2(config)#no ip name-server
R2(config)#ip name-server 2010:10:11::11

R2#IPexpert
Translating "IPexpert"...domain server (2010:10:11::11)
 (2010:10:11::11)
Translating "IPexpert"...domain server (2010:10:11::11)

Translating "IPexpert"...domain server (2010:10:11::11)

% Bad IP address or host name
% Unknown command or computer name, or unable to find computer address


R6#sh access-l MIRROR6
IPv6 access list MIRROR6 (reflexive) (per-user)
```

```
    permit udp host 2010:10:11::11 eq domain host 2172:6:2::2 eq 60060
timeout 60 (time left 55) sequence 4
    permit udp host 2010:10:11::11 eq domain host 2172:6:2::2 eq 62632
timeout 60 (time left 55) sequence 5
    permit udp host 2010:10:11::11 eq domain host 2172:6:2::2 eq 51192
timeout 60 (time left 55) sequence 6
    permit udp host 2010:10:11::11 eq domain host 2172:6:2::2 eq 52514
timeout 60 (time left 55) sequence 7

R6#sh access-l RACL6
IPv6 access list RACL6
    permit tcp any host 4::4 eq 22 reflect MIRROR6 timeout 180 (9 matches)
sequence 10
    permit tcp any host 10::10 eq 22 reflect MIRROR6 timeout 180 sequence 20
    permit tcp any any eq smtp reflect MIRROR6 timeout 180 sequence 30
    permit tcp any any eq www reflect MIRROR6 timeout 180 (14 matches)
sequence 40
    permit tcp any any eq 443 reflect MIRROR6 timeout 180 sequence 50
    permit tcp any any eq domain reflect MIRROR6 timeout 60 (1 match)
sequence 60
    permit udp any any eq domain reflect MIRROR6 timeout 60 (4 matches)
sequence 70
    permit ipv6 any any sequence 80

R4#telnet 2::2
Trying 2::2 ...
% Destination unreachable; gateway or host down

*Mar 22 18:34:36.689: %IPV6_ACL-6-ACCESSLOGP: list OUTSIDE6_IN/40 denied tcp
2172:46:46::4(44254) -> 2::2(23), 1 packet

R6#sh access-list OUTSIDE6_IN
IPv6 access list OUTSIDE6_IN
    permit 89 any any (145 matches) sequence 10
    permit icmp any any sequence 20
    evaluate MIRROR6 sequence 30
    deny ipv6 any any log (1 match) sequence 40
```

Finally you should realize that Reflexive ACLs work only for transit packets. Router-generated traffic is not seen as “transit” if you source packets from the LAN (F0/1) interface :

```
R6(config)#ip telnet source-interface f0/1

R6#telnet 4.4.4.4
Trying 4.4.4.4 ...
*Mar 22 18:45:41.729: %SEC-6-IPACCESSLOGP: list OUTSIDE_IN denied tcp
4.4.4.4(23) -> 172.46.46.6(24051), 1 packet
```

```
% Connection reset by user

R6#telnet 4::4
Trying 4::4 ...
*Mar 22 18:45:47.701: %IPV6_ACL-6-ACCESSLOGP: list OUTSIDE6_IN/40 denied tcp
4::4(23) -> 2172:46:46::6(17579), 1 packet
% Connection reset by user
```

A workaround would be to use a trick with local Policy Based Routing or simply allow the traffic destined to the router in the blocking ACL.

Task 4: CBAC

- Allow all TCP and UDP based traffic to go out and return from the “external” networks (172.x.x.x) on R10
- Inbound and outbound traffic should be inspected using CBAC
- Also inspect router-generated packets
- Make sure CBAC engine can properly inspect fragmented traffic
- Log all the denies. Only permit traffic as required by the lab
- Configure the same policy for IPv6 traffic

Detailed Solution

R10

```
ip access-list extended OUTSIDE_IN
 permit ospf any any
 permit icmp any any
 deny   ip any any log

ipv6 access-list OUTSIDE_IN6
 permit icmp any any
 permit 89 any any
 deny ipv6 any any log

ip inspect name CBAC tcp router-traffic
ip inspect name CBAC udp router-traffic

ipv6 inspect name CBAC6 tcp
ipv6 inspect name CBAC6 udp

ipv6 inspect routing-header

interface GigabitEthernet0/1
 ip access-group OUTSIDE_IN in
 ip inspect CBAC out
 ip virtual-reassembly in
```

```
 ipv6 inspect CBAC6 out
 ipv6 traffic-filter OUTSIDE_IN6 in
 ipv6 virtual-reassembly in

interface GigabitEthernet0/0
 ip virtual-reassembly in
 ipv6 virtual-reassembly in
```

CBAC adds real stateful firewall capability to the IOS code. IOS firewall keeps track of connections that it is monitoring by building a state table that contains information about each connection. Then any traffic coming to the interface with CBAC enabled is checked against those entries and the decision is made whether to forward packets or drop them.

When performing generic stateful inspection, CBAC focuses on L3 and L4 parameters, keeping track of state information for each connection established through it. The attributes held in the state table enable CBAC to dynamically create temporary openings to enable the pertinent return traffic.

Since ICMP was not required to be inspected we opened a hole in the ACL to allow it. If we were to inspect ICMP you could only open an entry for Echo packets.

IPv6 Considerations

CBAC inspection for IPv6 can be configured for TCP, UDP, ICMPv6 and FTP protocols.

By default all packets with Routing Extension Header will be dropped by CBAC. To start inspecting them use `ipv6 inspect routing-header`.

CBAC for IPv6 configuration is pretty much the same as for version 4 of IP. Just use "`ipv6`" instead of "`ip`".

Verification

As usually we will start with verification using IPv4:

```
R10#sh ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited]
connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
```

```
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name CBAC
    tcp alert is on audit-trail is off timeout 3600
 inspection of router local traffic is enabled
    udp alert is on audit-trail is off timeout 30
 inspection of router local traffic is enabled

Interface Configuration
 Interface GigabitEthernet0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is CBAC
    tcp alert is on audit-trail is off timeout 3600
 inspection of router local traffic is enabled
    udp alert is on audit-trail is off timeout 30
 inspection of router local traffic is enabled
  Inbound access list is OUTSIDE_IN
  Outgoing access list is not set

R11#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4>

R10#sh ip ins ses
Established Sessions
 Session 3167D814 (10.10.11.11:43166)=>(4.4.4.4:23) tcp SIS_OPEN

R11#traceroute 4.4.4.4
Type escape sequence to abort.
Tracing the route to 4.4.4.4
VRF info: (vrf in name/id, vrf out name/id)
  1 10.10.11.10 0 msec 0 msec 0 msec
  2 4.4.4.4 4 msec 0 msec *

R10#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... Open

R10#sh ip ins sess
Established Sessions
 Session 3167D19C (172.41.41.10:23364)=>(4.4.4.4:80) tcp SIS_OPEN
Half-open Sessions
 Session 3167D5EC (10.10.11.11:49158)=>(4.4.4.4:33438) udp SIS_OPENING
 Session 3167D3C4 (10.10.11.11:49159)=>(4.4.4.4:33439) udp SIS_OPENING
 Session 3167D814 (10.10.11.11:49157)=>(4.4.4.4:33437) udp SIS_OPENING
```

All is fine. Now IPv6 :

```
R11#telnet 4::4
```

```
Trying 4::4 ... Open
R4>

R10#sh ipv inspect se
Established Sessions
 Session 31B31E88 (2010:10:11::11:36662)=>(4::4:23) tcp SIS_OPEN
```

Before Routing Header inspection was enabled nothing comes back to R11 – this is because UDP packets are dropped by CBAC :

```
R11#trace ipv6
Target IPv6 address: 4::4
Source address:
Insert source routing header? [no]: yes
Nexthop address: 2172:41:41::4
Nexthop address:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 4::4

  1 2010:10:11::10 0 msec 0 msec 0 msec
  2  *  *  *
  3  *  *  *
  4  *  *  *
  5  *  *  *
```

After enabling inspection the situation changes. Traffic is allowed through R10 and R4 sends Parameter Problem message back to the source:

```
R10#sh ipv inspect config
Session audit trail is disabled
Session alert is enabled
Routing Header inspection is enabled
one-minute (sampling period) thresholds are [2147483647:2147483647]
connections
max-incomplete sessions thresholds are [2147483647:2147483647]
max-incomplete tcp connections per host is 4294967295. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
icmp idle-time is 10 sec
Session hash table size is 1021
Inspection Rule Configuration
```

```
 Inspection name CBAC6
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30

R11#traceroute ipv6
Target IPv6 address: 4::4
Source address:
Insert source routing header? [no]: yes
Nexthop address: 2172:41:41::4
Nexthop address:
Numeric display? [no]: yes
Timeout in seconds [3]: 1
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]: 5
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 4::4

  1 2010:10:11::10 0 msec 0 msec 0 msec
  2  ?  ?  ?
  3  ?  ?  ?
  4  ?  ?  ?
  5  ?  *  ?

R10#sh ipv ins se
Half-open Sessions
 Session 31B31948 (2010:10:11::11:61817)=>(4::4:33437) udp SIS_OPENING
 Session 31B32908 (2010:10:11::11:53950)=>(4::4:33446) udp SIS_OPENING
 Session 31B323C8 (2010:10:11::11:63226)=>(4::4:33443) udp SIS_OPENING
 Session 31B32748 (2010:10:11::11:50765)=>(4::4:33445) udp SIS_OPENING

R4#
*Mar   23   11:57:25.093:   ICMPv6:   Sent   Parameter,   Src=2172:41:41::4,
Dst=2010:10:11::11
*Mar   23   11:57:25.093:   ICMPv6:   Sent   Parameter,   Src=2172:41:41::4,
Dst=2010:10:11::11
*Mar   23   11:57:25.097:   ICMPv6:   Sent   Parameter,   Src=2172:41:41::4,
Dst=2010:10:11::11
*Mar   23   11:57:25.097:   ICMPv6:   Sent   Parameter,   Src=2172:41:41::4,
Dst=2010:10:11::11
```

Since there is no option to inspect router-generated traffic as of the current code release, return packets will be dropped:

```
R10#telnet 4::4
Trying 4::4 ...
```

```
*Mar 23 12:06:02.242: %IPV6_ACL-6-ACCESSLOGP: list OUTSIDE_IN6/30 denied tcp
4::4(23) -> 2172:41:41::10(13547), 1 packet
% Connection timed out; remote host not responding
```

Task 5: CBAC Application Inspection & Tuning

- R10 configuration should be modified to meet some additional requirements
- The router should delete TCP connections if they have been idle for 10 minutes
- For web traffic only allow Java applets to be downloaded from web servers 2.2.2.2 and 6.6.6.6
- POP3 inspection should be enabled. Make sure the firewall requires secure authentication by the clients
- Turn on logging of all TCP sessions for IPv4
- After FIN exchange was detected, session should be managed for no longer than 10 seconds
- Optimize firewall's performance by adjusting CBAC memory structure to ~2000 sessions
- IPv6 CBAC Alerts should be only enabled for TCP; UDP idle timeout should be 2 minutes
- Internal web servers 10.10.11.198 & .199 should be protected from SYN-Flood attacks
- These servers are reachable from the public network via 172.41.41.198 & .199 and are configured to listen for HTTP traffic at ports 80, 8080 and 10080
- R10 should start deleting half open sessions if they are at 800. This behavior should cease when this number drops below 600
- Also if there have been 100 new half-open connections detected within the last one minute, the router should start deleting them. When the number of these sessions drops below 50, this process should stop
- If there is more than 450 TCP half-opened sessions hanging on a single server drop all of them and don't allow for any new connections for the next 2 minutes

Detailed Solution

R10

```
access-list 5 permit host 2.2.2.2
access-list 5 permit host 6.6.6.6

ip inspect name CBAC tcp audit-trail on router-traffic
ip inspect name CBAC http java-list 5
ip inspect name CBAC pop3 secure-login

ip inspect tcp idle-time 600
ip inspect tcp finwait-time 10

ip inspect hashtable-size 2048

ipv6 inspect udp idle-time 120
ipv6 inspect name CBAC6 tcp alert on
```

```
ipv6 inspect name CBAC6 udp alert off

ipv6 inspect hashtable-size 2039

ip inspect name CBAC_IN http

ip port-map http port tcp 8080 10080

ip inspect max-incomplete high 800
ip inspect max-incomplete low 600

ip inspect one-minute low 50
ip inspect one-minute high 100

ip inspect tcp max-incomplete host 450 block-time 2

ip nat source static 10.10.11.198 172.41.41.198
ip nat source static 10.10.11.199 172.41.41.199

ip access-list ext OUTSIDE_IN
 22 per tcp any host 172.41.41.198 eq 80 8080 10080
 24 per tcp any host 172.41.41.199 eq 80 8080 10080

int g0/0
 ip inspect CBAC_IN in
```

CBAC uses timeouts and thresholds to determine how long state information should be kept for a session and when to drop sessions that were NOT fully established.

Alerts are used to inform us about some basic attacks, like for example when CBAC DoS thresholds are exceeded. Audit-trails allow you to log all network connection requests, including the IP addresses of the source and destination, the ports used in the connection, the number of bytes sent, and at what time the connection started and ended.

Hash Table is a memory structure used to map an incoming packet to an existing firewall session. Cisco recommends to set the Hash Table size to be about the same as the number of concurrent sessions managed by the firewall.

The Port to Application Mapping table, or just PAM in short, is used to determine what type of inspection should be performed for a particular traffic flow. Adding a new mapping is a must if we want to inspect traffic going over a non-standard port we know the application is using.

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, "half-open" means that the session has not reached the established state. Whenever the numbers of half-open sessions with the same destination host address rises above a threshold, the software will delete half-open sessions.

The difference between TCP intercept and the configuration applied to the CBAC policy is the addition of UDP protection by CBAC as well. Both TCP and UDP are checked for half open connectivity when applied to `ip inspect max-incomplete` or `ip inspect one-minute`. This is a loose definition as UDP does not perform a handshake like TCP but is considered a half open connection by the firewall when it has seen traffic in one direction but no return traffic in the other direction.

IPv6 Considerations

CBAC for IPv6 configuration is pretty much the same as for version 4 of IP. Just use "`ipv6`" instead of "`ip`".

Verification

Most of the verification for this part will be just show commands to double-verify the settings. For some reasons this IOS version does not update the hash-table size to the configured value – instead of 1024 it should show us 2048:

```
R10#sh ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [50 : 100] connections
max-incomplete sessions thresholds are [600 : 800]
max-incomplete tcp connections per host is 450. Block-time 2 minutes.
tcp synwait-time is 30 sec -- tcp finwait-time is 10 sec
tcp idle-time is 600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name CBAC
    tcp alert is on audit-trail is on timeout 600
 inspection of router local traffic is enabled
    udp alert is on audit-trail is off timeout 30
 inspection of router local traffic is enabled
    http java-list 5 alert is on audit-trail is off timeout 600
    pop3 secure-login is on alert is on audit-trail is off timeout 600
 Inspection name CBAC_IN
    http alert is on audit-trail is off timeout 600

Interface Configuration
 Interface GigabitEthernet0/1
  Inbound inspection rule is CBAC_IN
    http alert is on audit-trail is off timeout 600
  Outgoing inspection rule is CBAC
    tcp alert is on audit-trail is on timeout 600
 inspection of router local traffic is enabled
    udp alert is on audit-trail is off timeout 30
```

```
 inspection of router local traffic is enabled
    http java-list 5 alert is on audit-trail is off timeout 600
    pop3 secure-login is on alert is on audit-trail is off timeout 600
  Inbound access list is OUTSIDE_IN
  Outgoing access list is not set

R10#sh access-l 5
Standard IP access list 5
    10 permit 2.2.2.2
    20 permit 6.6.6.6
```

To test inbound connections from the public ranges we can configure one of our switches to emulate the WWW server:

```
CAT3(config)#int vlan 101
CAT3(config-if)#ip add 10.10.11.198 255.255.255.0

CAT3(config)#ip http ser
CAT3(config)#ip http port 8080

R4#telnet 172.41.41.198 8080
Trying 172.41.41.198, 8080 ... Open

R10#sh ip ins sess detail
Established Sessions
 Session 3167D19C (172.41.41.4:39776)=>(10.10.11.198:8080) http SIS_OPEN
  Created 00:00:02, Last heard 00:00:02
  Bytes sent (initiator:responder) [0:0]
```

We can also verify Audit Trails:

```
R11#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4>sh ip int br
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES unset  administratively down
down
FastEthernet0/1            172.41.41.4     YES manual up
up
Serial0/0/0                172.46.46.4     YES manual up
up
Serial0/1/0                unassigned      YES unset  administratively down
down
Loopback0                  4.4.4.4         YES manual up
up
R4>exit
```

```
R10#
*Mar  23  14:24:49.246:  %FW-6-SESS_AUDIT_TRAIL_START:  Start  tcp  session:
initiator (10.10.11.11:27317) -- responder (4.4.4.4:23)

*Mar  23  14:25:08.962:  %FW-6-SESS_AUDIT_TRAIL:  Stop  tcp  session:  initiator
(10.10.11.11:27317) sent 43 bytes -- responder (4.4.4.4:23) sent 573 bytes
```

And quick look at IPv6:

```
R10#sh ipv6 inspect all
Session audit trail is disabled
Session alert is enabled
Routing Header inspection is enabled
one-minute   (sampling   period)   thresholds   are   [2147483647:2147483647]
connections
max-incomplete sessions thresholds are [2147483647:2147483647]
max-incomplete tcp connections per host is 4294967295. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 120 sec
icmp idle-time is 10 sec
Session hash table size is 2039
Inspection Rule Configuration
 Inspection name CBAC6
    tcp alert is on audit-trail is off timeout 3600
    udp alert is off audit-trail is off timeout 120

Interface Configuration
 Interface GigabitEthernet0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is CBAC6
    tcp alert is on audit-trail is off timeout 3600
    udp alert is off audit-trail is off timeout 120
```

Task 6: Zone-Based Firewall

- Configure Zone-Based Firewall on R11
- Create three zones – IN (towards R7), OUT (towards R10) and DMZ (towards R5)
- All TCP and UDP traffic from inside should be allowed to go out OUT and DMZ
- Router 5's loopback0 (5.5.5.5 and 5::5) emulates an IPv4 VPN gateway & IPv4/IPv6 HTTP server (port 9080)
- Make sure these services will be accessible to anyone coming from the "outside"
- Don't use an ACL to classify HTTP traffic
- ICMP is allowed to pass freely between the zones
- Deploy the same policy for IPv6 traffic (except for VPN)
- Packets that are dropped by ZFW should be logged
- Make sure routing is still working after you are done with this section

Detailed Solution

R11

```
ip inspect log drop-pkt

ip port-map http port tcp 9080

ip access-list extended DMZ_SERVER
 permit ip any host 5.5.5.5

ip access-list extended ESP_FROM_DMZ
 permit esp host 5.5.5.5 any

ip access-list extended ESP_TO_DMZ
 permit esp any host 5.5.5.5

ip access-list extended IKE_FROM_DMZ
 permit udp host 5.5.5.5 any eq isakmp
 permit udp host 5.5.5.5 any eq non500-isakmp

ip access-list extended IKE_TO_DMZ
 permit udp any host 5.5.5.5 eq isakmp
 permit udp any host 5.5.5.5 eq non500-isakmp

ipv6 access-list DMZ_SERVER6
 permit tcp any host 5::5 eq 9080

class-map type inspect match-all ZFW_ICMP_CLASS
 match protocol icmp

class-map type inspect match-all ZFW_TCP_CLASS
 match protocol tcp

class-map type inspect match-all ZFW_UDP_CLASS
 match protocol udp

class-map type inspect match-all ZFW_DMZ_SERVER_HTTP_CLASS
 match protocol http
 match access-group name DMZ_SERVER

class-map type inspect match-all ZFW_DMZ_SERVER6_HTTP_CLASS
 match access-group name DMZ_SERVER6

class-map type inspect match-all ZFW_ESP_FROM_DMZ_CLASS
 match access-group name ESP_FROM_DMZ

class-map type inspect match-all ZFW_IKE_FROM_DMZ_CLASS
 match access-group name IKE_FROM_DMZ
```

```
class-map type inspect match-all ZFW_IKE_TO_DMZ_CLASS
 match access-group name IKE_TO_DMZ

class-map type inspect match-all ZFW_ESP_TO_DMZ_CLASS
 match access-group name ESP_TO_DMZ

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_ICMP_CLASS
  pass
 class type inspect ZFW_TCP_CLASS
  inspect
 class type inspect ZFW_UDP_CLASS
  inspect
 class class-default
  drop log

policy-map type inspect ZFW_INDMZ_POL
 class type inspect ZFW_ICMP_CLASS
  pass
 class type inspect ZFW_TCP_CLASS
  inspect
 class type inspect ZFW_UDP_CLASS
  inspect
 class class-default
  drop log

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ZFW_ICMP_CLASS
  pass
 class class-default
  drop log

policy-map type inspect ZFW_OUTDMZ_POL
 class type inspect ZFW_IKE_TO_DMZ_CLASS
  inspect
 class type inspect ZFW_ESP_TO_DMZ_CLASS
  pass
 class type inspect ZFW_ICMP_CLASS
  pass
 class type inspect ZFW_DMZ_SERVER_HTTP_CLASS
  inspect
 class type inspect ZFW_DMZ_SERVER6_HTTP_CLASS
  inspect
 class class-default
  drop log

policy-map type inspect ZFW_DMZOUT_POL
 class type inspect ZFW_IKE_FROM_DMZ_CLASS
```

```
  inspect
 class type inspect ZFW_ESP_FROM_DMZ_CLASS
  pass
 class type inspect ZFW_ICMP_CLASS
  pass
 class class-default
  drop log

policy-map type inspect ZFW_DMZIN_POL
 class type inspect ZFW_ICMP_CLASS
  pass
 class class-default
  drop log

zone security IN
zone security OUT
zone security DMZ

zone-pair security INOUT source IN destination OUT
 service-policy type inspect ZFW_INOUT_POL

zone-pair security INDMZ source IN destination DMZ
 service-policy type inspect ZFW_INDMZ_POL

zone-pair security DMZOUT source DMZ destination OUT
 service-policy type inspect ZFW_DMZOUT_POL

zone-pair security DMZIN source DMZ destination IN
 service-policy type inspect ZFW_DMZIN_POL

zone-pair security OUTDMZ source OUT destination DMZ
 service-policy type inspect ZFW_OUTDMZ_POL

zone-pair security OUTIN source OUT destination IN
 service-policy type inspect ZFW_OUTIN_POL

int g0/0
 zone-member security OUT

int g0/1
 zone-member security DMZ

int g0/2
 zone-member security IN
```

Zone Based Firewall is essentially a syntax wrapper for CBAC – all the features we saw previously are built-in into ZFW. The main advantage of ZFW is that the policies are built in a

more structured fashion that ultimately allows us to implement any type of policy we want regardless of the number of security zones.
The main advantage of ZFW is that the inter-zone policies offer much more flexibility and granularity comparing them to CBAC. With Zone Based Firewall different policies can be applied subnets, host groups or even hosts connected to the same interface on the router.

Here's the list of basic steps required to implement ZFW:

1. Define classes of traffic you want to match (`class-map type inspect`). If it is only traffic that should be match based on source or destination don't forget to include the access-list. Another option is to use the "`match protocol`" command that matches all traffic for a particular protocol according to ports defined in PAM. This allows for more optimized classification and is a recommended way. You can also combine "match protocol" with an ACL to narrow down the scope of the class
2. Remember, the difference between `match-any` and `match-all` on the class-map. If you want to match a single protocol when it is from a specific source and destination then you should use "match-all". If it is to match a group of protocols remember to use the "match-any". Without remembering these important rules you will get caught up trying to troubleshoot why your policies are not working
3. If it is a layer 3/4 protocol apply this class-map traffic to a inspection policy-map (`policy-map type inspect`). If it a layer 7 class-map with extended features you will apply this to a layer 3/4 inspection to be serviced for deeper packet inspection
4. What will you do with the class map: drop, log, reset, inspect pass?
5. By default the parameter-map default is applied to all inspection rules. If you need to change the default parameters such as DoS thresholds, TCP timeouts, ICMP timeouts, etc you will need to define a new parameter map and apply this to the "inspect" action
6. To finish configuration you need to still define the zones, associate them with interfaces and finally apply the previously created policy via `service-policy type inspect`.

An IPv4 ACL matches all IP packets to 5.5.5.5 only to narrow down the class; the main condition to classify HTTP is still the "`match protocol http`" statement, which to be met, must recognize packets sent to TCP port 9080 as web traffic. This was accomplished by modifying the Port Map table.

For the logging function it looks like the Global Parameter Map may not necessarily work well in that particular IOS version. If we did not enable the "`log`" action under every single class-default, we would not see any messages. Also, old good "`ip inspect log drop-pkt`" no more affects ZFW. It is now purely for CBAC deployments. More on the Parameter Maps in the next task.

The last bullet point asks us to ensure all routing information is in place after completing this task. This is not going to be a problem since we did not touch the Self zone. Remember that Self

zone is the only one that controls traffic to-the-router. Default policy for that one is to allow all packets so no additional changes are needed here.

IPv6 Considerations

ZFW for IPv6 configuration is pretty much the same as for version 4 of IP. Since only four inspection engines are available as of right now (TCP, UDP, ICMP and FTP) you must use ACLs as a classification tool to make your policies more granular.

Verification

A new command was introduced in newer releases that may be useful for verifying ZFW configuration – `show policy-firewall`. It is definitely shorter than "`show policy-map type inspect zone-pair`" and provides a lot of useful information. We start with looking at our general ZFW setup:

```
R11#sh policy-firewall config all
Zone: self
  Description: System defined zone

Zone: IN
  Member Interfaces:
    GigabitEthernet0/2

Zone: OUT
  Member Interfaces:
    GigabitEthernet0/0

Zone: DMZ
  Member Interfaces:
    GigabitEthernet0/1

Zone-pair               : INOUT
Source Zone             : IN
Destination Zone        : OUT
Service-policy inspect : ZFW_INOUT_POL
  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_TCP_CLASS(match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_UDP_CLASS(match-all)
   Match protocol udp
```

```
  Action : inspect
   Parameter-map : Default
  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

Zone-pair               : INDMZ
Source Zone             : IN
Destination Zone        : DMZ
Service-policy inspect : ZFW_INDMZ_POL
  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_TCP_CLASS(match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_UDP_CLASS(match-all)
   Match protocol udp
  Action : inspect
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

Zone-pair               : DMZOUT
Source Zone             : DMZ
Destination Zone        : OUT
Service-policy inspect : ZFW_DMZOUT_POL
  Class-map : ZFW_IKE_FROM_DMZ_CLASS(match-all)
   Match access-group name IKE_FROM_DMZ
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_ESP_FROM_DMZ_CLASS(match-all)
   Match access-group name ESP_FROM_DMZ
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default
```

```
  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

Zone-pair               : DMZIN
Source Zone             : DMZ
Destination Zone        : IN
Service-policy inspect : ZFW_DMZIN_POL
  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

Zone-pair               : OUTDMZ
Source Zone             : OUT
Destination Zone        : DMZ
Service-policy inspect : ZFW_OUTDMZ_POL
  Class-map : ZFW_IKE_TO_DMZ_CLASS(match-all)
   Match access-group name IKE_TO_DMZ
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_ESP_TO_DMZ_CLASS(match-all)
   Match access-group name ESP_TO_DMZ
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_DMZ_SERVER_HTTP_CLASS(match-all)
   Match protocol http
   Match access-group name DMZ_SERVER
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_DMZ_SERVER6_HTTP_CLASS(match-all)
   Match access-group name DMZ_SERVER6
  Action : inspect
   Parameter-map : Default
```

```
  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

Zone-pair               : OUTIN
Source Zone             : OUT
Destination Zone        : IN
Service-policy inspect : ZFW_OUTIN_POL
  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

Parameter-map Config:
 Global:
  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets enabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  tcp reset-PSH disabled

Default:
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

Now we are going to start testing this configuration from the “inside” network – it may help to just temporarily remove ACLs applied on F0/1 on R7:

```
R7(config-if)#no ip access-group OUTSIDE_IN in
R7(config-if)#no ipv6 traffic-filter OUTSIDE6_IN in

R7#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4>

R7#traceroute 4.4.4.4

Type escape sequence to abort.
Tracing the route to 4.4.4.4

  1 10.0.117.11 4 msec 0 msec 4 msec
  2 10.10.11.10 0 msec 4 msec 0 msec
  3 4.4.4.4 4 msec *  4 msec

R11#sh policy-firewall session
        Session       2CBE0720       (10.0.117.7:45208)=>(4.4.4.4:23)       tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:23, Last heard 00:00:12
          Bytes sent (initiator:responder) [30:32]
        Session 2CBE0AA0 (10.0.117.7:49157)=>(4.4.4.4:33437) udp SIS_OPENING
          Created 00:00:09, Last heard 00:00:09
          Bytes sent (initiator:responder) [0:0]
        Session 2CBE0E20 (10.0.117.7:49158)=>(4.4.4.4:33438) udp SIS_OPENING
          Created 00:00:09, Last heard 00:00:09
          Bytes sent (initiator:responder) [0:0]

R7#telnet 5.5.5.5
Trying 5.5.5.5 ... Open

R11#sh policy-fire sess
        Session       2CBE3F20       (10.0.117.7:12274)=>(5.5.5.5:23)       tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard 00:00:01
          Bytes sent (initiator:responder) [27:49]
      Established Sessions = 1
```

All right, now let’s take a look at connections coming to our DMZ:

```
R5(config)#ip http server
R5(config)#ip http port 9080
```

```
R10#telnet 5.5.5.5 9080
Trying 5.5.5.5, 9080 ... Open

R11#sh policy-map type inspect zone-pair OUTDMZ  sessions

policy exists on zp OUTDMZ
  Zone-pair: OUTDMZ

  Service-policy inspect : ZFW_OUTDMZ_POL

    Class-map: ZFW_IKE_TO_DMZ_CLASS (match-all)
      Match: access-group name IKE_TO_DMZ

   Inspect

    Class-map: ZFW_ESP_TO_DMZ_CLASS (match-all)
      Match: access-group name ESP_TO_DMZ
      Pass
        0 packets, 0 bytes

    Class-map: ZFW_ICMP_CLASS (match-all)
      Match: protocol icmp
      Pass
        0 packets, 0 bytes

    Class-map: ZFW_DMZ_SERVER_HTTP_CLASS (match-all)
      Match: protocol http
      Match: access-group name DMZ_SERVER

   Inspect

      Number of Established Sessions = 1
      Established Sessions
        Session    2CBE2320    (10.10.11.10:57413)=>(5.5.5.5:9080)    http:tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard 00:00:01
          Bytes sent (initiator:responder) [0:0]


    Class-map: class-default (match-any)
      Match: any
      Drop
        8 packets, 192 bytes

R11(config)#do sh ip port-map http
Default mapping:  http     tcp port 80                          system defined
Default mapping:  http     tcp port 9080                        user defined
```

And the VPN (one was configured just to test this part):

```
R10#ping 10.55.55.5 so g0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.55.55.5, timeout is 2 seconds:
Packet sent with a source address of 172.41.41.10
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R11#sh policy-firewall session
        Session 2CBE73A0 (10.10.11.10:500)=>(5.5.5.5:500) udp SIS_OPEN
          Created 00:00:07, Last heard 00:00:04
          Bytes sent (initiator:responder) [916:708]
      Established Sessions = 1

R11#sh policy-map type ins zone-pair OUTDMZ  | s ESP
    Class-map: ZFW_ESP_TO_DMZ_CLASS (match-all)
      Match: access-group name ESP_TO_DMZ
      Pass
        9 packets, 1188 bytes


R11#sh policy-map type ins zone-pair DMZOUT  | s ESP
    Class-map: ZFW_ESP_FROM_DMZ_CLASS (match-all)
      Match: access-group name ESP_FROM_DMZ
      Pass
        9 packets, 1188 bytes
```

Don’t forget to check if the tunnel can be initialized from the other side as well:

```
R5#ping 172.41.41.10 so loop55

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.41.41.10, timeout is 2 seconds:
Packet sent with a source address of 10.55.55.5
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms

R11#sh policy-firewall session
        Session 2CBE7020 (10.10.11.10:500)=>(5.5.5.5:500) udp SIS_OPEN
          Created 00:00:25, Last heard 00:00:15
          Bytes sent (initiator:responder) [784:840]
      Established Sessions = 1

R11#sh policy-map type ins zone-pair OUTDMZ  | s ESP
    Class-map: ZFW_ESP_TO_DMZ_CLASS (match-all)
      Match: access-group name ESP_TO_DMZ
      Pass
        13 packets, 1716 bytes
```

To finish verification just a bunch of tests for IPv6:

```
R10#ping 5::5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5::5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R10#ping 7::7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R11#sh policy-map type inspect zone-pair OUTDMZ | s ICMP
    Class-map: ZFW_ICMP_CLASS (match-all)
      Match: protocol icmp
      Pass
        5 packets, 300 bytes

R11#sh policy-map type inspect zone-pair OUTIN | s ICMP
    Class-map: ZFW_ICMP_CLASS (match-all)
      Match: protocol icmp
      Pass
        130 packets, 7680 bytes

R5#ping 7::7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/8 ms
R11#sh policy-map type inspect zone-pair DMZIN | s ICMP
    Class-map: ZFW_ICMP_CLASS (match-all)
      Match: protocol icmp
      Pass
        5 packets, 300 bytes

R7#telnet 4::4
Trying 4::4 ... Open

R4>
R7#telnet 5::5
Trying 5::5 ... Open

R11#sh policy-firewall ses
        Session       2CBE2A20       [2010:0:117::7]:28350=>[4::4]:23       tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:28, Last heard 00:00:27
```

```
          Bytes sent (initiator:responder) [30:32]
        Session       2CBE34A0       [2010:0:117::7]:13169=>[5::5]:23       tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard 00:00:01
          Bytes sent (initiator:responder) [27:49]
      Established Sessions = 2
```

One nice thing about "`show policy-firewall session`" is that you can also narrow down the output to a particular Zone Pair and then it will show you what class a particular session is associated with:

```
R10#telnet 5::5 9080
Trying 5::5, 9080 ... Open

R11#sh policy-firewall session zone-pair ?
  INOUT
  INDMZ
  DMZOUT
  DMZIN
  OUTDMZ
  OUTIN
  ha  show ha sessions
  |   Output modifiers
  <cr>

R11#sh policy-fire sess zone-pair OUTDMZ
 Zone-pair: OUTDMZ
  Service-policy inspect : ZFW_OUTDMZ_POL
    Class-map : ZFW_IKE_TO_DMZ_CLASS(match-all)
    Class-map : ZFW_ESP_TO_DMZ_CLASS(match-all)
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_DMZ_SERVER_HTTP_CLASS(match-all)
    Class-map : ZFW_DMZ_SERVER6_HTTP_CLASS(match-all)
      Established Sessions =  1
        Session      2CBE42A0      [2010:10:11::10]:17308=>[5::5]:9080      tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:01, Last heard 00:00:01
          Bytes sent (initiator:responder) [0:0]
    Class-map : class-default(match-any)
```

Key thing to note here is that packets sent to TCP 9080 are inspected as TCP. Even if we modified the PAM table and use "`match protocol http`" this would not work. Again, HTTP inspection engine is not available for IPv6 as of the current code release.

One more thing we did not test is logging of dropping packets. Generate a segment to a port you know firewall blocks:

```
R10#telnet 5::5 9081
Trying 5::5, 9081 ...
% Connection timed out; remote host not responding

*Mar 24 16:20:49.311: %FW-6-DROP_PKT: Dropping tcp session 10.10.11.10:22312
5.5.5.5:9081 on zone-pair OUTDMZ class class-default due to  DROP action
found in policy-map with ip ident 0

R11#sh policy-firewall stats drop-counters
DROP action found in policy-map                          54
RST inside current window                                5
Out-Of-Order Segment                                     2
Stray Segment                                            1
```

Task 7: Zone-Based Firewall Application Inspection & Tuning

- R11 configuration should be modified to meet some additional requirements
- Sessions originated on the “inside” destined to the “outside” should be managed in the following way:
  - TCP connections should be removed after 15 minutes of inactivity
  - TCP sessions should be kept for 12 seconds after FIN-exchange was detected
  - If a TCP session does not fully establish within 20 seconds it should be removed
  - UDP idle timeout should be set to 90 seconds
  - Change the DoS thresholds to 500/300 (total) and 100/50 (one minute)
  - Packets with Routing Extension Header should be inspected
- Tune configuration of the firewall for packets flowing in the “outside” -> “dmz” direction
- Java applets should not be downloaded
- Don’t allow users to send HTTP requests with a URI greater than 30 Bytes
- Log any violations

Detailed Solution

R11

```
parameter-map type inspect INOUT_PARA
 ipv6 routing-header-enforcement loose
 max-incomplete low 300
 max-incomplete high 500
 one-minute low 50
 one-minute high 100
 udp idle-time 90
 tcp idle-time 900
 tcp finwait-time 12
 tcp synwait-time 20

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_TCP_CLASS
  inspect INOUT_PARA
```

```
 class type inspect ZFW_UDP_CLASS
  inspect INOUT_PARA

class-map type inspect http match-any HTTP_DPI_CLASS
 match response body java-applet
 match request uri length gt 30

policy-map type inspect http HTTP_DPI_POL
 class type inspect http HTTP_DPI_CLASS
  reset
  log

policy-map type inspect ZFW_OUTDMZ_POL
 class type inspect ZFW_DMZ_SERVER_HTTP_CLASS
  inspect
  service-policy http HTTP_DPI_POL
```

Parameter Maps in Zone Based Firewall are structures used to control or just tune behavior of inspections we applied to the policy. The most prevalent parameter-map is of type "`inspect`" – two pre-built maps are called "default" and "global". "Default" is used to tune some generic L3/L4 settings for TCP, UDP and ICMP protocols. This one is applied by default to every inspect action, so under every class-map in the policy configured for inspection, to control the DoS thresholds like for example the maximum number of half-opened sessions – so we can say that it is very similar to tuning CBAC settings.

This is as opposed to the "global" parameter-map that affects behavior of Zone Based Firewall in general (all class-maps). This is where you can enable logging of dropped packets, summary logs, or clear PSH bit if it is set along with the SYN flag in a TCP segment.

Of course we can create our own customized Parameter Maps and apply them under a class which will override the "default' map.

The application layer policy is optional and is typically applied to control finer details of an application. Using L3/4 inspection on flows matched via an ACL or „`match protocol`" still does basic Level 7 inspection (e.g. secondary channels for FTP), but to control specific application-level options of a particular protocol we need to use L7 class & policy-maps (so called Deep Packet Inspection). These L7 structures must be of type inspect equal to the protocol we want to Inspect at L7 – so for HTTP this will be "`class/policy –map type inspect http`".

The main difference configuration-wise is that we apply this level 7 policy-map under the Parent class, which is class in our basic L3/L4 policy-map. In simple words we can say that this Level 7 policy is going to be nested in Layer3/Layer 4 policy via "`service-policy` *`proto_name`*".

With HTTP class-maps, you will find that there are three options for match; request, response, and req-resp. Each of them are required for different actions. Here a Java Applet is an application sent to the user from the server. So we used the response tag. For URI this is a request as it is either going to be manually entered into the address bar by the user or will be sent to the server after the user clicks a link somewhere on a webpage.

IPv6 Considerations

All packets with Routing Extension Header are dropped by default. Use "`ipv6 routing-header enforcement`" in the Parameter Map to start inspecting those packets.

Verification

We will start with looking at the configured settings; moving on we will test Routing EH:

```
R11#sh policy-firewall config parameter-map INOUT_PARA
 parameter-map type inspect INOUT_PARA
  audit-trail off
  alert on
  max-incomplete low 300
  max-incomplete high 500
  one-minute low 50
  one-minute high 100
  udp idle-time 90
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 900
  tcp finwait-time 12
  tcp synwait-time 20
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647

R11#sh policy-firewa conf zone-pair INOUT
Zone-pair               : INOUT
Source Zone             : IN
Destination Zone        : OUT
Service-policy inspect : ZFW_INOUT_POL
  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_TCP_CLASS(match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : INOUT_PARA

  Class-map : ZFW_UDP_CLASS(match-all)
```

```
   Match protocol udp
  Action : inspect
   Parameter-map : INOUT_PARA

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

This is before the Parameter Map was applied (meaning "default" is being used):

```
R7#traceroute ipv

Target IPv6 address: 2010:10:11::10
Source address:
Insert source routing header? [no]: yes
Nexthop address: 2010:10:11::10
Nexthop address:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 2010:10:11::10

  1 2010:0:117::11 8 msec 0 msec 4 msec
  2  *  *  *
  3  *  *  *
  4  *  *  *
  5  *  *  *
  6  *  *  *
```

Log says the packet is dropped due to Internal Error:

```
*Mar    24    16:52:00.731:    %FW-6-DROP_PKT:    Dropping    udp    session
[2010:0:117::7]:62791   [2010:10:11::10]:33497   on   zone-pair   INOUT   class
ZFW_UDP_CLASS due to  Internal Error with ip ident 0
```

After we apply the Parameter Map, Routing EH packets are allowed to go through:

```
R7#traceroute ipv

Target IPv6 address: 2010:10:11::10
Source address:
Insert source routing header? [no]: yes
```

```
Nexthop address: 2010:10:11::10
Nexthop address:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 2010:10:11::10

  1 2010:0:117::11 0 msec 0 msec 0 msec
  2  ?  ?  ?
  3  ?  ?  ?
  4  ?  ?  ?
  5  ?  *  ?

R11#sh policy-firewall session zone-pair INOUT
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_TCP_CLASS(match-all)
    Class-map : ZFW_UDP_CLASS(match-all)
      Half-open Sessions = 48
        Session  30D48FE0  [2010:0:117::7]:62419=>[2010:10:11::10]:33498  udp
SIS_OPENING
          Created 00:01:16, Last heard 00:01:16
          Bytes sent (initiator:responder) [0:0]
        Session  30D49360  [2010:0:117::7]:57580=>[2010:10:11::10]:33499  udp
SIS_OPENING
          Created 00:01:16, Last heard 00:01:16
          Bytes sent (initiator:responder) [0:0]
        Session  30D496E0  [2010:0:117::7]:54049=>[2010:10:11::10]:33500  udp
SIS_OPENING
```

You can also trace once again to check the UDP timeout. These are idle for 75 seconds and still there:

```
R11#sh policy-firewall session zone-pair INOUT
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_TCP_CLASS(match-all)
    Class-map : ZFW_UDP_CLASS(match-all)
      Half-open Sessions = 3
        Session  30D537E0  [2010:0:117::7]:52110=>[2010:10:11::10]:33437  udp
SIS_OPENING
          Created 00:01:15, Last heard 00:01:15
```

```
          Bytes sent (initiator:responder) [0:0]
        Session   30D53B60   [2010:0:117::7]:52952=>[2010:10:11::10]:33438   udp
SIS_OPENING
          Created 00:01:15, Last heard 00:01:15
          Bytes sent (initiator:responder) [0:0]
        Session   30D53EE0   [2010:0:117::7]:54071=>[2010:10:11::10]:33439   udp
SIS_OPENING
          Created 00:01:15, Last heard 00:01:15
          Bytes sent (initiator:responder) [0:0]
    Class-map : class-default(match-any)
```

This is as opposed to IN->DMZ direction where the "default" Parameter Map applies with only 30-second UDP timeout set (here it shows 29 seconds and 1 sec after they are gone):

```
R11#sh policy-firewall session zone-pair INDMZ
 Zone-pair: INDMZ
  Service-policy inspect : ZFW_INDMZ_POL
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_TCP_CLASS(match-all)
    Class-map : ZFW_UDP_CLASS(match-all)
      Half-open Sessions = 3
        Session 30D54260 [2010:0:117::7]:58245=>[5::5]:33437 udp SIS_OPENING
          Created 00:00:29, Last heard 00:00:29
          Bytes sent (initiator:responder) [0:0]
```

Source Routing can be easily used to create a DoS attack with UDP. As expected, router enters into Aggressive Mode:

```
R11#sh policy-firewall session zone-pair INOUT
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_TCP_CLASS(match-all)
    Class-map : ZFW_UDP_CLASS(match-all)
      Half-open Sessions = 101

*Mar       24       17:02:27.579:       %FW-4-ALERT_ON:       (target:class)-
(INOUT:ZFW_UDP_CLASS):getting aggressive, count (101/500) current 1-min rate:
101
```

The final test will be for HTTP Deep Packet Inspection Policy:

```
R11#sh policy-firewall config zone-pair OUTDMZ
Zone-pair               : OUTDMZ
Source Zone             : OUT
Destination Zone        : DMZ
Service-policy inspect : ZFW_OUTDMZ_POL
  Class-map : ZFW_IKE_TO_DMZ_CLASS(match-all)
```

```
   Match access-group name IKE_TO_DMZ
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_ESP_TO_DMZ_CLASS(match-all)
   Match access-group name ESP_TO_DMZ
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_ICMP_CLASS(match-all)
   Match protocol icmp
  Action : pass log
   Parameter-map : Default

  Class-map : ZFW_DMZ_SERVER_HTTP_CLASS(match-all)
   Match protocol http
   Match access-group name DMZ_SERVER
  Action : inspect
   Parameter-map : Default
   Service Policy: http HTTP_DPI_POL

  Class-map : ZFW_DMZ_SERVER6_HTTP_CLASS(match-all)
   Match access-group name DMZ_SERVER6
  Action : inspect
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default

R10#copy http://5.5.5.5:9080/PrinceOfPersia Null0
Destination filename [Null0]?
Accessing http://5.5.5.5:9080/PrinceOfPersia...
%Error opening http://5.5.5.5:9080/PrinceOfPersia (No such file or directory)
```

Here another file was downloaded which exists – just to show you the session entry:

```
R11#sh policy-firewall session zone-pair OUTDMZ
 Zone-pair: OUTDMZ
  Service-policy inspect : ZFW_OUTDMZ_POL
    Class-map : ZFW_IKE_TO_DMZ_CLASS(match-all)
    Class-map : ZFW_ESP_TO_DMZ_CLASS(match-all)
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_DMZ_SERVER_HTTP_CLASS(match-all)
      Established Sessions =  1
        Session    30D2E660    (10.10.11.10:38384)=>(5.5.5.5:9080)    http:tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:02, Last heard 00:00:00
```

```
        Bytes sent (initiator:responder) [167:376713]
    Class-map : ZFW_DMZ_SERVER6_HTTP_CLASS(match-all)
    Class-map : class-default(match-any)
```

But what about this URI ("/" + 44 chars)?:

```
R10#copy      http://5.5.5.5:9080/VeryLongURIVeryLongURIVeryLongURIVeryLongURI
Null0
Destination filename [Null0]?
Accessing http://5.5.5.5:9080/VeryLongURIVeryLongURIVeryLongURIVeryLongURI...
%Error                                                                opening
http://5.5.5.5:9080/VeryLongURIVeryLongURIVeryLongURIVeryLongURI (I/O error)

R11#
*Mar 24 17:10:48.095: %APPFW-4-HTTP_URI_LENGTH: HTTP URI length (45) out of
range - resetting session 10.10.11.10:11755 5.5.5.5:9080 on zone-pair OUTDMZ
class ZFW_DMZ_SERVER_HTTP_CLASS appl-class HTTP_DPI_CLASS

*Mar 24 17:10:48.095: %FW-6-DROP_PKT: Dropping tcp session 10.10.11.10:11755
5.5.5.5:9080    with ip ident 0
```

Task 8: User-Based Firewall

- Configure R4 with User-Based Firewall
- Create two zones – internal (F0/1) and external (s0/0/0)
- Prior to accessing the network connecting users should successfully authenticate using Authentication Proxy and RADIUS. Use ISE as an AAA server
- Authenticated users trying to access external networks through R4 should be subject to
- the following policy:
    - Members of the Sales department should be able to access all TCP applications on a server located at 6.6.6.6. Don't permit any other traffic for those users
    - Administrators should be able to access any outside destinations using TCP and ICMP, including the Sales server
    - Dropped inside -> outside packets should be logged
- All other traffic, including ICMP packets coming from the external networks, should be blocked

Detailed Solution

R10

```
ip access-list ext OUTSIDE_IN
 25 per udp any host 172.41.41.150  eq 1645 1646

ip nat source static 10.1.1.150 172.41.41.150

int g0/2
```

```
 ip nat enable
```

R4

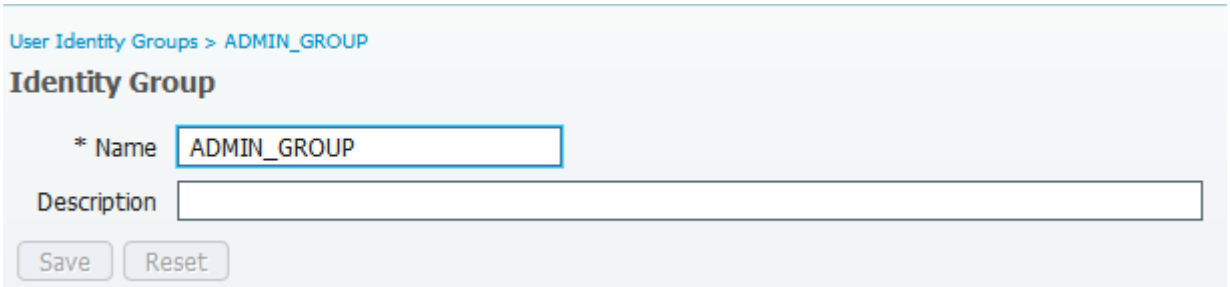
```
aaa new-model
aaa authentication login NO none
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius

line con 0
 login auth NO

ip radius source-interface Loopback0
radius-server host 172.41.41.150 auth-port 1645 acct-port 1646 key cisco

radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include

radius-server vsa send authentication

ip http server
ip http port 80
ip admission name AUTHP proxy http inactivity-time 60

ip access-list extended TO_R6
 permit ip any host 6.6.6.6

class-map type inspect match-all ZFW_ADMIN_ICMP_CLASS
 match protocol icmp
 match user-group ADMINS

class-map type inspect match-all ZFW_ADMIN_TCP_CLASS
 match protocol tcp
 match user-group ADMINS

class-map type inspect match-all ZFW_SALES_TCP_CLASS
 match protocol tcp
 match access-group name TO_R6
 match user-group SALES

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_SALES_TCP_CLASS
  inspect
 class type inspect ZFW_ADMIN_TCP_CLASS
  inspect
 class type inspect ZFW_ADMIN_ICMP_CLASS
  inspect
 class class-default
```

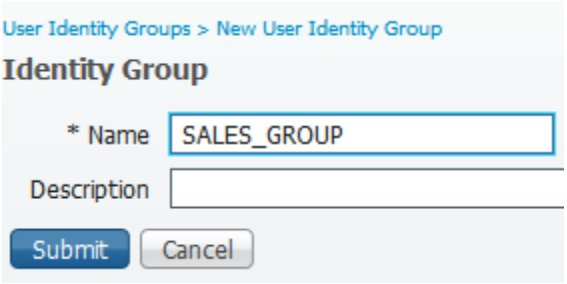
```
  drop log

zone security IN
zone security OUT

zone-pair security INOUT source IN destination OUT
 service-policy type inspect ZFW_INOUT_POL

int f0/1
 zone-member security IN
 ip admission AUTHP

int s0/
 zone-member security OUT
```

ISE

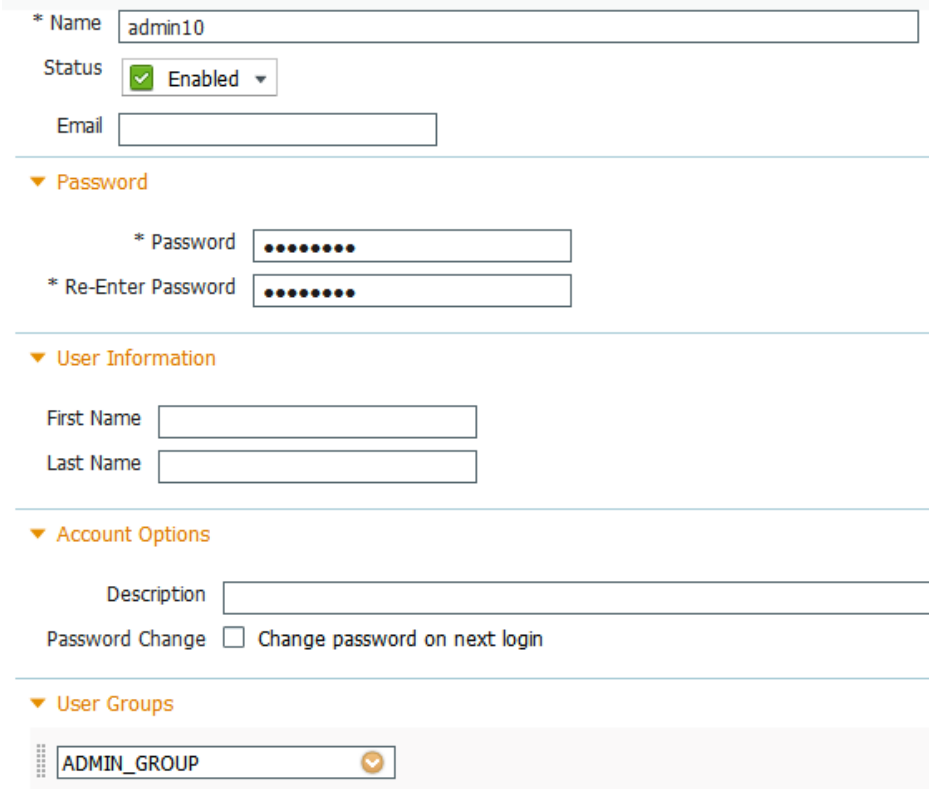
```
ip route 4.4.4.4 255.255.255.255 gateway 10.1.1.1
```

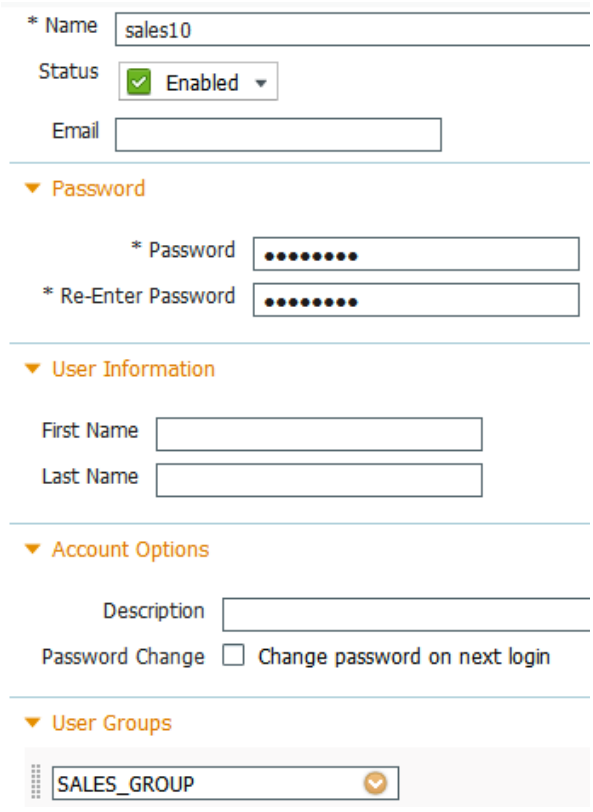
Create two groups, one for admins and one for sales team:



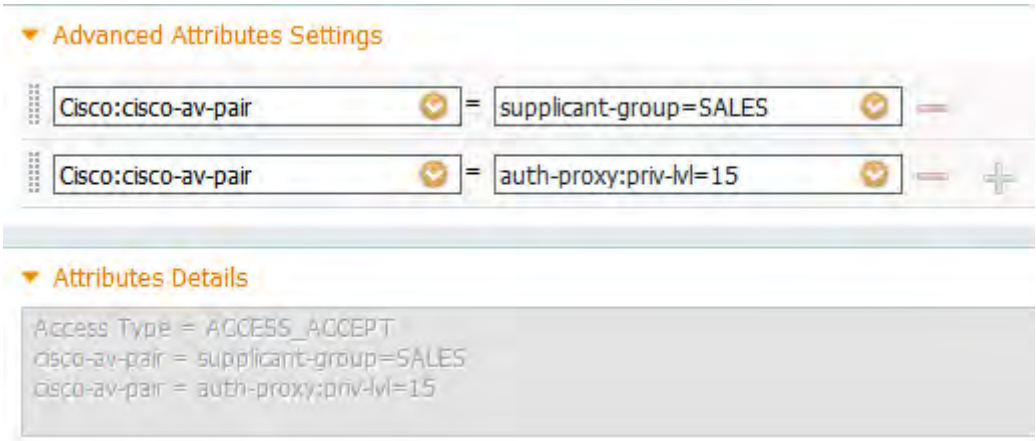


We definitely need users to test - “admin10” and “sales10” in my case. Make sure they are part of the respective group:

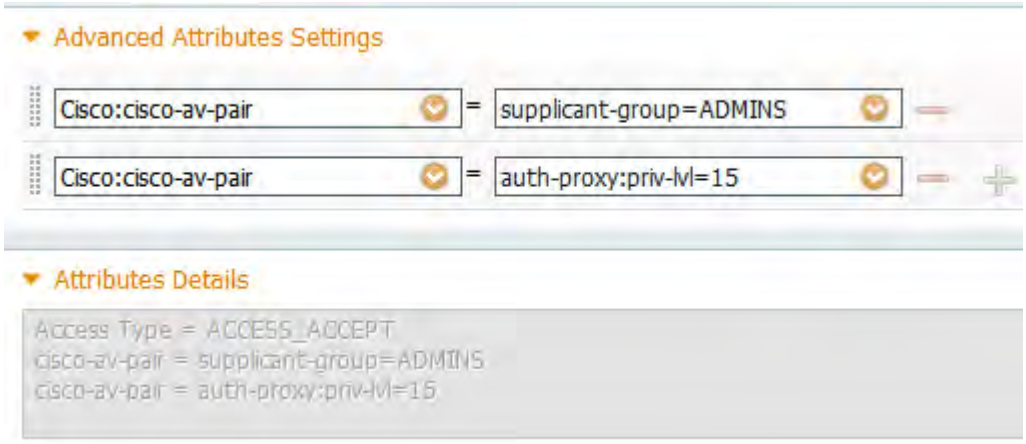




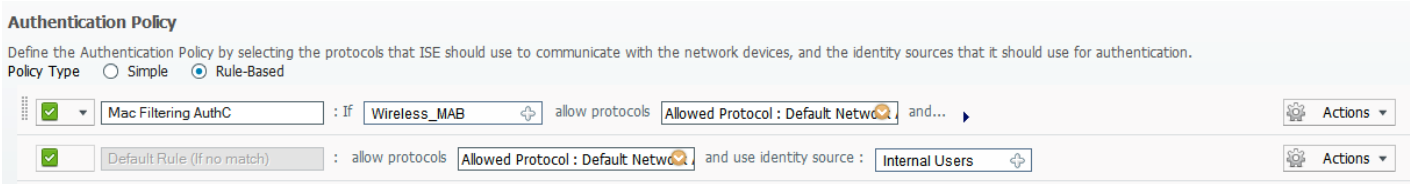
RADIUS Access Accept packet must carry the User Group name and Authentication Proxy parameters required for this feature to work. Authorization Profiles is our next step. SALES:

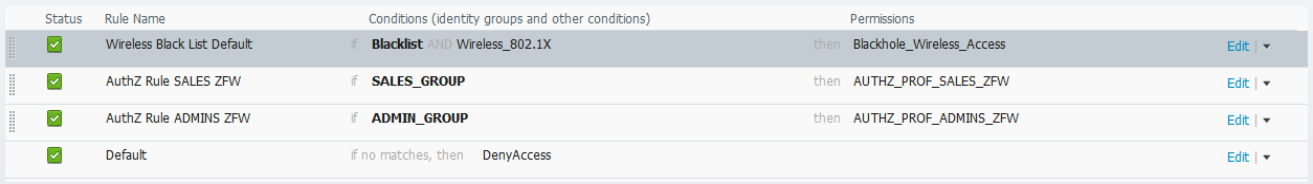


ADMINS:



We are going to keep Authentication & Authorization policies very simple. The “Default Rule” will be used for authentication and then the User Groups will act as our conditions in the AuthZ Policy:





Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Wireless Black List Default	if **Blacklist** AND Wireless_802.1X	then Blackhole_Wireless_Access	Edit
✓	AuthZ Rule SALES ZFW	if **SALES_GROUP**	then AUTHZ_PROF_SALES_ZFW	Edit
✓	AuthZ Rule ADMINS ZFW	if **ADMIN_GROUP**	then AUTHZ_PROF_ADMINS_ZFW	Edit
✓	Default	if no matches, then DenyAccess		Edit

The User-Based Firewall was designed to provide identity or User-Group based security that provides differentiated access for different classes of user. This feature leverages existing authentication and validation methods (such as Auth Proxy) to associate each source IP address to a User-Group.

There are two ways to configure User-Based firewall:

1. Based on the user's group alias (known as a Supplicant Group) returned by ACS/ISE
2. Based on the tag value & locally defined policy (known as Tag & Template). The tag is also returned by ACS/ISE

Speaking of the first method, the Supplicant Group attribute (supplicant-group) needs to be configured as a Cisco AV Pair on ACS/ISE. This information will be then sent inside of the Access Accept packet for a particular (successfully authenticated) user. The firewall will then bind the IP address of the authenticated client to the User Group and store this information in the User-Group table.

Now whenever traffic is to be sent by the user, the User-Group table is looked up to find a corresponding User Group name (Supplicant Group). Once this is done the firewall policy is being checked – actions defined under the classes configured with `match user-group` for this group name will be processed (if there are some other criteria they obviously must match as well assuming the class type is of "`match-all`").

The second method is somewhat similar, but instead of returning the User-Group name directly, a Tag value is returned. This Tag is then used as a matching criteria to the locally defined class-maps (`type control tag`) – the logic here is that we will be trying to derive User-Group name locally. So there will be a local policy on the NAS (also `type control tag`) that is processed, where every single class is associated with an Identity Policy (`identity policy`). Once a class is matched by returned tag, router automatically learns Identity Policy (locally defined), which points to User-Group name, and optionally an ACL. Then ZFW policy would be processed using locally derived User-Group as a matching criteria.

There is also an option to combine User-Based firewall policy with Authentication Proxy ACLs. First thing we would have to add an interface ACL inbound on the client-facing port (F0/1 in our case). This one could only allow all necessary traffic such as routing protocols and RADIUS. Then with the first method we would add a dACL or ProxyACL Cisco AV line to the AuthZ Profile; with the second method we would specify an ACL along with the User-Group name in the Identity Policy (`access-group`). The result would be combining an Auth Proxy ACL with the physical

one (as in regular Auth Proxy) – only when user packet is allowed by this ACL then the ZFW policy will be processed.

In our example we are providing the User-Group name off-hand (ISE). There is no interface ACL, which means that after successful authentication ZFW policy is processed.

IPv6 Considerations

It appears that Authentication Proxy & User-Based ZFW does not work with IPv6 in 15.2.

Verification

Place the Test PC in VLAN 41, configure an IP address to something from 172.41.41.0/24 range and configure routes as needed:

```
CAT3(config)#int g1/0/2
CAT3(config-if)#sw host
CAT3(config-if)#sw acc vlan 41
```

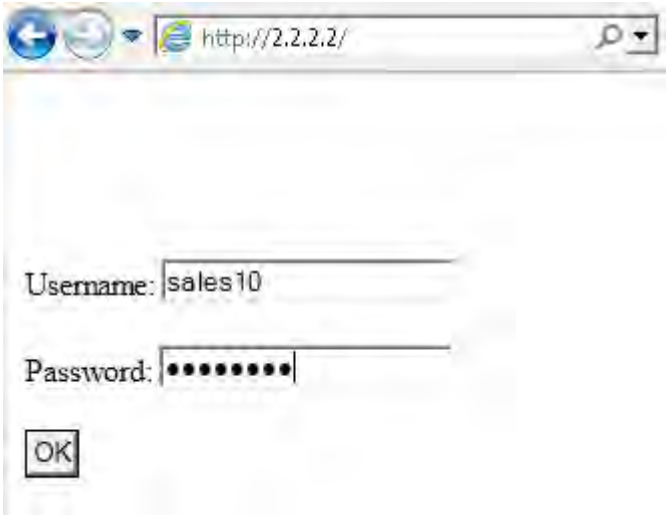
Test PC :

```
route add 2.2.2.2 mask 255.255.255.255 172.41.41.4
route add 6.6.6.6 mask 255.255.255.255 172.41.41.4
```

Remove any access-lists in transit between R4 and R2 (e.g. on R6):

```
R6(config)#int s0/1/0
R6(config-if)#no ip access-group OUTSIDE_IN in
```

We will now connect as “sales10” user who is part of the SALES_GROUP:



Authentication Summary	
Logged At:	March 25,2013 2:00:50.279 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	sales10
MAC/IP Address:	
Network Device:	R4 : 4.4.4.4 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	AUTHZ_PROF_SALES_ZFW
SGA Security Group:	
Authentication Protocol :	PAP_ASCII

Authentication Result

User-Name=sales10
State=ReauthSession:0ac806f40000000451505892
Class=CACS:0ac806f40000000451505892:pod124ise/152384777/5
Termination-Action=RADIUS-Request
cisco-av-pair=supplicant-group=SALES
cisco-av-pair=auth-proxy:priv-lvl=15
cisco-av-pair=auth-proxy:proxyacl#1=permit ip any any

And take a look at partial debugs from “debug radius”, “debug user-group all” and “debug epm all”:

```
*Mar 25 14:01:55.764: RADIUS(00000023): Send Access-Request to
172.41.41.150:1645 id 1645/4, len 89
*Mar 25 14:01:55.764: RADIUS: authenticator 05 30 46 08 76 9F EF 38 - B5 C1
B7 A6 00 7C 45 45
*Mar 25 14:01:55.764: RADIUS: User-Name [1] 9 "sales10"
*Mar 25 14:01:55.764: RADIUS: User-Password [2] 18 *
*Mar 25 14:01:55.768: RADIUS: Framed-IP-Address [8] 6 172.41.41.200
*Mar 25 14:01:55.768: RADIUS: Service-Type [6] 6 Outbound
[5]


*Mar 25 14:01:55.784: RADIUS: Received from id 1645/4 172.41.41.150:1645,
Access-Accept, len 253
*Mar 25 14:01:55.784: RADIUS: authenticator 03 98 BC A7 BA F5 05 6B - FE 0A
52 67 97 6D F2 F1
*Mar 25 14:01:55.788: RADIUS: User-Name [1] 9 "sales10"
*Mar 25 14:01:55.788: RADIUS: State [24] 40
*Mar 25 14:01:55.788: RADIUS: 52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30
61 [ReauthSession:0a]
*Mar 25 14:01:55.788: RADIUS: 63 38 30 36 66 34 30 30 30 30 30 30 30 34 35
31 [c806f40000000451]
*Mar 25 14:01:55.788: RADIUS: 35 30 35 38 39 32 [ 505892]
```

```
*Mar 25 14:01:55.788: RADIUS:  Class               [25]  53
*Mar 25 14:01:55.788: RADIUS:   43 41 43 53 3A 30 61 63 38 30 36 66 34 30 30
30  [CACS:0ac806f4000]
*Mar 25 14:01:55.788: RADIUS:   30 30 30 30 34 35 31 35 30 35 38 39 32 3A 70
6F  [0000451505892:po]
*Mar 25 14:01:55.788: RADIUS:   64 31 32 34 69 73 65 2F 31 35 32 33 38 34 37
37  [d124ise/15238477]
*Mar 25 14:01:55.788: RADIUS:   37 2F 35              [ 7/5]
*Mar 25 14:01:55.788: RADIUS:  Termination-Action  [29]  6   1
*Mar 25 14:01:55.788: RADIUS:  Message-Authenticato[80]  18
*Mar 25 14:01:55.788: RADIUS:   80 D1 0B 47 39 0E 0B BF E6 20 6F 32 8A E8 05
F9             [ G9 o2]
*Mar 25 14:01:55.788: RADIUS:  Vendor, Cisco       [26]  30
*Mar 25 14:01:55.788: RADIUS:    Cisco AVpair         [1]    24   "supplicant-
group=SALES"
*Mar 25 14:01:55.788: RADIUS:  Vendor, Cisco       [26]  30
*Mar 25 14:01:55.788: RADIUS:    Cisco AVpair          [1]    24   "auth-
proxy:priv-lvl=15"
*Mar 25 14:01:55.788: RADIUS(00000023): Received from id 1645/4


*Mar        25        14:01:55.804:        EPM_SESS_EVENT:In        function
epm_parse_aaa_access_policies
*Mar 25 14:01:55.804: EPM_SESS_EVENT:Proxy ACE: permit ip any any received
*Mar 25 14:01:55.804: EPM_SESS_EVENT:Recieved string tmpProxyACL-3221225476
*Mar 25 14:01:55.804: EPM_SESS_EVENT:Create nACL tmpProxyACL-3221225476 with
ACE=permit ip any any
*Mar 25 14:01:55.812: EPM_SESS_EVENT:Executed [ip access-list extended
tmpProxyACL-3221225476] command through parse_cmd. Result= 0
*Mar 25 14:01:55.816: EPM_SESS_EVENT:Executed [permit ip any any] command
through parse_cmd. Result= 0
*Mar 25 14:01:55.820: EPM_SESS_EVENT:Executed [end] command through
parse_cmd. Result= 0
*Mar 25 14:01:55.824: EPM_SESS_EVENT:Username sales10
*Mar 25 14:01:55.824: EPM_SESS_EVENT:Identity usergroup name SALES


*Mar 25 14:01:55.824: USRGRP-API: [Type=IPv4 Val=172.41.41.200 Group=SALES]:
Usergroup opcode entry addition.
*Mar 25 14:01:55.824: USRGRP-DB: Group=SALES Count=0: New usergroup db
created.
*Mar 25 14:01:55.824: USRGRP-ENTRY: [Type=IPv4 Val=172.41.41.200 ::
Group=SALES Count=1]: Usergroup entry added
*Mar 25 14:01:55.824: EPM_SESS_ERR:IP=172.41.41.200: Membership [Addition] to
usergroup=SALES swidb=FastEthernet0/1 [Success]
```

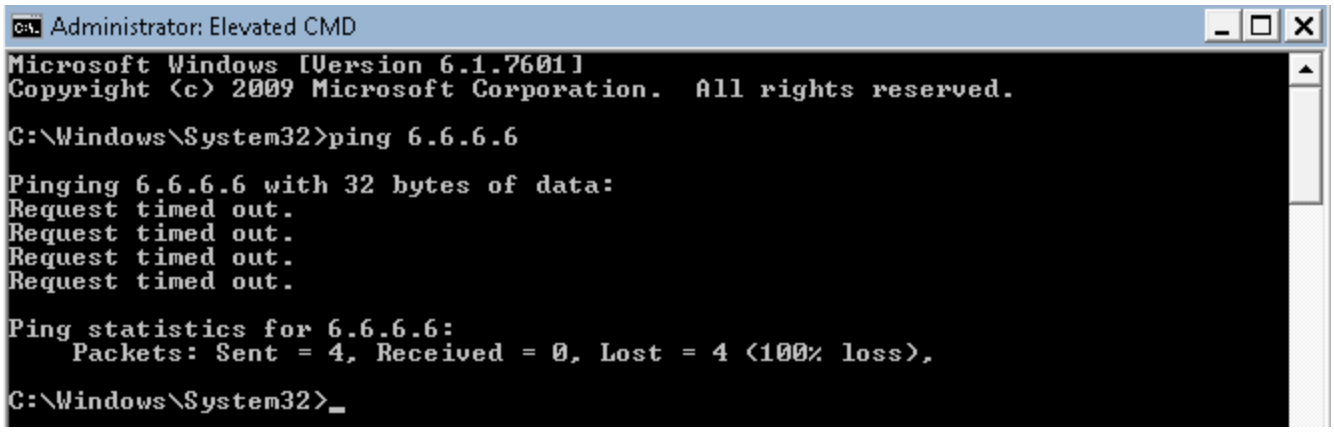
Based on the above information we can conclude user “sales10” was associated with the “SALES” user-group. Since “sales10” is coming from 172.41.41.200, this IP address will be used as the source filter criteria. Additional verification won’t hurt, though:

```
R4#show epm session ip 172.41.41.200
Admission feature       : Authproxy
AAA Policies            :
Supplicant-Group        : SALES

R4#sh user-group
Usergroup : SALES
-------------------------------------------------------------------------
User Name       Type     Interface               Learn          Age (min)
-------------------------------------------------------------------------
172.41.41.200   IPv4     FastEthernet0/1         Dynamic          5
```

This is our ZFW policy:

```
R4#sh policy-firewall config zone-pair INOUT
Zone-pair               : INOUT
Source Zone             : IN
Destination Zone        : OUT
Service-policy inspect : ZFW_INOUT_POL
  Class-map : ZFW_SALES_TCP_CLASS(match-all)
   Match protocol tcp
   Match access-group name TO_R6
   Match user-group SALES
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_ADMIN_TCP_CLASS(match-all)
   Match protocol tcp
   Match user-group ADMINS
  Action : inspect
   Parameter-map : Default

  Class-map : ZFW_ADMIN_ICMP_CLASS(match-all)
   Match protocol icmp
   Match user-group ADMINS
  Action : inspect
   Parameter-map : Default

  Class-map : class-default(match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

OK, let's try to ping R6 and then telnet to it. Only telnet should be successful based on our policy:

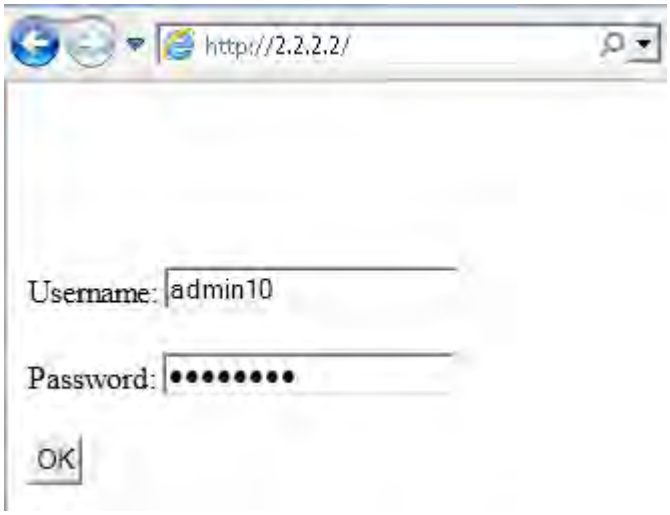



```
*Mar 25 14:09:35.804: %FW-6-DROP_PKT: Dropping icmp session 172.41.41.200:0
6.6.6.6:0 on zone-pair INOUT class class-default due to DROP action found in
policy-map with ip ident 0
```


```
R4#sh policy-firewall session zone-pair INOUT
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_SALES_TCP_CLASS(match-all)
      Established Sessions =  1
        Session      49D89CE0      (172.41.41.200:50072)=>(6.6.6.6:23)      tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:17, Last heard 00:00:12
          Bytes sent (initiator:responder) [34:26]
    Class-map : ZFW_ADMIN_TCP_CLASS(match-all)
    Class-map : ZFW_ADMIN_ICMP_CLASS(match-all)
    Class-map : class-default(match-any)

Also we will not be able to send any TCP traffic through our firewall to
anything else than R6 :

R4#
*Mar    25    14:12:44.388:    %FW-6-DROP_PKT:    Dropping    tcp    session
172.41.41.200:50233 2.2.2.2:23 on zone-pair INOUT class class-default due to
DROP action found in policy-map with ip ident 0
```

Time to test the “admin10” user (ADMIN_GROUP tagged as “ADMINS”):

```
R4#clear ip admission cache *
```



Authentication Summary	
Logged At:	March 25,2013 2:16:22.197 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	admin10
MAC/IP Address:	
Network Device:	R4 : 4.4.4.4 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	AUTHZ_PROF_ADMINS_ZFW
SGA Security Group:	
Authentication Protocol :	PAP_ASCII

Authentication Result

User-Name=admin10
State=ReauthSession:0ac806f40000000551505C36
Class=CACS:0ac806f40000000551505C36:pod124ise/152384777/6
Termination-Action=RADIUS-Request
cisco-av-pair=supplicant-group=ADMINS
cisco-av-pair=auth-proxy:priv-lvl=15
cisco-av-pair=auth-proxy:proxyacl#1=permit ip any any

```
*Mar 25 14:17:27.728: RADIUS: Received from id 1645/5 172.41.41.150:1645,
Access-Accept, len 254
*Mar 25 14:17:27.728: RADIUS:  authenticator 74 6D 75 BD 2B 5E 27 8F - 10 18
AB 0B 8A D9 82 B7
*Mar 25 14:17:27.728: RADIUS:  User-Name           [1]   9   "admin10"
*Mar 25 14:17:27.728: RADIUS:  State               [24]  40
*Mar 25 14:17:27.728: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30
61  [ReauthSession:0a]
*Mar 25 14:17:27.728: RADIUS:   63 38 30 36 66 34 30 30 30 30 30 30 30 35 35
31  [c806f40000000551]
```

```
*Mar 25 14:17:27.728: RADIUS:   35 30 35 43 33 36            [ 505C36]
*Mar 25 14:17:27.728: RADIUS:  Class               [25]  53
*Mar 25 14:17:27.728: RADIUS:   43 41 43 53 3A 30 61 63 38 30 36 66 34 30 30
30  [CACS:0ac806f4000]
*Mar 25 14:17:27.732: RADIUS:   30 30 30 30 35 35 31 35 30 35 43 33 36 3A 70
6F  [0000551505C36:po]
*Mar 25 14:17:27.732: RADIUS:   64 31 32 34 69 73 65 2F 31 35 32 33 38 34 37
37  [d124ise/15238477]
*Mar 25 14:17:27.732: RADIUS:   37 2F 36               [ 7/6]
*Mar 25 14:17:27.732: RADIUS:  Termination-Action  [29]  6   1
*Mar 25 14:17:27.732: RADIUS:  Message-Authenticato[80]  18
*Mar 25 14:17:27.732: RADIUS:   A8 7C B1 BF E1 35 75 67 56 69 62 94 43 3C 4F
8F        [ |5ugVibC<O]
*Mar 25 14:17:27.732: RADIUS:  Vendor, Cisco       [26]  31
*Mar 25 14:17:27.732: RADIUS:    Cisco AVpair         [1]    25   "supplicant-
group=ADMINS"
*Mar 25 14:17:27.732: RADIUS:  Vendor, Cisco       [26]  30
*Mar 25 14:17:27.732: RADIUS:    Cisco AVpair           [1]    24   "auth-
proxy:priv-lvl=15"
*Mar 25 14:17:27.732: RADIUS(00000024): Received from id 1645/5


R4#sh epm sess ip 172.41.41.200
Admission feature       : Authproxy
AAA Policies            :
Supplicant-Group        : ADMINS

R4#sh user-group
Usergroup : ADMINS
-------------------------------------------------------------------------
User Name       Type     Interface              Learn         Age (min)
-------------------------------------------------------------------------
172.41.41.200   IPv4     FastEthernet0/1        Dynamic         1
```

Ping and telnet to test. Administrators are not restricted to any certain destination IP:

```
C:\Windows\System32>ping 2.2.2.2

Pinging 2.2.2.2 with 32 bytes of data:
Reply from 2.2.2.2: bytes=32 time=15ms TTL=253
Reply from 2.2.2.2: bytes=32 time=12ms TTL=253
Reply from 2.2.2.2: bytes=32 time=12ms TTL=253
Reply from 2.2.2.2: bytes=32 time=12ms TTL=253

Ping statistics for 2.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 15ms, Average = 12ms

C:\Windows\System32>ping 6.6.6.6

Pinging 6.6.6.6 with 32 bytes of data:
Reply from 6.6.6.6: bytes=32 time=15ms TTL=254
Reply from 6.6.6.6: bytes=32 time=12ms TTL=254
Reply from 6.6.6.6: bytes=32 time=12ms TTL=254
Reply from 6.6.6.6: bytes=32 time=12ms TTL=254

Ping statistics for 6.6.6.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 15ms, Average = 12ms

C:\Windows\System32>_
```

```
R4#sh policy-firewall ses zone INOUT
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_SALES_TCP_CLASS(match-all)
    Class-map : ZFW_ADMIN_TCP_CLASS(match-all)
      Established Sessions =  2
        Session      49D8AE60      (172.41.41.200:50335)=>(2.2.2.2:23)      tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:19, Last heard 00:00:19
          Bytes sent (initiator:responder) [31:23]
        Session      49D8B1E0      (172.41.41.200:50336)=>(6.6.6.6:23)      tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:15, Last heard 00:00:15
          Bytes sent (initiator:responder) [31:23]
    Class-map : ZFW_ADMIN_ICMP_CLASS(match-all)
      Established Sessions =  1
        Session 49D8B560 (172.41.41.200:8)=>(2.2.2.2:0) icmp SIS_OPEN
          Created 00:00:02, Last heard 00:00:00
          ECHO request
          Bytes sent (initiator:responder) [96:96]
    Class-map : class-default(match-any)
```

Section 3: WSA Solutions

Lab-1: WSA Initialization Overview

Lab-1: WSA Initialization – This lab is intended to familiarize you with the initialization of the WSA to act as a web proxy, customizing EUN, testing basic proxy functions using PAC files for Firefox and integrating WSA with Active Directory for user authentication. We shall start configuring WSA initially in explicit forward proxy mode and later labs will focus on transparent mode.

We highly recommend creating your own diagram at the beginning of each lab so you are able to draw on your own diagram, making it much easier when you step into the real lab.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- Make it a common practice to verify the pre-configurations loaded on the devices.

Estimated Time to Complete: **1.5 Hour**

Pre-setup

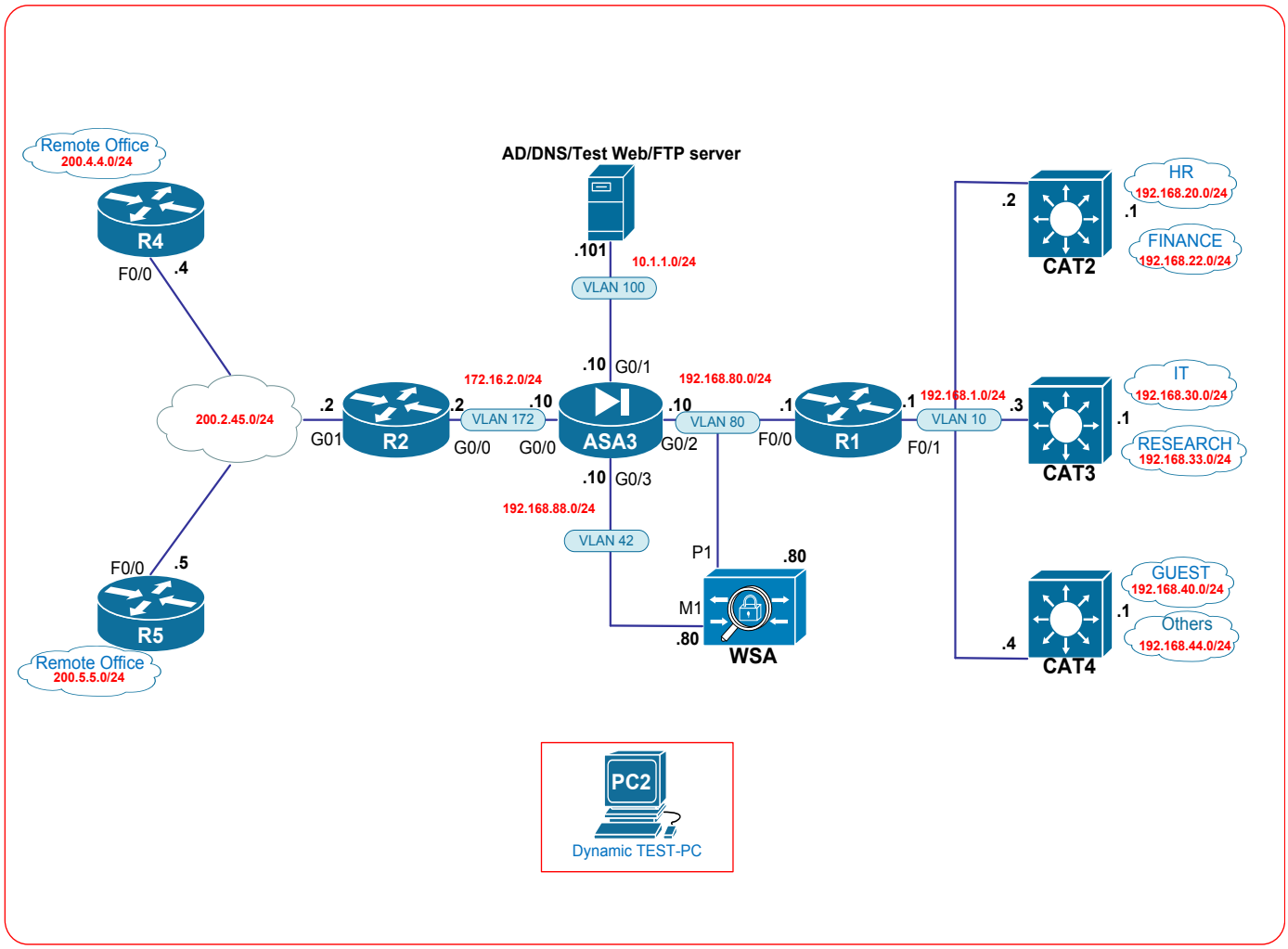
Load the initial configurations for the ASA, routers and switches. Note that routers and switches are pre-configured with these initial configurations.

NOTE: *Do not make additional configuration on the ASA and routers, unless explicitly asked for in the task; some switching configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 3.1 (Logical)



Lab 1: Configuration Tasks

Task 1: Initialization WSA

- Configure appropriate VLAN's on the switch for WSA as per topology diagram 3.1.
- Bootstrap WSA using GUI with system setup wizard. Therefore place TEST-PC in VLAN-42 and connect to the WSA using the factory default IP address and port. Use any IP for the TEST-PC to match the factory default subnet of WSA.
- Configure the below parameters when the system setup starts.

Network Settings	
Default System Hostname	wsa.ipexpert.com
DNS Servers	10.1.1.101
Network Time Protocol (NTP)	(Default)
Time Zone	America/New_York
Upstream proxy	none
Interface Management (M1): IP Address and Hostname	192.168.88.80/24 wsam1.ipexpert.com
M1 Management Access	Use M1 only for Management Access
Interface Proxy (P1): IP Address and Hostname	192.168.80.80/24 wsa.ipexpert.com
L4 Traffic Monitor	Duplex TAP: T1 (In/Out)
Default Gateway	M1 - 192.168.88.10 P1 - 192.168.80.10
Static Routes for P1	Network-192.168.0.0/16 Gateway-192.168.80.1
Transparent Connection Settings	None- Only explicit forward proxy
Email System Alerts To	admin@ipexpert.com
Internal SMTP Relay Hosts	mail.ipexpert.com
Administrator Password	"ironport" (Uncheck Autosupport and sender base participation)

Security Settings	
L4 Traffic Monitor	Monitoring
Acceptable Use Controls	Enabled
Active Acceptable Use Controls Engine	Cisco IronPort Web Usage Controls
Web Reputation Filters	Enabled
IronPort DVS™ Engine	Webroot: Enabled McAfee: Enabled Sophos: Enabled
IronPort Data Security Filtering	Enabled

NOTE: *After you install the above configuration you will lose access to the WSA since the IP address of WSA changes from the factory default IP.*

Detailed Solution: Lab-1

Task-1

Summary Guidelines

8. Make sure you know the physical and logical topology well
9. Do not start configuring tasks linearly. Read the entire lab to identity any dependency with other tasks and then proceed to configure.
10. Pre- load the configurations and check if the loaded configuration is correct
11. Before you begin with configuring the WSA. Configure the Layer-2 i.e. switch with VLAN's/Trunks
12. Once Layer 2 is in order. You may begin configuring the WSA which is in factory default.
13. When using the test PC, do not set the default gateway. Add static routes for reachability. You may also need to change the VLAN's for the PC accordingly.
14. Always use "students NIC/ inside NIC" on the test PC to change the IP.
15. **Do not change the password of WSA. Always use and configure admin/ironport**
16. Make sure the appropriate VLAN's are created on the switches as per the topology.

Step 1: Layer 2 configuration

Network Topology 3.1 is a logical topology. Physically all the Ethernet interfaces of routers and WSA are connected to switches. Hence we need to first build the layer 2 and then proceed to the layer 3 part of the configuration. Please refer the physical connection topology.

If the appropriate VLAN's are not created then you may create them. However if you do create them make sure the VLAN number matches with the topology.

Create appropriate VLAN's as per topology:

SW2

```
Vlan 20,22
```

SW3

```
Vlan 30,33,42,80,88
```

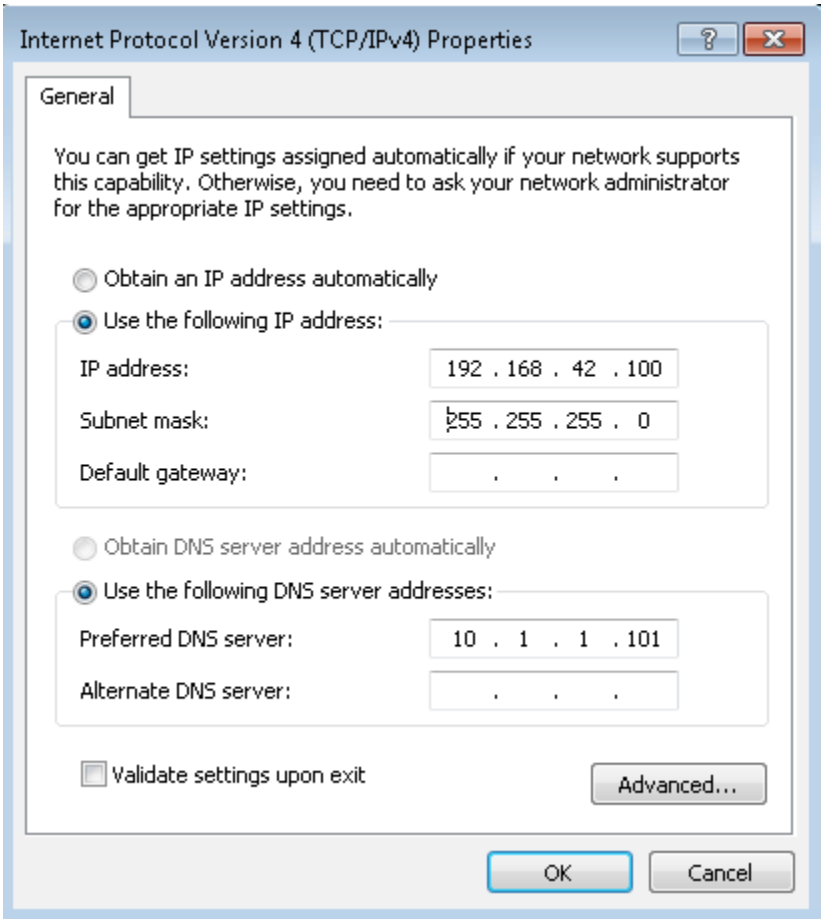
SW4

```
Vlan 40,44
```

SW3

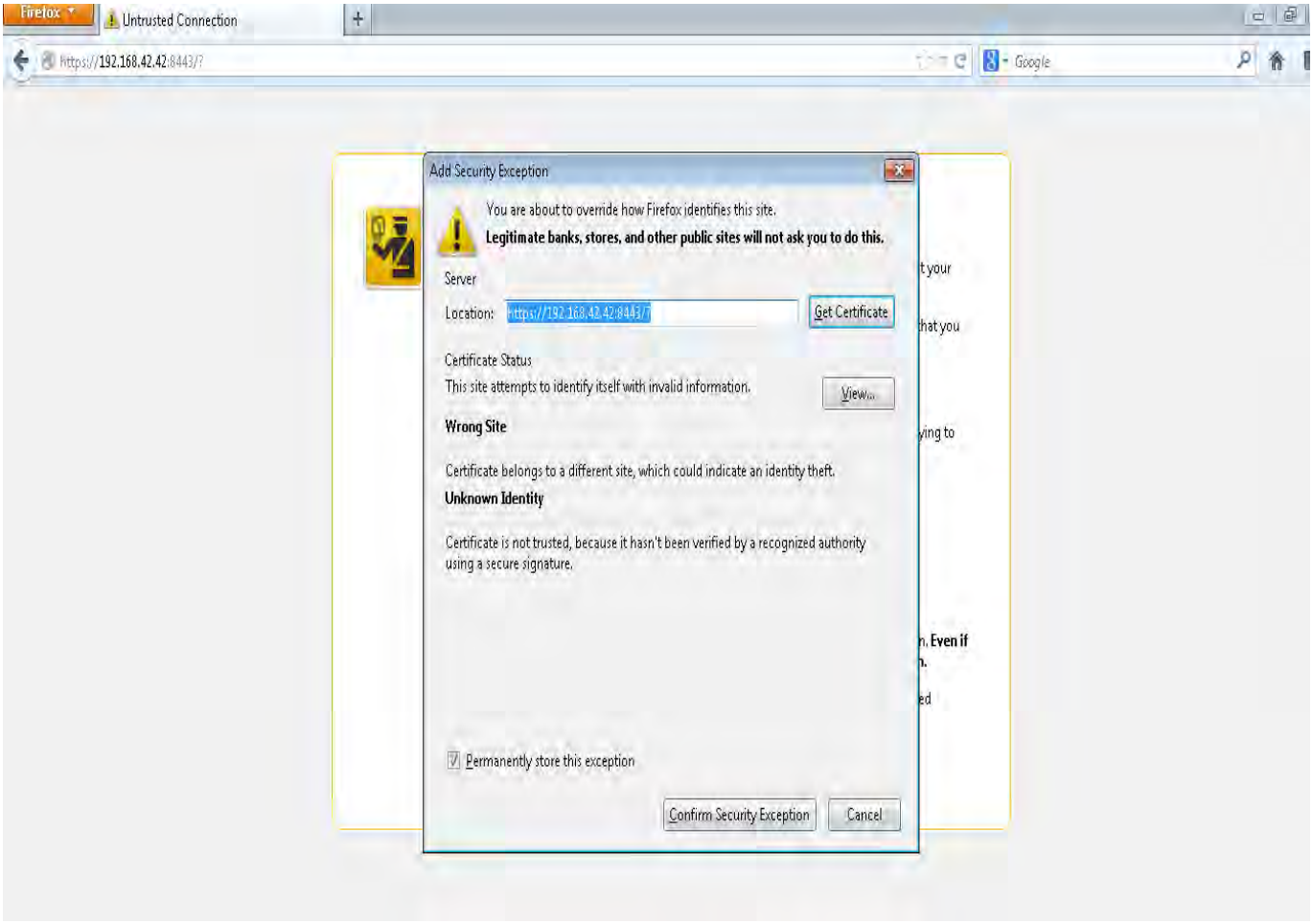
```
interface GigabitEthernet1/0/3
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/4
 switchport access vlan 80
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/2
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
```

Step 2: RDP into test PC 1 or 2. Here we are using test PC 1. Change the IP address of the test PC to 192.168.42.100. Do not set the default gateway. Do not set the default gateway.

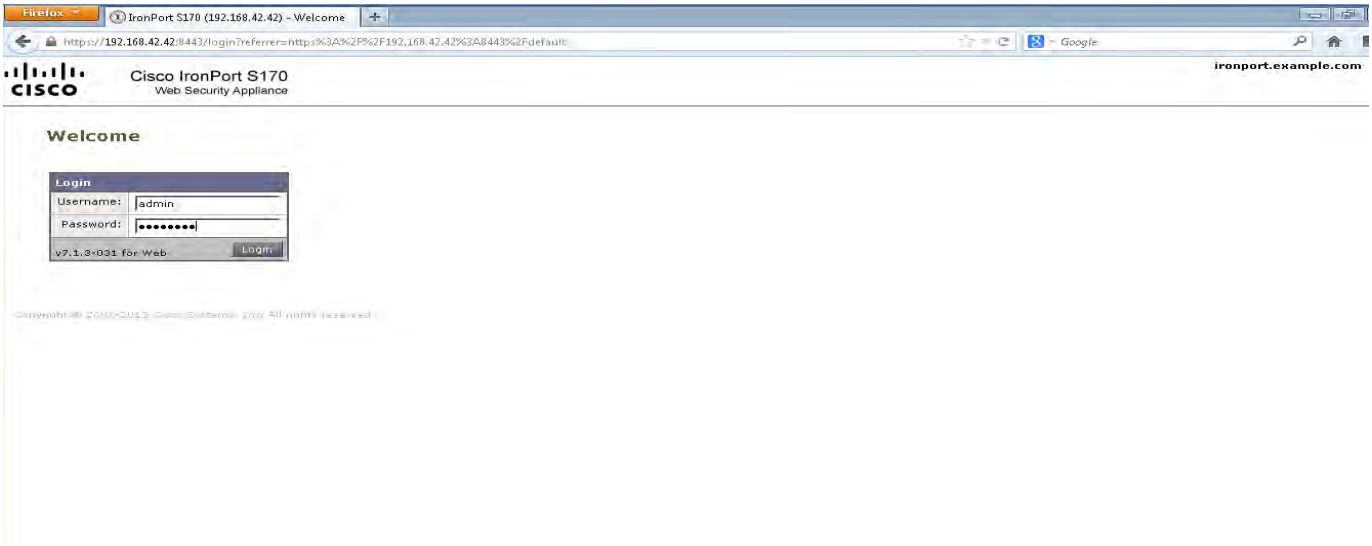


Step 3: Login to the WSA GUI using http://192.168.42.42:8080. This will automatically start the system setup wizard. Then you may begin network and security settings as per task.

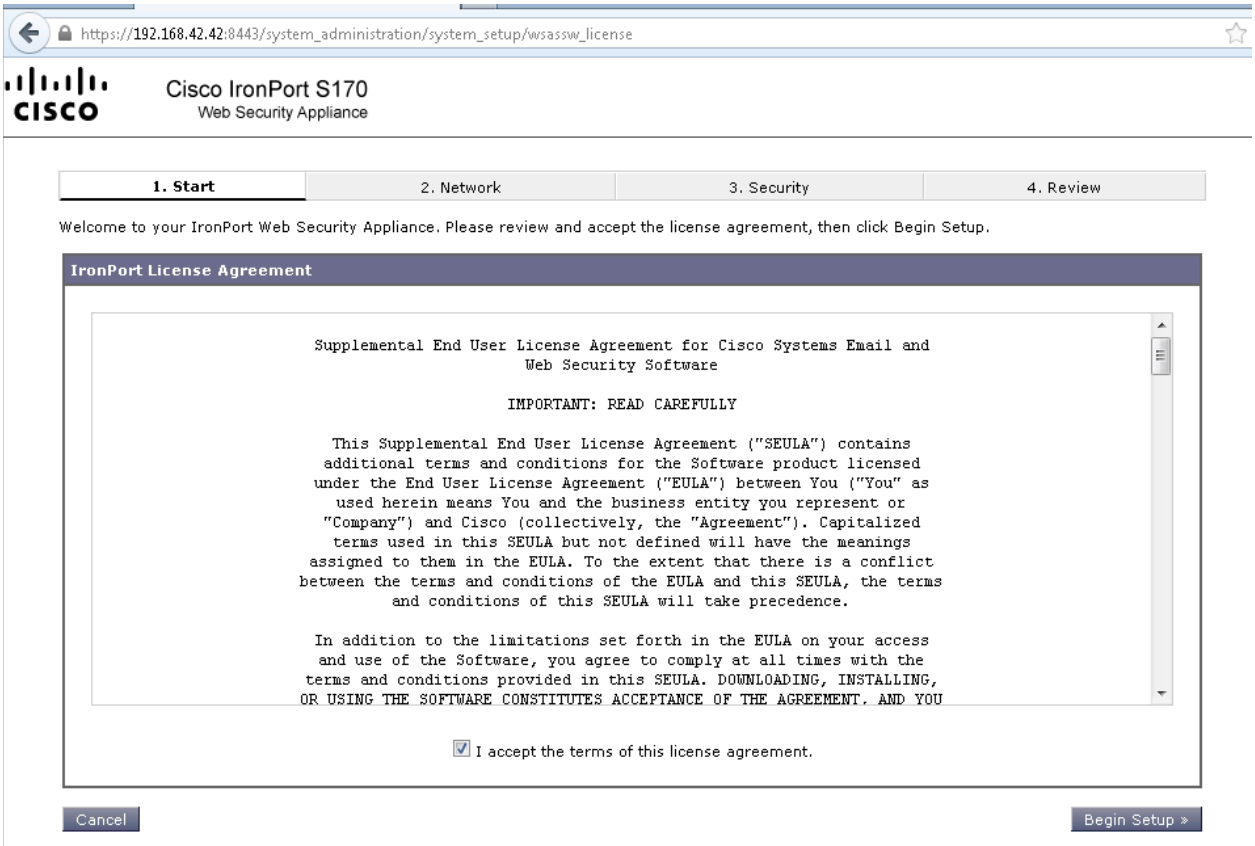
Trust the certificate and confirm the security exception.



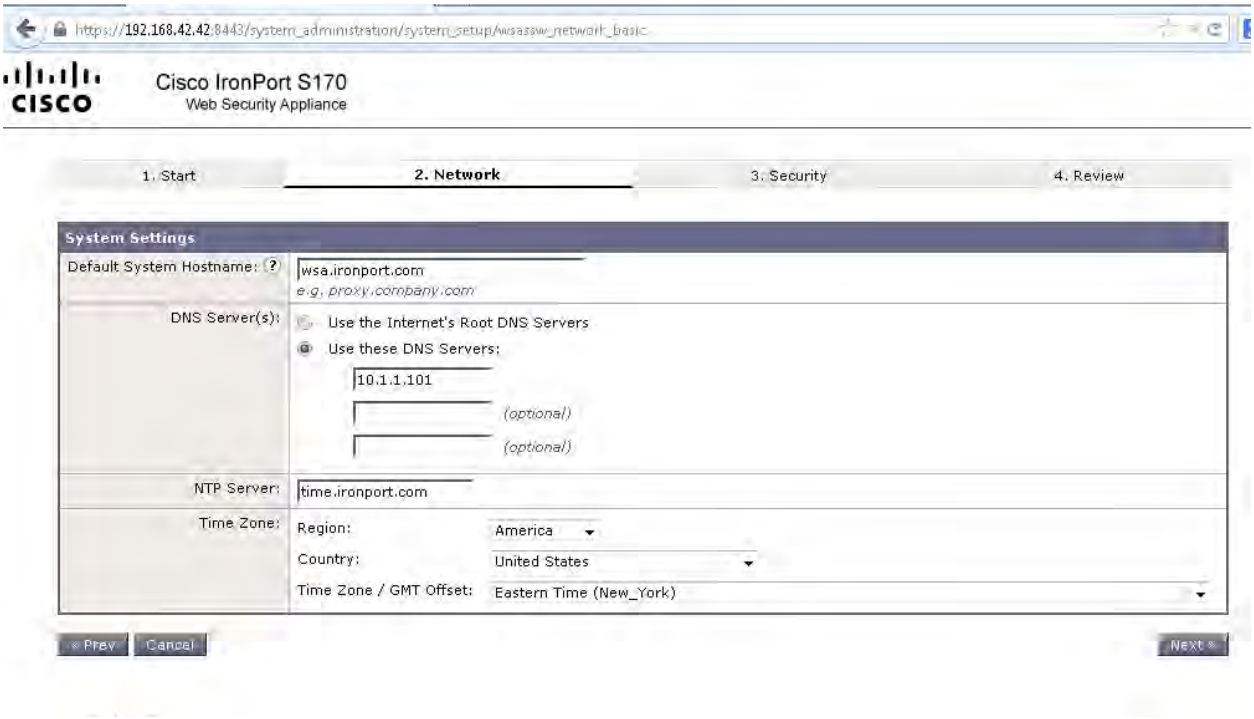
Use the credentials of admin/ironport to login



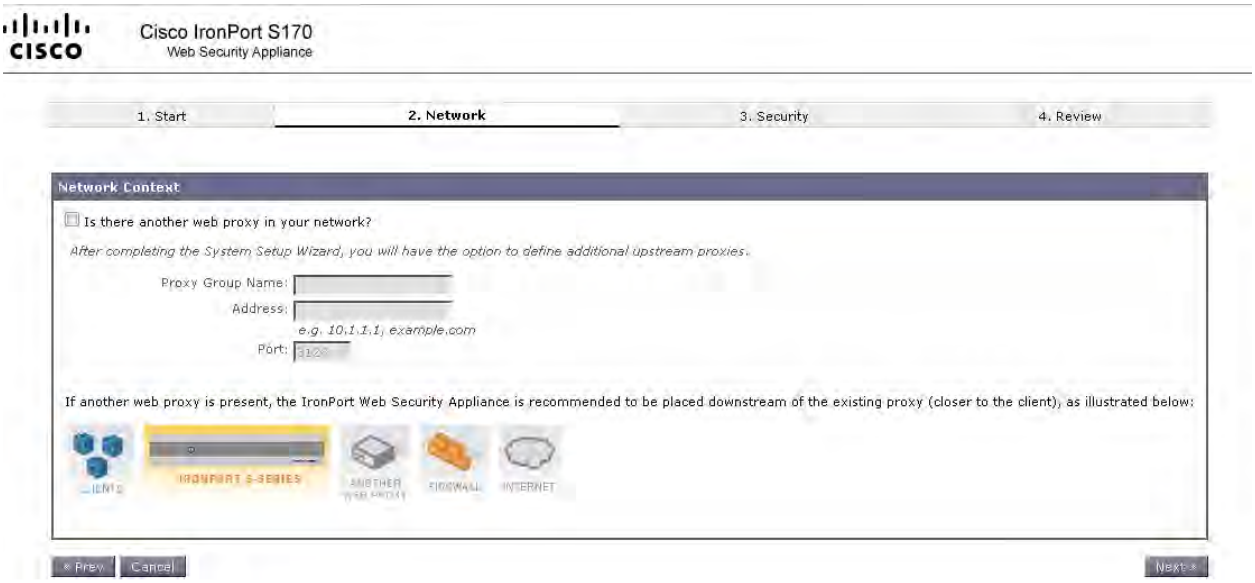
Accept the license agreement to begin system setup wizard.



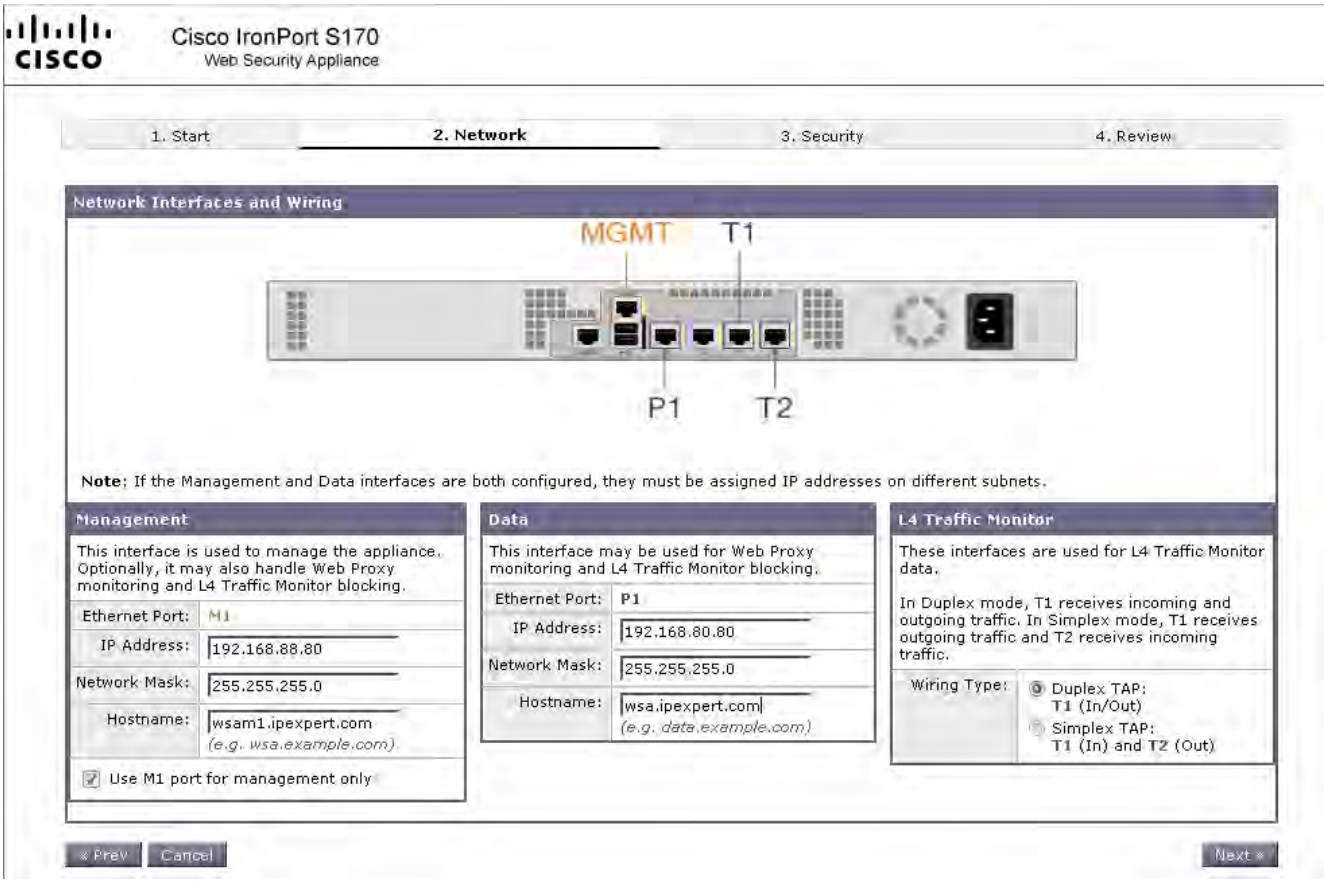
Configure the hostname, DNS and time zone. Leave the NTP settings as default and click next.



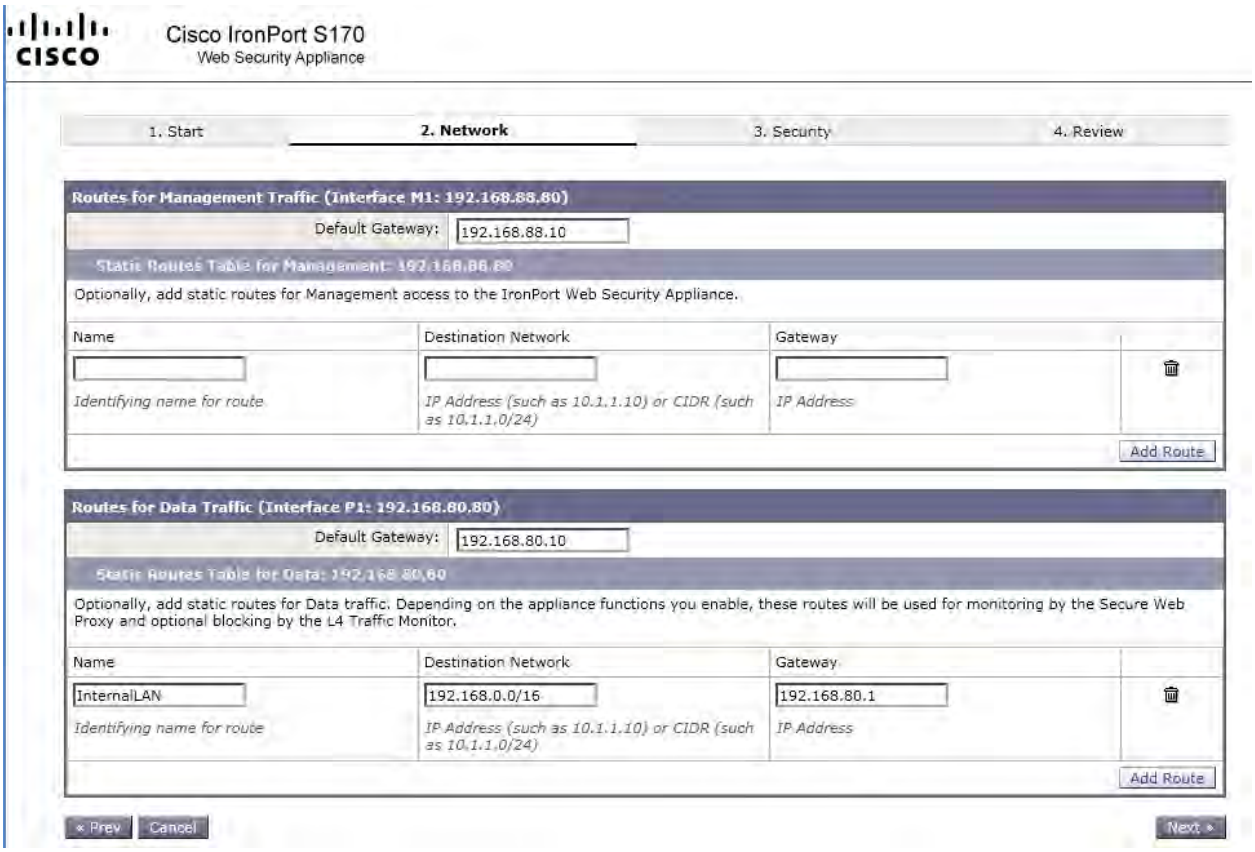
Click Next since there are no upstream proxy in the network



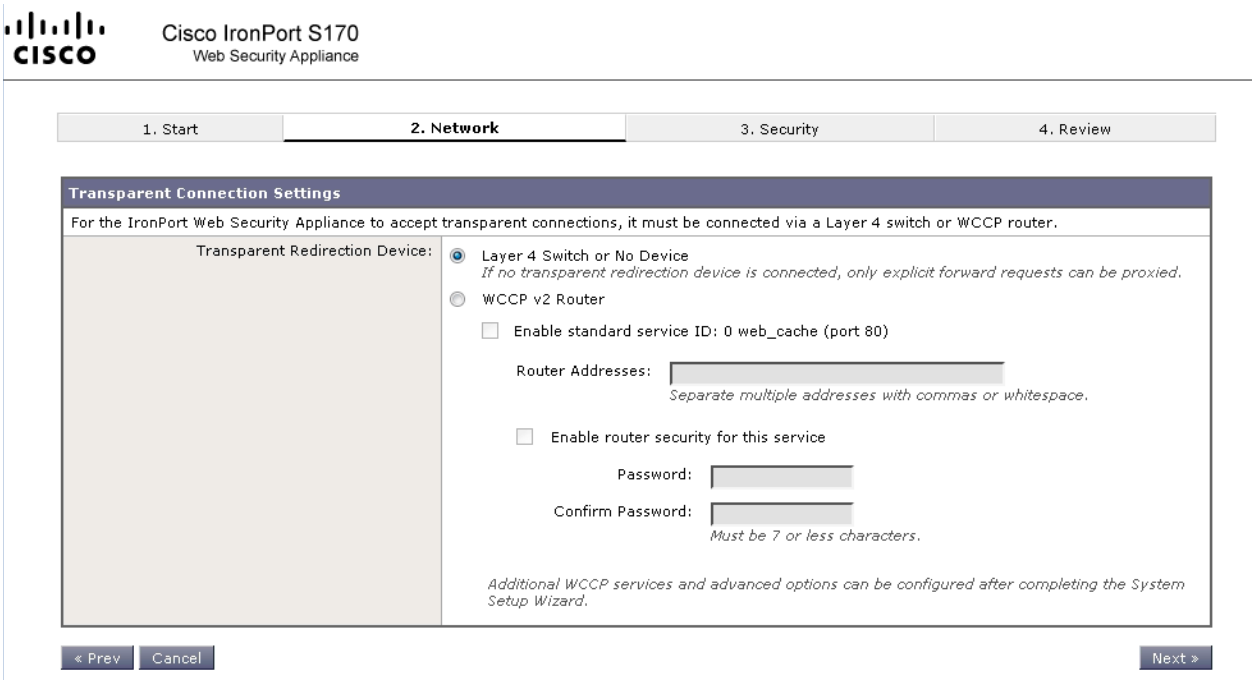
Configure the M1 and P2 interfaces as per task



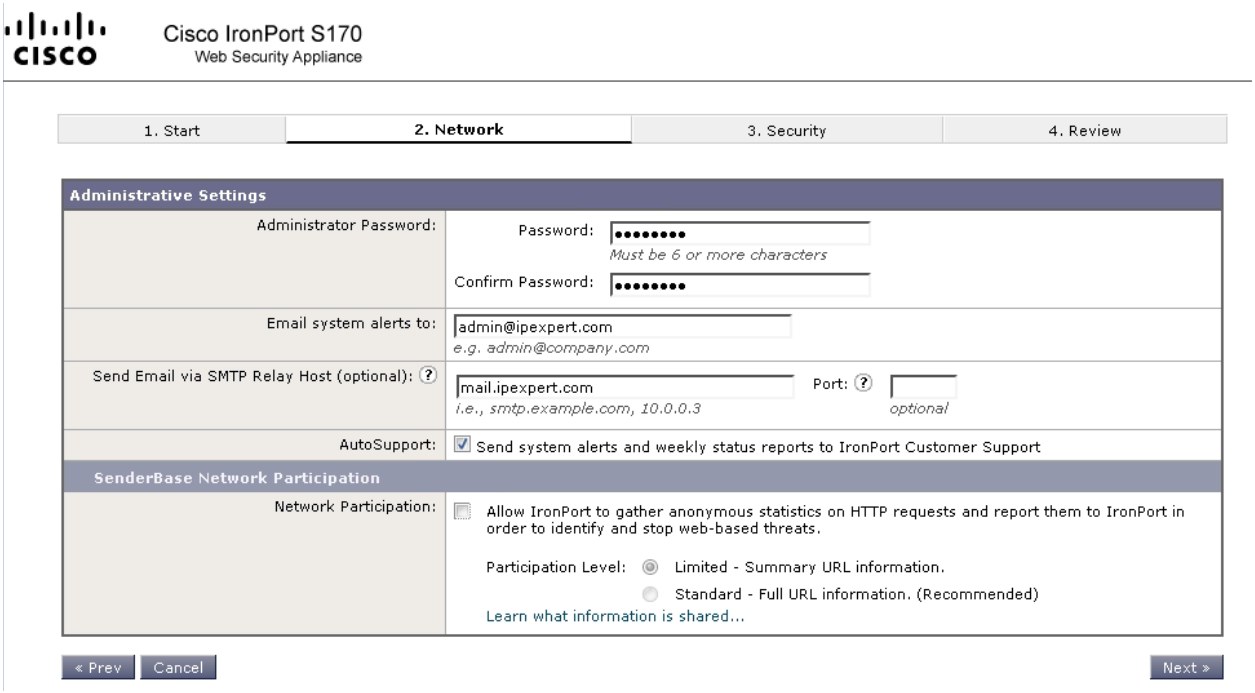
Add the appropriate default routes



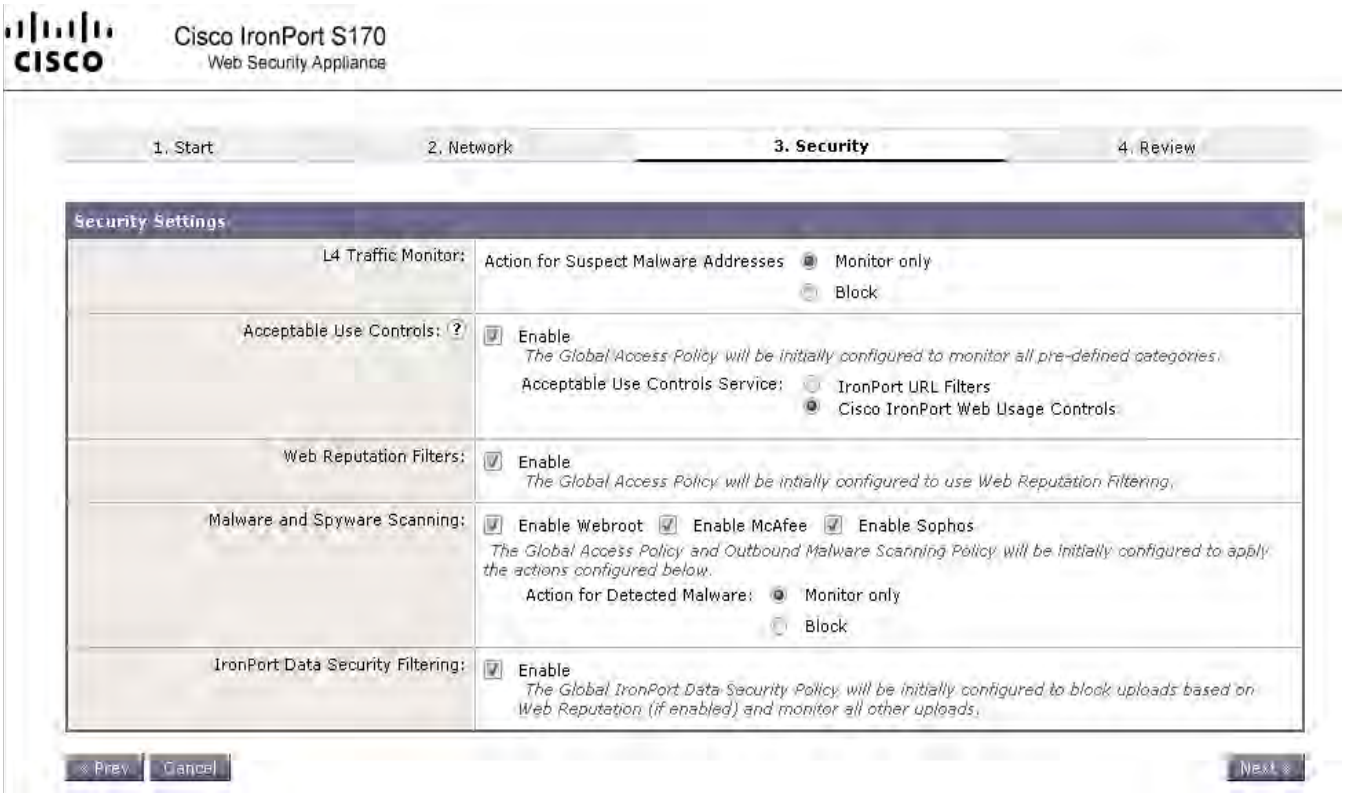
Do not enable WCCP/transparent redirection



Use “ironport” as the password and configure email alert settings. Uncheck senderbase participation.



Configure security settings as per task. Since the task does not state to configure action for malware detection, just leave to default of “Monitor Only”



Review the configuration summary and install. You may lose connectivity since the IP address of the WSA changes. Hence after installation change the IP address of the PC to 192.168.88.100 or to any IP of VLAN 42 subnet

Cisco IronPort S170
Web Security Appliance

1. Start | 2. Network | 3. Security | **4. Review**

Review Your Configuration

Printable Page

Please review your configuration. If you need to make changes, click the Previous button to return to the previous page.

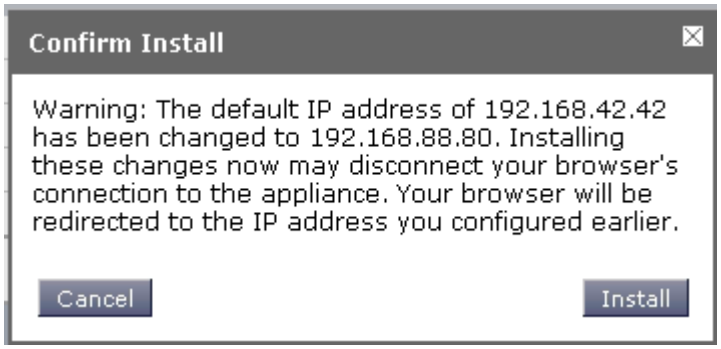
Network Settings	Edit
Default System Hostname:	wsa.ironport.com
DNS Servers:	10.1.1.101
Network Time Protocol (NTP):	time.ironport.com
Time Zone:	America/New_York
Network Context	
Upstream proxy:	No upstream proxy
Interfaces	Edit
Management (M1)	
IP Address:	192.168.88.80
Network Mask:	255.255.255.0
Hostname:	wsam1.ipexpert.com
Use M1 port for management only:	Yes
Data (P1)	
IP Address:	192.168.80.80
Network Mask:	255.255.255.0
Hostname:	wsa.ipexpert.com

SenderBase Network Participation:	No

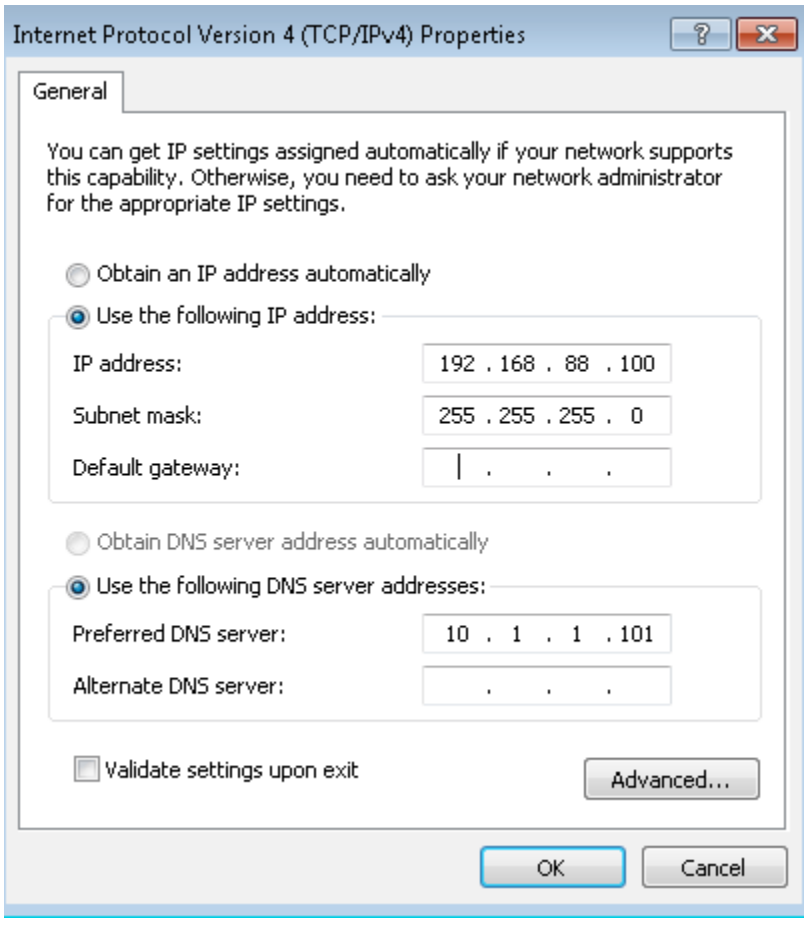
Security Settings	Edit
L4 Traffic Monitor:	Monitoring
Acceptable Use Controls:	Enabled Active Acceptable Use Controls Engine: Cisco IronPort Web Usage Controls
Web Reputation Filters:	Enabled
IronPort DVS™ Engine:	Webroot: Enabled McAfee: Enabled Sophos: Enabled
IronPort Data Security Filtering:	Enabled

« Previous | Cancel | Install This Configuration

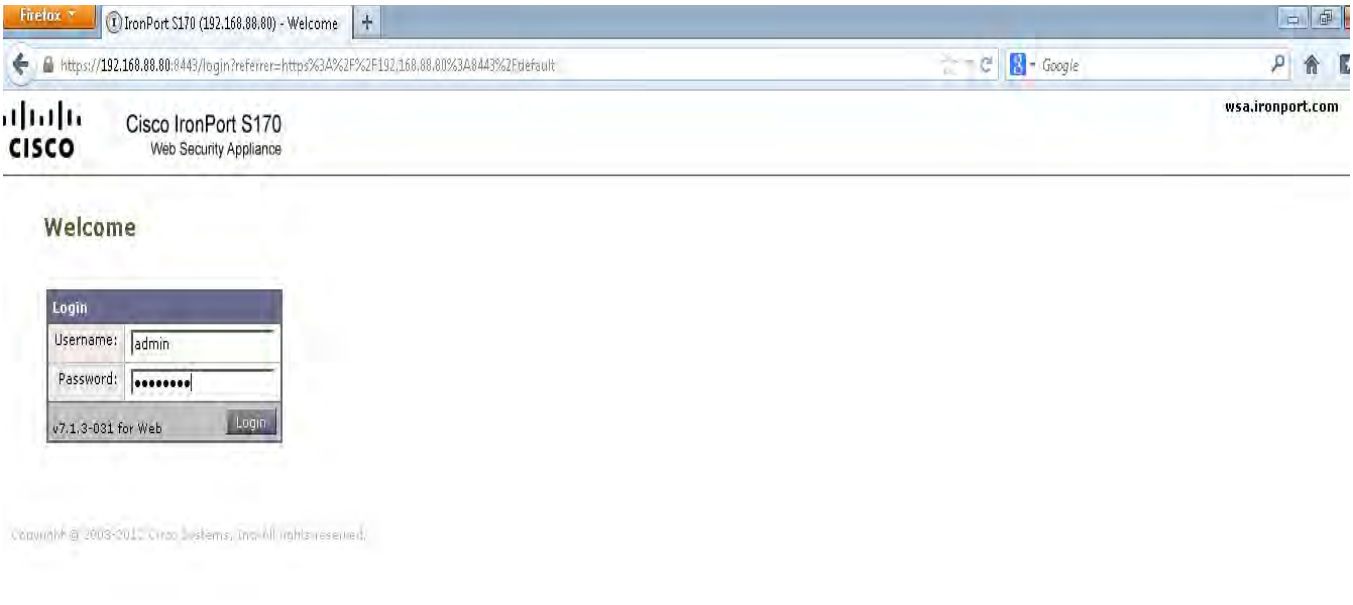
Confirm the installation

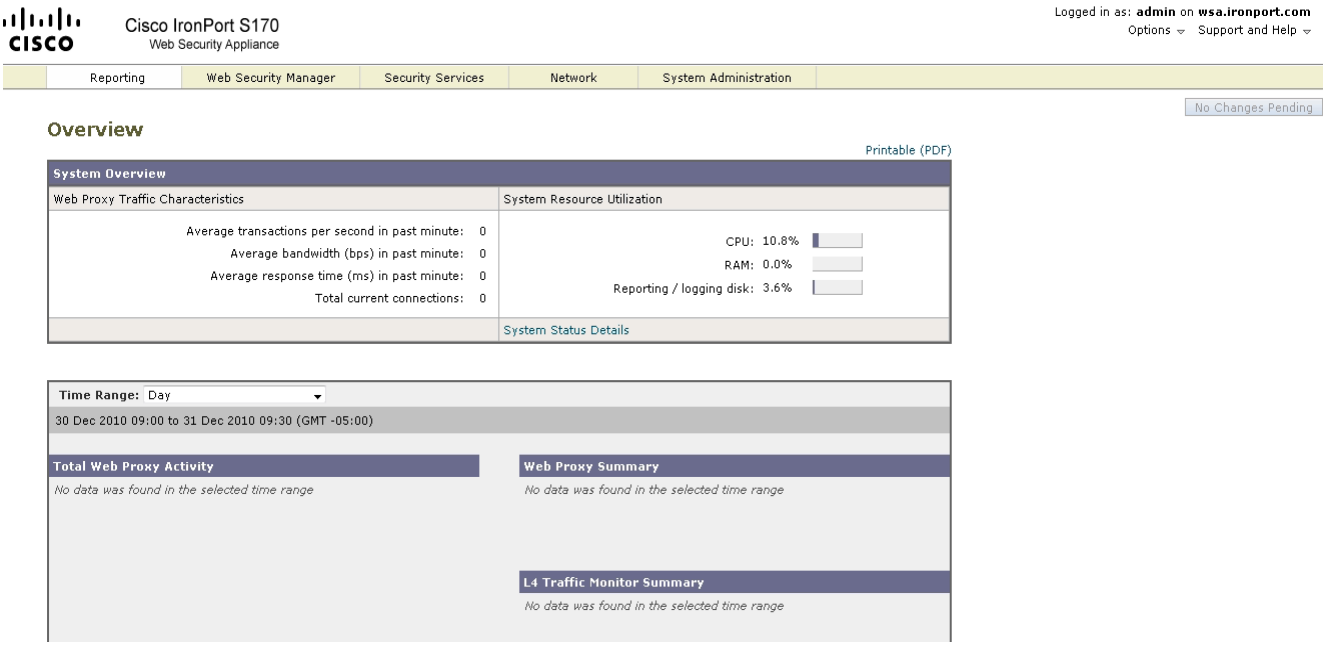


You will lose access to the WSA now. Hence re-configure the IP of the TEST PC and re-login to the WSA using 192.168.88.80



Login using admin/ironport





Task 2: Enable basic web and FTP proxy function and PAC file hosting

- Place the TEST-PC in VLAN 20 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally, configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW2 SVI VLAN 20 as the next hop.

NOTE: ***Do not set the default gateway when you change the IP address else you will lose RDP access.***

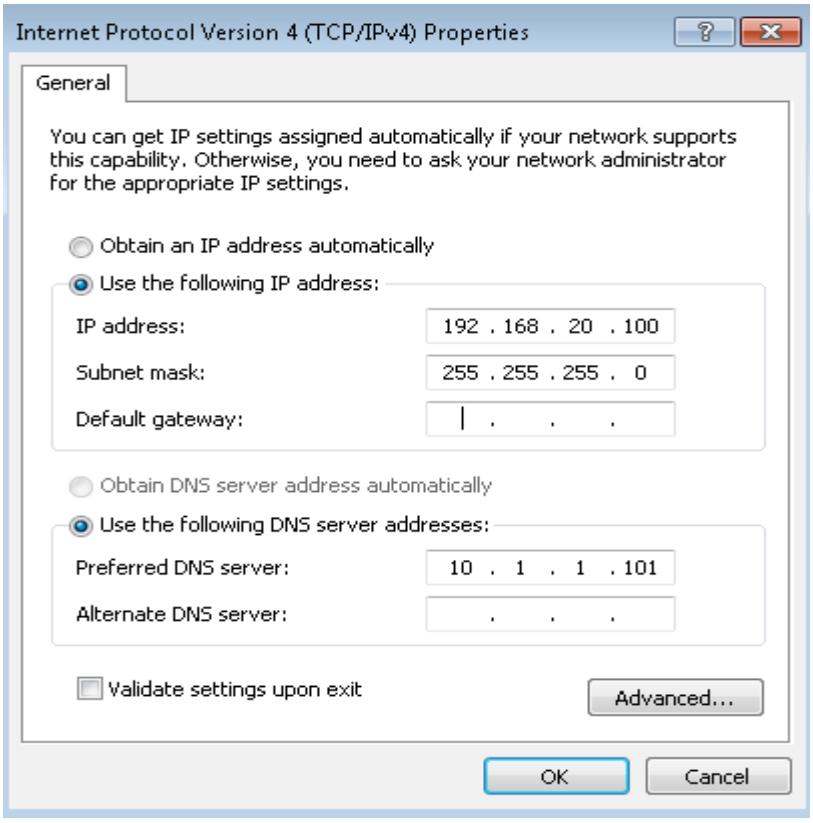
- Use Internet explorer or chrome for configuring WSA. Firefox will be used as the web browser to test explicit web proxy feature of WSA.
- Connect to the M1 interface and ensure Web proxy and FTP proxy is enabled on the proxy default ports. Configure a FTP banner of "IT FTP POLICY"
- Configure WSA to host PAC files on TCP port 9001
- Create a simple PAC file using notepad such that the web browsers should use wsa.ipexpert.com and TCP proxy port 3128 as the web proxy server for any URL's.
- Configure Firefox to use WSA as the proxy server. It should download the PAC file from the WSA automatically. Verify that the PAC file is downloaded to the Firefox using from log files (pacd_logs)
- Ensure you can connect to www.ipexpert.com using Firefox. Verify using that Firefox is using WSA from log files using accesslogs.

Task-2: Solutions

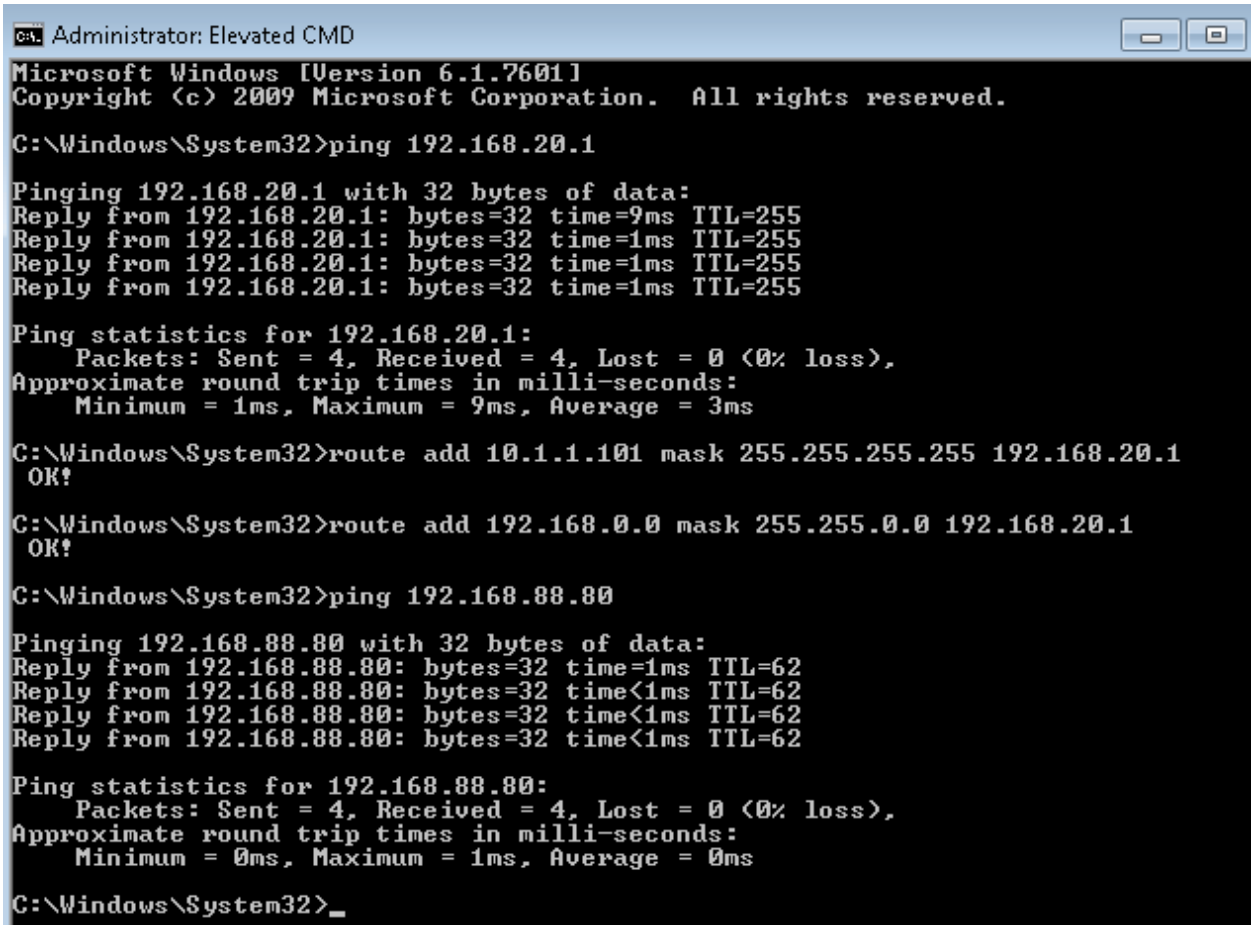
Step 1: Change the VLAN to 20 on SW3 for test pc and re-configure the IP address.

```
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
```

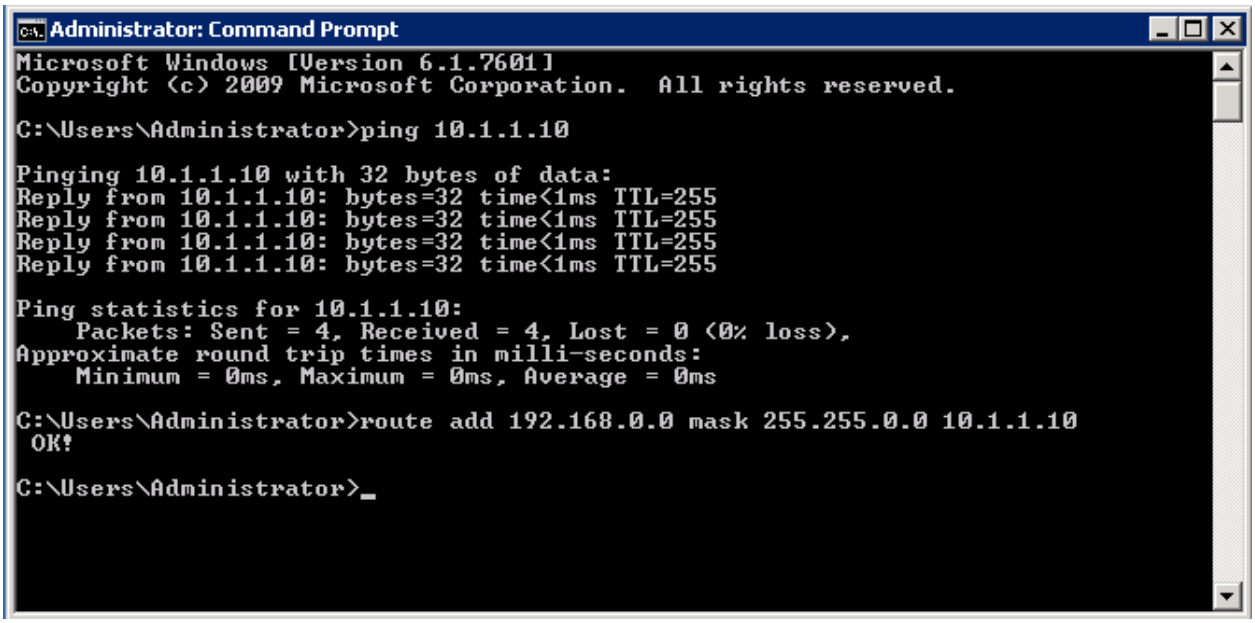
Change the IP address to 192.168.20.100



Ping the default gateway (192.168.20.1). Configure static route for 10.1.1.101/32 and 192.168.0.0/16 with SW2 as the default gateway. Ping M1 interface of WSA.

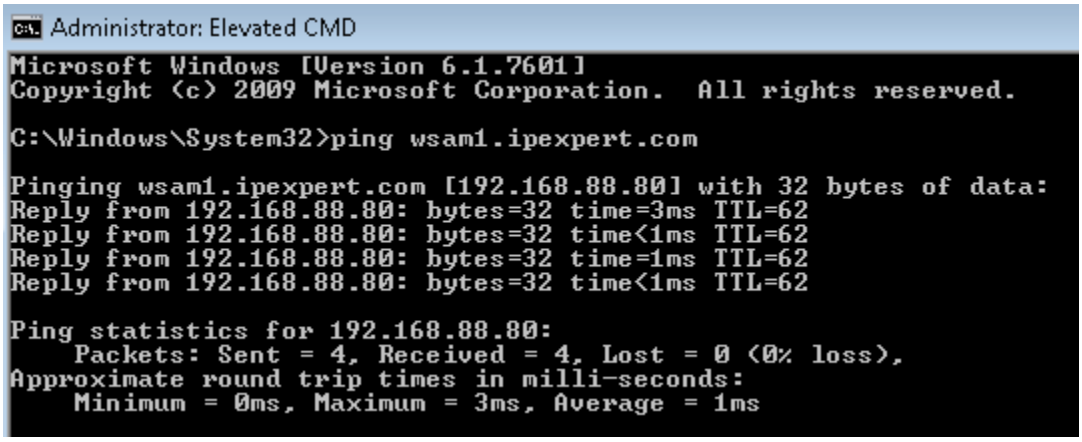


RDP into AD server which also acts like the DNS/FTP/webserver and add 192.168.0.0/16 with a next hop of ASA3 10.1.1.10



,

Check if the DNS resolution is working on the test pc. Ping wsam1.ipexpert.com



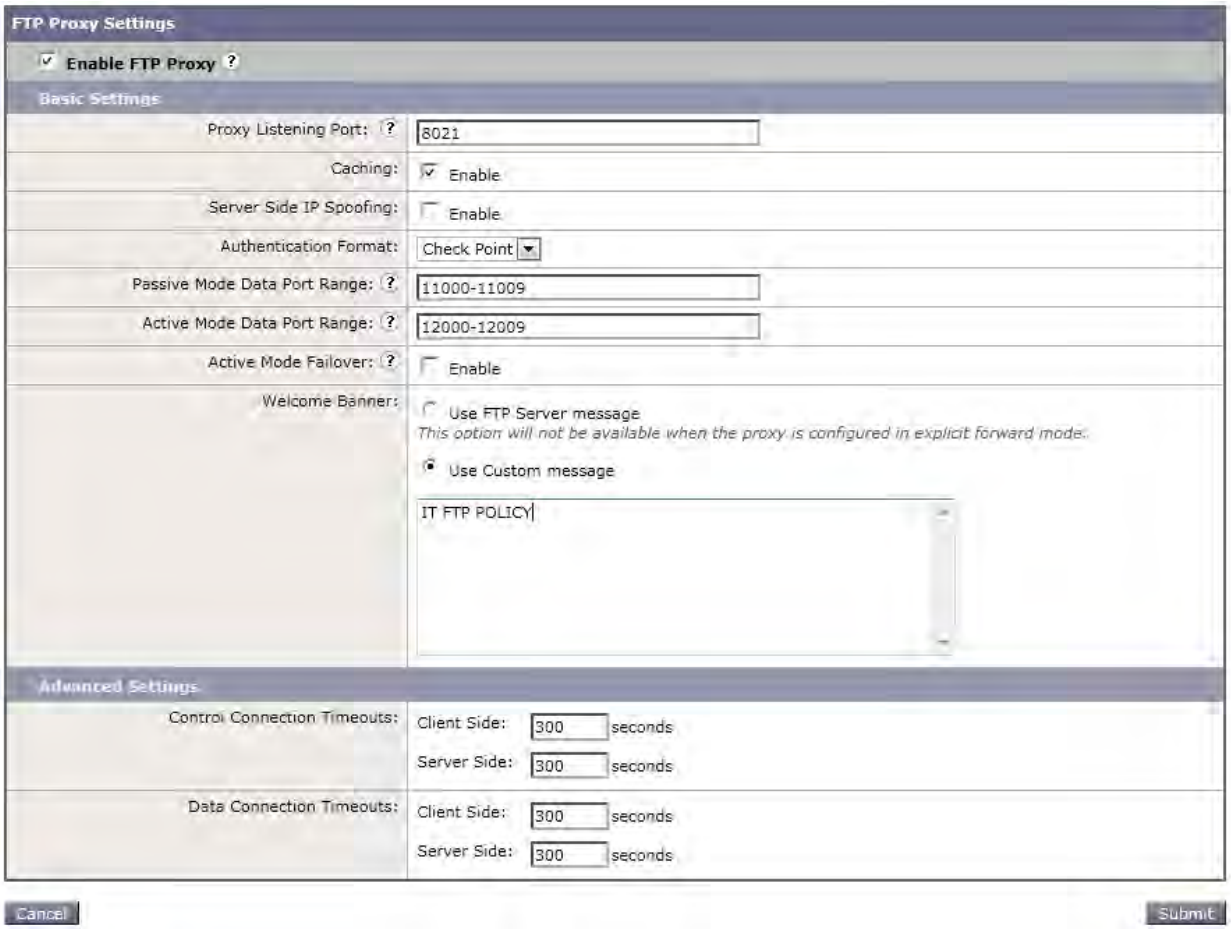
Step 2: Connect to WSA M1 using IE and check if the Web proxy is enabled.

Security Services -> Web Proxy

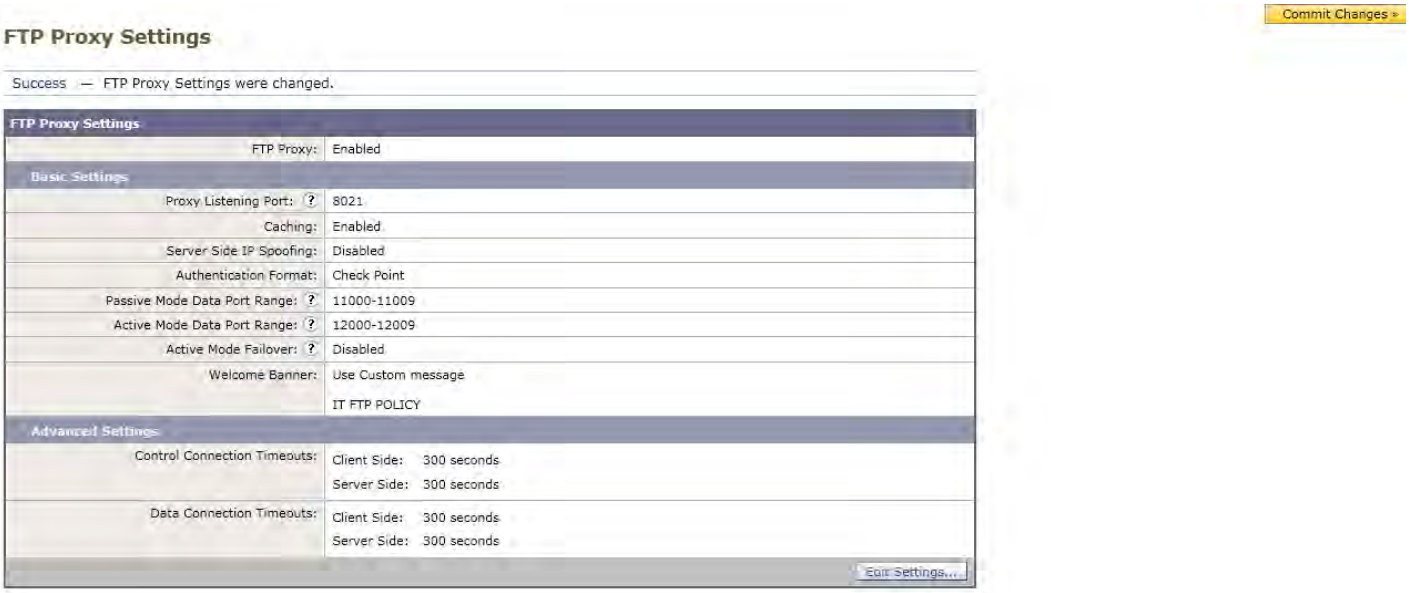
Make sure web proxy is “Enabled” on 80 and 3128 ports (defaults).

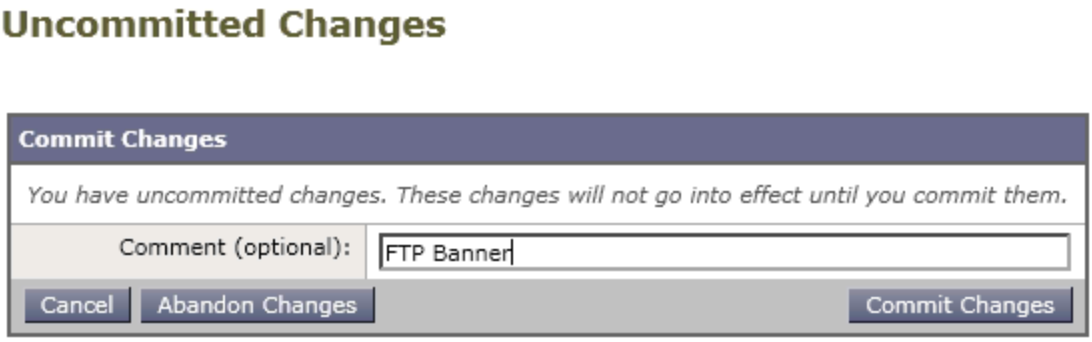
Step 3: Make sure FTP proxy is enabled and configure a custom banner for FTP “IT FTP POLICY”

Security Services -> FTP Proxy -> Edit Settings



Make sure you commit the changes and give a meaningful description/comment for the change



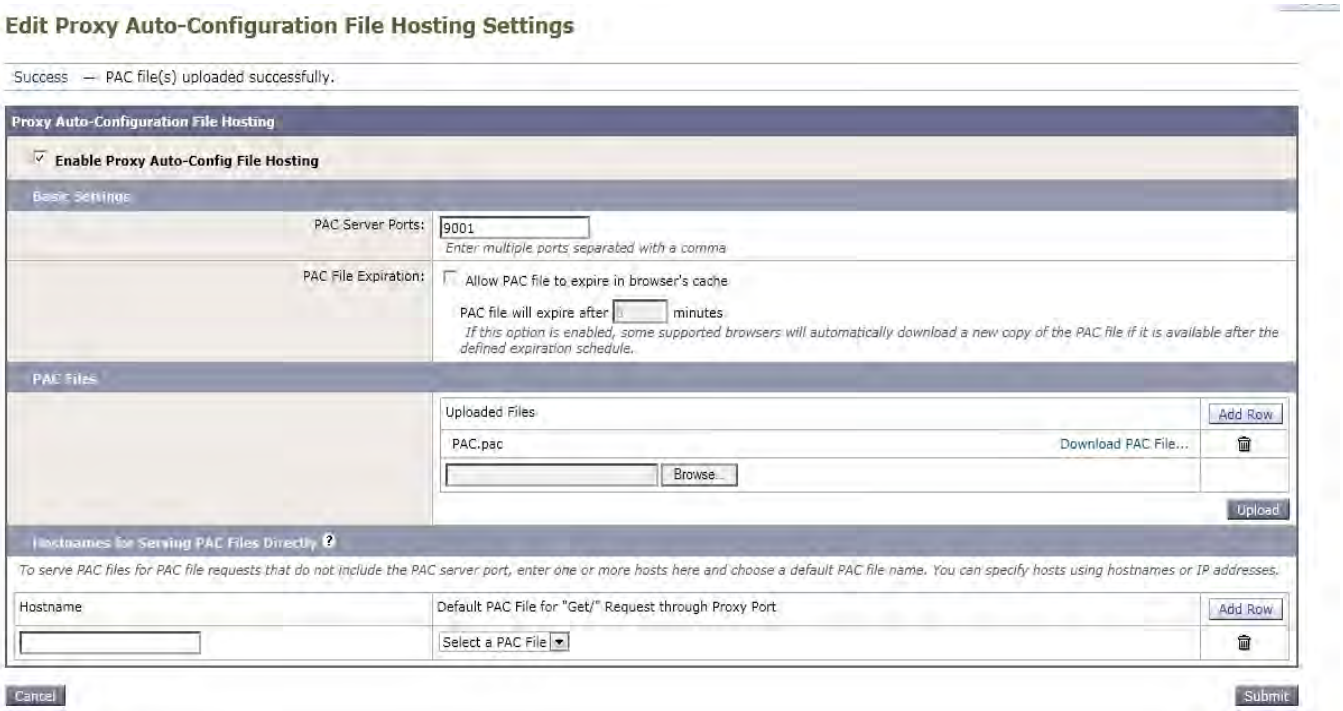


Step 4: Create a text file called PAC.pac on the TEST PC with the below function/strings

```
function FindProxyForURL (url, host) {
  return "PROXY wsa.ipexpert.com:3128";
}
```

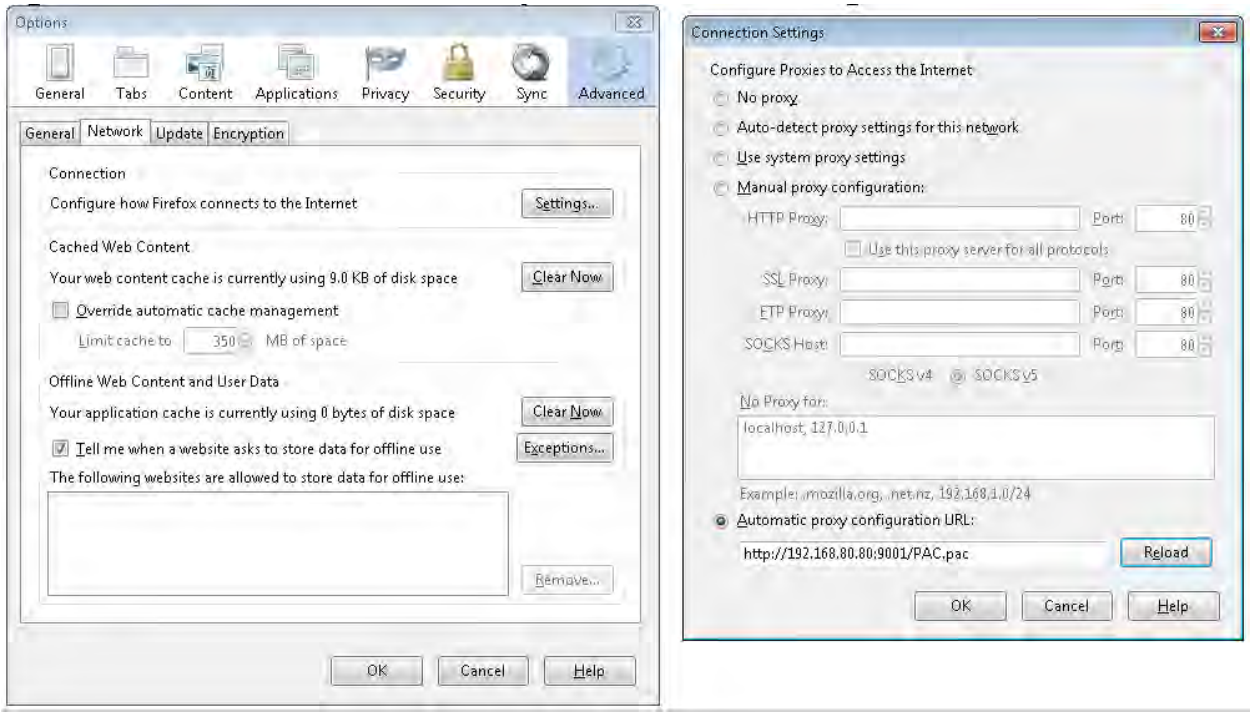
Step 5: Enable PAC files hosting on WSA and upload the PAC file from the test PC to the WSA

Security Services -> PAC File Hosting -> Enable/Edit settings



Make sure to commit the changes and give a meaningful comment

Step 6: Configure firefox to use web proxy. Make sure it uses PAC files hosted on the WSA.



Step 7: Verify the PAC file being downloaded from the log files. Browse to www.ipexpert.com.

```
wsa.ipexpert.com> tail

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
3. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
4. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
6. "dca_logs" Type: "DCA Engine Logs" Retrieval: FTP Poll
7. "external_auth_logs" Type: "External Authentication Logs" Retrieval: FTP
Poll
8. "feedback_logs" Type: "Feedback Logs" Retrieval: FTP Poll
9. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
10. "gui_logs" Type: "GUI Logs" Retrieval: FTP Poll
11. "haystackd_logs" Type: "Haystack Logs" Retrieval: FTP Poll
12. "idsdataloss_logs" Type: "Data Security Logs" Retrieval: FTP Poll
13. "logderrorlogs" Type: "Logging Logs" Retrieval: FTP Poll
14. "mcafee_logs" Type: "McAfee Logs" Retrieval: FTP Poll
15. "musd_logs" Type: "Mobile User Security Daemon Logs" Retrieval: FTP Poll
16. "pacd_logs" Type: "PAC File Hosting Daemon Logs" Retrieval: FTP Poll
17. "proxylogs" Type: "Default Proxy Logs" Retrieval: FTP Poll
18. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
19. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
20. "saas_auth_log" Type: "SaaS Auth Logs" Retrieval: FTP Poll
21. "shd_logs" Type: "SHD Logs" Retrieval: FTP Poll
22. "snmp_logs" Type: "SNMP Logs" Retrieval: FTP Poll
23. "sntpd_logs" Type: "NTP Logs" Retrieval: FTP Poll
24. "sophos_logs" Type: "Sophos Logs" Retrieval: FTP Poll
25. "status" Type: "Status Logs" Retrieval: FTP Poll
26. "system_logs" Type: "System Logs" Retrieval: FTP Poll
27. "trafmon_errlogs" Type: "Traffic Monitor Error Logs" Retrieval: FTP Poll
28. "trafmonlogs" Type: "Traffic Monitor Logs" Retrieval: FTP Poll
29. "uds_logs" Type: "UDS Logs" Retrieval: FTP Poll
30. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
31. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
32. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
33. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
34. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval:
FTP Poll
Enter the number of the log you wish to tail.
[]> 16

Press Ctrl-C to stop.
Fri Dec 31 14:26:09 2010 Info: Begin Logfile
Fri Dec 31 14:26:09 2010 Info: Version: 7.1.3-031 SN: E4D3F1CFFF36-
FTX1651M0AS
Fri Dec 31 14:26:09 2010 Info: Time offset from UTC: -18000 seconds
```

```
Fri Dec 31 14:26:09 2010 Info: System is coming up.
Fri Dec 31 14:26:09 2010 Info: PAC File Hosting Daemon started. status=0
Fri Dec 31 14:30:19 2010 Info: 192.168.20.100 - /PAC.pac is downloaded
successfully

wsa.ipexpert.com> tail accesslogs
1293824343.282      176      192.168.20.100      TCP_MISS/200      753      GET
http://www.ipexpert.com/ - DIRECT/www.ipexpert.com text/html DEFAULT_CASE_11-
DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_edu,0.0,"1","-",-,-
,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_edu,-,"-","-
","Unknown","Unknown","-","-",34.23,0,-,"-","-"> -
```

Task 3: Configure acknowledgement and custom end-user notifications

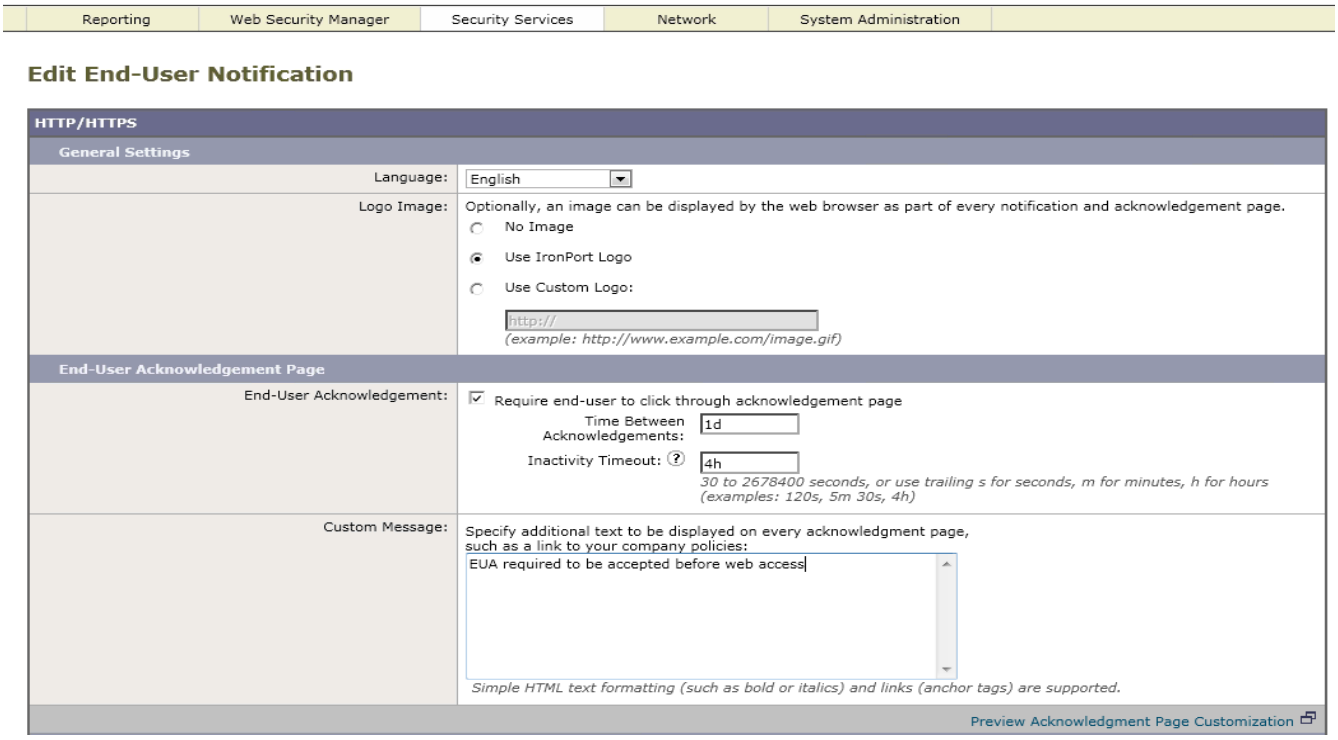
- Configure WSA to send EUA to users before they are allowed web access. Add any custom message. Use Iron port logo. Do not change the default timeout values.
- Configure WSA to send Ironport notification and warning messages to users.
- WSA should send the below message/custom EUN when there is a DNS resolution error for a URL to the users. Test this by entering a wrong URL.

"Re-Check your URL. Wrong URL entered"

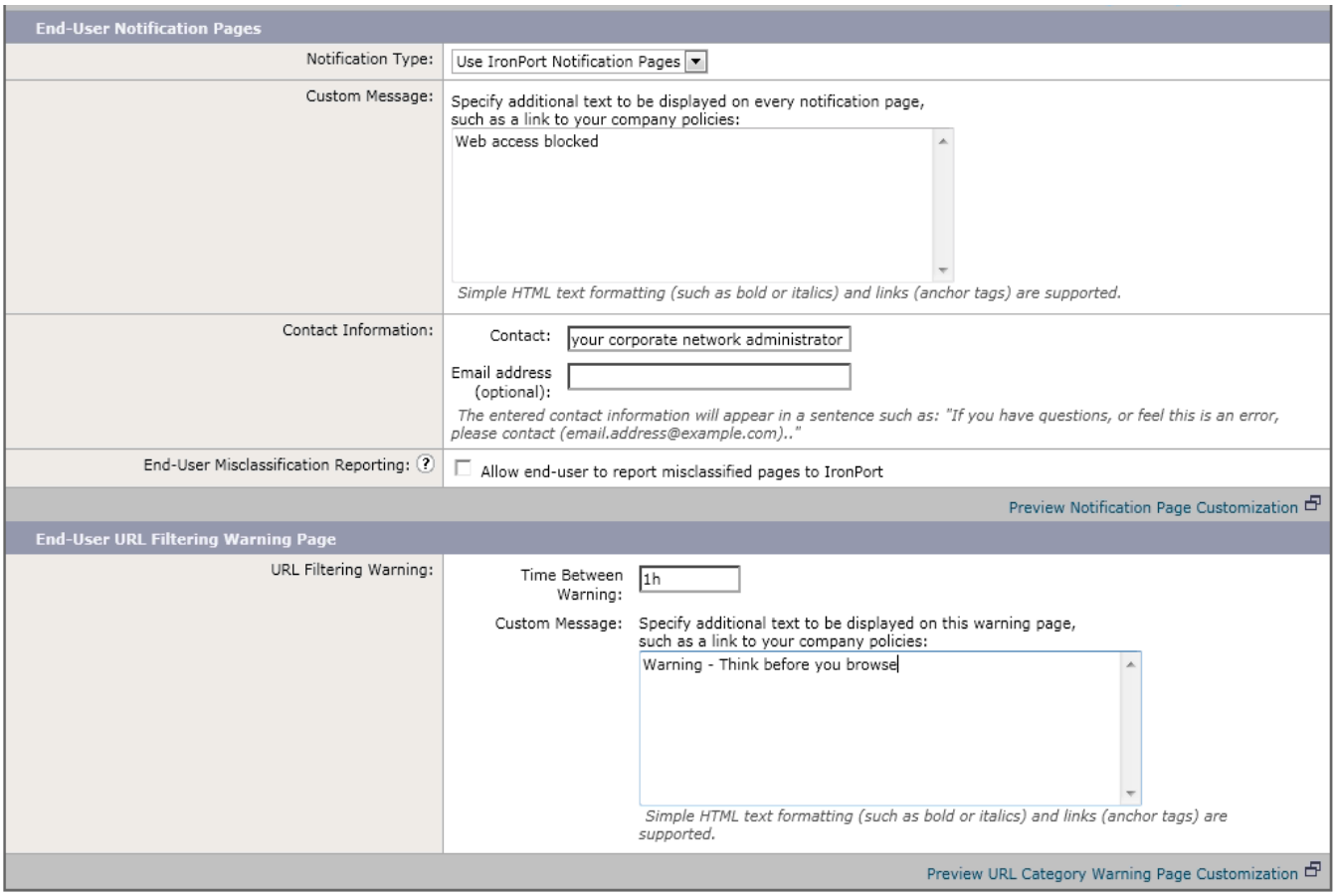
Task-3: Solutions

Step 1: Configure EUA and enable the use of Ironport logo. You may give any custom message

Security Services -> End User Notification -> Edit Settings

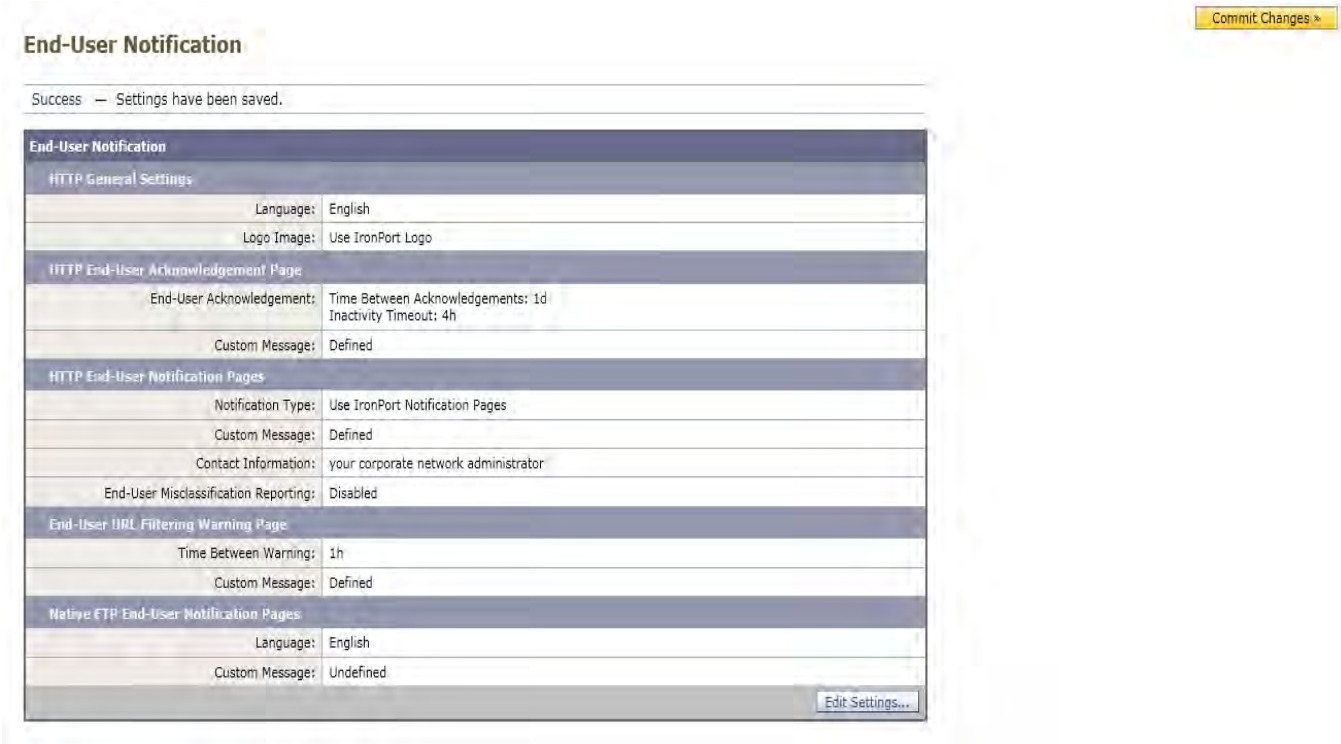


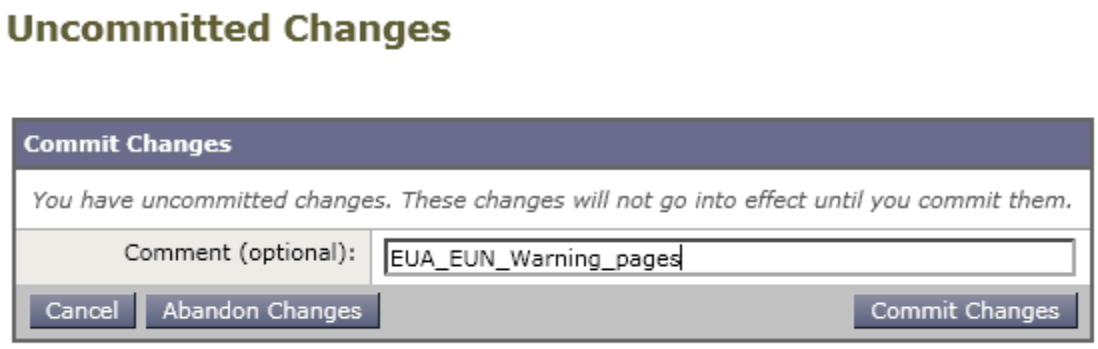
Step 2: Configure EUN/notification and warning page . You may give any custom message



S

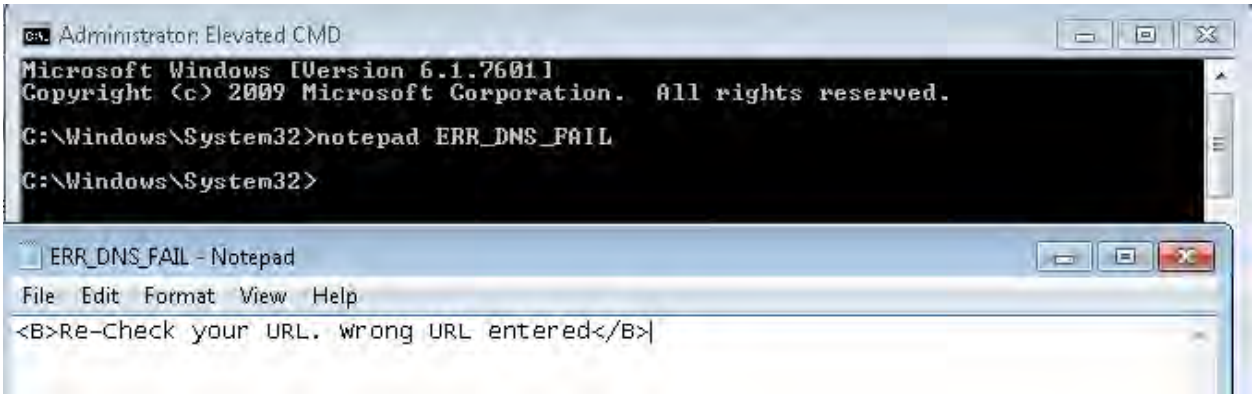
Step 3: Review and apply/commit the change



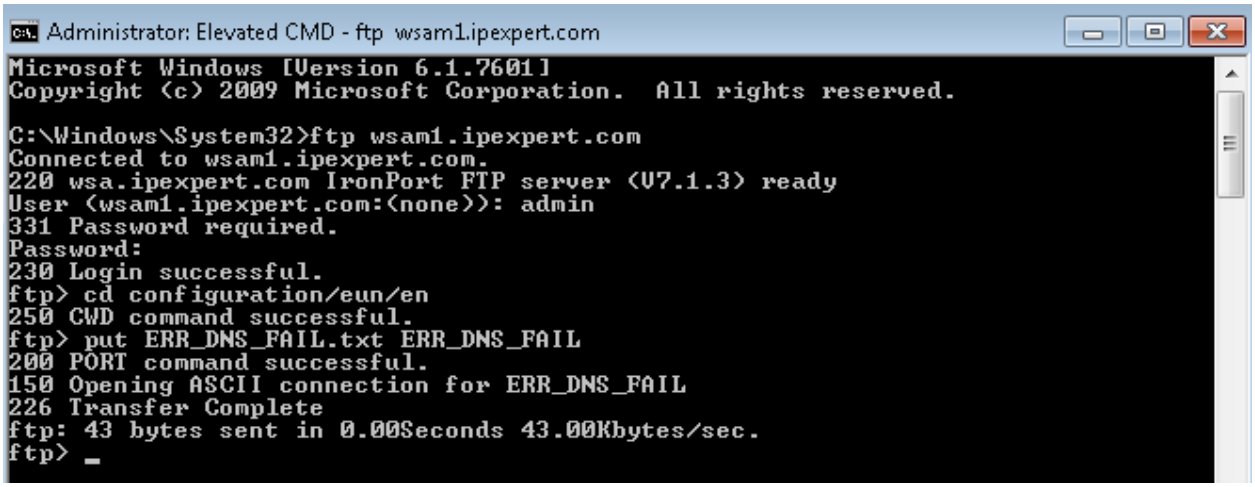


Step 3: Create a text file in the command prompt as per the task for the DNS resolution error. This file will be uploaded to the WSA to customize the DNS resolution error message using FTP.

Create the custom text file using notepad



Upload the custom text file to WSA to the correct directory using FTP

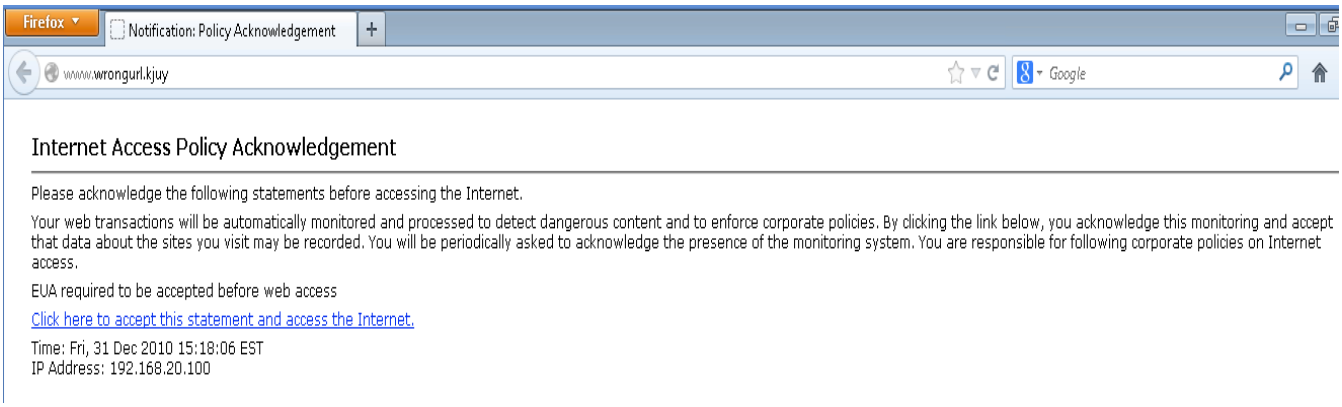


Configure the WSA to use the custom EUN and commit the changes

```
wsa.ipexpert.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- WCCP - WCCPv2 related parameters
- MISCELLANEOUS - Miscellaneous proxy related parameters
[]> EUN

Enter values for the EUN options:

Currently using: Standard EUN pages

Choose:
1. Refresh EUN pages
2. Use Custom EUN pages
3. Use Standard EUN pages
[3]> 2

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- WCCP - WCCPv2 related parameters
- MISCELLANEOUS - Miscellaneous proxy related parameters
[]>

wsa.ipexpert.com> commit

Please enter some comments describing your changes:
[]> DNS_ERROR_CUSTOM_EUN
Changes committed: Fri Dec 31 15:07:02 2010 EST
wsa.ipexpert.com>
```

Test the configuration by typing wrong URL using firefox. This only works for Explict forward mode since the DNS resolution is done by the WSA

Browse to www.wrongurl.kkuy Accept the EUA



Task 4: Configuring Active Directory authentication for users

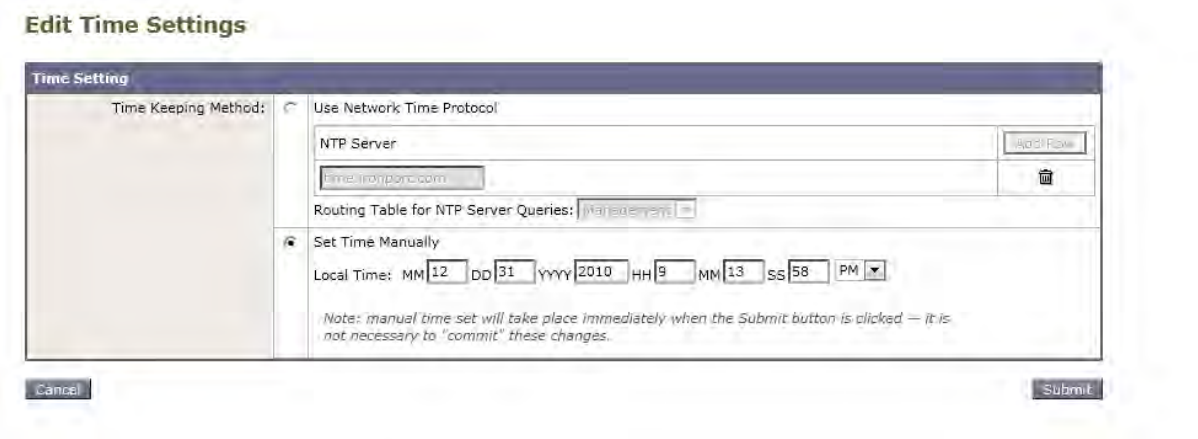
- Set the time and date manually on the WSA to match the AD server
- Configure WSA with an AD realm "ADServer"
- The authentication protocol would be NTLMSSP.
- The AD server IP is 10.1.1.101 and the AD domain is IPEXPERT.COM
- Join the Domain using username of "Administrator" and password "IPExpert123".
- Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction. IP Surrogate cache time out should be set to 5 minutes.
- Enable authentication in the global identity policy. Use IP surrogates only.
- Test by browsing to www.google.com or www.ipexpert.com using a username of "HRUSER1" with a password of "cisco". Verify from log files using accesslogs.

Task-4: Solutions

Step 1: Check the time settings of the AD server and configure the WSA to match similar time.

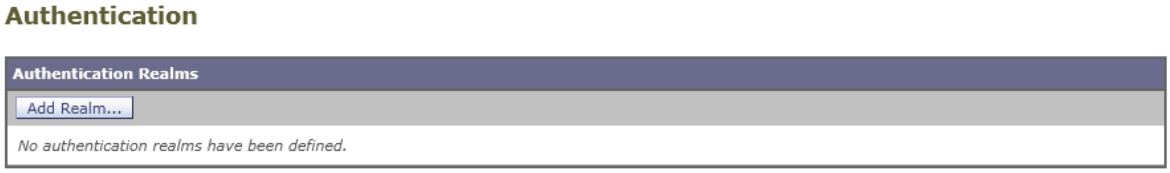
System Administration -> Time Settings -> Edit Settings

Check your AD server and configure appropriate time and apply the time setting changes.

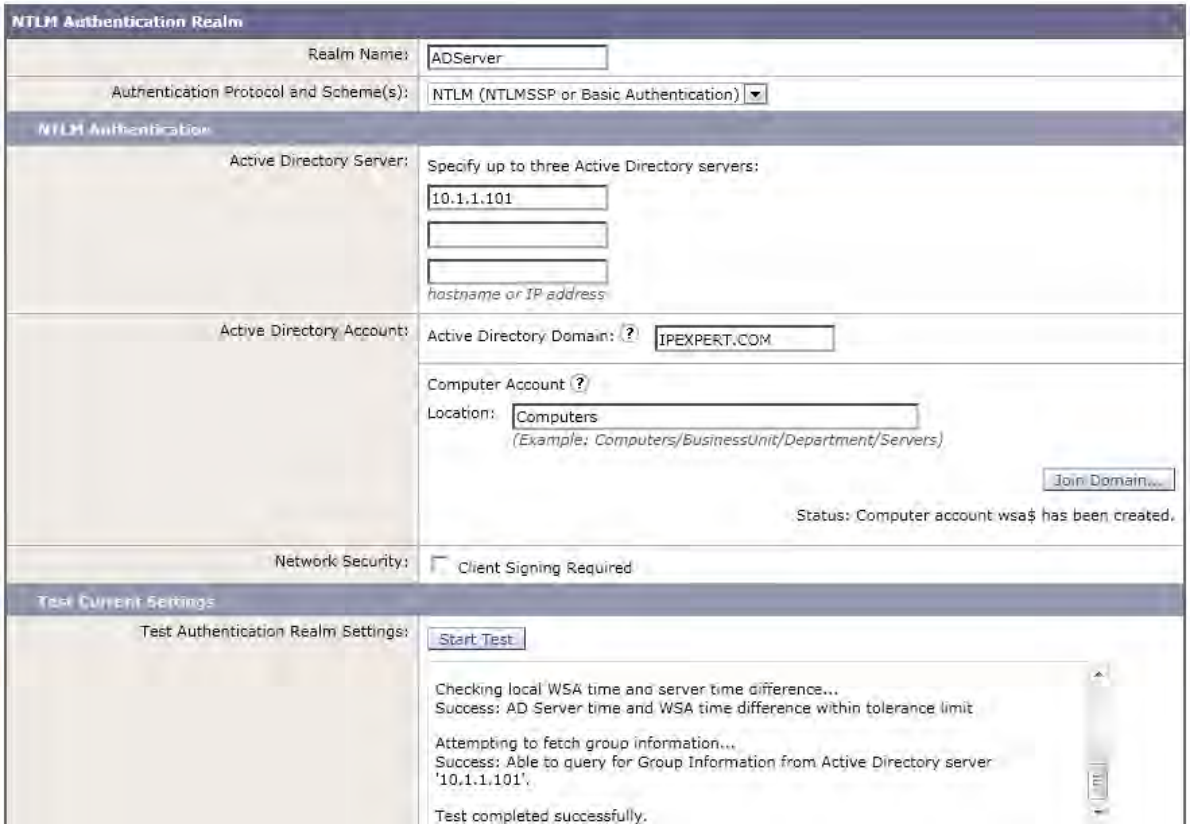


Step 2: Configure an AD realm of "ADServer" and use NTLMSSP as the protocol

Network -> Authentication -> Add realm



Configure AD realm and join the domain. You may eve test and find out is the time is out of sync

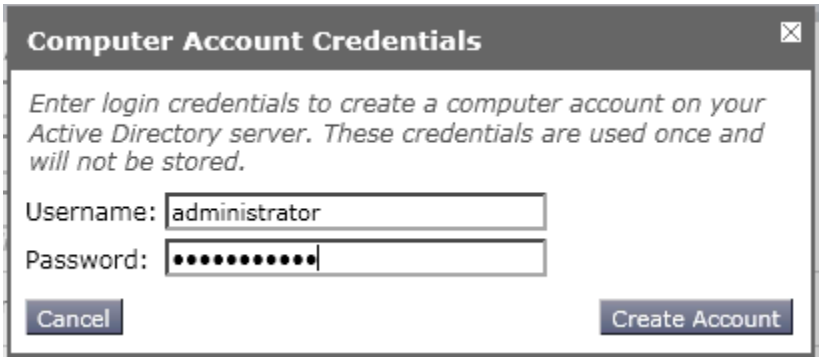


TEST AUTHENTICATION

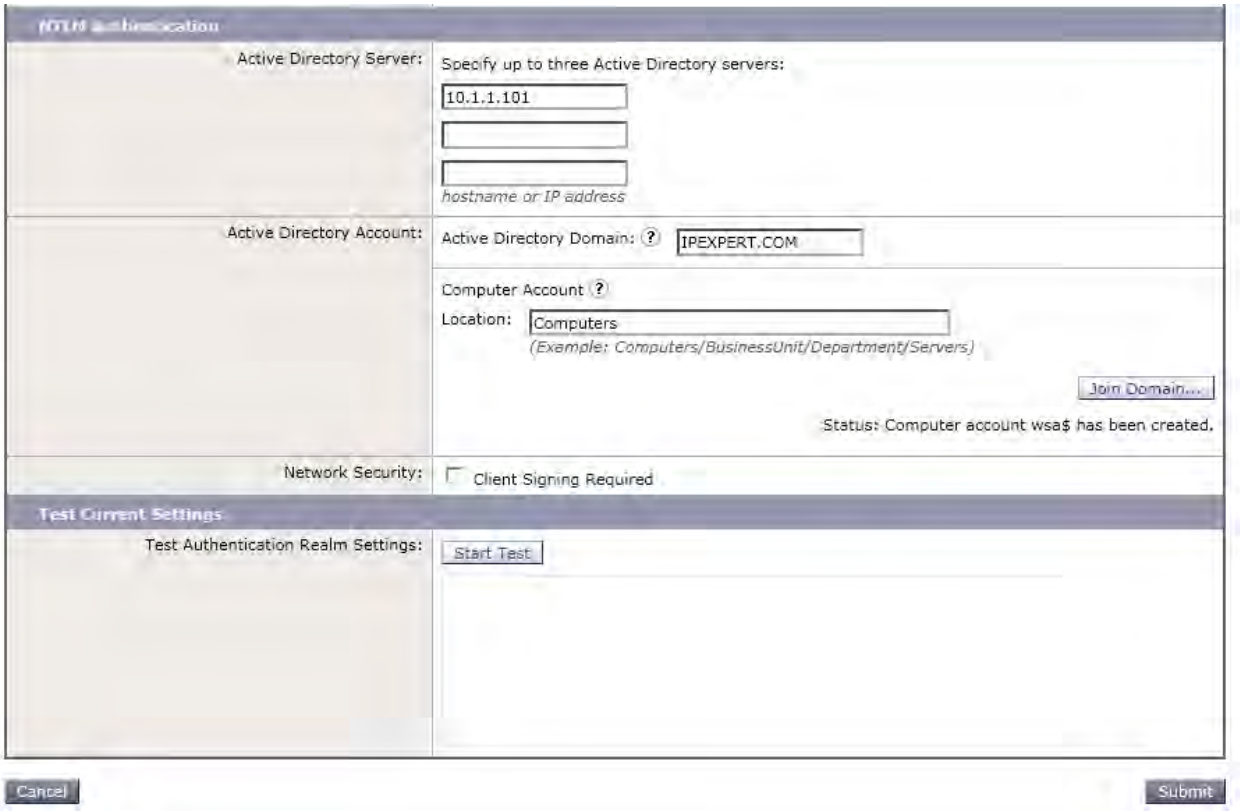
```
Checking DNS resolution of WSA hostname(s)...
Success: Resolved 'wsam1.ipexpert.com' address: 192.168.88.80
Success: Resolved 'wsa.ipexpert.com' address: 192.168.80.80

Checking DNS resolution of Active Directory Server(s)...
Success: Resolved '10.1.1.101' address: 10.1.1.101

Checking DNS resolution of AD Server(s)' full computer name(s)...
Success: Resolved 'WIN-D75PLBAOCA2.ipexpert.com' address: 10.1.1.101

Validating configured Active Directory Domain...
Success: Active Directory Domain Name for '10.1.1.101' : IPEXPERT.COM

Attempting to get TGT...
Success: Kerberos Tickets fetched from server '10.1.1.101' :
kinit: NOTICE: ticket renewable lifetime is 1 week

Checking local WSA time and server time difference...
Success: AD Server time and WSA time difference within tolerance limit

Attempting to fetch group information...
Success: Able to query for Group Information from Active Directory server
'10.1.1.101'.
```

```
Test completed successfully
```

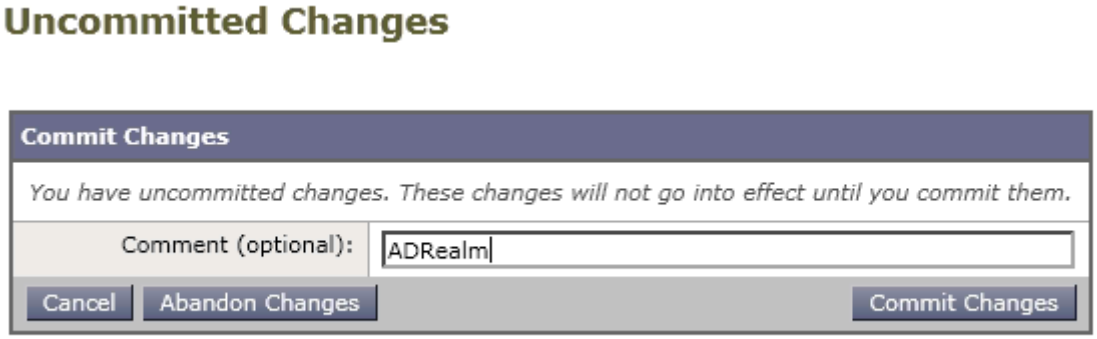
Step 3: Join the AD Domain



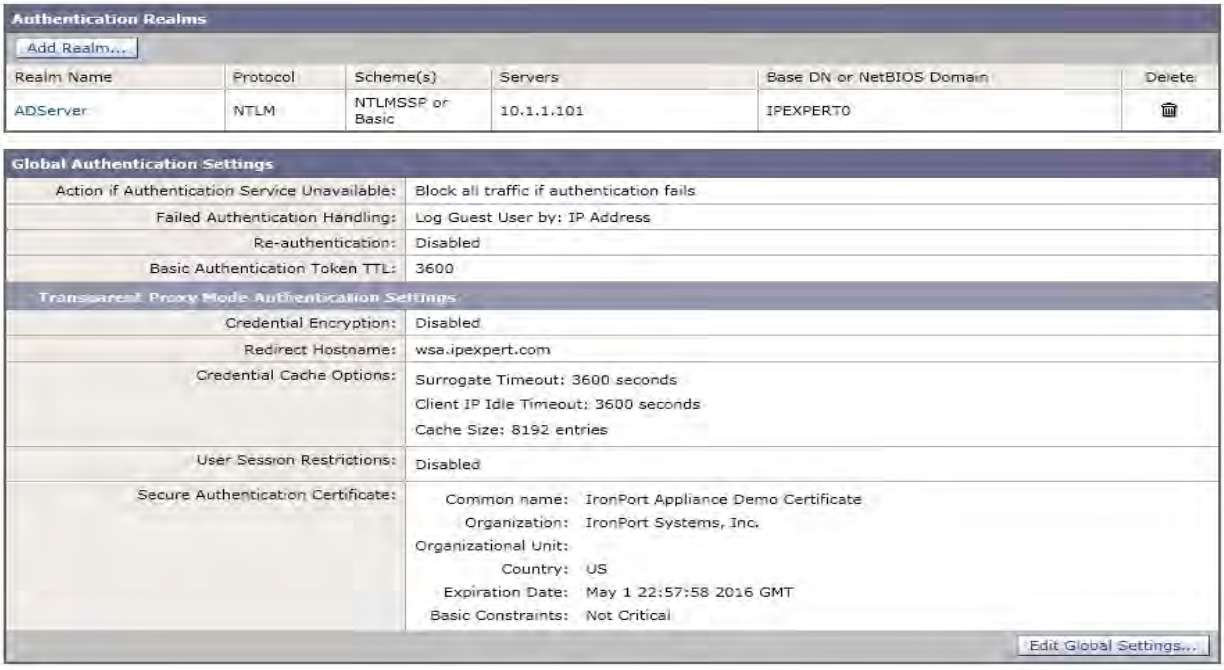
Submit and apply the changes



Apply the changes and give a meaningful description/comment



Step 3: Edit the global authentication settings and change the IP surrogate time to 5 minutes and enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction.



Authentication Realms

Add Realm...

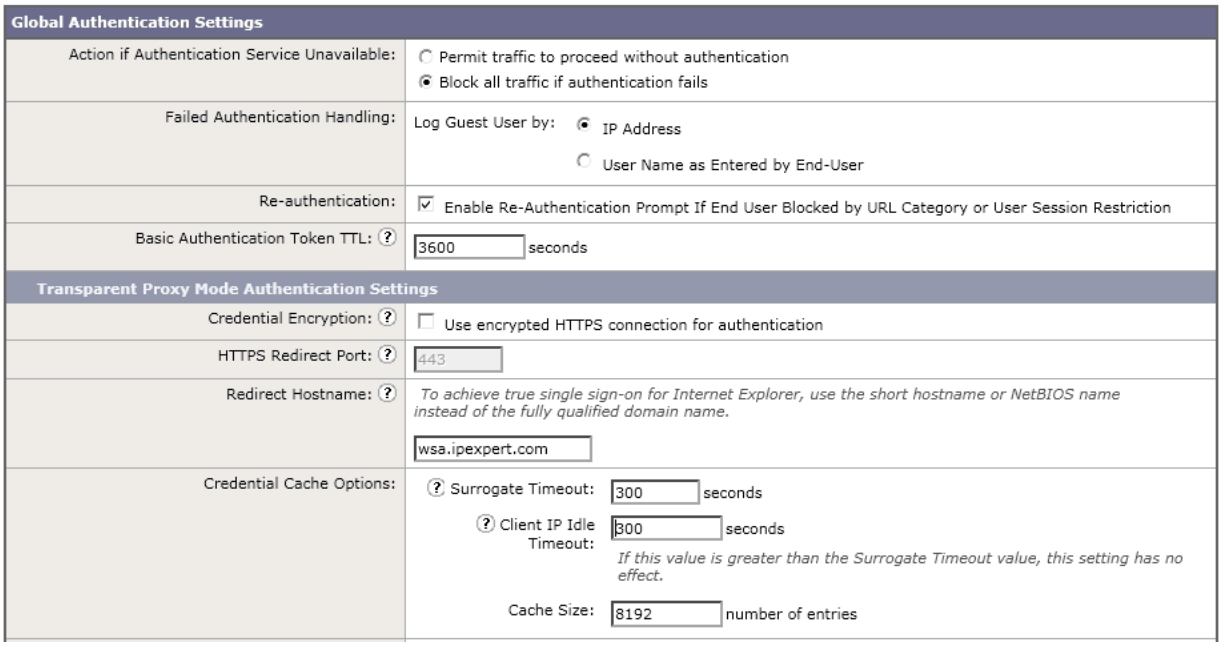
Realm Name	Protocol	Scheme(s)	Servers	Base DN or NetBIOS Domain	Delete
ADServer	NTLM	NTLMSSP or Basic	10.1.1.101	IPEXPERT0	

Global Authentication Settings

Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Disabled
Basic Authentication Token TTL:	3600
Transparent Proxy Mode Authentication Settings	
Credential Encryption:	Disabled
Redirect Hostname:	wsa.ipexpert.com
Credential Cache Options:	Surrogate Timeout: 3600 seconds Client IP Idle Timeout: 3600 seconds Cache Size: 8192 entries
User Session Restrictions:	Disabled
Secure Authentication Certificate:	Common name: IronPort Appliance Demo Certificate Organization: IronPort Systems, Inc. Organizational Unit: Country: US Expiration Date: May 1 22:57:58 2016 GMT Basic Constraints: Not Critical

Edit Global Settings...

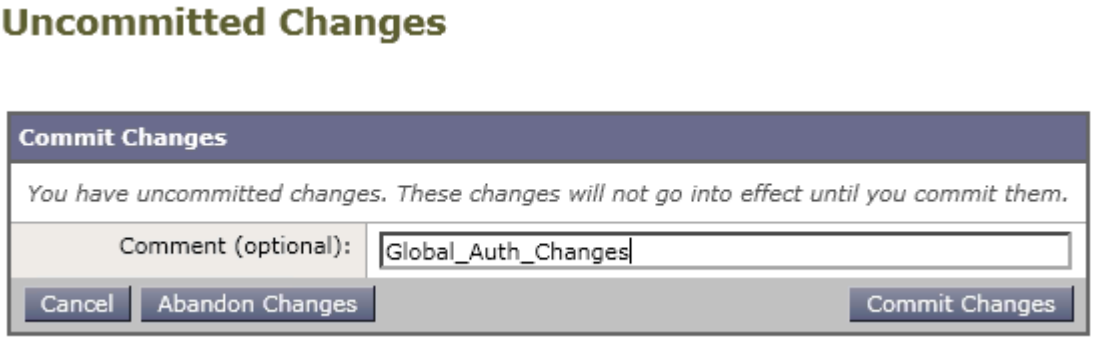
Edit Global Authentication Settings



Global Authentication Settings

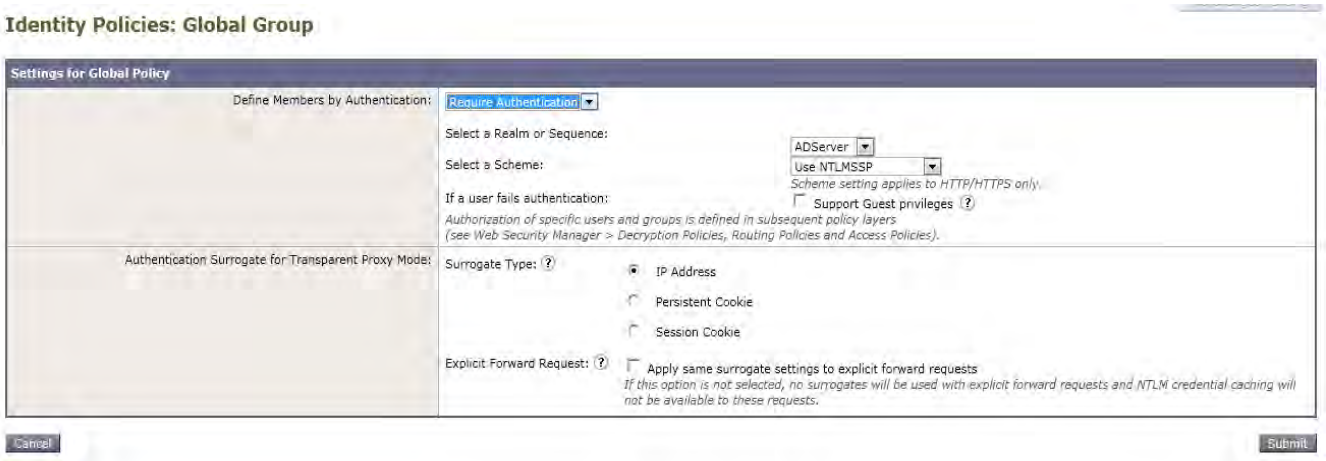
Action if Authentication Service Unavailable:	○ Permit traffic to proceed without authentication ◉ Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: ◉ IP Address ○ User Name as Entered by End-User
Re-authentication:	☑ Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction
Basic Authentication Token TTL:	3600 seconds
Transparent Proxy Mode Authentication Settings	
Credential Encryption:	☐ Use encrypted HTTPS connection for authentication
HTTPS Redirect Port:	443
Redirect Hostname:	*To achieve true single sign-on for Internet Explorer, use the short hostname or NetBIOS name instead of the fully qualified domain name.* wsa.ipexpert.com
Credential Cache Options:	Surrogate Timeout: 300 seconds Client IP Idle Timeout: 300 seconds *If this value is greater than the Surrogate Timeout value, this setting has no effect.* Cache Size: 8192 number of entries

Submit and apply the changes.

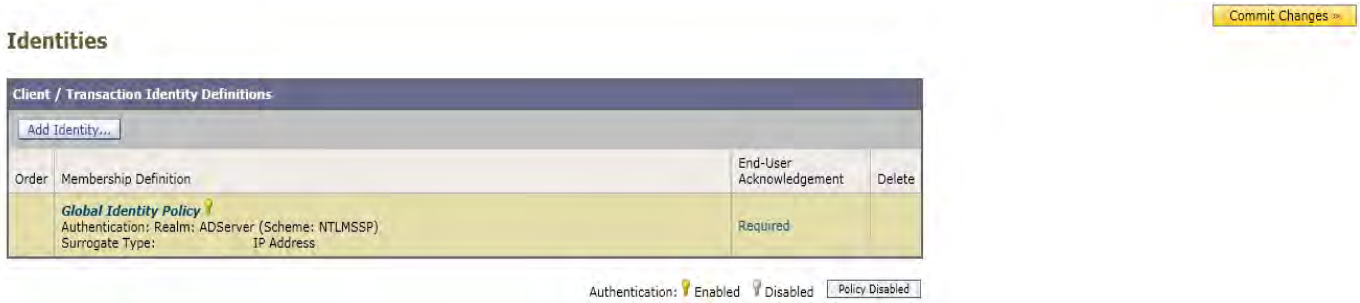


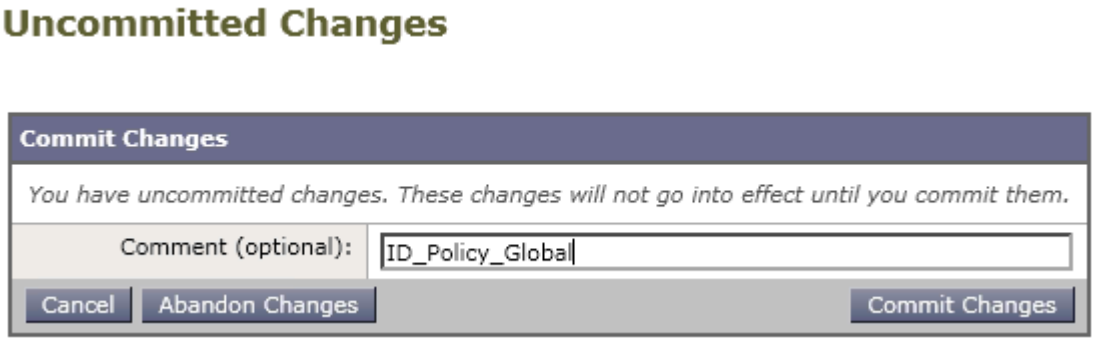
Step 4: Enable authentication in the global identity policy using the ADServer realm.

Web Security Manager -> Identities -> Global Identity Policy

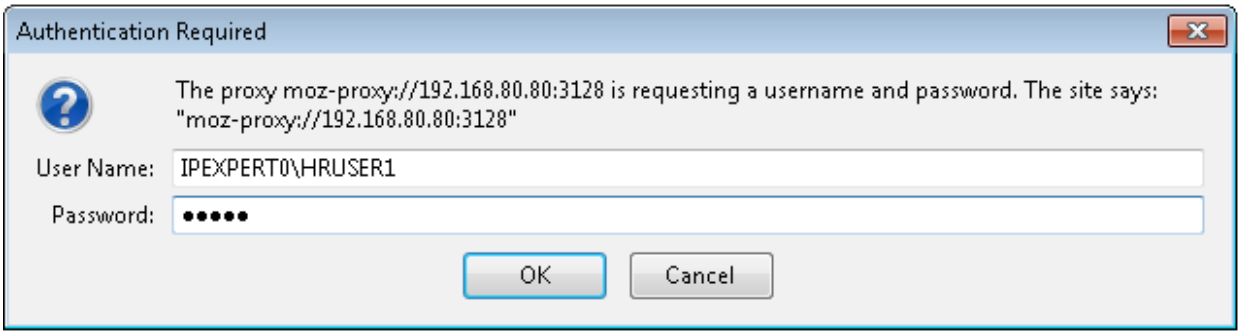


Submit and apply the changes





Step 5: Test by browsing to www.google.com using Firefox. (Remember to clear all history)



Accept the EUN for HRUSER1

Access Logs

```
AsyncOS 7.1.3 for Web build 031

Welcome to the IronPort S170 Web Security Appliance
wsa.ipexpert.com> tail accesslogs

1293832382.069      1      192.168.20.100      TCP_DENIED/407      1766      GET
http://www.google.com/  - NONE/-  - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-
","-",14128.00,0,-,"-","-"> -

1293832382.074 0 192.168.20.100 TCP_DENIED/407 451 GET http://www.google.com/
- NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE <-,-,"-","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,"-","-
"> -

1293832382.252    175    192.168.20.100    TCP_REFRESH_HIT/200    422    GET
http://www.google.com/    "IPEXPERT0\hruser1@ADServer"    DIRECT/www.google.com
text/html  ALLOW_WBRS_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_srch,8.2,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_srch,-,"-
","-","GenericSearchEngineTraffic","Search  Engine","-","-",19.29,0,-,"-","-">
-
```

Lab-2: Configuring Acceptable Use Policies on WSA for HTTP and FTP

Lab-2: Configuring AUP's for HTTP and FTP – This lab is intended to familiarize you with configuring various access and identity policies for HTTP and FTP traffic. You will also configure fall back policies using guest privilege feature, custom URL categories and authentication bypass for certain web traffic.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **4 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure Access Policies

- Your network has a very strict web access policy. Configure the Global policy such any authenticated user is allowed web access as per the below policy. Block any FTP requests. Test from the TEST-PC and check the access logs.
- Set to monitor for uncategorized URL's.
- Set URL content filtering to block for Search engines that don't support safe search and set site content rating to block web content which is explicitly rated as adult oriented.

URL Filtering	
Global Policy	Configure Monitor only the below categories and block all other URL categories.
	Business and Industry Computer Security Computers and Internet Education Government and Law News Streaming Media Search Engines and Portals

- Remote office LAN subnets users from 200.4.4.0/24 and 200.5.5.0/24 connect to the ASA main office for web access. They should be denied any streaming media access since it consumes bandwidth. The global policy permits streaming media. Hence configure a new access policy, which denies streaming media access for those subnets.

Task-1: Solutions

Step 1: Configure the Global Access policy to block FTP protocol.

Web Security Manager -> Access Policy -> Global Policy -> Protocols and User Agents

Commit the change after you submit

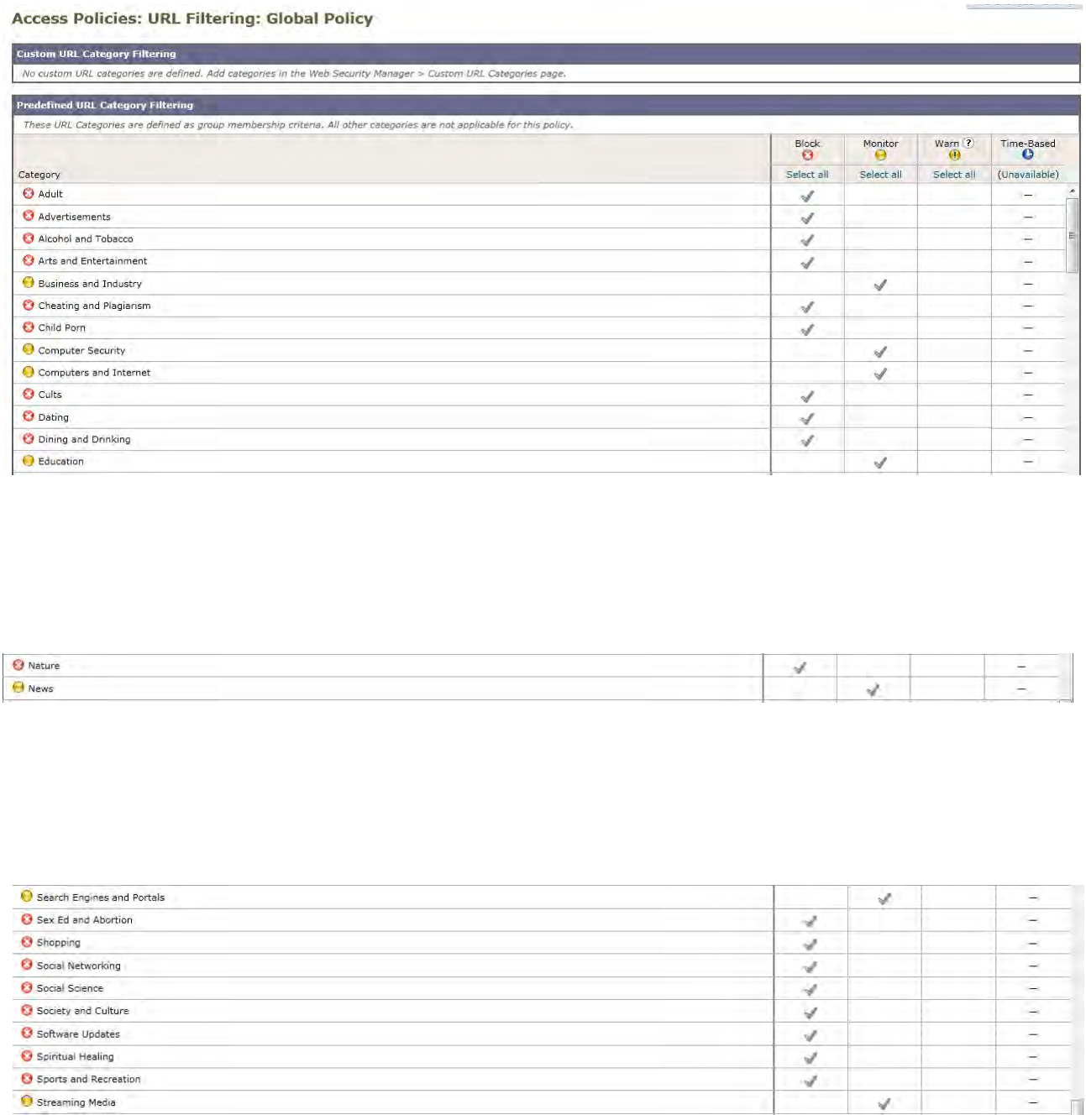
Step 2: In the URL filtering of the global policy, set to monitor for uncategorized URL's and configure the safe search policy as per task. You may need to scroll down for this.

Web Security Manager -> Access Policy -> Global Policy -> URL Filtering

Commit the change after you submit

Step 3: In the URL filtering of the global policy, block all the pre-defined categories and monitor only the categories specified in the task.

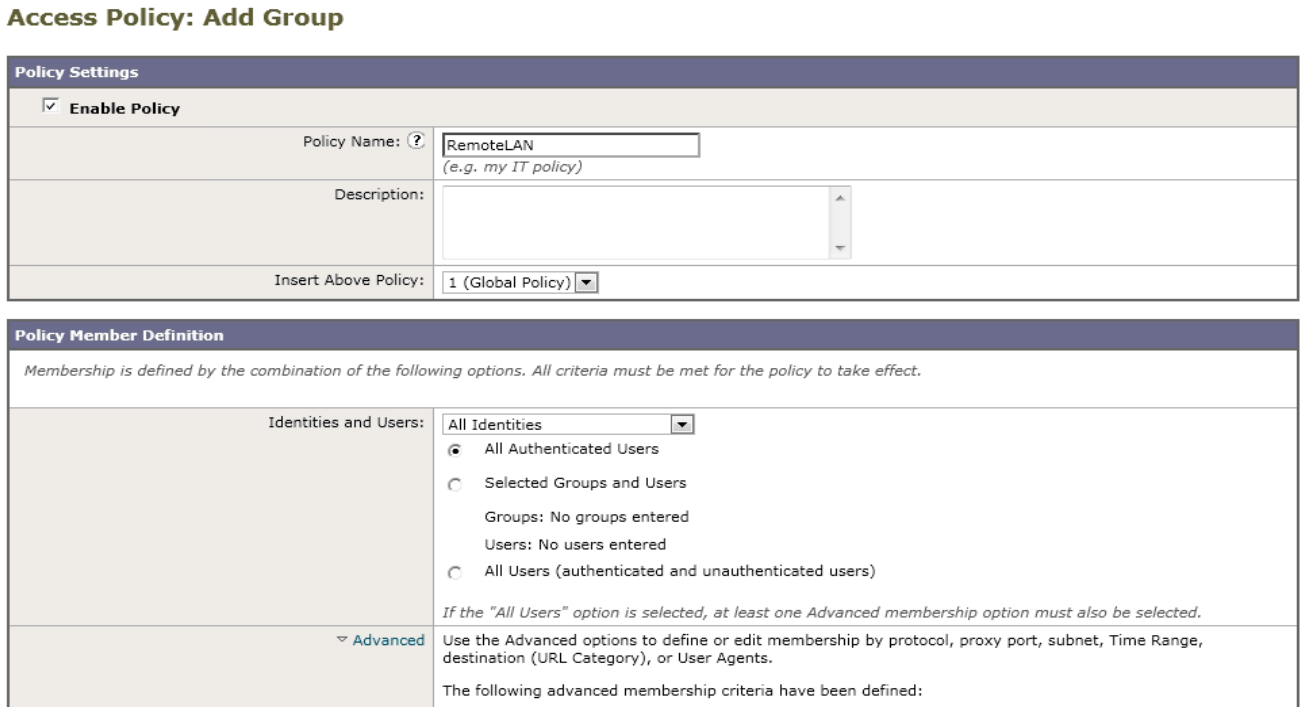
Web Security Manager -> Access Policy -> Global Policy -> URL Filtering



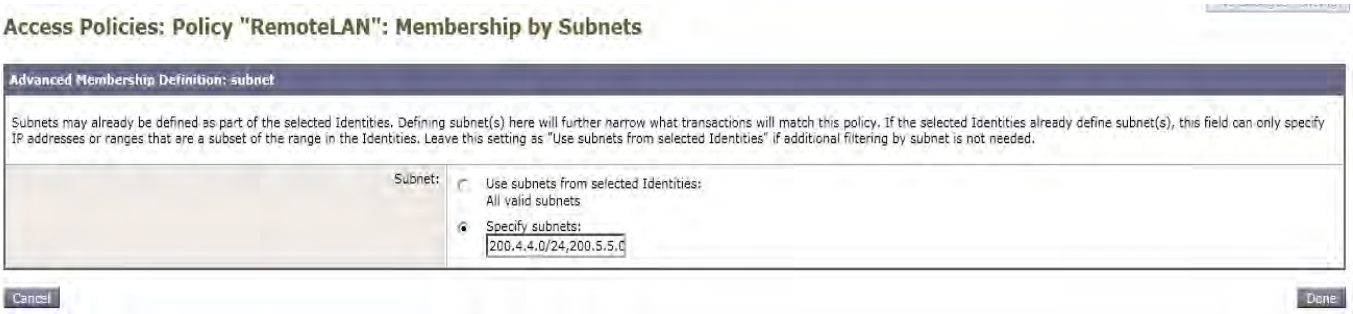
Submit and commit the changes

Step 4: Add a new access policy for the remote LAN users. Give a name to the policy and click on Advanced to apply this policy to a particular subnets (200.4.4.0/24, 200.5.5.0/24)

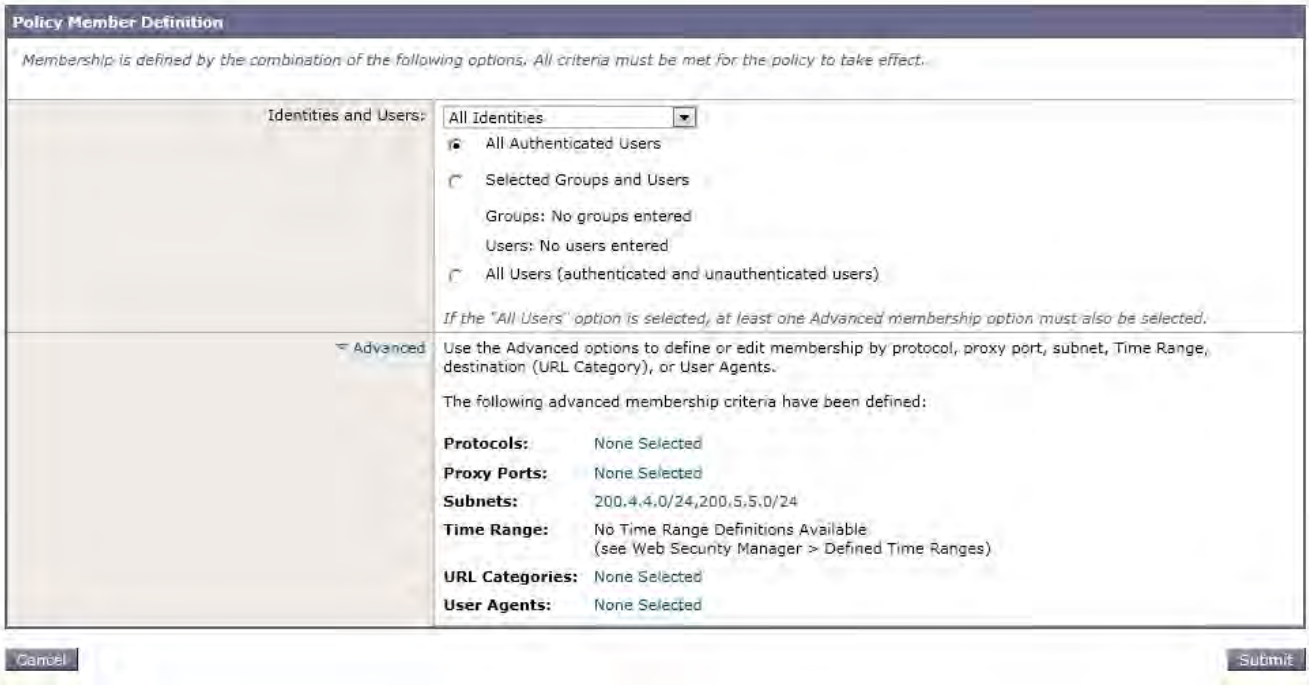
Web Security Manager -> Access Policy -> Global Policy -> Add Policy



Define the remote LAN IP subnets

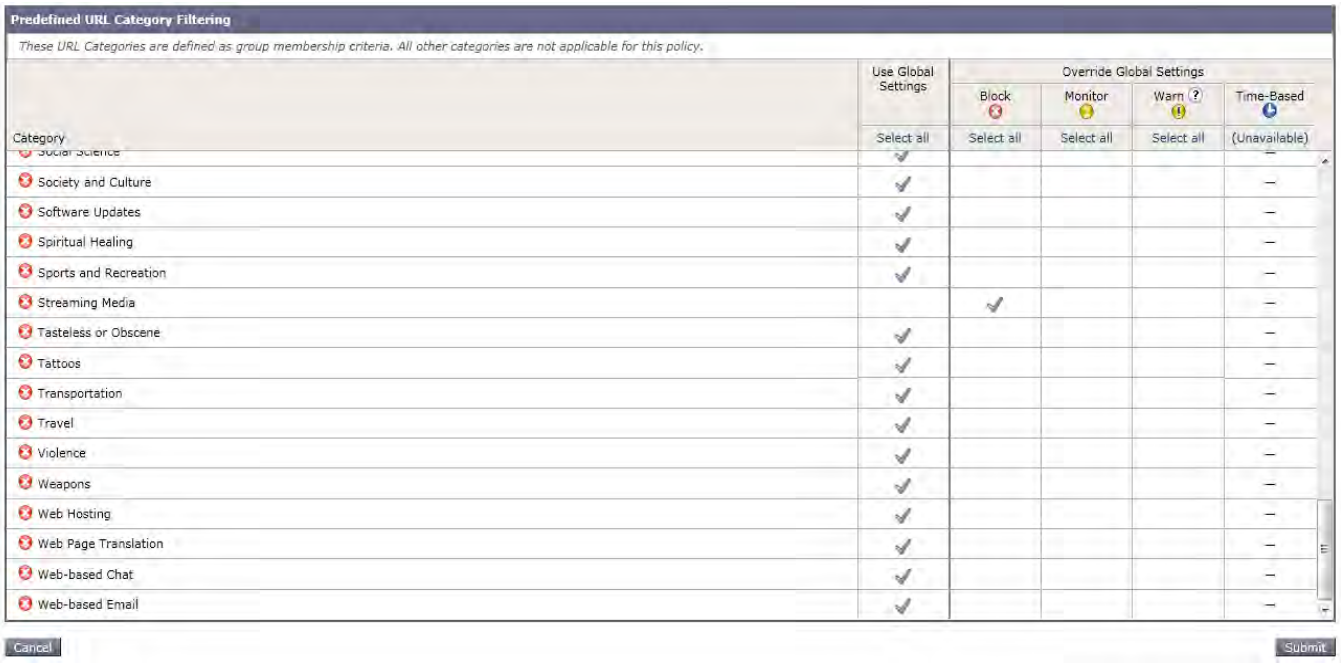


Click on submit and apply/commit the changes



Step 5: Deny Streaming Media pre-defined URL category for RemoteLAN access policy

Web Security Manager -> Access Policy -> RemoteLAN-> URL Category



Click on submit and apply/commit the changes

- HR department needs additional access, which is blocked by the global policy. They need access to various job search engines, social networking sites and conduct investigations of any mis-conduct by the employees. Configure a new access policy such that HR group and user IPEXPERT0\HRUSER1 user from 192.168.20.0/24 subnet can have additional web access as per the below table. Test by connecting to www.facebook.com. Verify using accesslog entries.

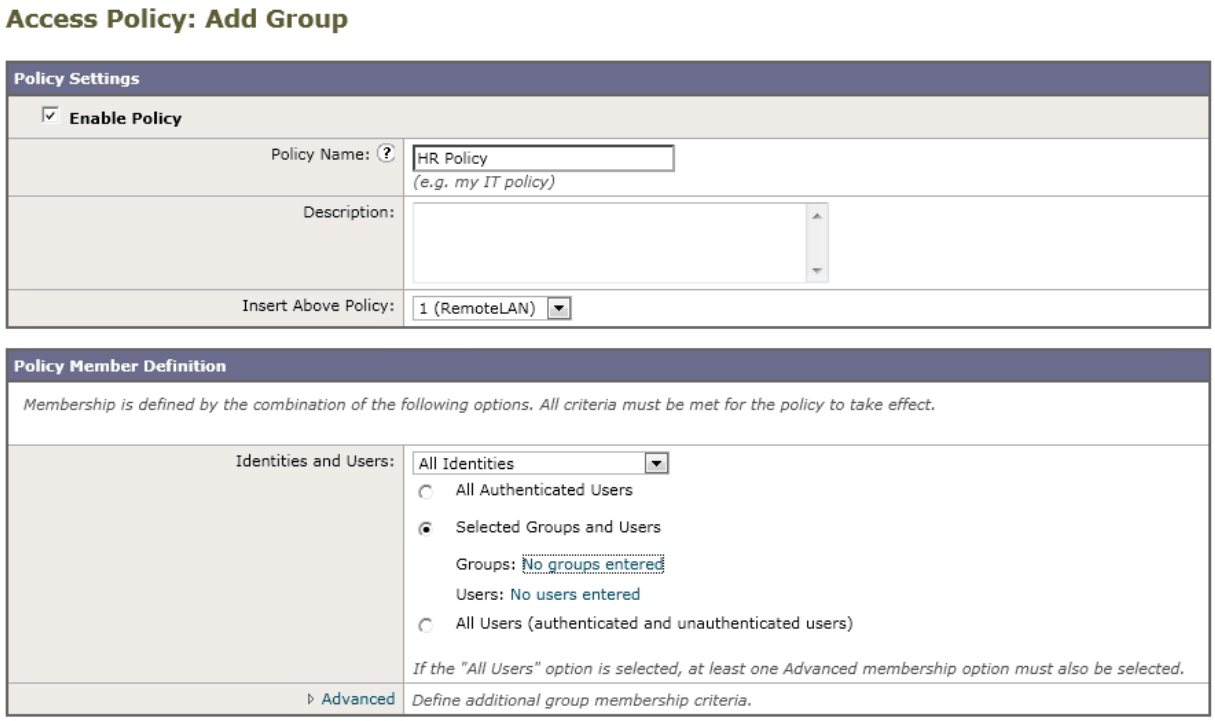
URL Filtering	
HR Policy	Besides the Global policy monitor the below URL categories based on giving warning/Splash page before they access those sites.
	Cheating and Plagiarism Illegal Activities Job Search Social Networking

Task-1: Solutions

Step 1: Create a new access policy called "HR Policy" based on 3 criteria i.e. webtraffic will match this access policy based on 3 conditions – AD group (HR), AD User (IPEXPERT0\HRUSER1) and subnet 192.168.20.0/24 (HR subnet)

Web Security Manager -> Access Policy -> Add Policy

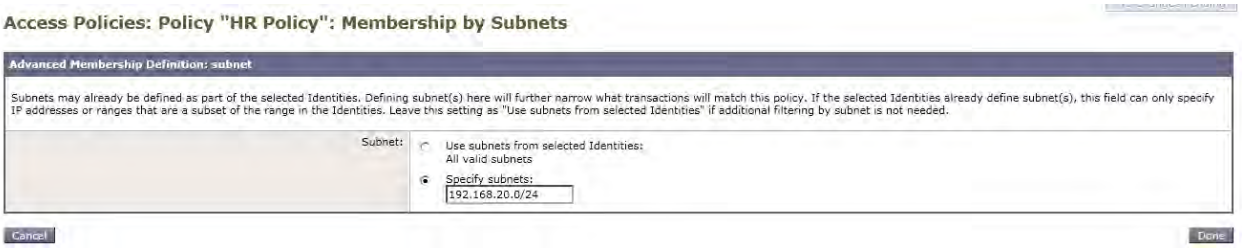
Create HR policy. In the Policy membership click on "Selected Groups and Users" and add the group and user information.

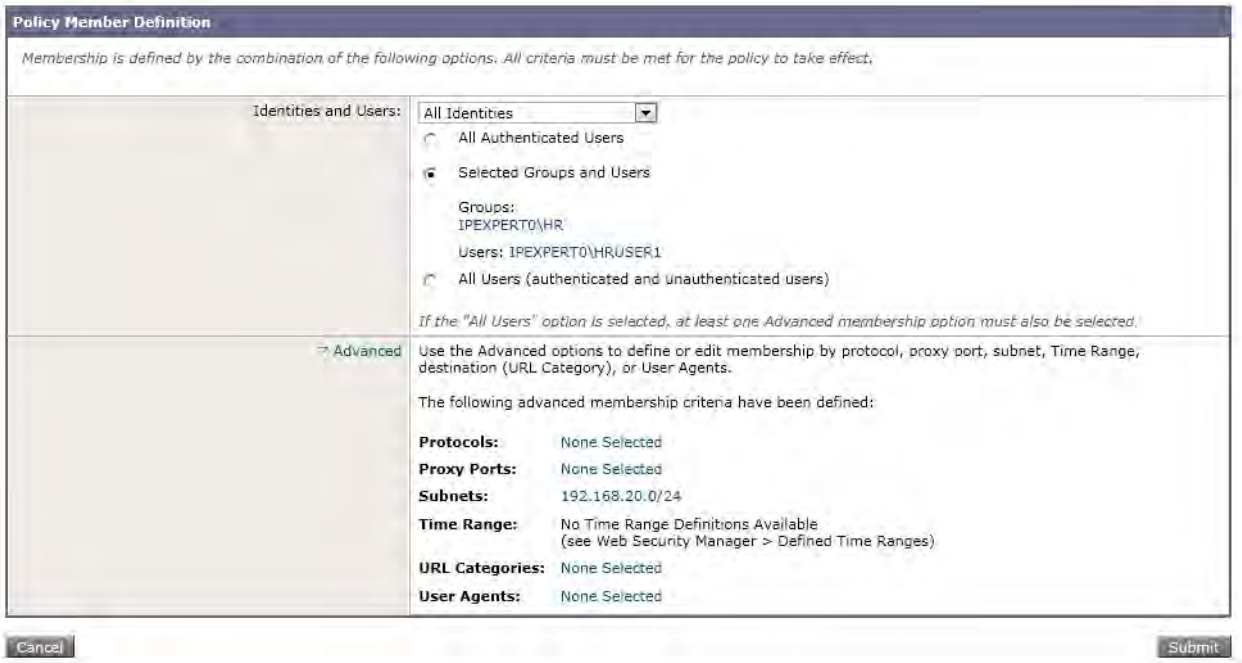


Select HR group from the AD directory

Add the username criteria to trigger this access policy

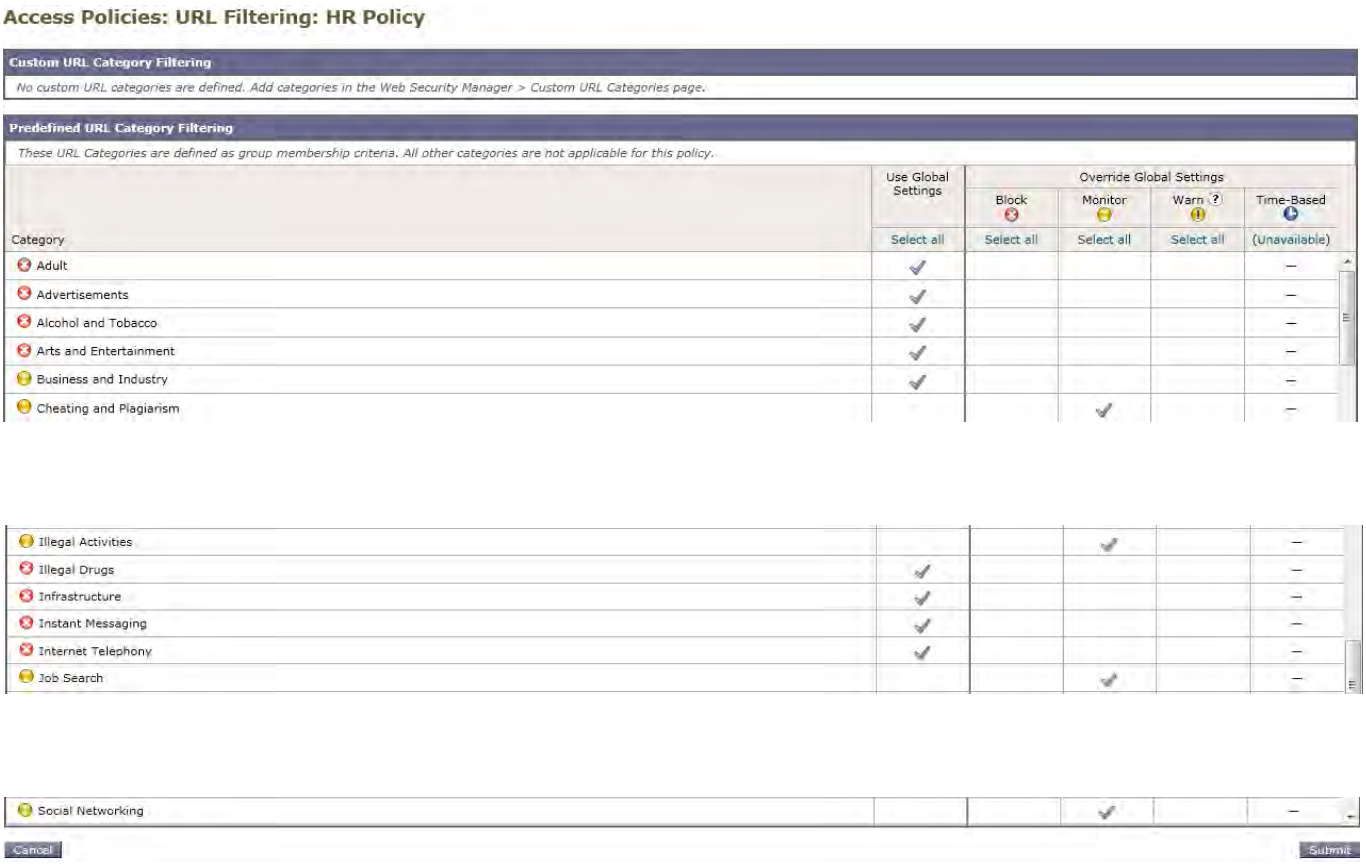
Add the subnet to trigger this access policy





Click on Submit and apply/commit the changes

Step 2: Monitor additional Pre-defined URL categories as per the task for HR policy



Click on Submit and apply/commit the changes

Commit Changes »

Access Policies

Success — Settings have been saved.

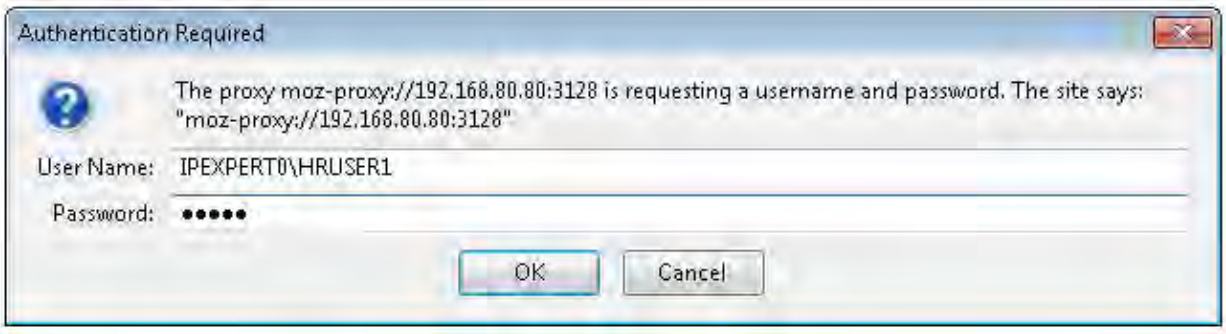
Policies

Add Policy...

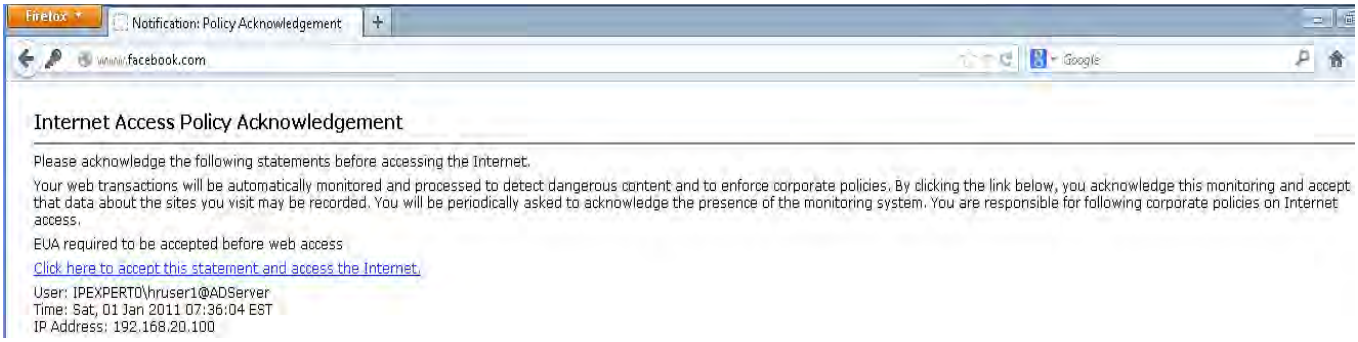
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	**HR Policy** Identity: All Subnets: 192.168.20.0/24	(global policy)	Block: 54 Monitor: 12 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	🗑
2	**RemoteLAN** Identity: All Subnets: 200.4.4.0/24, 200.5.5.0/24	(global policy)	Block: 59 Monitor: 7 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	🗑
	Global Policy Identity: All	Block: 2 Protocols	Block: 58 Monitor: 8 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 18	No blocked items	Web Reputation: Enabled	

Step 3: Test the HR policy from TEST-PC by browsing to www.facebook.com, which is allowed in the HR policy and blocked by the Global Policy. Use firefox and clear all history including offline data (Ctr+shift+delete). Note the PC is currently in the HR subnet.

Enter the user information



Accept the EUN. You may also notice your username and IP address information



You will successfully connected to www.facebook.com if your policy is correct. Below is the webpage that will be displayed when the traffic matches the access policy and authenticates correctly.

Access Logs

```
1293885407.634      1      192.168.20.100      TCP_DENIED/407      1766      GET
http://www.facebook.com/  -  NONE/-  -  OTHER-NONE-DefaultGroup-NONE-NONE-NONE-
NONE      <-,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-
","-","-","-",14128.00,0,-,"-","-"> -

1293885407.639      0      192.168.20.100      TCP_DENIED/407      451      GET
http://www.facebook.com/  -  NONE/-  -  OTHER-NONE-DefaultGroup-NONE-NONE-NONE-
NONE      <-,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-
","-","-","-",0.00,0,-,"-","-"> -

1293885408.014     373     192.168.20.100     TCP_REFRESH_HIT/200     426     GET
http://www.facebook.com/  "IPEXPERT0\hruser1@ADServer"  DIRECT/www.facebook.com
text/html      ALLOW_WBRS_11-HR_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_snet,7.0,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_snet,-,"-
","-","Facebook","Social Networking","-","-",9.14,0,-,"-","-"> -
```

- Finance department needs additional access, which is blocked by the global policy. They need access to various financial and trading sites. Configure a new access policy such that Finance group and user IPEXPERT0\FINUSER1 user from 192.168.22.0/24 subnet can have additional web access as per the below table. Test by connecting to www.ft.com. Verify using accesslog entries.

URL Filtering	
Finance Policy	Besides the Global policy monitor the below URL categories based on time based condition – Weekdays 9 AM to 5 PM.
	Finance – With time range – Monitor else Warn Online Trading – With time range – Monitor else block Real Estates – With time range – Monitor else block

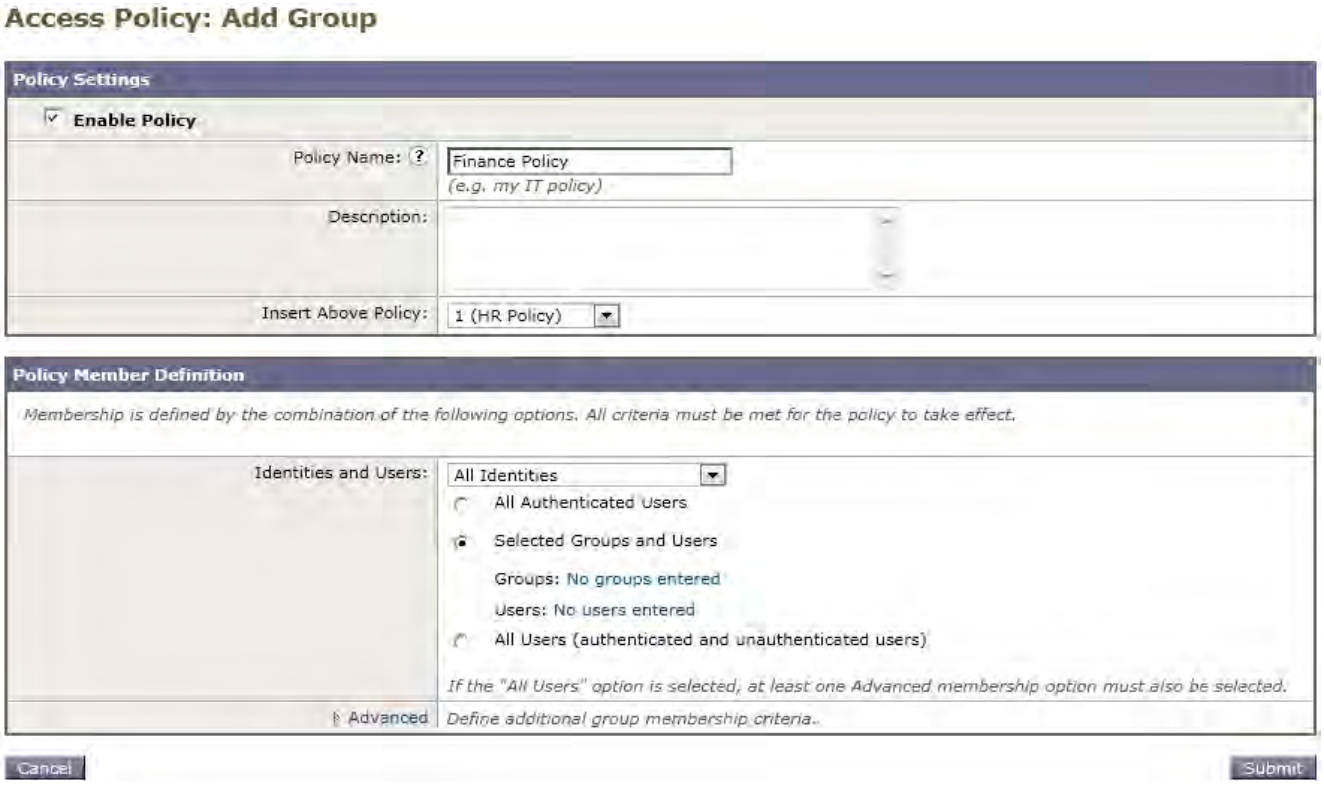
NOTE: *To test you will need to reconfigure the switch and the Test PC.*
Place the TEST-PC in VLAN 22 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW2 SVI VLAN 22 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

Task-1: Solutions

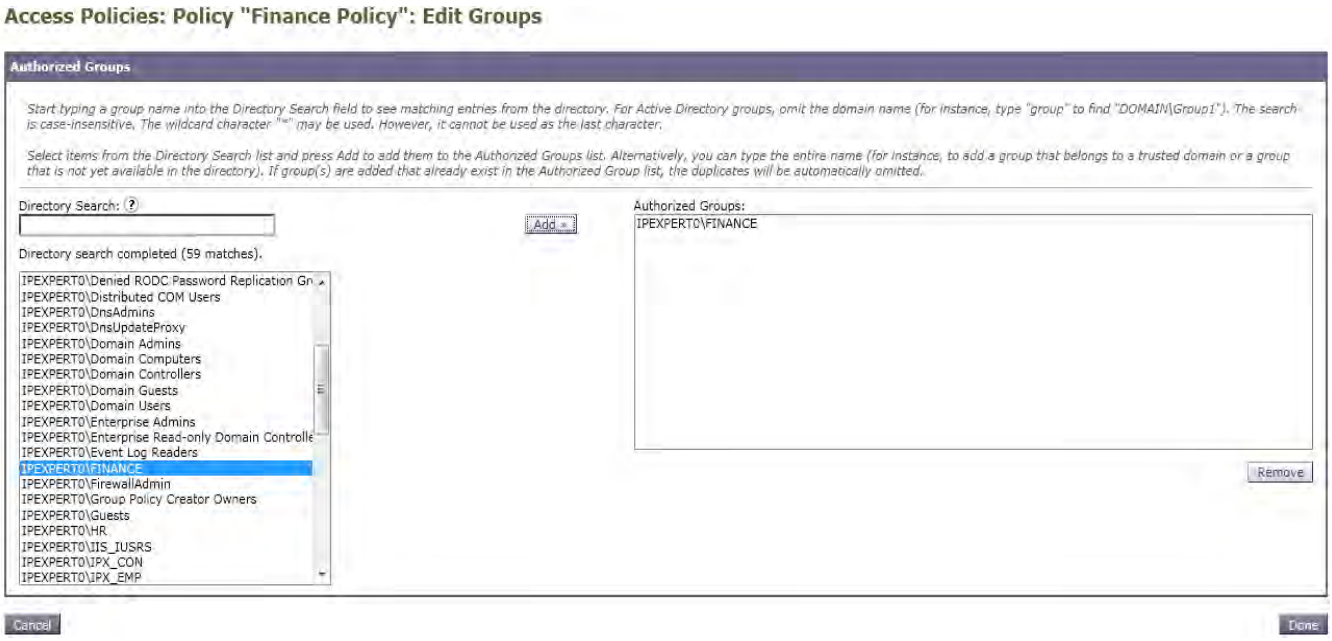
Step 1: Create a new access policy called "Finance Policy" based on 3 criteria i.e. webtraffic will match this access policy based on 3 conditions – AD group (Finance), AD User (IPEXPERT0\FINUSER1) and subnet 192.168.22.0/24 (Finance subnet)

Web Security Manager -> Access Policy -> Add Policy

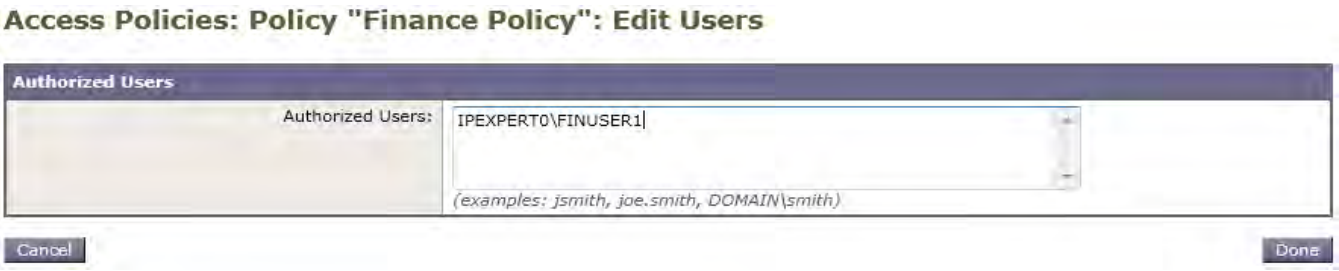
Create Finance policy. In the Policy membership click on "Selected Groups and Users" and add the group and user information.



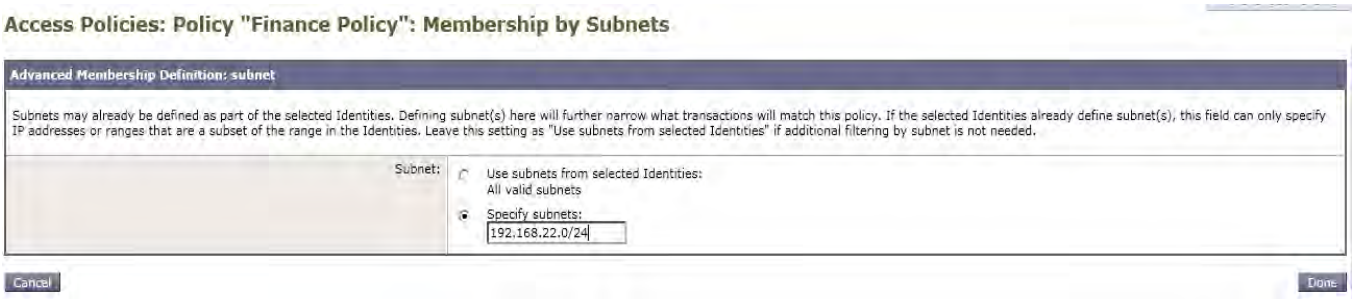
Select FINANCE group from the AD directory

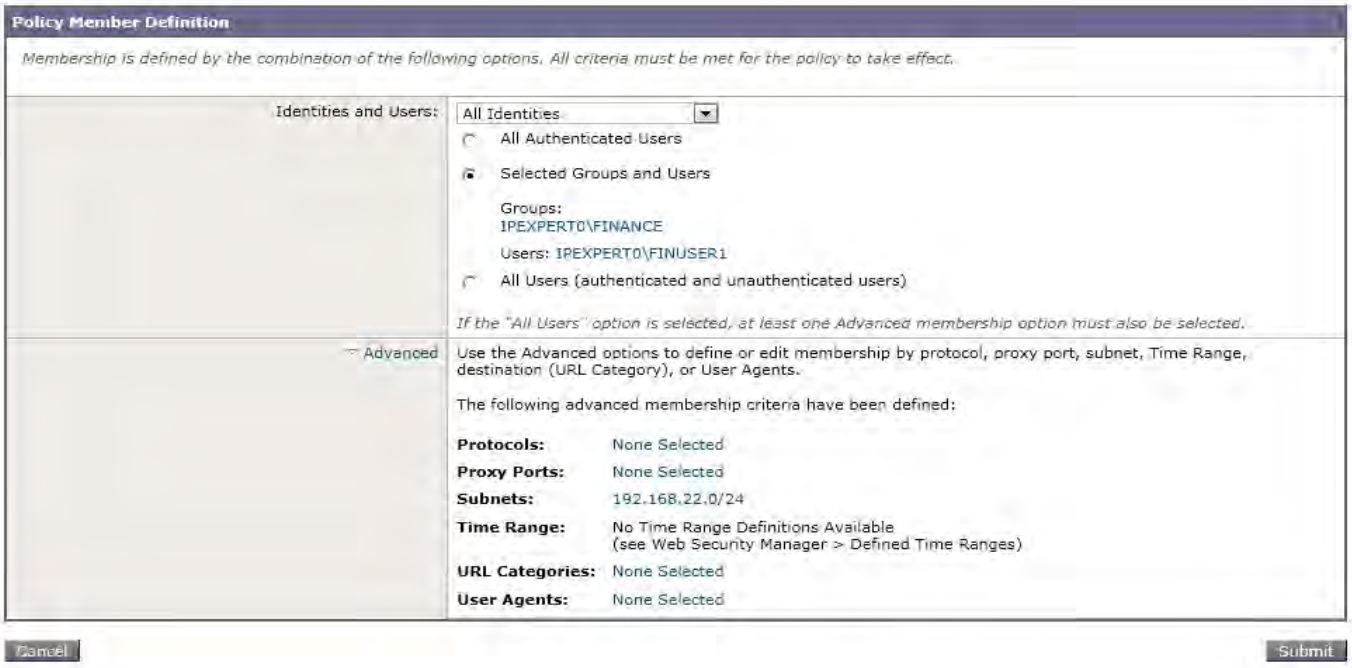


Add the username criteria to trigger this access policy



Add the subnet to trigger this access policy

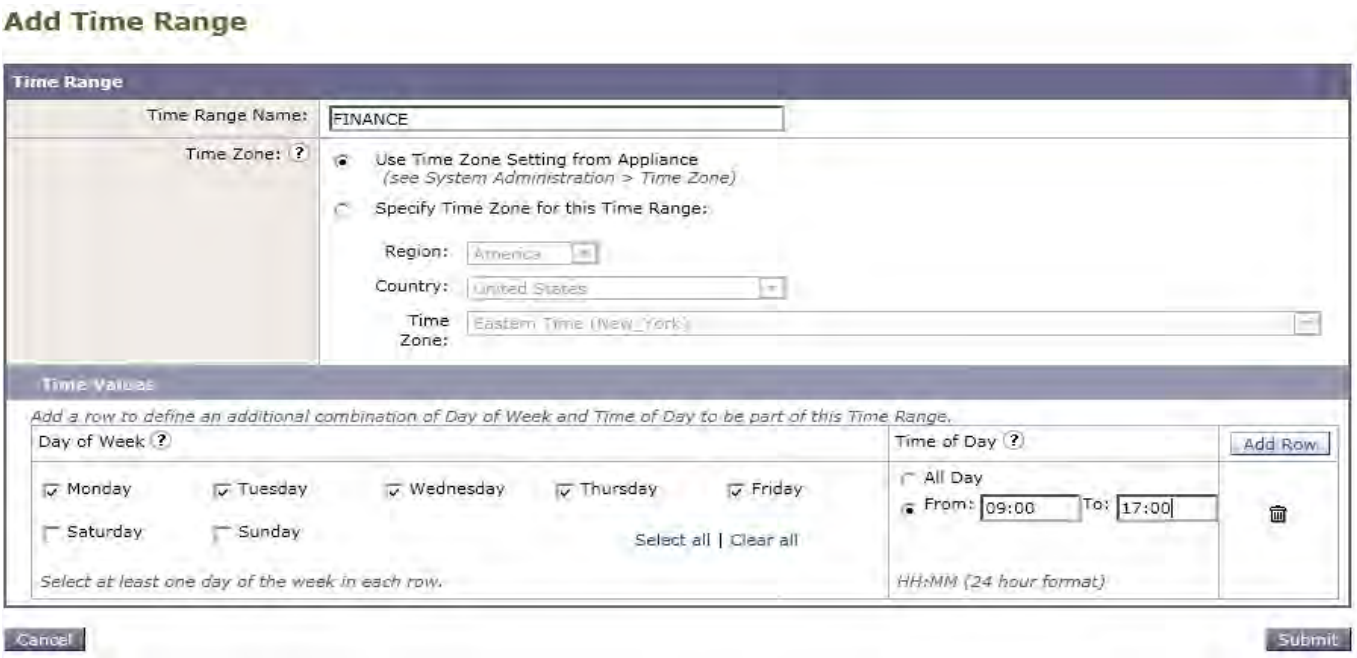




Click on Submit and apply/commit the changes

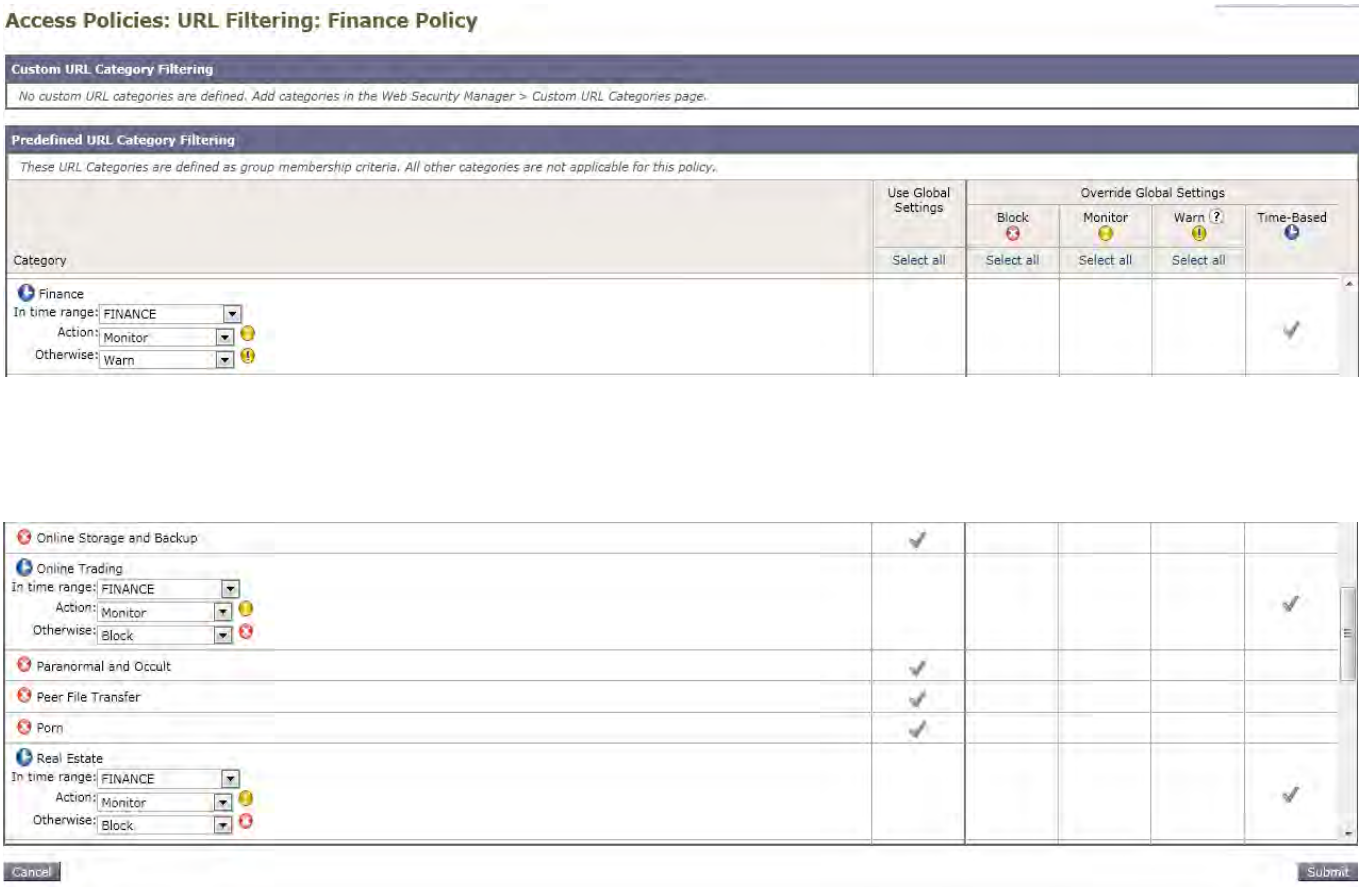
Step 2: Create a time range policy element needed for the Finance access policies as per the task.

Web Security Manager -> Defined Time Ranges -> Add Time Range

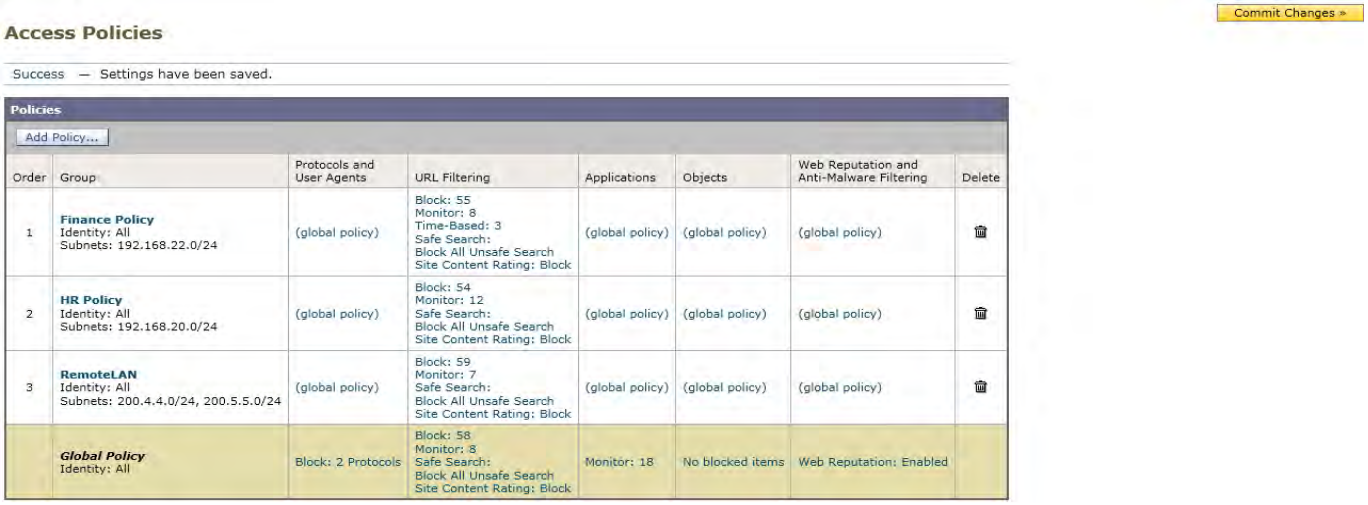


Click on Submit and apply/commit the changes

Step 3: Monitor additional Pre-defined URL categories as per the task for Finance policy based on time ranges.



Click on Submit and apply/commit the changes



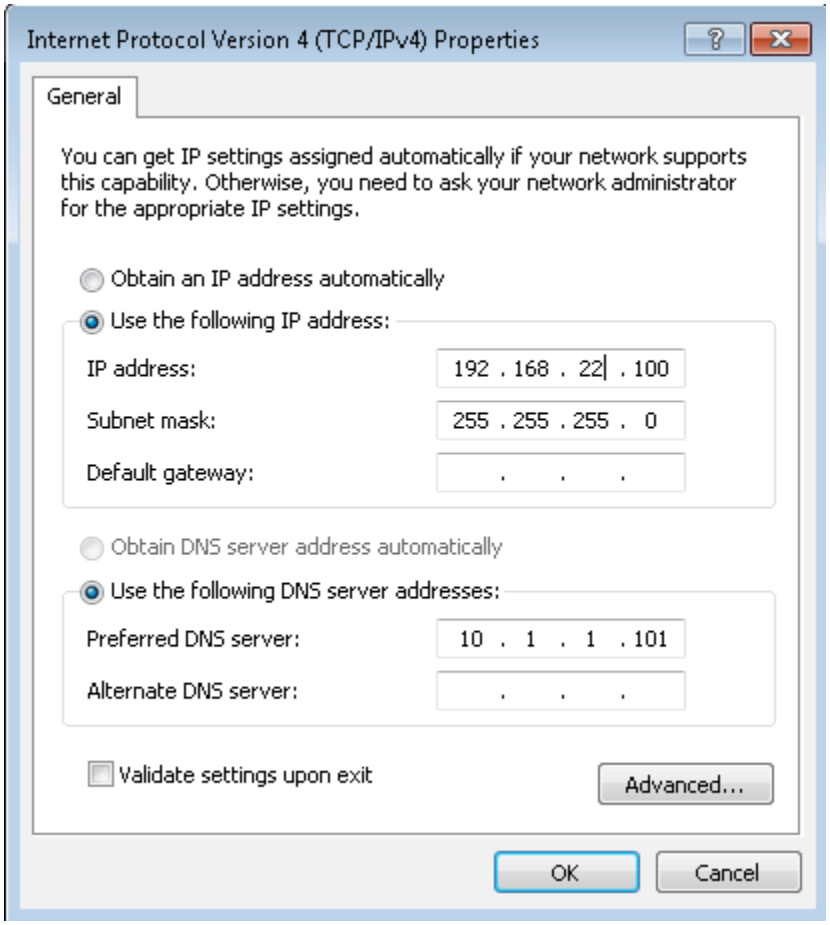
Step 4: Place the TEST PC in VLAN 22 and change the IP address to 192.168.22.100. Make sure you add the static routes on the PC

SW3

```
interface GigabitEthernet1/0/2
 switchport access vlan 22
 switchport mode access
 spanning-tree portfast
```

TEST PC

Configure the IP address to an IP from the Finance subnet. Do not set the default gateway.

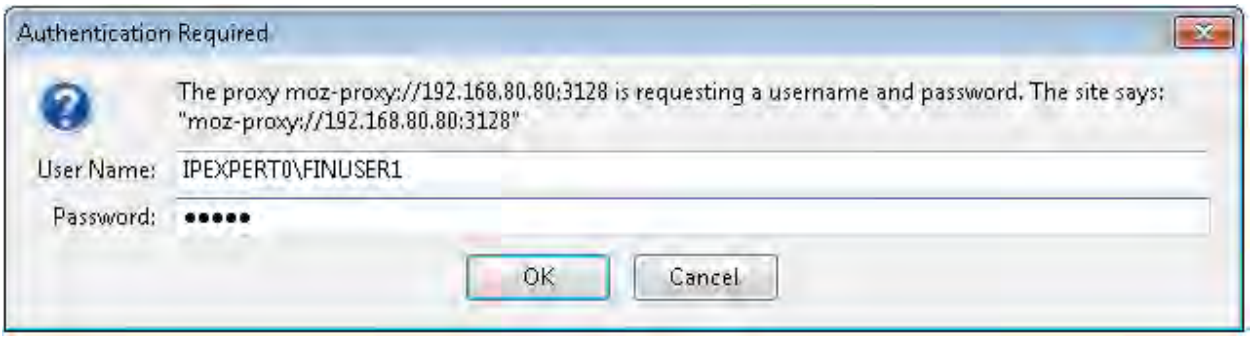


Delete the previously configured static routes and add the new static routes with next hop as SW2 (192.168.22.1). Ping the default gateway and WSA for testing purpose.

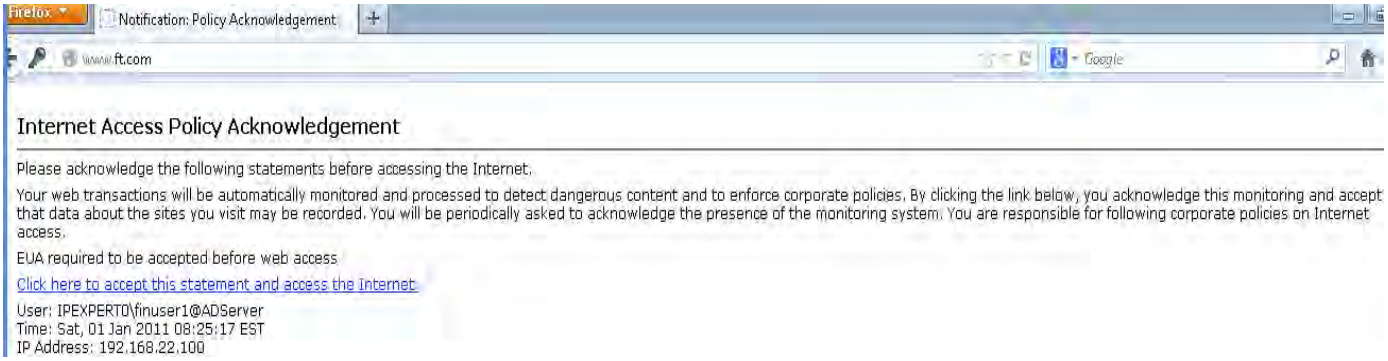
```
Administrator: Elevated CMD
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>route delete 10.1.1.101
 OK!

C:\Windows\System32>route delete 192.168.0.0
 OK!

C:\Windows\System32>route add 10.1.1.101 mask 255.255.255.255 192.168.22.1
 OK!

C:\Windows\System32>route add 192.168.0.0 mask 255.255.0.0 192.168.22.1
 OK!

C:\Windows\System32>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:
Reply from 192.168.22.1: bytes=32 time=4ms TTL=255
Reply from 192.168.22.1: bytes=32 time=1ms TTL=255
Reply from 192.168.22.1: bytes=32 time=1ms TTL=255
Reply from 192.168.22.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Windows\System32>ping 192.168.88.80

Pinging 192.168.88.80 with 32 bytes of data:
Reply from 192.168.88.80: bytes=32 time=2ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62

Ping statistics for 192.168.88.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Step 5: Test the Finance policy from TEST-PC by browsing to www.ft.com, which is allowed in the Finance policy and blocked by the Global Policy. Use Firefox and clear all history including offline data (Ctr+shift+delete).

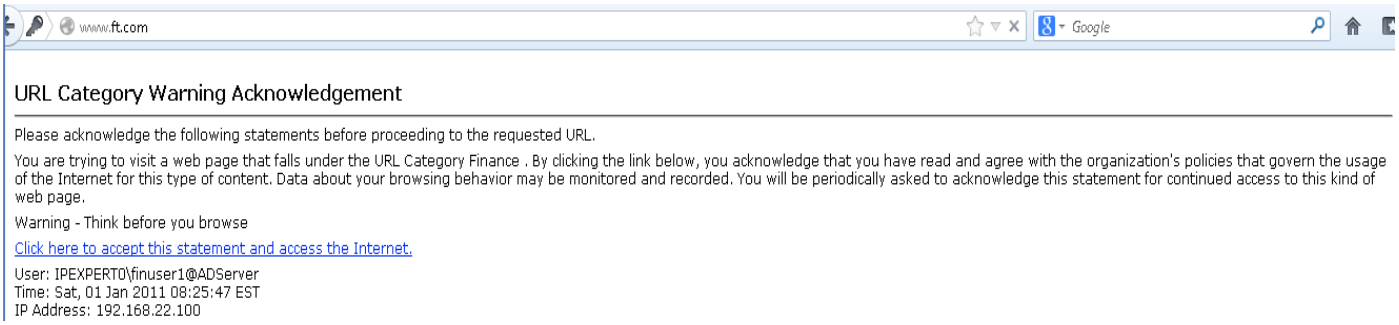
Enter the user information



Accept the EUN. Notice the uername/Group/IP information



Accept the Warning Page since Jan 1st 2011 is a Saturday (weekend)



If you policy is configured correctly you must see the below screen for www.ft.com

Access Logs

```
1293888347.243  1 192.168.22.100 TCP_DENIED/407 1766 GET http://www.ft.com/ -
NONE/-  -  OTHER-NONE-Default  Group-NONE-NONE-NONE-NONE  <-,-,"-","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",14128.00,0,-,"-
","-"> -

1293888347.249  0 192.168.22.100 TCP_DENIED/407 451 GET http://www.ft.com/ -
NONE/-  -  OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE  <-,-,"-","-",-,-,-,"-
```

","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,"-","-
"> -

1293888347.253 2 192.168.22.100 TCP_DENIED/403 2055 GET http://www.ft.com/
"IPEXPERT0\finuser1@ADServer" NONE/- - BLOCK_CONTINUE_WEBCAT_11-
Finance_Policy-DefaultGroup-NONE-NONE-NONE-NONE <IW_fnnc,4.9,"1","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,IW_fnnc,-,"-","-","Unknown","Unknown","-
","-",8220.00,0,-,"-","-"> -

1293888376.230 1211 192.168.22.100 TCP_MISS/200 413 GET http://www.ft.com/
"IPEXPERT0\finuser1@ADServer" DIRECT/www.ft.com text/html
MONITOR_CONTINUE_WEBCAT_11-Finance_Policy-DefaultGroup-NONE-NONE-NONE-
DefaultGroup <IW_fnnc,4.9,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-
,IW_fnnc,-,"-","-","Unknown","Unknown","-","-",2.73,0,-,"-","-"> -

- IT department needs additional access, which is blocked by the global policy. Configure a new access policy such that IT group and user IPEXPERT0\ITUSER1 user from 192.168.30.0/24 subnet can have additional web access as per the below table. IT users will need to use FTP. Hence allow FTP protocols. Test by connecting to www.gmail.com and also to the FTP server ftp.ipexpert.com.

- Use Filzilla client on TEST-PC to point to WSA for FTP proxy and configure checkpoint format for on the Native FTP client for FTP proxy authentication.

URL Filtering	
IT Policy	Besides the Global policy monitor the below URL categories. WSA should present warning only for File Transfer Services.
	File Transfer Series (WARN) Software Updates Web Hosting Web Page Translation Web-based Chat Web-based Email

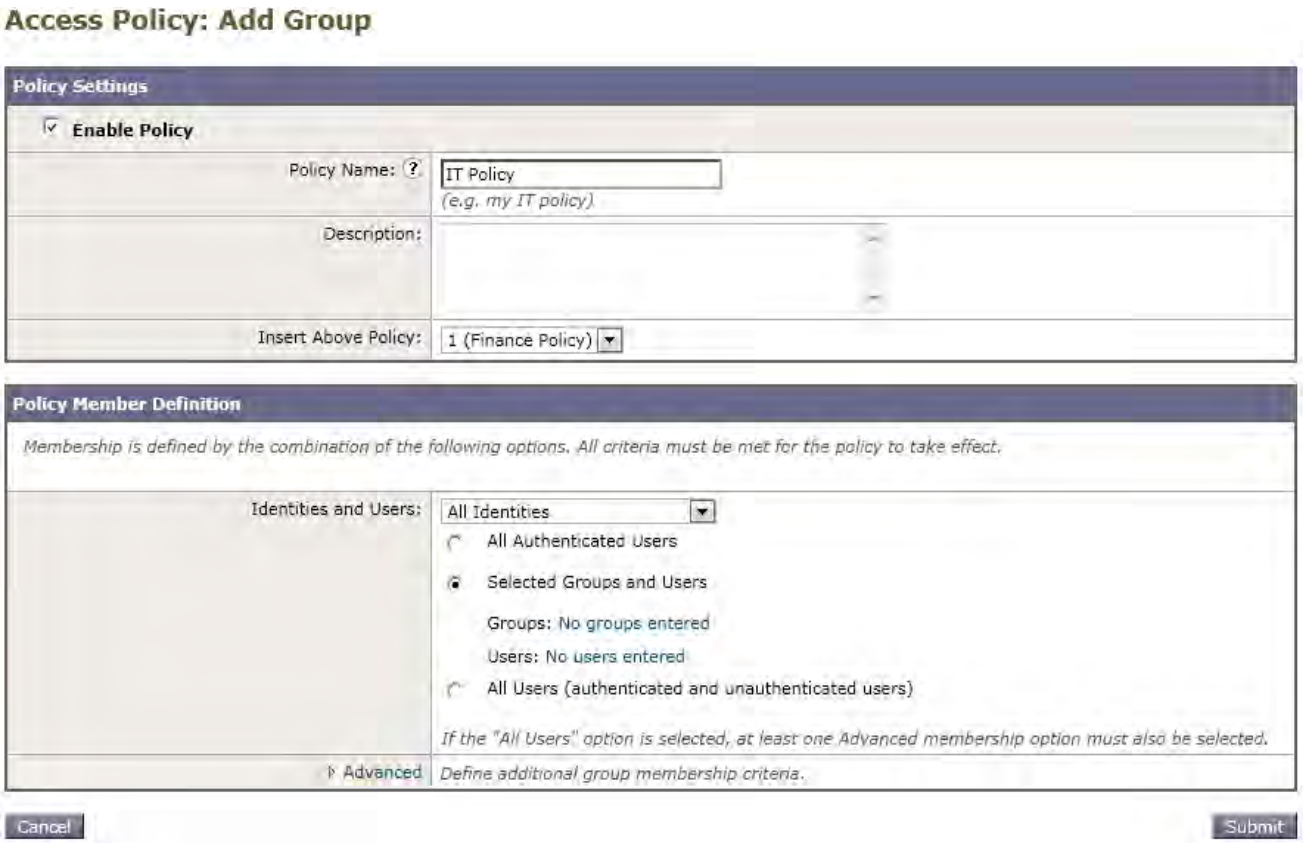
NOTE: *To test you will need to reconfigure the switch and the Test PC.*
Place the TEST-PC in VLAN 30 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW3 SVI VLAN 30 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

Task-1: Solutions

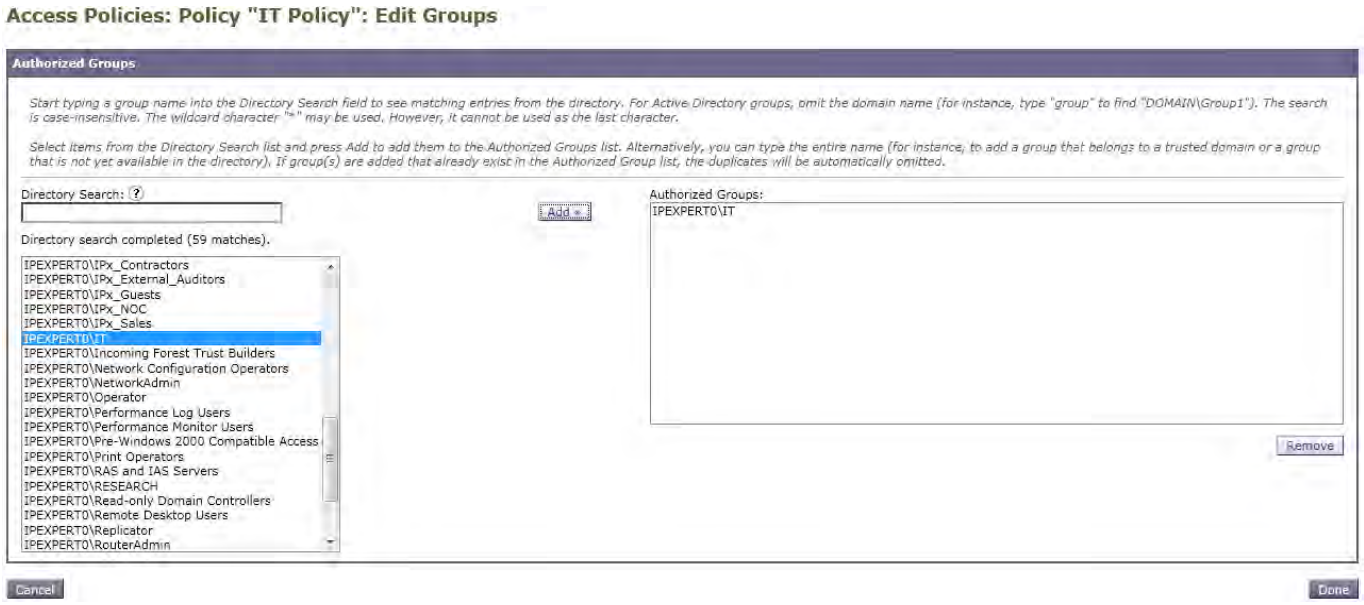
Step 1: Create a new access policy called "IT Policy" based on 3 criteria i.e. webtraffic/FTP will match this access policy based on 3 conditions – AD group (IT), AD User (IPEXPERT0\ITUSER1) and subnet 192.168.30.0/24 (IT subnet)

Web Security Manager -> Access Policy -> Add Policy

Create IT policy. In the Policy membership click on "Selected Groups and Users" and add the group and user information.

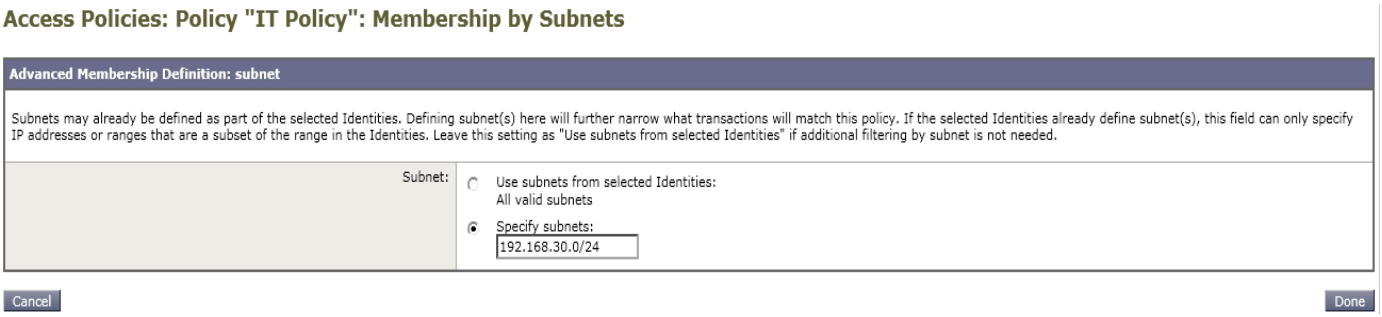


Select IT group from the AD directory

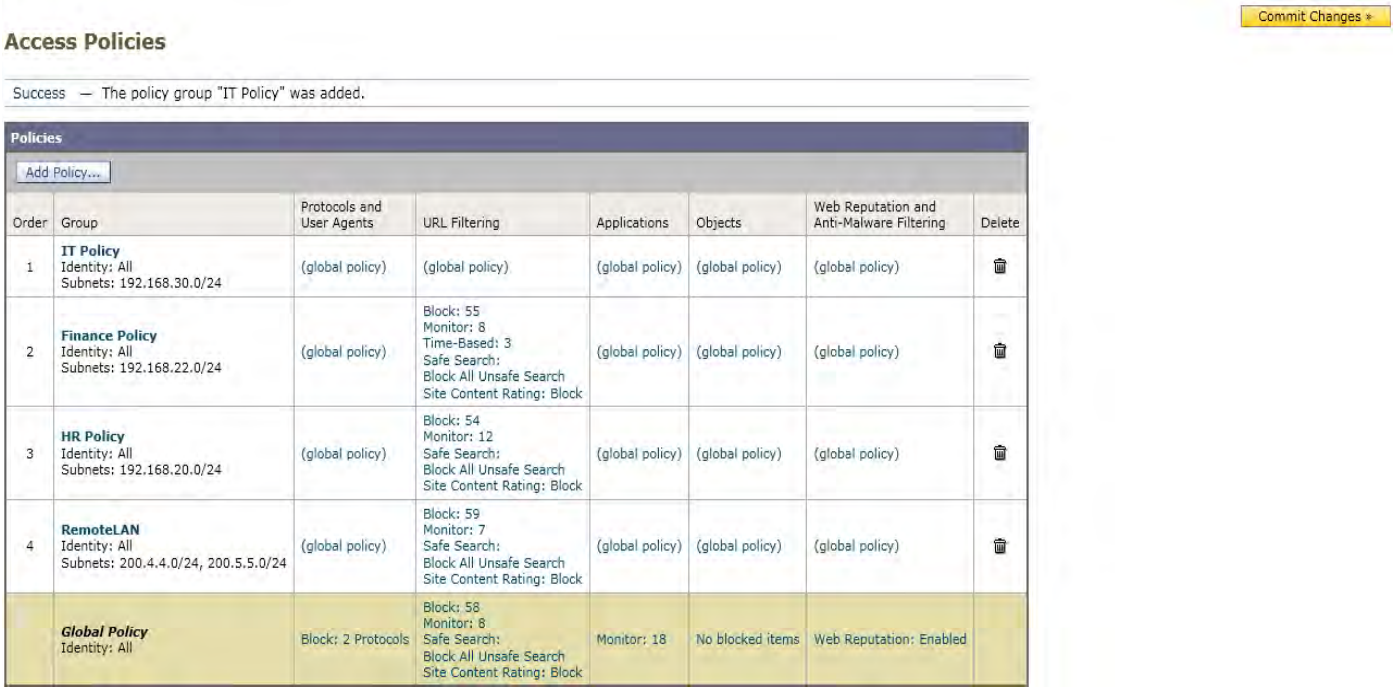


Add the username criteria to trigger this access policy

Add the subnet to trigger this access policy

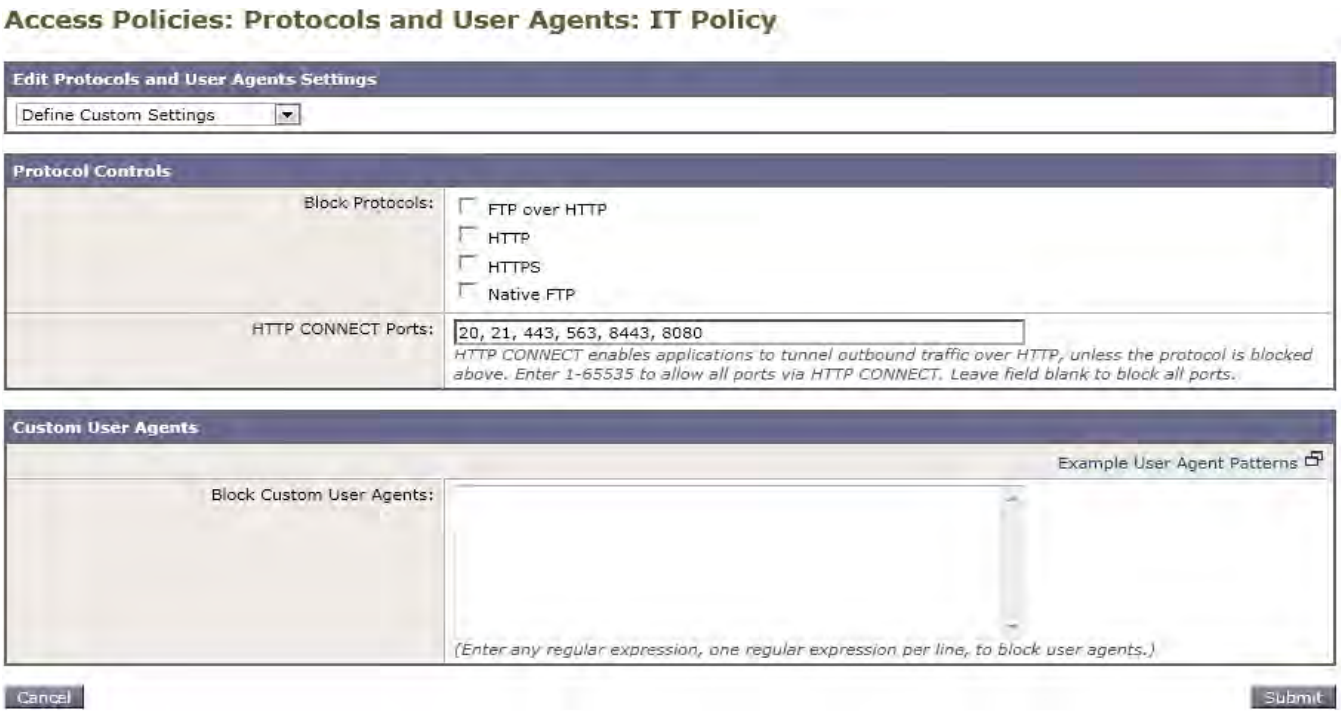


Click on Submit and apply/commit the changes

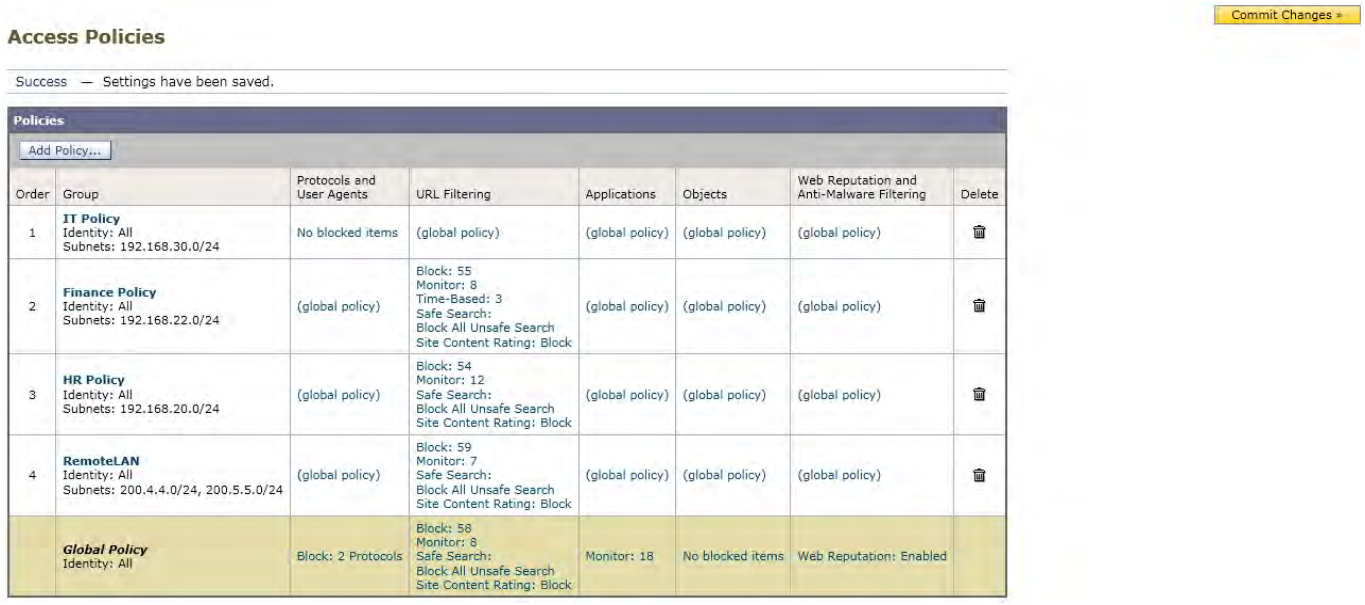


Step 2: Allow FTP protocol for IT Access policy.

Web Security Manager -> Access Policy -> Protocols and User Agents (IT Policy)

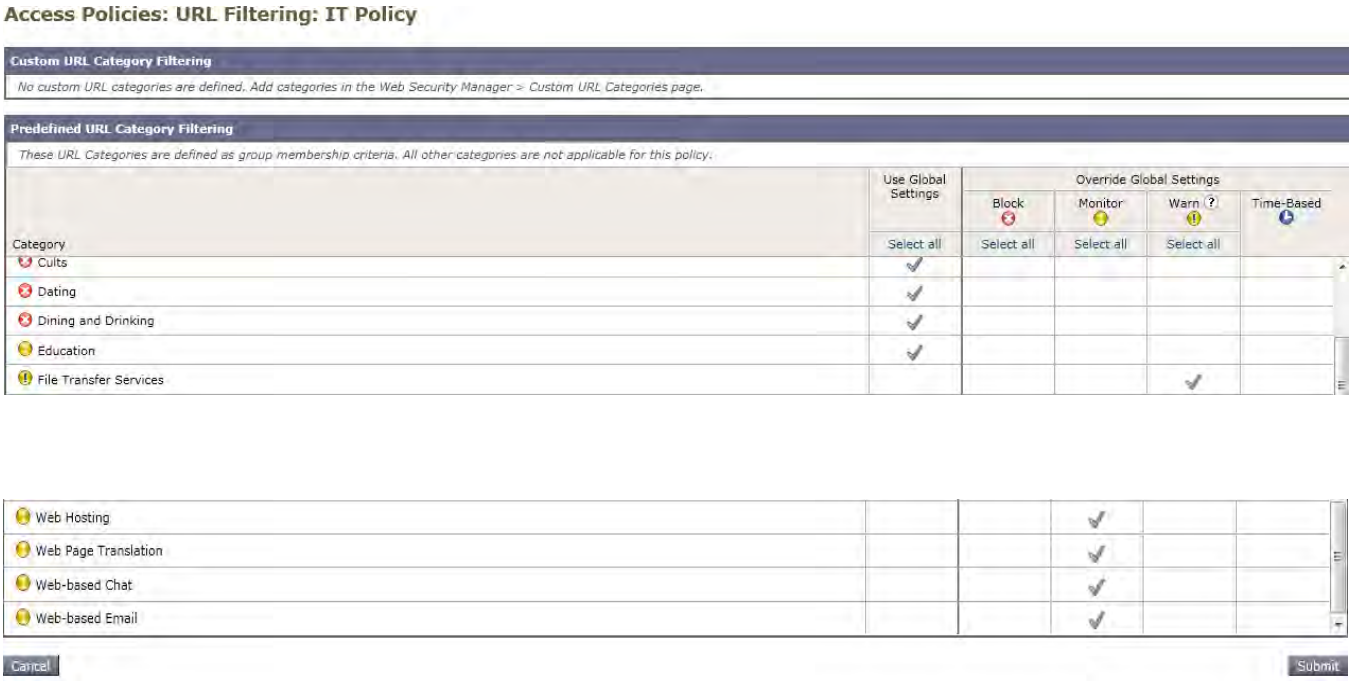


Click on Submit and apply/commit the changes



Step 3: Monitor additional Pre-defined URL categories as per the task for IT policy

Web Security Manager -> Access Policy -> URL Filtering (IT Policy)



Click on Submit and apply/commit the changes

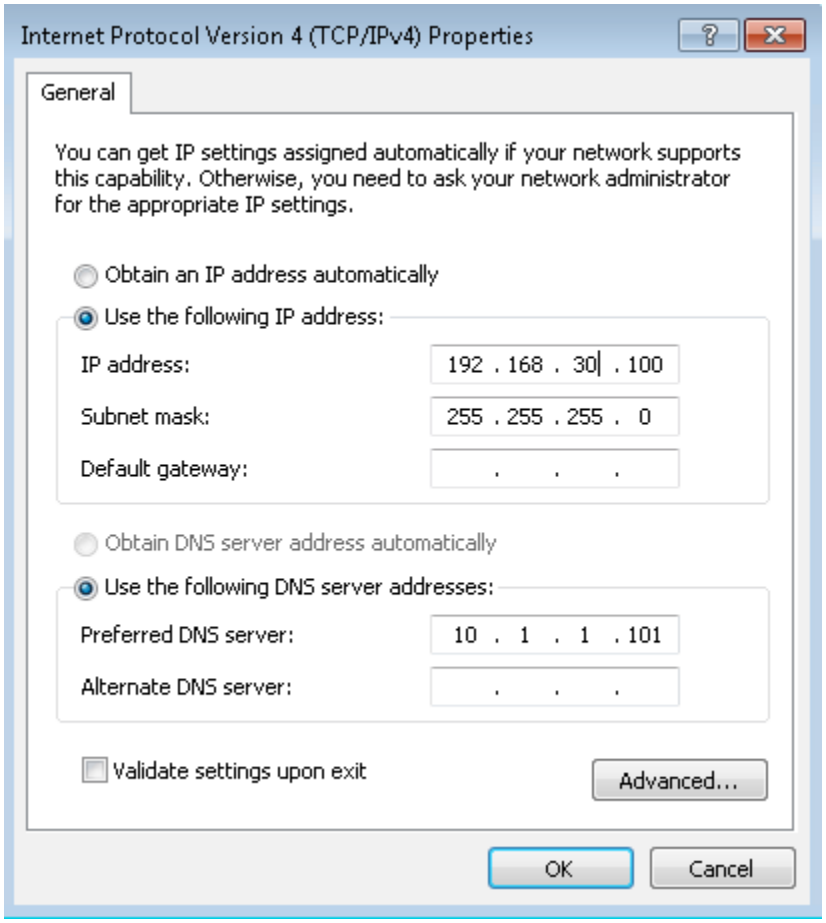
Step 4: Place the TEST PC in VLAN 30 and change the IP address to 192.168.30.100. Make sure you add the static routes on the PC

SW3

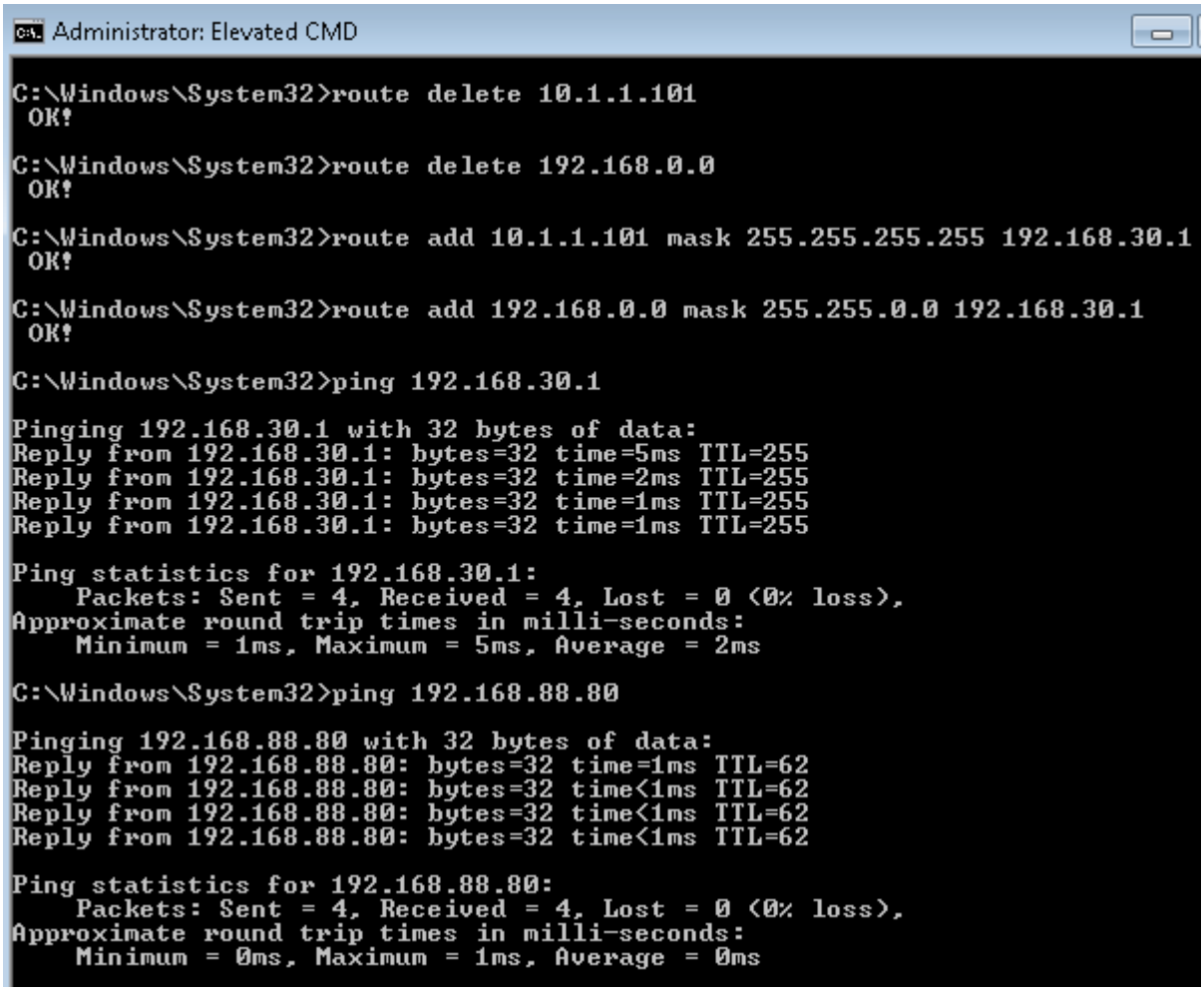
```
interface GigabitEthernet1/0/2
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
```

TEST PC

Configure the IP address to an IP from the IT subnet. Do not set the default gateway.

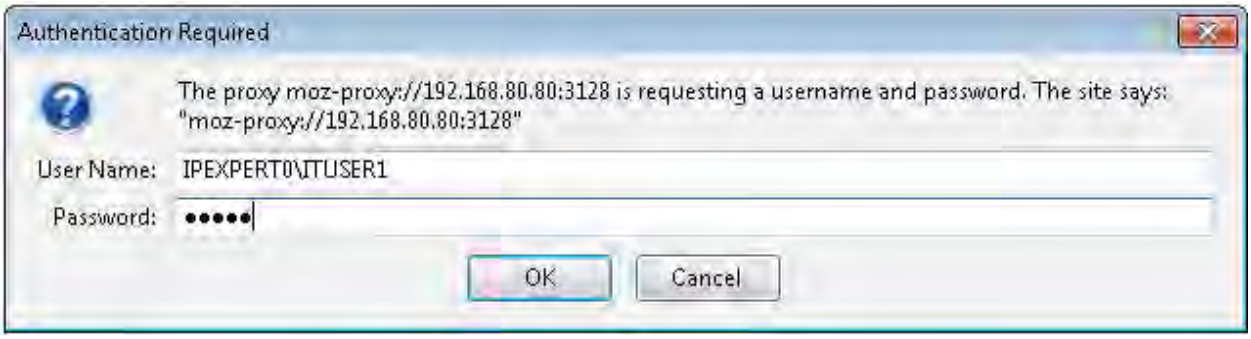


Delete the previously configured static routes and add the new static routes with next hop as SW3 (192.168.30.1). Ping the default gateway and WSA for testing purpose.

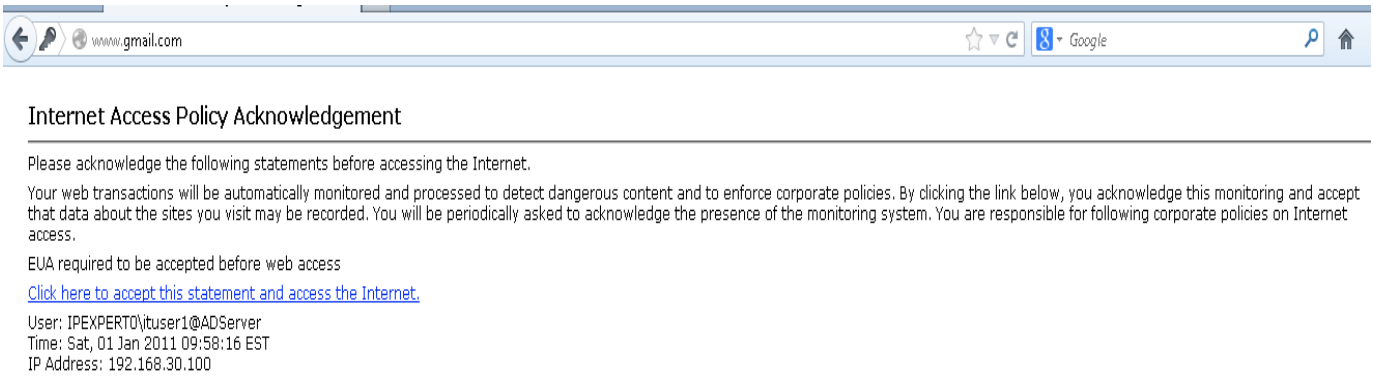


Step 4: Test the IT policy from TEST-PC by browsing to www.gmail.com, which is allowed in the HR policy and blocked by the Global Policy. Use Firefox and clear all history including offline data (Ctr+shift+delete). Note the PC is currently in the HR subnet.

Enter the user information



Accept the EUN. You may also notice your username and IP address information



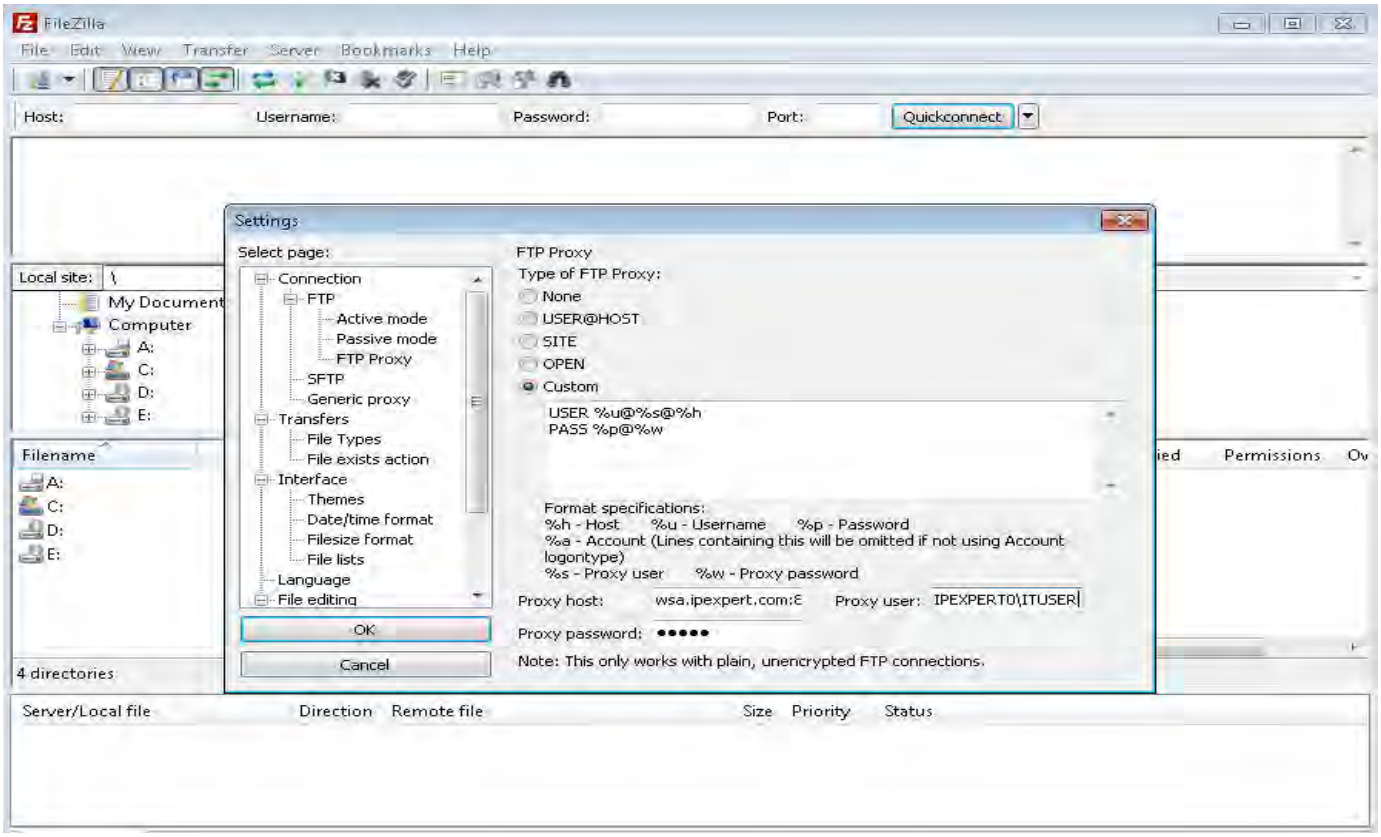
You will successfully connected to www.gmail.com if your policy is correct. Below is the webpage that will be displayed when the traffic matches the access policy and authenticates correctly.

Access Logs

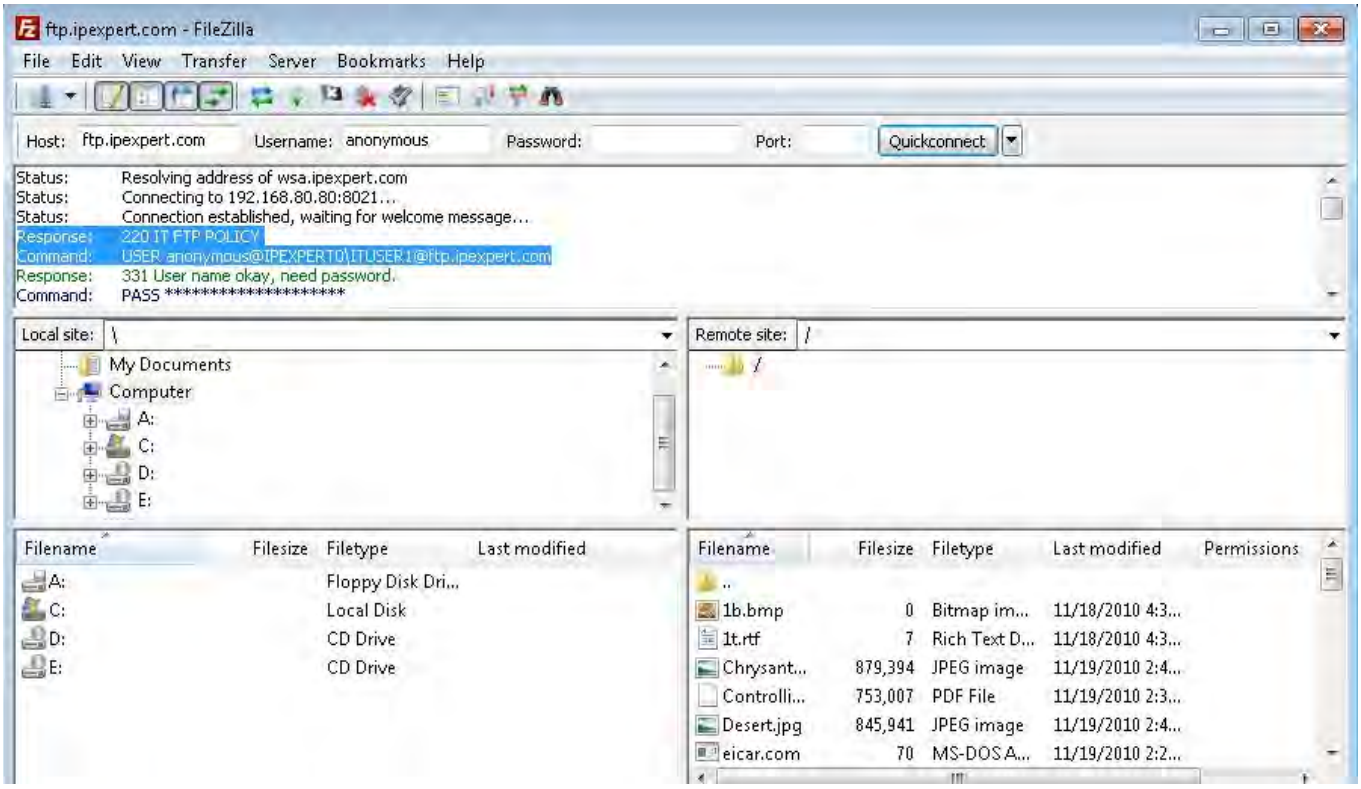
```
1293893917.451  1 192.168.30.100 TCP_DENIED/407 1766 GET http://www.gmail.com/
- NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE <-,-,"-","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",14128.00,0,-,"-
","-"> -

1293893917.457  0 192.168.30.100 TCP_DENIED/407 451 GET http://www.gmail.com/
- NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE <-,-,"-","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,"-","-
"> -

1293893917.592  133 192.168.30.100 TCP_MISS/200 417 GET http://www.gmail.com/
"IPEXPERT0\ituser1@ADServer" DIRECT/www.gmail.com text/html DEFAULT_CASE_11-
IT_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_mail,4.9,"1","-",-,-,-
,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_mail,-,"-","-","Unknown","Unknown","-
","-",25.08,0,-,"-","-"> -
```

Step 5: Configure the FileZilla client with checkpoint authentication.

Edit->Settings. (Proxy host – wsa.ipexpert.com:8021 with proxy username and password)



Download a file for testing purpose. You may also see the FTP custom banner in the below screenshot.



Access Logs

```
1293894718.593 12 192.168.30.100 NONE/226 1724 LIST ftp://ftp.ipexpert.com -
DIRECT/ftp.ipexpert.com - OTHER-NONE-NONE-NONE-NONE-NONE-NONE <-,-,"-","-",-
,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-
",1149.33,0,-,"-","-"> -

1293894825.536 12 192.168.30.100 NONE/226 0 RETR
ftp://ftp.ipexpert.com/1b.bmp "IPEXPERT0\ITUSER1@ADServer"
DIRECT/ftp.ipexpert.com - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<IW_edu,0.0,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_edu,-,"-","-
","Unknown","Unknown","-","-",0.00,0,-,"-","-"> -
```

- Research department users require complete web access for R&D purposes. Configure a new access policy such that Research group and user IPEXPERT0\RUSER1 from 192.168.33.0/24 research subnet can have full access to the web. Monitor all categories and allow FTP protocols. Do not enforce URL content filtering inherited from the global policy.
- Unless WBRS or other scanners block a website, the user should have complete access to the web. Test by connecting to www.facebook.com, www.google.com. You should be presented with a block page when you connect to www.ieplugin.com or www.ihaveabadreputation.com based on WBRS.
- 192.168.33.33 should bypass AD authentication. You are allowed to configure a new Identity and access policy for this. This policy should be effective any time during weekdays and between 10 AM to 4 PM during weekends.

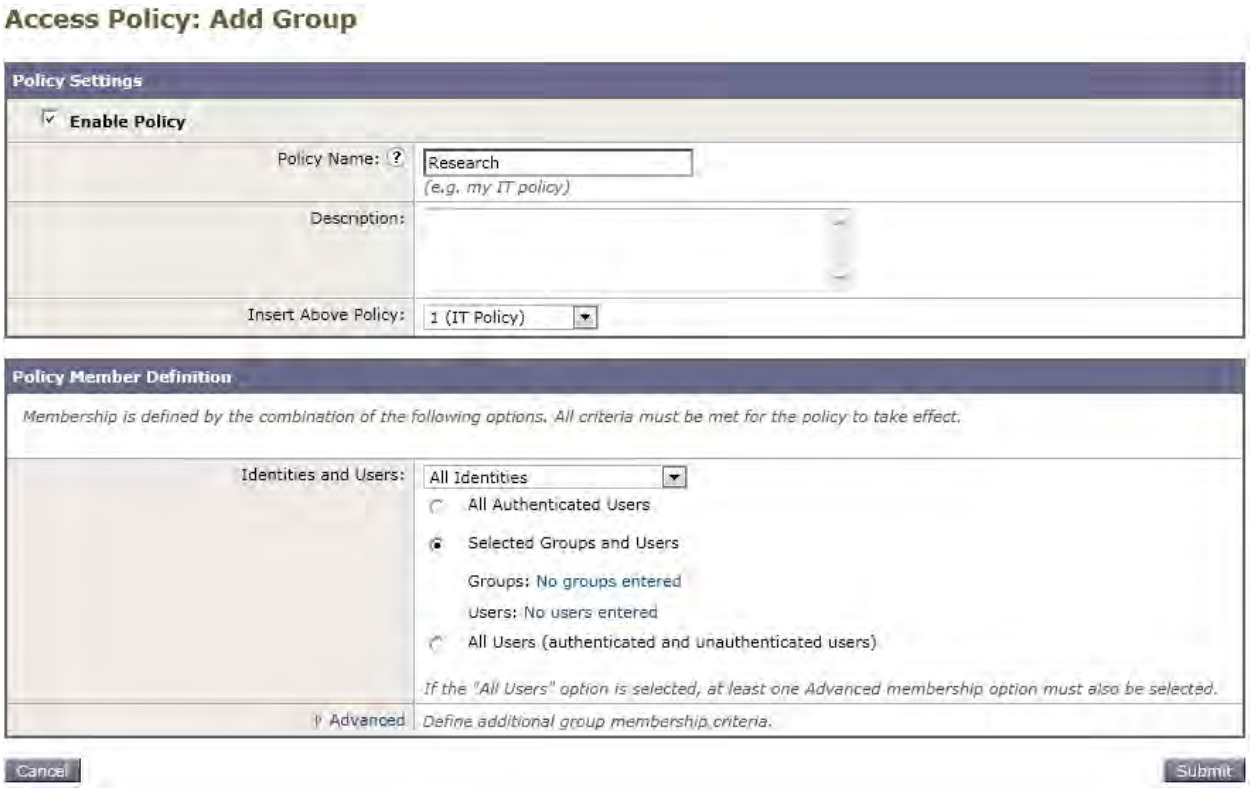
NOTE: To test you will need to reconfigure the switch and the Test PC.
Place the TEST-PC in VLAN 33 and use IP of 192.168.33.33. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW3 SVI VLAN 33 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

Task-1: Solutions

Step 1: Create a new access policy called “Research Policy” based on 3 criteria i.e. webtraffic will match this access policy based on 3 conditions – AD group (Research), AD User (IPEXPERT0\RUSER1) and subnet 192.168.33.0/24 (Research subnet)

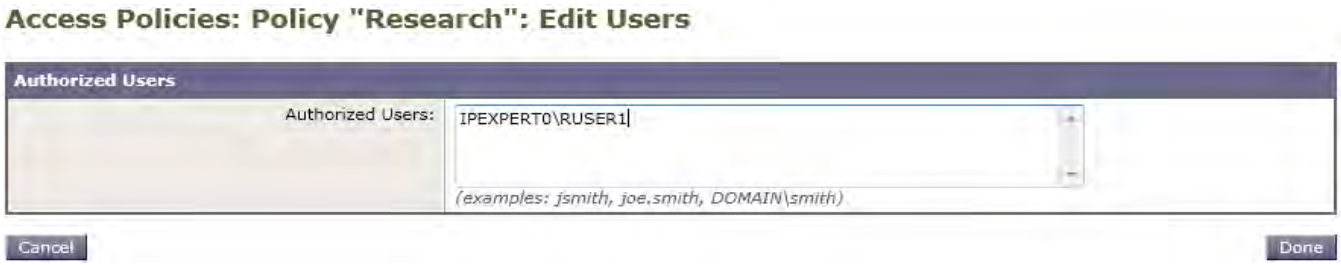
Web Security Manager -> Access Policy -> Add Policy

Create Research policy. In the Policy membership click on “Selected Groups and Users” and add the group and user information.

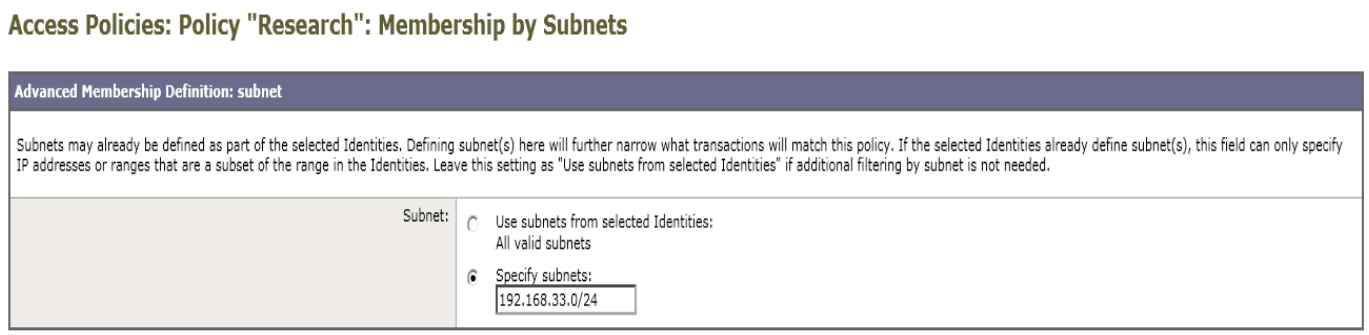


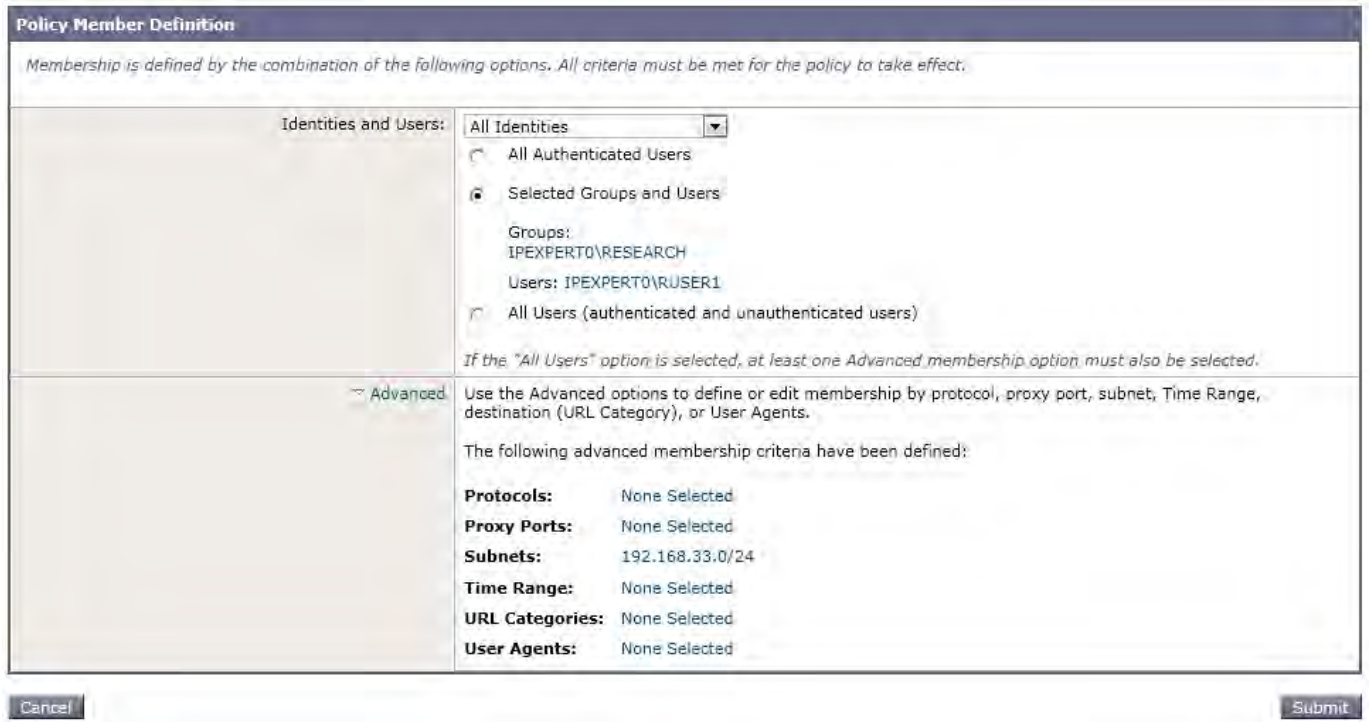
Select IT group from the AD directory

Add the username criteria to trigger this access policy



Add the subnet to trigger this access policy

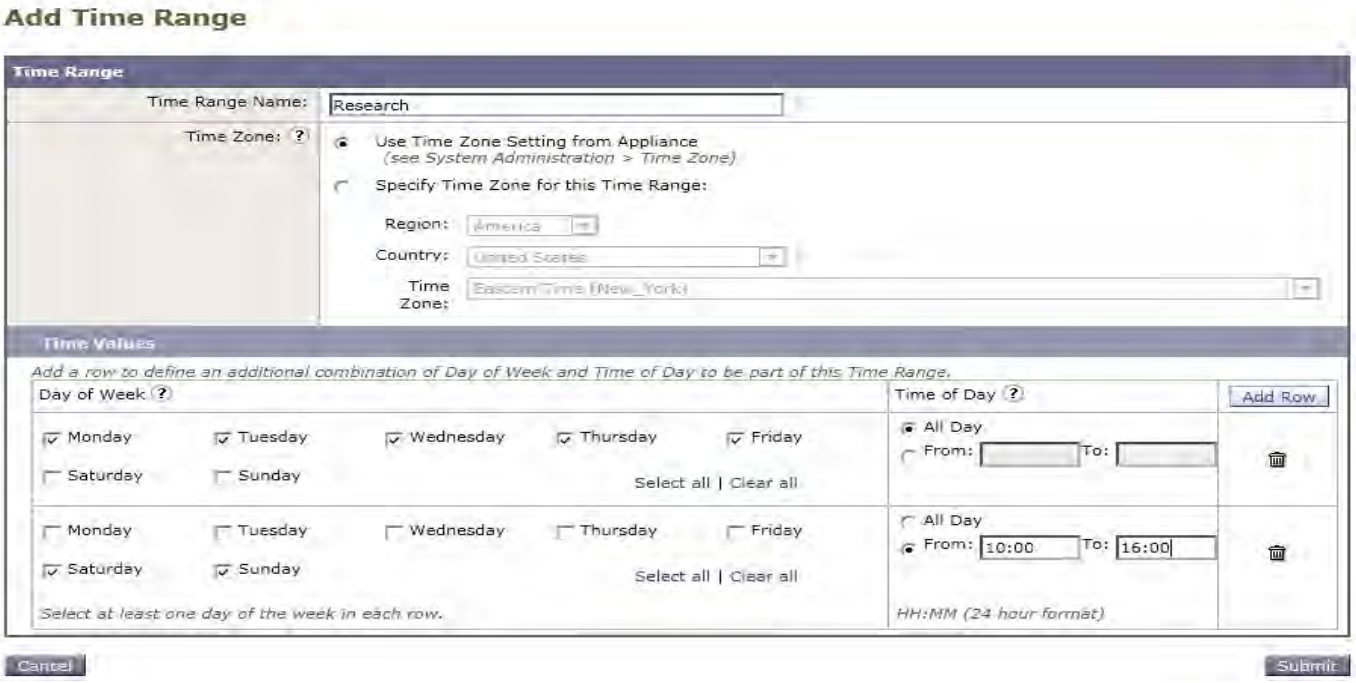




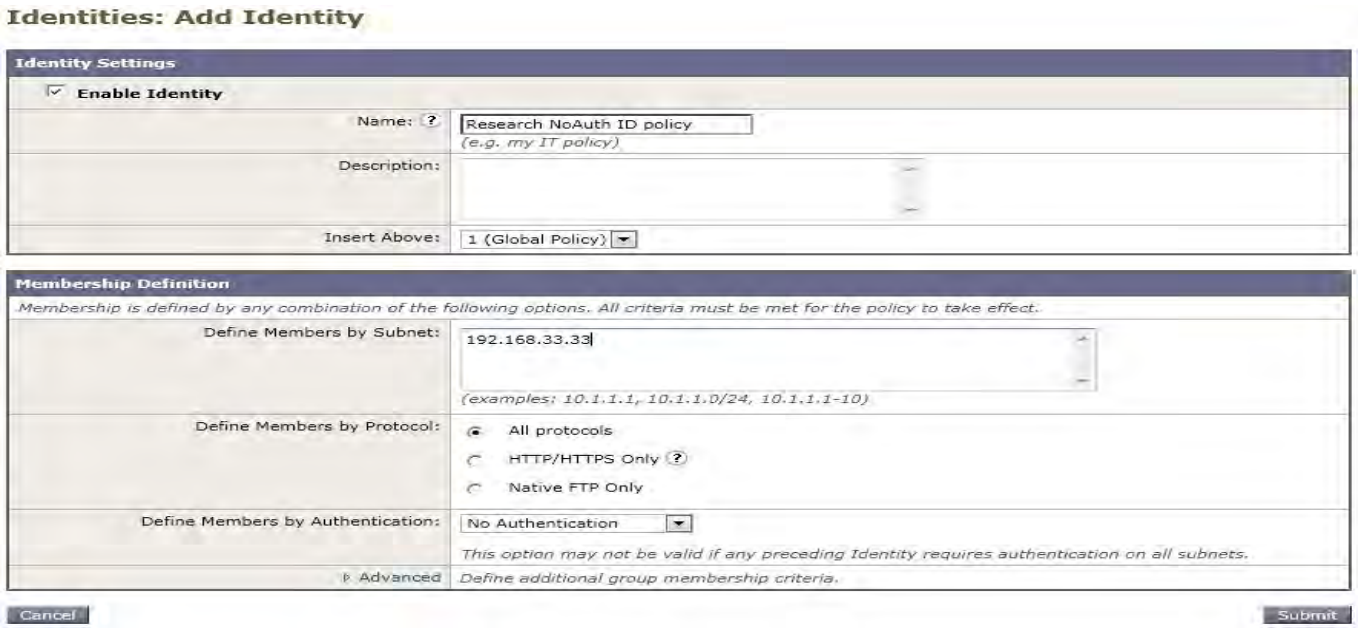
Click on Submit and apply/commit the changes

Step 2: Create a time range policy element needed for the new Research access policies as per the task.

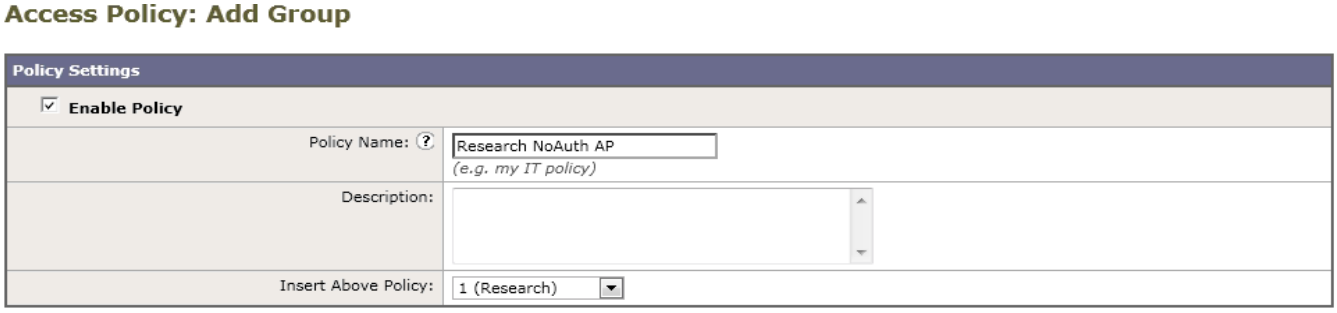
Web Security Manager -> Defined Time Ranges -> Add Time Range



Step 2: Create a new Idenity policy to bypass authentication for 192.168.33.33



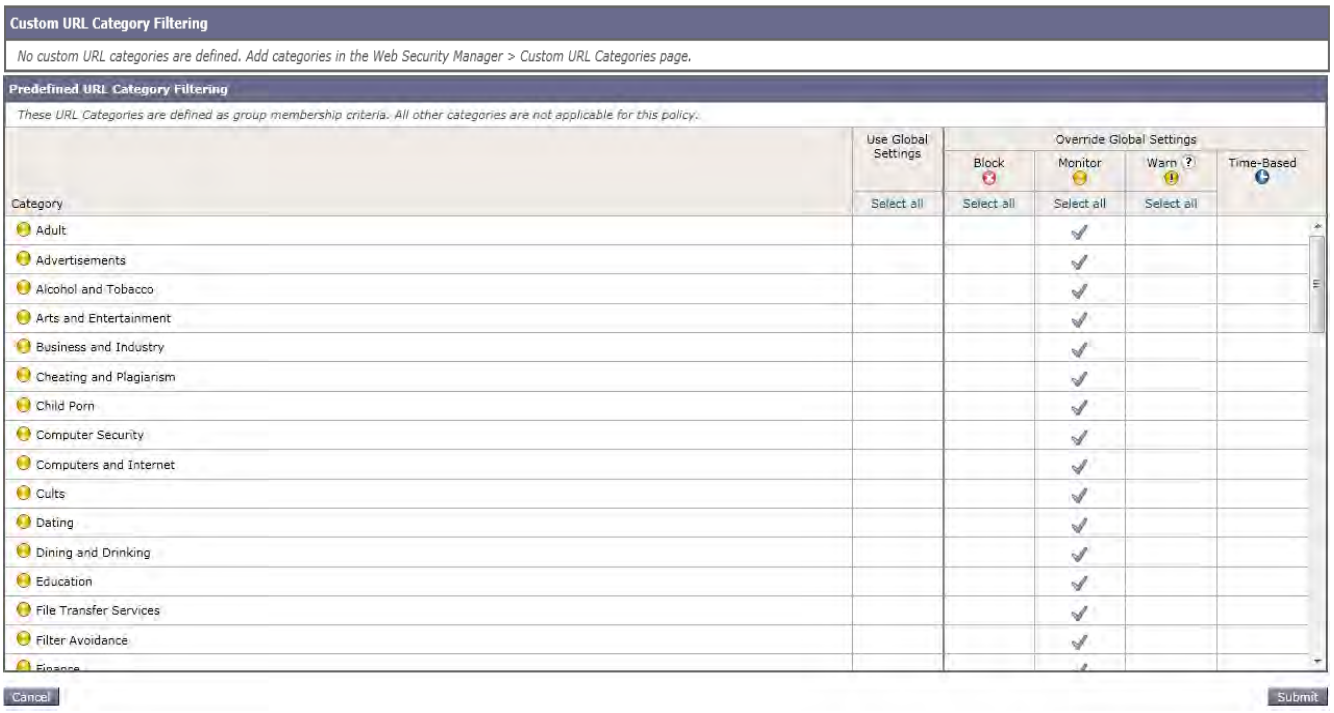
Step 3: Create a new access policy called “Research NoAuth AP” based on the time range and IP address as stated in the task.

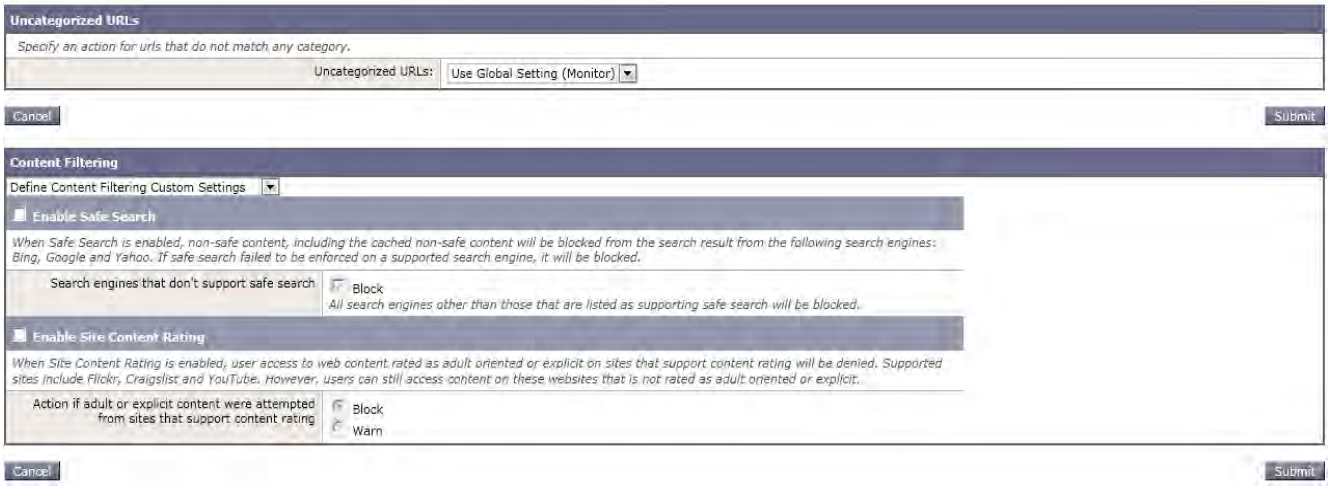


Click on Submit and apply/commit the changes

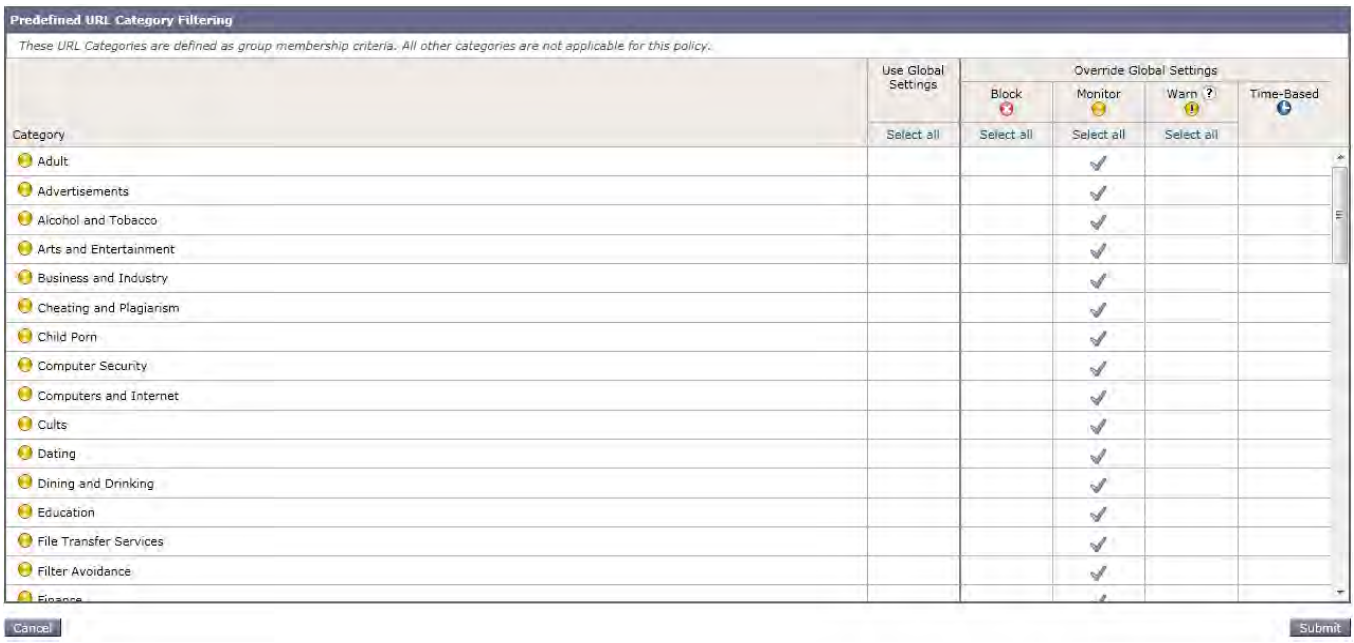
Step 3: Monitor all the pre-defined URL categories and disbale URL content filtering for the research subnet including 192.168.33.33

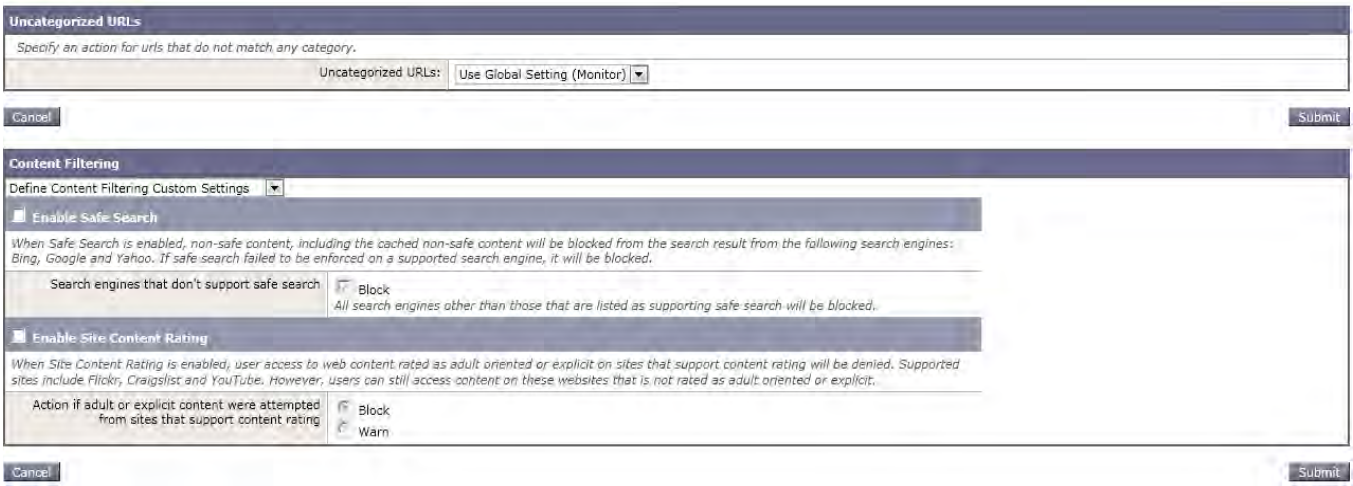
Access Policies: URL Filtering: Research



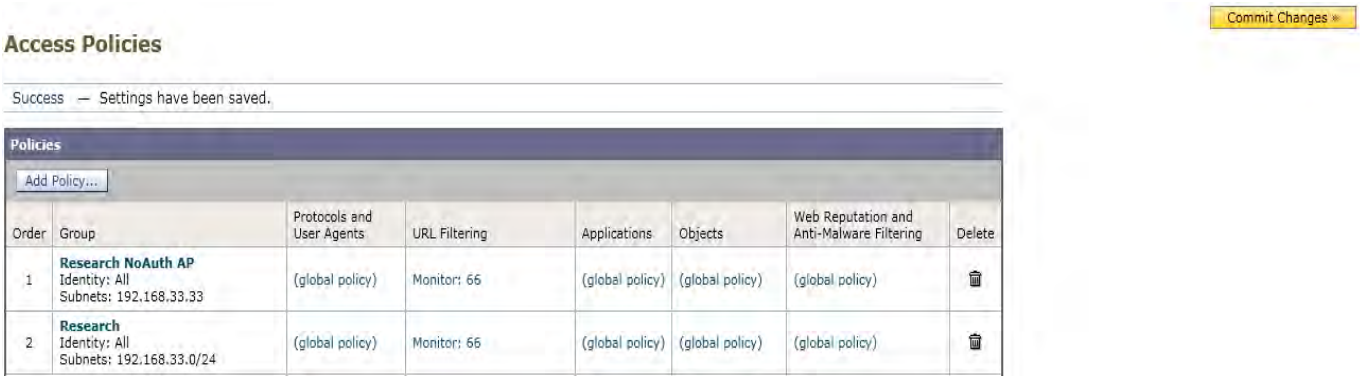


Access Policies: URL Filtering: Research NoAuth AP

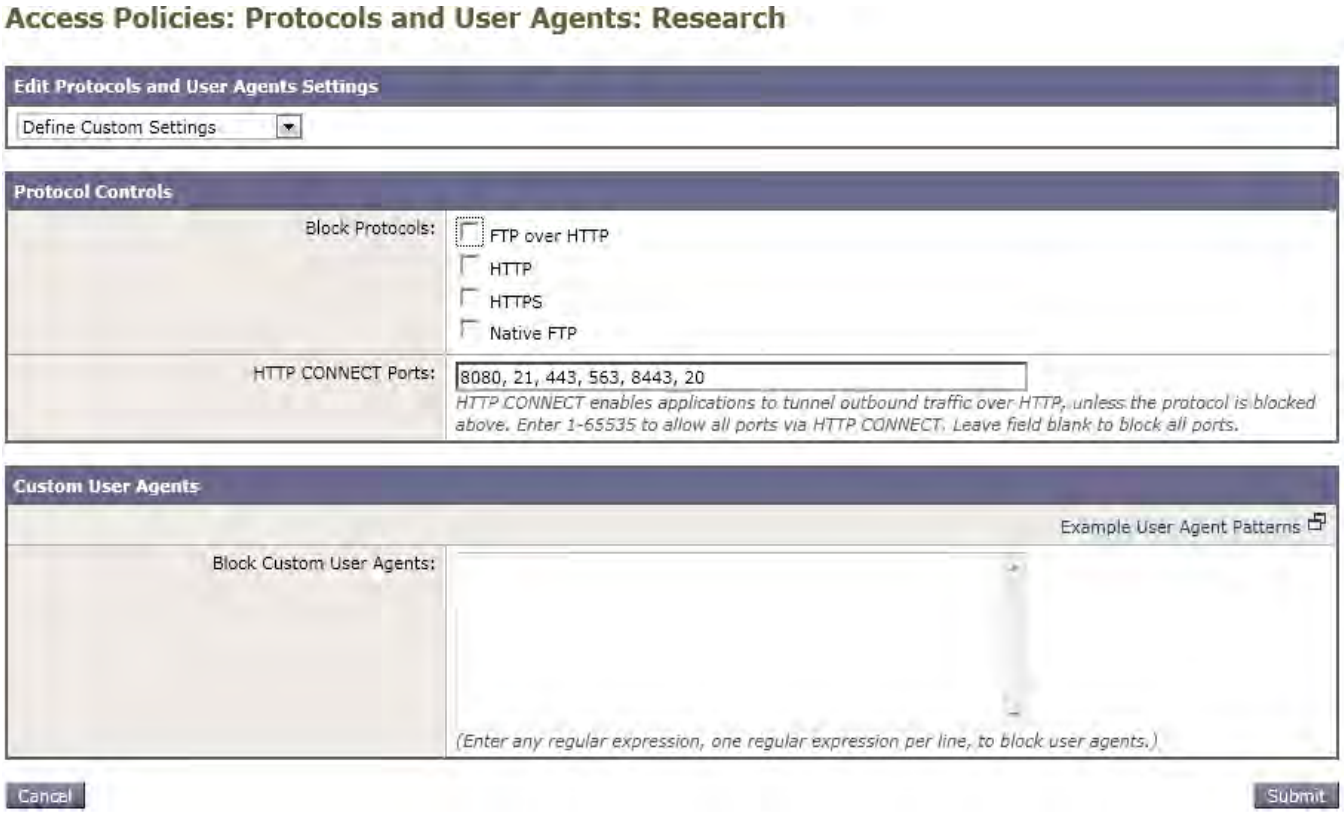


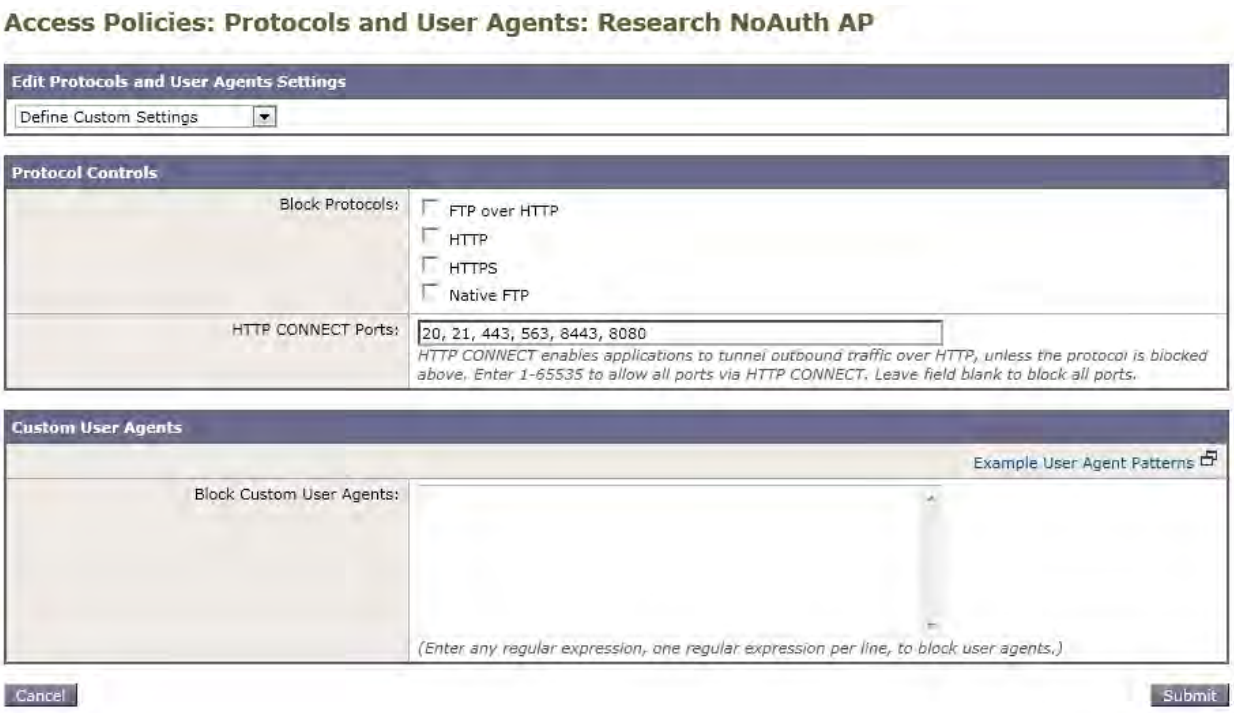


Commit the changes to apply the policies



Step 4: Allow FTP protocol for the research subnet including 192.168.33.33





Click on Submit and apply/commit the changes

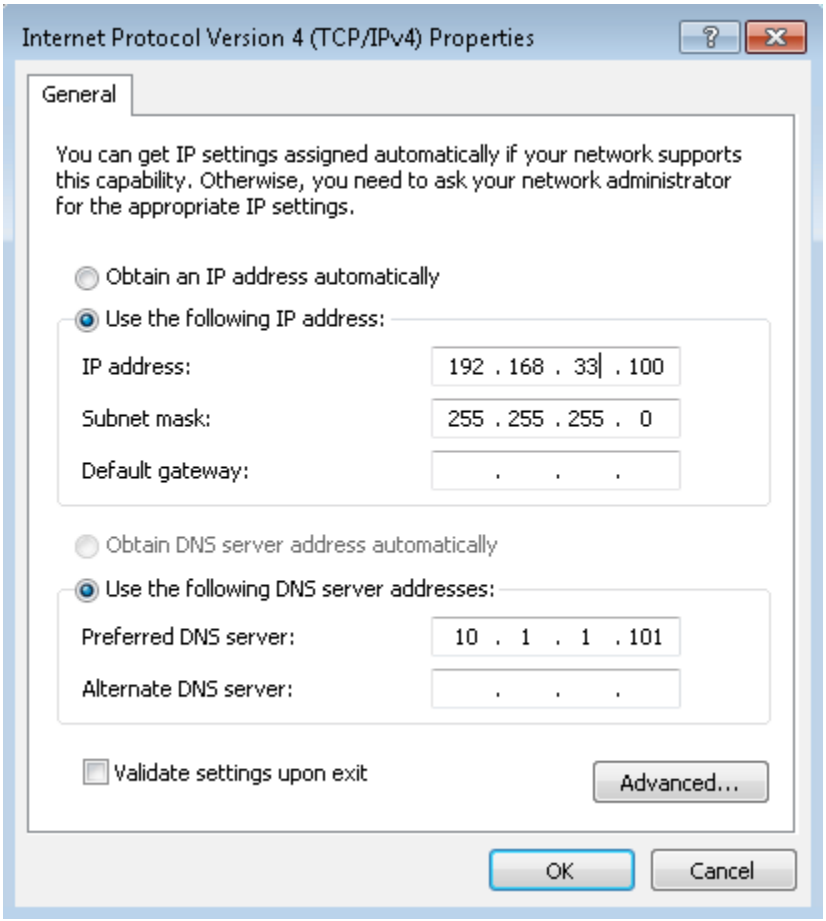
Step 5: Place the TEST PC in VLAN 33 and change the IP address to 192.168.33.100. Make sure you add the static routes on the PC

SW3

```
interface GigabitEthernet1/0/2
 switchport access vlan 33
 switchport mode access
 spanning-tree portfast
```

TEST PC

Configure the IP address to an IP from the Research subnet. Do not set the default gateway.

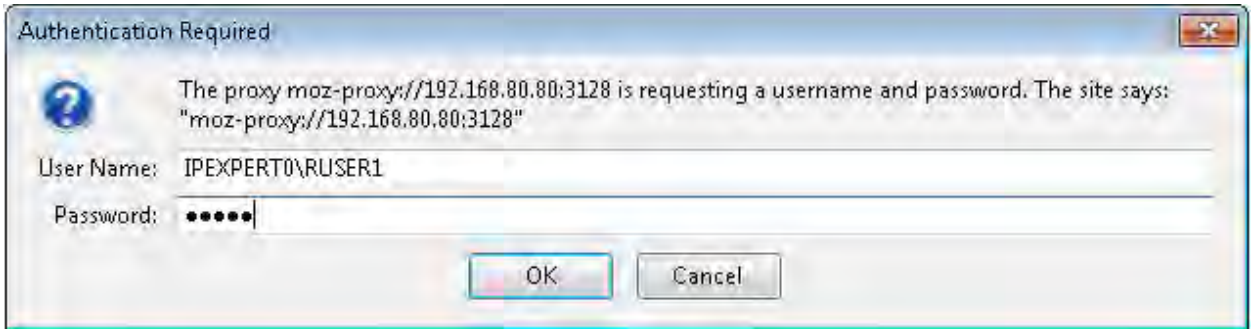


Delete the previously configured static routes and add the new static routes with next hop as SW3 (192.168.33.1). Ping the default gateway and WSA for testing purpose.

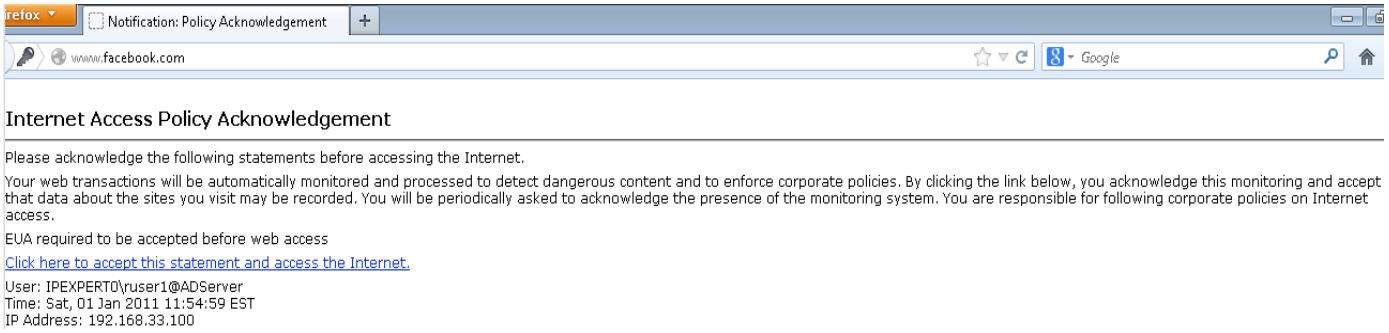
```
Administrator: Elevated CMD
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>route delete 10.1.1.101
 OK!

C:\Windows\System32>route delete 192.168.0.0
 OK!

C:\Windows\System32>route add 10.1.1.101 mask 255.255.255.255 192.168.33.1
 OK!

C:\Windows\System32>route add 192.168.0.0 mask 255.255.0.0 192.168.33.1
 OK!

C:\Windows\System32>ping 10.1.1.101

Pinging 10.1.1.101 with 32 bytes of data:
Reply from 10.1.1.101: bytes=32 time=4ms TTL=126
Reply from 10.1.1.101: bytes=32 time=1ms TTL=126
Reply from 10.1.1.101: bytes=32 time=1ms TTL=126
Reply from 10.1.1.101: bytes=32 time=1ms TTL=126

Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\Windows\System32>ping 192.168.88.80

Pinging 192.168.88.80 with 32 bytes of data:
Reply from 192.168.88.80: bytes=32 time=2ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62

Ping statistics for 192.168.88.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

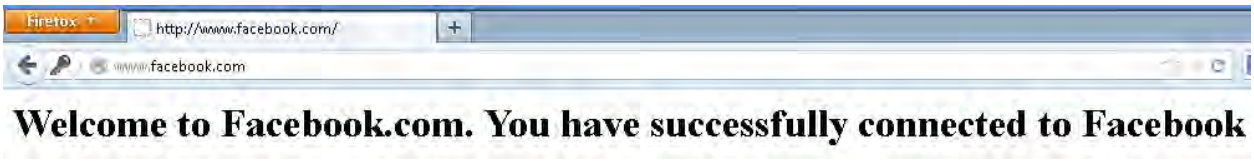
Step 3: Test the Research policy from TEST-PC by browsing using firefox as stated in the task. Clear all history including offline data (Ctr+shift+delete)

Enter the user information



Accept the EUN. You may also notice your username and IP address information



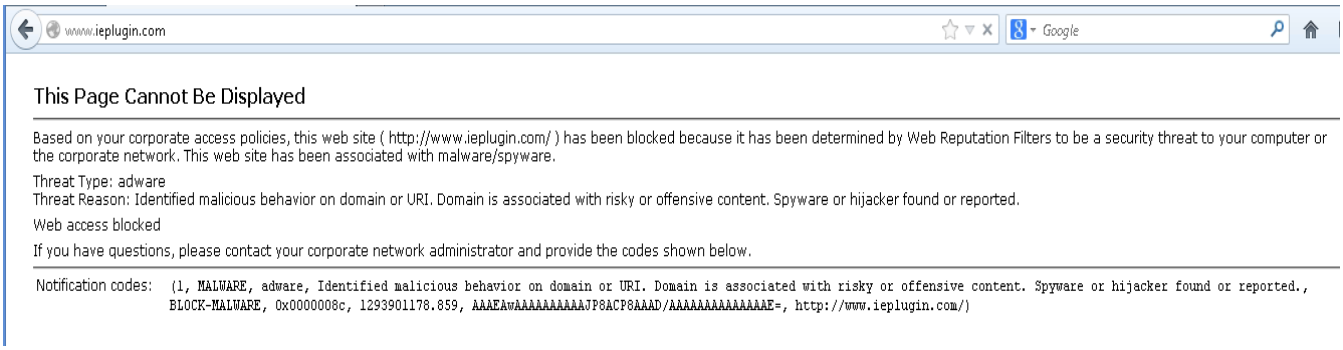


Access Logs

```
1293900936.666      2      192.168.33.100      TCP_DENIED/407      1766      GET
http://www.facebook.com/  -  NONE/-  -  OTHER-NONE-DefaultGroup-NONE-NONE-NONE-
NONE      <-,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-
","-","-","-",7064.00,0,-,"-","-"> -

1293900936.673      0      192.168.33.100      TCP_DENIED/407      451      GET
http://www.facebook.com/  -  NONE/-  -  OTHER-NONE-DefaultGroup-NONE-NONE-NONE-
NONE      <-,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-
","-","-","-",0.00,0,-,"-","-"> -
1293900936.822     146     192.168.33.100     TCP_REFRESH_HIT/200     426     GET
http://www.facebook.com/  "IPEXPERT0\ruser1@ADServer"  DIRECT/www.facebook.com
text/html      ALLOW_WBRS_11-Research-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_snet,7.0,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_snet,-,"-
","-","Facebook","Social Networking","-","-",23.34,0,-,"-","-"> -
```

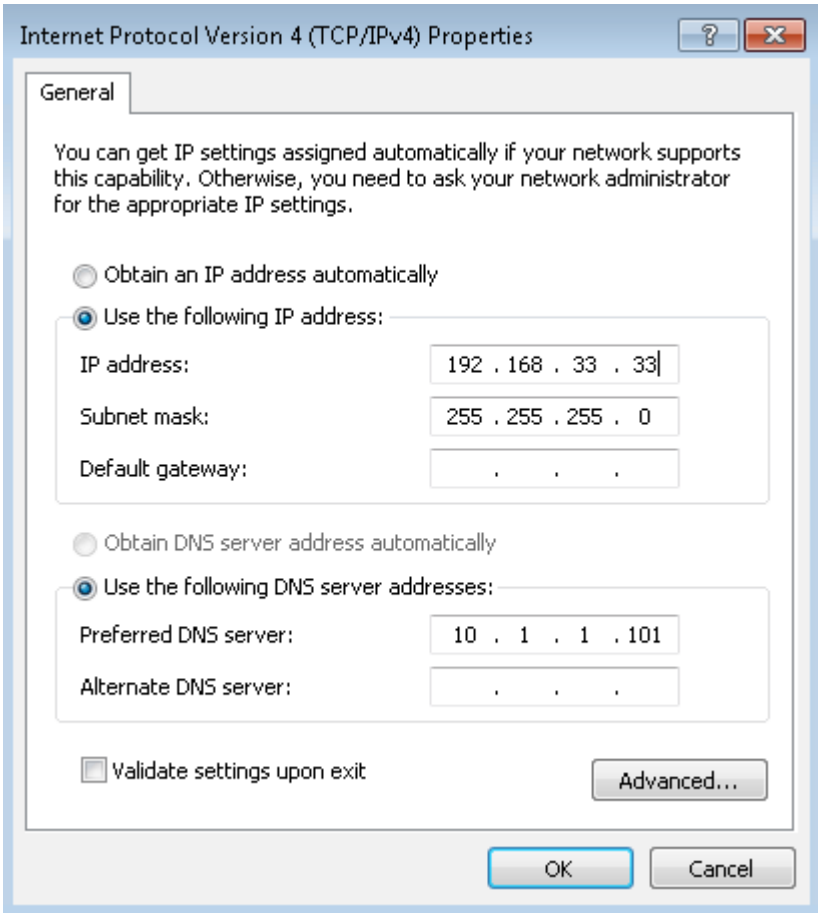

```
1293901094.665     138     192.168.33.100     TCP_REFRESH_HIT/200     417     GET
http://www.gmail.com/     "IPEXPERT0\ruser1@ADServer"     DIRECT/www.gmail.com
text/html     DEFAULT_CASE_11-Research-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_mail,4.9,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_mail,-,"-
","-","Unknown","Unknown","-","-",24.17,0,-,"-","-"> -
```

Browse to www.ieplugin.com

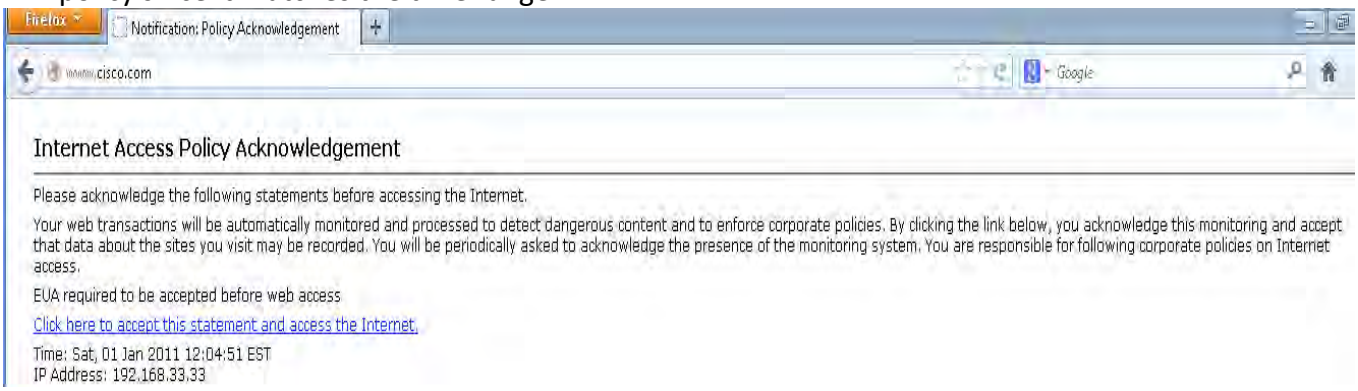



```
1293901178.859      16      192.168.33.100      TCP_DENIED/403      2258      GET
http://www.ieplugin.com/  "IPEXPERT0\ruser1@ADServer"  NONE/-  -  BLOCK_WBRS_11-
Research-DefaultGroup-NONE-NONE-NONE-NONE    <IW_adv,-6.4,"-","-",-,-,-,"-","-
",-,-,-,"-","-",-,"-","-",-,-,IW_adv,-,"-","adware","Unknown","Unknown","-
","-",1129.00,0,-,"-","-"> -
```

Change the IP address to 192.168.33.33 and test the policies



Broswe to www.cisco.com using firefox. Accept the EUN. This will match the "Research NoAuth AP" policy since it matches the time range.




```
1293901519.825    143    192.168.33.33    TCP_REFRESH_HIT/200    421    GET
http://www.cisco.com/    -    DIRECT/www.cisco.com    text/html    ALLOW_WBRS_11-
Research_NoAuth_AP-Research_NoAuth_ID_policy-NONE-NONE-NONE-DefaultGroup
<IW_comp,6.5,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_comp,-,"-
","-","Unknown","Unknown","-","-",23.55,0,-,"-","-"> -
```

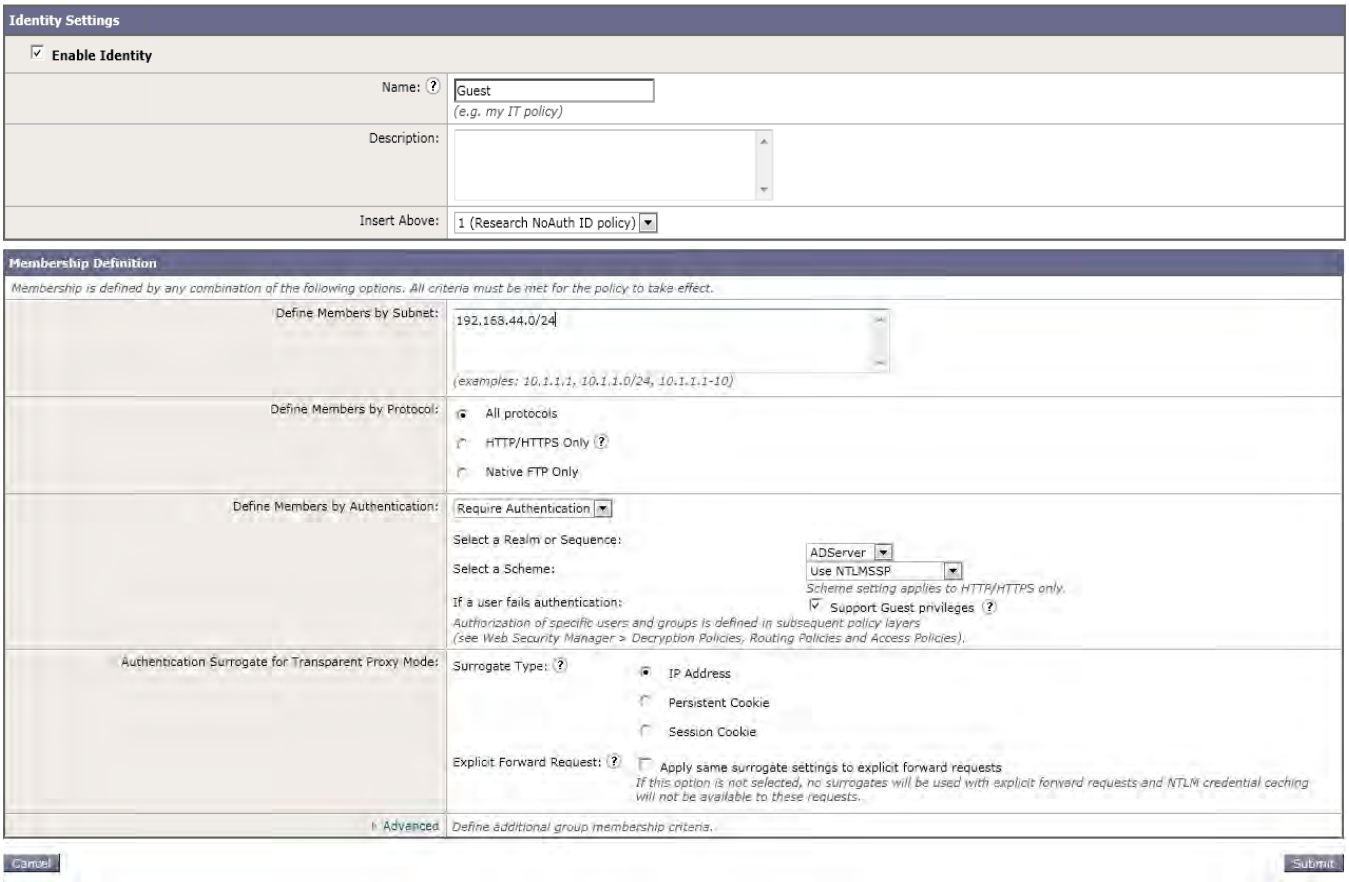
Task 2: Configure Guest privileges and Custom URL policy -1

- Users failing the authentication should be treated as guest users. All the guest users will connect from VLAN 44.
- Create a new identity policy for the guest subnet and enable guest privileges.
- Create a new access policy that matches guest users allow access (Monitor) only to www.ipexpert.com and block all other URL categories.
- You are allowed to create one custom URL category to accomplish this task.
- Place this access policy just above the global policy.
- Block uncategorized URL's.
- Test this policy from VLAN 44. You may need to reconfigure TEST-PC and switch accordingly.

Task-1: Solutions

Step 1: Configure an identity group called "Guest" to support guest fallback for failed authentications from 192.168.44.0/24 subnet

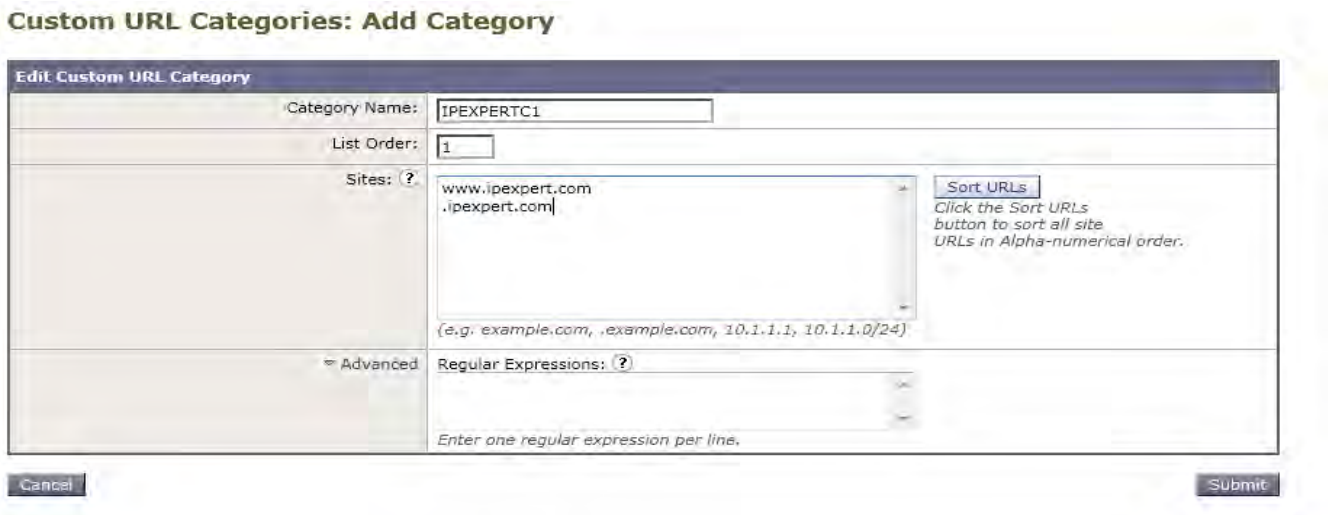
Identities: Add Identity



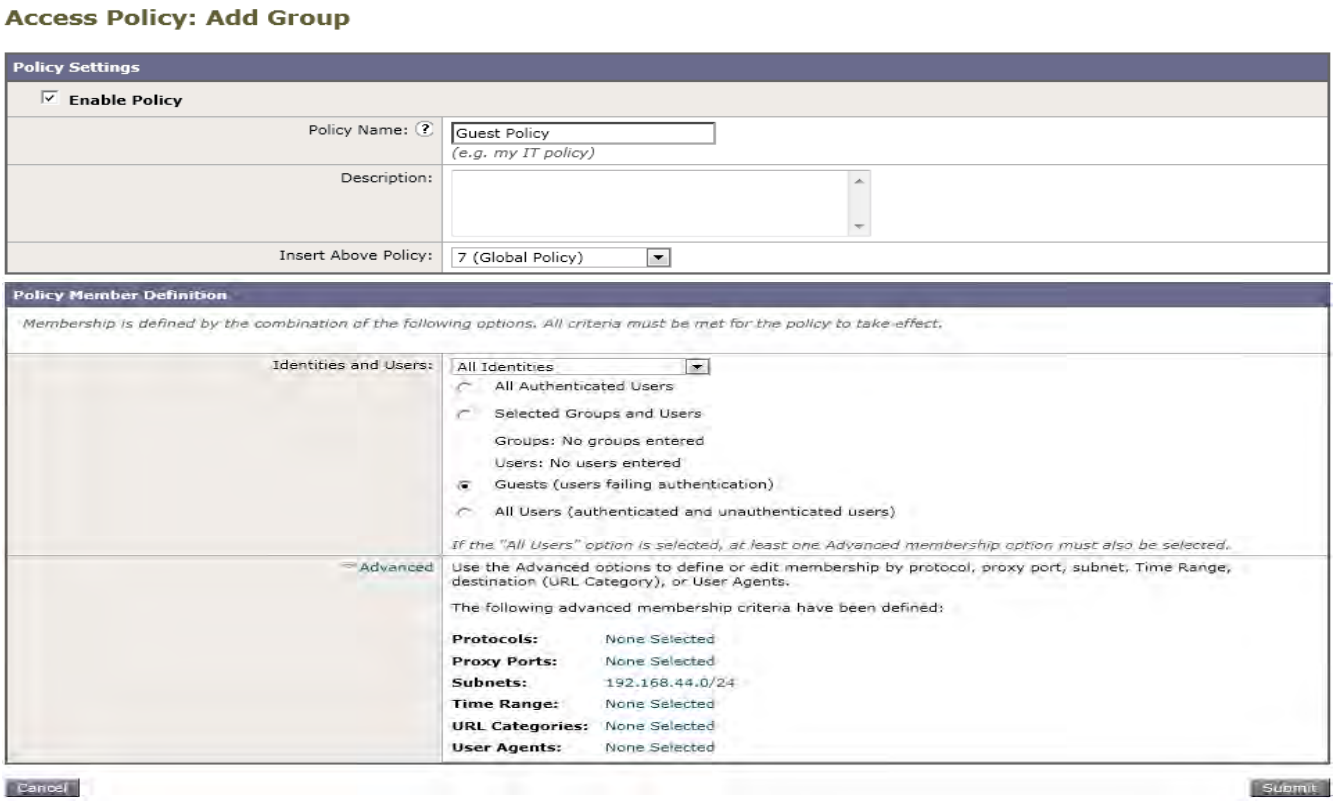
Submit and apply the changes

Step 2: Configure a new custom URL category for the guest access as per task.

Web Security Manager -> Custom URL Categories -> Add Custo



Step 3: Configure a new access policy called "Guest Policy" for the guest users as per task.

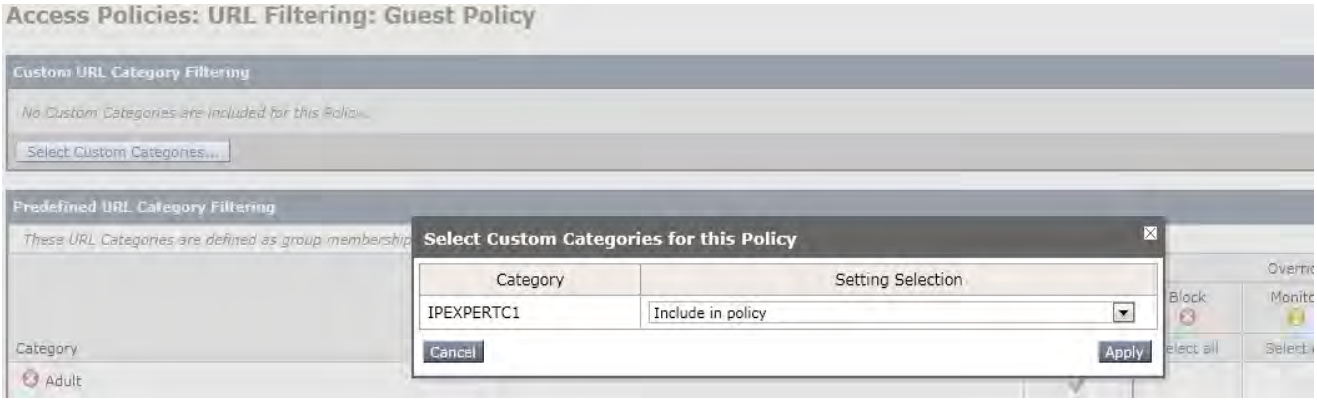


Submit and apply/commit the changes. Make sure the Guest policy is above the Global Policy

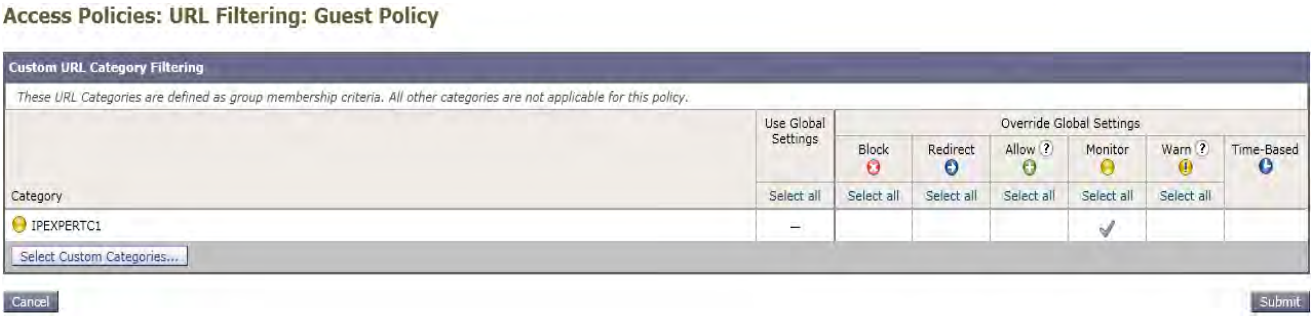
7	**Guest Policy** Identity: All, Guest privileges for users failing authentication Subnets: 192.168.44.0/24	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	🗑
	Global Policy Identity: All	Block: 2 Protocols	Block: 58 Monitor: 8 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 18	No blocked items	Web Reputation: Enabled	

Step 3: Block all pre-defined URL categories and allow access to www.ipexpert.com defined in the custom URL category.

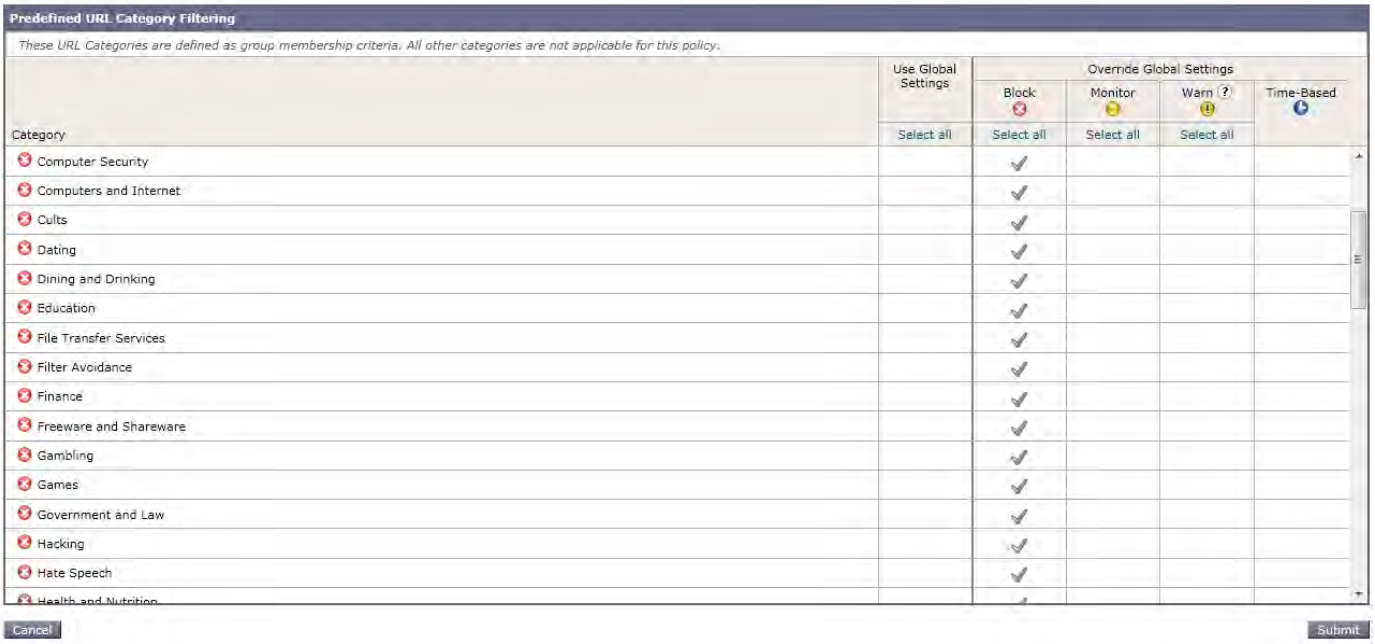
Include the appropriate custom URL category in the policy



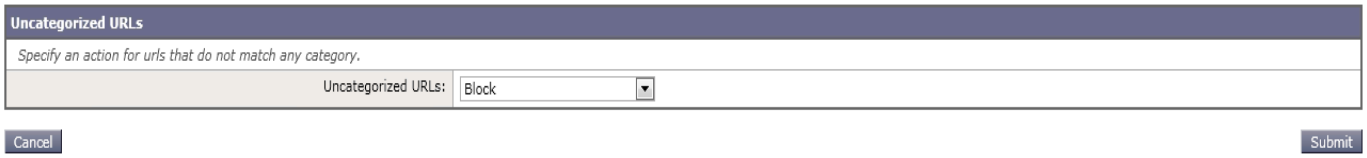
Configure the Guest policy to monitor the custom URL category



Configure the Guest policy to block all the other pre-defined URL category



Block all uncategorized URL's



Submit and apply/commit the changes

7	**Guest Policy** Identity: All, Guest privileges for users failing authentication Subnets: 192.168.44.0/24	(global policy)	Block: 66 Monitor: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
	Global Policy Identity: All	Block: 2 Protocols	Block: 58 Monitor: 8 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 18	No blocked items	Web Reputation: Enabled	

Step 5: Place the TEST PC in VLAN 44 and change the IP address to 192.168.44.100. Make sure you add the static routes on the PC

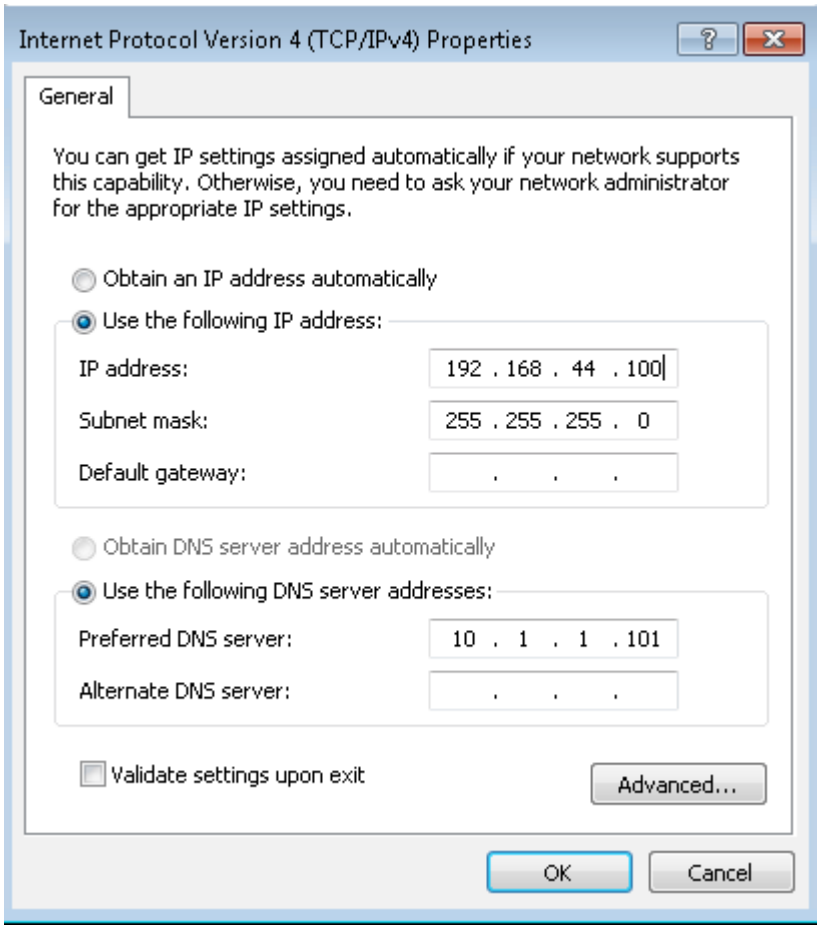
SW3

```
interface GigabitEthernet1/0/2
 switchport access vlan 44
```

```
switchport mode access
spanning-tree portfast
```

TEST PC

Configure the IP address to an IP from the Guest subnet. Do not set the default gateway.

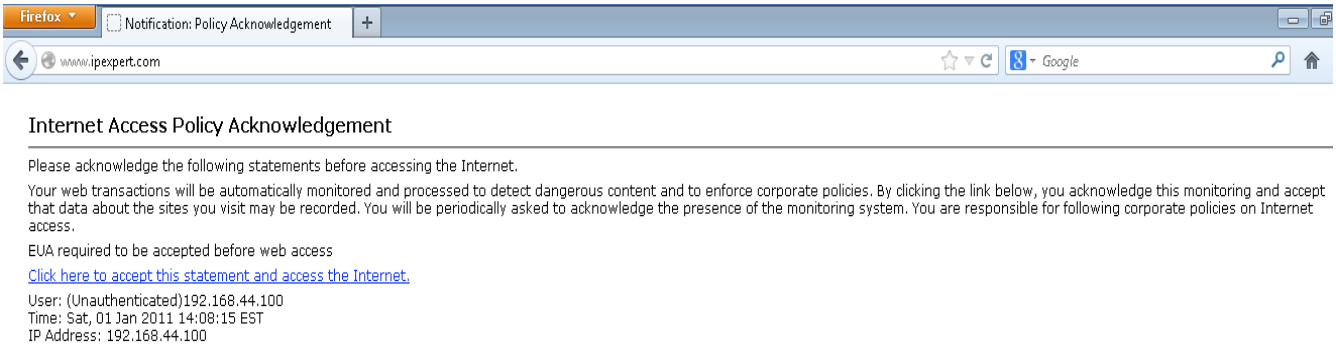


Delete the previously configured static routes and add the new static routes with next hop as SW4 (192.168.44.1). Ping the default gateway and WSA for testing purpose.

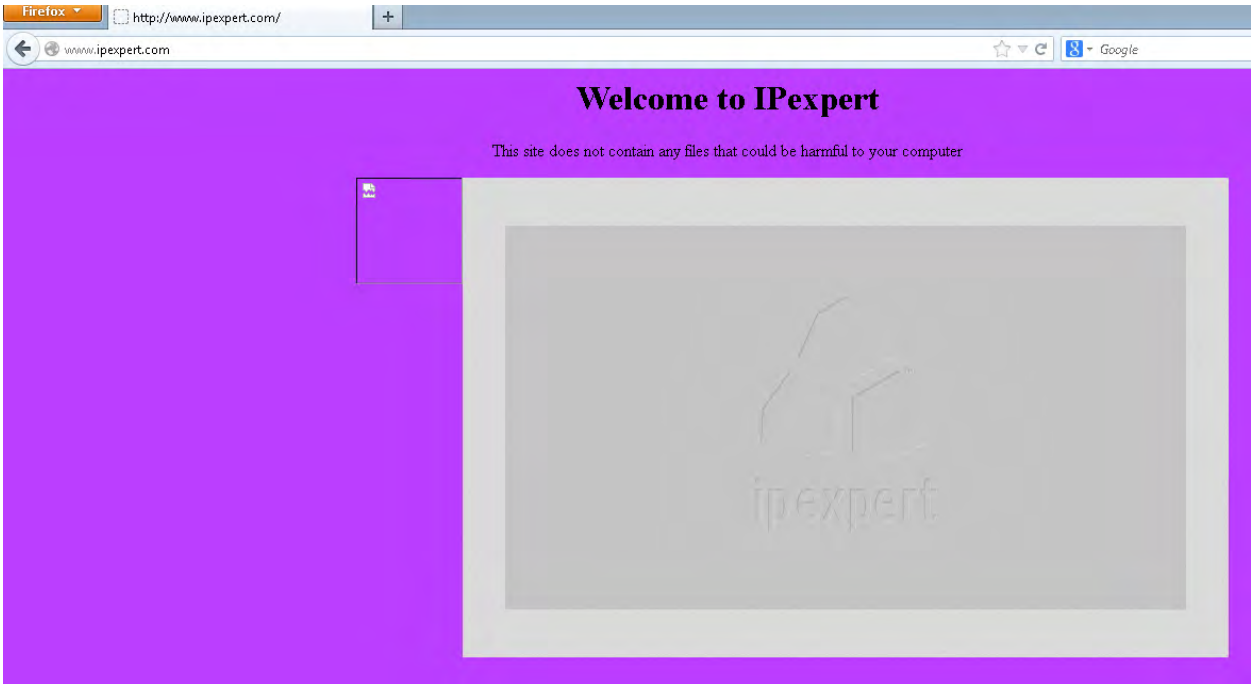
```
Administrator: Elevated CMD

C:\Windows\System32>route delete 10.1.1.101
 OK!

C:\Windows\System32>route delete 192.168.0.0
 OK!

C:\Windows\System32>route add 10.1.1.101 mask 255.255.255.255 192.168.44.1
 OK!

C:\Windows\System32>route add 192.168.0.0 mask 255.255.0.0 192.168.44.1
 OK!

C:\Windows\System32>ping 192.168.44.1

Pinging 192.168.44.1 with 32 bytes of data:
Reply from 192.168.44.1: bytes=32 time=2ms TTL=255
Reply from 192.168.44.1: bytes=32 time=1ms TTL=255
Reply from 192.168.44.1: bytes=32 time<1ms TTL=255
Reply from 192.168.44.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.44.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Windows\System32>ping 192.168.88.80

Pinging 192.168.88.80 with 32 bytes of data:
Reply from 192.168.88.80: bytes=32 time=3ms TTL=62
Reply from 192.168.88.80: bytes=32 time<1ms TTL=62
Reply from 192.168.88.80: bytes=32 time=1ms TTL=62
Reply from 192.168.88.80: bytes=32 time=1ms TTL=62

Ping statistics for 192.168.88.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Windows\System32>_
```

Step 6: Test the Guest policy from TEST-PC by browsing to www.ipexpert.com which is allowed in the Guest policy. Use firefox and clear all history including offline data (Ctr+shift+delete).

Accept the EUN. You may also notice your username and IP address information



You will successfully connected to www.ipexpert.com if your policy is correct. Below is the webpage that will be displayed when the traffic matches the access policy.



Access Logs

```
1293908926.027    190    192.168.44.100    TCP_REFRESH_HIT/200    753    GET
http://www.ipexpert.com/                    "(Unauthenticated)192.168.44.100"
DIRECT/www.ipexpert.com   text/html   MONITOR_CUSTOMCAT_11-Guest_Policy-Guest-
NONE-NONE-NONE-DefaultGroup  <C_IPEX,0.0,"1","-",-,-,-,"-","-",-,-,-,"-","-",-
,"-","-",-,-,IW_edu,-,"-","-","Unknown","Unknown","-","-",31.71,0,-,"-","-">
-
```

Browse to any other site apart from www.ipexpert.com and you should get a block page. Make sure the browser cache is cleared.

Access Logs

```
1293909124.500 2 192.168.44.100 TCP_DENIED/403 2734 GET http://www.cisco.com/
"(Unauthenticated)192.168.44.100"   NONE/-   -   BLOCK_WEBCAT_11-Guest_Policy-
Guest-NONE-NONE-NONE-NONE   <IW_comp,6.5,"-","-",-,-,-,"-","-",-,-,-,"-","-",-
,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",10936.00,0,-,"-
","-"> -
```

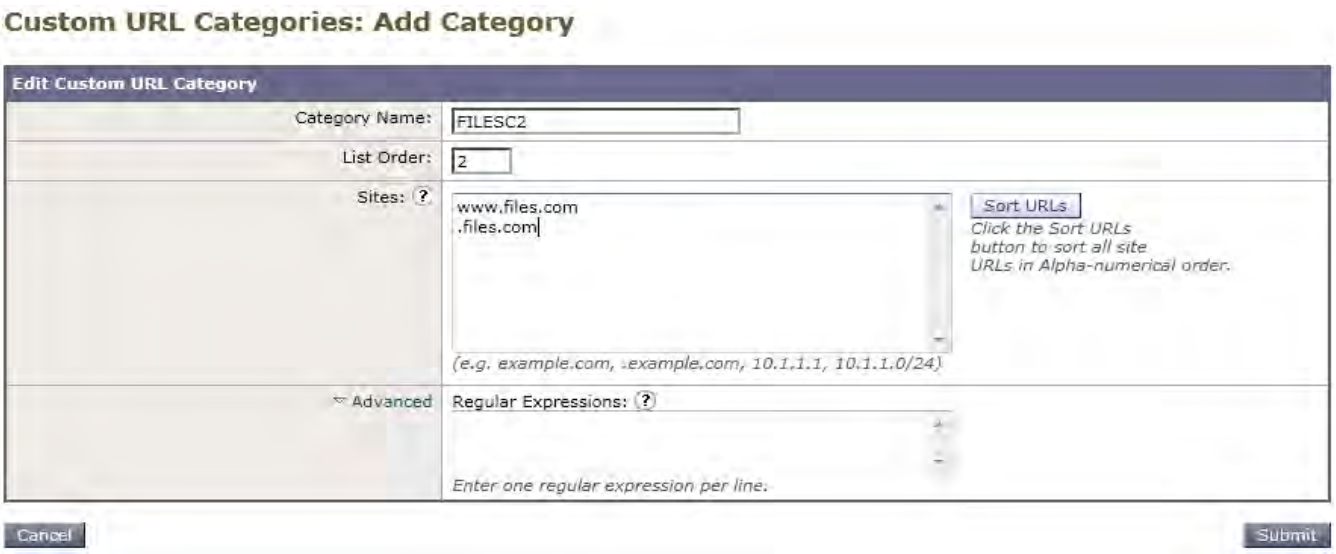
Task 3: Configure Custom URL policy - 2

- All users except guests should be allowed access (Monitor) to host URL and all subdomains of files.com
- You are allowed to create one custom URL category to accomplish this task.

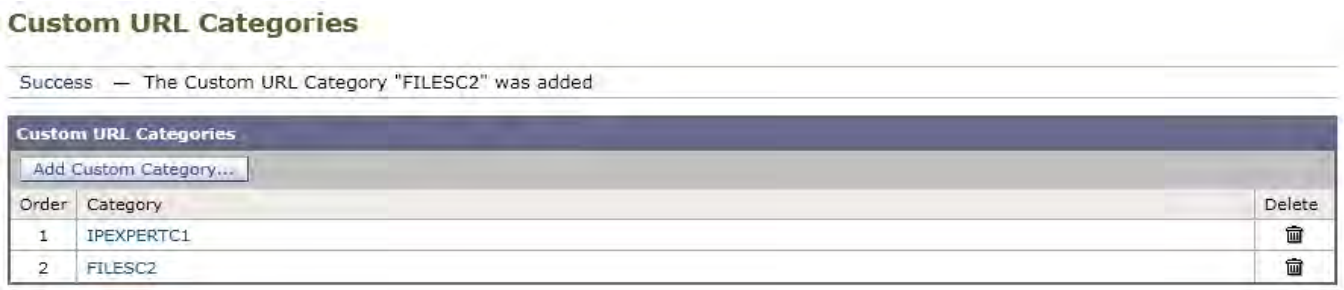
Task-3: Solutions

Step 1: Configure a new custom URL category for the guest access as per task.

Web Security Manager -> Custom URL Categories -> Add Custom Category



Submit and apply/commit changes



Step 2: Allow access to files.com and its subdomains in the global policy. Make sure guests do not have access to this site.

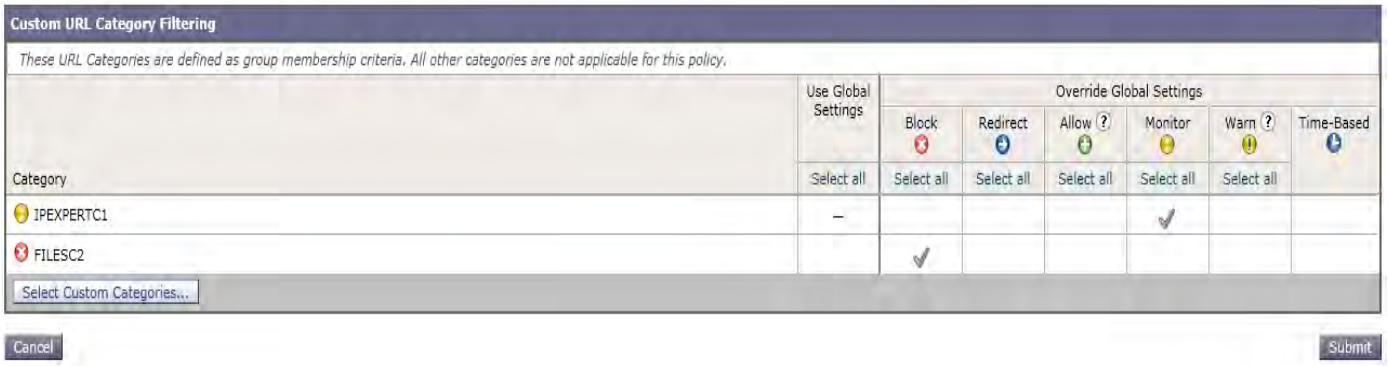
Include the custom URL category in the Global policy

Configure the Global Policy to monitor to this custom URL catrgory

Access Policies: URL Filtering: Global Policy

Configure the Guest Policy to block access to www.files.com and the sub domain of files.com

Access Policies: URL Filtering: Guest Policy



Submit and Commit the changes

7	**Guest Policy** Identity: All, Guest privileges for users failing authentication Subnets: 192.168.44.0/24	(global policy)	Block: 67 Monitor: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
	Global Policy Identity: All	Block: 2 Protocols	Block: 58 Monitor: 9 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 18	No blocked items	Web Reputation: Enabled	

Step 3: Configure the TEST PC to be part of IT VLAN

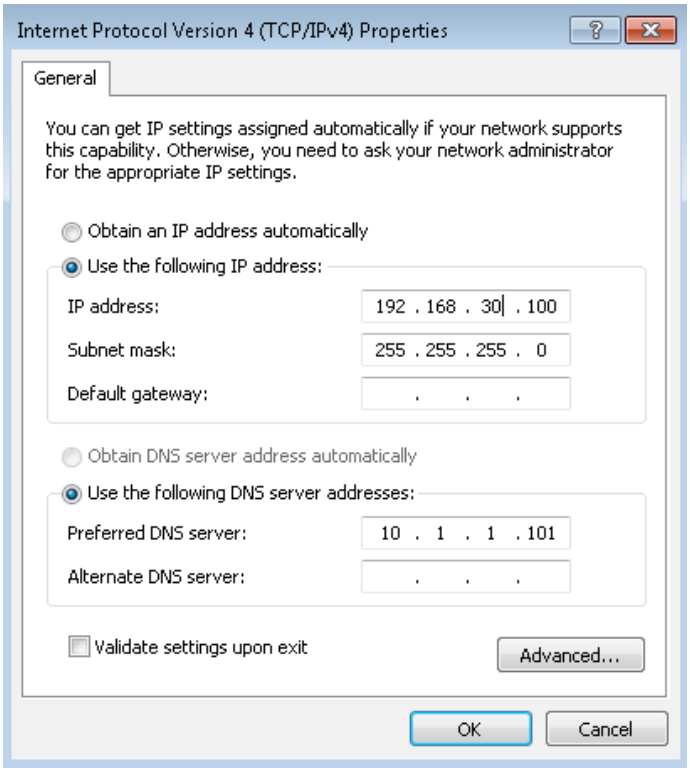
SW3

```
interface GigabitEthernet1/0/2
 switchport access vlan 30
 switchport mode access
```

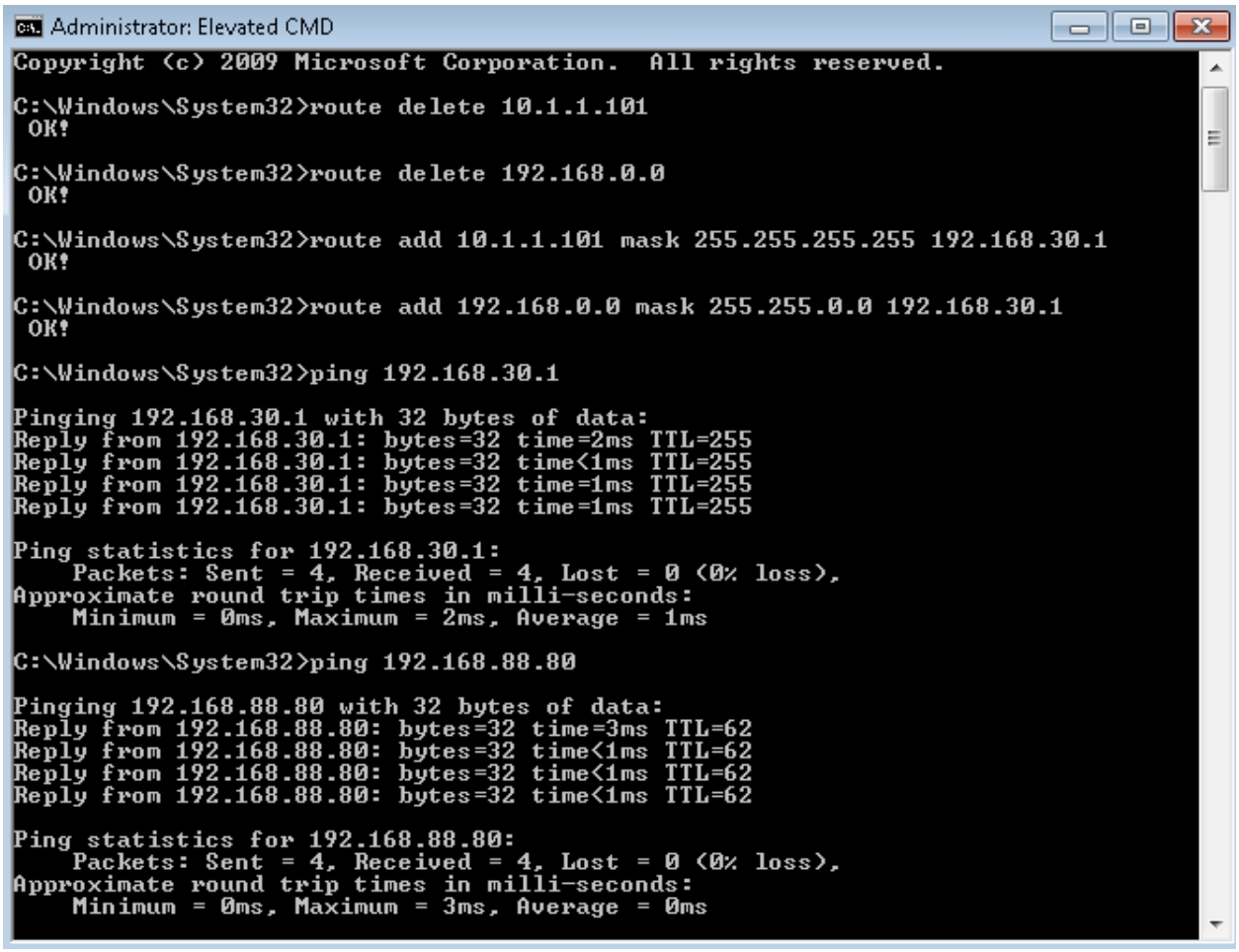
```
spanning-tree portfast
```

TEST PC

Configure the IP address to an IP from the Guest subnet. Do not set the default gateway.

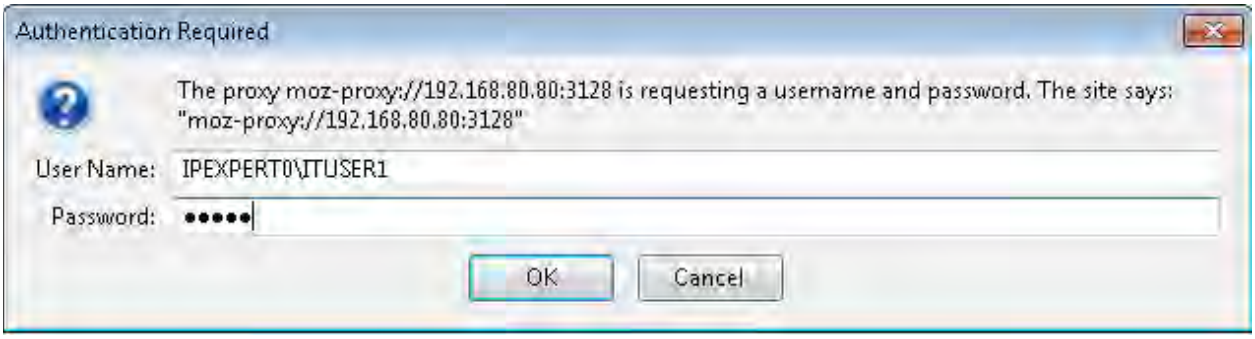


Delete the previously configured static routes and add the new static routes with next hop as SW3 (192.168.30.1). Ping the default gateway and WSA for testing purpose.

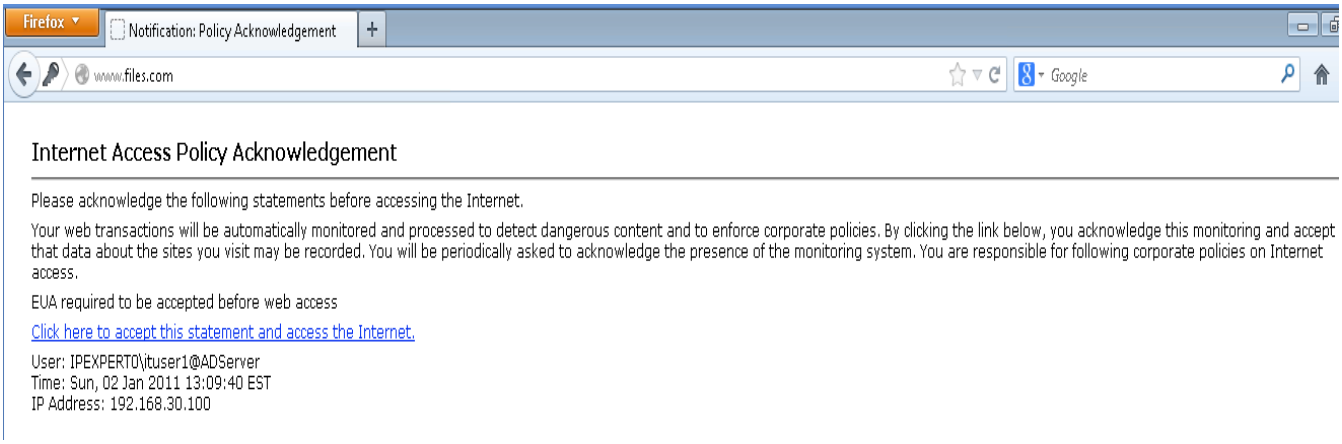


Step 4: Use firefox to browse to www.files.com and clear all history including offline data (Ctr+shift+delete). Note the PC is currently in the HR subnet.

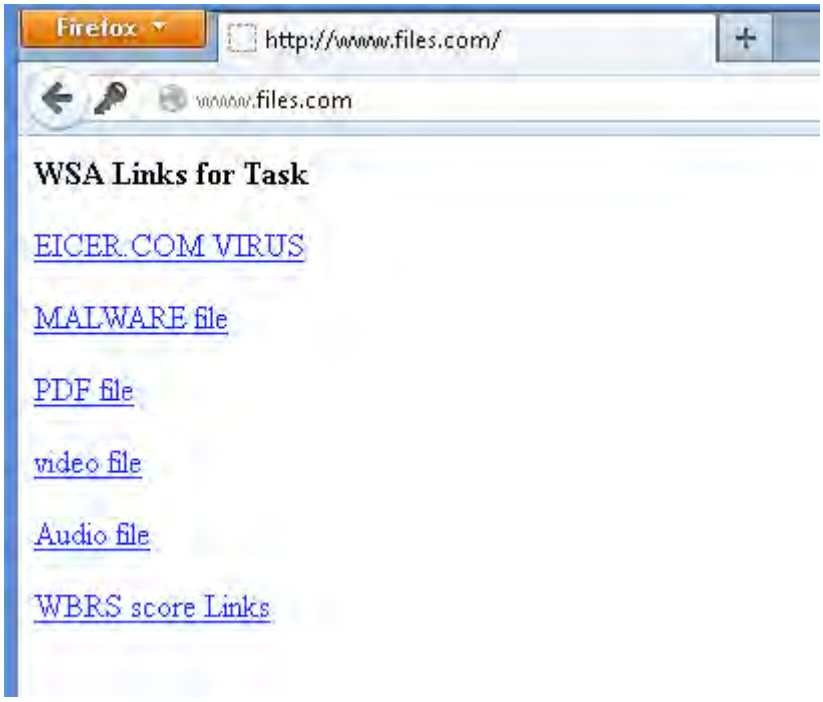
Enter the user information



Accept the EUN. You may also notice your username and IP address information



You will successfully connected to www.files.com if your policy is correct. Below is the webpage that will be displayed when the traffic matches the access policy and authenticates correctly.



Access Logs

```
1293991834.471 1769 192.168.30.100 TCP_MISS/200 708 GET http://www.files.com/
"IPEXPERT0\ituser1@ADServer"          DIRECT/www.files.com          text/html
MONITOR_CUSTOMCAT_11-IT_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<C_FILE,-5.8,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_comp,-,"-
","othermalware","Unknown","Unknown","-","-",3.20,0,-,"-","-"> -
```

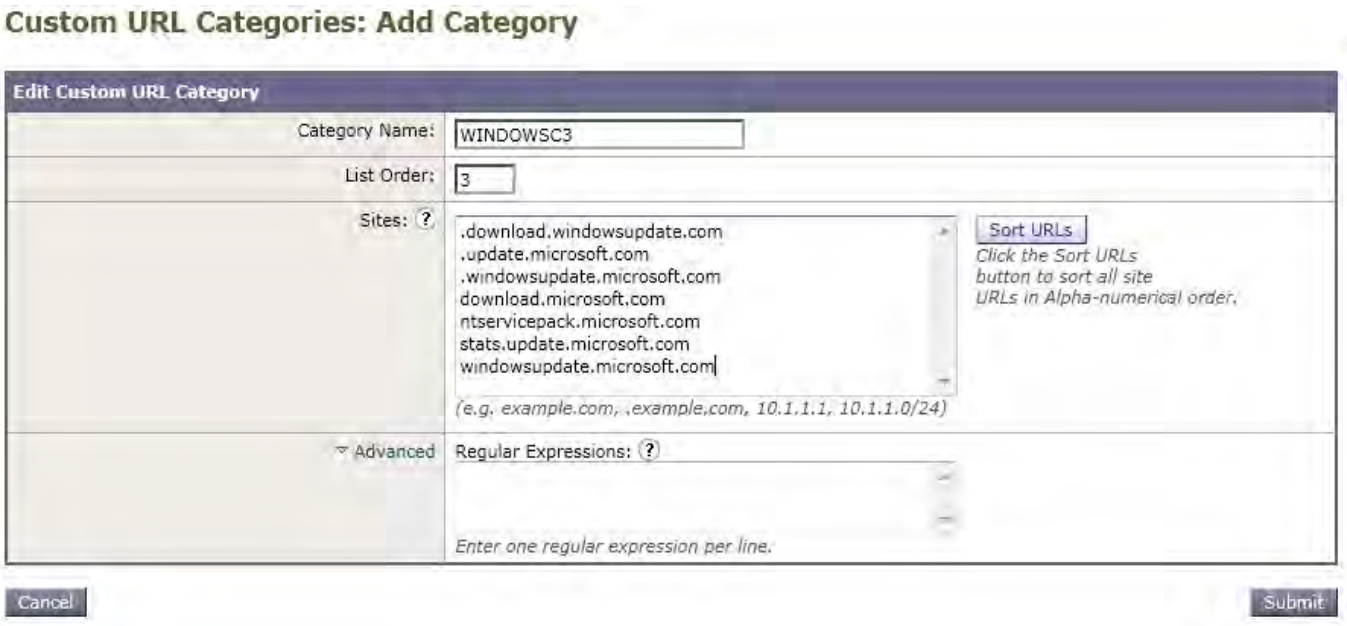
Task 4: Configure Custom URL policy - 3

- Authentication is breaking Microsoft windows update for the IT users.
- You are allowed to create one custom URL category for the below URL's
  - download.windowsupdate.com
  - update.microsoft.com
  - windowsupdate.com
  - windowsupdate.microsoft.com
  - download.microsoft.com
  - download.windowsupdate.com
  - ntservicepack.microsoft.com
  - stats.update.microsoft.com
  - windowsupdate.microsoft.com

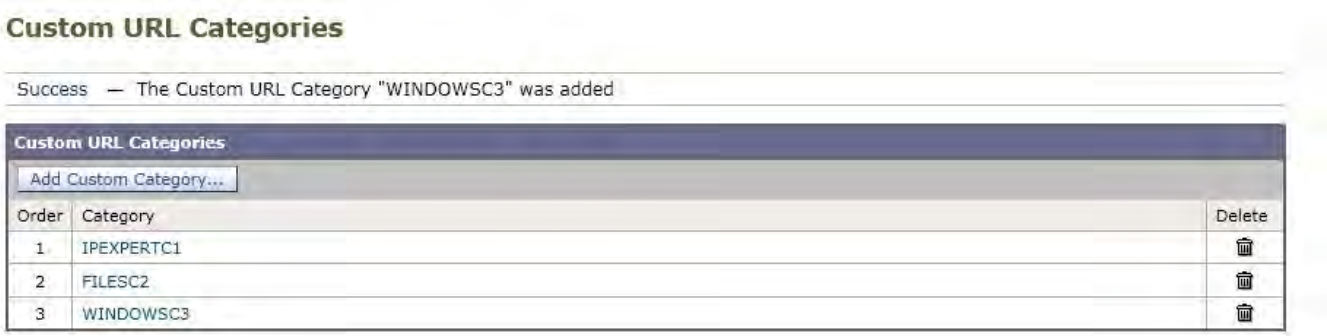
Task-3: Solutions

Step 1: Configure a new custom URL category for the guest access as per task.

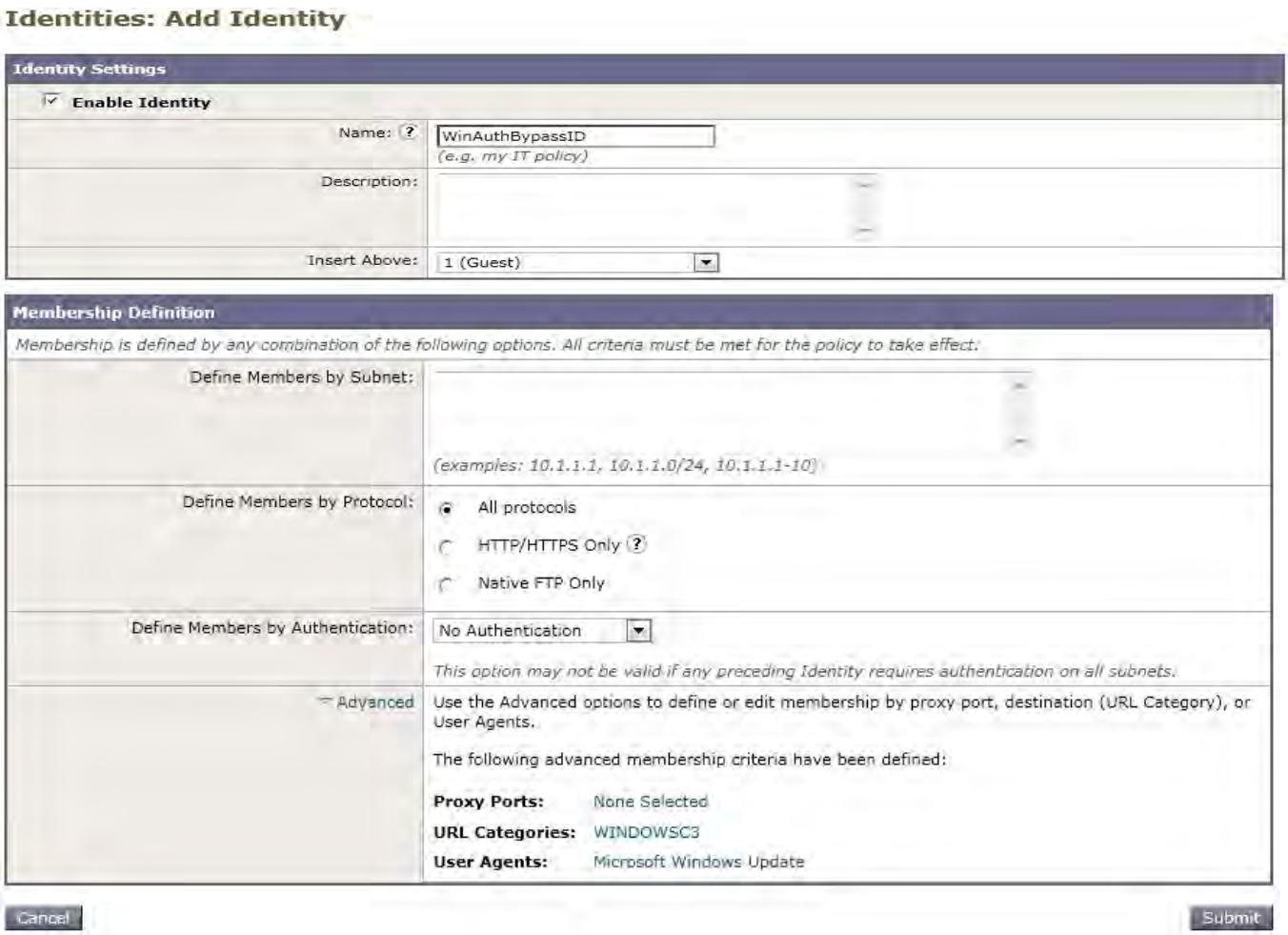
Web Security Manager -> Custom URL Categories -> Add Custom Category



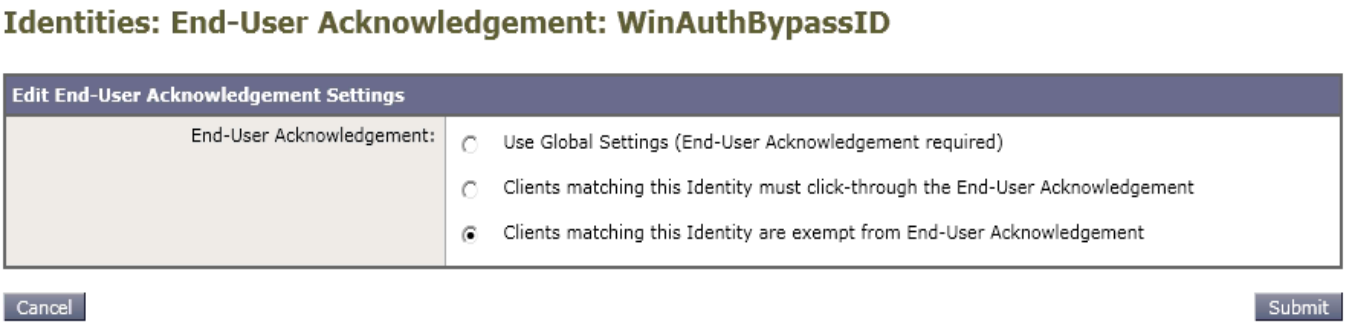
Click on Submit and apply/commit the changes



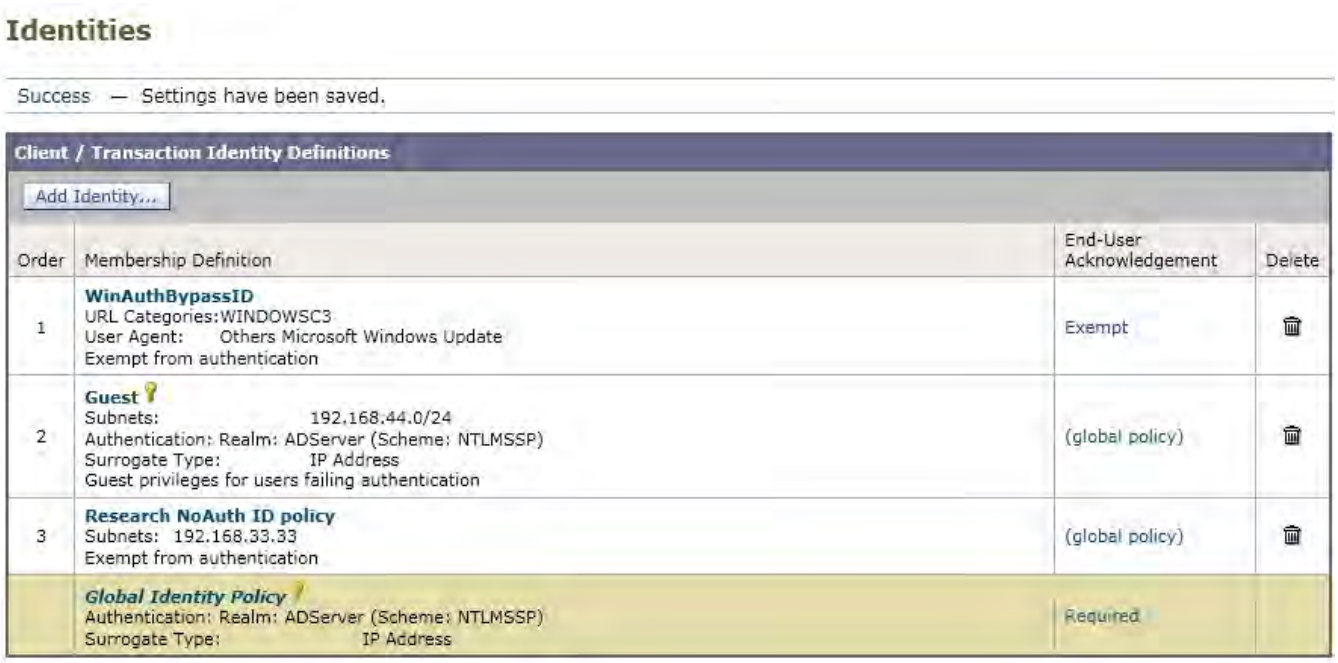
Step 2: Create a new identity policy to disable authentication for windows update traffic using custom URL categories.



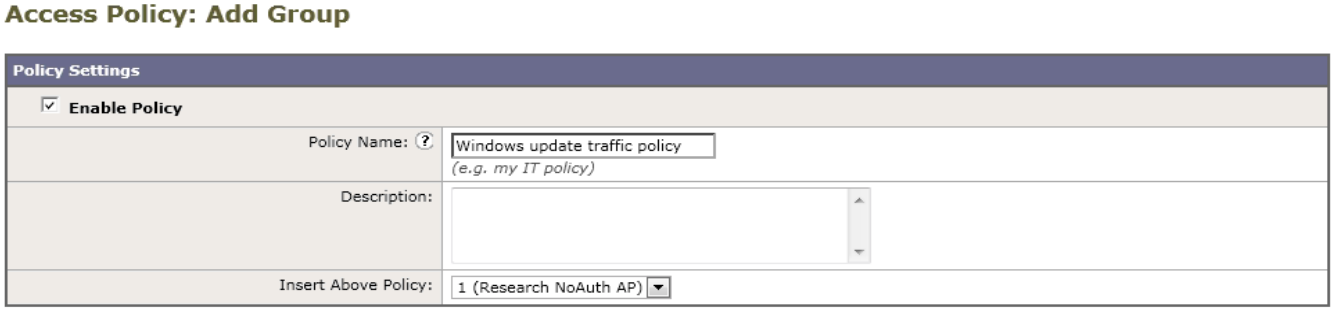
Step 3: Disable the EUA for WinAuthBypassID policy

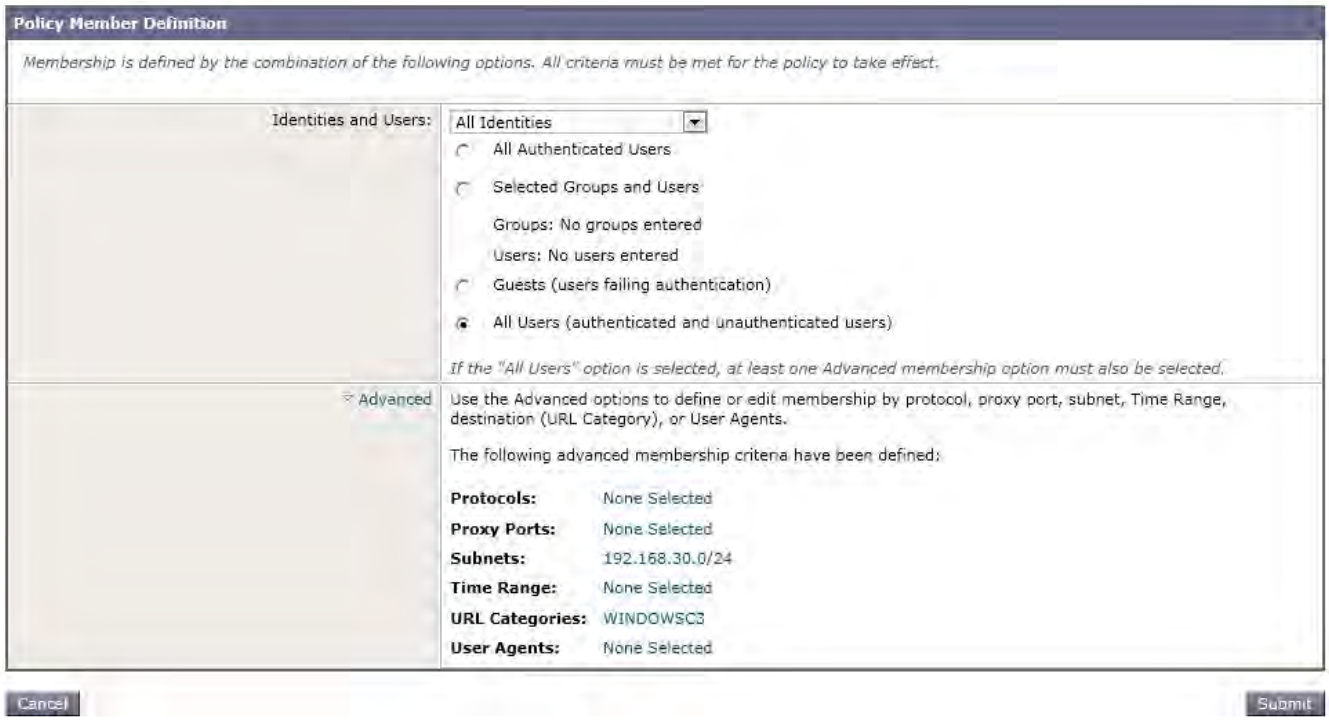


Click on Submit and apply/commit the changes



Step 4: Create a new access policy called “Windows update traffic policy” based on the custom URL category and subnets.





Step 5: Configure the Windows update traffic access policy to "ALLOW" traffic to destined to the custom URL category.

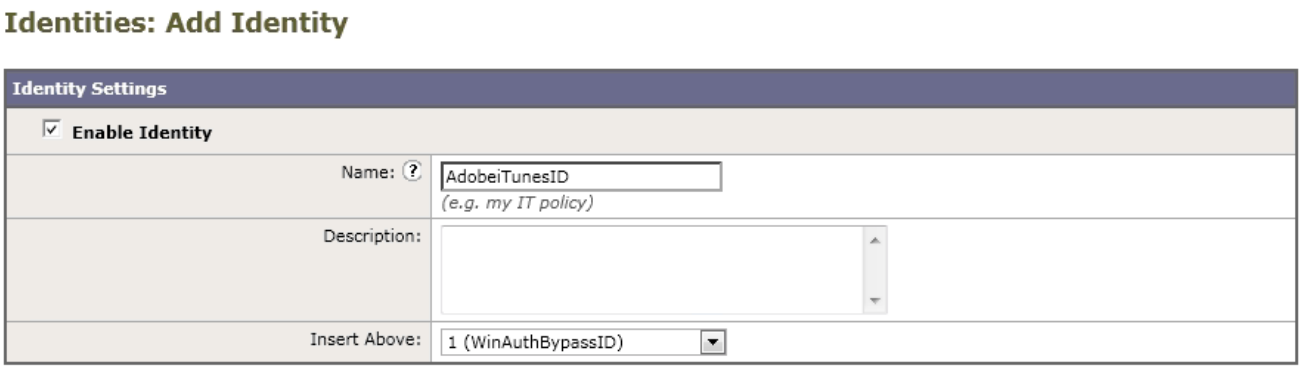
Click on Submit and apply/commit the changes

Task 5: Configure Custom URL policy – 4

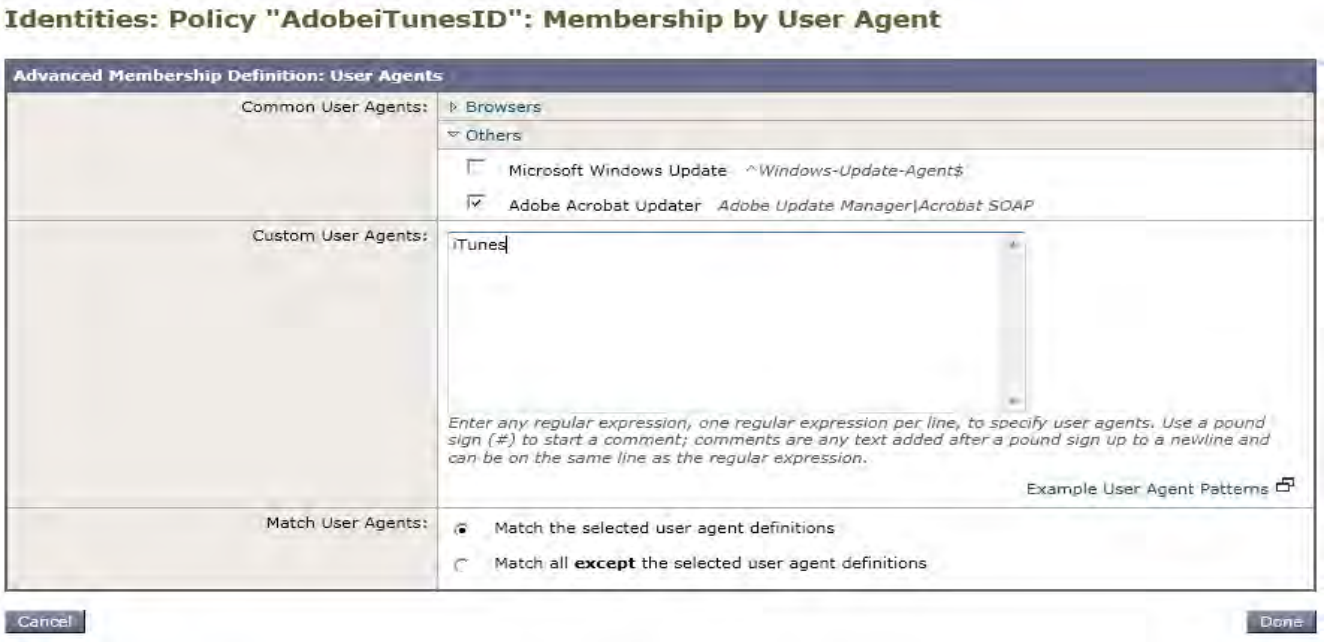
- Configure a new identity policy, which disables authentication for adobe acrobat and iTunes software updates.

Task-5: Solutions

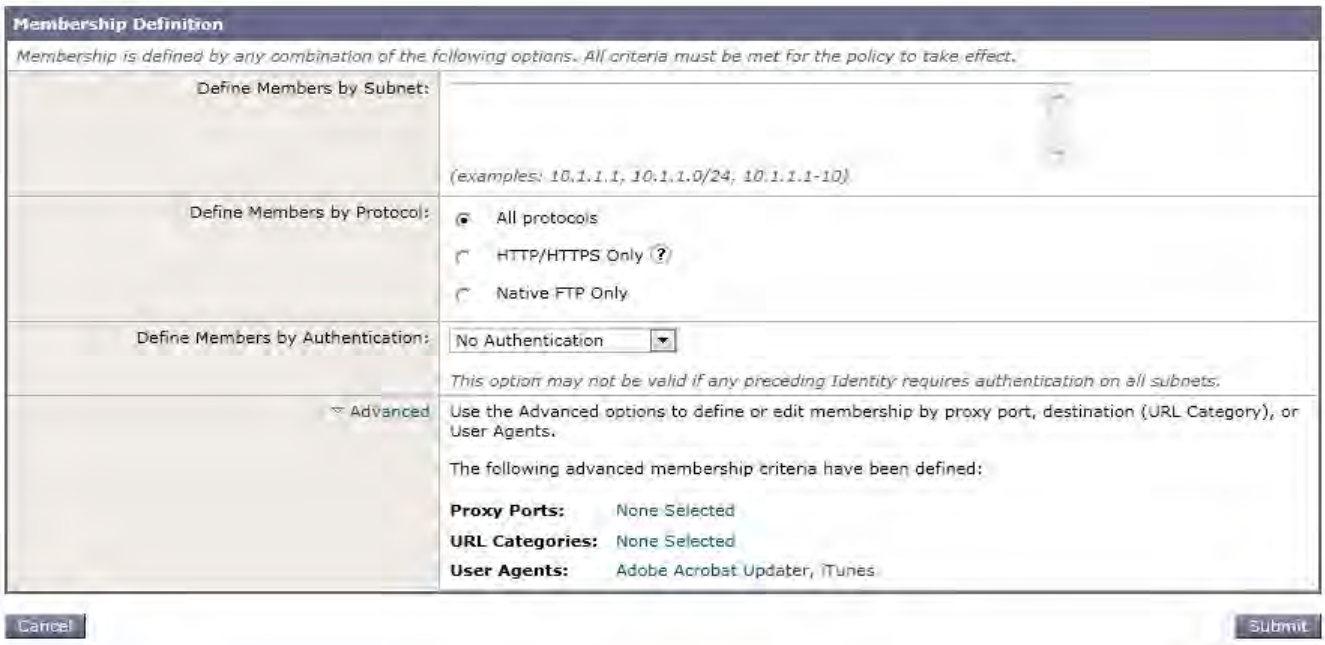
Step 1: Configure a new identity policy to disable authentication and EUA for adobe acrobat and iTunes software update based on user agent string



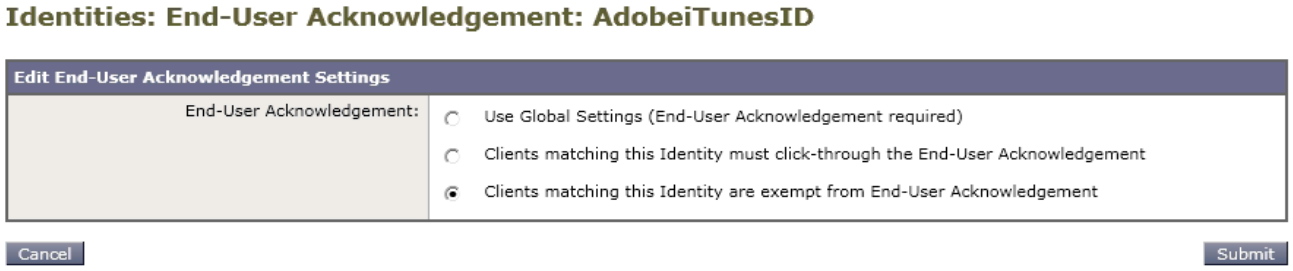
Add the useragent strings as the criteria



Click on Submit and apply/commit the changes



Disable EUA for traffic with these user agents



Click on Submit and apply/commit the changes

Task 6: Configure Custom URL policy – 5

- Only IT subnet users should be able to remotely manage R4 (HTTP-8888) and R5 on HTTP port 80. Create custom URL policy to allow access to R4 and R5. The custom URL should include the below URL's only. Test from the TEST-PC. R4 and R5 have been pre-configured for this task. Use a username of cisco and password of cisco for R4 local HTTP authentication of the routers.

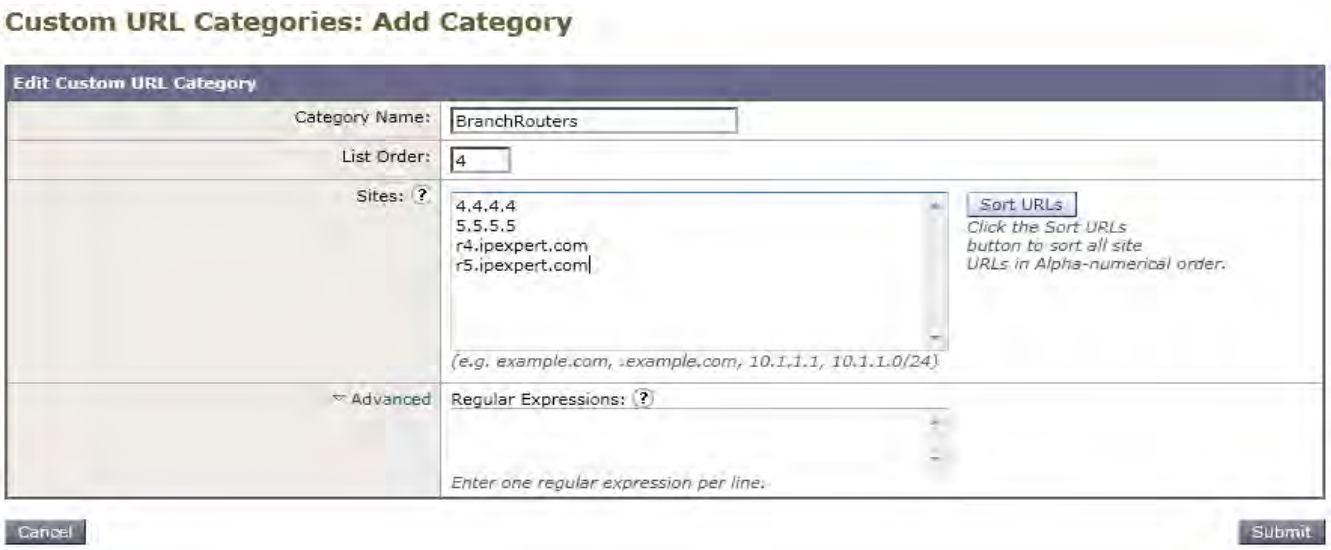
    - 4.4.4.4
    - 5.5.5.5
    - r4.ipexpert.com
    - r5.ipexpert.com

NOTE: *To test you will need to reconfigure the switch and the Test PC.*
Place the TEST-PC in VLAN 30 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 4.4.4.4/32, 5.5.5.5/32 and 192.168.0.0/16 with SW3 SVI VLAN 30 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

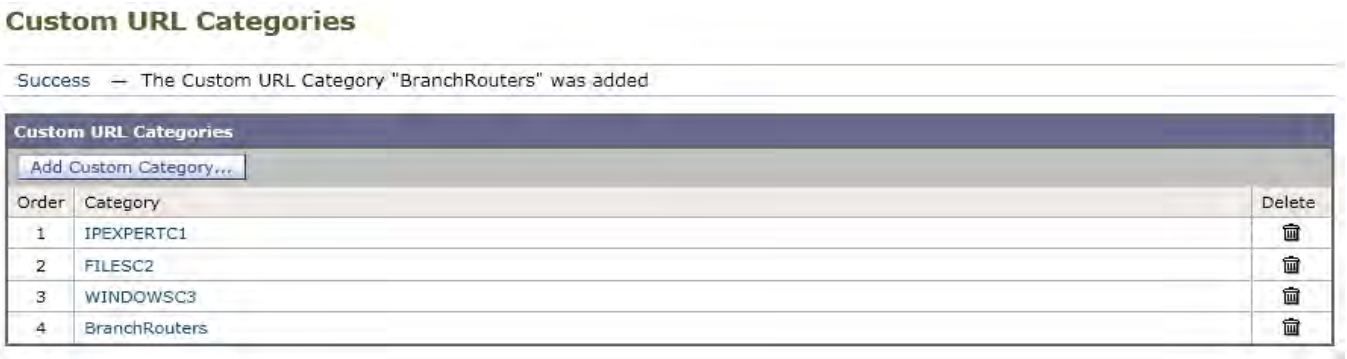
Task-6: Solutions

Step 1: Configure a new custom URL category for the guest access as per task.

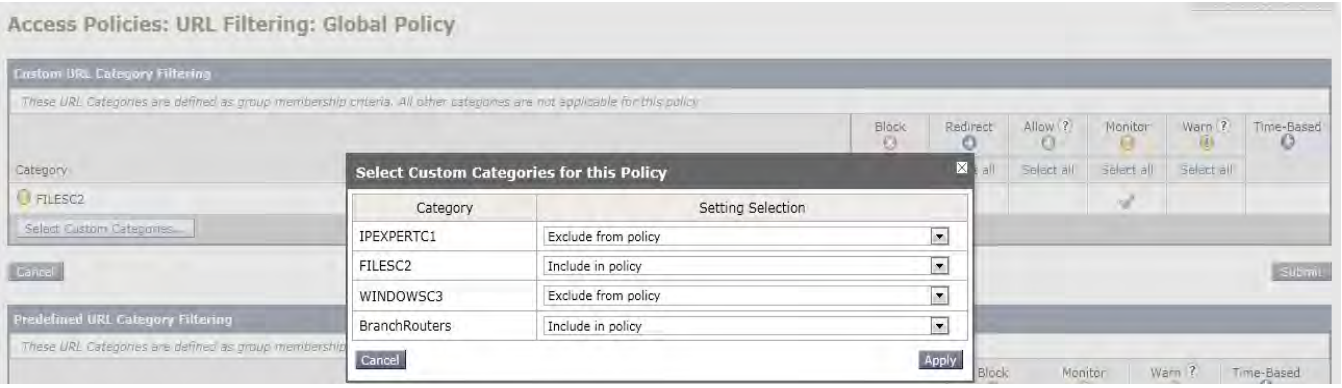
Web Security Manager -> Custom URL Categories -> Add Custom Category



Click on Submit and apply/commit the changes



Step 2: Modify Global access policy to block traffic to branch routers based on custom URL category.

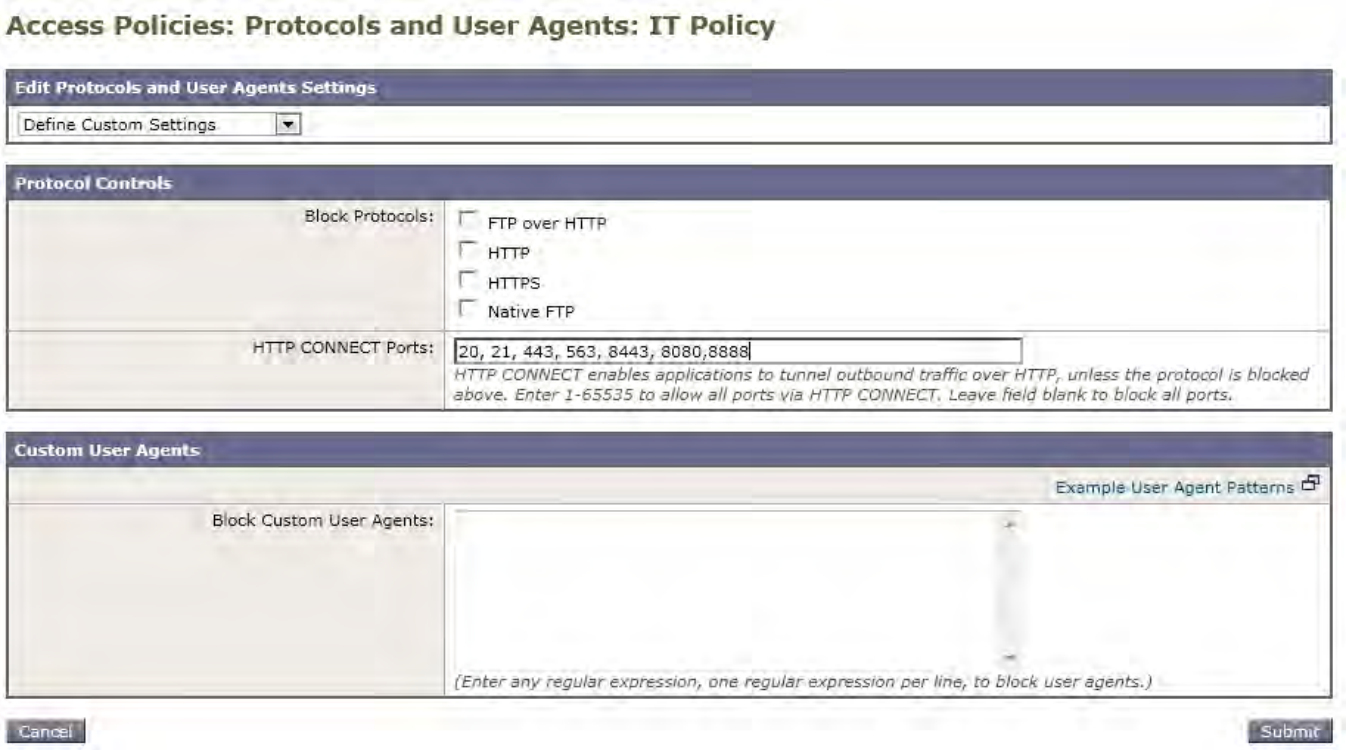


Block access to the branch routers

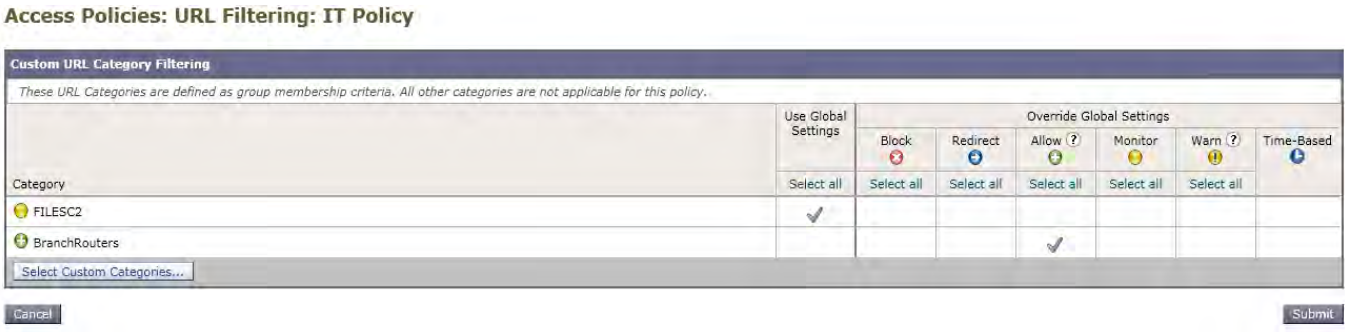
Click on Submit and apply/commit the changes

	Global Policy Identity: All	Block: 2 Protocols	Block: 59 Monitor: 9 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 18	No blocked items	Web Reputation: Enabled	

Step 2: Modify the IT policy to include TCP port 8888 as part of web traffic. (Protocols and User Agents) and commit the changes.



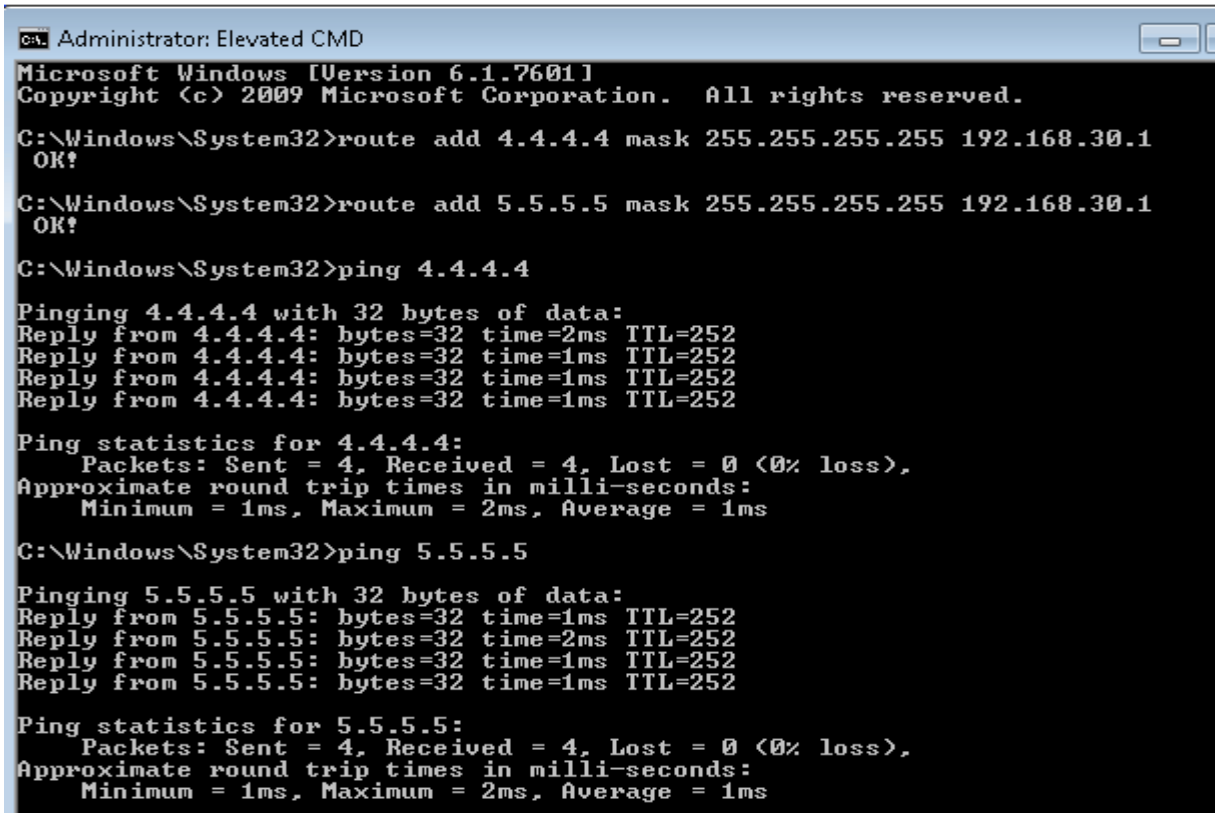
Step 3: Modify the IT access policy to allow web traffic to the branch routers.



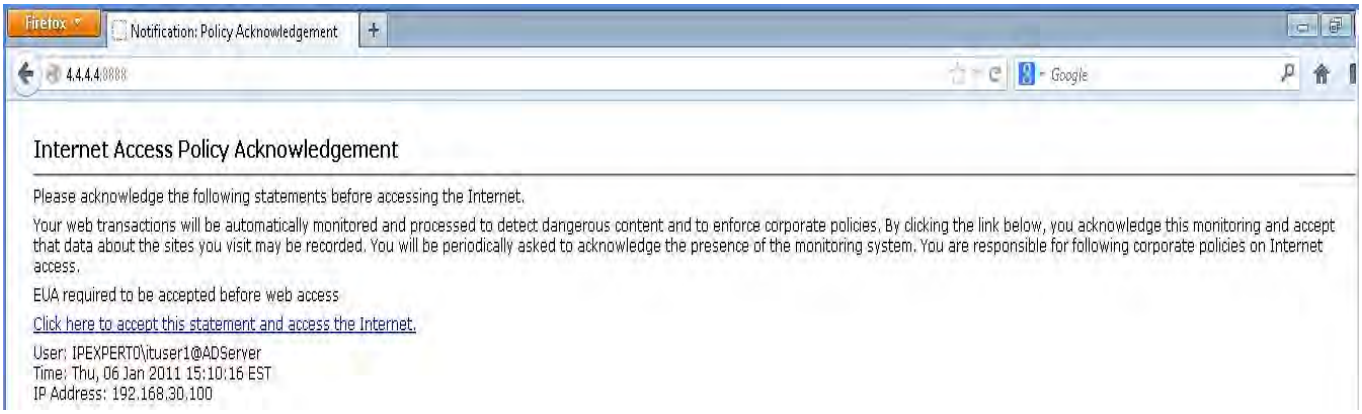
Click on Submit and apply/commit the changes

4	**IT Policy** Identity: All Subnets: 192.168.30.0/24	No blocked items	Block: 53 Warn: 1 Monitor: 13 Allow: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	🗑

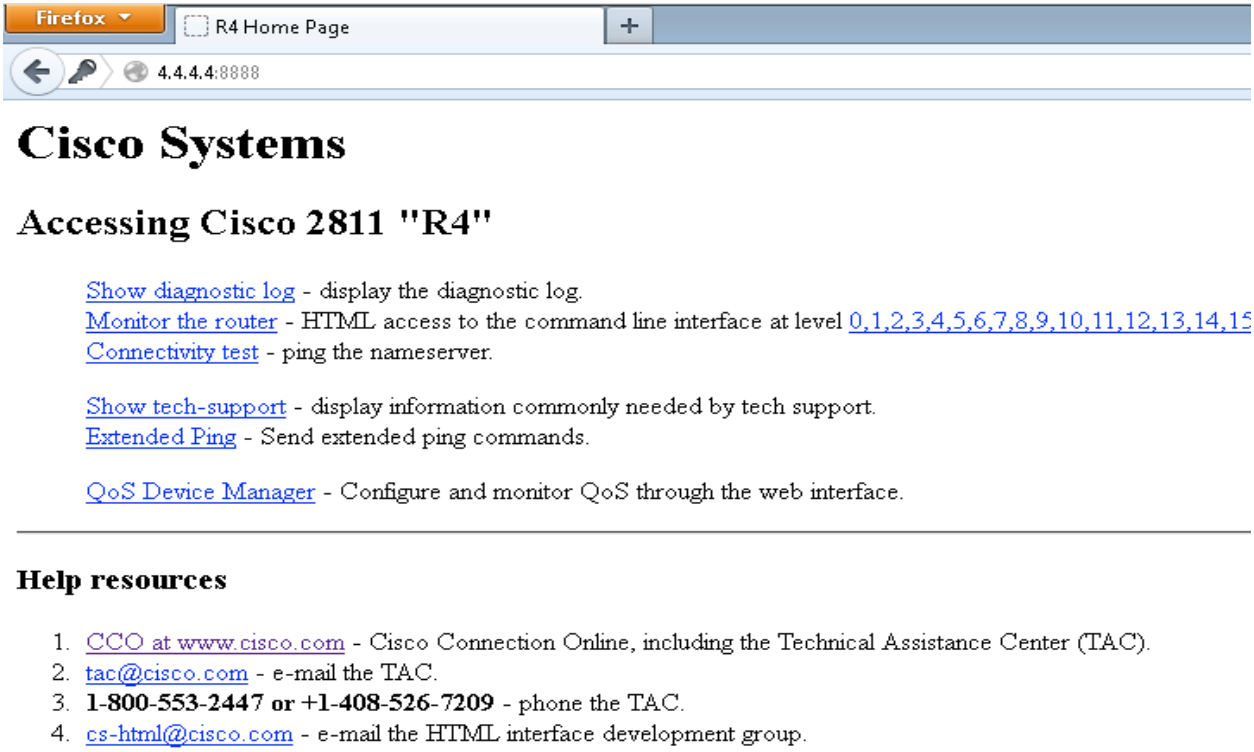
Step 4: Create static routes on the TEST PC for 4.4.4.4 and 5.5.5.5. The PC is placed in VLAN 30 based on the previous task.



Browse to 4.4.4.4:8888 Accept the AUP



Enter the username/password (cisco/cisco) for R4 web authentication



Access Logs

```
1294344694.814  26  192.168.30.100  TCP_MISS/200  2080  GET  http://4.4.4.4:8888/
"IPEXPERT0\ituser1@ADServer"   DIRECT/4.4.4.4   text/html   ALLOW_CUSTOMCAT_11-
IT_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup  <C_Bran,-,"-","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",640.00,0,-,"-
","-"> -
```

Task 7: Configure Custom URL policy – 6

- IT users should not be able to view images when they access www.ipexpert.com. Create a custom URL policy that blocks any jpeg files from www.ipexpert.com.

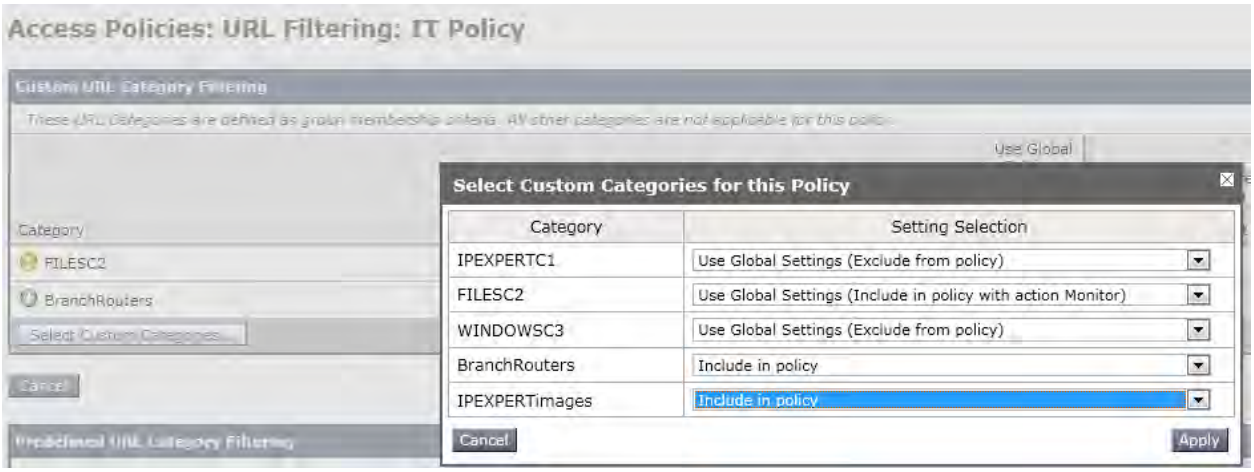
- Do not use object blocking.
- Test from test PC. You should be able to see the image when you browse into http://ipexpert.com and the image filtered when you browse to www.ipexpert.com if your custom URL category creation is correct.
- Configure the access policy appropriately.

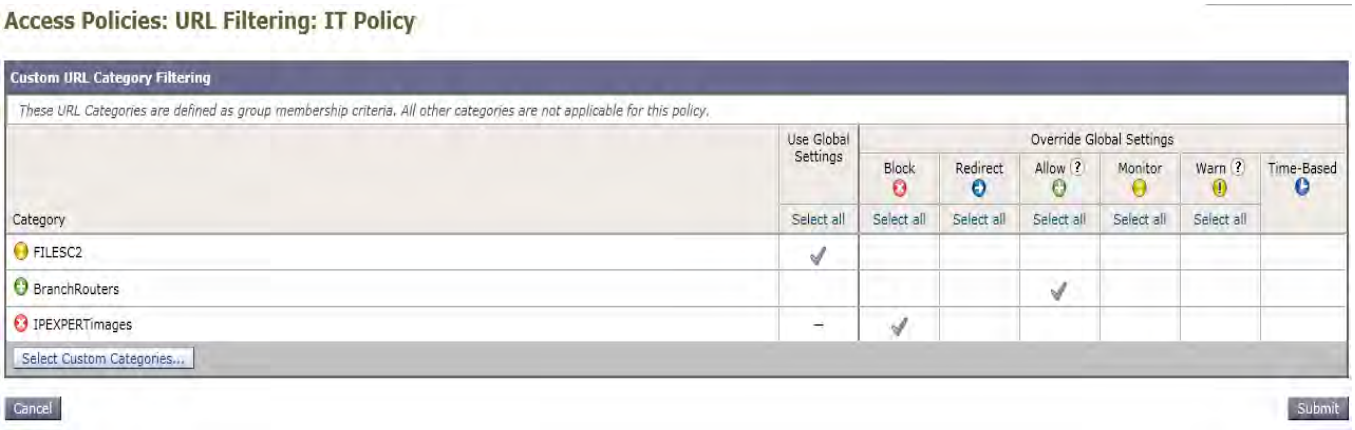
Task-7: Solutions

Step 1: Configure a new custom URL category for the guest access as per task. Submit and commit the changes.

Web Security Manager -> Custom URL Categories -> Add Custom Category

Step 2: Modify the IT policy to include the above custom category and block access to the custom URL's.

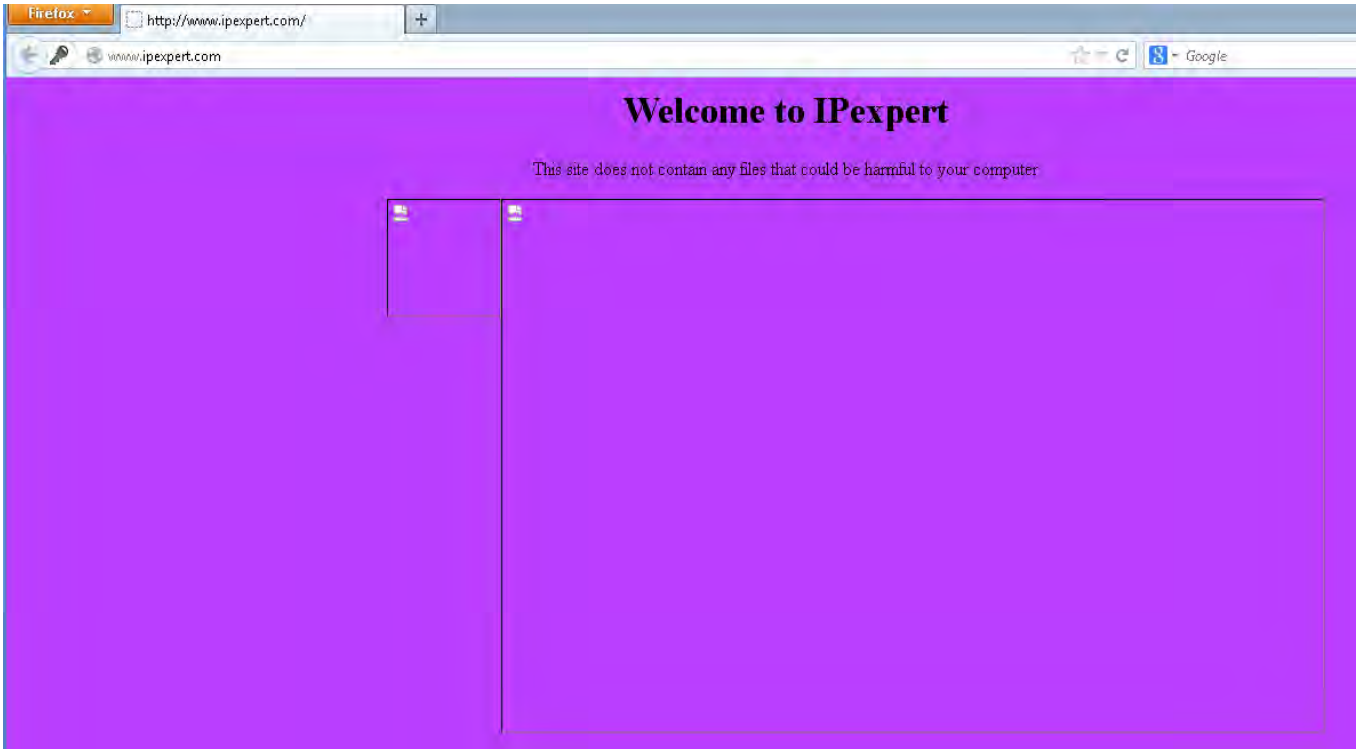




Click on Submit and apply/commit the changes

4	**IT Policy** Identity: All Subnets: 192.168.30.0/24	No blocked items	Block: 54 Warn: 1 Monitor: 13 Allow: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	

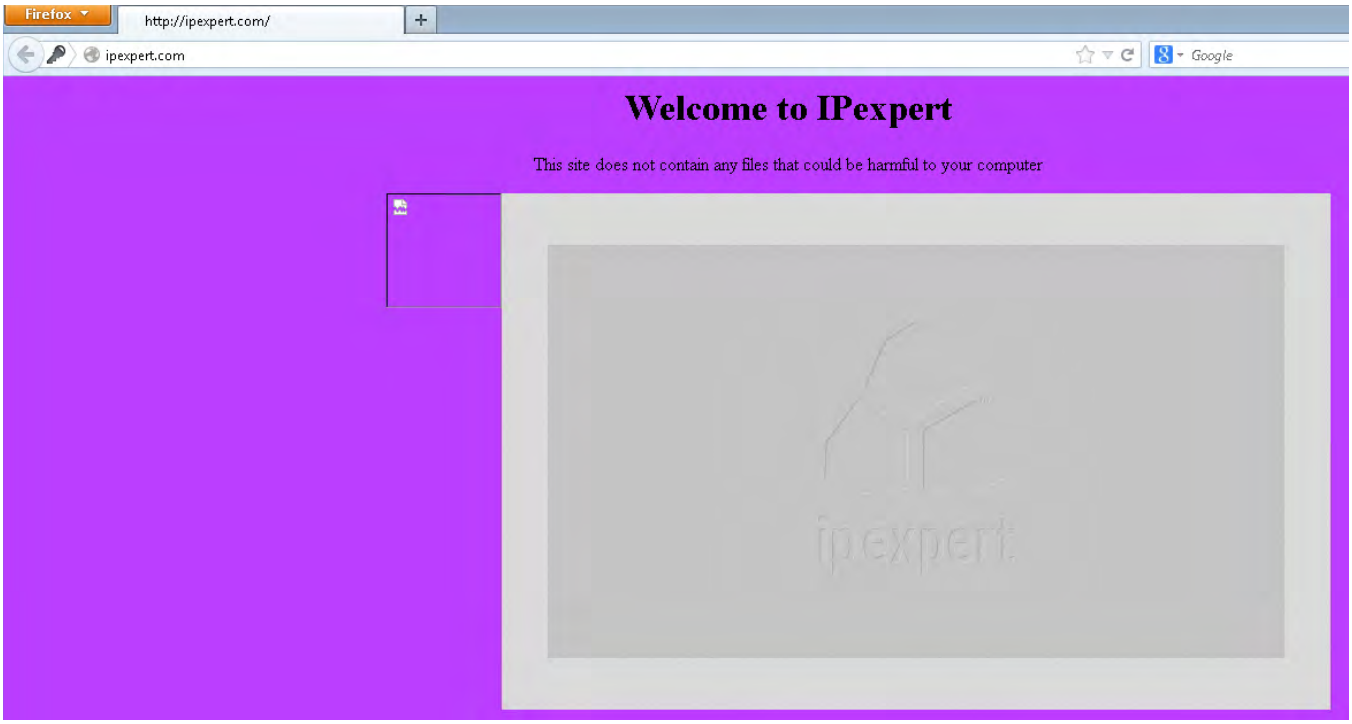
Step 3: Test from TEST PC. Browse to www.ipexpert.com. You should not be able to see any images. Make sure you clear the history/cache in firefox.



Access Logs

```
1294347253.845      2      192.168.30.100      TCP_DENIED/403      2492      GET
http://www.ipexpert.com/ipx-logo.jpg   "IPEXPERT0\ituser1@ADServer"   NONE/-   -
BLOCK_CUSTOMCAT_11-IT_Policy-DefaultGroup-NONE-NONE-NONE-NONE      <C_IPE0,-,"-
","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-
",9968.00,0,-,"-","-"> -
```

Step 4: Test from TEST PC. Browse to http://ipexpert.com. You should be able to see images. Make sure you clear the history/cache in Firefox.



Access Logs

```
1294347496.537 75002 192.168.30.100 TCP_MISS/200 753 GET http://ipexpert.com/
"IPEXPERT0\ituser1@ADServer" DIRECT/ipexpert.com text/html DEFAULT_CASE_11-
IT_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup <IW_edu,0.0,"1","-",-,-,-
,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_edu,-,"-","-","Unknown","Unknown","-
","-",0.08,0,-,"-","-"> -
1294347559.876 75330 192.168.30.100 TCP_MISS/200 240438 GET
http://ipexpert.com/ipx-logo.jpg "IPEXPERT0\ituser1@ADServer"
DIRECT/ipexpert.com image/jpeg DEFAULT_CASE_11-IT_Policy-DefaultGroup-NONE-
NONE-NONE-DefaultGroup <IW_edu,0.0,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-
","-",-,-,IW_edu,-,"-","-","Unknown","Unknown","-","-",25.53,0,-,"-","-"> -
```

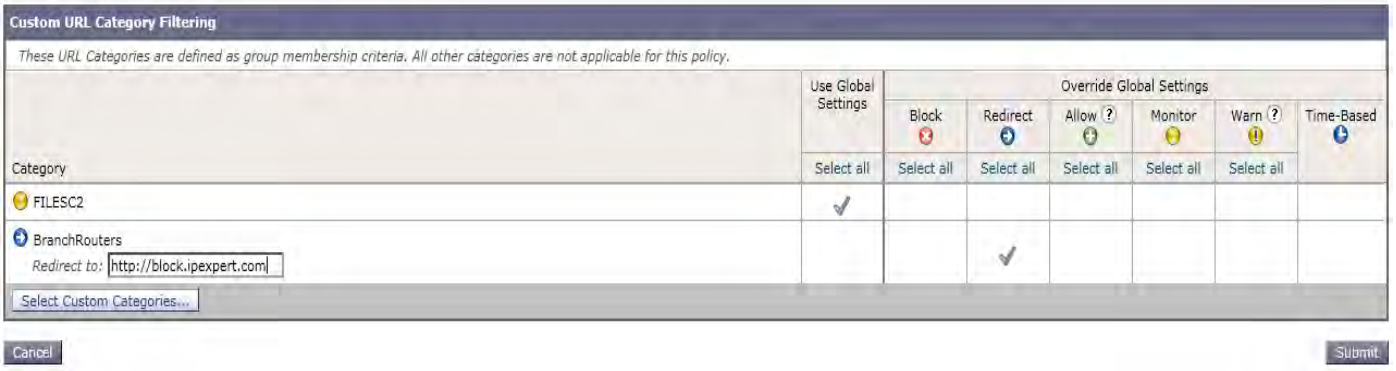
Task 8: Configure Custom URL policy – 7

- If any research user tries to access R4 and R5 routers they should be redirected to http://block.ipexpert.com. You are allowed to use custom URL categories in the access policy to accomplish this task.
- To test you may need to reconfigure the switch and TEST-PC accordingly.

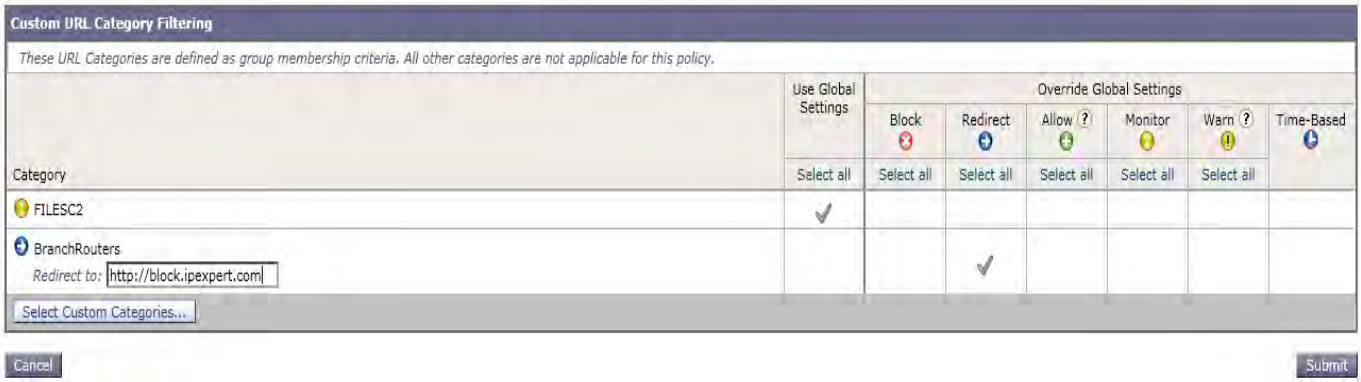
Task-8: Solutions

Step 1: Modify both the research access policy to redirect traffic to http://block.ipexpert.com when they browse to R4 or R5. Use custom URL's for this.

Access Policies: URL Filtering: Research



Access Policies: URL Filtering: Research NoAuth AP



Click on Submit and apply/commit the changes

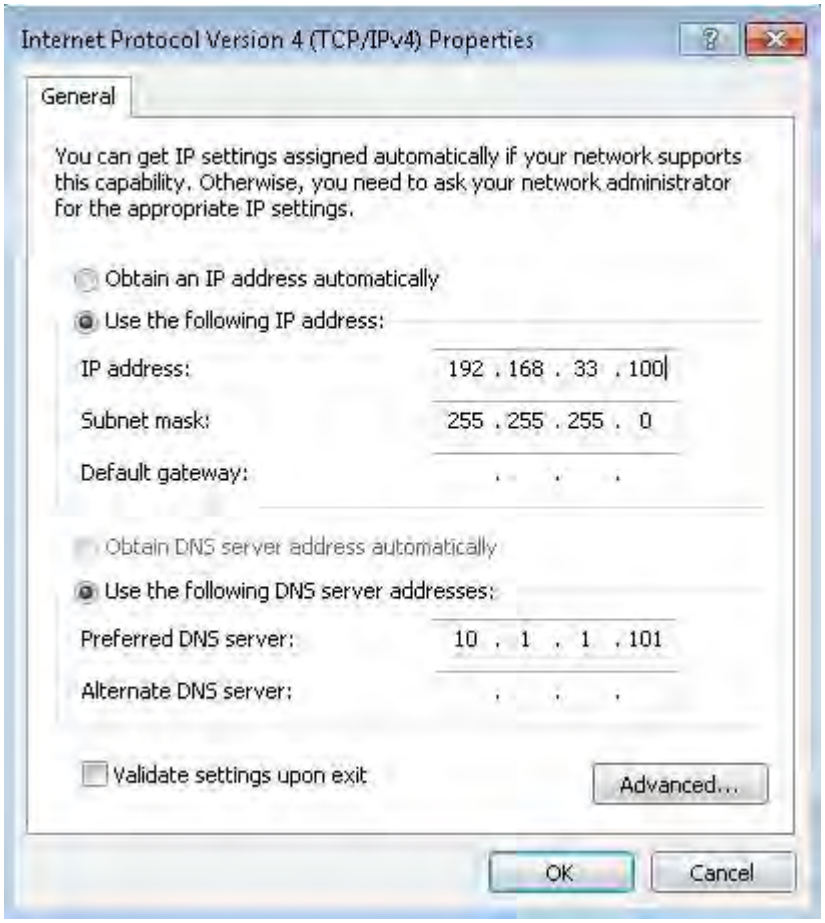
2	**Research NoAuth AP** Identity: All Subnets: 192.168.33.33	No blocked items	Monitor: 67 Redirect: 1	(global policy)	(global policy)	(global policy)	
3	**Research** Identity: All Subnets: 192.168.33.0/24	No blocked items	Monitor: 67 Redirect: 1	(global policy)	(global policy)	(global policy)	

Step 2: Place the TEST PC in VLAN 33 (Research) and configure IP address and add static routes.

SW3

```
interface GigabitEthernet1/0/2
 switchport access vlan 33
```

```
switchport mode access
spanning-tree portfast
```

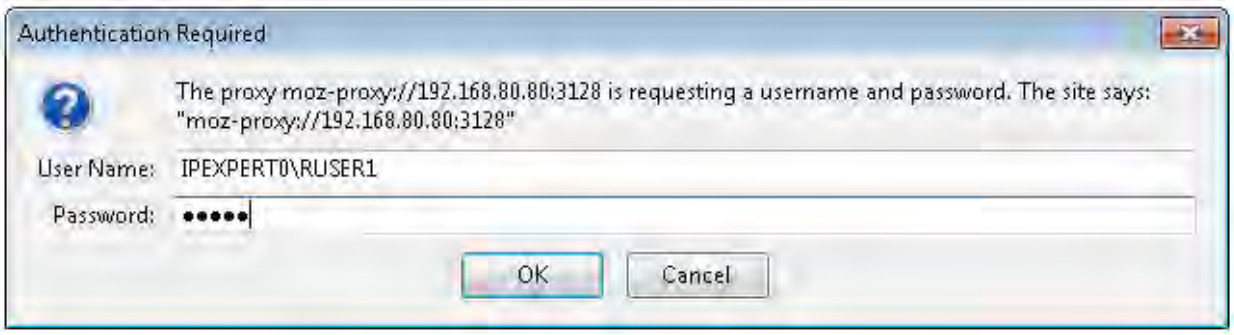


Remove the old static routes and add new static routes with next hop as 192.168.33.1 (SW3 VLAN 33 SVI). Perform basic ping test

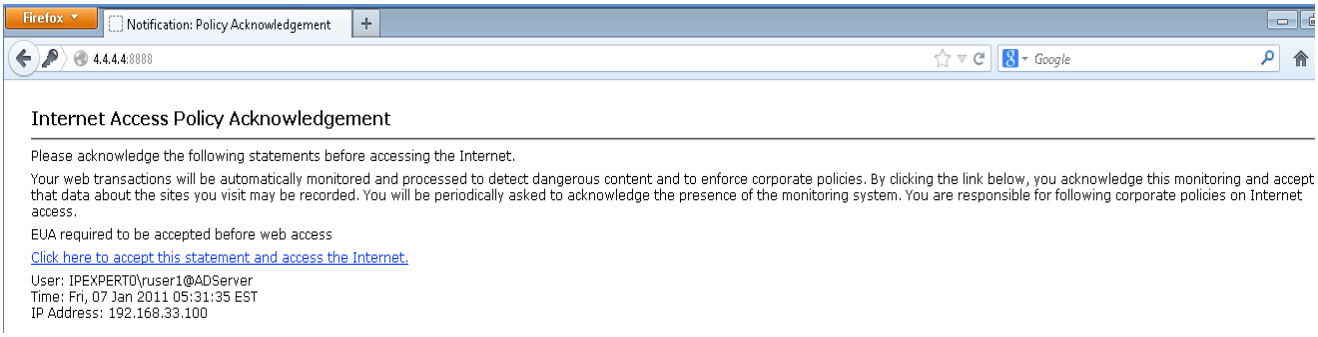
```
Administrator: Elevated CMD
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>route delete 4.4.4.4
 OK!

C:\Windows\System32>route delete 5.5.5.5
 OK!

C:\Windows\System32>route delete 192.168.0.0
 OK!

C:\Windows\System32>route delete 10.1.1.101
 OK!

C:\Windows\System32>route add 192.168.0.0 mask 255.255.0.0 192.168.33.1
 OK!

C:\Windows\System32>route add 10.1.1.101 mask 255.255.255.255 192.168.33.1
 OK!

C:\Windows\System32>route add 4.4.4.4 mask 255.255.255.255 192.168.33.1
 OK!

C:\Windows\System32>route add 5.5.5.5 mask 255.255.255.255 192.168.33.1
 OK!

C:\Windows\System32>ping 4.4.4.4

Pinging 4.4.4.4 with 32 bytes of data:
Reply from 4.4.4.4: bytes=32 time=4ms TTL=252
Reply from 4.4.4.4: bytes=32 time=1ms TTL=252
Reply from 4.4.4.4: bytes=32 time=1ms TTL=252
Reply from 4.4.4.4: bytes=32 time=1ms TTL=252

Ping statistics for 4.4.4.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

Step 3: Clear the browser history of Firefox and browse to wither 4.4.4.4:8888 or 5.5.5.5 and you must be redirected to the block page.

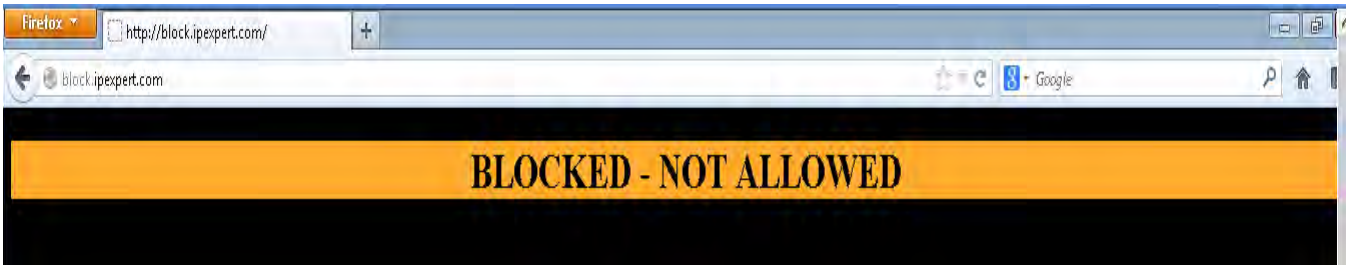
Enter the proxy user authentication information



Accept the EUA.



You will be redirect to http://block.ipexpert.com



Access Logs

```
1294396361.137  1  192.168.33.100  TCP_DENIED/302  1837  GET  http://4.4.4.4:8888/
"IPEXPERT0\ruser1@ADServer"     NONE/-     -     REDIRECT_CUSTOMCAT_11-Research-
DefaultGroup-NONE-NONE-NONE-NONE  <C_Bran,-,"-","-",-,-,-,"-","-",-,-,-,"-","-
",-,"-","-",-,-,-,-,"-","-","-","-","-","-",14696.00,0,-,"-","-"> -

1294396363.929    2771    192.168.33.100    TCP_REFRESH_HIT/200    577    GET
http://block.ipexpert.com/                          "IPEXPERT0\ruser1@ADServer"
DIRECT/block.ipexpert.com   text/html   DEFAULT_CASE_11-Research-DefaultGroup-
NONE-NONE-NONE-DefaultGroup  <IW_edu,0.0,"1","-",-,-,-,"-","-",-,-,-,"-","-",-
,"-","-",-,-,IW_edu,-,"-","-","Unknown","Unknown","-","-",1.67,0,-,"-","-"> -
```

Lab-3: Configuring Acceptable Use Policies on WSA for HTTPS

Lab-3: Configuring AUP's for HTTPS– This lab is intended to familiarize you with configuring WSA as a HTTPS proxy and configuring various decryption policies.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- To test a task you may need to re-configure the TEST-PC and the switch accordingly. DO not explicitly set the default gateway on the TEST-PC.

Estimated Time to Complete: 1.5 Hour

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-2 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Detailed Solution: Lab-3

Task 1: Configure WSA for HTTPS Proxy

- Enable HTTPS proxy services on the WSA. The WSA should act as a self-signed root authority when acting as man in the middle for HTTPS proxy. Use the below parameters for creating the self-signed root certificate. Enable decryption for AVC. Invalid certificate handling should be set to monitor.

Common name: WSA

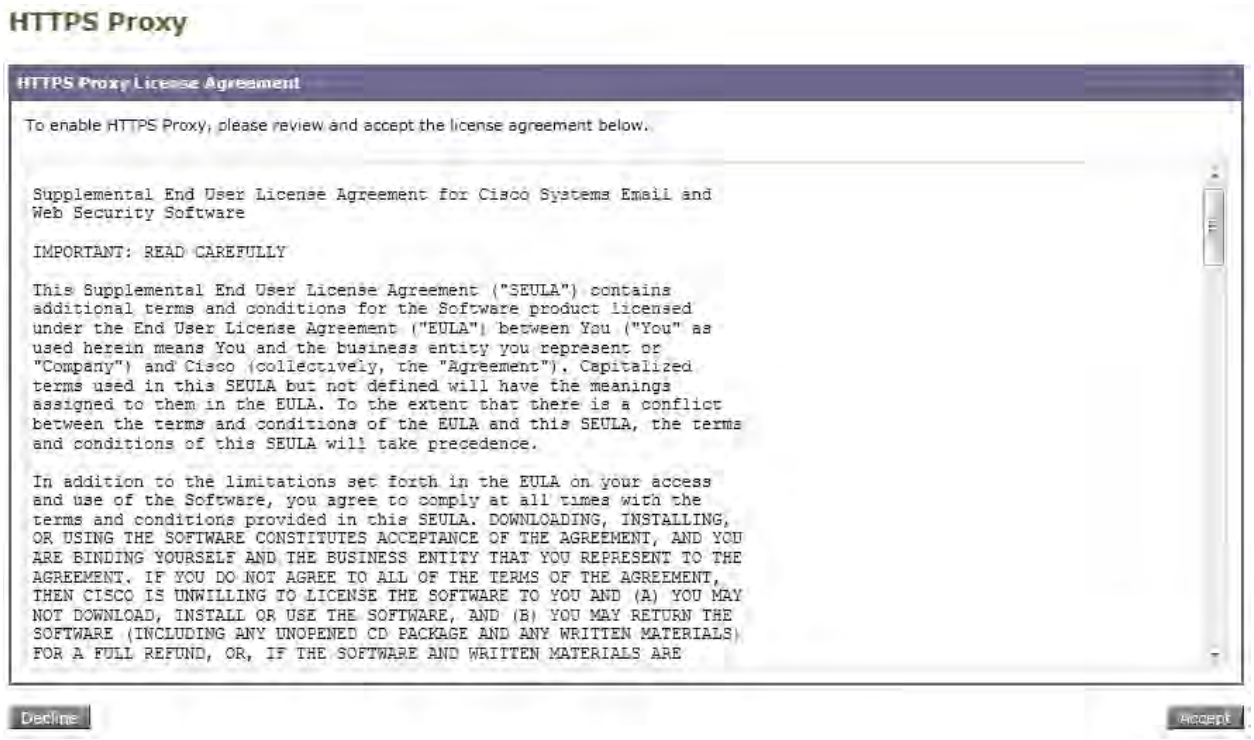
Organization: NETSEC
Organizational Unit: IPEXPERT
Country: US
Expiration Date: 36 Months

Task-1: Solutions

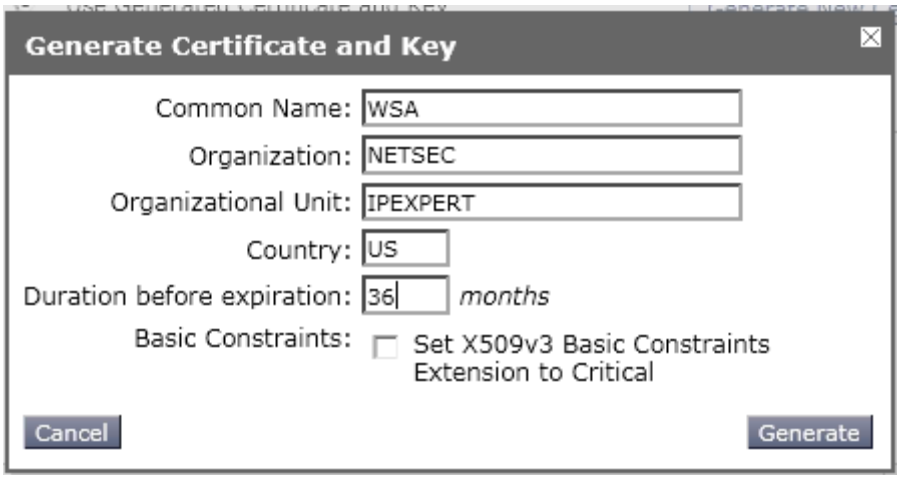
Step 1: Enable HTTPS proxy and create a new self-signed root certificate for the WSA to enable proxy function and enable Enable decryption for enhanced application visibility and control

Security Services -> HTTPS proxy -> Enable and Edit Settings

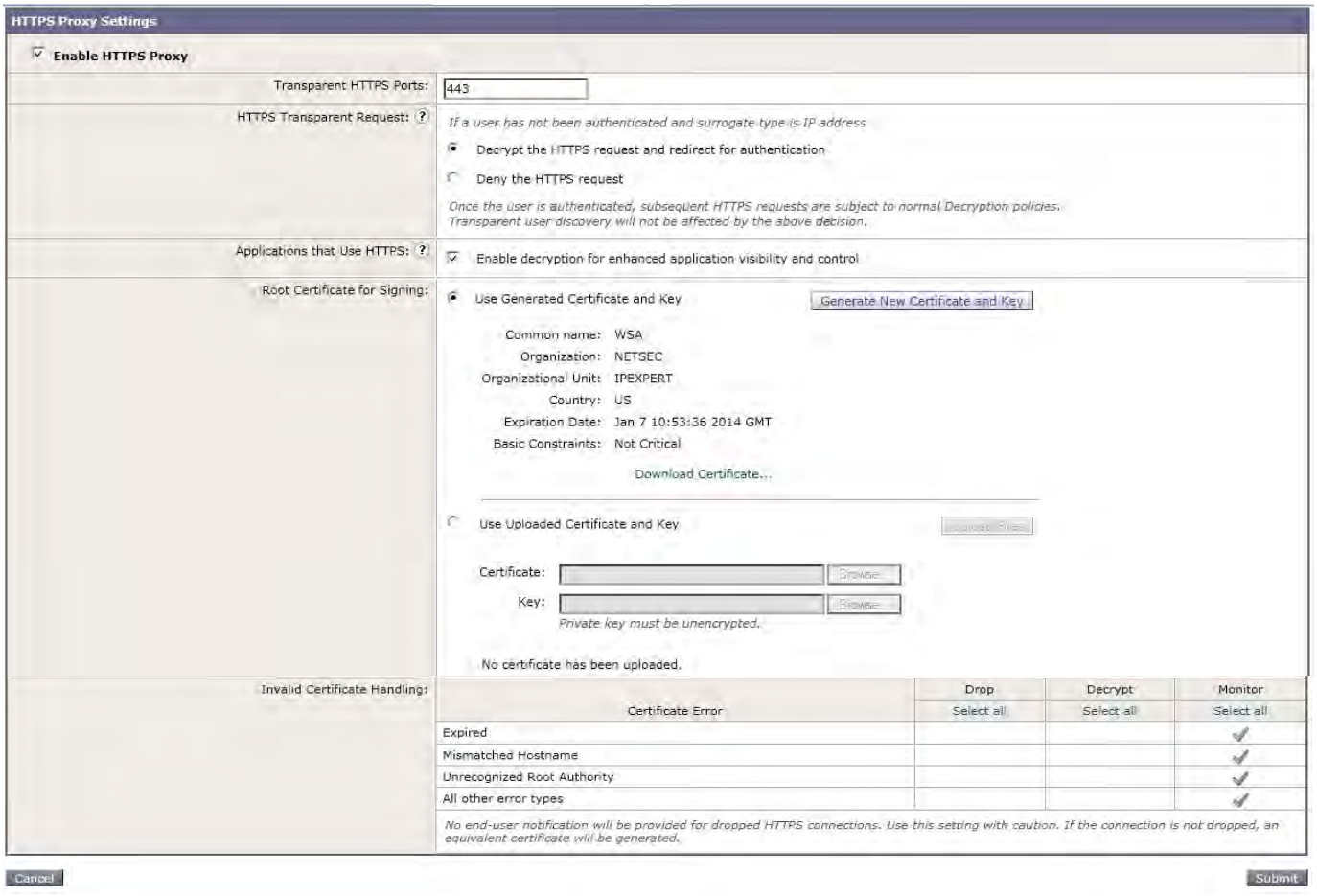
Accept the HTTPS proxy license



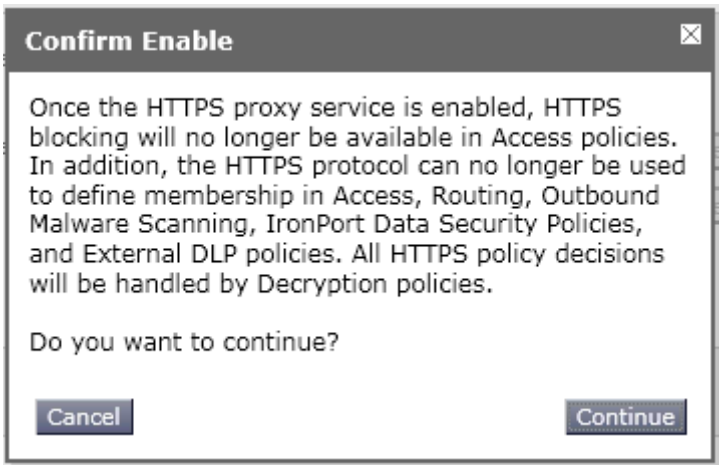
Generate a new self-signed root certificate using the parameters given in the task



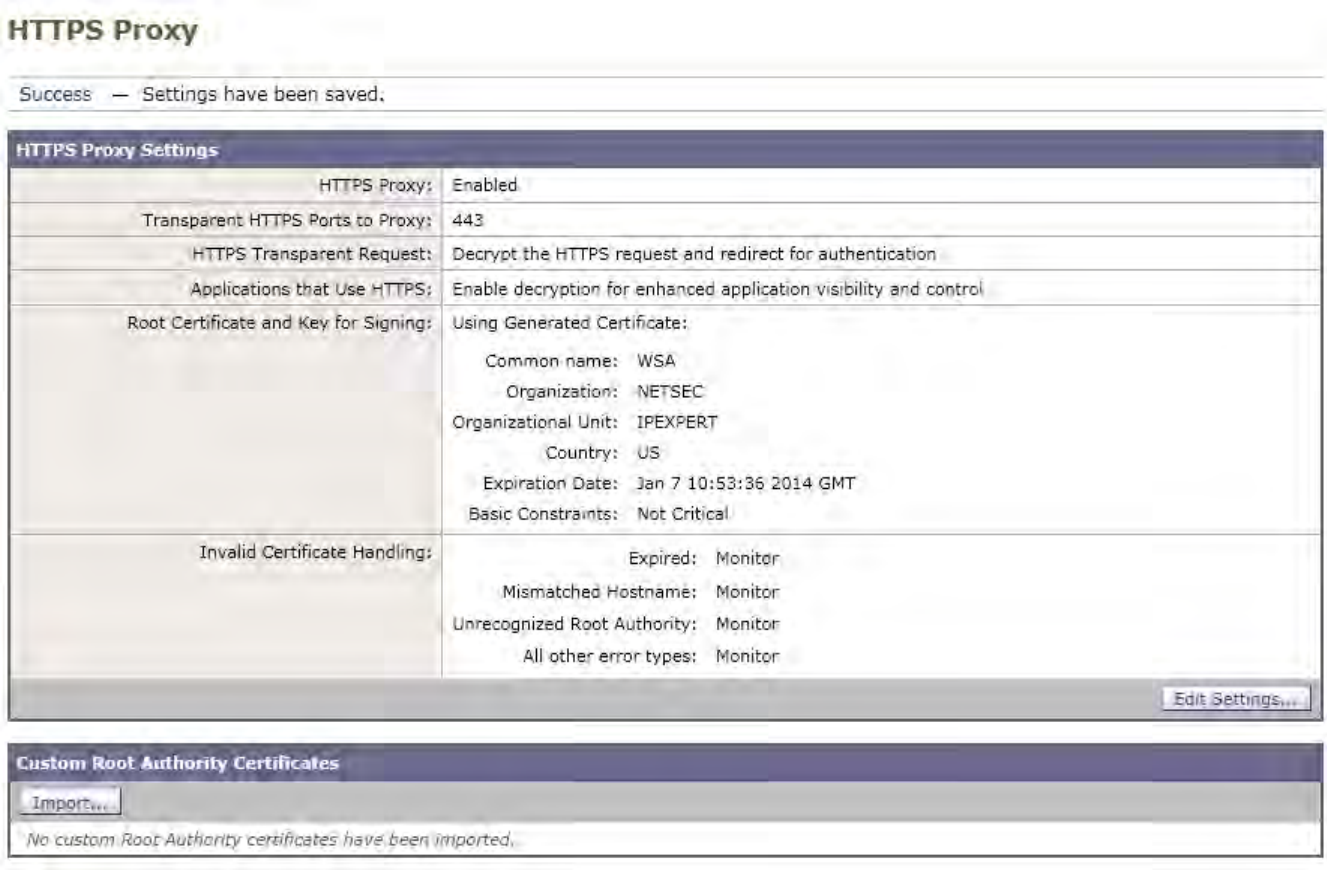
Enable AVC for HTTPS decryoted traffic



Click on Submit and apply/commit the changes



Commit the change. Vefify the information with the task.



Task 2: Decryption Policies – 1

- Configure decryption for the below URL categories so that access polices can be applied for them. WSA should drop all other SSL connections even for sites have no WBRS scores.

Business and Industry
Cheating and Plagiarism
Computer Security
Computers and Internet
Education
File Transfer Services
Finance
Government and Law
Illegal Activities
Job Search
News
Online Trading
Real Estate
Science and Technology
Search Engines and Portals
Streaming Media
Web Hosting
Web Page Translation
Web-based Chat
Web-based Email

Task-2: Solutions

Step 1: Configure the global decryption policy to decrypt traffic for the pre-defined URL's as per the task such that Access Policies can be applied after decryption (**Web Security Manager->Decryption Policies**)

Decryption Policies: URL Filtering: Global Policy

Custom URL Category Filtering

No Custom Categories are included for this Policy.

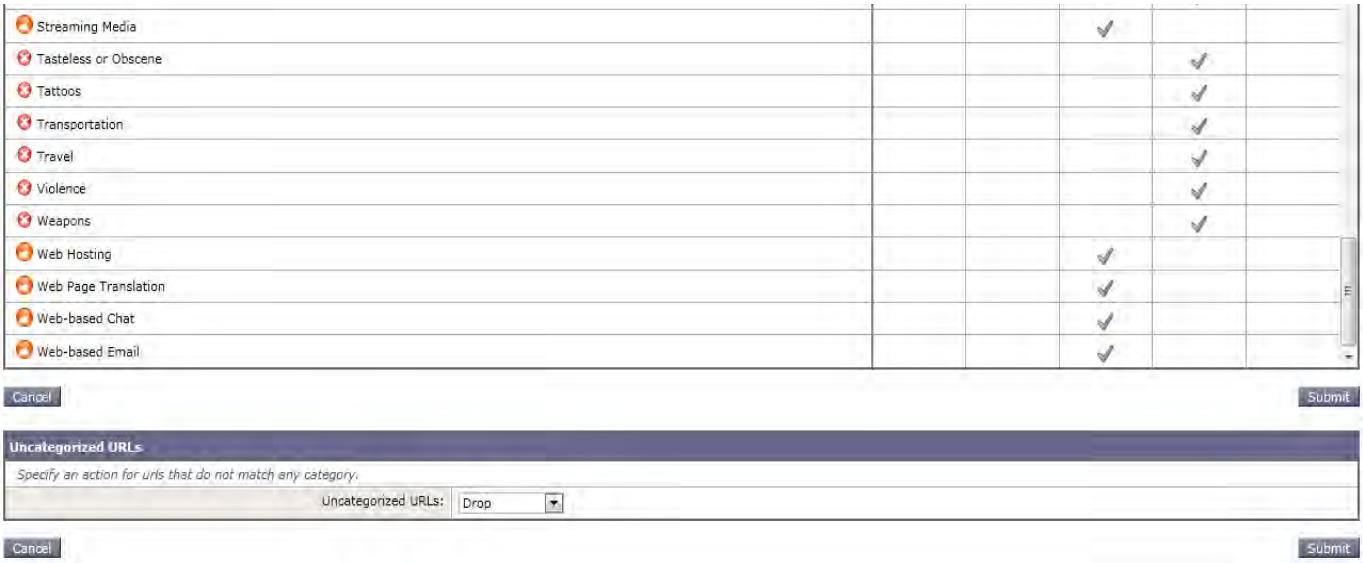
Select Custom Categories...

Predefined URL Category Filtering

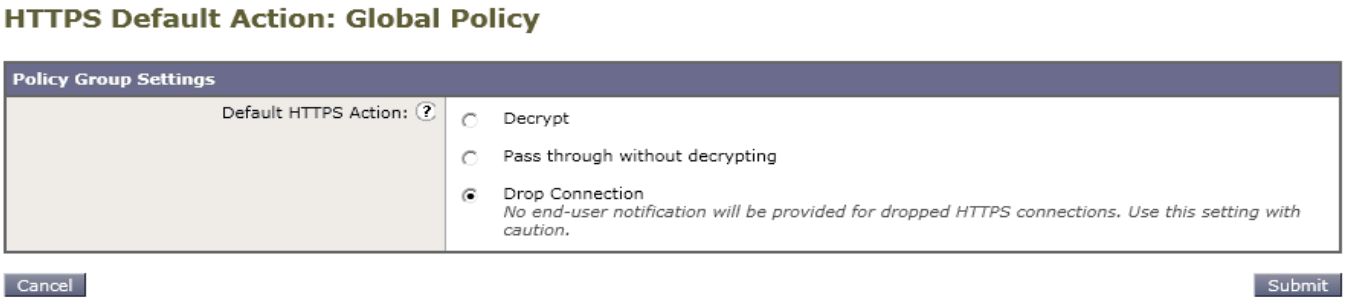
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Pass Through	Monitor	Decrypt	Drop	Time-Based
	Select all	Select all	Select all	Select all	
Adult				✓	
Advertisements				✓	
Alcohol and Tobacco				✓	
Arts and Entertainment				✓	
Business and Industry			✓		
Cheating and Plagiarism			✓		
Child Porn				✓	
Computer Security			✓		
Computers and Internet				✓	
Cults				✓	
Dating				✓	
Dining and Drinking				✓	
Education			✓		
File Transfer Services			✓		
Filter Avoidance				✓	
Finance			✓		
Freeware and Shareware				✓	
Gambling				✓	
Games				✓	
Government and Law			✓		
Hacking				✓	
Hate Speech				✓	
Health and Nutrition				✓	
Illegal Activities			✓		
Job Search			✓		
Lingerie and Swimsuits				✓	
Lottery and Sweepstakes				✓	
Mobile Phones				✓	
Nature				✓	
News			✓		
Non-sexual Nudity				✓	
Online Communities				✓	
Online Storage and Backup				✓	
Online Trading			✓		

Drop uncategorized URL's



Configure default action to drop



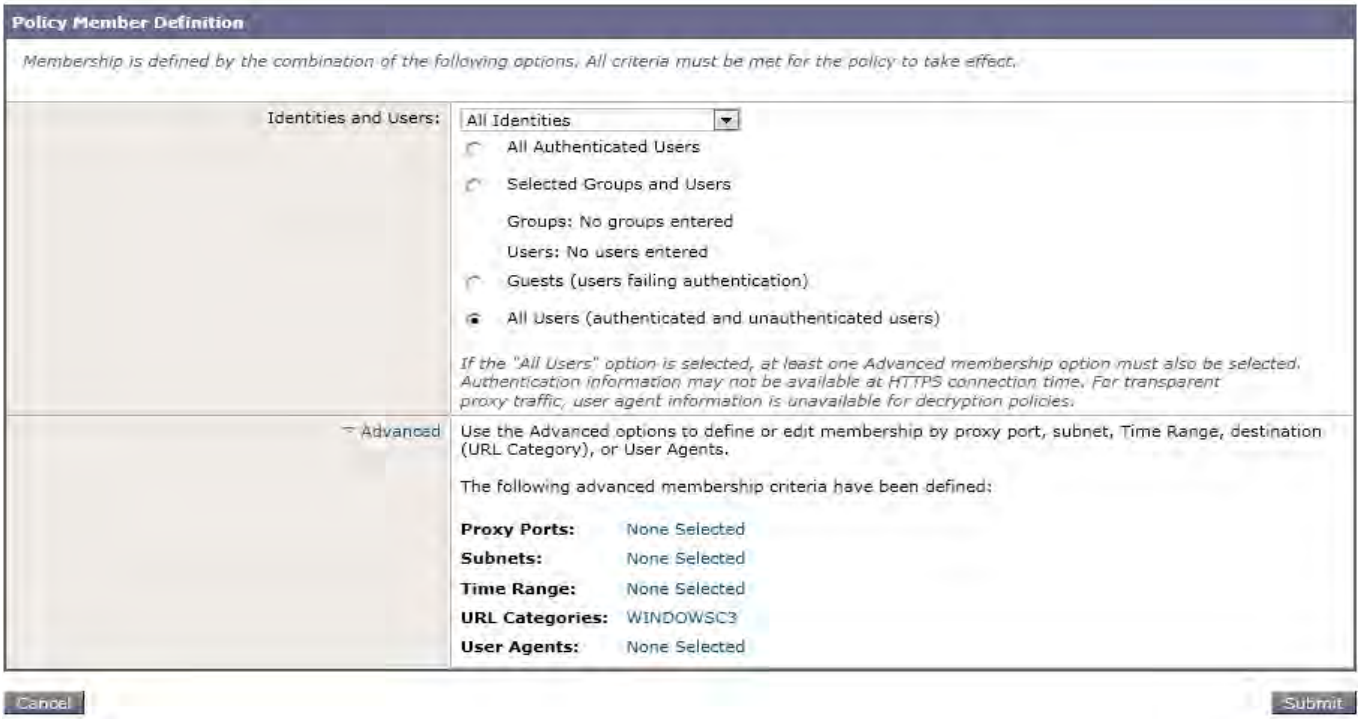
Click on Submit and apply/commit the changes

Task 3: Decryption Policies – 2

- All traffic destined to Microsoft update server should pass through without decryption. Configure a new decryption policy, which is applicable only for IT, subnet for the above mentioned traffic.

Task-3: Solutions

Step 1: Configure a new decryption policy based on the custom URL categories previously configured for windows update.



Click on Submit and apply/commit the changes

Change the action to “Pass through” for the custom URL category.

Decryption Policies: URL Filtering: WindowsD1

Click on Submit and apply/commit the changes

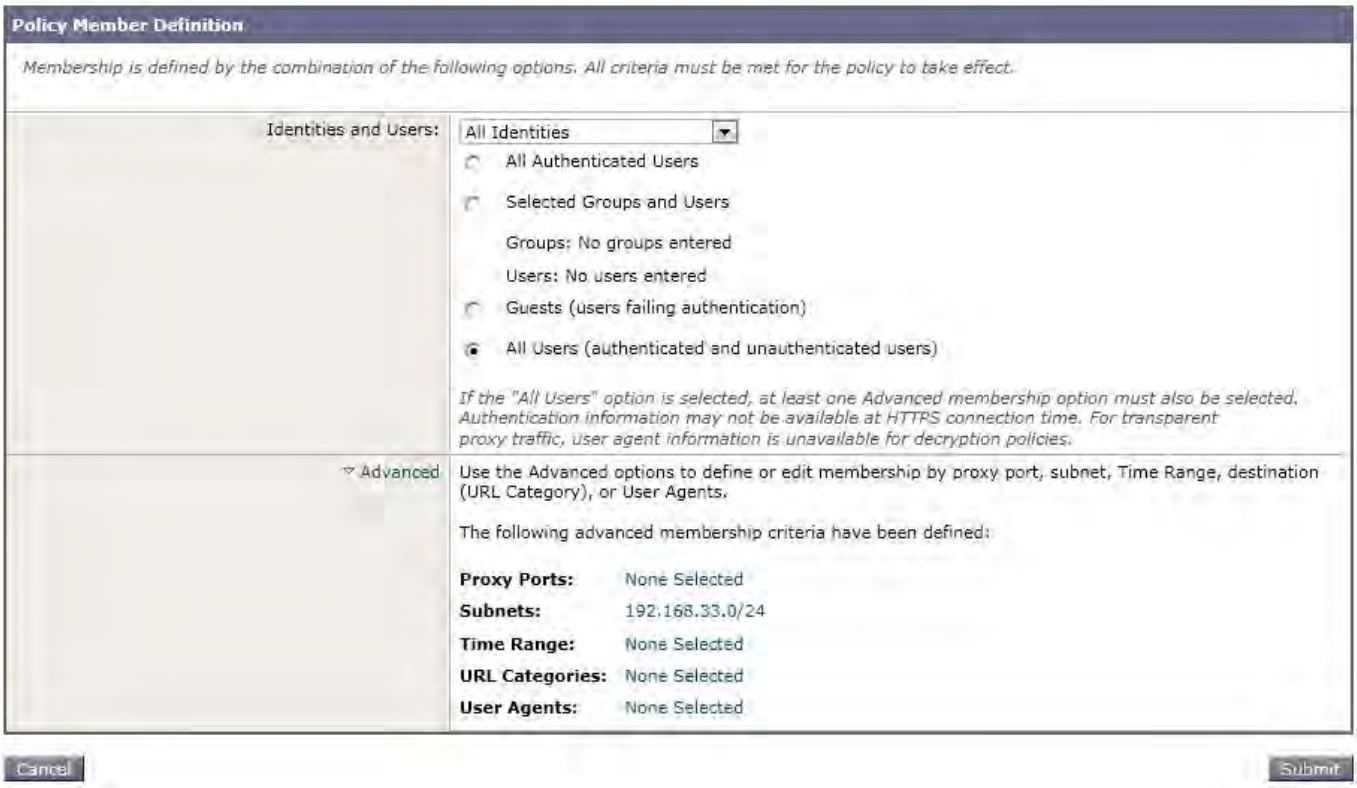
Task 4: Decryption Policies – 3

- Research user subnet should be allowed HTTPS access for all URL's based on WBRS. WBRS should either drop or decrypt based on WBRS score. Sites with no WBRS scores should be dropped. You are allowed to modify WBRS. However do not change the WBRS drop threshold.

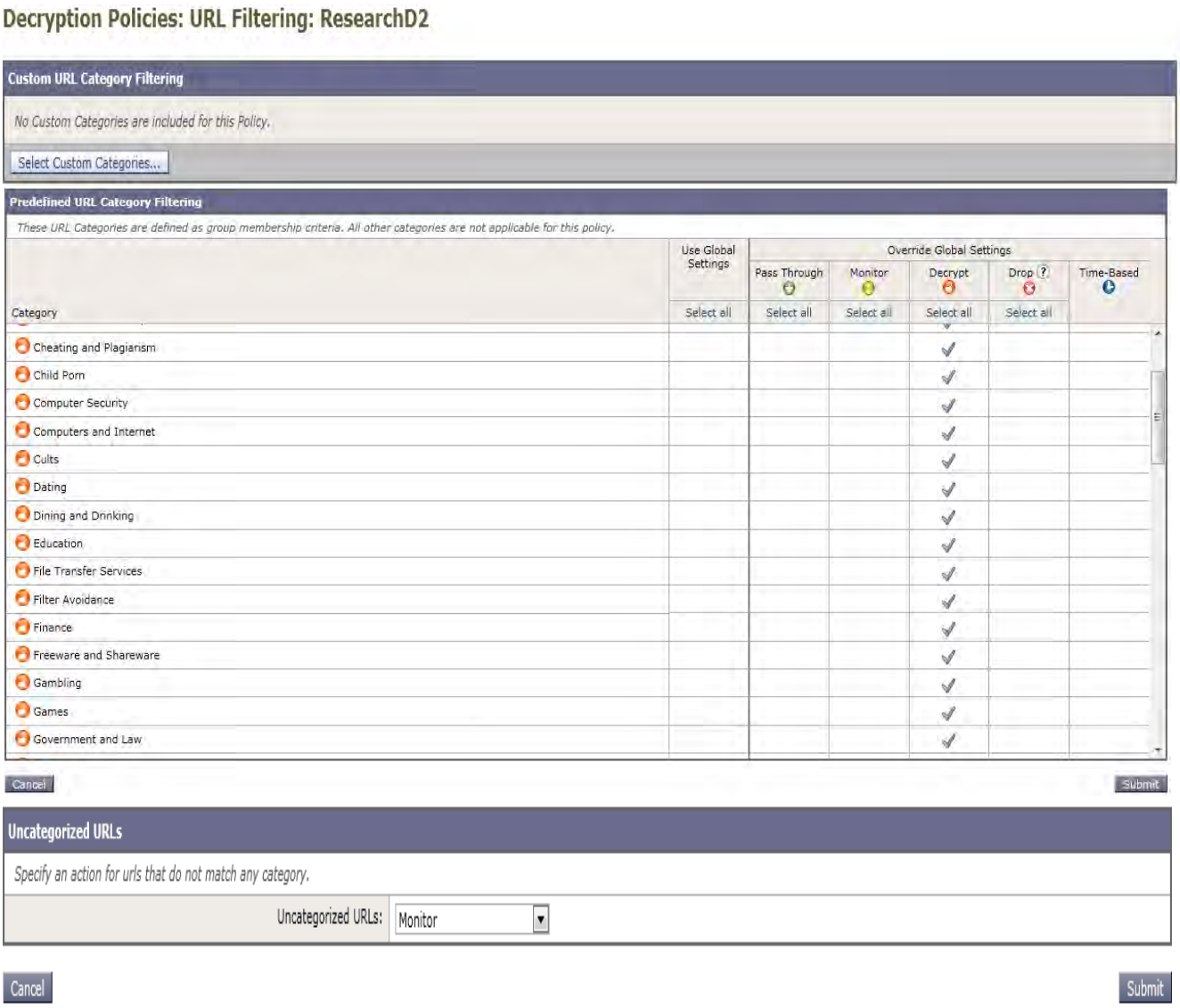
Task-4: Solutions

Step 1: Configure a new HTTPS decryption policy based on subnets (192.168.33.0/24) for research users. Choose all users (Authenticated and Unauthenticated) because 192.168.33.33 is unauthenticated based on a time range from the previous task/Lab.

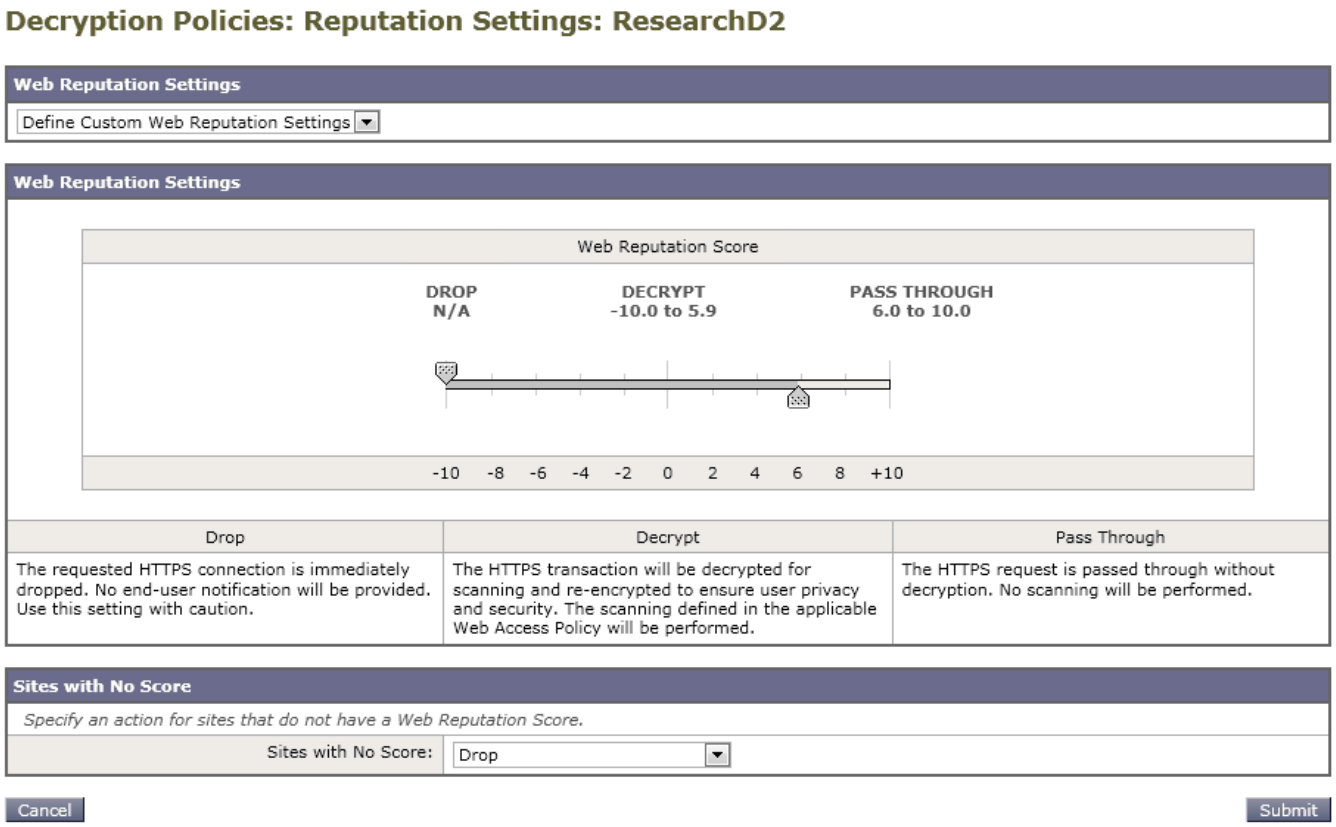
Decryption Policy: Add Group



Step 2: Change the URL categories for decryption to decrypt and monitor for uncategorized URL's



Step 3: Change the WBRS drop threshold to scan all traffic instead of dropping. DO not change the Pass through threshold. Also sites with no WBRS score should be dropped.



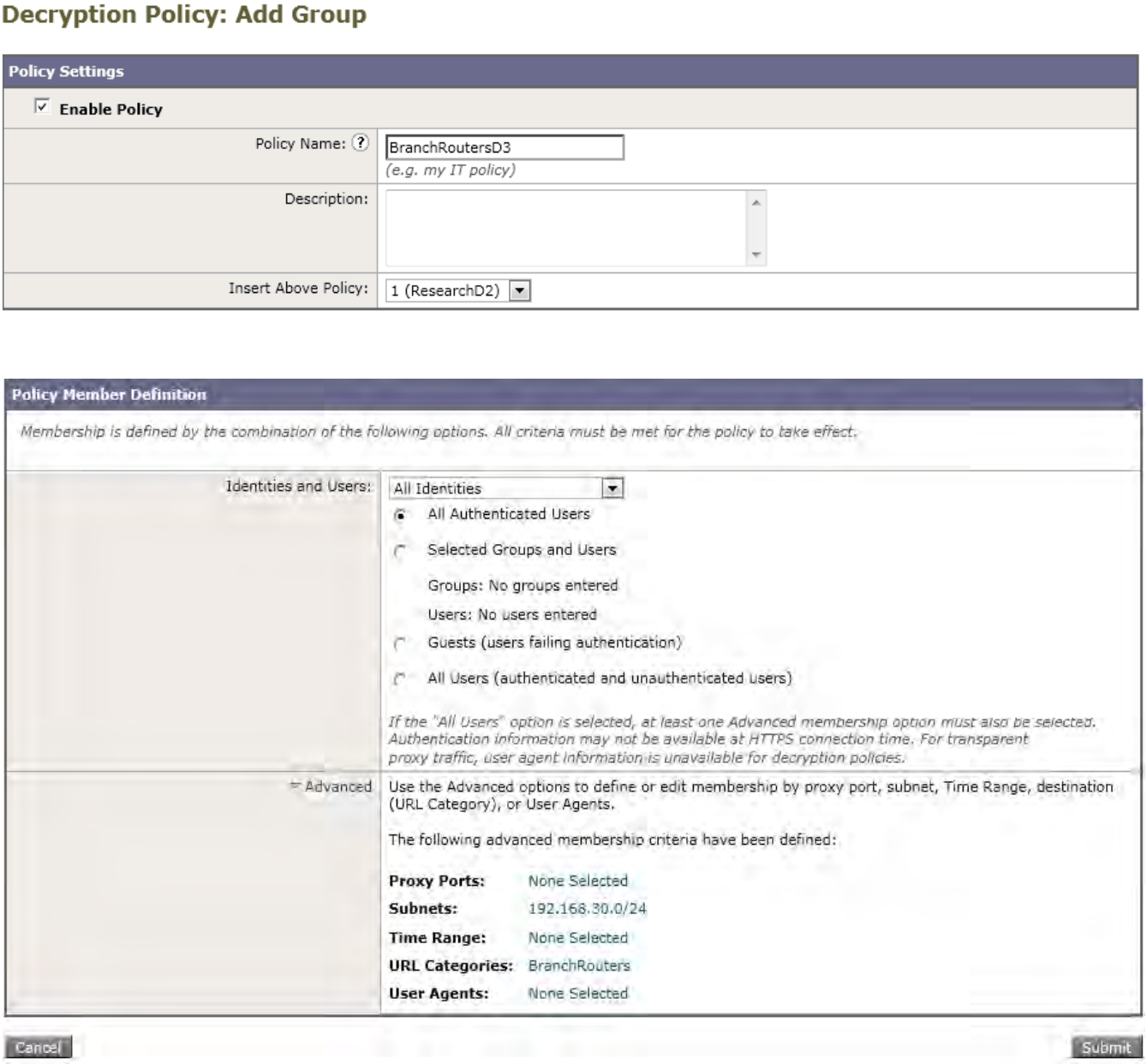
Click on Submit and apply/commit the changes

Task 5: Decryption Policies – 4

- Create a decryption policy to explicitly decrypt HTTPS traffic destined to R4 and R5 for only IT users/Subnet. All requests from others should be dropped.

Task-5: Solutions

Step 1: Create a new decryption policy based on the custom URL and IT subnet.



Step 2: Configure the decryption policy to decrypt traffic for the branch routers from the IT subnet.

Decryption Policies: URL Filtering: BranchRoutersD3

Click on Submit and apply/commit the changes

Decryption Policies

Success — Settings have been saved.

Policies

Add Policy...

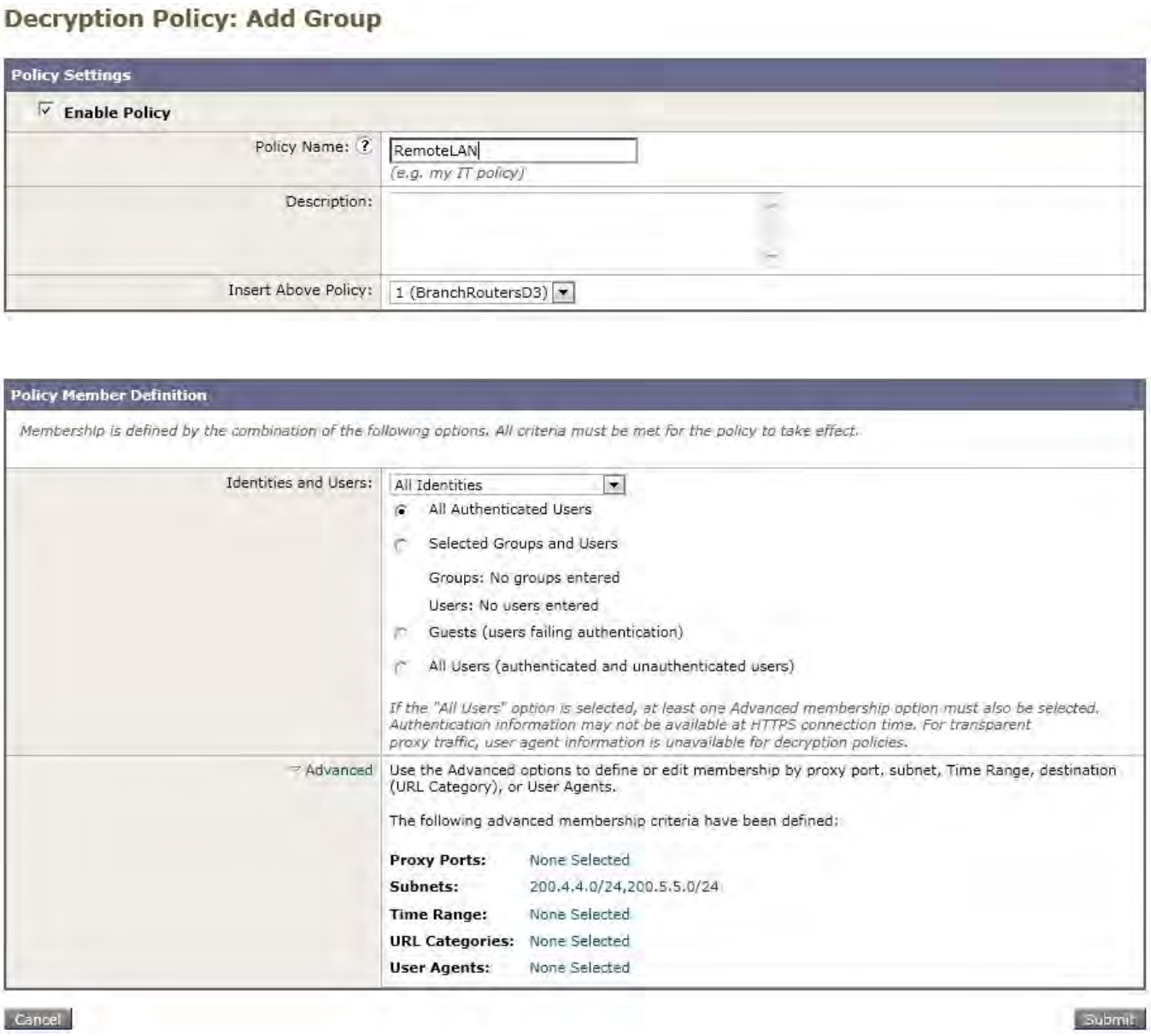
Order	Group	URL Categories	Web Reputation	Default Action	Delete
1	**BranchRoutersD3** Identity: All Subnets: 192.168.30.0/24 URL Categories: BranchRouters	Decrypt: 1	(global policy)	(global policy)	
2	**ResearchD2** Identity: All Subnets: 192.168.33.0/24	Decrypt: 66	Enabled	(global policy)	
3	**WindowsD1** Identity: All URL Categories: WINDOWSC3	Pass Through: 1	(global policy)	(global policy)	
	Global Policy Identity: All	Decrypt: 20 Drop: 46	Enabled	Drop	

Task 6: Decryption Policies – 5

- Drop all HTTPS requests to streaming media sites from the remote office LAN users.

Task-6: Solutions

Step 1: Create a new decryption policy based on the remote LAN subnets.



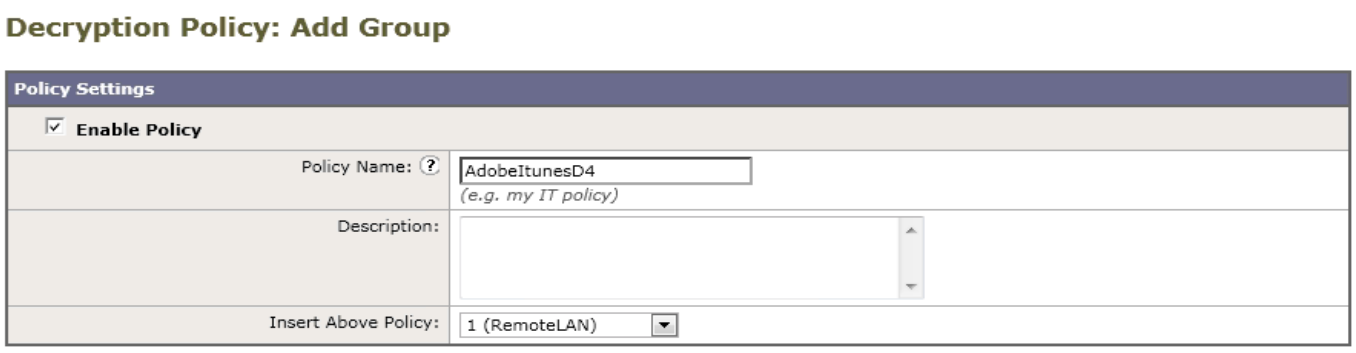
Click on Submit and apply/commit the changes

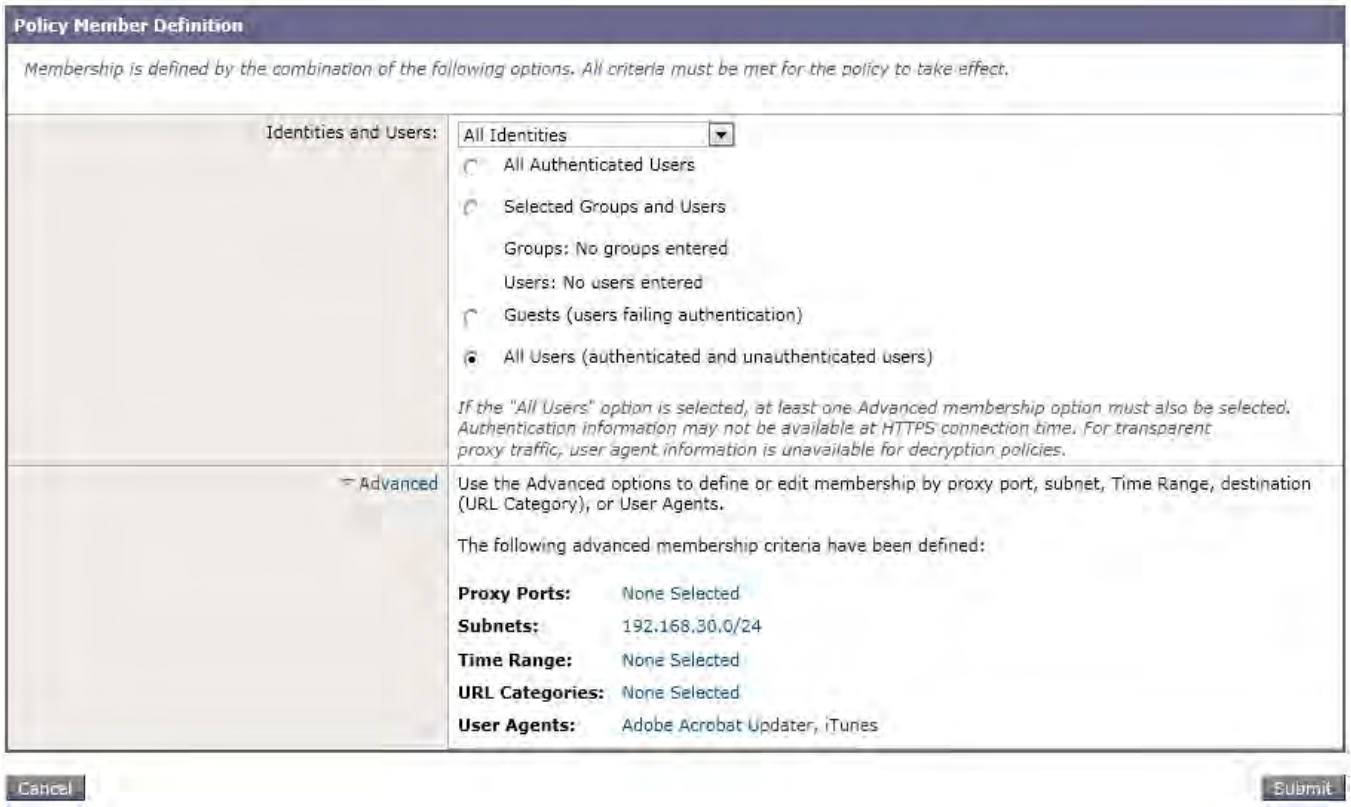
Task 7: Decryption Policies – 6

- All software updates with user agent of iTunes and Adobe Acrobat updater should pass through without decryption. This should apply for the IT subnet only.

Task-7: Solutions

Step 1: Configure a new decryption policy to match IT subnet and iTunes/adobe update user agent. (This only applies for explicit forward mode)





Click on Submit and apply/commit the changes

Decryption Policies

Success — The policy group "AdobeItunesD4" was added.

Policies

Add Policy...

Order	Group	URL Categories	Web Reputation	Default Action	Delete
1	**AdobeItunesD4** Identity: All Subnets: 192.168.30.0/24 User Agents: Others Adobe Acrobat Updater, iTunes	(global policy)	(global policy)	(global policy)	
2	**RemoteLAN** Identity: All Subnets: 200.4.4.0/24, 200.5.5.0/24	(global policy)	(global policy)	(global policy)	
3	**BranchRoutersD3** Identity: All Subnets: 192.168.30.0/24 URL Categories: BranchRouters	Decrypt: 1	(global policy)	(global policy)	
4	**ResearchD2** Identity: All Subnets: 192.168.33.0/24	Decrypt: 66	Enabled	(global policy)	
5	**WindowsD1** Identity: All URL Categories: WINDOWSC3	Pass Through: 1	(global policy)	(global policy)	
	Global Policy Identity: All	Decrypt: 20 Drop: 46	Enabled	Drop	

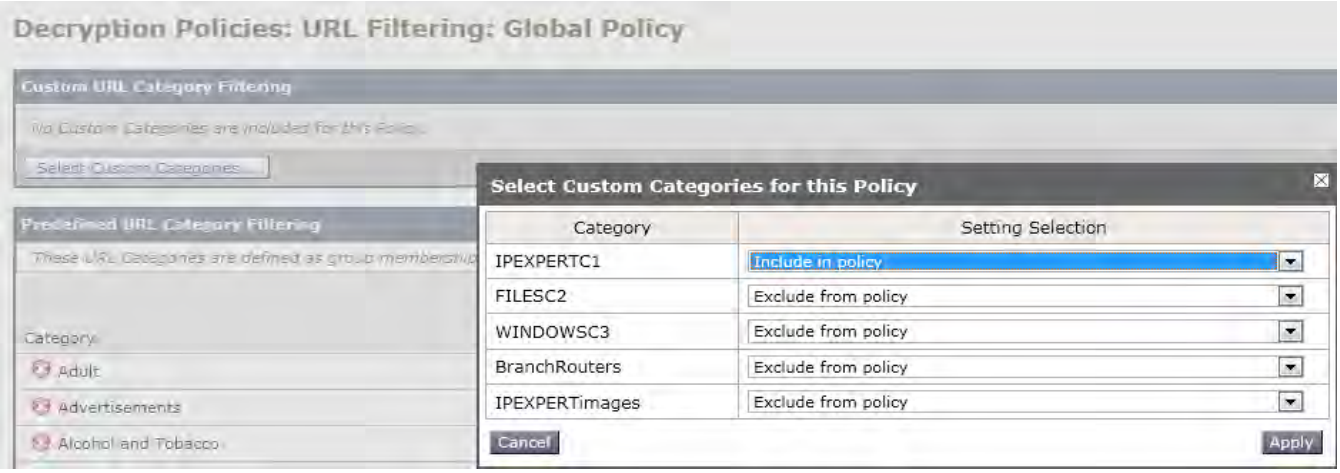
Task 8: Decryption Policies – 7

- Create decryption policies, which allow all users to directly connect to https://www.ipexpert.com without the need for a proxy in the middle.
- Guest users should be allowed access to only to https://www.ipexpert.com subject to other scanning verdicts. Drop all other URL categories for guest users.

Task-8: Solutions

Step 1: Configure the global decryption policy to perform "Pass Through" action for www.ipexpert.com based on predefined URL category.

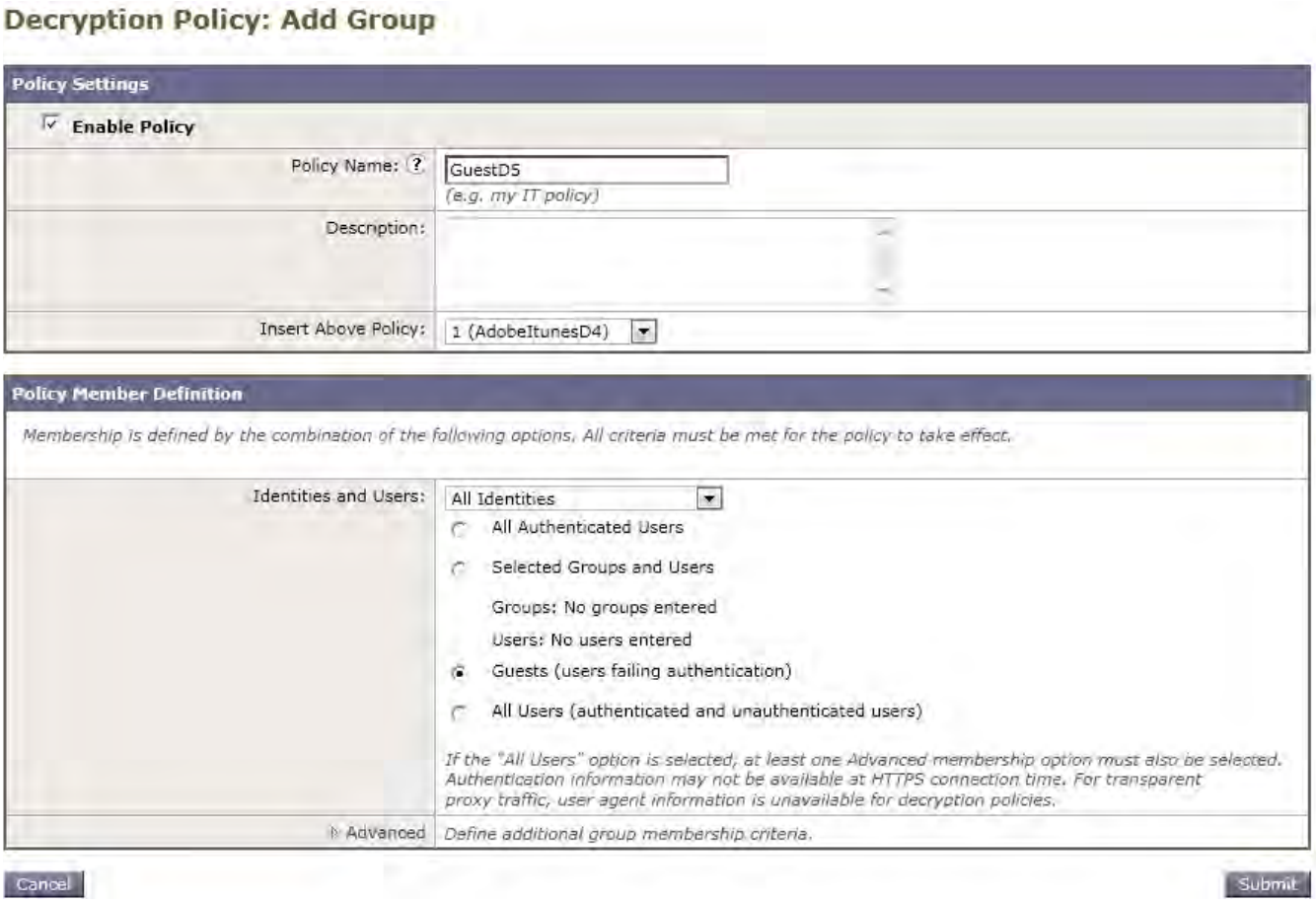
Include the custom URL category in the global decryption policy



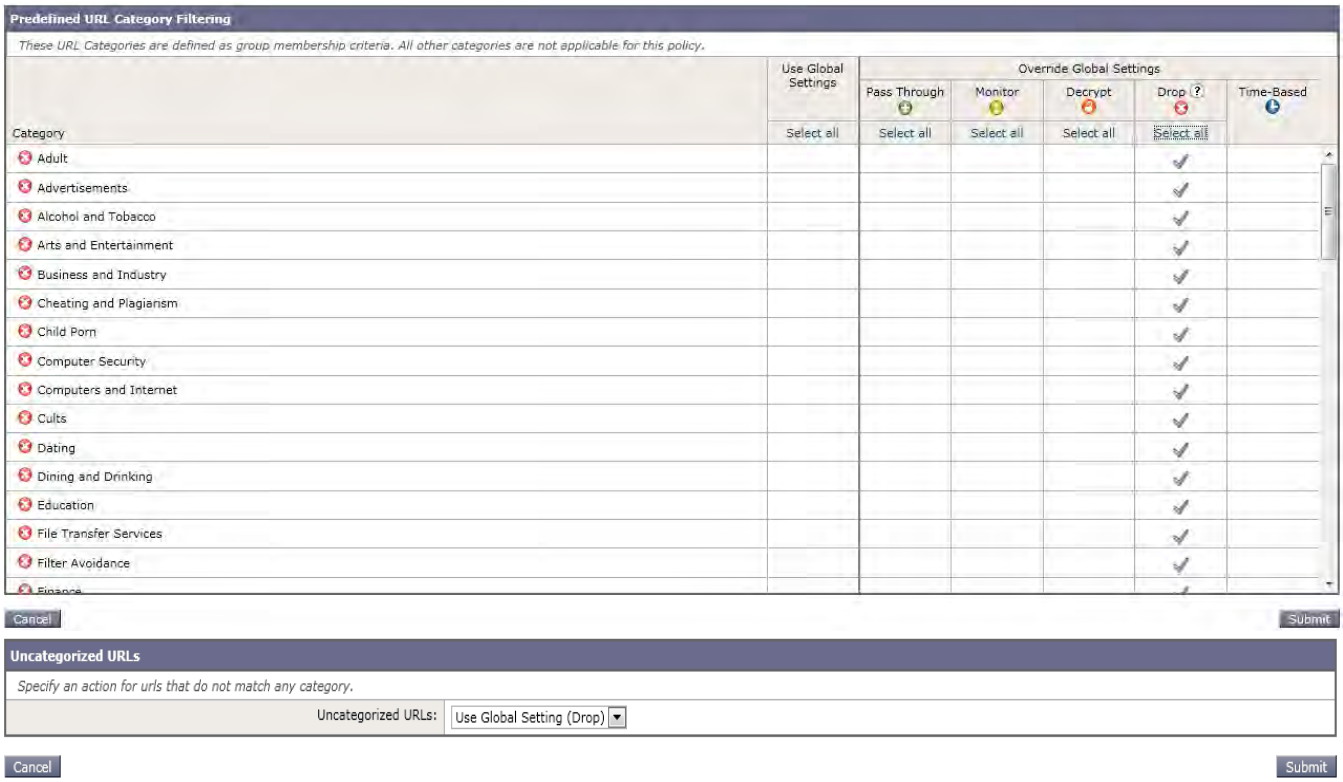
Configure pass through action for this custom URL. Submit and apply/Commit changes.

	Global Policy Identity: All	Pass Through: 1 Decrypt: 20 Drop: 46	Enabled	Drop	

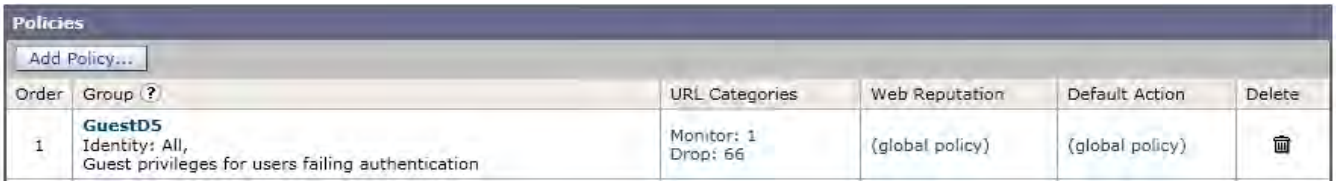
Step 2: Configure a new decryption policy for Guest users.



Step 3: Guest users traffic to www.ipexpert.com based on custom URL category should be set to monitor instead of pass through which is inherited from the global policy. Make sure all other pre-defined URL categories available in the Guest decryption policy are set to block.



Click on Submit and apply/commit the changes



Task 9: Decryption Policies – 8

- WSA should decrypt all traffic for the research subnet. Ensure that they can directly connect to https://www.ipexpert.com

Task-9: Solutions

Step 1: Configure the Custom URL policy for www.ipexpert.com to decrypt.

Decryption Policies: URL Filtering: ResearchD2

Click on Submit and apply/commit the changes

Decryption Policies

Success — Settings have been saved.

Policies

Add Policy...

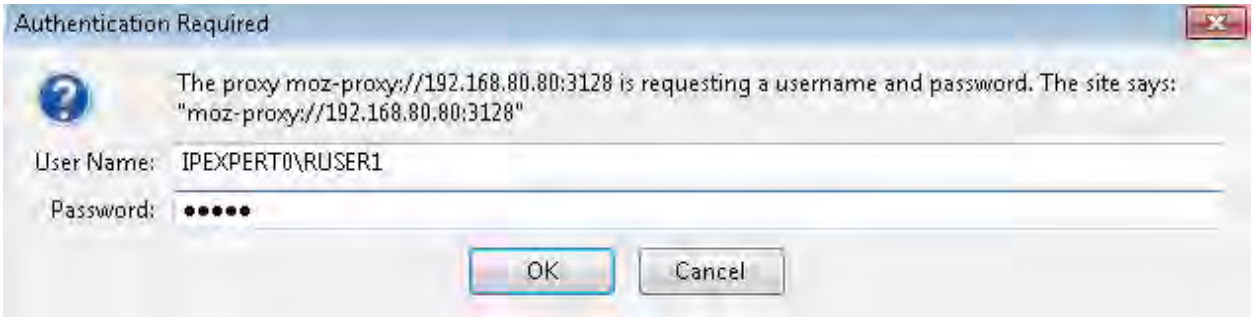
Order	Group	URL Categories	Web Reputation	Default Action	Delete
1	**GuestD5** Identity: All, Guest privileges for users failing authentication	Monitor: 1 Drop: 66	(global policy)	(global policy)	
2	**AdobeItunesD4** Identity: All Subnets: 192.168.30.0/24 User Agents: Others Adobe Acrobat Updater, iTunes	(global policy)	(global policy)	(global policy)	
3	**RemoteLAN** Identity: All Subnets: 200.4.4.0/24, 200.5.5.0/24	(global policy)	(global policy)	(global policy)	
4	**BranchRoutersD3** Identity: All Subnets: 192.168.30.0/24 URL Categories: BranchRouters	Decrypt: 1	(global policy)	(global policy)	
5	**ResearchD2** Identity: All Subnets: 192.168.33.0/24	Monitor: 1 Decrypt: 66	Enabled	(global policy)	
6	**WindowsD1** Identity: All URL Categories: WINDOWSC3	Pass Through: 1	(global policy)	(global policy)	
	Global Policy Identity: All	Pass Through: 1 Decrypt: 20 Drop: 46	Enabled	Drop	

Policy Disabled

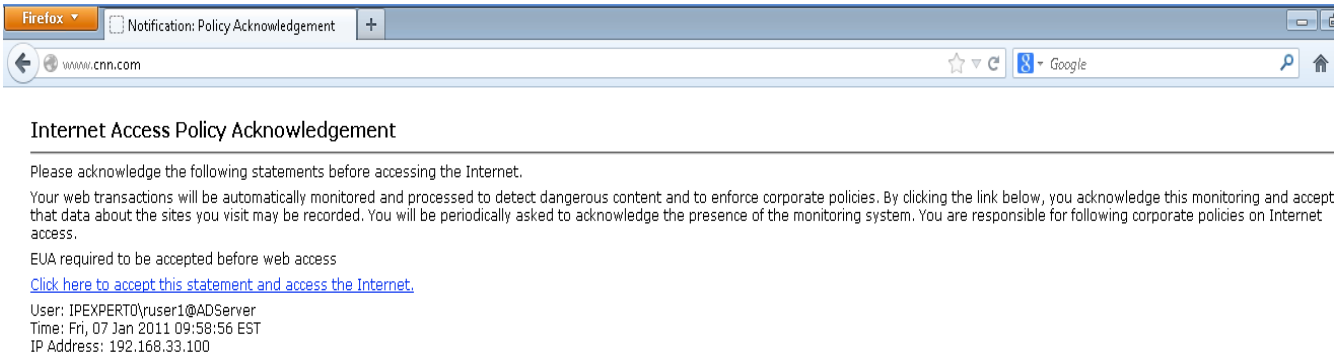
<u>Step 2:</u> Test the decryption policy. The PC is currently placed in the Research VLAN based on the previous task/Lab. Else you may need to configure the switch and TEST PC accordingly.

First browse to any website using http and then browse to https://www.ipexpert.com using Firefox. Clear the browser cache. This is because authentication is used. Until the user is authenticated the traffic cannot be decrypted. Hence we browse to a website using HTTP and establish the authentication surrogate and then web browse using HTTPS.

Enter the User Info

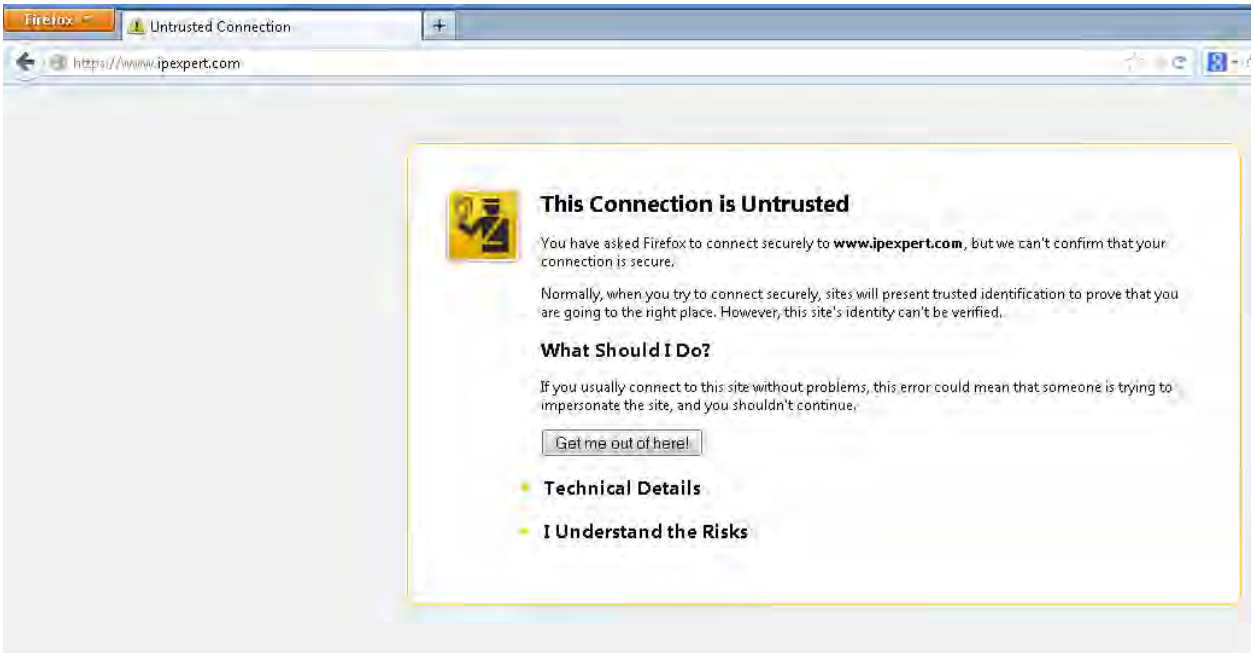


Accept EUA

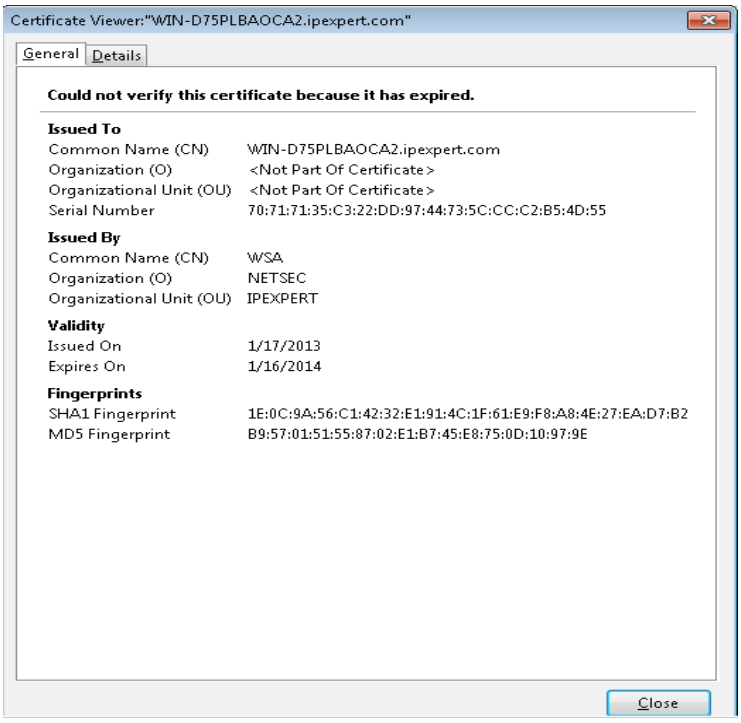


You will connect to CNN based successfully based on the Access Policy

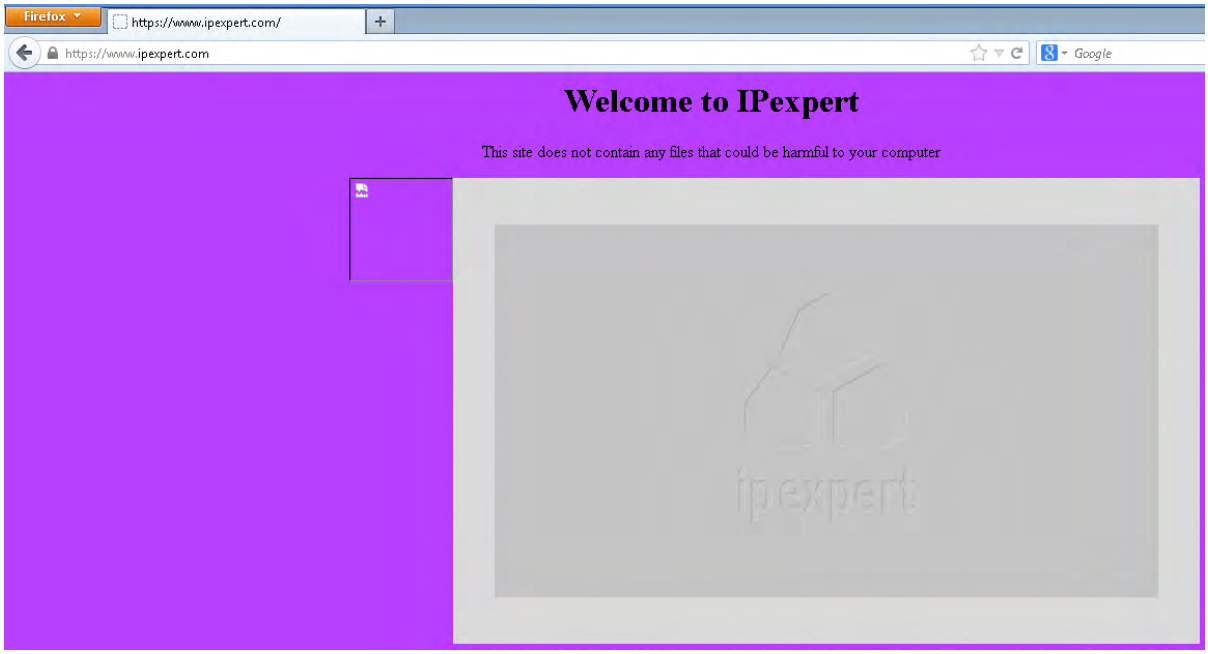
Browse to https://www.ipexpert.com



Confirm the security exception for the certicate



You should be able to successfully connect to ipexpert website



Access Logs

```
1294412468.460    187    192.168.33.100    TCP_MISS_SSL/200    39    CONNECT
tunnel://www.ipexpert.com:443/                    "IPEXPERT0\ruser1@ADServer"
DIRECT/www.ipexpert.com  -  DECRYPT_CUSTOMCAT_7-ResearchD2-DefaultGroup-NONE-
NONE-NONE-DefaultGroup  <C_IPEX,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-
",-,-,-,-,"-","-","-","-","-","-",1.67,0,-,"-","-">                        -
```

Lab-4: Configuring advanced access policies for downloads

Lab-4: Configuring advanced access policies– This lab is intended to familiarize you with configuring access policies with protocol & object download rules, AVS and DVS-Virus/Malware scanning for downloads.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 1.5 Hour

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-3 successfully.
Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Detailed Solution: Lab-4

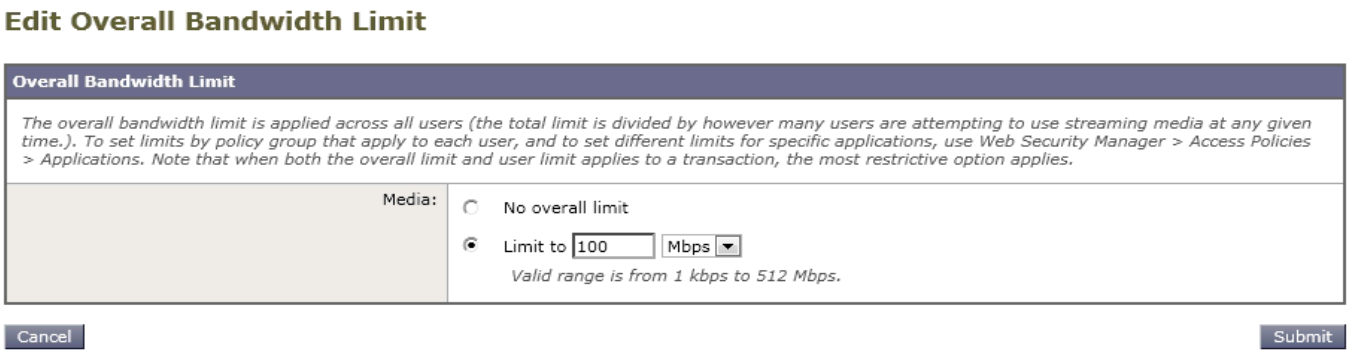
Task 1: Configure download bandwidth limits and object download blocking

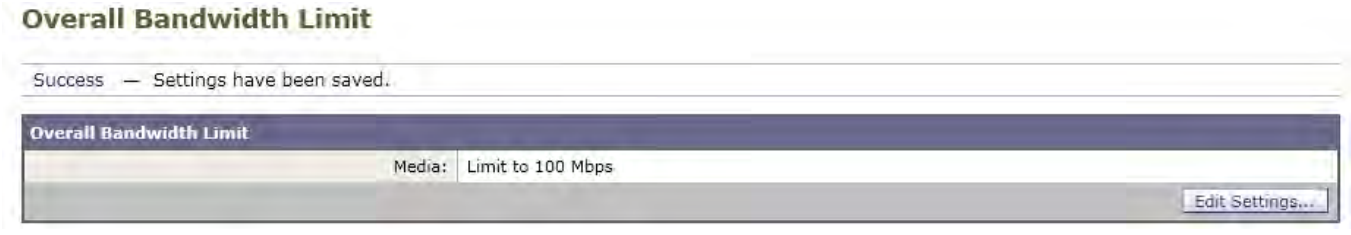
- Globally configure an overall download limit to 100 Mbps.
- Each group should be allowed a maximum download limit for HTTP/HTTPS to 20 MB and 5 MB for FTP. Configure this in the Global Policy.
- IT group should be allocated 50 MB download limit for HTTP/HTTPS and FTP.
- Research subnet user traffic and MS update traffic is should not be subject to any download limits
- Configure the global policy to block downloads of any archives, windows EXE files, audio, video and bit torrent links/files.
- Disable object blocking for MS update traffic, IT subnet users and Research subnet users.

Task-1: Solutions

Step 1: Configure an overall global download limit to 100 Mbps. Submit and commit the changes.

Web Security Manager -> Overall Bandwidth Limits -> Edit Settings





Step 2: Configure the global Access Policy to set the bandwidth limits for web and FTP traffic as per task. (Object Blocking)

Access Policies: Objects: Global Policy

Edit Objects Blocking Settings

Define Custom Objects Blocking Settings

Objects Blocking Settings

Object Size

HTTP/HTTPS Max Download Size:	20 MB / No Maximum
FTP Max Download Size:	5 MB / No Maximum

Submit and apply changes

	Global Policy Identity: All	Block: 2 Protocols	Block: 59 Monitor: 9 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 18	No blocked items HTTP/S Max Size: 20 MB FTP Max Size: 5 MB	Web Reputation: Enabled	

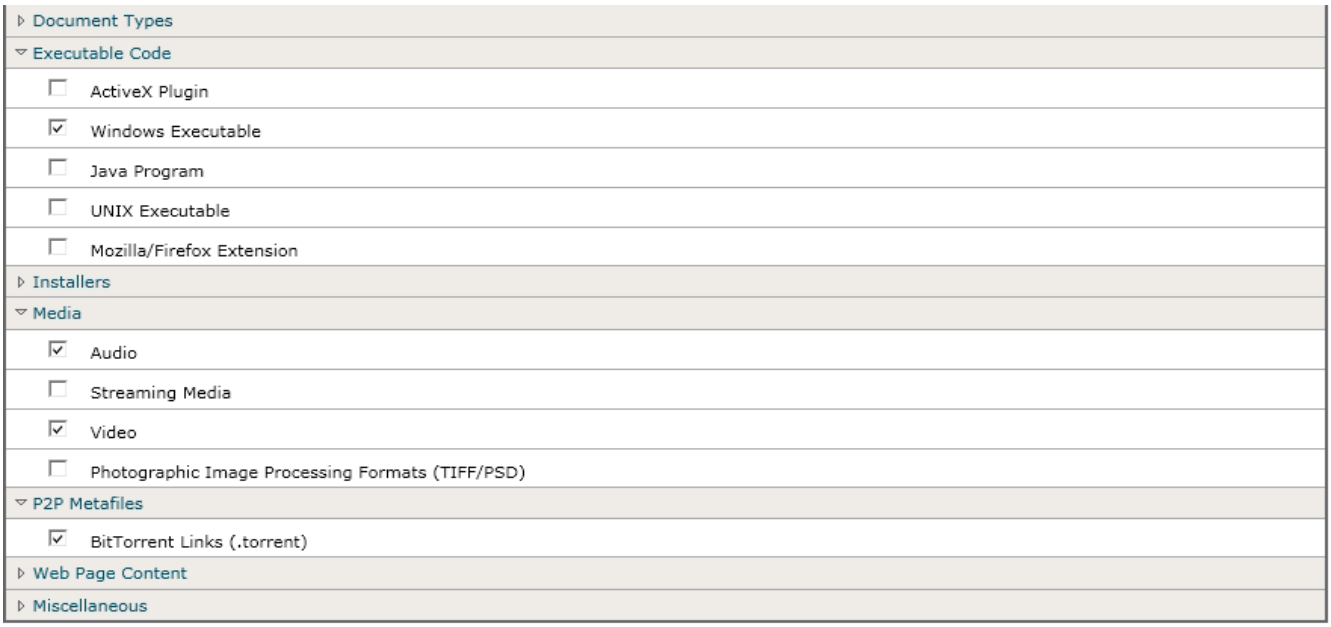
Step 2: Configure the global policy to block downloads of any archives, windows EXE files, audio, video and bit torrent links/files.

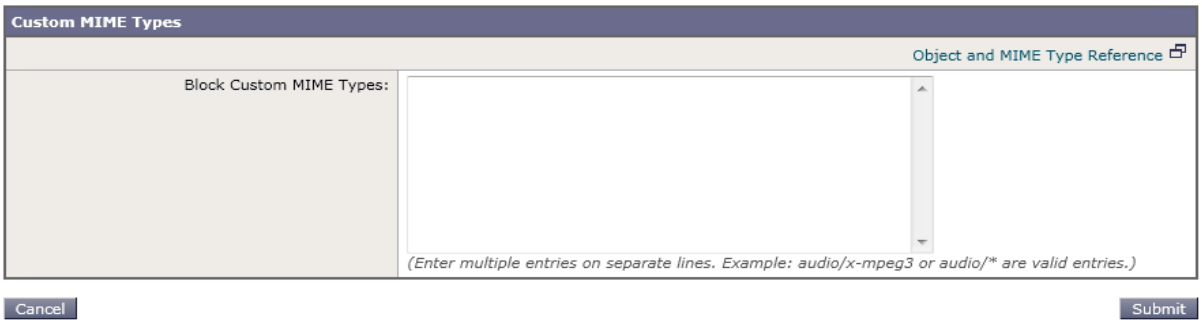
Block Object Type

Object and MIME Type Reference

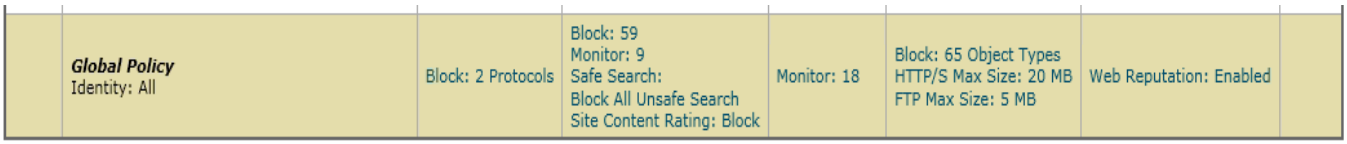
Archives

- [x] ARC
- [x] ARJ
- [x] BinHex
- [x] BZIP2
- [x] CPIO
- [x] GZIP
- [x] LHA
- [x] LHARC
- [x] Microsoft CAB
- [x] RAR
- [x] StuffIt
- [x] TAR
- [x] Compress Archive (Z)
- [x] ZIP Archive

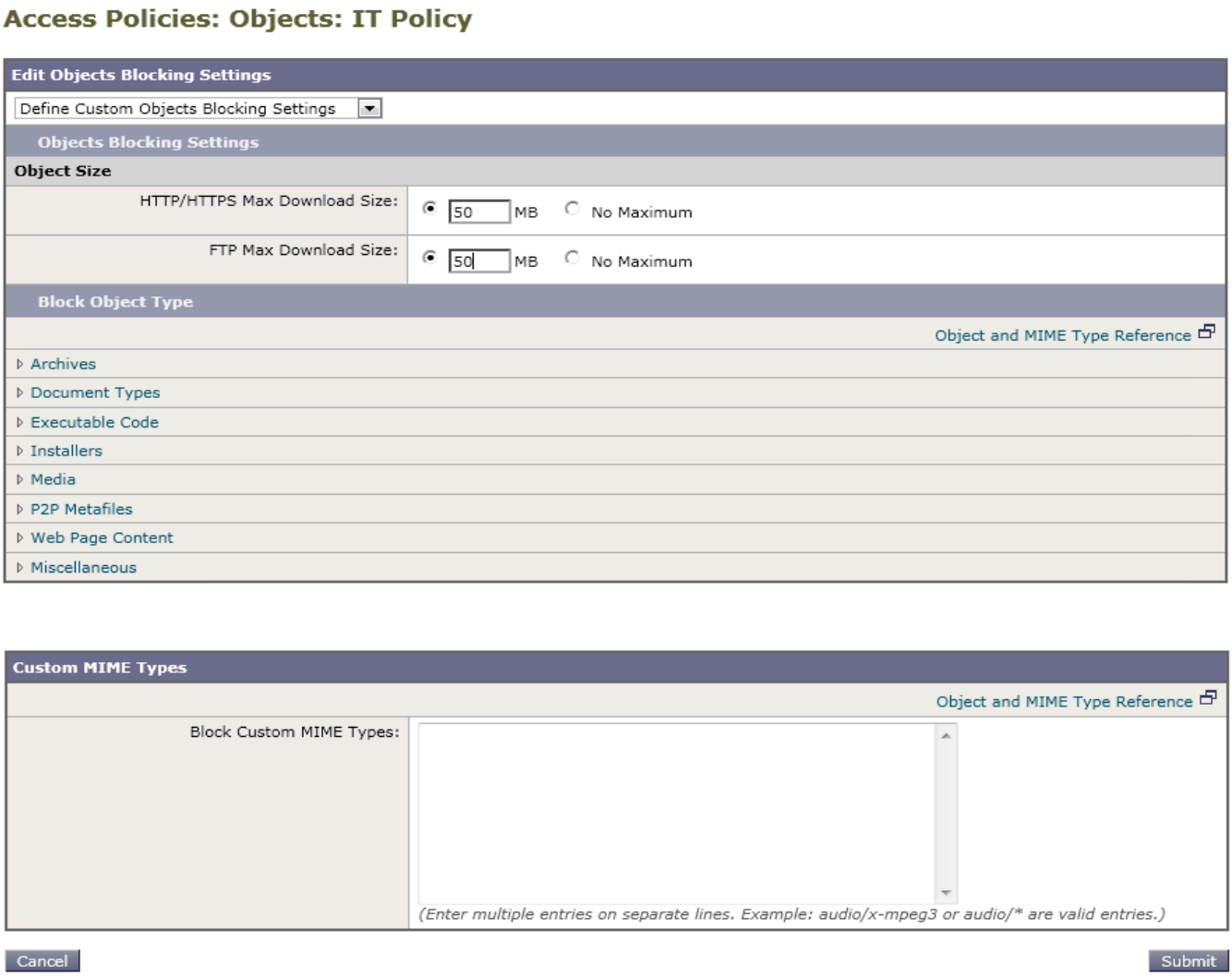




Click on Submit and apply/commit the changes



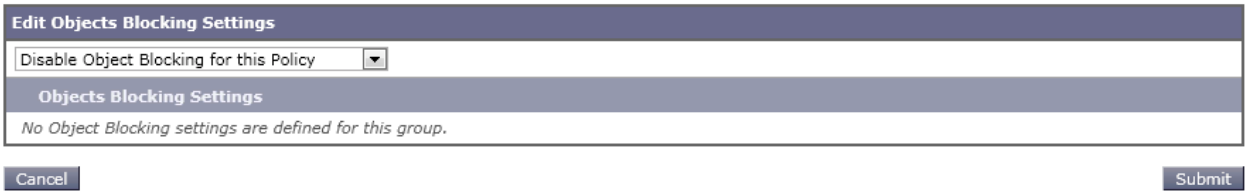
Step 3: Configure IT access policy to rate limit to 50 MB download for HTTP/HTTPS and FTP. Do not block any objects for IT access policy. Submit and apply the changes



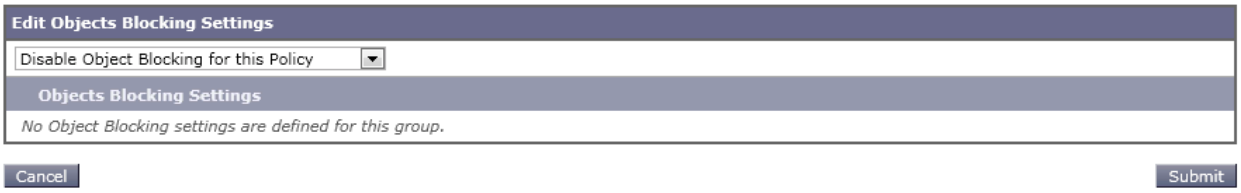
Click on Submit and apply/commit the changes

Step 4: Disable object blocking for MS update traffic and research subnet traffic

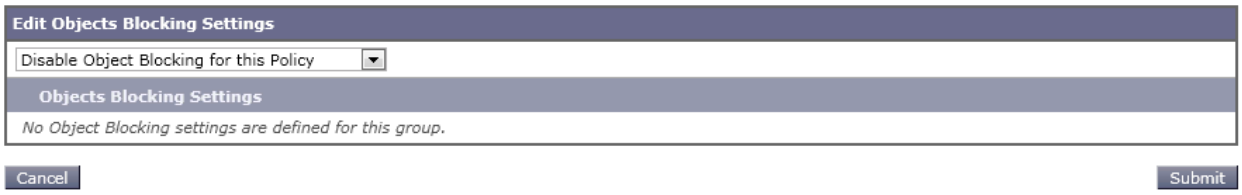
Access Policies: Objects: Windows update traffic policy



Access Policies: Objects: Research NoAuth AP



Access Policies: Objects: Research



Click on Submit and apply/commit the changes

Access Policies

Success — Settings have been saved.

Policies

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	**Windows update traffic policy** Identity: All Subnets: 192.168.30.0/24 URL Categories: WINDOWSC3	(global policy)	Allow: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(disabled)	(global policy)	
2	**Research NoAuth AP** Identity: All Subnets: 192.168.33.33	No blocked items	Monitor: 67 Redirect: 1	(global policy)	(disabled)	(global policy)	
3	**Research** Identity: All Subnets: 192.168.33.0/24	No blocked items	Monitor: 67 Redirect: 1	(global policy)	(disabled)	(global policy)	

Task 2: Configure Application visibility and control for web traffic

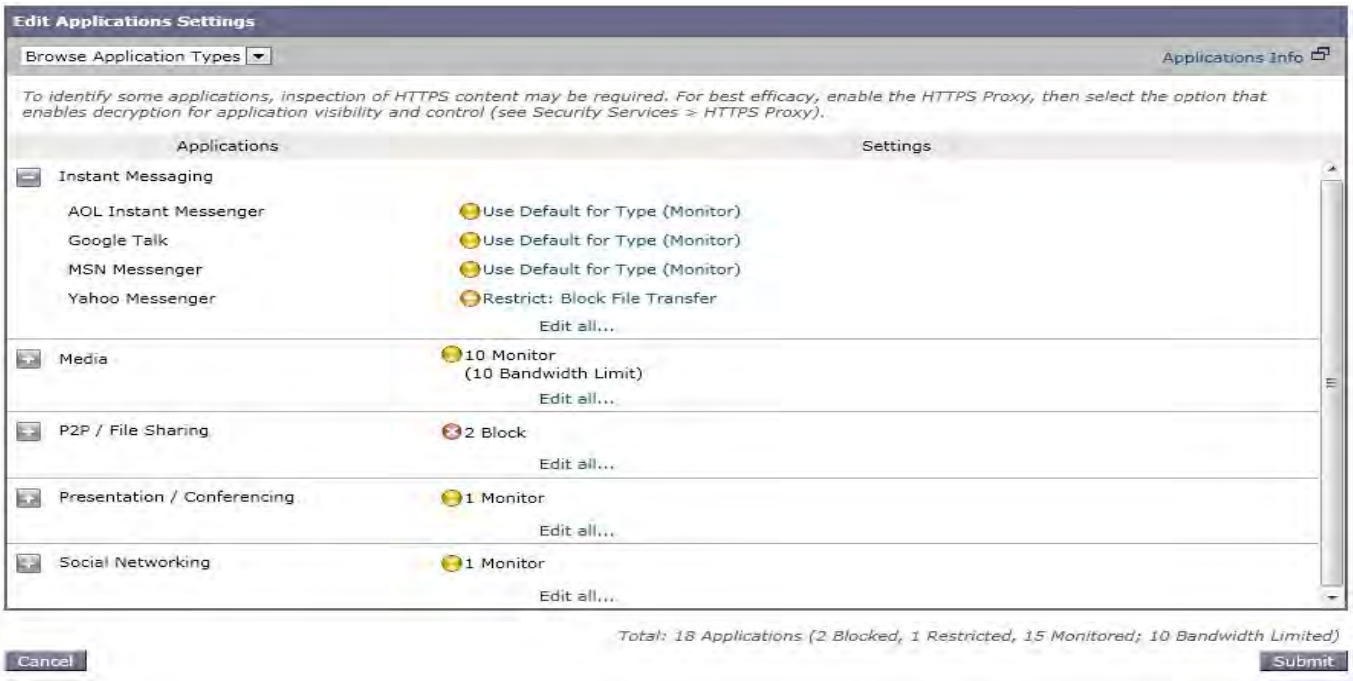
- Configure the global policy to block P2P file sharing and block files sent through IM chat, which uses web browsers.
- Globally configure media bandwidth limits per user to 512 Kbps
- 192.168.33.33 should not be subject to the above policies.

Task-2: Solutions

Step 1: Configure the global access policy (Applications) to block P2P file sharing and block files sent through IM chat, which uses web browsers. Additionally, configure media bandwidth limits per user to 512 Kbps.

Access Policies: Applications Visibility and Control: Global Policy

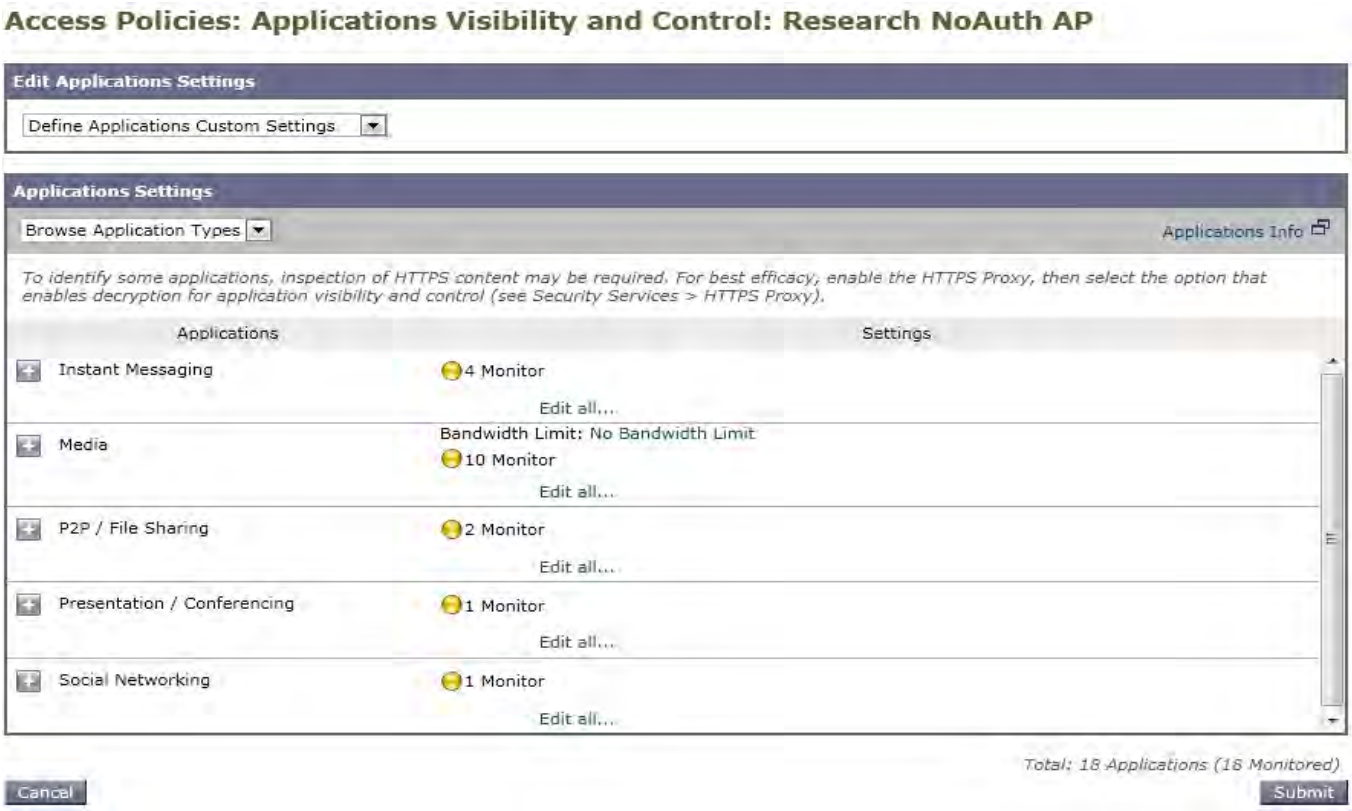
Default Actions for Application Types	
Application Types	Default Action for Type
Instant Messaging	Monitor
Media	Monitor Bandwidth Limit: 512 kbps
P2P / File Sharing	Block
Presentation / Conferencing	Monitor
Social Networking	Monitor



Click on Submit and apply/commit the changes

	Global Policy Identity: All	Block: 2 Protocols	Block: 59 Monitor: 9 Safe Search: Block All Unsafe Search Site Content Rating: Block	Block: 2 Restrict: 1 Monitor: 15 (Bandwidth Limit: 10)	Block: 65 Object Types HTTP/S Max Size: 20 MB FTP Max Size: 5 MB	Web Reputation: Enabled	

Step 2: Configure the Research User Access policy for 192.168.33.33 to disable AVC.



Click on Submit and apply/commit the changes

2	**Research NoAuth AP** Identity: All Subnets: 192.168.33.33	No blocked items	Monitor: 67 Redirect: 1	Monitor: 18	(disabled)	(global policy)	

Lab-5: Configuring data transfer policies.

Lab-5: Configuring DLP's and outbound malware scanning– This lab is intended to familiarize you with configuring outbound data transfer policies/DLP's and outbound malware scanning.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 1 Hour

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-4 successfully.
Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure data transfer policies

- Configure the global policy to block uploads of any Archives, Windows and UNIX executable files, Installers, Audio, Video and bit torrent links.
- Globally block all uploads of documents types except PDF/MS office files below 5 MB size and XML below 2 MB.
- Maximum upload limit for HTTP/HTTPS and FTP should be 5 Mbps globally.
- Research and IT subnet users should not be subject to the above upload blocking policies. Create a new policy to accomplish this.
- WBRS blocking threshold for IT and research users should be between -10 to -5.

Detailed Solution: Lab-5

Task-1: Solutions

Step 1: Globally configure the upload limit for HTTP/HTTPS and FTP to 5 Mbps

Web Security Manager -> Ironport Data Security (Content)

Submit and commit the changes

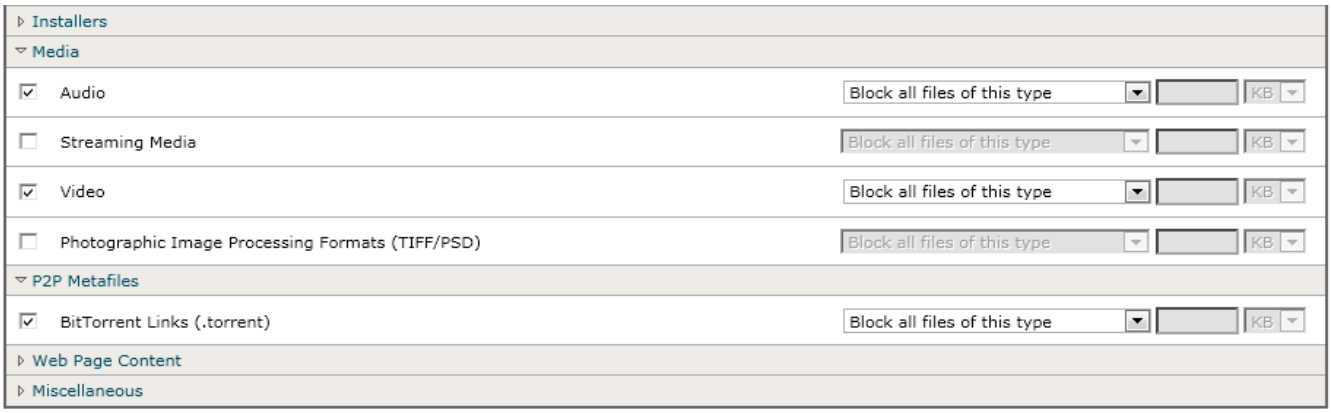
Step 2: Configure the global Ironport data transfer policy to block transfer of certain files as per the task

Web Security Manager -> Ironport Data Security (Content)

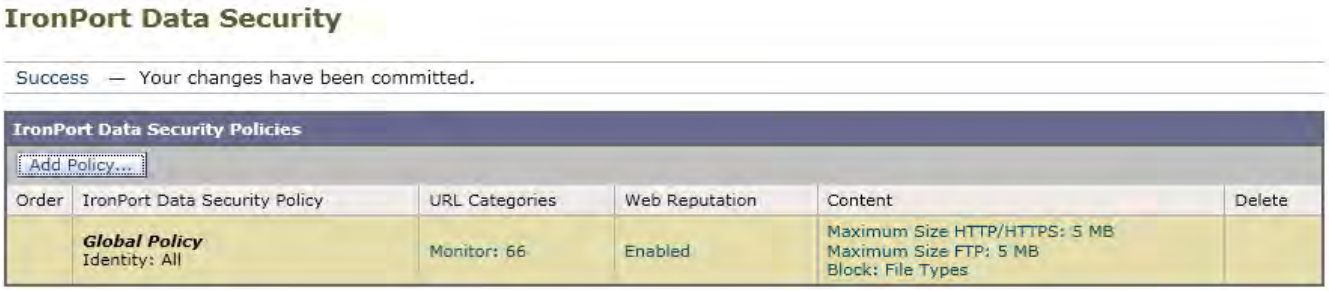
Block File Types

File and MIME Type Reference

Archives		
ARC	Block all files of this type	KB
ARJ	Block all files of this type	KB
BinHex	Block all files of this type	KB
BZIP2	Block all files of this type	KB
CPIO	Block all files of this type	KB
GZIP	Block all files of this type	KB
LHA	Block all files of this type	KB
LHARC	Block all files of this type	KB
Microsoft CAB	Block all files of this type	KB
RAR	Block all files of this type	KB
StuffIt	Block all files of this type	KB
TAR	Block all files of this type	KB
Compress Archive (Z)	Block all files of this type	KB
ZIP Archive	Block all files of this type	KB
Document Types		
Microsoft Office	Block file of this type if over size: 5	MB
FrameMaker Document (FM)	Block all files of this type	KB
Portable Document Format (PDF)	Block file of this type if over size: 5	MB
PostScript Document (PS)	Block all files of this type	KB
Rich Text Format (RTF)	Block all files of this type	KB
XML Document (XML)	Block all files of this type	KB
Executable Code		
ActiveX Plugin	Block all files of this type	KB
Windows Executable	Block all files of this type	KB
Java Program	Block all files of this type	KB
UNIX Executable	Block all files of this type	KB
Mozilla/Firefox Extension	Block all files of this type	KB



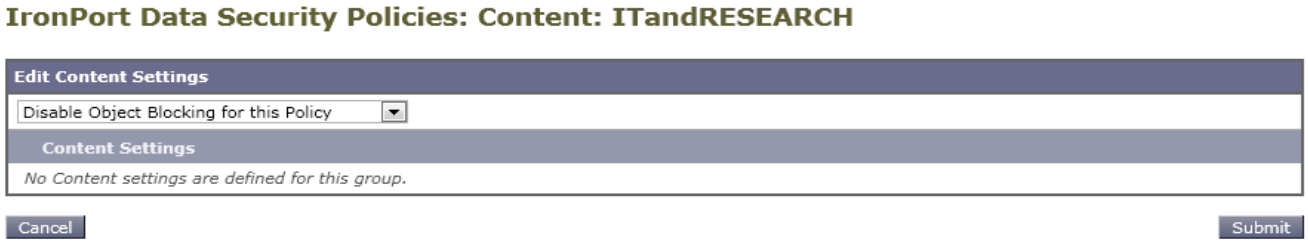
Submit and commit the changes



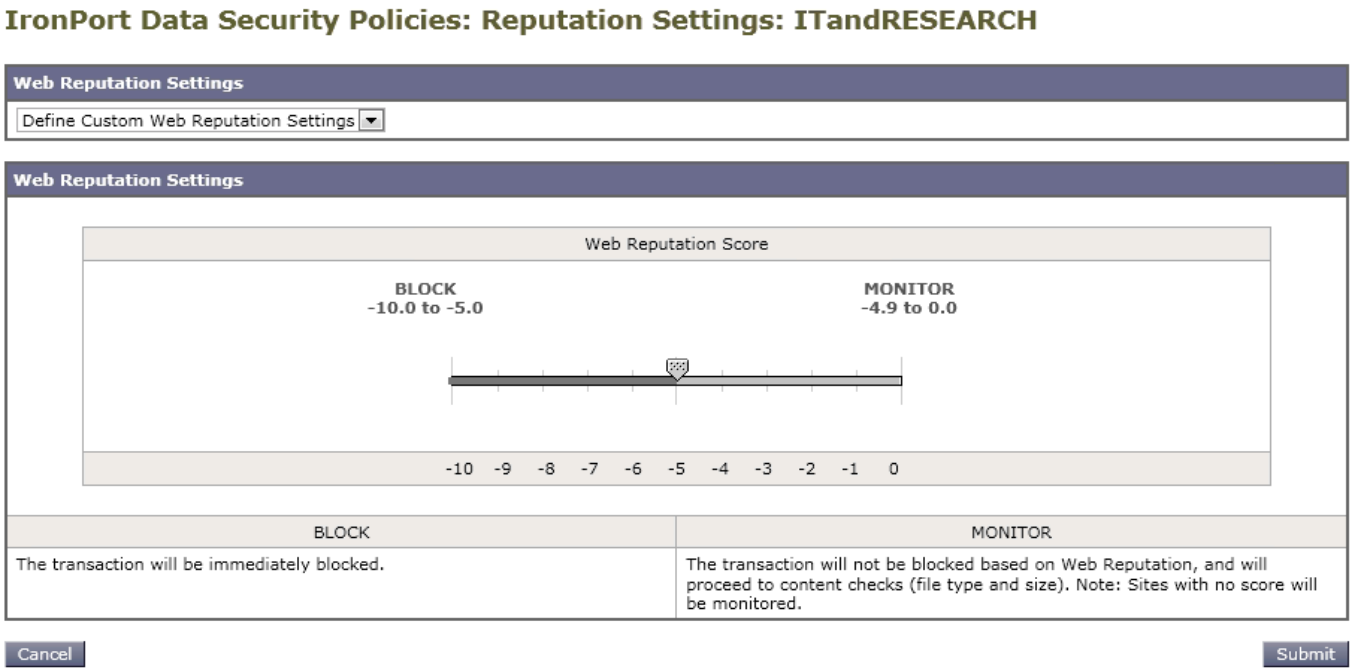
Step 3: Configure a new policy for the research and IT subnets and this policy should allow transfer of all outbound data transfers using HTTP/HTTPS/FTP.

Submit and commit the changes

Disable object blocking for this policy



Step 4: Configure the WBRS blocking threshold as per task for the IT and research subnet for outbound data transfer.



Submit and commit the changes

Lab-6: Configuring WCCP and transparent proxy mode with Single Sign On.

Lab-6: Configuring WCCP and transparent mode– This lab is intended to familiarize you with configuring WSA for transparent mode using WCCP on the ASA. It also focuses on proxy bypass feature and Single Sign on.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 1 Hour

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-5 successfully.
Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Detailed Solution: Lab-6

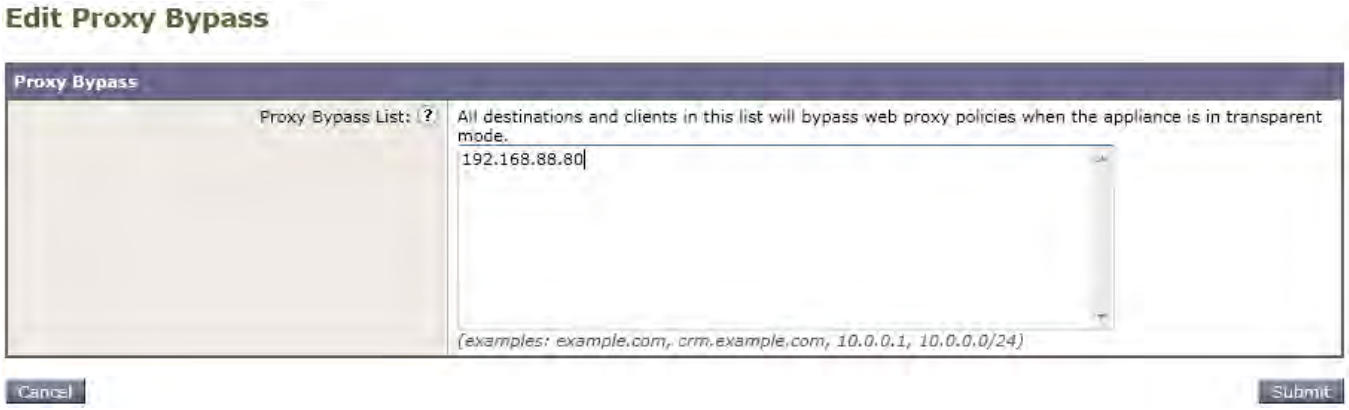
Task 1: Configure transparent proxy bypass

- Configure transparent proxy bypass for 192.168.88.80 and cisco WebEx traffic.

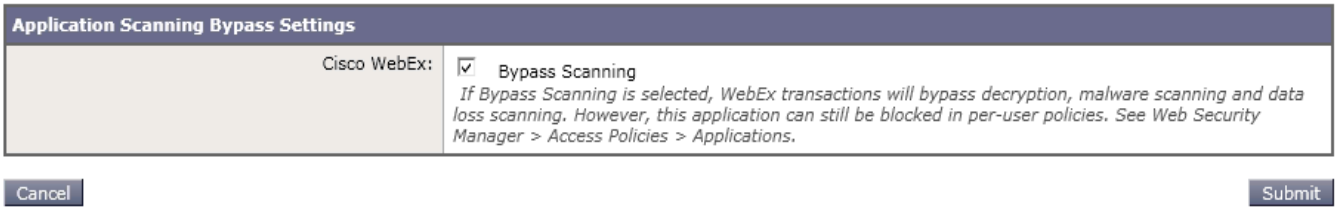
Task-1: Solutions

Step 1: Configure transparent proxy bypass for 192.168.88.80 and application bypass for cisco WebEx traffic.

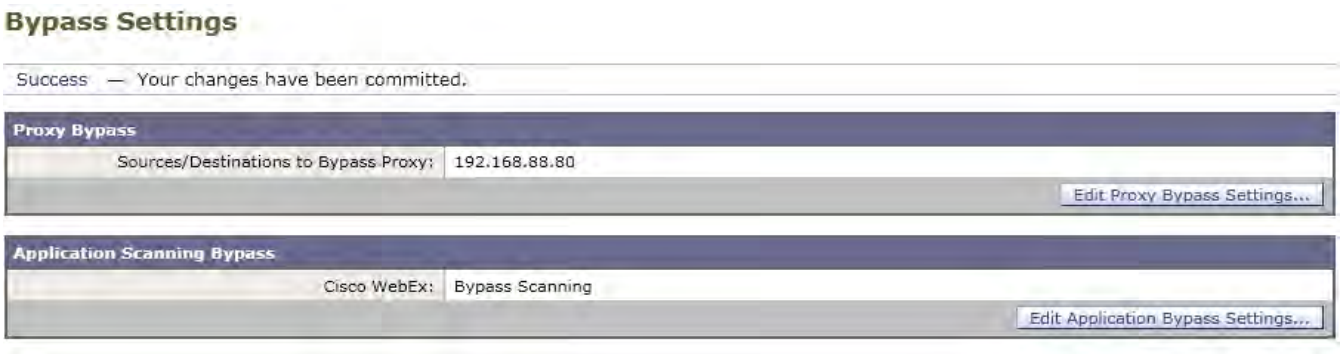
Web Security Manager -> Bypass Settings -> Edit Proxy Bypass Settings



Web Security Manager -> Bypass Settings -> Edit Application Bypass Settings



Submit and commit the changes



Task 2: Configure transparent proxy bypass

- Configure WCCPv2 using dynamic service ID of 90 for HTTP/HTTPS traffic (TCP-80 and 443) on the ASA. The ASA should redirect traffic all HTTP/HTTPS traffic arriving on the inside interface to the WSA. Use password of "C1SC0"
- Configure WSA accordingly for transparent redirection using WCCPv2
- Test from the internal LAN.

Task-2: Solutions

Step 1: Configure WCCP on ASA3

ASA3

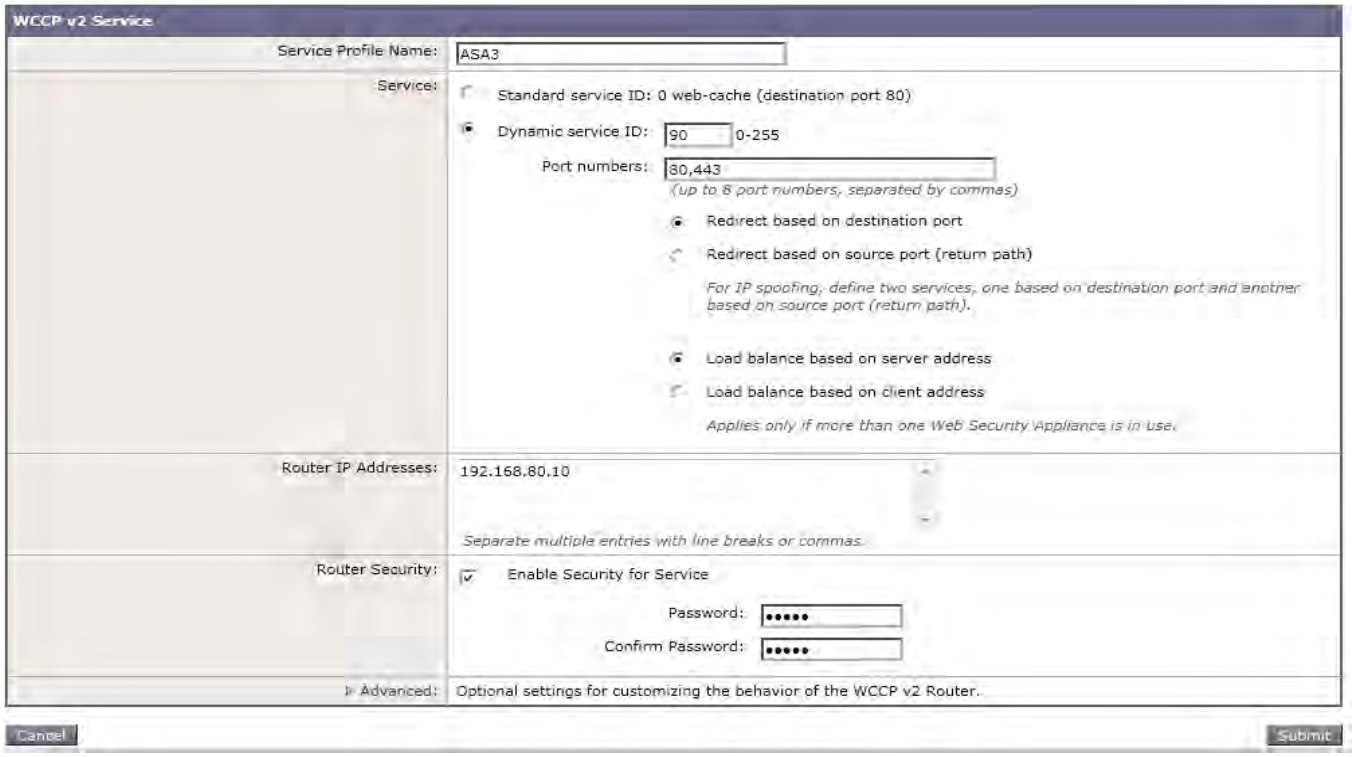
```
access-list clients extended permit ip 192.168.0.0 255.255.0.0 any
access-list wsa extended permit ip host 192.168.80.80 any
wccp 90 redirect-list clients group-list wsa password 1PEXPERT
wccp interface inside 90 redirect in
```

Step 2: Configure WCCP on WSA

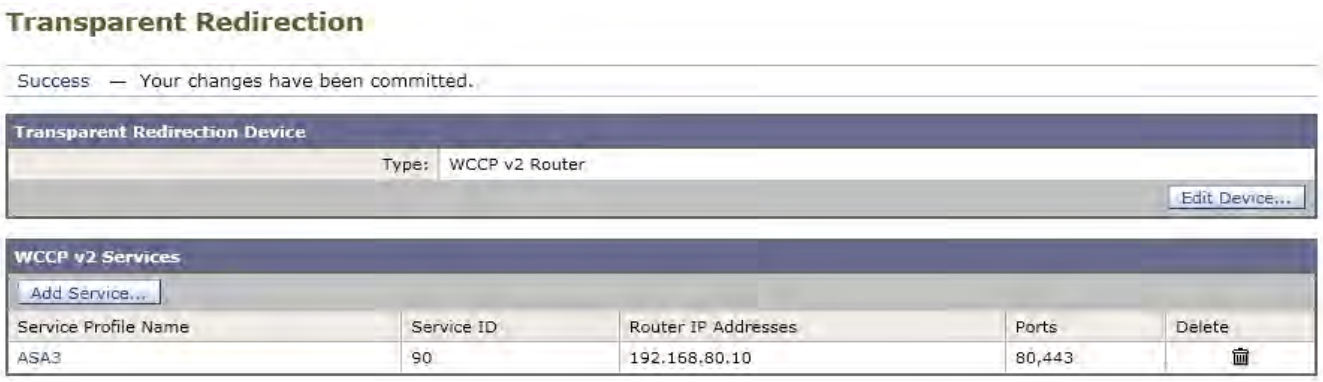
WSA

Network -> Transparent Redirection -> Edit Device

Network -> Transparent Redirection -> Add Service



Submit and commit the changes

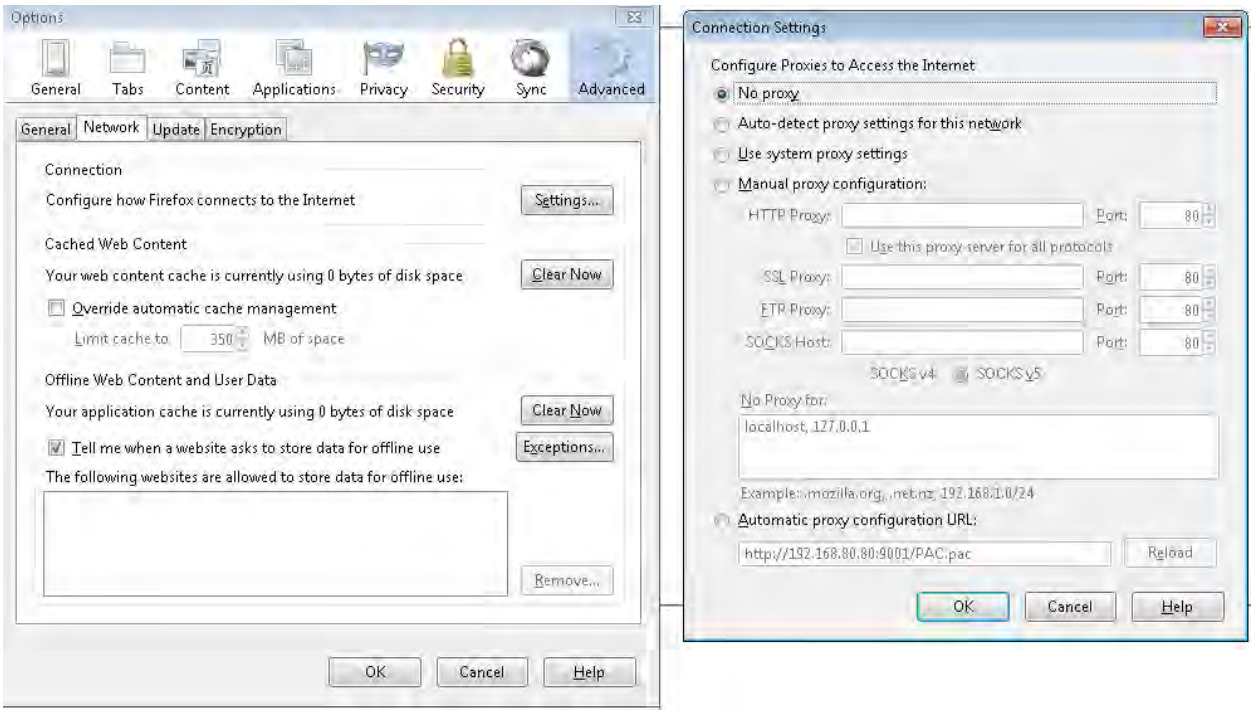


Verify on ASA3

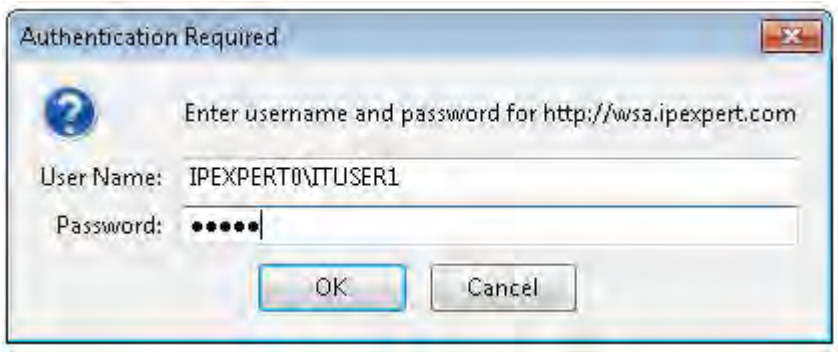
```
asa3(config)# sh wccp

Global WCCP information:
    Router information:
        Router Identifier:                  192.168.88.10
        Protocol Version:                   2.0

    Service Identifier: 90
```

```
Number of Cache Engines:              1
Number of routers:                    1
Total Packets Redirected:             0
Redirect access-list:                 clients
Total Connections Denied Redirect:    0
Total Packets Unassigned:             0
Group access-list:                    wsa
Total Messages Denied to Group:       0
Total Authentication failures:        0
Total Bypassed Packets Received:      0
```

Step 3: Test from TEST PC, remove the proxy configuration and browse to www.facebook.com



Enter the user credentials



Accept the EUA

You should be presented with a block page

Browse to Cisco.com and you should be able to successfully connect

Access Logs

```
1294752511.128      1      192.168.30.100      TCP_DENIED/403      2651      GET
http://www.facebook.com/      "IPEXPERT0\ituser1@ADServer"      NONE/-      -
BLOCK_WEBCAT_11-IT_Policy-DefaultGroup-NONE-NONE-NONE-NONE
<IW_snet,7.0,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_snet,-,"-
","-","Facebook","Social Networking","-","-",21208.00,0,-,"-","-"> -

1294752605.641     47     192.168.30.100     TCP_REFRESH_HIT/200     391     GET
http://www.cisco.com/     "IPEXPERT0\ituser1@ADServer"     DIRECT/www.cisco.com
text/html     ALLOW_WBRS_11-IT_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_comp,6.5,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_comp,-,"-
","-","Unknown","Unknown","-","-",66.55,0,-,"-","-"> -
```

ASA3

```
asa3(config)# sh wccp

Global WCCP information:
    Router information:
        Router Identifier:                   192.168.88.10
        Protocol Version:                    2.0

    Service Identifier: 90
        Number of Cache Engines:             1
        Number of routers:                   1
        Total Packets Redirected:            24
        Redirect access-list:                clients
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   wsa
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
```

Task 3: SSO using Mozilla.

- Configure WSA with a short hostname of “wsa” as the redirect hostname for SSO.
- Login as one of the domain users on the TEST-PC and test SSO. You are allowed to re-configure Mozilla and host file entries on the TEST-PC accordingly for SSO to work.

- To test you may need to reconfigure the TEST-PC and switch accordingly.

Task-3: Solutions

Step 1: Configure WSA with a short hostname of “wsa” as the redirect hostname for SSO.

Network -> Authentication -> Edit Global Settings

Edit Global Authentication Settings

Global Authentication Settings	
Action if Authentication Service Unavailable:	○ Permit traffic to proceed without authentication ◉ Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: ◉ IP Address ○ User Name as Entered by End-User
Re-authentication:	☑ Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction
Basic Authentication Token TTL: ?	3600 seconds
Transparent Proxy Mode Authentication Settings	
Credential Encryption: ?	☐ Use encrypted HTTPS connection for authentication
HTTPS Redirect Port: ?	443
Redirect Hostname: ?	*To achieve true single sign-on for Internet Explorer, use the short hostname or NetBIOS name instead of the fully qualified domain name.* wsa
Credential Cache Options:	? Surrogate Timeout: 300 seconds ? Client IP Idle Timeout: 300 seconds *If this value is greater than the Surrogate Timeout value, this setting has no effect.* Cache Size: 8192 number of entries

Submit and commit the changes

Success — Your changes have been committed.

Authentication Realms

Add Realm...

Realm Name	Protocol	Scheme(s)	Servers	Base DN or NetBIOS Domain	Delete
ADServer	NTLM	NTLMSSP or Basic	10.1.1.101	IPEXPERT0	

Global Authentication Settings

Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Enabled
Basic Authentication Token TTL:	3600
Transparent Proxy Mode Authentication Settings	
Credential Encryption:	Disabled
Redirect Hostname:	wsa
Credential Cache Options:	Surrogate Timeout: 300 seconds Client IP Idle Timeout: 300 seconds Cache Size: 8192 entries
User Session Restrictions:	Disabled
Secure Authentication Certificate:	Common name: IronPort Appliance Demo Certificate Organization: IronPort Systems, Inc. Organizational Unit: Country: US Expiration Date: May 1 22:57:58 2016 GMT Basic Constraints: Not Critical

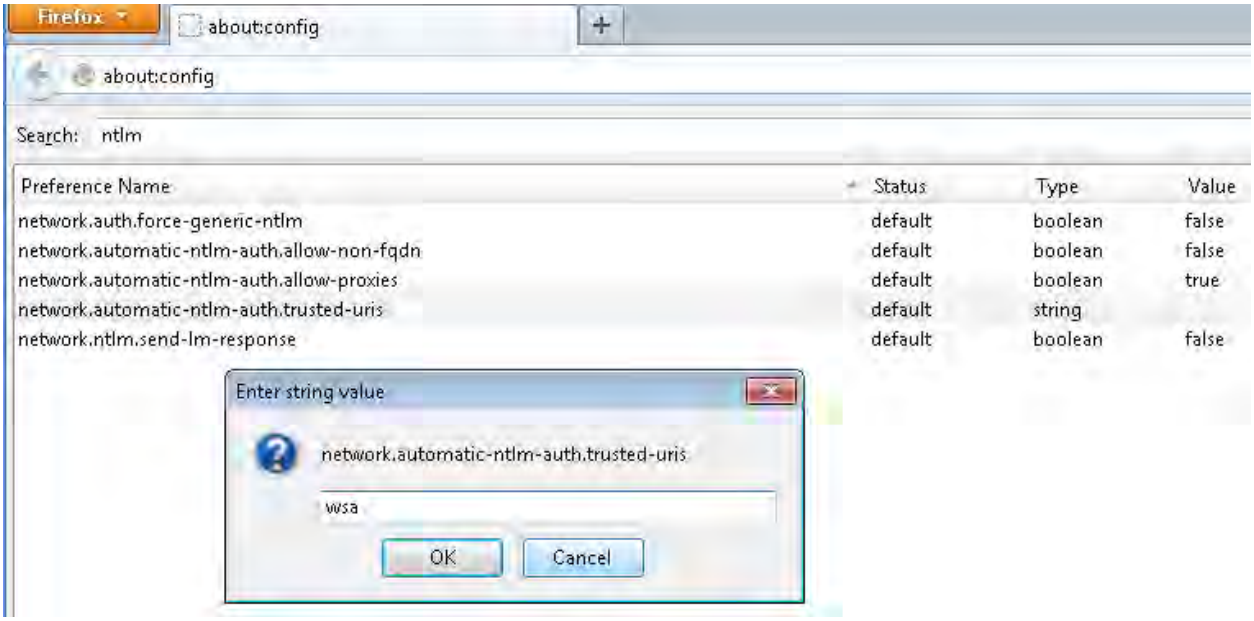
Edit Global Settings...

Step 2: Login as a domain user and re-configure the Mozilla web browser to support SSO.

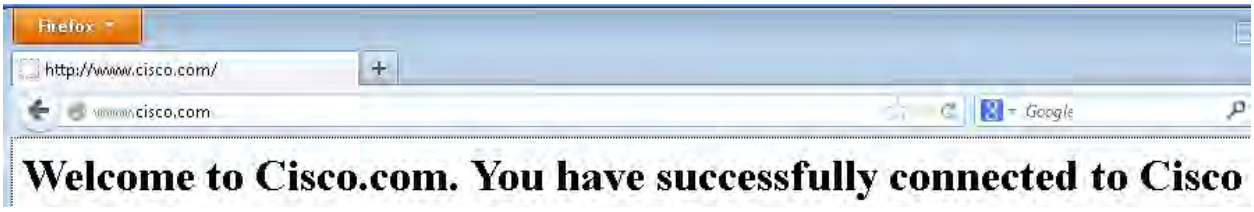
Configure Firefox to use SSO.

Enter the short hostname on the trusted NTLM trusted URI's

1. Enter about:config
2. Enter “ntlm” in the search
3. Click on network.automatic-ntlm-auth.trusted-uris and add “wsa”
4. Optional - Edit the host file to add a manual entry for “wsa”




```
1294756053.107    192    192.168.30.100    TCP_REFRESH_HIT/200    391    GET
http://www.cisco.com/    "IPEXPERT0\ituser1@ADServer"    DIRECT/www.cisco.com
text/html    ALLOW_WBRS_11-IT_Policy-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_comp,6.5,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_comp,-,"-
","-","Unknown","Unknown","-","-",16.29,0,-,"-","-">
```



Lab-7: Configuring L4TM on WSA

Lab-7: Configuring L4TM on WSA– This lab is intended to familiarize you with configuring WSA with L4TM blade.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 1 Hour

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-6 successfully.
Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Detailed Solution: Lab-7

Task 1: Configure SPAN/RSPAN

- Configure SPAN/RSPAN to mirror traffic from VLAN 200 (200.2.45.0/24) to T1 port of WSA.

Task-1: Solutions

Step 1: Configure RSPAN VLAN on SW1 and RSPAN on SW1 and SW2

SW1

```
vlan 999
remote-span

monitor session 1 source vlan 200
monitor session 1 destination remote vlan 999
```

SW2

```
monitor session 1 source remote vlan 999
monitor session 1 destination interface FastEthernet 0/21

SW2#sh monitor session 1
Session 1
---------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 999
Destination Ports      : Fa0/21
    Encapsulation      : Native
          Ingress      : Disabled

SW2#sh interfaces f0/21
FastEthernet0/21 is up, line protocol is down (monitoring)
```

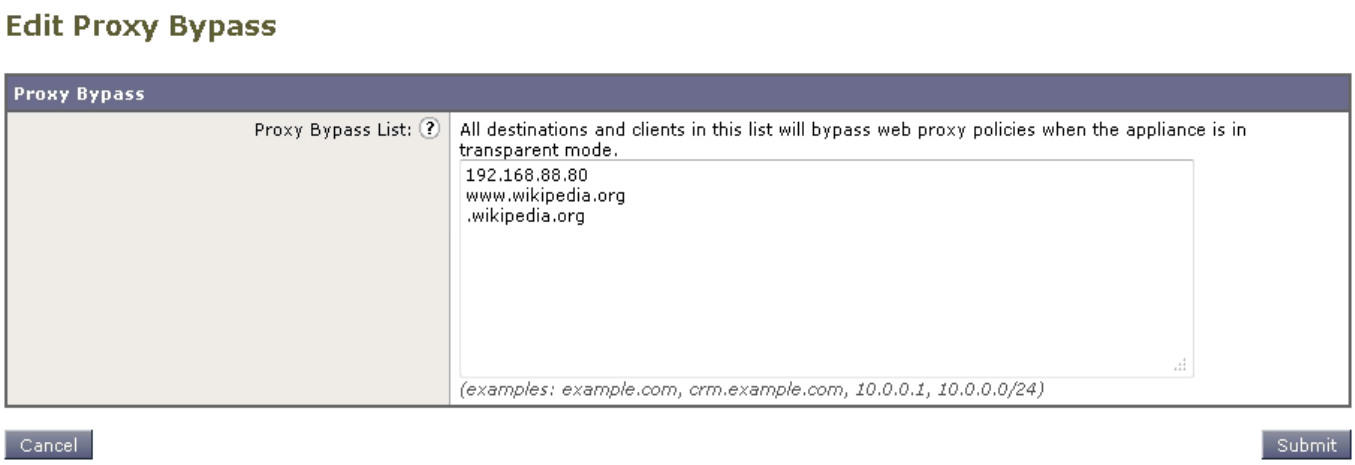
Task 2: Configure transparent proxy bypass

- Configure transparent proxy bypass for the host wikipedia.org and all subdomains of wikipedia.org

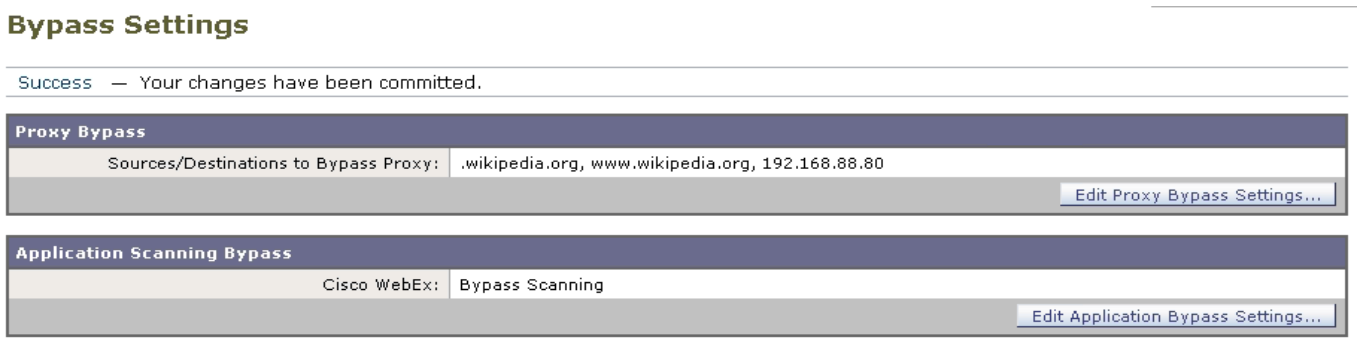
Task-2: Solutions

Step 1: Configure WSA for transparent proxy bypass for Wikipedia.org

Web Security Manager -> Bypass Settings -> Edit Proxy Bypass Settings



Submit and commit the changes



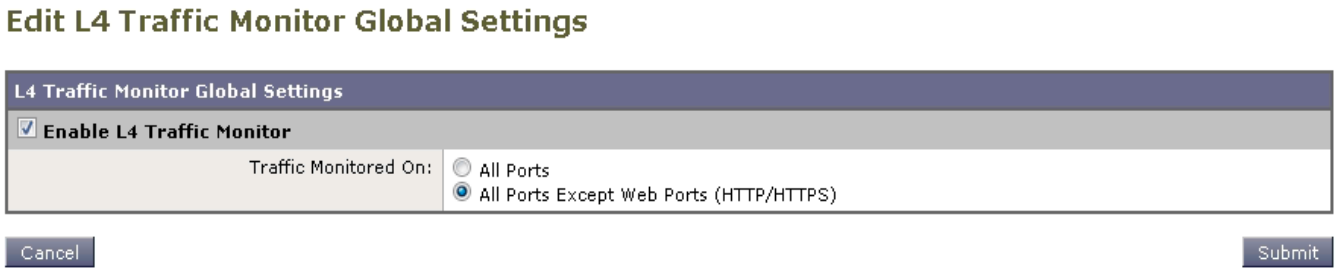
Task 3: Configure L4TM.

- L4TM should be enabled on all ports except web ports. T1 should be in duplex mode.
- Configure L4TM to block all suspected malware. Traffic destined to manage R4 and R5 should be explicitly allowed using White/Allow list.

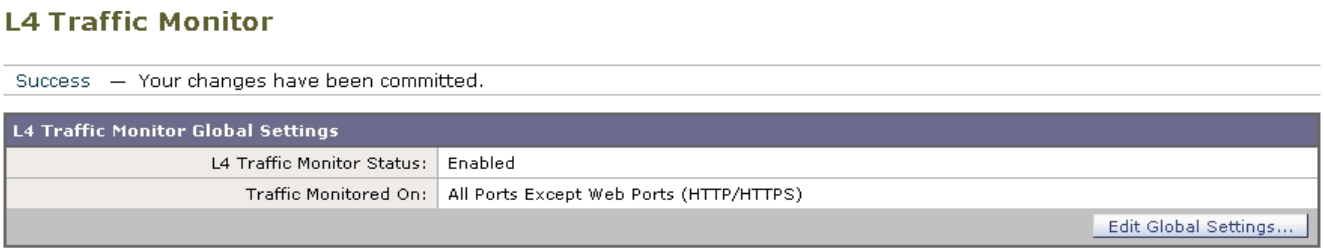
Task-3: Solutions

Step 1: Configure L4TM on all ports except web ports.

Security Services -> L4 Traffic Monitor -> Edit Global Settings

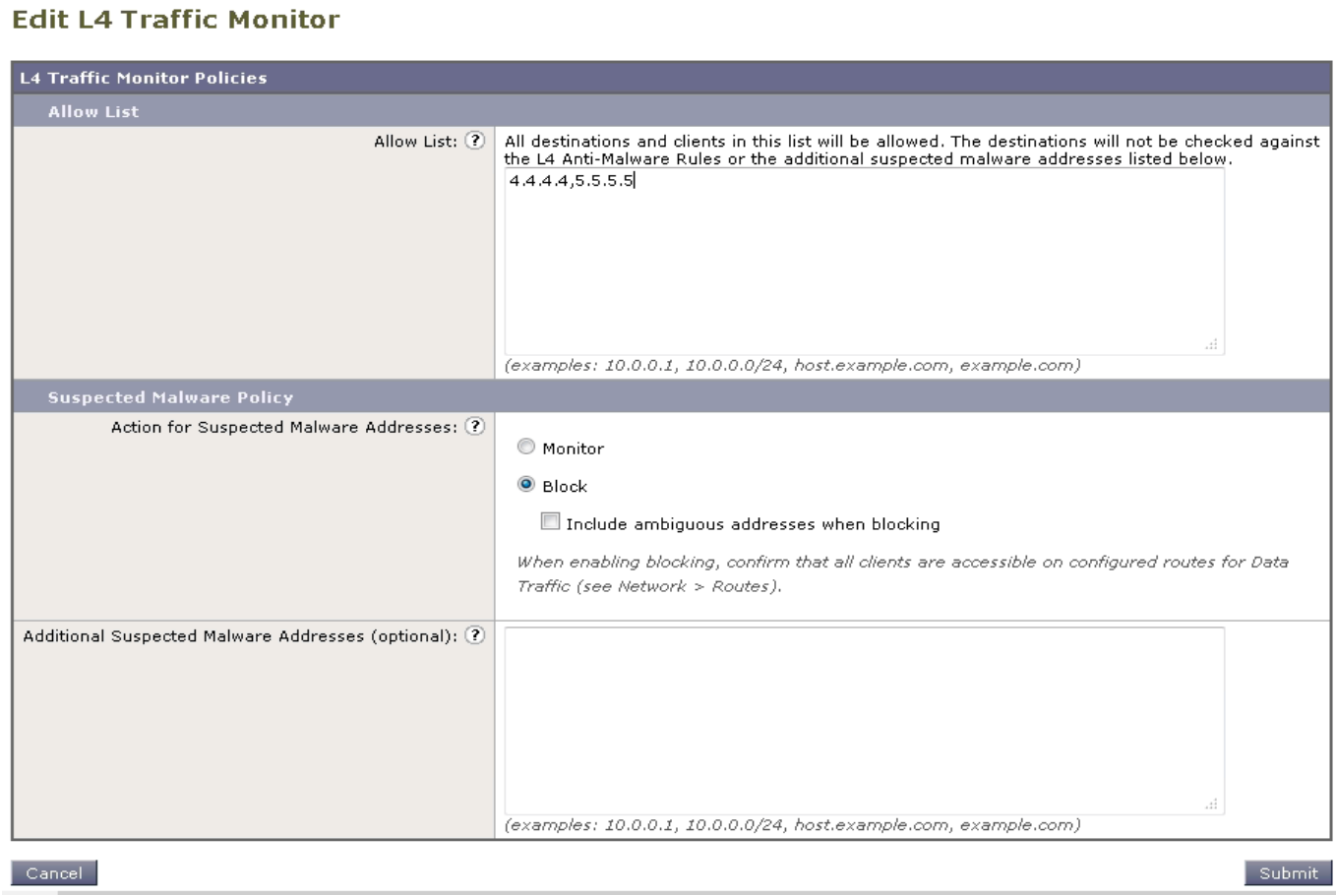


Submit and commit the changes

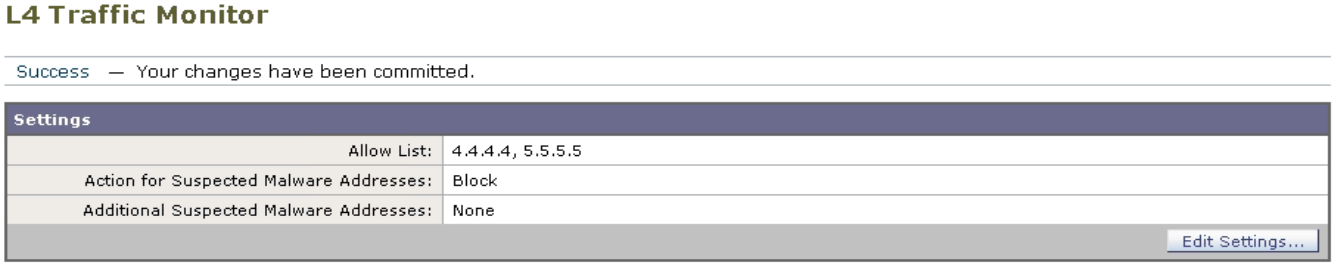


Step 2: Configure L4TM to block all suspected malware. Add R4 and R5 Lo0 IP address to the allow list.

Web Security Manager -> L4 Traffic Monitor -> Edit Settings



Submit and commit the changes



Section 4: ISE Solutions

Lab-1: Basic Configuration of ISE

Lab-1: ISE Basic Setup – This lab is intended to familiarize you with the basic configuration of the ISE. The VM appliance of ISE has already been initialized. The focus is to modify basic parameters and configure basic features on ISE. The basic features cover configuring a new self-signed certificate, RBAC for administrative control, repository configuration, routing configuration, NTP configuration, Integration with active directory.

We highly recommend creating your own diagram at the beginning of each lab so you are able to draw on your own diagram, making it much easier when you step into the real lab.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- Make it a common practice to verify the pre-configurations loaded on the devices.

Estimated Time to Complete: 2 Hours

Pre-setup

Load the initial configurations for the routers and switches. Note that routers and switches are pre-configured with these initial configurations.

NOTE: *Do not make additional configuration on the routers, unless explicitly stated in the task; some switching configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Error! Objects cannot be created from editing field codes.

Lab 1: Configuration Tasks and Solutions

Task 1: Basic Setup of ISE

- Configure appropriate VLAN's on the switch for ISE as per topology diagram 4.1.

Solutions

SW3

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
```

- R2 has been pre-configured to be the NTP server, make sure that R2 and the AD server has the same time settings.

Solutions

R2

```
Make sure R2 matches the time of the AD server. Use Clock Set command in the
privilege exec.
```

- Add a static route for 192.168.0.0/16 with R2 as the next-hop on the ISE.

Solutions

```
ip route 192.168.0.0 255.255.0.0 gateway 10.1.1.2
```

- Configure UTC as the time zone and set AD server and R2 as the NTP servers on ISE. Make sure R2 and AD have the same time.

Solutions

ISE

```
ntp server 10.1.1.101
ntp server 10.1.1.2
```

- Configure AD server as the repository using FTP protocol. The repository name should be “AD_FTP”. The URL should be configured as ftp.ipexpert.com. Use “administrator/IPexpert123” for the ftp login.

Solutions

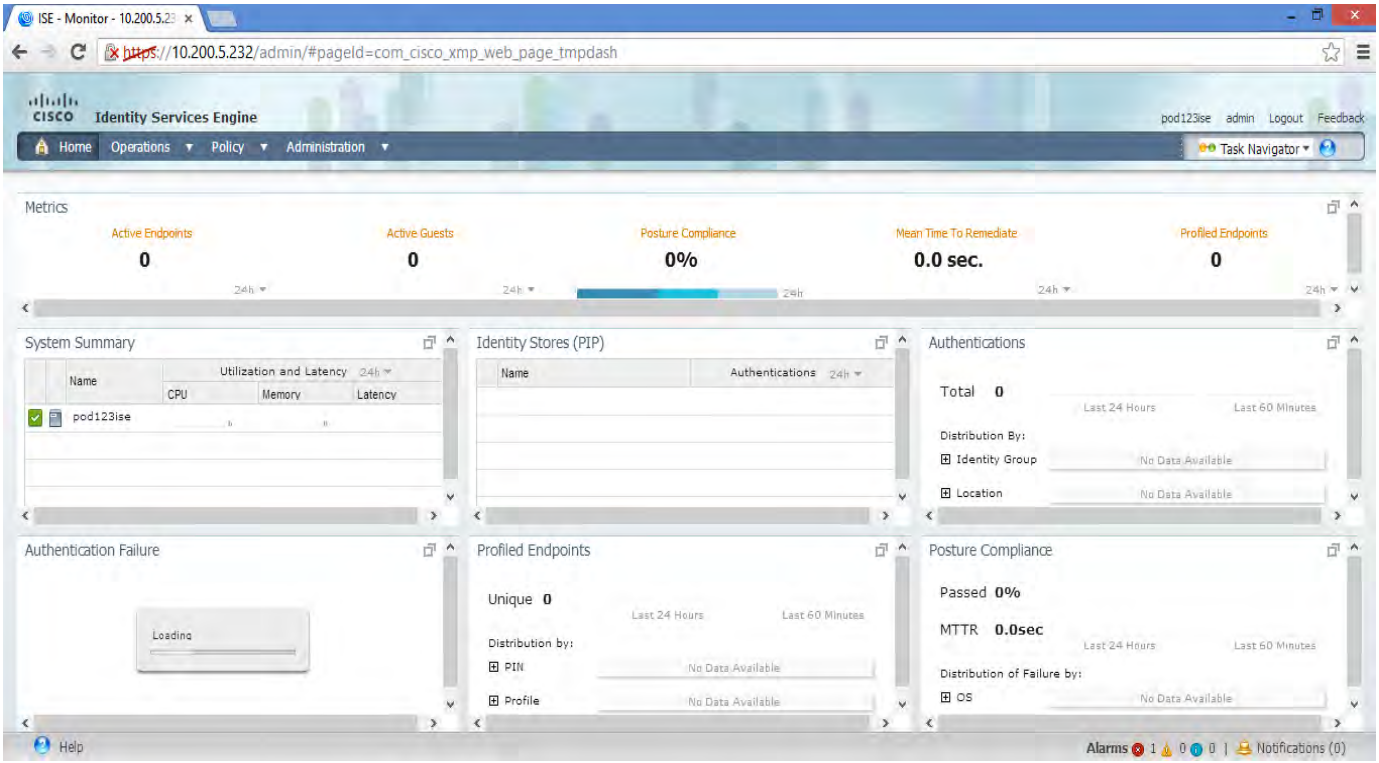
ISE

```
repository AD_FTP
  url ftp://ftp.ipexpert.com
  user administrator password plain IPexpert123
```

- Use “show application status ise” in the CLI and make sure all processes are running before you login to the GUI using the IP address of the ISE.

Solutions

```
show application status ise

ISE Database listener is running, PID: 19244
ISE Database is running, number of processes: 26
ISE Application Server is running, PID: 20849
ISE M&T Session Database is running, PID: 20053
ISE M&T Log Collector is running, PID: 21063
ISE M&T Log Processor is running, PID: 21147
ISE M&T Alert Process is running, PID: 20969
% WARNING: ISE DISK SIZE NOT LARGE ENOUGH FOR PRODUCTION USE
% RECOMMENDED DISK SIZE: 200 GB, CURRENT DISK SIZE: 64 GB
VPN into proctors labs and login into ISE using a web browser
(https://10.200.x.x)

Use admin/IPexpert123 as the login credentials
```



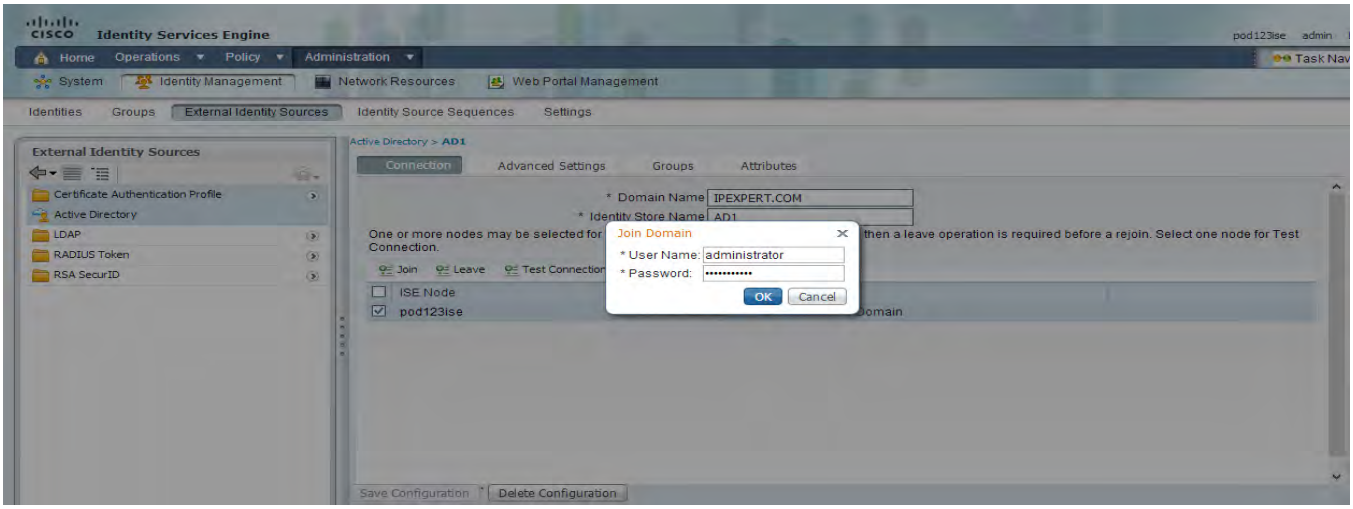
- Integrate ISE with active directory. Use a name of “AD1”. The AD domain name should be ipexpert.com. Use “administrator/IPexpert123” to join the domain.

Solutions

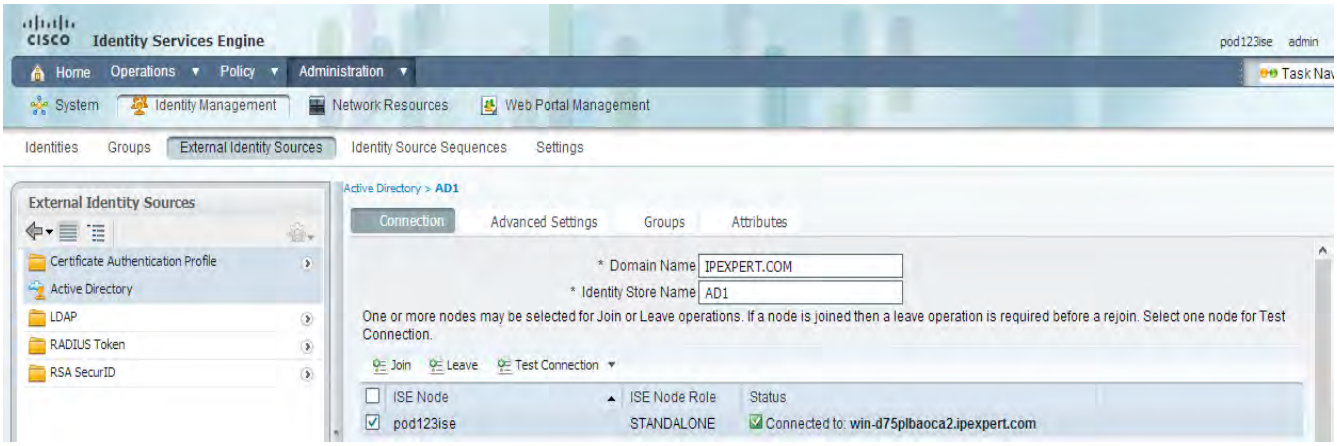
Step 1: Navigate to **Administration-> Identity Management -> External Identity Sources -> Active Directory**

Step 2: Enter the Domain Name and ID store name and then save the configuration

Step 3: Click on **Join** and enter the AD credentials (administrator/IPexpert123)



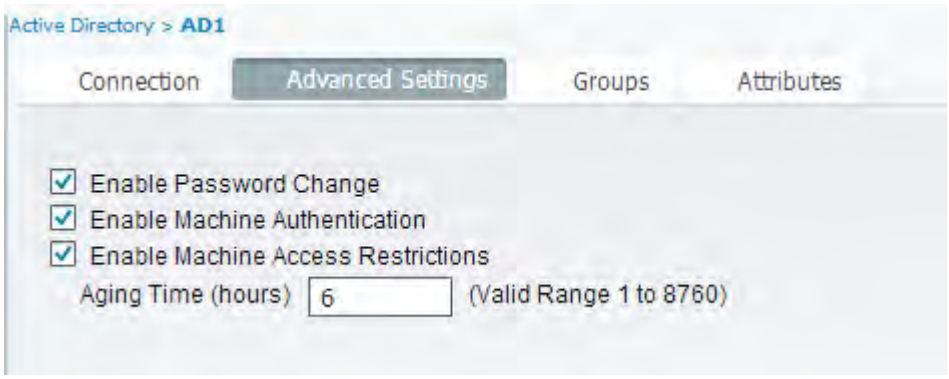
Make sure the ISE has joined the AD.



- Enable Password Change, Enable Machine Authentication and Enable Machine Access Restrictions for AD connection settings.

Solutions

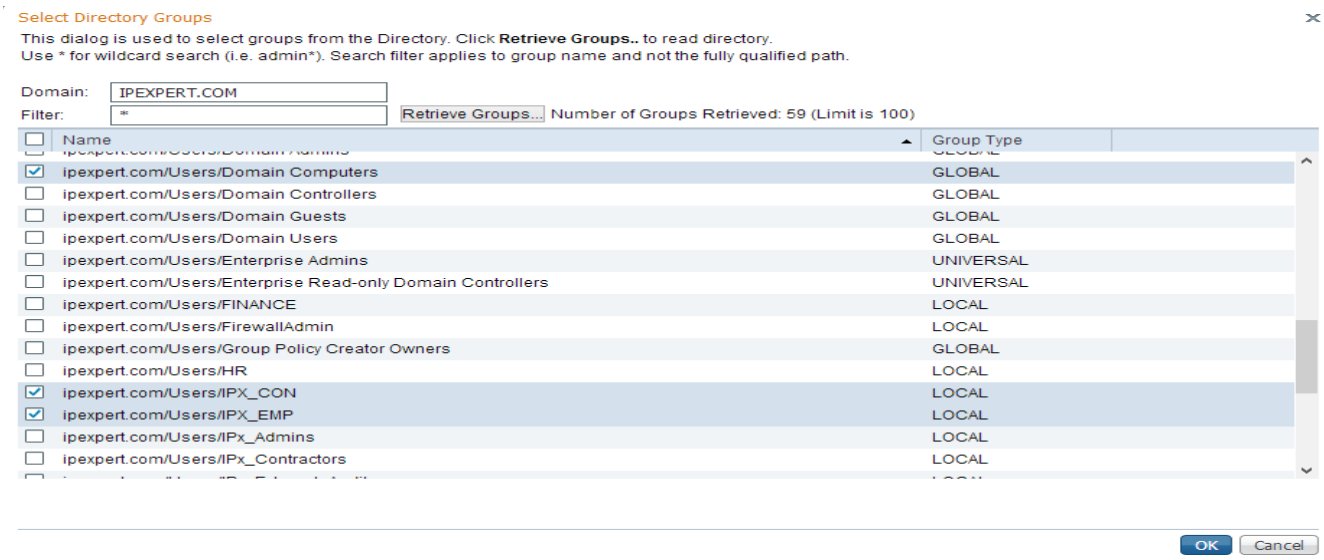
Step 1: Click on Advanced Settings configure accordingly



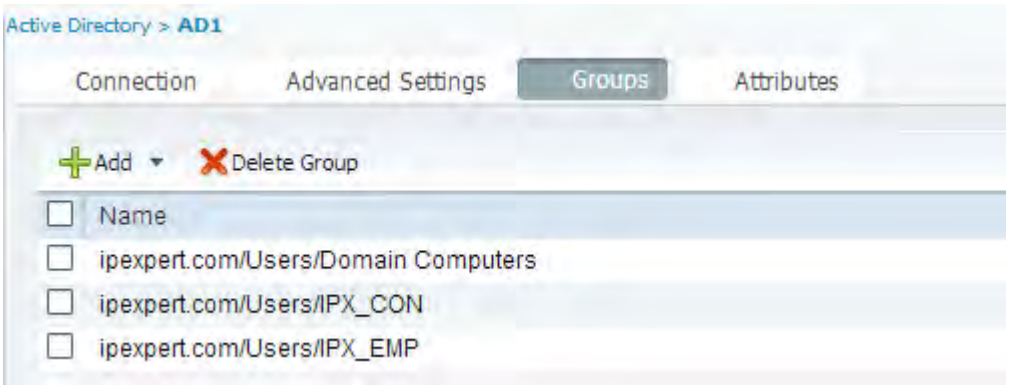
- Retrieve "IPX_EMP", "IPX_CON" and "Domain Computers" from the AD group attributes. These will be used for creating authorization policies/rules in the later section.

Solutions

Step 1: Click on Groups and click on Add to retrieve the group attributes. Select the appropriate group attributes



Step 2: Click on Save Configuration

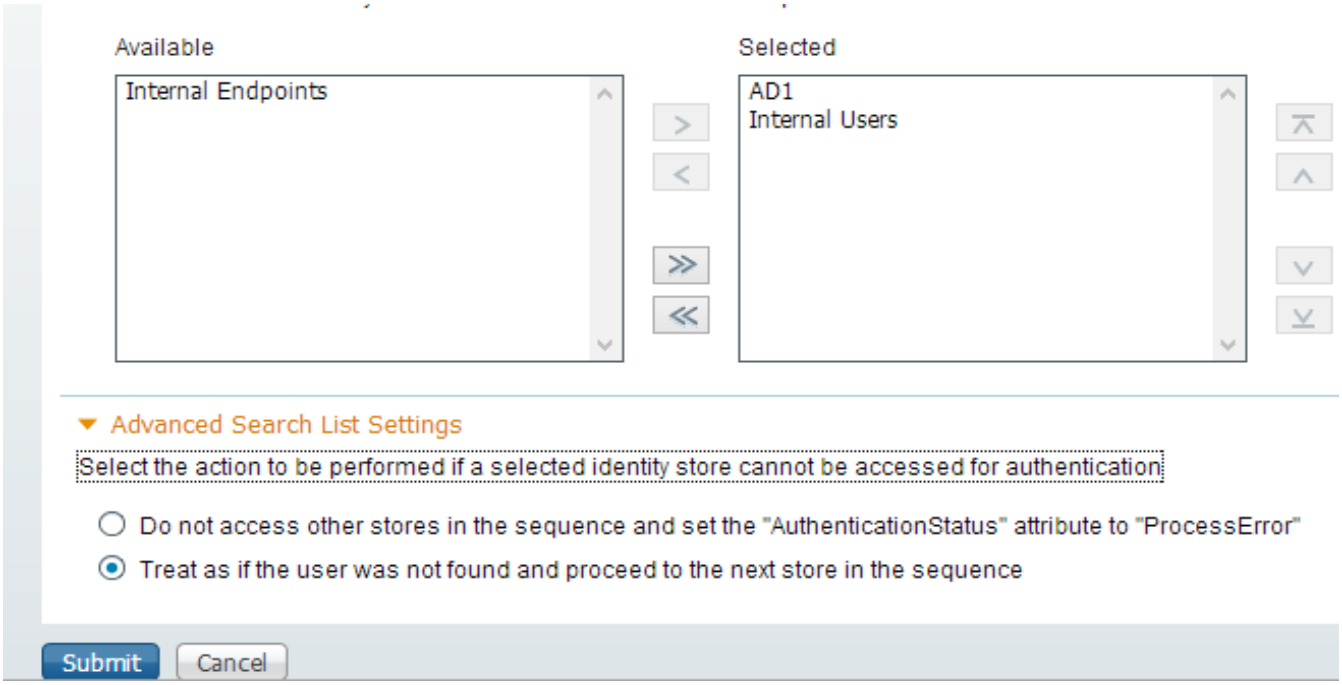


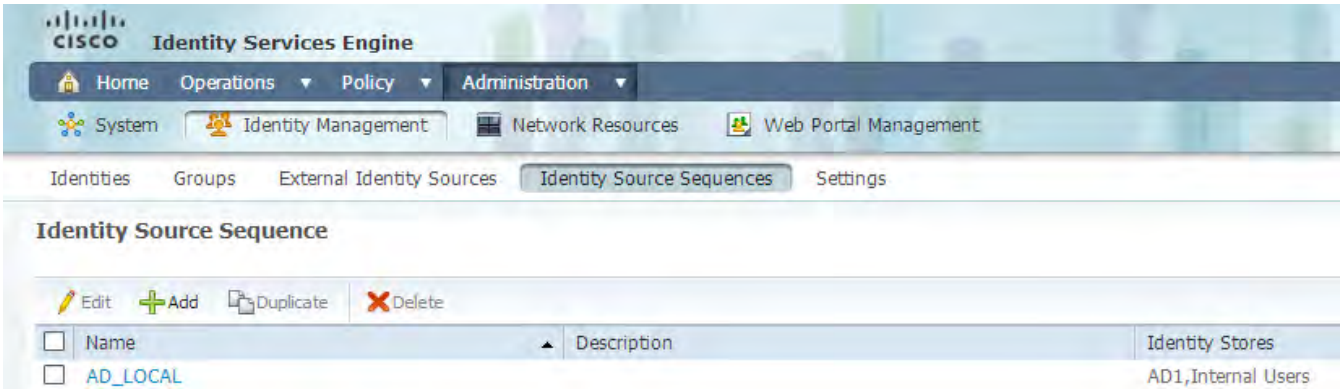
- Configure Identity Source sequence called “AD_LOCAL” such that users are first authenticated with AD server, if this server is not accessible or users are not found in the database then the internal user endpoint database will be used for authentication as the second method.

Solutions

Step 1: Go to **Administration -> identity Management -> Identity Source Sequence**

Step 2: Click on Add and enter the name if the ID Source sequence and select the Appropriate ID sources



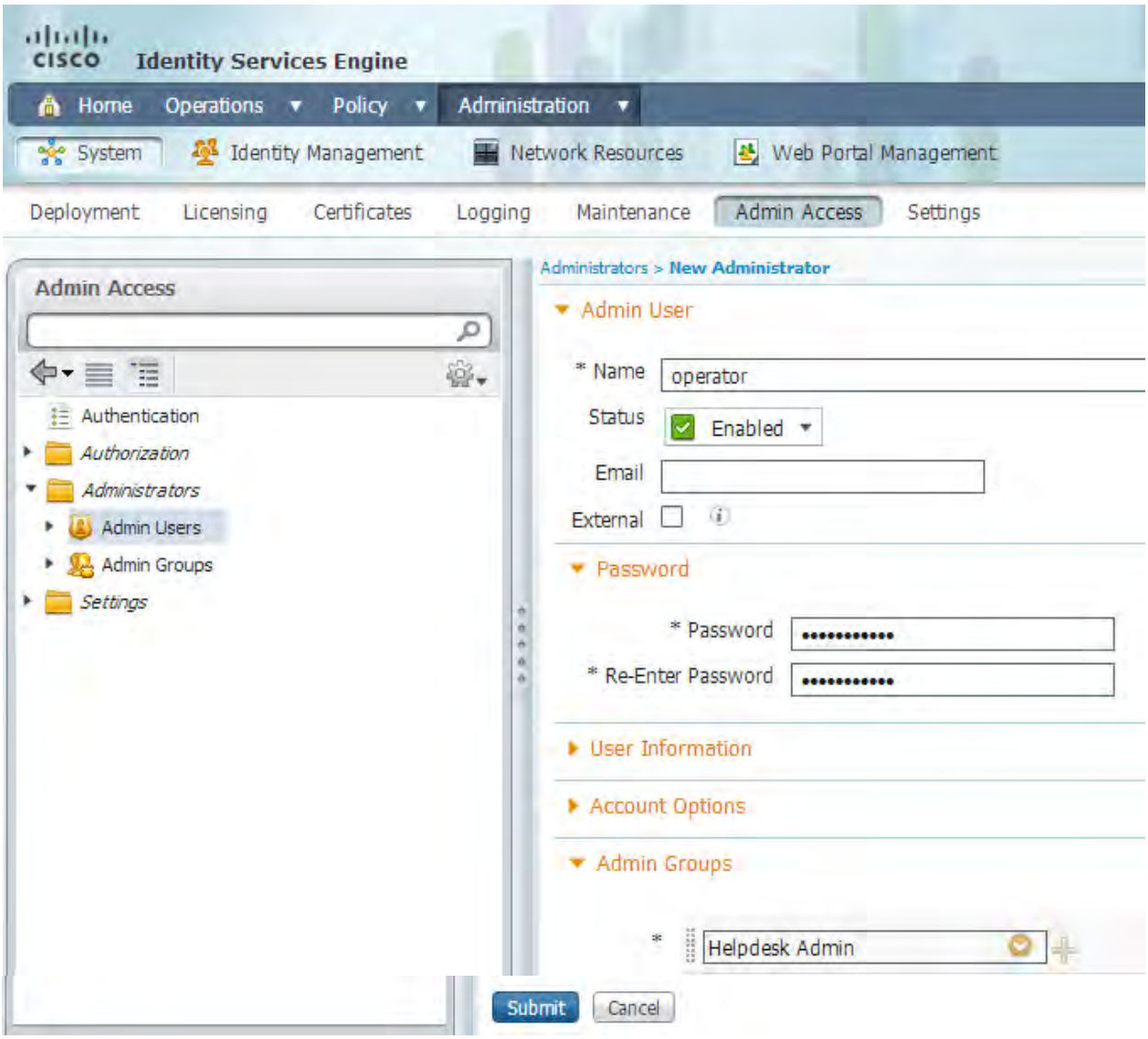


- Use predefined RBAC policies for administrative access. Create a new user operator/IPexpert321. Assign operator user to a pre-defined group of helpdesk, which can view only the operations menu.

Solutions

Step 1: Go to **Administration-> Admin Access -> Administrators**

Step 2: Click on Add and create a new admin user called “operator” with a password of “IPexpert321”



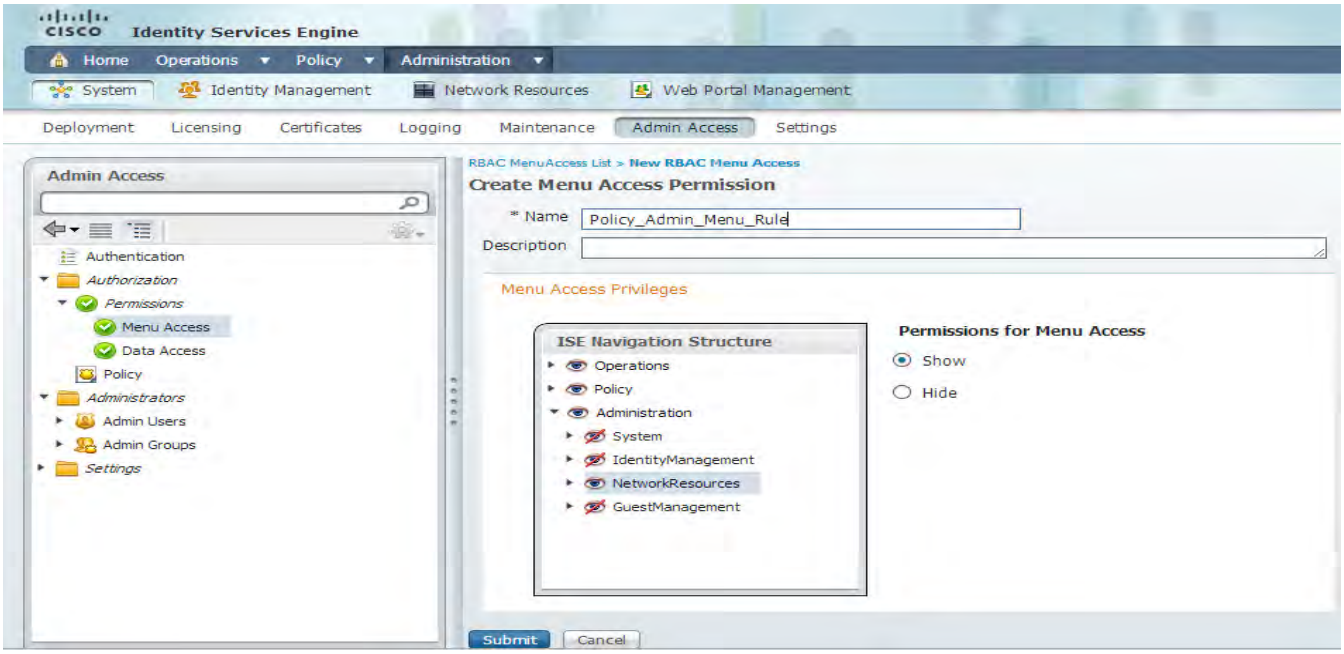
Assign the “operator” user to “Helpdesk Admin” group and click on submit

- Configure a new RBAC policy and group called “Policy_Admin” with the below parameters. Create a new user called policyadmin/IPexpert123 and test this admin policy. This user should be allowed to create/modify policies and view AAA clients/NDG’s.

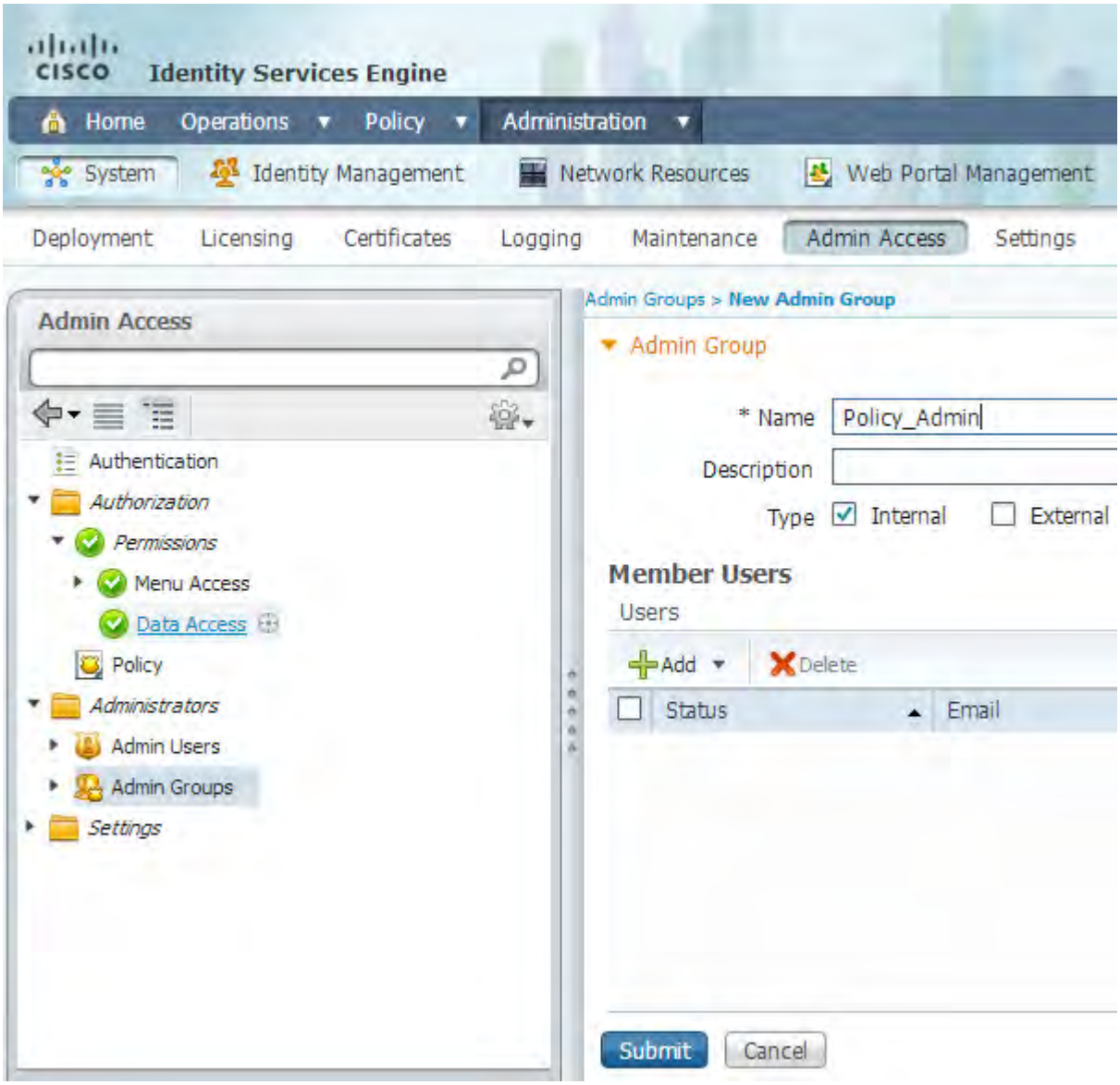
RBAC Policy and Group – "Policy_Admin"		
RBAC Menu Access policy	Allow – Operations (Allow All) Allow – Policy (Allow All) Limited - Administration	Only show "Networkresources"
RBAC Data Access Policy	Use pre-defined policy – "Network Admin Data Access"	

Solutions

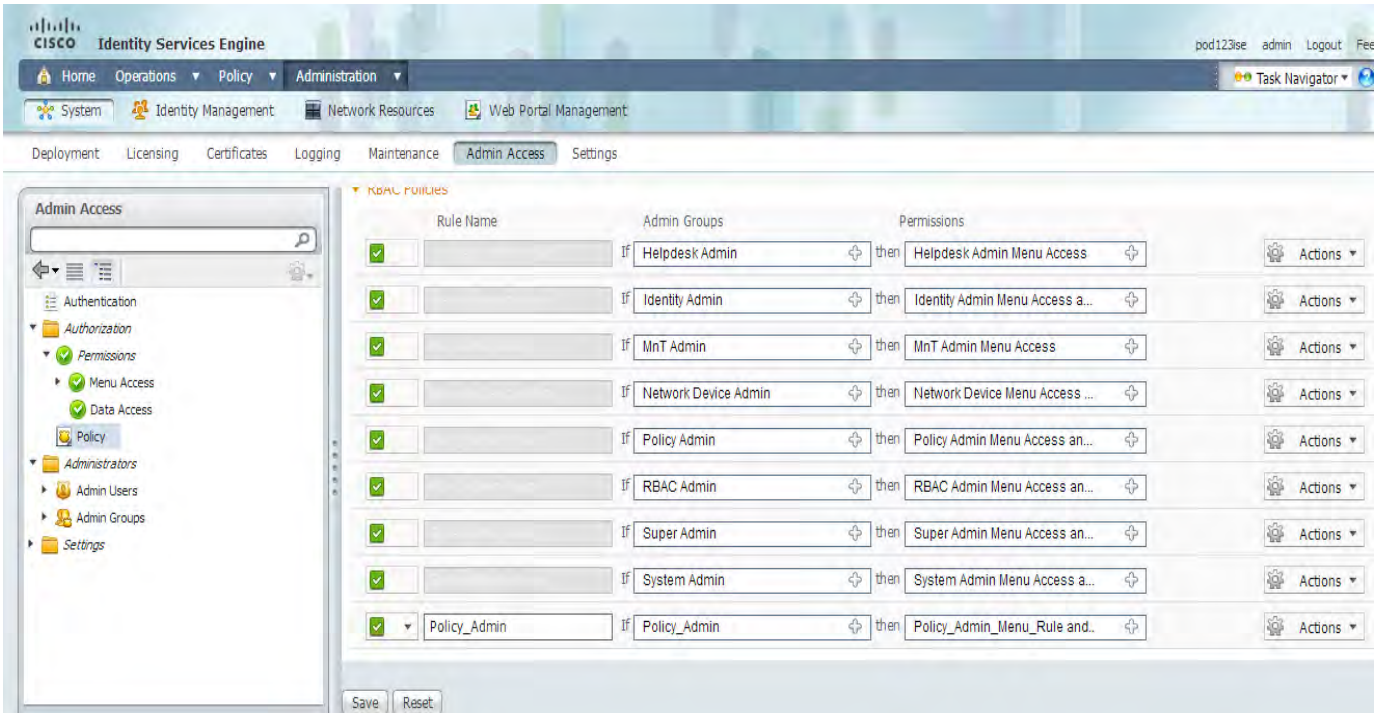
Step 1: Create a new Menus Access Permission as per the task



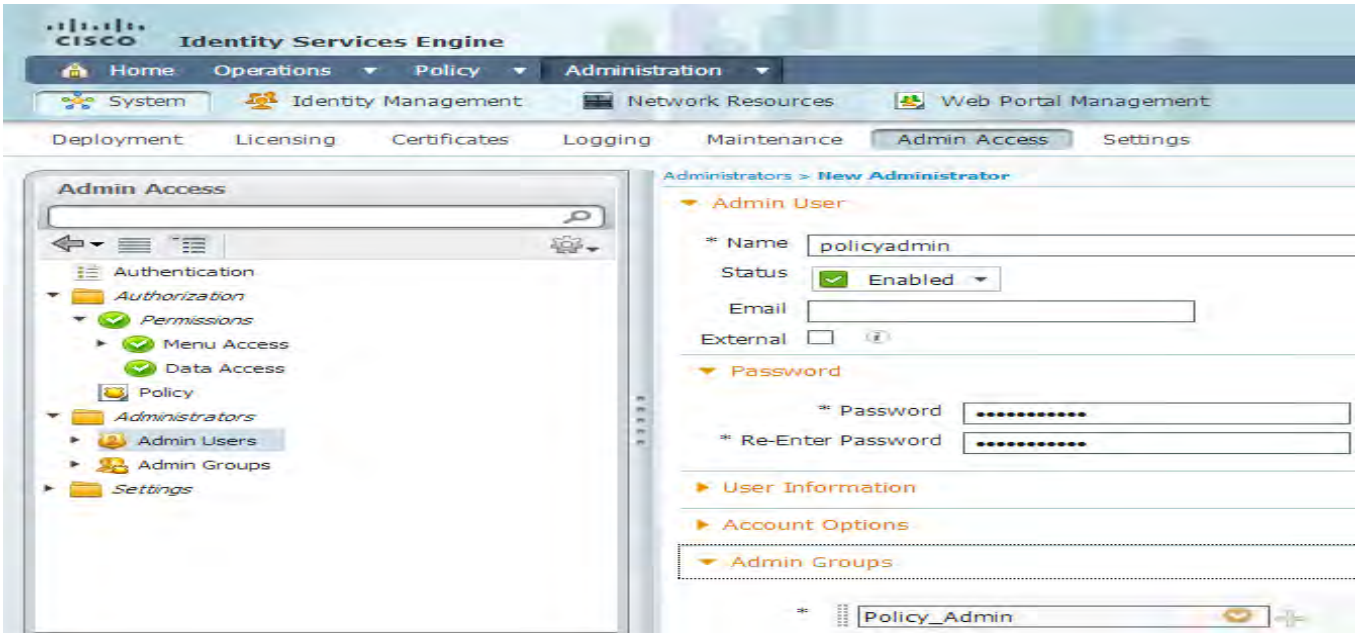
Step 2: Create a new group called "Policy_Admin".

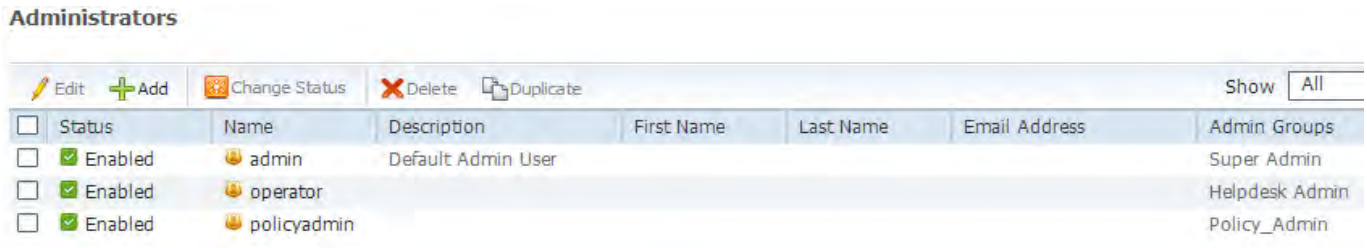


Step 3: Create a new RBAC policy for the new group to assign appropriate permissions.

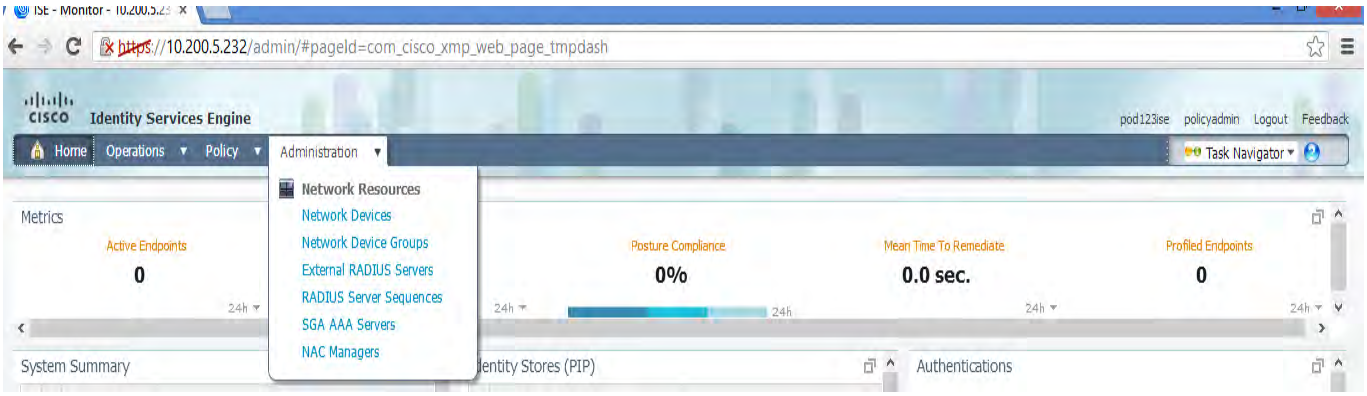


Step 4: Create a new admin user called “policyadmin” with a password of “IPexpert123” and assign the user to “Policy_Admin” group





Step 5: Login as "policyadmin" user to test the policy.



Lab-2: Configuring network resources and profiling on ISE

Lab-2: Configuring network resources and profiling – This lab is intended to familiarize you with configuring AAA clients, NDG's, Enabling profiling services and modifying existing profiling policies.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **1.5 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully.
Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

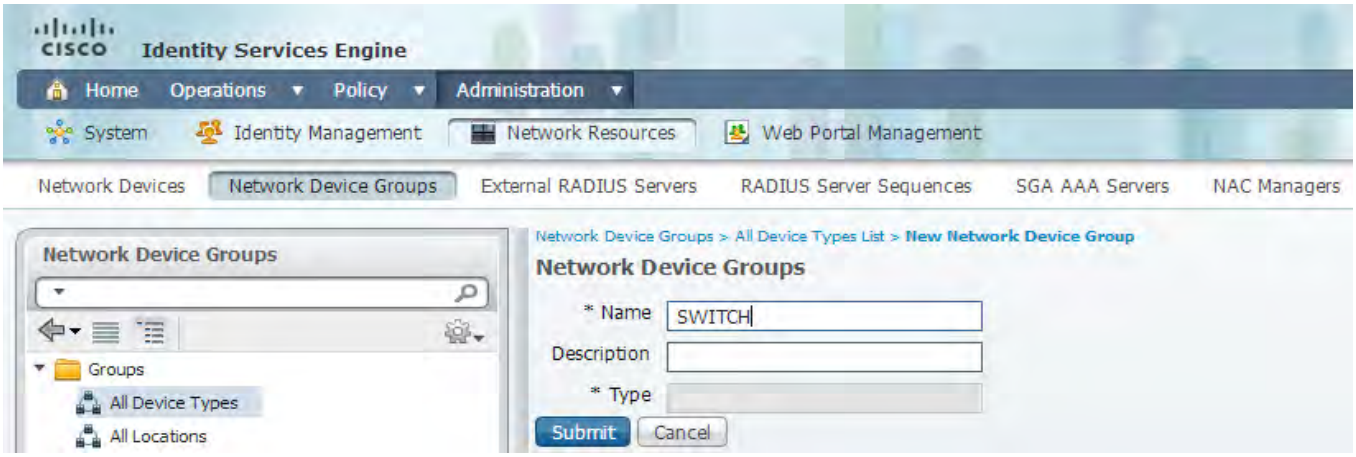
Task 1: Configure NDG's and AAA clients on ISE and switches.

- Create new NDG called "WLC" and "SWITCH" under "All device type".

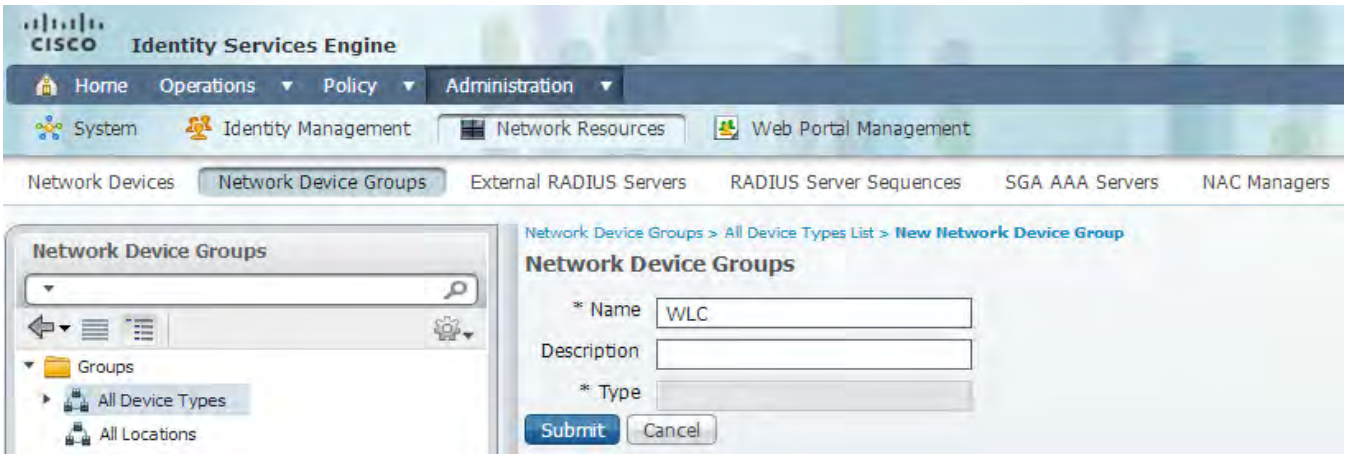
Solutions

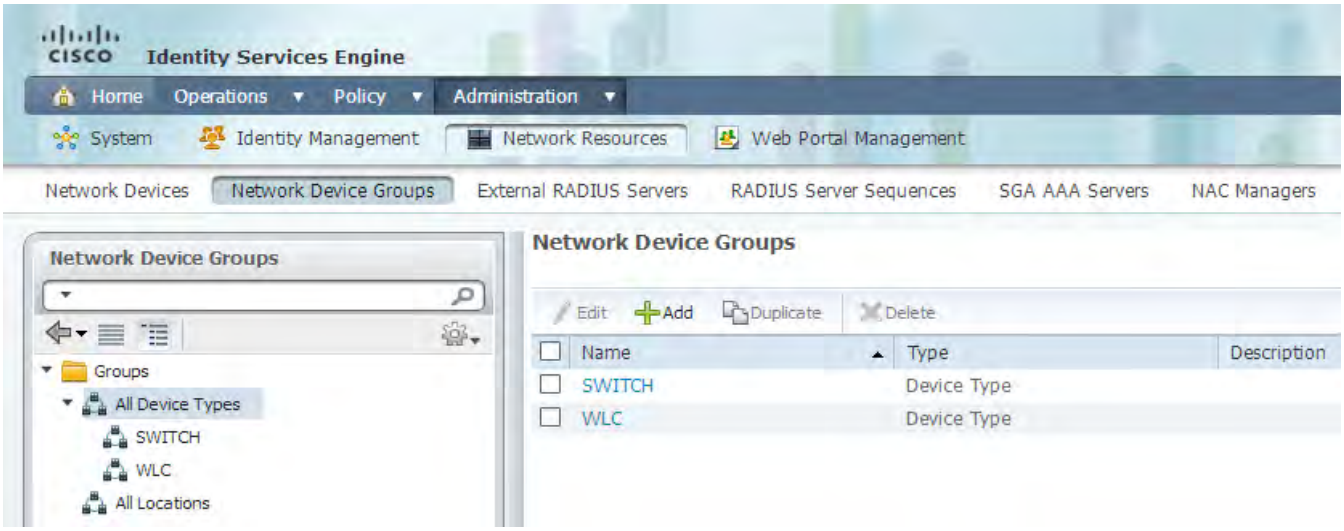
Step 1: Go to **Administration -> Network Resources -> Network Device Groups ->All Device Type** and create the appropriate NDG. Click on **Add**.

Create the "SWITCH" NDG



Create the "WLC" NDG



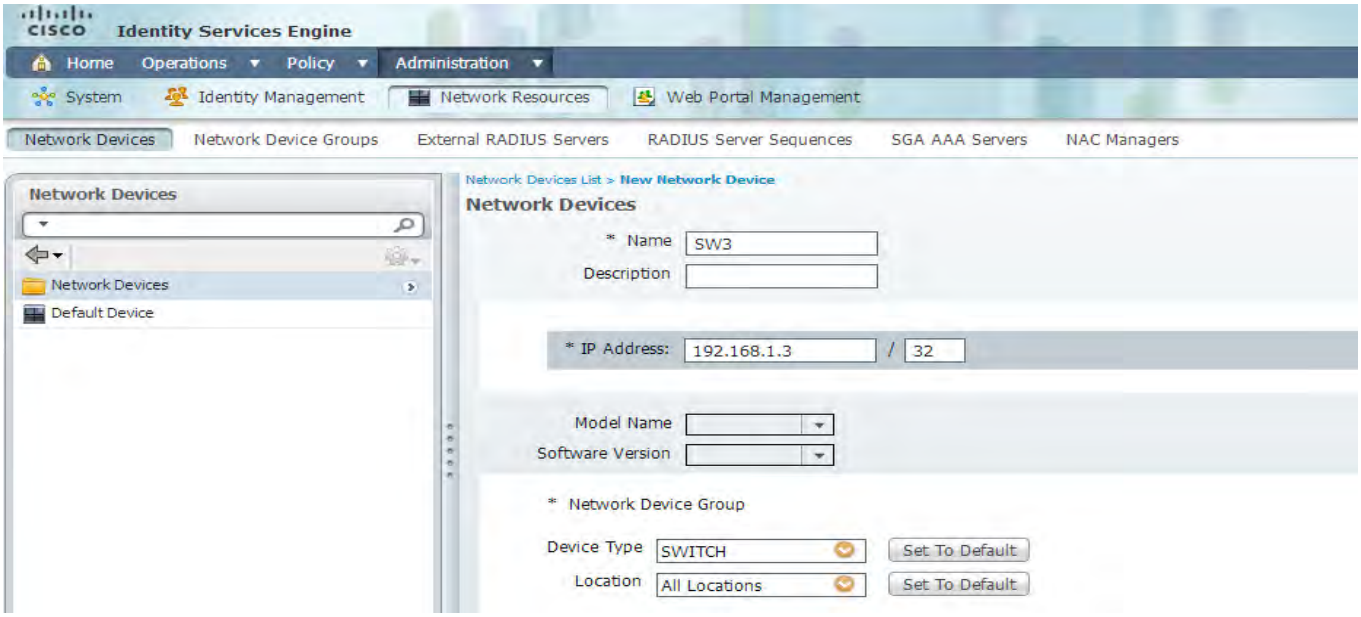


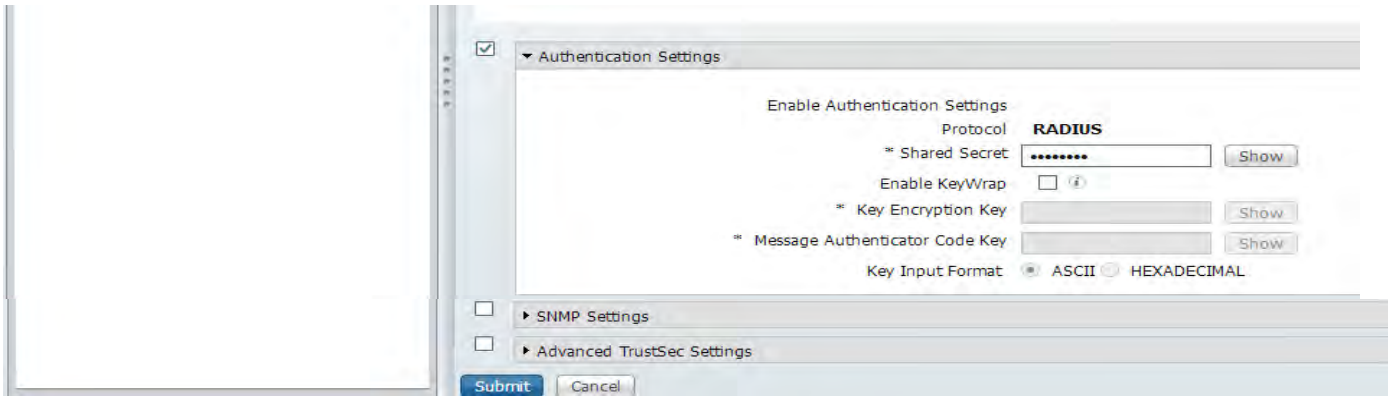
- Add SW3 and SW2 as the AAA client. SW3 will use VLAN 10 IP address as the source for sending RADIUS packets. Use a radius key of cisco123. Assign these switches to "SWITCH" NDG under All Device type

Solutions

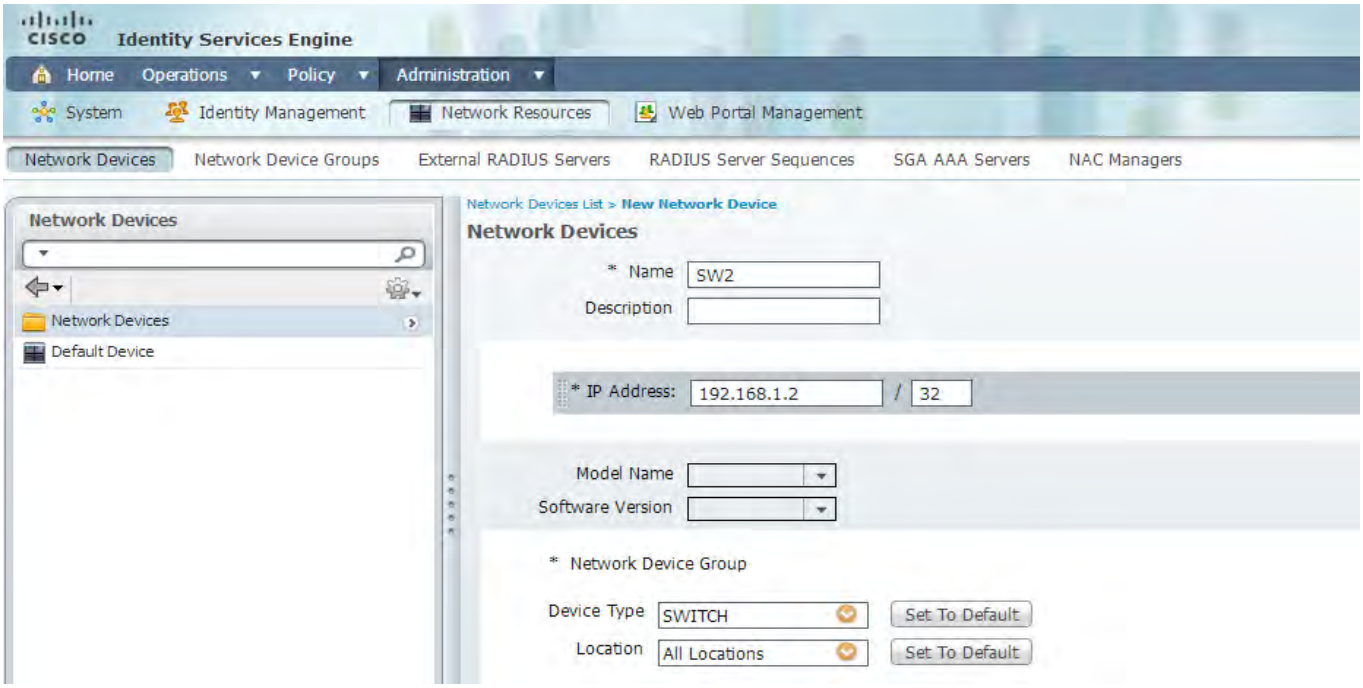
Step 1: Go to **Administration -> Network Resources -> Network Devices**. Click on **Add**.

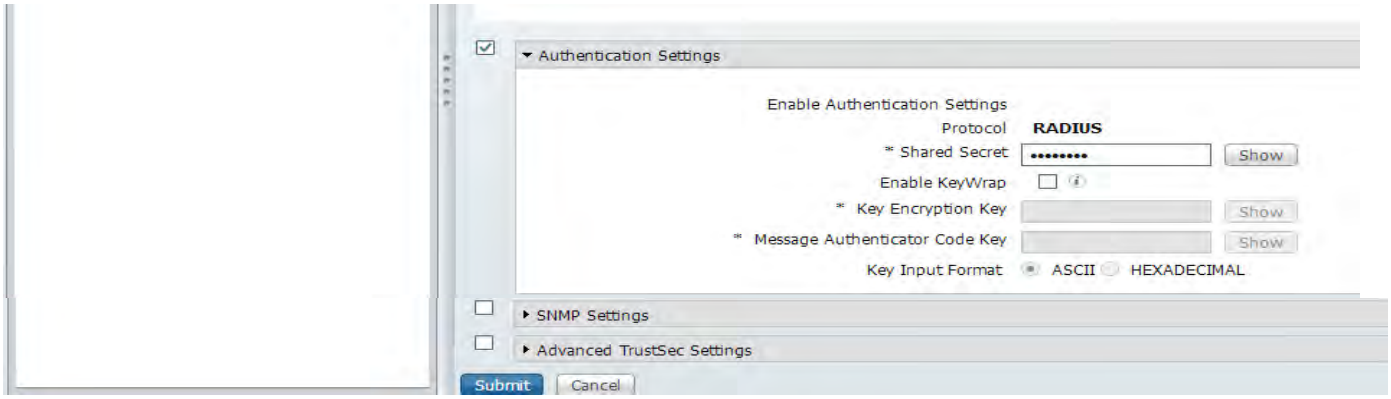
Add SW3 as an AAA client





Add SW2 as an AAA client

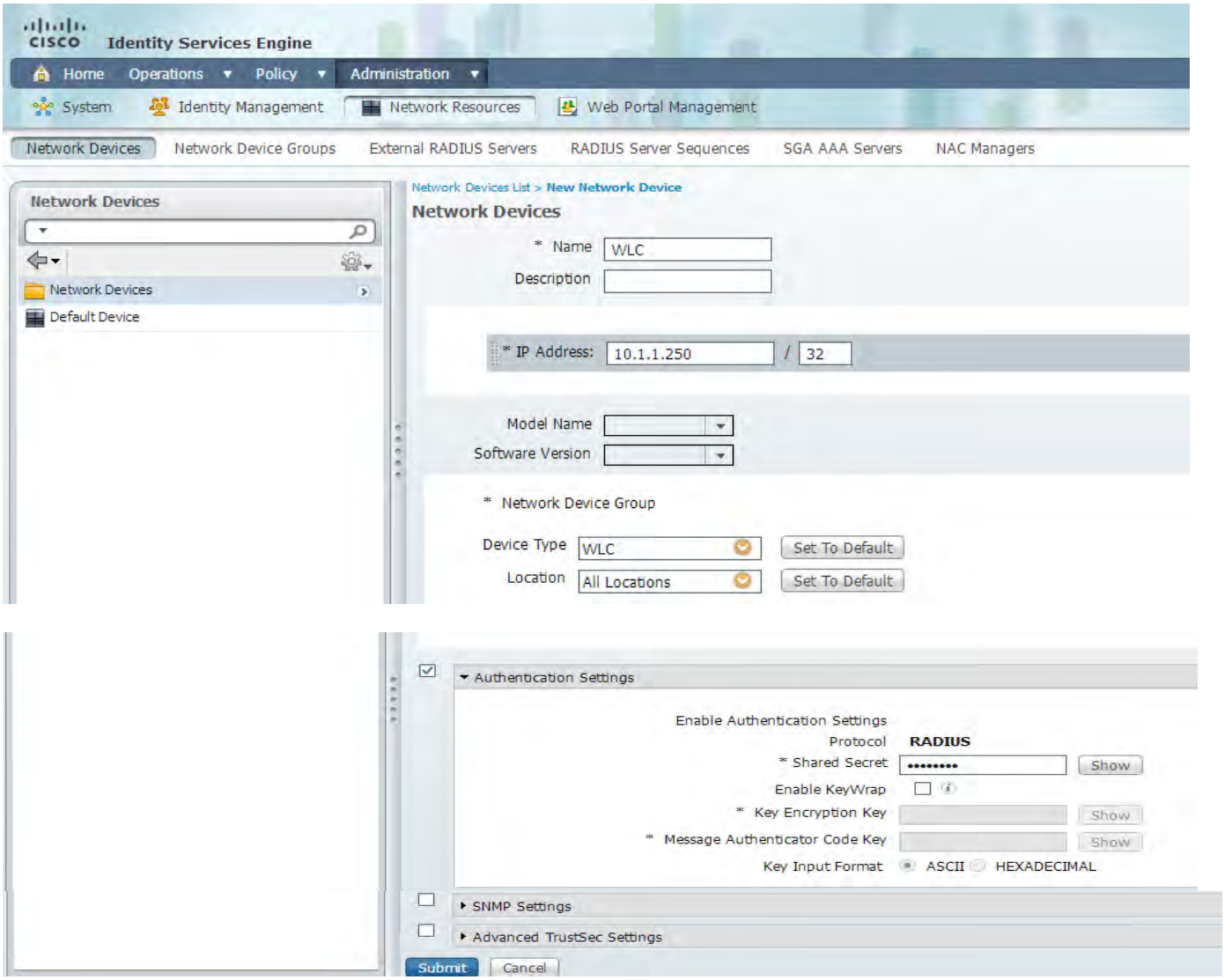




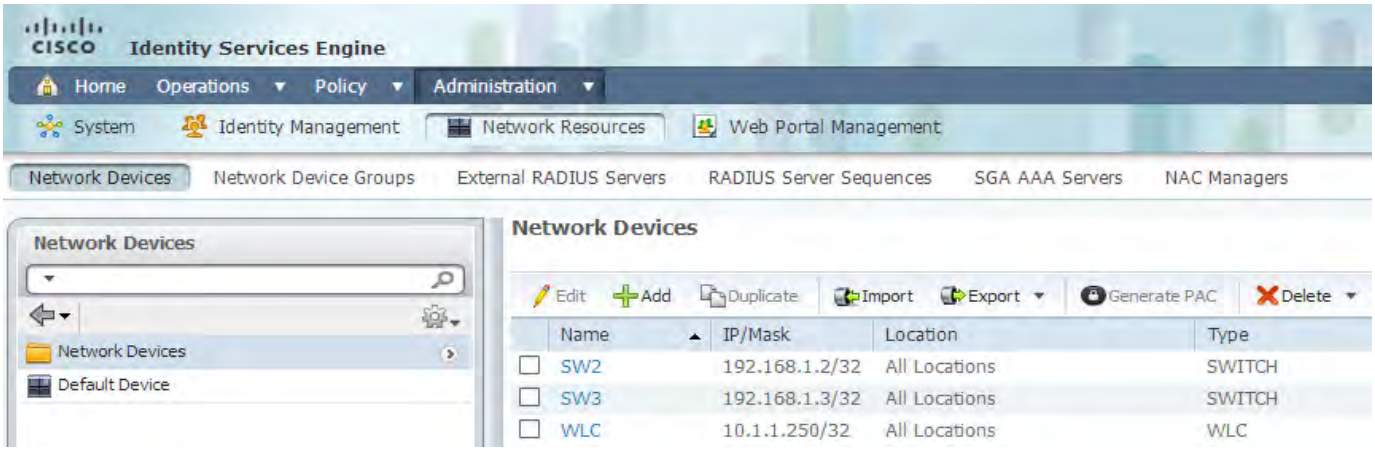
- Add WLC as the AAA client. Use a radius key of cisco123 and assign this device to “WLC” NDG under All Device type.

Solutions

Step 1: Add WLC as an AAA Client



Review all the AAA clients configured on the ISE



- Configure ISE (10.1.1.150) as the radius server on the switches
- SW3 should use test/cisco123 to test the connectivity between switch and ISE automatically every 1 hour. You are allowed to create a new network access user to accomplish this.
- Change the dead timer criteria for the AAA server on the switches such that if no valid response from the ISE within 15 seconds, the server should be marked as dead.
- Make sure G1/0/2 and G1/0/12 interfaces on SW3 and F0/22 on SW2 are in shutdown state.

Solutions

Step 1: Shutdown the interfaces as per the task

SW2

```
interface FastEthernet0/22
shutdown
```

SW3

```
interface GigabitEthernet1/0/2
shutdown

interface GigabitEthernet1/0/12
shutdown
```

Step 2: Configure SW3 and SW2 as the AAA client

SW2 and SW3

```
aaa new-model
```

```
radius-server dead-criteria time 5 tries 3
radius-server host 10.1.1.150 auth-port 1812 acct-port 1813
radius-server key cisco123
```

SW3

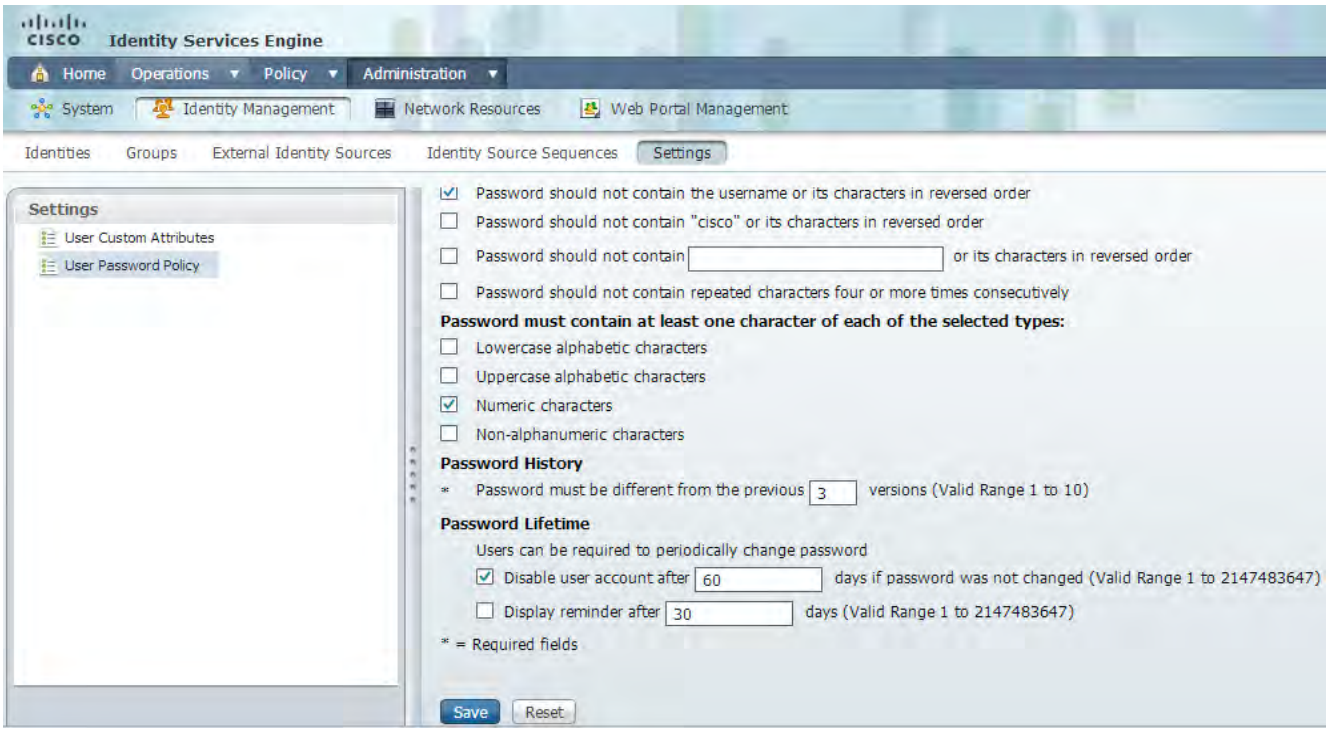
```
username test password 0 cisco123
radius-server host 10.1.1.150 auth-port 1812 acct-port 1813 test username
test key cisco123
```

Step 3: Configure a network access user on ISE

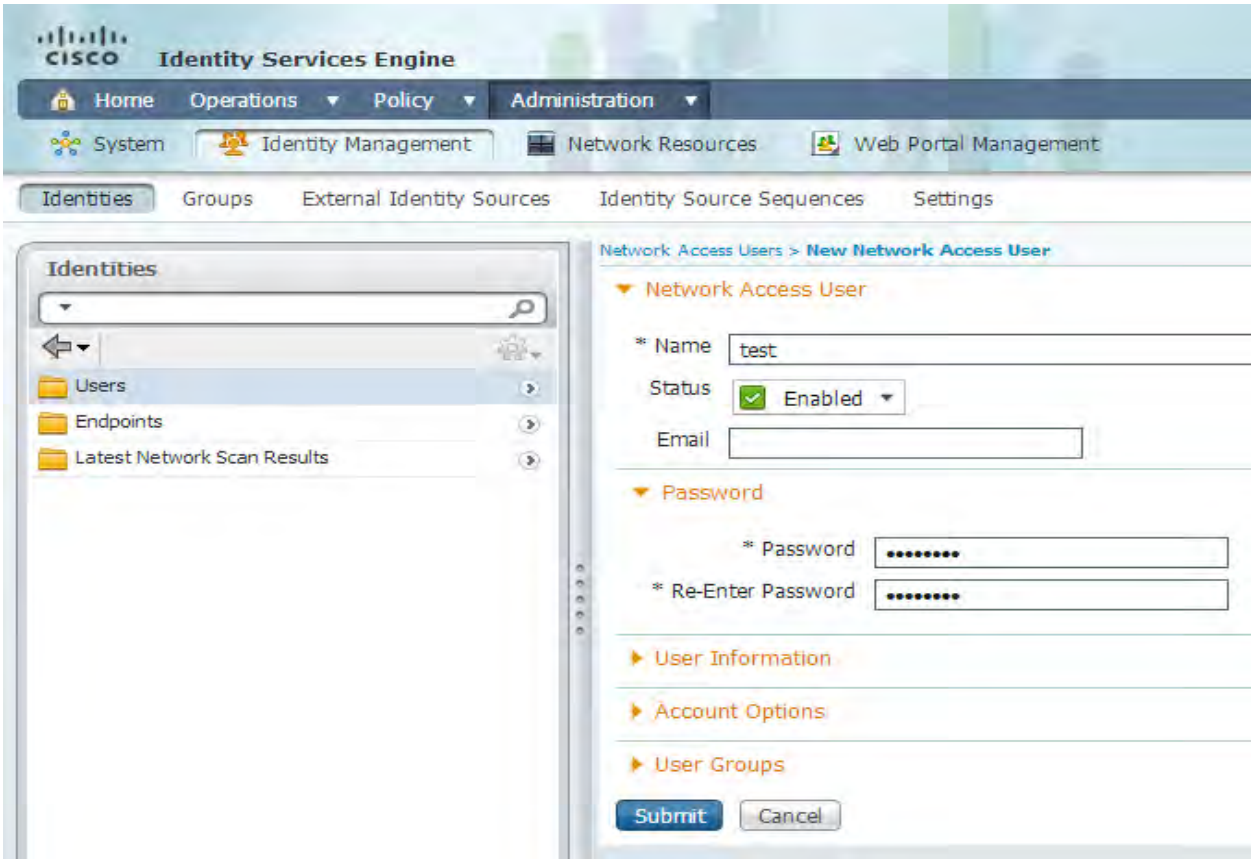
Before you configure Network Access User, make sure to change the default password policy.

Go to **Administration->Identity Management->Settings->User Password Policy**

Uncheck Password must contain Lowercase alphabet and uppercase alphabet.



Go to **Administration->Identity Management->Identities->Users**. Click on **Add** to create Network Access User. (test/cisco123)



Test AAA configuration on SW3

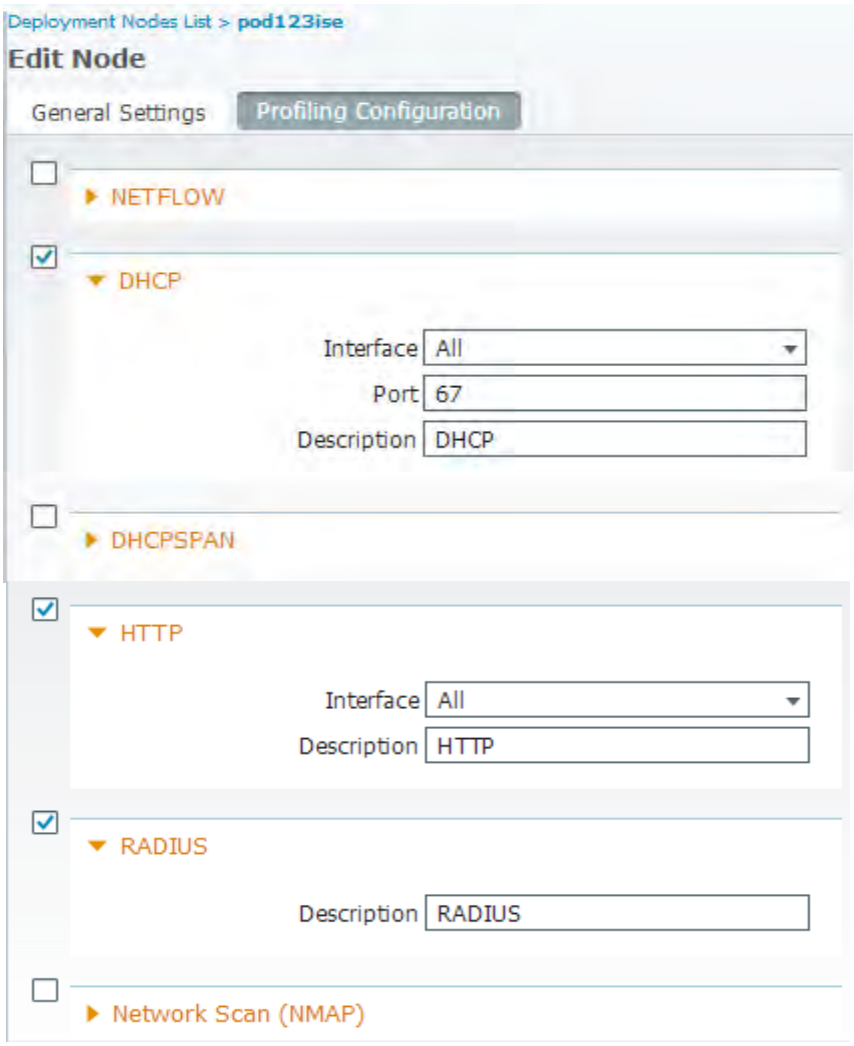
```
SW3#test aaa group radius test cisco123 legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

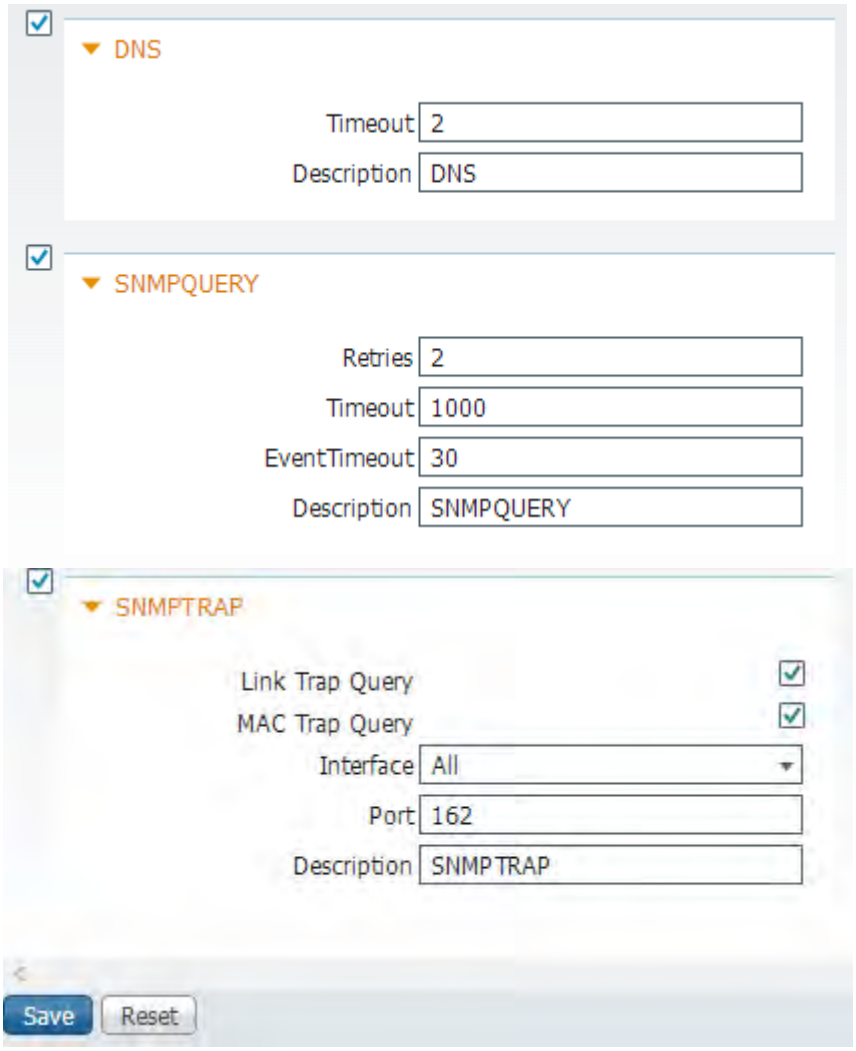
Task 2: Configure profiling.

- Enable profiling services on ISE. It should use DHCP probes, HTTP probes, RADIUS probes, DNS probes, SNMPQUERY probes and SMTPTRAP (all) probes on all interfaces for profiling.

Solutions

Step 1: Go to **Administration->System->Deployment**. Click on **podxxxise**. Then click on **Profiling Configuration** tab.

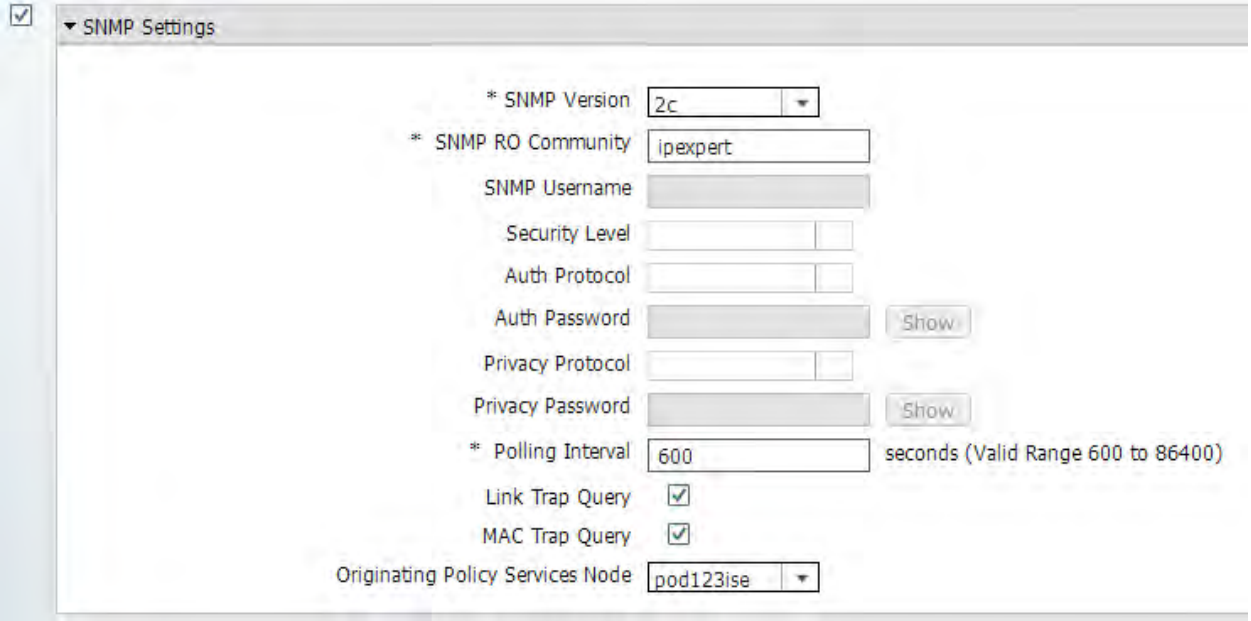




- Configure SNMP version 2c for AAA clients on ISE and on the NAD's with a community string of "ipexpert". Change the polling interval on ISE to the minimum possible.

Solutions

Step 1: Go **to Administration->Network Resources->Network Devices**. Click on the appropriate NAD's (SW2, SW3 and WLC) and configure SNMPv2c settings.



- Enable SNMP traps for linkup, linkdown, mac-notification change, mac-notification move on the NDA's/AAA clients. The SNMP trap and informs should be sourced from VLAN 10 interface.

Solutions

Step 1: Configure SNMPv2c on the switches as per the task

SW2 and SW3

```
snmp-server community ipexpert RW
snmp-server trap-source Vlan10
snmp-server source-interface informs Vlan10
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.1.1.150 version 2c ipexpert
```

- Configure additional DHCP helper address on SW3 pointing to the ISE server IP of 10.1.1.150 for SVI interfaces of VLAN 40, 50, 60, 200 and 250. AD has been preconfigured to be the DHCP servers for these VLAN's.

Solutions

Step 1: Configure additional DHCP helper address on the SVI's needed for profiling

SW2 and SW3

```
interface Vlan40
  ip helper-address 10.1.1.150
```

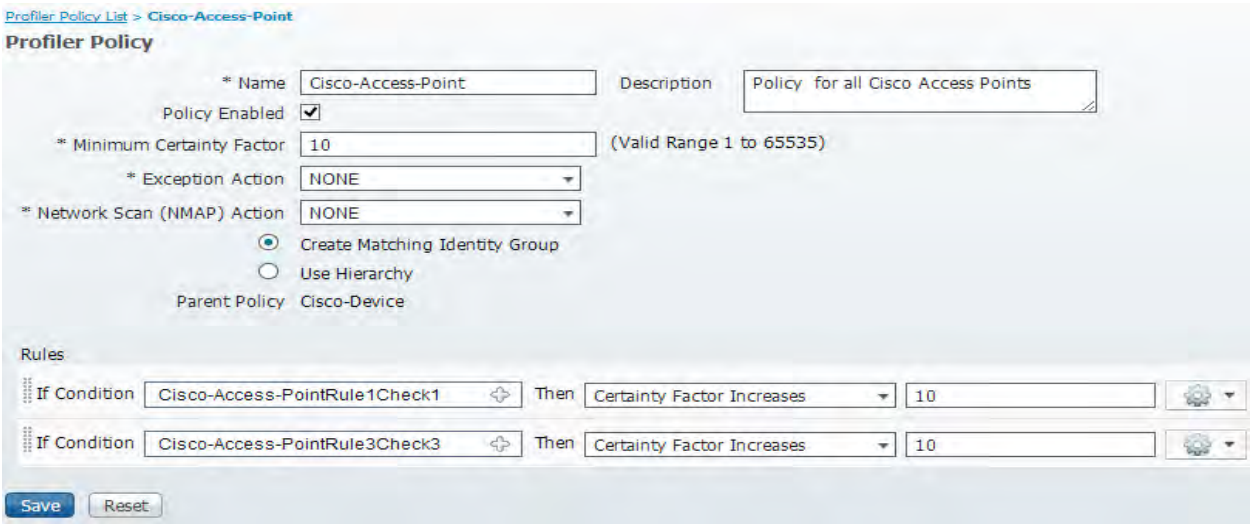
```
interface Vlan50
 ip helper-address 10.1.1.150

interface Vlan60
 ip helper-address 10.1.1.150

interface Vlan200
 ip helper-address 10.1.1.150

interface Vlan250
 ip helper-address 10.1.1.150
```

- Re-configure existing profiling policy to make sure that existing profiling policy “Cisco-IP-Phone” “Windows7-Workstation” and “Cisco-Access-Point” creates a matching endpoint identity group when devices match the profiling policy.

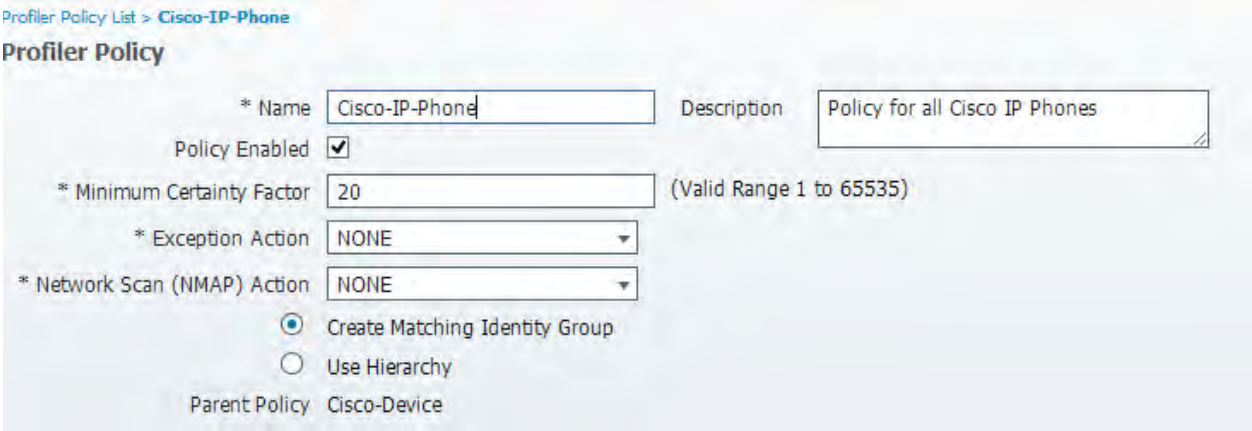
Solutions

Step 1: Go to **Policy-> Profiling -> Profiling Policies** and click on the appropriate profiling policies such that it creates a matching identity group.

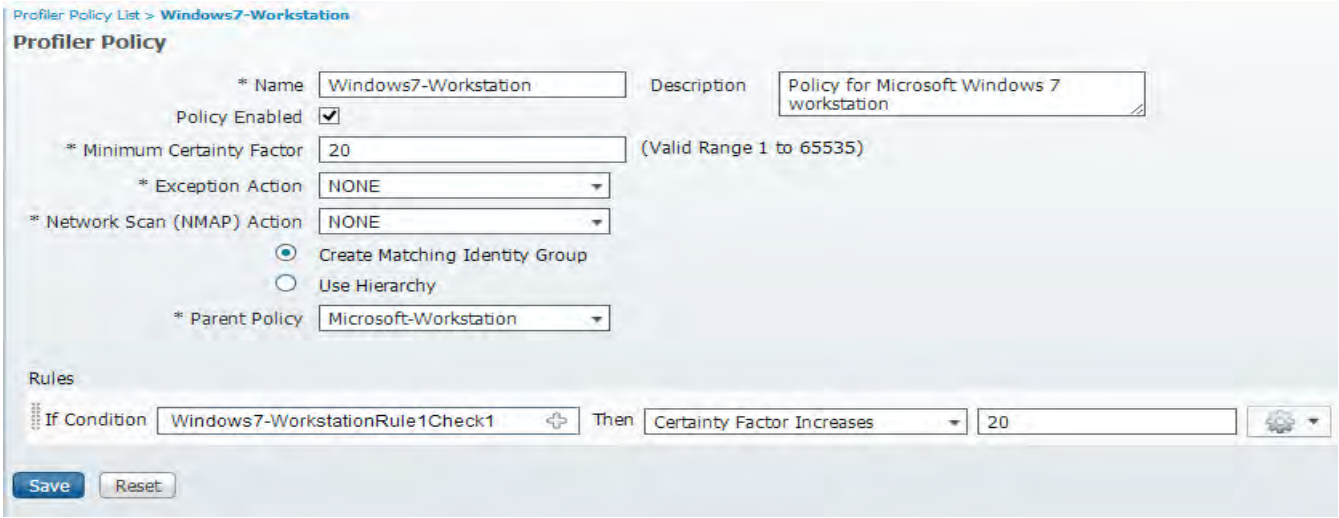
Modify “Cisco-Access-Point” profiling policy and click on **Save.**



“Cisco-Access-Point” profiling policy has a default of create matching identity group



Modify “Windows7-Workstation” profiling policy and click on **Save**.

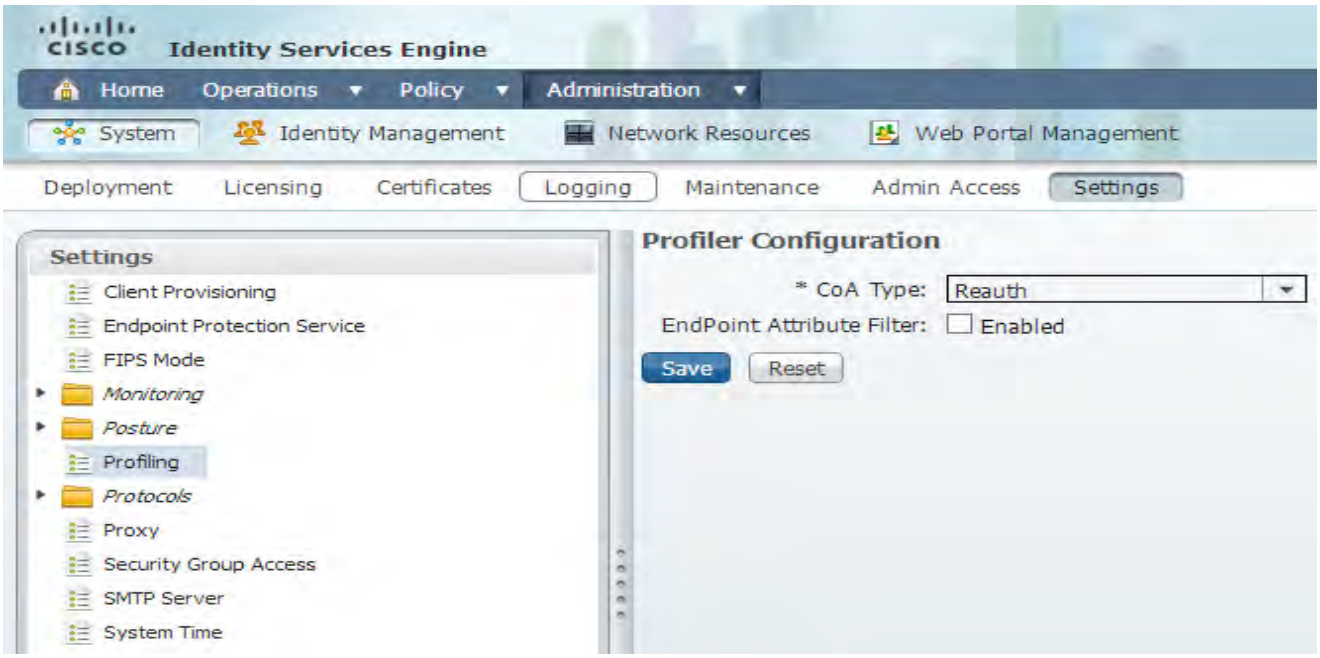


- Change the CoA for profiling to re-auth on the ISE globally.

Solutions

Step 1: Go to **Administration > System > Settings > Profiling**

Change the CoA Type to Reauth and click on Save.

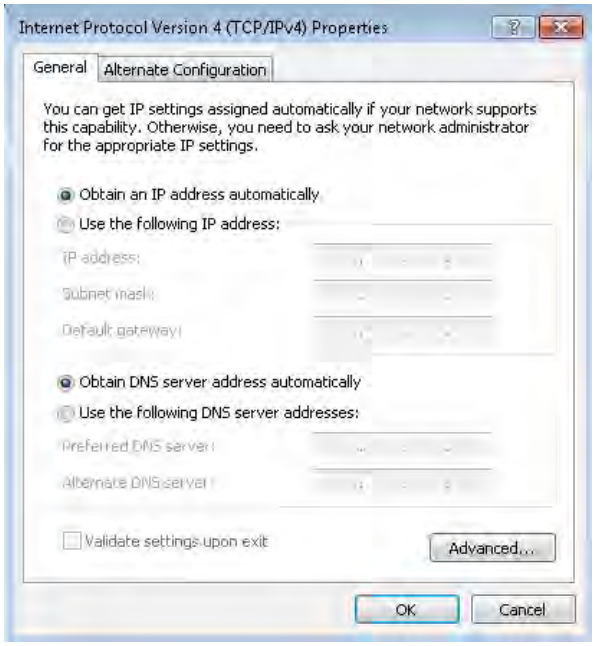


- Un-shut G1/0/12, G1/0/2 on SW3 and F0/22 to test profiling policy.

Solutions

Step 1: Un-Shut the interfaces as per the task. Make sure that the TEST-PC's can obtain the IP address automatically through DHCP. Also, add static route on the server for 192.168.0.0/16 subnet

```
C:\Users\Administrator>route add 192.168.0.0 mask 255.255.0.0 10.1.1.2
 OK!
```



SW2

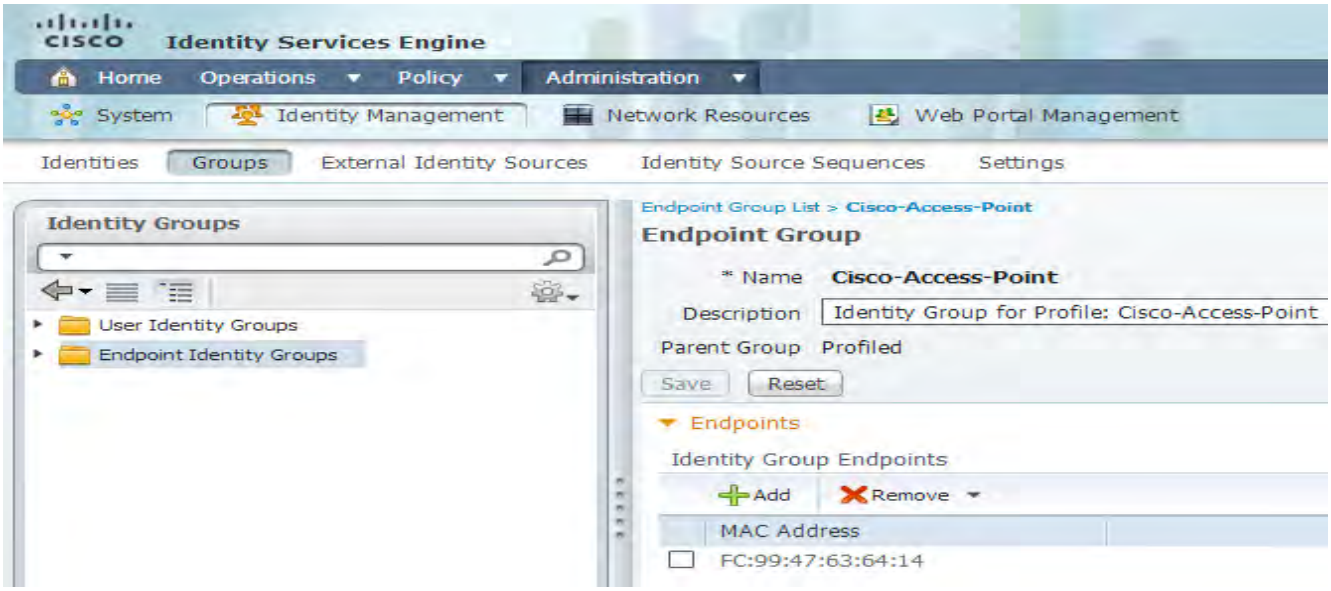
```
interface FastEthernet0/22
no shutdown
```

SW3

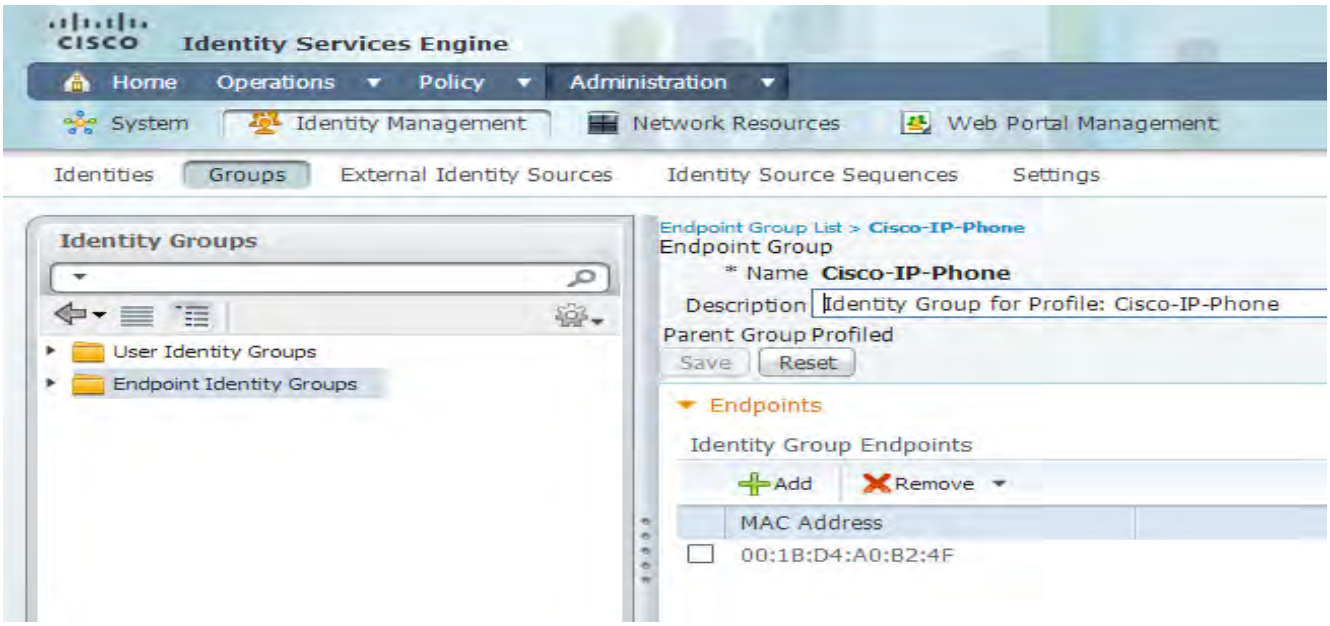
```
interface GigabitEthernet1/0/2
no shutdown

interface GigabitEthernet1/0/12
no shutdown
```

Navigate to **Administration-> Identity Management -> Groups -> Endpoint Identity Groups** and click on the appropriate endpoint group to verify if an endpoint MAC address entry exists.

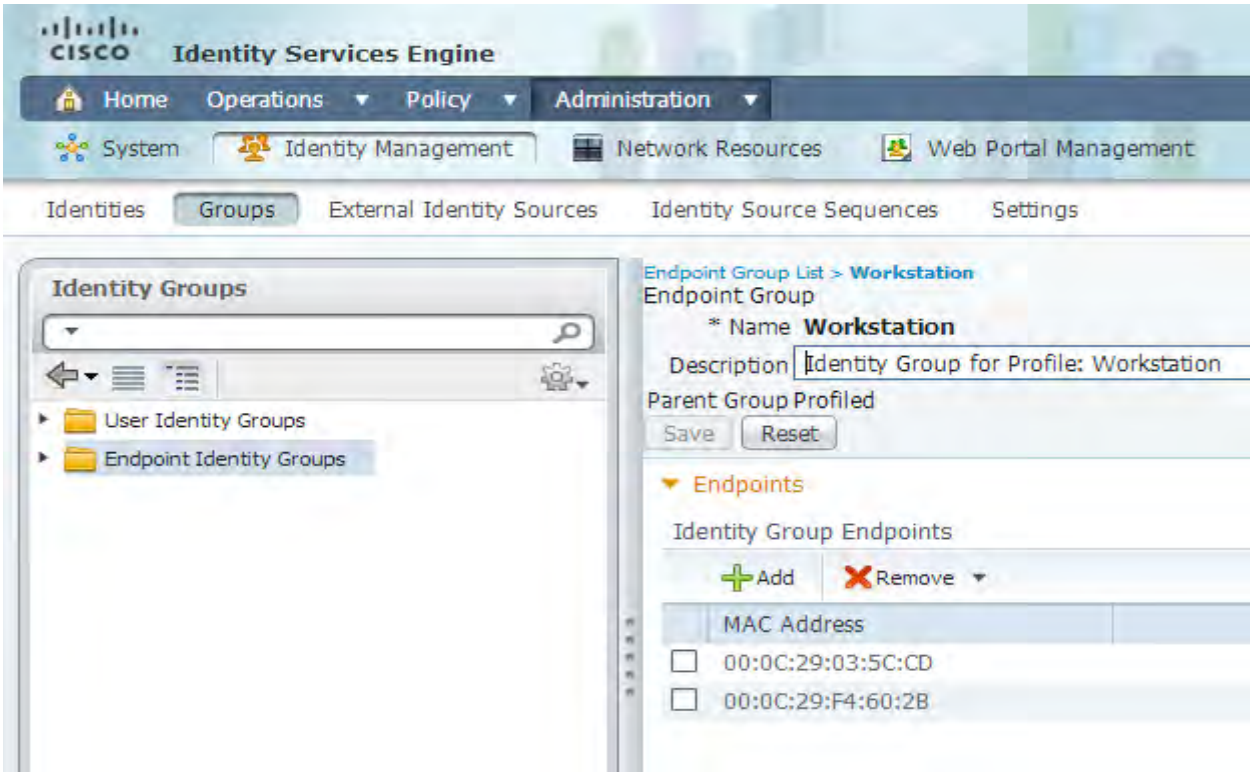
Verify from the Cisco-Access-Point identity group



Verify from the Cisco-IP-Phone identity group.



Verify from the Workstation identity group



Lab-3: Configuring ISE and Switches for MAB and 802.1x

Lab-3: Configuring ISE and switches for MAB and 802.1x– This lab is intended to familiarize you with configuring ISE with authentication and authorization policies for MAB and 802.1x for wired and wireless access. You will also be configuring switches for 802.1x with low impact mode, MAB and flex-auth and WLC for 802.1x authentication for wireless clients.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **5 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-2 successfully.
Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configuring AAA clients for wired MAB and 802.1x with low impact mode.

- Configure 802.1x globally on SW3 and SW2

Solutions:

SW2 & SW3

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
```

- Configure Access VLAN of 250 for SW3 G1/0/2 and G1/0/12 and VLAN 100 for G1/0/13. The voice VLAN for port G1/0/12 on SW3 should be set to 60.

Solutions

SW3

```
interface GigabitEthernet1/0/2
 switchport mode access
 spanning-tree portfast
 switchport access vlan 250

interface GigabitEthernet1/0/12
 switchport mode access
 spanning-tree portfast
 switchport access vlan 250
 switchport voice vlan 60
```

SW2

```
interface FastEthernet0/22
 switchport mode access
 spanning-tree portfast
 switchport access vlan 100
```

- Enable 802.1x and MAB on G1/0/12 and G1/0/2 on SW3 and F0/22 on SW2.

Solutions

SW2 & SW3

```
interface ()
 authentication port-control auto
 mab
 dot1x pae authenticator
```

- Configure Flex-auth for the above mention ports and change the order of authentication first to MAB and then to 802.1x method, however 802.1x authentication should have higher priority than MAB.

Solutions
SW2 & SW3

```
interface ()
 authentication order mab dot1x
 authentication priority dot1x mab
```

- Change the host mode to multi-auth and violation action to restrict.

Solutions
SW2 & SW3

```
interface ()
 authentication host-mode multi-auth
```

- Configure low impact mode and configure a port ACL that allows only DHCP, DNS, ICMP traffic. Log all the packets that are denied.

Solutions
SW2 & SW3

```
ip access-list extended ACL-DEFAULT-LIM
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
 permit tcp any any eq www
 permit tcp any any eq 443
 deny   ip any any log

interface GigabitEthernet1/0/XX
 authentication open
 ip access-group ACL-DEFAULT-LIM in
```

- Configure periodic re-authentication and the timeout values for re-authentication should be obtained from the ISE for G1/0/12 and G1/0/2 interfaces of SW3.

Solutions
SW3

```
interface GigabitEthernet1/0/XX
 authentication periodic
```

```
 authentication timer reauthenticate server
```

- Idle timeout value should be obtained from ISE for G1/0/2 of SW3

Solutions
SW3

```
interface GigabitEthernet1/0/2
 authentication periodic
  authentication timer inactivity server
```

- Change the 802.1x transmit timer to 10 seconds on all the ports configured for 802.1x.

Solutions
SW2 and SW3

```
interface ()
 dot1x timeout tx-period 10
```

- Switches should be configured to process RADIUS VSA for authentication and accounting

Solutions
SW2 and SW3

```
radius-server vsa send accounting
radius-server vsa send authentication
```

- Switches should include RADIUS attributes 6,8 and 25 in the RADIUS requests

Solutions
SW2 and SW3

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
```

- Configure CoA on the switches and enable device tracking.

Solutions
SW2 and SW3

```
ip device tracking probe use-svi
ip device tracking

aaa server radius dynamic-author
 client 10.1.1.150 server-key cisco123
```

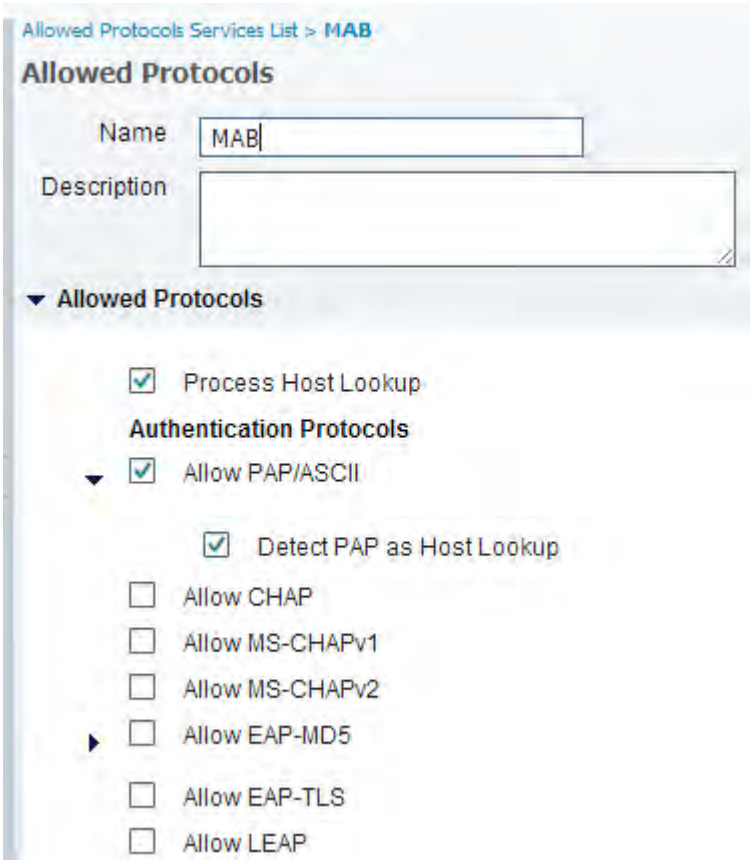
Task 2: Configuring ISE for wired MAB and 802.1x with low impact mode.

- Create a new authentication protocol result called “MAB” that allows only host lookup for MAB.

Solutions

Step 1: Go to **Policy -> Policy Elements -> Results -> Authentication -> Allowed Protocols**. Click on Add.

Select “Process Host Lookup” and “Detect PAP as Host Lookup” and uncheck all other protocols.

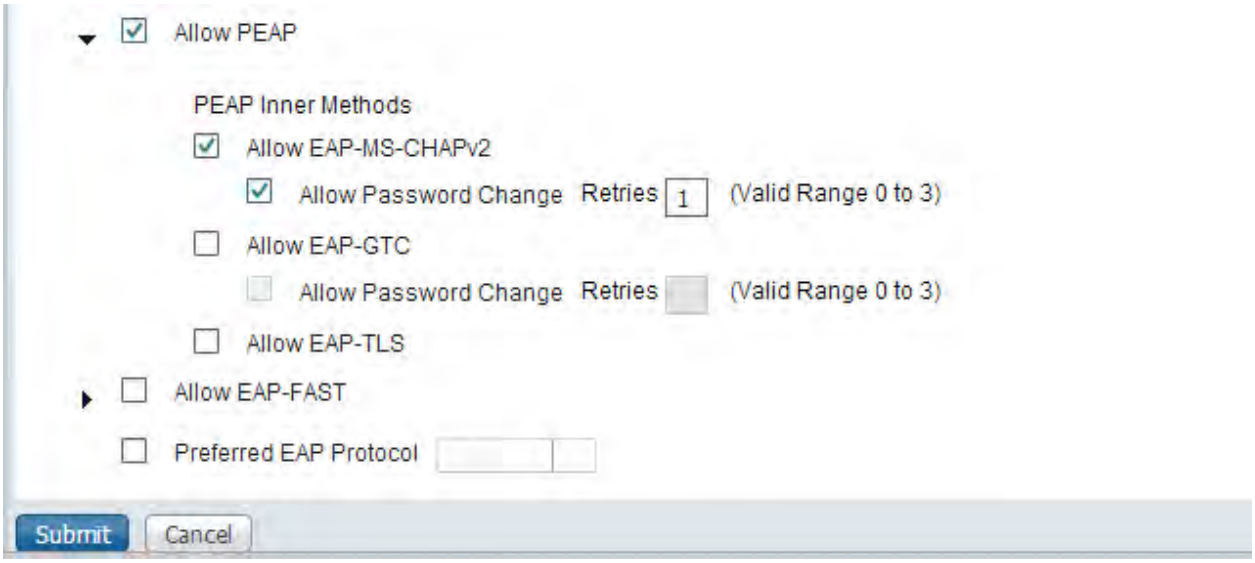


- Create a new authentication protocol result called “PEAP_MSCHAPv2” that allows only PEAP as the outer/tunneling method and the EAP-MS-CHAPv2 as the inner method for 802.1x authentications.

Solutions

Step 1: Go to **Policy -> Policy Elements -> Results -> Authentication -> Allowed Protocols**. Click on **Add**.

Select “Allow PEAP” and “Allow EAP-MS-CHAPv2” and uncheck all other protocols as per the task.



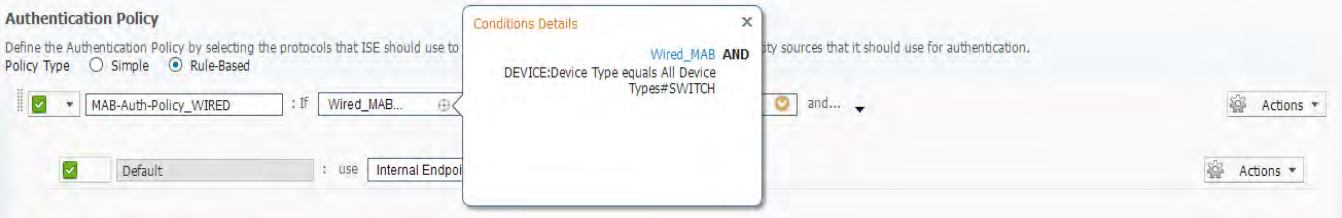
- Configure authentication policies as per the below table

Name		Condition		Protocols		Identity Source
MAB-Auth-Policy_WIRED	IF	Wired_MAB AND Device:Device Type = Device Type#All Device Types#SWITCH	allow protocols	MAB	and use	Internal Endpoints
Dot1X-Auth-Policy_WIRED	IF	Wired_802_1X AND Device:Device Type = Device Type#All Device Types#SWITCH	allow protocols	PEAP_MSCHAPv2	and use	AD_LOCAL
Default Rule (if no match)			allow protocols	Default Network Access	and use	AD_LOCAL

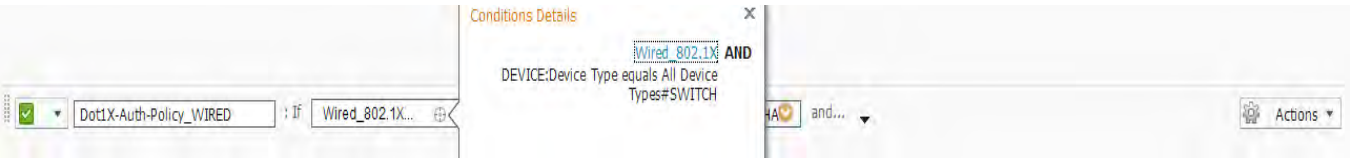
Solutions

Step 1: Go to **Policy->Authentication** and configure Authentication policies as per the task

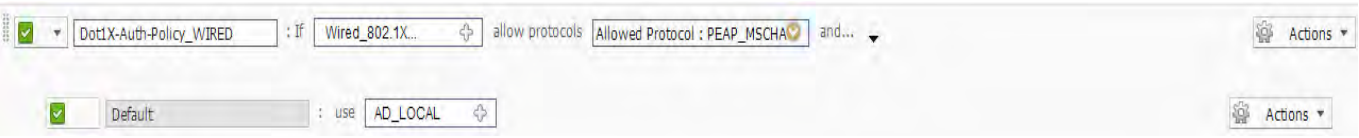
Create a policy called “MAB-Auth-Policy_WIRED” and add the condition for “MAB-Auth-Policy_WIRED” as per the task. Change the allowed protocol to “MAB”.



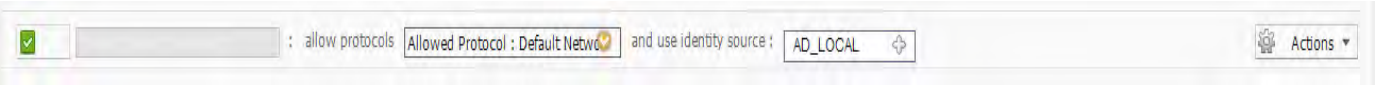
Create a policy called “Dot1X-Auth-Policy_WIRED” and add the condition for “Dot1X-Auth-Policy_WIRED” as per the task. Change the allowed protocol to “PEAP_MSCHAPv2”.



Make sure to change the authenticaion store to “AD_LOCAL”.



Change the default rule to use “AD_LOCAL” as identity store. Click on Save.



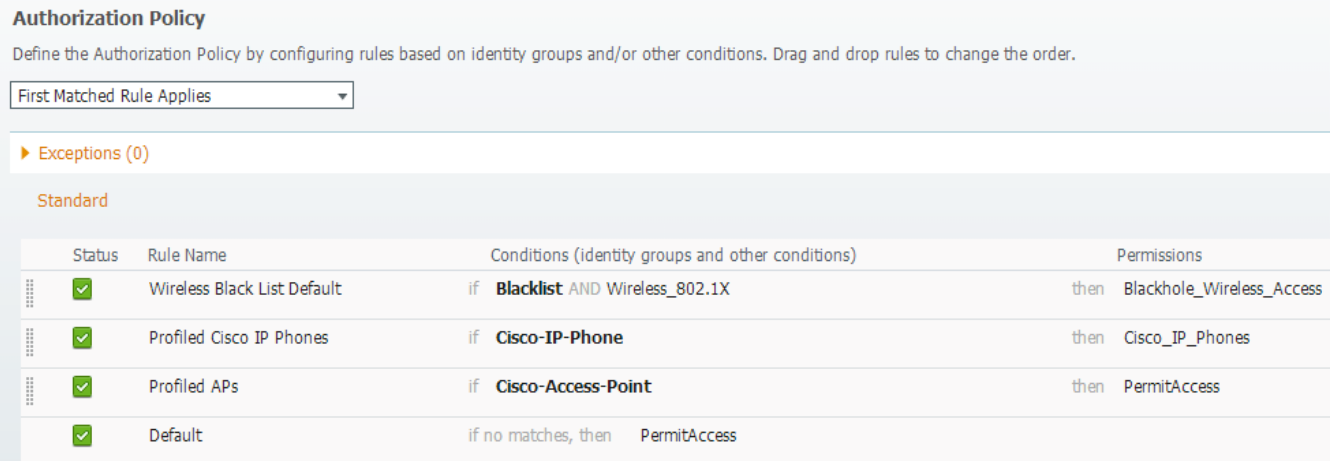
- To test MAB and 802.1x configure authorization policies as per the below table

Name		Identity Group		Conditions		Authorization
Profiled Cisco IP Phones	IF	Cisco-IP-Phone	AND	-	THEN	Cisco_IP_Phone
Profiled APs	IF	Cisco-Access-Point	AND	-	THEN	PermitAccess
Default	IF	no matches			THEN	PermitAccess

Solutions

Step 1: Go to **Policy->Authorization** and configure Authorization policies as per the task

Create a new authorization rule called “Profiled Aps”. Set the condition for this rule based on Endpoint Identity Group (Cisco-Access-Point). Select the “PermitAccess” authorization profile for this rule.



- Test the policies from SW3. MAB should be successful and the IP Phone should join the voice domain based on “Cisco_IP_Phone” pre-defined authorization profile.

Shut and unshut G1/0/12 on SW3 and verify.

```
SW3#show authentication sessions interface gigabitEthernet 1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  Unknown
            User-Name:  00-0C-29-F4-60-2B
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A801030000007B05CECAFF
      Acct Session ID:  0x00000058
               Handle:  0x7300007C

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

```
----------------------------------------
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4a0.b24f
           IP Address:  192.168.60.10
            User-Name:  00-1B-D4-A0-B2-4F
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-508adc03
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A801030000007A05CE7789
      Acct Session ID:  0x00000057
               Handle:  0x7900007B

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

- RDP into TEST-PC2 and configure it for 802.1x.

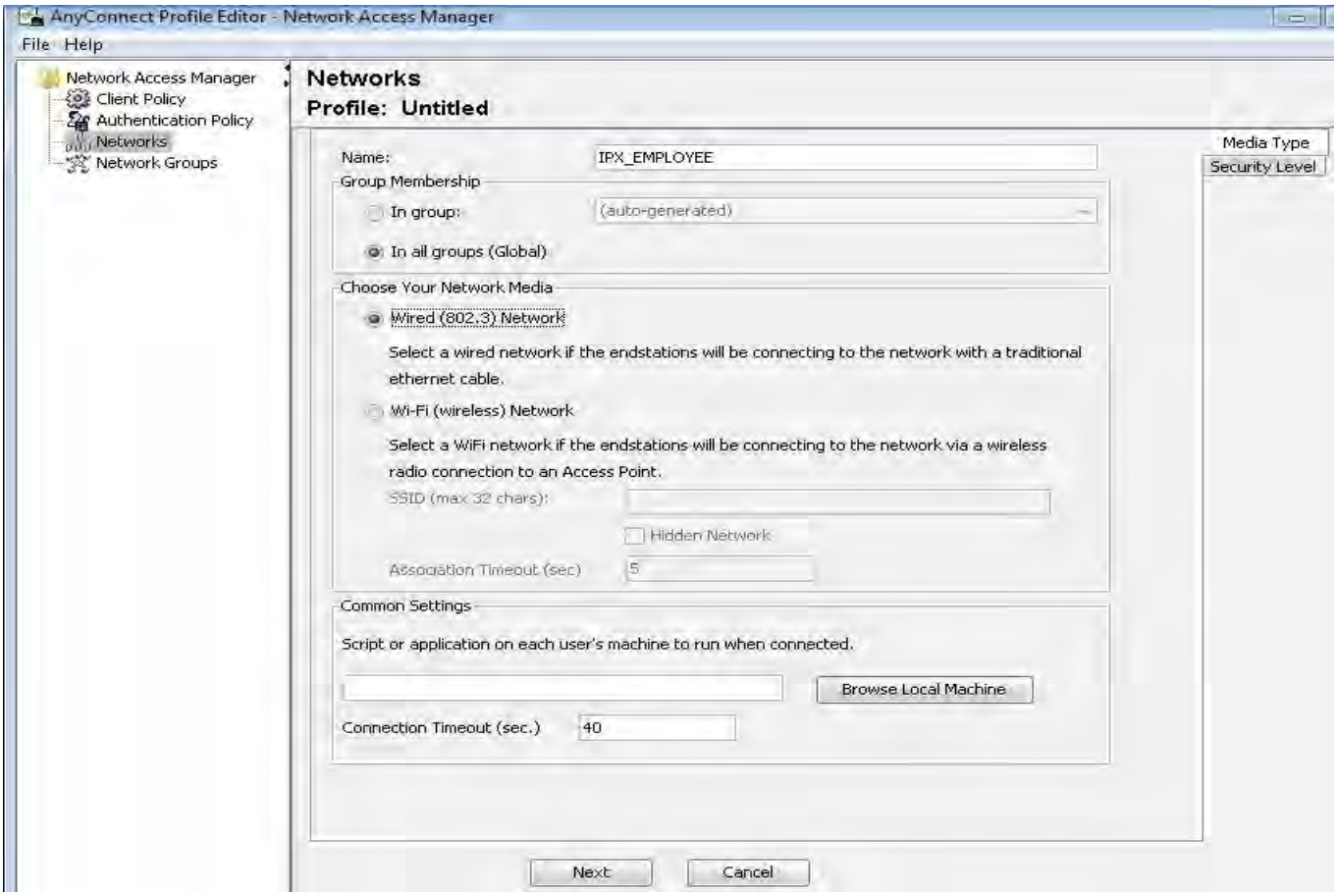
- Configure anyconnect profile using NAM profile editor called “IPX_EMPLOYEE” and test 802.1 x authentications. Test using “IPXEMP1/cisco” as the login details for 802.1x. Make sure anyconnect always prompts the user for username and password and does not store the credentials.

- For testing purposes, you are allowed to configure static routes on the PC. Do not set the default gateway. PC will automatically get the IP address from the pre-configured DHCP server.

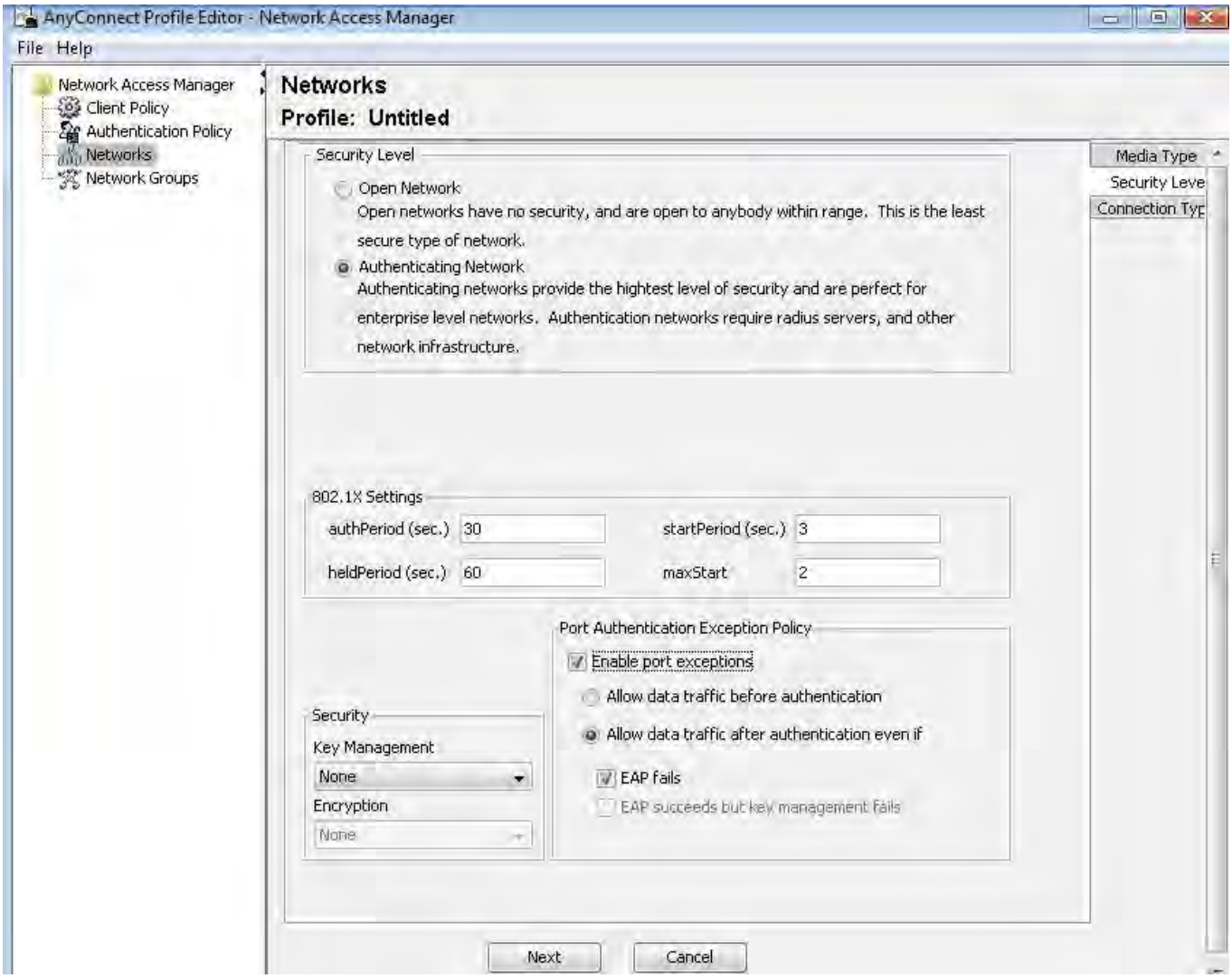
Solutions

Step 1: RDP into TEST-PC2 and configure a new anyconnect profile for 802.1x using NAM editor as per the task.

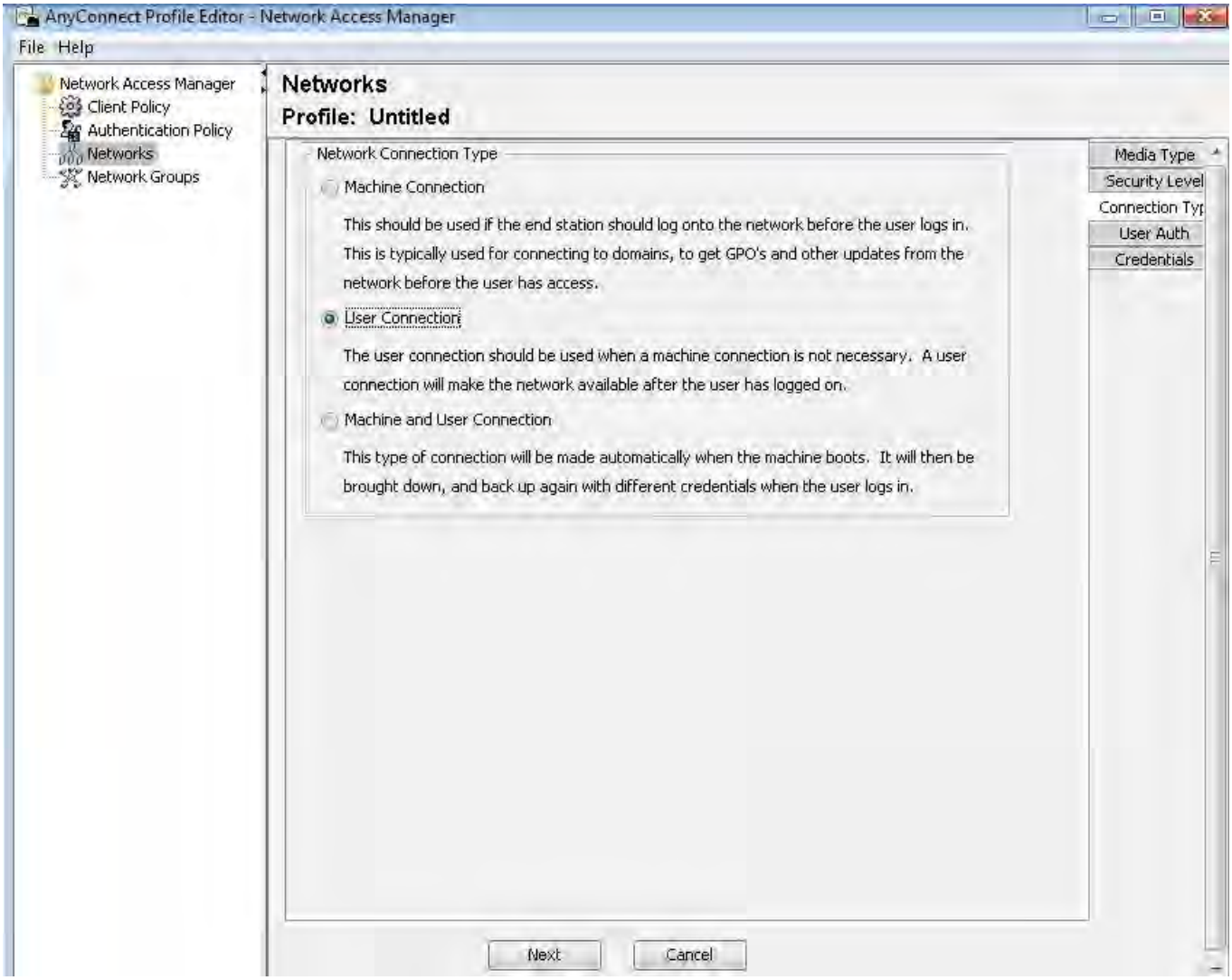
Use a profile name of “IPX_EMPLOYEE” select “In all groups (Global)” and choose wired network. Then click Next.



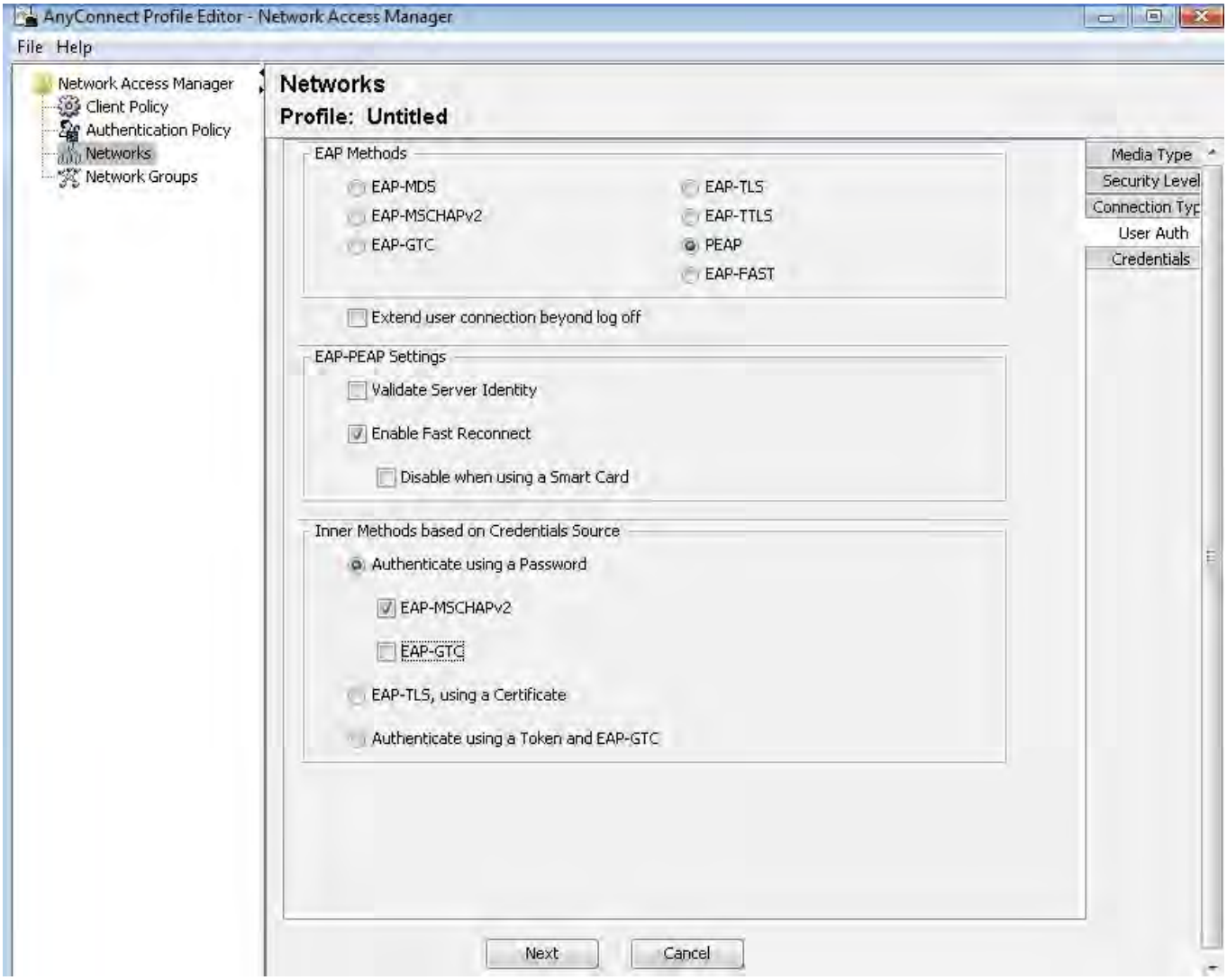
Choose “Authenticating Network” and enable port exceptions when EAP fails. Then click Next.



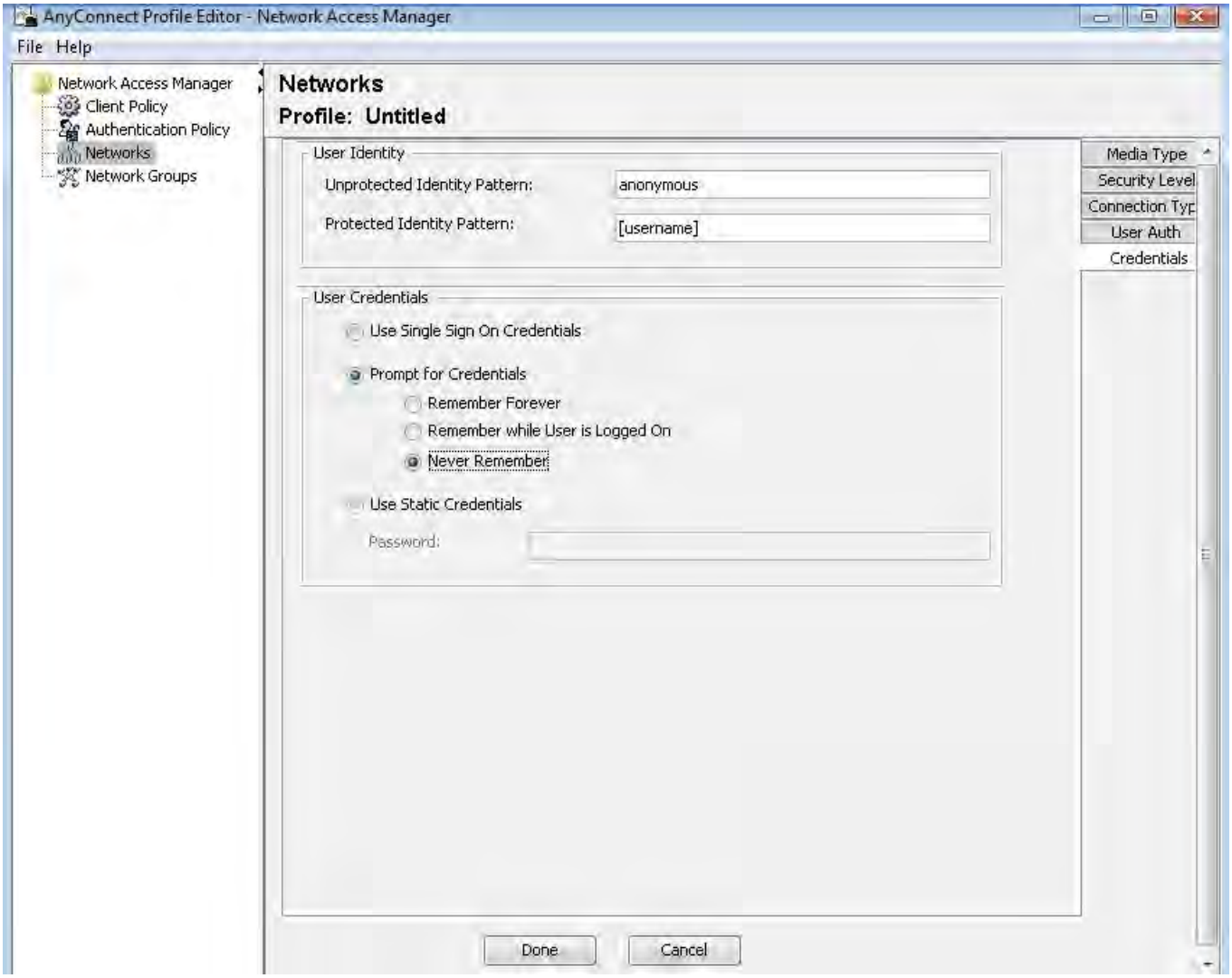
Choose User Connection. Then click Next.



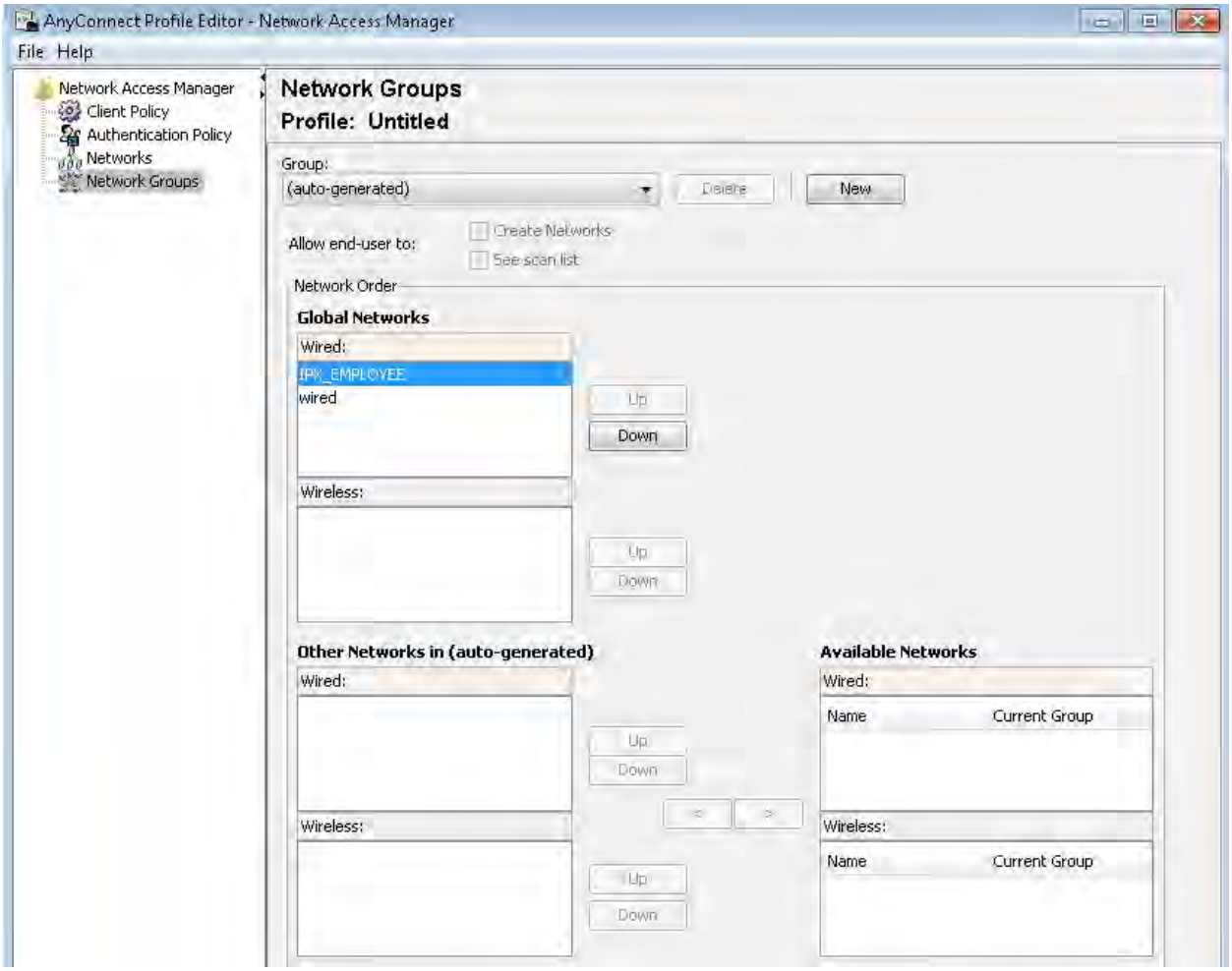
Choose PEAP and inner method of EAP-MSCHAPv2. Then click Next.



Choose prompt credentials. Then click Next.

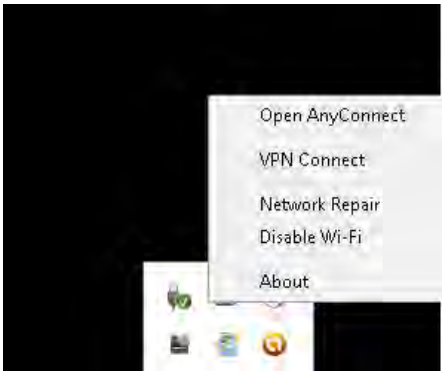


Move IPX_EMPLOYEE profile above the wired on the Global Networks. If you want you can remove the wired policy.

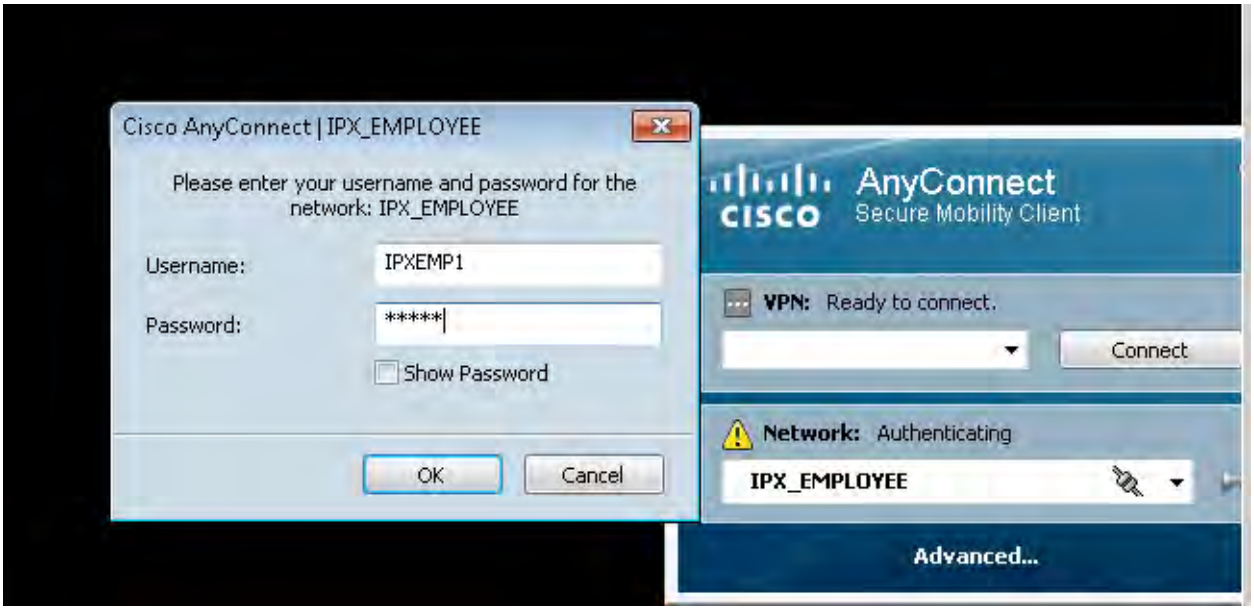


Save As configuration.xml

Perform a Network Repair for the anyconnect



Enter the username/password for 802.1x (IPXEMP1/cisco)



Verify on SW3

```
SW3#sh auth sessions interface g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  192.168.250.16
            User-Name:  IPXEMP1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
```

```
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000086063E7AD8
      Acct Session ID:  0x00000071
               Handle:  0x82000087

Runnable methods list:
       Method   State
       mab      Not run
       dot1x    Authc Success

----------------------------------------
           Interface:  GigabitEthernet1/0/12
         MAC Address:  001b.d4a0.b24f
          IP Address:  192.168.60.10
           User-Name:  00-1B-D4-A0-B2-4F
              Status:  Authz Success
              Domain:  VOICE
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-508adc03
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000087063ED245
      Acct Session ID:  0x00000072
               Handle:  0x51000088

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

Task 3: Configuring ISE with specific authorization policies.

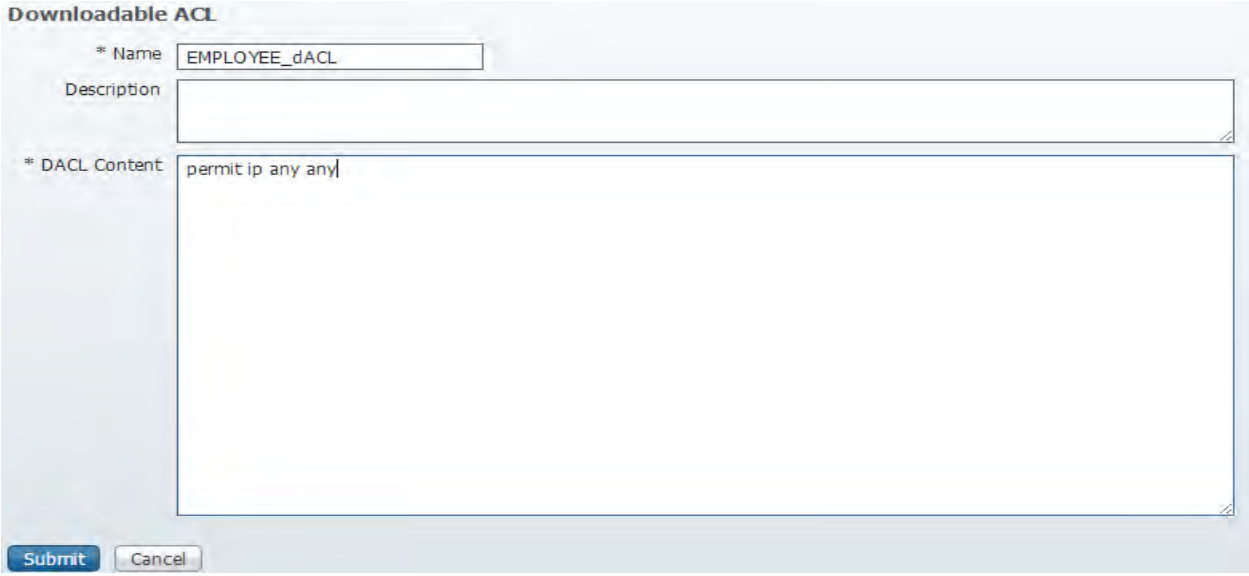
- Configure policies for employees in your network. Employees belong to “IPX_EMP” group in the AD. After successful authentication/authorization they should be given complete access with a change of VLAN from 250 to 40. VLAN 250 is the default restricted configured on the switchport and VLAN 40 is the employee VLAN.

- Configure dACL for employees as per the below table.

Downloadable ACL	
Name	EMPLOYEE_dACL
DACL Content	permit ip any any

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Downloadable ACLs**. Click on **Add.**



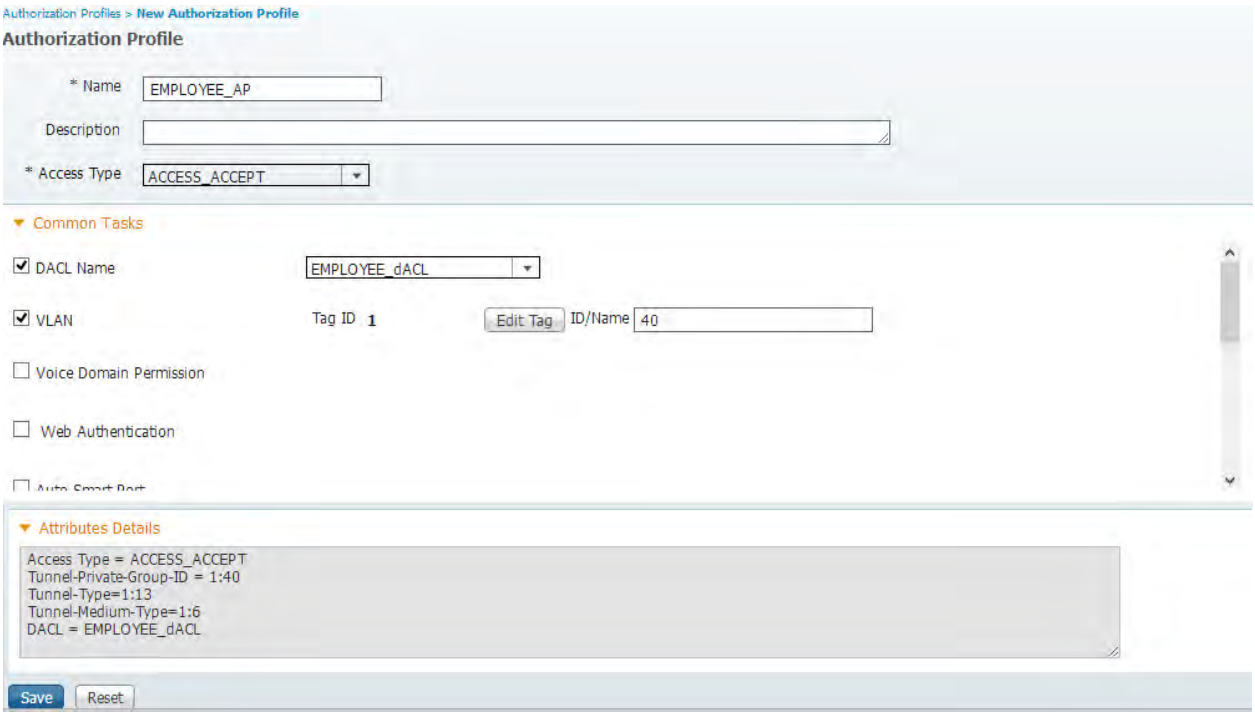
- Configure Authorization profile for employees as per the below table.

Authorization Profile	
Name	EMPLOYEE_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	EMPLOYEE_dACL
VLAN	40

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Click on **Add.**

Create the Employee authorization profile as per the task and click on submit



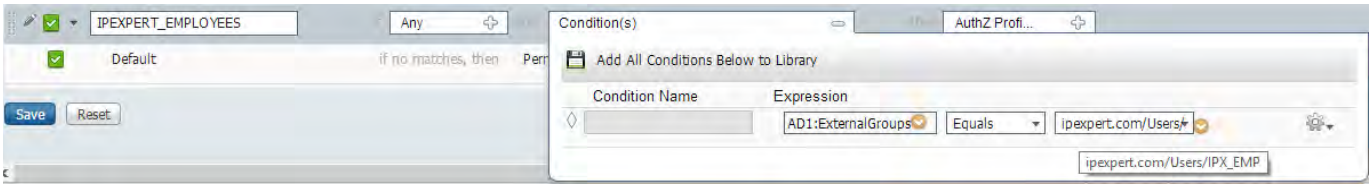
- Configure Authorization policies for employees as per the below table

Name		Identity Group		Conditions		Authorization
IPEXPERT_EMPLOYEES	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/**IPX_EMP**	THEN	EMPLOYEE_AP
Default	IF	no matches			THEN	DenyAccess

Solutions

Step 1: Go to **Policy->Authorization** and configure Authorization policies as per the task

Create a new authorization rule called “IPEXPERT_EMPLOYEES”. Set the condition for this rule based on AD group as per the task. Select the “EMPLOYEE_AP” authorization profile for this rule.



Choose EMPLOYEE_AP as the result/authorization profile for this policy and then click on save.

- RDP into TEST-PC2 and login as “IPXEMP1/cisco” and test the above created rule.

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID :	C0A8010300000086063E7AD8
AAA session ID :	pod123ise/84321195/646
Date :	January 14,2011

Generated on January 14, 2011 1:31:26 PM UTC

Actions
Troubleshoot Authentication
View Diagnostic Messages
Audit Network Device Configuration
View Network Device Configuration
View Server Configuration Changes

Authentication Summary	
Logged At:	January 14,2011 1:27:09.748 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	IPXEMP1
MAC/IP Address:	00:0C:29:F4:60:2B
Network Device:	SW3 : 192.168.1.3 : GigabitEthernet1/0/12
Allowed Protocol:	PEAP_MSCHAPv2
Identity Store:	AD1
Authorization Profiles:	EMPLOYEE_AP
SGA Security Group:	

Authentication Protocol :	PEAP(EAP-MSCHAPv2)

Authentication Result

User-Name=IPXEMP1
State=ReauthSession:C0A80103000000B40BADCA18
Class=CACS:C0A80103000000B40BADCA18:pod123ise/84321195/800
Termination-Action=RADIUS-Request
Tunnel-Type=(tag=1) VLAN
Tunnel-Medium-Type=(tag=1) 802
Tunnel-Private-Group-ID=(tag=1) 40
EAP-Key-Name=19:4d:30:b0:ef:e9:23:e1:18:f8:d5:a0:aa:61:c1:64:23:b5:f8:39:a8:d2:74:0a:55:b4:31:dc:d1:05:49:02:96:4d:30:b0:d4:41:1f:d4:c0:ee:f8:18:1a:4b:d3:12:09:2e:45:e0:a9:66:9b:5a:26:fe:9c:34:c2:9f:8e:17:af
MS-MPPE-Send-Key=b2:e4:25:b9:04:c2:fb:ac:36:f9:cc:3c:cf:9b:f5:6a:35:3b:36:c7:6d:cc:45:fd:36:a5:9e:ea:e7:63:f8:10
MS-MPPE-Recv-Key=20:85:e3:8d:3c:f4:48:e4:82:0a:4d:49:a0:59:c9:bb:b9:5f:90:c4:53:5a:c1:86:06:ed:c7:a0:0c:b1:b2:b8

Related Events

Authentication Details

Logged At:	January 14,2011 1:27:09.748 PM
Occurred At:	January 14,2011 1:27:09.747 PM
Server:	pod123ise
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
Username:	IPXEMP1
RADIUS Username :	anonymous
Calling Station ID:	00:0C:29:F4:60:2B
Framed IP Address:	192.168.250.16
Use Case:	
Network Device:	SW3
Network Device Groups:	Device Type#All Device Types#SWITCH,Location#All Locations
NAS IP Address:	192.168.1.3
NAS Identifier:	
NAS Port:	50112
NAS Port ID:	GigabitEthernet1/0/12
NAS Port Type:	Ethernet
Allowed Protocol:	PEAP_MSCHAPv2
Service Type:	Framed
Identity Store:	AD1
Authorization Profiles:	EMPLOYEE_AP

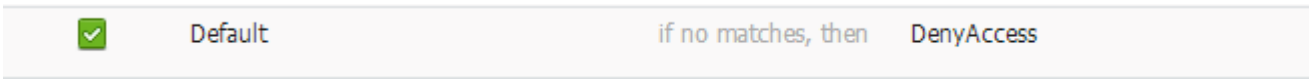
Active Directory Domain:	IPEXPERT.COM
Identity Group:	Profiled:Workstation
Allowed Protocol Selection Matched Rule:	Dot1X-Auth-Policy_WIRED
Identity Policy Matched Rule:	Default
Selected Identity Stores:	AD1,Internal Users
Authorization Policy Matched Rule:	IPEXPERT_EMPLOYEES
SGA Security Group:	
AAA Session ID:	pod123ise/84321195/646
Audit Session ID:	C0A8010300000086063E7AD8
Tunnel Details:	
Cisco-AVPairs:	service-type=Framed audit-session-id=C0A8010300000086063E7AD8
Other Attributes:	ConfigVersionId=10,DestinationPort=1812,Protocol=Radius,Framed-MTU=1500,State=37CPMSessionID=C0A8010300000086063E7AD8;32Se Name=,ExternalGroups=ipexpert.com/users/ipx_emp,ipexpert.com/users/d replication group,ipexpert.com/builtin/adminis users,CPMSessionID=C0A8010300000086063E7AD8,EndPointMACAddre Workstation,HostIdentityGroup=Endpoint Identity Groups:Profile Types#SWITCH,Location=Location#All Locations,Device IP Address=192.1
Posture Status:	NotApplicable
EPS Status:	

Steps
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
Evaluating Service Selection Policy
15048 Queried PIP
15048 Queried PIP
15048 Queried PIP
15004 Matched rule
11507 Extracted EAP-Response/Identity
12300 Prepared EAP-Request proposing PEAP with challenge
12625 Valid EAP-Key-Name attribute received
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12302 Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as n
12319 Successfully negotiated PEAP version 1
12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message

12810 Prepared TLS ServerDone message
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12319 Successfully negotiated PEAP version 1
12812 Extracted TLS ClientKeyExchange message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12509 EAP-TLS full handshake finished successfully
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12313 PEAP inner method started
11521 Prepared EAP-Request/Identity for inner EAP method
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11522 Extracted EAP-Response/Identity for inner EAP method
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method
Evaluating Identity Policy
15006 Matched Default Rule
15013 Selected Identity Store - AD1

24430 Authenticating user against Active Directory
24402 User authentication against Active Directory succeeded
22037 Authentication Passed
11824 EAP-MSCHAP authentication attempt passed
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814 Inner EAP-MSCHAP authentication succeeded
11519 Prepared EAP-Success for inner EAP method
12314 PEAP inner method finished successfully
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12306 PEAP authentication succeeded
11503 Prepared EAP-Success
24423 ISE has not been able to confirm previous successful machine authentication for user in A
Evaluating Authorization Policy
15048 Queried PIP
15004 Matched rule
15016 Selected Authorization Profile - EMPLOYEE_AP
11002 Returned RADIUS Access-Accept

Change the default rule to deny access.




```
SW3#show authentication sessions interface g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  192.168.40.10
            User-Name:  IPXEMP1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  40
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000B40BADCA18
      Acct Session ID:  0x000000A3
               Handle:  0xAA0000B5

Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Authc Success

----------------------------------------
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4a0.b24f
           IP Address:  192.168.60.10
            User-Name:  00-1B-D4-A0-B2-4F
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
```

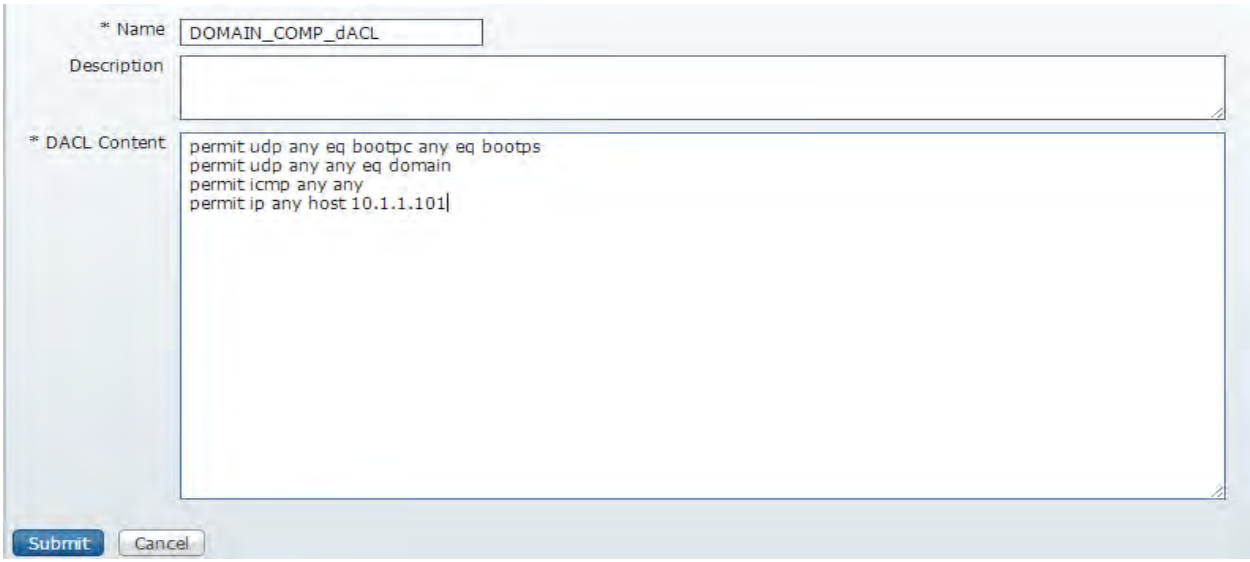
```
        Oper host mode:  multi-auth
      Oper control dir:  both
         Authorized By:  Authentication Server
               ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-508adc03
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  C0A80103000000B50BADF351
       Acct Session ID:  0x000000A4
                Handle:  0xCB0000B6

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

- Configure policies for Machine Authentication for Domain Computers.
- Configure dACL for authenticated domain computers as per the below table.

Downloadable ACL	
Name	DOMAIN_COMP_dACL
DACL Content	permit udp any eq bootpc any eq bootps permit udp any any eq domain permit icmp any any permit ip any host 10.1.1.101

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Downloadable ACLs**. Click on **Add.**

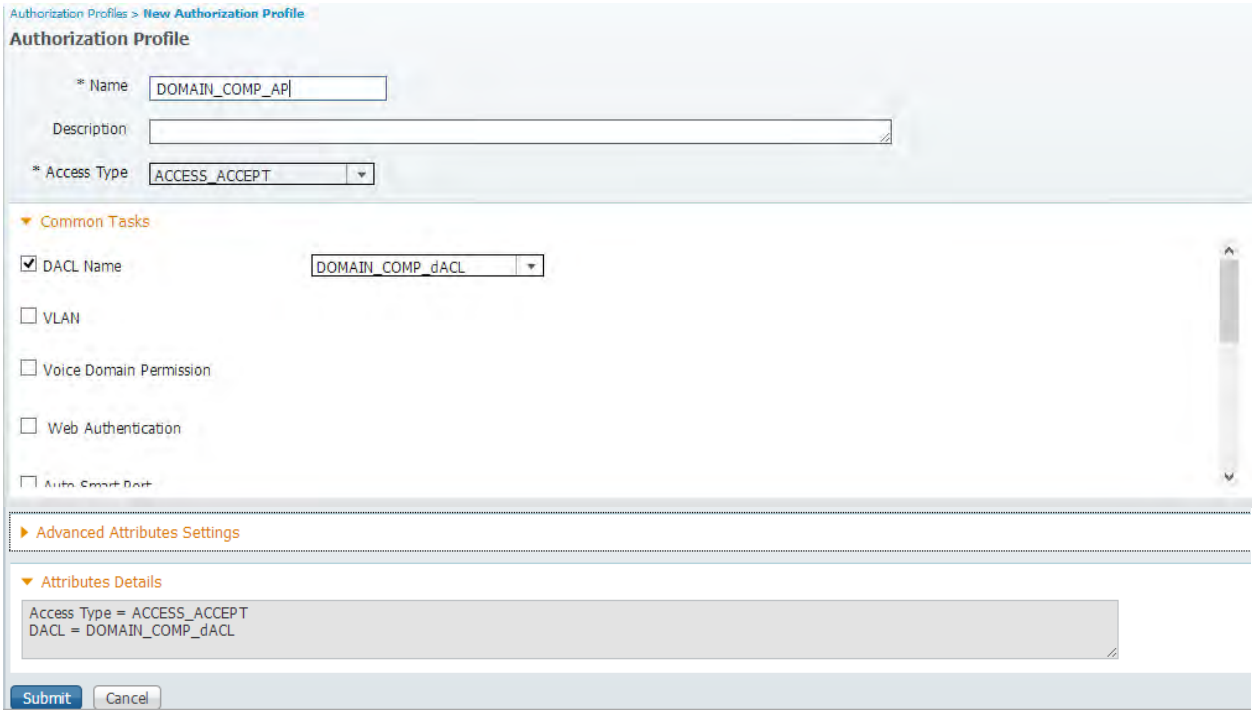


- Configure Authorization profile for domain computers as per the below table.

Authorization Profile	
Name	DOMAIN_COMP_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	DOMAIN_COMP_dACL

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Click on **Add.**



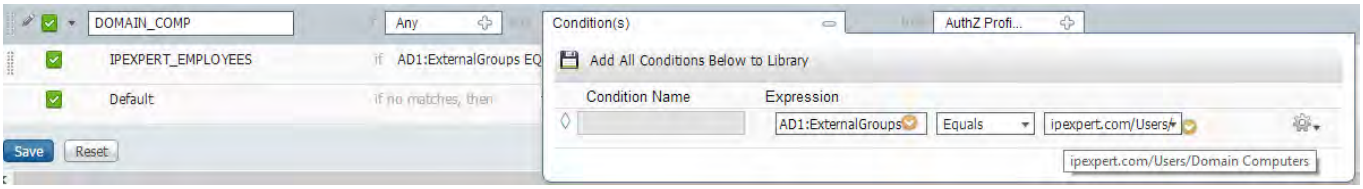
- Configure Authorization policy for machine authentication as per the below table

Name		Identity Group		Conditions		Authorization
DOMAIN_COMP	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/**Domain Computers**	THEN	DOMAIN_COMP_AP

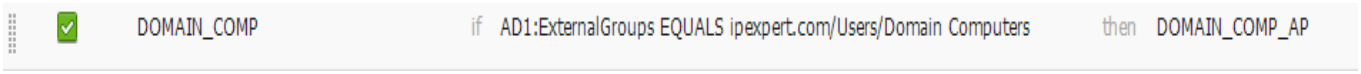
Solutions

Step 1: Go to **Policy->Authorization** and configure Authorization policies as per the task

Create a new authorization rule called “DOMAIN_COMP”. Set the condition for this rule based on AD group as per the task. Select the “DOMAIN_COMP_AP” authorization profile for this rule.



Select the correct Authorization profile and click on save after editing the rule.



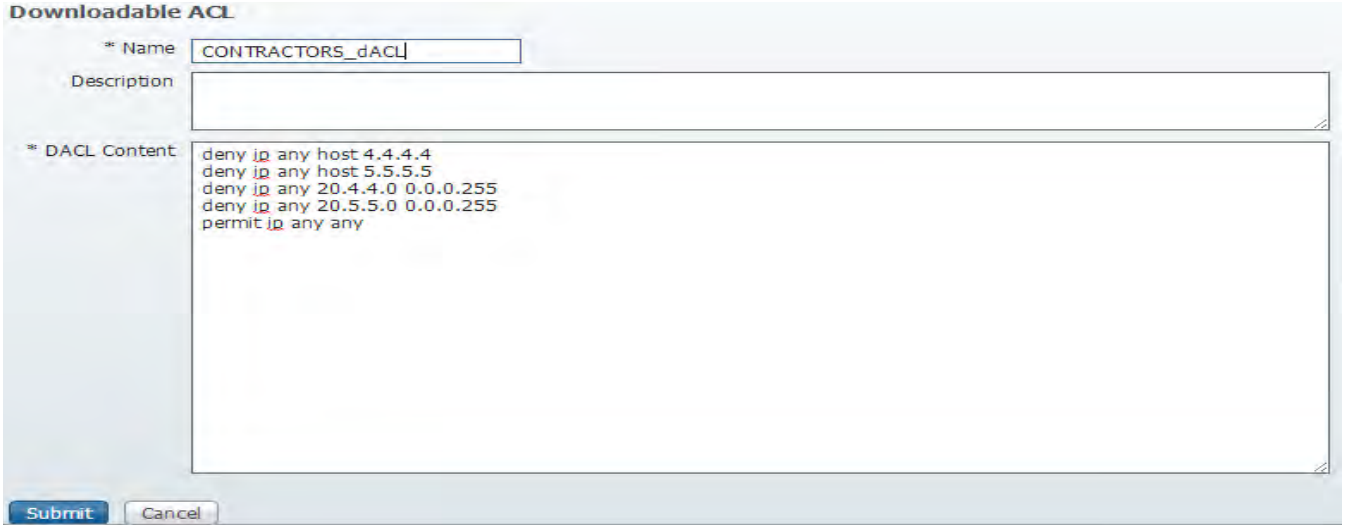
- Configure policies for contractors in your network. Contractors belong to “IPX_CON” group in the AD. After successful authentication/authorization they should be given complete access except to the data centers. Configure a change of VLAN from 250 to 50. VLAN 250 is the default restricted configured on the switchport and VLAN 50 is the Contractor’s VLAN. Configure Machine access restriction for contractors when they are connecting via wired network i.e. switch. They should re-authenticate every 8 hours

- Configure dACL for employees as per the below table. They should not be given access to the data centers.

Downloadable ACL	
Name	CONTRACTORS_dACL
DACL Content	deny ip any host 4.4.4.4 deny ip any host 5.5.5.5 deny ip any 20.4.4.0 0.0.0.255 deny ip any 20.5.5.0 0.0.0.255 permit ip any any

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Downloadable ACLs**. Click on **Add.**

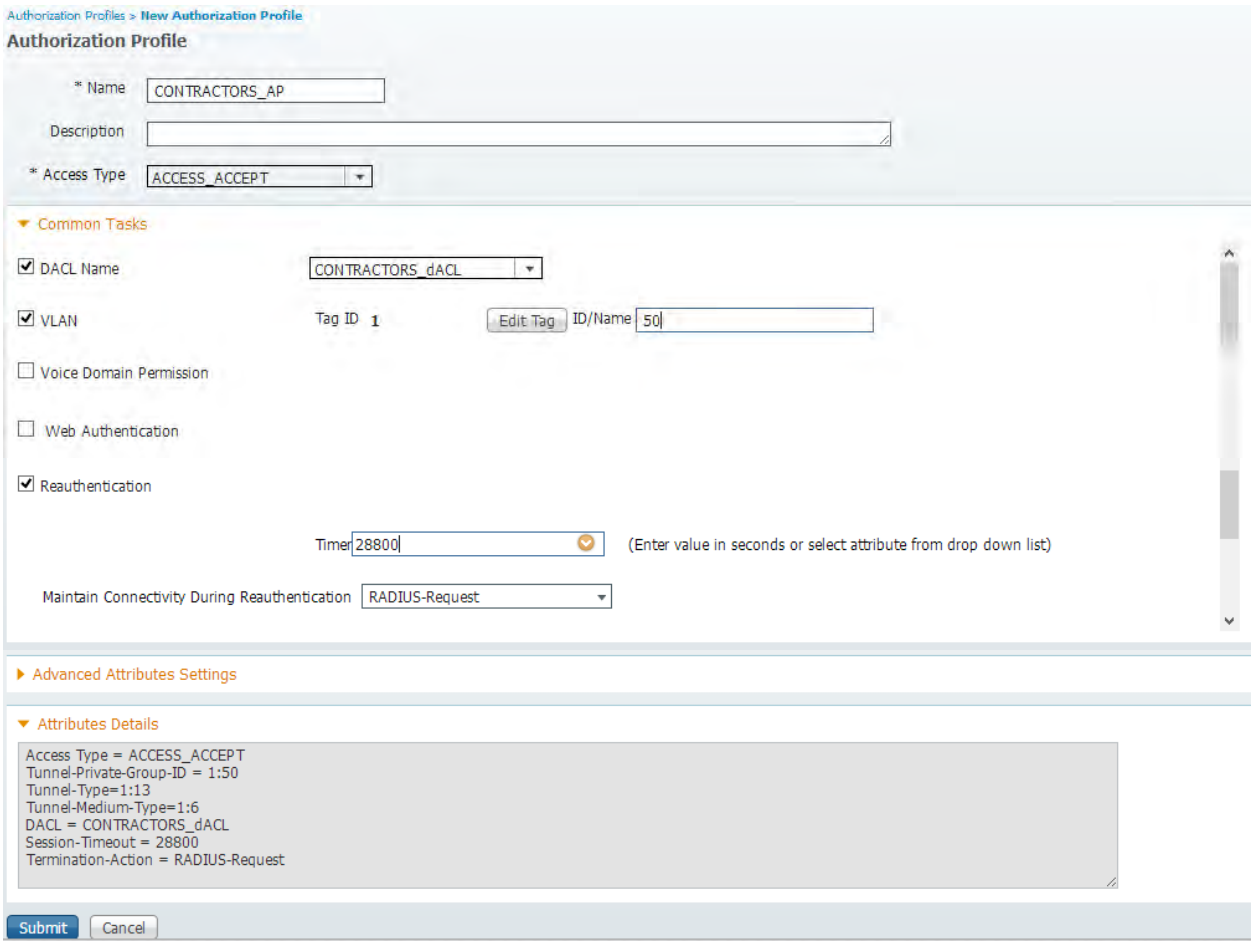


- Configure Authorization profile for contractors as per the below table.

Authorization Profile	
Name	CONTRACTORS_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	CONTRACTORS_dACL
VLAN	50
REAUTHENTICATION	28800
Radius:Termination-Action	RADIUS-Request

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Click on **Add.**



- Configure Authorization policy for contractors as per the below table.

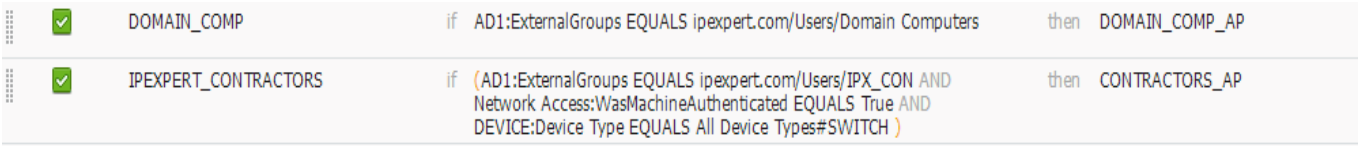
Name		Identity Group		Conditions		Authorization
IPEXPERT_CONTRACTORS	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/**IPX_CON** AND Network Access:WasMachineAuthenticated EQUALS **True** AND DEVICE:Device Type EQUALS All Device Types**#SWITCH**	THEN	CONTRACTORS_AP

Solutions

Step 1: Go to **Policy->Authorization** and configure Authorization policies as per the task

Create a new authorization rule called “IPEXPERT_CONTRACTORS”. Set the condition for this rule based on AD group as per the task. Select the “CONTRACTORS_AP” authorization profile for this rule.

Create this authorization rule below “DOMAIN_COMP” rule.



Task 4: Configuring WLC and ISE for Wireless 802.1x

Configure CAT 3 for trunking to WLC

```
interface GigabitEthernet1/0/13
 switchport trunk encap dot1q
 switchport mode trunk
 spanning-tree portfast trunk
```

Before you start this task make sure to initialize the WLC as per the below parameters

Initialize WLC with the following information:

- Administrator name MUST be “admin” and password “IPexpert123”
- SSID XXX_IPX_MGT where XXX is your pod number
- Management IP address should be 10.1.1.250
- Virtual Gateway IP should be 111.111.111.111
- Set User Mobility/RF Group name “RFGROUPXXX” where XXX is your pod number
- Use NTP Server 10.1.1.2

WLC

```
(Cisco Controller) reset system

Press <ESC> now to access the Boot Menu...

============================================================
 Boot Loader Menu
============================================================

 1. Run primary image (7.2.111.3) - Active
 2. Run backup image (7.0.220.0)
 3. Change active boot image
 4. Clear configuration
 5. Format FLASH Drive
 6. Manually update images
```

Then login once again as “Recover-Config” :

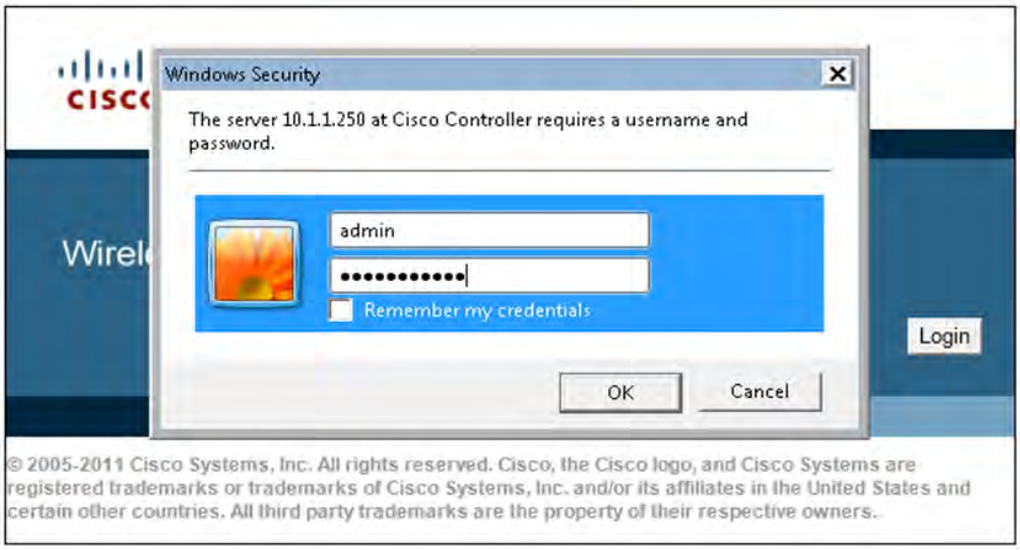
```
User:  Recover-Config
Initiating system recovery process... please wait

Rebooting system
Restarting system.


Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup


Would you like to terminate autoinstall? [yes]:

System Name [Cisco_b6:3d:84] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded WLC
```

Configure username “admin” and password “IPexpert123”. Don’t use any other credentials :

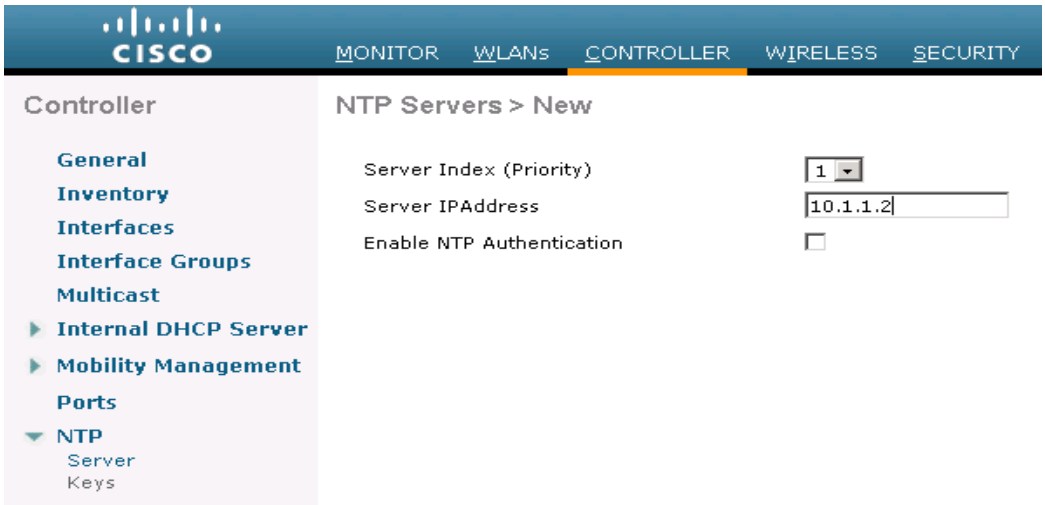
```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): ***********
Re-enter Administrative Password                  : ***********

Management Interface IP Address: 10.1.1.250
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.1.2
Management Interface VLAN Identifier (0 = untagged): 100
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.1.1.250

Virtual Gateway IP Address: 111.111.111.111
route: SIOC[ADD|DEL]RT: File exists

Mobility/RF Group Name: RFGROUP123
Network Name (SSID): 123_IPX_MGMT

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:
US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.
```

```
Please see documentation for more details.

Configuration correct? If yes, system will save it and reset.
[yes][NO]: yes

Configuration saved!
Resetting system with new configuration...
```

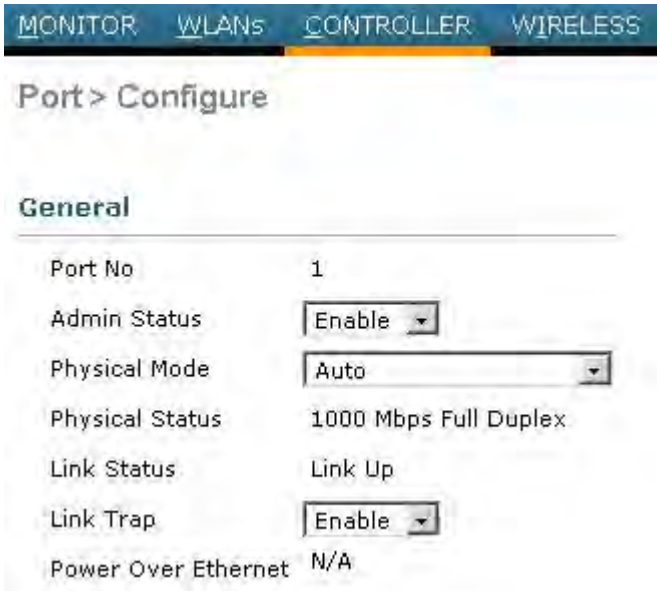
RDP into AD and browse to https://10.1.1.250



Go to **Controllers -> NTP -> Servers, click on New,** and add 10.1.1.2 as the NTP server



Check if the physical port 1 is up (Controller -> Ports) and then start to create interfaces for WLANs as per the tasks



- WLC should be configured to support 802.1x authentication for employees and contractors connecting through the wireless network. Create the appropriate interfaces, ACL's and WLAN's to accomplish this task.
- Create a new interfaces on the WLC for employee and contractors as per the below table.

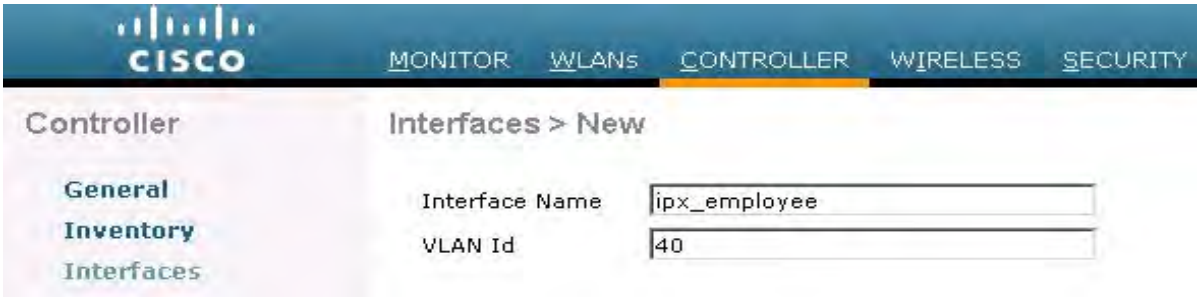
Employee Interface	
Interface Name	ipx_employee
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	40
IP Address	192.168.40.2
Netmask	255.255.255.0
Gateway	192.168.40.1
Primary DHCP Server	10.1.1.101
Secondary DHCP Server	-
ACL Name	none

Contractor Interface	
Interface Name	ipx_contractors
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	50
IP Address	192.168.50.2
Netmask	255.255.255.0
Gateway	192.168.50.1
Primary DHCP Server	10.1.1.101

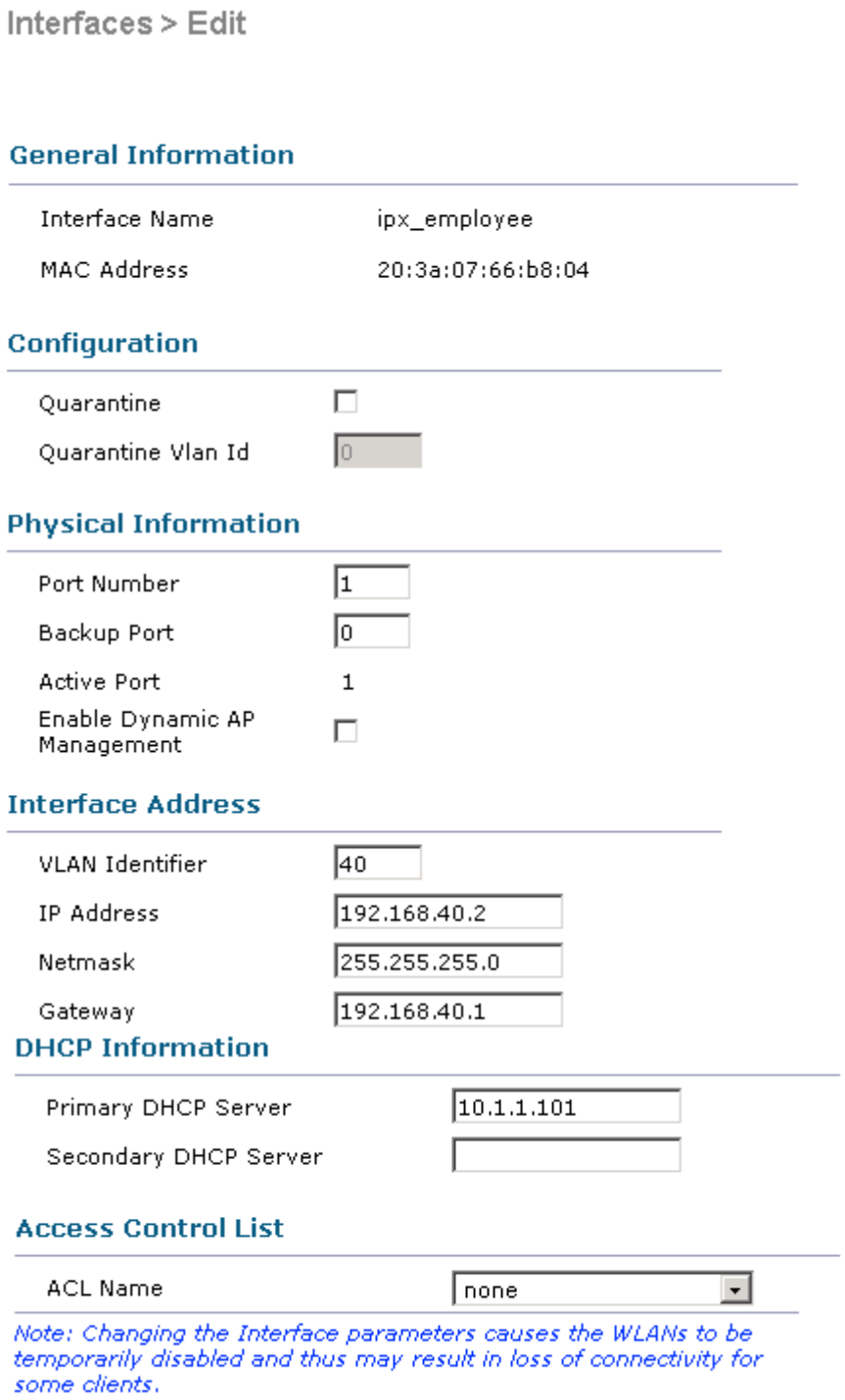
Secondary DHCP Server	-
ACL Name	none

Solutions

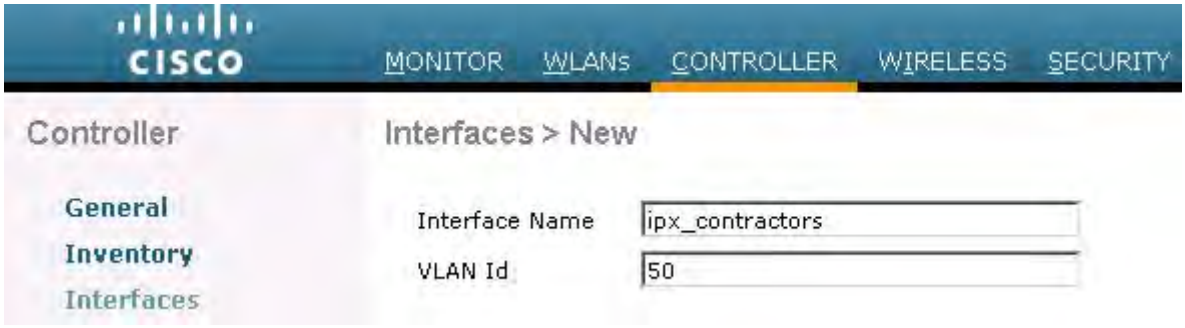
Step 1: Go **Controllers -> Interfaces**. Click on New. Configure the interface name and VLAN ID as per the task.



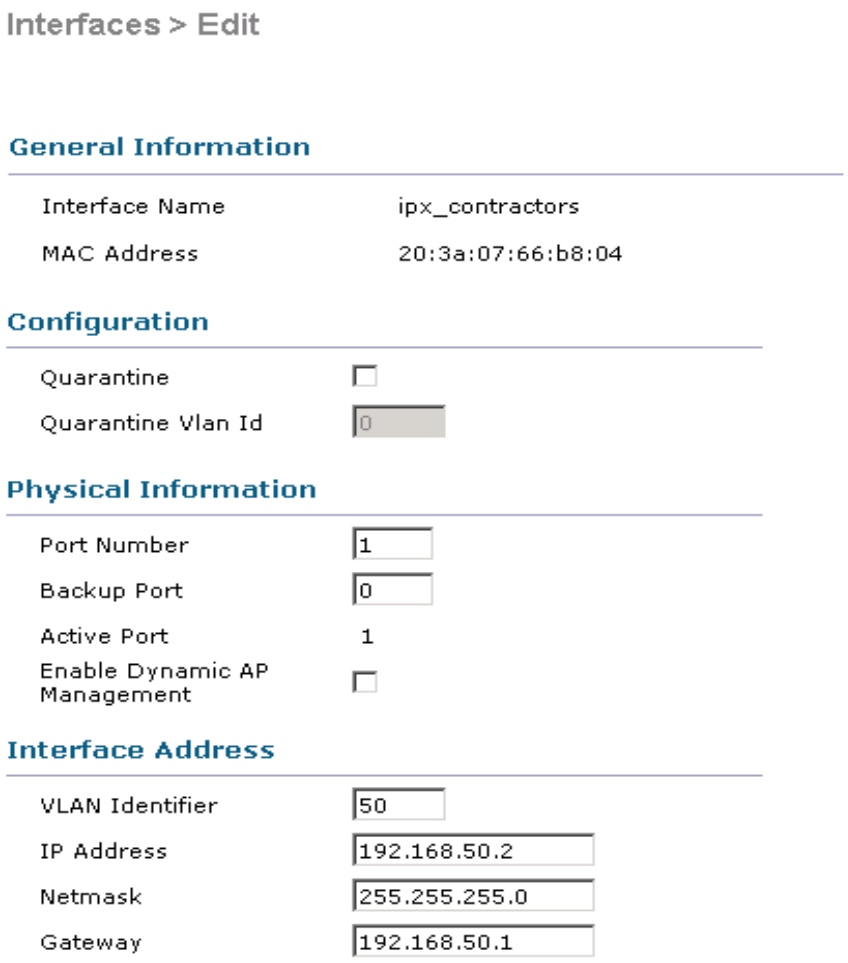
Step 2: Go **Controllers -> Interfaces**. Click on ipx_employee to configure that interface as per the task and click on apply.

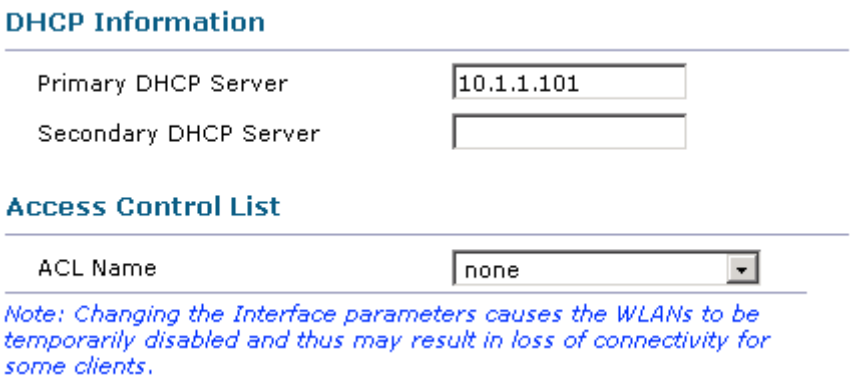


Step 3: Go to **Controllers -> Interfaces**. Click on New. Configure the interface name and VLAN ID as per the task.



Step 4: Go to **Controllers -> Interfaces**. Click on ipx_contractors to configure that interface as per the task and click on apply.





- Create WLAN's on the WLC for employee and contractors as per the below table.

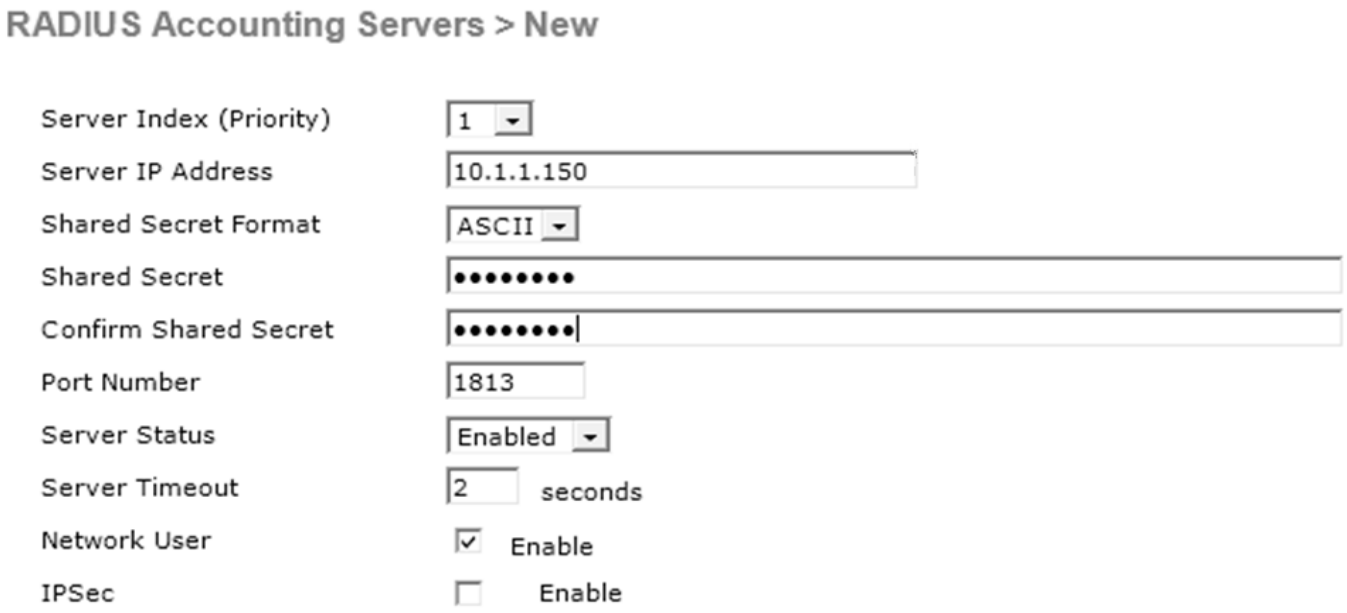
EMPLOYEE WLAN	
Type	WLAN
Profile Name	IPX_EMPLOYEE
SSID	IPX_EMPLOYEE
Status	✓ Enabled
Radio Policy	All
Interface / Group	ipx_employee
Broadcast SSID	✓ Enabled
Security – Layer 2	
Layer 2 Security	802.1X
Security – Layer 3	
Layer 3 Security	None
Web Policy	(Not checked)
Security – AAA Servers	
Authentication Server #1	10.1.1.150, Port:1812
Accounting Server #1	10.1.1.150, Port:1813
Advanced	
Allow AAA Override	✓ Enabled
NAC State	Radius NAC
IPX_CONTRACTOR	
Type	WLAN
Profile Name	IPX_CONTRACTOR
SSID	IPX_CONTRACTOR
Status	✓ Enabled
Radio Policy	All
Interface / Group	ipx_contractors
Broadcast SSID	✓ Enabled
Security – Layer 2	
Layer 2 Security	802.1X
Security – Layer 3	
Layer 3 Security	None
Web Policy	(Not checked)
Security – AAA Servers	

Authentication Server #1	10.1.1.150, Port:1812
Accounting Server #1	10.1.1.150, Port:1813
Advanced	
Allow AAA Override	✓ Enabled
NAC State	Radius NAC

Solutions

Step 1: Add ISE as a new RADIUS authentication and accounting server

WLC

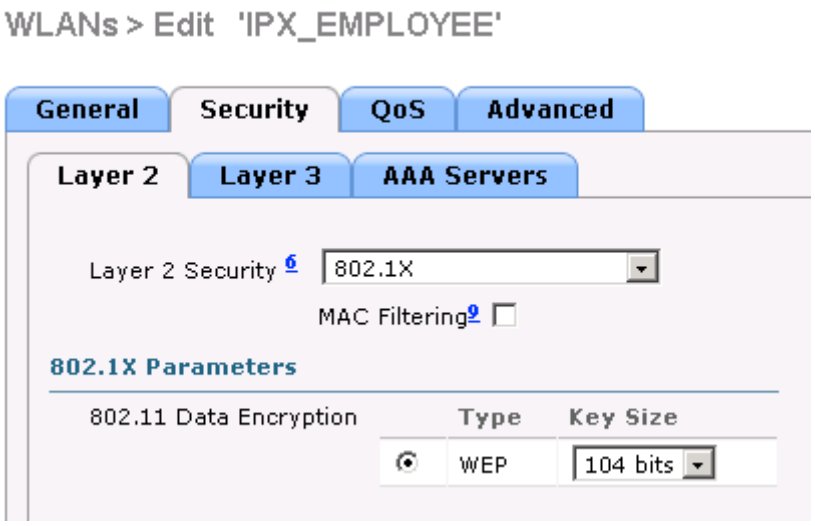


Step 2: Go to **WLANs** tab select "create new" and click on Go. Create WLAN for employees. Remove any existing WLAN's before configuring this WLAN. Make sure SSID matches as stated in the task.

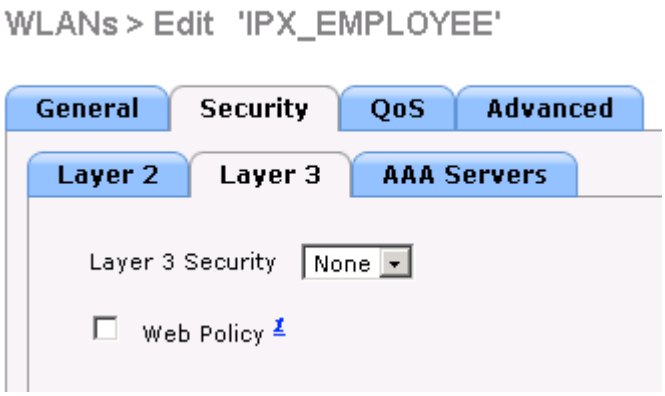
Step 3: Click on Edit "IPX_EMPLOYEE" WLAN and configure WLAN parameters as per the task

Make sure the status is set to "Enabled" and interface is set to "ipx_employee"

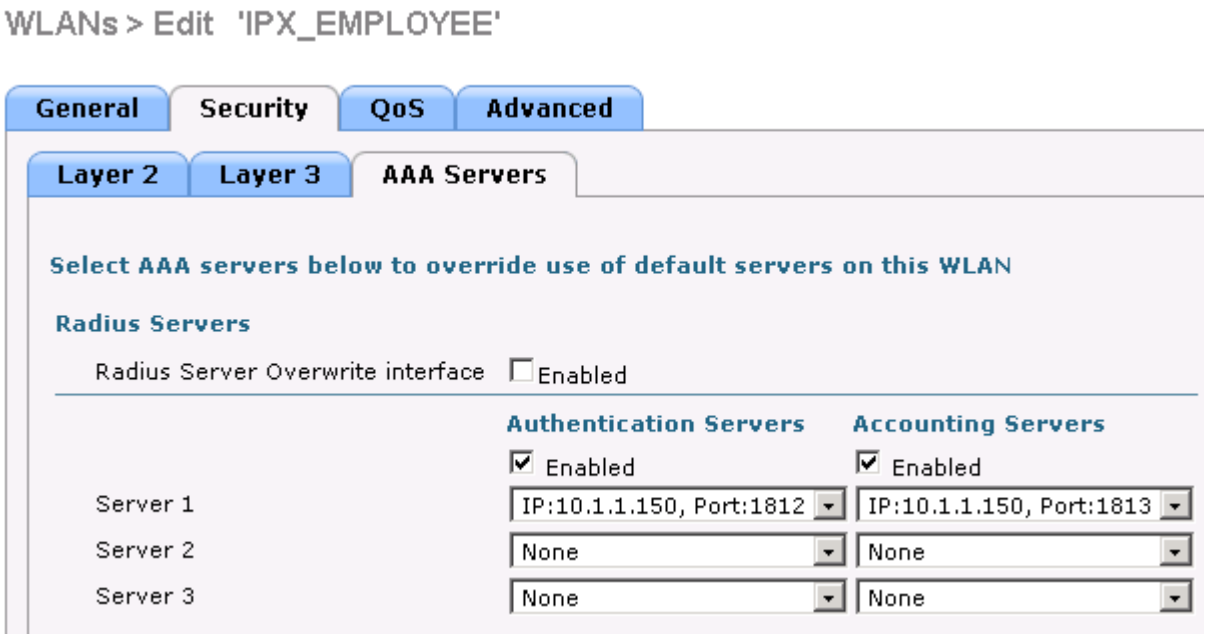
Click on the Security Tab. Select Layer 2 Security as 802.1X



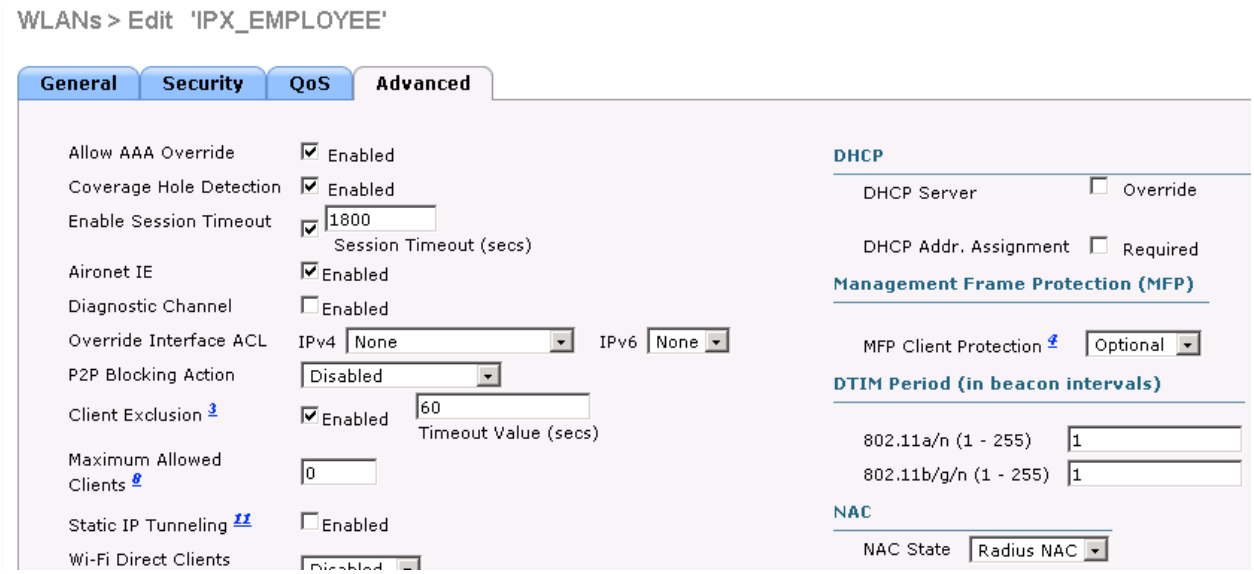
Under the Security Tab navigate to Layer 3 sub tab and make sure None is selected



Under the Security Tab navigate to AAA Server sub tab and add ISE as the AAA server.



Navigate to the Advanced tab. Make sure you enable “Allow AAA Overried” and “NAC State = Radius NAC”.

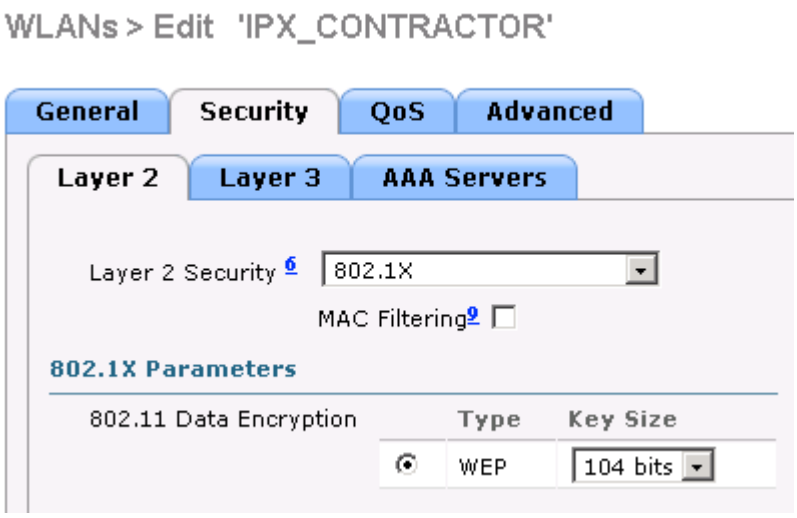


Step 4: Configure a new WLAN for Contractors. Make sure SSID matches as stated in the task.

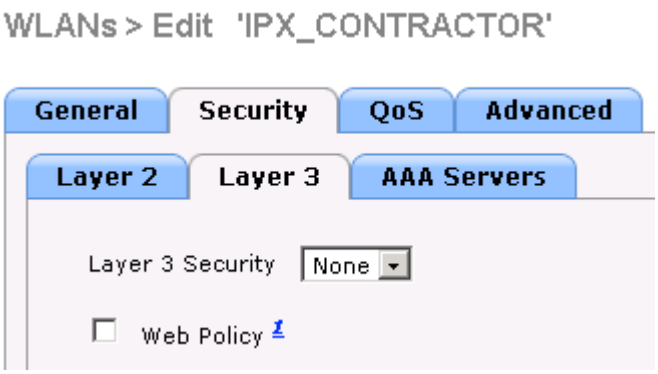
Step 3: Click on Edit "IPX_CONTRACTOR" WLAN and configure WLAN parameters as per the task

Make sure the status is set to "Enabled" and interface is set to "ipx_contractors"

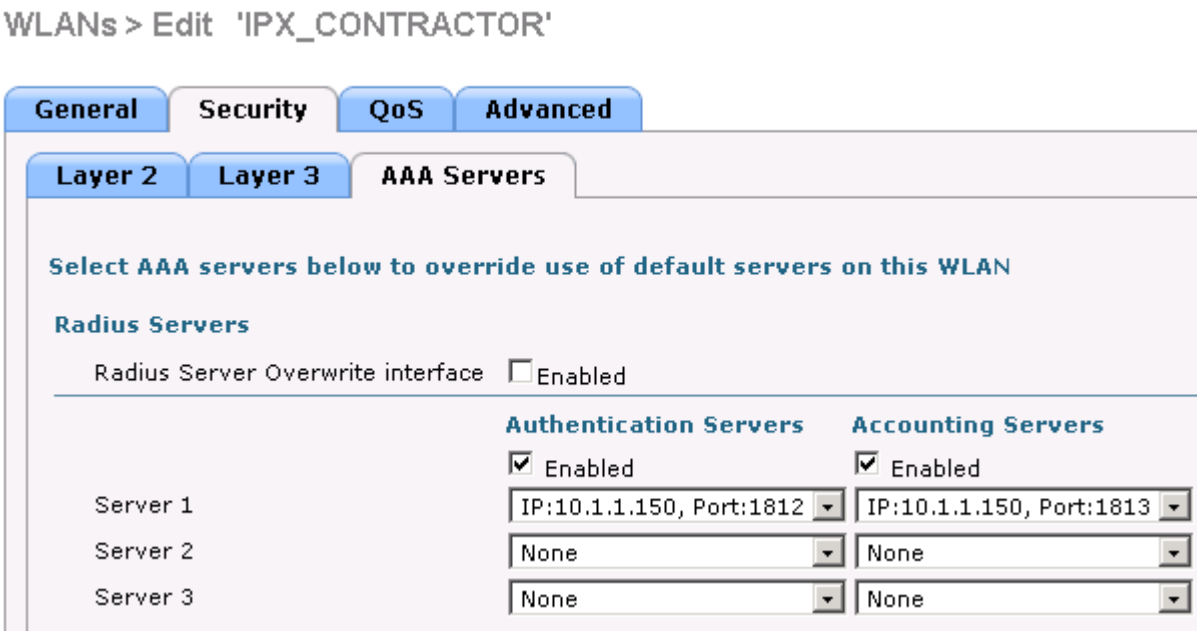
Click on the Security Tab. Select Layer 2 Security as 802.1X



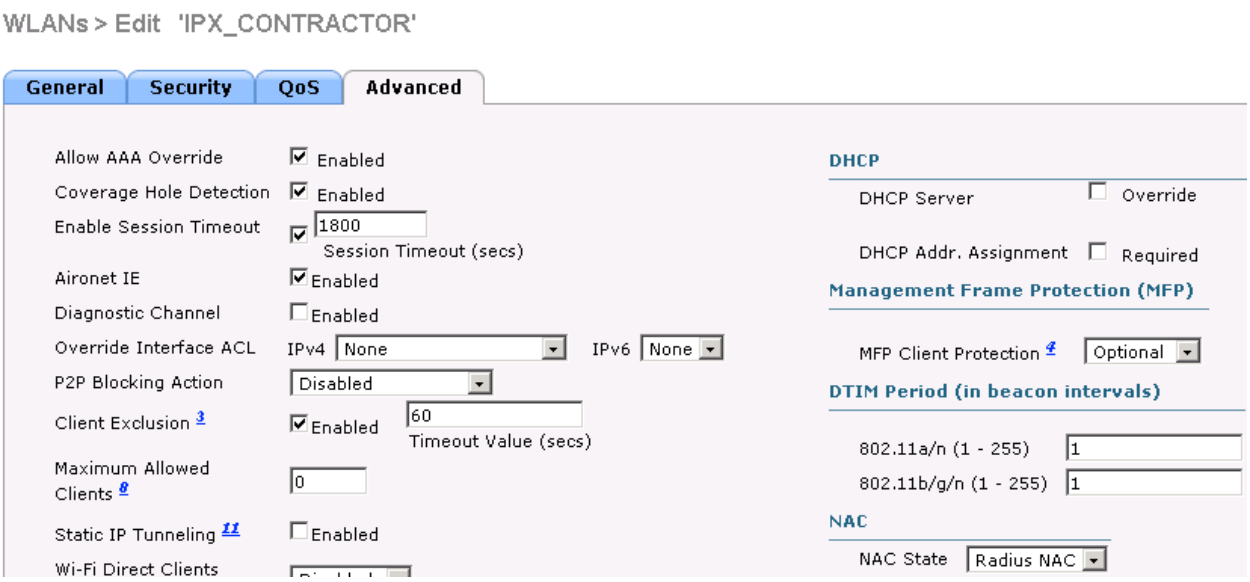
Under the Security Tab navigate to Layer 3 sub tab and make sure None is selected



Under the Security Tab navigate to AAA Server sub tab and add ISE as the AAA server.



Navigate to the Advanced tab. Make sure you enable “Allow AAA Overried” and “NAC State = Radius NAC”.



- Configure wireless authentication policies as per the below table

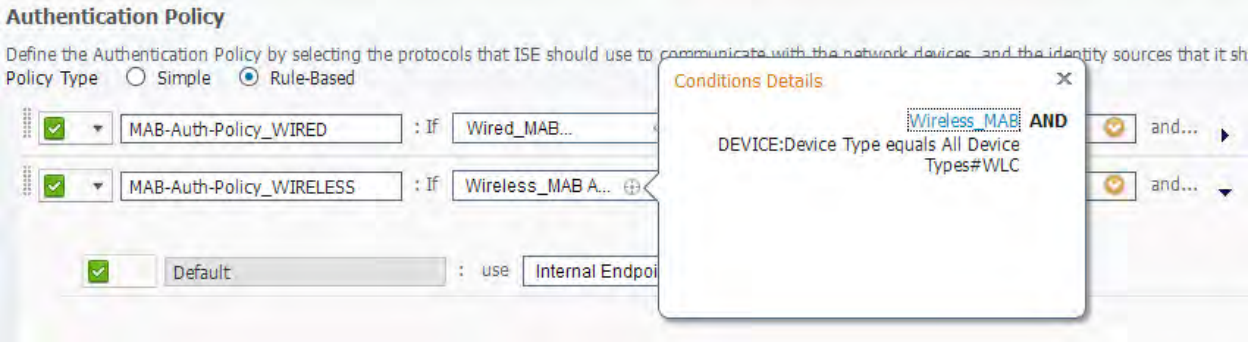
Name		Condition		Protocols		Identity Source
MAB-Auth-Policy_WIRELESS	IF	Wireless_MAB AND Device:Device Type = Device Type#All Device Types#WLC	allow protocols	MAB	and use	Internal Endpoints
Dot1X-Auth-Policy_WIRELESS	IF	Wireless_802_1X AND Device:Device Type = Device Type#All Device Types#WLC	allow protocols	PEAP_MSCHAPv2	and use	AD_LOCAL

Solutions

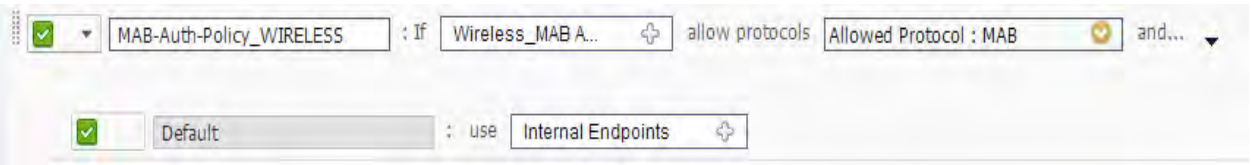
ISE

Step 1: Go to **Policy->Authentication** and add a wireless MAB rule as per the task

Make sure you add the correct condition as per the task.



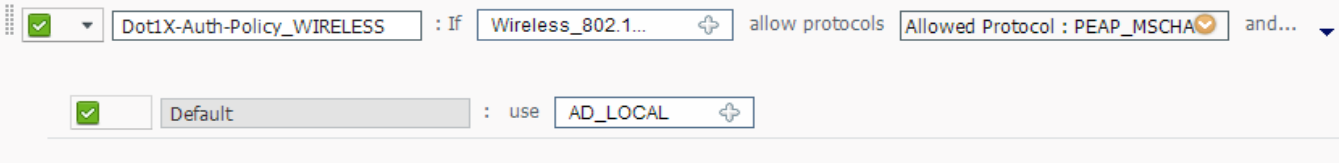
Make sure to select MAB as the allowed protocols and Internal Endpoints as the identity stores, then click on save.



Step 2: Now create wireless employee policy authentication rule.

Make sure you add the correct condition as per the task.

Make sure to select PEAP_MSCHAPv2 as the allowed protocols and AD_LOCAL as the identity stores, then click on save.



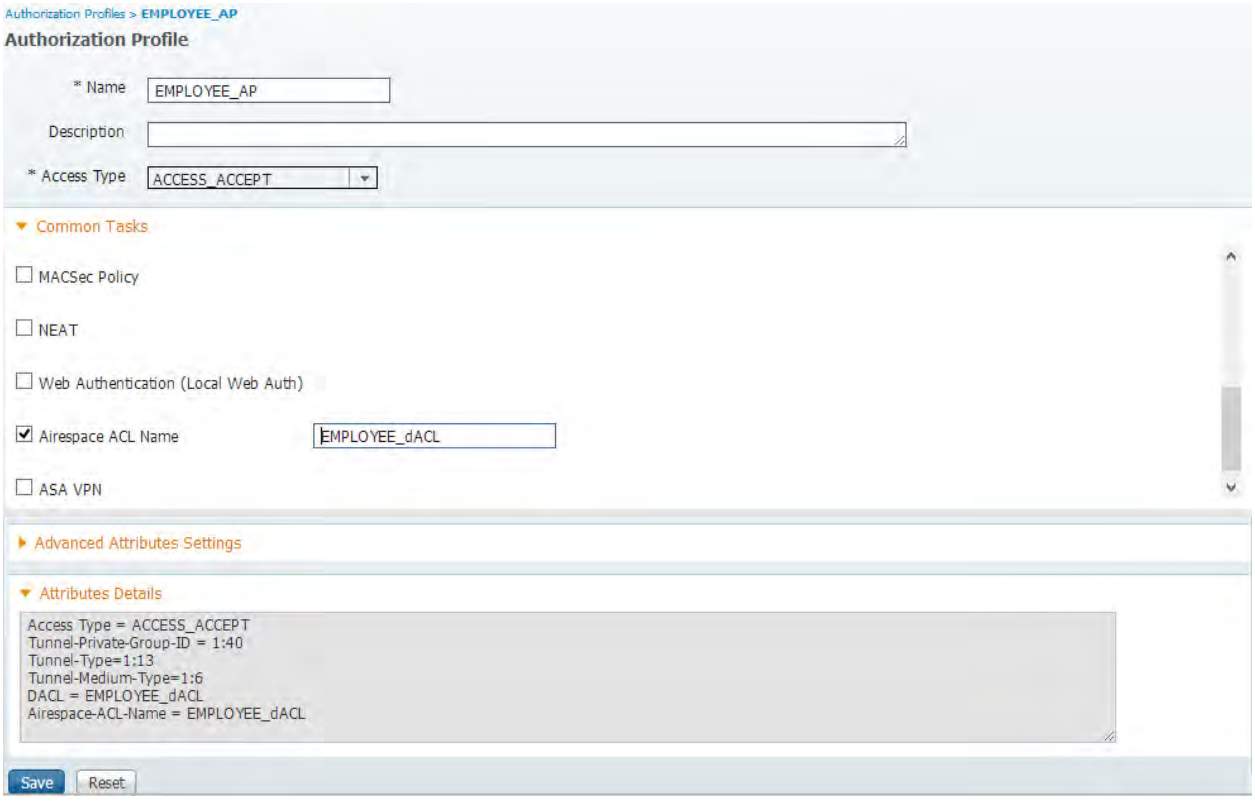
- Re-Configure Authorization profile for employees as per the below table.

Authorization Profile	
Name	EMPLOYEE_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	EMPLOYEE_dACL
VLAN	40
AIRSPACE ACL NAME	EMPLOYEE_dACL

Solutions

ISE

Step 1: Go to **Policy->Policy Elements-> Results->Authorization->Authorization Profiles.** Click on EMPLOYEE_AP profile and configure Airspace ACL Name attribute and save the profile.



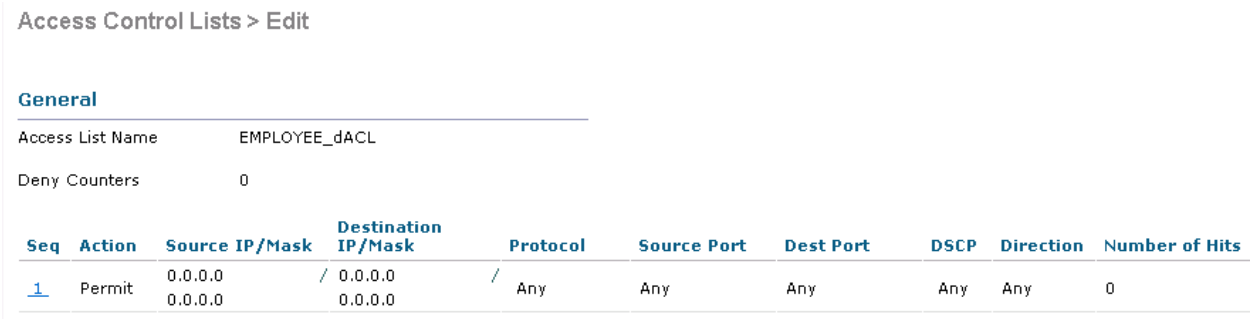
- Configure the appropriate ACL on the WLC for the employee policy from ISE to be applied.

Solutions

WLC

Step 1: Go to **Security->Access Control Lists.** Click on New and configure the ACL's similar to ISE. Make sure the name matches as per the task.

Step 2: Click on edit "EMPLOYEE_dACL" then choose Add a new rule and create the ACL rule. After creating the rule click on Apply tab.



- Contractors should be given access through wireless. The session should be re-authenticated every 2 hours. Create a new Authorization profile and policy as per the below

tables. Machine access restrictions should not apply when contractors connect though the wireless.

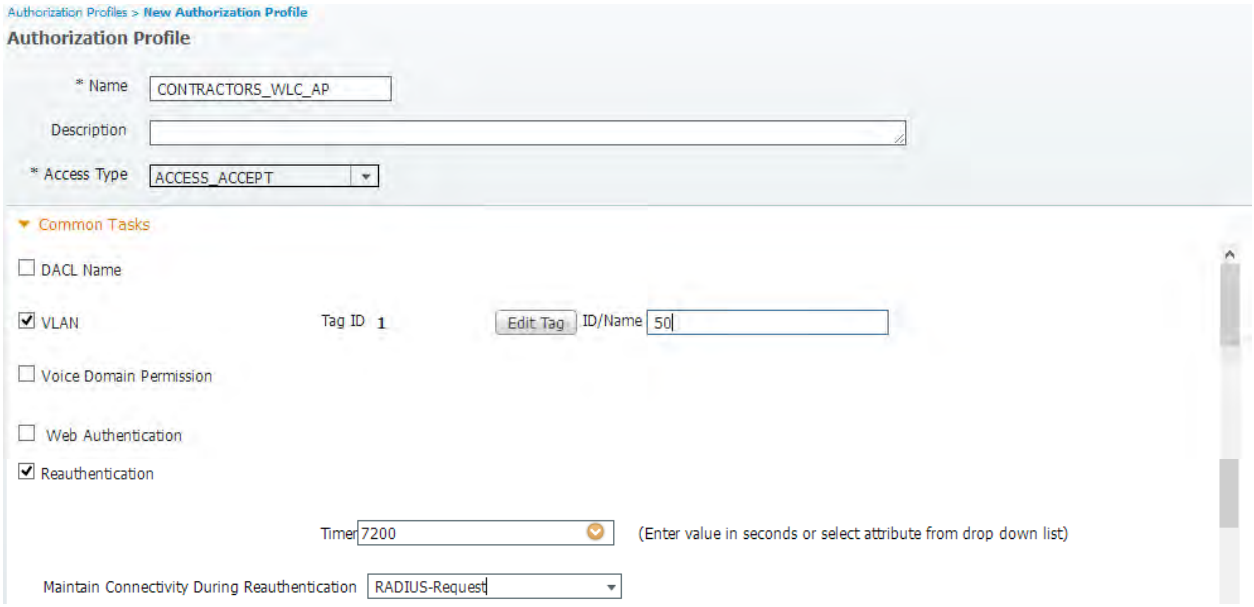
- Configure Authorization profile for wireless contractors as per the below table.

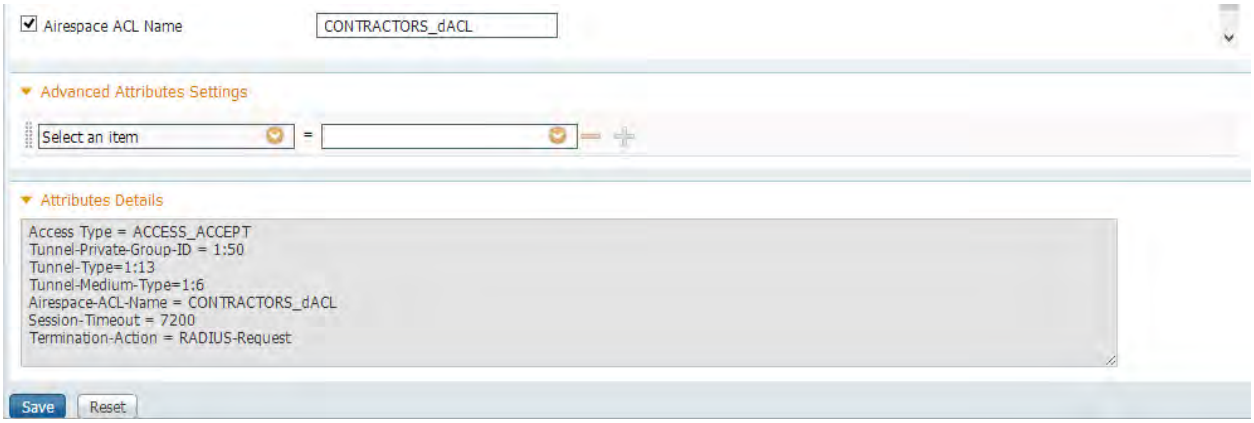
Authorization Profile	
Name	CONTRACTORS_WLC_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
VLAN	50
AIRSPACE ACL NAME	CONTRACTORS_dACL
Advanced RADIUS Attribute Settings	
Radius: Session-Timeout and Termination-Action	2 hours / Radius-Request

Solutions

ISE

Step 1: Go to Policy->Policy Elements-> Results->Authorization->Authorization Profile, click on Add and configure the profile parameters as per the task.





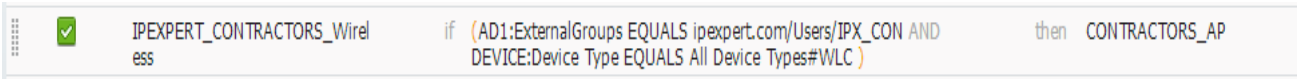
- Configure Authorization policy for contractors as per the below table. Make sure you place this policy in the table below the wired policy of contractors.

Name		Identity Group		Conditions		Authorization
IPEXPERT_CONTRACTORS_Wireless	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/**IPX_CON** AND DEVICE:Device Type EQUALS=**WLC**	THEN	CONTRACTORS_WLC_AP

Solutions

ISE

Step 1: Go **Policy->Authorization** and configire a new rule as per the parameters given in the task.



- Configure the appropriate ACL on the WLC for the contractor policy from ISE to be applied.

Solutions

ISE

Step 1: Go to **Security->Access Control Lists**. Click on New and configure the ACL's similar to ISE. Make sure the name matches as per the task.

Step 2: Click on edit "CONTRACTORS_dACL" then choose Add a new rules and configure rules as per the task.

Access Control Lists > Edit

General

Access List Name	CONTRACTORS_dACL
Deny Counters	0

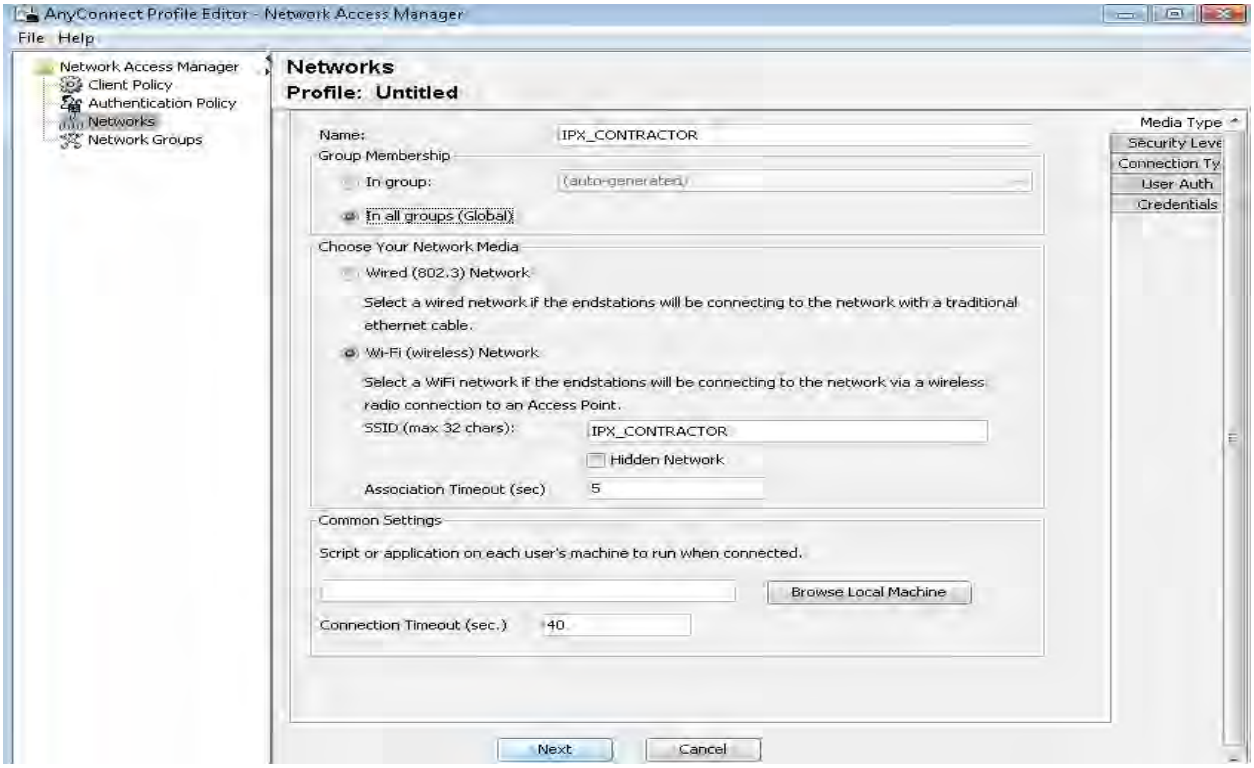
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0 / 0.0.0.0	4.4.4.4 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
2	Deny	0.0.0.0 / 0.0.0.0	5.5.5.5 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
3	Deny	0.0.0.0 / 0.0.0.0	20.4.4.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
4	Deny	0.0.0.0 / 0.0.0.0	20.5.5.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

- RDP into TEST-PC1 and configure it for 802.1x.
- Configure anyconnect profiles using NAM profile editor and test wireless 802.1x for employee and contractor WLAN's. Test using "IPXEMP1/cisco" (Employee) or "IPXCON1/cisco" (Contractor) as the login details for 802.1x. Make sure anyconnect always prompts the user for username and password and does not store the credentials.
- For testing purpose, you are allowed to configure static routes on the PC. Do not set the default gateway. PC will automatically get the IP address from the pre-configured DHCP server.

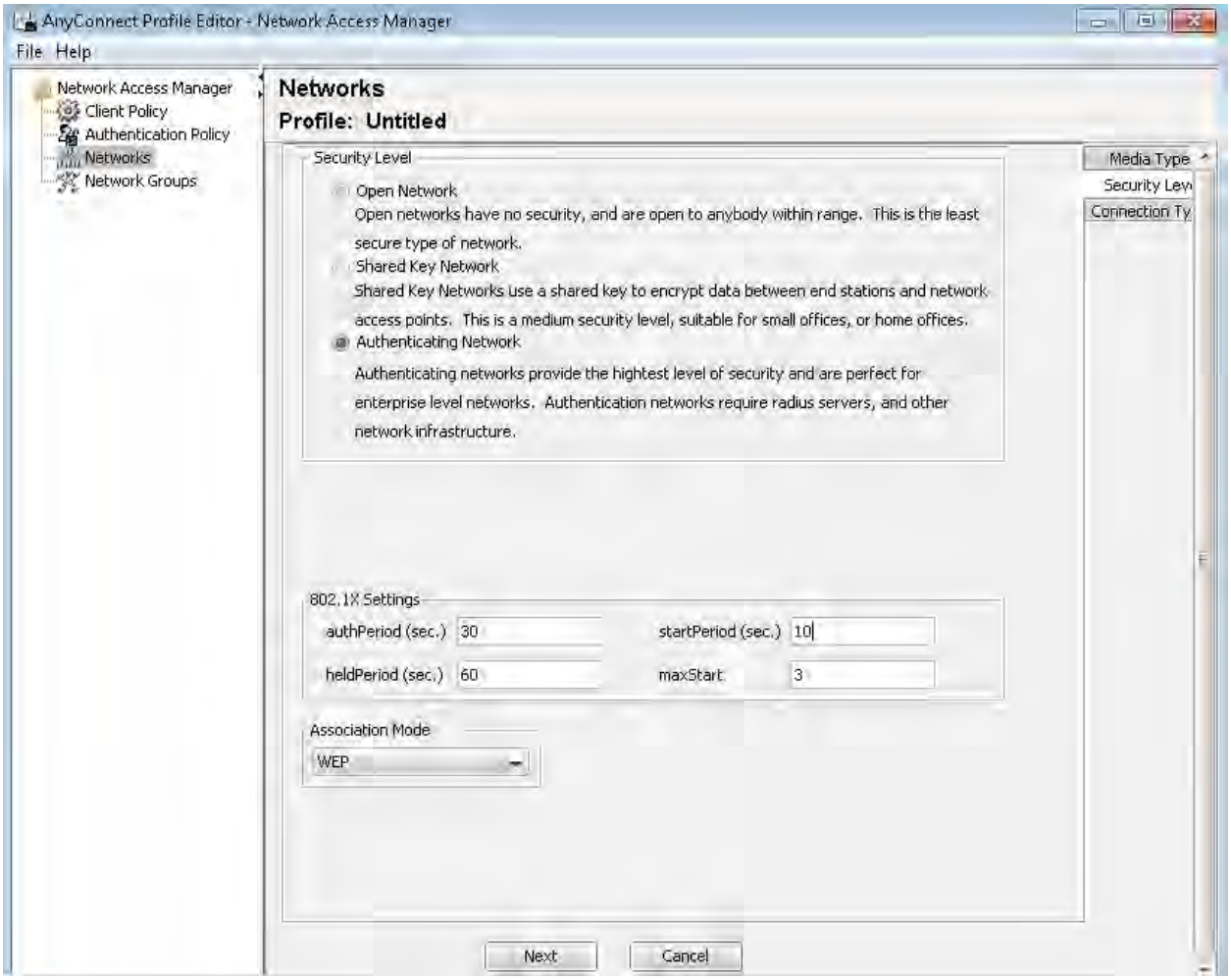
Solutions

Step 1: RDP into TEST-PC2 and configure a new anyconnect profile for 802.1x using NAM editor as per the task.

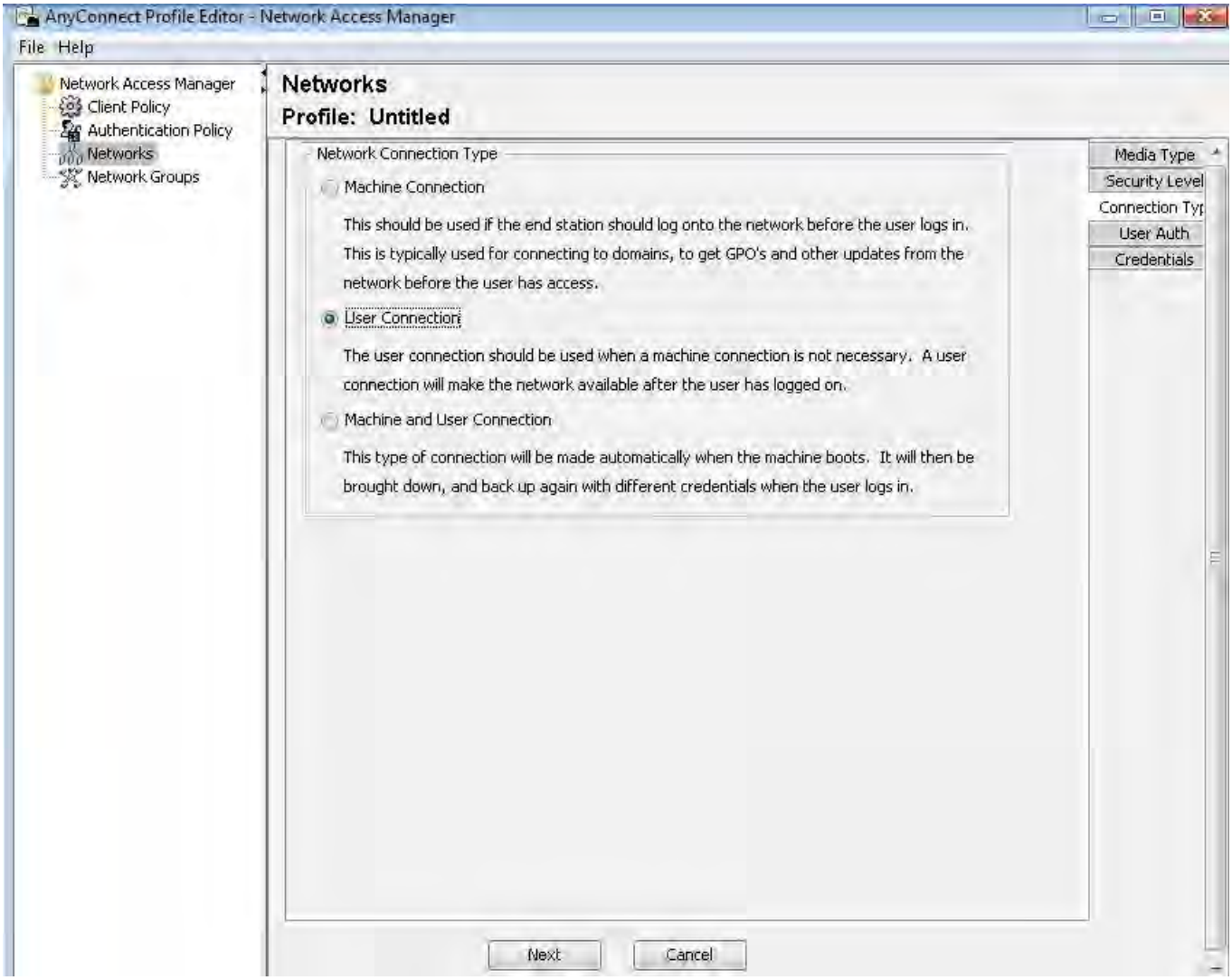
Use a profile name of "IPX_CONTRACTOR" select "In all groups (Global)" and choose wireless network with SSID of "IPX_CONTRACTOR". Then click Next.



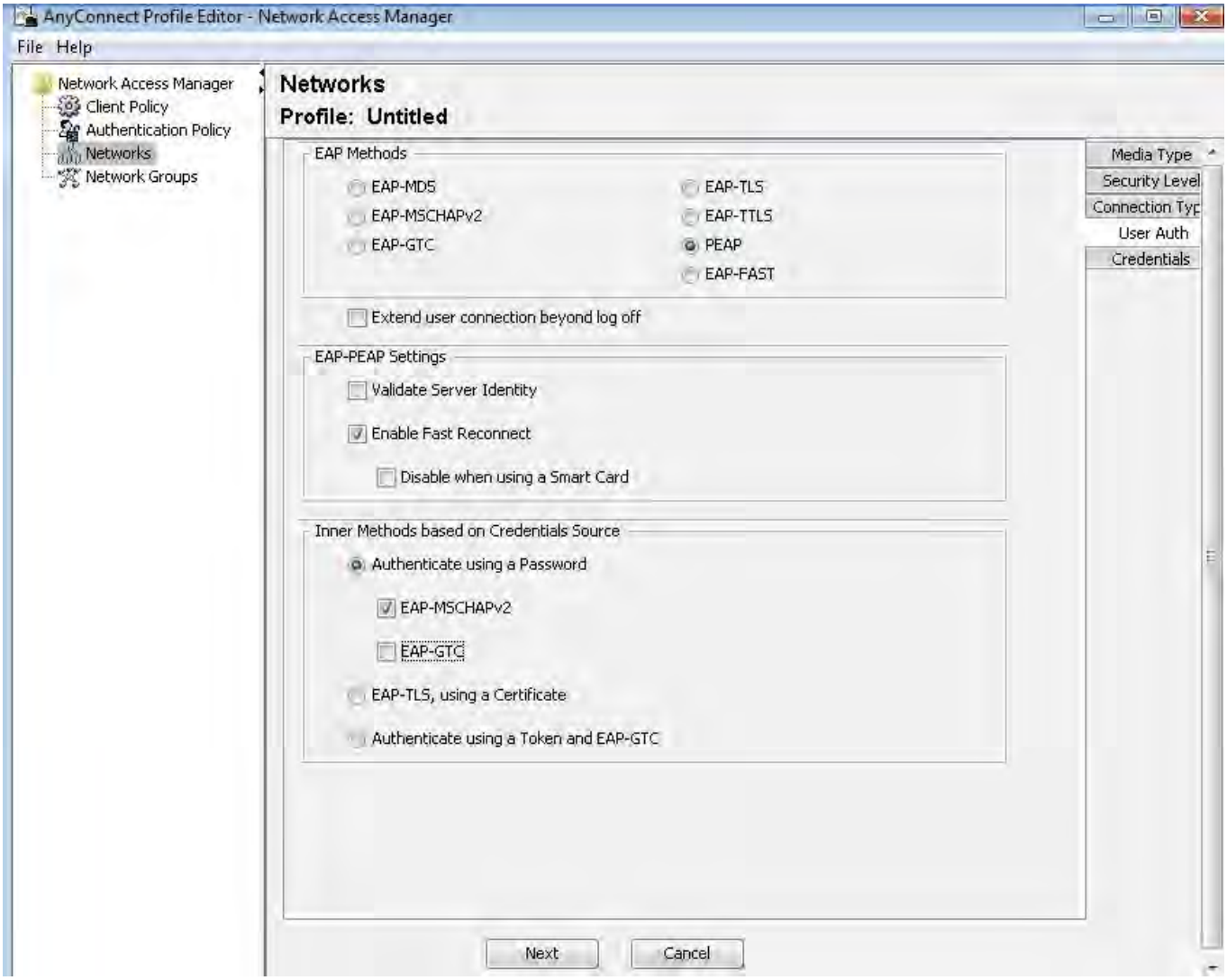
Choose “Authenticating Network” and enable port exceptions when EAP fails. Then click Next.



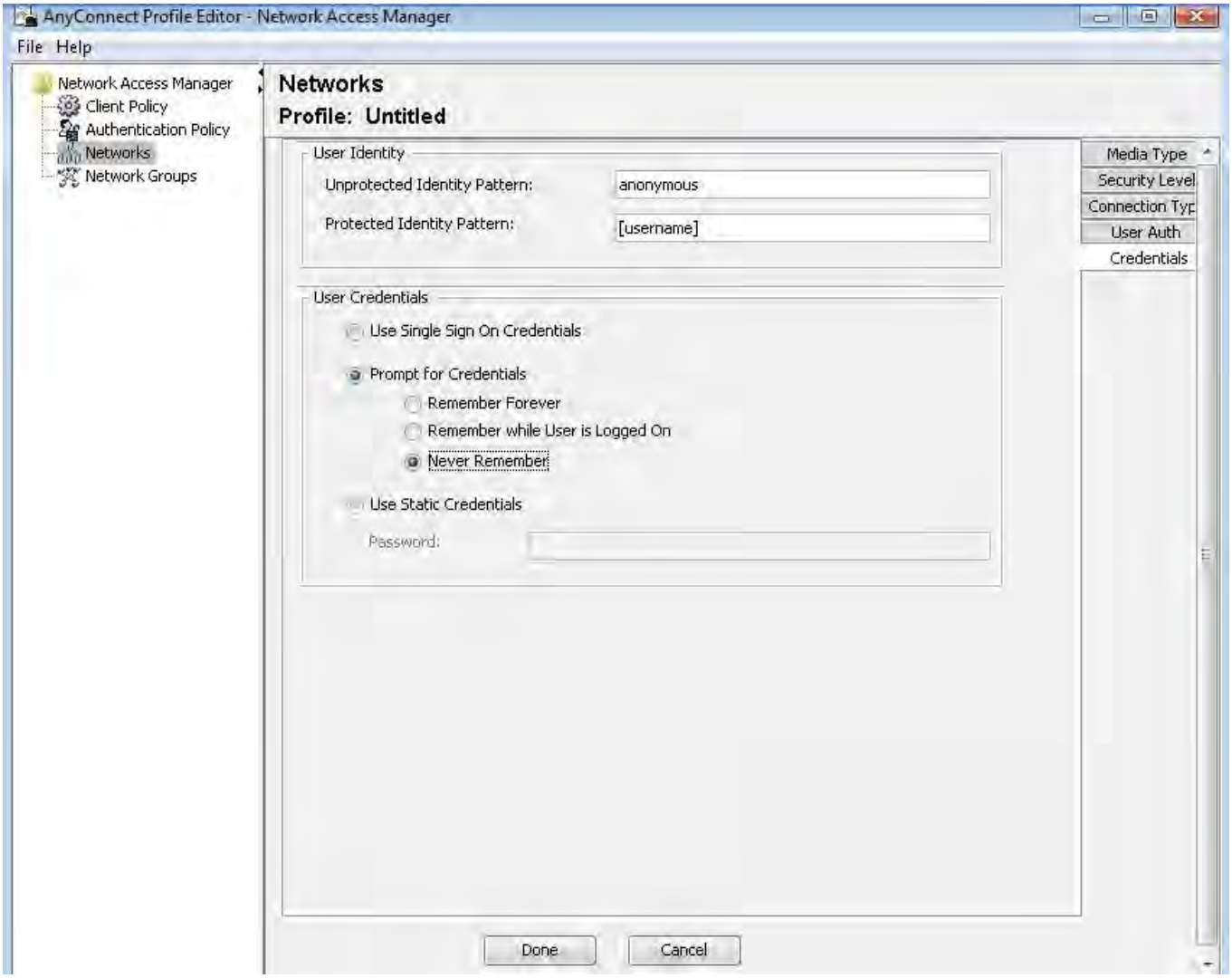
Choose User Connection. Then click Next.

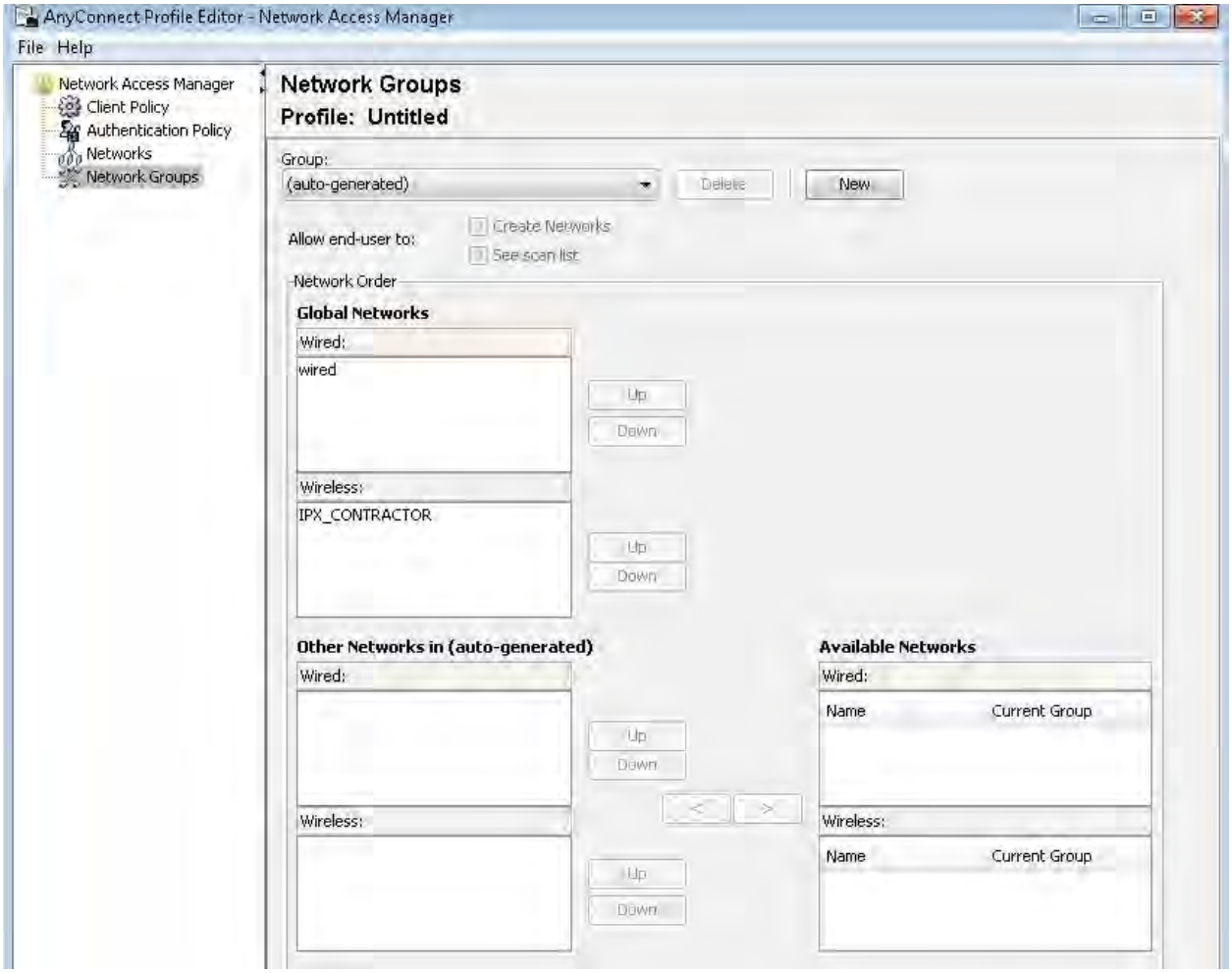


Choose PEAP and inner method of EAP-MSCHAPv2. Then click Next.



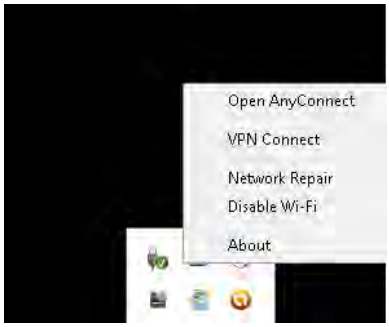
Choose prompt credentials. Then click Next.





Save As configuration.xml

Perform a Network Repair for the anyconnect and enter the appropriate username and password. (IPXCON1/cisco)



Lab-4: Configuring CWA and guest access

Lab-4: Configuring CWA and guest access – This lab is intended to familiarize you with configuring wired and wireless CWA and guest access. You will also configure guest portal, sponsor portal, sponsor group, sponsor group policies and appropriate authentication and authorization policies required for CWA and guest access.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 4 Hours

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-3 successfully.
Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

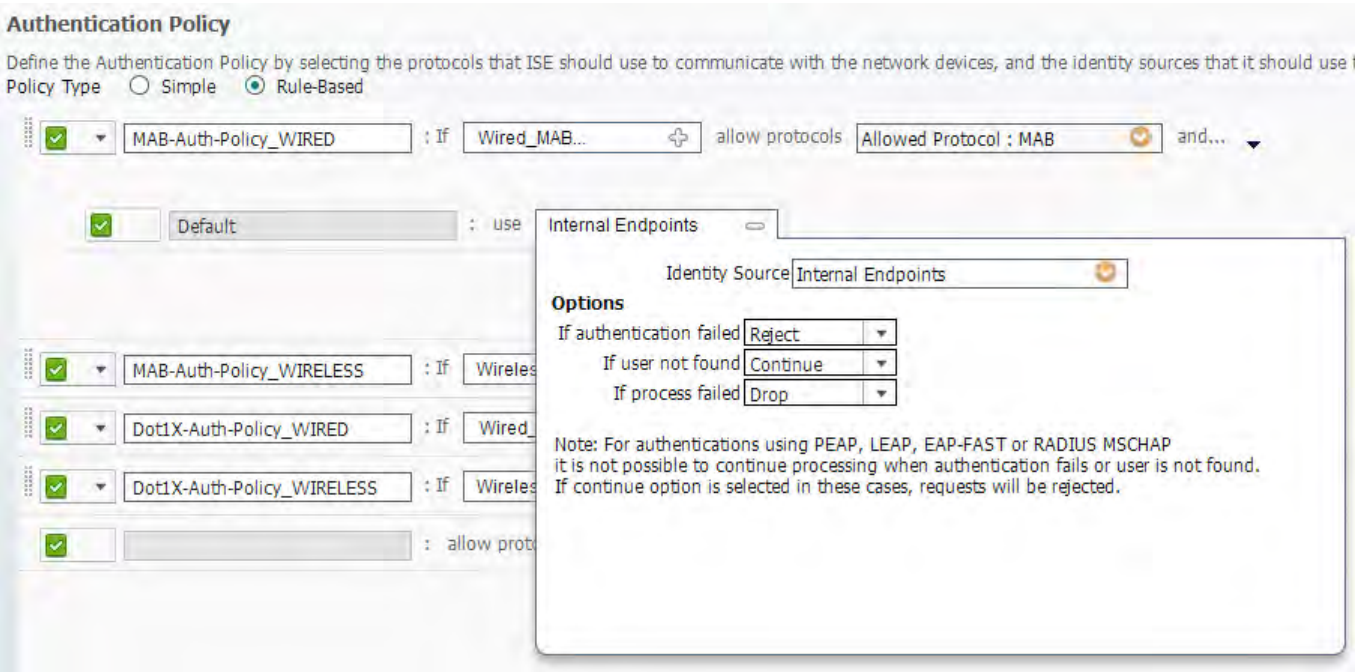
This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configuring Wired CWA

- Enable employees and contractors to login through guest web portal on ISE when they do not have supplicant installed on their devices.
- Re-configure wired MAB authentication policy to support wired CWA.

Solutions

Step 1: Go to **Policy-> Authentication** and edit the MAB rule to use the options **Continue** if user not found in the Identity Source/Store. Then click on Save.



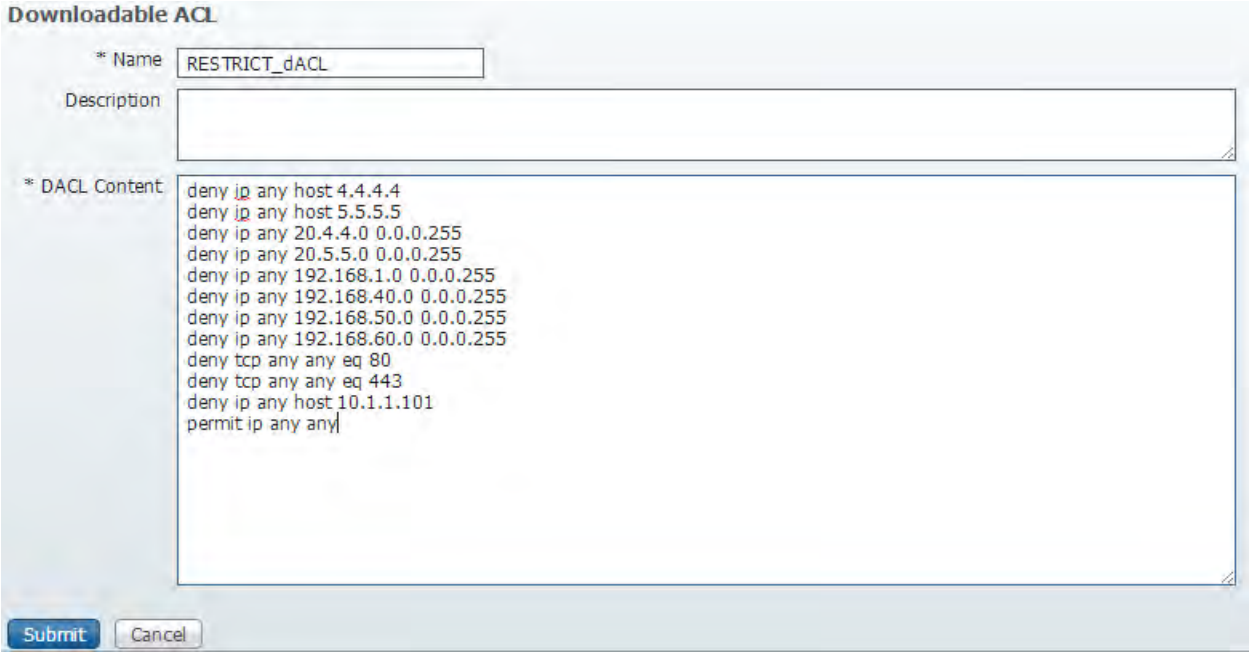
- When users connect to the wired network, they should be automatically placed in VLAN 250 with a restricted dACL being downloaded until they are re-authenticated and re-authorized using CWA.
- Add new authorization policy to support Wired CWA with the appropriate authorization profile.
- Configure a restricted dACL to be downloaded to the unauthenticated users as per the below table

Downloadable ACL	
Name	RESTRICT_dACL
DACL Content	deny ip any host 4.4.4.4 deny ip any host 5.5.5.5 deny ip any 20.4.4.0 0.0.0.255 deny ip any 20.5.5.0 0.0.0.255 deny ip any 192.168.1.0 0.0.0.255 deny ip any 192.168.40.0 0.0.0.255

	deny ip any 192.168.50.0 0.0.0.255 deny ip any 192.168.60.0 0.0.0.255 deny tcp any any eq 80 deny tcp any any eq 443 deny ip any host 10.1.1.101 permit ip any any

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Downloadable ACLs**. Click on **Add.**

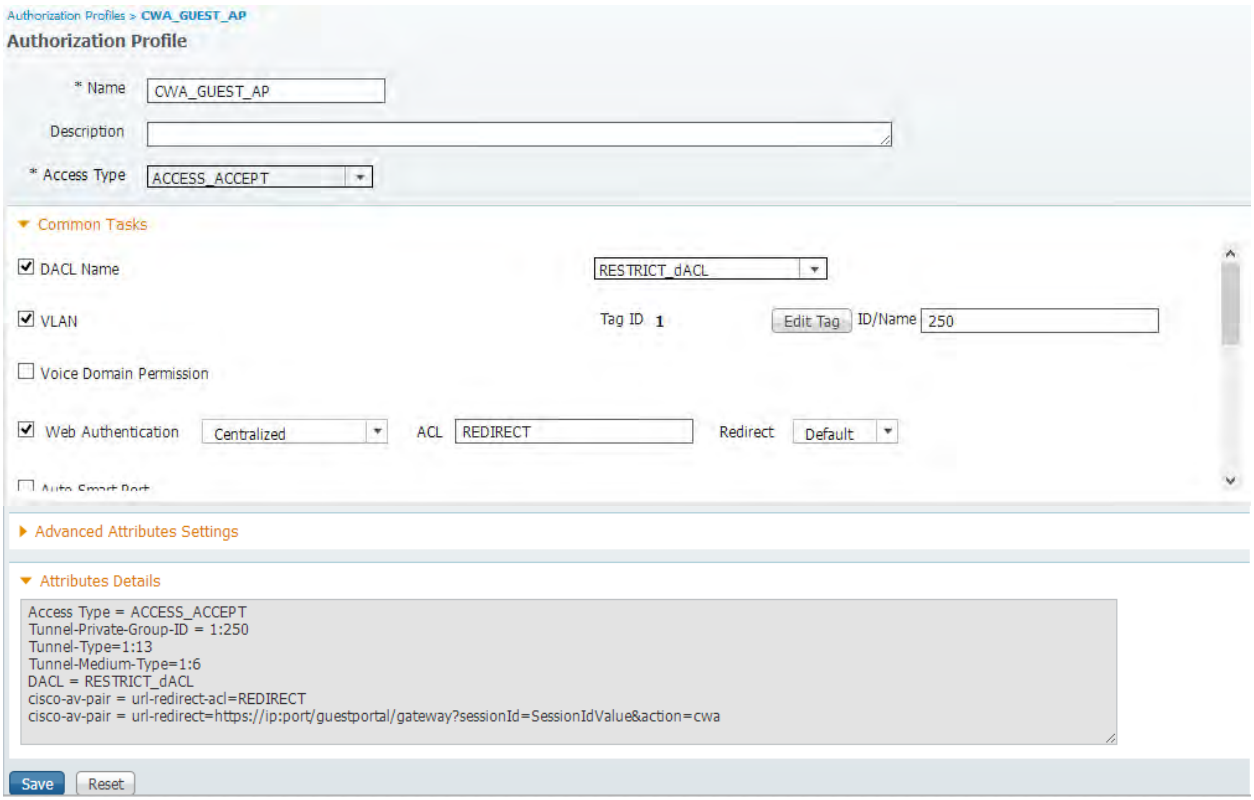


- Configure a CWA authorization profile as per the below table.

Authorization Profile	
Name	CWA_GUEST_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
VLAN	250
DOWNLOADABLE ACL	RESTRICT_dACL
WEB AUTHENTICATION	Centralized/ ACL=REDIRECT

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Click on Add.

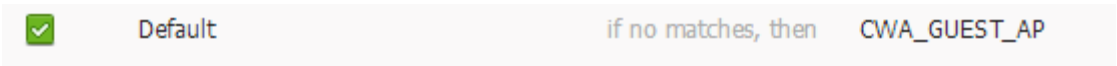


Configure a new authorization policy to support CWA as per the below table.

Name		Identity Group	Conditions		Authorization
Default	IF	no matches	----------	THEN	CWA_GUEST_AP

Solutions

Step 1: Go to **Policy->Authorization** and change the authorization profile of the default policy to CWA_GUEST_AP.

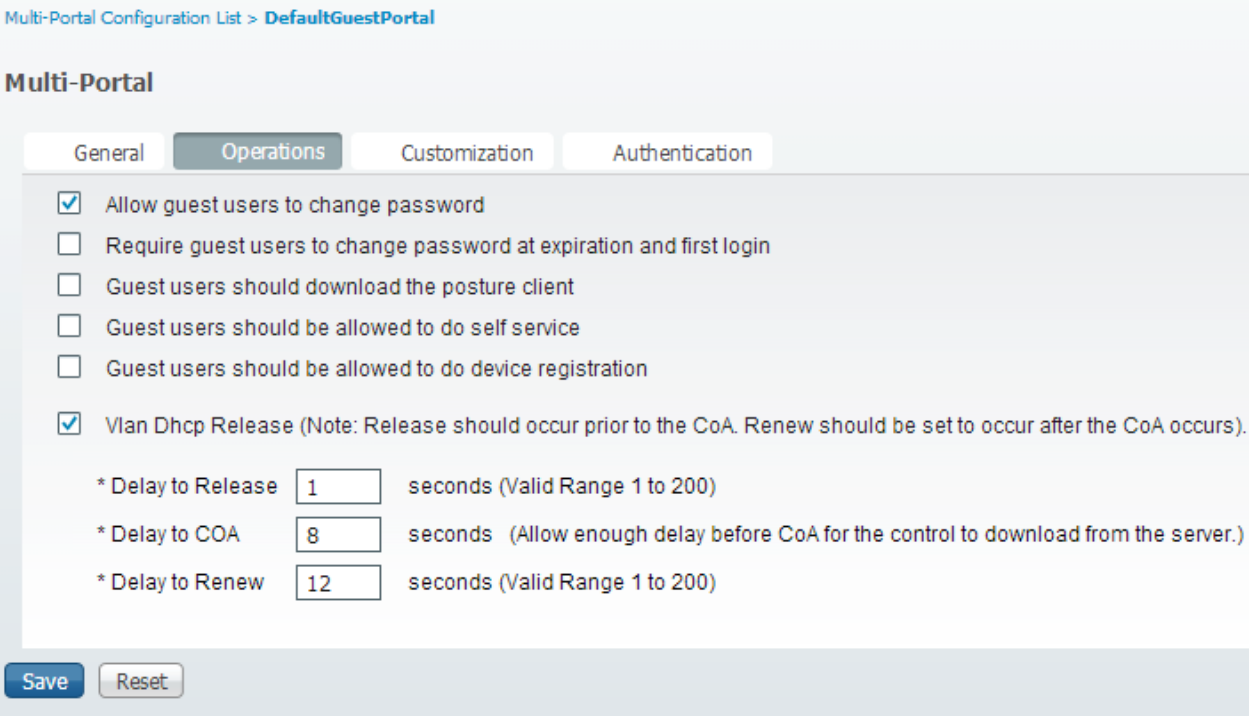


- Configure the default guest portal on ISE to support CWA and guest access using the identity source sequence created earlier. Enable VLAN DHCP release.

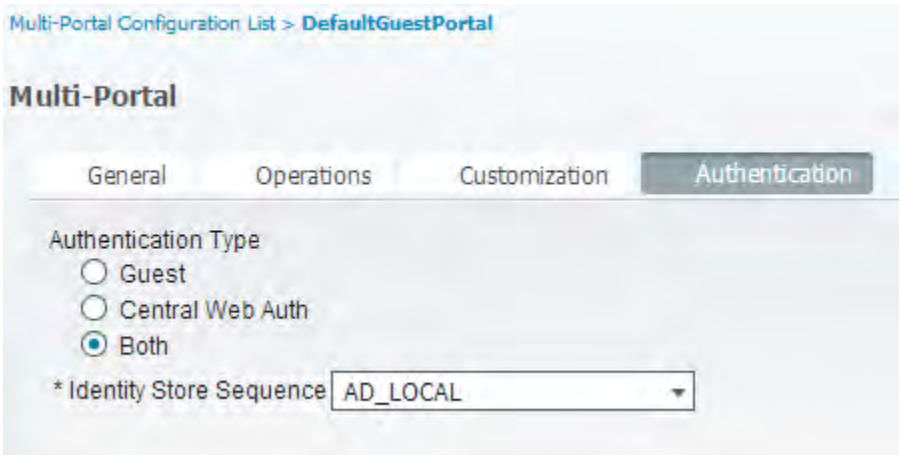
Solutions

Step 1: Go to **Administration->Web Portal Management->Settings->Guest->Multi-Portal Configurations**. Click on DefaultGuestPortal.

Click on Operations tab and configure VLAN DHCP release.



Navigate to Authentication tab and change the authentication type to both and the Identity Store to “AD_LOCAL”.



- Configure the switch to support CWA. Generate a new RSA key pair of length 2048. Enable HTTP / HTTPS server and configure the “REDIRECT” ACL.

Solutions

CAT3

```
ip http server
ip http secure-server

ip access-list extended REDIRECT
 deny   udp any any eq domain
 deny   icmp any any
 deny   ip any host 10.200.5.232 (G0 interface of ISE)
 permit ip any any
```

```
Note: Add a route on the test pc to G0 interface of ISE and the AD with a
next hop of 192.168.250.1.
Make sure the AD has a DNS entry for podxxxise.ipexpert.com for G0 interface,
else add a DNS entry.
```

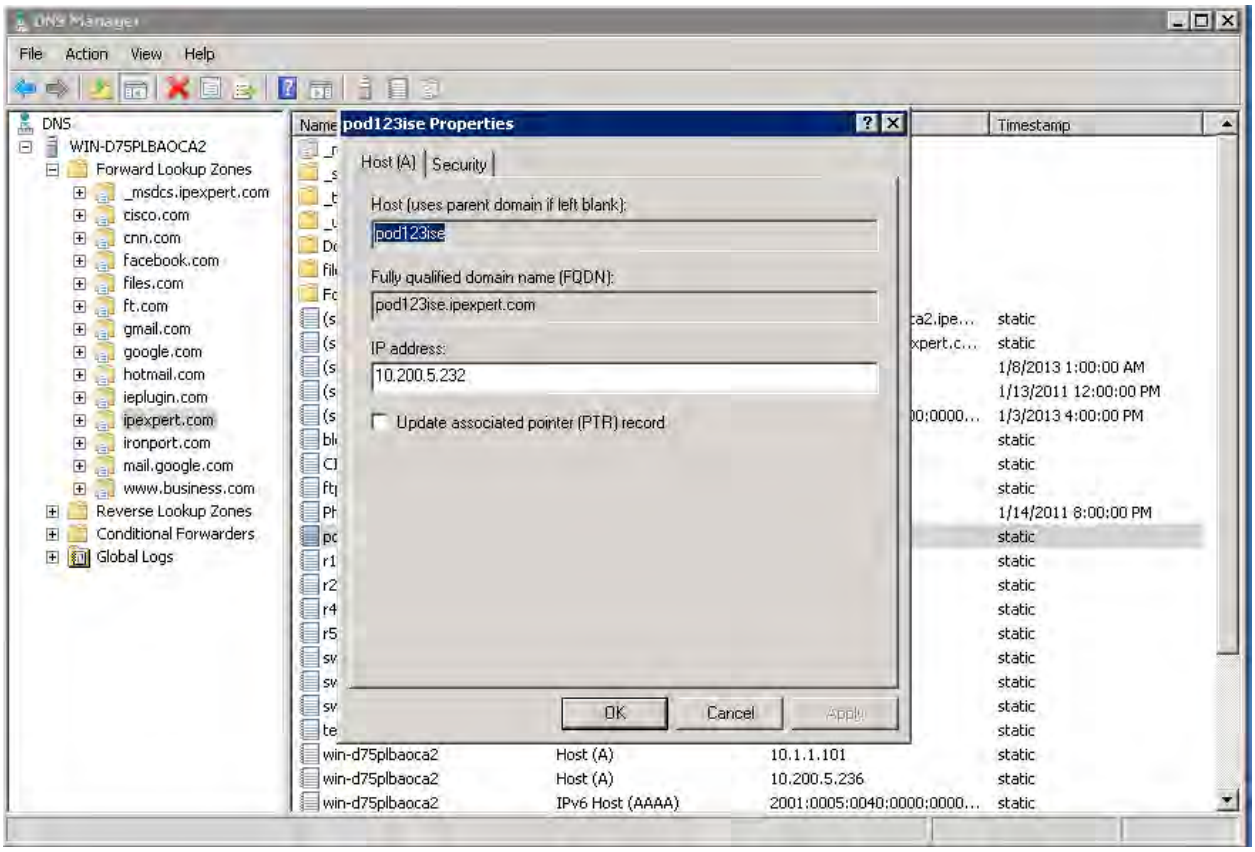
- You may test this configuration from any test PC.

Solutions

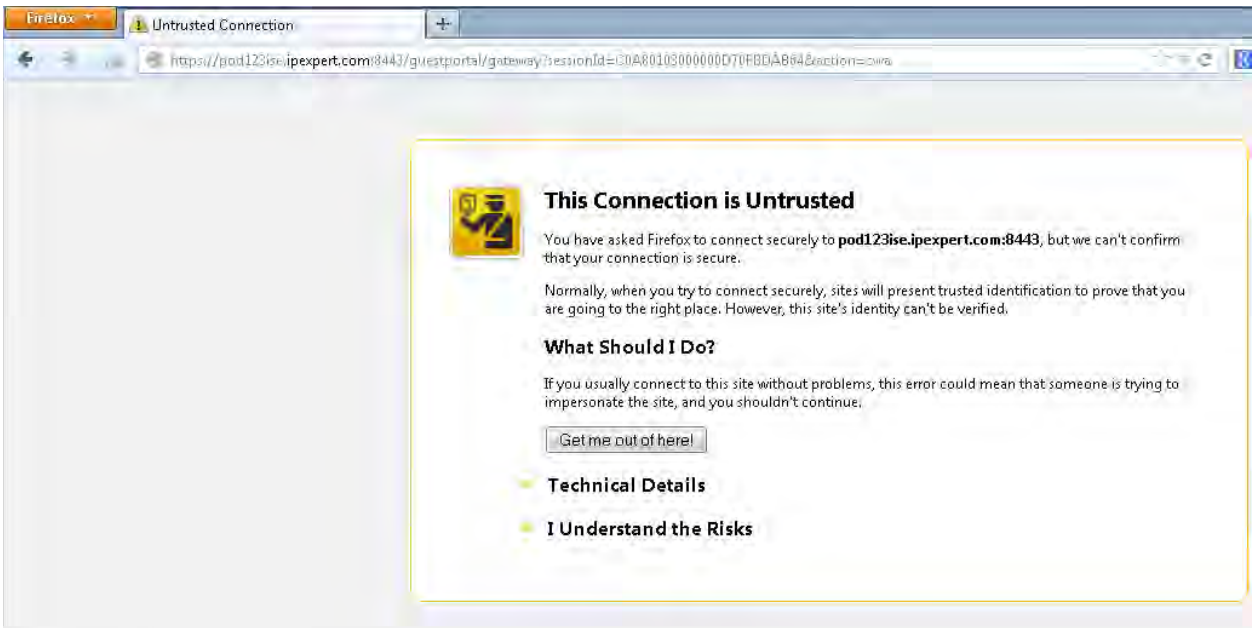
Add a route on Test PC for ISE G0 interface and the AD. Make sure you disable or stop anyconnect service.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>route add 10.200.5.232 mask 255.255.255.255 192.168.250.1
 OK!

C:\Windows\System32>route add 10.1.1.101 mask 255.255.255.255 192.168.250.1
 OK!
```

Make sure the AD has a DNS entry for your ISE for G0 interface (podxxxise.ipexpert.com)



Browse to 192.168.1.250 and you should be redirected to ISE. Confirm the security exception.



Verify from SW3

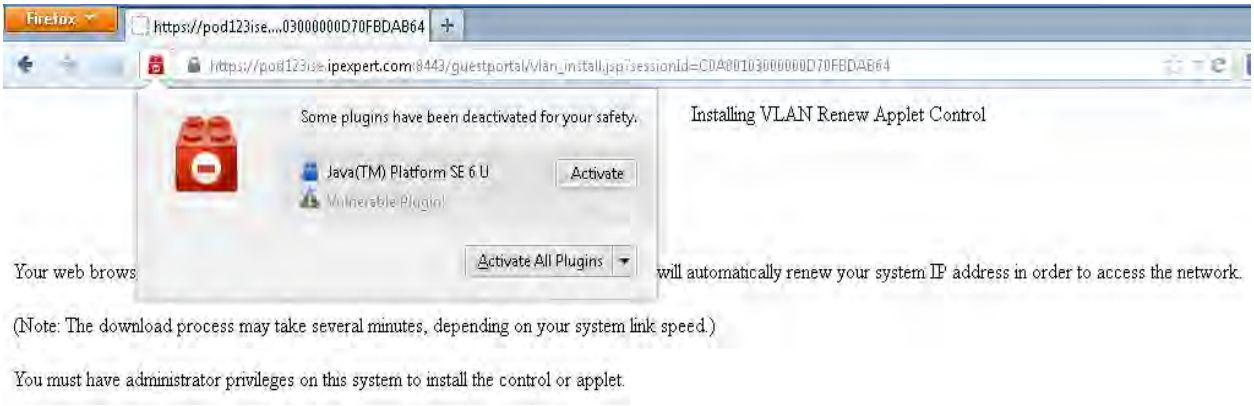
```
SW3#sh auth sess interface g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  Unknown
            User-Name:  00-0C-29-F4-60-2B
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  250
              ACS ACL:  xACSACLx-IP-CONTRACTORS_dACL-4d3056dd
     URL Redirect ACL:  REDIRECT
         URL                                                                Redirect:
https://pod123ise.ipexpert.com:8443/guestportal/gateway?sessionId=C0A80103000
000D70FBDAB64&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000D70FBDAB64
      Acct Session ID:  0x000000C7
               Handle:  0x130000D8

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run

----------------------------------------
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4a0.b24f
           IP Address:  192.168.60.10
            User-Name:  00-1B-D4-A0-B2-4F
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-508adc03
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000D60FBD888F
      Acct Session ID:  0x000000C6
               Handle:  0x110000D7
```

```
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

Enter the credentials.

Accept the AUP

Activate the JavaPlugin for VLAN DHCP renew.



Verify from SW3

```
SW3#sh authentication sessions interface g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  192.168.250.115
            User-Name:  IPXEMP1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  40
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000D70FBDAB64
      Acct Session ID:  0x000000C7
               Handle:  0x130000D8

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run

----------------------------------------
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4a0.b24f
           IP Address:  192.168.60.10
            User-Name:  00-1B-D4-A0-B2-4F
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
```

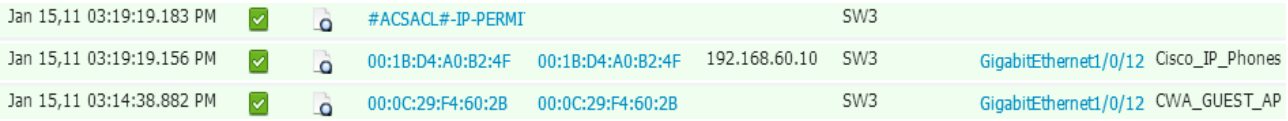
```
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-508adc03
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000D60FBD888F
      Acct Session ID:  0x000000C6
               Handle:  0x110000D7

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

ISE

Live authentication

Go to Operations->Authentications

Before authentication



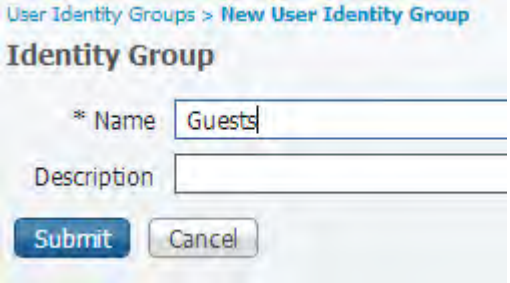
After authentication

Task 2: Configuring Guest Access

- Configure ISE to provide guest access for visitors. IPX employees should be able to create guest accounts and act like sponsors. Visitors should also be allowed create their own guest account. After successful authentication and authorization, the guest users should be given only Internet access and any traffic destined to the internal network of 192.168.0.0/16 should be dropped. Also configure a VLAN change from the default restricted VLAN 250 to the guest VLAN of 200.
- Create a new Identity group called “Guests” on the ISE

Solutions

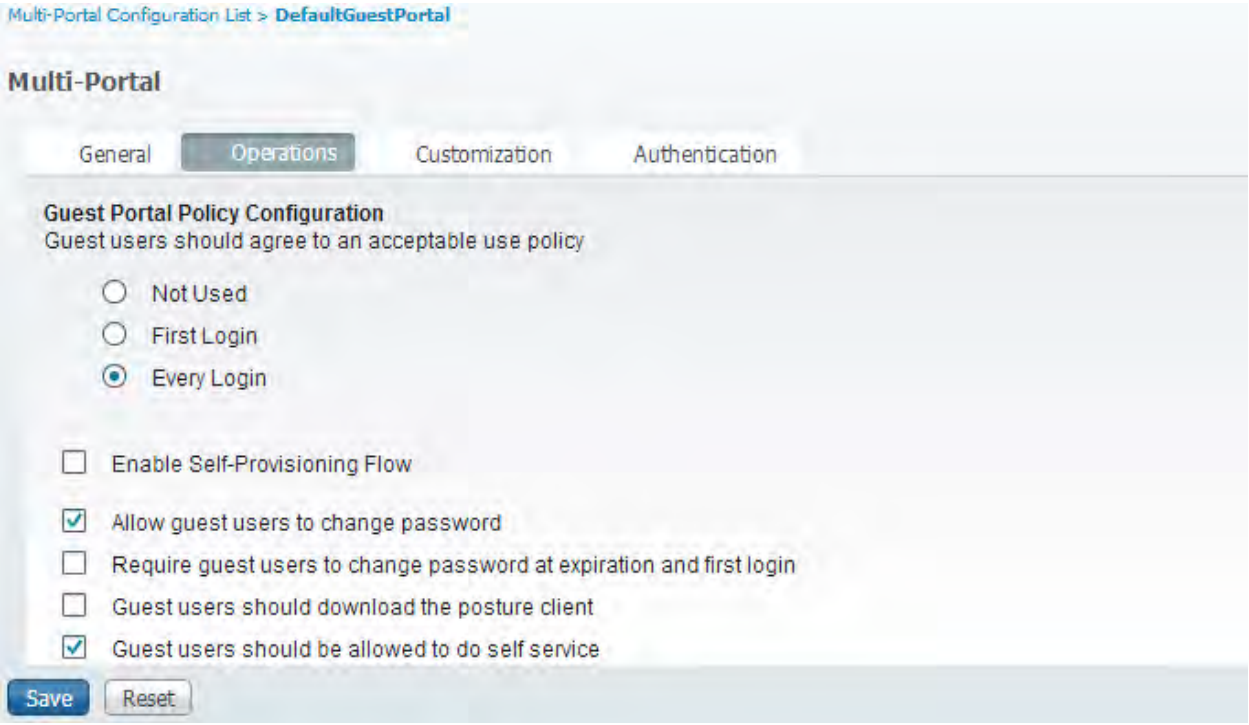
Step 1: Go to **Administration->identity Management-> Groups**. Click on Add.



- Configure the guest portal to support self-service and guest must agree the AUP on every login. Map the guest users who use self-service to "Guest" role/identity group. They should be given access for 1 hour from the account creation.

Solutions

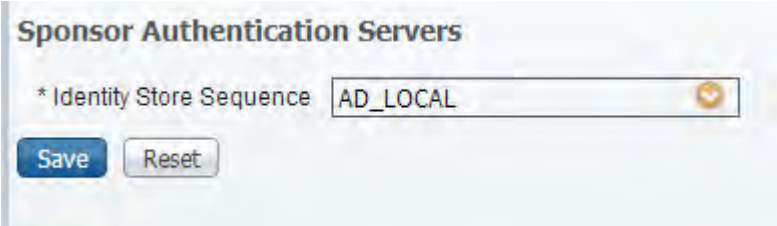
Step 1: Go to **Administration->Web Portal Management->Settings->Guest->Multi-Portal Configurations**. Click on DefaultGuestPortal.



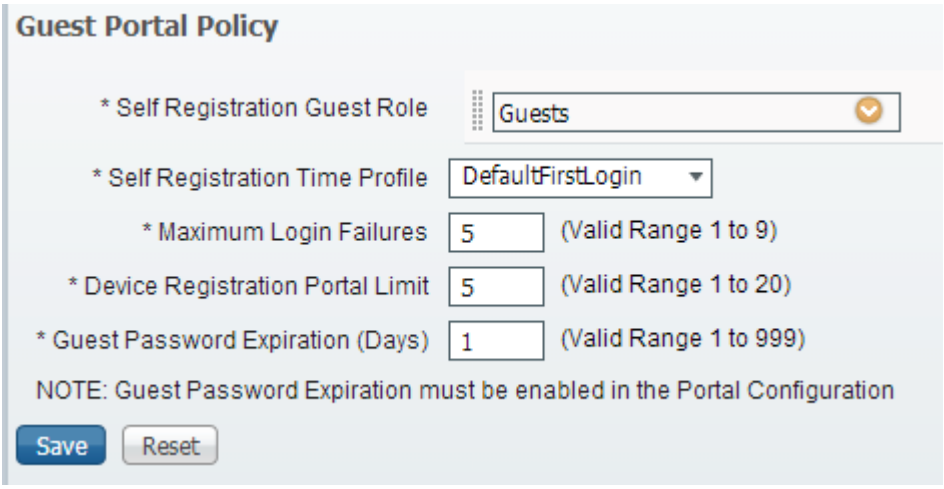
- Sponsor should be authenticated using the identity source sequence created earlier.

Solutions

Step 1: Go to **Administration->Web Portal Management->Settings->Sponsor->Authentication Source**.



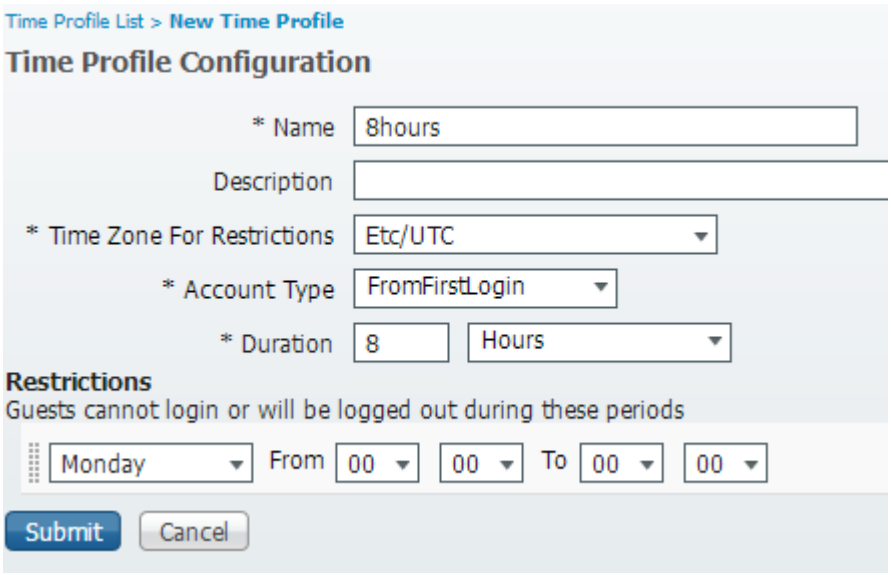
Step 2: Go to **Administration->Web Portal Management->Settings->Guest->Portal Policy**. Change the self-registration role to "Guests".



- Create a new time profile called "8hours" which provides 8 hours of access from the first login.

Solutions

Step 1: Go to **Administration->Web Portal Management->Settings->Guest->Time Profiles**. Click on Add.



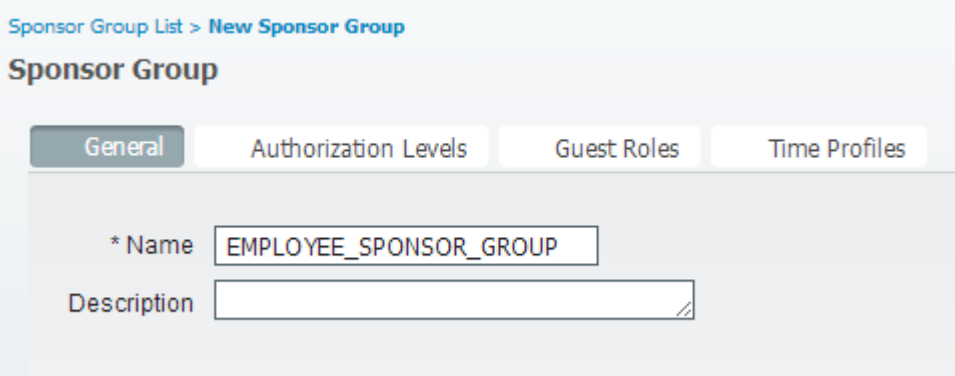
- Create sponsor policy as per the below table

Employee Sponsor Group	
General	
Name	EMPLOYEE_SPONSOR_GROUP
Authorization Levels	
Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	No
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	Own Accounts
Suspend/Reinstate Accounts	Own Accounts
Account Start Time	1 day
Maximum Duration of Account	1 day
Guest Roles	
	Guest
Time Profiles	
Pick:	DefaultStartEnd 8Hours

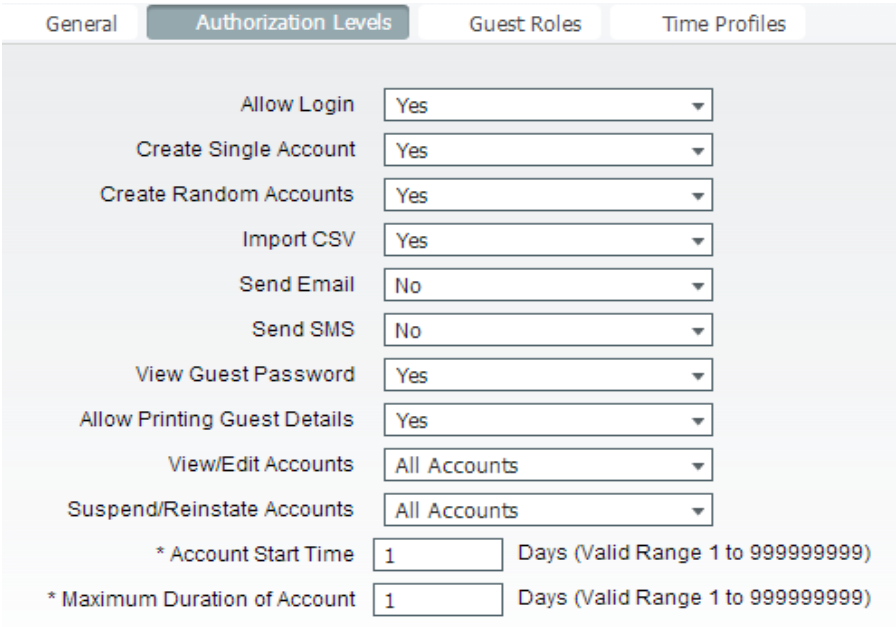
Solutions

Step 1: Go to **Administration->Web Portal Management->Guest->Guest Sponsor Groups**. Click on Add.

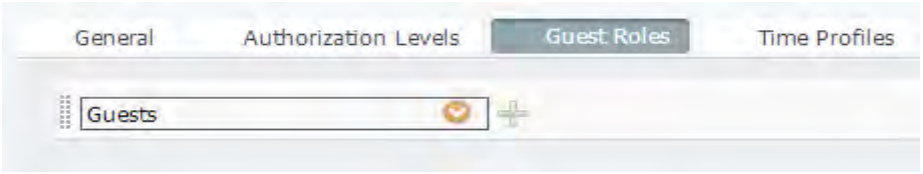
Create the name as per the task (EMPLOYEE_SPONSOR_GROUP)



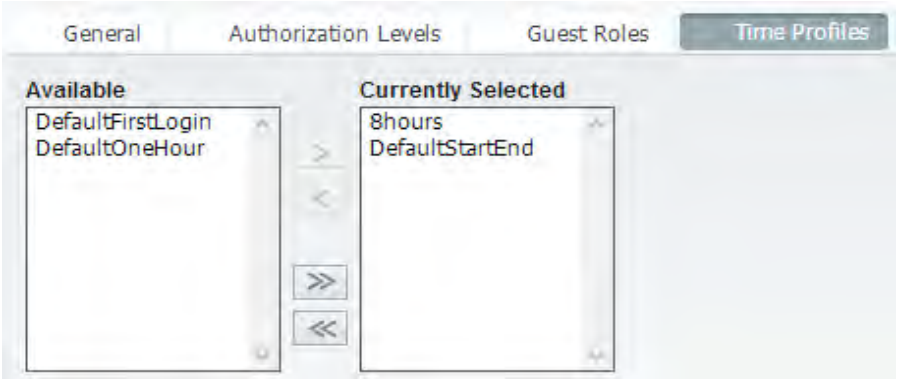
Click on Authorization tab and set the permission as per the task



Click on Guest Roles and select “Guests”



Click on Time Profiles tab and select the profiles as per the task. Then click on submit.

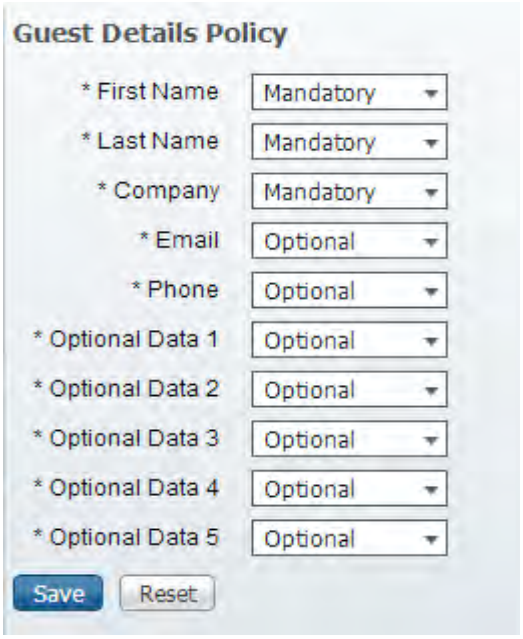


- When creating guest accounts only the first name, last name, company name and time zone details are mandatory.

Solutions

Step 1: Go to **Administration->Web Portal Management->Guest->Details Policy**. Click on Add.

Time zone is mandatory by default

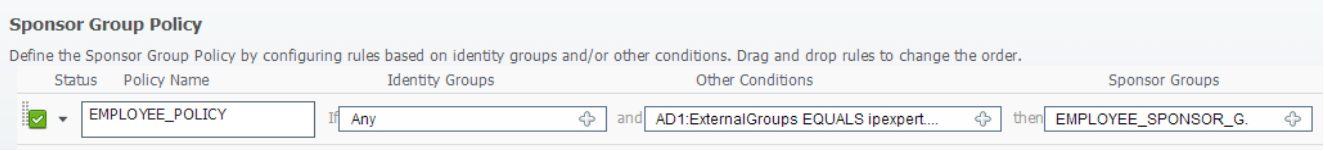


- Configure sponsor group policy as per the below table and remove all other pre-defined policies. Only IPX_EMP group can create guest accounts.

Rule Name	Identity Groups	Other Conditions	Sponsor Groups
EMPLOYEE_POLICY	Any	AD1:ExternalGroups EQUALS ipexpert.com/Users/**IPX_EMP**	EMPLOYEE_SPONSOR_GROUP

Solutions

Step 1: Go to **Administration->Web Portal Management->Sponsor Group Policy** and configure as per the task. (Condition = AD group of IPX_EMP and sponsor group = EMPLOYEE_SPONSOR_GROUP)



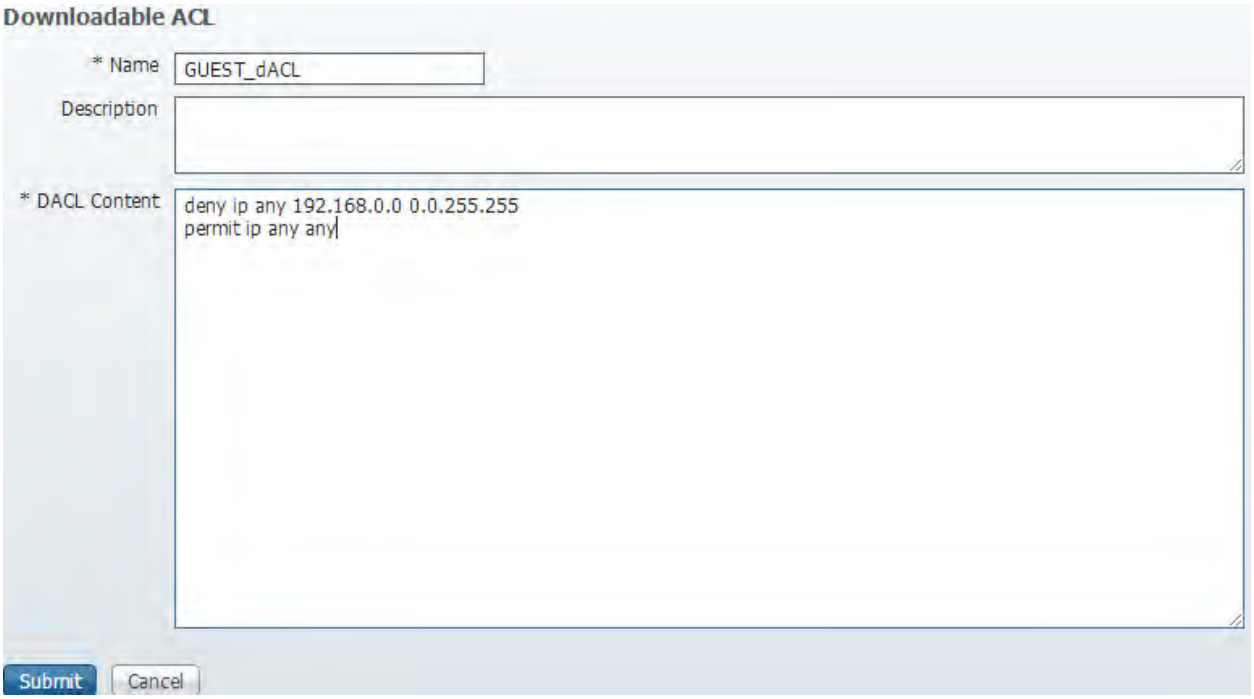
- Configure dACL and Authorization policies for the guest account and map it to the appropriate Guest identity group in the authorization policy.
- Create a dACL as per the below table.

Downloadable ACL	
Name	GUEST_dACL
DACL Content	deny ip any 192.168.0.0 0.0.255.255 permit ip any any

-
-

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Downloadable ACLs**. Click on **Add.**

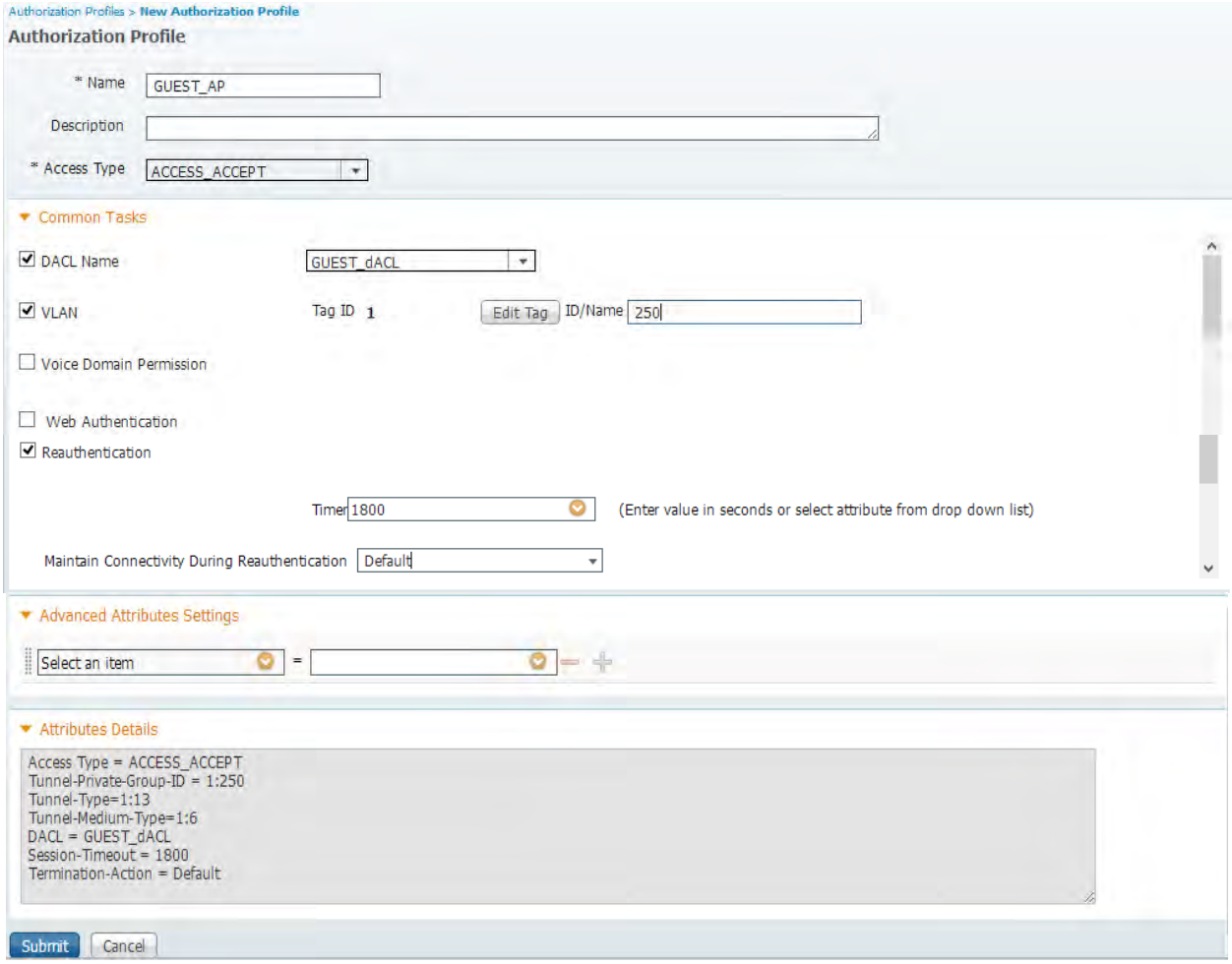


- Create a guest authorization profile as per the below table

Authorization Profile	
Name	GUEST_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	GUEST_dACL
VLAN	250
Advanced Attribute Settings	
Idle-Timeout	30 minutes
Radius:Termination-Action	Default / 0 (Terminate)

Solutions

Step 1: Go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Click on **Add.**



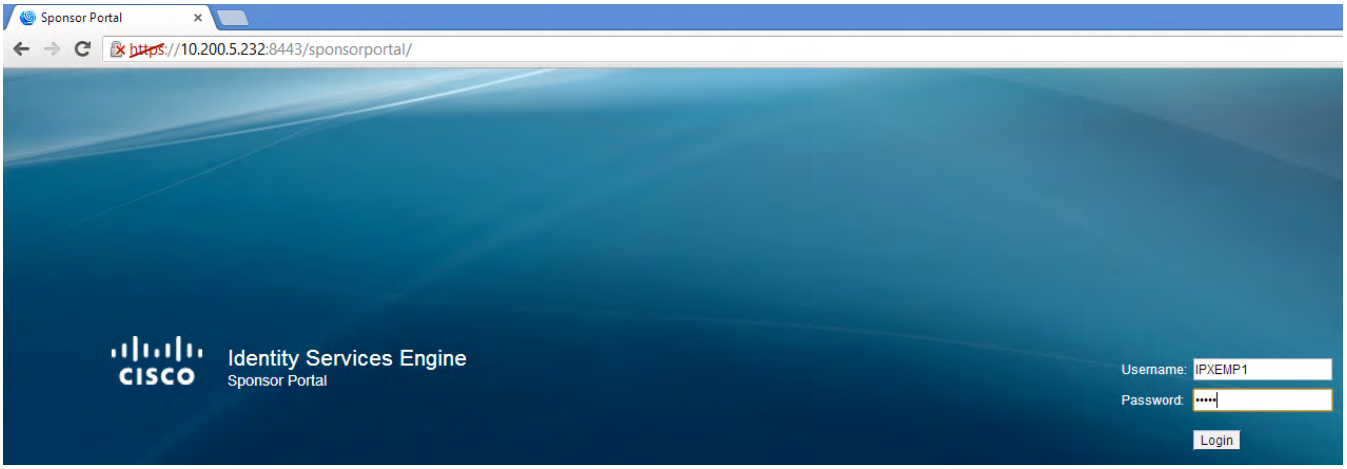
- Create a the guest authorization policy as per the below table

Name		Identity Group		Conditions		Authorization
GUEST	IF	Guest	AND	-----	THEN	GUEST_AP

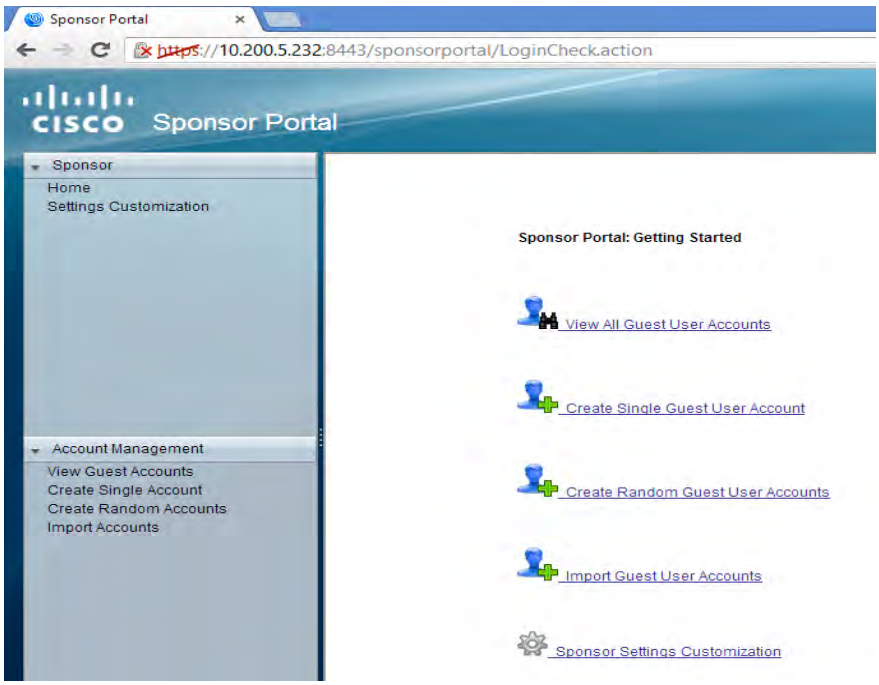
Solutions

Step 1: Go **Policy->Authorization** and configire a new rule as per the parameters given in the task. Add this policy rule the default rule.

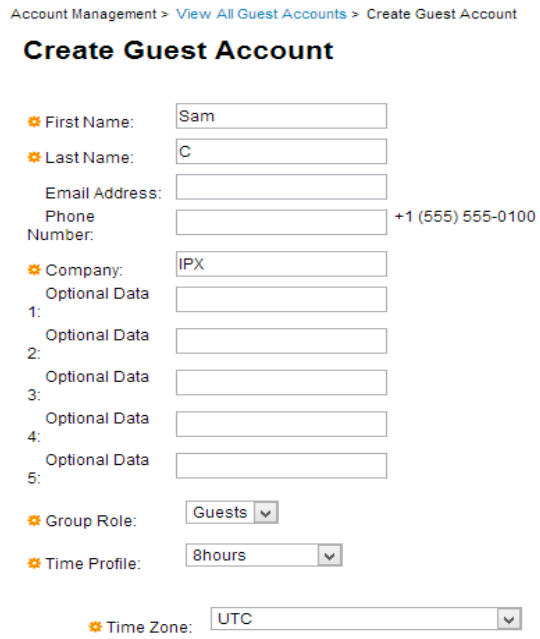
Browse to the sponsor portal https://10.x.x.x:8443/sponsorportal (Gig0 interface) and create a user.



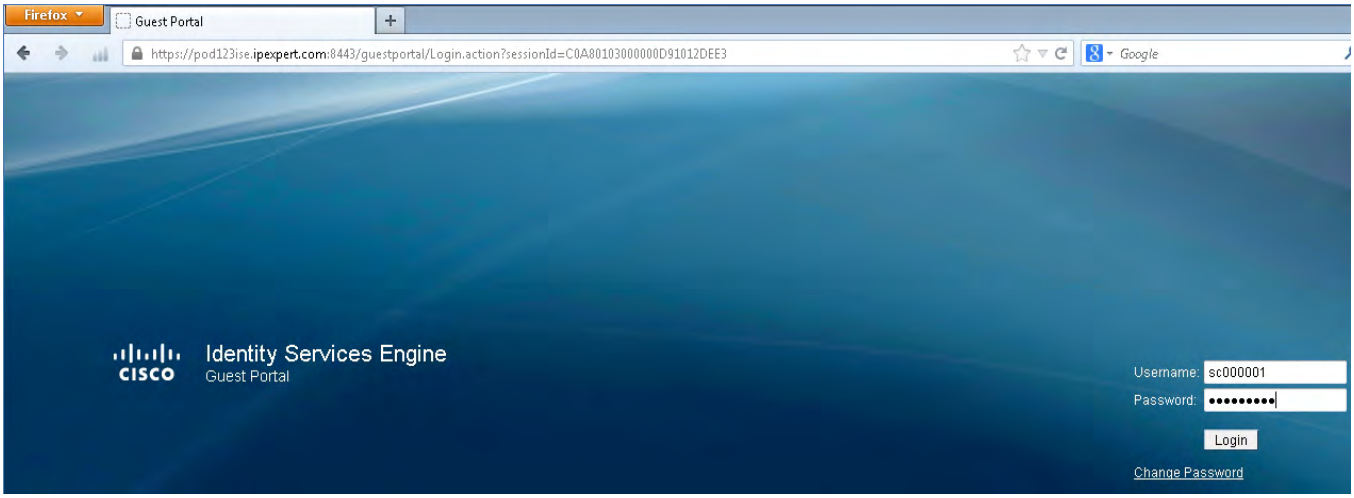
Click on "Create Single Guest User Account"



Create a Guest user account



Shut and unshut G1/0/12 of SW3. Test from TestPC2. Browse to 192.168.250.1 and you should be redirected to guest portal.



Accept the AUP and activate the java plugin after you enter the login credentials. Then verify on SW3.

Before successful guest authentication

```
SW3#show authentication sessions interface g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  192.168.250.115
            User-Name:  00-0C-29-F4-60-2B
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  250
              ACS ACL:  xACSACLx-IP-CONTRACTORS_dACL-4d3056dd
     URL Redirect ACL:  REDIRECT
          URL Redirect:
https://pod123ise.ipexpert.com:8443/guestportal/gateway?sessionId=C0A80103000
000D91012DEE3&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000D91012DEE3
      Acct Session ID:  0x000000CB
               Handle:  0x880000DA

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
<SNIP>
```

After successful guest authentication

```
SW3#show authentication sessions interface g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  192.168.250.115
            User-Name:  sc000001
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  250
      Session timeout:  28740s (server), Remaining: 28686s
       Timeout action:  Reauthenticate
         Idle timeout:  N/A
    Common Session ID:  C0A80103000000D91012DEE3
      Acct Session ID:  0x000000CB
               Handle:  0x880000DA

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

Live Authentication

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Jan 15,11 05:15:16.622 PM	✓		sc000001	00:0C:29:F4:60:2B	192.168.250.1...	SW3	GigabitEthernet1/0/12	GUEST_AP	Guests,Profiled:Win...

Task 3: Configuring Wireless Guest Access and CWA

- Configure ISE and WLC to provide guest access and CWA.
- Configure the WLC with new interfaces and WLAN's on WLC to support guest access. Guest user prior to successful authentication should be placed in restricted VLAN/interface (VLAN 250) on the WLC and after successful authentication should be placed in VLAN 200 i.e. the Guest VLAN/interface on the WLC with the same restrictions used for the wired users.
- Create new interfaces on the WLC as per the below table.

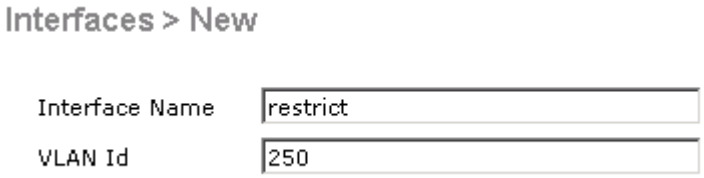
Restrict Interface	
Interface Name	restrict
Quarantine	(unchecked)

Port Number	1
VLAN Identifier	250
IP Address	192.168.250.2
Netmask	255.255.255.0
Gateway	192.168.250.1
Primary DHCP Server	10.1.1.101
Secondary DHCP Server	-
ACL Name	none

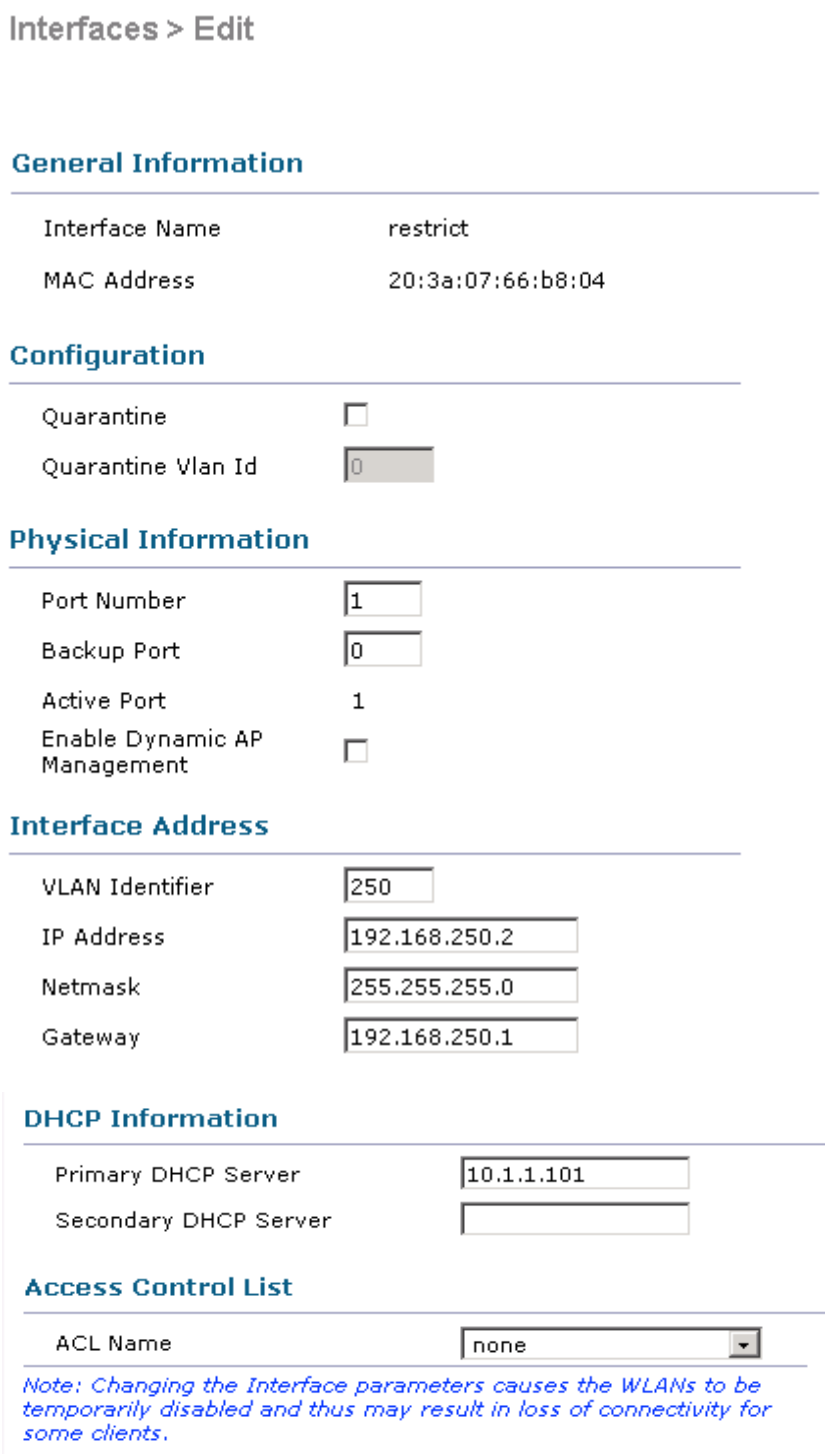
Guest Interface	
Interface Name	ipx_guest
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	200
IP Address	192.168.200.2
Netmask	255.255.255.0
Gateway	192.168.200.1
Primary DHCP Server	10.1.1.101
Secondary DHCP Server	-
ACL Name	none

Solutions

Step 1: Go **Controllers -> Interfaces**. Click on New. Configure the interface name and VLAN ID as per the task.

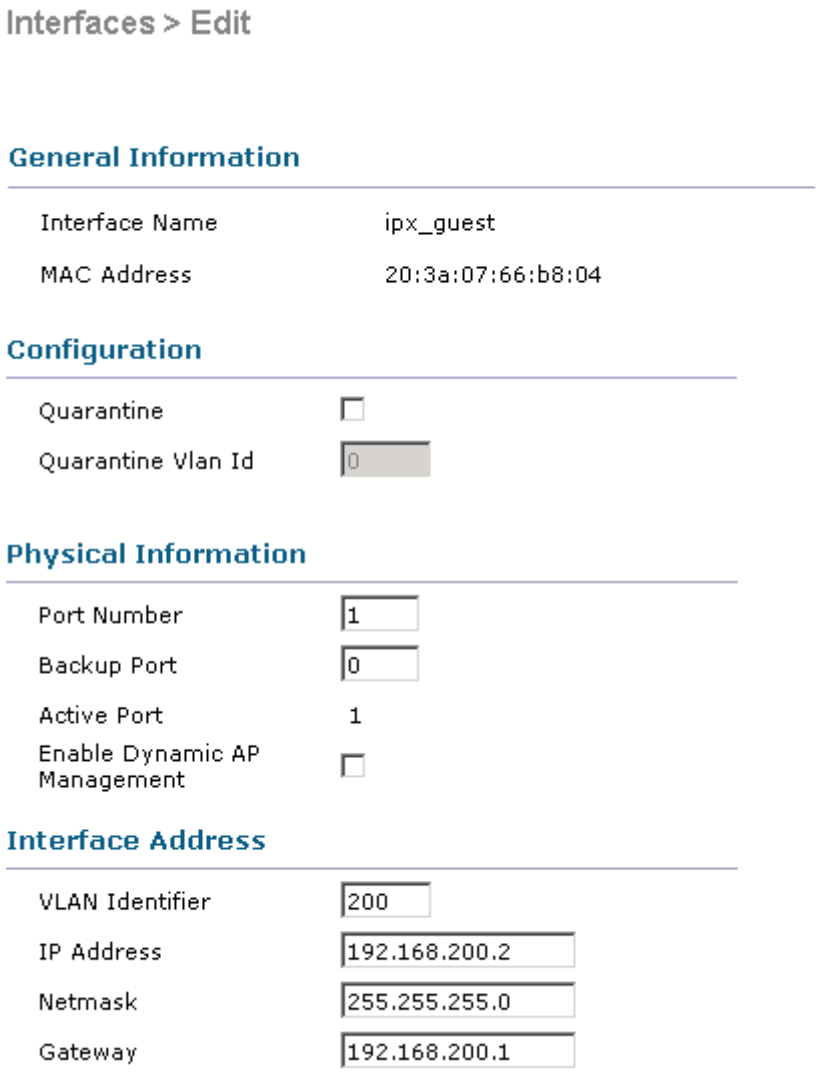


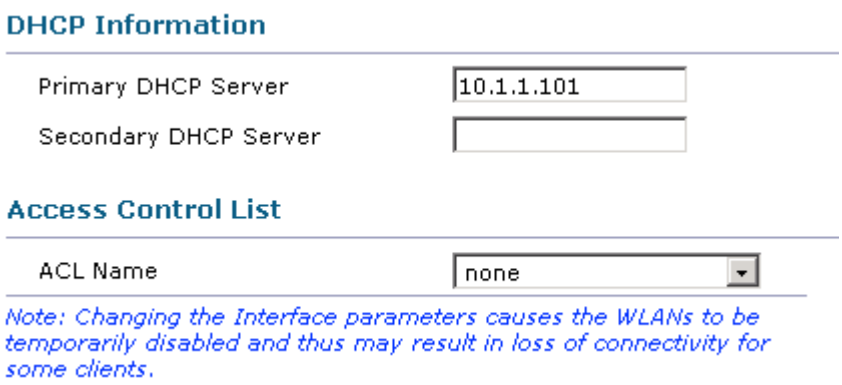
Step 2: Go **Controllers -> Interfaces**. Click on restrict to configure that interface as per the task and click on apply.



Step 3: Go **Controllers -> Interfaces**. Click on New. Configure the interface name and VLAN ID as per the task.

Step 4: Go **Controllers -> Interfaces**. Click on restrict to configure that interface as per the task and click on apply.



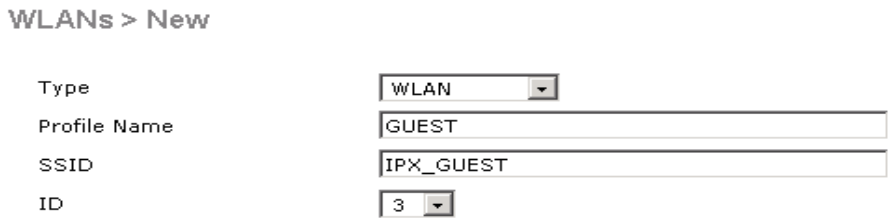


- Create a new WLAN for guests to connect as per the below table.

IPX_GUEST	
Type	WLAN
Profile Name	IPX_GUEST
SSID	IPX_GUEST
Status	✓ Enabled
Radio Policy	All
Interface / Group	ipx_guest
Broadcast SSID	✓ Enabled
Security – Layer 2	
Layer 2 Security	None/MAC-Filtering
Security – Layer 3	
Layer 3 Security	None
Web Policy	(Not checked)
Security – AAA Servers	
Authentication Server #1	10.1.1.150, Port:1812
Accounting Server #1	10.1.1.150, Port:1813
Advanced	
Allow AAA Override	✓ Enabled
NAC State	Radius NAC

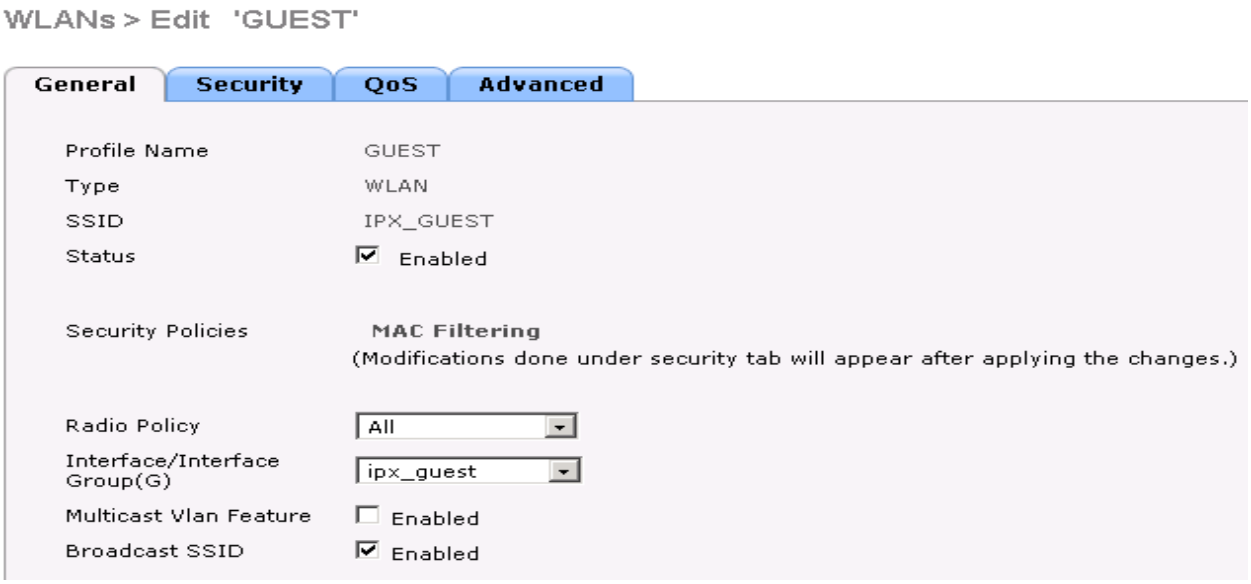
Solutions

Step 1: Go to WLANs tab select “create new” and click on Go. Create WLAN for employees. Make sure SSID matches as stated in the task.

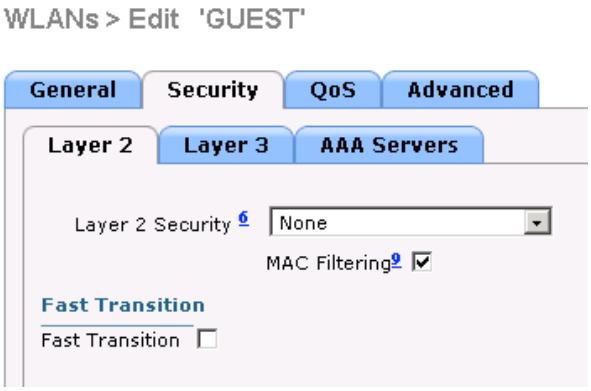


Step 2: Click on Edit "IPX_GUEST" WLAN and configure WLAN parameters as per the task

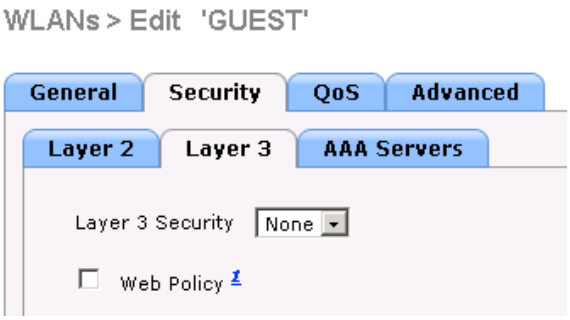
Make sure the status is set to "Enabled" and interface is set to "ipx_guest"



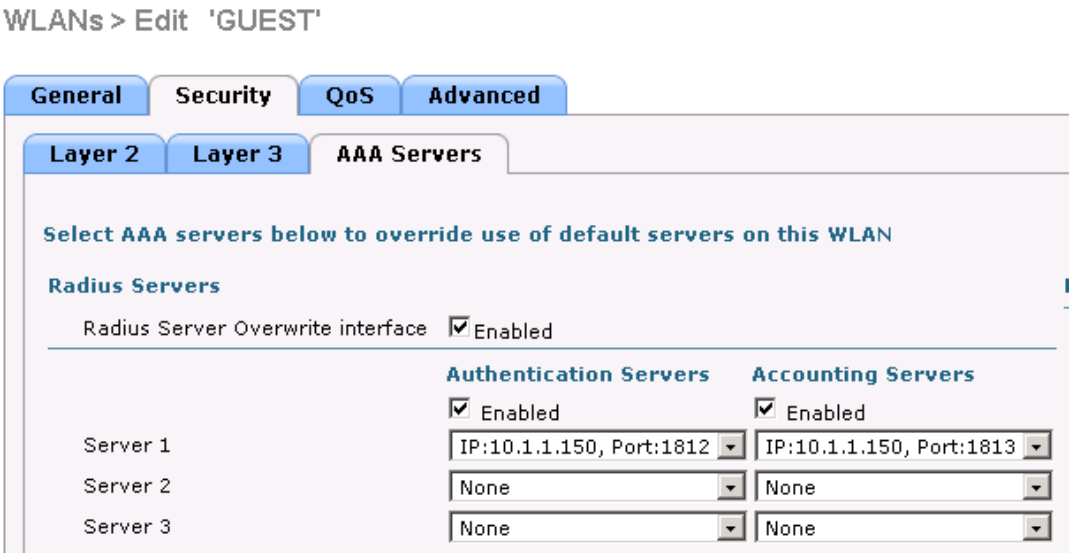
Click on the Security Tab. Select Layer 2 Security as None



Under the Security Tab navigate to Layer 3 sub tab and make sure None is selected



Under the Security Tab navigate to AAA Server sub tab and add ISE as the AAA server.



- Configure the WLC with appropriate ACL's to support the guest access, CWA and restricted access.

Solutions

WLC

Step 1: Go to **Security->Access Control Lists.** Click on New and configure the ACL's similar to ISE. Make sure the name matches as per the task.

Access Control Lists > Edit

General

Access List Name	RESTRICT_dACL
Deny Counters	0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0 / 0.0.0.0	4.4.4.4 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
2	Deny	0.0.0.0 / 0.0.0.0	5.5.5.5 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
3	Deny	0.0.0.0 / 0.0.0.0	20.4.4.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
4	Deny	0.0.0.0 / 0.0.0.0	20.5.5.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
5	Deny	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
6	Deny	0.0.0.0 / 0.0.0.0	192.168.40.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.50.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	192.168.60.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
9	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTP	Any	Inbound	0
10	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTPS	Any	Inbound	0
11	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Access Control Lists > New

Access Control List Name	REDIRECT
ACL Type	(•) IPv4 ( ) IPv6

Access Control Lists > Edit

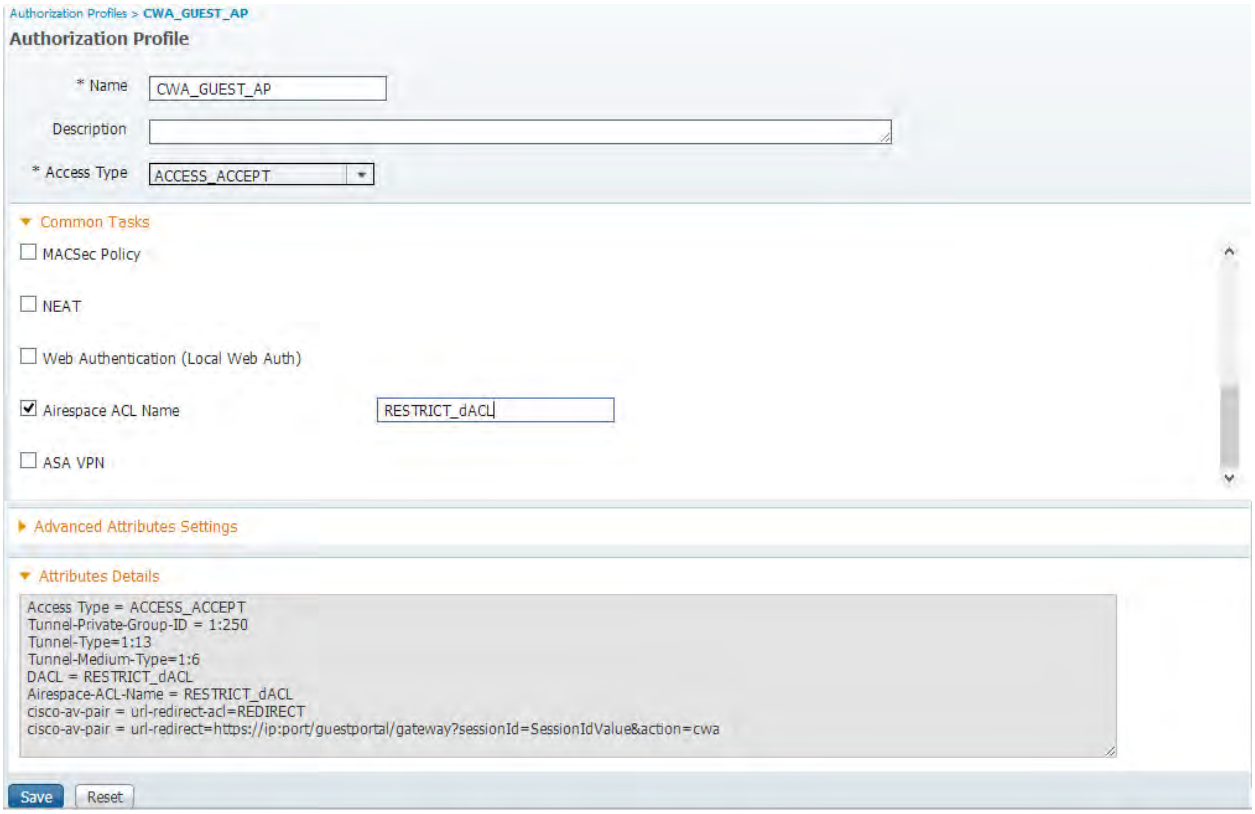
General

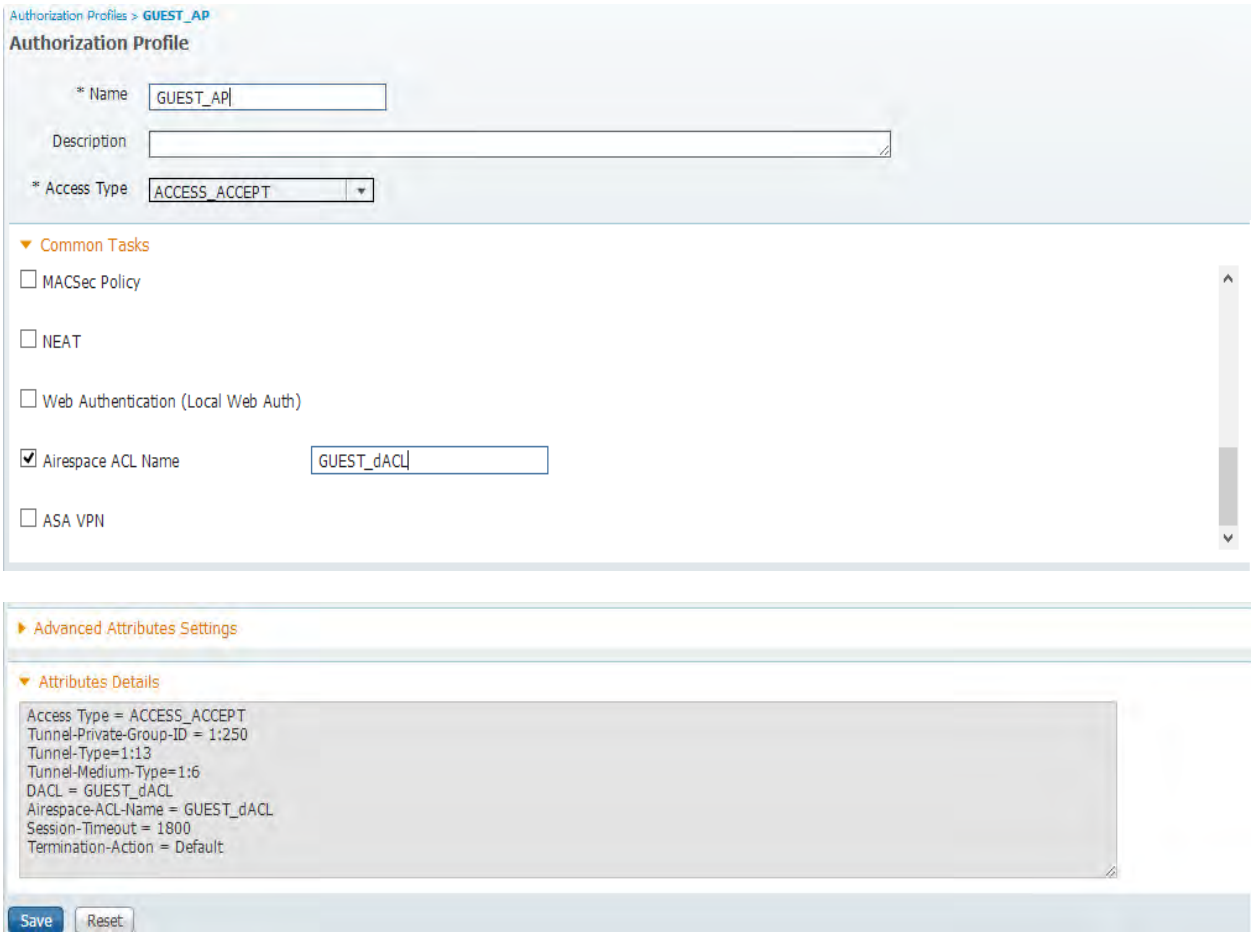
Access List Name REDIRECT

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	0
3	Permit	0.0.0.0 / 0.0.0.0	10.200.5.232 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
4	Permit	10.200.5.232 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	0
6	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

- Re-configure the appropriate authorization profiles to support dACL (Airspace ACL names).

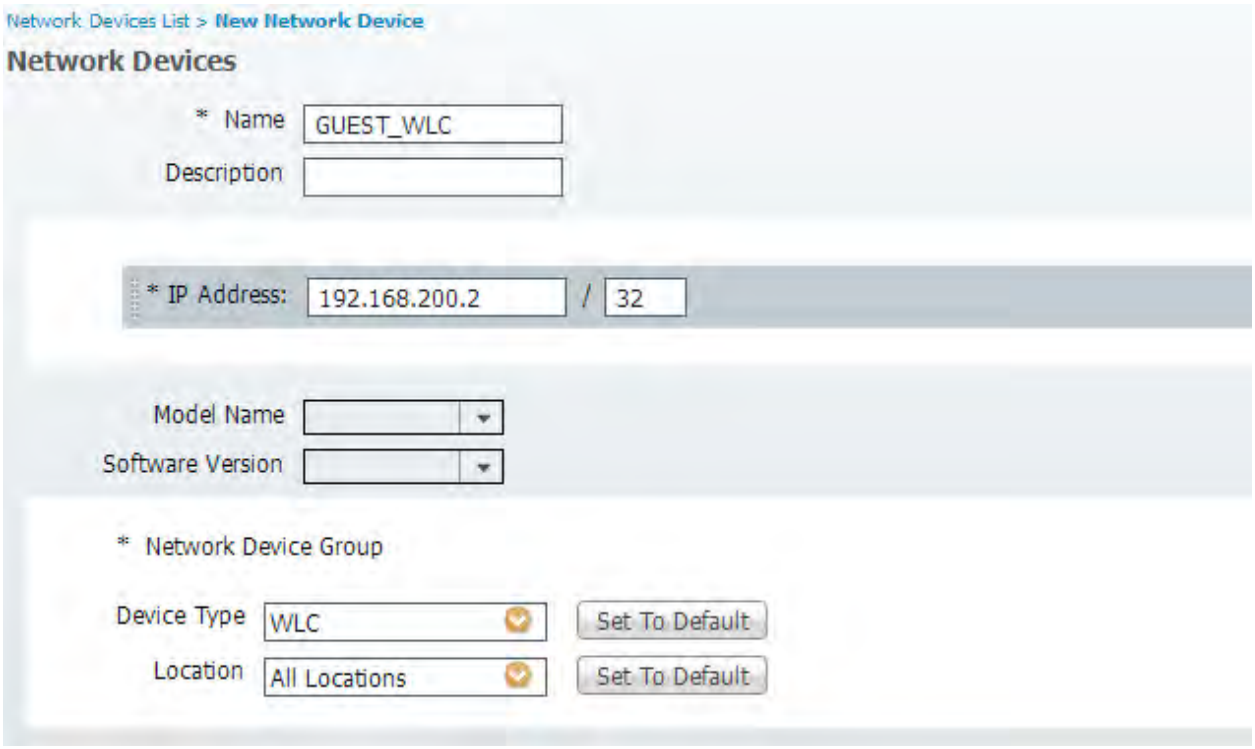




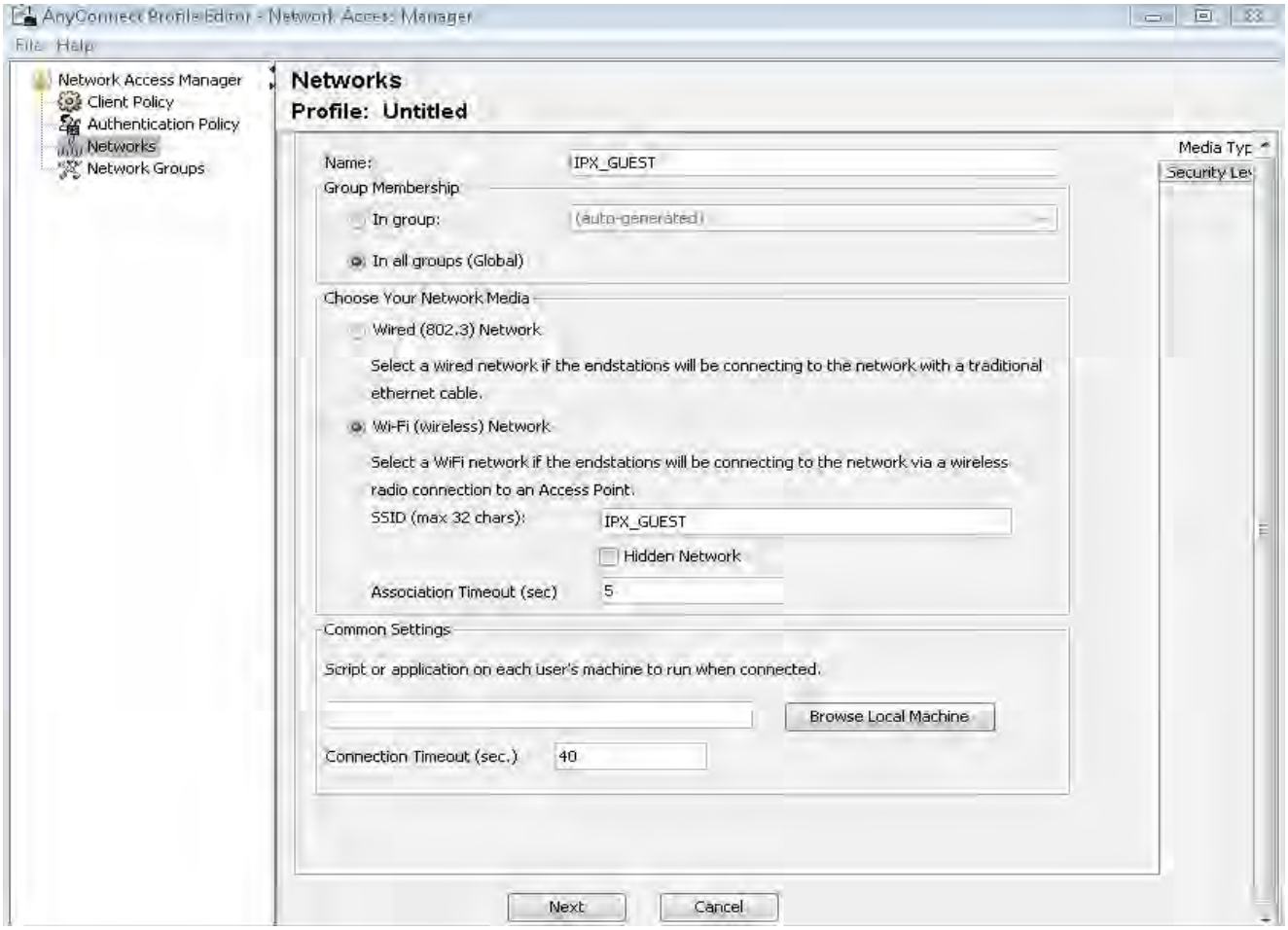
- You may test the configuration from TEST-PC1. Use anyconnect to connect to the network. You are allowed to create new profile for the guest access using NAM profile editor.

Solutions

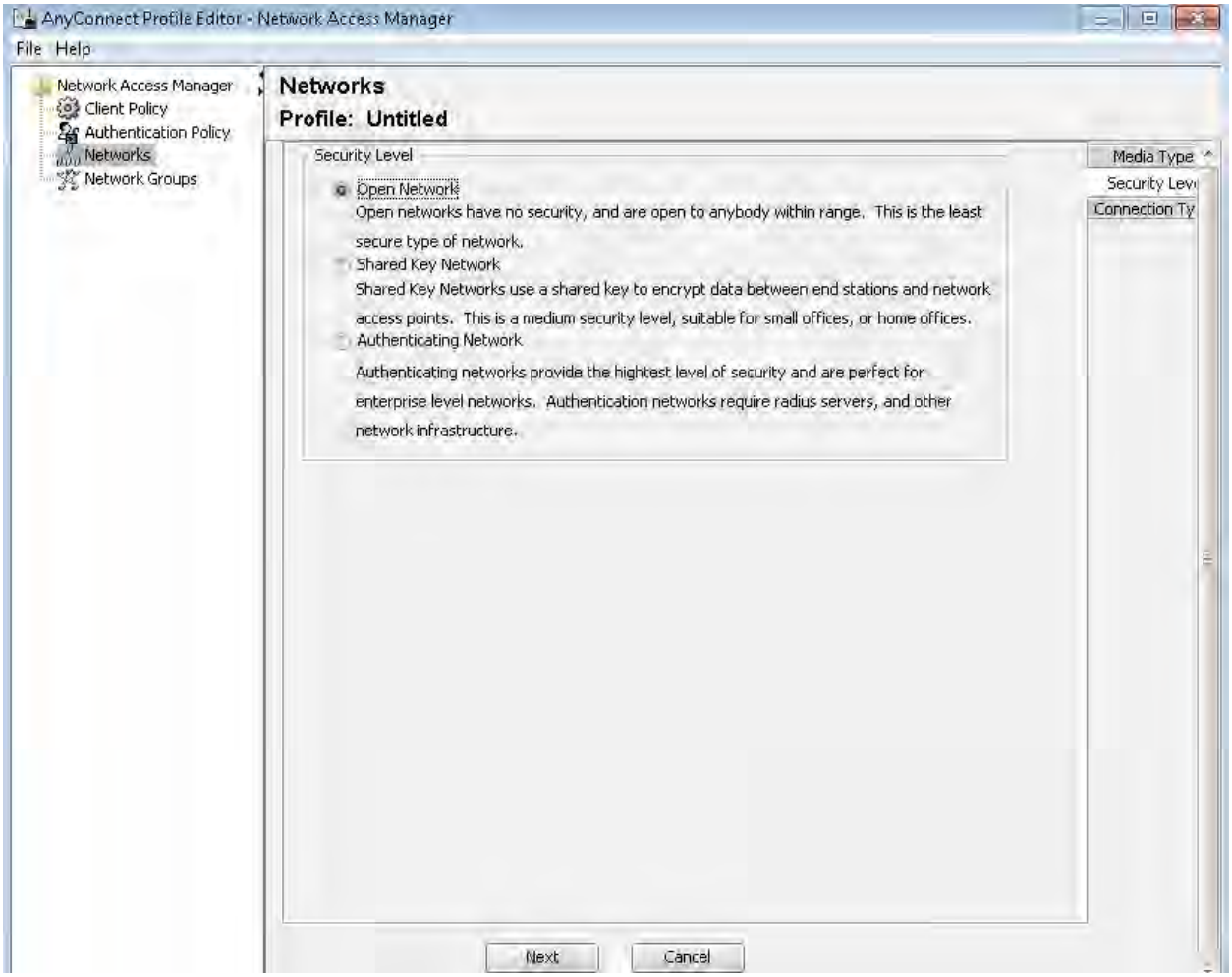
Add 192.168.200.2 (WLC IPX_GUEST) as the AAA client. Use cisco123 as the radius key.



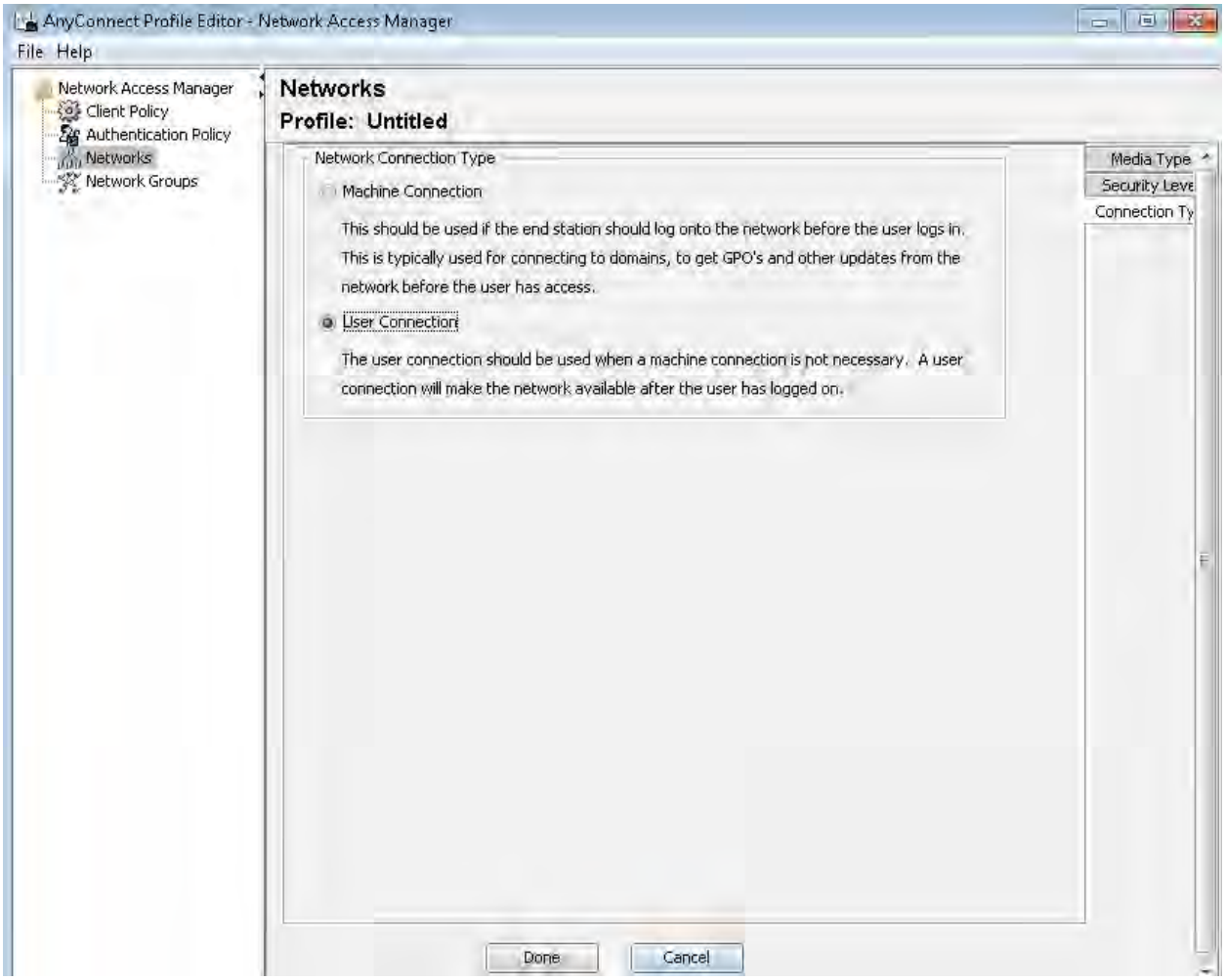
Configure a new anyconnect profile for the IPX_GUEST SSID and connect to the network.



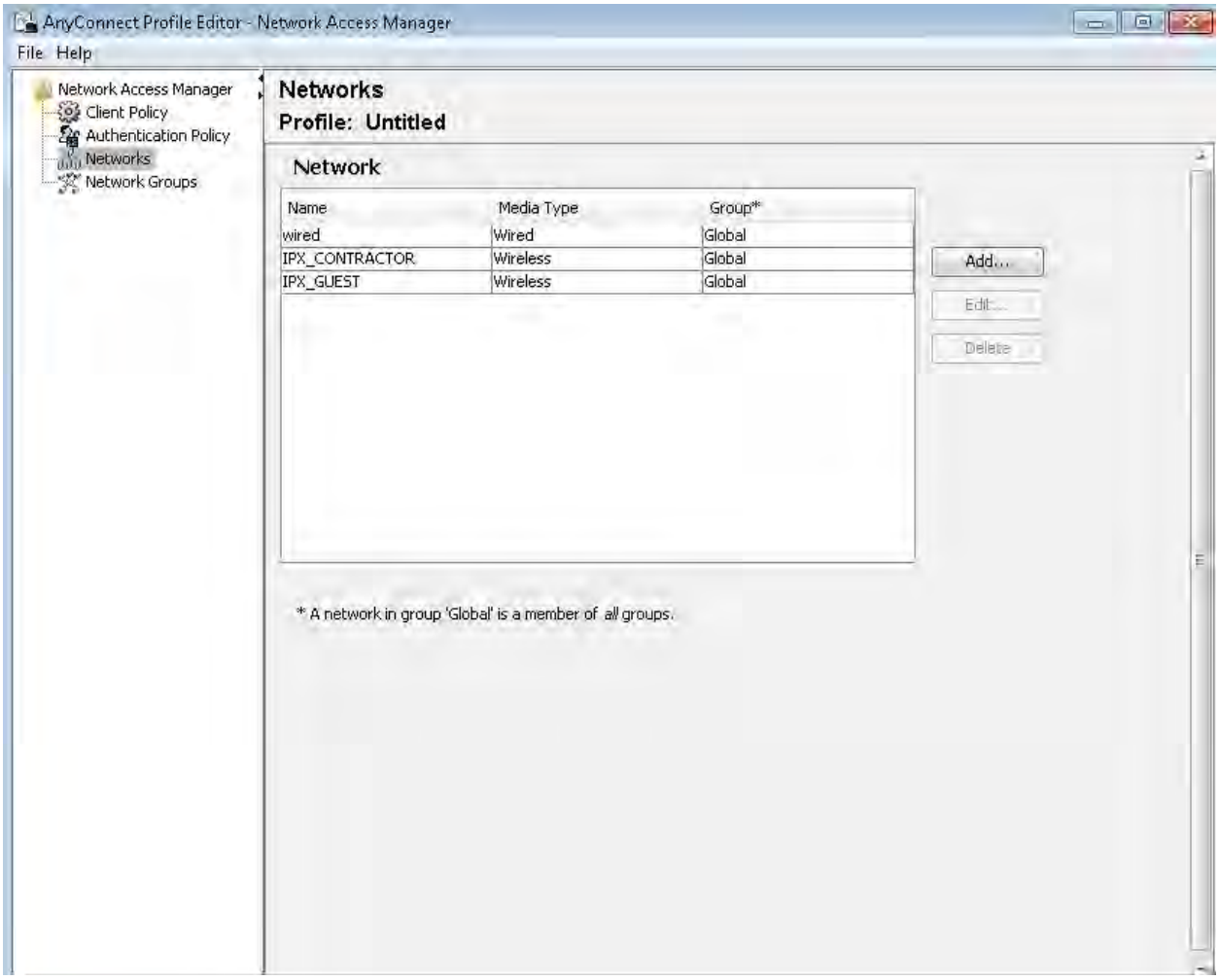
Choose Open Network



Choose User authentication and click on Done.



Perform Network Repair and enter the user credentials for CWA (IPXEMP1/cisco or IPXCON1/cisco) else the guest user ID/password created by the sponsor.



In the WLC, go to **Monitoring->Clients**

Clients > Detail

Client Properties

MAC Address	00:25:9c:f0:41:1d
IPv4 Address	192.168.250.18
IPv6 Address	fe80::9946:6a9c:889c:7aa2,
Client Type	Regular
User Name	
Port Number	1
Interface	restrict
VLAN ID	250
CCX Version	CCXv5
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	POSTURE_REQD
Management Frame Protection	No
UpTime (Sec)	11
Power Save Mode	OFF
Current TxRateSet	
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
KTS CAC Capability	No
802.11u	Not Supported

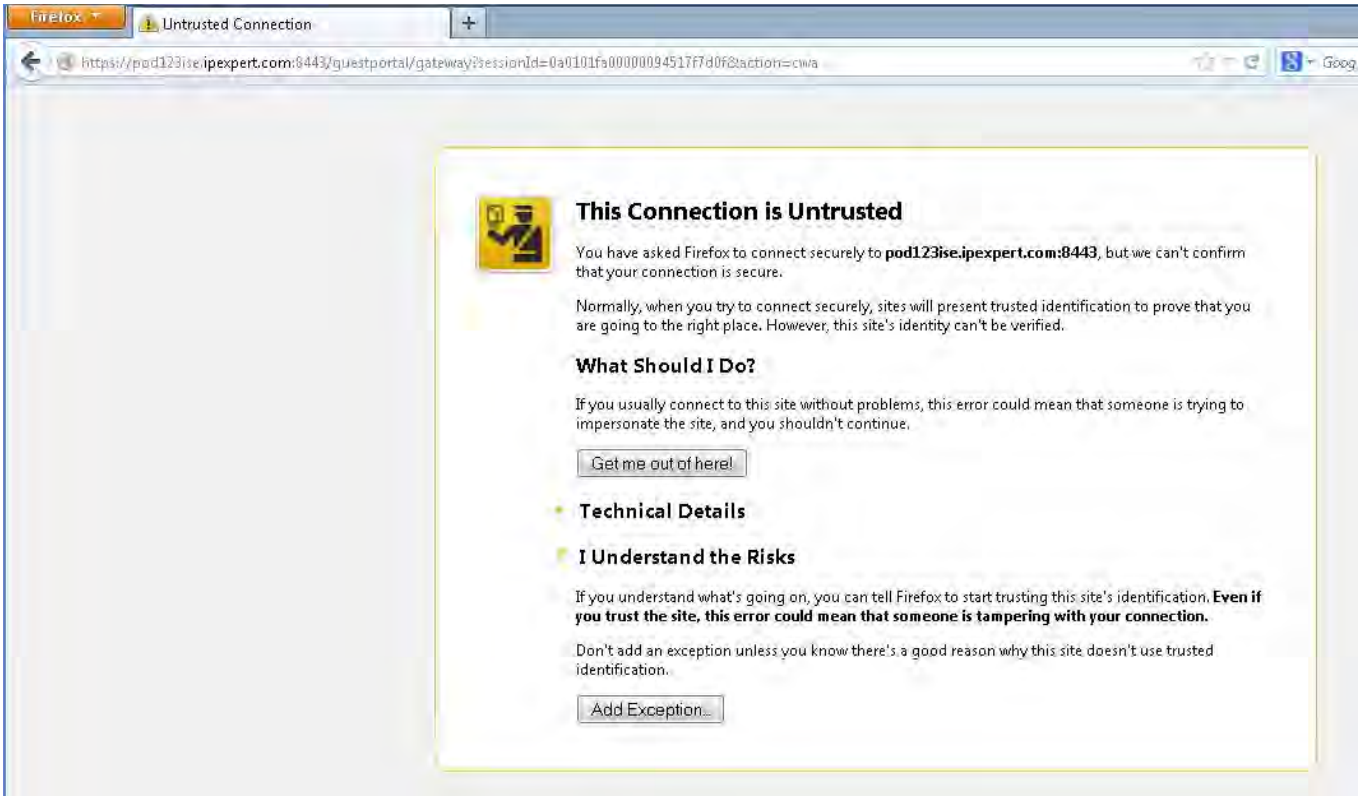
AP Properties

AP Address	00:3a:9a:bc:27:a0
AP Name	APfc99.4763.6414
AP Type	802.11a
WLAN Profile	GUEST
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	1800
WEP State	WEP Disable

Security Information

Security Policy Completed	No
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	POSTURE_REQD
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	REDIRECT
AAA Override ACL Applied Status	Yes
Redirect URL	https://pod123ise.ipexpert.com:8443/guestportal/gatev

Web browse to 192.168.250.1 and you should be redirected to Guest portal



Use IPXEMP1/cisco credentials for CWA. Accept the AUP.

Clients

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
00:25:9c:f0:41:1d	APfc99.4763.6414	GUEST	IPX_GUEST	802.11a	Associated	Yes	1	No

Clients > Detail

Client Properties

MAC Address	00:25:9c:f0:41:1d
IPv4 Address	192.168.250.18
IPv6 Address	fe80::9946:6a9c:889c:7aa2,
Client Type	Regular
User Name	
Port Number	1
Interface	ipx_employee
VLAN ID	40
CCX Version	CCXv5

AP Properties

AP Address	00:3a:9a:bc:27:a0
AP Name	APfc99.4763.6414
AP Type	802.11a
WLAN Profile	GUEST
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	1800
WEP State	WEP Disable

Security Information

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	REDIRECT
AAA Override ACL Applied Status	Yes
Redirect URL	none
IPv4 ACL Name	EMPLOYEE_dACL
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable

Lab-5: Configuring MACSec

Lab-5: Configuring MACsec – This lab is intended to familiarize you with configuring MACSec switch-to-host and MACSec Switch-to-Switch.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 1 hour

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-4 successfully.
Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configuring MACSec Switch-Host

- Enable MACSec on the G1/0/12 of SW3 with a MACSec policy of “must-secure”
- RDP into TEST-PC1 and configure anyconnect NAM to use MACSec with AES-GCM-128 as the encryption algorithm for 802.1x wired connections.
- Re-Configure the employee authorization profile on the ISE to send a MACSec policy of “must-secure” in the RADIUS AV pair.

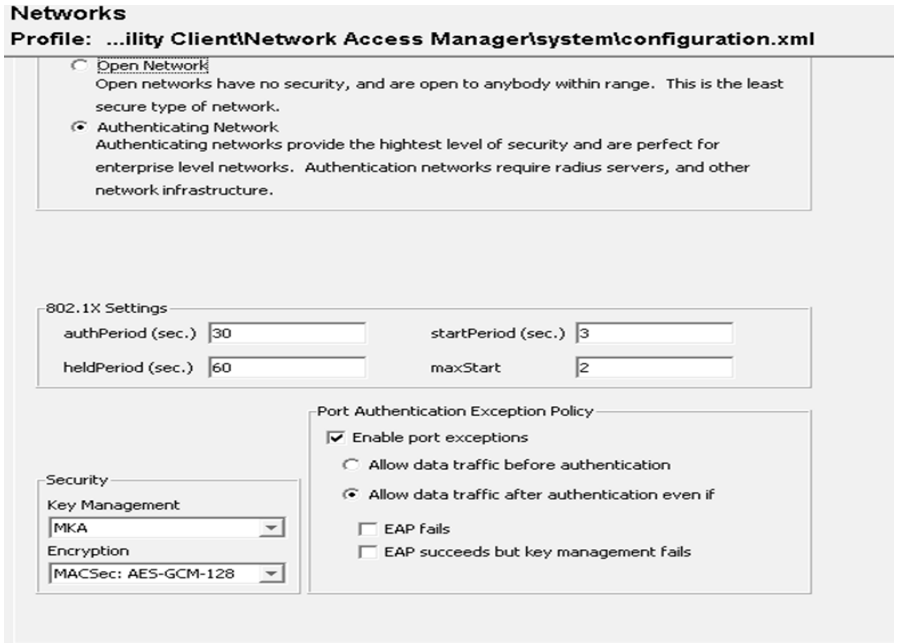
Solutions

SW3

```
int g1/0/12
 authentication linksec policy must-secure
 mka default-policy
 macsec
```

Test PC

Re-configure the existing IPX_EMPLOYEE profile to support MACSec. Save it and click on network repair.



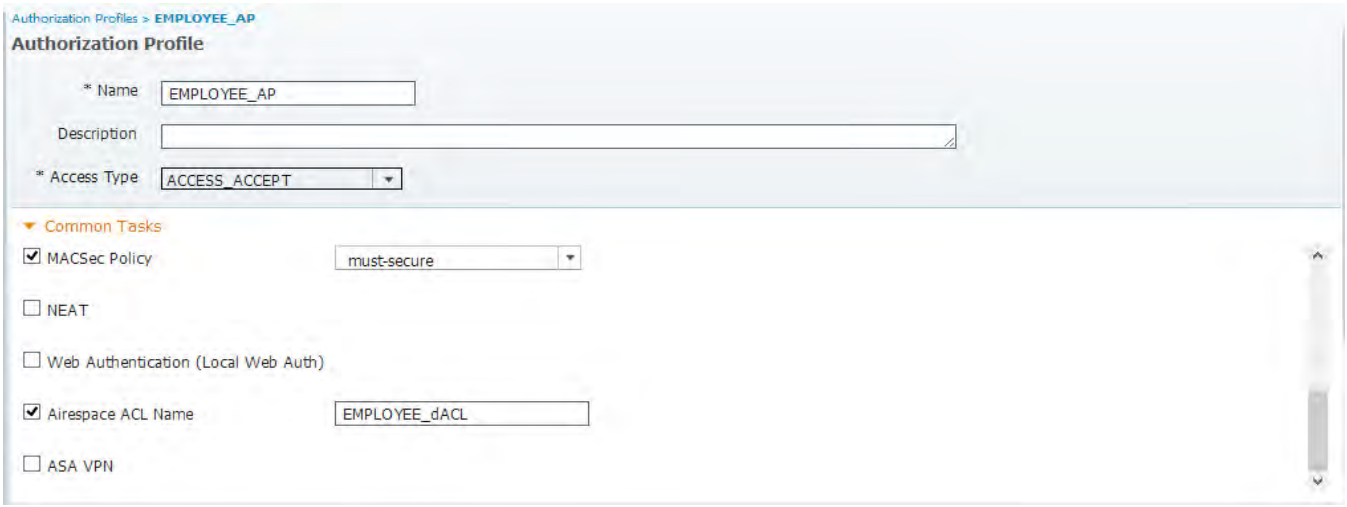

```
SW3#show mka default-policy

MKA Policy Summary...

Policy            KS       Delay   Replay  Window     Conf   Interfaces
Name              Priority Protect Protect Size       Offset Applied
```

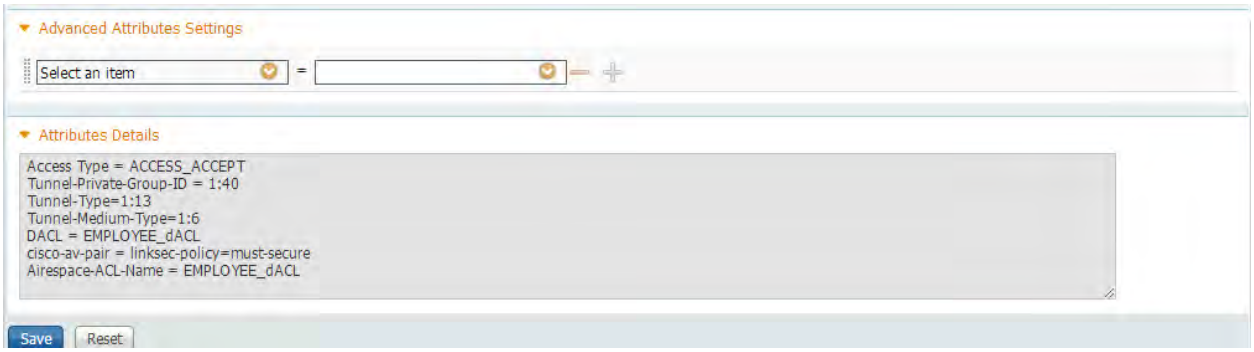
```
================================================================================
==
*DEFAULT POLICY*  0        NO      YES     0          0      Gi1/0/12


CAT3#sh mka sessions  detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI.............. c464.13d1.c58c/0002
Interface MAC Address.... c464.13d1.c58c
MKA Port Identifier...... 2
Interface Name........... GigabitEthernet1/0/12
Audit Session ID......... 0A0900820000062070CFFF47
CAK Name (CKN)........... B3F1A120C28EA4AB388D71EEEF199A21
Member Identifier (MI)... 75C32D267076509136AB728F
Message Number (MN)...... 370
Authenticator............ YES
Key Server............... YES

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... 75C32D267076509136AB728F00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Cipher Suite............. 0080020001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                        MN          Rx-SCI (Peer)
  ------------------------------------------------------------
```

```
  2923BE84E16CD6AE529049F1  369         000c.29f4.602b/0000

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)
  ------------------------------------------------------------

CAT3#sh macsec int g1/0/12
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : C46413D1C58C0002
   Elapsed time : 00:10:07
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (980 / 0)
 Receive Secure Channels
  SCI : 000C2905C1C60000
   Elapsed time : 00:10:07
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 734         Late pkts 10
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 258031
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 138823
   Ingress miss pkts 257178

SW3#sh authen sessions int g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.29f4.602b
           IP Address:  192.168.40.16
            User-Name:  IPXEMP1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Must Secure
```

```
        Security Status:  Secured
         Oper host mode:  multi-auth
       Oper control dir:  both
          Authorized By:  Authentication Server
            Vlan Policy:  40
                ACS ACL:  xACSACLx-EMPLOYEE_dACL-98534sp
    Common Session ID:  0A0900820000062070CFFF47
      Acct Session ID:  0x000001C9
              Handle:  0x41000621
```

Go to **Policy->Policy Elements->Results->Authorization->Authorization Profiles**. Modify the existing profile for employee to send MACSec radius attributes from ISE. Then click on Save.





Task 2: Configuring MACSec Switch-Switch

- Enable MACSec link encryption on the trunk links between SW3 and SW4. Use a manual encryption key of “123456789” with GCM-AES-128 encryption algorithm. ISE should not be used for this task.

SW3 and SW4

```
interface range g1/0/23 - 24
  cts manual
  no propagate sgt
  sap pmk 123456789 mode-list gcm-encrypt
```

SW3

```
SW3#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/23:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.


Interface GigabitEthernet1/0/24:
    CTS is enabled, mode:    MANUAL
```

```
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Disabled
    Cache Info:

   Cache applied to link : NONE


    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.
```

SW4

```
SW4#show cts interface
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/23:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              SUCCEEDED
        Version:             2
```

```
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:          Disabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.


Interface GigabitEthernet1/0/24:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:          Disabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
```

```
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.
```

SW3

```
SW3#show macsec summary
Interface                   Transmit SC          Receive SC
GigabitEthernet1/0/23             1                    1
GigabitEthernet1/0/24             1                    1
```

SW4

```
SW4#show macsec summary
Interface                   Transmit SC          Receive SC
GigabitEthernet1/0/23             1                    1
GigabitEthernet1/0/24             1                    1
```

SW3

```
SW3#show macsec interface g1/0/23
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : 4403A7C83A170000
   Elapsed time : 00:07:39
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (6196 / 0)
```

```
 Receive Secure Channels
  SCI : E02F6D0C4C970000
   Elapsed time : 00:07:39
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 151         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 53747
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 15252
   Ingress miss pkts 53747

SW3#show macsec interface g1/0/24
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : 4403A7C83A180000
   Elapsed time : 00:07:54
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (6342 / 0)
 Receive Secure Channels
  SCI : E02F6D0C4C980000
   Elapsed time : 00:07:54
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 128         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 53583
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 11704
   Ingress miss pkts 53583
```

SW4

```
SW4#show macsec interface g1/0/23
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : E02F6D0C4C970000
   Elapsed time : 00:09:57
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (107 / 0)
 Receive Secure Channels
  SCI : 4403A7C83A170000
   Elapsed time : 00:09:57
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 6024         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 39
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 482451
   Ingress miss pkts 39


SW4#show macsec interface g1/0/24
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
```

```
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
Transmit Secure Channels
  SCI : E02F6D0C4C980000
   Elapsed time : 00:10:26
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (111 / 0)
Receive Secure Channels
  SCI : 4403A7C83A180000
   Elapsed time : 00:10:26
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 6326         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 40
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 507147
   Ingress miss pkts 40
```

Section 5: ACS Solutions

Lab-1: Basic Configuration of ACS

Lab-1: ACS Basic Setup – This lab is intended to familiarize you with the basic configuration of the ACS. The VM appliance of ACS has already been initialized. The focus is to modify basic parameters and configure basic features on ACS. The basic feature cover setting the NTP server, routing, AD integration, Identity source sequence NDG setup, user and NDG schema modification, user and identity group configuration, custom attribute modification, TACACS+ general settings, modifying access policies and SSP. The focus of section 5/ACS is primarily related to AAA device administration. It also has few network access AAA tasks like Cut-through proxy and Authentication-proxy. However, generally it is recommended to configure any network access AAA policies using ISE.

We highly recommend creating your own diagram at the beginning of each lab so you are able to draw on your own diagram, making it much easier when you step into the real lab.

General Rules

- It is recommended to use internet explorer version 9 browser or IE-9 compatible mode (Developers tool option) when you access the GUI of the ACS.
- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.

- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- Make it a common practice to verify the pre-configurations loaded on the devices.

Estimated Time to Complete: 3 Hours

Pre-setup

Load the initial configurations for the ASA, routers and switches. Note that ASA, routers and switches are pre-configured with these initial configurations.

NOTE: *Do not make additional configuration on the routers, unless explicitly stated in the task; some switching and firewall configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Error! Objects cannot be created from editing field codes.

Lab 1: Configuration Tasks

Task 1: Basic Setup of ISE

- Configure appropriate VLAN's on the switch for ACS as per topology diagram 5.1.

Solutions

SW3

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
```

- SSH into ACS CLI from R2 use the credentials of admin/IPexpert123. Configure AD as the NTP server and make sure that the clock and timezone match the AD.

Solutions

ACS

```
ntp server 10.1.1.101
```

- Add a static route for 192.168.0.0/16, 172.16.2.0/24 and 200.2.45.0/24 with R2 as the next-hop on the ACS.

Solutions

ACS

```
ip route 200.2.45.0 255.255.255.0 gateway 10.1.1.2
ip route 172.16.2.0 255.255.255.0 gateway 10.1.1.2
ip route 192.168.0.0 255.255.0.0 gateway 10.1.1.2
```

- Configure AD server as the repository using FTP protocol. The repository name should be "AD_FTP". The URL should be configured as ftp.ipexpert.com. Use "administrator/IPexpert123" for the ftp login.

Solutions

ACS

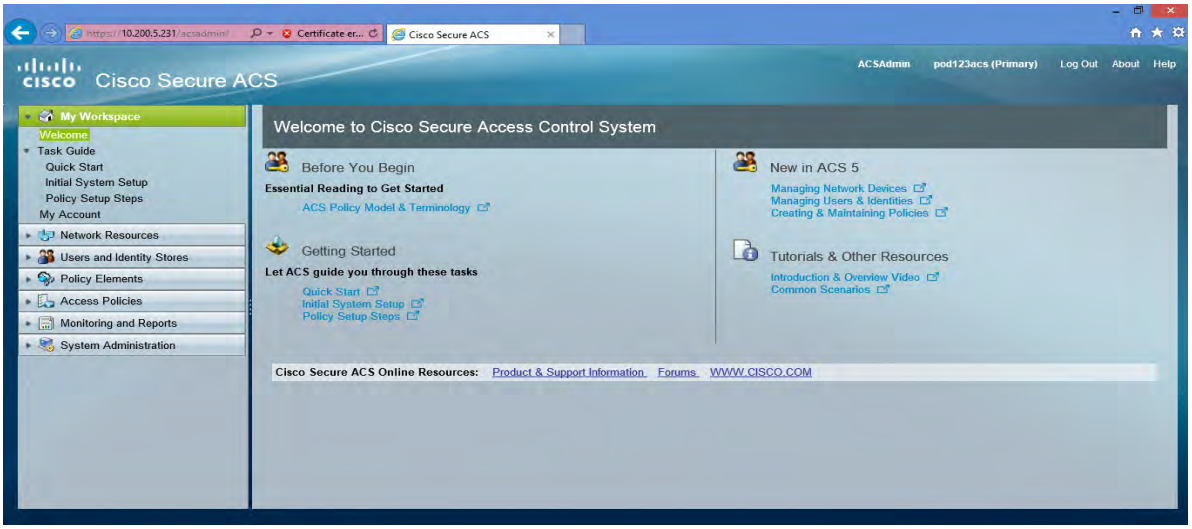
```
repository AD_FTP
  url ftp://ftp.ipexpert.com
  user administrator password plain IPexpert123
```

- Use “show application status acs” in the CLI and make sure all processes are running before you login to the GUI of the ACS.

Solutions

ACS

```
pod123acs/admin# show application status acs

ACS role: PRIMARY

Process 'database'                  running
Process 'management'                running
Process 'runtime'                   running
Process 'adclient'                  running
Process 'view-database'             running
Process 'view-jobmanager'           running
Process 'view-alertmanager'         running
Process 'view-collector'            running
Process 'view-logprocessor'         running
```

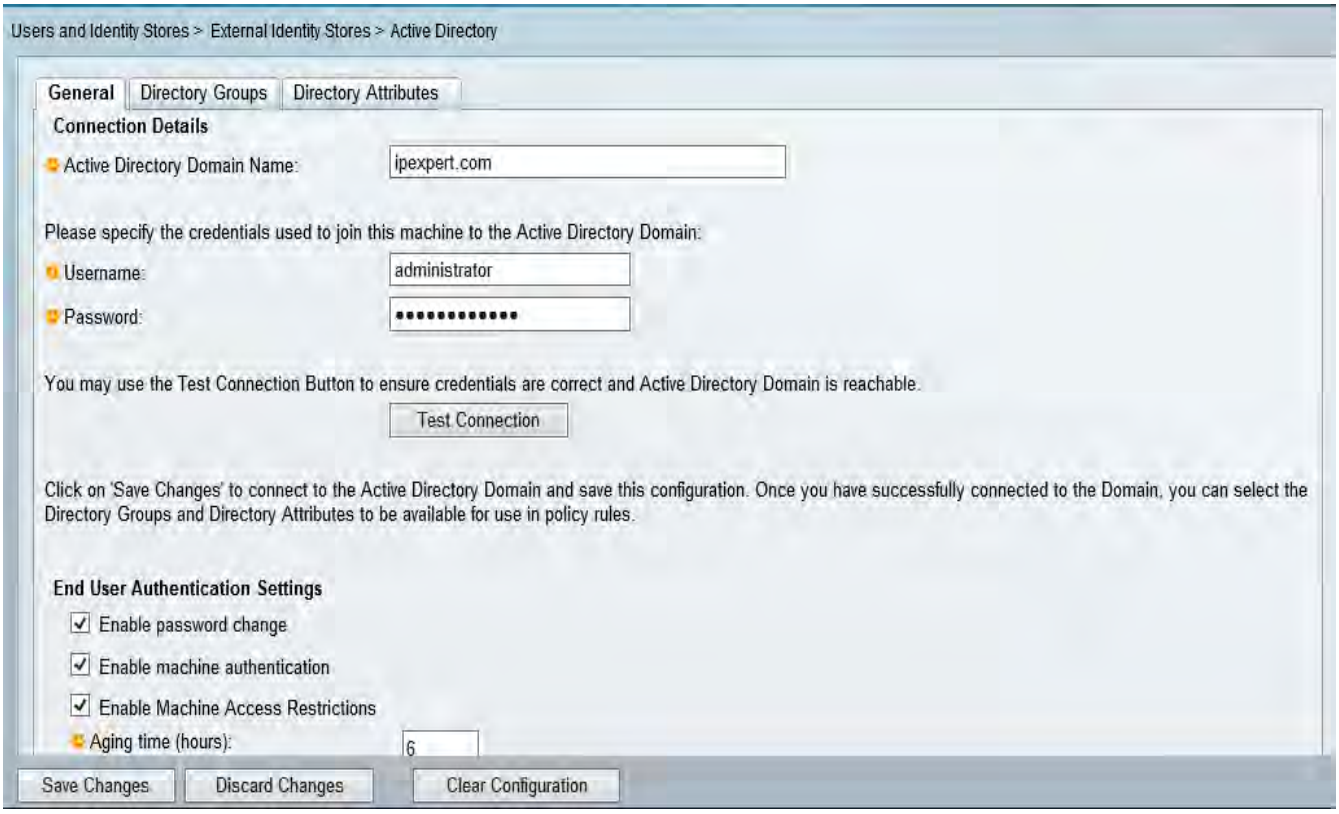


- Integrate ACS with active directory. The AD domain name should be ipexpert.com. Use “administrator/IPexpert123” to join the domain.
- Enable Password Change, Enable Machine Authentication and Enable Machine Access Restrictions for AD connection settings.

Solutions

ACS

Step 1: Go to **Users and Identity Stores-> External Identity Stores -> Active Directory**. Enter the AD domain name and the credentials. Then click on save.

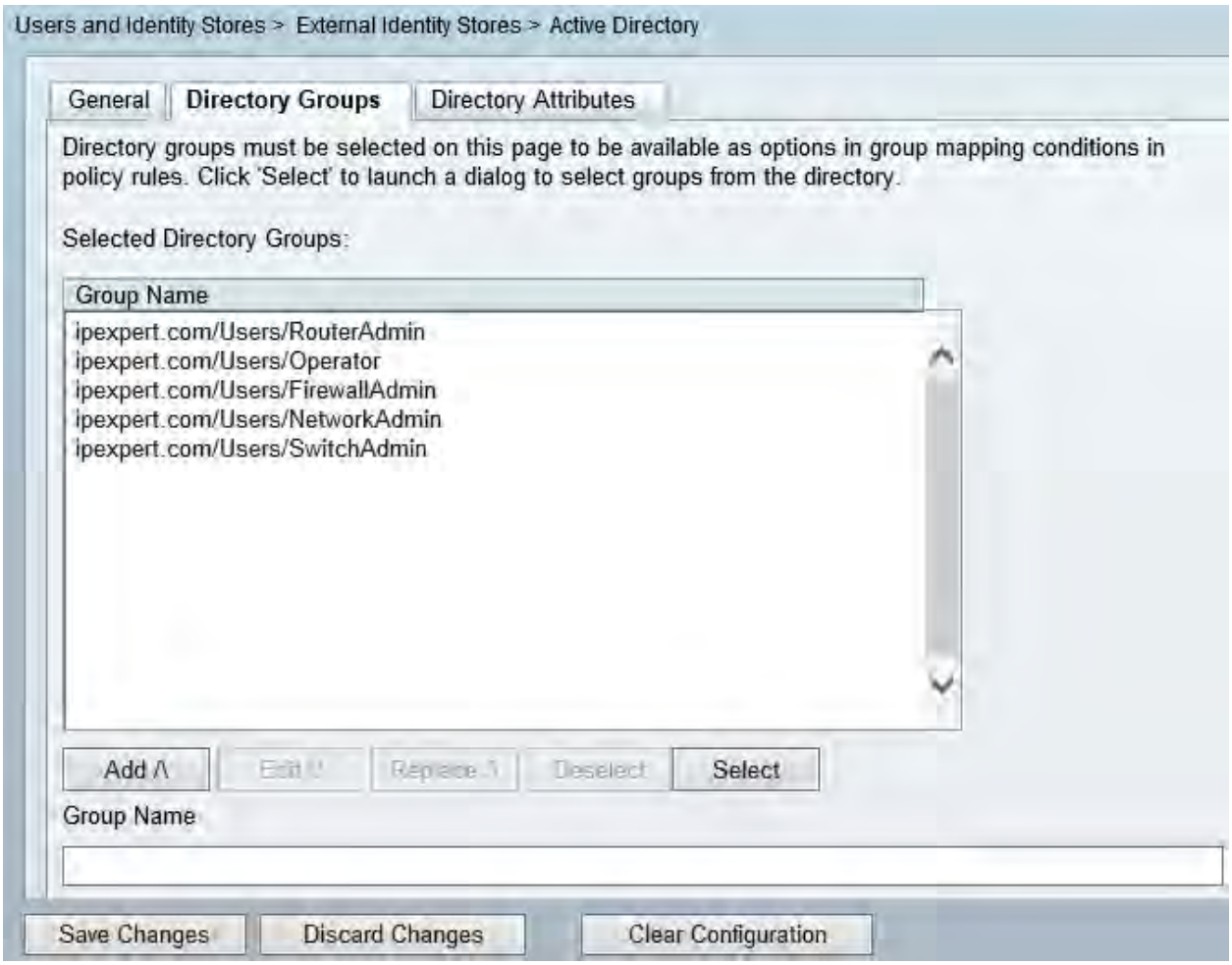


- Retrieve "NetworkAdmin" ,"RouterAdmin", "SwitchAdmin" "FirewallAdmin" and "Operator" groups from the AD.

Solutions

ACS

Step 1: Go to the **Directory Groups** tab and click on **Select** button to retrieve the AD groups.

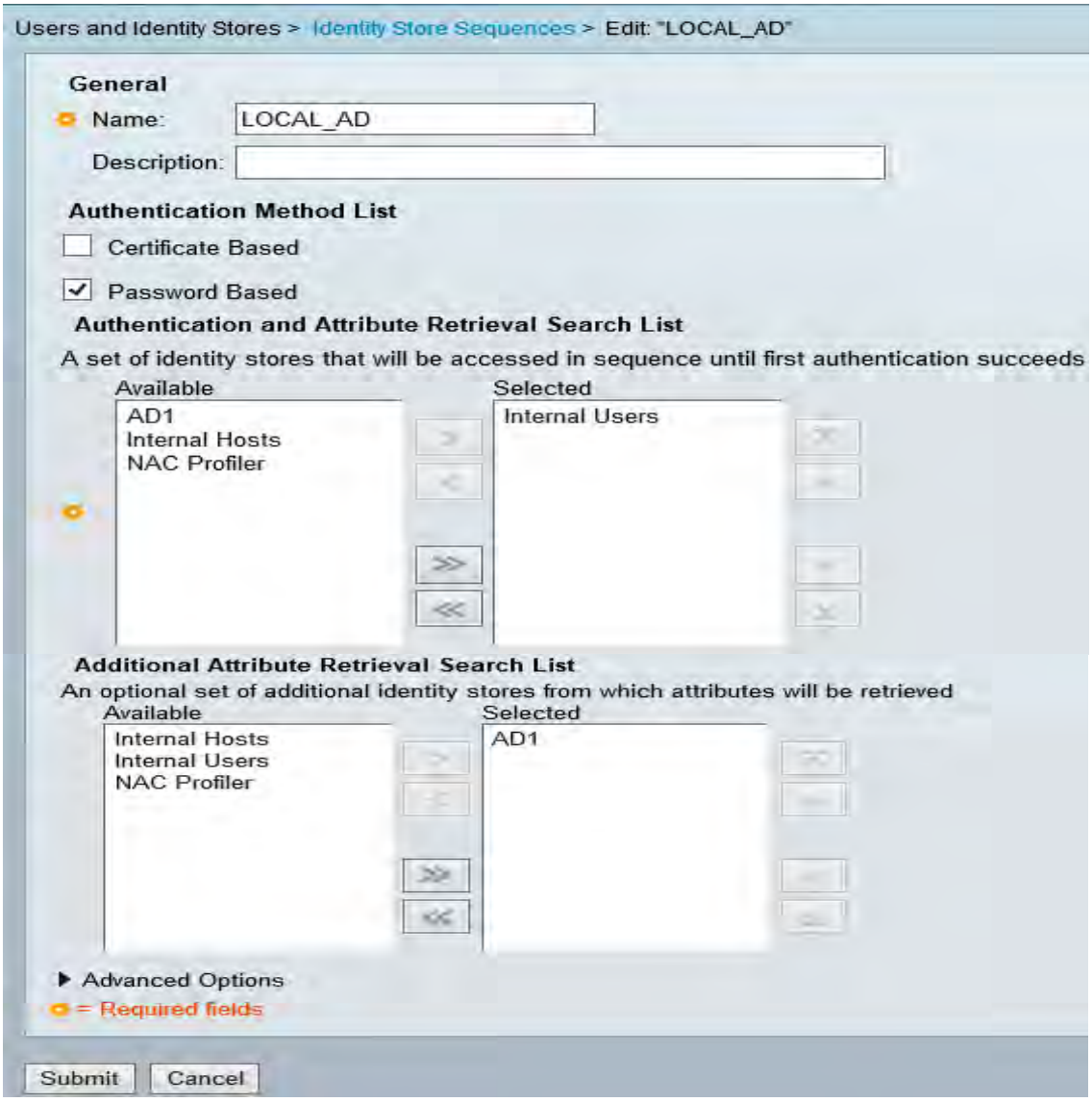


- Configure Identity Source sequence called "LOCAL_AD" such that users are authenticated with the Local User database and the ACS retrieves additional information/attributes about that user from the AD.

Solutions

ACS

Step 1: Go to **Users and Identity Stores-> Identity Store Sequences.** Click on **Create**.

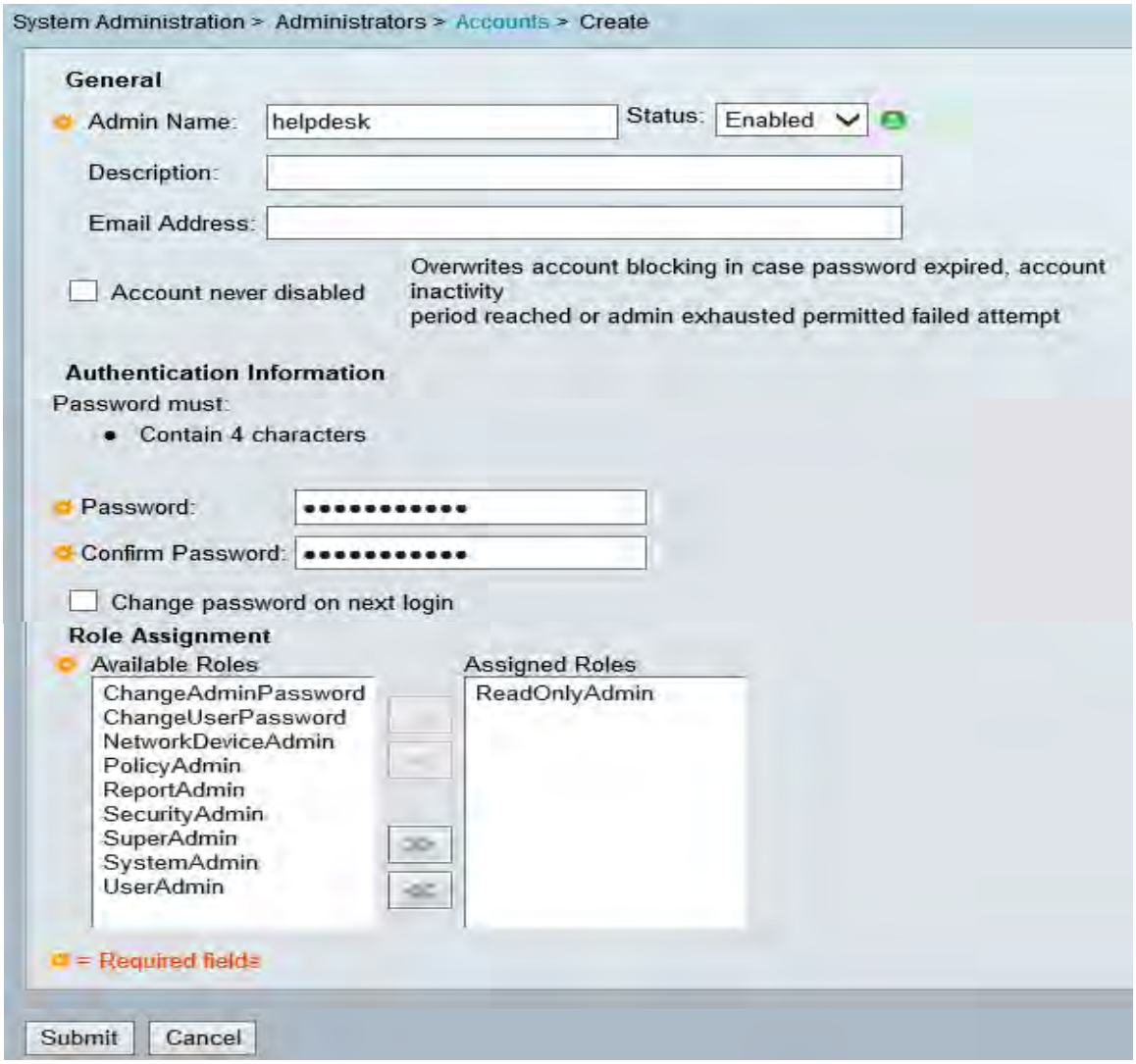


- Create a new user with the credentials of helpdesk/IPexpert123 for ACS GUI administration. Assign this user to a pre-defined group of "ReadOnlyAdmin" which has read only access to the ACS GUI.

Solutions

ACS

Step 1: Go to **System Administration -> Administrators -> Accounts**. Click on **Create.**

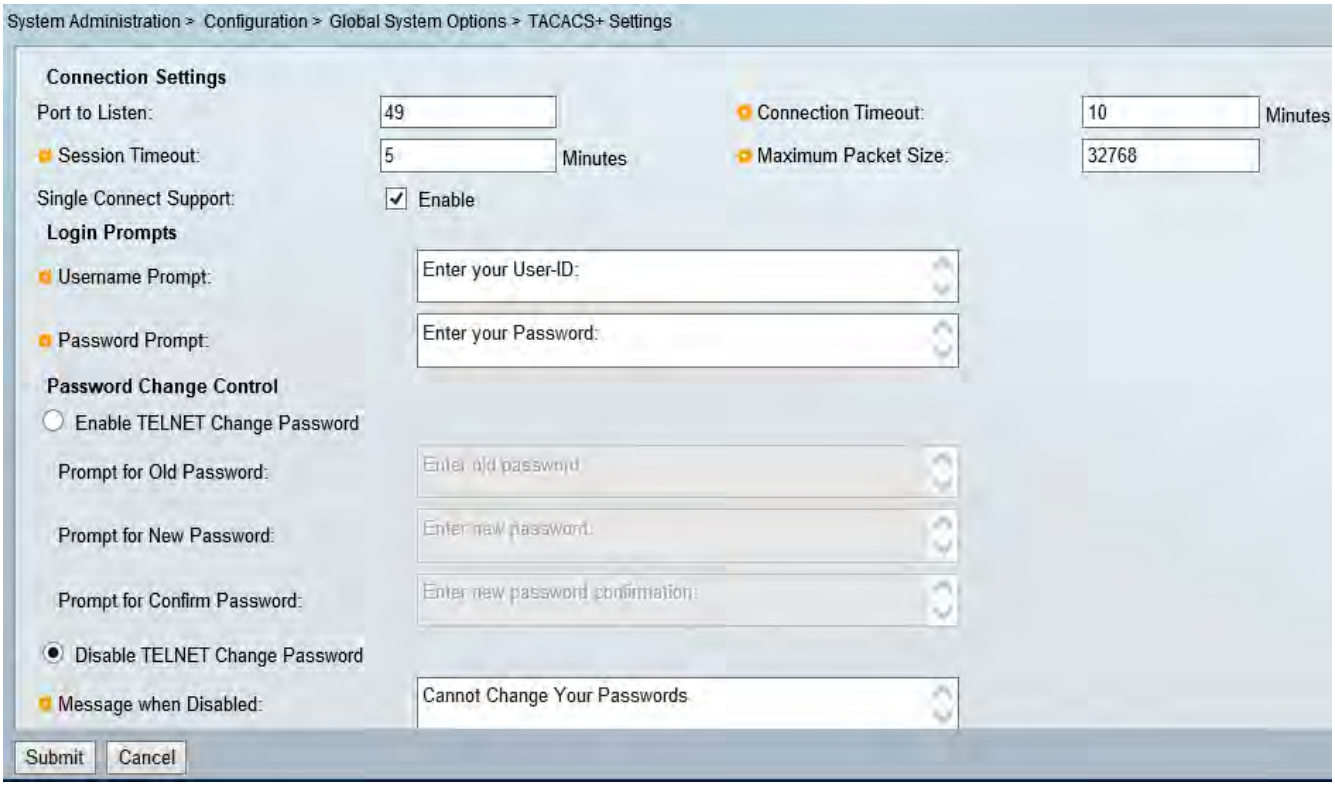


- Configure TACACS+ general settings such that the username and password prompt is changed to the below -
  "Enter your User-ID:"
  "Enter your Password:"

Solutions

ACS

Step 1: Go to **System Administration -> Configuration -> Global System Options -> TACACS+ Settings**. Then configure the username and password prompt.

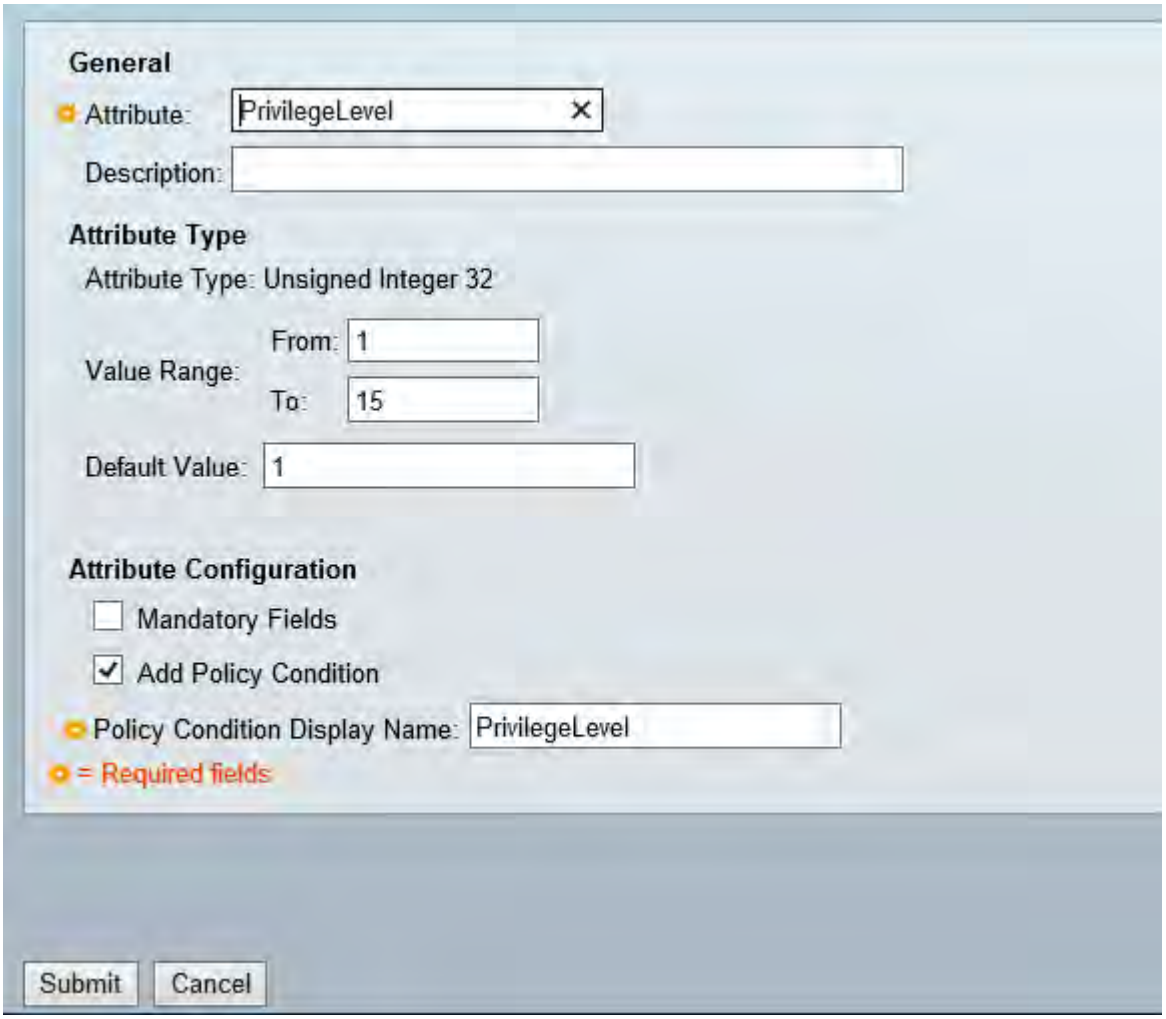


- Change the user schema to support a new field/attribute called “PriviligeLevel” whose value (Integer) should be between 1 to 15. The default value should be 1.

Solutions

ACS

Step 1: Go to **System Administration -> Configuration -> Dictionary -> Identity -> Internal Users**. Click on **Create**.

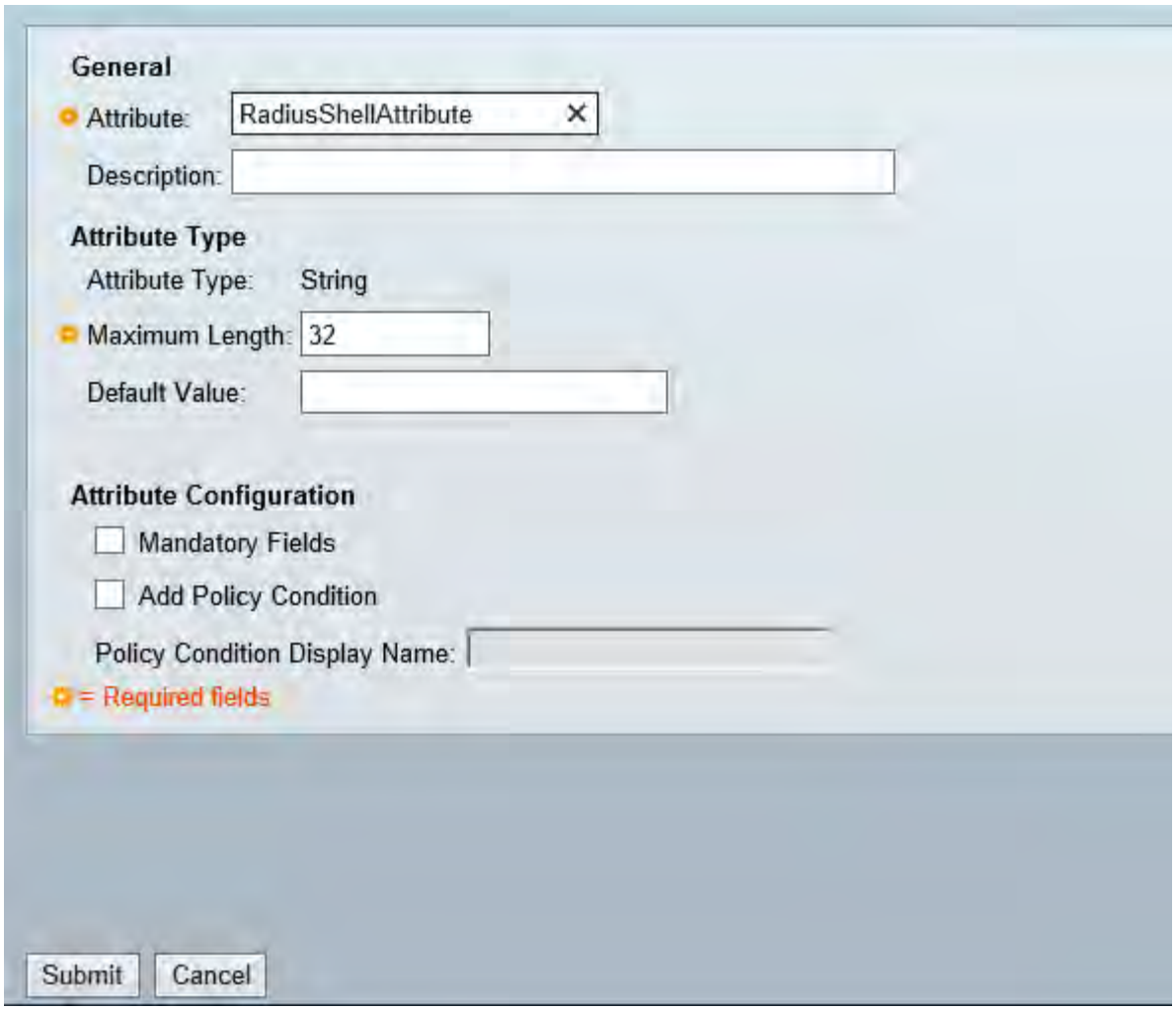


- Add another user attribute called “RadiusShellAttribute”. The value should return a string. Do not configure any default value.

Solutions

ACS

Step 1: Go to **System Administration -> Configuration -> Dictionary -> Identity -> Internal Users**. Click on **Create**.

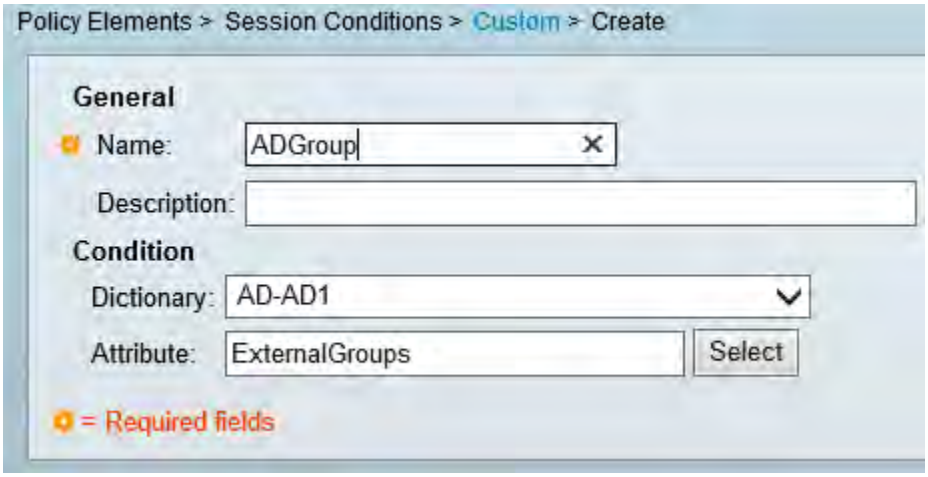


- Rename the AD1:ExternalGroups condition to a simple name of “ADGroup”

Solutions

ACS

Step 1: Go to **Policy Elements -> Session Conditions -> Custom**. Click on **Create**.



- Create a new NDG called Vendor. Under the Vendor hierarchy add two more NDG's – "CiscoDevice" and "NonCiscoDevice"

Solutions

ACS

Step 1: Go to **Network Resources -> Network Device Groups**. Click on **Create**.

Step 2: Go to **Network Resources -> Network Device Groups ->Vendors**. Click on **Create**.

- Create a new NDG under the existing Location hierarchy called “HQ” and “BranchOffice”

Solutions

ACS

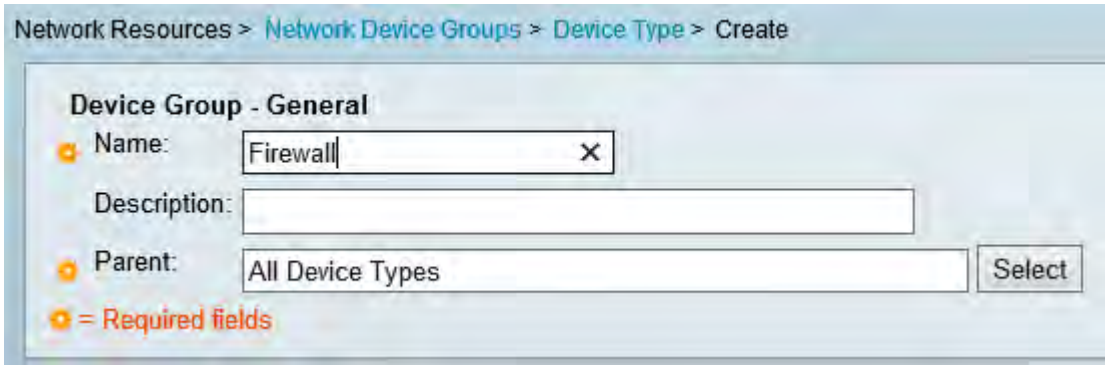
Step 1: Go to **Network Resources -> Network Device Groups ->Location**. Click on **Create**.

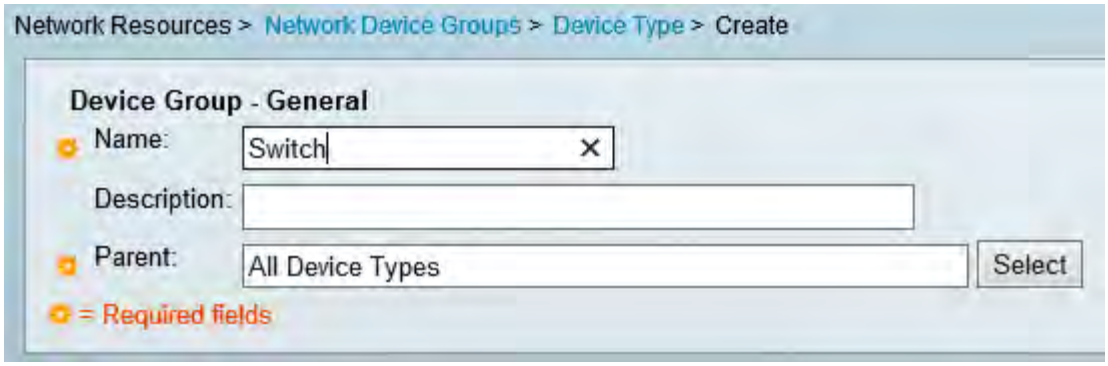
- Create a new NDG under the existing Device Type hierarchy called “Switch” “Router” and “Firewall”

Solutions

ACS

Step 1: Go to **Network Resources -> Network Device Groups ->Device Type**. Click on **Create**.





- Configure AAA clients on the ACS as per the below table. All AAA clients should use a shared key of “cisco123”

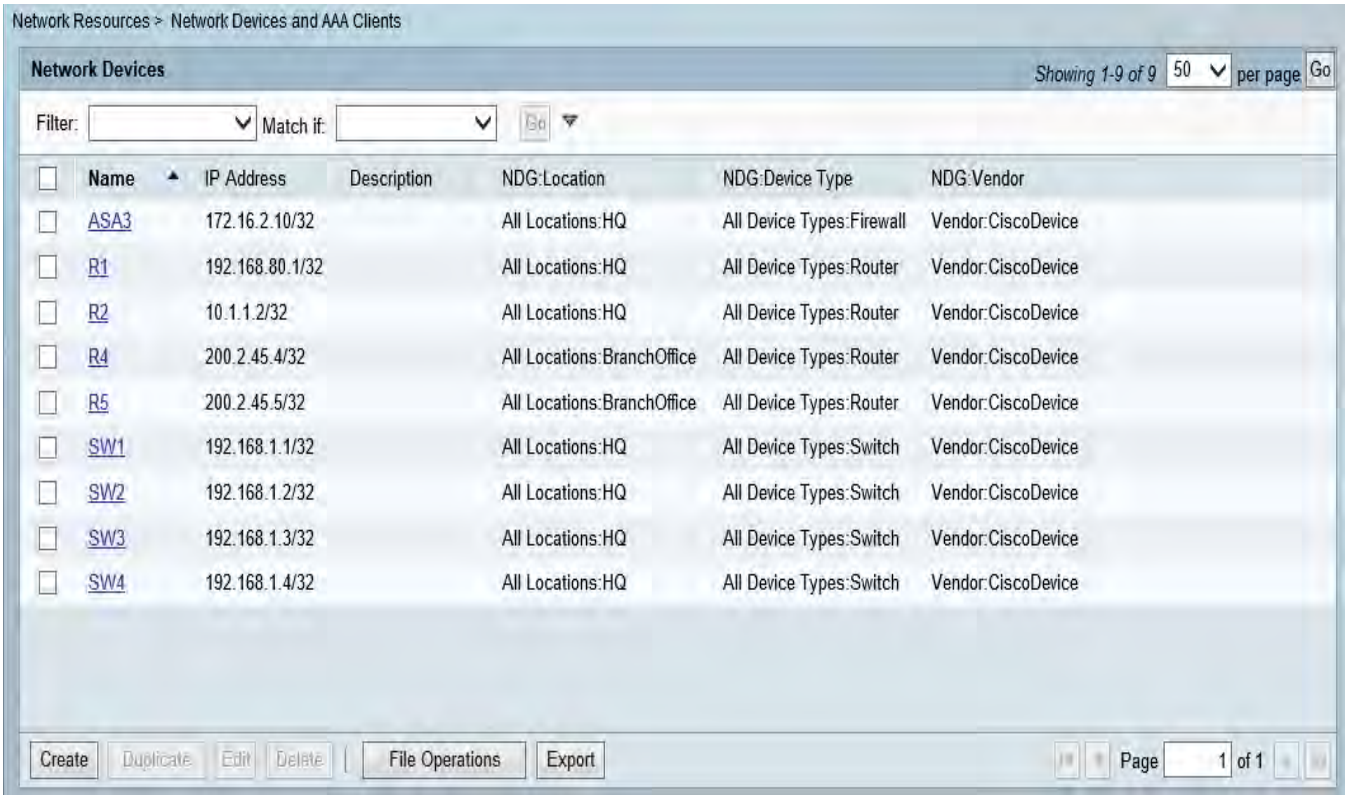
SW1-192.168.1.1-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
SW2-192.168.1.2-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
SW3-192.168.1.3-RADIUS	NDG-Device Type-Switch NDG-Location-HQ

	NDG-Vendor-CiscoDevice
SW4-192.168.1.4-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
R1-192.168.1.10-TACACS+	NDG-Device Type-Router NDG-Location-HQ NDG-Vendor-CiscoDevice
R2-10.1.1.2-TACACS+	NDG-Device Type-Router NDG-Location-HQ NDG-Vendor-CiscoDevice
R4-200.2.45.4-TACACS+	NDG-Device Type-Router NDG-Location-BranchOffice NDG-Vendor-CiscoDevice
R5-200.2.45.5-RADIUS	NDG-Device Type-Router NDG-Location- BranchOffice NDG-Vendor-CiscoDevice
ASA3-172.16.2.10-RADIUS and TACACS+	NDG-Device Type-Firewall NDG-Location- HQ NDG-Vendor-CiscoDevice

Solutions

ACS

Step 1: Go to **Network Resources -> Network Devices and AAA Clients**. Then click on **Create**.



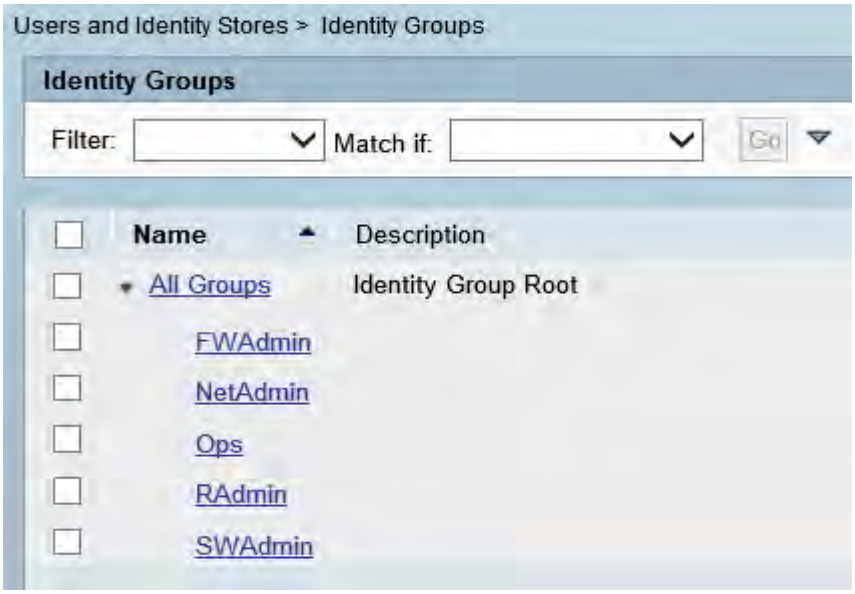
- Configure local User's and User Identity group as per the below table. All passwords should be set to "cisco". Set enable password of "cisco" only for "FWadmin" and "NetAdmin" user. These users are preconfigured on the AD and mapped to certain AD groups, which you have retrieved when you joined the ACS to the AD domain.

USER	IDENITY GROUP	PrivilegeLevel	RadiusShellAttribute
Radmin1	RAdmin	15	---
Radmin2	RAdmin	7	---
SWAdmin1	SWAdmin	15	shell:priv-lvl=15
SWAdmin2	SWAdmin	7	shell:priv-lvl=7
FWadmin	FWAdmin	--	---
NetAdmin	NetAdmin	15	shell:priv-lvl=15
NetOps	Ops	1	shell:priv-lvl=1
SecOps	Ops	15	---
AOps	Ops	15	---

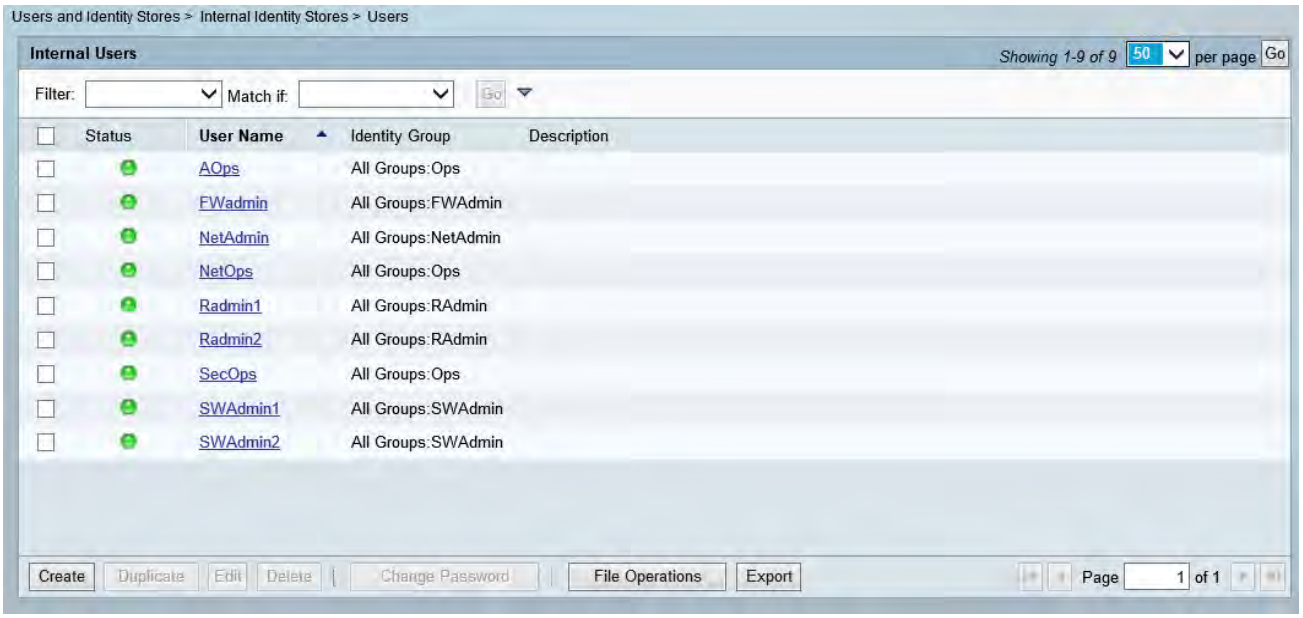
Solutions

ACS

Step 1: Go to **Users and Identity Stores-> Identity Groups**. Click on **Create**.



Step 2: Go to **Users and Identity Stores-> Internal Identity Store -> Users**. Click on **Create**. (Make sure you create enable password for NetAdmin and FWadmin user only.



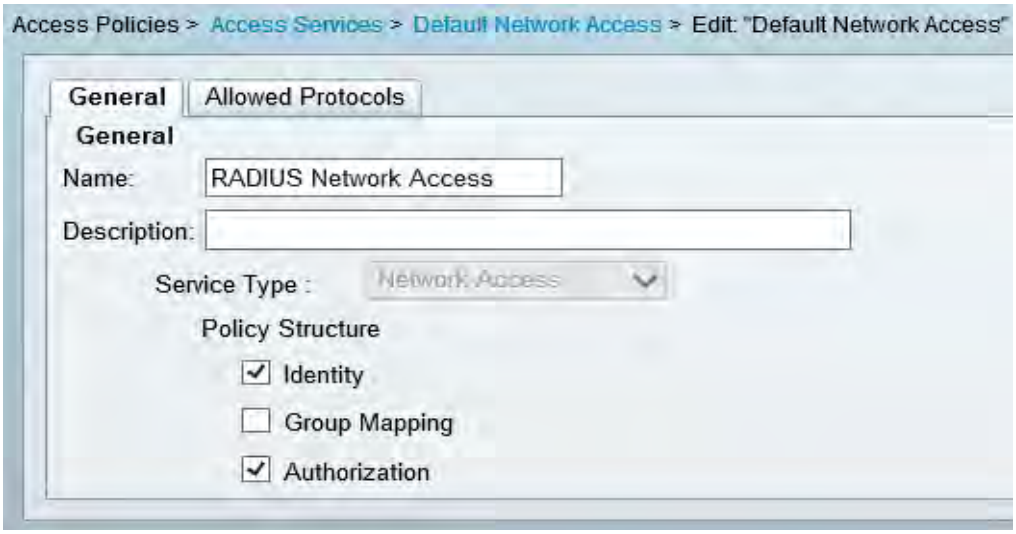
- Rename the existing access services. Change “Default Device Admin” to “TACACS+ Device Admin” and “Default Network Access” to “RADIUS Network Access”. Remove any descriptions.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> Default Device Admin**. Rename the Access Service.

Step 2: Go to **Access Policies -> Access Services -> Default Network Access**. Rename the Access Service.

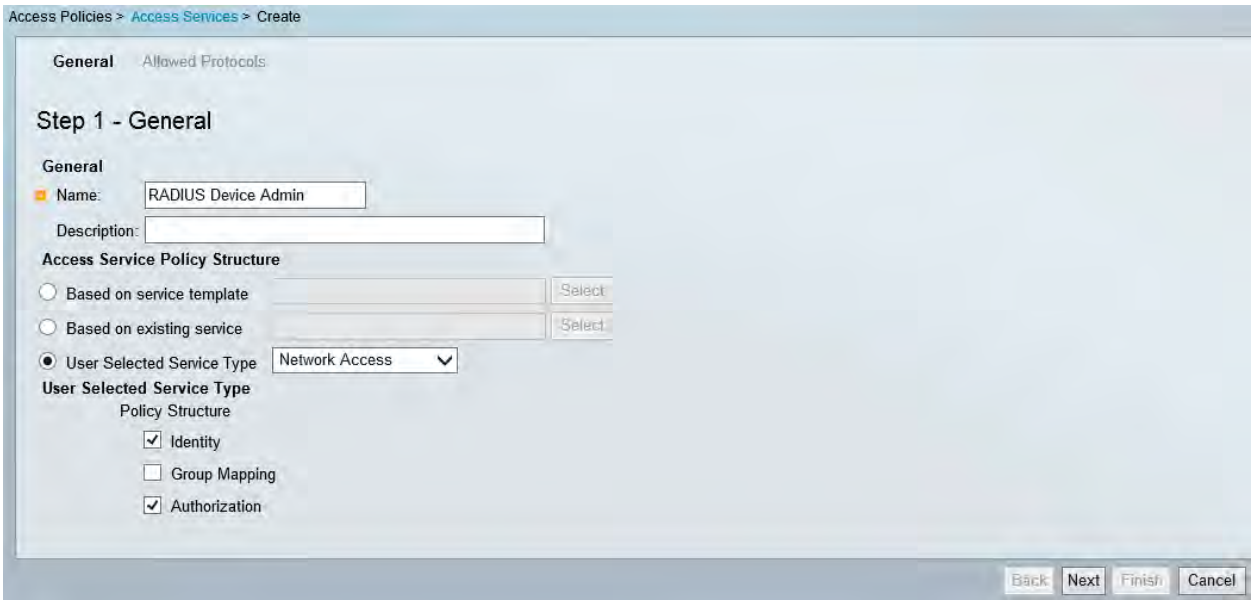


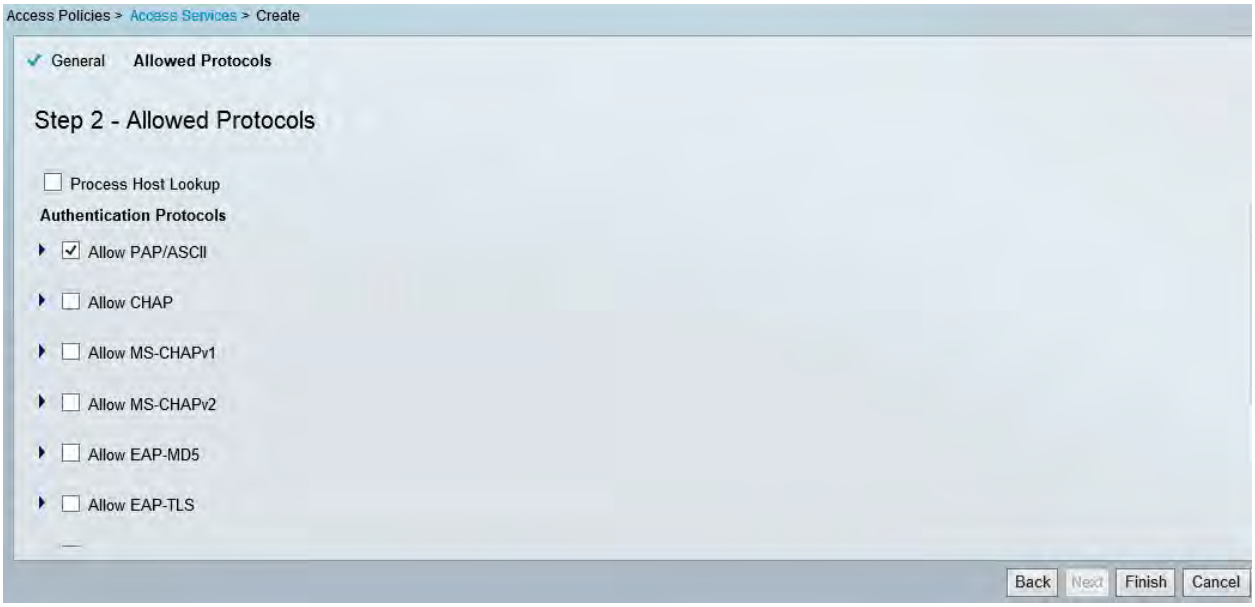
- Configure a new access service called “RADIUS Device Admin” the access type should be network access in the policy structure. Allowed protocol should be PAP/ASCII.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services**. Then click on Create.



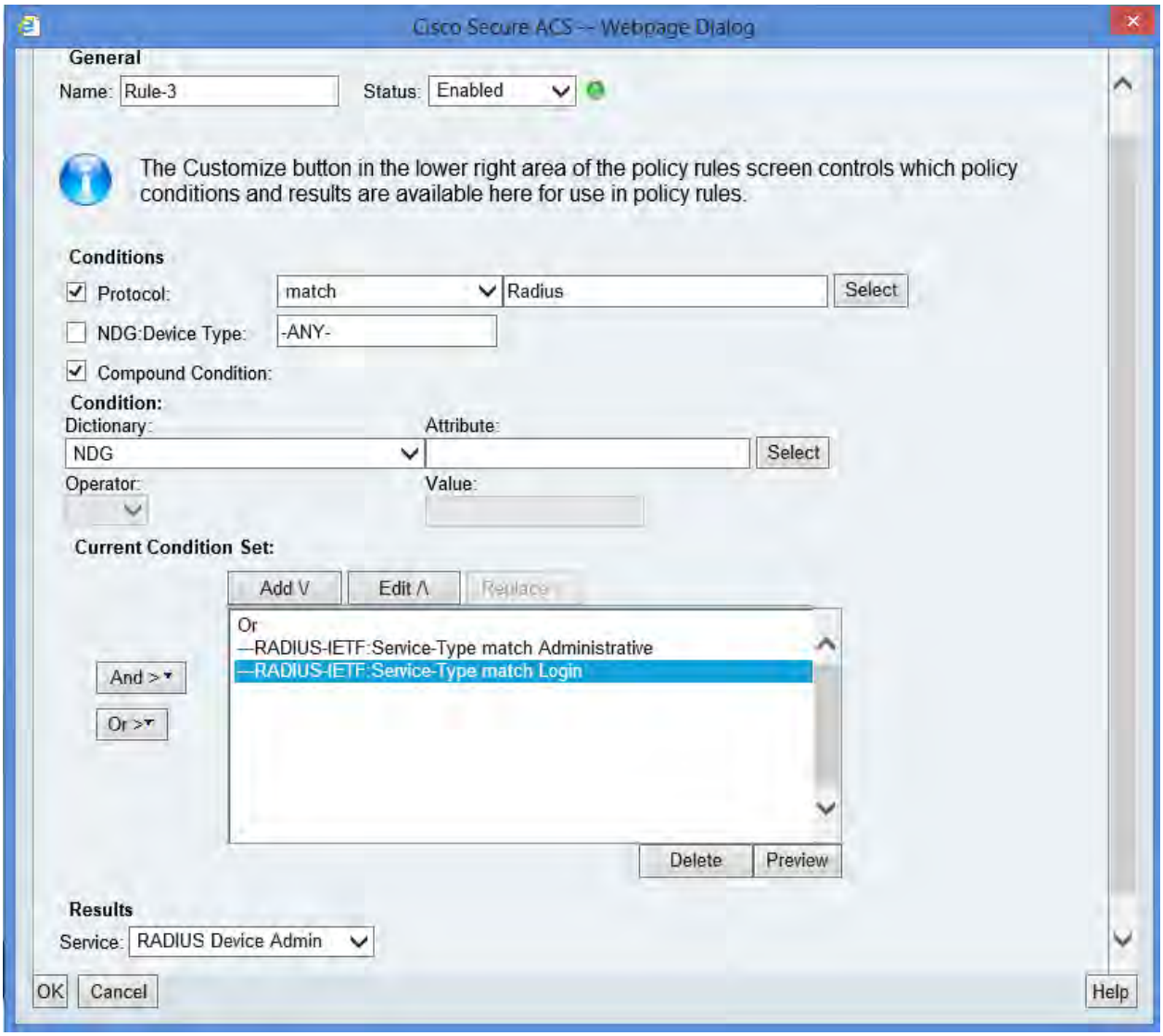


- Create a Service Selection Policy (SSP) rule to match IETF RADIUS attributes related to RADIUS device administration and map those conditions/rules to "RADIUS Device Admin" access service.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> Service Selection Rules.** Click on **Create**.

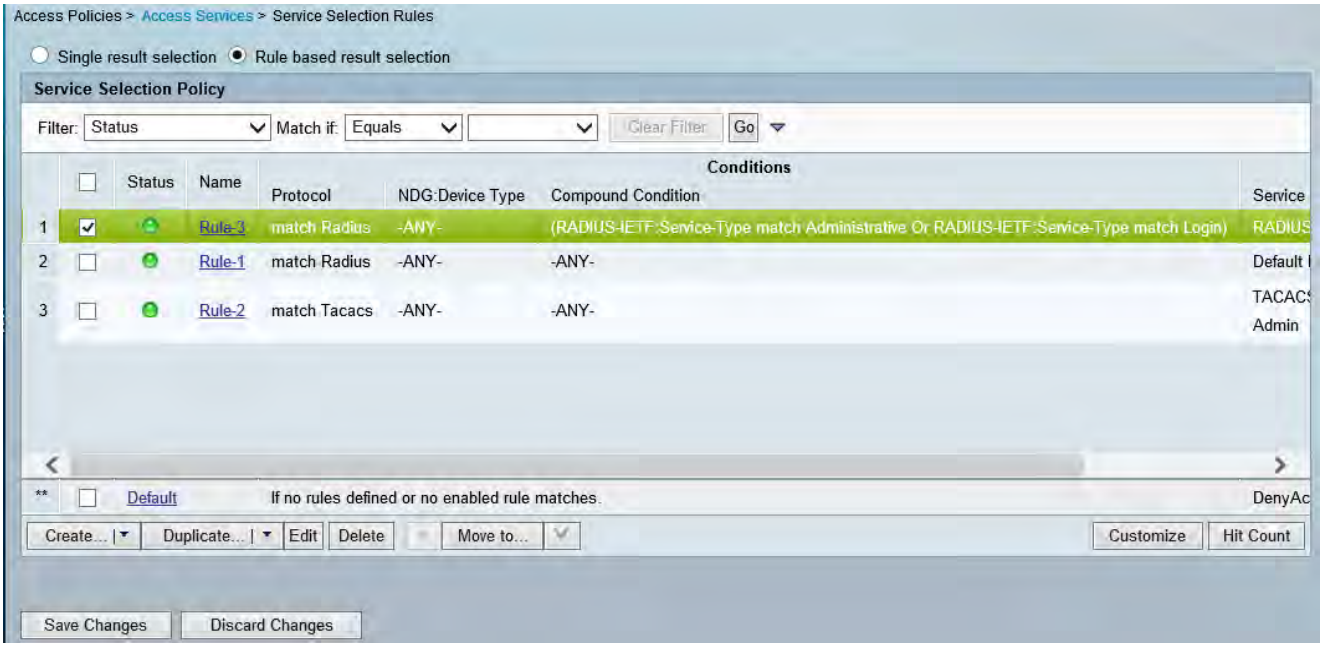


- Make sure you re-order the SSP rules accordingly.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> Service Selection Rules.** Re-order the rules such that Radius Device Admin rule is moved to the top.



Lab-2: Configuring AAA clients for authentication and EXEC authorization

Lab-2: Configuring AAA clients for authentication and EXEC authorization – This lab is intended to familiarize you with configuring AAA clients for authentication and EXEC authorization using privilege levels and role based CLI.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **4 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully.
Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure Switches (SW1 to SW4) for authentication and EXEC authorization.

- Configure a enable password of “ipexpert”

Solutions

SWITCHES

```
enable password ipexpert
```

- Configure a domain name of ipexpert.com and generate RSA keys for SSH.

Solutions

SWITCHES

```
ip domain-name ipexpert.com
crypto key generate rsa modulus 1024 (3750 SW3/SW4)
crypto key generate rsa general-keys modulus 1024 (3560 SW1/SW2)
```

- Create a local username and password of Sadmin1/cisco and NetAdmin/cisco. Assign a privilege level of 15 to these users.
- Create a local username and password of Sadmin2/cisco. Assign a privilege level of 7 to this user.
- Create a local username and password of NetOps/cisco. Assign a privilege level of 1 to this user.

Solutions

SWITCHES

```
username Sadmin1 privilege 15 password 0 cisco
username Sadmin2 privilege 7 password 0 cisco
username NetOps password 0 cisco
username NetAdmin privilege 15 password 0 cisco
```

- Change the privilege level of the below commands to level 7.
    - Show running-config
    - Configure terminal
    - vlan
    - ip routing
    - ip route

Solutions

SWITCHES

```
privilege exec level 7 configure terminal
privilege exec level 7 show running-config
privilege configure level 7 ip route
privilege configure level 7 vlan
privilege configure level 7 ip routing
```

- Add ACS as the RADIUS AAA server. It should process RADIUS VSA's and send attribute 6, 8 and 25 in the request packet.

Solutions

SWITCHES

```
aaa new-model
radius-server host 10.1.1.100 auth-port 1645 acct-port 1646 key cisco123
ip radius source-interface Vlan10
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server vsa send accounting
radius-server vsa send authentication
radius-server host 10.1.1.100 auth-port 1645 acct-port 1646 key cisco123
```

- Configure AAA authentication and exec authorization for the VTY lines and HTTP. Make sure console is not affected with this configuration. Do not use the default list.
- If the RADIUS server is not reachable then AAA should fallback to the local database.
- Limit the VTY lines to SSH only version 2.

Solutions

SWITCHES

```
aaa authentication login UseAAA group radius local
aaa authentication login NO none
aaa authorization exec UseAAA group radius local
ip http server
ip http authentication aaa login-authentication UseAAA
ip http authentication aaa exec-authorization UseAAA
ip ssh version 2

line con 0
 login authentication NO
line vty 0 4
 authorization exec UseAAA
 login authentication UseAAA
 transport input ssh
```

```
line vty 5 15
 authorization exec UseAAA
 login authentication UseAAA
 transport input ssh
```

- Configure the switches (SW3 and SW4) with a AAA login banner of “Unauthorized Access Prohibited”

Solutions

SW3 & SW4

```
aaa authentication banner “Unauthorized Access Prohibited”
```

- Configure the switches (SW3 and SW4) to display “Failed login. Try again” for any login failures

Solutions

SW3 & SW4

```
aaa authentication fail-message “Failed login. Try again”
```

- Configure switches such that the username and password prompt is changed to the below
  “Enter your User-ID:”
  “Enter your Password:”

Solutions

SWITCHES

```
aaa authentication password-prompt "Enter your Password:"
aaa authentication username-prompt "Enter your User-ID:"
```

Verification

Test the reachability to the ACS and perform basic AAA testing.

SW1

```
SW1#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

SW1#test aaa group radius SWadmin1 cisco legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

SW2

```
SW2#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

SW2#test aaa group radius SWadmin1 cisco legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

SW3

```
SW3#ping 10.1.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms

SW3#test aaa group radius SWadmin1 cisco legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

SW4

```
SW4#ping 10.1.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

SW4#test aaa group radius SWadmin1 cisco legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

SSH into SW3 from SW4 (Check the banner and login prompt)

```
SW4#ssh -l SWadmin1 192.168.1.3
Unauthorized Access Prohibited
Enter your Password:
```

```
Failed login. Try again.
Enter your Password:
```

Performing Local Authentication and Exec Authorization

```
SW4(config)#ip route 10.1.1.100 255.255.255.255 null 0

SW4#test aaa group radius SWadmin1 cisco legacy
Attempting authentication test to server-group radius using radius
No authoritative response from any server.


SW4#ssh -l Sadmin1 192.168.1.4
Unauthorized Access Prohibited
Enter your Password:

SW4#show privilege
Current privilege level is 15
SW4#exit
[Connection to 192.168.1.4 closed by foreign host]

SW4#ssh -l Sadmin2 192.168.1.4
Unauthorized Access Prohibited
Enter your Password:

Current privilege level is 7
SW4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW4(config)#?
Configure commands:
  beep     Configure BEEP (Blocks Extensible Exchange Protocol)
  cts      Cisco Trusted Security commands
  default  Set a command to its defaults
  end      Exit from configure mode
  exit     Exit from configure mode
  help     Description of the interactive help system
  ip       Global IP configuration subcommands
  license  Configure license features
  netconf  Configure NETCONF
  no       Negate a command or set its defaults
  sasl     Configure SASL
  vlan     Vlan commands
  wsma     Configure Web Services Management Agents

SW4(config)#ip ?
Global IP configuration subcommands:
  route    Establish static routes
  routing  Enable IP routing
```

```
SW4(config)#no ip route 10.1.1.100 255.255.255.255 null 0
```

Task 2: Configure Routers (R1 and R2) for authentication and EXEC authorization.

- Configure a domain name of ipexpert.com and generate RSA key's for SSH

Solutions

R1 & R2

```
ip domain-name ipexpert.com
crypto key generate rsa modulus 1024
```

- Create a local username and password of ROadmin1/cisco and NetAdmin/cisco. Assign a privilege level of 15 to these users.
- Create a local username and password of ROadmin2/cisco. Assign a privilege level of 7 to this user.
- Create a local username and password of NetOps/cisco. Assign a privilege level of 1 to this user.

Solutions

R1 & R2

```
username ROadmin1 privilege 15 password 0 cisco
username ROadmin2 privilege 7 password 0 cisco
username NetOps password 0 cisco
username NetAdmin privilege 15 password 0 cisco
```

- Change the privilege level of the below commands to level 7.
    - Show running-config
    - Configure terminal
    - Ip cef
    - mpls label protocol
    - mpls router-id
    - vrf definition and all its sub commands
    - ip route
    - router and all its sub commands
    - interface and all its sub commands

Solutions

R1 & R2

```
privilege exec level 7 configure terminal
privilege exec level 7 show running-config
privilege configure level 7 ip route
```

```
privilege configure all level 7 router
privilege configure all level 7 interface
privilege configure level 7 mpls label protocol
privilege configure level 7 mpls router-id
privilege configure level 7 ip cef
privilege configure all level 7 vrf definition
```

- Add ACS as the TACACS+ AAA server. Configure the appropriate source interface for TACACS+ packets.

Solutions

R1 & R2

```
tacacs-server host 10.1.1.100 key cisco123
ip tacacs source-interface FastEthernet0/0 (R1)
ip tacacs source-interface GigabitEthernet 0/1 (R2)
```

- Configure AAA authentication and exec authorization for the VTY lines and HTTP. Make sure console and aux is not authenticated. Do not use the default list.
- If the ACS is not reachable then AAA should fallback to the local database.

Solutions

R1 & R2

```
aaa new-model
aaa authentication login UseAAA group tacacs+ local
aaa authentication login NO none
aaa authorization exec UseAAA group tacacs+ local

ip http server
ip http authentication aaa login-authentication UseAAA
ip http authentication aaa exec-authorization UseAAA

line con 0
 login authentication NO

line aux 0
 login authentication NO

line vty 0 4
 authorization exec UseAAA
 login authentication UseAAA
```

Verification

Test the reachability to the ACS and perform basic AAA testing.

```
R2#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R2#test aaa group tacacs+ Radmin1 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.

R1#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#test aaa group tacacs+ Radmin1 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Performing Local Authentication and Exec Authorization

```
R1(config)#ip route 10.1.1.100 255.255.255.255 null 0

R1#test aaa group tacacs+ Radmin1 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
No authoritative response from any server.

R1#telnet 192.168.1.10
Trying 192.168.1.10 ... Open


User Access Verification

Username: ROadmin1
Password:

R1#show privilege
Current privilege level is 15
R1#exit

[Connection to 192.168.1.10 closed by foreign host]


R1#telnet 192.168.1.10
Trying 192.168.1.10 ... Open
```

```
User Access Verification

Username: ROadmin2
Password:

R1#show privilege
Current privilege level is 7

R1#show running-config
Building configuration...

Current configuration : 514 bytes
!
! Last configuration change at 15:10:37 IST Sun Apr 12 2013 by ROadmin2
!
boot-start-marker
boot-end-marker
!
!
ip cef
!
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 192.168.80.1 255.255.255.0
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.10 255.255.255.0
 ip ospf mtu-ignore
 ip ospf 1 area 0
 duplex auto
 speed auto
!
router ospf 1
!
!
ip route 10.1.1.100 255.255.255.255 Null0
!
end
```

```
R1#

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#?
Configure commands:
  beep       Configure BEEP (Blocks Extensible Exchange Protocol)
  call       Configure Call parameters
  default    Set a command to its defaults
  end        Exit from configure mode
  exit       Exit from configure mode
  help       Description of the interactive help system
  interface  Select an interface to configure
  ip         Global IP configuration subcommands
  license    Configure license features
  mpls       Configure MPLS parameters
  netconf    Configure NETCONF
  no         Negate a command or set its defaults
  oer        Optimized Exit Routing configuration submodes
  pfr        Performance Routing configuration submodes
  router     Enable a routing process
  sasl       Configure SASL
  vrf        VRF commands
  wsma       Configure Web Services Management Agents

R1(config)#no ip route 10.1.1.100 255.255.255.255 Null0
```

Task 3: Configure R4 for Role Based CLI

- Configure a enable secret of “ipexpert”

Solutions

R4

```
enable secret ipexpert
```

- Create a local username and password of NetAdmin/cisco.
- Create a local username and password of NetOps/cisco, SecOps/cisco and AOps/cisco

Solutions

R4

```
username SecOps password cisco
username AOps password cisco
username NetOps password cisco
username NetAdmin password cisco
```

- NetAdmin should be assigned to root view and should be given access to all commands
- NetOps should be assigned to NetOps view. The NetOps view should have a password of “netops”. This view should be able to view all show commands, ping, telnet, SSH and static routes and configure any dynamic routing protocols
- SecOps should be assigned to SecOps view. The SecOps view should have a password of “secops”. This view should be able to view all show crypto commands, ping, telnet, SSH and configure any crypto commands in the global config mode. Make sure NetOps view does not have access to any show crypto commands.
- Configure a superview called AOps which includes SecOps and NetOps view. The view password should be “aops”.

Solutions

R4

```
aaa new-model

enable view
(Enter the enable secret password)

parser view NetOps
 secret netops
 commands configure include ip route
 commands configure include all router
 commands exec include ssh
 commands exec include telnet
 commands exec include ping
 commands exec include configure terminal
 commands exec include all show

parser view SecOps
 secret secops
 commands configure include all interface
 commands configure include all crypto
 commands configure include ip
 commands exec include ssh
 commands exec include telnet
 commands exec include ping
 commands exec include configure terminal
 commands exec include-exclusive all show crypto

parser view Aops superview
 secret aops
 view NetOps
 view SecOps
```

```
username NetOps view NetOps
username NetAdmin view root
username SecOps view SecOps
username AOps view AOps
```

- Configure a Static Object NAT for the ACS on ASA3. Translate ACS to 200.2.45.100.

Solutions

ASA3

```
object network ACS
 host 10.1.1.100
  nat (inside,outside) static 200.2.45.100
```

- Configure appropriate ACL's on ASA3 for communication between R5 and ACS.

Solutions

ASA3

```
access-list OUT extended permit tcp host 200.2.45.4 any eq tacacs
access-group OUT in interface outside
```

- Add ACS as the TACACS+ AAA server. Configure F0/0 as the source interface for TACACS+ packets.

Solutions

R4

```
tacacs-server host 200.2.45.100 key cisco123
ip tacacs source-interface FastEthernet0/0
```

- Configure AAA authentication and exec authorization for the VTY lines. Make sure console and AUX lines are not authenticated. Do not use the default list.
- If the ACS is not reachable then AAA should fallback to the local database.

Solutions

R4

```
aaa authentication login UseAAA group tacacs+ local
aaa authentication login NO none
aaa authorization exec UseAAA group tacacs+ local

line con 0
```

```
 login authentication NO
line aux 0
 login authentication NO
line vty 0 4
 authorization exec UseAAA
 login authentication UseAAA
```

Verification

Test the reachability to the ACS and perform basic AAA testing. (ICMP is not allowed through the ASA)

```
R4>en
Password:
R4#test aaa group tacacs+ NetAdmin cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Performing Local Authentication and Exec Authorization

```
R4(config)#ip route 200.2.45.100 255.255.255.255 null 0
R4(config)#line con 0
R4(config)#no login authentication NO

R4#test aaa group tacacs+ NetAdmin cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
No authoritative response from any server.

R4#enable view SecOps
Password:

R4#
*Apr  12  10:10:40.199:  %PARSER-6-VIEW_SWITCH:  successfully  set  to  view
'SecOps'.

R4#?
Exec commands:
  configure   Enter configuration mode
  credential  load the credential info from file system
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  ping        Send echo messages
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection

R4#show ?
  crypto  Encryption module
```

```
  flash:  display information about flash: file system
  parser  Show parser commands

R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#?
Configure commands:
  crypto     Encryption module
  do         To run exec commands in config mode
  exit       Exit from configure mode
  interface  Select an interface to configure
  ip         Global IP configuration subcommands
```

Exit out of SecOps view and telnet to R4 itself.

```
R4#telnet 200.2.45.4
Trying 200.2.45.4 ... Open


User Access Verification

Username: SecOps
Password:

R4>show parser view
Current view is 'SecOps'
R4>conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)>?
Configure commands:
  crypto     Encryption module
  do         To run exec commands in config mode
  exit       Exit from configure mode
  interface  Select an interface to configure
  ip         Global IP configuration subcommands

R4(config)>

line con 0
 no login authentication NO
R4>exit

[Connection to 200.2.45.4 closed by foreign host]
R4#
*Apr 12 10:26:45.699: %SYS-5-CONFIG_I: Configured from console by SecOps on
vty0 (200.2.45.4)
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#no ip route 200.2.45.100 255.255.255.255 null 0
```

```
R4(config)#line con 0
R4(config-line)#login authentication NO
```

Task 4: Configure R5 for Role Based CLI

- Do not configure enable password or secret. The root view should use a password of "cisco". You are allowed to modify the ACS server for switching to the root view.

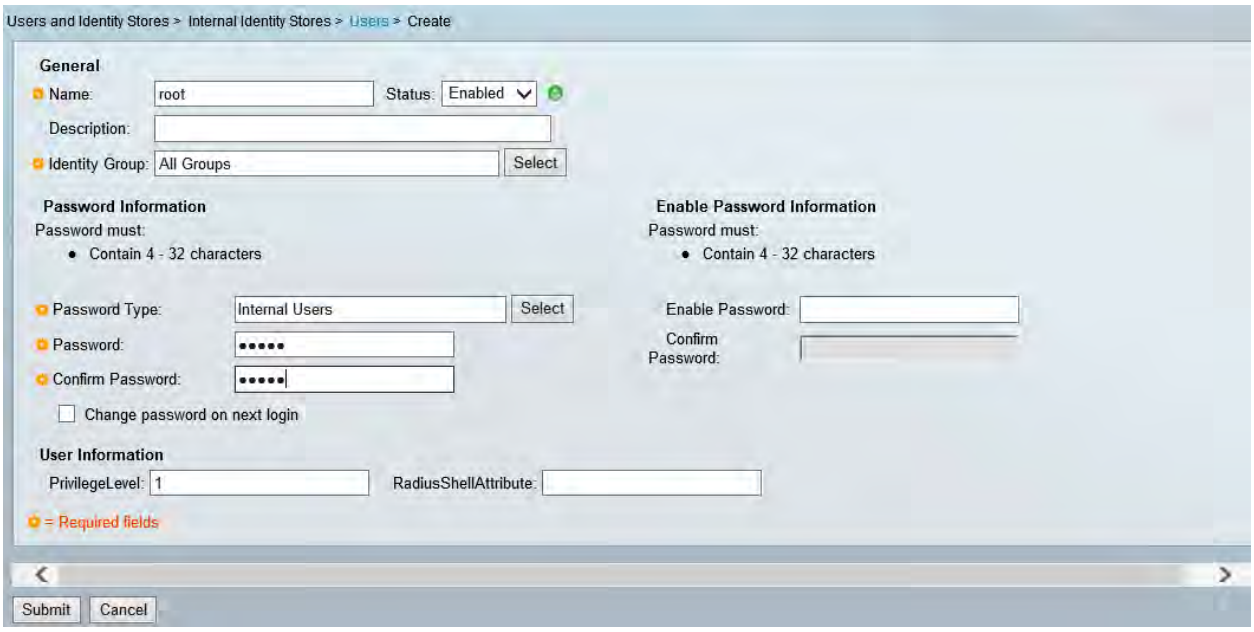
Solutions

R5

Step 1: Configure R5 as the AAA radius client. Configure the console line to use ACS for authentication to switch to root view.

```
aaa new-model
radius-server host 200.2.45.100 auth-port 1645 acct-port 1646
radius-server key cisco123
ip radius source-interface FastEthernet0/0
radius-server attribute 6 on-for-login-auth
radius-server vsa send authentication
aaa authentication login UseAAA group radius local
line con 0
 login authentication UseAAA
```

Step 2: Configure the ACS with a username of "root" and password of cisco



- Configure appropriate ACL's on ASA3 for communication between R5 and ACS.

Solutions

ASA3

```
access-list OUT extended permit udp host 200.2.45.5 any eq 1645
access-list OUT extended permit udp host 200.2.45.5 any eq 1646
```

- Create a local username and password of NetAdmin/cisco.
- Create a local username and password of NetOps/cisco, SecOps/cisco and AOps/cisco

Solutions

R5

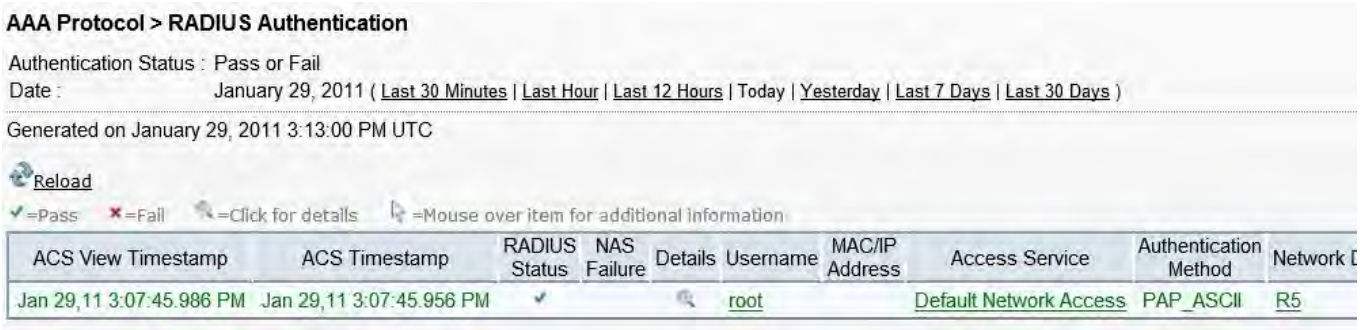
```
username SecOps password cisco
username AOps password cisco
username NetOps password cisco
username NetAdmin password cisco
```

- NetAdmin should be assigned to root view and should be given access to all commands
- NetOps should be assigned to NetOps view. The NetOps view should have a password of "netops". This view should be able to view all show commands, ping, telnet, SSH and static routes configure routing protocols
- SecOps should be assigned to SecOps view. The SecOps view should have a password of "secops". This view should be able to view all show crypto commands, ping, telnet, SSH and configure any crypto commands in the global config mode. Make sure NetOps view does not have access to any show crypto commands.
- Configure a superview called AOps, which includes SecOps and NetOps view. The view password should be "aops".

```
enable view
(Enter the enable secret password) /Make sure ACS is reachable.


parser view NetOps
 secret netops
 commands configure include ip route
 commands configure include all router
 commands exec include ssh
 commands exec include telnet
 commands exec include ping
 commands exec include configure terminal
 commands exec include all show


parser view SecOps
 secret secops
 commands configure include all interface
```

```
 commands configure include all crypto
 commands configure include ip
 commands exec include ssh
 commands exec include telnet
 commands exec include ping
 commands exec include configure terminal
 commands exec include-exclusive all show crypto

parser view Aops superview
 secret aops
 view NetOps
 view SecOps

username NetOps view NetOps
username NetAdmin view root
username SecOps view SecOps
username AOps view AOps
```

Verification on the ACS. Go to Monitoring and Reports and click on Launch Report viewer. Then browse to Catalog->AAA Protocol ->RADIUS Authentication



- Configure AAA authentication and exec authorization for the VTY lines. Make sure console and AUX lines are not authenticated after switching to the root view. Do not use the default list.
- If the ACS is not reachable then AAA should fallback to the local database.

Solutions

R5

```
aaa authentication login UseAAA group radius local (Already configured)
aaa authentication login NO none
aaa authorization exec UseAAA group radius local

line con 0
 login authentication NO
line aux 0
 login authentication NO
```

```
line vty 0 4
 authorization exec UseAAA
 login authentication UseAAA
```

- Configure R5 such that the username and password prompt is changed to the below
  "Enter your User-ID:"
  "Enter your Password:"

Solutions

R5

```
aaa authentication password-prompt "Enter your Password:"
aaa authentication username-prompt "Enter your User-ID:"
```

- Configure the R5 to display "Failed login. Try again" for any login failures

Solutions

R5

```
aaa authentication fail-message "Failed login. Try again"
```

Verification

Performing Local Authentication and Exec Authorization

```
R5(config)#ip route 200.2.45.100 255.255.255.255 null 0


R5#telnet 200.2.45.5
Trying 200.2.45.5 ... Open


User Access Verification

Enter your User-ID:NetAdmin
Enter your Password:
R5>show parser view
Current view is 'root'
R5(config)>^Z
R5>
*Apr 12 11:44:44.943: %SYS-5-CONFIG_I: Configured from console by NetAdmin on
vty0 (200.2.45.5)
R5>exit

[Connection to 200.2.45.5 closed by foreign host]
```

```
R5(config)#no ip route 200.2.45.100 255.255.255.255 null 0
```

Task 5: Configure ASA for authentication

- Configure an enable password of “ipexpert” on ASA3. Configure a domain name of ipexpert.com

Solutions

ASA3

```
enable password ipexpert
domain-name ipexpert.com
crypto key generate rsa modulus 1024
```

- Configure a local username and password of “FWadmin/cisco”. Set the service type to admin.

Solutions

ASA3

```
username FWadmin password cisco
username FWadmin attributes
 service-type admin
```

- Configure ASA3 to authenticate all logins to console, telnet, SSH and ASDM sessions using the ACS. If the ACS is unavailable then the ASA should use its local database.

Solutions

ASA3

```
aaa-server TACACS protocol tacacs+
aaa-server TACACS (inside) host 10.1.1.100
 key cisco123


aaa authentication ssh console TACACS LOCAL
aaa authentication telnet console TACACS LOCAL
aaa authentication serial console TACACS LOCAL
aaa authentication http console TACACS LOCAL

http server enable
asdm image disk0:/asdm-66114.bin
```

- Configure enable authentication using the ACS and should fall back to the local database if ACS is not reachable/down.

Solutions

ASA3

```
aaa authentication enable console TACACS LOCAL
```

- EXEC authorization should be done using the ACS.

Solutions

ASA3

```
 aaa authorization exec authentication-server
```

- Only allow management from anyone on the inside interface.

Solutions

ASA3

```
telnet 0 0 inside
ssh 0 0 inside
http 0 0 inside
```

Verification

Test reachability to the AAA server and perform basic AAA test.

```
ASA3(config)# ping 10.1.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA3(config)# test aaa authentication TACACS username FWadmin password cisco
Server IP Address or name: 10.1.1.100
INFO: Attempting Authentication test to IP address <10.1.1.100> (timeout: 12
seconds)
INFO: Authentication Successful
```

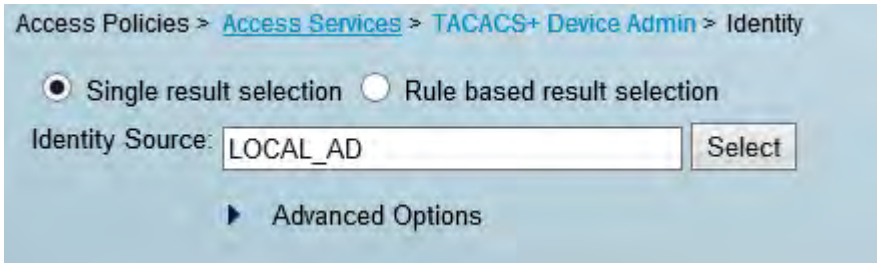
Task 6: Configure ACS for EXEC authorization TACACS+ Device Admin access service for routers

- Change the authentication method to “LOCAL_AD” identity sequence for “TACACS+ Device Admin” access service.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Identity** and click on **Select**. Then choose “LOCAL_AD” as the identity source.

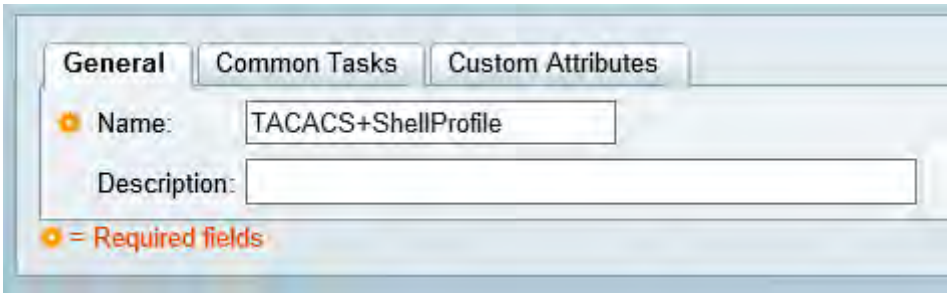


- Create a Shell Profile called “TACACS+ShellProfile”. Configure the default privilege level in this profile to use a dynamic value. The value for that attribute should be dynamically derived from the user attribute called “PrivilegeLevel”. This attribute is present the internal user store.

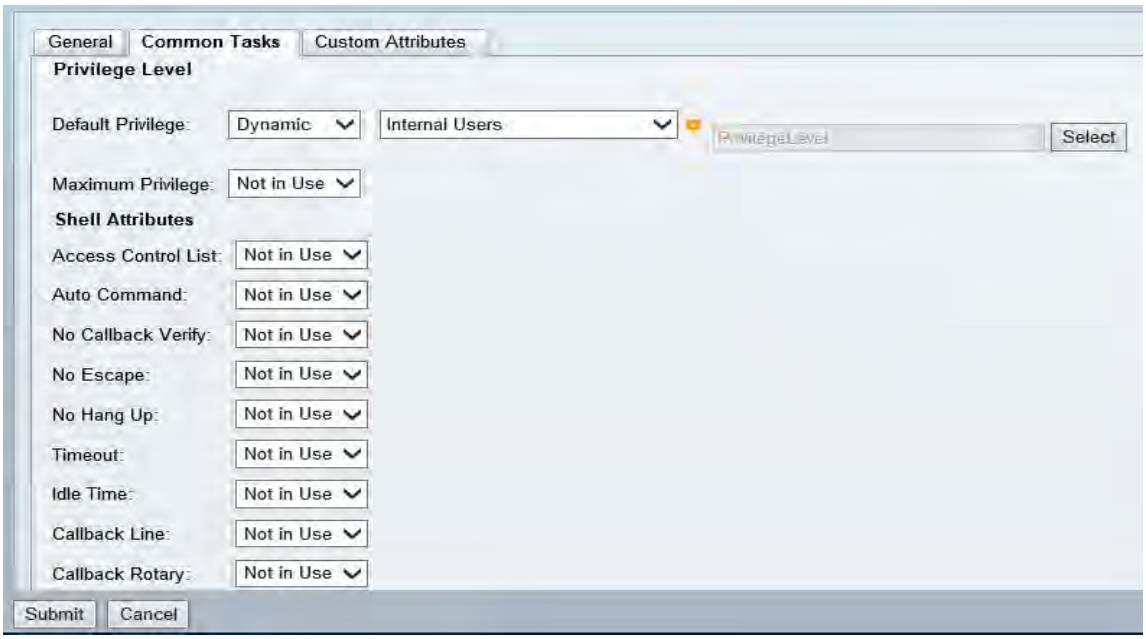
Solutions

ACS

Step 1: Go to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles** and click on **Create**. Name the shell profile as “TACACS+ShellProfile”.



Step 2: Click on **Common Tasks** tab and assign a dynamic value to the default privilege level attribute. The value for this attribute should be retrieved from the internal user database. Use PrivilegeLevel attribute from the internal users.

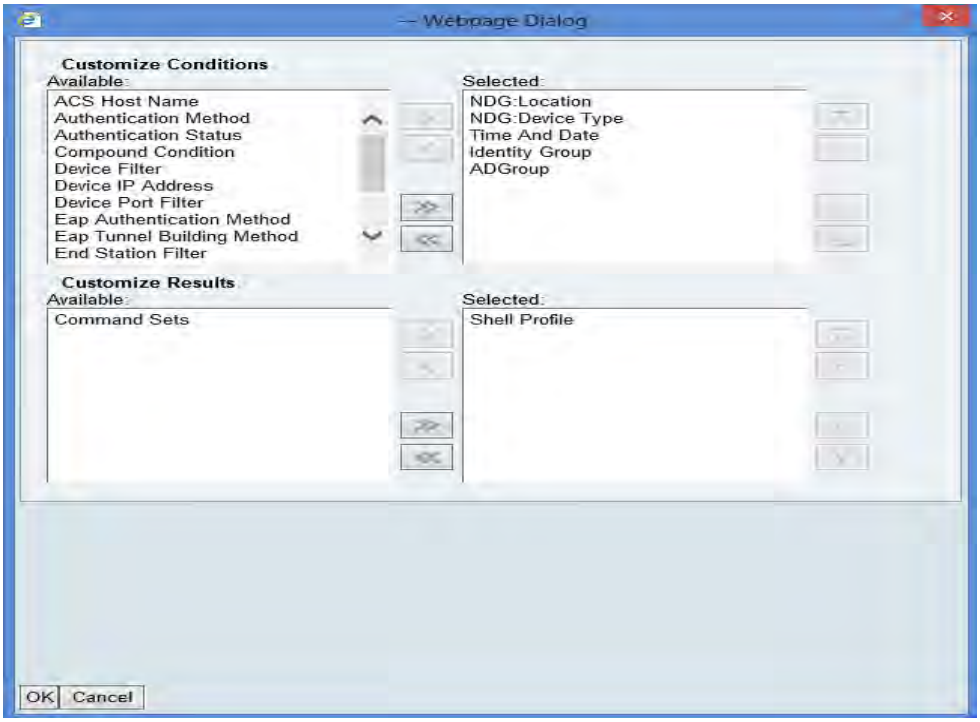


- Radmin1 user should be given complete access to any router in the HQ. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of RouterAdmin.
- Radmin2 user should be given access to routers in the HQ for all commands at privilege-level 7 and below. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of RouterAdmin.
- Configure only one authorization rule to reflect the above policy requirement.
- Policy conditions should include date and time, NDG location, NDG Device type, Identity Group and ADGroup.

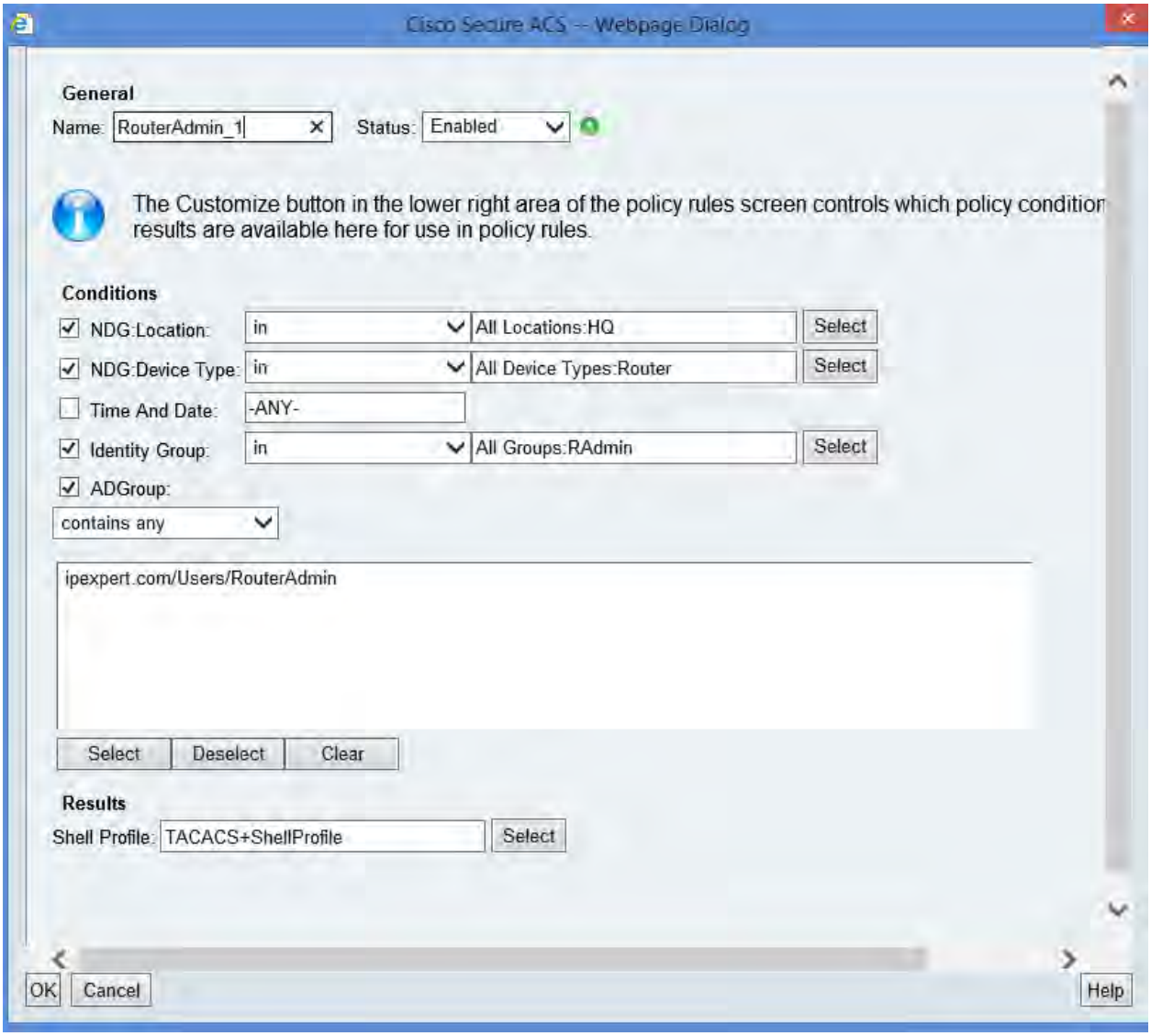
Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Customize** button and make sure you include date and time, NDG location, NDG Device type, Identity Group and ADGroup as conditions.



Step 2: Click on **Create** to configure authorization rules. Then click on **Save Changes**.

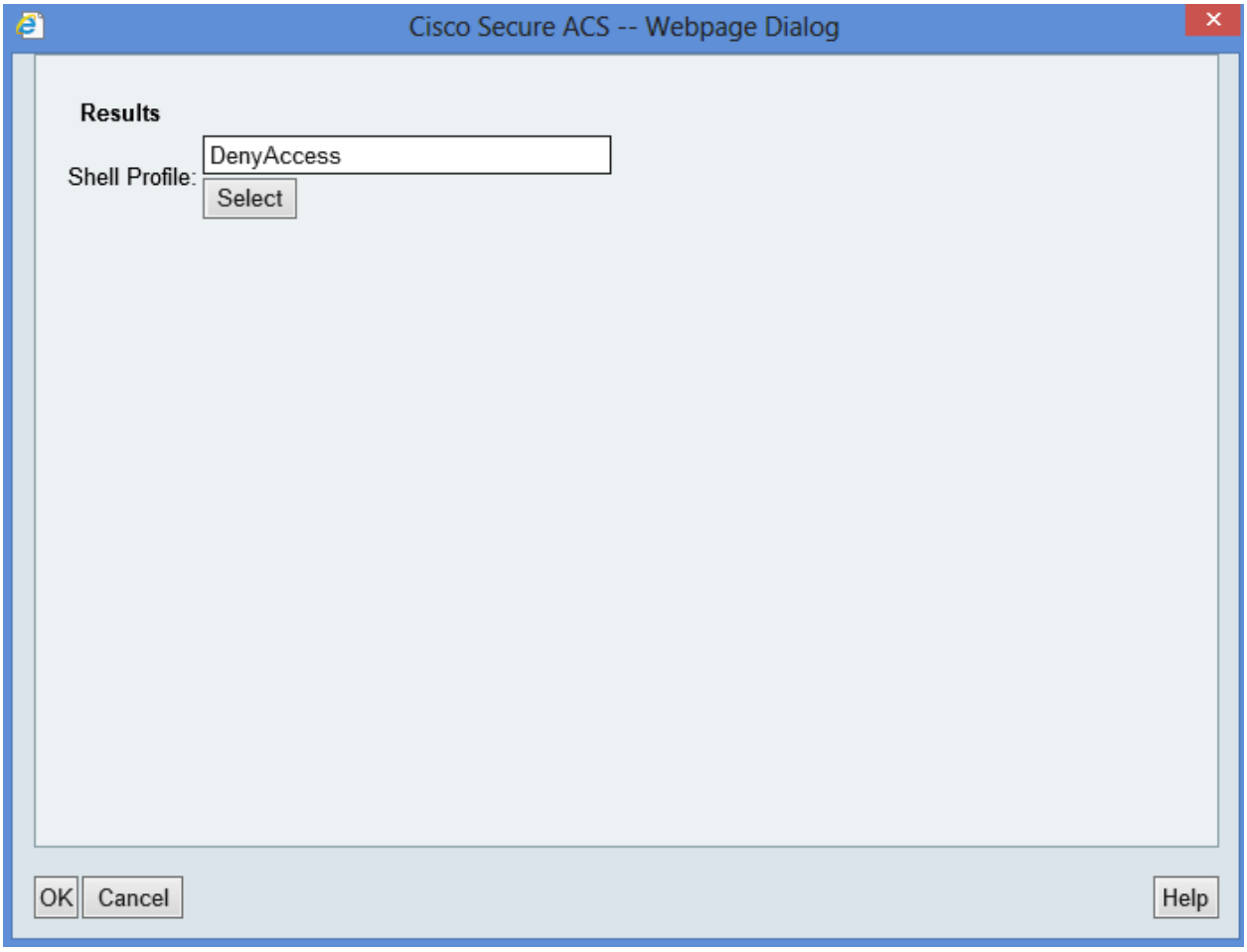


- Re-configure the default rule with DenyAccess shell profile.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Default** rule and change the Shell profile to DenyAccess.

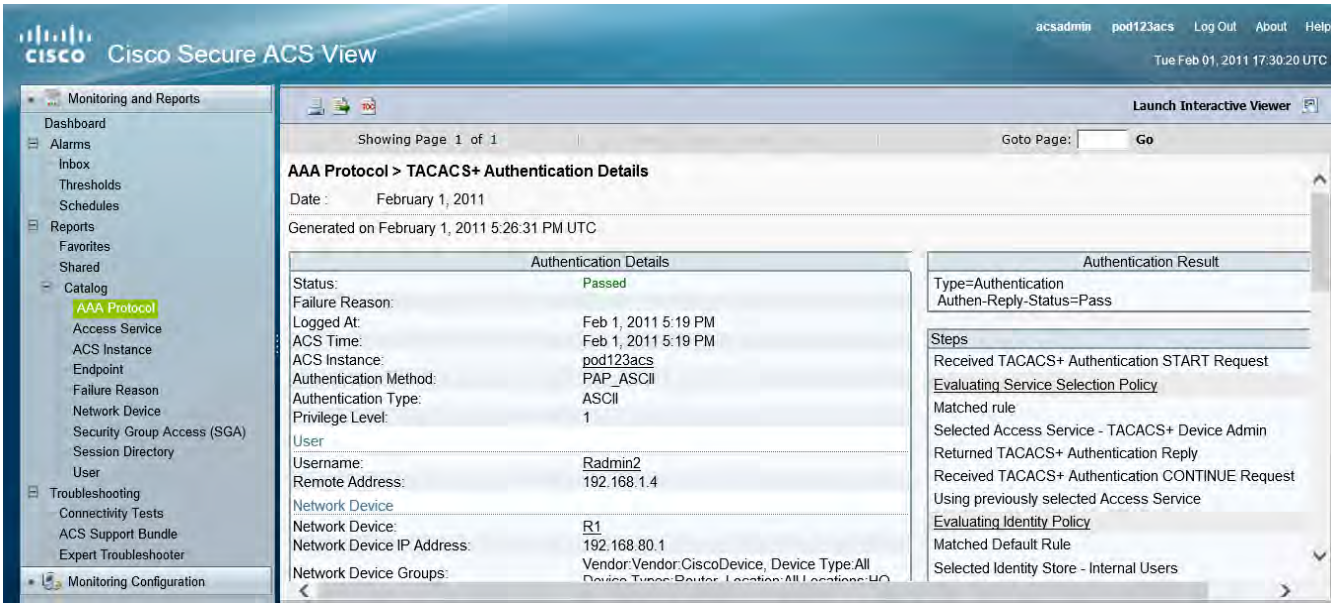


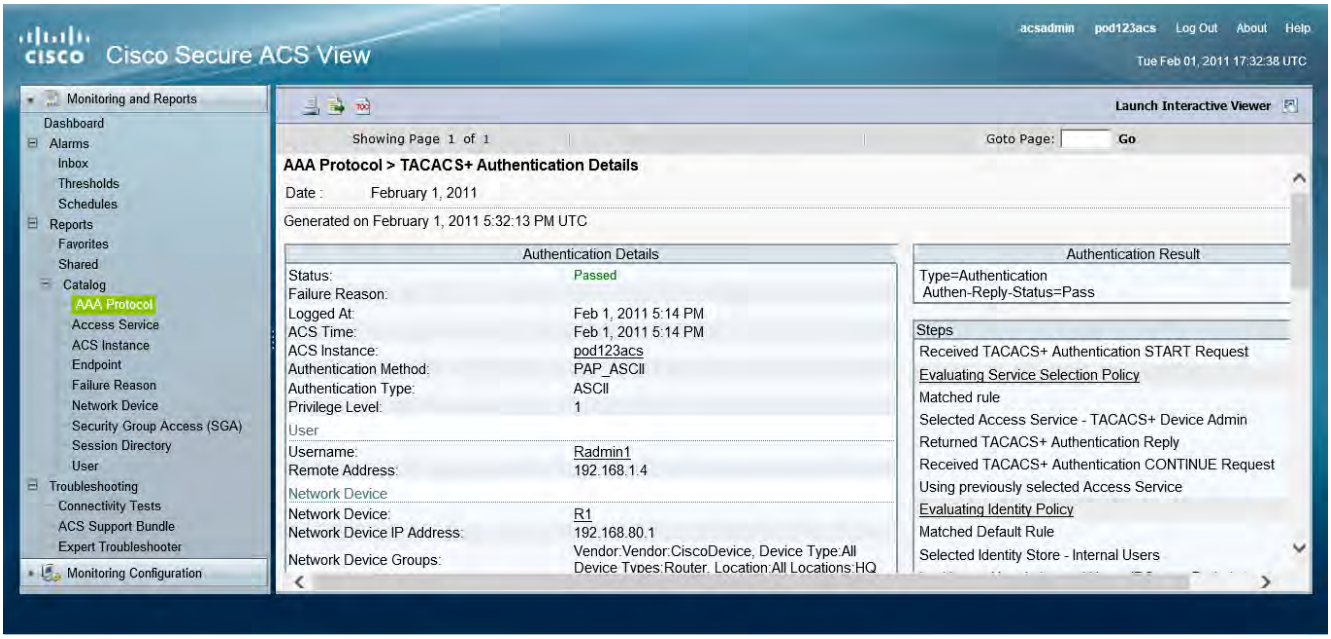
Verification

Telnet into R1 or R2 and test the command authorization.

```
SW4#telnet 192.168.1.10
Trying 192.168.1.10 ... Open

Enter your User-ID: Radmin1
Enter your Password:

R1#show privilege
Current privilege level is 15
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
R1#exit

[Connection to 192.168.1.10 closed by foreign host]

SW4#telnet 192.168.1.10
Trying 192.168.1.10 ... Open

Enter your User-ID: Radmin2
Enter your Password:

R1#show privilege
Current privilege level is 7
```

Go to Monitoring and Reports and click on Launch Report viewer. Then browse to Catalog->AAA Protocol ->TACACS+ Authentication. Then click on detail for the appropriate entry.





Task 7: Configure ACS for authorization rules in TACACS+ Device Admin access service for ASA

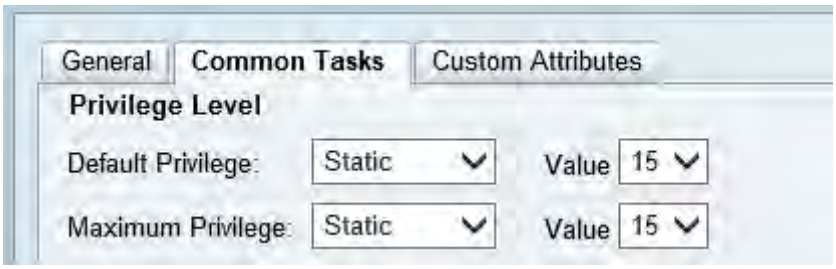
- Create a Shell Profile called “FWShellProfile” configure the privilege level to 15.

Solutions

ACS

Step 1: Go to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles** and click on **Create**. Name the shell profile as “FWShellProfile”.

Step 2: Click on **Common Tasks** tab and configure the value for the privilege level.

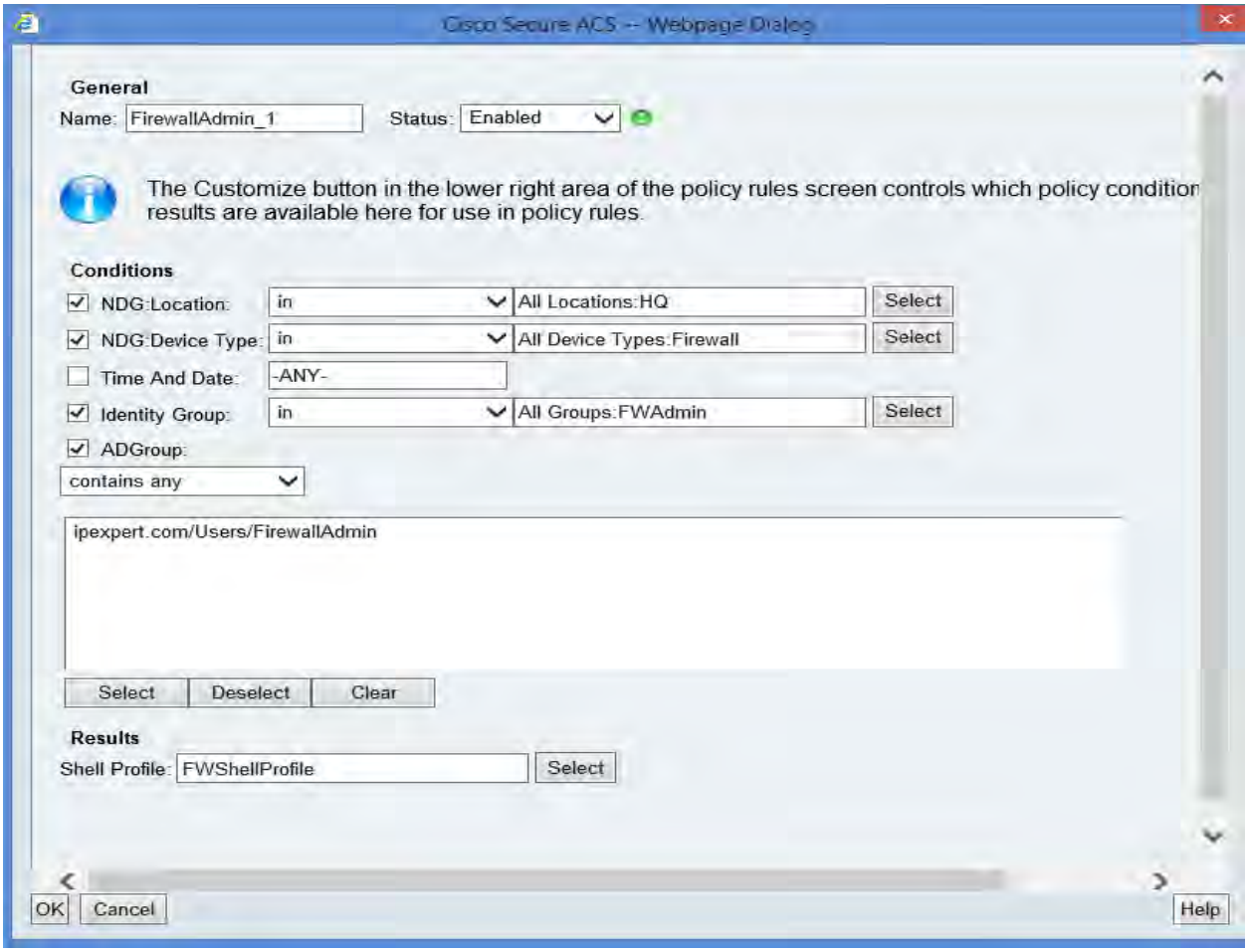


- Add another authorization rule for accessing the ASA in TACACS+ Device Admin access policy.
- Only users from FWAdmin group should be given access to the ASA. Policy should include local identity group as one of the condition and also check if users belong to an AD group of FirewallAdmin. Use “FWShellProfile” as the authorization result.

Solutions

ACS

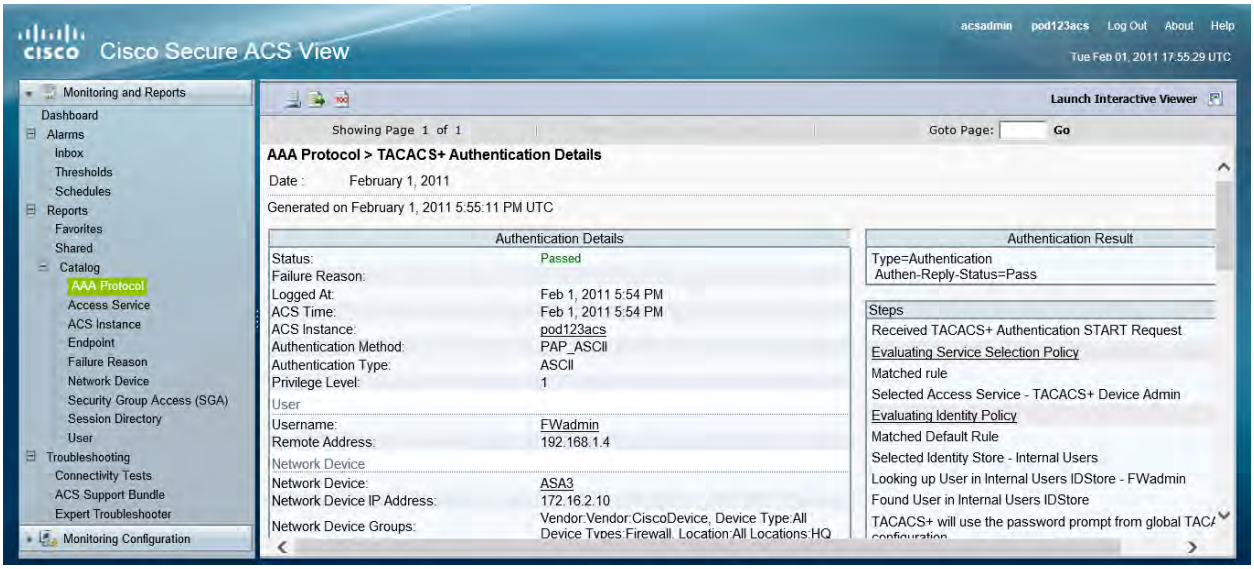
Step 1: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Create**. Then click on **Save Changes**.



Verification

Telnet or SSH into ASA3 inside interface from SW4.

```
SW4#telnet 172.16.2.10
Trying 172.16.2.10 ... Open


User Access Verification

Username: FWadmin
Password: *****
Type help or '?' for a list of available commands.
ASA3>
```



Task 8: Configure ACS for EXEC authorization RADIUS Device Admin access service for switches

- Change the authentication method to “LOCAL_AD” identity sequence for “RADIUS Device Admin” access service.

Solutions

ACS

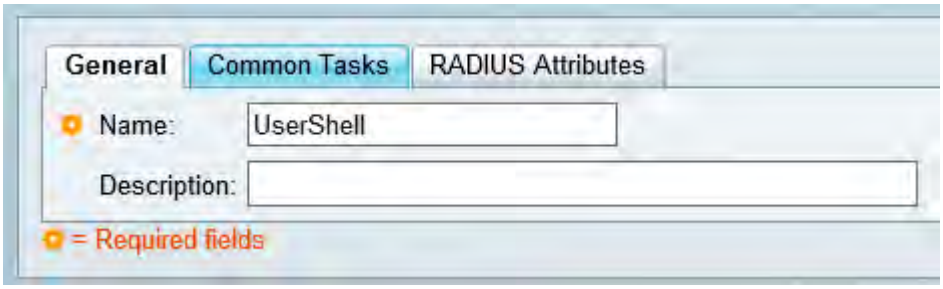
Step 1: Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Identity** and click on **Select**. Then choose “LOCAL_AD” as the identity source.

- Create a new authorization profile called “UserShell” to send Cisco-AV pair to assign a user to the appropriate shell privilege. The value for that attribute should be dynamically derived from the user attribute called “RadiusShellAttribute”. This attribute is present the internal user store.

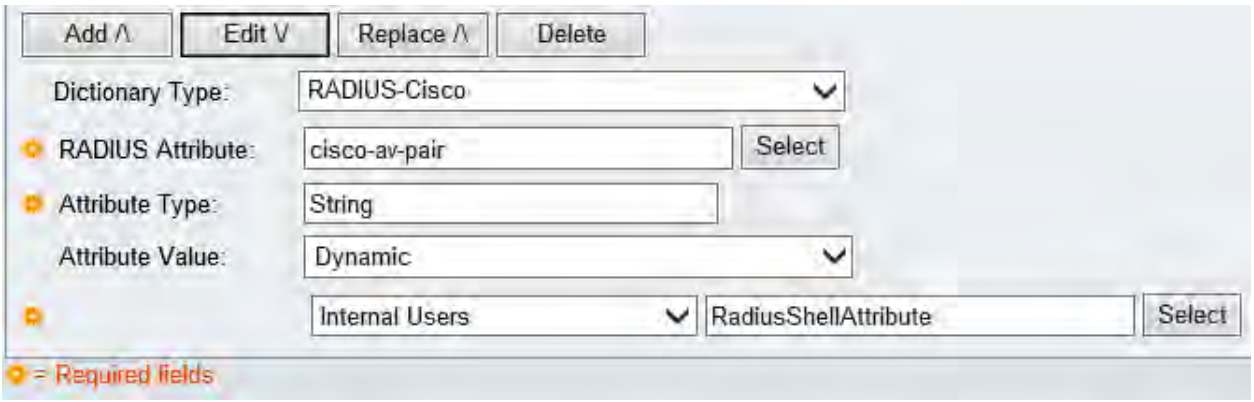
Solutions

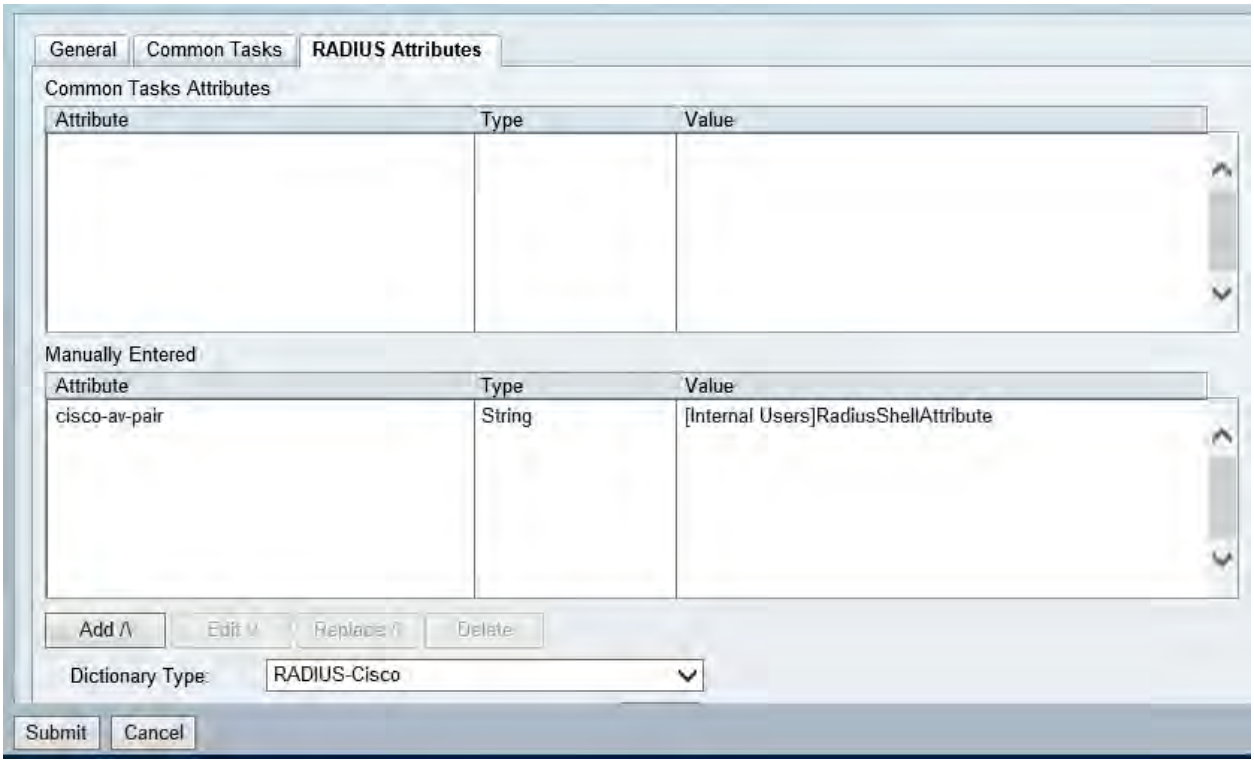
ACS

Step 1: Go to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click on **Create**. Name the shell profile as “UserShell”.



Step 2: Click on **RADIUS Attributes** tab and configure the cisco AV pair to use shell attribute value/string derived from an attribute (RadiusShellAttribute) in the internal users.



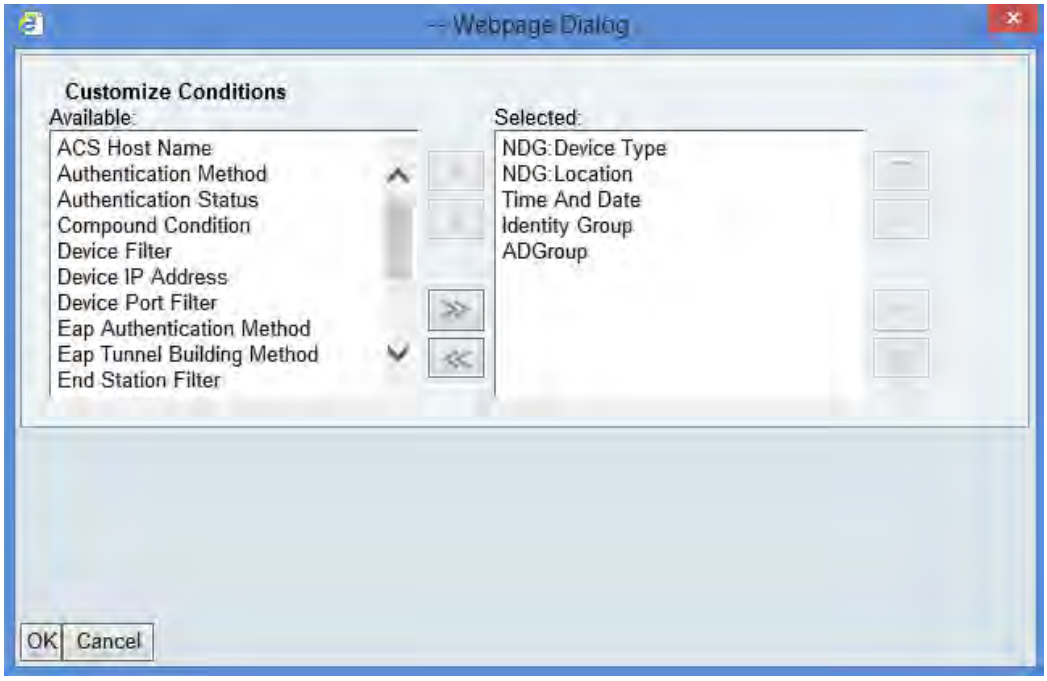


- SWAdmin1 user should be given complete to switches in the HQ for commands at privilege-level 15 and below. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of SwitchAdmin.
- SWAdmin2 user should be given access to switches in the HQ for all commands at privilege-level 7 and below. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of SwitchAdmin.
- Policy conditions should include date and time, NDG location, NDG Device type, Identity Group and ADGroup.
- Configure only one authorization rule to reflect the above policy requirement.

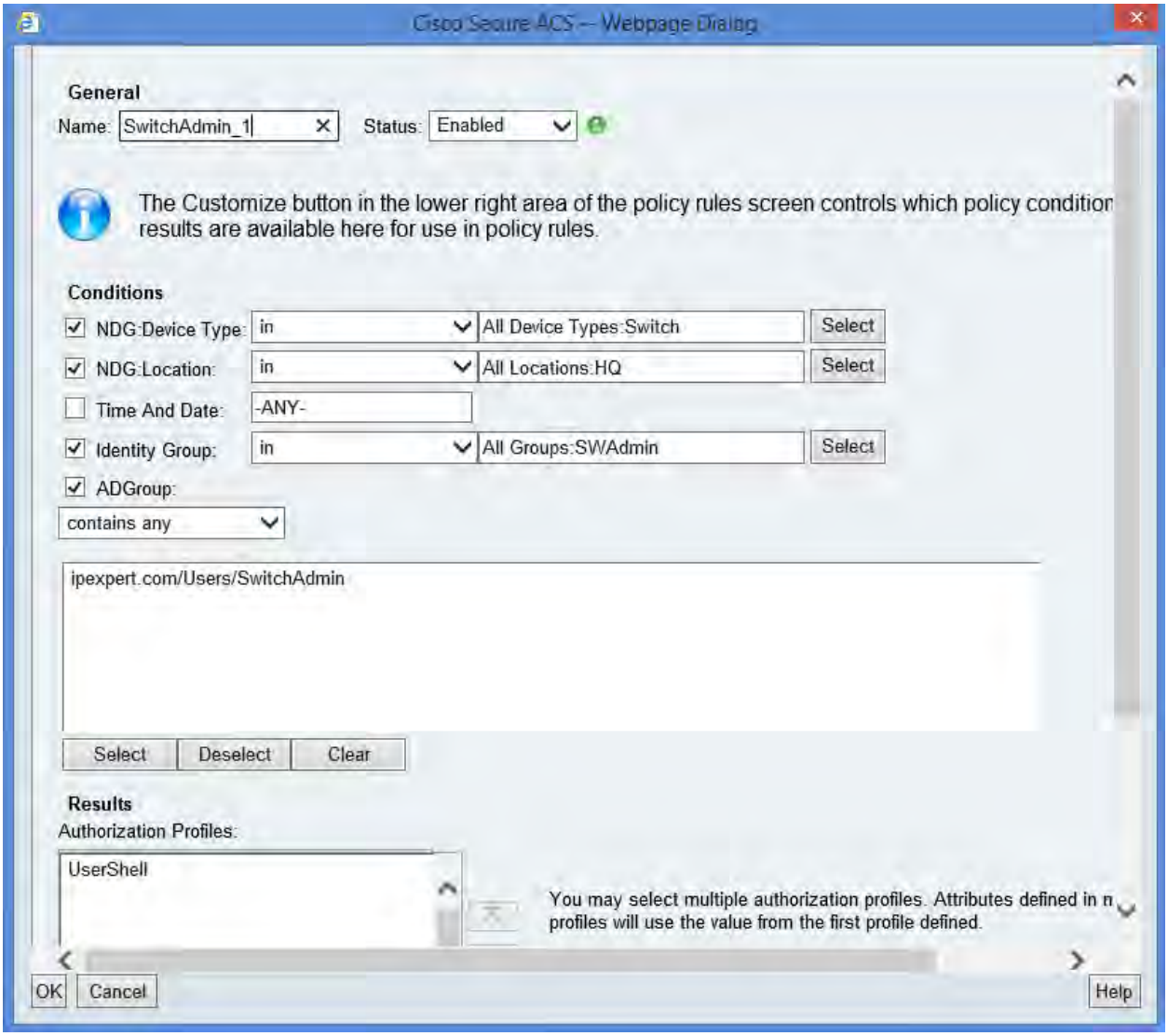
Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Customize** button and make sure you include date and time, NDG location, NDG Device type, Identity Group and ADGroup as conditions.



Step 2: Click on **Create** to configure authorization rules. Then click on **Save Changes**.

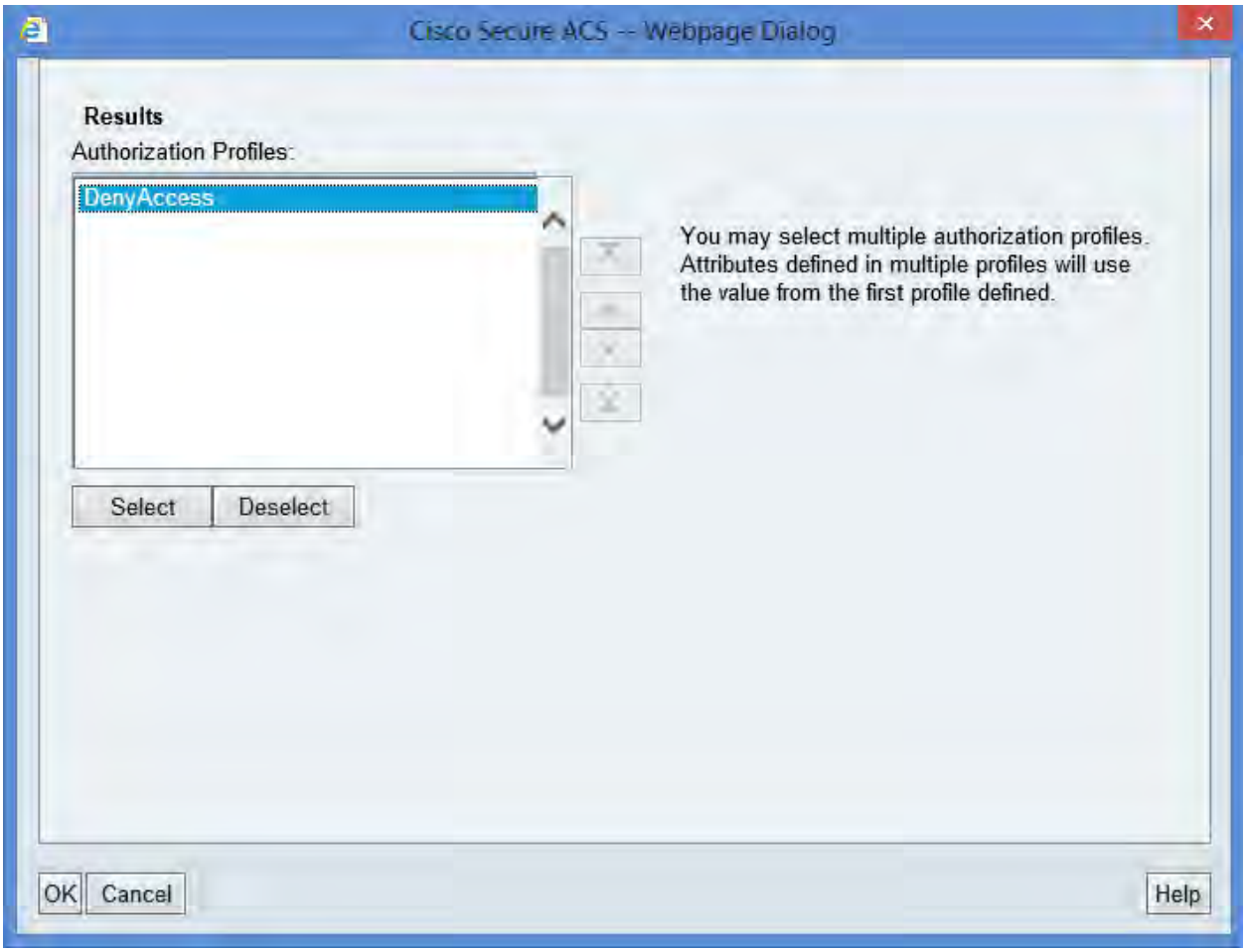


- Re-configure the default policy result to “DenyAccess”.

Solutions

ACS

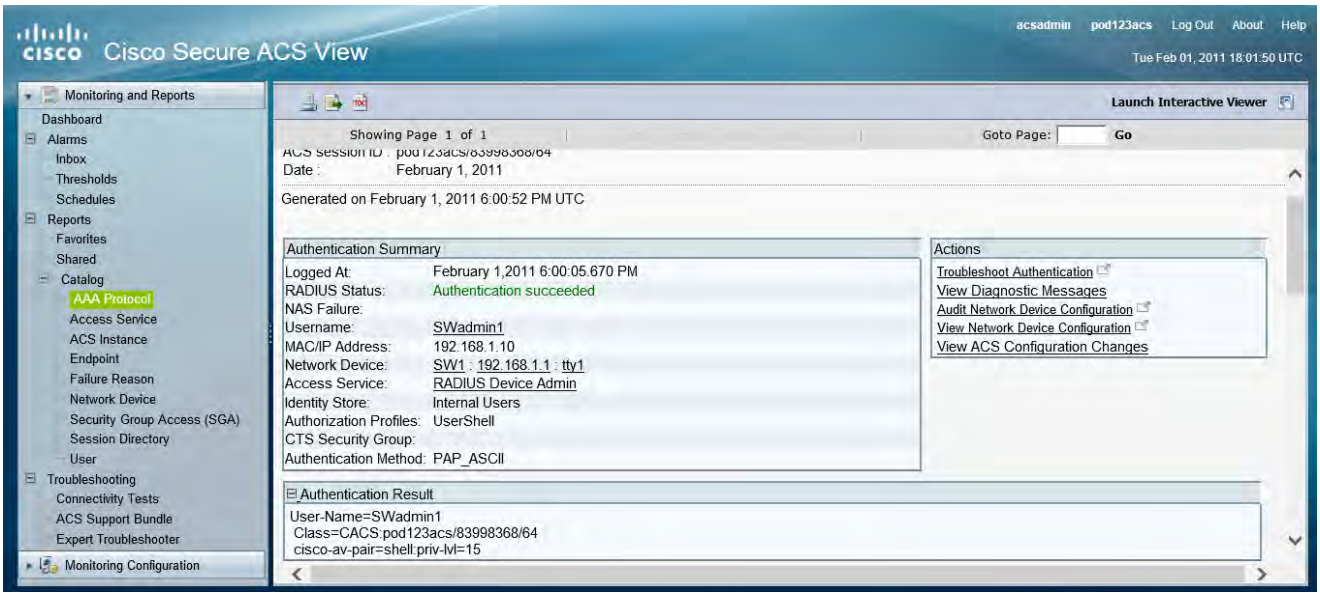
Step 1: Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Default** rule and change the Shell profile to DenyAccess.



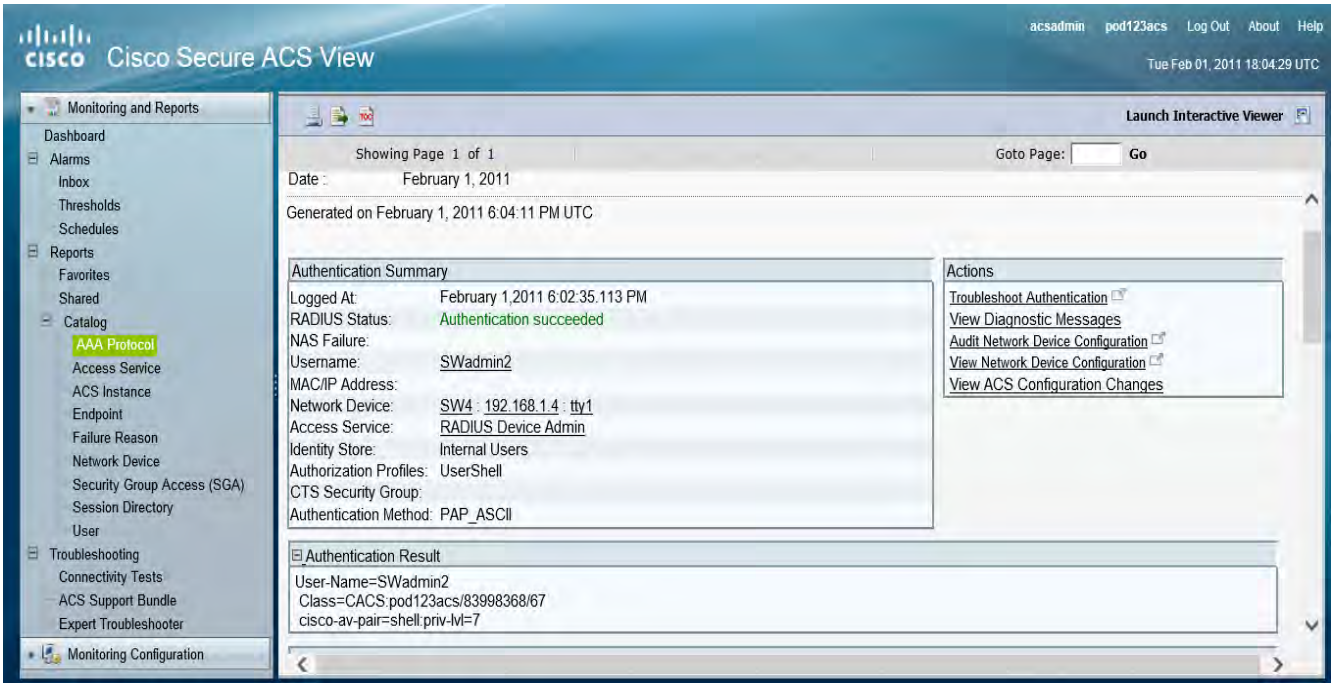
Verification

SSH into SW3 and SW1 from R1 or R2

```
R1#ssh -l SWadmin1 192.168.1.1

Enter your Password:

SW1#show privilege
Current privilege level is 15
```




```
R1#ssh -l SWadmin2 192.168.1.4
Unauthorized Access Prohibited
Enter your Password:
SW4#show privilege
Current privilege level is 7
SW4#conf t
SW4(config)#?
Configure commands:
  beep     Configure BEEP (Blocks Extensible Exchange Protocol)
  cts      Cisco Trusted Security commands
  default  Set a command to its defaults
  end      Exit from configure mode
  exit     Exit from configure mode
  help     Description of the interactive help system
  ip       Global IP configuration subcommands
  license  Configure license features
  netconf  Configure NETCONF
  no       Negate a command or set its defaults
  sasl     Configure SASL
  vlan     Vlan commands
  wsma     Configure Web Services Management Agents
```



Task 9: Advanced authorization rules for RADIUS and TACACS+ Device Admin access policies.

- NetAdmin user should be given complete access to any device in the network.
- Create a new Shellprofile called “NetAdmin” Assign a TACACS+ custom attribute used for role base CLI view of “root”. Assign the appropriate privilege level for this user.
- Create a new authorization profile called “NetAdmin” and configure the appropriate RADIUS A/V pairs.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for NetAdmin user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of NetworkAdmin.
- NetOPS user should not be able to make any configuration changes for devices in the HQ. This user can only execute privilege level 1 commands for any devices in the HQ except ASA3. This user should be able to login to branch routers with a view of “NetOps”.
- Create a new Shellprofile called “NetOps” Assign a TACACS+ custom attribute used for role base CLI view of “NetOps”. Assign the appropriate privilege level for this user.
- Create a new authorization profile called “NetOps” and configure the appropriate RADIUS A/V pairs.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for NetOps user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of Operator.
- SecOps user can only access branch routers.
- Create a new Shellprofile called “SecOps” Assign a TACACS+ custom attribute used for role base CLI view of “SecOps”.

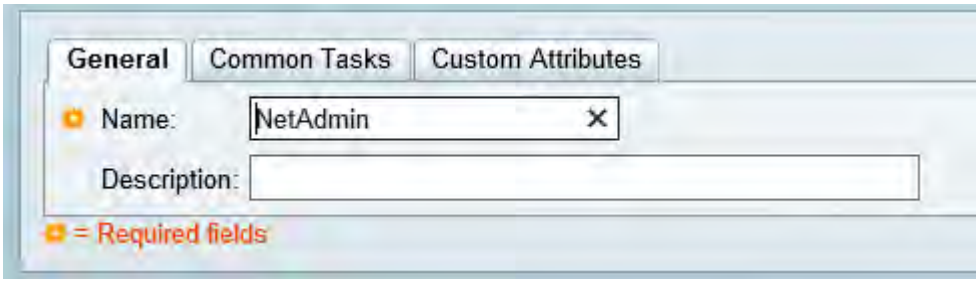
- Create a new authorization profile called “SecOps” and configure the appropriate RADIUS A/V pair.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for SecOps user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of Operator.
- AOps user can only access branch routers.
- Create a new Shellprofile called “AOps” Assign a TACACS+ custom attribute used for role base CLI view of “AOps”.
- Create a new authorization profile called “AOps” and configure the appropriate RADIUS A/V pair.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for AOps user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of Operator.
- All Ops/operator users should be able to login to the network only during weekdays between 8 AM to 6 PM. Limit maximum number of sessions to 1 for Ops/Operator group
- You are allowed to add extra condition of username in the authorization rules to accomplish task 9.

Solutions

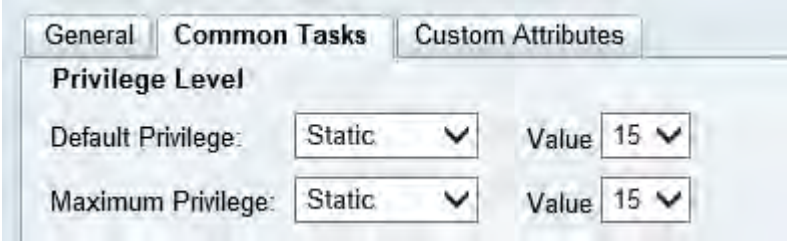
ACS

(Create policies for NetAdmin user)

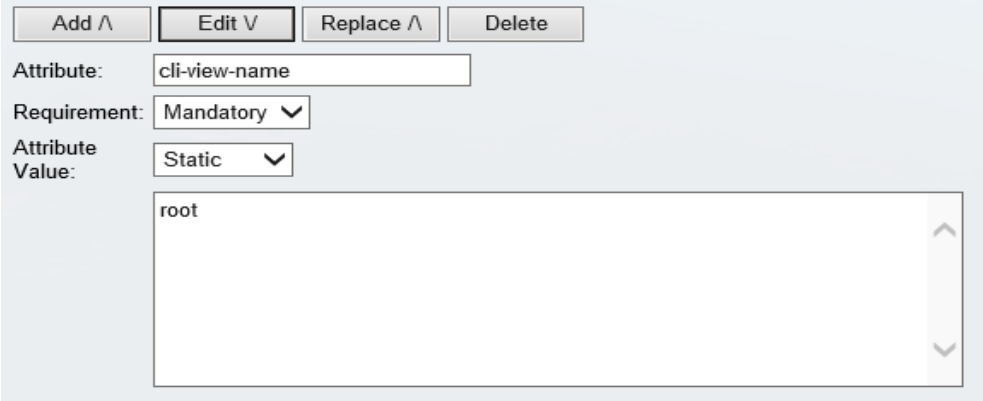
Step 1: Configure a shell profile called “NetAdmin”. Go to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles**. Click on **Create**.

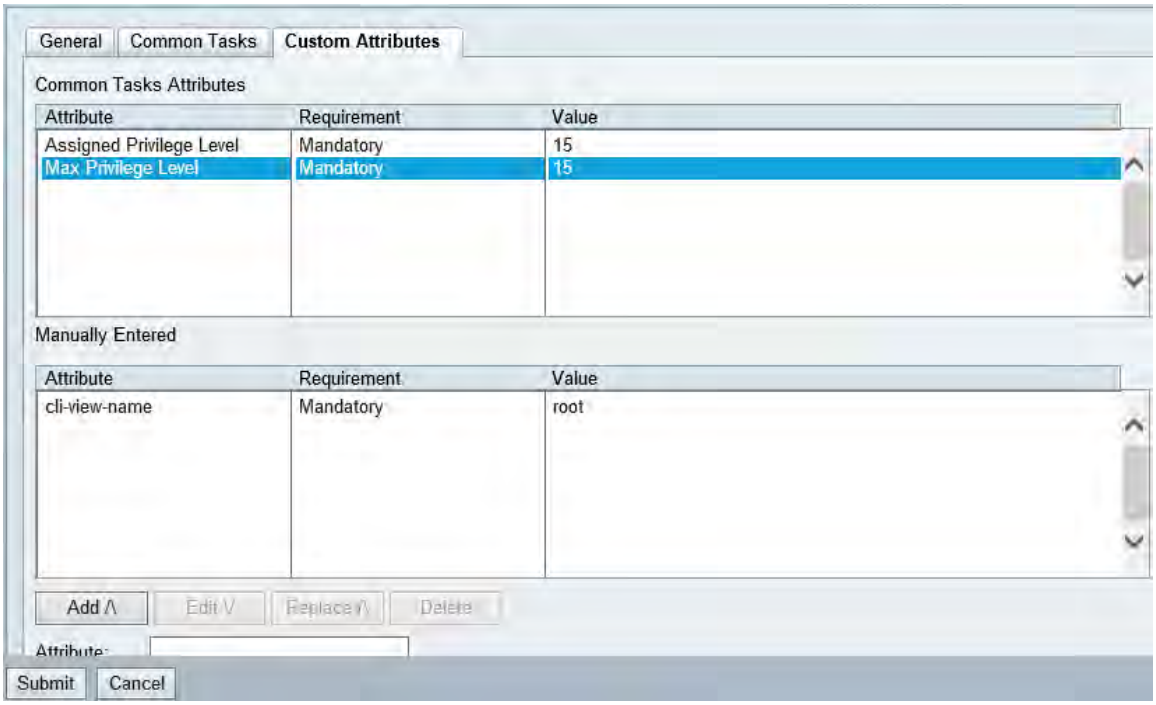


Step 2: Click on Common Tasks tab and configure the privilege level of 15.

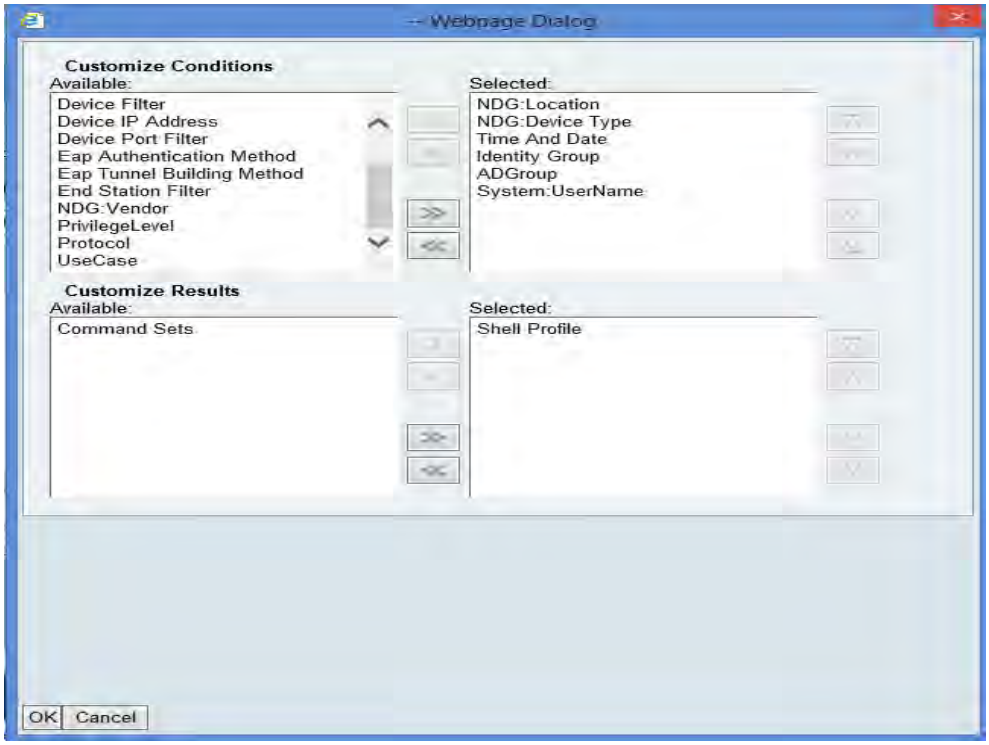


Step 3: Click on Custom Attributes and send the CLI view name of root for NetAdmin.

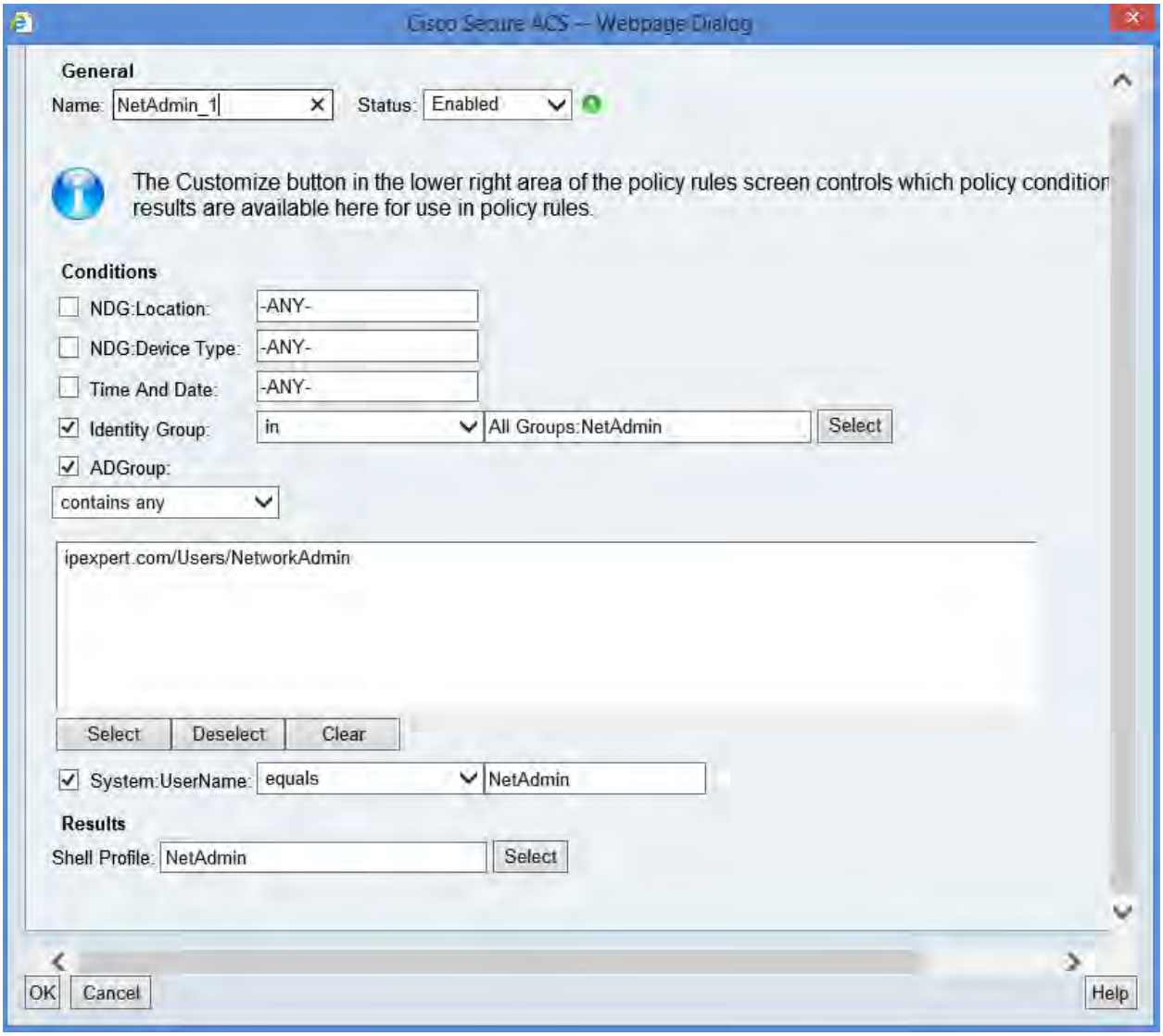




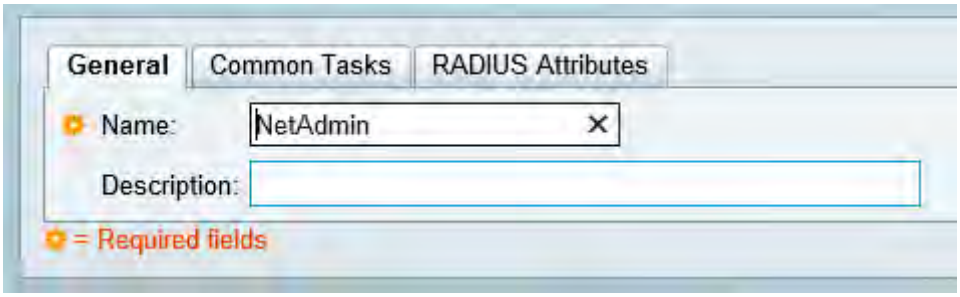
Step 4: Configure authorization rule for TACACS+ Device admin. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Customize** and add local username as an additional condition.



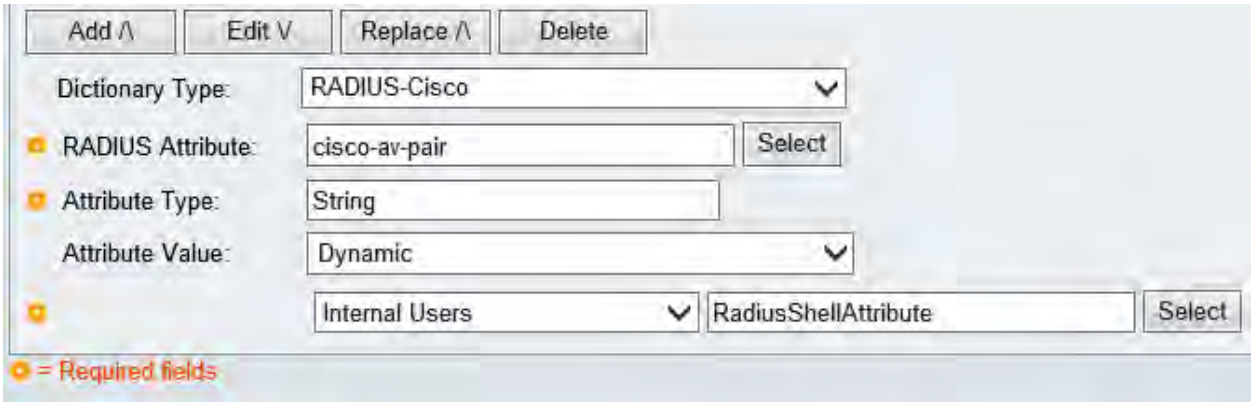
Step 5: Now add the authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.



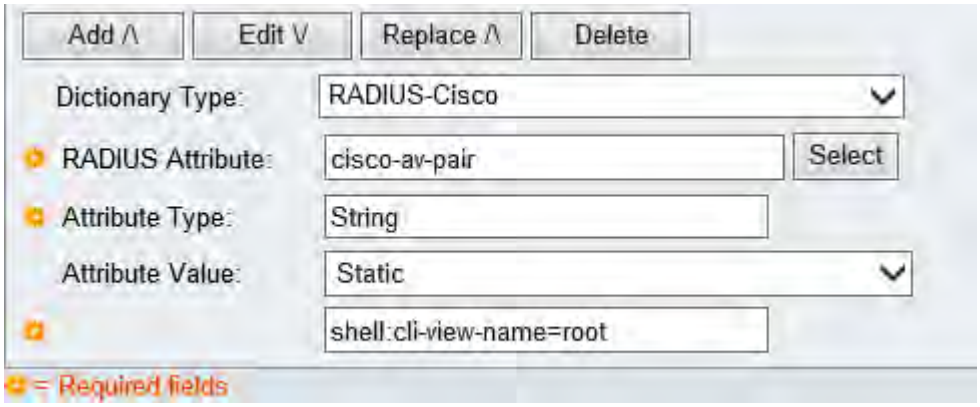
Step 6: Go to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click on **Create**. Name the shell profile as "NetAdmin".

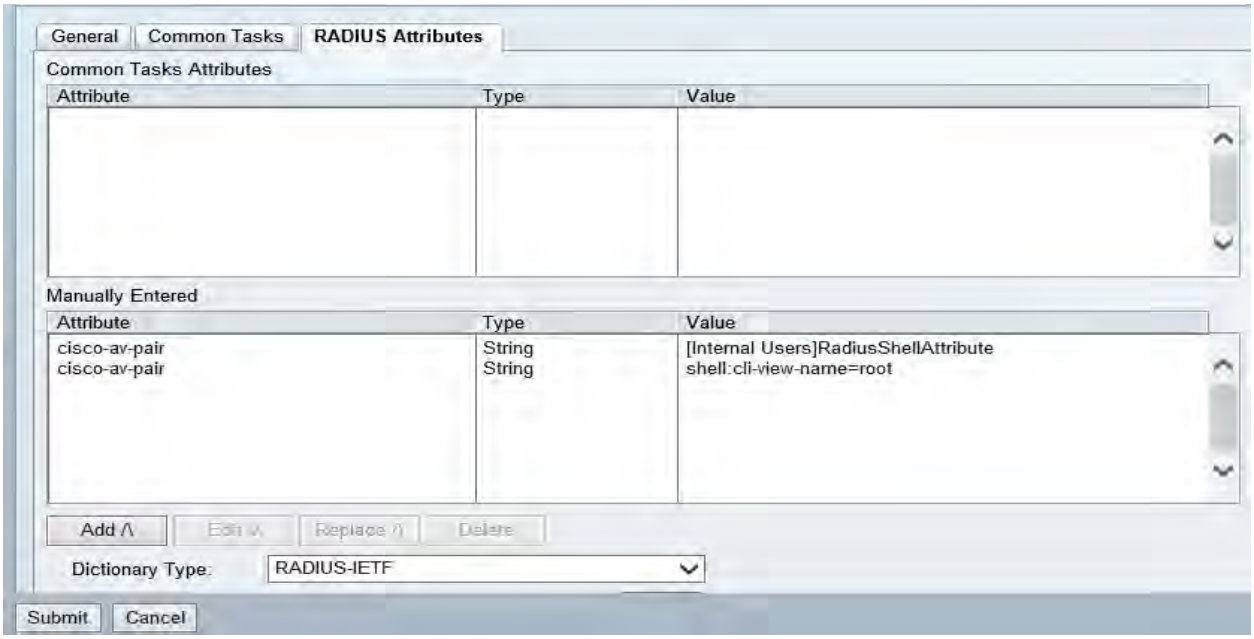


Step 7: Click on **RADIUS Attributes** tab and configure the Cisco AV pair to send Cisco AV pair for assigning privilege level.



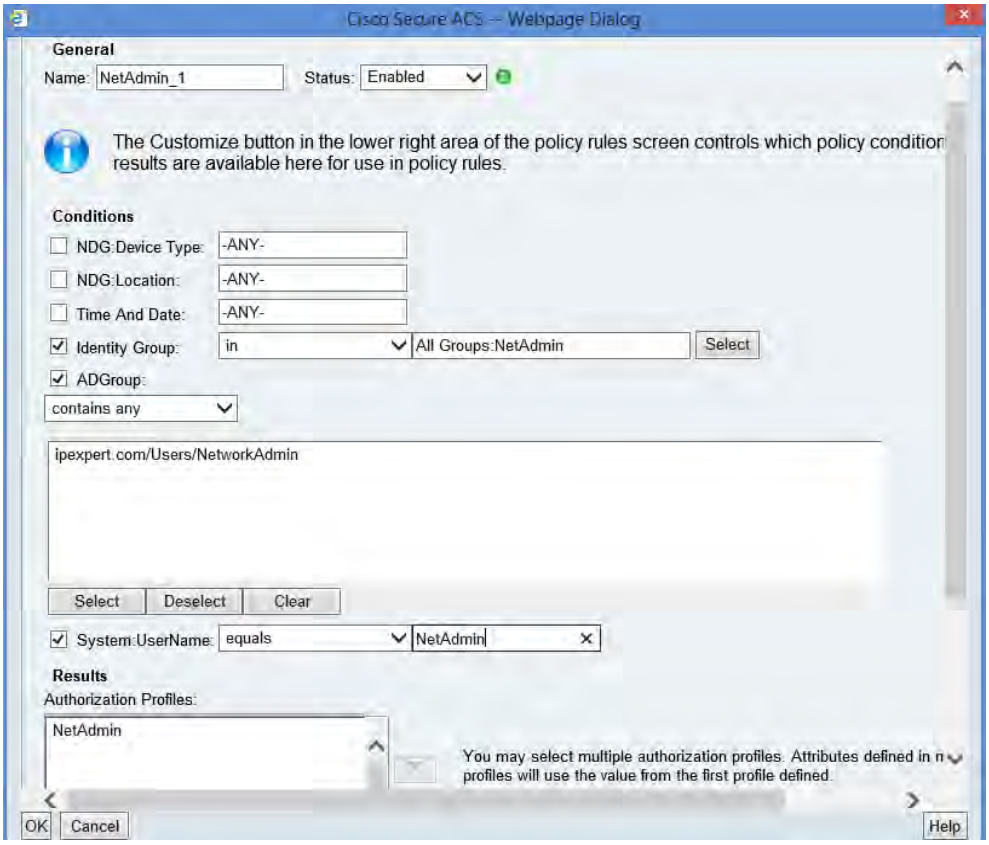
Step 8: Click on **RADIUS Attributes** tab and configure the Cisco AV pair to send the view name.





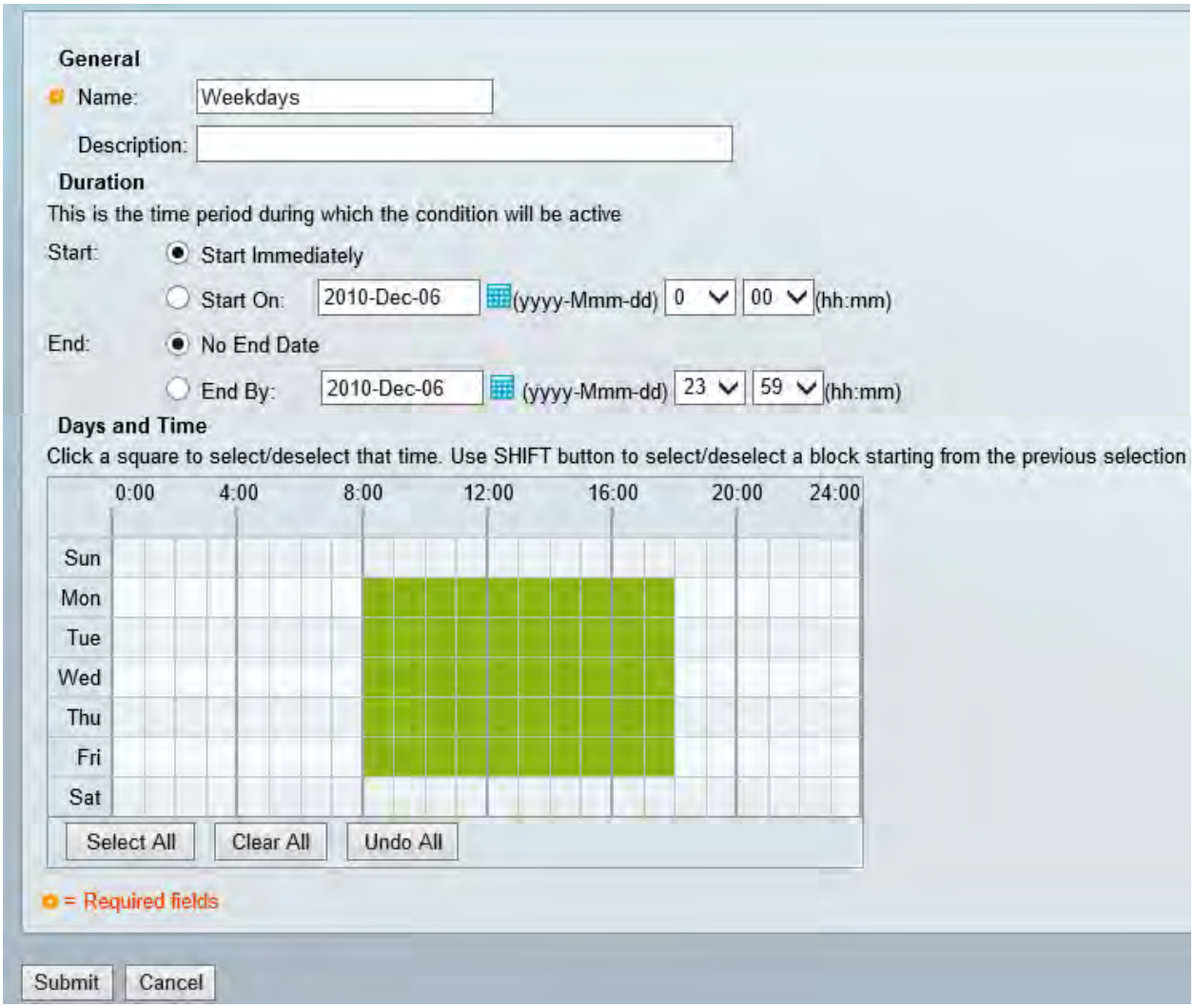
Step 9: Configure authorization rule for RADIUS Device admin. Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Customize** and add local username as an additional condition.

Step 10: Now add the authorization rule. Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.

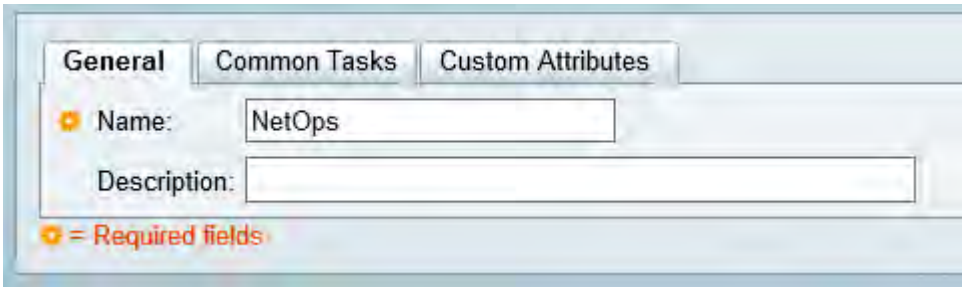


(Create policies for NetOps user)

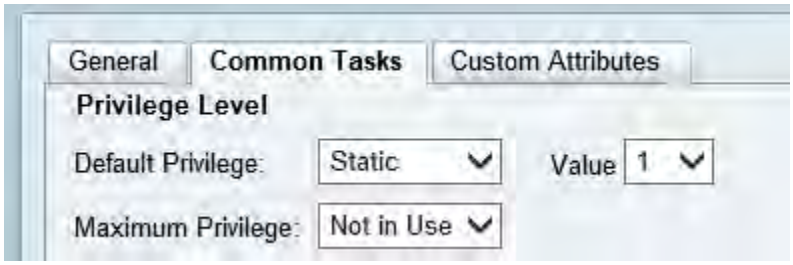
Step 1: Configure date and time policy element for the operator user. Go to **Policy Elements -> Session Conditions -> Date and Time** and click on **Create**.



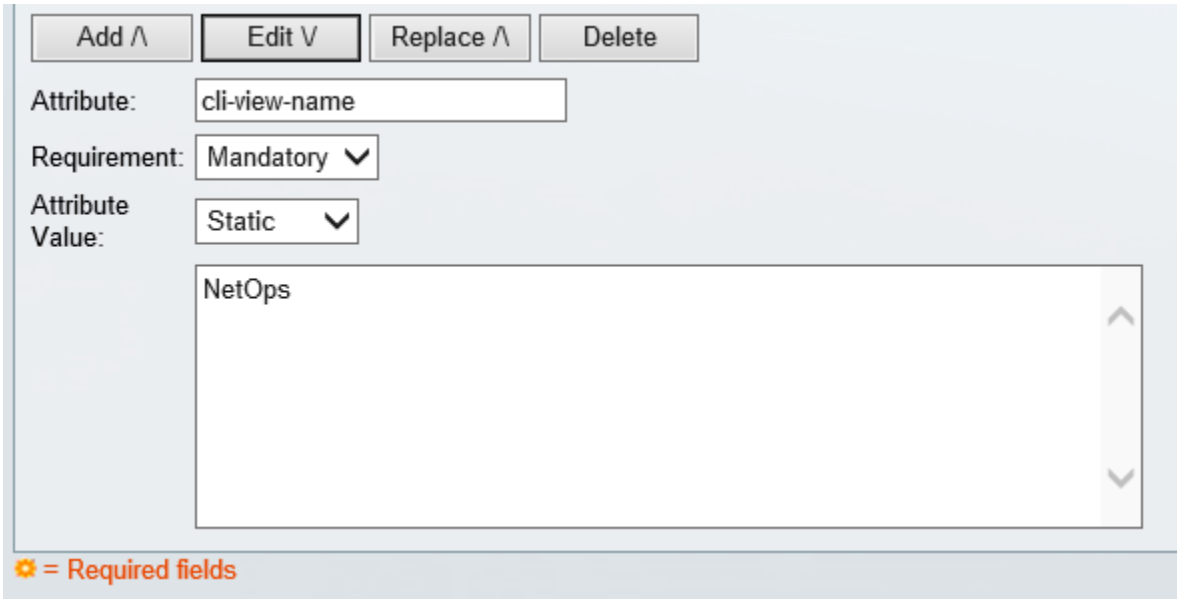
Step 2: Configure a shell profile called "NetOps". Go to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles**. Click on **Create**.

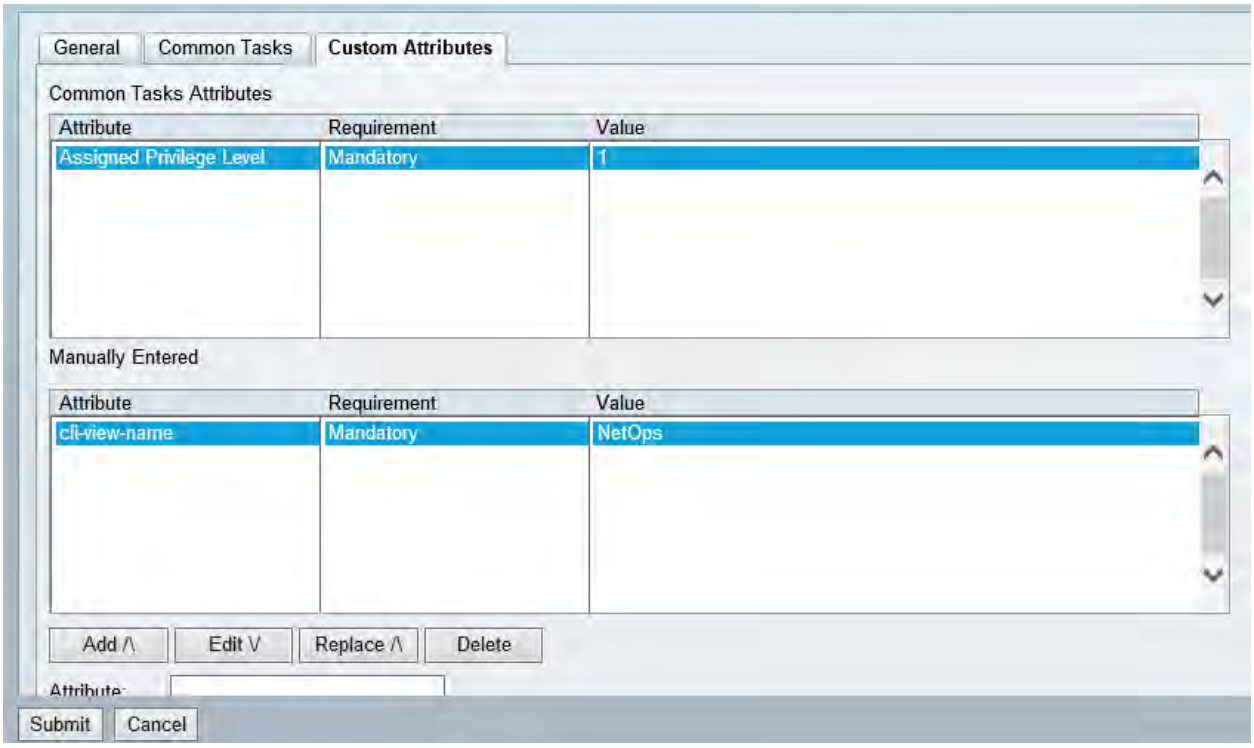


Step 3: Click on Common Tasks tab and configure the privilege level of 15.

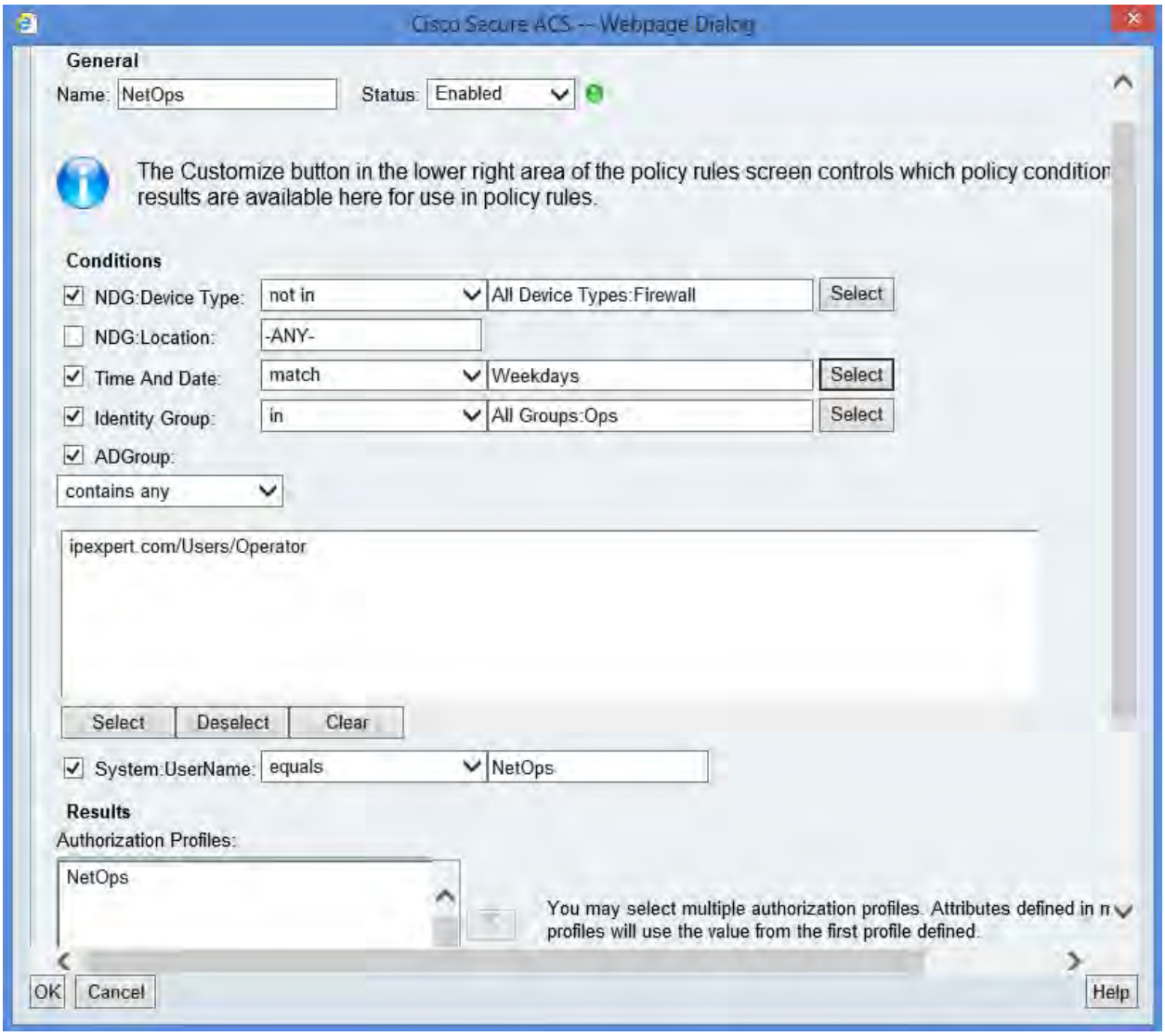


Step 4: Click on Custom Attributes and send the CLI view name of root for NetAdmin.

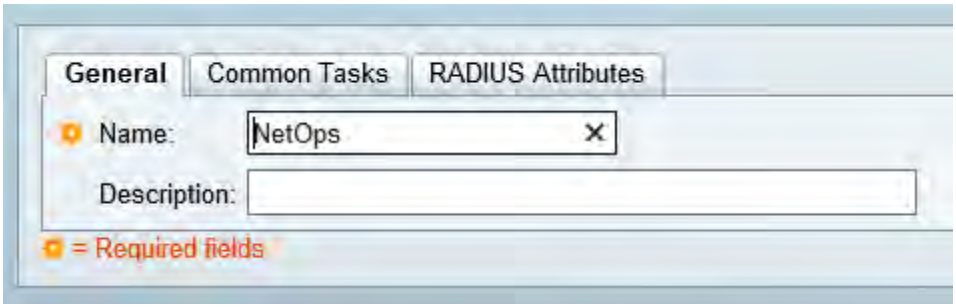




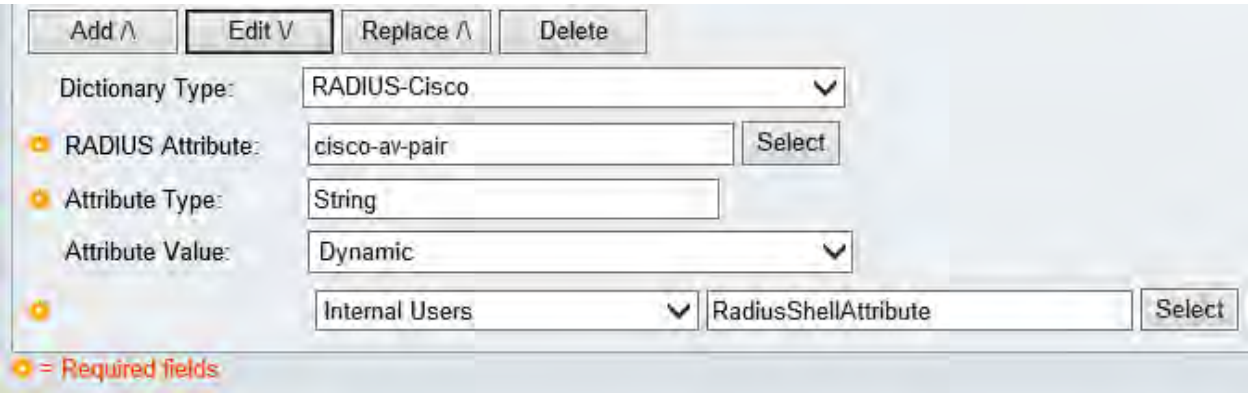
Step 5: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization.** Click on **Create**.



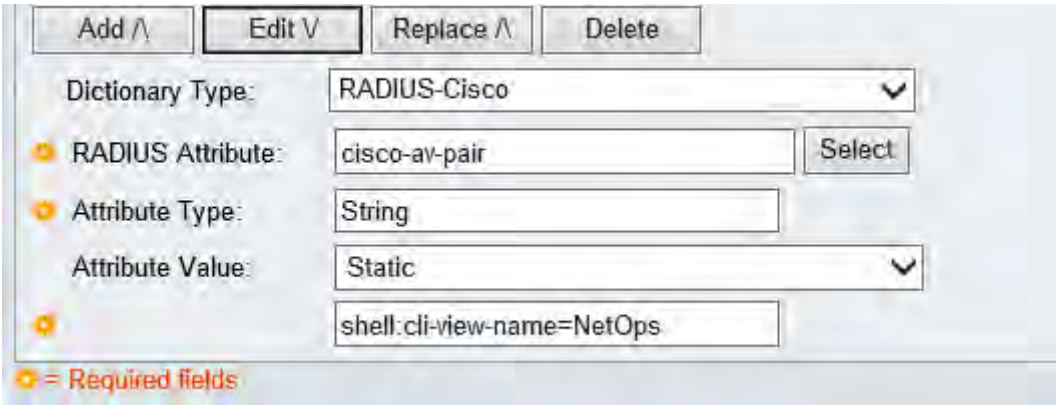
Step 6: Go to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click on **Create**. Name the shell profile as "NetOps".

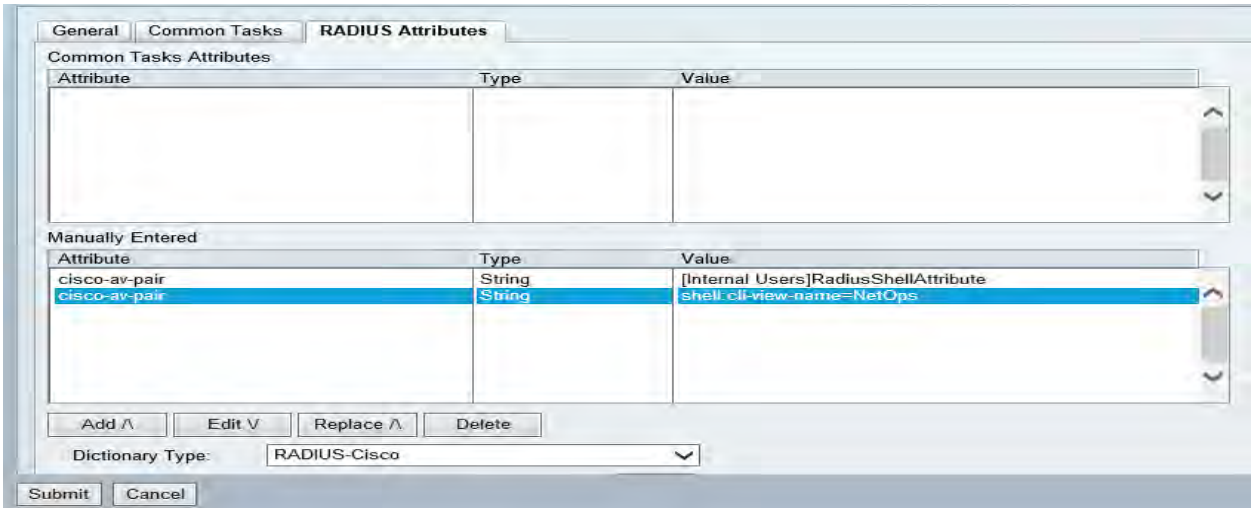


Step 7: Click on **RADIUS Attributes** tab and configure the Cisco AV pair to send Cisco AV pair for assigning privilege level.

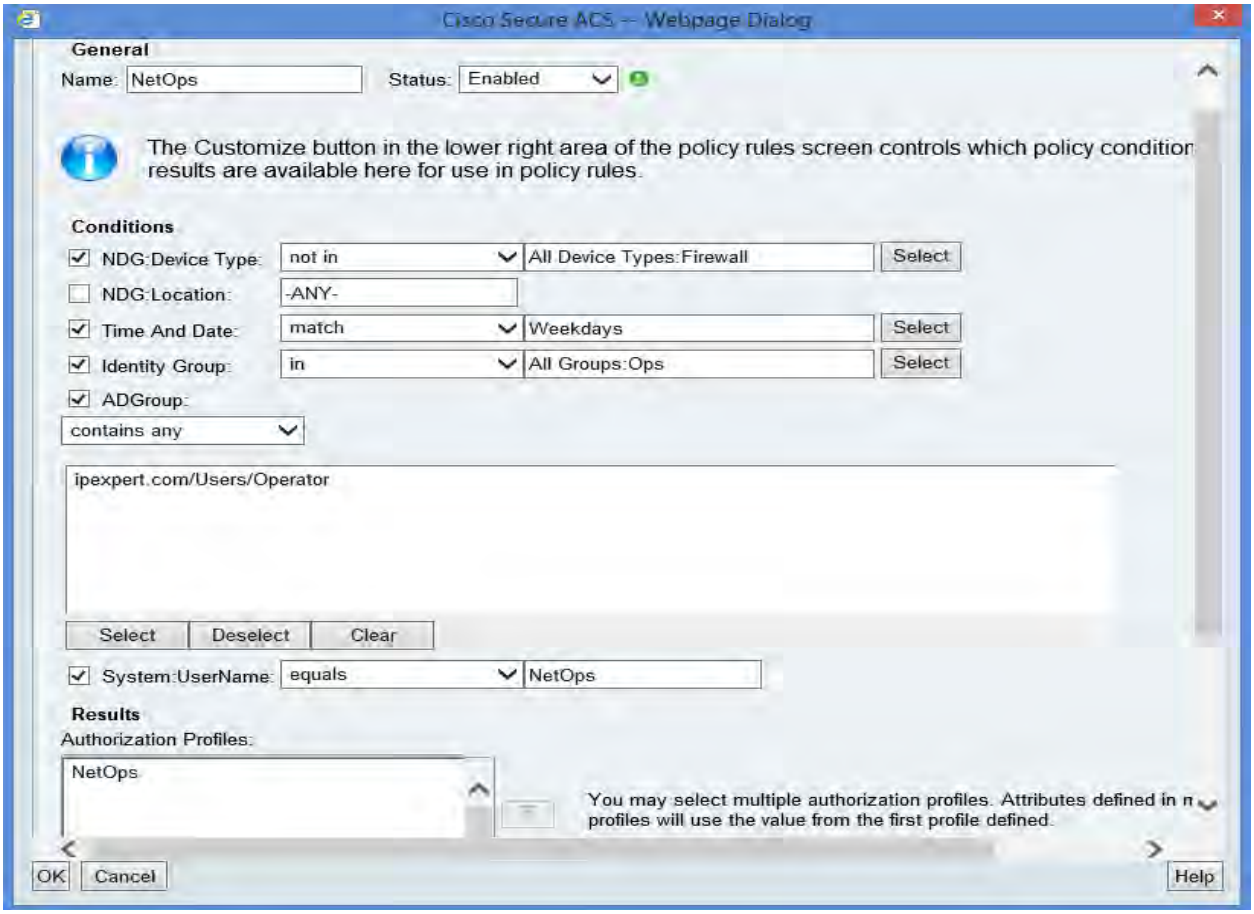


Step 8: Click on **RADIUS Attributes** tab and configure the Cisco AV pair to send the view name.



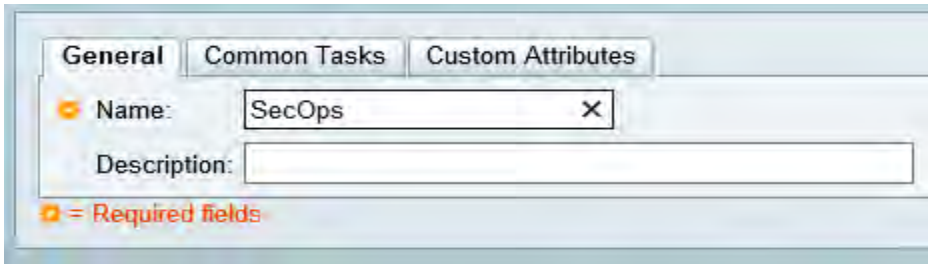


Step 9: Create the authorization rule. Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.

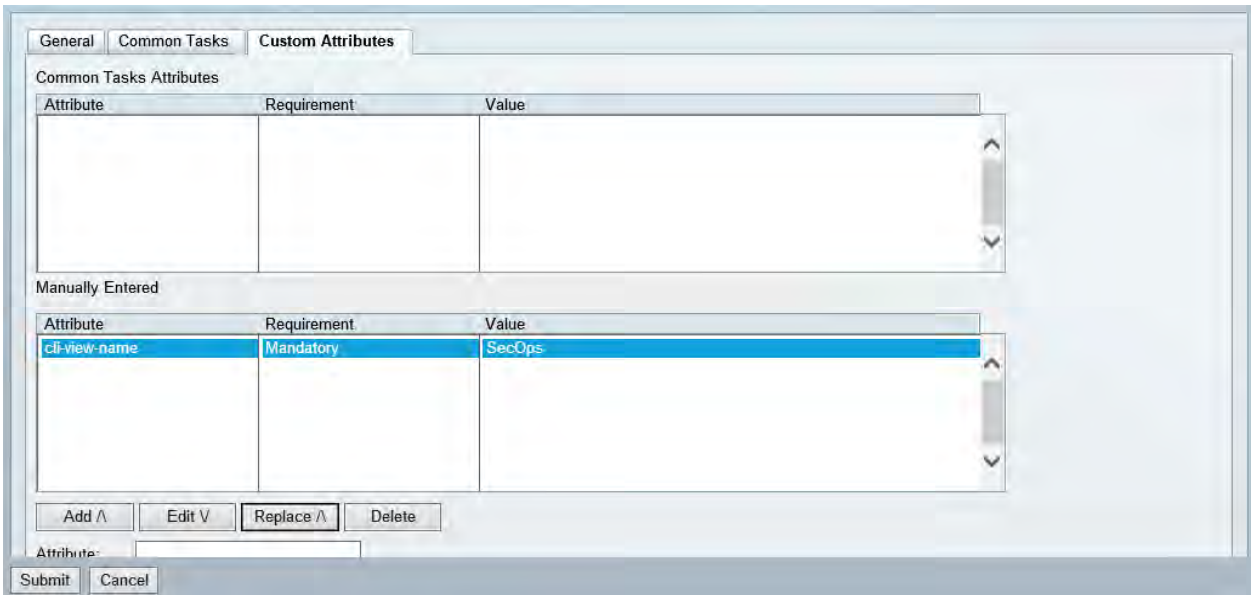


(Create policies for SecOps user)

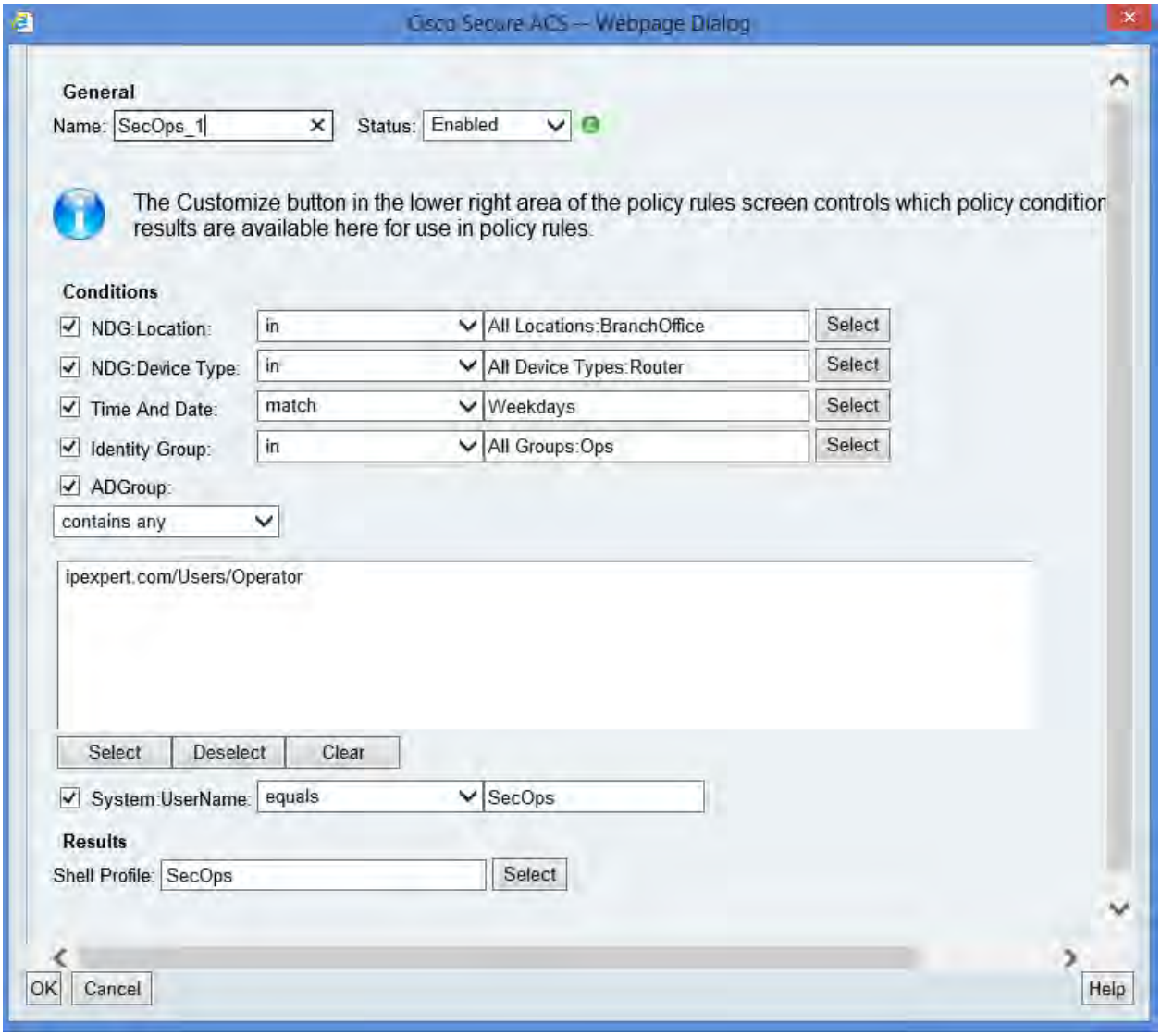
Step 1: Configure a shell profile called "SecOps". Go to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles**. Click on **Create**.



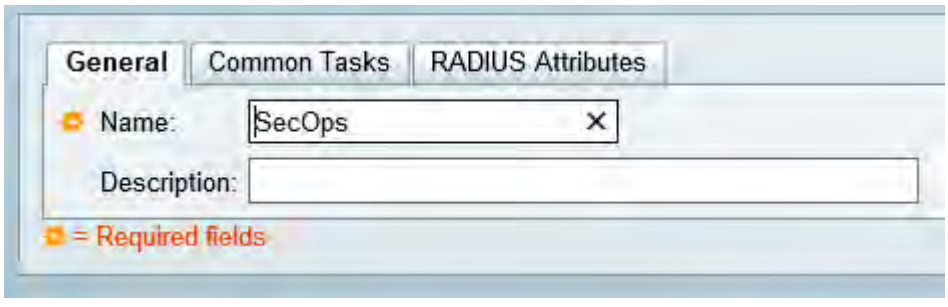
Step 2: Click on Custom Attributes and send the CLI view name of root for NetAdmin.



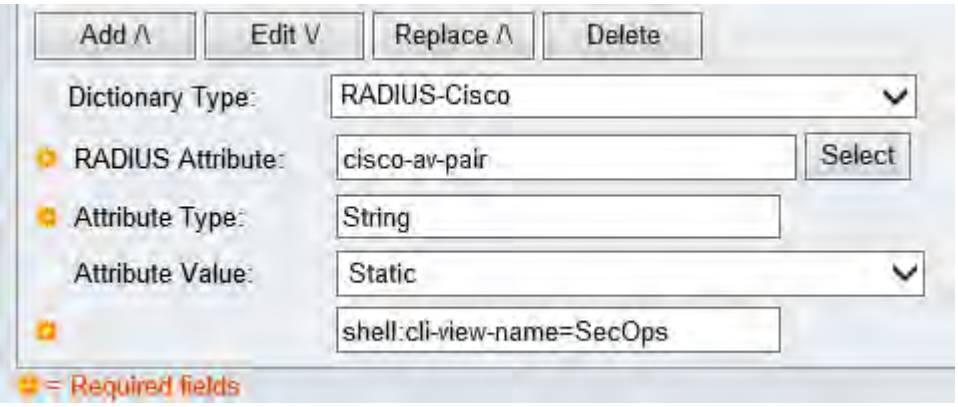
Step 3: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization.** Click on **Create**.

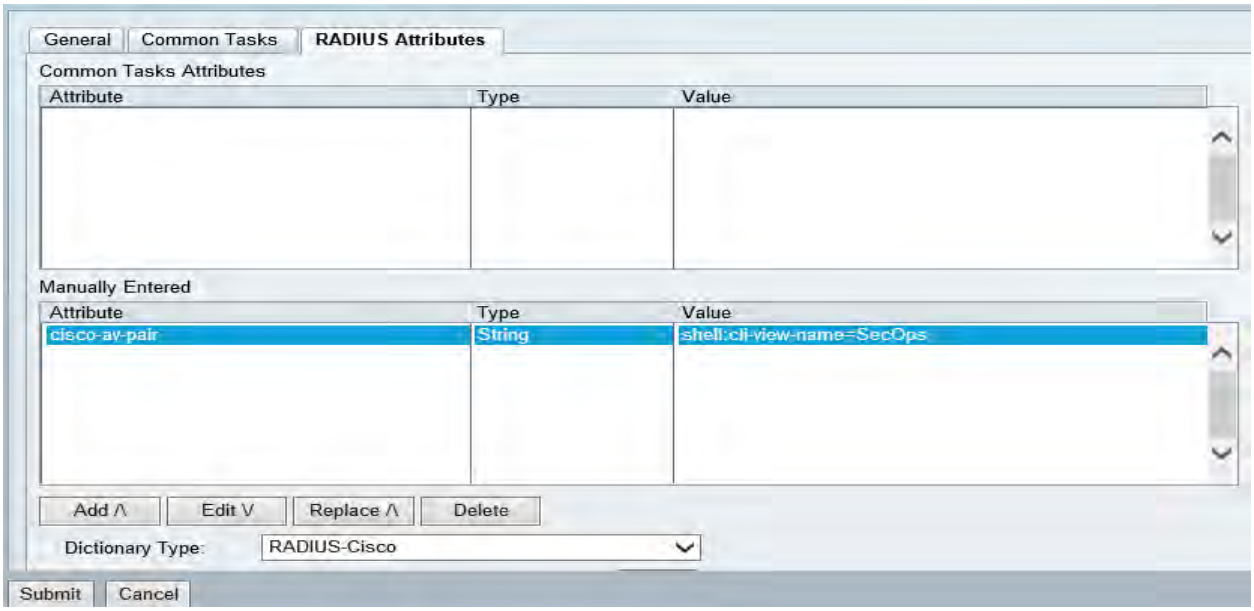


Step 4: Now add the authorization rule. Go to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click on **Create**. Name the shell profile as "SecOps".

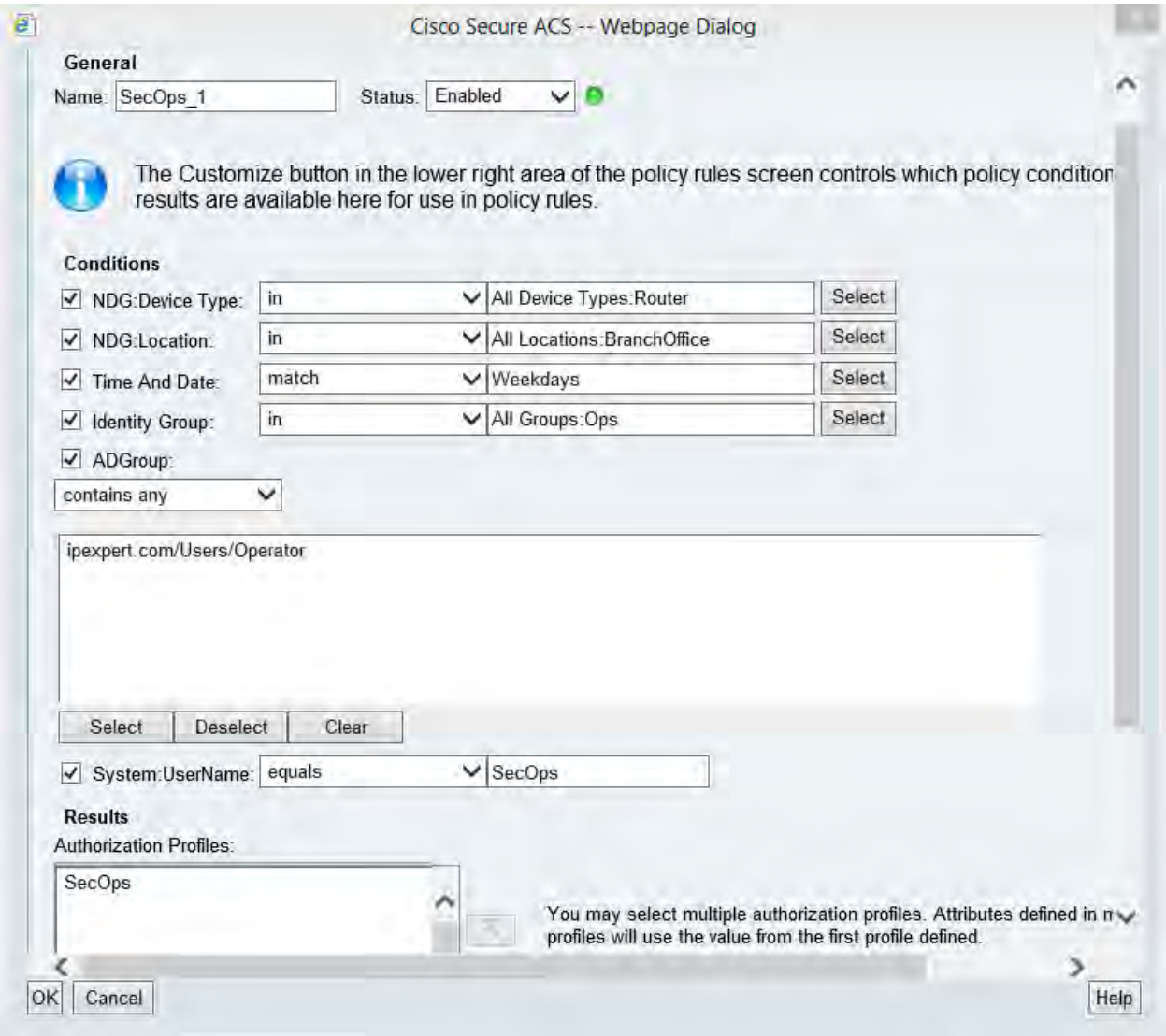


Step 5: Click on **RADIUS Attributes** tab and configure the Cisco AV pair to send the view name.



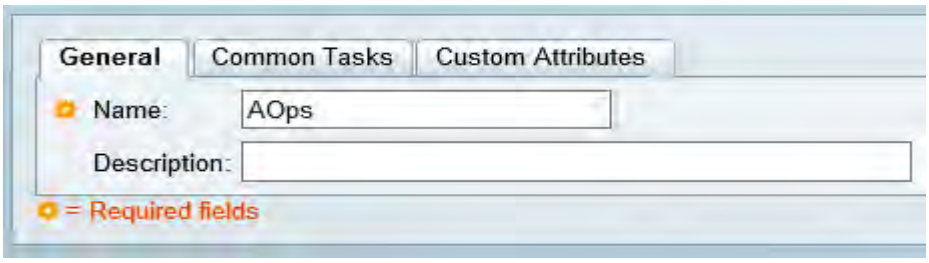


Step 6: Now add the authorization rule. Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.

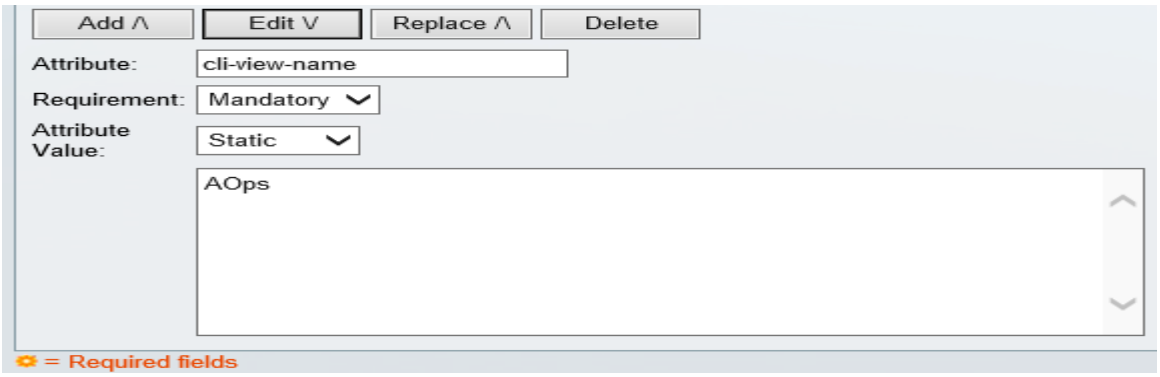


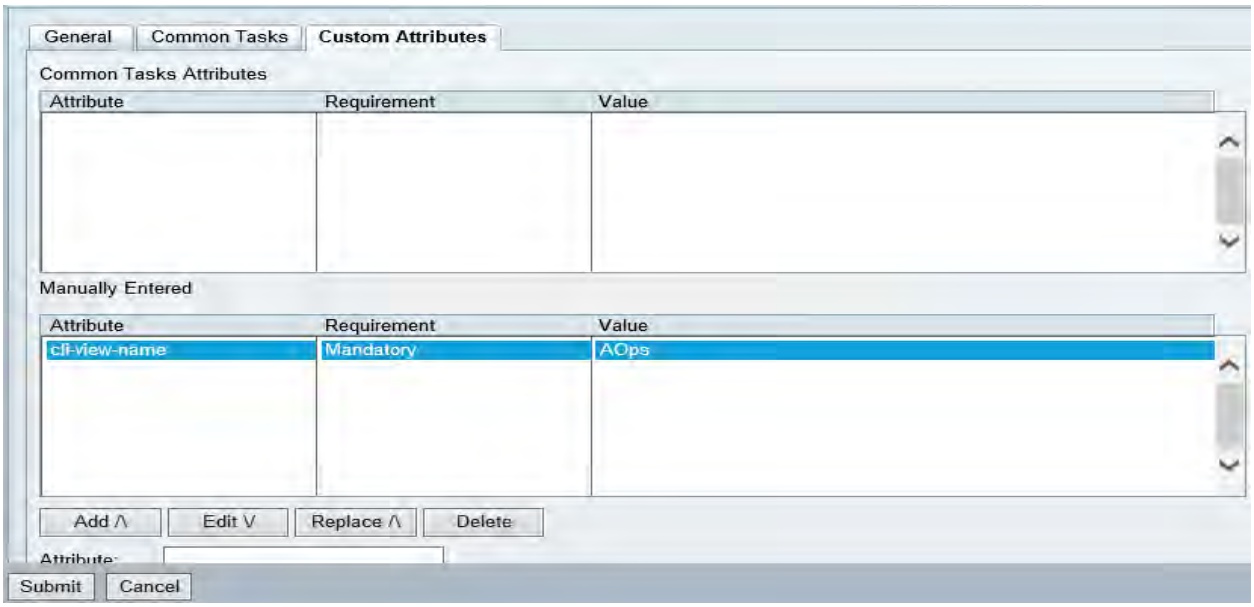
(Create policies for AOps user)

Step 1: Configure a shell profile called "AOps". Go to **Policy Elements -> Authorization and Permissions -> Device Administration -> Shell Profiles**. Click on **Create**.

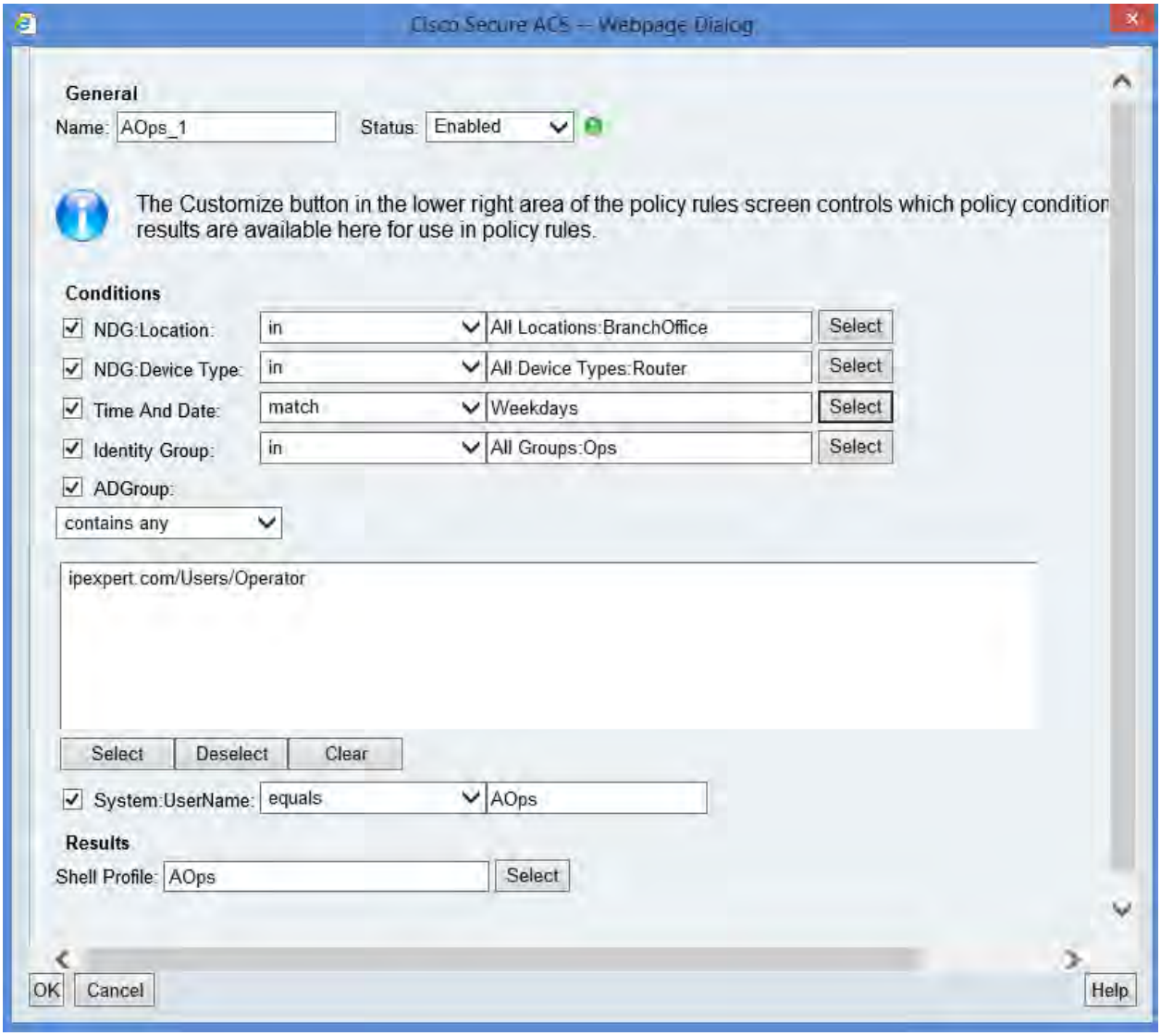


Step 2: Click on Custom Attributes and send the CLI view name of root for NetAdmin.

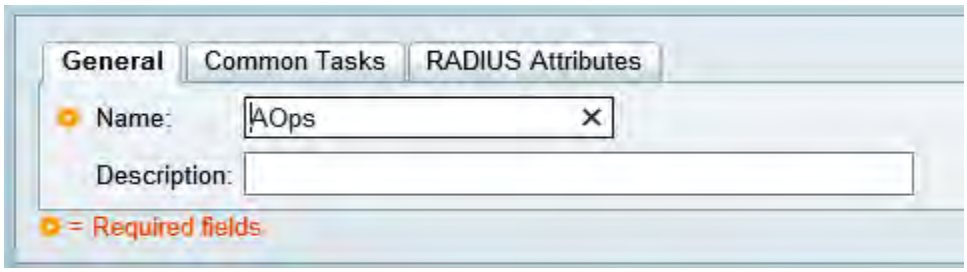




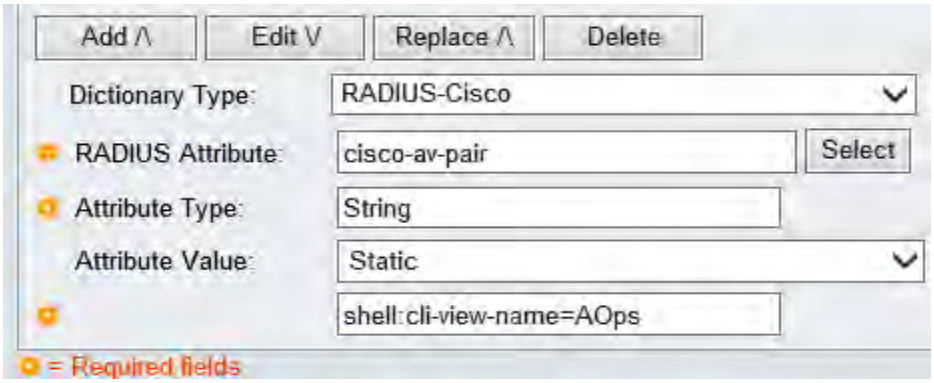
Step 3: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization.** Click on **Create**.

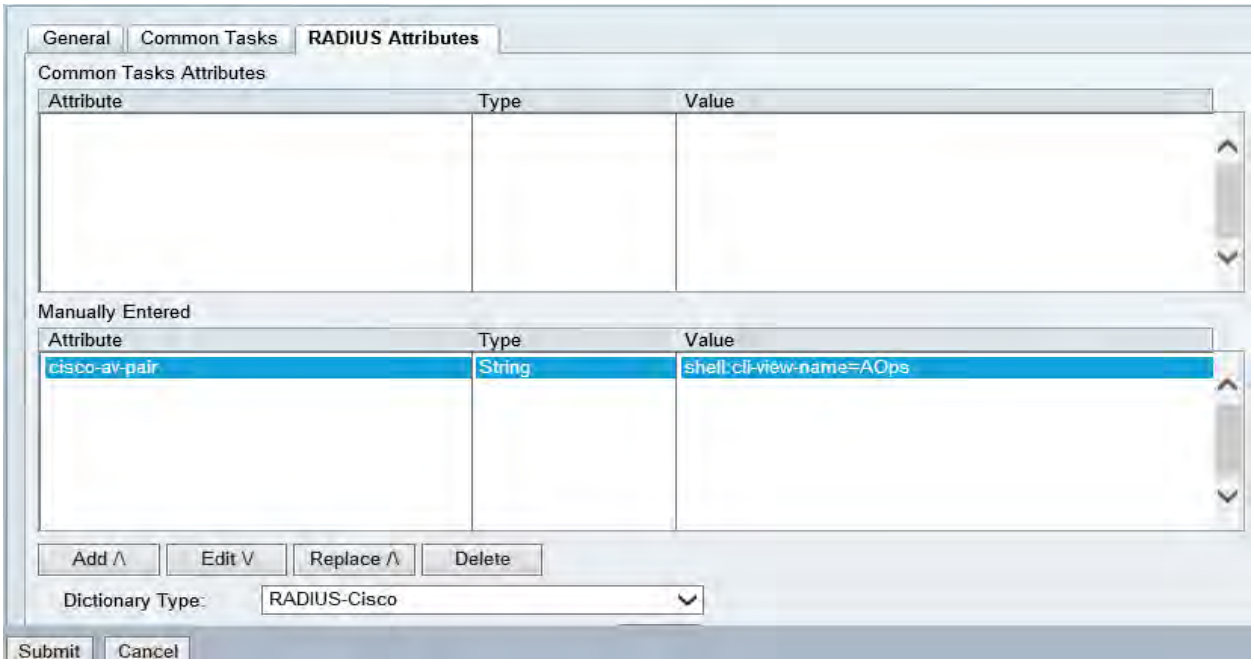


Step 4: Now add the authorization rule. Go to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click on **Create**. Name the shell profile as "AOps".

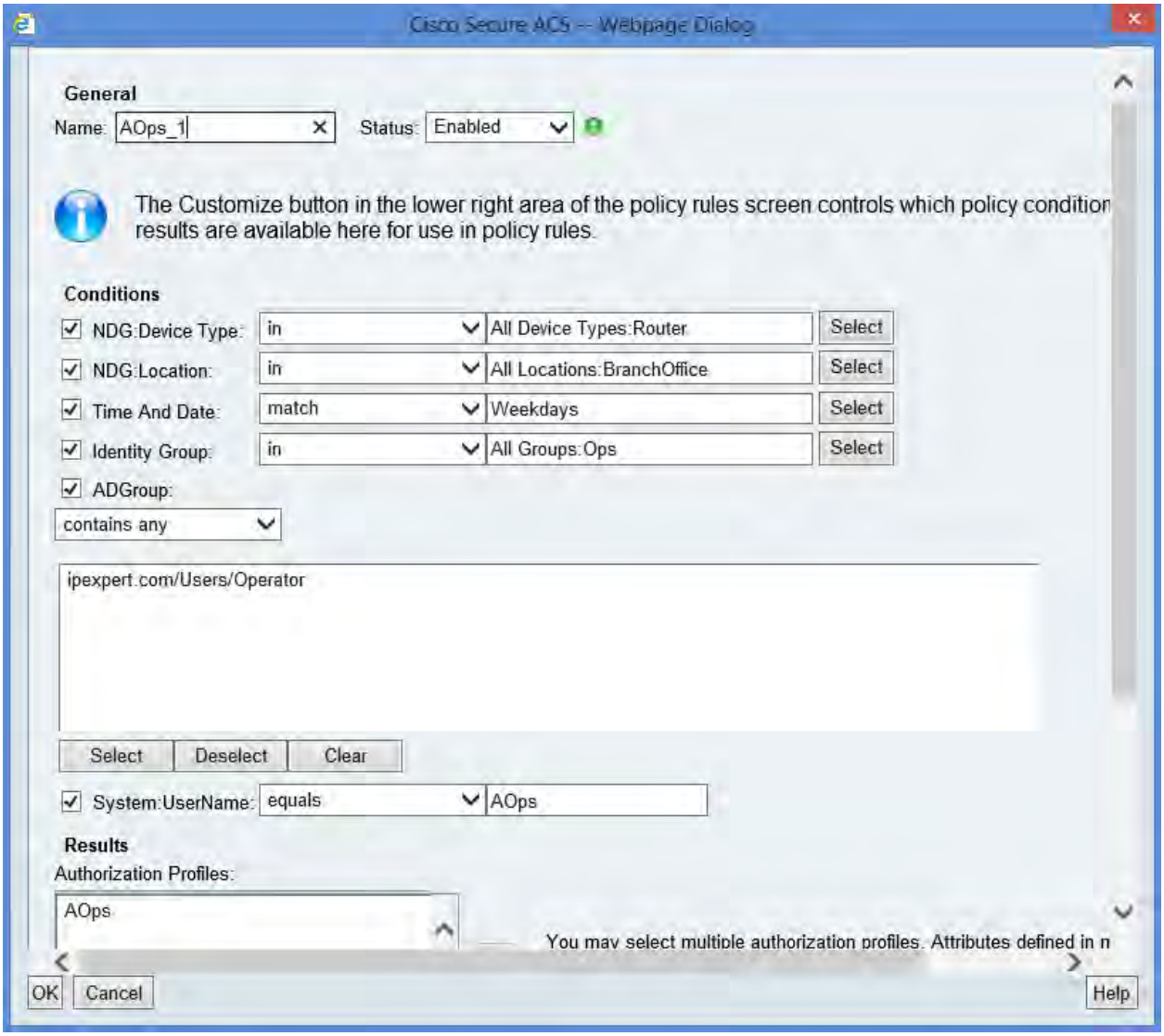


Step 5: Click on **RADIUS Attributes** tab and configure the Cisco AV pair to send the view name.





Step 6: Now add the authorization rule. Go to **Access Policies -> Access Services -> RADIUS Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.



Verification

Telnet or SSH from CAT4 to ASA3, R1, R4, R5 using various usernames created earlier.

```
SW4#ssh -l NetAdmin 172.16.2.10
Password:
Type help or '?' for a list of available commands.
ASA3> en
Password: ***** (cisco)
ASA3# show ssh sessions

SID  Client  IP              Version  Mode  Encryption  Hmac          State
Username
```

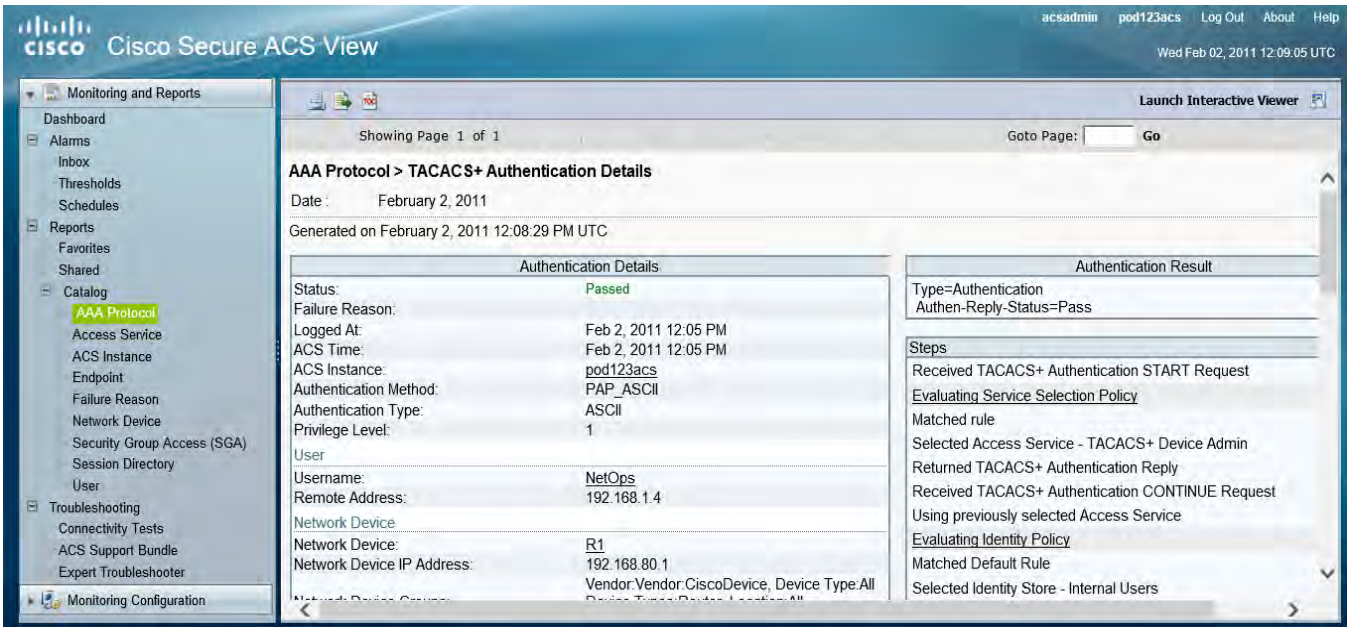
```
0     192.168.1.4        2.0        IN     aes128-cbc  sha1        SessionStarted
NetAdmin
                                OUT     aes128-cbc   sha1           SessionStarted
NetAdmin
```


```
SW4#telnet 192.168.1.10
Trying 192.168.1.10 ... Open

Enter your User-ID: NetAdmin
Enter your Password:

R1#show privilege
Currently in View Context with view 'root'
```

(Note – Since the Shell profile contain "cli-view-name=root" for NetAdmin, root view assignment takes precedence over privilege levels and the privilege level 15 is not assigned. Root view is one of the pre-configured views on the routers)

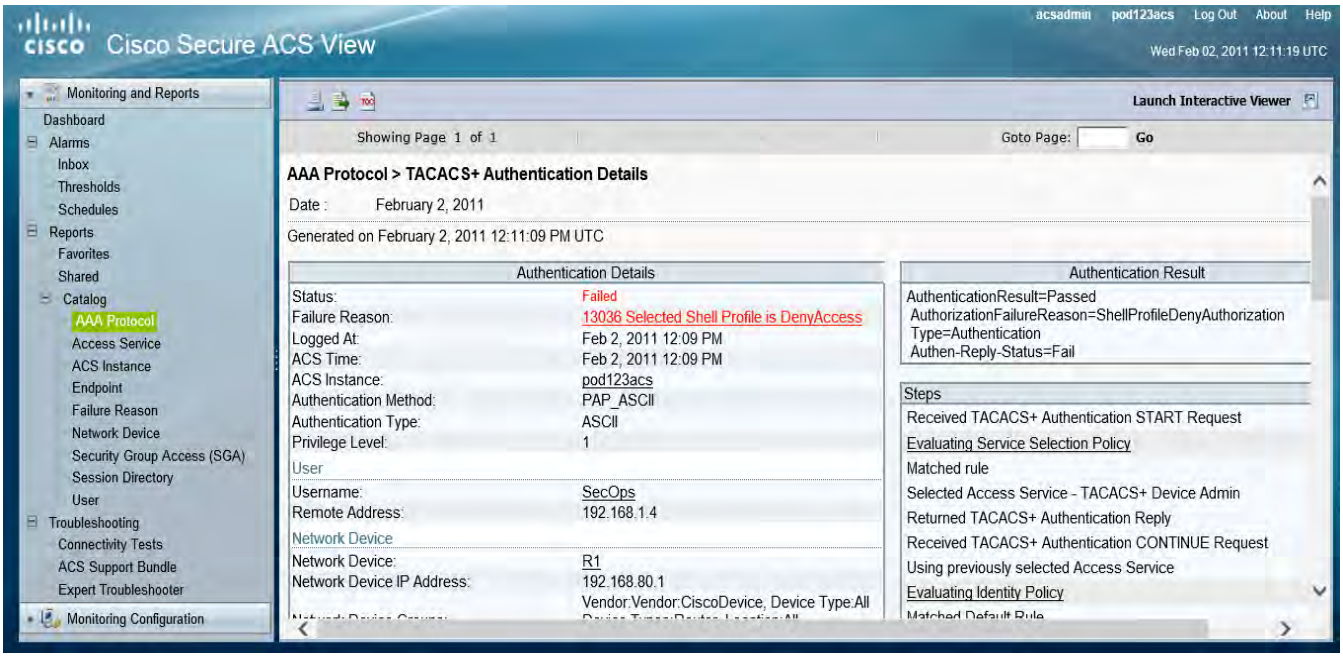
```
SW4#telnet 192.168.1.10
Trying 192.168.1.10 ... Open

Enter your User-ID: NetOps
Enter your Password:

R1>show privilege
Current privilege level is 1
R1>
```

(Note – Since the Shell profile contain "cli-view-name=NetOps" for NetOps, privilege level assignment takes precedence over view assignment because R1 does not have "NetOps" view configured.)

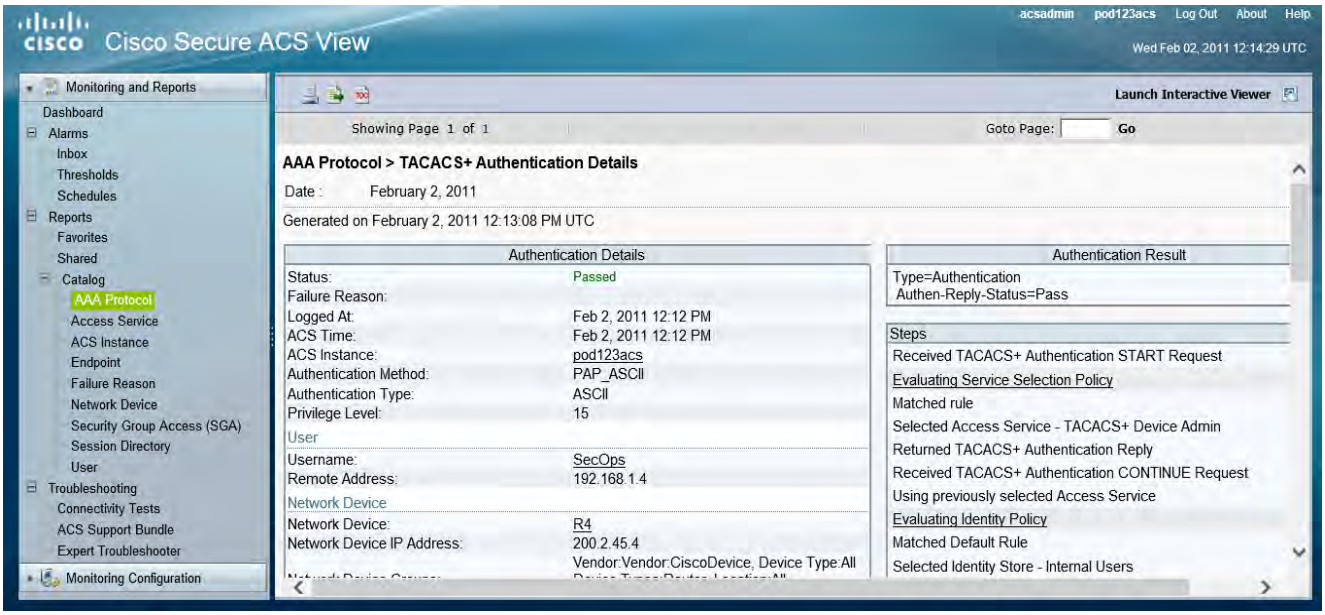



```
SW4#telnet 192.168.1.10
Trying 192.168.1.10 ... Open

Enter your User-ID: SecOps
Enter your Password:

% Authentication failed
```

(Note – SecOps can only login into branch routers)

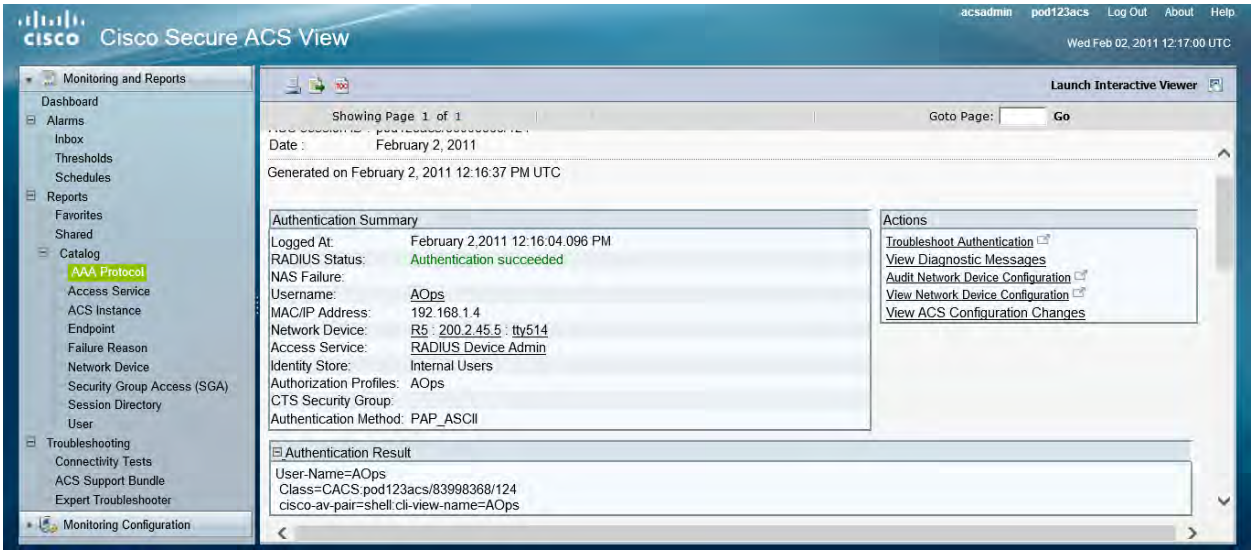



```
SW4#telnet 200.2.45.4
Trying 200.2.45.4 ... Open

Enter your User-ID: SecOps
Enter your Password:

R4#show parser view
Current view is 'SecOps'
R4#
```



Access Policy	
Access Service:	TACACS+ Device Admin
Identity Store:	Internal Users
Selected Shell Profile:	SecOps
Active Directory Domain:	ipexpert.com
Identity Group:	All Groups:Ops
Access Service Selection Matched Rule :	Rule-2
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users, Internal Users
Query Identity Stores:	AD1
Selected Query Identity Stores:	AD1
Group Mapping Policy Matched Rule:	
Authorization Policy Matched Rule:	SecOps_1
Authorization Exception Policy Matched Rule:	

```
SW4#telnet 200.2.45.5
Trying 200.2.45.5 ... Open


User Access Verification

Enter your User-ID:AOps
Enter your Password:

R5#show parser view
Current view is 'Aops'
R5#
```



Lab-3: Configuring AAA clients for command authorization and accounting

Lab-3: Configuring AAA clients for command authorization and accounting – This lab is intended to familiarize you with configuring AAA clients for command authorization using the ACS and EXEC/command accounting.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 3 Hours

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-2 successfully.

Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure R1 and R2 for command authorization.

- Configure R1 and R2 for command authorization for all commands when a user connects via telnet or SSH. Configure appropriate fallback policy.

Solutions

R1 & R2

```
aaa authorization commands 0 UseAAA group tacacs+ local
aaa authorization commands 1 UseAAA group tacacs+ local
aaa authorization commands 7 UseAAA group tacacs+ local
aaa authorization commands 15 UseAAA group tacacs+ local
aaa authorization config-commands

line vty 0 4
 authorization commands 0 UseAAA
 authorization commands 1 UseAAA
 authorization commands 7 UseAAA
 authorization commands 15 UseAAA
```

- Configure such that only privilege level 15 commands should to be authorized for HTTP sessions using the ACS on R1 and R2.

Solutions

R1 & R2

```
ip http authentication aaa command-authorization 15 UseAAA
```

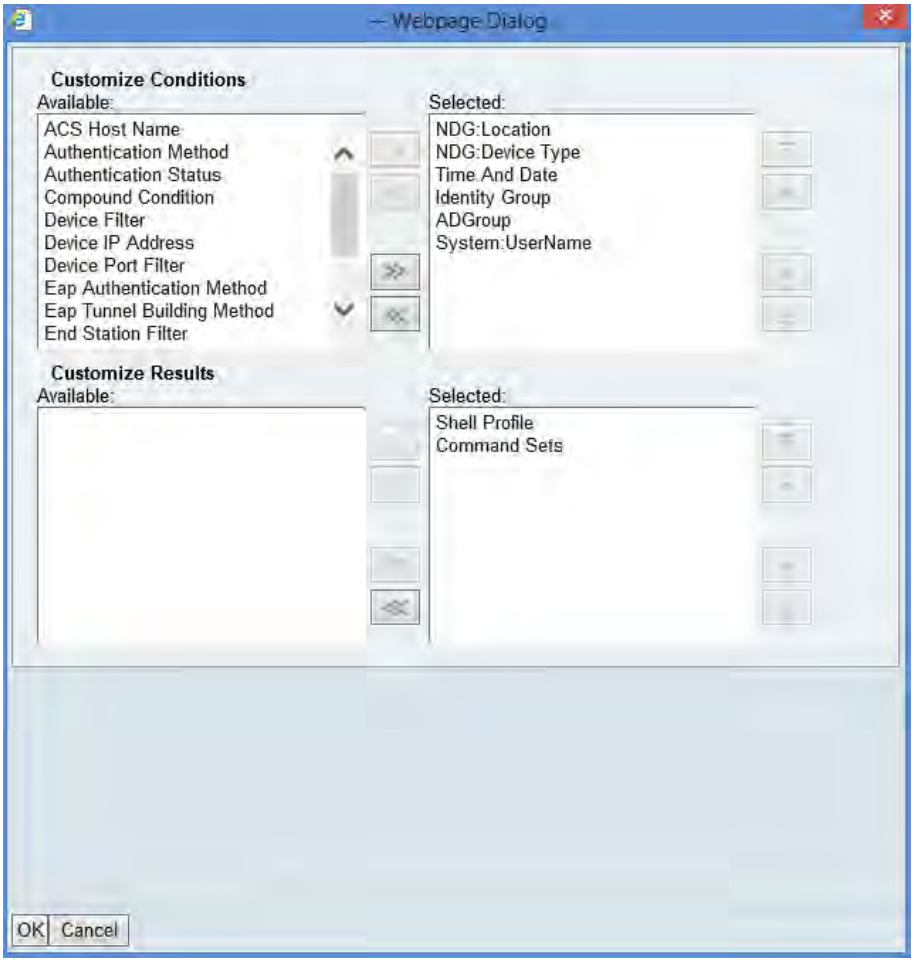
Task 2: Configure ACS for command authorization.

- Add a Command Sets as additional result in the TACACS+ Device Admin access policy in the authorization rules.

Solutions

ACS

Step 1: Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Customize** button and add Command Sets as an additional result.

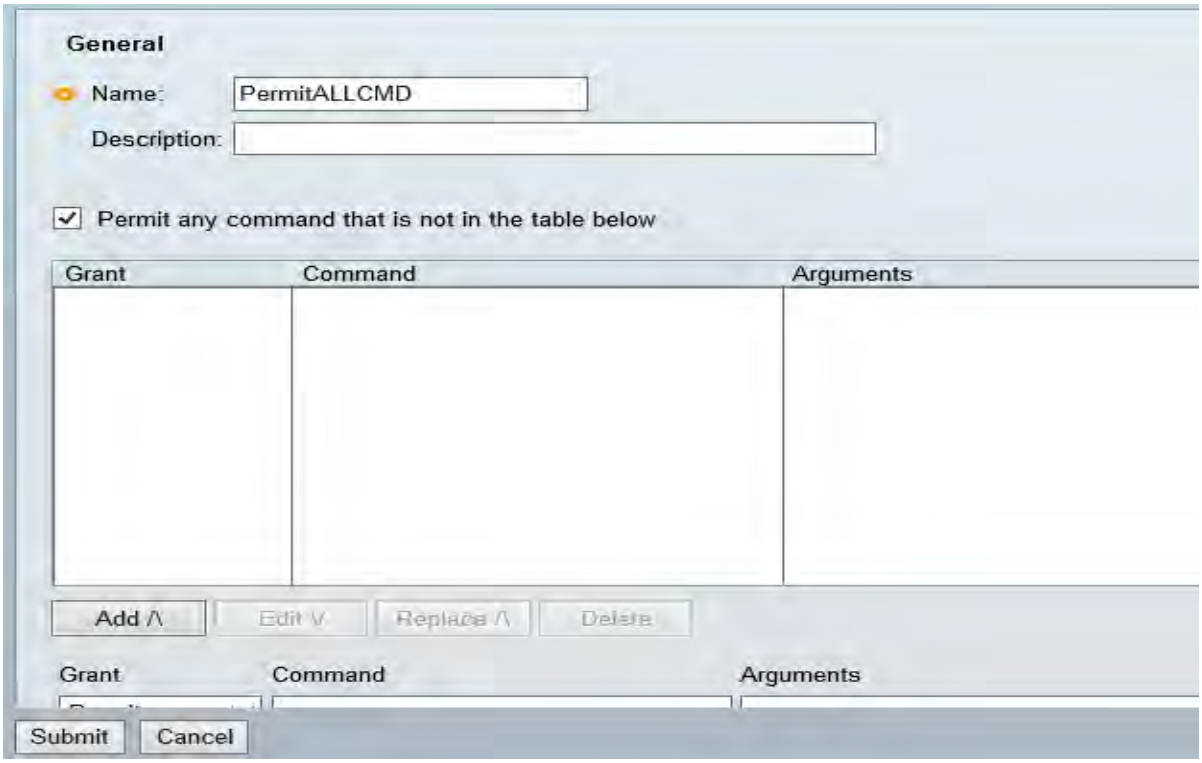


- Configure a command set call “PermitALLCMD” and permit all the commands for Radmin1 user. You are allowed to modify or change the authorization rules.

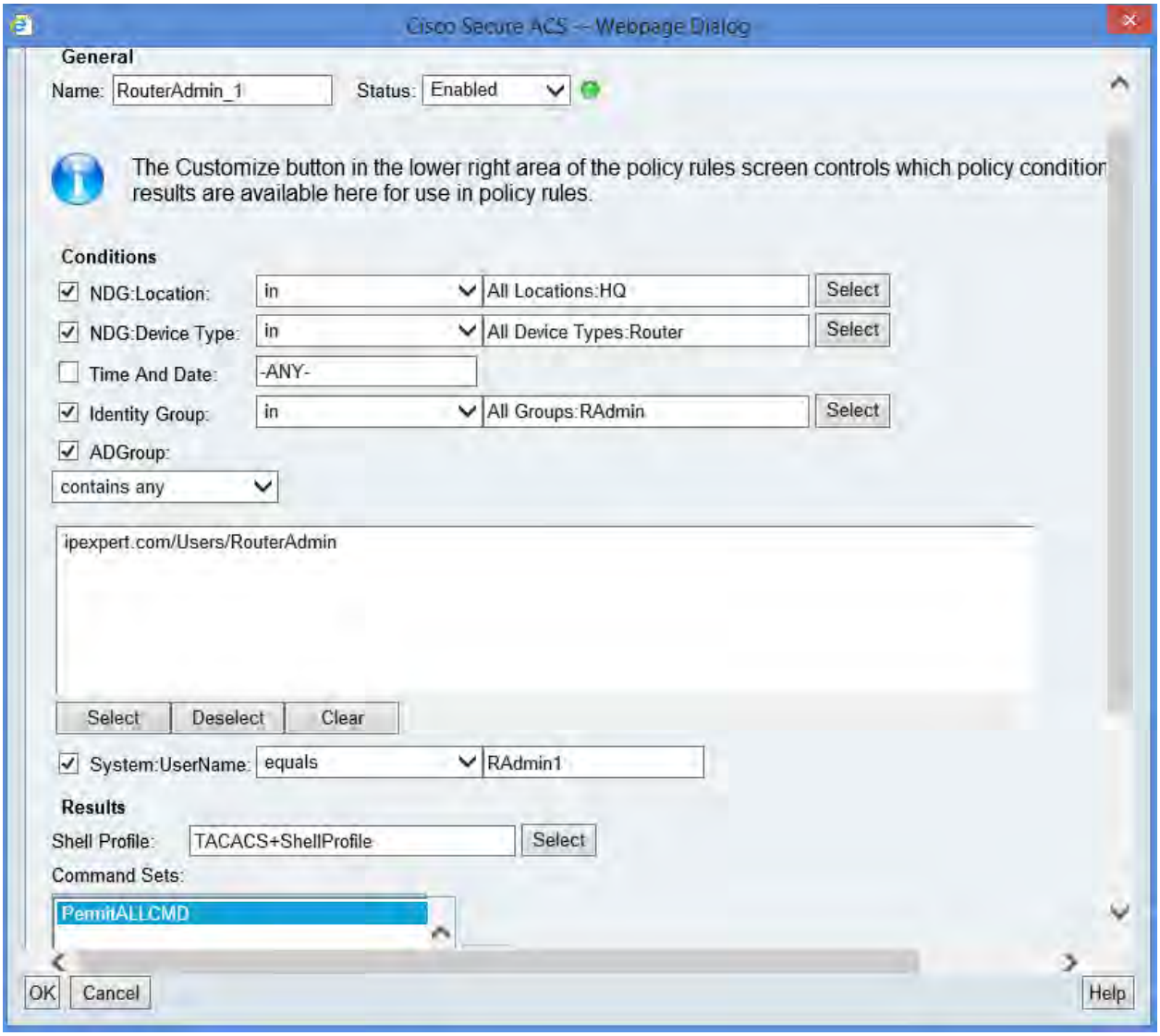
Solutions

ACS

Step 1: Go to **Policy Elements ->Authorization and Permissions ->Device Administration ->Command Sets**. Then click on **Create**.



Step 2: Modify the authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **RouterAdmin_1** rule**.** Then click on Save Changes.



- Configure a command set called “Priv7CMD” and permit commands given in the below table for Radmin2 user. Create additional authorization rule for this.

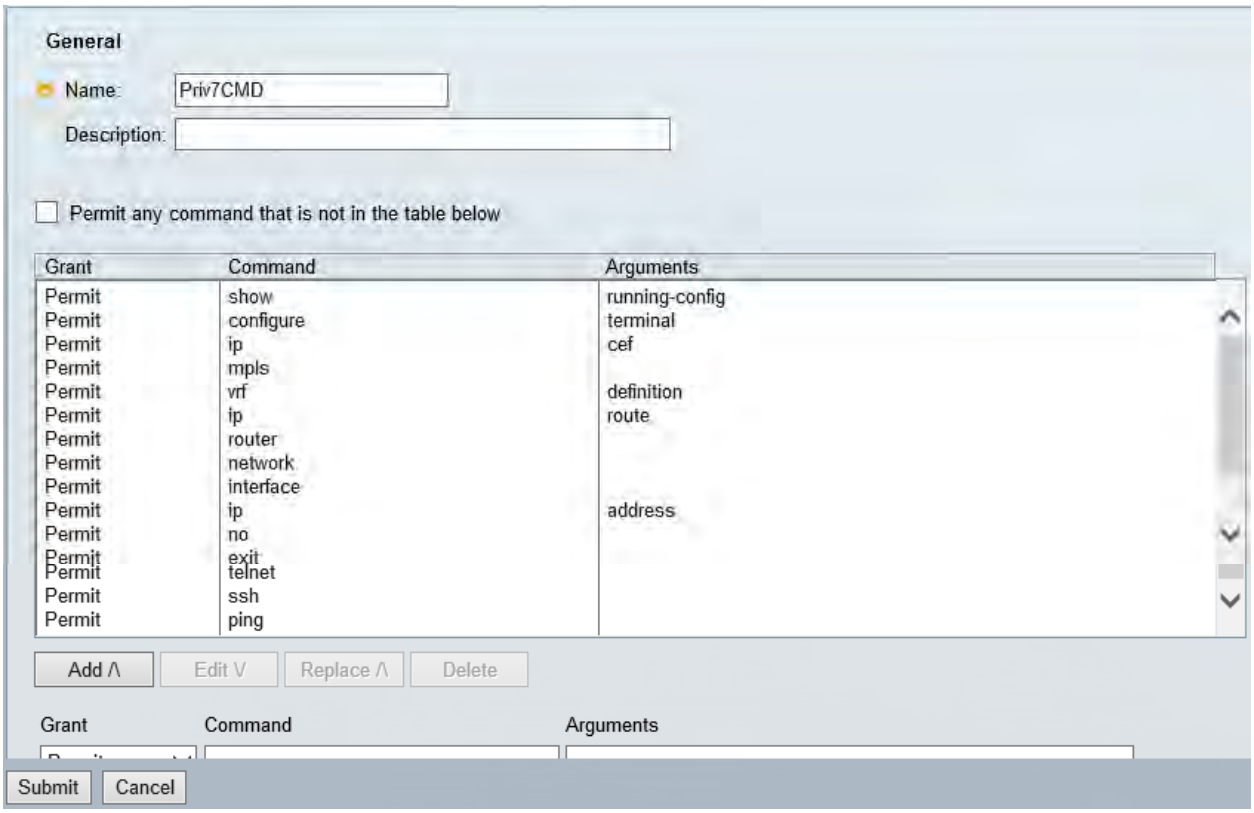
Command	Argument
show	running-config
configure	terminal
ip	cef
mpls	(ANY)
vrf	definition
ip	route
router	(ANY)
network	(ANY)
interface	(ANY)

ip	address
no	(ANY)
exit	(ANY)
ping	(ANY)
telnet	(ANY)
ssh	(ANY)

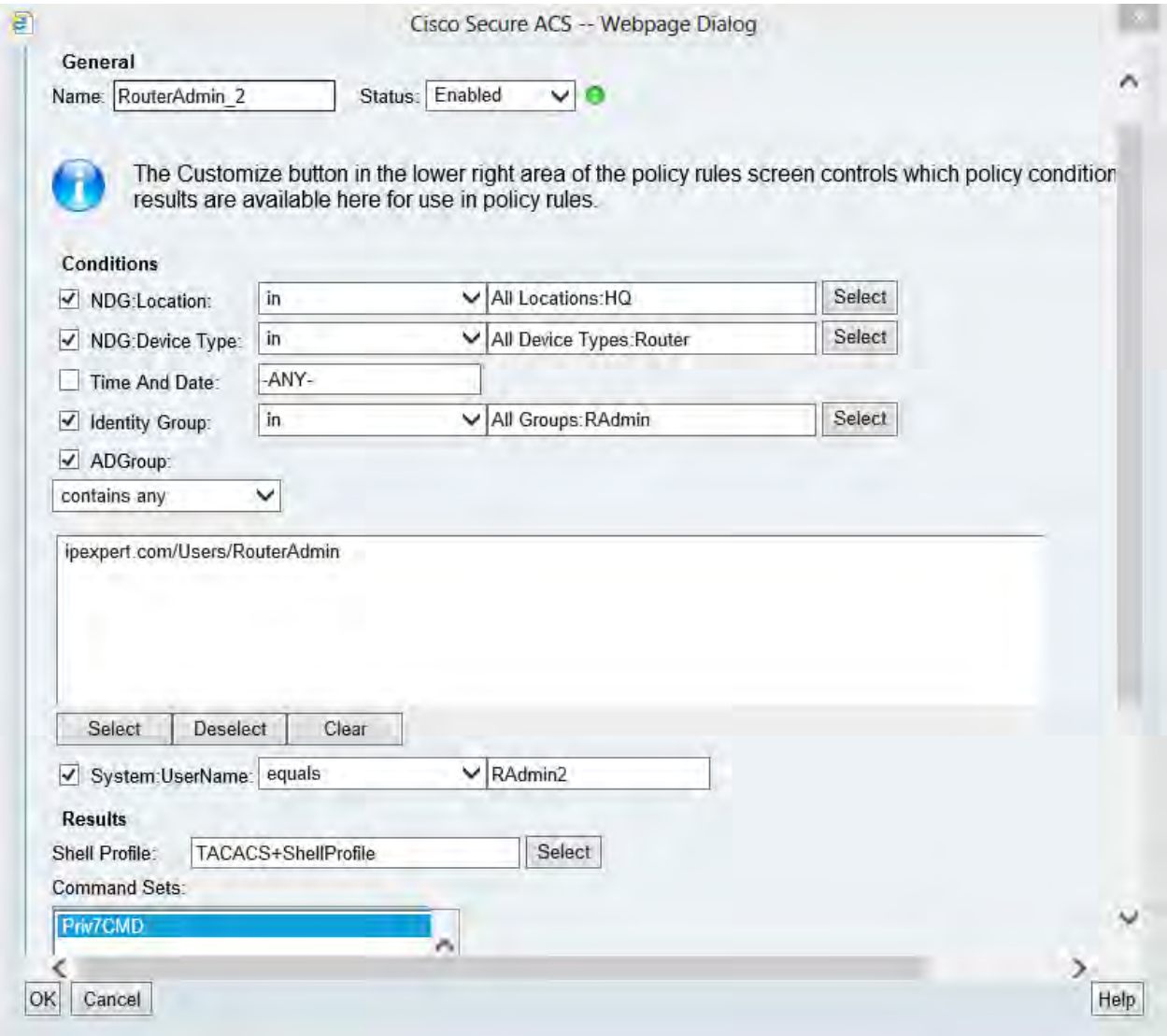
Solutions

ACS

Step 1: Go to **Policy Elements ->Authorization and Permissions ->Device Administration ->Command Sets**. Then click on **Create**.



Step 2: Create a new authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.

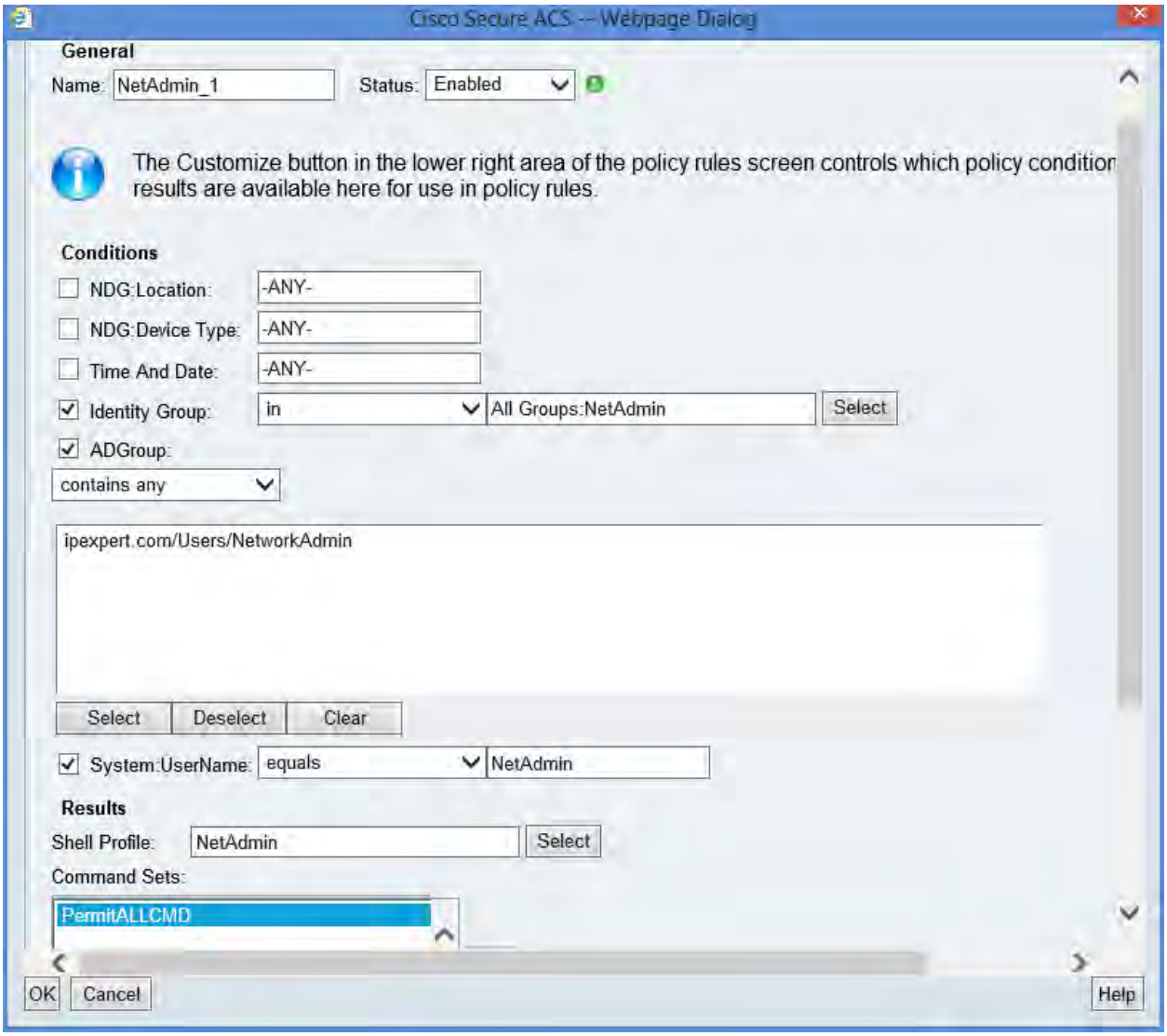


- NetAdmin user should be assigned “PermitALLCMD” command set.

Solutions

ACS

Step 1: Modify the authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **NetAdmin_1** rule**.** Then click on Save Changes.

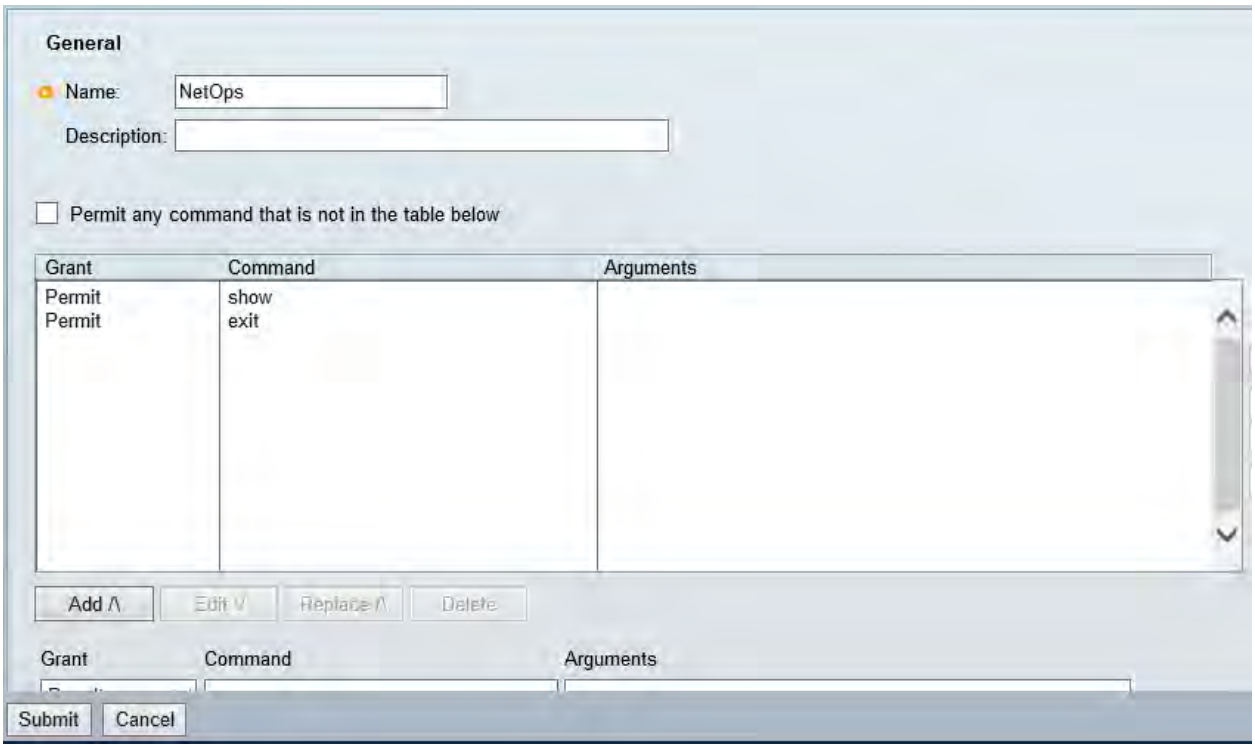


- NetOps user should able to view only basic show commands available at privilege level 1 and be able to exit/log-off. You are allowed to create a new command set to accomplish this and modify existing authorization rule. You may also need to make some additional configuration change on R1 and R2 for NetOps user to execute show commands.

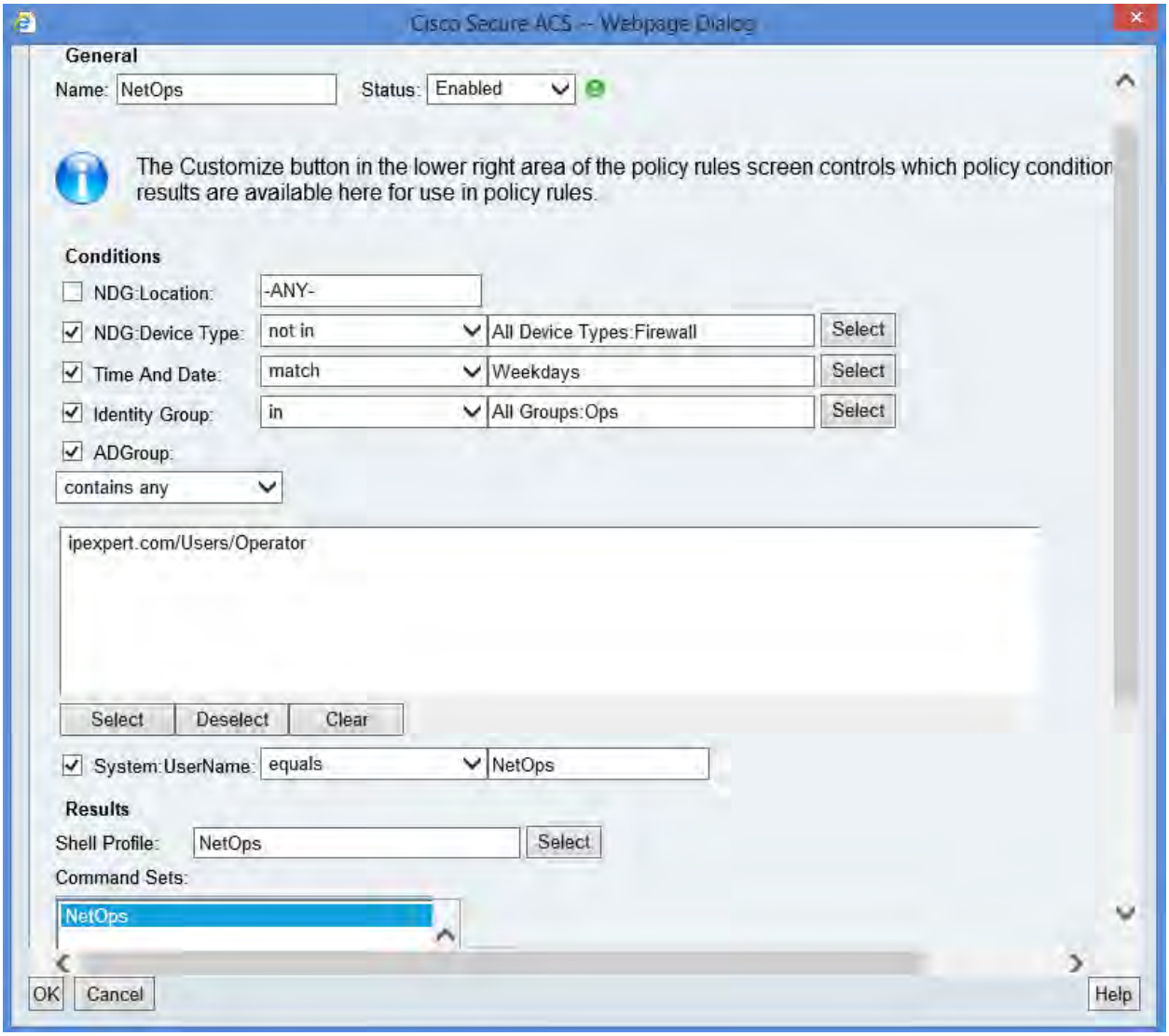
Solutions

ACS

Step 1: Go to **Policy Elements ->Authorization and Permissions ->Device Administration ->Command Sets**. Then click on **Create**.



Step 2: Modify the authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **NetOps** rule**.** Then click on Save Changes.



Step 3: Configuire R1 and R2 to change the privilege level for show command to privilege level 1

```
privilege exec level 1 show
```

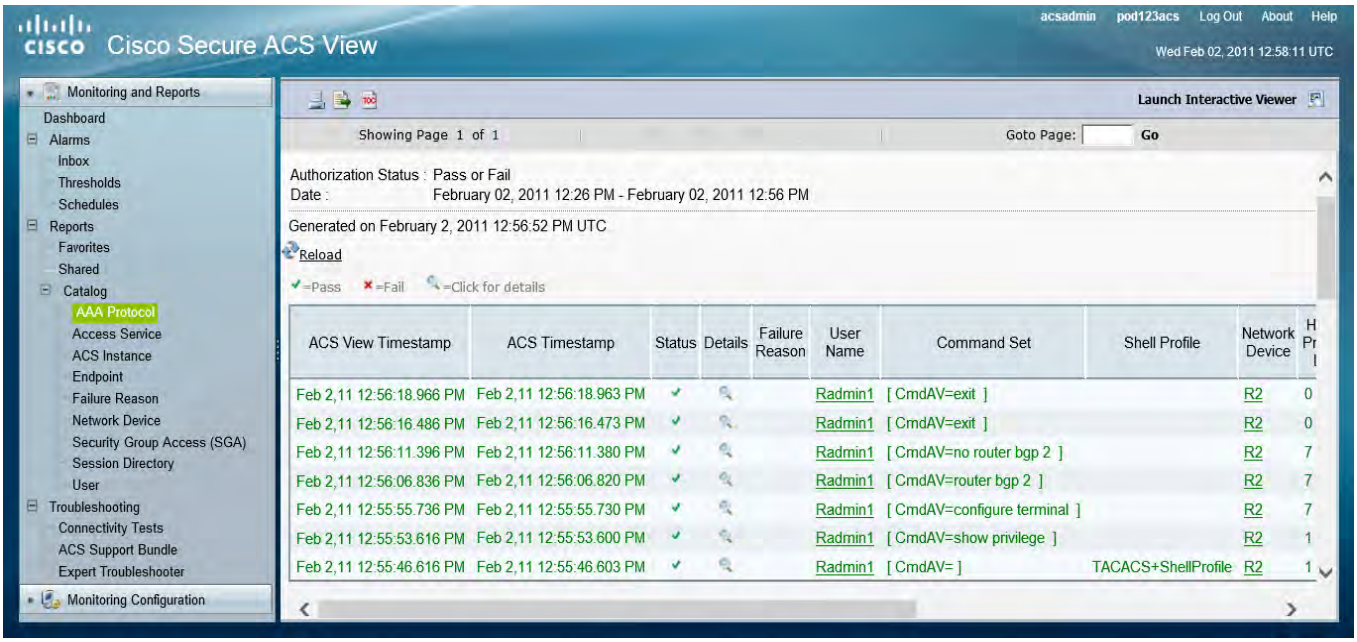
Verification

Test command authorization by logging into R1 or R2 as Radmin1 (Full access), Radmin2 (Restricted command access based on command sets) and NetOps user (Show commands only).

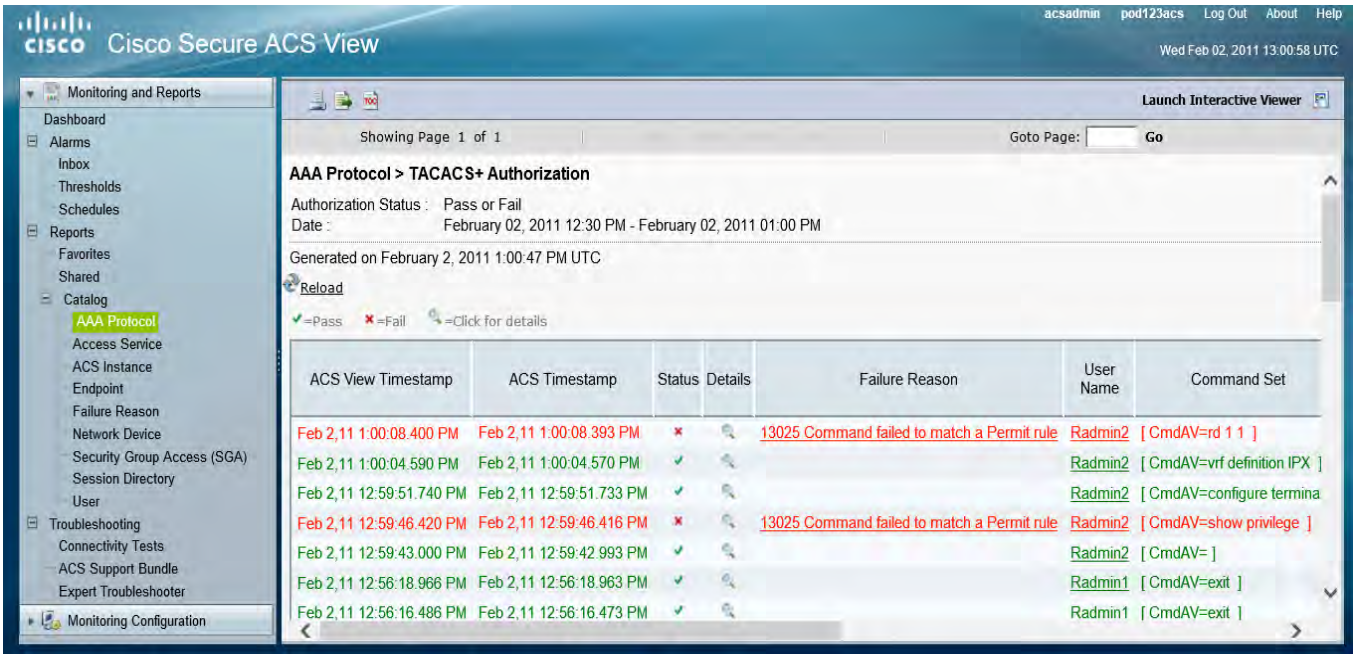
```
SW4#telnet 192.168.80.2
Trying 192.168.80.2 ... Open

Enter your User-ID: Radmin1
Enter your Password:
```

```
R2#show privilege
Current privilege level is 15
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#no router bgp 2
R2(config)#exit
R2#exit

[Connection to 192.168.80.2 closed by foreign host]
```

Go to Monitoring and Reports and click on Launch Report viewer. Then browse to Catalog->AAA Protocol ->TACACS+ Authorization.

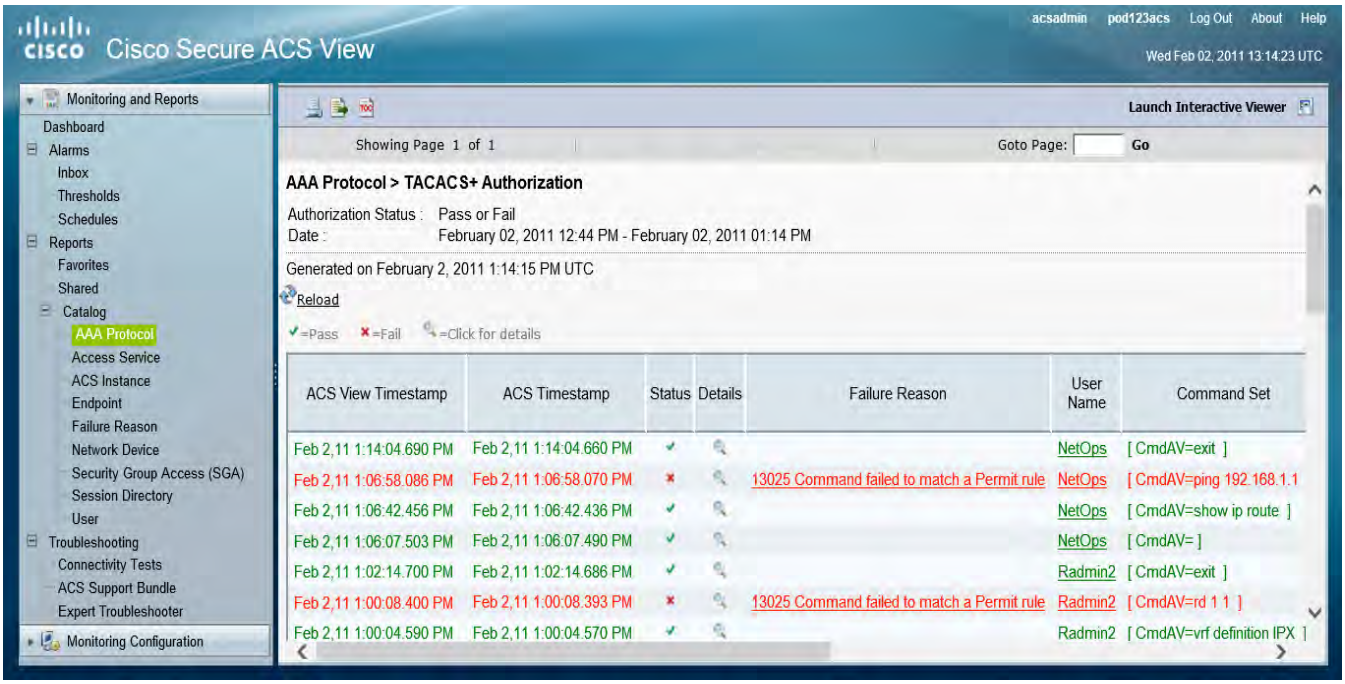



```
SW4#telnet 192.168.80.2
Trying 192.168.80.2 ... Open

Enter your User-ID: Radmin2
Enter your Password:

R2#show privilege
Command authorization failed.

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#vrf definition IPX
R2(config-vrf)#rd 1:1
Command authorization failed.

R2(config-vrf)#
```




```
SW4#telnet 192.168.80.2
Trying 192.168.80.2 ... Open

Enter your User-ID: NetOps
Enter your Password:

R2>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 192.168.80.1, 00:10:29, GigabitEthernet0/0.80
     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/12] via 172.16.2.10, 00:10:29, GigabitEthernet0/0.172
     20.0.0.0/24 is subnetted, 1 subnets
O       20.5.5.0 [110/12] via 172.16.2.10, 00:10:29, GigabitEthernet0/0.172
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/12] via 172.16.2.10, 00:10:29, GigabitEthernet0/0.172
     172.16.0.0/24 is subnetted, 1 subnets
```

```
C       172.16.2.0 is directly connected, GigabitEthernet0/0.172
C    192.168.80.0/24 is directly connected, GigabitEthernet0/0.80
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, GigabitEthernet0/1
S       10.0.0.0/8 [1/0] via 10.1.1.150
S       10.200.5.0/24 [1/0] via 10.1.1.150
O    200.2.45.0/24 [110/11] via 172.16.2.10, 00:10:29, GigabitEthernet0/0.172
O    192.168.1.0/24 [110/2] via 192.168.80.1, 00:10:29, GigabitEthernet0/0.80

R2>ping 192.168.1.1
Command authorization failed.
R2>exit

[Connection to 192.168.80.2 closed by foreign host]
```



Task 3: Configure ASA and ACS for command authorization.

- Configure command authorization on the ACS. Before you configure this, make sure you SSH into ACS as FWadmin user.

Solutions

ASA3 (SSH from CAT4 as FWadmin before configuring this command else login into console as FWadmin, else you will lock yourself)

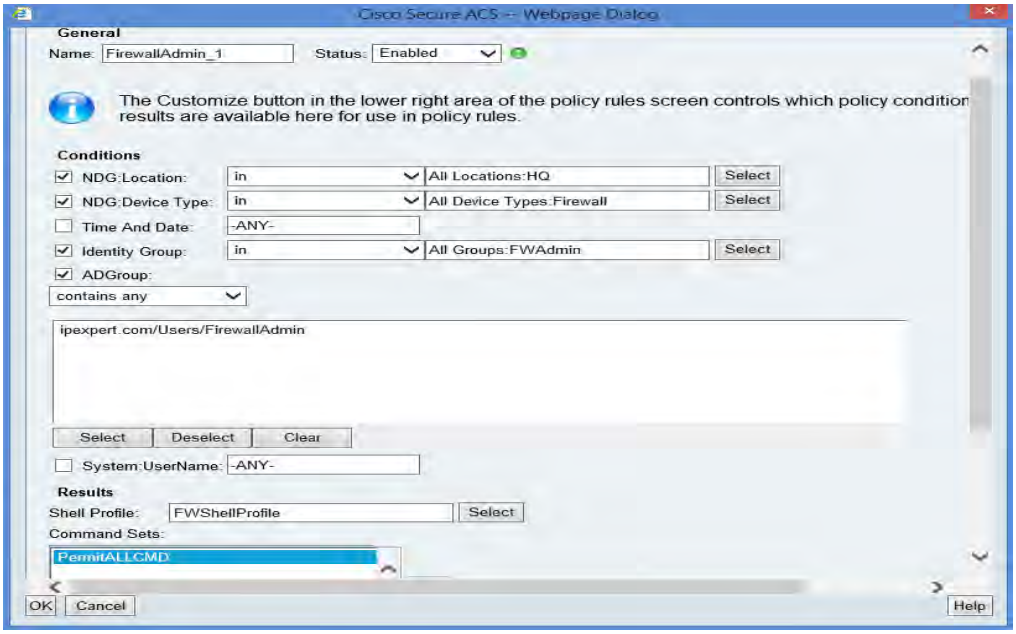
```
aaa authorization command TACACS LOCAL
```

- Modify or change existing authorization rule such that FWadmin user can get complete access to the ASA.

Solutions

ACS

Step 1: Modify the authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **FirewallAdmin_1** rule**.** Then click on Save Changes.

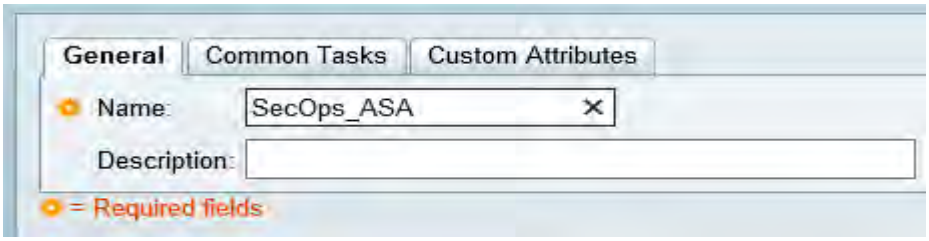


- Configure additional authorization rule such that SecOps is allowed to execute all commands except reload. You are allowed to create new shell profile and command set. The authorization profile should have NDG's (Location and Device Type), identity group, AD group and username as conditions. Do not enforce date and time condition for this rule.

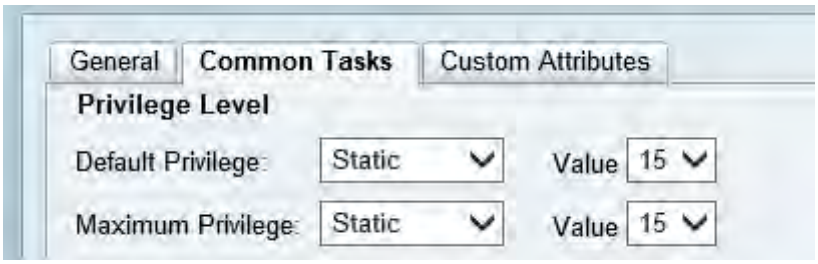
Solutions

ACS

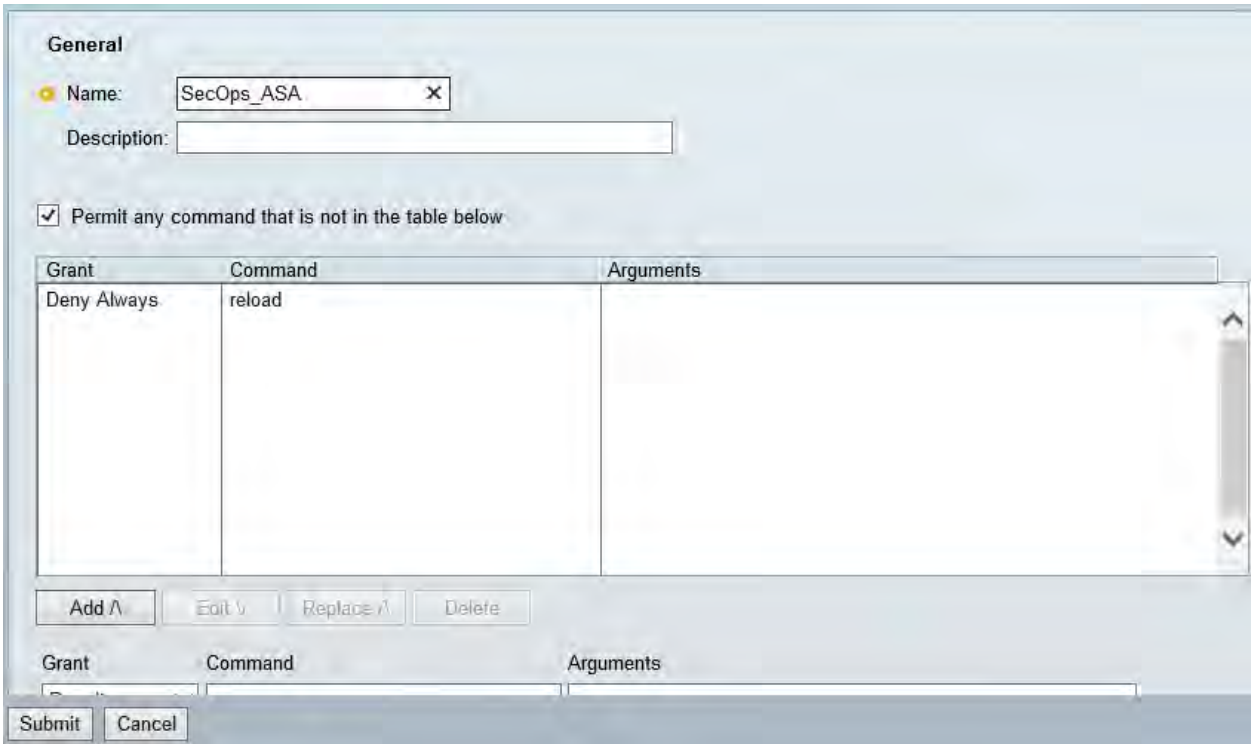
Step 1: Go to **Policy Elements -> Authorization and Permissions -> Network Access -> Authorization Profiles** and click on **Create**. Name the shell profile as "UserShell".



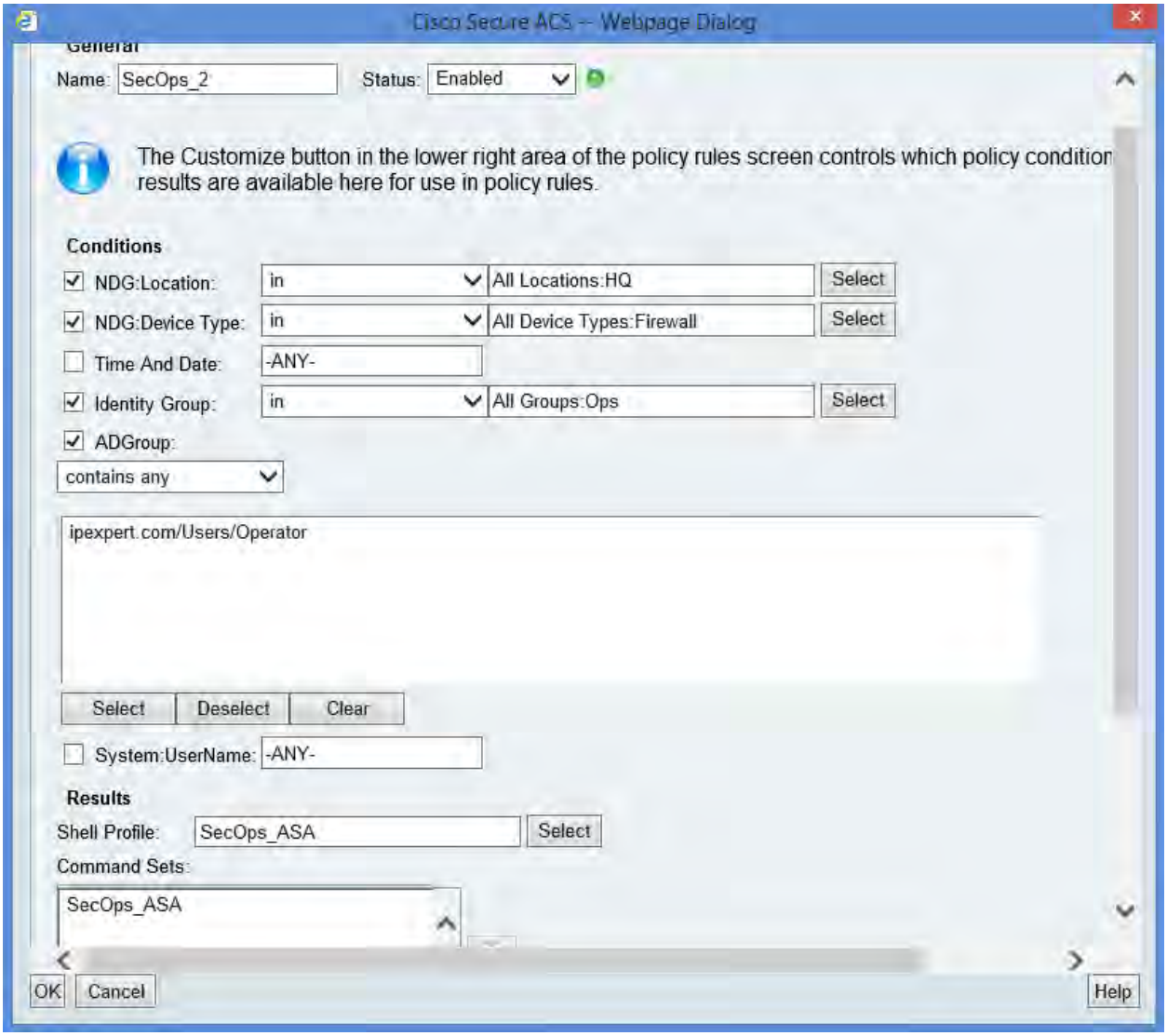
Step 2: Click on **Common Tasks** tab and configure the value for the privilege level.



Step 3: Go to **Policy Elements ->Authorization and Permissions ->Device Administration ->Command Sets**. Then click on **Create**.



Step 5: Now add the authorization rule. Go to **Access Policies -> Access Services -> TACACS+ Device Admin -> Authorization**. Click on **Add.** Then click on Save Changes.



Step 6: Configure an enable password of "cisco" for SecOps user. Go to **Users and Identity Stores -> Internal Identity Stores -> Users**. Click on SecOps and then click on change password.

Task 4: Configure EXEC Accounting.

- Configure all devices to log telnet/SSH sessions to the ACS.

Solutions

R1, R2 and R4

```
aaa accounting exec UseAAA start-stop group tacacs+
line vty 0 4
  accounting exec UseAAA
```

R5

```
aaa accounting exec UseAAA start-stop group radius
line vty 0 4
  accounting exec UseAAA
```

Switches

```
aaa accounting exec UseAAA start-stop group radius
line vty 0 15
  accounting exec UseAAA
```

Task 5: Configure R1 and R2 for command Accounting.

- Configure R1 and R2 for accounting all command executed by the user when they have logged in through telnet or SSH.
- Account only privilege level 15 commands when executed through HTTP on R1 and R2.
- Configure command account on the ASA.

Solutions

R1 & R2

```
aaa accounting commands 0 UseAAA start-stop group tacacs+
aaa accounting commands 1 UseAAA start-stop group tacacs+
aaa accounting commands 7 UseAAA start-stop group tacacs+
aaa accounting commands 15 UseAAA start-stop group tacacs+

line vty 0 4
 accounting commands 0 UseAAA
 accounting commands 1 UseAAA
 accounting commands 7 UseAAA
 accounting commands 15 UseAAA

ip http accounting commands 15 UseAAA
```

Task 6: AAA configuration removal on ASA

- Remove any existing AAA configs on ASA3. Execute “clear config aaa” and save the configs.

Solutions

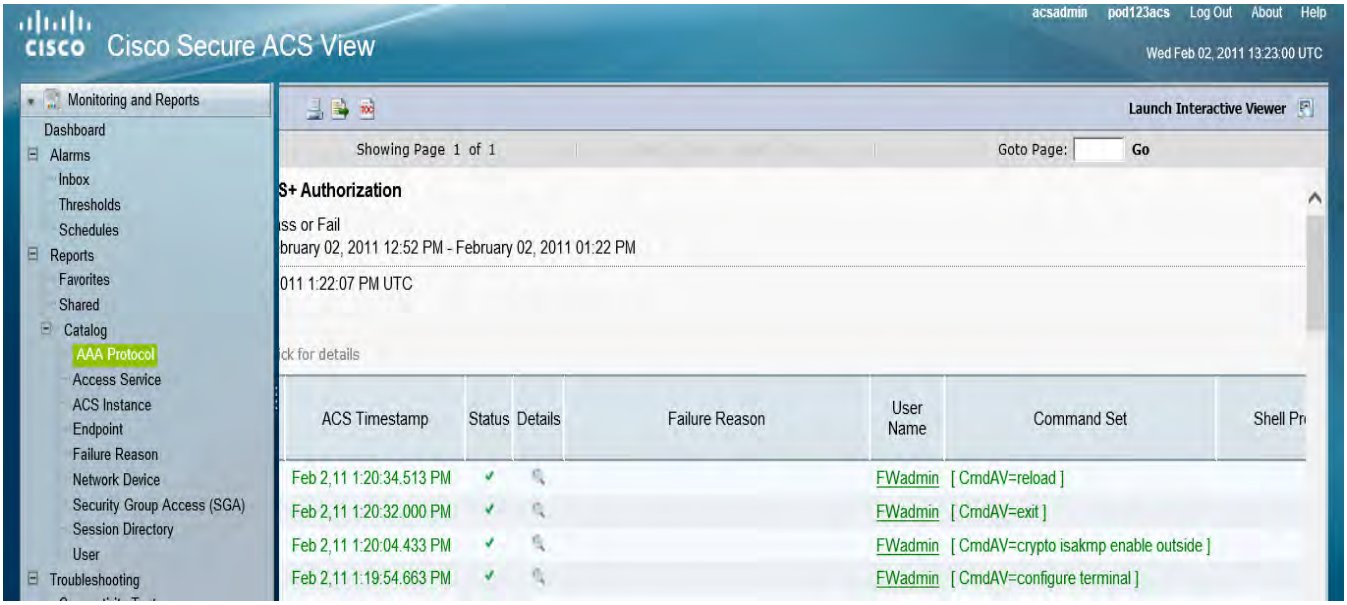
ASA3

```
clear config aaa

write memory
```

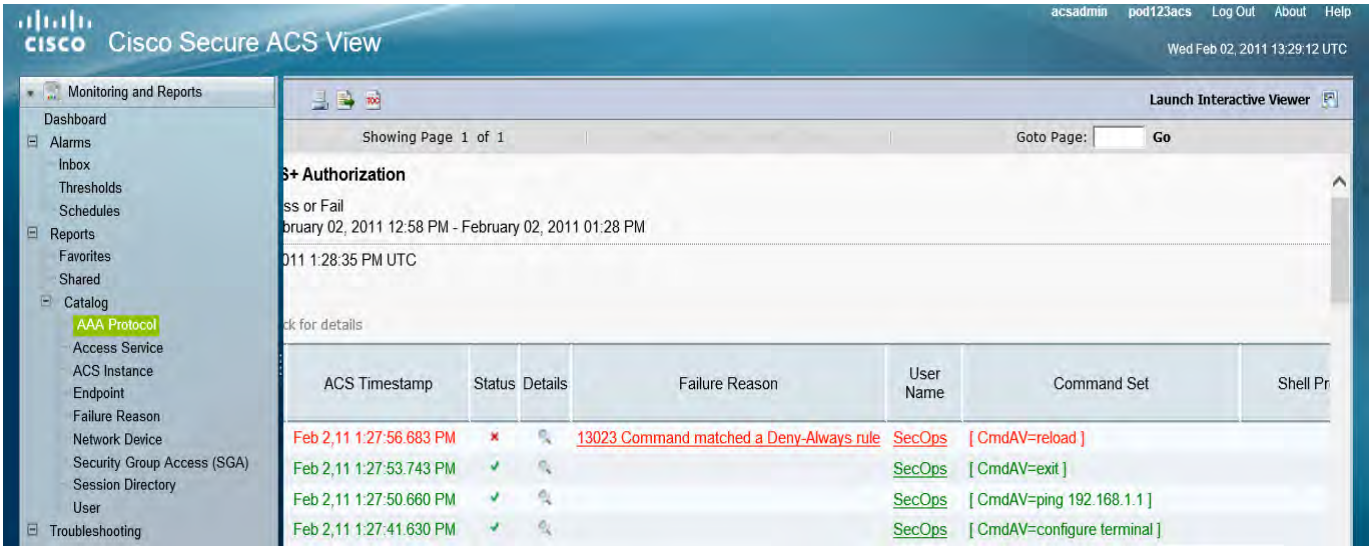
Verification

Test command authorization by logging into ASA3 as FWadmin (Full access) and SecOps (full access except reload command)

```
User Access Verification

Username: FWadmin
Password: *****
Type help or '?' for a list of available commands.
ASA3> en
Password: ********
Password: *****
ASA3# conf t
ASA3(config)# crypto isakmp enable outside
ASA3(config)#
ASA3(config)# exit
ASA3# reload

Logoff
[Connection to 172.16.2.10 closed by foreign host]
```




```
User Access Verification

Username: SecOps
Password: *****
Type help or '?' for a list of available commands.
ASA3> en
Password: *****
ASA3# conf t
ASA3(config)# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA3(config)# exit
ASA3# reload
Command authorization failed
ASA3#
```



Lab-4: Configuring Authentication proxy and cut-through proxy

Lab-4: Configuring Authentication proxy and cut-through proxy– This lab is intended to familiarize you with the configuration of IOS Authentication Proxy and ASA's Cut through proxy to implement AAA network access.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: 2 Hours

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully. Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Remove AAA configuration.

- Remove AAA configurations on R1.

Solutions

R1

```
no aaa authentication login UseAAA group tacacs+ local
no aaa authentication login NO none
no aaa authorization config-commands
no aaa authorization exec UseAAA group tacacs+ local
no aaa authorization commands 0 UseAAA group tacacs+ local
no aaa authorization commands 1 UseAAA group tacacs+ local
no aaa authorization commands 7 UseAAA group tacacs+ local
no aaa authorization commands 15 UseAAA group tacacs+ local
no aaa accounting exec UseAAA start-stop group tacacs+
no aaa accounting commands 0 UseAAA start-stop group tacacs+
no aaa accounting commands 1 UseAAA start-stop group tacacs+
no aaa accounting commands 7 UseAAA start-stop group tacacs+
no aaa accounting commands 15 UseAAA start-stop group tacacs+
no ip http authentication aaa login-authentication UseAAA
no ip http authentication aaa exec-authorization UseAAA
no ip http authentication aaa command-authorization 15 UseAAA
no ip http accounting commands 15 UseAAA

line vty 0 4
 no authorization commands 0 UseAAA
 no authorization commands 1 UseAAA
 no authorization commands 7 UseAAA
 no authorization commands 15 UseAAA
 no authorization exec UseAAA
 no accounting commands 0 UseAAA
 no accounting commands 1 UseAAA
 no accounting commands 7 UseAAA
 no accounting commands 15 UseAAA
 no accounting exec UseAAA
 no login authentication UseAAA

no tacacs-server host 10.1.1.100 key cisco123
```

Task 2: ASA Cut through proxy using RADIUS

- Configure ASA as a RADIUS client.

Solutions

ASA3

```
aaa-server RADACS protocol radius
```

```
aaa-server RADACS (inside) host 10.1.1.100
 key cisco123
```

- Configure ASA for cut-through proxy authentication using dACL's for any inbound HTTP and RDP connections and configure cut-through-proxy accounting.

Solutions

ASA3

```
access-list CP extended permit tcp any host 200.2.45.23 eq telnet
access-list CP extended permit tcp any any eq www
access-list CP extended permit tcp any any eq 3389
aaa authentication match CP outside RADACS
aaa accounting match CP outside RADACS
access-list OUT extended permit tcp any host 200.2.45.23
access-list OUT extended deny tcp any any eq 3389
access-list OUT extended deny tcp any any eq 80
access-group OUT in interface outside per-user-override
```

- Use a virtual telnet IP address of 200.2.45.23

Solutions

ASA3

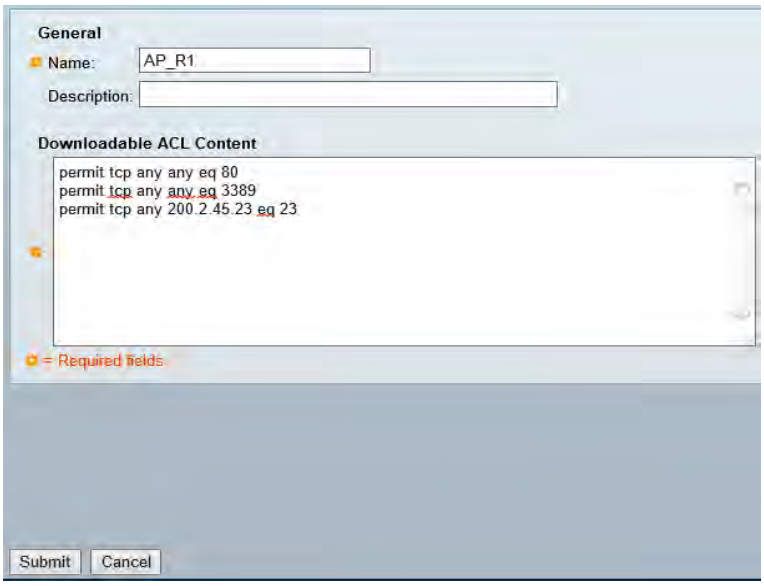
```
virtual telnet 200.2.45.23
object network VT
host 200.2.45.23
nat (inside,outside) static 200.2.45.23
```

- Configure the ASA and the ACS accordingly. Use "RADIUS Network Access" access service on the ACS. Test using any user. You are allowed to modify the VLAN's on the switch for the test PC. Do not set the default gateway on the test PC.

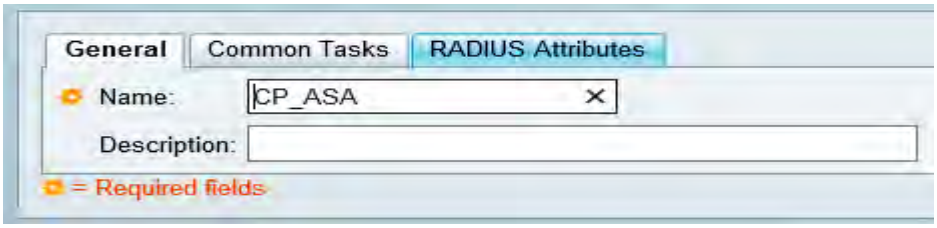
Solutions

ACS

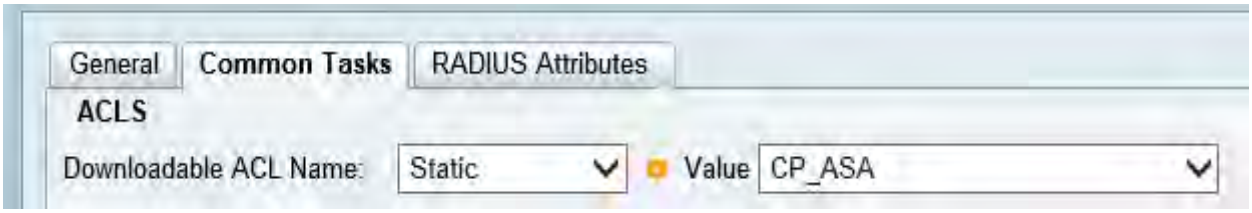
Step 1: Go to **Policy Elements -> Authorization and Permissions -> Named Permission Objects -> Downloadable ACLs** and create dACL's.



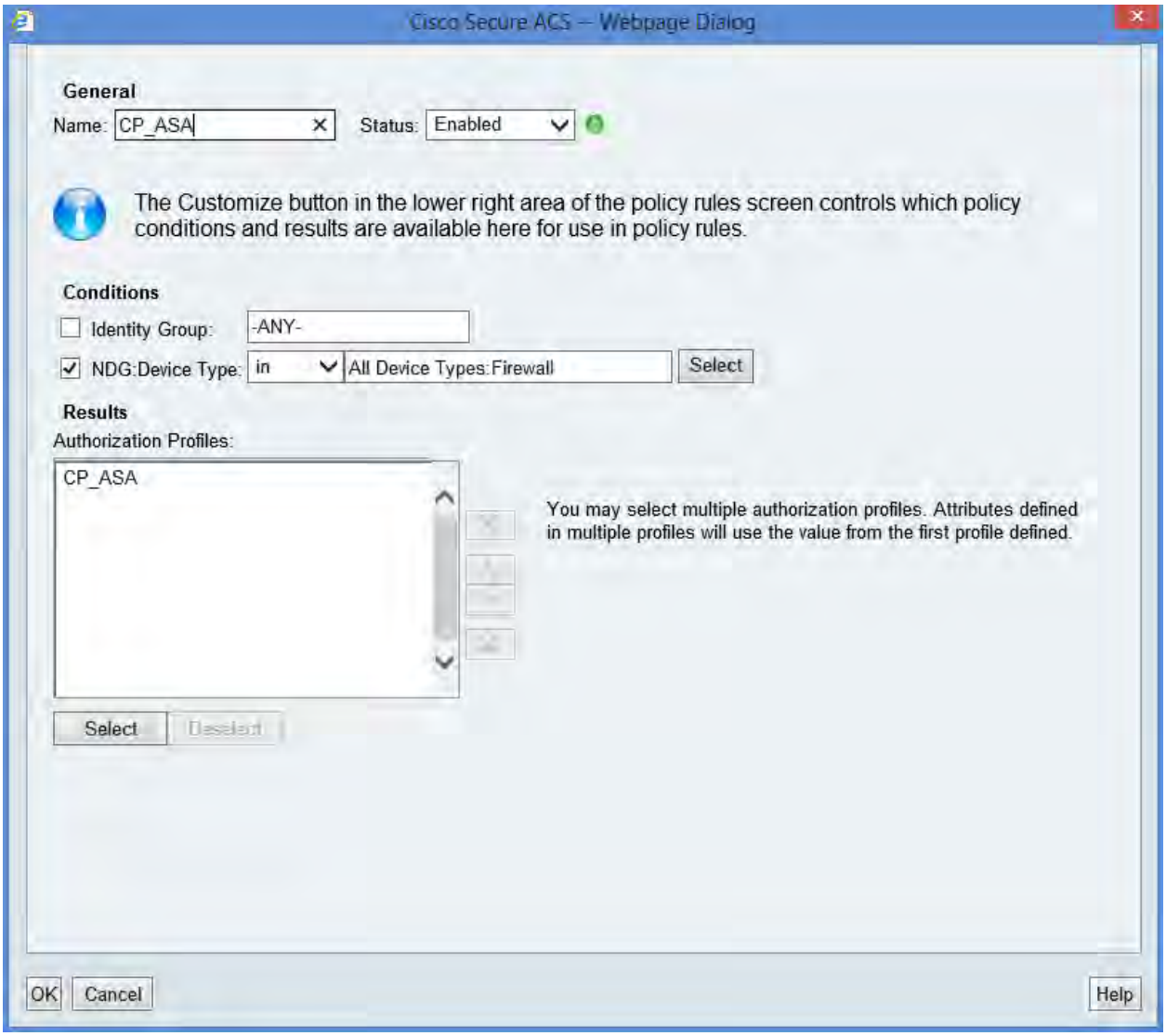
Step 2: Go to **Policy Elements -> Authorization and Permissions -> Network Access - > Authorization Profiles** and click on **Create**.



Step 3: Click on **Common Tasks** tab and configure the dACL.



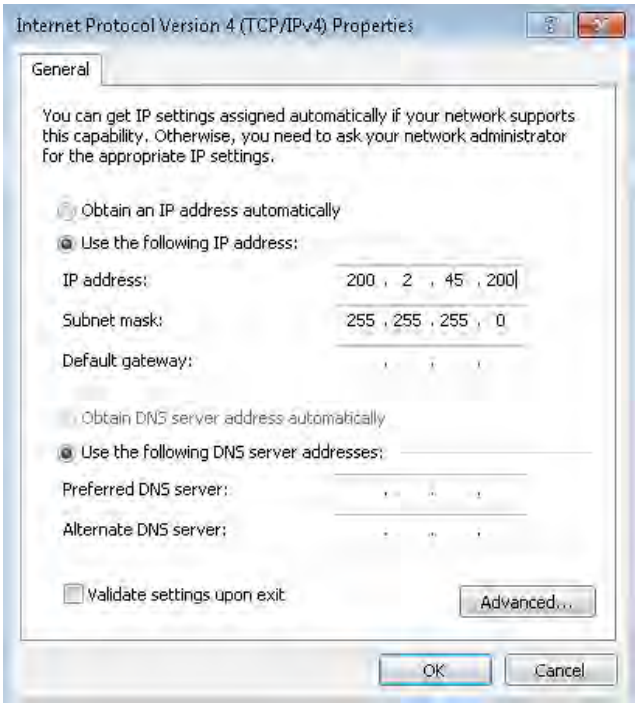
Step 4: Create a new the authorization rule. Go to **Access Policies -> Access Services -> RADIUS Network Access -> Authorization**. Click on **Create**.



Step 5: Configure VLAN 200 for TEST-PC1 and configure a static IP of 200.2.45.200.

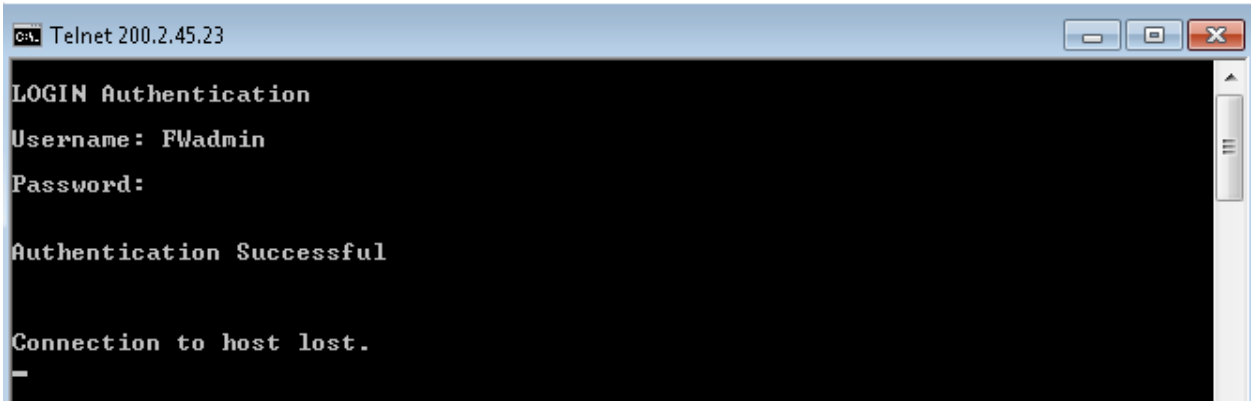
```
SW3(config)#int g1/0/2
SW3(config-if)#sw host
SW3(config-if)#sw acc vlan 200
```

Test PC



Verification

RDP into Test-PC 1 and telnet to the virtual IP of 200.2.45.23. Use any username.




```
Show access-list
<SNIP>
access-list #ACSACL#-IP-CP_ASA-4cff8cea; 4 elements; name hash: 0xcde694b0
(dynamic)
access-list #ACSACL#-IP-CP_ASA-4cff8cea line 1 extended permit tcp any host
200.2.45.23 eq telnet (hitcnt=1) 0xe450afde
access-list #ACSACL#-IP-CP_ASA-4cff8cea line 2 extended permit tcp any any eq
www (hitcnt=0) 0x2aeed5c2
access-list #ACSACL#-IP-CP_ASA-4cff8cea line 3 extended permit tcp any any eq
3389 (hitcnt=0) 0x2cf9846f
access-list #ACSACL#-IP-CP_ASA-4cff8cea line 4 extended permit icmp any any
(hitcnt=0) 0x72222944
```

```
ASA3# show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'FWadmin' at 200.2.45.200, authenticated
   access-list #ACSACL#-IP-CP_ASA-4cff8cea (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
ASA3#
```

Task 3: IOS Authentication proxy using RADIUS

- Re-configure R1 as a radius client on the ACS. R1 should source the RADIUS packets from 192.168.80.1 (F0/0) interface. The key should be cisco123.
- Configure R1 as the RADIUS client. R1 should process RADIUS VSA's and include attribute 6 in the RADIUS request packet.

Solutions

R1

```
aaa new-model
aaa authentication login default group radius
aaa authentication login NO none
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius

line con 0
 login authentication NO
line aux 0
 login authentication NO

radius-server attribute 6 on-for-login-auth
radius-server host 10.1.1.100 auth-port 1645 acct-port 1646 key cisco123
radius-server vsa send accounting
radius-server vsa send authentication
```

- Configure Authentication proxy such that a user needs to be authenticated, authorized and accounted before they are allowed any outbound access on TCP ports 23,80,8080 and for ICMP packets.
- Apply the Authentication proxy on F0/1 interface. R1 should directly authenticate any TCP 80 and 23 packets.

Solutions

R1

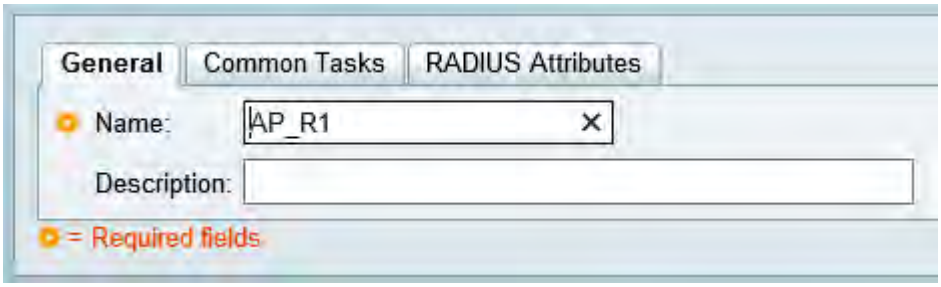
```
ip http server
ip auth-proxy name AP http
ip auth-proxy name AP telnet

access-list 102 deny   tcp any any eq www
access-list 102 deny   tcp any any eq telnet
access-list 102 deny   tcp any any eq 8080
access-list 102 deny   icmp any any
access-list 102 permit ip any any

interface FastEthernet0/1
 ip access-group 102 in
 ip auth-proxy AP
```

- Configure the ACS with appropriate authorization profile using cisco A/V pair's and authorization policy rule. Use "RADIUS Network Access" access service.
- Test using any user. Make sure that the default policy of RADIUS Network Access service has a DenyAccess. You are allowed to modify the VLAN's on the switch for the test PC. Do not set the default gateway on the test PC.

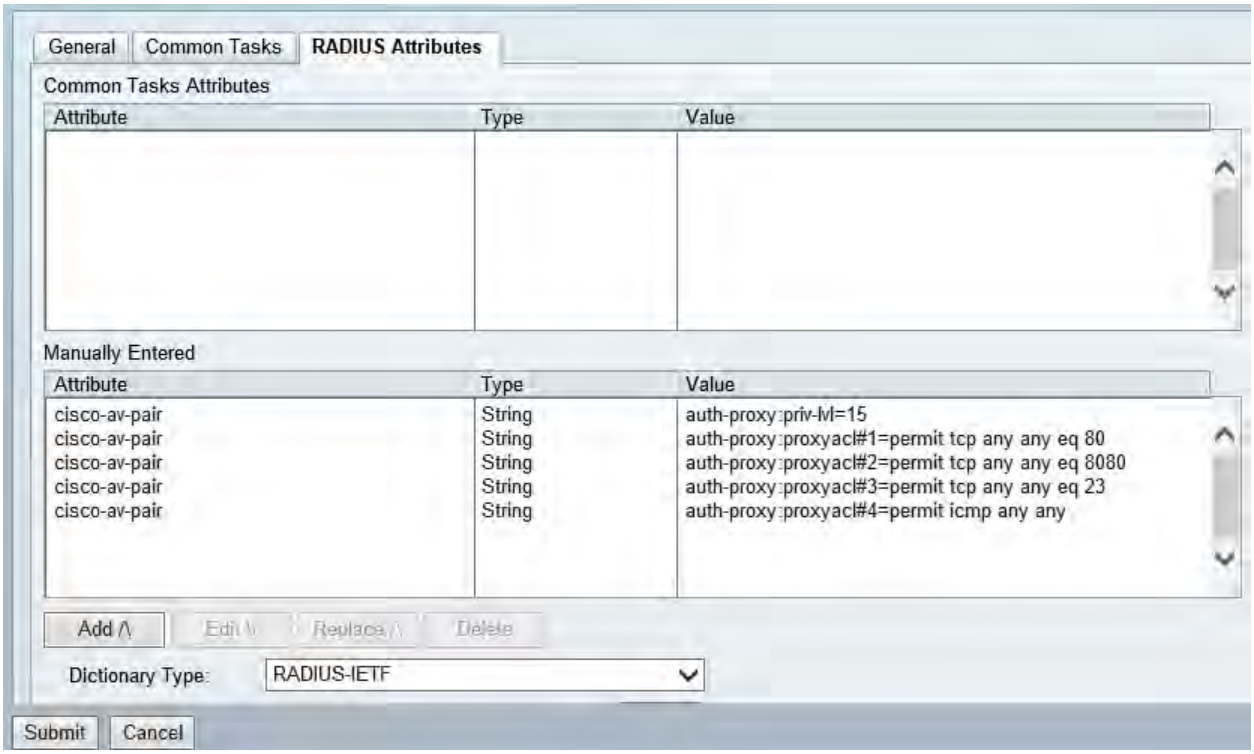
Solutions

ACS

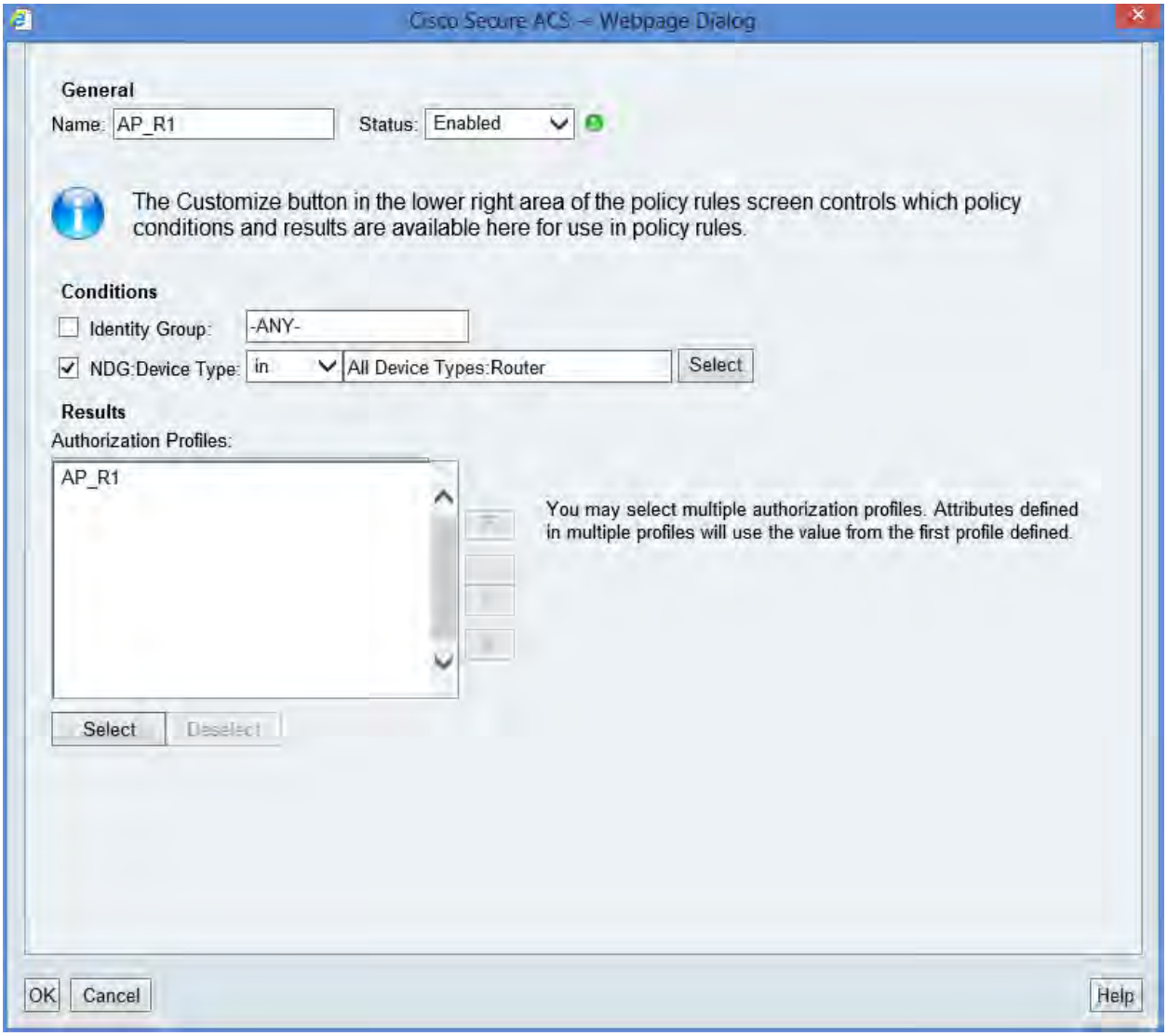
Step 1: Go to **Policy Elements -> Authorization and Permissions -> Network Access - > Authorization Profiles** and click on **Create**.



Step 2: Click on **RADIUS Attributes** tab and configure cisco AV pairs with auth-proxy attributes and values.



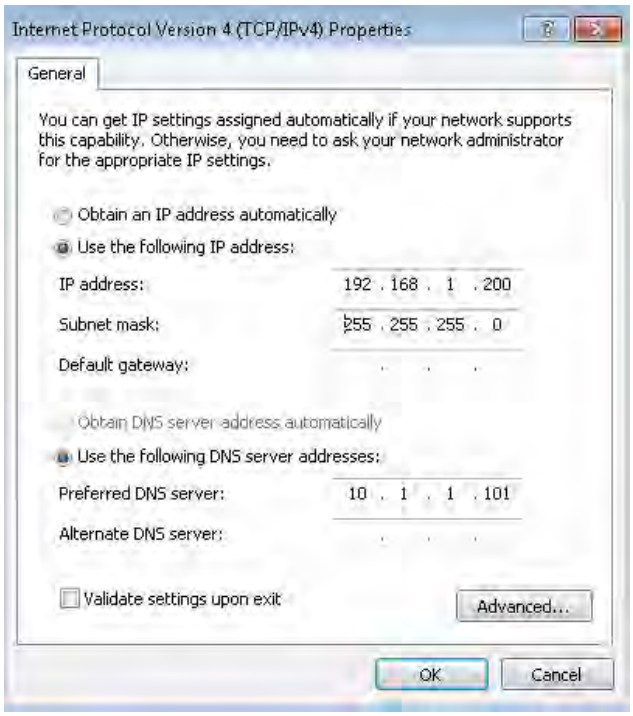
Step 3: Create a new the authorization rule. Go to **Access Policies -> Access Services -> RADIUS Network Access -> Authorization**. Click on **Create**.

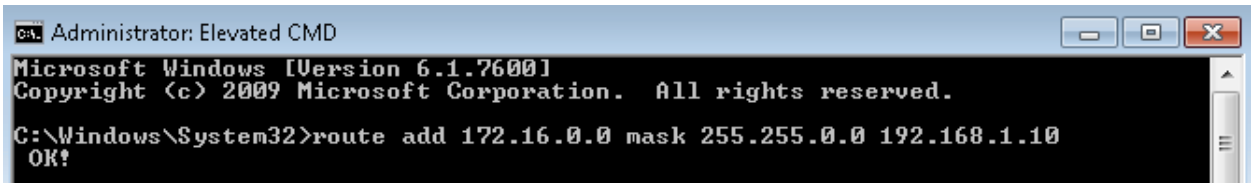


Verification

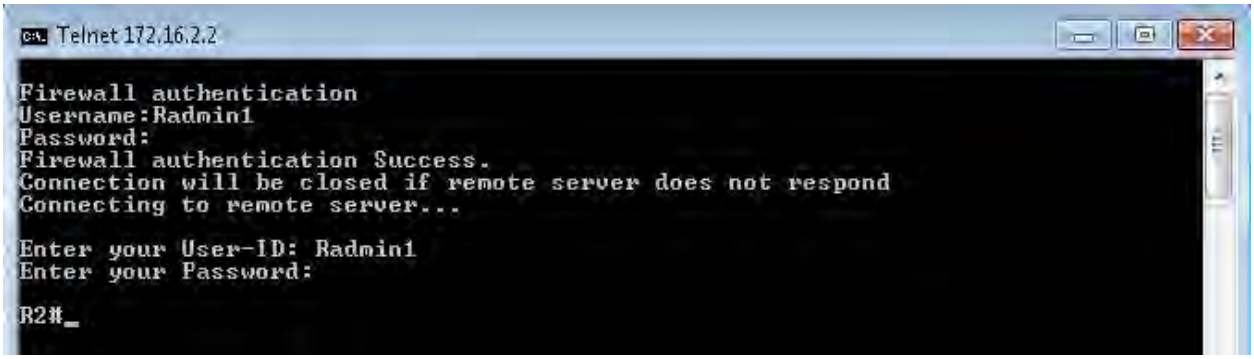
Configure SW3 to assign VLAN 10 for Test-PC2 then configure an IP address of 192.168.1.200 for the test PC. Add a static route for 172.16.0.0/16 with a next hop of 192.168.1.10

```
SW3(config)#int g1/0/12
SW3(config-if)#sw host
SW3(config-if)#sw acc vlan 10
```



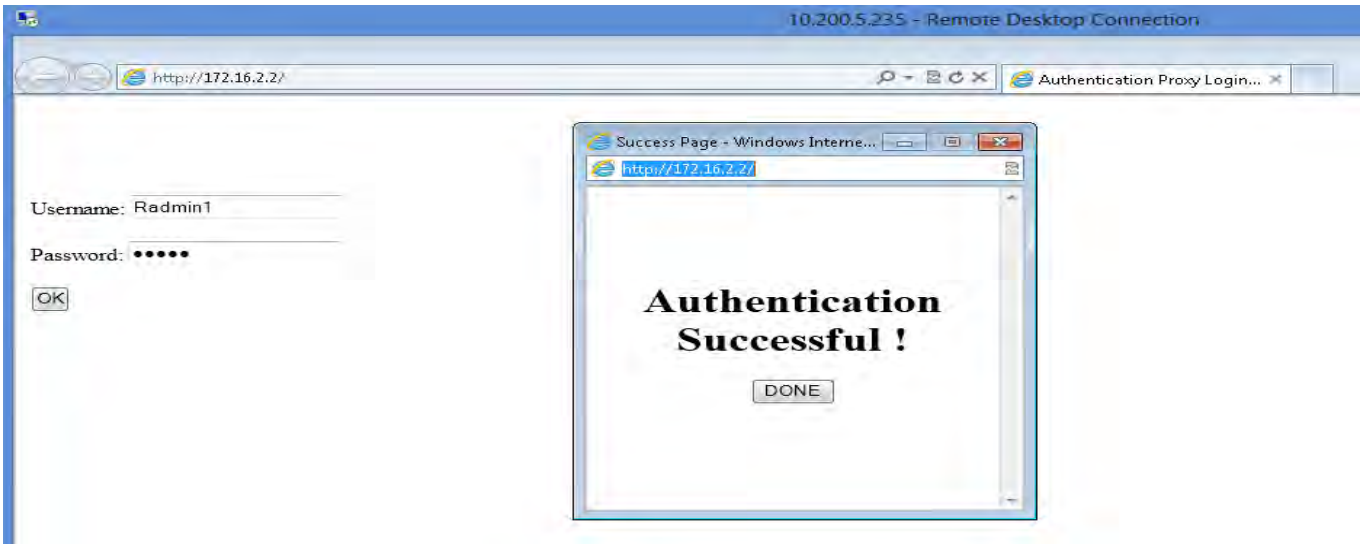


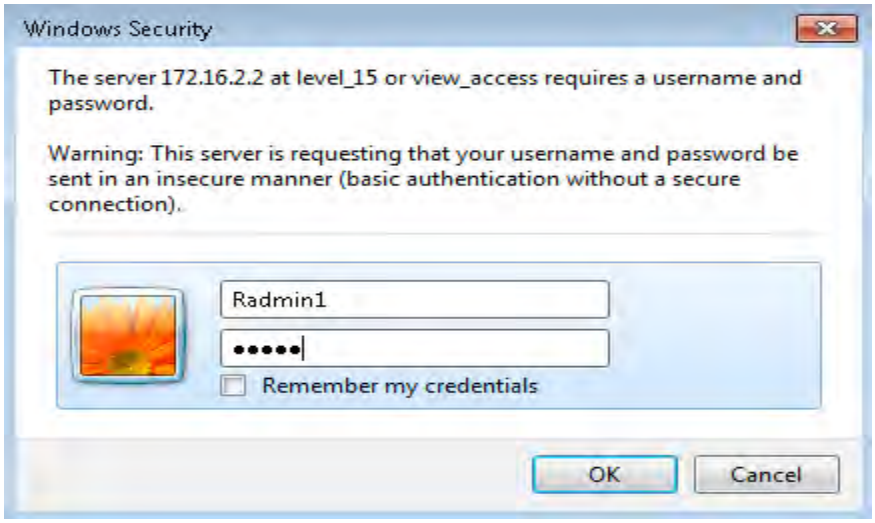
Telnet to R2 to test auth proxy from Test Pc 2. Use any username.

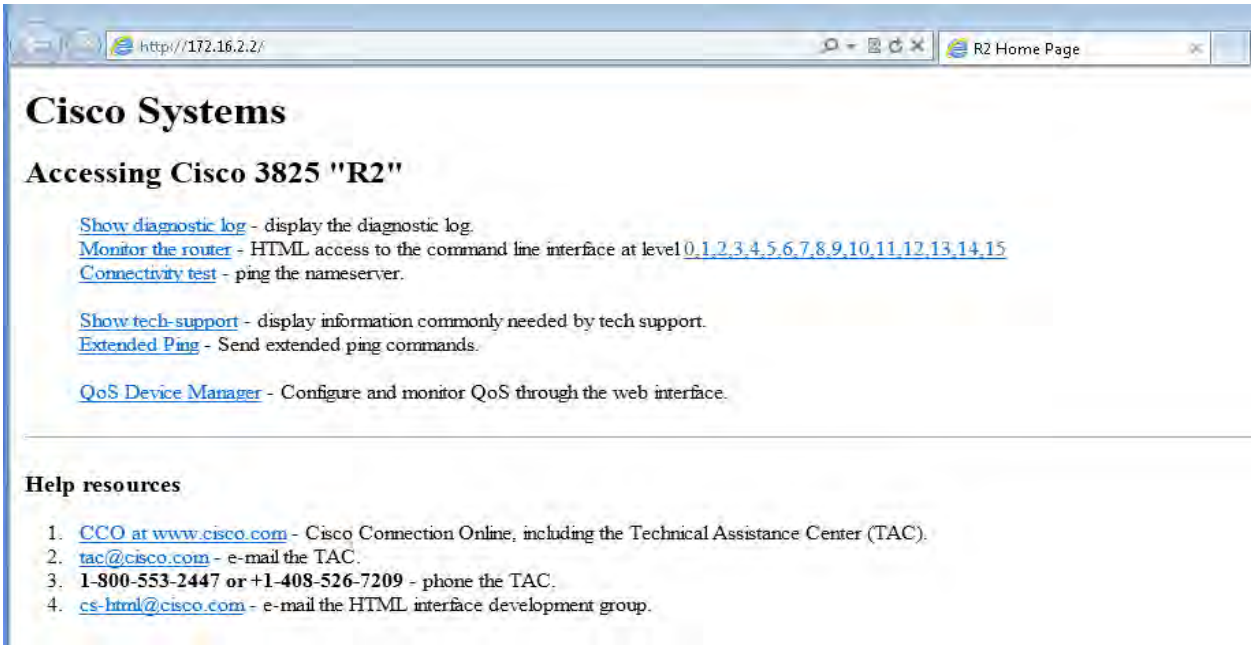



```
R1#show ip auth-proxy cache
Authentication Proxy Cache
 Client Name Radmin1, Client IP 192.168.1.200, Port 65513, timeout 60, Time
Remaining 58, state INTERCEPT

R1#sh access-lists
Extended IP access list 102
     permit tcp host 192.168.1.200 any eq www
     permit tcp host 192.168.1.200 any eq 8080
     permit tcp host 192.168.1.200 any eq telnet (22 matches)
     permit icmp host 192.168.1.200 any
    10 deny tcp any any eq www
    20 deny tcp any any eq telnet
    30 deny tcp any any eq 8080
    40 deny icmp any any (44 matches)
    50 permit ip any any (118160 matches)

R1#show ip auth-proxy configuration

Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 30

Authentication Proxy Rule Configuration
 Auth-proxy name AP
    http list not specified inactivity-timer 60 minutes

    telnet list not specified inactivity-timer 60 minutes

R1#clear ip auth-proxy cache *
```

Web browse to R2 from the test pc. Use Radmin1/cisco as credentials.








```
R1#show ip auth-proxy cache
Authentication Proxy Cache
 Client Name Radmin1, Client IP 192.168.1.200, Port 49358, timeout 60, Time
Remaining 60, state ESTAB

R1#show ip auth-proxy cache username Radmin1
Authentication Proxy Cache

User Name               : Radmin1
Client IP               : 192.168.1.200
Client Port             : 49358
Timeout                 : 60
Time  Remaining         : 59
Connection state        : ESTAB

EPM information : Authproxy
Admission feature       : Authproxy
AAA Policies            :
Proxy ACL               : permit tcp any any eq 80
Proxy ACL               : permit tcp any any eq 8080
Proxy ACL               : permit tcp any any eq 23
Proxy ACL               : permit icmp

<SNIP>

R1#show access-lists
Extended IP access list 102
     permit tcp host 192.168.1.200 any eq www (12 matches)
     permit tcp host 192.168.1.200 any eq 8080
     permit tcp host 192.168.1.200 any eq telnet
```

```
 permit icmp host 192.168.1.200 any
10 deny tcp any any eq www
20 deny tcp any any eq telnet
30 deny tcp any any eq 8080
40 deny icmp any any (68 matches)
50 permit ip any any (118564 matches)
```

ipexpert

IPexpert's Detailed Solution Guide

for the Cisco® CCIE™ Security Volume 1

Complete DSG Labs 6-10

Table of Contents

Section 6: IPS Solutions

Lab-1: IPS

Section 6: Cisco IPS is intended to let you be familiar with the IPS technologies that are available on IPS appliance and the IOS software. You will be configuring basic initialization, various deployment modes, virtual senor creation, signature tuning, anomaly detection, even action rules some advanced features related to those technologies.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

General Rules

- This lab will focus strictly on the Cisco IPS. You will need to pre-configure the network with the base configuration files

NOTE: Static/default routes are NOT allowed unless otherwise stated in the task

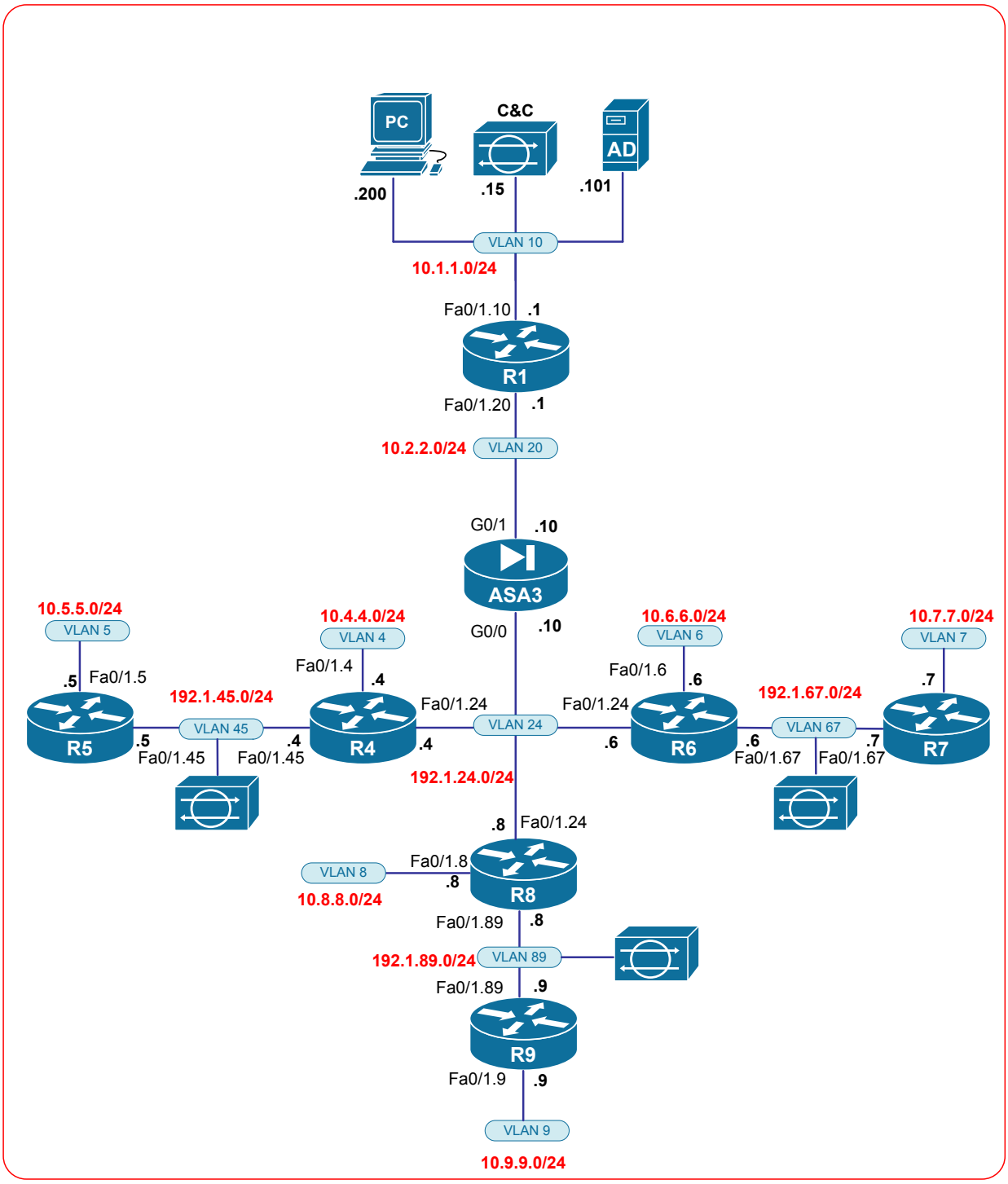
Estimated Time to Complete: 7 Hours

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R1	Fa0/1.10	10	10.1.1.1/24
	Fa0/1.20	20	10.2.2.1/24
	Loopback0	-	1.1.1.1/24
R4	Fa0/1.4	4	10.4.4.4/24
	Fa0/1.24	24	192.1.24.4/24
	Fa0/1.45	45	192.1.45.4/24
	Loopback0	-	4.4.4.4/24
R5	Fa0/1.5	5	10.5.5.5/24
	Fa0/1.45	45	192.1.45.5/24
	Loopback0	-	5.5.5.5/24
R6	Fa0/1.6	6	10.6.6.6/24
	Fa0/1.24	24	192.1.24.6/24
	Fa0/1.67	67	192.1.67.6/24
	Loopback0	-	6.6.6.6/24
R7	Fa0/1.7	7	10.7.7.7/24
	Fa0/1.67	67	192.1.67.7/24
	Loopback0	-	7.7.7.7/24
R8	Fa0/1.8	8	10.8.8.8/24
	Fa0/1.89	89	192.1.89.8/24
	Fa0/1/24	24	192.1.24.8/24
	Loopback0	-	8.8.8.8/24
R9	Fa0/1.9	9	10.9.9.9/24
	Fa0/1.89	89	192.1.89.9/24
	Loopback0	-	9.9.9.9/24
ASA3	G0/0 (outside)	24	192.1.24.10/24
	G0/1 (inside)	20	10.2.2.10/24
IPS	C&C	10	10.1.1.15/24

Network Topology 6.1 (Logical)



Lab 6: Cisco IPS

Task 1: Sensor Setup and Administration

- Before you begin erase the current configuration on the sensor using “erase current- config”.
- From the console, configure the hostname as “IPS” and the command-and-control interface of the sensor with an IP address of 10.1.1.15/24 and a default gateway of 10.1.1.1
- Configure the sensor to listen for HTTPS requests on port 10443 instead of the default of 443.
- From this point on, you may use either the command-line or IDS Device Manager (IDM) to configure the sensor. Note that IDM is specifically mentioned in the Blueprint, so you should be familiar with its use.

Configuration

IPS

When using the remote rack sessions before you start configuring the sensor, doing a quick erase current-config will ensure any previously configured virtual sensors, etc., have all been removed.

```
sensor# erase current-config
Warning: Removing the current-config file will result in all configuration being reset to default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no username" command.
Continue? []: yes
Warning: DNS or HTTP proxy is required for global correlation inspection and reputation filtering, but no DNS or proxy servers are defined.


Warning: The edit operation has no effect on the running configuration

sensor# show config
! ------------------------------
! Current configuration last modified Wed Apr 15 10:37:57 2013
! ------------------------------
! Version 7.0(6)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S549.0   2011-02-17
! ------------------------------
service interface
exit
! ------------------------------
service authentication
```

```
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

Type the setup command to begin the initial setup wizard.

```
sensor# setup


    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Wed May 15 10:40:33 2013

Setup Configuration last modified: Wed May 15 10:37:57 2013

Enter host name[sensor]: IPS
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.1.15/24,10.1.1.1
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 0.0.0.0/32
Permit:
Use DNS server for Global Correlation?[no]:
Use HTTP proxy server for Global Correlation?[no]:
Modify system clock settings?[no]:
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level?[off]:


The following configuration was entered.

service host
network-settings
host-ip 10.1.1.15/24,10.1.1.1
host-name IPS
telnet-option disabled
access-list 10.1.1.0/24
ftp-timeout 300
no login-banner-text
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy no-proxy
exit
time-zone-settings
```

```
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service global-correlation
network-participation off
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.

Enter your selection[3]: 3
Enter telnet-server status[disabled]:
Enter web-server port[443]: 10443
Modify interface/virtual sensor configuration?[no]:
Modify default threat prevention settings?[no]:

The following configuration was entered.

service host
network-settings
host-ip 10.1.1.15/24,10.1.1.1
host-name IPS
telnet-option disabled
access-list 10.1.1.0/24
ftp-timeout 300
no login-banner-text
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy no-proxy
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service global-correlation
network-participation off
exit
service web-server
port 10443
```

```
exit
service event-action-rules rules0
overrides
override-item-status Enabled
risk-rating-range 90-100
exit
exit
[0] Go to the command prompt without saving this config.
[1] Return to the Advance setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
Warning: DNS or HTTP proxy is required for global correlation inspection and
reputation filtering, but no DNS or proxy servers are defined.
Configuration Saved.
sensor#
```

Make sure Test PC is in VLAN 10.

```
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
```

SW4

```
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
```

Notes

The bulk of these tasks will be completed through the initial setup wizard.
Log into the sensor on the console port. If the initial setup wizard is already in progress, type Control-C to exit to the sensor# command prompt.

The first section of the wizard allows the configuration of the hostname, ip address and management access list. Continuing to the advanced setup using option 3 will allow you to pre configure the web servers listening port to 10443 as requested in the task.

Finally, don't forget to configure the switchport for the command and control interface in vlan 10. Make sure you configure an IP address of 10.1.1.200 for the TEST PC. Also make sure the IP C&C interface is in VLAN 10.

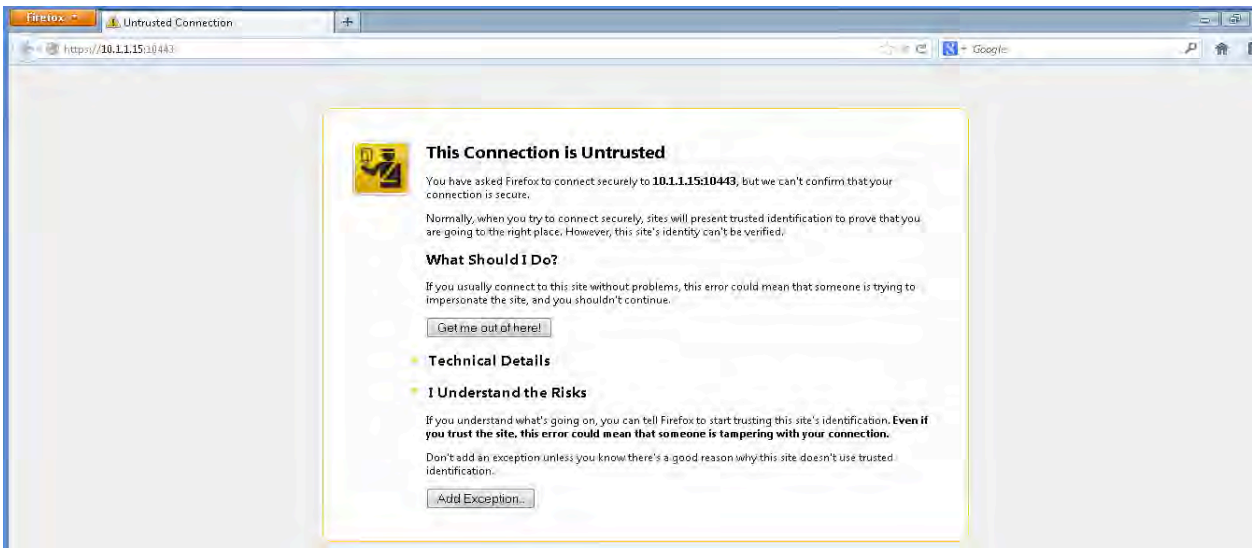
Verification

First confirm your IPS configuration is as required:

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Wed Apr 15 10:52:04 2013
! ------------------------------
! Version 7.0(6)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S549.0   2011-02-17
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.1.1.15/24,10.1.1.1
host-name IPS
telnet-option disabled
access-list 10.1.1.0/24
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
port 10443
```

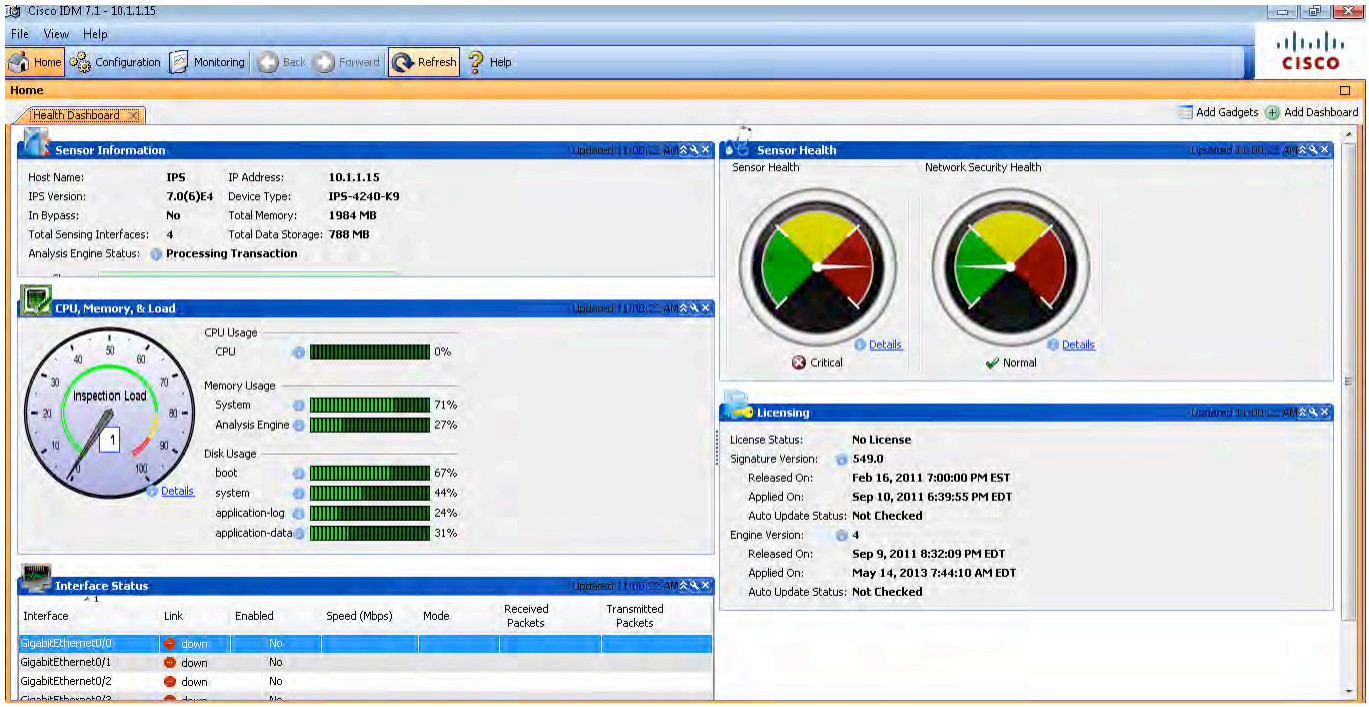
```
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
exit
```

If you‟re happy that this is correct, then open a web browser session to the IPS sensor from the ACS server, using the newly defined port 10443



Accept the security exception and click on the “Run IDM” button to start the Device Manager.

Login when requested using the credentials of cisco/IPexpert123



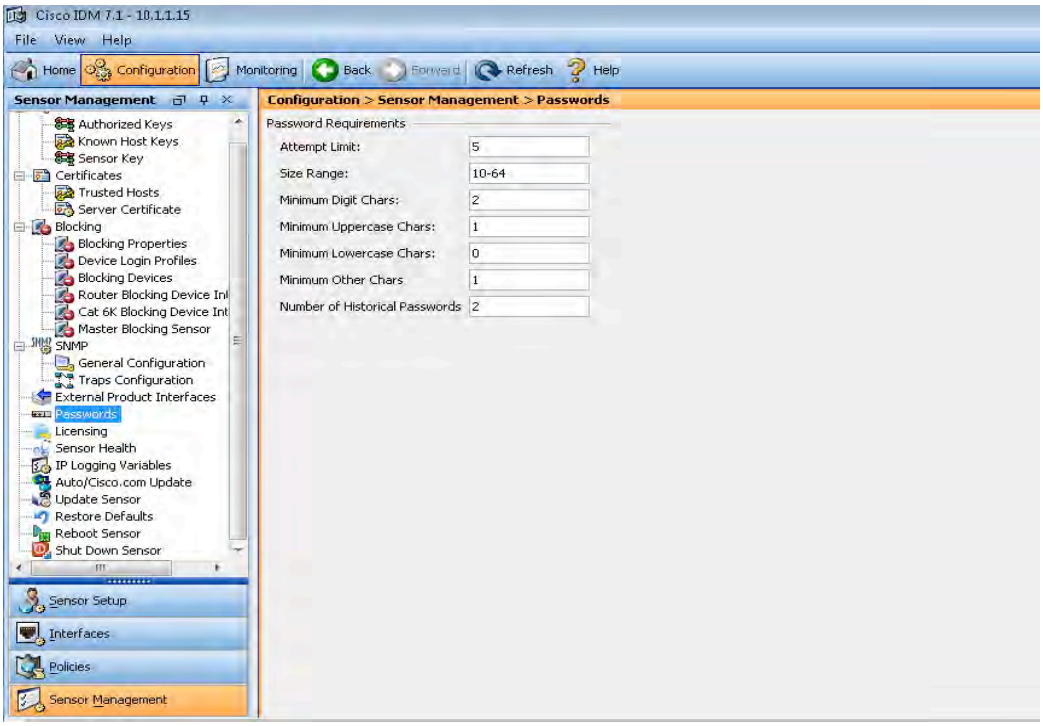
Task 2: Password Protection

- Your corporate security policy states that all passwords must be at least 10 characters in length, and must contain at least one uppercase letter, one non-alphanumeric character (such as # or $), and at least two numbers. The previous 2 passwords should also be remembered. Configure the sensor to enforce this policy.
- Your corporate security policy requires that accounts be locked after 5 invalid login attempts. Configure the sensor to implement this requirement.
- The operations team needs read-only access to the sensor to view events. Create a new user for their use called “nocadmin” with password “NOCread123#”.

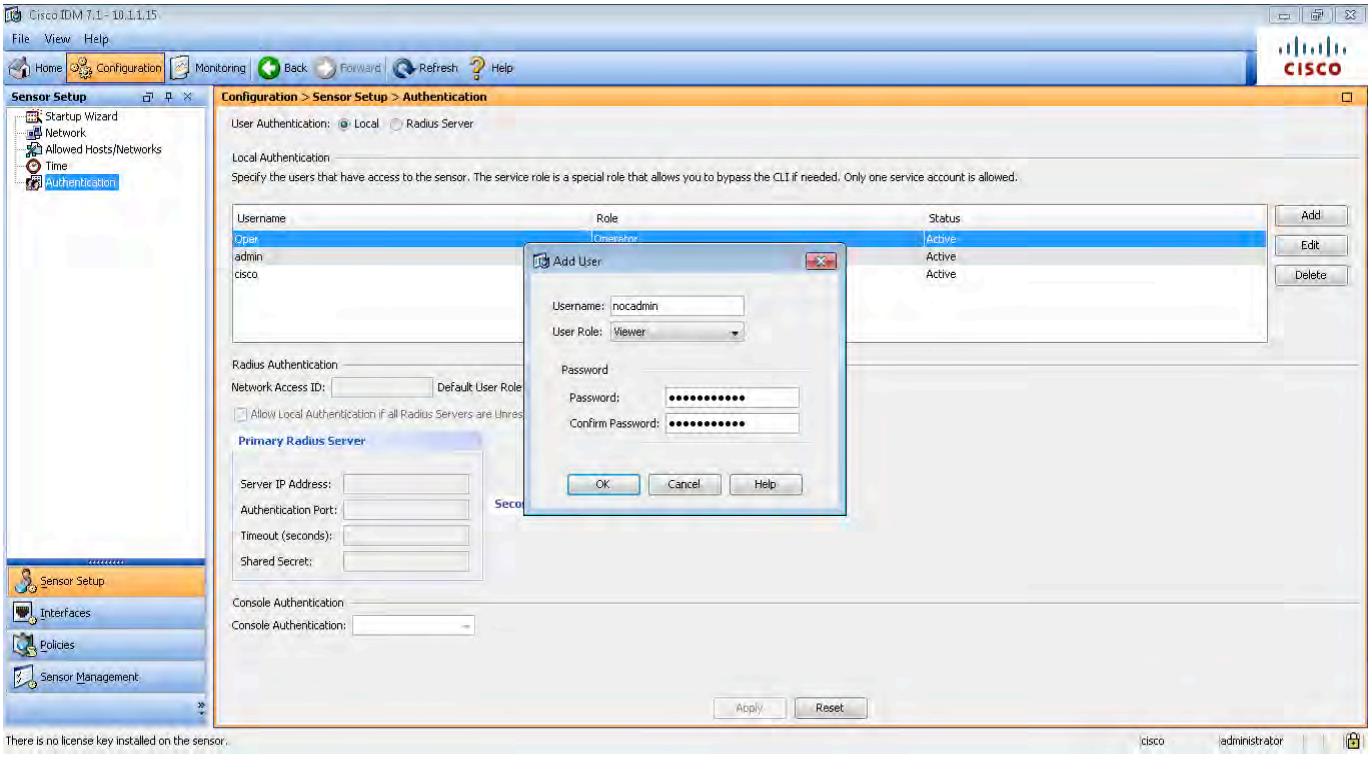
Configuration

IPS

Password policy is configured in IDM at Configuration > Sensor Management > Passwords.
Invalid login attempts are also configured here in IDM as the password requirement policy. Then click on Apply.



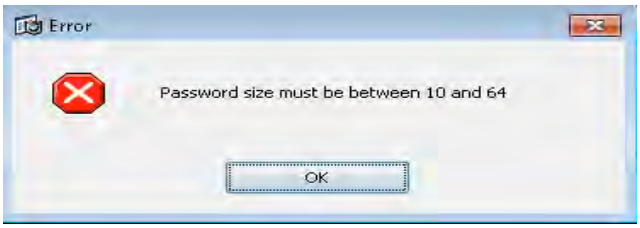
Sensor users can be configured on the Configuration > Sensor Setup > Authentication in IDM. Click on Add and configure the user and finally apply the changes.



Notes

This task included some simple user based security features, around role based access and password complexity requirements.
One thing to remember for role based access is that if the requirement is for the user not to make any changes then the it must use the viewer role, as the operator role does have access to tune signatures and make minor changes to configurations.

Verification
The password policy can be tested by creating a test user with a non-compliant password. Example- If the password length does not comply then the following message is displayed:



Login into the sensors cli to test the new nocadmin account. Issue a show privilege command to ensure the viewer role has been assigned.

```
IPS# exit


IPS login: nocadmin
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the IPS-4240.
The system will continue to operate with the currently installed
signature set.  A valid license must be obtained in order to apply
signature updates.  Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
```

```
IPS# show privilege
Current privilege level is viewer
```

Task 3: Network Time Protocol

- Configure R1 to act as an NTP master.
- Set the time zone to EST (GMT -5) and account for daylight saving
- Configure NTP authentication with MD5 key #1 and value “ipexpert”
- Configure the sensor to sync its clock to R1 using NTP

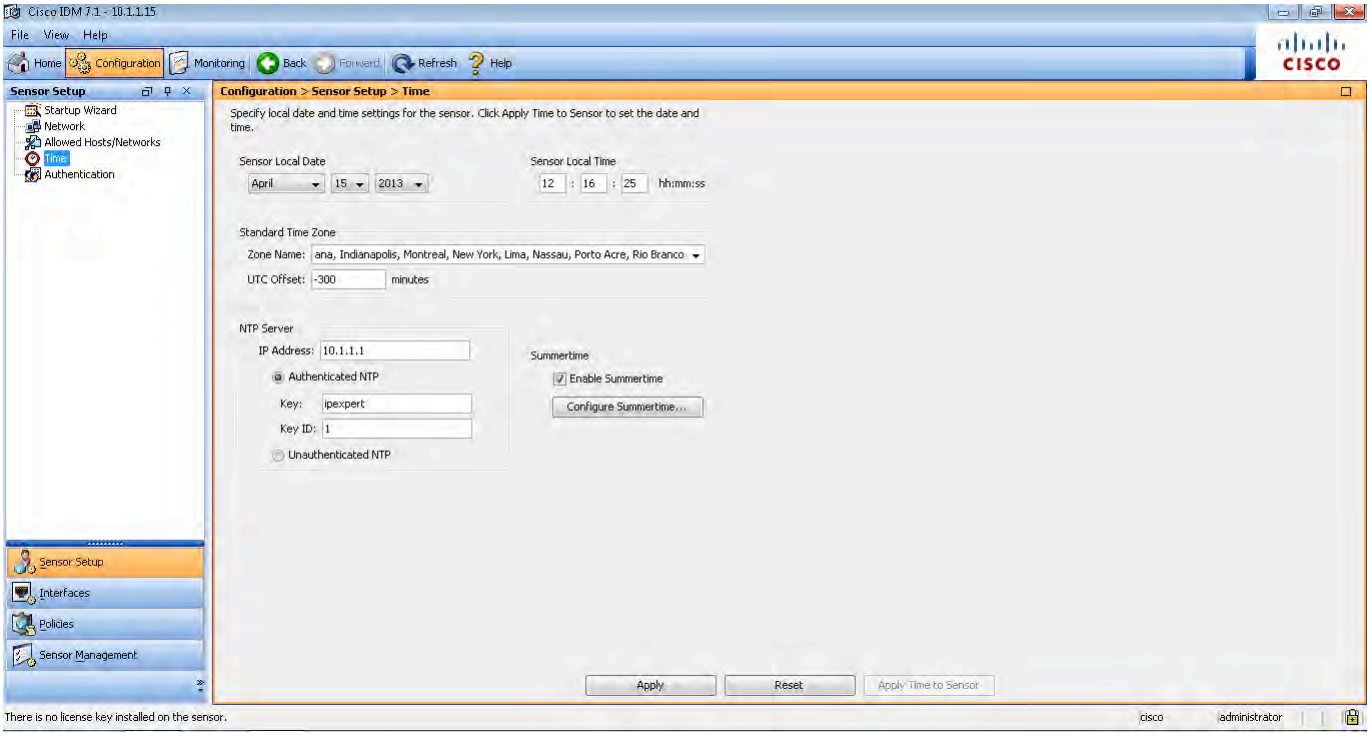
Configuration

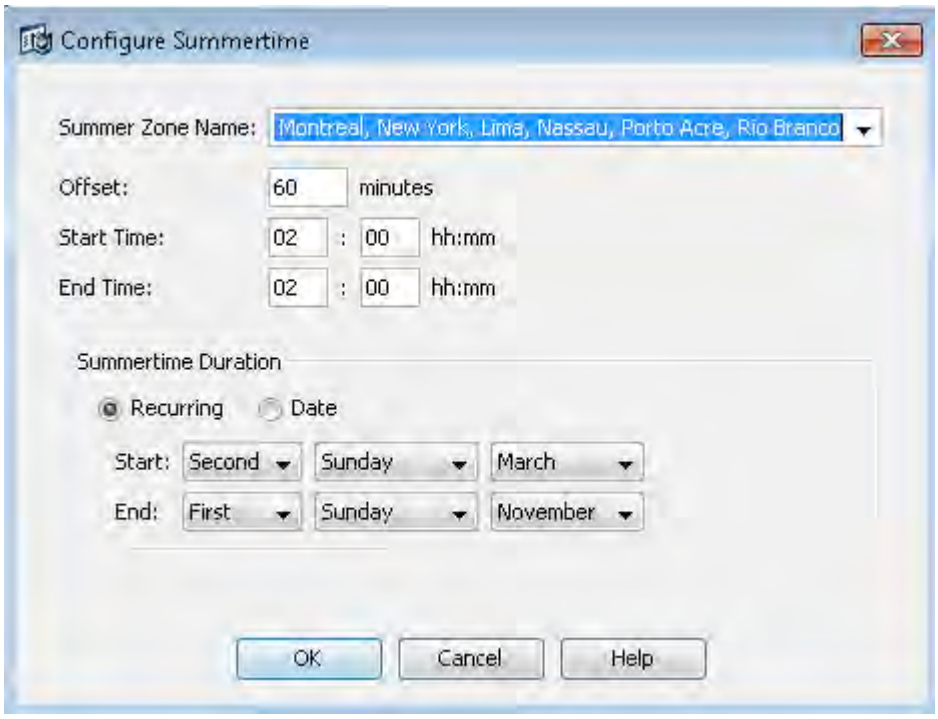
R1

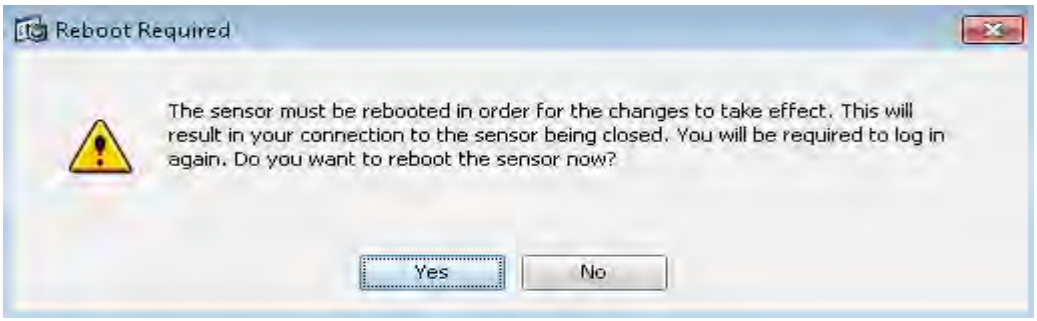
```
clock timezone EST -5
clock summer-time EDT recurring
ntp master 1
ntp authenticate
ntp authentication-key 1 md5 ipexpert
ntp trusted-key 1
```

IPS

NTP is configured under Configuration > Sensor Setup > Time.







Notes

Another fairly straight forward task to carry out. Configure NTP master on R1.
When configuring the IPS for NTP, the key ID and key string must match what was configured on R1, the same as IOS clients. Enable/configure summer time settings and set the timezone.
The sensor will need to be rebooted for NTP to be enabled successfully.

Verification

Verify that the R1 is running as a master server

```
R1#show ntp associations detail

127.127.1.1 configured, our_master, sane, valid, stratum 0
ref ID .LOCL., time D5167030.C9C57205 (08:25:20.788 EDT Mon Apr 15 2013)
```

```
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 2.80
delay 0.00 msec, offset 0.0000 msec, dispersion 0.24
precision 2**24, version 4
org time D5167030.C9C57205 (08:25:20.788 EDT Mon Apr 15 2013)
rec time D5167030.C9C61651 (08:25:20.788 EDT Mon Apr 15 2013)
xmt time D5167030.C9C4FA95 (08:25:20.788 EDT Mon Apr 15 2013)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.27    0.49    0.75    1.00    1.23    1.47    1.71
minpoll = 4, maxpoll = 4


IPS# show clock detail
08:32:07 GMT-05:00 Mon Apr 15 2013
Time source is NTP
Summer time starts 03:00:00 GMT-05:00 Sun Mar 10 2013
Summer time stops 01:00:00 GMT-05:00 Sun Nov 03 2013
```

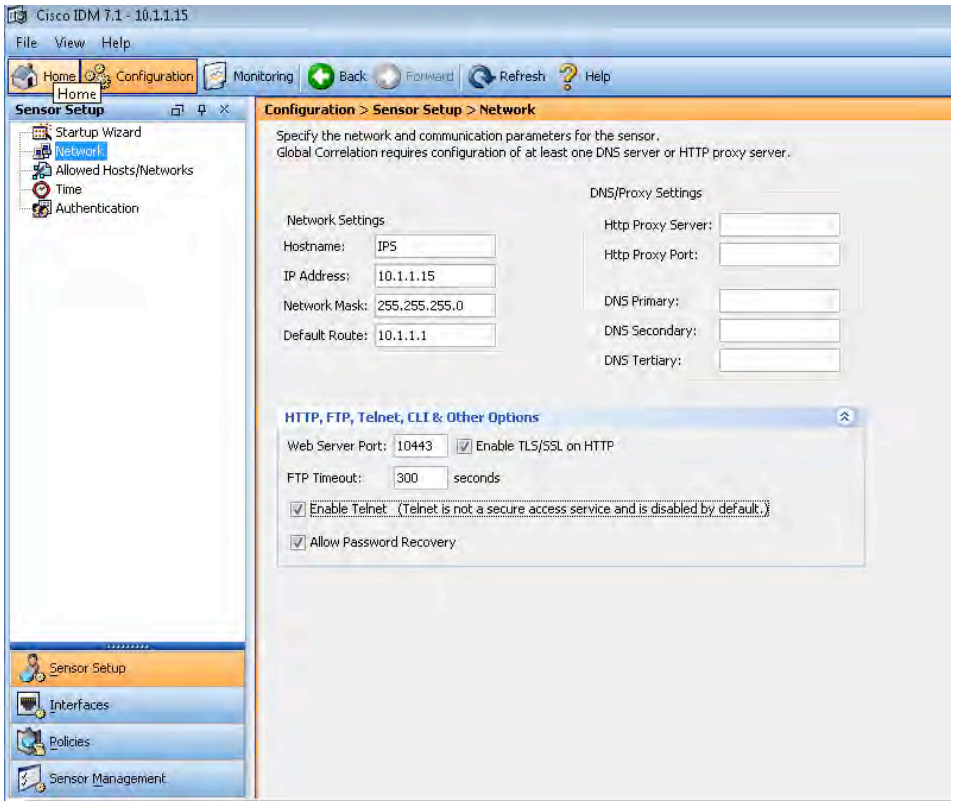
Task 4: Miscellaneous Configuration

- Although telnet is an inherently insecure protocol, the NOC requires it to be enabled for management purposes. The NOC will connect to the sensor from R1. Configure the sensor to allow this.
- Configure the sensor to allow SNMP management using the read-only community string “IPSro” and the read-write community string “IPSrw”. Set the system location to “IPexpert HQ” and the system contact to IPS@ipexpert.com. Traps should also be enabled to the ACS Server using read only community.
- When users log into the sensor, they should see a login banner indicating that access is restricted to authorized personnel only.

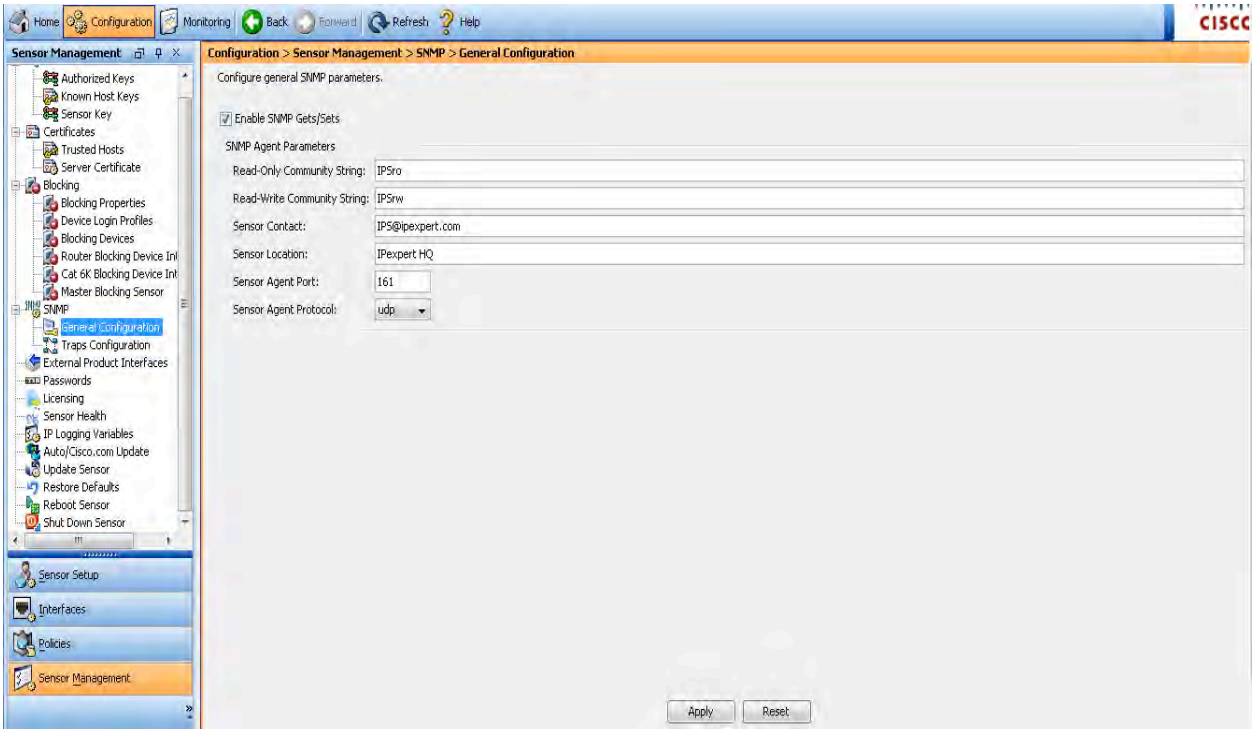
Configuration

IPS

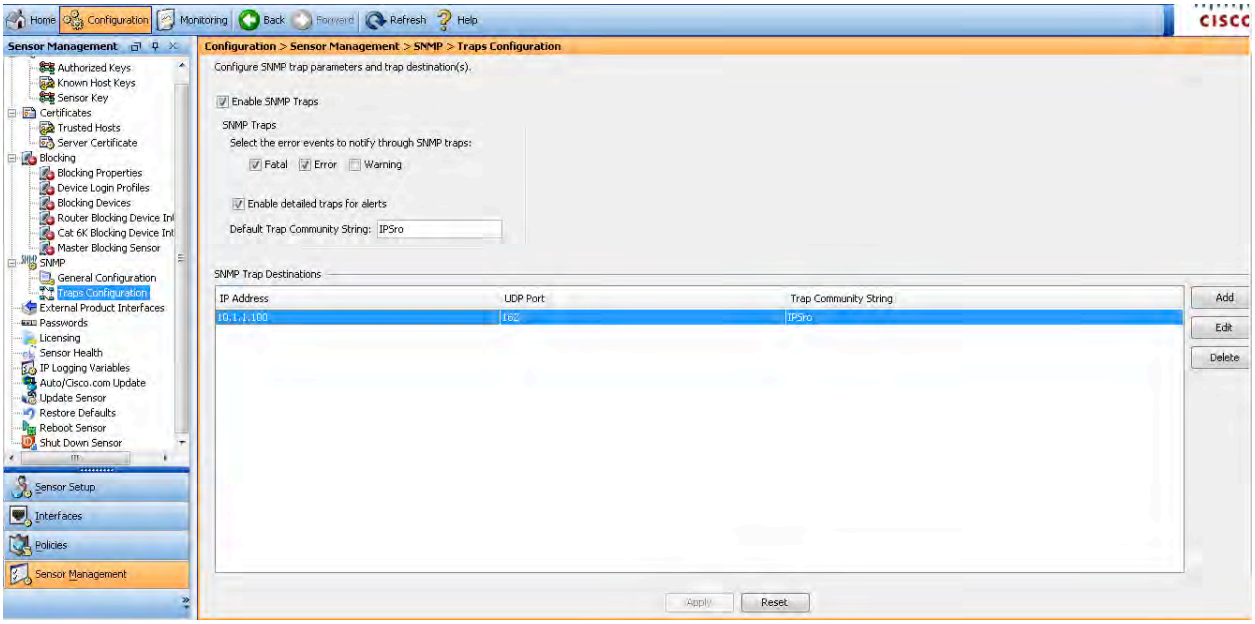
Telnet access is configured under Configuration > Sensor Setup > Network.



SNMP configuration is carried out under Configuration >Sensor Management > SNMP > General Configuration.



SNMP traps are enabled from Configuration > System Management > SNMP > Trap Configuration.



Use the Add button to include the ACS Server as a Trap destination. The login banner can only be configured from the command-line in the current version of the sensor software.

```
IPS# conf t
IPS(config)# service host
IPS(config-hos)# network-settings
IPS(config-hos-net)# login-banner-text *** Access is restricted to authorized
personnel only! ***
IPS(config-hos-net)#
IPS(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.1.1.15/24,10.1.1.1 default: 192.168.1.2/24,192.168.1.1
      host-name: IPS default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      -----------------------------------------------
         network-address: 10.1.1.0/24
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: *** Access is restricted to authorized personnel only! ***
default:
      dns-primary-server
      -----------------------------------------------
         disabled
         -----------------------------------------------
         -----------------------------------------------
```

```
      ------------------------------------------------
      dns-secondary-server
      ------------------------------------------------
         disabled
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      dns-tertiary-server
      ------------------------------------------------
         disabled
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      http-proxy
      ------------------------------------------------
         no-proxy
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ---------------------------------------------
IPS(config-hos-net)# exit
IPS(config-hos)# exit
Apply Changes?[yes]:
Warning: DNS or HTTP proxy is required for global correlation inspection and
reputation filtering, but no DNS or proxy servers are defined.
```

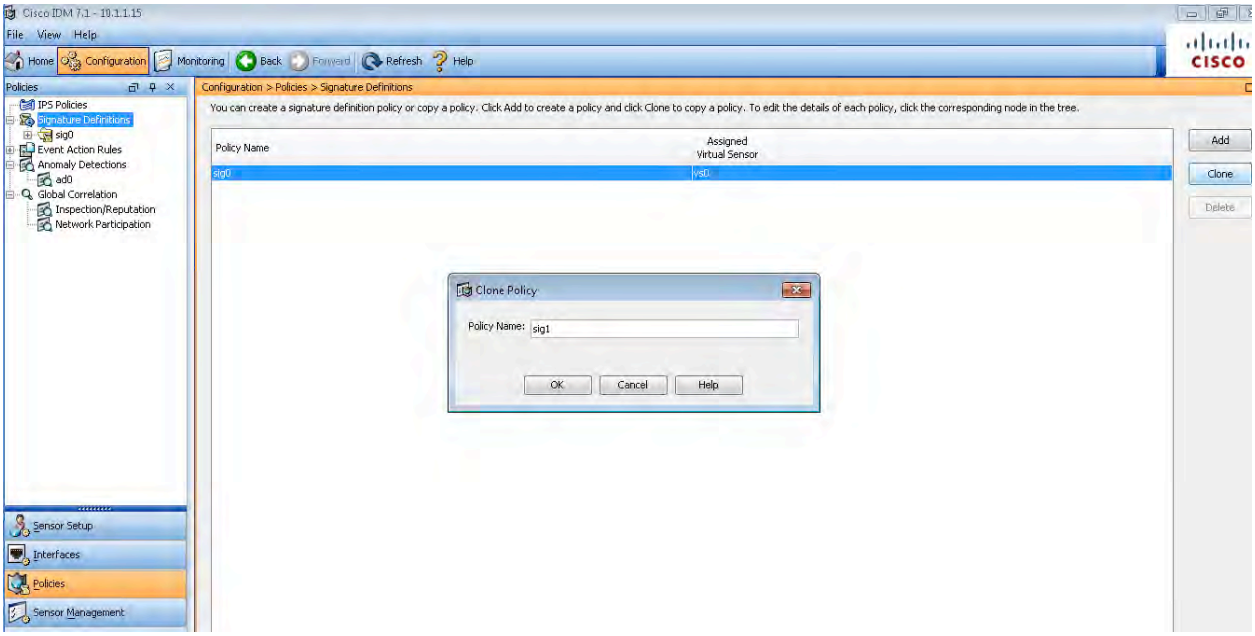
Notes

If you read the entire lab before starting, enabling telnet could have been completed in the initial setup wizard saving yourself a little time.

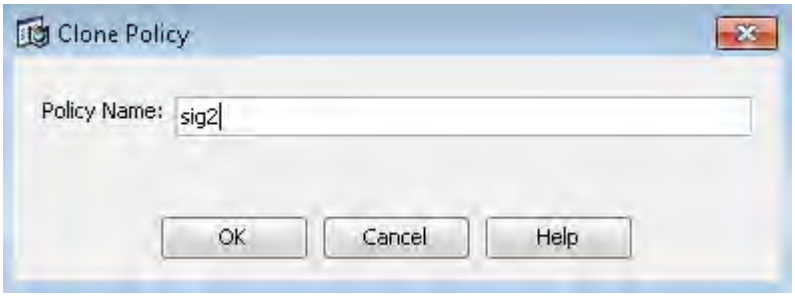
Task 5: Creating Virtual Sensors

- Create a new virtual sensor, vs1
- Set the description to “Inline Pair IPS monitoring for R6 and R7”
- Create new policy objects for vs1, sig1, rules1, and ad1. These should be exact copies of the policy objects in vs0.
- Create a new virtual sensor, vs2
- Set the description to “VLAN Pair IPS monitoring for R8 and R9”
- Create new policy objects for vs2, sig2, rules2, and ad2. These should be exact copies of the policy objects in vs0

Configuration

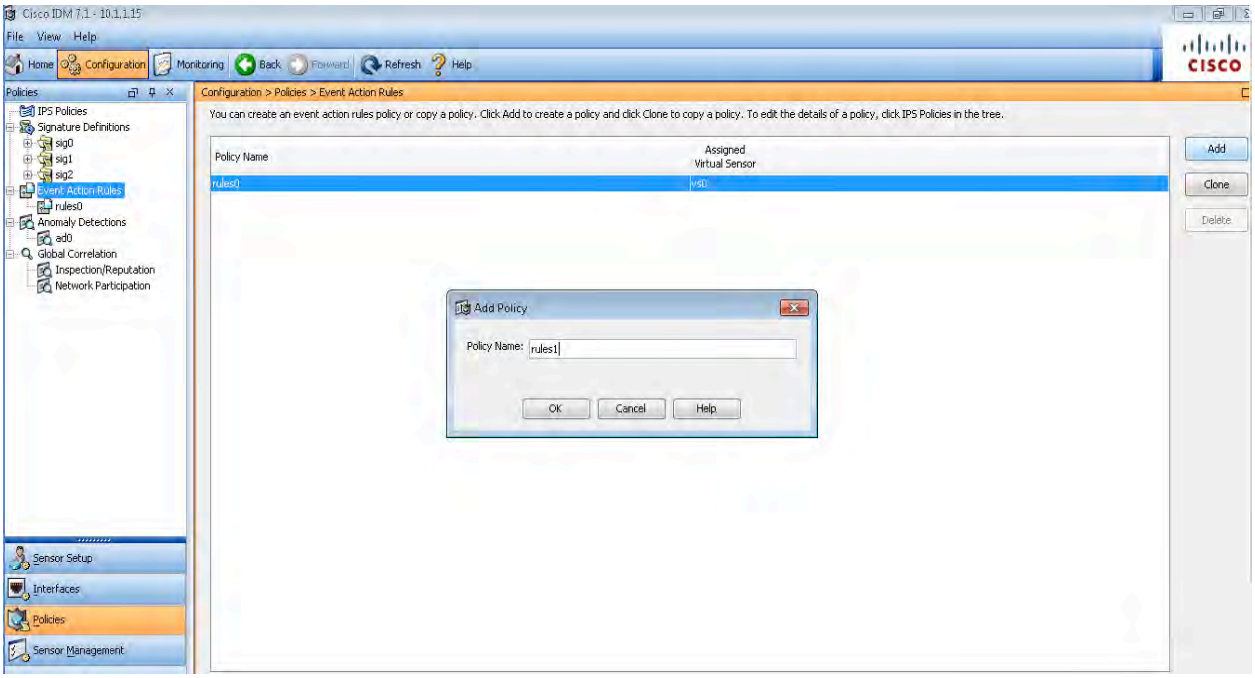


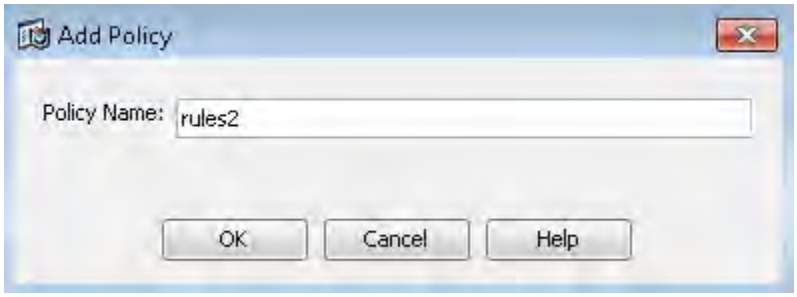
First create your policy objects for both vs1 and vs2, starting cloning the signature defintions.



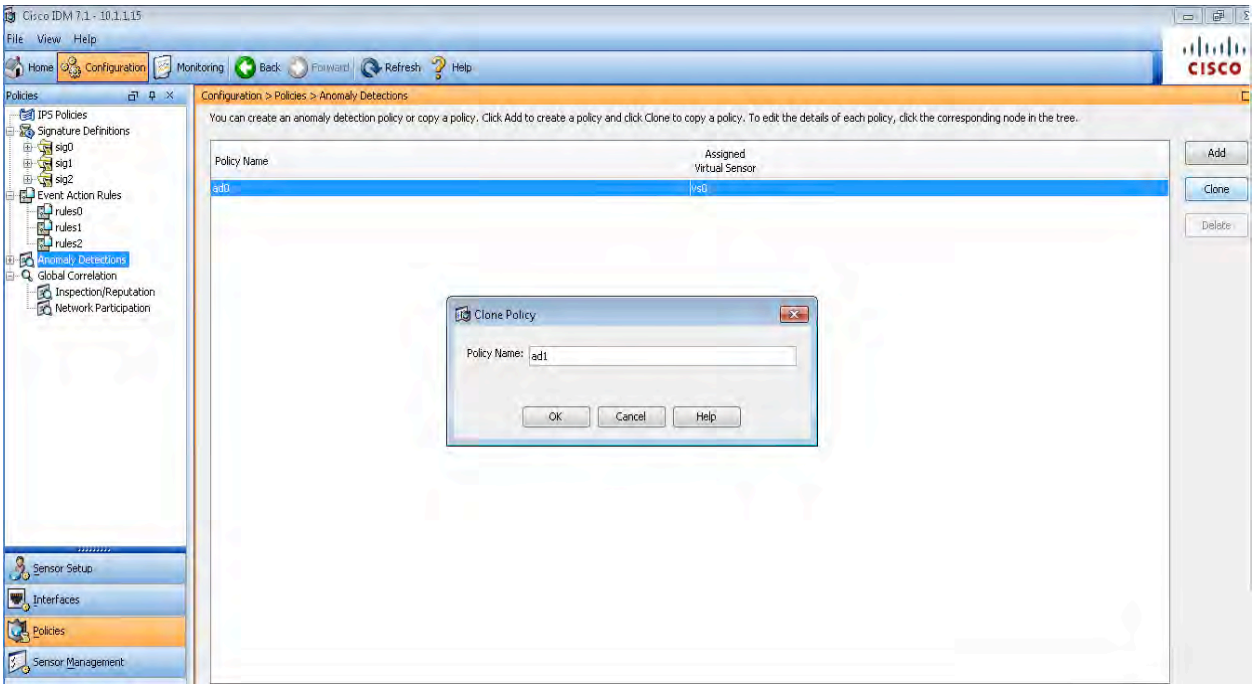
Carry out the same clone task for sig2.

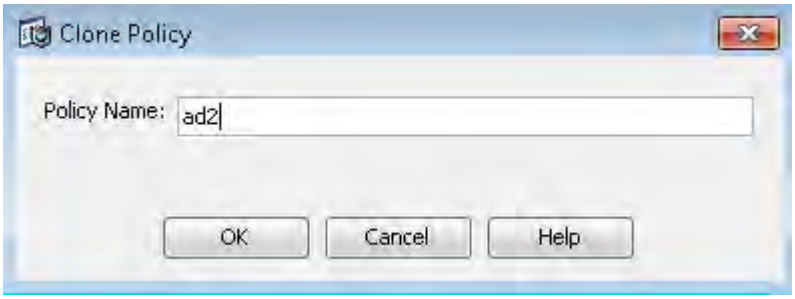
Then move to Event action rules and create both rules1 and rules2.



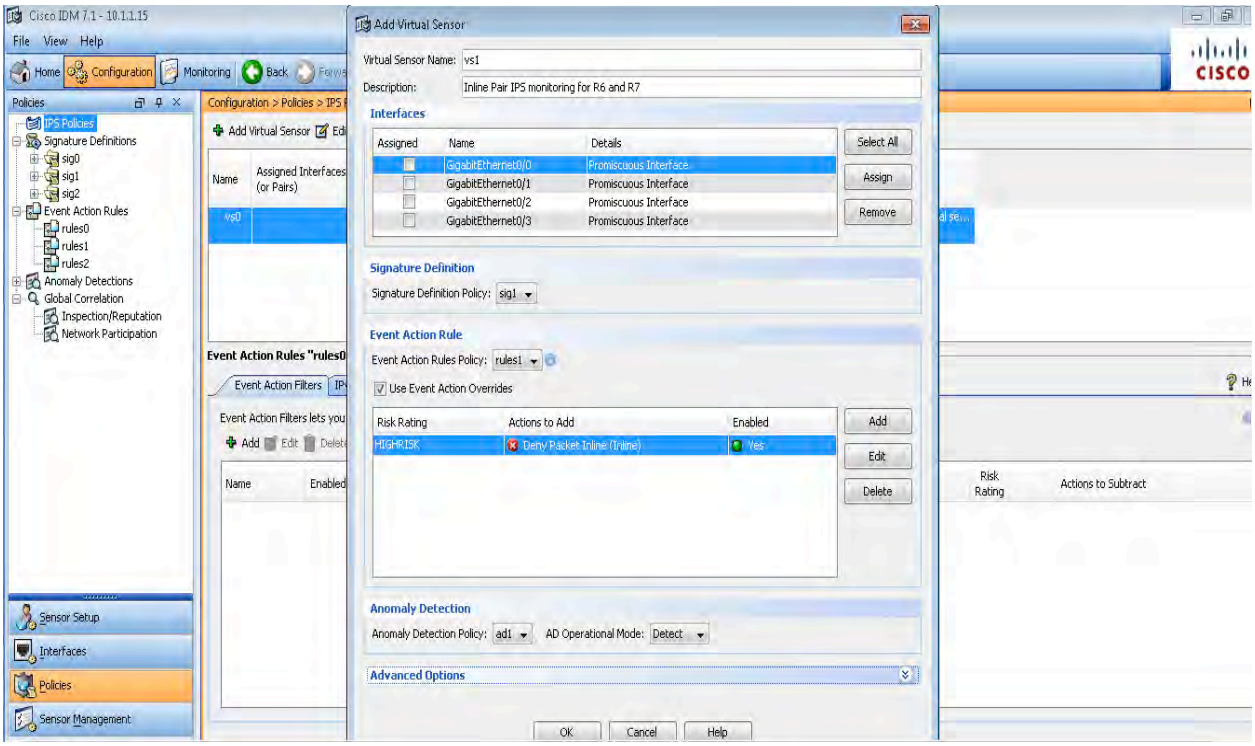


The final policy objects required are anomaly detection. Go to Configuration > Policies > Anomaly detections and clone ad0 to create both ad1 and ad2.

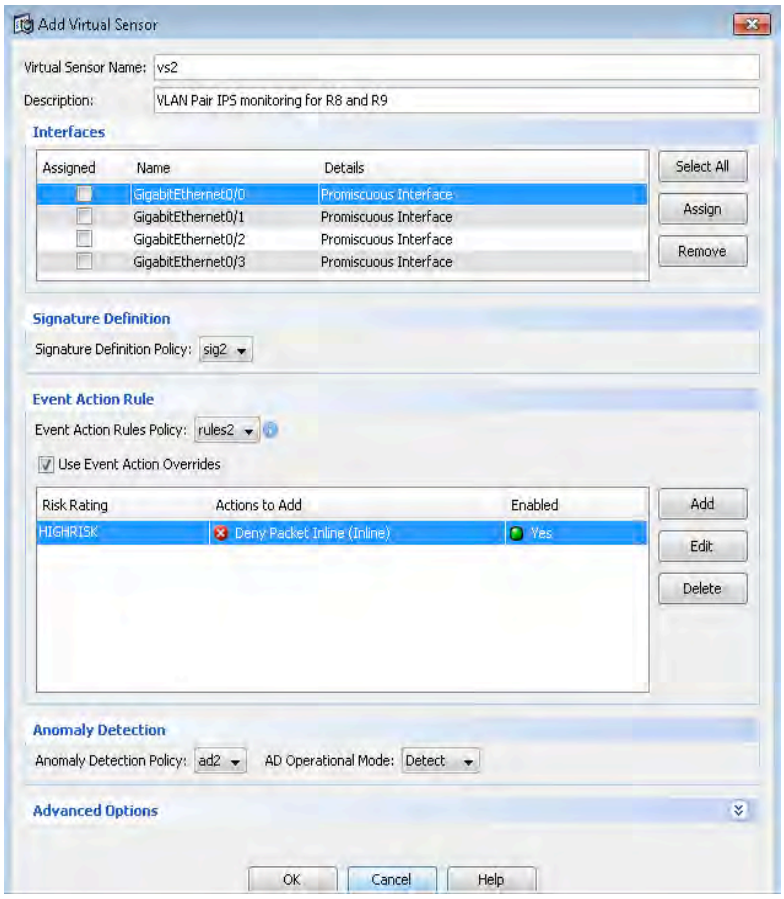




Go to Policies > IPS Policies click the Add Virtual Sensor button and define the vs1 virtual sensor, set the description and assign the newly created policy objects sig1, rules1 & ad1 to vs1.



Duplicate the above task to create vs2, remember to assign sig2,rules2 and ad2, and setting the description for the new virtual sensor.



If you havent jumped ahead and configured the interfaces for each virtual sensor you will see a warning message. This will be rectified in the upcoming tasks.

Notes

In this section we are asked to create virtual sensors on the appliance. This gives us the advantage of being able to apply different policies for different traffic flows types throughout the network. Version 7.x code gives us the ability to create upto 4 virtual sensors on the appliance.

Each IPS Policy is made up of 3 policy objects: Signature definitions, Event Actions Rules and Anomaly Detection. We need to create and assign a new set of these objects for each virtual sensor.
As we are asked to create exact copies of the vs0 objects for both vs1 and vs2 we need to Clone the existing sig, rules and ad, renaming accordingly.

Task 6: Monitoring Traffic with IDS

- Configure switches to copy all traffic between VLAN 4 and VLAN 5 to the Gi0/0 interface on the IPS sensor. If required, you may create VLAN 450 to complete this task.
- The sensor should be able to send TCP resets to VLAN 45.
- Configure interface Gi0/0 on the sensor to monitor traffic in promiscuous mode
- Add this interface to virtual sensor to vs0.
- Set the description to “IDS monitoring for R4 and R5”
- Enable the IP Echo Request and IP Echo Reply signatures under the default Signature Definition Policy.
- Tune the above two signatures so that they produce a medium-severity alert.
- Verify that pings between R4 & R 5 generate events. Also generate alerts with a severity of high fragmented ICMP packets.

Configuration

Cat2

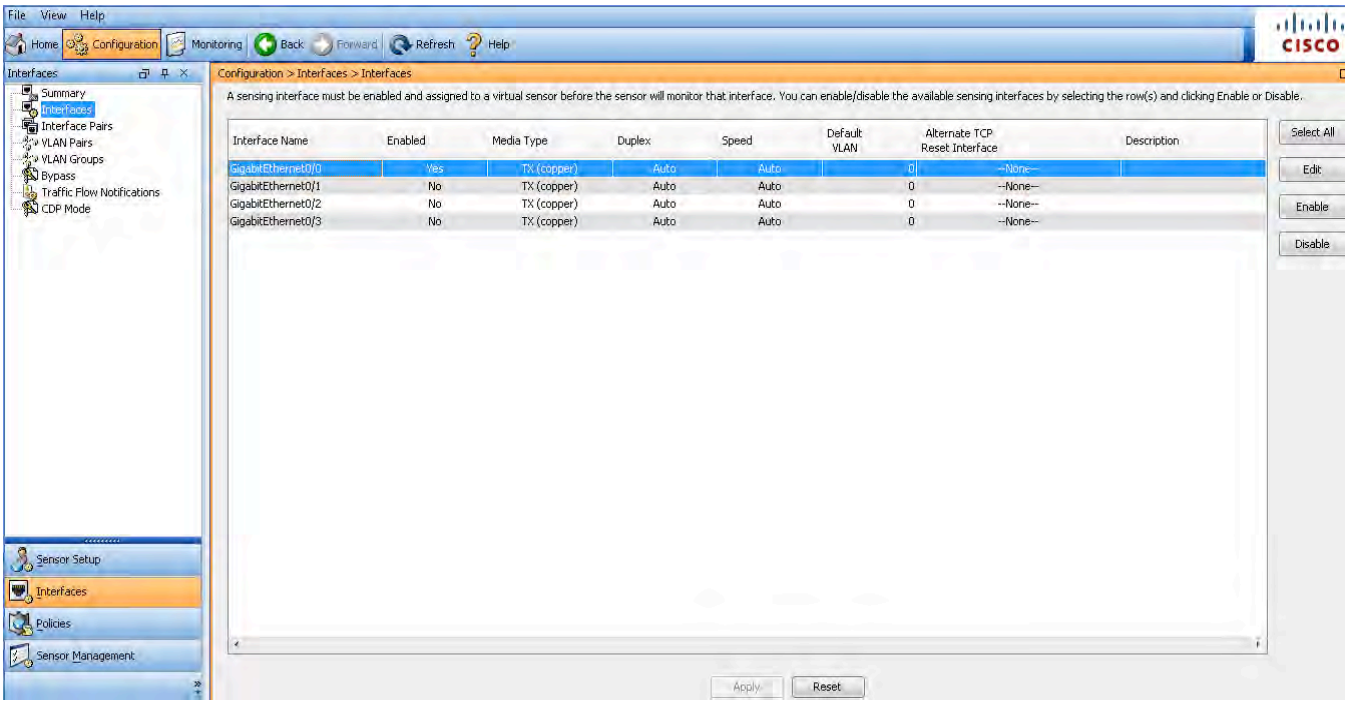
```
vlan 450
remote-span
monitor session 1 source vlan 45
monitor session 1 destination remote vlan 450
```

Cat4

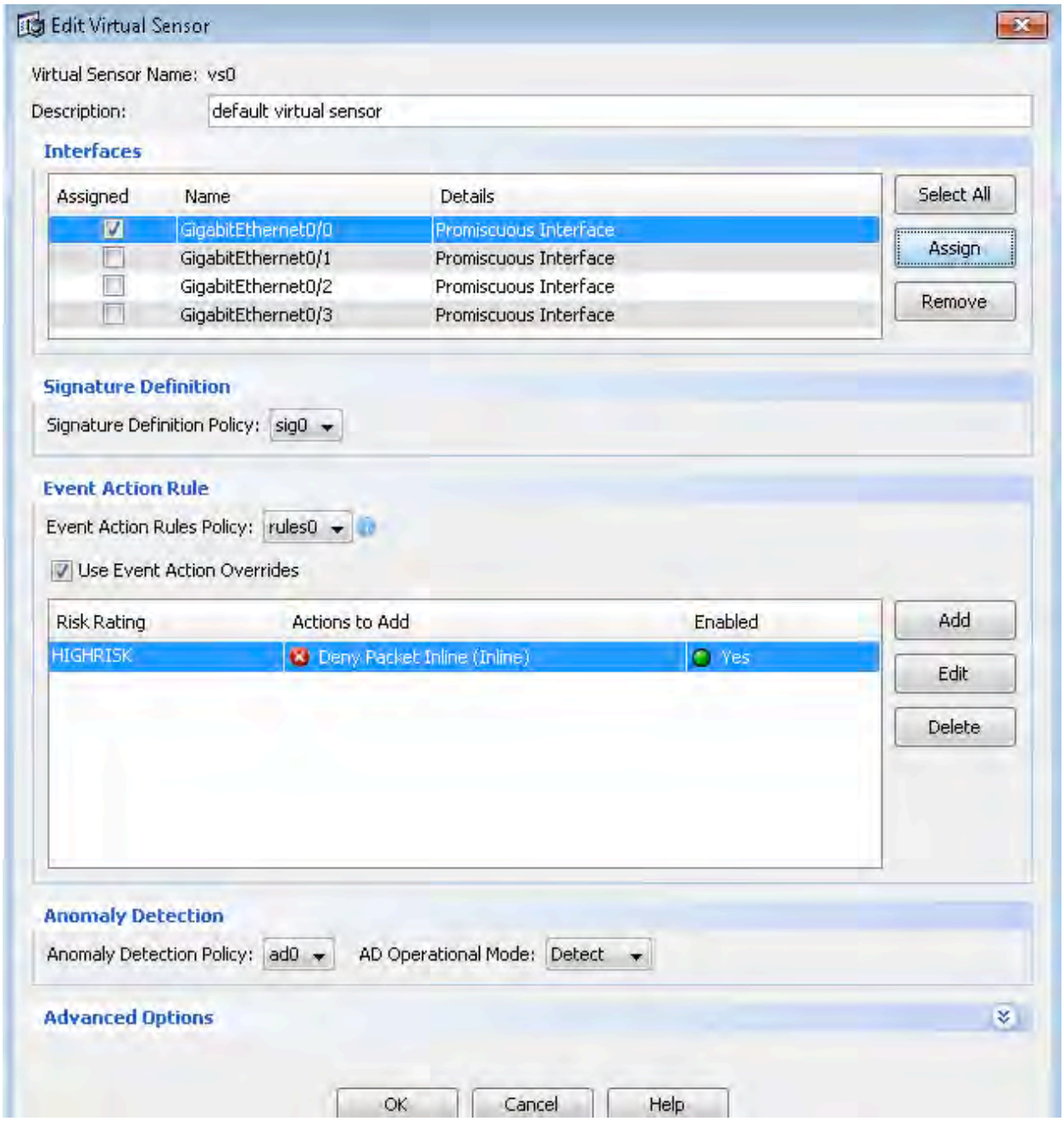
```
monitor session 1 source vlan 45 , 450
monitor session 1 destination interface g1/0/2 ingress vlan 45
```

IPS

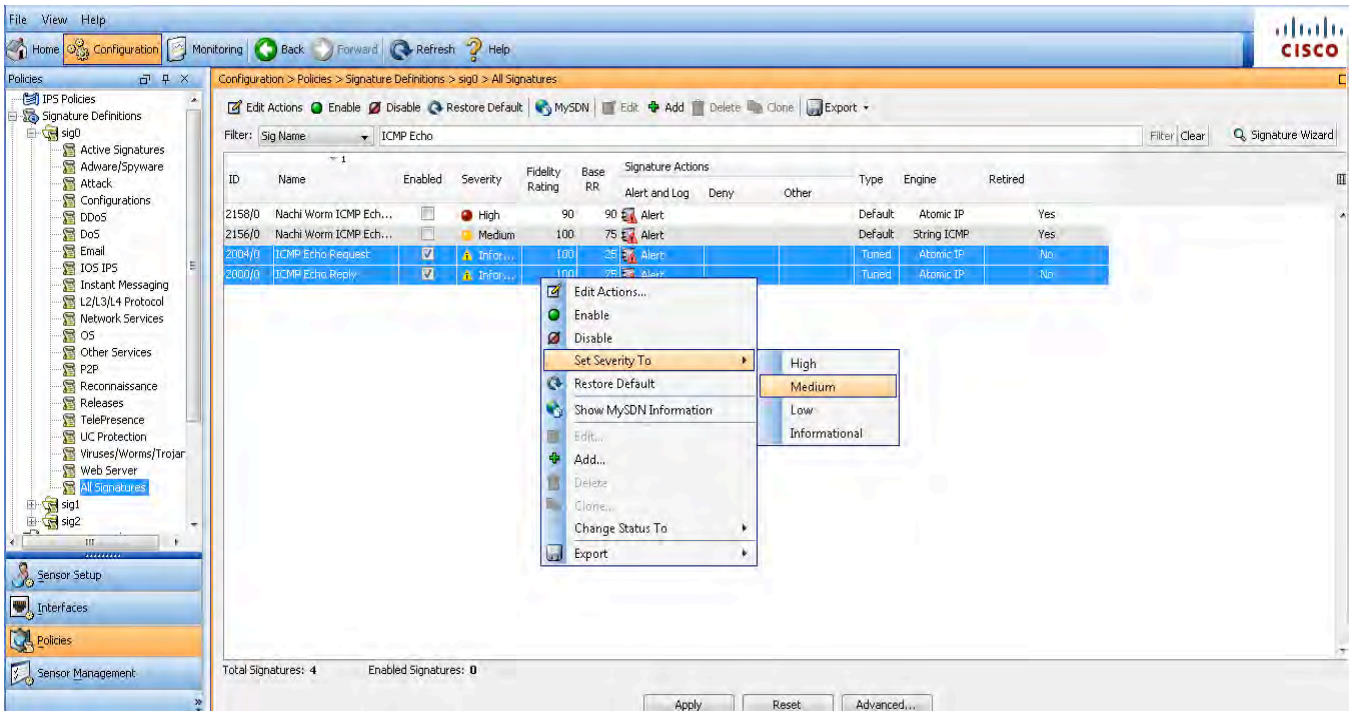
From the IDM, enable G0/0 by going to Configuration > Interfaces > Interfaces, select interface G0/0 and click the enable button.



We now need to assign the interface to vs0. Do this by going to Configuration > Policies > IPS Policies and editing vs0. Click the checkbox next to G0/0 and click the Assign button, then apply.



Go to Configuration > Policy > Signature Definitions > Sig0 > All Signatures. Search for the ICMP signatures, 2000 & 2004, under sig0 and set them to enabled and medium severity



Notes

In this question, we have implemented IDS promiscuous monitoring using remote span sessions between Cat 2 and 4, and the G0/0 interface of the appliance.
Adding the “ingress vlan” keywords to the monitor session destination allows us to send traffic back from the sensor via interface G0/0 to the specified vlan. This satisfies our requirement for sending TCP resets back to vlan 45.

Verification

The commands below highlight that vlan 450 has been successfully assigned to be a remote span vlan for Cat2 and Cat4.

```
Cat2#show vlan remote-span

Remote SPAN VLANs
------------------------------------------------------------------------------
450


Cat2#show vlan remote-span

Remote SPAN VLANs
------------------------------------------------------------------------------
450
Cat2#sh monitor session all
```

```
Session 1
---------
Type                   : Remote Source Session
Source VLANs           :
    Both               : 45
Dest RSPAN VLAN        : 450


Cat4#sh mon ses all
Session 1
---------
Type                   : Local Session
Source VLANs           :
    Both               : 45,450
Destination Ports      : Gi1/0/2
    Encapsulation      : Native
          Ingress      : Enabled, default VLAN = 45
    Ingress encap : Untagged
```

Cat4's G1/0/2 interface should now be showing as being in a promiscuous monitoring state

```
Cat4#show interfaces gigabitEthernet 1/0/2
GigabitEthernet1/0/2 is up, line protocol is down (monitoring)
  Hardware is Gigabit Ethernet, address is e02f.6d0c.4c82 (bia e02f.6d0c.4c82)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

As requested in the task, use icmp ping to verify that alerts are generated in the IDM event viewer. Do this by pinging across vlan 45 from R5 to R4 (or vice versa).

```
R5#ping 192.1.45.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.45.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms


IPS# show events


evIdsAlert: eventId=1368538386613477280 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/15 17:38:05 2013/04/15 13:38:05 GMT-05:00
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
```

```
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.45.5
    target:
      addr: locality=OUT 192.1.45.4
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85
  threatRatingValue: 85
  interface: ge0_0
  protocol: icmp


evIdsAlert: eventId=1368538386613477281 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/15 17:38:05 2013/04/15 13:38:05 GMT-05:00
  signature: description=ICMP Echo Reply id=2000 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.45.4
    target:
      addr: locality=OUT 192.1.45.5
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85
  threatRatingValue: 85
  interface: ge0_0
  protocol: icmp
```

Task 7: IPS Inline Interface Pair

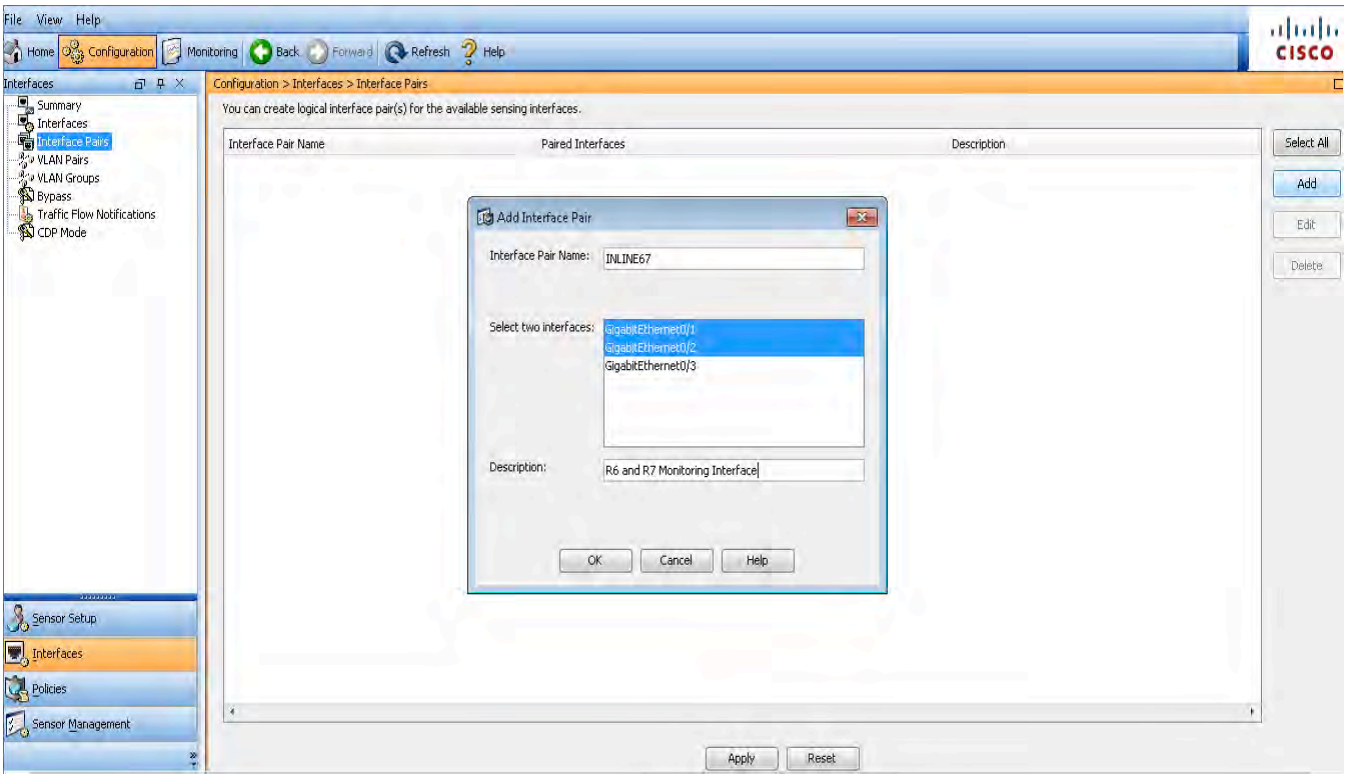
- Create a new inline interface on the sensor called INLINE67.
- Set the description to “R6 and R7 Monitoring Interface”.
- Add the ge0/1 and ge0/2 interfaces.
- R7 should belong to VLAN 670.
- Add the new interface to virtual sensor vs1.
- Verify that you can ping from R6 to R7.
- Verify that pings between R6 & R7 generate events. Also generate alerts with a severity of high fragmented ICMP packets.

Configuration

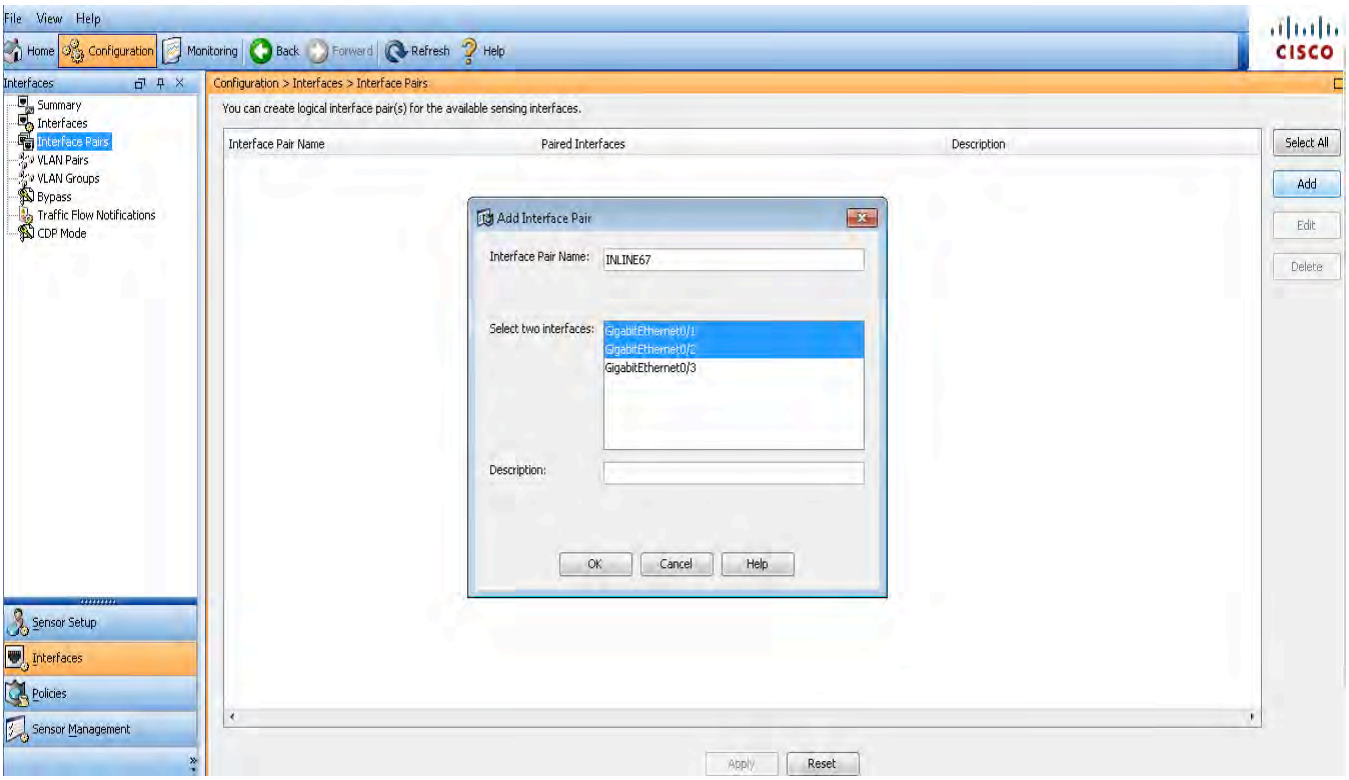
```
Cat4

vlan 670

interface GigabitEthernet1/0/3 (IPS G0/1)
 switchport access vlan 67
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/4 (IPS G0/2)
 switchport access vlan 670
 switchport mode access
 spanning-tree portfast

R7

int f0/1.67
encapsulation dot1Q 670
Cat2

int f0/7
switchport trunk allowed vlan add 670
switchport trunk allowed vlan remove 67
```

IPS

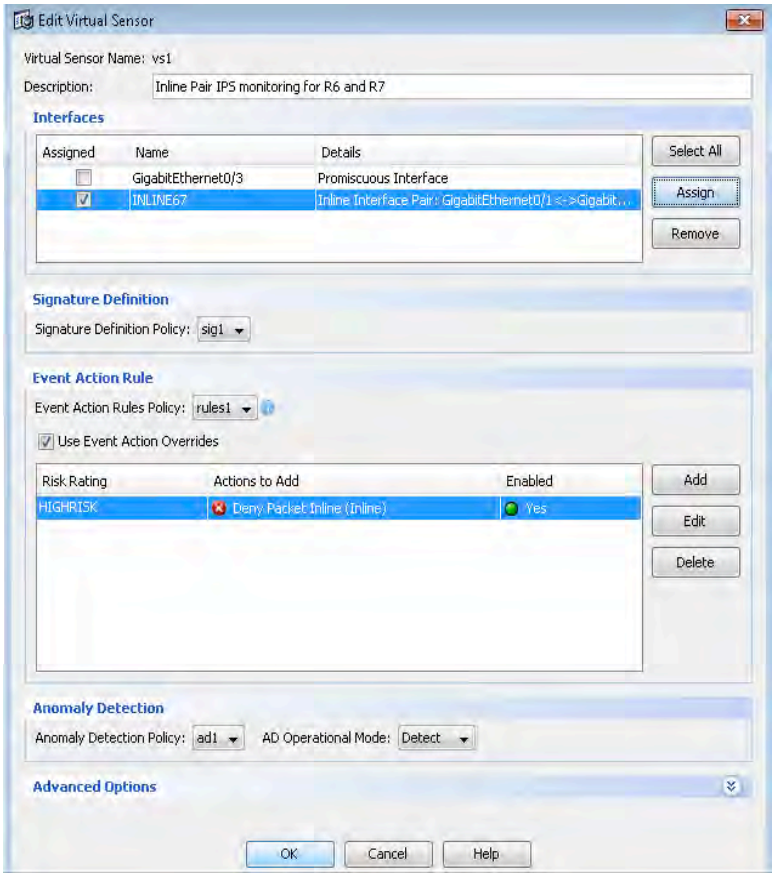
Enable the interfaces before attempting to create the Interface pair.



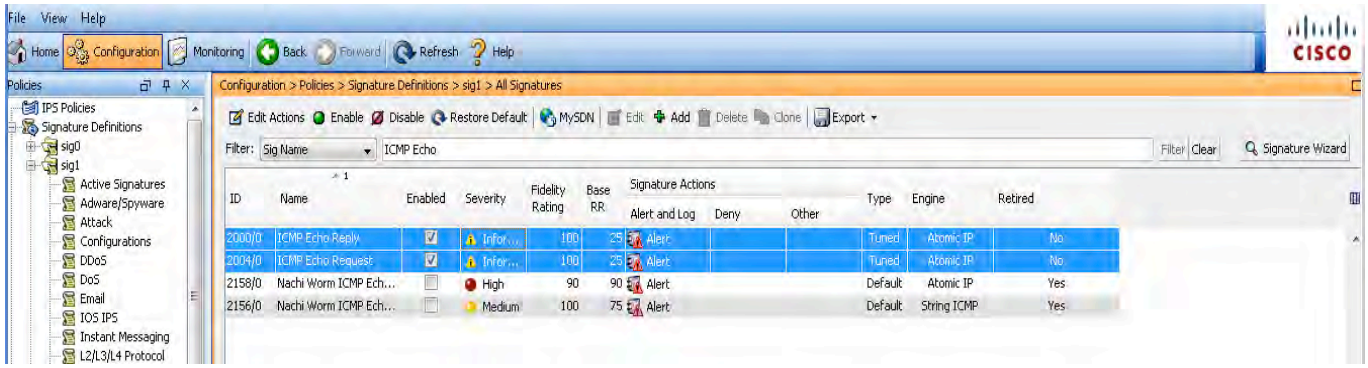
Create the Inline Interface Pair using G0/1 & G0/2.



Edit virtual sensor vs1 and assign the new inline pair to it.



As before, enable the icmp echo and echo reply signatures so we can verify the task has been completed successfully.

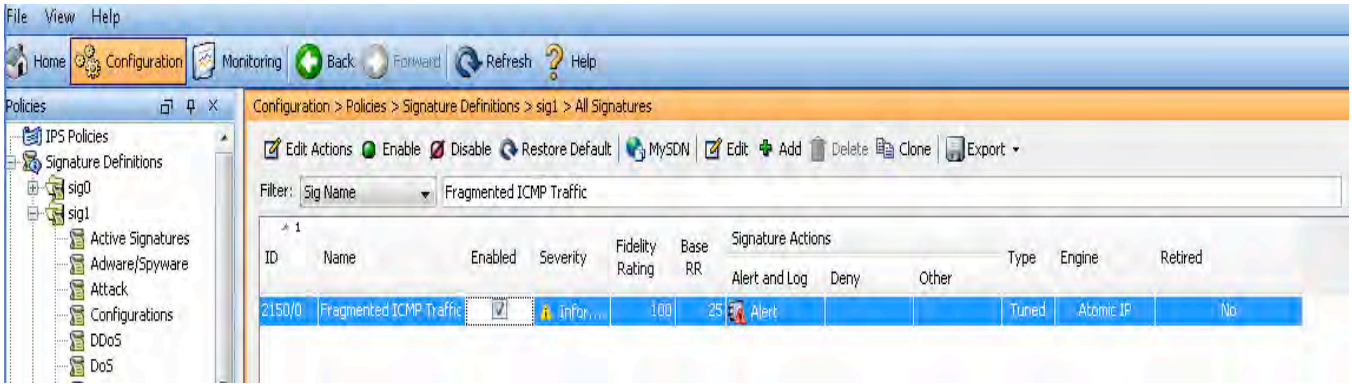


Verification

```
R7#ping 192.1.67.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.67.6, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

IPS# show events alert


evIdsAlert: eventId=1368538386613477530 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 09:51:54 2013/04/16 05:51:54 GMT-05:00
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.67.7
    target:
      addr: locality=OUT 192.1.67.6
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 35
  interface: ge0_2
  protocol: icmp


evIdsAlert: eventId=1368538386613477531 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 09:51:54 2013/04/16 05:51:54 GMT-05:00
  signature: description=ICMP Echo Reply id=2000 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.67.6
    target:
      addr: locality=OUT 192.1.67.7
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
```

```
  threatRatingValue: 35
  interface: ge0_1
  protocol: icmp
```



Enable signature 2150 i.e. Fragmented ICMP traffic and change the severity to high.

Verification

```
R7#ping 192.1.67.6 size 9000

Type escape sequence to abort.
Sending 5, 9000-byte ICMP Echos to 192.1.67.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

evIdsAlert: eventId=1368538386613477579 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 09:58:42 2013/04/16 05:58:42 GMT-05:00
  signature: description=Fragmented ICMP Traffic id=2150 created=20010202
type=anomaly version=S2
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs1
```

```
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.67.7
    target:
      addr: locality=OUT 192.1.67.6
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 65
  interface: ge0_2
  protocol: icmp
```

Notes

This task moves us into configuring the first of our virtual sensors, and utilizing the inline IPS functionality of the appliance. As we are using inline mode, we need to create a new vlan to insert the IPS inline between R6 and R7. First, Vlan 670 needs to be created. On Cat4 we then define G1/0/3 & 4 as access ports and assign them to vlans 67 and 670 respectively to bring the IPS inline. To ensure the traffic flows through the IPS the last thing we need to change R7's vlan to 670, on both the switchport and the vlan 67 sub interface on the router.

We then need to proceed to the IDM to enable the interfaces and create the Interface Pair, ensuring that it gets assigned to the correct virtual sensor (vs1). The ping generated with a size of 9000 gets dropped due to the default event action override.

Task 8: IPS Inline VLAN Pair

- Configure the port on Cat4 connecting to the sensor's ge0/3 interface to be a dot1q trunk.
- Configure this trunk port to only permit VLANs 89 and 890.
- Create a new sub-interface on the sensor's ge0/3 interface. Use sub-interface #89.
- Set the description to "R8 and R9 Monitoring Interface".
- Add the new interface to virtual sensor vs2.
- Verify that you can ping from R8 to R9.
- Verify that pings between R8 & R9 generate events. Also generate alerts with a severity of high fragmented ICMP packets.

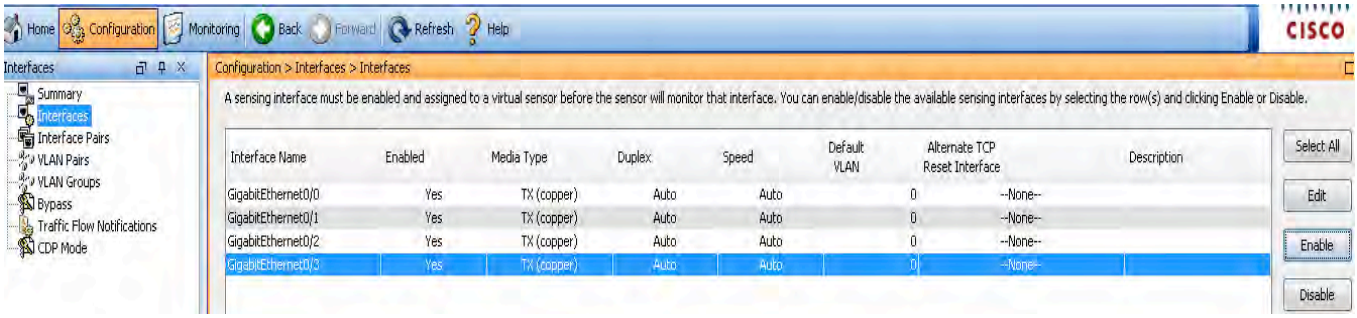
Configuration

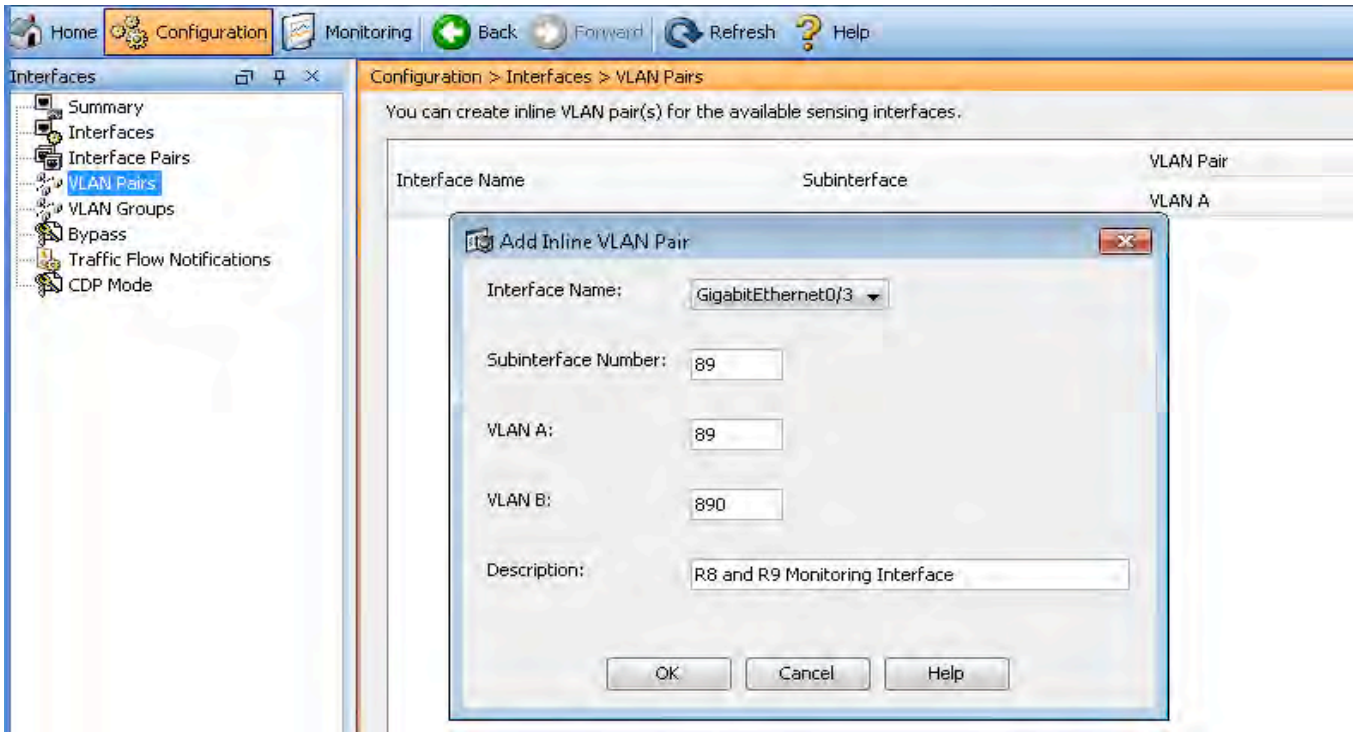
```
Cat4
Cat4(config)#vlan 890


Cat4
Cat4(config)#int g1/0/5
Cat4(config-if)#sw tru encap dot
```

```
Cat4(config-if)#sw mode trunk
Cat4(config-if)#sw trun allow vlan 89,890

Cat2
Cat2(config)#interface FastEthernet0/9
Cat2(config-if)#sw trun all vla remove 89
Cat2(config-if)#sw trun all vla add 890


R9
R9(config)#interface FastEthernet0/1.89
R9(config-subif)# encapsulation dot1Q 890
```

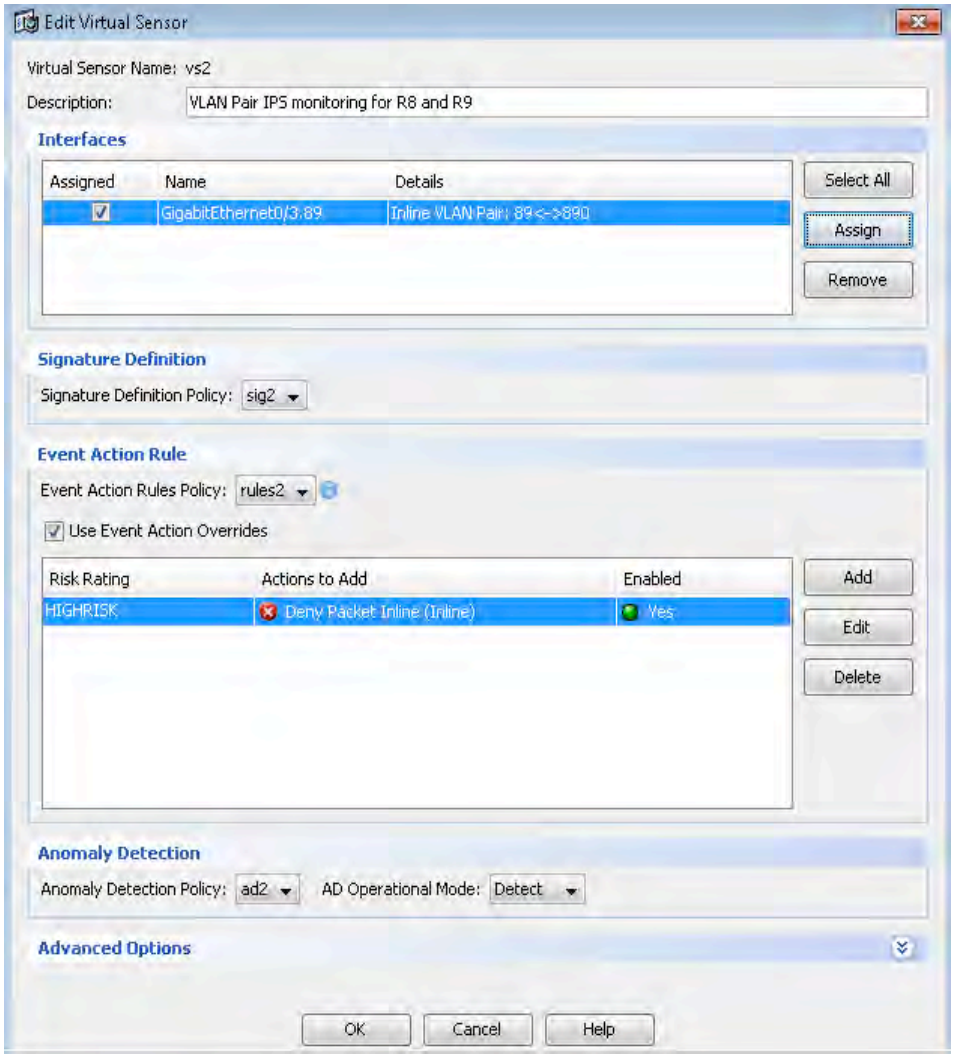
IPS

Enable Interface G0/3 as before and create a new Inline VLAN Pair, via Configuration > Interfaces > VLAN Pairs. Click Ok and apply the changes.

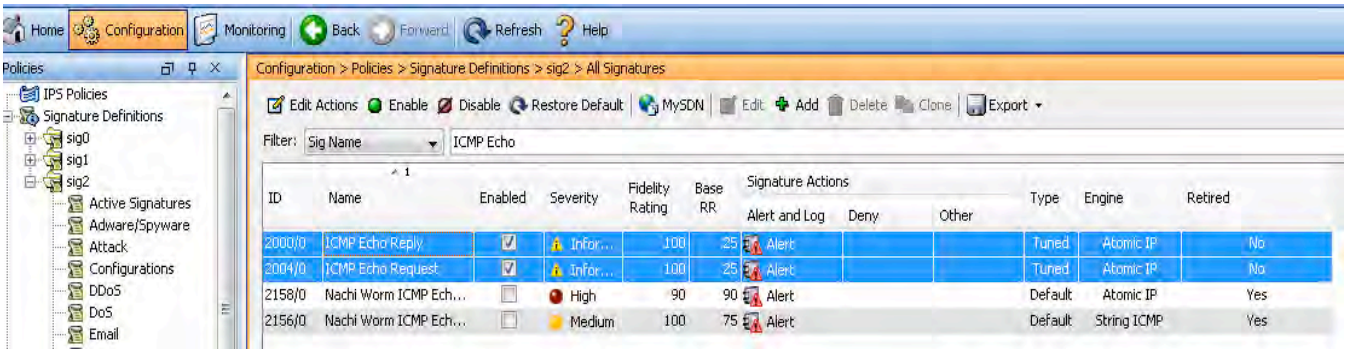




Next you assign the vlan pair to the sensor vs2.



Under Signature Definitions > sig2 enable the ICMP Echo and Echo Reply signatures.

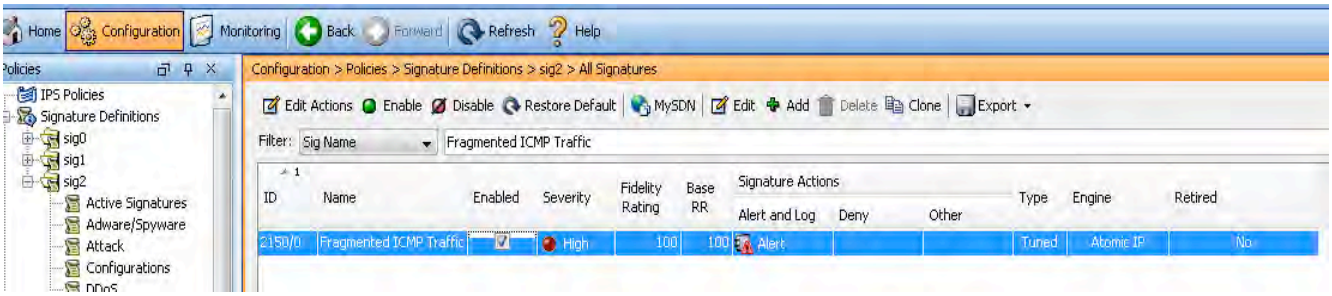


Verification

```
R9#ping 192.1.89.8 repeat 1

Type escape sequence to abort.
```

```
Sending 1, 100-byte ICMP Echos to 192.1.89.8, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
evIdsAlert: eventId=1368538386613477642 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 10:31:01 2013/04/16 06:31:01 GMT-05:00
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs2
  vlan: 890
  participants:
    attacker:
      addr: locality=OUT 192.1.89.9
    target:
      addr: locality=OUT 192.1.89.8
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 35
  interface: ge0_3
  protocol: icmp


evIdsAlert: eventId=1368538386613477643 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 10:31:01 2013/04/16 06:31:01 GMT-05:00
  signature: description=ICMP Echo Reply id=2000 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs2
  vlan: 89
  participants:
    attacker:
      addr: locality=OUT 192.1.89.8
    target:
      addr: locality=OUT 192.1.89.9
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
  threatRatingValue: 35
  interface: ge0_3
  protocol: icmp
```

Enable signature 2150 i.e. Fragmented ICMP traffic and change the severity to high.



Verification

```
R9#ping 192.1.89.8 repeat 1 size 5000

Type escape sequence to abort.
Sending 1, 5000-byte ICMP Echos to 192.1.89.8, timeout is 2 seconds:
.
Success rate is 0 percent (0/1)

evIdsAlert: eventId=1368538386613477647 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 10:32:20 2013/04/16 06:32:20 GMT-05:00
  signature: description=Fragmented ICMP Traffic id=2150 created=20010202
type=anomaly version=S2
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs2
  vlan: 890
  participants:
    attacker:
      addr: locality=OUT 192.1.89.9
    target:
      addr: locality=OUT 192.1.89.8
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 65
  interface: ge0_3
  protocol: icmp
```

Notes

This section included the secondary method for Inline IPS configuration using Vlan Pairs.

To bring the IPS inline between R8 & R9 we need to once again create another vlan to use on R9's side of the IPS and reconfigure Cat2 interfaces F0/9, Cat4's G1/0/5 and R9's F0/1.89 to utilize the newly created vlan 890.

We then need to enable interface g0/3 on the IPS and use it to create the Vlan pair. As per the question the description should be added as well as using 89 for the sub interface number.
Remember when adding the interface that it is assigned to the vs2 sensor.
Finally enable ICMP Echo and Echo Reply signatures under vs2 to confirm connectivity and alerts are being received.

Task 9: Tuning Signatures, Variables and Custom Signatures

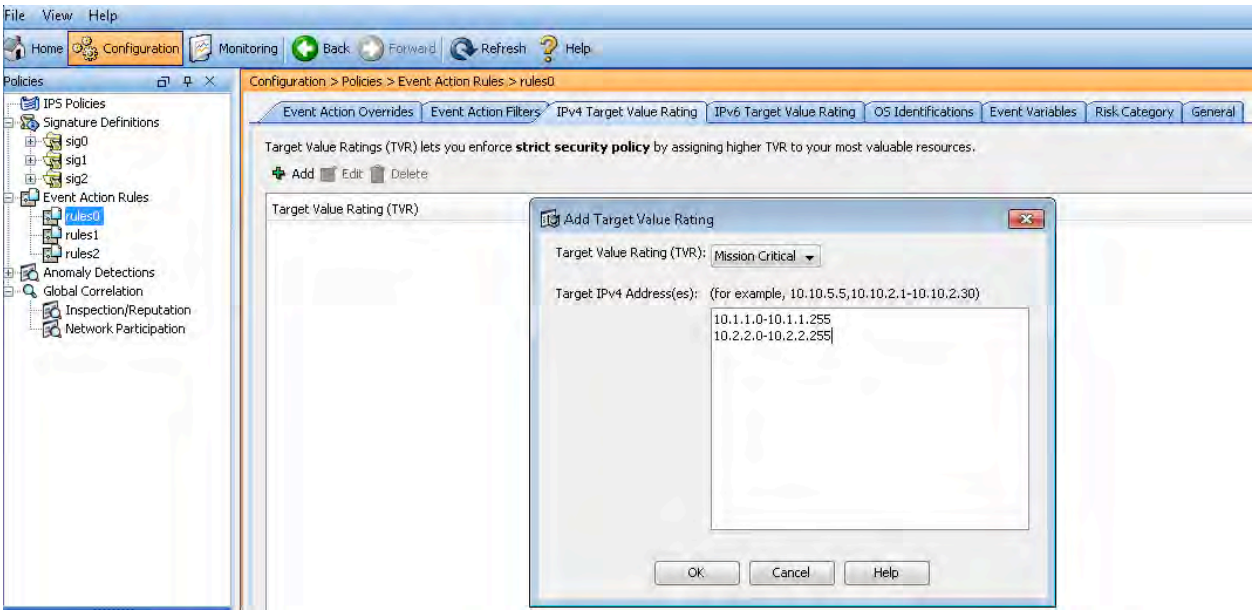
- For each of the Virtual Sensors make sure that the networks behind the ASA are viewed with the highest priority.

Configuration

IPS

Tuning signatures on a per-interface basis is easy when the interfaces in question belong to different virtual sensors. This allows each interface to be governed by a different detection/prevention policy.

Here we set the networks behind the ASA, Vlans 10 & 20, a Target Value Rating of Mission Critical. This needs to be repeated for rules1 and rules2



Verification

Ping from R9 to R1 and check the target value rating

```
R9#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
evIdsAlert: eventId=1368538386613477685 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 11:03:29 2013/04/16 07:03:29 GMT-05:00
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs2
  vlan: 890
  participants:
    attacker:
      addr: locality=OUT 192.1.89.9
    target:
      addr: locality=OUT 10.1.1.1
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=mission-critical
60
  threatRatingValue: 60
  interface: ge0_3
  protocol: icmp
```

Notes

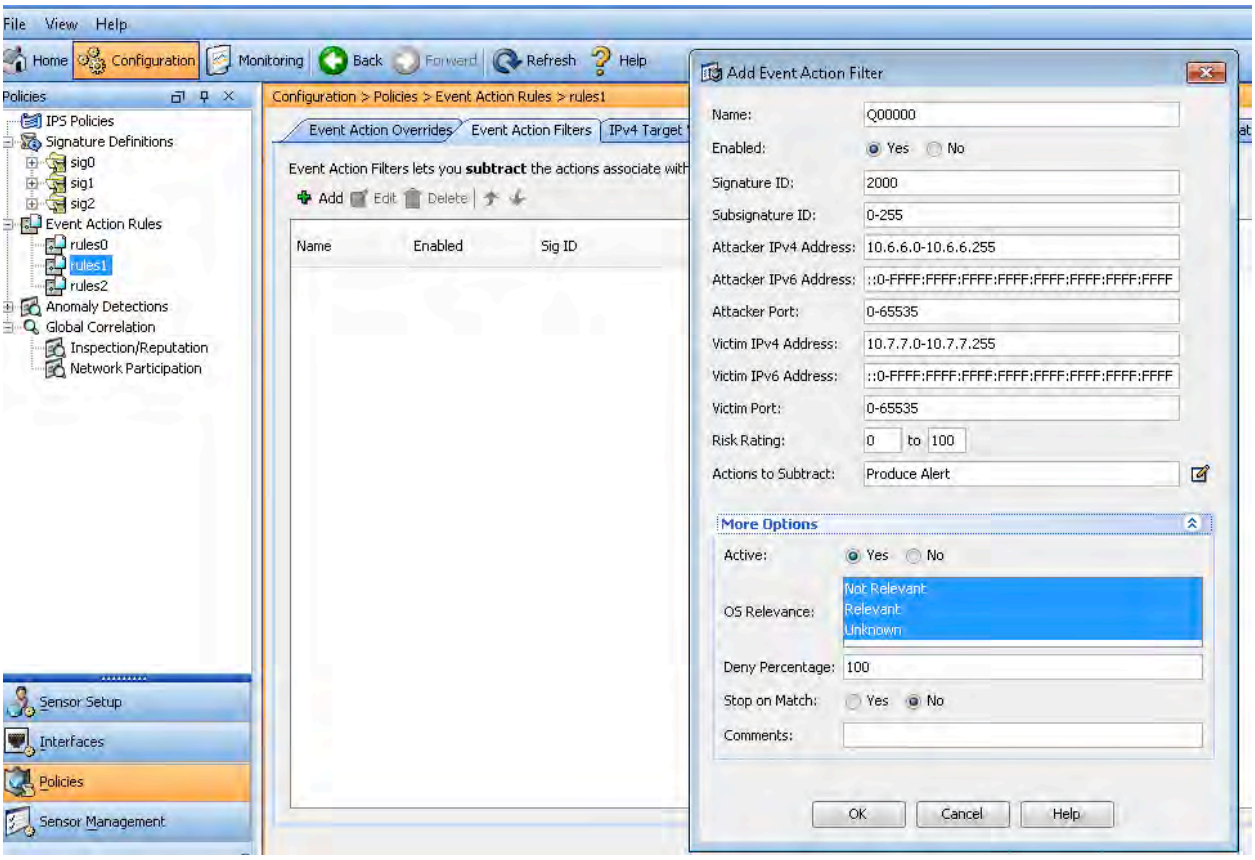
To adjust the IPS's perceived priority of a particular network or host, we need to adjust its target value rating. This can be manually achieved by modifying the rules policy for the virtual sensor.
The task requires us to have the IPS rate the networks behind the ASA (Vlan 10 & 20) with the highest priority, which is Mission Critical, this effectively applies a maximum risk rating of 100 to any events triggered for these networks.

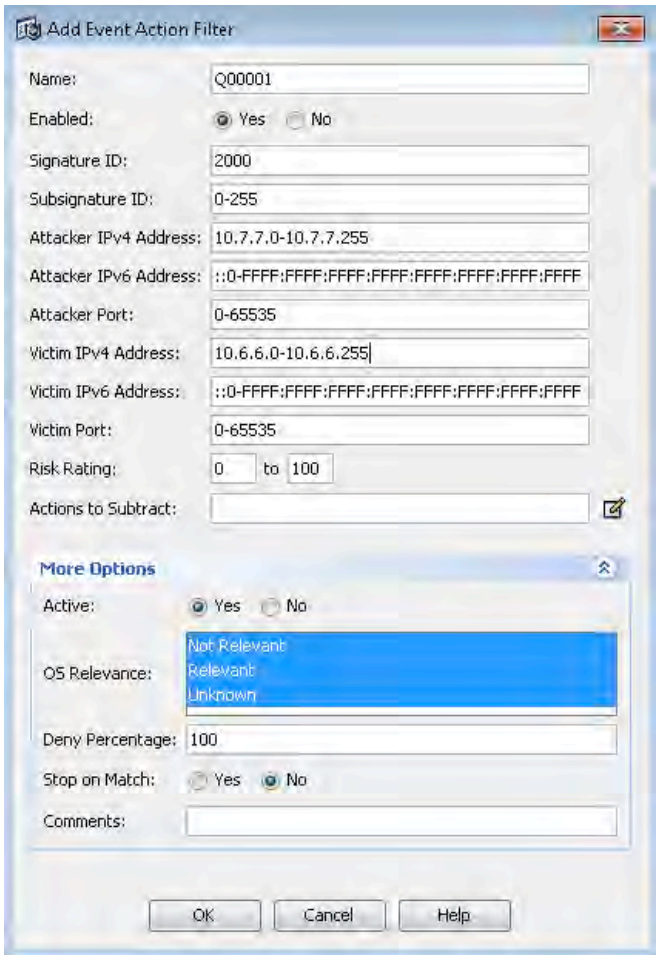
- In the previous sections you tuned the signatures for ICMP Pings. For traffic between VLAN 6 and VLAN 7, tune the Echo Request signature to generate a high-severity event, and for Echo Replies to not generate an event at all.

Configuration

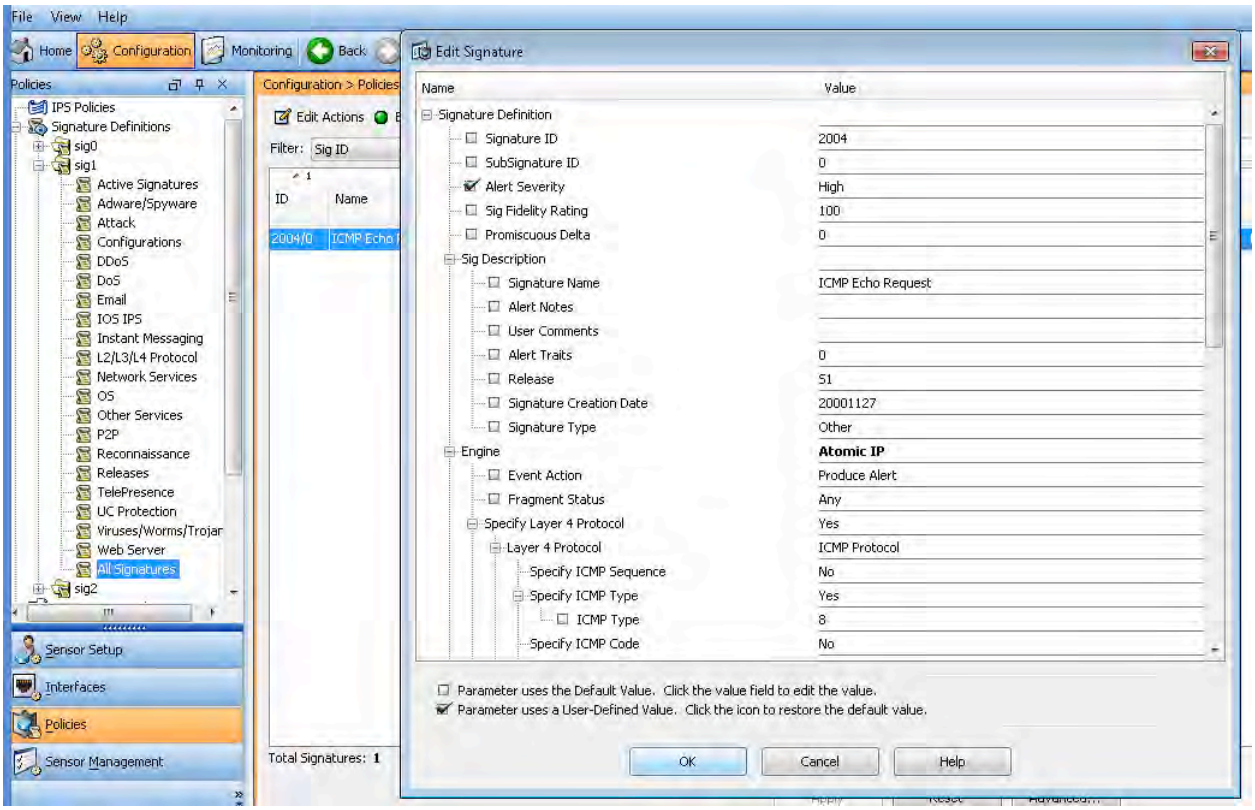
IPS

To disable the echo reply alerts we need to create two event action filters for bidirectional traffic between vlan 6 & 7, under vs1. The action will be to remove Produce Alert.





Under sig1 definitions find Sig 2004 ICMP Echo request and change the severity to High.



Verification

Note that when we ping between Vlan 6 & 7 (and vice versa), the pings now fail and we now get a high-priority event for the Echo Request, and no event at all for the Echo Reply. Due to the event action override a high risk rating will automatically apply a Deny Packet Inline action to the triggered event. Pings between VLANs 4 and 5 and VLANs 8 and 9 will continue to generate events as before, since they belong to different virtual sensors.

```
R6#ping 10.7.7.7 sou f0/1.6 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 10.6.6.6
.
Success rate is 0 percent (0/1)


evIdsAlert: eventId=1368538386613477689 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 11:06:04 2013/04/16 07:06:04 GMT-05:00
```

```
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.6.6.6
    target:
      addr: locality=OUT 10.7.7.7
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 65
  interface: ge0_1
  protocol: icmp

R7#ping 10.6.6.6 sou f0/1.7 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 10.7.7.7
.
Success rate is 0 percent (0/1)

evIdsAlert: eventId=1368538386613477690 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 11:07:15 2013/04/16 07:07:15 GMT-05:00
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.7.7.7
    target:
      addr: locality=OUT 10.6.6.6
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 65
```

```
interface: ge0_2
protocol: icmp
```

Notes

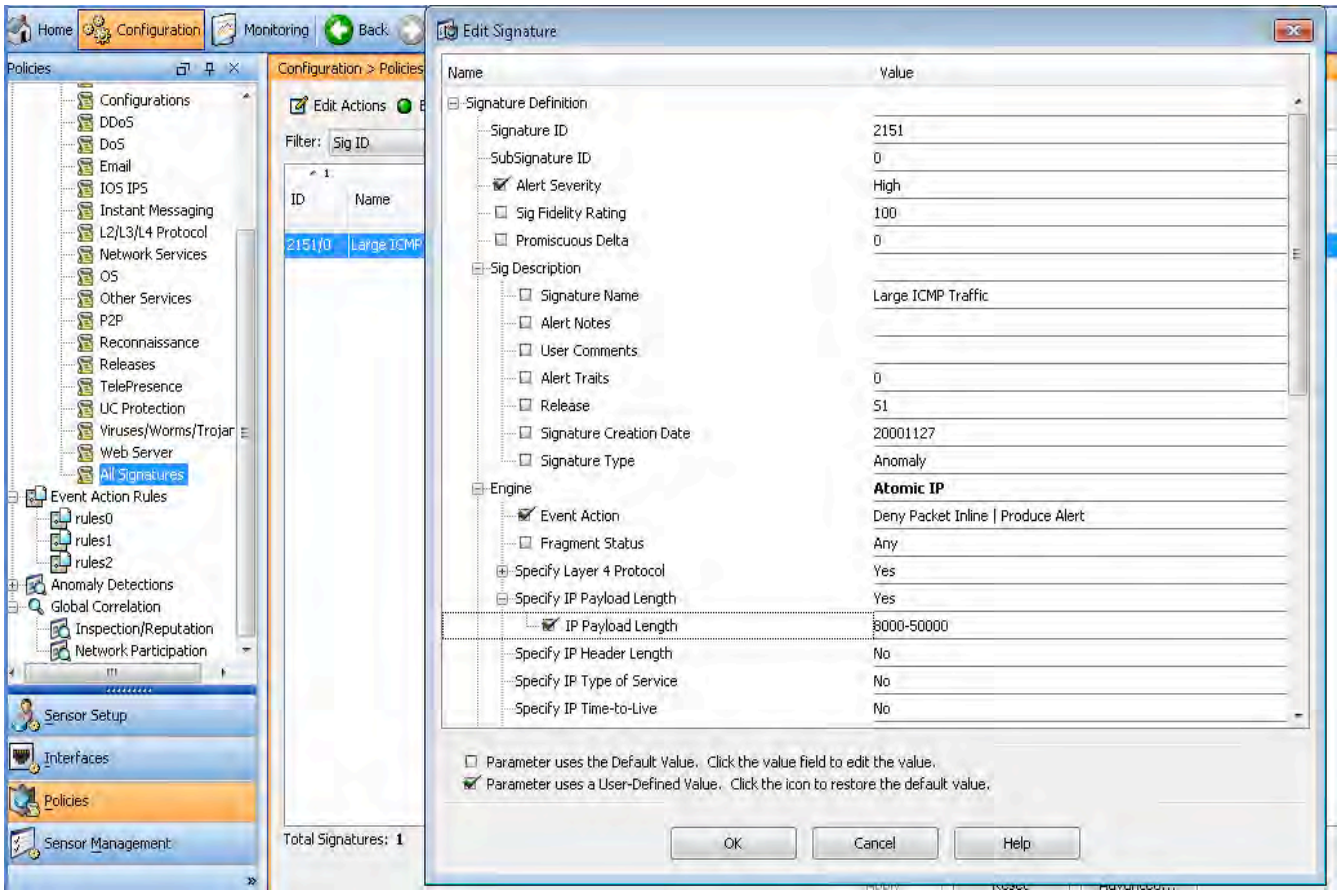
For the second bullet task, we need to do a couple things. First it's asking for echo requests to trigger high alerts, meaning the severity needs to be changed. Second, we need to not produce alerts for echo replies between Vlan 6 & 7. This is done using event actions filters which allows you to selectively subtract certain actions from events, based on customized traffic flows. This requires us to create 2 filters, one from vlan 6 to vlan 7, and the other from vlan 7 to vlan 6, subtracting the produce alert action in the process. As we have high severity enabled for icmp echo the ping will now fail, based on the high risk rating being applied, which by default applies the deny packet inline action.

- Configure an existing signature that will fire a high severity alert when ICMP packets with a size of between 8000-50000 bytes, are detected between R8 & R9. Drop the packet inline. The alert should fire every 4th event, and be summarized every 5th event.

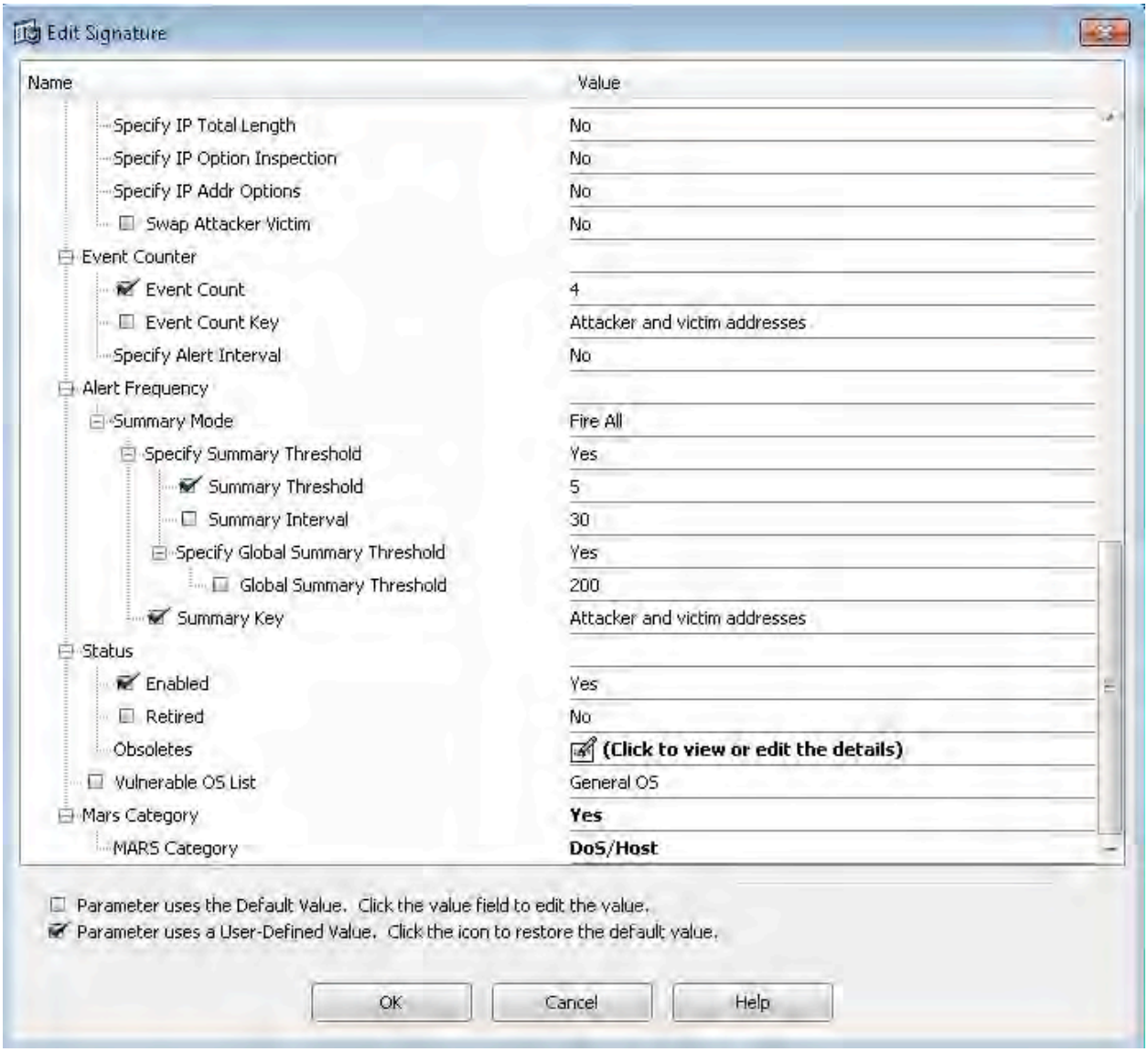
Configuration

IPS

Large ICMP has a signature id of 2151. Note the green ticks represent the settings we have changed. Here you see we have set the severity to high, event action to include Deny Packet Inline, and the IP Payload Length to the specified requirements.



Scrolling down the edit signature window, we modify the event count to 4, the summary threshold to 5 and enable the signature.



Verification

```
Disable signature 2050 and test

R8#ping 10.9.9.9 size 8020 repeat 50

Type escape sequence to abort.
Sending 50, 8020-byte ICMP Echos to 10.9.9.9, timeout is 2 seconds:
!!!..!!.!.!.!!..!!!..!!.!.!.!!..!!!..!!.!.!.!!..!!
Success rate is 58 percent (29/50), round-trip min/avg/max = 8/9/12 ms


evIdsAlert: eventId=1368538386613477991 severity=high vendor=Cisco
  originator:
    hostId: IPS
```

```
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:25:55 2013/04/16 08:25:55 GMT-05:00
  signature: description=Large ICMP Traffic id=2151 created=20001127 type=anomaly
version=S1
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs2
  vlan: 89
  participants:
    attacker:
      addr: locality=OUT 192.1.89.8
    target:
      addr: locality=OUT 10.9.9.9
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 65
  interface: ge0_3
  protocol: icmp


evIdsAlert: eventId=1368538386613477992 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:25:57 2013/04/16 08:25:57 GMT-05:00
  signature: description=Large ICMP Traffic id=2151 created=20001127 type=anomaly
version=S1
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs2
  vlan: 890
  participants:
    attacker:
      addr: locality=OUT 10.9.9.9
    target:
      addr: locality=OUT 192.1.89.8
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 65
  interface: ge0_3
  protocol: icmp
```

```
evIdsAlert: eventId=1368538386613478009 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:26:57 2013/04/16 08:26:57 GMT-05:00
  signature: description=Large ICMP Traffic id=2151 created=20001127 type=anomaly
version=S1
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs2
  vlan: 89
  participants:
    attacker:
      addr: locality=OUT 192.1.89.8
    target:
      addr: locality=OUT 10.9.9.9
      os: idSource=unknown relevance=relevant type=unknown
  summary: final=true initialAlert=0 summaryType=Regular 3
  alertDetails: Regular Summary: 3 events this interval ;
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 100
  interface: ge0_3
  protocol: icmp


evIdsAlert: eventId=1368538386613478010 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:26:59 2013/04/16 08:26:59 GMT-05:00
  signature: description=Large ICMP Traffic id=2151 created=20001127 type=anomaly
version=S1
    subsigId: 0
    marsCategory: DoS/Host
  interfaceGroup: vs2
  vlan: 890
  participants:
    attacker:
      addr: locality=OUT 10.9.9.9
    target:
      addr: locality=OUT 192.1.89.8
      os: idSource=unknown relevance=relevant type=unknown
  summary: final=true initialAlert=0 summaryType=Regular 2
  alertDetails: Regular Summary: 2 events this interval ;
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 100
  threatRatingValue: 100
  interface: ge0_3
```

```
protocol: icmp
```

The third sub task sees us utilizing the existing Large ICMP signature. We need to modify a few settings here. A couple to mention are: The event count which sets our trigger interval to only fire every four events, and the summary threshold which summarizes the alerts every five triggered events. So in our case, the IPS would need to detect four large icmp packets before the first event was fired and 20 large icmp packets for the first summary alert.

When presented with these packet size task requirements be sure to choose the right setting. For instance if asked to check on a variable packet length, set the range value under the 'IP Payload Length.' It's easy to get confused and choose the 'Total Length' setting, which only matches on the exact value specified, not greater than or equal to the value.

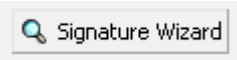
The final little gotcha here is remembering that we are matching on the IP PAYLOAD length, so when pinging across the IPS to trigger the event remember to include the IP header length of 20 in the byte size. So the minimum size would be 8020. To test it we also need to disable the ICMP fragmented packet signature (2050).

- Configure the sensor to block traffic between R7 and R8 if it detects the Code Red Worm traffic hitting a web server on VLAN 8. For the purpose of this task, consider URLs containing any of the following, to be Code Red traffic: "cmd.exe" "default.ida" or "root.exe". This task should account for the URL's using any case. Send an SNMP trap when this event is generated.

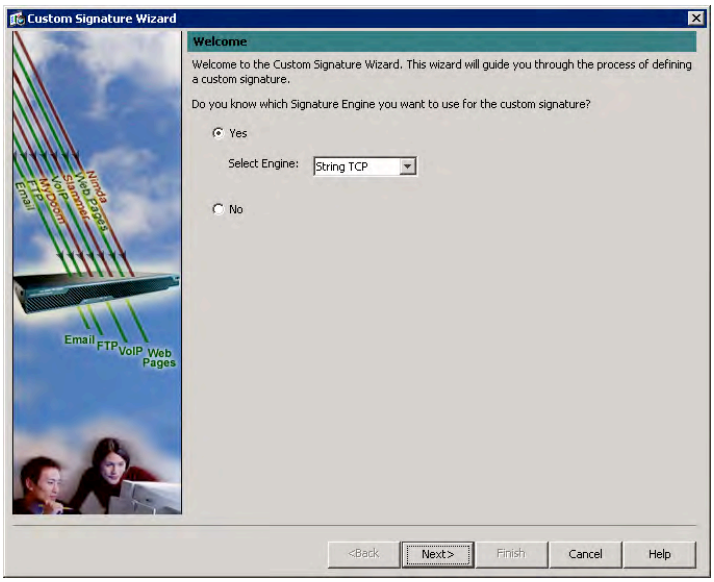
Configuration

IPS

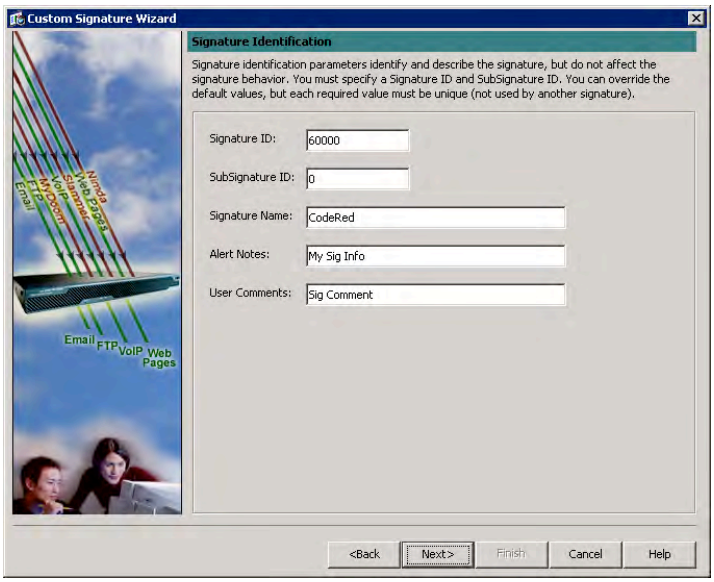
Here we need to create a new custom signature, within vs1. This is done using the Signature Wizard in the top right corner of sig1 > All Signatures.



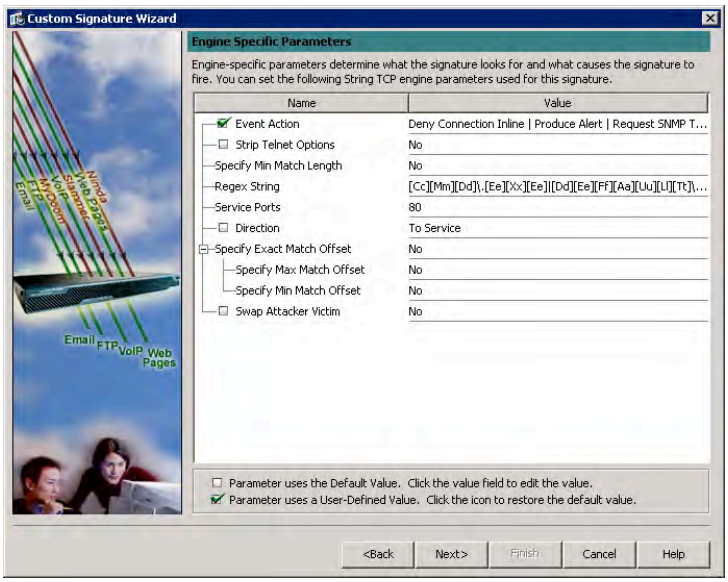
Here we need to create a new custom signature, within vs1. This is done using the Signature Wizard in the top right corner of sig1 > All Signatures.



Select String TCP as the engine.

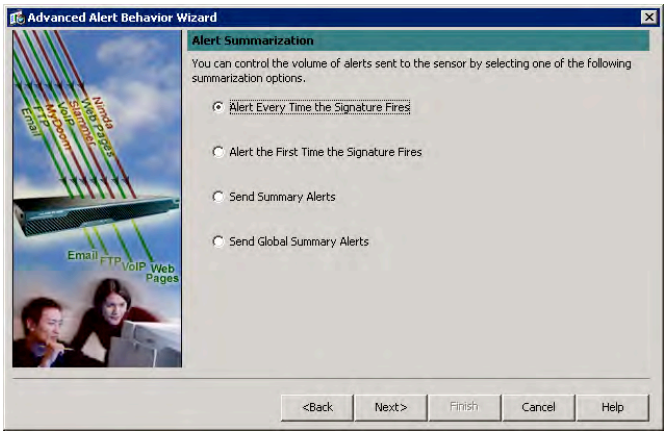


Give the new signature a meaningful name.



Add the required actions, service port of 80 for http and the regex string to match on.

[Cc][Mm][Dd]\.[Ee][Xx][Ee]|[Dd][Ee][Ff][Aa][Uu][Ll][Tt]\.[Ii][Dd][Aa]|[Rr][Oo][Oo][Tt]\.[Ee][Xx][Ee]



From the advanced wizard settings select to Alert on every fired event.
Accept all other defaults and click finish and apply.

Verification

```
R8(config)#ip http server
```

From R7 do a simple http copy to verify the sig is working. The first copy is an example of a non IPS blocked test.

```
R7#copy http://192.1.24.8/test null0
Destination filename [null0]?
%Error opening http://192.1.24.8/test (No such file or directory)
R7#
```

```
R7#copy http://192.1.24.8/cmd.exe null0
Destination filename [null0]?
%Error opening http://192.1.24.8/cmd.exe (I/O error)
R7#

evIdsAlert: eventId=1368538386613478039 severity=medium vendor=Cisco
alarmTraits=2147483648
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:48:19 2013/04/16 08:48:19 GMT-05:00
  signature: description=CodeRed id=60000 created=20000101 type=other version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.67.7
      port: 45073
    target:
      addr: locality=OUT 192.1.24.8
      port: 80
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedFlow: true
    snmpTrapRequested: true
  context:
    fromAttacker:
000000  47 45 54 20 2F 63 6D 64  2E 65 78 65 20 48 54 54  GET /cmd.exe HTT
000010  50 2F 31 2E 31 0D 0A 55  73 65 72 2D 41 67 65 6E  P/1.1..User-Agen
000020  74 3A 20 63 69 73 63 6F  2D 49 4F 53 0D 0A 48 6F  t: cisco-IOS..Ho
000030  73 74 3A 20 31 39 32 2E  31 2E 32 34 2E 38 0D 0A  st: 192.1.24.8..
000040  44 61 74 65 3A 20 54 68  75 2C 20 31 36 20 4D 61  Date: Thu, 16 Ma
000050  79 20 32 30 31 33 20 31  32 3A 35 30 3A 34 36 20  y 2013 12:50:46
000060  47 4D 54 0D 0A 43 6F 6E  6E 65 63 74 69 6F 6E 3A  GMT..Connection:
000070  20 4B 65 65 70 2D 41 6C  69 76 65 0D 0A 0D 0A      Keep-Alive....
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
  threatRatingValue: 31
  interface: ge0_2
  protocol: tcp

R7#copy http://192.1.24.8/rOoT.exe null0
Destination filename [null0]?
%Error opening http://192.1.24.8/rOoT.exe (I/O error)
R7#
```

```
evIdsAlert: eventId=1368538386613478040 severity=medium vendor=Cisco
alarmTraits=2147483648
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:50:31 2013/04/16 08:50:31 GMT-05:00
  signature: description=CodeRed id=60000 created=20000101 type=other version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.67.7
      port: 47710
    target:
      addr: locality=OUT 192.1.24.8
      port: 80
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedFlow: true
    snmpTrapRequested: true
  context:
    fromAttacker:
000000  47 45 54 20 2F 72 4F 6F  54 2E 65 78 65 20 48 54  GET /rOoT.exe HT
000010  54 50 2F 31 2E 31 0D 0A  55 73 65 72 2D 41 67 65  TP/1.1..User-Age
000020  6E 74 3A 20 63 69 73 63  6F 2D 49 4F 53 0D 0A 48  nt: cisco-IOS..H
000030  6F 73 74 3A 20 31 39 32  2E 31 2E 32 34 2E 38 0D  ost: 192.1.24.8.
000040  0A 44 61 74 65 3A 20 54  68 75 2C 20 31 36 20 4D  .Date: Thu, 16 M
000050  61 79 20 32 30 31 33 20  31 32 3A 35 32 3A 35 39  ay 2013 12:52:59
000060  20 47 4D 54 0D 0A 43 6F  6E 6E 65 63 74 69 6F 6E   GMT..Connection
000070  3A 20 4B 65 65 70 2D 41  6C 69 76 65 0D 0A 0D 0A  : Keep-Alive....
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
  threatRatingValue: 31
  interface: ge0_2
  protocol: tcp


R7#copy http://192.1.24.8/defAUlt.IDA null0
Destination filename [null0]?
%Error opening http://192.1.24.8/defAUlt.IDA (I/O error)
R7#

evIdsAlert: eventId=1368538386613478041 severity=medium vendor=Cisco
alarmTraits=2147483648
  originator:
```

```
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 12:51:02 2013/04/16 08:51:02 GMT-05:00
  signature: description=CodeRed id=60000 created=20000101 type=other version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.67.7
      port: 49552
    target:
      addr: locality=OUT 192.1.24.8
      port: 80
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedFlow: true
    snmpTrapRequested: true
  context:
    fromAttacker:
000000  47 45 54 20 2F 64 65 66  41 55 6C 74 2E 49 44 41  GET /defAUlt.IDA
000010  20 48 54 54 50 2F 31 2E  31 0D 0A 55 73 65 72 2D   HTTP/1.1..User-
000020  41 67 65 6E 74 3A 20 63  69 73 63 6F 2D 49 4F 53  Agent: cisco-IOS
000030  0D 0A 48 6F 73 74 3A 20  31 39 32 2E 31 2E 32 34  ..Host: 192.1.24
000040  2E 38 0D 0A 44 61 74 65  3A 20 54 68 75 2C 20 31  .8..Date: Thu, 1
000050  36 20 4D 61 79 20 32 30  31 33 20 31 32 3A 35 33  6 May 2013 12:53
000060  3A 33 30 20 47 4D 54 0D  0A 43 6F 6E 6E 65 63 74  :30 GMT..Connect
000070  69 6F 6E 3A 20 4B 65 65  70 2D 41 6C 69 76 65 0D  ion: Keep-Alive.
000080  0A 0D 0A                                          ...
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66
  threatRatingValue: 31
  interface: ge0_2
  protocol: tcp
```

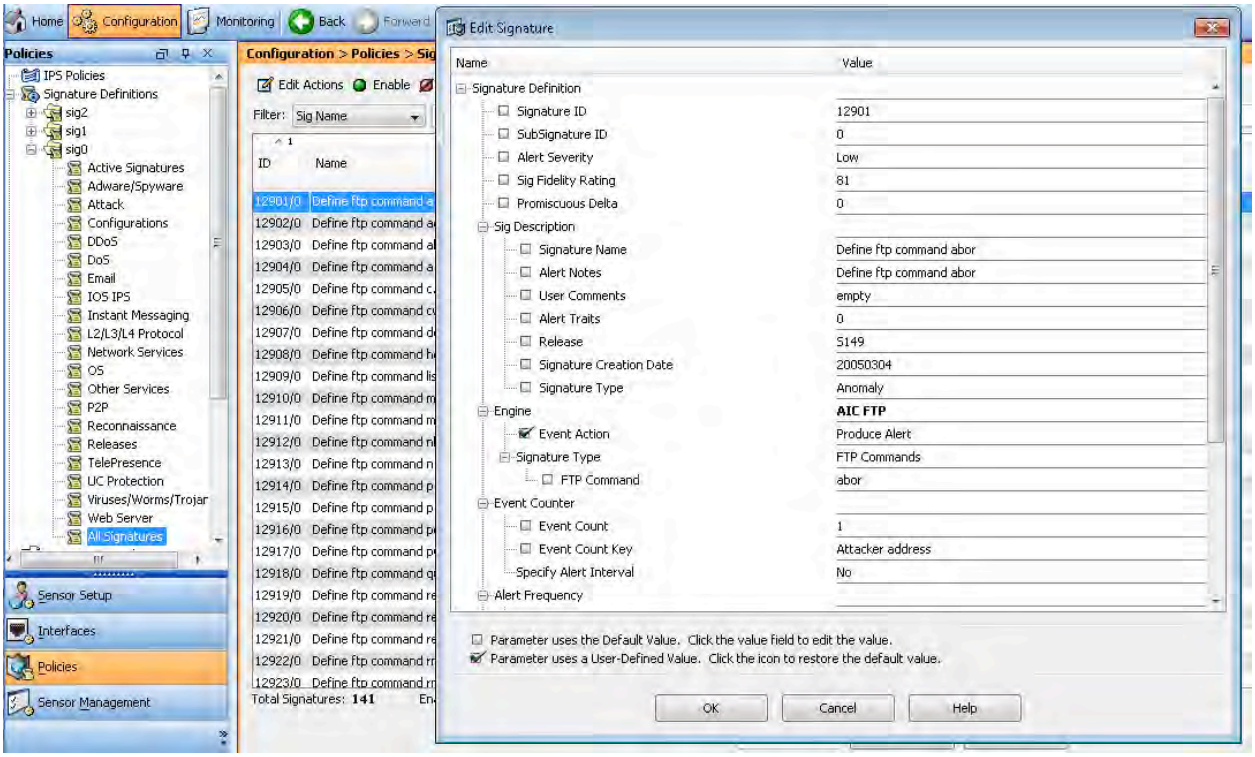
Notes

This task calls for a custom string based signature using a regex string to match on the required URL contents. As we are required to match on any case for the urls we need to enclose each characters upper and lower case form within square brackets, i.e. [Aa]. We also need to include the pipe '|' between each of the three defined strings. This does make the string quite long and introduces the possibility for mistakes.
To save time troubleshooting the regex side test the string on the ASA prior to creating the signature.
** When testing this signature ensure that the HTTP server is enabled on R8.

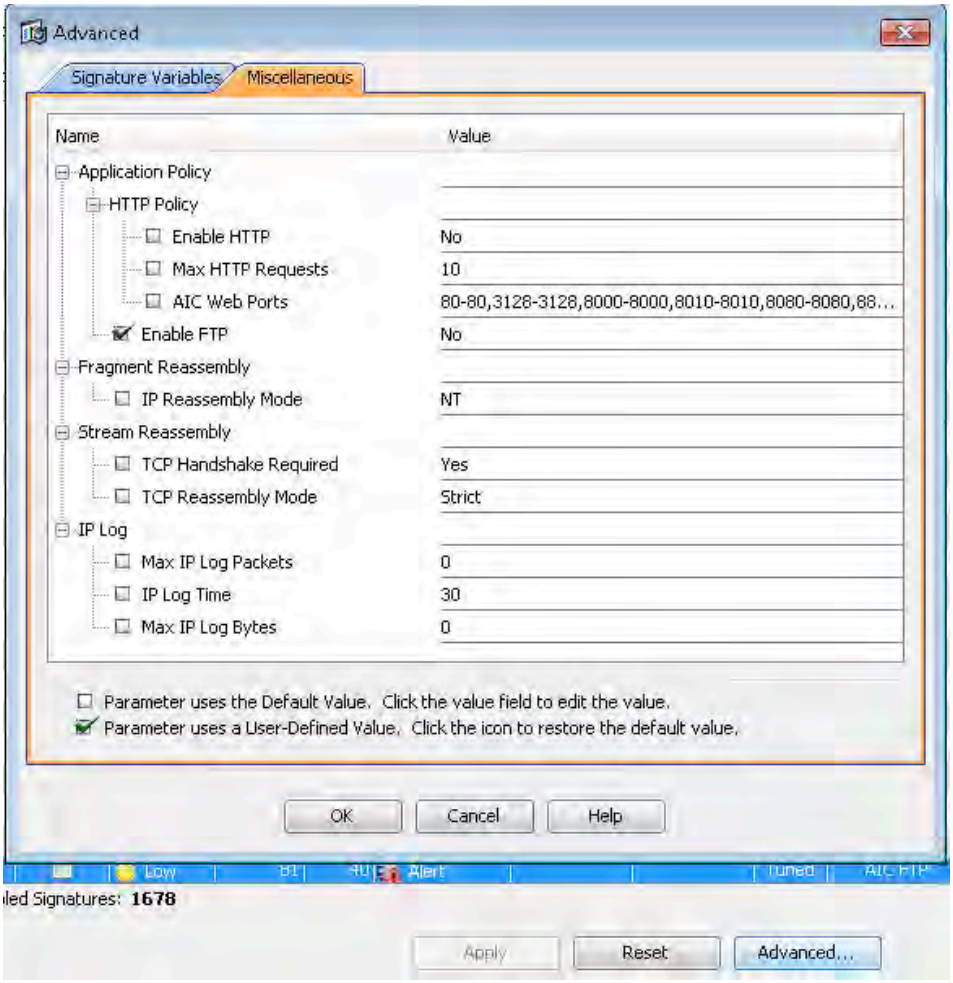
- Configure the sensor to alert when it detects a file being deleted on the FTP server at 10.4.4.100 from Vlan 5. A low-priority IPS event should also be logged.

Configuration

Search the FTP signatures on vs0 and edit the existing Sig for the FTP Delete command.
As the alert is already a low severity all we need to do is remove the Deny action and enable it.



Hopefully you noticed that the engine was AIC FTP which requires FTP inspection to be enabled to function. This is achieved via the Advanced button at the bottom of the Signature Definition window.



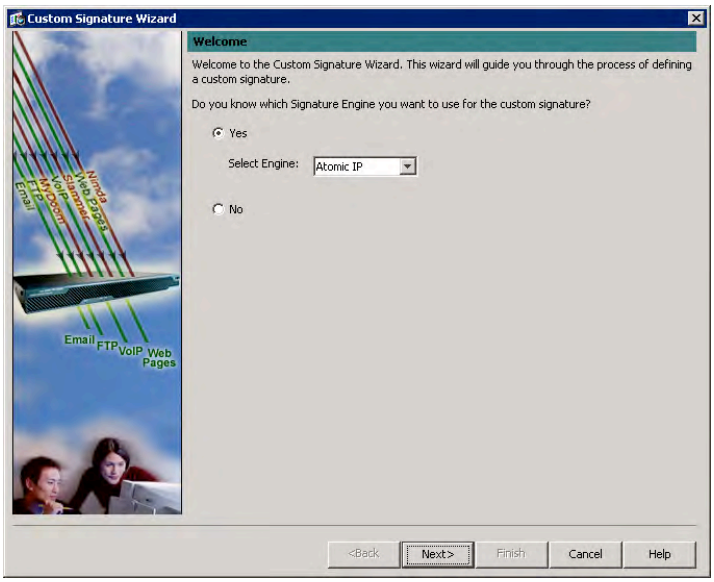
Notes

This is a fairly straight forward task, utilizing an existing FTP signature 12907, which detects the use of the FTP delete command. The only potential gotcha is to remember to enable the AIC FTP inspection engine, which is disabled by default.

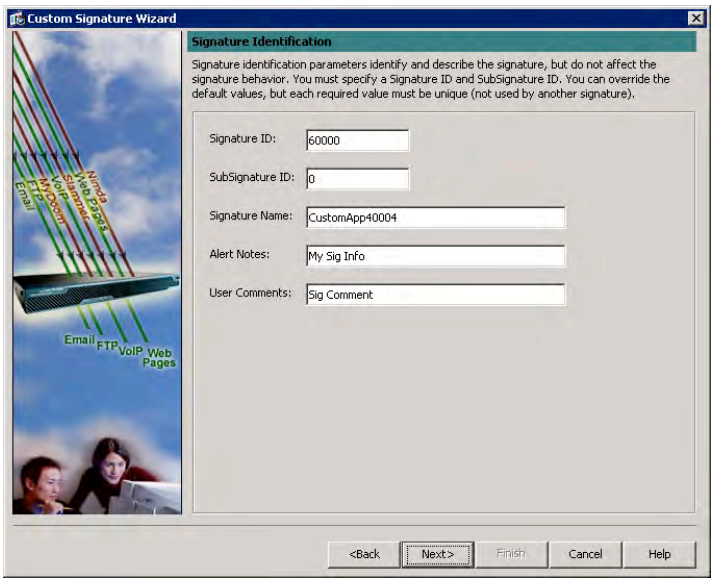
- A custom TCP application is running in Vlan 5 on port 40004. This application should only be accessed from Vlan 7. An SNMP trap should be sent to the ACS Server in Vlan 10 if this traffic is detected being sourced from any other location. Standard severity and Risk Ratings should be used. Do not use IP or IP ranges for defining Vlan 7 when configuring this task.

Configuration

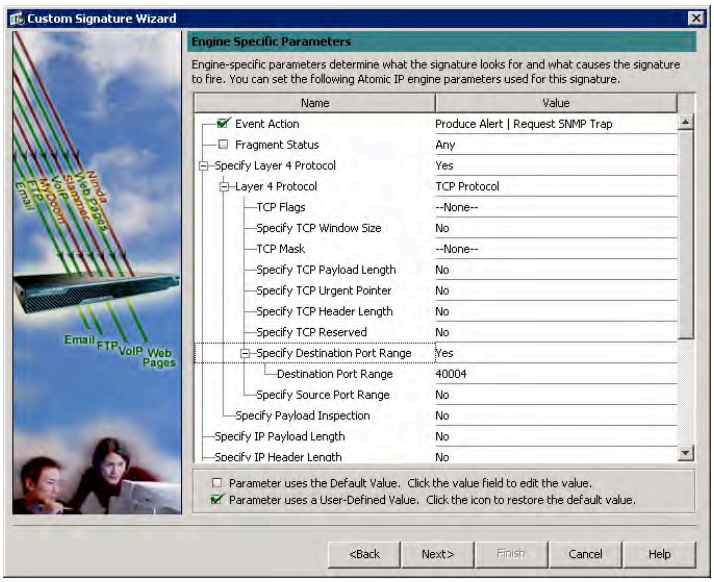
Start the Signature Wizard for vs0.



Select the Atomic IP engine.



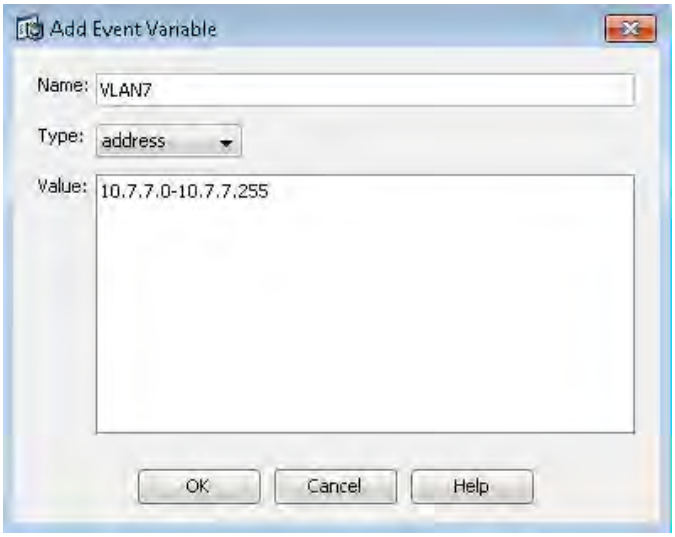
Name the sig.



Add the Request SNMP trap action.
Select TCP as the protocol and 40004 as the destination port.

Accept all remaining defaults, click finish then apply.

Under Event Action Rules > Rules0 > Event Variables create a new entry for vlan 7.



Create a new Event Action Filter to prevent the actions being applied when accessed from Vlan 7.
Subtract all the actions for sig 60000. Use the variable to define VLAN7 in the fillter.

Verification

To test enable the HTTP Server on R5 and set the port to 40004.

R5(config)#ip http server
R5(config)#ip http port 40004

Test using a telnet connection to R5 on port 40004.

```
R8#telnet 5.5.5.5 40004
Trying 5.5.5.5, 40004 ... Open
TEST
HTTP/1.1 400 Bad Request
Date: Thu, 16 Apr 2013 13:31:16 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 5.5.5.5 closed by foreign host]

evIdsAlert: eventId=1368538386613478133 severity=medium vendor=Cisco
alarmTraits=2147483648
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 13:29:26 2013/04/16 09:29:26 GMT-05:00
  signature: description=CustomApp40004 id=60000 created=20000101 type=other
version=custom
```

```
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.24.8
      port: 0
    target:
      addr: locality=OUT 0.0.0.0
      port: 0
      os: idSource=unknown relevance=unknown type=unknown
  actions:
    snmpTrapRequested: true
  summary: final=true initialAlert=1368538386613478132 summaryType=Regular 120
  alertDetails: Regular Summary: 120 events this interval ;
  riskRatingValue: targetValueRating=medium 56
  threatRatingValue: 56
  interface: ge0_0
  protocol: tcp
```

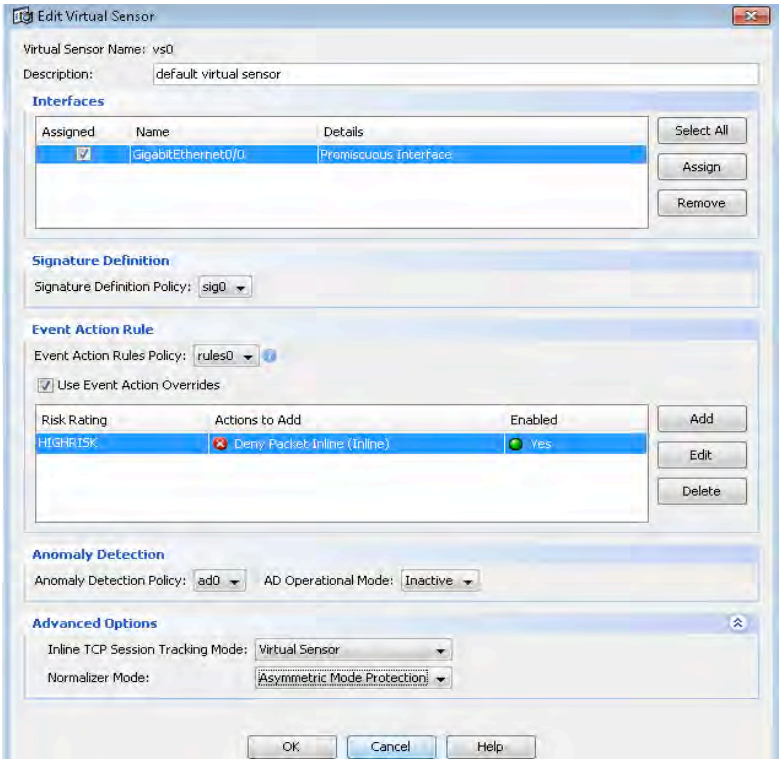
Notes

A short task utilizing the Atomic IP engine and Event Variables. If asked not to use any attacker or victim IP's while defining events / signatures, use Event Variables to define them under the Event Action Rules section, so you can call on them later. One thing to remember is that when you are call a variable you need to prepend the variable name with the $ sign.
I.e $Variable1 – where Variable1 is the name.

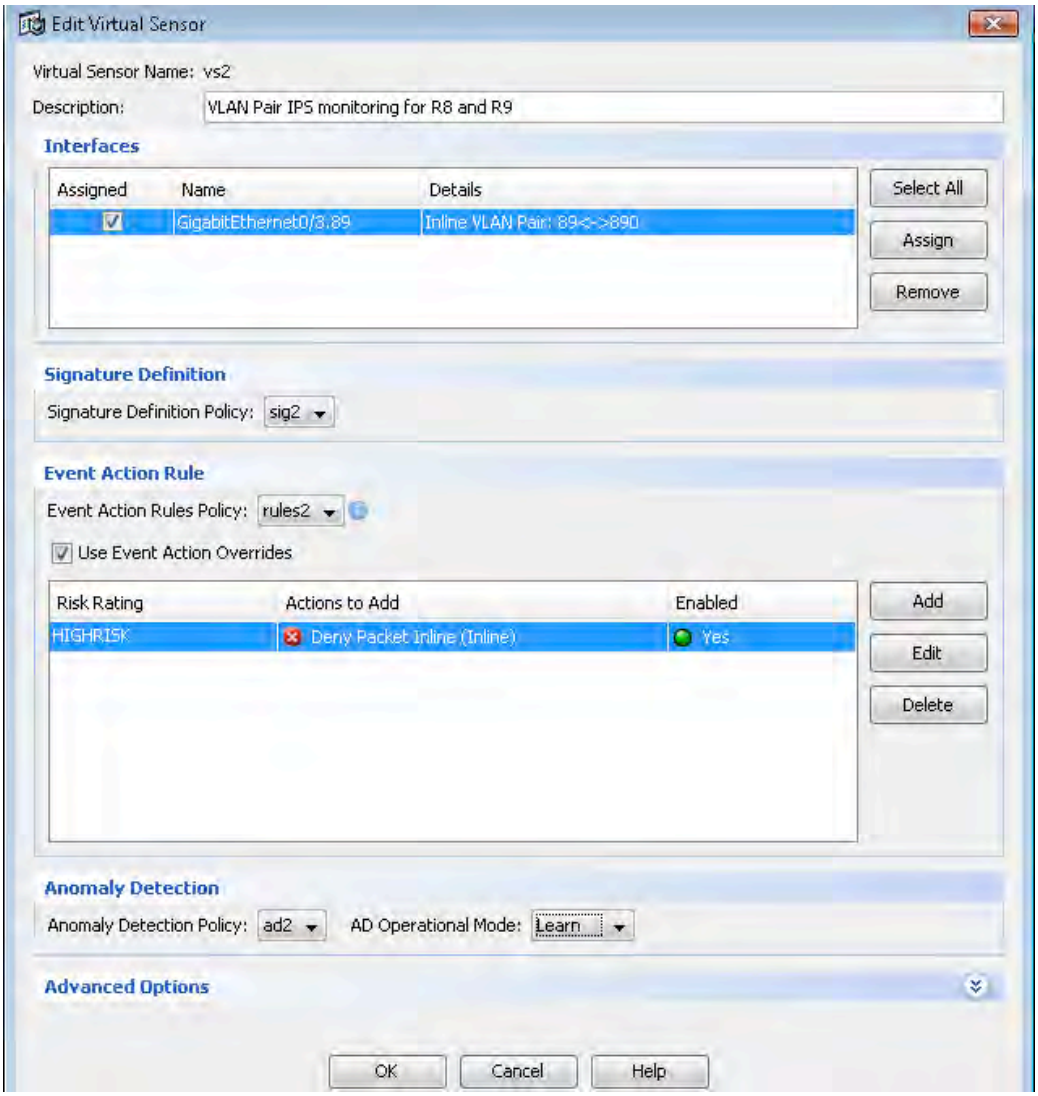
Task 10: Advanced IPS and Anomaly Detection

- Due to potential asymmetric traffic flows for VLAN 5 disable AD for Sensor vs0, and set the Normalizer mode accordingly.
- AD for Virtual Sensor 2 should be set to learning mode, the learning period should be 72hrs. The learning action should be so that after the learning period the new Knowledge Base is saved and loaded, replacing the initial KB.
- Ensure that Vlan 6 and 8 are seen as the Internal networks in their respective AD policies.
- You have some unallocated dark ip that will eventually be reachable via R6, 10.16.16.0/24, 10.66.66.0/24 & 10.166.166.0/24, these subnets should not be present in any traffic flows and should be handled accordingly. The scanner thresholds should be reduced to 100 for both TCP and UDP.
- In vs1 restrict the OS fingerprinting to the 10.0.0.0/8 network. Add two mappings one for the ACS server, so it is always seen as type WinNT, and one for a Linux Server called RedHat1 with an ip of 10.7.7.100.

Configuration



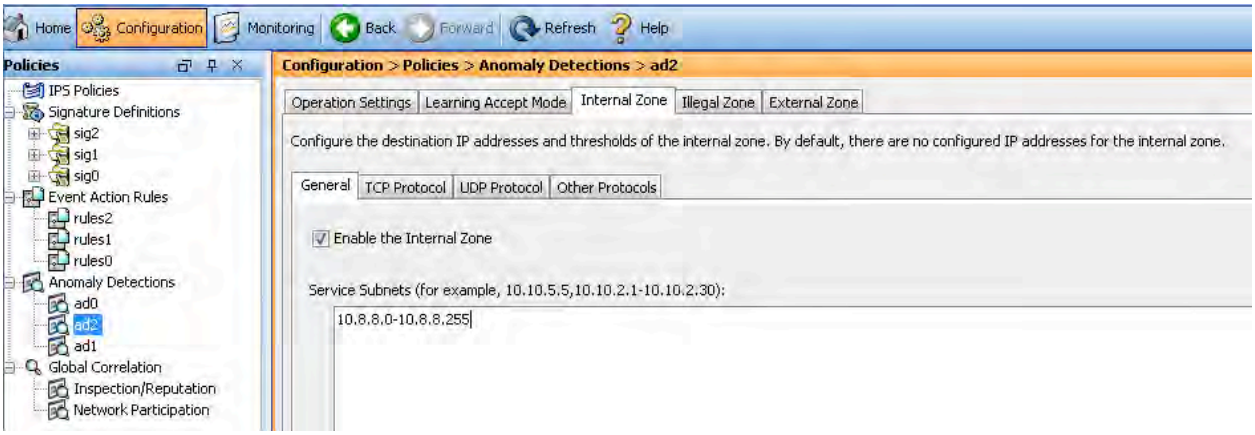
Go to Configuration > IPS Policies and edit vs0. Change the AD Operational Mode to 'Inactive.' Collapse the Advanced options section and change the Normalizer mode to 'Asymmetric Mode Protection.' This requires a reboot of the sensor.



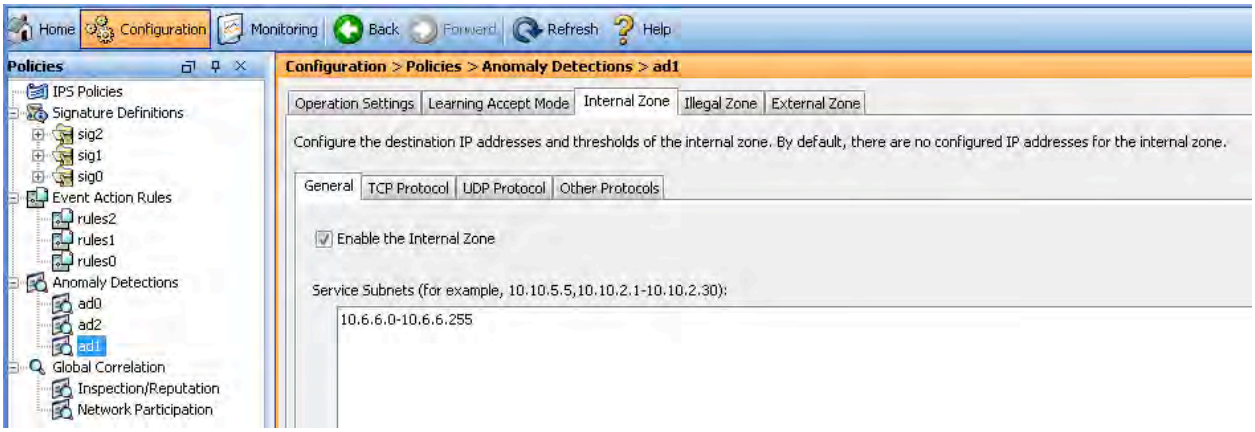
Goto Configuration > IPS Policies and edit vs2. Change the AD Operational Mode to 'Learn.'

Go to the Learning Accept Mode tab under ad2 to modify the Learning Period.
The default action of Rotate should be left as is.

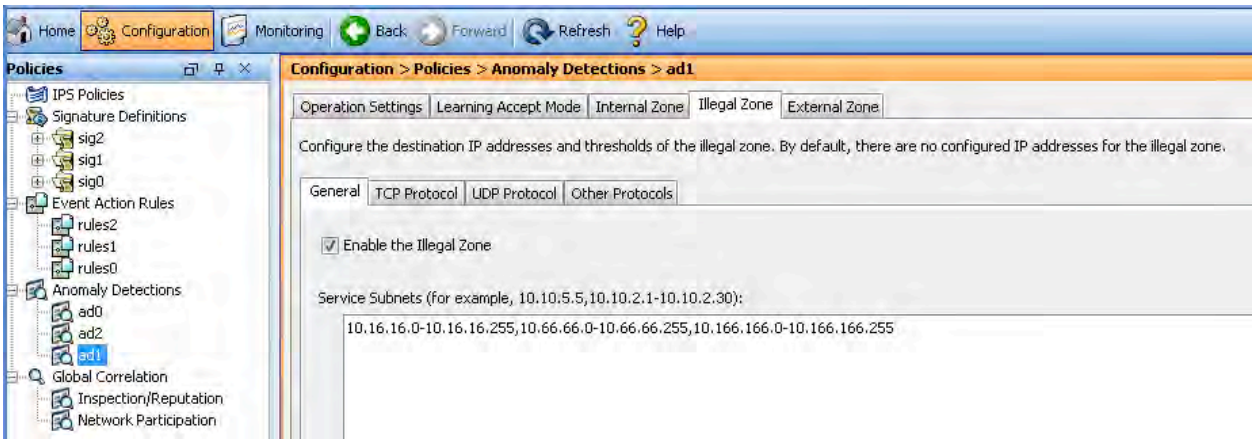
Internal trusted networks should be assigned to the Internal zone, goto ad2 and add vlan 8



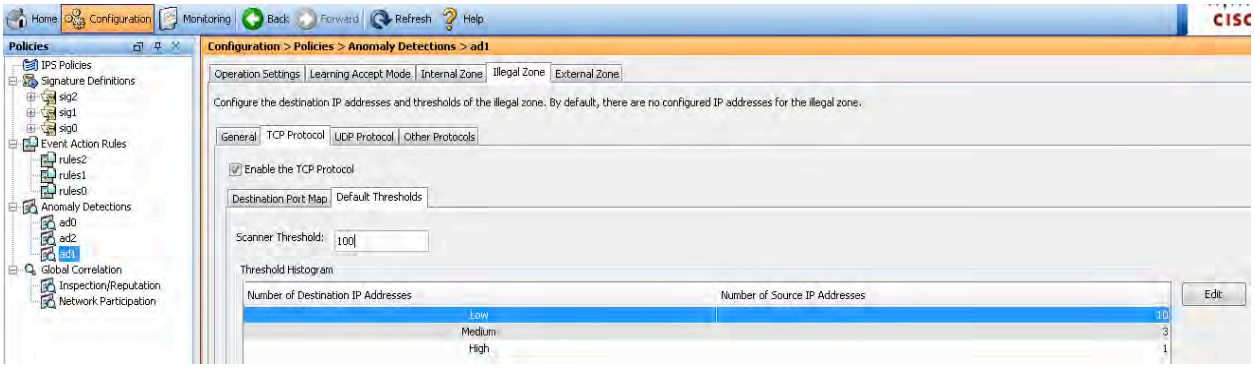
Repeat the previous steps for Vlan 6 in ad1 policy.

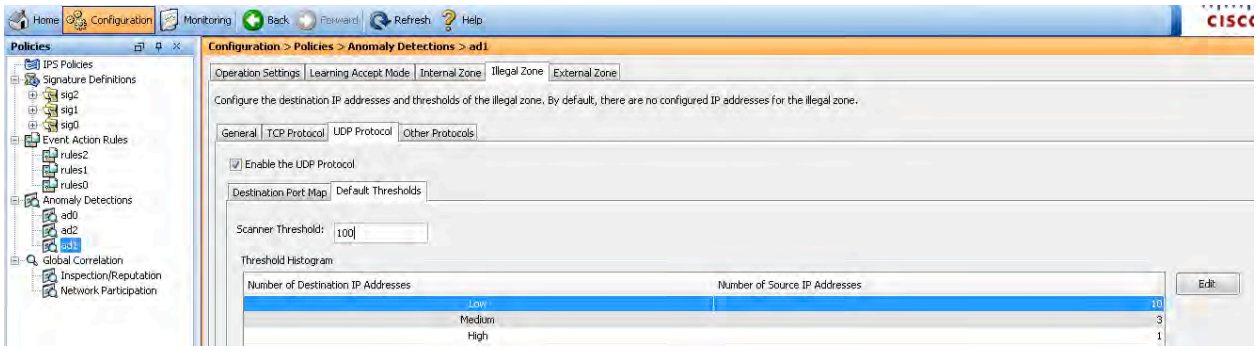


Any unallocated space should be protected using the illegal zone, add the R6 subnets here.

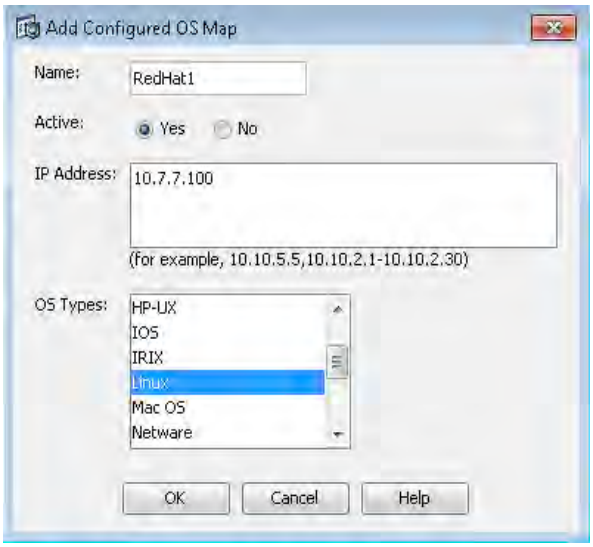


Tweak the Scanner thresholds in the illegal zone, under the Default Thresholds tab for each protocol. Repeat the same task for the UDP protocol.

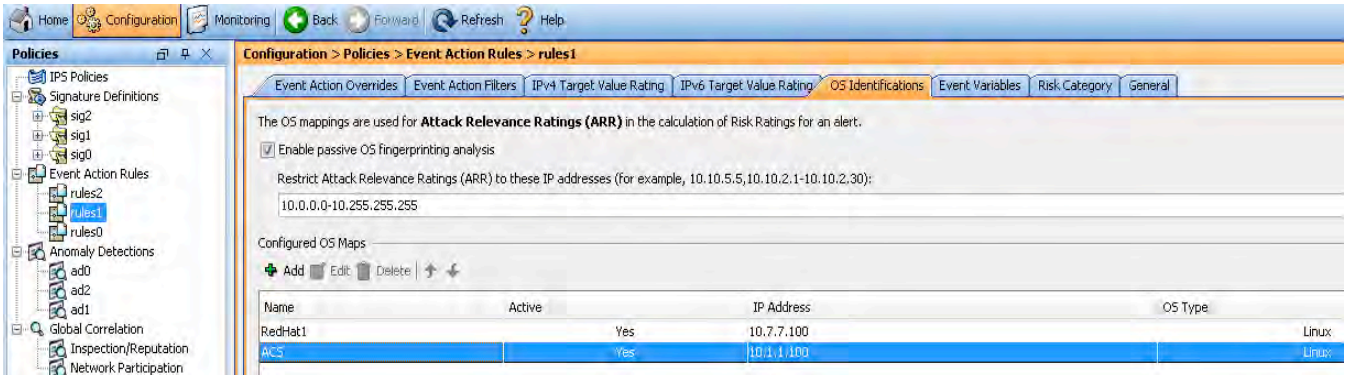




Use the Add button under the Configured OS Maps in Event Actions Rules 1, specifying the name ip address and OS type.



Repeat the task for the ACS server, while also the 10/8 network in the Restrict field above.



Notes

This is a config only type of question

I'm not sure of the possibilities of these topics showing up in the lab, but as everything seems to be fair game, and we have an ambiguous Advanced Features section in the blueprint, though it was worth a mention.

The section touches on some advanced features, in terms of Anomaly Detection and OS identification. AD is used to classify and detect dynamic attacks such as scanning threats and worms, based on deviations from normal traffic pattern behavior, which would be too difficult to detect using signatures. As AD expects to see the normal bidirectional flow of traffic, if you have an asymmetric environment, AD should be disabled, as it will detect incomplete connections, causing the sensor to classify normal traffic as scanning threats etc.

The default behavior of AD is detect mode which starts of in Learning mode for the first 24 hrs, and once complete saves and loads the KB, automatically switching to detect mode. Best practice is to run learning mode for a week or more to allow the sensor to fully gauge the normal legitimate traffic flows. By default all network ranges are assigned to the external zone. The internal zone in AD should be used to define all your trusted networks on the inside of the sensor. The illegal zone allows you to define dark or unallocated IP, as you should never see traffic flowing to these IP ranges you can be aggressive with your thresholds and policies.

We finish the task with OS identification. This is a handy addition that allows learning the OS type of hosts on the network, by inspecting the TCP handshake. Static mappings can also be set, as we have done here. These mappings are then used by the sensor to determine the relevance of the attack according to the OS and Associated Risk Rating.

Task 11: Blocking using the Security Appliance.

- A host on VLAN 5 is carrying out an access attack on R1 using telnet with a username of “Admin".
- Make sure this attack is detected as high severity, and the triggered event contains as much information as possible.
- When the event is triggered the IPS should connect to the ASA using SSH and perform a shun.
- Use the ASA local database for authentication with user “IPS_Admin" and password "ipexpert". Enable password should also be "ipexpert".

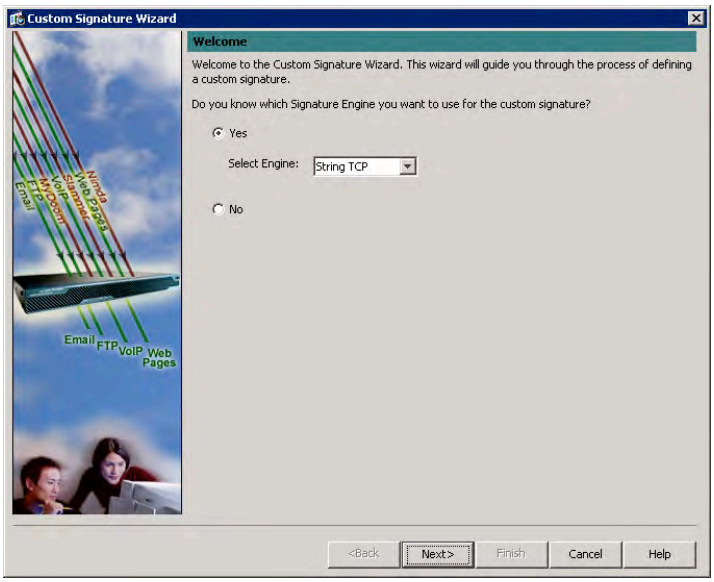
Configuration

ASA3

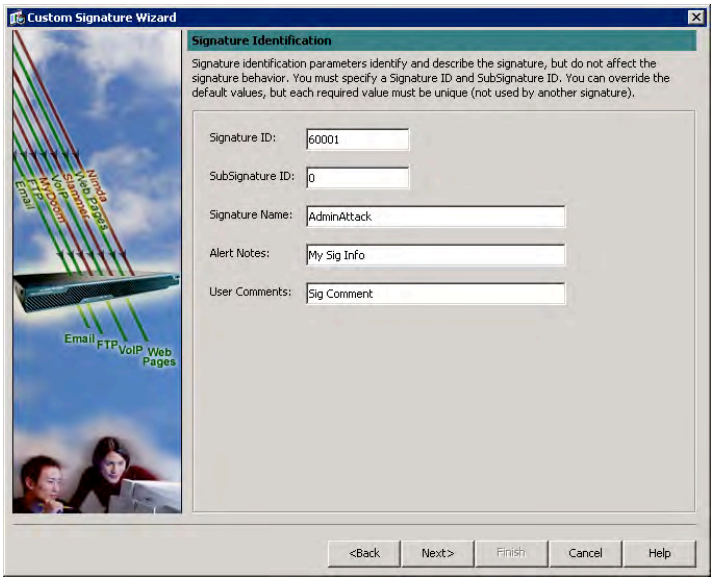
```
username IPS_Admin password ipexpert
ssh 10.1.1.15 255.255.255.255 inside
aaa authentication ssh console LOCAL
enable pass ipexpert
```

IPS

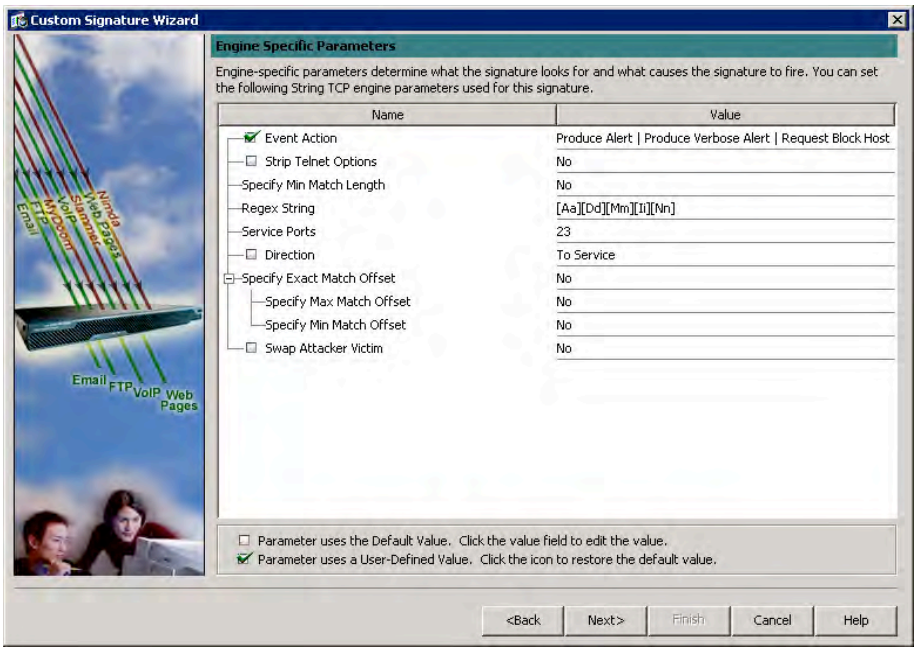
Create a new custom signature, using the signature wizard for vs0.



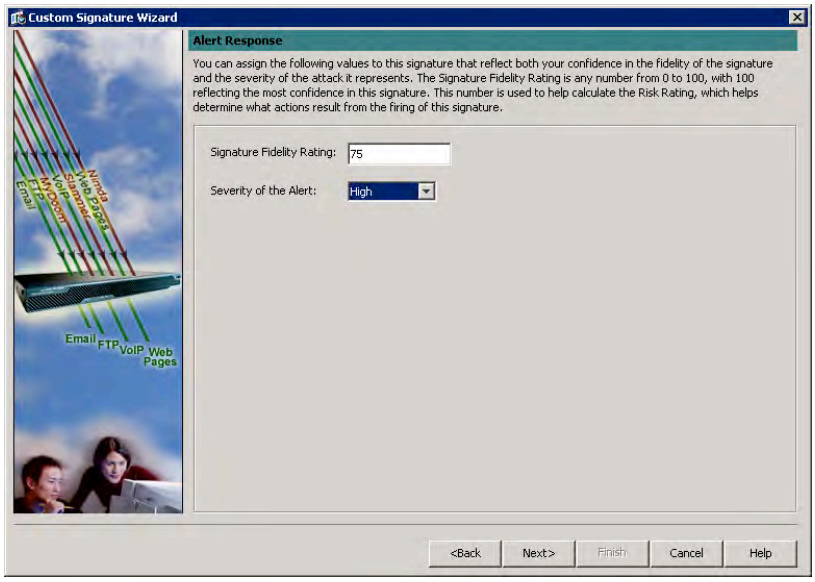
Select the String TCP engine. Click 'Next'.



Name the Signature. Click 'Next'.

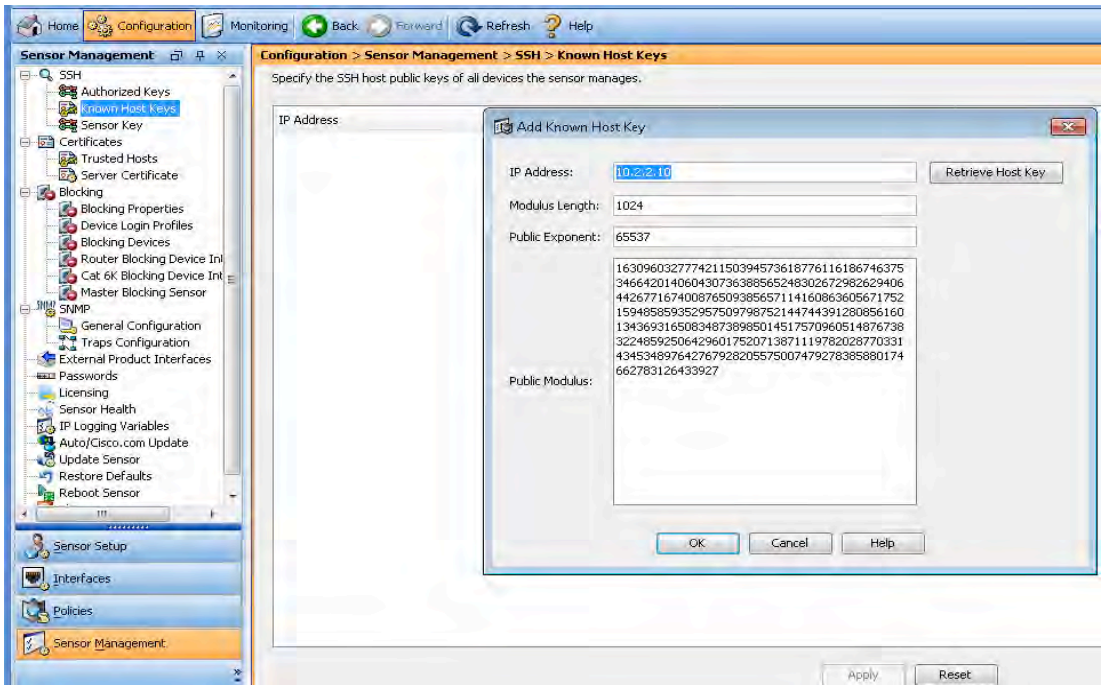


Add Produce Verbose Alert & Request Block Host as event actions. The username Admin should be added to regex field. As it was not requested to include upper and lower case, an exact match would be sufficient. The Service port should be equal to telnet (23).

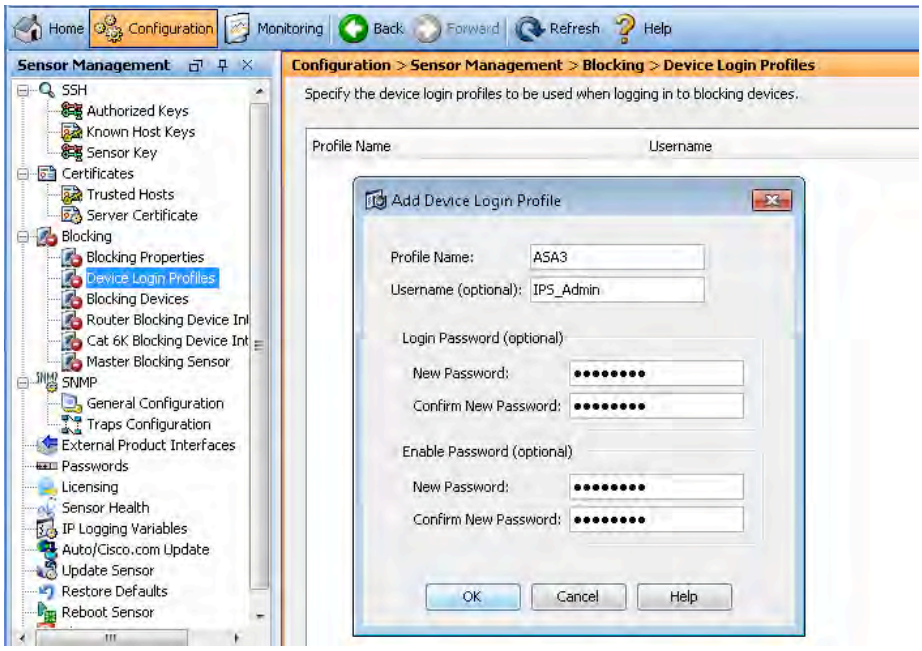


Change the Severity to ‘High’. Click ‘Next,’ then ‘Finish’.

Now we need to add the blocking configuration. Use the the Sensor Management > SSH > Known Host Keys to add the ASA’s SSH keys.



Add a login profile for the ASA under the Sensor Management > Blocking > Device Login Profiles.



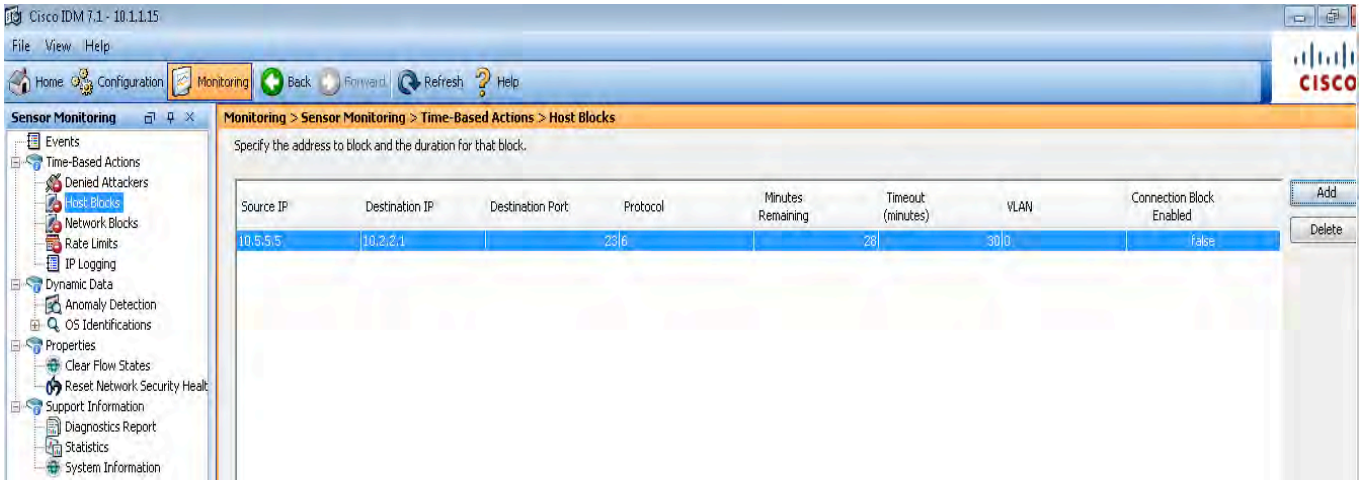
Add the ASA as a blocking device under the Sensor Management > Blocking > Blocking Devices.

Verification

```
R5#telnet 10.2.2.1 /source-interface f0/1.5
Trying 10.2.2.1 ... Open

R1#admIn

evIdsAlert: eventId=1368538386613478226 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 436
  time: 2013/04/16 15:09:56 2013/04/16 11:09:56 GMT-05:00
  signature: description=AdminAttack id=60001 created=20000101 type=other
version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.5.5.5
      port: 21248
    target:
      addr: locality=OUT 10.2.2.1
      port: 23
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    blockRequested: true
    denyPacketRequestedNotPerformed: true
    denyFlowRequestedNotPerformed: true
  context:
```

```
    fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 52 31  ..............R1
000010  23 FF FE 20 FF FD 21 FF  FA 21 00 FF F0 FF FE 18  #.. ..!..!......
000020  61 64 6D 49                                       admI
    fromAttacker:
000000  FF FD 03 FF FB 20 FF FB  1F FF FB 21 FF FD 01 FF  ..... .....!....
000010  FC 18 FF FA 1F 00 50 00  18 FF F0 FF FC 20 61 64  ......P...... ad
000020  6D 49 6E                                          mIn
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=mission-critical
100
  threatRatingValue: 80
  interface: ge0_0
  protocol: tcp


ASA(config)# show shun statistics
outside=ON, cnt=7
inside=OFF, cnt=0

Shun 10.5.5.5 cnt=7, time=(0:00:52)
```

From the Monitoring tab, navigate to Time Based Actions > Host Blocks to see the host address entries currently blocked by the IPS. Use the delete button to clear the block.



Notes

This task focuses on Host blocking or shunning using the ASA.
To achieve these we need to create a custom signature, which Request a Block Host action to the ASA. We are asked to ensure that the event contains as much info as possible, which requires a verbose alert. For configuring Host Blocking on the IPS we need to do a few things. First is add the RSA keys from the ASA. We then need to add a login profile including the IPS_Admin user account details and the enable password.

Finally, add the ASA as a blocking device, ensuring the ASA Login Profile and device type are set correctly.

Task 12: Blocking using IOS Devices

- FTP & HTTP traffic is required to be inspected on vs1.
- If malicious traffic is tunneled through HTTP from Vlan 4 to Vlan 7 a block should placed on R6's f0/1.24 interface, and all the traffic should be logged.
- Use SSH to connect to R6 from the IPS
- R6 should have a local user "R6Admin" with password "ipexpert".

Configuration

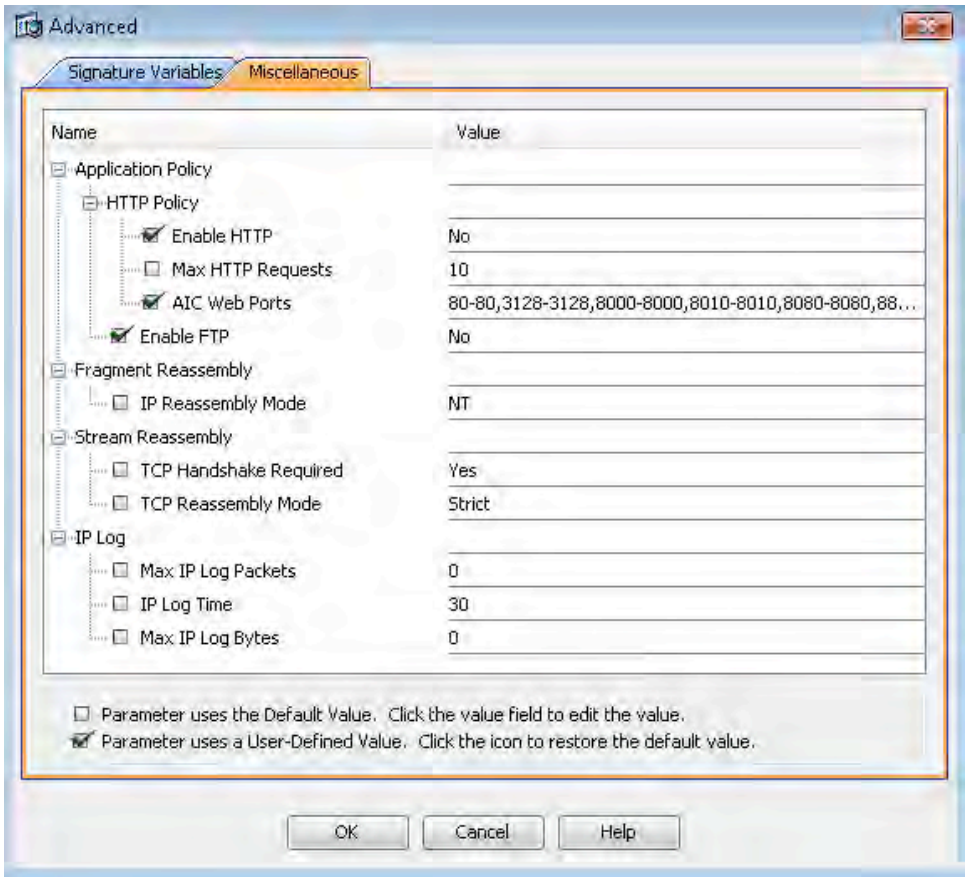
R6

Create RSA keys for use with SSH, remembering to add a domain name prior to generating them.

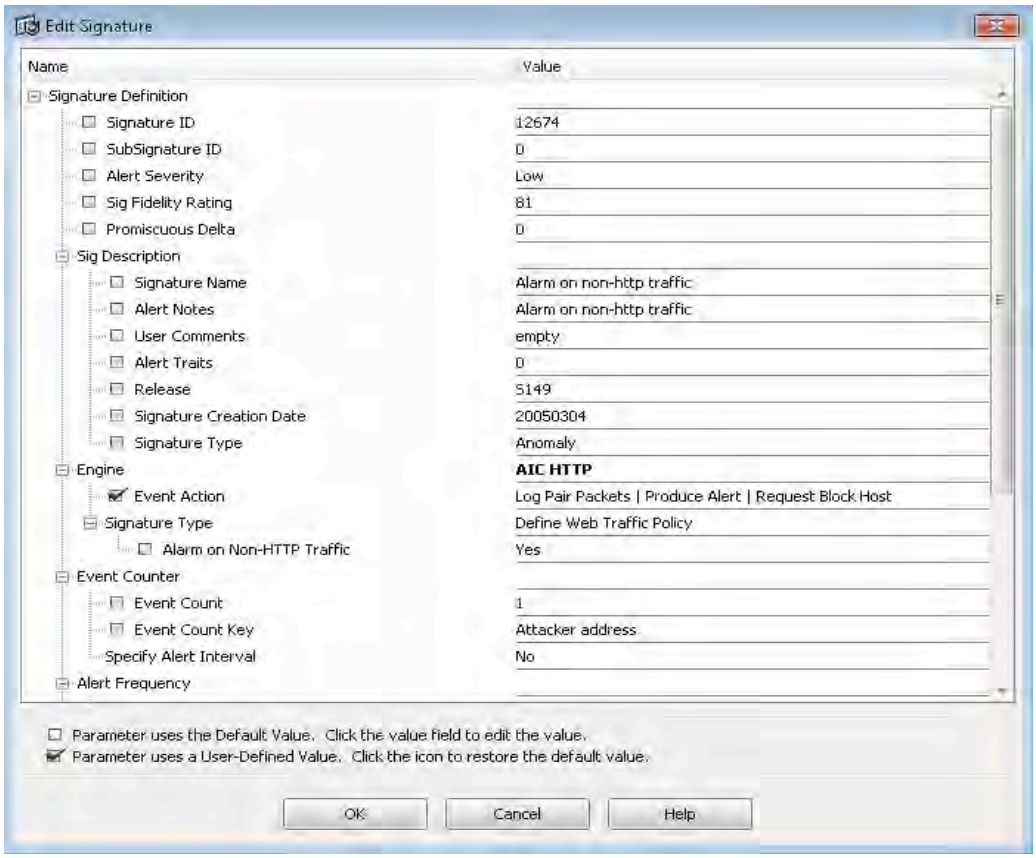
```
ip domain name ipexpert.com
crypto key generate rsa general-keys modulus 1024

username R6Admin password ipexpert
enable secret ipexpert

line vty 0 4
login local
```

IPS

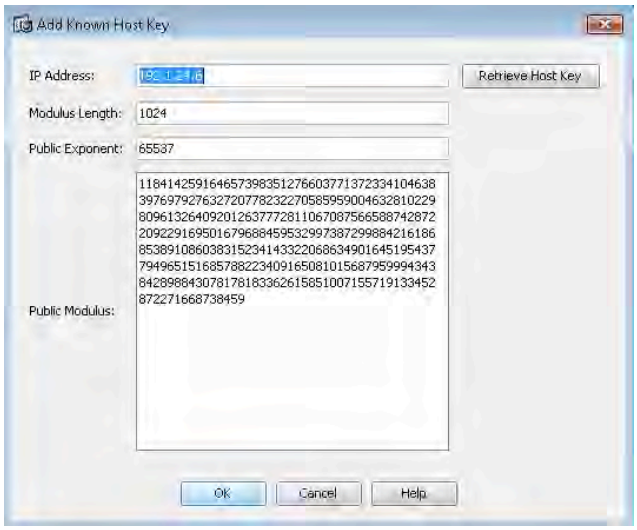
From sig1 > All Signatures click the Advanced button at the bottom of the page.
Enable the AIC Engine for FTP and HTTP Inspection.



Use the existing Alarm on Non-HTTP traffic signature for this task. Enable it. Remove the Deny Connection Inline action and replace it with Request Block Connection. Also add the Log Pair packets to capture all the traffic.



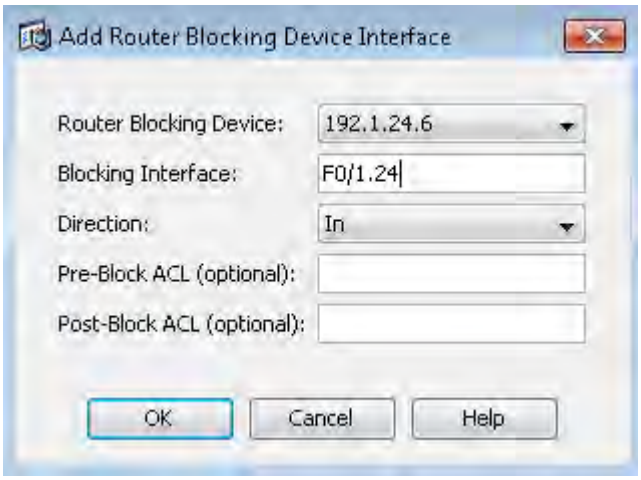
Retrieve R6's RSA keys.



Add the login profile for R6.

Configure R6 as a blocking device.

Add R6's F0/1.24 as a blocking interface as requested in the task.



Verification

Test SSH Login to R6.

```
R7#ssh -l R6Admin 192.1.67.6

Password:

R6>en
Password:
R6#
```

Enable the HTTP Server on R7.

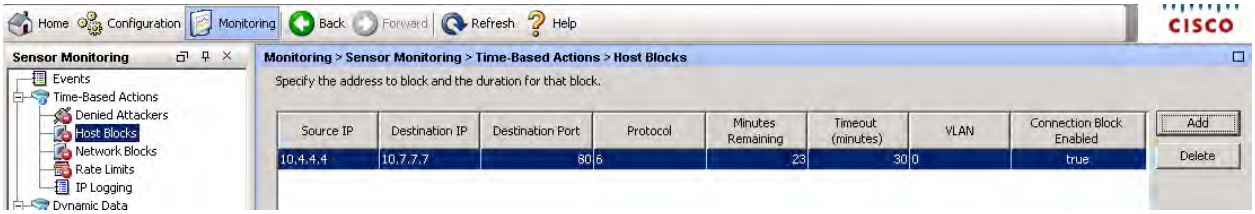
```
R7(config)#ip http server
```

Test by connecting via telnet to the HTTP server on R7.

```
R4#telnet 10.7.7.7 80 /source-interface f0/1.4
Trying 10.7.7.7, 80 ... Open


jkhg
HTTP/1.1 400 Bad Request
Date: Sat, 27 Apr 2013 19:07:45 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 10.7.7.7 closed by foreign host]
R4#
```

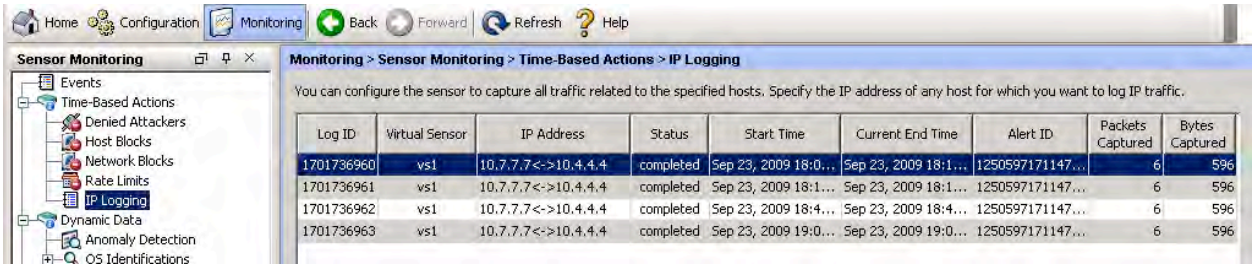
On R6 we can see that the IPS has logged in a made changes to the configuration.
A new ACL has been created and applied to the selected interface. Not that the first entry in the ACL is a permit any for the Sensor.

```
*Apr 27 19:05:29.013: %SYS-5-CONFIG_I: Configured from console by R6Admin on vty0
(10.1.1.15)
R6#sh run  int f0/1.24
Building configuration...

Current configuration : 228 bytes
!
interface FastEthernet0/1.24
 encapsulation dot1Q 24
 ip address 192.1.24.6 255.255.255.0
 ip access-group IDS_fastethernet0/1.24_in_1 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRP
end

R6#sh access-list
Extended IP access list IDS_fastethernet0/1.24_in_1
    10 permit ip host 10.1.1.15 any (38 matches)
    20 deny tcp host 10.4.4.4 host 10.7.7.7 eq www
    30 permit ip any any (6 matches)
R6#
```



We can see from the Host Blocks screen that a block is in place for R4 to R7 on port 80. Subsequent connections on port 80 from R4 are blocked by the ACL.

```
R4#telnet 10.7.7.7 80 /source-interface f0/1.4
Trying 10.7.7.7, 80 ...
% Destination unreachable; gateway or host down

R4#

R6#sh access-list
Extended IP access list IDS_fastethernet0/1.24_in_1
    10 permit ip host 10.1.1.15 any (186 matches)
    20 deny tcp host 10.4.4.4 host 10.7.7.7 eq www (1 match)
    30 permit ip any any (534 matches)
R6#
```



Final verification is to check that the IP logging is taking place. This is done by navigating to IP Logging secion within Sensor Monitoring. These logs can be downloaded for viewing in capture utilities such as Wireshark.

Notes

This task moves us to blocking using an IOS router, where the IPS creates an ACL and applies it to the specified interface.

The process here is fairly similar to the ASA blocking but with an additional step. For IOS devices we also need to create a Router Blocking Device Interface, to tell the IPS which interface the block will be applied to.

Note: If you already had an ACL assigned to the specified interface you would need to specify the pre and post block acls under the Router Blocking device Interface settings.
The signature we used for this task id# 12674 ‘Alarm on non-http traffic’ uses the AIC engine to inspect inside the HTTP traffic to ensure it conforms to RFCs etc. The AIC HTTP or FTP inspection are disabled by default, so needs to be enabled from the advanced signature settings.

If you’re unsure of the signature to use in a task, try changing the Filter menu to Sig Name and use the filter field to search for potential signatures, you may find an existing one matches your requirements.

Task 13: Rate Limiting

- An ICMP Flood is being generated by multiple hosts on Vlan 6 destined for Vlan 9.
- Tune an existing signature in vs2 to place a rate limit on R8's F0/1.24 interface.
- Login to R8 using Telnet and the local user "R8Admin" password "ipexpert".
- The rate limit should be set to 2% when more than 25 pings occur within a 1 second period

Configuration

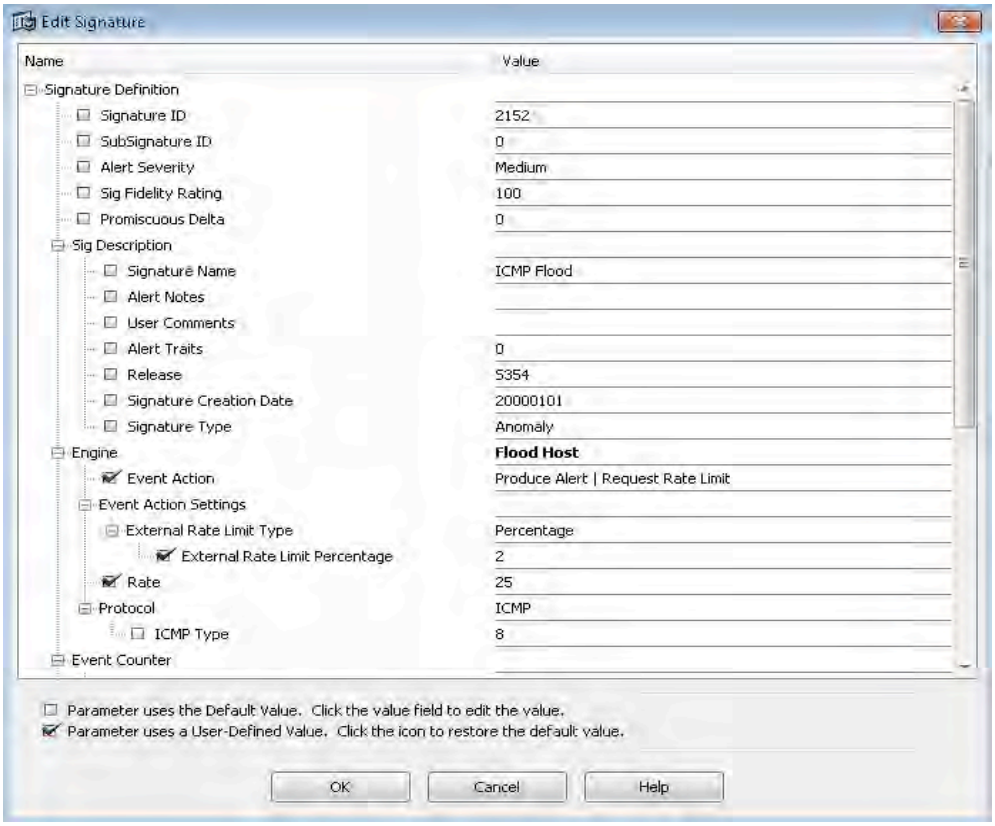
R8

```
enable secret ipexpert
```

IPS

Search for the icmp flood in the filter field for vs2 sig definitions.

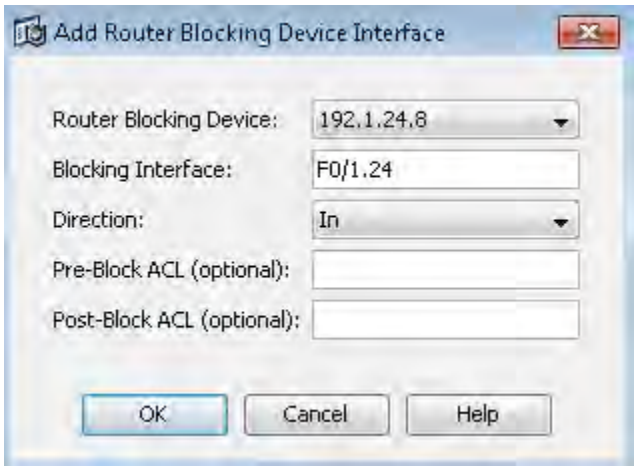
Edit the existing sig id 2152 ICMP Flood. Add the Request Rate Limit action and modify the both the rate limit percentage to 2 and the rate to 25.



Create a new profile for R8. Login password should be cisco as this is already configured on the Line of R8, with an enable of ipexpert.

Create a new profile for R8. Login password should be cisco as this is already configured on the Line of R8, with an enable of ipexpert.

As we did with blocking on the IOS device, we need to enable rate limiting by create a Router Blocking Interface for R8.



Verification

Ping Vlan 9 interface on R9 from Vlan 6.

```
R6#ping 10.9.9.9 source f0/1.6 size 5000 rep 300

Type escape sequence to abort.
Sending 300, 5000-byte ICMP Echos to 10.9.9.9, timeout is 2 seconds:
Packet sent with a source address of 10.6.6.6
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!.!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!.!!!
!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!
!!!!!!.!!!!!!!!!!!!!!
Success rate is 97 percent (292/300), round-trip min/avg/max = 4/7/12 ms
R6#
```

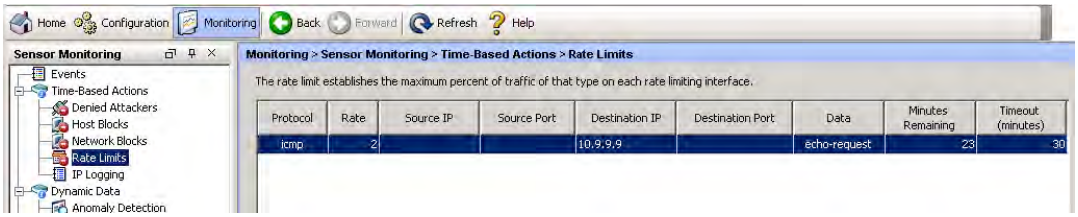
The IPS logs into R8 and applies the Rate limit to R8, to the specified interface.

```
R8#
*Apr 27 19:48:25.166: %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.1.15)
R8#
R8#sh run int f0/1.24
Building configuration...

Current configuration : 222 bytes
!
interface FastEthernet0/1.24
 encapsulation dot1Q 24
 ip address 192.1.24.8 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRP
 service-policy input IDS_RL_POLICY_MAP_1
end

R8#
```

As you can see, a service policy is used for rate limiting, so you can check the statistics output for the interface.

```
R8#sh policy-map interface
 FastEthernet0/1.24

  Service-policy input: IDS_RL_POLICY_MAP_1

    Class-map: IDS_RL_CLASS_MAP_icmp-xxBx-8-2_1 (match-any)
      1050 packets, 1380900 bytes
      5 minute offered rate 41000 bps, drop rate 2000 bps
      Match: access-group name IDS_RL_ACL_icmp-xxBx-8-2_1
        1050 packets, 1380900 bytes
        5 minute rate 41000 bps
      police:
          cir 2 %
          cir 2000000 bps, bc 62500 bytes
        conformed 1038 packets, 1364124 bytes; actions:
          transmit
        exceeded 12 packets, 16776 bytes; actions:
          drop
        conformed 144000 bps, exceed 2000 bps

    Class-map: class-default (match-any)
      113 packets, 11706 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

IPS Event Alerts

evIdsAlert: eventId=1368545206613477111 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 439
  time: 2013/04/20 10:26:48 2013/04/20 06:26:48 GMT-05:00
  signature: description=ICMP Flood id=2152 created=20000101 type=anomaly
version=S354
    subsigId: 0
    marsCategory: DoS/Network/ICMP
  interfaceGroup: vs2
  vlan: 89
  participants:
    attacker:
      addr: locality=OUT 10.6.6.6
    target:
      addr: locality=OUT 10.9.9.9
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    rateLimitRequested: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85
  threatRatingValue: 65
```

```
  interface: ge0_3
  protocol: icmp
```



You should also have an entry for rate limit under the Sensor Monitoring > Rate Limits section.

Notes

The final task for the IPS appliance in this lab is to apply a rate limit to an IOS device. Configuration for this very similar to the blocking section earlier. The one thing which has caught me out in the past is an error saying that rate limiting is not enabled. This was basically due to not having a blocking interface configured for the device. Don't be fooled by the title Router Blocking Device Interface. This is actually required to enable the rate limiting functions. Logically thinking, how would it know where to apply the rate limit without this?

One key point to mention with Rate Limiting is how the rate limit is applied. The IPS dynamically creates a classed based policy to apply the rate limit to the devices interface.

For instance:

```
class-map match-any IDS_RL_CLASS_MAP_icmp-xxBx-8-2_1
 match access-group name IDS_RL_ACL_icmp-xxBx-8-2_1
!
policy-map IDS_RL_POLICY_MAP_1
 class IDS_RL_CLASS_MAP_icmp-xxBx-8-2_1
   police cir percent 2
!
interface FastEthernet0/1.24
 service-policy input IDS_RL_POLICY_MAP_1
```

The key thing to remember here is that when applying rate limits via the IPS, if you already have a service policy applied in the same direction on the devices interface then the IPS rate limit policy will override any existing policies.

So be mindful of the lab task or network design when using this feature.

Task 14: IOS IPS

- Configure R1 to enable the IPS feature set inbound on vlan 10 and 20 interfaces.
- The IPS v5 signature package is contained in the path: flash:/IOS-Sxxx-CLI.pkg
- Be sure to follow the documented prerequisites.
- Enable only basic signature set
- Once completed enable ICMP Echo Request signature and ensure that the IPS is monitoring successfully

Solutions

R1

Add a domain name and create an rsa key pair.

```
ip domain name ipexpert.com
cry key gen rsa gen mod 1024
```

As per the pre-requisites, add the public key to decrypt the signatures.

```
R1(config)#crypto key pubkey-chain rsa
R1(config-pubkey-chain)#named-key realm-cisco.pub signature
Translating "realm-cisco.pub"

R1(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....

R1(config-pubkey)#$64886 F70D0101 01050003 82010F00 3082010A 02820101
R1(config-pubkey)#$C7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
R1(config-pubkey)#$BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
R1(config-pubkey)#$FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
R1(config-pubkey)#$8AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
R1(config-pubkey)#$AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
R1(config-pubkey)#$189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
R1(config-pubkey)#$3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
R1(config-pubkey)#$A4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
R1(config-pubkey)#F3020301 0001
R1(config-pubkey)#quit
R1(config-pubkey-key)#
R1(config-pubkey-key)#end
R1#wr
```

Verify the IPS version running in IOS (Version 3.xxx.xxx denotes IPS version 5).

```
R1#show subsys name ips
Name                Class     Version
ips                 Protocol    3.001.002
R1#
```

Retire all signature categories:

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
```

Un-retire the ios basic signature category:

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#end
Do you want to accept these changes? [confirm]
```

Make a new directory in flash for the IPS files.

```
R1#mkdir flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
R1#
```

Configure IPS on R1, applying it inbound on both Fa0/1.10 & Fa0/1.20.

```
R1(config)#ip ips name MYIPS
R1(config)#ip ips config location flash:/ips5
R1(config)#int f0/1.10
R1(config-subif)#ip ips MYIPS in
R1(config-subif)#int f0/1.20
R1(config-subif)#ip ips MYIPS in
```

Load the signature file in flash into the IPS.

```
R1#copy flash:IOS-S376-CLI.pkg idconf

Apr 27 18:54:20.041: %IPS-6-ENGINE_BUILDS_STARTED:  14:54:20 EDT Apr 27 2013
Apr 27 18:54:20.041: %IPS-6-ENGINE_BUILDING: multi-string - 12 signatures - 1 of 13 engines
Apr 27 18:54:20.073: %IPS-6-ENGINE_READY: multi-string - build time 32 ms - packets for this
engine will be scanned
Apr 27 18:54:20.093: %IPS-6-ENGINE_BUILDING: service-http - 667 signatures - 2 of 13 engines
Apr 27 18:54:28.201: %IPS-6-ENGINE_READY: service-http - build time 8108 ms - packets for this
engine will be scanned
Apr 27 18:54:28.233: %IPS-6-ENGINE_BUILDING: string-tcp - 1211 signatures - 3 of 13 engines
Apr 27 18:54:58.249: %IPS-6-ENGINE_READY: string-tcp - build time 30016 ms - packets for this
engine will be scanned
Apr 27 18:54:58.253: %IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
```

```
Apr 27 18:54:58.885: %IPS-6-ENGINE_READY: string-udp - build time 632 ms - packets for this
engine will be scanned
Apr 27 18:54:58.889: %IPS-6-ENGINE_BUILDING: state - 31 signatures - 5 of 13 engines
Apr 27 18:54:58.961: %IPS-6-ENGINE_READY: state - build time 72 ms - packets for this engine
will be scanned
Apr 27 18:54:59.025: %IPS-6-ENGINE_BUILDING: atomic-ip - 307 signatures - 6 of 13 engines
Apr 27 18:55:00.313: %IPS-6-ENGINE_READY: atomic-ip - build time 1288 ms - packets for this
engine will be scanned
Apr 27 18:55:00.365: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
Apr 27 18:55:00.405: %IPS-6-ENGINE_READY: string-icmp - build time 40 ms - packets for this
engine will be scanned
Apr 27 18:55:00.409: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
Apr 27 18:55:00.429: %IPS-6-ENGINE_READY: service-ftp - build time 20 ms - packets for this
engine will be scanned
Apr 27 18:55:00.429: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13 engines
Apr 27 18:55:00.753: %IPS-6-ENGINE_READY: service-rpc - build time 324 ms - packets for this
engine will be scanned
Apr 27 18:55:00.753: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
Apr 27 18:55:00.821: %IPS-6-ENGINE_READY: service-dns - build time 68 ms - packets for this
engine will be scanned
Apr 27 18:55:00.821: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
Apr 27 18:55:00.877: %IPS-6-ENGINE_READY: service-smb-advanced - build time 52 ms - packets
for this engine will be scanned
Apr 27 18:55:00.877: %IPS-6-ENGINE_BUILDING: service-msrpc - 29 signatures - 13 of 13 engines
Apr 27 18:55:00.949: %IPS-6-ENGINE_READY: service-msrpc - build time 68 ms - packets for this
engine will be scanned
Apr 27 18:55:00.949: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 40908 ms
R1#
```

Enable and un-retire the ICMP Echo Request signature 2004.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 2004
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#end
Do you want to accept these changes? [confirm]
R1#
Apr 27 19:09:10.331: %IPS-6-ENGINE_BUILDS_STARTED:  15:09:10 EDT Apr 27 2013
Apr 27 19:09:10.695: %IPS-6-ENGINE_BUILDING: atomic-ip - 307 signatures - 1 of 13 engines
Apr 27 19:09:11.367: %IPS-6-ENGINE_READY: atomic-ip - build time 672 ms - packets for this
engine will be scanned
Apr 27 19:09:11.719: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 1388 ms
Apr 27 19:09:12.099: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
```

Verification

Once you are happy that the IOS IPS is configured, verify your config using the following:

```
R1#sh ip ips configuration

IPS Signature File Configuration Status
    Configured Config Locations: flash:/ips5/
    Last signature default load time: 14:55:00 EDT Apr 27 2013
    Last signature delta load time: 15:24:05 EDT Apr 27 2013
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is disabled

IPS Signature Status
    Total Active Signatures: 339
    Total Inactive Signatures: 2167

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name MYIPS
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface FastEthernet0/1.10
        Inbound IPS rule is MYIPS
        Outgoing IPS rule is not set
      Interface FastEthernet0/1.20
        Inbound IPS rule is MYIPS
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False

R1#
```

Check the IPS signature count will show you what categories are enabled, compiled or retired:

```
R1#sh ip ips signature count

Cisco SDF release version S376.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total Signatures 12
      multi-string enabled signatures: 10
      multi-string retired signatures: 12

Signature Micro-Engine: service-http: Total Signatures 667
      service-http enabled signatures: 164
      service-http retired signatures: 570
      service-http compiled signatures: 97
      service-http obsoleted signatures: 2

**OUTPUT TRUNCATED**

Signature Micro-Engine: atomic-ip: Total Signatures 307
      atomic-ip enabled signatures: 100
      atomic-ip retired signatures: 285
      atomic-ip compiled signatures: 22

Total Signatures: 2506
   Total Enabled Signatures: 1117
   Total Retired Signatures: 2167
   Total Compiled Signatures: 339
   Total Obsoleted Signatures: 25

R1#
```

The ‘show ip ips signature sigid’ gives you detailed information about the signatures. Note from the output below that in this instance the sig2004 was successfully enabled, but the compiled state is ‘Nr’ or not compiled due to sig being retired. If the signature is not compiled, it is not yet in use, so will not generate any alarms. As you can see this gives some handy info regarding what each column is related to.

```
R1#sh ip ips signature sigid 2004 subid 0

En  - possible values are Y, Y*, N, or N*
      Y:  signature is enabled
      N:  enabled=false in the signature definition file
      *:  retired=true in the signature definition file
Cmp - possible values are Y, Ni, Nr, Nf, or No
      Y:  signature is compiled
      Ni: signature not compiled due to invalid or missing parameters
      Nr: signature not compiled because it is retired
```

```
      Nf: signature compile failed
      No: signature is obsoleted
Action=(A)lert, (D)eny, (R)eset, Deny-(H)ost, Deny-(F)low
Trait=alert-traits             EC=event-count          AI=alert-interval
GST=global-summary-threshold   SI=summary-interval     SM=summary-mode
SW=swap-attacker-victim        SFR=sig-fidelity-rating Rel=release

 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  2004:0     Y*  Nr    A      INFO     0     1    0    200   30  FA  N 100 S1
```

Here is the output for a successfully enabled Echo request signature, both enabled and compiled.

```
R1#sh ip ips signature sigid 2004 subid 0

**OUTPUT TRUNCATED**

 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  2004:0     Y   Y     A      INFO     0     1    0    200   30  FA  N 100 S1
      sig-name: ICMP Echo Request
```

Confirm that R1's IPS is now functioning as expected by pinging the ACS from R4.

```
R4#ping 10.1.1.100 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/8 ms
R4#

R1#
Apr 27 20:17:05.588: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo Request
[192.1.24.4:8 -> 10.1.1.100:0] VRF:NONE RiskRating:25
Apr 27 20:17:05.592: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo Request
[192.1.24.4:8 -> 10.1.1.100:0] VRF:NONE RiskRating:25

R1#sh ip ips statistics
Signature statistics [process switch:fast switch]
  signature 2004:0: packets checked [0:1204] alarmed [0:400] dropped [0:0]
Interfaces configured for ips 2
Session creations since subsystem startup or last reset 6
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:0:0]
Last session created 00:02:24
Last statistic reset never
TCP reassembly statistics
```

```
received 0 packets out-of-order; dropped 0
peak memory usage 0 KB; current usage: 0 KB
peak queue length 0
```

Notes

The pre-requisites in the config guide need to be followed for deploying IPS Feature set on an IOS Router.

Although this may seem like a simple task on the surface, the ips behavior in IOS has changed dramatically in the version 5 format. I would recommend following this config guide when you deploy IOS IPS v5, just to ensure things go smoothly.

The pre-requisites start with creating an rsa key pair on R1 and installing the public key to enable the signature package to be decrypted. This public key is found at the beginning of the guide above.
The next step is critical to ensuring this task is successful, all signatures must be retired prior to enabling the IPS. If you do not retire all the sigs, there is a large probability that your device will run out of resources and die, due to the large amount of signatures it will have to compile. If this happens your going to be in a world of hurt trying to regain access your device.

Once you have retired all the categories, un-retire a small subset of signatures. We have followed the guide and enabled the ios basic category.

We are then safe to enable the IPS feature set on the device. To enable the IPS we need to define a policy, giving it a name, and a stored config location in flash. Once this is done apply the policy to your interface/s.

The final stage to enabling the IPS is the loading and compiling of the signatures.
Use the 'copy flash:/IOS-Sxxx-CLI.pkg idconf' command to load the signature package from flash into the IPS, and compile all the non-retired signatures. This can take some time depending on how many signatures/categories are enabled.

All that's left is to start tuning any required signatures. The task asks for ICMP Echo Request signature to be enabled, the ID is the same as on the IPS appliance so is sig id 2004. Just remember when doing the task, ensure that the signature is both in an enabled state of true and a retired state of false.

Task 15: IOS IPS Tuning

- Set the event notification method to syslog.
- Create the ACS as a mission critical device.
- Configure Sig ID 2150 to drop and alarm on receipt of the fragmented icmp traffic.
- Enable the ICMP Flood category.

Configuration

R1

Configure event notifications using syslog.

```
R1(config)#ip ips notify log
```

Configure the IPS so that it see the ACS Server as a mission critical device:

```
R1(config)#ip ips event-action-rules
R1(config-rul)#target-value mission-critical target-address 10.1.1.100
R1(config-rul)#end
Do you want to accept these changes? [confirm]
R1#
```

Configure signature 2150 to drop and alarm:

```
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 2150
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#exit
R1(config-sigdef-sig)#engine
R1(config-sigdef-sig-engine)#event-action produce-alert deny-packet-inline
R1(config-sigdef-sig-engine)#end
Do you want to accept these changes? [confirm]
R1#
Apr 27  21:38:47.626: %IPS-6-ENGINE_BUILDS_STARTED:  17:38:47 EDT Apr 27  2013
Apr 27  21:38:47.986: %IPS-6-ENGINE_BUILDING: atomic-ip - 307 signatures - 1 of 13 engines
Apr 27  21:38:48.650: %IPS-6-ENGINE_READY: atomic-ip - build time 664 ms - packets for this
engine will be scanned
Apr 27  21:38:48.990: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 1364 ms
Apr 27  21:38:49.394: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Enable the ICMP Flood Category.

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category dos icmp_floods
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#enabled true
R1(config-ips-category-action)#end
Do you want to accept these changes? [confirm]

Apr 27  21:56:10.019: Applying Category configuration to signatures
Apr 27  21:56:25.739: %IPS-6-ENGINE_BUILDS_STARTED:  17:56:25 EDT Apr 27  2013
Apr 27  21:56:25.755: %IPS-6-ENGINE_BUILDING: multi-string - 12 signatures - 1 of 13 engines
Apr 27  21:56:25.779: %IPS-6-ENGINE_READY: multi-string - build time 24 ms - packets for this
engine will be scanned
Apr 27  21:56:26.191: %IPS-6-ENGINE_BUILDING: service-http - 667 signatures - 2 of 13 engines
```

```
Apr 27  21:56:26.551: %IPS-6-ENGINE_READY: service-http - build time 360 ms - packets for this
engine will be scanned
R1#
Apr 27  21:56:27.695: %IPS-6-ENGINE_BUILDING: string-tcp - 1211 signatures - 3 of 13 engines
Apr 27  21:56:28.283: %IPS-6-ENGINE_READY: string-tcp - build time 588 ms - packets for this
engine will be scanned
Apr 27  21:56:29.015: %IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
Apr 27  21:56:29.035: %IPS-6-ENGINE_READY: string-udp - build time 20 ms - packets for this
engine will be scanned
Apr 27  21:56:29.095: %IPS-6-ENGINE_BUILDING: state - 31 signatures - 5 of 13 engines
Apr 27  21:56:29.103: %IPS-6-ENGINE_READY: state - build time 8 ms - packets for this engine
will be scanned
Apr 27  21:56:29.459: %IPS-6-ENGINE_BUILDING: atomic-ip - 307 signatures - 6 of 13 engines
Apr 27  21:56:30.119: %IPS-6-ENGINE_READY: atomic-ip - build time 660 ms - packets for this
engine will be scanned
Apr 27  21:56:30.459: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
Apr 27  21:56:30.499: %IPS-6-ENGINE_READY: string-icmp - build time 40 ms - packets for this
engine will be scanned
Apr 27  21:56:30.503: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
Apr 27  21:56:30.503: %IPS-6-ENGINE_READY: service-ftp - build time 0 ms - packets for this
engine will be scanned
Apr 27  21:56:30.555: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13 engines
Apr 27  21:56:30.583: %IPS-6-ENGINE_READY: service-rpc - build time 28 ms - packets for this
engine will be scanned
Apr 27  21:56:30.663: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
Apr 27  21:56:30.679: %IPS-6-ENGINE_READY: service-dns - build time 16 ms - packets for this
engine will be scanned
Apr 27  21:56:30.707: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
Apr 27  21:56:30.875: %IPS-6-ENGINE_READY: service-msrpc - build time 48 ms - packets for this
engine will be scanned
Apr 27  21:56:30.895: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 5156 ms
Apr 27  21:56:30.895: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Verification

Check the status of your configuration on R1.

```
R1#sh ip ips configuration

IPS Signature File Configuration Status
    Configured Config Locations: flash:/ips5/
    Last signature default load time: 14:55:00 EDT Apr 27  2013
    Last signature delta load time: 17:56:30 EDT Apr 27  2013
    Last event action (SEAP) load time: 17:07:53 EDT Apr 27  2013

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured
```

```
IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is disabled

IPS Signature Status
    Total Active Signatures: 341
    Total Inactive Signatures: 2165

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name MYIPS
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface FastEthernet0/1.10
        Inbound IPS rule is MYIPS
        Outgoing IPS rule is not set
      Interface FastEthernet0/1.20
        Inbound IPS rule is MYIPS
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
    Category dos icmp_floods:
        Retire: False
        Enable: True

R1#
```

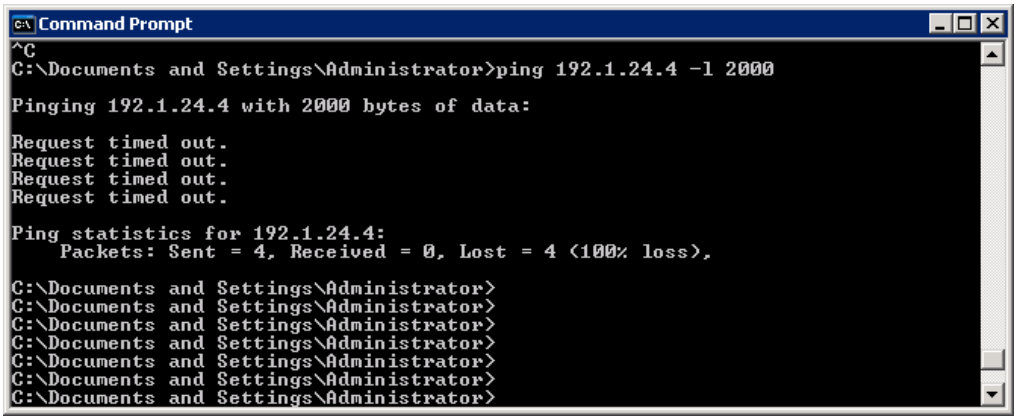
Verify the addition of the target value rating for the ACS Server.

```
R1#sh ip ips event-action-rules target-value-rating
Target Value Ratings
Target Value Setting   IP range
mission-critical       10.1.1.100-10.1.1.100

R1#
```

Confirm that the ICMP Fragment signature is configured as expected, and that the alarms are fired, after pinging from the ACS Server.

```
R1(config)#do sh ip ips sig sig 2150 sub 0

**OUTPUT TRUNCATED**

 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  2150:0     Y   Y     AD    INFO     0     1    0    200   30  FA  N 100 S2
      sig-name: Fragmented ICMP Traffic
```

```
      sig-string-info: My Sig Info
      sig-comment: Sig Comment
      Engine atomic-ip params:
           regex-string :
           address-with-localhost :
           dst-ip-addr :
           dst-port :
           exact-match-offset :
           fragment-status : want-fragments
```




```
R1#
Apr 27  22:26:33.023: %IPS-4-SIGNATURE: Sig:2150 Subsig:0 Sev:25 Fragmented ICMP
Traffic [10.1.1.100:0 -> 192.1.24.4:0] VRF:NONE RiskRating:25
Apr 27  22:26:38.479: %IPS-4-SIGNATURE: Sig:2150 Subsig:0 Sev:25 Fragmented ICMP
Traffic [10.1.1.100:8 -> 192.1.24.4:0] VRF:NONE RiskRating:25
Apr 27  22:26:38.479: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo Request
[10.1.1.100:8 -> 192.1.24.4:0] VRF:NONE RiskRating:25

R1#sh ip ips statistics
Signature statistics [process switch:fast switch]
  signature 2150:0: packets checked [0:29] alarmed [0:22] dropped [0:22]
  signature 2004:0: packets checked [27:4509] alarmed [27:669] dropped [0:0]
Interfaces configured for ips 2
Session creations since subsystem startup or last reset 19
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:0:0]
Last session created 00:30:31
Last statistic reset never
TCP reassembly statistics
  received 0 packets out-of-order; dropped 0
  peak memory usage 0 KB; current usage: 0 KB
  peak queue length 0

R1#

R1#sh ip ips category dos icmp_floods config
```

```
    Category dos icmp_floods:
        Retire: False
        Enable: True
```

Notes

We finish off this lab with tuning the signatures on the IOS IPS. Due to the shear amount of signatures available to the new v5 IPS its now a little more difficult to search for signature types, etc. The documentation also seems a little light in detail, so be prepared for some digging around. To save a little time you might do a quick search on the IPS Sensor, if you are having a hard time finding a particular signature, etc.

Some of the features available on the sensor are also now available in IOS, although behavior does not seem entirely consistent between the two. For instance, here we use the Event action rules, target value rating to classify the ACS with mission critical priority.

We also need to enable the ICMP Fragmented traffic signature and apply a drop action to the traffic, it wasn't specified but we chose to use deny packet inline. Remember to include the produce-alert in the event action, or it will be removed.

Finally we enable another signature category. ICMP Floods is located under the dos category and needs setting to both enabled true and retired false.

Don't forget that a lot of these sigs will have been retired, so remember to check their state, once configured

Section 7
Virtual Private Networks

Section 7: Virtual Private Networks is intended to let you be familiar with the VPN technologies that are available on IOS and the ASA. You will be configuring Site to Site, Remote Access & Flex VPNs along with some advanced features related to those technologies.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on the Virtual Private Networks. You will need to pre-configure the network with the base configuration files

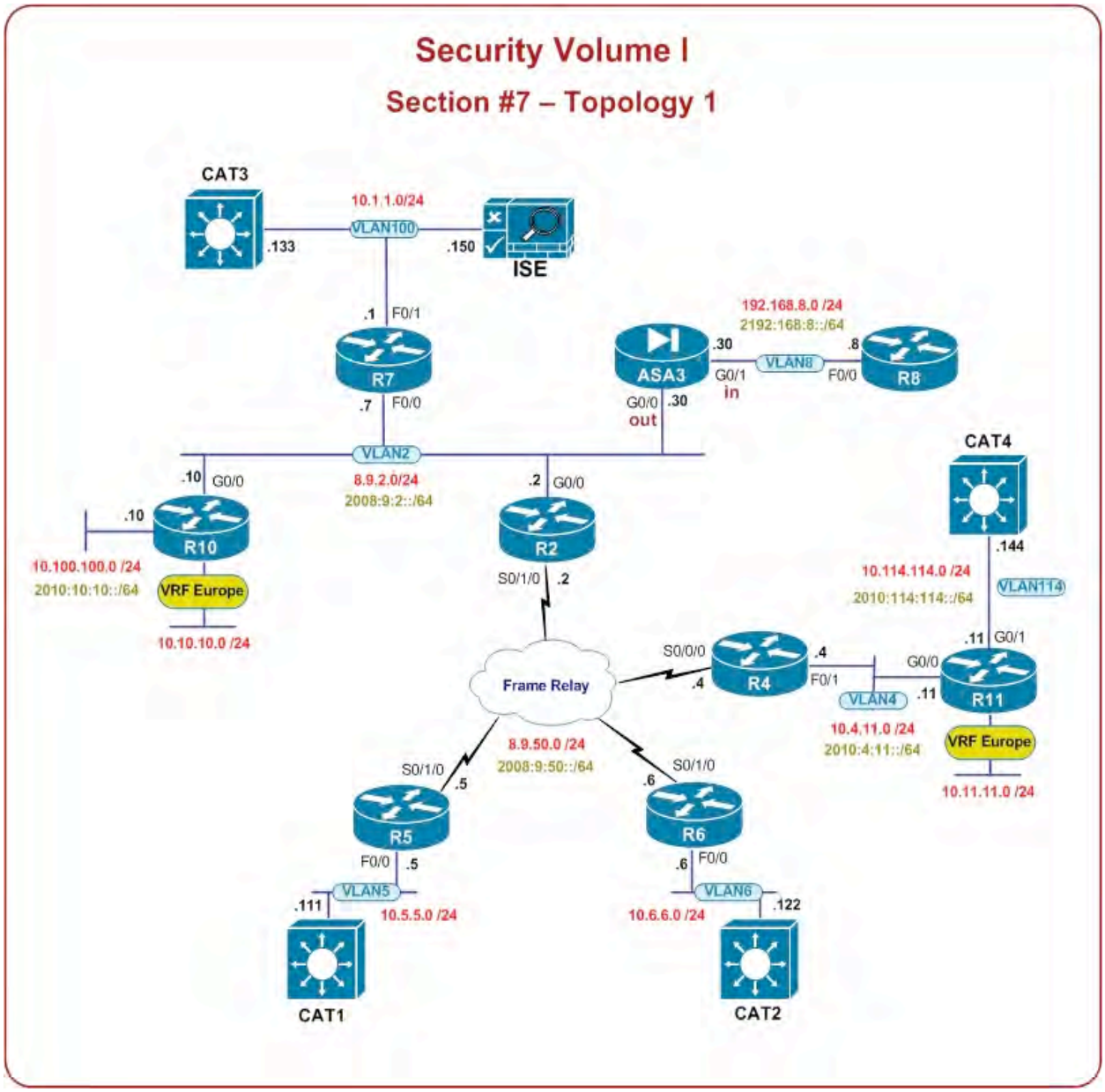
NOTE: *Static/default routes are NOT allowed unless otherwise stated in the task*

Estimated Time to Complete: **12 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R2	G0/0	2	8.9.2.2/24 2008:9:2::2/64
	Ser0/1/0		8.9.50.2/24 2008:9:50::2/64
R4	Fa0/1	4	10.4.11.4/24 2010:4:11::4/64
	Ser0/0/0		8.9.50.4/24 2008:9:50::4/64
R5	Fa0/0	5	10.5.5.5/24
	Ser0/1/0		8.9.50.5/24 2008:9:50::5/64
R6	Fa0/0	6	10.6.6.6/24
	Ser0/1/0		8.9.50.6/24 2008:9:50::6/64
R7	Fa0/0	2	8.9.2.7/24
	Fa0/1	100	10.1.1.1/24
R8	F0/0	8	192.168.8.8/24
R10	G0/0	2	8.9.2.10/24 2008:9:2::10/64
R11	G0/0	4	10.4.11.11/24 2010:4:11::11/64
CAT1	VLAN5	5	10.5.5.111/24
CAT2	VLAN6	6	10.6.6.122/24
CAT3	VLAN100	100	10.1.1.133/24
ASA3	G0/0 (outside)	2	8.9.2.30/24
	G0/1 (inside)	8	192.168.8.30/24
ISE	Internal NIC	100	10.1.1.150/24



Solutions

Task 1: IOS CA Server

- Make R2 start acting as IOS CA & CDP Server
- Use key-pair CAKEYS for that purpose
- Make sure CA keys can be further archived
- Automatically rollover Root Certificate 30 days prior to expiration
- Certificates should be granted automatically
- CRLs should be obtained through CDP
- Configure R2 as a NTP Server
- Synchronize R10 and R11 with the NTP Server
- R2, R10 and R11 should be in time zone GMT+1
- Daylight Savings Time should be enabled
- Use the domain name of ipexpert.com

Detailed Solution

R2

```
ip domain-name ipexpert.com

clock timezone GMT+1 1
clock summer-time CET recurring

ntp master 2
ntp source Loopback0

crypto key generate rsa label CAKEYS exportable modulus 1024

crypto pki trustpoint IOSCA
 revocation-check crl
 rsakeypair CAKEYS

crypto pki server IOSCA
 cdp-url http://2.2.2.2/cgi-bin/pkiclient.exe?operation=GetCRL
 database archive pem password ipexpert
 grant auto
 auto-rollover
 no sh

ip http server
```

R10

```
ip domain-name ipexpert.com
```

```
clock timezone GMT+1 1
clock summer-time CET recurring

ntp server 2.2.2.2
```

R10

```
ip domain-name ipexpert.com

clock timezone GMT+1 1
clock summer-time CET recurring

ntp server 2.2.2.2
ntp source loopback0
```

NTP configuration should be performed as soon as possible. This is because it may take some significant amount of time for the devices to synchronize. Keep in mind that usually it is a good idea to set the same time zone on all the devices (unless stated otherwise). If in doubt, go ahead and ask the proctor for clarification.

To force IOS to use the specific RSA Key Pair for IOS CA give it a name, which is exactly the same as the Key Pair label. The other solution (our) is to create IOS CA but without issuing "`no shut`" command and then moving to the CA's trustpoint which has been automatically created (or you can simply start with creating a trustpoint). There we could assign an arbitrary Key Pair and this way the CA name may be different than the Key Label. Note that so CA's Key Pair could be archived, keys have to be marked as "exportable".

CDP syntax can be found in the IOS Security Configuration Guide for PKI : "Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment", under "Certificate Revocation Lists (CRLs)"

Note that after 12.3(11)T, when the certificate server is turned on the first time, the CA certificate and CA key will be automatically generated. Key will be marked as "noexportable", however if automatic archive is also enabled (and by default it is) the CA certificate and the CA key will be still exported (archived) to the server database. For any manually generated Key Pairs you must make them "exportable" so they could be archived. The archive can be in PKCS12 or privacy-enhanced mail (PEM) format. The default file storage location is NVRAM.

Auto-Rollover feature allows certificates that are about to expire to be reissued automatically. When the CA certificate is expiring it must generate a new certificate and possibly a new key pair. This allows for continuous operation of the network while clients and the certificate server are switching from an expiring CA certificate to a new CA certificate. To use this feature CA certificate and key archive format and password has to be specified.

One important thing I did not mention before is that to start IOS CA service HTTP server has to be enabled.

IPv6 Considerations

In order to enroll using IPv6, the IPv6 address must be enclosed in brackets in the URL.

For example : `enrollment url http://[2001:DB8:1:1::1]:80`

Verification

```
R2#show crypto pki trustpoints status
Trustpoint IOSCA:
  Issuing CA certificate configured:
    Subject Name:
     cn=IOSCA
    Fingerprint MD5: F222A4CF 985D04D9 76D4DEB3 221742A8
    Fingerprint SHA1: 72BC4392 116FEF6D B9193300 7E10ACF3 6768D7E0
  State:
    Keys generated ..... Yes (General Purpose, exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None

R2(config)#cry pki server IOSCA
R2(cs-server)#no sh
Certificate server 'no shut' event has been queued for processing.
R2(config)#% Exporting Certificate Server signing certificate and keys...
Feb 23 13:18:58.876: %PKI-6-CS_ENABLED: Certificate server now enabled.

R2#sh cry pki server
Certificate Server IOSCA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=IOSCA
    CA cert fingerprint: F222A4CF 985D04D9 76D4DEB3 221742A8
    Granting mode is: auto
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 14:18:28 GMT+1 Feb 23 2016
    CRL NextUpdate timer: 20:18:35 GMT+1 Feb 23 2013
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Auto-Rollover configured, overlap period 30 days
    Autorollover timer: 14:18:28 GMT+1 Jan 24 2016

R2#sh cry pki ser IOSCA crl
Certificate Revocation List:
    Issuer: cn=IOSCA
```

```
    This Update: 14:18:35 GMT+1 Feb 23 2013
    Next Update: 20:18:35 GMT+1 Feb 23 2013
    Number of CRL entries: 0
    CRL size: 215 bytes

R2#sh cryto pki certificate
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=IOSCA
  Subject:
    cn=IOSCA
  Validity Date:
    start date: 14:18:28 GMT+1 Feb 23 2013
    end   date: 14:18:28 GMT+1 Feb 23 2016
  Associated Trustpoints: IOSCA

R10(config)#do sh ntp status
Clock is synchronized, stratum 3, reference is 2.2.2.2
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**21
reference time is D4D33FEB.DF561482 (14:17:31.872 GMT+1 Sat Feb 23 2013)
clock offset is -0.6923 msec, root delay is 0.81 msec
root dispersion is 7.33 msec, peer dispersion is 2.41 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000002 s/s
system poll interval is 64, last update was 238 sec ago.

R11(config)#do sh ntp association detail
2.2.2.2 configured, our_master, sane, valid, stratum 2
ref ID 127.127.1.1     , time D4D3431C.5913B541 (14:31:08.347 GMT+1 Sat Feb 23 2013)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.22, reach 377, sync dist 4.16
delay 2.11 msec, offset -3.1043 msec, dispersion 2.24
precision 2**24, version 4
org time 00000000.00000000 (01:00:00.000 GMT+1 Mon Jan 1 1900)
rec time D4D3431C.8C86CE25 (14:31:08.548 GMT+1 Sat Feb 23 2013)
xmt time D4D3431C.8C86CE25 (14:31:08.548 GMT+1 Sat Feb 23 2013)
filtdelay =     2.11    2.18    2.20    2.15    2.14    2.13    2.17    2.24
filtoffset =   -3.10   -3.01   -2.83   -2.69   -2.54   -2.40   -2.27   -2.07
filterror =     0.00    1.03    2.07    3.10    4.09    5.13    6.15    7.17
minpoll = 6, maxpoll = 10
```

Task 2: IOS – ASA L2L

- Create a VPN Tunnel on ASA3 and R5 protecting all IP traffic between VLANs 8 and 5
- For Phase I, create ISAKMP policy 30 on ASA and use its default values. Use PSK of "ipexpert". For Phase II use 3DES and SHA algorithms
- On the ASA3, ensure that ICMP traffic is not allowed across the tunnel

- Create an additional loopback 30 on R5. Assign it an IP address of 10.30.30.5/24
- Add traffic sourced from this newly created loopback into the existing tunnel
- Give priority treatment to all telnet packets flowing between VLAN5 and VLAN8 across the VPN tunnel on R5 and restrict this traffic to 200Kbps. Loopback 30 traffic should not be subject to this policy
- You are allowed to use 2 static routes in this task

Detailed Solution

R5

```
ip access-list extended QOS
 permit tcp 10.5.5.0 0.0.0.255 192.168.8.0 0.0.0.255 eq telnet
 permit tcp 10.5.5.0 0.0.0.255 eq telnet 192.168.8.0 0.0.0.255

class-map match-all QOS
 match access-group name QOS

policy-map QOS
 class QOS
  priority 200

crypto isakmp policy 30
 auth pre-share
 encryption 3des
 hash sha
 group 2

cry isakmp key 0 ipexpert address 8.9.2.30

access-list 120 permit ip 10.5.5.0 0.0.0.255 192.168.8.0 0.0.0.255
access-list 120 permit ip 10.30.30.0 0.0.0.255 192.168.8.0 0.0.0.255

cry ipsec transform-set SET1 esp-3des esp-sha-hmac

crypto map MAP1 10 ipsec-isakmp
 set peer 8.9.2.30
 set transform-set SET1
 match address 120
 reverse-route static

interface Serial0/1/0
 service-policy output QOS
 crypto map MAP1

interface loopback 30
 ip add 10.30.30.5 255.255.255.0
```

```
crypto map CMAP1 10 ipsec-isakmp
qos pre-classify
```

ASA3

```
crypto ikev1 policy 30

access-list PROXYACL extended permit ip 192.168.8.0 255.255.255.0 10.5.5.0
255.255.255.0
access-list PROXYACL extended permit ip 192.168.8.0 255.255.255.0 10.30.30.0
255.255.255.0

access-list VPNFILTER extended deny icmp any any
access-list VPNFILTER extended permit ip any any

group-policy L2L internal
group-policy L2L attributes
 vpn-filter value VPNFILTER

tunnel-group 8.9.50.5 type ipsec-l2l
tunnel-group 8.9.50.5 ipsec-attributes
 ikev1 pre-shared-key ipexpert
tunnel-group 8.9.50.5 general-attributes
 default-group-policy L2L

crypto ipsec ikev1 transform-set SET1 esp-3des esp-sha-hmac

crypto map MAP1 10 match address PROXYACL
crypto map MAP1 10 set peer 8.9.50.5
crypto map MAP1 10 set ikev1 transform-set SET1
crypto map MAP1 interface outside
crypto ikev1 enable outside

route outside 10.5.5.0 255.255.255.0 8.9.2.2 1
route outside 10.30.30.0 255.255.255.0 8.9.2.2 1

sysopt connection permit-vpn
```

VPN tunnel establishment consists of two phases – IKE Phase I where the “management” connection is established and IKE Phase II that is “data” connection. Phase I is required to protect Phase II information, so the encryption and authentication keys for the data connection can be exchanged securely. This connection uses UDP on port 500 and is bidirectional, which means that traffic flowing in both directions uses the same socket. Three things always occur in during ISAKMP/IKE Phase I :

1. The cryptographic algorithms to secure the connection are negotiated
2. Diffie-Hellman exchange occurs to derive a shared secret over an insecure medium

3. Peers authenticate each other. Possible authentication methods are : Pre-Shared Key, Digital Certificates and RSA-nonces (this last is available only on IOS)

Phase 1 consists of Main Mode or Aggressive Mode. Main Mode performs three two-packet exchanges, which totals to six packets. The advantage of Main Mode over Aggressive Mode is that authentication stage is performed across the already secured connection. Identity information (IKE ID) that two peers exchange is protected from eavesdropping attacks. Main Mode is the default when digital certificates are used for authentication for both – site-to-site and remote access VPNs.

Aggressive Mode is the default for Remote Access VPN connections when Pre-Shared Key is used for authentication. It is quicker in establishing the secure management connection. However, its downside is that any identity information is sent in clear text. Most commonly IKE ID values used are : IP address, FQDN, Group Name and DN.
The advantage of Aggressive Mode is the ability to use IKE ID as a key-matching (key lookup) criteria during Phase I authentication negotiation. This is because DH exchange is not completed before IKE IDs are exchanged. When Main Mode is used with Pre-Shared Key, DH happens before authentication stage and because it uses Pre-Shared Key in it's own calculations, only the peer's source ISAKMP packet IP address can be used to find it.

IKE Phase 2 has one mode, called Quick mode. Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec transform, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode exchanges nonces that are used to generate new shared secret key material and prevent replay attacks from generating bogus SAs. IPSec SAs are unidirectional. This plays an important role if there is a device, which may filter AH/ESP packets in the path between the security gateways.

To trigger the IPSec negotiation process the router will consult the SPD to see if there is a policy match for a packet. The SPD is built based on the access-list defined for interesting traffic. As the access-list includes the packet's source and destination address, the router will decide that the traffic needs to be IPSec protected. The next step is to see if an IKE or IPSec SA is already established to the IPSec peer. Because this is the first packet to this destination, there will be no SA existing in the SADB. All packets that match this policy can be queued or dropped until the IKE and IPSec SA are established. IOS IPSec drops all packets while waiting for IKE and IPSec SAs to be established. That's why if you ping you will first see some one- or two-packet loss.

For the negotiation to be successful, few requirements have to be met. For ISAKMP phase I authentication method, encryption & integrity algorithms and DH group must match. For lifetime, lower value will be negotiated if they don't match. For phase II IPSec security protocols (ESP, AH), encryption and integrity algorithms, transport/tunnel mode and Proxy ACLs must match.

On the ASA basic L2L configuration involves adding few elements comparing to IOS. Tunnel Group is a connection profile used to specify some tunnel-related parameters such as Authentication Server.

Group Policy, on the other hand, defines attributes we will apply to the connecting users. These two elements are more relevant to Remote Access VPNs, but for site-to-site at least the Tunnel Group must be defined.

You don't have to create ACL entries on the ASA for the IKE & IPSec traffic destined to the firewall itself (tunnels terminating on the ASA). However, if "`sysopt connection permit-vpn`" was turned off, you would have to create entries for the tunneled (protected) traffic. With this option set, however, all tunneled traffic is automatically allowed. To filter VPN traffic on the ASA use "`vpn-filter`" command which is a way to control protected/tunneled packets only.

IPSec processing happens before QoS on the IOS Routers. It means that if you were trying to match traffic for QoS classification, the only traffic you could match would be the IPSec protected traffic (AH or ESP). To match the unencrypted traffic, use "`qos pre-classify`" command. In our case this allows you to choose which exact traffic you want to prioritize. Also note that this command is not required on the ASA – it allows us to match unencrypted packets by default.

Finally, to meet the last requirement we can use "`reverse-route static`" option. It creates a route for the destination network from the Proxy ACL when the crypto map is applied to an interface.

IPv6 Considerations

On IOS it is possible to implement VPNs running on IPv6 using static crypto maps (dynamic ones are not supported with IPv6) or tunnel interfaces (VTIs). Crypto map support is platform and code version dependent (`crypto map ipv6` *`map_name`*; applied to the interface via `ipv6 crypto map`). Just remember that all address information would then also have to be IPv6 (address on the interface, peer's address, Proxy ACL etc.) – there is no way to protect IPv4 packets using IPv6 for transport.

The other way (widely supported) would be to use tunnel interfaces (SVTIs) with tunnel mode set to "`ipsec ipv6`". Example config :

```
interface Tunnel10
  ipv6 address 2001:1001::10/64
  ipv6 cef
  tunnel source G0/0
  tunnel destination 2013:10:2002::20
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile IPSEC_PROF
```

IPv6 on the ASA is implemented using regular Crypto Maps. Just make sure to use appropriate addresses in the Crypto Map and Proxy Access-list. There is also an option to select an IPv6 address for the connection for situations where you have multiple addresses configured on a port. Use the "`ipv6-local-address`" keyword when applying a crypto map to the interface.

Verification

```
R5#sh crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.8.0/255.255.255.0 [1/0] via 8.9.2.30 tag 0
                                on Serial0/1/0 RRI  S
```

BEFORE applying VPN Filter:

```
R5#ping 192.168.8.8 source f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.8, timeout is 2 seconds:
Packet sent with a source address of 10.5.5.5
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/29/32 ms

R5#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/1/0
Uptime: 00:00:49
Session status: UP-ACTIVE
Peer: 8.9.2.30 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.2.30
      Desc: (none)
  IKEv1 SA: local 8.9.50.5/500 remote 8.9.2.30/500 Active
          Capabilities:(none) connid:1001 lifetime:23:59:09
  IPSEC FLOW: permit ip 10.5.5.0/255.255.255.0 192.168.8.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4607787/3550
        Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4607787/3550
  IPSEC FLOW: permit ip 10.30.30.0/255.255.255.0 192.168.8.0/255.255.255.0
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
```

AFTER applying VPN Filter:

```
R5#ping 192.168.8.8 so f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.8, timeout is 0 seconds:
Packet sent with a source address of 10.5.5.5
.....
Success rate is 0 percent (0/5)

ASA3(config)# sh access-l VPNFILTER
access-list VPNFILTER; 2 elements; name hash: 0xa81069a6
access-list VPNFILTER line 1 extended deny icmp any any (hitcnt=5) 0x2701e672
access-list VPNFILTER line 2 extended permit ip any any (hitcnt=0) 0xef1d7408
```

BEFORE QoS Pre-Classify:

```
R5#telnet 192.168.8.8 /source-interface f0/0
Trying 192.168.8.8 ... Open

Password required, but none set

[Connection to 192.168.8.8 closed by foreign host]

R5#sh policy-map interface s0/1/0

 Serial0/1/0

  Service-policy output: QOS

    queue stats for all priority classes:

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

    Class-map: QOS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name QOS
      Priority: 200 kbps, burst bytes 5000, b/w exceed drops: 0


    Class-map: class-default (match-any)
      615 packets, 40494 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: any

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
```

```
      (pkts output/bytes output) 1405/117560

AFTER adding "qos pre-classify" to the Crypto Map :

R5#sh cry map int s0/1/0
Crypto Map "MAP1" 10 ipsec-isakmp
        Peer = 8.9.2.30
        Extended IP access list 120
            access-list 120 permit ip 10.5.5.0 0.0.0.255 192.168.8.0 0.0.0.255
            access-list 120 permit ip 10.30.30.0 0.0.0.255 192.168.8.0 0.0.0.255
        Current peer: 8.9.2.30
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                SET1:  { esp-3des esp-sha-hmac  } ,
        }
        QOS pre-classification
        Reverse Route Injection Enabled
        Interfaces using crypto map MAP1:
                Serial0/1/0


R5#telnet 192.168.8.8 /source-interface f0/0
Trying 192.168.8.8 ... Open

Password required, but none set

[Connection to 192.168.8.8 closed by foreign host]
R5#sh policy-map interface s0/1/0

 Serial0/1/0

  Service-policy output: QOS

    queue stats for all priority classes:

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 18/1816

    Class-map: QOS (match-all)
      18 packets, 1465 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: access-group name QOS
      Priority: 200 kbps, burst bytes 5000, b/w exceed drops: 0

      Class-map: class-default (match-any)
      677 packets, 45088 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

```
      Match: any

R5#telnet 192.168.8.8 /source-interface loopback30
Trying 192.168.8.8 ... Open

Password required, but none set

[Connection to 192.168.8.8 closed by foreign host]

R5#sh policy-map interface s0/1/0

 Serial0/1/0

  Service-policy output: QOS

    queue stats for all priority classes:

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 18/1816

    Class-map: QOS (match-all)
      18 packets, 1465 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name QOS
      Priority: 200 kbps, burst bytes 5000, b/w exceed drops: 0


    Class-map: class-default (match-any)
      747 packets, 50318 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 1665/140360

ASA3(config)# sh crypto isakmp sa detail

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 8.9.50.5
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
    Encrypt : 3des            Hash    : SHA
```

```
    Auth    : preshared       Lifetime: 86400
    Lifetime Remaining: 85801

There are no IKEv2 SAs


ASA3(config)# sh vpn-sessiondb det l2l

Session Type: LAN-to-LAN Detailed

Connection   : 8.9.50.5
Index        : 1                       IP Addr      : 8.9.50.5
Protocol     : IKEv1 IPsec
Encryption   : 3DES                    Hashing      : SHA1
Bytes Tx     : 1719                    Bytes Rx     : 2107
Login Time   : 07:20:01 UTC Sat Feb 23 2013
Duration     : 0h:11m:04s
IKEv1 Tunnels: 1
IPsec Tunnels: 2

IKEv1:
  Tunnel ID    : 1.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : 3DES                  Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 85736 Seconds
  D/H Group    : 2
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 1.2
  Local Addr   : 192.168.8.0/255.255.255.0/0/0
  Remote Addr  : 10.5.5.0/255.255.255.0/0/0
  Encryption   : 3DES                  Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 2936 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607999 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 24 Minutes
  Bytes Tx     : 1346                  Bytes Rx     : 1634
  Pkts Tx      : 25                    Pkts Rx      : 33

IPsec:
  Tunnel ID    : 1.3
  Local Addr   : 192.168.8.0/255.255.255.0/0/0
  Remote Addr  : 10.30.30.0/255.255.255.0/0/0
  Encryption   : 3DES                  Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3422 Seconds
```

```
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
  Bytes Tx     : 373                    Bytes Rx     : 473
  Pkts Tx      : 8                      Pkts Rx      : 11

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 664 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Task 3: IPv6 L2L IOS

- Create a site-to-site IPv6 VPN Tunnel between R10 and R11
- Protect communication between Loopback 100 interfaces
- Use AES 128 encryption, SHA-1 HMAC, DH group 5 and RSA-SIG for Phase I
- Use R2 as the CA
- Use the same encryption and authentication/integrity algorithms for Phase II and also make sure that any further session keys will not be derived based on previous ones
- You are allowed to configure two static routes in this task

Detailed Solution

R10

```
crypto pki trustpoint VPNTRUST
 enrollment url http://2.2.2.2:80
 password cisco123
 subject-name cn=R10.ipexpert.com, ou=INSTRUCTORS, l=San Jose, c=US
 revocation-check crl

crypto pki authen VPNTRUST
crypto pki enroll VPNTRUST

crypto isakmp policy 20
 authen rsa-sig
 encr aes
 hash sha
 group 5

ipv6 access-list PROXYACL
 permit ipv6 2010:10:10::/64 2011:11:11::/64

crypto ipsec transform-set SET2 esp-aes esp-sha-hmac

crypto pki certificate map CMAP 10
 subject-name co cn = r11.ipexpert.com
```

```
crypto isakmp profile ISA_PROF2
   match certificate CMAP

crypto map ipv6 MAP2 10 ipsec-isakmp
 set peer 2010:4:11::11
 set transform-set SET2
 set pfs group5
 set isakmp-profile ISA_PROF2
 match address PROXYACL

int g0/0
 ipv6 crypto map MAP2

ipv6 route 2011:11:11::/64 2008:9:2::2
```

R11

```
crypto pki trustpoint VPNTRUST
 enrollment url http://2.2.2.2:80
 password 7 030752180500701E1D
 subject-name cn=R11.ipexpert.com, ou=INSTRUCTORS, l=Warsaw, c=PL
 revocation-check crl
 source interface Loopback0

crypto pki authe VPNTRUST
crypto pki enroll VPNTRUST

crypto isakmp policy 20
 authen rsa-sig
 encr aes
 hash sha
 group 5

ipv6 access-list PROXYACL
 permit ipv6 2011:11:11::/64 2010:10:10::/64

crypto ipsec transform-set SET2 esp-aes esp-sha-hmac

crypto pki certificate map CMAP 10
 subject-name co cn = r10.ipexpert.com

crypto isakmp profile ISA_PROF2
 match certificate CMAP

crypto map ipv6 MAP2 10 ipsec-isakmp
 set peer 2008:9:2::10
 set transform-set SET2
 set pfs group5
 set isakmp-profile ISA_PROF2
 match address PROXYACL
```

```
int g0/0
 ipv6 crypto map MAP2

ipv6 route 2010:10:10::/64 2010:4:11::4
```

In this particular task we are asked to perform digital certificate authentication. It is good to know how the X.509 v3 digital certificate structure looks like :

- Version
- Serial Number
- Issuer
- Validity
- Subject (unstructed and structured portions)
- Subject Public Key Info
- Extensions (Optional)
- Certificate Signature Algorithm
- Certificate Signature

Structured portion of the certificate's Subject field is called Distinguish Name (DN). It has it's own attributes like CN, O, OU, C, L and so on. Unstructured portion consists of FQDN, which is always present, plus it may also contain the IP address and serial number.

Now few words about certificate validation process performed on the peer's identity certificate. After the trustpoint has been found (the one which contains the appropriate Root CA Certificate), certificate validation is performed. The signature, CRL list and validity dates are checked on the certificate (and possibly authorization is performed). If the certificate is verified, then it will be cached in the Public Key keyring. Certificate Maps (Certificate ACLs) can be used to perform an additional check or to skip some of the validation steps mentioned above. If the certificate of the peer matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the certificate of the peer, the certificate of the peer is considered valid. The validation steps, which can be omitted, are CRL and authorization check plus we can allow also the expired certificates. Note that cached certificates (which were previously successfully verified) are not subject to the validation process again until they time out. To manage the Public Keyring (you can clear the cache there) use "`crypto key pubkey-chain rsa`" command.

ISAKMP Profile is generally intended to set some additional Phase I negotiation parameters either when initiating VPN traffic or responding to it. There are two types ISAKMP Profiles : Request (which is used at the beginning of the negotiation) and Respond (which is used when IKE ID of the peer is received). Request Profile does not contain "`match`" command set, but it has to be applied either to a crypto map or IPSec Profile. Respond Profile must contain "`match`" option but it does not have to be applied.

Request Profile can be also a Respond Profile in the same time (when it contains “match” statement and is applied to the crypto map or IPSec Profile) and this is the most common implementation of this feature.

In our case we don’t set any additional parameters for the connection but the intent of using ISAKMP Profiles in this example is to show you how to match the incoming VPN connections to the Profile when digital certificates are used for authentication. The way this can be accomplished is by using Certificate Maps (same feature as what we can also used for certificate validation) - they allow us to match an arbitrary field from the peer’s certificate. In our case we are matching the CN field.

IPv6 Considerations

Extended IPv6 Ping (`ping ipv6`) may be useful when testing any IPv6 scenario. It allows you to send UDP Echos instead of ICMPv6, include Hop-by-Hop/Destination Options Extension Header or set a specific ToS setting.

Verification

```
R10#sh cry pki certificate
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=IOSCA
  Subject:
    Name: R10.ipexpert.com
    hostname=R10.ipexpert.com
    cn=R10.ipexpert.com
    ou=INSTRUCTORS
    l=San Jose
    c=US
  CRL Distribution Points:
    http://2.2.2.2/cgi-bin/pkiclient.exe?operation=GetCRL
  Validity Date:
    start date: 16:30:43 GMT+1 Feb 23 2013
    end   date: 16:30:43 GMT+1 Feb 23 2014
  Associated Trustpoints: VPNTRUST
  Storage: nvram:IOSCA#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=IOSCA
```

```
  Subject:
    cn=IOSCA
  Validity Date:
    start date: 14:18:28 GMT+1 Feb 23 2013
    end   date: 14:18:28 GMT+1 Feb 23 2016
  Associated Trustpoints: VPNTRUST
  Storage: nvram:IOSCA#1CA.cer

R11#sh cry pki cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 05
  Certificate Usage: General Purpose
  Issuer:
    cn=IOSCA
  Subject:
    Name: R11.ipexpert.com
    hostname=R11.ipexpert.com
    cn=R11.ipexpert.com
    ou=INSTRUCTORS
    l=Warsaw
    c=PL
  CRL Distribution Points:
    http://2.2.2.2/cgi-bin/pkiclient.exe?operation=GetCRL
  Validity Date:
    start date: 16:36:41 GMT+1 Feb 23 2013
    end   date: 16:36:41 GMT+1 Feb 23 2014
  Associated Trustpoints: VPNTRUST
  Storage: nvram:IOSCA#5.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=IOSCA
  Subject:
    cn=IOSCA
  Validity Date:
    start date: 14:18:28 GMT+1 Feb 23 2013
    end   date: 14:18:28 GMT+1 Feb 23 2016
  Associated Trustpoints: VPNTRUST
  Storage: nvram:IOSCA#1CA.cer

R2#deb cry pki mess
R2#deb cry pki server

R11# deb cry pki transaction
R11# deb cry pki validation
```

```
R11# deb cry pki messages


R10#ping 2011:11:11::11 so l100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2011:11:11::11, timeout is 2 seconds:
Packet sent with a source address of 2010:10:10::10

Feb 23 17:22:08.124: %CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH: ID of 2010:4:11::11 (type
5) and certificate addr with
Feb 23 17:22:08.124: %CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH: ID of 2010:4:11::11 (type
5) and certificate addr with .!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/6/8 ms

R11#
Feb 23 17:33:16.956: CRYPTO_PKI: Found a issuer match
Feb 23 17:33:16.956: CRYPTO_PKI: (A0017) Suitable trustpoints are: VPNTRUST,
Feb 23 17:33:16.956: CRYPTO_PKI: (A0017) Attempting to validate certificate using
VPNTRUST policy
Feb 23 17:33:16.956: CRYPTO_PKI: (A0017) Using VPNTRUST to validate certificate
Feb 23 17:33:16.956: CRYPTO_PKI: Prepare session revocation service providers
Feb 23 17:33:16.956:  CRYPTO_PKI: Deleting cached key having key id 5
Feb 23 17:33:16.956:
R11# CRYPTO_PKI: Attempting to insert the peer's public key into cache
Feb 23 17:33:16.956:  CRYPTO_PKI:Peer's public inserted successfully with key id 6
Feb 23 17:33:16.956:  CRYPTO_PKI: Expiring peer's cached key with key id 6
Feb 23 17:33:16.956: CRYPTO_PKI: (A0017) Certificate is verified
Feb 23 17:33:16.956: CRYPTO_PKI: (A0017) Checking certificate revocation
Feb 23 17:33:16.956: CRYPTO_PKI: (A0017) Starting CRL revocation check
Feb 23 17:33:16.956: CRYPTO_PKI: Matching CRL not found
Feb 23 17:33:1
R11#6.956: CRYPTO_PKI: (A0017)Retreive CRL using HTTP URI
Feb 23 17:33:16.956: CRYPTO_PKI: pki request queued properly
Feb 23 17:33:16.956: CRYPTO_PKI: Revocation check is complete, 0
Feb 23 17:33:16.956: CRYPTO_PKI: Revocation status = 3
Feb 23 17:33:16.956: CRYPTO_PKI: status = 0: poll CRL
Feb 23 17:33:16.956: CRYPTO_PKI: Remove session revocation service providers
Feb 23 17:33:16.960: CRYPTO_PKI: Sending Get Capabilities Request:
GET /cgi-bin/pkiclient.exe?operation=GetCACaps&message=VPNTRUST HTTP/

R2#
Feb 23 17:33:16.965: CRYPTO_CS: received a SCEP GetCACaps request
Feb 23 17:33:16.965: CRYPTO_CS: Capabilities sent
Feb 23 17:33:16.973: CRYPTO_CS: received a HTTP GetCRL request
Feb 23 17:33:16.973: CRYPTO_CS: CRL sent
```

…

```
Feb 23 17:33:16.984: CRYPTO_PKI: (A0017) Attempting to validate certificate using
VPNTRUST policy
Feb 23 17:33:16.984: CRYPTO_PKI: (A0017) Using VPNTRUST to validate certificate
Feb 23 17:33:16.984: CRYPTO_PKI: Prepare session revocation service p
R11#roviders
Feb 23 17:33:16.984: CRYPTO_PKI: (A0017) Checking certificate revocation
Feb 23 17:33:16.988: CRYPTO_PKI: (A0017) Starting CRL revocation check
Feb 23 17:33:16.988:  CRYPTO_PKI: Deleting cached key having key id 7
Feb 23 17:33:16.988:  CRYPTO_PKI: Attempting to insert the peer's public key into
cache
Feb 23 17:33:16.988:  CRYPTO_PKI:Peer's public inserted successfully with key id 8
Feb 23 17:33:16.988:  CRYPTO_PKI: Expiring peer's cached key with key id 8
Feb 23 17:33:16.988: CRYPTO_PKI: Re
R11#vocation check is complete, 0
Feb 23 17:33:16.988: CRYPTO_PKI: Revocation status = 0
Feb 23 17:33:16.988: CRYPTO_PKI: Remove session revocation service providers
Feb 23 17:33:16.988: CRYPTO_PKI: Remove session revocation service providers
Feb 23 17:33:16.988: CRYPTO_PKI: (A0017) Certificate validated
Feb 23 17:33:16.988: CRYPTO_PKI: Selected AAA username: 'R10.ipexpert.com'
Feb 23 17:33:16.988: CRYPTO_PKI: Selected AAA username: 'R10.ipexpert.com'
Feb 23 17:33:16.988: CRYPTO_PKI: (A0017)chain cert was anchored to trustpoint
VPNTRUST, and chain validation result was: CRYPTO_VALID_CERT
Feb 23 17:33:16.988: CRYPTO_PKI: (A0017) Validation TP is VPNTRUST
Feb 23 17:33:16.988: CRYPTO_PKI: (A0017) Certificate validation succeeded

R11#sh cry key pubkey-chain rsa
Codes: M - Manually configured, C - Extracted from certificate

Code Usage         IP-Address/VRF         Keyring          Name
C    Signing                              default          cn=Cisco Root CA
M1,o=Cisco
C    Signing                              default          cn=Cisco Root CA
2048,o=Cisco Systems
C    Signing                              default          cn=Cisco Manufacturing
CA,o=Cisco Systems
C    Signing                              default          ou=Class 3 Public Primary
Certification Authority,o=VeriSign, Inc.,c=US
C    Signing                              default          cn=IOSCA
C    Signing                              default          R10.ipexpert.com


R10#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
```

```
Profile: ISA_PROF2
Uptime: 00:08:31
Session status: UP-ACTIVE
Peer: 2010:4:11::11 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 2010:4:11::11
      Desc: (none)
  IKEv1 SA: local 2008:9:2::10/500
          remote 2010:4:11::11/500 Active
          Capabilities:(none) connid:1011 lifetime:23:51:28
  IPSEC FLOW: permit ipv6 2010:10:10::/64 2011:11:11::/64
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4264632/3088
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4264632/3088
```

Task 4: IPv6 VRF-Aware L2L

- Create a site-to-site IPv6 VPN Tunnel between R10 and R11
- Use Pre-Shared Key for authentication
- Protect all communication between devices that belong to VRF “Europe”
- You are not allowed to configure any static routes in this task

Detailed Solution

R10

```
crypto isakmp policy 10
 authentication pre-share

crypto isakmp key ipexpert address 11.11.11.11

access-list 125 permit ip 10.10.10.0 0.0.0.255 10.11.11.0 0.0.0.255

crypto isakmp profile ISA_PROF3
   vrf Europe
   keyring default
   match identity address 11.11.11.11 255.255.255.255

crypto map MAP3 10 ipsec-isakmp
 set peer 11.11.11.11
 set transform-set SET2
 set isakmp-profile ISA_PROF3
 match address 125
 reverse-route static

interface g0/0
 crypto map MAP3
```

R11

```
crypto isakmp policy 10
 authentication pre-share

crypto isakmp key ipexpert address 8.9.2.10

access-list 125 permit ip 10.11.11.0 0.0.0.255 10.10.10.0 0.0.0.255

crypto isakmp profile ISA_PROF3
   vrf Europe
   keyring default
   match identity address 8.9.2.10 255.255.255.255

crypto map MAP3 10 ipsec-isakmp
 set peer 8.9.2.10
 set transform-set SET2
 set isakmp-profile ISA_PROF3
 match address 125
 reverse-route static

crypto map MAP3 local-address Loopback0

int g0/0
 cry map MAP3
```

The VRF-Aware IPsec feature was created to allow mapping IP Security tunnels to MPLS Virtual Private Networks. The design problem with MPLS VPNs and IPSec becomes apparent when multiple IPSec tunnels try to terminate on a single interface, which is also an entry point to multiple VRFs. In that type of scenarios there is no way to say which VRF the protected traffic should belong to because the original IPSec specification does not provide any mechanism we could use to distinguish between tunnels originated by different Customers.

VRF-Aware IPSec feature provides a solution to this problem. The thing that is central to understand with this technology is that each IPSec tunnel is associated with two VRF domains. The outer, encapsulated packet, belongs to one VRF domain, known as Front VRF (FVRF), while the inner, protected IP packet belongs to another domain called Internal VRF (IVRF). Using a feature known as ISAKMP Profile can specify IVRF.

In our case only the most important setting we will specify is the IVRF (`ivrf`). Also remember that whenever PSK is used for authentication and ISAKMP Profile is used, a Key Ring (`keyring`) should be always specified.

Note ISAKMP Policy for PSK must be higher than RSA Sig one from the previous task. Otherwise the devices will try to authenticate using certificates.

To meet the last requirement from this task we are using static RRI feature that, when enabled, creates a route based on the destination portion of the Proxy ACL. Important thing to note here is that the VRF is properly reflected when using this method (including the Next-Hop for the prefix; Next-Hop is reachable through the global RIB).

IPv6 Considerations

As of 15.2 VRF-Aware IPSec does not work with IPv6. The problem is that the ISAKMP Profile only handles IPv4 VRFs (IPv6 VRF cannot be attached to the Profile – bug). Even if you activate IPv4 address-family in an IPv6 VRF and the "show" commands will confirm iVRF is specified for an IPv6 SA, router still cannot properly map tunneled packets to the VRF and all traffic ends up in the "default" (global) RIB. The same applies to SVTIs – they cannot properly handle IPv6 VRFs as of the current code.

Verification

```
R10#sh cry route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table Europe
10.11.11.0/255.255.255.0 [1/0] via 11.11.11.11 tag 0 count 2 rtid 1
                                on GigabitEthernet0/0 RRI  S

R10#sh ip route vrf Europe 10.11.11.11

Routing Table: Europe
Routing entry for 10.11.11.0/24
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 11.11.11.11 (default)
      Route metric is 0, traffic share count is 1

R10#ping vrf Europe 10.11.11.11 so loop200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.11.11.11, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.10
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms

R10#sh cry isa sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
```

```
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime
Cap.

1030  8.9.2.10        11.11.11.11     Europe ACTIVE des  sha    psk  1  23:58:49


R10#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Profile: ISA_PROF3
Uptime: 00:01:33
Session status: UP-ACTIVE
Peer: 11.11.11.11 port 500 fvrf: (none) ivrf: Europe
      Phase1_id: 11.11.11.11
      Desc: (none)
  IKEv1 SA: local 8.9.2.10/500 remote 11.11.11.11/500 Active
          Capabilities:(none) connid:1030 lifetime:23:58:26
  IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.11.11.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4180036/3506
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4180036/3506

R11#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Profile: ISA_PROF3
Uptime: 00:02:34
Session status: UP-ACTIVE
Peer: 8.9.2.10 port 500 fvrf: (none) ivrf: Europe
      Phase1_id: 8.9.2.10
      Desc: (none)
  IKEv1 SA: local 11.11.11.11/500 remote 8.9.2.10/500 Active
          Capabilities:(none) connid:1030 lifetime:23:57:25
  IPSEC FLOW: permit ip 10.11.11.0/255.255.255.0 10.10.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4260508/3445
```

```
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4260508/3445
```

Task 5: IPSec Remote Access IOS

- Configure R7 as Easy VPN Server
- Use 3DES and MD-5 algorithms for both phases
- Perform local authentication and authorization for remote users. Use the following parameters:
    - Username “ipexpert” with password “ipexpert”
    - Use the group name “LONDON”
    - Key should be set to “SkyFall”
    - Domain name should be “ipexpert.com”
    - Users should only access VLAN 100 through the tunnel
    - Don’t configure any IP address pool
- R7 should see the route to remote clients with distance of 15
- Configure R8 as a Easy VPN Client
- Create Loopback 8 interface (8.8.8.8/24) which will emulate internal network & client
- Make sure your credentials are stored on the device so you don’t have to type them whenever you connect
- For configuration of both, server & client, use a method that allows to apply additional features for only the tunneled packets

Detailed Solution

R7

```
aaa new-model
aaa authentication login NO none
aaa authentication login XAUTH local
aaa authorization network EZ_POL local

line con 0
 login authentication NO

username ipexpert password ipexpert

crypto isakmp policy 60
 auth pre
 encr 3des
 hash md5
 group 2

access-list 170 permit ip 10.1.1.0 0.0.0.255 any

crypto isakmp client configuration group LONDON
 key SkyFall
 acl 170
```

```
 domain ipexpert.com
 save-password

crypto isakmp profile ISA_PROF6
 match identity group LONDON
 client authentication list XAUTH
 isakmp authorization list EZ_POL
 client configuration address respond
 virtual-template 2

crypto ipsec transform-set SET6 esp-3des esp-md5-hmac

crypto ipsec profile IPSEC_PROF6
 set transform-set SET6
 set reverse-route distance 15
 set isakmp-profile ISA_PROF6

interface Virtual-Template2 type tunnel
 ip unnumbered F0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF6
```

R8

```
interface Virtual-Template1 type tunnel
 ip unnumbered FastEthernet0/0
 tunnel mode ipsec ipv4

crypto ipsec client ezvpn EZCLIENT
 connect manual
 group LONDON key SkyFall
 mode network-extension
 peer 8.9.2.7
 virtual-interface 1
 username ipexpert password ipexpert
 xauth userid mode local

interface Loopback8
 ip address 8.8.8.8 255.255.255.0
 crypto ipsec client ezvpn EZCLIENT inside
int f0/0
 crypto ipsec client ezvpn EZCLIENT
```

ASA3

```
object network R8NAT
 host 192.168.8.8
 nat (inside,outside) static 8.9.2.8
```

Easy VPN is Cisco's implementation of IPSec Remote Access VPNs. This type of Virtual Private Networks is different from site-to-site tunnels for a couple of reasons. First of all – we don't know in advance the Remote Peer's IP address. The other thing is that it is a centralized solution – vast majority of configuration is done on the headend (server) device to simplify configuration on the client. And that is actually the reason that regular L2L negotiation must be now somehow modified to support/implement this new paradigm. This is known as IKE Phase 1.5, which consists of three elements :

1. XAUTH - User authentication. This is different then device authentication performed in Phase I
2. Mode Config - If the Cisco IOS VPN device indicates that authentication was successful, the client requests further configuration parameters from the peer. The remaining system parameters (for example, IP address, DNS, and split tunnel attributes) are "pushed" to the client
3. After each client is assigned an internal IP address via Mode Configuration, it is important that the Cisco IOS VPN device knows how to route packets through the appropriate VPN tunnel. Reverse route injection (RRI) will ensure that a static route is created on the Cisco IOS VPN device for each client internal IP address

Easy VPN configuration leverages AAA for authentication and group authorization. Always remember to safeguard the console, even if you are not using a default list for authentication. In some cases you might get yourself lock out of the console, which on the real exam is one of those things we definitely would not like to run into.

There are two ways of configuring EasyVPN on IOS – legacy method using dynamic crypto maps (deprecated) or using Dynamic Virtual Tunnel Interfaces (DVTIs - recommended). The main advantage of DVTIs is the ability to apply other features to the VPN tunnels, such as ZFW or QoS, without affecting the physical interface and non-VPN packets.

In this task the Group Policy (PSK, Split Tunneling etc.) is configured locally on the router. For Split Tunneling configuration on IOS always remember to use extended ACLs (on ASA you may use a standard ACL). Note that syntax is a bit confusing - the source IP part of the ACL is used to specify the VPN destination network, which should be reachable through the tunnel.
ISAKMP Policy must use group DH 2 so the Easy VPN connection could be established, at least for the hardware clients.

The remaining configuration includes defining an ISAKMP Profile that binds AAA methods, tells the router to assign an IP address to the connecting client and specifies what Virtual Template Interface should be used for cloning. The Profile must be then nested under IPSec Profile where attach our transform-set (Phase II parameters) and can also tune RRI settings. Whenever you are using RRI routes as part of your solution remember that typically we would want to redistribute them (not necessary in this case). Here note that instead of setting a specific distance for RRI routes, we could tag them and further redistribute only those tagged routes using route-maps to match them.

Another technology used in this lab is Cisco Easy VPN Remote, which makes a router act as an Easy VPN Client. Similar to the server setup, it can be configured by using one of the two methods – with or

without VTIs. As a general rule if you configure a server to use DVTIs, configure the client in the same way. DVTIs is also a recommended method.

This feature supports three modes of operation: client, network extension, and network extension plus:

Client - Specifies that NAT or PAT be done so that the PCs and other hosts at the remote end of the VPN tunnel form a private network that does not use any IP addresses in the IP address space of the destination server. An enhancement has been made so that the IP address that is received via mode configuration is automatically assigned to an available loopback interface. The IPsec Security Associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

Network extension - Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts at the destination network.

Network extension plus (mode network-plus) - Identical to network extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec SAs for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

All modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an Internet service provider (ISP) or other service - thereby eliminating the corporate network from the path for web access.
The "`save-password`" option has to be set on the server to allow clients to store their credentials locally.

NAT on the ASA is needed since 192.168.8.0/24 is not advertised into OSPF. Since NAT-T is negotiated there is no need to create any entries on the outside interface ACL for ESP.

IPv6 Considerations
Remember that legacy implementation of Remote Access VPNs (dynamic crypto map) cannot be configured for IPv6 on IOS.

With DVTIs, tunnel interface mode should be definitely set to "`ipsec ipv6`". Also if you are using Client Mode, IP pool should be configured using "`ipv6 local pool`".

Regular Cisco VPN Client does not support IPv6. Use AnyConnect instead.

Verification

```
R7#deb crypto isakmp
```

```
R8#crypto ipsec client ezvpn connect

                                --- OUTPUT OMITTED ---
*Feb 24 16:06:11.405: ISAKMP (1007): received packet from 8.9.2.8 dport 4500 sport
4500 Global (R) QM_IDLE
*Feb 24 16:06:11.405: ISAKMP: set new node -1414004014 to QM_IDLE
*Feb 24 16:06:11.409: ISAKMP:(1007):processing transaction payload from 8.9.2.8.
message ID = -1414004014
*Feb 24 16:06:11.409: ISAKMP: Config payload REQUEST
*Feb 24 16:06:11.409: ISAKMP:(1007):checking request:
*Feb 24 16:06:11.409: ISAKMP:    MODECFG_CONFIG_URL
*Feb 24 16:06:11.409: ISAKMP:    MODECFG_CONFIG_VERSION
*Feb 24 16:06:11.409: ISAKMP:    MODECFG_IPSEC_INT_CONF
*Feb 24 16:06:11.409: ISAKMP:    IP4_DNS
*Feb 24 16:06:11.409: ISAKMP:    IP4_DNS
*Feb 24 16:06:11.409: ISAKMP:    IP4_NBNS
*Feb 24 16:06:11.409: ISAKMP:    IP4_NBNS
*Feb 24 16:06:11.409: ISAKMP:    SPLIT_INCLUDE
*Feb 24 16:06:11.409: ISAKMP:    SPLIT_DNS
*Feb 24 16:06:11.409: ISAKMP:    DEFAULT_DOMAIN
*Feb 24 16:06:11.409: ISAKMP:    MODECFG_SAVEPWD
*Feb 24 16:06:11.409: ISAKMP:    INCLUDE_LOCAL_LAN
*Feb 24 16:06:11.409: ISAKMP:    PFS
*Feb 24 16:06:11.409: ISAKMP:    BACKUP_SERVER
*Feb 24 16:06:11.409: ISAKMP:    APPLICATION_VERSION
*Feb 24 16:06:11.409: ISAKMP: Client Version is : Cisco IOS Software, 2800 Software
(C2800NM-ADVENT
*Feb 24 16:06:11.409: ISAKMP:    MODECFG_BANNER
*Feb 24 16:06:11.409: ISAKMP:    MODECFG_HOSTNAME
*Feb 24 16:06:11.409: ISAKMP/author: Author request for group LONDON successfully
sent to AAA
*Feb 24 16:06:11.409: ISAKMP:(1007):Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
*Feb 24 16:06:11.409: ISAKMP:(1007):Old State = IKE_P1_COMPLETE  New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

*Feb 24 16:06:11.429: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access1, changed state to down
*Feb 24 16:06:11.429: ISAKMP:(1007):attributes sent in message:
*Feb 24 16:06:11.429: ISAKMP: Sending IPsec Interface Config reply value 1
*Feb 24 16:06:11.429: ISAKMP: Sending split include name 170 network 10.1.1.0 mask
255.255.255.0 protocol 0, src port 0, dst port 0

*Feb 24 16:06:11.429: ISAKMP: Sending DEFAULT_DOMAIN default domain name:
ipexpert.com
*Feb 24 16:06:11.429: ISAKMP: Sending save password reply value 1
*Feb 24 16:06:11.429: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS
Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 15.1(3)T4, RELEASE
SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 24-May-12 01:37 by prod_rel_team
*Feb 24 16:06:11.429: ISAKMP (1007): Unknown Attr: MODECFG_HOSTNAME (0x700A)
*Feb 24 16:06:11.429: ISAKMP:(1007): responding to peer config from 8.9.2.8. ID = -
1414004014
*Feb 24 16:06:11.429: ISAKMP: Marking node -1414004014 for late deletion
*Feb 24 16:06:11.429: ISAKMP:(1007): sending packet to 8.9.2.8 my_port 4500
peer_port 4500 (R) CONF_ADDR
*Feb 24 16:06:11.433: ISAKMP:(1007):Sending an IKE IPv4 Packet.
*Feb 24 16:06:11.433: ISAKMP:(1007):Talking to a Unity Client
*Feb 24 16:06:11.433: ISAKMP:(1007):Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
*Feb 24 16:06:11.433: ISAKMP:(1007):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT  New
State = IKE_P1_COMPLETE

*Feb 24 16:06:11.433: ISAKMP:FSM error - Message from AAA grp/user.

*Feb 24 16:06:11.437: ISAKMP:(1007):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Feb 24 16:06:11.437: ISAKMP:(1007):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE

*Feb 24 16:06:11.437: ISAKMP:(1007):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Feb 24 16:06:11.437: ISAKMP:(1007):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE

*Feb 24 16:06:11.441: ISAKMP (1007): received packet from 8.9.2.8 dport 4500 sport
4500 Global (R) QM_IDLE
*Feb 24 16:06:11.441: ISAKMP: set new node 63663990 to QM_IDLE
*Feb 24 16:06:11.441: ISAKMP:(1007):processing transaction payload from 8.9.2.8.
message ID = 63663990
*Feb 24 16:06:11.445: ISAKMP: Config payload SET
*Feb 24 16:06:11.445: ISAKMP:(1007):checking SET:
*Feb 24 16:06:11.445: ISAKMP:    MODECFG_IP4_ROUTE
*Feb 24 16:06:11.445: ISAKMP:(1007):attributes sent in message:
*Feb 24 16:06:11.445:         Client subnet: 8.8.8.0 255.255.255.0
*Feb 24 16:06:11.445: ISAKMP:(1007): sending packet to 8.9.2.8 my_port 4500
peer_port 4500 (R) CONF_ADDR
*Feb 24 16:06:11.445: ISAKMP:(1007):Sending an IKE IPv4 Packet.
*Feb 24 16:06:11.445: ISAKMP:(1007):deleting node 63663990 error FALSE reason "No
Error"
*Feb 24 16:06:11.445: ISAKMP:(1007):Input = IKE_MESG_FROM_PEER, IKE_CFG_SET
*Feb 24 16:06:11.445: ISAKMP:(1007):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE

*Feb 24 16:06:11.445: ISAKMP:(1007):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Feb 24 16:06:11.449: ISAKMP:(1007):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
                                --- OUTPUT OMITTED ---
```

```
R7#sh crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
8.8.8.0/255.255.255.0 [15/0] via Virtual-Access1 tag 0 VTI

R7#sh crypto isakmp peer det
Peer: 8.9.2.8 Port: 4500 Local: 8.9.2.7
 Phase1 id: LONDON
  flags:
 NAS Port: 1 (Normal)
Configuration:
Configured Address: 0.0.0.0, State: free,   Attributes: RESPOND
  XAUTH: user ipexpert      FLAGS: (Need xauth on next phase 1) (xauth done)

Group Policy :
  group name      = LONDON
  pre-shared key = SkyFall
  address pool    =
  default domain = ipexpert.com
  configuration URL [version] =  [0]
  acl             = 170
  dns primary     = 0.0.0.0
  dns secondary   = 0.0.0.0
  wins primary    = 0.0.0.0
  wins secondary = 0.0.0.0
  save password  = on
  smartcard_removal_disconnect  = disable
  pfs             = off
  banner =
  local_lan       = off
  split-dns     =
  backup-servers =

User Config :
  local_lan       = off
  save password  = off

  IKE SAs: 1 IPSec SA bundles: 1
  last_locker: 0x44A1B810, last_last_locker: 0x0
  last_unlocker: 0x0, last_last_unlocker: 0x0


R8#ping 10.1.1.1 so loop8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

```
R8#sh cry sess de
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access1
Uptime: 00:05:08
Session status: UP-ACTIVE
Peer: 8.9.2.7 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.2.7
      Desc: (none)
  IKEv1 SA: local 192.168.8.8/4500 remote 8.9.2.7/4500 Active
          Capabilities:CXN connid:1005 lifetime:23:54:18
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 4597241/3281
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4597242/3281

R7#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access1
Username: ipexpert
Profile: ISA_PROF6
Group: LONDON
Uptime: 00:11:12
Session status: UP-ACTIVE
Peer: 8.9.2.8 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: LONDON
      Desc: (none)
  IKEv1 SA: local 8.9.2.7/4500 remote 8.9.2.8/4500 Active
          Capabilities:CXN connid:1007 lifetime:23:48:46
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 4501691/2927
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4501692/2927
```

Task 6: IPSec Remote Access IOS with RADIUS

- Modify configuration from the previous task
- Authentication & Group Policy information should be now stored on ISE
- Use “outofcontrol” as RADIUS shared secret
- Connecting users should now get an IP address assigned from the 172.16.70.0/24 range
- You can add two static routes
- Re-configure R7 and R8 to meet these requirements

Detailed Solution

R7

```
no aaa authentication login XAUTH local
aaa authentication login XAUTH gr rad
no aaa authorization network EZ_POL local
aaa authorization network EZ_POL gr rad

no crypto isakmp client configuration group LONDON

radius-server host 10.1.1.150 key outofcontrol

ip local pool EZPOOL 172.16.70.1 172.16.70.254

ip route 8.8.8.0 255.255.255.0 8.9.2.30
```

R8

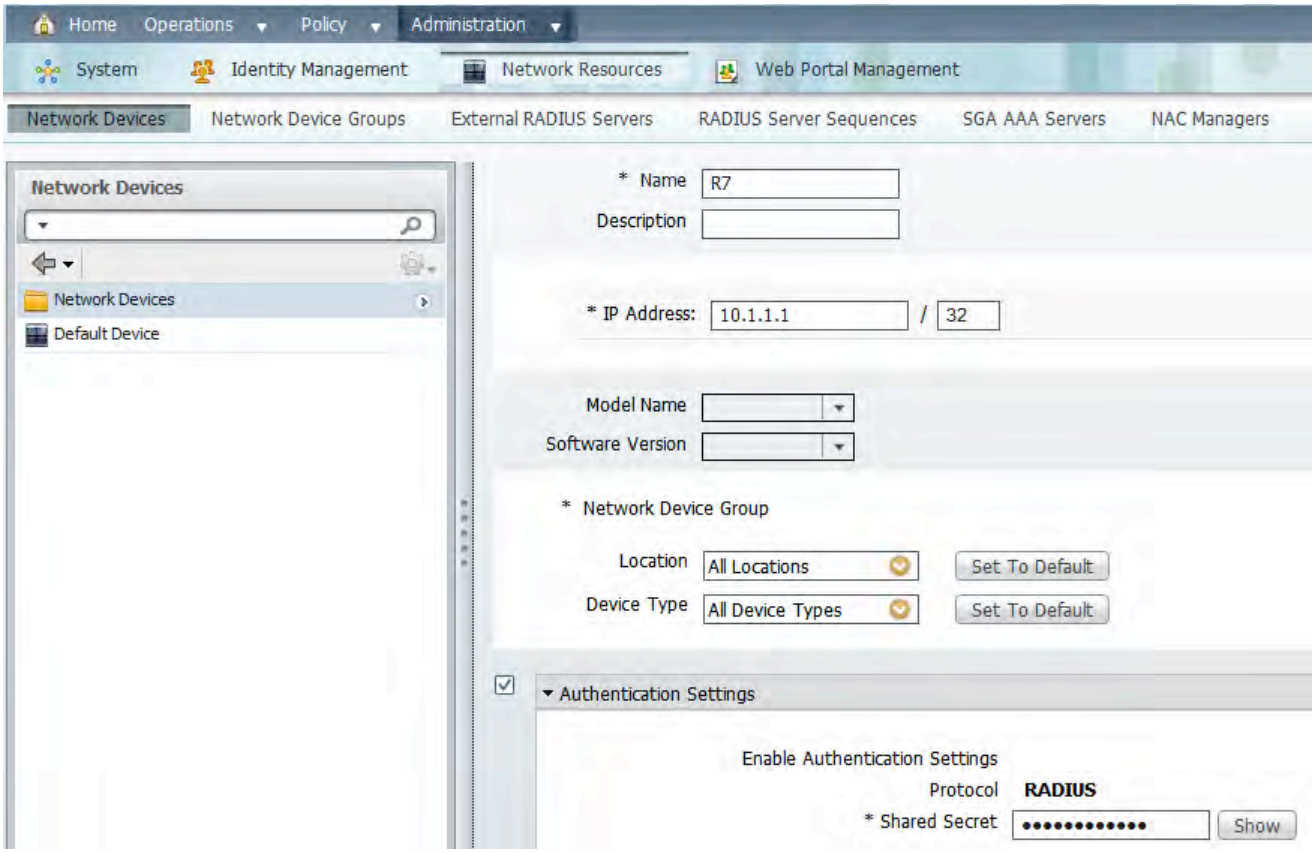
```
crypto ipsec client ezvpn EZCLIENT
 mode client
```

ASA3

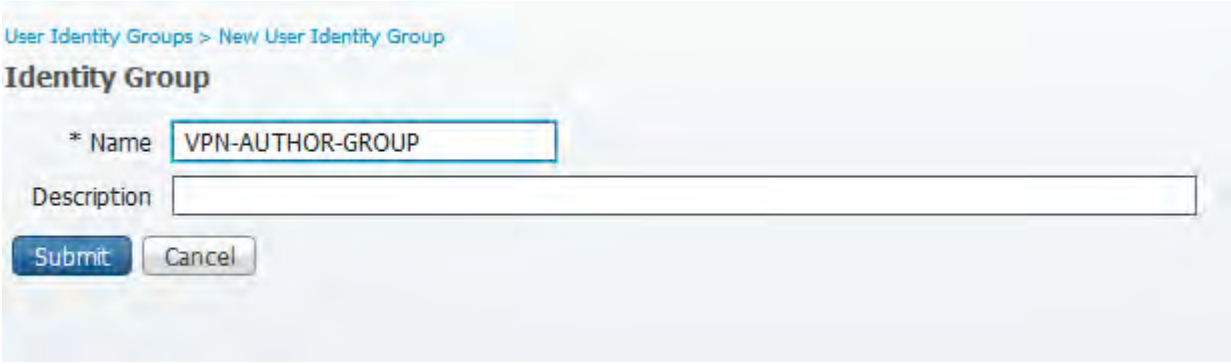
```
route inside 8.8.8.8 255.255.255.255 192.168.8.8
```

ISE

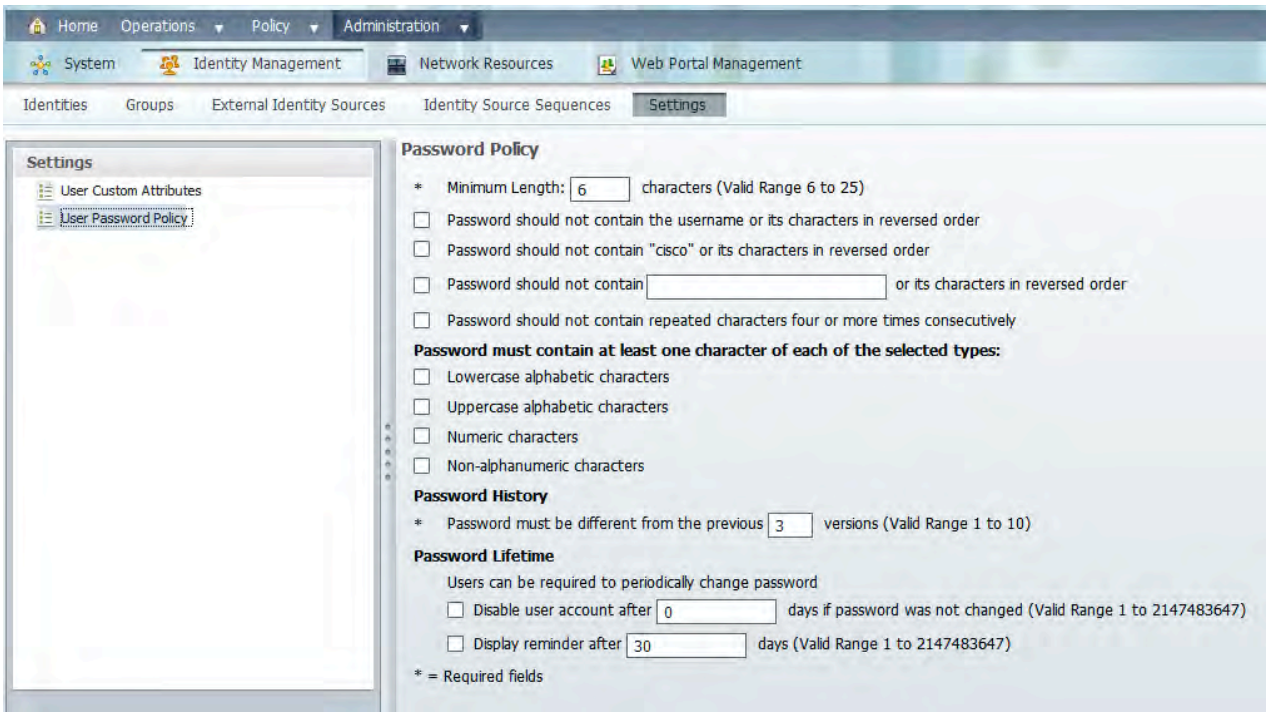
First thing we want to add R7 as AAA Client :



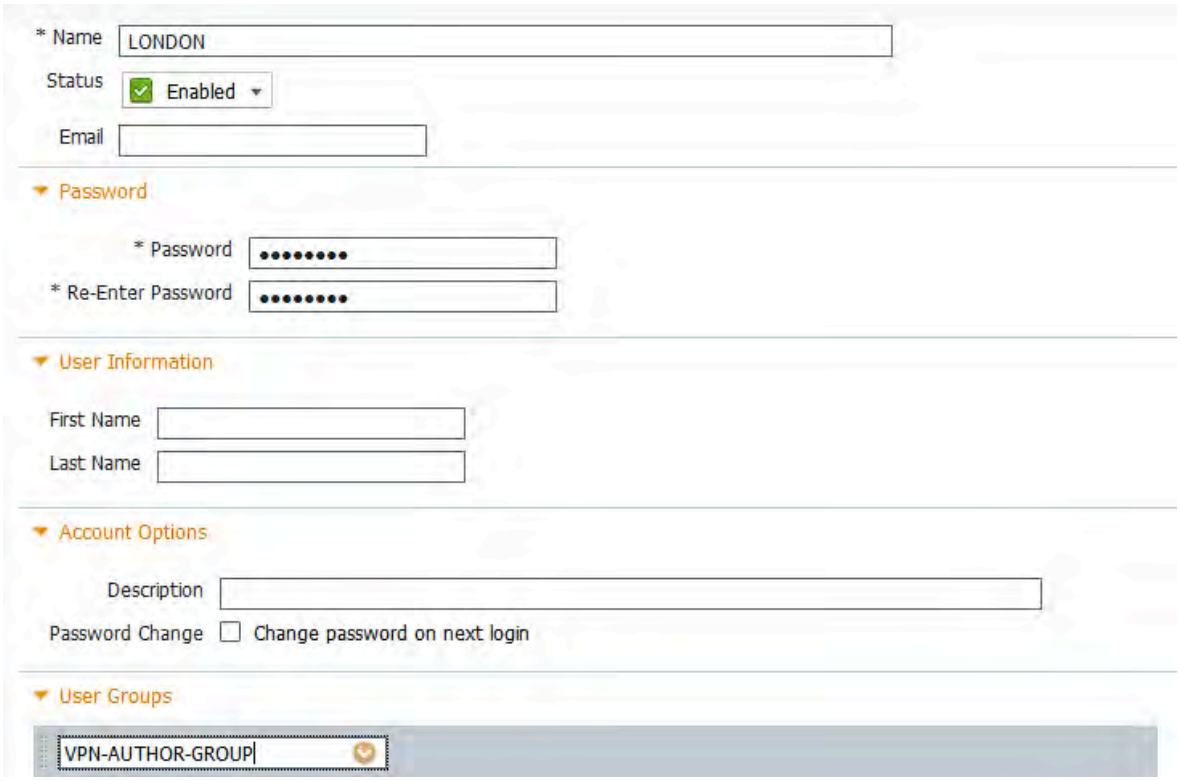
Then we should create a group for Users who symbolize the VPN Group Policy :

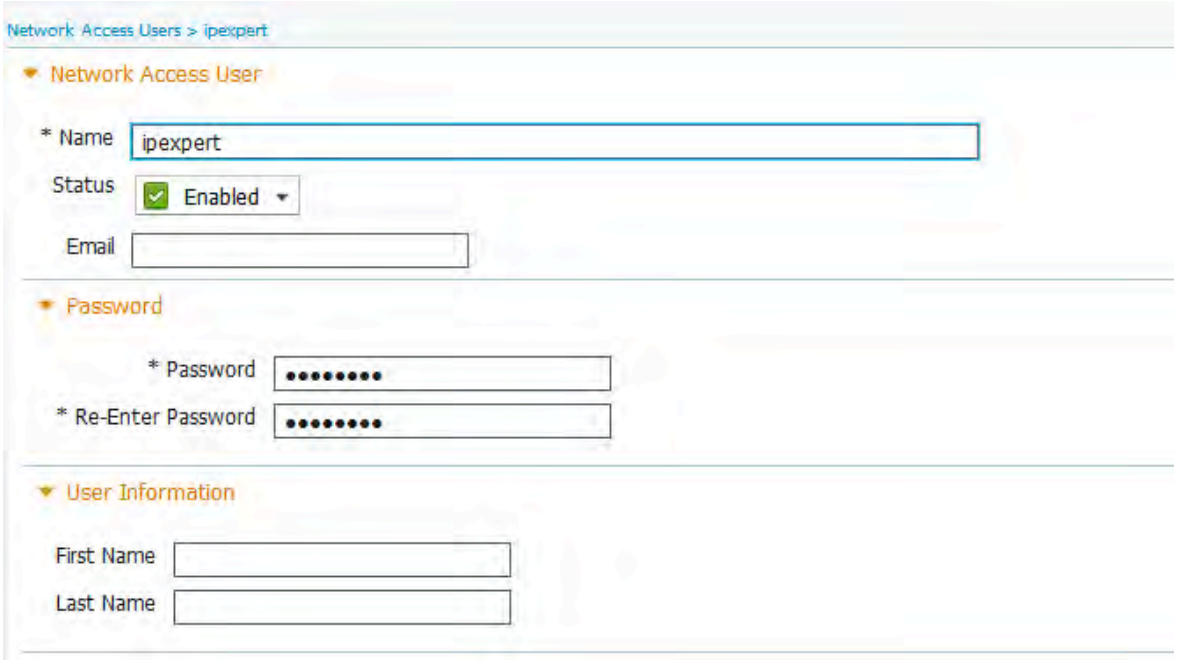


Before we start adding users it may be useful to change the Password Policy settings. This is just to remove the restrictions configured by default :

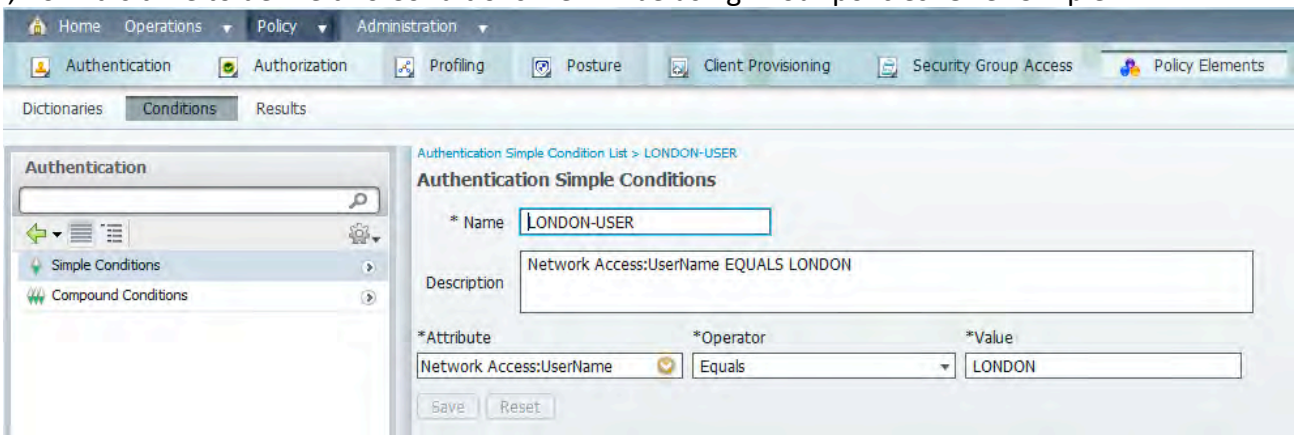


Next we will need to create two users. One will represent the VPN Group Policy ("LONDON"; this is what NAS sends to ISE as the username) and the other one will be used during XAUTH ("ipexpert" in our case). Don't forget to add "LONDON" to the previously created group - "VPN-AUTHOR-GROUP":

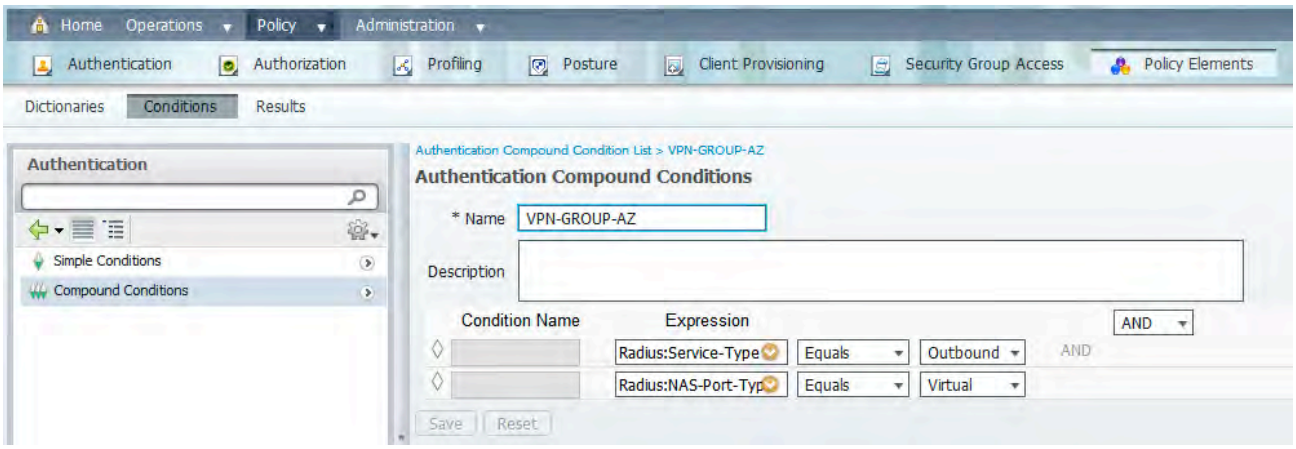




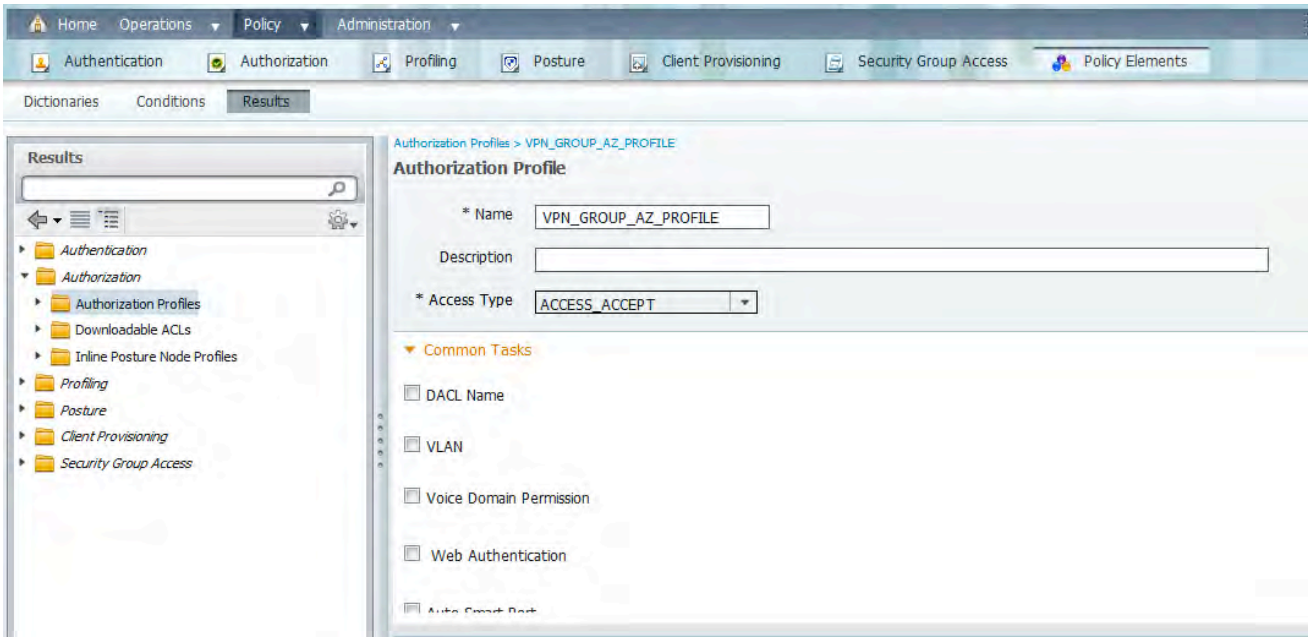
OK, now it is time to define two Conditions we will be using in our policies. One “Simple” :

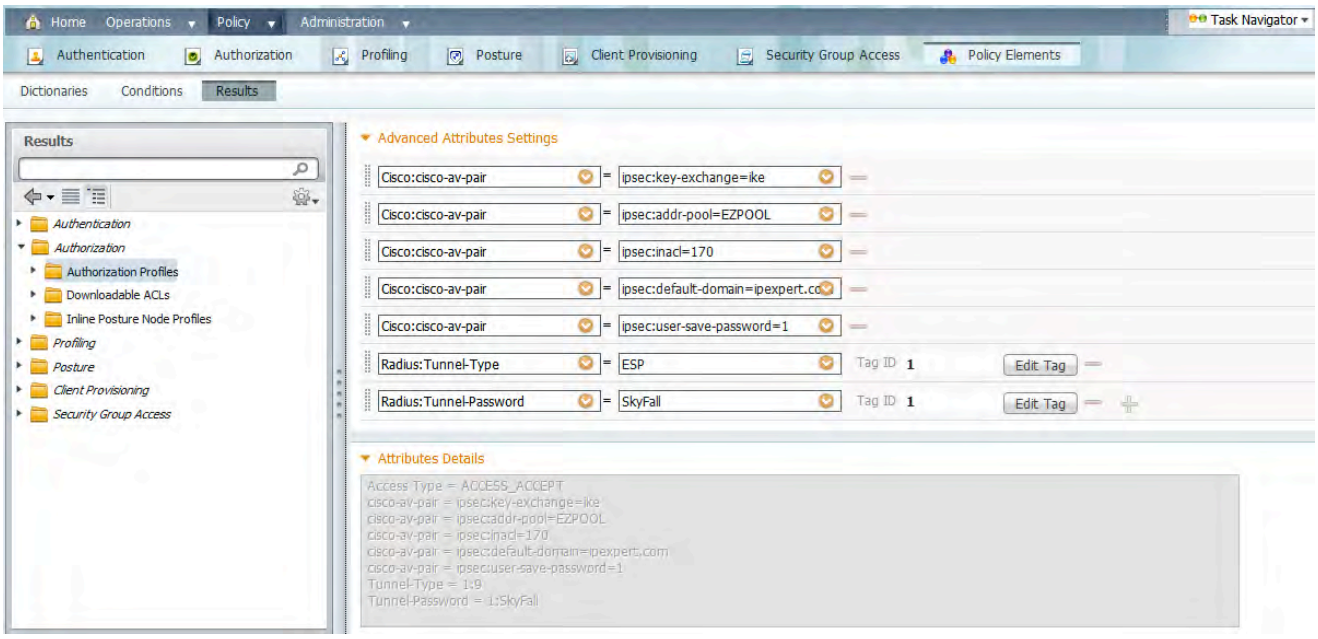


And the other one is “Compound” :

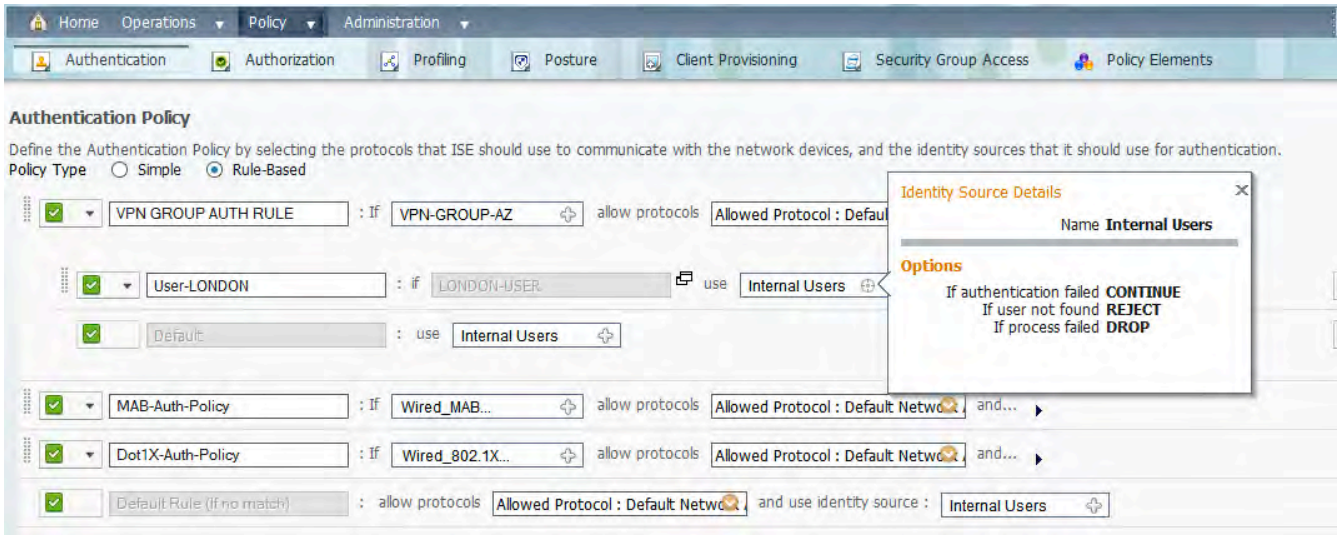


One more thing we will need is the Authorization Profile:

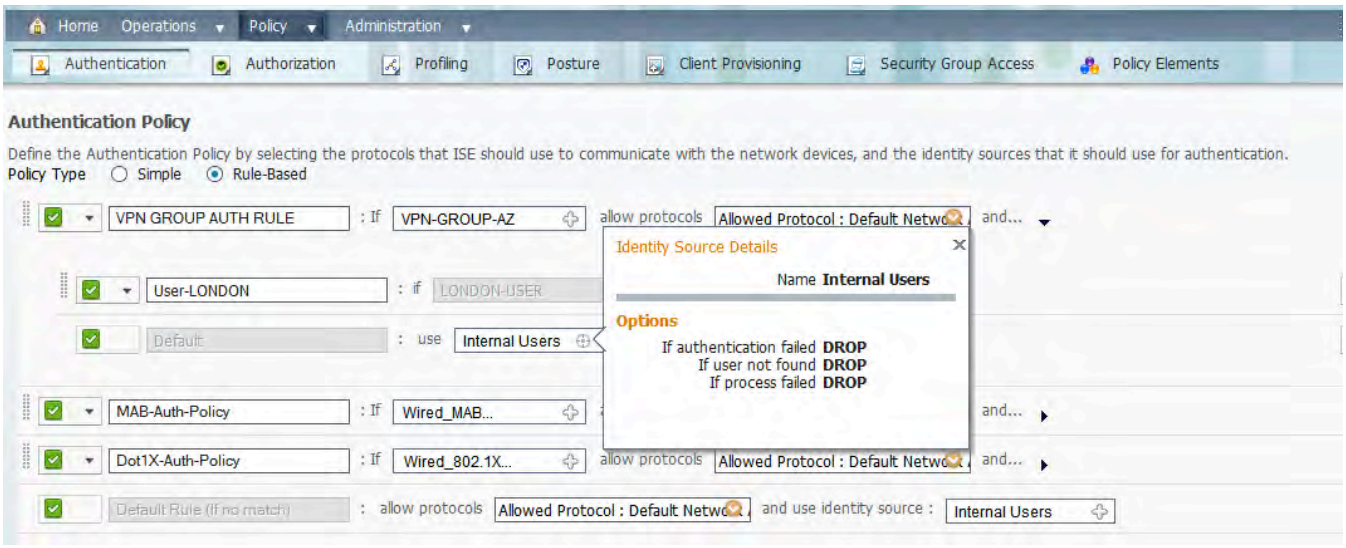




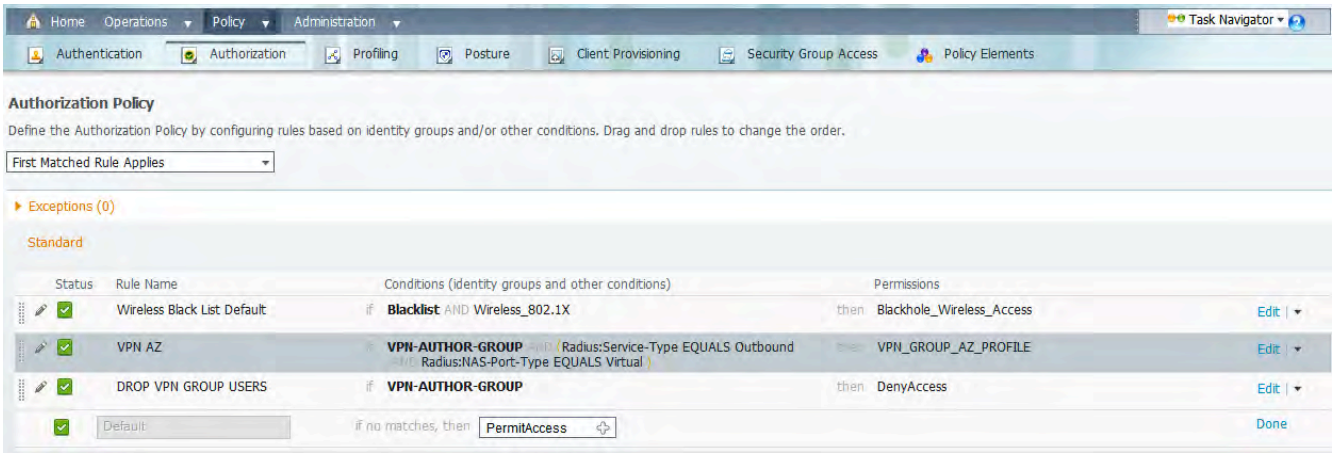
Now the policies. Let's start with Authentication:



Note that for the Identity Rule the "If authentication failed" is set to CONTINUE; then for any other user matching our rule we want to deny access.



And the Authorization Policy – the Group Policy Rule was added via "Create New Condition (Advanced Option)":



This tasks shows you how to use an external database (RADIUS) for both, user authentication and authorization (Group Policy download).

Easy VPN Server configuration does not need many modifications. We definitely need to change the authentication and authorization method lists to point to the RADIUS server; server should be also defined. On the VPN Client change the mode to "Client" (we will be using an IP pool) and then add a static route on the R7 and the ASA. You must also define an IP Pool on R7 (ISE will return its name).

ISE configuration is a bit more complicated. First thing you should understand here is that a VPN Group Policy is represented by a user account in the local ISE Identity Store. The user's name is exactly the same as Group Policy name; this is why in our case the user must be called "LONDON". Now before the attributes can be downloaded for this user, it must be first authenticated - and what router will be always sending as a password is "cisco". The problem with password "cisco" is that it is only 5

characters long, which does not meet the User Password Policy defined on ISE (minimum password length you can specify on ISE is 6 characters for a User). What it essentially means is that authentication will be always failing (since we cannot put the correct password) so what we need to do instead is to say that for this particular user we want to proceed to the Authorization Policy even if it fails authentication.

The second Authentication Identity Rule is just to make sure that any other user matching this Rule will never proceed to Authorization.

In the Authorization Policy we want to match VPN Group Authorization Requests (Service Type "Outbound" and NAS-Port-Type "Virtual" coming for all possible users (so VPN Groups) we know are valid names of VPN Groups we are using in our network. And obviously the Identity Group VPN-AUTHOR-GROUP is supposed to group those users. Note that there is one additional rule below just for the Group as a Condition – this is for situations when someone would try to use the VPN Group user credential to access our network (any service) - we definitely don't want to allow for this and that's why this Rule Denies Access (This is Spart…! I mean Security). Finally the Default Rule will be used to authorize our XAUTH user.

In this example all VPN attributes will be downloaded for the Group user i.e. will be applied to all users connecting to this VPN Group. It is also possible to change the structure of the Authorization Policy so part of the attributes would be applied to only a particular user (per-User Authorization). For this to work you would have to create separate AuthZ Rules, one for individual user.

Speaking of the Authorization Profile, Tunnel-Password attribute is the actual Pre-Shared Key for this connection. Tunnel Type must be set to "ESP", Key Exchange must be "IKE" and the remaining attributes build up our Group Policy. If you are interested in syntax for other attributes go to the Secure Connectivity IOS Configuration Guide and you can find it under "Easy VPN Server" -> "Example: RADIUS Group Profile with IPsec AV Pairs".

IPv6 Considerations

Address pool should be IPv6.

Verification

```
R8#crypto ipsec client ezvpn connect
```

```
R7#deb radius
```

Note that Group Authentication/Authorization happens twice – first to authenticate the tunnel (PSK) and assign an IP address, second to download other attributes we may want to assign to the user:

```
*Feb 24 20:36:49.804: RADIUS/ENCODE(00000023):Orig. component type = VPN IPSEC
*Feb 24 20:36:49.808: RADIUS:  AAA Unsupported Attr: interface         [209] 7
```

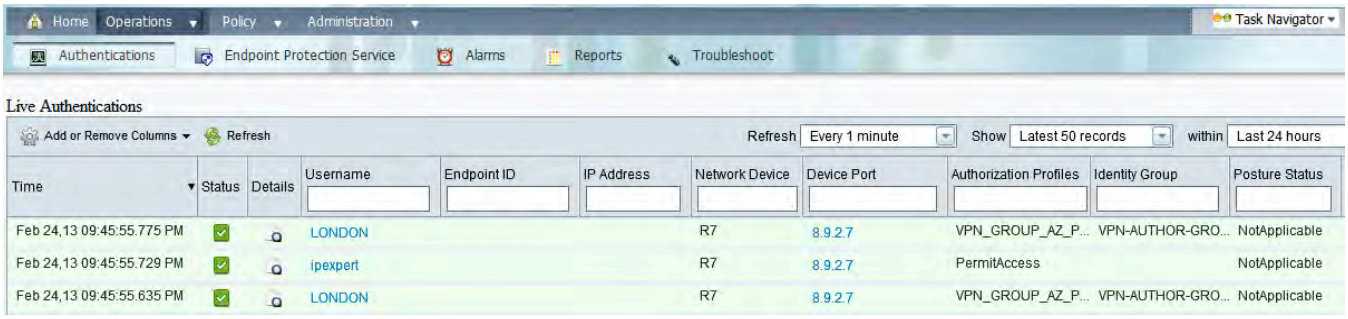
```
*Feb 24 20:36:49.808: RADIUS:   38 2E 39 2E 32             [ 8.9.2]
*Feb 24 20:36:49.808: RADIUS(00000023): Config NAS IP: 0.0.0.0
*Feb 24 20:36:49.808: RADIUS/ENCODE(00000023): acct_session_id: 23
*Feb 24 20:36:49.808: RADIUS(00000023): sending
*Feb 24 20:36:49.808: RADIUS/ENCODE: Best Local IP-Address 10.1.1.1 for Radius-
Server 10.1.1.150
*Feb 24 20:36:49.808: RADIUS(00000023): Send Access-Request to 10.1.1.150:1645 id
1645/15, len 85
*Feb 24 20:36:49.808: RADIUS:  authenticator 8F 56 EB 35 70 41 D3 27 - 49 8A E4 57
9C 3A F3 DB
*Feb 24 20:36:49.808: RADIUS:  User-Name           [1]   8   "LONDON"
*Feb 24 20:36:49.808: RADIUS:  User-Password       [2]   18  *
*Feb 24 20:36:49.808: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Feb 24 20:36:49.812: RADIUS:  NAS-Port-Type       [61]  6   Vir
R7#
R7#tual                    [5]
*Feb 24 20:36:49.812: RADIUS:  NAS-Port            [5]   6   1
*Feb 24 20:36:49.812: RADIUS:  NAS-Port-Id         [87]  9   "8.9.2.7"
*Feb 24 20:36:49.812: RADIUS:  Service-Type        [6]   6   Outbound
[5]
*Feb 24 20:36:49.812: RADIUS:  NAS-IP-Address      [4]   6   10.1.1.1
*Feb 24 20:36:49.812: RADIUS(00000023): Started 5 sec timeout
*Feb 24 20:36:49.844: RADIUS: Received from id 1645/15 10.1.1.150:1645, Access-
Accept, len 315
*Feb 24 20:36:49.844: RADIUS:  authenticator E0 73 53 0C 14 ED 64 6F - 22 92 92 9F
4E 49 B0 49
*Feb 24 20:36:49.844: RADIUS:  User-Name           [1]   8   "LONDON"
*Feb 24 20:36:49.844: RADIUS:  State               [24]  40
*Feb 24 20:36:49.844: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
[ReauthSession:0a]
*Feb 24 20:36:49.844: RADIUS:   63 38 30 36 66 34 30 30 30 30 30 46 33 43 35 31
[c806f400000F3C51]
*Feb 24 20:36:49.844: RADIUS:   32 41 37 38 46 41            [ 2A78FA]
*Feb 24 20:36:49.844: RADIUS:  Class               [25]  56
*Feb 24 20:36:49.844: RADIUS:   43 41 43 53 3A 30 61 63 38 30 36 66 34 30 30 30
[CACS:0ac806f4000]
*Feb 24 20:36:49.844: RADIUS:   30 30 46 33 43 35 31 32 41 37 38 46 41 3A 70 6F
[00F3C512A78FA:po]
*Feb 24 20:36:49.844: RADIUS:   64 31 32 34 69 73 65 2F 31 34 39 33 39 38 32 36
[d124ise/14939826]
*Feb 24 20:36:49.844: RADIUS:   34 2F 34 31 31 37            [ 4/4117]
*Feb 24 20:36:49.844: RADIUS:  Termination-Action  [29]  6   1
*Feb 24 20:36:49.844: RADIUS:  Tunnel-Type         [64]  6   01:ESP
[9]
*Feb 24 20:36:49.848: RADIUS:  Tunnel-Password     [69]  21  01:*
*Feb 24 20:36:49.848: RADIUS:  Vendor, Cisco       [26]  30
*Feb 24 20:36:49.848: RADIUS:   Cisco AVpair       [1]   24  "ipsec:key-
exchange=ike"
*Feb 24 20:36:49.848: RADIUS:  Vendor, Cisco       [26]  30
*Feb 24 20:36:49.848: RADIUS:   Cisco AVpair       [1]   24  "ipsec:addr-
pool=EZPOOL"
*Feb 24 20:36:49.848: RADIUS:  Vendor, Cisco       [26]  23
*Feb 24 20:36:49.848: RADIUS:   Cisco AVpair       [1]   17  "ipsec:inacl=170"
*Feb 24 20:36:49.848: RADIUS:  Vendor, Cisco       [26]  41
*Feb 24 20:36:49.848: RADIUS:   Cisco AVpair       [1]   35  "ipsec:default-
domain=ipexpert.com"
```

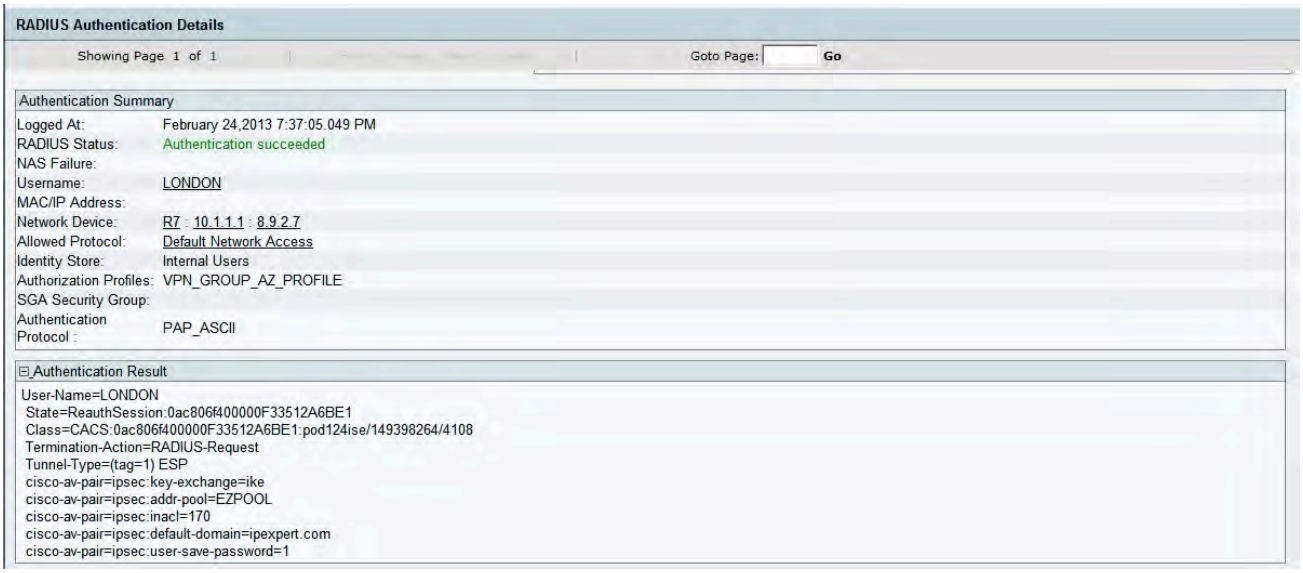
```
*Feb 24 20:36:49.848: RADIUS:  Vendor, Cisco       [26]  34
*Feb 24 20:36:49.848: RADIUS:   Cisco AVpair       [1]   28  "ipsec:user-save-
password=1"
*Feb 24 20:36:49.848: RADIUS(00000023): Received from id 1645/15
*Feb 24 20:36:49.920: RADIUS/ENCODE(00000024):Orig. component type = VPN IPSEC
*Feb 24 20:36:49.924: RADIUS:  AAA Unsupported Attr: interface         [209] 7
*Feb 24 20:36:49.924: RADIUS:   38 2E 39 2E 32             [ 8.9.2]
*Feb 24 20:36:49.924: RADIUS/ENCODE(00000024): dropping service type, "radius-server
attribute 6 on-for-login-auth" is off
*Feb 24 20:36:49.924: RADIUS(00000024): Config NAS IP: 0.0.0.0
*Feb 24 20:36:49.924: RADIUS/ENCODE(00000024): acct_session_id: 24
*Feb 24 20:36:49.924: RADIUS(00000024): sending
*Feb 24 20:36:49.924: RADIUS/ENCODE: Best Local IP-Address 10.1.1.1 for Radius-
Server 10.1.1.150
*Feb 24 20:36:49.924: RADIUS(00000024): Send Access-Request to 10.1.1.150:1645 id
1645/16, len 75
*Feb 24 20:36:49.924: RADIUS:  authenticator 50 F4 A7 91 32 FB D9 A3 - AD CB 12 07
3B C3 2E 98
*Feb 24 20:36:49.924: RADIUS:  User-Name           [1]   10  "ipexpert"
*Feb 24 20:36:49.924: RADIUS:  User-Password       [2]   18  *
*Feb 24 20:36:49.924: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Feb 24 20:36:49.924: RADIUS:  NAS-Port            [5]   6   1
*Feb 24 20:36:49.924: RADIUS:  NAS-Port-Id         [87]  9   "8.9.2.7"
*Feb 24 20:36:49.924: RADIUS:  NAS-IP-Address      [4]   6   10.1.1.1
*Feb 24 20:36:49.928: RADIUS(00000024): Started 5 sec timeout
*Feb 24 20:36:49.936: RADIUS: Received from id 1645/16 10.1.1.150:1645, Access-
Accept, len 132
*Feb 24 20:36:49.940: RADIUS:  authenticator CD C2 DA 6D 0D 6F 3C 4A - 16 B6 28 6A
F1 CB C5 16
*Feb 24 20:36:49.940: RADIUS:  User-Name           [1]   10  "ipexpert"
*Feb 24 20:36:49.940: RADIUS:  State               [24]  40
*Feb 24 20:36:49.940: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
[ReauthSession:0a]
*Feb 24 20:36:49.940: RADIUS:   63 38 30 36 66 34 30 30 30 30 30 46 33 44 35 31
[c806f400000F3D51]
*Feb 24 20:36:49.940: RADIUS:   32 41 37 38 46 41            [ 2A78FA]
*Feb 24 20:36:49.940: RADIUS:  Class               [25]  56
*Feb 24 20:36:49.940: RADIUS:   43 41 43 53 3A 30 61 63 38 30 36 66 34 30 30 30
[CACS:0ac806f4000]
*Feb 24 20:36:49.940: RADIUS:   30 30 46 33 44 35 31 32 41 37 38 46 41 3A 70 6F
[00F3D512A78FA:po]
*Feb 24 20:36:49.940: RADIUS:   64 31 32 34 69 73 65 2F 31 34 39 33 39 38 32 36
[d124ise/14939826]
*Feb 24 20:36:49.940: RADIUS:   34 2F 34 31 31 38            [ 4/4118]
*Feb 24 20:36:49.940: RADIUS:  Termination-Action  [29]  6   1
*Feb 24 20:36:49.940: RADIUS(00000024): Received from id 1645/16
*Feb 24 20:36:49.968: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access1, changed state to down
*Feb 24 20:36:49.968: RADIUS/ENCODE(00000024):Orig. component type = VPN IPSEC
*Feb 24 20:36:49.968: RADIUS:  AAA Unsupported Attr: interface         [209] 7
*Feb 24 20:36:49.968: RADIUS:   38 2E 39 2E 32             [ 8.9.2]
*Feb 24 20:36:49.972: RADIUS(00000024): Config NAS IP: 0.0.0.0
*Feb 24 20:36:49.972: RADIUS/ENCODE(00000024): acct_session_id: 24
*Feb 24 20:36:49.972: RADIUS(00000024): sending
*Feb 24 20:36:49.972: RADIUS/ENCODE: Best Local IP-Address 10.1.1.1 for Radius-
Server 10.1.1.150
```

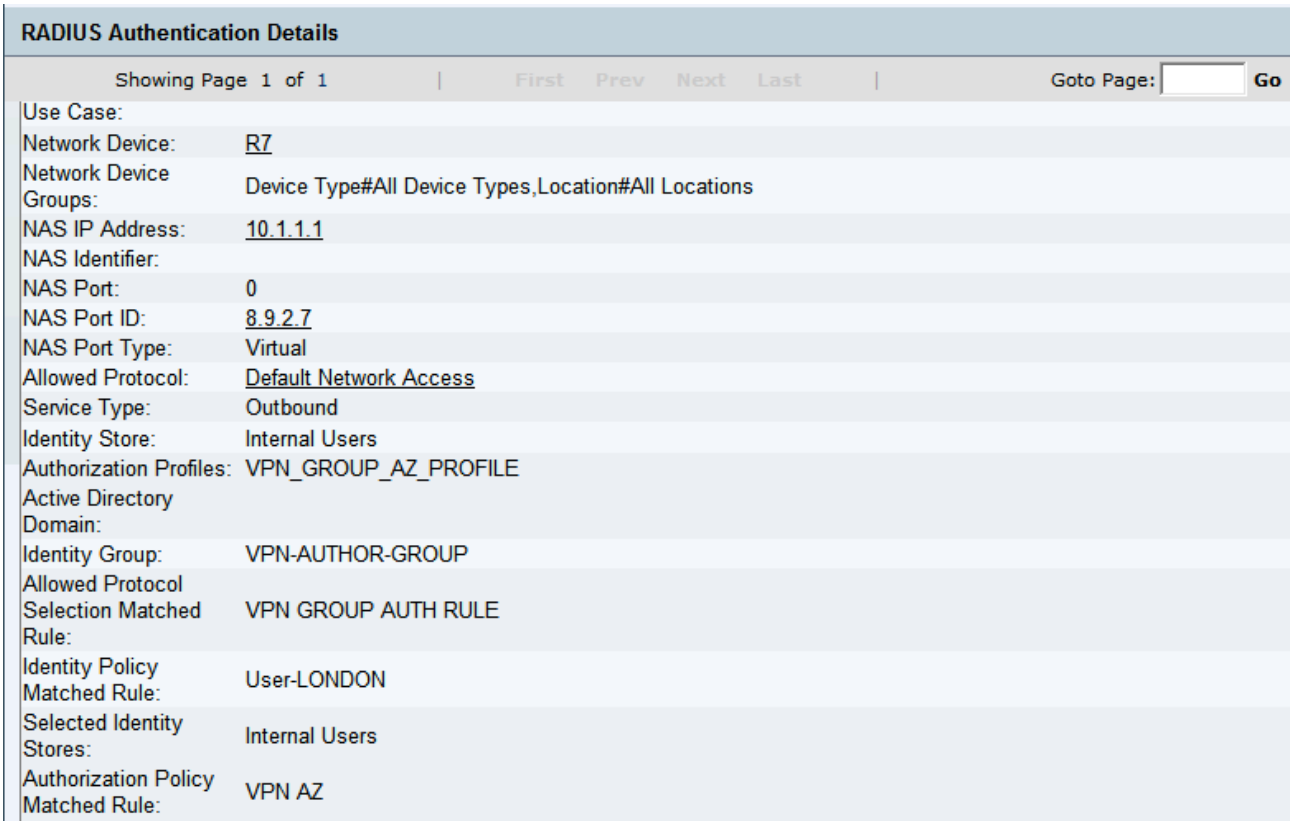
```
*Feb 24 20:36:49.976: RADIUS(00000024): Send Access-Request to 10.1.1.150:1645 id
1645/17, len 85
*Feb 24 20:36:49.976: RADIUS:  authenticator 85 30 74 FB 19 02 B9 E1 - 97 70 4F 7D
A3 FB A3 5C
*Feb 24 20:36:49.976: RADIUS:  User-Name           [1]   8   "LONDON"
*Feb 24 20:36:49.976: RADIUS:  User-Password       [2]   18  *
*Feb 24 20:36:49.976: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Feb 24 20:36:49.976: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Feb 24 20:36:49.976: RADIUS:  NAS-Port            [5]   6   1
*Feb 24 20:36:49.976: RADIUS:  NAS-Port-Id         [87]  9   "8.9.2.7"
*Feb 24 20:36:49.976: RADIUS:  Service-Type        [6]   6   Outbound
[5]
*Feb 24 20:36:49.976: RADIUS:  NAS-IP-Address      [4]   6   10.1.1.1
*Feb 24 20:36:49.976: RADIUS(00000024): Started 5 sec timeout
*Feb 24 20:36:49.992: RADIUS: Received from id 1645/17 10.1.1.150:1645, Access-
Accept, len 315
*Feb 24 20:36:49.992: RADIUS:  authenticator DA 3D 36 4C 3C 7C C6 6C - 35 4C 20 D2
D9 11 8D 5E
*Feb 24 20:36:49.996: RADIUS:  User-Name           [1]   8   "LONDON"
*Feb 24 20:36:49.996: RADIUS:  State               [24]  40
*Feb 24 20:36:49.996: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
[ReauthSession:0a]
*Feb 24 20:36:49.996: RADIUS:   63 38 30 36 66 34 30 30 30 30 30 46 33 45 35 31
[c806f400000F3E51]
*Feb 24 20:36:49.996: RADIUS:   32 41 37 38 46 41            [ 2A78FA]
*Feb 24 20:36:49.996: RADIUS:  Class               [25]  56
*Feb 24 20:36:49.996: RADIUS:   43 41 43 53 3A 30 61 63 38 30 36 66 34 30 30 30
[CACS:0ac806f4000]
*Feb 24 20:36:49.996: RADIUS:   30 30 46 33 45 35 31 32 41 37 38 46 41 3A 70 6F
[00F3E512A78FA:po]
*Feb 24 20:36:49.996: RADIUS:   64 31 32 34 69 73 65 2F 31 34 39 33 39 38 32 36
[d124ise/14939826]
*Feb 24 20:36:49.996: RADIUS:   34 2F 34 31 31 39            [ 4/4119]
*Feb 24 20:36:49.996: RADIUS:  Termination-Action  [29]  6   1
*Feb 24 20:36:49.996: RADIUS:  Tunnel-Type         [64]  6   01:ESP
[9]
*Feb 24 20:36:49.996: RADIUS:  Tunnel-Password     [69]  21  01:*
*Feb 24 20:36:49.996: RADIUS:  Vendor, Cisco       [26]  30
*Feb 24 20:36:49.996: RADIUS:   Cisco AVpair       [1]   24  "ipsec:key-
exchange=ike"
*Feb 24 20:36:49.996: RADIUS:  Vendor, Cisco       [26]  30
*Feb 24 20:36:49.996: RADIUS:   Cisco AVpair       [1]   24  "ipsec:addr-
pool=EZPOOL"
*Feb 24 20:36:49.996: RADIUS:  Vendor, Cisco       [26]  23
*Feb 24 20:36:49.996: RADIUS:   Cisco AVpair       [1]   17  "ipsec:inacl=170"
*Feb 24 20:36:49.996: RADIUS:  Vendor, Cisco       [26]  41
*Feb 24 20:36:49.996: RADIUS:   Cisco AVpair       [1]   35  "ipsec:default-
domain=ipexpert.com"
*Feb 24 20:36:49.996: RADIUS:  Vendor, Cisco       [26]  34
*Feb 24 20:36:49.996: RADIUS:   Cisco AVpair       [1]   28  "ipsec:user-save-
password=1"
*Feb 24 20:36:50.000: RADIUS(00000024): Received from id 1645/17
*Feb 24 20:36:59.956: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access1, changed state to up
```

```
R7#sh cry route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
172.16.70.3/255.255.255.255 [15/0] via Virtual-Access1 tag 0 VTI

R7#sh cry isa peer detail
Peer: 8.9.2.8 Port: 4500 Local: 8.9.2.7
 Phase1 id: LONDON
  flags:
 NAS Port: 1 (Normal)
Configuration:
Configured Address: 172.16.70.3, State: in use,   Attributes: RESPOND
  XAUTH: user ipexpert      FLAGS: (Need xauth on next phase 1) (xauth done)


Group Policy :
  group name      = LONDON
  pre-shared key = SkyFall
  address pool    = EZPOOL
  default domain = ipexpert.com
  configuration URL [version] =  [0]
  acl             = 170
  dns primary     = 0.0.0.0
  dns secondary   = 0.0.0.0
  wins primary    = 0.0.0.0
  wins secondary = 0.0.0.0
  save password   = off
  smartcard_removal_disconnect  = disable
  pfs             = off
  banner =
  local_lan       = off
  split-dns     =
  backup-servers =


User Config :
  local_lan       = off
  save password   = on


R8#ping 10.1.1.133 so l8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.133, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/16 ms

R8#sh cry sess de
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
```

```
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access1
Uptime: 00:09:02
Session status: UP-ACTIVE
Peer: 8.9.2.7 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.2.7
      Desc: (none)
  IKEv1 SA: local 192.168.8.8/4500 remote 8.9.2.7/4500 Active
          Capabilities:CXN connid:1012 lifetime:23:50:09
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 4400430/3047
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4400431/3047

R8#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.8.8     YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/0/0                unassigned      YES unset  administratively down down
Loopback8                  8.8.8.8         YES manual up                    up
Loopback10000              172.16.70.3     YES TFTP   up                    up
NVI0                       192.168.8.8     YES unset  up                    up
Virtual-Access1            172.16.70.3     YES unset  up                    up
Virtual-Template1          192.168.8.8     YES unset  up                    down
```







Task 7: IPSec Remote Access ASA

- Configure ASA3 to accept remote VPN connections
- Use AES encryption and SHA-1 hashing for both phases
- Group Policy should be stored locally

- Use the following parameters for Group configuration:
    - VPN group name “MIAMI”
    - Key should be set to “MiamiVice”
    - IP address pool should be 172.16.30.30/24
    - DNS Server should be 192.168.8.30
    - VPN connection should be terminated after 10 minutes of inactivity
    - Users should only access VLAN 8 through the tunnel
- Make sure user “cisco” (password “cisco”) can only access the “MIAMI” group
- Configure Cisco VPN Client to test this setup (use PC#1)

Detailed Solution

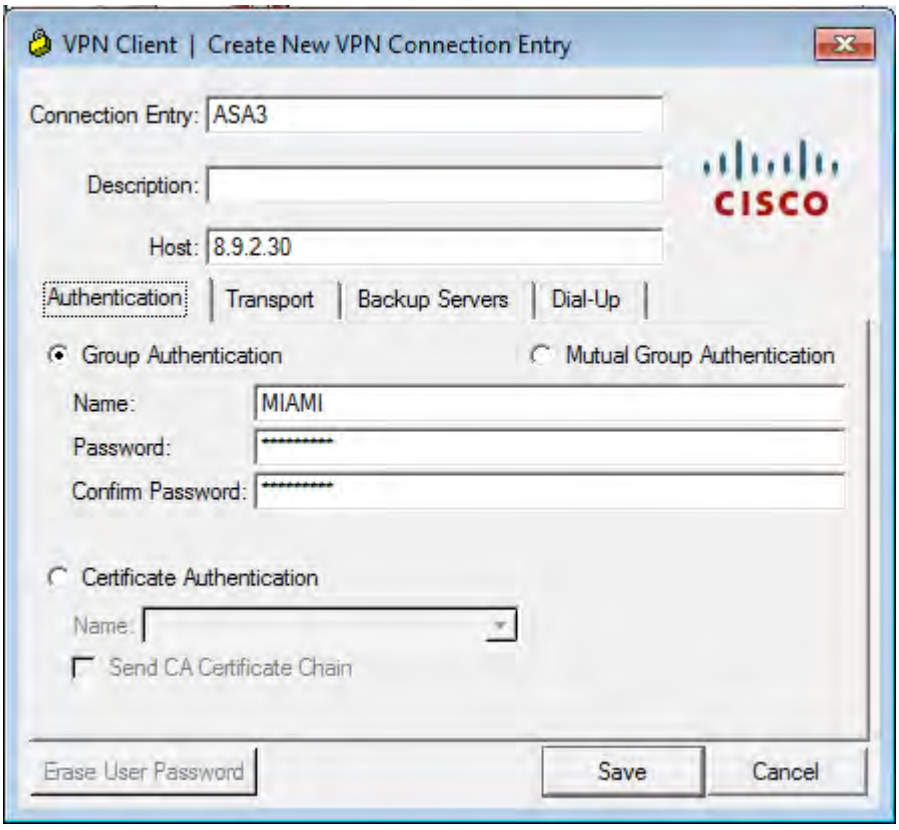
ASA3

```
object network R8
 host 192.168.8.8
object network VPNPOOL
 subnet 172.16.30.0 255.255.255.0

nat (inside,outside) source static R8 R8 dest static VPNPOOL VPNPOOL

username cisco password cisco
username cisco attributes
 group-lock value MIAMI

ip local pool EZPOOL 172.16.30.1-172.16.30.254

crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400

crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac

access-list SPLIT standard permit 192.168.8.0 255.255.255.0

group-policy EZGROUP internal
group-policy EZGROUP attributes
 dns-server value 192.168.8.30
 vpn-idle-timeout 10
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT
 address-pools value EZPOOL

tunnel-group MIAMI type remote-access
```

```
tunnel-group MIAMI general-attributes
 default-group-policy EZGROUP
 authentication-server-group LOCAL
tunnel-group MIAMI ipsec-attributes
 ikev1 pre-shared-key MiamiVice

crypto dynamic-map DYNMAP 10 set transform-set SET1
crypto map MAP1 10 ipsec-isakmp dynamic DYNMAP
crypto map MAP1 interface outside

crypto isakmp enable outside

sysopt connection permit-vpn

vpn-addr-assign local
```

Test PC

Create a Profile for ASA3 in the VPN Client:



Groups and users are core concepts in managing the security of virtual private networks (VPNs) and in configuring the security appliance. They specify attributes that determine user access to and use of the VPN. A group is a collection of users treated as a single entity. Users get their attributes from group policy. Connection profiles (tunnel groups) identify the group policy for a specific connection and the

connection settings. If you do not assign a particular group policy to a user, the default group policy for the connection applies.

Tunnel group consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. When digital certificates are used, ASA matches a tunnel group based on OU attribute of certificate's DN by default. If you want to match it based on other attributes, you can use Certificate ACL rules and then associate each rule with the desired tunnel group. If Pre-Shared-Key is used then the Group Name passed by the client will be used to find a matching Tunnel Group.

Connection profiles and group policies simplify system management. To streamline the configuration task, the ASA provides a default LAN-to-LAN connection profile, a default remote access connection profile, a default connection profile for SSL/IKEv2 VPN, and a default group policy (DfltGrpPolicy). The default connection profiles and group policy provide settings that are likely to be common for many users. As you add users, you can specify that they "inherit" parameters from a group policy. Thus you can quickly configure VPN access for large numbers of users.

User Attributes are applied to the users according to the following hierarchy :

1. Dynamic Access Policy (DAP) record
2. Username
3. Group Policy (IETF-Class-25 attribute)
4. Group Policy for the connection profile
5. Default group policy

If an attribute is defined by more than one element, the one specified by the higher-priority element is applied. For non-overlapping attributes, once again, they are inherited (meaning that most of them will use value specified by the Default Group Policy).

VPN Group Lock feature ensures that a particular user can only connect to a single VPN Group; the one it was configured for.

NAT Exemption configuration is required so R8 can be also accessible via the tunnel. The tasks states that VLAN8 traffic should be protected (all IPs).

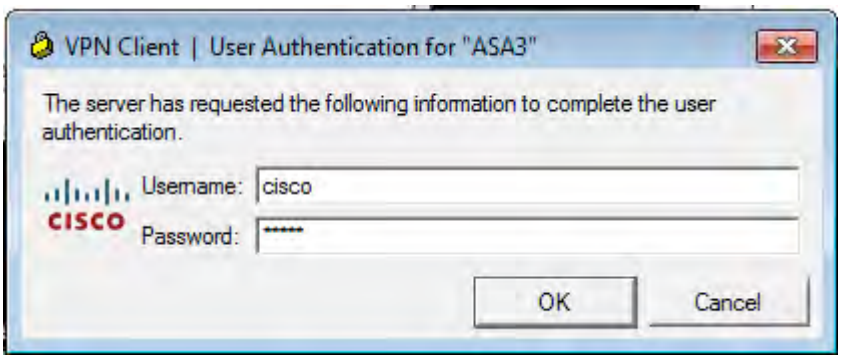
IPv6 Considerations

Address pool must be configured using "`ipv6 local pool`" command and then applied under the tunnel-group or group-policy with "`ipv6-address-pool`".

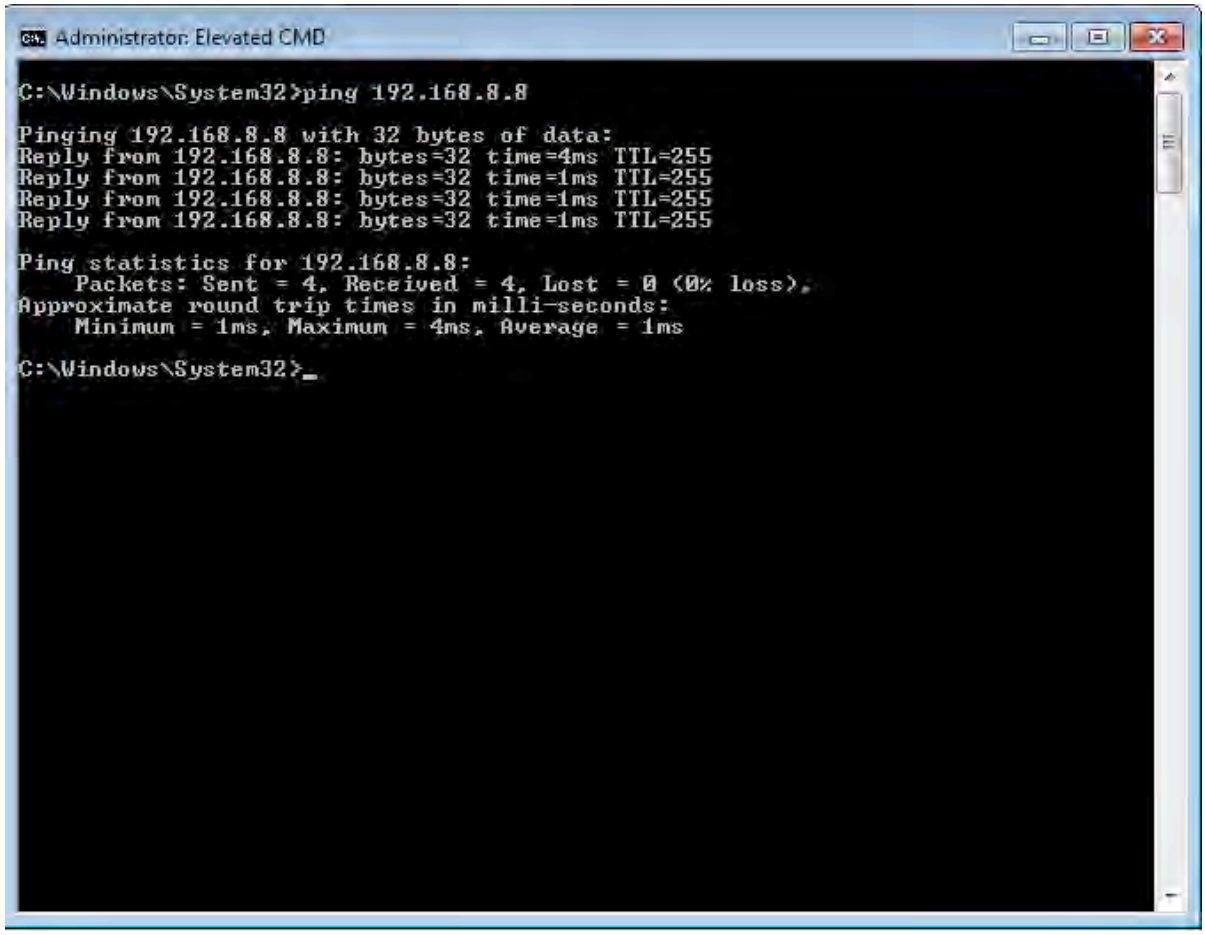
Regular Cisco VPN Client does not support IPv6. Use AnyConnect instead.

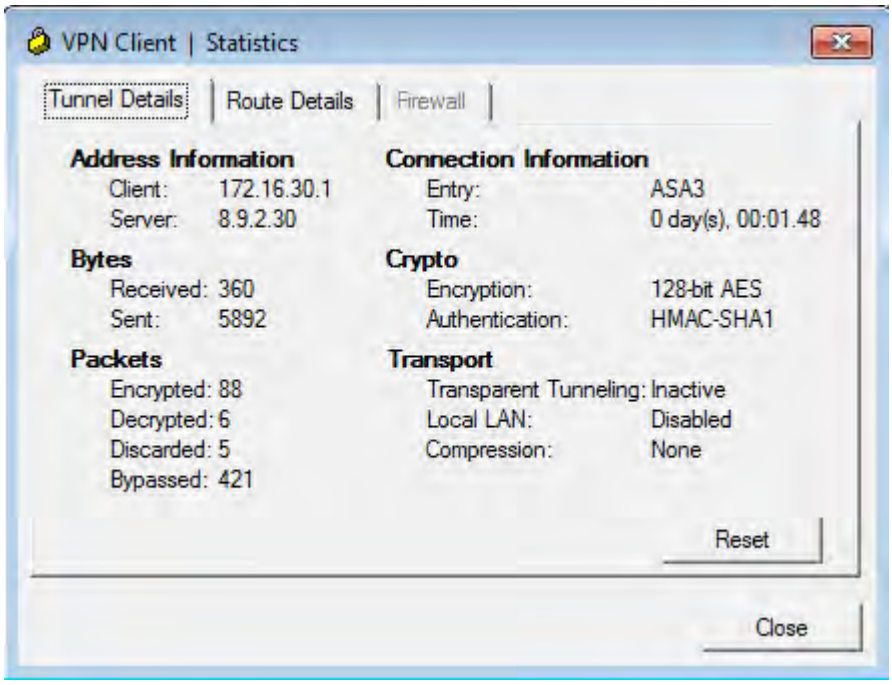
Verification

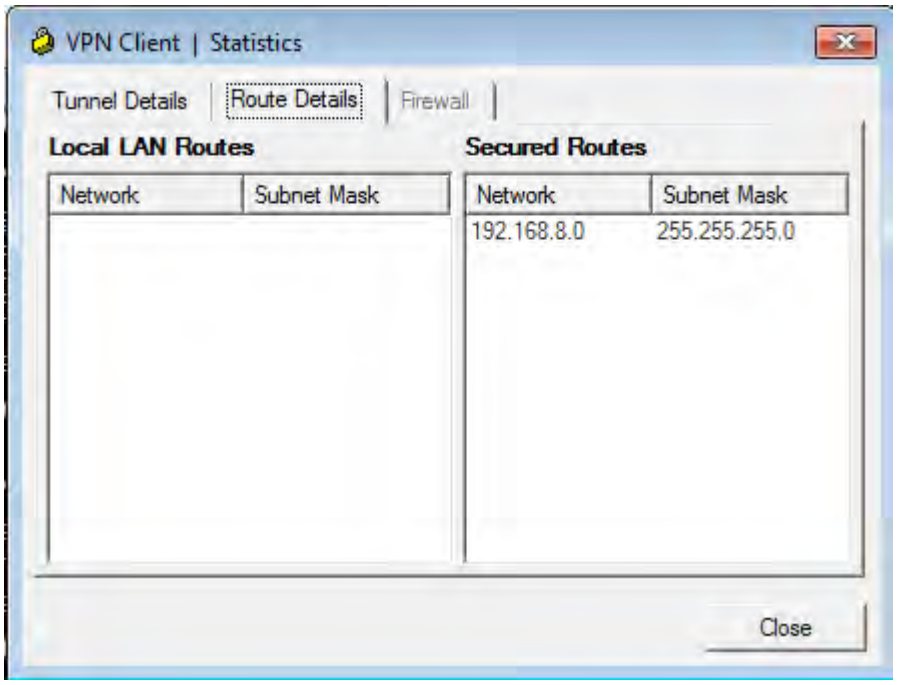
Connect from the Test PC using Cisco VPN Client. You should be prompted for authentication:

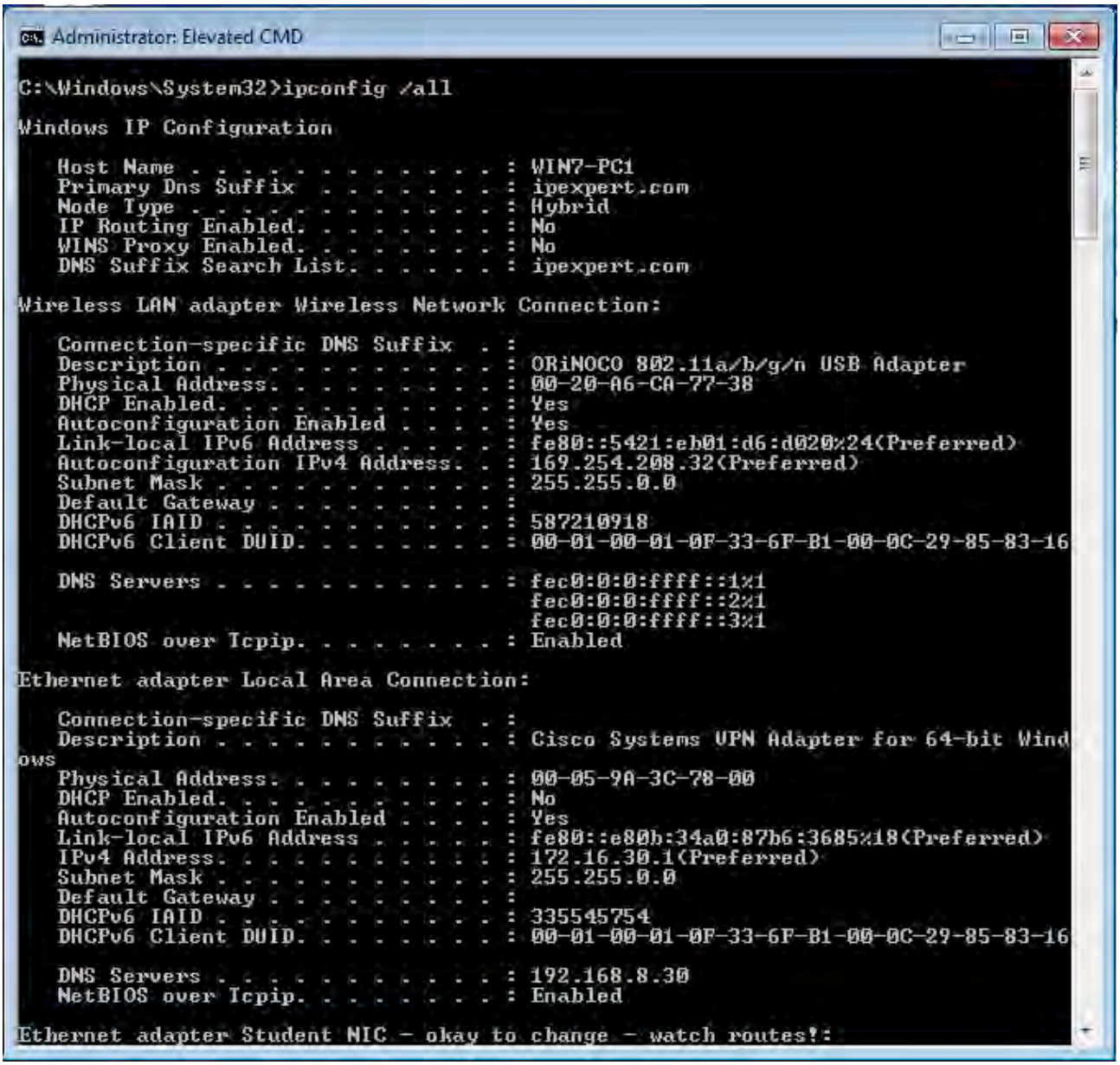


Start testing:










```
ASA3(config)# sh vpn-sessiondb detail ra-ikev1-ipsec


Session Type: IKEv1 IPsec Detailed

Username     : cisco                  Index        : 5
Assigned IP  : 172.16.30.1            Public IP    : 8.9.2.200
Protocol     : IKEv1 IPsec
License      : Other VPN
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 240                    Bytes Rx     : 4101
Pkts Tx      : 4                      Pkts Rx      : 60
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
```

```
Group Policy : EZGROUP                 Tunnel Group : MIAMI
Login Time   : 14:53:50 UTC Sun Feb 24 2013
Duration     : 0h:00m:58s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN         : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 5.1
  UDP Src Port : 64893                 UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeys
  Encryption   : AES128                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86344 Seconds
  D/H Group    : 2
  Filter Name  :
  Client OS    : WinNT                 Client OS Ver: 5.0.07.0290

IPsec:
  Tunnel ID    : 5.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 172.16.30.1/255.255.255.255/0/0
  Encryption   : AES128                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28742 Seconds
  Idle Time Out: 10 Minutes            Idle TO Left : 9 Minutes
  Bytes Tx     : 240                   Bytes Rx     : 4166
  Pkts Tx      : 4                     Pkts Rx      : 61

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 58 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

Task 8: IPSec Remote Access ASA with RADIUS

- Modify configuration from the previous task
- Authentication & Group Policy information should be now stored on ISE
- Use “outofcontrol” as RADIUS shared secret
- User “cisco” should be now always assigned an IP address 172.16.30.100
- Use password of “cisco1” for this user
- Other settings/requirements from the previous task (except VPN Idle Timeout) still apply

Detailed Solution

R7

```
int f0/0
 ip nat enable
int f0/1
 ip nat enable

ip nat source static 10.1.1.150 8.9.2.150
```

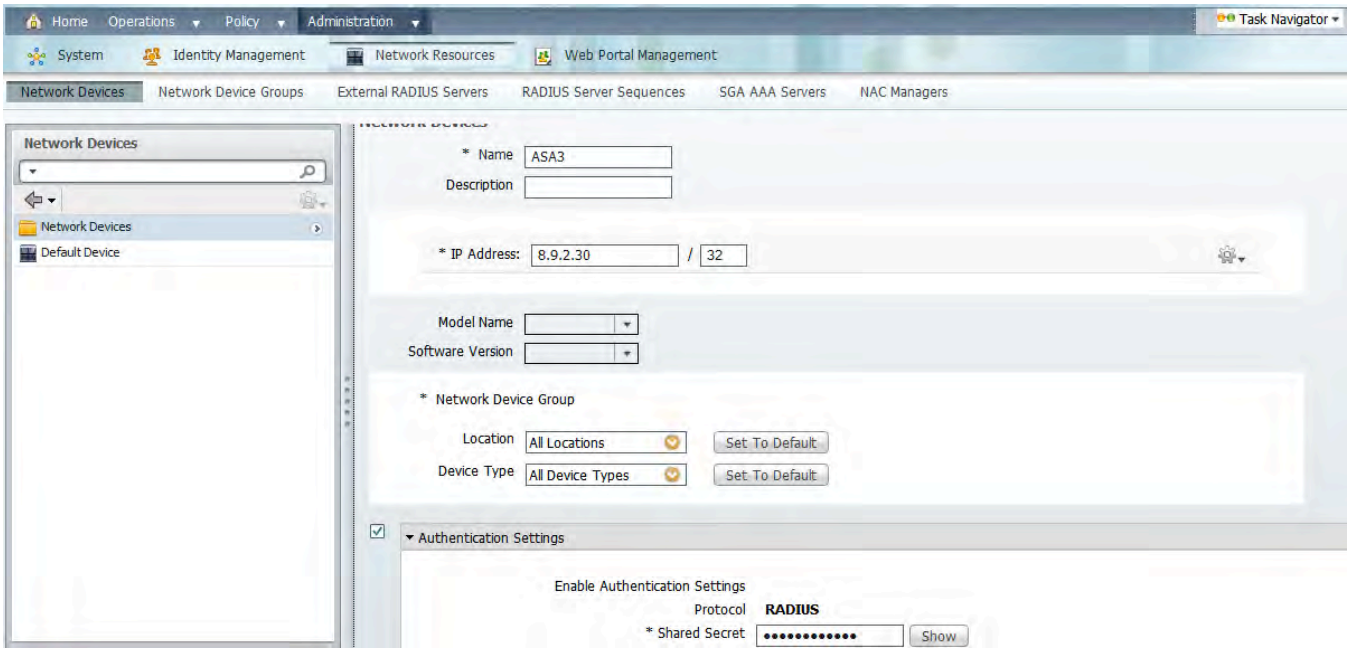
ASA3

```
no group-policy EZGROUP

group-policy EZGROUP external server-group ISE password EZGROUP

aaa-server ISE protocol radius
aaa-server ISE (outside) host 8.9.2.150
 key outofcontrol

tunnel-group MIAMI general-attributes
 default-group-policy EZGROUP
 authentication-server-group ISE
```

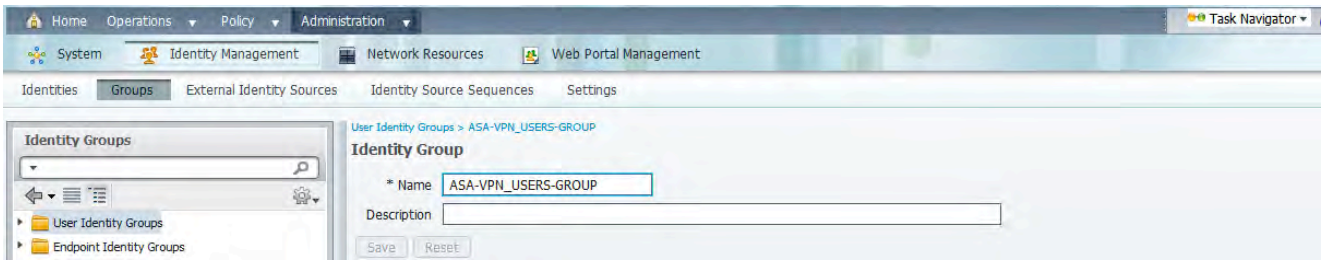
ISE

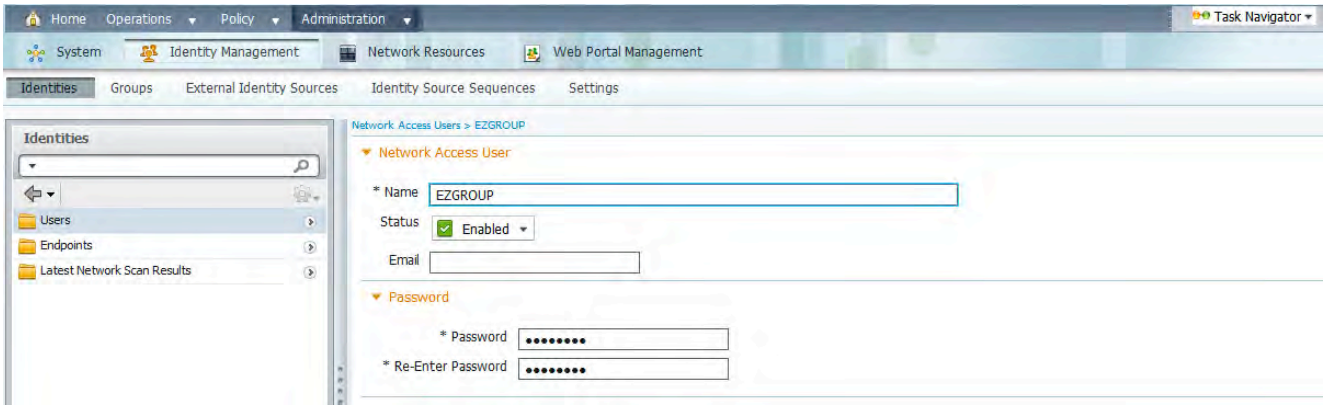
```
ip route 8.9.2.0 255.255.255.0 gateway 10.1.1.1
```

As usually start with adding NAS:

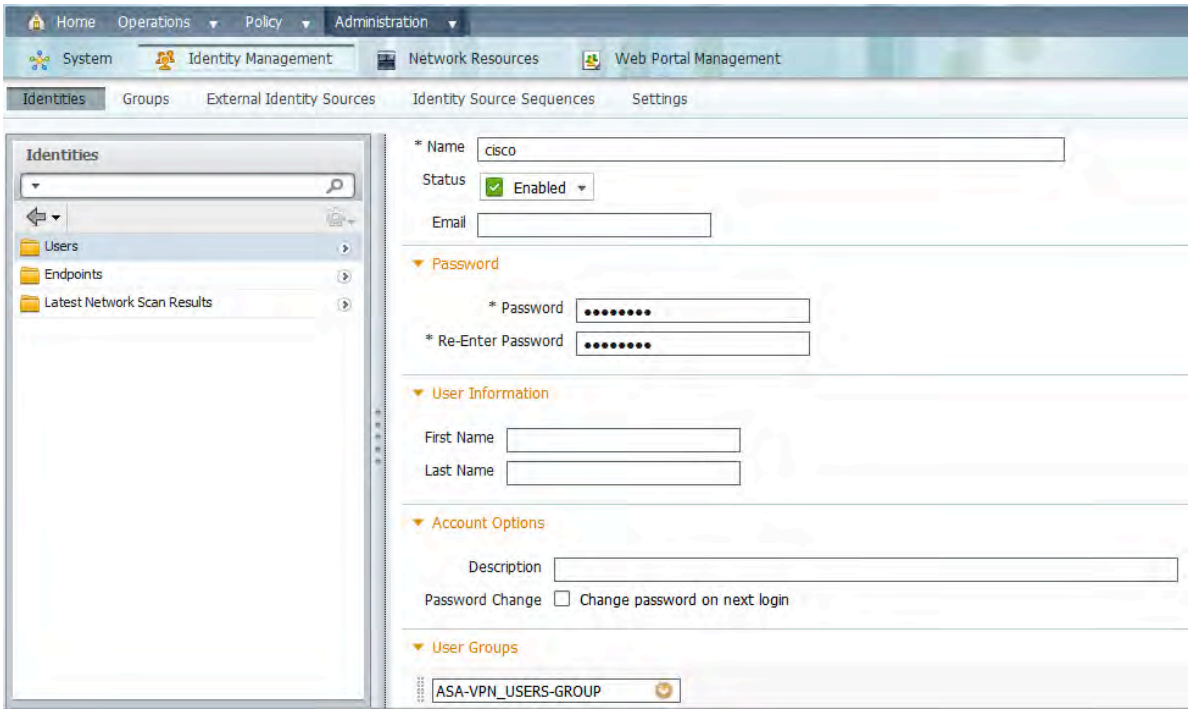


Then we will create Group for VPN Users and the users themselves:

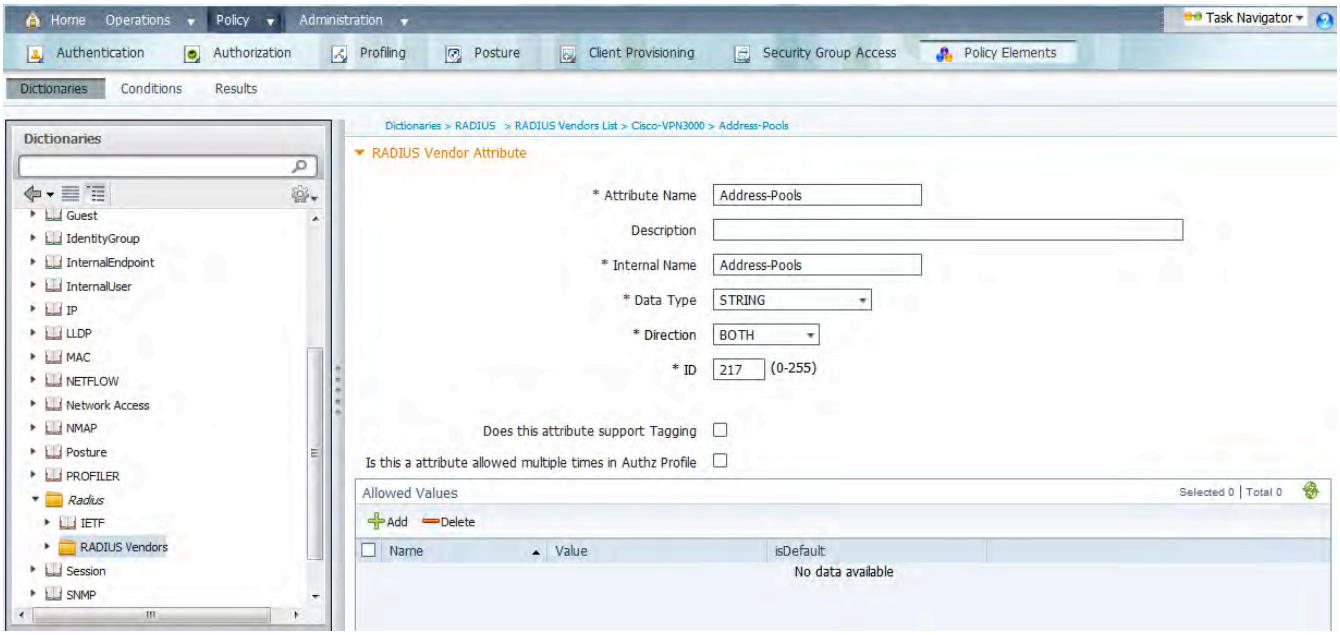


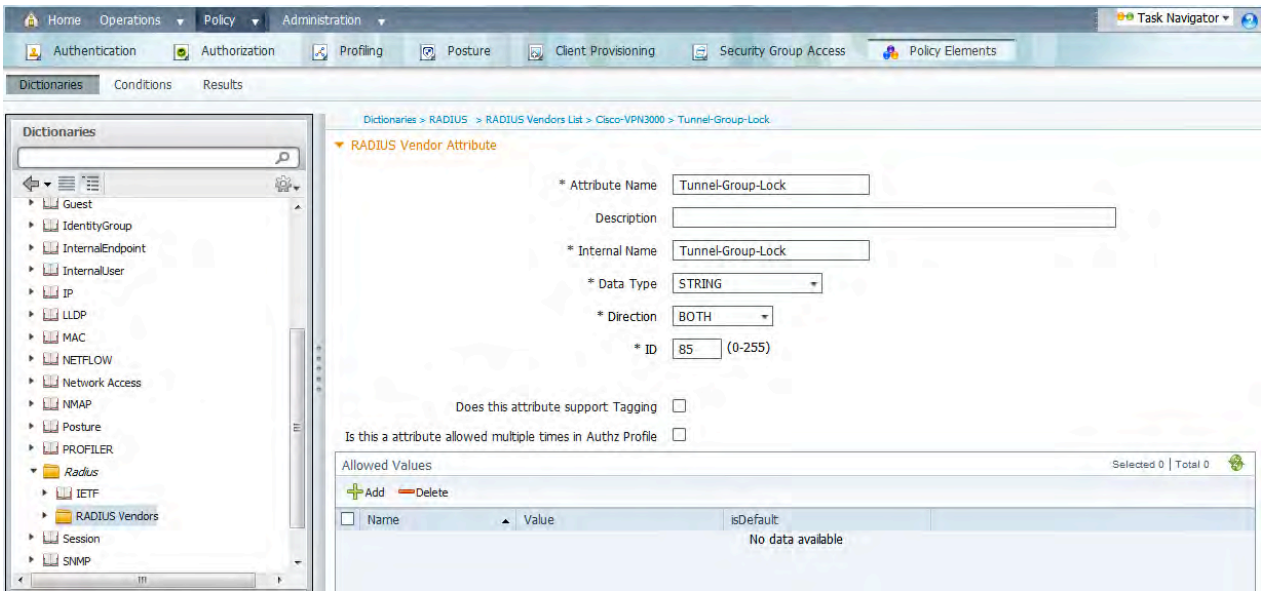


Note user “cisco” is made part of the “ASA-VPN_USERS-GROUP”:

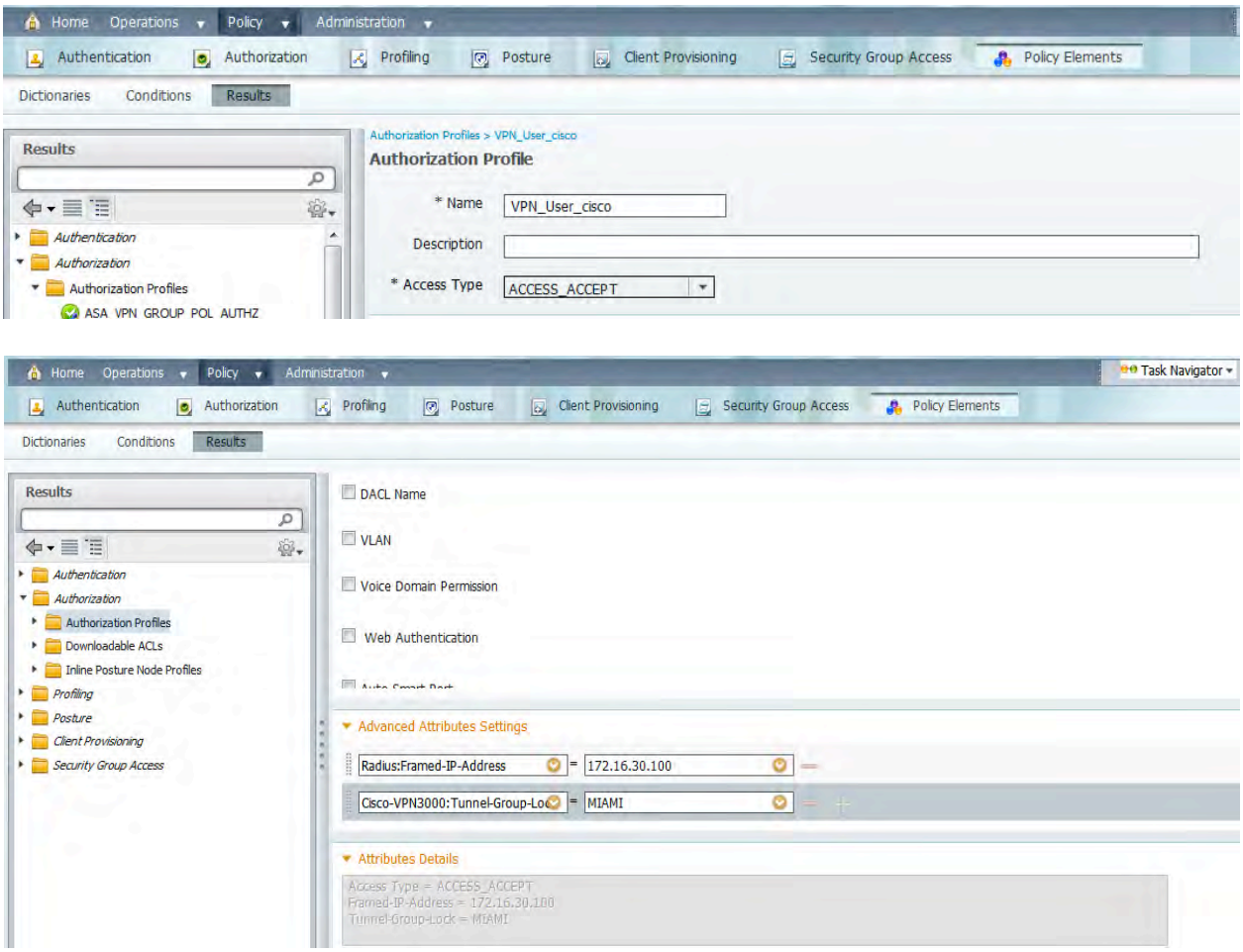


Then we need to define two new attributes in the VPN 3000 Dictionary. This is to support the Group Lock feature and to assign an address pool:

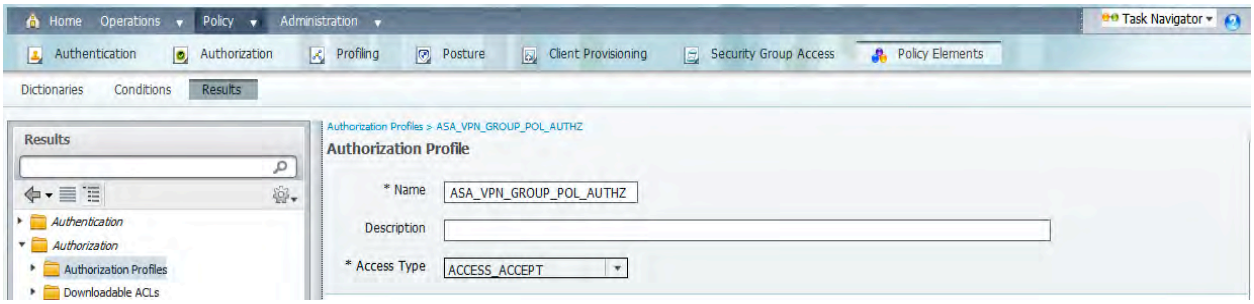


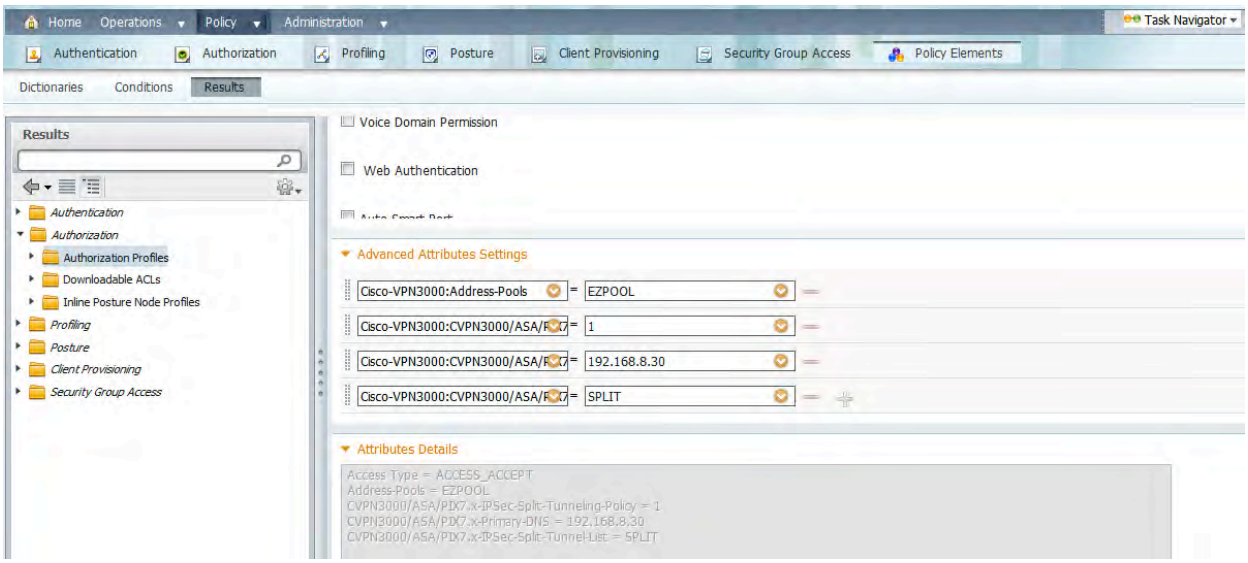


Once we have all necessary attributes it is time to create Authorization Profiles. Note that to assign a static IP address a standard IETF attribute is used – “Framed IP Address”:

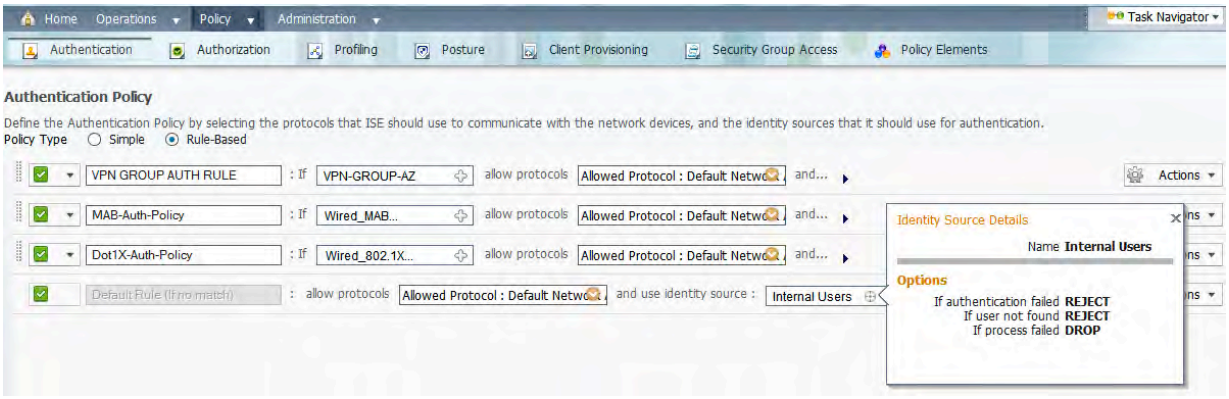


And the Group Policy Profile :

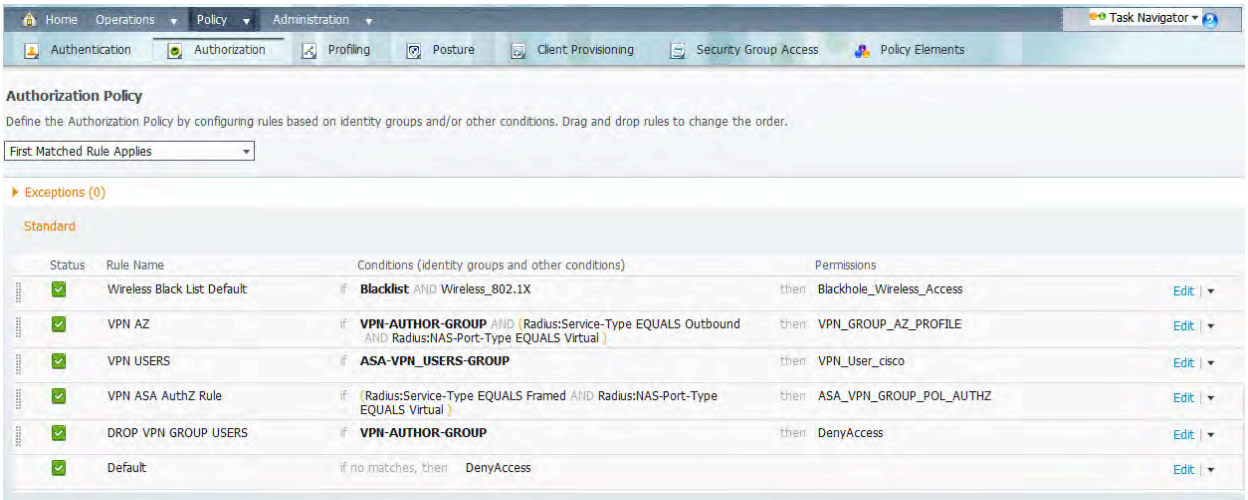




Moving on to Authentication Policy. We are using the Default Rule, nothing special here:



Finally Authorization Rules – the Group Policy Rule was added via “Create New Condition (Advanced Option)”:



To authenticate VPN users via RADIUS we have to first configure basic AAA support. Authorization in RADIUS happens along with authentication, the attributes will be downloaded from the profile (same as on IOS). One thing that is different from IOS is that now what's being sent to the ASA is the name of the Group Policy (specified in the `group-policy … external` on the ASA) and not the VPN Group name. And the password is no longer "cisco" – we can configure whatever you want and this way we don't need to modify the Authentication Policy. In our example the Default Rule is used.

Since we will be using some of the attributes that are not predefined in Cisco's VPN 3000 Dictionary, we need to create them first (this Dictionary will be most useful for any type of RADIUS authorization on the ASA). The full list of RADIUS Authorization attributes for ASA (and their types/numbers) can be found in ASA's documentation under "Reference" -> "Configuring an External Server for Security Appliance User Authorization" -> "ASA RADIUS Authorization Attributes".

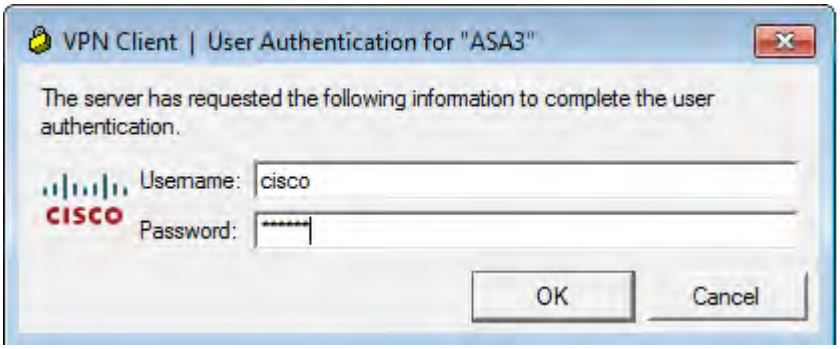
Authorization Policy is bit tricky. First rule is for VPN Users (Group) and it must be above the rule for Group Policy. This is because both authorizations use the same attributes in the Access Request packet (Service Type "Framed" + NAS Port Type "Virtual"). This way second rule will be only matched by the Group Policy requests.

IPv6 Considerations

For an IPv6 Pool you would create another attribute in the VPN 3000 Dictionary - IPv6-Address-Pools (Type 218).

Verification

Connect from the Test PC (VPN Client) :



Testing the Group Lock feature (other group than "MIAMI" specified in the AuthZ profile) :

```
Feb 24 17:50:54 [IKEv1]Group = MIAMI, Username = cisco, IP = 8.9.2.200, Tunnel
Rejected: User (cisco) not member of group (MIAMI), group-lock check failed.
```

```
ASA3#deb radius
```

And with the correct group:

```
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=8.9.2.200

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 137).....
01 24 00 89 3f 0c 55 6a 5b f8 d1 36 37 a4 0d c2    |  .$..?.Uj[..67...
d3 10 09 0e 01 07 63 69 73 63 6f 02 12 51 7f 4a    |  ......cisco..QJ
eb e0 11 45 12 e6 ad e4 a1 46 81 9e fb 05 06 47    |  ...E.....F.....G
e0 40 00 06 06 00 00 00 02 07 06 00 00 00 01 1e    |  .@..............
0a 38 2e 39 2e 32 2e 33 30 1f 0b 38 2e 39 2e 32    |  .8.9.2.30..8.9.2
2e 32 30 30 3d 06 00 00 00 05 42 0b 38 2e 39 2e    |  .200=.....B.8.9.
32 2e 32 30 30 04 06 08 09 02 1e 1a 1e 00 00 00    |  2.200...........
09 01 18 69 70 3a 73 6f 75 72 63 65 2d 69 70 3d    |  ...ip:source-ip=
38 2e 39 2e 32 2e 32 30 30                         |  8.9.2.200

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 36 (0x24)
Radius: Length = 137 (0x0089)
Radius: Vector: 3F0C556A5BF8D13637A40DC2D310090E
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
63 69 73 63 6f                                     |  cisco
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
51 7f 4a eb e0 11 45 12 e6 ad e4 a1 46 81 9e fb    |  QJ...E.....F...
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x47E04000
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 10 (0x0A)
Radius: Value (String) =
38 2e 39 2e 32 2e 33 30                            |  8.9.2.30
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 11 (0x0B)
Radius: Value (String) =
```

```
38 2e 39 2e 32 2e 32 30 30                          |  8.9.2.200
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 11 (0x0B)
Radius: Value (String) =
38 2e 39 2e 32 2e 32 30 30                          |  8.9.2.200
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 8.9.2.30 (0x0809021E)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 38 2e 39    |  ip:source-ip=8.9
2e 32 2e 32 30 30                                   |  .2.200
send pkt 8.9.2.150/1645
rip 0x00007fff2e160820 state 7 id 36
rad_vrfy() : response message verified
rip 0x00007fff2e160820
 : chall_state ''
 : state 0x7
 : reqauth:
     3f 0c 55 6a 5b f8 d1 36 37 a4 0d c2 d3 10 09 0e
 : info 0x00007fff2e160960
     session_id 0x2d
     request_id 0x24
     user 'cisco'
     response '***'
     app 0
     reason 0
     skey 'outofcontrol'
     sip 8.9.2.150
     type 1

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 148).....
02 24 00 94 84 8a f9 53 aa 01 c3 b8 91 4c 8a 0c    |  .$.....S.....L..
f6 2d a7 60 01 07 63 69 73 63 6f 08 06 ac 10 1e    |  .-.`..cisco.....
64 18 28 52 65 61 75 74 68 53 65 73 73 69 6f 6e    |  d.(ReauthSession
3a 30 61 63 38 30 36 66 34 30 30 30 30 31 30 32    |  :0ac806f40000102
30 35 31 32 41 42 39 44 46 19 38 43 41 43 53 3a    |  0512AB9DF.8CACS:
30 61 63 38 30 36 66 34 30 30 30 30 31 30 32 30    |  0ac806f400001020
35 31 32 41 42 39 44 46 3a 70 6f 64 31 32 34 69    |  512AB9DF:pod124i
```

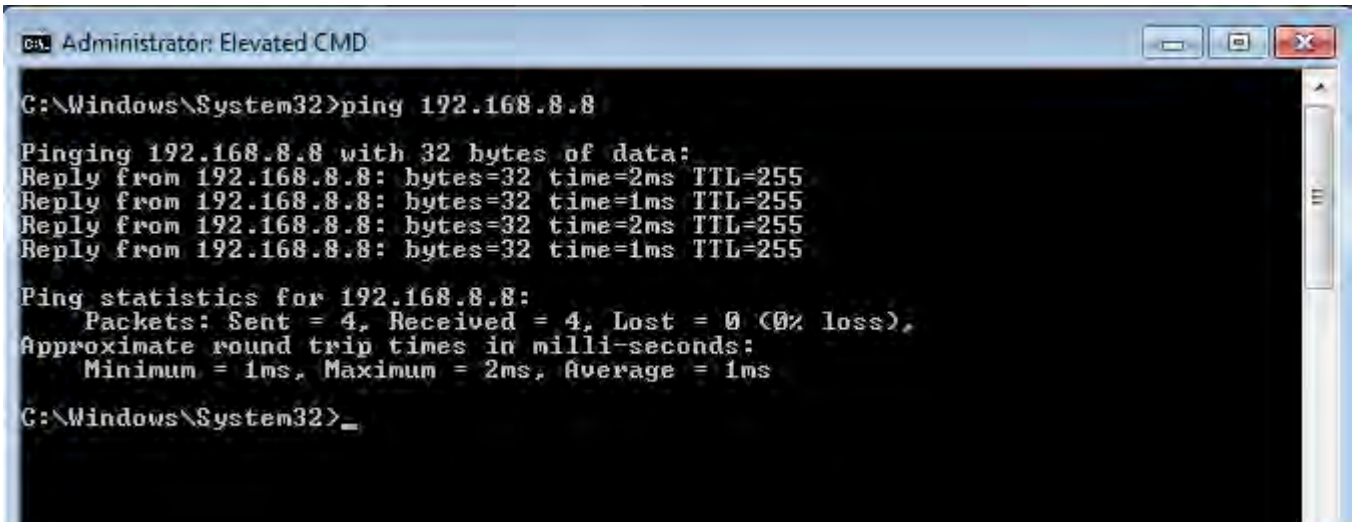
```
73 65 2f 31 34 39 33 39 38 32 36 34 2f 34 34 34    |  se/149398264/444
35 1d 06 00 00 00 01 1a 0d 00 00 0c 04 55 07 4d    |  5.............U.M
49 41 4d 49                                        |  IAMI

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 36 (0x24)
Radius: Length = 148 (0x0094)
Radius: Vector: 848AF953AA01C3B8914C8A0CF62DA760
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
63 69 73 63 6f                                     |  cisco
Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 172.16.30.100 (0xAC101E64)
Radius: Type = 24 (0x18) State
Radius: Length = 40 (0x28)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
63 38 30 36 66 34 30 30 30 30 31 30 32 30 35 31    |  c806f40000102051
32 41 42 39 44 46                                  |  2AB9DF
Radius: Type = 25 (0x19) Class
Radius: Length = 56 (0x38)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 38 30 36 66 34 30 30 30    |  CACS:0ac806f4000
30 31 30 32 30 35 31 32 41 42 39 44 46 3a 70 6f    |  01020512AB9DF:po
64 31 32 34 69 73 65 2f 31 34 39 33 39 38 32 36    |  d124ise/14939826
34 2f 34 34 34 35                                  |  4/4445
Radius: Type = 29 (0x1D) Termination-Action
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 13 (0x0D)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 85 (0x55) The tunnel group that tunnel must be associated with
Radius: Length = 7 (0x07)
Radius: Value (String) =
4d 49 41 4d 49                                     |  MIAMI
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
radius mkreq: 0x2e
alloc_rip 0x00007fff2e1613a8
    new request 0x2e --> 37 (0x00007fff2e1613a8)
got user 'EZGROUP'
got password
add_req 0x00007fff2e1613a8 session 0x2e id 37
RADIUS_DELETE
remove_req 0x00007fff2e160820 session 0x2d id 36
```

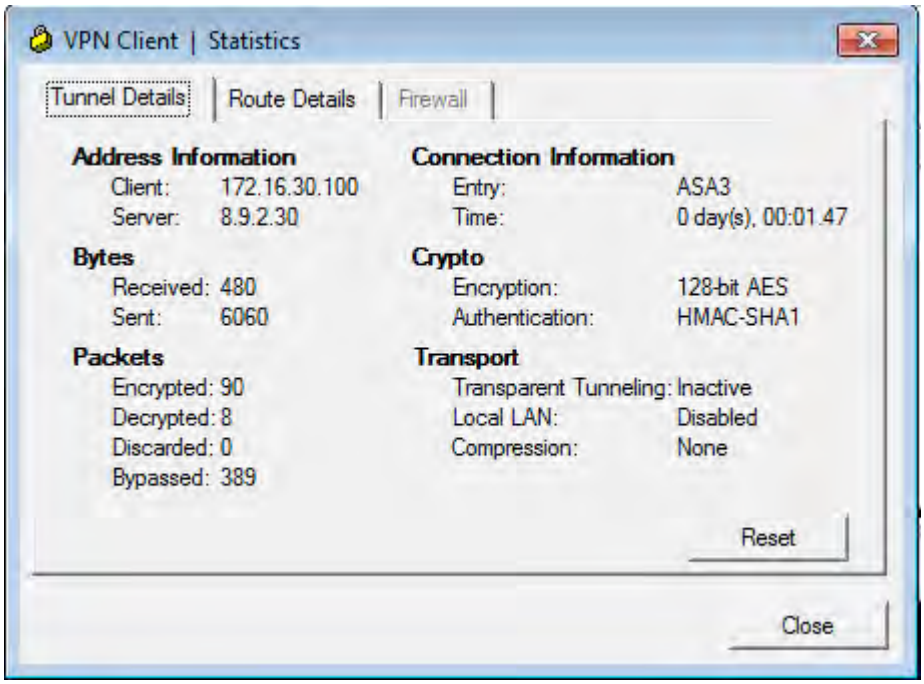
```
free_rip 0x00007fff2e160820
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=8.9.2.200

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 139).....
01 25 00 8b 2f 3c c5 1a 4b 28 41 e6 27 d4 7d 72    |  .%../<..K(A.'.}r
c3 40 79 be 01 09 45 5a 47 52 4f 55 50 02 12 4a    |  .@y...EZGROUP..J
98 2f 6a a3 78 d5 33 b5 22 8d 6c ec a9 63 9d 05    |  ./j.x.3.".l..c..
06 00 00 00 00 06 06 00 00 00 02 07 06 00 00 00    |  ................
01 1e 0a 38 2e 39 2e 32 2e 33 30 1f 0b 38 2e 39    |  ...8.9.2.30..8.9
2e 32 2e 32 30 30 3d 06 00 00 00 05 42 0b 38 2e    |  .2.200=.....B.8.
39 2e 32 2e 32 30 30 04 06 08 09 02 1e 1a 1e 00    |  9.2.200.........
00 00 09 01 18 69 70 3a 73 6f 75 72 63 65 2d 69    |  .....ip:source-i
70 3d 38 2e 39 2e 32 2e 32 30 30                   |  p=8.9.2.200

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 37 (0x25)
Radius: Length = 139 (0x008B)
Radius: Vector: 2F3CC51A4B2841E627D47D72C34079BE
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
45 5a 47 52 4f 55 50                               |  EZGROUP
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
4a 98 2f 6a a3 78 d5 33 b5 22 8d 6c ec a9 63 9d    |  J./j.x.3.".l..c.
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 10 (0x0A)
Radius: Value (String) =
38 2e 39 2e 32 2e 33 30                            |  8.9.2.30
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 11 (0x0B)
Radius: Value (String) =
38 2e 39 2e 32 2e 32 30 30                         |  8.9.2.200
```

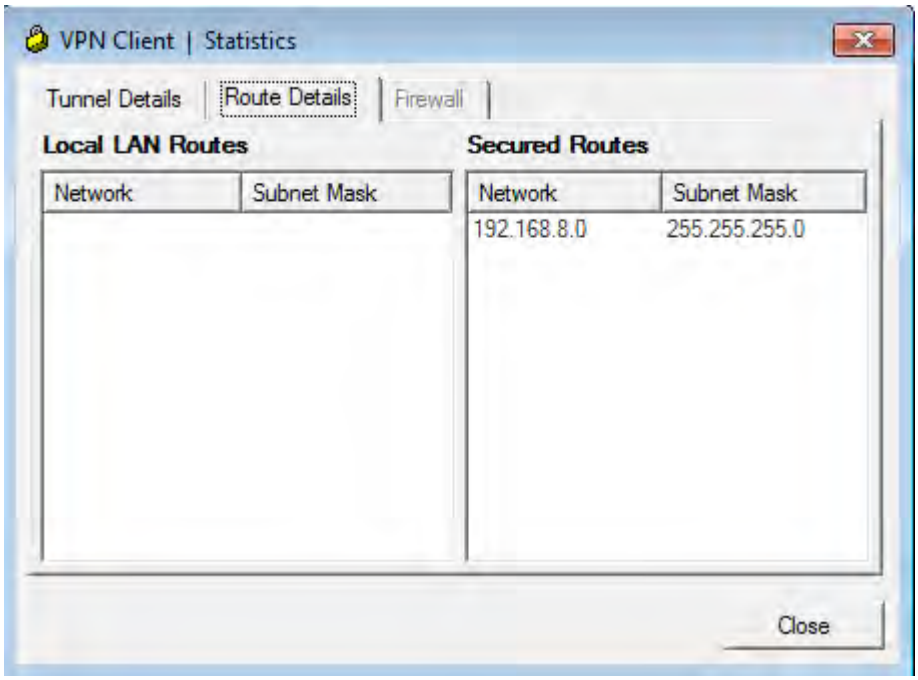
```
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 11 (0x0B)
Radius: Value (String) =
38 2e 39 2e 32 2e 32 30 30                          |  8.9.2.200
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 8.9.2.30 (0x0809021E)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 38 2e 39    |  ip:source-ip=8.9
2e 32 2e 32 30 30                                   |  .2.200
send pkt 8.9.2.150/1645
rip 0x00007fff2e1613a8 state 7 id 37
rad_vrfy() : response message verified
rip 0x00007fff2e1613a8
 : chall_state ''
 : state 0x7
 : reqauth:
     2f 3c c5 1a 4b 28 41 e6 27 d4 7d 72 c3 40 79 be
 : info 0x00007fff2e1614e8
     session_id 0x2e
     request_id 0x25
     user 'EZGROUP'
     response '***'
     app 0
     reason 0
     skey 'outofcontrol'
     sip 8.9.2.150
     type 1

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 182).....
02 25 00 b6 3b e8 e2 35 f9 90 25 21 b9 30 f8 ff    |  .%..;..5..%!.0..
d6 b6 20 e5 01 09 45 5a 47 52 4f 55 50 18 28 52    |  .. ...EZGROUP.(R
65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 63    |  eauthSession:0ac
38 30 36 66 34 30 30 30 30 31 30 32 31 35 31 32    |  806f400001021512
41 42 39 44 46 19 38 43 41 43 53 3a 30 61 63 38    |  AB9DF.8CACS:0ac8
30 36 66 34 30 30 30 30 31 30 32 31 35 31 32 41    |  06f400001021512A
42 39 44 46 3a 70 6f 64 31 32 34 69 73 65 2f 31    |  B9DF:pod124ise/1
34 39 33 39 38 32 36 34 2f 34 34 34 36 1d 06 00    |  49398264/4446...
```

```
00 00 01 1a 0c 00 00 0c 04 05 06 c0 a8 08 1e 1a    |  ................
0d 00 00 0c 04 1b 07 53 50 4c 49 54 1a 0c 00 00    |  .......SPLIT....
0c 04 37 06 00 00 00 01 1a 0e 00 00 0c 04 d9 08    |  ..7.............
45 5a 50 4f 4f 4c                                  |  EZPOOL

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 37 (0x25)
Radius: Length = 182 (0x00B6)
Radius: Vector: 3BE8E235F9902521B930F8FFD6B620E5
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
45 5a 47 52 4f 55 50                               |  EZGROUP
Radius: Type = 24 (0x18) State
Radius: Length = 40 (0x28)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
63 38 30 36 66 34 30 30 30 30 31 30 32 31 35 31    |  c806f40000102151
32 41 42 39 44 46                                  |  2AB9DF
Radius: Type = 25 (0x19) Class
Radius: Length = 56 (0x38)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 38 30 36 66 34 30 30 30    |  CACS:0ac806f4000
30 31 30 32 31 35 31 32 41 42 39 44 46 3a 70 6f    |  01021512AB9DF:po
64 31 32 34 69 73 65 2f 31 34 39 33 39 38 32 36    |  d124ise/14939826
34 2f 34 34 34 36                                  |  4/4446
Radius: Type = 29 (0x1D) Termination-Action
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 5 (0x05) Primary-DNS
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.8.30 (0xC0A8081E)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 13 (0x0D)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 27 (0x1B) Split-Tunnel-Inclusion-List
Radius: Length = 7 (0x07)
Radius: Value (String) =
53 50 4c 49 54                                     |  SPLIT
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 55 (0x37) Split-Tunneling-Policy
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 1 (0x0001)
```

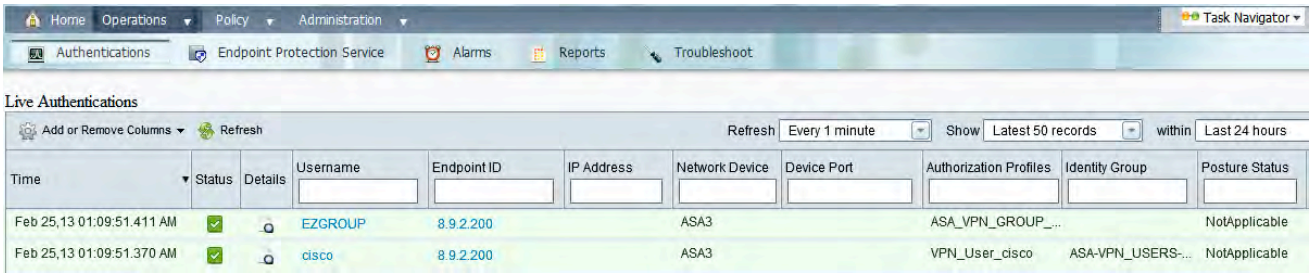
```
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 14 (0x0E)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 217 (0xD9) List of address pools to assign addresses from
Radius: Length = 8 (0x08)
Radius: Value (String) =
45 5a 50 4f 4f 4c                                       |   EZPOOL
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x00007fff2e1613a8 session 0x2e id 37
free_rip 0x00007fff2e1613a8
radius: send queue empty
```







Note the Authorization Profiles matched for the users :




```
ASA3# sh vpn-ses detail ra-ikev1-ipsec

Session Type: IKEv1 IPsec Detailed

Username     : cisco                  Index        : 20
Assigned IP  : 172.16.30.100          Public IP    : 8.9.2.200
Protocol     : IKEv1 IPsec
License      : Other VPN
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 240                    Bytes Rx     : 12680
Pkts Tx      : 4                      Pkts Rx      : 189
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : EZGROUP                Tunnel Group : MIAMI
Login Time   : 18:09:43 UTC Sun Feb 24 2013
Duration     : 0h:06m:43s
Inactivity   : 0h:00m:00s
```

```
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 20.1
  UDP Src Port : 60904                  UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeys
  Encryption   : AES128                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86000 Seconds
  D/H Group    : 2
  Filter Name  :
  Client OS    : WinNT                  Client OS Ver: 5.0.07.0290

IPsec:
  Tunnel ID    : 20.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 172.16.30.100/255.255.255.255/0/0
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28398 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 240                    Bytes Rx     : 12680
  Pkts Tx      : 4                      Pkts Rx      : 189

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 402 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Task 9: DMVPN Phase I

- Configure DMVPN between R5, R6 and R8
- R8 should be seen as 8.9.2.8 on VLAN 2 and should act as a Hub in this configuration
- Traffic between VLAN 5 and VLAN 6 should be switched by the Hub
- Only one tunnel network is allowed for this task – 172.16.100.0/24
- Run EIGRP process to advertise both private networks to the Hub. Use AS 100
- Protect the DMVPN network using IPSec
- Use AES 192 and SHA-1 for Phase I. Use 3DES and MD5 for Phase II
- PSK “cisco” should be used for authentication

Detailed Solution

ASA3

```
access-list OUTSIDE_IN permit icmp any any
```

```
access-list OUTSIDE_IN permit udp any host 192.168.8.8 eq 500
access-list OUTSIDE_IN permit udp any host 192.168.8.8 eq 4500
```

R8

```
cry isa key 0 cisco address 8.9.50.0 255.255.255.0

crypto isakmp policy 12
 encr aes 192
 hash sha
 authentication pre-share

crypto ipsec transform-set SET12 esp-3des esp-md5-hmac
 mode transport

crypto ipsec profile IPSEC_PROF12
 set transform-set SET12

interface Tunnel100
 ip address 172.16.100.8 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 1
 no ip split-horizon eigrp 100
 tunnel protection ipsec profile IPSEC_PROF12

router eigrp 100
 network 172.16.100.8 0.0.0.0
 no auto-summary
```

R5

```
crypto isakmp policy 12
 encr aes 192
 hash sha
 authentication pre-share

crypto isakmp key cisco address 8.9.2.8

crypto ipsec transform-set SET12 esp-3des esp-md5-hmac
 mode transport

crypto ipsec profile IPSEC_PROF12
 set transform-set SET12

interface Tunnel100
 ip address 172.16.100.5 255.255.255.0
 ip nhrp map 172.16.100.8 8.9.2.8
```

```
 ip nhrp map multicast 8.9.2.8
 ip nhrp network-id 1
 ip nhrp nhs 172.16.100.8
 tunnel source Serial0/1/0
 tunnel destination 8.9.2.8
 tunnel key 1
 tunnel protection ipsec profile IPSEC_PROF12

router eigrp 100
 network 10.5.5.0 0.0.0.255
 network 172.16.100.5 0.0.0.0
 no auto-summary
```

R6

```
crypto isakmp policy 12
 encr aes 192
 hash sha
 authentication pre-share

crypto isakmp key cisco address 8.9.2.8

crypto ipsec transform-set SET12 esp-3des esp-md5-hmac
 mode transport

crypto ipsec profile IPSEC_PROF12
 set transform-set SET12

interface Tunnel100
 ip address 172.16.100.6 255.255.255.0
 ip nhrp map 172.16.100.8 8.9.2.8
 ip nhrp map multicast 8.9.2.8
 ip nhrp network-id 1
 ip nhrp nhs 172.16.100.8
 tunnel source Serial0/1/0
 tunnel destination 8.9.2.8
 tunnel key 1
 tunnel protection ipsec profile IPSEC_PROF12

router eigrp 100
 network 10.6.6.6 0.0.0.0
 network 172.16.100.6 0.0.0.0
 no auto-summary
```

The Dynamic Multipoint VPN (DMVPN) feature combines GRE tunnels, IPsec encryption, and NHRP routing to provide users an ease of configuration via crypto profiles - which override the requirement for defining static crypto maps - and dynamic discovery of tunnel endpoints. This feature relies on the following technologies:

1. GRE – A tunneling protocol which is designed to encapsulate IP unicast, multicast and broadcast traffic
2. Multipoint GRE (mGRE) – Allows a single GRE interface to support multiple IPSec tunnels and simplifies the size and complexity of the configuration
3. NHRP – A client-server resolution protocol used to map tunnel IP address to an NBMA address (maps L3 to another L3 address). Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes to build direct tunnels
4. IPSec – Used to protect tunnels in the DMVPN solution

DMVPN was introduced in multiple phases to address various topological needs. Phase I was designed mainly for hub to spoke communication where spoke to spoke traffic traverses the hub (hub routes spoke-to-spoke traffic). The advantage of this deployment over regular P2P GRE tunnels is simplified configuration & IP address space conservation.

In Phase I all spokes are configured with plain point-to-point GRE tunnel to the hub whereas the hub is configured with mGRE interface to accommodate multiple spoke connections. The "`ip nhrp map multicast dynamic`" command tells the hub how it should proceed with multicast/broadcast traffic for which it does not have a mapping available – all registered spokes will receive it. Note that spokes also have a static NHRP mapping configured – this is to register their public IP address on the hub.

In a real-world deployment you would use digital certificates for tunnel authentication. With PSK a wildcard would have to be configured because we rarely know IP addresses of the Spokes. In Phase II and III this would also apply to the Spoke configuration - here we don't really care.

Since NAT for R8 was configured in one of the earlier tasks, this configuration is not shown as part of the solution.

IPv6 Considerations

Before 15.2(1)T the public (NBMA) network must be pure IPv4; private (protected) networks can be IPv6. Starting in 15.2(1)T the public network can be also IPv6.

Tunnel interface configuration should include a statically-defined Link-Local address (to ensure its uniqueness). In full IPv6 DMVPN deployments (NBMA + Tunneled) make sure NHRP mappings use IPv6 address and that the tunnel mode is set to "`gre multipoint ipv6`". Sample showing configuration required on the tunnel interface :

```
int tu 100
 ipv6 address …
 ipv6 address … link-local
 ipv6 nhrp …
 tunnel mode gre multipoint ipv6
```

Verification

```
R8#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.8.8     8.9.50.5        QM_IDLE           1014 ACTIVE
192.168.8.8     8.9.50.6        QM_IDLE           1015 ACTIVE

R8#sh cry ipse sa | in encap|decap|addr
     Crypto map tag: Virtual-Access1-head-0, local addr 192.168.8.8
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
     Crypto map tag: Tunnel100-head-0, local addr 192.168.8.8
   local  ident (addr/mask/prot/port): (192.168.8.8/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (8.9.50.5/255.255.255.255/47/0)
     #pkts encaps: 115, #pkts encrypt: 115, #pkts digest: 115
     #pkts decaps: 137, #pkts decrypt: 137, #pkts verify: 137
   local  ident (addr/mask/prot/port): (192.168.8.8/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (8.9.50.6/255.255.255.255/47/0)
     #pkts encaps: 115, #pkts encrypt: 115, #pkts digest: 115
     #pkts decaps: 125, #pkts decrypt: 125, #pkts verify: 125

R8#sh ip nhrp br
   Target              Via             NBMA           Mode   Intfc   Claimed
172.16.100.5/32      172.16.100.5    8.9.50.5         dynamic  Tu100   <   >
172.16.100.6/32      172.16.100.6    8.9.50.6         dynamic  Tu100   <   >


R8#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.8.30 to network 0.0.0.0

      10.0.0.0/24 is subnetted, 3 subnets
D        10.5.5.0 [90/26882560] via 172.16.100.5, 00:09:23, Tunnel100
D        10.6.6.0 [90/26882560] via 172.16.100.6, 00:09:23, Tunnel100
```

Note there is just one IPSec tunnel (2 SAs) with the Hub:

```
R6#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel100 is up/up, Addr. is 172.16.100.6, VRF ""
   Tunnel Src./Dest. addr: 8.9.50.6/8.9.2.8, Tunnel VRF ""
   Protocol/Transport: "GRE/IP", Protect "IPSEC_PROF12"
   Interface State Control: Disabled

IPv4 NHS:
172.16.100.8  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1         8.9.2.8    172.16.100.8    UP 00:10:42    S    172.16.100.8/32



Crypto Session Details:
--------------------------------------------------------------------------------

Interface: Tunnel100
Session: [0x48F7DD34]
  IKEv1 SA: local 8.9.50.6/4500 remote 8.9.2.8/4500 Active
          Capabilities:N connid:1001 lifetime:23:49:16
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.168.8.8
  IPSEC FLOW: permit 47 host 8.9.50.6 host 8.9.2.8
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 153 drop 0 life (KB/Sec) 4379057/2956
        Outbound: #pkts enc'ed 162 drop 0 life (KB/Sec) 4379076/2956
   Outbound SPI : 0xC3B0C728, transform : esp-3des esp-md5-hmac
    Socket State: Open

Pending DMVPN Sessions:


R6#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
172.16.100.8/32      172.16.100.8    8.9.2.8         static   Tu100   <   >
```

Same on the other Spoke:

```
R5#sh cry sess int tu100 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel100
Uptime: 00:15:10
Session status: UP-ACTIVE
Peer: 8.9.2.8 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.168.8.8
      Desc: (none)
  IKEv1 SA: local 8.9.50.5/4500 remote 8.9.2.8/4500 Active
          Capabilities:N connid:1003 lifetime:23:44:38
  IPSEC FLOW: permit 47 host 8.9.50.5 host 8.9.2.8
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 199 drop 0 life (KB/Sec) 4516321/2689
        Outbound: #pkts enc'ed 220 drop 6 life (KB/Sec) 4516318/2689
```

As you can see Spoke-Spoke packets definitely traverse the Hub:

```
R5#traceroute 10.6.6.6 source F0/0

Type escape sequence to abort.
Tracing the route to 10.6.6.6

  1 172.16.100.8 20 msec 24 msec 24 msec
  2 172.16.100.6 44 msec *  40 msec
```

Task 10: DMVPN Phase II

- Migrate DMVPN configuration from the previous task to Phase II
- Traffic between VLANs 5 and 6 should be no longer going through the Hub

Detailed Solution

R8

```
interface Tunnel100
 no ip next-hop-self eigrp 100
```

R5

```
interface Tunnel100
 no tunnel destination
 tunnel mode gre multipoint

crypto isakmp key cisco address 8.9.50.6
```

R6

```
interface Tunnel100
 no tunnel destination
 tunnel mode gre multipoint

crypto isakmp key cisco address 8.9.50.5
```

Phase II introduced the ability for dynamic spoke-to-spoke tunnels without having the traffic to go through the hub. Spokes are also configured with mGRE interface to emulate a multi-access network.

For spoke-to-spoke to work correctly, the hub must preserve and advertise the private network's next hop as advertised by the spokes themselves (as the tunnel interface IP address). Different routing protocols behave differently in terms of preserving the next-hop information :

1. EIGRP – Next-Hop preservation is not default. Turn it on using "`no ip next-hop-self eigrp <AS>`" command. Also remember to turn off Split Horizion
2. RIP – Keeps the next-hop information by default when the NH is in the same subnet as source of the update
3. OSPF – Next-Hop preservation happens naturally except in point-to-multipoint mode
4. BGP – Next-Hop preservation is a default (within the same AS). Hub must be configured as a route reflector.

First few data packets exchanged between the Spokes will always traverse the Hub (in this phase, they are, however NOT CEF-switched which may cause temporary CPU spikes if there is a lot of new tunnels being established by the Spokes). This is so NHRP could finish its job and populate tables on the Spokes. Once this process is complete, packets no longer flow through the Hub.

IPv6 Considerations

Same as in DMVPN Phase I.

Verification

```
R8#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
172.16.100.5/32      172.16.100.5    8.9.50.5        dynamic  Tu100   <   >
172.16.100.6/32      172.16.100.6    8.9.50.6        dynamic  Tu100   <   >


R8#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.8.30 to network 0.0.0.0

      10.0.0.0/24 is subnetted, 3 subnets
D        10.5.5.0 [90/26882560] via 172.16.100.5, 00:00:42, Tunnel100
D        10.6.6.0 [90/26882560] via 172.16.100.6, 00:00:45, Tunnel100
```

Note what's the Spoke shows us initially. There is only a static NHRP mapping for the Hub but the other Spoke's prefix is said to be reachable via the Spoke:

```
R5#sh ip nhrp br
   Target             Via             NBMA           Mode    Intfc    Claimed
172.16.100.8/32      172.16.100.8    8.9.2.8          static   Tu100    <    >

R5#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D        10.6.6.0/24 [90/28162560] via 172.16.100.6, 00:01:23, Tunnel100
```

How do I get to the NH?

```
R5#sh ip cef 172.16.100.6
172.16.100.0/24
  attached to Tunnel100


R5#sh adjacency tunnel100
Protocol Interface                 Address
IP       Tunnel100                 172.16.100.6(5) (incomplete)
IP       Tunnel100                 172.16.100.8(7)
```

Well, the router still doesn't know :

```
R5#sh adjacency tunnel100 encapsulation
Protocol Interface                 Address
IP       Tunnel100                 172.16.100.6(5) (incomplete)
```

```
  adjacency is incomplete
IP       Tunnel100                172.16.100.8(7)
  Encap length 28
  4500000000000000FF2F77B008093205
  0809020820000080000000001
  Provider: TUNNEL
  Protocol header count in macstring: 2
    HDR 0: ipv4
       dst: static, 8.9.2.8
       src: static, 8.9.50.5
      prot: static, 47
       ttl: static, 255
        df: static, cleared
      per packet fields: tos ident tl chksm
    HDR 1: gre
      prot: static, 0x800
       key: static, 1
      per packet fields: none
```

Same situation on the other Spoke:

```
R6#sh adj tunn 100
Protocol Interface                Address
IP       Tunnel100                172.16.100.5(5) (incomplete)
IP       Tunnel100                172.16.100.8(7)
```

Let's send a data packet to trigger NHRP Resolution:

```
R5#traceroute 10.6.6.6 so F0/0

Type escape sequence to abort.
Tracing the route to 10.6.6.6

  1 172.16.100.8 28 msec 20 msec 24 msec
  2 172.16.100.6 44 msec *  36 msec

R5#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
172.16.100.6/32      172.16.100.6    8.9.50.6        dynamic  Tu100   <   >
172.16.100.8/32      172.16.100.8    8.9.2.8         static   Tu100   <   >

R5#sh adj tu 100
Protocol Interface                Address
IP       Tunnel100                172.16.100.6(11)
IP       Tunnel100                172.16.100.8(7)
```

We now have CEF adjacency built for the NH. From this point on the packets will now be sent to R6 directly bypassing the Hub:

```
R5#sh adjacency tunnel100 encapsulation
Protocol Interface                 Address
IP       Tunnel100                 172.16.100.6(11)
  Encap length 28
  4500000000000000FF2F47B208093205
  0809320620000800000000001
  Provider: TUNNEL
  Protocol header count in macstring: 2
    HDR 0: ipv4
       dst: static, 8.9.50.6
       src: static, 8.9.50.5
      prot: static, 47
       ttl: static, 255
        df: static, cleared
      per packet fields: tos ident tl chksm
    HDR 1: gre
      prot: static, 0x800
       key: static, 1
      per packet fields: none

R5#traceroute 10.6.6.6 so F0/0

Type escape sequence to abort.
Tracing the route to 10.6.6.6

  1 172.16.100.6 36 msec *  36 msec


R5#sh cry sess int tu 100 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel100
Uptime: 00:14:19
Session status: UP-ACTIVE
Peer: 8.9.2.8 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.168.8.8
      Desc: (none)
  IKEv1 SA: local 8.9.50.5/4500 remote 8.9.2.8/4500 Active
          Capabilities:N connid:1006 lifetime:23:45:40
  IPSEC FLOW: permit 47 host 8.9.50.5 host 8.9.2.8
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 202 drop 0 life (KB/Sec) 4537413/2740
        Outbound: #pkts enc'ed 203 drop 0 life (KB/Sec) 4537413/2740
```

```
Interface: Tunnel100
Uptime: 00:04:16
Session status: UP-ACTIVE
Peer: 8.9.50.6 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.50.6
      Desc: (none)
  IKEv1 SA: local 8.9.50.5/500 remote 8.9.50.6/500 Active
          Capabilities:(none) connid:1007 lifetime:23:55:43
  IPSEC FLOW: permit 47 host 8.9.50.5 host 8.9.50.6
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4594175/3343
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4594175/3343
```

Task 11: DMVPN Phase III

- Migrate DMVPN configuration from the previous task to Phase III
- Enable summarization
- Routing information should be summarized as efficient as possible

Detailed Solution

R8

```
interface tunnel 100
 ip next-hop eigrp 100
 ip nhrp redirect
 ip summary-address eigrp 100 10.4.0.0 255.252.0.0
```

R5

```
interface tunnel 100
 ip nhrp shortcut
 ip nhrp redirect
```

R6

```
interface tunnel 100
 ip nhrp shortcut
 ip nhrp redirect
```

In a DMVPN Phase 2 network, each DMVPN network is independent and causes traffic between spokes in different regions to have to traverse through the regional hubs (didn't have to go through the central hubs). In a DMVPN Phase 3 network, all the regional DMVPN networks are "glued" together into a single hierarchical DMVPN network (including the central hubs) and spokes in different regions can build direct spoke-to-spoke tunnels with each other, bypassing both the regional and central hubs.

Our example shows that this feature, among other things, allows data packets to be Cisco Express Forwarding switched (including the initial packets – since NH points to the HUB CEF already knows how to get there) along the routed path until a spoke-to-spoke tunnel is established. Moreover, although the spokes use routes with the IP next-hop set to the hub router (which allows for route summarization), traffic will bypass the hub. This is because this feature forces NHRP entries to overwrite CEF.

To enable NHRP shortcut switching, all spokes need to have the commands "`ip nhrp shortcut`" and the "`ip nhrp redirect`" added to their tunnel interfaces. For the hubs use only "`ip nhrp redirect`".

IPv6 Considerations

Same as in DMVPN Phase I.

Verification

The beginning is the same as in previous Phases. Spokes have only a single entry in the NHRP Table, for the Hub:

```
R5#sh ip nhrp br
   Target              Via             NBMA           Mode    Intfc    Claimed
172.16.100.8/32      172.16.100.8    8.9.2.8          static   Tu100    <   >

R5#sh cry isa peer
Peer: 8.9.2.8 Port: 4500 Local: 8.9.50.5
 Phase1 id: 192.168.8.8
```

Note that the NH points to the Hub, not R6 :

```
R5#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D        10.4.0.0/14 [90/28162560] via 172.16.100.8, 00:00:58, Tunnel100
```

Obviously the Hub knows how to get to real routing information sources :

```
R8#do sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.8.30 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D        10.4.0.0/14 is a summary, 00:02:11, Null0
D        10.5.5.0/24 [90/26882560] via 172.16.100.5, 00:02:11, Tunnel100
D        10.6.6.0/24 [90/26882560] via 172.16.100.6, 00:02:09, Tunnel100
```

Initial packets will be definitely sent to the Hub:

```
R5#sh ip cef 10.6.6.6
10.4.0.0/14
  nexthop 172.16.100.8 Tunnel100

R5#sh adj tu 100
Protocol Interface                 Address
IP       Tunnel100                 172.16.100.8(12)
```

Let's enable NHRP debug on R5 and the Hub to see what's going to change after first data packet is sent by the Spoke:

```
R5#deb nhrp packet
R5#deb nhrp

R8#deb nhrp packet
R8#deb nhrp

R5#ping 10.6.6.6 so f0/0 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 10.5.5.5
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 60/60/60 ms

R8#
*Feb 25 18:21:40.095: NHRP: Attempting to Redirect, remote_nbma: 8.9.50.5
*Feb 25 18:21:40.095: NHRP: inserting (8.9.50.5/10.6.6.122) in redirect table
```

```
*Feb 25 18:21:40.095: NHRP: Attempting to send packet via DEST 10.5.5.5
*Feb 25 18:21:40.095: NHRP: Encapsulation succeeded.  Tunnel IP addr 8.9.50.5
*Feb 25 18:21:40.095: NHRP: Send Traffic Indication via Tunnel100 vrf 0, packet
size: 84
*Feb 25 18:21:40.095:  src: 172.16.100.8, dst: 10.5.5.5
*Feb 25 18:21:40.095:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:21:40.099:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:21:40.099:      pktsz: 84 extoff: 68
*Feb 25 18:21:40.099:  (M) traffic code: redirect(0)
*Feb 25 18:21:40.099:      src NBMA: 192.168.8.8
*Feb 25 18:21:40.099:      src protocol: 172.16.100.8, dst protocol: 10.5.5.5
*Feb 25 18:21:40.099:      Contents of nhrp traffic indication packet:
*Feb 25 18:21:40.099:         45 00 00 64 00 39 00 00 FE 01 9C D6 0A 05 05 05
*Feb 25 18:21:40.099:
R8# 0A 06 06 7A 08 00 35 8F 00 10 00
*Feb 25 18:21:40.099: NHRP: 112 bytes out Tunnel100
```

Second Redirection is for the reply from R6 :

```
*Feb 25 18:21:40.127: NHRP: Attempting to Redirect, remote_nbma: 8.9.50.6
*Feb 25 18:21:40.127: NHRP: inserting (8.9.50.6/10.5.5.5) in redirect table
*Feb 25 18:21:40.127: NHRP: Attempting to send packet via DEST 10.6.6.122
*Feb 25 18:21:40.127: NHRP: Encapsulation succeeded.  Tunnel IP addr 8.9.50.6
*Feb 25 18:21:40.131: NHRP: Send Traffic Indication via Tunnel100 vrf 0, packet
size: 84
*Feb 25 18:21:40.131:  src: 172.16.100.8, dst: 10.6.6.122
*Feb 25 18:21:40.131:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:21:40.131:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:21:40.131:      pktsz: 84 extoff: 68
*Feb 25 18:21:40.131:  (M) traffic code: redirect(0)
*Feb 25 18:21:40.131:      src NBMA: 192.168.8.8
*Feb 25 18:21:40.131:      src protocol: 172.16.100.8, dst protocol: 10.6.6.122
*Feb 25 18:21:40.131:      Contents of nhrp traffic indication packet:
*Feb 25 18:21:40.131:         45 00 00 64 00 39 00 00 FD 01 9D D6 0A 06 06 7A
*Feb 25 18:21:40.131:         0A 05 05 05 00 00 3D 8F 00 10 00
*Feb 25 18:21:40.131: NHRP: 112 bytes out Tunnel100


R5#
*Feb 25 18:18:05.691: NHRP: NHRP successfully resolved 172.16.100.8 to NBMA 8.9.2.8
*Feb 25 18:18:05.727: NHRP: Receive Traffic Indication via Tunnel100 vrf 0, packet
size: 84
*Feb 25 18:18:05.727:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:18:05.727:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:18:05.727:      pktsz: 84 extoff: 68
*Feb 25 18:18:05.727:  (M) traffic code: redirect(0)
*Feb 25 18:18:05.727:      src NBMA: 192.168.8.8
*Feb 25 18:18:05.727:      src protocol: 172.16.100.8, dst protocol: 10.5.5.5
*Feb 25 18:18:05.727:      Contents of nhrp traffic indication packet:
```

```
*Feb 25 18:18:05.727:         45 00 00 64 00 39 00 00 FE 01 9C D6 0A 05 05 05
R5#
*Feb 25 18:18:05.727:         0A 06 06 7A 08 00 35 8F 00 10 00
*Feb 25 18:18:05.727: NHRP: netid_in = 1, to_us = 0
*Feb 25 18:18:05.727: NHRP: nhrp_rtlookup yielded FastEthernet0/0
*Feb 25 18:18:05.727: NHRP: netid_out 0, netid_in 1
```

As a result an "incomplete" entry was added to NHRP Table. This means that for the next data packet we will be sending NHRP Resolution Request to learn the corresponding NBMA.

```
R5#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
10.6.6.122/32        10.6.6.122      incomplete
172.16.100.8/32      172.16.100.8    8.9.2.8         static   Tu100   <   >
```

Let's send another one to trigger the Shortcut feature:

```
R5#ping 10.6.6.122 so f0/0 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.6.6.122, timeout is 2 seconds:
Packet sent with a source address of 10.5.5.5
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 60/60/60 ms
```

As you will see in this debug there will be few Request/Replies exchanges going on to also learn the mapping for the logical/physical address of the Spoke (R6). Similar output would be seen on R6 – this is so the devices know how to build the new GRE tunnel (Spoke-to-Spoke):

```
R5#
*Feb 25 18:20:23.383: NHRP: Enqueued NHRP Resolution Request for destination:
10.6.6.122
*Feb 25 18:20:23.395: NHRP: Checking for delayed event /10.6.6.122 on list
(Tunnel100).
*Feb 25 18:20:23.395: NHRP: No node found.
```

Note that first "Shortcut" from R5 is sent to the Hub. R6 will reply directly – it will learn the IP address of R5 from this shortcut packet (Hub will forward it to R6):

```
*Feb 25 18:20:23.395: NHRP: Sending NHRP Resolution Request for dest: 10.6.6.122 to
NHS: 172.16.100.8 using our src: 172.16.100.5
*Feb 25 18:20:23.395: NHRP: Attempting to send packet via DEST 172.16.100.8
*Feb 25 18:20:23.395: NHRP: NHRP successfully resolved 172.16.100.8 to NBMA 8.9.2.8
*Feb 25 18:20:23.395: NHRP: Encapsulation succeeded.  Tunnel IP addr 8.9.2.8
*Feb 25 18:20:23.395: NHRP: Send Resolution Request via Tunnel100 vrf 0, packet
size: 72
*Feb 25 18:20:23.395:  src: 172.16.100.5, dst: 172.16.100.8
```

```
*Feb 25 18:20:23.395:  (F) afn: IP
R5#v4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:20:23.395:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:20:23.395:      pktsz: 72 extoff: 52
*Feb 25 18:20:23.395:  (M) flags: "router auth src-stable nat ", reqid: 5
*Feb 25 18:20:23.395:      src NBMA: 8.9.50.5
*Feb 25 18:20:23.395:      src protocol: 172.16.100.5, dst protocol: 10.6.6.122
*Feb 25 18:20:23.395:  (C-1) code: no error(0)
*Feb 25 18:20:23.395:        prefix: 32, mtu: 17912, hd_time: 7200
*Feb 25 18:20:23.395:         addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0,
pref: 0
*Feb 25 18:20:23.395: NHRP: 100 bytes out Tunnel100
```

Redirect from R8:

```
*Feb 25 18:20:23.415: NHRP: Receive Traffic Indication via Tunnel100 vrf 0, packet
size: 84
*Feb 25 18:20:23.415:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:20:23.415:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:20:23.415:      pktsz: 84 extoff: 68
*Feb 25 18:20:23.415:  (M) traffic code: redirect(0)
*Feb 25 18:20:23.415:      src NBMA: 192.168.8.8
*Feb 25 18:20:23.415:      src protocol: 172.16.100.8, dst protocol: 10.5.5.5
*Feb 25 18:20:23.415:      Contents of nhrp traffic indication packet:
*Feb 25 18:20:23.415:         45 00 00 64 00 3A 00 00 FE 01 9C D5 0A 05 05 05
*Feb 25 18:20:23.415:         0A 06 06 7A 08 00 1B B0 00 11 00
*Feb 25 18:20:23.415: NHRP: netid_in = 1, to_us = 0
*Feb 25 18:20:23.419: NHRP: nhrp_rtlookup yielded FastEthernet0/0
*Feb 25 18:20:23.419: NHRP: netid_out 0, netid_in 1
```

Now R6 tries to learn the mapping for R5's 10.5.5.5 so it could reply to the original shortcut packet:

```
*Feb 25 18:20:23.459: NHRP: Receive Resolution Request via Tunnel100 vrf 0, packet
size: 92
*Feb 25 18:20:23.459:  (F) afn: IPv4(1), type: IP(800), hop: 254, ver: 1
*Feb 25 18:20:23.459:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:20:23.459:      pktsz: 92 extoff: 52
*Feb 25 18:20:23.459:  (M) flags: "router auth src-stable nat ", reqid: 4
*Feb 25 18:20:23.459:      src NBMA: 8.9.50.6
*Feb 25 18:20:23.463:      src protocol: 172.16.100.6, dst protocol: 10.5.5.5
*Feb 25 18:20:23.463:  (C-1) code: no error(0)
*Feb 25 18:20:23.463:        prefix: 32, mtu: 17912, hd_time: 7200
*Feb 25 18:20:23.463:         addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0,
pref: 0
*Feb 25 18:20:23.463: NHRP: netid_in = 1, to_us = 0
*Feb 25 18:20:23.463: NHRP: nhrp_rtlookup yielded FastEthernet0/0
*Feb 25 18:20:23.463: NHRP: netid_out 0, netid_in 1
```

Before we reply, we must wait for the IPSec tunnel to come up:

```
*Feb 25 18:20:23.463: NHRP: We are egress router for target 10.5.5.5, recevied via
Tunnel100
*Feb 25 18:20:23.463: NHRP: Redist mask now 11
*Feb 25 18:20:23.463: NHRP: Checking for delayed event 172.16.100.6/10.5.5.5 on list
(Tunnel100).
*Feb 25 18:20:23.463: NHRP: No node found.
*Feb 25 18:20:23.463: NHRP: Delaying resolution request nbma src:8.9.50.5 nbma
dst:8.9.50.6 reason:IPSEC-IFC: need to wait for IPsec SAs.
*Feb 25 18:20:23.767: NHRP: Enqueueing delayed event to be processed.
src:172.16.100.6 dst:10.5.5.5
*Feb 25 18:20:23.771: NHRP: Process delayed resolution request src:172.16.100.6
dst:10.5.5.5
*Feb 25 18:20:23.771: NHRP: nhrp_rtlookup yielded FastEthernet0/0
*Feb 25 18:20:23.771: NHRP: netid_out 0, netid_in 1
*Feb 25 18:20:23.771: NHRP: We are egress router for target 10.5.5.5, recevied via
Tunnel100
*Feb 25 18:20:23.771: NHRP: Redist mask now 11
*Feb 25 18:20:23.771: NHRP: Checking for delayed event 172.16.100.6/10.5.5.5 on list
(Tunnel100).
*Feb 25 18:20:23.771: NHRP: No node found.
*Feb 25 18:20:23.771: NHRP: No need to delay processing of resolution event nbma
src:8.9.50.5 nbma dst:8.9.50.6

*Feb 25 18:20:23.771: NHRP: Adding Tunnel Endpoints (VPN: 172.16.100.6, NBMA:
8.9.50.6)
*Feb 25 18:20:23.775: NHRP: Successfully attached NHRP subblock for Tunnel Endpoints
        (VPN: 172.16.100.6, NBMA: 8.9.50.6)
*Feb 25 18:20:23.775: NHRP: Attempting to send packet via DEST 172.16.100.6
*Feb 25 18:20:23.775: NHRP: NHRP successfully resolved 172.16.100.6 to NBMA 8.9.50.6
```

OK let's tell R6 how to get to 10.5.5.5 in a efficient way:

```
*Feb 25 18:20:23.775: NHRP: Encapsulation succeeded.  Tunnel IP addr 8.9.50.6
*Feb 25 18:20:23.775: NHRP: Send Resolution Reply via Tunnel100 vrf 0, packet size:
120
*Feb 25 18:20:23.775:   src: 172.16.100.5, dst: 172.16.100.6
*Feb 25 18:20:23.775:   (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:20:23.775:       shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:20:23.775:       pktsz: 120 extoff: 60
*Feb 25 18:20:23.775:    (M) flags: "router auth dst-stable unique src-stable nat ",
reqid: 4
*Feb 25 18:20:23.775:       src NBMA: 8.9.50.6
*Feb 25 18:20:23.775:       src protocol: 172.16.100.6, dst protocol: 10.5.5.5
*Feb 25 18:20:23.775:   (C-1) code: no error(0)
*Feb 25 18:20:23.775:         prefix: 32, mtu: 17912, hd_time: 7200
*Feb 25 18:20:23.775:           addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4,
pref: 0
*Feb 25 18:20:23.779:         client NBMA: 8.9.50.5
```

```
*Feb 25 18:20:23.779:        client protocol: 172.16.100.5
*Feb 25 18:20:23.779: NHRP: 148 bytes out Tunnel100
*Feb 25 18:20:25.171: NHRP: Checking for delayed event /10.6.6.122 on list
(Tunnel100).
```

NHRP Resolution Request for 10.6.6.122 is re-sent:

```
*Feb 25 18:20:25.171: NHRP: No node found.
*Feb 25 18:20:25.171: NHRP: Sending NHRP Resolution Request for dest: 10.6.6.122 to
NHS: 172.16.100.8 using our src: 172.16.100.5
*Feb 25 18:20:25.171: NHRP: Attempting to send packet via DEST 172.16.100.8
*Feb 25 18:20:25.171: NHRP: NHRP successfully resolved 172.16.100.8 to NBMA 8.9.2.8
*Feb 25 18:20:25.171: NHRP: Encapsulation succeeded.  Tunnel IP addr 8.9.2.8
*Feb 25 18:20:25.171: NHRP: Send Resolution Request via Tunnel100 vrf 0, packet
size: 72
*Feb 25 18:20:25.171:  src: 172.16.100.5, dst: 172.16.100.8
*Feb 25 18:20:25.171:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:20:25.171:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:20:25.171:      pktsz: 72 extoff: 52
*Feb 25 18:20:25.171:  (M) flags: "router auth src-stable nat ", reqid: 5
*Feb 25 18:20:25.171:      src NBMA: 8.9.50.5
*Feb 25 18:20:25.171:      src protocol: 172.16.100.5, dst protocol: 10.6.6.122
*Feb 25 18:20:25.171:  (C-1) code: no error(0)
*Feb 25 18:20:25.171:        prefix: 32, mtu: 17912, hd_time: 7200
*Feb 25 18:20:25.171:         addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0,
pref: 0
*Feb 25 18:20:25.171: NHRP: 100 bytes out Tunnel100
```

Finally the reply comes in directly from R6 (along with the prefix length /24):

```
*Feb 25 18:20:25.235: NHRP: Receive Resolution Reply via Tunnel100 vrf 0, packet
size: 120
*Feb 25 18:20:25.235:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Feb 25 18:20:25.235:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 25 18:20:25.235:      pktsz: 120 extoff: 60
*Feb 25 18:20:25.235:  (M) flags: "router auth dst-stable unique src-stable nat ",
reqid: 5
*Feb 25 18:20:25.235:      src NBMA: 8.9.50.5
*Feb 25 18:20:25.239:      src protocol: 172.16.100.5, dst protocol: 10.6.6.122
*Feb 25 18:20:25.239:  (C-1) code: no error(0)
*Feb 25 18:20:25.239:        prefix: 24, mtu: 17912, hd_time: 7199
*Feb 25 18:20:25.239:         addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4,
pref: 0
*Feb 25 18:20:25.239:        client NBMA: 8.9.50.6
*Feb 25 18:20:25.239:        client protocol: 172.16.100.6
*Feb 25 18:20:25.239: NHRP: netid_in = 0, to_us = 1
*Feb 25 18:20:25.239: NHRP: Checking for delayed event /10.6.6.122 on list
(Tunnel100).
*Feb 25 18:20:25.239: NHRP: No node found.
```

```
*Feb 25 18:20:25.239: NHRP: No need to delay processing of resolution event nbma
src:8.9.50.5 nbma dst:8.9.50.6
*Feb 25 18:20:25.239: NHRP: Adding Tunnel Endpoints (VPN: 172.16.100.6, NBMA:
8.9.50.6)
```

NHRP Tables are now fully populated:

```
R6#sh ip nhrp br
   Target              Via             NBMA           Mode   Intfc   Claimed
10.5.5.5/32          172.16.100.5     8.9.50.5        dynamic  Tu100   <   >
10.6.6.0/24          172.16.100.6     8.9.50.6        dynamic  Tu100   <   >
172.16.100.5/32      172.16.100.5     8.9.50.5        dynamic  Tu100   <   >
172.16.100.8/32      172.16.100.8     8.9.2.8         static   Tu100   <   >
```

Note R5 has a learnt the full prefix, 10.6.6.0/24 :

```
R5#sh ip nhrp br
   Target              Via             NBMA           Mode   Intfc   Claimed
10.5.5.5/32          172.16.100.5     8.9.50.5        dynamic  Tu100   <   >
10.6.6.0/24          172.16.100.6     8.9.50.6        dynamic  Tu100   <   >
172.16.100.6/32      172.16.100.6     8.9.50.6        dynamic  Tu100   <   >
172.16.100.8/32      172.16.100.8     8.9.2.8         static   Tu100   <   >
```

Now even that FIB says “send packet to the NH 172.16.100.8” NHRP table will override this :

```
R5#sh ip cef 10.6.6.122
10.4.0.0/14
  nexthop 172.16.100.8 Tunnel100

R5#sh adj tu 100
Protocol Interface                 Address
IP       Tunnel100                 172.16.100.6(9)
IP       Tunnel100                 172.16.100.8(12)

R5#sh ip nhrp br
   Target              Via             NBMA           Mode   Intfc   Claimed
10.5.5.5/32          172.16.100.5     8.9.50.5        dynamic  Tu100   <   >
10.6.6.0/24          172.16.100.6     8.9.50.6        dynamic  Tu100   <   >
172.16.100.6/32      172.16.100.6     8.9.50.6        dynamic  Tu100   <   >
172.16.100.8/32      172.16.100.8     8.9.2.8         static   Tu100   <   >
```

NHRP says go to 172.16.100.6 which means send the packet physically to 8.9.50.6 – CEF entry is overwritten:

```
R5#traceroute 10.6.6.122 so f0/0

Type escape sequence to abort.
Tracing the route to 10.6.6.122
```

```
  1 172.16.100.6 36 msec 36 msec 36 msec
  2 10.6.6.122 36 msec *  36 msec

R5#sh cry sess int tu 100 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel100
Uptime: 00:39:41
Session status: UP-ACTIVE
Peer: 8.9.2.8 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.168.8.8
      Desc: (none)
  IKEv1 SA: local 8.9.50.5/4500 remote 8.9.2.8/4500 Active
          Capabilities:N connid:1010 lifetime:23:20:17
  IPSEC FLOW: permit 47 host 8.9.50.5 host 8.9.2.8
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 534 drop 0 life (KB/Sec) 4592894/1218
        Outbound: #pkts enc'ed 531 drop 0 life (KB/Sec) 4592895/1218

Interface: Tunnel100
Uptime: 00:26:10
Session status: UP-ACTIVE
Peer: 8.9.50.6 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.50.6
      Desc: (none)
  IKEv1 SA: local 8.9.50.5/500 remote 8.9.50.6/500 Active
          Capabilities:(none) connid:1011 lifetime:23:33:49
  IKEv1 SA: local 8.9.50.5/500 remote 8.9.50.6/500 Active
          Capabilities:(none) connid:1012 lifetime:23:33:49
  IPSEC FLOW: permit 47 host 8.9.50.5 host 8.9.50.6
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 6 drop 0 life (KB/Sec) 4592115/2029
        Outbound: #pkts enc'ed 7 drop 1 life (KB/Sec) 4592115/2029

R6#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
```

```
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2         8.9.50.5     172.16.100.5    UP 00:26:31     D
                            172.16.100.5    UP 00:26:31     D
     1          8.9.2.8     172.16.100.8    UP 00:40:00     S
```

Task 12: Redundant GETVPN

- Configure GET VPN between R2, R5 and R6
- R2 should act as primary KS
- Protect the ICMP traffic between GMs
- Use AES 192 and SHA-1 for both phases
- Use pre-shared key “ipexpert” for authentication.
- Rekey messages should be sent as multicast to 239.5.5.5
- Secure the re-key transmission
- Configure R4 as redundant KS

Detailed Solution

R2

```
crypto isakmp policy 15
 encr aes 192
 hash sha
 authentication pre-share

crypto isakmp key ipexpert address 8.9.50.4
crypto isakmp key ipexpert address 8.9.50.5
crypto isakmp key ipexpert address 8.9.50.6

cry isa keepalive 10 periodic

access-list 150 permit icmp host 8.9.50.5 host 8.9.50.6
access-list 150 permit icmp host 8.9.50.6 host 8.9.50.5

ip access-list extended REKEY
 permit udp host 8.9.50.2 eq 848 host 239.5.5.5 eq 848

crypto ipsec transform-set GETSET esp-aes 192 esp-sha-hmac

crypto ipsec profile IPSEC_GET_PROF
 set transform-set GETSET

crypto key generate rsa label GETKEY exportable

crypto gdoi group GR1
 identity number 1
```

```
 server local
  rekey address ipv4 REKEY
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa GETKEY
  sa ipsec 1
   profile IPSEC_GET_PROF
   match address ipv4 150
   replay counter window-size 64
  address ipv4 8.9.50.2
  redundancy
   local priority 15
   peer address ipv4 8.9.50.4

cry key export rsa GETKEY pem terminal 3des cisco123
```

R4

```
crypto isakmp policy 15
 encr aes 192
 hash sha
 authentication pre-share

crypto isakmp key ipexpert address 8.9.50.2
crypto isakmp key ipexpert address 8.9.50.5
crypto isakmp key ipexpert address 8.9.50.6

cry isa keepalive 10 periodic

crypto key import rsa GETKEY terminal cisco123

access-list 150 permit icmp host 8.9.50.5 host 8.9.50.6
access-list 150 permit icmp host 8.9.50.6 host 8.9.50.5

ip access-list extended REKEY
 permit udp host 8.9.50.4 eq 848 host 239.5.5.5 eq 848

crypto ipsec transform-set GETSET esp-aes 192 esp-sha-hmac
crypto ipsec profile IPSEC_GET_PROF
 set transform-set GETSET

crypto gdoi group GR1
 identity number 1
 server local
  rekey address ipv4 REKEY
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa GETKEY
  sa ipsec 1
   profile IPSEC_GET_PROF
   match address ipv4 150
   replay counter window-size 64
```

```
 address ipv4 8.9.50.4
  redundancy
   local priority 1
   peer address ipv4 8.9.50.2
```

R5, R6

```
crypto isakmp policy 15
 encr aes 192
 hash sha
 authentication pre-share

crypto isakmp key ipexpert address 8.9.50.2
crypto isakmp key ipexpert address 8.9.50.4

crypto gdoi group GR1
 identity number 1
 server address ipv4 8.9.50.2
 server address ipv4 8.9.50.4

crypto map MAP1 15 gdoi
 set group GR1

interface Serial0/1/0
 crypto map MAP1
```

GET VPN (tunnel-less VPN) eliminates the need for tunnels. By removing the need for point-to-point tunnels, meshed networks can scale higher while maintaining network-intelligence features critical to voice and video quality. GET VPN offers a new standards-based security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

The Group Member (GM) is the router that registers with the key server to get the IPsec SA to communicate with other devices in the group. During registration, group member provides the group ID and receives the security policy and keys for this group from the server (KS). The registration process consists of ISAKMP Phase I followed by the GDOI exchange – the key server authenticates and authorizes the group members. ISAKMP/GDOI connection works over UDP port 848.

Key Server (KS) is the router responsible for maintaining the policy and creating and maintaining the keys for the group. The key server also “rekeys” the group before existing keys expire. The server can send two types of keys: the traffic encryption key (TEK) and the key encryption key (KEK). The TEK is the shared key used by IPsec SAs to protect data, whereas the KEK is used to encrypt the rekey messages (which mostly contain new TEKs and possibly new KEK) and is used by the group members to decrypt the incoming rekey messages from the key server.

Cooperative key servers (COOP KS) provide redundancy to GET VPN. Multiple key servers are supported by GET VPN to ensure redundancy, high availability, and fast recovery if the primary key server fails. Cooperating GDOI key servers jointly manage the GDOI registrations for the group. Each key server is an active key server, handling GDOI registration requests from group members. Because the key servers are cooperating, each key server distributes the same state to the group members that register with it. Load balancing is achieved because each of the GDOI key servers can service a portion of the GDOI registrations.

Before you start doing any GET VPN configuration make sure to take care of ISAKMP Phase I policy. If pre-shared keys are used for authentication, spokes should have only one key configured – for the KS. GET VPN configuration involves setting the group ID, group ACL, IPSec protection and optionally rekeying and COOP KS.

COOP configuration requires the policy to be the same on both key servers. Higher priority value determines which server will act as primary for the group. RSA keys have to be configured as exportable and copied to the secondary KS. This is because server's public key is downloaded during the registration and will be used to authenticate incoming rekey messages.

IPv6 Considerations

GETVPN supports IPv6 from 15.2(3)T but only in the Data Plane. GETVPN Control Plane can be only configured over IPv4.

Groups can be either IPv4 or IPv6; Mixed Modes configurations are not supported.

A quick way to see if all devices support IPv6 is to issue "`show crypto gdoi feature ipv6-crypto-path`".

When configuring, both the GETVPN Group & Crypto Map must be IPv6:

```
crypto gdoi group ipv6 group_name
crypto map ipv6 MAP1 seq_nr gdoi
```

Verification

```
R2#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
8.9.50.2        8.9.50.4        GDOI_IDLE         1011 ACTIVE
8.9.50.2        8.9.50.5        GDOI_IDLE         1012 ACTIVE
8.9.50.2        8.9.50.6        GDOI_IDLE         1013 ACTIVE
```

Our GMs successfully registered:

```
R2#sh crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group GR1 : 0

Group Member ID   : 8.9.50.5
Group ID          : 1
Group Name        : GR1
Key Server ID     : 8.9.50.2

Group Member ID   : 8.9.50.6
Group ID          : 1
Group Name        : GR1
Key Server ID     : 8.9.50.2
```

The key size for TEK encryption is 24B which is 192 bits (AES 192):

```
R2#sh crypto gdoi ks pol
Key Server Policy:
For group GR1 (handle: 2147483650) server 8.9.50.2 (handle: 2147483650):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Multicast)
    spi : 0xB0ADFE0ED4304EF4189F4E096F7CE33
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec): 86400       remaining life(sec): 86388
    sig hash algorithm : enabled     sig key length    : 94
    sig size           : 64
    sig key name       : GETKEY

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xECBD7140    access-list           : 150
    # of transforms    : 0             transform             : ESP_AES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 24            sig key size          : 20
    orig life(sec)     : 3600          remaining life(sec)   : 3589
    tek life(sec)      : 3600          elapsed time(sec)     : 11
    antireplay window size: 64

For group GR1 (handle: 2147483650) server 8.9.50.4 (handle: 2147483655):
    antireplay window size: 64

For group GR1 (handle: 2147483650) server 8.9.50.4 (handle: 2147483655):

R2#sh crypto gdoi ks acl
```

```
Group Name: GR1
 Configured ACL:
   access-list 150 permit icmp host 8.9.50.5 host 8.9.50.6
   access-list 150 permit icmp host 8.9.50.6 host 8.9.50.5
```

R2 is definitely a Primary KS. R4 is "UP" but due to the lower priority value it acts as a secondary unit:

```
R2#sh crypto gdoi ks coop
Crypto Gdoi Group Name :GR1
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 8.9.50.2
        Local Priority: 15
        Local KS Role: Primary    , Local KS Status: Alive
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 8
                Antireplay Sequence Number: 9

        Peer Sessions:
        Session 1:
                Server handle: 2147483655
                Peer Address: 8.9.50.4
                Peer Priority: 1
                Peer KS Role: Secondary , Peer KS Status: Alive
                Antireplay Sequence Number: 1

                IKE status: Established
                Counters:
                    Ann msgs sent: 7
                    Ann msgs sent with reply request: 0
                    Ann msgs recv: 0
                    Ann msgs recv with reply request: 1
                    Packet sent drops: 2
                    Packet Recv drops: 0
                    Total bytes sent: 2830
                    Total bytes recv: 56


R4#sh cry gd ks
Total group members registered to this box: 2

Key Server Information For Group GR1:
    Group Name               : GR1
    Group Identity           : 1
    Group Members            : 2
    IPSec SA Direction       : Both
    ACL Configured:
        access-list 150
```

```
    Redundancy                : Configured
        Local Address         : 8.9.50.4
        Local Priority        : 1
        Local KS Status       : Alive
        Local KS Role         : Secondary
```

GM information is synchronized between KSes:

```
R4#sh cry gdoi ks mem

Group Member Information :

Number of rekeys sent for group GR1 : 0

Group Member ID    : 8.9.50.5
 Group ID          : 1
 Group Name        : GR1
 Key Server ID     : 8.9.50.2

Group Member ID    : 8.9.50.6
 Group ID          : 1
 Group Name        : GR1
 Key Server ID     : 8.9.50.2
```

Both GMs registered. No rekeys as of right now:

```
R5#sh cry gdoi gm

Group Member Information For Group GR1:
    IPSec SA Direction        : Both
    ACL Received From KS      : gdoi_group_GR1_temp_acl

    Group member              : 8.9.50.5         vrf: None
       Registration status    : Registered
       Registered with        : 8.9.50.2
       Re-registers in        : 3330 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from        : 0.0.0.0
       Last rekey seq num     : 0
       Multicast rekey rcvd   : 0
```

Test connectivity:

```
R6#ping 8.9.50.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.9.50.5, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms

R6#sh cry sess int s0/1/0 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/1/0
Uptime: 00:35:13
Session status: UP-ACTIVE
Peer: 0.0.0.0 port 848 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.50.2
      Desc: (none)
  IKEv1 SA: local 8.9.50.6/848 remote 8.9.50.2/848 Active
          Capabilities:(none) connid:1025 lifetime:23:56:30
  IKEv1 SA: local 239.5.5.5/848 remote 8.9.50.2/848 Active
          Capabilities:(none) connid:1026 lifetime:6w2d
  IPSEC FLOW: permit 1 host 8.9.50.6 host 8.9.50.5
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/3382
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/3382
  IPSEC FLOW: permit 1 host 8.9.50.5 host 8.9.50.6
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/3382
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/3382
```

OK now let's trigger a rekey and see if it goes through:

```
R2(config)#crypto ipsec transform-set SET2 esp-3des esp-md5-hmac
R2(config)#crypto ipsec profile IPSEC_GET_PROF
R2(ipsec-profile)#set transform-set SET2
R2(ipsec-profile)#end

R2#
Feb 25 23:10:06.251: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group
GR1 from address 8.9.50.2 to 239.5.5.5  with seq # 3
R5#sh cry gdoi gm reke
Group GR1 (Multicast)
    Number of Rekeys received (cumulative)       : 1
    Number of Rekeys received after registration : 1

R6#sh cry gdoi gm reke
Group GR1 (Multicast)
    Number of Rekeys received (cumulative)       : 1
    Number of Rekeys received after registration : 1
```

Now I am going to mimic the Primary KS Failure and this way test redundancy:

```
R2(config)#int s0/1/0
R2(config-if)#sh
```

R4 is now Primary KS. R2 shows as “Dead”:

```
R4#sh cry gdoi ks coop
Crypto Gdoi Group Name :GR1
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 8.9.50.4
        Local Priority: 1
        Local KS Role: Primary   , Local KS Status: Alive
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 3
                Antireplay Sequence Number: 18

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 8.9.50.2
                Peer Priority: Unknown
                Peer KS Role: Primary   , Peer KS Status: Dead
                Antireplay Sequence Number: 28

                IKE status: Failed
                Counters:
                    Ann msgs sent: 0
                    Ann msgs sent with reply request: 1
                    Ann msgs recv: 27
                    Ann msgs recv with reply request: 0
                    Packet sent drops: 18
                    Packet Recv drops: 0
                    Total bytes sent: 56
                    Total bytes recv: 12807
```

Now we will re-register on R5 and test rekeying:

```
R5#clear cry gd
% The Key Server and Group Member will destroy created and downloaded policies.
% All Group Members are required to re-register.

Are you sure you want to proceed ? [yes/no]: yes

R5#
```

```
*Feb 25 23:10:11.157: %CRYPTO-5-GM_REGSTER: Start registration to KS 8.9.50.2 for
group GR1 using address 8.9.50.5
R5#
*Feb 25 23:10:51.157: %CRYPTO-5-GM_REGSTER: Start registration to KS 8.9.50.4 for
group GR1 using address 8.9.50.5
*Feb 25 23:10:51.397: %GDOI-5-SA_KEK_UPDATED: SA KEK was updated
*Feb 25 23:10:51.397: %GDOI-5-SA_TEK_UPDATED: SA TEK was updated
*Feb 25 23:10:51.453: %GDOI-5-GM_REGS_COMPL: Registration to KS 8.9.50.4 complete
for group GR1 using address 8.9.50.5

R5#sh cry gdoi gm

Group Member Information For Group GR1:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GR1_temp_acl

    Group member             : 8.9.50.5         vrf: None
       Registration status   : Registered
       Registered with       : 8.9.50.4
       Re-registers in       : 3189 sec
       Succeeded registration: 1
       Attempted registration: 2
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 0
```

And finally rekey from R4:

```
R4(config)#crypto ipsec transform-set SET2 esp-3des esp-md5-hmac
R4(config)#crypto ipsec profile IPSEC_GET_PROF
R4(ipsec-profile)#set transform-set SET2
R4(ipsec-profile)#end

R5#
*Feb 25 23:13:15.705: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GR1 from
8.9.50.4 to 239.5.5.5 with seq # 11

R5#sh cry gd gm reke
Group GR1 (Multicast)
    Number of Rekeys received (cumulative)       : 1
    Number of Rekeys received after registration : 1

R6#sh cry gd gm reke
Group GR1 (Multicast)
    Number of Rekeys received (cumulative)       : 2
    Number of Rekeys received after registration : 2
```

Note even R6 registered with R2, after a failure it was still able to process rekeys from R4 :

```
R6#sh cry gdoi gm

Group Member Information For Group GR1:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GR1_temp_acl

    Group member             : 8.9.50.6         vrf: None
       Registration status   : Registered
       Registered with       : 8.9.50.2
       Re-registers in       : 3439 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 8.9.50.4
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 2
```

Task 13: SSL Remote Access IOS

- Configure R7 to provide WebVPN connections on F0/0 interface port 443
- HTTP connections should be redirected to HTTPS automatically
- Create user “john” with password “matrix”
- That user should authenticate in domain “VALVERDE”
- Remote users should be able to access CAT3 via Telnet using local port 5000
- Remote users should be able to WWW to CAT3 through a link on the portal page

Detailed Solution

R7

```
aaa new-model
aaa authentication login NO none
aaa authentication login SSLAUTH local

line con 0
 login authentication NO

webvpn gateway SSLGW
 ip address 8.9.2.7 port 443
 http-redirect port 80
 inservice

webvpn context SSLCONTEXT
 ssl authenticate verify all

 url-list "CAT3-HTTP"
   heading "CAT3 GUI"
   url-text "CAT3" url-value "http://10.1.1.133"

 port-forward "PF"
```

```
   local-port 5000 remote "10.1.1.133" remote-p 23 desc "CAT3_TELNET"

 policy group SSLPOL
   url-list "CAT3-HTTP"
   port-forward "PF"
 default-group-policy SSLPOL
 aaa authentication list SSLAUTH
 gateway SSLGW domain VALVERDE
 inservice

username john pass matrix
```

SSL VPN is a second example of Remote Access VPNs where the policy and connection settings are pre-defined on the headend device. SSL VPNs can be deployed in one of the following modes:

1. Clientless
    a. Browser-based - Content can be securely accessed via a web browser (but only web-based content is accessible)
    b. Port-Forwarding/Smart Tunnels – This mode (also known as “Thin Client”) provides access to TCP-based services like Telnet or SSH. Access is delivered via a Java/ActiveX applet that is dynamically downloaded from the SSL VPN appliance upon session establishment (initial session must be still established via a web browser)
2. Full Client (Tunnel Mode) – remote access is provided by downloading SSL VPN client software such as AnyConnect. This mode delivers L3 access to virtually any application that runs over IP

IOS SSL VPN configuration consists of few components. The Gateway is the destination IP endpoint for the user session, and the Context is where the Group Policy is defined and applied to the user session. The Group Policy determines the parameters of the user session, and how the session will behave.

General SSL process on IOS can be described in four steps. This applies to all SSL modes :

1. The end user initiates the SSL VPN connection to the WebVPN gateway
2. The context a user is attempting to connect to is identified by the URL or login information. Now the user must be authenticated under the context they belong to
3. The secure gateway must determine if it will let this user into the WebVPN context, so it will send the username and password to the AAA server. The method of AAA does not matter, just so authentication can be done
4. The AAA server authenticates the user and it will indicate this to the context. It may also push down any RADIUS attributes for that user. The WebVPN context will build a user session under the context, and apply the policy group information and RADIUS attributes (if RADIUS was used). Now the workflow changes depending on the policy group parameters applied to the user session

In Clientless mode, which is the default mode for a context, the process is complete. The WebVPN portal will now be displayed to the end user in the Web browser. The user will have the specified access to the VPN.

In our example the SSL gateway configuration does not have a specific SSL trustpoint assigned. It means that a self-signed certificate is automatically generated when an SSL VPN gateway is put in service and the auto-generated trustpoint will be associated with it. In case you want to use any other certificate you would need to create the trustpoint manually, specify all required settings and then tell the router to use certificate stored by this particular trustpoint (`ssl trustpoint`) under the "`webvpn gateway`".

Additionally, remember that whenever you are doing any AAA configuration you should think about safeguarding the console and/or whatever else they ask you to do in that matter in the real exam.

IPv6 Considerations

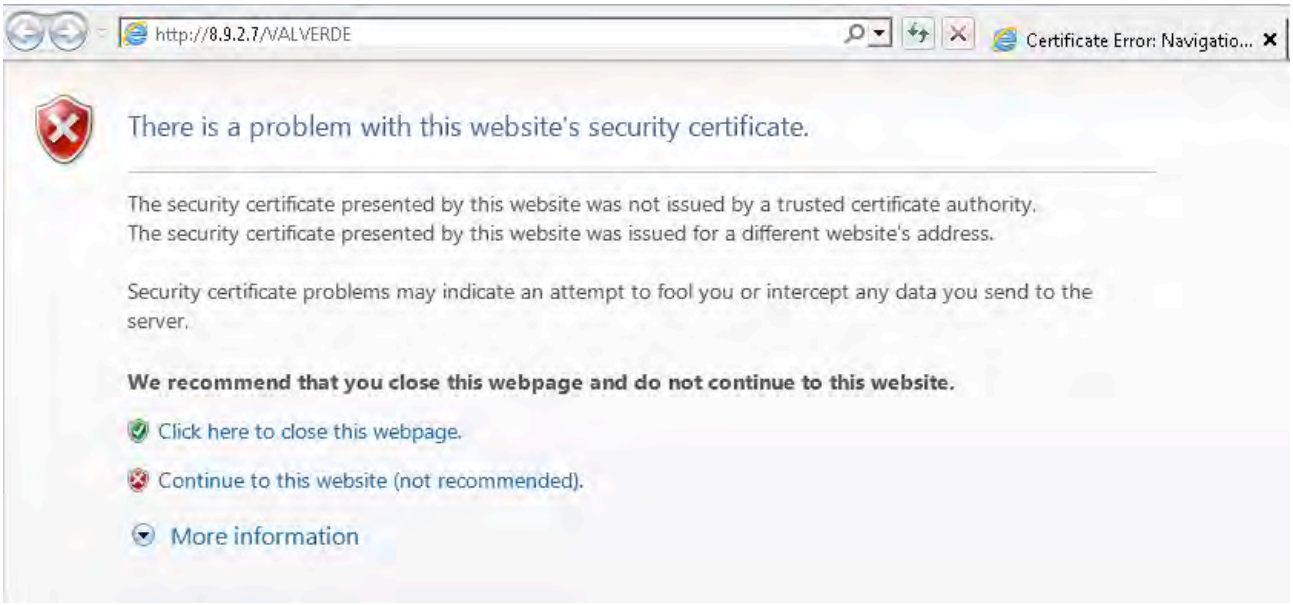
Not supported as of 15.2 IOS version.

Verification

```
R7#sh webvpn gateway SSLGW
Admin Status: up
Operation Status: up
Error and Event Logging: Disabled
IP: 8.9.2.7, port: 443
HTTP Redirect port: 80
SSL Trustpoint: TP-self-signed-2461677768
FVRF Name not configured


R7#sh webvpn context SSLCONTEXT
Admin Status: up
Operation Status: up
Error and Event Logging: Disabled
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List: SSLAUTH
AAA Authorization List not configured
AAA Accounting List not configured
AAA Authentication Domain not configured
Authentication mode: AAA authentication
Default Group Policy: SSLPOL
Associated WebVPN Gateway: SSLGW
Domain Name: VALVERDE
Maximum Users Allowed: 1000 (default)
NAT Address not configured
```

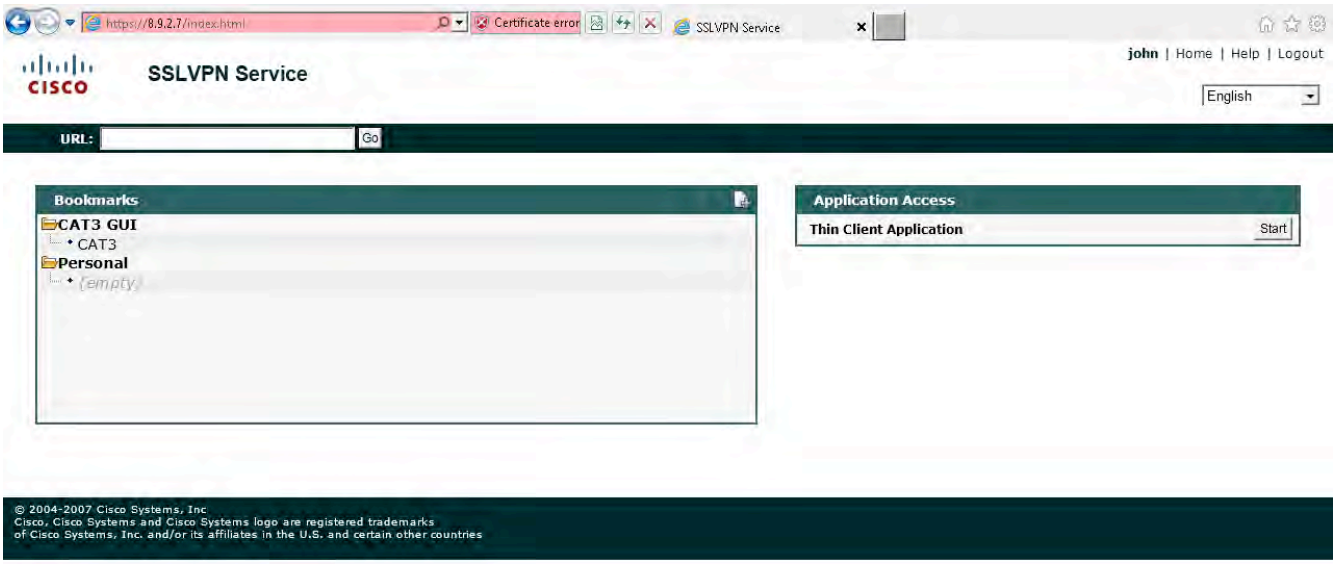
```
VRF Name not configured
Virtual Template not configured

R7#sh webvpn policy group SSLPOL context SSLCONTEXT
WV: group policy = SSLPOL ; context = SSLCONTEXT
      url list name = "CAT3-HTTP"
      idle timeout = 2100 sec
      session timeout = Disabled
      port forward name = "PF"
      functions =

      citrix disabled
      netmask = 255.255.255.255
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keepalive interval = 30 sec
      SSLVPN Full Tunnel mtu size = 1406 bytes
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

Connect to the SSL VPN Portal page:

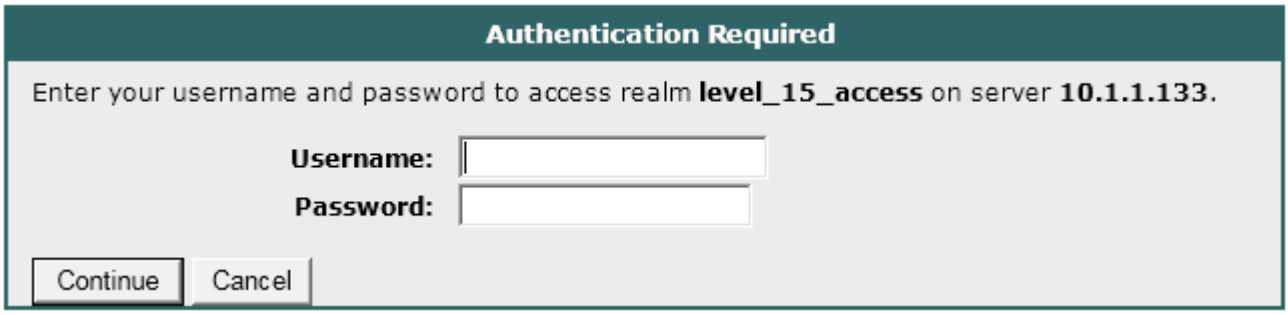


Login as John Matrix:

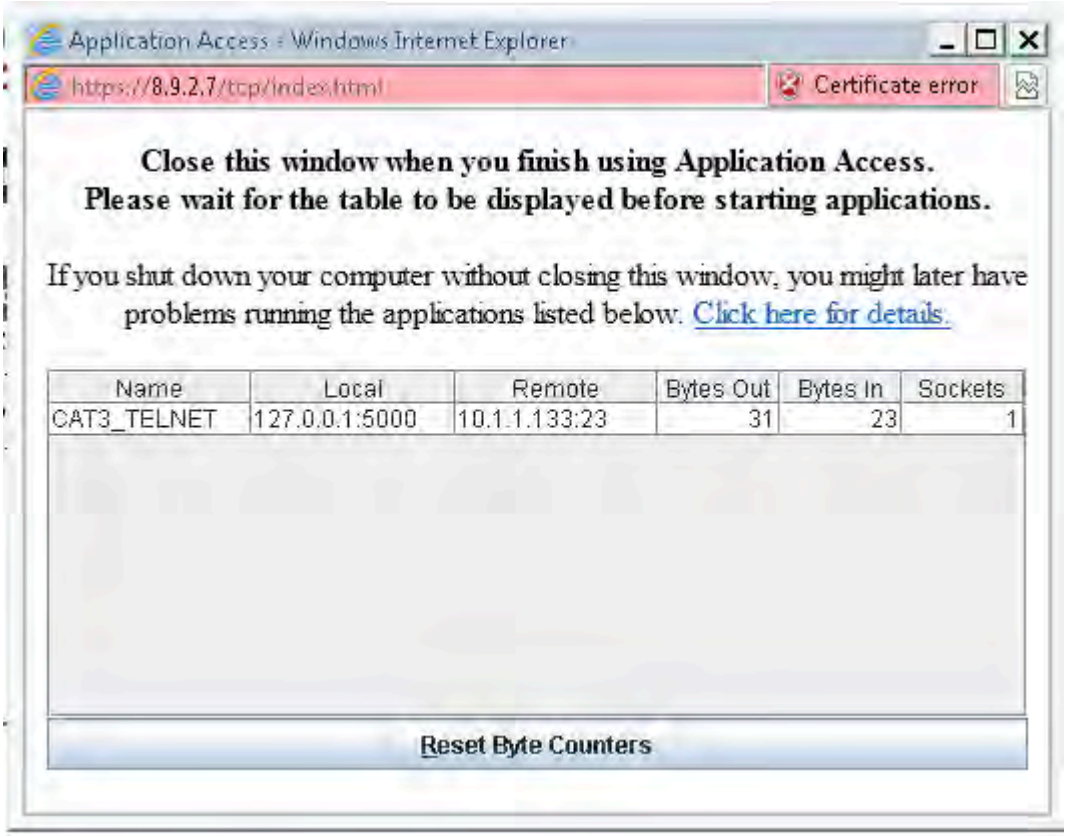
You should see a similar Portal page:



Test CAT3 WWW (click on “CAT3” bookmark):



Then open up "Thin Client Application" and telnet to 127.0.0.1:5000:



Task 14: SSL Remote Access IOS - AnyConnect

- Configure R7 to provide Full Client connections for remote users
- Create a separate context "ISLAND" - make sure only AnyConnect clients are allowed

- Use local IP address pool 10.140.140.0/24 for the connecting clients
- Tunnel only traffic going to VLAN 100
- Assign the clients domain-name of “ipexpert.com” and DNS Server of 10.1.1.101

Detailed Solution

R7

```
ip local pool ANYPOOL 10.140.140.2 10.140.140.254

int loopback 100
 ip address 10.140.140.1 255.255.255.0

webvpn install svc flash:/anyconnect-dart-win-2.4.0202-k9.pkg

webvpn context ANYCONNECT
 ssl encryption rc4-md5
 ssl authenticate verify all

 policy group ANYCONNECT_POL
   functions svc-required
   svc address-pool "ANYPOOL"
   svc default-domain "ipexpert.com"
   svc split include 10.1.1.0 255.255.255.0
   svc dns-server primary 10.1.1.101
 default-group-policy ANYCONNECT_POL
 aaa authentication list SSLAUTH
 gateway SSLGW domain ISLAND
 inservice
```

If the user is going to do Tunnel mode, using function “svc-enabled” or “svc-required” in the group policy or RADIUS attributes, the process to push down the SSL VPN Client will happen next, in addition to the four general steps described in the solution to previous task. This will mean that the SSL VPN Client once installed on the client PC will establish a new SSL session to the context, and the original context will be removed. Furthermore, it will alter the PC routing table to do the specified tunnel function defined in the policy. Now that the user session is established to the WebVPN secure gateway, the backend interfaces handle the access to the inside network. Once a user is authenticated under a given context, the user session is established. This user session will embody the parameters specified globally in the context, the group policy, and any RADIUS attributes pushed down during authentication for that user.

To implement the Full Client Mode on IOS there is just few additions to the Clientless configuration. First is to load the SVC image to the router. To load AnyConnect File use the "`webvpn install`" (older codes) or "`crypto vpn anyconnect`" command (newer IOSes). The rest is to define an IP address pool and in our case also the loopback interface which must be configured with an IP address and subnet mask from the address pool. The interface would not be necessary if you used a pool reachable from a directly connected network. Finally, under the Policy Group, the pool should be specified (`svc address-pool`) and SVC enabled (`functions svc-enable`) or required for a successful connection (`functions svc-required`). Any other task-specific configurations would be also typically configured under the Group Policy.

IPv6 Considerations

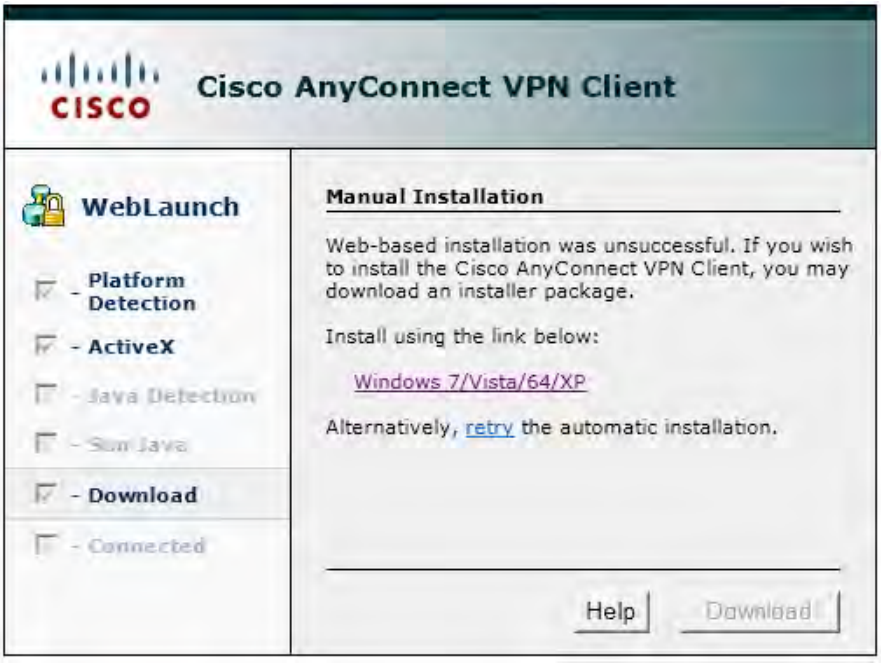
Not supported as of 15.2 IOS version.

Verification

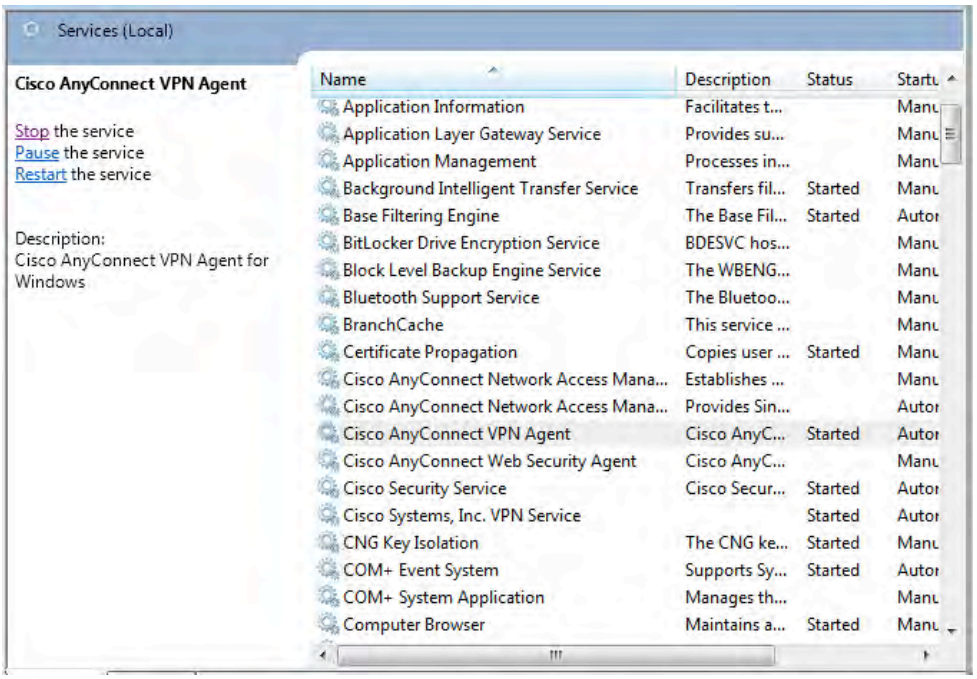
```
R7#sh webvpn gateway SSLGW
Admin Status: up
Operation Status: up
Error and Event Logging: Disabled
IP: 8.9.2.7, port: 443
HTTP Redirect port: 80
SSL Trustpoint: TP-self-signed-2461677768
FVRF Name not configured

R7#sh webvpn context ANYCONNECT
Admin Status: up
Operation Status: up
Error and Event Logging: Disabled
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List: SSLAUTH
AAA Authorization List not configured
AAA Accounting List not configured
AAA Authentication Domain not configured
Authentication mode: AAA authentication
Default Group Policy: ANYCONNECT_POL
Associated WebVPN Gateway: SSLGW
Domain Name: ISLAND
Maximum Users Allowed: 1000 (default)
NAT Address not configured
VRF Name not configured
Virtual Template not configured

R7#sh webvpn policy group ANYCONNECT_POL context all
WEBVPN: group policy = ANYCONNECT_POL ; context = ANYCONNECT
      idle timeout = 2100 sec
      session timeout = Disabled
```

```
functions =
          svc-required

citrix disabled
address pool name = "ANYPOOL"
netmask = 255.255.255.255
default domain = "ipexpert.com"
dpd client timeout = 300 sec
dpd gateway timeout = 300 sec
keepalive interval = 30 sec
SSLVPN Full Tunnel mtu size = 1406 bytes
keep sslvpn client installed = disabled
rekey interval = 3600 sec
rekey method =
lease duration = 43200 sec
split include = 10.1.1.0 255.255.255.0
DNS primary server = 10.1.1.101
```

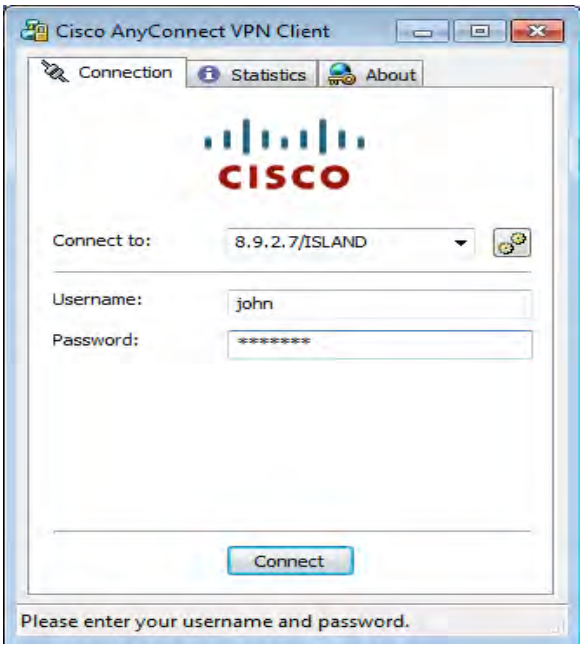
Use VNC (Remote Desktop is by default not allowed to be used for AnyConnect connections) and connect to “8.9.2.7/ISLAND” and download AnyConnect. You may need to manually click on the “Download” button and then select “Windows 7/Vista/64/XP” :



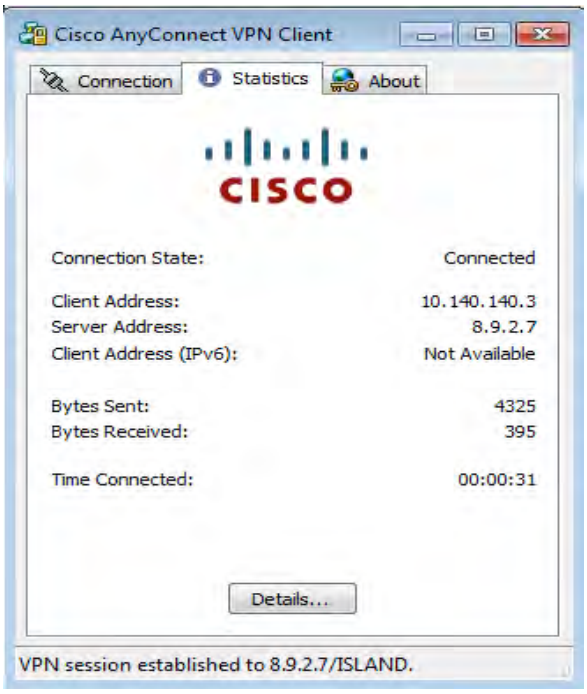
You may also want to disable installed AnyConnect 3.x before being able to use the older client (the one you downloaded). Click on Windows “Start” button, “run” and type “services.msc”. Configure services for Cisco AnyConnect as shown below – only VPN Agent should be “Started”:



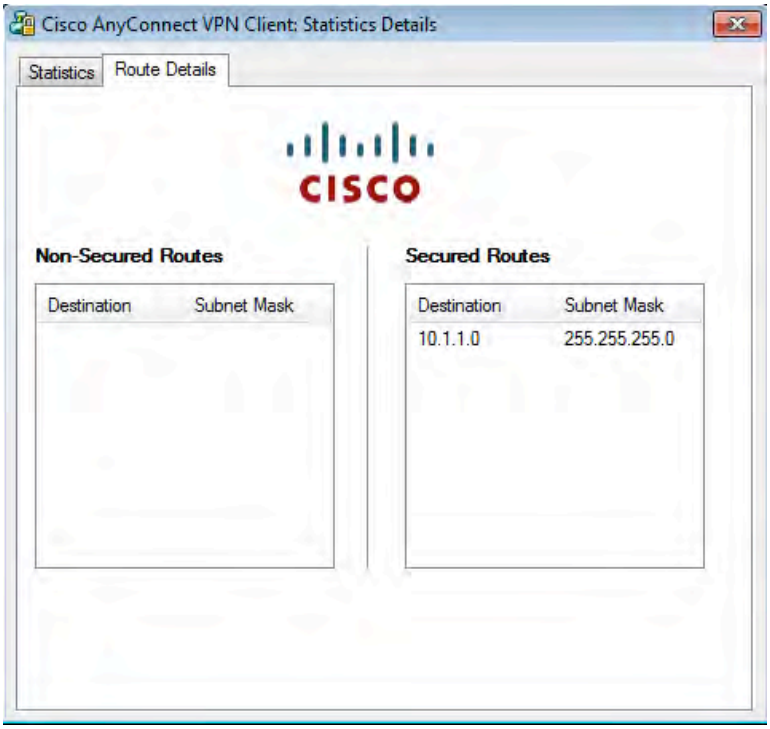
Login to context “ISLAND”:

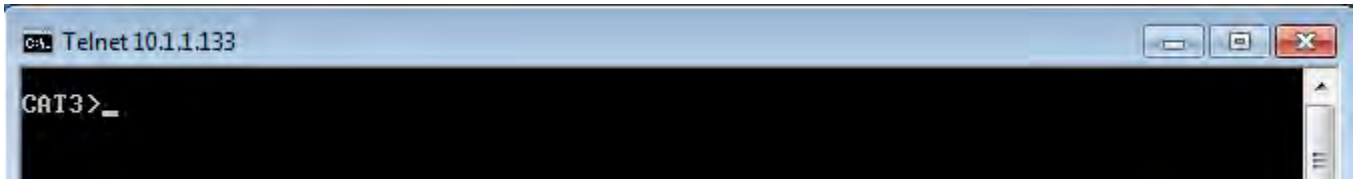


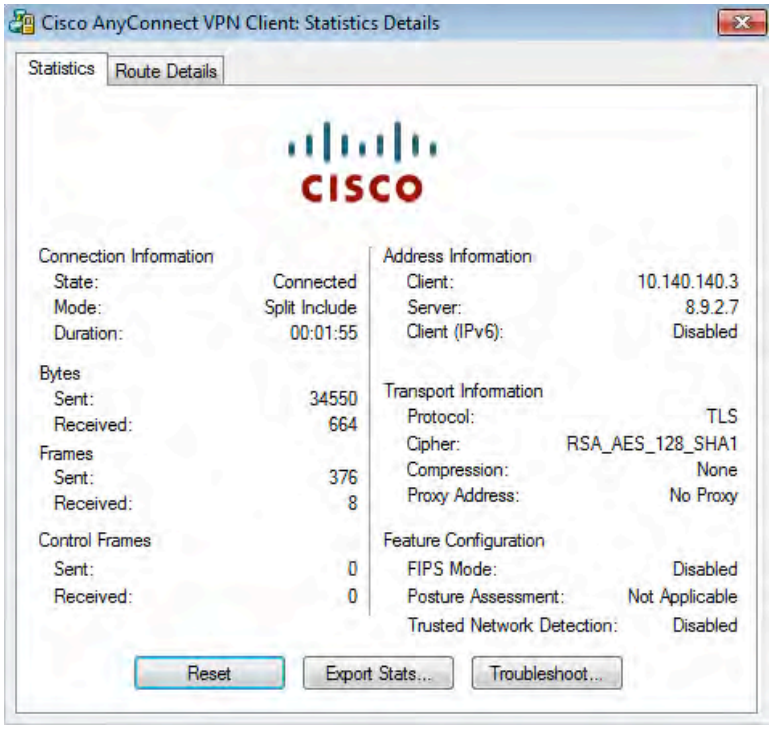
You should see the following window:

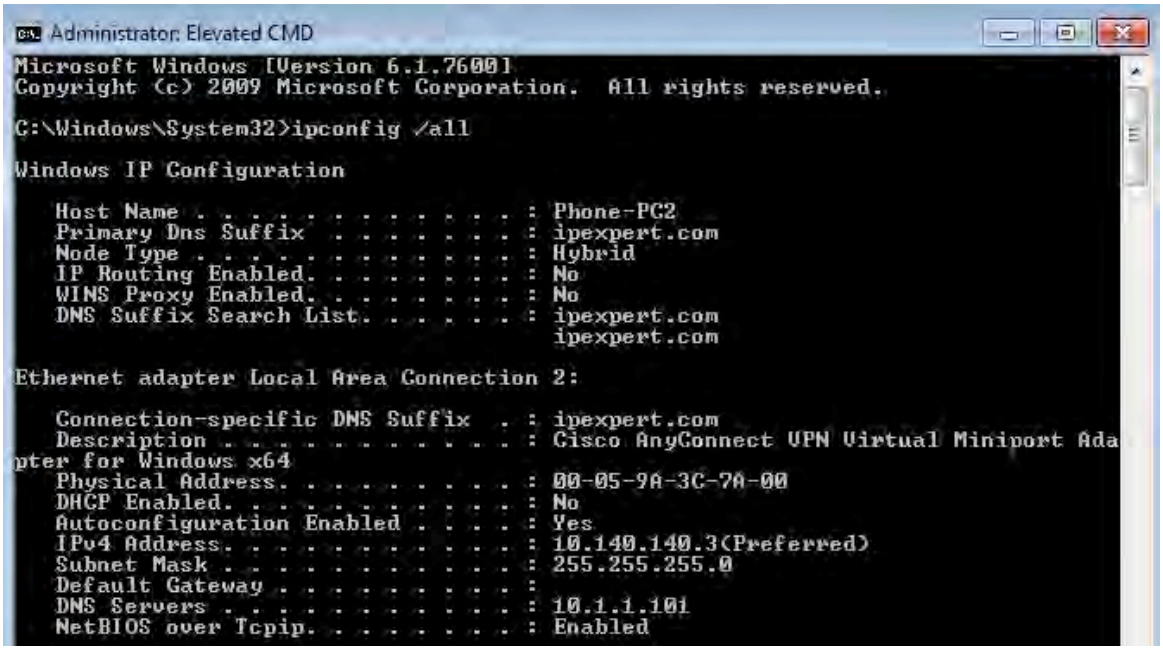


Verify route details and test connectivity by telnetting to CAT3:









Task 15: SSL Remote Access ASA

- Configure ASA3 to provide WebVPN connections on G0/0 interface port 443
- Create user “mad” with password “max”
- That user should authenticate to group AUSTRALIA
- Remote users should be able to access R8’s console using Putty
- Disable the ability to enter any HTTP/HTTPS URL on the portal page

Detailed Solution

ASA3

```
webvpn
 port 443
 smart-tunnel list PUTTY PUTTY putty.exe
 tunnel-group-list enable
 enable outside

group-policy WEBPOL internal
group-policy WEBPOL attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  smart-tunnel enable PUTTY
  url-entry disable

tunnel-group WEBGROUP type remote-access
tunnel-group WEBGROUP general-attributes
 default-group-policy WEBPOL
tunnel-group WEBGROUP webvpn-attributes
 group-alias AUSTRALIA enable

username mad password max
```

R8

```
line vty 0 4
 no login
```

WebVPN configuration on the ASA involves setting some SSL-specific options as well as defining a group policy and a tunnel group. Global “`webvpn`” mode allows us to choose the port ASA will be accepting the incoming SSL connections on, plus we can also define our Port Forwarding/Smart Tunnel configuration and enable the tunnel group list. This feature (“`tunnel-group-list`”) allows the users to select a group for login and authentication.

Clientless SSL VPN attributes and options for tunnel groups and group policies can be looked up in the ASA Configuration Guide under “Configuring VPN” -> „Configuring Tunnel Groups, Group Policies, and Users” -> “Configuring Connection Profiles for Clientless SSL VPN Sessions”.

For Tunnel (Full Client) mode, few other things would need to be configured. In addition to a standard group policy (here "`vpn-tunnel-protocol`" has to be set to "`ssl-client`" or "`svc`" in older code versions) and tunnel group configuration, we would need to define an address pool (`ip local pool`; don't forget to apply it to the Group Policy/Tunnel Group) and load an SVC image to the appliance's memory. This last step could be accomplished from within the "`webvpn`" configuration mode – the commands needed are "`anyconnect image`" and "`anyconnect enable`".

IPv6 Considerations

See the next task.

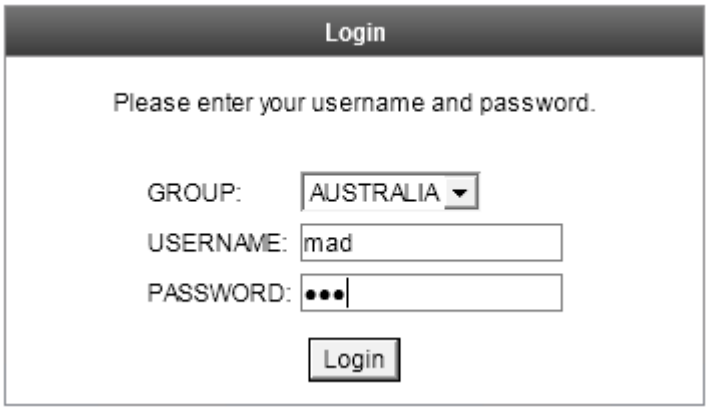
Verification

```
ASA3(config)# sh vpn-sessiondb det webvpn

Session Type: WebVPN Detailed

Username     : mad                    Index        : 21
Public IP    : 8.9.2.200
Protocol     : Clientless
License      : AnyConnect Premium
Encryption   : RC4                    Hashing      : SHA1
Bytes Tx     : 958208                 Bytes Rx     : 66372
Pkts Tx      : 5                      Pkts Rx      : 1
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : WEBPOL                 Tunnel Group : WEBGROUP
Login Time   : 06:54:41 UTC Tue Feb 26 2013
Duration     : 0h:03m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

Clientless Tunnels: 1

Clientless:
  Tunnel ID    : 21.1
  Public IP    : 8.9.2.200
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 28 Minutes
  Client Type  : Web Browser
  Client Ver   : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0)
  Bytes Tx     : 958208                 Bytes Rx     : 66372

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
```

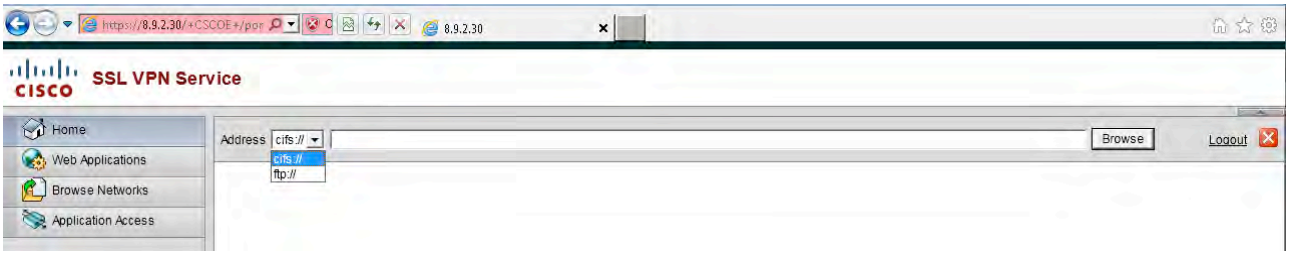
```
  SQ Int (T)    : 0 Seconds              EoU Age(T)    : 194 Seconds
  Hold Left (T): 0 Seconds               Posture Token:
```

```
ASA3(config)# sh webvpn group-alias
Tunnel Group: WEBGROUP    Group Alias: AUSTRALIA enabled
```

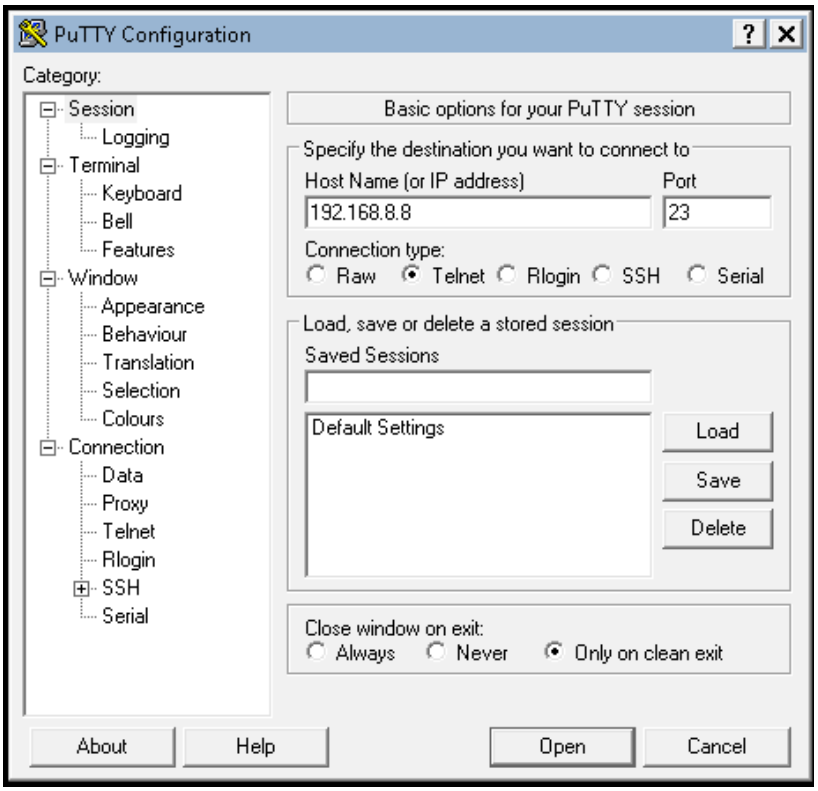
Navigate to https://8.9.2.30 :

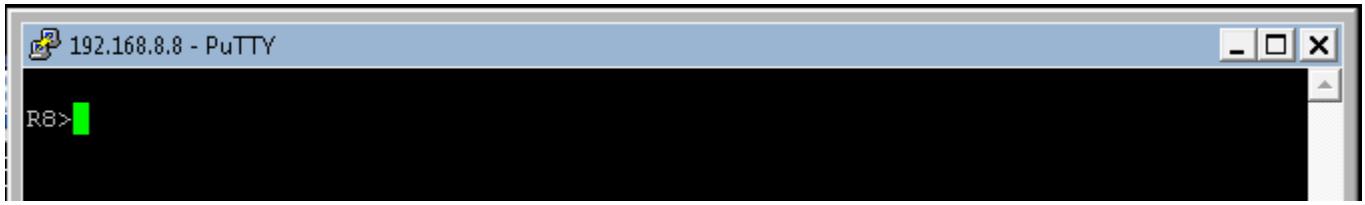


Note HTTP URLs can no longer be entered:

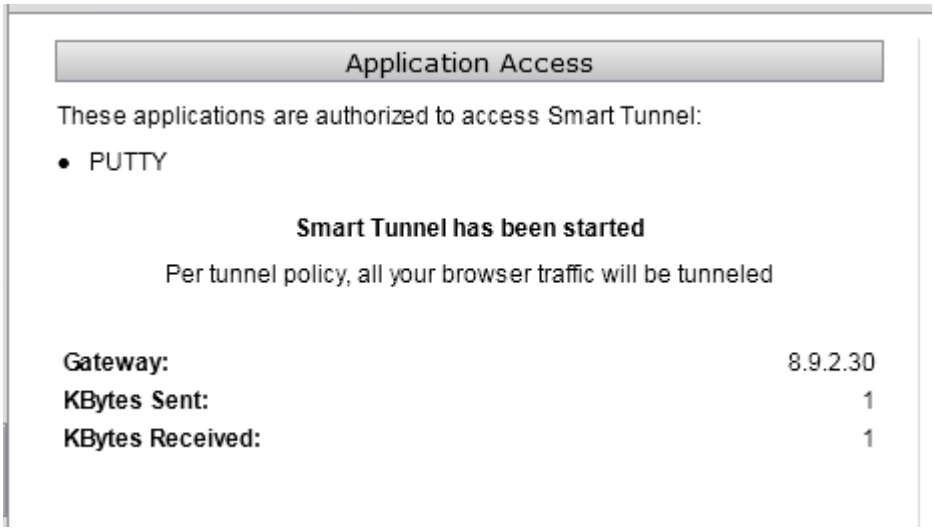


Go to “Application Access”. Start PUTTY:





Confirm traffic is going through the Smart Tunnel:



Task 16: IPv6 SSL Remote Access ASA - AnyConnect

- Configure ASA3 to provide SSL (AnyConnect) connections on G0/0 interface port 443
- Initial clientless connection (client download) should be redirected to HTTPs
- Use local IPv4 address pool 10.170.170.0/24
- ASA should only allow to access to VLAN8
- User “mad” should authenticate to group “DESERT”
- For SSL connection use the protocol that avoids latency and bandwidth problems
- IPv6 access should be also included – use 2192:168:8::0/64 in VLAN8
- You can add a default route on R8

Detailed Solution

ASA3

```
webvpn
 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
 anyconnect enable
 enable outside

http redirect outside 80

access-list SSLSPLIT standard permit 192.168.8.0 255.255.255.0

ip local pool SSLPOOL 10.170.170.1-10.170.170.254
ipv6 local pool SSL6POOL 2010:170:170::1/64 100

group-policy SSLPOL internal
group-policy SSLPOL attributes
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SSLSPLIT
 address-pools value SSLPOOL
 ipv6-address-pools value SSL6POOL
 webvpn
  anyconnect ssl dtls enable
  anyconnect keep-installer none
  anyconnect ask enable default anyconnect

tunnel-group SSLGROUP type remote-access
tunnel-group SSLGROUP general-attributes
 default-group-policy SSLPOL
tunnel-group SSLGROUP webvpn-attributes
 group-alias DESERT enable

object-group network NAT_EXEMPT
 network-object 10.170.170.0 255.255.255.0
 network-object 172.16.30.0 255.255.255.0
```

```
no nat (in,out) source static R8 R8 dest static VPNPOOL VPNPOOL
nat (in,out) source static R8 R8 dest static NAT_EXEMPT NAT_EXEMPT
```

R8

```
ipv route ::/0 2192:168:8::30
```

Configuring SSL VPN in the ASA is similar to regular WebVPN configuration. In addition to a standard group policy (here "`vpn-tunnel-protocol`" has to be set to "`ssl-client`") and tunnel group configuration, there few steps that are client SSL VPN specific : AnyConnect image has to be loaded to the appliance (in the older ASA versions use the "`svc`" keyword instead of "`anyconnect`") and an address pool has to be also configured whereas Split Tunneling is optional.

Using DTLS, which is UDP-based, reduces the delays associated with stream protocols (delay and latency can result in poor VoIP and other real-time applications quality).

NAT Exemption is required for R8 to successfully communicate with SSL VPN clients.

IPv6 Considerations

ASA allows to tunnel IPv6 packets over an IPv4 SSL tunnel to provide support for both protocols – note that the client PC must be a dual-stack device. This feature is supported only in Full Client Mode (with AnyConnect) with IKEv1 using CLI (ASDM cannot be used for this particular configuration). The ASA does not support IPv6 over IPsec IKEv2 VPN sessions.

The ASA does not currently support Split Tunneling for IPv6 traffic. The ASA tunnels all IPv6 traffic through the VPN connection.

To enable IPV6 SSL VPN, do the following general actions:

1. Assign an IPv6 address / enable IPv6 on the outside interface (e.g. `ipv6 enable`)
2. Assign an IPv6 address / enable IPv6 on the inside interface (e.g. `ipv6 address`)
3. Configure an IPv6 address local pool for client assigned IP Addresses (`ipv6 local pool`). IPv4 Pool must be also defined – the SSL VPN tunnel will be established using IPv4
4. Assign both pools to the Tunnel Group : IPv6 (`ipv6-address-pool`) and IPv4 (address-pools)
5. Make sure IPv6 routing is configured correctly

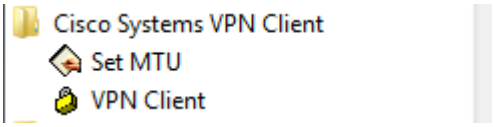
Verification

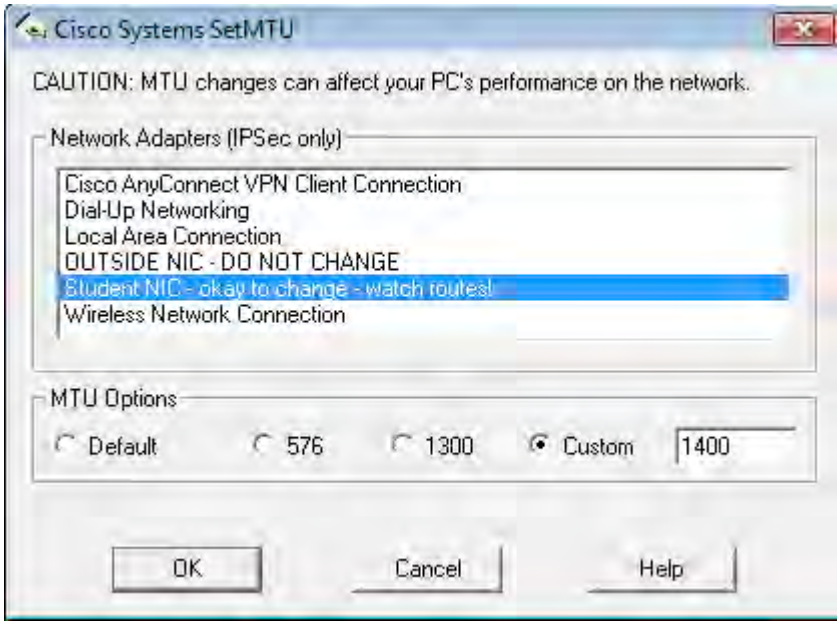
```
ASA3(config)# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : mad                    Index        : 5
Assigned IP  : 10.170.170.1           Public IP    : 8.9.2.200
```

```
Assigned IPv6: 2010:170:170::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 12723                  Bytes Rx     : 170488
Pkts Tx      : 26                     Pkts Rx      : 944
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : SSLPOL                 Tunnel Group : SSLGROUP
Login Time   : 08:53:20 UTC Tue Feb 26 2013
Duration     : 0h:27m:56s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 5.1
  Public IP    : 8.9.2.200
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 2 Minutes
  Client Type  : AnyConnect
  Client Ver   : AnyConnect Windows 2.5.2014
  Bytes Tx     : 11069                  Bytes Rx     : 3141
  Pkts Tx      : 13                     Pkts Rx      : 6
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 5.2
  Assigned IP  : 10.170.170.1           Public IP    : 8.9.2.200
  Assigned IPv6: 2010:170:170::1
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Src Port : 49375
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 3 Minutes
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 2.5.2014
  Bytes Tx     : 854                    Bytes Rx     : 876
  Pkts Tx      : 1                      Pkts Rx      : 11
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

DTLS-Tunnel:
  Tunnel ID    : 5.3
  Assigned IP  : 10.170.170.1           Public IP    : 8.9.2.200
  Assigned IPv6: 2010:170:170::1
```

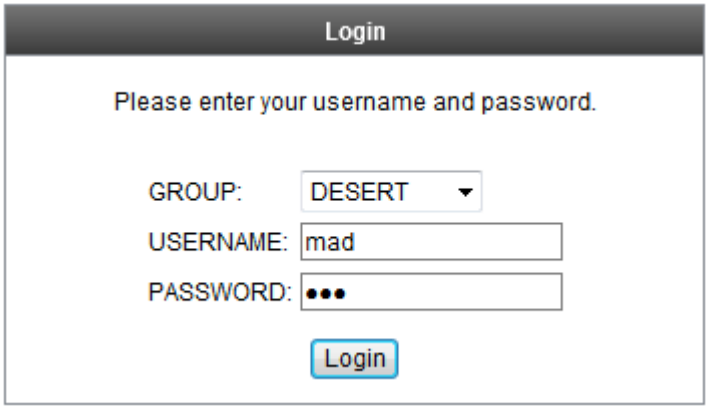
```
  Encryption    : AES128                  Hashing      : SHA1
  Encapsulation: DTLSv1.0                 UDP Src Port : 54175
  UDP Dst Port : 443                      Auth Mode    : userPassword
  Idle Time Out: 30 Minutes               Idle TO Left : 30 Minutes
  Client Type   : DTLS VPN Client
  Client Ver    : AnyConnect Windows 2.5.2014
  Bytes Tx      : 800                     Bytes Rx     : 166633
  Pkts Tx       : 12                      Pkts Rx      : 928
  Pkts Tx Drop : 0                        Pkts Rx Drop : 0

NAC:
  Reval Int (T): 0 Seconds                Reval Left(T): 0 Seconds
  SQ Int (T)    : 0 Seconds               EoU Age(T)   : 1678 Seconds
  Hold Left (T): 0 Seconds                Posture Token:
  Redirect URL :
```

First thing adjust MTU so IPv6 connections could work (minimum MTU supported is 1374B). Use regular VPN Client's "Set MTU" tool – in our case I set it to 1400B:



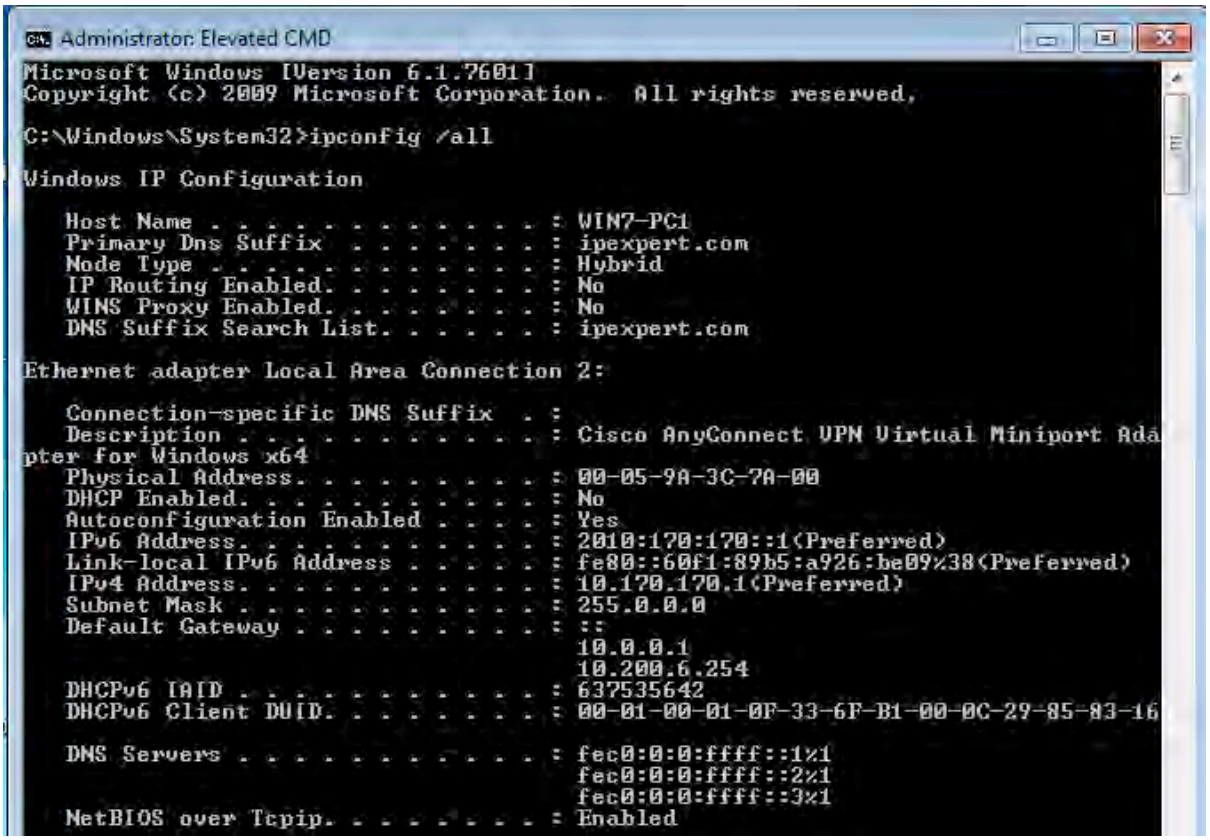


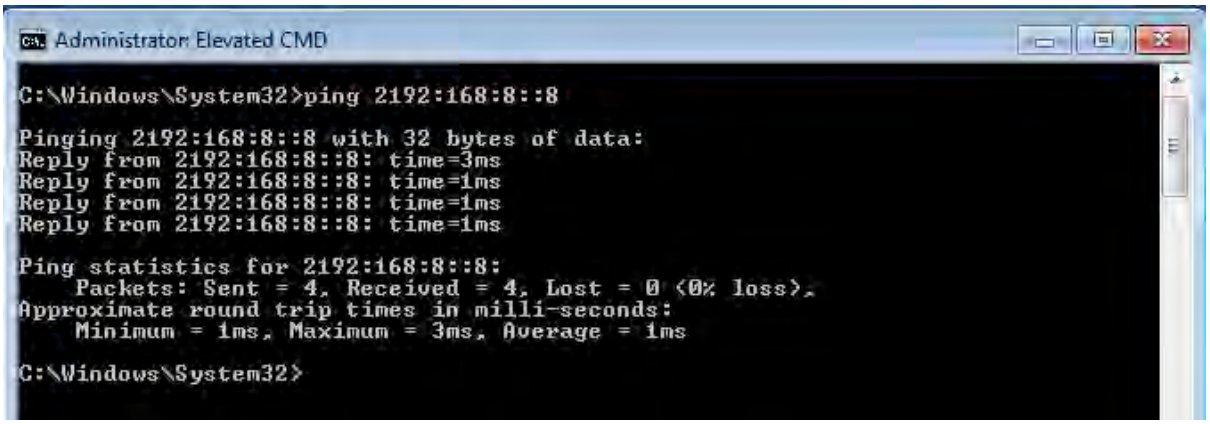
Reboot the PC and navigate to http://8.9.2.30 (test redirection) to download the AnyConnect Client. For this task to test you will need to use VNC as a remote desktop application – RDP is by default not allowed in AnyConnect profile:



You may need to download the client manually; then after installation connect to “8.9.2.30”, select group “DESERT” and authenticate Mad Max.

Do some basic ping tests trying to reach R8 using both versions of IP and check the statistics:





Task 17: IKEv2 L2L IOS ASA

- Configure IKEv2 L2L VPN between R10 and ASA3
- R10 should authenticate using digital certificate. Setup R2 as CA if needed
- ASA3 should authenticate using PSK “ipexpert”
- AES 256 should be used for AUTH SA along with SHA384 hashing and DH Group 14
- IKEv2 Policy should be bound to G0/0 on R10
- IPSec tunnels should be protected by AES 128 encryption and SHA-1 integrity algos
- IKE lifetime on ASA3 should be set to 1 hour and 40 minutes
- PFS should be enabled with a recommended key size
- DPD Keepalives should be enabled with the interval set to 15 seconds. Retries should be sent every 3 seconds
- Enable NAT-Traversal Keepalives
- You are allowed to add two static routes to accomplish this task

BEFORE YOU BEGIN

Unless you started with “fresh” config files, you may want to reload initial configuration on R10, R11 and ASA3 so the crypto components from the previous tasks don’t interfere with IKEv2 configuration.

Detailed Solution

R2

Just in case you are not using CA from the first Task:

```
crypto pki server IOSCA
 grant auto
 cdp-url http://2.2.2.2/cgi-bin/pkiclient.exe?operation=GetCRL
 no sh

ip http server
```

R10

```
ip domain name ipexpert.com
ntp server 2.2.2.2

access-list 120 permit ip 10.100.100.0 0.0.0.255 192.168.8.0 0.0.0.255

crypto pki trustpoint VPNTRUST
 enrollment url http://2.2.2.2:80
 password 7 030752180500701E1D
 subject-name cn=R10.ipexpert.com, ou=INSTRUCTORS, l=San Jose, c=US
 revocation-check crl

crypto pki authen VPNTRUST
crypto pki enro VPNTRUST

crypto ikev2 proposal IKE_PROP
 encryption aes-cbc-256
 integrity sha384
 group 14

crypto ikev2 policy IKE_POL
 match address local 8.9.2.10
 proposal IKE_PROP

crypto ikev2 keyring IKE_KRING
 peer ASA3
  address 8.9.2.30
  pre-shared-key remote ipexpert

crypto ikev2 profile IKE_PROF
 match identity remote address 8.9.2.30 255.255.255.255
 authentication remote pre-share
 authentication local rsa-sig
 keyring local IKE_KRING
 pki trustpoint VPNTRUST
 dpd 15 3 on-demand
 nat keepalive 10
 identity local dn
```

```
crypto ipsec transform-set SET1 esp-aes esp-sha384-hmac

crypto ipsec profile IPSEC_PROF1
 set transform-set SET1
 set pfs group14
 set ikev2-profile IKE_PROF

crypto map MAP1 10 ipsec-isakmp
 set peer 8.9.2.30
 set transform-set SET1
 set pfs group14
 set ikev2-profile IKE_PROF
 match address 120

ip route 192.168.8.0 255.255.255.0 8.9.2.30
```

ASA3

```
domain name ipexpert.com
ntp server 2.2.2.2

crypto ca trustpoint VPNTRUST
 revocation-check crl
 enrollment url http://2.2.2.2:80
 crl configure

crypto ca authenticate VPNTRUST

crypto ikev2 policy 10
 encryption aes-256
 integrity sha384
 group 14
 prf sha384
 lifetime seconds 6000

crypto ipsec ikev2 ipsec-proposal SET2
 protocol esp encryption aes
 protocol esp integrity sha-1

crypto map MAP2 10 match address PROXY6
crypto map MAP2 10 set pfs group14
crypto map MAP2 10 set peer 8.9.2.10
crypto map MAP2 10 set ikev2 ipsec-proposal SET2
crypto map MAP2 interface outside
crypto ikev2 enable outside

crypto isakmp nat-traversal 10

tunnel-group 8.9.2.10 type ipsec-l2l
```

```
tunnel-group 8.9.2.10 ipsec-attributes
 isakmp keepalive threshold 15 retry 3
 ikev2 remote-authentication certificate
 ikev2 local-authentication pre-shared-key ipexpert

access-list PROXY6 extended permit ip 192.168.8.0 255.255.255.0 10.100.100.0
255.255.255.0

route outside 10.100.100.0 255.255.255.0 8.9.2.10
```

NAT Exemption is needed to fix previous configs – if you started with fresh initials you don't need it:

```
object-group network NAT_EXEMPT
 network-object 10.100.100.0 255.255.255.0
```

In general we can say that IKEv2 streamlined the original packet exchanges during Phase I and II operation that were used to create IKE and IPSec Security Associations. Instead of having three or six messages for Phase I and 3 messages being exchanged for the data tunnels, IKEv2 can use as low as just 4 messages (2 exchanges) to create secure connections (though in some scenarios that number may grow). These exchanges are known as:

1. IKE_SA_INIT (old Phase I)
2. IKE_AUTH (old Phase I and II)

IKE_SA_INIT (from Initiator) contains crypto algorithms (the proposal or just SA payload), including Security Protocol and SPI number, nonces and DH information. Reply from the Responder includes selected cipher-suit, SPI, nonces, DH and optionally CERTREQ payload which may indicate CAs the responder finds acceptable for validating certificates used in subsequent exchange. This exchange derives 7 keys used to protect IKE_AUTH exchange and derive further keys for CHILD_SA (each direction of SA uses different keys - that's why so many of them must be computed). At the end of this phase an IKE_SA is built which is required to protect the subsequent exchange.

IKE_AUTH, the second exchange, is already protected by IKE_SA and is used to create the first CHILD_SA (data tunnel). Initiator sends IKE_ID, another SA payload for first CHILD_SA, Traffic Selectors and AUTH payload (that proves its identity). Optionally certificate may be sent and CERTREQ payload that identifies Certificate Authorities the Initiator can use for cert validation. Moreover this exchange may also contain so-called Configuration Payloads (legacy Mode Config; there is no more Phase 1.5). Responder replies with IKE_ID, SA payload, Traffic Selectors, AUTH payload and optionally its CERT (certificate). For Traffic Selectors (Proxy ACL), when one range is smaller than another, the smaller range is selected for use in a process called „narrowing" (they are negotiated as opposed to yes/no in IKEv1). The authentication methods available are Pre-Shared Key, Digital Certificates and EAP (note that when EAP is used for authentication, AUTH payload is skipped and IKE_AUTH exchange stops until EAP finishes its processing).

The first CHILD_SA created in the second exchange is commonly the only SA created for IPsec communication. However, if an application or peer requires the use of additional SAs to secure traffic through an encrypted tunnel, IKEv2 uses the CREATE_CHILD_SA exchange. During the CREATE_CHILD_SA exchange, new Diffie-Hellman values may be generated (similar to PFS) and cryptographic protocols used. This exchange can be also used to rekey an SA.

For a working PKI you must always remember about Time Synchronization. NTP is the best way to do get this work. Also note that since only R10 will be authenticating to the ASA3 with a digital certificate, the firewall does not need an Identity certificate for itself – only the CA's cert is required for validation.

The overall IKEv2 configuration on IOS (along with Tunnel Interfaces known as FlexVPN) should be performed in the following way:

1. Defining IKE Proposal
2. Binding the proposal to the IKE Policy
3. Defining authentication credential store (Keyring or Trustpoint)
4. Creating an IKEv2 Profile that specifies the connection-matching criteria, authentication method to be used (along with the appropriate credential store) and possibly some other options we want to enable

IKEv2 Proposal – a collection of transforms used in the negotiation of IKE_SA. The transform types used in the negotiation are as follows:

- Encryption algorithm
- Integrity algorithm
- Pseudo-Random Function (PRF) algorithm
- Diffie-Hellman (DH) group

The Proposal does not have any priority defined; algorithms will be selected based on the order in configuration.

IKEv2 Policy – contains Proposal(s) that will be used to negotiate a transform responsible for protection of IKE_SA. In other words a similar concept to IKEv1 Policy but with two differences :

1. May have one or more "`match`" statements which are used to select a particular IKEv2 Policy for a peer
2. Authentication method is not negotiated

IKEv2 Policy configuration syntax:

```
crypto ikev2 policy policy_name
 proposal name
 match fvrf [fvrf_name|any]
 match address local address
```

In terms of the "`match`" statements within a policy - if there are multiple of them, as long as they are of the same type they will be logically ORed; if they are of different types they will be ANDed. If you

don't configure any "`match`" criteria, the policy will match all peers but only in the global FVRF (if you want to match all peers in all VRFs you must use match fvrf any). Just in case you want to create multiple policies with overlapping matching criteria – don't do it because only the first policy in the configuration will be selected. Simply put IKEv2 policies should never overlap.

IKEv2 Keyring & Profile will be discussed in later tasks.

IPSec SA parameters are defined in exactly the same way as for IKEv1. Since the recommended method is to use the tunnel interface paradigm (Flex VPNs), a transform set must be defined which is then nested in an IPSec Profile. The Profile goes to the tunnel interface and "`tunnel mode`" is adjusted to be "`ipsec ipv4/ipv6`".

It is still possible to configure IKEv2 connections using legacy crypto maps, as shown in this task, and this is the only method to get the tunnel up and working when e.g. the peer does not support VTIs, such as when the peer is an ASA firewall.

Speaking of phase I parameters not only the encryption/integrity & DH group must match but also the Pseudo Random Function (PRF). It is by default set to the same value as hashing algorithm on IOS (in order), but on the ASA it must be adjusted by using the "`prf`" command.

Same as with IKEv1 whenever digital certificate is validated by the ASA during authentication stage in IKEv2, it may by default complain about the incorrect Peer Identity. This is an additional security check done by the ASA – it tries to compare IKE_ID to the content of the certificate (part of the Subject Name). Since IOS sends FQND or IP address by default (depending on cert settings), it will never match what ASA expects to see. One solution is to set IKE_ID on IOS to be Distinguished Name (DN) or the other one would be to use the "`peer-id-validate`" command along with "`cert`" or "`nocheck`" options to make this check optional/disable it.

IPv6 Considerations

On IOS it is possible to implement VPNs running on IPv6 using static crypto maps (dynamic ones are not supported with IPv6) or tunnel interfaces (VTIs). Crypto map support is platform and code version dependent (`crypto map ipv6 map_name`; applied to the interface via `ipv6 crypto map`). Just remember that all address information would then also have to be IPv6 (address on the interface, peer's address, Proxy ACL etc.) – there is no way to protect IPv4 packets using IPv6 for transport.

The other way (widely supported) would be to use tunnel interfaces (SVTIs) with tunnel mode set to "`ipsec ipv6`".

IPv6 on the ASA is implemented using regular Crypto Maps. Just make sure to use appropriate addresses in the Crypto Map and Proxy Access-list. There is also an option to select an IPv6 address for the connection for situations where you have multiple addresses configured on a port. Use the "`ipv6-local-address`" keyword when applying a crypto map to the interface.

Verification

Few basic verifications and we can start to bring up the tunnel:

```
R10#sh cry ikev2 proposal
 IKEv2 proposal: IKE_PROP
      Encryption : AES-CBC-256
      Integrity  : SHA384
      PRF        : SHA384
      DH Group   : DH_GROUP_2048_MODP/Group 14

R10#do sh cry ikev2 policy

 IKEv2 policy : IKE_POL
       Match fvrf  : global
       Match address local : 8.9.2.10
       Proposal    : IKE_PROP

R10#show cry ikev2 profile

IKEv2 profile: IKE_PROF
 Ref Count: 3
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   address 8.9.2.30 255.255.255.255
  Certificate maps: none
 Local identity: DN
 Remote identity: none
 Local authentication method: rsa-sig
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: IKE_KRING
 Trustpoint(s):
  VPNTRUST
 Lifetime: 86400 seconds
 DPD: interval 15, retry-interval 3, on-demand
 NAT-keepalive: 10 seconds
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none

R10#do sh cry ipse profile
IPSEC profile IPSEC_PROF1
```

```
        IKEV2 profile IKE_PROF
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group14
        Transform sets={
                SET1:  { esp-aes esp-sha-hmac  } ,


R8#ping 10.100.100.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.100.10, timeout is 2 seconds:
.!!!!
```

My favorite "`show crypto session`" statement will always show you all SAs – no matter what version of IKE was used for negotiation and what was the transport protocol:

```
R10#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:06:49
Session status: UP-ACTIVE
Peer: 8.9.2.30 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 8.9.2.30
      Desc: (none)
  IKEv2 SA: local 8.9.2.10/500 remote 8.9.2.30/500 Active
          Capabilities:(none) connid:1 lifetime:23:53:11
  IPSEC FLOW: permit ip 10.100.100.0/255.255.255.0 192.168.8.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4190701/3191
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4190701/3191
```

The "`show crypto ikev2 session detailed`" command can be used to see the details regarding IKEv2 including Child SAs ("`show crypto ikev2 sa detail`" shows information about only IKE SA). Note DPD is configured and NAT-T was not detected:

```
R10#sh cry ikev2 session detailed
 IPv4 Crypto IKEv2 Session

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
```

```
1          8.9.2.10/500          8.9.2.30/500          none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA384, DH Grp:14, Auth sign: RSA, Auth
verify: PSK
      Life/Active Time: 86400/363 sec
      CE id: 1038, Session-id: 4
      Status Description: Negotiation done
      Local spi: 4C5151B9BFD508CE       Remote spi: 6FE91FA6BD306C35
      Local id: hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San
Jose,c=US
      Remote id: 8.9.2.30
      Local req msg id:  1              Remote req msg id:  17
      Local next msg id: 1              Remote next msg id: 17
      Local req queued:  1              Remote req queued:  17
      Local window:      5              Remote window:      1
      DPD configured for 15 seconds, retry 3
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
Child sa: local selector  10.100.100.0/0 - 10.100.100.255/65535
          remote selector 192.168.8.0/0 - 192.168.8.255/65535
          ESP spi in/out: 0x1868E0B7/0xA26BE5E6
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

 IPv6 Crypto IKEv2 Session
```

ASA's "`show crypto ikev2 sa detail`" is an equivalent of "`show crypto ikev2 session detail`" on IOS. Note that output of these two commands is unified between IOS and ASA which makes verification easier:

```
ASA3(config)# sh cry ikev2 sa detail

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status          Role
 13872365          8.9.2.30/500          8.9.2.10/500      READY     INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA384, DH Grp:14, Auth sign: PSK, Auth
verify: RSA
      Life/Active Time: 6000/443 sec
      Session-id: 4
      Status Description: Negotiation done
      Local spi: 6FE91FA6BD306C35       Remote spi: 4C5151B9BFD508CE
      Local id: 8.9.2.30
```

```
      Remote id: hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San
Jose,c=US
      Local req mess id: 21             Remote req mess id: 1
      Local next mess id: 21            Remote next mess id: 1
      Local req queued: 21              Remote req queued: 1
      Local window: 1                   Remote window: 5
      DPD configured for 15 seconds, retry 3
      NAT-T is not detected
Child sa: local selector  192.168.8.0/0 - 192.168.8.255/65535
          remote selector 10.100.100.0/0 - 10.100.100.255/65535
          ESP spi in/out: 0xa26be5e6/0x1868e0b7
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel


ASA3(config)# sh vpn-sessiondb detail l2l

Session Type: LAN-to-LAN Detailed

Connection    : 8.9.2.10
Index         : 9                     IP Addr      : 8.9.2.10
Protocol      : IKEv2 IPsec
Encryption    : AES256 AES128         Hashing      : SHA384 SHA1
Bytes Tx      : 400                   Bytes Rx     : 400
Login Time    : 01:26:12 UTC Wed Feb 27 2013
Duration      : 0h:09m:56s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 9.1
  UDP Src Port : 500                   UDP Dst Port : 500
  Rem Auth Mode: rsaCertificate
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                Hashing      : SHA384
  Rekey Int (T): 6000 Seconds          Rekey Left(T): 5405 Seconds
  PRF          : SHA384                D/H Group    : 14
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 9.2
  Local Addr   : 192.168.8.0/255.255.255.0/0/0
  Remote Addr  : 10.100.100.0/255.255.255.0/0/0
  Encryption   : AES128                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 14
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28205 Seconds
```

```
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 20 Minutes
  Bytes Tx     : 400                    Bytes Rx     : 400
  Pkts Tx      : 4                      Pkts Rx      : 4

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 598 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

R10 authenticates using digital certificate. Even that ASA's "`show crypto ca cert`" does not allow to check the certificate details (this is CA's cert):

```
ASA3(config)# sh cry ca cert
CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: MD5 with RSA Encryption
  Issuer Name:
    cn=IOSCA
  Subject Name:
    cn=IOSCA
  Validity Date:
    start date: 13:18:28 UTC Feb 23 2013
    end   date: 13:18:28 UTC Feb 23 2016
  Associated Trustpoints: VPNTRUST
```

We can still verify CRL was downloaded (and by using what method) by issuing "`show crypto ca crl`":

```
ASA3(config)# sh crypto ca crl

CRL Issuer Name:
    cn=IOSCA
    LastUpdate: 01:13:47 UTC Feb 27 2013
    NextUpdate: 07:13:47 UTC Feb 27 2013
    Cached Until: 02:16:25 UTC Feb 27 2013
    Retrieved from CRL Distribution Point:
      http://2.2.2.2/cgi-bin/pkiclient.exe?operation=GetCRL
    Size (bytes): 215
    Last used at: 01:26:13 UTC Feb 27 2013
    Associated Trustpoints: VPNTRUST
```

NAT Keepalives are NOT sent because NAT was not detected in transit. DPDs are being exchanged, however:

```
ASA3(config)# sh cry ikev2 stat

Global IKEv2 Statistics
  Active Tunnels:                            1
  Previous Tunnels:                          3
  In Octets:                             15760
  In Packets:                               41
  In Drop Packets:                           0
  In Drop Fragments:                         0
  In Notifys:                               61
  In P2 Exchange:                           20
  In P2 Exchange Invalids:                   0
  In P2 Exchange Rejects:                    0
  In IPSEC Delete:                           3
  In IKE Delete:                             3
  Out Octets:                             7827
  Out Packets:                              41
  Out Drop Packets:                          0
  Out Drop Fragments:                        0
  Out Notifys:                              34
  Out P2 Exchange:                          20
  Out P2 Exchange Invalids:                  0
  Out P2 Exchange Rejects:                   0
  Out IPSEC Delete:                          0
  Out IKE Delete:                            0
  SAs Locally Initiated:                     1
  SAs Locally Initiated Failed:              0
  SAs Remotely Initiated:                    7
  SAs Remotely Initiated Failed:             9
  System Capacity Failures:                  0
  Authentication Failures:                   4
  Decrypt Failures:                          0
  Hash Failures:                             0
  Invalid SPI:                               0
  In Configs:                                0
  Out Configs:                               0
  In Configs Rejects:                        0
  Out Configs Rejects:                       0
  Previous Tunnels:                          3
  Previous Tunnels Wraps:                    0
  In DPD Messages:                          14
  Out DPD Messages:                         14
  Out NAT Keepalives:                        0
  IKE Rekey Locally Initiated:               0
  IKE Rekey Remotely Initiated:              0
  CHILD Rekey Locally Initiated:             0
```

```
  CHILD Rekey Remotely Initiated:          0
```

Task 18: IKEv2 Remote Access IPSec ASA (AnyConnect)

- Configure IKEv2 Remote Access IPSec VPN with ASA3
- AnyConnect should be the client used to test this configuration
- ASA should authenticate to the client using certificates
- Client should authenticate with user “total” and password “recall”
- Use IP pool 10.210.210.0/24
- DNS server should be set to 192.168.8.8
- Clients should be only able to access 192.168.8.0/24 (VLAN 8)

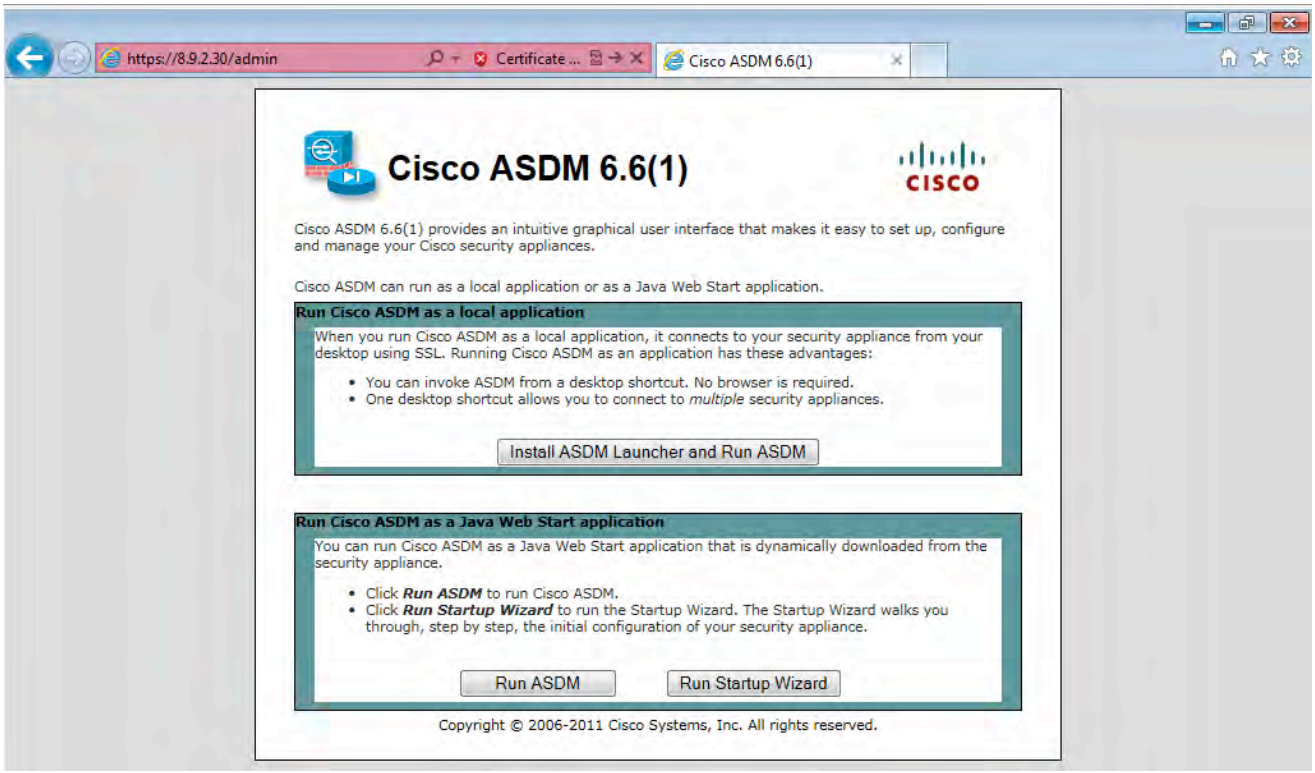
Detailed Solution

ASA3

```
http server enable
http 0.0.0.0 0.0.0.0 outside
asdm image disk0:/asdm-66114.bin

aaa authentication http console LOCAL

username ipexpert pass ipexpert priv 15

cry key gen rsa mod 1024

crypto ca trustpoint VPNTRUST
 revocation-check crl
 enrollment url http://2.2.2.2:80
 crl configure

crypto ca auth VPNTRUST
crypto ca enroll VPNTRUST

crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5
 prf sha
 lifetime seconds 86400

ip local pool ANYPOOL 10.210.210.1-10.210.210.20 mask 255.255.255.0

object-group network NAT_EXEMPT
 network-object 10.210.210.0 255.255.255.0

webvpn
 anyconnect image disk0:/anyconnect-win-3.0.10057-k9.pkg 1
 anyconnect enable
```

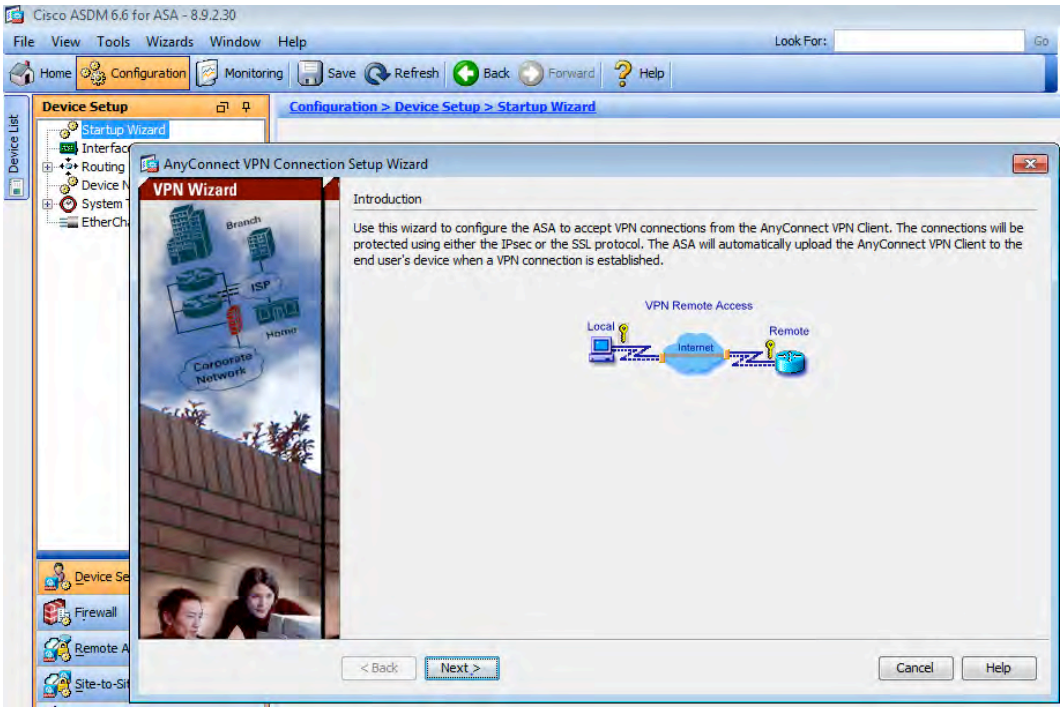
```
enable outside
```

Connect to ASA (https://8.9.2.30/admin) to use ASDM:

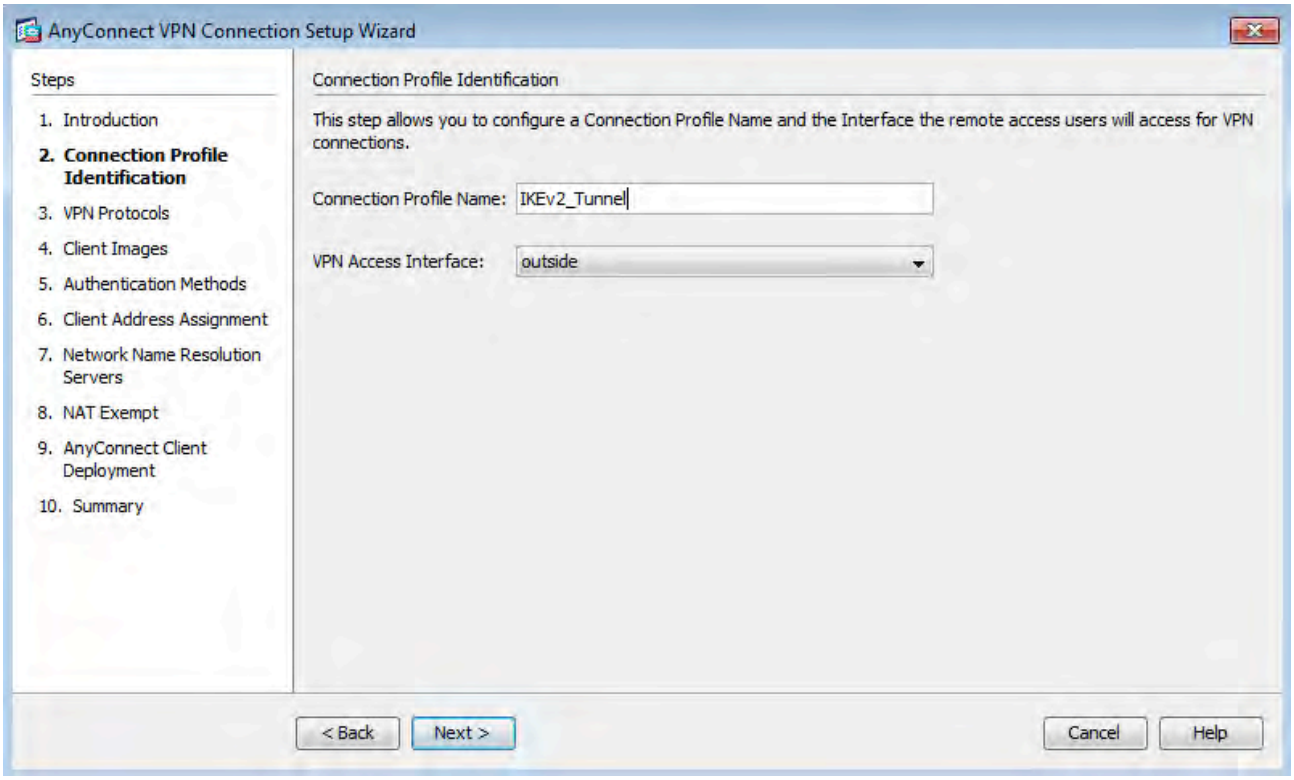


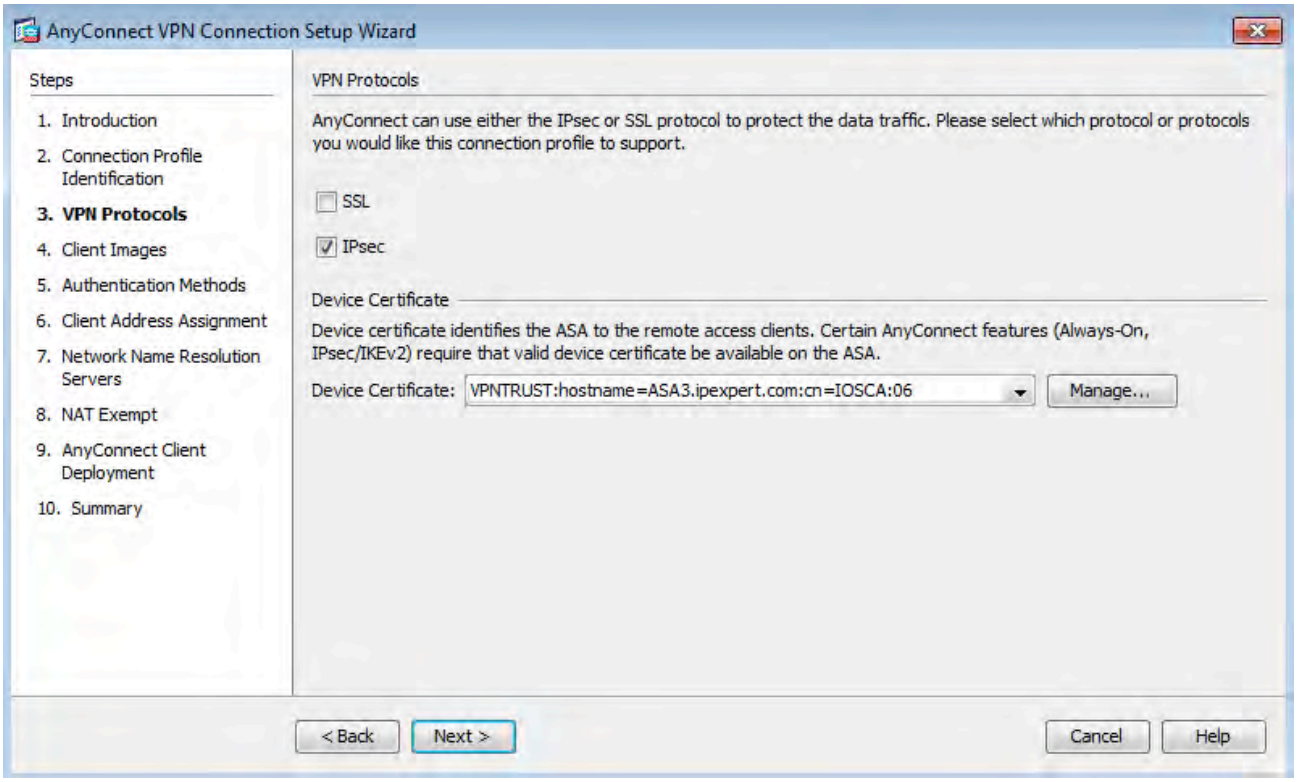
Login as ipexpert//ipexpert:

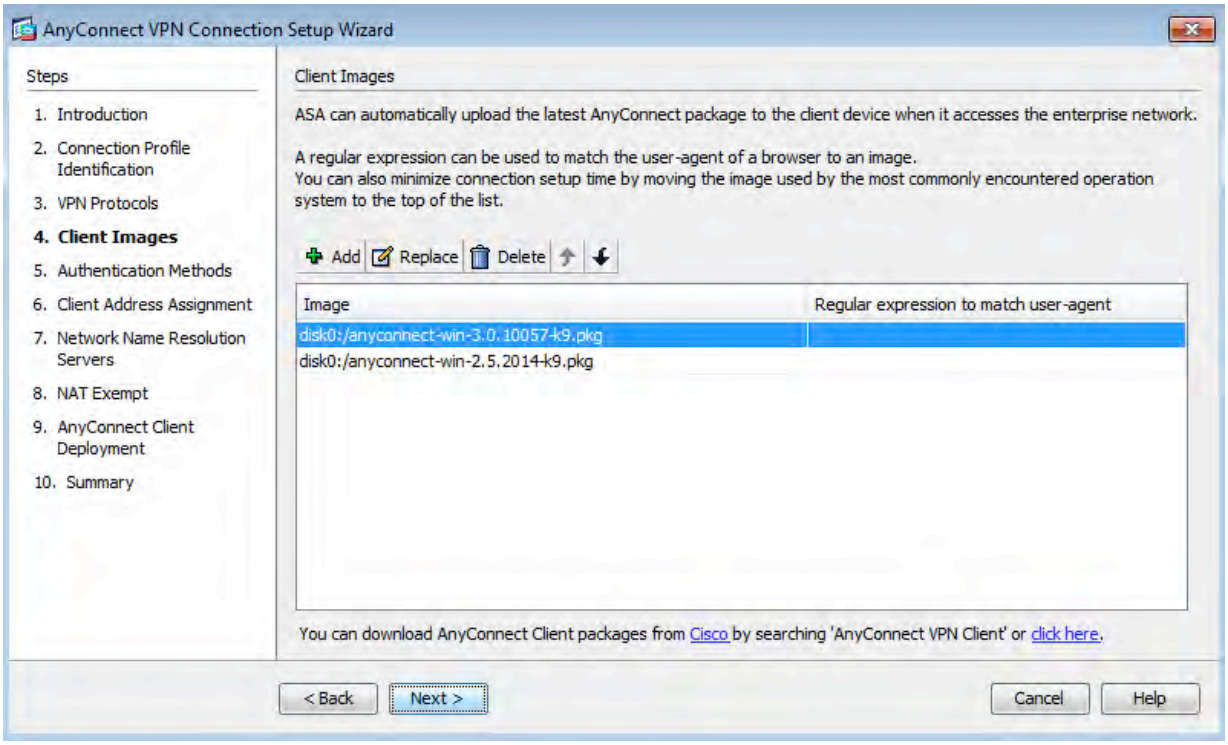
Open up VPN Wizard (Click on “Wizards”), then AnyConnect:

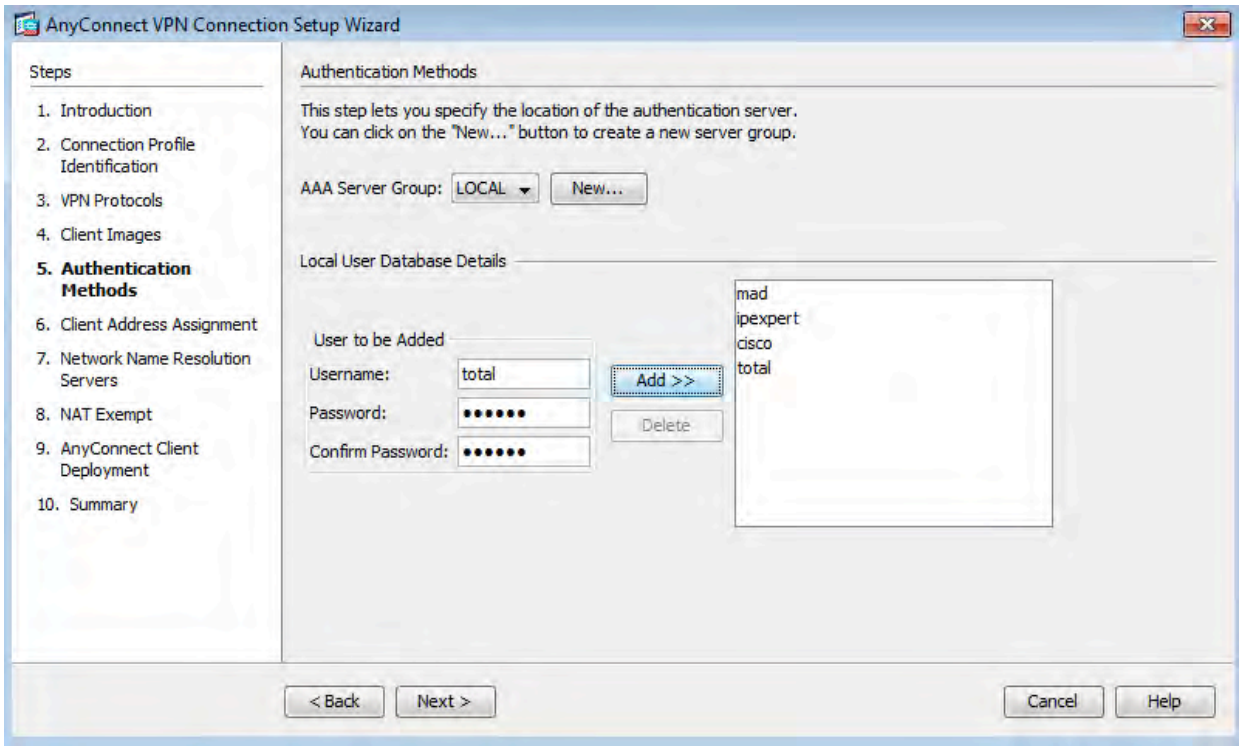


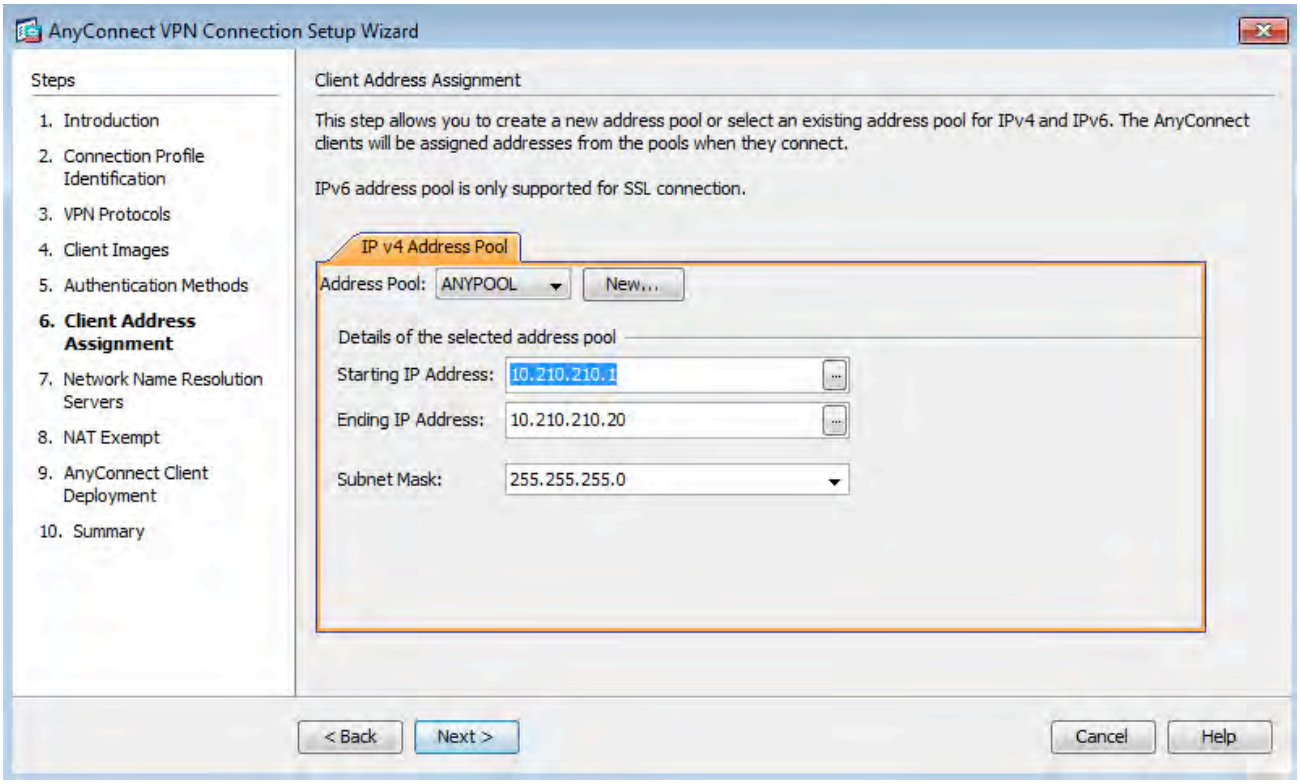
Follow the screenshots. Note the name of the Tunnel Profile is “IKEv2_Tunnel”:

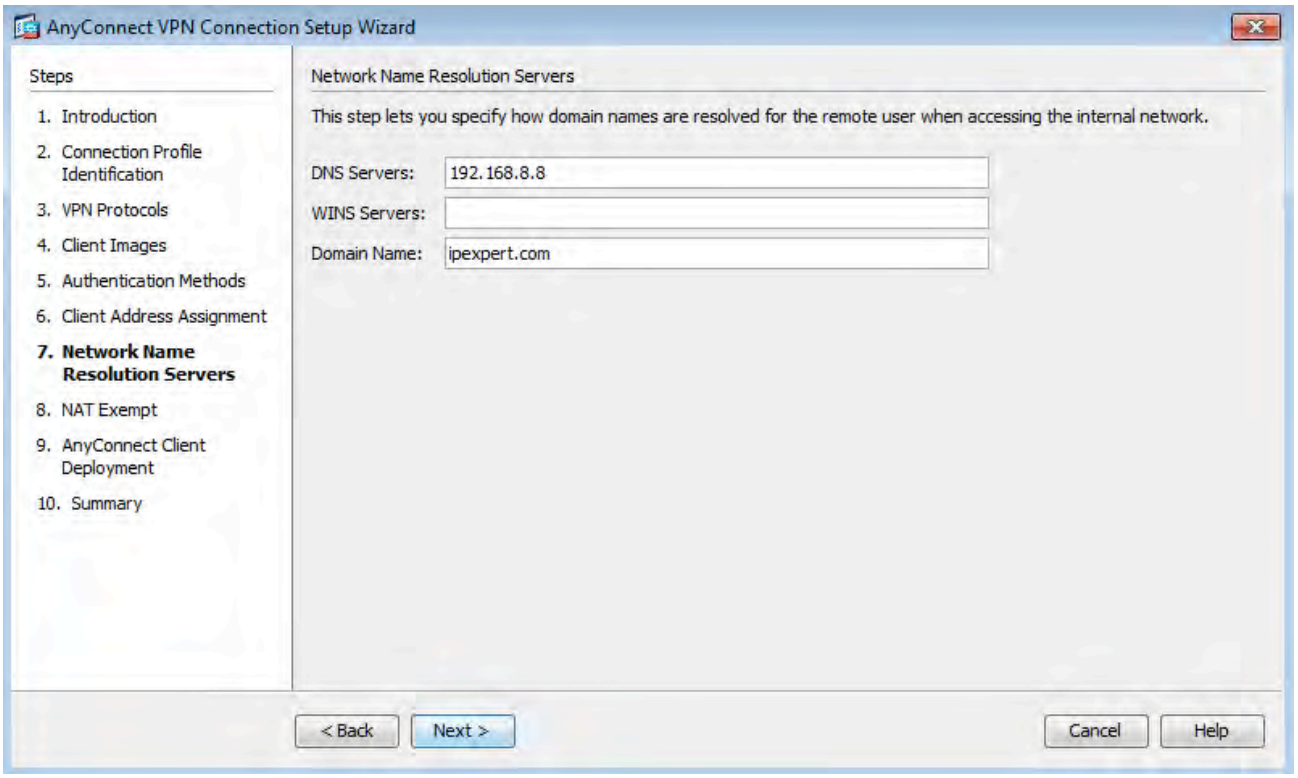


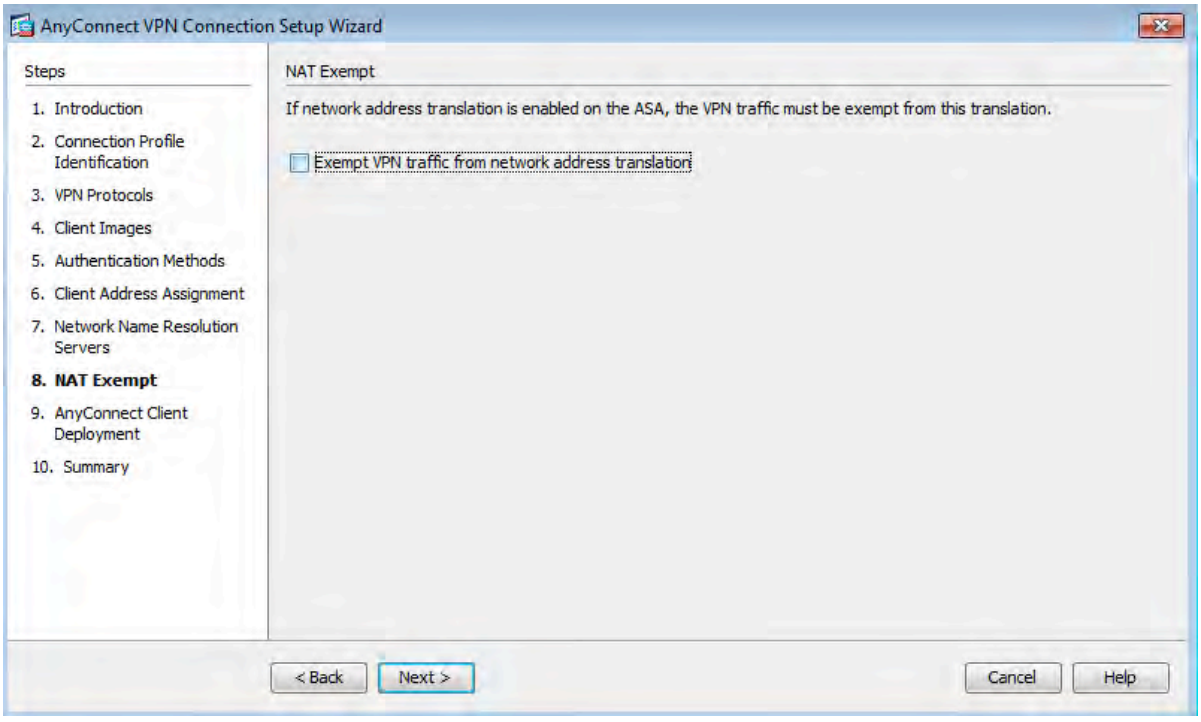




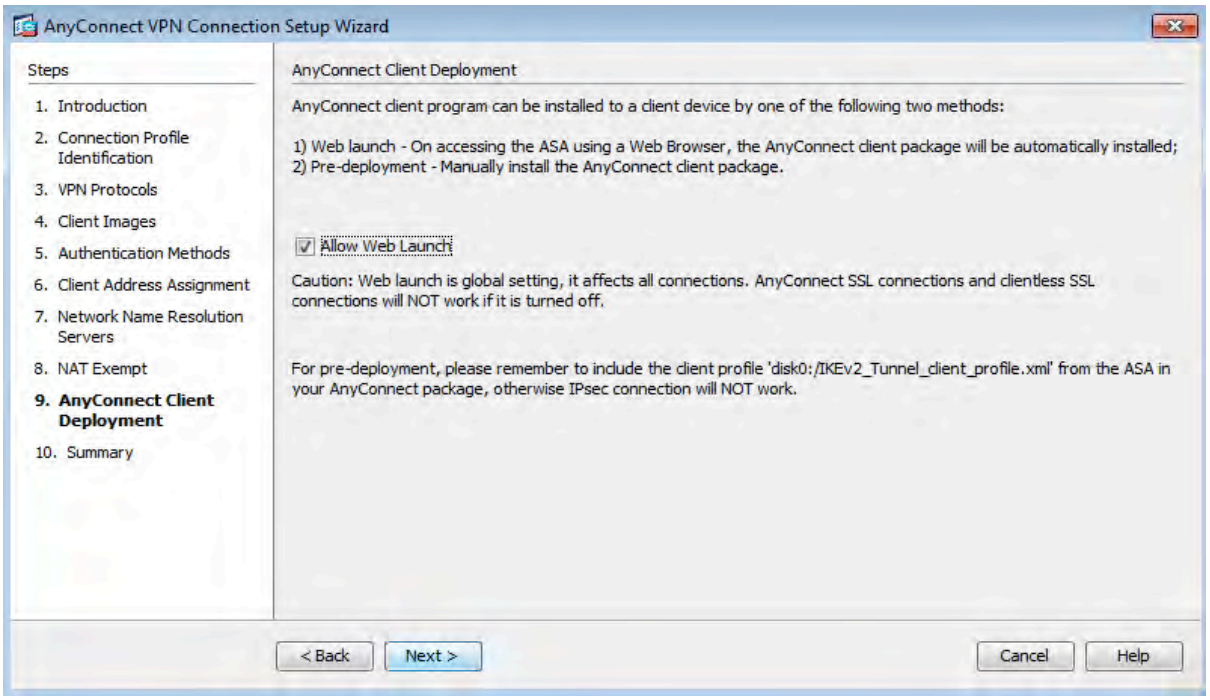


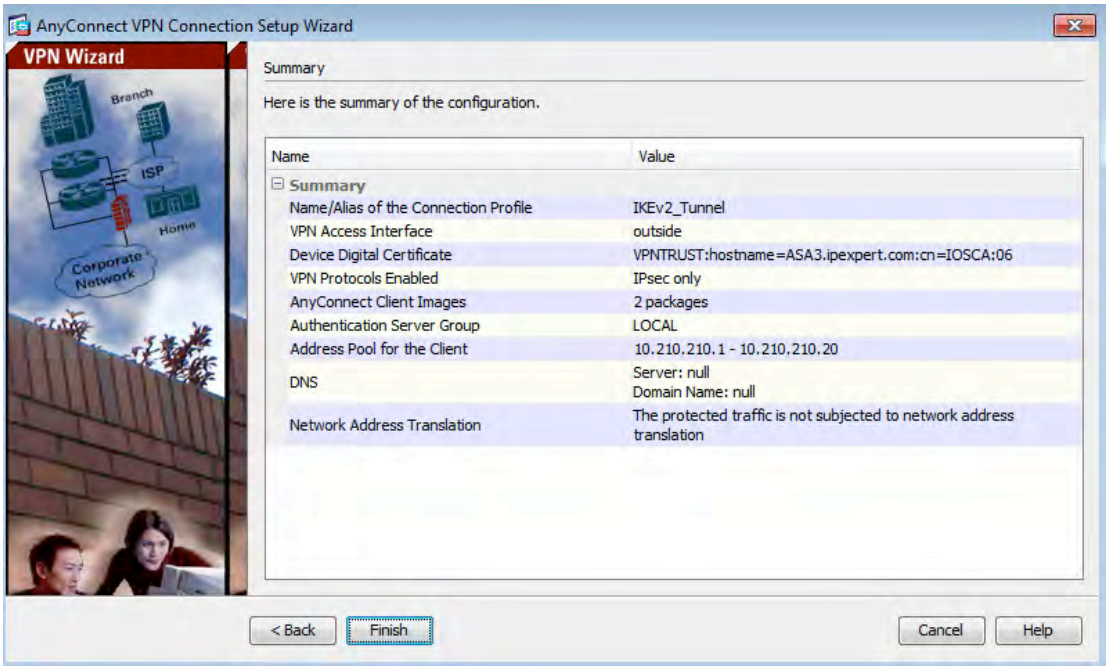




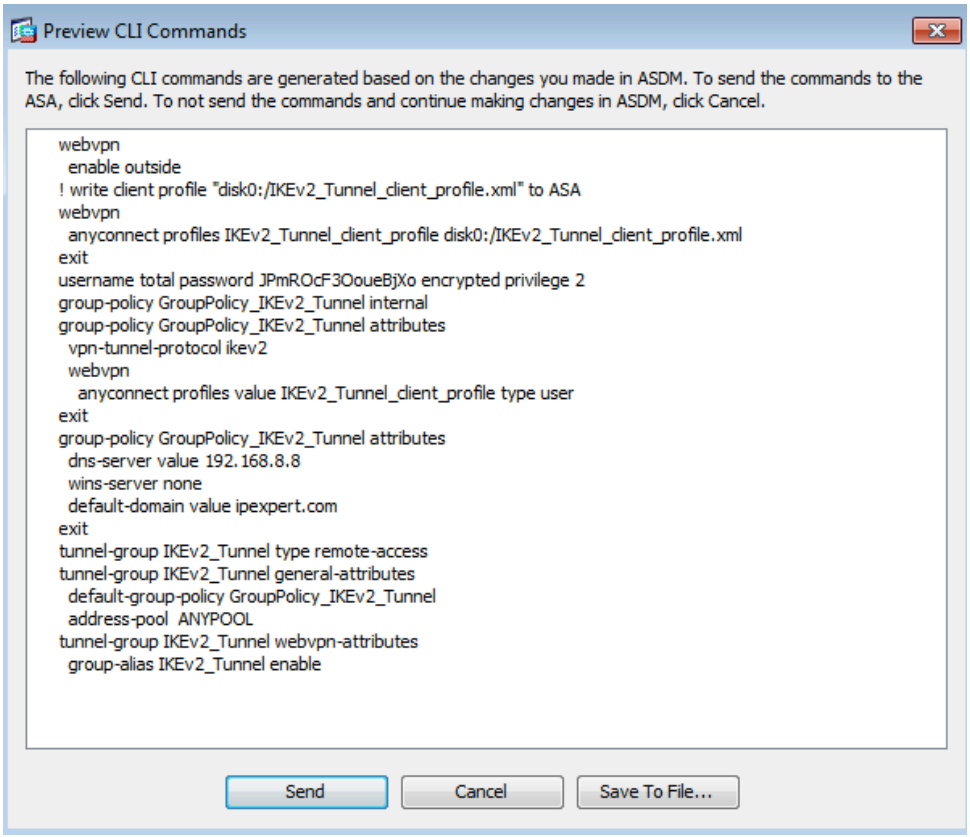


Web Launch allows to download the client via a browser. If you check it off, you will be only able to connect when the client is already pre-installed on the PC:





And the CLI config Summary (if you enabled the “Preview” option – not shown here):



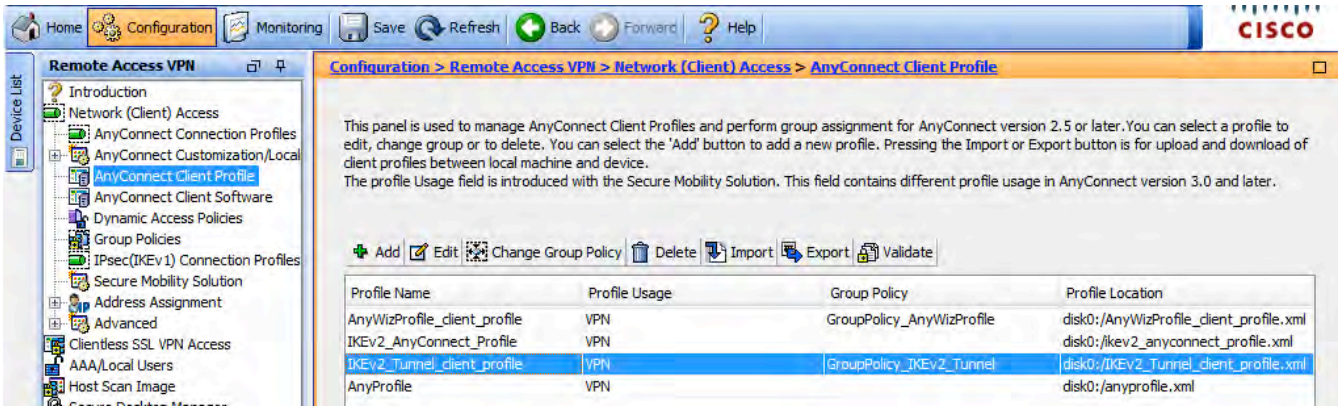
Now for the remaining configuration we can do it either from ASDM or using CLI - I used to prefer the Command Line. We need to figure out what is the Group Policy name so we can configure Split Tunneling (this is shown on the preview but just in case you did not have it enabled):

```
ASA3(config)# sh run tunnel-group IKEv2_Tunnel
tunnel-group IKEv2_Tunnel type remote-access
tunnel-group IKEv2_Tunnel general-attributes
 address-pool ANYPOOL
 default-group-policy GroupPolicy_IKEv2_Tunnel
tunnel-group IKEv2_Tunnel webvpn-attributes
 group-alias IKEv2_Tunnel enable
```

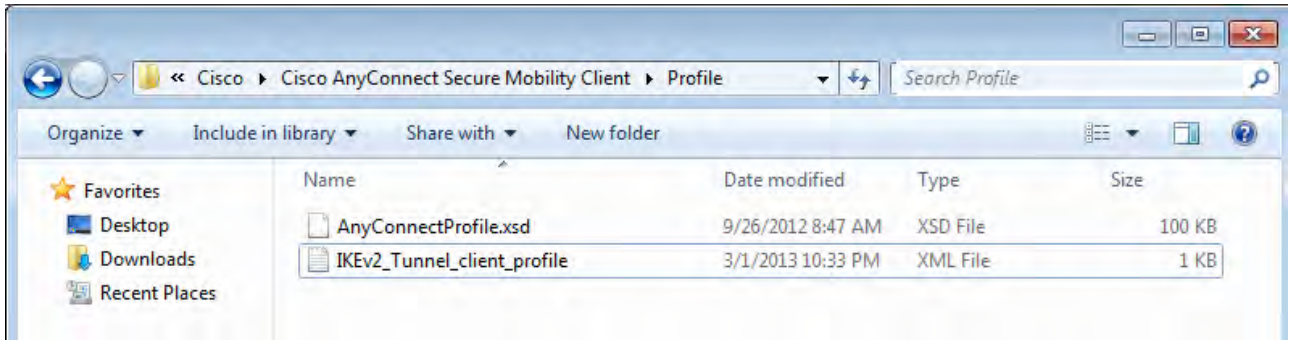
OK, let's configure Split Tunneling:

```
access-list ANYSPLIT standard permit 192.168.8.0 255.255.255.0

group-policy GroupPolicy_IKEv2_Tunnel attributes
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value ANYSPLIT
```

Now the last element is to export ("Export") the Wizard-generated AnyConnect Profile to the Test PC and upload it to the Profile directory:

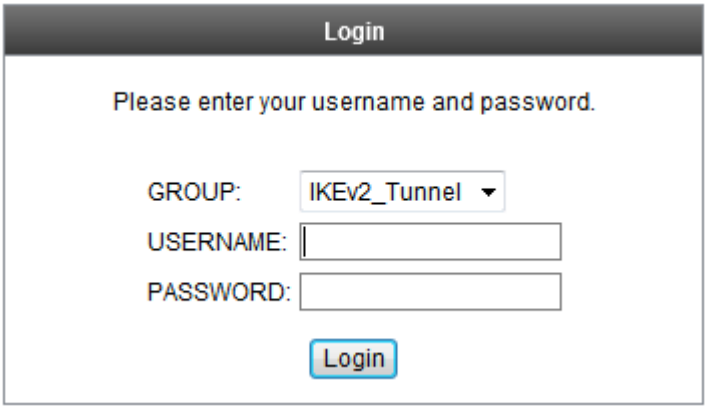


Put the file into "%PROGRAMDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile". To figure out where the .xml Profile file should be placed use the AnyConnect Configuratin Guide. Open up "Cisco AnyConnect Secure Mobility Client Administrator Guide 3.0" and navigate to : "Deploying the AnyConnect Secure Mobility Client " -> "Locations to Deploy the AnyConnect Profiles"



Once the file is placed in the appropriate location you should restart the AnyConnect Client.

The other option would be to connect via a browser and download the client along with Profile (we have enabled Web Launch):



The Cisco AnyConnect Secure Mobility Client provides secure SSL and IPsec/IKEv2 connections to the ASA for remote users. Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept SSL or IPsec/IKEv2 VPN connections. Unless the ASA is configured to redirect http:// requests to https://, users must enter the URL in the form **Error! Hyperlink reference not valid.**>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the ASA identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL or IPsec/IKEv2 connection and either remains or uninstalls itself (depending on the configuration) when the connection terminates.

To enable Cisco AnyConnect Secure Mobility client features you need to use so-called AnyConnect Profiles which are just XML files that store configuration settings for the VPN connection and for the optional client modules - Network Access Manager, Posture, Telemetry, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates.

You can configure a profile using the AnyConnect Profile Editor, a convenient GUI-based configuration tool launched from ASDM. The AnyConnect software package for Windows, version 2.5 and later, includes the editor, which activates when you load the AnyConnect package on the ASA and specify it as an AnyConnect client image.

There is also what's known as a Standalone Profile Editor for Windows that you can use as an alternative to the Profile Editor integrated with ASDM. If you are predeploying the client, you can use the Standalone Profile Editor to create profiles for the VPN service and other modules that you can then deploy to client stations.

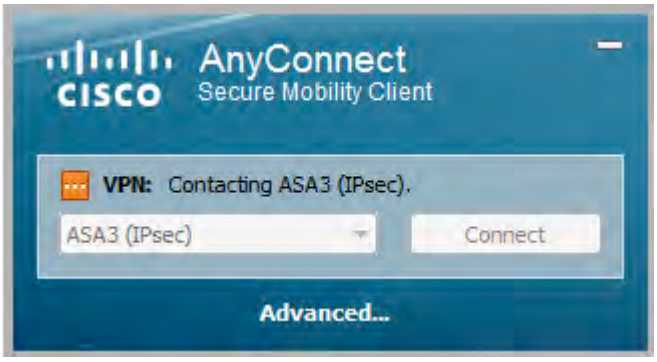
In our case I used a mixed approach to the configuration – some preparations were done using CLI (preparing ASA for ASDM, creating IKEv2 Policy to specify a DH group AnyConnect is capable handling – 5) and then the AnyConnect part along with Profile generation was done using ASDM. At the end Split Tunneling list was configured using CLI as well. This is probably the most efficient way of configuring Remote Access AnyConnect VPNs with the ASA.

IPv6 Considerations

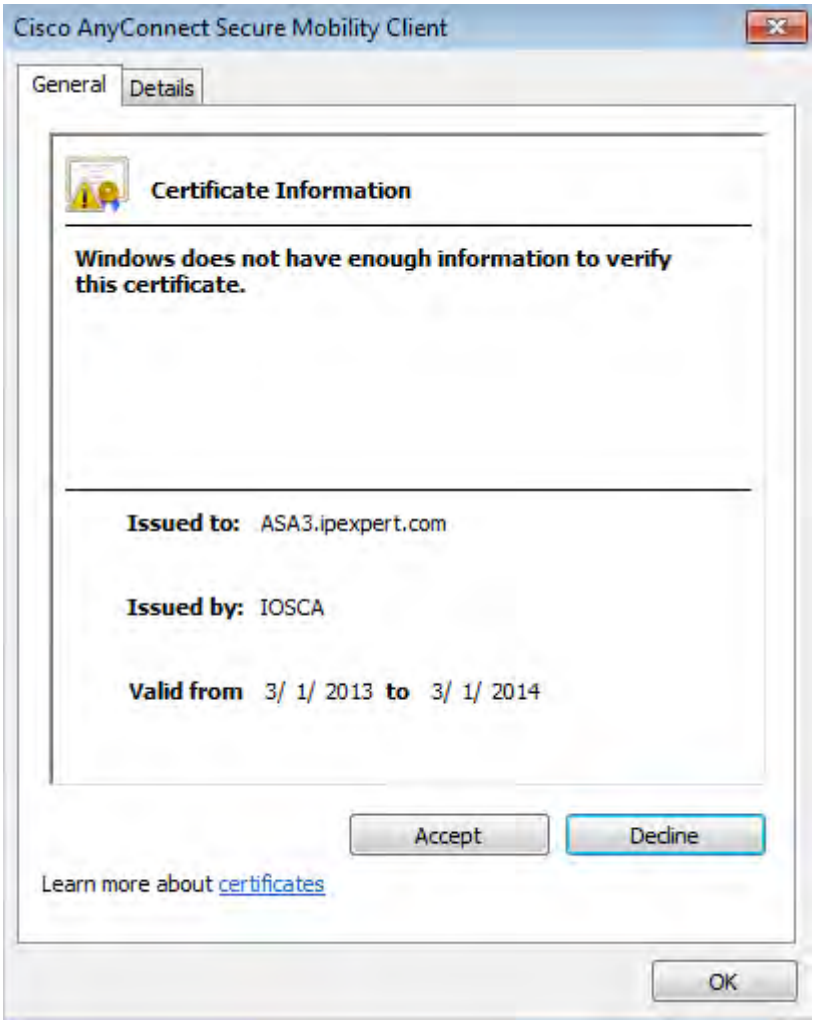
The ASA does not support IPv6 over IKEv2 Remote Access VPN sessions. Only IKEv1 is supported with AnyConnect.

Verification

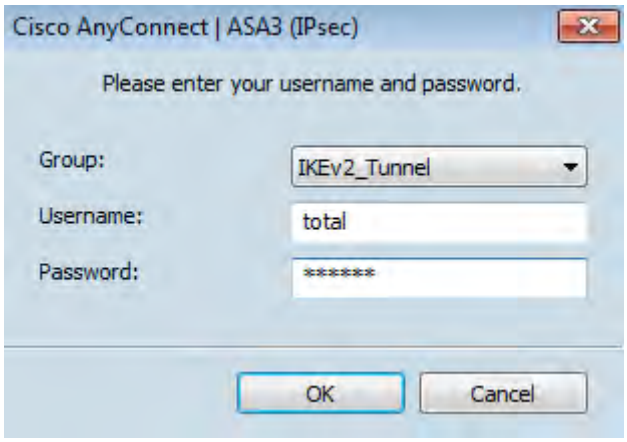
Open AnyConnect and connect to the Profile-created Server :



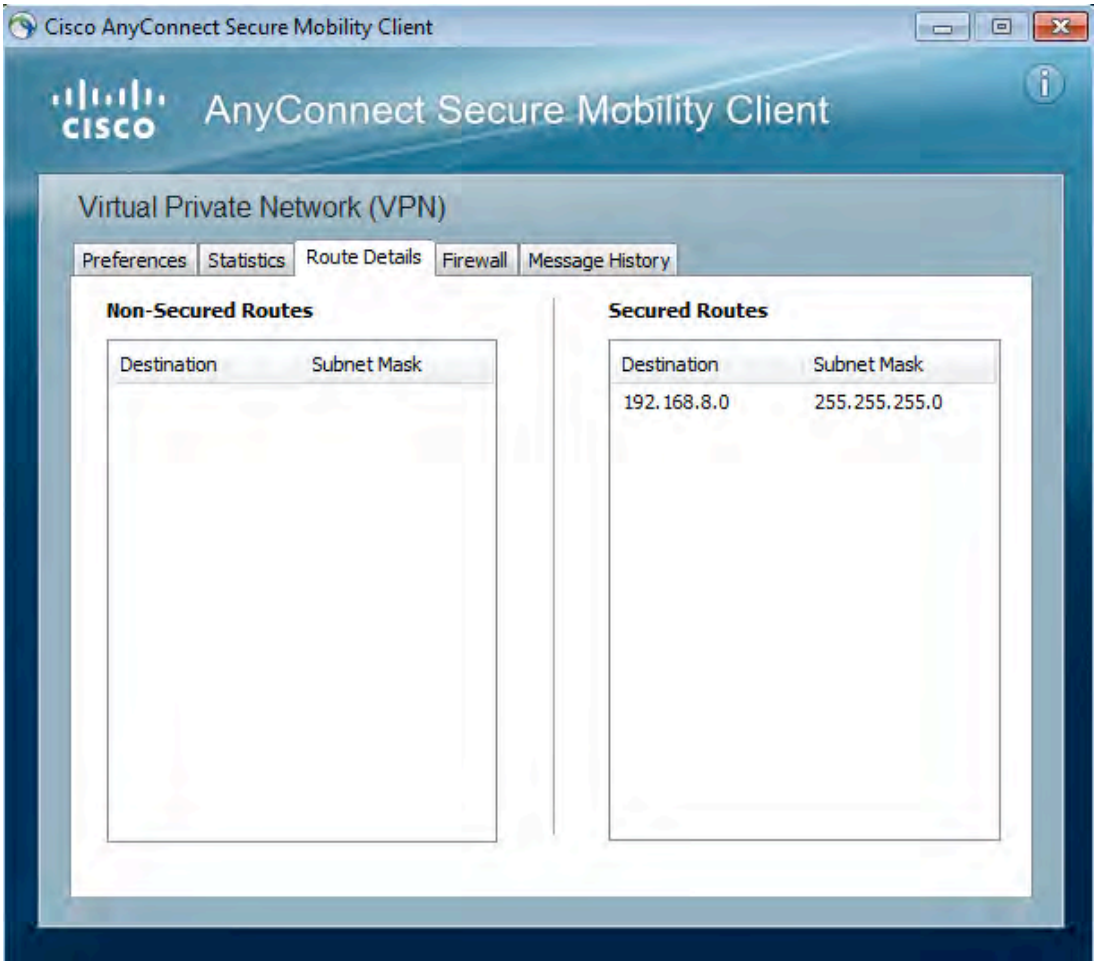
Accept the certificate:



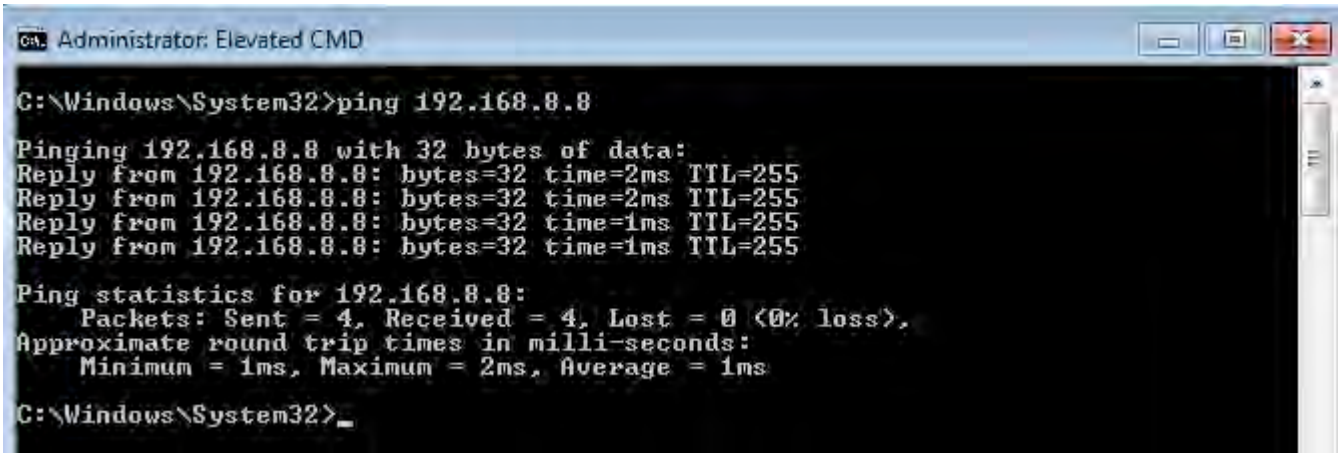
And authenticate:



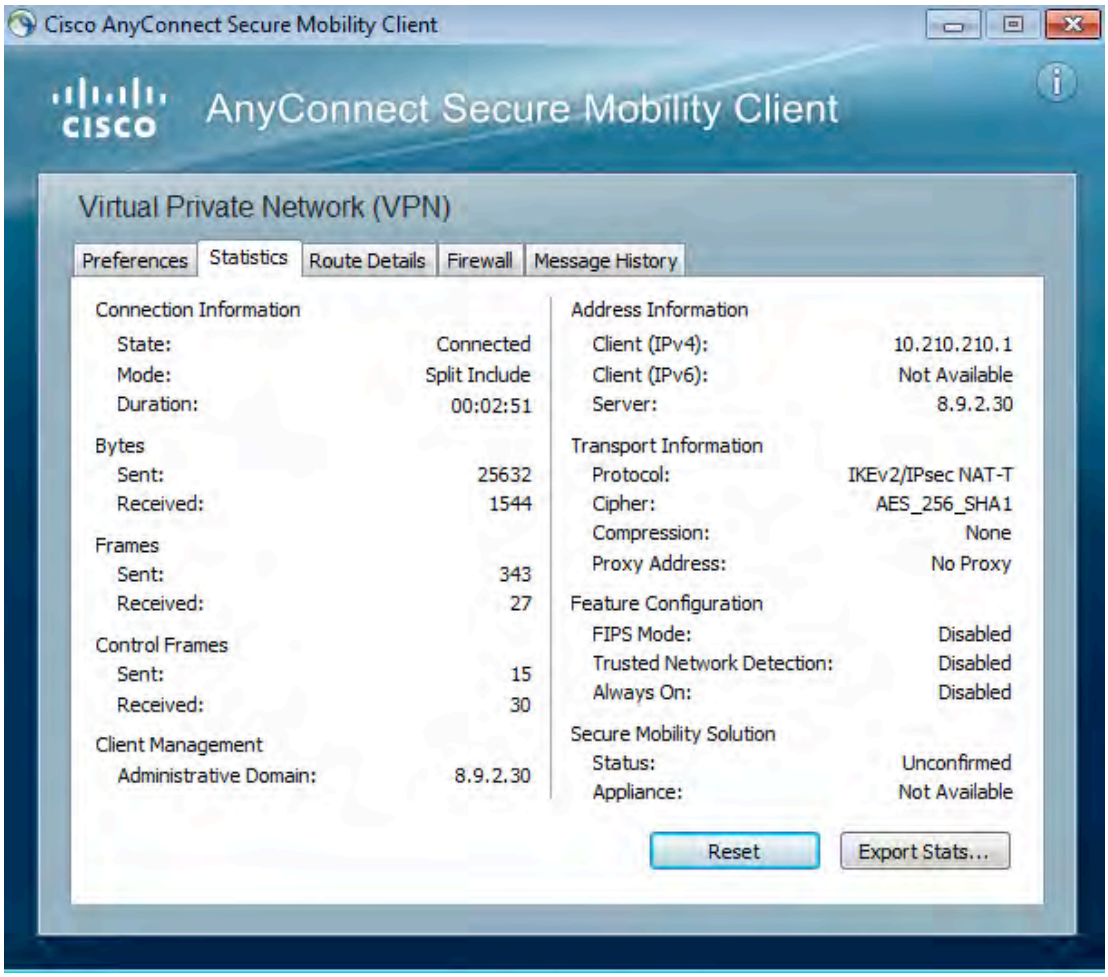
Let's take a look at Split Tunneling Policy:



Let's do a quick ping test:



All's good:



Finally some CLI verifications:

```
ASA3(config)# sh cry ikev2 sa detail

IKEv2 SAs:

Session-id:8, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote      Status          Role
 19475249         8.9.2.30/4500       8.9.2.201/57510       READY     RESPONDER
      Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5, Auth sign: RSA, Auth
verify: EAP
      Life/Active Time: 86400/1681 sec
      Session-id: 8
      Status Description: Negotiation done
      Local spi: 9027EECD423D3157       Remote spi: BB24EA125FD8A3AC
      Local id: hostname=ASA3.ipexpert.com
      Remote id: *$AnyConnectClient$*
      Local req mess id: 17             Remote req mess id: 22
      Local next mess id: 17            Remote next mess id: 22
```

```
      Local req queued: 17              Remote req queued: 22
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 10.210.210.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.210.210.1/0 - 10.210.210.1/65535
          ESP spi in/out: 0x81dbe30/0xbd0b8b7d
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel


ASA3(config)# sh route | in 10.210
S     10.210.210.1 255.255.255.255 [1/0] via 8.9.2.201, outside


ASA3(config)# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : total                  Index        : 22
Assigned IP  : 10.210.210.1           Public IP    : 8.9.2.201
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES128 AES256          Hashing      : none SHA1
Bytes Tx     : 8376                   Bytes Rx     : 43440
Pkts Tx      : 149                    Pkts Rx      : 591
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEv2_Tunnel
Tunnel Group : IKEv2_Tunnel
Login Time   : 03:48:16 UTC Sat Mar 2 2013
Duration     : 0h:06m:37s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 22.1
  Public IP    : 8.9.2.201
  Encryption   : none                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 23 Minutes
  Client Type  : AnyConnect
  Client Ver   : 3.0.10057
```

```
IKEv2:
  Tunnel ID    : 22.2
  UDP Src Port : 57510                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES128                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86001 Seconds
  PRF          : SHA1                   D/H Group    : 5
  Filter Name  :
  Client OS    : Windows

IPsecOverNatT:
  Tunnel ID    : 22.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 10.210.210.1/255.255.255.255/0/0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28401 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607958 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 8376                   Bytes Rx     : 43440
  Pkts Tx      : 149                    Pkts Rx      : 591

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 401 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Task 19: IPv6 FlexVPN L2L

- Configure IKEv2 L2L VPN between R10 and R11
- Protect IPv6 traffic between 2010:10:10::/64 and 2010:114:114::/64
- Use Smart Defaults for this configuration
- R10 should authenticate using PSK “Warsaw”
- R11 should authenticate using PSK “SanFrancisco”
- Devices should be identifying themselves as “R10_ID” (R10) and “R11_ID” (R11)

Detailed Solution

R10

```
crypto ikev2 policy IKE_POL2
 proposal default

crypto ikev2 keyring IKE_KRING2
 peer R11
```

```
  address 2010:4:11::11/128
  pre-shared-key local Warsaw
  pre-shared-key remote SanFrancisco

crypto ikev2 profile IKE_PROF2
 match identity remote key-id R11_ID
 identity local key-id R10_ID
 authentication remote pre-share
 authentication local pre-share
 keyring local IKE_KRING2

crypto ipsec profile default
 set ikev2-profile IKE_PROF2

interface Tunnel20
 no ip address
 ipv6 unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2010:4:11::11
 tunnel protection ipsec profile default

ipv route 2010:114:114::/64 tunn20
```

R11

```
crypto ikev2 keyring IKE_KRING2
 peer R10
  address 2008:9:2::10/128
  pre-shared-key local SanFrancisco
  pre-shared-key remote Warsaw

crypto ikev2 profile IKE_PROF2
 match identity remote key-id R10_ID
 identity local key-id R11_ID
 authentication remote pre-share
 authentication local pre-share
 keyring local IKE_KRING2

crypto ipsec profile default
 set ikev2-profile IKE_PROF2

interface Tunnel20
 no ip address
 ipv6 unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2008:9:2::10
 tunnel protection ipsec profile default
```

```
ipv route 2010:10:10::/64 tunn20
```

FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site to site, remote access, hub & spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm. As said earlier, IKEv2 on IOS can be also implemented by using legacy crypto maps but unless you have a particular reason to do it, this is not a recommended configuration.

Whenever you want to use PSK as the authentication method, you need to attach an IKEv2 Keyring to the Profile - unlike IKEv1 where keys are looked up on receipt of MM1 message to negotiate the PSK authentication method. Because of that, a Keyring configuration should always refer to VPN peers that will match the profile keyring is attached to. The "`peer`" option is just to divide Keyring into separate sub-sections giving it some structure. The "`address`" keyword refers to the peer's physical IP address whereas the "`identity`" option is used to match a device based on its IKEv2 ID (note that Identity matching can be only used on the Responder side).

In our example we have defined IKEv2 Policy on R10 – there was another policy already created in the previous task which was "blocking" using the default one (it was only matching an IPv4 address). This is not needed on R11 where the only policy that exists is the one defined by Smart Defaults with match for an address of "any".

As you can see from this task not only the authentication method can be asymmetrical but also the Pre-Shared Keys. This feature is inherent to IKEv2.

To set IKEv2 IDs to an arbitrary value we can use the "key_id" type of ID which is designed to match vendor-proprietary types of identification information.

The IKEv2 Smart Defaults feature minimizes the FlexVPN configuration by covering most of the use cases. This feature basically provides five different IKEv2-related configuration components (Authorization Policy, Proposal, Policy, Transform Set and IPSec Profile), each with its own pre-defined value/set of values. Note that even that we are using Smart Defaults it does not mean that a new IKEv2 Profile will be automatically attached to the default IPSec Profile – you have to do it manually (there is an option to create an IKEv2 Profile called "default" and it would get assigned to the IPSec Profile automatically but here we are using a custom name so we need to attach it). By the way, whenever you want to restore a Smart Default component to its original settings you can use the "`default crypto`" command, e.g. "`default crypto ipsec profile`". Whenever you want to disable a particular Smart Default, use the "`no`" version of command e.g. "`no crypto ipsec transform-set default`".

On the tunnel interface since we are tunneling IPv6 packets the tunnel mode must be set to "`ipsec ipv6`". If this was a regular IPv4 tunnel we would set this option to "`ipsec ipv4`".

The most useful debug commands for IKEv2 & IPSec are "`debug crypto ikev2`" (or "`debug crypto ikev2 protocol`" on ASA) and "`debug crypto ipsec`".

IPv6 Considerations

Extended IPv6 Ping (`ping ipv6`) may be useful when testing any IPv6 scenario. It allows you to send UDP Echos instead of ICMPv6, include Hop-by-Hop/Destination Options Extension Header or set a specific ToS setting.

Verification

Let's take a look at task-related Smart Defaults first:

```
R10#sh cry ikev2 proposal default
 IKEv2 proposal: default
      Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
      Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
      PRF        : SHA512 SHA384 SHA256 SHA1 MD5
      DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2

R10#sh cry ikev2 policy default
 IKEv2 policy : default
       Match fvrf : any
       Match address local : any
       Proposal    : default

R10#sh cry ipsec transform-set default
{ esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

This one has our IKEv2 Profile assigned, that's fine:

```
R10#sh cry ipsec profile default
IPSEC profile default
        IKEV2 profile IKE_PROF2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Notice encapsulation protocol and Tunnel Protection:

```
R11#sh int tu 20 | in Tunnel
Tunnel20 is up, line protocol is up
  Hardware is Tunnel
  Tunnel source 2010:4:11::11 (GigabitEthernet0/0), destination 2008:9:2::10
   Tunnel Subblocks:
         Tunnel20 source tracking subblock associated with GigabitEthernet0/0
```

```
  Tunnel protocol/transport IPSEC/IPV6
  Tunnel TTL 255
  Tunnel transport MTU 1382 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "default")
```

Now some more in-depth verifications – I want to take a look at the IKEv2 debug to see if our IKEv2 Identities are being used and show you IKEv2 negotiation in general:

```
R10# debug crypto ikev2
R10(config)#int tunnel 20
R10(config-if)#sh
R10(config-if)#no sh
```

Since R10 is using PSK authentication (IKEv2 Profile for this peer) it will try to find a key for the connection. Once this is done we will look for the policy to be sent to the peer in IKE_SA_INIT Request:

```
Feb 27 15:42:43.606: IKEv2:% Getting preshared key from profile keyring IKE_KRING2
Feb 27 15:42:43.606: IKEv2:% Matched peer block 'R11'
Feb 27 15:42:43.606: IKEv2:Searching Policy with fvrf 0, local address 2008:9:2::10
Feb 27 15:42:43.606: IKEv2:Found Policy 'IKE_POL2'
```

DH information is also part of the INITial exchange:

```
Feb 27 15:42:43.606: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public
key, DH Group 5
Feb 27 15:42:43.606: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
Feb 27 15:42:43.606: IKEv2:(SA ID = 1):Request queued for computation of DH key
Feb 27 15:42:43.606: IKEv2:IKEv2 initiator - no config data to send in IKE_SA_INIT
exch
```

Here's our Proposal (from the "IKE_POL2" Policy):

```
Feb 27 15:42:43.606: IKEv2:(SA ID = 1):Generating IKE_SA_INIT message
Feb 27 15:42:43.606: IKEv2:(SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial
negotiation),
Num. transforms: 15
   AES-CBC   AES-CBC   AES-CBC   SHA512   SHA384   SHA256   SHA1   MD5   SHA512
SHA384   SHA256   SHA96   MD596   DH_GROUP_1536_MODP/Group 5
DH_GROUP_1024_MODP/Group 2
```

NAT Detection also happens during SA_INIT:

```
Feb 27 15:42:43.610:
```

```
R10#IKEv2:(SA ID = 1):Sending Packet [To 2010:4:11::11:500/From 2008:9:2::10:500/VRF
i0:f0]
Initiator SPI : BDDADE33ECE5EA6D - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)

Feb 27 15:42:43.610: IKEv2:(SA ID = 1):Insert SA
```

Now part of the same debug output from R11:

```
R11#
Feb 27 15:42:43.611: IKEv2:Received Packet [From 2008:9:2::10:500/To
2010:4:11::11:500/VRF i0:f0]
Initiator SPI : BDDADE33ECE5EA6D - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)

Feb 27 15:42:43.611: IKEv2:(SA ID = 1):Verify SA init message
Feb 27 15:42:43.611: IKEv2:(SA ID = 1):Insert SA
Feb 27 15:42:43.611: IKEv2:Searching Policy with fvrf 0, local
R11#address 2010:4:11::11
Feb 27 15:42:43.611: IKEv2:Using the Default Policy for Proposal
Feb 27 15:42:43.611: IKEv2:Found Policy 'default'
```

After doing DH calculations R11 also selects the Proposal (part of the output omitted):

```
R11#
Feb 27 15:42:43.615: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public
key, DH Group 5
Feb 27 15:42:43.615: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
Feb 2
R11#7 15:42:43.615: IKEv2:(SA ID = 1):Request queued for computation of DH key
Feb 27 15:42:43.615: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret
key, DH Group 5
Feb 27 15:42:43.679: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
Feb 27 15:42:43.679: IKEv2:(SA ID = 1):Request queued for computation of DH secret
Feb 27 15:42:43.679: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKEYSEED
and create rekeyed IKEv2 SA
Feb 27 15:42:43.683: IKEv2:(SA ID = 1):[Crypto
R11#Engine -> IKEv2] SKEYSEED calculation and creation of rekeyed IKEv2 SA PASSED
Feb 27 15:42:43.683: IKEv2:IKEv2 responder - no config data to send in IKE_SA_INIT
exch
Feb 27 15:42:43.683: IKEv2:(SA ID = 1):Generating IKE_SA_INIT message
```

```
Feb 27 15:42:43.683: IKEv2:(SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial
negotiation),
Num. transforms: 4
   AES-CBC   SHA512   SHA512   DH_GROUP_1536_MODP/Group 5
```

R11 replies with IKE_SA_INIT Response which completes IKE_SA_INIT Exchange:

```
R11#
Feb 27 15:42:43.683: IKEv2:(SA ID = 1):Sending Packet [To 2008:9:2::10:500/From
2010:4:11::11:500/VRF i0:f0]
Initiator SPI : BDDADE33ECE5EA6D - Respond
R11#er SPI : 5166785788D21E3C Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

Feb 27 15:42:43.683: IKEv2:(SA ID = 1):Completed SA init exchange
```

R10 receives the and processes the reply:

```
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):Received Packet [From 2010:4:11::11:500/To
2008:9:2::10:500/VRF i0:f0]
Initiator SPI : BDDADE33EC
R10#E5EA6D - Responder SPI : 5166785788D21E3C Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)
```

NAT was not detected. Verification of DH information closes IKE_SA_INIT Exchange:

```
R10#
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):Verify SA init message
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):Checking NAT discov
R10#ery
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):NAT not found
Feb 27 15:42:43.690: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret
key, DH Group 5
Feb 27 15:42:43.754: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
Feb 27 15:42:43.754: IKEv2:(SA ID = 1):Request queued for computation of DH secret
Feb 27 15:42:43.754: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKEYSEED
and create rekeyed IKEv2 SA
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED calculation
and creation of rekeyed IKEv2 SA PASSED
```

```
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Completed SA init exchange
```

Mode Config (legacy Phase 1.5) is now built-in to IKEv2. Not relevant in our case; it will become important in Remote Access scenarios:

```
R10#
Feb 27 15:42:43.758: IKEv2:Config data to send:
Feb 27 15:42:43.758: Config-type: Config-request
Feb 27 15:42:43.758: Attrib type: ipv6-dns, length: 0
Feb 27 15:42:43.758: Attrib type: ipv6-subnet, length: 0
Feb 27 15:42:43.758: Attrib type: app-version, length: 244, data: Cisco IOS
Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 26-Sep-12 07:24 by prod_rel_team}_+4M
Feb 27 15:42:43.758: Attrib type: split-dns, length: 0
Feb 27 15:42:43.758: Attrib type: banner, length: 0
Feb 27 15:42:43.758: Attrib type: config-url, length: 0
Feb 27 15:42:43.758: Attrib type: backup-gateway, length: 0
Feb 27 15:42:43.758: Attrib type: def-domain, length: 0
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Have config mode data to send
Feb
```

We don't use EAP so there will not be any additional exchange taking place, we are moving on directly to the IKE_AUTH Exchange:

```
R10#
R10#27 15:42:43.758: IKEv2:(SA ID = 1):Check for EAP exchange
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Generate my authentication data
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Use preshared key for id R10_ID, key len 6
Feb 27 15:42:43.758: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Feb 27 15:42:43.758: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
```

We are using PSK. Our IKEv2_ID is "R10_ID:

```
R10#
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Get my authentication method
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):My authentication method is 'PSK'
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Check for EAP exchange
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Generating IKE_AUTH message
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Constructing IDi payload: 'R10_ID' of
type 'key ID'
```

IPSec SAs are to be protected using AES 128 and SHA-1:

```
R10#
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec
negotiation),
Num. transforms: 3
   AES-CBC    SHA96    Don't use ESN
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDi AUTH CFG SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE)
NOTIFY(ESP_TFC_NO_SUPPORT) NOTIFY(NON_FIRST_FRAGS)
```

We have got all the necessary information so we can now send it to the peer:

```
R10#
Feb 27 15:42:43.758: IKEv2:(SA ID = 1):Sending Packet [To 2010:4:11::11:500/From
2008:9:2::10:500/VRF i0:f0]
Initiator SPI : BDDADE33ECE5EA6D - Responder SPI : 5166785788D21E3C Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
 ENCR
```

R11 receives the IKE_AUTH Request packet and starts processing it:

```
R11#
Feb 27 15:42:43.763: IKEv2:(SA ID = 1):Received Packet [From 2008:9:2::10:500/To
2010:4:11::11:500/VRF i0:f0]
Initiator SPI : BDDADE33ECE5EA6D - Responder SPI : 5166785788D21E3C Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
 VID IDi AUTH CFG SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE)
NOTIFY(ESP_TFC_NO_SUPPORT) NOTIFY(NON_FIRST_FRAGS)

Feb 27 15:42:43.763: IKEv2:(SA ID = 1):Stopping timer to wait for auth message
Feb 27 15:42:43.763: IKEv2:(SA ID = 1):Checking NAT discovery
Feb 27 15:42:43.763: IKEv2:(SA ID = 1):NAT not found
```

IKEv2 Policy/Profile Lookup based succeeds (IKE_PROF2 matches “R10_ID”):

```
R11#
Feb 27 15:42:43.763: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'R10_ID' of type 'key ID'
Feb 27 15:42:43.763: IKEv2:found matching IKEv2 profile 'IKE_PROF2'
```

Profile says use PSK for authentication so R11 tries to find a keyring:

```
R11#
Feb 27 15:42:43.763: IKEv2:% Getting preshared key from profile keyring IKE_KRING2
Feb 27 15:42:43.763: IKEv2:% Matched peer block 'R10'
Feb 27 15:42:43.767: IKEv2:Searching Policy with fvrf 0, local address 2010:4:11::11
```

```
Feb 27 15:42:43.767: IKEv2:Using the Default Policy for Proposal
Feb 27 15:42:43.767: IKEv2:Found Policy 'default'
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Verify peer's policy
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Peer's policy verified
```

Remote authentication is PSK; R11 uses the Key for R10 and verifies AUTH information:

```
R11#
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Get peer's authentication method
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Get peer's preshared key for R10_ID
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Verify peer's authentication data
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Use preshared key for id R10_ID, key len 6
Feb 27 15:42:43.767: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Feb 27 15:42:43.767: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Verification of peer's authenctication data
PASSED
```

After processing Mode Config payload, R11 prepares its own AUTH information and sends it along with IPSec policy to the R10:

```
R11#
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Get my authentication method
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):My authentication method is 'PSK'
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Get peer's preshared key for R10_ID
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Generate my authentication data
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Use preshared key for id R11_ID, key len 12
Feb 27 15:42:43.767: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Feb 27 15:42:43.767: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):Get my authentication method
Feb 27 15:42:43.767: IKEv2:(SA ID = 1):My authentication method is 'PSK'
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Generating IKE_AUTH message
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Constructing IDr payload: 'R11_ID' of type
'key ID'
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec
negotiation),
Num. transforms: 3
   AES-CBC   SHA96   Don't use ESN
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDr AUTH SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)
```

```
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Sending Packet [To 2008:9:2::10:500/From
2010:4:11::11:500/VRF i0:f0]
Initiator SPI : BDDADE33ECE5EA6D - Responder SPI : 5166785788D21E3C Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
```

In the meantime R11 creates IKEv2 SA, IPSec SAs (not shown) and brings the tunnel up:

```
R11#
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database.
SA lifetime timer (86400 sec) started
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Session with IKE ID PAIR (R10_ID, R11_ID) is
UP
Feb 27 15:42:43.771: IKEv2:IKEv2 MIB tunnel started, tunnel index 1
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Load IPSEC key material
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):No duplicate IKEv2 SA found
Feb 27 15:42:43.771: IKEv2:(SA ID = 1):Starting timer (8 sec) to delete negotiation
context
Feb 27 15:42:43.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel20,
changed state to up
```

R10 received the packet and similar processing occurs to what we saw on R11. IKEv2 SA is created, negotiation is finished, IPSec SAs are created (shown after) and the tunnel is brought up:

```
R10#
Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Received Packet [From 2010:4:11::11:500/To
2008:9:2::10:500/VRF i0:f0]
Initiator SPI : BDDADE
R10#33ECE5EA6D - Responder SPI : 5166785788D21E3C Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 VID IDr AUTH SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Process auth response notify
Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'R11_ID' of type 'key ID'
Feb 27 15:42:43.774: IKEv2:Searching Policy with fvrf 0, local address 2008:9:2::10
Feb 27 15:42:43.774: IKEv2:Found Policy 'IKE_POL2'
Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Verify peer's policy
Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Peer's policy verified
Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Get peer's authentication method
Feb 27 15:42:43.774: IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Get peer's preshared key for R11_ID
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Verify peer's authentication data
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Use preshared key for id R11_ID, key len 12
```

```
Feb 27 15:42:43.778: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Feb 27 15:42:43.778: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Verification of peer's authenctication data
PASSED
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Check for EAP exchange
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Processing IKE_AUTH message
Feb 27 15:42:43.778: IKEv2:KMI/verify policy/sending to IPSec:
         prot: 3 txfm: 12 hmac 2 flags 8177 keysize 128 IDB 0x0
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database.
SA lifetime timer (86400 sec) started
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Session with IKE ID PAIR (R11_ID, R10_ID) is
UP
Feb 27 15:42:43.778: IKEv2:IKEv2 MIB tunnel started, tunnel index 1
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Load IPSEC key material
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
Feb 27 15:42:43.778: IKEv2:(SA ID = 1):No duplicate IKEv2 SA found
Feb 27 15:42:43.782: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel20,
changed state to up
```

IPSec SA creation (R10):

```
R10#
Feb 27 16:49:49.278: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 2008:9:2::10:0, remote= 2010:4:11::11:0,
    local_proxy= ::/0/256/0,
    remote_proxy= ::/0/256/0,
    protocol= ESP, transform= NONE  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
Feb 27 16:49:49.278: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Feb 27 16:49:49.278: IPSEC(crypto_ipsec_create_ipsec_sas): Map found Tunnel20-head-0
Feb 27 16:49:49.278: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the
same proxies and peer 2010:4:11::11
Feb 27 16:49:49.278: IPSEC(create_sa): sa created,
  (sa) sa_dest= 2008:9:2::10, sa_proto= 50,
    sa_spi= 0x2633C32E(640926510),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 2014
    sa_lifetime(k/sec)= (4608000/3600)
Feb 27 16:49:49.278: IPSEC(create_sa): sa created,
  (sa) sa_dest= 2010:4:11::11, sa_proto= 50,
    sa_spi= 0x4D350EC9(1295322825),
    sa_trans=esp-aes esp-sha-hmac , sa_conn_id= 2013
    sa_lifetime(k/sec)= (4608000/3600)
```

OK, time to test connectivity:

```
R10#ping 2010:114:114::11 so l100
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:114:114::11, timeout is 2 seconds:
Packet sent with a source address of 2010:10:10::10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R10#sh cry sess int tu20 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel20
Uptime: 00:01:06
Session status: UP-ACTIVE
Peer: 2010:4:11::11 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: R11_ID
      Desc: (none)
  IKEv2 SA: local 2008:9:2::10/500
          remote 2010:4:11::11/500 Active
          Capabilities:(none) connid:1 lifetime:23:58:54
  IPSEC FLOW: permit ipv6 ::/0 ::/0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 11 drop 0 life (KB/Sec) 4342294/3533
        Outbound: #pkts enc'ed 11 drop 0 life (KB/Sec) 4342295/3533
```

IKEv2-specific verification. Note that VTI interfaces always use Proxy ACL of "`permit ip/ipv6 any any`" (not configurable) which means whatever gets routed to the tunnel will be IPSec protected:

```
R10#sh cry ikev2 sess det
 IPv4 Crypto IKEv2 Session

 IPv6 Crypto IKEv2 Session

Session-id:7, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2008:9:2::10/500
Remote  2010:4:11::11/500
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/101 sec
      CE id: 1007, Session-id: 7
      Status Description: Negotiation done
      Local spi: F820B6F8FB66115B       Remote spi: C139E07EDB0DAAA9
      Local id: R10_ID
      Remote id: R11_ID
```

```
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
Child sa: local selector  ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
          remote selector ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
          ESP spi in/out: 0xC158C4B4/0x97186788
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel


R11#sh cry ikev2 sess det
 IPv4 Crypto IKEv2 Session

 IPv6 Crypto IKEv2 Session

Session-id:8, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2010:4:11::11/500
Remote  2008:9:2::10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/143 sec
      CE id: 1058, Session-id: 8
      Status Description: Negotiation done
      Local spi: C139E07EDB0DAAA9       Remote spi: F820B6F8FB66115B
      Local id: R11_ID
      Remote id: R10_ID
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
Child sa: local selector  ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
          remote selector ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
          ESP spi in/out: 0x97186788/0xC158C4B4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
```

```
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Task 20: FlexVPN IPSec Remote Access

- Configure R11 as FlexVPN Server and R10 as FlexVPN Client
- You can use Smart Defaults and/or policies from the previous task
- Use PSK “AncientPersia” for authentication
- Devices should identify to each other using their FQDNs
- Group Policy on R11 should be stored locally
- Only access to VLAN 114 should be given
- Use IP pool 10.190.190.0/24
- R11 should see client-assigned IP address with AD set to 3 and a tag value 99
- R10 should be able to reach CAT4 through the tunnel
- No static routes are allowed to be added to accomplish this task

Detailed Solution

R10

```
aaa new-model
aaa authorization network FLEX_AUTHZ local

crypto ikev2 proposal IKE_PROP
 group 14 5

crypto ikev2 authorization policy LOCAL_POL
 route set interface

crypto ikev2 keyring KRING3
 peer R11
  address 11.11.11.11
  pre-shared-key AncientPersia

crypto ikev2 profile IKE_PROF3
 match identity remote fqdn domain ipexpert.com
 identity local fqdn R10.ipexpert.com
 authentication remote pre-share
 authentication local pre-share
 keyring local KRING3
 aaa authorization group psk list FLEX_AUTHZ LOCAL_POL

crypto ipsec profile IPSEC_PROF3
 set ikev2-profile IKE_PROF3


interface Tunnel3
 ip address negotiated
 tunnel source GigabitEthernet0/0
```

```
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPSEC_PROF3

crypto ikev2 client flexvpn FLEX
  peer 1 11.11.11.11
  connect manual
  client connect Tunnel3
```

R11

```
aaa new-model
aaa authorization network FLEX_AUTHZ local

ip local pool FLEXPOOL 10.190.190.1 10.190.190.254

ip access-list standard SPLIT
 permit 10.114.114.0 0.0.0.255

crypto ikev2 authorization policy GROUP_POL
 pool FLEXPOOL
 netmask 255.255.255.0
 route set access-list SPLIT
 route accept any tag 99 distance 3

crypto ikev2 keyring KRING3
 peer R10
  address 8.9.2.10
  identity fqdn R10.ipexpert.com
  pre-shared-key AncientPersia

crypto ikev2 profile IKE_PROF3
 match identity remote fqdn R10.ipexpert.com
 identity local fqdn R11.ipexpert.com
 authentication remote pre-share
 authentication local pre-share
 keyring local KRING3
 aaa authorization group psk list FLEX_AUTHZ GROUP_POL
 virtual-template 3

crypto ipsec profile IPSEC_PROF3
 set ikev2-profile IKE_PROF3

interface Virtual-Template3 type tunnel
 ip unnumbered loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF3

route-map FLEX_TO_OSPF permit 10
 match tag 99
```

```
router ospf 1
 network 10.114.114.11 0.0.0.0 area 0
 redistribute static subnets route-map FLEX_TO_OSPF
```

CAT4

```
router ospf 1
 network 10.114.114.144 0.0.0.0 area 0
```

Before we start discussing the solution, let me describe the last (and most important) FlexVPN component, namely the IKEv2 Profile. This element is simply a container holding non-negotiable parameters of the IKE_SA_INIT and IKE_AUTH exchanges, such as:

- An authentication method (can be asymmetric)
- A Keyring and/or Trustpoint if certificates are used
- Authorization/CFG (legacy Mode Config) parameters

Before those different options can be applied to negotiated connection, a peer must first match the Profile (`match` command). There are three selection methods that can be used here:

1. Remote Peer Identity (IKE IDentifier)
2. Certificate Map (useful when Digital Certificates are used for authentication)
3. Scope Identifier – a VRF, local address or an interface where connection terminates

When selecting a profile multiple match statements of the same type are logically ORed, and multiple match statements of different types are logically ANDed; same as with IKEv2 Policy.

IKEv2 Profile configuration syntax:

```
crypto ikev2 profile profile_name
 aaa authentication eap list_name
 aaa authorization {group [override]|user} list [name-mangler name]
 aaa accounting list
 authentication {local|remote {rsa-sig|pre-share|ecdsa-sig}
 dpd interval retry-interval {on-demand | periodic}
 identity local {address | dn | email | fqdn | key-id}
 initial-contact [force]
 ivrf name
 keyring {local kring-name | aaa listname name-mangler mangler-name}
 lifetime seconds
 match {address local | interface} | certificate | fvrf name | any} |
  identity remote {address | email [domain] | fqdn [domain] | key-id }}
 nat-keepalive value
 pki trustpoint label [sign | verify]
 virtual-template number
```

As you can see, apart from the `match` statement there are several options available here. The `aaa authentication` is simple - it specifies the location of an external EAP authentication server. For `aaa authorization`, it is generally used to define the location of group/user policy. If both are used (user & group), user-policy takes precedence unless you add the "`override`" keyword. There are also three other options here (not shown above – `cert`, `eap` and `psk`) that allow you to use another method list depending on the authentication method used for a connection.

The `name-mangler` function is used to derive a username for the AAA group or user authorization requests sent to RADIUS server (you must first create a mangler with the `crypto ikev2 name-mangler` statement). For example if you create a mangler that looks for fqdn domain, only the domain name will be sent to the RADIUS server as a username for the group/user. This function is gonna be useful when digital certificates are used for authentication.

The `authentication` statement is where you choose an authentication method to be used for a connection – `local` is for the device itself and `remote` is for a VPN peer. Note that only one local method can be specified in a single Profile, however multiple statements (methods) are allowed for the peer. This is useful if a Profile matches multiple peers and you want to allow more than one authentication method for incoming connections. Don't forget that if PSK is used for authentication you must specify a `keyring`; if certificates are used you must specify a trustpoint. For `pki trustpoint` you can either use a single one for both signing and verifying or one can be specified only for signing AUTH payload when sending it to the peer (`sign`), and another one to verify received AUTH Payloads (`verify`).

Another keyword, `identity local`, is a way of setting own IKE_ID that will be send to the peer during IKE_AUTH exchange. By default if a device uses PSK for authentication, local identity will be set to an IP address; if device authenticates using certificate to the peer a distinguished name will be used.

The `initial-contact` option can be used to enable processing of INITIAL _CONTACT notification used to delete old/stale Security Associations between the peers leaving only one active SA.

The `ivrf` keyword is useful for VRF-Aware scenarios where IVRF differs from FVRF (IVRF is where the clear-text packets go/come from; by default IVRF=FVRF=global RIB).

To change the default lifetime of 24 hours (86400 seconds) for IKE_SA use the `lifetime` option. In IKEv2 the lifetime is not negotiated but managed locally between each peer, making it possible to configure lifetime independently on each peer.

Two types of keepalives you can activate are NAT (`nat-keepalive`) and DPD (`dpd`) packets.

Finally the `virtual-template` command is used to specify an interface used for cloning (e.g. in dVTI scenarios, like ours).

OK, let's now go over our task and discuss the configuration.

Since only the DH Groups 2 and 5 are supported for IPSec Remote Access scenarios, we need to modify the Proposal on R10 – this is a leftover from one of the previous tasks where we said we want to use Group 14. Since the Policy used for the peer (local address 8.9.2.10) points to this component, we have to modify it so DH Group 5 or 2 is used in calculations.

Keyring configuration on R10 and R11 contains only one "`pre-shared-key`" statement – if there is no "`local`" and "`remote`" keywords it means that the key defined by this command is symmetrical (same as in IKEv1).

Now a couple words about Mode Config. IKEv2 configuration mode allows IKE peers to exchange configuration information such as IP addresses and routes (known as **IKEv2 Routing**). The configuration information is obtained from IKEv2 authorization. Both "pull" and "push" models are supported. The "pull" model involves the exchange of Configuration Requests and Replies; the "push" model involves the exchange of Configuration Sets and Acknowledgements. Here note that the commands to send Configuration Requests and Configuration Set payloads are enabled by default.

Table below summarizes Mode Config behavior for an Initiator and Responder :

Configuration Payload Type	Sent By...	When...
CFG_REQUEST	Initiator	The initiator is the FlexVPN client or if the **config-exchange request** command is enabled in the IKEv2 profile.
CFG_REPLY	Responder	The responder receives the CFG_REQUEST.
CFG_SET	Initiator and responder	Initiator--The **config-exchange set send** command is enabled in the IKEv2 profile. Responder--The CFG_REQUEST is not received, the configuration data is available, and the **config-exchange set send** command is enabled in the IKEv2 profile.
CFG_ACK	Initiator and responder	Initiator--The **config-exchange set accept** command is enabled in the IKEv2 profile. Responder--The **config-exchange set accept** command is enabled in the IKEv2 profile.

In our case we had to configure our Client to tell the Server about the VPN IP address the Client will use on the tunnel interface (`route set interface`) – and this is exactly the same address the Client gets assigned from the Server. This feature is known as IKEv2 Routing and it can be used to tell the remote VPN Peer what prefixes are reachable through the VPN tunnel. You can think of it as an equivalent of RRI & Split Tunneling features – this way e.g. the Server can install the assigned IP address in the RIB and further redistribute it. IKEv2 Routing also allows running routing protocols, such as BGP over VPN (feature called BGP Dynamic Peering).

If you take a look at the Tunnel interface configuration, the tunnel destination is set to "`dynamic`". What it essentially means is that it will be our Flex Client (`crypto ikev2 client flexvpn`) what determines the IP address of our VPN Peer (note that since multiple "`peer`" statements can be specified under the Client Profile it allows for redundancy).

FlexVPN Server configuration is more similar to IKEv1 EasyVPN equivalent. IP address pool, Split Tunneling ACL – this stuff goes to the Group Policy which in our case is defined locally (AAA authorization list). The "`route accept`" command turns on IKEv2 Routing on the server – since the prefix gets tagged it is now easy to match it in a route-map and redistribute to Cat4.

IPv6 Considerations

Apart from changing IP addresses to IPv6 everywhere (Keyrings, Peers, Identities etc.), the tunnel interface (Client) would have to be configured with "`ipv6 address negotiated`" and tunnel mode would have to be set to "`ipsec ipv6`" (this last step is also needed on the Virtual Template interface - Server). On the server we also need to define an IPv6 pool rather than IPv4 – you would use "`ipv6 local pool`" to accomplish this - then just assign it to the Authorization Group Policy ("`ipv6 pool`"). Last thing to remember about would be to change Split Tunneling ACL to IPv6 and apply it via "`route set access-list ipv6`" in the Policy.

Verification

Since R10 acts as a client (Initiator), it tries to "pull" or just request for Mode Configuration options ("CFG_REQUEST" payload) in the IKE_AUTH Request packet (IKE_SA_INIT is already completed). The server is supposed to reply with CFG_REPLY payload of course assuming that it was configured to provide the Authorization data :

```
R10#
Feb 28 02:40:49.449: IKEv2:(SA ID = 1):Completed SA init exchange
Feb 28 02:40:49.449: IKEv2:Config data to send:
Feb 28 02:40:49.449: Config-type: Config-request
Feb 28 02:40:49.449: Attrib type: ipv4-addr, length: 0
Feb 28 02:40:49.449: Attrib type: ipv4-netmask, length: 0
Feb 28 02:40:49.449: Attrib type: ipv4-dns, length: 0
Feb 28 02:40:49.449: Attrib type: ipv4-dns, length: 0
Feb 28 02:40:49.449: Attrib type: ipv4-nbns, length: 0
Feb 28 02:40:49.449: Attrib type: ipv4-nbns, length: 0
Feb 28 02:40:49.449: Attrib type: ipv4-subnet, length: 0
Feb 28 02:40:49.449: Attrib type: app-version, length: 244, data: Cisco IOS
Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T2, RELEASE SOFTWARE
(fc1)Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by
Cisco Systems, Inc.
Compiled Wed 26-Sep-12 07:24 by prod_rel_team}_+4M
Feb 28 02:40:49.449: Attrib type: split-dns, length: 0
Feb 28 02:40:49.449: Attrib type: banner, length 0
Feb 28 02:40:49.449: Attrib type: config-url, length: 0
Feb 28 02:40:49.449: Attrib type: backup-gateway, length: 0
Feb 28 02:40:49.449: Attrib type: def-domain, length: 0

                              --- omitted ---

Feb 28 02:40:49.449: IKEv2:(SA ID = 1):Building packet for encryption.
```

```
Payload contents:
 VID IDi AUTH CFG SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE)
NOTIFY(ESP_TFC_NO_SUPPORT) NOTIFY(NON_FIRST_FRAGS)
```

R11 gets the packet – note the payload is exactly what R10 sent:

```
R11#
Feb 28 02:40:49.456: IKEv2:(SA ID = 1):Received Packet [From 8.9.2.10:500/To
11.11.11.11:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
 VID IDi AUTH CFG SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE)
NOTIFY(ESP_TFC_NO_SUPPORT) NOTIFY(NON_FIRST_FRAGS)


Feb 28 02:40:49.460: IKEv2:(SA ID = 1):Received valid config mode data
Feb 28 02:40:49.460: IKEv2:Config data recieved:
Feb 28 02:40:49.460: Config-type: Config-request
Feb 28 02:40:49.460: Attrib type: ipv4-addr, length: 0
Feb 28 02:40:49.460: Attrib type: ipv4-netmask, length: 0
Feb 28 02:40:49.460: Attrib type: ipv4-dns, length: 0
Feb 28 02:40:49.460: Attrib type: ipv4-dns, length: 0
Feb 28 02:40:49.460: Attrib type: ipv4-nbns, length: 0
Feb 28 02:40:49.460: Attrib type: ipv4-nbns, length: 0
Feb 28 02:40:49.460: Attrib type: ipv4-subnet, length: 0
Feb 28 02:40:49.460: Attrib type: app-version, length: 244, data: Cisco IOS
Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 26-Sep-12 07:24 by prod_rel_team
Feb 28 02:40:49.460: Attrib type: split-dns, length: 0
Feb 28 02:40:49.460: Attrib type: banner, length: 0
Feb 28 02:40:49.460: A
R11#ttrib type: config-url, length: 0
Feb 28 02:40:49.460: Attrib type: backup-gateway, length: 0
Feb 28 02:40:49.460: Attrib type: def-domain, length: 0
```

Since authorization information is in place (IKE_PROF3 is matched as shown below), R11 prepares the CFG_REPLY payload:

```
R11#
Feb 28 02:40:49.460: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'R10.ipexpert.com' of type 'FQDN'
Feb 28 02:40:49.460: IKEv2:found matching IKEv2 profile 'IKE_PROF3'

                                    --- omitted ---
```

```
Feb 28 02:40:49.472: IKEv2:% DVTI Vi1 created for profile IKE_PROF3 with PSH index
1.
Feb 28 02:40:49.472: IKEv2:KMI/verify policy/sending to IPSec:
         prot: 3 txfm: 12 hmac 2 flags 8177 keysize 128 IDB 0x2CE73E5C
Feb 28 02:40:49.472: IKEv2:Config data to send:
Feb 28 02:40:49.472: Config-type: Config-reply
Feb 28 02:40:49.472: Attrib type: ipv4-addr, length: 4, data: 10.190.190.15
Feb 28 02:40:49.472: Attrib type: ipv4-netmask, length: 4, data: 255.255.255.0
Feb 28 02:40:49.472: Attrib type: ipv4-subnet, length: 8, data: 10.114.114.0
255.255.255.0
Feb 28 02:40:49.472: Attrib type: app-version, length: 244, data: Cisco IOS
Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 26-Sep-12 07:24 by prod_rel_team}_+4M
Feb 28 02:40:49.472: IKEv2:(SA ID = 1):Have config mode data to send

                                    --- omitted ---

Feb 28 02:40:49.472: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 VID IDr AUTH CFG SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

Feb 28 02:40:49.476: IKEv2:(SA ID = 1):Sending Packet [To 8.9.2.10:500/From
11.11.11.11:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
```

R10 receives the Authorization Policy (IP address, mask & Split Tunneling subnet) and accepts ("sets") this information:

```
R10#
Feb 28 02:40:49.477: IKEv2:(SA ID = 1):Received Packet [From 11.11.11.11:500/To
8.9.2.10:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 VID IDr AUTH CFG SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

Feb 28 02:40:49.481: IKEv2:(SA ID = 1):Received valid config mode data
Feb 28 02:40:49.481: IKEv2:Config data recieved:
Feb 28 02:40:49.481: Config-type: Config-reply
Feb 28 02:40:49.481: Attrib type: ipv4-addr, length: 4, data: 10.190.190.15
Feb 28 02:40:49.481: Attrib type: ipv4-netmask, length: 4, data: 255.255.255.0
```

```
Feb 28 02:40:49.481: Attrib type: ipv4-subnet, length: 8, data: 10.114.114.0
255.255.255.0
Feb 28 02:40:49.481: Attrib type: app-version, length: 244, data: Cisco IOS
Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T2, RELEASE SOFTWARE
(fc1)Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by
Cisco Systems, Inc.
Compiled Wed 26-Sep-12 07:24 by prod_rel_team}_+4M
Feb 28 02:40:49.485: IKEv2:(SA ID = 1):Set received config mode data
```

This concludes IKE_AUTH stage but now INFORMATIONAL Exchange will follow ("push" model). This is because "`config-exchange set send`" is enabled by default in the IKEv2 Profile. We want to tell the server what is our IP address (the same it assigned us) so it can configure routing accordingly (RRI):

```
R10#
Feb 28 02:40:49.489: Config-type: Config-set
Feb 28 02:40:49.489: Attrib type: ipv4-subnet, length: 8, data: 10.190.190.15
255.255.255.255
                                  --- omitted ---

Feb 28 02:40:49.489: IKEv2:(SA ID = 1):Sending info exch config
Feb 28 02:40:49.489: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 CFG
Feb 28 02:40:49.489: IKEv2:(SA ID = 1):Checking if request will fit in peer window
Feb 28 02:40:49.489: IKEv2:(SA ID = 1):Sending Packet [To 11.11.11.11:500/From
8.9.2.10:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 2
IKEv2 INFORMATIONAL Exchange REQUEST


R11#
Feb 28 02:40:49.492: IKEv2:(SA ID = 1):Received Packet [From 8.9.2.10:500/To
11.11.11.11:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 2
IKEv2 INFORMATIONAL Exchange REQUEST
Payload contents:
 CFG

Feb 28 02:40:49.496: IKEv2:Config data recieved:
Feb 28 02:40:49.496: Config-type: Config-set
Feb 28 02:40:49.496: Attrib type: ipv4-subnet, length: 8, data: 10.190.190.15
255.255.255.255
Feb 28 02:40:49.496: IKEv2:(SA ID = 1):Set received config mode data
```

R11 will now reply with the CFG_ACK Payload ("`config-exchange set accept`" is also enabled by default in the IKEv2 Profile) to finish INFORMATIONAL Exchange:

```
R11#
```

```
Feb 28 02:40:49.496: IKEv2:Config data to send:
Feb 28 02:40:49.496: Config-type: Config-ack
Feb 28 02:40:49.496: Attrib type: ipv4-subnet, length: 0
Feb 28 02:40:49.496: IKEv2:(SA ID = 1):Have config mode data to send
Feb 28 02:40:49.496: IKEv2:(SA ID = 1):Sending info exch config resp
Feb 28 02:40:49.496: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 CFG

Feb 28 02:40:49.496: IKEv2:(SA ID = 1):Sending Packet [To 8.9.2.10:500/From
11.11.11.11:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 2
IKEv2 INFORMATIONAL Exchange RESPONSE
Payload contents:
 ENCR

R10#
Feb 28 02:40:49.497: IKEv2:(SA ID = 1):Received Packet [From 11.11.11.11:500/To
8.9.2.10:500/VRF i0:f0]
Initiator SPI : D33A65767EFC6846 - Responder SPI : D1A6AD65107BFEFD Message id: 2
IKEv2 INFORMATIONAL Exchange RESPONSE
Payload contents:
 CFG
```

No other information is sent by R11, negotiation is over:

```
Feb 28 02:40:49.497: IKEv2:(SA ID = 1):Processing ACK to informational exchange
Feb 28 02:40:49.497: IKEv2:Config data recieved:
Feb 28 02:40:49.497: Config-type: Config-ack
Feb 28 02:40:49.497: Attrib type: ipv4-subnet, length: 0
Feb 28 02:40:49.497: IKEv2:(SA ID = 1):Set received config mode data
```

Let's start with verifying our IKEv2 settings:

```
R10#sh crypto ikev2 profile IKE_PROF3

IKEv2 profile: IKE_PROF3
 Ref Count: 4
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn domain ipexpert.com
  Certificate maps: none
 Local identity: fqdn R10.ipexpert.com
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
```

```
 Keyring: KRING3
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization:
  psk: list FLEX_AUTHZ, username LOCAL_POL
 AAA user authorization: none


R11#sh crypto ikev2 profile IKE_PROF3

IKEv2 profile: IKE_PROF3
 Ref Count: 5
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   fqdn R10.ipexpert.com
  Certificate maps: none
 Local identity: fqdn R11.ipexpert.com
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: KRING3
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: 3
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization:
  psk: list FLEX_AUTHZ, username GROUP_POL
 AAA user authorization: none


R11#sh crypto ikev2 authorization policy GROUP_POL
 IKEv2 Authorization Policy : GROUP_POL
  IPV4 Address Pool : FLEXPOOL
  Netmask : 255.255.255.0
  route set acl: SPLIT
  route accept any tag : 99 distance : 3
```

```
R10#sh crypto ikev2 authorization policy LOCAL_POL
 IKEv2 Authorization Policy : LOCAL_POL
  route set interface
  route accept any tag : 1 distance : 2
```

Time to connect and test our configuration:

```
R10#crypto ikev2 client flexvpn connect

R10#sh crypto ikev2 client flexvpn FLEX detail

  Profile : FLEX
  Current state:ACTIVE
  Peer : 11.11.11.11
  Source : GigabitEthernet0/0
  ivrf : IP DEFAULT
  fvrf : IP DEFAULT
  Backup group: Default
  Tunnel interface : Tunnel3
  Assigned IP address: 10.190.190.15
```

Let's see if we have a route for the Client (RRI) – note the tag value 99. It should now get redistributed into OSPF so CAT4 knows how to reach the Client:

```
R11#sh ip route 10.190.190.15
Routing entry for 10.190.190.15/32
  Known via "static", distance 3, metric 0
  Tag 99
  Redistributing via ospf 1
  Advertised by ospf 1 subnets route-map FLEX_TO_OSPF
  Routing Descriptor Blocks:
  * directly connected, via Virtual-Access1, permanent
      Route metric is 0, traffic share count is 1
      Route tag 99

CAT4(config)#do sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2     10.190.190.15/32 [110/20] via 10.114.114.11, 00:00:13, Vlan114
```

So far, so good. What about connectivity?:

```
R10#ping 10.114.114.144
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.114.114.144, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms

R10#sh cry sess int tu3 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel3
Uptime: 00:58:12
Session status: UP-ACTIVE
Peer: 11.11.11.11 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: R11.ipexpert.com
      Desc: (none)
  IKEv2 SA: local 8.9.2.10/500 remote 11.11.11.11/500 Active
          Capabilities:(none) connid:1 lifetime:23:01:48
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 4347885/3515
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4347885/3515
```

Cool. At the end we want to make sure that Mode Config information was exchanged between the devices:

```
R10#sh cry ikev2 sess det
 IPv4 Crypto IKEv2 Session

Session-id:46, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         8.9.2.10/500          11.11.11.11/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA384, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/3607 sec
      CE id: 1056, Session-id: 46
      Status Description: Negotiation done
      Local spi: FD08FA58AE4495FF       Remote spi: 572B6721674B3532
```

```
      Local id: R10.ipexpert.com
      Remote id: R11.ipexpert.com
      Local req msg id:  5              Remote req msg id:  0
      Local next msg id: 5              Remote next msg id: 0
      Local req queued:  5              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
      Pushed IP address: 10.190.190.15
      Remote subnets:
      10.114.114.0 255.255.255.0
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xD32C21B9/0xFF3BCF61
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel


R11#sh cry ikev2 sess det
 IPv4 Crypto IKEv2 Session

Session-id:51, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         11.11.11.11/500       8.9.2.10/500          none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA384, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/3625 sec
      CE id: 1056, Session-id: 51
      Status Description: Negotiation done
      Local spi: 572B6721674B3532       Remote spi: FD08FA58AE4495FF
      Local id: R11.ipexpert.com
      Remote id: R10.ipexpert.com
      Local req msg id:  0              Remote req msg id:  5
      Local next msg id: 0              Remote next msg id: 5
      Local req queued:  0              Remote req queued:  5
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Assigned host addr: 10.190.190.15
      Initiator of SA : No
      Remote subnets:
      10.190.190.15 255.255.255.255
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
```

```
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xFF3BCF61/0xD32C21B9
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Task 21: FlexVPN Hub & Spoke

- Configure IKEv2 VPN between R10 and R11
- This should be a Hub (R11) & Spoke (R10) deployment
- Use digital certificates for authentication. R2 acts as a CA
- Use IKEv2 Routing to protect traffic between 10.100.100.0/24 and VLAN114 behind R11
- Create additional loopback interface on R10 – 10.251.251.10/24
- This subnet should be dynamically advertised to the Hub using OSPF
- Hub should be able to reach this network through the VPN Tunnel
- You are only allowed to use Smart Defaults configurations

BEFORE YOU BEGIN WORKING ON THIS TASK:

You may load initial configurations on R10 & R11. If you don't want to do this make sure any previously configured tunnels (R10-R11) are shut down and that any other earlier configuration does not interfere with this task.

Detailed Solution

R10

```
ntp server 2.2.2.2
ip domain-name ipexpert.com

crypto pki trustpoint VPNTRUST
 enrollment url http://2.2.2.2:80
 password ipexpert123
 subject-name cn=R10.ipexpert.com, ou=INSTRUCTORS, l=San Jose, c=US
 revocation-check crl

crypto pki authen VPNTRUST
crypto pki enroll VPNTRUST

aaa new-model
aaa authorization network FLEX_AUTHZ local

access-list 50 permit 10.100.100.0 0.0.0.255

crypto pki certificate map CMAP4 10
 subject-name co cn = r11.ipexpert.com
```

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 50

crypto ikev2 profile default
 match certificate CMAP4
 identity local dn
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint VPNTRUST
 aaa authorization group cert list FLEX_AUTHZ default

interface Loopback51
 ip address 10.251.251.10 255.255.255.0
 ip ospf 2 area 0
 ip ospf network point-to-point

interface Tunnel50
 ip address negotiated
 ip ospf 2 area 0
 tunnel source GigabitEthernet0/0
 tunnel destination 11.11.11.11
 tunnel protection ipsec profile default
```

R11

```
ntp server 2.2.2.2
ntp server 2.2.2.2 source Loopback0
ip domain-name ipexpert.com

crypto pki trustpoint VPNTRUST
 enrollment url http://2.2.2.2:80
 password ipexpert123
 subject-name cn=R11.ipexpert.com, ou=INSTRUCTORS, l=Warsaw, c=PL
 revocation-check crl
 source interface Loopback0

aaa new-model
aaa authorization network FLEX_AUTHZ local

access-list 50 permit 10.114.114.0 0.0.0.255

ip local pool HUBPOOL 10.50.50.21 10.50.50.254

crypto pki certificate map CMAP4 10
 subject-name co cn = r10.ipexpert.com

crypto ikev2 authorization policy default
 pool HUBPOOL
```

```
 netmask 255.255.255.0
 route set access-list 50

crypto ikev2 profile default
 match certificate CMAP4
 identity local dn
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint VPNTRUST
 aaa authorization group cert list FLEX_AUTHZ default
 virtual-template 51

int loop 50
 ip add 10.50.50.11 255.255.255.0

interface Virtual-Template51 type tunnel
 ip unnumbered Loopback50
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel protection ipsec profile default
```

FlexVPN Hub & Spoke design is somewhat similar to IPSec Remote Access VPNs using the Network Extension Mode. The Hub (server) does not know the clients in advance and then once the clients connect they will have to somehow tell the Hub about subnets they want to protect.

In this lab we are using digital certificates for authentication. In order to match an incoming connection to the profile, certificate maps are used. We are no longer restricted to only using OU for matching, as in older versions of IOS prior to introducing the feature (this was a problem with certain IOSes and IKEv1).

In the IKEv2 Profile we set IKE_ID to be DN (from the certificate), we specified the authentication method (certs) and the credential store (Trustpoint VPNTRUST). Mode Config has been also enabled so the peers could exchange routing information using IKEv2.

An important thing to note here is that "`route set interface`" is only configured on the Spoke. This is required so the Hub learns that the "pushed"/assigned IP address is reachable via the Tunnel. Without this feature, since every single Virtual Access interface gets an IP address from the loopback (as unnumbered), it is always a /32 address – and no 10.50.50.0/24 subnet is associated with the cloned port. This is as opposed to R10 which "pulls" the subnet length along with a VPN IP address (thanks to our Group Policy configuration). This way we don't have to enable this command on the Hub (although we could to tell R10 about /32 prefix explicitly).

In case you wonder why we need to create a loopback on R11 and assign a VPN address to the Virtual Template as "unnumbered" – it is because statically assigned IPs don't get cloned to the Access interfaces.

Another important thing to realize is the difference in interface types used on the Spoke vs the Hub. Spoke uses a regular Tunnel interface, where we specify the source and destination (we know the physical IP address of the Hub), but the Hub is configured with a Virtual-Template. This is required because headend device does not know who will be connecting to it.

Last but not the least – we did not put "`tunnel mode ipsec ipv4`" on the interfaces. This is just to show you that GRE can be also used as an encapsulating protocol (actually this is GRE over IPSec) – this would be useful for situations when we would like to tunnel IPv6 packets over this IPv4 IPSec VPN.

IPv6 Considerations

Apart from changing IP addresses to IPv6 everywhere, the tunnel interface (Client) would have to be configured with "`ipv6 address negotiated`". Hub's Virtual Template would use "ipv6 unnumbered" and loopback would be also configured with an IPv6 address rather than IPv4. On the Headend device we also need to define an IPv6 pool – you would use "`ipv6 local pool`" to accomplish this - then just assign it to the Authorization Group Policy ("`ipv6 pool`"). Last thing to remember about would be to change Split Tunneling ACLs to IPv6 and apply them via "`route set access-list ipv6`" in the Policies.

Verification

First some basic config verifications:

```
R10#sh cry ikev2 authorization policy default
 IKEv2 Authorization Policy : default
  route set interface
  route set acl: 50
  route accept any tag : 1 distance : 2

R11#sh cry ikev2 author pol default
 IKEv2 Authorization Policy : default
  IPV4 Address Pool : HUBPOOL
  Netmask : 255.255.255.0
  route set acl: 50
  route accept any tag : 1 distance : 2
```

Although not shown in the IPSec Profile, the IKEv2 Profile "default" will be called out:

```
R11#sh cry ipse prof default
IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Now the session state:

```
R10#sh cry ikev2 sess det
 IPv4 Crypto IKEv2 Session

Session-id:60, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         8.9.2.10/500          11.11.11.11/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: RSA
      Life/Active Time: 86400/1649 sec
      CE id: 1081, Session-id: 60
      Status Description: Negotiation done
      Local spi: 2034A1A007805C00       Remote spi: AE93EA5BF4FED9CB
      Local id: hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San
Jose,c=US
      Remote id:
hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL
      Local req msg id:  3              Remote req msg id:  0
      Local next msg id: 3              Remote next msg id: 0
      Local req queued:  3              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
      Pushed IP address: 10.50.50.27
      Remote subnets:
      10.114.114.0 255.255.255.0
Child sa: local selector  8.9.2.10/0 - 8.9.2.10/65535
          remote selector 11.11.11.11/0 - 11.11.11.11/65535
          ESP spi in/out: 0x60D5D484/0xE69F5F36
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode transport


R11#sh ip int br | in Access
Virtual-Access2            10.50.50.11     YES unset  up                    up


R11#sh cry ikev2 sa det
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         11.11.11.11/500       8.9.2.10/500          none/none            READY
```

```
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: RSA
      Life/Active Time: 86400/1674 sec
      CE id: 1081, Session-id: 65
      Status Description: Negotiation done
      Local spi: AE93EA5BF4FED9CB       Remote spi: 2034A1A007805C00
      Local id:
hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL
      Remote id: hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San
Jose,c=US
      Local req msg id:  0              Remote req msg id:  3
      Local next msg id: 0              Remote next msg id: 3
      Local req queued:  0              Remote req queued:  3
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Assigned host addr: 10.50.50.27
      Initiator of SA : No
      Remote subnets:
      10.50.50.27 255.255.255.255
      10.100.100.0 255.255.255.0
```

And routing information along with some connectivity tests:

```
R10#sh ip route static | be Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S        10.114.114.0/24 [2/0] via 0.0.0.0, Tunnel50
S     192.168.8.0/24 [1/0] via 8.9.2.30


R10#ping 10.50.50.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.50.50.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R10#ping 10.114.114.11 source l100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.114.114.11, timeout is 2 seconds:
Packet sent with a source address of 10.100.100.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R10#sh cry sess int tu 50 det
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel50
Uptime: 00:28:29
Session status: UP-ACTIVE
Peer: 11.11.11.11 port 500 fvrf: (none) ivrf: (none)
      Phase1_id:
hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL
      Desc: (none)
  IKEv2 SA: local 8.9.2.10/500 remote 11.11.11.11/500 Active
          Capabilities:(none) connid:1 lifetime:23:31:31
  IPSEC FLOW: permit 47 host 8.9.2.10 host 11.11.11.11
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 197 drop 0 life (KB/Sec) 4230412/1891
        Outbound: #pkts enc'ed 197 drop 0 life (KB/Sec) 4230412/1891


R11#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.4.11.4 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O        10.251.251.0/24 [110/2] via 10.50.50.27, 00:28:45, Virtual-Access2


R11#sh ip route stati | be Gateway
Gateway of last resort is 10.4.11.4 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.4.11.4
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S        10.50.50.27/32 [2/0] via 0.0.0.0, Virtual-Access2
S        10.100.100.0/24 [2/0] via 0.0.0.0, Virtual-Access2

R11#ping 10.251.251.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.251.251.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

```
R11#sh cry sess int virtual-acc2 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Virtual-Access2
Uptime: 00:29:19
Session status: UP-ACTIVE
Peer: 8.9.2.10 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San
Jose,c=US
      Desc: (none)
  IKEv2 SA: local 11.11.11.11/500 remote 8.9.2.10/500 Active
          Capabilities:(none) connid:1 lifetime:23:30:41
  IPSEC FLOW: permit 47 host 11.11.11.11 host 8.9.2.10
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 207 drop 0 life (KB/Sec) 4148094/1841
        Outbound: #pkts enc'ed 207 drop 0 life (KB/Sec) 4148094/1841
```

Getting into more depth with verification. Only relevant debug outputs are shown in this example. The "default" Policy and Proposal is used on both routers; the correct trustpoint is found:

```
Feb 28 23:15:39.246: IKEv2:Using the Default Policy for Proposal
Feb 28 23:15:39.246: IKEv2:Found Policy 'default'

R11#
Feb 28 23:15:39.250: IKEv2:Found Policy 'default'
Feb 28 23:15:39.254: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieve configured
trustpoint(s)
Feb 28 23:15:39.254: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
'Trustpool4'   'Trustpool3'   'Trustpool2'   'Trustpool1'   'Trustpool'   'VPNTRUST'

R10#
ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from received certificate hash(es)
Feb 28 23:15:39.330: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
'VPNTRUST'
Feb 28 23:15:39.330: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the
trustpoint VPNTRUST
Feb 28 23:15:39.330: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the
trustpoint PASSED
```

IKE_SA_INIT is finished, moving on to IKE_AUTH Exchange:

```
R10#
3:15:39.398: IKEv2:(SA ID = 1):Completed SA init exchange
Feb 28 23:15:39.398: IKEv2:Config data to send:
```

```
Feb 28 23:15:39.398: Config-type: Config-request
Feb 28 23:15:39.398: Attrib type: ipv4-addr, length: 0
Feb 28 23:15:39.398: Attrib type: ipv4-netmask, length: 0
Feb 28 23:15:39.398: Attrib type: ipv4-dns, length: 0
Feb 28 23:15:39.398: Attrib type: ipv4-dns, length: 0
Feb 28 23:15:39.398: Attrib type: ipv4-nbns, length: 0
Feb 28 23:15:39.398: Attrib type: ipv4-nbns, length: 0
Feb 28 23:15:39.398: Attrib type: ipv4-subnet, length: 0

R10#
Feb 28 23:15:39.402: IKEv2:(SA ID = 1):Get my authentication method
Feb 28 23:15:39.402: IKEv2:(SA ID = 1):My authentication method is 'RSA'
Feb 28 23:15:39.402: IKEv2:(SA ID = 1):Sign authentication data
Feb 28 23:15:39.410: IKEv2:(SA ID = 1):Authentication material has been sucessfully
signed

Feb 28 23:15:39.410: IKEv2:(SA ID = 1):Constructing IDi payload:
'hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San Jose,c=US' of
type 'DER ASN1 DN'
```

IKEv2 Profile lookup on R11. Correct trustpoint is found, authentication & validation can be now performed:

```
R11#
Feb 28 23:15:39.426: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'hostname=R10.ipexpert.com,cn=R10.ipexpert.com,ou=INSTRUCTORS,l=San Jose,c=US' of
type 'DER ASN1 DN'
Feb 28 23:15:39.426: IKEv2:Optional profile description not updated in PSH
Feb 28 23:15:39.426: IKEv2:Searching Policy with fvrf 0, local address 11.11.11.11
Feb 28 23:15:39.426: IKEv2:Using the Default Policy for Proposal
Feb 28 23:15:39.426: IKEv2:Found Policy 'default'
Feb 28 23:15:39.426: IKEv2:Found matching IKEv2 profile 'default'

Feb 28 23:15:39.430: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s):
'VPNTRUST'
Feb 28 23:15:39.430: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the
trustpoint VPNTRUST
Feb 28 23:15:39.430: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the
trustpoint PASSED
Feb 28 23:15:39.434: IKEv2:(SA ID = 1):Get peer's authentication method
Feb 28 23:15:39.434: IKEv2:(SA ID = 1):Peer's authentication method is 'RSA'
Feb 28 23:15:39.434: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Validating certificate chain
Feb 28 23:15:39.434: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate
chain PASSED

Feb 28 23:15:39.434: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Feb 28 23:15:39.434: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Verify signed
authenticaiton data
```

```
Feb 28 23:15:39.438: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Verification of
signed authentication data PASSED
```

Processing of the Mode Config payload starts on R1. The Spoke asked for an IPv4 address, mask and subnet, among other things:

```
R11#
Feb 28 23:15:39.438: IKEv2:Using mlist FLEX_AUTHZ and username default for group
author request
Feb 28 23:15:39.438: IKEv2:(SA ID = 1):[IKEv2 -> AAA] Authorisation request sent
Feb 28 23:15:39.438: IKEv2:(SA ID = 1):[AAA -> IKEv2] Received AAA authorisation
response
Feb 28 23:15:39.438: IKEv2:(SA ID = 1):Received valid config mode data
Feb 28 23:15:39.438: IKEv2:Config data recieved:
Feb 28 23:15:39.438: Config-type: Config-request
Feb 28 23:15:39.438: Attrib type: ipv4-addr, length: 0
Feb 28 23:15:39.438: Attrib type: ipv4-netmask, length: 0
                                ---- omitted ----
```

It is now time to return requested information in the CFG_REPLY payload:

```
R11#
Feb 28 23:15:39.450: IKEv2:Config data to send:
Feb 28 23:15:39.450: Config-type: Config-reply
Feb 28 23:15:39.450: Attrib type: ipv4-addr, length: 4, data: 10.50.50.27
Feb 28 23:15:39.450: Attrib type: ipv4-netmask, length: 4, data: 255.255.255.0
Feb 28 23:15:39.450: Attrib type: ipv4-subnet, length: 8, data: 10.114.114.0
255.255.255.0

Feb 28 23:15:39.462: IKEv2:(SA ID = 1):Constructing IDr payload:
'hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL' of type
'DER ASN1 DN'
```

R10 gets the packet and starts processing it. The Profile matches (default), we can now finish authentication:

```
R10#
Feb 28 23:15:39.474: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL' of type
'DER ASN1 DN'
Feb 28 23:15:39.474: IKEv2:Optional profile description not updated in PSH
Feb 28 23:15:39.474: IKEv2:Searching Policy with fvrf 0, local address 8.9.2.10
Feb 28 23:15:39.474: IKEv2:Using the Default Policy for Proposal
Feb 28 23:15:39.474: IKEv2:Found Policy 'default'
Feb 28 23:15:39.478: IKEv2:Found matching IKEv2 profile 'default'

Feb 28 23:15:39.478: IKEv2:(SA ID = 1):Peer's authentication method is 'RSA'
Feb 28 23:15:39.478: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Validating certificate chain
```

```
Feb 28 23:15:39.478: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate
chain PASSED
Feb 28 23:15:39.478: IKEv2:(SA ID = 1):Save pubkey
Feb 28 23:15:39.478: IKEv2:(SA ID = 1):Verify peer's authentication data
Feb 28 23:15:39.478: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Feb 28 23:15:39.478: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Feb 28 23:15:39.478: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Verify signed
authenticaiton data
Feb 28 23:15:39.482: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Verification of
signed authentication data PASSED
```

Mode Config data is applied, IKE_AUTH is finished, IPSec SAs are created:

```
R10#
Feb 28 23:15:39.482: IKEv2:Config data recieved:
Feb 28 23:15:39.482: Config-type: Config-reply
Feb 28 23:15:39.482: Attrib type: ipv4-addr, length: 4, data: 10.50.50.27
Feb 28 23:15:39.482: Attrib type: ipv4-netmask, length: 4, data: 255.255.255.0
Feb 28 23:15:39.482: Attrib type: ipv4-subnet, length: 8, data: 10.114.114.0
255.255.255.0

Feb 28 23:15:39.490: IKEv2:(SA ID = 1):Load IPSEC key material
Feb 28 23:15:39.490: IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
Feb 28 23:15:39.490: IKEv2:(SA ID = 1):No duplicate IKEv2 SA found
```

Now the INFORMATIONAL Exchange. The CFG_SET payload is being sent to R11:

```
Feb 28 23:15:39.490: Config-type: Config-set
Feb 28 23:15:39.490: Attrib type: ipv4-subnet, length: 8, data: 10.50.50.27
255.255.255.255
Feb 28 23:15:39.494: Attrib type: ipv4-subnet, length: 8, data: 10.100.100.0
255.255.255.0
Feb 28 23:15:39.494: Attrib type: app-version, length: 244, data: Cisco I
```

Hub receives this information, processes it:

```
R11#
Feb 28 23:15:39.498: IKEv2:Config data recieved:
Feb 28 23:15:39.498: Config-type: Config-set
Feb 28 23:15:39.498: Attrib type: ipv4-subnet, length: 8, data: 10.50.50.27
255.255.255.255
Feb 28 23:15:39.498: Attrib type: ipv4-subnet, length: 8, data: 10.100.100.0
255.255.255.0
Feb 28 23:1
```

And finally an empty CFG_ACK is sent to R10 to finish the transaction:

```
R11#
Feb 28 23:15:39.498: Config-type: Config-ack
Feb 28 23:15:39.498: Attrib type: ipv4-subnet, length: 0
Feb 28 23:15:39.498: IKEv2:(SA ID = 1):Have config mode data to send
Feb 28 23:15:39.498: IKEv2:(SA ID = 1):Sending info exch config resp
```

Task 22: FlexVPN EAP Authentication

- Modify the configuration from the previous task
- Use EAP as the authentication method
- Authenticate as “Prince” with a password “OfPersia”
- RADIUS communication should be protected with key “ipexpert”

Detailed Solution

R10

```
aaa new-model
aaa authorization network FLEX_AUTHZ local

crypto ikev2 profile default
 match certificate CMAP4
 identity local key-id Prince
 authentication remote rsa-sig
 authentication local eap
 pki trustpoint VPNTRUST
 aaa authorization group cert list FLEX_AUTHZ default

interface Tunnel50
 ip address negotiated
 ip ospf mtu-ignore
 ip ospf 2 area 0
 tunnel source GigabitEthernet0/0
 tunnel destination 11.11.11.11
 tunnel protection ipsec profile default
```

R11

```
aaa new-model
aaa authentication login EAPAUTH group radius
aaa authorization network FLEX_AUTHZ local

radius server ISE
 address ipv4 8.9.2.150 auth-port 1645 acct-port 1646
 key ipexpert

ip radius source-interface Loopback0

crypto ikev2 profile default
 match identity remote key-id Prince
```

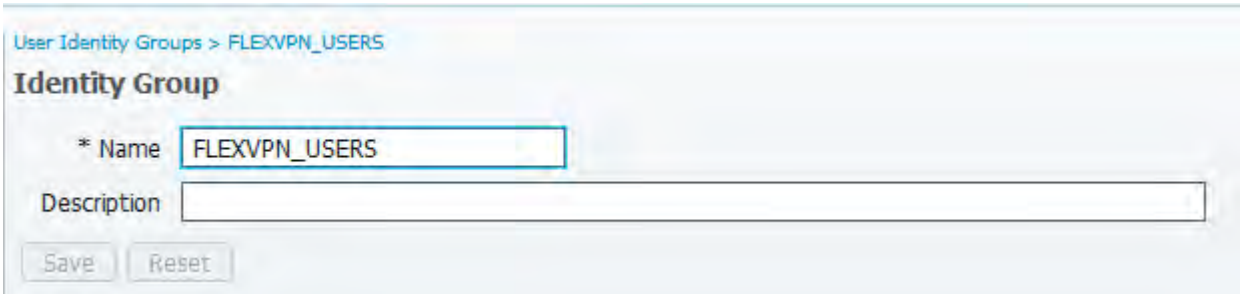
```
identity local dn
authentication remote eap
authentication local rsa-sig
pki trustpoint VPNTRUST
aaa authentication eap EAPAUTH
aaa authorization user eap cached
aaa authorization group eap list FLEX_AUTHZ default
virtual-template 51
```

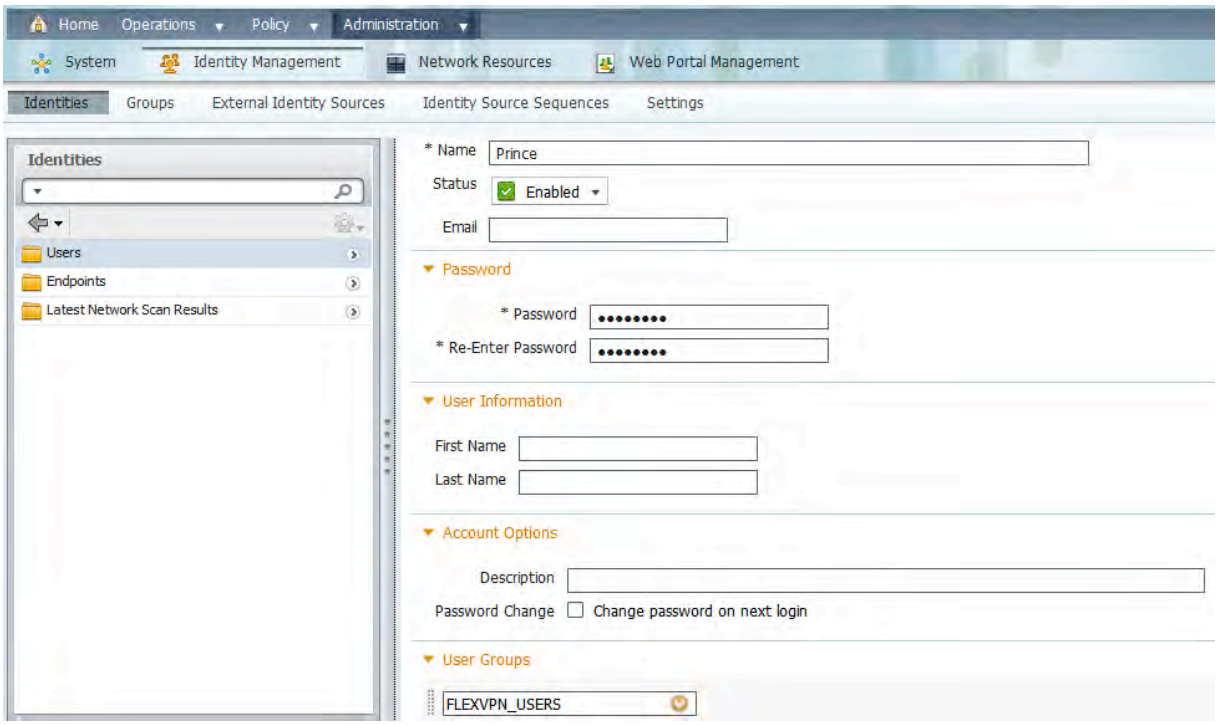
ISE

```
ip route 11.11.11.11 255.255.255.255 gateway 10.1.1.1
```

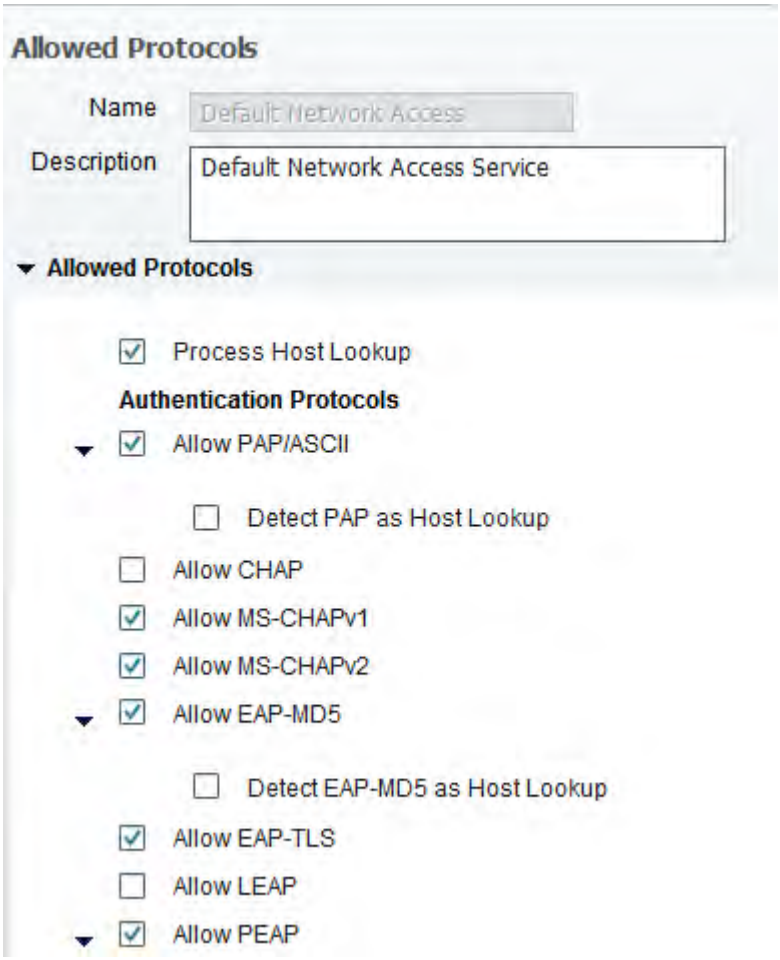
We have fixed routing, now it is time to configure ISE to handle EAP Authentication Requests and assign them to appropriate Authorization Profile. We start with adding R11 to Network Devices:

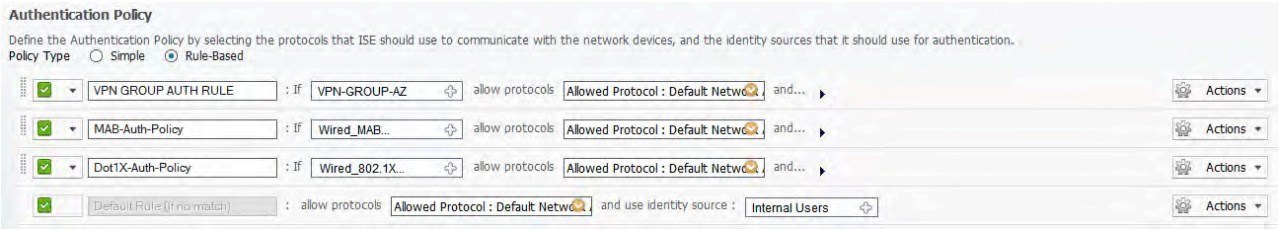
Next we will create a Group (which will be then used as part of our Authorization Rule) and then assign there a User (“Prince”) we will use to authenticate :



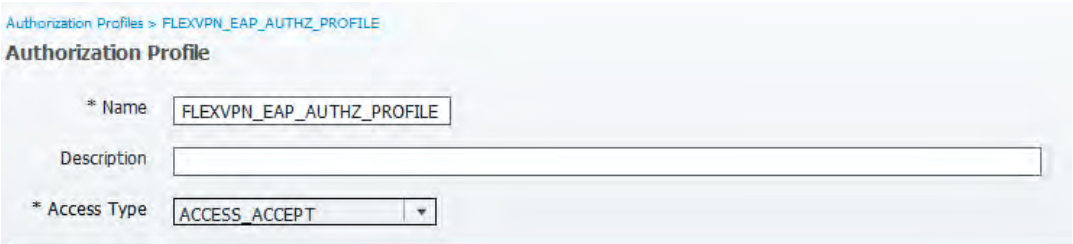


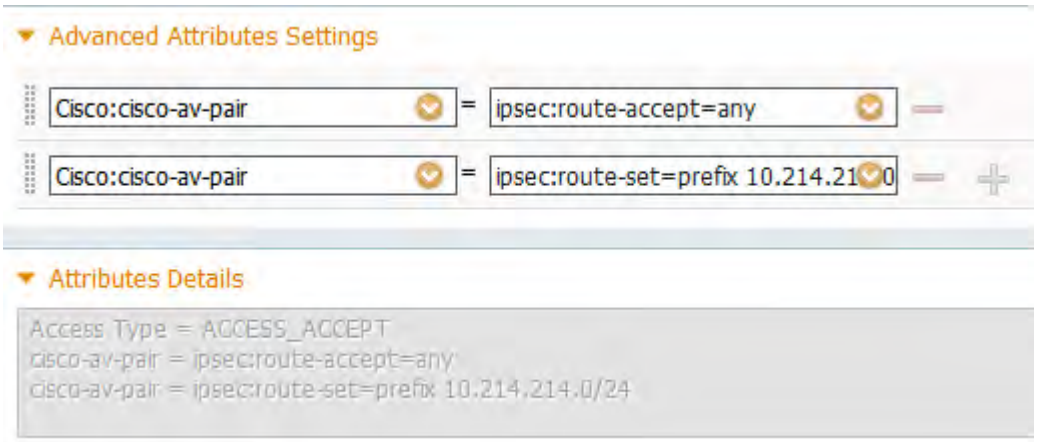
Authentication Policy is simple – we will use the Default rule and the internal database for authentication. Since this rule uses "Default Network Access" element as "Allowed Protocol" you want to check and see if it allows some non-cert EAP methods such as EAP-MD5 and then also PAP/ASCII:



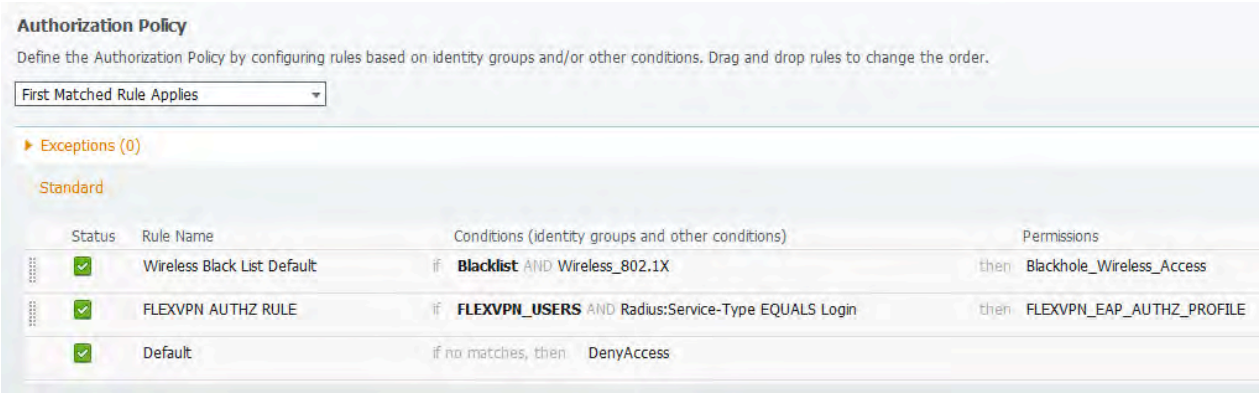


Another thing we will need before we move on is the Authorization Profile:





We now have all the required elements and can proceed to the Authorization Policy. EAP Authentication uses Service-Type of "Login" – coupled with our User Group we can use it as a Condition (theoretically we could also add another RADIUS Attribute – EAP Message id 79):



Extensible Authentication Protocol (EAP) as the local authentication method is supported only on the IKEv2 initiator and EAP as the remote authentication is supported only on the IKEv2 responder. This means that only the Initiator can authenticate using EAP to the Responder and not vice-versa. More over if EAP is specified as the local authentication method, the remote authentication method MUST be certificate based.

The NAS places any EAP messages received from the user into the Value part EAP Message attributes (ID 79) and forwards them to the RADIUS Server as part of the Access-Request, which can return EAP messages in Access-Challenge, Access-Accept and Access-Reject packets. The other RADIUS attribute, Message-Authenticator is simply a checksum to verify the integrity of the RADIUS packet. The Message-Authenticator attribute is mandatory within a RADIUS packet if it contains a EAP-Message attribute.

What is gonna be important to understand is how the EAP Identity is derived for Authentication. If the "`aaa authentication eap`" command on the Responder was configured with the "**`query-identity`**" keyword, the FlexVPN server will ask for the Identity from the client. Otherwise, the

FlexVPN client's IKEv2 identity is used as the EAP identity ("Prince" in our case), with one exception – if the client's IKEv2 identity is an IPv4 or IPv6 address, the session is terminated because IP addresses cannot be used as the EAP identity.

The FlexVPN Server starts the EAP authentication by passing the FlexVPN client's EAP Identity to the EAP server; the FlexVPN server then relays EAP messages between the Client and the EAP server until the authentication is complete. If the authentication succeeds, the EAP server is expected to return the authenticated EAP Identity to the FlexVPN server in the EAP success message.

After EAP authentication, the EAP Identity used for the IKEv2 configuration is obtained from the following sources in the given order:

- The EAP identity provided by the EAP server with the EAP success message
- The EAP identity queried from the client when the query-identity keyword is configured
- The FlexVPN client IKEv2 identity used as the EAP identity

In our task the changes made on the Client were to set the local authentication method to EAP and modify the IKE_ID to be "Prince". This will be further used by the server as EAP Username (we did not use "`query-identity`" so we will not get prompted for the username on R10).

OSPF is not the best choice for a routing protocol over P2P links where one is configured with an "unnumbered" IP address and the other is not. This creates discrepancies in the OSPF database and prevents prefixes from being installed on the "numbered" side of the link (tunnel in our case). In our case R11, as shown in previous task, installed R10's prefix successfully but if you tried to advertise Hub's network to R10 the Client would not install the prefixes. If the intent was to advertise IPv6 we could use EIGRPv6 but for IPv4 BGP could be used along with the Dynamic Neighbors feature. Either way in our case we had to disable MTU checking on the Tunnel interface so at least the Hub could learn a prefix (10.251.251.0/24).

New way of configuring RADIUS/TACACS servers in IOSes 15.x is to use the "`radius/tacacs server`" command. This way you can give a particular AAA server a name (and then refer to it in the AAA method list) and also specify an IPv6 address if you want to use IPv6 for transport.

One more interesting command on R11 is "`aaa authorization user eap cache`". This tells the Server to re-use the Authentication Profile for Authorization. In other words whatever attributes were returned for the user during EAP Authentication (remember RADIUS combines Authentication with Authorization), they *should* be used for VPN User Authorization. I said *should* because this feature does not appear to be working correctly – only the IP address & mask are applied, remaining attributes are not even returned to the Client (sounds like a bug). Interestingly enough adding Group Authorization to the mix forces the Server to return all attributes, from User & Group profiles combined (as it should be).

At the end I want to quickly discuss our ISE Authorization Profile – what we are saying there is that we want the Client to accept received IKEv2 routes and in addition one route we want to send is 10.214.214.0/24. This is not part of the requirements in this task but I just wanted to show you how to create RADIUS authorization profiles for FlexVPNs. Unfortunately it looks that current version of ISE does not include IETF attribute (88) "Framed-Pool" which could be used to assign an IPv4 pool to the Client/Spoke. More over it does not look like you can add an IETF attribute manually, which leaves us with only "Framed-IP-Address" and "Framed-IP-Netmask" as the only way to assign an IPv4 address from RADIUS.

The list of remaining attributes and Cisco AV syntax for IKEv2 can be found under FlexVPN Configuration Guide "Appendix FlexVPN RADIUS Attributes" document.

IPv6 Considerations

Apart from changing IP addresses to IPv6 everywhere, the tunnel interface (Client) would have to be configured with "`ipv6 address negotiated`". Hub's Virtual Template would use "`ipv6 unnumbered`" and loopback would be also configured with an IPv6 address rather than IPv4. On the Headend device we also need to define an IPv6 pool – you would use "`ipv6 local pool`" to accomplish this - then just assign it to the Authorization Group Policy ("`ipv6 pool`"). Last thing to remember about would be to change Split Tunneling ACLs to IPv6 and apply them via "`route set access-list ipv6`" in the Policies.

To check RADIUS attributes (including IPv6) that could be assigned to the User or Group Profile go to the FlexVPN Configuration Guide, "Appendix FlexVPN RADIUS Attributes" document.

Verification

First some basic config verifications:

```
R10#sh cry ikev2 profile default

IKEv2 profile: default
 Ref Count: 4
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities: none
  Certificate maps:
   CMAP4
 Local identity: key-id Prince
 Remote identity: none
 Local authentication method: eap
 Remote authentication method(s): rsa-sig
 EAP options: none
```

```
 Keyring: none
 Trustpoint(s):
  VPNTRUST
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization:
  cert: list FLEX_AUTHZ, username default
 AAA user authorization: none


R11#sh cry ikev profile default

IKEv2 profile: default
 Ref Count: 2
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   key-id Prince
  Certificate maps: none
 Local identity: DN
 Remote identity: none
 Local authentication method: rsa-sig
 Remote authentication method(s): eap
 EAP options: none
 EAP authentication timeout: 90 seconds
 Keyring: none
 Trustpoint(s):
  VPNTRUST
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: 51
 AAA EAP authentication mlist: EAPAUTH
 AAA Accounting: none
 AAA group authorization:
  eap: list FLEX_AUTHZ, username default
 AAA user authorization:
  eap: use cached attribs
  eap: list
```

Then let's take a look at IKEv2 SAs. Note that Mode Config information appears to be processed and used:

```
R10#sh cry ikev2 sa det
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         8.9.2.10/500          11.11.11.11/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: EAP, Auth
verify: RSA
      Life/Active Time: 86400/441 sec
      CE id: 1009, Session-id: 5
      Status Description: Negotiation done
      Local spi: 4BBC04202741762A       Remote spi: 6354C748649E6A64
      Local id: Prince
      Remote id:
hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL
      Local req msg id:  6              Remote req msg id:  0
      Local next msg id: 6              Remote next msg id: 0
      Local req queued:  6              Remote req queued:  0
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
      Pushed IP address: 10.50.50.25
      Remote subnets:
      10.50.50.11 255.255.255.255
      10.114.114.0 255.255.255.0
      10.214.214.0 255.255.255.0

 IPv6 Crypto IKEv2  SA


R11#sh cry ikev2 sa det
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         11.11.11.11/500       8.9.2.10/500          none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: EAP
      Life/Active Time: 86400/457 sec
      CE id: 1009, Session-id: 5
      Status Description: Negotiation done
      Local spi: 6354C748649E6A64       Remote spi: 4BBC04202741762A
      Local id:
hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL
      Remote id: Prince
      Remote EAP id: Prince
      Local req msg id:  0              Remote req msg id:  6
      Local next msg id: 0              Remote next msg id: 6
```

```
      Local req queued:  0              Remote req queued:  6
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Assigned host addr: 10.50.50.25
      Initiator of SA : No
      Remote subnets:
      10.50.50.25 255.255.255.255
      10.100.100.0 255.255.255.0
```

If we verify the RIB, however, it looks that only R11 added the IKEv2-reeived Routes to the routing table:

```
R11#sh ip route static | be Gat
Gateway of last resort is 10.4.11.4 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.4.11.4
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S        10.50.50.25/32 [2/0] via 0.0.0.0, Virtual-Access1
S        10.100.100.0/24 [2/0] via 0.0.0.0, Virtual-Access1


Mar  1 15:53:10.428: RT: updating static 10.50.50.26/32 (0x0):
    via 0.0.0.0 Vi1
Mar  1 15:53:10.428: RT: add 10.50.50.26/32 via 0.0.0.0, static metric [2/0]
Mar  1 15:53:10.428: RT: updating static 10.100.100.0/24 (0x0):
    via 0.0.0.0 Vi1
Mar  1 15:53:10.428: RT add 10.100.100.0/24 via 0.0.0.0, static metric [2/0]
Mar  1 15:53:25.903: RT: updating ospf 10.251.251.0/24 (0x0):
    via 10.50.50.26 Vi1
Mar  1 15:53:25.903: RT: add 10.251.251.0/24 via 10.50.50.26, ospf metric [110/2]
Mar  1 15:53:25.903: RT: updating ospf 10.50.50.0/24 (0x0):
    via 10.50.50.26 Vi1


R11#sh ip int br | in Access
Virtual-Access1            10.50.50.11     YES unset  up                    up
```

I am pretty certain that the problem we run into here is related to an IOS bug. All the route information was received from ISE/local Group Policy and was sent to R10. As we will see later R10 appears to be processing this information but the routes are not placed in the RIB (only the assigned IP address is considered):

```
Mar  1 15:53:10.416: is_up: Tunnel50 1 state: 4 sub state: 1 line: 0
Mar  1 15:53:10.416: RT: updating connected 10.50.50.0/24 (0x0):
    via 0.0.0.0 Tu50
Mar  1 15:53:10.416: RT: add 10.50.50.0/24 via 0.0.0.0, connected metric [0/0]
Mar  1 15:53:10.416: RT: interface Tunnel50 added to routing table
```

```
Mar  1 15:53:10.416: RT: updating connected 10.50.50.26/32 (0x0):
    via 0.0.0.0 Tu50
Mar  1 15:53:10.416: RT: add 10.50.50.26/32 via 0.0.0.0, connected metric [0/0]


R10#sh ip route static | be Gat
Gateway of last resort is not set

S     192.168.8.0/24 [1/0] via 8.9.2.30


R10#sh ip int br | in Tunnel
Tunnel3                unassigned      YES NVRAM  administratively down down
Tunnel20               unassigned      YES unset  administratively down down
Tunnel50               10.50.50.25     YES NVRAM  up                    up


R10#ping 10.114.114.11 rep 2
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 10.114.114.11, timeout is 2 seconds:
..
Success rate is 0 percent (0/2)

R10#ping 10.50.50.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.50.50.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Packets destined to VLAN114 are obviously not routed anywhere due to the lack of routing information. This is why IPSec counters are symmetric for Tunnel 50:

```
R10#sh cry sess int tu 50 det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel50
Uptime: 00:07:06
Session status: UP-ACTIVE
Peer: 11.11.11.11 port 500 fvrf: (none) ivrf: (none)
      Phase1_id:
hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL
      Desc: (none)
  IKEv2 SA: local 8.9.2.10/500 remote 11.11.11.11/500 Active
         Capabilities:(none) connid:1 lifetime:23:52:54
  IPSEC FLOW: permit 47 host 8.9.2.10 host 11.11.11.11
```

```
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 62 drop 0 life (KB/Sec) 4366127/3173
        Outbound: #pkts enc'ed 62 drop 0 life (KB/Sec) 4366127/3173


R11#ping 10.100.100.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.100.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

In-depth analysis of the exchange (only selected outputs are shown). R10 requests for an IP address, subnet mask and Split Tunneling/IKEv2 routes:

```
R10#
Mar  1 15:15:38.465: IKEv2:(SA ID = 1):Completed SA init exchange
Mar  1 15:15:38.465: IKEv2:Config data to send:
Mar  1 15:15:38.465: Config-type: Config-request
Mar  1 15:15:38.465: Attrib type: ipv4-addr, length: 0
Mar  1 15:15:38.465: Attrib type: ipv4-netmask, length: 0
                                                    …
Mar  1 15:15:38.465: Attrib type: ipv6-subnet, length: 0
```

Note IKEv2 ID is “Prince”. This will be then used as a username during EAP authentication:

```
Mar  1 15:15:38.465: IKEv2:(SA ID = 1):Sending ID payload without AUTH intend to do
EAP
Mar  1 15:15:38.465: IKEv2:(SA ID = 1):Constructing IDi payload: 'Prince' of type
'key ID'
```

The Profile is found, EAP exchange starts:

```
R11#
R11#5:15:38.476: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'Prince' of type 'key ID'
Mar  1 15:15:38.476: IKEv2:found matching IKEv2 profile 'default'

Mar  1 15:15:38.480: IKEv2:(SA ID = 1):My authentication method is 'RSA'
Mar  1 15:15:38.480: IKEv2:(SA ID = 1):Sign authentication data


Mar  1 15:15:38.488: IKEv2:(SA ID = 1):Asking the authenticator to send EAP request
Mar  1 15:15:38.492: IKEv2:Use authen method list EAPAUTH
Mar  1 15:15:38.492: IKEv2:sending Prince [IDi] as username to AAA
```

```
Mar  1 15:15:38.492: RADIUS(0000001A): Send Access-Request to 8.9.2.150:1645 id
1645/18, len 81
Mar  1 15:15:38.492: RADIUS:  authenticator 5A B9 F4 98 AA 81 08 D0 - 69 2C C5 9F 49
7D D9 BA
Mar  1 15:15:38.492: RADIUS:  Service-Type        [6]   6   Login
[1]
Mar  1 15:15:38.492: RADIUS:  Calling-Station-Id  [31
R11#]  10  "8.9.2.10"
Mar  1 15:15:38.492: RADIUS:  User-Name           [1]   8   "Prince"
Mar  1 15:15:38.492: RADIUS:  EAP-Message         [79]  13
Mar  1 15:15:38.492: RADIUS:   02 01 00 0B 01 50 72 69 6E 63 65            [ Prince]
Mar  1 15:15:38.492: RADIUS:  Message-Authenticato[80]  18
Mar  1 15:15:38.492: RADIUS:   4C 5F 2A D9 20 B0 D6 8A 63 2E A2 36 87 7C 38 39
[ L_* c.6|89]
Mar  1 15:15:38.492: RADIUS:  NAS-IP-Address      [4]   6   11.11.11.11


Mar  1 15:15:38.516: RADIUS: Received from id 1645/18 8.9.2.150:1645, Access-
Challenge, len 126
                                        …
Mar  1 15:15:38.516: RADIUS:  EAP-Message         [79]  8
Mar  1 15:15:38.516: RADIUS:   01 2A 00 06 0D 20               [ * ]
Mar  1 15:15:38.516: RADIUS:  Message-Authenticato[80]  18
Mar  1 15:15:38.516: RADIUS:   A7 2C C0
R11# D9 3A 2C 46 DC 03 D1 C3 AF 84 95 50 30           [ ,:,FP0]
Mar  1 15:15:38.516: RADIUS(0000001A): Received from id 1645/18
Mar  1 15:15:38.516: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Mar  1 15:15:38.516: IKEv2:(SA ID = 1):[AAA -> IKEv2] Successful response received

Mar  1 15:15:38.516: IKEv2:(SA ID = 1):Constructing IDr payload:
'hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL' of type
'DER ASN1 DN'
Mar  1 15:15:38.516: IKEv2:(SA ID = 1):Building packet for encryption.
```

The Profile is found on the Spoke. EAP exchange continues:

```
R10#
Mar  1 15:15:38.525: IKEv2:(SA ID = 1):Received Packet [From 11.11.11.11:500/To
8.9.2.10:500/VRF i0:f0]
Initiator SPI 4BBC04202741762A - Responder SPI : 6354C748649E6A64 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
 VID IDr CERT AUTH EAP

Mar  1 15:15:38.525: IKEv2:(SA ID = 1):Searching policy based on peer's identity
'hostname=R11.ipexpert.com,cn=R11.ipexpert.com,ou=INSTRUCTORS,l=Warsaw,c=PL' of type
'DER ASN1 DN'

Mar  1 15:15:38.529: IKEv2:Found matching IKEv2 profile 'default'
```

```
Mar  1 15:15:38.533: IKEv2:(SA ID = 1):Processing EAP request
Mar  1 15:15:38.533: IKEv2:Received response from authenticator
Mar  1 15:15:38.533: IKEv2:(SA ID = 1):Sending EAP response
Mar  1 15:15:38.533: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 EAP
```

Then we need to authenticate for EAP on R10:

```
R10#crypto eap credentials default
Enter the password for username Prince:


Mar  1 15:16:13.145: IKEv2:(SA ID = 1):Sending EAP response
Mar  1 15:16:13.145: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 EAP
```

Authentication data is passed by NAS to ISE (encapsulated in EAP):

```
R11#
Mar  1 15:16:13.148: RADIUS(0000001A): Send Access-Request to 8.9.2.150:1645 id
1645/20, len 172
Mar  1 15:16:13.148: RADIUS:  authenticator F7 5D B6 FD 36 B2 E4 B7 - 7D 4D 2D C8 77
B9 C3 D2
Mar  1 15:16:13.148: RADIUS:  Service-Type        [6]   6   Login
[1]
Mar  1 15:16:13.148: RADIUS:  Calling
R11#-Station-Id  [31]  10  "8.9.2.10"
Mar  1 15:16:13.148: RADIUS:  User-Name           [1]   8   "Prince"
Mar  1 15:16:13.148: RADIUS:  EAP-Message         [79]  24
Mar  1 15:16:13.148: RADIUS:   02 2B 00 16 04 10 8F 18 CA 07 F4 7B E6 DA 1E 23 14 F5
67 09 F7 21             [ +{#g!]
Mar  1 15:16:13.148: RADIUS:  Message-Authenticato[80]  18
Mar  1 15:16:13.148: RADIUS:   F4 99 33 F0 92 8D A8 18 82 8A D0 32 61 0D 05 20
[ 32a ]
Mar  1 15:16:13.148: RADIUS:  State               [24]  80
```

User is successfully authenticated, authorization information is returned according to the matched Profile:

```
Mar  1 15:16:13.172: RADIUS: Received from id 1645/20 8.9.2.150:1645, Access-Accept,
len 231
Mar  1 15:16:13.172: RADIUS:  authenticator 7F BD 66 38 85 0C 01 2A - 7C E1 EA E6 55
3B 52 D5
Mar  1 15:16:13.172: RADIUS:  User-Name           [1]   8   "Prince"
```

```
Mar  1 15:16:13.172: RADIUS:  State                 [24]  40
Mar  1 15:16:13.172: RADIUS:   52 65 61 75 74 68 53 65 7
R11#3 73 69 6F 6E 3A 30 61  [ReauthSession:0a]
Mar  1 15:16:13.172: RADIUS:   63 38 30 36 66 34 30 30 30 30 31 45 31 30 35 31
[c806f400001E1051]
Mar  1 15:16:13.172: RADIUS:   33 30 43 35 37 35            [ 30C575]
Mar  1 15:16:13.172: RADIUS:  Class                 [25]  57
Mar  1 15:16:13.172: RADIUS:   43 41 43 53 3A 30 61 63 38 30 36 66 34 30 30 30
[CACS:0ac806f4000]
Mar  1 15:16:13.176: RADIUS:   30 31 45 31 30 35 31 33 30 43 35 37 35 3A 70 6F
[01E105130C575:po]
Mar  1 15:16:13.176: RADIUS:   64
R11#31 32 34 69 73 65 2F 31 34 39 33 39 38 32 36  [d124ise/14939826]
Mar  1 15:16:13.176: RADIUS:   34 2F 33 31 39 37 34           [ 4/31974]
Mar  1 15:16:13.176: RADIUS:  Termination-Action  [29]  6   1
Mar  1 15:16:13.176: RADIUS:  EAP-Message         [79]  6
Mar  1 15:16:13.176: RADIUS:   03 2B 00 04                 [ +]
Mar  1 15:16:13.176: RADIUS:  Message-Authenticato[80]  18
Mar  1 15:16:13.176: RADIUS:   1F 73 20 32 76 48 EF 71 35 22 B9 2D 68 DC 1B 1C
[ s 2vHq5"-h]
Mar  1 15:16:13.176: RADIUS:  Vendor, Cisco       [26]  30
Mar  1 15:16:13.176: RADIUS:   Cisco AVpair       [1]   24  "ipsec:route-accept=any"
Mar  1 15:16:13.176: RADIUS:  Vendor, Cisco       [26]  46
Mar  1 15:16:13.176: RADIUS:   Cisco AVpair       [1]   40  "ipsec:route-set=prefix
10.214.214.0/24"
Mar  1 15:16:13.176: RADIUS(0000001A): Received from id 1645/20

Mar  1 15:16:13.176: IKEv2:Received response from authenticator
Mar  1 15:16:13.176: IKEv2:(SA ID = 1):Sending EAP status message
Mar  1 15:16:13.176: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 EAP
```

Now IKEv2 tunnel authentication occurs. The User ID was returned in EAP success (“Prince”), user’s password is used as PSK:

```
R10#
Mar  1 15:16:13.181: IKEv2:(SA ID = 1):Processing EAP status message
Mar  1 15:16:13.181: IKEv2:Received response from authenticator
Mar  1 15:16:13.181: IKEv2:(SA ID = 1):Send AUTH, to verify peer after EAP exchange
Mar  1 15:16:13.181: IKEv2:(SA ID = 1):Generate my authentication data
Mar  1 15:16:13.181: IKEv2:(SA ID = 1):Use preshared key for id Prince, key len 64
Mar  1 15:16:13.181: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Mar  1 15:16:13.181: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Mar  1 15:16:13.181: IKEv2:(SA ID = 1):Get my authentication method
Mar  1 15:16:13.181: IKEv2:(SA ID = 1):My authentication method is 'PSK'
```

```
R11#
Mar  1 15:16:13.188: IKEv2:(SA ID = 1):Verify peer's authentication data
Mar  1 15:16:13.188: IKEv2:(SA ID = 1):Use preshared key for id Prince, key len 64
Mar  1 15:16:13.188: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication
data
Mar  1 15:16:13.188: IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data
generation PASSED
Mar  1 15:16:13.188: IKEv2:(SA ID = 1):Verification of peer's authenctication data
PASSED
```

Now the Group Authorization starts:

```
Mar  1 15:16:13.188: IKEv2:Using mlist FLEX_AUTHZ and username default for group
author request
Mar  1 15:16:13.188: IKEv2:(SA ID = 1):[IKEv2 -> AAA] Authorisation request sent
Mar  1 15:16:13.188: IKEv2:(SA ID = 1):[AAA -> IKEv2] Received AAA authorisation
response

R11#
Mar  1 15:16:13.200: IKEv2:Config data to send:
Mar  1 15:16:13.200: Config-type: Config-reply
Mar  1 15:16:13.200: Attrib type: ipv4-addr, length: 4, data: 10.50.50.25
Mar  1 15:16:13.200: Attrib type: ipv4-netmask, length: 4, data: 255.255.255.0
Mar  1 15:16:13.200: Attrib type: ipv4-subn
R11#et, length: 8, data: 10.50.50.11 255.255.255.255
Mar  1 15:16:13.200: Attrib type: ipv4-subnet, length: 8, data: 10.114.114.0
255.255.255.0
Mar  1 15:16:13.200: Attrib type: ipv4-subnet, length: 8, data: 10.214.214.0
255.255.255.0
```

Note that R10 receives all authorization data, including IKEv2 routes. Only part of them were processed, as we saw during initial Verification, and the reason is once again (I am pretty certain) a bug on IOS. EAP comes with many caveats and there is still some unresolved issues as of this code release [15.2(3)T2]:

```
R10#
Mar  1 15:16:13.209: IKEv2:(SA ID = 1):Received valid config mode data
Mar  1 15:16:13.209: IKEv2:Config data recieved:
Mar  1 15:16:13.209: Config-type: Config-reply
Mar  1 15:16:13.209: Attrib type: ipv4-addr, length: 4, data: 10.50.50.25
Mar  1 15:16:13.209: Attrib type: ipv4-netmask, length: 4, data: 255.255.255.0
Mar  1 15:16:13.209: Attrib type: ipv4-subnet, length: 8, data: 10.50.50.11
255.255.255.255
Mar  1 15:16:13.209: Attrib type: ipv4-subnet, length: 8, data: 10.114.114.0
255.255.255.0
Mar  1 15:16:13.209: Attrib type: ipv4-subnet, length: 8, data: 10.214.214.0
255.255.255.0
```

```
Mar  1 15:16:13.209: Attrib type: app-version, length: 244, data: Cisco IOS
Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(3)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 26-Sep-12 07:24 by prod_rel_team
Mar  1 15:16:13.213: IKEv2:(SA ID = 1):Set received config mode data

R10#sh ip route static | be Gat
Gateway of last resort is not set

S     192.168.8.0/24 [1/0] via 8.9.2.30
```

Finally we are sending the Group Policy to the Hub so it can learn routes protected by R10 and the assigned IP address:

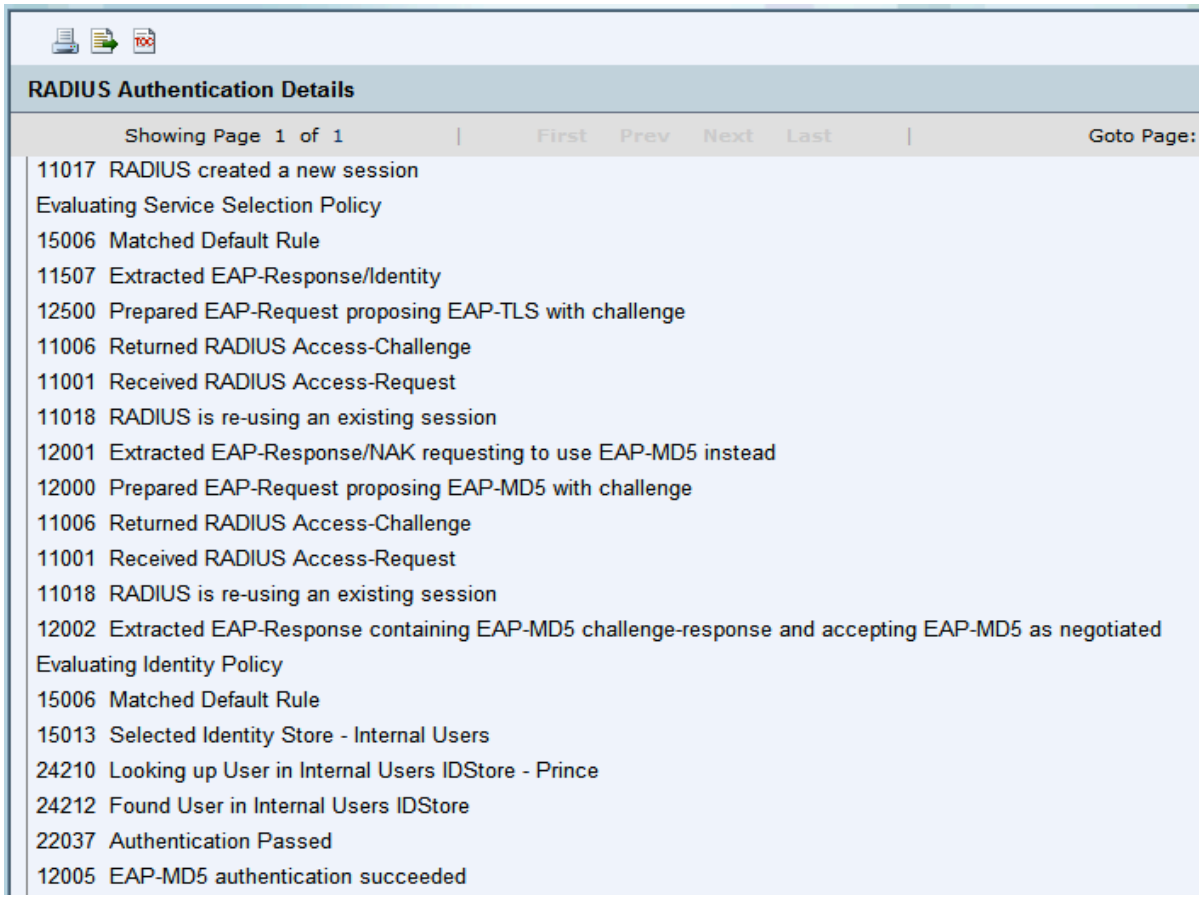
```
R10#
Mar  1 15:16:13.221: Config-type: Config-set
Mar  1 15:16:13.221: Attrib type: ipv4-subnet, length: 8, data: 10.50.50.25
255.255.255.255
Mar  1 15:16:13.221: Attrib type: ipv4-subnet, length: 8, data: 10.100.100.0
255.255.255.0
```

R11 processes the received information, and, as opposed to R10, updates the RIB:

```
R11#
Mar  1 15:16:13.228: IKEv2:Config data recieved:
Mar  1 15:16:13.228: Config-type: Config-set
Mar  1 15:16:13.228: Attrib type: ipv4-subnet, length: 8, data: 10.50.50.25
255.255.255.255
Mar  1 15:16:13.228: Attrib type: ipv4-subnet, length: 8, data: 10.100.100.0
255.255.255.0

Mar  1 15:16:13.228: IKEv2:(SA ID = 1):Set received config mode data


R11#sh ip route static | be Gat
Gateway of last resort is 10.4.11.4 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.4.11.4
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S        10.50.50.26/32 [2/0] via 0.0.0.0, Virtual-Access1
S        10.100.100.0/24 [2/0] via 0.0.0.0, Virtual-Access1


Mar  1 15:16:13.228: IKEv2:Config data to send:
Mar  1 15:16:13.228: Config-type: Config-ack
Mar  1 15:16:13.228: Attrib type: ipv4-subnet, length: 0
```

```
Mar  1 15:16:13.228: IKEv2:(SA ID = 1):Have config mode data to send
Mar  1 15:16:13.228: IKEv2:(SA ID = 1):Sending info exch config resp
Mar  1 15:16:13.228: IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
 CFG
```

Finally quick look at logs on ISE. All's good here:



Authentication Summary	
Logged At:	March 1,2013 3:13:27.934 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	Prince
MAC/IP Address:	8.9.2.10
Network Device:	R11 : 11.11.11.11 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	FLEXVPN_EAP_AUTHZ_PROFILE
SGA Security Group:	
Authentication Protocol :	EAP-MD5

⊟ Authentication Result

```
User-Name=Prince
 State=ReauthSession:0ac806f400001E105130C575
 Class=CACS:0ac806f400001E105130C575:pod124ise/149398264/31974
 Termination-Action=RADIUS-Request
 cisco-av-pair=ipsec:route-accept=any
 cisco-av-pair=ipsec:route-set=prefix 10.214.214.0/24
```

Section 8 Wireless

Section 8: Wireless is intended to let you be familiar with the Wireless technologies that are available on AP & WLC. You will be configuring WLC and features related to Wireless Security.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on Wireless technologies. You will need to pre-configure the network with the base configuration files

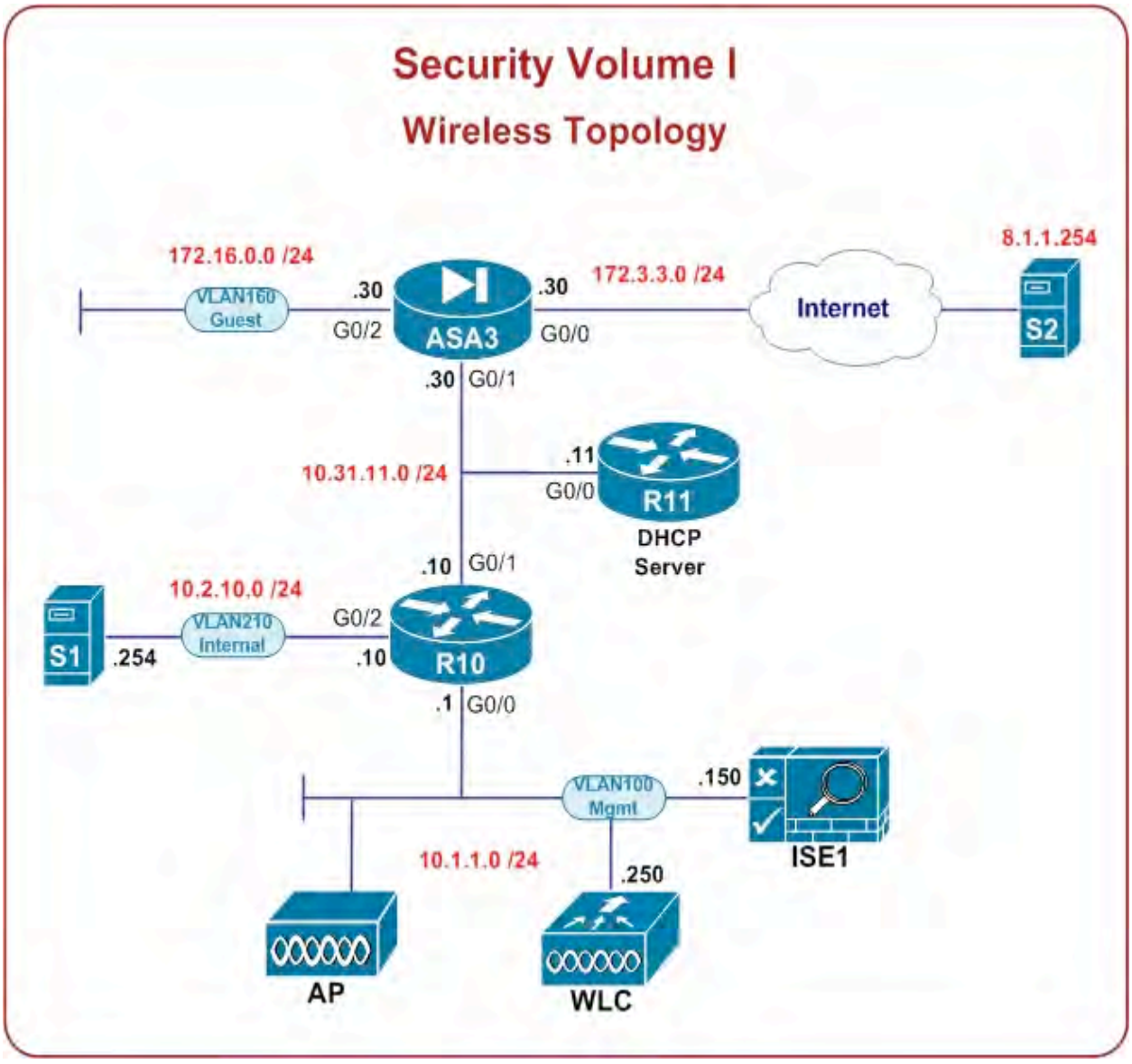
NOTE: Static/default routes are NOT allowed unless otherwise stated in the task

Estimated Time to Complete: **4 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R10	G0/0	100	10.1.1.1/24 2010:1:1::10/64
	G0/1	311	10.31.11.10/24
	G0/2	210	10.2.10.10/24
R11	G0/0	311	10.31.11.11/24
ASA3	G0/0	33	172.3.3.30/24
	G0/1	311	10.31.11.30/24
	G0/2	160	172.16.0.30/24
ISE	G0/0	100	10.1.1.150/24
WLC	Mgmt	100	10.1.1.250/24



Solutions

Task 1: WLC Initialization

- Initialize WLC using CLI
- Administrator name should be “admin”, password “IPexpert123”
- Management interface (Port #1) IP address should be set to 10.1.1.250
- DHCP Server IP address should be set to 10.1.1.250
- Virtual Gateway IP should be 1.250.250.250
- User Mobility/RF Group name “RFGROUP”

Detailed Solution

WLC

```
(Cisco Controller) reset system

Press <ESC> now to access the Boot Menu...

============================================================
 Boot Loader Menu
============================================================

 1. Run primary image (7.2.111.3) - Active
 2. Run backup image (7.0.220.0)
 3. Change active boot image
 4. Clear configuration
 5. Format FLASH Drive
 6. Manually update images

User:  Recover-Config
Initiating system recovery process... please wait

Rebooting system
Restarting system.


Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup


Would you like to terminate autoinstall? [yes]:

System Name [Cisco_b6:3d:84] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded WL
```

Configure username "**admin**" and password "**IPexpert123**". **Don't use any other credentials:**

```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): ***********
Re-enter Administrative Password                  : ***********

Management Interface IP Address: 10.1.1.250
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.1.1
Management Interface VLAN Identifier (0 = untagged): 100
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.1.1.250

Virtual Gateway IP Address: 1.250.250.250
route: SIOC[ADD|DEL]RT: File exists

Mobility/RF Group Name: RFGROUP
Network Name (SSID): IPx_Sec_Mgmt

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.
Please see documentation for more details.

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!
Resetting system with new configuration...
```

In the real lab it may turn out that WLC is already pre-configured for you. But it won't hurt to know what to do if things are not going the way (you think) they should. To trigger the Initialization dialog you must first reset WLC to its factory defaults.

Don't use any other credentials than "admin" and "IPexpert123".

NTP & RADIUS will be configured in other tasks.

Verification

```
(Cisco Controller) >show interface summary

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    100      10.1.1.250      Static  Yes    No
virtual                          N/A  N/A      1.250.250.250   Static  No     No
```

Task 2: WLC Basic Configuration

- Make sure you can access Controller using GUI
- Enable HTTP access to WLC
- Configure WLC to use NTP Server 10.1.1.101
- Any device in the management VLAN should be able to poll WLC using SNMP v1/2c
- AP should obtain an IP address from the internal DHCP pool (10.1.1.81-10.1.1.90)
- Create WLAN with SSID "IPx_Sec_Internal". Users connecting to this network should be placed in VLAN 210
- Create WLAN with SSID "IPx_Sec_Guests". Users connecting to this network should be placed in VLAN 160

CAT3

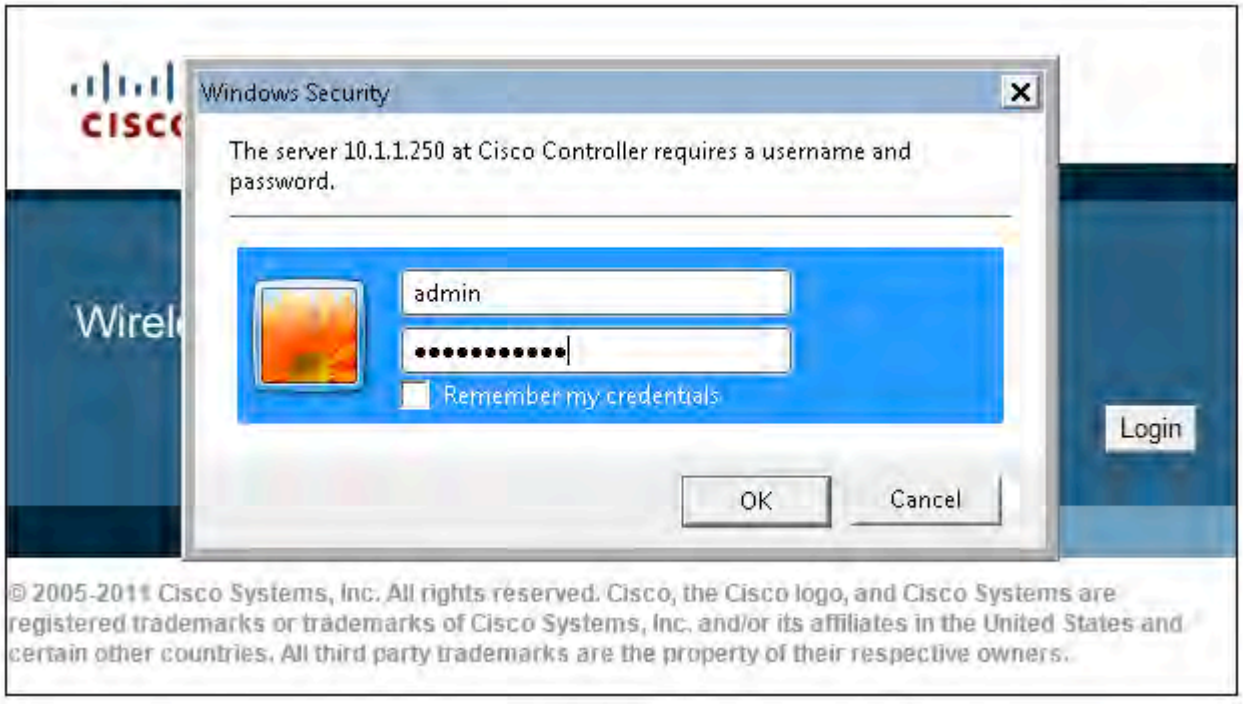
```
interface GigabitEthernet1/0/13
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
```

CAT4

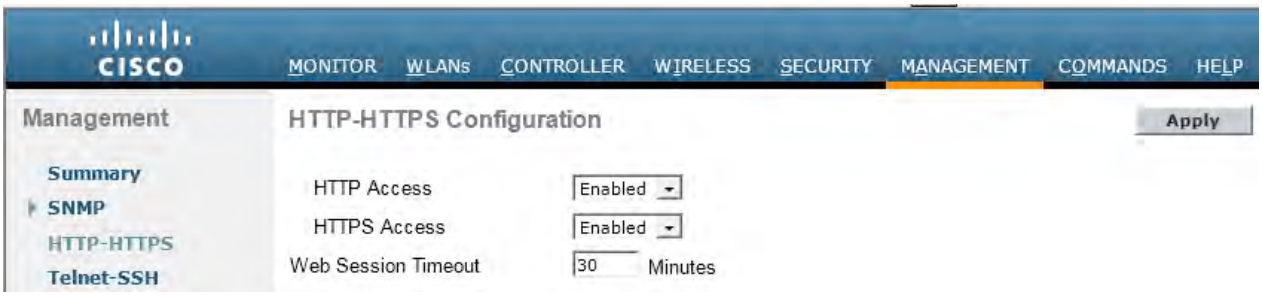
```
interface GigabitEthernet1/0/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,160,210
 switchport mode trunk
 spanning-tree portfast trunk
```

WLC

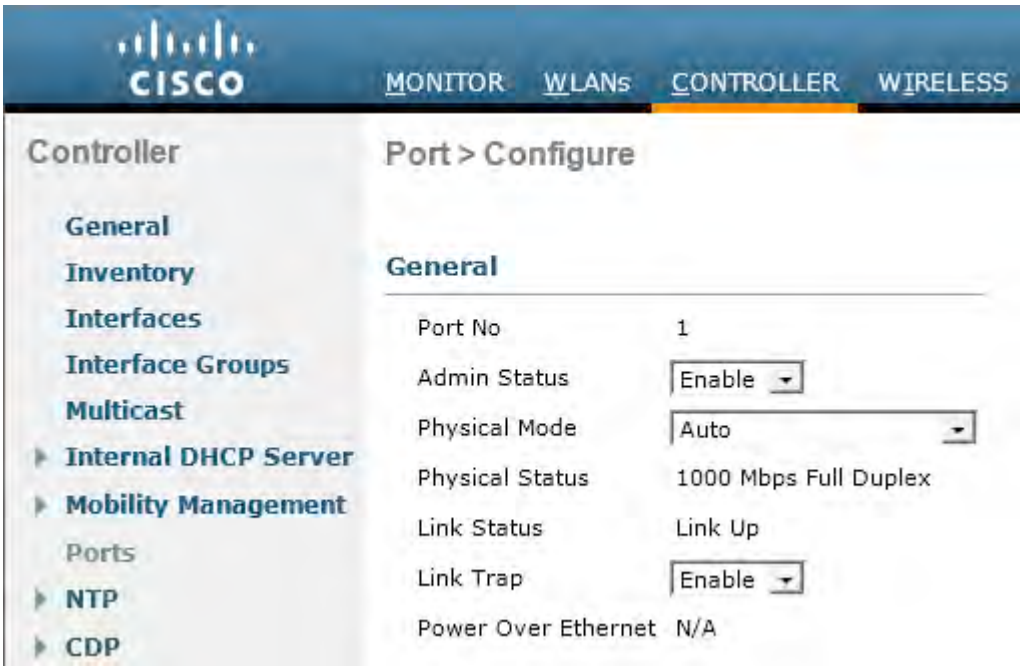
Put Test PC to VLAN 100, assign it an appropriate IP address and navigate to the management address of the Controller using a browser and HTTPs :



Configure HTTP, NTP & SNMP as per task requirements. Don't forget to apply the changes after each step:

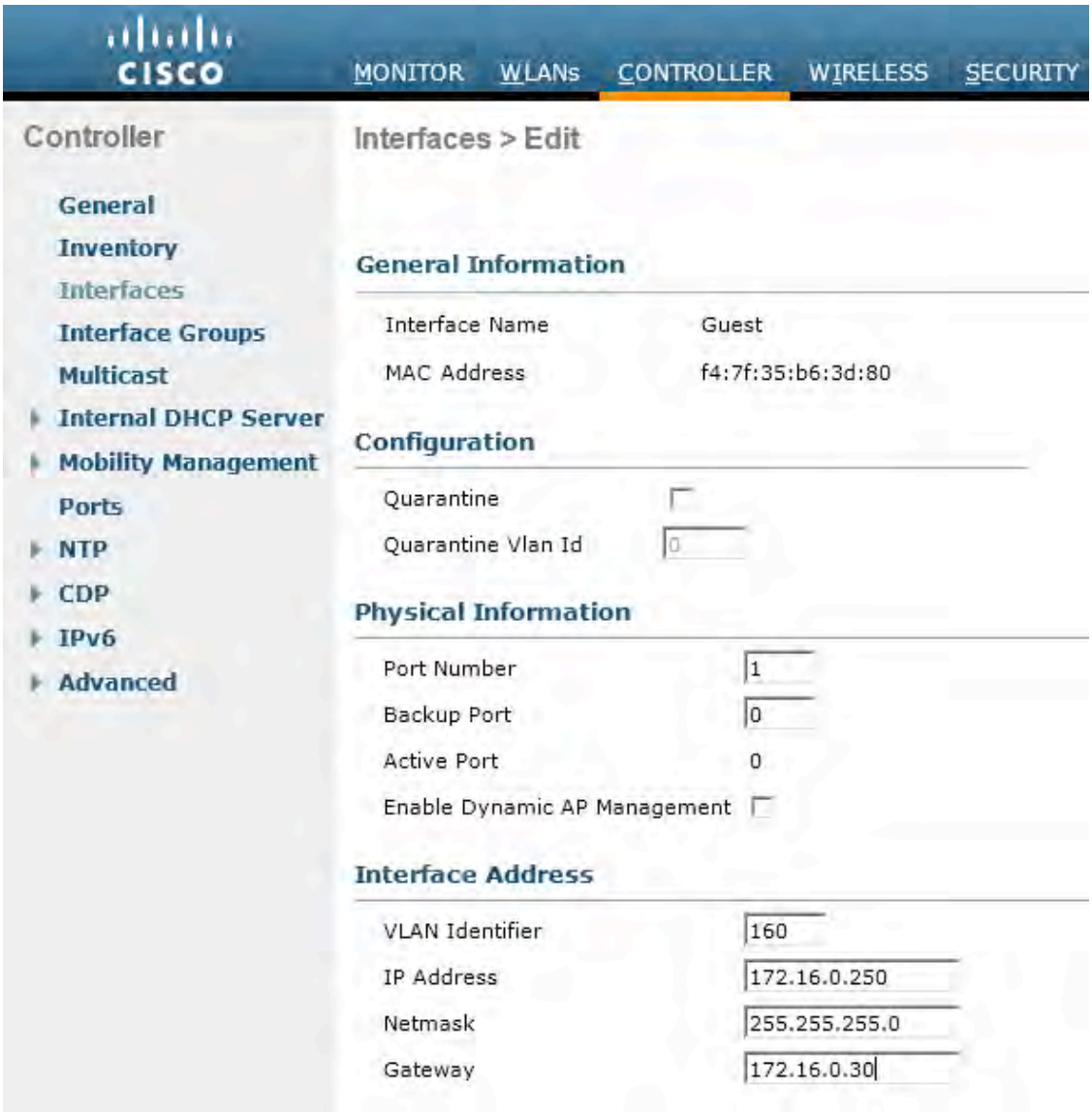


Make sure Port #1 is enabled:



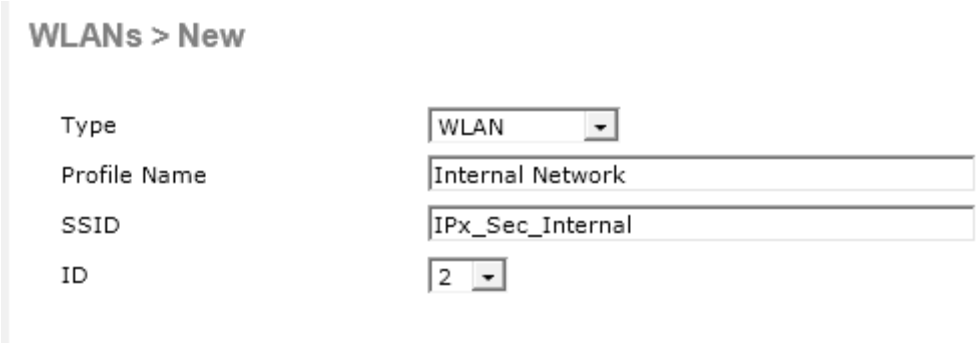
Create Dynamic Interface that will be used to handle Internal WLAN:

And one for Guest WLAN:

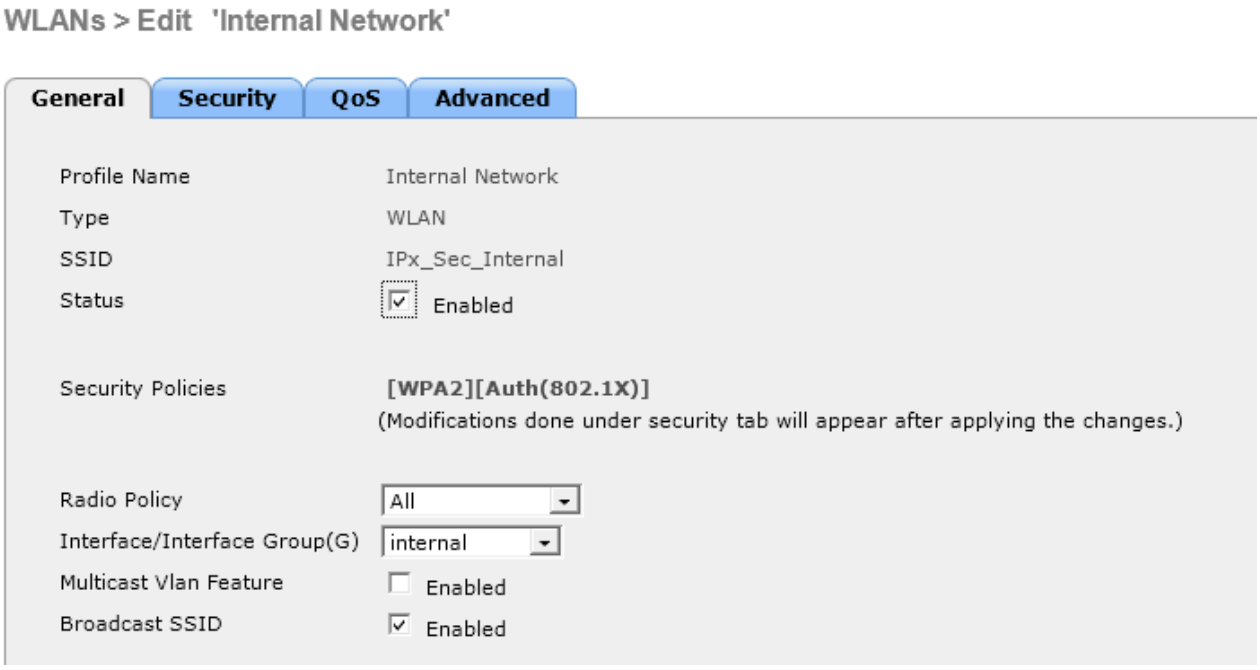


Now WLANs. Go to “WLANs” -> “WLANs”, choose “Create New” from the drop down menu and click on “Go”:

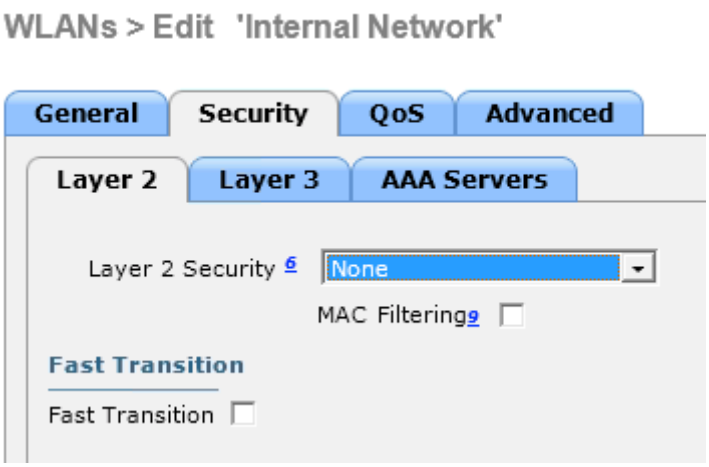
We start with “Internal”:



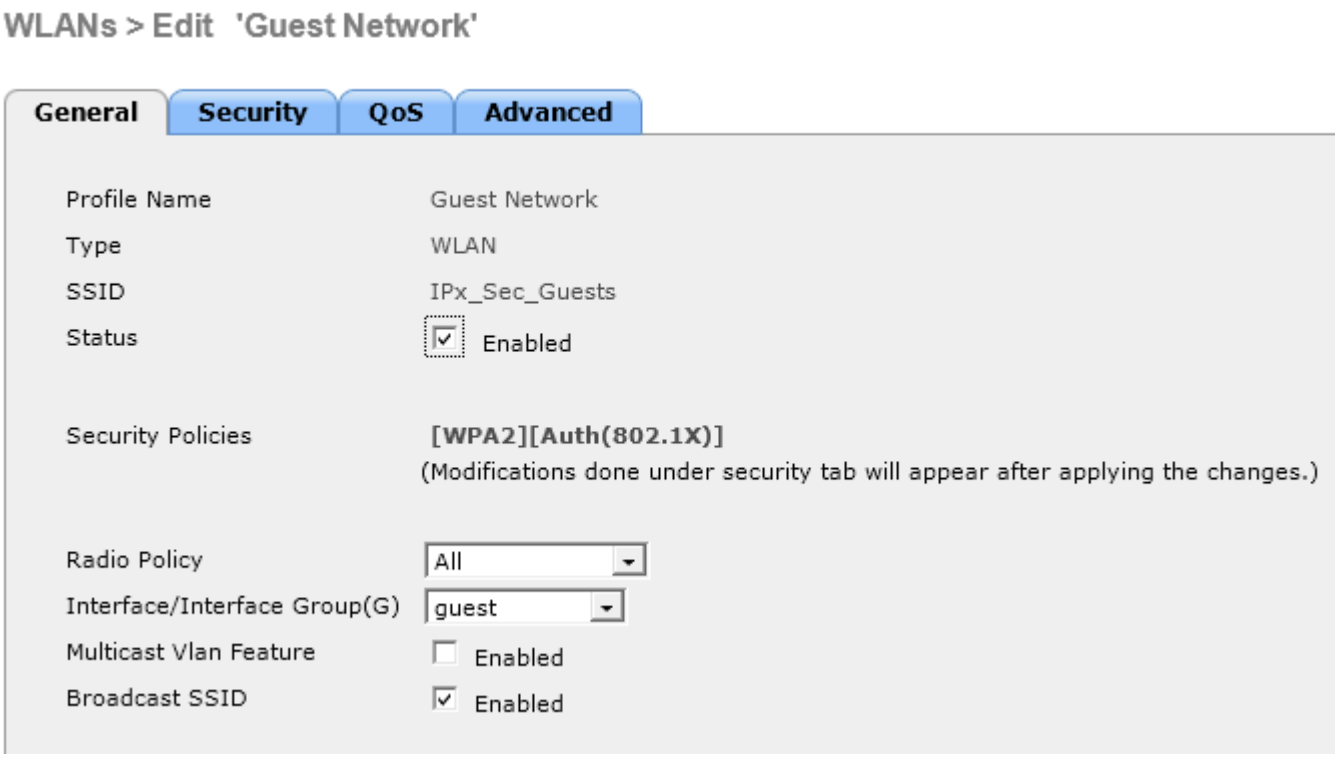
Make sure “Status” is checked and that the selected interface are “internal”. SSID should be broadcasted as well:

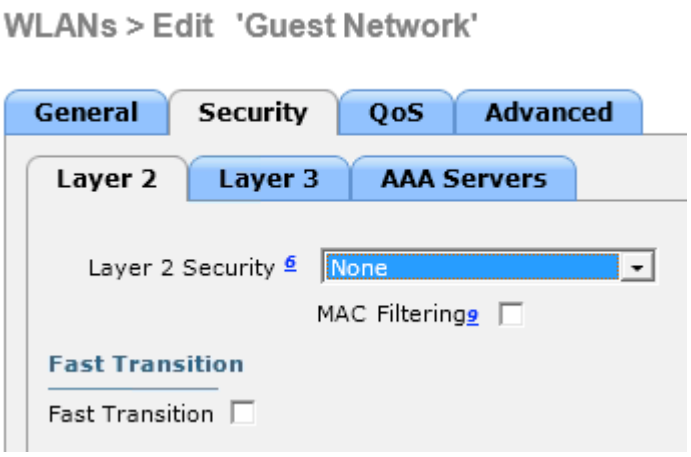


Layer 2 should be set to “None” and “MAC Filtering” checked off – we will not be adding any Security in this initial phase of the deployment:

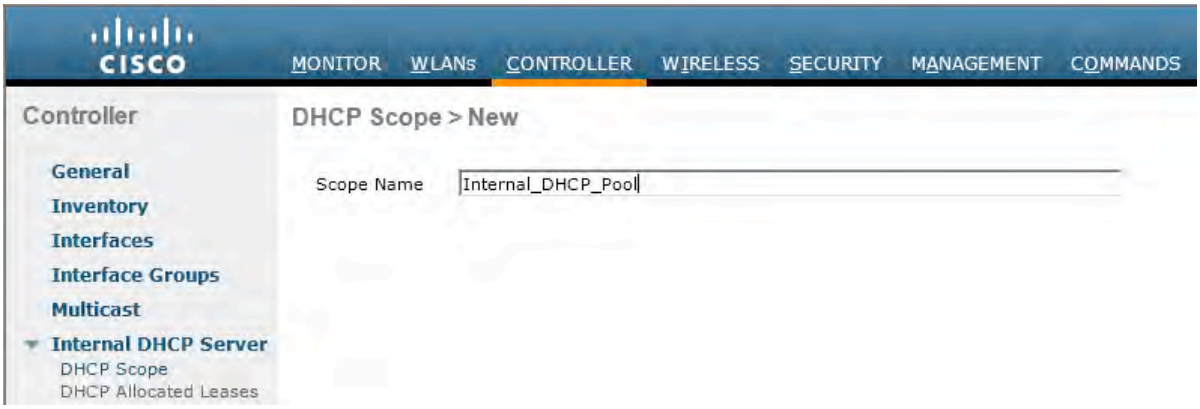


Now configure “Guest” WLAN in a similar way:

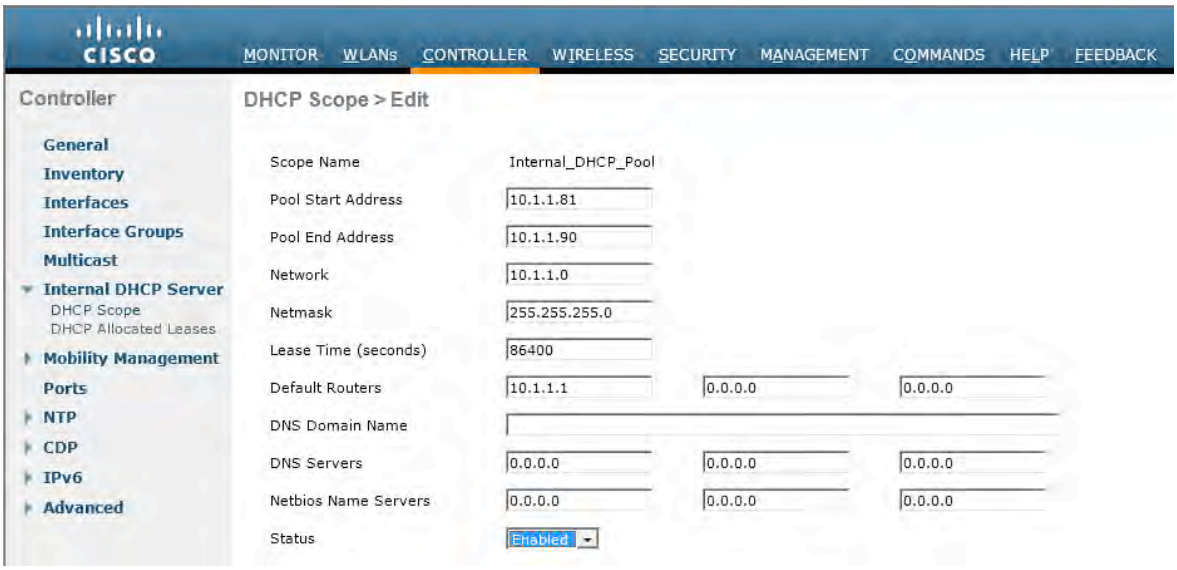




OK now we are going to focus on obtaining connectivity with an AP. Per the task requirements Access Point should obtain an IP address from the WLC itself (internal DHCP pool). Let's create one:

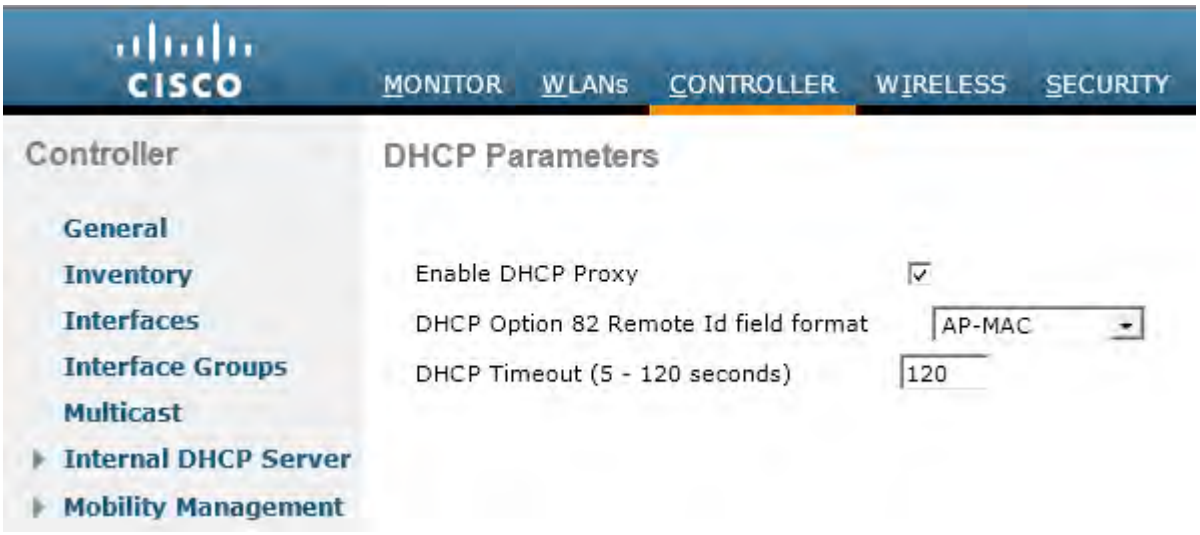


Our Access Point will only use this Pool so we can safely add a default gateway pointing to R10. Don't forget to enable it:



Now we need to point to the management interface IP address on the WLAN we want to use the internal pool[s]. In our case this is going to be the management interface/WLAN:

And the last thing you want to make sure is enabled is the DHCP Proxy mode. It must be “on” for the internal allocation to work:



After WLC was initialized it may be a good idea to first focus on the configuration required for an AP to join the Controller. And what we will need here is to make sure that AP gets assigned an IP address (which in our case, and also in vast majority of real-world deployments, is going to happen via DHCP) and that the underlying L2 network configuration is correct.

We are going to be using a single physical port on WLC, which will be configured to support subinterfaces, which means that the corresponding switchport must be an 802.1q trunk. As a best practice (to increase the Controller's performance) switch should only allow traffic for VLANs WLC will be bridging for, which in our case are management (100), Internal (210) and Guest (160). Access point to goes to VLAN 100, according to our diagram.

What we are going to be dealing with in this workbook is a so-called CUWN or just Controller (WLC) - based architecture. This means that APs no longer need to be individually configured; instead a WLC along with CAPWAP protocol (Control And Provisioning of Wireless Access Points) is used to provide centralized management and configuration. CAPWAP is an IETF standards-based version of LWAPP for communications between the lightweight AP and the WLC. Think of CAPWAP as a superset of LWAPP, which was the original Cisco controller- to-AP protocol and is the foundation for CAPWAP.

With CAPWAP, when an AP boots up it must first discover WLC through a CAPWAP Discovery Request message. The "hunting" process uses few different techniques to learn about WLC:

1. AP sends a L3 broadcast to the local subnet. For this to work an AP and WLC must be in the same L2 network

2. The AP attempts to utilize a locally stored IP address. It is possible to statically assign WLC information in the APs using a console connection or through the WLC if the AP in question has been associated with a controller in the past
3. AP remembers the last IP address of the WLC it was connected in the past, it will try it as well
4. You can also program DHCP servers to return WLC IP addresses in the vendor-specific "Option 43" in the DHCP offer to LAPs
5. The AP utilizes Domain Name System (DNS) resolution to find the WLC. The access point will attempt to resolve “CISCO-LWAP-CONTROLLER.localdomain” or “CISCO-CAPWAP-CONTROLLER.localdomain.”
6. If a WLC is not discovered, the process is repeated until a WLC is discovered

For situations when AP is located off the local subnet one more thing you could do, would be to configure a router to forward L3 broadcast Discovery Request message to the WLC as unicast (`ip helper-address` *`wlc_IP`*+`ip forward-protocold udp 5246`).

One’s WLCs were discovered, AP will Join a Controller by using some internal algorithm to choose between the WLCs. In our case there will be always one WLC and this device will be always selected.

HTTP was enabled just to show you the option, same as SNMP. NTP, however, is way more important – the discovery process is dependent upon security handshakes that are dependent upon accurate timestamps.

Now just few words about WLC interfaces:

1. Management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points (CAPWAP tunnel)
2. Dynamic interfaces, also known as VLAN interfaces, are created by users and designed to be analogous to VLANs for wireless LAN clients. A controller can support up to 512 dynamic interfaces (VLANs)
3. Virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication and VPN termination. It also acts as the DHCP server placeholder for wireless clients that obtain their IP address from a DHCP server. For the system to operate correctly, a virtual interface IP address must be set (it cannot be 0.0.0.0), and no other device on the network can have the same address as the virtual interface. It must be configured with an unused address and this address should not exist in any routing table in your network

To enable the internal DHCP Server function on WLC make sure that “DHCP Proxy” box is checked. Also on the interface you will have the DHCP clients connecting you must point to the IP address of the management interface of WLC as an IP address of the DHCP Server.

Verification

```
(Cisco Controller) >show time

Time.......................................... Mon Mar  4 17:34:15 2013

Timezone delta................................ 0:0
Timezone location.............................

NTP Servers
    NTP Polling Interval.....................     86400

     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              0          10.1.1.101        AUTH DISABLED
```

We will not be testing this configuration in this task. Just a quick recap on things we can verify without connecting – starting with interface & WLAN summary:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
guest	160	172.16.0.250	Dynamic	Disabled
internal	210	10.2.10.250	Dynamic	Disabled
management	100	10.1.1.250	Static	Enabled
virtual	N/A	1.250.250.250	Static	Not Supported

Then we definitely want to see if AP joined the Controller (“Monitor” tab). You can also take a look at the allocated addresses (Controller->Internal DHCP Server->DHCP Allocated Leases):

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	1	1	0	Detail
802.11b/g/n Radios	1	1	0	Detail
All APs	1	1	0	Detail

DHCP Allocated Lease

Entries 1 - 1 of 1

MAC Address	IP Address	Lease Remaining Time
00:1f:ca:26:c3:26	10.1.1.81	20 h 10 m 57 s

And finally our two WLANs appear to be available:

Task 3: DHCP Proxy Mode

- Clients connecting to the Internal WLAN should obtain an IP address via DHCP
- Configure WLC to support this requirement
- WLC should act as a Proxy for client messages
- Treat R10 as a DHCP Server

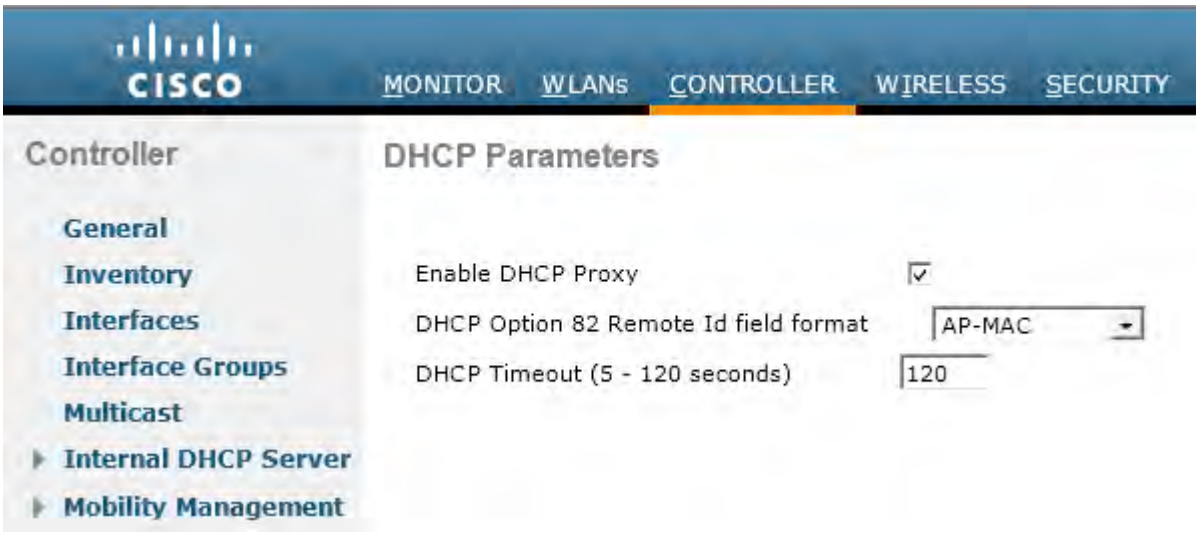
R10

```
ip dhcp excluded-address 10.2.10.10

ip dhcp pool INTERNALPOOL
 network 10.2.10.0 255.255.255.0
```

WLC

Just go back to the Interface settings and specify an IP address of the appropriate DHCP Server (WLC must know how to get there which in our case it knows because the devices are directly connected):

And last thing to remember about is that for the DHCP Proxy Mode we always want to make sure that the “Enable DHCP Proxy” box is checked:

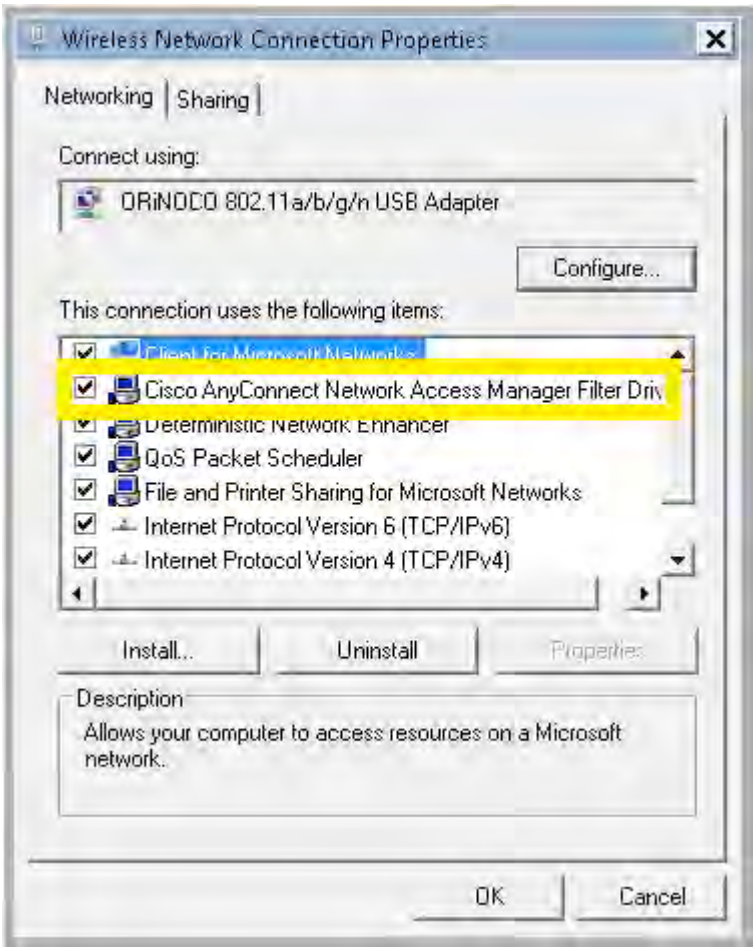


In the previous task it was shown how to enable and use the Internal DHCP Pool managed by WLC, but two main DHCP modes on the controller are DHCP Proxy and DHCP Bridging.

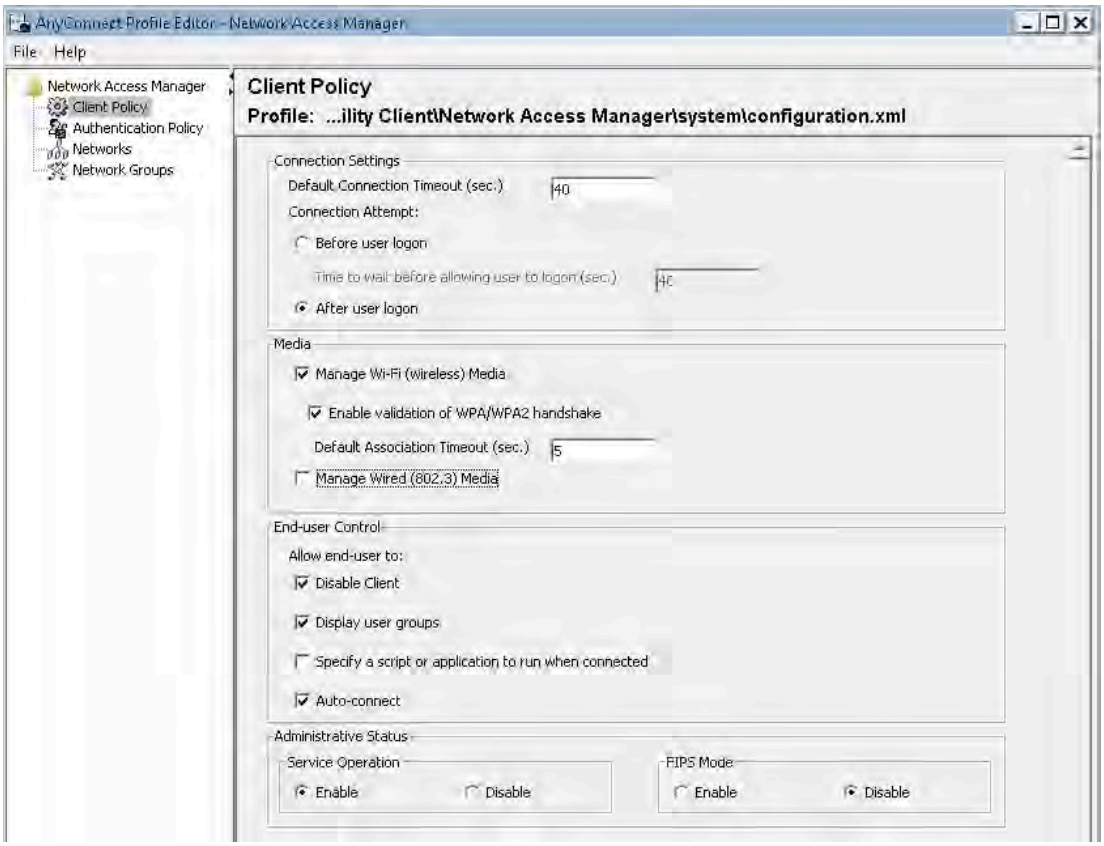
The default mode is to proxy all of the DHCP requests and unicast them on to the configured DHCP servers. In this mode, the wireless client DHCP broadcasts never make it past the WLC onto the wired network. Which DHCP servers get the forwarded broadcasts is determined by the Interface the client is associated to. On the Interface config in the WLC, you can specify up to 2 DHCP servers. You can also override the Interface config using the options on a given WLAN's Advanced tab.

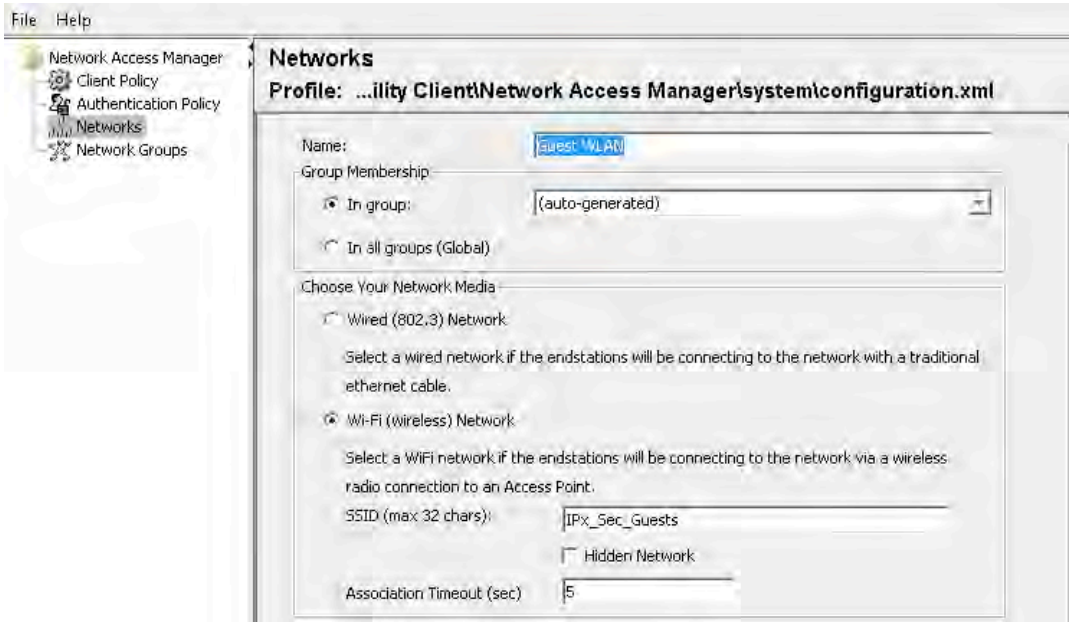
Verification

Time to test our configuration. We are going to use AnyConnect Network Manager module but for this to work we need to first configure a Profile. Open up “Network Access Manager Profile Editor” and then click on “File -> Open” and select the “configuration.xml” file in the “system” folder. This is the default config file, which we will edit to fit our needs. You must also make sure that AnyConnect manages the Wireless NIC:

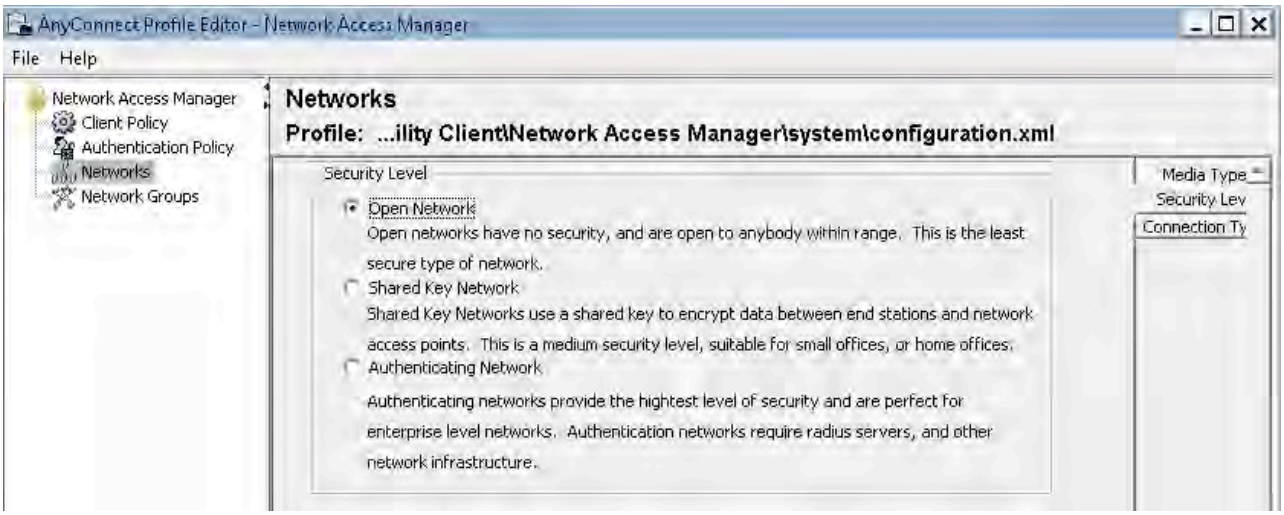


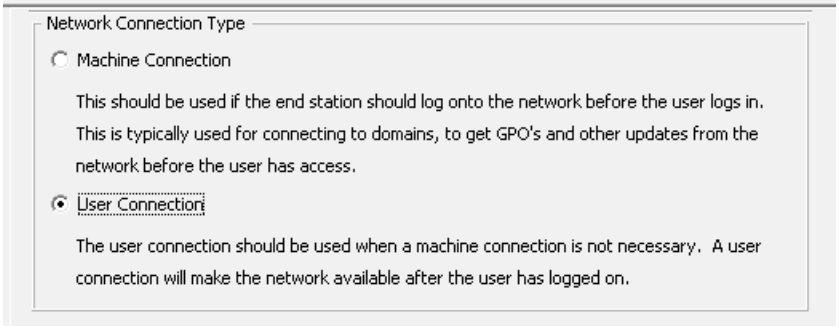
We will start with adding two entries, one for “IPx_Sec_Internal” and the other one for “IPx_Sec_Guests” SSIDs:



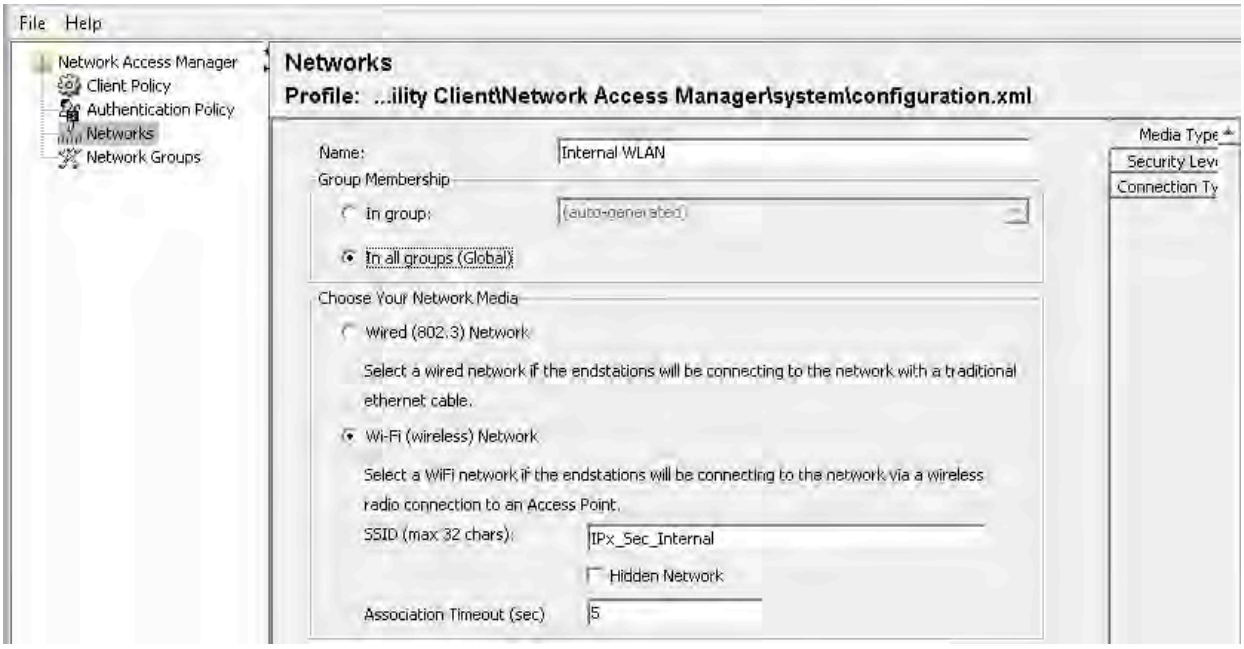


No security as of right now:





Then add an entry for the "Internal" WLAN. One difference is that we will put it in the "In all Groups (Global)" – this way Internal connection will be showing up first in the AnyConnect Network drop-down menu. All other settings should be configured as for the Guest WLAN (not shown here):



So the changes take effect you MUST save the file and right-click on the AnyConnect icon in the tray and then on the “Network Repair”. This is going to fetch the new Profile to the Client. Time for verification – we will try to connect and observer the DHCP debug on WLC:


```
(Cisco Controller) >debug dhcp message enable

*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP DISCOVER
*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP option: 61 (len 7) -
skipping
*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP option: hostname =
WIN7-PC1 (len 8)
*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP option: vendor class
id = MSFT 5.0 (len 8)
*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP option: 55 (len 12) -
skipping
*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64
```

It is the WLC what forwards the DISCOVERY packet to R10 (as unicast, similar to a DHCP Relay Agent):

```
*DHCP Socket Task: Mar 04 22:48:32.049: 00:20:a6:ca:77:38 DHCP Forwarding DHCP
packet (332 octets)                    -- packet received on direct-connect port
requires forwarding to external DHCP server. Next-hop is 10.2.10.10
```

We’ve got an offer back from R10, then REQUEST comes in:

```
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
```

```
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option:
message type = DHCP OFFER
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option: server id =
10.2.10.10
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option: lease time =
86400 seconds
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option: 58 (len 4) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option: 59 (len 4) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP option: netmask =
255.255.255.0
*DHCP Socket Task: Mar 04 22:48:34.047: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64

*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 97*
DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: message type =
DHCP REQUEST
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: 61 (len 7) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: requested ip
= 10.2.10.1
```

Note WLC changed the Server ID to the Virtual Gateway IP address:

```
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: server id =
1.250.250.250
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: hostname =
WIN7-PC1 (len 8)
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: 81 (len 24) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: vendor class
id = MSFT 5.0 (len 8)
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP option: 55 (len 12) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.051: 00:20:a6:ca:77:38 DHCP options end, len 97,
actual 89

*DHCP Socket Task: Mar 04 22:48:34.052: 00:20:a6:ca:77:38 DHCP Forwarding DHCP
packet (356 octets)                    -- packet received on direct-connect port
requires forwarding to external DHCP server. Next-hop is 10.2.10.10
```

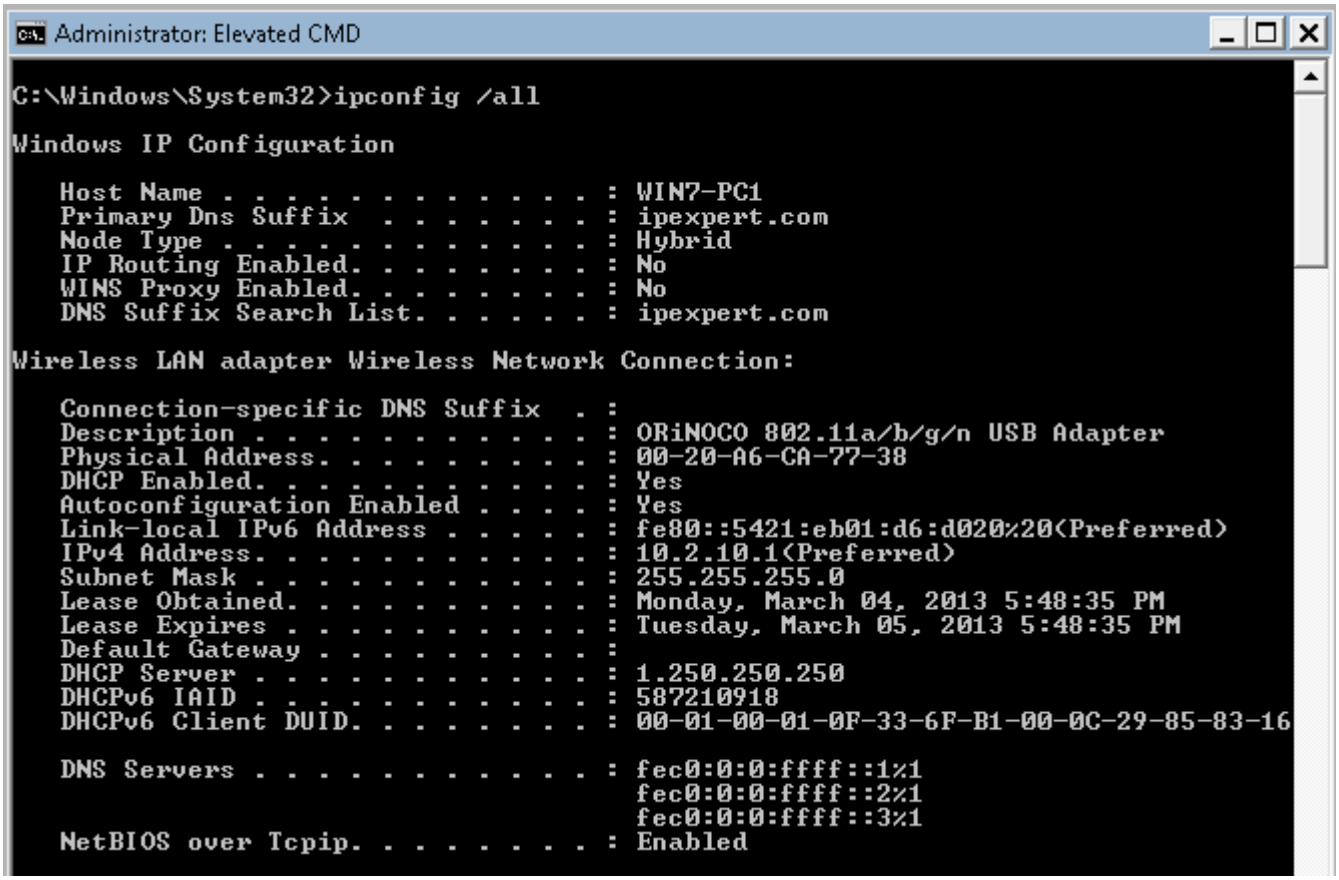
Finally ACK, INFORM (to ask for some additional options such as DNS Server or default gateway IP address), ACK and the transaction is finished:

```
*DHCP Socket Task: Mar 04 22:48:34.052: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
```

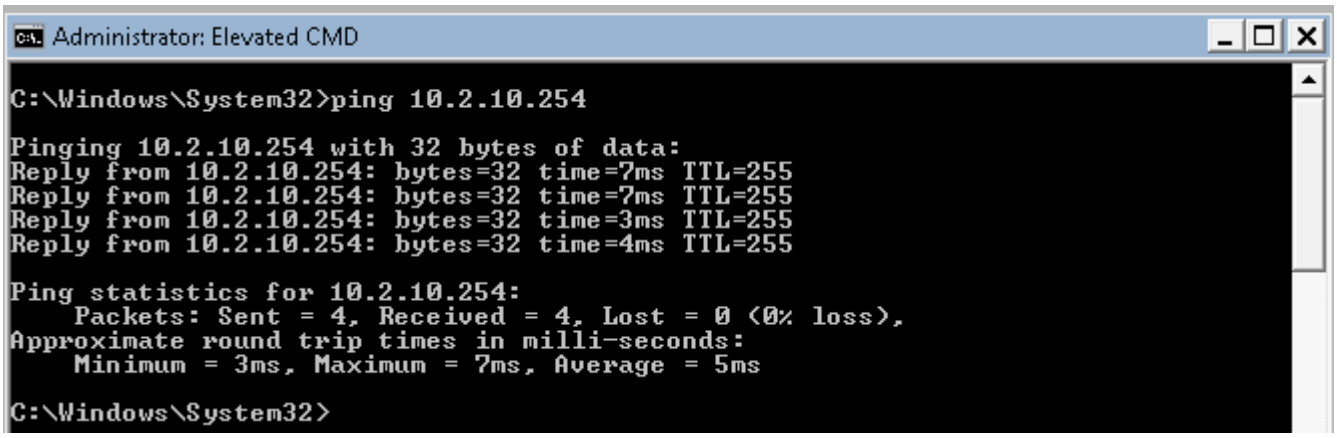
```
*DHCP Socket Task: Mar 04 22:48:34.052: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP ACK
*DHCP Socket Task: Mar 04 22:48:34.052: 00:20:a6:ca:77:38 DHCP option: server id =
10.2.10.10
*DHCP Socket Task: Mar 04 22:48:34.053: 00:20:a6:ca:77:38 DHCP option: lease time =
86400 seconds
*DHCP Socket Task: Mar 04 22:48:34.053: 00:20:a6:ca:77:38 DHCP option: 58 (len 4) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.053: 00:20:a6:ca:77:38 DHCP option: 59 (len 4) -
skipping
*DHCP Socket Task: Mar 04 22:48:34.053: 00:20:a6:ca:77:38 DHCP option: netmask =
255.255.255.0
*DHCP Socket Task: Mar 04 22:48:34.053: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64

*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP INFORM
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP option: 61 (len 7) -
skipping
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP option: hostname =
WIN7-PC1 (len 8)
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP option: vendor class
id = MSFT 5.0 (len 8)
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP option: 55 (len 13) -
skipping
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64
```

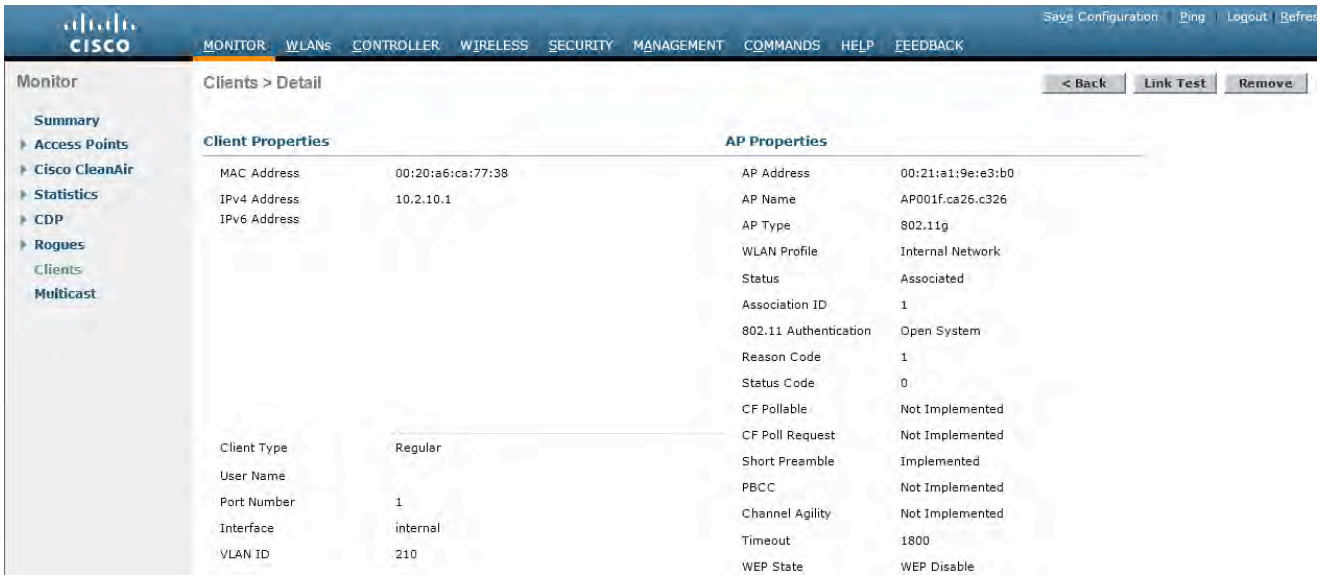
Forward INFORM. Since no other options were configured on the server there is nothing to return but the network mask:

```
*DHCP Socket Task: Mar 04 22:48:37.384: 00:20:a6:ca:77:38 DHCP Forwarding DHCP
packet (332 octets)                    -- packet received on direct-connect port
requires forwarding to external DHCP server. Next-hop is 10.2.10.10

*DHCP Socket Task: Mar 04 22:48:37.385: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
*DHCP Socket Task: Mar 04 22:48:37.385: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP ACK
*DHCP Socket Task: Mar 04 22:48:37.385: 00:20:a6:ca:77:38 DHCP option: server id =
10.2.10.10
*DHCP Socket Task: Mar 04 22:48:37.385: 00:20:a6:ca:77:38 DHCP option: netmask =
255.255.255.0
*DHCP Socket Task: Mar 04 22:48:37.385: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64
```



And we have connectivity within the network:





Task 4: DHCP Bridging Mode

- Clients connecting to Guest WLAN should obtain an IP address via DHCP
- Configure WLC to support this requirement
- WLC should act as a Bridge for client messages
- Treat R11 as a DHCP Server

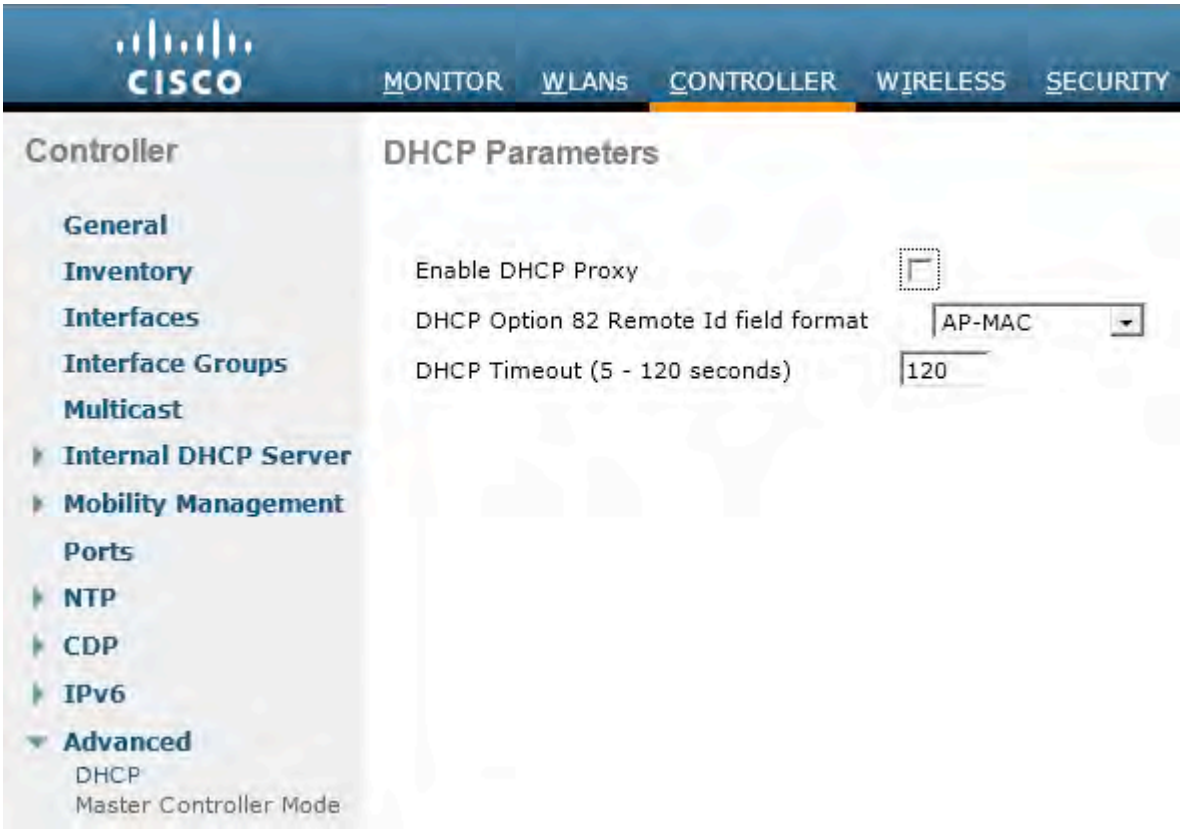
R11

```
ip dhcp excluded-address 172.16.0.30

ip dhcp pool GUESTPOOL
 network 172.16.0.0 255.255.255.0
```

ASA3

```
dhcprelay server 10.31.11.11 inside
dhcprelay enable GUEST
```

WLC



The DHCP Bridging feature is designed to make the controller's role in the DHCP transaction entirely transparent to the client. With the exception of 802.11 to Ethernet II conversion, packets from the client are bridged unmodified from the CAPWAP tunnel to the client's VLAN. Similarly, with the exception of Ethernet II to 802.11 conversion, packets to the client are bridged unmodified from the client's VLAN to the CAPWAP tunnel. Think of this as wiring a client into a switchport and the client performing a traditional DHCP transaction.

When you turn off the Proxy mode, the WLC will then allow the client DHCP broadcasts to flow onto the wired network where an "`ip helper-address`" on an SVI/routed port can forward the request onto the DHCP server. This is the only way to use more than 2 DHCP servers. This is a common option to use when you want to get profiling info over to ISE.

In our case since we are using ASA, the command to enable DHCP Relay function is actually "`dhcprelay`" and not "`ip helper-address`".

Verification

This configuration does not break previous task because R10 will still see the DISCOVERY packet in VLAN 210 after Proxy Mode is disabled (only part of the debug is shown):

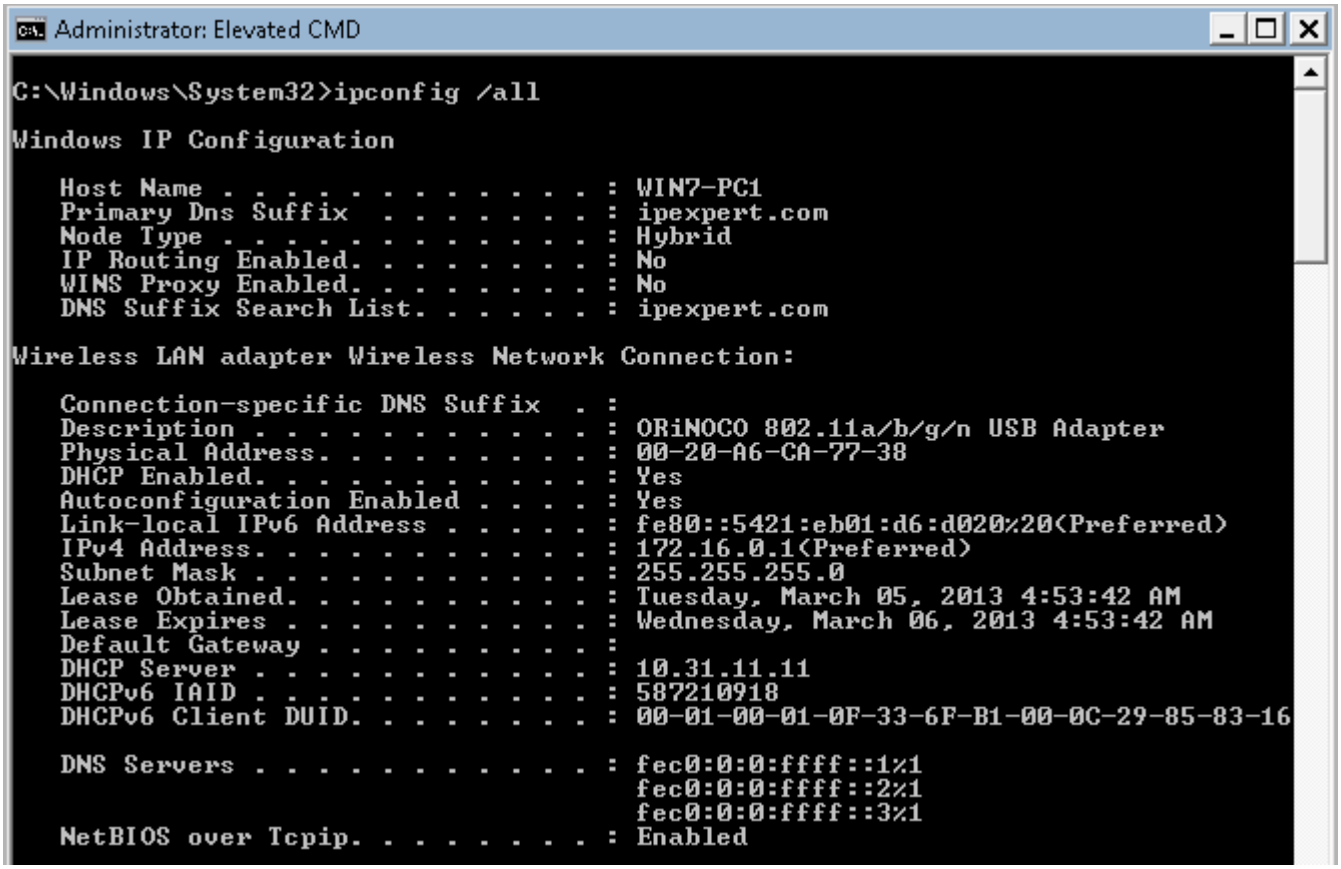
```
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP DISCOVER
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP option: 61 (len 7) -
skipping
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP option: requested ip
= 10.2.10.1
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP option: hostname =
WIN7-PC1 (len 8)
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP option: vendor class
id = MSFT 5.0 (len 8)
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP option: 55 (len 12) -
skipping
*DHCP Socket Task: Mar 05 10:25:40.481: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64

*DHCP Socket Task: Mar 05 10:25:42.480: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP OFFER
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP option: server id =
10.2.10.10
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP option: lease time =
86400 seconds
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP option: 58 (len 4) -
skipping
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP option: 59 (len 4) -
skipping
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP option: netmask =
255.255.255.0
*DHCP Socket Task: Mar 05 10:25:42.481: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64

*DHCP Socket Task: Mar 05 10:25:42.485: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 97
*DHCP Socket Task: Mar 05 10:25:42.485: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP REQUEST
```

The situation is going to be a little bit different in Guest WLAN. DHCP packets will be still bridged to the VLAN but since the ASA is configured as a Relay Agent, it will forward the packets to VLAN 311 (R11):

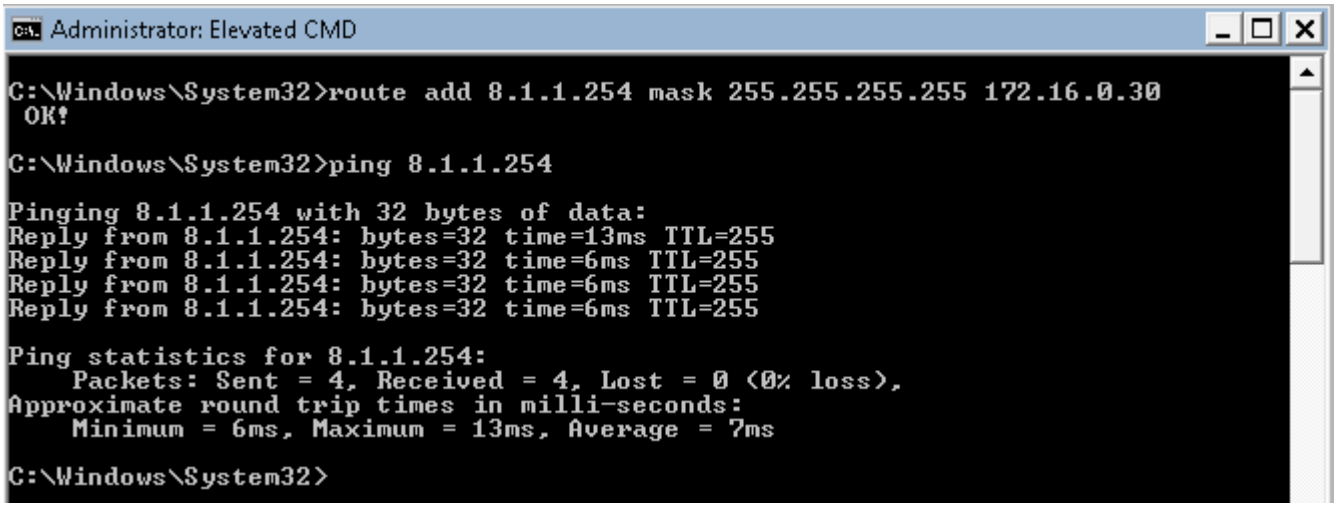

```
*DHCP Socket Task: Mar 05 09:39:40.801: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP DISCOVER
*DHCP Socket Task: Mar 05 09:39:40.801: 00:20:a6:ca:77:38 DHCP option: 61 (len 7) -
skipping
*DHCP Socket Task: Mar 05 09:39:40.801: 00:20:a6:ca:77:38 DHCP option: hostname =
WIN7-PC1 (len 8)
*DHCP Socket Task: Mar 05 09:39:40.801: 00:20:a6:ca:77:38 DHCP option: vendor class
id = MSFT 5.0 (len 8)
*DHCP Socket Task: Mar 05 09:39:40.801: 00:20:a6:ca:77:38 DHCP option: 55 (len 12) -
skipping
*DHCP Socket Task: Mar 05 09:39:40.801: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64

R11#
*Mar  5 09:57:00.559: DHCPD: DHCPDISCOVER received from client 0100.20a6.ca77.38
through relay 172.16.0.30.
*Mar  5 09:57:00.559: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 09:57:00.559:   DHCPD: htype 1 chaddr 0020.a6ca.7738
*Mar  5 09:57:00.559:   DHCPD: remote id 020a00000a1f0b0b00000000
*Mar  5 09:57:00.559:   DHCPD: circuit id 00000000
*Mar  5 09:57:00.559: DHCPD: Allocate an address without class information
(172.16.0.0)
*Mar  5 09:57:00.559: DHCPD: Adding binding to radix tree (172.16.0.1)
*Mar  5 09:57:00.559: DHCPD: Adding binding to hash tree
*Mar  5 09:57:00.559: DHCPD: assigned IP address 172.16.0.1 to client
0100.20a6.ca77.38.


*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
```

```
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP OFFER
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option: server id =
10.31.11.11
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option: lease time =
86400 seconds
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option: 58 (len 4) -
skipping
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option: 59 (len 4) -
skipping
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP option: netmask =
255.255.255.0
*DHCP Socket Task: Mar 05 09:53:37.896: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64

*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 97
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP REQUEST
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: 61 (len 7) -
skipping
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: requested ip
= 172.16.0.1
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: server id =
10.31.11.11
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: hostname =
WIN7-PC1 (len 8)
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: 81 (len 24) -
skipping
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: vendor class
id = MSFT 5.0 (len 8)
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP option: 55 (len 12) -
skipping
*DHCP Socket Task: Mar 05 09:53:37.899: 00:20:a6:ca:77:38 DHCP options end, len 97,
actual 89

*DHCP Socket Task: Mar 05 09:53:37.900: 00:20:a6:ca:77:38 DHCP option len (including
the magic cookie) 72
*DHCP Socket Task: Mar 05 09:53:37.900: 00:20:a6:ca:77:38 DHCP option: message type
= DHCP ACK
*DHCP Socket Task: Mar 05 09:53:37.901: 00:20:a6:ca:77:38 DHCP option: server id =
10.31.11.11
*DHCP Socket Task: Mar 05 09:53:37.901: 00:20:a6:ca:77:38 DHCP option: lease time =
86400 seconds
*DHCP Socket Task: Mar 05 09:53:37.901: 00:20:a6:ca:77:38 DHCP option: 58 (len 4) -
skipping
*DHCP Socket Task: Mar 05 09:53:37.901: 00:20:a6:ca:77:38 DHCP option: 59 (len 4) -
skipping
```

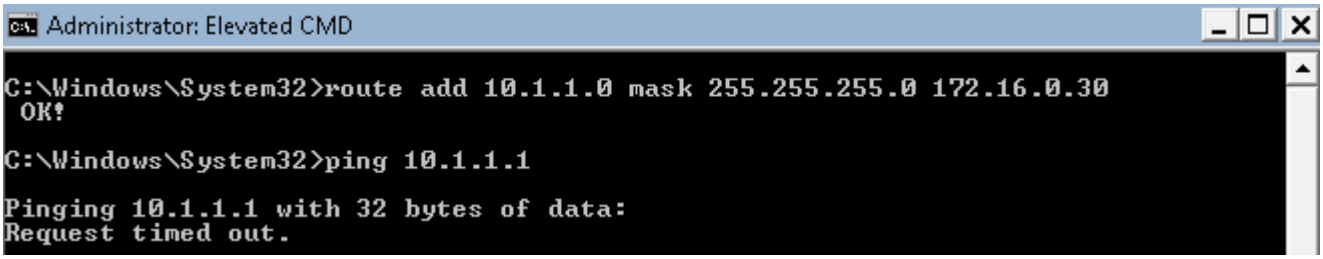
```
*DHCP Socket Task: Mar 05 09:53:37.901: 00:20:a6:ca:77:38 DHCP option: netmask =
255.255.255.0
*DHCP Socket Task: Mar 05 09:53:37.901: 00:20:a6:ca:77:38 DHCP options end, len 72,
actual 64
```



We have to add a route to Server2 manually – including default gateway info in DHCP could break routing and RDP session to the Test PC:



You should not be able to reach internal destinations from the Guest VLAN – ASA was configured with an ACL that prevents this from happening:



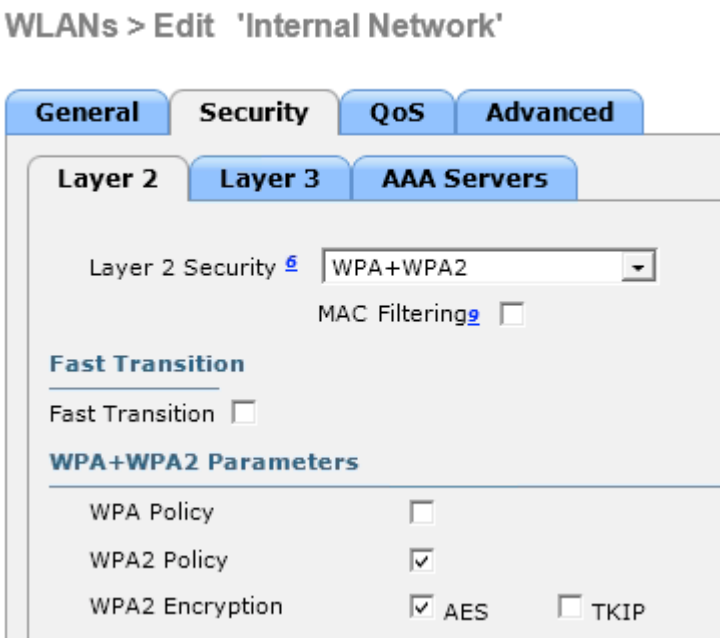

```
%ASA-4-106023: Deny icmp src GUEST:172.16.0.1 dst inside:10.1.1.1 (type 8, code 0)
by access-group "GUEST_IN" [0xd2b7562a, 0x0]
```

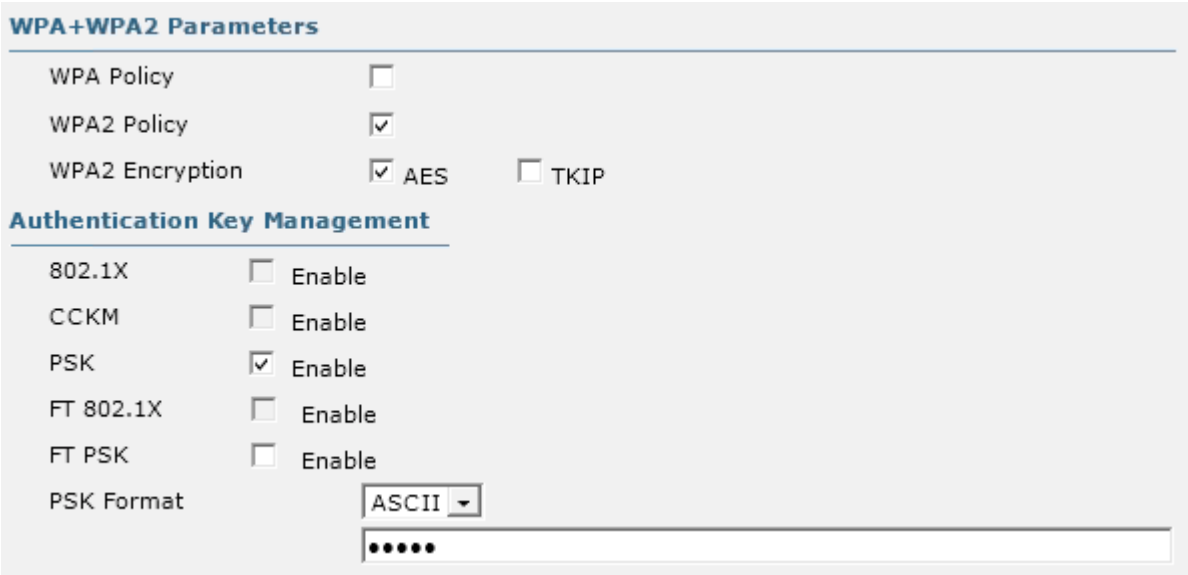
Task 5: WLAN Security

- Use WPA2 to protect communication in the Internal WLAN
- Clients should be authenticating using key “outofcontrol”
- Communication should be encrypted using AES
- Apply an ACL to the Internal WLAN that restricts traffic in the following way :
    - Blocks all Telnet connections initiated by wireless clients
    - Blocks all HTTP connections from the wired network to wireless clients
    - Permits all other traffic
- Hit counters should be enabled for this ACL
- This ACL should not be applied to the dynamic interface
- Guest WLAN connections should be authenticated based on MAC address of the client
- Only known Endpoints should be given access to the network
- Use ISE as the source of Endpoint information
- RADIUS shared secret used should be “ipexpert”

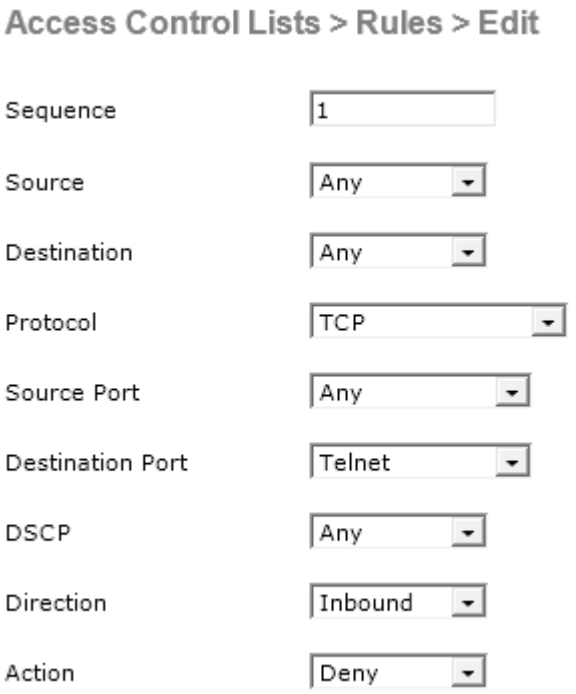
WLC

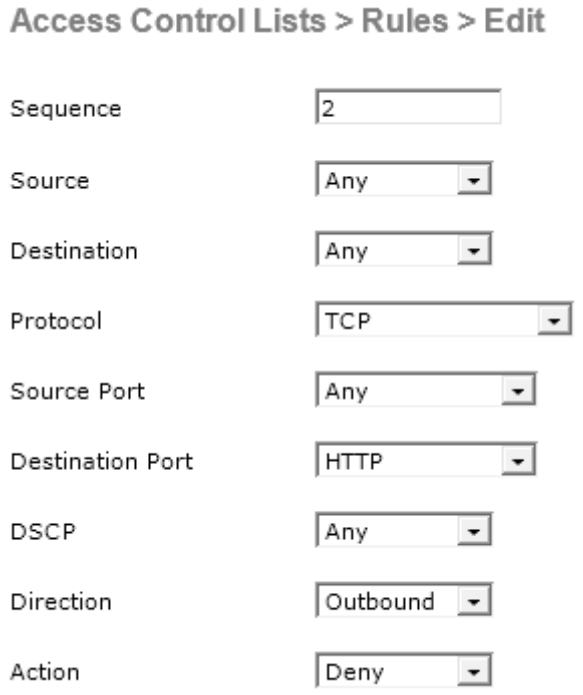
Reconfigure security settings of the Internal WLAN according to the pictures below:



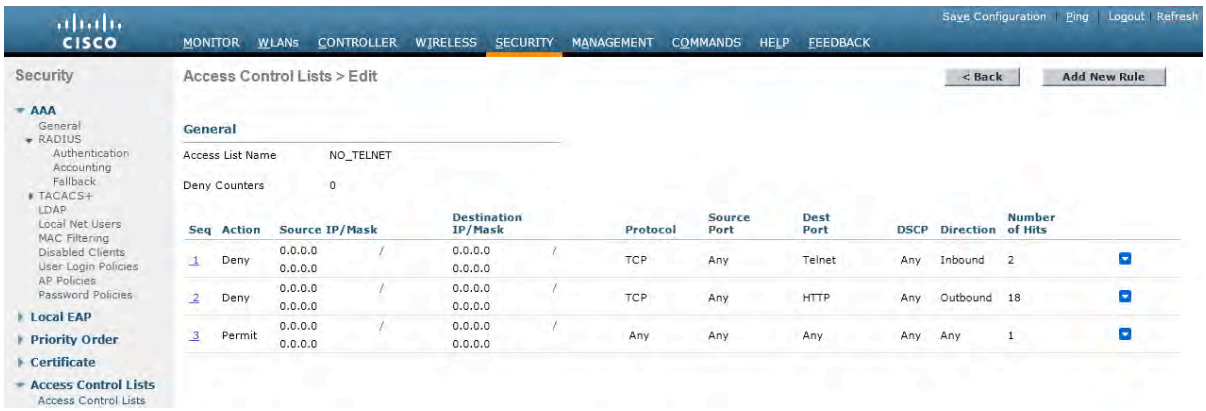


Create an ACL. Go to “Security”-> “Access Control Lists” and add a New one:

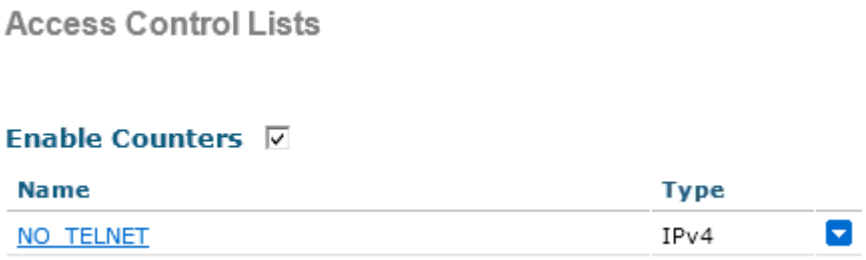




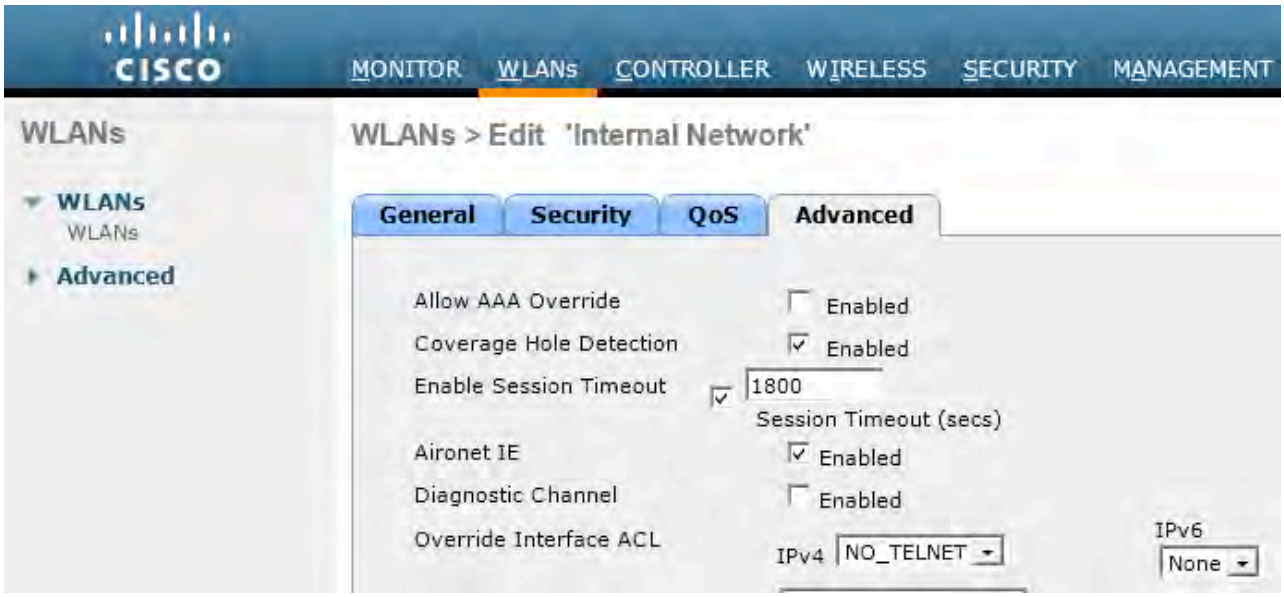
Here's how the ACL should look like:



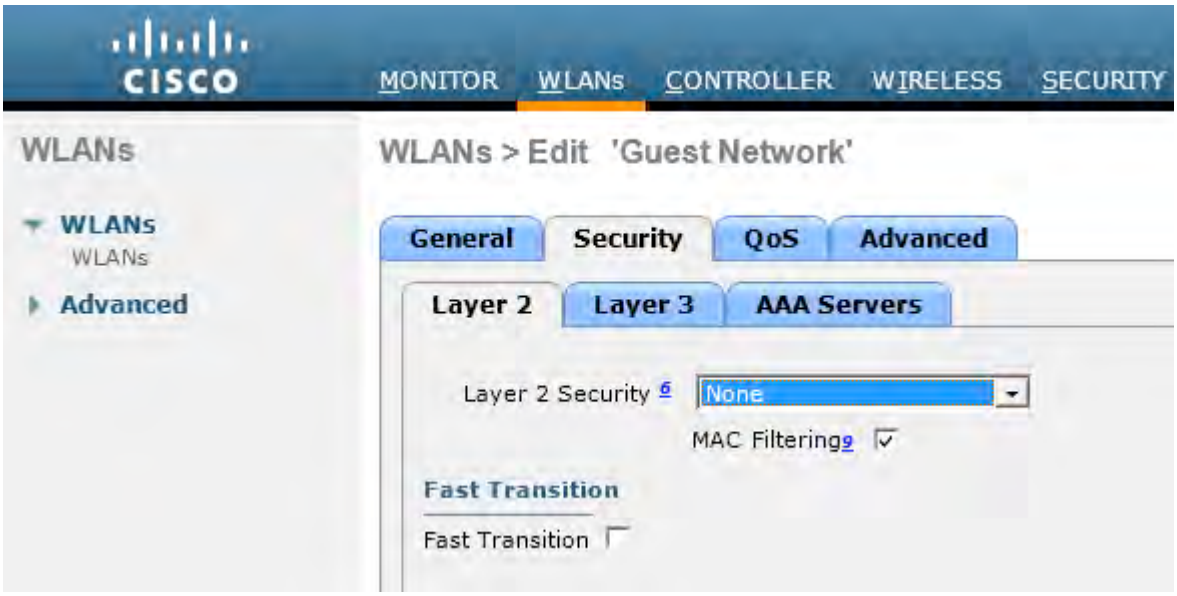
Make sure ACL counters are ON:



Now go to the WLAN (not interface) and apply the ACL:



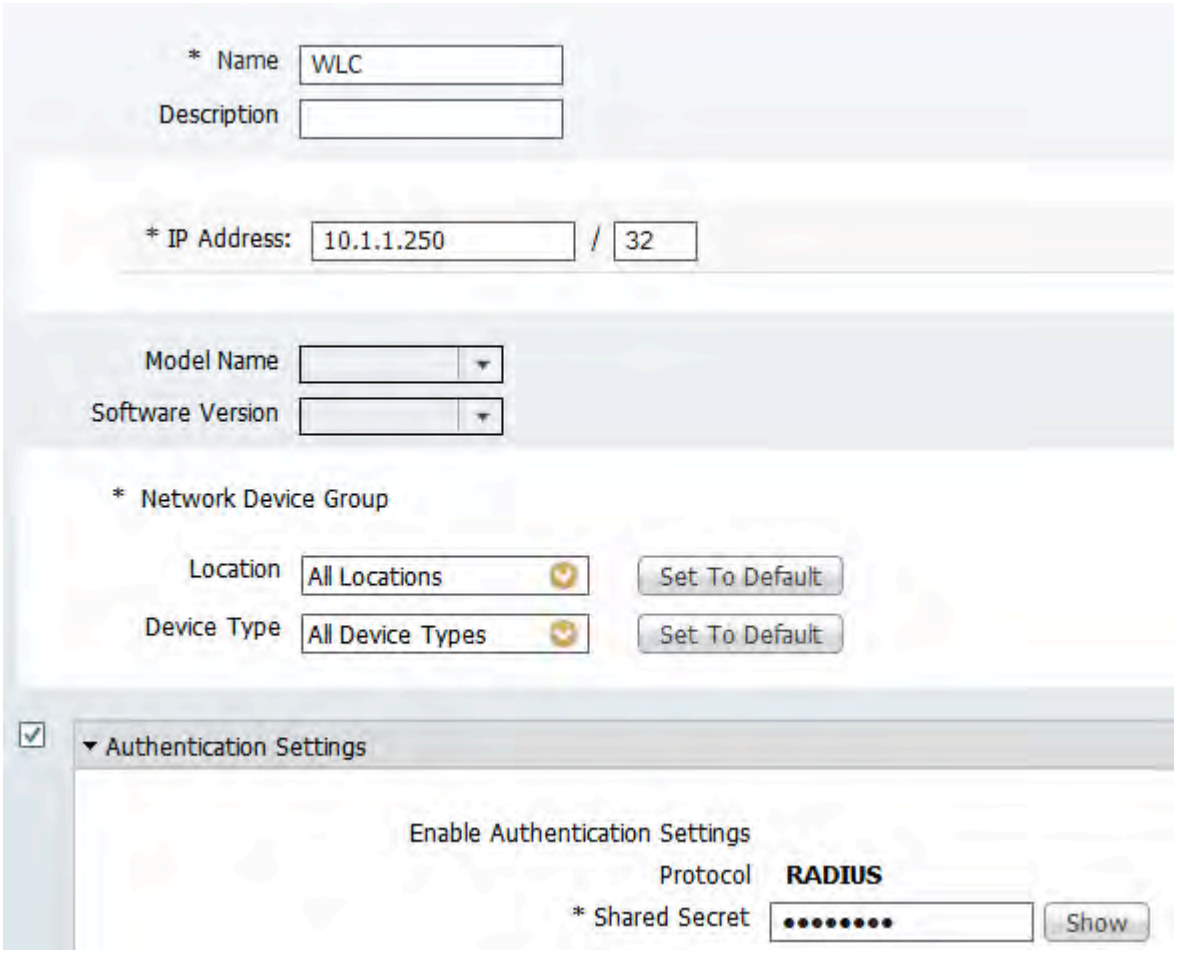
OK, now the Guest WLAN part. First we want to enable MAC Filtering:

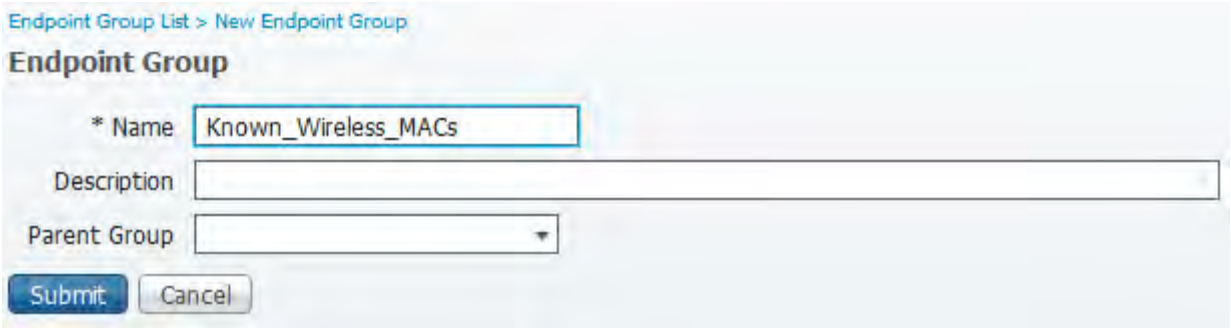


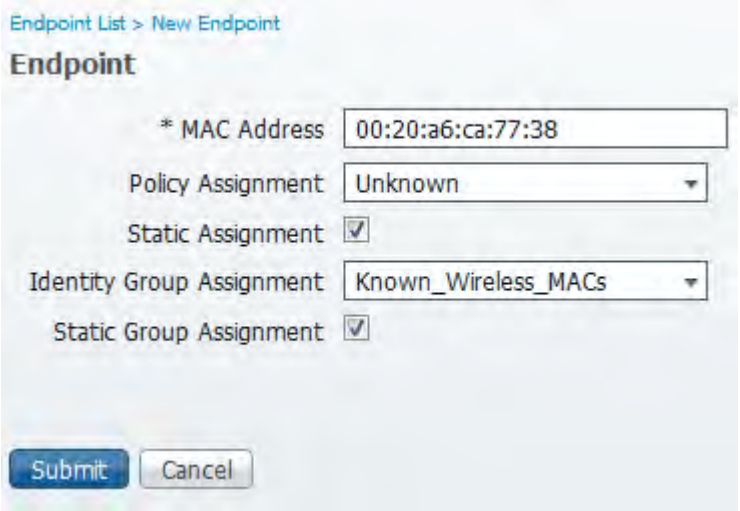
Then we need to create an entry for ISE and add it to the WLAN:

Then one more thing on WLC – you may want to ensure that the format of MAC Filtering Requests is the one used on old ACS (username=password):

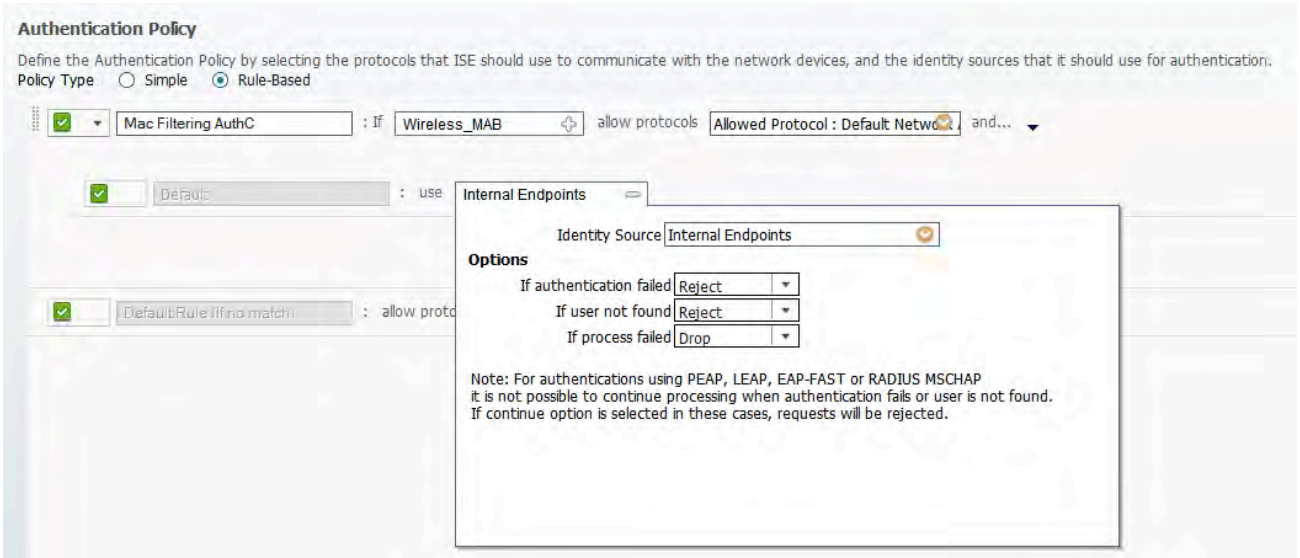
Couple more things we need to take care of are going to be done on ISE. We want to add WLC to Network Devices, create a group for Known MAC addresses we will then use in Au THz Policy and obviously we want to add MAC address of Test PC's Wireless NIC so it can get access to the Guest WLAN:

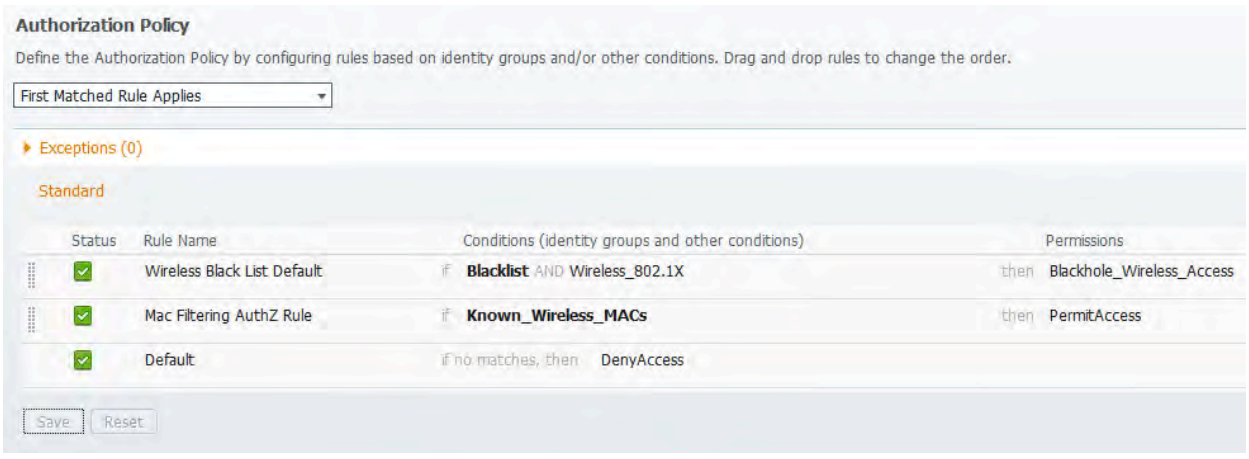






Next step is to build up our Authentication (make sure Host Lookup is allowed) & Authorization Rules. The assigned Profile will be the pre-defined "Permit Access":





Access-lists entries on WLC can be created for a single direction. The WLC's notion of inbound versus outbound is nonintuitive. It is from the perspective of the WLC facing towards the wireless client, rather than from the perspective of the client. So, inbound direction means a packet that comes into the WLC from the wireless client and outbound direction means a packet that exits from the WLC towards the wireless client.

Same as in a regular IOS/ASA, ACL entries are processed one by one up to the first match. There is also an implicit default “deny any any” at the end, which is for “Any” direction meaning Inbound & Outbound.

There are 3 types or groups of security features that are available on WLC:

1. Layer 1 - Ensures that all clients gain access within a user-set number of attempts. If a client fails to gain access within that limit, it is automatically excluded (blocked from access) until the user-set timer expires. The operating system can also disable SSID broadcasts on a per-WLAN basis
2. Layer 2 – Industry-standard authentication & encryption mechanisms such as 802.1x, WPA, WPA2 or WEP (never use WEP)
3. Layer 3 – IPSec, Web Authentication and their variations

Here’s the summary of L2 Security settings (L2 Security is most commonly used) that can be configured on WLC:

Layer 2 Security	None	No Layer 2 security selected.
	WPA+WPA2	Use this setting in order to enable Wi-Fi Protected Access.
	802.1X	Use this setting in order to enable 802.1x authentication.
	Static WEP	Use this setting in order to enable Static WEP encryption.
	Static WEP + 802.1x	Use this setting in order to enable both Static WEP and 802.1x parameters.
	CKIP	Use this setting in order to enable Cisco Key Integrity Protocol (CKIP). Functional on AP Models 1100, 1130, and 1200, but not AP 1000. Aironet IE needs to be enabled for this feature to work. CKIP expands the encryption keys to 16 bytes.

WPA is a standard-based security solution from the Wi-Fi Alliance that addresses the vulnerabilities in native WLANs. WPA provides enhanced data protection and access control for WLAN systems – this method was designed to address all known Wired Equivalent Privacy (WEP) vulnerabilities.

WPA 2 is the next generation of Wi-Fi security. It implements Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame. WPA 2 offers a higher level of security than WPA because AES offers stronger encryption than Temporal Key Integrity Protocol (TKIP).

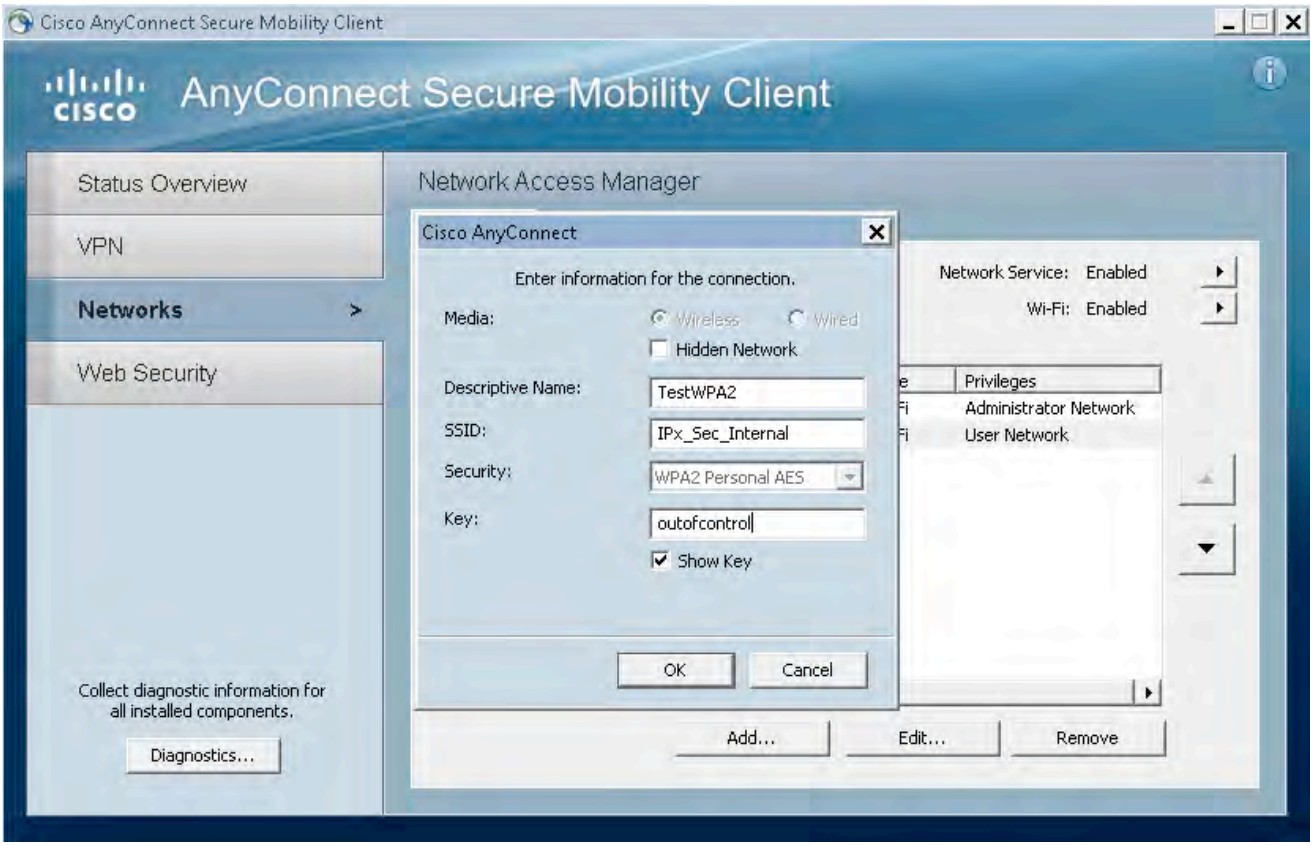
In a nutshell we can say that WPA provides AES, 802.1X authentication and dynamic key management. WPAv2 adds CCMP. Both WPA and WPAv2 have the following modes:

- Personal mode: Allows pre-shared keys for authentication
- Enterprise mode: Requires 802.1X authentication

In our case we were asked to configure a Password-based authentication, which is the Personal Mode.

Verification

We will need another AnyConnect entry to test WPA. You can either use the Standalone Profile Editor or add it directly from the AnyConnect client – but then it won't survive "Network Repair" you use to apply the changes done in the Profile Editor:



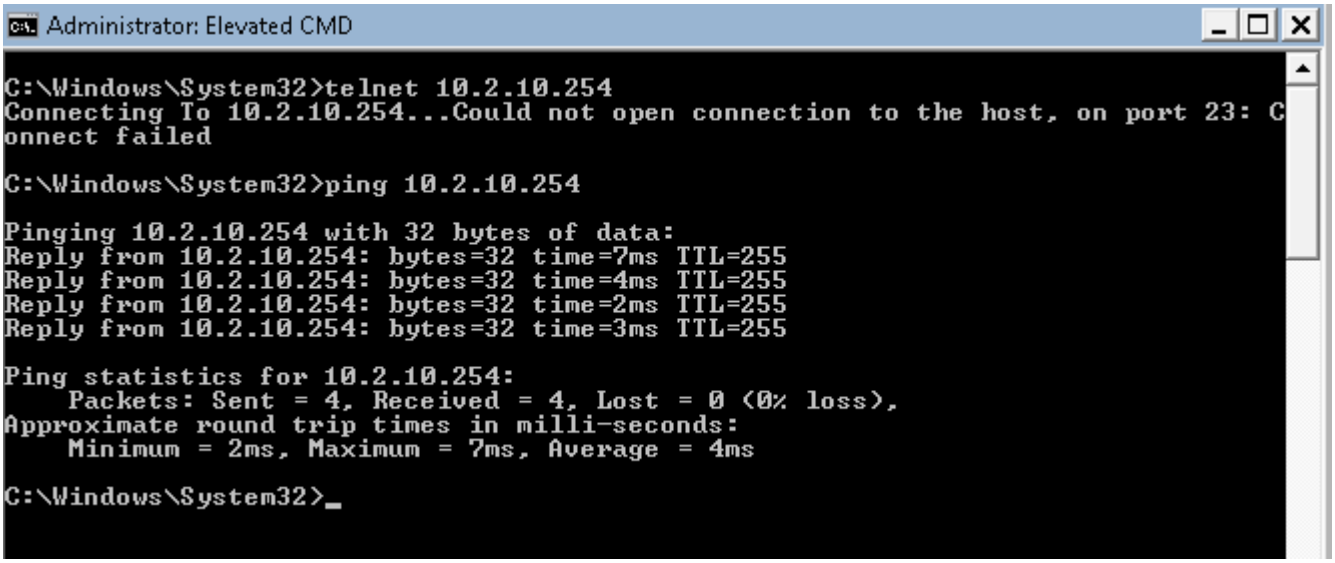
OK so let's connect and look at the client details ("Monitor" tab). Note the Security Policy and ACL name:

Client Type	Regular
User Name	
Port Number	1
Interface	internal
VLAN ID	210

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	NO_TELNET
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable

We will now generate some packets to test connectivity. Telnet is blocked but ping works on the Test PC:



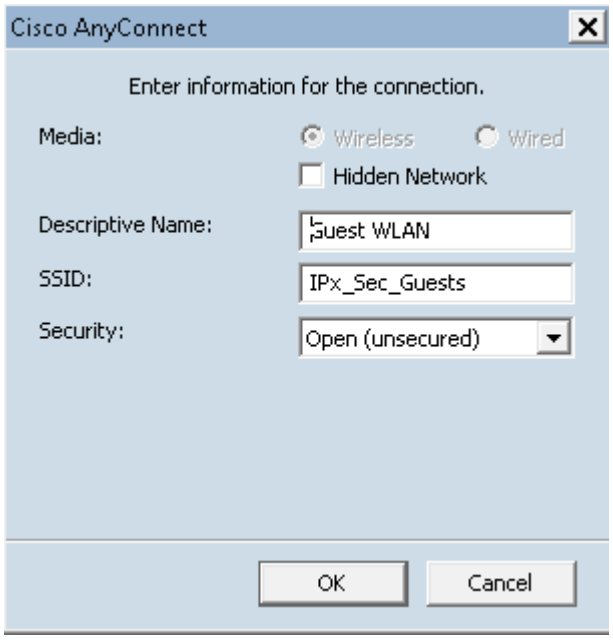
What about our Server1 (Cat3) ? HTTP is blocked but ping & HTTPs work:

```
CAT3#telnet 10.2.10.1 80
Trying 10.2.10.1, 80 ...
% Connection timed out; remote host not responding

CAT3#ping 10.2.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/17 ms

CAT3#telnet 10.2.10.1 443
Trying 10.2.10.1, 443 ...
% Connection refused by remote host
```

After removing the ACL and re-associating:

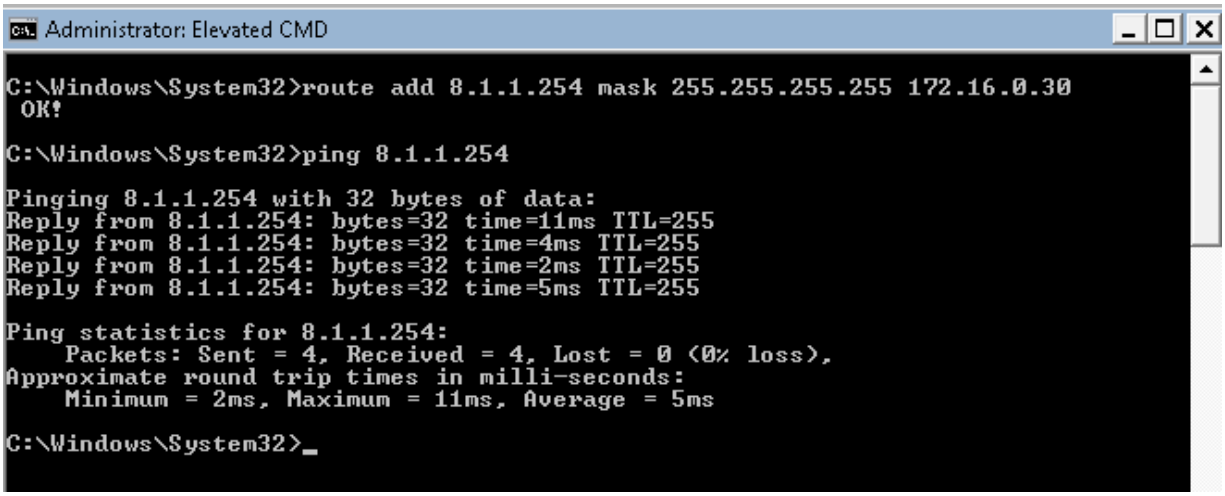
```
CAT3#telnet 10.2.10.1 80
Trying 10.2.10.1, 80 ... Open
get -
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid URL</h2>
<hr><p>HTTP Error 400. The request URL is invalid.</p>
</BODY></HTML>
[Connection to 10.2.10.1 closed by foreign host]
```

All right, let's now test the second part of our task (Guest WLAN):



I will start with showing you part of the aaa debug on WLC. Access-Accept was returned after the user was found and matched the AuthZ Rule:

```
*aaaQueueReader: Mar 05 22:27:24.257: AuthenticationRequest: 0x2b9ac92c

*aaaQueueReader: Mar 05 22:27:24.257:
Callback.....................................0x1010cae0

*aaaQueueReader: Mar 05 22:27:24.257:
protocolType.................................0x40000001

*aaaQueueReader: Mar 05 22:27:24.257:
proxyState...................................00:20:A6:CA:77:38-00:00

                                                    …

*radiusTransportThread: Mar 05 22:27:24.276: 00:20:a6:ca:77:38 Access-Accept
received from RADIUS server 10.1.1.150 for mobile 00:20:a6:ca:77:38 receiveId = 0
```



Looks good. Let's take a look on ISE:

Authentication Summary	
Logged At:	March 5,2013 10:19:39.682 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	00:20:A6:CA:77:38
MAC/IP Address:	00:20:A6:CA:77:38
Network Device:	WLC : 10.1.1.250 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Endpoints
Authorization Profiles:	PermitAccess
SGA Security Group:	
Authentication Protocol :	Lookup

NAS Port Type:	Wireless - IEEE 802.11
Allowed Protocol:	Default Network Access
Service Type:	Call Check
Identity Store:	Internal Endpoints
Authorization Profiles:	PermitAccess
Active Directory Domain:	
Identity Group:	Known_Wireless_MACs
Allowed Protocol Selection Matched Rule:	Mac Filtering AuthC
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Endpoints
Authorization Policy Matched Rule:	Mac Filtering AuthZ Rule

What if our MAC was not in the endpoint DB?

Authentication Summary	
Logged At:	March 5,2013 10:12:45.668 PM
RADIUS Status:	Authentication failed : 22056 Subject not found in the applicable identity store(s)
NAS Failure:	
Username:	00:20:A6:CA:77:38
MAC/IP Address:	00:20:A6:CA:77:38
Network Device:	WLC : 10.1.1.250 :
Allowed Protocol:	Default Network Access

Section 9
Advanced Security

Section 9 : Advanced Security is intended to let you be familiar with System Hardening and Advanced Security technologies that are available on IOS & the ASA. You will be configuring features related to Traffic Plane protection, Services protection and general System Hardening & Availability.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on Advanced Security technologies. You will need to pre-configure the network with the base configuration files

NOTE: Static/default routes are NOT allowed unless otherwise stated in a task.

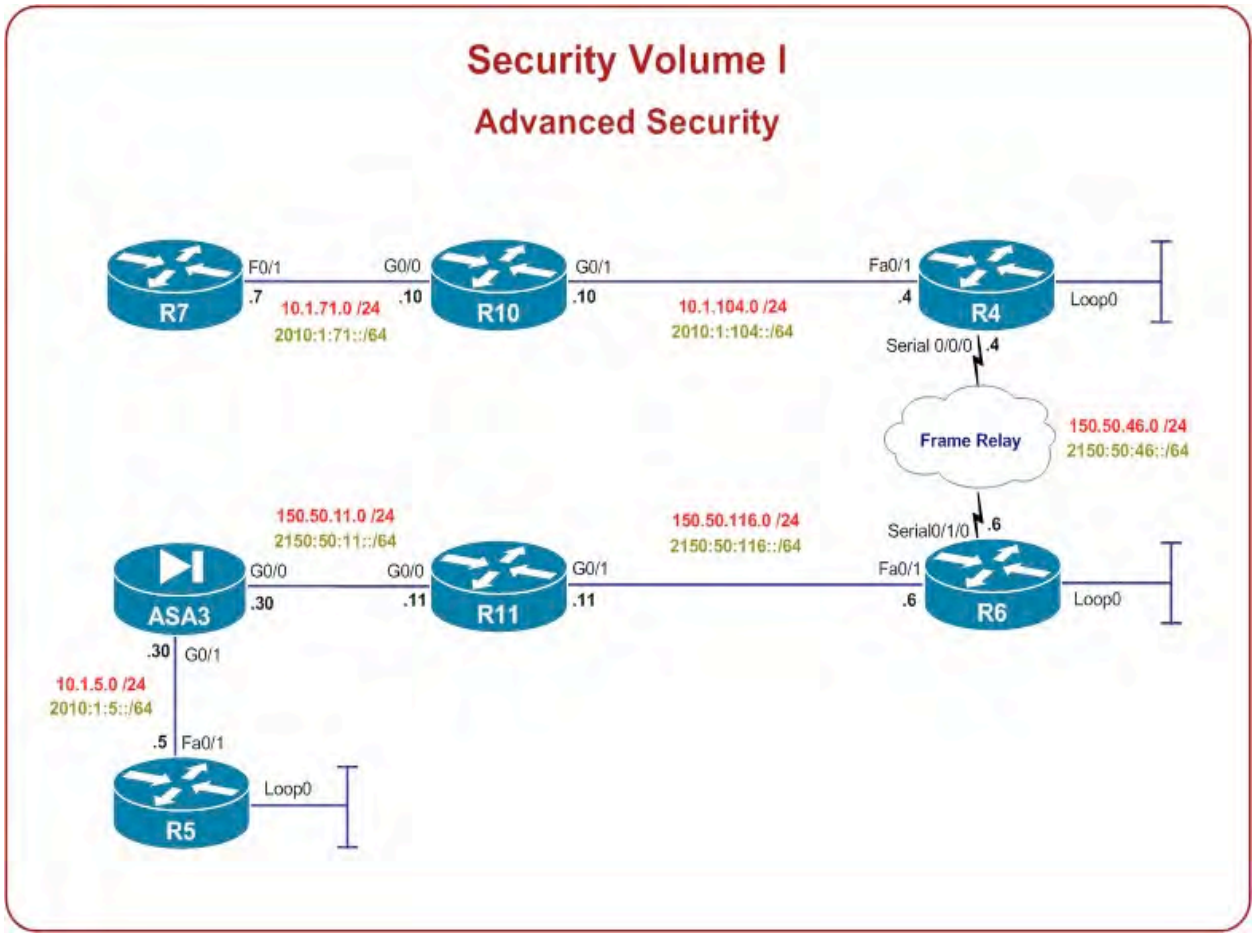
NOTE: You can allow ICMP for testing throughout the network

Estimated Time to Complete: **6 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R4	F0/1	104	10.1.104.4/24 2010:1:104::4/64
	S0/0/0		150.50.46.4/24 2150:50:46::4/64
	Loop0		4.4.4.4/24
R5	F0/1	305	10.1.5.5/24 2010:1:5::5/64
	Loop0		5.5.5.5/24
R6	F0/1	116	150.50.116.6/24 2150:50:116::6/64
	S0/1/0		150.50.46.6/24 2150:50:46::6/64
	Loop0		6.6.6.6/24
R7	F0/1	71	10.1.71.7/24 2010:1:71::7/64
R10	G0/0	71	10.1.71.10/24 2010:1:71::10/64
	G0/1	104	10.1.104.10/24 2010:1:104::10/64
R11	G0/0	501	150.50.11.11/24 2150:50:11::11/64
	G0/1	116	150.50.116.11/24 2150:50:116::11/64
ASA3	G0/0	501	150.50.11.30/24 2150:50:11::30/64
	G0/1	305	10.1.5.30/24 2010:1:5::30/64



Solutions

Task 1: IP Routing & Route Filtering

- Configure IPv6 on all devices according to the table and lab topology
- Enable EIGRPv6 between R11 and R6's F0/1
- Enable OSPFv3 between R7, R10 and R4's F0/1
- Enable BGP for IPv6 over the Frame Relay cloud
- Use AS numbers 400 (R4) and 600 (R6)
- Make sure 2010:1:5::/64 is reachable in AS 600. Exchange all IPv6 routes between ASes, ensure full IPv6 connectivity
- You are allowed to add one default route on R5 and the ASA
- You are allowed to add one static route on R11
- Make sure RFC1918 subnets are not advertised to AS 600 devices. You can modify OSPF configuration on routers R4, R7 and R10 to accomplish this
- Advertise loopback of R5 into OSPF (IPv4) but not the 10.1.5.0/24 network
- Create loopback0 (7.7.7.7/24) on R7 and advertise it to OSPF as /24

Detailed Solution

R7

```
ipv6 unicast-routing

int f0/1
 ipv6 address 2010:1:71::7/64
 ipv6 ospf 1 area 0
 no ip ospf 1 ar 0
 ip ospf 1 ar 1

interface Loopback0
 ip address 7.7.7.7 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 1
```

R10

```
ipv6 unicast-routing

int g0/0
 ipv6 address 2010:1:71::10/64
 ipv6 ospf 1 area 0
 no ip ospf 1 ar 0
 ip ospf 1 ar 1
```

```
int g0/1
 ipv6 address 2010:1:104::10/64
 ipv6 ospf 1 area 0
 no ip ospf 1 ar 0
 ip ospf 1 ar 1
```

R4

```
ipv6 unicast-routing

router bgp 400
 bgp log-neighbor-changes
 neighbor 2150:50:46::6 remote-as 600

 address-family ipv4
  no neighbor 2150:50:46::6 activate
  no auto-summary

 address-family ipv6
  redistribute ospf 1 include-connected
  neighbor 2150:50:46::6 activate

int s0/0/0
 ipv6 address FE80::4 link-local
 ipv6 address 2150:50:46::4/64
 frame-relay map ipv6 2150:50:46::6 406
 frame-relay map ipv6 FE80::6 406 broadcast

int f0/1
 ipv6 address 2010:1:104::4/64
 ipv6 ospf 1 area 0
 no ip ospf 1 ar 0
 ip ospf 1 ar 1

ip prefix-list NO_INTERNAL seq 5 deny 10.1.71.0/24
ip prefix-list NO_INTERNAL seq 10 deny 10.1.104.0/24
ip prefix-list NO_INTERNAL seq 15 permit 0.0.0.0/0 le 32

router ospf 1
 area 0 filter-list prefix NO_INTERNAL in

ipv6 router ospf 1
 redistribute connected
 redistribute bgp 400 metric 50 metric-type 1

int l0
 ipv6 ospf 1 area 0
```

R6

```
ipv6 unicast-routing
```

```
int f0/1
 ipv6 address 2150:50:116::6/64
 ipv6 eigrp 1

ipv6 router eigrp 1
 no shut
 redistribute connected
 redistribute bgp 600 metric 1 1 1 1 1

router bgp 600
 bgp log-neighbor-changes
 neighbor 2150:50:46::4 remote-as 400

 address-family ipv4
  no neighbor 2150:50:46::4 activate
  no auto-summary

 address-family ipv6
  redistribute eigrp 1
  network 2150:50:116::/64
  neighbor 2150:50:46::4 activate

int s0/1/0
 ipv6 address FE80::6 link-local
 ipv6 address 2150:50:46::6/64
 frame-relay map ipv6 2150:50:46::4 604
 frame-relay map ipv6 FE80::4 604 broadcasts
```

R11

```
ipv6 unicast-routing

int g0/0
 ipv6 address 2150:50:11::11/64
 ipv6 eigrp 1

int g0/1
 ipv6 address 2150:50:116::11/64
 ipv6 eigrp 1

ipv6 route 2010:1:5::/64 2150:50:11::30

ipv6 router eigrp 1
 no shut
 redistribute static metric 1 1 1 1 1
```

ASA3

```
ipv6 unicast-routing
```

```
int g0/0
 ipv6 address 2150:50:11::30/64

int g0/1
 ipv6 address 2010:1:5::30/64

ipv6 route outside ::/0 2150:50:11::11

router ospf 2
 network 10.1.5.30 255.255.255.255 area 0
 redistribute ospf 1 subnets

prefix-list NO_R5_NET seq 5 deny 10.1.5.0/24
prefix-list NO_R5_NET seq 10 permit 0.0.0.0/0 le 32

route-map RED_TO_OSPF1 permit 10
 match ip address prefix-list NO_R5_NET

router ospf 1
 redistribute ospf 2 subnets route-map RED_TO_OSPF1

ipv6 access-list OUTSIDE6_IN permit icmp6 any any
access-group OUTSIDE6_IN in interface outside
```

R5

```
ipv6 unicast-routing

int f0/1
 ipv6 address 2010:1:5::5/64

ipv route ::/0 2010:1:5::30
```

Frame Relay mappings are required for link-local addresses because these are used by IPv6 routing protocols as the Next-Hop value. It is considered to be a good practice to assign Link-Local addresses manually to ease further configuration and help with any potential troubleshooting.

It is not possible to filter routes within a single OSPF area (unless you are just trying to stop an LSA from being sent to the RIB). You can only summarize and filter routes between the areas or when doing redistribution.

OSPF treats loopback interfaces as Network Type “Loopback” (as a stub host). This means that a /32 prefix will be advertised by default – to change this modify the OSPF network type to point-to-point.

On the ASA it is possible to create two OSPF processes. This can be very useful for any type of route-filtering scenarios when you want have granular control over routes exchanged between e.g. inside and

outside domains. In the newer versions of code (e.g. 8.6) prefix-lists can be now called out from a route-map, which simplifies the overall filtering configuration (comparing to access-lists).

IPv6 Considerations

Directly connected subnets the protocol are running on are not automatically redistributed – use "`include-connected`" keyword to account for them as well (or in BGP simply advertise them via `network`).

Verification

```
R7#sh ip route ospf | be Gateway
Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O IA     4.4.4.4 [110/3] via 10.1.71.10, 12:44:51, FastEthernet0/1
      5.0.0.0/32 is subnetted, 1 subnets
O E2     5.5.5.5 [110/11] via 10.1.71.10, 12:44:51, FastEthernet0/1
      6.0.0.0/32 is subnetted, 1 subnets
O IA     6.6.6.6 [110/67] via 10.1.71.10, 12:44:51, FastEthernet0/1
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.104.0/24 [110/2] via 10.1.71.10, 12:44:51, FastEthernet0/1
      150.50.0.0/24 is subnetted, 3 subnets
O IA     150.50.11.0 [110/68] via 10.1.71.10, 12:44:51, FastEthernet0/1
O IA     150.50.46.0 [110/66] via 10.1.71.10, 12:44:51, FastEthernet0/1
O IA     150.50.116.0 [110/67] via 10.1.71.10, 12:44:51, FastEthernet0/1

R7#sh ipv ro ospf
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2004::4/128 [110/2]
     via FE80::32E4:DBFF:FECE:8490, FastEthernet0/1
OE1 2010:1:5::/64 [110/52]
     via FE80::32E4:DBFF:FECE:8490, FastEthernet0/1
O   2010:1:104::/64 [110/2]
     via FE80::32E4:DBFF:FECE:8490, FastEthernet0/1
OE1 2150:50:11::/64 [110/52]
     via FE80::32E4:DBFF:FECE:8490, FastEthernet0/1
OE2 2150:50:46::/64 [110/20]
     via FE80::32E4:DBFF:FECE:8490, FastEthernet0/1
OE1 2150:50:116::/64 [110/52]
     via FE80::32E4:DBFF:FECE:8490, FastEthernet0/1
```

```
R6#sh ip ro ospf | be Gat
Gateway of last resort is not set

      4.0.0.0/32 is subnetted, 1 subnets
O        4.4.4.4 [110/65] via 150.50.46.4, 12:55:00, Serial0/1/0
      5.0.0.0/32 is subnetted, 1 subnets
O E2     5.5.5.5 [110/11] via 150.50.116.11, 13:00:47, FastEthernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
O IA     7.7.7.0 [110/67] via 150.50.46.4, 12:39:01, Serial0/1/0
      150.50.0.0/16 is variably subnetted, 5 subnets, 2 masks
O        150.50.11.0/24 [110/2] via 150.50.116.11, 23:47:19, FastEthernet0/1


R6#sh ipv ro eigrp
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
EX  2010:1:5::/64 [170/2560005376]
     via FE80::CA4C:75FF:FE1F:DDC1, FastEthernet0/1
D   2150:50:11::/64 [90/30720]
     via FE80::CA4C:75FF:FE1F:DDC1, FastEthernet0/1

R6#ping 2010:1:5::5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:1:5::5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/12 ms

R5#ping 7.7.7.7 source loop0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms


R4#sh bgp ipv6 uni summ
BGP router identifier 4.4.4.4, local AS number 400
BGP table version is 11, main routing table version 11
5 network entries using 800 bytes of memory
5 path entries using 380 bytes of memory
5/5 BGP path/bestpath attribute entries using 620 bytes of memory
```

```
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1824 total bytes of memory
BGP activity 7/2 prefixes, 8/3 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
2150:50:46::6   4          600     908     904       11    0    0 13:34:33        3


R4#sh bgp ipv6 uni
BGP table version is 11, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2004::/64        ::                       0         32768 ?
*> 2010:1:5::/64    2150:50:46::6   2560005376             0 600 ?
*> 2010:1:71::/64   ::                       2         32768 ?
*> 2010:1:104::/64  ::                       0         32768 ?
*> 2150:50:11::/64  2150:50:46::6        30720             0 600 ?
*> 2150:50:116::/64 2150:50:46::6            0             0 600 i


R6#sh bgp ipv6 unicast
BGP table version is 11, local router ID is 6.6.6.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2004::/64        2150:50:46::4            0             0 400 ?
*> 2010:1:5::/64    ::                2560005376         32768 ?
*> 2010:1:71::/64   2150:50:46::4            2             0 400 ?
*> 2010:1:104::/64  2150:50:46::4            0             0 400 ?
*> 2150:50:11::/64  ::                   30720         32768 ?
*> 2150:50:116::/64 ::                       0         32768 i

R7#ping 2010:1:5::5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:1:5::5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms
```

Task 2: Routing Protocol Authentication

- Authenticate OSPF adjacencies in area 0 using MD5
- Area 1 should be secured using clear-text password
- Authentication on R10 can be only enabled for the entire area; link to R7 should be exempted from clear-text / MD5 authentication
- Enable authentication for EIGRPv6
- Secure OSPFv3 adjacencies using SHA-1 and AES 128
- IPv6 BGP peerings should be authenticated as well
- Use “ipexpert” for all passwords

R5

```
interface f0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert
```

ASA3

```
interface g0/0
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest

int g0/1
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest
```

R11

```
key chain EIGRPv6
 key 1
  key-string ipexpert

interface g0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert

int g0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 EIGRPv6
```

R6

```
key chain EIGRPv6
 key 1
  key-string ipexpert

interface f0/1
```

```
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 EIGRPv6

interface s0/1/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert

router bgp 600
 neighbor 2150:50:46::4 password ipexpert
```

R4

```
interface s0/0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert

int f0/1
 ip ospf authentication
 ip ospf authentication-key ipexpert
 ipv6 ospf encryption ipsec spi 410 esp aes-cbc 128 12345678901234567890123456789012
 sha1 1234567890123456789012345678901234567890

router bgp 400
 neighbor 2150:50:46::6 password ipexpert
```

R10

```
router ospf 1
 area 1 authentication

interface g0/0
 ip ospf authentication null
 ipv6 ospf encryption ipsec spi 710 esp aes-cbc 128 12345678901234567890123456789012
 sha1 1234567890123456789012345678901234567890

interface g0/1
 ip ospf authentication-key ipexpert
 ipv6 ospf encryption ipsec spi 410 esp aes-cbc 128 12345678901234567890123456789012
 sha1 1234567890123456789012345678901234567890
```

R7

```
int f0/1
 ipv6 ospf encryption ipsec spi 710 esp aes-cbc 128 12345678901234567890123456789012
 sha1 1234567890123456789012345678901234567890
```

Without neighbor authentication, unauthorized or deliberately malicious routing updates could compromise the security of your network traffic. A security compromise could occur if an unfriendly

party diverts or analyzes that traffic. For example, an unauthorized router could send a fictitious routing update to convince your router to send traffic to an incorrect destination. The unfriendly party could analyze the diverted traffic to learn confidential information about your organization or merely use it to disrupt your organization's ability to communicate effectively using the network.

Key Chains are security components used to protect routing protocol updates in IPv4/IPv6 RIP and EIGRP. Key Chains give us an ability to specify multiple passwords and their lifetime so we can rotate the keys and increase the overall security. Here just remember that only the first active key will be always used (when sending packets), but for the received protocol updates, even that the software may show multiple keys are valid, also the key number must match and not only the password or hash.

RIP supports both, clear-text and MD5 authentication. EIGRP only supports MD5 (obviously the recommended method).

Authentication in OSPF can be enabled for the entire area or on a per-interface basis. There are three types of OSPF authentication:

- Type 0 – Null (default)
- Type 1 – Plain Text
- Type2 – MD5

Remember that if you are asked to secure Area 0 you must also account for any Virtual Links that are also part of the backbone. For Virtual Links the syntax would be `area virtual-link authentication-key/message-digest-key`.

IPv6 Considerations

EIGRPv6 and BGP for IPv6 authentication works and is configured in exactly same way as in version four of IP.

OSPFv3 no longer supports Null/Plain/MD5 authentication – IPSec Extension Headers are used to protect communication – AH (`ipv6 ospf authentication`) or ESP (`ipv6 ospf encryption`). Just remember about two things here:

1. Inbound & Outbound SPI number must be the same between the two neighbors (no way to use “asymmetrical” numbers). If there is more than one neighbor a separate number must be used (SPI numbers must be unique)
2. Depending on the algorithm selected they key length is going to be different – use the Context Sensitive Help (“?”) to figure out the number, e.g. :

```
R10(config-if)#ipv ospf authentication ipse spi 256 md5 ?
  0           The key is not encrypted (plain text)
  7           The key is encrypted
  Hex-string  MD5 key (32 chars)
```

Verification

```
R5#sh ip ospf int
Loopback0 is up, line protocol is up
  Internet Address 5.5.5.5/24, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type LOOPBACK, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Loopback interface is treated as a stub Host
FastEthernet0/1 is up, line protocol is up
  Internet Address 10.1.5.5/24, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.1.5.30, Interface address 10.1.5.30
  Backup Designated router (ID) 5.5.5.5, Interface address 10.1.5.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.5.30  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1

R10#sh ip ospf int
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 10.1.104.10/24, Area 1, Attached via Interface Enable
  Process ID 1, Router ID 10.1.71.10, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.71.10, Interface address 10.1.104.10
```

```
  Backup Designated router (ID) 4.4.4.4, Interface address 10.1.104.4
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 6
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 4.4.4.4  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Simple password authentication enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.71.10/24, Area 1, Attached via Interface Enable
  Process ID 1, Router ID 10.1.71.10, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.71.10, Interface address 10.1.71.10
  Backup Designated router (ID) 10.1.71.7, Interface address 10.1.71.7
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 4, maximum is 5
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.71.7  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

R6#sh ipv eigrp int detail
EIGRP-IPv6 Interfaces for AS(1)
                       Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/1              1        0/0         1       0/1           50           0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Un/reliable mcasts: 0/9  Un/reliable ucasts: 9/3
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 1  Out-of-sequence rcvd: 1
```

```
  Topology-ids on interface - 0
  Authentication mode is md5,  key-chain is "EIGRPv6"


R10#sh ipv6 ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Link Local Address FE80::32E4:DBFF:FECE:8491, Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 10.1.104.10
  Network Type BROADCAST, Cost: 1
  AES-CBC-128 encryption SHA-1 auth SPI 410, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.104.10, local address FE80::32E4:DBFF:FECE:8491
  Backup Designated router (ID) 4.4.4.4, local address FE80::21B:D5FF:FE0F:F371
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 5
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 4.4.4.4  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::32E4:DBFF:FECE:8490, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 10.1.104.10
  Network Type BROADCAST, Cost: 1
  AES-CBC-128 encryption SHA-1 auth SPI 710, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.104.10, local address FE80::32E4:DBFF:FECE:8490
  Backup Designated router (ID) 10.1.71.7, local address FE80::21B:D5FF:FE17:BA89
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 4
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.71.7  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

R10#sh crypto ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-710
Policy refcount:  1
Inbound  ESP SPI:         710 (0x2C6)
Outbound ESP SPI:         710 (0x2C6)
```

```
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901
Outbound ESP Auth Key:   12345678901234567890123456789012345678901
Inbound  ESP Cipher Key: 123456789012345678901234567890123
Outbound ESP Cipher Key: 123456789012345678901234567890123
Transform set:    esp-aes esp-sha-hmac

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-410
Policy refcount:  1
Inbound  ESP SPI:        410 (0x19A)
Outbound ESP SPI:        410 (0x19A)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901
Outbound ESP Auth Key:   12345678901234567890123456789012345678901
Inbound  ESP Cipher Key: 123456789012345678901234567890123
Outbound ESP Cipher Key: 123456789012345678901234567890123
Transform set:    esp-aes esp-sha-hmac
```

Note since IKE is not used for negotiation there is actually no Phase I tunnel between the devices:

```
R10#sh cry isa sa


R10#sh cry sess det
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Session status: UP-NO-IKE
Peer: :: port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: permit 89 FE80::/10 ::/0
        Active SAs: 2, origin: manual-keyed crypto map
        Inbound:  #pkts dec'ed 62 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 59 drop 0 life (KB/Sec) 0/0

Interface: GigabitEthernet0/1
Session status: UP-NO-IKE
Peer: :: port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: permit 89 FE80::/10 ::/0
        Active SAs: 2, origin: manual-keyed crypto map
        Inbound:  #pkts dec'ed 46 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 46 drop 0 life (KB/Sec) 0/0
```

```
R10#sh cry ipsec sa identity

interface: GigabitEthernet0/0
    Crypto map tag: (none), local addr 2010:1:71::10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer (none) port 500
     DENY, flags={ident_is_root,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
   IPsecv6 policy name: OSPFv3-1-710
   IPsecv6-created ACL name: GigabitEthernet0/0-ipsecv6-ACL

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (FE80::/10/89/0)
   remote ident (addr/mask/prot/port): (::/0/89/0)
   current_peer :: port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 143, #pkts encrypt: 143, #pkts digest: 143
    #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

R10#sh access-l
IPv6 access list GigabitEthernet0/0-ipsecv6-ACL
    permit 89 FE80::/10 any (70 matches) sequence 1
IPv6 access list GigabitEthernet0/1-ipsecv6-ACL
    permit 89 FE80::/10 any (61 matches) sequence 1
```

19A in Hex is 410 in decimal; 2C6 is 710 :

```
R10#sh cry ipsec spi-lookup
Active SPI table
     SPI Prot Local Address           M Type
0000019A ESP  Any                     * OSPFv3 IPSec SA
000002C6 ESP  Any                     * OSPFv3 IPSec SA


R6#sh bgp ipv6 unicast neighbors 2150:50:46::4 | in Option
Option Flags: nagle, path mtu capable, md5
```

```
R4#sh bgp ipv6 uni neighbors 2150:50:46::6 | in Opt
Option Flags: nagle, path mtu capable, md5, 0x1000000

R4#sh bgp ipv6 uni summary
BGP router identifier 4.4.4.4, local AS number 400
BGP table version is 21, main routing table version 21
5 network entries using 800 bytes of memory
5 path entries using 380 bytes of memory
5/5 BGP path/bestpath attribute entries using 620 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1824 total bytes of memory
BGP activity 12/7 prefixes, 13/8 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
2150:50:46::6   4          600      28      27       21    0    0 00:19:43        3
```

Task 3: Basic Device Access Configurations

- Configure a domain of ipexpert.com on R5, R7, R10 and R11
- Use a username of “ipexpert” and a password of “cisco” unless otherwise specified
- Make sure any username password in this lab is not easily decrypted
- Configure a message on R5 that will appear before the password prompt when connecting via Telnet/SSHv2 (only allow SSH version 2)
- Configure a message that will appear after the session is interacting with the EXEC
- Connecting users should see the VTY line number the session terminates on
- VTY connections should timeout after 15 minutes of inactivity and should be disconnected after 1 hour regardless of activity

R5, R7, R10, R11

```
ip domain-name ipexpert.com
```

R5

```
line vty 0 4
 exec-timeout 15 0
 absolute-timeout 60
 login local

crypto key generate rsa mod 768

banner exec * Connected to $(hostname).$(domain) *
banner login & You are connected to VTY $(line) &

ip ssh version 2
```

Banner messages all display their messages at different times during user initiation:

1. MOTD Banner - displayed on all connected terminals. This banner is displayed at login and is useful for sending messages (such as impending system shutdowns) that affect all network users.
2. Login Banner - displayed on all connected terminals after the MOTD banner appears and before the login prompts (both, MOTD and login are configured in global config mode)
3. EXEC banner - displayed whenever an EXEC process is initiated (right before the user EXEC mode prompt shows up)

The "`service password encryption`" command uses a Vigenere cipher, which simply shifts letters and numbers a number of spaces that the key requires. There are plenty of sources on the internet to easily decrypt these passwords. You can also decrypt this passwords manually if you are interested using the constant value of "tfd;kfoA,.iyewrkldJKD" as shown in Eric Cole‟s book "Hackers Beware." Thus the question is looking for a "secret" password which uses a stronger MD5 encryption algorithm.

Although the task does not state to configure local authentication, to use the login banner you need to configure a type of authentication for the login banner to work. Whether that just be a password on the line, AAA, or local authentication.

This task could be answered using session timeout or exec-timeout. Either will disconnect the user after a period of inactivity.

IPv6 Considerations

IPv6 addresses can be also used for Device Management.

Verification

```
R5#ssh -l ipexpert 5.5.5.5
 You are connecting to VTY 514

Password:
 Connected to R5.ipexpert.com
R5>sh ssh
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0     IN   aes128-cbc  hmac-sha1    Session started       ipexpert
0          2.0     OUT  aes128-cbc  hmac-sha1    Session started       ipexpert
%No SSHv1 server connections running.


R5#sh line vty 0
```

```
   Tty Line Typ     Tx/Rx    A Modem  Roty AccO AccI  Uses  Noise Overruns  Int
    514  514 VTY               -    -      -    -    -    12      0    0/0      -

Line 514, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: Ready, No Exit Banner
Capabilities: none
Modem state: Ready
Group codes:    0
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:15:00        never                    01:00:00    not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 20.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are lat pad telnet rlogin lapb-ta mop udptn v120 ssh.
Allowed output transports are lat pad telnet rlogin lapb-ta mop v120 ssh.
Preferred transport is lat.
Shell: enabled
Shell trace: off
No output characters are padded
No special data dispatching characters
```

Task 4: Controlling Device Access

- The administrator of R7 wants to reserve a VTY line for himself. Accomplish this by changing the TCP port for VTY 15 to 2015. Only allow SSH version 2 connections on VTY 15
- The administrator of R7 does not want anybody to telnet from R7. Disable outbound telnet on R7. Do not make any changes in global configuration to accomplish this task
- When anyone else Telnets to R7, they should not have the ability to access the CLI. Instead, they should receive a menu that only allows them the ability to perform the following commands :
  - Show ip interface brief
  - Show ip route
  - Show ip ospf neighbor
  - Exit

R7

```
crypto key generate rsa usage-keys mod 1024

ip ssh port 2015 rotary 15
ip ssh version 2

username ipexpert pass cisco

line vty 0 15
 login local
 transport output ssh

line vty 15
 rotary 15

line con 0
 transport output ssh


menu IPEXPERT title % DEVICE TELNET MENU %
menu IPEXPERT prompt % Please Enter Your Selection : %
menu IPEXPERT text 1 Show IP Interface Brief
menu IPEXPERT command 1 show ip interface brief
menu IPEXPERT options 1 pause
menu IPEXPERT text 2 Show IP Route
menu IPEXPERT command 2 show ip route
menu IPEXPERT options 2 pause
menu IPEXPERT text 3 Show IP OSPF Neighbor
menu IPEXPERT command 3 show ip ospf neighbor
menu IPEXPERT text 4 Exit
menu IPEXPERT command 4 Exit
menu IPEXPERT line-mode
menu IPEXPERT single-space

line vty 0 14
 autocommand menu IPEXPERT
```

Although not stated, you must create the crypto key to enable SSH. And note that it states to only accept SSH version 2 on VTY 15 (i.e. no Telnet, no other SSH versions to be used).

This lab takes rotary configuration a step further and has you change the default SSH port R7 is listening too. When you use the command `ip ssh port <num> rotary` group it tells the router to search for the valid group assigned to a VTY. Reference Secure Shell FAQ.

Global configuration is when the command prompt states `<device-name>(config)#`. When the prompt changes to `<device-name>(config-router)#` it is now in router configuration mode. A sub mode to global configuration. Thus we provided the solution to this by entering transport output ssh in line configuration mode `R7(config-line)#`. Don't forget the Console line when doing this.

Menu configuration is a way to limit user access while still given the users the tools they need to service the device. Here we are simply limiting the commands allows on R7 to a few basic show commands but this could also extend to further configuration commands if required.

The `menu <name> text <line number> <text>` specifies what will be displayed on the line to the user. The associated command number should correlate to the same command reference unless you are wanting to mess with your help desks head. Finally, I chose to change the default behavior of a double spaced to single-space purely out of preference.

The `menu <name>` option lines are not required for this task but to pause to the set terminal length to allow users to parse data before moving to the next screen.

IPv6 Considerations

IPv6 addresses can be also used for Device Access/Management.

Verification

```
R7#ssh -l ipexpert -p 2015 7.7.7.7
Password:

R7>

R7>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                 7.7.7.7              00:00:00
*529 vty 15     ipexpert   idle                 00:00:00 7.7.7.7

  Interface    User               Mode         Idle     Peer Address

R7#ssh -l ipexpert 7.7.7.7
```

```
Password:
 DEVICE TELNET MENU
    1          Show IP Interface Brief
    2          Show IP Route
    3          Show IP OSPF Neighbor
    4          Exit

 Please Enter Your Selection : 3

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.71.10        1   FULL/DR         00:00:37    10.1.71.10      FastEthernet0/1
DEVICE TELNET MENU
    1          Show IP Interface Brief
    2          Show IP Route
    3          Show IP OSPF Neighbor
    4          Exit

 Please Enter Your Selection : 1
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES TFTP   up                    up
FastEthernet0/1            10.1.71.7       YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Loopback0                  7.7.7.7         YES manual up                    up
--More-- DEVICE TELNET MENU
    1          Show IP Interface Brief
    2          Show IP Route
    3          Show IP OSPF Neighbor
    4          Exit

 Please Enter Your Selection : 4

[Connection to 7.7.7.7 closed by foreign host]
```

Task 5: Management Restrictions

- Configure R10 to only allow inbound SSH sessions to the VTYs. Accomplish this without the use of an ACL
- Configure R10 to drop all SSH connections except from 10.1.71.0/24 & 2010:1:71::/64
- The administrator of R4 does not want anybody to telnet outbound from this device – you must accomplish this task using a single line ACL on R4
- Outbound telnet traffic from R6 should be sent to Null0
- Telnet and SSH traffic through the routers should not be affected

R10

```
cry key gen rsa mod 768

access-list 5 permit  10.1.71.0 0.0.0.255
```

```
ipv6 access-list VTY
 permit ipv6 2010:1:71::/64 any

line vty 0 4
 login local
 transport input ssh
 access-class 5 in
 ipv6 access-class VTY in

username ipexpert password 0 cisco
```

R6

```
ip telnet source f0/1

ip access-list extended NO_TELNET
 permit tcp host 150.50.116.6 any eq telnet

ipv6 access-list NO_TELNET6
 permit tcp host 2150:50:116::6 any eq telnet

route-map DROP_TELNET_RMAP permit 10
 match ip address NO_TELNET
 set interface Null0

route-map DROP_TELNET6_RMAP permit 10
 match ipv6 address NO_TELNET6
 set interface Null0

ip local policy route-map DROP_TELNET_RMAP
ipv6 local policy route-map DROP_TELNET6_RMAP
```

R4

```
ip telnet source Loopback0

ip access-list extended NO_TELNET
 permit tcp host 4.4.4.4 any eq 23

ipv6 access-list NO_TELNET6
 permit tcp host 2004::4 any eq telnet

ipv6 access-list ND
 permit icmp any any nd-na
 permit icmp any any nd-ns

class-map match-any TELNET_CLASS
 match access-group name NO_TELNET
 match access-group name NO_TELNET6


policy-map DROP_TELNET
 class ND_CLASS
 class TELNET_CLASS
  drop

interface FastEthernet0/1
```

```
 service-policy output DROP_TELNET

interface Serial0/0/0
 service-policy output DROP_TELNET
```

Limiting R10 to only allow SSH inbound should be simple as we already did this in the opposite direction. Or we could accomplish this with a service-policy applied to the control-plane using a Control Plane Port-filter Policy.

Now R10 also needs to limit inbound SSH to only VLAN71. This is where so-called VTY Access Control feature can be useful – watch out for the differences in syntax to apply the ACL (IPv4 vs IPv6).

On R4 you could either use the Control Plane Policing or a service-policy outbound on the interfaces to drop this traffic. Access-lists applied to the interfaces don't affect router-generated packets and we only have one entry here (so even Object Groups would not help you much).

One problem you may run into once you apply the policy is that the ND packets generated by R4 will start getting dropped by the feature on F0/1 interface. This must be a bug – our IPv6 ACL only matches Telnet packets but without an explicit entry for ND traffic those packets are also classified as part of the Telnet class for IPv6.

R6 is configured with Local Policy Based Routing feature – this way transit traffic is not affected.

IPv6 Considerations

As you can see both, MQC techniques and Policy Based Routing feature support IPv6. If you are having problems with figuring out the correct syntax you can always look things up in the IOS IPv6 Configuration Guide.

Verification

```
R7#ssh -l ipexpert 10.1.71.10

Password:

R10>

[Connection to 10.1.71.10 closed by foreign host]

R7#ssh -l ipexpert 2010:1:71::10

Password:
R10>

R7(config)#ip ssh source-interface loop0
```

```
R7#ssh -l ipexpert 10.1.71.10
% Connection refused by remote host

R4#ssh -l ipexpert 2010:1:104::10
% Connection refused by remote host


R4#telnet 150.50.46.6
Trying 150.50.46.6 ...
% Connection timed out; remote host not responding

R4#telnet 2150:50:46::6
Trying 2150:50:46::6 ...
% Connection timed out; remote host not responding

R4#sh access-list
Extended IP access list NO_TELNET
    10 permit tcp host 4.4.4.4 any eq telnet (2 matches)
IPv6 access list FastEthernet0/1-ipsecv6-ACL
    permit 89 FE80::/10 any (21367 matches) sequence 1
IPv6 access list NO_TELNET6
    permit tcp host 2004::4 any eq telnet (2 matches) sequence 10

R4#sh policy-map int f0/1
 FastEthernet0/1

  Service-policy output: DROP_TELNET

    Class-map: ND_CLASS (match-all)
      3 packets, 208 bytes
      5 minute offered rate 0 bps
      Match: access-group name ND

    Class-map: TELNET_CLASS (match-any)
      4 packets, 302 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name NO_TELNET
        2 packets, 174 bytes
        5 minute rate 0 bps
      Match: access-group name NO_TELNET6
        2 packets, 128 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      18 packets, 1694 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
R6#debug ipv6 policy
R6#telnet 2004::4
Trying 2004::4 ...
*Mar  9 18:07:39.518: IPv6 PBR: local, matched src 2150:50:116::6 dst 2004::4
protocol 6
*Mar  9 18:07:39.518: IPv6 PBR: set nexthop 2004::4, interface Null0
*Mar  9 18:07:39.518: IPv6 PBR: policy route via Null0/2004::4
*Mar  9 18:07:41.518: IPv6 PBR: local, matched src 2150:50:116::6 dst 2004::4
protocol 6
*Mar  9 18:07:41.518: IPv6 PBR: set nexthop 2004::4, interface Null0
*Mar  9 18:07:41.518: IPv6 PBR: policy route via Null0/2004::4

R6#telnet 7.7.7.7
Trying 7.7.7.7 ...
% Connection timed out; remote host not responding

R6#sh ip local policy
Local policy routing is enabled, using route map DROP_TELNET_RMAP
route-map DROP_TELNET_RMAP, permit, sequence 10
  Match clauses:
    ip address (access-lists): NO_TELNET
  Set clauses:
    interface Null0
Interface tracking current: NULL
Null0, adj_lh:0,oce:0,status:0

  Policy routing matches: 4 packets, 166 bytes

R6#sh route-map
route-map DROP_TELNET_RMAP, permit, sequence 10
  Match clauses:
    ip address (access-lists): NO_TELNET
  Set clauses:
    interface Null0
Interface tracking current: NULL
Null0, adj_lh:0,oce:0,status:0

  Policy routing matches: 6 packets, 239 bytes
route-map DROP_TELNET6_RMAP, permit, sequence 10
  Match clauses:
     ipv6 address NO_TELNET6
  Set clauses:
    interface Null0
Interface tracking current: NULL
Null0, adj_lh:0,oce:0,status:0

  Policy routing matches: 24 packets, 1514 bytes
```

Task 6: ASA Control Plane protection

- Configure ASA3 to allow VPN connections coming from IP address 11.11.11.11
- Tunnel establishment attempts coming from any other address should be blocked
- Transit traffic should not be affected

ASA3

```
access-list CONTROL extended permit udp host 11.11.11.11 any eq isakmp
access-list CONTROL extended permit udp host 11.11.11.11 any eq 4500
access-list CONTROL extended permit esp host 11.11.11.11 any
access-list CONTROL extended deny udp any any eq isakmp
access-list CONTROL extended deny udp any any eq 4500
access-list CONTROL extended deny esp any any
access-list CONTROL extended permit ip any any

access-group CONTROL in interface outside control-plane
```

It is possible to control management/control/services plane traffic destined to the ASA itself. This can be accomplished by applying an ACL to the interface with the "`control-plane`" option.

An important thing to realize is that with this feature enabled all other commands used to enable the firewall for e.g. management traffic (`telnet`, `ssh`, `http`) have higher precedence than the ACL rules - such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box access list.

IPv6 Considerations

This feature is also supported for IPv6 – apply an IPv6 ACL with the same ("`control-plane`") option.

Verification

R11 was configured to emulate a VPN peer. Only IKE packets coming from 11.11.11.11 are allowed:

```
%ASA-4-106023: Deny udp src outside:150.50.11.11/500 dst identity:150.50.11.30/500
by access-group "CONTROL" [0xd2257af5, 0x0]
%ASA-4-106023: Deny udp src outside:150.50.11.11/500 dst identity:150.50.11.30/500
by access-group "CONTROL" [0xd2257af5, 0x0]
%ASA-4-106023: Deny udp src outside:150.50.11.11/500 dst identity:150.50.11.30/500
by access-group "CONTROL" [0xd2257af5, 0x0]

ASA3# sh access-list CONTROL
access-list CONTROL; 7 elements; name hash: 0xd02e5536
access-list CONTROL line 1 extended permit udp host 11.11.11.11 any eq isakmp
(hitcnt=1) 0xc40af18f
access-list CONTROL line 2 extended permit udp host 11.11.11.11 any eq 4500
(hitcnt=0) 0x76a33844
access-list CONTROL line 3 extended permit esp host 11.11.11.11 any (hitcnt=0)
0x9a22edfe
```

```
access-list CONTROL line 4 extended deny udp any any eq isakmp (hitcnt=6) 0xd2257af5
access-list CONTROL line 5 extended deny udp any any eq 4500 (hitcnt=0) 0x78f23c02
access-list CONTROL line 6 extended deny esp any any (hitcnt=0) 0x3befe516
access-list CONTROL line 7 extended permit ip any any (hitcnt=0) 0x7e9ac143
```

Task 7: Control Plane Policing

- R11 should be configured to protect its CPU using CoPP feature
- Rate-limit all ICMP packets to 15 per second
- Rate-limit all ICMPv6 packets to 70000 bps
- All HTTP packets sent from 5.5.5.5 should be dropped
- Outbound telnet packets destined to 7.7.7.7 should be dropped
- Make sure OSPF packets are not affected by this configuration

R11

```
ip access-list extended ICMP
 permit icmp any any

ipv6 access-list ICMP6
 permit icmp any any

ip access-list extended HTTP_FROM_R5
 permit tcp host 5.5.5.5 any eq www

ip access-list extended TELNET_TO_R7
 permit tcp any host 7.7.7.7 eq telnet

ip access-list extended OSPF
 permit ospf any any


class-map match-all ICMP_CLASS
 match access-group name ICMP

class-map match-all OSPF_CLASS
 match access-group name OSPF

class-map match-all ICMP6_CLASS
 match access-group name ICMP6

class-map match-all TELNET_TO_R7_CLASS
 match access-group name TELNET_TO_R7

class-map match-all HTTP_FROM_R5_CLASS
 match access-group name HTTP_FROM_R5


policy-map COPP_OUT_POL
 class TELNET_TO_R7_CLASS
  drop

policy-map COPP_IN_POL
 class OSPF_CLASS
```

```
 class ICMP_CLASS
  police rate 15 pps burst 5 packets
 class ICMP6_CLASS
  police 70000
 class HTTP_FROM_R5_CLASS
  drop

control-plane
 service-policy input COPP_IN_POL
 service-policy output COPP_OUT_POL
```

Control Plane Policing is kind of a virtual interface that sits before CPU. It provides filtering and rate-limiting capabilities. What is important for us, are two main characteristics of this feature :

1. It works on Aggregate Traffic from all interfaces – it affects ALL packets destined to the Route Processor
2. It can be configured for ingress and egress flows, meaning from the router as well. Note that for the egress direction it does not provide any performance benefits, it is just to limit the traffic leaving the router

To configure CoPP we use well-known MQC syntax. Traffic of interest must be first identified in a class-map and then the policy can be specified inside a policy-map. The main tool used for classification is an Access-List, however NBAR can be used to match ARP and PPPoE packets. The last option is to use DSCP or IP Precedence values.

IPv6 Considerations

This feature is supported for IPv6 (as shown in this task) but the classification engine may be buggy depending on the IOS version.

Verification

```
R11#sh control-plane aggregate features
Control plane aggregate path features :

------------------------------------------------------
Control-plane Policing activated Mar 10 2013 18:1

------------------------------------------------------


R11#telnet 7.7.7.7
Trying 7.7.7.7 ...
% Connection timed out; remote host not responding

R11#sh policy-map control-plane output
 Control Plane
```

```
  Service-policy output: COPP_OUT_POL

    Class-map: TELNET_TO_R7_CLASS (match-all)
      2 packets, 120 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name TELNET_TO_R7
      drop

    Class-map: class-default (match-any)
      52 packets, 6148 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match: any


R6#telnet 150.50.116.11 80
Trying 150.50.116.11, 80 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Sun, 10 Mar 2013 18:22:15 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

R5(config)#ip telnet so l0
R5#telnet 150.50.116.11 80
Trying 150.50.116.11, 80 ...
% Connection timed out; remote host not responding

R11#sh policy-map control-plane input
 Control Plane

  Service-policy input: COPP_IN_POL

    Class-map: OSPF_CLASS (match-all)
      41 packets, 4774 bytes
      5 minute offered rate 0000 bps
      Match: access-group name OSPF

    Class-map: ICMP_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ICMP
      police:
          rate 15 pps, burst 5 packets
        conformed 0 packets, 0 bytes; actions:
          transmit
```

```
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 pps, exceeded 0 pps

    Class-map: ICMP6_CLASS (match-all)
      2 packets, 236 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ICMP6
      police:
          cir 70000 bps, bc 2187 bytes
        conformed 2 packets, 236 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: HTTP_FROM_R5_CLASS (match-all)
      2 packets, 120 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name HTTP_FROM_R5
      drop

    Class-map: class-default (match-any)
      86 packets, 11418 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Note that for IPv4 ICMP size of the packet does not matter since we are controlling pps rate:

```
ASA3# ping 150.50.11.11 rep 15 size 500
Type escape sequence to abort.
Sending 15, 500-byte ICMP Echos to 150.50.11.11, timeout is 2 seconds:
!!!!!?!!!!!?!!!
Success rate is 86 percent (13/15), round-trip min/avg/max = 1/1/1 ms

ASA3# ping 150.50.11.11 rep 15
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 150.50.11.11, timeout is 2 seconds:
!!!!!?!!!!!?!!!
Success rate is 86 percent (13/15), round-trip min/avg/max = 1/1/10 ms

R6#ping 2150:50:116::11 rep 300

Type escape sequence to abort.
Sending 300, 100-byte ICMP Echos to 2150:50:116::11, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!
!!!!.!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!
!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!
!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!
```

```
!!!!!!!!!!!!!!!!!!.!
Success rate is 96 percent (288/300), round-trip min/avg/max = 0/0/4 ms


R11#sh policy-map control-plane input
 Control Plane

  Service-policy input: COPP_IN_POL

    Class-map: OSPF_CLASS (match-all)
      78 packets, 9084 bytes
      5 minute offered rate 0000 bps
      Match: access-group name OSPF

    Class-map: ICMP_CLASS (match-all)
      63 packets, 31782 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ICMP
      police:
          rate 15 pps, burst 5 packets
        conformed 54 packets, 54 bytes; actions:
          transmit
        exceeded 9 packets, 9 bytes; actions:
          drop
        conformed 0 pps, exceeded 0 pps

    Class-map: ICMP6_CLASS (match-all)
      276 packets, 31452 bytes
      5 minute offered rate 3000 bps, drop rate 0000 bps
      Match: access-group name ICMP6
      police:
          cir 70000 bps, bc 2187 bytes
        conformed 264 packets, 30084 bytes; actions:
          transmit
        exceeded 12 packets, 1368 bytes; actions:
          drop
        conformed 3000 bps, exceeded 0000 bps

    Class-map: HTTP_FROM_R5_CLASS (match-all)
      2 packets, 120 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name HTTP_FROM_R5
      drop

    Class-map: class-default (match-any)
      185 packets, 39859 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

```
R11#sh control-plane aggregate counters
Control plane aggregate path counters :

Feature                  Packets Processed/Dropped/Errors

-----------------------------------------------------------
Control-plane Policing       6667/35/0

-----------------------------------------------------------
```

Task 8: Control Plane Protection

- R10 should be configured to protect its CPU using CPPr
- Packets destined to non-listening ports should be dropped
- Telnet connections on port 3020 to VTY line 16 should be allowed
- Input queue of R10 should not be overwhelmed by any single protocol traffic
- No more than 100 BGP and 4 Telnet packets should be seen in the queue
- No more than 30 packets for all other TCP/UDP enabled protocols enabled on the router should be seen in the queue
- Allowed and over the limit Telnet packets should be logged
- All packets allowed by the Host subinterface should be logged and rate-limited to no more than one message every 5 seconds

R10

```
ip cef

line vty 16
 password cisco
 login
 rotary 20

class-map type port-filter match-all PF_CLASS
 match  closed-ports
 match not  port tcp 3020

class-map type queue-threshold match-all TELNET_CLASS
 match  protocol telnet

class-map type queue-threshold match-all BGP_CLASS
 match  protocol bgp

class-map type queue-threshold match-all OTHER_CLASS
 match  host-protocols

class-map type logging match-all LOG_CLASS
 match  packets dropped


policy-map type queue-threshold QT_POL
 class BGP_CLASS
```

```
   queue-limit 100
 class TELNET_CLASS
   queue-limit 6
    log
 class OTHER_CLASS
   queue-limit 30

policy-map type port-filter PF_POL
 class PF_CLASS
   drop

policy-map type logging LOG_POL
 class LOG_CLASS
    log interval 5000

control-plane host
 service-policy type port-filter input PF_POL
 service-policy type queue-threshold input QT_POL
 service-policy type logging input LOG_POL
```

Control Plane Protection allows more granular control (than CoPP) over what packets the router to make a forwarding decision will examine going to the CPU. This feature includes traffic classifier that breaks aggregate interface of Control Plane Policing into three categories, known as subinterfaces:

- CEF Exception
- Host
- And Transit

CEF Exception receives all traffic that is either redirected as a result of a configured input feature in the CEF packet forwarding path for process switching or directly enqueued in the control plane input queue by the interface driver (that is, ARP, external BGP (eBGP), OSPF, LDP, Layer2 Keepalives, and all non-IP host traffic).

Transit subinterface receives all control-plane IP traffic that is software switched by the route processor. This means packets that are not directly destined to the router itself but rather traffic traversing through the router.

Host subinterface receives all control-plane IP traffic that is directly destined for one of the router interfaces. Examples include management traffic or routing protocols such as SSH, SNMP, internal BGP (iBGP), and EIGRP. All host traffic terminates on and is processed by the router. Most control plane protection features and policies operate strictly on the control-plane host subinterface. Since most critical router control plane services, such as routing protocols and management traffic, is received on the control-plane host subinterface, it is critical to protect this traffic through policing and protection

policies. This CPPr component also allows to configure two additional features which are addition to the CoPP technology – Port Filtering and Queue Thresholding.

Port-filtering enhances control plane protection by providing for early dropping of packets directed toward closed or nonlistened IOS TCP/UDP ports on the router. The Port Filter maintains a global database of all open TCP and UDP ports on the router, including random ephemeral ports created by applications. The port database is dynamically populated with entries provided by the registered applications as they start listening on their advertised ports either by configuration of an application (that is SNMP) or initiation of an application (that is, TFTP transfer). Key thing to remember when working with this technology is that it not always correctly update the dynamic port database. There can be many bugs depending on the IOS version that are related to this feature – never forget to test Port Filtering configuration and make some exceptions if necessary (e.g. GDOI, IKE etc.)

Queue Thresholding provides a mechanism for limiting the number of unprocessed packets a protocol can have at process-level. The intent of this feature is to prevent the input queue from being overwhelmed by any single protocol traffic. Same as Port Filtering, Queue Thresholding can be only applied to the Host subinterface.

Control Plane Logging feature can be either configured globally (`type logging` class/policy –map) or within a class-map (class-specific Logging). Global Logging allows to generate a log message for packets allowed, dropped and/or malformed.

Configuration is similar to CoPP. Speaking of differences MQC components can be now of a particular type (`port-filter`, `queue-threshold` and `logging`). If you don't specify a type it means that you are configuring a drop/rate-limit policy.

Finally keep in mind that control Plane Protection feature set depends on Cisco Express Forwarding (CEF) for IP packet redirection – CEF must be always enabled when working with this feature.

IPv6 Considerations
Control Plane Protection feature set is restricted to IPv4 input path only.

Verification

Before an exception was added to the PF_CLASS for port TCP 3020 :

```
R4#telnet 10.1.104.10 3020
Trying 10.1.104.10, 3020 ...
% Connection timed out; remote host not responding
```

After:

```
R4#telnet 10.1.104.10 3020
Trying 10.1.104.10, 3020 ... Open


User Access Verification

Password:
R10>

R10#sh policy-map type port-filter control-plane host
 Control Plane Host

  Service-policy port-filter input: PF_POL

    Class-map: PF_CLASS (match-all)
      7 packets, 420 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  closed-ports
      Match: not  port tcp 3020
      drop

    Class-map: class-default (match-any)
      1226 packets, 73791 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Now test one of the closed ports:

```
R7#telnet 10.1.71.10 99
Trying 10.1.71.10, 99 ...
% Connection timed out; remote host not responding
```

See the Log message (Global Logging feature):

```
R10#
Mar 10 20:40:16.883: %CP-6-TCP: DROP TCP/UDP Portfilter  10.1.71.7(36388) ->
10.1.71.10(99)
```

For queue thresholding try to overwhelm device with Telnet packets (e.g. telnet from itself and other device):

```
R10#
Mar 10 20:31:24.115: %CP-6-TCP: PERMIT  10.1.71.7(16013) -> 10.1.71.10(23)
Mar 10 20:31:24.827: %CP-6-TCP: PERMIT  10.1.71.7(16013) -> 10.1.71.10(23)
```

```
Mar 10 20:35:56.099: %CP-6-TCP: DROP Protocol Queue Thresholding  10.1.71.7(16013) -
> 10.1.71.10(23)


R10#sh policy-map type queue-threshold control-plane host
      queue-limit 100
      queue-count 0     packets allowed/dropped 0/0
      queue-limit 4
      queue-count 4     packets allowed/dropped 28/29

      queue-limit 30
      queue-count 0     packets allowed/dropped 497/0
 Control Plane Host

  Service-policy queue-threshold input: QT_POL

    Class-map: BGP_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  protocol bgp

    Class-map: TELNET_CLASS (match-all)
      57 packets, 3536 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  protocol telnet
      log

    Class-map: OTHER_CLASS (match-all)
      497 packets, 29826 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  host-protocols

    Class-map: class-default (match-any)
      1 packets, 60 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

R10#sh policy-map type logging control-plane host

 Control Plane Host

  Service-policy logging input: LOG_POL

    Class-map: LOG_CLASS (match-all)
      19 packets, 1152 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  packets dropped
      log interval 5000
```

```
    Class-map: class-default (match-any)
      12 packets, 722 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any


R10#sh control-plane features
Total 3 features configured

Control plane host path features :

------------------------------------------------------
Control-plane Logging activated Mar 10 2013 20:3
TCP/UDP Portfilter activated Mar 10 2013 20:1
Protocol Queue Thresholding activated Mar 10 2013 20:2

------------------------------------------------------


R10#sh control-plane host counters
Control plane host path counters :

Feature                   Packets Processed/Dropped/Errors

------------------------------------------------------
Control-plane Logging          17/0/0
TCP/UDP Portfilter           1230/7/0
Protocol Queue Threshold     1202/89/0

------------------------------------------------------
```

Task 9: Management Plane Protection

- Only allow SSH and HTTP packets to R4
- Don’t use any access-list or VTY line modification to accomplish this task
- Management traffic should be only allowed through the F0/1 interface

R4

```
ip domain-name ipexpert.com

cry key gen rsa mod 768

username ipexpert pass cisco

line vty 0 4
 login local

control-plane host
 management-interface FastEthernet0/1 allow http ssh
```

Management Plane Protection provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. After designating one or more interfaces for management, traffic is permitted to enter a device only through these management interfaces. No interfaces except designated management interfaces will accept network management traffic destined to the device.

To configure MPP use the "`management-interface`" command under Host subinterface. More than one interface can be designated for management (by adding another command).

IPv6 Considerations

Management Plane Protection feature does not work with IPv6.

Verification

```
R4#sh control-plane features
Total 1 features configured

Control plane host path features :

------------------------------------------------------
Management-Interface activated Mar 10 2013 21:2
```

```
R11#sh control-plane aggregate features
Control plane aggregate path features :

R11#telnet 4.4.4.4
Trying 4.4.4.4 ...
% Connection timed out; remote host not responding

R10#ssh -l ipexpert 10.1.104.4
Password:

R4>

R10#telnet 10.1.104.4 80
Trying 10.1.104.4, 80 ... Open
get ./
HTTP/1.1 400 Bad Request
Date: Sun, 10 Mar 2013 21:31:02 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request
```

```
[Connection to 10.1.104.4 closed by foreign host]

R4#sh management-interface
Management interface FastEthernet0/1
        Protocol        Packets processed
            http                33
             ssh                38

R4#sh control-plane host counters
Control plane host path counters :

Feature                   Packets Processed/Dropped/Errors

-------------------------------------------------------
Management-Interface             77/6/0

-------------------------------------------------------
```

Task 10: NTP

- All involved routers except R5 should source NTP requests from their Loop 0 interface
- Set R4 as NTP master with a stratum of 2
- R6 should get its time from R4 and send NTP log messages to 150.50.116.200
- R6 should periodically update the hardware clock from NTP time source
- Configure R10 as NTP server (stratum 4); R5 & R11 should act as NTP Clients
- NTP packets exchanged between those three routers should be using IPv6 for transport
- If one of the clients loses connectivity to the server it should obtain time from its peer
- All devices should account for daylight savings time
- All NTP communication should be authenticated (use key “ipexpert”)

R4

```
ntp source Loopback0

ntp authentication-key 1 md5 ipexpert
ntp trusted-key 1
ntp master 2


clock summer-time CST recurring
```

R6

```
ntp source Loopback0

ntp authentication-key 1 md5 ipexpert
ntp authenticate
ntp trusted-key 1
ntp server 4.4.4.4 key 1
ntp logging

ntp update calendar
```

```
logging host 150.50.116.200
logging trap debugging

clock summer-time CST recurring
```

R5

```
ntp source F0/1

ntp authentication-key 1 md5 ipexpert
ntp authenticate
ntp trusted-key 1

ntp server 2010::10 key 1 version 4
ntp peer 2011::11 key 1 ver 4

clock summer-time CST recurring
```

R10

```
interface Loopback0
 ipv6 address 2010::10/64
 ipv6 ospf 1 area 0

ntp source Loopback0

ntp authentication-key 1 md5 ipexpert
ntp authenticate
ntp trusted-key 1

ntp master 4

clock summer-time CST recurring
```

R11

```
int l0
 ipv6 address 2011::11/64
 ipv6 eigrp 1

ntp source Loopback0

ntp authentication-key 1 md5 ipexpert
ntp authenticate
ntp trusted-key 1

ntp server 2010::10 key 1 ver 4
ntp peer 2010:1:5::5 key 1 ver 4

clock summer-time CST recurring
```

ASA3

```
ipv6 access-list OUTSIDE6_IN permit udp host 2011::11 host 2010:1:5::5 eq ntp
```

NTP configuration should be a core technology that you are aware of knowing how to configure 80% of the tasks above by heart when you feel prepared to take the exam.

Although in past experience trusted-key was only required on clients to servers, in the current releases you must configure it on both clients and servers. One thing not needed on the server side is enabling authentication (`ntp authenticate`) – this is because in NTP it is the client what's authenticating time information and not the server (unless your server is also configured as a NTP peer; then you need to enable authentication & specify keys on both Peers as well).

You may or may not be familiar with the various time zone codes. I do not think it is as important to know the name abbreviations for these. This information would most likely be given to you the test as the test is not focused on your knowledge of global time zones. One trick you could use is to go to ISE's CLI and issue the "`show timezones`" command – although it rather shows full names instead of abbreviations it may be still useful at some times.

Most routers have internal clocks, such as these 2811s. This way, even when you reboot the router, the time is still there. The Catalyst Switches do not have a hardware clock.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift) and the software clock and hardware clock may become out of synchronization with each other. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

NTP Version 4 (NTPv4) is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3. For NTPv4, it works in much the same way as does its older version. The main advantage is support of IPv6 as the transport (UDP port 123 is still the same) and enhanced security.

IPv6 Considerations

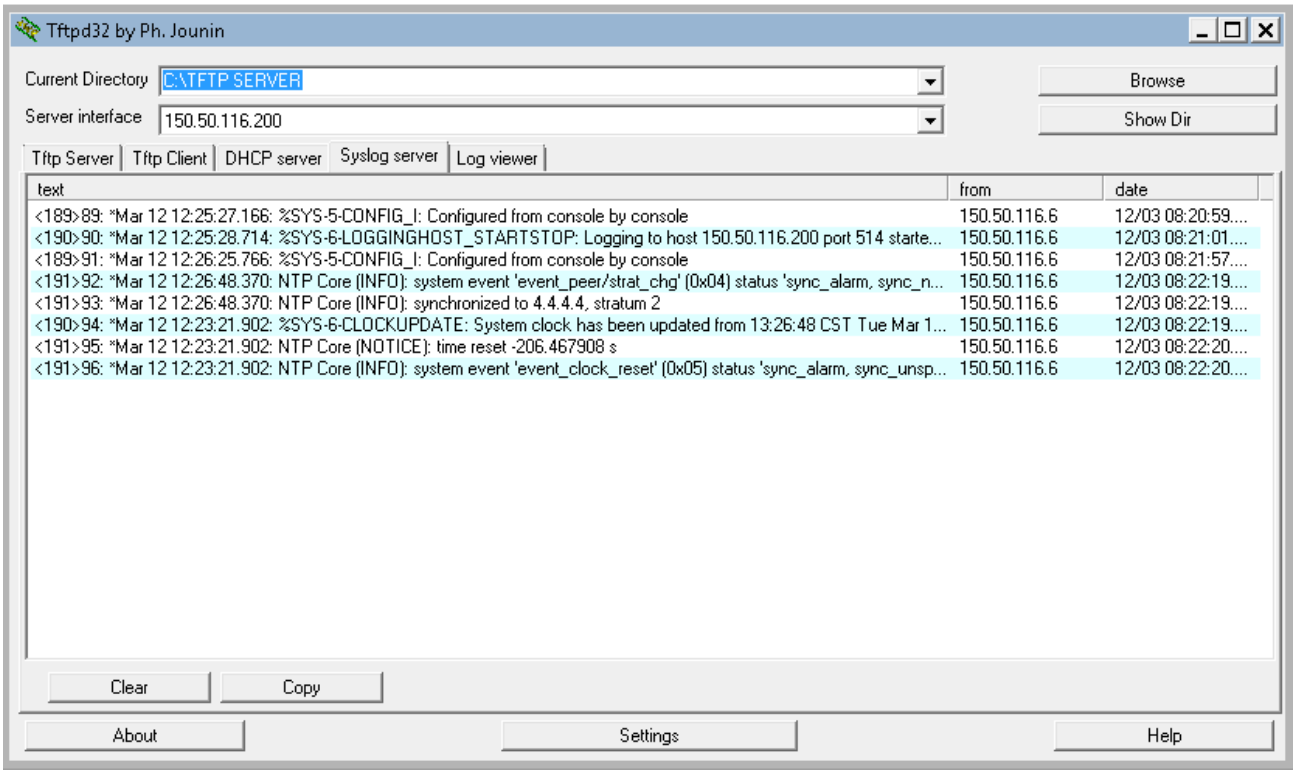
Supported in NTP version 4 (default on newer code versions). Just use IPv6 addresses instead of IPv4.

Verification

```
R6#sh ntp association det
4.4.4.4 configured, authenticated, our_master, sane, valid, stratum 2
ref ID 127.127.1.1   , time D4E99FFA.7C471004 (13:37:14.485 CST Tue Mar 12 2013)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.28, reach 377, sync dist 19.35
delay 19.11 msec, offset 9.8405 msec, dispersion 5.33
precision 2**24, version 4
org time D4E99FFF.E9A890B1 (13:37:19.912 CST Tue Mar 12 2013)
rec time D4E99FFF.E813D5D4 (13:37:19.906 CST Tue Mar 12 2013)
xmt time D4E99FFF.E3143650 (13:37:19.887 CST Tue Mar 12 2013)
filtdelay =    19.37   19.30   19.51   19.25   19.45   19.27   19.11   19.23
```

```
filtoffset =    15.86    14.83    13.82    12.76    11.90    10.72     9.84     8.56
filterror =      0.00     0.94     1.92     2.88     3.85     4.84     5.82     6.78
minpoll = 6, maxpoll = 10
```

Quick look at the logs on the Test PC which was configured with 150.50.116.200 in VLAN 116:



Note whenever you configure an IOS router as NTP Server in stratum X the device internally creates a server with stratum X-1 (127.127.1.1 but the IP address used may depend on platform & IOS version) to which it synchronizes. This is something you would have to account for when dealing with NTP ACLs (not part of this task):

```
R10#sh ntp asso det
127.127.1.1 configured, our_master, sane, valid, stratum 3
ref ID .LOCL., time D4E99EC6.0152E525 (13:32:06.005 CST Tue Mar 12 2013)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 1.00
delay 0.00 msec, offset 0.0000 msec, dispersion 0.23
precision 2**21, version 4
org time D4E99EC6.0152E525 (13:32:06.005 CST Tue Mar 12 2013)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D4E99EC6.0152C3D3 (13:32:06.005 CST Tue Mar 12 2013)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.24    0.48    0.72    0.96    1.20    1.44    1.68
```

```
minpoll = 4, maxpoll = 4

R10#sh ntp status
Clock is synchronized, stratum 4, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0005 Hz, precision is 2**21
reference time is D4E99EC6.01531CFB (13:32:06.005 CST Tue Mar 12 2013)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.23 msec, peer dispersion is 0.23 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000002156 s/s
system poll interval is 16, last update was 0 sec ago.
```

Looking at R5 and R11 – they both prefer R10 which is Stratum 4 rather than their peer which is one more stratum away (that's how NTP works):

```
R11#sh ntp asso det
2010::10 configured, authenticated, our_master, sane, valid, stratum 4
ref ID 127.127.1.1     , time D4E9A776.000F0351 (14:09:10.000 CST Tue Mar 12 2013)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.39, reach 377, sync dist 15.60
delay 20.37 msec, offset 1.0236 msec, dispersion 4.37
precision 2**21, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time D4E9A781.733C044C (14:09:21.450 CST Tue Mar 12 2013)
xmt time D4E9A781.733C044C (14:09:21.450 CST Tue Mar 12 2013)
filtdelay =    20.48   20.43   20.44   20.56   20.37   20.58   20.44   20.42
filtoffset =    1.00    0.95    0.98    0.97    1.02    1.03    1.02    0.96
filterror =     0.00    0.99    1.99    2.98    4.00    5.01    6.04    7.06
minpoll = 6, maxpoll = 10

2010:1:5::5 configured, authenticated, insane, invalid, stratum 5
ref ID 145.202.40.145 , time D4E9A6BA.ABA9241B (14:06:02.670 CST Tue Mar 12 2013)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 21.43 msec, root disp 8.10, reach 6, sync dist 3958.34
delay 2.02 msec, offset -0.4135 msec, dispersion 3937.74
precision 2**24, version 4
org time D4E9A786.7057CAD8 (14:09:26.438 CST Tue Mar 12 2013)
rec time D4E9A776.A729CFEF (14:09:10.652 CST Tue Mar 12 2013)
xmt time D4E9A776.A729CFEF (14:09:10.652 CST Tue Mar 12 2013)
filtdelay =     2.02    2.05    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =   -0.41   -0.41    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.97 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10


R11#sh ntp status
Clock is synchronized, stratum 5, reference is 145.202.40.145
nominal freq is 250.0000 Hz, actual freq is 250.0008 Hz, precision is 2**21
reference time is D4E9A781.75994315 (14:09:21.459 CST Tue Mar 12 2013)
clock offset is 1.0236 msec, root delay is 20.37 msec
```

```
root dispersion is 6.78 msec, peer dispersion is 4.37 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000003530 s/s
system poll interval is 64, last update was 64 sec ago.


R5#sh ntp asso det
2010::10 configured, authenticated, our_master, sane, valid, stratum 4
ref ID 127.127.1.1   , time D4E9A776.000F0351 (14:09:10.000 CST Tue Mar 12 2013)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.33, reach 376, sync dist 15.44
delay 21.44 msec, offset 1.3800 msec, dispersion 3.11
precision 2**21, version 4
org time D4E9A77D.AA598F62 (14:09:17.665 CST Tue Mar 12 2013)
rec time D4E9A77D.ACCCE890 (14:09:17.675 CST Tue Mar 12 2013)
xmt time D4E9A7BF.A78F06A0 (14:10:23.654 CST Tue Mar 12 2013)
filtdelay =    21.84   21.68   21.71   21.44   21.66   21.76   21.70   21.79
filtoffset =    1.34    1.32    1.40    1.38    1.39    1.35    1.54    1.51
filterror =     0.00    0.99    1.95    2.92    3.87    4.86    5.82    7.75
minpoll = 6, maxpoll = 10

2011::11 configured, authenticated, insane, invalid, stratum 5
ref ID 145.202.40.145, time D4E9A781.75994315 (14:09:21.459 CST Tue Mar 12 2013)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 20.37 msec, root disp 6.94, reach 367, sync dist 40.69
delay 2.01 msec, offset 0.4387 msec, dispersion 2.10
precision 2**21, version 4
org time D4E9A7CB.704CFC37 (14:10:35.438 CST Tue Mar 12 2013)
rec time D4E9A7CB.707DB20A (14:10:35.439 CST Tue Mar 12 2013)
xmt time D4E9A7B6.A7820441 (14:10:14.654 CST Tue Mar 12 2013)
filtdelay =     2.10    2.03    2.04    2.01    2.07    2.11    2.01    2.04
filtoffset =    0.30    0.40    0.42    0.43    0.40    0.38    0.43    0.42
filterror =     0.31    1.27    2.24    2.24    2.24    2.24    2.24    2.24
minpoll = 6, maxpoll = 10


R5#sh ntp status
Clock is synchronized, stratum 5, reference is 145.202.40.145
nominal freq is 250.0000 Hz, actual freq is 249.9950 Hz, precision is 2**24
reference time is D4E9A6BA.ABA9241B (14:06:02.670 CST Tue Mar 12 2013)
clock offset is 1.3800 msec, root delay is 21.44 msec
root dispersion is 9.65 msec, peer dispersion is 3.11 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000019967 s/s
system poll interval is 64, last update was 291 sec ago.
```

Now we're going to simulate a failure in communication between R5 and R10 – an IPv6 ACL was applied that blocks NTP packets from R5. As a result R5 should now synchronize to its peer - R11:

```
R5#sh ntp asso det
2010::10 configured, authenticated, insane, invalid, unsynced, stratum 16
```

```
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.32
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D4E9A9CB.AA641D5E (14:19:07.665 CST Tue Mar 12 2013)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10

2011::11 configured, authenticated, our_master, sane, valid, stratum 5
ref ID 145.202.40.145, time D4E9A88C.756902EF (14:13:48.458 CST Tue Mar 12 2013)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 20.38 msec, root disp 8.85, reach 36, sync dist 980.62
delay 1.99 msec, offset 0.4626 msec, dispersion 939.25
precision 2**21, version 4
org time D4E9A9A6.6FF96CA2 (14:18:30.437 CST Tue Mar 12 2013)
rec time D4E9A9A6.701C60C2 (14:18:30.437 CST Tue Mar 12 2013)
xmt time D4E9A9AE.AA351036 (14:18:38.664 CST Tue Mar 12 2013)
filtdelay =     2.01    1.99    2.11    2.08    0.00    0.00    0.00    0.00
filtoffset =    0.47    0.46    0.39    0.42    0.00    0.00    0.00    0.00
filterror =     0.85    1.81    2.78    3.73 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10


R5#sh ntp status
Clock is synchronized, stratum 6, reference is 168.87.230.18
nominal freq is 250.0000 Hz, actual freq is 249.9950 Hz, precision is 2**24
reference time is D4E9A9A6.701C60C2 (14:18:30.437 CST Tue Mar 12 2013)
clock offset is 0.4626 msec, root delay is 22.37 msec
root dispersion is 950.16 msec, peer dispersion is 439.88 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000019969 s/s
system poll interval is 64, last update was 102 sec ago.
```

Task 11: SNMP & CPU Statistical Gathering

- Configure R5 to allow SNMP polls from 10.1.5.0/24 using version 2c
- Only allow SNMP GET packets to be processed – use community string “ipexpert”
- R5 typically runs between 20 to 40% CPU utilization. Lately it has been running high CPU utilization at times
- To find the source of the problem configure R5 to send a SNMP Trap to 2010:1:5::100 any time the total CPU utilization hits 65%
- Encrypt & authenticate SNMP packets using 3DES and SHA; use “ipexpert” as keys
- You will also want it to inform you once it falls back below 50% to allow you to do trend analysis. Use a 5 second polling interval
- Only gather statistics for processes that use at least 3% of processor time. Gather the last 400 seconds of history

R5

```
snmp-server community ipexpert RO 5

snmp-server group SGROUP v3 priv
snmp-ser user SUSER SGROUP v3 auth sha ipexpert priv 3des ipexpert

snmp-server enable traps cpu threshold
snmp-server host 2010:1:5::100 version 3 priv SUSER  cpu

process cpu threshold type total rising 65 interval 5 falling 50 interval 5
process cpu statistics limit entry-percentage 3 size 400
```

SNMP Polling is a process of sending periodic queries (GET messages) to the network devices. Note that because queries are periodic, setting a correct poll interval is always a trade-off between excessive bandwidth usage and on-time failure detection. Polling can be also used to modify a value of a particular MIB element – this is what SET messages are used for.

Independent of this polling interaction, the agent can send the manager unsolicited SNMP Notifications to notify the manager about network conditions. There are two types of SNMP Notifications – TRAPS and INFORMS. Traps are less reliable than Informs, because the receiver does not send an acknowledgment when it receives a trap. Informs are always ACKed.

SNMP version 3 moves away from the community string approach in favor of user-based authentication and view-based access control. The users are not actual local user accounts, rather they are simply a means to determine who can authenticate to the device and how SNMP Traps should be protected. The view is used to define what MIB objects the user account may access on the IOS device. Finally, each user is added to a group, which determines the security model (noAuthNoPriv, AuthNoPriv, AuthPriv).

The CPU Thresholding Notification feature notifies users when generating a SNMP trap message for the top users of the CPU crosses a predefined threshold of CPU usage.

IPv6 Considerations

Fully supported. The command structure is almost exactly the same as in IPv4, the only difference is that for an access-list used to restrict management access to some certain devices we need to add the `ipv6` keyword to the `snmp-server` command.

Verification

```
R5#sh snmp user SUSER

User name: SUSER
Engine ID: 800000090300001BD50FF2F8
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: 3DES
Group-name: SGROUP

R5#sh snmp host
Notification host: 2010:1:5::100         udp-port: 162    type: trap
user: SUSER      security model: v3 priv


R5#deb snmp packets
SNMP packet debugging is on
```

Now generate some CPU intensive tasks (like write-mem) and observe the debugs syslog & debugs:

```
Mar 12 18:15:22.343: %SYS-1-CPURISINGTHRESHOLD: Threshold: Total CPU
Utilization(Total/Intr): 76%/0%, Top 3 processes(Pid/Util):  12/75%, 114/0%,
29/0%[OK]

R5#
Mar 12 18:17:22.525: SNMP: Queuing packet to 2010:1:5::100
Mar 12 18:17:22.525: SNMP: V2 Trap, reqid 1, errstat 0, erridx 0
 sysUpTime.0 = 45668518
 snmpTrapOID.0 = ciscoProcessMIB.2.0.1
 cpmCPUThresholdTable.1.2.1.1 = 65
 cpmCPUTotalTable.1.10.1 = 76
 cpmCPUTotalTable.1.11.1 = 0
 ciscoProcessMIB.1.2.3.1.5.1.12 = 75
 cpmProcessTable.1.5.1.12 = 45656494
Mar 12 18:17:22.777: SNMP: Packet sent via UDP to 2010:1:5::100


R5#sh snmp
Chassis: FTX1123F06Q
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
```

```
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
1 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    1 Trap PDUs
SNMP Dispatcher:
   queue 0/75 (current/max), 0 dropped
SNMP Engine:
   queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
    Logging to 2010:1:5::100.162, 0/10, 1 sent, 0 dropped.
```

Task 12: DHCP & DHCPv6

- Enable R5 as a DHCP Server with the following information :
  - Network 10.1.5.0 /24
  - WINS address 10.1.5.135
  - DNS address 10.1.5.53
  - Default Gateway 10.1.5.30
  - Lease Time 3 days 12 hours
- Enable Conflict Logging
- Enable option 19 to configure clients to do IP layer packet forwarding
- Make sure the router securely updates the ARP Table
- Specify five ping attempts by the DHCP server before ceasing any further ping attempts
- Configure CAT3 as a DHCPv6 Server for VLAN 116
- Assign a domain-name “ipexpert.com”
- CAT4 should obtain an IPv6 address from CAT3 on its SVI 116

R5

```
ip dhcp pool DPOOL
 network 10.1.5.0 255.255.255.0
 netbios-name-server 10.1.5.135
 dns-server 10.1.5.53
 default-router 10.1.5.30
 lease 3 12
 option 19 hex 01
 update arp
```

```
ip dhcp conflict logging

ip dhcp excluded-address 10.1.5.5
ip dhcp excluded-address 10.1.5.30
ip dhcp excluded-address 10.1.5.53
ip dhcp excluded-address 10.1.1.135

ip dhcp ping packets 5
```

CAT3

```
ipv6 dhcp pool DPOOL6
 address prefix 2150:50:116::/64
 domain-name ipexpert.com

interface Vlan116
 ipv6 address 2150:50:116::133/64
 ipv6 dhcp server DPOOL6
```

CAT4

```
interface Vlan116
 ipv6 enable
 ipv6 address dhcp
```

Configuring DHCP on an IOS router is pretty straight forward and is probably not required to know most of the advanced features for the Security exam. So we won't go into a lot of detail here. Understanding the above configuration is important as other security features like DHCP Snooping are covered by the exam so understanding the functionality of DHCP is important.

Cisco recommends using a DHCP server database agent to store automatic bindings. By default, the Cisco IOS DHCP Server records DHCP address conflicts in a log file.

I don't imagine they are going to ask many option questions without giving you additional detail on the exam, since it is hard to find any options in the Cisco Documentation. But a full list of the DHCP options can be found on IANA's website.

The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use, and assigns the address to a new requesting client.

IPv6 Considerations

DHCPv6 clients and servers use UDP (ports 546/547) to exchange messages. The client will make use of Link Local addressing to send and receive DHCPv6 messages. DHCPv6 servers make use of the reserved link-local "ff02::1:2" (All DHCPv6 relay agents and servers) and site-local "ff05::1:3" (All DHCPv6 Servers) multicast addresses.
Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. A practical example would be the stateful address assignment of

"2150:50:116:abc:abc:123:123:123" from a DHCPv6 server to a DHCPv6 client. Note that this type of configuration does NOT include subnet information. To assign complete subnets and other interface parameters so-called Prefix Delegation could be used, which is an extension to DHCPv6. This feature is probably outside the scope of the CCIE Security lab.

Note that basic DHCPv6 configuration is somewhat different from IPv4 in a way that we need to activate the server functionality on the interface using the `ipv6 dhcp server` command (the `automatic` keyword, if used, forces the router to find a matching pool automatically – in our case we have specified the pool explicitly).

Verification

```
CAT2(config)#int vlan 305
CAT2(config-if)#ip add dhcp

*May 21 18:18:57.245: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan305 assigned DHCP
address 10.1.5.1, mask 255.255.255.0, hostname CAT2

R5#sh ip dhcp pool

Pool DPOOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.1.5.2             10.1.5.1         - 10.1.5.254        1

R5#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.1.5.1            0063.6973.636f.2d30.    Mar 16 2013 08:54 AM    Automatic
                    3031.622e.6434.6331.
                    2e35.3434.322d.566c.
                    3330.35
```

For IPv6 let's first quickly verify the server config and take a look at the DHCPv6 message exchange between our switches. The process start with sending an equivalent of DHCPv4 DISCOVERY message which in IPv6 is called "SOLICIT":

```
CAT3#sh ipv dhcp int
Vlan116 is in server mode
```

```
  Using pool: DPOOL6
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit: disabled


CAT3#deb ipv dhcp det
CAT4#debug ipv6 dhcp

CAT4#
*Mar 14 21:25:41.806: IPv6 DHCP: Sending SOLICIT to FF02::1:2 on Vlan116

CAT3#
Mar 12 20:34:06.952: IPv6 DHCP: Received SOLICIT from FE80::207:7DFF:FEBC:C6C5 on
Vlan116
Mar 12 20:34:06.952: IPv6 DHCP: detailed packet contents
Mar 12 20:34:06.952:   src FE80::207:7DFF:FEBC:C6C5 (Vlan116)
Mar 12 20:34:06.952:   dst FF02::1:2
Mar 12 20:34:06.952:   type SOLICIT(1), xid 1079494
Mar 12 20:34:06.952:   option ELAPSED-TIME(8), len 2
Mar 12 20:34:06.952:     elapsed-time 0
Mar 12 20:34:06.952:   option CLIENTID(1), len 10
Mar 12 20:34:06.952:     0003000100077DBCC680
Mar 12 2034:06.952:   option ORO(6), len 4
Mar 12 20:34:06.952:     DNS-SERVERS,DOMAIN-LIST
Mar 12 20:34:06.952:   option IA-NA(3), len 12
Mar 12 20:34:06.952:     IAID 0x08880001, T1 0, T2 0
```

Since CAT3 received the SOLICIT message on SVI 116 it uses “DPOOL6” to allocate an IPv6 address:

```
Mar 12 20:34:06.952: IPv6 DHCP: Using interface pool DPOOL6
Mar 12 20:34:06.952: IPv6 DHCP: Creating binding for FE80::207:7DFF:FEBC:C6C5 in
pool DPOOL6
Mar 12 20:34:06.952: IPv6 DHCP: Binding for IA_NA 08880001 not found  20:34:06.960:
IPv6 DHCP: Allocating IA_NA 08880001 in binding for FE80::207:7DFF:FEBC:C6C5
Mar 12 20:34:06.960: IPv6 DHCP: Looking up pool 2150:50:116::/64 entry with username
'0003000100077DBCC68008880001'
Mar 12 20:34:06.960: IPv6 DHCP: Poolentry for user not found
Mar 12 20:34:06.960: IPv6 DHCP: Allocated new address
2150:50:116:0:B95A:D7C:435B:D7EA
Mar 12 20:34:06.960: IPv6 DHCP: Allocating address 2150:50:116:0:B95A:D7C:435B:D7EA
in binding for FE80::207:7DFF:FEBC:C6C5, IAID 08880001
Mar 12 20:34:06.960: IPv6 DHCP: Updating binding address entry for address
2150:50:116:0:B95A:D7C:435B:D7EA
Mar 12 20:34:06.960: IPv6 DHCP: Setting timer on 2150:50:116:0:B95A:D7C:435B:D7EA
for 60 seconds
```

The ADVERTISE message is an equivalent of v4 OFFER:

```
CAT3#
Mar 12 20:34:06.960: IPv6 DHCP: Sending ADVERTISE to FE80::207:7DFF:FEBC:C6C5 on
Vlan116
Mar 12 20:34:06.960: IPv6 DHCP: detailed packet contents
Mar 12 20:34:06.960:   src FE80::C664:13FF:FED1:C5C4
Mar 12 20:34:06.960:   dst FE80::207:7DFF:FEBC:C6C5 (Vlan116)
Mar 12 20:34:06.960:   type ADVERTISE(2), xid 1079494
Mar 12 20:34:06.960:   option SERVERID(2), len 10
Mar 12 20:34:06.960:     00030001C46413D1C580
Mar 12 20:34:06.960:   option CLIENTID(1), len 10
Mar 12 20:34:06.960:     0003000100077DBCC680
Mar 12 20:34:06.960:   option IA-NA(3), len 40
Mar 12 20:34:06.960:     IAID 0x08880001, T1 43200, T2 69120
Mar 12 20:34:06.960:     option IAADDR(5), len 24
Mar 12 20:34:06.960:       IPv6 address 2150:50:116:0:B95A:D7C:435B:D7EA
Mar 12 20:34:06.960:       preferred 86400, valid 172800
Mar 12 20:34:06.960:   option DOMAIN-LIST(24), len 14
Mar 12 20:34:06.960:     ipexpert.com


CAT4#
*Mar 14 21:25:41.831: IPv6 DHCP: Received ADVERTISE from FE80::C664:13FF:FED1:C5C4
on Vlan116
*Mar 14 21:25:41.831: IPv6 DHCP: Adding server FE80::C664:13FF:FED1:C5C4
```

REQUEST is REQUEST ☺

```
CAT4#
*Mar 14 21:25:43.005: IPv6 DHCP: Sending REQUEST to FF02::1:2 on Vlan116
*Mar 14 21:25:43.005: IPv6 DHCP: DHCPv6 address changes state from SOLICIT to
REQUEST (ADDR_ADVERTISE_RECEIVED) on Vlan116
```

The client has no problems with the proposed address and wants to have it assigned. The server finally responds with the REPLY message (v4 ACK):

```
CAT3#
Mar 12 20:34:08.151: IPv6 DHCP: Received REQUEST from FE80::207:7DFF:FEBC:C6C5 on
Vlan116
Mar 12 20:34:08.151: IPv6 DHCP: detailed packet contents
Mar 12 20:34:08.151:   src FE80::207:7DFF:FEBC:C6C5 (Vlan116)
Mar 12 20:34:08.151:   dst FF02::1:2
Mar 12 20:34:08.151:   type REQUEST(3), xid 1081719
Mar 12 20:34:08.151:   option ELAPSED-TIME(8), len 2
Mar 12 20:34:08.151:     elapsed-time 0
Mar 12 20:34:08.151:   option CLIENTID(1), len 10
Mar 12 20:34:08.151:     0003000100077DBCC680
Mar 12 20:34:08.151:   option ORO(6), len 4
Mar 12 20:34:08.151:     DNS-SERVERS,DOMAIN-LIST
```

```
Mar 12 20:34:08.151:   option SERVERID(2), len 10
Mar 12 20:34:08.151:     00030001C46413D1C580
Mar 12 20:34:08.151:   option IA-NA(3), len 40
Mar 12 20:34:08.151:     IAID 0x08880001, T1 0, T2 0
Mar 12 20:34:08.151:     option IAADDR(5), len 24
Mar 12 20:34:08.151:       IPv6 address 2150:50:116:0:B95A:D7C:435B:D7EA
Mar 12 20:34:08.160:       preferred 86400, valid 172800
Mar 12 20:34:08.160: IPv6 DHCP: Using interface pool DPOOL6
Mar 12 20:34:08.160: IPv6 DHCP: Looking up pool 2150:50:116::/64 entry with username
'0003000100077DBCC68008880001'
Mar 12 20:34:08.160: IPv6 DHCP: Poolentry for user found
Mar 12 20:34:08.160: IPv6 DHCP: Found address 2150:50:116:0:B95A:D7C:435B:D7EA in
binding for FE80::207:7DFF:FEBC:C6C5, IAID 08880001
Mar 12 20:34:08.160: IPv6 DHCP: Updating binding address entry for address
2150:50:116:0:B95A:D7C:435B:D7EA
Mar 12 20:34:08.160: IPv6 DHCP: Setting timer on 2150:50:116:0:B95A:D7C:435B:D7EA
for 172800 seconds


Mar 12 20:34:08.160: IPv6 DHCP: Sending REPLY to FE80::207:7DFF:FEBC:C6C5 on Vlan116
Mar 12 20:34:08.160: IPv6 DHCP: detailed packet contents
Mar 12 20:34:08.160:   src FE80::C664:13FF:FED1:C5C4
Mar 12 20:34:08.160:   dst FE80::207:7DFF:FEBC:C6C5 (Vlan116)
Mar 12 20:34:08.160:   type REPLY(7), xid 1081719
Mar 12 20:34:08.160:   option SERVERID(2), len 10
Mar 12 20:34:08.160:     00030001C46413D1C580
Mar 12 20:34:08.160:   option CLIENTID(1), len 10
Mar 12 20:34:08.160:     0003000100077DBCC680
Mar 12 20:34:08.160:   option IA-NA(3), len 40
Mar 12 20:34:08.160:     IAID 0x08880001, T1 43200, T2 69120
Mar 12 20:34:08.160:     option IAADDR(5), len 24
Mar 12 20:34:08.160:       IPv6 address 2150:50:116:0:B95A:D7C:435B:D7EA
Mar 12 20:34:08.160:       preferred 86400, valid 172800
Mar 12 20:34:08.160:   option DOMAIN-LIST(24), len 14
Mar 12 20:34:08.160:     ipexpert.com
```

The address is finally assigned to the SVI and CAT3 starts using it:

```
CAT4#
*Mar 14 21:25:43.014: IPv6 DHCP: Received REPLY from FE80::C664:13FF
CAT4#:FED1:C5C4 on Vlan116
*Mar 14 21:25:43.014: IPv6 DHCP: Processing options
*Mar 14 21:25:43.014: IPv6 DHCP: Adding address
2150:50:116:0:A01F:368D:8CEE:4439/128 to Vlan116
*Mar 14 21:25:43.014: IPv6 DHCP: T1 set to expire in 43200 seconds
*Mar 14 21:25:43.014: IPv6 DHCP: T2 set to expire in 69120 seconds
*Mar 14 21:25:43.014: IPv6 DHCP: Configuring domain name ipexpert.com
*Mar 14 21:25:43.022: IPv6 DHCP: DHCPv6 address changes state from REQUEST to OPEN
(ADDR_REPLY_RECEIVED) on Vlan116
```

```
CAT4#sh ipv6 dhcp int
Vlan116 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:47:57
  List of known servers:
    Reachable via address: FE80::C664:13FF:FED1:C5C4
    DUID: 00030001C46413D1C580
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x08880001, T1 43200, T2 69120
        Address: 2150:50:116:0:B95A:D7C:435B:D7EA /128
                 preferred lifetime 86400, valid lifetime 172800
                 expires at Mar 16 1993 09:25 PM (172078 seconds)
      Domain name: ipexpert.com
      Information refresh time: 0
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled

CAT4#sh ipv int br vlan116
Vlan116                    [up/up]
    FE80::207:7DFF:FEBC:C6C5
    2150:50:116:0:B95A:D7C:435B:D7EA


CAT3#sh ipv dhcp pool
DHCPv6 pool: DPOOL6
  Address allocation prefix: 2150:50:116::/64 valid 172800 preferred 86400 (1 in
use, 0 conflicts)
  Domain name: ipexpert.com
  Active clients: 1

CAT3#sh ipv dhcp bindi
Client: FE80::207:7DFF:FEBC:C6C5 (Vlan116)
  DUID: 0003000100077DBCC680
  IA NA: IA ID 0x08880001, T1 43200, T2 69120
    Address: 2150:50:116:0:B95A:D7C:435B:D7EA
             preferred lifetime 86400, valid lifetime 172800
             expires at Mar 14 2013 08:57 PM (172718 seconds)
```

Task 13: Unnecessary Services & Hardening

- Disable unnecessary services on R7 :
  - PAD
  - DHCP
  - BOOTP
  - HTTP
  - DNS Client
- R7 should not send any IPv6 Router Advertisments
- This should account for messages sent in response to Router Solicitations
- No more than five ICMPv6 error messages should be sent by R7 per two seconds

R7

```
int f0/1
 ipv6 nd ra suppress all

ipv6 icmp error-interval 2000 5

no service pad
no service dhcp
no ip bootp server
no ip domain lookup
no ip http server
```

Although there are many other services on the router that may need to be disabled most are disabled by default now. The above services are all enabled by default, thus as a part of the unnecessary services these must be disabled for this question.

IPv6 Considerations

Disabling HTTP server via `no ip http server` does the trick for both versions of IP.

The `ipv6 nd ra suppress` command only suppresses periodic unsolicited RAs. It does not suppress RAs sent in response to a router solicitation. To suppress all RAs, including those sent in response to a router solicitation, use the `ipv6 nd ra suppress` command with the `all` keyword.

The `ipv6 icmp error-interval` command is used to limit the rate at which IPv6 ICMP error messages are sent (e.g. Destination Unreachables or Time Exceeded). This particular policing function is implemented by using a token bucket algorithm with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached; spillage is wasted. A single token is refilled every *`milliseconds; bucket size`* defines how many tokens can be accumulated. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the bucket size

is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Verification

```
R7#sh ip http ser status
HTTP server status: Disabled
HTTP server port: 80
HTTP server active supplementary listener ports:
HTTP server authentication method: enable
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server base path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 1
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL


R7# do sh ipv int f0/1
FastEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::21B:D5FF:FE17:BA89
  No Virtual link-local address(es):
  Global unicast address(es):
    2010:1:71::7, subnet is 2010:1:71::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::1:FF00:7
    FF02::1:FF17:BA89
  MTU is 1500 bytes
  ICMP error messages limited to one every 2000 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (all)
```

```
  Hosts use stateless autoconfig for addresses.
```

Test ICMPv6 Error rate-limiting. Note that 5 messages are sent almost immediately but for every other message 2 seconds must elapse for the bucket to refill with a single token:

```
R10(config)#ipv route 1::1/128 2010:1:71::7

R10#ping 1::1 rep 20 timeout 1
Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 1::1, timeout is 1 seconds:
UUUUU..U..U..U..U..U
Success rate is 0 percent (0/20)

R7#
*Mar 12 22:07:21.187: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10
*Mar 12 22:07:21.187: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10
*Mar 12 22:07:21.191: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10
*Mar 12 22:07:21.191: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10
*Mar 12 22:07:21.191: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10
*Mar 12 22:07:23.191: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10
*Mar 12 22:07:25.191: ICMPv6: Sent Unreachable code 0, Src=2010:1:71::7,
Dst=2010:1:71::10

R7#sh ipv traffic
IPv6 statistics:
        Rcvd:  34 total, 14 local destination
               0 source-routed, 0 truncated
               0 format errors, 0 hop count exceeded
               0 bad header, 0 unknown option, 0 bad source
               0 unknown protocol, 0 not a router
               0 fragments, 0 total reassembled
               0 reassembly timeouts, 0 reassembly failures
        Sent:  24 generated, 0 forwarded
               0 fragmented into 0 fragments, 0 failed
               0 encapsulation failed, 10 no route, 0 too big
               0 RPF drops, 0 RPF suppressed drops
        Mcast: 10 received, 5 sent

ICMP statistics:
        Rcvd: 4 input, 0 checksum errors, 0 too short
              0 unknown info type, 0 unknown error type
              unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
              parameter: 0 error, 0 header, 0 option
```

```
               0 hopcount expired, 0 reassembly timeout,0 too big
               0 echo request, 0 echo reply
               0 group query, 0 group report, 0 group reduce
               0 router solicit, 0 router advert, 0 redirects
               2 neighbor solicit, 2 neighbor advert
          Sent: 14 output, 10 rate-limited
               unreach: 10 routing, 0 admin, 0 neighbor, 0 address, 0 port
               parameter: 0 error, 0 header, 0 option
               0 hopcount expired, 0 reassembly timeout,0 too big
               0 echo request, 0 echo reply
               0 group query, 0 group report, 0 group reduce
               0 router solicit, 0 router advert, 0 redirects
               2 neighbor solicit, 2 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Task 14: IP Accounting

- You would like to gather traffic statistics for the traffic received by R6 on both interfaces
- This accounting should be based on IP precedence
- The maximum number of accounting entries to be created should be 500
- Maximum number of transit entries should be 50
- Don’t account for 7.7.7.7 in the transit table

R6

```
interface FastEthernet0/1
 ip accounting output-packets
 ip accounting precedence input

interface Serial0/1/0
 ip accounting output-packets
 ip accounting precedence input

ip accounting-threshold 500
ip accounting-transits 50

ip accounting-list 7.7.7.7 0.0.0.0
```

IP Accounting records the total bytes of packets switched through the device on a source and destination basis. Only traffic that goes through the router is recorded. Traffic destined to and from the router are not measured by the statistics. To turn on accounting you must first enter the command `ip`

`accounting output-packets`. You can then enter the second command used in this lab of `precedence input` to record traffic based on precedence inbound.

Setting the threshold will limit the number entries in the accounting table. The accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates, preventing IP Accounting from possibly consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. Overflows will be recorded; see the monitoring commands for display formats. The default accounting threshold of 512 entries results in a maximum table size of 12,928 bytes. Active and check pointed tables can reach this size independently.

The precedence accounting feature provides accounting information for IP traffic, summarized by IP precedence values. This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on IP precedence. This feature is supported on all interfaces and subinterfaces and supports CEF, dCEF, flow, and optimum switching.

Transit entries are those that do not match any of the filters specified in the `ip accounting-list` global configuration commands.

IPv6 Considerations

This feature is not supported for IPv6. Use Flexible NetFlow with permanent cache instead.

Verification

Generate some traffic through R6 and verify:

```
R6#sh ip accounting
   Source            Destination               Packets               Bytes
 4.4.4.4           150.50.116.11                     5                 500
 150.50.116.11     4.4.4.4                           7                 588

R6#sh int f0/1 precedence
FastEthernet0/1
  Input
    Precedence 0:  10 packets, 1839 bytes
    Precedence 6:  9 packets, 910 bytes
```

Task 15: Core Dumps

- Configure R5 to send a Core Dump to a RCP Server located at 10.1.5.100
- Rename the files to “R5-crashinfo”, and set the dump size to 32768
- Use the username “ipexpert”

R5

```
ip rcmd remote-username ipexpert
```

```
exception core-file R5-crashinfo
exception protocol rcp
exception region-size 32768
exception dump 10.1.5.100
```

Troubleshooting and Fault Management is a core component of network management. In the event of problems with a router it is important to understand how to find the source of software forced crashes. Configuring the router to send Core Dumps is an important element in gathering data for fault management.

Above we have configured R5 to send core dumps to 10.1.5.100 using RCP as the transfer protocol. We want the files to begin with the name "R5-crashinfo", to easily distinguish crash dumps from this device and others. The region-size sets the size of the region for the exception-time memory pool.

More information on this feature can be found under IOS "Network Management Configuration Guide Library" -> "Basic System Management Configuration Guide" -> "Troubleshooting and Fault Management".

IPv6 Considerations

This feature is not supported for IPv6.

Verification

```
R5#show exception
10.1.5.100
```

Task 16: Memory Checks

- R5's current IOS has a memory block overflow problem in the packet memory
- Configure R5 to recover from this error unless it happens twice in less than 10 seconds
- The maximum number of error connections before a reboot should be set to 200
- Also, enable the chunk validation to see if it can give further information as to what is causing the io memory corruption
- After setting up this protection on R5 you have noticed you are filling up the flash too quickly. Configure a maximum number of 20 crash dump files before old files are overwritten

R5

```
exception memory ignore overflow io frequency 10 maxcount 200

scheduler heapcheck process memory io

exception crashinfo maximum files 20
```

IO is the packet memory.

Buffer Overflow is one of many exploits used on the internet to crash devices. With this new Detection and Correction of Redzone Corruption feature a router can recover and correct memory block overflows while continuing to operate.

The Heapcheck feature enables the router to check the memory chunk structure and determine the process or processes that are corrupting the memory chunks. Be leery of doing this in the real world unless directed by TAC to do so as it increases CPU utilization dramatically.

Configuring the maximum crashinfo files to 20, allows the router to delete old crashinfo files once this number has been reached.

IPv6 Considerations

Not relevant.

Verification

```
R5#show memory overflow

Count   Buffer Count   Lastcorrected      Crashinfo files

R5#show chunk
Chunk Manager:
 1671 chunks created, 53 chunks destroyed
 932 siblings created, 47 siblings trimmed
Chunk element  Block Maximum  Element Element Total

                                  --- Omitted ---
```

Task 17: CPU, Memory Protection & NVGEN Enhancement

- With the memory problem you are having on R6 you have also noticed it is running low on memory over time and requires a reboot. Configure R6 to send a Syslog message to 150.50.116.200 when the packet memory available falls below 2 MB free
- In addition if this occurs make sure there is still 2 MB reserved for critical management processes
- If all else fails make sure there is still 4MB free memory, to console into R6 so you can gather debug/crashinfo to further troubleshoot the problem
- Enable the feature that reduces the amount of time required for running configuration management
- Once enabled, interface configuration should be cached in the system memory

R6

```
memory free low-watermark io 2048

memory reserve critical 2048
```

```
memory reserve console 4096

logging host 150.50.116.200

parser config cache interface
```

Memory threshold notifications allows an administrator to reserve memory for critical system notifications and to configure the router to send notification about the memory issues that are occurring on a network device.

Having dealt with many problems on the network when a router is running at 100% CPU utilization and trying to login to the router even through console results in a 30 minute process trying to gather information. I am glad these features are available to prevent a device from becoming completely unresponsive. Now memory can be reserved for things like console access so you can be successful in gathering troubleshooting information.

In the Cisco IOS software configuration model, the configuration state is maintained in a distributed manner, with each component storing its own configuration state. To retrieve configuration information, the software must poll every component to collect the distributed information. This configuration state retrieval operation is performed by a process known as nonvolatile generation (NVGEN), and it is used by command line interpreter (CLI) commands such as `show running-configuration`, `write memory`, and `copy system:running-configuration` to display or copy the running system configuration. When invoked, NVGEN queries each system component and each instance of interface or other configuration objects. A running configuration file is constructed as NVGEN traverses the system performing these queries.
The `parser config cache interface` command is especially useful for managing large system configurations that contain numerous interface configurations. Once enabled, the command provides faster execution of the NVGEN commands that process the running system configuration by caching interface configurations in system memory, and by retrieving only configuration information that has changed. The first time you display the configuration file, you will not see much evidence of improvement in performance because the interface cache will be filled up. However, you will notice performance improvements when you enter subsequent NVGEN-type commands.

IPv6 Considerations

Not relevant.

Verification

```
R6#show memory console reserved
Memory reserved for console is 4456448 bytes

R6#sh run | in memory
memory-size iomem 15
memory reserve critical 2048
memory reserve console 4096
```

```
memory free low-watermark IO 2048
```

Task 18: Managing Configuration Files

- Configure R7 to automatically archive its running configuration twice per day
- Save this file to the local flash as R7-archived-config. Save no more than 5 of these files
- Configure R7 to store a secure copy of the boot-config
- On R11 you have been running into issues with multiple administrators making changes at the same time
- Configure R11 to prevent from happening by locking the configuration automatically
- Configure R11 to archive any config changes made
- Keep it below 75 lines and do not log passwords
- Send a message to the logging server whenever a configuration change occurs

R7

```
archive
 path flash:/R7-archived-config
 maximum 5
 time-period 720

secure boot-config
```

R11

```
configuration mode exclusive

archive
 log config
  logging enable
  logging size 75
  notify syslog contenttype plaintext
  hidekeys

logging host 150.50.116.200
```

Starting with 12.3T you can now save config backups and you can also use these configuration archives to rollback your configuration to an earlier state in the event a configuration change causes issues on a router. Very handy for change management.

On R11 you will notice some differences from R7. On this device we are actually logging the configuration changes done on the router (and not backing up the config). So we are generating a Syslog message and send it to 150.50.116.200. We limit the size to 75 lines and in the solution we have specified the `hidekeys` command to exclude passwords (although this is done by default) – any passwords typed will be “starred out” in the logs.

The exclusive configuration lock allows single-user access to configuration modes using single-user configuration mode. While the device configuration is locked, no other users can enter configuration commands.

IOS Resilient Configuration feature is intended to speed up the recovery process in the event such as when system was compromised or configuration was erased. What this feature does is that when enabled it maintains a secure working copy of the router image (`secure boot-image`) and the startup configuration (`secure boot-config`) at all times. And more importantly these secured images or the remote user cannot remove files, you will be only able to disable Resilient Configuration from the console port.

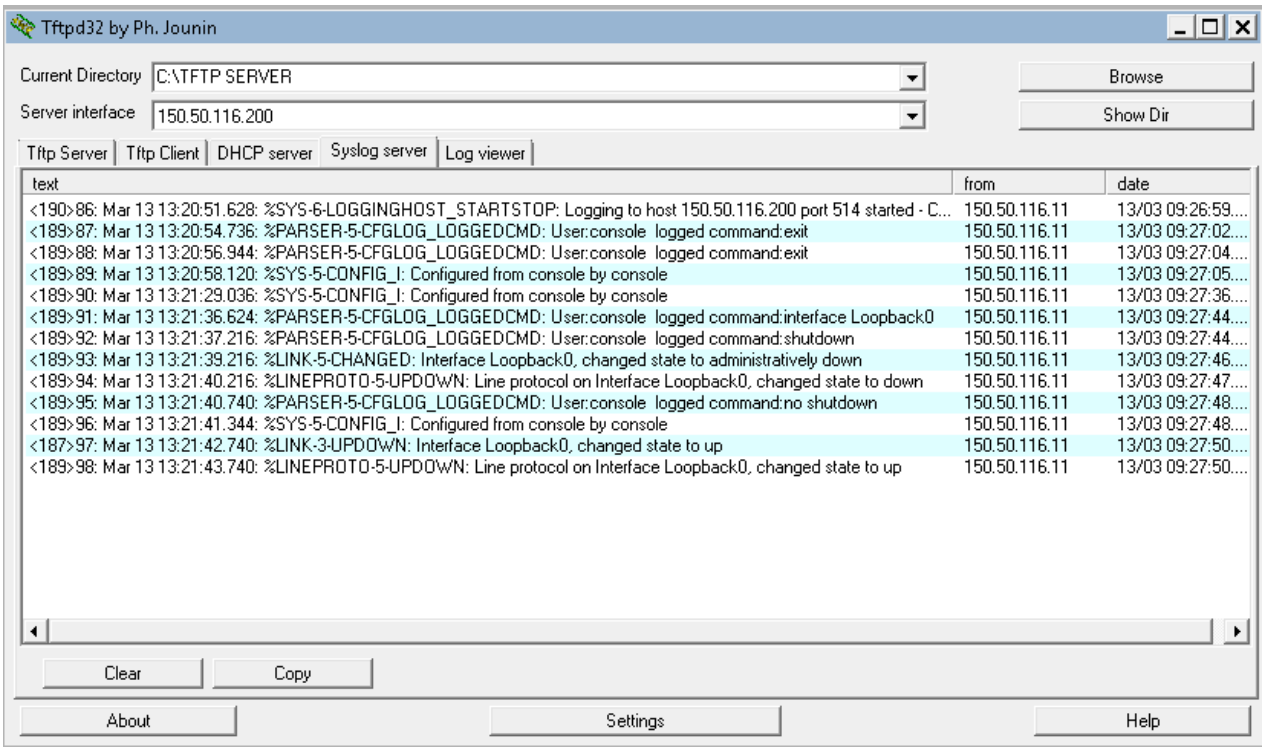
IPv6 Considerations

Not relevant.

Verification

```
R7(config-archive)#do sh archive
The maximum archive configurations allowed is 5.
There are currently 1 archive configurations saved.
The next archive file will be named flash:/R7-archived-config-<timestamp>-1
 Archive #  Name
   1        flash:/R7-archived-config-Mar-13-13-23-07.363-0 <- Most Recent
   2
   3
   4
   5
R7#sh secure bootset
IOS resilience router id FTX1123F06E

IOS image resilience is not active

IOS configuration resilience version 12.4 activated at 13:25:04 UTC Wed Mar 13 2013
Secure archive flash:.runcfg-20130313-132503.ar type is config
configuration archive size 2601 bytes
configuration archive ready for upgrade
R11#conf t
Configuration session is locked. The lock will be cleared once you exit out of
configuration mode.
Enter configuration commands, one per line.  End with CNTL/Z.


R11#sh archive log config all
 idx    sess           user@line      Logged command
    1       1        console@console   |  logging enable
    2       1        console@console   |  exit
    3       1        console@console   |   exit
    4       3        console@console   |interface Loopback0
    5       3        console@console   | shutdown
    6       3        console@console   | no shutdown
```

Now a quick look at the logs on the Test PC:



At the end I want to mention that if you were to set a smaller number of entries for the config logs it would still show you the total number of configuration changes that were made since enabling the feature. From the example output below you can conclude that the log size was set to 10, meaning only 10 issued commands will be shown, but based on the Index # we can say there were 16 configuration changes done total :

```
R11#sh arch log config all
 idx    sess           user@line      Logged command
    7       2        console@console   | no shutdown
    8       2        console@console   | exit
    9       2        console@console   |interface GigabitEthernet0/0
   10       2        console@console   | shutdown
   11       2        console@console   | no shutdown
   12       3        console@console   |interface GigabitEthernet0/1
   13       3        console@console   | shutdown
   14       3        console@console   | no shutdown
   15       4        console@console   |interface l1
   16       4        console@console   | no interface Loopback1
```

Section 10 Network Attack Mitigation

Section 10 : Network Attack Mitigation & Prevention is intended to let you be familiar with common network attacks and methods/tools that can be used to prevent them. You will be configuring features related to attack detection, QoS techniques, L2 security, IPv6 security & attack-specific scenarios.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on Network Attack Mitigation technologies. You will need to pre-configure the network with the base configuration files

NOTE: Static/default routes are NOT allowed unless otherwise stated in a task.

NOTE: You can allow ICMP for testing throughout the network

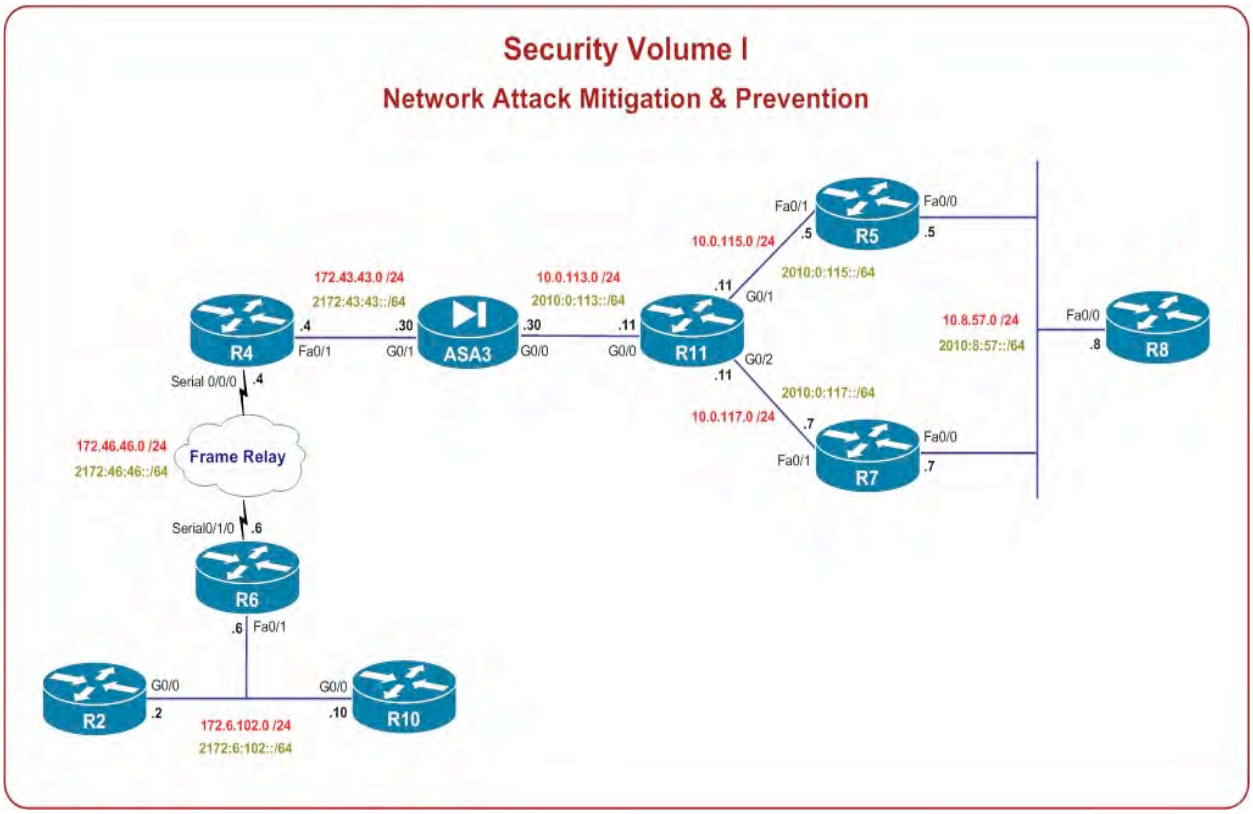
Estimated Time to Complete: **6 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R2	G0/0	102	172.6.102.2/24 2172:6:102::2/64
	Loop0		2.2.2.2/24 2::2/64
R4	F0/1	43	172.43.43.4/24 2172:43:43::4/64
	S0/0/0		172.46.46.0/24 2172:46:46::4/64
	Loop0		4.4.4.4/24 4::4/64
R5	F0/0	857	10.8.57.5/24 2010:8:57::5/64
	F0/1	115	10.0.115.5/24 2010:0:115::5/64
	Loop0		5.5.5.5/24 5::5/64
R6	F0/1	102	172.6.102.6/24 2172:6:102::6/64
	S0/1/0		172.46.46.6/24 2172:46:46::6/64
	Loop0		6.6.6.6/24 6::6/64
R7	F0/0	857	10.8.57.7/24 2010:8:57::7/64
	F0/1	117	10.0.117.7/24 2010:0:117::7/64
	Loop0		7.7.7.7/24 7::7/64
R8 R8	F0/0 F0/0	857	10.8.57.8/24 2010:8:57::8/64
	Loop0		8.8.8.8/24 8::8/64
R10	G0/0	102	172.6.102.10/24

			2172:6:102::10/64
	Loop0		100.100.100.10/24
			10::10/64
R11	G0/0	113	10.0.113.11/24
			2010:0:113::11/64
	G0/1	115	10.0.115.11/24
			2010:0:115::11/64
	G0/2	117	10.0.117.11/24
			2010:0:117::11/64
	Loop0		11.11.11.11/24
			11::11/64
ASA3	G0/0	113	10.0.113.30/24
			2010:0:113::30/24
	G0/1	43	172.43.43.30/24
			2172:43:43::30/64



Solutions

Task 1: Traffic Marking & Classification

- Configure R6 so that all IPv4 Telnet packets are marked with IP Precedence 4
- HTTP packets (IPv4) should be colored with DSCP 31
- ICMPv6 traffic should be marked with IP Precedence 4
- All other IPv6 packets should be transported over FR cloud with the DE bit set
- On R4 all IPv4 packets with IP Precedence 4 received on DLCI 406 should be re-marked as IP Precedence 0
- IPv6 traffic with IP Precedence 4 should be marked with DSCP value 11
- Don’t use an ACL to accomplish this
- IPv4 packets received with DSCP 31 should be now colored with DSCP cs4
- All traffic received with FR DE bit set should be marked as IP Precedence 7

Detailed Solution

R6

```
ip access-list extended HTTP
 permit tcp any any eq www
ip access-list extended TELNET
 permit tcp any any eq telnet
ipv6 access-list ICMPv6
 permit icmp any any
ipv6 access-list ALL_IPv6
 permit ipv6 any any

class-map match-all HTTP_CLASS
 match access-group name HTTP
class-map match-all TELNET_CLASS
 match access-group name TELNET
class-map match-all ICMPv6_CLASS
 match access-group name ICMPv6
class-map match-all ALL_IPv6_CLASS
 match access-group name ALL_IPv6

policy-map MARK_OUT_POL
 class TELNET_CLASS
  set ip precedence 4
 class HTTP_CLASS
  set ip dscp 31
 class ICMPv6_CLASS
  set precedence 4
 class ALL_IPv6_CLASS
  set fr-de
```

```
int s0/1/0
 service-policy output MARK_OUT_POL
```

R4

```
class-map match-all IPP4_IPv4_DLCI406_CLASS
 match fr-dlci 406
 match ip precedence 4
class-map match-all DE_CLASS
 match fr-de
class-map match-all DSCP31_CLASS
 match ip dscp 31
class-map match-all IPP4_IPv6_CLASS
 match  precedence 4
 match protocol ipv6

policy-map MARK_IN_POL
 class IPP4_IPv6_CLASS
  set dscp 11
 class IPP4_IPv4_DLCI406_CLASS
  set ip precedence 0
 class DSCP31_CLASS
  set ip dscp cs4
 class DE_CLASS
  set precedence 7

int s0/1/0
 service-policy input MARK_IN_POL
```

Traffic classification and marking techniques can be used in many Network Attack scenarios. Make sure you are familiar with the MQC fundamentals, syntax and configuration options.

IPv6 Considerations

The "`match/set dscp/precedence`" command is generally used to classify/mark IPv4 AND IPv6 packets. This is as opposed to "`match/set ip dscp/precedence`" that should be only used when working with IPv4 packets.

To match IPv6 packets only using IP Precedence or DSCP you need to combine "`match dscp/precedence`" with "`match protocol ipv6`" – don't forget that a class-map must be then using boolean "AND" operator.

Verification

Note since Telnet to 4.4.4.4 is IPv4, first class in R4's policy does not match anything even that packets are sent as IPP 4:

```
R2#telnet 4.4.4.4
Trying 4.4.4.4 ... Open


Password required, but none set

[Connection to 4.4.4.4 closed by foreign host]

R4#sh policy-map int s0/0/0

 Serial0/0/0

  Service-policy input: MARK_IN_POL

    Class-map: IPP4_IPv6_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 4
      Match: protocol ipv6
      QoS Set
        dscp 11
          Packets marked 0

    Class-map: IPP4_IPv4_DLCI406_CLASS (match-all)
      11 packets, 517 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 4
      Match: fr-dlci 406
      QoS Set
        precedence 0
          Packets marked 11
                                    --- Omitted ---


R2#ping 4::4 rep 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4::4, timeout is 2 seconds:
!!!!!!!!!!

R4#sh policy-map int s0/0/0

 Serial0/0/0

  Service-policy input: MARK_IN_POL
```

```
    Class-map: IPP4_IPv6_CLASS (match-all)
      10 packets, 1040 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 4
      Match: protocol ipv6
      QoS Set
        dscp 11
          Packets marked 10

    Class-map: IPP4_IPv4_DLCI406_CLASS (match-all)
      11 packets, 517 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 4
      Match: fr-dlci 406
      QoS Set
        precedence 0
          Packets marked 11
                                    --- Omitted ---
```

Compare to what R6 colored before sending traffic out the FR cloud:

```
R6#sh policy-map int s0/1/0

 Serial0/1/0

  Service-policy output: MARK_OUT_POL

    Class-map: TELNET_CLASS (match-all)
      11 packets, 517 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name TELNET
      QoS Set
        precedence 4
          Packets marked 11

    Class-map: HTTP_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name HTTP
      QoS Set
        dscp 31
          Packets marked 0

    Class-map: ICMPv6_CLASS (match-all)
      10 packets, 1040 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name ICMPv6
      QoS Set
        precedence 4
```

```
          Packets marked 10


R4(config)#ip http server

R2#telnet 4::4 80
Trying 4::4, 80 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Thu, 14 Mar 2013 22:51:58 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 4::4 closed by foreign host]


R4#sh policy-map interface s0/0/0

 Serial0/0/0

  Service-policy input: MARK_IN_POL

    Class-map: IPP4_IPv6_CLASS (match-all)
      10 packets, 1040 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 4
      Match: protocol ipv6
      QoS Set
        dscp 11
          Packets marked 10

    Class-map: IPP4_IPv4_DLCI406_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: fr-dlci 406
      Match: ip precedence 4
      QoS Set
        precedence 0
          Packets marked 0

    Class-map: DSCP31_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp 31
      QoS Set
        dscp cs4
```

```
          Packets marked 0

    Class-map: DE_CLASS (match-all)
      191 packets, 15986 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        precedence 7
          Packets marked 191

    Class-map: class-default (match-any)
      167 packets, 14108 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any


R2#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Thu, 14 Mar 2013 22:53:30 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

R6#sh policy-map int s0/1/0

 Serial0/1/0

  Service-policy output: MARK_OUT_POL

    Class-map: TELNET_CLASS (match-all)
      49 packets, 2291 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name TELNET
      QoS Set
        precedence 4
          Packets marked 49

    Class-map: HTTP_CLASS (match-all)
      11 packets, 495 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name HTTP
      QoS Set
        dscp 31
          Packets marked 11
                                  --- Omitted ---
```

```
R4#sh policy-map interface s0/0/0

 Serial0/0/0

  Service-policy input: MARK_IN_POL

    Class-map: IPP4_IPv6_CLASS (match-all)
      10 packets, 1040 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 4
      Match: protocol ipv6
      QoS Set
        dscp 11
          Packets marked 10

    Class-map: IPP4_IPv4_DLCI406_CLASS (match-all)
      17 packets, 786 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: fr-dlci 406
      Match: ip precedence 4
      QoS Set
        precedence 0
          Packets marked 17

    Class-map: DSCP31_CLASS (match-all)
      11 packets, 495 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp 31
      QoS Set
        dscp cs4
          Packets marked 11

    Class-map: DE_CLASS (match-all)
      202 packets, 16910 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        precedence 7
          Packets marked 202

    Class-map: class-default (match-any)
      179 packets, 15116 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 2: NBAR & NBAR Next Generation

- Using NBAR create and apply a policy outbound on R11's G0/0 interface to drop the Slammer worm
- The Slammer worm uses UDP port 1434; its packets are exactly 404B in length
- Also all HTTP packets with string "attack" in the URL should be dropped but only when sent to/coming from 4.4.4.4
- The "attack" string should not be case-sensitive
- Using the same policy-map drop all terminal-related traffic except PCANYWHERE
- Also implement a policy for Peer-to-Peer traffic :
  - All clear-text packets should be rate-limited to 200kbps
  - All encrypted traffic should be dropped
- Enable classification of IPv6 traffic that is carried over Teredo tunnels

R11

```
ip nbar custom SLAM1434 udp 1434

class-map match-all SLAMMER
 match protocol SLAM1434
 match packet length min 404 max 404

class-map match-all BAD_HTTP
 match protocol http url "*[Aa][Tt][Tt][Aa][Cc][Kk]*"
 match protocol http host "4.4.4.4"

class-map match-all PCANYWHERE
 match proto attribute sub-category terminal pcanywhere

class-map match-all TERMINAL_APPS
 match protocol attribute sub-category terminal

class-map match-all ENC_P2P
 match protocol attribute p2p-technology p2p-tech-yes
 match protocol attribute encrypted encrypted-yes

class-map match-all CLEAR_P2P
 match protocol attribute p2p-technology p2p-tech-yes
 match protocol attribute encrypted encrypted-no
policy-map MITIGATE_POL
 class SLAMMER
  drop
 class BAD_HTTP
  drop
 class PCANYWHERE
 class TERMINAL_APPS
  drop
 class CLEAR_P2P
```

```
  police 200000
 class ENC_P2P
  drop

ip nbar classification tunneled-traffic teredo

int G0/0
 service-policy output MITIGATE_POL
```

NBAR or Network-Based Application Recognition is a feature that takes packet classification to another level. It allows us to look deeper into the packet, up to the application layer, and classify based on the content within the payload. For example, HTTP traffic can be classified based on URL, host part or even MIME type.

As you can imagine, this technique can be useful when dealing with some type of worms, like for example Code Red or NIMDA. The propagation mechanism in these was copying, downloading, or executing a particular file via HTTP GET requests.

Next Generation NBAR (NBAR2) is basically the re-architectured old-style Network Based Application Recognition with improved classification engine, increased accuracy and way more signatures available.

The main advantage of NBAR2 is advanced classification including the ability to match protocols running on top of IPv6. Packets are identified using a new SCE engine, which allows classification of not only IPv4 and IPv6 packets but also the transition techniques. So things like ISATAP, Teredo, this traffic can be now matched using this feature.

NBAR version 2 groups applications based on various attributes (`match protocol attribute`). And an attribute can be one of the following:

1. “Application-group” - a grouping of applications that are part of the same suite or brand. An example me be the “`Yahoo-Messenger-group`” keyword that actually matches Yahoo Messenger, Yahoo VoIP and VoIP over SIP traffic
2. “Category” - a group of applications which support similar functionality from an end-user standpoint. For example `email', `gaming' or ‘`file-sharing`’
3. “Sub-category” - similar to category, but the classification of applications was done more from the networking standpoint. Examples : '`routing-protocol`', `network-management' or `terminal'
4. “Peer-to-Peer” - to match applications based on whether they were classified as P2P, not Peer-to-Peer and unassigned
5. “Tunnel” is to match traffic that was classified as tunneled, not tunneled or unassigned
6. “Encrypted” is to configure matching criteria based on encryption (yes, no, unassigned)

To figure out what protocols were classified as characterized by a particular attribute use the "`show ip nbar attribute`" command. To see all attributes of a particular protocol use "`show ip nbar protocol-attribute`".

Also don't forget that for both of these technologies to work CEF must be turned on (`ip cef, ipv6 cef`).

IPv6 Considerations

NBAR2 supports classification of protocols running over IPv6.

Verification

```
R11#sh ip nbar port-map SLAM1434
port-map SLAM1434                  udp 1434

R7(config)#ip http client source-interface l0

R7#copy http://4.4.4.4/AttaCk.pdf null0
Destination filename [null0]?
Accessing http://4.4.4.4/AttaCk.pdf...

R11#sh policy-map int class BAD_HTTP
 GigabitEthernet0/0

  Service-policy output: MITIGATE_POL

    Class-map: BAD_HTTP (match-all)
      16 packets, 2007 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol http url "*[Aa][Tt][Tt][Aa][Cc][Kk]*"
      Match: protocol http host "4.4.4.4"
      Drop
```

Traffic destined to server other than 4.4.4.4 is not affected:

```
R2(config)#ip http server

R7#copy http://2.2.2.2/AttaCk.pdf null0
Destination filename [null0]?
Accessing http://2.2.2.2/AttaCk.pdf...
%Error opening http://2.2.2.2/AttaCk.pdf (No such file or directory)

R11#sh policy-map int class BAD_HTTP
 GigabitEthernet0/0
```

```
  Service-policy output: MITIGATE_POL

    Class-map: BAD_HTTP (match-all)
      16 packets, 2007 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol http url "*[Aa][Tt][Tt][Aa][Cc][Kk]*"
      Match: protocol http host "4.4.4.4"
      drop
```

OK, now let's test TELNET which is part of the terminal applications. Note that even you are able to login you will not be able to issue anything – right after you receive R4's prompt all further packets are blocked by NBAR:

```
R4(config)#line vty 0 4
R4(config-line)#no login

R7(config)#ip telnet source-interface loop0

R7#telnet 4.4.4.4
Trying 4.4.4.4 ... Open

R4>

R7#telnet 4::4
Trying 4::4 ... Open

R4>

R11#sh policy-map int class TERMINAL_APPS
 GigabitEthernet0/0

  Service-policy output: MITIGATE_POL

    Class-map: TERMINAL_APPS (match-all)
      24 packets, 1362 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol attribute sub-category terminal
      Drop
```

For PCANYWHERE, even that it is part of the "terminal" sub-category, since the corresponding class is higher in the policy the PCANYWHERE packets would not be matched by the TERMINAL_APPS class (look at the entire policy below):

```
R11#sh ip nbar protocol-attribute pcanywhere
           Protocol Name :  pcanywhere
                category :  net-admin
            sub-category :  terminal
```

```
       application-group :  other
          p2p-technology :  p2p-tech-no
                  tunnel :  tunnel-no
               encrypted :  encrypted-no
```

And the entire policy. The counters may not match exactly what's shown above due to additional segments being sent (retransmissions). This is because of how NBAR works - it classifies only bidirectional traffic flows. Initial packets always make their way to the destination server; only when the response is seen packets start to be dropped:

```
R11#sh policy-map int g0/0
 GigabitEthernet0/0

  Service-policy output: MITIGATE_POL

    Class-map: SLAMMER (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol SLAM1434
      Match: packet length min 404 max 404
      drop

    Class-map: BAD_HTTP (match-all)
      17 packets, 2061 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol http url "*[Aa][Tt][Tt][Aa][Cc][Kk]*"
      Match: protocol http host "4.4.4.4"
      drop

    Class-map: PCANYWHERE (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: protocol pcanywhere

    Class-map: TERMINAL_APPS (match-all)
      24 packets, 1362 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol attribute sub-category terminal
      drop

    Class-map: CLEAR_P2P (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol attribute p2p-technology p2p-tech-yes
      Match: protocol attribute encrypted encrypted-no
      police:
          cir 200000 bps, bc 6250 bytes
        conformed 0 packets, 0 bytes; actions:
```

```
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: ENC_P2P (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol attribute p2p-technology p2p-tech-yes
      Match: protocol attribute encrypted encrypted-yes
      drop

    Class-map: class-default (match-any)
      189 packets, 17406 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Task 3: Policy Based Routing

- Use Policy-Based Routing on R6 to drop MSBlaster worm traffic
- Offending packets are coming from VLAN 102 using IPv6 and TCP port 135 for transport
- Also make sure IPv6 Telnet connections to port 135 cannot be initiated from R6

R6

```
ipv6 access-list TCP_135
 permit tcp any any eq 135

route-map PBR6 permit 10
 match ipv6 address TCP_135
 set interface Null0

int f0/1
 ipv6 policy route-map PBR6

ipv6 local policy route-map PBR6
```

This task is just to show minor differences in syntax (IPv4 vs IPv6) in implementing PBR/Local PBR on the routers.

One more Route-Map matching option useful in certain attack scenarios would be to specify the packet length (`match length` *`min max`*).

IPv6 Considerations

To match IPv6 traffic use "`match ipv6`" in a route-map. To apply Local PBR use "`ipv6 local policy`".

Verification

Before the feature was implemented an RST packet was sent by R4:

```
R10#telnet 4::4 135
Trying 4::4, 135 ...
% Connection refused by remote host

R6#telnet 4::4 135
Trying 4::4, 135 ...
% Connection refused by remote host
```

With PBR packets are simply black-holed on R6 :

```
R10#telnet 4::4 135
Trying 4::4, 135 ...
% Connection timed out; remote host not responding

R6#telnet 4::4 135
Trying 4::4, 135 ...
% Connection timed out; remote host not responding

R6#sh route-map
route-map PBR6, permit, sequence 10
  Match clauses:
     ipv6 address TCP_135
  Set clauses:
    interface Null0
  Policy routing matches: 6 packets, 384 bytes

R6#sh ipv policy
Interface                 Routemap
Local                     PBR6
FastEthernet0/1           PBR6
```

Task 4: CAR

- Rate-limit inbound ICMP traffic on R6's Serial interface to 16kbps. Use the minimum burst values available
- Conforming traffic should be transmitted and exceeding traffic should be dropped
- Other IPv4 traffic should be rate-limited to 64kbps. Use 64kbps for both of the burst values
- Conforming traffic should have the DSCP set to AF21 and exceeding traffic should be transmitted unchanged

R6

```
access-list 110 permit icmp any any

access-list 115 deny   icmp any any
access-list 115 permit ip any any

int s0/1/0
 rate-limit input access-group 110 16000 1500 2000 conform-action
  transmit exceed-action drop
 rate-limit input access-group 115 64000 8000 8000 conform-action set-
  dscp-continue 18 exceed-action transmit

ipv6 local policy route-map PBR6
```

Rate limiting of traffic with CAR is used to police the flow of traffic into an interface. To implement this we have defined rate-limit access-lists and used those ACLs as the input for our CAR policy. In case burst values are not explicitly mentioned you may use Cisco's recommended values (you can find them in the documentation for the `rate-limit` command):

1. Normal Burst = configured rate * (1 byte)/(8 bits) * 1.5 seconds
2. Extended Burst = 2 * normal burst

So for example if traffic rate is 64000 bps you would use Normal Burst of 12kB and Extended Burst of 24kB.

To input a DSCP of AF21 we can use the quick conversion logic of multiplying the first number by 8 and the second by 2 and then adding them (i.e 2*8 + 1*2 = 18).

Finally note the `rate-limit` command takes rate in bits per second but burst values in bytes. Always double check the unit by using the "?".

IPv6 Considerations

CAR, as of current code release, is not supported for IPv6 traffic.

Verification

```
R4#ping 2.2.2.2 rep 50 size 200

Type escape sequence to abort.
Sending 50, 200-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!.!!!!!!!!!!!!!!.!!!
Success rate is 94 percent (47/50), round-trip min/avg/max = 32/33/64 ms

R6#sh access-l 110
Extended IP access list 110
    10 permit icmp any any (50 matches)
```

```
R6#sh interfaces s0/1/0 rate-limit
Serial0/1/0
  Input
    matches: access-group 110
      params:  16000 bps, 1500 limit, 2000 extended limit
      conformed 47 packets, 9588 bytes; action: transmit
      exceeded 3 packets, 612 bytes; action: drop
      last packet: 138408ms ago, current burst: 280 bytes
      last cleared 00:05:36 ago, conformed 228 bps, exceeded 14 bps
    matches: access-group 115
      params:  512000 bps, 8000 limit, 8000 extended limit
      conformed 26 packets, 2152 bytes; action: set-dscp-continue 18
      exceeded 0 packets, 0 bytes; action: transmit
      last packet: 144ms ago, current burst: 0 bytes
      last cleared 00:03:51 ago, conformed 74 bps, exceeded 0 bps
```

Now initiate a file transfer from behind R6. Observe the counters:

```
R4(config)#username cisco priv 15 pass cisco
R4(config)#ip http authentication local
R4(config)#ip http path flash:

R2(config)#ip http client username cisco
R2(config)#ip http client password cisco

R2#copy http://4.4.4.4/c2800nm-adventerprisek9-mz.151-3.T4.bin null0
Destination filename [null0]?
Loading http://4.4.4.4/c2800nm-adventerprisek9-mz.151-3.T4.bin !!!!!!!!!!!!!

R6#sh interfaces s0/1/0 rate-limit
Serial0/1/0
  Input
    matches: access-group 110
      params:  16000 bps, 1500 limit, 2000 extended limit
      conformed 47 packets, 9588 bytes; action: transmit
      exceeded 3 packets, 612 bytes; action: drop
      last packet: 664552ms ago, current burst: 280 bytes
      last cleared 00:14:22 ago, conformed 88 bps, exceeded 5 bps
    matches: access-group 115
      params:  64000 bps, 8000 limit, 8000 extended limit
      conformed 356 packets, 201696 bytes; action: set-dscp-continue 18
      exceeded 240 packets, 137673 bytes; action: transmit
      last packet: 32ms ago, current burst: 7452 bytes
      last cleared 00:00:24 ago, conformed 66467 bps, exceeded 45369 bps
```

Task 5: Flexible NetFlow

- Configure R11 to detect SYN Flooding attack coming from VLAN 113 network
- During this initial phase of monitoring you are only interested in the IPv4 addresses of target devices being under attack (VLANs 115, 117 and 857)
- You want to know the number of packets sent to a particular device and the time attack has started (based on System Uptime)
- The collected information should be never removed from the Cache
- No more than 200 entries should be cached
- R11 should be also monitoring unicast IPv6 traffic received on G0/1 and G0/2 interfaces
- Cache entries should depend on the input interface, destination address and name of the application used
- You want to know the number of bytes seen for the flow and also the first 20 bytes of the payload from the first packet matching the flow
- Cache information should be exported to the Collector Engine with an IP address 2010:8:57::100 over UDP port 90
- Don't analyze every IPv6 packet; only one out of 5 packets should be processed

R11

```
flow record DOS_RECORD
 match ipv4 destination address
 match transport tcp flags syn
 collect counter packets
 collect timestamp sys-uptime first

flow record IPv6_REC
 match ipv6 destination address
 match interface input
 match application name
 collect ipv6 section payload size 20
 collect counter bytes

flow monitor FMON
 cache type permanent
 cache entries 200
 record DOS_RECORD

flow monitor FMON6
 exporter FEX
 record IPv6_REC

flow exporter FEX
 destination 2010:8:57::100
 transport udp 90
```

```
sampler FSAM
 mode deterministic 1 out-of 5

int g0/0
 ip flow monitor FMON input

int g0/1
 ipv6 flow monitor FMON6 sampler FSAM unicast input

int g0/2
 ipv6 flow monitor FMON6 sampler FSAM unicast input
```

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. It provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting.

Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. It facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

Flexible NetFlow (same as the legacy version) uses the concept of flows. And a flow is defined as a stream of packets sharing common characteristics, such as source, destination IP address, port numbers, TCP flags and so on. These characteristics are known as Key fields and they are used as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. When the value of the data in the key field of a datagram is unique with respect to the flows that already exist, a new flow is created. If key field values are the same as in one of the flows that is already cached, the existing entry is updated.

There is also another element used by NetFlow, Nonkey fields, and these are used as the criteria for identifying fields from which data is captured from the flows. Simply put whenever a new packet is received that is processed by NetFlow, a corresponding flow entry (either already existing in the cache or a new one) is populated with data from the packet, which data is captured from the values in the nonkey fields defined for the flow.

The main benefit of using Flexible NetFlow is the ability of defining structure of the flow. With the Original NetFlow we were restricted to well-known fixed seven tuples of IP information that was used to identify the flow (source IP address & port, destination IP address & port, protocol, ingress interface and ToS). With Flexible NetFlow we can specify the Key and Nonkey fields on our own which greatly improves flexibility and enhances this feature as a security-monitoring tool. For instance, new flow keys can be defined for packet length or MAC address, allowing users to search for a specific type of attack in the network (e.g. certain dDoS attacks).

Flexible NetFlow consists of a few components we can define when implementing the feature. First (mandatory) component is known as Flow Monitor.

Flow Monitor is applied directly to the interfaces and this element performs the actual traffic monitoring. Each Flow Monitor is defined by a Record that is a combination of Key and Nonkey fields – which in turn defines the Cache structure. We can either use pre-defined records or create our own by using the `match` (Key fields) and `collect` (Nonkey fields) commands.

Each Flow Monitor has a Cache that it uses to store all the flows it monitors. Each cache has various configurable elements, such as the number of entries and the time that a flow is allowed to remain in it. When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor. One exception here is Cache type "`permanent`" which never allows entries to be removed from the Cache. Here note when a Cache becomes full, new flows will not be monitored. If this occurs, a "Flows not added" statistic will appear in the cache statistics.

One optional component is the Exporter, which is where you define a system you want to send the cached information to for further analysis. So basically an IP address of a device that is running NetFlow Collector. By the way the only format of exporting NetFlow data in Flexible Netflow is version 9.

Finally there is also a Sampler (`sampler`) element that allows you to limit the number of packets selected for analysis. So instead of looking at every single packet going through an interface, you can say that you only want to examine every 10th packet. And this of course saves router's resources but you are losing on the accuracy of monitoring.

IPv6 Considerations

IPv6 support was removed from original NetFlow in Cisco IOS Release 12.4(20)T but Flexible NetFlow fully supports IPv6 flows.

Verification

First round of verifications just to make sure what we configured matches task requirements:

```
R11#sh flow interface g0/0
Interface GigabitEthernet0/0
  FNF:  monitor:           FMON
        direction:         Input
        traffic(ip):       on


R11#show flow record DOS_RECORD
flow record DOS_RECORD:
  Description:        User defined
  No. of users:       1
  Total field space:  13 bytes
  Fields:
    match ipv4 destination address
    match transport tcp flags syn
    collect counter packets
```

```
    collect timestamp sys-uptime first
```

Active and Inactive timeout only matters when the cache type is set to “Normal”:

```
R11#show flow monitor FMON
Flow Monitor FMON:
  Description:       User defined
  Flow Record:       DOS_RECORD
  Cache:
    Type:              permanent
    Status:            allocated
    Size:              200 entries / 8556 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

OK, let’s generate some TCP traffic (e.g. telnet) and take a look at the Cache. In my case at some point I put a blocking ACL so only SYN packets are seen (TCP flags set to 0x2 means SYN bit is set) – here this would be an indication of a SYN Flood attack targeted at R7:

```
R11#show flow monitor FMON cache
  Cache type:                               Permanent
  Cache size:                                     200
  Current entries:                                  5
  High Watermark:                                   5

  Flows added:                                      5
  Updates sent             (  1800 secs)            0

IPV4 DST ADDR    TCP FLAGS    time first         pkts long perm
===============  =========  ============  ====================
224.0.0.5        0x00       22:19:31.128                   111
5.5.5.5          0x02       22:21:45.104                     6
5.5.5.5          0x00       22:21:45.108                    80
7.7.7.7          0x02       22:21:51.928                   171
7.7.7.7          0x00       22:21:51.940                    10
```

Now IPv6 – let’s start with basic config verification:

```
R11#sh flow int g0/1
Interface GigabitEthernet0/1
  FNF:  checking sub traffic.
  FNF:  monitor:           FMON6
        direction:         Input
        traffic(ipv6):     sampler FSAM unicast
```

```
R11#sh flow record IPv6_REC
flow record IPv6_REC:
  Description:        User defined
  No. of users:       1
  Total field space:  48 bytes
  Fields:
    match ipv6 destination address
    match interface input
    match application name
    collect ipv6 section payload size 20
    collect counter bytes

R11#sh flow exporter FEX
Flow Exporter FEX:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 2010:8:57::100
    Source IP address:      2010:0:115::11
    Transport Protocol:     UDP
    Destination Port:       90
    Source Port:            56921
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Not Used
```

Note there was some traffic seen by “FMON6” but only 20% of packets were sampled:

```
R11#sh sampler FSAM
Sampler FSAM:
  ID:             2326270854
  export ID:      1
  Description:    User defined
  Type:           deterministic
  Rate:           1 out of 5
  Samples:        49
  Requests:       246
  Users (2):
    flow monitor FMON6 (ipv6,Gi0/1,Input)  30 out of 151
    flow monitor FMON6 (ipv6,Gi0/2,Input)  19 out of  95

R11#sh flow monitor FMON6
Flow Monitor FMON6:
  Description:       User defined
  Flow Record:       IPv6_REC
  Flow Exporter:     FEX
  Cache:
    Type:              normal
```

```
    Status:            allocated
    Size:              4096 entries / 344088 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

OK let's generate some traffic and take a look at the Cache. This time entries do timeout so you must be pretty fast to see them ☺:

```
R8#ping 2::2 size 1000 rep 10

Type escape sequence to abort.
Sending 10, 1000-byte ICMP Echos to 2::2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 148/151/152 ms
```

Note even we said we only want to "collect" part of the payload, this information is automatically used to differentiate between the flows. This is because there is no way to show two different payloads for a single flow. The difference from setting this as a Key field would be that then this information would not get exported. Also note that Key fields are upper-case; Nonkey fields are lower-case:

```
R11#sh flow monitor FMON6 cache
  Cache type:                                Normal
  Cache size:                                  4096
  Current entries:                                2
  High Watermark:                                 5

  Flows added:                                   38
  Flows aged:                                    36
    - Active timeout      (  1800 secs)           0
    - Inactive timeout    (    15 secs)          36
    - Event aged                                  0
    - Watermark aged                              0
    - Emergency aged                              0

IPV6 DESTINATION ADDRESS:   2::2
INTERFACE INPUT:            Gi0/2
APPLICATION NAME:           prot ipv6-icmp
counter bytes:              1000
ip payload packet section:  0x80003DF9 0x07A10000 0x00010203 0x04050607
                            0x08090A0B

IPV6 DESTINATION ADDRESS:   2::2
INTERFACE INPUT:            Gi0/1
APPLICATION NAME:           prot ipv6-icmp
counter bytes:              1000
ip payload packet section:  0x8000AA5F 0x07A10003 0x03040506 0x0708090A
                            0x0B0C0D0E
```

```
R8#copy http://[4::4]/test.cfg null0
Destination filename [null0]?
Accessing http://[4::4]/test.cfg...
%Error opening http://[4::4]/test.cfg (No such file or directory)

R11#sh flow monitor FMON6 cache
  Cache type:                                Normal
  Cache size:                                  4096
  Current entries:                                2
  High Watermark:                                 5

  Flows added:                                   54
  Flows aged:                                    52
    - Active timeout      (  1800 secs)           0
    - Inactive timeout    (    15 secs)          52
    - Event aged                                  0
    - Watermark aged                              0
    - Emergency aged                              0

IPV6 DESTINATION ADDRESS:   4::4
INTERFACE INPUT:            Gi0/1
APPLICATION NAME:           port http
counter bytes:              184
ip payload packet section:  0x865B0050 0x79506B49 0x9FB75CAA 0x50101020
                            0xC4CE0000

IPV6 DESTINATION ADDRESS:   4::4
INTERFACE INPUT:            Gi0/2
APPLICATION NAME:           port http
counter bytes:              60
ip payload packet section:  0x865B0050 0x79506BC5 0x9FB75D34 0x50190F97
                            0x17090000
```

Task 6: ICMP & UDP Flooding Attacks

- Modify the configuration on the ASA to increase protection against ICMP Floods
- Make sure only one Echo Reply packet is allowed through the firewall for every single Echo Request seen
- Recently there were several incidents of high-volume traffic (Echo Requests) coming from the FR cloud destined to 172.6.102.255
- Configure R6 so those packets never get to other routers in VLAN 102
- Use only one command to accomplish this
- R8 appears to be vulnerable to IPv6 Fraggle attacks and can be used as an amplifier
- Configure R11 to rate-limit Fraggle Echos to 24kbps when destined to 2010:8:57::/64
- Processing of those packets on R8 should be disabled

ASA3

```
no ipv6 access-list OUTSIDE6_IN permit icmp6 any any
ipv6 access-list OUTSIDE6_IN permit icmp6 any any echo

no access-list OUTSIDE_IN extended permit icmp any any
access-list OUTSIDE_IN extended permit icmp any any echo

access-group OUTSIDE_IN in int outside
access-group OUTSIDE6_IN in int outside

fixup protocol icmp
```

R6

```
int f0/1
 no ip directed-broadcast
```

R11

```
ipv6 access-list FRAGGLE
 permit udp any 2010:8:57::/64 eq 7

class-map match-all FRAGGLE_CLASS
 match access-group name FRAGGLE

policy-map OUT_POL
 class FRAGGLE_CLASS
  police 24000

int g0/1
 service-policy output OUT_POL

int g0/2
 service-policy output OUT_POL
```

R8

```
no service udp-small-servers
```

Modifying the ACL on the ASA was not required to meet first two task requirements. Once ICMP inspection is enabled some additional checks will be done on all ICMP packets, including sequence number check, which will ultimately prevent flooding attacks carried over ICMP. Blocking non-matching Replies by the ACL, however, is a more efficient way of dropping unwanted packets on the ASA.

A Smurf attack is an attack where an ICMP echo (or ping) packet is sent to the broadcast address on a network. The source address for the packet is spoofed to emulate the IP address of the victim. On a large network the victim might receive large numbers of ICMP echo replies from all of the hosts on the VLAN and this could cause denial of service.

The Fraggle attack works in a very similar way to the Smurf attack, except that rather than sending spoofed ICMP echo packets, it instead sends spoofed UDP echo packets (which are designed to have the same end result – denial of service against the victim.

IPv6 Considerations

ICMP inspection works also for ICMPv6 packets.

Since there is no concept of broadcast address in IPv6, typical Smurf and Fraggle attacks don't apply. There are, however, some known modified versions of these attacks that use multicasts (like FF02::1). Some OSes may be still vulnerable to those so you may consider rate-limiting or RFC 2827+ RFC3330 filtering at the edge.

Verification

If you did not modify the ACL on the ASA to drop Reply packets the following log messages show up (directed broadcast translation is ON on R6):

```
R11#ping 172.6.102.255 so loop0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.6.102.255, timeout is 2 seconds:
Packet sent with a source address of 11.11.11.11
.....
Success rate is 0 percent (0/5)

%ASA-4-313004: Denied ICMP type=0, from laddr 172.6.102.2 on interface outside to
11.11.11.11: no matching session
%ASA-4-313004: Denied ICMP type=0, from laddr 172.46.46.6 on interface outside to
11.11.11.11: no matching session
%ASA-4-313004: Denied ICMP type=0, from laddr 172.6.102.10 on interface outside to
11.11.11.11: no matching session
```

Before disabling directed broadcast translation:

```
R4#ping 172.6.102.255

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.6.102.255, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/24 ms
R4#
*Mar 16 17:26:57.695: ICMP: echo reply rcvd, src 172.6.102.10, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.703: ICMP: echo reply rcvd, src 172.6.102.2, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.711: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
```

```
*Mar 16 17:26:57.715: ICMP: echo reply rcvd, src 172.6.102.10, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.723: ICMP: echo reply rcvd, src 172.6.102.2, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.731: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.739: ICMP: echo reply rcvd, src 172.6.102.10, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.747: ICMP: echo reply rcvd, src 172.6.102.2, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.755: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.763: ICMP: echo reply rcvd, src 172.6.102.10, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.767: ICMP: echo reply rcvd, src 172.6.102.2, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.775: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.783: ICMP: echo reply rcvd, src 172.6.102.10, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.791: ICMP: echo reply rcvd, src 172.6.102.2, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:26:57.799: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
```

After the feature was disabled, only R6 replies:

```
R6#sh ip int f0/1
FastEthernet0/1 is up, line protocol is up
  Internet address is 172.6.102.6/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
                                  --- Omitted ---

R4#ping 172.6.102.255

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.6.102.255, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

*Mar 16 17:27:07.843: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:27:07.863: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
```

```
*Mar 16 17:27:07.883: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:27:07.903: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
*Mar 16 17:27:07.923: ICMP: echo reply rcvd, src 172.46.46.6, dst 172.46.46.4,
topology BASE, dscp 0 topoid 0
```

Before disabling UDP services on R8:

```
R4#ping ipv6
Target IPv6 address: 2010:8:57::8
Repeat count [5]: 100
Datagram size [100]: 250
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface:
UDP protocol? [no]: yes
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:
Include destination option? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 100, 250-byte UDP Echos to 2010:8:57::8, timeout is 2 seconds:
!!!!!!.!!!!..!!!!!.!!!!!..!!!!!.!!!!!..!!!!!.!!!!!..!!!!!.!!!!!..!!!!!
.!!!!!..!!!!!.!!!!!..!!!!!.!!!
Success rate is 78 percent (78/100), round-trip min/avg/max = 4/4/8 ms

R11#sh policy-map interface g0/1
 GigabitEthernet0/1

  Service-policy output: OUT_POL

    Class-map: FRAGGLE_CLASS (match-all)
      100 packets, 26400 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name FRAGGLE
      police:
          cir 24000 bps, bc 1500 bytes
        conformed 92 packets, 24288 bytes; actions:
          transmit
        exceeded 8 packets, 2112 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: class-default (match-any)
      227 packets, 37909 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
```

```
      Match: any
```

After UDP services were disabled:

```
R4#ping ipv6
Target IPv6 address: 2010:8:57::8
*Mar 16 17:24:44.459: ICMPv6: Sent R-Advert, Src=FE80::21B:D5FF:FE0F:F371,
Dst=FF02::1
2010:8:57::8
Repeat count [5]: 10
Datagram size [100]: 250
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface:
UDP protocol? [no]: yes
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:
Include destination option? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 10, 250-byte UDP Echos to 2010:8:57::8, timeout is 2 seconds:
PPPPP.PPPP
Success rate is 0 percent (0/10)

*Mar 16 17:24:53.587: ICMPv6: Received Unreachable code 4, Src=2010:8:57::8,
Dst=2172:43:43::4
*Mar 16 17:24:53.591: ICMPv6: Received Unreachable code 4, Src=2010:8:57::8,
Dst=2172:43:43::4
*Mar 16 17:24:53.595: ICMPv6: Received Unreachable code 4, Src=2010:8:57::8,
Dst=2172:43:43::4
*Mar 16 17:24:53.599: ICMPv6: Received Unreachable code 4, Src=2010:8:57::8,
Dst=2172:43:43::4
*Mar 16 17:24:53.603: ICMPv6: Received Unreachable code 4, Src=2010:8:57::8,
Dst=2172:43:43::4
```

Task 7: Fragmentation Attacks

- Router 6's F0/1 interface should be configured to prevent Buffer Overflow fragment attack
- No more than 25 packets should be in the process of reassembly at any point in time
- Ensure that a packet of up to 13 fragments can be reassembled successfully
- R11 should be blocking IP fragments on its G0/1 interface
- Configure ASA3 to physically reassemble all IP fragments

R6

```
int f0/1
 ip virtual-reassembly in max-fragments 13 max-reassemblies 25
 ipv6 virtual-reassembly in max-fragments 13 max-reassemblies 25
```

R11

```
ip access-list extended BLOCK
 deny   ip any any fragments
 permit ip any any

ipv6 access-list BLOCK6
 deny ipv6 any any fragments
 permit ipv6 any any

int g0/1
 ip access-group BLOCK in
 ipv6 traffic-filter BLOCK6 in
```

ASA3

```
fragment reassembly full inside
fragment reassembly full outside
```

Virtual Fragment Reassembly (VFR) is responsible for detecting the Tiny Fragment Attack, Overlapping Fragment Attack, and Buffer Overflow attacks caused by fragmentations. If asked about protection against any of these attacks VFR would be a viable solution.

In this particular task you are asked to ensure that no more than 25 packets should be in the process of reassembly at any point in time. This would prevent a Buffer Overflow attack in which bogus fragments are being handled by a router, thus consuming unnecessary resources. Also setting the maximum fragments allowed will cause any fragments over 13 to be dropped.

IPv6 Considerations

As shown in this task Virtual Fragment Reassembly can be also enabled for IPv6 on IOS.
The "`fragment`" ACL keyword is only enabled when "IP" is used as the protocol.

On the ASA the "`fragment`" command affects IPv4 and IPv6 packets.

Verification

From the partial debug output below we see R6 switches IP fragments (ping was used to generate traffic):

```
*Mar 17 20:38:40.105: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
g=172.46.46.4, len 1500, forward
```

```
*Mar 17 20:38:40.109: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
len 1500, post-encap feature, CAR(4), rtype 0, forus FALSE, sendself FALSE, mtu 0,
fwdchk FALSE
*Mar 17 20:38:40.109: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
len 1500, sending fragment


*Mar 17 20:38:40.109: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
g=172.46.46.4, len 21, forward
*Mar 17 20:38:40.109: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
len 21, sending last fragment
*Mar 17 20:38:40.113: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
len 21, post-encap feature, CAR(4), rtype 0, forus FALSE, sendself FALSE, mtu 0,
fwdchk FALSE
*Mar 17 20:38:40.113: IP: s=172.6.102.2 (FastEthernet0/1), d=4.4.4.4 (Serial0/1/0),
len 21, sending last fragment
```

For IPv6 note Next Header is 44 in both packets which is Extension Header “Fragment”:

```
*Mar 17 20:40:49.057: IPV6: source 2172:6:102::2 (FastEthernet0/1)
*Mar 17 20:40:49.057:       dest 4::4 (Serial0/1/0)
*Mar 17 20:40:49.057:       traffic class 0, flow 0x0, len 1496+14, prot 44, hops
63, forwarding

*Mar 17 20:40:49.061: IPV6: source 2172:6:102::2 (FastEthernet0/1)
*Mar 17 20:40:49.061:       dest 4::4 (Serial0/1/0)
*Mar 17 20:40:49.061:       traffic class 0, flow 0x0, len 61+14, prot 44, hops 63,
forwarding
```

The feature is now enabled and as we will see later packets will be virtually reassembled before being switched or just sent to the upper layer for processing:

```
R6#sh ip virtual-reassembly f0/1
FastEthernet0/1:
   Virtual Fragment Reassembly (VFR) is ENABLED [in]
   Concurrent reassemblies (max-reassemblies): 25
   Fragments per reassembly (max-fragments): 13
   Reassembly timeout (timeout): 3 seconds
   Drop fragments: OFF

   Current reassembly count:0
   Current fragment count:0
   Total reassembly count:3
   Total reassembly timeout count:0


R6#sh ipv virtual-reassembly
 All enabled IPv6 interfaces...
```

```
%Interface FastEthernet0/1 [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 25
   IPv6 configured fragments per reassembly (max-fragments): 13
   IPv6 configured reassembly timeout (timeout): 3 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:1
   IPv6 total reassembly timeout count:0
```

Two fragments were received – Initial packet is 1480 byte long; second fragment is just 1 byte:

```
IP_VFR: fragment 0x49FD43E0(sa:172.6.102.2, da:4.4.4.4, id:23, offset:0, len:1480)
in proc path...
IP_VFR: created frag state for pak:ox49FD43E0, sa:172.6.102.2, da:4.4.4.4, id:23...
IP_VFR: Locking frag state new lock 1 old lock  0                    for
sa:172.6.102.2, da:4.4.4.4, id:23
IP_VFR: Pak 0x49FD43E0 seen in Proc path while Processing frag state
IP_VFR: fragment queued to frag state
IP_VFR: pak incomplete cpak-offset:0, cpak-len:1480, flag: 1
IP_VFR: dgrm incomplete, returning...


IP_VFR: fragment 0x490510DC(sa:172.6.102.2, da:4.4.4.4, id:23, offset:1480, len:1)
in proc path...
IP_VFR: Locking frag state new lock 1 old lock  0                    for
sa:172.6.102.2, da:4.4.4.4, id:23
IP_VFR: Pak 0x490510DC seen in Proc path while Processing frag state
IP_VFR: fragment queued to frag state
IP_VFR: cpak-offset:0, cpak-len:1480, npak-offset:1480
IP_VFR: dgrm complete, switching the frags.
IP_VFR: switching fragment (sa:172.6.102.2, da:4.4.4.4, id:23, offset:0, len:1480)
IP_VFR: switching fragment (sa:172.6.102.2, da:4.4.4.4, id:23, offset:1480, len:1)
IP_VFR: all fragments have been switched.
IP_VFR: deleted frag state for sa:172.6.102.2, da:4.4.4.4, id:23
```

And the same for IPv6 – VFR reassembles the fragments before router starts processing them:

```
*Mar 17 20:49:15.841: VFR FUNC: ipv6_vfr_feature, fragment (srcaddr:2172:6:102::2,
dstaddr:4::4,
 id 5, offset:0, packet len:1456

*Mar 17 20:49:15.841: VFR FUNC: ipv6_vfr_find_frag_state, no match for frag state
 inputs were:  srsaddr:2172:6:102::2,
 dstaddr:4::4, id:5
```

```
*Mar 17 20:49:15.845: VFR FUNC: ipv6_vfr_feature, fragment (srcaddr:2172:6:102::2,
dstaddr:4::4,
 id 5, offset:1448, packet len:21

*Mar 17 20:49:15.845: VFR FUNC: ipv6_vfr_find_frag_state, matched frag state =
0x4AF92718,
 srsaddr:2172:6:102::2,dstaddr:4::4, id:5
```

Moving on to R11. Before an ACL was applied:

```
R5#ping 4.4.4.4 so l0 rep 2 size 1501

Type escape sequence to abort.
Sending 2, 1501-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 8/8/8 ms
```

After applying ACL all fragments are dropped:

```
R5#ping 4.4.4.4 so l0 rep 2 size 1501

Type escape sequence to abort.
Sending 2, 1501-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
..
Success rate is 0 percent (0/2)

R11(config-if)#do sh access-l BLOCK
Extended IP access list BLOCK
    10 deny ip any any fragments (2 matches)
    20 permit ip any any (8 matches)


R5#ping 4::4 so l0 rep 2 size 1499

Type escape sequence to abort.
Sending 2, 1499-byte ICMP Echos to 4::4, timeout is 2 seconds:
Packet sent with a source address of 5::5
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 4/4/4 ms

R5#ping 4::4 so l0 rep 2 size 1501

Type escape sequence to abort.
Sending 2, 1501-byte ICMP Echos to 4::4, timeout is 2 seconds:
Packet sent with a source address of 5::5
..
Success rate is 0 percent (0/2)
```

```
R11#sh ipv6 access-list BLOCK6
IPv6 access list BLOCK6
    deny ipv6 any any fragments (2 matches) sequence 10
    permit ipv6 any any (9 matches) sequence 20
```

Prior to enabling Fragment Reassembly on the ASA R4 receives fragmented traffic:

```
R4#
*Mar 17 21:06:54.244: IP: s=7.7.7.7 (FastEthernet0/1), d=4.4.4.4, len 1500, rcvd 4
*Mar 17 21:06:54.244:      IP Fragment, Ident = 21, fragment offset = 0
*Mar 17 21:06:54.244:      ICMP type=8, code=0
*Mar 17 21:06:54.244: IP: s=7.7.7.7 (FastEthernet0/1), d=4.4.4.4, len 1500, stop
process pak for forus packet
*Mar 17 21:06:54.244:      IP Fragment, Ident = 21, fragment offset = 0
*Mar 17 21:06:54.244:      ICMP type=8, code=0
*Mar 17 21:06:54.244: IP: recv fragment from 7.7.7.7 offset 0 bytes
*Mar 17 21:06:54.244: IP: s=7.7.7.7 (FastEthernet0/1), d=4.4.4.4, len 21, input
feature
*Mar 17 21:06:54.244:      IP Fragment, Ident = 21, fragment offset = 1480, MCI
Check(78), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE

R4#sh ip traffic | in rag
  Frags: 1 reassembled, 0 timeouts, 0 couldn't reassemble
         1 fragmented, 2 fragments, 0 couldn't fragment

R4#sh ipv tra | in rag
               2 fragments, 1 total reassembled
               1 fragmented into 2 fragments, 0 failed
```

After the feature was enabled, even that packets appear to be reassembled, they are then dropped due to the “invalid” length – it is probably a problem related to this particular code version:

```
ASA3(config)# sh fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: full
    Queue: 0, Assembled: 25, Fail: 6, Overflow: 0
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: full
    Queue: 0, Assembled: 0, Fail: 1, Overflow: 0

R7(config)#int f0/1
R7(config-if)#mtu 1280

R7#ping 4.4.4.4 so l0 rep 1 size 1281

Type escape sequence to abort.
```

```
Sending 1, 1281-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
.
Success rate is 0 percent (0/1)

R7#ping 4::4 rep 1 size 1281

Type escape sequence to abort.
Sending 1, 1281-byte ICMP Echos to 4::4, timeout is 2 seconds:
.
Success rate is 0 percent (0/1)

R7#ping 4.4.4.4 so l0 rep 1 size 1280

Type escape sequence to abort.
Sending 1, 1280-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms

R7#ping 4::4 rep 1 size 1280

Type escape sequence to abort.
Sending 1, 1280-byte ICMP Echos to 4::4, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
```

Task 8: IP Options Attacks

- Router 6's should be configured to drop packets with Route-Record option on S0/1/0
- Traffic with Home Test (HoT) messages should be also blocked
- R11 should be configured to prevent attacks that use RH0
- In addition packets with any IPv4 Option set should be blocked
- ASA3 should stop traffic with Hop-by-Hop EH; traffic with Router Alert option should be forwarded
- Make sure IPv6 Extensions are ordered according to the RFC; otherwise drop the packet

R6

```
ip access-list extended NO_RR
 deny   ip any any option record-route
 permit ip any any

ipv6 access-list NO_HOT
 deny ipv6 any any mobility-type hot
 permit ipv6 any any

int s0/1/0
 ip access-group NO_RR in
 ipv6 traffic-filter NO_HOT in
```

R11

```
no ipv6 source-route
ip options drop
```

ASA3

```
policy-map type inspect ipv6 OP6_POL
 parameters
  verify-header order
 match header hop-by-hop
  drop log

policy-map type inspect ip-options OP_POL
 parameters
  router-alert action allow

policy-map global_policy
 class inspection_default
  inspect ip-options OP_POL

policy-map IF_POL
 class class-default
  inspect ipv6 OP6_POL

service-policy IF_POL interface inside
service-policy IF_POL interface outside
```

IP options are extensions of the Internet Protocol that are typically used for debugging purposes or to give some additional information to certain applications or protocols, such as RSVP. Attackers typically use IP options for source routing, which is a way of forcing a packet to go via set of networking devices, for example to bypass security systems.

Access-lists can be used to block a particular IP/IPv6 option and its type.

The "`ip options drop`" command forces a router to drop transit and non-transit packets with any IP option set.

On the ASA by default behavior is to perform inspection of IPv4 packets with IP Options. Only three can be cleared or allowed, namely EOOL, NOP and Router Alert. Packets with all other options are dropped.

IPv6 Considerations

In IPv6 functionality of options is removed from the main header and is implemented through a set of additional headers called extension headers. Probably the most important EH from the security standpoint is the Routing EH – which can be actually one of three types:

1. Type 0 (RH0), which is the evil mechanism that provides an extended version of IPv4 source routing
2. Type 1 (RH1) was developed by DARPA and is currently unused
3. And Type 2 (RH2) which is only used by Mobility IPv6 devices

Type 1 and Type 2 Routing Headers are completely inoffensive and as of today there is no point in blocking those. For the Type 0, RH0, it opened IPv6 stack to multiple vulnerabilities, including various Denial of Service attacks or even susceptibility to so-called killer packets that could melt down some old-code IOS routers (with just a single malformed packet). This is why this Type 0 Routing Header was deprecated in RFC 5095 and it is now ignored or dropped in newer IOS versions by default (`no ipv6 source-route`).

On the ASA the default behavior is to pass packets with Hop-by-Hop or Destination Option Headers; packets containing Routing Header Extension will be dropped. To change this we can configure IPv6 inspection (MPF) and specify what extensions we want to allow and what to drop.

Note that once you create the ipv6 inspect policy-map, the ASA automatically adds some commands to block all possible Types of Routing EH :

```
match header routing-type range 0 255
  drop log
```

This configuration can be modified or removed, if for some reasons we would want to allow packets with Routing Extensions or just some particular Routing EH Types.

Verification

First R6. Let's see how traffic is handled before an ACL is applied:

```
R4#ping
Protocol [ip]:
Target IP address: 2.2.2.2
Repeat count [5]: 2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]: 4
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 19, padded length=20
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)

Reply to request 0 (20 ms).  Received packet has options
 Total option bytes= 20, padded length=20
 Record route:
   (172.46.46.4)
   (172.6.102.6)
   (2.2.2.2)
   (172.6.102.2)
   <*>
 End of list

Reply to request 1 (20 ms).  Received packet has options
 Total option bytes= 20, padded length=20
 Record route:
   (172.46.46.4)
   (172.6.102.6)
   (2.2.2.2)
   (172.6.102.2)
   <*>
 End of list

Success rate is 100 percent (2/2), round-trip min/avg/max = 20/20/20 ms
```

Packets are definitely allowed, Route Record is processed. Now ACL has been applied and another ping is issued. The result is different:

```
Unreachable from 172.46.46.6.  Received packet has options
 Total option bytes= 19, padded length=20
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)

R6#sh access-l
Extended IP access list NO_RR
    10 deny ip any any option record-route (5 matches)
    20 permit ip any any (12 matches)
```

To test configuration on R6 I will slightly modify routing so packets go through R11 instead of directly across VLAN 857:

```
R7(config-if)#ipv6 ospf cost 200
R7(config-if)#ip ospf cost 200

R7#ping
Protocol [ip]:
Target IP address: 5.5.5.5
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: timestamp
Number of timestamps [ 9 ]: 5
Loose, Strict, Record, Timestamp, Verbose[TV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 24, padded length=24
 Timestamp: Type 0.  Overflows: 0 length 24, ptr 5
  >>Current pointer<<
  Time= 00:00:00.000 UTC (00000000)
  Time= 00:00:00.000 UTC (00000000)
  Time= 00:00:00.000 UTC (00000000)
  Time= 00:00:00.000 UTC (00000000)
  Time= 00:00:00.000 UTC (00000000)

Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
Success rate is 0 percent (0/5)
```

Since "`ip options drop`" was issued, traffic is blocked:

```
R11#sh ip traffi | in options
         0 security failures, 0 bad options, 0 with options
         5 options denied
```

Now let's test IPv6 Source Routing:

```
R7#trace ipv

Target IPv6 address: 5::5
Source address:
Insert source routing header? [no]: yes
Nexthop address: 2010:0:115::11
Nexthop address:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 5::5

  1 2010:0:117::11 0 msec 0 msec 0 msec
  2 2010:0:115::5 4 msec 4 msec 0 msec
  3 2010:0:115::5 0 msec 4 msec 0 msec
  4 2010:0:115::5 4 msec 4 msec 0 msec
  5 2010:0:115::5 4 msec *  0 msec
  6 2010:0:115::5 4 msec 4 msec 0 msec
  7 2010:0:115::5 4 msec 4 msec 0 msec
  8 2010:0:115::5 4 msec 0 msec 0 msec
  9  *  0 msec 4 msec

R11#sh ipv traf  | in source
               44 source-routed, 0 truncated
               0 bad header, 0 unknown option, 0 bad source
```

After "`no ipv6 source-route`" is issued, R11 starts dropping packets. It will send ICMPv6 Unreachable message "Parameter Problem" back to the source; this is why we see "?" in the output:

```
R7#trace ipv

Target IPv6 address: 5::5
Source address:
Insert source routing header? [no]: yes
Nexthop address: 2010:0:115::11
Nexthop address:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
```

```
Tracing the route to 5::5

  1   ?   ?   ?
  2   ?   ?   ?
  3   ?   ?   ?
  4   ?   *   ?
  5   ?   ?   ?
  6   ?   ?   ?
  7   ?   ?   ?
  8   *   ?   ?
  9   ?   ?   ?
```

And the ASA. For some reasons ICMPv6 packets with Hop-by-Hop options are getting through the firewall – to show you our policy is correct we will generate UDP traffic:

```
ASA3(config)# ipv access-list OUTSIDE6_IN per icmp6 any any 1 4
```

```
R11#ping ipv
Target IPv6 address: 4::4
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface:
UDP protocol? [no]: yes
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]: yes
Include destination option? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte UDP Echos to 4::4, timeout is 2 seconds:
PPPPP
Success rate is 0 percent (0/5)


R11#ping ipv6
Target IPv6 address: 4::4
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface:
UDP protocol? [no]: yes
Verbose? [no]:
Precedence [0]:
DSCP [0]:
```

```
Include hop by hop option? [no]: yes
Include destination option? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte UDP Echos to 4::4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)


%ASA-4-325004: IPv6 Extension Header hop-by-hop denied and logged by configuration.
UDP from inside:2010:0:113::11/56294 to outside:4::4/7
%ASA-4-325004: IPv6 Extension Header hop-by-hop denied and logged by configuration.
UDP from inside:2010:0:113::11/62373 to outside:4::4/7
%ASA-4-325004: IPv6 Extension Header hop-by-hop denied and logged by configuration.
UDP from inside:2010:0:113::11/57821 to outside:4::4/7


ASA3(config)# sh service-policy inspect ipv6

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default

Interface inside:
  Service-policy: IF_POL
    Class-map: class-default
      Inspect: ipv6 OP6_POL, packet 0, lock fail 0, drop 0, reset-drop 0
        params verify-header type fails 0
        params verify-header order fails 0
        match header hop-by-hop
          drop log, packet 0
        match header routing-type
          drop, packet 0
          log, packet 0

Interface outside:
  Service-policy: IF_POL
    Class-map: class-default
      Inspect: ipv6 OP6_POL, packet 5, lock fail 0, drop 5, reset-drop 0
        params verify-header type fails 0
        params verify-header order fails 0
        match header hop-by-hop
          drop log, packet 5
        match header routing-type
          drop, packet 0
          log, packet 0
```

Task 9: Layer 3 Spoofing Attacks

- Implement RFC 2827 on R6's FR interface
- Make sure RFC 1918 ranges are blocked as well
- RFC 3330 should be implemented for IPv6 – only account for the multicast range
- Prevent IP Spoofing Attacks on R4
- Only traffic received from a network that exists in the routing table for a given network should be allowed
- Default route should be considered as a valid route for IPv6 packets but the interface the packet is received on must match egress interface from the entry in the RIB

R4

```
int s0/0/0
 ip verify unicast source reachable-via any
 ipv6 verify unicast source reachable-via rx allow-default
```

R6

```
ip access-list extended NO_RR
 deny   ip any any option record-route
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 deny   ip 172.6.102.0 0.0.0.255 any
 deny   ip host 2.2.2.2 any
 deny   ip host 6.6.6.6 any
 deny   ip host 100.100.100.10 any
 permit ip any any
ip access-list extended IP_OUT
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 permit ip 172.6.102.0 0.0.0.255 any
 permit ip host 2.2.2.2 any
 permit ip host 100.100.100.10 any
 deny   ip any any log

ipv6 access-list NO_HOT
 deny ipv6 any any mobility-type hot
 permit ipv6 host FF02::5 any
 permit ipv6 host FF02::6 any
 deny ipv6 FF00::/8 any
 deny ipv6 2172:6:102::/64 any
 deny ipv6 host 2::2 any
 deny ipv6 host 6::6 any
 deny ipv6 host 10::10 any
 permit ipv6 any any
```

```
ipv6 access-list IP6_OUT
 permit ipv6 2172:6:102::/64 any
 permit ipv6 host 2::2 any
 permit ipv6 host 10::10 any
 deny ipv6 any any log

int s0/1/0
 ip access-group IP_OUT out
 ipv6 traffic-filter IP6_OUT out
```

The RFC 1918 ranges are 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 so well block them in our ACL.

RFC 2827 says we only want to allow our assigned ranges as valid sources; traffic coming to us, on the other hand, should never use our address space.

RFC 3330 ranges are created to cover all other RFCs that specify ranges that should never be seen in source headers on the Internet. IPv4 examples : 0.0.0.0/8, RFC 1918, 127.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, 224.0.0.0/3

Our ACLs only block/allow host prefixes for loopbacks. On the exam you may want to ask the proctor if they want to filter the entire subnet or just treat a loopback as a single host.

Loose mode uRPF is designed to ensure that traffic is received only from networks known to the router. This helps prevent against spoofing of packets from illegitimate ranges (such as RFC1918 or RFC3330) that shouldn't ever be seen in an internet routing table.

Strict mode uRPF is configured to ensure that any packet that is received is compared to the routing table to ensure that it was received via interface that provides the best possible path back to the source of the traffic.

The challenge with strict mode uRPF is that there must be specific routes in the routing table for every possible source of traffic (default routes aren't considered without explicitly allowing them) and that symmetric routing is potentially required on the network. If your router is receiving a default route (for example on an internet link) then the additional option to compare the default route may be required.

IPv6 Considerations

RFC 1918 does not apply to IPv6.

For RFC 3330, ranges other than multicast you might want to block at the edge would be 6to4 and Teredo prefixes, unspecified address (::/128), Loopback (::1/128) and few more. This is not something I would bother trying to memorize – just remember about FF00::/8, unspecified and loopback addresses.

uRPF can be configured for IPv6 by using the "`ipv6 verify unicast source`" command.

Verification

```
R2#ping 4.4.4.4 so l0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms

R4(config)#int l2
R4(config-if)#ip add 6.6.6.6 255.255.255.0
R4(config-if)#ipv add 6::6/64

R4(config-if)#do ping 2.2.2.2 so l2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 6.6.6.6
.....
Success rate is 0 percent (0/5)

R4(config-if)#do ping 2::2 so l2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2::2, timeout is 2 seconds:
Packet sent with a source address of 6::6
.....
Success rate is 0 percent (0/5)

R6(config)#do sh access-list NO_RR
Extended IP access list NO_RR
    10 deny ip any any option record-route (5 matches)
    11 deny ip 10.0.0.0 0.255.255.255 any
    12 deny ip 172.16.0.0 0.15.255.255 any
    13 deny ip 192.168.0.0 0.0.255.255 any
    14 deny ip 172.6.102.0 0.0.0.255 any
    15 deny ip host 2.2.2.2 any
    16 deny ip host 6.6.6.6 any (5 matches)
    17 deny ip host 100.100.100.10 any
    20 permit ip any any (751 matches)

R6(config)#do sh access-list NO_HOT
IPv6 access list NO_HOT
    deny ipv6 any any mobility-type hot sequence 10
    permit ipv6 host FF02::5 any sequence 50
    permit ipv6 host FF02::6 any sequence 60
    deny ipv6 FF00::/8 any sequence 70
    deny ipv6 2172:6:102::/64 any sequence 80
```

```
    deny ipv6 host 2::2 any sequence 90
    deny ipv6 host 6::6 any (5 matches) sequence 100
    deny ipv6 host 10::10 any sequence 110
    permit ipv6 any any (142 matches) sequence 120


R4(config)#do sh ip ro 60.60.60.60
% Network not in table
```

We have a default route pointing go the ASA for IPv6. This means that the egress interface for this entry is F0/1:

```
R4(config)#do sh ipv ro 60::60
Routing entry for ::/0
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2172:43:43::30
      Last updated 02:17:42 ago
```

If we try to send packets with a spoofed source from the FR cloud, they are all dropped:

```
R6(config)#int l6
R6(config-if)#ip add 60
R6(config-if)#ip add 60.60.60.60 255.255.255.0
R6(config-if)#ipv add 60::60/64

R6(config-if)#do ping 4.4.4.4 so l6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 60.60.60.60
.....
Success rate is 0 percent (0/5)

R6(config-if)#do ping 4::4 so l6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4::4, timeout is 2 seconds:
Packet sent with a source address of 60::60
.....
Success rate is 0 percent (0/5)

R4#sh ip int s0/0/0 | in verif
  IP verify source reachable-via ANY
   5 verification drops
   0 suppressed verification drops
   0 verification drop-rate
```

```
R4#sh ipv int s0/0/0 | in verif
 IPv6 verify source reachable-via rx, allow default
   0 verification drop(s) (process), 5 (CEF)
   0 suppressed verification drop(s) (process), 0 (CEF)
```

Since the default route is taken into account for IPv6 RPF, packet with 60::60 in the source is allowed from the ASA side of the network:

```
R11(config)#int l11
R11(config-if)#ipv add 60::60/64

R11(config)#do ping 4::4 so l11

R4#deb ipv icmp
  ICMP Packet debugging is on

R4#
*Mar 18 18:14:47.611: ICMPv6: Received echo request, Src=60::60, Dst=4::4
*Mar 18 18:14:47.611: ICMPv6: Sent echo reply, Src=4::4, Dst=60::60
R4#
*Mar 18 18:14:49.607: ICMPv6: Received echo request, Src=60::60, Dst=4::4
*Mar 18 18:14:49.611: ICMPv6: Sent echo reply, Src=4::4, Dst=60::60
```

Task 10: TCP SYN Attacks

- Routers 5 and 7 should protect VLAN 857 from SYN Flooding attack
- Use TCP Intercept as a protection tool
- Routers should not act as a proxy for the connections
- Aggressive mode should start when there is more than 500 half-open connections detected total or 60 during last minute
- Aggressive mode should cease once the number of half-open sessions falls below 250 total or 30 within the last 60 seconds
- ASA should limit the number of simultaneous TCP and/or UDP connections to 1000
- Embryonic connection limit should be set to 400 with a per-device limit of 50
- ASA's limits should also apply to IPv6 traffic

R5, R7

```
access-list 110 permit tcp any 10.8.57.0 0.0.0.255

ip tcp intercept list 110
ip tcp intercept watch-timeout 10
ip tcp intercept max-incomplete low 250 high 500
ip tcp intercept one-minute low 30 high 60
ip tcp intercept mode watch
```

ASA3

```
access-list TCP_UDP extended permit tcp any any
access-list TCP_UDP extended permit udp any any

class-map TCP_UDP_CLASS
 match access-list TCP_UDP

policy-map global_policy
 class TCP_UDP_CLASS
  set connection conn-max 1000 embryonic-conn-max 400 per-client-
  embryonic-max 5
 class class-default
  set connection conn-max 1000 embryonic-conn-max 400 per-client-
  embryonic-max 50
```

TCP Intercept can be configured to act in one of two modes:

1. The default mode is “Intercept” which means that the router intercepts SYN packets from clients and establishes a connection with them on behalf of the real servers. Then only if final ACK is received, router establishes a connection with the server and merges the two connections together
2. The second mode is called “Watch”. Here the difference is that router does not participate in the initial TCP session establishment, it only watches the connection requests that flow through the router. Then if a connection fails to get established in a specified interval, the router will terminate attempt sending an RST packet to the Server

When an attack is being detected (“high” threshold is exceeded) TCP Intercept enters the so-called Aggressive Mode, which means that every new connection attempt software deletes one oldest half-open session (this default behavior can be changed by `ip tcp intercept drop-mode` command). More over, TCP packets will be retransmitted two times faster, this is for Intercept Mode, and in the Watch Mode the watch-timeout will be reduced by half.

An embryonic (also known as half-open) connection is a TCP connection request that has not finished the necessary handshake between source and destination.

On the ASA if the embryonic connection limit is reached, then the security appliance responds to every SYN packet sent to the server with a SYN+ACK, and does not pass the SYN packet to the internal server. If the external device responds with an ACK packet, then the security appliance knows it is a valid request (and not part of a potential SYN attack). The security appliance then establishes a connection with the server and joins the connections together. If the security appliance does not get an ACK back from the server, it aggressively times out that embryonic connection.

IPv6 Considerations

IOS TCP Intercept cannot be configured for IPv6.

For MPF features that support IPv6 the `match any` and `match default-inspection-traffic` commands are the only commands that match IPv6 traffic

Verification

Lower the thresholds and emulate some half-open sessions by e.g. dropping final ACK:

```
R5(config)#ip tcp intercept one-minute low 1 high 2

R5#sh tcp intercept connections
Incomplete:
Client                  Server                  State    Create   Timeout  Mode
10.0.115.11:21062       10.8.57.8:23            SYNRCVD  00:00:02 00:00:07 W
10.0.113.130:60534      10.8.57.8:23            SYNSENT  00:00:03 00:00:06 W
10.0.115.11:51958       10.8.57.8:23            SYNRCVD  00:00:08 00:00:01 W

R5#sh tcp intercept statistics
Watching new connections using access-list 110
3 incomplete, 0 established connections (total 3)
19 connection requests per minute

*Mar 18 20:38:11.426: %TCP-6-INTERCEPT: getting aggressive, count (2/2) 1 min 5
```

After a while once the amount of half-open sessions falls below the threshold router leaves Aggressive Mode:

```
*Mar 18 20:41:08.130: %TCP-6-INTERCEPT: calming down, count (0/1) 1 min 0
```

On the ASA use regular MPF verification command (`show service-policy`):

```
ASA3(config)# sh service-policy set connection de

Global policy:
  Service-policy: global_policy
    Class-map: TCP_UDP_CLASS
      Set connection policy: conn-max 1000 embryonic-conn-max 400 per-client-
embryonic-max 50
        current embryonic conns 2, current conns 2, drop 0
        Per client                Embryonic     Total
        inside     10.0.113.11    2             2
    Class-map: class-default
      Set connection policy: conn-max 1000 embryonic-conn-max 400 per-client-
embryonic-max 50
        current embryonic conns 0, current conns 0, drop 0
        Per client                Embryonic     Total
           None                   -             -
```

```
ASA3(config)# sh service-policy set connection de

Global policy:
  Service-policy: global_policy
    Class-map: TCP_UDP_CLASS
      Set connection policy: conn-max 1000 embryonic-conn-max 400 per-client-
embryonic-max 50
        current embryonic conns 0, current conns 0, drop 0
        Per client                Embryonic     Total
           None                   -             -
    Class-map: class-default
      Set connection policy: conn-max 1000 embryonic-conn-max 400 per-client-
embryonic-max 50
        current embryonic conns 0, current conns 1, drop 0
        Per client                Embryonic     Total
        inside     2010:0:113::11  0             1
```

Task 11: Application Attacks & FPM

- Use Flexible Packet Matching to drop malicious traffic
- Packets containing the string of characters „BADCC1E" within 100 bytes from the start of the UDP header should be blocked
- Those packets are destined to the well-known UDP port 53
- This policy should be applied to R7's F0/0 interface inbound
- You are allowed to use Protocol Header Definition Files to implement this
- R5 should be configured to drop and log ICMP packets with "AZ" in the payload
- Those packets will be carried in an IP-IP tunnel
- You are only interested in dropping Echo packets only

R5

```
class-map type access-control match-all FPM_IPIP_CLASS
 match start l3-start offset 9 size 1 eq 4
 match start l3-start offset 29 size 1 eq 1
 match start l3-start offset 40 size 1 eq 8
 match start l3-start offset 44 size 100 regex ".*AZ.*"

policy-map type access-control FPM_POL
 class FPM_IPIP_CLASS
   drop
   log

interface f0/0
 service-policy type access-control input FPM_POL
```

R7

```
load protocol system:/fpm/phdf/ip.phdf
load protocol system:/fpm/phdf/udp.phdf

class-map type access-control match-all FPM_UDP_CLASS
```

```
 match start UDP payload-start offset 0 size 100 string "BADCC1E"

class-map type stack match-all FPM_STACK_CLASS
 match field IP protocol eq 0x11 next UDP
 match field UDP dest-port eq 0x35 next UDP

policy-map type access-control FPM_POL
 class FPM_UDP_CLASS
   drop

policy-map type access-control FPM_STACK_POL
 class FPM_STACK_CLASS
  service-policy FPM_POL

int f0/0
 service-policy type access-control input FPM_STACK_POL
```

FPM or Flexible Packet Matching can be thought of as a next-generation access-list providing more thorough and customized packet filters. The main advantage of this feature is that it allows us to match an arbitrary string of bits within either the packet header or its payload.

Things to be aware of about FPM:

- It is completely stateless; it does not keep track of dynamic ports
- It cannot match across packets - it treats each packet independently from each other
- It cannot classify packets with IP Options
- It is not supported on tunnel and MPLS interfaces

One important component of FPM are Protocol Header Definition Files. These are just predefined files containing structure of protocol headers and their fields. If we don't load PHDFs to the memory, the `match field` command will not be available for us, only the `match start` option. This means that you would need to know the exact structure of a particular header in order to successfully implement a FPM policy.

Configuration-wise don't forget whenever you use FPM policies you need to define the class-map, the policy-map and the service-policy command with the "`type access-control`" so that the router realizes you are leveraging FPM. More over, if PHDFs are to be used, the protocol stack must be defined via `class-map type stack`.

To find translations of decimal/hex ASCII to text use the IOS Configuration Fundamentals Command Reference, "ASCII Character Set and Hexadecimal Values".

IPv6 Considerations

FPM can only "inspect" IPv4 unicast packets.

Verification

On R7 we should be at least able to see UDP port 53 traffic matches our Stack class:

```
R8(config)#ip domain lookup
R8(config)#ip name-server 7.7.7.7

R8#SkyFall
Translating "SkyFall"...domain server (7.7.7.7)
 (7.7.7.7)

R7#show policy-map type access-control int f0/0
 FastEthernet0/0

  Service-policy access-control input: FPM_STACK_POL

    Class-map: FPM_STACK_CLASS (match-all)
      11 packets, 836 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x11 next UDP
      Match: field UDP dest-port eq 0x35 next UDP

      Service-policy access-control : FPM_POL

        Class-map: FPM_UDP_CLASS (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps
          Match: start UDP payload-start offset 0 size 100 string "BADCC1E"
      drop

        Class-map: class-default (match-any)
          11 packets, 836 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

    Class-map: class-default (match-any)
      52 packets, 5096 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

An IPinIP tunnel was configured between R8 and R11 to test this configuration. Packets generated on R8 (0x415A is “AZ” in ASCII) go through R5’s F0/0:

```
R8#ping
Protocol [ip]:
Target IP address: 172.100.100.11
Repeat count [5]:
```

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0x415A
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.100.100.11, timeout is 2 seconds:
Packet has data pattern 0x415A
.....
Success rate is 0 percent (0/5)

R5#
*Mar 18 22:39:13.174: %SEC-6-IPACCESSLOGRP: list FPM_C3 denied ipinip 8.8.8.8
(FastEthernet0/0 ) -> 11.11.11.11, 1 packet

R5#sh policy-map type access-control int f0/0
 FastEthernet0/0

  Service-policy access-control input: FPM_POL3

    Class-map: FPM_C3 (match-all)
      5 packets, 670 bytes
      5 minute offered rate 0 bps
      Match: start l3-start offset 9 size 1 eq 4
      Match: start l3-start offset 29 size 1 eq 1
      Match: start l3-start offset 40 size 1 eq 8
      Match: start l3-start offset 44 size 100 regex ".*AZ.*"
      drop
      log

    Class-map: class-default (match-any)
      70 packets, 7020 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

ICMP Echos with something else than “AZ” in the payload can come through:

```
R8#ping 172.100.100.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.100.100.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 12: DDoS Attacks & RTBH

- AS 600 needs to be configured with RTBH to protect itself against potential attacks
- All traffic sent to R2's loopback 20 interface should be blackholed at the edge of AS
- Use R10 as the trigger router
- Don't inform attacker packets never make their way to the victim
- You are allowed to use static routes in this task

R2

```
ip route 192.0.2.1 255.255.255.255 null 0
```

R6

```
ip route 192.0.2.1 255.255.255.255 null 0

router bgp 600
 neighbor 172.46.46.4 send-community

int null0
 no ip unreachables
```

R10

```
ip route 192.0.2.1 255.255.255.255 null 0

route-map BLACKHOLE permit 10
 match tag 25665
 set local-preference 200
 set origin igp
 set community no-export
 set ip next-hop 192.0.2.1

router bgp 600
 redistribute static route-map BLACKHOLE
 neighbor 172.6.102.6 send-community

ip route 20.20.20.20 255.255.255.255 192.0.2.1 tag 25665
```

RTBH filtering provides a method for quickly dropping undesirable traffic at the edge of the network, based on either source addresses or destination addresses by forwarding it to a Null0 interface. Null0 is a pseudointerface that is always up and can never forward or receive traffic.
Forwarding packets to Null0 is a common way to filter packets to a specific destination.

No matter we want to implement source or destination based RTBH we need to create static routes on the BGP devices (including the trigger router) so they know that a particular Next-Hop value should resolve to Null0.

On the trigger router we define our RTBH policy. This involves defining a route-map, which will be used to redistribute the static "trigger" route into BGP.

The route-map will set a high local preference and an IGP origin type to help ensure it is the best route (if another were to exist) for this network. It will then mark the route with the “no-export” community so that the route will not leave AS600 and set the next hop to the discard address.

We then need to enable the sending of communities (so that the no-export community will be transmitted) and to redistribute static routes matching the RTBH route-map on R6.

There is also other variation of RTBH known as “Source” based. This one works in a similar way to “Destination” based RTBH except that traffic is blocked based on the source IP of the packets. To implement source based RTBH we combine Strict Mode uRPF to block packets where the source address is not the same as the next hop in the routing table. We could achieve this by using RTBH on the trigger router to specify that the best source for the packet is the Null0 interface.

IPv6 Considerations

RTBH can be also implemented with IPv6 BGP. The configuration logic is exactly the same as in IPv4.

Verification

You will need to modify an ACL on R6 to test this (you could have already done this in the Anti-Spoofing task):

```
R6(config)#ip access-list ext IP_OUT
R6(config-ext-nacl)#55 per ip host 20.20.20.20 any
```

All right, let’s take a look at BGP before the trigger route is added:

```
R6#sh ip bgp
BGP table version is 7, local router ID is 6.6.6.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i20.20.20.0/24    172.6.102.2              0    100      0 i
```

Now we’re going to start sending packets to the Victim and at some point later trigger RTBH. ICMP Unreachables were disabled few packets later:

```
R4#ping 20.20.20.20 rep 10000

Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!U.U.U.U.U.U.U.U.....
```

```
Success rate is 86 percent (156/181), round-trip min/avg/max = 16/17/20 ms

R6#sh ip bgp 20.20.20.20
BGP routing table entry for 20.20.20.20/32, version 5
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     2          3
  Local, (Received from a RR-client)
    192.0.2.1 from 172.6.102.10 (100.100.100.10)
      Origin IGP, metric 0, localpref 200, valid, internal, best

R6#sh ip cef 192.0.2.1
192.0.2.1/32
  attached to Null0
```

Note R4 does not know about the “triggered” route :

```
R4#sh ip bgp
BGP table version is 6, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 20.20.20.0/24    172.46.46.6                            0 600 i
```

Task 13: Layer 2 Security & Attacks

- Prevent MAC Spoofing & Flooding attacks on the L2 port connected to R11’s G0/1
- On the same interface limit the amount of unicast packets to 5000 per second
- Broadcast traffic should be restricted to 1Mbps; once the threshold is crossed packets should stop to be dropped after broadcast rate falls below 700kbps
- CAT1 should be configured to black-hole frames with MAC address 00ba.dbad.cc1e seen in VLAN 857
- On CAT1’s F0/7 only allow non-IP packets from MAC address R7 uses on F0/0
- Don’t use Port Security to accomplish this
- Protect CAT4’s CPU from ARP & IGMP flooding attacks
- When the number of offending ARP/IGMP packets exceeds 25 per second the offending VLAN should be shutdown on a port
- After a minute interfaces should be put back into the normal state automatically

CAT3

```
int g1/0/11
 shut
 switchport port-security
 switchport port-security mac-address c84c.751f.ddc1
```

```
 switchport port-security maximum 1
 storm-control broadcast level bps 1m 700k
 storm-control unicast level pps 5k
 no shut
```

CAT1

```
mac address-table static 00ba.dbad.cc1e vlan 857 drop

mac access-list extended MAC_ACL
 permit host 001b.d517.ba88 any
 deny   any any

int f0/7
 mac access-group MAC_ACL in



ip route 192.0.2.1 255.255.255.255 null 0
```

CAT4

```
psp arp pps 25
psp igmp pps 25

errdisable detect cause psp shutdown vlan

errdisable recovery cause psp
errdisable recovery interval 30
```

Port Security is a protection mechanism that can be used to mitigate MAC Spoofing and Flooding attacks. There are two different things we can configure with Port Security:

- We can say that only frames with certain source MAC addresses will be allowed through the port
- We can limit the amount of addresses that we will learn and associate with the port in the Port Security Table which protects the CAM Table from being exhausted

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. This feature uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

Storm control uses one of these methods to measure traffic activity:

- Bandwidth based
- Traffic rate at which packets are received (in packets per second)

The thresholds can either be expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic, or as the rate at which the interface receives traffic. MAC ACLs can be used to filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs. Note that IPv4 traffic is not affected by those ACLs.

Even that the CAM table building process is dynamic in nature, there is an option we can use to enter a MAC address manually (which is termed a static MAC address) into the table. These static MAC entries are retained across a reboot of the switch.

To add an entry into the CAM table manually the "`mac address-table static`" command is used; if you add the "`drop`" keyword at the end it blackhole all frames sourced from/destined to that MAC address on the switch.

Using Protocol Storm Protection, you can control the rate at which control packets are sent to the switch by specifying the upper threshold for the packet flow rate. The supported protocols are ARP, ARP snooping, Dynamic Host Configuration Protocol (DHCP) v4, DHCP snooping, Internet Group Management Protocol (IGMP), and IGMP snooping.

When the packet rate exceeds the defined threshold, the switch drops all traffic arriving on the specified virtual port for 30 seconds. The packet rate is measured again, and protocol storm protection is again applied if necessary. There is also an option to shutdown the offending VLAN on a port for increased security. In that situation you will need to re-enable the port manually or by using the error-disable recovery feature.

IPv6 Considerations

Does not apply.

Verification

The default action taken after violation occurs is "shutdown". This is why the port goes down when we spoof frames with a new MAC:

```
CAT3#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
   Gi1/0/11              1            1                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 2048
```

```
CAT3#sh port-security interface g1/0/11 address
               Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
 115    c84c.751f.ddc1    SecureConfigured              Gi1/0/11     -
------------------------------------------------------------------------------
Total Addresses: 1

R11(config-if)#mac-address 00ab.ab11.ab11

*Mar 19 12:49:07.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down

CAT3#
Mar 19 12:45:36.210: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 00ab.ab11.ab11 on port GigabitEthernet1/0/11.

CAT3#sh port-security int g1/0/11
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00ab.ab11.ab11:115
Security Violation Count   : 1
```

Here are the limits we configure for Storm Control:

```
CAT3#sh storm-control unicast
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Gi1/0/11   Link Down           5k pps       5k pps        0 pps

CAT3#sh storm-control broadcast
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Gi1/0/11   Link Down           1m bps     700k bps        0 bps
```

Change the unicast limit to something low and generate an ICMP flood through the port:

```
R11#ping 5.5.5.5 rep 500
Type escape sequence to abort.
```

```
Sending 500, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!.!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!.
Success rate is 98 percent (205/209), round-trip min/avg/max = 1/1/4 ms

Mar 19 12:52:28.937: %STORM_CONTROL-3-FILTERED: A Unicast storm detected on
Gi1/0/11. A packet filter action has been applied on the interface.
```

Prior to making any changes on CAT1 we can specify a different MAC and it won't affect connectivity in the long run:

```
R8(config-if)#mac-address 00ba.dbad.cc1e
R8(config-if)#do ping 5.5.5.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/2/4 ms
```

After MAC blackholing was enabled R8 can no longer communicate with R5:

```
CAT1#sh mac address-table vlan 857  | in Drop
 857    00ba.dbad.cc1e    STATIC      Drop

R8(config-if)#do ping 5.5.5.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

On R7 I changed MAC address to a random one – from this point on our MAC ACL starts dropping non-IP packets (ARP here):

```
R7#ping 10.8.57.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.57.8, timeout is 2 seconds:

*Mar 19 13:12:46.714: IP ARP: sent req src 10.8.57.7 1212.abab.abaa,
                 dst 10.8.57.8 0000.0000.0000 FastEthernet0/0.
*Mar 19 13:12:48.714: IP ARP: sent req src 10.8.57.7 1212.abab.abaa,
                 dst 10.8.57.8 0000.0000.0000 FastEthernet0/0.
                                --- Omitted ---

CAT1#sh access-lists hardware counters
 L2 ACL INPUT Statistics
```

```
     Drop:                       All frame count: 10
     Drop:                       All bytes count: 640
                                     --- Omitted ---
R8#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.8.57.5                0   001b.d50f.f2f8  ARPA   FastEthernet0/0
Internet  10.8.57.7                0   Incomplete      ARPA
Internet  10.8.57.8                -   001b.d4ef.e728  ARPA   FastEthernet0/0
```

If you generate large enough number of ARP packets received by CAT4 you should be able to see the counter increases:

```
Mar 19 13:47:21.973: %PM-4-ERR_DISABLE_VP: psp error detected on Gi1/0/15, vlan 117.
Putting in err-disable state.
Mar 19 13:47:21.998: %PM-4-ERR_DISABLE_VP: psp error detected on Gi1/0/17, vlan 33.
Putting in err-disable state.
Mar 19 13:47:22.023: %PM-4-ERR_DISABLE_VP: psp error detected on Gi1/0/15, vlan 33.
Putting in err-disable state.

CAT4#sh int status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Gi1/0/15                     connected    psp                  33,117
Gi1/0/17                     connected    psp                  33
Gi1/0/23                     connected    psp                  33

CAT4#sh psp statistics

---------------------------------
PSP Protocol Drop Counter Summary:
---------------------------------
ARP  Drop Counter : 3

DHCP Drop Counter : 0

IGMP Drop Counter : 0

CAT4#sh psp config

---------------------------------
PSP Protocol Configuration Summary:
---------------------------------

ARP  Rate Limit     : 25 packets/sec
PSP Action          : Packet Drop


DHCP Rate Limit     : 0 packets/sec
```

```
PSP Action          : Packet Drop


IGMP Rate Limit     : 25 packets/sec
PSP Action          : Packet Drop
```

Finally after 60 seconds expires interfaces recover:

```
CAT4#
Mar 19 13:49:57.531: %PM-4-ERR_RECOVER_VP: Attempting to recover from psp err-
disable state on Gi1/0/15, vlan 33.
Mar 19 13:49:57.531: %PM-4-ERR_RECOVER_VP: Attempting to recover from psp err-
disable state on Gi1/0/15, vlan 117.
Mar 19 13:49:57.531: %PM-4-ERR_RECOVER_VP: Attempting to recover from psp err-
disable state on Gi1/0/23, vlan 33.
Mar 19 13:49:57.548: %PM-4-ERR_RECOVER_VP: Attempting to recover from psp err-
disable state on Gi1/0/17, vlan 33.
```

Task 14: Spanning-Tree Attacks

- Prevent STP Root attack on CAT4
- If a Superior BPDU is received on G1/0/23 or G1/0/24 the port should be put into Root-Inconsistent state
- Make sure devices connected to PortFast-enabled ports on CAT3 cannot affect STP
- Enable BPDU Guard to accomplish this
- On CAT2 port connected to R10 should be put into err-disabled state if a BPDU is detected

CAT4

```
int range g1/0/23 – 24
 spanning-tree guard root
```

CAT3

```
spanning-tree portfast bpduguard default
```

CAT2

```
int f0/10
 spanning-tree bpduguard enable
```

The standard STP does not provide any means for network engineers to securely enforce the topology of a switched Layer 2 network. Of course root bridge priority can be set to 0 but such configuration, does not protect against another bridge with a priority of 0 and a lower MAC address. And that's the exact reason why the Root Guard feature has been created.

Root Guard places the interface into the Root-Inconsistent state, which corresponds to the STP listening phase, but only if Superior BPDU is received (with a lower Bridge ID). Other BPDUs have no effect on this feature.

Root-Inconsistent essentially means that interface is blocked, so no traffic is forwarded across such interface. Also note Root-Inconsistent port will remain in this state as long as Superior BPDUs are detected - if they cease, the port will move back into the STP forwarding state.

BPDU Guard, is used to ensure that STP domain is terminated at some point in the network. As a result, the devices behind the ports that have this feature enabled are not able to influence the STP topology.

There are two ways we can enable this feature – either globally or per-interface level. Enabled globally BPDU Guard works only on PortFast enabled ports, and when we enable it on the interface it works only for this interface regardless if it is a PortFast interface or not.

IPv6 Considerations

Does not apply.

Verification

Root Guard was enabled on G1/0/23 and G1/0/24:

```
CAT4#sh spanning-tree vlan 857 interface g1/0/23 de
 Port 23 (GigabitEthernet1/0/23) of VLAN0857 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.23.
   Designated root has priority 33625, address 0007.7dbc.c680
   Designated bridge has priority 33625, address 0007.7dbc.c680
   Designated port id is 128.23, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 225733, received 1
```

Configure CAT3 to be more preferred Bridge for VLAN 857 and observe CAT4:

```
CAT3(config)#spanning-tree vlan 857 priority 4096

CAT4#
Mar 19 22:35:54.140: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port
GigabitEthernet1/0/23 on VLAN0857.


CAT4#sh span vlan 1-4094 inconsistentports
```

```
Name                 Interface                Inconsistency
-------------------- ------------------------ ------------------
VLAN0857             GigabitEthernet1/0/23    Root Inconsistent
VLAN0857             GigabitEthernet1/0/24    Root Inconsistent

CAT4#sh span vlan 857 int g1/0/23 det
 Port 23 (GigabitEthernet1/0/23) of VLAN0857 is broken  (Root Inconsistent)
   Port path cost 4, Port priority 128, Port Identifier 128.23.
   Designated root has priority 4953, address c464.13d1.c580
   Designated bridge has priority 33625, address 0007.7dbc.c680
   Designated port id is 128.23, designated path cost 38
   Timers: message age 1, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 225840, received 37
```

BPDU Guard was enabled globally on CAT3 so on all PortFast interfaces:

```
CAT3(config)#do sh span int g1/0/1 portfast
VLAN0100            enabled

CAT3(config)#do sh span int g1/0/1 det
 Port 1 (GigabitEthernet1/0/1) of VLAN0100 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32868, address 0007.7dbc.c680
   Designated bridge has priority 32868, address c464.13d1.c580
   Designated port id is 128.1, designated path cost 4
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled by default
   BPDU: sent 2201200, received 0
```

On CAT2 the same feature is turned on F0/10. No BPDUs received as of right now:

```
CAT2(config-if)#do sh span int f0/10 det
 Port 12 (FastEthernet0/10) of VLAN0102 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.12.
   Designated root has priority 32870, address 0007.7dbc.c680
   Designated bridge has priority 32870, address 001b.d4c1.5400
   Designated port id is 128.12, designated path cost 19
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
```

```
   Bpdu guard is enabled
   BPDU: sent 225953, received 0
```

We will now configure R10's G0/0 to start participating in STP – this way it will start sending BPDUs:

```
R10(config)#bridge 10 protocol ieee
R10(config)#int g0/0
R10(config-if)#bridge-group 10

CAT2#
Mar 19 22:53:00.731: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/10 with
BPDU Guard enabled. Disabling port.

Mar 19 22:53:00.731: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/10, putting
Fa0/10 in err-disable state

Mar 19 22:53:01.788: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/10, changed state to down

Mar 19 22:53:02.786: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to
down

CAT2#sh int status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Fa0/10                       err-disabled bpduguard
```

Task 15: DHCP Attacks & First Hop Security

- There will be a DHCP server put into use on the network connected to CAT1's port F0/13
- The DHCP server will hand out IPv4 addresses to VLAN 857 clients
- Configure the switch to protect against DHCP Starvation and Rouge Server attacks
- Rate-limit the potential client ports to only allow 6 DHCP packets per second
- Make sure frames with spoofed MAC addresses will be dropped in DHCP Requests
- R11's G1/0/11 will be configured with DHCPv6 services in the future
- Configure one of the First Hop Security features to protect DHCP communication in VLAN 115
- DHCP Server packets should be only allowed to come from R11's IPv6 address
- Enable IPv6 Snooping for VLAN 115

CAT1

```
ip dhcp snooping
ip dhcp snooping vlan 857
ip dhcp snoping verify mac-address

int f0/13
 ip dhcp snooping trust
```

```
int f0/5
 ip dhcp snooping limit rate 6

int f0/7
 ip dhcp snooping limit rate 6

int f0/8
 ip dhcp snooping limit rate 6
```

R11

```
int g0/1
 ipv6 address FE80::11 link-local
```

CAT3

```
ipv6 access-list DSERVER
 sequence 20 permit ipv6 host FE80::11 any

ipv6 dhcp guard policy TRUSTED_SERVER
 device-role server
 match server access-list DSERVER

vlan configuration 115
 ipv6 dhcp guard
 ipv6 snooping

int g1/0/10
 ipv6 dhcp guard

int g1/0/11
 ipv6 dhcp guard attach-policy TRUSTED_SERVER vlan 115
```

DHCP Snooping is a security feature for DHCP that lets you filter untrusted DHCP messages. DHCP Snooping builds and maintains a DHCP snooping binding table. An untrusted DHCP message is one that is seen on a port that is not trusted.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is not configured as trusted (all by default). A trusted interface is an interface that is configured as trusted (ip dhcp snooping trust). This table, as we will see in the next task, will be used as a source of information for other L2 security features – DAI and IP Source Guard.

One caveat when using DHCP Snooping is that it enables insertion of Option 82 to all DHCP Discovery packets received on the protected VLAN. And this make cause problems with allocation of addresses on

certain DHCP Servers because option 82 is a relay Option and it is only supposed to be used with relays when Relay address is also specified.

IOS DHCP Server is one of the examples here – it will not assign an IP address to the client if the switch inserted Option 82 so you may want to disable it by using `no ip dhcp snooping information option`. This would be required if you want to test DHCP Snooping by configuring one of the routers as a DHCP Server.

By using the `ip dhcp snooping verify mac` command the switch will verify that the MAC address is not begin spoofed in the DHCP packets.

IPv6 Considerations

First Hop Security is a suite of features designed specifically to harden IPv6 link operation, as well as help with scale in large L2 domains. The base set of functionality provides solid protection from a wide host of rogue or mis-configured users, and this can be extended with additional features for different deployment scenarios, or attack vectors.

The functions available under First Hop Security (FHS) are also called as IPv6 policies. These Policies can be applied at the interface or VLAN level, depending on how "broad" control want to enable.

One of the more important components of FHS is IPv6 Snooping. This feature, once activated, makes the switch start looking at various traffic (Neighbor Discovery, DHCPv6 and possibly also data packets), depending on the configuration. The information obtained by this inspection is then parsed to create a so-called Binding Table, which in turn is then used by some other FHS features, such as Neighbor Discovery Inspection (to validate the link-layer address), per-port address limit (to validate the IPv4 or IPv6 addresses), Source Guard (to prevent spoofing) and IPv6 Device Tracking (to prefix binding of the neighbors to prevent spoofing and redirect attacks).

Other FHS features include DHCP Guard, which prevents Rouge Servers (ipv6 dhcp guard policy), and Router Advertisement (RA) Guard that blocks or rejects unwanted/rogue RA messages (`ipv6 nd raguard`).

Whenever you work with FHS it maybe be useful to enable Snooping Logging feature to see what traffic is dropped (`ipv6 snooping logging packet drop`). Also a group of debugs (`debug ipv6 snooping [options]`) can be useful in any troubleshooting related to First Hop Security.

The solution enables DHCP Guard explicitly on G1/0/10 ("default" meaning Client role) – this would not be required assuming that this port is part of VLAN 115 (because we have already enabled the "default" policy for the entire VLAN). This is just to show you that untrusted/client roles can be enabled on

individual interfaces as well. To enable FHS features for the entire VLAN (which makes more sense for most of them) enter the VLAN configuration (`vlan configuration`) and use a feature-specific command.

Verification

R5, R7 and R8 are the only devices connected to VLAN 857. Once the feature is enabled for that VLAN, we can test:

```
CAT1(config)#do sh vlan br | In 857
857  VLAN0857                         active    Fa0/5, Fa0/7, Fa0/8

CAT2(config)#do sh vlan br | In 857
857  VLAN0857                         active

CAT3(config)#do sh vlan br | In 857
857  VLAN0857                         active

CAT4(config)#do sh vlan br | In 857
857  VLAN0857                         active

CAT1#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
857
DHCP snooping is operational on following VLANs:
857
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/5              no          6
FastEthernet0/7              no          6
FastEthernet0/8              no          6
FastEthernet0/13             yes         unlimited
```

Let's temporarily configure R5 as a DHCP Server; R7 will act as a client:

```
R5(config)#ip dhcp pool DHPOOL
R5(dhcp-config)#network 10.8.57.0 /24
```

```
R7(config)#int f0/0
R7(config-if)#ip add dhcp

Mar 20 16:22:21.700: DHCP_SNOOPING: received new DHCP packet from input interface
(FastEthernet0/7)
Mar 20 16:22:21.700: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER, input interface: Fa0/7, MAC d
CAT1#a: ffff.ffff.ffff, MAC sa: 001b.d517.ba88, IP da: 255.255.255.255, IP sa:
0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP
giaddr: 0.0.0.0, DHCP chaddr: 001b.d517.ba88
Mar 20 16:22:21.700: DHCP_SNOOPING: add relay information option.
Mar 20 16:22:21.700: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port format
Mar 20 16:22:21.700: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format
Mar 20 16:22:21.700: DHCP_SNOOPING: binary dump of relay info option, length: 20
CAT1# data:
0x52 0x12 0x1 0x6 0x0 0x4 0x3 0x59 0x1 0x9 0x2 0x8 0x0 0x6 0x0 0x1B 0xD4 0xC8 0xA
0x80
Mar 20 16:22:21.700: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (857)
```

Note R5 does not get any DHCP messages because CAT1 F0/5 is not a trusted port. With DHCP Snooping enabled DISCOVERY packets will be only flooded to trusted ports (and here F0/13 is down). If you were to set F0/5 as trusted, you would see the packet got forwarded:

```
Mar 20 16:30:48.599: DHCP_SNOOPING_SW: bridge packet send packet to port:
FastEthernet0/5, vlan 857.
```

For IPv6 DHCP Guard, we first want to see if feature is enabled and correctly applied:

```
CAT3#sh ipv snooping features
Feature name   priority state
DHCP Guard        200   READY

CAT3#sh ipv dhcp guard pol
Dhcp guard policy: TRUSTED_SERVER
        Device Role: dhcp server
        Target: Gi1/0/11
        Max Preference: 255
        Min Preference: 0
        Source Address Match Access List: DSERVER

Dhcp guard policy: default
        Device Role: dhcp client
        Target: Gi1/0/10 vlan 115
```

Let's now configure DHCPv6 Server on R11 to test. This is before a link-local address was modified to match our ACL:

```
R11(config)#ipv6 dhcp pool DPOOL
R11(config-dhcpv6)# address prefix 2010:0:115:1::/64
R11(config-dhcpv6)#int g0/1
R11(config-if)# ipv6 dhcp server DPOOL


CAT3#debug ipv6 snooping dhcp-guard

CAT3#
Mar 20 12:45:35.837: SISF[DHG]: Gi1/0/11 vlan 115 DHCP Guard setting sec level to
GUARD
Mar 20 12:45:35.837: SISF[DHG]: Gi1/0/11 vlan 115 DHCP Server Advertise Msg dropped
due to invalid source FE80::CA4C:75FF:FE1F:DDC1
```

When we change the ACL to include the correct IPv6 address, DHCP Guard allows the packets coming from the server:

```
CAT3#
Mar 20 12:47:44.958: SISF[DHG]: Gi1/0/11 vlan 115 DHCP Guard setting sec level to
GUARD
Mar 20 12:47:44.958: SISF[DHG]: Gi1/0/11 vlan 115 DHCP Server message for role dhcp
server - Permit
```

One more thing we want to test is DHCPv6 Rouge server – configure R10 for DHCPv6 and try to obtain an IPv6 address from e.g. CAT4:

```
CAT3#
Mar 20 13:26:19.527: SISF[DHG]: Gi1/0/23 vlan 115 DHCP Guard setting sec level to
GUARD
Mar 20 13:26:19.527: SISF[DHG]: Gi1/0/23 vlan 115 DHCP Client message for role dhcp
client - Permit
Mar 20 13:26:19.535: SISF[DHG]: Gi1/0/10 vlan 115 DHCP Guard setting sec level to
GUARD
Mar 20 13:26:19.535: SISF[DHG]: Gi1/0/10 vlan 115 DHCP Server message for role dhcp
client - Deny
```

Finally let's take a look at the Snooping Binding table. We should see an entry for a DHCP-assigned IPv6 address and few entries obtained from Neighbor Discovery packets:

```
CAT3#sh ipv neighbors binding
Binding Table has 6 entries, 4 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
```

```
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address                              Link-Layer addr Interface vlan prlvl
age   state    Time left
L   FE80::C664:13FF:FED1:C5C4                 C464.13D1.C5C4  Vl1116      116  0100
14mn REACHABLE
ND  FE80::32E4:DBFF:FECE:8491                 30E4.DBCE.8491  Gi1/0/10    115  0005
12mn STALE      88472 s
ND  FE80::207:7DFF:FEBC:C6C9                  0007.7DBC.C6C9  Gi1/0/23    115  0005
12mn STALE      86468 s
ND  FE80::11                                  C84C.751F.DDC1  Gi1/0/11    115  0005
12mn STALE      86769 s
L   2150:50:116::133                          C464.13D1.C5C4  Vl1116      116  0100
14mn REACHABLE
DH  2010:0:115:1:208F:6E04:2FEF:DE8D          0007.7DBC.C6C9  Gi1/0/23    115  0024
12mn STALE      167572 s
```

Task 16: ARP & L2 Spoofing Attacks

- Prevent ARP MiTM attacks in VLAN 857
- Routers R5, R7 and R8 should be still able to successfully communicate
- ARP packets generated by those devices should be logged
- Also enable source and destination MAC address validation
- Prevent L2 & L3 IPv4 spoofing attacks on port F0/8 on CAT1
- You are not allowed to modify the DHCP Snooping database in this task
- CAT3 should be configured to protect against spoofed IPv6 packets on its L2 ports
- Configure Source Guard on G1/0/10 and G1/0/11 interfaces

Detailed Solution

CAT1

```
arp access-list ARP_ACL
 permit ip host 10.8.57.5 mac host 001b.d50f.f2f8 log
 permit ip host 10.8.57.7 mac host 001b.d517.ba88 log
 permit ip host 10.8.57.8 mac host 001b.d4ef.e728 log

ip arp inspection vlan 857
ip arp inspection vlan 857 logging acl-match matchlog
ip arp inspection validate src-mac dst-mac
ip arp inspection filter ARP_ACL vlan  857

int f0/8
 switchport port-security
 ip verify source port-security

ip source binding 001B.D4EF.E728 vlan 857 10.8.57.8 interface Fa0/8
```

CAT3

```
vlan configuration 115
 ipv6 snooping

ipv6 source-guard policy SGUARD

int g1/0/10
 ipv6 source-guard attach-policy SGUARD

int g1/0/11
 ipv6 source-guard attach-policy SGUARD
```

There are several attacks that target the IP-to-MAC resolution. Dynamic Arp inspection (DAI) validates ARP packets and determines their validity by performing an IP-to-MAC address binding inspection against entries stored in a trusted database - the DHCP snooping binding database that was created in previous task. If the packets can be verified, they are forwarded; otherwise ARP packet is dropped. This means that the DHCP snooping binding database must be built before DAI works.

For non-DHCP environments or just to make some exceptions for statically-numbered hosts ARP ACLs can be used to add exceptions. It is also possible to add entries to the DHCP Snooping table to get this work, but we are prohibited from doing this in this task.

When you enable IPv4 Source Guard feature on an interface, you are telling the port that you don't want to pass traffic if the source address doesn't match the IP-to-MAC binding table created by DHCP snooping or by a manually created binding. With "`port-security`" added to the command you are also enabling validation of MAC address (L2). For this function to work, however, Port Security must be also enabled on the interface.

One caveat for this feature, when L2 validation is turned on, is that the switch must insert Option 82 to the DISCOVERY packet to properly track DHCP communication. This is because the host MAC address is not learned until the host is granted a lease – and to forward packets from the server to the host DHCP snooping uses Option-82 data to identify the host port.
In the newer IOSs there is also an option to enable IPv4 Source Guard to send the content of dropped packets to the NetFlow Collector. Use "`ip verify source smartlog`" to implement this.

IPv6 Considerations

The IPv6 Source Guard (part of the First Hop Security feature set) works similarly to its IPv4 counterpart - it provides the ability to use the IPv6 Binding Table to install PACLs to prevent a host from sending packets with an invalid IPv6 source address.

In terms of restrictions for using this feature, it can be only enabled on a port via `ipv6 source-guard policy` (you cannot turn it on for the entire VLAN). Also note that Neighbor Discovery or DHCP Snooping must be enabled on the interface to which the Source Guard switchport belongs. Otherwise all data traffic from this port will be blocked.

Two options available in the Source Guard policy we can configure are "`deny global-autoconf`" and "`permit link-local`". The first keyword forces the switch to deny all data traffic from auto or manually configured global addresses. This is useful when all global addresses on a link are DHCP-assigned and the administrator wants to block hosts with self-configured addresses to send traffic. The "`permit link-local`" allows all traffic that is sourced by a link-local address.

Verification

If you did not add static entries for routers R5, R7 and R8 similar messages should show up on CAT1:

```
CAT1#
Mar 20 18:36:16.669: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Res) on Fa0/5,
vlan 857.([001b.d50f.f2f8/10.8.57.5/ffff.ffff.ffff/10.8.57.5/18:36:16 UTC Wed Mar 20
2013])
Mar 20 18:36:16.669: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa0/5,
vlan 857.([001b.d50f.f2f8/10.8.57.5/001b.d4ef.e728/10.8.57.8/18:36:16 UTC Wed Mar 20
2013])
Mar 20 18:36:16.669: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa0/5,
vlan 857.([001b.d50f.f2f8/10.8.57.5/001b.d517.ba88/10.8.57.7/18:36:16 UTC Wed
```

After entries were added you should see log entries for allowed packets:

```
CAT1(config)#
Mar 20 18:43:36.073: %SW_DAI-6-ACL_PERMIT: 1 ARPs (Res) on Fa0/5, vlan
857.([001b.d50f.f2f8/10.8.57.5/ffff.ffff.ffff/10.8.57.5/18:43:35 UTC Wed Mar 20
2013])
Mar 20 18:43:36.073: %SW_DAI-6-ACL_PERMIT: 1 ARPs (Req) on Fa0/5, vlan
857.([001b.d50f.f2f8/10.8.57.5/001b.d517.ba88/10.8.57.7/18:43:35 UTC Wed Mar 20
2013])
Mar 20 18:43:36.073: %SW_DAI-6-ACL_PERMIT: 1 ARPs (Req) on Fa0/5, vlan
857.([001b.d50f.f2f8/10.8.57.5/001b.d4ef.e728/10.8.57.8/18:43:35 UTC Wed Mar 20
2013])

CAT1#sh ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

```
 Vlan      Configuration     Operation    ACL Match          Static ACL
 ----      -------------     ---------    ---------          ----------
  857      Enabled           Active       ARP_ACL            No

 Vlan      ACL Logging       DHCP Logging       Probe Logging
 ----      -----------       ------------       -------------
  857      Acl-Match         Deny               Off

 Vlan       Forwarded         Dropped     DHCP Drops      ACL Drops
 ----       ---------         -------     ----------      ---------
  857              66              29             29              0

 Vlan    DHCP Permits     ACL Permits  Probe Permits   Source MAC Failures
 ----    ------------     -----------  -------------   -------------------
  857               0              61              0                     0

 Vlan    Dest MAC Failures    IP Validation Failures    Invalid Protocol Data
 ----    -----------------    ----------------------    ---------------------
  857                    0                        0                       0
```

To verify IPv4 Source Guard feature use the following commands:

```
CAT1#sh ip source binding static
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------
------
00:1B:D4:EF:E7:28   10.8.57.8        infinite    static          857
FastEthernet0/8
Total number of bindings: 1

CAT1(config-if)#do sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/8      ip-mac       active       10.8.57.8        00:1B:D4:EF:E7:28  857
```

You could also try to change the IP or MAC address on R8's F0/0 – then the data traffic will be blocked:

```
CAT1#debug ip verify source packet
Mar 20 18:56:33.403: DHCP_SECURITY_SW: validate port security packet, recv port:
FastEthernet0/8, recv vlan: 857, mac: 1212.1212.1212, invalid flag: 1.
```

Moving on to IPv6 Source Guard. Let's start with looking at the global IPv6 Snooping configuration and Source Guard Policy:

```
CAT3#sh ipv snooping features
Feature name   priority state
DHCP Guard        200   READY
```

```
Snooping           128   READY
Source guard        32   READY

CAT3#sh ipv snooping policies
Target                Type  Policy               Feature        Target range
Gi1/0/10              PORT  SGUARD               Source guard   vlan all
Gi1/0/11              PORT  TRUSTED_SERVER       DHCP Guard     vlan 115
Gi1/0/11              PORT  SGUARD               Source guard   vlan all
vlan 115              VLAN  default              DHCP Guard     vlan all
vlan 115              VLAN  default              Snooping       vlan all

CAT3(config-if)#do sh ipv source-g pol SGUARD
Policy SGUARD configuration:
Policy SGUARD is applied on the following targets:
Target                Type  Policy               Feature        Target range
Gi1/0/10              PORT  SGUARD               Source guard   vlan all
Gi1/0/11              PORT  SGUARD               Source guard   vlan all
```

The Binding Table is populated for both, Link-Local and Global IPv6 addresses of R10 & R11 so everything should be fine:

```
CAT3(config-if-range)#do sh ipv nei bi
Binding Table has 7 entries, 5 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other
Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address                              Link-Layer addr Interface vlan prlvl
age   state    Time left
L   FE80::C664:13FF:FED1:C5C4                 C464.13D1.C5C4  Vl116      116  0100
4mn REACHABLE
ND  FE80::207:7DFF:FEBC:C6C9                 0007.7DBC.C6C9  Gi1/0/23   115  0005
63s  REACHABLE  244 s
ND  FE80::11                                 C84C.751F.DDC1  Gi1/0/11   115  0005
63s  REACHABLE  243 s
ND  FE80::10                                 30E4.DBCE.8491  Gi1/0/10   115  0005
63s  REACHABLE  245 s
L   2150:50:116::133                         C464.13D1.C5C4  Vl116      116  0100
4mn REACHABLE
ND  2010:0:115::11                           C84C.751F.DDC1  Gi1/0/11   115  0005
3mn REACHABLE  93 s
ND  2010:0:115::10                           30E4.DBCE.8491  Gi1/0/10   115  0005
3mn REACHABLE  124 s
```

```
R11(config-if)#do ping 2010:0:115::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:0:115::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Now let's clear the Snooping Table and try to communicate between the devices once again:

```
CAT3#clear ipv neighbors binding

R10(config-if)#do ping 2010:0:115::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:0:115::11, timeout is 2 seconds:
.....
```

Task 17: ND Cache Poisoning Attacks & SEND

- Prevent ND Cache Poisoning attacks in VLAN 102
- Two routers (R2 and R6) should have their IPv6 addresses cryptographically secured
- Addresses used by routing protocol updates should be protected as well
- The highest level of protection against brute-force attacks must be ensured
- All non-SEND messages seen by R2 and R6 devices should be dropped

Detailed Solution

R2

```
cry key gen rsa label CGAKEY modulus 1024

ipv cga modifier rsakeypair CGAKEY sec-level 1

int g0/0
 ipv6 cga rsakeypair CGAKEY
 ipv6 address FE80:: link-local cga
 ipv6 address 2172:6:102::/64 cga

ipv nd secured full-secure
```

R6

```
cry key gen rsa label CGAKEY modulus 1024

ipv cga modifier rsakeypair CGAKEY sec-level 1

int f0/1
 ipv6 cga rsakeypair CGAKEY
 ipv6 address FE80:: link-local cga
 ipv6 address 2172:6:102::/64 cga
```

```
ipv nd secured full-secure
```

SEND configuration starts with generating an RSA Key Pair and then generating a modifier for it so it can be further used for Secure ND. The value you put after sec-level determines how well the modifier will protect CGA against brute-force attacks; 1 is the most secure value.

Next we want to go to an interface and say that this particular Key Pair we want to use it for SEND here. Then we should generate CGAs for at minimum link-local address and probably also for a global one (to protect ND resolution for data traffic).

There is also a command `ipv6 nd secured full-secure` you can issue globally or under interface, that when enabled causes the router to reject non-SEND messages.

Since R10's code does not support SEND, with the above configuration after ND Cache entries expire this router will not be able to communicate with other routers in VLAN 102.

IPv6 Considerations

Secure Neighbor Discovery (SEND), which is an extension to Neighbor Discovery protocol that defines a set of new messages and attributes.

The main component that makes SEND perform its functions is called a Cryptographically Generated Address or CGA in short. With SEND nodes cannot choose their own interface Identifier (or e.g. use EUI-64 format) but instead this part of an IPv6 address is generated based on the IPv6 Prefix and the Public Key of the device.

Note that anyone can actually generate a cryptographic address or CGA (just given a subnet Prefix and their own Public Key) so in addition to the CGA generation each Neighbor Discovery packet is actually extended by few new fields, from which the most important one is the signature.

From the point CGA is generated on when an ND message is to be sent for the address, hash of the message will be signed by the private key of the CGA owner. This way, if the packet was tampered with in transit, the decrypted hash will never match the original one.

More over for situations when an attacker captures/spoofs a message (trying to re-calculate the hash and sign it with its own Private Key) - this is also prevented by SEND by virtue of the Public Key being part of the Interface ID calculations. In other words only the owner of the Public Key is able to calculate an IPv6 address "X".

Few IPv6 attacks that Secure ND can be used to mitigate:

1. NA/NS Spoofing –prevents from poisoning ND Cache on the devices
2. RA Spoofing – SEND can authenticate incoming RA messages if PKI is involved
3. DAD DoS - Neighbor Advertisements sent in response to DAD NS are also validated
4. Reply Attacks – SEND uses nonces and/or timestamps which can prevent that type of attacks

Verification

A quick look at our SEND configuration on R2:

```
R2#sh ipv cga modifier-db
D77C:C082:7F7E:2CDA:113C:4FD8:138F:5C17
        label:          CGAKEY
        sec level:      1
        Addresses:
                2172:6:102:0:2CB6:4D5A:823:74AC
                FE80::381F:84B1:1360:D804

R2#sh ipv cga address-db
2172:6:102::/64 ::2CB6:4D5A:823:74AC - table 0x0
        interface:      GigabitEthernet0/0 (2)
        modifier:       CGAKEY
        collisions:     0
FE80::/64 ::381F:84B1:1360:D804 - table 0x12000002
        interface:      GigabitEthernet0/0 (2)
        modifier:       CGAKEY
        collisions:     0
```

To test SEND we will initially not configure it on R6. Clear ND cache and try to talk to R6:

```
R2#clear ipv neighbors
R2#ping 2172:6:102::6 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 2172:6:102::6, timeout is 2 seconds:
```

ND Solicitation was sent to learn MAC of R6:

```
*Mar 20 22:11:34.690: SEND: Send: ND_NEIGHBOR_SOLICIT
*Mar 20 22:11:34.690: SEND:      src 2172:6:102:0:2CB6:4D5A:823:74AC
*Mar 20 22:11:34.690: SEND:      dst FF02::1:FF00:6
*Mar 20 22:11:34.690: SEND:      CGA 2172:6:102:0:2CB6:4D5A:823:74AC, 0x0 : found
*Mar 20 22:11:34.690: SEND:     Timestamp: 0x514A3416B0DC = 22:11:34 UTC Mar 20 2013
*Mar 20 22:11:34.690: SEND:     Nonce length: 6, value: B3F9874A3D25
*Mar 20 22:11:34.718: SEND:              option 1 len 8: ND_OPT_SOURCE_LINKADDR
*Mar 20 22:11:34.718: SEND:              option 11 len 192: ND_OPT_CGA
*Mar 20 22:11:34.718: SEND:              option 13 len 16: ND_OPT_TIMESTAMP
*Mar 20 22:11:34.718: SEND:              option 14 len 8: ND_OPT_NONCE
```

```
*Mar 20 22:11:34.718: SEND:              option 12 len 152: ND_OPT_RSA
```

We see R6 replies with ND Advertisement but since this message is not SEND-secured, R2 drops it:

```
*Mar 20 22:11:34.722: SEND: Receive:  ND_NEIGHBOR_ADVERT
*Mar 20 22:11:34.722: SEND:      src 2172:6:102::6
*Mar 20 22:11:34.722: SEND:      dst 2172:6:102:0:2CB6:4D5A:823:74AC
*Mar 20 22:11:34.722: SEND:      Received at: 0x514A3416B964 = 22:11:34 UTC Mar 20
2013
*Mar 20 22:11:34.722: SEND:              option 2 len 8: ND_OPT_TARGET_LINKADDR
*Mar 20 22:11:34.722: SEND:      Target: 2172:6:102::6
*Mar 20 22:11:34.722: SEND: !NA without CGA option
*Mar 20 22:11:34.722: SEND: Unsecure message discarded
*Mar 20 22:11:34.722: SEND: ! DROP:  ND_NEIGHBOR_ADVERT  src 2172:6:102::6 dst
2172:6:102:0:2CB6:4D5A:823:74AC reason=2


R2#sh ipv nd secured counters int g0/0
Received ND messages on GigabitEthernet0/0:
        rcvd    accept  SLLA    TLLA    PREFIX  MTU     CGA     RSA     TS
NONCE
RA      26      1       23      0       22      23      12      12      12      0
NS      58      4       58      0       0       0       2       2       2       2
NA      97      7       0       96      0       0       7       7       7       3

Dropped ND messages on GigabitEthernet0/0:
Codes   NO_CGA : Required CGA option missing in msg
        TIMEOUT: Timed out while waiting for rsp

        drop    NO_CGA  TIMEOUT
RA      25      13      12
NS      54      54      0
NA      90      90      0

Sent ND messages on GigabitEthernet0/0:
        sent    aborted SLLA    TLLA    PREFIX  MTU     CGA     RSA     TS
NONCE
RA      11      0       10      0       9       10      10      10      10      0
NS      93      0       90      0       0       0       92      92      92      92
NA      7       0       0       5       0       0       6       6       6       2
```

We will now configure R6 with CGA addresses and see what happens:

```
R6#sh ipv int f0/1 | in unicast|subnet
  Global unicast address(es):
    2172:6:102:0:3C04:99AC:EE9:B15E, subnet is 2172:6:102::/64

R2#ping 2172:6:102:0:3C04:99AC:EE9:B15E rep 1
```

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 2172:6:102:0:3C04:99AC:EE9:B15E, timeout is 2
seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 128/128/128 ms
```

NS is sent to the node-solicited multicast address to ask for corresponding MAC:

```
*Mar 20 22:22:35.222: SEND: Send: ND_NEIGHBOR_SOLICIT
*Mar 20 22:22:35.222: SEND:      src 2172:6:102:0:2CB6:4D5A:823:74AC
*Mar 20 22:22:35.222: SEND:      dst FF02::1:FFE9:B15E
*Mar 20 22:22:35.222: SEND:      CGA 2172:6:102:0:2CB6:4D5A:823:74AC, 0x0 : found
*Mar 20 22:22:35.222: SEND:     Timestamp: 0x514A36AB390A = 22:22:35 UTC Mar 20 2013
*Mar 20 22:22:35.222: SEND:     Nonce length: 6, value: 81B4FB23EBA5
*Mar 20 22:22:35.250: SEND:              option 1 len 8: ND_OPT_SOURCE_LINKADDR
*Mar 20 22:22:35.250: SEND:              option 11 len 192: ND_OPT_CGA
*Mar 20 22:22:35.250: SEND:              option 13 len 16: ND_OPT_TIMESTAMP
*Mar 20 22:22:35.250: SEND:              option 14 len 8: ND_OPT_NONCE
*Mar 20 22:22:35.254: SEND:              option 12 len 152: ND_OPT_RSA

*Mar 20 22:22:35.342: SEND: Receive:  ND_NEIGHBOR_ADVERT
*Mar 20 22:22:35.342: SEND:      src 2172:6:102:0:3C04:99AC:EE9:B15E
*Mar 20 22:22:35.342: SEND:      dst 2172:6:102:0:2CB6:4D5A:823:74AC
*Mar 20 22:22:35.342: SEND:      Received at: 0x514A36AB5874 = 22:22:35 UTC Mar 20
2013
*Mar 20 22:22:35.342: SEND:              option 2 len 8: ND_OPT_TARGET_LINKADDR
*Mar 20 22:22:35.342: SEND:              option 11 len 192: ND_OPT_CGA
*Mar 20 22:22:35.342: SEND:              option 13 len 16: ND_OPT_TIMESTAMP
*Mar 20 22:22:35.342: SEND:              option 14 len 8: ND_OPT_NONCE
*Mar 20 22:22:35.342: SEND:              option 12 len 152: ND_OPT_RSA
*Mar 20 22:22:35.342: SEND:      Target: 2172:6:102:0:3C04:99AC:EE9:B15E
*Mar 20 22:22:35.342: SEND: Solicit advertisement
*Mar 20 22:22:35.342: SEND:     Verifying address 2172:6:102:0:3C04:99AC:EE9:B15E
*Mar 20 22:22:35.342: SEND:      sec is 1
*Mar 20 22:22:35.342: SEND:      keylen is 1024
*Mar 20 22:22:35.342: SEND:      Address verified
*Mar 20 22:22:35.342: SEND:     Nonce length: 6, value: 81B4FB23EBA5
*Mar 20 22:22:35.342: SEND:     Timestamp: 0x514A362FF166 = 22:20:31 UTC Mar 20 2013
*Mar 20 22:22:35.346: SEND:     Good signature

R2#sh ipv neighbors g0/0
IPv6 Address                              Age Link-layer Addr State Interface
FE80::3C4A:F494:79BE:3DAB                   7 001b.d518.4159  STALE Gi0/0
2172:6:102:0:3C04:99AC:EE9:B15E             7 001b.d518.4159  STALE Gi0/0
FE80::32E4:DBFF:FECE:8490                  10 30e4.dbce.8490  STALE Gi0/0

R2#sh ipv nd secured timestamp-db
Total number of entries: 2
Number of unreached peer entries: 0 / 1024
```

```
FE80::3C4A:F494:79BE:3DAB on GigabitEthernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 57m 34s (reached)
        TSlast: 0x514A36C6BB1E = 22:23:02 UTC Mar 20 2013
        RDlast: 0x514A37422237 = 22:25:06 UTC Mar 20 2013
2172:6:102:0:3C04:99AC:EE9:B15E on GigabitEthernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 55m 3s (reached)
        TSlast: 0x514A362FF166 = 22:20:31 UTC Mar 20 2013
        RDlast: 0x514A36AB5874 = 22:22:35 UTC Mar 20 2013


R6#sh ipv cga address-db
2172:6:102::/64 ::3C04:99AC:EE9:B15E - table 0x0
        interface:      FastEthernet0/1 (4)
        modifier:       CGAKEY
        collisions:     0
FE80::/64 ::3C4A:F494:79BE:3DAB - table 0x12000004
        interface:      FastEthernet0/1 (4)
        modifier:       CGAKEY
        collisions:     0
```

Since OSPF database synchronization cannot be completed between the routers, adjacency will stuck in the EXCHANGE state:

```
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.10.10.10       1   EXCHANGE/DROTHER00:00:38    3               GigabitEthernet0/0
6.6.6.6           1   FULL/BDR        00:00:34    4               GigabitEthernet0/0

R2#sh ipv ne
IPv6 Address                             Age Link-layer Addr State Interface
FE80::3C4A:F494:79BE:3DAB                  0 001b.d518.4159  REACH Gi0/0
FE80::10                                   0 -               INCMP Gi0/0
```