ipexpert

IPexpert's Lab Preparation Workbook

for the Cisco® CCIE™ Security Volume 2

Complete DSG Labs 1-3

LAB 1

Please look at the provided diagrams and read through the whole lab before you start. Read the directions very carefully to make sure you are doing what is being asked of you. This concept is very important when you take the CCIE lab administered by Cisco

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

- 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

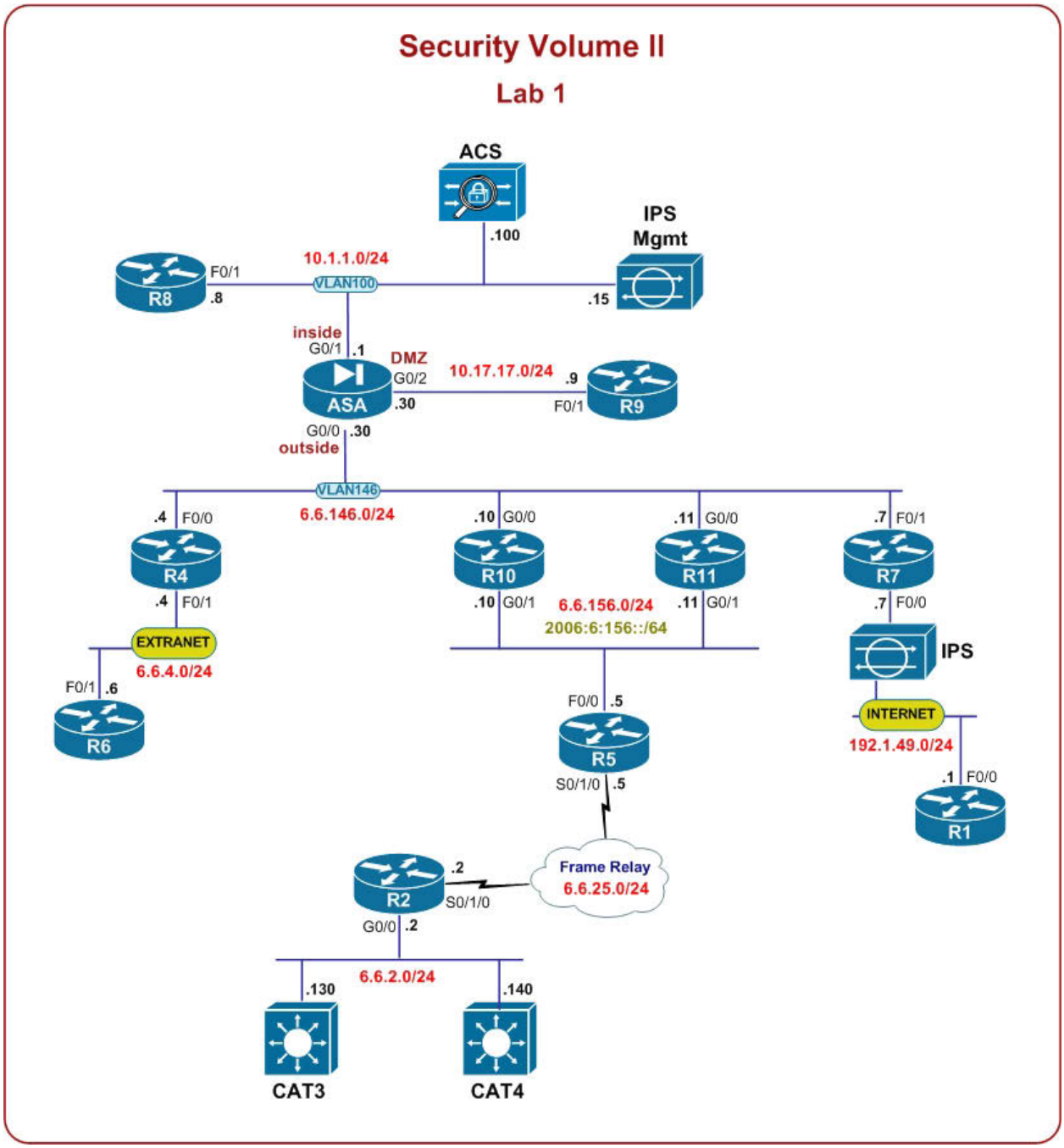
NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device

Estimated Time to Complete: **8-10 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	F0/1	49	192.1.49.1/24
	Loop0		6.6.99.1/32
R2	G0/0	2	6.6.2.2/24
	S0/1/0		6.6.25.2/24
	Loop0		6.6.99.2/32
R4	F0/0	146	6.6.146.4/24
	F0/1	4	6.6.4.4/24
	Loop0	160	6.6.99.4/32
R5	F0/0	156	6.6.156. 5/24
			2006:6:156::5/64
	S0/1/0		6.6.25.5/24
	Loop0		6.6.99.5/32
R6	F0/1	4	6.6.4.6/24
	Loop0		6.6.99.6/32
R7	F0/0	49	192.1.49.7/24
	F0/1	146	6.6.146.7/24
	Loop0		6.6.99.7/32
R8	F0/1	100	10.1.1.8/24
	Loop0		6.6.99.8/32
R9	F0/1	17	10.17.17.9/24
	Loop0		6.6.99.9/32
R10	G0/0	146	6.6.146.10/24
	G0/1	156	6.6.156.10/24
			2006:6:156::10/64
	Loop0		6.6.99.10/32
R11	G0/0	146	6.6.146.11/24
	G0/1	156	6.6.156.11/24
			2006:6:156::11/64
	Loop0		6.6.99.11/32
CAT3	VLAN2	2	6.6.2.130/24
CAT4	VLAN2	2	6.6.2.140/24
ASA	G0/0	146	6.6.146.30/24
	G0/1	100	10.1.1.1/24
	G0/2	17	10.17.17.30/24
ACS		100	10.1.1.100/24
IPS	Mgmt	100	10.1.1.15/24



Solutions

1.0 ASA Firewalls (20 points)

Task 1.1: ASA Setup (4 Points)

- Configure ASA interfaces according to the IP Addressing table and diagram
- Configure the host name to be ASA
- Configure ASA3 and ASA4 to backup each other. ASA3 should be the primary
- Use Gig0/3 for the backup communication. Make sure failover replication and state replication doesn't share the same broadcast domain. Make sure the HTTP states are replicated. Failure detection should occur in one second
- The communication between the failover pair should be encrypted

Detailed Solution

ASA3

```
hostname ASA
!
interface G0/0
 nameif outside
 sec 0
 ip address 6.6.146.30 255.255.255.0 standby 6.6.146.31
 no shutdown

interface G0/1
 nameif inside
 sec 100
 ip address 10.1.1.1 255.255.255.0 standby 10.1.1.31
 no shutdown

int g0/2
 nameif DMZ
 security-level 50
 ip address 10.17.17.30 255.255.255.0 standby 10.17.17.31
 no shutdown
```

```
interface G0/3
 no shutdown

interface G0/3.98
 vlan 98

interface G0/3.99
 vlan 99

failover lan unit primary
failover lan interface FAILOVER G0/3.98
failover int ip FAILOVER 10.98.98.30 255.255.255.0 standby 10.98.98.31
failover link STATE G0/3.99
failover int ip STATE 10.99.99.30 255.255.255.0 standby 10.99.99.31
failover replication http
failover key cisco
!
failover polltime msec 300 holdtime 1
!
failover
```

ASA4

```
interface G0/3
 no shutdown
!
interface G0/3.98
 vlan 98
!
interface G0/3.99
 vlan 99
!
failover lan unit secondary
failover lan interface FAILOVER G0/3.98
failover key cisco
failover int ip FAILOVER 10.98.98.30 255.255.255.0 standby 10.98.98.31
failover
```

CAT3

```
interface GigabitEthernet1/0/22
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 98,99
 switchport mode trunk
```

CAT4

```
vlan 98,99

interface GigabitEthernet1/0/22
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 98,99
 switchport mode trunk
```

Configuring IPs and basic failover should be almost second nature for you at this point. In most scenarios, the failover and link state interfaces share the same IP. For us to separate them here into separate broadcast domains means they will be running on separate interfaces. So we needed to configure two subnets (and two VLANs – choose arbitrary numbers that are unused if they don't tell you them).

Without a encryption key failover, information is shared unencrypted between peers. By configuring the key failover, replication is encrypted.

And to make sure a failure is detected in one second, we need to decrease the poll interval to less than one second. Here we choose 300 msec as 3 missed hellos (900 msec), which should cause a failover to occur.

Verification

```
ASA(config)# sh failover interface
        interface FAILOVER GigabitEthernet0/3.98
                System IP Address: 10.98.98.30 255.255.255.0
                My IP Address    : 10.98.98.30
                Other IP Address : 10.98.98.31
        interface STATE GigabitEthernet0/3.99
                System IP Address: 10.99.99.30 255.255.255.0
                My IP Address    : 10.99.99.30
                Other IP Address : 10.99.99.31
```

```
ASA(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FAILOVER GigabitEthernet0/3.98 (up)
Unit Poll frequency 300 milliseconds, holdtime 1 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
failover replication http
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 20:21:20 UTC May 9 2013
        This host: Primary - Active
                Active time: 121 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface outside (6.6.146.30): Normal (Monitored)
                  Interface inside (10.1.1.1): Normal (Monitored)
                  Interface DMZ (10.17.17.30): 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: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                  Interface outside (6.6.146.31): Normal (Monitored)
                  Interface inside (10.1.1.31): Normal (Monitored)
                  Interface DMZ (10.17.17.31): 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 : STATE GigabitEthernet0/3.99 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         17         0          15         0
        sys cmd         15         0          15         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         1          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    0           0           0           0
User-Identity    1           0           0           0

Logical Update Queue Information
                 Cur     Max     Total
Recv Q:          0       6       406
Xmit Q:          0       30      181
```

Task 1.2: Source Protection (4 Points)

- The hosts on the inside interface should be seen on the outside as 6.6.146.199
- The ACS should be seen on the outside as 6.6.146.100, R8 should be seen as 6.6.146.8 and the R9 should be seen as 6.6.146.9
- Internal device with an IP address 10.1.1.80 should be reachable from the outside via 6.6.146.80 but when it initiates connection on its own it should match the PAT rule.
- This translation should go to Section 1 NAT Rules
- Make sure there are no more than 100 concurrent TCP sessions to the ACS

Detailed Solution

ASA3

```
object network PAT_POOL
 host 6.6.146.199

object network INSIDE_NET
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic PAT_POOL interface

object network ACS
 host 10.1.1.100
 nat (inside,outside) static 6.6.146.100
```

```
object network R8
 host 10.1.1.8
 nat (inside,outside) static 6.6.146.8

object network R9
 host 10.17.17.9
 nat (DMZ,outside) static 6.6.146.9

object network IP80
 host 10.1.1.80

object network POST_IP80
 host 6.6.146.80

nat (outside,inside) source static any any destination static POST_IP80
IP80 unidirectional

access-list TO_ACS extended permit tcp any host 10.1.1.100

class-map TO_ACS_CLASS
 match access-list TO_ACS

policy-map OUT_POL
 class TO_ACS_CLASS
  set connection conn-max 100

service-policy OUT_POL interface outside
```

Since these ASAs are running the newer code we had to choose to either use Auto or Manual NAT configuration. For basic source translations where no policy is involved Auto NAT is the recommended method because of its simplicity.

Normally static NATs are bidirectional meaning address gets always translated statically no matter what side initiated the connection (for example if you do source inside->outside NAT it also implies you create another XLATE for outside->inside - but for the destination IP) . To change this behavior we can use the “unidirectional” option. It only works with static translations and, as the name implies, only makes the translation for one direction - when packet goes from the Original (PRE) to Translated (POST) interface. So when you do source NAT

inside -> outside only then the source will change; XLATE will not be “visible” to the POST-NAT side. In our case we do outside-> inside but for the destination IP – so on the inside packet goes to 10.1.1.80 and return packets will match this entry; however when .80 initiates connection to the outside it matches another NAT Rule which is PAT in our case.

How would you configure static translations in 8.2 and below? Using the static command. Just remember that addresses on IOS are always LOCAL then Global. On the ASA it is Global then LOCAL. Use a technique to remember the two and it will help you in the test. I like to think of the command as a mirror on the ASA. It begins with the local interface then global. The NAT statements are then global to local. Whatever works for you is what’s important.

What you may not have been familiar with is how to limit ACS to 100 TCP connections. With newer code we can only do that via MPF – and here remember same as with ACLs you refer to the original address (Pre-NAT) when matching traffic, not the translated one.

For any type of NAT configuration done from the command line and also other commands the ASAs have a “help” very similar to UNIX MAN that can aid you with little tidbits (e.g. “help nat”).

Example:

```
ASA(config)# help object

USAGE:

    [no] object network | service <obj_id>
    object network | service <old_obj_id> [rename <new_obj_id>]
    show running-config [all] object
         [network | service | id <obj_id>] [in-line]
    clear configure [all] object [network | service]


DESCRIPTION:

object      Create an object

SYNTAX:

network     Specifies a host, subnet, FQDN or range IP addresses
service     Specifies a protocol and/or port
```

```
<obj_id>    The identifier for the object:
            Must be 1 - 64 characters long, consisting
            of letters, digits and special characters.

rename      Rename the <old_obj_id> to <new_obj_id>

show        Show object(s) running config

in-line     Show the output in one line

clear       Remove existing object(s) config

see also:   object-group
```

Verification

To test this part you will have to play with ACLs and static routes as some devices don't have full IP reachability at this point (e.g. ACS).

```
ASA(config)# sh nat det
Manual NAT Policies (Section 1)
1 (outside) to (inside) source static any any   destination static
POST_IP80 IP80
    translate_hits = 4, untranslate_hits = 4
    Source - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Destination - Origin: 6.6.146.80/32, Translated: 10.1.1.80/32

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R8 6.6.146.8
    translate_hits = 3, untranslate_hits = 2
    Source - Origin: 10.1.1.8/32, Translated: 6.6.146.8/32
2 (inside) to (outside) source static ACS 6.6.146.100
    translate_hits = 3, untranslate_hits = 4
    Source - Origin: 10.1.1.100/32, Translated: 6.6.146.100/32
3 (DMZ) to (outside) source static R9 6.6.146.9
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 10.17.17.9/32, Translated: 6.6.146.9/32
4 (inside) to (outside) source dynamic INSIDE_NET PAT_POOL interface
```

```
    translate_hits = 11, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 6.6.146.199/32,
6.6.146.30/24

R8#telnet 6.6.146.10
Trying 6.6.146.10 ... Open

R10>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:03
*388 vty 0                 idle                 00:00:00 6.6.146.8

  Interface    User               Mode         Idle     Peer Address

pod124acs/admin# telnet 6.6.146.10
Trying 6.6.146.10...
Connected to 6.6.146.10.
Escape character is '^]'.

R10>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:25
 388 vty 0                 idle                 00:00:21 6.6.146.8
*389 vty 1                 idle                 00:00:00 6.6.146.100

  Interface    User               Mode         Idle     Peer Address

R9#telnet 6.6.146.10
Trying 6.6.146.10 ... Open

R10>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:29
*388 vty 0                 idle                 00:00:00 6.6.146.9

  Interface    User               Mode         Idle     Peer Address
```

You can also change an IP address on R8 and see if PAT kicks in as it should:

```
ASA(config)# sh xlate
```

```
4 in use, 4 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
NAT from inside:10.1.1.8 to outside:6.6.146.8
    flags s idle 0:02:46 timeout 0:00:00
NAT from inside:10.1.1.100 to outside:6.6.146.100
    flags s idle 0:02:43 timeout 0:00:00
NAT from DMZ:10.17.17.9 to outside:6.6.146.9
    flags s idle 0:02:03 timeout 0:00:00
TCP PAT from inside:10.1.1.88/33193 to outside:6.6.146.199/31448 flags ri
idle 0:00:11 timeout 0:00:30
```

Unidirectional translation was done for .80 on the inside – change IP on R8 again and test this configuration:

```
R10#telnet 6.6.146.80
Trying 6.6.146.80 ... Open


R8>


R10#sh tcp br
TCB       Local Address               Foreign Address             (state)
31A1F3D8  6.6.146.10.50637            6.6.146.80.23               ESTAB

R8#telnet 6.6.146.10
Trying 6.6.146.10 ... Open
R10>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 6.6.146.80           00:02:56
*388 vty 0                 idle                 00:00:00 6.6.146.199

  Interface    User               Mode         Idle     Peer Address
```

If you were to exceed the configured limit a following syslog would show up:

```
ASA(config-pmap-c)# %ASA-3-201011: Connection limit exceeded 100/100 for
input packet from 6.6.146.4/59232 to 10.1.1.100/23 on interface outside
```

Task 1.3: Traffic Filtering (4 Points)

- Allow the following services to ACS from loopbacks of all routers except R8 :
  - FTP
  - HTTPs
  - Echo Request
  - RADIUS (both RFCs)
  - TACACS+
  - TFTP
- Allow HTTPS and SSHv2 access to R8 from any network
- Allow echo replies to the inside network & DMZ. Only one reply is allowed per single request
- Use as few ACE entries (as few lines) as possible to complete this task
- You can add one static route on the ACS (don't use a default route)

Detailed Solution

ACS

```
ip route 6.6.0.0 255.255.0.0 gateway 10.1.1.1
```

ASA3

```
fixup protocol icmp

object-group service ACS_PORTS
 service-object tcp destination eq ftp
 service-object tcp destination eq https
 service-object tcp destination eq tacacs
 service-object udp destination range radius radius-acct
 service-object udp destination range 1812 1813
 service-object udp destination eq tftp
 service-object icmp echo
object-group service R8_PORTS tcp
 port-object eq https
 port-object eq ssh

object-group network LOOPBACKS
 network-object host 6.6.99.1
 network-object host 6.6.99.2
 network-object host 6.6.99.4
```

```
 network-object host 6.6.99.5
 network-object host 6.6.99.6
 network-object host 6.6.99.7
 network-object host 6.6.99.10
 network-object host 6.6.99.11

access-l OUTSIDE_IN ex pe object-g ACS_PORTS object-g LOOPBACKS ho
10.1.1.100
access-list OUTSIDE_IN ext perm tcp any host 10.1.1.8 object-group
R8_PORTS
access-list DMZ_IN ext perm tcp host 6.6.99.9 host 10.1.1.8 object-g
R8_PORTS

access-group OUTSIDE_IN in interface outside
access-group DMZ_IN in interface DMZ
```

R8

```
ip domain-name ipexpert.com
crypto key generate rsa mod 768
ip ssh version 2

line vty 0 4
 login local

username cisco pass cisco

ip http secure-server
```

Well, the fewest ACE entries possible would have been a “permit any any” on this question. But I have to assume the lab writer was thinking a little more than that ;-). This is a security lab remember – you have to be specific.

We can do all the ports in one ACE via a service object-group without “tcp”, “udp” or “tcp-udp” keywords specified.

Verification

You will not be able to test these requirements until you configure the next task.

```
R10#ping 6.6.146.100 so 10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.146.100, timeout is 2 seconds:
Packet sent with a source address of 6.6.99.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R10#telnet 6.6.146.100 49 /source-interface l0
Trying 6.6.146.100, 49 ... Open

[Connection to 6.6.146.100 closed by foreign host]

pod124acs/admin# ping 6.6.146.4
PING 6.6.146.4 (6.6.146.4) 56(84) bytes of data.
64 bytes from 6.6.146.4: icmp_seq=0 ttl=255 time=0.195 ms
64 bytes from 6.6.146.4: icmp_seq=1 ttl=255 time=8.05 ms
64 bytes from 6.6.146.4: icmp_seq=2 ttl=255 time=11.2 ms
64 bytes from 6.6.146.4: icmp_seq=3 ttl=255 time=8.52 ms

--- 6.6.146.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.195/7.002/11.236/4.114 ms, pipe 2

R9#telnet 10.1.1.8 443 /source-interface l0
Trying 10.1.1.8, 443 ... Open
get /
^C
[Connection to 10.1.1.8 closed by foreign host]

R11#telnet 6.6.146.8 443 /source-interface l0
Trying 6.6.146.8, 443 ... Open

ASA(config)# sh run access-l
access-list TO_ACS extended permit tcp any host 10.1.1.100
access-list OUTSIDE_IN extended permit object-group ACS_PORTS object-group
LOOPBACKS host 10.1.1.100
access-list OUTSIDE_IN extended permit tcp any host 10.1.1.8 object-group
R8_PORTS
access-list DMZ_IN extended permit tcp host 6.6.99.9 host 10.1.1.8 object-
group R8_PORTS

ASA(config)# sh access-list OUTSIDE_IN
```

```
access-list OUTSIDE_IN; 58 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit object-group ACS_PORTS
object-group LOOPBACKS host 10.1.1.100 0x40879d61
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.1 host
10.1.1.100 eq ftp (hitcnt=0) 0x1c57842d
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.2 host
10.1.1.100 eq ftp (hitcnt=0) 0x72d8021e
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.4 host
10.1.1.100 eq ftp (hitcnt=0) 0xdbbeabdd
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.5 host
10.1.1.100 eq ftp (hitcnt=0) 0x76be809f
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.6 host
10.1.1.100 eq ftp (hitcnt=0) 0x4b14223f
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.7 host
10.1.1.100 eq ftp (hitcnt=0) 0x064e68a8
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.10 host
10.1.1.100 eq ftp (hitcnt=0) 0x3deae10a
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.11 host
10.1.1.100 eq ftp (hitcnt=0) 0x6dfd1205
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.1 host
10.1.1.100 eq https (hitcnt=0) 0x24be5740
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.2 host
10.1.1.100 eq https (hitcnt=0) 0xd6cdd43b
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.4 host
10.1.1.100 eq https (hitcnt=0) 0x935da19a
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.5 host
10.1.1.100 eq https (hitcnt=0) 0x48b195ef
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.6 host
10.1.1.100 eq https (hitcnt=0) 0x7a1b70f7
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.7 host
10.1.1.100 eq https (hitcnt=0) 0xd48bef31
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.10 host
10.1.1.100 eq https (hitcnt=0) 0x7432e5ef
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.11 host
10.1.1.100 eq https (hitcnt=0) 0xf780030e
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.1 host
10.1.1.100 eq tacacs (hitcnt=0) 0x061b3483
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.2 host
10.1.1.100 eq tacacs (hitcnt=0) 0x30037979
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.4 host
10.1.1.100 eq tacacs (hitcnt=0) 0xed388187
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.5 host
10.1.1.100 eq tacacs (hitcnt=0) 0x15317f58
```

```
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.6 host
10.1.1.100 eq tacacs (hitcnt=0) 0xbd6b4c7d
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.7 host
10.1.1.100 eq tacacs (hitcnt=0) 0x5064065b
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.10 host
10.1.1.100 eq tacacs (hitcnt=1) 0xfd225556
  access-list OUTSIDE_IN line 1 extended permit tcp host 6.6.99.11 host
10.1.1.100 eq tacacs (hitcnt=0) 0xc965cdef
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.1 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0xb681dcba
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.2 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0xd035b247
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.4 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0x0a488601
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.5 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0x277b8707
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.6 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0x72bb965e
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.7 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0x00379b70
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.10 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0xb4bccb6d
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.11 host
10.1.1.100 range radius radius-acct (hitcnt=0) 0x8b67d72c
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.1 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0xbcaf0e67
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.2 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0x6f64af8a
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.4 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0xe012dbe8
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.5 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0x28d01833
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.6 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0x207f9392
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.7 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0xe209b7bb
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.10 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0x208d3ed4
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.11 host
10.1.1.100 range 1812 1813 (hitcnt=0) 0x1a60a8f5
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.1 host
10.1.1.100 eq tftp (hitcnt=0) 0x646a533b
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.2 host
10.1.1.100 eq tftp (hitcnt=0) 0xca10a486
```

```
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.4 host
10.1.1.100 eq tftp (hitcnt=0) 0xedd94962
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.5 host
10.1.1.100 eq tftp (hitcnt=0) 0x574f31da
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.6 host
10.1.1.100 eq tftp (hitcnt=0) 0xd0d5fa6b
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.7 host
10.1.1.100 eq tftp (hitcnt=0) 0xd334d10c
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.10 host
10.1.1.100 eq tftp (hitcnt=0) 0xe4b7bc56
  access-list OUTSIDE_IN line 1 extended permit udp host 6.6.99.11 host
10.1.1.100 eq tftp (hitcnt=0) 0x329820b6
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.1 host
10.1.1.100 echo (hitcnt=0) 0x828f64c1
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.2 host
10.1.1.100 echo (hitcnt=0) 0xeb766e35
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.4 host
10.1.1.100 echo (hitcnt=0) 0xa0ac3fb3
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.5 host
10.1.1.100 echo (hitcnt=0) 0x387031a0
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.6 host
10.1.1.100 echo (hitcnt=0) 0x4f8069ce
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.7 host
10.1.1.100 echo (hitcnt=0) 0x6dac1ef3
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.10 host
10.1.1.100 echo (hitcnt=20) 0x322613a8
  access-list OUTSIDE_IN line 1 extended permit icmp host 6.6.99.11 host
10.1.1.100 echo (hitcnt=5) 0x1e1269b9
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.8
object-group R8_PORTS (hitcnt=4) 0xb61a79ba
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.8 eq
https (hitcnt=0) 0xf0bec5bc
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.8 eq
ssh (hitcnt=4) 0x09d0a2ce


ASA(config)# sh access-list DMZ_IN
access-list DMZ_IN; 2 elements; name hash: 0x229557de
access-list DMZ_IN line 1 extended permit tcp host 6.6.99.9 host 10.1.1.8
object-group R8_PORTS (hitcnt=9) 0xa28cb73c
  access-list DMZ_IN line 1 extended permit tcp host 6.6.99.9 host
10.1.1.8 eq https (hitcnt=6) 0xe22207cc
  access-list DMZ_IN line 1 extended permit tcp host 6.6.99.9 host
10.1.1.8 eq ssh (hitcnt=3) 0xfacf9151
```

Task 1.4: Routing (4 Points)

- Configure EIGRP AS 89 on the inside and DMZ interface of the ASA
- The DMZ interface should only receive a default route
- Authenticate the EIGRP neighbors with strong authentication. The key should be “ipexpert”
- Configure the outside interface for OSPF. The area should be 0.0.0.0
- Authenticate Area 0.0.0.0 with key 5 password "cisco"
- Make sure that ASA & VLAN 146 devices prefer to go via R10 to get to Networks behind R10 and R11
- Redistribute OSPF to EIGRP but only permit 0.0.0.0/0 and 6.6.2.0/24 into EIGRP

Detailed Solution

ASA3

```
access-list O2E permit 6.6.2.0 255.255.255.0
access-list O2E permit host 0.0.0.0
!
access-list DMZ standard permit host 0.0.0.0
!
route-map O2E permit 10
 match ip address O2E
!
router eigrp 89
 distribute-list DMZ out interface DMZ
 default-metric 1 1 1 1 1
 network 10.1.1.0 255.255.255.0
 network 10.17.17.0 255.255.255.0
 redistribute ospf 1 route-map O2E
 no auto-summary
!
router ospf 1
 area 0.0.0.0 authentication message-digest
 network 6.6.146.30 255.255.255.0 area 0.0.0.0
!
interface G0/0
 ospf message-digest-key 1 md5 cisco
!
interface G0/1
 authentication key eigrp 89 ipexpert key-id 1
```

```
 authentication mode eigrp 89 md5
interface G0/2
 authentication key eigrp 89 ipexpert key-id 1
 authentication mode eigrp 89 md5
```

R2

```
router ospf 1
 area 0 authentication message-digest
int s0/1/0
 ip ospf message-digest-key 1 md5 cisco
```

R4

```
router ospf 1
 area 0 authentication message-digest
!
interface FastEthernet0/0
 ip ospf message-digest-key 1 md5 cisco
```

R5

```
router ospf 1
 area 0 authentication message-digest
!
interface FastEthernet0/0
 ip ospf message-digest-key 1 md5 cisco
int s0/1/0
 ip ospf message-digest-key 1 md5 cisco
```

R7

```
router ospf 1
 area 0 authentication message-digest
!
interface FastEthernet0/1
 ip ospf message-digest-key 1 md5 cisco
```

R8, R9

```
key chain EIGRP
 key 1
```

```
  key-string ipexpert
!
interface FastEthernet0/1
 ip authentication mode eigrp 89 md5
 ip authentication key-chain eigrp 89 EIGRP
```

R10

```
router ospf 1
 area 0 authentication message-digest
!
interface G0/0
 ip ospf message-digest-key 1 md5 cisco
interface G0/1
 ip ospf message-digest-key 1 md5 cisco
```

R11

```
router ospf 1
 area 0 authentication message-digest
!
interface G0/0
 ip ospf message-digest-key 1 md5 cisco
interface G0/1
 ip ospf message-digest-key 1 md5 cisco

int g0/1
 ip ospf cost 2
```

It's a lot of steps, but all very doable. Getting familiar with basic route filtering techniques is important for the test.

To make sure R10 is selected as the egress point for prefixes behind R10 and R11 increase OSPF cost on R11's G0/1. This will work for all routes here since Externals are Type 1.

Verification

Just take a look at the routing tables of the devices and test reachability using Ping. You can also verify the previous task if you haven't already done so.

```
R8#sh ip route  | be Gateway
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/2560002816] via 10.1.1.1, 00:07:43, FastEthernet0/1
      6.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX     6.6.2.0/24 [170/2560002816] via 10.1.1.1, 00:07:43,
FastEthernet0/1
C        6.6.99.8/32 is directly connected, Loopback0
D        6.6.99.9/32 [90/156416] via 10.1.1.1, 00:07:43, FastEthernet0/1
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/24 is directly connected, FastEthernet0/1
L        10.1.1.8/32 is directly connected, FastEthernet0/1
D        10.17.17.0/24 [90/28416] via 10.1.1.1, 00:07:43, FastEthernet0/1

R9#sh ip ro | be Gate
Gateway of last resort is 10.17.17.30 to network 0.0.0.0

     6.0.0.0/32 is subnetted, 1 subnets
C       6.6.99.9 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.17.17.0 is directly connected, FastEthernet0/1
D*EX 0.0.0.0/0 [170/2560002816] via 10.17.17.30, 00:46:50, FastEthernet0/1

R4#sh ip route | in 6.6.99
O IA     6.6.99.1/32 [110/3] via 6.6.146.7, 00:46:35, FastEthernet0/0
O        6.6.99.2/32 [110/67] via 6.6.146.10, 00:43:53, FastEthernet0/0
C        6.6.99.4/32 is directly connected, Loopback0
O        6.6.99.5/32 [110/3] via 6.6.146.10, 00:43:53, FastEthernet0/0
O        6.6.99.6/32 [110/2] via 6.6.4.6, 06:09:04, FastEthernet0/1
O        6.6.99.7/32 [110/2] via 6.6.146.7, 00:46:35, FastEthernet0/0
O        6.6.99.10/32 [110/2] via 6.6.146.10, 06:08:27, FastEthernet0/0
O        6.6.99.11/32 [110/2] via 6.6.146.11, 06:08:17, FastEthernet0/0

ASA# sh route | in 6.6.99
O    6.6.99.2 255.255.255.255 [110/76] via 6.6.146.10, 0:18:40, outside
O IA 6.6.99.1 255.255.255.255 [110/12] via 6.6.146.7, 0:18:40, outside
O    6.6.99.7 255.255.255.255 [110/11] via 6.6.146.7, 0:18:40, outside
O IA 6.6.99.6 255.255.255.255 [110/12] via 6.6.146.4, 0:18:40, outside
O    6.6.99.5 255.255.255.255 [110/12] via 6.6.146.10, 0:18:40, outside
```

```
O    6.6.99.4 255.255.255.255 [110/11] via 6.6.146.4, 0:18:40, outside
O    6.6.99.11 255.255.255.255 [110/11] via 6.6.146.11, 0:18:40, outside
O    6.6.99.10 255.255.255.255 [110/11] via 6.6.146.10, 0:18:40, outside
D    6.6.99.9 255.255.255.255 [90/130816] via 10.17.17.9, 0:52:01, DMZ
D    6.6.99.8 255.255.255.255 [90/130816] via 10.1.1.8, 0:10:33, inside

R6#ping 6.6.99.1 so l0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.99.1, timeout is 2 seconds:
Packet sent with a source address of 6.6.99.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 1.5: Filtering Techniques (4 Points)

- On ASA, prevent outside hosts from using FTP to AD based on the FTP message response 220 - “220 Microsoft FTP Service”. Make sure this server is reachable from the outside
- Configure ASA to block any java or active X for clients browsing the internet. Make sure servers located in the lab public network are unaffected
- Configure ASA to allow packets larger than the MSS for TCP sessions
- Configure ASA to not allow fragments coming to the outside interface

Detailed Solution

ASA

```
access-list FTP extended permit tcp any host 10.1.1.101 eq ftp
!
class-map FTP_CLASS
 match access-list FTP
!
regex MSG220 ".*Microsoft FTP Service.*"
!
tcp-map MSS
  exceed-mss allow
!
class-map cmTCP
 match port tcp range 1 65535
```

```
!
policy-map type inspect ftp FTP
 parameters
 match server regex MSG220
  reset log

policy-map global_policy
 no class inspection_default
 class FTP_CLASS
  inspect ftp strict FTP
 class cmTCP
  set connection advanced-options MSS
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp

object network AD
 host 10.1.1.101
 nat (inside,outside) static 6.6.146.101

access-list OUTSIDE_IN extended permit tcp any host 10.1.1.101 eq ftp

filter java except 0.0.0.0 0.0.0.0 6.6.0.0 255.255.0.0
filter activex except 0.0.0.0 0.0.0.0 6.6.0.0 255.255.0.0
filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

```
!
fragment chain 1 outside
```

So, message 220 is the response by the FTP server as to what its name is. We can use this string for our regex string to match and reset the FTP sessions to the server.

We configured Java filtering on ASA. Do not filter java or activex packets going to the inside networks of 6.6.0.0/16.

The TCP map allows us to exceeding MSS. To make sure all TCP ports are matched, the class-map cmTCP was configured with the full range of TCP ports. We then applied each of these maps to the default global policy prior to the class default policies.

Configuring ASA to allow only one fragment in the outside fragment chain results in not allowing fragments, as fragments need more than one.

Verification

If you want to test FTP part you will have to enable FTP server on AD. This can be accomplished by adding an FTP site to the IIS Manager – note this is something outside the scope of the CCIE Security lab.

```
R10#telnet 6.6.146.101 21
Trying 6.6.146.101, 21 ... Open
220 Microsoft FTP Service
quit
221 Goodbye.
[Connection to 6.6.146.101 closed by foreign host]
```

After you applied the policy :

```
R10#telnet 6.6.146.101 21
Trying 6.6.146.101, 21 ... Open

[Connection to 6.6.146.101 closed by foreign host]
```

```
ASA(config)# %ASA-4-507003: tcp flow from outside:6.6.146.10/33968 to
inside:10.1.1.101/21 terminated by inspection engine, reason - inspector
reset unconditionally.

R10#ping 6.6.146.100 so l0 size 1500
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 6.6.146.100, timeout is 2 seconds:
Packet sent with a source address of 6.6.99.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R10#ping 6.6.146.100 so l0 size 1501
Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 6.6.146.100, timeout is 2 seconds:
Packet sent with a source address of 6.6.99.10
.....
Success rate is 0 percent (0/5)

ASA(config)# %ASA-4-209005: Discard IP fragment set with more than 1
elements:  src = 6.6.99.10, dest = 6.6.146.100, proto = ICMP, id = 56

ASA(config)# sh fragment outside
Interface: outside
    Size: 200, Chain: 1, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 5, Overflow: 0


ASA(config)# sh service-policy global set connection detail

Global policy:
  Service-policy: global_policy
    Class-map: cmTCP
      Set connection policy:         drop 0
      Set connection advanced-options: MSS
        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
```

2.0 IOS Firewall (12 points)

Task 2.1: IOS Firewall (4 Points)

- Configure R4 to protect traffic going to the Extranet
- Allow only necessary traffic coming from the Extranet
- Allow inside hosts to access FTP servers on the Extranet
- Some FTP servers use ports 2121, 2122 as well as port 21 for FTP service
- Allow any other ICMP/TCP/UDP connection from the inside hosts to the Extranet including router originated traffic
- R4 should silently drop packets from the Extranet

Detailed Solution

R4

```
ip port-map ftp port tcp 2121 2122
!
ip inspect name CBAC ftp
ip inspect name CBAC udp router-traffic
ip inspect name CBAC tcp router-traffic
ip inspect name CBAC icmp router-traffic
!
ip access-list extended OUTSIDE_IN
 permit ospf host 6.6.4.6 host 224.0.0.5
 permit ospf host 6.6.4.6 host 6.6.4.4
 250 deny ip any any log
!
interface FastEthernet0/1
 ip access-group OUTSIDE_IN in
 ip inspect CBAC out
 no ip unreachables
```

Modifying the Port Map table was needed to account for non-standard FTP ports.

Unreachables were enabled on F0/1 – here we disabled them to make sure no information is sent back to the devices that are located in the Extranet.

Verification

```
R4#telnet 6.6.99.6
Trying 6.6.99.6 ... Open


Password required, but none set

[Connection to 6.6.99.6 closed by foreign host]

R4#ping 6.6.99.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.99.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R6#ping 6.6.99.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.99.4, timeout is 2 seconds:
...
Success rate is 0 percent (0/3)

R4#sh ip port-map ftp
Default mapping:  ftp      tcp port 21                          system
defined
Default mapping:  ftp      tcp port 2121,2122                   user
defined

R4#sh ip ins se detail
Established Sessions
 Session 49DE3F54 (6.6.146.10:51857)=>(6.6.99.6:23) tcp SIS_OPEN
  Created 00:00:03, Last heard 00:00:03
  Bytes sent (initiator:responder) [24:29]
  In  SID 6.6.99.6[23:23]=>6.6.146.10[51857:51857] on ACL OUTSIDE_IN  (8
matches)
```

Task 2.2: Zone-Based Firewall (4 Points)

- Configure R7 for ZBF

- Treat networks behind F0/0 as outside zone and networks behind F0/1 as inside
- Allow all outbound HTTP, ICMP, TCP, and UDP traffic
- Allow traffic back in as required for tasks in this lab
- Enable logging of dropped packets and log summaries

Detailed Solution

R7

```
parameter-map type inspect global
 log dropped-packets enable
 log summary

class-map type inspect match-any ZFW_ALL_INOUT_CLASS
 match protocol http
 match protocol tcp
 match protocol udp
 match protocol icmp
!
policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_ALL_INOUT_CLASS
  inspect
class class-default
 drop log
policy-map type inspect ZFW_OUTIN_POL
 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
zone-pair security OUTIN source OUT destination IN
 service-policy type inspect ZFW_OUTIN_POL
!
interface FastEthernet0/0
 zone-member security OUT
 ip virtual-reassembly in
```

```
interface FastEthernet0/1
 zone-member security IN
 ip virtual-reassembly in
```

The configuration is lengthy, but the technology is straightforward. Just watch out for the order of match statements in the class-map when they "overlap".

One note here is on Virtual Reassembly. This was not required by the task but it may be beneficial to enable this feature when dealing with ZFW or CBAC (even that those feature in newer code versions appear to do a better work with fragments). This is so the firewall can properly handle fragmented traffic and to prevent certain fragmentation attacks such as Buffer Overflow.

Verification

```
R7#sh policy-firewall config
Zone: self
  Description: System defined zone

Zone: IN
  Member Interfaces:
    FastEthernet0/1

Zone: OUT
  Member Interfaces:
    FastEthernet0/0

Zone-pair              : INOUT
Source Zone            : IN
Destination Zone       : OUT
Service-policy inspect : ZFW_INOUT_POL
  Class-map : ZFW_ALL_INOUT_CLASS(match-any)
  Action : inspect

  Class-map : class-default(match-any)
  Action : drop log

Zone-pair              : OUTIN
Source Zone            : OUT
```

```
Destination Zone       : IN
Service-policy inspect : ZFW_OUTIN_POL
  Class-map : class-default(match-any)
  Action : drop log

Parameter-map Config:
 Global:
  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets enabled
  log summary flows 16 time-interval 60
  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

R7#sh policy-firewall session zone-pair
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_ALL_INOUT_CLASS(match-any)
      Established Sessions =  1
```

```
        Session 49BD8AA0 (6.6.146.10:28558)=>(192.1.49.1:80) http:tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:05, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
      Half-open Sessions = 1
        Session 49BD8720 (192.1.6.200:138)=>(192.1.6.255:138) udp
SIS_OPENING
          Created 00:00:09, Last heard 00:00:02
          Bytes sent (initiator:responder) [478:0]
    Class-map : class-default(match-any)
 Zone-pair: OUTIN
  Service-policy inspect : ZFW_OUTIN_POL
    Class-map : class-default(match-any)

R7#
*May 11 12:56:41.295: %FW-6-DROP_PKT: Dropping tcp session
192.1.49.1:42736 6.6.99.10:23 on zone-pair OUTIN class class-default due
to  DROP action found in policy-map with ip ident 0

R7#sh policy-firewall summary-log

Configured number of flows       : [16]
Number of flows summarized       : [1]

FW-LOG-SUMMARY:2 tcp packets were dropped from 192.1.49.1:42736 =>
6.6.99.10:23 (target:class)-(OUTIN:class-default)

R7#sh ip virtual-reassembly
FastEthernet0/0:
   Virtual Fragment Reassembly (VFR) is ENABLED [in]
   Concurrent reassemblies (max-reassemblies): 16
   Fragments per reassembly (max-fragments): 32
   Reassembly timeout (timeout): 3 seconds
   Drop fragments: OFF

   Current reassembly count:0
   Current fragment count:0
   Total reassembly count:20
   Total reassembly timeout count:0

FastEthernet0/1:
```

```
Virtual Fragment Reassembly (VFR) is ENABLED [in]
Concurrent reassemblies (max-reassemblies): 16
Fragments per reassembly (max-fragments): 32
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF

Current reassembly count:0
Current fragment count:0
Total reassembly count:20
Total reassembly timeout count:0
```

Task 2.3: Zone-Based Firewall (4 Points)

- Configure ZFW to restrict traffic to R7
- Only allow R8 to manage R7 using SSH. Other SSH sessions should be dropped & logged
- Internet/External devices should not be able to ping R7
- If inside users try to use IM protocols, Peer-to-Peer applications, tunneling or things that shouldn't be done in HTTP make sure to reset this traffic
- Allow Yahoo Instant Messenger services other than text-chat but only to server "messenger.yahoo.com"

Detailed Solution

R7

```
ip access-list extended ICMP_TO_R7
 deny   icmp 6.6.0.0 0.0.255.255 any
 permit icmp any any

ip access-list extended SSH_TO_R7
 deny   tcp host 6.6.146.8 any eq 22
 permit tcp any any eq 22

class-map type inspect match-all ZFW_SELF_SSH_CLASS
 match access-group name SSH_TO_R7
 match protocol ssh

class-map type inspect match-all ZFW_SELF_ICMP_CLASS
 match access-group name ICMP_TO_R7
```

```
 match protocol icmp

class-map type inspect http match-any ZFW_HTTP_DPI_CLASS
 match  req-resp protocol-violation
 match  request port-misuse any

class-map type inspect ymsgr match-any ZFW_YAH_CLASS
 match  service text-chat

class-map type inspect ymsgr match-any ZFW_YAH_REST_CLASS
 match  service any

policy-map type inspect http HTTP_DPI
 class type inspect http ZFW_HTTP_DPI_CLASS
  reset

policy-map type inspect im ZFW_IM_POL
 class type inspect ymsgr ZFW_YAH_CLASS
  reset
 class type inspect ymsgr ZFW_YAH_REST_CLASS
  allow

class-map type inspect match-any ZFW_ALL_INOUT_CLASS
 no match protocol http

class-map type inspect match-all ZFW_INOUT_HTTP_CLASS
 match protocol http

parameter-map type protocol-info YAHOO-SERVER
 server name messenger.yahoo.com

class-map type inspect match-all ZFW_YAHOO_CLASS
 match protocol ymsgr YAHOO-SERVER

policy-map type inspect ZFW_INOUT_POL
 no class ZFW_ALL_INOUT_CLASS
 class type inspect ZFW_INOUT_HTTP_CLASS
  inspect
  service-policy http HTTP_DPI
 class type inspect ZFW_YAHOO_CLASS
```

```
  inspect
  service-policy im ZFW_IM_POL
 class type inspect ZFW_ALL_INOUT_CLASS
  inspect
 class class-default
  drop log

policy-map type inspect ZFW_TOSELF_POL
 class type inspect ZFW_SELF_SSH_CLASS
  drop log
 class type inspect ZFW_SELF_ICMP_CLASS
  drop
 class class-default
  pass

zone-pair security OUTSELF source OUT destination self
 service-policy type inspect ZFW_TOSELF_POL
zone-pair security INSELF source IN destination self
 service-policy type inspect ZFW_TOSELF_POL
```

An example situation when reading ahead would save you some time on the real lab. In the previous task we created a single class for TCP, UDP, ICMP and HTTP but here we need a separate one to tune some application-level inspection options for HTTP. Watch out for the order of classes in the policy.

Verification

Based on the output from the command below you could think that logging is also enabled for "passed" traffic, which is not the case. Something Cisco should fix in later releases.

```
R7#sh policy-firewall config
Zone: self
  Description: System defined zone

Zone: IN
  Member Interfaces:
    FastEthernet0/1

Zone: OUT
```

```
    Member Interfaces:
      FastEthernet0/0

  Zone-pair              : INOUT
  Source Zone            : IN
  Destination Zone       : OUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_INOUT_HTTP_CLASS(match-all)
    Action : inspect
     Service Policy: http HTTP_DPI

    Class-map : ZFW_YAHOO_CLASS(match-all)
    Action : inspect
     Service Policy: im ZFW_IM_POL

    Class-map : ZFW_ALL_INOUT_CLASS(match-any)
    Action : inspect

    Class-map : class-default(match-any)
    Action : drop log

  Zone-pair              : OUTIN
  Source Zone            : OUT
  Destination Zone       : IN
  Service-policy inspect : ZFW_OUTIN_POL
    Class-map : class-default(match-any)
    Action : drop log

  Zone-pair              : OUTSELF
  Source Zone            : OUT
  Destination Zone       : self
  Service-policy inspect : ZFW_TOSELF_POL
    Class-map : ZFW_SELF_SSH_CLASS(match-all)
    Action : drop log

    Class-map : ZFW_SELF_ICMP_CLASS(match-all)
    Action : drop log

    Class-map : class-default(match-any)
    Action : pass log
```

```
Zone-pair               : INSELF
Source Zone             : IN
Destination Zone        : self
Service-policy inspect : ZFW_TOSELF_POL
  Class-map : ZFW_SELF_SSH_CLASS(match-all)
  Action : drop log

  Class-map : ZFW_SELF_ICMP_CLASS(match-all)
  Action : drop log

  Class-map : class-default(match-any)
  Action : pass log

Parameter-map Config:
 Global:
  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets enabled
  log summary flows 16 time-interval 60
  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

R1#ping 192.1.49.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.49.7, timeout is 2 seconds:
..
Success rate is 0 percent (0/2)

R1#ping 192.1.49.7 so l0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.49.7, timeout is 2 seconds:
Packet sent with a source address of 6.6.99.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R8#ssh -l cisco 6.6.146.7

Password:

R7>

R4#ssh -l cisco 6.6.146.7

R4#

*May 11 14:09:52.359: %FW-6-DROP_PKT: Dropping ssh session 6.6.146.4:22830
6.6.146.7:22 on zone-pair INSELF class ZFW_SELF_SSH_CLASS due to  DROP
action found in policy-map with ip ident 0

R7#sh access-l
Extended IP access list ICMP_TO_R7
    30 deny icmp 6.6.0.0 0.0.255.255 any (20 matches)
    40 permit icmp any any (4 matches)
Extended IP access list SSH_TO_R7
    10 deny tcp host 6.6.146.8 any eq 22 (32 matches)
    20 permit tcp any any eq 22 (4 matches)
```

3.0 Cisco IPSand Content Security (8 points)

Task 3.1: IPS Initialization (4 Points)

- Configure the IPS between R7 and the "Internet"
- Configure the Management interface according to the IP Addressing table
- Allow only 10.1.1.200 to manage the device
- Configure the IPS to send a High alert for each echo reply packet passing through it

Detailed Solution

CAT4

```
vlan 49,490

interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/2
 switchport access vlan 490
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/3
 switchport access vlan 49
 switchport mode access
 spanning-tree portfast
```

CAT1

```
interface FastEthernet0/1
 switchport access vlan 49
 switchport mode access
 spanning-tree portfast

interface FastEthernet0/7
```

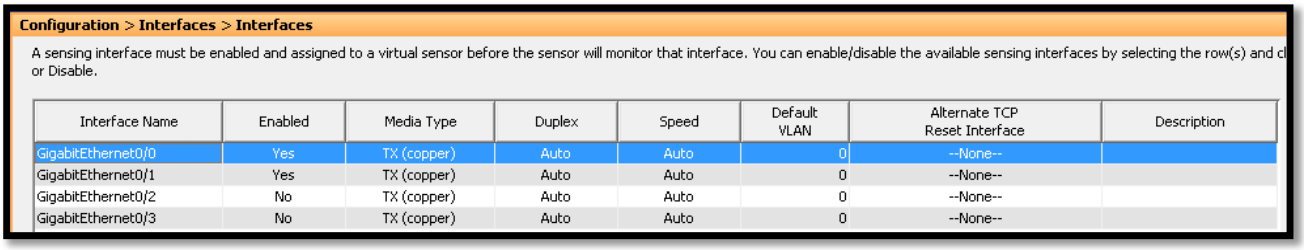
```
 switchport access vlan 490
 switchport mode access
 spanning-tree portfast
```

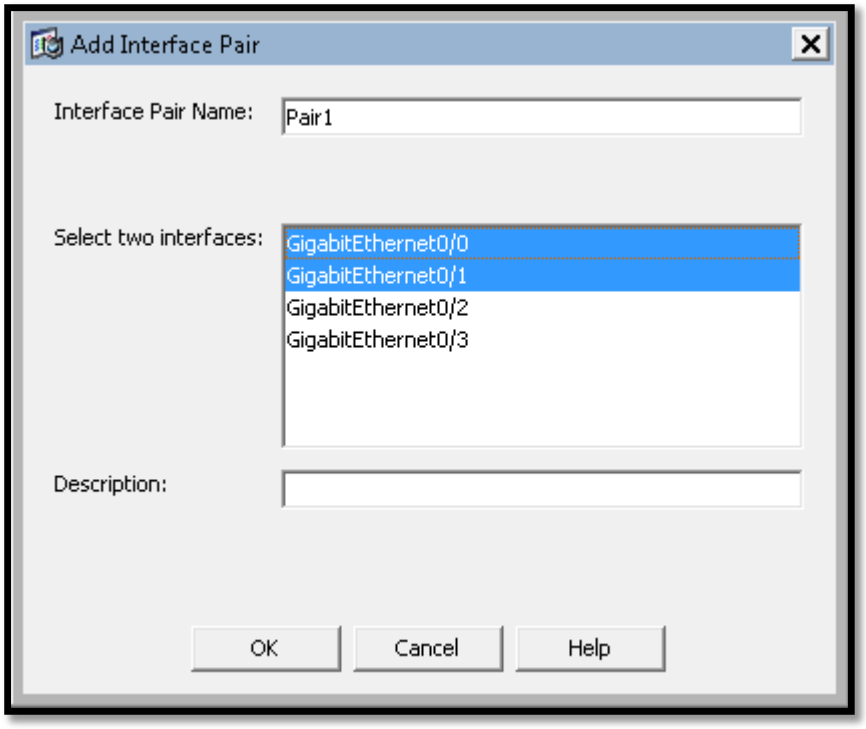
IPS

```
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: 10.1.1.200/32
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 10.1.1.200/32
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
```

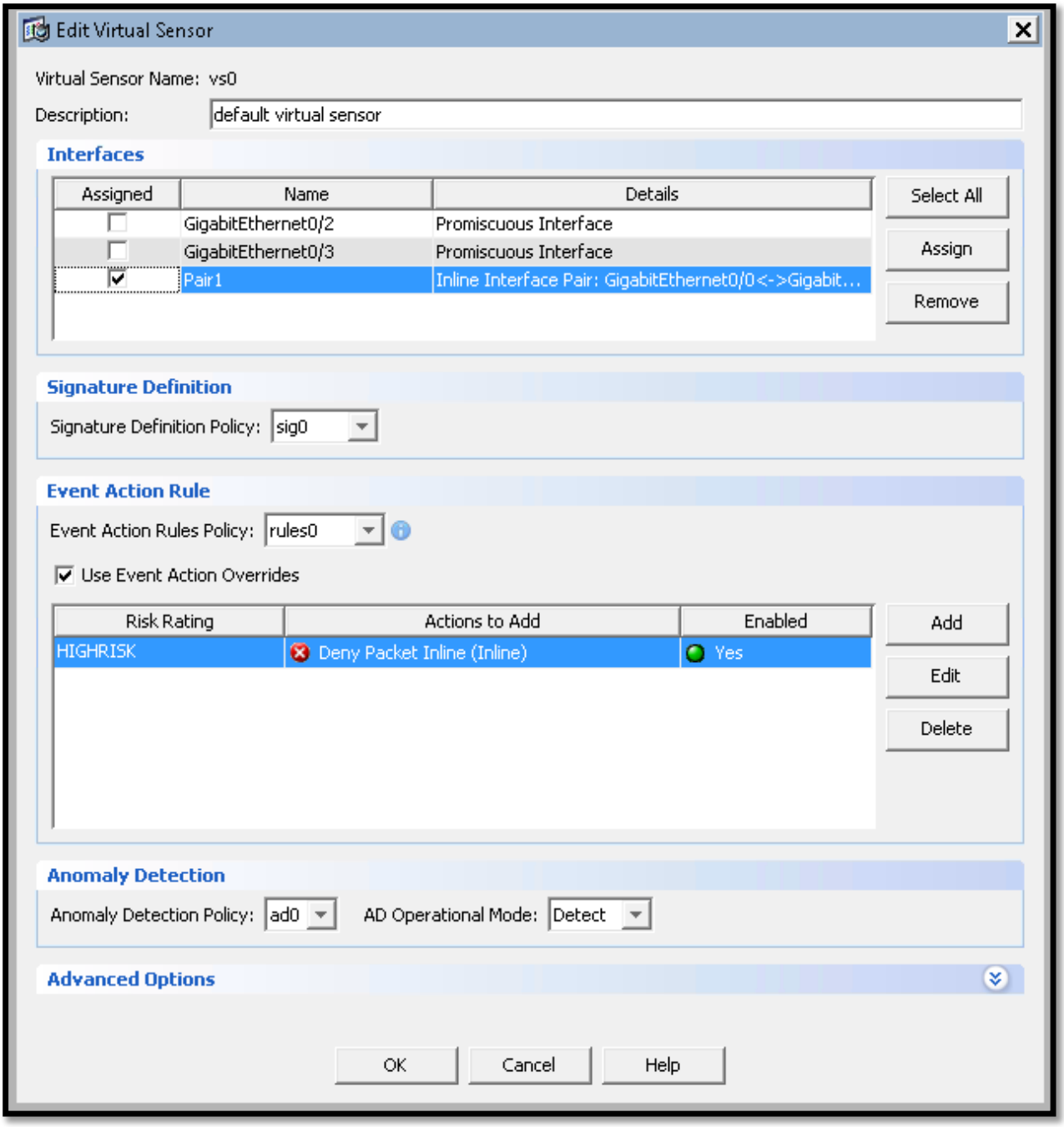
```
exit
service global-correlation
network-participation off
exit


[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]: 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 ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.
```

Now connect through the Test PC (10.1.1.200) and finish the remaining configuration. Bring up the ports, configure Interface Pair :

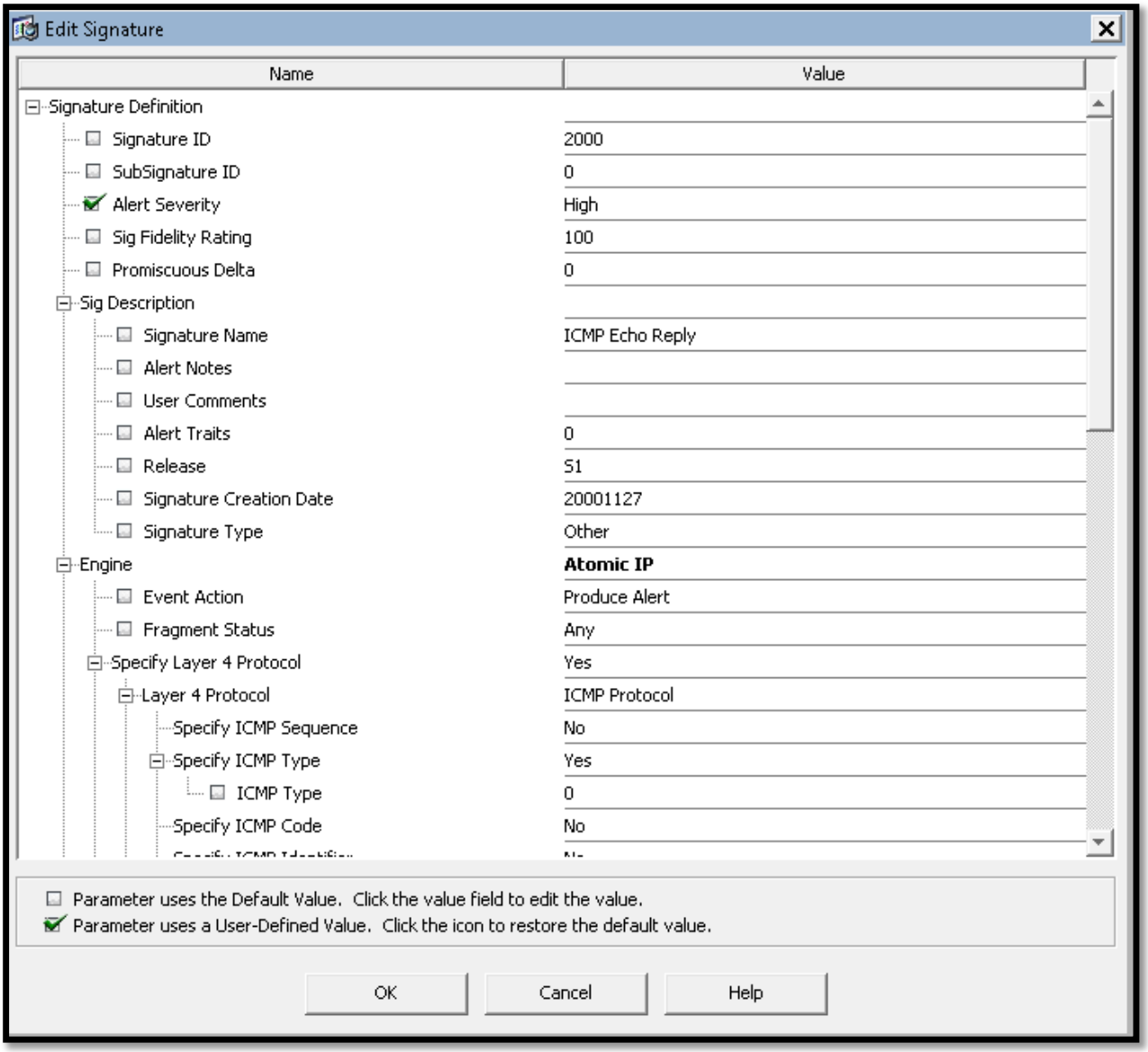


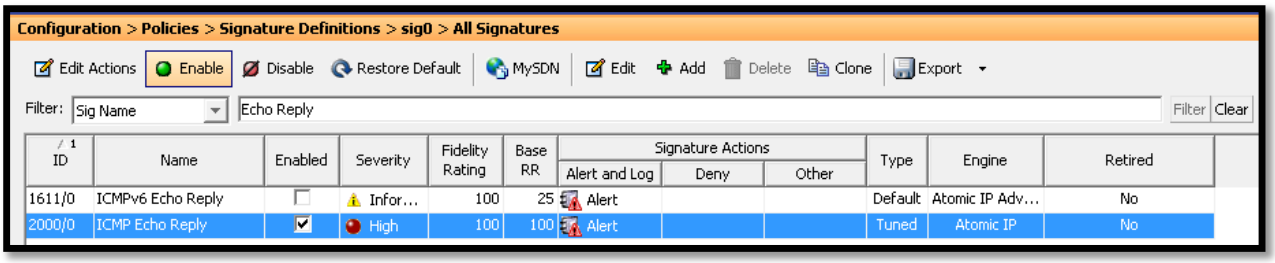


Assign the Pair to vs0:



Enable Echo Reply and change Severity to High:





Based on the requirements of the question, the IPS will be running in inline mode.

Always remember to double-check the L2 settings; in this question we had to adjust VLAN configuration on the interfaces connected to R1, R7 and IPS.

Verification

Ping R1 from R7 and observe the alert:

```
IPS# show events alert

evIdsAlert: eventId=1041379286523781737 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2003/05/23 12:40:11 2003/05/23 12:40:11 UTC
  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 192.1.49.1
    target:
      addr: locality=OUT 192.1.49.7
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
100
  threatRatingValue: 65
  interface: ge0_1
  protocol: icmp


R1#sh ip ospf neigh
```

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
192.1.49.7        1   FULL/DR         00:00:39    192.1.49.7
FastEthernet0/0
```

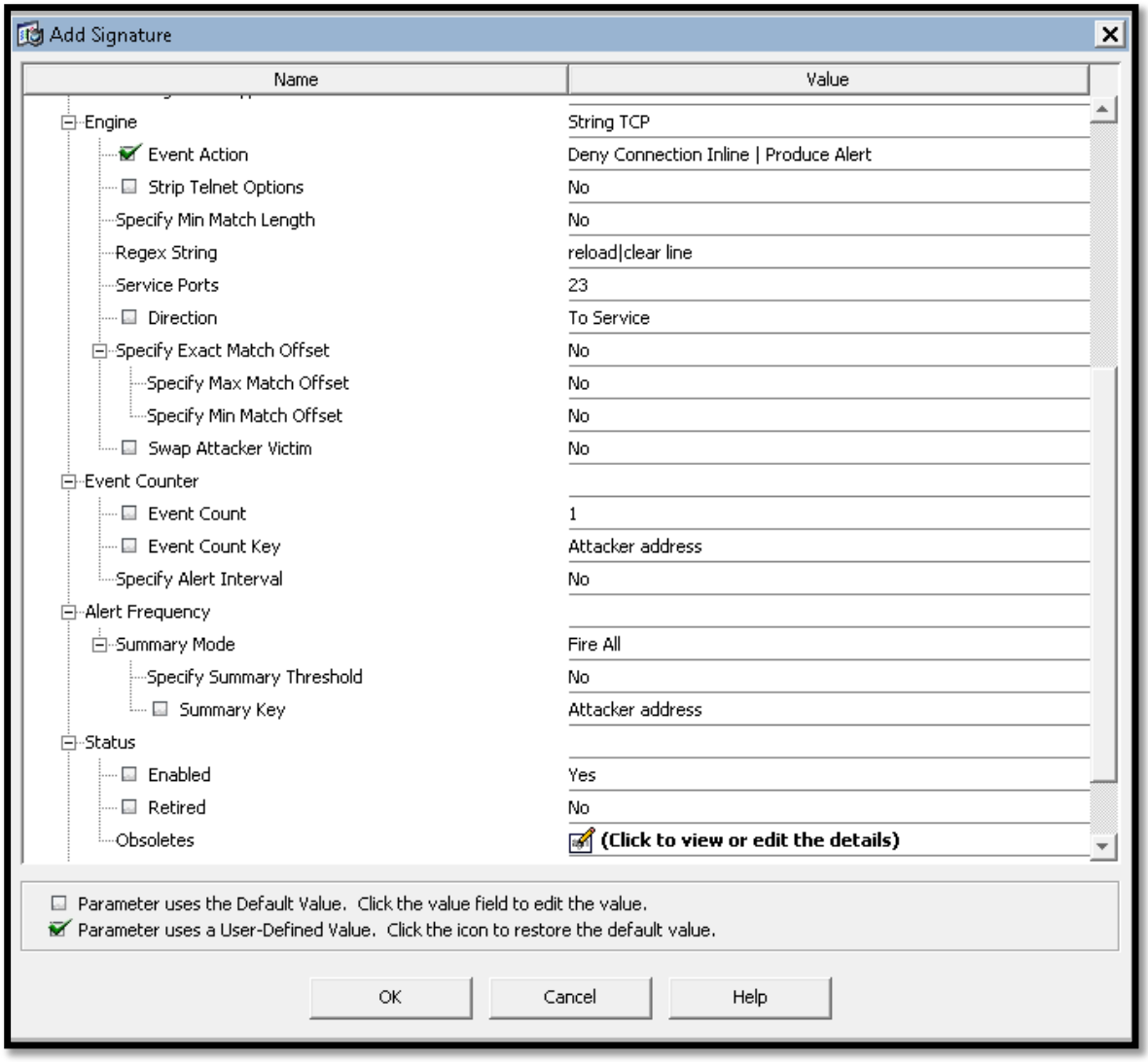
Task 3.2: Blocking Attacks (4 Points)

- Configure the IPS to block the connection and send an alert if there are any attempts to send the following strings via Telnet : “reload” or “clear line”
- The alarm should be sent each time IPS sees these strings in a telnet session

Detailed Solution

IPS

Add a new Signature using the plus button. Choose TCP String Engine and configure as shown below:



Getting used to the signature configuration - different engines & regular expressions is important for success in the CCIE exam. Be sure you understand when you will want to use each type of signature.

Verification

Ping R1 from R7 and observe the alert:

```
IPS# show events alert

evIdsAlert: eventId=1041379286523781849 severity=medium vendor=Cisco
  originator:
```

```
      hostId: IPS
      appName: sensorApp
      appInstanceId: 413
    time: 2003/05/23 13:35:29 2003/05/23 13:35:29 UTC
    signature: description=Custom Telnet Attack id=60000 created=20000101
type=other version=custom
      subsigId: 0
      sigDetails: Custom Telnet Attack
      marsCategory: Info/Misc
    interfaceGroup: vs0
    vlan: 0
    participants:
      attacker:
        addr: locality=OUT 6.6.146.10
        port: 56008
      target:
        addr: locality=OUT 192.1.49.1
        port: 23
        os: idSource=unknown relevance=relevant type=unknown
    actions:
      deniedFlow: true
    context:
      fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 52 31  ..............R1
000010  3E FF FD 21 FF FA 21 00  FF F0 FF FE 18 63 6C 20  >..!..!......af
000020  65 61 72 20 6C 69 6E 65  20 72 65 6C 6F 61        ear 12za reloa
      fromAttacker:
000000  FF FD 03 FF FB 1F FF FB  21 FF FD 01 FF FC 18 FF  ........!.......
000010  FA 1F 00 50 00 18 FF F0  63 6C 20 65 61 72 20 6C  ...P....af ear 1
000020  69 6E 65 20 72 65 6C 6F  61 64                    2za reload
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
66
    threatRatingValue: 31
    interface: ge0_0
    protocol: tcp


evIdsAlert: eventId=1041379286523781851 severity=medium vendor=Cisco
    originator:
      hostId: IPS
      appName: sensorApp
```

```
    appInstanceId: 413
  time: 2003/05/23 13:36:13 2003/05/23 13:36:13 UTC
  signature: description=Custom Telnet Attack id=60000 created=20000101
type=other version=custom
    subsigId: 0
    sigDetails: Custom Telnet Attack
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 6.6.146.10
      port: 62842
    target:
      addr: locality=OUT 192.1.49.1
      port: 23
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedFlow: true
  context:
    fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 52 31  ..............R1
000010  3E FF FD 21 FF FA 21 00  FF F0 FF FE 18 73 64 20  >..!..!......sd
000020  61 20 20 64 20 63 6C 65  61 72 20 6C 69 6E        a  d clear lin
    fromAttacker:
000000  FF FD 03 FF FB 1F FF FB  21 FF FD 01 FF FC 18 FF  ........!.......
000010  FA 1F 00 50 00 18 FF F0  73 64 20 61 20 20 64 20  ...P....sd a  d
000020  63 6C 65 61 72 20 6C 69  6E 65                    clear line
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
66
  threatRatingValue: 31
  interface: ge0_0
  protocol: tcp
```

4.0 Cisco VPN Solutions (18 points)

Task 4.1: Site to Site (4 Points)

- Configure R4 and R9 to encrypt packets between VLAN4 and VLAN100
- Use the most secure Main Mode messages 3, 4. The authentication key should be "ipexpert"
- Make sure the tunnel can be initiated from both sides and that devices on the Extranet can ping the ACS server
- Don't introduce any additional transport overhead for the data traffic
- You are allowed one static route to get this to work

Detailed Solution

R4

```
crypto isakmp policy 10
 encr aes 192
 hash sha
 authentication pre-share
 group 5

crypto isakmp key ipexpert address 6.6.146.9
!
ip access-list extended L2L
 permit ip 6.6.4.0 0.0.0.255 10.1.1.0 0.0.0.255
!
crypto ipsec transform-set SET1 esp-aes 192 esp-sha-hmac

crypto map MAP1 10 ipsec-isakmp
 set peer 6.6.146.9
 set transform-set SET1
 match address L2L
 reverse-route static
!
interface FastEthernet0/0
 crypto map MAP1

ip access-list ext OUTSIDE_IN
 30 per ip 6.6.4.0 0.0.0.255 10.1.1.0 0.0.0.255
```

```
no crypto ipsec nat-transparency udp-encaps
```

R9

```
crypto isakmp policy 10
 encr aes 192
 hash sha
 authentication pre-share
 group 5

crypto isakmp key ipexpert address 6.6.146.4
!
ip access-list extended L2L
 permit ip 10.1.1.0 0.0.0.255 6.6.4.0 0.0.0.255
!
crypto ipsec transform-set SET1 esp-aes 192 esp-sha-hmac

crypto map MAP1 10 ipsec-isakmp
 set peer 6.6.146.4
 set transform-set SET1
 match address L2L
!
interface FastEthernet0/1
 crypto map MAP1
```

ASA3

```
access-list DMZ_IN per udp host 10.17.17.9 host 6.6.146.4 eq 500
access-list DMZ_IN per esp host 10.17.17.9 host 6.6.146.4
access-list DMZ_IN per ip 6.6.4.0 255.255.255.0 10.1.1.0 255.255.255.0

access-list OUTSIDE_IN per udp host 6.6.146.4 host 10.17.17.9 eq 500
access-list OUTSIDE_IN per esp host 6.6.146.4 host 10.17.17.9

route DMZ 6.6.4.0 255.255.255.0 10.17.17.9 1
```

Diffe Helman group 5 is the most secure MM message 3, and 4 authentication method.

Because R9 is behind ASA there are a few things we need to fix on ASA to get the traffic working. We need to change the outside & DMZ ACLs to allow communication to VLAN10 from

the traffic coming in from the ExtraNet. Also since we know no additional overhead will be involved in transport (NAT-T is disabled), allowing ISAKMP and ESP through is enough. For the ASA to send traffic to 6.6.4.0/24 to R9 we need to add a static route to override the desire it has to go to R4 for this by default.

Verification

Make sure the tunnel comes up when initiated from Extranet and also from VLAN 100.

```
R4#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
10.1.1.0/255.255.255.0 [1/0] via 6.6.146.9 tag 0
                                on FastEthernet0/0 RRI  S

R9#sh ip ro 6.6.4.6
% Subnet not in table

R9#sh ip ro 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "eigrp 89", distance 170, metric 2560002816, candidate default
path, type external
  Redistributing via eigrp 89
  Last update from 10.17.17.30 on FastEthernet0/1, 06:32:07 ago
  Routing Descriptor Blocks:
  * 10.17.17.30, from 10.17.17.30, 06:32:07 ago, via FastEthernet0/1
      Route metric is 2560002816, traffic share count is 1
      Total delay is 110 microseconds, minimum bandwidth is 1 Kbit
      Reliability 1/255, minimum MTU 1 bytes
      Loading 1/255, Hops 1

R6#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 80 percent (4/5), round-trip min/avg/max = 4/9/24 ms

R4#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: FastEthernet0/0
Uptime: 00:01:09
Session status: UP-ACTIVE
Peer: 6.6.146.9 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.17.17.9
      Desc: (none)
  IKEv1 SA: local 6.6.146.4/500 remote 6.6.146.9/500 Active
          Capabilities:(none) connid:1005 lifetime:23:58:50
  IPSEC FLOW: permit ip 6.6.4.0/255.255.255.0 10.1.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4418112/3530
        Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4418112/3530

R4#clear cry sess

R8#ping 6.6.4.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.4.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms

R9#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: FastEthernet0/1
```

```
Uptime: 00:01:12
Session status: UP-ACTIVE
Peer: 6.6.146.4 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 6.6.146.4
      Desc: (none)
  IKE SA: local 10.17.17.9/500 remote 6.6.146.4/500 Active
          Capabilities:(none) connid:1006 lifetime:23:58:47
  IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 6.6.4.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4478491/3592
        Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4478491/3592
```

Task 4.2: Stateful HA IPSec (5 Points)

All traffic behind R2 Serial0/1/0 and VLAN146 should be encrypted R10 and R11 should act as a failover IPSec pair In the event of a host failure the IPSec tunnel should remain active without requiring a new SA negotiation. A Failure should be detected in less than 300 msec DH exchange should take place every Quick Mode negotiation

Disable Antil Reply checks on R2 Tune OSPF timers on all devices in VLAN 146 to speed up the convergence

Tune OSPF timers on all devices in VLAN 146 to speed up the convergence

Make sure IPSec peers verify if the tunnel is actually operational. It should only occur when traffic is actively traversing the IPSec tunnel

Detailed Solution

ASA3

```
int g0/0
 ospf hello 1
 ospf dead 1
```

R2

```
ip access-list extended HA_VPN
```

```
 permit ip 6.6.2.0 0.0.0.255 6.6.146.0 0.0.0.255
 permit ip host 6.6.99.2 6.6.146.0 0.0.0.255
!
crypto isakmp policy 10
 encryption aes
 hash sha
 authentication pre-share
 group 2

crypto ipsec security-association replay disable

crypto isakmp key cisco address 6.6.156.100
!
crypto ipsec transform-set SET2 esp-aes esp-sha-hmac
!
crypto map MAP2 10 ipsec-isakmp
 set peer 6.6.156.100
 set transform-set SET2
 set pfs group2
 match address HA_VPN
!
interface serial 0/1/0
 crypto map MAP2
!
crypto isakmp keepalive 10 2 on-demand
```

R4

```
int f0/0
 ip ospf hello-int 1
 ip ospf dead-int 2
```

R7

```
int f0/1
 ip ospf hello-int 1
 ip ospf dead-int 2
```

R10

```
track 1 interface GigabitEthernet0/0 line-protocol
```

```
track 2 interface GigabitEthernet0/1 line-protocol
track 3 list boolean and
 object 1
 object 2

int g0/0
 ip ospf hello-interval 1
 ip ospf dead-interval 2

interface G0/1
 standby version 2
 standby 2 ip 6.6.156.100
 standby 2 priority 110
 standby 2 preempt
 standby 2 timers msec 100 1
 standby 2 name HSRP
 standby 2 track 3 decrement 30

ip access-list extended HA_VPN
 permit ip 6.6.146.0 0.0.0.255 6.6.2.0 0.0.0.255
 permit ip 6.6.146.0 0.0.0.255 host 6.6.99.2

crypto isakmp policy 10
 encryption aes
 hash sha
 authentication pre-share
 group 2

crypto isakmp key cisco address 6.6.25.2
!
crypto ipsec transform-set SET2 esp-aes esp-sha-hmac
!
crypto map MAP2 10 ipsec-isakmp
 set peer 6.6.25.2
 set transform-set SET2
 set pfs group2
 match address HA_VPN
!
redundancy inter-device
 scheme standby HSRP
```

```
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 6.6.146.10
    retransmit-timeout 300 10000
    path-retransmit 5
    assoc-retransmit 5
   remote-port 5000
    remote-ip 6.6.146.11
!
interface G0/1
 crypto map MAP2 redundancy HSRP stateful
!
crypto isakmp keepalive 10 2 on-demand
```

R11

```
track 1 interface GigabitEthernet0/0 line-protocol
track 2 interface GigabitEthernet0/1 line-protocol
track 3 list boolean and
 object 1
 object 2

interface G0/1
 standby version 2
 standby 2 ip 6.6.156.100
 standby 2 priority 100
 standby 2 preempt
 standby 2 timers msec 100 1
 standby 2 name HSRP
 standby 2 track 3 decrement 30

ip access-list extended HA_VPN
 permit ip 6.6.146.0 0.0.0.255 6.6.2.0 0.0.0.255
 permit ip 6.6.146.0 0.0.0.255 host 6.6.99.2
crypto isakmp policy 10
 encryption aes
 hash sha
```

```
 authentication pre-share
 group 2

crypto isakmp key cisco address 6.6.25.2
!
crypto ipsec transform-set SET2 esp-aes esp-sha-hmac
!
crypto map MAP2 10 ipsec-isakmp
 set peer 6.6.25.2
 set transform-set SET2
 set pfs group2
 match address HA_VPN
!
redundancy inter-device
 scheme standby HSRP
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 6.6.146.11
    retransmit-timeout 300 10000
    path-retransmit 5
    assoc-retransmit 5
   remote-port 5000
    remote-ip 6.6.146.10
!
int g0/0
 ip ospf hello-interval 1
 ip ospf dead-interval 2

interface G0/1
 crypto map MAP2 redundancy HSRP stateful
!
crypto isakmp keepalive 10 2 on-demand
```

Stateful failover for IPsec is designed to work in conjunction with stateful switchover (SSO) and Hot Standby Routing Protocol (HSRP). HSRP provides network redundancy for IP networks,

ensuring that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. That is, HSRP monitors both the inside and outside interfaces so that if either interface goes down, the whole router is deemed to be down and the ownership of Internet Key Exchange (IKE) and IPsec security associations (SAs) is passed to the standby router (which transitions to the HSRP active state). Here note that this monitoring must be mutual, which is known as Mutual Tracking. Mutual tracking means that if the outside interface does fail, the inside interface on the same router will also be deemed down, allowing for complete router failover to the secondary router.

SSO is a method of providing redundancy and synchronization for many Cisco IOS applications and features. In our case it allows the active and standby routers to share IKE and IPsec state information so both routers have enough information to become the active router at any time.

For any type of IPSec HA configurations remember that the configuration information between the active and standby devices is not automatically transferred; you are responsible for ensuring that the crypto configurations match on both devices. If the crypto configurations on both devices do not match, failover from the active device to the standby device will not be successful.

In our case we did not have to worry about RRI since OSPF configuration was engineered to point to R10 for prefixes behind R10 and R11 in one of the earlier tasks.

HSRP version 1 only allows a minimum of 1 second for each hello. Version 2 decreases that timer to 1 millisecond. This allowed us to have the hellos exchanged every 100 milliseconds.

Finally remember that only PSK can be used for this feature and that legacy IKE Keepalives are not supported – DPD is, however, as shown in this task.

Verification

Note: A reload is required on the standby device (R11) to activate the standby redundancy scheme.

First verify HSRP and SSO:

```
R10#sh stan br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       2    110 P Active  local           6.6.156.11      6.6.156.100
```

```
R10#sh cry ha
IKE VIP: 6.6.156.100
  stamp: 47 ED C4 D0 39 DA 3D AA 4B 5E 9B F7 BE 20 53 17
IPSec VIP: 6.6.156.100

R10#sh redundancy inter-device
Redundancy inter-device state: RF_INTERDEV_STATE_ACT
  Scheme: Standby
      Groupname: HSRP Group State: Active
  Peer present: RF_INTERDEV_PEER_COMM
  Security: Not configured

R10#sh redundancy states
       my state = 13 -ACTIVE
      peer state = 8  -STANDBY HOT
            Mode = Duplex
         Unit ID = 0

     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 13
 client_notification_TMR = 60000 milliseconds
           RF debug mask = 0x0


R11#sh redundancy inter-device
Redundancy inter-device state: RF_INTERDEV_STATE_STDBY
  Scheme: Standby
      Groupname: HSRP Group State: Standby
  Peer present: RF_INTERDEV_PEER_COMM
  Security: Not configured

R11#sh cry ha
IKE VIP: 6.6.156.100
  stamp: 9C C3 73 4B 61 85 06 32 20 85 D7 BE C1 BC 78 56
IPSec VIP: 6.6.156.100
```

We can now test IPSec and state replication:

```
R4#ping 6.6.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.99.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/29/32 ms

R4#ping 6.6.2.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.130, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/29/32 ms


R2#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: Serial0/1/0
Uptime: 00:00:31
Session status: UP-ACTIVE
Peer: 6.6.156.100 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 6.6.156.100
      Desc: (none)
  IKE SA: local 6.6.25.2/500 remote 6.6.156.100/500 Active
         Capabilities:D connid:1001 lifetime:23:59:28
  IPSEC FLOW: permit ip host 6.6.99.2 6.6.146.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4491266/3568
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4491266/3568
  IPSEC FLOW: permit ip 6.6.2.0/255.255.255.0 6.6.146.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4477913/3575
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4477913/3575
```

```
R10#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: GigabitEthernet0/1
Uptime: 00:01:58
Session status: UP-ACTIVE
Peer: 6.6.25.2 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 6.6.25.2
      Desc: (none)
  IKEv1 SA: local 6.6.156.100/500 remote 6.6.25.2/500 Active
          Capabilities:D connid:1001 lifetime:23:58:01
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 6.6.2.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4370223/3537
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4370223/3537
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 host 6.6.99.2
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4301331/3481
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4301331/3481
```

Note R11 also shows 4 Active IPSec SAs; this information was replicated from R10 which is the Active VPN Peer. IKE SA was also replicated; it is Standby on R11:

```
R11#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: GigabitEthernet0/1
Session status: UP-STANDBY
Peer: 6.6.25.2 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IKEv1 SA: local 6.6.156.100/500 remote 6.6.25.2/500 Active
          Capabilities:D connid:1001 lifetime:23:58:09
```

```
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 6.6.2.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 3817223/3545
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 3817223/3545
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 host 6.6.99.2
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 3858364/3490
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 3858364/3490


R11#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
6.6.25.2        6.6.156.100     QM_IDLE           1001 STDBY

IPv6 Crypto ISAKMP SA

R10#sh cry isa sa active
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
6.6.25.2        6.6.156.100     QM_IDLE           1001 ACTIVE
```

We will now start testing the failover (by shutting down G0/0 on R10). Here remember that each time the Active device changes its state to Standby it will do a self-reload to ensure that the state of the new Standby device synchronizes correctly with the new Active device.

```
R4#ping 6.6.99.2 rep 10000000 timeout 1

Type escape sequence to abort.
Sending 10000000, 100-byte ICMP Echos to 6.6.99.2, timeout is 1 seconds:
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!........!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.

R10#
*May 12 22:33:59.815: %TRACKING-5-STATE: 3 list boolean and Up->Down
*May 12 22:33:59.875: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 2 state
Active -> Speak
```

```
*May 12 22:34:02.935: %RF-5-RF_RELOAD: Self reload. Reason: Not in correct
state for becoming Standby
*May 12 22:34:02.935: %RF_INTERDEV-4-RELOAD: % RF induced self-reload. my
state = ACTIVE peer state = STANDBY HOT
*May 12 22:34:05.367: %LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to administratively down



R11#
*May 12 22:45:02.355: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 2 state
Standby -> Active
*May 12 22:45:02.359: %CRYPTO-5-IKE_SA_HA_STATUS: IKE sa's if any, for vip
6.6.156.100 will change from STANDBY to ACTIVE
*May 12 22:45:02.363: %CRYPTO-5-IPSEC_SA_HA_STATUS: IPSec sa's if any, for
vip  6.6.156.100 will change from STANDBY to ACTIVE



R11#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: GigabitEthernet0/1
Session status: UP-ACTIVE
Peer: 6.6.25.2 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IKEv1 SA: local 6.6.156.100/500 remote 6.6.25.2/500 Active
          Capabilities:D connid:1001 lifetime:23:57:28
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 6.6.2.0/255.255.255.0
        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
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 host 6.6.99.2
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 115 drop 0 life (KB/Sec) 3784768/3450
        Outbound: #pkts enc'ed 115 drop 0 life (KB/Sec) 3784768/3450
```

```
R2#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: Serial0/1/0
Uptime: 00:02:45
Session status: UP-ACTIVE
Peer: 6.6.156.100 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 6.6.156.100
      Desc: (none)
  IKE SA: local 6.6.25.2/500 remote 6.6.156.100/500 Active
          Capabilities:D connid:1005 lifetime:23:57:14
  IPSEC FLOW: permit ip host 6.6.99.2 6.6.146.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 259 drop 0 life (KB/Sec) 4590751/3434
        Outbound: #pkts enc'ed 259 drop 0 life (KB/Sec) 4590751/3434
  IPSEC FLOW: permit ip 6.6.2.0/255.255.255.0 6.6.146.0/255.255.255.0
        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
```

Finally a second reload occurs (now on R11 since it detected a new active HSRP device – we enabled preemption and R10 has higher priority) but the session is still UP and working:

```
R4#ping 6.6.99.2 rep 10000000 tim 1

Type escape sequence to abort.
Sending 10000000, 100-byte ICMP Echos to 6.6.99.2, timeout is 1 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 98 percent (54/55), round-trip min/avg/max = 28/28/40 ms

R10#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: GigabitEthernet0/1
Session status: UP-ACTIVE
Peer: 6.6.25.2 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IKEv1 SA: local 6.6.156.100/500 remote 6.6.25.2/500 Active
          Capabilities:D connid:1001 lifetime:23:56:05
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 6.6.2.0/255.255.255.0
        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
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 host 6.6.99.2
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 55 drop 0 life (KB/Sec) 4315679/3226
        Outbound: #pkts enc'ed 55 drop 0 life (KB/Sec) 4315679/3226
```

Task 4.3: Site to Site IOS-ASA (5 Points)

- Configure Loopback1 on R5, with IP address 6.6.55.5/24
- Configure R5 and the ASA to protect traffic between R5's Loopback1 and VLAN100 using IPSec
- Use the first default ISAKMP policy on R5. Use R8 if you need another device to complete this Task. Make sure for the certificates the strongest cryptographic hash and signing functions supported are used

Detailed Solution

R8

```
ntp master 2

ip http server

ip domain-name ipexpert.com

crypto key generate rsa general-keys label CAKEY exportable modulus 4096
!
crypto pki trustpoint CA
 revocation-check crl
 rsakeypair CAKEY
```

```
 password ipexpert123
!
crypto pki server CA
 database level min
 database archive pem password ipexpert
 issuer-name CN=R8 CA, O=IPexpert, OU=Instructors, L=Warsaw, C=PL
 grant auto
 hash sha512
 database url flash:
 no shutdown
```

R5

```
interface Loopback1
 ip address 6.6.55.5 255.255.255.0

ntp server 6.6.146.8

ip domain name ipexpert.com

crypto key generate rsa general-keys label VPNKEY exportable modulus 4096

crypto pki trustpoint VPNTRUST
 enrollment url http://6.6.146.8:80
 usage ike
 fqdn R5.ipexpert.com
 password 7 011A1601431B031D351D1C5A
 subject-name CN=R5.ipexpert.com,O=IPexpert,OU=Security Training,L=San
 Jose,ST=CA,C=US
 revocation-check crl
 rsakeypair VPNKEY
 hash sha512

crypto isakmp identity dn

ip access-list extended PROXYACL
 permit ip 6.6.55.0 0.0.0.255 10.1.1.0 0.0.0.255

crypto ipsec transform-set SET3 esp-aes esp-sha-hmac
```

```
crypto map MAP3 10 ipsec-isakmp
 set peer 6.6.146.30
 set transform-set SET3
 match address PROXYACL

int f0/0
 crypto map MAP3
```

ASA3

```
ntp server 10.1.1.8

access-list OUTSIDE_IN per tcp any host 10.1.1.8 eq 80
access-list OUTSIDE_IN per udp any host 10.1.1.8 eq 123

object network NONAT
 subnet 10.1.1.0 255.255.255.0
object network VPNNET5
 subnet 6.6.55.0 255.255.255.0

nat (in,out) 1 source static NONAT NONAT destination static VPNNET5
VPNNET5

domain-name ipexpert.com
!
cry key generate rsa label VPNKEY mod 2048

crypto ca trustpoint VPNTRUST
 revocation-check crl
 enrollment url http://10.1.1.8:80
 fqdn ASA.ipexpert.com
 keypair VPNKEY
 subject-name CN=ASA.ipexpert.com, O=IPexpert, OU=CCIE Training, L=San
 Francisco, ST=CA, C=US
 password ipexpert123
!
crypto ca authenticate VPNTRUST
crypto ca enroll VPNTRUST

crypto isakmp policy 10
 authentication rsa-sig
```

```
 encryption aes
 hash sha
 group 5
!
cry ikev1 enable outside
!
tunnel-group "Security Training" type ipsec-l2l
tunnel-group "Security Training" ipsec-attributes
 ikev1 trust-point VPNTRUST
!
crypto ipsec transform-set SET3 esp-aes esp-sha-hmac
!
access-l PROXYACL permit ip 10.1.1.0 255.255.255.0 6.6.55.0 255.255.255.0
!
crypto map L2L 10 match address PROXYACL
crypto map L2L 10 set peer 6.6.156.5
crypto map L2L 10 set transform-set SET3
crypto map L2L 10 set trustpoint VPNTRUST
crypto map L2L interface outside
```

Since the first default ISAKMP Policy on R5 negotiates RSA Signatures we need to setup R8 as IOS CA.

It takes a while to generate 4096 bit key pair, this is all perfectly fine.

Some additional options were set for the CA, not needed by the task, just to show you the configuration syntax.

Don't forget about NAT Exemption that in the newer code versions was replaced by Static Identity NAT.

Verification

This is how you can check the default policies on IOS :

```
R5#sh cry isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128
bit keys).
```

```
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128
bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128
bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128
bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
```

```
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Before you bring up the tunnel check if the devices can reach each other and also if the time sync and certificates are in place:

```
R5#ping 6.6.146.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.146.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R5#sh ntp status
Clock is synchronized, stratum 3, reference is 6.6.146.8
nominal freq is 250.0000 Hz, actual freq is 249.9928 Hz, precision is
2**24
reference time is D53B7B3C.3F934BC6 (14:46:20.248 UTC Mon May 13 2013)
clock offset is -0.0008 msec, root delay is 2.74 msec
root dispersion is 940.67 msec, peer dispersion is 438.90 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000028488
s/s
system poll interval is 64, last update was 119 sec ago.

ASA(config)# sh ntp status
Clock is synchronized, stratum 3, reference is 10.1.1.8
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is d53b7b6f.d348f903 (14:47:11.825 UTC Mon May 13 2013)
clock offset is -15.6385 msec, root delay is 1.28 msec
root dispersion is 157.01 msec, peer dispersion is 140.90 msec

R5#sh cry pki cer ver VPNTRUST
Certificate
  Status: Available
  Version: 3
```

```
    Certificate Serial Number (hex): 02
    Certificate Usage: General Purpose
    Issuer:
      cn=R8 CA
      o=IPexpert
      ou=Instructors
      l=Warsaw
      c=PL
    Subject:
      Name: R5.ipexpert.com
      hostname=R5.ipexpert.com
      cn=R5.ipexpert.com
      o=IPexpert
      ou=Security Training
      l=San Jose
      st=CA
      c=US
    Validity Date:
      start date: 14:50:51 UTC May 13 2013
      end   date: 14:50:51 UTC May 13 2014
    Subject Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (4096 bit)
    Signature Algorithm: SHA512 with RSA Encryption
    Fingerprint MD5: 53BBE9C0 DC7919B9 DCCEDB68 FB4D3474
    Fingerprint SHA1: 5E6F4EA4 EC3268FE 95D89F90 A61568AA 46D87B10
    X509v3 extensions:
      X509v3 Key Usage: A0000000
        Digital Signature
        Key Encipherment
      X509v3 Subject Key ID: 4913EF7D 84F6603F E4BDEA41 D8591967 26D52F9B
      X509v3 Authority Key ID: B6154ED8 2F852904 0A38D8F1 D43B98E6 02539CD0
      Authority Info Access:
    Associated Trustpoints: VPNTRUST
    Key Label: VPNKEY

  CA Certificate
    Status: Available
    Version: 3
    Certificate Serial Number (hex): 01
```

```
    Certificate Usage: Signature
    Issuer:
      cn=R8 CA
      o=IPexpert
      ou=Instructors
      l=Warsaw
      c=PL
    Subject:
      cn=R8 CA
      o=IPexpert
      ou=Instructors
      l=Warsaw
      c=PL
    Validity Date:
      start date: 14:37:03 UTC May 13 2013
      end   date: 14:37:03 UTC May 12 2016
    Subject Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (4096 bit)
    Signature Algorithm: SHA512 with RSA Encryption
    Fingerprint MD5: 2CCECAD8 3227BED0 E7789E25 7717CA4D
    Fingerprint SHA1: 243DF4B4 2696762A F9674CFB 57C39839 9E20B6AB
    X509v3 extensions:
      X509v3 Key Usage: 86000000
        Digital Signature
        Key Cert Sign
        CRL Signature
      X509v3 Subject Key ID: B6154ED8 2F852904 0A38D8F1 D43B98E6 02539CD0
      X509v3 Basic Constraints:
          CA: TRUE
      X509v3 Authority Key ID: B6154ED8 2F852904 0A38D8F1 D43B98E6 02539CD0
      Authority Info Access:
    Associated Trustpoints: VPNTRUST

ASA(config)# sh cry ca certificates
Certificate
    Status: Available
    Certificate Serial Number: 03
    Certificate Usage: General Purpose
    Public Key Type: RSA (2048 bits)
```

```
    Signature Algorithm: SHA512 with RSA Encryption
    Issuer Name:
      cn=R8 CA
      o=IPexpert
      ou=Instructors
      l=Warsaw
      c=PL
    Subject Name:
      hostname=ASA.ipexpert.com
      cn=ASA.ipexpert.com
      o=IPexpert
      ou=CCIE Training
      l=San Francisco
      st=CA
      c=US
    Validity Date:
      start date: 14:55:32 UTC May 13 2013
      end   date: 14:55:32 UTC May 13 2014
    Associated Trustpoints: VPNTRUST

  CA Certificate
    Status: Available
    Certificate Serial Number: 01
    Certificate Usage: Signature
    Public Key Type: RSA (4096 bits)
    Signature Algorithm: SHA512 with RSA Encryption
    Issuer Name:
      cn=R8 CA
      o=IPexpert
      ou=Instructors
      l=Warsaw
      c=PL
    Subject Name:
      cn=R8 CA
      o=IPexpert
      ou=Instructors
      l=Warsaw
      c=PL
    Validity Date:
      start date: 14:37:03 UTC May 13 2013
```

```
    end   date: 14:37:03 UTC May 12 2016
  Associated Trustpoints: VPNTRUST
```

Ping from R5's loopback 1 and see if the tunnel comes up:

```
R5#ping 10.1.1.8 so loop1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.8, timeout is 2 seconds:
Packet sent with a source address of 6.6.55.5
.....
Success rate is 0 percent (0/5)
```

Not really. If you take a look at debugs there will be some retransmissions taking place in the background. Hopefully you have enabled logging on the ASA and see these messages:

```
%ASA-4-209005: Discard IP fragment set with more than 1 elements:  src =
6.6.156.5, dest = 6.6.146.30, proto = UDP, id = 52205
%ASA-4-209005: Discard IP fragment set with more than 1 elements:  src =
6.6.156.5, dest = 6.6.146.30, proto = UDP, id = 52210
%ASA-4-209005: Discard IP fragment set with more than 1 elements:  src =
6.6.156.5, dest = 6.6.146.30, proto = UDP, id = 52216
```

Change the fragment size to be 2 on the outside (you could talk to the Proctor about that):

```
ASA(config)# fragment chain 2 outside
```

If the tunnel is still not established and you see the following messages it means R8 has some problems with internal HTTP server (probably related to the key size and hashing function selected) and will not return the CRL to R5 when validating ASA's cert:

```
May 13 15:57:28.730: CRYPTO_PKI: Socket timeout
May 13 15:57:28.730: %PKI-3-SOCKETSELECT: Failed to select the socket.
May 13 15:57:28.730: CRYPTO_PKI: Certificate validation failed
May 13 15:57:28.734: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from
6.6.146.30 is bad: CA request failed!
May 13 15:57:29.738: CRYPTO_PKI: Adding peer certificate
May 13 15:57:29.750: %CRYPTO-3-IKMP_QUERY_KEY: Querying key pair failed.

R5(config)# crypto pki trustpoint VPNTRUST
R5(ca-trustpoint)#revocation-check none
```

Note the ASA did not have any problems with getting the CRL:

```
ASA(config)# sh cry ca crls

CRL Issuer Name:
    cn=R8 CA,o=IPexpert,ou=Instructors,l=Warsaw,c=PL
    LastUpdate: 14:37:08 UTC May 13 2013
    NextUpdate: 20:37:08 UTC May 13 2013
    Cached Until: 17:15:24 UTC May 13 2013
    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP
    Size (bytes): 673
    Last used at: 16:39:02 UTC May 13 2013
    Associated Trustpoints: VPNTRUST


R5#ping 10.1.1.8 so loop1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.8, timeout is 2 seconds:
Packet sent with a source address of 6.6.55.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R5#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: FastEthernet0/0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 6.6.146.30 port 500 fvrf: (none) ivrf: (none)
      Phase1_id:
hostname=ASA.ipexpert.com,cn=ASA.ipexpert.com,o=IPexpert,ou=CCIE
Training,l=San
      Desc: (none)
  IKEv1 SA: local 6.6.156.5/500 remote 6.6.146.30/500 Active
          Capabilities:(none) connid:1001 lifetime:23:58:54
  IPSEC FLOW: permit ip 6.6.55.0/255.255.255.0 10.1.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

```
          Inbound:  #pkts dec'ed 7 drop 0 life (KB/Sec) 4552653/3538
          Outbound: #pkts enc'ed 7 drop 3 life (KB/Sec) 4552653/3538

ASA(config)# sh vpn-sessiondb det l2l

Session Type: LAN-to-LAN Detailed

Connection   : Security Training
Index        : 30                    IP Addr      : 6.6.156.5
Protocol     : IKEv1 IPsec
Encryption   : AES128                Hashing      : SHA1
Bytes Tx     : 700                   Bytes Rx     : 700
Login Time   : 16:39:02 UTC Mon May 13 2013
Duration     : 0h:01m:23s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 30.1
  UDP Src Port : 500                 UDP Dst Port : 500
  IKE Neg Mode : Main                Auth Mode    : rsaCertificate
  Encryption   : AES128              Hashing      : SHA1
  Rekey Int (T): 86400 Seconds       Rekey Left(T): 86316 Seconds
  D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 30.2
  Local Addr   : 10.1.1.0/255.255.255.0/0/0
  Remote Addr  : 6.6.55.0/255.255.255.0/0/0
  Encryption   : AES128              Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds        Rekey Left(T): 3516 Seconds
  Rekey Int (D): 4608000 K-Bytes     Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes          Idle TO Left : 28 Minutes
  Bytes Tx     : 700                 Bytes Rx     : 700
  Pkts Tx      : 7                   Pkts Rx      : 7

NAC:
```

```
    Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
    SQ Int (T)   : 0 Seconds              EoU Age(T)   : 84 Seconds
    Hold Left (T): 0 Seconds              Posture Token:
    Redirect URL :
```

Task 4.4: GRE (4 Points)

- Configure R4 and R2 to encrypt traffic between the Extranet and VLAN 2
- Use pre-shared key authentication, but you cannot use the IP address to identify the key of each peer. You must use the hostname of each device.
- You may not use the command “ip host” on either device
- Compress the traffic between R2 and R4 including multicast packets
- Use Network 6.6.24.0/24 for this Connection
- EIGRP has been pre-configured for you to run over this tunnel. Do not make changes to the pre-configured EIGRP

Detailed Solution

R1

```
ip host R2.ipexpert.com 6.6.25.2
ip host R4.ipexpert.com 6.6.146.4
ip dns server
```

R2

```
ip domain-name ipexpert.com
ip name-server 192.1.49.1
ip domain-lookup
!
cry isa pol 20
 auth pre
 enc 3des
 gr 2

crypto isakmp key cisco hostname R4.ipexpert.com
!
crypto ipsec transform-set SET4 esp-aes esp-sha-hmac comp-lzs
 mode transport
!
crypto isakmp profile ISA_PROF4
   match identity host R4.ipexpert.com
```

```
   initiate mode aggressive
   self-identity fqdn
   keyring default

crypto ipsec profile IPSEC_PROF4
 set transform-set SET4
 set isakmp-profile ISA_PROF4
!
interface Tunnel24
 ip address 6.6.24.2 255.255.255.0
 tunnel source Serial0/1/0
 tunnel destination 6.6.146.4
 tunnel protection ipsec profile IPSEC_PROF4
```

R4

```
ip domain-name ipexpert.com
ip name-server 192.1.49.1
ip domain-lookup
!
cry isa pol 5
 auth pre
 enc 3des
 gr2

crypto isakmp key cisco hostname R2.ipexpert.com
!
crypto ipsec transform-set SET4 esp-aes esp-sha-hmac comp-lzs
 mode transport
!
crypto isakmp profile ISA_PROF4
   match identity host R2.ipexpert.com
   initiate mode aggressive
   self-identity fqdn
   keyring default

crypto ipsec profile IPSEC_PROF4
 set transform-set SET4
 set isakmp-profile ISA_PROF4
!
```

```
interface Tunnel24
 ip address 6.6.24.4 255.255.255.0
 tunnel source F0/0
 tunnel destination 6.6.25.2
 tunnel protection ipsec profile IPSEC_PROF4
```

We are not allowed to use the “address” keyword when working with the pre-shared keys. That is not too bad. Pretty easy to change them to the hostnames. What you may not have been aware of prior to this, though, is the fact that to use hostnames with the pre-shared keys, you will need to set it to Aggressive Mode for negotiation as well. Main mode isn’t supported using the hostname.

So, using the hostname means we will need to configure the two devices to resolve the hostname of each device for negotiation. The question states we cannot use the command “ip host” on either R2 or R4. All that means, though, is that we cannot do it on those two routers. The question didn’t state that we couldn’t do it on any router. So pick another router, and make it a DNS server so that we can finish this task. We chose R1.

Using the “comp-lzs” option on the end of the transform-set tells the IPSec phase 2 negotiation that we want to configure the tunnel to compress traffic after encryption and authentication have been completed for the traffic going through the tunnel.

Verification

This is how you can check the default policies on IOS:

```
R4#sh cry isa key
Keyring      Hostname/Address                              Preshared Key

default      6.6.146.9                                     ipexpert
             R2.ipexpert.com                               cisco

R4#sh cry sess int tu 24 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: Tunnel24
```

```
Profile: ISA_PROF4
Uptime: 00:00:14
Session status: UP-ACTIVE
Peer: 6.6.25.2 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: R2.ipexpert.com
      Desc: (none)
  IKEv1 SA: local 6.6.146.4/500 remote 6.6.25.2/500 Active
          Capabilities:(none) connid:1003 lifetime:23:59:45
  IKEv1 SA: local 6.6.146.4/500 remote 6.6.25.2/500 Inactive
          Capabilities:(none) connid:1002 lifetime:0
  IPSEC FLOW: permit 47 host 6.6.146.4 host 6.6.25.2
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 3 drop 0 life (KB/Sec) 4497585/3585
        Outbound: #pkts enc'ed 3 drop 0 life (KB/Sec) 4497585/3585

R4#sh cry ipse sa int tu 24

interface: Tunnel24
    Crypto map tag: Tunnel24-head-0, local addr 6.6.146.4

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (6.6.146.4/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (6.6.25.2/255.255.255.255/47/0)
   current_peer 6.6.25.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
    #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 39, #pkts compr. failed: 0
    #pkts not decompressed: 40, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 6.6.146.4, remote crypto endpt.: 6.6.25.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xFBB07838(4222646328)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x344657C9(877025225)
        transform: esp-aes esp-sha-hmac ,
```

```
         in use settings ={Transport, }
         conn id: 2005, flow_id: NETGX:5, sibling_flags 80000006, crypto
map: Tunnel24-head-0
         sa timing: remaining key lifetime (k/sec): (4497580/3416)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:
       spi: 0xA6CE(42702)
         transform: comp-lzs ,
         in use settings ={Transport, }
         conn id: 2005, flow_id: NETGX:5, sibling_flags 80000006, crypto
map: Tunnel24-head-0
         sa timing: remaining key lifetime (k/sec): (4497580/3416)
         replay detection support: Y
         Status: ACTIVE

      outbound esp sas:
       spi: 0xFBB07838(4222646328)
         transform: esp-aes esp-sha-hmac ,
         in use settings ={Transport, }
         conn id: 2006, flow_id: NETGX:6, sibling_flags 80000006, crypto
map: Tunnel24-head-0
         sa timing: remaining key lifetime (k/sec): (4497580/3416)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
       spi: 0x5FBF(24511)
         transform: comp-lzs ,
         in use settings ={Transport, }
         conn id: 2006, flow_id: NETGX:6, sibling_flags 80000006, crypto
map: Tunnel24-head-0
         sa timing: remaining key lifetime (k/sec): (4497580/3416)
         replay detection support: Y
```

```
          Status: ACTIVE

R2#sh ip eigrp nei
EIGRP-IPv4 Neighbors for AS(24)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
0   6.6.24.4                Tu24              13 00:05:45 1992   5000  0  1
```

Finally check if compression is working:

```
R2#ping 6.6.24.4 size 1400 rep 10

Type escape sequence to abort.
Sending 10, 1400-byte ICMP Echos to 6.6.24.4, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 28/28/32 ms

R2#sh cry ipse sa int tu 24  | in compress
     #pkts compressed: 10, #pkts decompressed: 10
     #pkts not compressed: 151, #pkts compr. failed: 0
     #pkts not decompressed: 147, #pkts decompress failed: 0
```

5.0 Identity Management (18 points)

Task 5.1: Cut-Through Proxy (4 Points)

- HTTP & HTTPs traffic sourced in Extranet destined to the ACS should be only allowed through the ASA if it is coming from an authenticated user
- Authentication should be done using RADIUS with ACS acting as an Identity Store
- User “cutproxy” with password “cisco” should be given HTTP, HTTPs and TCP 8080 access to the ACS
- If HTTP is used for the connection make sure it will be authenticated in a secure way

Detailed Solution

R4

```
ip access-list ext OUTSIDE_IN
 no deny ip any any log
 40 per tcp any host 6.6.146.100 eq 80
 50 per tcp any host 6.6.146.100 eq 443
 60 per tcp any host 6.6.146.100 eq 8080
 100 deny ip any any log
```

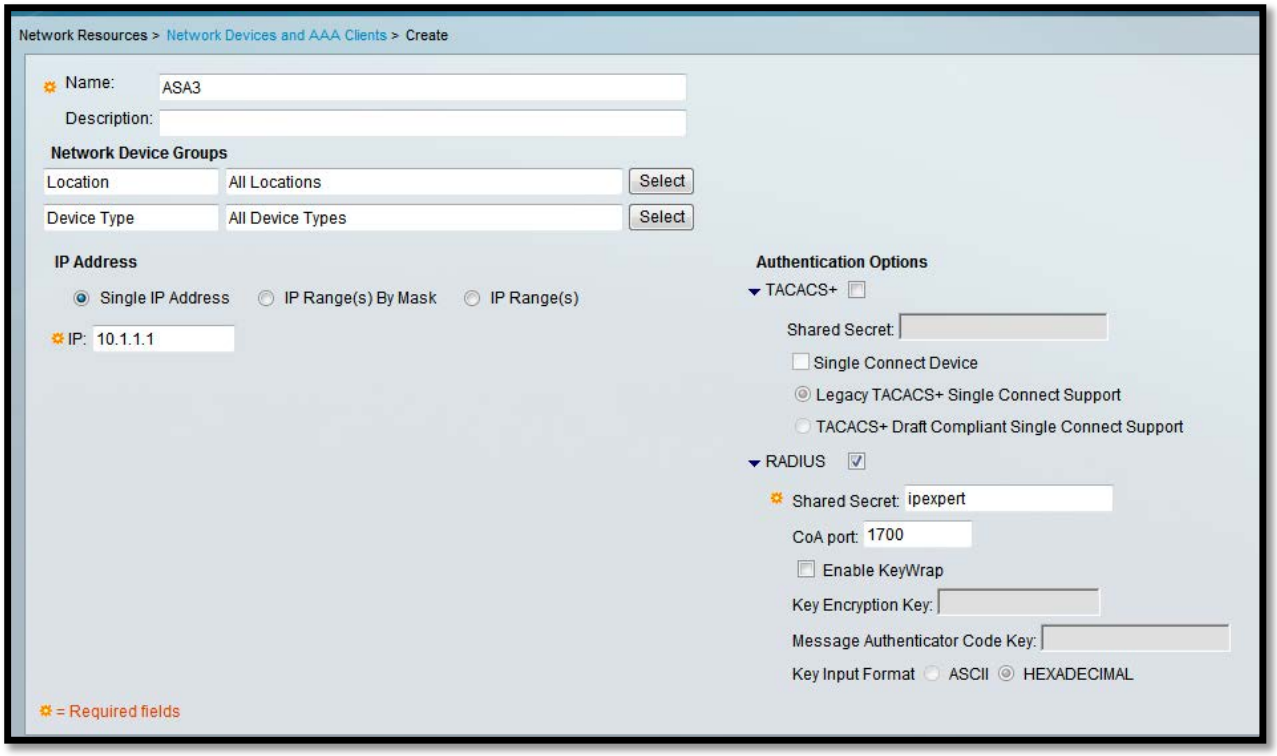
ASA3

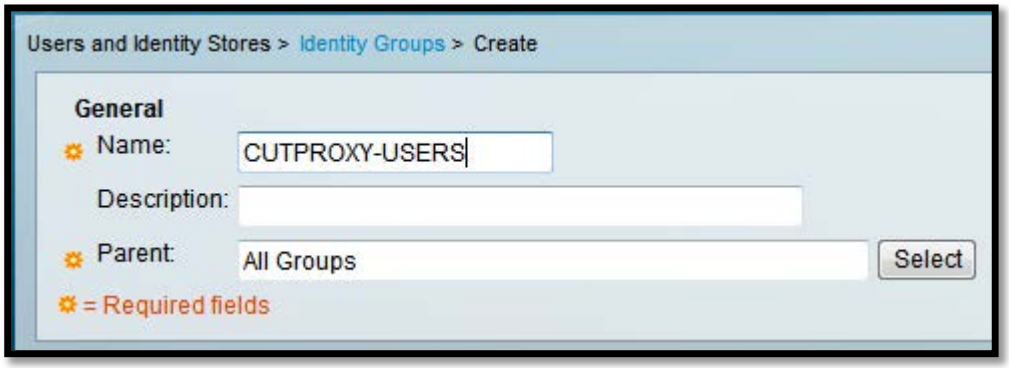
```
object-group service AUTHPROXY_PORTS tcp
 port-object eq www
 port-object eq https

access-l OUTSIDE_IN permit tcp 6.6.4.0 255.255.255.0 host 10.1.1.100
object-group AUTHPROXY_PORTS

aaa-server RAD protocol radius
aaa-server RAD (inside) host 10.1.1.100
 key ipexpert

access-list CUTP permit tcp 6.6.4.0 255.255.255.0 host 10.1.1.100 eq www
access-list CUTP permit tcp 6.6.4.0 255.255.255.0 host 10.1.1.100 eq https
aaa authentication match CUTP outside RAD

aaa authentication secure-http-client
```

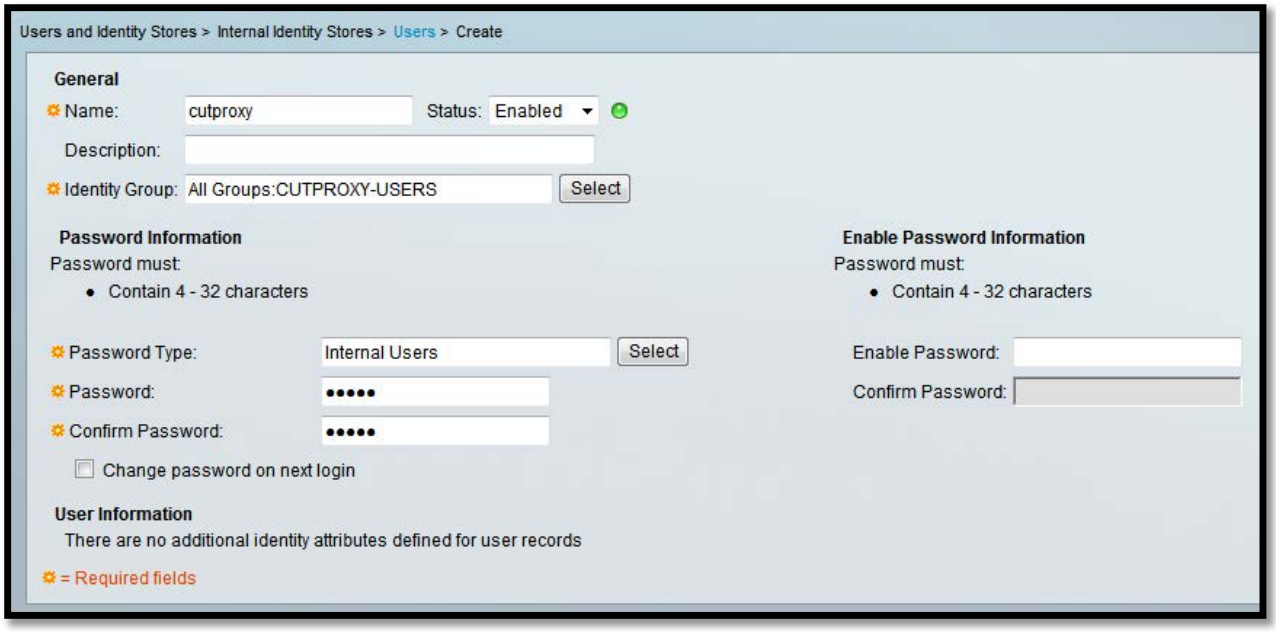
```
access-group OUTSIDE_IN in interface outside per-user-override
```

ACS

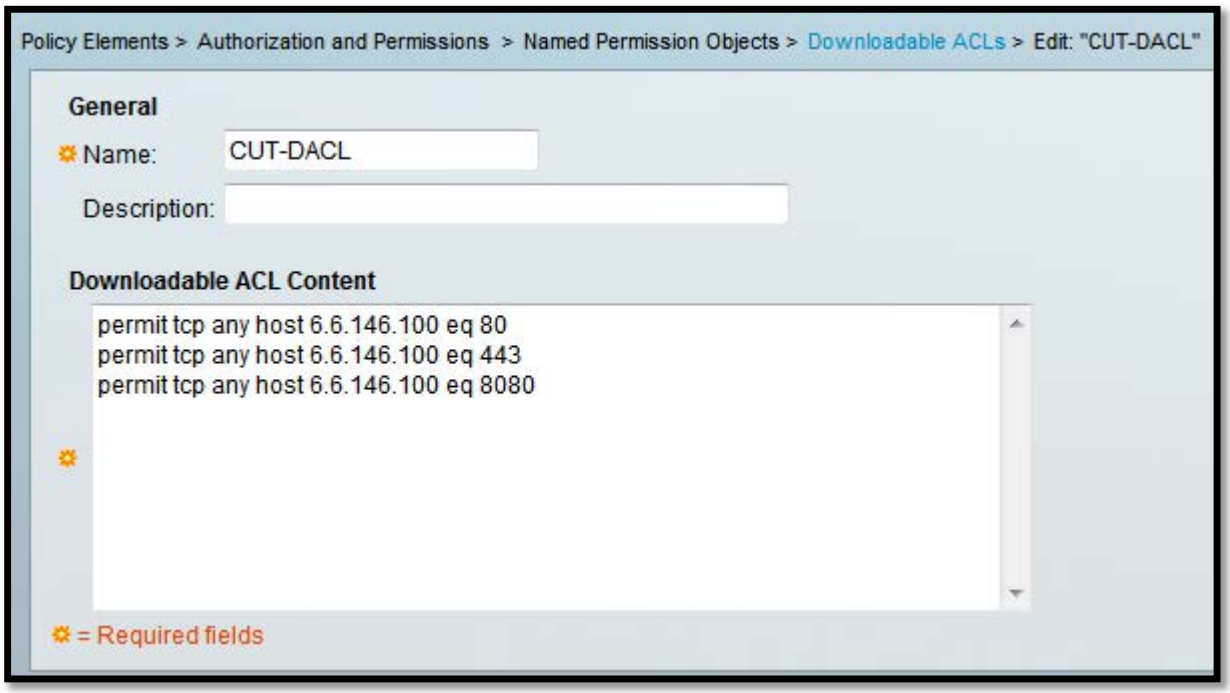
In this and few following tasks the print screens show you the exact navigation path you need to take on ACS to configure a particular element.



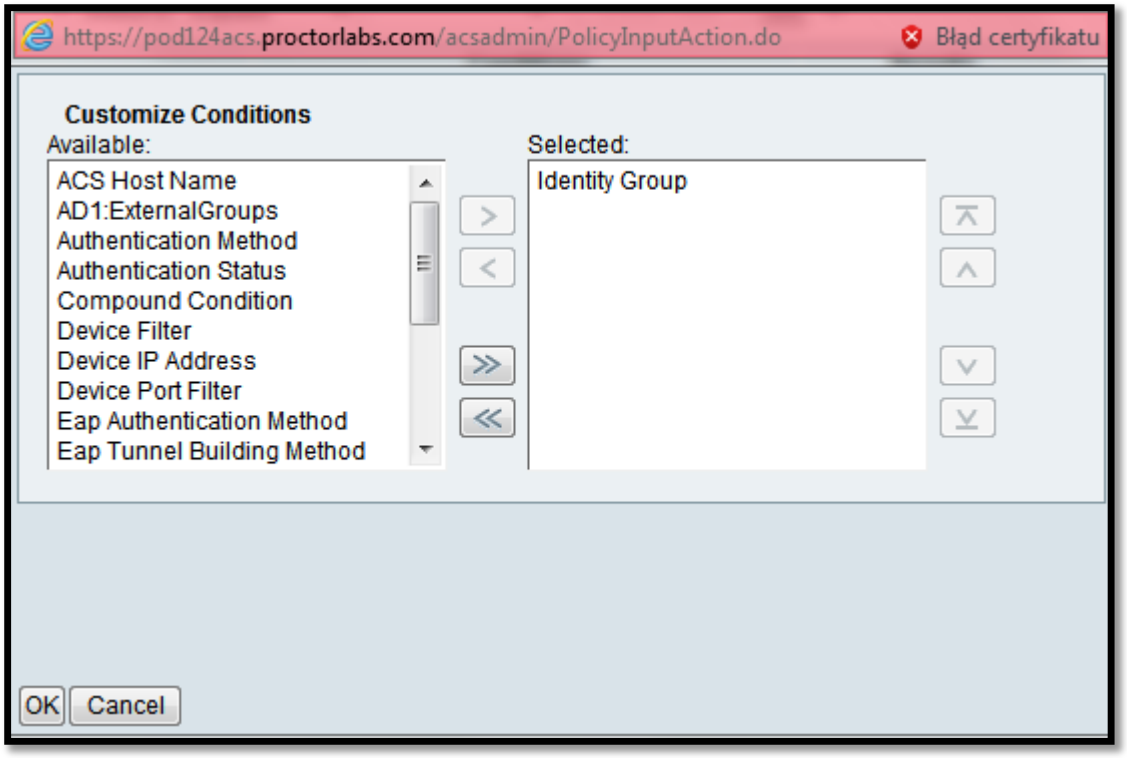




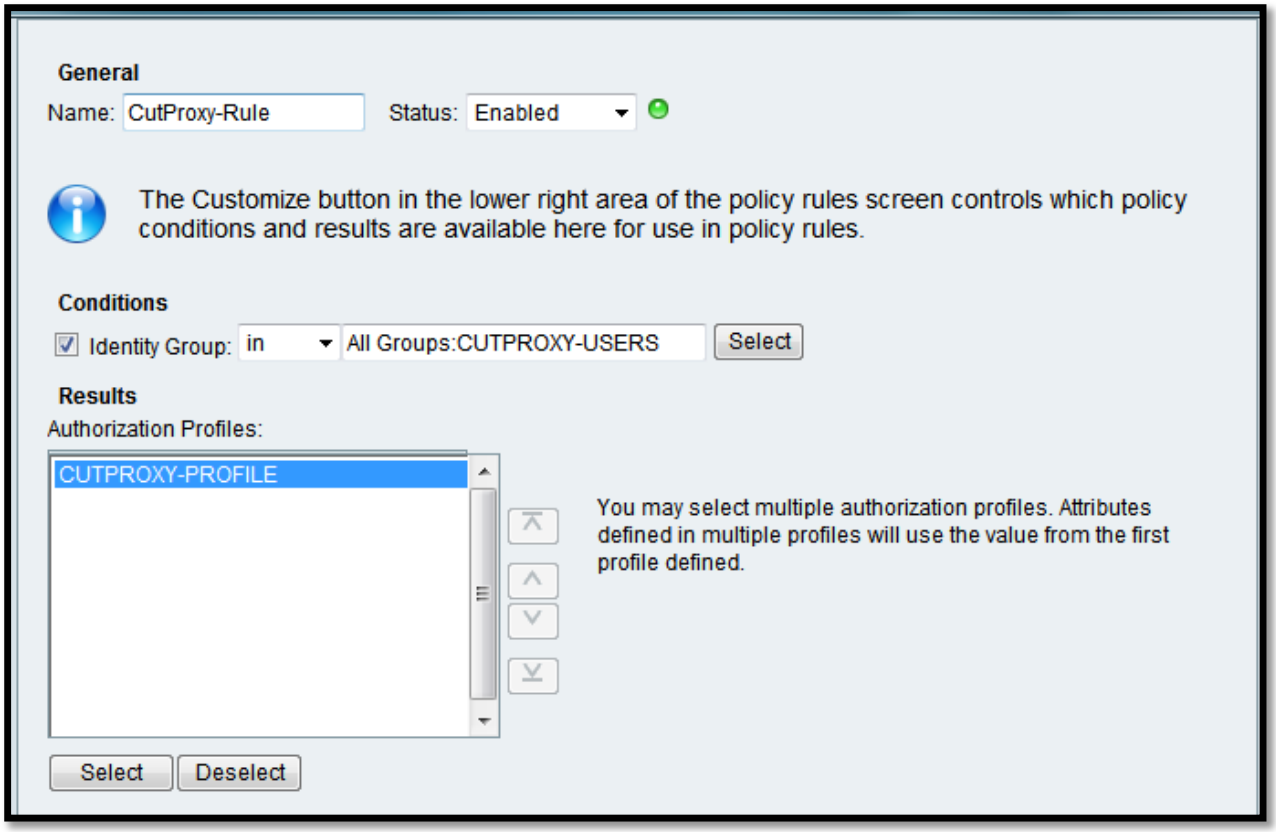
Note the dACL points to the translated, not the original addresses:



In the Authorization Policy for Default Network Access click on “Customize” and select “Identity Group” as the only condition:



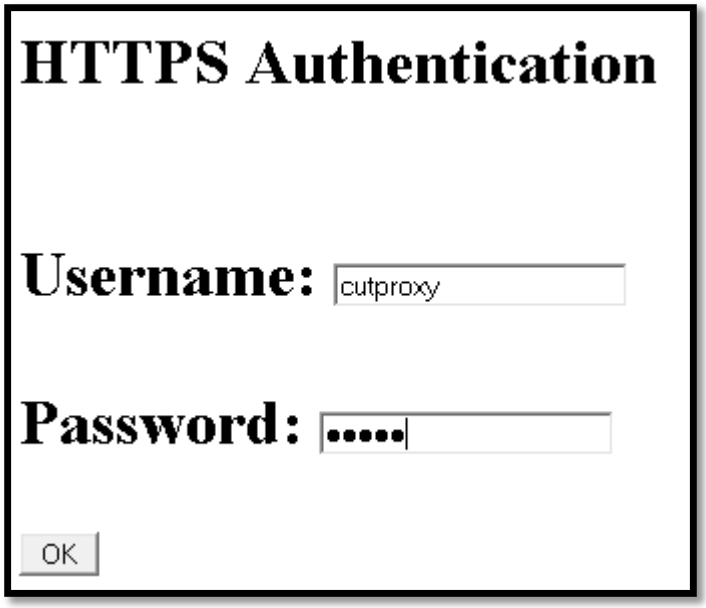
Now create a new Rule. Select the Group and AuthZ Profile:

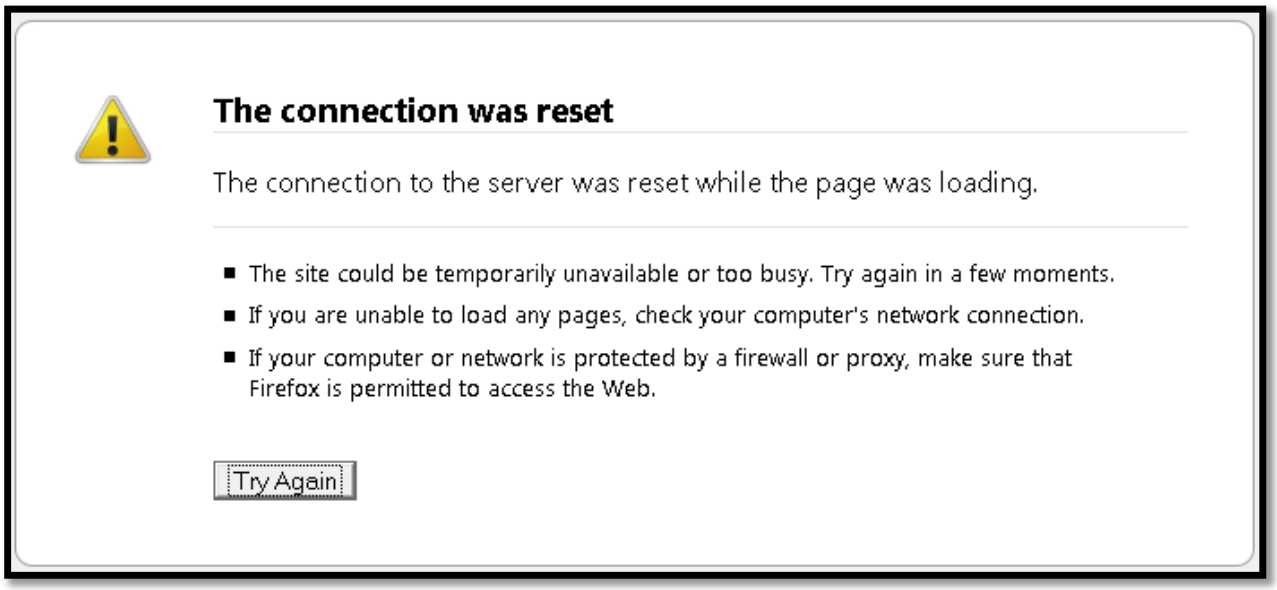


Note that the ACL downloaded from ACS must refer to the translated addresses; interface ACL points to the original ones.

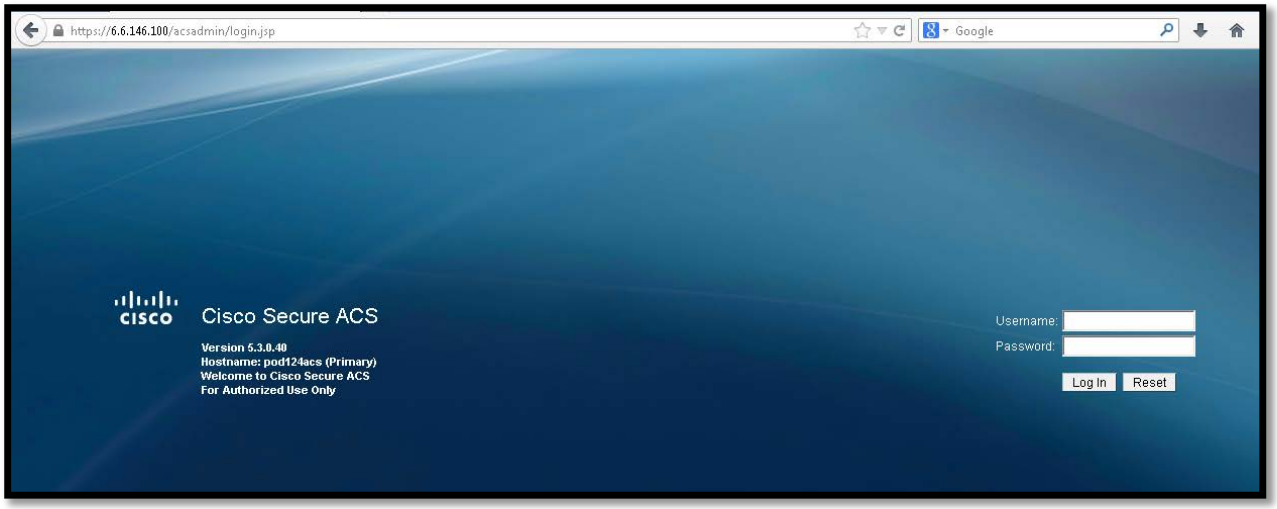
Verification

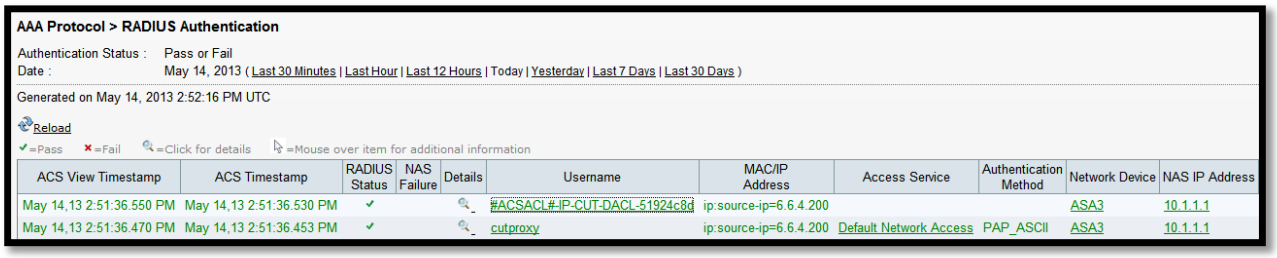
Move Test PC to VLAN 4. Add route and try to access http://6.6.146.100 to test redirection:





Now connect to https://6.6.146.100:






```
ASA(config)# sh uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          2
user 'cutproxy' at 6.6.4.200, authenticated
   access-list #ACSACL#-IP-CUT-DACL-519250a7 (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00

ASA(config)# sh access-l | in CUT-DACL
access-list #ACSACL#-IP-CUT-DACL-519250a7; 3 elements; name hash:
0x9c48d926 (dynamic)
access-list #ACSACL#-IP-CUT-DACL-519250a7 line 1 extended permit tcp any
host 6.6.146.100 eq www (hitcnt=1) 0xcb3dd88f
access-list #ACSACL#-IP-CUT-DACL-519250a7 line 2 extended permit tcp any
host 6.6.146.100 eq https (hitcnt=2) 0x9fa40e7a
access-list #ACSACL#-IP-CUT-DACL-519250a7 line 3 extended permit tcp any
host 6.6.146.100 eq 8080 (hitcnt=2) 0x458b8b7a
```

Task 5.2: Authentication Proxy (4 Points)

- Authentication Proxy should be enabled on R2 for all HTTP traffic going over TCP port 8090 sourced from VLAN 2 network
- Use ACS as the Identity Store
- Authenticated user (“authproxy” pw “cisco”) must accept the policy prior to being granted access over port 8090
- The following message should show up on the login page : “PLEASE ACCEPT THE POLICY PRIOR TO LOGIN”
- Protect RADIUS communication between ACS and R2 with key “ipexpert”

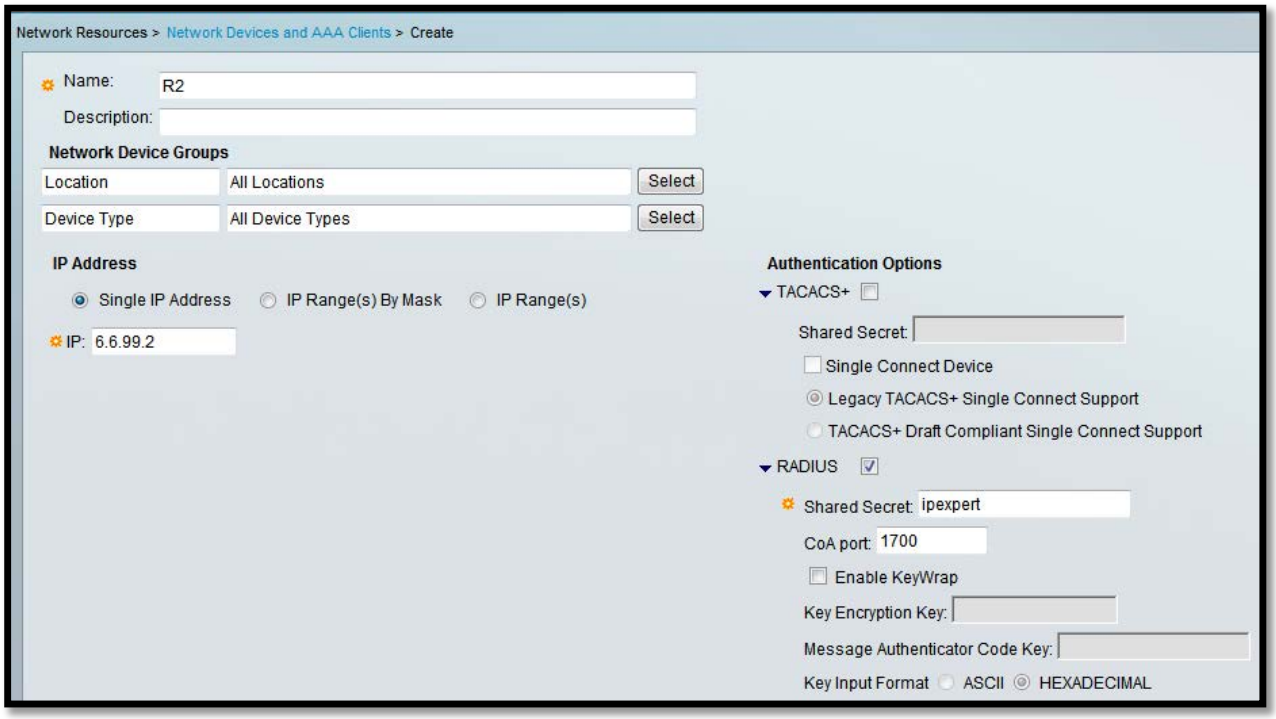
Detailed Solution

R2

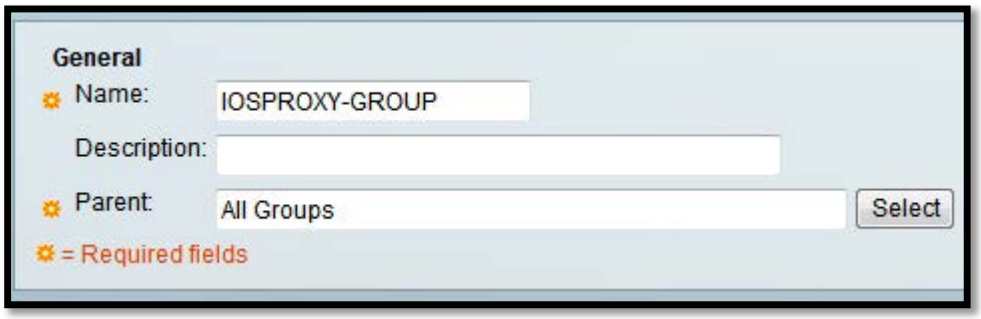
```
aaa new-model
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa authentication login NO none

line con 0
 login auth NO

access-list 160 permit tcp 6.6.2.0 0.0.0.255 any eq 8090

ip radius source-interface Loopback0
radius-server host 6.6.146.100 key ipexpert

ip access-list extended BLOCK
 deny tcp 6.6.2.0 0.0.0.255 any eq 8090
 permit ip any any

ip admission name AUTHP proxy http inactivity-time 60 list 160
ip admission name AUTHP consent inactivity-time 60 list 160
ip admissi auth-proxy-banner http ^ PLEASE ACCEPT THE POLICY PRIOR TO
LOGIN ^

ip http server
ip http port 8090
```

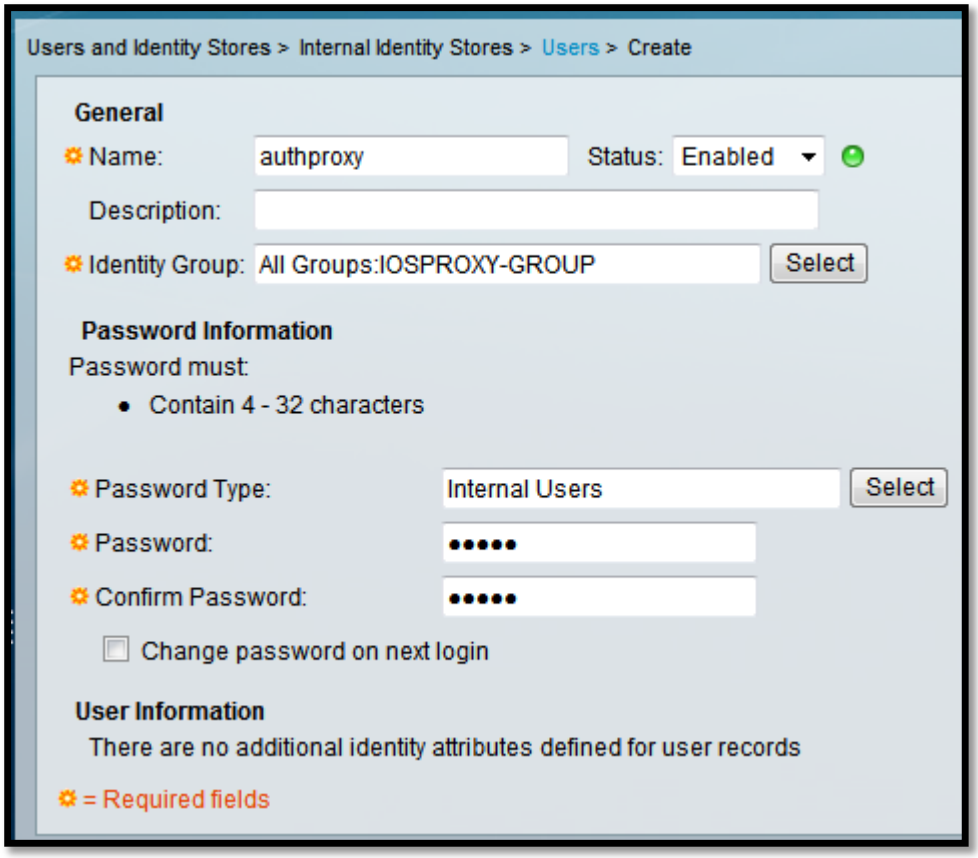
```
ip port-map http port tcp 8090

int g0/0
 ip admission AUTHP
 ip access-group BLOCK in
```

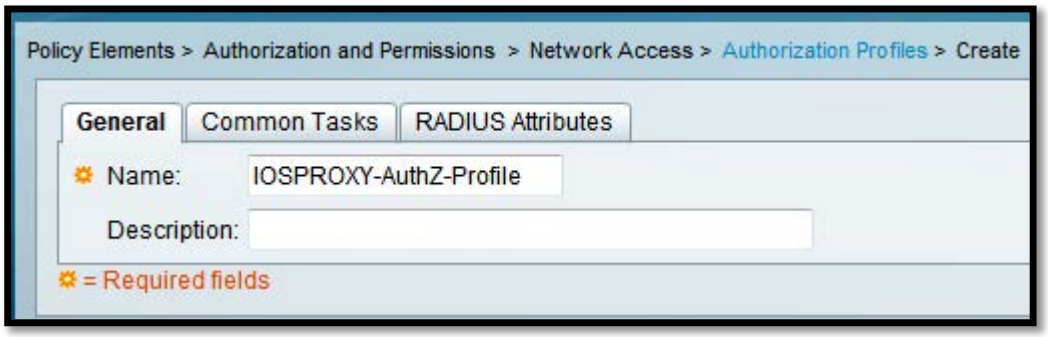
ACS

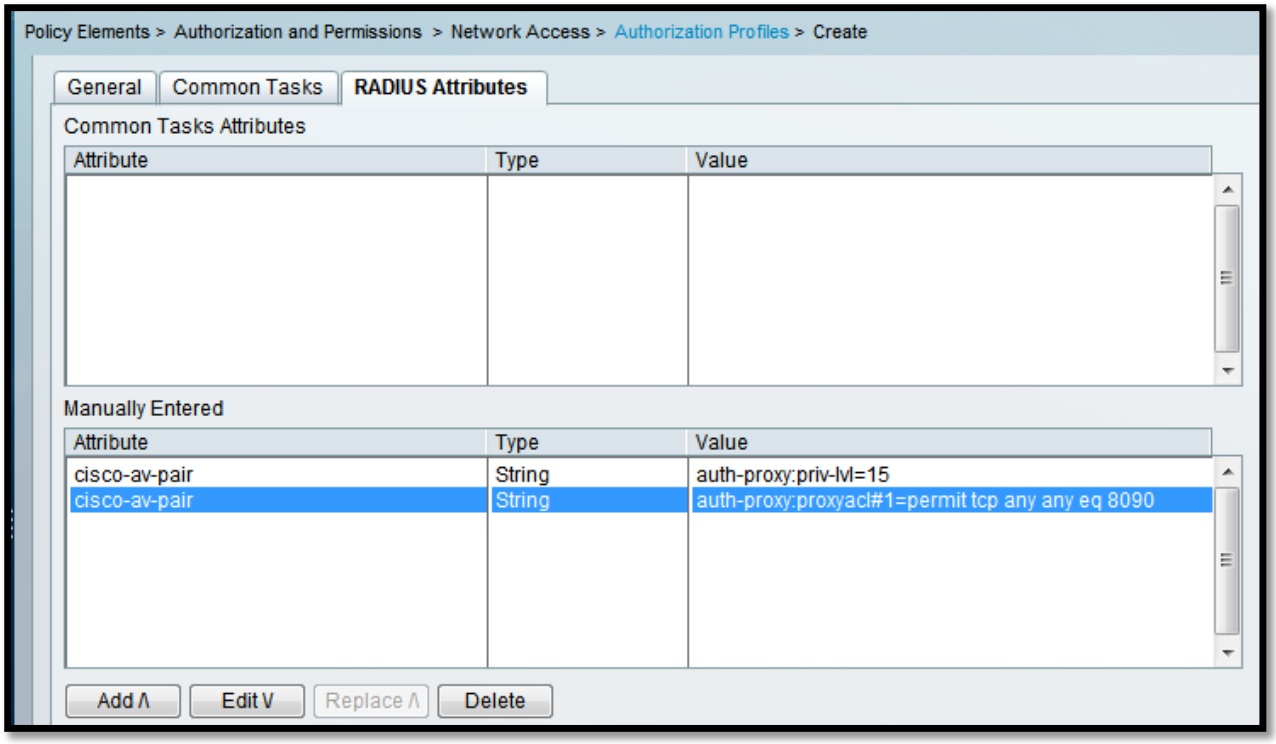


Now a new Identity Group:

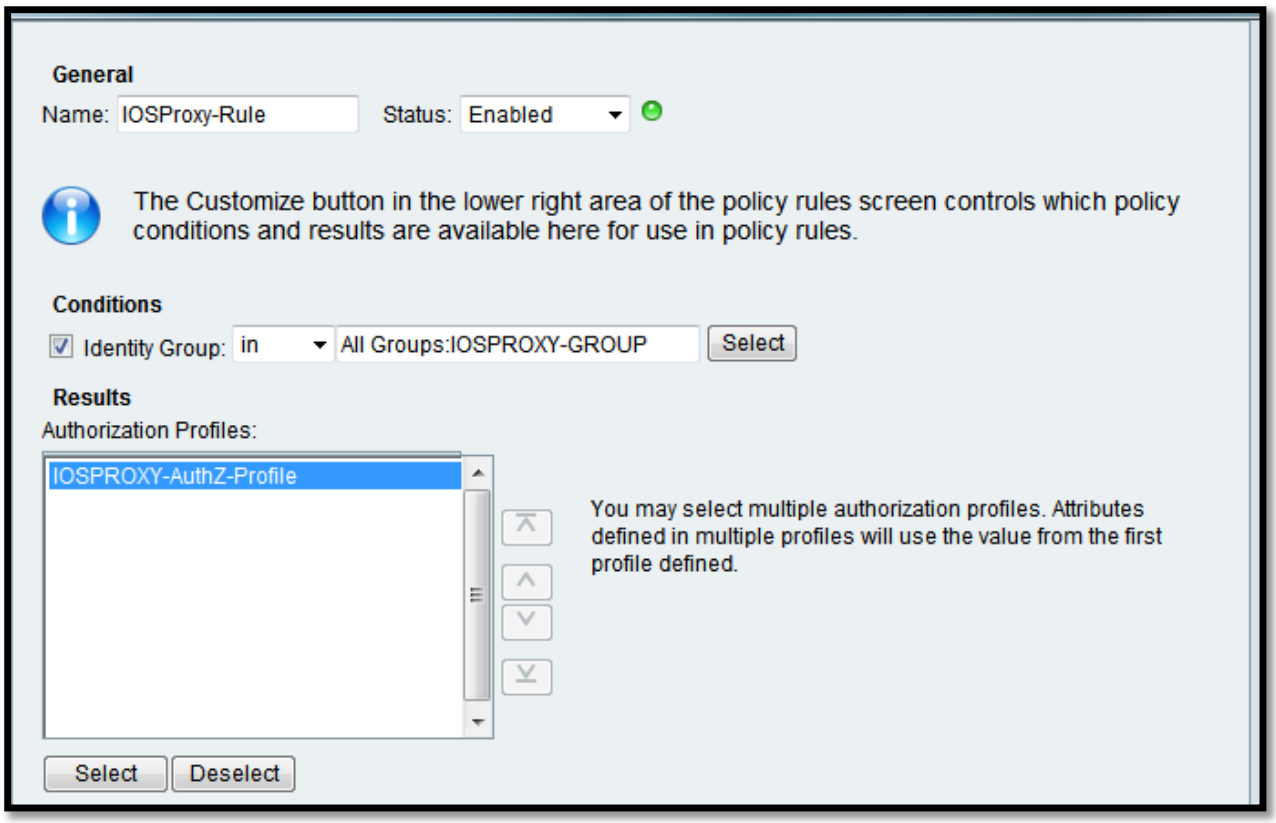


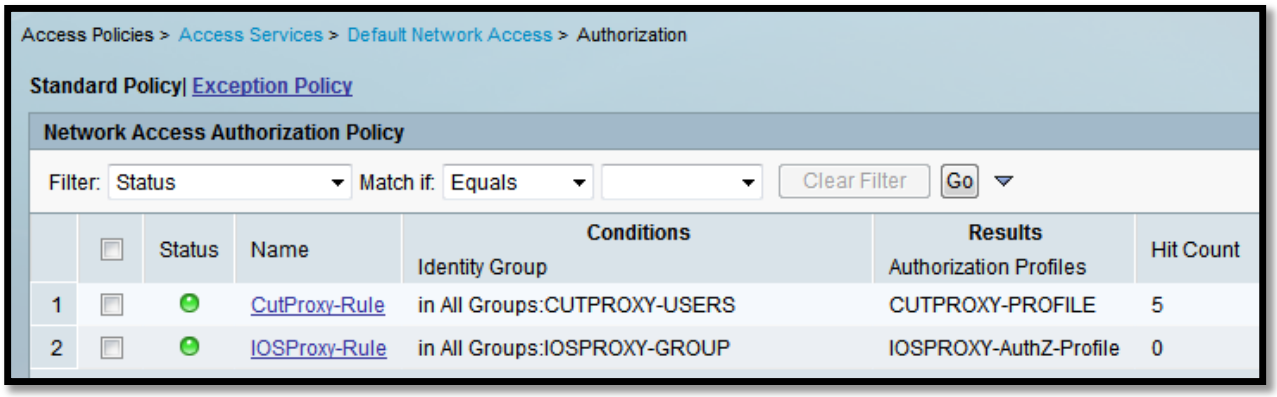






Time for the Authorization Rule for Auth Proxy:



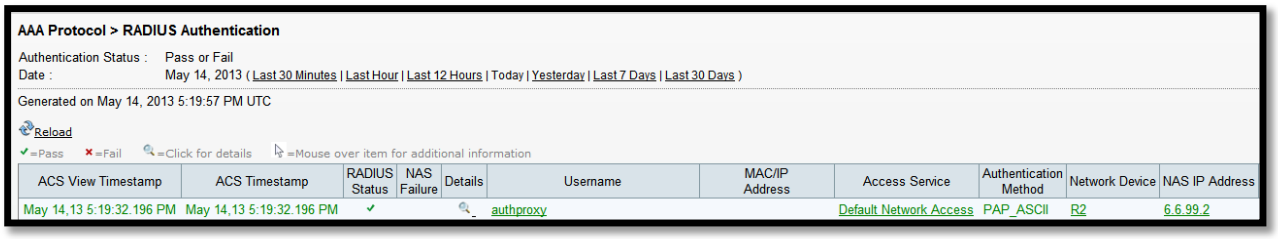


TACACS+ is not supported for Authentication Proxy with ACS 5.3 unless you have applied patch # 5.

To figure out the RADIUS attributes used and their structure (Cisco AV Pair) here, refer to the documentation: IOS 15.2 M&T -> User Services Configuration Library -> Authentication Proxy Configuration Guide.

Verification

Temporarily enable HTTP Server on R11 (change port to 8090). Move Test PC to VLAN 2 and start testing:




```
R2#sh ip admission cache
Authentication Proxy Cache
 Client Name authproxy, Client IP 6.6.2.200, Port 50377, timeout 60, Time
Remaining 60, state ESTAB
```

```
R2#sh access-l BLOCK
Extended IP access list BLOCK
     permit tcp host 6.6.2.200 any eq 8090 (5 matches)
    10 deny tcp 6.6.2.0 0.0.0.255 any eq 8090
    20 permit ip any any (251 matches)
```

Task 5.3: Device Management (6 Points)

- Configure R1 for Telnet & SSH management using TACACS+ for authentication
- All TACACS+ Shell Login requests coming from R1 should result in Privilege Level 15 access. Create a separate Access Service just for this purpose with a specific condition to meet this requirement
- Use TACACS+ to authorize each and every command
- User “admin” (pw “cisco”) should be able to issue all commands

- User “oper” (pw “cisco”) should be able to issue all show commands except “show memory”
- Connecting user should see the following prompt when authenticating : “T-username:”, “T-password:”
- Send accounting information to ACS as well
- Configure a backup solution so user “admin” can login to the router when the ACS is not available
- This configuration should not affect console access

Detailed Solution

R1

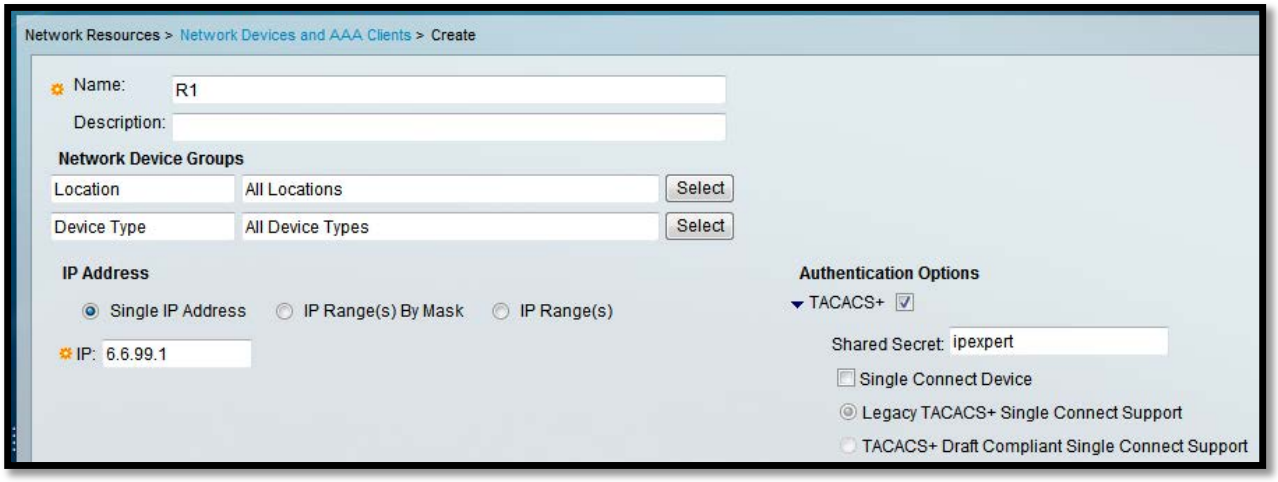
```
aaa new-model

tacacs-server host 6.6.146.100 key ipexpert
ip tacacs source-interface loop0

aaa authentication login default none
aaa authentication login AUTHC group tacacs+ local

aaa authorization exec AUTHZ group tacacs+ local

aaa authorization commands 0 CMD group tacacs+ local
aaa authorization commands 1 CMD group tacacs+ local
aaa authorization commands 15 CMD group tacacs+ local

aaa authorization config-commands

aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
line vty 0 4
 login authentication AUTHC
 authorization exec AUTHZ
 authorization commands 0 CMD
 authorization commands 1 CMD
 authorization commands 15 CMD
!
```

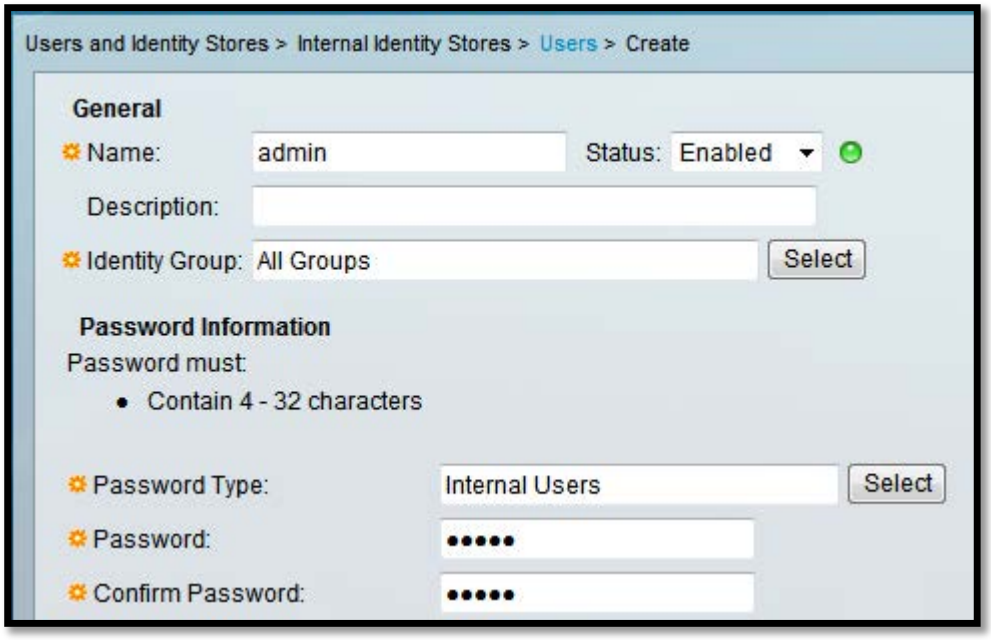
```
username admin privilege 15 password cisco
```

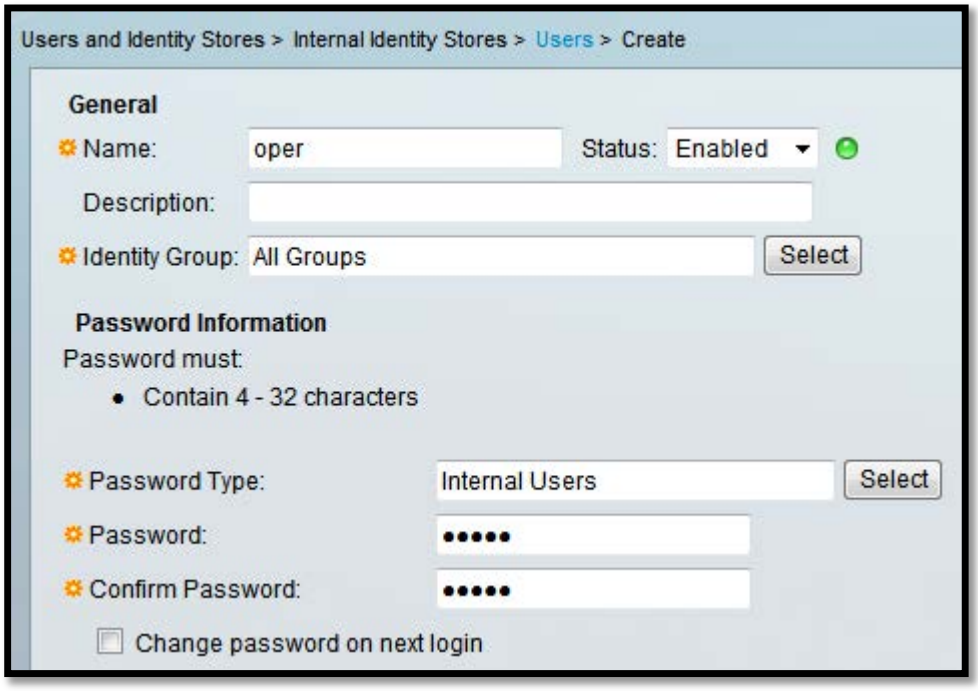
R7

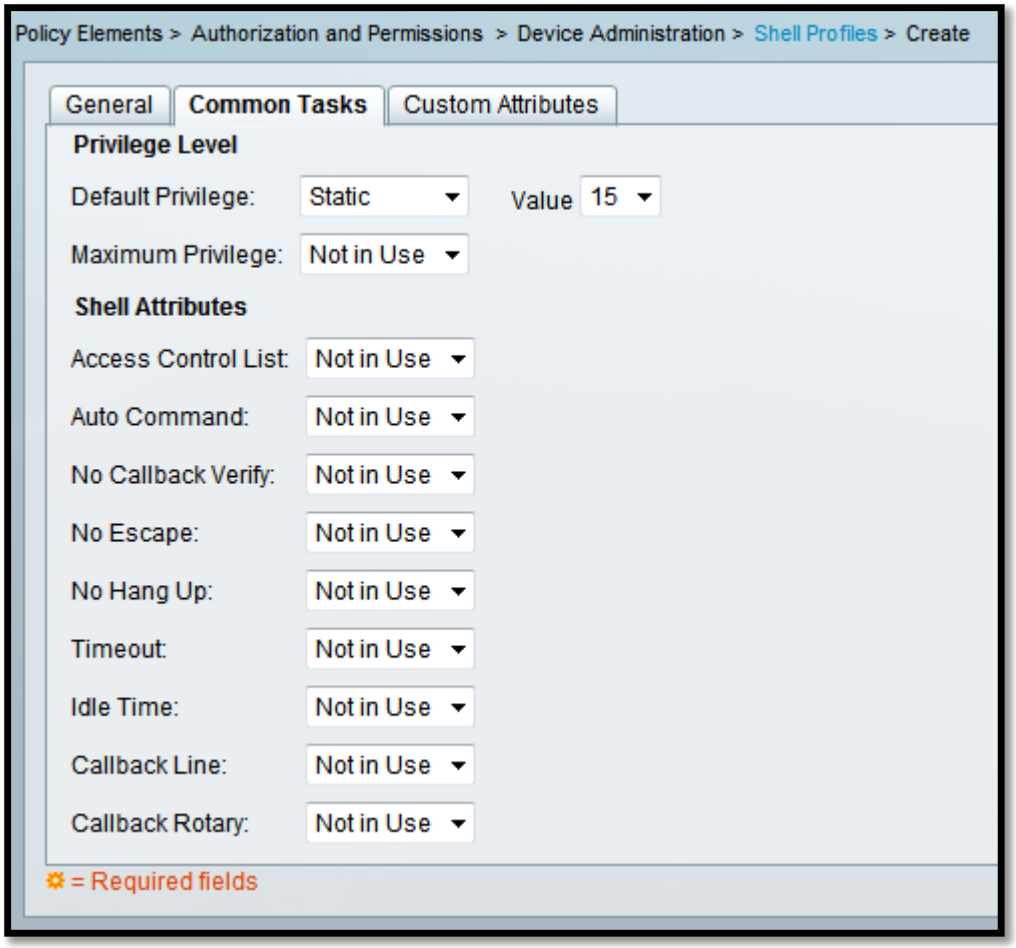
```
ip access-list extended TACACS
 permit tcp host 6.6.99.1 host 6.6.146.100 eq tacacs

class-map type inspect match-all ZFW_OUTIN_TACACS_CLASS
 match access-group name TACACS

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ZFW_OUTIN_TACACS_CLASS
  inspect
```

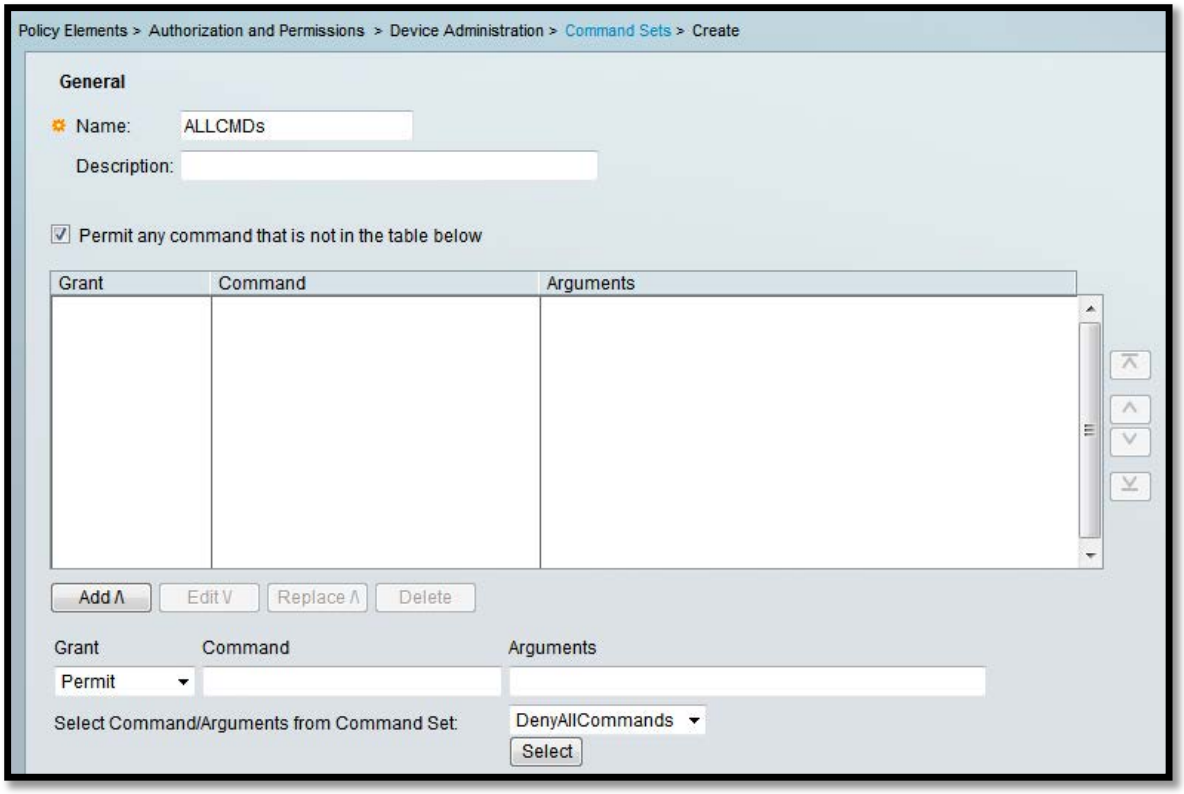
ACS

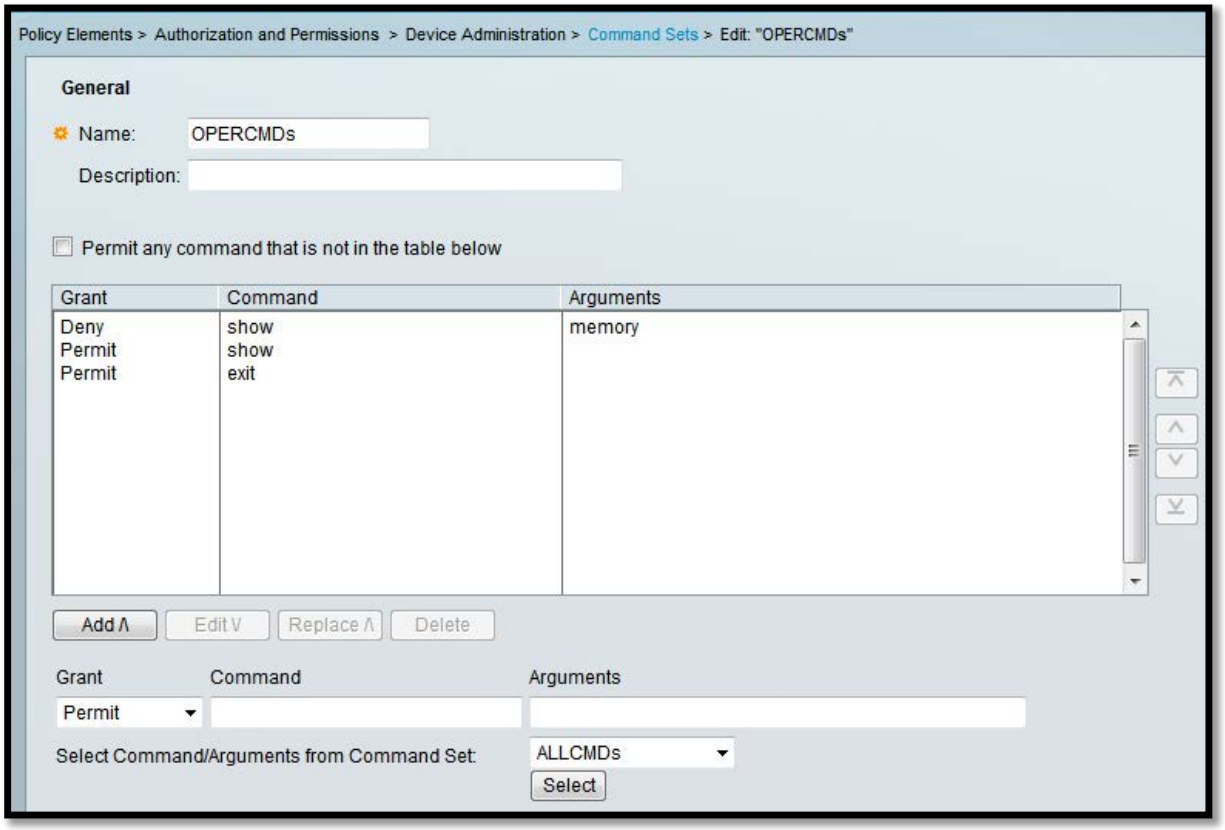




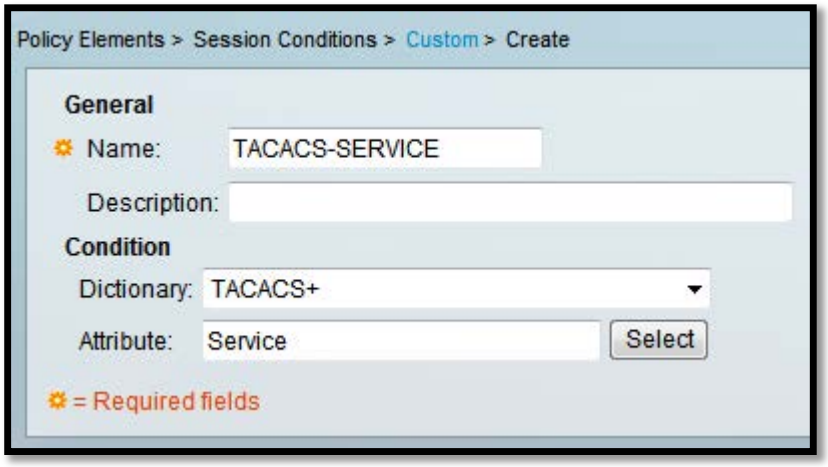


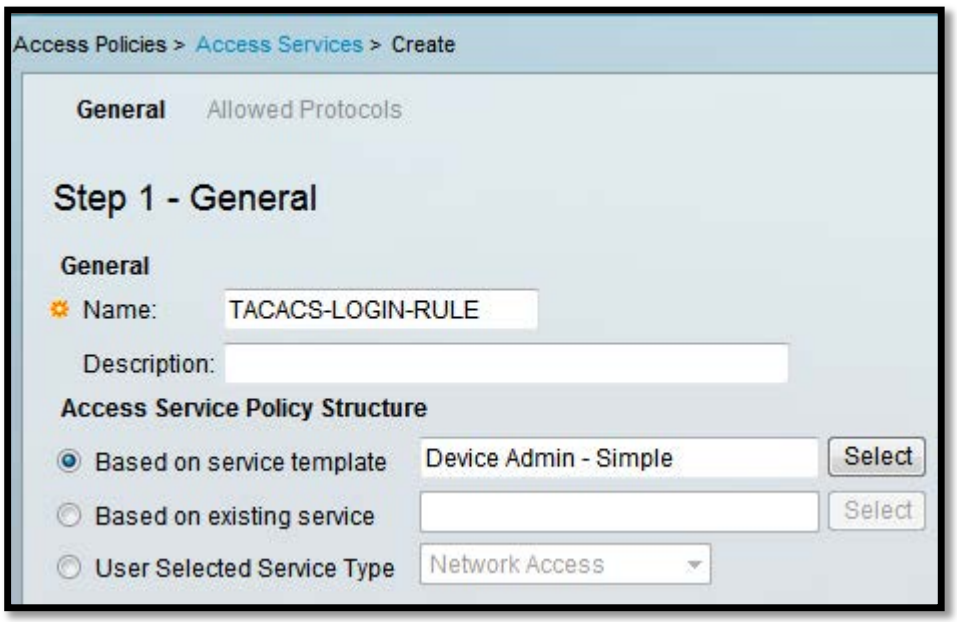




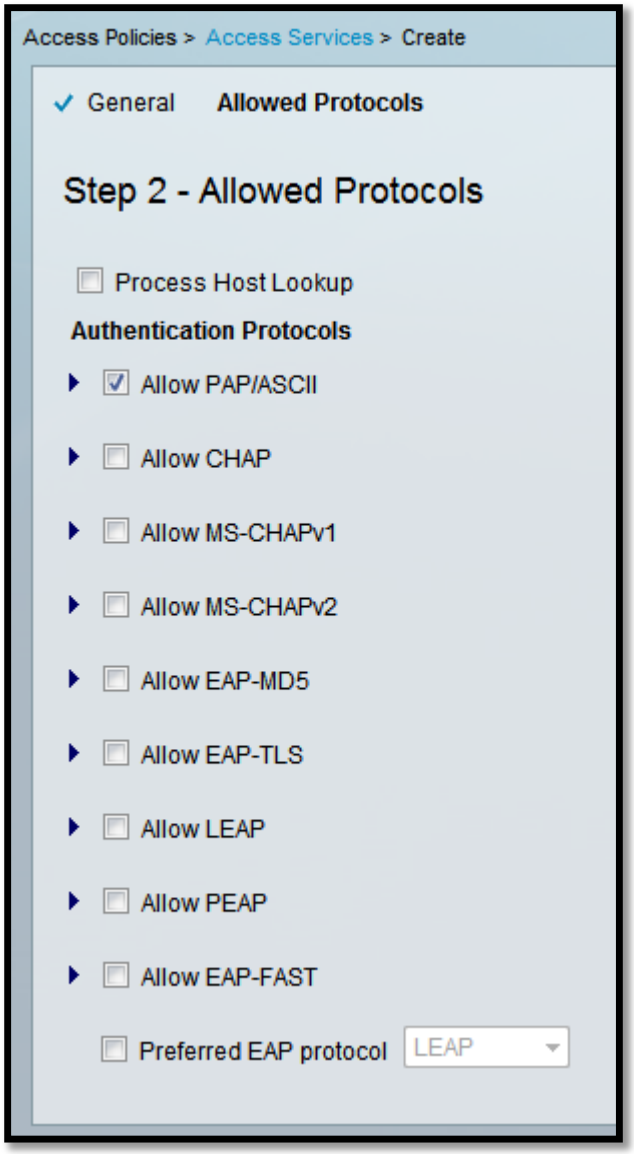


This Custom Condition will be used to differentiate between TACACS+ Shell/Login access and command authorization requests (“Service” attribute):

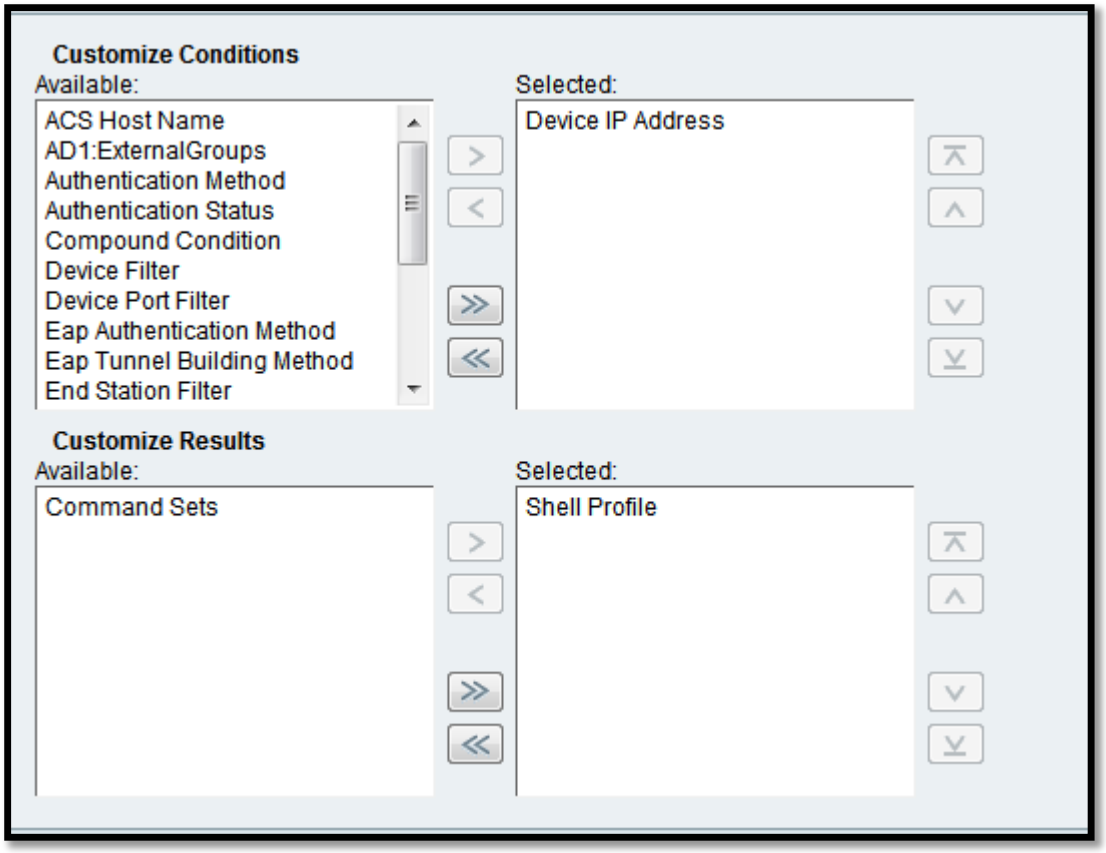




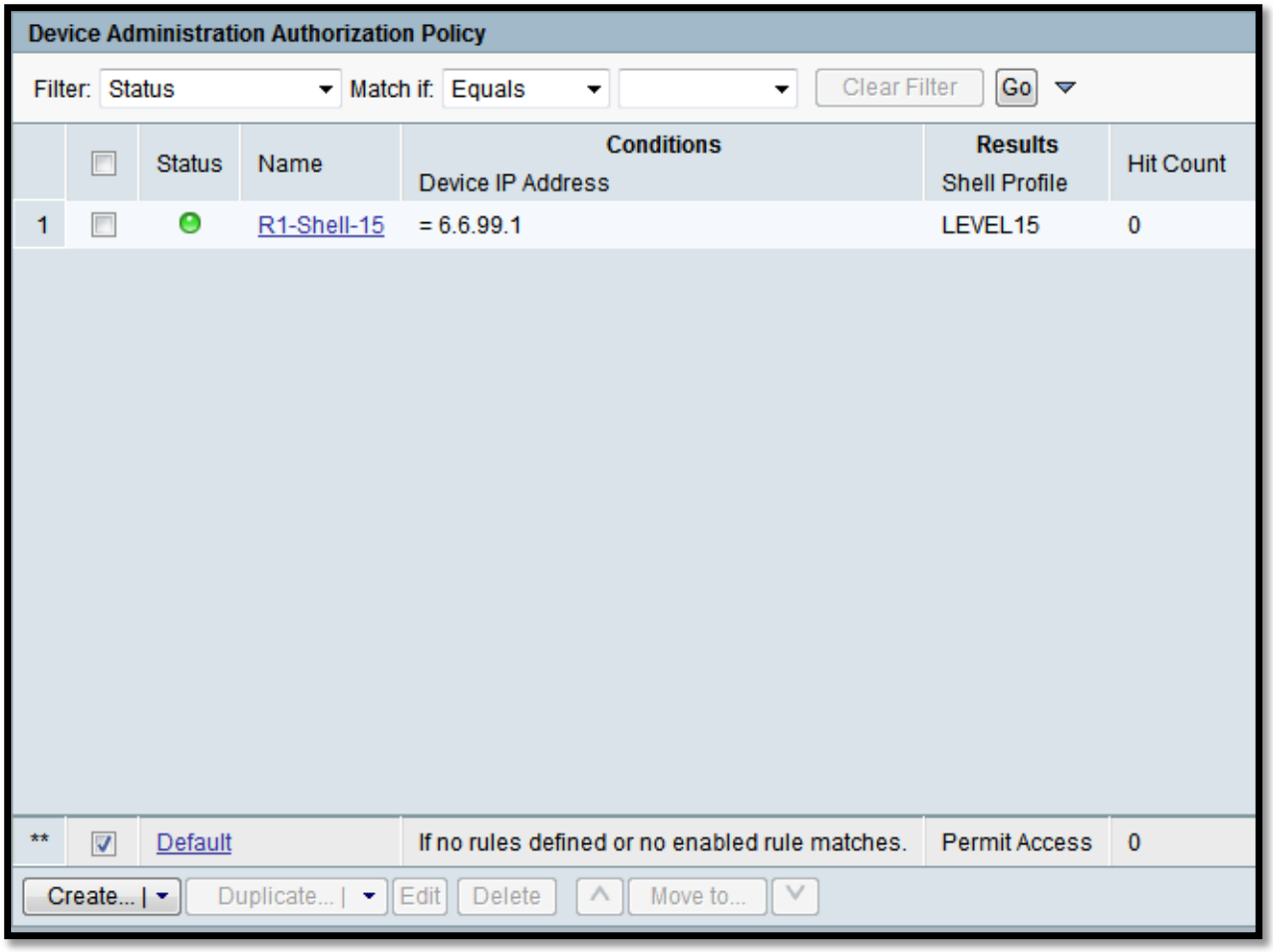
PAP/ASCII is enough for Device Management with TACACS+.



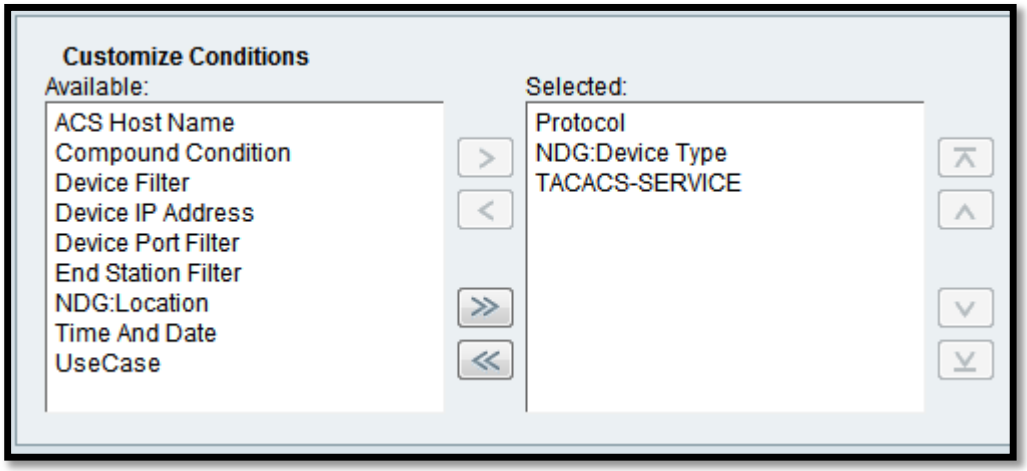
Make sure Local ID Store will be used for authentication and then Customize AuthZ Policy Conditions & Results:



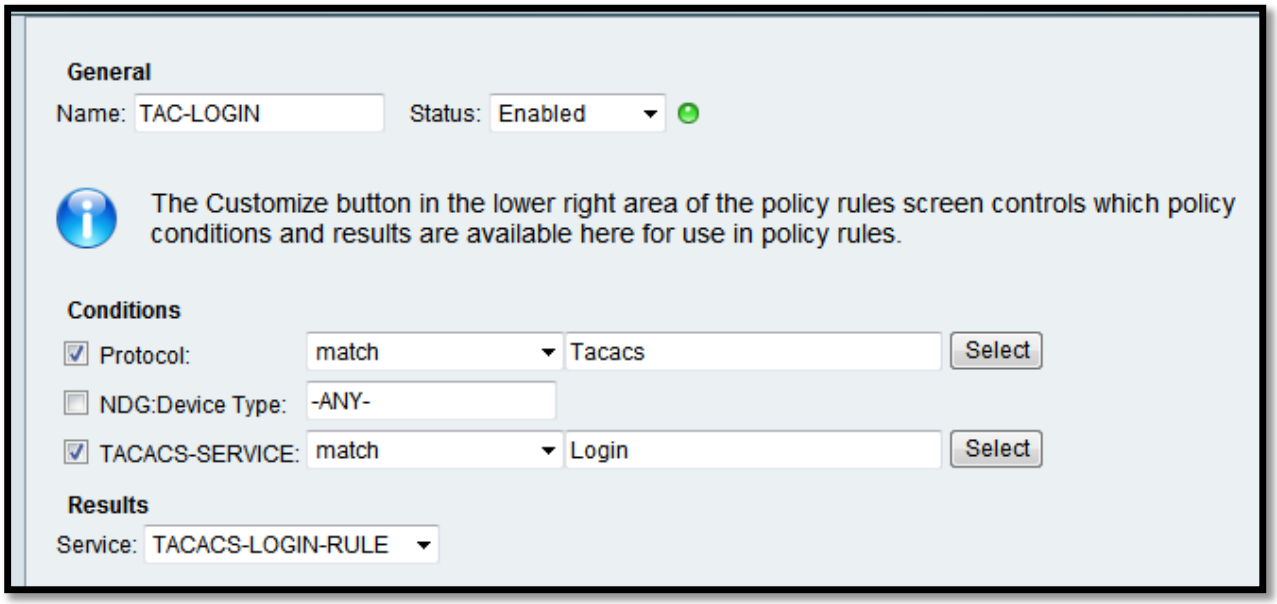
Add a rule to the new Access Service AuthZ policy. One is enough, we don't care about the default one – here all Login requests from R1 will end up having Privilege Level 15 assigned:

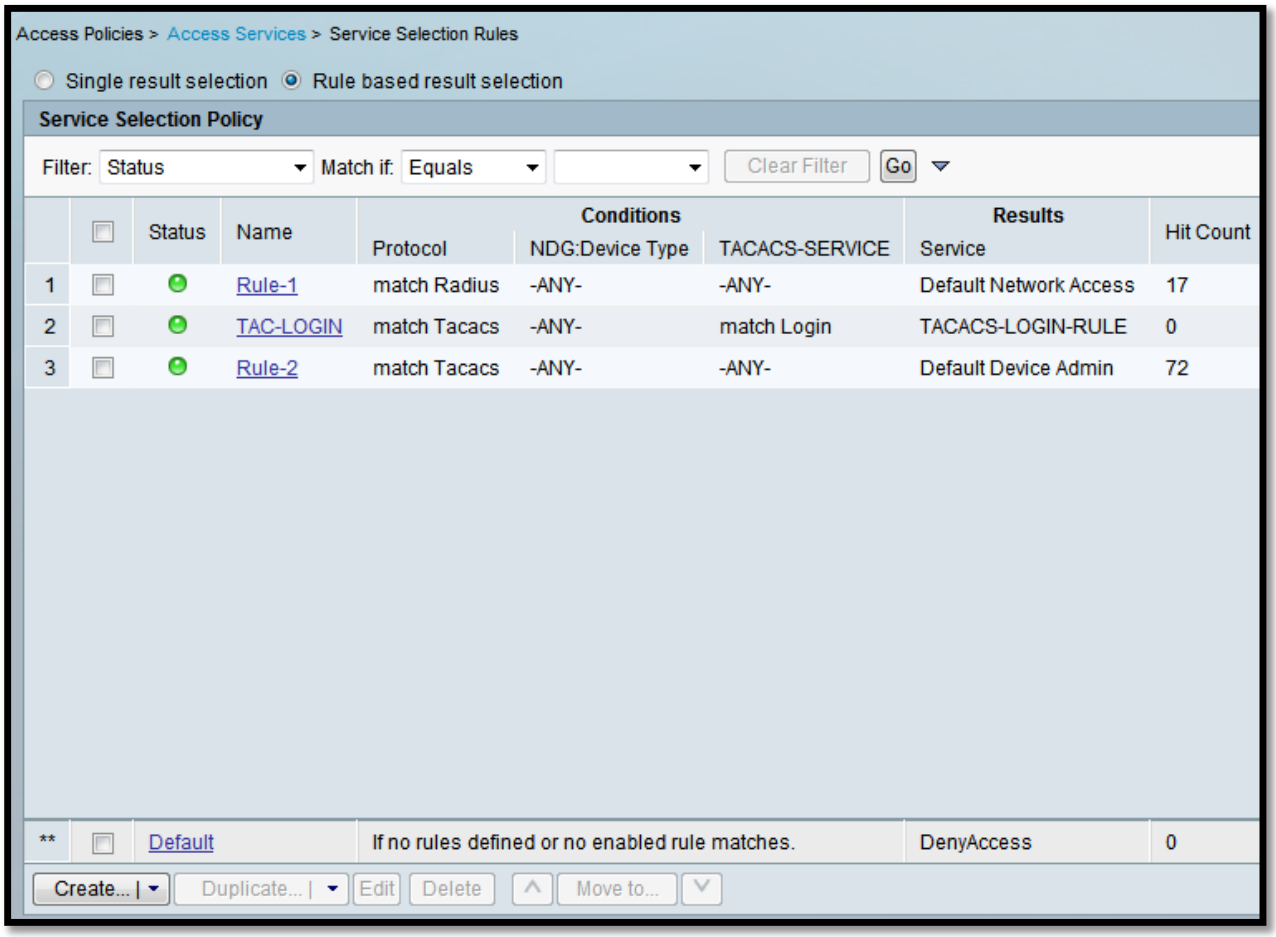


Now we need a new Service Selection Rule. First Customize Conditions to include our TACACS+ Service Attribute:

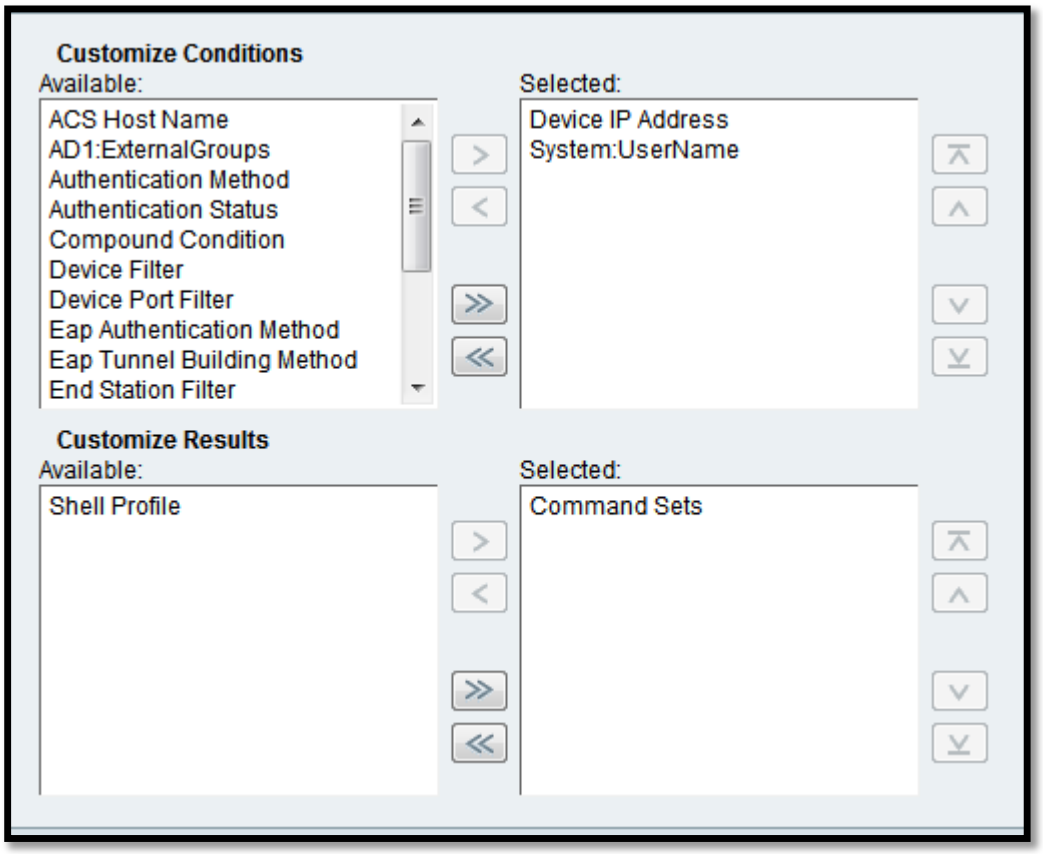


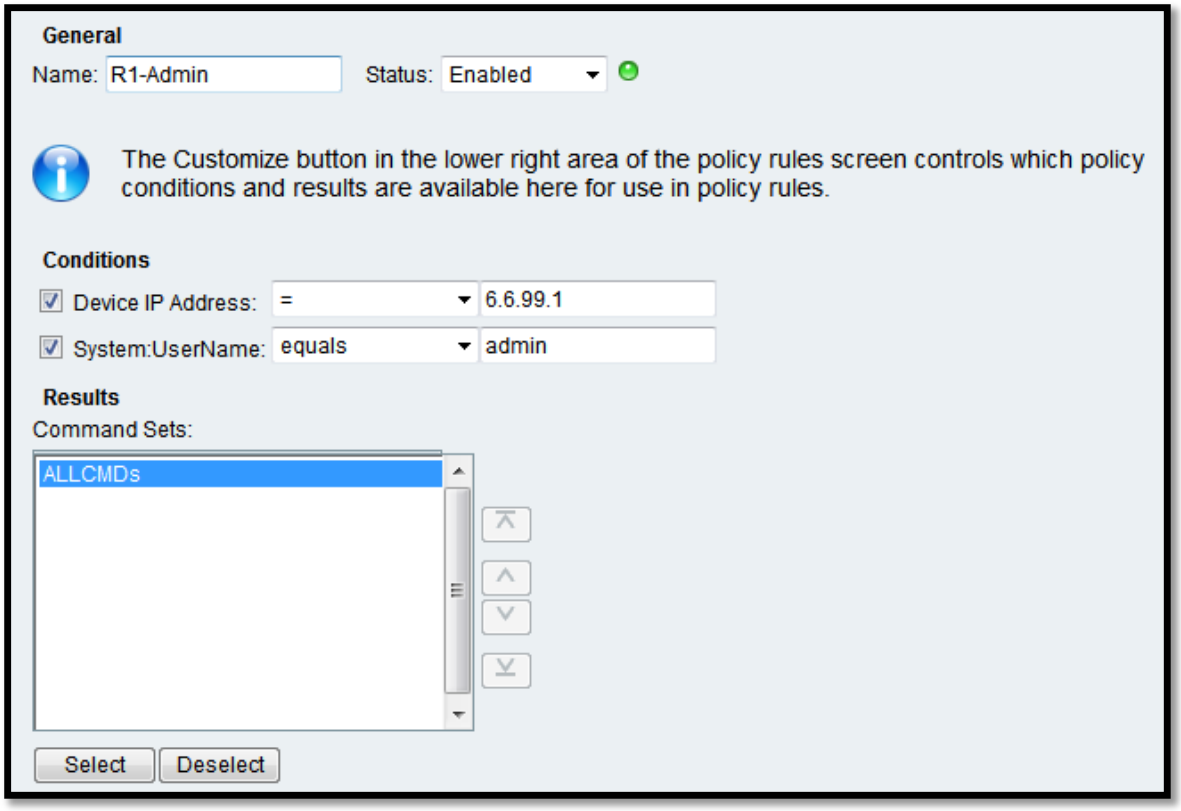
Then add a new Service Selection Rule. Make sure it is above the default Rule-2 that we will use to select only the Command Authorization Requests:

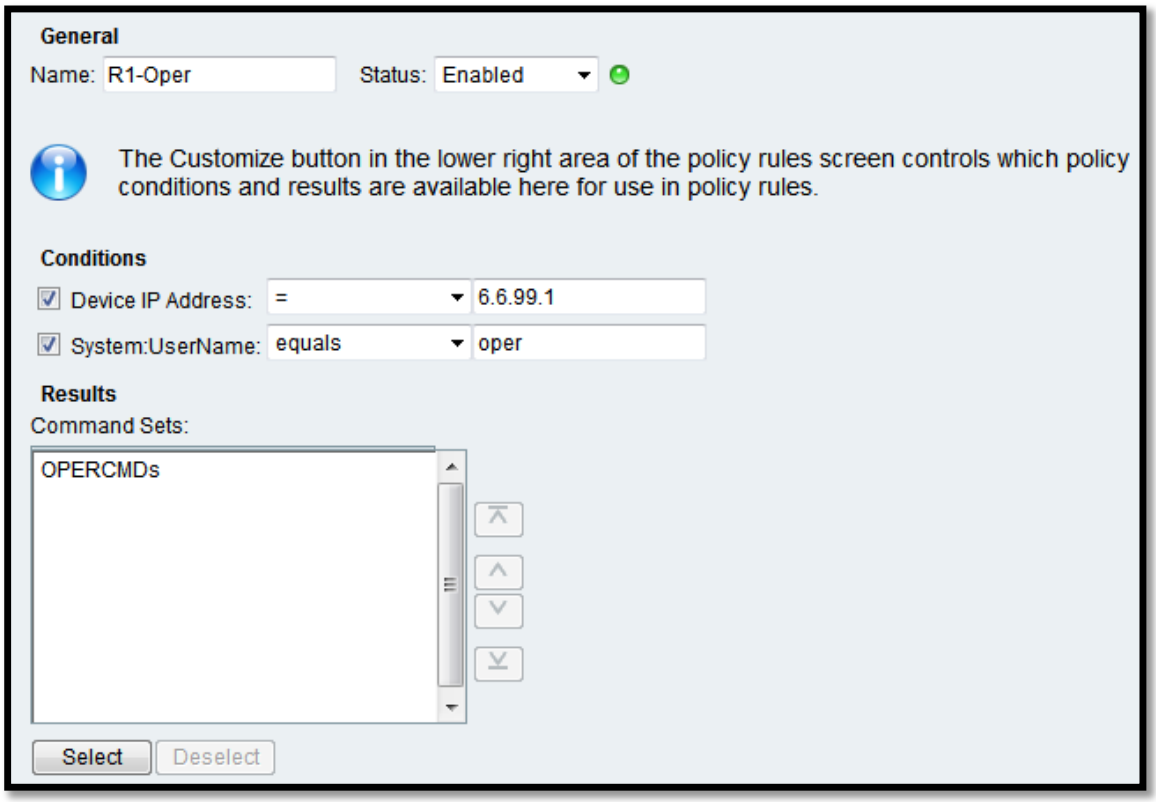


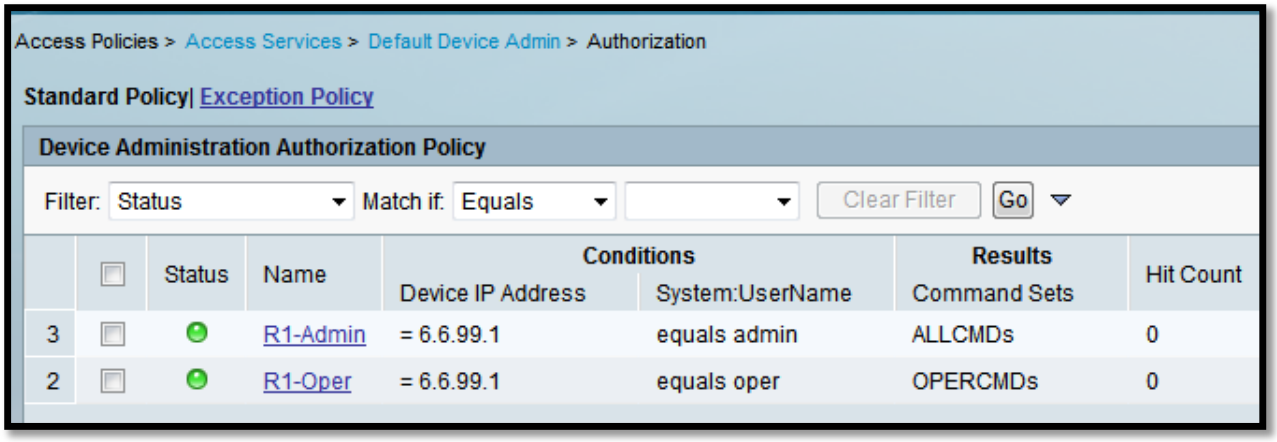


We now need to tune our “Default Device Admin” Policy, the AuthZ part. Then two rules inside – one for “admin”, one for “oper”:









The question states to configure authorization for all commands. By default commands are mapped to 3 privilege levels: 0, 1 and 15. To authorize all the commands, configure authorization for the 3 privilege levels.

As well by default config-commands are not subject to the authorization - you must enable this function on the router.

Don't add "match protocol tacacs" on R7 – this is not the same protocol as tacacs+.

For the ACS part – this task shows you how to create separate Access Policies for TACACS+ based on the type of request coming to the ACS. The ability to differentiate between Authentication/Authorization requests based on their type is very useful and allows you to create very granular policies, either on ACS or ISE. In our case we wanted to have a separate Access Policy for simple TACACS+ Shell/EXEC Authorization, and another one for Command Authorization.

Verification

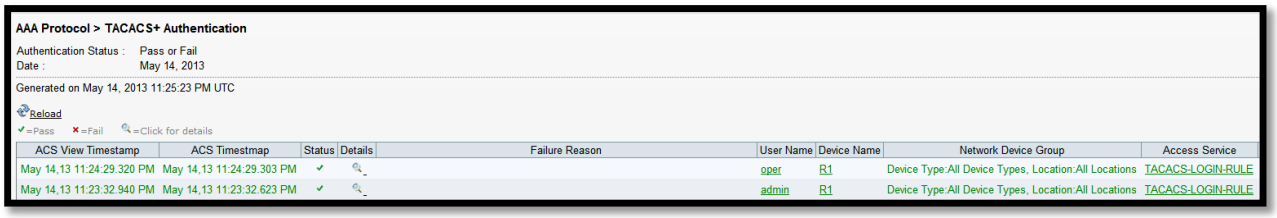
Start with a telnet from R7 - login as "admin":

```
R7#telnet 192.1.49.1
Trying 192.1.49.1 ... Open

T-username: admin
T-password:

R1#sh mem
                Head    Total(b)     Used(b)     Free(b)    Lowest(b)
Largest(b)
```

```
Processor    48DF6AE0     79729952     34148620     45581332     45491328
45529140
      I/O    3DA00000     39845888      5734808     34111080     34040592
34069308


R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
```

Now connect as „oper” :

```
R7#telnet 192.1.49.1
Trying 192.1.49.1 ... Open

T-username: oper
T-password:

R1#sh mem
Command authorization failed.

R1#sh ip int br
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            192.1.49.1      YES manual up
up
FastEthernet0/1            unassigned      YES unset  administratively
down down
Loopback0                  6.6.99.1        YES manual up
up

R1#conf t
Command authorization failed.

R1#
```



AAA Protocol > TACACS+ Authentication

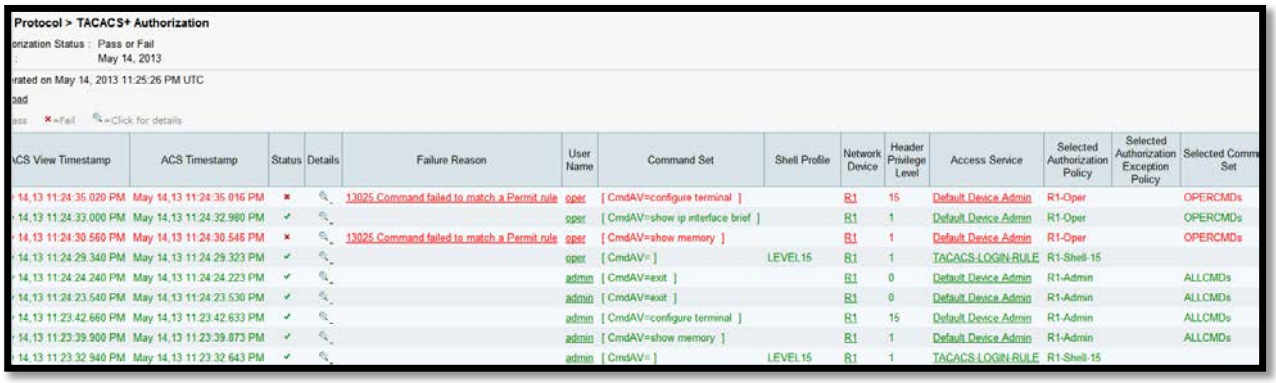
Authentication Status : Pass or Fail
Date : May 14, 2013

Generated on May 14, 2013 11:25:23 PM UTC

Reload

✔=Pass ✖=Fail 🔍=Click for details

ACS View Timestamp	ACS Timestmap	Status	Details	Failure Reason	User Name	Device Name	Network Device Group	Access Service
May 14,13 11:24:29.320 PM	May 14,13 11:24:29.303 PM	✔	🔍		oper	R1	Device Type:All Device Types, Location:All Locations	TACACS-LOGIN-RULE
May 14,13 11:23:32.940 PM	May 14,13 11:23:32.623 PM	✔	🔍		admin	R1	Device Type:All Device Types, Location:All Locations	TACACS-LOGIN-RULE



Protocol > TACACS+ Authorization

orization Status : Pass or Fail
May 14, 2013

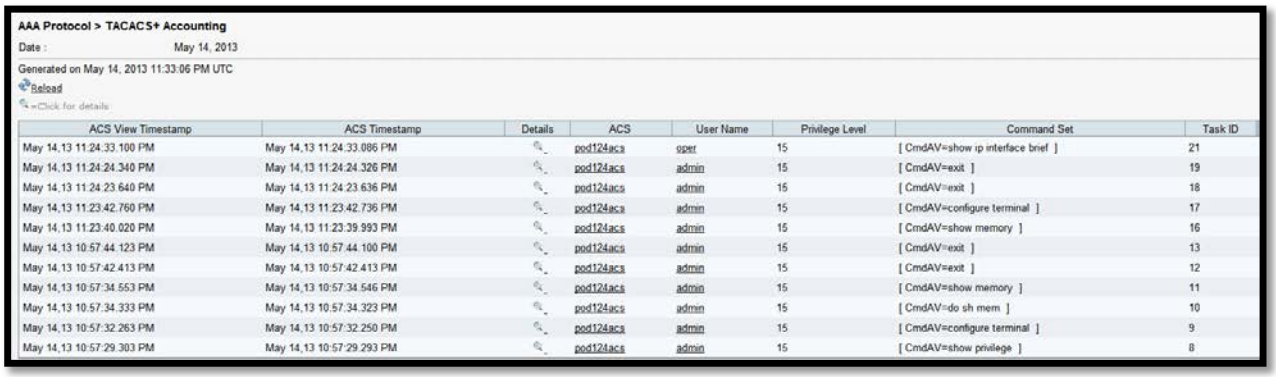
rated on May 14, 2013 11:25:26 PM UTC

oad

ss ×=Fail =Click for details

ACS View Timestamp	ACS Timestamp	Status	Details	Failure Reason	User Name	Command Set	Shell Profile	Network Device	Header Privilege Level	Access Service	Selected Authorization Policy	Selected Authorization Exception Policy	Selected Comm Set
14,13 11:24:35.020 PM	May 14,13 11:24:35.016 PM	×		13025 Command failed to match a Permit rule	oper	[CmdAV=configure terminal]		R1	15	Default Device Admin	R1-Oper		OPERCMDs
14,13 11:24:33.000 PM	May 14,13 11:24:32.980 PM	✓			oper	[CmdAV=show ip interface brief]		R1	1	Default Device Admin	R1-Oper		OPERCMDs
14,13 11:24:30.560 PM	May 14,13 11:24:30.546 PM	×		13025 Command failed to match a Permit rule	oper	[CmdAV=show memory]		R1	1	Default Device Admin	R1-Oper		OPERCMDs
14,13 11:24:29.340 PM	May 14,13 11:24:29.323 PM	✓			oper	[CmdAV=]	LEVEL15	R1	1	TACACS-LOGIN-RULE	R1-Shell-15		
14,13 11:24:24.240 PM	May 14,13 11:24:24.223 PM	✓			admin	[CmdAV=exit]		R1	0	Default Device Admin	R1-Admin		ALLCMDs
14,13 11:24:23.540 PM	May 14,13 11:24:23.530 PM	✓			admin	[CmdAV=exit]		R1	0	Default Device Admin	R1-Admin		ALLCMDs
14,13 11:23:42.660 PM	May 14,13 11:23:42.633 PM	✓			admin	[CmdAV=configure terminal]		R1	15	Default Device Admin	R1-Admin		ALLCMDs
14,13 11:23:39.900 PM	May 14,13 11:23:39.873 PM	✓			admin	[CmdAV=show memory]		R1	1	Default Device Admin	R1-Admin		ALLCMDs
14,13 11:23:32.940 PM	May 14,13 11:23:32.643 PM	✓			admin	[CmdAV=]	LEVEL15	R1	1	TACACS-LOGIN-RULE	R1-Shell-15		

To access Accounting Logs in a separate tab you must first add them to the Favorites.



AAA Protocol > TACACS+ Accounting

Date : May 14, 2013

Generated on May 14, 2013 11:33:06 PM UTC

Reload

=Click for details

ACS View Timestamp	ACS Timestamp	Details	ACS	User Name	Privilege Level	Command Set	Task ID
May 14,13 11:24:33.100 PM	May 14,13 11:24:33.086 PM		pod124acs	oper	15	[CmdAV=show ip interface brief]	21
May 14,13 11:24:24.340 PM	May 14,13 11:24:24.326 PM		pod124acs	admin	15	[CmdAV=exit]	19
May 14,13 11:24:23.640 PM	May 14,13 11:24:23.636 PM		pod124acs	admin	15	[CmdAV=exit]	18
May 14,13 11:23:42.760 PM	May 14,13 11:23:42.736 PM		pod124acs	admin	15	[CmdAV=configure terminal]	17
May 14,13 11:23:40.020 PM	May 14,13 11:23:39.993 PM		pod124acs	admin	15	[CmdAV=show memory]	16
May 14,13 10:57:44.123 PM	May 14,13 10:57:44.100 PM		pod124acs	admin	15	[CmdAV=exit]	13
May 14,13 10:57:42.413 PM	May 14,13 10:57:42.413 PM		pod124acs	admin	15	[CmdAV=exit]	12
May 14,13 10:57:34.553 PM	May 14,13 10:57:34.546 PM		pod124acs	admin	15	[CmdAV=show memory]	11
May 14,13 10:57:34.333 PM	May 14,13 10:57:34.323 PM		pod124acs	admin	15	[CmdAV=do sh mem]	10
May 14,13 10:57:32.263 PM	May 14,13 10:57:32.250 PM		pod124acs	admin	15	[CmdAV=configure terminal]	9
May 14,13 10:57:29.303 PM	May 14,13 10:57:29.293 PM		pod124acs	admin	15	[CmdAV=show privilege]	8

Task 5.4: Access Control with LDAP (4 Points)

- Configure the ASA for remote SSH access
- Only R1 should be able to manage the firewall from the outside
- Use LDAP Server for authentication (MS Active Directory 10.1.1.101)
- The AD domain is “ipexpert.com”
- Connect to the server using account “Administrator” with password “IPexpert123”
- This account is located in AD hierarchy under “Users”
- Use LDAP Naming Attribute “sAMAccountName”
- Authenticate to the ASA as “IPXEMP1” with password “cisco”

Detailed Solution

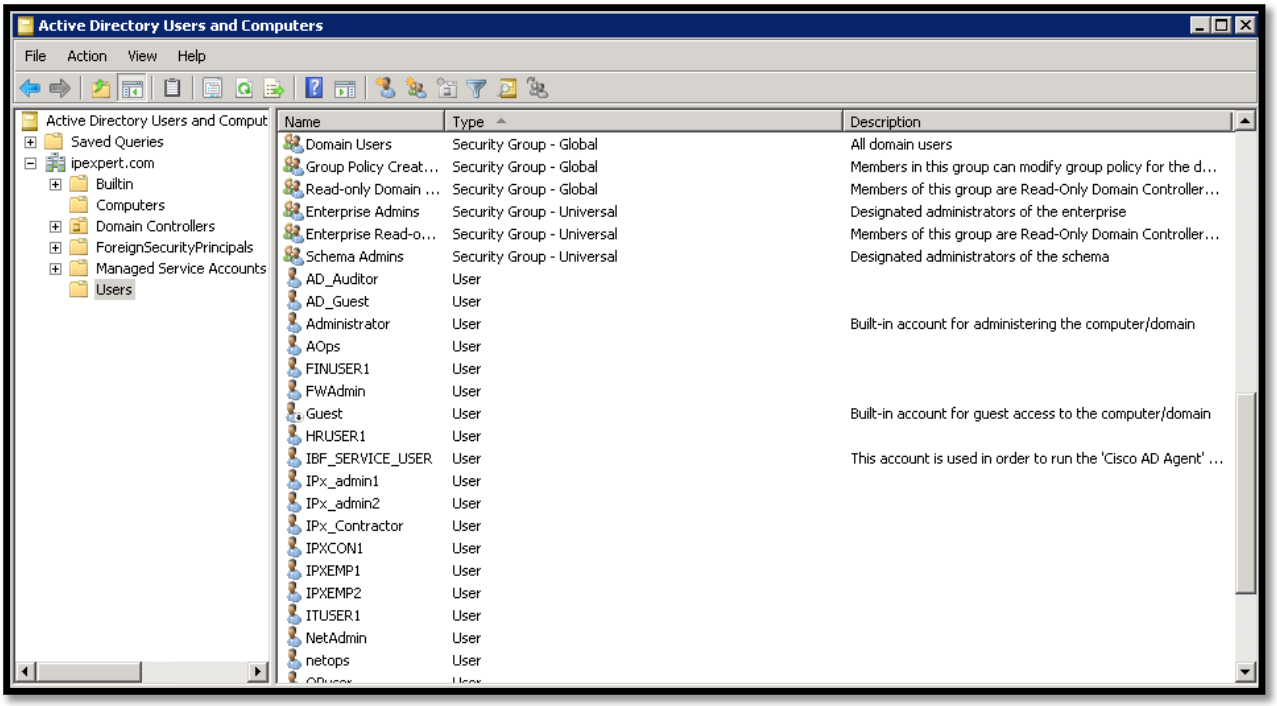
ASA3

```
aaa-server AD protocol ldap
aaa-server AD (inside) host 10.1.1.101
 ldap-base-dn dc=ipexpert, dc=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password IPexpert123
 ldap-login-dn cn=Administrator, cn=Users, dc=ipexpert, dc=com
 server-type Microsoft

aaa authentication ssh console AD

crypto key generate rsa mod 1024

ssh 192.1.49.1 255.255.255.255 outside
```

R7

```
ip access-list extended SSH_TO_ASA
 permit tcp host 192.1.49.1 host 6.6.146.30 eq 22

class-map type inspect match-all ZFW_OUTIN_SSH_CLASS
 match access-group name SSH_TO_ASA
 match protocol ssh

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ZFW_OUTIN_SSH_CLASS
  inspect
```

Here's the AD structure we use in Proctor Labs. On the exam, if you can access the AD Server, you will probably see a similar setup so even if they don't tell you the DNs you should be able to figure them out on your own:



As you can see "ipexpert.com" is the domain, top of the tree. Then under "Users" is when the Administrator is defined (which account we use to connect to the AD) and there is also our IPXEMP1 we use for Device Management. First six entries seen here are the User Groups.

Verification

If you SSH from something else than CAT3 a log message shows up saying connection was blocked:

```
R4#ssh -l IPXEMP1 6.6.146.30

R4#

%ASA-3-710003: TCP access denied by ACL from 6.6.146.4/18574 to
outside:6.6.146.30/22

R1#ssh -l IPXEMP1 6.6.146.30
Password:
Type help or '?' for a list of available commands.

ASA> ena
Password:
```

```
ASA# sh ssh sess

SID Client IP       Version Mode Encryption Hmac     State
Username
0   192.1.49.1      1.99    IN   aes128-cbc sha1     SessionStarted
IPXEMP1
                            OUT  aes128-cbc sha1     SessionStarted
IPXEMP1
```

You can also enable LDAP (**debug ldap 20**) debug to see what's going on in the background. More important stuff here is the information about successful connection to the server and then the LDAP/AD attributes returned for the user "IPXEMP1" (e.g. "memberOf" which is the Group this user belongs to) :

```
ASA#
[53] Session Start
[53] New request Session, context 0x00007fff2e9bc218, reqType =
Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://10.1.1.101:389
[53] Connect to LDAP server: ldap://10.1.1.101:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] Binding as Administrator
[53] Performing Simple authentication for Administrator to 10.1.1.101
[53] LDAP Search:
        Base DN = [dc=ipexpert, dc=com]
        Filter  = [sAMAccountName=IPXEMP1]
        Scope   = [SUBTREE]
[53] User DN = [CN=IPXEMP1,CN=Users,DC=ipexpert,DC=com]
[53] Talking to Active Directory server 10.1.1.101
[53] Reading password policy for IPXEMP1,
dn:CN=IPXEMP1,CN=Users,DC=ipexpert,DC=com
[53] Read bad password count 0
[53] Binding as IPXEMP1
[53] Performing Simple authentication for IPXEMP1 to 10.1.1.101
[53] Processing LDAP response for user IPXEMP1
[53] Message (IPXEMP1):
[53] Authentication successful for IPXEMP1 to 10.1.1.101
[53] Retrieved User Attributes:
[53]    objectClass: value = top
```

```
[53]    objectClass: value = person
[53]    objectClass: value = organizationalPerson
[53]    objectClass: value = user
[53]    cn: value = IPXEMP1
[53]    givenName: value = IPXEMP1
[53]    distinguishedName: value = CN=IPXEMP1,CN=Users,DC=ipexpert,DC=com
[53]    instanceType: value = 4
[53]    whenCreated: value = 20101127081729.0Z
[53]    whenChanged: value = 20130502190933.0Z
[53]    displayName: value = IPXEMP1
[53]    uSNCreated: value = 41351
[53]    memberOf: value = CN=IPX_EMP,CN=Users,DC=ipexpert,DC=com
[53]    memberOf: value = CN=Domain Admins,CN=Users,DC=ipexpert,DC=com
[53]    memberOf: value = CN=Remote Desktop
Users,CN=Builtin,DC=ipexpert,DC=com
[53]    memberOf: value = CN=Administrators,CN=Builtin,DC=ipexpert,DC=com
[53]    uSNChanged: value = 792800
[53]    name: value = IPXEMP1
[53]    objectGUID: value = .FC..w3E...d.w.L
[53]    userAccountControl: value = 66048
[53]    badPwdCount: value = 0
[53]    codePage: value = 0
[53]    countryCode: value = 0
[53]    badPasswordTime: value = 130099201321838000
[53]    lastLogoff: value = 0
[53]    lastLogon: value = 130101054355114801
[53]    pwdLastSet: value = 129353194493769531
[53]    primaryGroupID: value = 513
[53]    objectSid: value = ................!..(.......
[53]    adminCount: value = 1
[53]    accountExpires: value = 9223372036854775807
[53]    logonCount: value = 30
[53]    sAMAccountName: value = IPXEMP1
[53]    sAMAccountType: value = 805306368
[53]    userPrincipalName: value = IPXEMP1@ipexpert.com
[53]    objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ipexpert,DC=com
[53]    dSCorePropagationData: value = 20101127111002.0Z
[53]    dSCorePropagationData: value = 16010101000000.0Z
[53]    lastLogonTimestamp: value = 130119953731542248
[53] Fiber exit Tx=538 bytes Rx=2703 bytes, status=1
```

```
[53] Session End
```

6.0 Advanced Security (12 points)

Task 6.1: OSPFv3 Authentication Troubleshooting (4 Points)

- OSPFv3 was configured in VLAN 156 between R5, R10 and R11
- To increase overall network security a decision was made to protect IPv6 Control Plane
- After enabling OSPFv3 authentication it turned out that some adjacencies have fallen
- Re-establish OSPFv3 adjacencies between R5, R10 and R11 without removing authentication/encryption services enabled for this communication

Detailed Solution

Follow the Verification section.

Verification

Since the task asks us to troubleshoot OSPFv3 authentication, which is IPSec, we will start with looking at IPSec Security Associations – and here we see they are UP and packets get encrypted/decrypted on R11:

```
R11#sh crypto sockets

Number of Crypto Socket connections 1

 Gi0/1 Peers: (local): ::
              (remote): ::
       Local Ident (addr/plen/port/prot): (FE80::/10/0/89)
       Remote Ident (addr/plen/port/prot): (::/0/0/89)
       IPSec Profile: "OSPFv3-51011"
       Socket State: Open
       Client: "OSPFv3" (Client State: Active)

R11#sh cry sess int g0/1 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: GigabitEthernet0/1
Session status: DOWN
Peer: 6.6.25.2 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 6.6.2.0/255.255.255.0
        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
  IPSEC FLOW: permit ip 6.6.146.0/255.255.255.0 host 6.6.99.2
        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

Interface: GigabitEthernet0/1
Session status: UP-NO-IKE
Peer: FF02::5 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 29 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/4294967023
        Outbound: #pkts enc'ed 29 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/4294967023
```

What about R10? Here only the encryption counters increase, same as on R5:

```
R10#sh cry sess remote ff02::5 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: GigabitEthernet0/1
Session status: UP-NO-IKE
Peer: FF02::5 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 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/4294966092
        Outbound: #pkts enc'ed 127 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/4294966092

R5#sh cry sess int F0/0 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: FastEthernet0/0
Session status: DOWN
Peer: 6.6.146.30 port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: permit ip 6.6.55.0/255.255.255.0 10.1.1.0/255.255.255.0
        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

Interface: FastEthernet0/0
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 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 58 drop 0 life (KB/Sec) 0/0
```

What maybe a reason only R11 receives OSPF packets but other devices don't? Let's take a look at OSPF interface config to see what settings were configured:

```
R11#sh ipv ospf int g0/1
GigabitEthernet0/1 is up, line protocol is up
  Link Local Address FE80::CA4C:75FF:FE1F:DDC1, Interface ID 5
```

```
  Area 0, Process ID 1, Instance ID 0, Router ID 6.6.99.11
  Network Type BROADCAST, Cost: 1
  3DES encryption MD5 auth SPI 51011, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 6.6.99.11, local address
FE80::CA4C:75FF:FE1F:DDC1
  Backup Designated router (ID) 6.6.99.5, local address
FE80::21B:D5FF:FE0F:F2F8
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  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 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 6.6.99.5  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
                        Current    Most Seen
Authenticated Users       1          1

R10#sh ipv ospf int g0/1
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 6.6.99.10
  Network Type BROADCAST, Cost: 1
  3DES encryption MD5 auth SPI 51001, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 6.6.99.10, local address
FE80::32E4:DBFF:FECE:8491
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  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 0, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

```
R5#sh ipv ospf int f0/0
FastEthernet0/0 is up, line protocol is up
  Link Local Address FE80::21B:D5FF:FE0F:F2F8, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 6.6.99.5
  Network Type BROADCAST, Cost: 1
  3DES encryption MD5 auth SPI 51011, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 6.6.99.11, local address
FE80::CA4C:75FF:FE1F:DDC1
  Backup Designated router (ID) 6.6.99.5, local address
FE80::21B:D5FF:FE0F:F2F8
  Flush timer for old DR LSA due in 00:02:17
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  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 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 6.6.99.11  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OK looks like R10 is out of sync in terms of the SPI number. We will try to fix it and see what's left:

```
R10(config-if)#no ipv6 ospf encryption ipsec spi 51001 esp 3des
12345678901234567890123456789012345678909999999 md5
1234567890123456789012345678909
```

```
R10(config-if)#ipv6 ospf encryption ipsec spi 51011 esp 3des
12345678901234567890123456789012345678909999999 md5
1234567890123456789012345678909
```

```
*May 15 10:13:21.249: %OSPFv3-5-ADJCHG: Process 1, Nbr 6.6.99.5 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done
```

So far, so good. So now the situation may look like we are adjacent with everyone on R10 :

```
R10(config-if)#do sh ipv ospf ne

            OSPFv3 Router with ID (6.6.99.10) (Process ID 1)
```

```
Neighbor ID     Pri   State           Dead Time   Interface ID
Interface
6.6.99.5          1   FULL/DROTHER    00:00:37    3
GigabitEthernet0/1
6.6.99.11         1   FULL/DR         00:00:39    5
GigabitEthernet0/1
```

Moving on to R5 – here the adjacency was established with R10 but it is now flapping:

```
May 15 10:27:42.780: %OSPFv3-5-ADJCHG: Process 1, Nbr 6.6.99.10 on
FastEthernet0/0 from LOADING to FULL, Loading Done
R5#
May 15 10:28:28.046: %OSPFv3-5-ADJCHG: Process 1, Nbr 6.6.99.10 on
FastEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

On R11, on the other hand, adjacency is in the "INIT" state all the time. So looks like we are getting packets from R5 but it does not get anything back from us.

```
R11#sh ipv ospf ne

            OSPFv3 Router with ID (6.6.99.11) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID
Interface
6.6.99.5          1   INIT/DROTHER    00:00:39    3
GigabitEthernet0/1
6.6.99.10         1   FULL/BDR        00:00:38    4
GigabitEthernet0/1
```

If you take a look at IPSec counters on R5 again you will now notice some packets are getting decrypted. These are not the multicast packets, as we will see in just a second:

```
Interface: FastEthernet0/0
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 64 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 252 drop 0 life (KB/Sec) 0/0
```

If you put those pieces all together, it looks like R10 and R11 hear from R5 but not the other way round. Since this is all a single L2 network, this may be an indication of a problem in the local Data Plane. You could look at the switch config, but in our case they are not enabled for IPv6. So we should probably focus on the routers since there are no other devices involved here. Quick look at the interface config shows an ACL applied to F0/0 on R5 that blocks encrypted OSPFv3 multicasts:

```
R5#sh run int f0/0
Building configuration...

Current configuration : 370 bytes
!
interface FastEthernet0/0
 ip address 6.6.156.5 255.255.255.0
 ip ospf message-digest-key 1 md5 cisco
 duplex auto
 speed auto
 ipv6 address 2006:6:156::5/64
 ipv6 ospf 1 area 0
 ipv6 ospf encryption ipsec spi 51011 esp 3des
123456789012345678901234567890123456789099999999 md5
12345678901234567890123456789099
 ipv6 traffic-filter PERMIT_ALL in
 crypto map MAP3

R5#sh ipv access-l PERMIT_ALL
IPv6 access list PERMIT_ALL
    deny esp any host FF02::5 (811 matches) sequence 30
    permit ipv6 any any (660 matches) sequence 40
```

In this case removing an ACL entry or the entire ACL will have the same effect so we can do either:

```
R5(config)#int f0/0
R5(config-if)#no ipv traffic-filter PERMIT_ALL in

May 15 10:42:41.142: %OSPFv3-5-ADJCHG: Process 1, Nbr 6.6.99.10 on
FastEthernet0/0 from LOADING to FULL, Loading Done

May 15 10:42:44.454: %OSPFv3-5-ADJCHG: Process 1, Nbr 6.6.99.11 on
FastEthernet0/0 from LOADING to FULL, Loading Done
```

Task 6.2: DHCP (4 Points)

- Configure R2 as a DHCP server. Configure it to assign IP addresses and the default gateway. Make sure R2 updates the ARP table when it assigns DHCP addresses
- Make sure it's the only DHCP server on VLAN2 on all four switches and the only authoritative ARP source
- Configure Cat2 Vlan2 to request a DHCP address from R2

Detailed Solution

R2

```
ip dhcp pool VLAN2
 network 6.6.2.0 255.255.255.0
 default-router 6.6.2.2
 update arp
!
ip dhcp excluded-address 6.6.2.2
ip dhcp excluded-address 6.6.2.130
ip dhcp excluded-address 6.6.2.140

interface GigabitEthernet0/0
 ip dhcp relay information trust
```

CAT1

```
spanning-tree vlan 2 root primary

int f0/2
 ip dhcp snoop trust

arp access-list SARP
 permit ip host 6.6.2.2 mac host 001b.d4a9.e400
 permit ip host 6.6.2.130 mac host c464.13d1.c5c1
 permit ip host 6.6.2.140 mac host 0007.7dbc.c6c1

ip dhcp snooping
ip dhcp snooping vlan 2
```

```
ip arp inspection vlan 2
ip arp inspection filter SARP vlan  2
```

CAT2

```
int vlan 2
 ip add dhcp

int range f0/23 – 24
 ip dhcp snooping trust
 ip arp inspection trust

ip dhcp snooping
ip dhcp snooping vlan 2
ip arp inspection vlan 2
```

CAT3

```
int range g1/0/15 – 16
 ip dhcp snooping trust
 ip arp inspection trust

ip dhcp snooping
ip dhcp snooping vlan 2
ip arp inspection vlan 2
```

CAT4

```
int range g1/0/17 – 18
 ip dhcp snooping trust
 ip arp inspection trust

ip dhcp snooping
ip dhcp snooping vlan 2
ip arp inspection vlan 2
```

I think the hardest thing when working with DHCP snooping is making sure you understand which direction the traffic is traversing. By controlling the root switch for VLAN 2, we can make sure we are properly making the traffic go the direction we expect. Otherwise, we may need to trust all trunks.

Verification

```
CAT1#sh ip dhcp snoo binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----  ----
----------------
00:1B:D4:C1:54:41   6.6.2.1          85399       dhcp-snooping   2
FastEthernet0/23

CAT1#sh ip arp inspection vlan 2

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    2     Enabled          Active      SARP               No

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    2     Deny             Deny              Off

CAT2#sh ip arp inspection vl 2

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    2     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    2     Deny             Deny              Off

CAT3#sh ip arp ins int | ex Untrust
```

```
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/15         Trusted              None              N/A
 Gi1/0/16         Trusted              None              N/A
```

You can start testing this task after CAT2 gets an address assigned:

```
CAT2#
*Mar  7 18:15:13.438: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan2 assigned
DHCP address 6.6.2.1, mask 255.255.255.0, hostname CAT2
```

```
CAT4#ping 6.6.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/10/25 ms

CAT4#ping 6.6.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms

CAT4#ping 6.6.2.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms

CAT3#ping 6.6.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/9 ms

CAT3#ping 6.6.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.2, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

CAT3#ping 6.6.2.140
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.140, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

CAT2#ping 6.6.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

Task 6.3: Port Protection (4 Points)

- Configure a macro to set the port with the following security parameters :
  - Turn off DTP
  - Disable EtherChannel
  - Turn on Spanning Tree PortFast
  - Port should be shut down if BPDUs are received
  - Protect the port from MAC address flood. Allow only 1 MAC per port
- Apply the macro to all non-trunking ports connected to the ASA

Detailed Solution

CAT3, CAT4

```
macro name SEC
 Enter macro commands one per line. End with the character '@'.
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  no channel-group
  spanning-tree bpduguard enable
  sw port-security
  sw port-security maximum 1
```

```
@

int range g1/0/19 - 21
 macro apply SEC
```

Being familiar with the option is the only trick to this question. Macro's allow you to apply multiple commands using the single command macro apply.

Verification

```
CAT3#show pars macro br
    default global   : cisco-global
    default interface: cisco-desktop
    default interface: cisco-phone
    default interface: cisco-switch
    default interface: cisco-router
    default interface: cisco-wireless
    customizable     : SEC

CAT3#sh pars macro name SEC
Macro name : SEC
Macro type : customizable
switchport mode access
switchport nonegotiate
spanning-tree portfast
no channel-group
spanning-tree bpduguard enable
sw port-security
sw port-security maximum 1

CAT3(config)#do sh run int g1/0/19
Building configuration...

Current configuration : 115 bytes
! interface GigabitEthernet1/0/19
 switchport access vlan 146
 switchport mode access
 spanning-tree portfast


CAT3(config-if)#macro apply SEC
```

```
CAT3(config-if)#do sh run int g1/0/19
Building configuration...

Current configuration : 220 bytes
!
interface GigabitEthernet1/0/19
 switchport access vlan 146
 switchport mode access
 switchport nonegotiate
 switchport port-security
 macro description SEC
 spanning-tree portfast
 spanning-tree bpduguard enable
```

7.0 Attack Mitigation (12 points)

Task 7.1: FPM (4 Points)

- You have found invalid DNS responses coming from DNS servers on the Internet
- You know the DNS server R1 is sending an address 199.99.99.99 for R10.ipexpert.com that it should not
- Configure R7 to drop DNS Responses from Internet DNS Servers if they respond to request for R10.ipexpert.com

Detailed Solution

R7

```
load protocol system:fpm/phdf/ip.phdf
load protocol system:fpm/phdf/udp.phdf

class-map type stack match-all STACK
 match field IP protocol eq 0x11 next UDP
 match field UDP source-port eq 0x35 next UDP

class-map type access-control match-all FPM_BAD_DNS_CLASS
 match field UDP source-port eq 53
 match start UDP payload-start offset 0 size 100 regex
".*[Rr]10.[Ii][Pp][Ee][Xx][Pp][Ee][Rr][Tt].[Cc][Oo][Mm].*"

policy-map type access-control FPM_DNS_POL
 class FPM_BAD_DNS_CLASS
   log
   drop

policy-map type access-control FPM_POL
 class STACK
  service-policy FPM_DNS_POL
!
interface FastEthernet0/0
 service-policy type access-control input FPM_POL
```

Working with Flexible Packet Matching is a task in and of itself. It is a very powerful tool in its ability to look deep into packets and check even the payload of a packet for conformity. It is not quite as powerful as IPS in that it cannot look at a string of TCP or UDP packets to match on a string. I would think of it more in terms of the Atomic IP engine of IPS.

To use FPM you may need to use some type of packet capturing technique to first look at an offending packet so you can determine how to inspect the packet. What you need to be looking for etc. In our case we assumed we will be only looking into the first 100 Bytes of DNS responses. This should be enough in this case when the URI is short.

Verification

First let's see what's going on before we configure FPM:

```
R4#ping R10.ipexpert.com

Translating "R10.ipexpert.com"...domain server (192.1.49.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 199.99.99.99, timeout is 2 seconds:
U.
Success rate is 0 percent (0/2)
```

After we apply FPM policy:

```
R4#ping R10.ipexperT.com

Translating "R10.ipexperT.com"...domain server (192.1.49.1)
% Unrecognized host or address, or protocol not running.

R4#ping r10.iPexpert.com

Translating "r10.iPexpert.com"...domain server (192.1.49.1)

R4#ping r10.ipexpert.com

Translating "r10.ipexpert.com"...domain server (192.1.49.1)
```

```
R7#
*May 15 13:58:01.159: %SEC-6-IPACCESSLOGP: list FPM_BAD_DNS_CLASS3 denied
udp 192.1.49.1(53) (FastEthernet0/0 ) -> 6.6.146.4(60257), 1 packet
R7#
*May 15 13:58:40.587: %SEC-6-IPACCESSLOGP: list FPM_BAD_DNS_CLASS3 denied
udp 192.1.49.1(53) (FastEthernet0/0 ) -> 6.6.146.4(63598), 1 packet
R7#
*May 15 13:58:57.515: %SEC-6-IPACCESSLOGP: list FPM_BAD_DNS_CLASS3 denied
udp 192.1.49.1(53) (FastEthernet0/0 ) -> 6.6.146.4(59393), 1 packet


R7#sh policy-map type access-control int f0/0
 FastEthernet0/0

  Service-policy access-control input: FPM_POL

    Class-map: STACK (match-all)
      25 packets, 2196 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x11 next UDP
      Match: field UDP source-port eq 0x35 next UDP

      Service-policy access-control : FPM_DNS_POL

        Class-map: FPM_BAD_DNS_CLASS (match-all)
          9 packets, 828 bytes
          5 minute offered rate 0 bps
          Match: field UDP source-port eq 53
          Match: start UDP payload-start offset 0 size 100 regex
".*[Rr]10.[Ii][Pp][Ee][Xx][Pp][Ee][Rr][Tt].[Cc][Oo][Mm].*"
      log
      drop

        Class-map: class-default (match-any)
          16 packets, 1368 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

    Class-map: class-default (match-any)
      12 packets, 1128 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

```
        Match: any
```

Task 7.2: Preventing Network Attacks (4 Points)

- A hub is going to be connected to VLAN 146 via CAT1 port F0/9
- On that hub there is a host with MAC address 4200.8111.0000 which should not be accessed outside the hub
- Do not use an ACL to prevent communication
- Prevent users from using embedded commands in all FTP sessions through the ASA
- To enable future investigation of attacks coming from the Internet, enable accounting on R7 F0/0. The accounting reports should include protocol details

Detailed Solution

CAT1

```
interface FastEthernet0/9
 switchport access vlan 146
!
mac address-table static 4200.8111.0000 vlan 146 drop
```

ASA3

```
policy-map global_policy
 class inspection_default
  inspect ftp strict
```

R7

```
interface FastEthernet0/0
 ip nbar protocol-discovery
```

Configuring the CAM table to drop packets with destination address 4200.8111.0000 will effectively drop traffic for that device on the switch but will not affect it on the hub.

As was shown earlier in the lab configuring strict FTP prevents the use of unknown commands.

NBAR is usually used for QoS classification, but it can also be used as accounting tool.

Verification

First let's see what's going on before we configure FPM:

```
CAT1#sh mac address-table vlan 146 | in Drop
 146    4200.8111.0000    STATIC      Drop

ASA(config)# sh service-policy global inspect ftp

Global policy:
  Service-policy: global_policy
    Class-map: FTP_CLASS
      Inspect: ftp strict FTP, packet 5, lock fail 0, drop 0, reset-drop 1
        match server regex MSG220
          reset log, packet 1
    Class-map: inspection_default
      Inspect: ftp strict, packet 0, lock fail 0, drop 0, reset-drop 0

R7#sh ip nbar protocol-discovery

 FastEthernet0/0

 Last clearing of "show ip nbar protocol-discovery" counters 00:00:18


                            Input                    Output
                            -----                    ------
   Protocol                 Packet Count             Packet Count
                            Byte Count               Byte Count
                            5min Bit Rate (bps)      5min Bit Rate (bps)
                            5min Max Bit Rate (bps)  5min Max Bit Rate
(bps)
   ------------------------ ------------------------ ----------------------
---
   netbios                  0                        1
                            0                        243
                            0                        0
                            0                        0
   ospf                     0                        2
                            0                        188
                            0                        0
                            0                        0
   unknown                  3                        0
                            180                      0
```

```
                              0                         0
                              0                         0
      Total                   3                         3
                              180                       431
                              0                         0
                              0                         0
```

Task 7.3: Preventing Network Attacks (4 Points)

- A web server on VLAN 2 is under attack. Its IP address is 6.6.2.199
- Using a sniffer you notice the following line: “GET /scripts../winnt/system32/cmd.exe?”
- It looks like users on VLAN 4 are infected with a Trojan
- The web server is using the following ports: 80, 8080 and 21
- Configure R2 S0/1/0 interface to prevent such attacks

Detailed Solution

R2

```
ip nbar port-map ftp tcp 9999
ip nbar port-map http tcp 80 8080 21
!
access-list 101 permit ip 6.6.4.0 0.0.0.255 host 6.6.2.199

class-map match-all HTTP_ATTACK_CLASS
 match access-group 101
 match protocol http url "*cmd.exe*”

policy-map STOP_IN
 class HTTP_ATTACK_CLASS
   drop

interface s0/1/0
 service-policy in STOP_IN
```

Because FTP by default is defined to be using port 21, it is not possible to configure NBAR to look for HTTP on port 21. Configure NBAR to look for FTP on port 9999. Then NBAR can be changed to look for HTTP traffic on ports 80, 8080 and 21.

Configure class-maps to differentiate between legitimate HTTP traffic and an attack. The attack will match HTTP sessions that includes “cmd.exe” in their URL:

Verification

First let’s see what’s going on before we configure FPM:

```
R2#sh ip nbar port-map http
port-map http                       tcp 80 8080 21

R2#sh policy-map int s0/1/0

 Serial0/1/0

  Service-policy input: STOP_IN

    Class-map: HTTP_ATTACK_CLASS (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Match: protocol http url "*cmd.ex*e"
      drop

    Class-map: class-default (match-any)
      27 packets, 3716 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

LAB 2

Please look at the provided diagrams and read through the whole lab before you start. Read the directions very carefully to make sure you are doing what is being asked of you. This concept is very important when you take the CCIE lab administered by Cisco

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

- 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

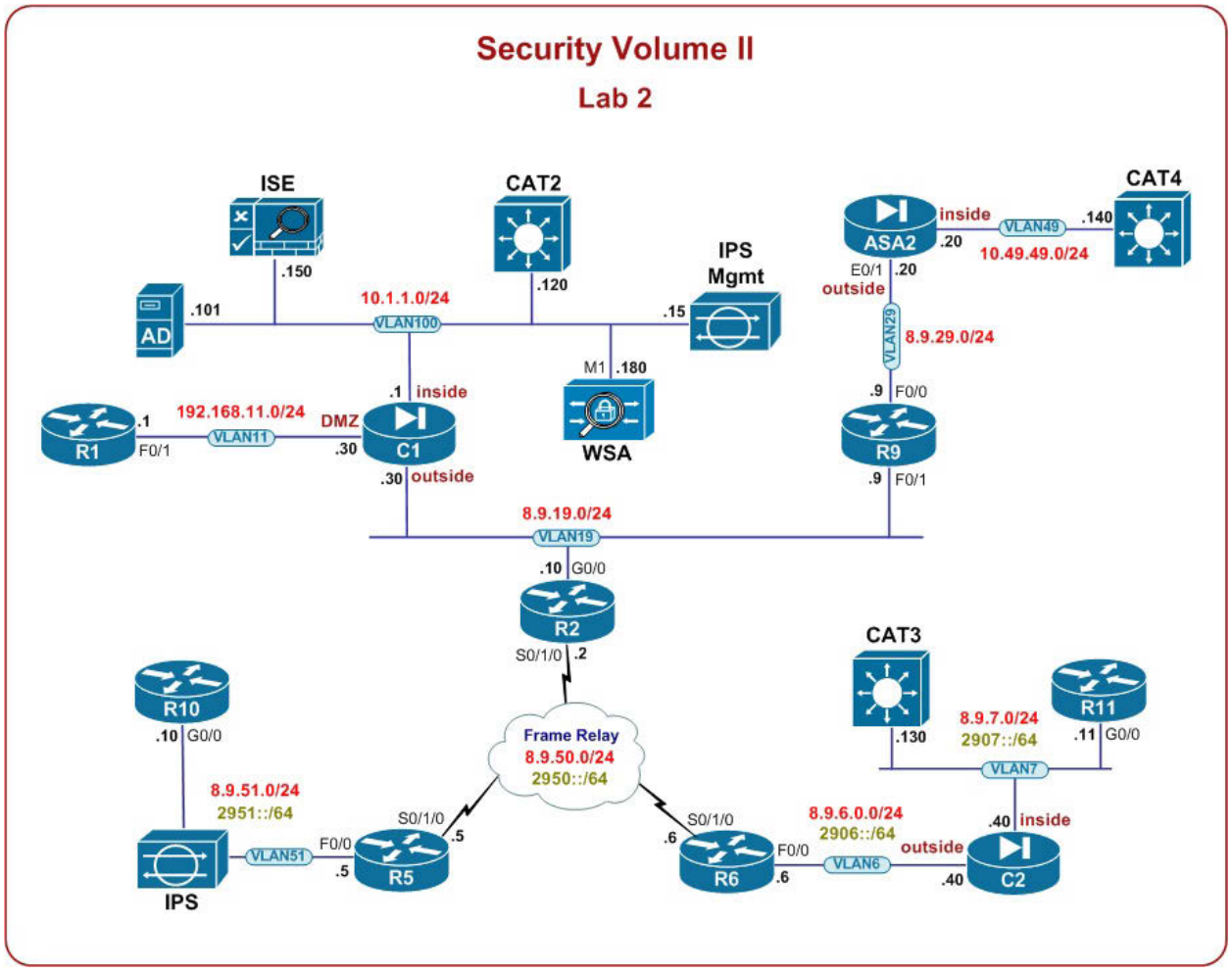
NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device

Estimated Time to Complete: **8-10 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	F0/1	11	192.168.11.1/24
	Loop0		8.9.100.1/32
R2	G0/0	19	8.9.19.2/24
	S0/1/0		8.9.50.2/24
			2950::2/64
	Loop0		8.9.100.2/32
R5	F0/0	51	8.9.51.5/24
			2951::5/64
	S0/1/0		8.9.50.5/24
	Loop0		2950::5/64
			8.9.100.5/32
R6	F0/0	6	8.9.6.6/24
			2906::6/64
	S0/1/0		8.9.50.6/24
			2950::6/64
	Loop0		8.9.100.6/32
R9	F0/0	29	8.9.29.9/24
	F0/1	19	8.9.19.9/24
	Loop0		8.9.100.9/32
R10	G0/0		8.9.51.10/24
			2951::10/64
	Loop0		8.9.100.10/32
R11	G0/0	7	8.9.7.11/24
			2907::11/64
	Loop0		8.9.100.11/32
CAT2	VLAN100	100	10.1.1.120/24
CAT3	VLAN7	7	8.9.7.130/24
CAT4	VLAN49	49	10.49.49.140/24
ASA2	Redundant1	49	10.49.49.20/24
	E0/1	29	8.9.29.20/24
ASA – C1	PortChannel1.100	100	10.1.1.1/24
	PortChannel1.11	11	192.168.11.30/24
	PortChannel1.19	19	8.9.19.30/24
ASA – C2	G0/3.6	6	8.9.6.40/24
			2906::40/24
	G0/3.7	7	8.9.7.40/24
			2907::40/64
ISE		100	10.1.1.150/24
IPS	Mgmt	100	10.1.1.15/24
WSA	M1	100	10.1.1.180/24
AD		100	10.1.1.101/24



Solutions

1.0 ASA Firewalls (28 points)

Task 1.1: ASA Setup (4 Points)

- Create two contexts on ASA3. Name one context "C1" and the other "C2"
- Configure the interfaces according to the diagram and the IP Addressing table
- Ports G0/0 and G0/1 should be load-balancing the traffic
- Don't create any interface mappings for the contexts
- Set security-level to 50 on interface DMZ
- Configure C1 to be the admin context
- Make sure ICMP Echo replies are allowed across the contexts but don't use an ACL to accomplish this
- You can add 3 static routes on ASA C2 to obtain full IP reachability for public networks

Detailed Solution

CAT3, CAT4

```
int range g1/0/19 – 20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 1 mode passive

int g1/0/22
 sw trunk encap dot1
 sw mode trunk
 spanning-tree portfast trunk
```

ASA3

```
mode multiple

hostname ASA
!
```

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no sh

interface GigabitEthernet0/1
 channel-group 1 mode active
 no sh

interface GigabitEthernet0/2
 no sh

interface GigabitEthernet0/3
 no sh

int management0/0
 no sh

interface GigabitEthernet0/3.6
 vlan 6
interface GigabitEthernet0/3.7
 vlan 7

interface Port-channel1.11
 vlan 11
interface Port-channel1.100
 vlan 100
interface Port-channel1.19
 vlan 19

context C1
  allocate-interface Port-channel1.11
  allocate-interface Port-channel1.100
  allocate-interface Port-channel1.19
  config-url disk0:/C1.cfg

context C2
  allocate-interface GigabitEthernet0/3.6
  allocate-interface GigabitEthernet0/3.7
  config-url disk0:/C2.cfg
```

```
admin-context C1
```

ASA3/C1

```
change context C1

interface Port-channel1.19
 nameif outside
 security-level 0
 ip address 8.9.19.30 255.255.255.0 standby 8.9.19.31
!
interface Port-channel1.11
 nameif DMZ
 security-level 50
 ip address 192.168.11.30 255.255.255.0 standby 192.168.11.31
!
interface Port-channel1.100
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0 standby 10.1.1.31

fixup proto icmp
```

ASA3/C2

```
change context C2

interface GigabitEthernet0/3.6
 nameif outside
 security-level 0
 ip address 8.9.6.40 255.255.255.0 standby 8.9.6.41
 ipv6 address 2906::40/64 standby 2906::41
!
interface GigabitEthernet0/3.7
 nameif inside
 security-level 100
 ip address 8.9.7.40 255.255.255.0 standby 8.9.7.41
 ipv6 address 2907::40/64 standby 2907::41

route outside 0.0.0.0 0.0.0.0 8.9.6.6 1
route inside 8.9.100.11 255.255.255.255 8.9.7.11 1
```

```
ipv6 route outside ::/0 2906::6

fixup proto icmp
```

Always make sure to read the whole lab prior to beginning. This way you can save a lot of time during the exam day. Here we prepared switches and interface configs on the ASA for future failover task.

It is always a good idea to check the Layer 2 configuration especially when trunks are used on the ASA.

EtherChannels can be only created in system context and in this case their subinterfaces will be used as inside and DMZ. Since we were not told to statically configure a bundle vs dynamically negotiate it I would go for a recommended solution, which is LACP.

We are not allowed to use any ACLs for ICMP Echo replies so we are being led to add ICMP inspection to the global policy.

Verification

```
CAT3#sh etherchannel 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) Gi1/0/20(P)

ASA3(config)# sh port-channel 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)   Gi0/1(P)

ASA3/C1(config)# sh int ip br
Interface                 IP-Address      OK? Method Status
Protocol
Port-channel1.19           8.9.19.30     YES manual up
up
Port-channel1.11           192.168.11.30 YES manual up
up
Port-channel1.100          10.1.1.1      YES manual up
up

ASA3/C2(config)# sh int ip br
Interface                IP-Address        OK? Method Status
Protocol
GigabitEthernet0/3.6      8.9.6.40        YES manual up
up
GigabitEthernet0/3.7      8.9.7.40        YES manual up
up

ASA3/C1(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 = 1/2/10 ms

ASA3/C2(config)# ping 8.9.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.9.6.6, timeout is 2 seconds:
```

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

ASA3/C2(config)# ping 8.9.7.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.9.7.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms

ASA3/C2(config)# ping 2906::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2906::6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R11#ping 2950::5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2950::5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
```

Task 1.2: ASA2 Setup (3 Points)

- Initialize ASA2 according to the topology and IP addressing table
- Increase the security appliance's reliability by ensuring that if E0/0 interface fails, the standby interface becomes active and starts passing traffic
- Use E0/2 as a backup port
- Allow Echo Replies through the firewall but don't inspect ICMP

Detailed Solution

CAT4

```
interface GigabitEthernet1/0/6
 switchport access vlan 49
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/8
```

```
 switchport access vlan 49
 switchport mode access
 spanning-tree portfast
```

ASA2

```
hostname ASA2

interface Redundant1
 member-interface Ethernet0/0
 member-interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.49.49.20 255.255.255.0

interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 8.9.29.20 255.255.255.0
 no sh

int e0/0
 no sh

int e0/2
 no sh

access-list OUTSIDE_IN extended permit icmp any any echo-reply
access-group OUTSIDE_IN in interface outside
```

Whenever you deal with redundant ports don't forget to mirror the switch interface configuration.

Verification

```
ASA2(config)# sh int ip br
Interface              IP-Address      OK? Method Status
Protocol
```

```
Ethernet0/0             unassigned      YES unset  up
up
Ethernet0/1             8.9.29.20       YES manual up
up
Ethernet0/2             unassigned      YES unset  up
up
Ethernet0/3             unassigned      YES unset  administratively down
up
Management0/0           unassigned      YES unset  administratively down
down
Redundant1              10.49.49.20     YES manual up
up

ASA2(config)# ping 8.9.29.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.9.29.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA2(config)# ping 10.49.49.140
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.49.49.140, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

Task 1.3: Failover (4 Points)

- Implement stateful failover for both firewall contexts
- ASA3 should be active for context C1. ASA4 must handle C2
- If one firewall fails the other unit should be active for both contexts
- Use the G0/2 interface as the failover link (172.99.99.0/24)
- Every single interface in both contexts should send and receive failover keepalives
- Set the interface polling timers to 1 second and holdtime to the minimal possible value
- Secure the failover communication

Detailed Solution

CAT4

```
vlan 99
```

```
int g1/0/21
 sw host
 sw acc vlan 99
```

CAT3

```
int g1/0/21
 sw host
 sw acc vlan 99
```

ASA3

```
failover lan unit primary

failover lan interface FAIL g0/2
failover int ip FAIL 172.99.99.1 255.255.255.0 standby 172.99.99.254
failover link FAIL G0/2

failover key cisco

failover polltime msec 300 holdtime 1

failover group 1
  primary
  polltime interface 1 holdtime 5
  preempt
failover group 2
  secondary
  polltime interface 1 holdtime 5
  preempt

context C1
  join-failover-group 1
context C2
  join-failover-group 2
```

Not required but useful :

```
prompt hostname context state
```

ASA4

```
mode multiple

int g0/2
 no sh

failover lan unit secondary
failover lan interface FAIL g0/2
failover int ip FAIL 172.99.99.1 255.255.255.0 standby 172.99.99.254

failover key cisco
```

ASA3/C1

```
monitor-interface outside
monitor-interface DMZ
monitor-interface inside
```

ASA4/C2

```
monitor-interface outside
monitor-interface inside
```

Logical interfaces are not monitored by default. Ensure to add them in both contexts. Use context sensitive help to determine the minimal polling values.

Interface polltime values don't appear to be displayed correctly in the "show failover" output in this code version.

Verification

You will not be able to test these requirements until you configure the next task.

```
CAT4#sh eth summ
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) Gi1/0/20(P)


ASA3/stby(config)# sh port sum
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)   Gi0/1(P)


ASA3/C1/act(config)# sh monitor-interface
        This host: Primary - Active
                Interface outside (8.9.19.30): Normal (Monitored)
                Interface DMZ (192.168.11.30): Normal (Monitored)
                Interface inside (10.1.1.1): Normal (Monitored)
        Other host: Secondary - Standby Ready
                Interface outside (8.9.19.31): Normal (Monitored)
                Interface DMZ (192.168.11.31): Normal (Monitored)
                Interface inside (10.1.1.31): Normal (Monitored)


ASA3/C1/act(config)# sh failover
Failover On
```

```
Last Failover at: 14:57:27 UTC May 17 2013
        This context: Active
                Active time: 287 (sec)
                  Interface outside (8.9.19.30): Normal (Monitored)
                  Interface DMZ (192.168.11.30): Normal (Monitored)
                  Interface inside (10.1.1.1): Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface outside (8.9.19.31): Normal (Monitored)
                  Interface DMZ (192.168.11.31): Normal (Monitored)
                  Interface inside (10.1.1.31): Normal (Monitored)

Stateful Failover Logical Update Statistics
        Status: Configured.
        Stateful Obj    xmit       xerr       rcv        rerr
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP 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          0          0
        User-Identity   1          0          0          0


ASA3/C2/act(config)# sh failover
Failover On
Last Failover at: 14:57:23 UTC May 17 2013
        This context: Active
                Active time: 312 (sec)
                  Interface outside (8.9.6.40/fe80::2a0:c9ff:fe04:201):
Normal (Monitored)
                  Interface inside (8.9.7.40/fe80::2a0:c9ff:fe04:201):
Normal (Monitored)
        Peer context: Standby Ready
                Active time: 0 (sec)
                  Interface outside (8.9.6.41/fe80::2a0:c9ff:fe04:202):
Normal (Monitored)
                  Interface inside (8.9.7.41/fe80::2a0:c9ff:fe04:202):
Normal (Monitored)
```

```
Stateful Failover Logical Update Statistics
        Status: Configured.
        Stateful Obj    xmit       xerr       rcv        rerr
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP 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          0          0
        User-Identity   1          0          0          0
```

Task 1.4: NAT & Routing (3 Points)

- PAT all internal and DMZ networks to the outside's interface IP address on context C1
- ISE should be always seen as 8.9.19.150 on the outside
- CAT2 should be translated to 8.9.19.120 unless it communicates with R5's loopback – then the address should be changed to 8.9.19.220
- NAT R1 to 8.9.19.1. Hosts on the DMZ using an outside DNS server should see R1's original IP address in the DNS replies
- Enable OSPF on ASA's outside interface
- Add a default route on C1 pointing to R2; also configure a route to R1's loopback0 and a route to R1's loopback 99 (99.99.99.0/24) in the DMZ

Detailed Solution

ASA2

```
router ospf 1
 network 8.9.29.20 255.255.255.255 area 0
```

C1

```
object network INTERNAL
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

```
object network DMZ
 subnet 192.168.11.0 255.255.255.0
 nat (DMZ,outside) dynamic interface

object network ISE
 host 10.1.1.150
 nat (inside,outside) static 8.9.19.150

object network R1
 host 192.168.11.1
 nat (DMZ,outside) static 8.9.19.1 dns

object network CAT2
 host 10.1.1.120
object network CAT2_120
 host 8.9.19.120
object network CAT2_220
 host 8.9.19.220
object network R5LOOP
 host 8.9.100.5

nat (inside,outside) source static CAT2 CAT2_220 destin static R5LOOP
R5LOOP
nat (inside,outside) source static CAT2 CAT2_120

route outside 0.0.0.0 0.0.0.0 8.9.19.2 1
route DMZ 8.9.100.1 255.255.255.255 192.168.11.1
route DMZ 99.99.99.0 255.255.255.0 192.168.11.1 1
```

The “dns” keyword added to the static command for R1 will translate the A record in DNS replies coming back to the DMZ network.

Verification

```
ASA3/C1/act(config)# sh nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static CAT2 CAT2_220 destination static
R5LOOP R5LOOP
    translate_hits = 1, untranslate_hits = 1
2 (inside) to (outside) source static CAT2 CAT2_120
```

```
    translate_hits = 2, untranslate_hits = 11

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static ISE 8.9.19.150
    translate_hits = 0, untranslate_hits = 0
2 (DMZ) to (outside) source static R1 8.9.19.1   dns
    translate_hits = 3, untranslate_hits = 0
3 (inside) to (outside) source dynamic INTERNAL interface
    translate_hits = 2, untranslate_hits = 3
4 (DMZ) to (outside) source dynamic DMZ interface
    translate_hits = 0, untranslate_hits = 0



CAT2#telnet 8.9.19.2
Trying 8.9.19.2 ... Open

R2>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:44
*578 vty 0                 idle                 00:00:00 8.9.19.120

  Interface    User               Mode         Idle     Peer Address


CAT2#telnet 8.9.100.5
Trying 8.9.100.5 ... Open

R5>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:51
*514 vty 0                 idle                 00:00:00 8.9.19.220

  Interface    User               Mode         Idle     Peer Address


Gateway of last resort is 10.1.1.1 to network 0.0.0.0
```

Change IP address on CAT2 and test PAT. Don't forget to put the correct address afterwards :

```
CAT2(config-if)#do telnet 8.9.19.2
```

```
Trying 8.9.19.2 ... Open

R2>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:05:24
*578 vty 0                 idle                 00:00:00 8.9.19.30

  Interface    User               Mode         Idle     Peer Address


R1#telnet 8.9.19.2
Trying 8.9.19.2 ... Open

R2>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:08:21
*578 vty 0                 idle                 00:00:00 8.9.19.1

  Interface    User               Mode         Idle     Peer Address

ASA3/C1/act(config)# sh xlate
4 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
NAT from inside:10.1.1.120 to outside:8.9.19.220
    flags s idle 0:05:08 timeout 0:00:00
NAT from inside:10.1.1.120 to outside:8.9.19.120
    flags s idle 0:07:46 timeout 0:00:00
NAT from inside:10.1.1.150 to outside:8.9.19.150
    flags s idle 0:48:15 timeout 0:00:00
NAT from DMZ:192.168.11.1 to outside:8.9.19.1
    flags sD idle 0:00:06 timeout 0:00:00
```

Task 1.5: Access Control (2 Points)

- Allow the following traffic to ISE & CAT2 on C1 :
  - HTTP standard port + port 8081
  - HTTPs standard port + port 8443
  - SSH

    - RADIUS (both RFCs)
- Accomplish this with just one ACL entry
- ICMP Echos should be allowed across all ASAs/contexts
- Enable ACL optimization on C1

Detailed Solution

C1

```
object-group service ISE_PORTS
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq 8443
 service-object tcp destination eq 8081
 service-object tcp destination eq ssh
 service-object udp destination eq radius
 service-object udp destination eq radius-acct
 service-object udp destination eq 1812
 service-object udp destination eq 1813

access-list OUTSIDE_IN extended permit icmp any any echo
access-list OUTSIDE_IN per object-group ISE_PORTS any object-group
ISE_CAT2
access-group OUTSIDE_IN in interface outside

object-group-search access-control
```

C2

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

ASA2

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

The “object-group-search” command optimizes all ACLs in the inbound direction – with this feature enabled all ACL entries are reinserted with object-group IDs instead of their elements.

Verification

Before ACL Optimization was enabled we have 17 elements here (object-groups are expanded) :

```
ASA3/C1/act(config)# sh access-l
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTSIDE_IN; 17 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit icmp any any echo (hitcnt=0)
0x869bdf05
access-list OUTSIDE_IN line 2 extended permit object-group ISE_PORTS any
object-group ISE_CAT2 0x00ff84d7
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.150 eq
www (hitcnt=0) 0xda2a3260
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.120 eq
www (hitcnt=0) 0x192cb3b1
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.150 eq
https (hitcnt=0) 0xfea42943
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.120 eq
https (hitcnt=0) 0xd35771c6
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.150 eq
8443 (hitcnt=0) 0x41aa726d
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.120 eq
8443 (hitcnt=0) 0xb03b5007
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.150 eq
ssh (hitcnt=0) 0x89e184cd
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.120 eq
ssh (hitcnt=0) 0xba91b793
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.150 eq
radius (hitcnt=0) 0x1de58bf6
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.120 eq
radius (hitcnt=0) 0x01b5d2ad
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.150 eq
radius-acct (hitcnt=0) 0xac536814
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.120 eq
radius-acct (hitcnt=0) 0x278abd8a
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.150 eq
1812 (hitcnt=0) 0x2f30e6dd
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.120 eq
1812 (hitcnt=0) 0xcdeea7e8
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.150 eq
1813 (hitcnt=0) 0x9d4490f9
  access-list OUTSIDE_IN line 2 extended permit udp any host 10.1.1.120 eq
1813 (hitcnt=0) 0x647a4222
```

After the feature is enabled we cut down on the amount of ACL entries in the output of “show access-list” :

```
ASA3/C1/act(config)# sh access-l
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTSIDE_IN; 9 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit icmp any any echo (hitcnt=0)
0x869bdf05
access-list OUTSIDE_IN line 2 extended permit object-group ISE_PORTS any
object-group ISE_CAT2 0x00ff84d7
  access-list OUTSIDE_IN line 2 extended permit tcp any(65536) object-
group ISE_CAT2(2) eq www (hitcnt=0) 0xc20923fe
  access-list OUTSIDE_IN line 2 extended permit tcp any(65536) object-
group ISE_CAT2(2) eq https (hitcnt=0) 0x06656a1e
  access-list OUTSIDE_IN line 2 extended permit tcp any(65536) object-
group ISE_CAT2(2) eq 8443 (hitcnt=0) 0x6c5d5519
  access-list OUTSIDE_IN line 2 extended permit tcp any(65536) object-
group ISE_CAT2(2) eq ssh (hitcnt=0) 0x8acbcde9
  access-list OUTSIDE_IN line 2 extended permit udp any(65536) object-
group ISE_CAT2(2) eq radius (hitcnt=0) 0x4b2051ed
  access-list OUTSIDE_IN line 2 extended permit udp any(65536) object-
group ISE_CAT2(2) eq radius-acct (hitcnt=0) 0x492462ef
  access-list OUTSIDE_IN line 2 extended permit udp any(65536) object-
group ISE_CAT2(2) eq 1812 (hitcnt=0) 0xfe283df0
  access-list OUTSIDE_IN line 2 extended permit udp any(65536) object-
group ISE_CAT2(2) eq 1813 (hitcnt=0) 0xaa27852a
```

Task 1.6: BGP Authentication (3 Points)

- R1 (AS11) and R2 (AS256) should be able to establish a BGP session through C1
- Configure the firewall to allow BGP devices authenticate each other
- Enable BGP authentication (use password “ip?expert”)
- R2 should be able to initiate a session to R1

Detailed Solution

R1

```
router bgp 11
 neighbor 8.9.100.2 password ip?expert
```

R2

```
router bgp 256
 neighbor 8.9.100.1 password ip?expert
```

C1

```
access-list OUTSIDE_IN permit tcp host 8.9.100.2 host 8.9.100.1 eq bgp

access-list BGP extended permit tcp any any eq bgp
class-map BGP
 match access-list BGP

tcp-map BGP_MAP
  tcp-options range 19 19 allow

policy-map global_policy
 class BGP
  set connection random-sequence-number disable
  set connection advanced-options BGP_MAP
```

To include a "?" in the password first press CTRL+V.

There are two key things to remember when it comes to authentication of a BGP session across PIX/ASA firewall. First is to leave option 19 in the TCP header (MD-5 hash) and the other is to disable sequence number randomization for that connection.

Also, if there was a translation going on for an address used by the peering you would have to exempt it (static identity) from the NAT process (IP address is also a part of hash calculation).

Verification

```
ASA3/C1/act(config)# sh service-pol global set connection

Global policy:
  Service-policy: global_policy
```

```
    Class-map: BGP
      Set connection policy: random-sequence-number disable
        drop 0
      Set connection advanced-options: BGP_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

R1#sh ip bgp neighbors 8.9.100.2 | in md5
Option Flags: nagle, path mtu capable, md5, 0x1000000

R1#sh ip bgp summary
BGP router identifier 8.9.100.1, local AS number 11
BGP table version is 2, main routing table version 2
1 network entries using 136 bytes of memory
1 path entries using 52 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 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 336 total bytes of memory
BGP activity 2/1 prefixes, 2/1 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
8.9.100.2       4            256      12      10        2    0    0 00:06:30
1
```

Task 1.7: HTTP Inspection (3 Points)

- Enable HTTP Server on Cat2 on port 8081 and inspect all HTTP traffic going to it
- ASA should substitute a string for the server header field with “APACHE 2.2.3 (Linux/SUSE)”
- Drop and log connection if HTTP Protocol violation occurs
- HTTP Inspection should be performed on TCP port 80 and 8081 on the outside
- Drop and log connection if users are trying to connect to “badsite.com” domain

Detailed Solution

CAT2

```
ip http server
ip http port 8081
```

C1

```
access-list HTTP_TO_CAT2 permit tcp any host 10.1.1.120 eq 80
access-list HTTP_TO_CAT2 permit tcp any host 10.1.1.120 eq 8081

regex BADSITE "[Bb][Aa][Dd][Ss][Ii][Tt][Ee]\.[Cc][Oo][Mm]"
class-map HTTP_CAT2_CLASS
 match access-list HTTP_TO_CAT2

policy-map type inspect http HTTP_DPI
 parameters
  spoof-server "APACHE 2.2.3 (Linux/SUSE)"
  protocol-violation action drop-connection log
 match request header host regex BADSITE
  drop-connection log

policy-map OUTSIDE_POL
 class HTTP_CAT2_CLASS
  inspect http HTTP_DPI

service-policy OUTSIDE_POL interface outside
```

To set application-level parameters for deep packet inspection you have to use “type inspect” policy-maps. Next step is to apply it to the “inspect” action in the policy-map for a particular class of traffic.

Although not necessary for this task, the regular expression used allows us to match case insensitive strings in the URL.

Verification

```
R2#telnet 8.9.19.120 8081
Trying 8.9.19.120, 8081 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Wed, 03 Mar 1993 07:20:09 GMT
Server:APACHE 2.2.3 (Linux/SUSE)
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 8.9.19.120 closed by foreign host]
```

For the second part of the test temporarily change the HTTP port to 80 on CAT2 :

```
CAT2(config)#ip http port 80

R2#copy http://badsite.com/file null0
Destination filename [null0]?
Accessing http://badsite.com/file...
Translating "badsite.com"

ASA3/C1/act(config)# %ASA-4-507003: tcp flow from outside:8.9.19.2/29088
to inside:10.1.1.120/80 terminated by inspection engine, reason -
disconnected, dropped packet.


ASA3/C1/act(config)# sh service-policy interface outside inspect http

Interface outside:
  Service-policy: OUTSIDE_POL
```

```
    Class-map: HTTP_CAT2_CLASS
      Inspect: http HTTP_DPI, packet 22, lock fail 0, drop 1, reset-drop 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
        protocol violations
          log, packet 0
        server spoofs, packet 1
        match request header host regex BADSITE
          drop-connection log, packet 1
```

Task 1.8: Traffic Control (3 Points)

- Permit the following ICMP and ICMPv6 traffic to the ASA C2 interfaces :
  - Echo Replies
  - Time-Exceed messages
  - Unreachables
- All other unnecessary ICMP & ICMPv6 traffic should be explicitly dropped & logged
- Users on VLAN 7 are using a telnet application. Sometimes they leave the sessions open for 2 hours, and when they return they are forced to reestablish the session. Configure the ASA to keep all the Telnet sessions alive for more than 2 hours
- Only invalid/expired sessions should be removed from the connection table
- This configuration should only apply to Telnet traffic

Detailed Solution

C2

```
icmp permit any echo-reply inside
icmp permit any time-exceeded inside
icmp permit any unreachable inside
icmp deny any inside

icmp permit any echo-reply outside
icmp permit any time-exceeded outside
icmp permit any unreachable outside
icmp deny any outside

ipv6 icmp permit any echo-reply inside
ipv6 icmp permit any unreachable inside
ipv6 icmp permit any time-exceeded inside
ipv6 icmp permit any neighbor-advertisement inside
ipv6 icmp permit any neighbor-solicitation inside
```

```
ipv6 icmp deny any inside

ipv6 icmp permit any echo-reply outside
ipv6 icmp permit any unreachable outside
ipv6 icmp permit any time-exceeded outside
ipv6 icmp permit any neighbor-advertisement outside
ipv6 icmp permit any neighbor-solicitation outside
ipv6 icmp deny any outside

class-map TELNET
 match port tcp eq telnet

policy-map global_policy
 class TELNET
    set connection timeout idle 2:01:00 dcd
```

Don't forget L3-L2 resolution in IPv6 relies on ICMPv6 ND/NA messages. Explicit deny would normally drop those packets so this is something we want to allow in order not to break IPv6 communication.

DCD detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist.

Verification

```
ASA3/C2/act(config)# ping 8.9.7.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.9.7.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms

CAT3#ping 8.9.7.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.9.7.40, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

%ASA-3-313001: Denied ICMP type=8, code=0 from 8.9.7.130 on interface
inside
```

```
ASA3/C2/act(config)# ping 2907::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2907::11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

R11#ping 2907::40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2907::40, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

%ASA-3-313008: Denied IPv6-ICMP type=128, code=0 from 2907::11 on
interface inside

ASA3/C2/act(config)# clear ipv neighbors

ping 2907::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2907::11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA3/C2/act(config)# ping 2906::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2906::6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3/C2/act(config)# sh ipv neighbor
IPv6 Address                              Age Link-layer Addr State
Interface
2906::6                                     0 001b.d518.4158  REACH
outside
2907::11                                    0 c84c.751f.ddc0  REACH inside
fe80::ca4c:75ff:fe1f:ddc0                   0 c84c.751f.ddc0  DELAY inside
```

If you establish an Idle Telnet session through C2, after 3 hours expire the DCD counters will increase. This does not mean the session is removed from the table – as long as it is valid it will be left untouched :

```
ASA3/C2/act(config-pmap-c)# sh service-policy global set connection

Global policy:
  Service-policy: global_policy
    Class-map: TELNET
      Set connection policy:          drop 0
      Set connection timeout policy:
        idle 3:00:00
        DCD: enabled, retry-interval 0:00:15, max-retries 5
        DCD: client-probe 1, server-probe 1, conn-expiration 0


ASA3/C2/act# sh conn
5 in use, 10 most used
TCP outside 8.9.100.6:23 inside 8.9.7.11:57183, idle 0:00:03, bytes 53,
flags UIO
```

Task 1.9: Logging (3 Points)

- Configure console logging on C2. Log warning messages and above
- Logging messages should be time-stamped
- Use the facility LOCAL2 for syslog messages at level information and higher
- Syslog messages should be sent to the ISE
- Console logs should inform you whenever new stateful ICMP session is built

Detailed Solution

C1

```
access-list OUTSIDE_IN permit udp host 8.9.6.40 host 10.1.1.150 eq syslog
```

C2

```
logging enable
logging timestamp
logging console warnings
logging trap informational
```

```
logging facility 18
logging host outside 8.9.19.150
logging message 302020 level warnings
```

To verify which logging facility name corresponds to which number you check the documentation. Just refer to the “logging” command.

Other part of the question asks you to include information about newly created ICMP sessions (we have ICMP inspection enabled) in the console logs. Because we are told that console logging should be working on level 4, this information will not be included by default. To move a particular message to an arbitrary log level use the “logging message” command. To find the message number use the documentation (you can use CTRL+F and try to search for keywords they give you in the question).

Verification

Ping through C2 and observe the logs :

```
ASA3/C2/act(config)# May 20 2013 11:07:22: %ASA-4-302020: Built inbound
ICMP connection for faddr fe80::21b:d5ff:fe18:4158/0 gaddr ff02::1/0 laddr
ff02::1/0

May 20 2013 11:07:24: %ASA-4-302020: Built outbound ICMP connection for
faddr 8.9.6.6/0 gaddr 8.9.7.11/2 laddr 8.9.7.11/2
May 20 2013 11:07:24: %ASA-4-302020: Built outbound ICMP connection for
faddr 8.9.6.6/0 gaddr 8.9.7.11/2 laddr 8.9.7.11/2
May 20 2013 11:07:24: %ASA-4-302020: Built outbound ICMP connection for
faddr 8.9.6.6/0 gaddr 8.9.7.11/2 laddr 8.9.7.11/2

ASA3/C2/act(config)# sh logging
Syslog logging: enabled
    Facility: 18
    Timestamp logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: level warnings, 1811 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 18, 49 messages logged
        Logging to outside 8.9.19.150
```

```
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled

ASA3/C2/act(config)# sh loggi message
syslog 302020: default-level informational, current-level warnings
(enabled)
```

2.0 IOS Firewall (11 points)

Task 2.1: CBAC (3 Points)

- On R6, inspect TCP, UDP and ICMP traffic from the Ethernet segment going towards the Frame Relay network
- Only allow relevant traffic coming in
- All other traffic should be blocked
- Make sure router generated traffic is also inspected

Detailed Solution

R6

```
ip inspect name CBAC tcp router-traffic
ip inspect name CBAC udp router-traffic
ip inspect name CBAC icmp router-traffic

ip access-list extended OUTSIDE_IN
 permit ospf host 8.9.50.2 host 224.0.0.5
 permit ospf host 8.9.50.5 host 224.0.0.5
 permit ospf host 8.9.50.2 host 8.9.50.6
 permit ospf host 8.9.50.5 host 8.9.50.6
 permit ospf host 8.9.50.2 host 224.0.0.6
 permit ospf host 8.9.50.5 host 224.0.0.6
 permit tcp host 8.9.100.2 host 8.9.100.6 eq bgp
 100 deny   ip any any log

int s0/1/0
 ip inspect CBAC out
 ip access-group OUTSIDE_IN in
```

In this task we need to define the CBAC policy and apply it to outbound traffic (so that return traffic is permitted) and apply an inbound access-list to restrict traffic (with exceptions for all the various tasks in this lab). Always remember to verify if routing protocols are working correctly after you apply any type of filter on the devices.

Verification

```
R6#sh access-l
```

```
Extended IP access list OUTSIDE_IN
    10 permit ospf host 8.9.50.2 host 224.0.0.5 (47 matches)
    20 permit ospf host 8.9.50.5 host 224.0.0.5 (44 matches)
    30 permit ospf host 8.9.50.2 host 8.9.50.6
    40 permit ospf host 8.9.50.5 host 8.9.50.6
    50 permit ospf host 8.9.50.2 host 224.0.0.6
    60 permit ospf host 8.9.50.5 host 224.0.0.6
    70 permit tcp host 8.9.100.2 host 8.9.100.6 eq bgp (8 matches)
    100 deny ip any any log

R11#telnet 8.9.100.5
Trying 8.9.100.5 ... Open

R5>

R6#sh ip inspect sessions de
Established Sessions
 Session 49F502EC (8.9.7.11:54133)=>(8.9.100.5:23) tcp SIS_OPEN
  Created 00:00:04, Last heard 00:00:03
  Bytes sent (initiator:responder) [24:29]
  In  SID 8.9.100.5[23:23]=>8.9.7.11[54133:54133] on ACL OUTSIDE_IN  (8
matches)
Half-open Sessions
 Session 49F4FEAC (8.9.6.40:514)=>(8.9.19.150:514) udp SIS_OPENING
  Created 00:00:26, Last heard 00:00:04
  Bytes sent (initiator:responder) [780:0]
  In  SID 8.9.19.150[514:514]=>8.9.6.40[514:514] on ACL OUTSIDE_IN


R6#sh ip inspect config
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
    icmp alert is on audit-trail is off timeout 10
 inspection of router local traffic is enabled
```

Task 2.2: Firewall Tuning (3 Points)

- Only HTTP traffic from the CAT2 server (all) is allowed to contain JAVA applets
- Generate syslog message for each HTTP session creation and deletion
- Optimize the hash table size for an average of 4000 connections
- Limit the number of established firewall session to 5000
- DNS sessions should be managed for 4 seconds when there is no activity

Detailed Solution

R7

```
ip port-map http port tcp 8081

access-list 3 permit 8.9.19.120

ip inspect name CBAC http java-list 3 audit-trail on
ip inspect name CBAC parameter max-sessions 5000
ip inspect hashtable-size 4096
ip inspect dns-timeout 4
```

Because you were asked to allow JAVA applets in all HTTP traffic coming from Cat2 you have to add TCP port 8081 to the PAM table (Task 1.5). Otherwise traffic coming from that port will not be HTTP-inspected.

Verification

```
R6#sh ip inspect config
```

```
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 4 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
    icmp alert is on audit-trail is off timeout 10
 inspection of router local traffic is enabled
    http java-list 3 alert is on audit-trail is on timeout 3600
    session threshold is 5000

R11#telnet 8.9.19.120 8081
Trying 8.9.19.120, 8081 ... Open



R6#
*May 20 11:33:45.627: %FW-6-SESS_AUDIT_TRAIL_START: Start http session:
initiator (8.9.7.11:41814) -- responder (8.9.19.120:8081)

R6#sh ip ins sess de
Established Sessions
 Session 49F502EC (8.9.7.11:41814)=>(8.9.19.120:8081) http SIS_OPEN
  Created 00:00:05, Last heard 00:00:05
  Bytes sent (initiator:responder) [0:0]
  In  SID 8.9.19.120[8081:8081]=>8.9.7.11[41814:41814] on ACL OUTSIDE_IN
(1 matches)
Half-open Sessions
 Session 49F4FEAC (8.9.6.40:514)=>(8.9.19.150:514) udp SIS_OPENING
  Created 00:00:14, Last heard 00:00:01
  Bytes sent (initiator:responder) [1283:0]
```

```
In  SID 8.9.19.150[514:514]=>8.9.6.40[514:514] on ACL OUTSIDE_IN
```

Task 2.3: User-based Firewall (5 Points)

- Configure ZFW to control traffic traversing R9. Treat VLANs 29 & 49 as an internal networks
- All TCP, UDP and ICMP traffic should be allowed for authenticated users who are part of Active Directory domain IPEXPERT.COM (ALL_IPx_Users)
- Authenticate as “IPx_admin1” // “IPexpert123”
- Credentials required to join the domain are “Administrator” with password “IPexpert123”
- Outgoing ICMP packets should be limited to 16kbps
- AD server can be used as a source of Time and DNS information
- Protect RADIUS communication with key “ipexpert”
- Allow all other traffic necessary for this lab

Detailed Solution

R9

```
aaa new-model
aaa authentication login default group radius
aaa authentication login NO none
aaa authorization auth-proxy default group radius
line con 0
 login auth NO

radius-server host 8.9.19.150 auth-port 1645 acct-port 1646 key ipexpert

ip admission name AUTHP proxy http inactivity-time 60

ip http server

ip access-list extended OUTIN_INSPECT
ip access-list extended OUTIN_PASS

class-map type inspect match-all ZFW_OUTIN_PASS_CLASS
 match access-group name OUTIN_PASS

class-map type inspect match-all ZFW_INOUT_ICMP_CLASS
```

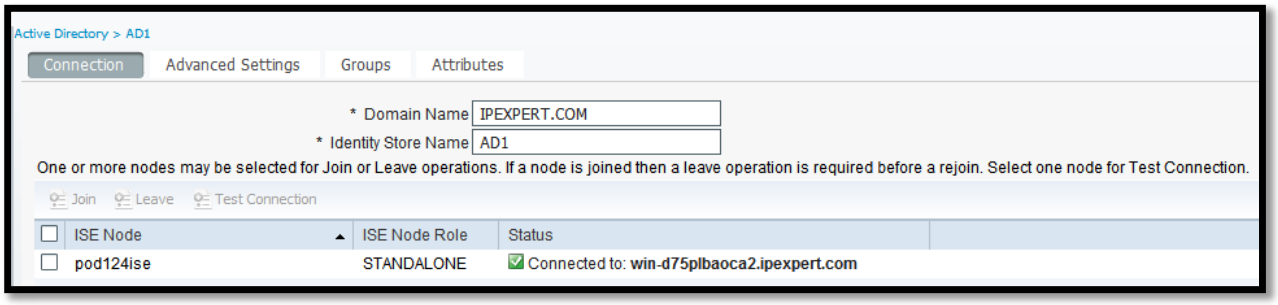
```
 match protocol icmp
 match user-group INTERNAL

class-map type inspect match-all ZFW_OUTIN_INSPECT_CLASS
 match access-group name OUTIN_INSPECT

class-map type inspect match-any ZFW_TCP_UDP_CLASS
 match protocol tcp
 match protocol udp

class-map type inspect match-all ZFW_INOUT_TCP_UDP_CLASS
 match class-map ZFW_TCP_UDP_CLASS
 match user-group INTERNAL

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_INOUT_TCP_UDP_CLASS
  inspect
 class type inspect ZFW_INOUT_ICMP_CLASS
  inspect
  police rate 16000 burst 2000
 class class-default
  drop

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ZFW_OUTIN_PASS_CLASS
  pass
 class type inspect ZFW_OUTIN_INSPECT_CLASS
  inspect
 class class-default
  drop log

parameter-map type inspect global
 log dropped-packets enable

zone security IN
zone security OUT
zone-pair security INOUT source IN destination OUT
 service-policy type inspect ZFW_INOUT_POL

int f0/0
```

```
 ip admission AUTHP
 zone-member security IN

int f0/1
 zone-member security OUT
```

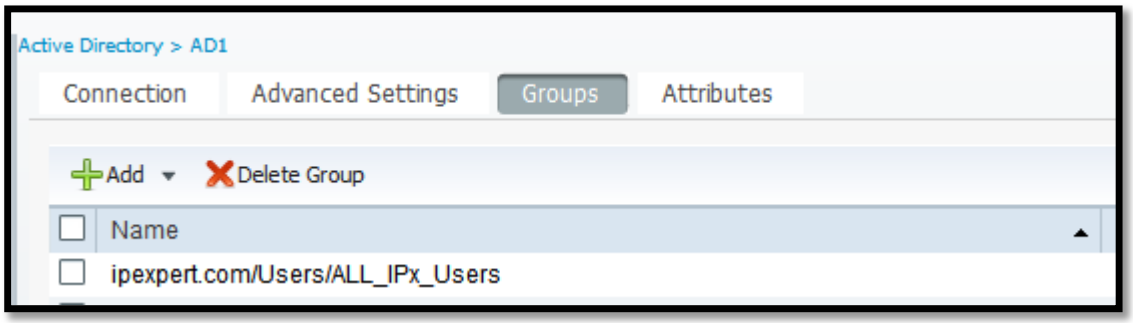
ISE

```
ip route 8.9.0.0 255.255.0.0 gateway 10.1.1.1
ntp server 10.1.1.101
ip name-server 10.1.1.101
```

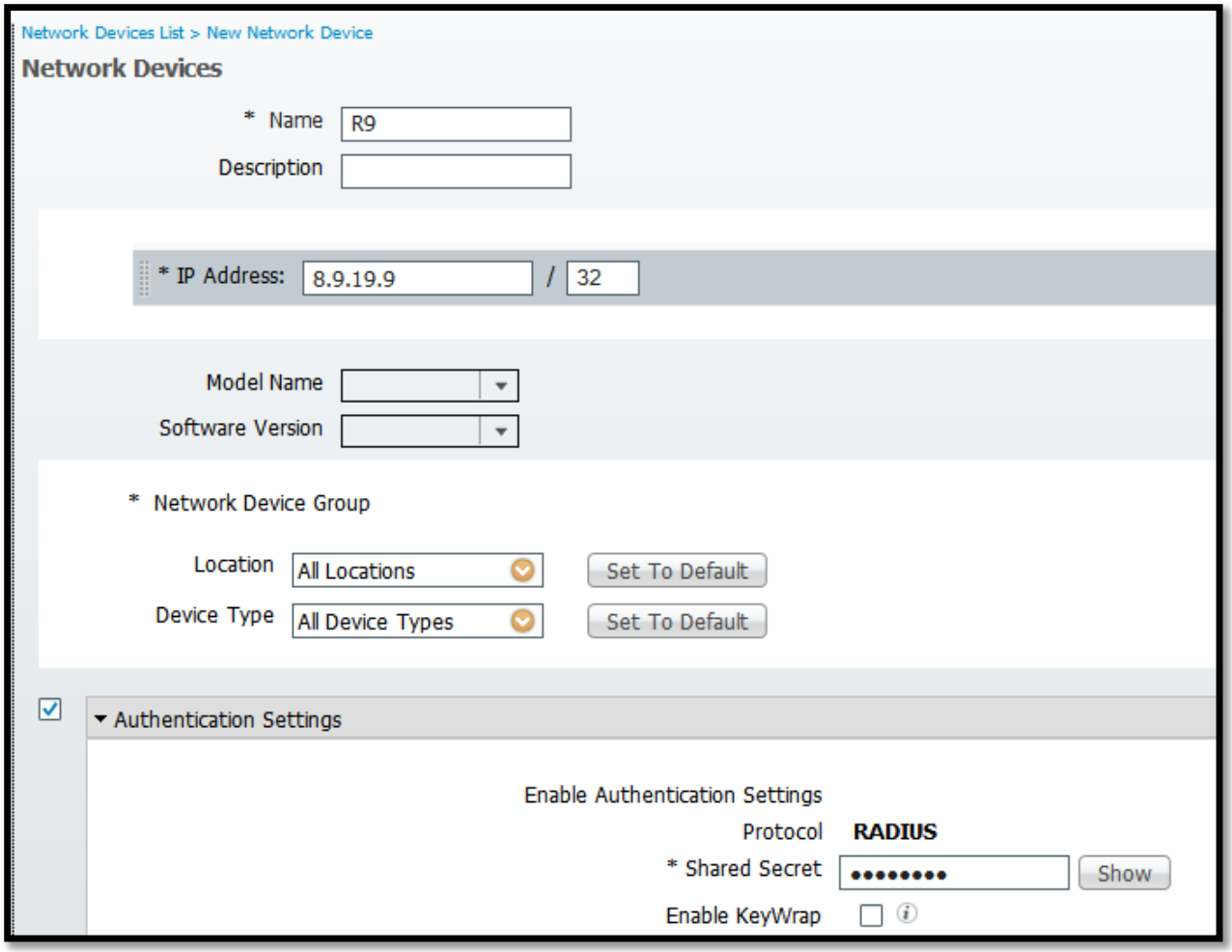
First join AD. This is what you should get after connection is established ("Connected") :



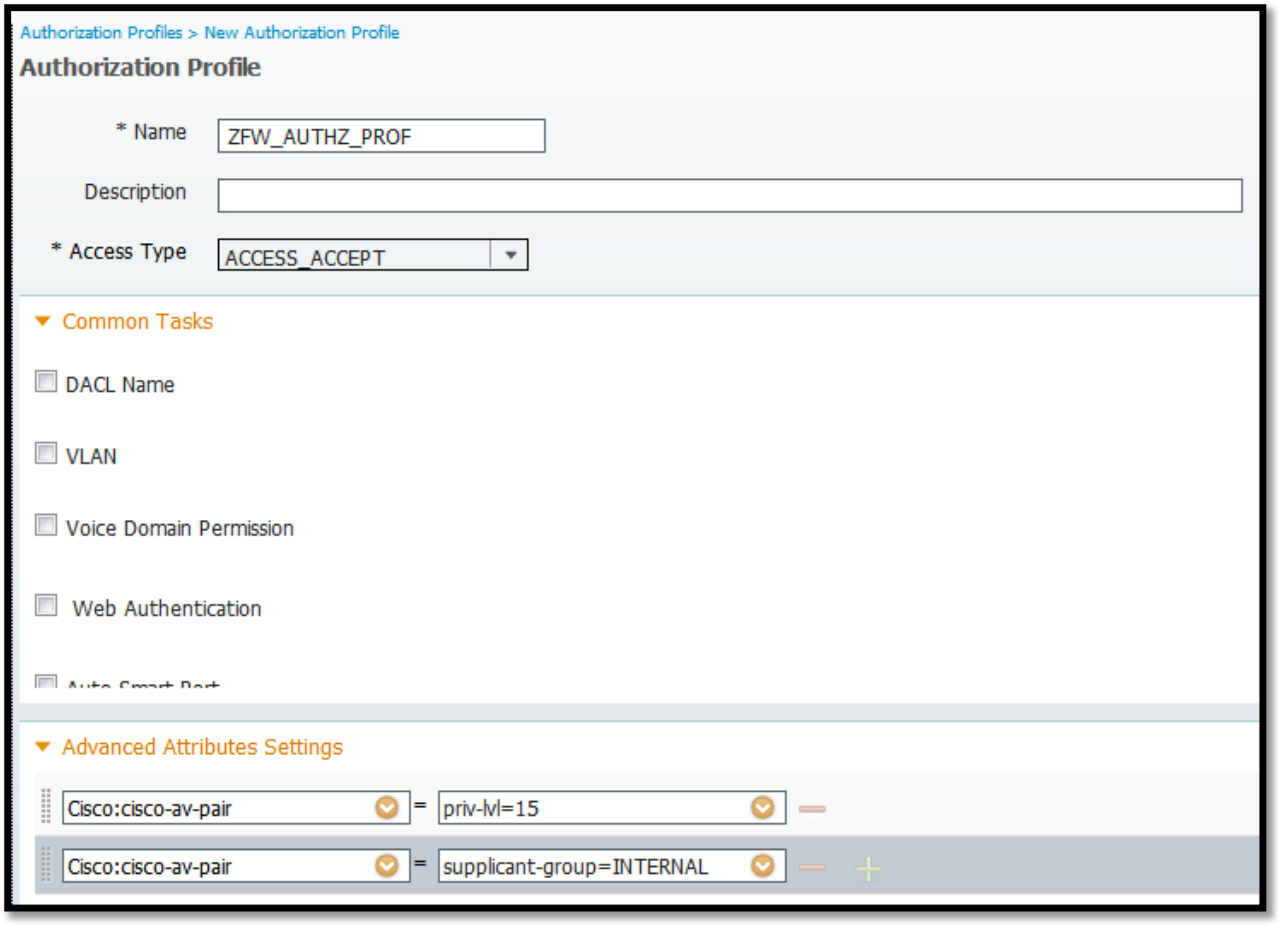
Now select an AD group we will then use in our policy. In our case all internal users are represented by "ALL_IPx_Users" :



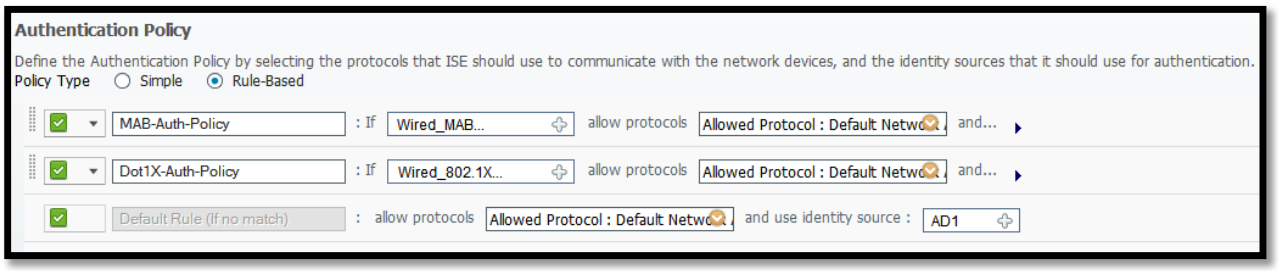
Add R9 to the Network Devices.



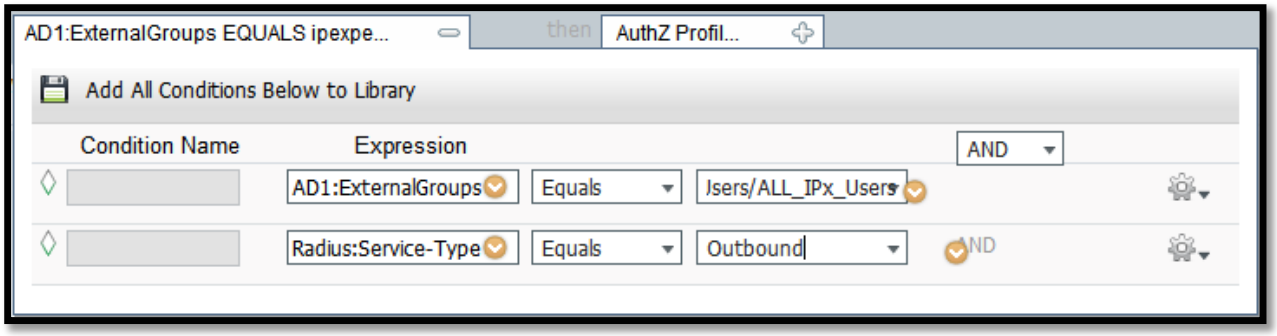
Create an Authorization Profile. Two attributes we use are “priv-lvl” and “supplicant-group” :



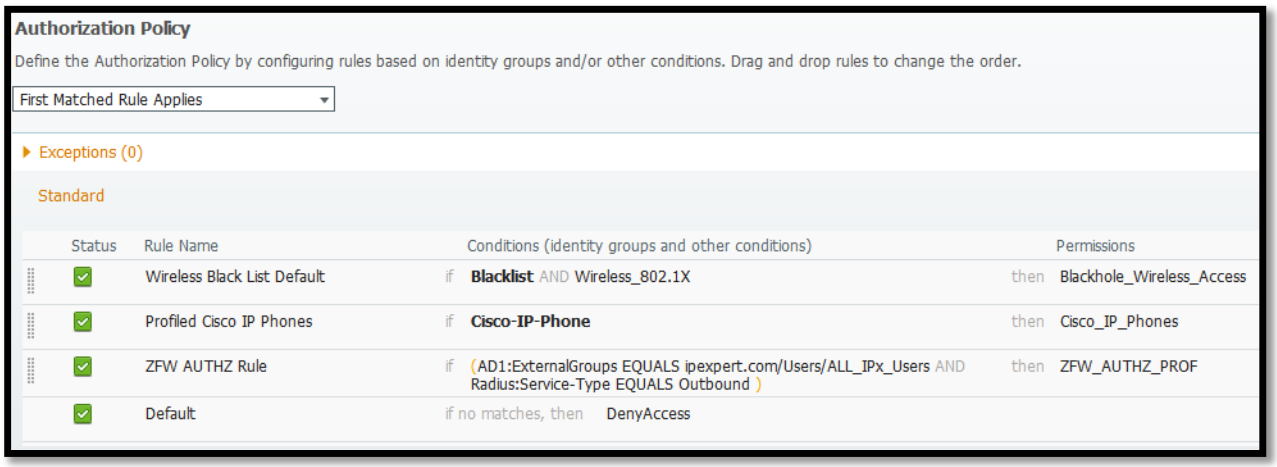
Our authentication policy is simple – we will use a default rule to say we will be authenticating using the AD :



Authorization Rule condition consists of two elements (choose “Create New Condition”) – first is to catch only the AD users, second is RADIUS Service-Type Attribute used by Authentication Proxy (Outbound) :



This is how AuthZ Policy should look like :



Whenever you start working with ISE you want to make sure it has a DNS & NTP Servers configured. Also make sure it knows how to reach NADs you will configure to talk to ISE.

The task says traffic should be allowed for authenticated users who are stored in AD. This is why we used it as our condition in the AuthZ Policy – the Default rule will catch all the rest and was configured with “Deny Access”.

In case you don’t remember attributes required to get this setup working you can always refer to the documentation. Data Plane Security Configuration Guide Library for ZFW can be used to find the Supplicant-Group (“User-based firewall support” document), whereas Authentication Proxy Guide (User Services Security Configuration Guide Library) is where it tells you about the Privilege Level.

Verification

```
R9#sh policy-firewall config
Zone: self
  Description: System defined zone

Zone: IN
  Member Interfaces:
    FastEthernet0/0

Zone: OUT
  Member Interfaces:
    FastEthernet0/1

Zone-pair              : INOUT
Source Zone            : IN
Destination Zone       : OUT
Service-policy inspect : ZFW_INOUT_POL
  Class-map : ZFW_INOUT_TCP_UDP_CLASS(match-all)
  Action : inspect

  Class-map : ZFW_INOUT_ICMP_CLASS(match-all)
  Action : inspect
  Action : Police rate 16000 burst 2000

  Class-map : class-default(match-any)
  Action : drop log

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
```

Put TEST PC to VLAN 29. Authenticate with the router (open a browser and navigate to 8.9.29.2 to trigger the credential window). Then telnet to R2, check the sessions :

```
R9#sh policy-firewall session zone-pair
 Zone-pair: INOUT
  Service-policy inspect : ZFW_INOUT_POL
    Class-map : ZFW_INOUT_TCP_UDP_CLASS(match-all)
      Established Sessions =  1
        Session 49DBF0A0 (8.9.29.200:51962)=>(8.9.19.2:23) tcp
SIS_OPEN/TCP_ESTAB
          Created 00:02:37, Last heard 00:00:37
          Bytes sent (initiator:responder) [31:23]
    Class-map : ZFW_INOUT_ICMP_CLASS(match-all)
    Class-map : class-default(match-any)

R9#sh user-group
Usergroup : INTERNAL
-------------------------------------------------------------------------
User Name       Type     Interface              Learn         Age (min)
-------------------------------------------------------------------------
8.9.29.200      IPv4     FastEthernet0/0        Dynamic         2
```

Now ping R2, send some large packets from the PC (-l *size* option) :

```
*May 20 19:31:30.091: %FW-6-DROP_PKT: Dropping icmp session 8.9.19.2:0
8.9.29.200:0 on zone-pair INOUT class ZFW_INOUT_ICMP_CLASS due to  Police
rate limiting with ip ident 0

R9#sh policy-firewall stats zone-pair INOUT

policy exists on zp INOUT
 Zone-pair: INOUT

  Service-policy inspect : ZFW_INOUT_POL

    Class-map: ZFW_INOUT_TCP_UDP_CLASS (match-all)
      Match: class-map match-any ZFW_TCP_UDP_CLASS
        Match: protocol tcp
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol udp
          0 packets, 0 bytes
          30 second rate 0 bps
      Match: user-group INTERNAL

   Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [4:69]

        Session creations since subsystem startup or last reset 4
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:02:12
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: ZFW_INOUT_ICMP_CLASS (match-all)
      Match: protocol icmp
```

```
    Match: user-group INTERNAL

  Inspect
       Packet inspection statistics [process switch:fast switch]
       icmp packets: [7:36]

       Session creations since subsystem startup or last reset 2
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [1:1:0]
       Last session created 00:01:15
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 2
       Last half-open session total 0
       TCP reassembly statistics
       received 0 packets out-of-order; dropped 0
       peak memory usage 0 KB; current usage: 0 KB
       peak queue length 0

      Police
       rate 16000 bps,2000 limit
       conformed 43 packets, 24942 bytes; actions: transmit
       exceeded 7 packets, 7414 bytes; actions: drop
       conformed 0 bps, exceed 0 bps

 Class-map: class-default (match-any)
   Match: any
   Drop
     5 packets, 400 bytes
```

3.0 Cisco IPSand Content Security (18 points)

Task 3.1: IPS Initialization (3 Points)

- Configure the IPS Sensor's Command and Control Interface through the CLI to allow

HTTPS access to the Sensor only from VLAN 100 based on the Network Diagram

- Use IP address 10.1.1.15/24 and gateway 10.1.1.1
- You would like to monitor all traffic inline between R5 and R10
- Use a single interface on IPS and configure the switches to support this deployment
- Synchronize time on the sensor with the AD Server

Detailed Solution

CAT4

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk

vlan 501
```

CAT2

```
interface FastEthernet0/10
 sw acc vlan 501
```

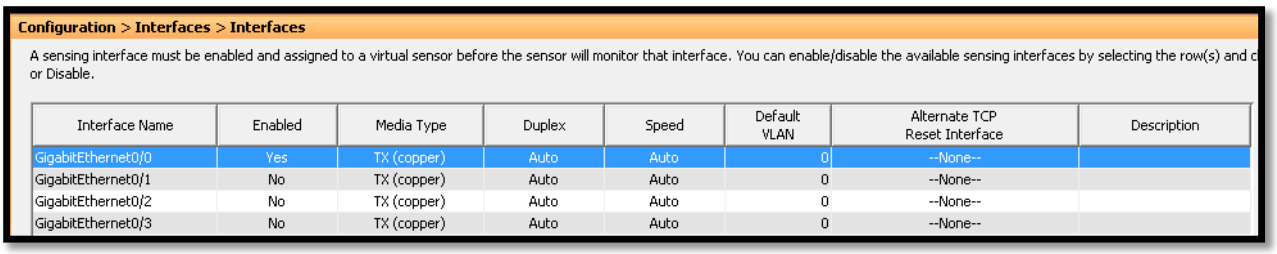
IPS

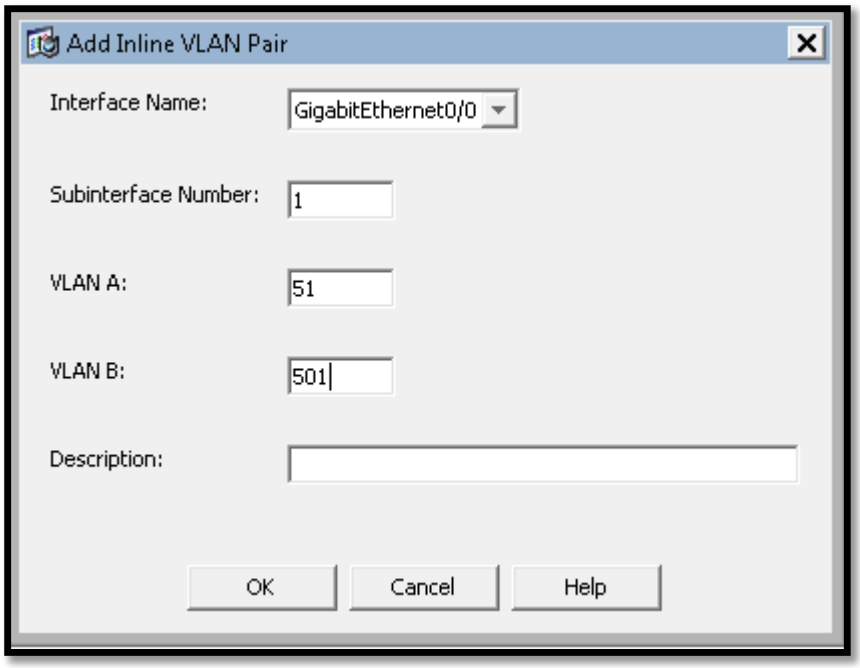
```
Enter host name[sensor]: IPS
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.1.15/24,10.1.1.1
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.1.0/24
Permit:
Use DNS server for Global Correlation?[no]:
Use HTTP proxy server for Global Correlation?[no]:
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]: 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 ---

Complete the advanced setup using CLI or IDM.
```

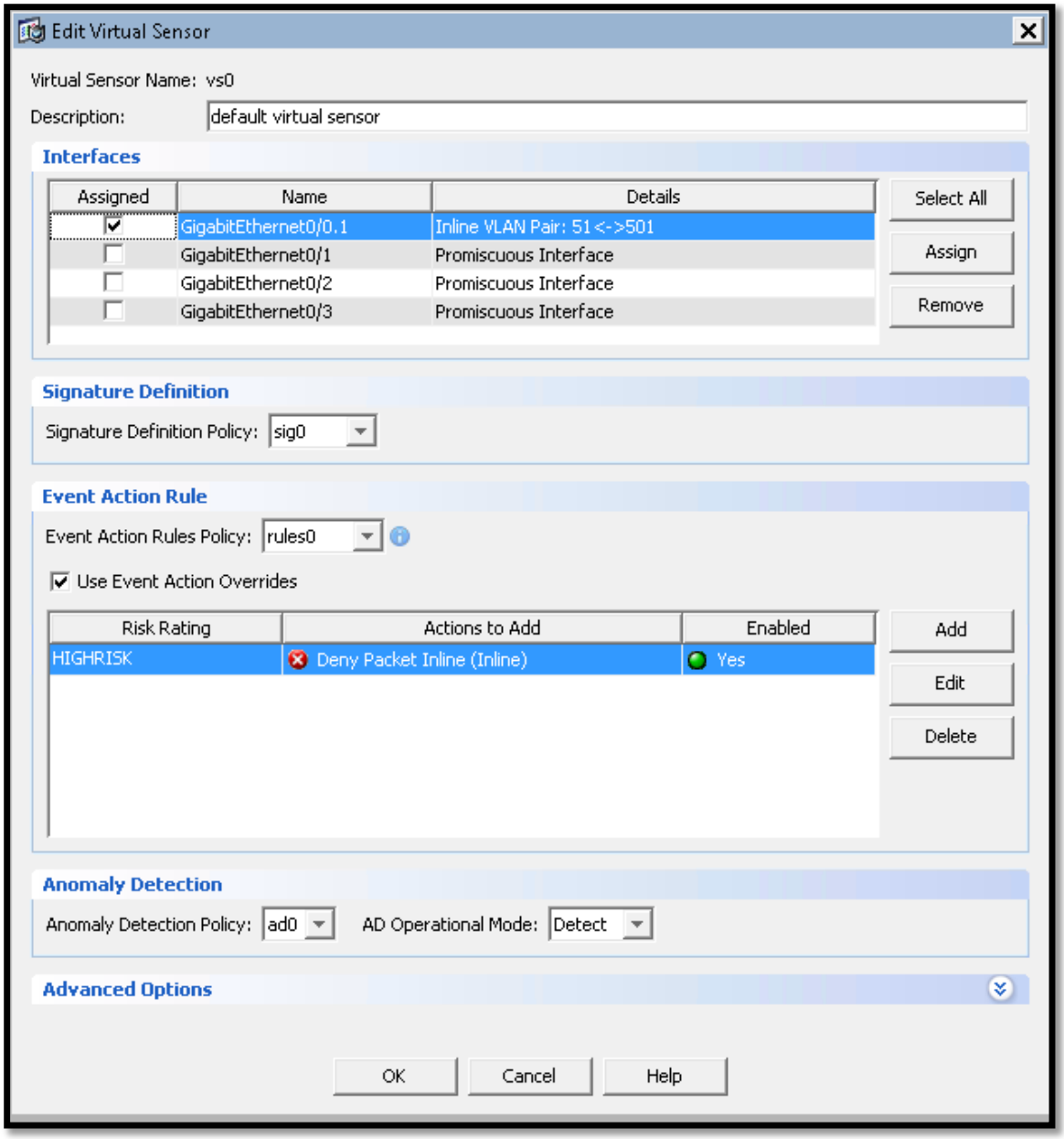
```
To use IDM,point your web browser at https://<sensor-ip-address>.
```

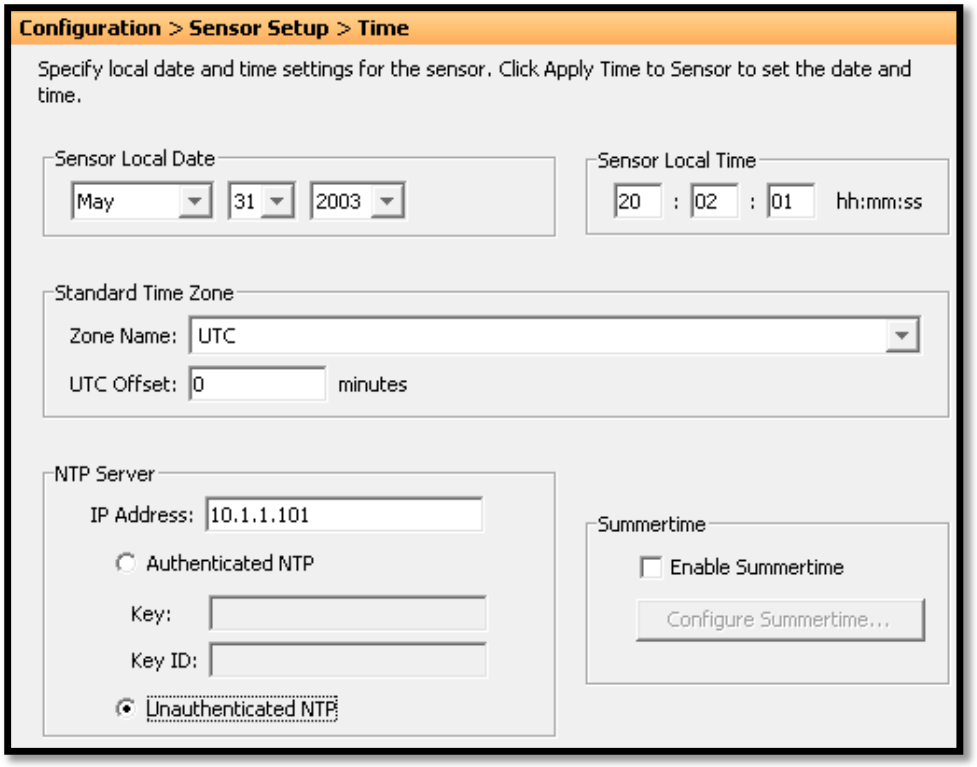
Now connect through the Test PC (10.1.1.200) and finish the remaining configuration. Bring up the port and configure VLAN Pair :



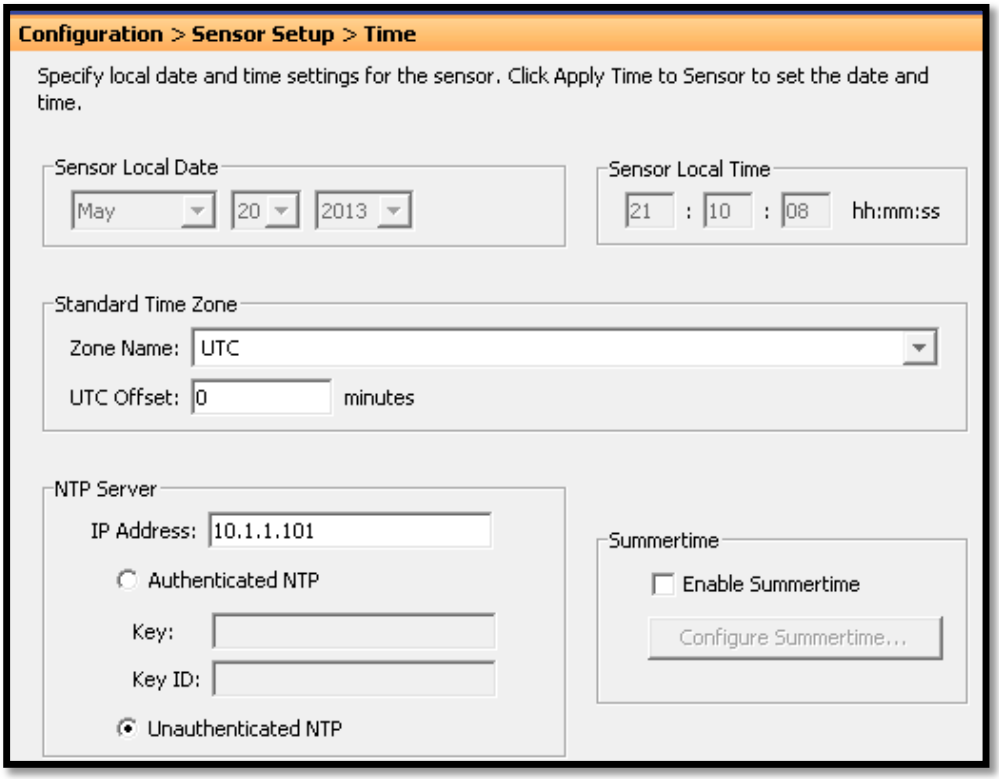


Assign the Pair to the VS. Configure NTP :





After you apply the change time gets adjusted :



For Inline VLAN Pair mode you have to split the L2 domain into two parts. Configure the switches according to the logical topology.

Watch for the syntax in “setup” command. For an ACL to be considered as finished hit “Enter” twice. For NTP and virtual sensor configuration use GUI. Enable and assign the interfaces.

Verification

Since the OSPF adjacency came up we can be now certain packets are going through the IPS :

```
sensor# sh interfaces brief
CC   Interface            Sensing State   Link   Inline Mode        Pair
Status
     GigabitEthernet0/0   Enabled         Up     Inline-vlan-pair   N/A
*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Disabled        Down   Unpaired           N/A
     GigabitEthernet0/2   Disabled        Down   Unpaired           N/A
     GigabitEthernet0/3   Disabled        Down   Unpaired           N/A

R5#
*May 20 21:06:34.977: %OSPF-5-ADJCHG: Process 1, Nbr 8.9.100.10 on
FastEthernet0/0 from LOADING to FULL, Loading Done

sensor# show clock  det

.21:10:39 UTC Mon May 20 2013
Time source is NTP
```

Task 3.2: Custom Signature (4 Points)

- Create a custom signature which allows SSH connections only if server has SSH version 2 configured
- If version 1 and 2 is allowed on the server, packet should be denied
- Configure R5 as the SSH server
- You are allowed to change the VTY configuration on R5 for this task

Detailed Solution

R5

```
ip domain-name ipexpert.com
cry key generate rsa modulus 768
username cisco pass cisco

ip ssh version 2

line vty 0 4
login local
```

IPS

Before you start your signature configuration, take a look what does the server returns when you connect. Change SSH version to 1 and telnet from R10 :

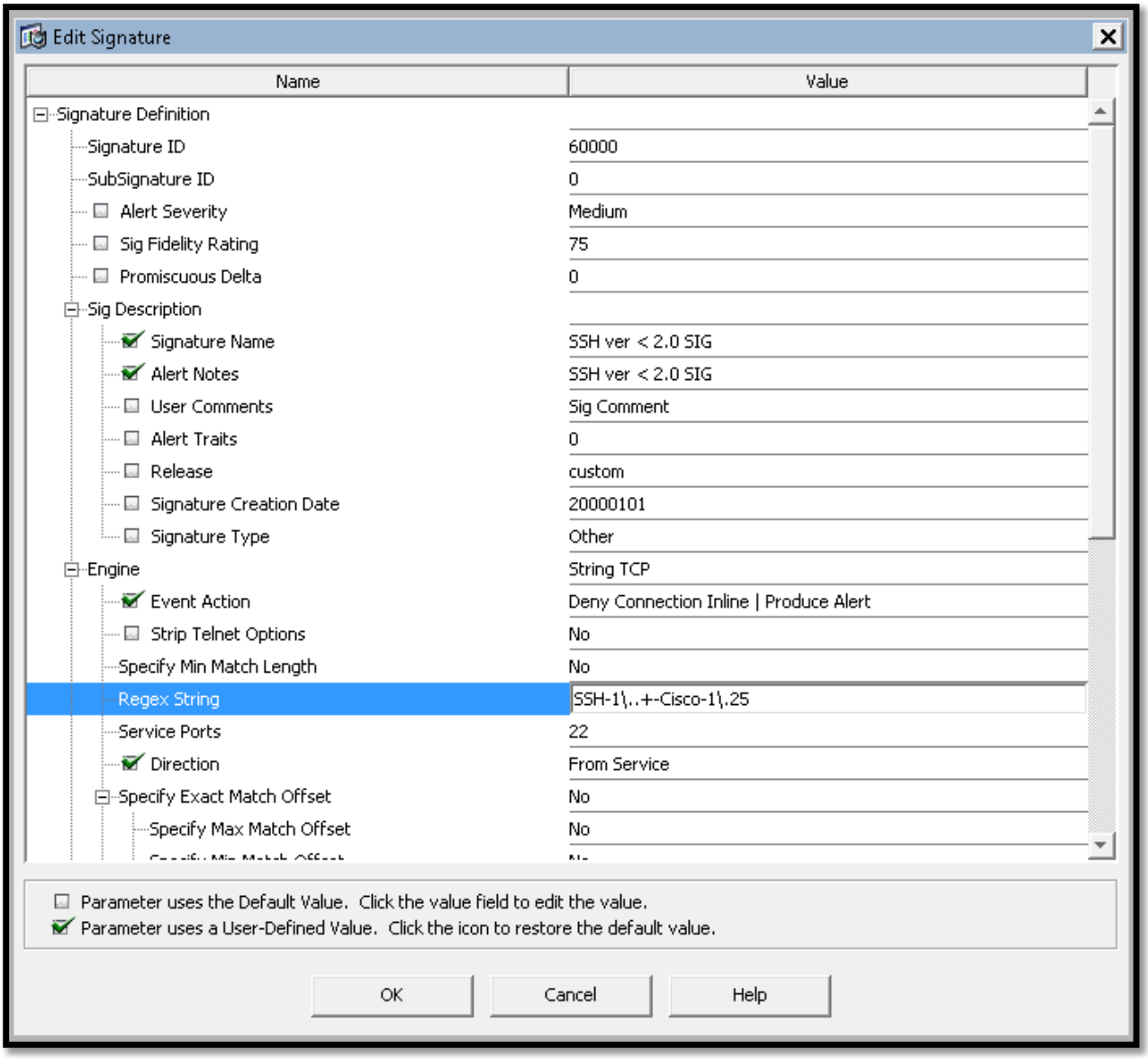
```
R10#telnet 8.9.100.5 22
Trying 8.9.100.5, 22 ... Open
SSH-1.5-Cisco-1.25

Connection to host lost.
```

Now try with version 2 :

```
R10#telnet 8.9.100.5 22
Trying 8.9.100.5, 22 ... Open
SSH-2.0-Cisco-1.25

Connection to host lost.
```

By default, both version are configured which would show SSH-1.99-Cisco-1.25. Based on this information you can now create a signature that will match something else than “SSH-2.0-Cisco-1.25”.

Add a new Signature using the plus button. Choose TCP String Engine and configure as shown below :



As mentioned in the configuration section, use telnet to find out what server returns when particular version is configured. Because this traffic is going from the server, set Direction to "From Service" in the signature. The regular expression used matches at least one digit after "SSH-1".

Verification

Change version to 1 on R5 and SSH from R10 to test :

```
IPS# show events alert
evIdsAlert: eventId=1041379286523798637 severity=medium vendor=Cisco
```

```
    originator:
      hostId: IPS
      appName: sensorApp
      appInstanceId: 413
    time: 2013/05/20 21:34:29 2013/05/20 21:34:29 UTC
    signature: description=SSH ver < 2.0 SIG id=60000 created=20000101
type=other version=custom
      subsigId: 0
      sigDetails: SSH ver < 2.0 SIG
      marsCategory: Info/Misc
    interfaceGroup: vs0
    vlan: 51
    participants:
      attacker:
        addr: locality=OUT 8.9.100.5
        port: 22
      target:
        addr: locality=OUT 8.9.51.10
        port: 14693
        os: idSource=unknown relevance=relevant type=unknown
    actions:
      deniedFlow: true
    context:
      fromAttacker:
000000  53 53 48 2D 31 2E 35 2D  43 69 73 63 6F 2D 31 2E  SSH-1.5-Cisco-1.
000010  32 35 0A                                          25.
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
66
    threatRatingValue: 31
    interface: ge0_0
    protocol: tcp
```

Change the version back to 2 and re-test :

```
R10#ssh -l cisco 8.9.100.5
Password:


R5>exi
```

Task 3.3: ASA IPS (5 Points)

- Initialize the IPS module on the ASA
- Create an additional Virtual Sensor that will be monitoring all traffic coming from VLAN7 through C2
- The C1 firewall should be inspecting packets using the default vs0 – only look at packets sourced in the DMZ
- Block all ICMP & ICMPv6 Echos traversing C2. Make sure you will see an alert in the console for every dropped packet
- ICMP Echos going through C1 should be allowed but an alert must be generated whenever 5 Echos are seen within 15 seconds
- Since the first alert was generated no more alerts should fire for the next 25 seconds for a particular Attacker/Victim address pair
- If there is more than 50 alerts generated you only want to see one alert message generated per interval no matter who the Attacker/Victim is

Detailed Solution

CAT1

```
int f0/19
 sw host
 sw acc vlan 100
```

** If there is already some configuration on the module you can first issue the “erase current-config” command and exit IPS. Then login again using “cisco”//“IPexpert123” **

ASA3/System

```
interface management0/0
 no shut

session ips console

Enter host name[sensor]: IPS
Enter IP interface[192.168.1.2/24,192.168.1.1]:
Modify current access list?[no]: yes
Current access list entries:
```

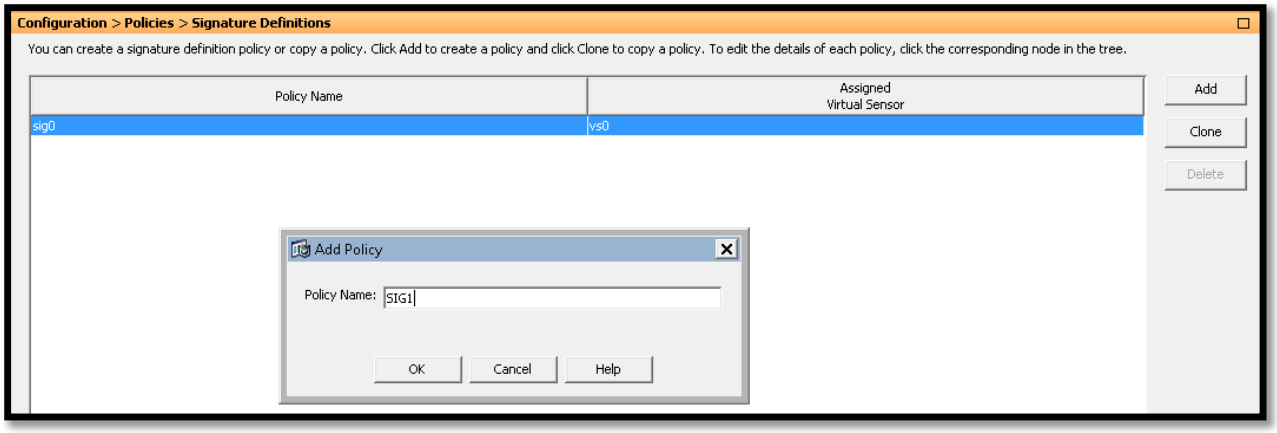
```
  No entries
Permit: 192.168.1.0/24
Permit:
Use DNS server for Global Correlation?[no]:
Use HTTP proxy server for Global Correlation?[no]:
Modify system clock settings?[no]:
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level?[off]:

The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name IPS
telnet-option disabled
access-list 192.168.1.0/24
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]: 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 ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.
```

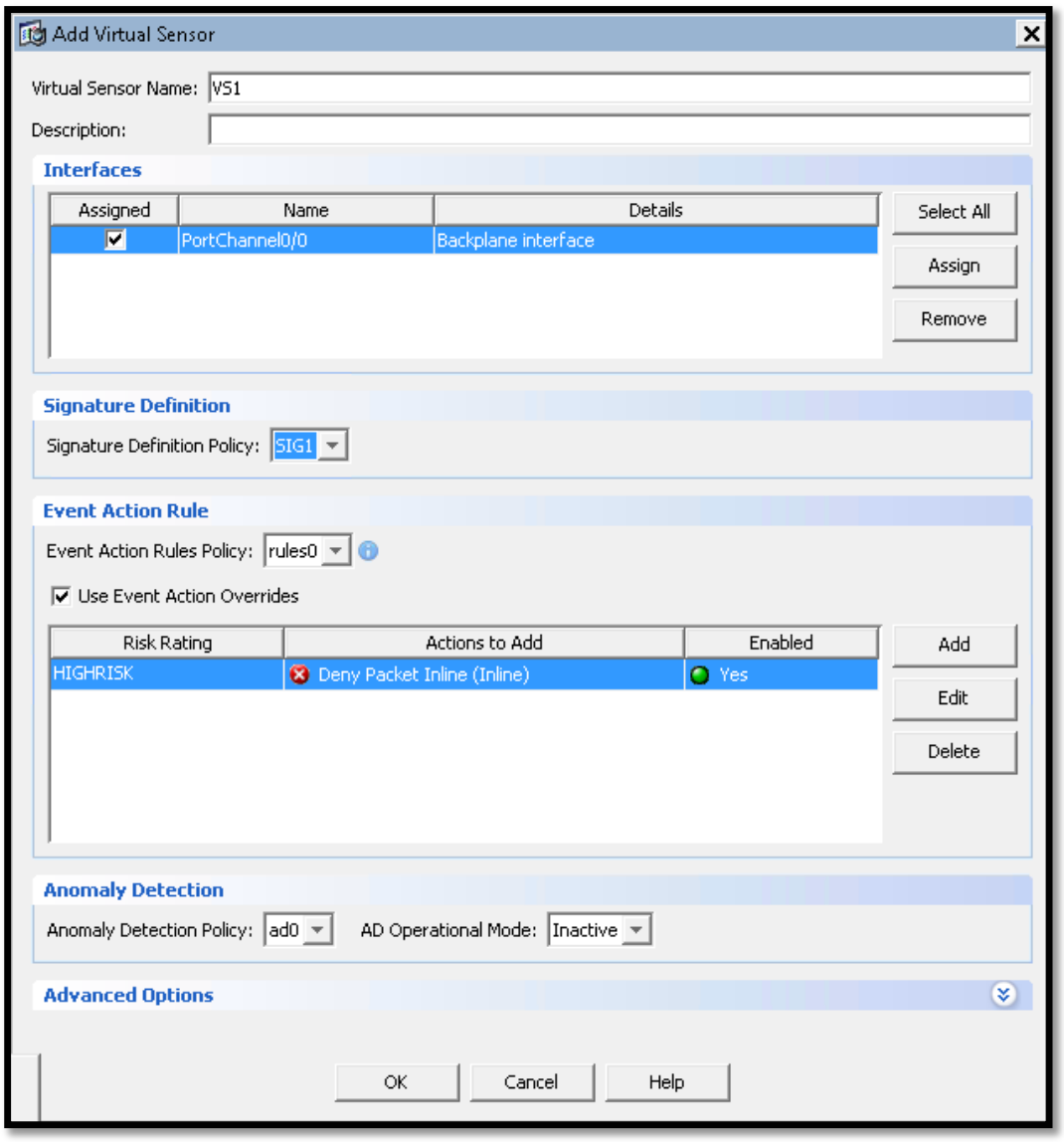
IPS/C1

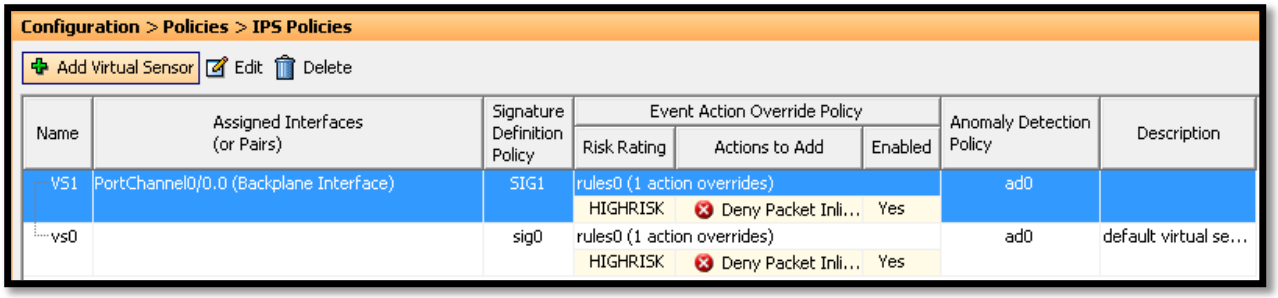
Put one of the Test PCs into VLAN 100, assign it an IP address from the 192.168.1.0/24 range (e.g. 192.168.1.200). Connect to 192.168.1.2 using HTTPs :

Create a new set of signatures :

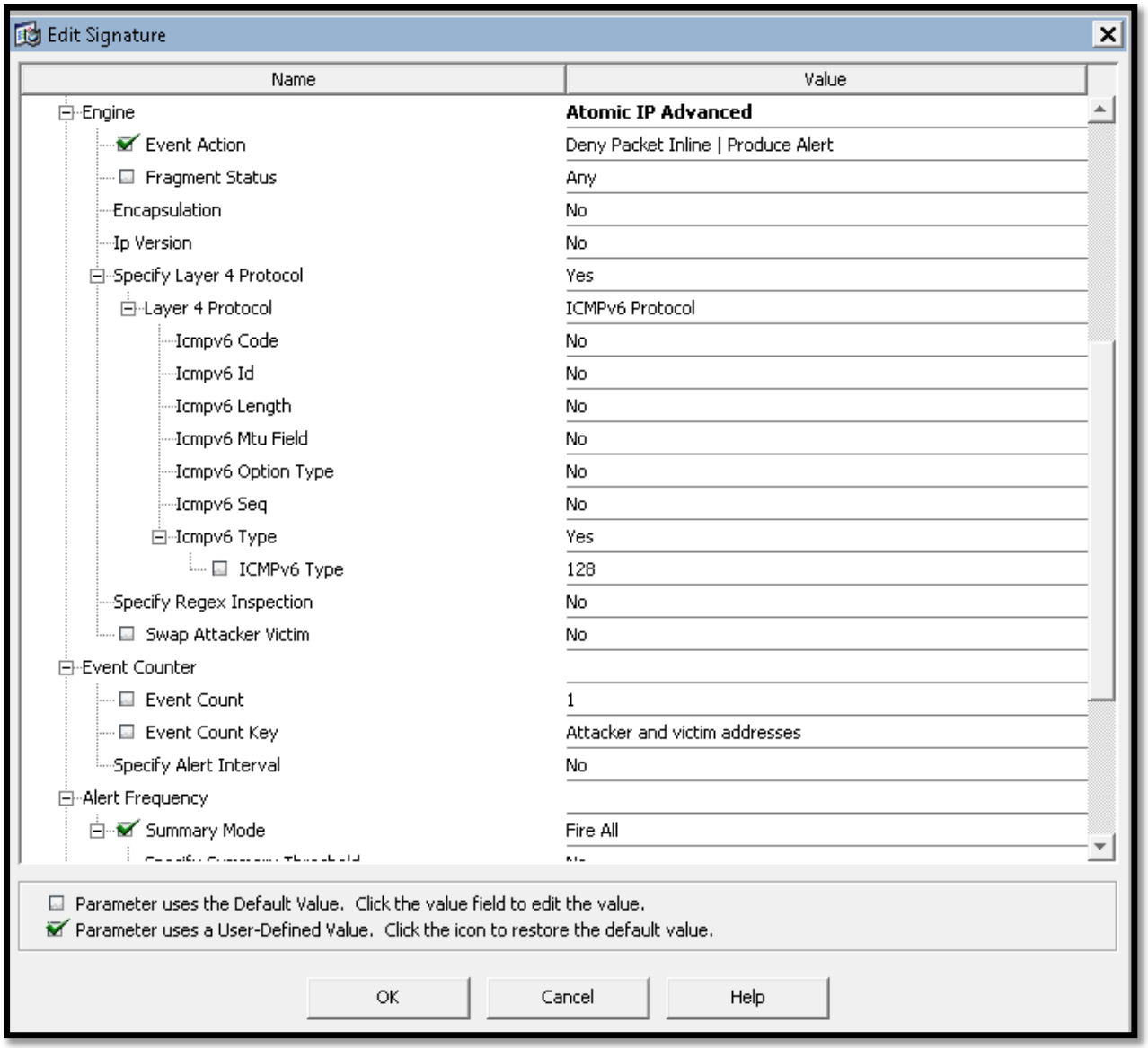


Create a new Virtual Sensor. Select the PortChannel interface and the new sig set :

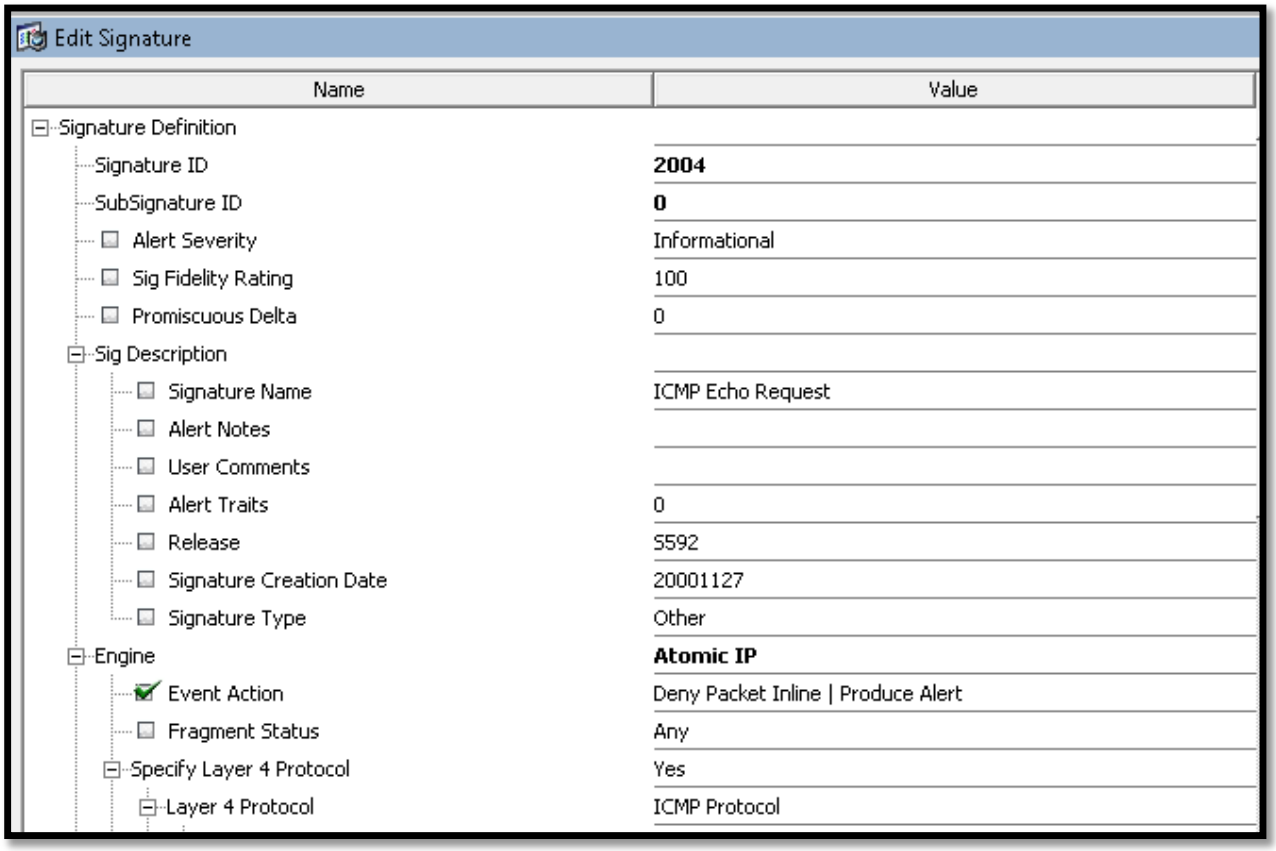


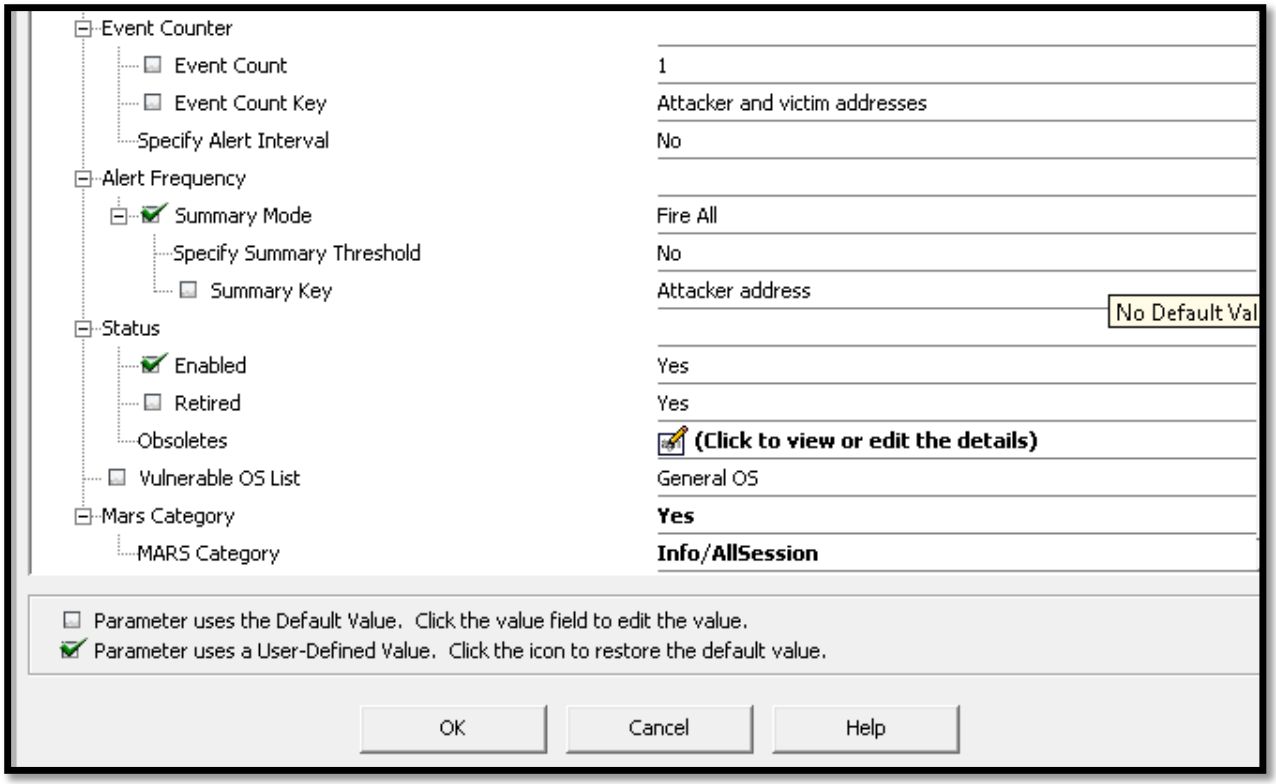


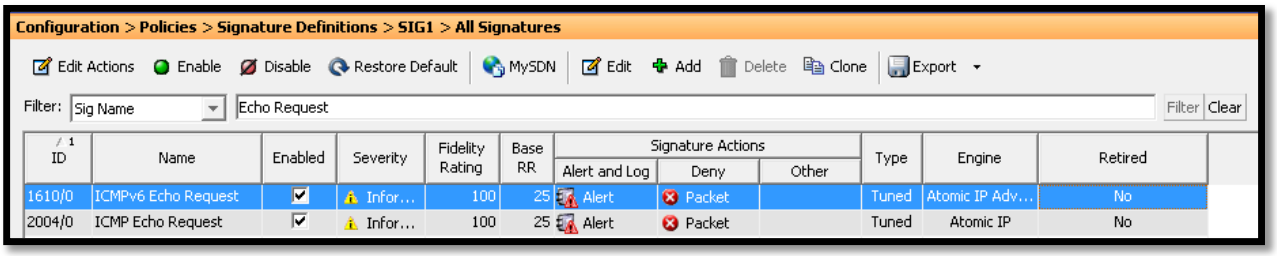
Now go ahead and edit Signature Ruleset #1. First ICMPv6 Echo – we want to enable the signature, un-retire it, add "Deny Packet Inline" action and change the Summary Mode to "Fire All" :



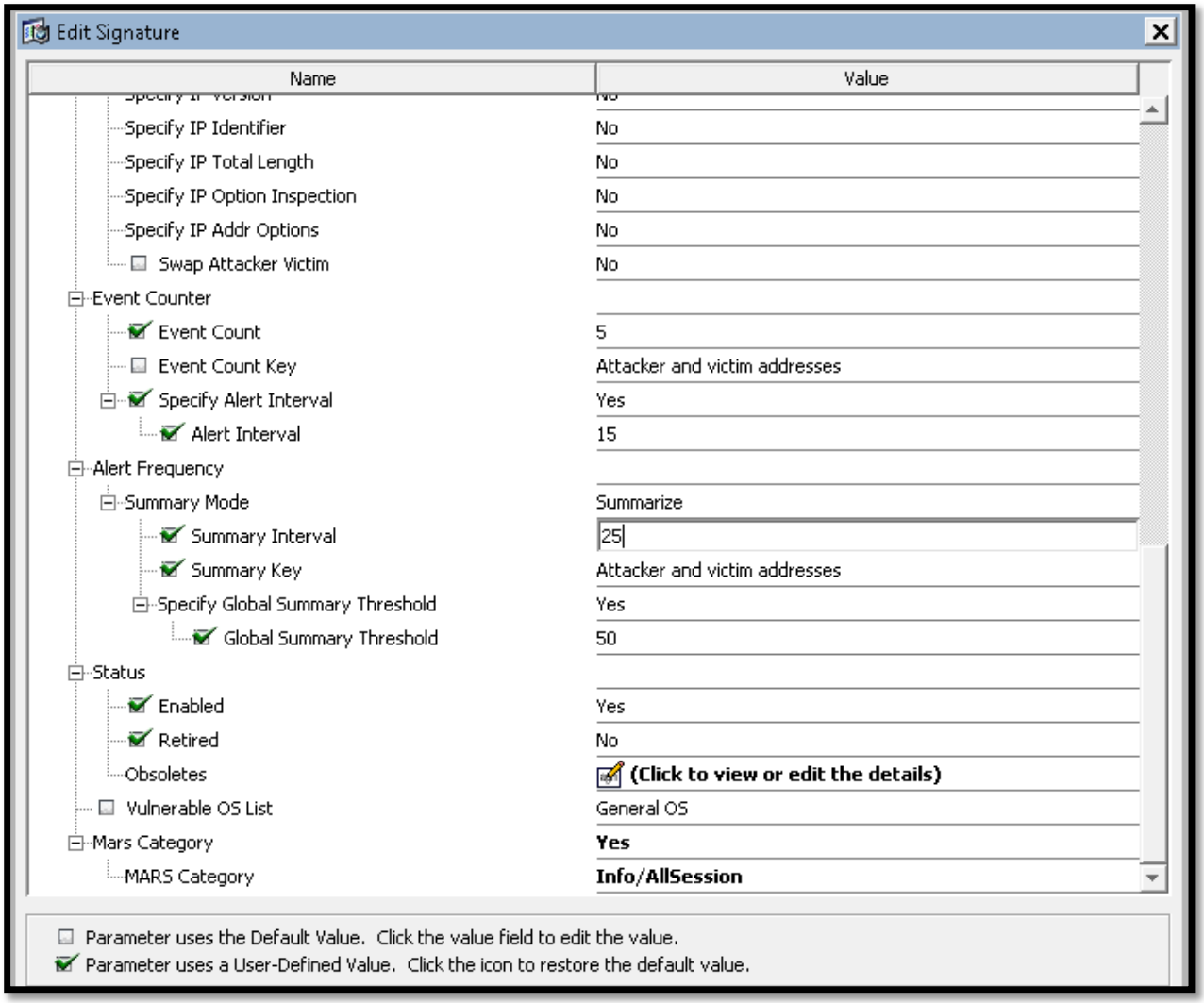
Do a similar configuration for ICMP Echo :







Now the default signature ruleset (sig0). Here we want to change ICMP Echo Alert Frequency and Summary Mode settings :



IPS/C2

** In my opinion the fastest way to configure the 2nd module is to copy the config from C1 **

```
service host
network-settings
host-name IPS
access-list 192.168.1.0/24
dns-primary-server disabled
exit
exit
yes

service signature-definition SIG1
signatures 1610 0
```

```
engine atomic-ip-advanced
event-action produce-alert|deny-packet-inline
exit
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
retired false
exit
exit
signatures 2004 0
engine atomic-ip
event-action produce-alert|deny-packet-inline
exit
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
retired false
exit
exit
exit
yes

service signature-definition sig0
signatures 2004 0
event-counter
event-count 5
specify-alert-interval yes
alert-interval 15
exit
exit
alert-frequency
summary-mode summarize
summary-interval 25
summary-key AxBx
```

```
specify-global-summary-threshold yes
global-summary-threshold 50
exit
exit
exit
status
enabled true
retired false
exit
exit
exit
yes

service analysis-engine
virtual-sensor VS1
signature-definition SIG1
physical-interface PortChannel0/0
exit
exit
yes
```

ASA3/System

```
context C1
  allocate-ips vs0

context C2
 allocate-ips VS1
```

C1

```
access-list DMZ extended permit ip 192.168.11.0 255.255.255.0 any
class-map DMZ
 match access-list DMZ

policy-map IPS
 class DMZ
  ips inline fail-open sensor vs0

service-policy IPS interface DMZ
```

C2

```
access-list VLAN7 extended permit ip 8.9.7.0 255.255.255.0 any

class-map VLAN7
 match access-list VLAN7

class-map VLAN7_6
 match any

policy-map IPS
 class VLAN7
  ips inline fail-open sensor VS1
 class VLAN7_6
  ips inline fail-open sensor VS1

service-policy IPS interface inside
```

A key thing to remember from this task is that the IPS module configuration IS NOT REPLICATED BETWEEN THE ASAs. No matter if you are running Active/Standby or Active/Active this is something you have to make sure is in sync manually or by using some sort of management application from Cisco.

In our case we have initialized the module on ASA3 only. This is to get the GUI up and working so we could configure what's needed for the task. Test PC and management 0/0 interface were put to the same VLAN (100) but we had to use a different L3 address space since 10.1.1.0/24 is used on the inside port. You could technically put them into any other existing L2 network and use the corresponding L3 addresses but it does not really matter. The point was to configure the module from the GUI, that's it.

As I mentioned in the solution probably the fastest way to configure the second module is to copy the configuration from the CLI of the already deployed box.

We did not have to worry about the ASA System space config (IPS allocation) since this stuff is automatically replicated from the unit that is active for Failover Group 1 (ASA3 here). Context configuration, however, is something we have to do on the Active device, as usually.

Verification

You can still use the IPS CLI (session from the ASA) for basic verifications. We start on ASA3 since we will be testing C1 first :

```
ASA3/act(config)# sh ips
Sensor Name      Sensor ID        Allocated To     Mapped Name
-----------      ---------        ------------     -----------
vs0              1                C1               vs0
VS1              2                C2               VS1

sensor# sh int brief
CC   Interface        Sensing State   Link   Inline Mode   Pair Status
*    Management0/0    Disabled        Up
     PortChannel0/0   Enabled         Up     Unpaired      N/A


sensor# sh events alert

R1#ping 8.9.19.2 rep 4

Type escape sequence to abort.
Sending 4, 100-byte ICMP Echos to 8.9.19.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4), round-trip min/avg/max = 1/1/4 ms
```

At this point there is no alert being generated. Ping one more time :

```
evIdsAlert: eventId=6823621015642 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1262
  time: 2013/05/21 11:24:48 2013/05/21 11:24:48 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127
type=other version=S592
    subsigId: 0
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.11.1
    target:
```

```
        addr: locality=OUT 8.9.19.2
        os: idSource=unknown relevance=relevant type=unknown
    alertDetails: InterfaceAttributes:  context="C1" physical="Unknown"
backplane="PortChannel0/0" ;
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
    threatRatingValue: 35
    interface: backplane=PortChannel0/0 context=C1 physical=Unknown
PortChannel0/0
    protocol: icmp
```

Now generate some more Echos and wait for the Summary :

```
evIdsAlert: eventId=6823621015643 severity=informational vendor=Cisco
    originator:
      hostId: IPS
      appName: sensorApp
      appInstanceId: 1262
    time: 2013/05/21 11:25:13 2013/05/21 11:25:13 UTC
    signature: description=ICMP Echo Request id=2004 created=20001127
type=other version=S592
      subsigId: 0
    interfaceGroup: vs0
    vlan: 0
    participants:
      attacker:
        addr: locality=OUT 192.168.11.1
      target:
        addr: locality=OUT 8.9.19.2
        os: idSource=unknown relevance=relevant type=unknown
    summary: final=true initialAlert=6823621015642 summaryType=Regular 25
    alertDetails: InterfaceAttributes:  context="C1" physical="Unknown"
backplane="PortChannel0/0" ; Regular Summary: 25 events this interval ;
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
    threatRatingValue: 35
    interface: backplane=PortChannel0/0 context=C1 physical=Unknown
PortChannel0/0
    protocol: icmp
```

And now 800 pings more :

```
evIdsAlert: eventId=6823621015645 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1262
  time: 2013/05/21 11:25:52 2013/05/21 11:25:52 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127
type=other version=S592
    subsigId: 0
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 0.0.0.0
    target:
      addr: locality=OUT 0.0.0.0
      os: idSource=unknown relevance=unknown type=unknown
  summary: final=true initialAlert=6823621015644 summaryType=Global 160
  alertDetails: InterfaceAttributes:  context="C1" physical="Unknown"
backplane="PortChannel0/0" ; Global Summary: 160 events this interval ;
  riskRatingValue: targetValueRating=medium 25
  threatRatingValue: 25
  interface: backplane=PortChannel0/0 context=C1 physical=Unknown
PortChannel0/0
  protocol: icmp

ASA3/C1/act(config)# sh service-pol ips

Interface DMZ:
  Service-policy: IPS
    Class-map: DMZ
      IPS: card status Up, license status Enabled, mode inline fail-open,
sensor vs0
        packet input 1930, packet output 1930, drop 0, reset-drop 0
```

If you change the source to be something else than DMZ network (e.g. Loopback0) you will obviously not see any alerts.

Let's now test another context, C2. Remember that you have to connect to the ACTIVE unit to see the IPS in action (ASA4 in our case) :

```
R11#ping 8.9.100.6 rep 2
```

```
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 8.9.100.6, timeout is 2 seconds:
..
Success rate is 0 percent (0/2)

evIdsAlert: eventId=6820428300353 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1261
  time: 2013/05/21 11:52:37 2013/05/21 11:52:37 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127
type=other version=S592
    subsigId: 0
  interfaceGroup: VSMay 21 2013 11:53:20:

  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 8.9.7.11
    target:
      addr: locality=OUT 8.9.100.6
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  alertDetails: InterfaceAttributes:  context="C2" physical="Unknown"
backplane="PortChannel0/0" ;
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
  threatRatingValue: 0
  interface: backplane=PortChannel0/0 context=C2 physical=Unknown
PortChannel0/0
  protocol: icmp


evIdsAlert: eventId=6820428300354 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1261
  time: 2013/05/21 11:52:39 2013/05/21 11:52:39 UTC
```

```
  signature: description=ICMP Echo Request id=2004 created=20001127
type=other version=S592
    subsigId: 0
  interfaceGroup: VS1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 8.9.7.11
    target:
      addr: locality=OUT 8.9.100.6
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  alertDetails: InterfaceAttributes:  context="C2" physical="Unknown"
backplane="PortChannel0/0" ;
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
  threatRatingValue: 0
  interface: backplane=PortChannel0/0 context=C2 physical=Unknown
PortChannel0/0
  protocol: icmp

%ASA-4-420002: IPS requested to drop ICMP packet from inside:8.9.7.11/2048
to outside:8.9.100.6/0
1
May 21 2013 11:53:22: %ASA-4-420002: IPS requested to drop ICMP packet
from inside:8.9.7.11/2048 to outside:8.9.100.6/0



R11#ping 2906::6 rep 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 2906::6, timeout is 2 seconds:
.
Success rate is 0 percent (0/1)

evIdsAlert: eventId=6820428300355 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1261
  time: 2013/05/21 11:55:04 2013/05/21 11:55:04 UTC
```

```
  signature: description=ICMPv6 Echo Request id=1610 created=20081031
type=other version=S567
    subsigId: 0
    sigDetails: ICMPv6 Echo Request
  interfaceGroup: VS1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 0.0.0.0
      ipv6Address: locality=OUT 2907::11
    target:
      addr: locality=OUT 0.0.0.0
      ipv6Address: locality=OUT 2906::6
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    deniedPacket: true
  alertDetails: InterfaceAttributes:  context="C2" physical="Unknown"
backplane="PortChannel0/0" ;
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
  threatRatingValue: 0
  interface: backplane=PortChannel0/0 context=C2 physical=Unknown
PortChannel0/0
  protocol: IP protocol 58

May 21 2013 11:55:46: %ASA-4-420002: IPS requested to drop IPv6-ICMP
packet from inside:2907::11/8192 to outside:2906::6/0

ASA3/C2/act(config)# sh service-policy ips

Interface inside:
  Service-policy: IPS
    Class-map: VLAN7
      IPS: card status Up, license status Enabled, mode inline fail-open,
sensor VS1
        packet input 2, packet output 2, drop 2, reset-drop 0
    Class-map: VLAN7_6
      IPS: card status Up, license status Enabled, mode inline fail-open,
sensor VS1
        packet input 1, packet output 1, drop 1, reset-drop 0
```

To make sure IPS configuration is in sync between the ASAs you could also make ASA4 active for both groups and re-test.

Task 3.4: WSA Basic Configuration (3 Points)

- Perform basic WSA Initialization. Configure addresses according to the topology
- Make sure the device is listening for incoming HTTP connections on port 8080
- Use 10.1.1.101 as the NTP and DNS server
- Password MUST BE SET TO "**ironport**"
- Set default gateway to 10.1.1.1

Detailed Solution

CAT3

```
int g1/0/3
 sw host
 sw acc vlan 100
```

WSA

A quick way to restore WSA configuration to its factory defaults is to use the "resetconfig" command (then logout for few seconds). Just in case the scripts did not clear the WSA properly.

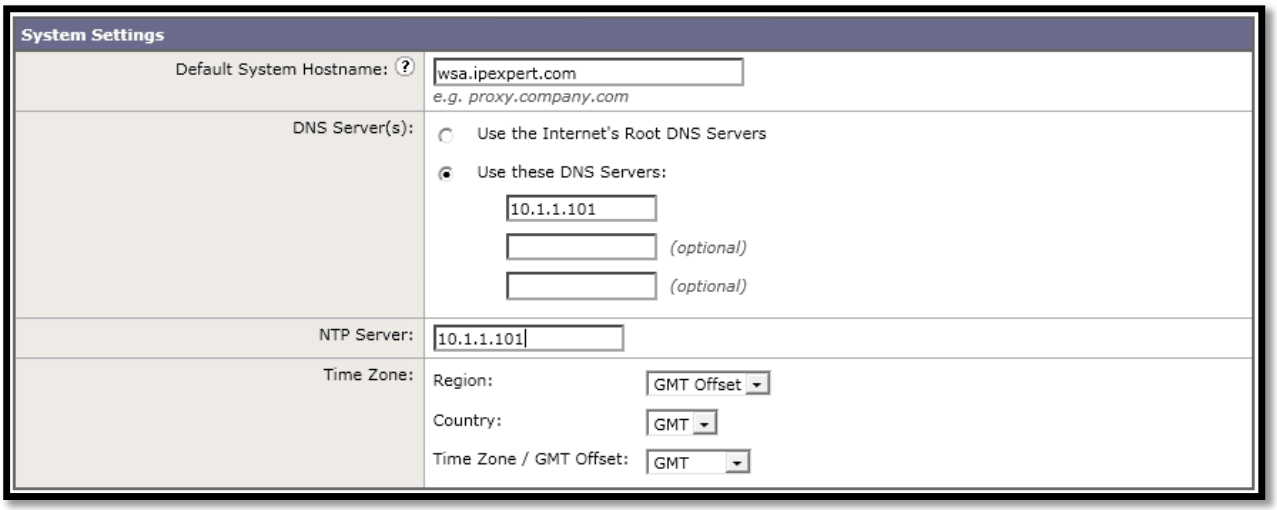
We start basic WSA config from the CLI. Just assign an IP address and enable web services :

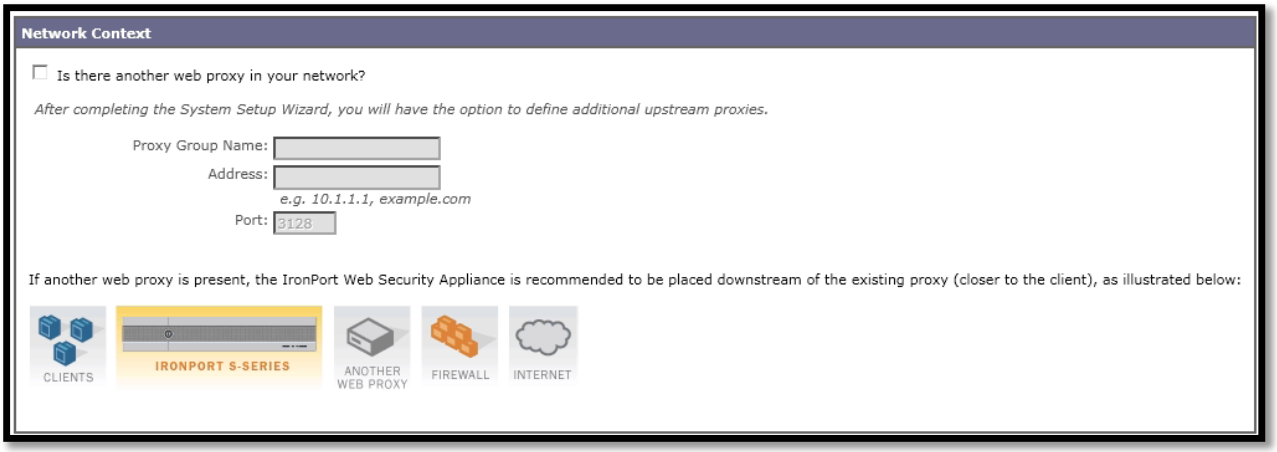
```
ironport.example.com> interfaceconfig

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
```

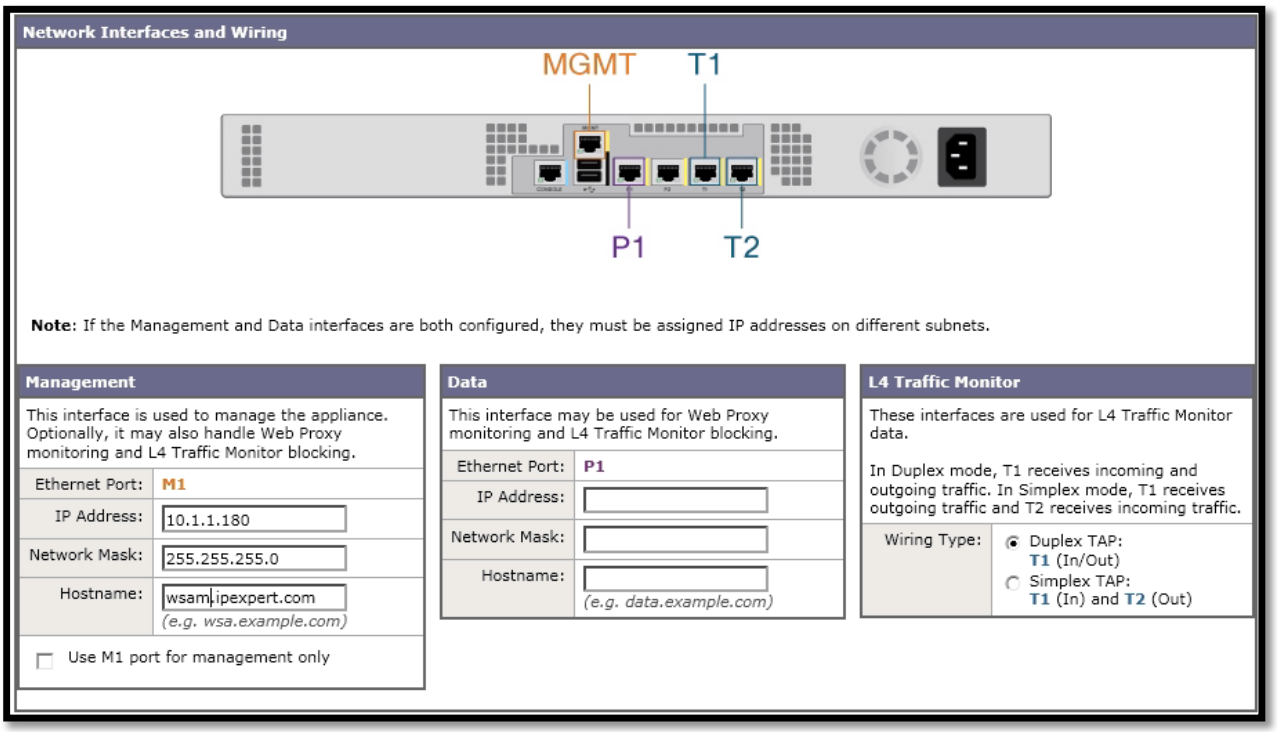
```
[]> 1

IP Address (Ex: 192.168.1.2):
[192.168.42.42]> 10.1.1.180
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>

Hostname:
[ironport.example.com]> wsam.ipexpert.com

Do you want to enable FTP on this interface? [Y]>

Which port do you want to use for FTP?
[21]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?
[22]>

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?
[8080]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?
[8443]>

You have not entered an HTTPS certificate.  To assure privacy, run
"certconfig" first.  You may use the demo, but this will not be secure.
Do you really wish to use a demo certificate? [Y]>

Both HTTP and HTTPS are enabled for this interface, should HTTP requests
redirect to the secure service? [Y]>

The interface you edited might be the one you are currently logged into.
Are
you sure you want to change it? [Y]>
```

```
Currently configured interfaces:
1. Management (10.1.1.180/24 on Management: wsa.ipexpert.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>

Please run System Setup Wizard at http://192.168.42.42:8080

ironport.example.com> commit

Please enter some comments describing your changes:
[]>

Changes committed: Tue May 21 14:33:31 2013 GMT
Please run System Setup Wizard at http://192.168.42.42:8080
ironport.example.com>
```

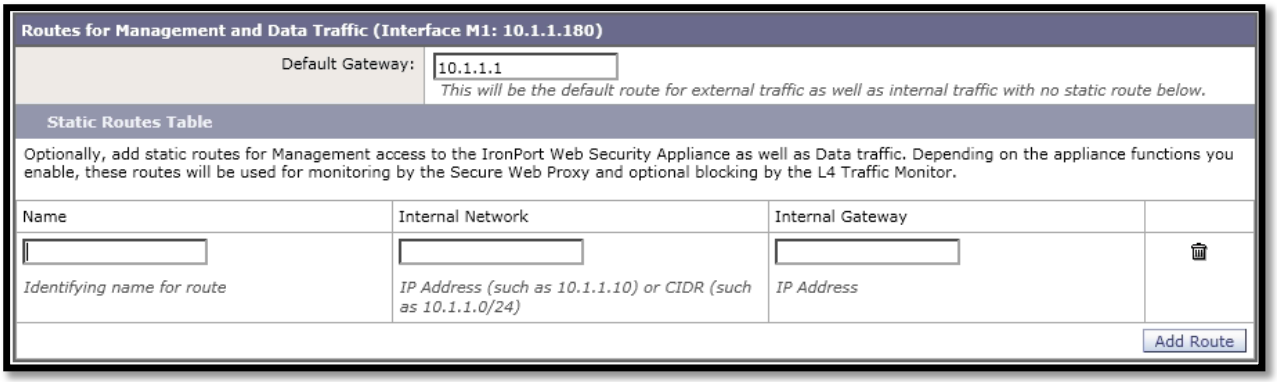
Now connect to 10.1.1.180 using port 8080 (HTTP) or 8443 (HTTPs) and run the System Setup Wizard (under "System Administration"). Configure hostname, DNS & NTP Servers and basic interface settings :

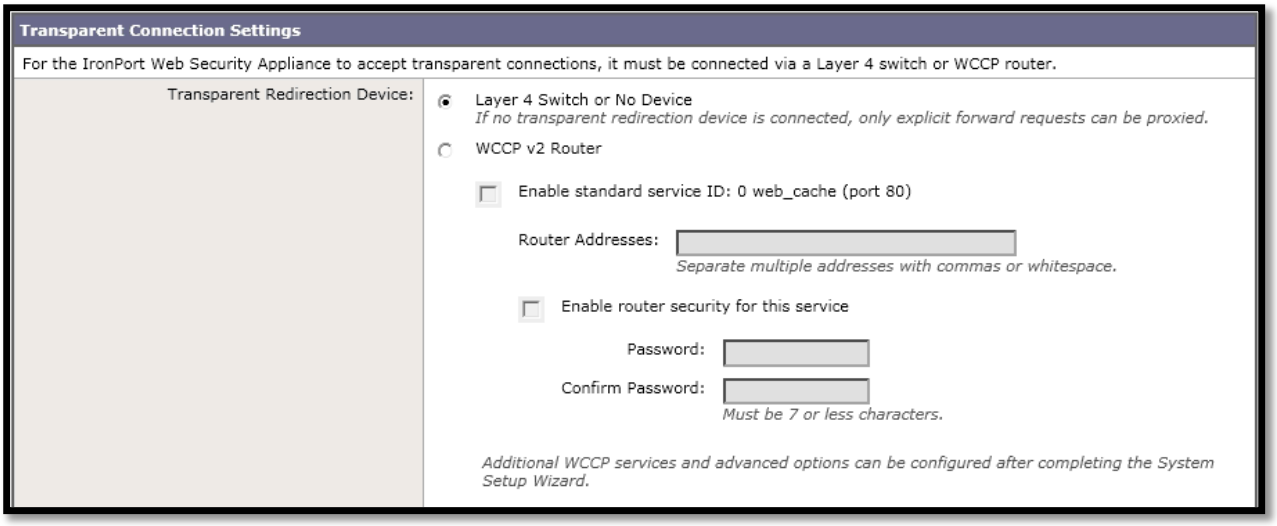




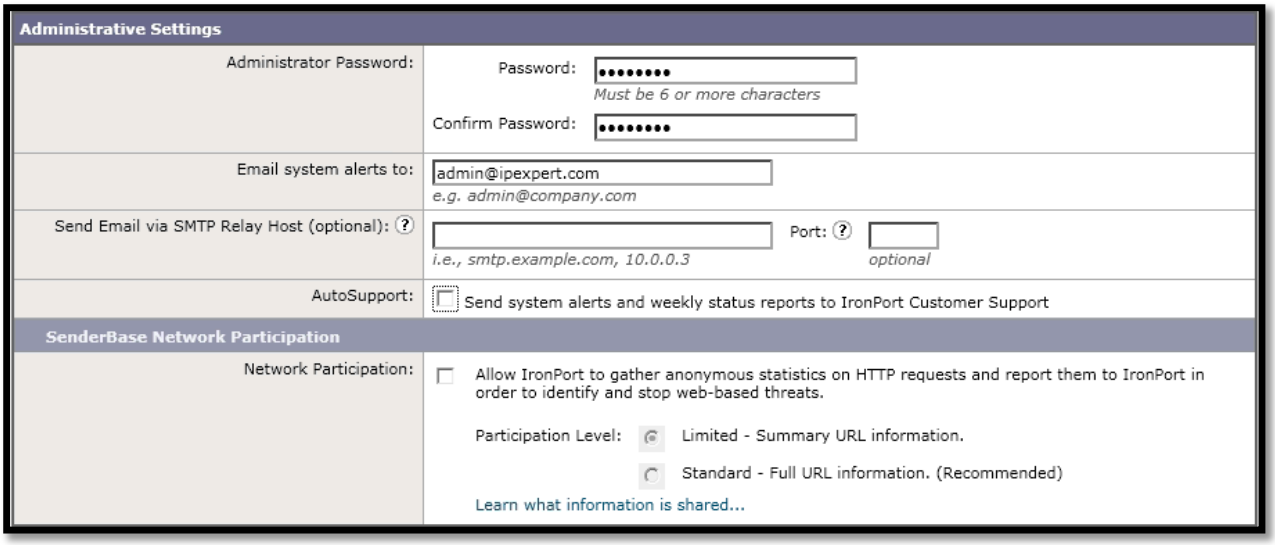


A single default route will do the job in our topology :

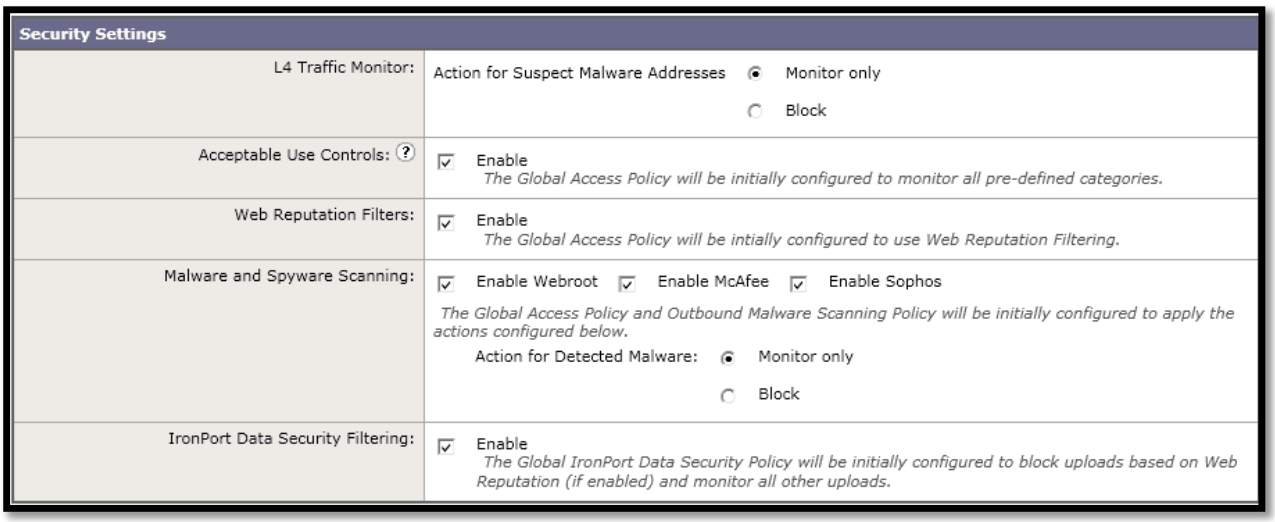




Password MUST be configured to “ironport” (if you are using ProctorLabs). I also turned off Network Participation and AutoSupport reports (in the lab you may ask the Proctor) :



You can leave the Security Features on :



This is what we end up with :

Network Settings	Edit
Default System Hostname:	wsa.ipexpert.com
DNS Servers:	10.1.1.101
Network Time Protocol (NTP):	10.1.1.101
Time Zone:	Etc/GMT
Network Context	
Upstream proxy:	No upstream proxy
Interfaces	Edit
Management (M1)	
IP Address:	10.1.1.180
Network Mask:	255.255.255.0
Hostname:	wsam.ipexpert.com
Use M1 port for management only:	No
L4 Traffic Monitor:	
Wiring Type:	Duplex TAP: T1 (In/Out)
Routes	Edit
Default Gateway:	10.1.1.1
Static Routes:	No static routes have been defined.
Transparent Connection Settings	Edit
Transparent Redirection Device Type:	Layer 4 Switch or No Device
Administrative Settings	Edit
Administrator Password:	*(hidden)*
Email System Alerts To:	admin@ipexpert.com
Internal SMTP Relay Hosts:	No internal relay host is defined
AutoSupport:	No
SenderBase Network Participation:	No

Security Settings	Edit
L4 Traffic Monitor:	Monitoring
Acceptable Use Controls:	Enabled
Web Reputation Filters:	Enabled
IronPort DVS™ Engine:	Webroot: Enabled McAfee: Enabled Sophos: Enabled
IronPort Data Security Filtering:	Enabled

Verification

```
ironport.example.com> ping 8.9.19.2

Press Ctrl-C to stop.
PING 8.9.19.2 (8.9.19.2): 56 data bytes
64 bytes from 8.9.19.2: icmp_seq=0 ttl=255 time=1.146 ms
64 bytes from 8.9.19.2: icmp_seq=1 ttl=255 time=0.681 ms
64 bytes from 8.9.19.2: icmp_seq=2 ttl=255 time=0.803 ms
```

```
^C
--- 8.9.19.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.681/0.877/1.146/0.197 ms
```

This is something you might have not known how to test – facebook.com is one of the websites defined on the AD Server. There is also a DNS entry for it and we see resolution is OK. In the lab they should give you that kind of information; worst case if you can access the AD server you may want to look at the "Administrative Tools" -> IIS or DNS.

```
ironport.example.com> nslookup

Please enter the host or IP address to resolve.
[]> facebook.com

Choose the query type:
1. A       the host's Internet address
2. CNAME   the canonical name for an alias
3. MX      the mail exchanger
4. NS      the name server for the named zone
5. PTR     the hostname if the query is an Internet address,

 otherwise the pointer to other information
6. SOA     the domain's "start-of-authority" information
7. TXT     the text information
[1]> 1

A=10.1.1.101 TTL=1h
Please run System Setup Wizard at http://192.168.42.42:8080
```

Task 3.5: WCCP (3 Points)

- WSA should act as a proxy to HTTP (port 80 & 8081) and HTTPs (port 443) connections
- Clients will reside in VLAN 100 and ASA C1 should be configured to redirect the traffic coming from the 10.1.1.192/26 subnet
- Make sure the ASA only accepts packets from the WSA and not any other Content Engine
- Protect the WCCP communication with a password "ipx123"

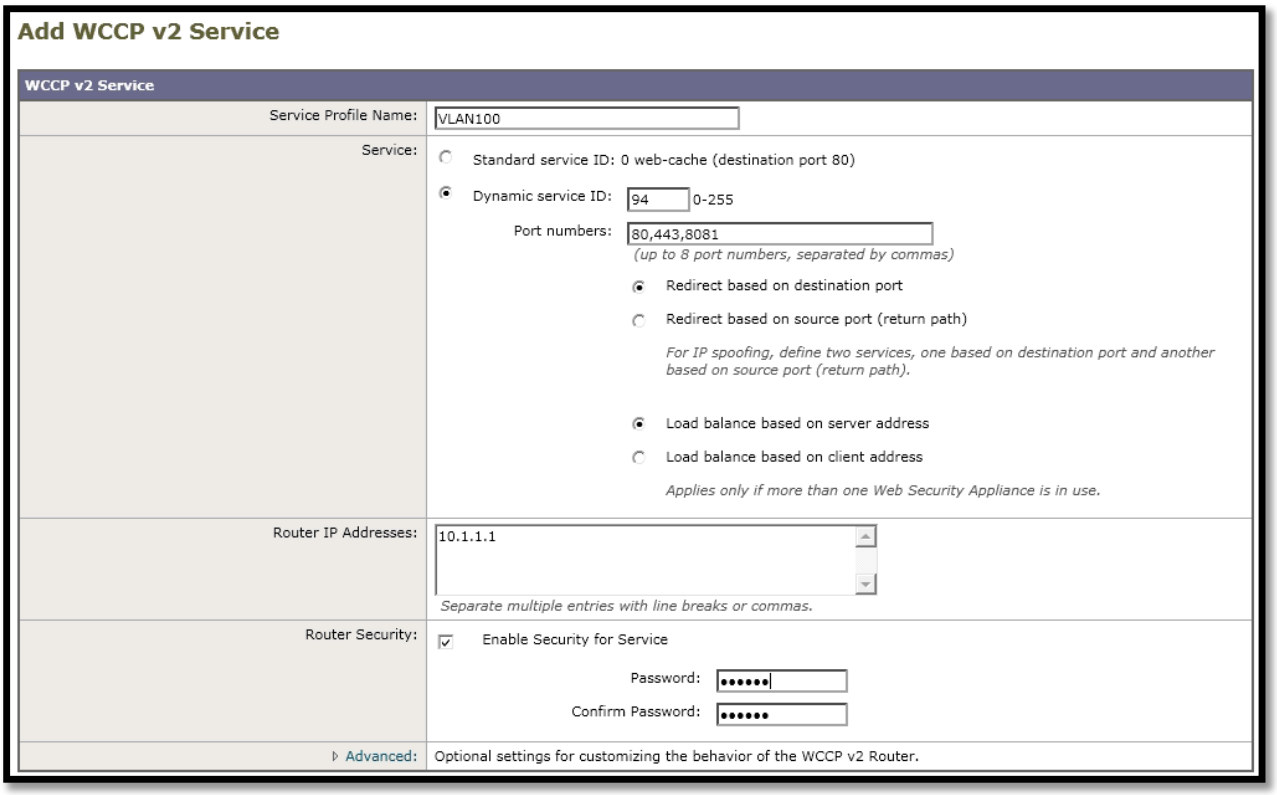
Detailed Solution

C1

```
access-list WSA extended permit ip host 10.1.1.180 any
access-list VLAN100_64 extended permit ip 10.1.1.192 255.255.255.192 any

wccp 94 redirect-list VLAN100_64 group-list WSA password ipx123
wccp interface inside 94 redirect in
```

WSA

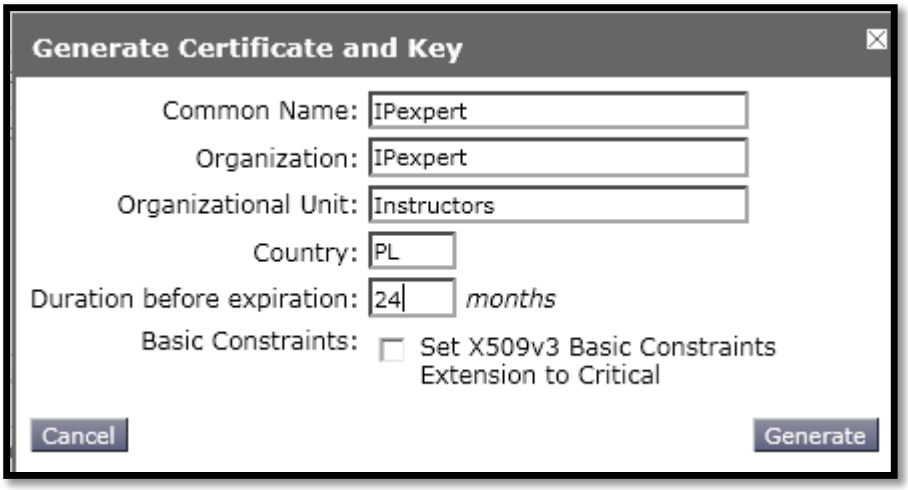
Go under “Network -> Transparent Redirection” and configure a dynamic service group :



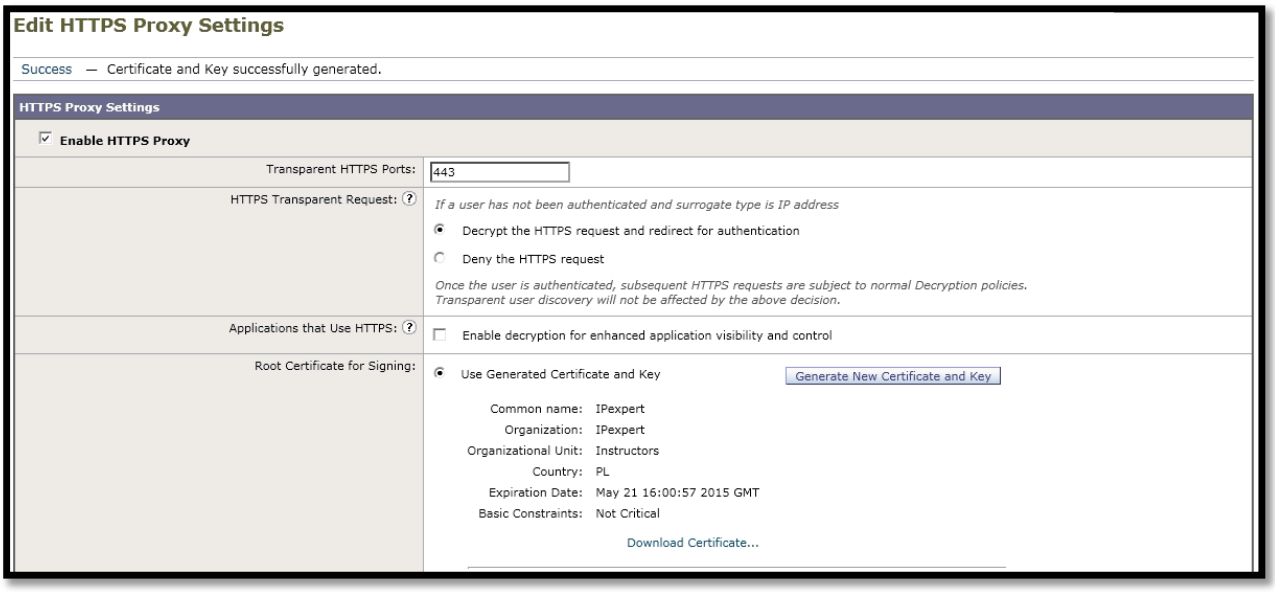
Now we want to make sure WSA is listening on ports 80 and 8081 for HTTP and that HTTPs proxy is enabled for 443. Go under "Security Services -> Web Proxy" and then under the same tab to "HTTPs Proxy" :

Enable and edit :

First generate a self-signed certificate :



And then enable the feature :



So the WSA can forward requests over certain ports you must ensure the port is enabled for the service. For HTTPs, the proxy feature is disabled by default so this is another thing to remember about.

When you finish configuring WSA never forget to commit the changes you've made.

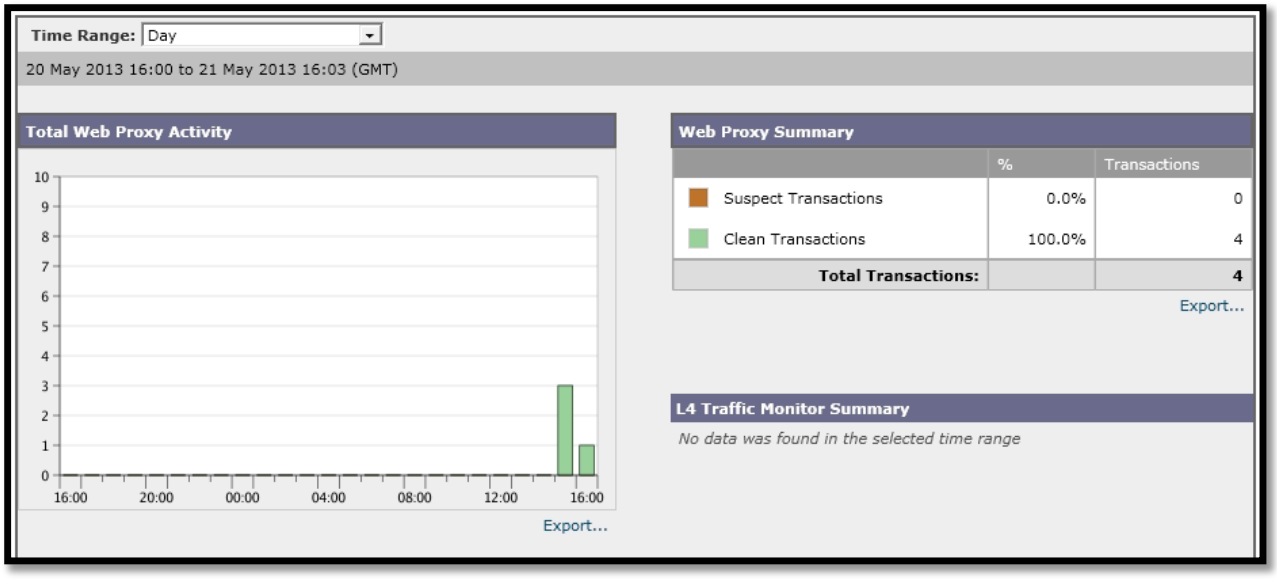
Verification

```
ASA3/C1/act(config)# sh wccp
```

```
Global WCCP information:
    Router information:
        Router Identifier:                  192.168.11.30
        Protocol Version:                   2.0

    Service Identifier: 94
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           0
        Redirect access-list:               VLAN100_64
        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

ASA3/C1/act(config)# sh wccp 94 view

    WCCP Routers Informed of:
        192.168.11.30

    WCCP Cache Engines Visible:
        10.1.1.180

    WCCP Cache Engines NOT Visible:
        -none-

ASA3/C1/act(config)# sh wccp 94 service

WCCP service information definition:
        Type:          Dynamic
        Id:            94
        Priority:      240
        Protocol:      6
        Options:       0x00000012
        --------
            Hash:      DstIP
            Alt Hash:  -none-
            Ports:     Destination:: 80 443 8081 0 0 0 0 0
```

Temporarily enable HTTP server on R9 (I used port 8081). Try to connect from VLAN 100 – just make sure TEST PC's IP address belongs to 10.1.1.192/26 subnet. Also don't forget to test HTTPs.

```
ASA3/C1/act(config)# sh wccp 94 det

WCCP Cache-Engine information:
        Web Cache ID:          10.1.1.180
        Protocol Version:      2.0
        State:                 Usable
        Initial Hash Info:     00000000000000000000000000000000
                               00000000000000000000000000000000
        Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                               FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:        256 (100.00%)
        Packets Redirected:    107
        Connect Time:          00:08:53
```



Remember to remove any changes done to R9 to test this or otherwise you will break User-Based firewall task.

4.0 Cisco VPN Solutions (14 points)

Task 4.1: DMVPN Troubleshooting (4 Points)

- There is a broken DMVPN between R2, R5 and R6
- You are supposed to fix the configuration so DMVPN verification gives outputs similar to those below (packet counters, timers etc. don't have to match) :

```
R2#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 172.16.100.2, VRF ""
   Tunnel Src./Dest. addr: 8.9.100.2/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "IPSEC_PROF41"
   Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target
Network
----- --------------- --------------- ----- -------- ----- ---------------
--
    1      8.9.100.5    172.16.100.5    UP 00:22:30    D
172.16.100.5/32

    1      8.9.100.6    172.16.100.6    UP 00:14:22    D
172.16.100.6/32



Crypto Session Details:
----------------------------------------------------------------------------
------
```

```
Interface: Tunnel100
Session: [0x712CF3E0]
  IKEv1 SA: local 8.9.100.2/500 remote 8.9.100.5/500 Active
          Capabilities:(none) connid:1004 lifetime:23:37:29
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.5
  IPSEC FLOW: permit 47 host 8.9.100.2 host 8.9.100.5
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 309 drop 0 life (KB/Sec) 4416442/2249
        Outbound: #pkts enc'ed 317 drop 0 life (KB/Sec) 4416441/2249
   Outbound SPI : 0x1D1E11A1, transform : esp-3des esp-md5-hmac
    Socket State: Open

Interface: Tunnel100
Session: [0x712CF2F0]
  IKEv1 SA: local 8.9.100.2/500 remote 8.9.100.6/500 Active
          Capabilities:(none) connid:1006 lifetime:23:45:36
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.6
  IPSEC FLOW: permit 47 host 8.9.100.2 host 8.9.100.6
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 180 drop 0 life (KB/Sec) 4594523/2737
        Outbound: #pkts enc'ed 208 drop 0 life (KB/Sec) 4594520/2737
   Outbound SPI : 0x20C8F68F, transform : esp-3des esp-md5-hmac
    Socket State: Open

Pending DMVPN Sessions:

R2#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
1   172.16.100.5            Tu100             12 00:14:48 1334  5000  0  8
0   172.16.100.6            Tu100             10 00:14:48  292  1752  0  7

R5#sh ip route eigrp | be Gateway
Gateway of last resort is not set

D     192.168.2.0/24 [90/27008000] via 172.16.100.2, 00:15:05, Tunnel100
```

```
D     192.168.6.0/24 [90/28288000] via 172.16.100.6, 00:14:59, Tunnel100

R6#sh ip route eigrp | be Gateway
Gateway of last resort is not set

D     192.168.2.0/24 [90/27008000] via 172.16.100.2, 00:15:19, Tunnel100
D     192.168.5.0/24 [90/28288000] via 172.16.100.5, 00:15:14, Tunnel100

R5#ping 192.168.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/52/56 ms

R5#traceroute 192.168.6.6

Type escape sequence to abort.
Tracing the route to 192.168.6.6

  1 172.16.100.6 36 msec *  36 msec
```

Detailed Solution

R2

```
no crypto ipsec transform-set SET41
crypto ipsec transform-set SET41 esp-3des esp-md5-hmac
 mode transport

int tu 100
  tunn prot ipsec prof IPSEC_PROF41
  no ip next-hop-self eigrp 100
```

R5

```
no crypto isakmp key ipexprt address 2.2.2.2
no crypto isakmp key ipexprt address 6.6.6.6

crypto isakmp key 0 ipexpert address 2.2.2.2
crypto isakmp key 0 ipexpert address 6.6.6.6
```

```
int tu 100
 no shut
 tunn so loop0
```

R6

```
interface Tunnel100
 no ip nhrp map 8.9.100.2 172.16.100.2
 ip nhrp map 172.16.100.2 8.9.100.2

router eigrp 100
 network 172.16.100.6 0.0.0.0

ip access-list ext OUTSIDE_IN
 no deny ip any any log
 permit udp host 8.9.100.2 host 8.9.100.6 eq isakmp
 permit udp host 8.9.100.5 host 8.9.100.6 eq isakmp
 permit esp host 8.9.100.2 host 8.9.100.6
 permit esp host 8.9.100.5 host 8.9.100.6
 200 deny ip any any log
```

Even that UDP packets generated by R6 are inspected you should still make an entry for anyone else who may want to establish a tunnel with this Spoke.

Verification

We will start on R5. First thing I want to see if the DMVPN is up with the Hub :

```
R5#sh ip nhrp br
   Target             Via             NBMA           Mode    Intfc    Claimed
172.16.100.2/32      172.16.100.2    8.9.100.2         static    Tu100    <
>


R5#sh ip nhrp traffic
Tunnel100: Max-send limit:100Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
```

```
            0 Error Indication  0 Traffic Indication
      Rcvd: Total 0
            0 Resolution Request  0 Resolution Reply  0 Registration Request
            0 Registration Reply  0 Purge Request  0 Purge Reply
            0 Error Indication  0 Traffic Indication

R5#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

OK – zero NHRP activity although we have the static mapping for the Hub. The ISAKMP tunnel does not exist and is not even tried to be brought up. Let's first take a look at the tunnel interface settings :

```
R5#sh run int tu 100
Building configuration...

Current configuration : 321 bytes
!
interface Tunnel100
 ip address 172.16.100.5 255.255.255.0
 no ip redirects
 ip nhrp map multicast 8.9.100.2
 ip nhrp map 172.16.100.2 8.9.100.2
 ip nhrp network-id 1
 ip nhrp nhs 172.16.100.2
 shutdown
 tunnel source Serial0/1/0
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile IPSEC_PROF41
```

OK, no shut and see what else may be broken :

```
R5#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
8.9.100.2       8.9.50.5        MM_NO_STATE          0 ACTIVE
```

Just run “debug crypto isakmp” on R5 and the Hub and try to find out what’s causing IKE negotiation to break :

```
*May 21 21:30:48.735: ISAKMP:(0): SA request profile is (NULL)
*May 21 21:30:48.735: ISAKMP: Created a peer struct for 8.9.100.2, peer
port 500
*May 21 21:30:48.735: ISAKMP: New peer created peer = 0x4B089694
peer_handle = 0x80000009
*May 21 21:30:48.735: ISAKMP: Locking peer struct 0x4B089694, refcount 1
for isakmp_initiator
*May 21 21:30:48.735: ISAKMP: local port 500, remote port 500
*May 21 21:30:48.735: ISAKMP: set new node 0 to QM_IDLE
*May 21 21:30:48.735: ISAKMP: Find a dup sa in the avl tree during calling
isadb_insert sa = 4B0E1DD0
*May 21 21:30:48.735: ISAKMP:(0):Can not start Aggressive mode, trying
Main mode.
*May 21 21:30:48.735: ISAKMP:(0):found peer pre-shared key matching
8.9.100.2


*May 21 21:30:48.739: ISAKMP:(0): beginning Main Mode exchange
*May 21 21:30:48.739: ISAKMP:(0): sending packet to 8.9.100.2 my_port 500
peer_port 500 (I) MM_NO_STATE
*May 21 21:30:48.739: ISAKMP:(0):Sending an IKE IPv4 Packet.
R5#
*May 21 21:30:58.739: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
```

OK so R5 sends first Phase I packet but it does not get anything back. I will enable “debug ip udp” on R2 to see if it gets those messages :

```
R2#
*May 21 21:35:43.779: UDP: rcvd src=8.9.50.5(500), dst=8.9.100.2(500),
length=176
```

It does, so this is not a problem in the Data Plane. But the ISAKMP debug still does not show anything. So looks like the device may not be listening for ISAKMP :

```
R2#sh control-plane host open-ports
Active internet connections (servers and established)
Prot               Local Address             Foreign Address
Service    State
 tcp                       *:23                          *:0
Telnet   LISTEN
```

```
 tcp                        *:80                         *:0
HTTP CORE   LISTEN
 tcp                        *:80                         *:0
HTTP CORE   LISTEN
 tcp                     *:23605               8.9.100.6:179         IOS
host service ESTABLIS
 tcp                     *:11108               8.9.100.1:179         IOS
host service ESTABLIS
 tcp                       *:179                         *:0
BGP   LISTEN
 tcp                       *:179                         *:0
BGP   LISTEN
 tcp                       *:179                         *:0
BGP   LISTEN
 tcp                     *:29925               8.9.100.5:179         IOS
host service ESTABLIS
 udp                      *:1975                         *:0
IPC   LISTEN

R2#sh cry map
No crypto maps found.
```

This is correct. But at least we have a transform and profile :

```
R2#sh cry ipse tra
Transform set SET41: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },


R2#sh cry ipse prof
IPSEC profile IPSEC_PROF41
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                SET41:  { esp-3des esp-sha-hmac  } ,
```

Before I apply the Profile, I want to make sure it matches what R5 has :

```
R5#sh cry ipse tra
Transform set SET41: { esp-3des esp-md5-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Based on our output we should use MD5. Another thing to fix, this time on R2. Does the tunnel come up now?

```
R5#
*May 21 21:39:50.683: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of
Informational mode failed with peer at 8.9.100.2
```

Not really :

```
*May 21 21:45:28.067: ISAKMP:(0):No pre-shared key with 8.9.50.5!
*May 21 21:45:28.067: ISAKMP:(0):no offers accepted!
*May 21 21:45:28.067: ISAKMP:(0): phase 1 SA policy not acceptable! (local
8.9.100.2 remote 8.9.50.5)
*May 21 21:45:28.067: ISAKMP (0): incrementing error counter on sa,
attempt 1 of 5: construct_fail_ag_init
```

Looks like R5 is sending packets from the incorrect interface. We need to change the tunnel source to be loopback0 :

```
R5#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
8.9.100.2       8.9.100.5       MM_KEY_EXCH       1001 ACTIVE
```

Now we stuck at the authentication stage. I saw in the debug we negotiated PSK so I definitely want to check the keys, if they match :

```
R5#sh cry isa ke
Keyring      Hostname/Address                          Preshared Key
default      8.9.100.2                                 ipexprt
```

```
              8.9.100.6                                       ipexprt

R2#sh cry isa key
Keyring      Hostname/Address                                 Preshared Key

default      8.9.100.5                                       ipexpert
             8.9.100.6                                       ipexpert
```

OK I have fixed both, for R2 and R6. We finally see the tunnel comes up :

```
R5#
*May 21 21:46:24.783: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
172.16.100.2 (Tunnel100) is up: new adjacency
```

I will now move on to R6 :

```
R6#sh ip nhrp br
   Target             Via             NBMA            Mode    Intfc   Claimed
8.9.100.2/32         8.9.100.2       172.16.100.2     static   Tu100   <
>

R6#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA

R6#sh ip nhrp traf
Tunnel100: Max-send limit:100Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication
```

R6 does not try to register with the Hub, same as R5 initially. But here - well, it says NBMA it is trying to use to get to the loopback is the logical address. Looks like the mapping is configured the other way round (first output from the “sh ip nhrp brief” command):

```
R6#sh run int tu 100 | in nhrp
 ip nhrp map 8.9.100.2 172.16.100.2
 ip nhrp map multicast 8.9.100.2
 ip nhrp network-id 1
 ip nhrp nhs 172.16.100.2
```

After changing the order in the “ip nhrp map” command it starts sending packets but a log showed up saying packets are dropped :

```
*May 21 21:53:37.591: %SEC-6-IPACCESSLOGNP: list OUTSIDE_IN denied 50
8.9.100.2 -> 8.9.100.6, 1 packet
```

Uhm, R6 is configured for CBAC. We need to modify the ACL to allow for DMVPN with R2 and R5 (IKE + ESP).

```
R6#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
8.9.100.2       8.9.100.6       QM_IDLE           1002 ACTIVE
```

Tunnel’s up, no adjacency though :

```
R6#sh ip eigrp ne
EIGRP-IPv4 Neighbors for AS(100)

R6#sh ip eigrp int
EIGRP-IPv4 Interfaces for AS(100)
                       Xmit Queue   Mean   Pacing Time   Multicast
Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer
Routes
Lo256              0        0/0         0       0/1            0
0
```

I need to enable EIGRP on the tunnel as well.

```
*May 21 21:58:33.775: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
172.16.100.2 (Tunnel100) is up: new adjacency

R6#sh ip ro ei
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

D     192.168.2.0/24 [90/27008000] via 172.16.100.2, 00:00:13, Tunnel100
D     192.168.5.0/24 [90/28288000] via 172.16.100.2, 00:00:13, Tunnel100
```

Right, but the next-hop does not match our output. Let's fix.

```
R6#sh ip ro ei
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

D     192.168.2.0/24 [90/27008000] via 172.16.100.2, 00:00:05, Tunnel100
D     192.168.5.0/24 [90/28288000] via 172.16.100.5, 00:00:00, Tunnel100



R5#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 172.16.100.5, VRF ""
   Tunnel Src./Dest. addr: 8.9.100.5/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "IPSEC_PROF41"
   Interface State Control: Disabled

IPv4 NHS:
172.16.100.2  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      8.9.100.2    172.16.100.2    UP 00:17:24    S
172.16.100.2/32



Crypto Session Details:
--------------------------------------------------------------------------
------

Interface: Tunnel100
Session: [0x4B112B60]
  IKEv1 SA: local 8.9.100.5/500 remote 8.9.100.2/500 Active
          Capabilities:(none) connid:1004 lifetime:23:42:35
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.2
  IPSEC FLOW: permit 47 host 8.9.100.5 host 8.9.100.2
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 251 drop 0 life (KB/Sec) 4395801/2555
        Outbound: #pkts enc'ed 243 drop 50 life (KB/Sec) 4395803/2555
   Outbound SPI : 0x8E9414B5, transform : esp-3des esp-md5-hmac
    Socket State: Open

Pending DMVPN Sessions:


R6#sh dmvpn det
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: 8.9.100.6/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "IPSEC_PROF41"
   Interface State Control: Disabled

IPv4 NHS:
172.16.100.2  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      8.9.100.2    172.16.100.2    UP 00:09:38    S
172.16.100.2/32



Crypto Session Details:
--------------------------------------------------------------------------
------

Interface: Tunnel100
Session: [0x4B156770]
  IKEv1 SA: local 8.9.100.6/500 remote 8.9.100.2/500 Active
          Capabilities:(none) connid:1002 lifetime:23:50:19
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.2
  IPSEC FLOW: permit 47 host 8.9.100.6 host 8.9.100.2
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 147 drop 0 life (KB/Sec) 4479595/3019
        Outbound: #pkts enc'ed 118 drop 0 life (KB/Sec) 4479598/3019
   Outbound SPI : 0xD33FE0FD, transform : esp-3des esp-md5-hmac
    Socket State: Open
```

```
Pending DMVPN Sessions:


R2#sh dmvpn det
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 172.16.100.2, VRF ""
   Tunnel Src./Dest. addr: 8.9.100.2/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "IPSEC_PROF41"
   Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target
Network
----- --------------- --------------- ----- -------- ----- ---------------
--
    1      8.9.100.5    172.16.100.5    UP 00:22:30    D
172.16.100.5/32

    1      8.9.100.6    172.16.100.6    UP 00:14:22    D
172.16.100.6/32



Crypto Session Details:
--------------------------------------------------------------------------
------

Interface: Tunnel100
Session: [0x712CF3E0]
  IKEv1 SA: local 8.9.100.2/500 remote 8.9.100.5/500 Active
          Capabilities:(none) connid:1004 lifetime:23:37:29
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.5
```

```
    IPSEC FLOW: permit 47 host 8.9.100.2 host 8.9.100.5
          Active SAs: 2, origin: crypto map
          Inbound:  #pkts dec'ed 409 drop 0 life (KB/Sec) 4416442/2249
          Outbound: #pkts enc'ed 417 drop 0 life (KB/Sec) 4416441/2249
     Outbound SPI : 0x1D1E11A1, transform : esp-3des esp-md5-hmac
      Socket State: Open

Interface: Tunnel100
Session: [0x712CF2F0]
  IKEv1 SA: local 8.9.100.2/500 remote 8.9.100.6/500 Active
          Capabilities:(none) connid:1006 lifetime:23:45:36
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.6
  IPSEC FLOW: permit 47 host 8.9.100.2 host 8.9.100.6
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 280 drop 0 life (KB/Sec) 4594523/2737
        Outbound: #pkts enc'ed 308 drop 0 life (KB/Sec) 4594520/2737
     Outbound SPI : 0x20C8F68F, transform : esp-3des esp-md5-hmac
      Socket State: Open

Pending DMVPN Sessions:
```

Task 4.2: FlexVPN with ASA (5 Points)

- A FlexVPN session should be established with ASA2
- ASA2 should act as the Initiator of this connection
- Protect the traffic between VLAN 49 and Loopback10 of R10
- Use AES-128, the strongest supported DH Group and SHA-256 for IKE_SA_INIT
- Authentication method selected should be PSK with a key “ipexpert”
- Use AES-128 and SHA-1 to protect CHILD_SA
- R10 should install a route to VLAN 49 with a tag of 100. Don’t use a crypto map
- You are allowed to add one static route to accomplish this task

Detailed Solution

ASA2

```
route outside 10.10.10.0 255.255.255.0 8.9.29.9 1
```

```
access-list PROXYACL per ip 10.49.49.0 255.255.255.0 10.10.10.0
255.255.255.0

crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 14
 prf sha256
 lifetime seconds 86400

crypto ipsec ikev2 ipsec-proposal SET1
 protocol esp encryption aes
 protocol esp integrity sha-1

tunnel-group 8.9.51.10 type ipsec-l2l
tunnel-group 8.9.51.10 ipsec-attributes
 ikev2 remote-authentication pre-shared-key ipexpert
 ikev2 local-authentication pre-shared-key ipexpert

crypto map MAP1 10 match address PROXYACL
crypto map MAP1 10 set peer 8.9.51.10
crypto map MAP1 10 set ikev2 ipsec-proposal SET1
crypto map MAP1 interface outside
crypto ikev2 enable outside
```

R10

```
crypto ikev2 proposal IKE_PROP
 encryption aes-cbc-128
 integrity sha256
 group 14

crypto ikev2 policy IKE_POL
 proposal IKE_PROP

crypto ikev2 keyring KRING
 peer ASA2
  address 8.9.29.20
  pre-shared-key ipexpert
```

```
crypto ikev2 profile IKE_PROF
 match identity remote address 8.9.29.20 255.255.255.255
 identity local address 8.9.51.10
 authentication remote pre-share
 authentication local pre-share
 keyring local KRING
 virtual-template 1

crypto ipsec transform-set SET1 esp-aes esp-sha-hmac

crypto ipsec profile IPSEC_PROF
 set transform-set SET1
 set reverse-route tag 100
 set ikev2-profile IKE_PROF

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF
```

R9

```
ip access-list extended OUTIN_PASS
 permit udp host 8.9.51.10 host 8.9.29.20 eq isakmp
 permit esp host 8.9.51.10 host 8.9.29.20

ip access-list extended INOUT_VPN
 permit udp host 8.9.29.20 host 8.9.51.10 eq isakmp
 permit esp host 8.9.29.20 host 8.9.51.10

class-map type inspect match-all ZFW_INOUT_VPN_CLASS
 match access-group name INOUT_VPN

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_INOUT_VPN_CLASS
  pass

zone-pair security OUTIN source OUT destination IN
 service-policy type inspect ZFW_OUTIN_POL
```

The use of Dynamic Virtual Tunnel Interface (DVTI) on the FlexVPN router allows this device to respond to the presented Traffic Selector with a mirror of the Traffic Selector that was presented by the Initiator. This feature can be used to establish a Flex VPN tunnel (not regular IKEv2 based on a crypto map) with the ASA.

Zone-Based Firewall elements for OUT->IN were partially configured in the ZFW task. This is why only needed to configure few of them here.

Verification

R10 initially does not know about VLAN 49. ASA2 will tell it about the prefix during tunnel establishment :

```
R10#sh ip route static | be Gate
Gateway of last resort is not set

CAT4#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 25/29/34 ms
```

Part of the IPSec debugs is shown :

```
*May 22 13:56:50.379: IPSEC: Expand action denied, discard or forward
packet.
*May 22 13:56:50.383: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 8.9.51.10:0, r
    remote= 8.9.29.20:0,
    local_proxy= 10.10.10.0/255.255.255.0/256/0,
    remote_proxy= 10.49.49.0/255.255.255.0/256/0,
    protocol= ESP, transform= NONE  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*May 22 13:56:50.383: Crypto mapdb : proxy_match
        src addr     : 10.10.10.0
        dst addr     : 10.49.49.0
        protocol     : 0
        src port     : 0
        dst port
```

```
*May 22 13:56:50.383: IPSEC(crypto_ipsec_create_ipsec_sas): Map found
Virtual-Access1-head-0

*May 22 13:56:50.387: IPSEC(rte_mgr): VPN Route Event Install new outbound
sa: Create IPV4 route from ACL for 8.9.29.20
*May 22 13:56:50.387: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access1
*May 22 13:56:50.387: IPSEC(rte_mgr): VPN Route Added 10.49.49.0
255.255.255.0 via Virtual-Access 1 in IP DEFAULT TABLE with tag 100
distance 1
```

And the prefix got installed :

```
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 GLOBAL DEFAULT
10.49.49.0/255.255.255.0 [1/0] via 8.9.29.20 tag 100 count 1 rtid 5
                               on Virtual-Access1 RRI

R10#sh ip route static | be Gate
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S        10.49.49.0/24 is directly connected, Virtual-Access1


R10#sh cry ikev2 session det
 IPv4 Crypto IKEv2 Session

Session-id:5, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf
Status
1         8.9.51.10/500         8.9.29.20/500         none/none
READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:14, Auth sign:
PSK, Auth verify: PSK
      Life/Active Time: 86400/190 sec
      CE id: 1008, Session-id: 5
```

```
        Status Description: Negotiation done
        Local spi: DA4940A390F88D90       Remote spi: 07A5D40D45F971C6
        Local id: 8.9.51.10
        Remote id: 8.9.29.20
        Local req msg id:  0              Remote req msg id:  15
        Local next msg id: 0              Remote next msg id: 15
        Local req queued:  0              Remote req queued:  15
        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 : No
    Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
              remote selector 10.49.49.0/0 - 10.49.49.255/65535
              ESP spi in/out: 0xE34CA7E5/0xF7575B18
              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


    ASA2(config)# sh vpn-sessiondb det l2l

    Session Type: LAN-to-LAN Detailed

    Connection   : 8.9.51.10
    Index        : 9                     IP Addr      : 8.9.51.10
    Protocol     : IKEv2 IPsec
    Encryption   : AES128 AES128         Hashing      : SHA256 SHA1
    Bytes Tx     : 400                   Bytes Rx     : 400
    Login Time   : 14:05:51 UTC Wed May 22 2013
    Duration     : 0h:04m:20s
    IKEv2 Tunnels: 1
    IPsec Tunnels: 1

    IKEv2:
      Tunnel ID    : 9.1
      UDP Src Port : 500                 UDP Dst Port : 500
      Rem Auth Mode: preSharedKeys
      Loc Auth Mode: preSharedKeys
```

```
    Encryption   : AES128                 Hashing      : SHA256
    Rekey Int (T): 86400 Seconds          Rekey Left(T): 86140 Seconds
    PRF          : SHA256                 D/H Group    : 14
    Filter Name  :
    IPv6 Filter  :

  IPsec:
    Tunnel ID    : 9.2
    Local Addr   : 10.49.49.0/255.255.255.0/0/0
    Remote Addr  : 10.10.10.0/255.255.255.0/0/0
    Encryption   : AES128                 Hashing      : SHA1
    Encapsulation: Tunnel
    Rekey Int (T): 28800 Seconds          Rekey Left(T): 28540 Seconds
    Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
    Idle Time Out: 30 Minutes             Idle TO Left : 25 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)   : 261 Seconds
    Hold Left (T): 0 Seconds              Posture Token:
    Redirect URL :


  R9#sh policy-firewall stats zone-pair  INOUT | s VPN
      Class-map: ZFW_INOUT_VPN_CLASS (match-all)
        Match: access-group name INOUT_VPN
        Pass
          4 packets, 400 bytes
```

Task 4.3: IPv6 FlexVPN (5 Points)

- Configure a FlexVPN tunnel between R10 and R11
- VPN traffic should be transported using IPv6
- Protect packets exchanged between Loopback10 interfaces of those devices
- Use Smart Defaults on R11
- Authenticate the tunnel using PSK “ipexpert1011”

Detailed Solution

R10

```
crypto ikev2 proposal IKE_PROP
  group 14 5

crypto ikev2 keyring KRING2
 peer R11
  address 2907::11/128
  pre-shared-key ipexpert1011

crypto ikev2 profile IKE_PROF2
 match identity remote address 2907::11/128
 identity local address 2951::10
 authentication remote pre-share
 authentication local pre-share
 keyring local KRING2

crypto ipsec profile IPSEC_PROF2
 set transform-set SET1
 set ikev2-profile IKE_PROF2

interface Tunnel1011
 ipv6 address 2000:1011::10/64
 ipv6 eigrp 1011
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2907::11
 tunnel protection ipsec profile IPSEC_PROF2

ipv6 router eigrp 1011
 no shut
```

R11

```
crypto ikev2 keyring KRING2
 peer R10
  address 2951::10/128
```

```
 pre-shared-key ipexpert1011

crypto ikev2 profile IKE_PROF2
 match identity remote address 2951::10/128
 identity local address 2907::11
 authentication remote pre-share
 authentication local pre-share
 keyring local KRING2

crypto ipsec profile default
 set ikev2-profile IKE_PROF2

interface Tunnel1011
 ipv6 address 2000:1011::11/64
 ipv6 eigrp 1011
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2951::10
 tunnel protection ipsec profile default

ipv6 router eigrp 1011
 no shut
```

IPS C2

```
ipv6 access-list OUTSIDE6_IN permit udp host 2951::10 host 2907::11 eq
isakmp
ipv6 access-list OUTSIDE6_IN permit esp host 2951::10 host 2907::11

access-group OUTSIDE6_IN in interface outside
```

IPS C1 & C2

```
service signature-definition SIG1
signatures 1250 0
status
enabled false
exit
exit
yes
```

Since we were told to use Smart Defaults on R11 we had to adjust the Proposal on R10. This way we use group 14 for the ASA and group 5 for R11.

General Rules for this lab forbid to use static routes unless otherwise stated in the task. This task did not mention anything about static routes so we enabled EIGRP over the tunnel to learn about loopbacks.

For explanations that pertain to IPS refer to the Verification section below.

Verification

OK first thing you should notice when routers try to bring up the tunnel (assuming you have not applied IPS solution) is that the ASA is complaining about IPS dropping IKEv2 packets :

```
May 22 2013 16:03:32: %ASA-4-420002: IPS requested to drop UDP packet from
inside:2907::11/500 to outside:2951::10/500
May 22 2013 16:03:40: %ASA-4-420002: IPS requested to drop UDP packet from
inside:2907::11/500 to outside:2951::10/500
```

The problem is that if you log to the IPS console to see what signature triggers the drop action, nothing is shown. This means that the sig has the “Produce Alert” action turned off.

Here’s the trick you can use to quickly find the culprit (instead of adding Produce Alert everywhere) – just observe what counters increase. In our case 2004 and 1610 and Echo signatures we tested in one of the previous task. So it must be 1250 :

```
IPS# show statistics virtual-sensor | in Sig
      Name of current Signature-Defintion instance = SIG1
      The Signature Database Statistics.
      SigEvent Preliminary Stage Statistics
         Number of Active SigEventDataNodes  = 6
         Per-Signature SigEvent count since reset
            Sig 1250.0 = 69
            Sig 1610.0 = 7
            Sig 2004.0 = 2
      SigEvent Action Override Stage Statistics
      SigEvent Action Filter Stage Statistics
      SigEvent Action Handling Stage Statistics.
      Name of current Signature-Defintion instance = sig0
      The Signature Database Statistics.
```

```
        SigEvent Preliminary Stage Statistics
           Number of Active SigEventDataNodes  = 1
           Per-Signature SigEvent count since reset
              Sig 2004.0 = 41
        SigEvent Action Override Stage Statistics
        SigEvent Action Filter Stage Statistics
        SigEvent Action Handling Stage Statistics.


IPS(config)# service signature-definition SIG1
IPS(config-sig)# signatures 1250 0
IPS(config-sig-sig)# show settings
      <protected entry>
   sig-id: 1250
   subsig-id: 0
   ------------------------------------------------
      alert-severity: medium <defaulted>
      sig-fidelity-rating: 100 <defaulted>
      promisc-delta: 0 <defaulted>
      sig-description
      ------------------------------------------------
         sig-name: Packet Bad Length <defaulted>
         sig-string-info: Packet Bad Length <defaulted>
         sig-comment:  <defaulted>
         alert-traits: 0 <defaulted>
         release: S230 <defaulted>
         sig-creation-date: 20050725 <defaulted>
         sig-type: Anomaly <defaulted>
      ------------------------------------------------
      engine
      ------------------------------------------------
         normalizer
         ------------------------------------------------
            event-action: deny-packet-inline <defaulted>
            event-action-settings
            ------------------------------------------------
               external-rate-limit-type

--- Omitted ---
```

Based on this information you can go ahead and enable Produce Alert to make sure that's the sig that causes problems :

```
IPS(config-sig-sig)# engine normalize
IPS(config-sig-sig-nor)# event-action produce-alert|deny-packet-inline
IPS(config-sig-sig-nor)# exit
IPS(config-sig-sig)# exit
IPS(config-sig)# exit
Apply Changes?[yes]:
```

```
evIdsAlert: eventId=6820428300717 severity=medium vendor=Cisco
alarmTraits=32768
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 1261
  time: 2013/05/22 16:22:00 2013/05/22 16:22:00 UTC
  signature: description=Packet Bad Length id=1250 created=20050725
type=anomaly version=S230
    subsigId: 0
    sigDetails: Packet Bad Length
  interfaceGroup: VS1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 0.0.0.0
      port: 500
      ipv6Address: locality=OUT 2951::10
    target:
      addr: locality=OUT 0.0.0.0
      port: 500
      ipv6Address: locality=OUT 2907::11
      os: idSource=unknown relevance=relevant type=unknown
actions:
    deniedPacket: true
  alertDetails: InterfaceAttributes:  context="C2" physical="Unknown"
backplane="PortChannel0/0" ;
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
```

```
  interface: backplane=PortChannel0/0 context=C2 physical=Unknown
PortChannel0/0
  protocol: udp
```

In the solution we have simply disabled it.

```
R11#
*May 22 16:38:53.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel1011, changed state to up



R10#sh cry ikev2 session de | be IPv6
 IPv6 Crypto IKEv2 Session

Session-id:9, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id    fvrf/ivrf              Status
2          none/none             READY
Local  2951::10/500
Remote  2907::11/500
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/148 sec
      CE id: 1012, Session-id: 9
      Status Description: Negotiation done
      Local spi: CE06A0EB8E1C5126       Remote spi: 4CCA8547A8FEE7B8
      Local id: 2951::10
      Remote id: 2907::11
      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: 0xD91B9850/0x9AEEA0CA
          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


R10#sh ipv route eigrp
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D   2011::/64 [90/27008000]
     via FE80::CA4C:75FF:FE1F:DDC0, Tunnel1011
R11#ping 2010::10 so loop10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::10, timeout is 2 seconds:
Packet sent with a source address of 2011::11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms


R10#sh cry sess local 2951::10 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: Tunnel1011
Uptime: 00:05:54
Session status: UP-ACTIVE
Peer: 2907::11 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 2907::11
      Desc: (none)
  IKEv2 SA: local 2951::10/500
            remote 2907::11/500 Active
```

```
          Capabilities:(none) connid:2 lifetime:23:54:06
    IPSEC FLOW: permit ipv6 ::/0 ::/0
          Active SAs: 2, origin: crypto map
          Inbound:  #pkts dec'ed 105 drop 0 life (KB/Sec) 4276916/3245
          Outbound: #pkts enc'ed 110 drop 0 life (KB/Sec) 4276920/3245
```

5.0 Identity Management (12 points)

Task 5.1: Cut-Through Proxy (5 Points)

- Users in VLAN 51 should be authenticated prior to reaching HTTP, MS SQL and Oracle services hosted in VLAN 49
- The following devices should be accessible to authenticated users :
  - 10.49.49.51 (HTTP & MS SQL)
  - 10.49.49.52 (Oracle)
- ISE should be used as a source of authentication and authorization information
- You are expected to use a granular feature-specific condition in your policies – use Client-Type VSA to accomplish this
- Authenticate using Telnet as “cutproxy” with password “cisco1”
- Protect RADIUS communication with a key “ipexpert”

Detailed Solution

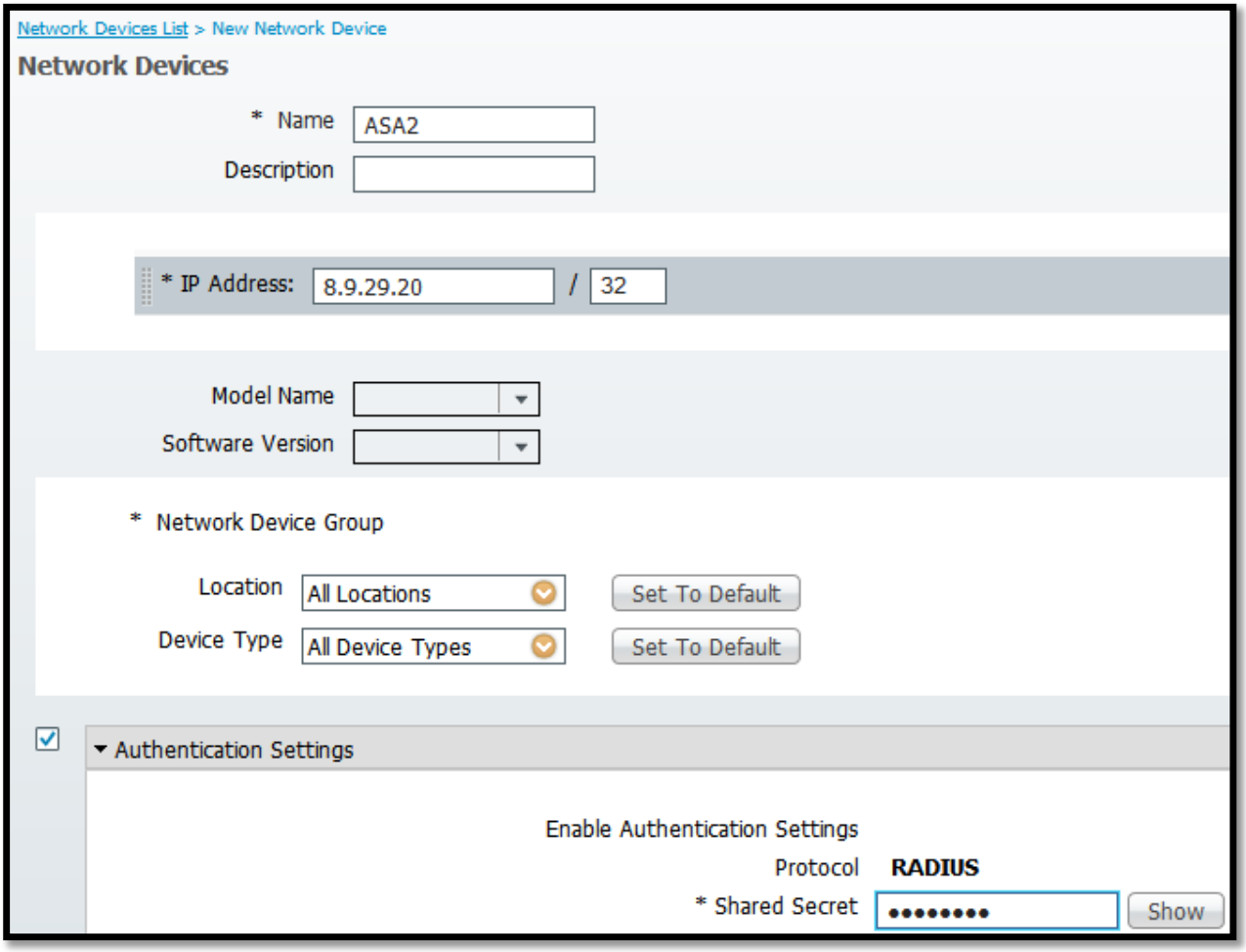
R9

```
ip access-list extended OUTIN_INSPECT
 permit tcp 8.9.51.0 0.0.0.255 host 8.9.29.50 eq www 1433
 permit tcp 8.9.51.0 0.0.0.255 host 8.9.29.51 eq www 1521
 permit tcp 8.9.51.0 0.0.0.255 host 8.9.29.100 eq telnet

ip access-list extended RADIUS
 permit udp host 8.9.29.20 host 8.9.19.150 eq 1645
 permit udp host 8.9.29.20 host 8.9.19.150 eq 1646

class-map type inspect match-all ZFW_INOUT_RADIUS_CLASS
 match access-group name RADIUS

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_INOUT_RADIUS_CLASS
  inspect
```

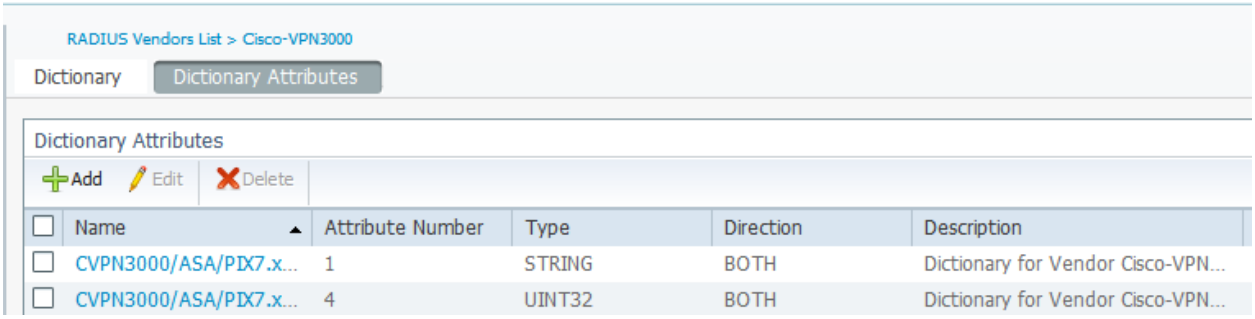
ASA2

```
virtual telnet 8.9.29.100

object network VIP
 host 8.9.29.100
 nat (inside,outside) static 8.9.29.100

object network SERVER_50
 host 10.49.49.50
 nat (inside,outside) static 8.9.29.50

object network SERVER_51
 host 10.49.49.51
 nat (inside,outside) static 8.9.29.51

access-l OUTSIDE_IN permit tcp 8.9.51.0 255.255.255.0 host 8.9.29.100 eq
23

aaa-server RAD protocol radius
aaa-server RAD (outside) host 8.9.19.150
 key ipexpert

access-list CUTP permit tcp 8.9.51.0 255.255.255.0 host 8.9.29.100 eq 23

aaa authentication match CUTP outside RAD

access-group OUTSIDE_IN in interface outside per-user-override
```

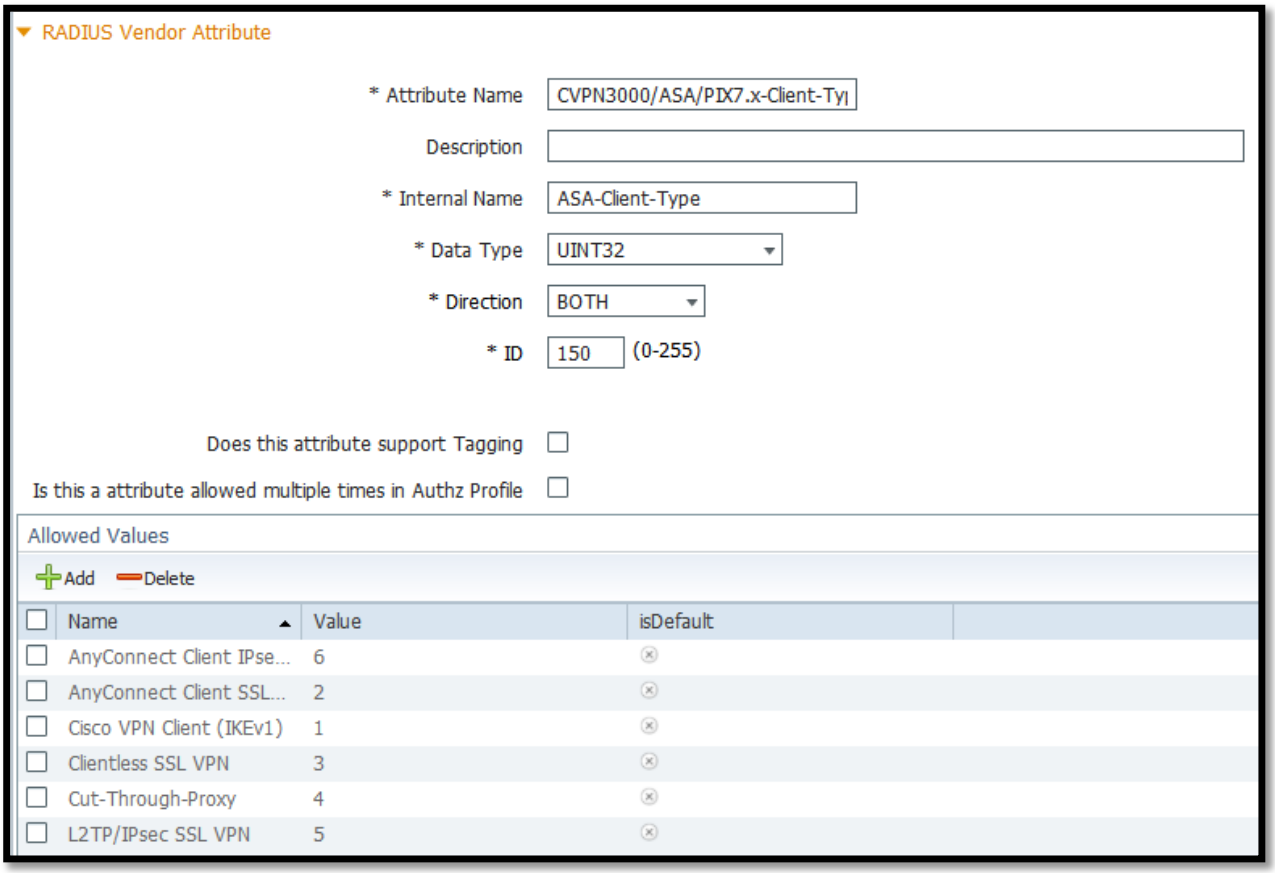
ISE



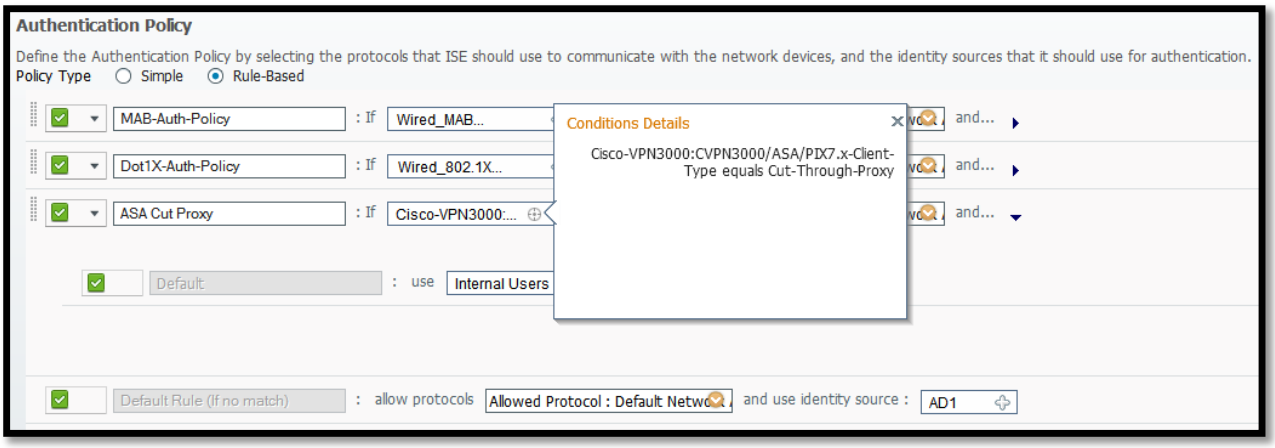
Since the "Client-Type" attribute is not part of the default Dictionary for VSA 3076 (Cisco-VPN3000), we need to add it manually. Go under Policies -> Dictionaries -> RADIUS -> RADIUS Vendors > Cisco-VPN3000 and add a new Attribute



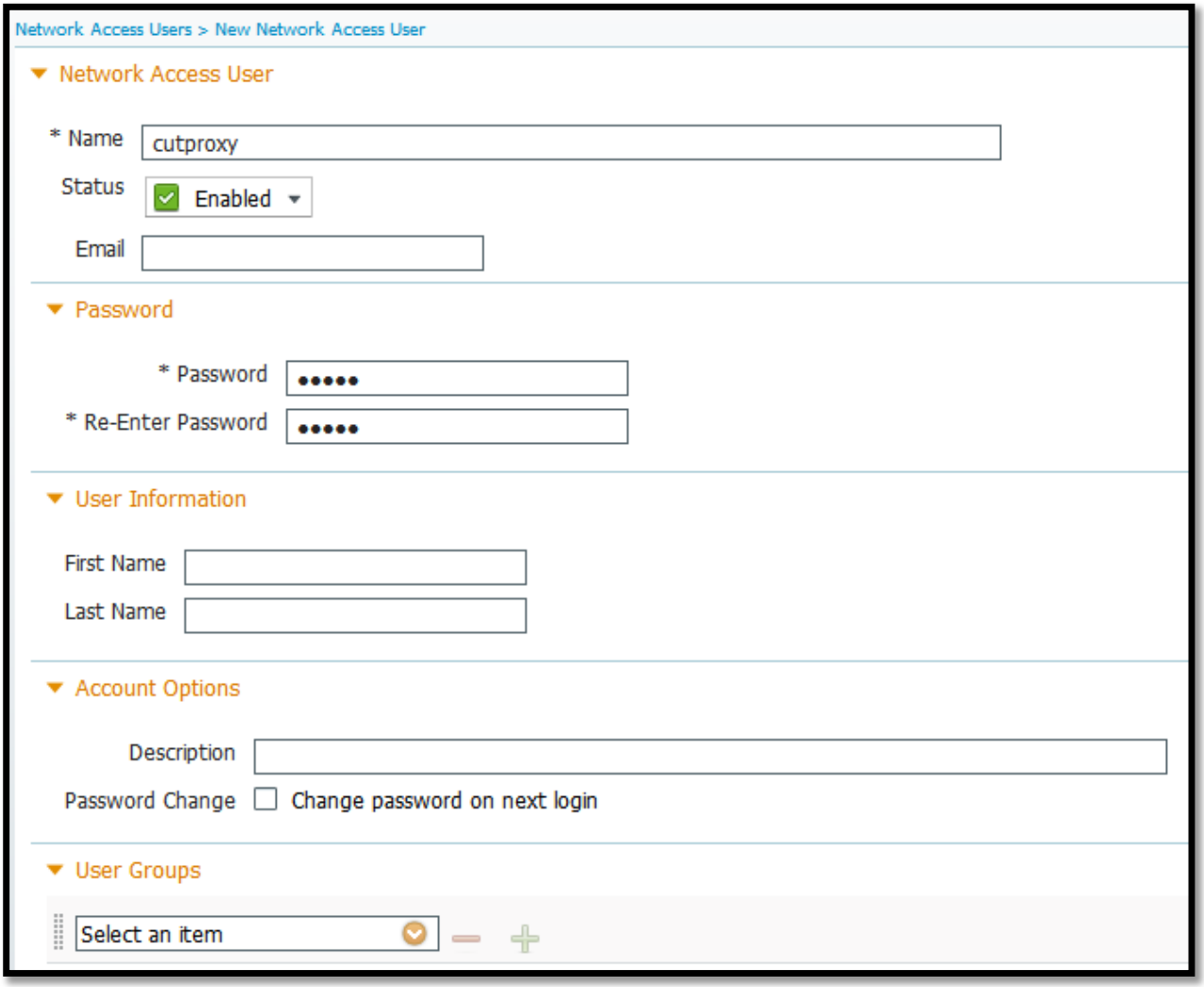
You don't have to populate full names, in our case just one Attribute for Value "4" would be enough. The example shows you how to populate all defined attributes :

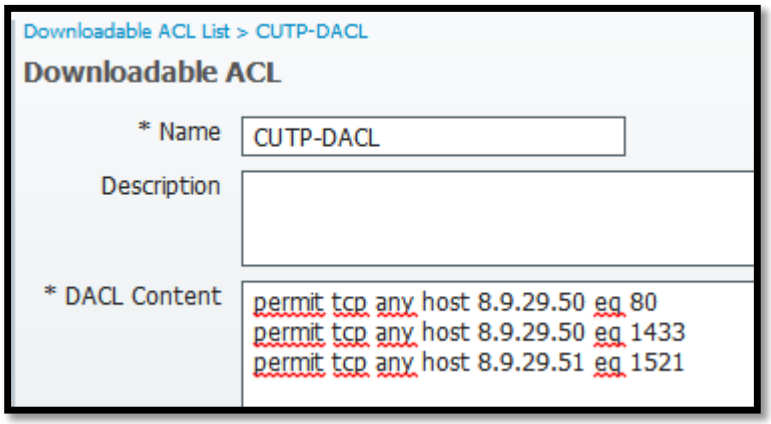


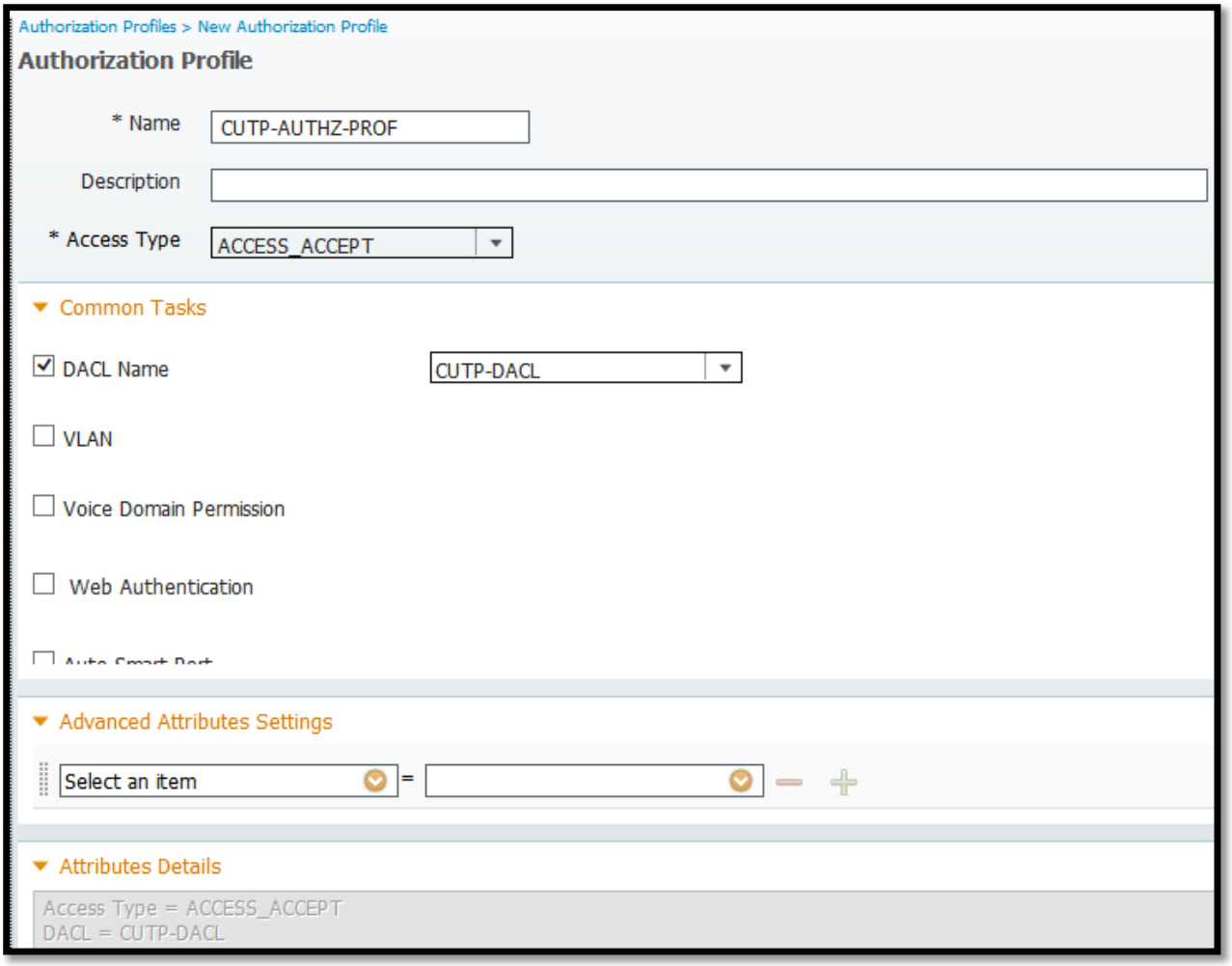
Now we're going to create an Authentication rule that will use Internal DB for all Cut-Proxy requests from ASAs :

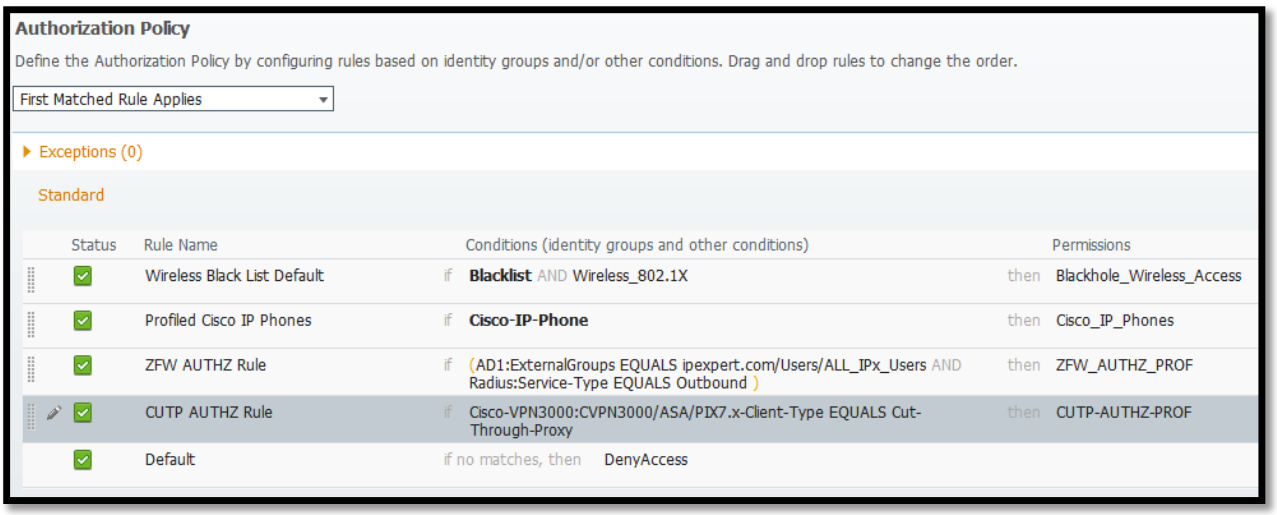


Now create the remaining elements we need for this task and configure an AuthZ rule :









The Client-Type attribute (VSA 3076/150) allows the ASA to send the type of service/client that is being authenticated to the ISE in Access-Request (and Accounting-Request) packets, and allows ISE to make policy decisions based on that attribute. Note that there is no configuration required on the ASA to use this attribute – it is sent automatically (at least in single mode – when multiple contexts are used this attribute does not appear to be sent).

Currently defined values for the Client-Type are as follows :

1. Cisco VPN Client (IKEv1)
2. AnyConnect Client SSL VPN
3. Clientless SSL VPN
4. Cut-Through-Proxy
5. L2TP/IPsec SSL VPN
6. AnyConnect Client IPsec VPN (IKEv2)

OK now how do you know what value is used by what service and what is the VSA ID? You don't have to memorize that – just go to the ASA Configuration Guide, "Configuring an External Server for Security Appliance User Authorization" -> "ASA RADIUS Authorization Attributes" and look for "Client-Type".

Verification

Telnet to 8.9.29.100 from R10 to trigger an authentication prompt. Authenticate as "cutproxy" :

```
R10#telnet 8.9.29.100
Trying 8.9.29.100 ... Open

LOGIN Authentication

Username:cutproxy
Password:

Error:  acl authorization denied
```

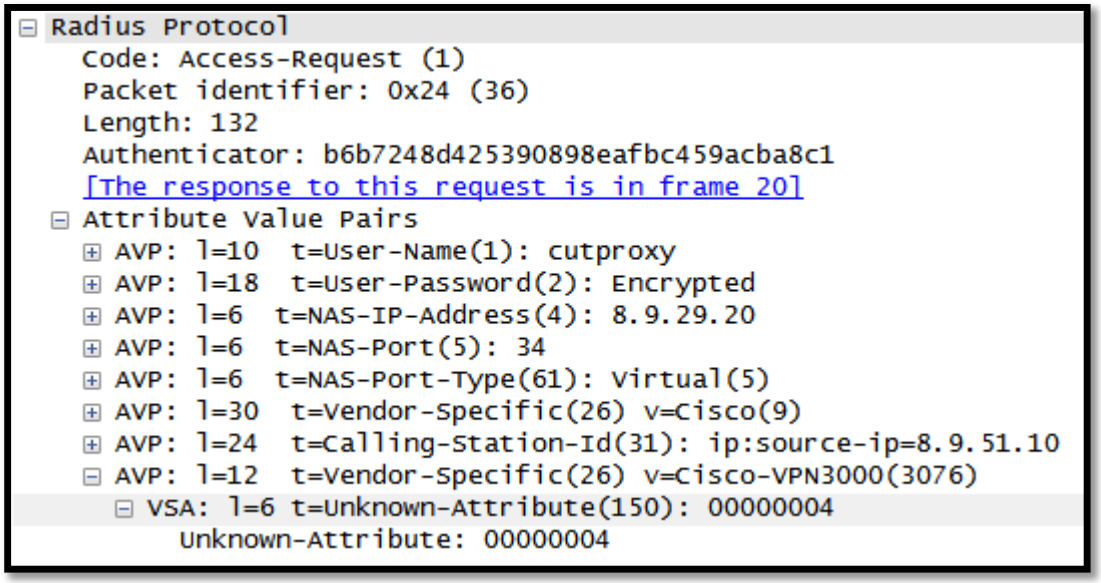
It says "acl authorization denied" because Telnet is not allowed by the downloaded ACL. This is all fine.

If you enabled RADIUS debug on ASA2 you would note the Client-Type is populated with a value of 4 (Cut-Through Proxy) :

```
RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 132).....
01 27 00 84 aa 9b 38 11 76 77 e4 4d 02 13 50 49    |  .'....8.vw.M..PI
4e 6f 7c 05 01 0a 63 75 74 70 72 6f 78 79 02 12    |  No|...cutproxy..
c6 b4 39 d9 75 20 c2 f2 5f 1d 2d ba c1 dd e8 ad    |  ..9.u .._.-.....
04 06 08 09 1d 14 05 06 00 00 00 25 3d 06 00 00    |  ...........%=...
00 05 1a 1e 00 00 00 09 01 18 69 70 3a 73 6f 75    |  ..........ip:sou
72 63 65 2d 69 70 3d 38 2e 39 2e 35 31 2e 31 30    |  rce-ip=8.9.51.10
1f 18 69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 38    |  ..ip:source-ip=8
2e 39 2e 35 31 2e 31 30 1a 0c 00 00 0c 04 96 06    |  .9.51.10........
00 00 00 04                                        |  ....

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 39 (0x27)
Radius: Length = 132 (0x0084)
Radius: Vector: AA9B38117677E44D021350494E6F7C05
Radius: Type = 1 (0x01) User-Name
Radius: Length = 10 (0x0A)
Radius: Value (String) =
63 75 74 70 72 6f 78 79                            |  cutproxy
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
c6 b4 39 d9 75 20 c2 f2 5f 1d 2d ba c1 dd e8 ad    |  ..9.u .._.-.....
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 8.9.29.20 (0x08091D14)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x25
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
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 35 31 2e 31 30                                  |  .51.10
Radius: Type = 31 (0x1F) Calling-Station-Id
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 35 31 2e 31 30                                  |  .51.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 4 (0x0004)
send pkt 8.9.19.150/1645
rip 0xac642eac state 7 id 39
```

This information is received by ISE (you can run TCP Dump to verify that) but due to a bug it may not be properly processed by the appliance in this code version. It took me 3 hours to play with the values, restarting the services, using “Not Equal”/“Equals” and it finally worked out for me but if it does not work for you and you have configured all as in the solution you get the full credit for this task :



```
ASA2(config)# sh uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'cutproxy' at 8.9.51.10, authenticated
   access-list #ACSACL#-IP-CUTP-DACL-519e358d (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00

R10#telnet 8.9.29.50 80
Trying 8.9.29.50, 80 ...
% Connection timed out; remote host not responding

R10#telnet 8.9.29.50 1433
Trying 8.9.29.50, 1433 ...
% Connection timed out; remote host not responding

R10#telnet 8.9.29.51 1521
Trying 8.9.29.51, 1521 ...
% Connection timed out; remote host not responding

ASA2(config)# sh access-list | in DACL
access-list #ACSACL#-IP-CUTP-DACL-519e358d; 3 elements; name hash:
0xa741bdba (dynamic)
access-list #ACSACL#-IP-CUTP-DACL-519e358d line 1 extended permit tcp any
host 8.9.29.50 eq www (hitcnt=2) 0xfbbd2d85
access-list #ACSACL#-IP-CUTP-DACL-519e358d line 2 extended permit tcp any
host 8.9.29.50 eq 1433 (hitcnt=2) 0x7744dce2
access-list #ACSACL#-IP-CUTP-DACL-519e358d line 3 extended permit tcp any
host 8.9.29.51 eq sqlnet (hitcnt=2) 0x7d29e6f2
```

Note the “Other Attributes” section – it says the Client-Type is “4” :

RADIUS Authentication Details

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

Username:	cutproxy
RADIUS Username :	cutproxy
Calling Station ID:	ip:source-ip=8.9.51.10
Framed IP Address:	
Use Case:	
Network Device:	ASA2
Network Device Groups:	Device Type#All Device Types,Location#All Locations
NAS IP Address:	8.9.29.20
NAS Identifier:	
NAS Port:	45
NAS Port ID:	
NAS Port Type:	Virtual
Allowed Protocol:	Default Network Access
Service Type:	
Identity Store:	Internal Users
Authorization Profiles:	CUTP-AUTHZ-PROF
Active Directory Domain:	
Identity Group:	
Allowed Protocol Selection Matched Rule:	Standard Rule 1
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users
Authorization Policy Matched Rule:	CutProxy Rule AuthZ
SGA Security Group:	
AAA Session ID:	pod124ise/158696514/8
Audit Session ID:	
Tunnel Details:	
Cisco-AVPairs:	ip:source-ip=8.9.51.10
Other Attributes:	ConfigVersionId=5,DestinationPort=1645,Protocol=Radius,Client-Type=4,CPMSessionID=0ac806f400000007519E3598,Device Type=Device Type#All Device Types,Location=Location#All Locations,Device IP Address=8.9.29.20

Authentication Summary

Logged At:	May 23,2013 3:28:24.574 PM
RADIUS Status:	DACL Download Succeeded
NAS Failure:	
Username:	#ACSACL#-IP-CUTP-DACL-519e358d
MAC/IP Address:	ip:source-ip=8.9.51.10
Network Device:	ASA2 : 8.9.29.20 :
Allowed Protocol:	
Identity Store:	
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	

Authentication Result

User-Name=#ACSACL#-IP-CUTP-DACL-519e358d
State=ReauthSession:0ac806f400000008519E3598
Class=CACS:0ac806f400000008519E3598:pod124ise/158696514/9
Termination-Action=RADIUS-Request
cisco-av-pair=ip:inacl#1=permit tcp any host 8.9.29.50 eq 80
cisco-av-pair=ip:inacl#2=permit tcp any host 8.9.29.50 eq 1433
cisco-av-pair=ip:inacl#3=permit tcp any host 8.9.29.51 eq 1521

Task 5.2: 802.1x (4 Points)

Deploy 802.1x authentication on G1/0/12 interface of CAT3

Only two devices are allowed to connect through this port – Phone and PC

All Profiling Services should be turned off

If ISE becomes unreachable make sure the Phone gets assigned to the Voice VLAN (599)

Authenticated user should be placed into VLAN 29

Unless the port is authenticated no user traffic should be allowed through it

Use AD database for authentication (e.g. IPXEMP1//cisco)

Protect RADIUS communication with key “ipexpert”

Detailed Solution

CAT4

```
vlan 599
 name VOICE
```

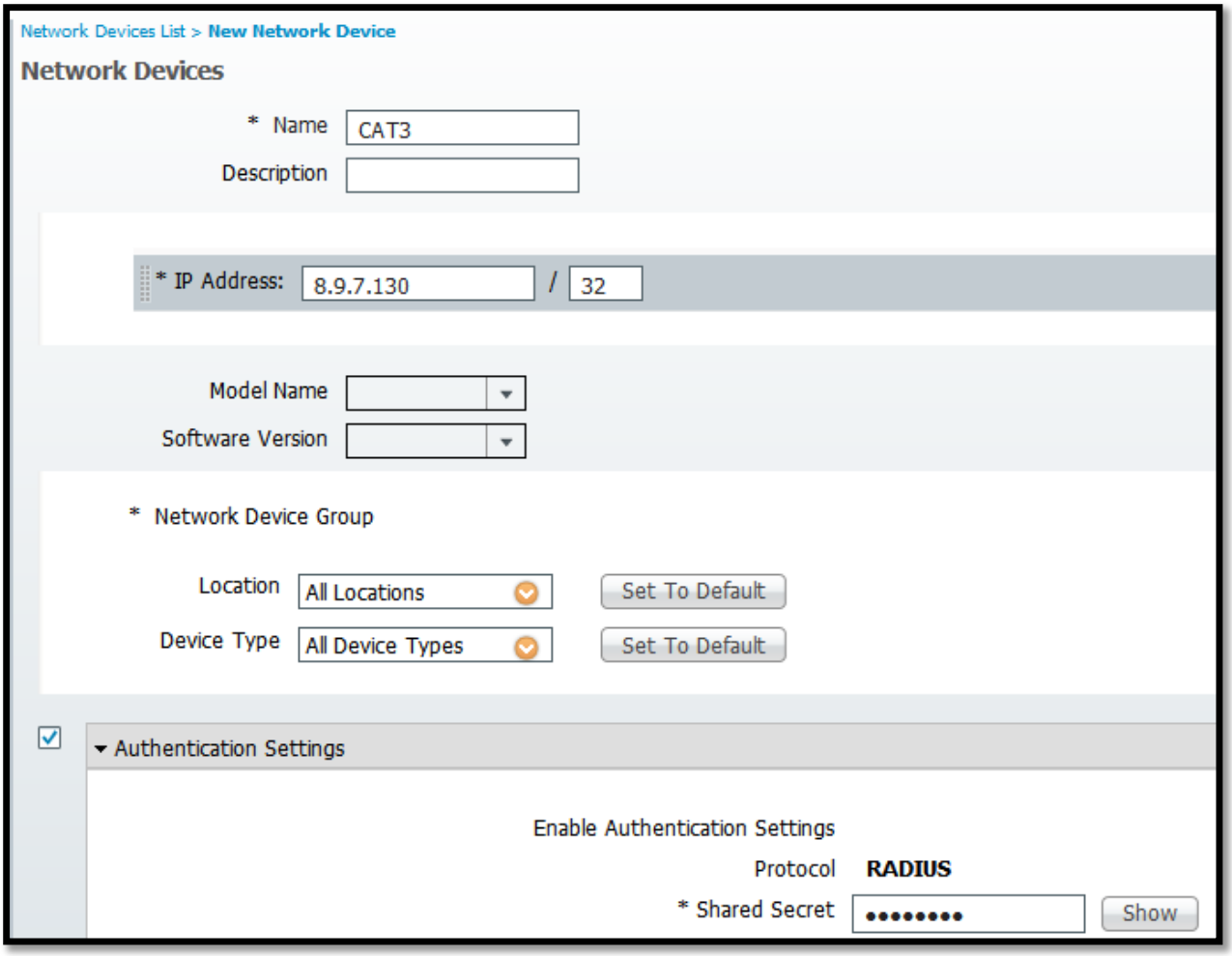
CAT3

```
aaa new-model
aaa authentication login default none
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

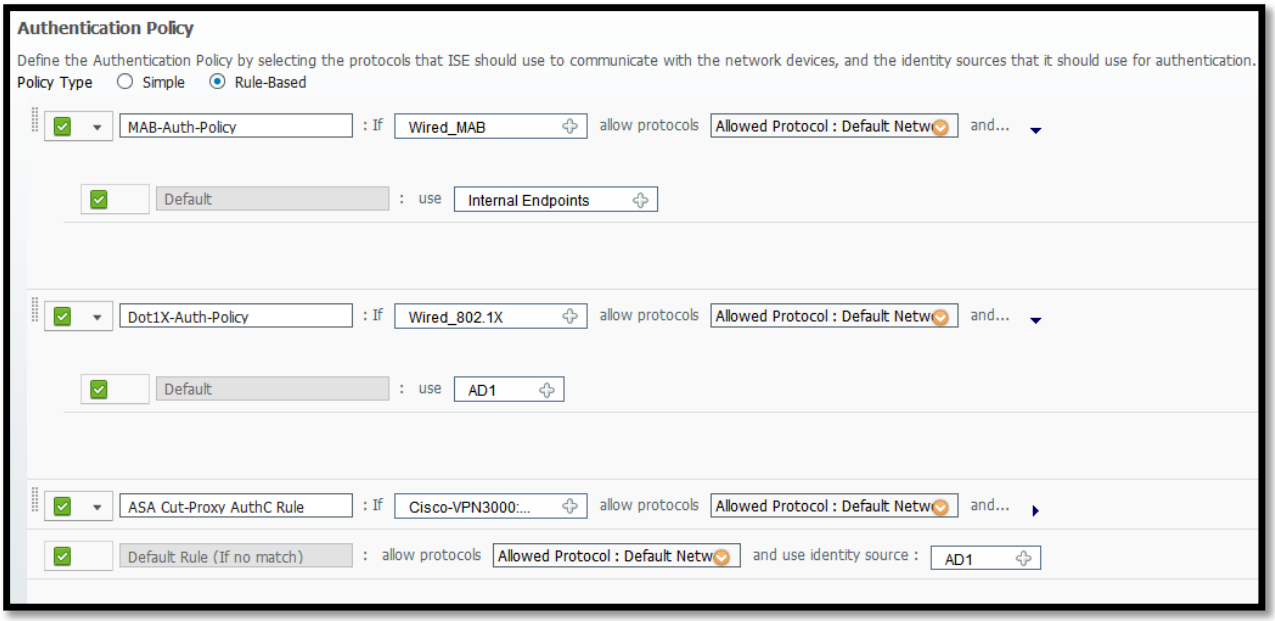
```
radius server ISE
 address ipv4 8.9.19.150 auth-port 1645 acct-port 1646
 key ipexpert

dot1x system-auth-control

interface GigabitEthernet1/0/12
 switchport mode access
 switchport voice vlan 599
 spanning-tree portfast
 authentication event fail action next-method
 authentication event server dead action authorize voice
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-domain
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
```

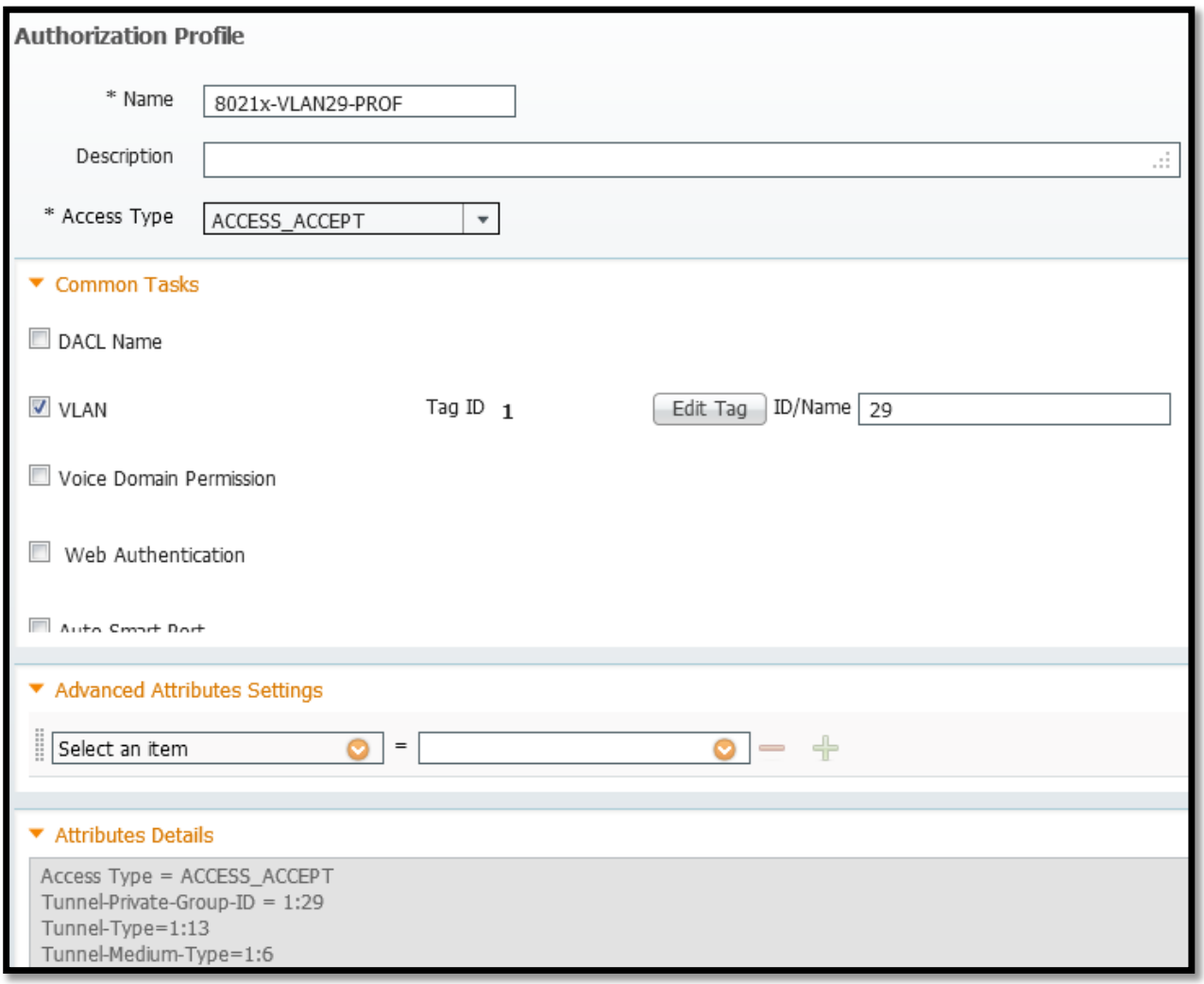
ISE

Part of the ISE configuration was done in the User-Based firewall task.

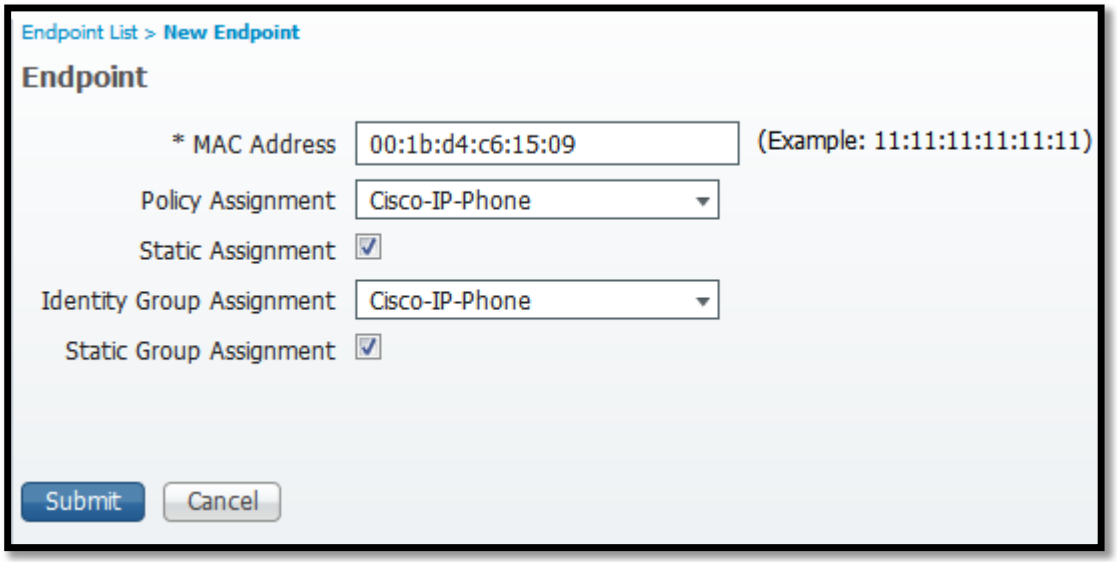


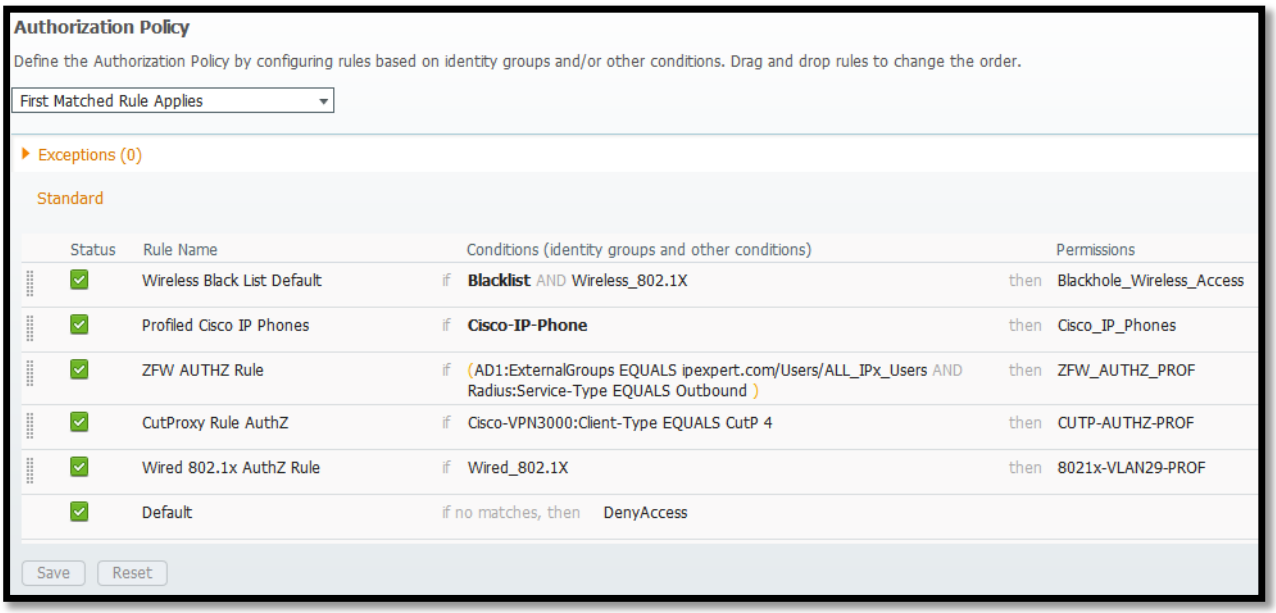
The AuthC policy should point to Internal Endpoint DB for MAB and AD1 for 802.1x :





We definitely want to add a static entry for our Phone. Otherwise MAB will always fail. Also since we will be using a default AuthZ rule for the Phones (that selects Voice Permission Profile) we should statically Profile the endpoint to be a Cisco Phone and assign it to Cisco-IP-Phone group (you could be more accurate and use CDP to figure out the exact Phone Model but here we don't care) :





If you did not select a Static Group for the Phone endpoint the Group would be derived from the Profile which would work as well.

Verification

We will first test the Critical Voice VLAN feature. Apply an ACL blocking RADIUS on the inside of C2 and wait for MAB to timeout :

```
CAT3#
*Mar  8 07:40:43.605: %AUTHMGR-5-START: Starting 'mab' for client
(001b.d4c6.1509) on Interface Gi1/0/12 AuditSessionID
08090782000001B125B1D987

*Mar  8 07:41:03.041: %MAB-5-FAIL: Authentication failed for client
(001b.d4c6.1509) on Interface Gi1/0/12 AuditSessionID
08090782000001B125B1D987

*Mar  8 07:41:03.041: %AUTHMGR-7-RESULT: Authentication result 'server
dead' from 'mab' for client (001b.d4c6.1509) on Interface Gi1/0/12
AuditSessionID 08090782000001B125B1D987

*Mar  8 07:41:03.050: %AUTHMGR-5-FAIL: Authorization failed or unapplied
for client (001b.d4c6.1509) on Interface Gi1/0/12 AuditSessionID
08090782000001B125B1D987

CAT3(config-if)#do sh authen sess int g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4c6.1509
           IP Address:  Unknown
            User-Name:  001bd4c61509
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  08090782000001B125B1D987
      Acct Session ID:  0x00000017
               Handle:  0xC20001B2

Runnable methods list:
```

```
          Method   State
          dot1x    Failed over
          mab      Authc Failed

   Critical Authorization is in effect for domain(s) VOICE
```

After we add an entry for the Phone to the Endpoint DB it should get successfully authenticated and Voice Permission should be received from ISE :

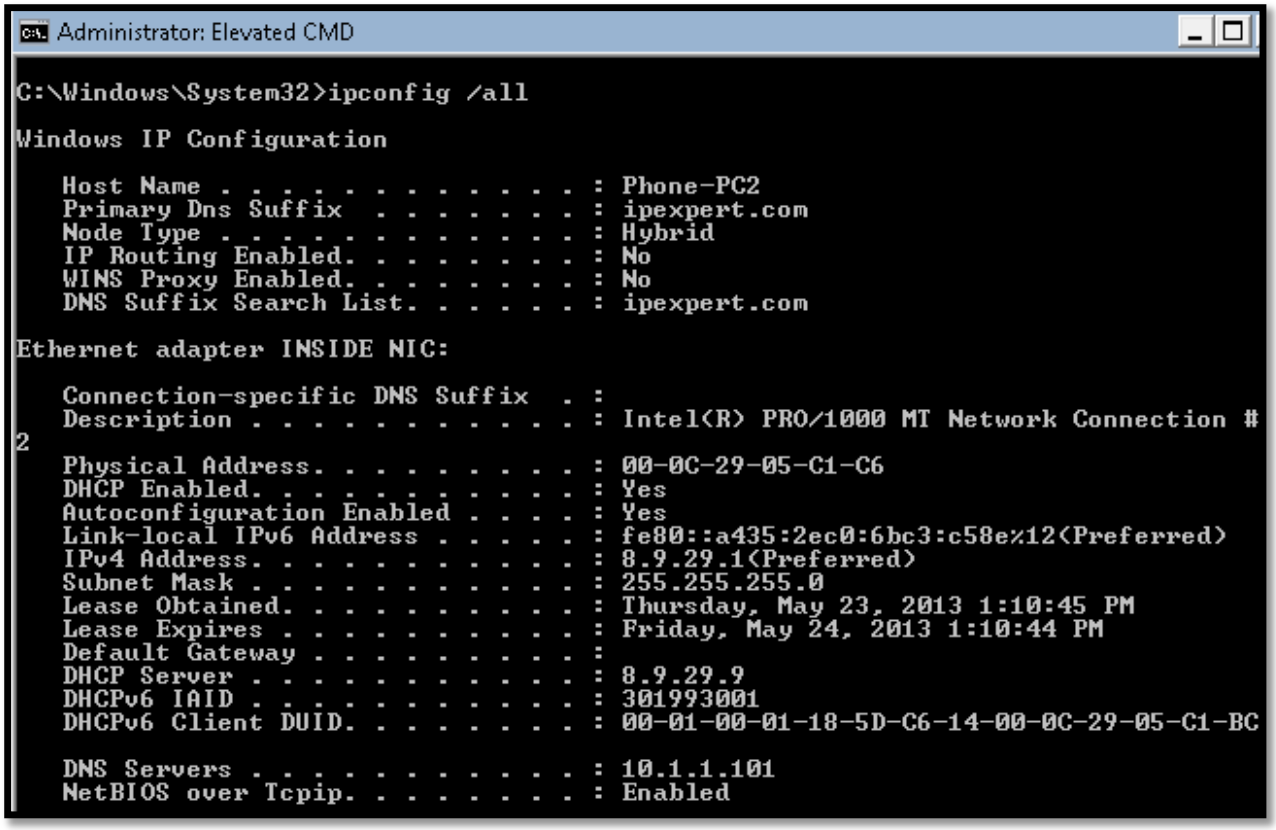
```
   CAT3#sh authen sessions int g1/0/12
               Interface:  GigabitEthernet1/0/12
             MAC Address:  000c.2905.c1c6
              IP Address:  Unknown
                  Status:  Running
                  Domain:  UNKNOWN
         Security Policy:  Should Secure
         Security Status:  Unsecure
          Oper host mode:  multi-domain
        Oper control dir:  both
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  08090782000001BC25BA3EE1
         Acct Session ID:  0x00000022
                  Handle:  0xE30001BD

   Runnable methods list:
          Method   State
          dot1x    Running
          mab      Not run

   ----------------------------------------
               Interface:  GigabitEthernet1/0/12
             MAC Address:  001b.d4c6.1509
              IP Address:  Unknown

               User-Name:  00-1B-D4-C6-15-09
                  Status:  Authz Success
                  Domain:  VOICE
         Security Policy:  Should Secure
         Security Status:  Unsecure
```

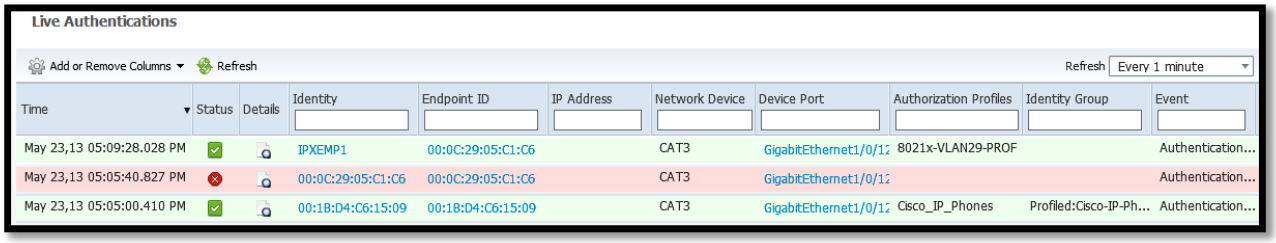
```
          Oper host mode:  multi-domain
        Oper control dir:  both
           Authorized By:  Authentication Server
             Vlan Policy:  N/A
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  08090782000001B125B1D987
         Acct Session ID:  0x00000017
                  Handle:  0xC20001B2

   Runnable methods list:
          Method   State
          dot1x    Failed over
          mab      Authc Success
```

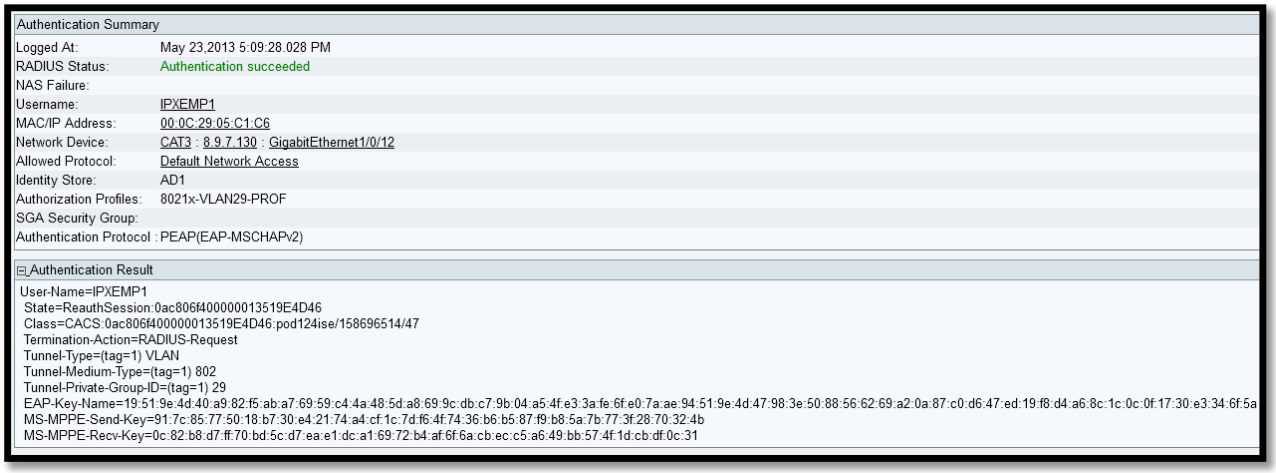
Now when you connect to TEST PC#2 you should be able to see AnyConnect Authentication Prompt. You may need to create AnyConnect Profile for 802.1x if not already available for selection. After successful authentication user should be assigned to VLAN 29 and obtain an IP address via DHCP :

```
   CAT3#sh authen sessions int g1/0/12
               Interface:  GigabitEthernet1/0/12
             MAC Address:  000c.2905.c1c6
              IP Address:  Unknown
               User-Name:  IPXEMP1
                  Status:  Authz Success
                  Domain:  DATA
          Security Policy:  Should Secure
          Security Status:  Unsecure
           Oper host mode:  multi-domain
         Oper control dir:  both
            Authorized By:  Authentication Server
              Vlan Policy:  29
          Session timeout:  N/A
             Idle timeout:  N/A
        Common Session ID:  08090782000001C125BE28AA
          Acct Session ID:  0x00000027
                   Handle:  0x5C0001C2

   Runnable methods list:
          Method   State
```

```
        dot1x     Authc Success
        mab       Not run

----------------------------------------

             Interface:  GigabitEthernet1/0/12
           MAC Address:  001b.d4c6.1509
            IP Address:  Unknown
             User-Name:  00-1B-D4-C6-15-09
                Status:  Authz Success
                Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  08090782000001B125B1D987
      Acct Session ID:  0x00000017
               Handle:  0xC20001B2

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```







Authentication Details	
Logged At:	May 23,2013 5:09:28.028 PM
Occurred At:	May 23,2013 5:09:28.027 PM
Server:	pod124ise
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
Username:	IPXEMP1
RADIUS Username :	anonymous
Calling Station ID:	00:0C:29:05:C1:C6
Framed IP Address:	
Use Case:	
Network Device:	CAT3
Network Device Groups:	Device Type#All Device Types,Location#All Locations
NAS IP Address:	8.9.7.130
NAS Identifier:	
NAS Port:	50112
NAS Port ID:	GigabitEthernet1/0/12
NAS Port Type:	Ethernet
Allowed Protocol:	Default Network Access
Service Type:	Framed
Identity Store:	AD1
Authorization Profiles:	8021x-VLAN29-PROF
Active Directory Domain:	IPEXPERT.COM
Identity Group:	
Allowed Protocol Selection Matched Rule:	Dot1X-Auth-Policy
Identity Policy Matched Rule:	Default
Selected Identity Stores:	AD1
Authorization Policy Matched Rule:	Wired 802.1x AuthZ Rule

Task 5.3: Basic Wireless (3 Points)

- Initialize WLC with the following information :
  - Administrator name MUST be “admin” and password “IPexpert123”
  - SSID IPX-XXX where XXX is your pod number
  - Management IP address should be 10.1.1.250
  - Virtual Gateway IP should be 1.250.250.250

  - Set User Mobility/RF Group name “RFGROUPXXX” where XXX is your pod number
  - Use NTP Server 10.1.1.101
- Create a wireless network “IPX-EMP-XXX” where XXX is your pod number
- This WLAN should map to VLAN 29 and require 802.1x authentication
- Also enable WPA2 encryption (AES) and CCKM Fast Secure Roaming
- AP should obtain an IP address from the C1 ASA

Detailed Solution

CAT2

```
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
```

CAT4

```
interface GigabitEthernet1/0/13
 switchport trunk encap dot1q
 switchport trunk allowed vlan 29,100
 sw mode trunk
 spanning-tree portfast trunk
```

ASA C1

```
dhcpd address 10.1.1.80-10.1.1.90 inside
dhcpd enable inside
```

WLC

Clear WLC config if needed (“reset system”) and Initialize it from the CLI :

```
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
```

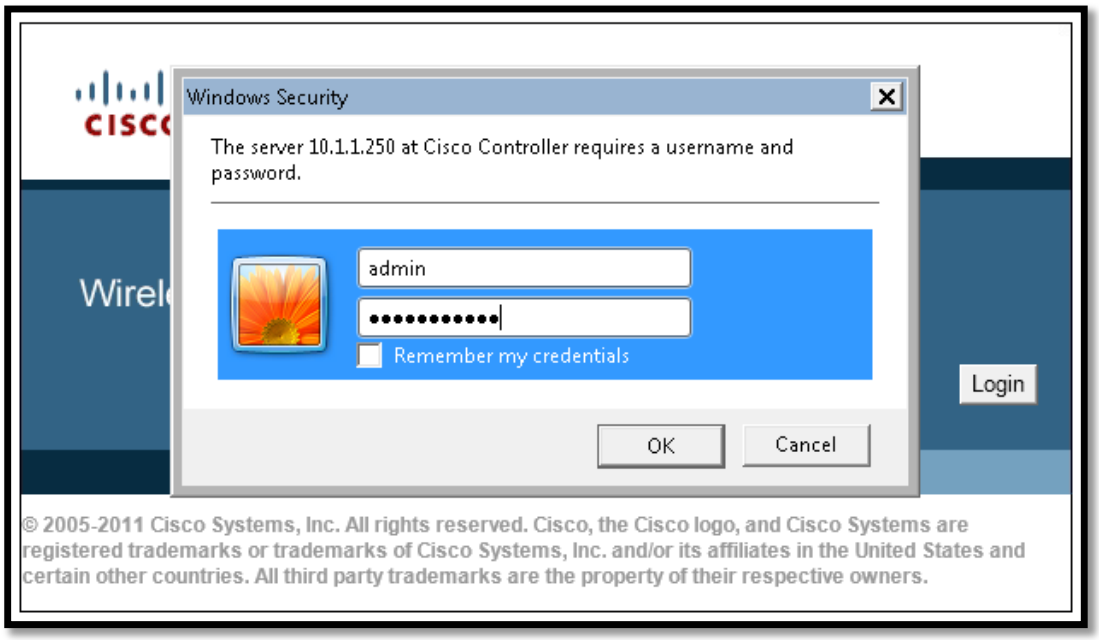
```
Would you like to terminate autoinstall? [yes]:

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 :

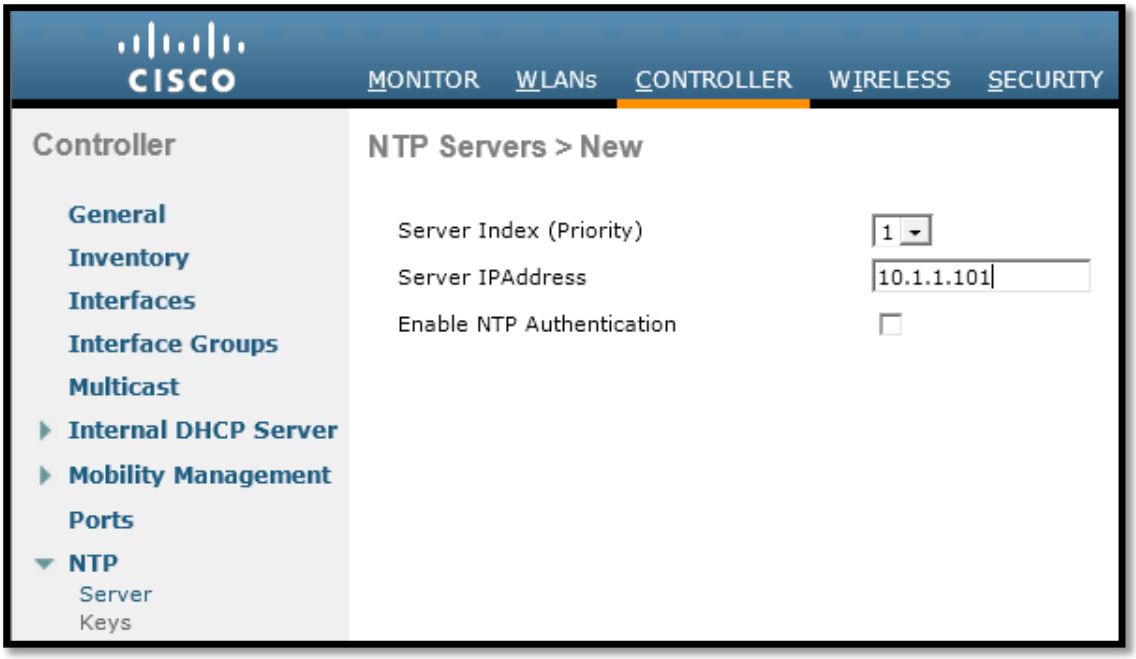
```
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): IPexpert123
Re-enter Administrative Password                  : IPexpert123

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: 10.1.1.1

Virtual Gateway IP Address: 1.250.250.250
route: SIOC[ADD|DEL]RT: File exists

Mobility/RF Group Name: RFGROUP124
Network Name (SSID): IPX-124

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]: PL

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...
```

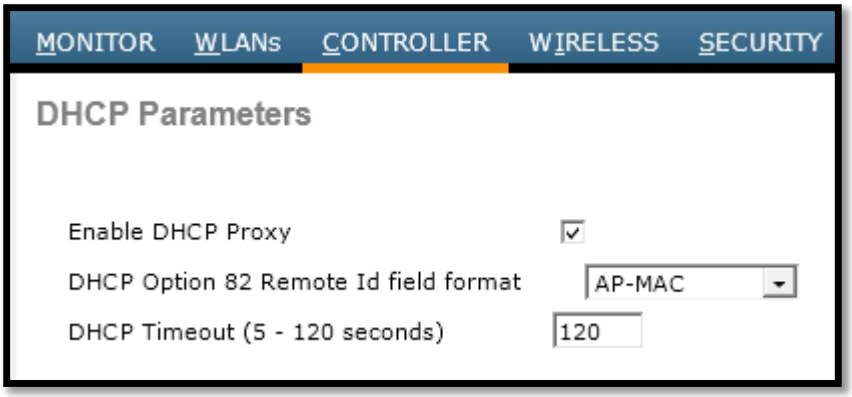
Login to the Controller using HTTPs :



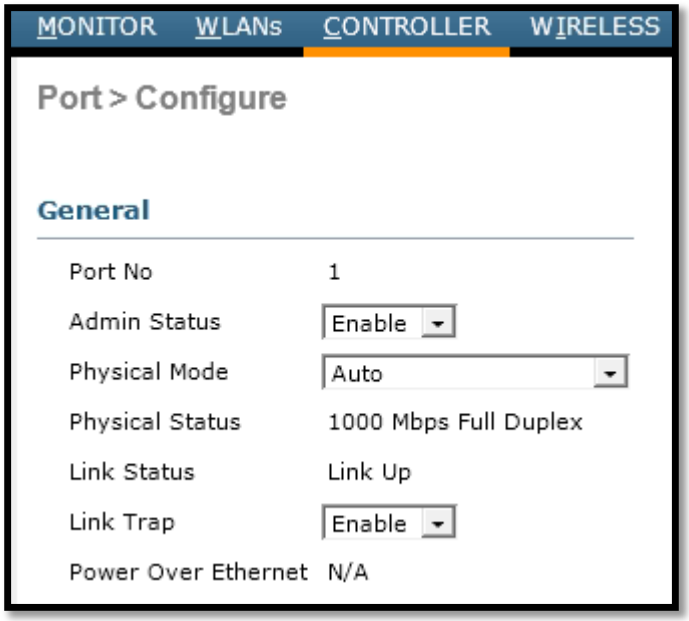
Now configure NTP under “Controller” :

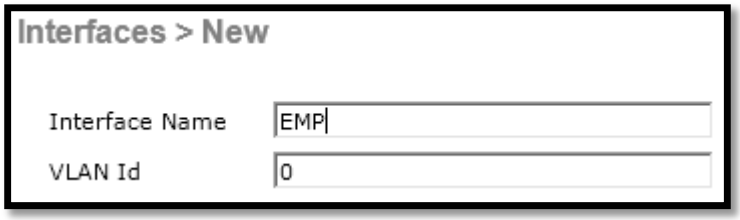


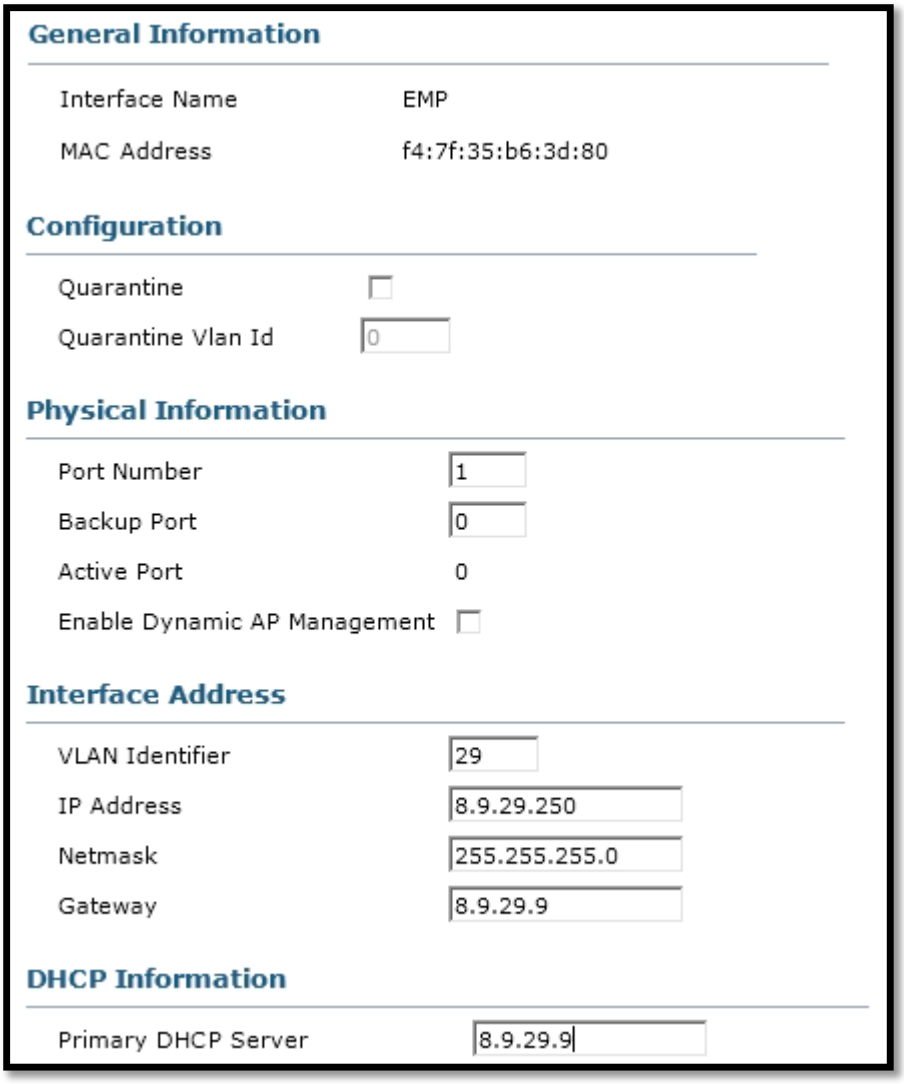
Also make sure "DHCP Proxy" is enabled under Controller -> Advanced -> DHCP :



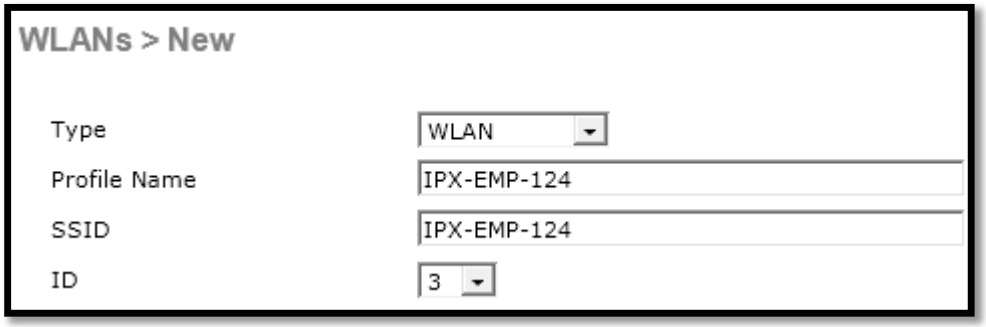
Now the interfaces – we want to check if the physical port is up (Controller -> Ports) and then create interfaces for WLANs (Controller -> Interfaces) :



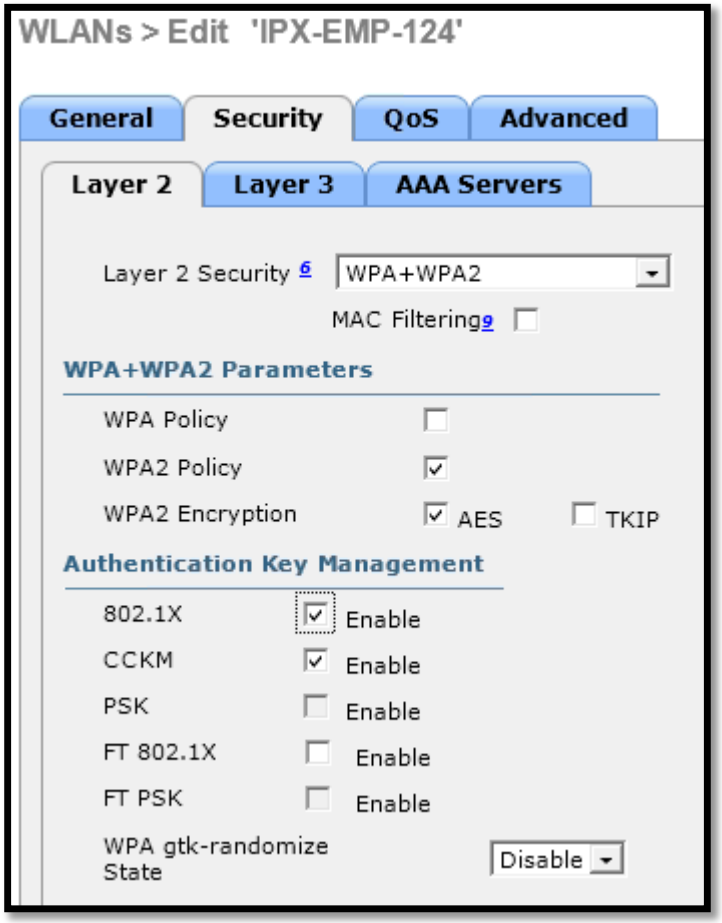




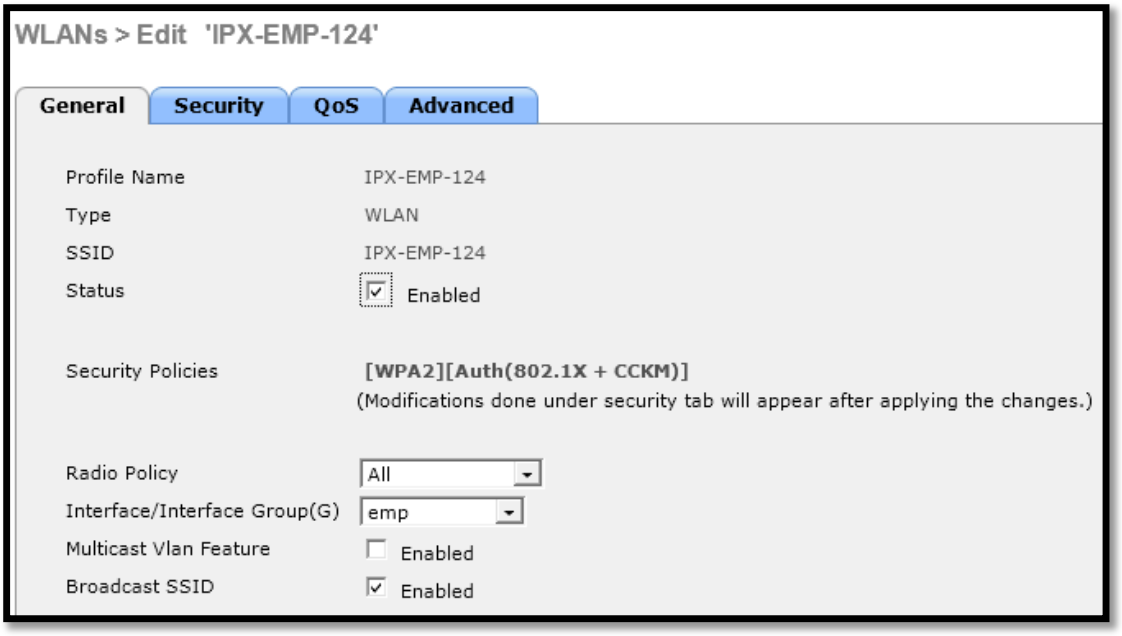
Now add a new WLAN :



And configure Security settings as needed :



Don’t forget to enable the WLAN :



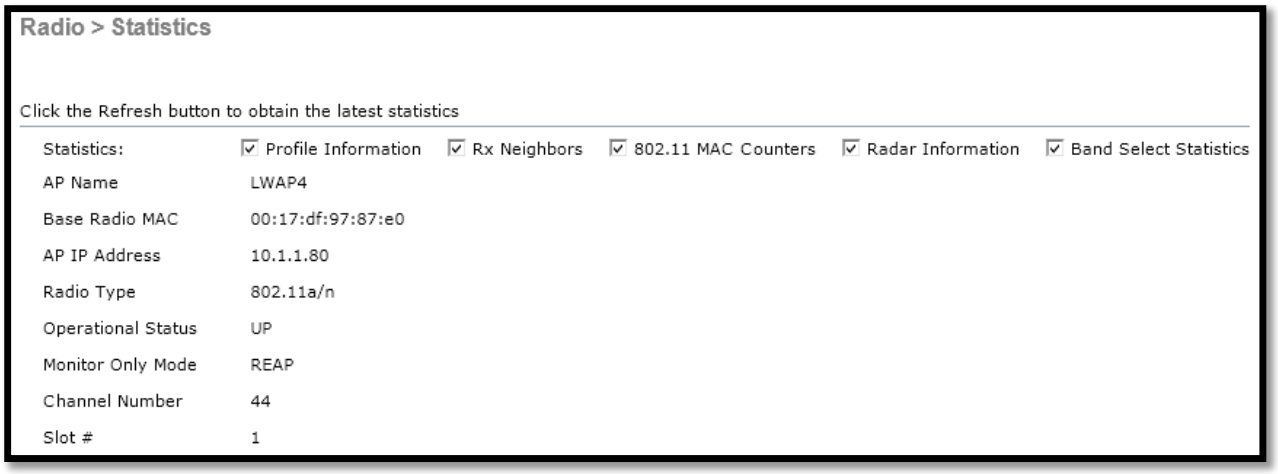
You were not explicitly asked to configure wireless 802.1x or use a RADIUS server so don't do it.

Verification

Verification for this task is only partial since we were not asked to configure 802.1x and RADIUS. First make sure AP joined the Controller :

```
ASA3/C1/act(config)# sh dhcpd binding all

IP address       Client Identifier        Lease expiration        Type

      10.1.1.80    0100.1873.cfef.0e            3488 seconds    Automatic


 (Cisco Controller) >show ap summ

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model              Ethernet MAC
Location          Port  Country  Priority
------------------  -----  -------------------  -----------------  ------
----------  ----  -------  ------
```

```
LWAP4                2     AIR-LAP1242AG-A-K9    00:18:73:cf:ef:0e
default location  1        US       1
```



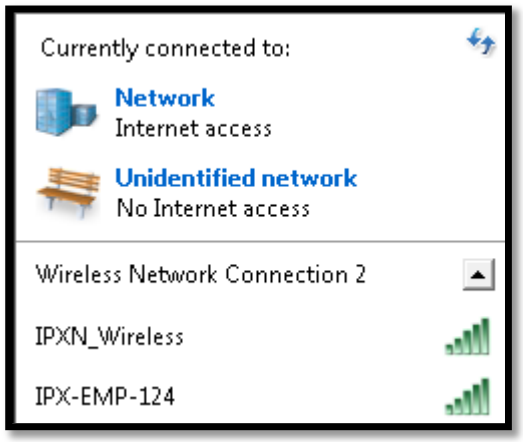
Verify if the WLC synchronized to the NTP server :

```
 (Cisco Controller) >show time

Time..................................... Thu May 23 21:41:45 2013

Timezone delta.................................. 0:0
Timezone location..............................
NTP Servers
    NTP Polling Interval.....................     3600

     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
--
       1              0          10.1.1.101       AUTH DISABLED
```

Then make sure you can see the WLAN :

```
 (Cisco Controller) >show wlan summary

Number of WLANs................................. 2

WLAN ID  WLAN Profile Name / SSID              Status    Interface Name
```

```
-------  ------------------------------------  --------  ----------------
----
1        IPX-124 / IPX-124                     Enabled   management
2        IPX-EMP-124 / IPX-EMP-124               Enabled   emp
```



6.0 Advanced Security (9 points)

Task 6.1: CPPr (3 Points)

- Configure early dropping of packets that are directed toward closed or non-listened TCP/UDP ports on R6
- Ensure ISAKMP packets are not affected
- Limit the total number of BGP and Telnet packets allowed in the control-plane input queue to 100

Detailed Solution

R6

```
class-map type queue-threshold match-any CPPR_Q_CLASS
 match  protocol bgp
 match  protocol telnet

class-map type port-filter match-all CPPR_PF_CLASS
 match  closed-ports
 match not  port udp 500
 match not  port udp 4500

policy-map type queue-threshold CPPR_Q_POL
 class CPPR_Q_CLASS
   queue-limit 100

policy-map type port-filter CPPR_PF_POL
 class CPPR_PF_CLASS
   drop

control-plane host
 service-policy type port-filter input CPPR_PF_POL
 service-policy type queue-threshold input CPPR_Q_POL
```

In some older IOS versions ISAKMP was not automatically detected by the CPPr. If you had matched only the closed ports it would have dropped all incoming ISAKMP packets.

Watch out for wording – total number of BGP and Telnet packets means that they should be configured in the same class-map (match-any) which does not necessarily has to make sense. It is just to test your attention to details.

Verification

```
R6#sh control-plane host features
Control plane host path features :

------------------------------------------------------
TCP/UDP Portfilter activated May 24 2013 10:2
Protocol Queue Thresholding activated May 24 2013 10:2

------------------------------------------------------


R6>show tech-support unpriv

------------------ show version ------------------

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

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

--- Omitted ---

R6#sh policy-map type queue-threshold control-plane host
      queue-limit 100
      queue-count 4     packets allowed/dropped 331/0
 Control Plane Host

  Service-policy queue-threshold input: CPPR_Q_POL

    Class-map: CPPR_Q_CLASS (match-any)
      331 packets, 19827 bytes
      5 minute offered rate 2000 bps, drop rate 0 bps
      Match:  protocol bgp
```

```
          6 packets, 321 bytes
          5 minute rate 0 bps
        Match:  protocol telnet
          325 packets, 19506 bytes
          5 minute rate 2000 bps

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any

R11#telnet 8.9.100.6 1234
Trying 8.9.100.6, 1234 ...

R6#sh policy-map type port-filter control-plane host
 Control Plane Host

  Service-policy port-filter input: CPPR_PF_POL

    Class-map: CPPR_PF_CLASS (match-all)
      2 packets, 120 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  closed-ports
      Match: not  port udp 500
      Match: not  port udp 4500
      drop

    Class-map: class-default (match-any)
      646 packets, 38698 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 6.2: OSPF Security (2 Points)

- Authenticate OSPFv2 adjacencies between routers R2, R5 and R6
- Use OSPF Type 2 authentication
- Protect OSPF neighbor sessions from CPU-based attacks – only accept OSPF packets if they come from the local L2 network

Detailed Solution

R2, R5, R6

```
int s0/1/0
 ip ospf ttl-security hops 1
 ip ospf authen message-digest
 ip ospf message-digest-key 1 md5 cisco
```

When OSPF TTL Security feature is enabled, a host cannot attack an OSPF session if the host is not a member of the local or remote OSPF network, or if the host is not directly connected to a network segment between the local and remote OSPF networks. This solution greatly reduces the effectiveness of Denial of Service attacks against an OSPF autonomous system.

Verification

```
R5#sh ip ospf int s0/1/0 | in TTL
  Strict TTL checking enabled

R6#sh ip ospf int s0/1/0 | s authen
  Message digest authentication enabled
    Youngest key id is 1

R2#sh ip ospf ne

Neighbor ID     Pri   State           Dead Time   Address
Interface
8.9.100.5         1   FULL/DROTHER    00:00:36    8.9.50.5
Serial0/1/0
8.9.100.6         1   FULL/DR         00:00:31    8.9.50.6
Serial0/1/0
8.9.100.9         1   FULL/DR         00:00:36    8.9.19.9
GigabitEthernet0/0
```

Task 6.3: SNMP (4 Points)

- Configure R2 for SNMP Support. Create two SNMP views – one which includes all objects in the MIB "internet" and the other which includes entire "cisco" MIB
- Create SNMP Group FULL with read/write access to the "internet" view for users in VLAN 7 only and security model allowing for encryption and authentication
- Create SNMP Group PART with read access to the "internet" view and write access to the "cisco" view. Security model for this group should allow for authentication
- LinkUp and LinkDown SNMP Traps sent to a management station in VLAN 100 (10.1.1.200) should be encrypted and authenticated using 3DES and SHA algorithms with password "cisco"
- BGP SNMP Traps sent should be authenticated using SHA algorithm with password "cisco"
- Interface indexes should remain constant after a reboot

Detailed Solution

C2

```
object network SNMPMGMT
 host 10.1.1.200
 nat (i,o) static 8.9.19.200

access-list OUTSIDE_IN permit udp host 8.9.19.2 object SNMPMGMT eq
snmptrap
```

R2

```
access-list 2 permit 8.9.7.0 0.0.0.255
snmp-server view V_CISCO cisco included
snmp-server view V_INTERNET internet included

snmp-ser gr FULL v3 priv match exact read V_INTERNET wr V_INTERNET access
2
snmp-server group PART v3 auth match exact read V_INTERNET write V_CISCO

snmp-server user USERF FULL v3 auth sha cisco priv 3des cisco
snmp-server user USERP PART v3 auth sha cisco
```

```
snmp-server ifindex persist

snmp-server enable traps snmp linkdown linkup
snmp-server enable traps bgp

snmp-server host 8.9.19.200 version 3 priv USERF  snmp
snmp-server host 8.9.19.200 version 3 auth USERP  bgp
```

SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. There are three security levels for SNMPv3 : noAuthNoPriv, authNoPriv and authPriv (this one allows for encryption).

SNMP Views are used to limit which MIB objects can be accessed by a SNMP manager. SNMP Group maps SNMP users to SNMP views. SNMP Users act as the actual passwords. The configuration steps should reflect this logic.

The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics.

Verification

```
R2#sh snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
V_CISCO cisco - included nonvolatile active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded permanent active
v1default internet.6.3.16 - excluded permanent active
v1default internet.6.3.18 - excluded permanent active
v1default ciscoMgmt.394 - excluded permanent active
v1default ciscoMgmt.395 - excluded permanent active
v1default ciscoMgmt.399 - excluded permanent active
v1default ciscoMgmt.400 - excluded permanent active
V_INTERNET internet - included nonvolatile active
*tv.00000001.00000000.00000000.00000000.000000000F iso - included volatile
active
```

```
*tv.00000001.00000000.00000000.00000000.000000000F ieee802dot11 - included
volatile active
*tv.00002000.00000000.00000000.00000000.000000000F iso - included volatile
active
*tv.00002000.00000000.00000000.00000000.000000000F ieee802dot11 - included
volatile active

R2#sh snmp user

User name: USERF
Engine ID: 800000090300001BD4A9E400
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: 3DES
Group-name: FULL

User name: USERP
Engine ID: 800000090300001BD4A9E400
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: PART

R2#sh snmp group
groupname: FULL                             security model:v3 priv
readview : V_INTERNET                       writeview: V_INTERNET
notifyview: *tv.00000001.00000000.00000000.0
row status: active      access-list: 2

groupname: ILMI                             security model:v1
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                             security model:v2c
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: PART                             security model:v3 auth
readview : V_INTERNET                       writeview: V_CISCO
```

```
notifyview: *tv.00002000.00000000.00000000.0
row status: active


R2#sh snmp mib ifmib ifindex det
Description                    ifIndex  Active  Persistent  Saved
TrapStatus
-------------------------------------------------------------------------
-----

GigabitEthernet0/1              2       yes     enabled      yes
enabled
Serial0/1/0                     3       yes     enabled      yes
enabled
Async0/2/0                      8       no      enabled      yes  n/a
VoIP-Null0                      5       yes     enabled      yes
enabled
Tunnel100                       11      yes     enabled      yes
enabled
Loopback0                       9       yes     enabled      yes
enabled
Null0                           6       yes     enabled      yes
enabled
Loopback256                     10      yes     enabled      yes
enabled
Serial0/2/0                     4       yes     enabled      yes
enabled
GigabitEthernet0/0              1       yes     enabled      yes
enabled
Async0/1/0                      7       no      enabled      yes  n/a
```

Now enable “debug snmp packet” and clear BGP peerings :

```
R2#debug snmp packet
SNMP packet debugging is on

R2#clear ip bgp *

*May 24 11:29:42.124: SNMP: Queuing packet to 8.9.19.200
*May 24 11:29:42.124: SNMP: V2 Trap, reqid 106, errstat 0, erridx 0
 sysUpTime.0 = 69329721
 snmpTrapOID.0 = bgpTraps.2
```

```
 bgpPeerEntry.14.8.9.100.1 = 00 00
 bgpPeerEntry.2.8.9.100.1 = 1
*May 24 11:29:42.148: SNMP: Queuing packet to 8.9.19.200

R2#sh snmp | s logging
SNMP logging: enabled
    Logging to 8.9.19.200.162, 0/10, 35 sent, 41 dropped.


ASA3/C1/act(config)# sh access-list | in snmptrap
access-list OUTSIDE_IN line 5 extended permit udp host 8.9.19.2 object
SNMPMGMT eq snmptrap (hitcnt=0) 0x935e85f4
  access-list OUTSIDE_IN line 5 extended permit udp host 8.9.19.2 host
10.1.1.200 eq snmptrap (hitcnt=1) 0x935e85f4
```

7.0 Attack Mitigation (8 points)

Task 7.1: RTBH (4 Points)

- You have detected a DoS attack coming from AS 11 (99.99.99.11)
- Attacks are targeted at subnet 5.5.5.0/24 which is part of your AS 256
- Use BGP to stop this activity at the edge of your AS
- Ensure legitimate clients can still access the services provided by devices in 5.5.5.0/24
- Treat R6 as the main controlling device
- You can use 3 static routes to complete this task

Detailed Solution

R6

```
ip route 192.0.2.1 255.255.255.255 null 0

route-map BLACKHOLE permit 10
 match tag 999
 set local-preference 200
 set origin igp
 set community no-export
 set ip next-hop 192.0.2.1

router bgp 256
 redistribute static route-map BLACKHOLE
 neighbor 8.9.100.2 send-community
```

Trigger Route :

```
ip route 99.99.99.11 255.255.255.255 192.0.2.1 tag 999
```

R2

```
ip route 192.0.2.1 255.255.255.255 null 0

int g0/0
```

```
 ip verify unicast source reachable-via any

router bgp 256
 neighbor 8.9.100.5 send-community
R5
ip route 192.0.2.1 255.255.255.255 null 0
```

Don't forget to enable sending BGP communities to the peers. Otherwise the injected prefix gets propagated to other (neighboring) ASes as well.

Verification

Generate multiple ICMP Echos from R1's loopback 99 towards 5.5.5.5. Then at some point configure the trigger route on R6 :

```
R1#ping 5.5.5.5 so loop99 rep 20000000

Type escape sequence to abort.
Sending 20000000, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 99.99.99.11
...........!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.................................


R2#sh ip traffic | s drop
         6471 no route, 160 unicast RPF, 0 forced drop
  Queue drops: 0
  Queue drops: 0

R2#sh ip int g0/0 | s IP verify
  IP verify source reachable-via ANY
   169 verification drops
   26 suppressed verification drops
   0 verification drop-rate

R2#sh ip bgp
BGP table version is 15, local router ID is 8.9.100.2
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
*>i5.5.5.0/24       8.9.100.5                0    100      0 i
*> 99.99.99.0/24    8.9.100.1                0             0 11 i
*>i99.99.99.11/32   192.0.2.1                0    200      0 i


R2#sh ip bgp 99.99.99.11
BGP routing table entry for 99.99.99.11/32, version 15
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
  Advertised to update-groups:
     11
  Local, (Received from a RR-client)
    192.0.2.1 from 8.9.100.6 (8.9.100.6)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      Community: no-export

R2#sh ip cef 192.0.2.1
192.0.2.1/32
  attached to Null0
```

Note the BGP information about attacker is not advertised to the neighboring AS :

```
R2#sh ip bgp neighbors 8.9.100.1 advertised-routes
BGP table version is 11, local router ID is 8.9.100.2
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
*>i5.5.5.0/24       8.9.100.5                0    100      0 i
```

Also “legitimate” devices from AS11 are still able to reach 5.5.5.5 (add secondary IP on loopback99 on R2 for testing) :

```
R1#ping 5.5.5.5 so 99.99.99.11 rep 20000000

Type escape sequence to abort.
Sending 20000000, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 99.99.99.11
........

R1#ping 5.5.5.5 so 99.99.99.200 rep 20000000

Type escape sequence to abort.
Sending 20000000, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 99.99.99.200
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!.
```

Task 7.2: IPv6 Attacks (4 Points)

- R5 should drop IPv6 fragments coming from the FR cloud
- Configure R10's g0/0 interface so the router is always capable of properly dealing with IPv6 fragments
- If more than 10 fragments are received for a packet or if the reassembly takes longer than 10 seconds all currently received data for the packet should be dropped
- Configure ASA C2 to drop & log IPv6 packets with RH Type 0
- All other RHs should be allowed and logged

Detailed Solution

R5

```
ipv6 access-list NO_FRAGS
 deny ipv6 any any fragments
 permit ipv6 any any
```

```
int s0/1/0
 ipv6 traffic-filter NO_FRAGS in
```

R10

```
int g0/0
 ipv virtual-reassembly in max-fragments 10 timeout 10
```

C2

```
policy-map type inspect ipv6 NO_RH0
 parameters
 no match header routing-type range 1 255
 match header routing-type eq 0
  drop log
 match header routing-type range 1 255
  log

policy-map global_policy
 class class-default
  inspect ipv6 NO_RH0
```

When you selectively block some traffic in an ACL never forget to permit all the rest so other tasks will not get broken.

Verification

Send some large ICMPv6 Echos to R10 from R6 :

```
R6#ping 2951::10 size 1501

Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 2951::10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R6#ping 2951::10 size 1499

Type escape sequence to abort.
```

```
Sending 5, 1499-byte ICMP Echos to 2951::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 428/429/432 ms

R5#sh ipv access-l
IPv6 access list NO_FRAGS
    deny ipv6 any any fragments (5 matches) sequence 10
    permit ipv6 any any (35 matches) sequence 20
```

Now few large packets from R5 so they the fragments don't get dropped on S0/1/0 :

```
R5#ping 2951::10 size 1501

Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 2951::10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/4 ms

R10#sh ipv virtual-reassembly g0/0
%Interface GigabitEthernet0/0 [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 64
   IPv6 configured fragments per reassembly (max-fragments): 10
   IPv6 configured reassembly timeout (timeout): 10 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:5
   IPv6 total reassembly timeout count:0
```

Finally use IPv6 traceroute to test the RH0 EH :

```
R11#traceroute ipv
Target IPv6 address: 2906::6
Source address:
Insert source routing header? [no]: yes
Nexthop address: 2906::6
Nexthop address:
Numeric display? [no]:
```

```
Timeout in seconds [3]: 1
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]: 3
Priority [0]:
Port Number [0]:
Type escape sequence to abort.
Tracing the route to 2906::6

  1  *  *  *
  2  *  *  *
  3  *  *  *
Destination not found inside max hopcount diameter.

ASA3/C2/act(config)#
May 24 2013 14:10:03: %ASA-4-325004: IPv6 Extension Header routing-type
denied and logged by configuration. UDP from inside:2907::11/63407 to
outside:2906::6/33434
May 24 2013 14:10:04: %ASA-4-325004: IPv6 Extension Header routing-type
denied and logged by configuration. UDP from inside:2907::11/53136 to
outside:2906::6/33435

ASA3/C2/act(config)# sh service-pol global inspect ipv6

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: class-default
      Inspect: ipv6 NO_RH0, packet 2114, lock fail 0, drop 9, reset-drop 0
        params verify-header type fails 0
        params verify-header order fails 0
        match header routing-type
          drop, packet 9
          log, packet 9
```

Lab 3

Please look at the provided diagrams and read through the whole lab before you start. Read the directions very carefully to make sure you are doing what is being asked of you. This concept is very important when you take the CCIE lab administered by Cisco

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

- 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: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device

NOTE: Unless explicitly prohibited in a section, you may permit ICMP for connectivity testing

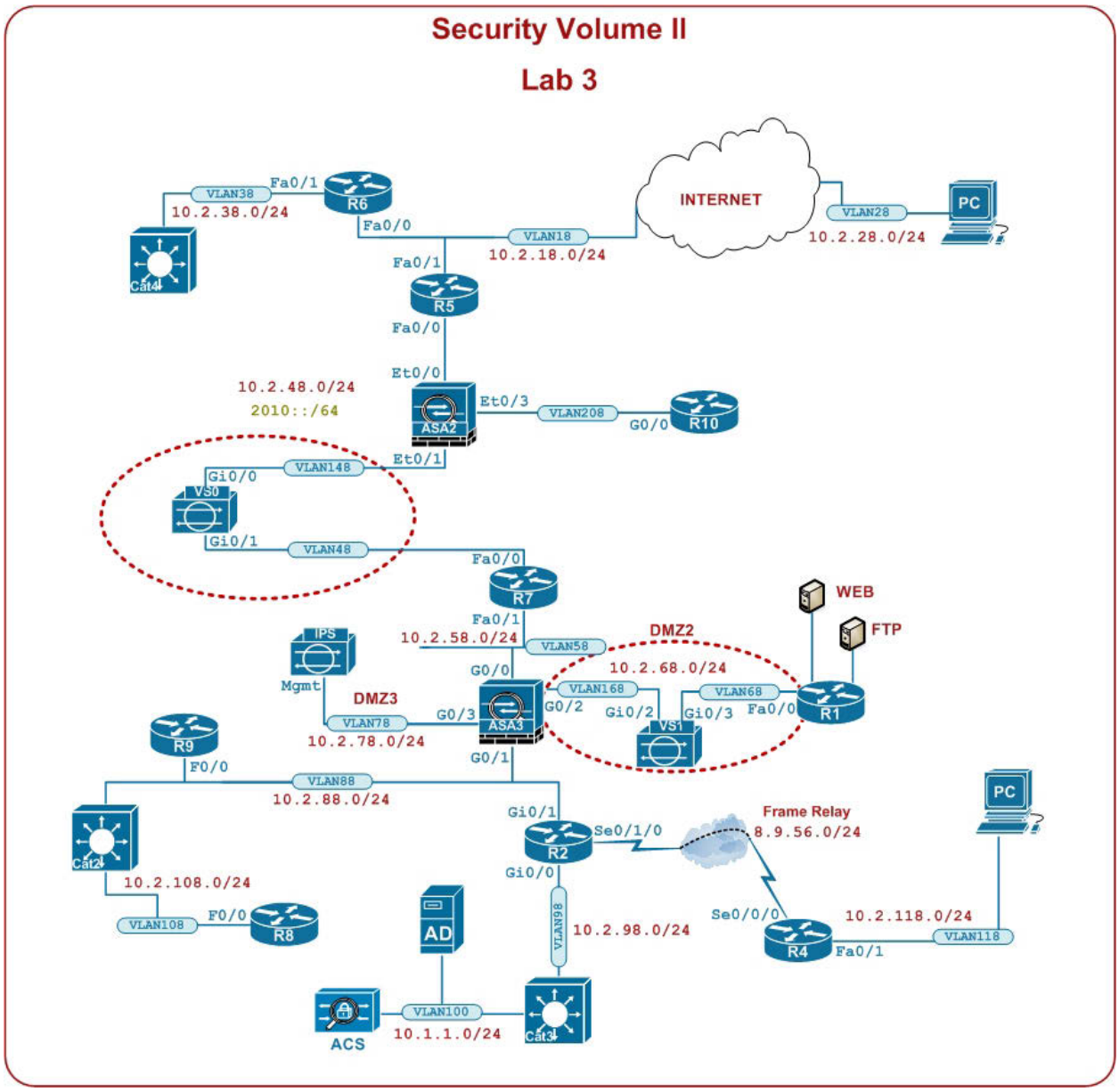
Estimated Time to Complete: **10 Hours**

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	FastEthernet0/0	68	10.2.68.1/24
	Loopback0		10.10.10.1/32
	Loopback12		10.3.68.1/24
	Loopback11		11.11.11.11/24
R2	GigabitEthernet0/0	98	10.2.98.2/24
	GigabitEthernet0/1	88	10.2.88.2/24
	Serial0/1/0.2		8.9.56.2/24
	Loopback0		22.22.22.22/32
	Loopback1		2.2.2.2/32
R4	FastEthernet 0/1	118	10.2.118.4/24
	Loopback0		44.44.44.44/32
	Serial0/0/0.2		8.9.56.4/24
R5	FastEthernet 0/0	158	10.2.48 5/24 2010::5/64
	FastEthernet 0/1	18	10.2.18.5/24
	Loopback0		55.55.55.55/32
	Loopback1		52.52.52.52/32
R6	FastEthernet 0/0	18	10.2.18.6/24
	FastEthernet 0/1	38	10.2.38.6/24
	Loopback0		66.66.66.66/24
R7	FastEthernet 0/0	48	10.2.48.7/24 2010::7/64
	FastEthernet 0/1	58	10.2.58.7/24
	Loopback0		77.77.77.77/32
R8	FastEthernet 0/0	108	10.2.108.8/24
R9	FastEthernet 0/0	88	10.2.88.9/24
R10	Gig 0/0	48	10.2.48.10/24 2010::10/64
CAT4	VLAN38		10.2.38.24/24
CAT2	VLAN88	88	10.2.88.22/24
	VLAN108	108	10.2.108.22/24
CAT3	VLAN98	98	10.2.98.23/24
	VLAN100	100	10.1.1.1/24
ASA2	Ethernet0/0 (outside)	158	
	Ethernet0/1 (inside)	148	
	Ethernet0/3 (DMZ)	208	
ASA3	Gig0/0 (outside)	58	10.2.58.30/24
	Gig0/1 (inside)	88	10.2.88.30/24
	Gig0/2 (DMZ2)	168	10.2.68.30/24
	Gig0/3 (DMZ3)	78	10.2.78.30/24
IPS	Management	78	10.2.78.15/24
ACS		100	10.1.1.100/24
AD		100	10.1.1.101/24



Solutions

1.0 ASA Firewalls (16 points)

Task 1.1: ASA2 Configuration (4 Points)

- Configure ASA2 according to the IP addressing table and the diagram
- Configure the host name to be ASA2
- Enable ARP inspection on outside interface and specify that packets that do not exactly match a static ARP entry are dropped
- Configure ACLs so that any ICMP & ICMPv6 traffic is permitted through the ASA
- Ensure you are able to ping between routers R5, R7 and R10
- Ensure EIGRP and OSPFv3 adjacencies come up

NOTICE: this question 1.1 depends on the configuration of Question 3.1 "Cisco IPS section" which requires configuration of Cisco IPS inline on the inside network as shown in diagram.

Detailed Solution

CAT4

```
interface GigabitEthernet1/0/6
 switchport access vlan 158
 switchport mode access
 spanning-tree portfast
```

R10

```
key chain ipexpert
 key 1
  key-string ipexpert

int g0/0
 ip authentication mode eigrp 55 md5
```

```
 ip authentication key-chain eigrp 55 ipexpert
 ipv add fe80::10 link-local
```

R5

```
int f0/0
 ipv add fe80::5 link-local
```

R7

```
int f0/0
 ipv add fe80::7 link-local
```

ASA2

```
firewall transparent
hostname ASA2

interface Ethernet0/0
 nameif outside
 bridge-group 1
 security-level 0

interface Ethernet0/1
 nameif inside
 bridge-group 1
 security-level 100

interface Ethernet0/3
 nameif DMZ
 bridge-group 1
 security-level 50

interface BVI1
 ip address 10.2.48.20 255.255.255.0
 ipv add 2010::20/64

access-list OUTSIDE_IN extended permit icmp any any
access-list OUTSIDE_IN extended permit eigrp host 10.2.48.5 host
224.0.0.10
access-list OUTSIDE_IN extended permit eigrp host 10.2.48.5 host 10.2.48.7
```

```
access-list OUTSIDE_IN extended permit eigrp host 10.2.48.5 host
10.2.48.10
access-list INSIDE_IN extended permit ip any any

access-list DMZ_IN extended permit icmp any any
access-list DMZ_IN extended permit eigrp host 10.2.48.10 host 224.0.0.10
access-list DMZ_IN extended permit eigrp host 10.2.48.10 host 10.2.48.5
access-list DMZ_IN extended permit eigrp host 10.2.48.10 host 10.2.48.7

ipv6 access-list DMZ6_IN permit ospf any host ff02::5
ipv6 access-list DMZ6_IN permit ospf any host ff02::6
ipv6 access-list DMZ6_IN permit icmp6 any any
ipv6 access-list DMZ6_IN permit ospf any host fe80::5
ipv6 access-list DMZ6_IN permit ospf any host fe80::7

ipv6 access-list OUTSIDE6_IN permit icmp6 any any
ipv6 access-list OUTSIDE6_IN permit ospf any host ff02::5
ipv6 access-list OUTSIDE6_IN permit ospf any host ff02::6
ipv6 access-list OUTSIDE6_IN permit ospf any host fe80::10
ipv6 access-list OUTSIDE6_IN permit ospf any host fe80::7

ipv6 access-list INSIDE6_IN permit ip any any

access-group OUTSIDE_IN in interface outside
access-group OUTSIDE6_IN in interface outside
access-group INSIDE_IN in interface inside
access-group INSIDE6_IN in interface inside
access-group DMZ_IN in interface DMZ
access-group DMZ6_IN in interface DMZ

arp inside 10.2.48.7 001b.d517.ba88
arp outside 10.2.48.5 001b.d50f.f2f8
arp DMZ 10.2.48.10 30e4.dbce.8490

arp-inspection outside enable no-flood
```

Since the IP & IPv6 addresses were not given to you, you could choose whatever you want as long as they don't interfere with what's already assigned in this segment.

The VLAN number and authentication key were derived by looking at the configuration of other devices (switchport connected to R5) and authentication settings configured on R5/R7.

It is always a good idea to check the Layer 2 configuration especially when trunks are used on the ASA.

MAC addresses for ARP inspection will be probably different in your case – they depend on pod number used for this lab. Make sure to put the correct ones.

Verification

```
R10#sh ip eigrp ne
EIGRP-IPv4 Neighbors for AS(55)
H   Address                 Interface              Hold Uptime   SRTT
RTO  Q  Seq
                                                   (sec)     (ms)       Cnt
Num
0   10.2.48.5               Gi0/0                  12 00:07:55    3   100  0
22

R5#sh ipv ospf ne

Neighbor ID     Pri   State           Dead Time   Interface ID
Interface
10.2.48.10        1   FULL/BDR        00:00:38    3
FastEthernet0/0

R5#ping 2010::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/8 ms

R10#ping 10.2.48.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
ASA2(config)# sh arp
        outside 10.2.48.5 001b.d50f.f2f8 -
        inside 10.2.48.7 001b.d517.ba88 -
        DMZ 10.2.48.10 30e4.dbce.8490 –

ASA2(config)# sh mac-address-table
interface                   mac  address          type      Age(min)
bridge-group
-------------------------------------------------------------------------
---------
DMZ                         0007.7dbc.c689          dynamic      2
1
inside                      0007.7dbc.c687          dynamic      2
1
outside                     0007.7dbc.c686          dynamic      2
1
DMZ                         30e4.dbce.8490          static
1
inside                      001b.d517.ba88          static
1
outside                     001b.d50f.f2f8          static
1
```

Task 1.2: ASA3 Setup (4 Points)

- Configure ASA3 according to the IP addressing table below and the diagram above
- Configure the host name to be ASA3
- Configure ACLs so that any ICMP traffic is permitted on any interface through the ASA
- You must configure an inbound access-list for inside interface (specific)
- Configure OSPF area 50 on inside interface
- You must authenticate OSPF neighbors using MD5 with key “1” and the password “ipexpert”
- Configure EIGRP AS 55 on ASA2 on the outside interface
- You must authenticate EIGRP neighbors using MD5 and the password “ipexpert”
- Ensure you are able to ping R6 from ASA3
- Ensure that you are able to ping R6 from R1, R2 and IPS

NOTICE: this question 1.1 depends on the configuration of Question 3.1 "Cisco IPS section" which requires configuration of Cisco IPS inline on the inside network as shown in diagram

AS A3	10.2.58.3 0/24	outs ide	0
AS A3	10.2.78.3 0/24	DM Z3	60
AS A3	10.2.68.3 0/24	DM Z2	50

AS A3	10.2.88.3 0/24	e insid	0 10

Detailed Solution

ASA3

```
hostname ASA3

interface G0/0
 nameif outside
 security-level 0
 ip address 10.2.58.30 255.255.255.0
 authentication key eigrp 55 ipexpert key-id 1
 authentication mode eigrp 55 md5
 no sh

interface G0/1
 nameif inside
 security-level 100
 ip address 10.2.88.30 255.255.255.0
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest
 no sh

interface G0/2
 nameif DMZ2
 security-level 50
 ip address 10.2.68.30 255.255.255.0
 no sh

interface G0/3
 nameif DMZ3
```

```
 security-level 60
 ip address 10.2.78.30 255.255.255.0
 no sh

access-list OUTSIDE_IN permit icmp any any
access-list INSIDE_IN permit icmp any any
access-list DMZ2_IN permit icmp any any
access-list DMZ3_IN permit icmp any any

access-group OUTSIDE_IN in interface outside
access-group INSIDE_IN in interface inside
access-group DMZ2_IN in interface DMZ2
access-group DMZ3_IN in interface DMZ3

router eigrp 55
 no auto-summary
 network 10.2.58.0 255.255.255.0

router ospf 1
 network 10.2.88.0 255.255.255.0 area 50
```

Pretty straightforward configuration. Note some things we will not be able to verify at this point.

Verification

```
ASA3(config)# sh ei ne
EIGRP-IPv4 neighbors for process 55
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
0   10.2.58.7               Gi0/0            12  00:04:24 4    200   0   5

ASA3(config)# sh ospf ne


Neighbor ID     Pri   State           Dead Time   Address
Interface
```

```
22.22.22.22       1   FULL/DR         0:00:39     10.2.88.2       inside
```

Task 1.3: NAT (4 Points)

- A web server (10.3.68.1) is configured on loopback 2 of R1. Configure ASA3 such that the server is seen on the outside interface of ASA3 as 10.2.58.1
- On the same server IP address an telnet service is also running on port 3021, configure ASA3 such that incoming telnet traffic (port 23) is redirected to the telnet server on port 3021
- Configure ASA3 to translate 10.2.108.0/24 network behind the outside interface of ASA3
- Configure static translation on ASA3 for ACS server (10.1.1.100) to 10.2.58.100 on the outside network
- Verify that CAT2 can ping the original IP address of ACS server from its interface VLAN108
- Configure ASA3 such that R1 for its interface F0/0, R2 for its interface Gi0/1 and R4 for its interface s0/0/0.2 are not translated when they connect to R7 on interface F0/1, but are translated respectively to 10.2.58.31, 10.2.58.32 and 10.2.58.34 for all others outside destinations
- You are authorized to add two static routes on the ASA to achieve this task
- To test ping reachability from CAT2 to ACS server you are allowed to add a static route on the ACS

Detailed Solution

ACS

```
ip route 10.2.0.0 255.255.0.0 gat 10.1.1.1
```

ASA2

```
access-list OUTSIDE_IN permit tcp any host 10.2.58.1 eq www
access-list OUTSIDE_IN permit tcp any host 10.2.58.1 eq telnet
```

ASA3

```
route inside 10.2.108.0 255.255.255.0 10.2.88.22 1
route DMZ2 10.3.68.0 255.255.255.0 10.2.68.1 1

router ospf 1
 redistribute eigrp 55 subnets

router eigrp 55
```

```
 network 10.2.68.30 255.255.255.255
 redistribute static metric 1 1 255 1 1500
 redistribute ospf 1 metric 1 1 255 1 1500

same-security-traffic permit intra-interface

object network WWW
 host 10.3.68.1
object network WWW_NAT
 host 10.2.58.1

object service HTTP
 service tcp source eq www
object service TELNET
 service tcp source eq telnet
object service TELNET_3021
 service tcp source eq 3021

nat (DMZ2,outside) source static WWW WWW_NAT service HTTP HTTP
nat (DMZ2,outside) source static WWW WWW_NAT service TELNET_3021 TELNET

access-list OUTSIDE_IN extended permit tcp any host 10.3.68.1 eq www
access-list OUTSIDE_IN extended permit tcp any host 10.3.68.1 eq 3021

object network NET_108
 subnet 10.2.108.0 255.255.255.0
 nat (inside,outside) dynamic interface

object network ACS
 host 10.1.1.100
 nat (inside,outside) static 10.2.58.100



object network R7_F01
 host 10.2.58.7
object network R1_F00
 host 10.2.68.1
object network R2_G01
 host 10.2.88.2
```

```
object network R4_S0002
 host 8.9.56.4
object network R1_NAT
 host 10.2.58.31
object network R2_NAT
 host 10.2.58.32
object network R4_NAT
 host 10.2.58.34

nat (DMZ2,outside) source static R1_F00 R1_F00 dest static R7_F01 R7_F01
nat (inside,outside) source static R2_G01 R2_G01 dest static R7_F01 R7_F01
nat (inside,outside) source stat R4_S0002 R4_S0002 dest static R7_F01
R7_F01

nat (DMZ2,outside) source static R1_F00 R1_NAT
nat (inside,outside) source static R2_G01 R2_NAT
nat (inside,outside) source static R4_S0002 R4_NAT

access-list INSIDE_IN per ip host 10.2.88.2 any
access-list INSIDE_IN per ip host 8.9.56.4 any
access-list DMZ2_IN per ip host 10.2.68.1 any
```

Access-lists to authorize Web and telnet traffic need to be configured on ASA2 for the tests from R5/R6.

CAT2 has a default route to ASA3, so its traffic generated towards ACS server will make an U-turn on ASA3 inside interface to reach the ACS server. That's why it will be necessary to configure authorization for Intra-interface traffic on ASA.

In addition, a static routing configuration is needed to reach 10.2.108.0/24 network from ASA2. R2 router already knows the network 108 via a static route in the initial configuration then replies from ACS server will be allowed on their way back.

There is a lot of translations configured in this task – just know the order of rule processing for each of the NAT sections (1, 2 and 3).

Verification

Test as many things as you can, ideally all :

```
R6#telnet 10.2.58.1 23
Trying 10.2.58.1 ... Open


User Access Verification

Username: cisco
Password:
R1>sh tcp br
TCB       Local Address               Foreign Address             (state)
4AEB1DB8  10.3.68.1.3021              10.2.18.6.14697             ESTAB
R1>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:17
*514 vty 0     cisco      idle                 00:00:00 10.2.18.6

  Interface    User               Mode         Idle     Peer Address

CAT2#ping 10.2.58.7 so vlan 108

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.58.7, timeout is 2 seconds:
Packet sent with a source address of 10.2.108.22
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

pod124acs/admin# ping 10.2.18.6
PING 10.2.18.6 (10.2.18.6) 56(84) bytes of data.
64 bytes from 10.2.18.6: icmp_seq=0 ttl=251 time=9.55 ms
64 bytes from 10.2.18.6: icmp_seq=1 ttl=251 time=11.2 ms
64 bytes from 10.2.18.6: icmp_seq=2 ttl=251 time=11.1 ms
64 bytes from 10.2.18.6: icmp_seq=3 ttl=251 time=11.1 ms

--- 10.2.18.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 9.554/10.769/11.210/0.709 ms, pipe 2

CAT2#ping 10.1.1.100 so vlan 108
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
Packet sent with a source address of 10.2.108.22
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms

R1#telnet 10.2.58.7
Trying 10.2.58.7 ... Open


User Access Verification

Username: cisco
Password:

R4#telnet 10.2.58.7
Trying 10.2.58.7 ... Open


User Access Verification

Username: cisco
Password:

R2#telnet 10.2.58.7
Trying 10.2.58.7 ... Open


User Access Verification

Username: cisco
Password:
R7>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:27
*514 vty 0     cisco      idle                 00:00:00 10.2.88.2
 515 vty 1     cisco      idle                 00:00:54 8.9.56.4
 516 vty 0/0/0 cisco      idle                 00:00:43 10.2.68.1
```

Temporarily allow telnets to R6 :

```
R6(config)#line vty 0 4
R6(config-line)#no logi

R1#telnet 10.2.18.6
Trying 10.2.18.6 ... Open

R2#telnet 10.2.18.6
Trying 10.2.18.6 ... Open

R4#telnet 10.2.18.6
Trying 10.2.18.6 ... Open

R6>who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:11
 514 vty 0                 idle                 00:00:26 10.2.58.31
*515 vty 1                 idle                 00:00:09 10.2.58.34
 516 vty 2                 idle                 00:00:13 10.2.58.32


ASA3(config)# sh nat det
Manual NAT Policies (Section 1)
1 (DMZ2) to (outside) source static WWW WWW_NAT   service HTTP HTTP
    translate_hits = 0, untranslate_hits = 6
    Source - Origin: 10.3.68.1/32, Translated: 10.2.58.1/32
    Service - Origin: tcp source eq www , Translated: tcp source eq www
2 (DMZ2) to (outside) source static WWW WWW_NAT   service TELNET_3021
TELNET
    translate_hits = 0, untranslate_hits = 6
    Source - Origin: 10.3.68.1/32, Translated: 10.2.58.1/32
    Service - Origin: tcp source eq 3021 , Translated: tcp source eq
telnet
3 (DMZ2) to (outside) source static R1_F00 R1_F00   destination static
R7_F01 R7_F01
    translate_hits = 2, untranslate_hits = 16
    Source - Origin: 10.2.68.1/32, Translated: 10.2.68.1/32
    Destination - Origin: 10.2.58.7/32, Translated: 10.2.58.7/32
4 (inside) to (outside) source static R2_G01 R2_G01   destination static
R7_F01 R7_F01
    translate_hits = 2, untranslate_hits = 13
    Source - Origin: 10.2.88.2/32, Translated: 10.2.88.2/32
```

```
    Destination - Origin: 10.2.58.7/32, Translated: 10.2.58.7/32
5 (inside) to (outside) source static R4_S0002 R4_S0002   destination
static R7_F01 R7_F01
    translate_hits = 6, untranslate_hits = 17
    Source - Origin: 8.9.56.4/32, Translated: 8.9.56.4/32
    Destination - Origin: 10.2.58.7/32, Translated: 10.2.58.7/32
6 (DMZ2) to (outside) source static R1_F00 R1_NAT
    translate_hits = 2, untranslate_hits = 0
    Source - Origin: 10.2.68.1/32, Translated: 10.2.58.31/32
7 (inside) to (outside) source static R2_G01 R2_NAT
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 10.2.88.2/32, Translated: 10.2.58.32/32
8 (inside) to (outside) source static R4_S0002 R4_NAT
    translate_hits = 3, untranslate_hits = 0
    Source - Origin: 8.9.56.4/32, Translated: 10.2.58.34/32

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static ACS 10.2.58.100
    translate_hits = 5, untranslate_hits = 3
    Source - Origin: 10.1.1.100/32, Translated: 10.2.58.100/32
2 (inside) to (outside) source dynamic NET_108 interface
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 10.2.108.0/24, Translated: 10.2.58.30/24
```

Task 1.4: Redundant Interface (4 Points)

- Configure the interfaces Ethernet 0/0 and Ethernet 0/2 of ASA2 as members of the redundant interface 1, so that you have the following output :

```
ASA2(config)# sh int red 1 | be Information
  Redundancy Information:
        Member Ethernet0/2(Active), Ethernet0/0
        Last switchover at 16:38:50 UTC May 27 2013
```

Detailed Solution

CAT4

```
int g1/0/8
 sw host
 sw acc vlan 158
```

ASA2

```
clear configure interface e0/0

int e0/0
 no sh

int e0/2
 no sh

interface Redundant1
 member-interface Ethernet0/2
 member-interface Ethernet0/0
 nameif outside
 bridge-group 1
 security-level 0

redundant-interface red1 active-member ethernet 0/2

arp outside 10.2.48.5 001b.d50f.f2f8

access-group OUTSIDE_IN in interface outside
access-group OUTSIDE6_IN in interface outside

arp-inspection outside enable no-flood
```

This exercise is not complex, its main goal is to remember that you MUST read all the questions before starting the lab to avoid breaking already done configuration or lose 4 points.

Note that when we cleared configuration on the outside interface, ASA automatically disabled all features that had been previously enabled on that port. On the real lab you would want to configure this part along with Task 1.1.

Also always verify initial configuration.

Verification

```
ASA2(config)# sh int red 1 | be Information
  Redundancy Information:
        Member Ethernet0/2(Active), Ethernet0/0
        Last switchover at 16:38:50 UTC May 27 2013

ASA2(config)# sh arp-inspection
interface                arp-inspection         miss
-----------------------------------------------------
outside                  enabled                no-flood
inside                   disabled                -
DMZ                      disabled                -

ASA2(config)# sh mac-address-table static
interface                   mac  address          type      Age(min)
bridge-group
-------------------------------------------------------------------------
---------
DMZ                       30e4.dbce.8490          static
1
inside                    001b.d517.ba88          static
1
outside                   001b.d50f.f2f8          static
1

R5#ping 10.2.48.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R5#ping 10.2.48.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

2.0 IOS Firewall (4 points)

Task 2.1: CBAC (4 Points)

- After recent network security internal issues, you have been requested to secure connection to VLAN 38 by implementing CBAC using the following parameters :
  - Treat the link to VLAN 38 as the inside; Internet interface as the outside
  - Allow TCP and UDP sessions initiated from the inside to return into the outside interface and generate alert and audit messages
  - Permit outside PC host to connect via SSH and Telnet to CAT4 for management and inspect this traffic. Log and enable alerts for these two protocols
  - Idle TCP sessions should timeout after 30 minutes
  - UDP sessions should be timed out after 180 seconds

Detailed Solution

R6

```
ip inspect udp idle-time 180
ip inspect tcp idle-time 1800

ip inspect name CBAC_OUT tcp alert on audit-trail on
ip inspect name CBAC_OUT udp alert on audit-trail on

ip inspect name CBAC_IN telnet alert on audit-trail on
ip inspect name CBAC_IN ssh alert on audit-trail on

access-list 102 permit icmp any any
access-list 102 permit eigrp any host 10.2.18.6
access-list 102 permit eigrp host 10.2.18.6 host 224.0.0.10
access-list 102 permit eigrp host 10.2.18.5 host 224.0.0.10
access-list 102 permit tcp host 10.2.28.200 host 10.2.38.24 eq telnet
access-list 102 permit tcp host 10.2.28.200 host 10.2.38.24 eq 22
access-list 102 deny   ip any any log

interface FastEthernet0/0
```

```
 ip access-group 102 in
 ip inspect CBAC_IN in
 ip virtual-reassembly

interface FastEthernet0/1
 ip inspect CBAC_OUT in
 ip virtual-reassembly
```

The pitfall here is on the inspection of incoming traffic destined to internal Telnet/SSH server.

Access-list 102 allow outside traffic to reach Telnet and SSH server. Also dynamic routing protocol and icmp are allowed to come in.

Verification

```
R6#sh ip inspect sessions detail
Established Sessions
 Session 4A0557AC (10.2.38.24:23113)=>(10.2.18.5:23) tcp SIS_OPEN
  Created 00:00:01, Last heard 00:00:01
  Bytes sent (initiator:responder) [27:49]
  In  SID 10.2.18.5[23:23]=>10.2.38.24[23113:23113] on ACL 102  (6
matches)
```

The “outside” part can be verified from the Test PC. You can also quickly change IP on CAT1 to be .200 (restore the original value after testing) and test :

```
CAT1#telnet 10.2.38.24 /source-interface vlan28
Trying 10.2.38.24 ... Open


User Access Verification

Username: cisco
Password:

R6#sh access-l
Extended IP access list 102
    10 permit icmp any any
    20 permit eigrp any host 10.2.18.6
```

```
    30 permit eigrp host 10.2.18.6 host 224.0.0.10
    40 permit eigrp host 10.2.18.5 host 224.0.0.10 (73 matches)
    50 permit tcp host 10.2.28.200 host 10.2.38.24 eq telnet (17 matches)
    60 permit tcp host 10.2.28.200 host 10.2.38.24 eq 22
    70 deny ip any any log
```

```
R6#sh ip inspect config
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 1800 sec -- udp idle-time is 180 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_OUT
    tcp alert is on audit-trail is on timeout 1800
    udp alert is on audit-trail is on timeout 180
 Inspection name CBAC_IN
    telnet alert is on audit-trail is on timeout 1800
    ssh alert is on audit-trail is on timeout 180
```

3.0 Cisco IPS and Content Security (12 points)

Task 3.1: IPS Initialization (4 Points)

- Configure the IPS according to the diagram and IP Addressing table
- Allow the networks 10.2.48.0/24, 10.2.78.0/24 and 10.2.118.0/24 to manage the IPS
- Configure two inline interfaces pairs using the interfaces GigabitEthernet0/0 and GigabitEthernet0/1 as Pair1 and GigabitEthernet0/2 and GigabitEthernet0/3 as Pair2
- Create a second virtual sensor named vs1
- Inline Pair1 should be configured to be used by vs0 sensor
- Inline Pair2 should be configured to be used by vs1 sensor

- Configure Anomaly Detection Configuration, Signature Definition Configuration and Event Action Rules Configuration according to the table below
- Configure IPS to be managed through HTTP (no encryption) on port 8181
- Enable telnet on the IPS

Inline interface pair	Pair1	Gi0/0 Gi0/1	vs0	sig0	ad0
Inline interface pair	Pair2	Gi0/2 Gi0/3	vs1	sig1	ad1

Detailed Solution

CAT4

```
interface GigabitEthernet1/0/1
 switchport access vlan 78
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/2
 sw host
 sw acc vlan 148

interface GigabitEthernet1/0/3
 sw host
 sw acc vlan 48

interface GigabitEthernet1/0/4
 sw host
 sw acc vlan 168

interface GigabitEthernet1/0/5
 sw host
 sw acc vlan 68
```

IPS

```
Enter host name[sensor]: IPS
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.2.78.15/24,10.2.78.30
Modify current access list?[no]: yes
```

```
Current access list entries:
  No entries
Permit: 10.2.48.0/24
Permit: 10.2.78.0/24
Permit: 10.2.118.0/24
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 10.2.78.15/24,10.2.78.30
host-name IPS
telnet-option disabled
access-list 10.2.48.0/24
access-list 10.2.78.0/24
access-list 10.2.118.0/24
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]: 2

conf t
service interface
 physical-interfaces GigabitEthernet0/0
 admin-state enabled
 exit
 physical-interfaces GigabitEthernet0/1
 admin-state enabled
 exit
 physical-interfaces GigabitEthernet0/2
 admin-state enabled
 exit
 physical-interfaces GigabitEthernet0/3
 admin-state enabled
 exit
inline-interfaces Pair1
 interface1 GigabitEthernet0/0
 interface2 GigabitEthernet0/1
 exit
inline-interfaces Pair2
 interface1 GigabitEthernet0/2
 interface2 GigabitEthernet0/3
 exit
exit

service host
 network-settings
 host-ip 10.2.78.15/24,10.2.78.30
 host-name IPS
 telnet-option enabled
 access-list 10.2.48.0/24
 access-list 10.2.78.0/24
```

```
 access-list 10.2.118.0/24
 exit
exit

service event-action-rules rules1
exit

service signature-definition sig1
exit

service anomaly-detection ad1
exit

service analysis-engine
virtual-sensor vs0
 logical-interface Pair1
 exit
virtual-sensor vs1
 signature-definition sig1
 event-action-rules rules1
 anomaly-detection
 anomaly-detection-name ad1
 exit
logical-interface Pair2
 exit
exit

service web-server
 enable-tls false
 port 8181
 exit
```

You did not have to configure this task from the CLI – you could use the GUI.

A separate set of Event Action Rules was defined since it will be needed according to the requirements of future tasks.

Verification

Since the OSPF adjacency came up we can be now certain packets are going through the IPS:

```
sensor# sh interfaces brief
CC   Interface            Sensing State   Link   Inline Mode
Pair Status
     GigabitEthernet0/0   Enabled       Up     Paired with interface
GigabitEthernet0/1   Up
*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Enabled         Up     Paired with interface
GigabitEthernet0/0   Up
     GigabitEthernet0/2   Enabled         Up     Paired with interface
GigabitEthernet0/3   Up
     GigabitEthernet0/3   Enabled         Up     Paired with interface
GigabitEthernet0/2   Up

R5#sh ip ei neighbors
EIGRP-IPv4 Neighbors for AS(55)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
2   10.2.48.7               Fa0/0             14 00:14:45   13   200  0
12
1   10.2.48.10              Fa0/0             14 02:11:45    4   200  0  6
0   10.2.18.6               Fa0/1             10 1d20h       1   200  0
17

R7#sh ipv ospf ne

Neighbor ID     Pri   State           Dead Time   Interface ID
Interface
10.2.48.10        1   FULL/BDR    00:00:35    3
FastEthernet0/0
55.55.55.55       1   FULL/DR     00:00:39    3
FastEthernet0/0

R1#ping 10.2.18.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.18.6, timeout is 2 seconds:
!!!!!
```

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

R2#ping 10.2.18.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.18.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 3.2: Signatures (4 Points)

- Configure IPS to synchronize to NTP server installed on R7 using “cisco” as authentication password
- Configure the IPS to trigger an alert in event store for traffic that generates an “ICMP echo request” and “ICMP echo reply” events. Also, start to log packets containing the attacker-victim address pair
- Configure IPS to send a detailed alert each time a signature with risk rating superior to 92 fired. Don't take any other actions (besides what was configured under the signature itself)
- Make sure the detailed alert appears on the management console
- Ping R7 from R5 and R1 from R7 to ensure you have the alerts generated
- Do not translate any IP address to 10.2.58.0/24 network for this task

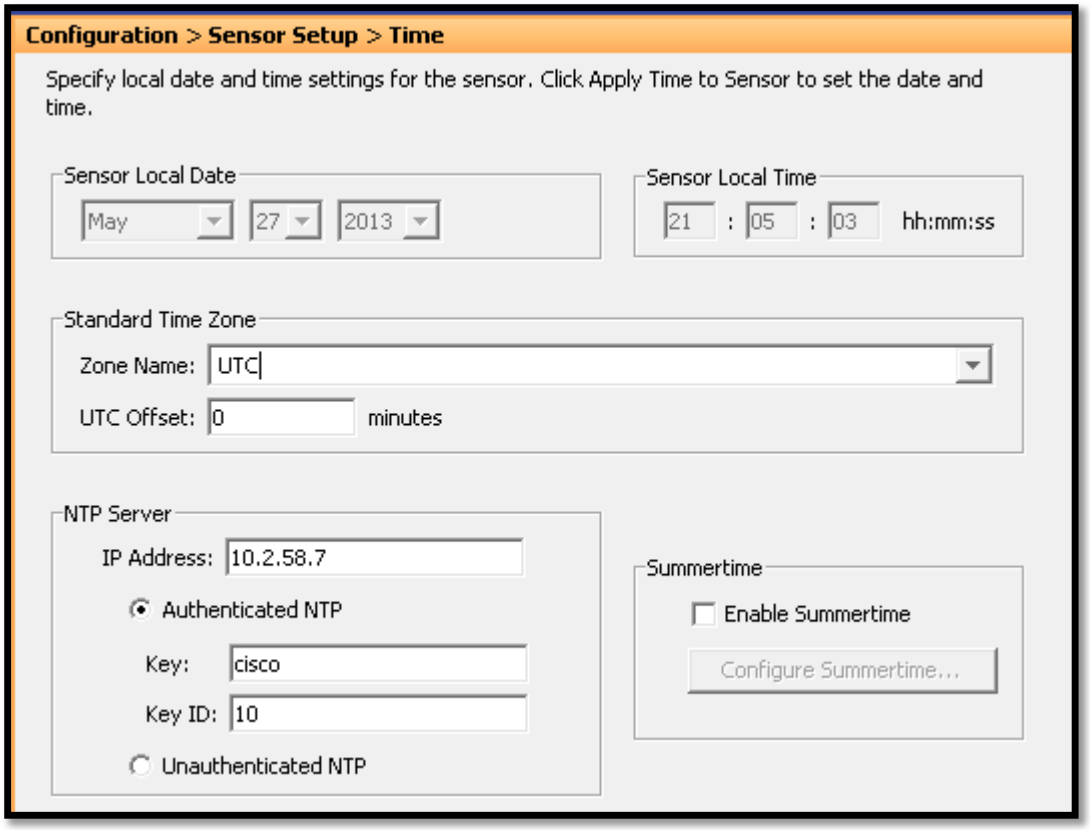
Detailed Solution

ASA3

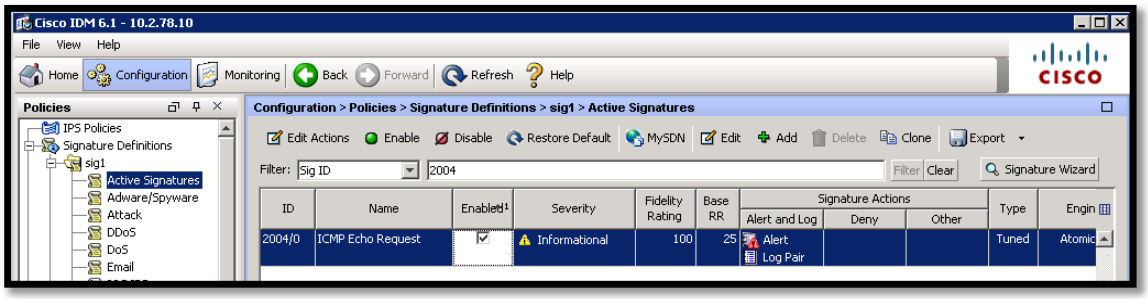
```
router eigrp 55
 redistribute connected

access-list DMZ3_IN per udp host 10.2.78.15 host 10.2.58.7 eq 123
```

IPS

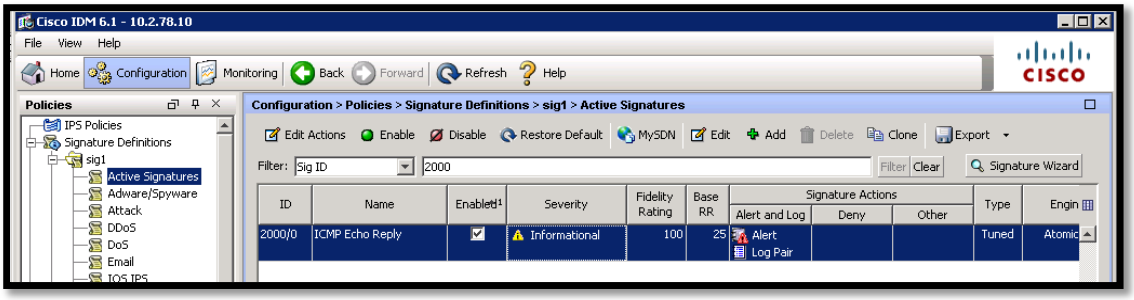
First sync time with R7 :



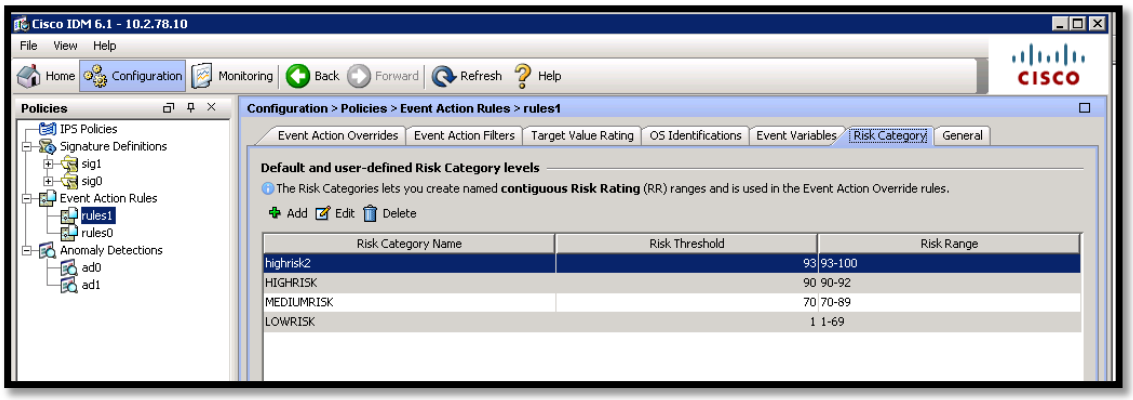
Signature 2004, ICMP echo request on signature definitions sig0 and sig1 :



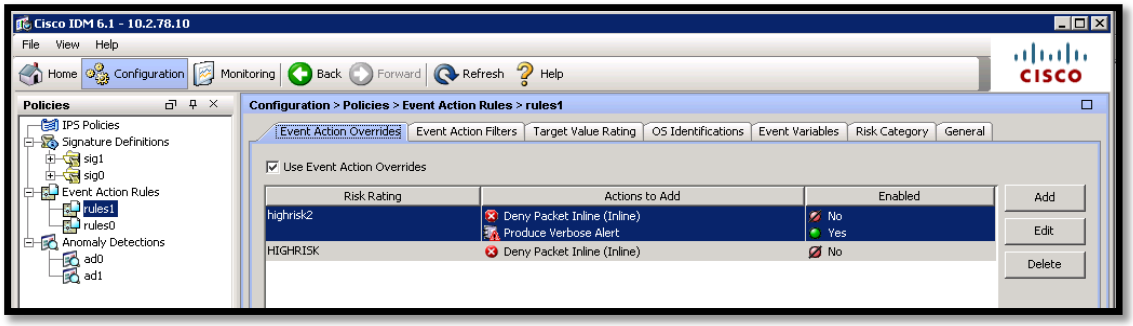
Signature 2000, ICMP echo reply on signature definitions sig0 and sig1 :



Risk category (rules0 and rules1) :



Event action rule (rules0 and rules1) :



Since the question asks to trigger an alert for ANY icmp request and reply traffic, signature should be configured on both VS0 and VS1.

As well, event action rules should be configured VS0 and VS1. In this case the risk category needs to be updated first with a new category, which fill the risk range between 93 and 100 then, configure actions for event action rules.

Since “deny packet inline” action is configured by default for risk range upper to 90 and cannot be deleted so, you need to disable this action and add the required one.

At last, the task didn't specify on which sensor you should apply the changes so, you will apply them to both sensors.

Verification

Ping between R1, R5 and R7 :

```
IPS# show events alert

evIdsAlert: eventId=1041379286523800835 severity=informational
vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/05/27 21:10:21 2013/05/27 21:10:21 UTC
  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 10.2.68.1
    target:
      addr: locality=OUT 10.2.58.7
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    logPacketsActivated: true
    logPairPacketsActivated: true
  ipLogIds:
    ipLogId: 1701736963
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
  threatRatingValue: 35
  interface: ge0_3
  protocol: icmp
```

```
evIdsAlert: eventId=1041379286523800856 severity=informational
vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/05/27 21:13:24 2013/05/27 21:13:24 UTC
  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 10.2.48.7
    target:
      addr: locality=OUT 10.2.48.5
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    logPacketsActivated: true
    logPairPacketsActivated: true
  ipLogIds:
    ipLogId: 1701736964
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
  threatRatingValue: 35
  interface: ge0_1
  protocol: icmp


sensor# sh clock det
21:15:08 UTC Mon May 27 2013
Time source is NTP
```

Task 3.3: Custom IPS Signature (4 Points)

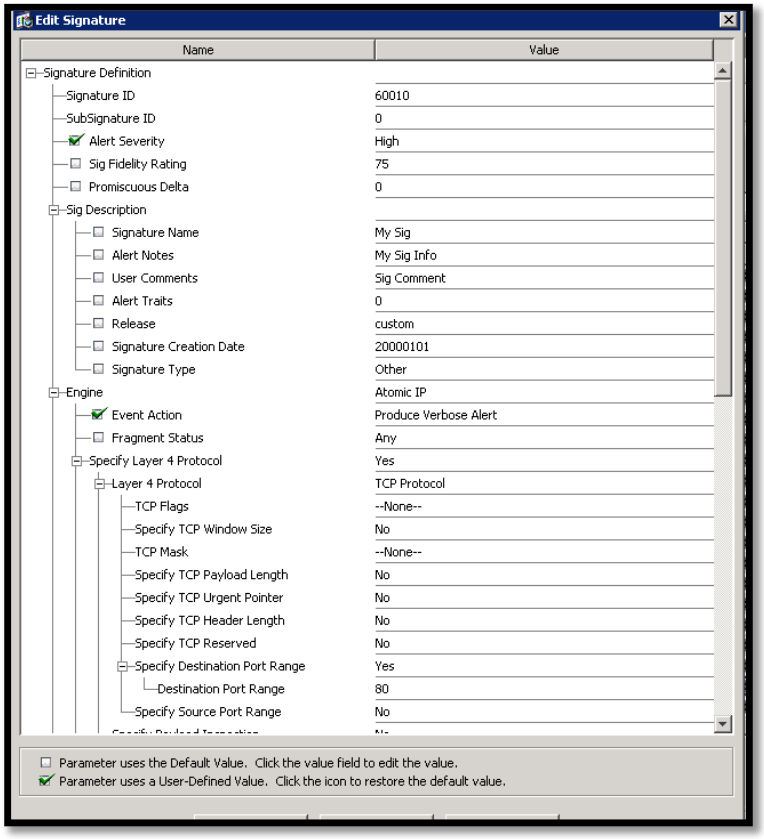
- Create a custom signature with the ID 60009
- This signature should trigger when a HTTP session is initiated from IP address

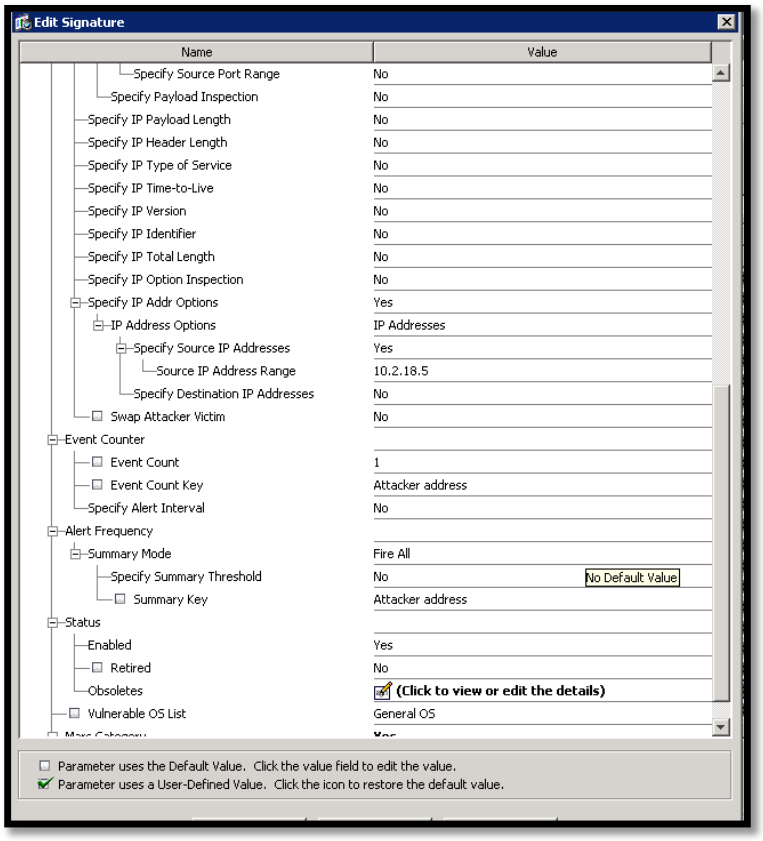
"10.2.18.5" to the web server on R1. The IPS will generate a High severity detailed alert
- Create another signature with ID 60010
- This signature will trigger if a Telnet session is opened from IP address "10.2.18.5" to R1. The IPS will generate a High Severity detailed alert
- When signatures 60009 and 60010 fire within a 20s interval in any order, then trigger a detailed alert and do not transmit this packet and future packets originating from the attacker address for 25 minutes
- Apply the signatures 60009, 60010 and 60011 to sensor vs0
- Do not modify ASA2 or ASA3 configuration for this task

Detailed Solution

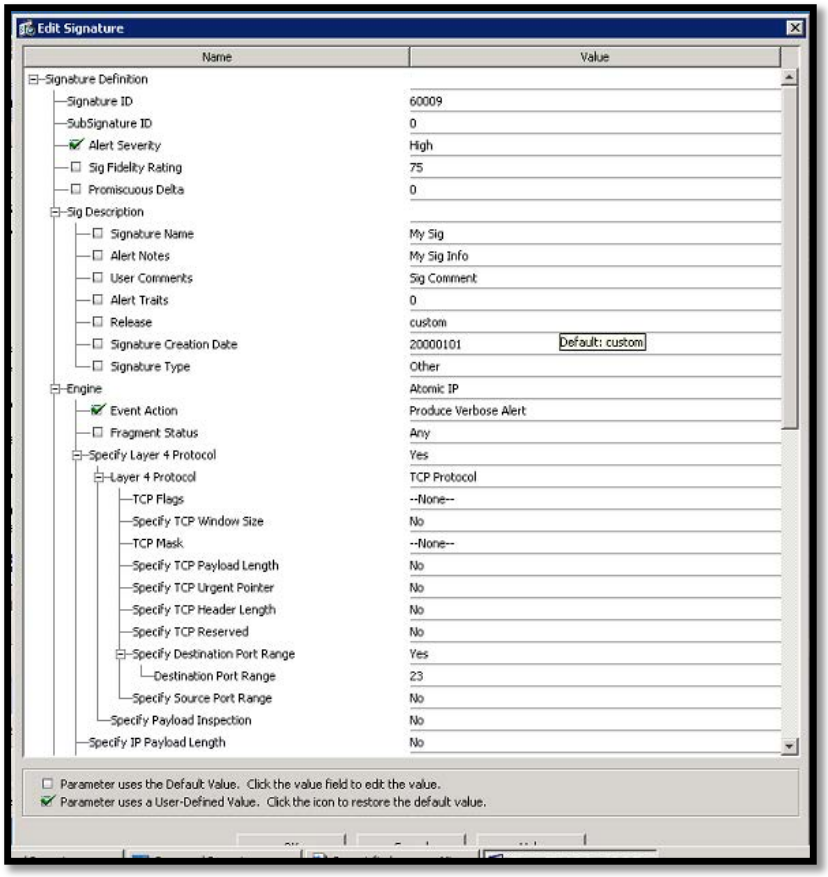
IPS

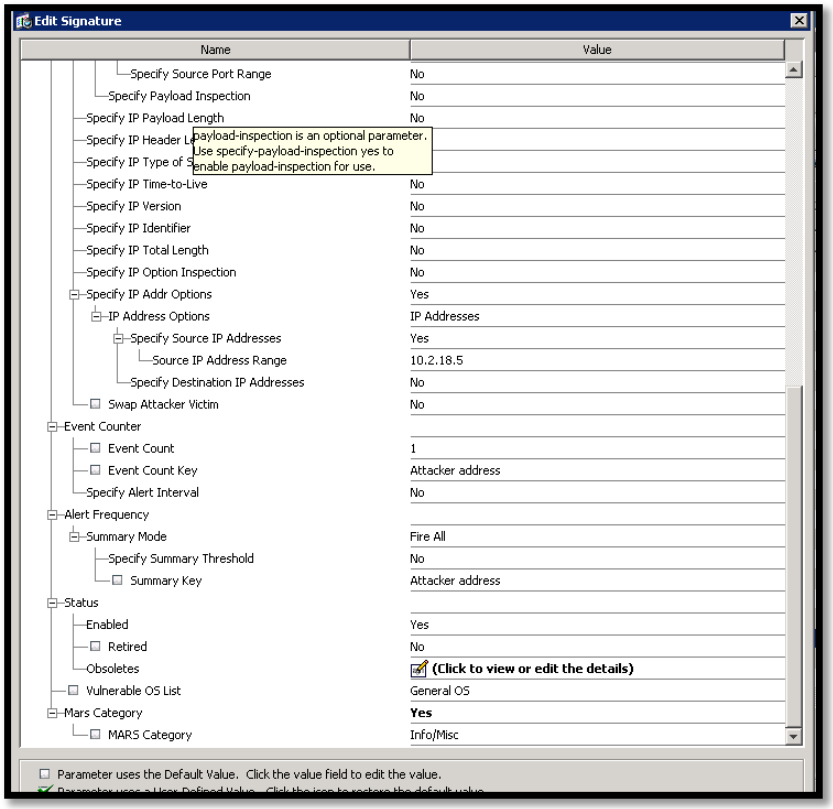
Signature 60009 :



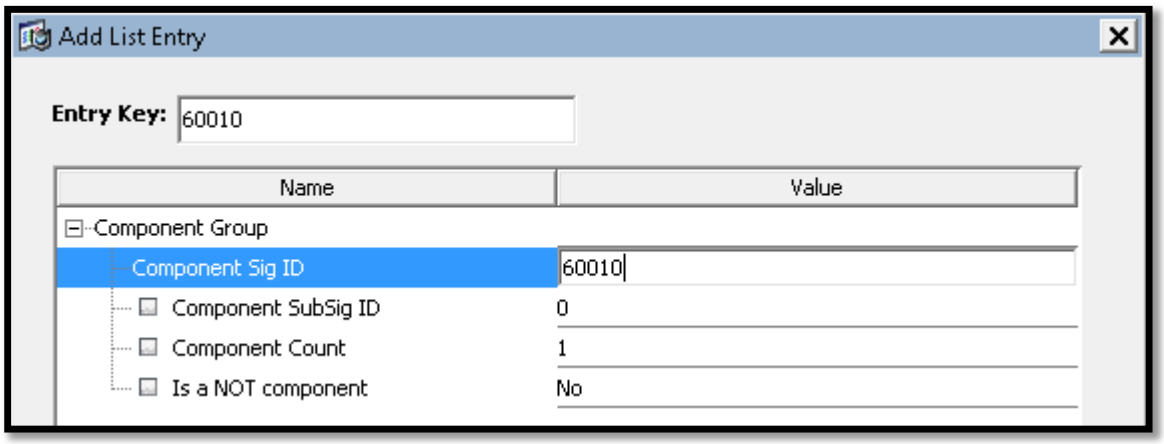


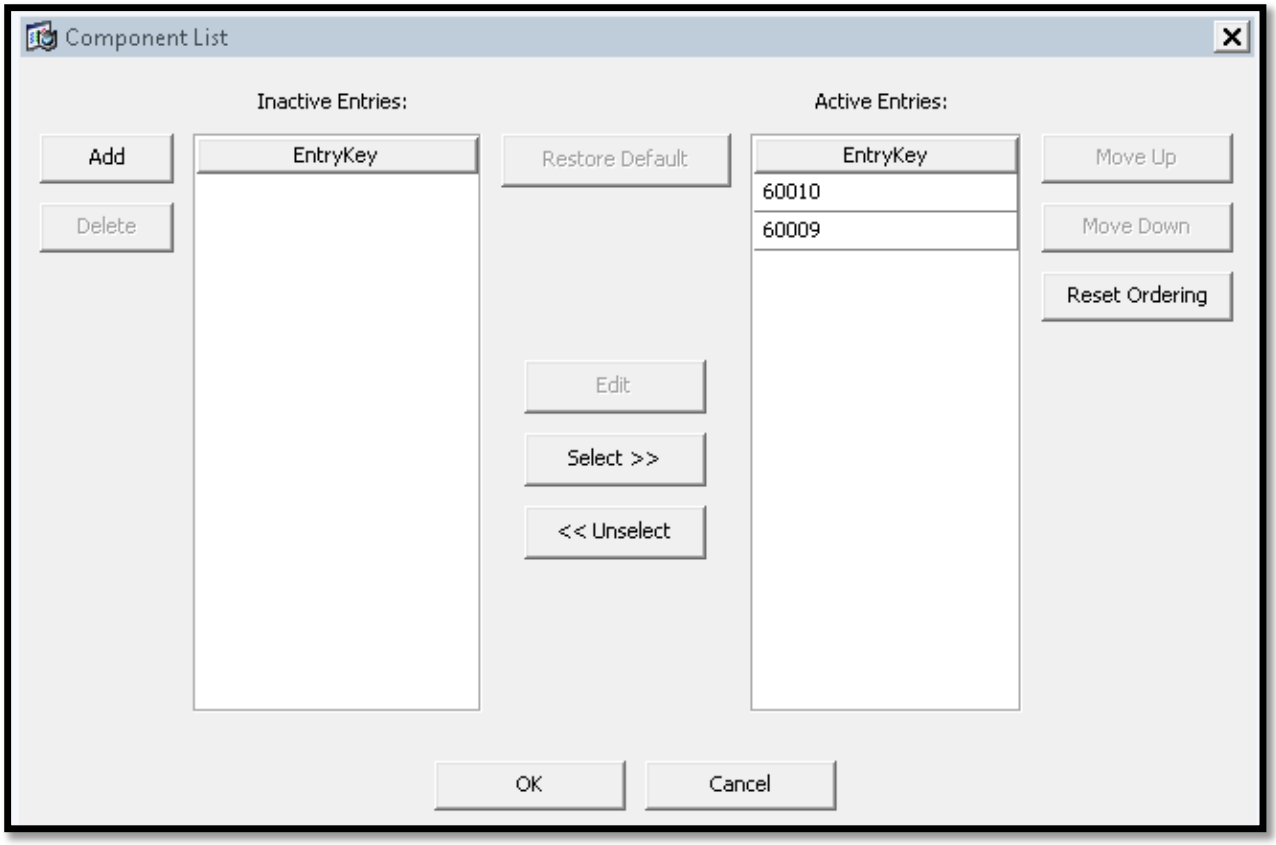
Signature 60010



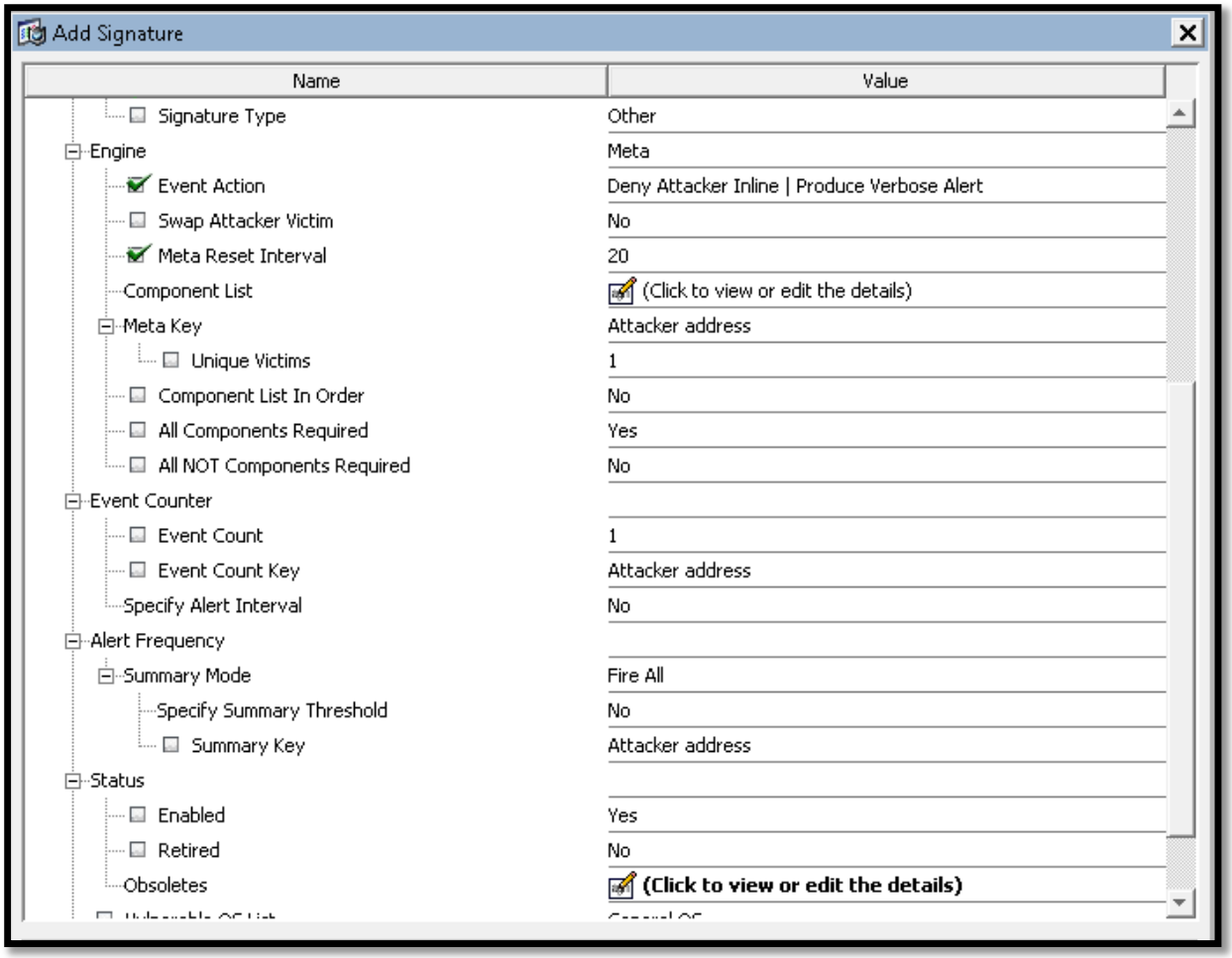


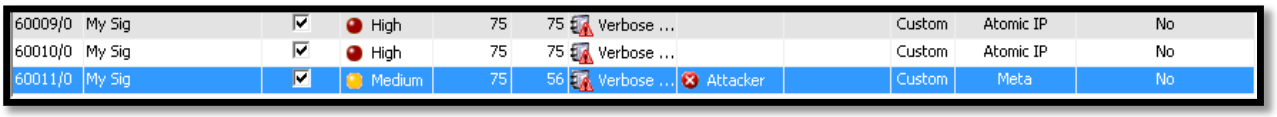
Signature 60011 – first create a new signature (ID 60011), select the “Meta” engine and modify the Component List :



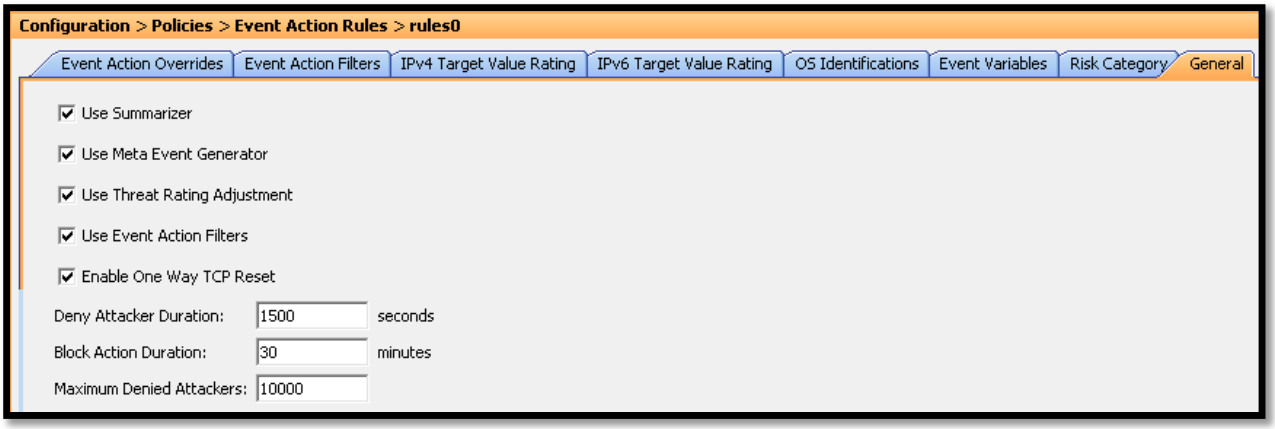


The order does not matter in our case so we can leave 60010 and then 60009.





Set “Deny Attacker Duration” to 25 minutes (1500 seconds) :



They key things in this task is the use of Atomic IP and Meta engines.

The "Atomic IP" engine allow to specify the attacker IP address and the TCP destination port so, use this engine to create signatures 60009 and 60010.

The "Meta" engine is designed to configure using several options, IPS actions when multiple signatures triggered in certain conditions.

Alert summarization was turned off ("Fire All") to see all alerts although this was not required for this task.

To clear denied attacker address during tests, select the related line and click "clear list" in the GUI or use the "clear denied-attackers" CLI command.

Verification

First thing – if you telnet/HTTP from F0/0 nothing is triggered on IPS. That's what we want to see:

```
R5#telnet 10.2.58.1
Trying 10.2.58.1 ... Open


User Access Verification

Username: cisco
Password:
R1>

sensor# sh events past 00:01:00
```

Now let's observe real time (first Telnet, wait 20 seconds, then HTTP):

```
sensor# sh events alert

R5#telnet 10.2.58.1 /source-interface f0/1
Trying 10.2.58.1 ... Open

evIdsAlert: eventId=1041379286523800929 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/05/27 22:30:48 2013/05/27 22:30:48 UTC
  signature: description=My Sig id=60010 created=20000101 type=other
version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.2.18.5
      port: 21494
    target:
      addr: locality=OUT 10.2.58.1
      port: 23
      os: idSource=unknown relevance=relevant type=unknown
  triggerPacket:
000000  00 1B D5 17 BA 88 00 1B  D5 0F F2 F8 08 00 45 C0  ..............E.
000010  00 28 40 73 00 00 FF 06  1A 93 0A 02 12 05 0A 02  .(@s............
000020  3A 01 53 F6 00 17 2C F8  0A BE 67 B2 86 5A 50 10  :.S...,...g..ZP.
000030  0F DE C6 1C 00 00 00 00  00 00 00 00              ............
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
  interface: ge0_0
  protocol: tcp


R5#telnet 10.2.58.1 80 /source-interface f0/1
```

```
Trying 10.2.58.1, 80 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Mon, 27 May 2013 22:30:54 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 10.2.58.1 closed by foreign host]

evIdsAlert: eventId=1041379286523800948 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/05/27 22:31:56 2013/05/27 22:31:56 UTC
  signature: description=My Sig id=60009 created=20000101 type=other
version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.2.18.5
      port: 32469
    target:
      addr: locality=OUT 10.2.58.1
      port: 80
      os: idSource=unknown relevance=relevant type=unknown
  triggerPacket:
000000  00 1B D5 17 BA 88 00 1B  D5 0F F2 F8 08 00 45 C0  ..............E.
000010  00 2C 4C B9 00 00 FF 06  0E 49 0A 02 12 05 0A 02  .,L......I......
000020  3A 01 7E D5 00 50 3B 13  75 7E 00 00 00 00 60 02  :.~..P;.u~....`.
000030  10 20 FB E1 00 00 02 04  02 18 00 00              . ..........
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
```

```
  interface: ge0_0
  protocol: tcp
```

Now Telnet and HTTP one by one (or vice versa):

```
R5#telnet 10.2.58.1 80 /source-interface f0/1
Trying 10.2.58.1, 80 ... Open
get /
HTTP/1.1 400 Bad Request
Date: Mon, 27 May 2013 22:32:55 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 10.2.58.1 closed by foreign host]
R5#
R5#
R5#telnet 10.2.58.1 /source-interface f0/1
Trying 10.2.58.1 ...

evIdsAlert: eventId=1041379286523800982 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/05/27 22:34:09 2013/05/27 22:34:09 UTC
  signature: description=My Sig id=60011 created=20000101 type=other
version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.2.18.5
  actions:
    deniedAttacker: true
```

```
  alertDetails: Component Signature List: 60009.0 60010.0  ;
  triggerPacket:
000000  00 1B D5 17 BA 88 00 1B  D5 0F F2 F8 08 00 45 C0  ..............E.
000010  00 2C 26 42 00 00 FF 06  34 C0 0A 02 12 05 0A 02  .,&B....4.......
000020  3A 01 A1 F1 00 17 3D 29  AD EE 00 00 00 00 60 02  :.....=).....`.
000030  10 20 9E 78 00 00 02 04  02 18 00 00              . .x........
  riskRatingValue: targetValueRating=medium 56
  threatRatingValue: 11
  interface: ge0_0
  protocol: tcp

sensor# show statistics denied-attackers
Statistics for Virtual Sensor vs0
   Denied Attackers and hit count for each.
      10.2.18.5 = 6
   Denied Attackers with percent denied and hit count for each.
         Attacker Address   Victim Address   Port   Protocol   Requested
Percentage   Actual Percentage   Hit Count   Reputation Action
         10.2.18.5                                              100
100                6          false

Statistics for Virtual Sensor vs1
   Denied Attackers and hit count for each.
   Denied Attackers with percent denied and hit count for each.

R5#telnet 10.2.58.1 /source-interface f0/1
Trying 10.2.58.1 ...
% Connection timed out; remote host not responding
```

4.0 Cisco VPN Solutions (20 points)

Task 4.1: PKI Server (4 Points)

- Create an exportable RSA key on R6 with the default key size labeled “iosca”
- Configure R6 as a IOS Server using the following parameters :
  - Common name of cisco1.ipexpert.com, Locality of NY and country of US
  - CRL lifetime – 24 hours
- Export key to non-volatile RAM (NVRAM) with the following parameters :
  - Encryption : 3des

  - Password : cisco123
- Configure R6 to synchronize its clock to NTP server on R7; configure ASA2 accordingly NTP password is “cisco”

Detailed Solution

ASA2

```
access-list OUTSIDE_IN per udp host 10.2.18.6 host 10.2.58.7 eq 123
```

R6

```
ntp logging
ntp authentication-key 10 md5 cisco
ntp authenticate
ntp trusted-key 10
ntp server 10.2.58.7 key 10

ip http server

crypto key generate rsa label iosca exportable

crypto pki trustpoint iosca
 revocation-check crl
 rsakeypair iosca

crypto pki server iosca
 issuer-name CN=cisco1.ipexpert.com,L=NY,C=US
 lifetime crl 24
 no shutdown

ip access-list ext 102
 no deny ip any any log
 per udp host 10.2.58.7 host 10.2.18.6 eq 123
 200 deny ip any any log

cry key export rsa iosca pem url nvram:CAKEYPAIR 3des cisco123
```

Make sure CA is enabled AFTER the time is synchronized with R7.

Verification

A similar output should show up when exporting the keys :

```
R6(config)#cry key export rsa iosca pem url nvram:CAKEYPAIR 3des cisco123
% Key name: iosca
Usage: General Purpose Key
Exporting public key...
Destination filename [CAKEYPAIR.pub]?
Writing file to nvram:CAKEYPAIR.pub
Exporting private key...
Destination filename [CAKEYPAIR.prv]?
Writing file to nvram:CAKEYPAIR.prv

R6#dir nvram: | in CAKEYPAIR
   12  -rw-         272                    <no date>  CAKEYPAIR.pub
   13  -rw-         951                    <no date>  CAKEYPAIR.prv


R6#sh ntp status
Clock is synchronized, stratum 9, reference is 10.2.58.7
nominal freq is 250.0000 Hz, actual freq is 249.9989 Hz, precision is
2**24
reference time is D54E63EC.AC5978B4 (23:59:56.673 UTC Mon May 27 2013)
clock offset is -0.8333 msec, root delay is 3.15 msec
root dispersion is 940.39 msec, peer dispersion is 938.65 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000004243
s/s
system poll interval is 64, last update was 3 sec ago.

R6#sh cry pki server
Certificate Server iosca:
    Status: enabled
    State: enabled
    Server's configuration is locked (enter "shut" to unlock it)
    Issuer name: CN=cisco1.ipexpert.com,L=NY,C=US
    CA cert fingerprint: F262BB58 4705A747 2BFA7879 5AC4A5D8
    Granting mode is: manual
    Last certificate issued serial number (hex): 1
    CA certificate expiration timer: 00:00:24 UTC May 27 2016
    CRL NextUpdate timer: 00:00:24 UTC May 29 2013
```

```
Current primary storage dir: nvram:
Database Level: Minimum - no cert data written to storage
```

Task 4.2: GETVPN (4 Points)

- R7 is configured as GETVPN key server and group members are R1 and R2
- One (1) fault has been inserted in pre-configuration files
- Configure R2 (Gi0/1) and R1 (F0/0) as GETVPN group members of the key server R7
- You are allowed to use two static routes for this task

Detailed Solution

ASA3

```
access-list OUTSIDE_IN permit udp host 10.2.58.7 host 10.2.68.1 eq 848
access-list OUTSIDE_IN permit udp host 10.2.58.7 host 10.2.88.2 eq 848

access-list DMZ2_IN per esp host 11.11.11.11 host 22.22.22.22
access-list INSIDE_IN per esp host 22.22.22.22 host 11.11.11.11

route DMZ2 11.11.11.11 255.255.255.255 10.2.68.1
```

R7

```
no crypto isakmp key cisco address 10.3.68.1
crypto isakmp key cisco address 10.2.68.1
```

R2

```
crypto gdoi group GET
 identity number 1357924680
 server address ipv4 10.2.58.7

crypto map MAP1 10 gdoi
 set group GET

int g0/1
```

```
 cry map MAP1

ip route 11.11.11.11 255.255.255.255 10.2.88.30

router ospf 1
 network 22.22.22.22 0.0.0.0 ar 50
```

R1

```
crypto gdoi group GET
 identity number 1357924680
 server address ipv4 10.2.58.7

crypto map MAP1 10 gdoi
 set group GET

int f0/0
 cry map MAP1
```

Based on the R7's configuration you should be able to figure out what traffic needs to be protected plus you should also check if all GET VPN components were properly defined and exist in the config. This is how we spot the PSK is wrong on the KS – it should be for 10.2.68.1, not 10.3.68.1.

Since GETVPN preserve original IP header, you would announce 22.22.22.22 network in R2 OSPF process so ASA3 will learn route to this network.

Also between group members R1 and R2, ASA should authorize to allow encrypted traffic - notice that original IP address are allowed due to, again, GETVPN IP header preservation feature.

Verification

```
R7#sh cry gd ks
Total group members registered to this box: 2

Key Server Information For Group GETVPN-CCIE:
    Group Name               : GETVPN-CCIE
    Group Identity           : 1357924680
    Group Members            : 2
```

```
        IPSec SA Direction      : Both
        ACL Configured:
            access-list sa-acl

    R1#sh cry gd gm

    Group Member Information For Group GET:
        IPSec SA Direction      : Both
        ACL Received From KS    : gdoi_group_GET_temp_acl

        Group member            : 10.2.68.1        vrf: None
           Registration status  : Registered
           Registered with      : 10.2.58.7
           Re-registers in      : 6487 sec
           Succeeded registration: 1
           Attempted registration: 1
           Last rekey from      : 0.0.0.0
           Last rekey seq num   : 0
           Unicast rekey received: 0
           Rekey ACKs sent      : 0
           Rekey Received       : never

    R1#sh cry gd gm acl
    Group Name: GET
     ACL Downloaded From KS 10.2.58.7:
       access-list  permit ip host 22.22.22.22 host 11.11.11.11
       access-list  permit ip host 11.11.11.11 host 22.22.22.22
     ACL Configured Locally:

    R1#sh cry isa sa
    IPv4 Crypto ISAKMP SA
    dst             src             state          conn-id status
    10.2.68.1       10.2.58.7       GDOI_REKEY        1003 ACTIVE
    10.2.58.7       10.2.68.1       GDOI_IDLE         1001 ACTIVE
    10.2.68.1       10.2.58.7       GDOI_REKEY        1002 ACTIVE

    R2#sh cry isa sa
    IPv4 Crypto ISAKMP SA
    dst             src             state          conn-id status
    10.2.88.2       10.2.58.7       GDOI_REKEY        1003 ACTIVE
```

```
10.2.58.7       10.2.88.2       GDOI_IDLE          1001 ACTIVE
10.2.88.2       10.2.58.7       GDOI_REKEY         1002 ACTIVE

R2#sh cry gdoi gm reke
Group GET (Unicast)
    Number of Rekeys received (cumulative)       : 1
    Number of Rekeys received after registration : 1
    Number of Rekey Acks sent                    : 1

Rekey (KEK) SA information :
          dst             src             conn-id  my-cookie  his-cookie
New     : 10.2.88.2       10.2.58.7         1003   DD0F3E06   5B5FDD82
Current : 10.2.88.2       10.2.58.7         1002   2C0E8639   549ED299
Previous: 10.2.88.2       10.2.58.7         1002   2C0E8639   549ED299

R1#ping 22.22.22.22 so l11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
Packet sent with a source address of 11.11.11.11
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#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: FastEthernet0/0
Uptime: 00:00:08
Session status: UP-ACTIVE
Peer: 0.0.0.0 port 848 fvrf: (none) ivrf: (none)
      Phase1_id: 10.2.58.7
      Desc: (none)
  IKEv1 SA: local 10.2.68.1/848 remote 10.2.58.7/848 Active
          Capabilities:(none) connid:1006 lifetime:6w5d
  IKEv1 SA: local 10.2.68.1/848 remote 10.2.58.7/848 Active
          Capabilities:(none) connid:1005 lifetime:23:59:51
```

```
  IKEv1 SA: local 10.2.68.1/848 remote 10.2.58.7/848 Inactive
          Capabilities:(none) connid:1001 lifetime:0
  IPSEC FLOW: permit ip host 11.11.11.11 host 22.22.22.22
        Active SAs: 6, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/6427
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/6427
  IPSEC FLOW: permit ip host 22.22.22.22 host 11.11.11.11
        Active SAs: 6, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/6427
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/6427
```

Task 4.3: SSL VPN (4 Points)

- The IPS administrator needs to access remotely the IPS management interface in a secure way from PC host. After thorough research, SSL VPN solutions have been selected to do so
- Configure a SSL VPN access on R5 with the following parameters :
    - Use a SSL certificate issued by R6, configured as a CA server in task 4.1
    - Authentication : local
    - Create two local accounts admin/cisco and cisco/cisco
    - URL link label to access the IPS management interface is “IPS management”
    - Use https://R5.ipexpert.com to access to Web VPN portal page
    - After being authenticated to SSL VPN, manage the IPS through link http://127.0.0.1:8181
    - Allow a maximum of ten (10) users to connect to the router through SSL VPN
- If needed NTP authentication password is “cisco” and NTP server is R7
- Make the necessary modifications on access-lists on ASA2 and ASA3 firewalls
- You are allowed to modify the PC host file to achieve this task
- Make sure that there is no authentication on console access
- Ensure that you are able to access IPS management interface after login on WebVPN Portal
- To make the test, change the VLAN of PC Host to VLAN 28, configure network IP address as 10.2.28.200 without a default gateway and add the following route in DOS command: route add 10.2.0.0 mask 255.255.0.0 10.2.28.23

Detailed Solution

ASA2

```
access-list OUTSIDE_IN per tcp host 10.2.48.5 host 10.2.78.15 eq 8181
```

ASA3

```
access-list OUTSIDE_IN per tcp host 10.2.48.5 host 10.2.78.15 eq 8181
access-list OUTSIDE_IN per udp host 10.2.48.5 host 10.2.58.7 eq 123
```

R7

```
access-list 10 per host 10.2.48.5
```

R6

```
ip access-list ext 102
 80 per tcp any host 10.2.18.6 eq 80
```

After R5's enrollment :

```
cry pki server iosca grant all
```

R5

```
aaa new-model

aaa authentication login default local
aaa authentication login NO none
aaa authorization exec default local

ntp logging
ntp authentication-key 10 md5 cisco
ntp authenticate
ntp trusted-key 10
ntp server 10.2.58.7 key 10

cry key gen rsa lab SSLKEY mod 1024

crypto pki trustpoint SSLVPN_TRUST
 enrollment url http://10.2.18.6:80
 revocation-check crl
 rsa SSLKEY
```

```
 password ipexpert

crypto pki authen SSLVPN_TRUST
crypto pki enroll SSLVPN_TRUST

username admin password 0 cisco
username cisco password 0 cisco

line con 0
 login authentication NO

webvpn gateway SSLVPNGW
 hostname R5
 ip address 10.2.18.5 port 443
 http-redirect port 80
 ssl trustpoint SSLVPN_TRUST
 inservice

webvpn context SSLCON
 ssl authenticate verify all
 url-list "IPSsensor"
   heading "IPS System"
   url-text "IPS management" url-value "http://10.2.78.15:8181"

port-forward "PF_IPS"
   local-port 8181 remote-server "10.2.78.15" remote-po 8181 desc "Mgmt
IPS"
  policy group SSLPOL
   url-list "IPSsensor"
   port-forward "PF_IPS"
 default-group-policy SSLPOL
 gateway SSLVPNGW
 aaa authentication list default
 max-users 10
 inservice
```

Time synchronization is needed whenever digital certificates are used.

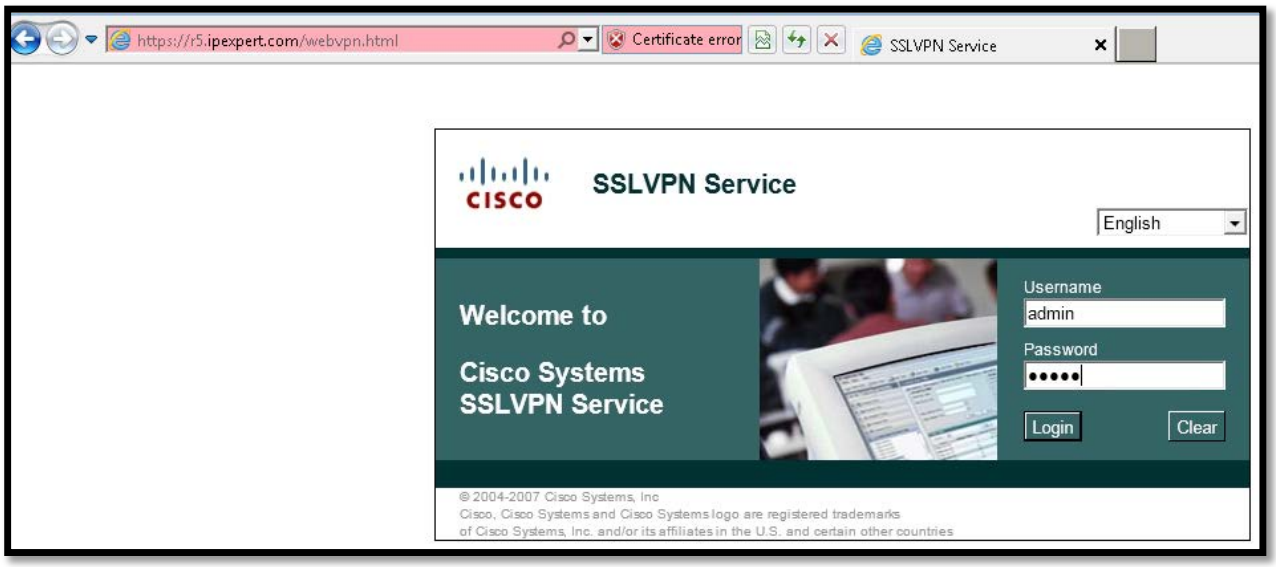
The R6's ACL could be more specific – e.g. allow only R5 to enroll but typically you don't know where the enrollment requests are going to be coming from so in this case we can leave "any". On the exam I'd be specific, especially on the security lab.

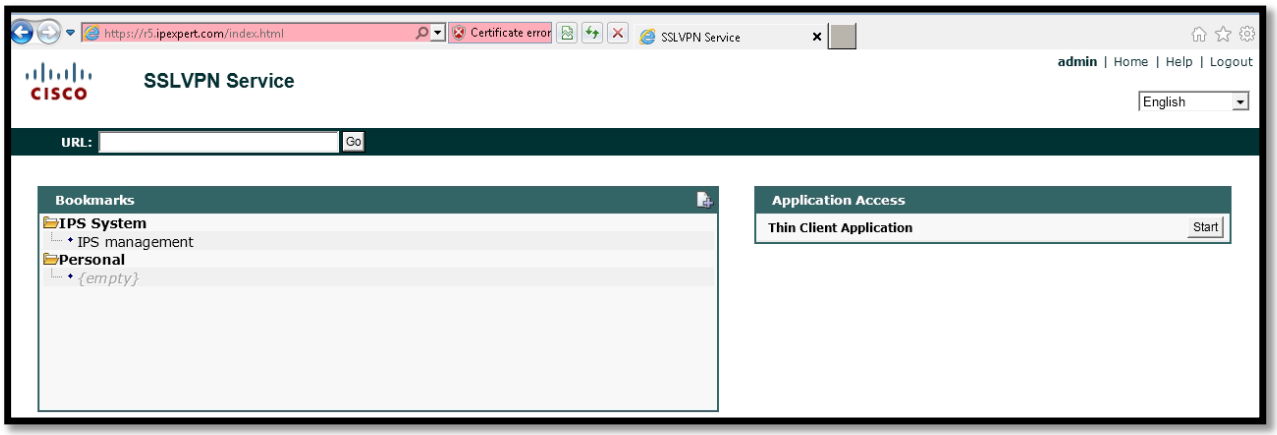
Verification

Verify if all of the settings are correct; then create a host entry (C:\Windows\System32\drivers\etc\hosts) for R5.ipexpert.com that maps to 10.2.18.5 and connect through the browser.

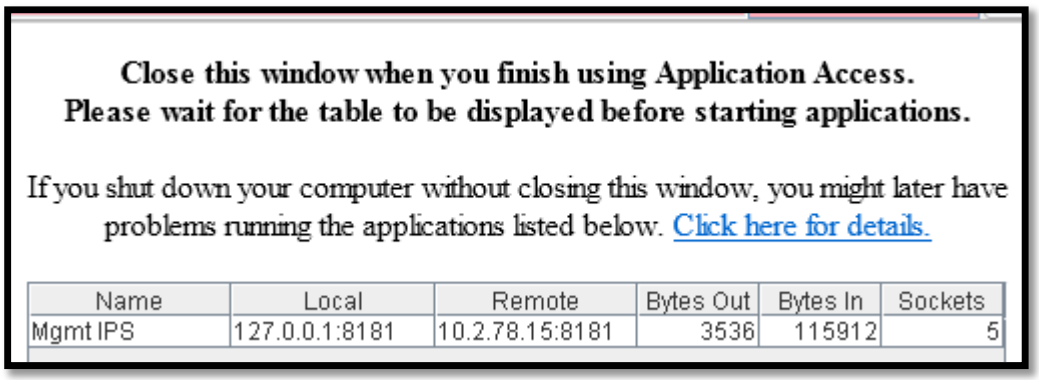
```
R5#sh webvpn gateway SSLVPNGW
Admin Status: up
Operation Status: up
Error and Event Logging: Disabled
IP: 10.2.18.5, port: 443
HTTP Redirect port: 80
SSL Trustpoint: SSLVPN_TRUST
Mangling Hostame: R5
FVRF Name not configured


R5#sh webvpn context brief

Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host

Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
SSLCON              SSLVPNGW -                 -        up    up


R5#sh web pol group SSLPOL context all
WEBVPN: group policy = SSLPOL ; context = SSLCON
      url list name = "IPSsensor"
      idle timeout = 2100 sec
      session timeout = Disabled
      port forward name = "PF_IPS"
      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
```





First try to access IPS using the URL, then using Port Forwarding :



Task 4.4: Troubleshooting Remote Access IPSec VPN (4 Points)

- An easy VPN with IPSec Dynamic Virtual Tunnel Interface have been configured on R4 to allow remote access VPN from PC host
- Two (2) faults have been inserted into R4 pre-configuration
- Correct the inserted faults and configure ASA2 and ASA3 in order to make the easy VPN connection working
- You're not authorized to modify the NAT config; also make sure that there no authentication on console access
- You should be able to ping the F0/1 interface of R4 from PC host once the VPN connection is up

Detailed Solution

ASA2

```
access-list OUTSIDE_IN permit udp any host 10.2.58.34 eq isakmp
access-list OUTSIDE_IN permit esp any host 10.2.58.34
access-list OUTSIDE_IN permit udp any host 10.2.58.34 eq 4500
```

ASA3

```
access-list OUTSIDE_IN permit udp any host 8.9.56.4 eq isakmp
access-list OUTSIDE_IN permit esp any host 8.9.56.4
access-list OUTSIDE_IN permit udp any host 8.9.56.4 eq 4500
```

R4

```
cry isa pol 1
 auth pre

int s0/0/0.2
 no ip access-group 104
```

For ASAs configuration, the challenge is to identify IP addresses that should be inserted in ACL for direction of traffic flows. If NAT was not used you would also have to make permissions on the INSIDE_IN ACL on ASA3 for returning ESP packets.

Verification

Start with connecting from the PC (after making ACL permissions on the ASA). You will see a log message saying that Aggressive Mode processing failed – enable ISAKMP debug to see why, at least errors:

```
R4#debug crypto isa error

May 28 12:17:44.971: ISAKMP:(0):no offers accepted!
May 28 12:17:44.971: ISAKMP:(0): phase 1 SA policy not acceptable! (local
8.9.56.4 remote 10.2.28.200)
May 28 12:17:44.975: ISAKMP:(0): Failed to construct AG informational
message.
May 28 12:17:44.975: ISAKMP:(0):deleting SA reason "Phase1 SA policy
proposal not accepted" state (R) AG_NO_STATE (peer 10.2.28.200)
```

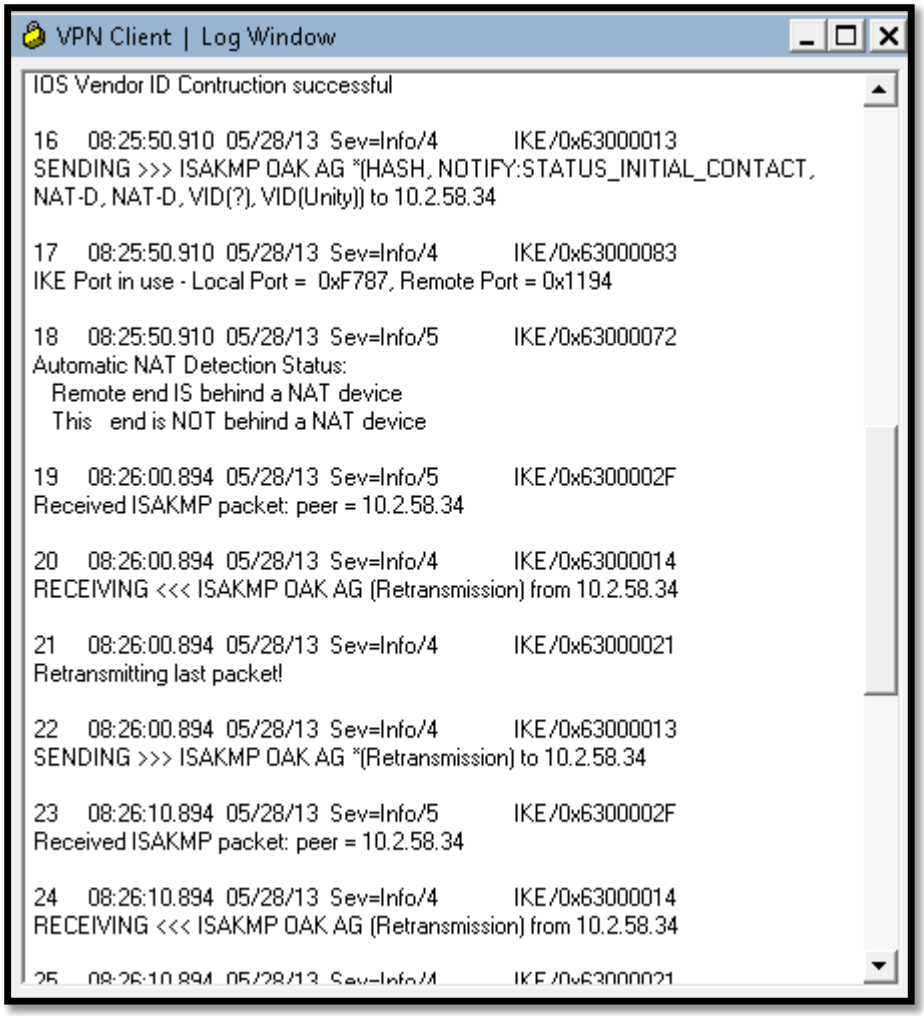
When you change the authentication method to PSK (1st fault) and connect again, you will see the negotiation simply stops at some point:

```
R4#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
8.9.56.4        10.2.28.200     AG_INIT_EXCH      1003 ACTIVE
```

Run full ISAKMP debug and troubleshoot further:

```
May 28 12:30:20.564: ISAKMP:(1004): sending packet to 10.2.28.200 my_port
500 peer_port 63300 (R) AG_INIT_EXCH
May 28 12:30:20.564: ISAKMP:(1004):Sending an IKE IPv4 Packet.
May 28 12:30:20.564: ISAKMP:(1004):Input = IKE_MESG_FROM_AAA,
PRESHARED_KEY_REPLY
May 28 12:30:20.564: ISAKMP:(1004):Old State = IKE_R_AM_AAA_AWAIT  New
State = IKE_R_AM2
```

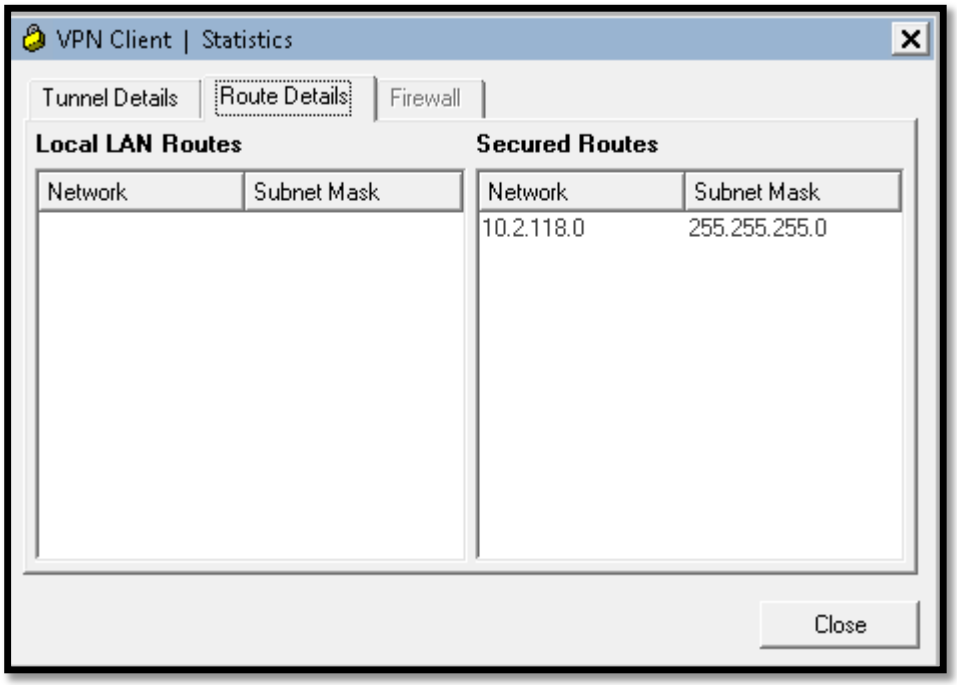
OK, looks R4 replies and then retransmission starts. What about the Client? Does it get AM_MSG2 ?

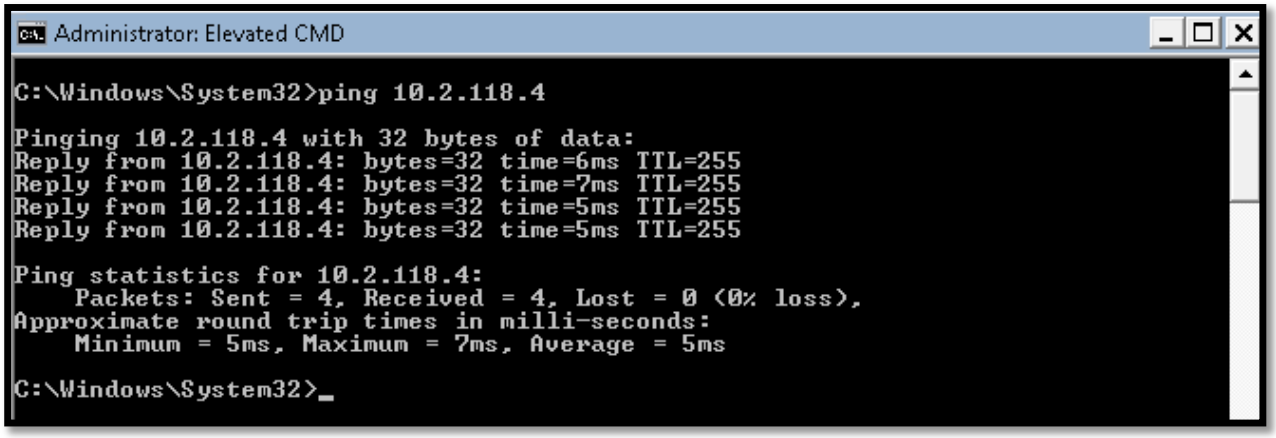


Yes, it does. It says NAT was detected and then it sends Message 3 to R4. But R4 does not get it. So Messages 1 & 2 came through but not message 3. Why? Control Plane must be fine but don't exclude problems in the data plane just because first message made it way – remember, NAT was detected which means that remaining part of the negotiation floated to UDP 4500. Both ASAs allow that, we have switch[es] between ASAs and R2/R5, those routers and then R4. So check those devices; you might also enable IP packet debug to see how far the packet goes. In our case the ACL on is blocking stuff on R4 (2nd fault).

```
R4#sh access-l
Extended IP access list 101
    10 permit ip 10.2.118.0 0.0.0.255 any
Extended IP access list 104
    10 deny esp any host 8.9.56.4
    15 deny udp any host 8.9.56.4 eq non500-isakmp (41 matches)
    20 permit ip any any (27728 matches)
```

We can either remove an entry or the entire ACL – since only VPN is blocked we can remove the whole ACL.






```
R4#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: cisco
Profile: vi
Group: cisco
Assigned address: 10.2.118.129
Uptime: 00:00:47
Session status: UP-ACTIVE
Peer: 10.2.28.200 port 62146 fvrf: (none) ivrf: (none)
      Phase1_id: cisco
      Desc: (none)
  IKEv1 SA: local 8.9.56.4/4500 remote 10.2.28.200/62146 Active
          Capabilities:CDXN connid:1006 lifetime:23:59:10
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.2.118.129
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 86 drop 0 life (KB/Sec) 4390526/3552
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4390555/3552
```

Task 4.5: Troubleshooting Site-to-Site VPN (4 Points)

- A site-to-site IPSec tunnel is preconfigured on R5 to run between ASA3 on its “outside” interface and R5 on its Fa0/0 interface, but three (3) faults have been inserted into pre-configuration
- Configure ASA3 for L2L tunnel and fix the inserted faults following these guidelines :
    - ISAKMP authentication is RSA-Sig. IPSec should use 3DES and SHA-1
    - You are required to use certificates issued by R6 configured as a CA server
    - Protected network are R5 loopback0 and CAT2 interface VLAN88
    - You are not authorized to modify ASA3 outside access-list
    - You are not allowed to add static route on ASA3 for this task
- You should be able to ping between CAT2 VLAN88 and R5 loopback0 from either side.
- All other IP traffic should be allowed as well

Detailed Solution

R2

```
no ip route 55.55.55.55 255.255.255.255 Null0
```

R5

```
crypto isakmp identity dn
```

CAT3

```
interface GigabitEthernet1/0/20
 no ip access-group 102 in
```

ASA2

```
access-list OUTSIDE_IN permit udp host 10.2.48.5 host 10.2.58.30 eq 500
access-list OUTSIDE_IN permit esp host 10.2.48.5 host 10.2.58.30
```

ASA3

```
access-list INSIDE_IN per ip host 10.2.88.22 host 55.55.55.55

ntp authentication-key 10 md5 cisco
ntp authenticate
ntp trusted-key 10
ntp server 10.2.58.7 key 10

domain-name ipexpert.com

crypto ca trustpoint VPN
 enrollment url http://10.2.18.6:80
 subject-name cn=ASA3.ipexpert.com
 crl configure

crypto ca authe VPN
crypto ca enro VPN

crypto ikev1 policy 10
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2

access-list PROXYACL permit ip host 10.2.88.22 host 55.55.55.55

crypto ipsec transform-set 3des-sha esp-3des esp-sha-hmac

tunnel-group 10.2.48.5 type ipsec-l2l
tunnel-group 10.2.48.5 ipsec-attributes
 ikev1 trust-point VPN
```

```
crypto map vpn 10 match address PROXYACL
crypto map vpn 10 set peer 10.2.48.5
crypto map vpn 10 set ikev1 transform-set 3des-sha
crypto map vpn 10 set trustpoint VPN

crypto map vpn interface outside
crypto isakmp enable outside
```

For ASAs configuration, the challenge is to identify IP addresses that should be inserted in ACL for direction of traffic flows. If NAT was not used you would also have to make permissions on the INSIDE_IN ACL on ASA3 for returning ESP packets.

Verification

We'll try to bring the tunnel up from the switch side. First thing I want to know if it has a route to the protected subnet. Here it says it will route via ASA3, which is all we want :

```
CAT2#sh ip ro 55.55.55.55
% Network not in table

CAT2#sh ip ro 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
  * 10.2.88.30
      Route metric is 0, traffic share count is 1

CAT2#ping 55.55.55.55

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 55.55.55.55, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Why I'm not surprised? OK, even if we enable ISAKMP debug on the ASA it does not try to bring up the tunnel – ACL says 0 hits :

```
ASA3(config)# sh access-l PROXYACL
access-list PROXYACL; 1 elements; name hash: 0x2f8851f3
```

```
access-list PROXYACL line 1 extended permit ip host 10.2.88.22 host
55.55.55.55 (hitcnt=0) 0x648bb49e
```

Let's see if we receive those packets at all :

```
ASA3(config)# deb icmp tr
debug icmp trace enabled at level 1
ICMP echo request from inside:10.2.88.22 to inside:55.55.55.55 ID=11 seq=0
len=72
ICMP echo request from inside:10.2.88.22 to inside:55.55.55.55 ID=11 seq=1
len=72
```

You see, the problem is ASA routes them back via inside so they never match our Crypto Map. Why does that happen? Looks like R2 is advertising this route via EIGRP :

```
ASA3(config)# sh route | in 55.55
O E2 55.55.55.55 255.255.255.255 [110/20] via 10.2.88.2, 5:42:20, inside
```

```
R2#sh ip ro 55.55.55.55
Routing entry for 55.55.55.55/32
  Known via "static", distance 1, metric 0 (connected)
  Redistributing via ospf 1
  Advertised by ospf 1 subnets
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 0, traffic share count is 1
```

After you remove it (1st fault), routing should point to R7. The following log shows up on the ASA after you ping from CAT2 :

```
%ASA-3-713020: IP = 10.2.48.5, No Group found by matching OU(s) from ID
payload:   Unknown
%ASA-3-713902: Group = 10.2.48.5, IP = 10.2.48.5, Unable to compare IKE ID
against peer cert Subject Alt Name
```

Fix by changing IKE_ID on R5 to DN (this is not a fault – if you remember about it and configured ahead you are all good). What's next :

```
%ASA-4-752012: IKEv1 was unsuccessful at setting up a tunnel.  Map Tag =
vpn.  Map Sequence Number = 10.
%ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All
configured IKE versions failed to establish the tunnel. Map Tag= vpn.  Map
Sequence Number = 10.
```

```
%ASA-4-113019: Group = 10.2.48.5, Username = 10.2.48.5, IP = 10.2.48.5,
Session disconnected. Session Type: LAN-to-LAN, Duration: 0h:00m:32s,
Bytes xmt: 140733193388032, Bytes rcv: 0, Reason: Lost Service
```

OK, this does not tell us much. Let's enable ISAKMP debug at level 7 on the ASA :

```
May 28 14:54:45 [IKEv1]Group = 10.2.48.5, IP = 10.2.48.5, PHASE 1
COMPLETED

--- Omitted ---

May 28 14:54:45 [IKEv1]Group = 10.2.48.5, IP = 10.2.48.5, Received non-
routine Notify message: No proposal chosen (14)
```

Looks like Phase II mismatch (2nd fault). Once you fix the transform set on R5 you will see at least the tunnel's up and ASA3 gets return packets from R5's loopback :

```
ASA3(config)# sh vpn-sessiondb de l2l

Session Type: LAN-to-LAN Detailed

Connection   : 10.2.48.5
Index        : 8                     IP Addr      : 10.2.48.5
Protocol     : IKEv1 IPsec
Encryption   : 3DES                  Hashing      : SHA1
Bytes Tx     : 400                   Bytes Rx     : 400
Login Time   : 15:01:16 UTC Tue May 28 2013
Duration     : 0h:00m:21s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 8.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : rsaCertificate
  Encryption   : 3DES                  Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86379 Seconds
  D/H Group    : 2
  Filter Name  :
  IPv6 Filter  :

IPsec:
```

```
  Tunnel ID    : 8.2
  Local Addr   : 10.2.88.22/255.255.255.255/0/0
  Remote Addr  : 55.55.55.55/255.255.255.255/0/0
  Encryption   : 3DES                  Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3579 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 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)   : 22 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

But CAT2 does not get any replies – even ASA can reach it :

```
ASA3(config)# deb icmp trace
debug icmp trace enabled at level 1
ICMP echo request from inside:10.2.88.22 to outside:55.55.55.55 ID=22
seq=0 len=72
ICMP echo reply from outside:55.55.55.55 to inside:10.2.88.22 ID=22 seq=0
len=72
ICMP echo request from inside:10.2.88.22 to outside:55.55.55.55 ID=22
seq=1 len=72

ASA3(config)# ping 10.2.88.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.88.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The only devices between ASA and CAT2 are the switches. Go ahead and check their config – you'll find out there's an ACL on CAT3 blocking replies from R5's loopback. Remove it and all should be good now (3rd fault).

```
CAT2#ping 55.55.55.55

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 55.55.55.55, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms

R5#ping 10.2.88.22 so l0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.88.22, timeout is 2 seconds:
Packet sent with a source address of 55.55.55.55
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

R5#telnet 10.2.88.22 /so loop0
Trying 10.2.88.22 ... Open


Password required, but none set

R5#sh cry sess int f0/0 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: FastEthernet0/0
Uptime: 00:06:35
Session status: UP-ACTIVE
Peer: 10.2.58.30 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: hostname=ASA3.ipexpert.com,cn=ASA3.ipexpert.com
      Desc: (none)
  IKEv1 SA: local 10.2.48.5/500 remote 10.2.58.30/500 Active
          Capabilities:(none) connid:1013 lifetime:23:53:24
  IPSEC FLOW: permit ip host 55.55.55.55 host 10.2.88.22
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 19 drop 0 life (KB/Sec) 4452021/3204
        Outbound: #pkts enc'ed 19 drop 0 life (KB/Sec) 4452021/3204
```

5.0 Identity Management (16 points)

Task 5.1: ACS Management (4 Points)

- Create a new password policy for ACS Administrators :
  - Password must be at least 6 character long and must be changed every 30 days
  - It cannot contain words “cisco” or “nimda” or their characters in reversed order
  - At least one alphabetic and numeric character must be part of the password
  - Disable account after 3 unsuccessful login attempts
- Create a new password policy for Users :
  - Password must be at least 6 character long
  - It cannot contain words “cisco” or “nimda” or their characters in reversed order
  - At least one alphabetic and numeric character must be part of the password
- Generate a self-signed certificate for ACS Management (only) with CN=ACS-Mgmt and O=IPexpert. Hashing function used should be SHA-1 and key size used 1024 bits
- Create a new Administrator “ReadConfig” password “IPexpert123”
- This user should be only able to read ACS configuration without the ability of configuring anything
- Restrict management connections to the ACS to only Test PC 10.2.28.200
- Make sure Test PC 10.2.28.200 can access the ACS

Detailed Solution

ASA2

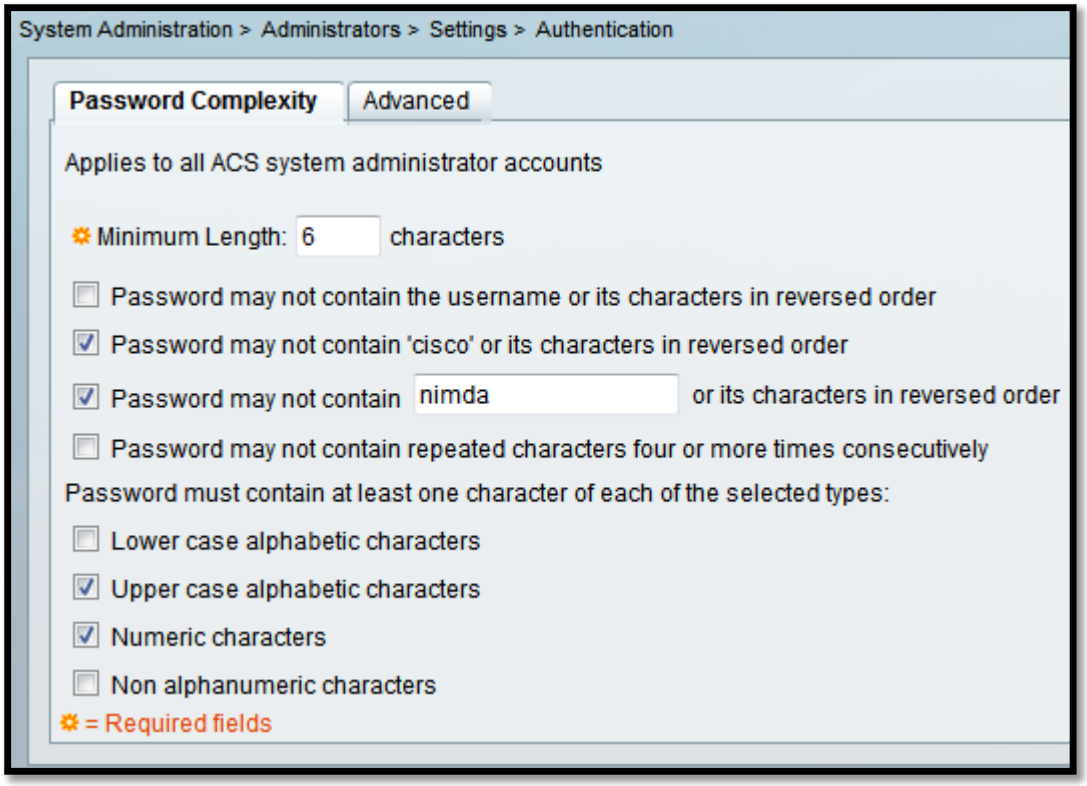
```
access-list OUTSIDE_IN permit tcp host 10.2.28.200 host 10.2.58.100 eq
https
```

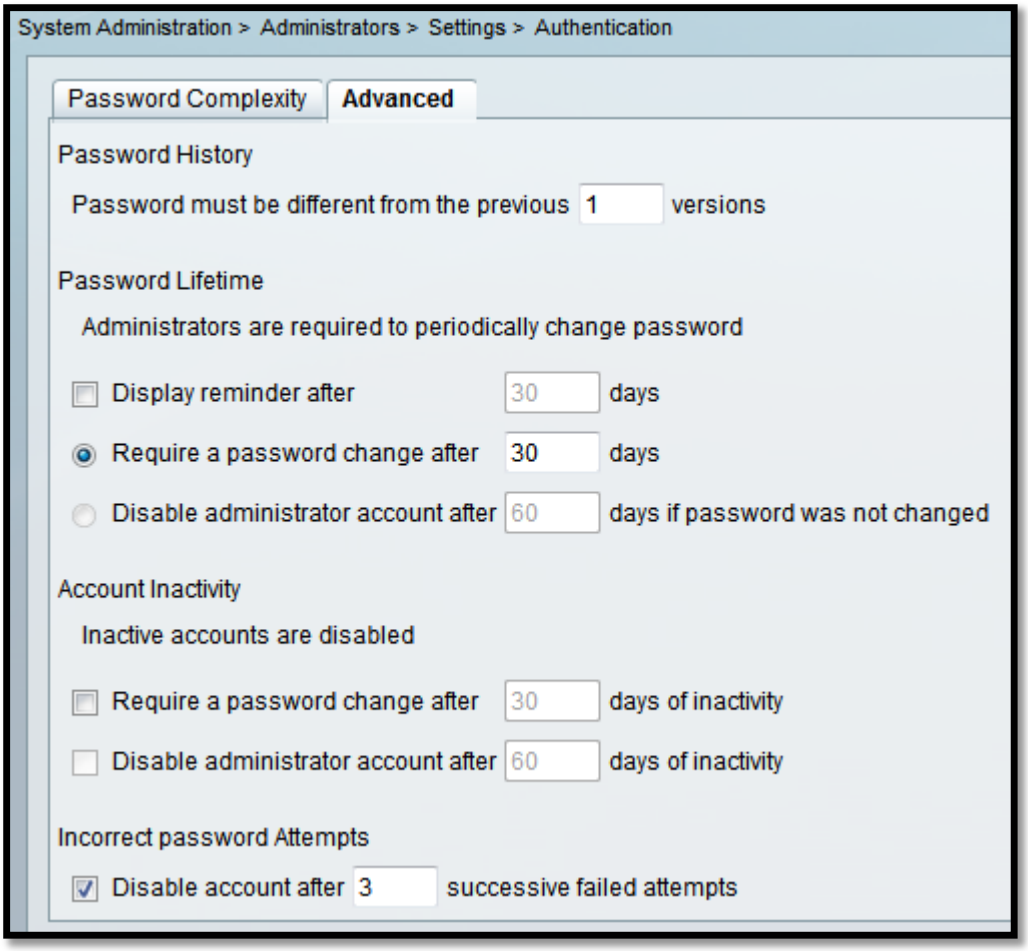
ASA3

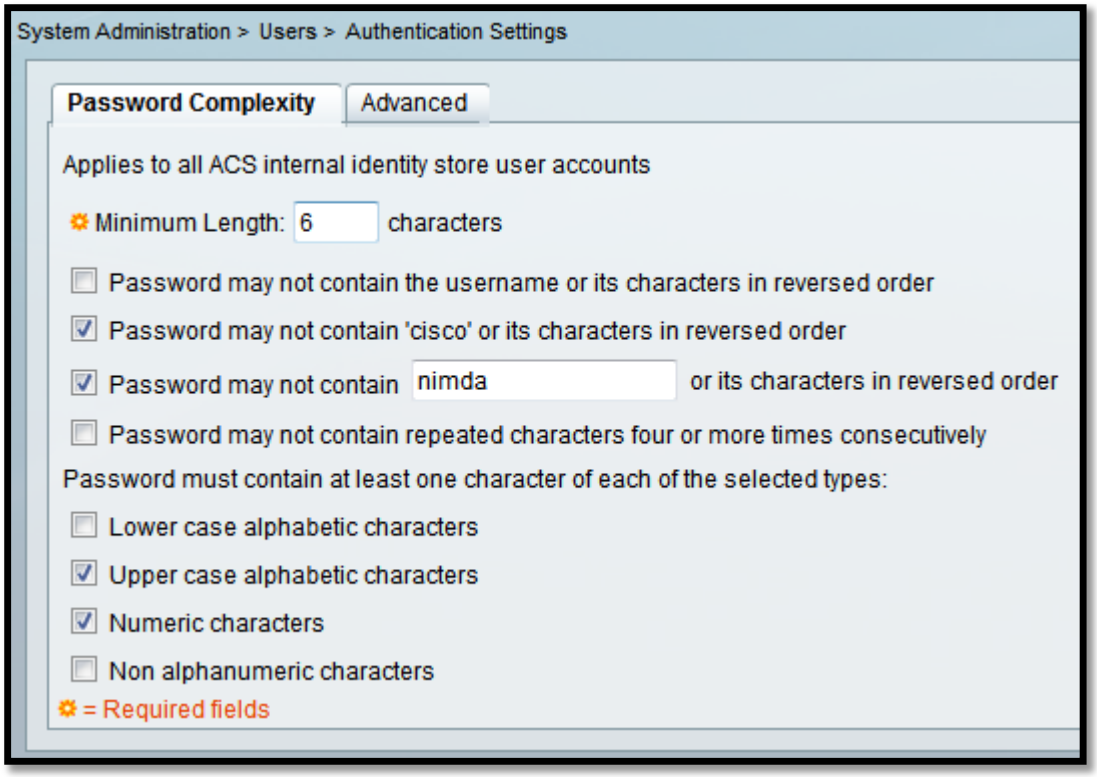
```
access-list OUTSIDE_IN permit tcp host 10.2.28.200 host 10.1.1.100 eq
https
```

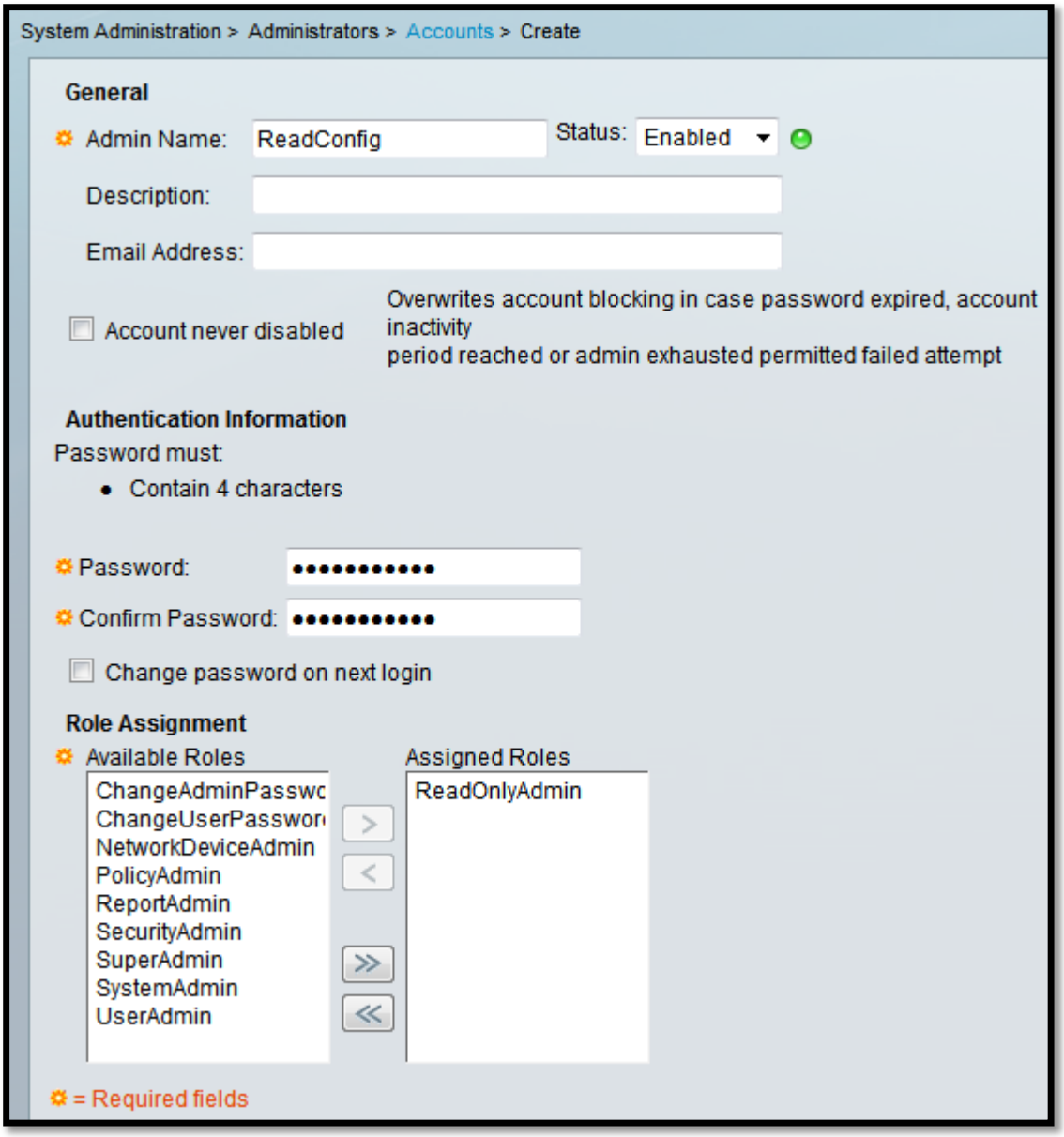
ACS

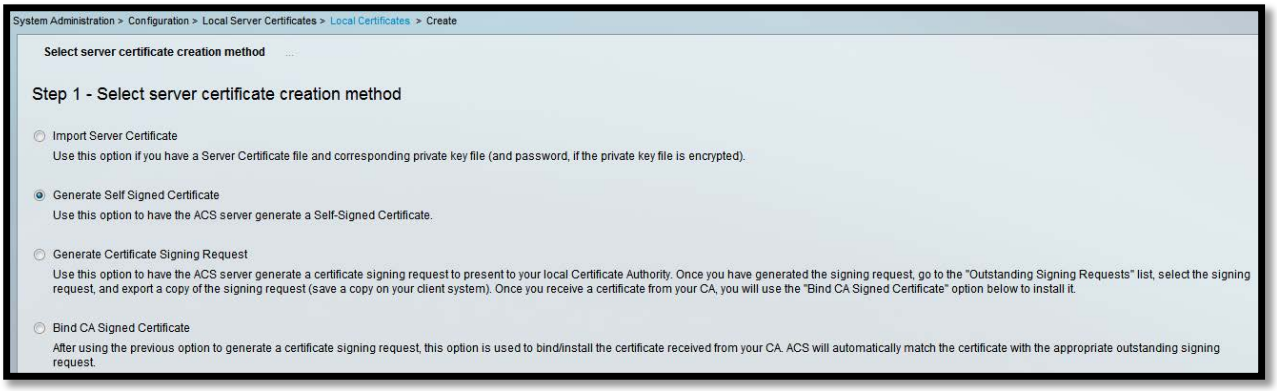
Print screens (top portion) show you how to navigate through ACS GUI to configure a particular feature.

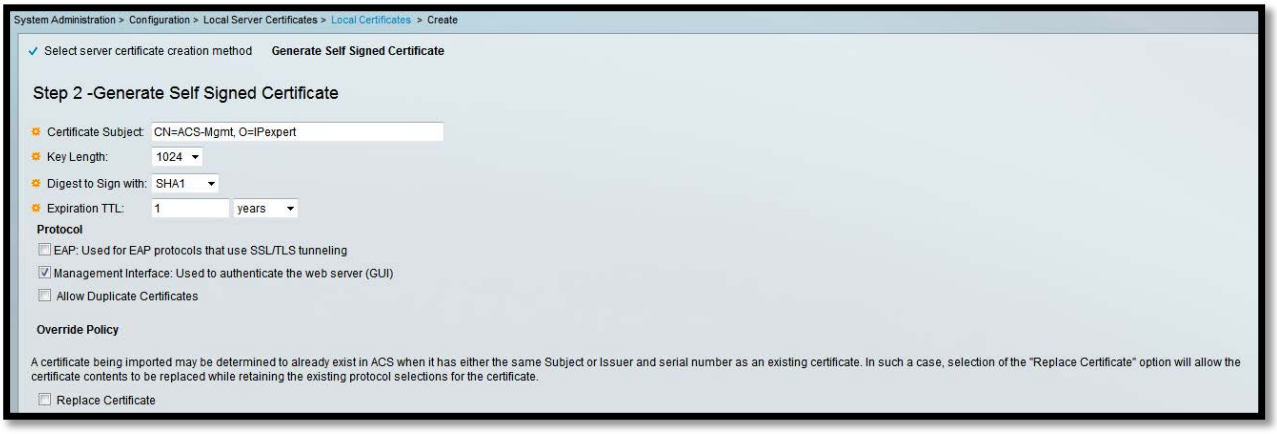








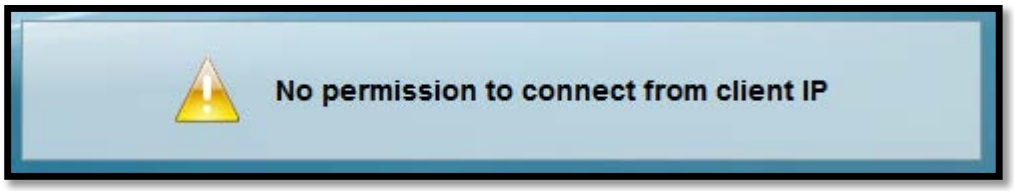




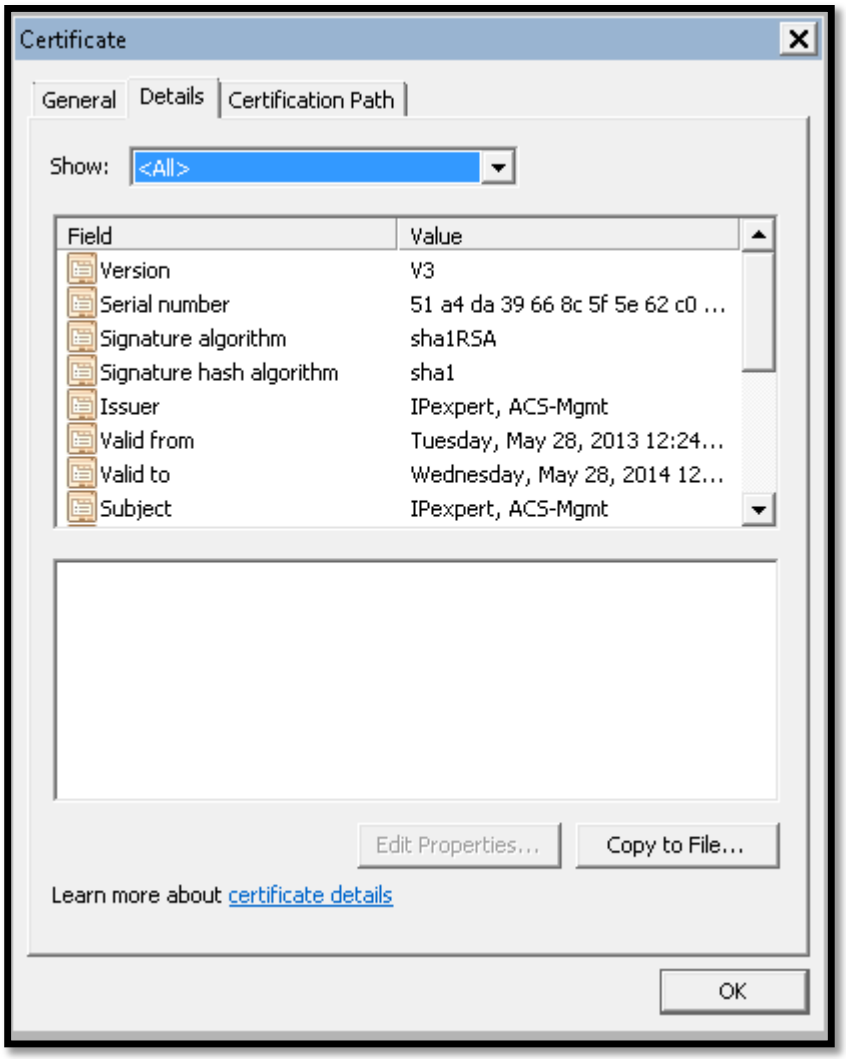
Just be familiar with where certain things can be configured on the GUI.

Verification

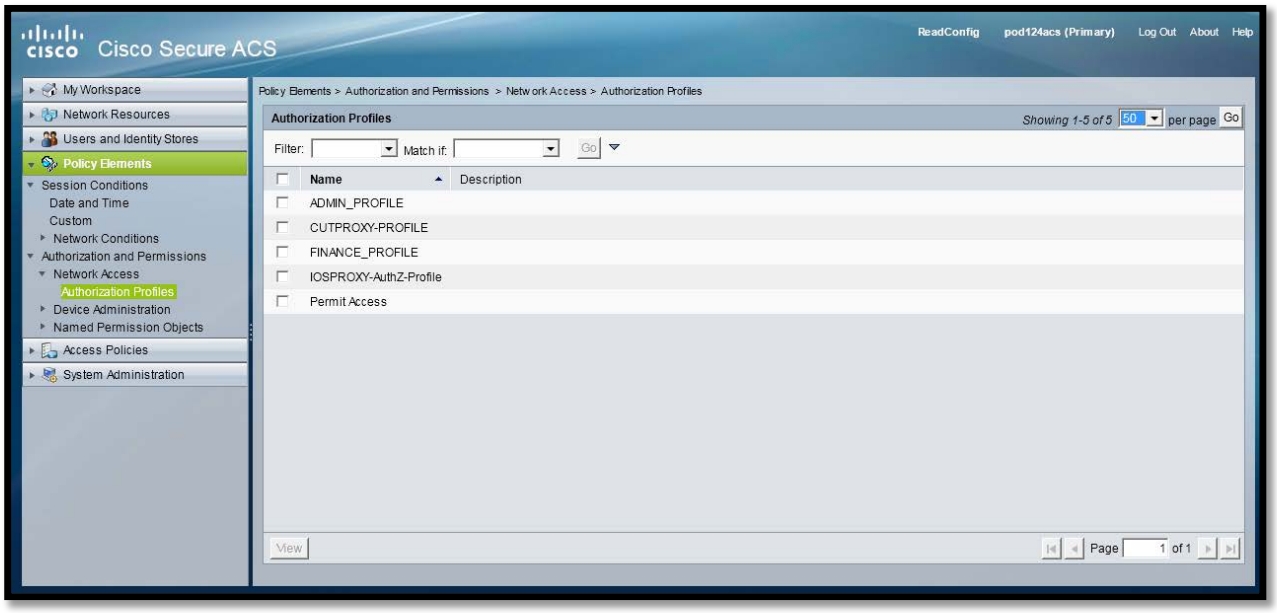
If you try to connect from an IP address different than 10.2.28.200 a following message appears:



Connect from the Test PC 10.2.28.200 - take a look at the management certificate (CN, O) :



Login as “ReadConfig” to verify read-only access:



Let's also test Account policy – login as "ReadConfig" 3 times with incorrect password :

Task 5.2: Remote Management (4 Points)

- Configure ASA3 so that users connecting using SSH will be authenticated using TACACS.
- Use "ipexpert" as the TACACS+ password. On ACS, configure the user "adminssh" with the password "IPexpert123"
- Also, configure CAT3 for telnet access such that:
    - The first session will authenticate with only password for EXEC ("ipexpert")
    - The second sessions will be prompted for username and password on ACS server – username "admincat3" and password "IPexpert123" using TACACS+
    - The third session will be authenticated locally. Use "adminloc" with password for this purpose "ipexpert"
    - No matter what session was used to access the device a user should be able to connect to the Privileged-EXEC mode using password "ipexpert"
- From R2 start a SSH session on ASA3 inside interface and verify that you are connected with "adminssh"
- From R2 start a telnet session on CAT3 and verify that you are prompted for password

only. Then start another telnet session and verify that you are authenticating with the user: “admincat3” from ACS server

- Establish again a third session and verify that you are connecting using the account : “adminloc” with password: ipexpert

Detailed Solution

Note : If you experience any problems with ACS at this point (e.g. Monitoring Dashboard does not work) go under Local Certificates and revert to the previous management certificate. Click on podxxxacs and then check **“Management Interface: Used to authenticate the web server (GUI)”.** Restart ACS from the CLI (application stop acs, application start acs).

ASA3

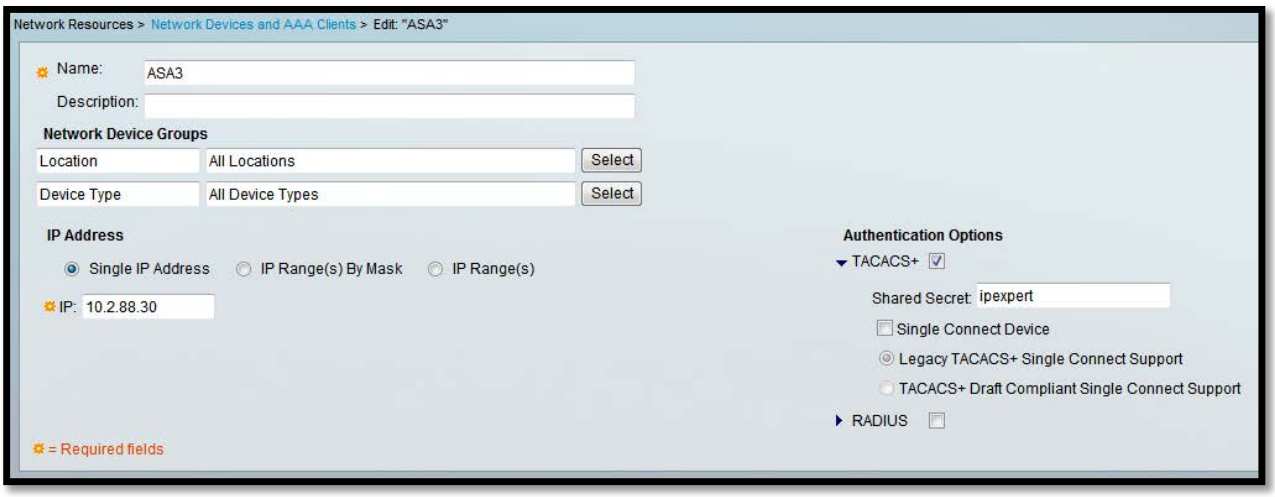
```
aaa-server ACS protocol tacacs+
aaa-server ACS (inside) host 10.1.1.100
 key ipexpert

ssh 0.0.0.0 0.0.0.0 inside
aaa authentication ssh console ACS
```

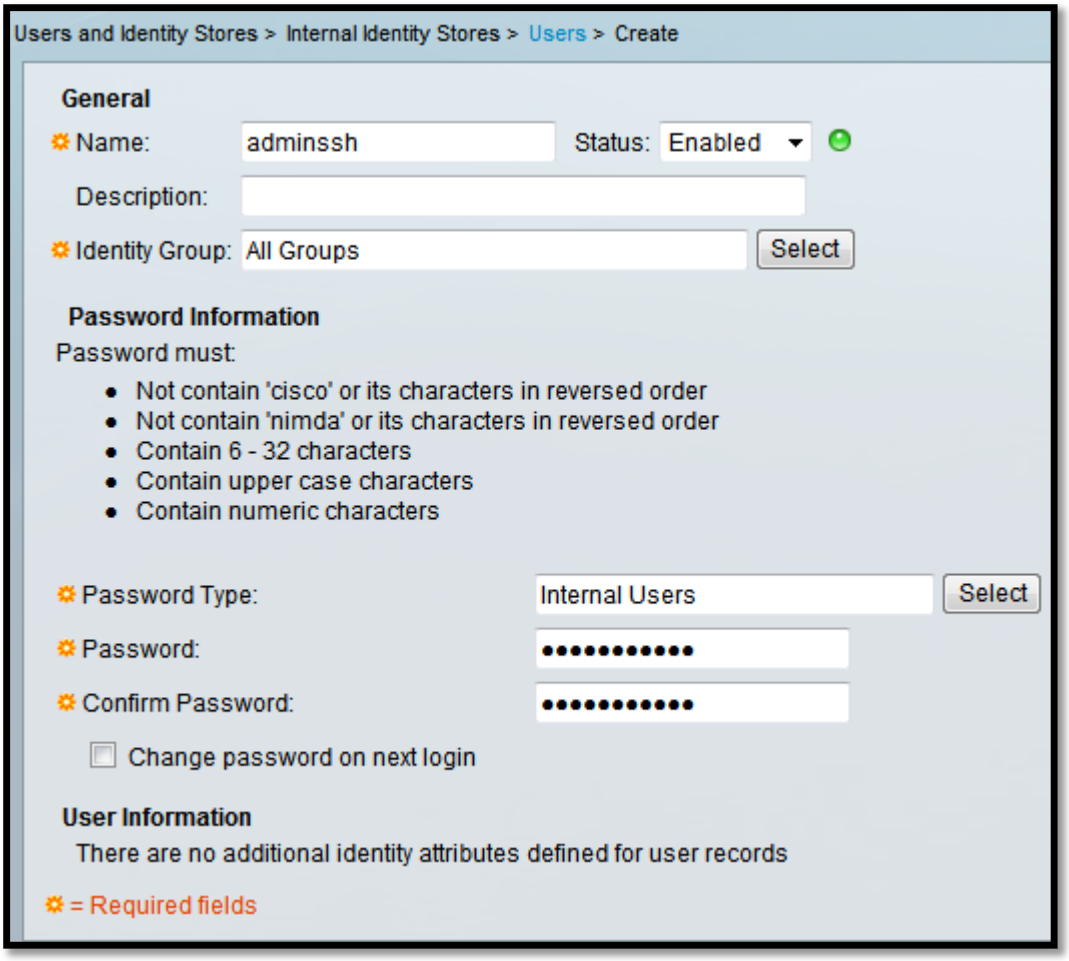
CAT3

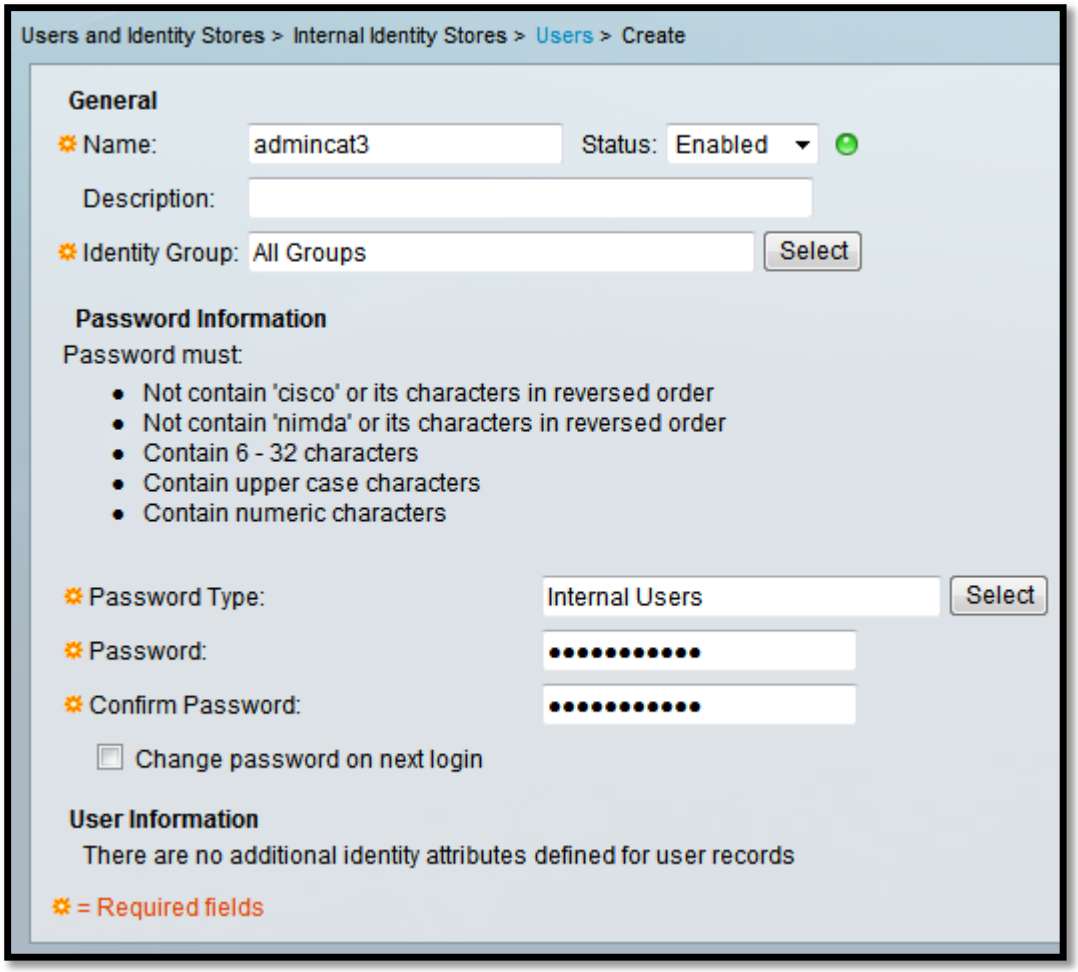
```
enable password ipexpert
username adminloc password 0 ipexpert

aaa new-model
aaa authentication login NO none
aaa authentication login ACS group tacacs+
aaa authentication login VTYLINE line
aaa authentication login VTYLOC local
aaa authentication enable default enable

tacacs server ACS
 address ipv4 10.1.1.100
 key ipexpert

line con 0
 login authentication NO

line vty 0
```

```
 password ipexpert
 login authentication VTYLINE
line vty 1
 login authentication ACS
line vty 2
 login authentication VTYLOC
```

ACS







Configurations are pretty straightforward. You should paid attention on what line number you are configuring to respect task guideline.

Verification

```
R2#ssh -l adminssh 10.2.88.30

Password:

ASA3>
```

```
R2#telnet 10.2.98.23
Trying 10.2.98.23 ... Open


User Access Verification

Password:

CAT3>ena
Password:
CAT3#

R2#telnet 10.2.98.23
Trying 10.2.98.23 ... Open

Username: admincat3
Password:

CAT3>ena
Password:
CAT3#

R2#telnet 10.2.98.23
Trying 10.2.98.23 ... Open


User Access Verification

Username: adminloc
Password:

CAT3>ena
Password:
CAT3#who
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:03:06
   1 vty 0                 idle                 00:00:42 10.2.98.2
   2 vty 1     admincat3   idle                 00:00:14 10.2.98.2
```

```
*  3 vty 2      adminloc    idle                 00:00:00 10.2.98.2

  Interface     User               Mode         Idle     Peer Address
```

Task 5.3: Proxy Authentication - IOS (4 Points)

- Configure R4 (F0/1) to perform auth-proxy when candidate PC is trying to manage the IPS on URL link: http://10.2.78.15:8181
- Configure the auth-proxy banner to say “IPS management authentication”
- Configure a auth-proxy cache time of 10 minutes
- Use interface F0/1 of R4 for RADIUS client
- Create a username : adminips and password : IPexpert123
- After successful authentication access to the IPS should be granted
- To test the IPS management access through the auth-proxy, change the VLAN of PC Host to VLAN 118, configure network IP address as 10.2.118.200 without a default gateway and add the following route in DOS command: route add 10.2.0.0 mask 255.255.0.0 10.2.118.4

Detailed Solution

ASA3

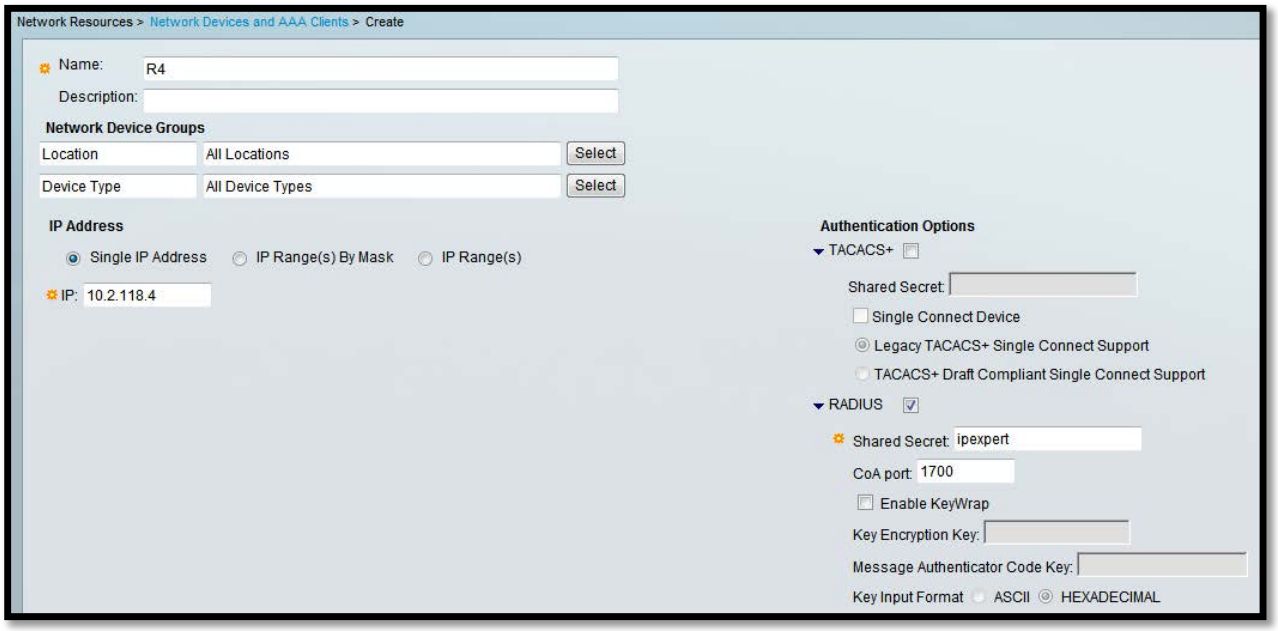
```
router ospf 1
 network 10.2.78.30 255.255.255.255 area 50

access-list INSIDE_IN permit tcp host 10.2.118.200 host 10.2.78.15 eq 8181
```

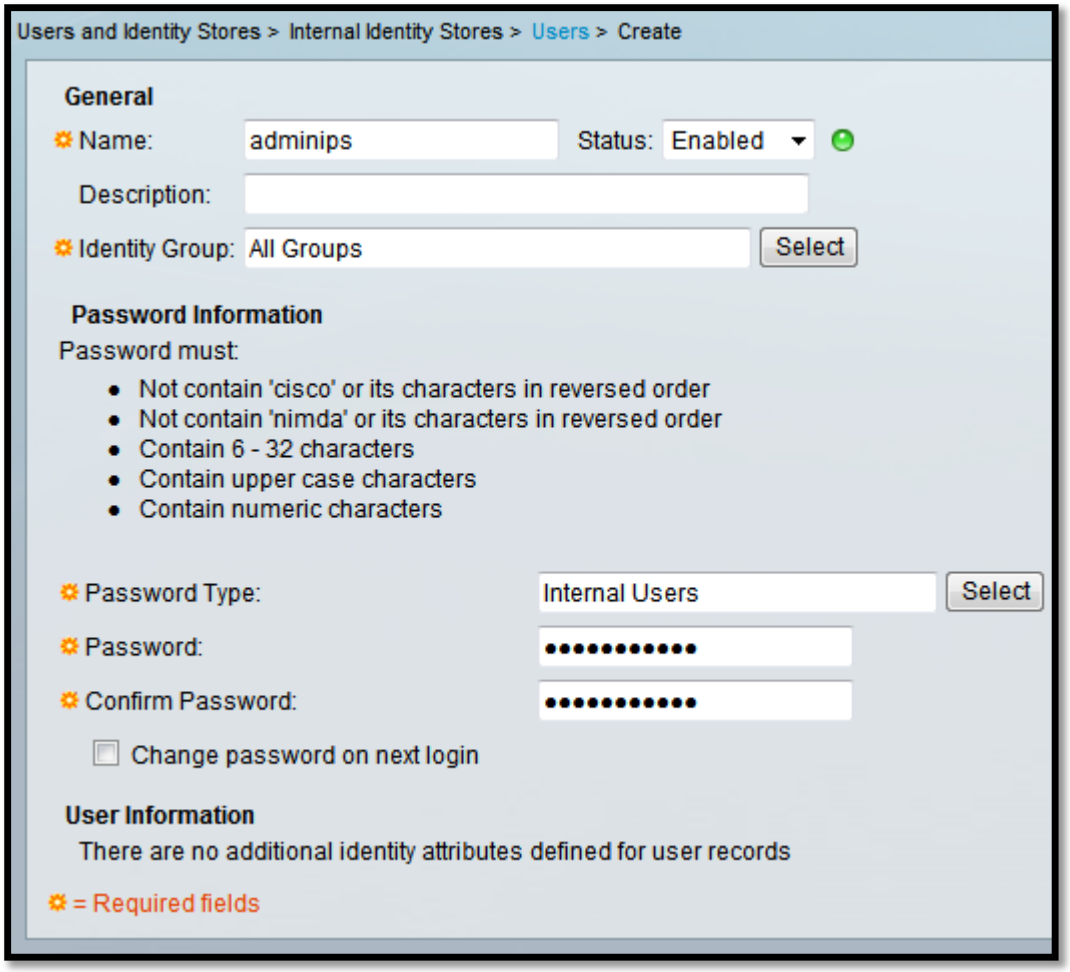
R4

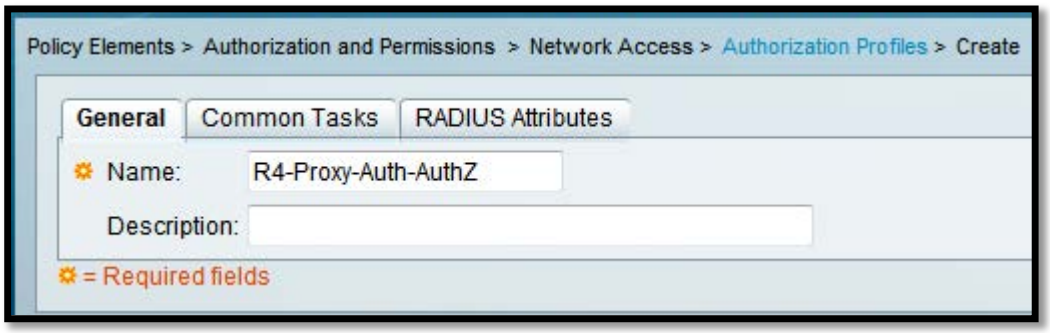
```
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
```

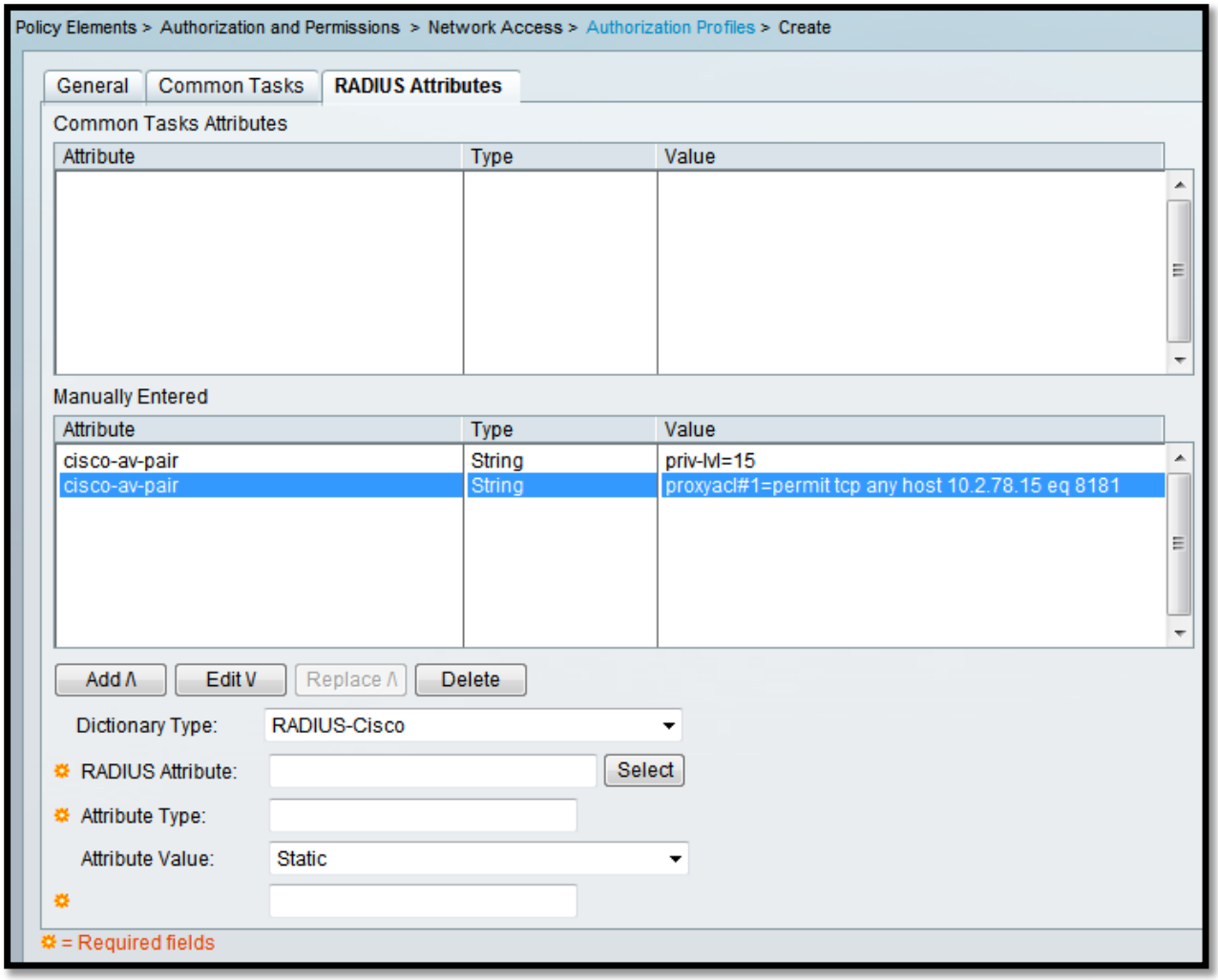
```
radius-server host 10.1.1.100 key ipexpert
ip radius source f0/1

ip admission auth-proxy-banner http % IPS management authentication %
ip admission inactivity-timer 10
ip admission name AUTHP proxy http inactivity-time 10

ip port-map http port tcp 8181

ip http server
ip http port 8181

access-list 102 deny ip any any log

interface FastEthernet0/1
 ip access-group 102 in
 ip admission AUTHP
```

ACS

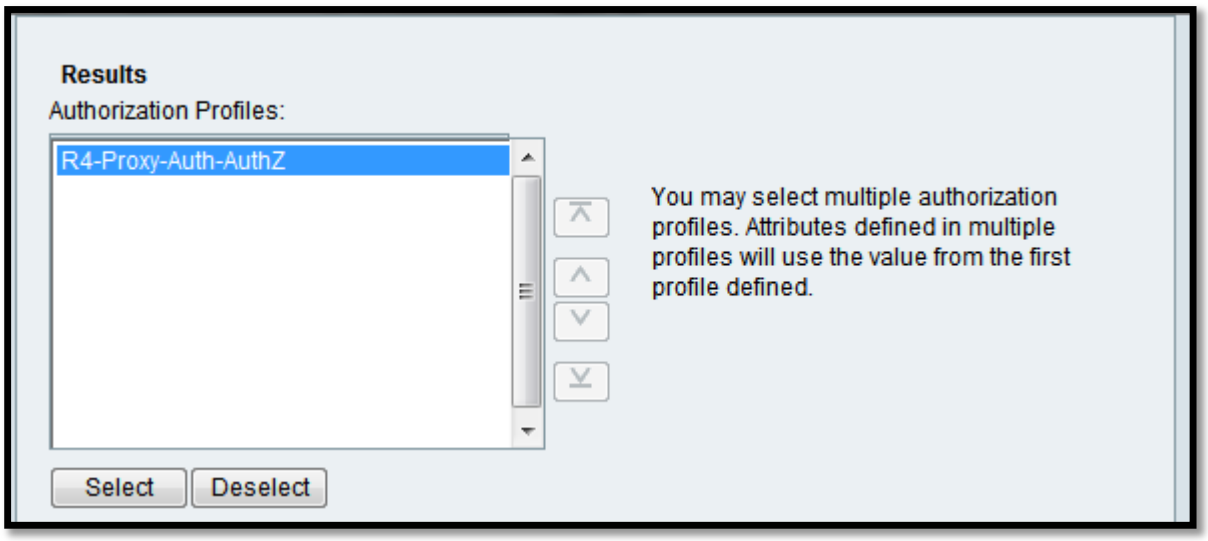


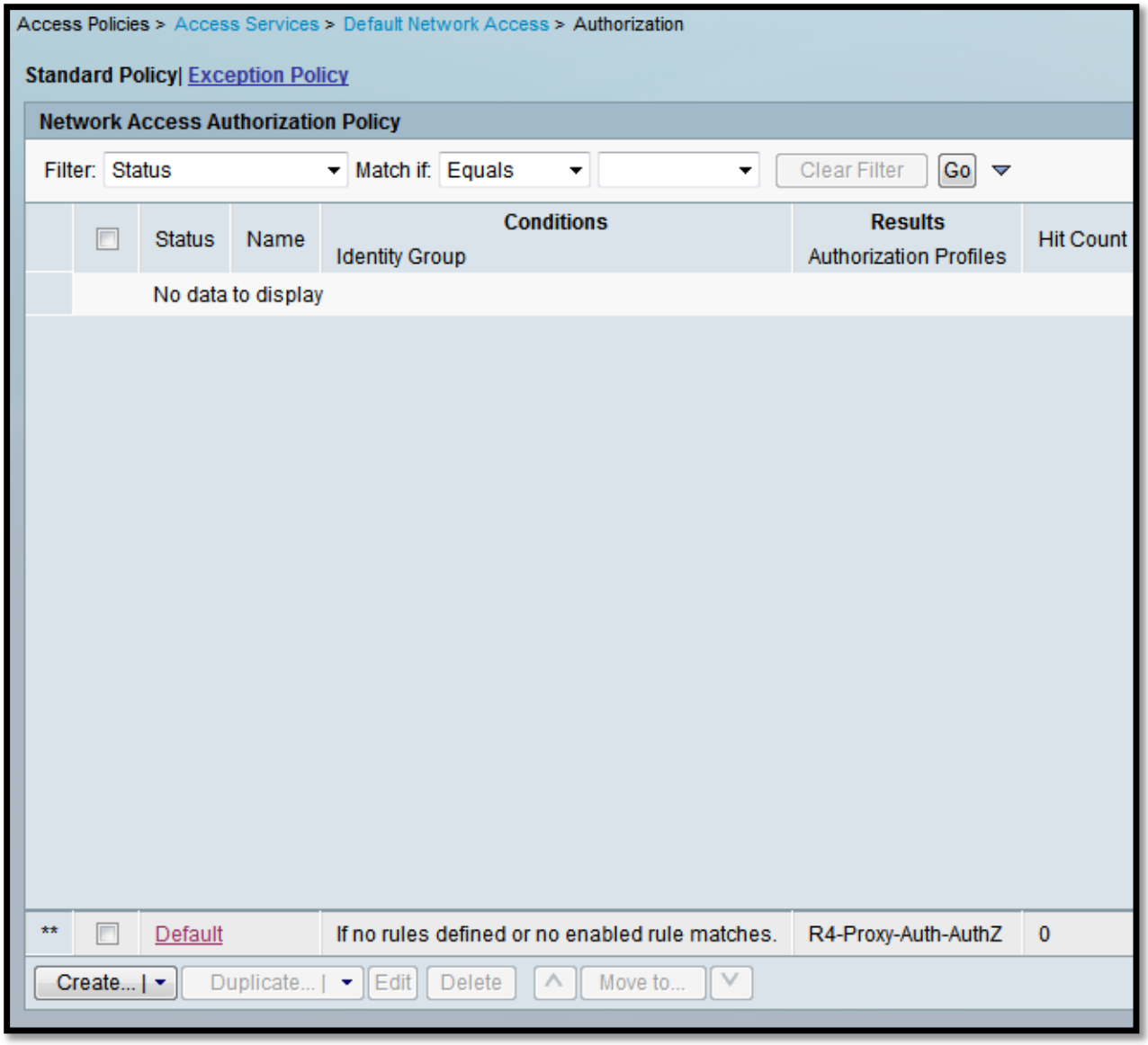






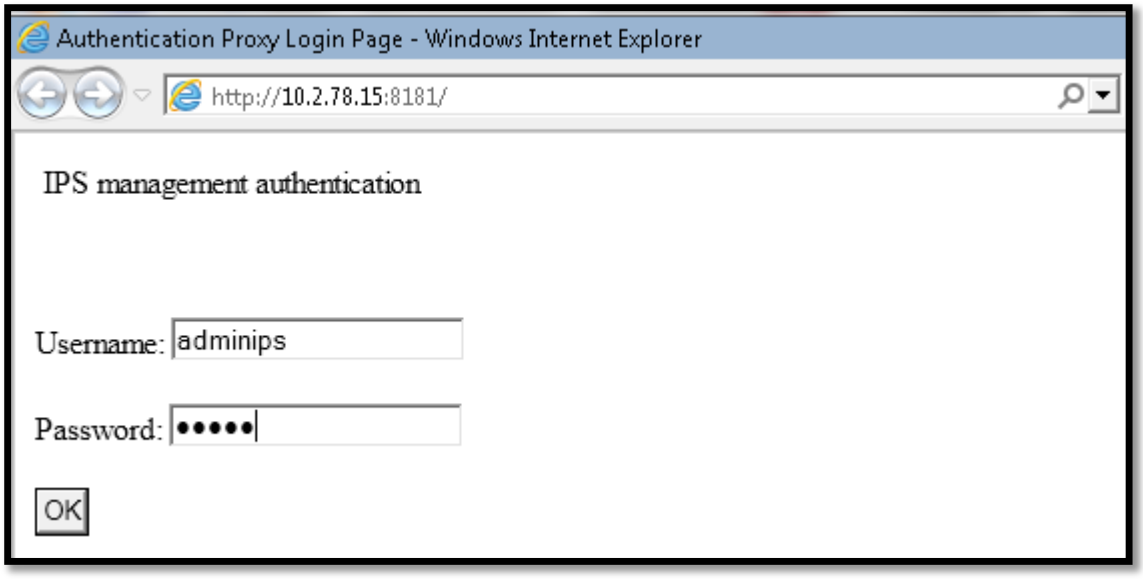
Now modify the Default Rule's Authorization Profile :





ACL 102 could also only deny traffic to the IPS and permit everything else. We actually don't care here since this segment is only connected to the Test PC and its only role, at least at this point, is to access IPS after successful authentication.

Verification




```
R4#sh ip auth-proxy cache
Authentication Proxy Cache
 Client Name adminips, Client IP 10.2.118.200, Port 51665, timeout 10,
Time Remaining 10, state ESTAB


R4#sh access-l 102
Extended IP access list 102
```

```
        permit tcp host 10.2.118.200 host 10.2.78.15 eq 8181 (86 matches)
      20 deny ip any any log (323 matches)
```

Task 5.4: Lightweight Directory Access Protocol - IOS (4 Points)

- After a major migration by system administrators, a new powerful Microsoft LDAP server has been installed in your company so, you have been asked to authenticate and authorize incoming VPN users on the ASA3 according to the following parameters :
  - LDAP server IP : 10.1.1.101
  - LDAP Administrator : Administrator
  - LDAP Administrator password: IPexpert123
  - Finance department (Group) : CN=FINANCE,CN=Users,DC= ipexpert,DC=com
  - Technical department (Group): CN=IPx_Admins,CN=Users,DC= ipexpert,DC=com
  - Finance users (e.g. FINUSER1//cisco) should be assigned to the ASA3 group policy "FINANCE"
  - Technical users (e.g. IPx_admin1//IPexpert123) should be assigned to the ASA3 group policy "ADMIN"
- Deactivate the LDAP server after 4 failed attempts to authenticate to the LDAP server; the reactivation will occurs after 30 seconds
- Add a static route on the AD server so it can talk to the ASA

Detailed Solution

AD

```
route add 10.2.0.0 mask 255.255.0.0 10.1.1.1
```

ASA3

```
aaa-server LDAP protocol ldap
 reactivation-mode timed
 max-failed-attempts 4

ldap attribute-map LDAP_MAP
  map-name  memberOf Group-Policy
  map-value memberOf CN=FINANCE,CN=Users,DC=ipexpert,DC=com FINANCE
  map-value memberOf CN=IPx_Admins,CN=Users,DC=ipexpert,DC=com ADMIN

aaa-server LDAP (inside) host 10.1.1.101
```

```
ldap-base-dn DC=ipexpert,DC=com
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password IPexpert123
ldap-login-dn CN=Administrator,CN=users,DC=ipexpert,DC=com
server-type microsoft
ldap-attribute-map LDAP_MAP
```

Note that LDAP server type is Microsoft so server-type option is needed, be careful with all task words.

Watch out for all DNs, they ARE case-sensitive.

To figure out the LDAP Naming Attribute (sAMAccountName) use ASA documentation – go under “Reference” -> “Configuring an External Server for Security Appliance User Authorization” and then “Searching the LDAP Hierarchy“.

Verification

For verification of this task configure ASA3 for Telnet (inside) using LDAP server for authentication.

```
ASA3(config)# telnet 0.0.0.0 0.0.0.0 inside
ASA3(config)# aaa authentication telnet console LDAP


ASA3(config)# deb ldap 10

R2#telnet 10.2.88.30
Trying 10.2.88.30 ... Open


User Access Verification

Username: FINUSER1
Password: *****

ASA3>
```

```
[17] Session Start
[17] New request Session, context 0x00007fff2e7a6d48, reqType =
Authentication
[17] Fiber started
[17] Creating LDAP context with uri=ldap://10.1.1.101:389
[17] Connect to LDAP server: ldap://10.1.1.101:389, status = Successful
[17] supportedLDAPVersion: value = 3
[17] supportedLDAPVersion: value = 2
[17] Binding as Administrator
[17] Performing Simple authentication for Administrator to 10.1.1.101
[17] LDAP Search:
        Base DN = [DC=ipexpert,DC=com]
        Filter  = [sAMAccountName=FINUSER1]
        Scope   = [SUBTREE]
[17] User DN = [CN=FINUSER1,CN=Users,DC=ipexpert,DC=com]
[17] Talking to Active Directory server 10.1.1.101
[17] Reading password policy for FINUSER1,
dn:CN=FINUSER1,CN=Users,DC=ipexpert,DC=com
[17] Read bad password count 0
[17] Binding as FINUSER1
[17] Performing Simple authentication for FINUSER1 to 10.1.1.101
[17] Processing LDAP response for user FINUSER1
[17] Message (FINUSER1):
[17] Authentication successful for FINUSER1 to 10.1.1.101
[17] Retrieved User Attributes:
[17]    objectClass: value = top
[17]    objectClass: value = person
[17]    objectClass: value = organizationalPerson
[17]    objectClass: value = user
[17]    cn: value = FINUSER1
[17]    givenName: value = FINUSER1
[17]    distinguishedName: value = CN=FINUSER1,CN=Users,DC=ipexpert,DC=com
[17]    instanceType: value = 4
[17]    whenCreated: value = 20101119110913.0Z
[17]    whenChanged: value = 20130529160506.0Z
[17]    displayName: value = FINUSER1
[17]    uSNCreated: value = 33374
[17]    memberOf: value = CN=FINANCE,CN=Users,DC=ipexpert,DC=com
[17]            mapped to Group-Policy: value = FINANCE
[17]            mapped to LDAP-Class: value = FINANCE
[17]    memberOf: value = CN=Domain Admins,CN=Users,DC=ipexpert,DC=com
```

```
[17]            mapped to Group-Policy: value = CN=Domain
Admins,CN=Users,DC=ipexpert,DC=com
[17]            mapped to LDAP-Class: value = CN=Domain
Admins,CN=Users,DC=ipexpert,DC=com
[17]    memberOf: value = CN=Remote Desktop
Users,CN=Builtin,DC=ipexpert,DC=com
[17]            mapped to Group-Policy: value = CN=Remote Desktop
Users,CN=Builtin,DC=ipexpert,DC=com
[17]            mapped to LDAP-Class: value = CN=Remote Desktop
Users,CN=Builtin,DC=ipexpert,DC=com
[17]    memberOf: value = CN=Administrators,CN=Builtin,DC=ipexpert,DC=com
[17]            mapped to Group-Policy: value =
CN=Administrators,CN=Builtin,DC=ipexpert,DC=com
[17]            mapped to LDAP-Class: value =
CN=Administrators,CN=Builtin,DC=ipexpert,DC=com
[17]    uSNChanged: value = 1595300
[17]    name: value = FINUSER1
[17]    objectGUID: value = %..V..OL....j...
[17]    userAccountControl: value = 66048
[17]    badPwdCount: value = 0
[17]    codePage: value = 0
[17]    countryCode: value = 0
[17]    badPasswordTime: value = 0
[17]    lastLogoff: value = 0
[17]    lastLogon: value = 129349363213130390
[17]    pwdLastSet: value = 129346385536411640
[17]    primaryGroupID: value = 513
[17]    objectSid: value = ................!..(...y...
[17]    adminCount: value = 1
[17]    accountExpires: value = 9223372036854775807
[17]    logonCount: value = 1
[17]    sAMAccountName: value = FINUSER1
[17]    sAMAccountType: value = 805306368
[17]    userPrincipalName: value = FINUSER1@ipexpert.com
[17]    objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ipexpert,DC=com
[17]    dSCorePropagationData: value = 20101119113026.0Z
[17]    dSCorePropagationData: value = 16010101000000.0Z
[17]    lastLogonTimestamp: value = 130143171060908004
[17] Fiber exit Tx=537 bytes Rx=2695 bytes, status=1
```

Now login as “IPx_admin1”:

```
R2#telnet 10.2.88.30
Trying 10.2.88.30 ... Open


User Access Verification

Username: IPx_admin1
Password: ***********
Type help or '?' for a list of available commands.
ASA3>

[18] Session Start
[18] New request Session, context 0x00007fff2e7a6d48, reqType =
Authentication
[18] Fiber started
[18] Creating LDAP context with uri=ldap://10.1.1.101:389
[18] Connect to LDAP server: ldap://10.1.1.101:389, status = Successful
[18] supportedLDAPVersion: value = 3
[18] supportedLDAPVersion: value = 2
[18] Binding as Administrator
[18] Performing Simple authentication for Administrator to 10.1.1.101
[18] LDAP Search:
        Base DN = [DC=ipexpert,DC=com]
        Filter  = [sAMAccountName=IPx_admin1]
        Scope   = [SUBTREE]
[18] User DN = [CN=IPx_admin1,CN=Users,DC=ipexpert,DC=com]
[18] Talking to Active Directory server 10.1.1.101
[18] Reading password policy for IPx_admin1,
dn:CN=IPx_admin1,CN=Users,DC=ipexpert,DC=com
[18] Read bad password count 0
[18] Binding as IPx_admin1
[18] Performing Simple authentication for IPx_admin1 to 10.1.1.101
[18] Processing LDAP response for user IPx_admin1
[18] Message (IPx_admin1):
[18] Authentication successful for IPx_admin1 to 10.1.1.101
[18] Retrieved User Attributes:
[18]    objectClass: value = top
[18]    objectClass: value = person
[18]    objectClass: value = organizationalPerson
```

```
[18]    objectClass: value = user
[18]    cn: value = IPx_admin1
[18]    c: value = PL
[18]    l: value = Warsaw
[18]    givenName: value = IPx_admin1
[18]    distinguishedName: value =
CN=IPx_admin1,CN=Users,DC=ipexpert,DC=com
[18]    instanceType: value = 4
[18]    whenCreated: value = 20121227172813.0Z
[18]    whenChanged: value = 20130520192009.0Z
[18]    displayName: value = IPx_admin1
[18]    uSNCreated: value = 12779
[18]    memberOf: value = CN=IPx_Admins,CN=Users,DC=ipexpert,DC=com
[18]            mapped to Group-Policy: value = ADMIN
[18]            mapped to LDAP-Class: value = ADMIN
```

6.0 Advanced Security (16 points)

Task 6.1: Resource Protection (4 Points)

- Configure R6 to stamp log messages with a sequence number
- Configure R6 to display up to 7200 messages an hour on console
- Configure R1 to accept management traffic only through interface F0/0
- Configure R1 to accept only SSH as management protocol - do not configure lines or access-list to do that
- Configure R1 to log all incoming management traffic from VLAN68, every 20 seconds
- Ensure that you have SSH access to R1 from R4

Detailed Solution

R6

```
service sequence-numbers
logging rate-limit console 2
```

R1

```
class-map type logging match-all FROMASA2
 match input-interface FastEthernet0/0

policy-map type logging FROMASA2
 class FROMASA2
   log interval 20000

control-plane host
 management-interface FastEthernet0/0 allow ssh http
 service-policy type logging input FROMASA2

cry key generate rsa mod 1024
```

For command “management-interface” in control-plane do not forget to open HTTP in addition to SSH - otherwise the R1 webserver will be broken, Task 1.3.

Verification

```
R6#
000229: May 30 10:43:27.792: %SYS-5-CONFIG_I: Configured from console by
console
```

Then generate a bunch of logs (e.g. shut f0/0) and check with “show logging”:

```
R6#sh loggi
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 367 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
```

```
                    filtering disabled
    Buffer logging:  level debugging, 331 messages logged, xml disabled,
                   filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
--- Omitted ---

R1#sh control-plane host features
Control plane host path features :

------------------------------------------------------
Control-plane Logging activated May 30 2013 10:4
Management-Interface activated May 30 2013 10:4

------------------------------------------------------

R1#sh ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQC0zYibLvLgOyUe9CqutT6hDXyjUhX5kDSgM400lTmZ
VWpu7RLi3xUNf9EW17ak2sQwYaizJUKmtNFdMIULfatAOlWWxeb5KaQ5iCPK4JuTw7ycHSGZSi
5m756Q
suhvW6STDAYt20pFkag3tkbxI6goa+F8YvhiFP7EejuYu/W6pw==

R4#ssh -l cisco 10.2.68.1

Password:

R1>

*May 30 10:48:54.557: %CP-6-TCP: PERMIT  8.9.56.4(56298) -> 10.2.68.1(22)

R1#sh management-interface f0/0
Management interface FastEthernet0/0
        Protocol        Packets processed
            http                 0
             ssh                73
```

```
R1#sh policy-map type logging control-plane host

 Control Plane Host

  Service-policy logging input: FROMASA2

    Class-map: FROMASA2 (match-all)
      21 packets, 1260 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: input-interface FastEthernet0/0
      log interval 20000

    Class-map: class-default (match-any)
      69 packets, 6152 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 6.2: Troubleshooting NTP (4 Points)

- For time synchronization purposes, an NTP server has been configured on R7
- R1, R2 and R4 have been configured as NTP clients but they will not synchronize with R7
- There were few faults introduced to their config and you are supposed to fix them
- NTP authentication password is “cisco”
- Do not modify any NTP or NTP-related configuration on the time server R7

Detailed Solution

R1

```
ntp source F0/0
no ntp authentication-key 10

ntp authentication-key 10 md5 cisco
ntp trusted-key 10
```

R2

```
ntp source G0/1
```

R4

```
ntp authentication-key 10 md5 cisco
ntp authenticate
ntp trusted-key 10
ntp server 10.2.58.7 key 10
```

An NTP Access-List has been configured on R7 for NTP peer filtering – this means IP address for NTP source interface on R1, R2 and R4 must correspond with the ones in access-list 10 of R7.

Then on R1 NTP source interface shouldn't be loopack12, this the first fault.

Another fault is about NTP password, which is not correctly configured on R1 so authentication is failing. You should issue a "no ntp authentication-key 10 md5" command and re-enter the command with "cisco" as password.

For R4, the first fault is that NTP key has a wrong number and there is few missing commands required to sync time on R4 with R7.

Verification

If you enable NTP debugs on R1 you should see a crypto-NAK failure message – this means authentication is failing. After you fix the key all should be good :

```
R1#
*May 30 11:06:57.497: NTP message sent to 10.2.58.7, from interface
'FastEthernet0/0' (10.2.68.1).
*May 30 11:06:57.501: NTP message received from 10.2.58.7 on interface
'FastEthernet0/0' (10.2.68.1).
*May 30 11:06:57.501: NTP Core(DEBUG): ntp_receive: message received
*May 30 11:06:57.501: NTP Core(DEBUG): ntp_receive: peer is 0x482E9098,
next action is 1.
*May 30 11:06:57.501: NTP Core (NOTICE): ntp_receive: dropping message:
crypto-NAK.
```

```
R1#sh ntp status
Clock is synchronized, stratum 9, reference is 10.2.58.7
nominal freq is 250.0000 Hz, actual freq is 250.0009 Hz, precision is
2**24
reference time is D551B435.D4CFE373 (11:19:17.831 UTC Thu May 30 2013)
```

```
clock offset is -2.3868 msec, root delay is 2.88 msec
root dispersion is 945.92 msec, peer dispersion is 3.67 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000003697
s/s
system poll interval is 64, last update was 274 sec ago.


R2#sh ntp status
Clock is synchronized, stratum 9, reference is 10.2.58.7
nominal freq is 250.0000 Hz, actual freq is 249.9981 Hz, precision is
2**24
reference time is D551B08D.F75F9AE1 (12:03:41.966 UTC Thu May 30 2013)
clock offset is -0.0006 msec, root delay is 0.00 msec
root dispersion is 0.94 msec, peer dispersion is 0.93 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000007639
s/s
system poll interval is 64, last update was 10 sec ago.

R4#sh ntp status
Clock is synchronized, stratum 9, reference is 10.2.58.7
nominal freq is 250.0000 Hz, actual freq is 250.0050 Hz, precision is
2**24
reference time is D551B115.D70D35EF (12:05:57.840 UTC Thu May 30 2013)
clock offset is -0.1077 msec, root delay is 4.13 msec
root dispersion is 941.51 msec, peer dispersion is 440.32 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000019958
s/s
system poll interval is 64, last update was 96 sec ago.
```

Task 6.3: Control Network Flooding Using MQC (4 Points)

- After the IT department has experienced a huge TCP flooding on ACS server, it has been determined that attacks came from CAT4
- Therefore, the managing IT director asked you to drop all TCP requests from CAT4 toward the ACS
- Configurations for this task should be done only on R5 and R2 (on both routers)
- Dropping packets should be done only on R2 GigabitEthernet0/0 interface
- Do not apply an access-group on any interface for this task

Detailed Solution

ASA2

```
access-list OUTSIDE_IN per tcp host 10.2.38.24 host 10.2.58.100
```

ASA3

```
access-list OUTSIDE_IN per tcp host 10.2.38.24 host 10.1.1.100
```

R5

```
access-list 130 permit tcp host 10.2.38.24 host 10.2.58.100

class-map match-all CAT3_TO_ACS
 match access-group 130

policy-map MARK
 class CAT3_TO_ACS
  set precedence 1

interface FastEthernet0/0
 service-policy output MARK
```

R2

```
class-map match-all CAT3_TO_ACS
 match precedence 1

policy-map DROP
 class CAT3_TO_ACS
   drop

interface GigabitEthernet0/0
 service-policy output DROP
```

The trick in that task is to understand that packets should be only marked on R5 and dropped on R2.

Verification

```
CAT4#telnet 10.2.58.100 22
```

```
Trying 10.2.58.100, 22 ...

R5#sh policy-map interface
 FastEthernet0/0

  Service-policy output: MARK

    Class-map: CAT3_TO_ACS (match-all)
      4 packets, 232 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      QoS Set
        precedence 1
          Packets marked 4

    Class-map: class-default (match-any)
      272 packets, 26739 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

R2#sh policy-map interface g0/0
 GigabitEthernet0/0

  Service-policy output: DROP

    Class-map: CAT3_TO_ACS (match-all)
      4 packets, 232 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  precedence 1
      drop

    Class-map: class-default (match-any)
      25 packets, 2064 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 6.4: IOS NAT (4 Points)

- The network administrator has asked to be authorized to manage CAT4 from his home, so you have been asked to configure the access with the following guidelines :

    - Only SSH and Telnet access is authorized from IP address 10.2.38.200 and 10.2.28.200
    - Configure R6 such as when PC host attempts connection to VLAN38, its IP address is translated to 10.2.38.200
    - Configure CAT4 such that it will respond also to requests directed to IP address 10.2.38.34
    - Configure R6 such that IP address 10.2.38.34 will be seen always as 10.2.18.34 on outside interface for SSH and Telnet protocols
- Create a local account for testing purposes on CAT4 : username : “admin” with password “ipexpert”
- From PC host issue a SSH session to CAT4 and then do a “who” command to ensure that the connected IP address is 10.2.38.200
- From PC host issue a SSH session to IP address 10.2.18.34 and then a “who” command to ensure that the connected IP address is 10.2.28.200
- For the test, change the VLAN of PC Host to VLAN 28, configure network IP address as 10.2.28.100 without a default gateway and add the following route in DOS command: route add 10.2.0.0 mask 255.255.0.0 10.2.28.23

Detailed Solution

CAT4

```
interface Vlan38
 ip address 10.2.38.34 255.255.255.0 secondary

access-list 20 permit 10.2.38.200
access-list 20 permit 10.2.28.200

line vty 0 15
 access-class 20 in
 transport input ssh telnet
 login local
```

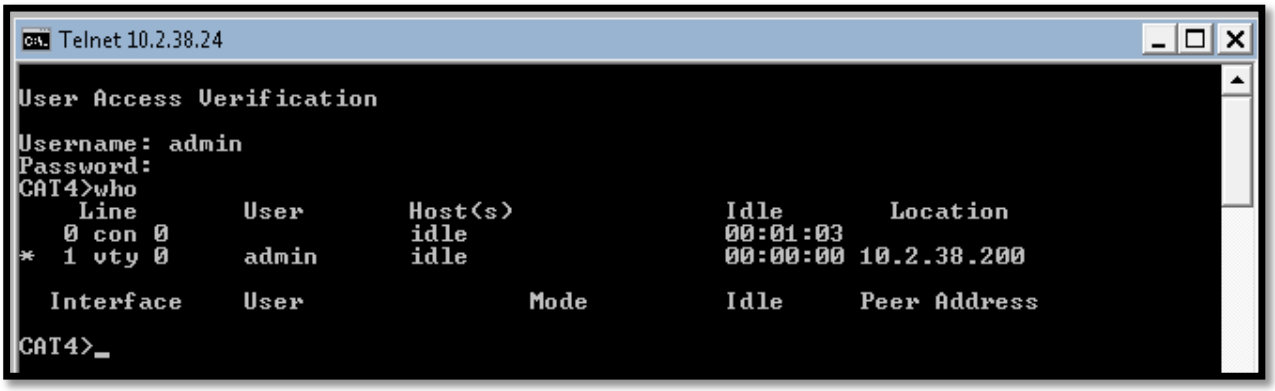
R6

```
interface FastEthernet0/0
 ip nat outside
interface FastEthernet0/1
 ip nat inside

ip access-list ext 102
 100 permit tcp host 10.2.28.200 host 10.2.18.34 eq telnet
```

```
 110 permit tcp host 10.2.28.200 host 10.2.18.34 eq 22

ip access-list extended NAT_IN_OUT
 permit ip host 10.2.28.200 host 10.2.38.24

route-map NAT_IN_OUT permit 10
 match ip address NAT_IN_OUT
route-map NAT_IN_OUT deny 20

ip nat pool NPOOL 10.2.38.200 10.2.38.200 netmask 255.255.255.0
ip nat outside source route-map NAT_IN_OUT pool NPOOL add-route

ip nat ins source static tcp 10.2.38.34 22 10.2.18.34 22 extendable
ip nat ins source static tcp 10.2.38.34 23 10.2.18.34 23 extendable
```

The parameter “add-route” is necessary to create a static route between the NAT global IP and the NAT local IP as soon as NAT translation has taken place.

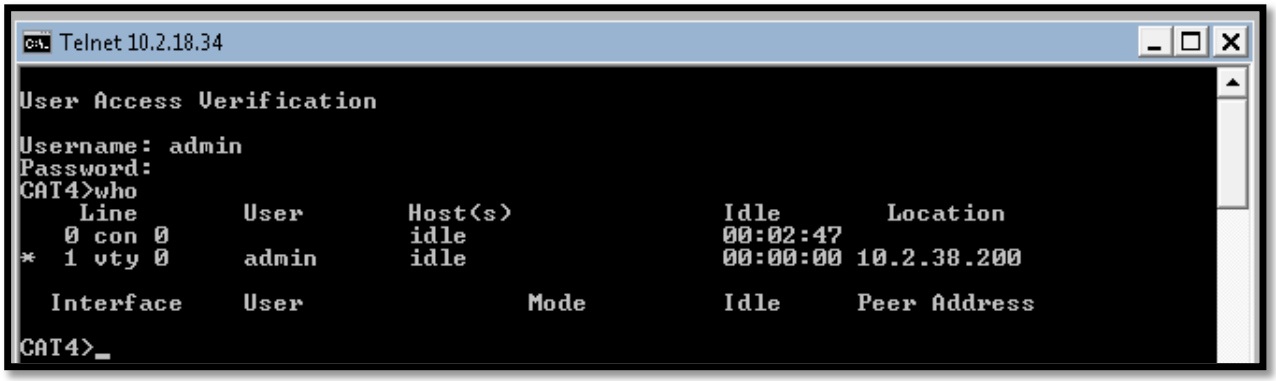
Verification



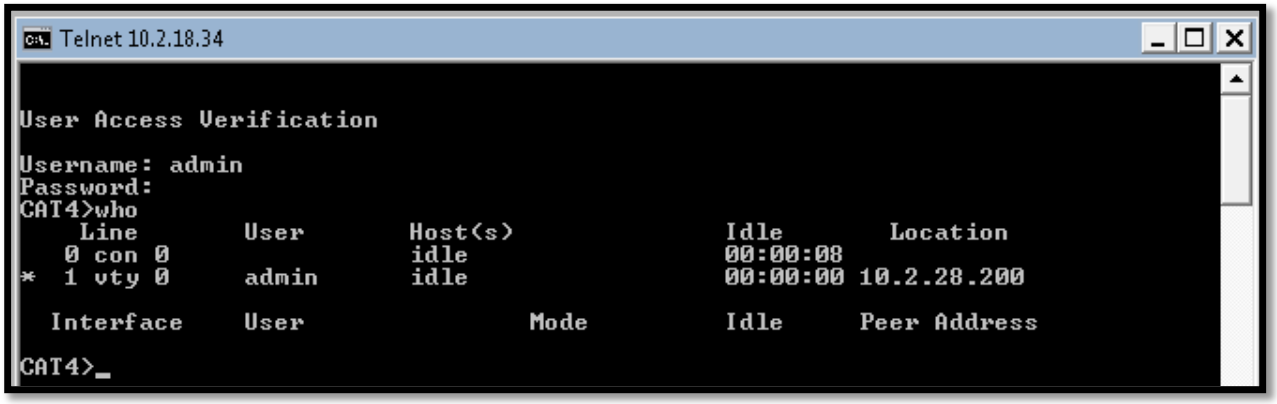
Here’s the problem with this IOS version – even there is no match for the packet sent to 10.2.18.34 in the NAT rules it “finds” a match and does the translation. This only happens when you first telnetted to 10.2.38.24 (as shown above):

```
R6#sh ip nat t
Pro Inside global      Inside local       Outside local      Outside
global
--- ---                ---                10.2.38.200        10.2.28.200
```

```
tcp 10.2.38.24:23     10.2.38.24:23       10.2.38.200:58692
10.2.28.200:58692
tcp 10.2.18.34:22       10.2.38.34:22       ---                 ---
tcp 10.2.18.34:23       10.2.38.34:23       ---                 ---

001217: May 30 16:03:46.882: NAT: Existing entry found in the global
tree,updating it to point to the latest node passed
001218: May 30 16:03:46.882: NAT: o: tcp (10.2.28.200, 58694) ->
(10.2.18.34, 23) [1490]
001219: May 30 16:03:46.882: NAT: s=10.2.28.200->10.2.38.200, d=10.2.18.34
[1490]

tcp 10.2.18.34:23     10.2.38.34:23       10.2.38.200:58711
10.2.28.200:58711
```



If you telnet to 10.2.18.34 first, it doesn't translate the packet what we should see in both cases (looks like a bug since we are using a route-map that should create extended entries):



7.0 Attack Mitigation (16 points)

Task 7.1: Filtering Malicious Traffic (4 Points)

- It's been found out that spoofed addresses are initiating sessions from behind R5
- You have been asked to filter this traffic within these guidelines :
  - All configurations should be done on F0/1 interface of R5
  - Path to the source IP address must be through the same interface as that
  - on which the packet arrived
  - Router should be allow to ping its own interface IP
  - Packets sourced from 10.1.1.0/24 subnet arriving at F0/1 and failing the
  - anti-spoofing check are logged and dropped
  - Packets sourced from 172.16.1.0/24 subnet arriving at F0/0 and failing
  - the anti-spoofing check are logged and forwarded

Detailed Solution

R5

```
access-list 105 deny   ip 10.1.1.0 0.0.0.255 any log
access-list 105 permit ip 172.16.1.0 0.0.0.255 any log
access-list 105 deny   ip any any

interface FastEthernet0/1
 ip verify unicast source reachable-via rx allow-self-ping 105
```

Don't forget to enable sending BGP communities to the peers. Otherwise the injected prefix gets propagated to other (neighboring) ASes as well.

Verification

Configure three loopbacks on R6 – one for 10.1.1.6, one for 172.16.1.6 and the other for 192.168.99.6. Remove "redistribute connected" from EIGRP 55 process and test :

```
R6#ping 10.2.48.7 so loop101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.7, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.6
```

```
.....
Success rate is 0 percent (0/5)

May 30 16:37:38.864: %SEC-6-IPACCESSLOGDP: list 105 denied icmp 10.1.1.6 -
> 10.2.48.7 (0/0), 1 packet

R5#sh access-l 105
Extended IP access list 105
    10 deny ip 10.1.1.0 0.0.0.255 any log (5 matches)
    20 permit ip 172.16.1.0 0.0.0.255 any log
    30 deny ip any any

R5#sh ip int f0/1 | in verif
  IP verify source reachable-via RX, allow self-ping, ACL 105
   5 verification drops
   0 suppressed verification drops
   0 verification drop-rate

R6#ping 10.2.48.7 so l102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.7, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.6
.....
Success rate is 0 percent (0/5)

May 30 16:39:40.639: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp
172.16.1.6 -> 10.2.48.7 (0/0), 1 packet
```

Note packets are subject to uRPF but ACL allows it so uRPF action is suppressed:

```
R5#sh ip int f0/1 | in verif
  IP verify source reachable-via RX, allow self-ping, ACL 105
   10 verification drops
   5 suppressed verification drops
   0 verification drop-rate

R6#ping 10.2.48.7 so l103

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.2.48.7, timeout is 2 seconds:
Packet sent with a source address of 192.168.99.6
.....
Success rate is 0 percent (0/5)

R5#sh ip int f0/1 | in verif
  IP verify source reachable-via RX, allow self-ping, ACL 105
   15 verification drops
   5 suppressed verification drops
   0 verification drop-rate
```

Put “redistribute connected” back in:

```
R6#ping 10.2.48.7 so f0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.7, timeout is 2 seconds:
Packet sent with a source address of 10.2.38.6
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R5#ping 10.2.18.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.18.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Task 7.2: Preventing Network Attacks (4 Points)

- After dealing with huge DoS attack that leads to crash ASA2, your manager asked you to configure ASA2 in order to meet the following requirements :
    - ASA should send a Syslog message when the number of denied packets by denial by access-lists is up to 300drops/second over the last 15 minutes
    - Another Syslog should be sent when the number of dropped packets caused by an incomplete session, is up to 500drops/second with a burst of 2000drops/second over the last 20 second period
    - ASA2 should automatically shun detected attackers from host performing a scan, except for hosts on the 10.2.0.0/16 network

- Do not use Modular Policy Framework or ACL to configure this task

Detailed Solution

ASA2

```
threat-detect rate acl-drop rate-interval 900 average-rat 300 burst-rate
1200
threat-detect rate syn-attack rate-interval 600 average- 500 burst-rate
2000
threat-detection basic-threat
threat-detection scanning-threat shun except ip-address 10.2.0.0
255.255.0.0
```

For the first question, “burst-rate” is not specified so it could be every value. But the result of “show run all threat-detection rate” shows that burst-rate value is four time the average-rate in default configurations. So, we adopted this ratio to be 4*300 = 1200.

For the second question, the trick is to know the ratio between average-rate period and burst-rate period which is 1/30th starting in 8.2 (see command reference for “threat-detection rate”).

So since the burst period given is 20 seconds, we calculate rate interval (average-rate period) like this : 30 * 20 seconds = 600seconds

In other words you cannot specify burst-rate period in the command; it is calculated automatically by dividing rate interval by 30.

The third question is pretty straightforward.

Verification

Just double-check the settings :

```
ASA2(config)# sh run threat-detection
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-
rate 800
threat-detection rate acl-drop rate-interval 900 average-rate 300 burst-
rate 1200
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-
rate 640
```

```
threat-detection rate syn-attack rate-interval 600 average-rate 500 burst-
rate 2000
threat-detection rate syn-attack rate-interval 1200 average-rate 500
burst-rate 40
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-
rate 160
threat-detection basic-threat
threat-detection scanning-threat shun except ip-address 10.2.0.0
255.255.0.0
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
```

Task 7.3: Layer 2 Attacks (4 Points)

- Configure CAT3 to block any Ethernet traffic on VLAN268 that is originating from and destined to 0015.C5B7.818C MAC address
- A DHCP server will be connected to the switch on port G1/0/14
- Configure DHCP snooping on VLAN268
- Configure ARP inspection on VLAN268
- Another VLAN is to be added in the future to the network (399) along with two servers which will be made part of that VLAN
- Those servers will be connected to ports F0/20 and F0/21 on CAT1 and they should not be able to talk to each other at L2
- Make sure no matter what type of the traffic server #1 sends will not be received by the second server and vice-versa

Detailed Solution

CAT4

```
vlan 399
```

CAT1

```
int range f0/20 – 21
 sw host
 sw acc vlan 399
 switchport protected
 switchport block multicast
```

```
 switchport block unicast
```

CAT3

```
mac access-list extended BADHOST
 permit host 0015.c5b7.818c any
 permit any host 0015.c5b7.818c

vlan access-map VACL_268 10
 match mac address BADHOST
 action drop
vlan access-map VACL_268 20
 action forward

vlan filter VACL_268 vlan-list 268

ip dhcp snooping vlan 268
ip dhcp snooping
ip arp inspection vlan 268

interface G1/0/14
 switchport access vlan 268
 ip dhcp snooping trust
 ip arp inspection trust
```

Make sure the VLANs exist.

DHCP Server port was also made DAI-trusted since the server does not obtain an IP address for itself dynamically – it uses a static IP which will never get to the DHCP Snooping database. This would break ARP traffic from the server.

Verification

```
CAT3#sh vlan filter
VLAN Map VACL_268 is filtering VLANs:
  268

CAT3#sh vlan access-map
Vlan access-map "VACL_268"  10
  Match clauses:
```

```
    mac address: BADHOST
  Action:
    drop
Vlan access-map "VACL_268"  20
  Match clauses:
  Action:
    forward

CAT3#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
268
DHCP snooping is operational on following VLANs:
268
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: c464.13d1.c580 (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    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0/14      yes        yes             unlimited
  Custom circuit-ids:


CAT3#sh ip arp inspection vlan 268

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

```
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  268     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  268     Deny             Deny              Off

CAT3#sh ip arp inspection interfaces gigabitEthernet 1/0/14

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/14         Trusted               None               N/A


CAT1#sh int f0/20 sw
Name: Fa0/20
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 399 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

```
Protected: true
Unknown unicast blocked: enabled
Unknown multicast blocked: enabled
Appliance trust: none
```

Task 7.4: RA Spoofing (4 Points)

- Your security policy states that the only legitimate source of RA messages in VLANs 48, 148, 158 & 208 should be R5
- Configure R5 and R7 to implement this policy
- Disable Router Advertisements on R7 and R10
- NTP password is “cisco”
- Use R10 as a CA; cert signatures should be created with SHA-1
- Make sure R10 will be still able to communicate with R5 and R7 using IPv6

Detailed Solution

ASA2

```
access-list DMZ_IN per udp host 10.2.48.10 host 10.2.58.7 eq 123
access-list OUTSIDE_IN permit tcp host 10.2.48.5 host 10.2.48.10 eq www

no ipv6 access-list DMZ6_IN permit ospf any host fe80::5
no ipv6 access-list DMZ6_IN permit ospf any host fe80::7
ipv6 access-list DMZ6_IN permit ospf any host fe80::2cc5:701a:c1dd:7546
ipv6 access-list DMZ6_IN permit ospf any host fe80::205f:cd15:d716:550b

no ipv6 access-list OUTSIDE6_IN permit ospf any host fe80::7
ipv6 access-list OUTSIDE6_IN permit ospf any host
fe80::2cc5:701a:c1dd:7546
```

R10

```
ntp authentication-key 10 md5 cisco
ntp authenticate
ntp trusted-key 10
ntp server 10.2.58.7 key 10
ntp logging
```

```
ip http server

crypto pki trustpoint CA
 ip-extension prefix 2010::/64
 revocation-check crl

crypto pki server CA
 grant auto
 issuer cn=CA
 no shut

int g0/0
 ipv6 nd ra suppress all
```

R5

```
cry key gen rsa label CGAKEY2 modulus 1024

ipv cga modifier rsakeypair CGAKEY2 sec-level 1

crypto pki trustpoint STRUST
 ip-extension prefix 2010::/64
 enrollment url http://10.2.48.10:80
 password 7 030752180500701E1D
 subject-name cn=R5
 revocation-check crl
 rsakeypair CGAKEY2

crypto pki authen STRUST
crypto pki enro STRUST

int F0/0
 ipv6 cga rsakeypair CGAKEY2
 ipv6 address FE80:: link-local cga
 ipv6 address 2010::5/64
 ipv6 nd ra interval 40
 ipv6 nd secured trustpoint STRUST
 no ipv6 nd secured full-secure
```

R7

```
cry key gen rsa label CGAKEY modulus 1024

ipv cga modifier rsakeypair CGAKEY sec-level 1

crypto pki trustpoint STRUST
 enrollment url http://10.2.48.10
 password 7 110A1016141D5A5E57
 revocation-check crl
 rsakeypair CGAKEY

crypto pki authen STRUST

int f0/0
 ipv6 cga rsakeypair CGAKEY
 ipv6 address FE80:: link-local cga
 ipv6 address 2010::7/64
 ipv6 nd ra suppress
 ipv6 nd secured trustanchor STRUST
 no ipv6 nd secured full-secure
```

IOS CA does not have to use a CGA-enabled Key Pair when used with SEND.

Since Link-Local addresses changed we had to update ACLs on the ASA.

The “full-secure” option must be disabled since R10’s code does not support SEND – otherwise all non-signed messages from R10 would be dropped by R5 & R7, which would break IPv6 for this device.

Verification

```
R7# debug ipv nd secured
Jun  1 11:21:24.458: SEND: Receive: ND_ROUTER_ADVERT
Jun  1 11:21:24.458: SEND:       src FE80::205F:CD15:D716:550B
Jun  1 11:21:24.458: SEND:       dst FF02::1
Jun  1 11:21:24.458: SEND:       Received at: 0x51A9D93475A6 = 11:21:24
UTC Jun 1 2013
Jun  1 11:21:24.458: SEND:               option 1 len 8:
ND_OPT_SOURCE_LINKADDR
```

```
Jun  1 11:21:24.458: SEND:                option 5 len 8: ND_OPT_MTU
Jun  1 11:21:24.458: SEND:                option 3 len 32:
ND_OPT_PREFIX_INFORMATION
Jun  1 11:21:24.458: SEND:                option 11 len 192: ND_OPT_CGA
Jun  1 11:21:24.458: SEND:                option 13 len 16:
ND_OPT_TIMESTAMP
Jun  1 11:21:24.458: SEND:                option 12 len 152: ND_OPT_RSA
Jun  1 11:21:24.458: SEND:       Verifying address
FE80::205F:CD15:D716:550B
Jun  1 11:21:24.458: SEND:        keylen is 1024
Jun  1 11:21:24.458: SEND:        sec is 1
Jun  1 11:21:24.458: SEND:        Address verified
Jun  1 11:21:24.458: SEND:       Timestamp: 0x51A9D93460BA = 11:21:24 UTC
Jun 1 2013
Jun  1 11:21:24.458: SEND:        TS opt check RC = 0
Jun  1 11:21:24.466: SEND:       Good signature
Jun  1 11:21:24.466: SEND:       RA with prefix option 2010::
Jun  1 11:21:24.466: SEND: Send : CPS
Jun  1 11:21:24.466: SEND:        adding trustanchor cn=R10-CA
Jun  1 11:21:24.466: SEND:                option 15 len 24:
ND_OPT_TRUST_ANCHOR
Jun  1 11:21:24.474: SEND: Receive: ND_CERTIFICATE_ADVERT
Jun  1 11:21:24.474: SEND:        src FE80::205F:CD15:D716:550B
Jun  1 11:21:24.474: SEND:        dst FF02::1:FFDD:7546
Jun  1 11:21:24.478: SEND:        Received at: 0x51A9D9347A8B = 11:21:24
UTC Jun 1 2013
Jun  1 11:21:24.478: SEND:                option 15 len 24:
ND_OPT_TRUST_ANCHOR
Jun  1 11:21:24.478: SEND:                option 16 len 568:
ND_OPT_CERTIFICATE
Jun  1 11:21:24.478: SEND: Certificate has trust anchor cn=R10-CA -
Storing ...
Jun  1 11:21:24.506: SEND:      Deliver RA held in cert DB
Jun  1 11:22:31.482: SEND: NEW STATE TR: CERT_VALIDATED


R7#sh ipv nd secured certificates
Total number of entries: 1 / 32

Hash                             id         RA  certcnt certrcv state
CAB0AA0F675A07B2D44771F159191253 0x000014ED no  1       1
CERT_VALIDATED
```

```
  certificate No 0
         subject  hostname=R5.ipexpert.com,cn=R5
         issuer  cn=R10-CA

R7#sh ipv nd secured counters int f0/0
Received ND messages on FastEthernet0/0:
        rcvd    accept  SLLA   PREFIX  MTU    CGA    RSA   TS    TA
CERT
RA      2       2       2      2       2      2      2       2       0
0
CPA     1       0       0      0       0      0      0       0       1
1

Dropped ND messages on FastEthernet0/0:
Codes   CLI    : CLI initialted

        drop    CLI
CPA     1       1

Sent ND messages on FastEthernet0/0:
        sent    aborted TA
CPS     1       0       1
```

Also check if you still have IPv6 reachability between the devices – clear IPv6 Cache everywhere, clear OSPF processes and see if all is good :

```
R10#clear ipv neig

R10#clear ipv ospf pr
Reset ALL OSPF processes? [no]: yes

R10#sh ipv ospf ne

            OSPFv3 Router with ID (10.2.48.10) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID
Interface
10.2.58.7         1   FULL/DR         00:00:32    3
GigabitEthernet0/0
55.55.55.55       1   FULL/BDR        00:00:36    3
GigabitEthernet0/0
```

```
R10#sh ipv ne
IPv6 Address                              Age Link-layer Addr State
Interface
FE80::2CC5:701A:C1DD:7546                   0 001b.d517.ba88  REACH Gi0/0
FE80::205F:CD15:D716:550B                   0 001b.d50f.f2f8  REACH Gi0/0

R5#clear ipv ne

R5#ping 10.2.48.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R5#ping 10.2.48.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.48.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

ipexpert

IPexpert's Lab Preparation Workbook

for the Cisco® CCIE™ Security Volume 2

Complete DSG Labs 4-5

Lab 4

Please look at the provided diagrams and read through the whole lab before you start. Read the directions very carefully to make sure you are doing what is being asked of you. This concept is very important when you take the CCIE lab administered by Cisco

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. You may add static routes on your Test PCs, AD Server, ISE, ACS and WSA to reach any networks.

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

NOTE: Unicast static/default routes are NOT allowed (except on Test PCs, AD server, ISE, ACS and WSA) unless otherwise stated in the task

NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device

NOTE: Unless explicitly prohibited in a section, you may permit ICMP for connectivity testing

NOTE: Any reference to a password that is not defined should use "ipexpert"

Estimated Time to Complete: **8 Hours**

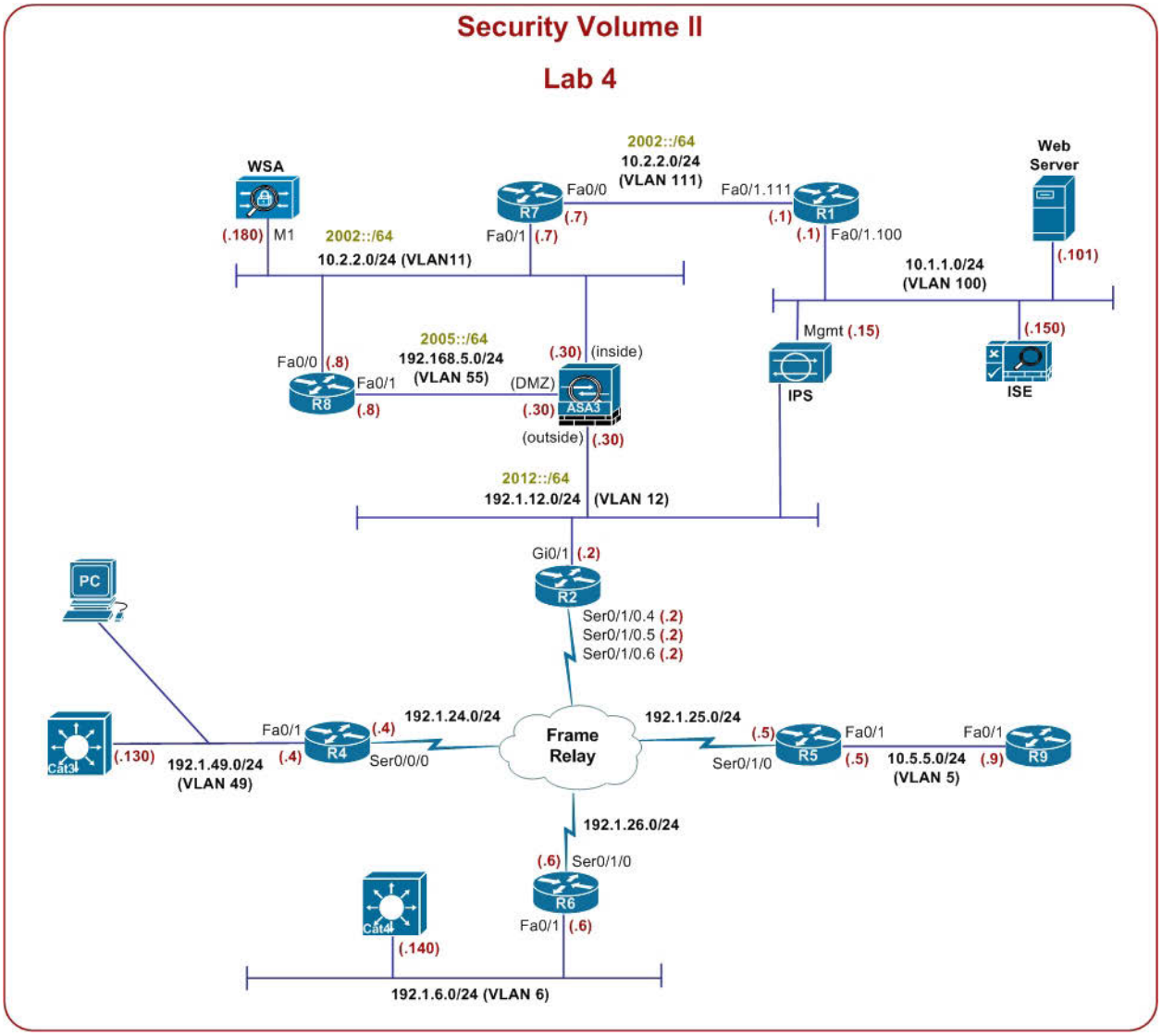
Pre-setup

- 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	Fa0/1.100	100	10.1.1.1/24
	Fa0/1.111	111	10.2.2.1/24 2002::1/64
	Loopback0		1.1.1.1/8
R2	Gi0/1	12	192.1.12.2/24 2012::2/64
	Serial0/1/0.4		192.1.24.2/24
	Serial0/1/0.5		192.1.25.2/24
	Serial0/1/0.6		192.1.26.2/24
	Loopback0		2.2.2.2/8
R4	Fa0/1	49	192.1.49.4/24
	Serial0/0/0		192.1.24.4/24
	Loopback0		4.4.4.4/8
R5	Fa0/1	5	10.5.5.5/24
	Serial0/1/0		192.1.25.5/24
	Loopback0		5.5.5.5/8
R6	Fa0/1	6	192.1.6.6/24
	Serial0/1/0		192.1.26.6/24
	Loopback0		6.6.6.6/8
R7	BVI		10.2.2.7
R8	Fa0/0	11	10.2.2.8 2002::8/64
	Fa0/1	55	192.168.5.8/24 2005::8/64
	Loopback0		8.8.8.8/8
R9	Fa0/1	5	10.5.5.9/24

	Loopback0		9.9.9.9/8
ASA3	outside	12	192.1.12.30/24 2012::30/64
	inside	11	10.2.2.30/24 2002::30/64
	DMZ	55	192.168.5.30/24 2005::30/64
Cat3	VLAN49	49	192.1.49.130/24
Cat4	VLAN6	6	192.1.6.140/24
IPS	Management	100	10.1.1.15/24
WSA	M1	11	10.2.2.180/24
ISE		100	10.1.1.150/24
Web Server		100	10.1.1.101/24
PC		49	192.1.49.200



Solutions

1.0 ASA Firewalls (15 points)

Task 1.1: ASA3 Configuration (4 Points)

- Configure ASA3 as per the diagram and table above
- Create a sub-interface off of G0/0 interface, G0/0.55
- The subinterface should belong to VLAN 55. The main interface belongs to the outside VLAN. Assign the new sub-interface a name of DMZ and a security level of 55
- Configure the switch to allow the ASA to communicate to the rest of the network
- Assign IP addresses to the Interfaces
- The inside interfaces should account for redundancy

Detailed Solution

CAT3

```
interface GigabitEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport mode trunk

int range g1/0/20 - 21
 sw host
 sw acc vlan 11


ASA3
hostname ASA3

interface G0/0
 nameif outside
 security-level 0
 ip address 192.1.12.30 255.255.255.0 standby 192.1.12.31
 ipv add 2012::30/64 stan 2012::31
```

```
 no shut

interface G0/0.55
 vlan 55
 nameif DMZ
 security-level 55
 ip address 192.168.5.30 255.255.255.0 standby 192.168.5.31
 ipv add 2005::30/64 stan 2005::31
 no shut

interface G0/1
 no shut
interface G0/2
 no shut

interface Redundant1
 member-interface G0/1
 member-interface G0/2
 nameif inside
 security-level 100
 ip address 10.2.2.30 255.255.255.0 standby 10.2.2.31
 ipv address 2002::30/64 stan 2002::31
```

Basic ASA setup starts with interface configuration on the switches and ASA's. First thing to note here is that for G0/0 we need to sub interface it for the DMZ while using the main interface for outside. This is simply done by changing G1/0/19 on CAT3 to a trunk port allowing both the DMZ and outside VLANs (by default all VLANs are allowed). The trunk native VLAN is then assigned the outside VLAN 12, which covers of the requirements for interface G0/0.

Then we move to the matter of the redundancy for the inside interface. For this we use the logical redundant interface feature. This works similarly (but is completely separate) to active/standby failover, in when the active interface fails the standby interface becomes active and will start to handle traffic flow. The ASA supports up to eight redundant interfaces. When using this feature, all we need to do on the physical interfaces is enable them.

Looking forward to the next section, we see that we are required to use failover with ASA4, using G0/3 as the fail/state interface. This leaves us with G0/2 as the only spare interface to use for redundancy. We then create the redundant interface 1 and assign G0/1 & 2 as the members of it, this then clears whatever config is on the physical interfaces. The physical interfaces then

inherit the logical configuration from Redundant1. The key to remember here is that the Switch config for G0/2 port needs to be a copy of G0/1 port.

The other thing to notice here is that the standby IPs have been assigned. It is always better to apply the standby interface IPs as you setup the interfaces, if failover is to be configured in a later task. Small things like this will save you valuable time to use later in the lab for verification, etc. This is another reason why it is key to read through the lab fully prior to beginning.

Verification

```
ASA3(config)# ping 192.168.5.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3(config)# ping 192.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3(config)# ping 10.2.2.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3(config)# ping 2012::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2012::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3(config)# sh int ip br | ex unas
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0        192.1.12.30     YES manual up
up
```

```
GigabitEthernet0/0.55      192.168.5.30    YES manual up
up
Internal-Control0/0        127.0.1.1       YES unset  up
up
Redundant1                 10.2.2.30       YES manual up
up

ASA3(config)# sh int red 1 | be Redundancy
  Redundancy Information:
        Member GigabitEthernet0/1(Active), GigabitEthernet0/2
        Last switchover at 17:53:35 UTC Jun 9 2013

ASA3(config)# sh ipv6 interface br | ex Gig|una
outside [up/up]
    fe80::d68c:b5ff:fe4e:6d9c
    2012::30
DMZ55 [up/up]
    fe80::d68c:b5ff:fe4e:6d9c
    2005::30
Management0/0 [administratively down/down]
Port-channel1 [administratively down/down]
inside [up/up]
    fe80::d68c:b5ff:fe4e:6d99
    2002::30
```

Task 1.2: Failover and ASA routing (4 Points)

- Configure IP & IPv6 default route on the ASA3 pointing towards R2
- Configure a static route for the network behind R1
- Configure ASA4 as a failover device for ASA3
- Once the devices are synchronized the output should match as per below :

```
ASA3/act(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FAIL GigabitEthernet0/3.98 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 2 seconds, holdtime 10 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
```

```
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 18:23:14 UTC Jun 9 2013
        This host: Primary - Active
                Active time: 3955 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
This host: Primary - Active
                Active time: 4321 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                Interface outside (192.1.12.30/fe80::30): Normal
(Monitored)
                Interface DMZ55 (192.168.5.30/fe80::30): Normal
(Monitored)
                Interface inside (10.2.2.30/fe80::30): 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: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                Interface outside (192.1.12.31/fe80::31): Normal
(Monitored)
                Interface DMZ55 (192.168.5.31/fe80::31): Normal
(Monitored)
                Interface inside (10.2.2.31/fe80::31): 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 : STATE GigabitEthernet0/3.99 (up)
Stateful Obj    xmit       xerr       rcv        rerr

--- OUTPUT TRUNCATED ---
```

Detailed Solution

```
CAT4
vlan 98,99

interface GigabitEthernet1/0/19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 12
 switchport mode trunk
```

```
int range g1/0/20 - 21
 sw host
 sw acc vlan 11

int g1/0/22
 sw tru enca dot
 sw mode trunk
 sw trunk allowed vlan 98,99
```

CAT3

```
int g1/0/22
 sw tru enca dot
 sw mode trunk
 sw trunk allowed vlan 98,99
```

ASA3

```
route outside 0.0.0.0 0.0.0.0 192.1.12.2
ipv6 route outside ::/0 2012::2
route inside 10.1.1.0 255.255.255.0 10.2.2.1

int g0/0
 ipv6 address fe80::30 link-local standby fe80::31
int g0/0.55
 ipv6 address fe80::30 link-local standby fe80::31
int red 1
 ipv6 address fe80::30 link-local standby fe80::31

interface G0/3
 no shut

interface G0/3.98
 vlan 98

interface G0/3.99
 vlan 99

failover lan unit primary
```

```
failover lan interface FAIL G0/3.98
failover key ipexpert
failover link STATE G0/3.99
failover interface ip FAIL 98.98.98.1 255.255.255.252 standby 98.98.98.2
failover interface ip STATE 99.99.99.1 255.255.255.252 standby 99.99.99.2

failover polltime interface 2 holdtime 10

monitor-interface DMZ
prompt hostname state
failover
```

ASA4

```
interface G0/3
 no shut
interface G0/3.98
 vlan 98

interface G0/3.99
 vlan 99

failover lan unit secondary
failover lan interface FAIL G0/3.98
failover key ipexpert
failover interface ip FAIL 98.98.98.1 255.255.255.252 standby 98.98.98.2
failover
```

A few things to note from the output provided, the first is the failover interface. We see from here that it's actually using sub-interfaces in VLANs 98 and 99.

We also need to take a close look at the ip addresses, particularly the standby IPs which are all set to 31 in the last octet (including IPv6 link-locals).

Finally, with the interfaces we can see that we have three monitored interfaces, and that the states are normal, meaning we need to set the monitor-interface cmd for the DMZ interface.

Once ASA3 ports on CAT3 are configured, remember to replicate these configurations over to the ASA4 connected ports on CAT4.

A little issue has been introduced as part of troubleshooting on switch 4. The Outside interface of ASA4 goes into a failed mode. This is due to 'vlan dot1q tag native' being configured on the switch. The outside interface is configured to accept VLAN 12 untagged. In applying this command, we ensure that all vlans are tagged, hence the ASA interface fails.

Verification

```
CAT4#sh vlan dot1q tag native
dot1q native vlan tagging is enabled
```

After you disable Native VLAN tagging failover should finally converge :

```
ASA3/act(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FAIL GigabitEthernet0/3.98 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 2 seconds, holdtime 10 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 18:23:14 UTC Jun 9 2013
        This host: Primary - Active
                Active time: 4467 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                 Interface outside (192.1.12.30/fe80::30): Normal
(Monitored)
                 Interface DMZ55 (192.168.5.30/fe80::30): Normal
(Monitored)
                 Interface inside (10.2.2.30/fe80::30): 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: 0 (sec)
```

```
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                 Interface outside (192.1.12.31/fe80::31): Normal
(Monitored)
                 Interface DMZ55 (192.168.5.31/fe80::31): Normal
(Monitored)
                 Interface inside (10.2.2.31/fe80::31): 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 : STATE GigabitEthernet0/3.99 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         78         0          74         0
        sys cmd         74         0          74         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         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   0          0          0          0
        User-Identity   1          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       9       642
        Xmit Q:         0       48      785
```

Task 1.3: NAT (4 Points)

- Configure PAT on ASA3 for all RFC 1918 networks
- Addresses should be translated to the outside interface IP
- R1 is configured with Loopback125 and has an IP Address 195.1.1.1/24. This is a network with a public address
- Allow this network to go out without getting translated
- R2 should be able to ping this network. You are allowed a static route on R2 and the ASA to accomplish this step
- Create a static NAT entry for the AAA server at 10.1.1.150. Translate it to 192.1.12.150
- Allow R2 Gi0/1 interface to communicate with ISE using RADIUS
- Create a static NAT entry for R1 Fa0/1.111 10.2.2.1. Translate it to 192.1.12.1

Detailed Solution

R2

```
ip route 195.1.1.0 255.255.255.0 192.1.12.30
```

ASA3

```
route inside 195.1.1.0 255.255.255.0 10.2.2.1

object network NET-10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0
 nat (any,outside) dynamic interface

object network NET-10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
 nat (any,outside) dynamic interface

object network NET-192.168.5.0_24
 subnet 192.168.5.0 255.255.255.0
 nat (any,outside) dynamic interface

object network ISE
 host 10.1.1.150
 nat (any,outside) static 192.1.12.150
```

```
object network R1
 host 10.2.2.1
 nat (any,outside) static 192.1.12.1

access-list OUTSIDE_IN permit icmp any any
access-list OUTSIDE_IN permit udp host 192.1.12.2 host 10.1.1.150 eq
radius
access-list OUTSIDE_IN per udp host 192.1.12.2 host 10.1.1.150 eq radius-
acct
access-group OUTSIDE_IN in interface outside
```

Nothing really out of the ordinary in this question. Just note NAT statements use “any,outside” to account for all possible paths a packet may take (via inside or DMZ).

The instructions at the beginning of the lab allow you to run ICMP throughout so permit this in to the outside interface.

Verification

```
R8#ping 192.1.12.2 source f0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.5.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R8#ping 192.1.12.2 source f0/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms


ASA3/act(config)# sh x
2 in use, 9 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
ICMP PAT from any:192.168.5.8/6 to outside:192.1.12.30/23129 flags ri idle
0:00:01 timeout 0:00:30
ICMP PAT from any:10.2.2.8/7 to outside:192.1.12.30/30642 flags ri idle
0:00:00 timeout 0:00:30

ASA3/act(config)# sh nat det

Auto NAT Policies (Section 2)
1 (any) to (outside) source static ISE 192.1.12.150
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.150/32, Translated: 192.1.12.150/32
2 (any) to (outside) source static R1 192.1.12.1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.2.2.1/32, Translated: 192.1.12.1/32
3 (any) to (outside) source dynamic NET-10.1.1.0_24 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 192.1.12.30/24
4 (any) to (outside) source dynamic NET-10.2.2.0_24 interface
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 10.2.2.0/24, Translated: 192.1.12.30/24
5 (any) to (outside) source dynamic NET-192.168.5.0_24 interface
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 192.168.5.0/24, Translated: 192.1.12.30/24
```

Remaining verification can be done after transparent firewall configuration.

Task 1.4: Management Access (3 Points)

- Configure ASDM access to the ASA
- Only allow access to users in VLANs 11 and 100
- Authenticate as “ipexpert” with password “ipexpert”
- Use local database for authentication

Detailed Solution

ASA3

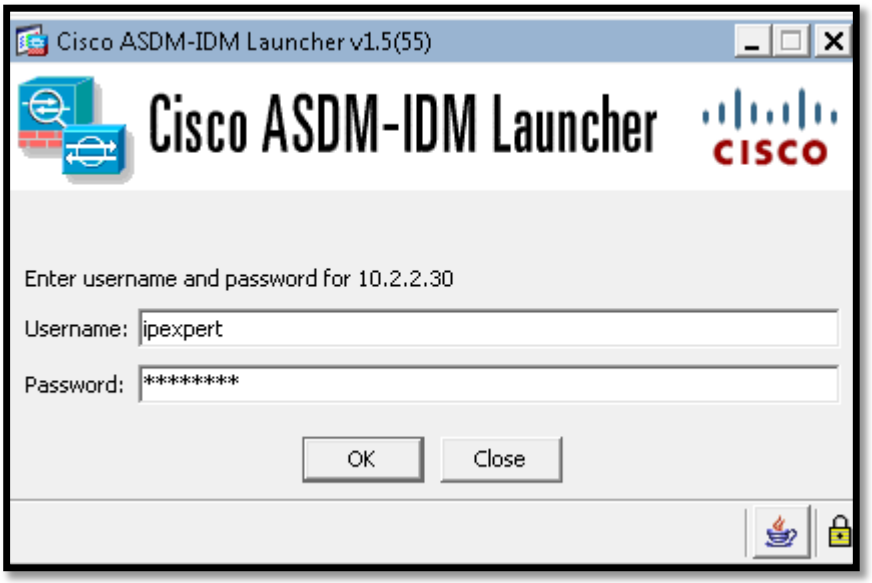
```
http server enable
http 10.1.1.0 255.255.255.0 inside
http 10.2.2.0 255.255.255.0 inside

username ipexpert password ipexpert priv 15

aaa authentication http console LOCAL

asdm image disk0:/asdm-66114.bin
```

Enabling ASDM on the ASA is somewhat similar to setting up Telnet or SSH access – you need to specify who can manage the device and use the "aaa authentication http" command to specify an authentication database.

Verification

```
ASA3/act(config)# sh asdm image
Device Manager image file, disk0:/asdm-66114.bin
```

Connect from the Test PC from VLAN 11 or 100 (https://10.2.2.30) :



2.0 IOS Firewall (8 points)

Task 2.1: IOS Firewall (4 Points)

- Inspect all TCP, UDP, and ICMP traffic going towards the Frame networks on R5
- Only allow relevant traffic coming in
- ACL should be set to inbound on the Serial interface
- Log all session based information, but do not log suspicious activity for ICMP
- Set the maximum embryonic connections per host to 75 and block for 15 minutes if this limit is exceeded

Detailed Solution

R6

```
ip inspect audit-trail
ip inspect tcp max-incomplete host 75 block-time 15

ip inspect name CBAC tcp router-traffic
ip inspect name CBAC udp router-traffic
ip inspect name CBAC icmp alert off router-traffic

ip access-list extended OUTSIDE_IN
 permit ospf host 192.1.25.2 host 224.0.0.5
 permit ospf host 192.1.25.2 host 224.0.0.6
 permit ospf host 192.1.25.2 host 192.1.25.5
 permit tcp host 2.2.2.2 host 5.5.5.5 eq bgp
 permit tcp host 2.2.2.2 eq bgp host 5.5.5.5
 permit icmp any any
 100 deny   ip any any log

interface Serial0/1/0
 ip access-group OUTSIDE_IN in
 ip inspect CBAC out
```

This task requires the use of CBAC. Generally this is a pretty straight forward CBAC configuration, but with some key points to observe. As we require ALL TCP, UDP & ICMP in the question, ensure that you included the “router-traffic” keyword in your inspection commands.

The “audit-trail” command will allow the logging of the session based info, and the “alert off” keywords in the ICMP inspection line will prevent logging of the suspicious activity for that protocol.

When using CBAC or Zone based firewall always remember to use “deny ip any any log” at the end of your ACL – it will highlight any denied flows through the device.

Verification

```
R5#sh ip inspect config
Session audit trail is enabled
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 75. Block-time 15 minutes.
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 on timeout 3600
 inspection of router local traffic is enabled
    udp alert is on audit-trail is on timeout 30
 inspection of router local traffic is enabled
    icmp alert is off audit-trail is on timeout 10
 inspection of router local traffic is enabled


R5#telnet 192.1.25.2
Trying 192.1.25.2 ... Open

Password required, but none set
```

```
*Jun  9 20:44:26.200: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (192.1.25.5:21376) -- responder (192.1.25.2:23)

R5#ping 192.1.24.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.24.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

R5#
*Jun  9 20:44:46.184: %FW-6-SESS_AUDIT_TRAIL_START: Start icmp session:
initiator (192.1.25.5:8) -- responder (192.1.24.4:0)



R5#sh access-l
Extended IP access list OUTSIDE_IN
    10 permit ospf host 192.1.25.2 host 224.0.0.5 (34 matches)
    20 permit ospf host 192.1.25.2 host 224.0.0.6
    30 permit ospf host 192.1.25.2 host 192.1.25.5
    40 permit tcp host 2.2.2.2 host 5.5.5.5 eq bgp
    50 permit tcp host 2.2.2.2 eq bgp host 5.5.5.5 (13 matches)
    60 permit icmp any any
    100 deny ip any any log
```

Task 2.2: Transparent Firewall (4 Points)

- Configure R7 as a zone-based transparent Firewall between VLAN 11 (outside) and VLAN 111 (inside). Deny all ICMP traffic, other than Echo and Echo Reply. Allow all other traffic
- Ensure any DHCP traffic is forwarded without inspection
- Log all session based information
- Limit the amount of inspected sessions per class to 125
- Police the allowed ICMP inbound traffic to 56k, using the minimum burst value

Detailed Solution

R7

```
bridge 1 protocol ieee
bridge 1 route ip
bridge irb

interface FastEthernet0/0
 bridge-group 1
 no shut

interface FastEthernet0/1
 bridge-group 1
 no shut

interface BVI1
 ip address 10.2.2.7 255.255.255.0

ip inspect L2-transparent dhcp-passthrough

parameter-map type inspect ZBFW_PM
 audit-trail on
 sessions maximum 125

ip access-list extended ICMP
 permit icmp any any echo
 permit icmp any any echo-reply

ip access-list extended ICMP_DROP
 deny   icmp any any echo
 deny   icmp any any echo-reply
 permit icmp any any

class-map type inspect match-all ICMP
 match access-group name ICMP

class-map type inspect match-all ICMP_DROP
 match access-group name ICMP_DROP

policy-map type inspect INOUT
 class type inspect ICMP_DROP
  drop
 class type inspect ICMP
```

```
  inspect ZBFW_PM
 class class-default
  pass

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ICMP
  inspect ZBFW_PM
  police rate 56000 burst 1000
 class type inspect ICMP_DROP
  drop
 class class-default
  pass

zone security IN
zone security OUT

zone-pair security INOUT source IN destination OUT
 service-policy type inspect ZFW_INOUT_POL

zone-pair security OUTIN source OUT destination IN
 service-policy type inspect ZFW_OUTIN_POL

interface FastEthernet0/1
 zone-member security OUT

interface FastEthernet0/0
 zone-member security IN
```

First stage of this task is to convert R7 into a transparent bridge using Integrated Routing and Bridging. We start with the 'bridge 1 protocol ieee' cmd which assigns bridge group id 1 and defines the spanning tree protocol (IEEE) for the group. R7 then needs to be configured to route the IP protocol across the bridge group. You then need to enable transparent bridging in IRB mode ('bridge irb'), this allows the ability in IOS to route and/or bridge traffic between interfaces.

The next step is to assign the bridge group to our interfaces, and create a bridged virtual interface to bind this routed instance to the bridge group. The BVI number should match the number assigned to the bridge group.

Now we move to the ZB FW Setup. CBAC/ZFW contains the layer2 DHCP pass-through feature, which allows DHCP traffic to be forwarded through the bridge without inspection, this occurs even if all traffic is denied, allowing client address allocation to succeed without interruption (in our case since we pretty much allow everything it does not help a lot but since it was required we had to enable it).

The next 2 sub tasks, logging and session limiting are enabled in the inspection parameter map, using the “audit trail” and “session maximum” commands. This is then enabled by assigning it to an inspection policy.

Follow the usual tasks for configuring the Zone Based Firewall. Here we created two ACLs to match on in the classes. The ICMP ACL which classifies the traffic we wont to allow and ICMP Drop ACL which denies the echo and echo reply that we want to be inspected, and permits any other ICMP that is required to be dropped. These are then added to the respective classes which are in turn added to the inspection policies, ensuring that all class and policy maps are of the same inspect type. Within the policy maps note that the parameter map ZBFW_PM is assigned after the inspect command, and that the class-default class is assigned the “pass” action. This allows all other traffic requirement for this task. For the inbound inspection policy we needed to police the ICMP traffic, to do this we first need to issue the “inspect” command in order for policing to function in the policy.

Finish of the configuration of this task by creating the zones (inside and outside) and the zone-pairs, assigning the inspection policies to the zone-pairs, and making the required interfaces members of each zone.

Verification

```
R1#ping 10.2.2.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R7#
*Jun  9 21:29:10.579: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-
(INOUT:ICMP):Start icmp session: initiator (10.2.2.1:8) -- responder
(10.2.2.8:0)
```

```
*Jun  9 21:29:21.371: %FW-6-SESS_AUDIT_TRAIL: (target:class)-
(INOUT:ICMP):Stop icmp session: initiator (10.2.2.1:8) sent 360 bytes --
responder (10.2.2.8:0) sent 360 bytes

R8#ping 10.2.2.1 rep 8

Type escape sequence to abort.
Sending 8, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!.!!!
Success rate is 87 percent (7/8), round-trip min/avg/max = 1/1/4 ms

R7#sh policy-firewall stats drop-counters
policy match failure                                    10
Police rate limiting                                    2

R7#sh policy-firewall stats zone-pair OUTIN

policy exists on zp OUTIN
 Zone-pair: OUTIN

  Service-policy inspect : ZFW_OUTIN_POL

    Class-map: ICMP (match-all)
      Match: access-group name ICMP

   Inspect
        Packet inspection statistics [process switch:fast switch]
        icmp packets: [0:24]

        Session creations since subsystem startup or last reset 1
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:0]
        Last session created 00:01:25
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0
```

```
        Police
         rate 56000 bps,1000 limit
         conformed 24 packets, 2736 bytes; actions: transmit
         exceeded 2 packets, 228 bytes; actions: drop
         conformed 0 bps, exceed 0 bps

    Class-map: ICMP_DROP (match-all)
      Match: access-group name ICMP_DROP
      Drop
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Pass
        0 packets, 0 bytes

R8#traceroute 10.2.2.1 timeout 1 probe 1 ttl 2 10

Type escape sequence to abort.
Tracing the route to 10.2.2.1

  2  *
  3  *
  4  *
  5  *
  6  *
  7  *
  8  *
  9  *
 10  *


R7#sh policy-firewall stats zone-pair INOUT

policy exists on zp INOUT
 Zone-pair: INOUT

  Service-policy inspect : ZFW_INOUT_POL
```

```
       Class-map: ICMP_DROP (match-all)
         Match: access-group name ICMP_DROP
         Drop
           18 packets, 648 bytes

       Class-map: ICMP (match-all)
         Match: access-group name ICMP

      Inspect
           Packet inspection statistics [process switch:fast switch]
           icmp packets: [0:10]

           Session creations since subsystem startup or last reset 1
           Current session counts (estab/half-open/terminating) [0:0:0]
           Maxever session counts (estab/half-open/terminating) [1:1:0]
           Last session created 00:06:43
           Last statistic reset never
           Last session creation rate 0
           Maxever session creation rate 1
           Last half-open session total 0
           TCP reassembly statistics
           received 0 packets out-of-order; dropped 0
           peak memory usage 0 KB; current usage: 0 KB
           peak queue length 0


       Class-map: class-default (match-any)
         Match: any
         Pass
           0 packets, 0 bytes

  R7#sh policy-firewall config parameter-map global
    alert on
    sessions maximum 2147483647
    waas disabled
    l2-transparent dhcp-passthrough enabled
    log dropped-packets disabled
    log summary disabled
    max-incomplete low 2147483647
    max-incomplete high 2147483647
```

```
    one-minute low 2147483647
    one-minute high 2147483647
    tcp reset-PSH disabled
```

Don’t forget to test the remaining part of the ASA’s NAT task :

```
R2#ping 195.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

3.0 Cisco IPS and Content Security (24 points)

Task 3.1: Basic IPS (4 Points)

- Configure the IPS Sensor's Management Interface through the CLI to allow access to the Sensor from VLAN 100 based on the Network Diagram
- Make sure you ping the IPS from R1 and manage the IPS via HTTPS port 4433
- You would like to monitor all traffic received in VLAN 12
- Configure the switches to copy all relevant traffic to the monitoring port G0/0
- Assign G0/0 to virtual sensor 0 and set G0/2 as an alternate reset interface

Detailed Solution

CAT4

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/2
 sw mode access
 no shut

interface GigabitEthernet1/0/4
 sw host
 sw acc vlan 12

monitor session 1 source vlan 12 rx
monitor session 1 destination interface Gi1/0/2
```

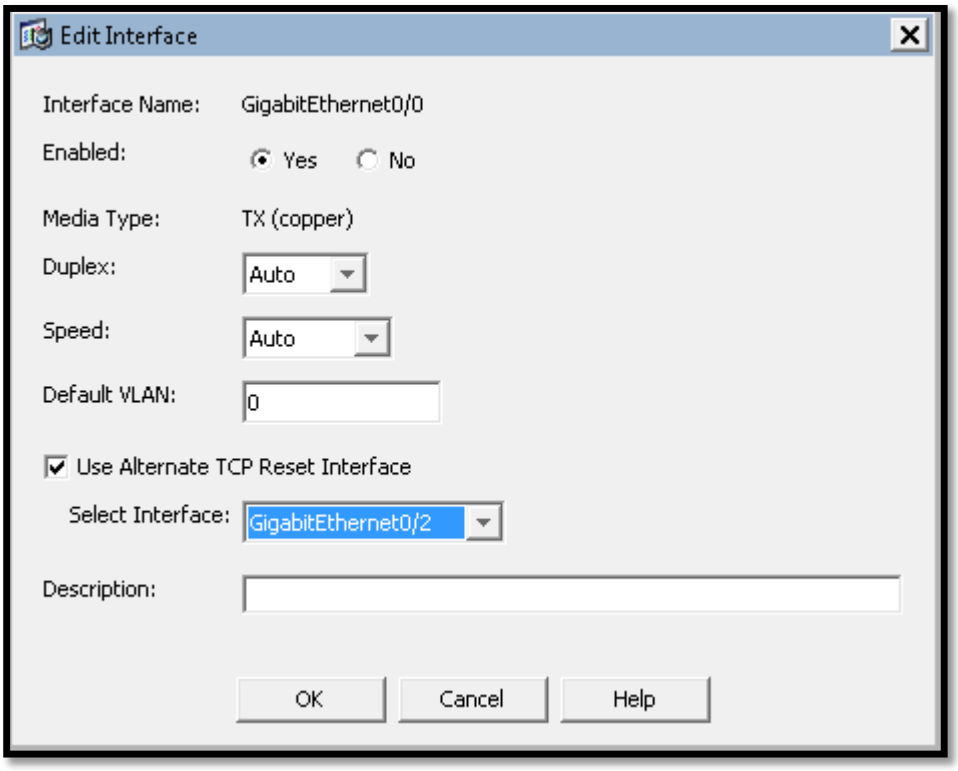
IPS

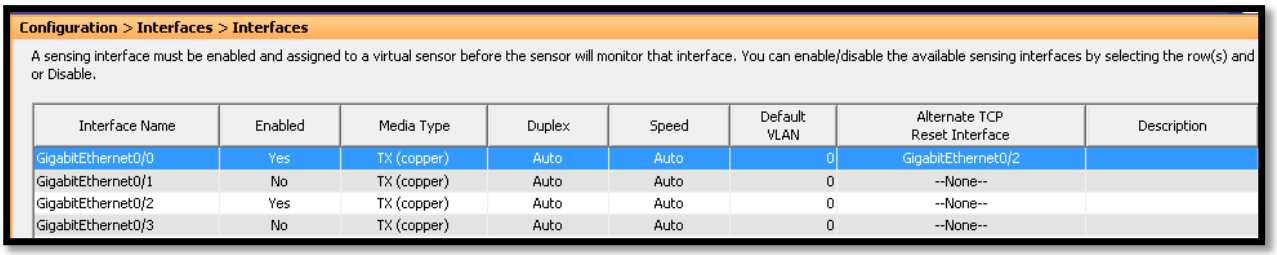
```
Enter host name[sensor]: IPS
Enter IP interface[192.168.1.2/24,192.168.1.1]: 10.1.1.15/24,10.1.1.1
```

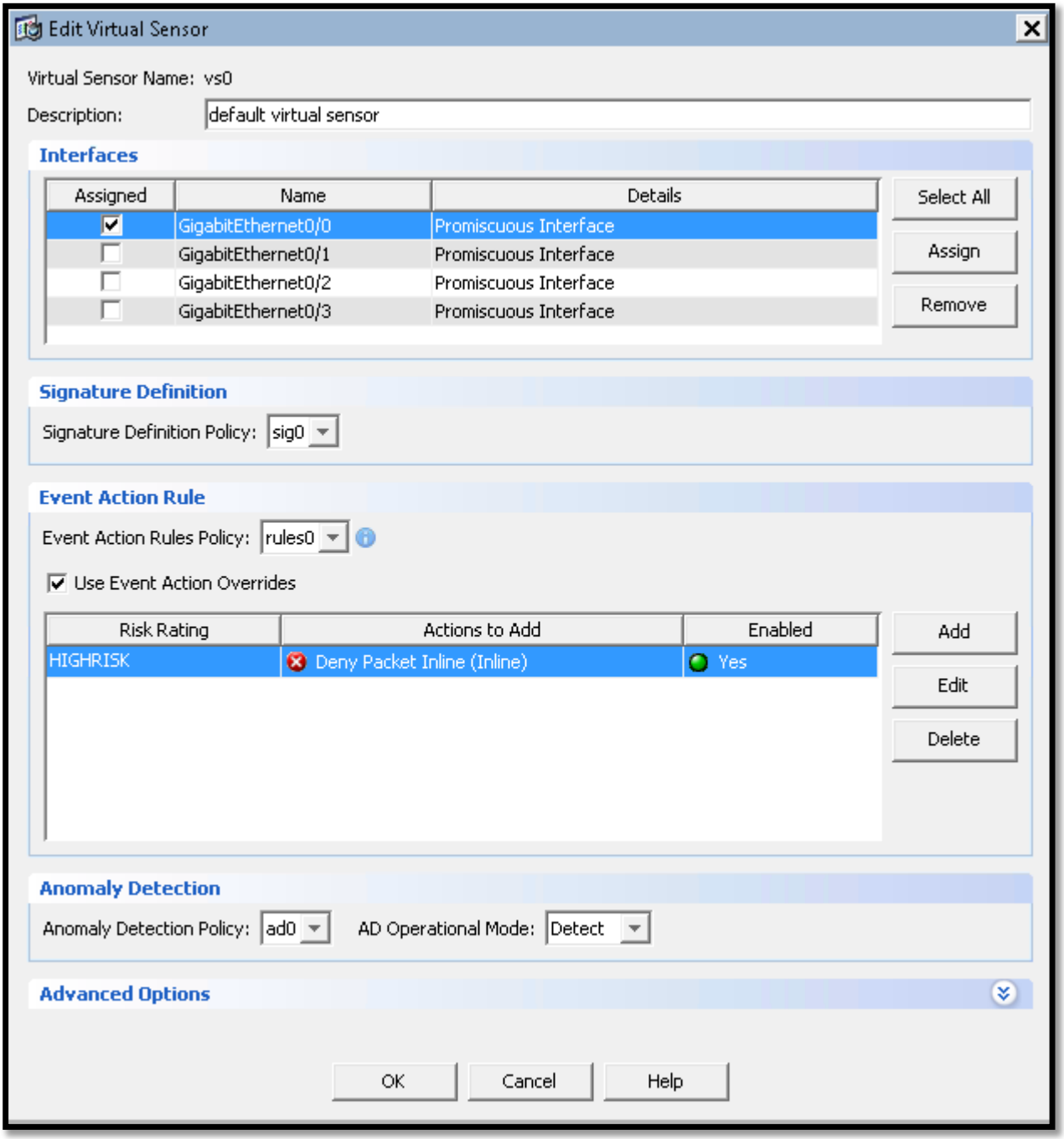
```
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.1.0/24
Permit:
Use DNS server for Global Correlation?[no]:
Use HTTP proxy server for Global Correlation?[no]:
Modify system clock settings?[no]:
Participation in the SensorBase Network allows Cisco to
collect 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]: 2

conf t
 port 4433
```

Now connect from the browser using port 4433. Configure the Alternate Interface, enable G0/0 and G0/2 ports and assign G0/0 to the default sensor :







Okay. So we see that we are required to do a few things here. First, setup the IPS from the CLI so we can gain connectivity via VLAN 100. The easiest way to do this is by running the setup wizard, this is a test based wizard that guides us through the initial setup process. Simply type 'setup' from the CLI to begin. Here we assign the name, the IP address with prefix mask , the gateway, and modify the current access-list. By default the IPS does not allow any IPs to

manage the device, so you need to add the IP address/subnet of any management stations into this ACL. Our task required us to allow VLAN 100 to manage the IPS so go ahead and enter VLAN 100's IP subnet in here, again with the prefix mask, not the usual subnet mask. Press enter on a blank line to exit the modify ACL portion of the wizard.

After accepting the default of not modifying the clock you will be presented with four menu options (0-3), as we are asked to modify the web server port number we should continue to the advanced setup (option 3) or select 2 and configure it from the CLI

Before moving on we need to configure the switches for the IPS. As the question refers to copying the traffic to G0/0 we need to use SPAN/RSPAN sessions for promiscuous capture. Since CAT4 is the root for VLAN 12 and other path between CAT2 and CAT3 is blocked for that VLAN, all traffic between R2 and ASA3 will always transit CAT4. So we can simply SPAN all received packets in VLAN 12 on that switch.

Don't forget to configure a switchport for IPS's G0/2 – CAT4 G1/0/4 needs to be in access VLAN 12, as it will be used for the alternate TCP Reset interface.

Verification

```
R1#ping 10.1.1.15

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.15, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

CAT4#sh mon sess 1
Session 1
---------
Type                   : Local Session
Source VLANs           :
    RX Only            : 12
Destination Ports      : Gi1/0/2
    Encapsulation      : Native
          Ingress      : Disabled


IPS# packet display gigabitEthernet0/0 expression ip proto \icmp
Warning: This command will cause significant performance degradation
```

```
tcpdump: WARNING: ge0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 65535 bytes

R2#ping 192.1.12.30 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 192.1.12.30, timeout is 2 seconds:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms


23:06:44.951392 IP 192.1.12.2 > 192.1.12.30: ICMP echo request, id 2, seq
0, length 80
23:06:44.951692 IP 192.1.12.30 > 192.1.12.2: ICMP echo reply, id 2, seq 0,
length 80
23:06:44.952091 IP 192.1.12.2 > 192.1.12.30: ICMP echo request, id 2, seq
1, length 80
23:06:44.952191 IP 192.1.12.30 > 192.1.12.2: ICMP echo reply, id 2, seq 1,
length 80
```

Task 3.2: Signatures (4 Points)

- Create a new virtual sensor called vs1, while also cloning the existing policy objects to create sig1, rules1 and ad1 that will be assigned to that sensor
- Using interface G0/1 create a VLAN pair between VLAN 11 and R7
- Use VLAN 211 as the additional VLAN for R7
- Configure the signatures so you can see a similar output on IPS CLI :

```
IPS# show events alert

evIdsAlert: eventId=1041379286523809524 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/10 12:06:56 2013/06/10 12:06:56 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
```

```
      marsCategory: Info/AllSession
    interfaceGroup: vs1
    vlan: 211
    participants:
      attacker:
        addr: locality=OUT 10.2.2.1
      target:
        addr: locality=OUT 192.1.12.2
        os: idSource=unknown relevance=relevant type=unknown
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
    threatRatingValue: 35
    interface: ge0_1
    protocol: icmp


  evIdsAlert: eventId=1041379286523809525 severity=informational vendor=Cisco
    originator:
      hostId: IPS
      appName: sensorApp
      appInstanceId: 413
    time: 2013/06/10 12:06:56 2013/06/10 12:06:56 UTC
    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 192.1.12.1
      target:
        addr: locality=OUT 192.1.12.2
        os: idSource=unknown relevance=relevant type=unknown
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
    threatRatingValue: 35
    interface: ge0_0
  protocol: icmp
```

Detailed Solution

CAT4

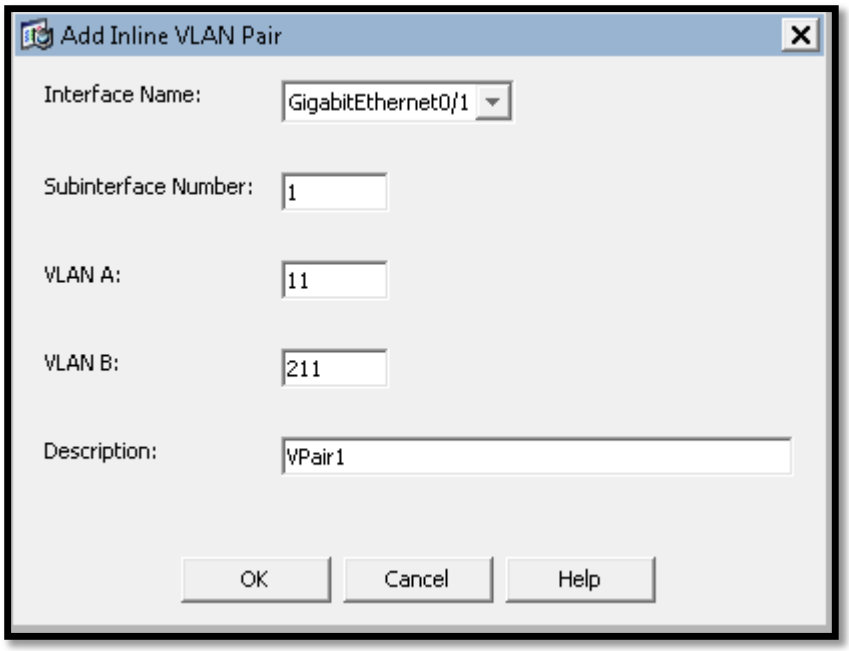
```
vlan 211

interface GigabitEthernet1/0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 11,211
 switchport mode trunk
```

CAT2

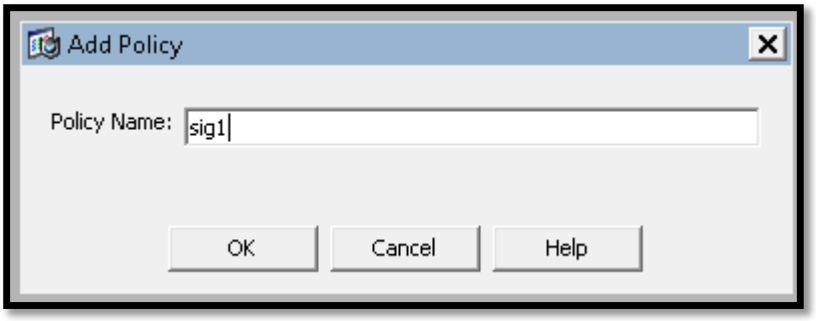
```
int f0/7
 sw acc vlan 211
```

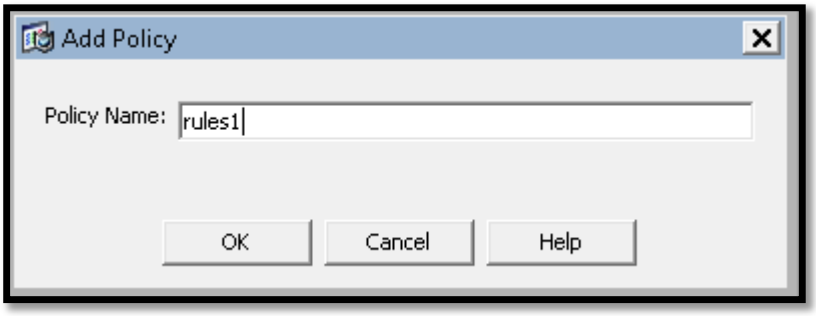
IPS

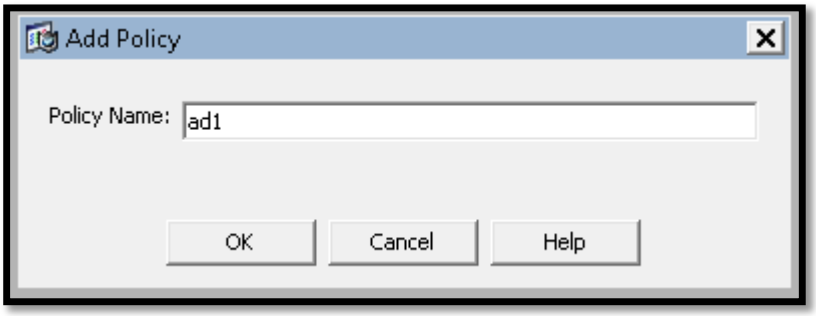
Bring up G0/1 and then configure a VLAN Pair :



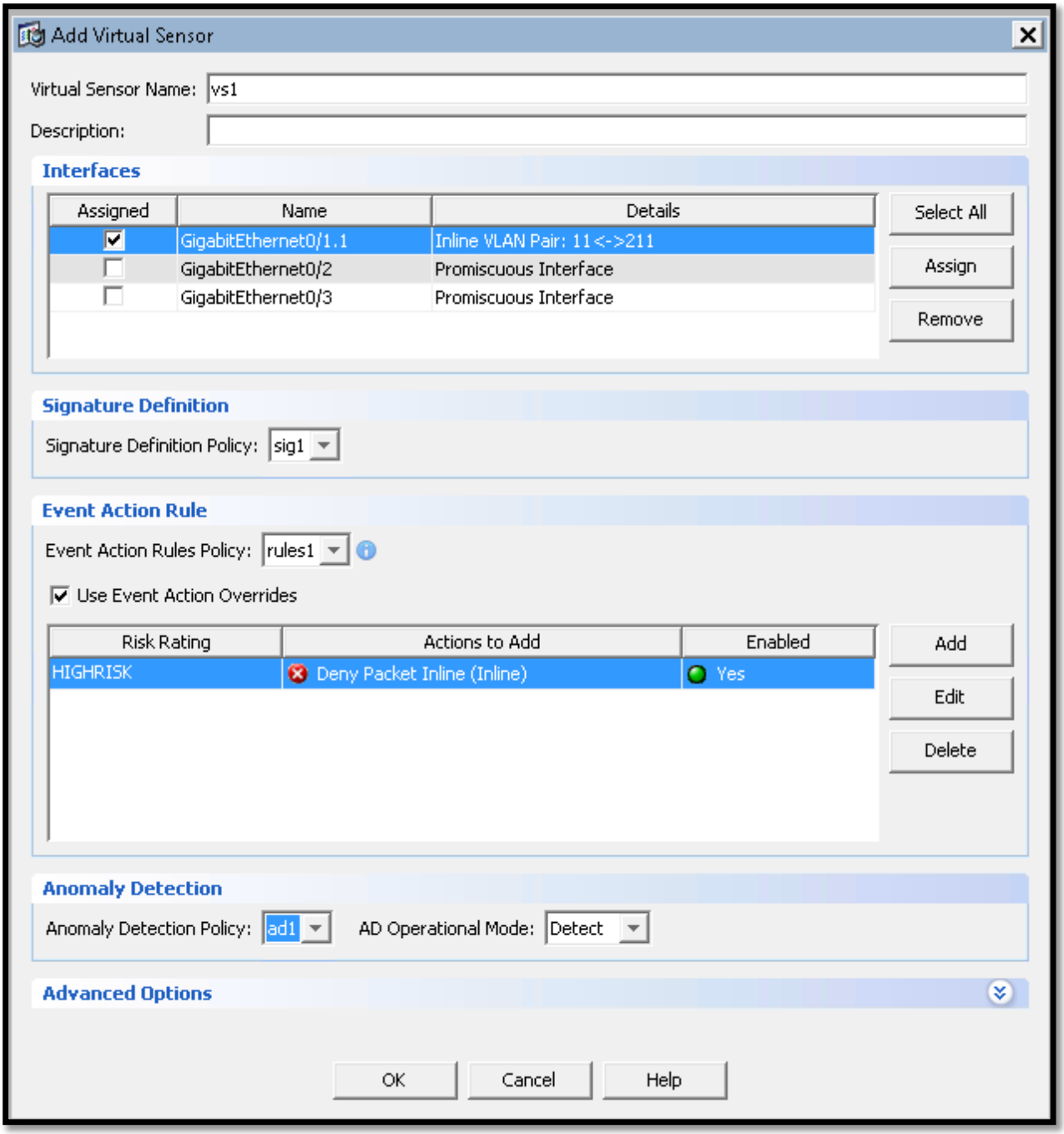
Add a new set of Signatures, Event Action Rules and Anomaly Detection. Click on “Signature Definitions”/”Event Action Rules”/”Anomaly Detections” on the left-hand window and add a respective policy :



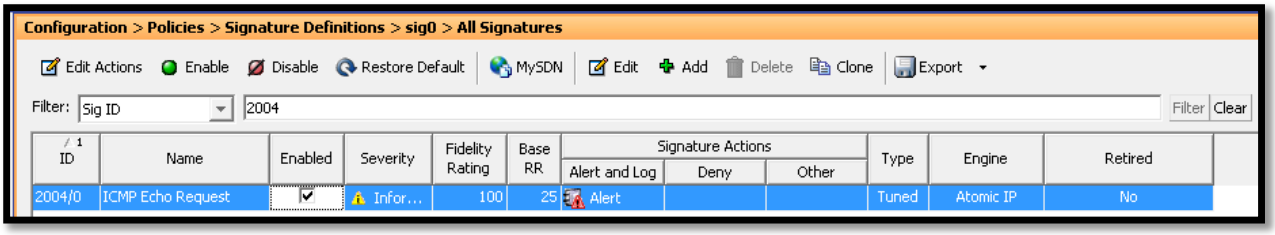




Now add a Virtual Sensor; select appropriate ruleset and assign the VLAN Pair :



Finally enable ICMP Echo Request (2004) signatures under sig0 and sig1 :



As of v6.x code the IPS has the ability to create multiple virtual sensors. This gives you the advantage of having separate policies, to protect different areas of the network, and not be bound by a single set of signature definitions for example. The IPS is capable of running up to four virtual sensors.

Based on the output show in the question we see that two Virtual Sensors are activated. Signature 2004 was triggered and the attacker is R1 (once with its original IP and then with a translated one). This gives us a hint on what signature to enable and under what signature ruleset (both in our case).

Verification

```
IPS# sh interfaces brief
CC    Interface              Sensing State    Link    Inline Mode         Pair
Status
      GigabitEthernet0/0     Enabled          Up      Unpaired            N/A
*     Management0/0          Disabled         Up
      GigabitEthernet0/1     Enabled          Up      Inline-vlan-pair    N/A
      GigabitEthernet0/2     Enabled          Up      Unpaired            N/A
      GigabitEthernet0/3     Disabled         Down    Unpaired            N/A

IPS# show events alert

R1#ping 192.1.12.2 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
```

```
IPS#
evIdsAlert: eventId=1041379286523809524 severity=informational
vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/10 12:06:56 2013/06/10 12:06:56 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127
type=other version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs1
  vlan: 211
  participants:
    attacker:
      addr: locality=OUT 10.2.2.1
    target:
      addr: locality=OUT 192.1.12.2
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
  threatRatingValue: 35
  interface: ge0_1
  protocol: icmp


evIdsAlert: eventId=1041379286523809525 severity=informational
vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/10 12:06:56 2013/06/10 12:06:56 UTC
  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 192.1.12.1
      target:
        addr: locality=OUT 192.1.12.2
        os: idSource=unknown relevance=relevant type=unknown
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
35
    threatRatingValue: 35
    interface: ge0_0
    protocol: icmp
```

Task 3.3: Custom IPS Signature (3 Points)

- For vs0 create a custom string signature that detects the word “cmd.exe” anywhere in a HTTP URL. Allow for any case in the string
- Set the Alarm Severity to High, and reset the TCP connection
- When R2 does a broadcast DNS lookup, signature 4620 fires on the IDS sensor
- Configure R2 to not send DNS broadcasts. Also, disable signature 4620 on the IDS sensor

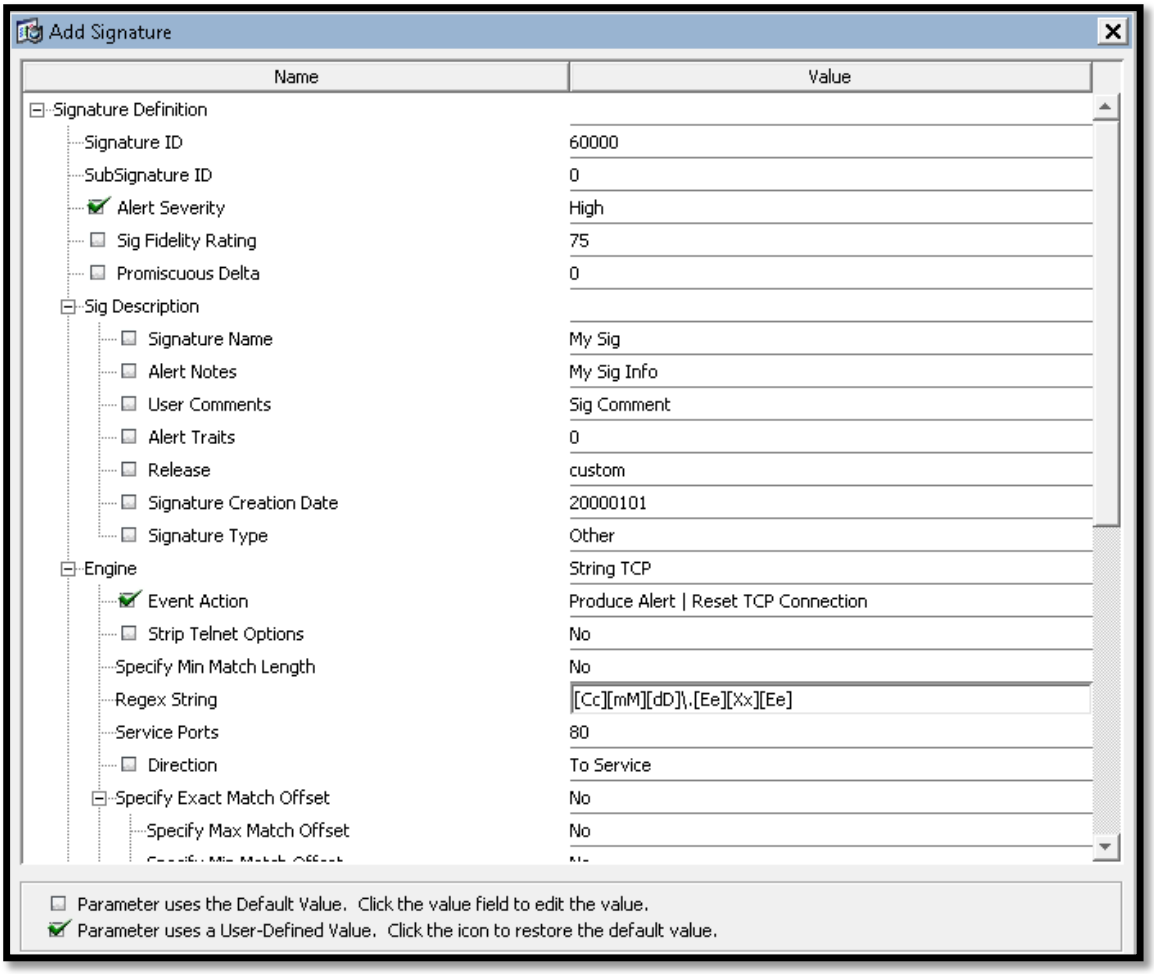
Detailed Solution

R2

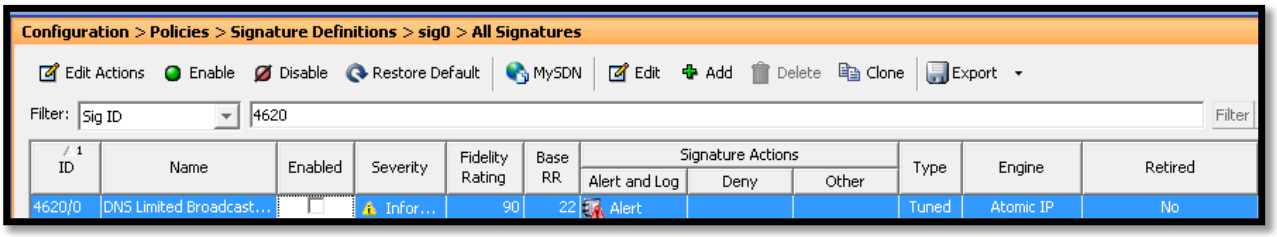
```
no ip domain-lookup
```

IPS

Configure a signature – you can either use a Signature Wizard or add manually as in the solution below :



Then disable signature 4620 :



This task is fairly straightforward. As we want to detect a string in an HTTP URL, the String TCP engine seems the logical choice. The only real stumbling block here would be the regex string.

As we are looking to match on any case of the string cmd.exe, we need to encapsulate both the uppercase and lowercase instance of each character within square brackets. The correct regex string would be: **[Cc][Mm][Dd]\.[Ee][Xx][Ee]**

Note that the period character is preceded by the backslash character. The role of the period character in a regex is to match on any single character, so to ensure we only match the '.' we place a backslash to denote this is not a special character.

Verification

Allow HTTP to R1 on ASA3 and enable HTTP server on the router. Then try to download the file from R2 :

```
R2#copy http://192.1.12.1/cMd.ExE null0
Destination filename [null0]?
%Error opening http://192.1.12.1/cMd.ExE (I/O error)

R2#
*Jun 10 15:17:33.987: TCP0: RST received, Closing connection
*Jun 10 15:17:33.987: TCP0: state was ESTAB -> CLOSED [26082 ->
192.1.12.1(80)]
*Jun 10 15:17:33.991: Released port 26082 in Transport Port Agent for TCP
IP type 1 delay 240000
*Jun 10 15:17:33.991: TCB 0x70DBDE98 destroyed

IPS#
evIdsAlert: eventId=1041379286523809628 severity=high vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/10 15:16:01 2013/06/10 15:16:01 UTC
  signature: description=My Sig 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 192.1.12.2
      port: 35765
    target:
      addr: locality=OUT 192.1.12.1
      port: 80
      os: idSource=unknown relevance=relevant type=unknown
  actions:
    resetTcpFlowSent: true
  context:
    fromAttacker:
000000  47 45 54 20 2F 63 4D 64  2E 45 78 45 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 31 32 2E 31 0D 0A  st: 192.1.12.1..
000040  44 61 74 65 3A 20 4D 6F  6E 2C 20 31 30 20 4A 75  Date: Mon, 10 Ju
000050  6E 20 32 30 31 33 20 31  35 3A 31 36 3A 30 34 20  n 2013 15:16:04
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
85
  threatRatingValue: 65
  interface: ge0_0
  protocol: tcp
```

Task 3.4: ASA IPS (3 Points)

- Configure the ASA to send message to the SYSLOG server 10.1.1.190
- Configure Console Logging to level 4. Configure Trap logging level to debugging
- Configure ASA3 IPS with the following parameters :
  - Send an alarm for Info signatures
  - Send an alarm and drop packets for Attack signatures
  - Enable the IPS sensing on the outside interface of the ASA
- There are a large amount of false positives for DNS Zones Transfers, prevent these alarms from being generated regardless of the port used

Detailed Solution

ASA3

```
logging enable
logging console warnings
logging trap debugging
logging host inside 10.1.1.190

ip audit name IPS_A attack action alarm drop
ip audit name IPS_I info action alarm

ip audit interface outside IPS_I
ip audit interface outside IPS_A

ip audit signature 6051 disable
ip audit signature 6052 disable
```

Logging is part of the basic setup of network devices in general, and should be familiar to all, whether it's locally logging to a buffer, monitor or console, or to an external syslog server.

The IDS/IPS functionality of the ASA (not to confuse with IPS module) is pretty limited, making configuration fairly simple. IPS Policies are created using the 'ip audit name' cmd and we define both an info signature policy and attack signature policy as required. Each policy is then enabled by being allocated to an interface. All that's really left for IDS on the ASA is the ability to enable / disable signatures.

In this task we are asked to disable signatures related to DNS zone transfers. Create the policies and enable them. You can then use the 'show ip audit count' cmd, to view the current signatures :

```
ASA3/act(config)# sh ip audit count | in DNS
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
```

Note that we have 2 sigs related to DNS Zone transfers 6051 & 6052. We simply disable these signatures to prevent false positives alarms.

Verification

Ping through the ASA and observe logs :

```
%ASA-4-400014: IDS:2004 ICMP echo request from 192.1.12.2 to 192.1.12.1 on
interface outside
%ASA-4-400014: IDS:2004 ICMP echo request from 192.1.12.2 to 192.1.12.1 on
interface outside
%ASA-4-400014: IDS:2004 ICMP echo request from 192.1.12.2 to 192.1.12.1 on
interface outside
%ASA-4-400014: IDS:2004 ICMP echo request from 192.1.12.2 to 192.1.12.1 on
interface outside

ASA3/act(config)# sh loggi
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: level warnings, 1043 messages logged
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: level debugging, facility 20, 278 messages logged
    Logging to inside 10.1.1.190
Permit-hostdown logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Task 3.5: WSA Setup (4 Points)

- Configure WSA interfaces according to the topology & addressing table
- Initialize Web Security Appliance with the following settings :
  - Use 10.1.1.101 as the NTP and DNS server
  - Password MUST BE SET TO “ironport”
  - Use a single interface for management and proxy functions
  - Web Reputation should be disabled
  - Disable McAfee and Webroot scanning engines
- Set default gateway to ASA3
- Make sure Test PC in VLAN 100 can manage WSA

Detailed Solution

CAT3

```
int g1/0/3
 sw host
 sw acc vlan 11
```

WSA

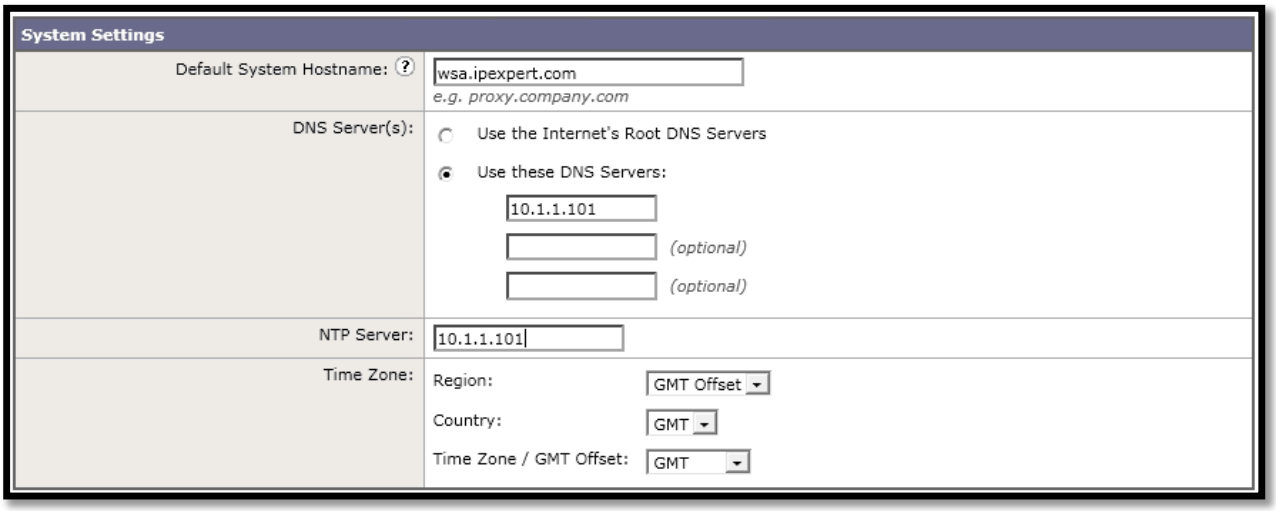
```
ironport.example.com> interfaceconfig

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.example.com)
```

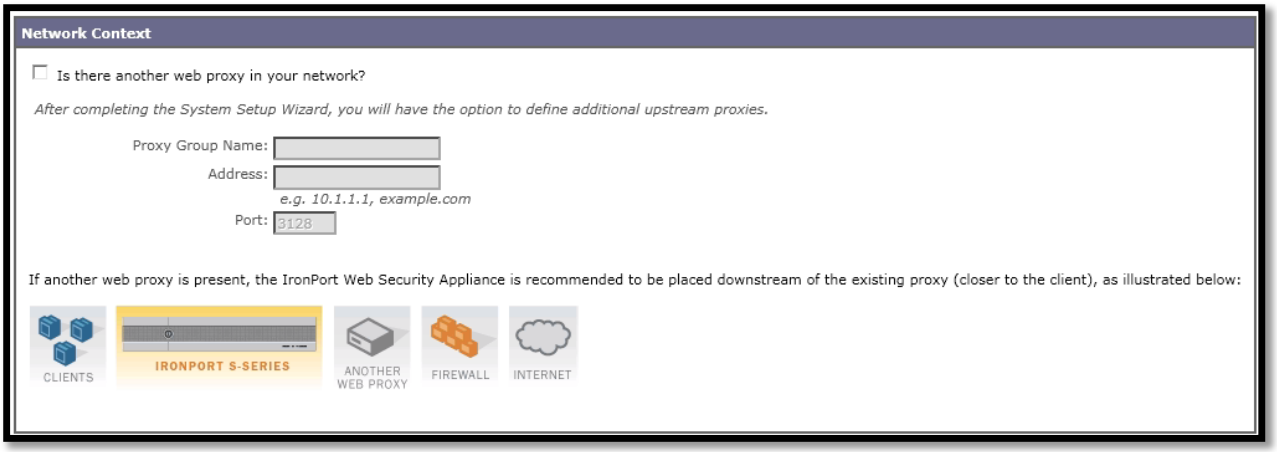
```
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP Address (Ex: 192.168.1.2):
[192.168.42.42]> 10.2.2.180

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.0

Hostname:
[ironport.example.com]> wsam.ipexpert.com

Do you want to enable FTP on this interface? [Y]>

Which port do you want to use for FTP?
[21]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?
[22]>

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?
[8080]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?
[8443]>

You have not entered an HTTPS certificate.  To assure privacy, run
"certconfig" first.  You may use the demo, but this will not be secure.
```

```
Do you really wish to use a demo certificate? [Y]>

Both HTTP and HTTPS are enabled for this interface, should HTTP requests
redirect to the secure service? [Y]>

The interface you edited might be the one you are currently logged into.
Are
you sure you want to change it? [Y]>

Please run System Setup Wizard at http://192.168.42.42:8080
ironport.example.com>


ironport.example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]> management

Currently configured routes:
No routes currently configured.

Choose the operation you want to perform:
- NEW - Create a new route.
[]> new

Please create a name for the route:
[]> VLAN100

Please enter the destination IP address to match on.
CIDR addresses such as 192.168.42.0/24 are also allowed.
[]> 10.1.1.0/24

Please enter the gateway IP address for traffic to 10.1.1.0/24:
[]> 10.2.2.1

Currently configured routes:
1. VLAN100 Destination: 10.1.1.0/24 Gateway: 10.2.2.1
```

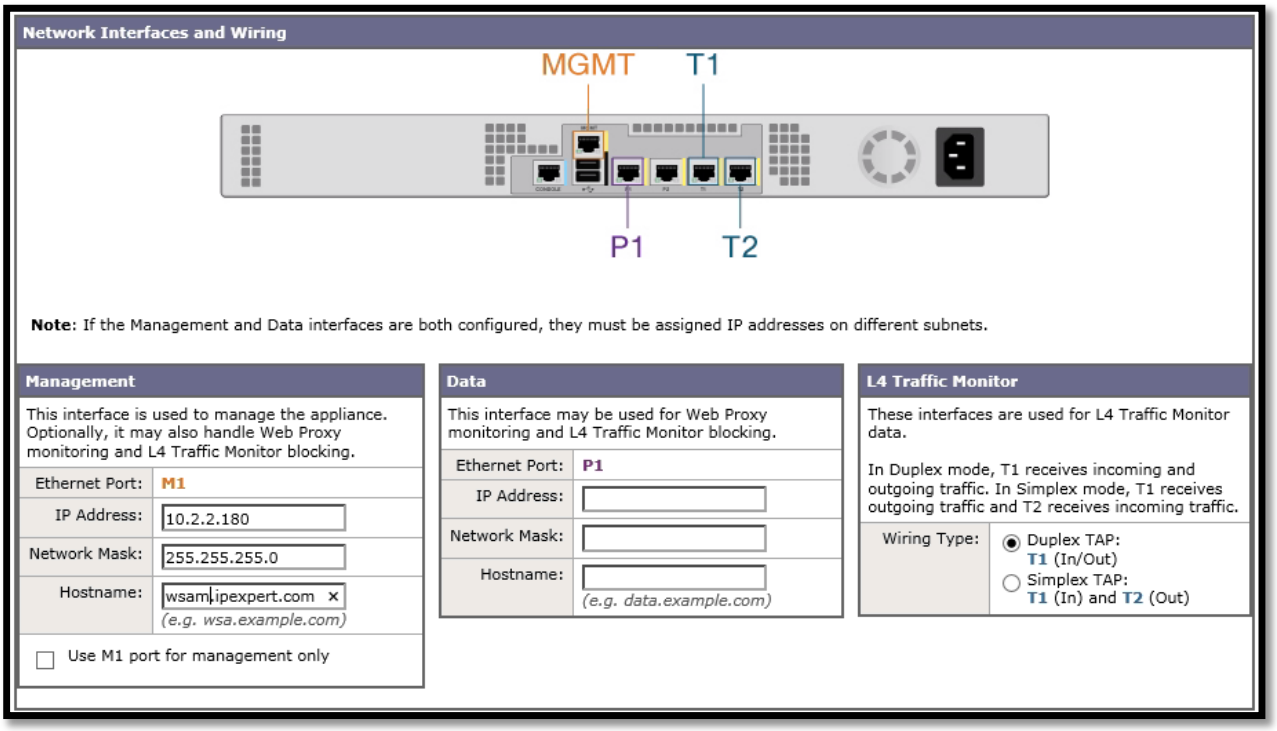
```
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[]>

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>

Please run System Setup Wizard at http://192.168.42.42:8080
ironport.example.com> commit

Please enter some comments describing your changes:
[]>
```

Add a route on Test PC to VLAN 11 (10.2.2.0/24). Then connect to 10.2.2.180 using port 8080 (HTTP) or 8443 (HTTPs) and run the System Setup Wizard (under "System Administration"). Configure hostname, DNS & NTP Servers and basic interface settings :

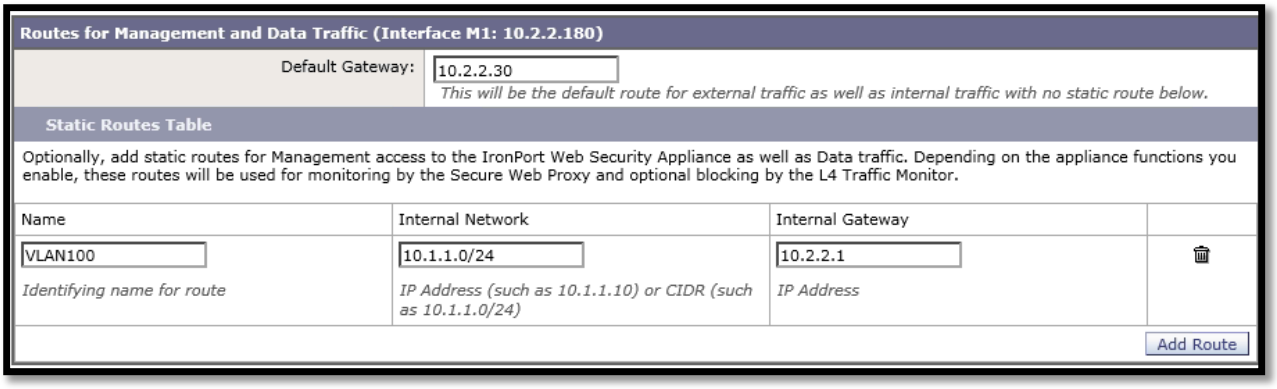


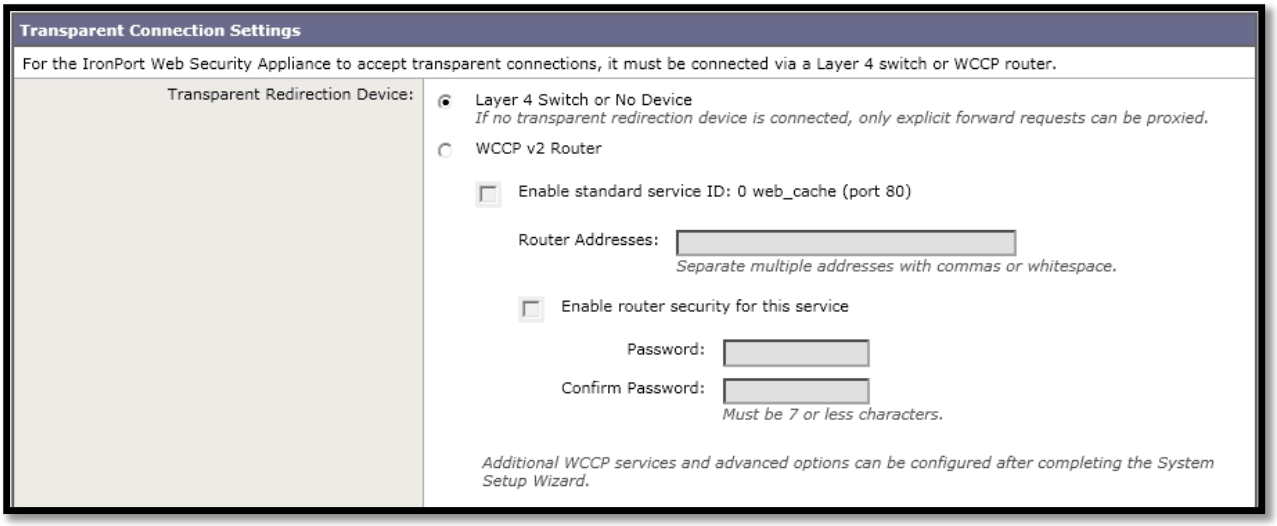


Don't check „Use M1 port for management only". This way the port will be also used for the data traffic :

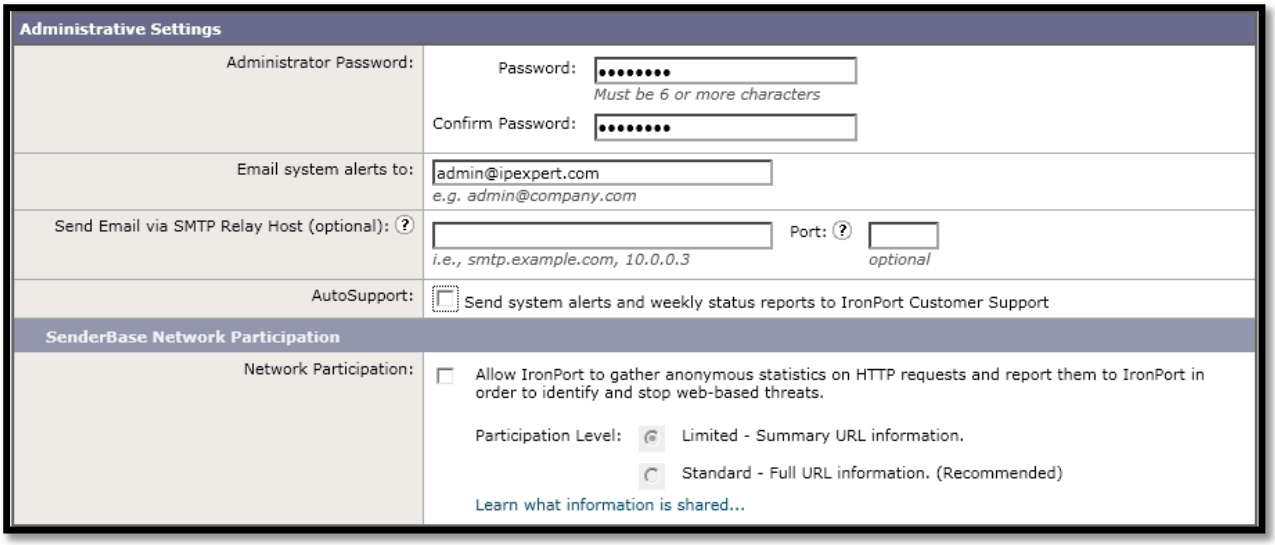


Specify a default gateway and static route to VLAN 100 once again. If you add the latter one you will loss connectivity to WSA assuming you are connecting from VLAN 100 :

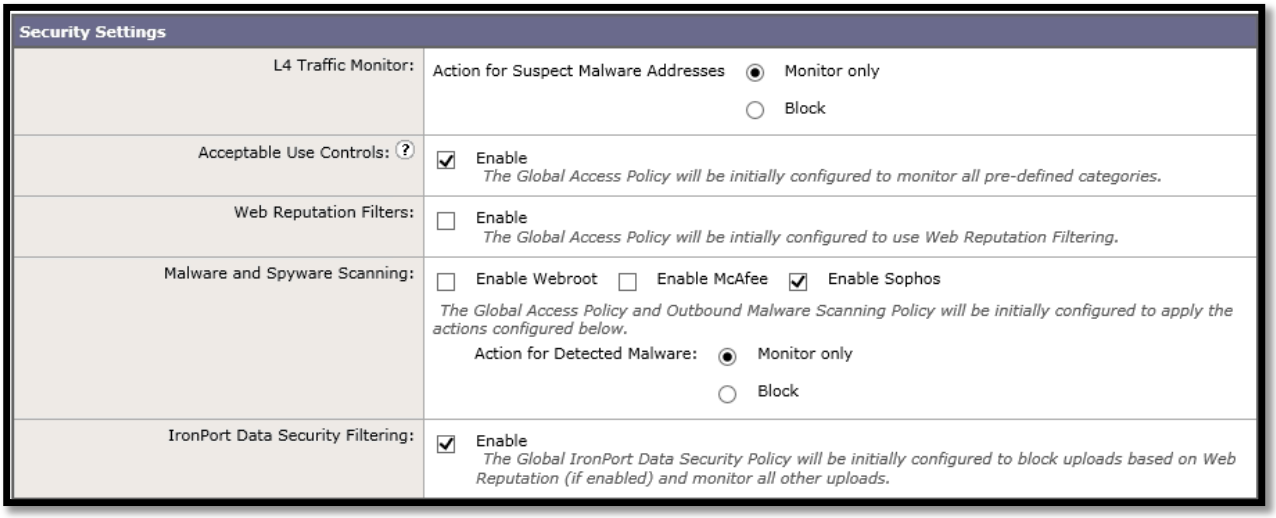




Password MUST be “ironport” :



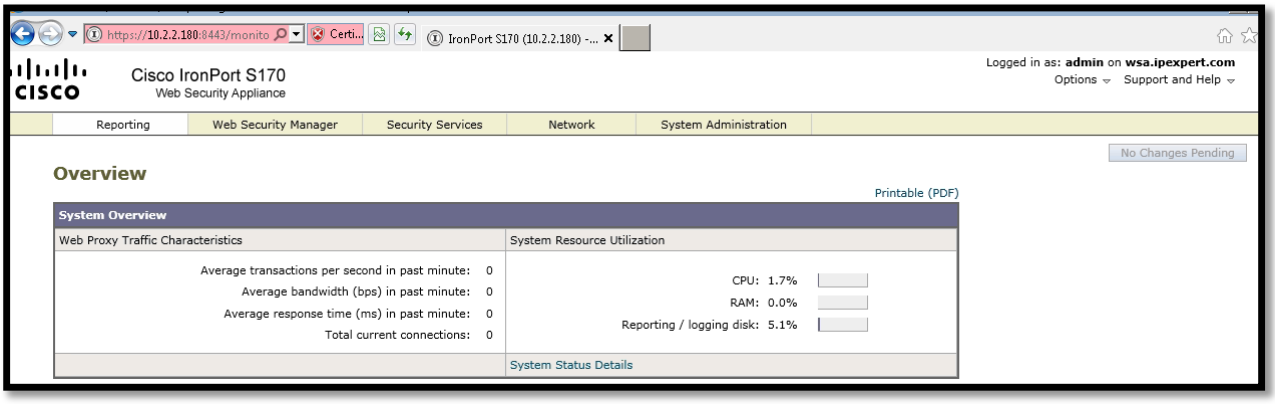
Turn off Web Reputation and two requested Scanning Engines :



It's a somewhat similar approach in configuring WSA as with IPS. We want to make sure L2 configuration is correct and that initialize few basic settings from the CLI so we can access WSA through the GUI. Then probably the fastest way is to use a Setup Wizard to configure other basic settings although you could enable everything manually.

Verification

```
ironport.example.com> ping 10.1.1.200

Press Ctrl-C to stop.
PING 10.1.1.200 (10.1.1.200): 56 data bytes
64 bytes from 10.1.1.200: icmp_seq=0 ttl=127 time=5.914 ms
64 bytes from 10.1.1.200: icmp_seq=1 ttl=127 tim^C
--- 10.1.1.200 ping statistics ---
```



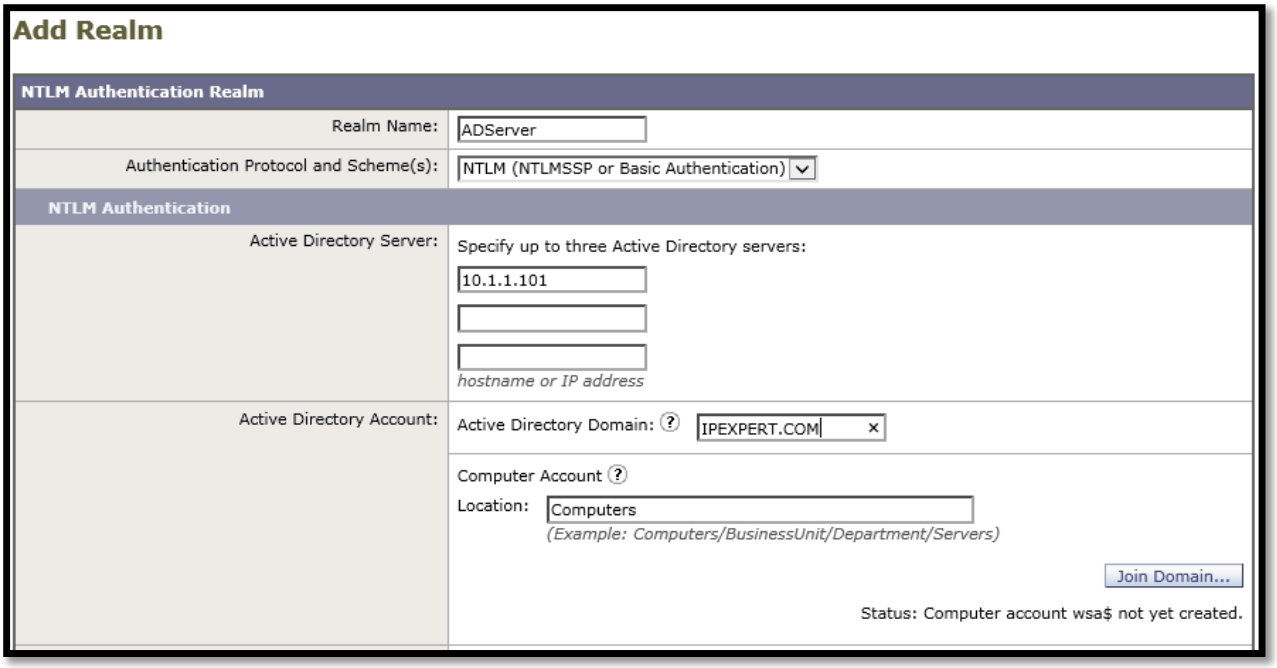
Task 3.6: WSA Advanced Configuration (6 Points)

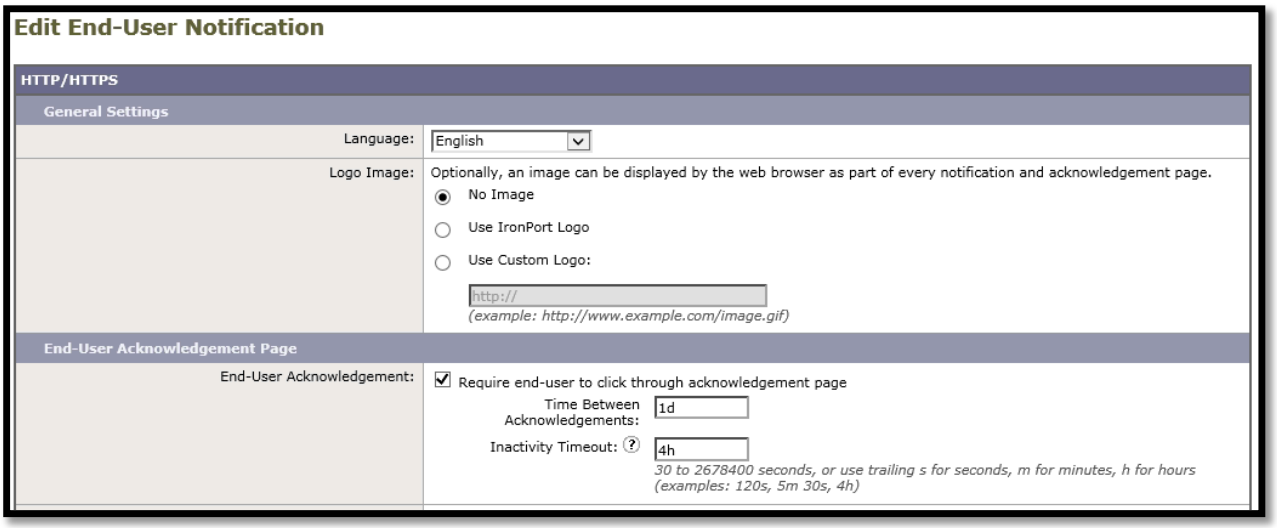
- Integrate WSA with the AD Server. The domain name is "IPEXPERT.COM"
- Use "Administrator" with password "IPexpert123" to join the domain
- Enable End-User Notifications
- Create a custom Policy which ensures that access to the following websites/domains never requires authentication :
  - update.microsoft.com (domain)
  - windowsupdate.com (domain)
  - mirrorlist.centos.com (domain)
  - mirror.centos.org (server)
- Configure WSA to limit the overall bandwidth for downloaded content to 50Mbps
- All Media applications except QuickTime should be limited to 5Mbps each (don't set a limit for QuickTime)
- Restrict users who try to upload files through WSA :
  - A maximum size of uploaded files should be 2Mbps for HTTP/HTTPs and 10Mbps when they use FTP
  - Microsoft Office docs can be only uploaded when they are smaller than 1Mb
  - PDF files should never go through the WSA

Detailed Solution

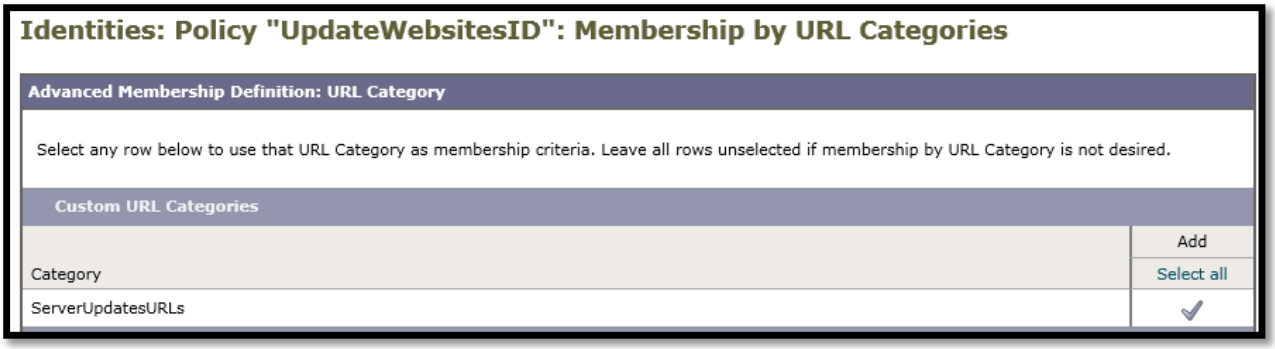
WSA

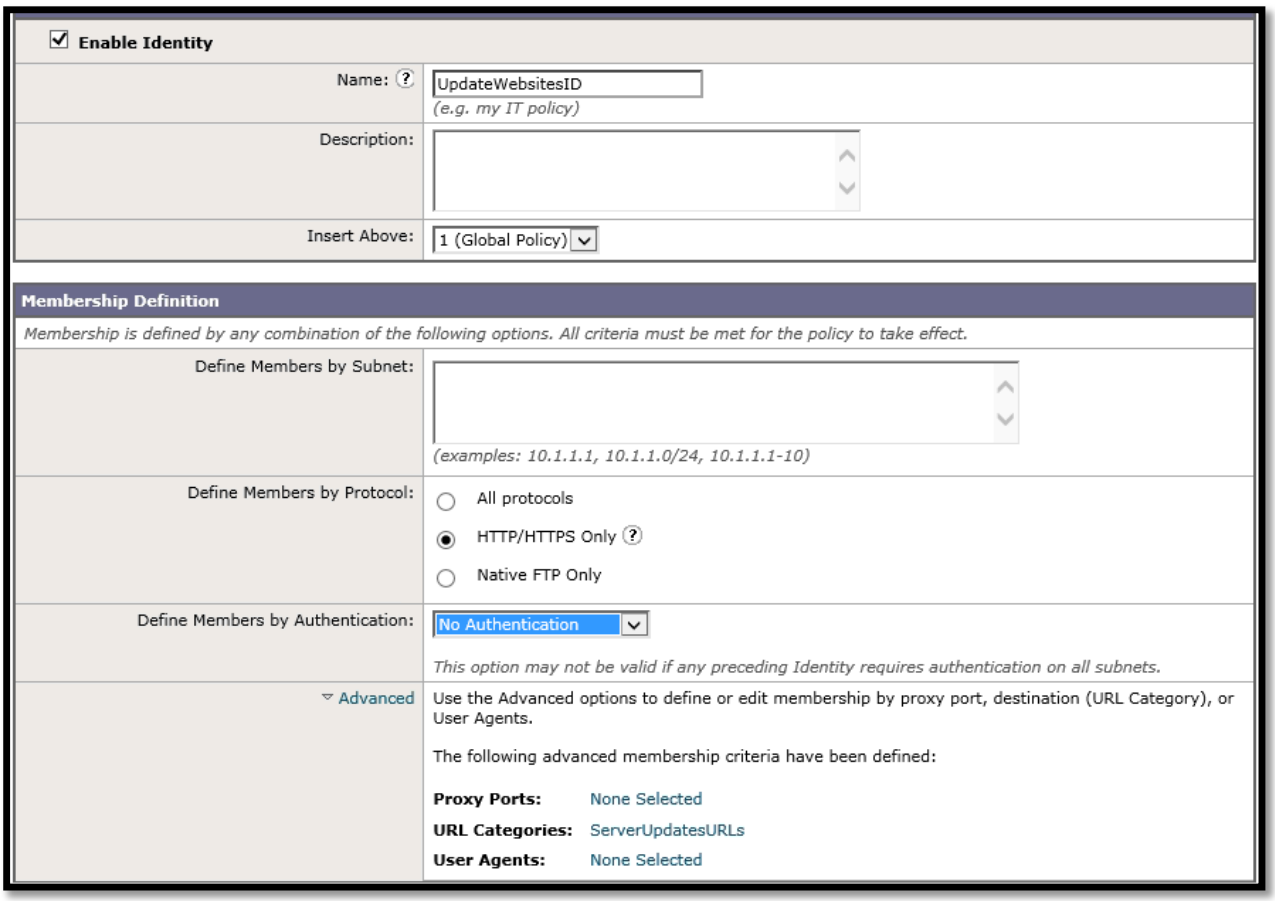
First integrate with AD (Network -> Authentication) and enable End User Notifications (Security Services -> End-User Notifications) :



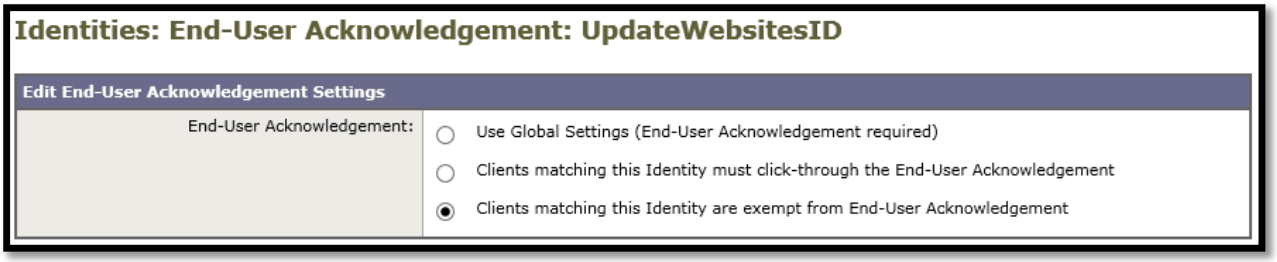


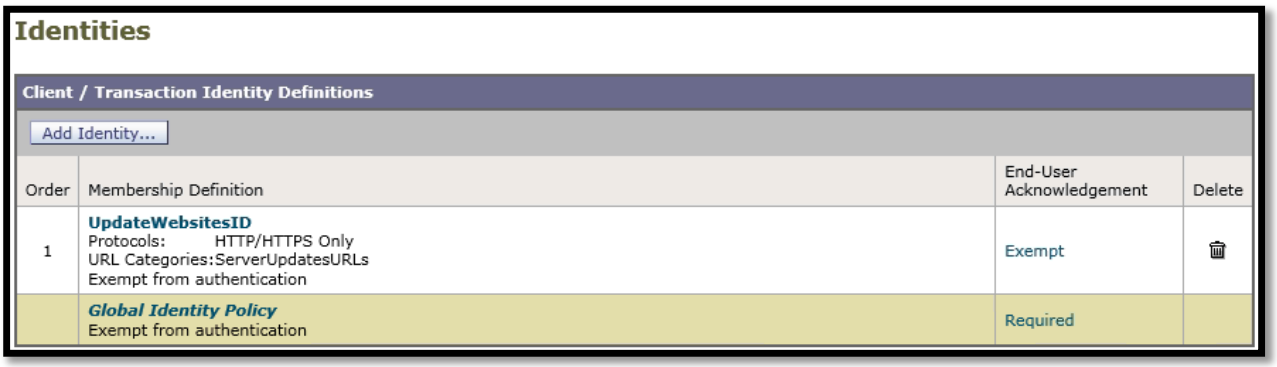
Now create a new Identity Policy. Select an Advanced option “URL Categories”. Make sure Authentication is off :



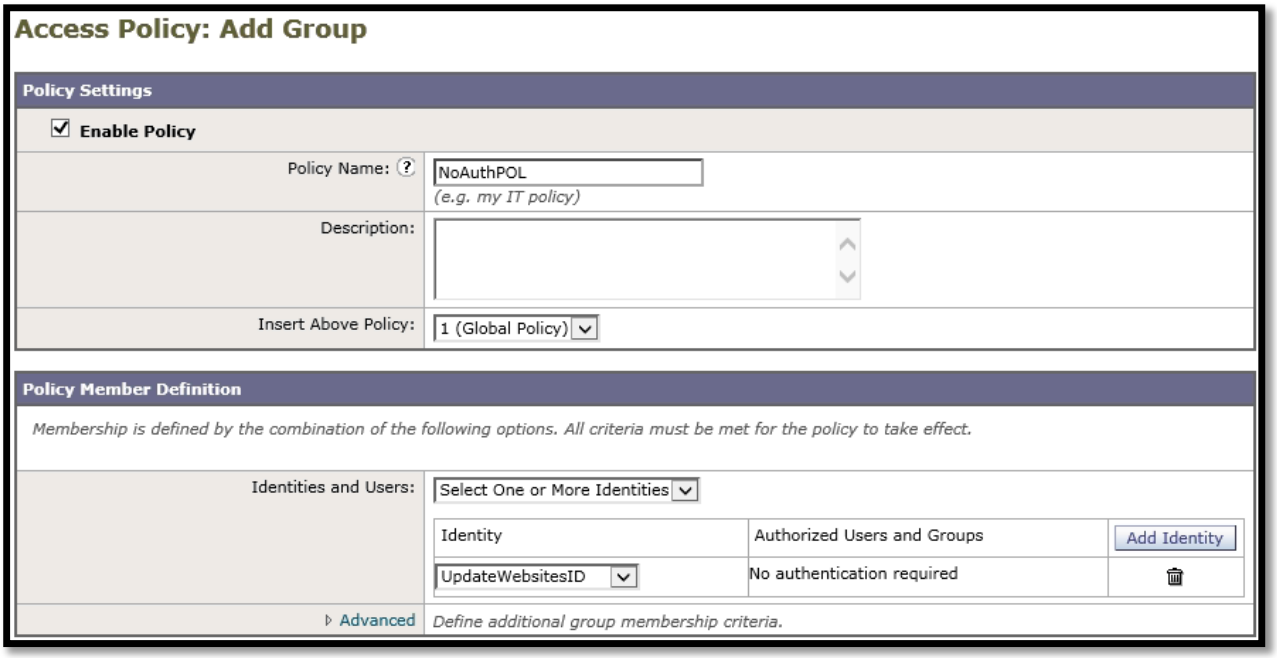


Although not explicitly stated in the question you also want to exempt this Identity from EUA :

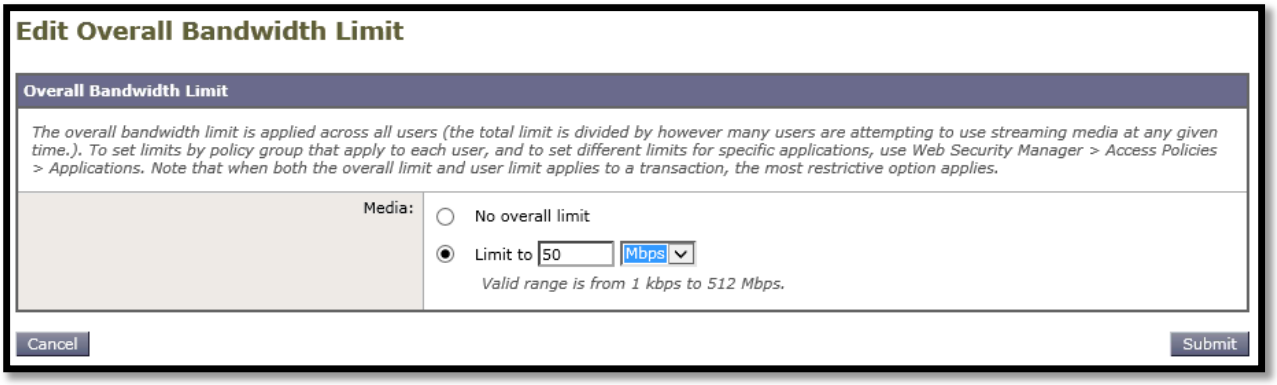




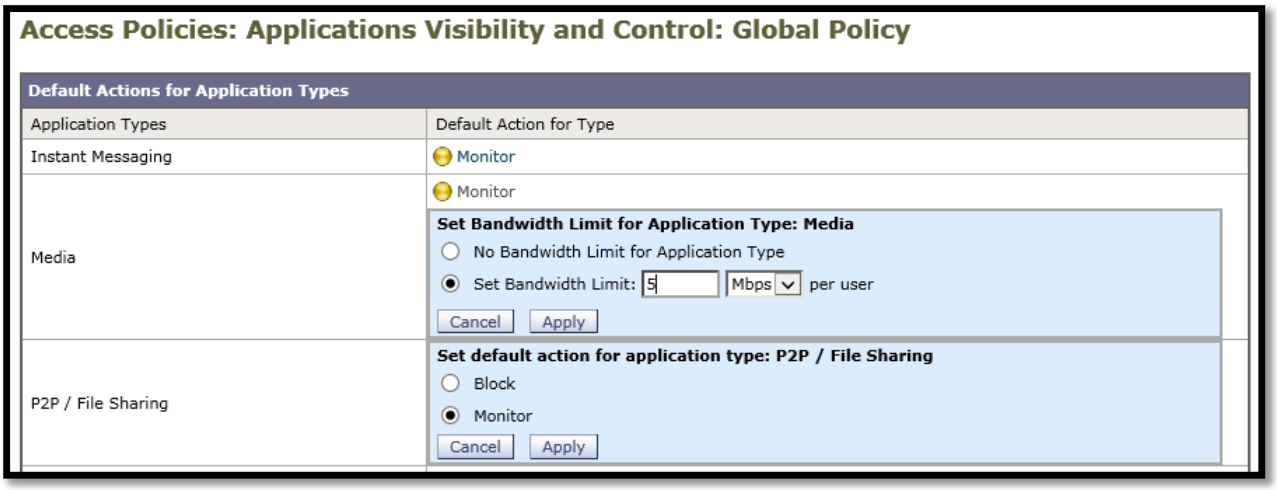
Create new Access Policy. Use previously created Identity :

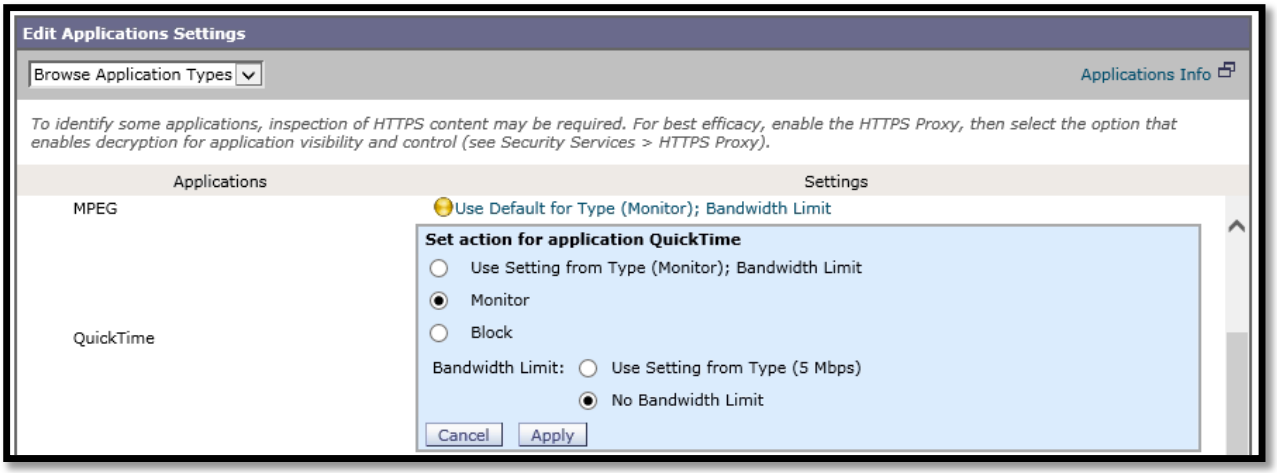


Go under “Web Security Manager” -> “Overall Bandwidth Limit” and configure it to 50Mbps :

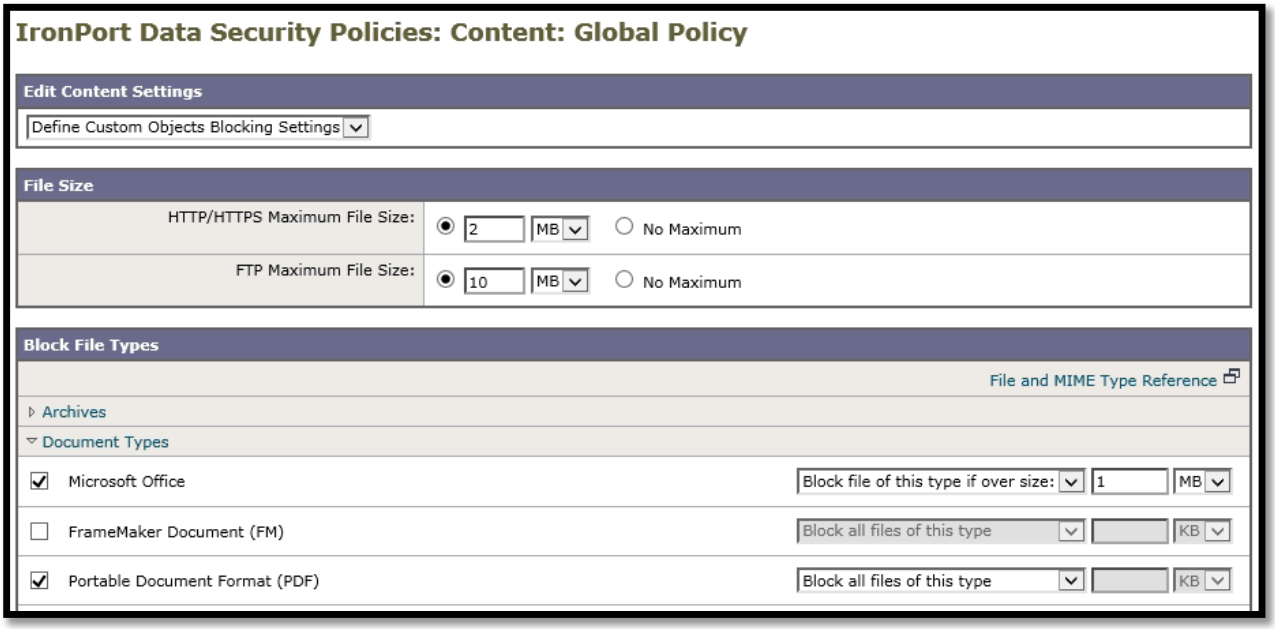


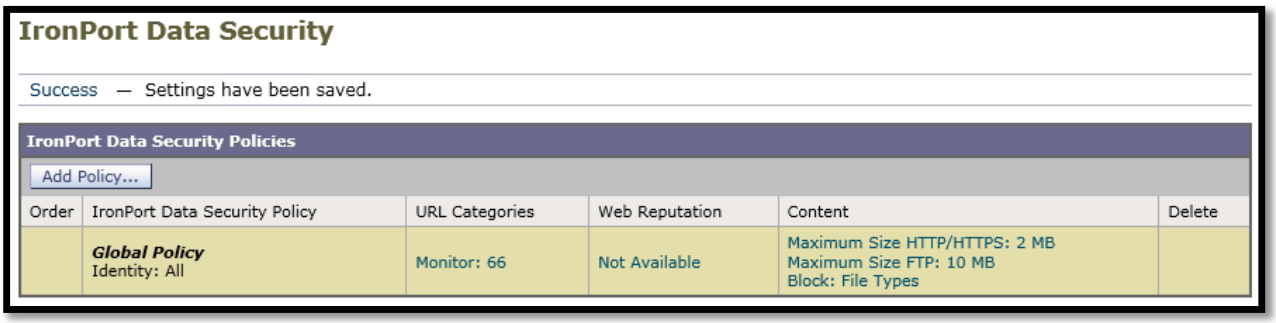
Modify AIC bandwidth settings under Global Access Policy for all Media applications except QuickTime :





Now configure IronPort Data Security. Set the limits and block PDFs :





Many different things to configure in a single task.

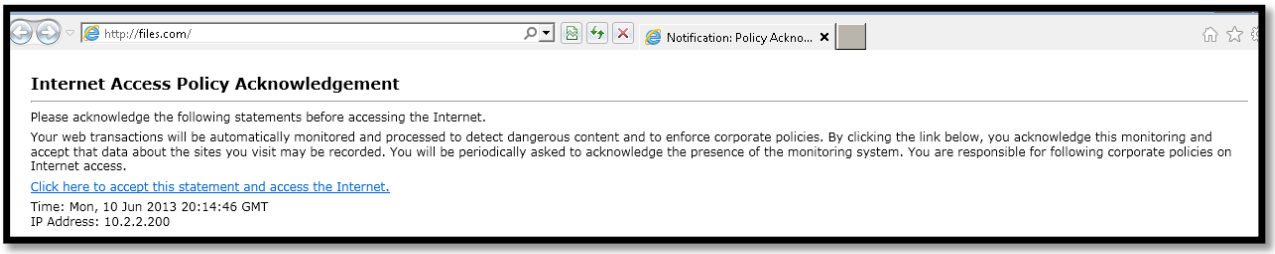
Although End User Notifications were not explicitly asked to be turned off for our Update Servers it makes perfect sense to do that. We don't want WSA to interact with transactions to those websites in any way.

IronPort Data Security Policies use URL filtering, Web Reputation, and Upload Content information when evaluating the upload request (in that order). Similarly to Access Policies (which are for download) Allow/Block is a final action versus Monitor means that next Security Component should be evaluated. You can obviously configure each of these Security Components to determine whether or not to block the upload request, or maybe just one like

in our case, which as a result blocks PDF uploads and uploads of files larger than what we have specified in the policy (for Content Policy options are File Size, File Type and File Name).

Verification

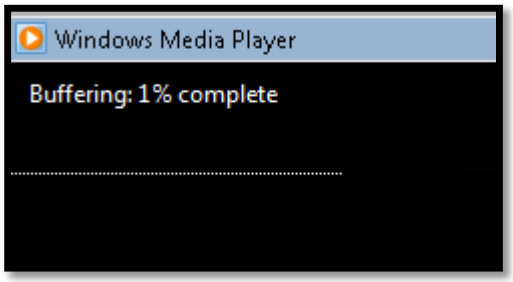
We will use Explicit Forward mode to test. Put Test PC into any VLAN (e.g. 11) and point to the WSA as a proxy in the browser :



This site requires accepting the default EUN agreement. If you now make a static entry in the windows host file to resolve www.windowsupdate.com to 10.1.1.101 you will notice that this connection (although webpage is not accessible since our server does not host it) is allowed in the logs and no End User Notification shows up :

```
1370895438.174 25338 10.2.2.200 NONE/504 1770 GET
http://www.windowsupdate.com/ - DIRECT/www.windowsupdate.com -
MONITOR_CUSTOMCAT_11-NoAuthPOL-UpdateWebsitesID-NONE-NONE-NONE-
DefaultGroup <C_Serv,-,"1","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-
,IW_swup,-,"-","-","Unknown","Unknown","-","-",0.56,0,-,"-","-"> -
```

You can now again try to access files.com and try to download the video file (.wmv). Just before you do this change Bandwidth limit to something low like 10kbps. You should observer very slow buffering on the WMV screen :



Then change the limit to 5Mbps and re-test. The difference should be easy to notice.

```
1370896131.042 292 10.2.2.200 TCP_MISS/200 76085 GET
http://www.files.com/Wildlife.wmv - DIRECT/www.files.com audio/x-ms-wma
DEFAULT_CASE_11-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_comp,-,"1","-",-,-,-,"1","-",-,-,-,"-","1",-,"-","-",-,-,IW_comp,-,"-
","-","Windows Media","Media","-","-",2084.52,1,-,"-","-"> -
```

4.0 Cisco VPN Solutions (14 points)

Task 4.1: IKEv2 Remote Access (5 Points)

- ASA3 should act as a IPSec Remote Access gateway for clients connecting from the outside
- IKEv2 should be the protocol used for tunnel negotiation
- Use the following parameters when configuring the VPN :
  - R8 should act as a CA for the ASA
  - AnyConnect clients should authenticate as “ipexpert” with password “ipexpert”
  - Only VLANs 11 and 100 should be reachable via the tunnel
  - Assign the connecting clients an IP address from the following pool : 172.30.30.10 – 172.30.30.20
  - DNS server should be 10.1.1.101 and the domain is “ipexpert.com”

Detailed Solution

R8

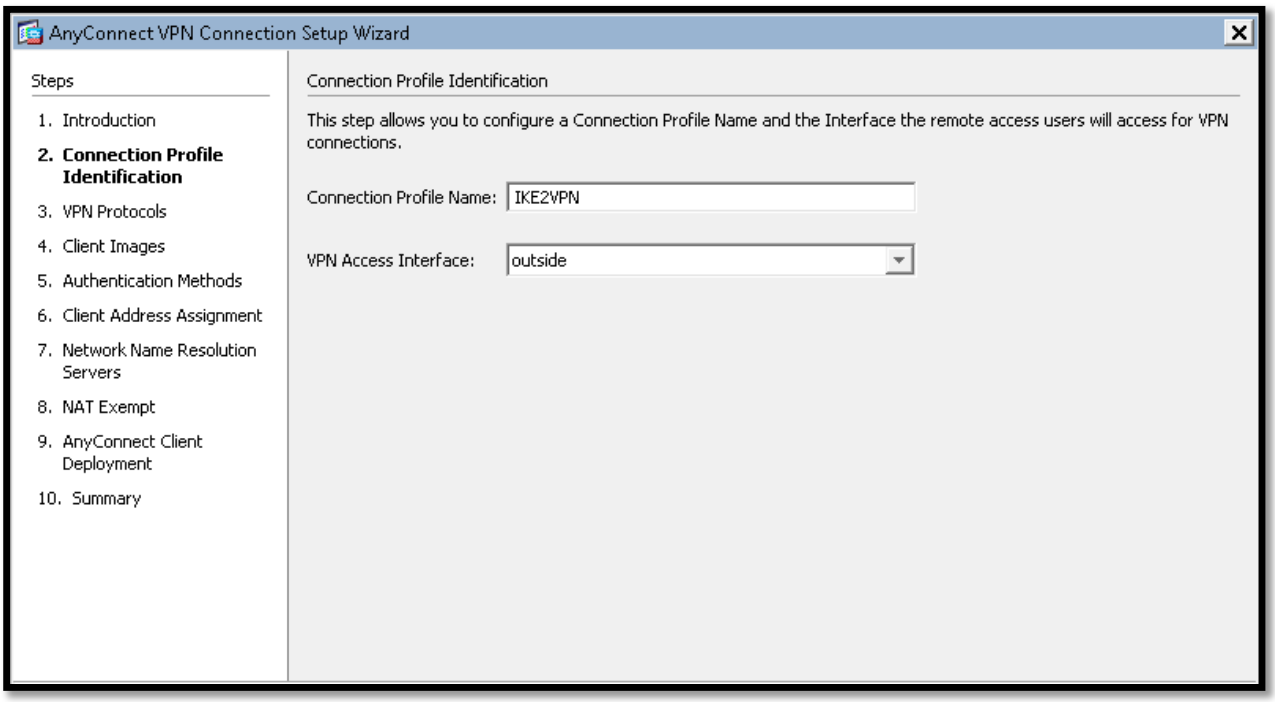
```
crypto pki server CA
 issuer-name cn=R8CA
 grant auto
 no shut

ip http server
```

ASA3

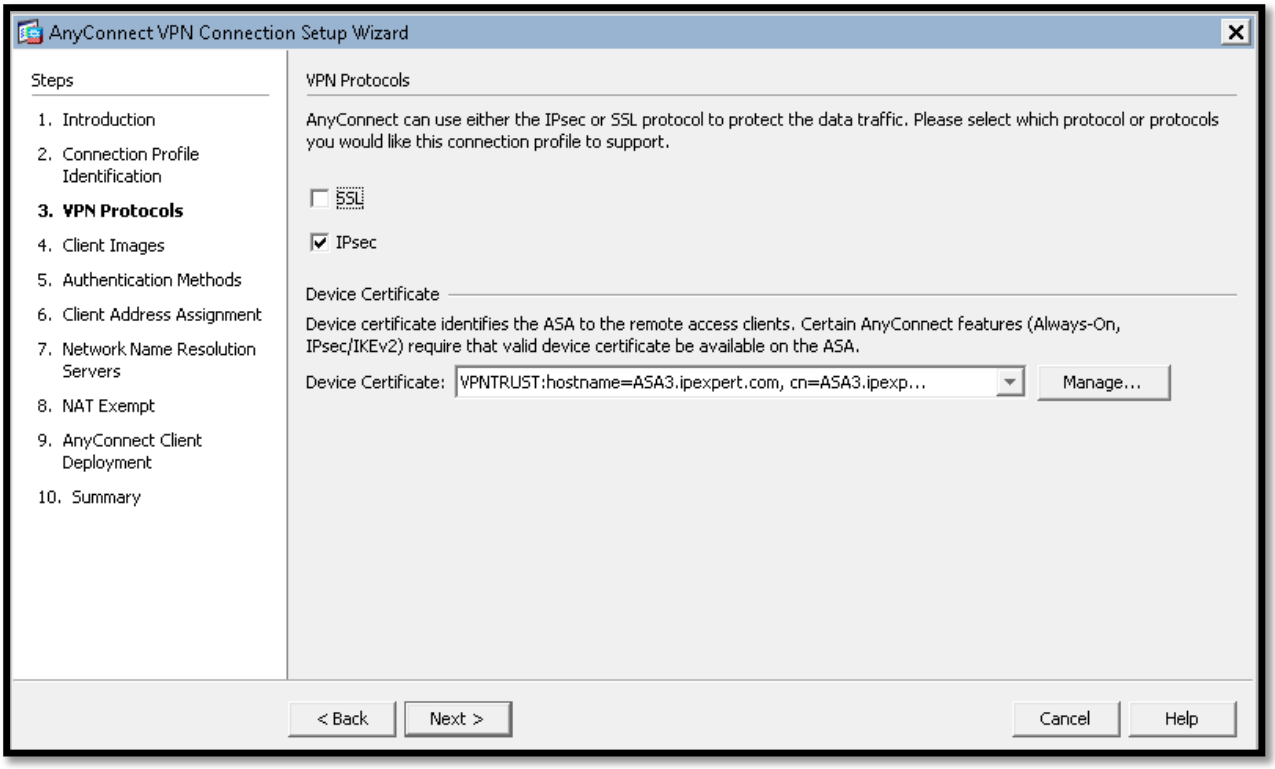
```
domain-name ipexpert.com

crypto ca trustpoint VPNTRUST
 enrollment url http://192.168.5.8:80
 fqdn ASA3.ipexpert.com
 subject-name cn=ASA3.ipexpert.com
 crl configure

crypto ca authen VPNTRUST
```

```
crypto ca enroll VPNTRUST
```

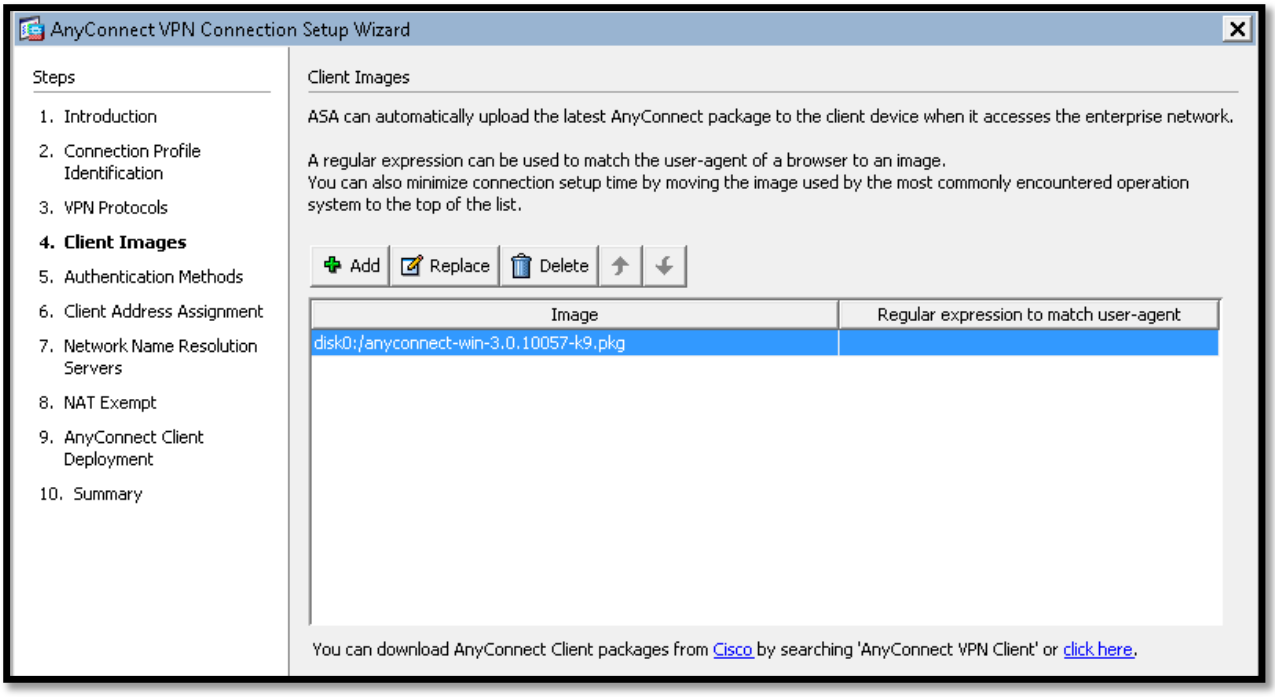
Now connect to the ASA using ASDM and run a VPN Wizard :



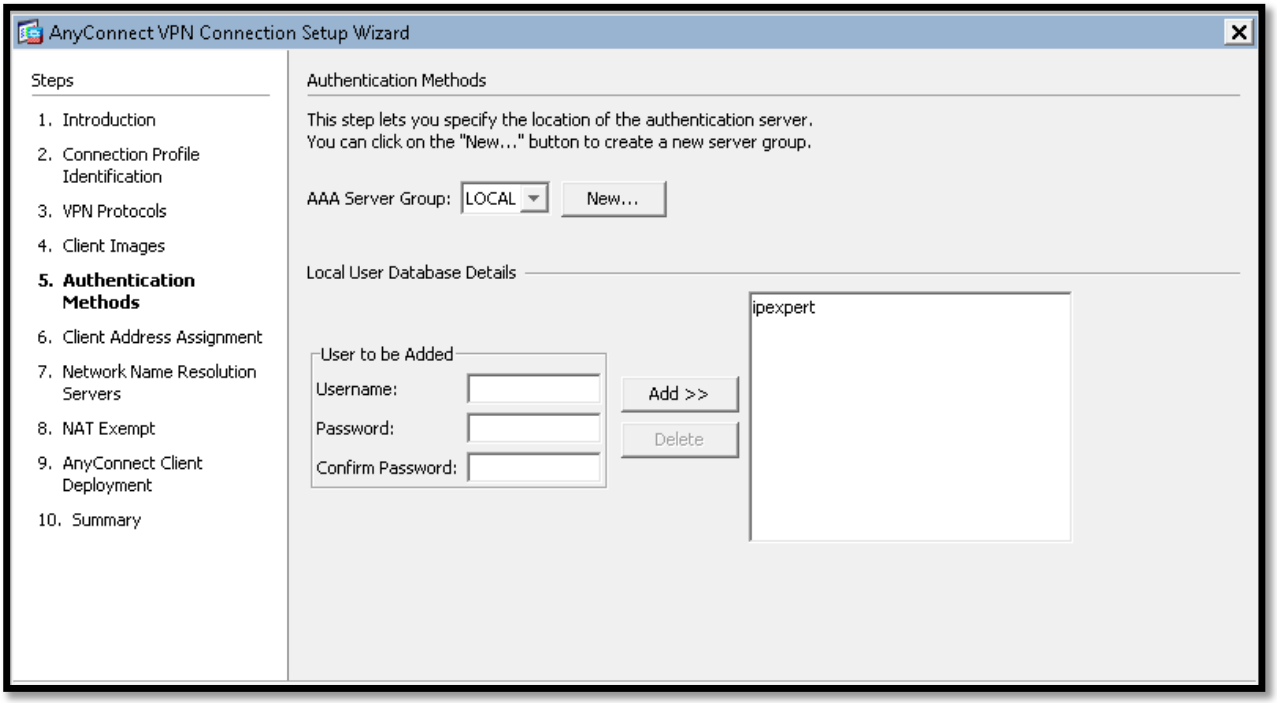
Select the trustpoint you have configured from the CLI :



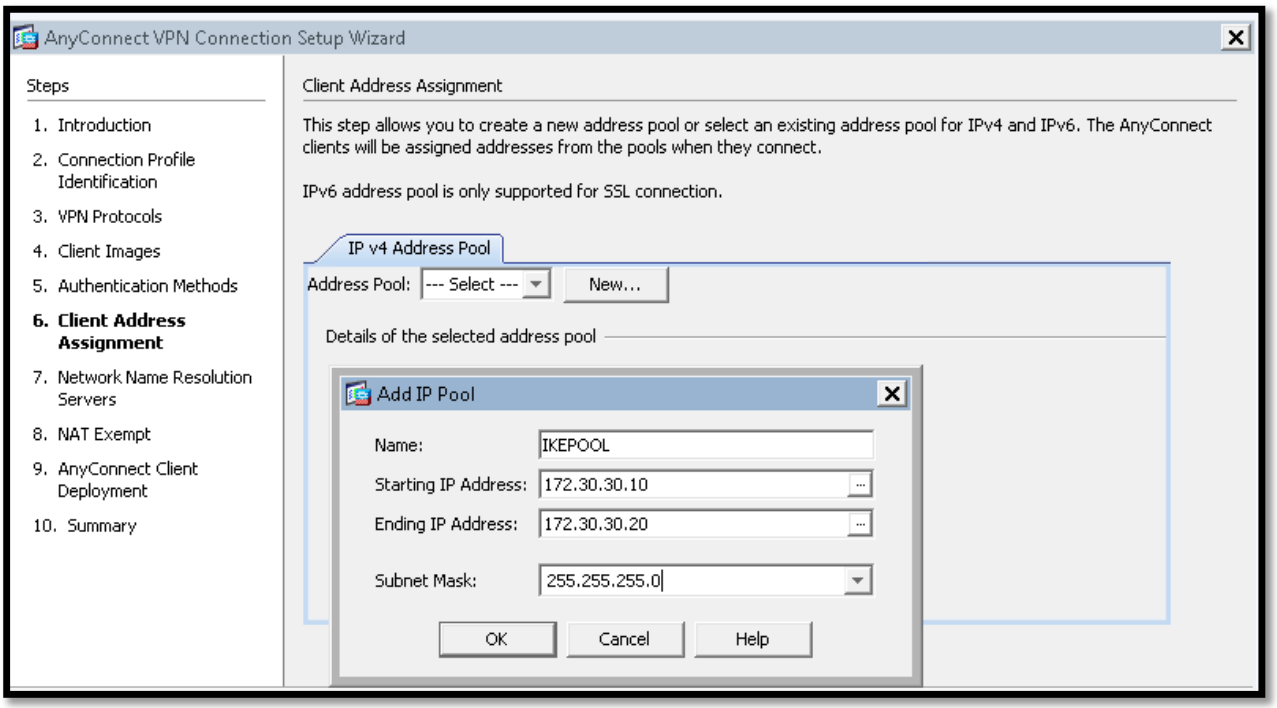
Choose AnyConnect 3.0 :



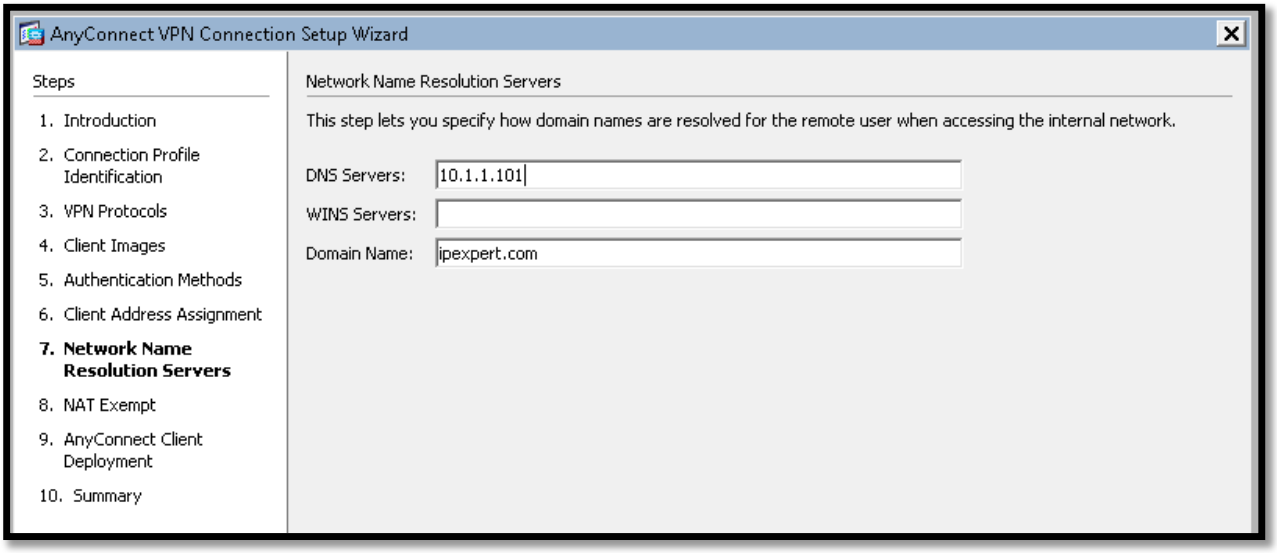
User should be already there from the ASDM task :



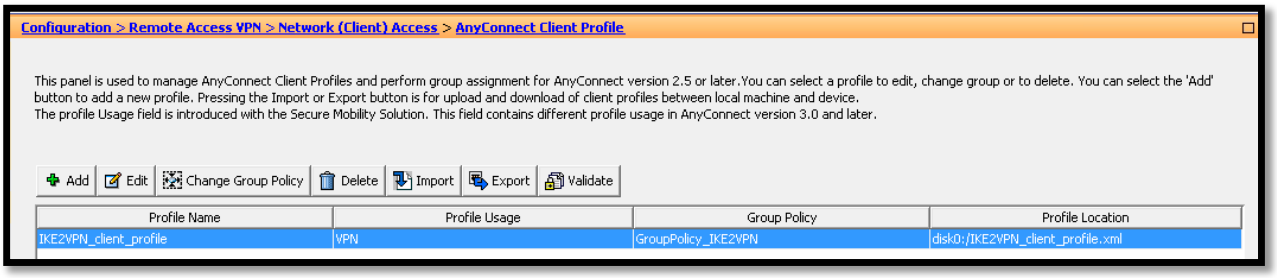
Add a new IP Pool (don't forget to select it after you create it).

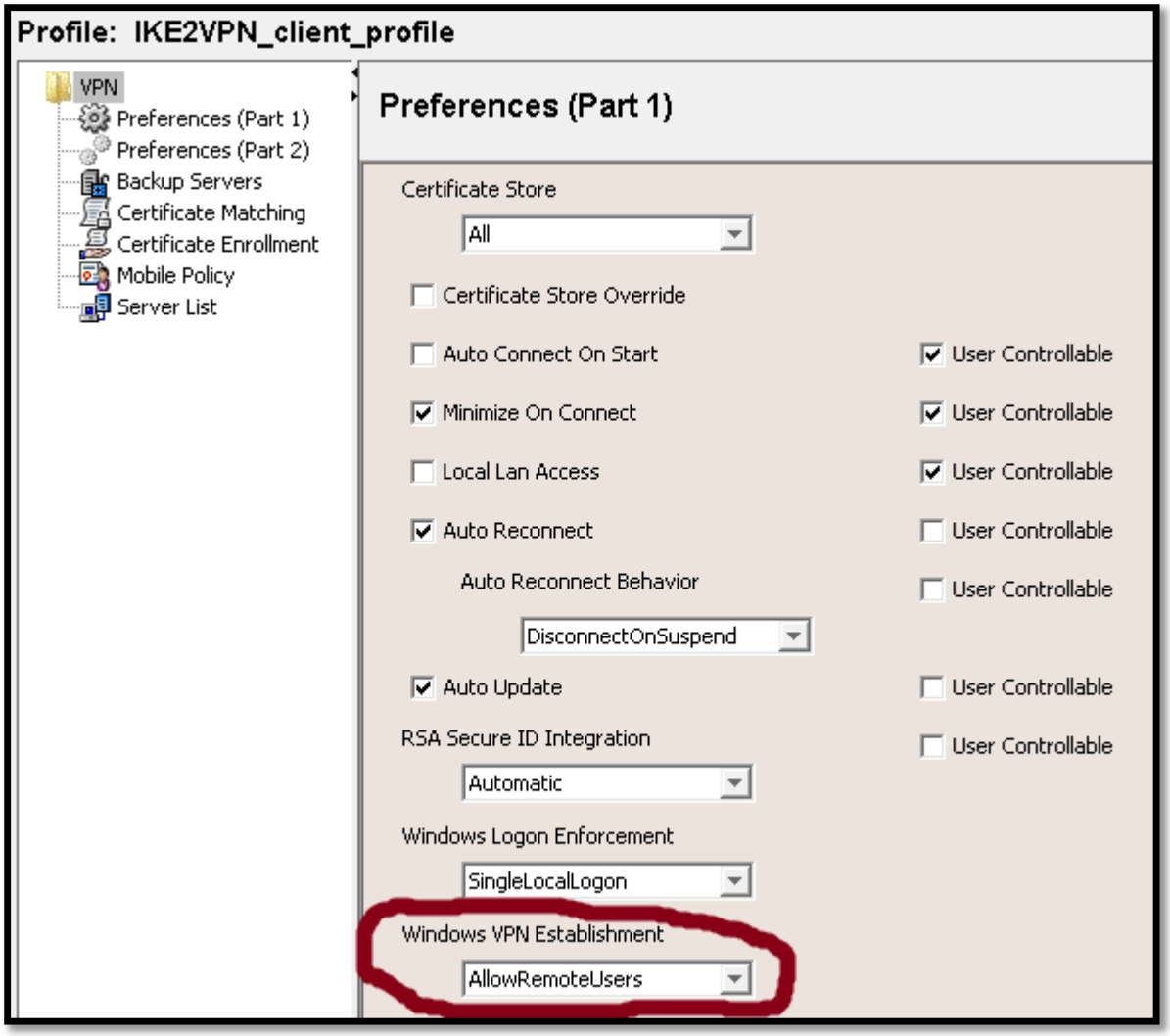


Then the DNS and domain :



Finally you may want to modify the Profile setting so it allows connections via RDP sessions :





Now go back to the Profile page and click on "Export". This file should be then downloaded/copied to the Test PC you will be using to verify this configuration under "**%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**". Also make sure name of the file is the same as what's on the ASA or otherwise the client will try to connect to the ASA via HTTP/HTTPs to validate the Profile.

Remaining part of the configuration is to make sure NAT won't break communication and that only the requested VLANs can be accessed through the VPN tunnel :

```
object-group network NONAT
 network-object object NET-10.1.1.0_24
 network-object object NET-10.2.2.0_24
```

```
object network IKEPOOL
 range 172.30.30.10 172.30.30.20

nat (any,outside) source stat NONAT NONAT dest static IKEPOOL IKEPOOL

access-list SPLIT standard permit 10.1.1.0 255.255.255.0
access-list SPLIT standard permit 10.2.2.0 255.255.255.0

group-policy GroupPolicy_IKE2VPN attributes
 split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT
```

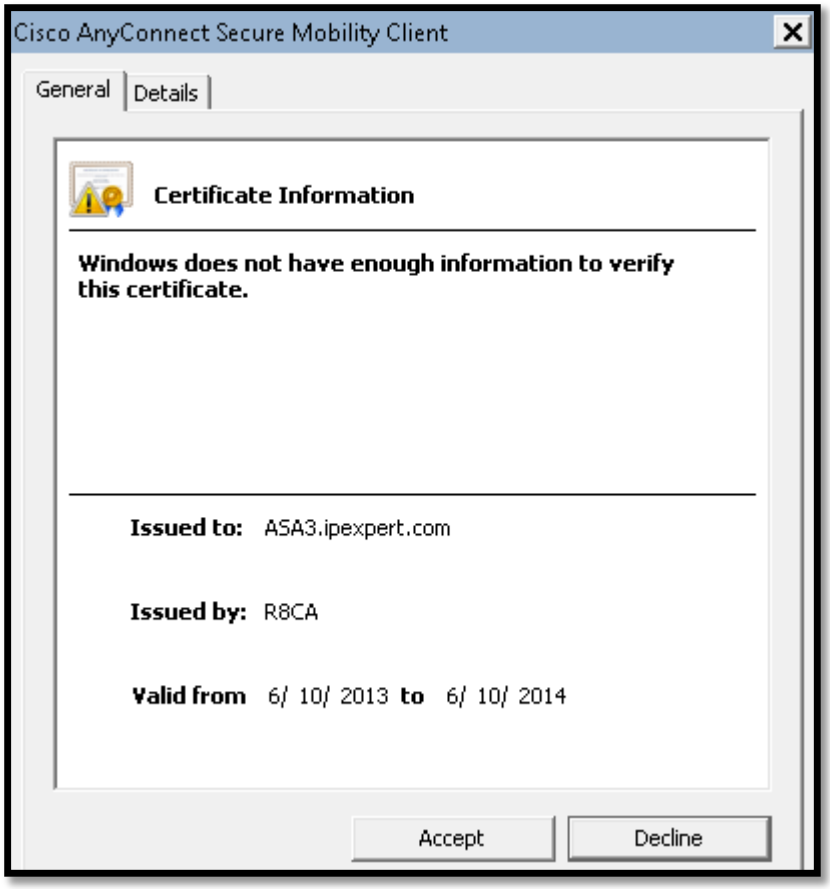
FQDN of the ASA's certificate should match its FQDN. This is useful when the client is to be initially downloaded via HTTPs from the ASA or for SSL (URL validation).

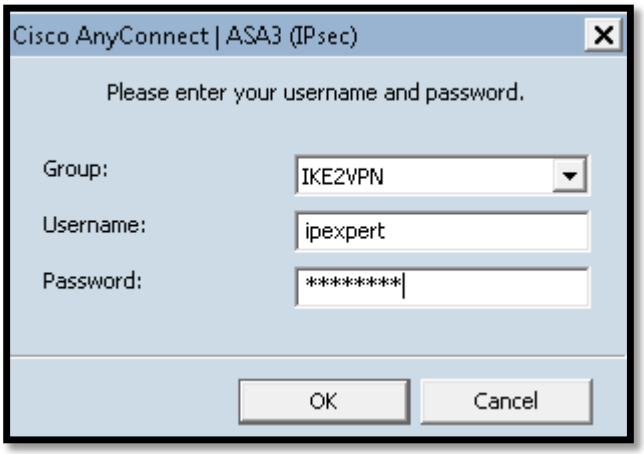
You can find a location for the AnyConnect Profile using AnyConnect Administrator Guide -> Deploying the AnyConnect Secure Mobility Client -> Locations to Deploy the AnyConnect Profiles.

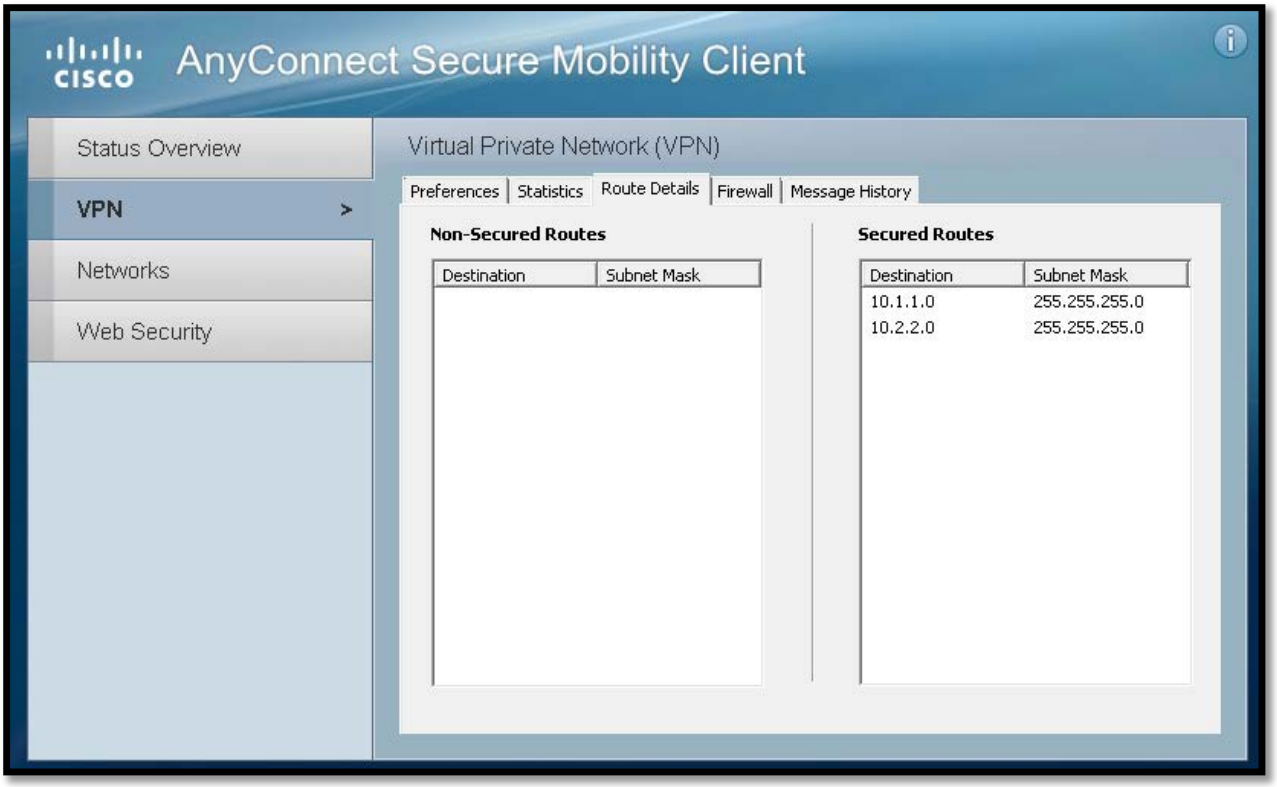
Verification

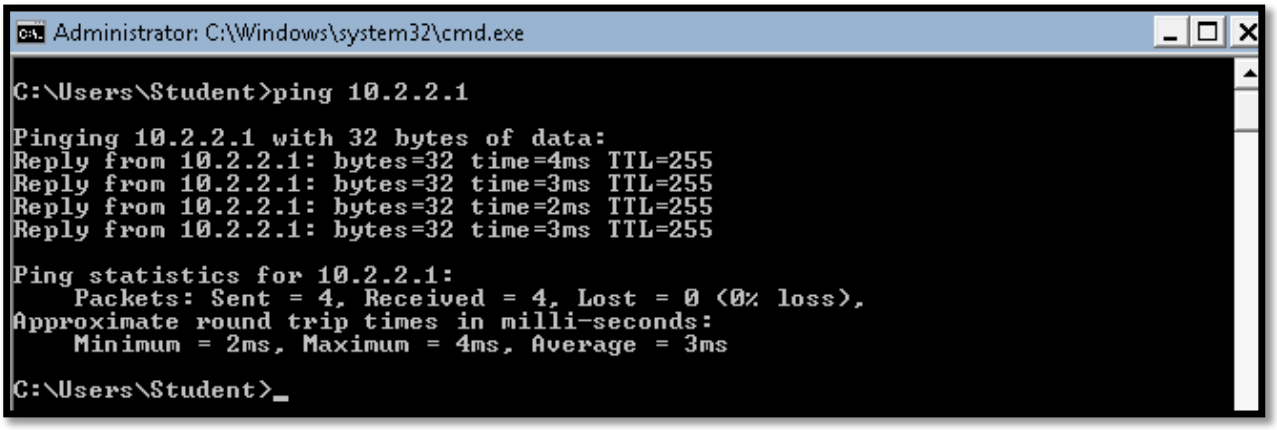
Use AnyConnect client to connect to the ASA. You should see an entry populated from the downloaded profile – if not right-click on the tray icon and select "Network Repair".

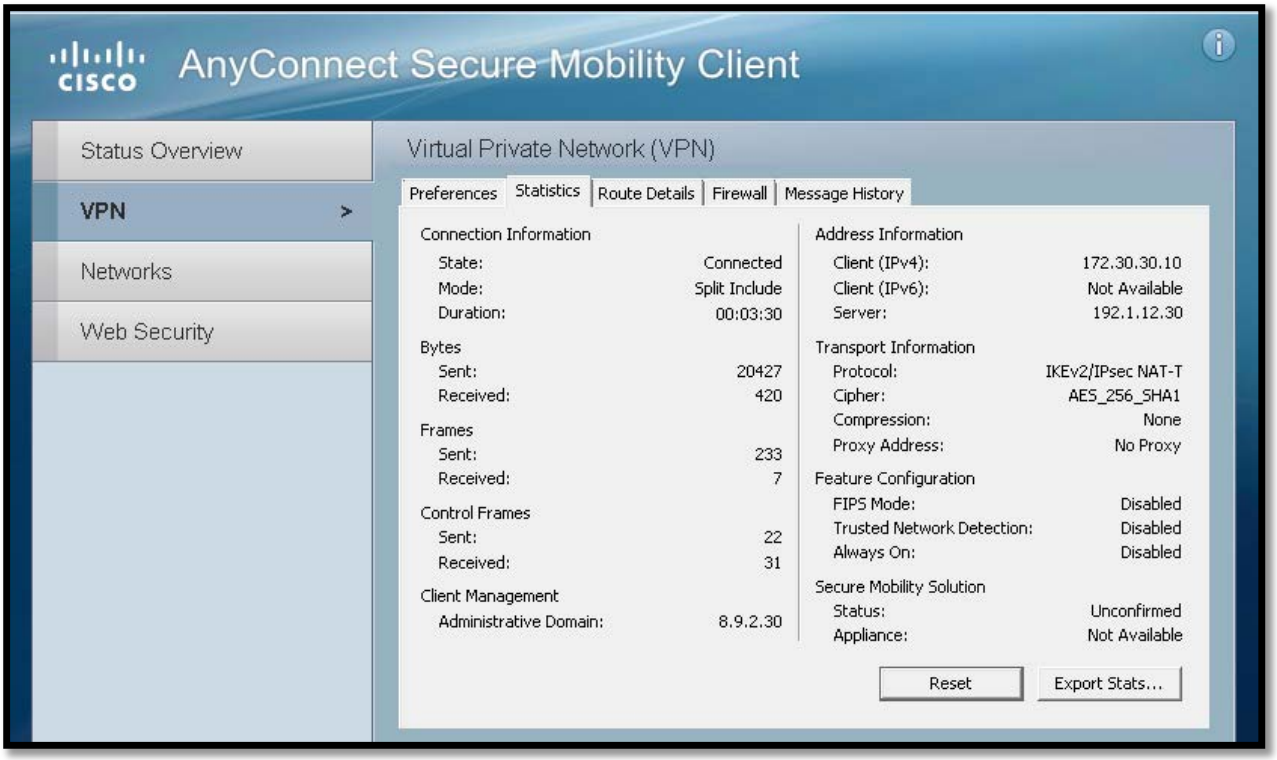
Accept the certificate and authenticate :

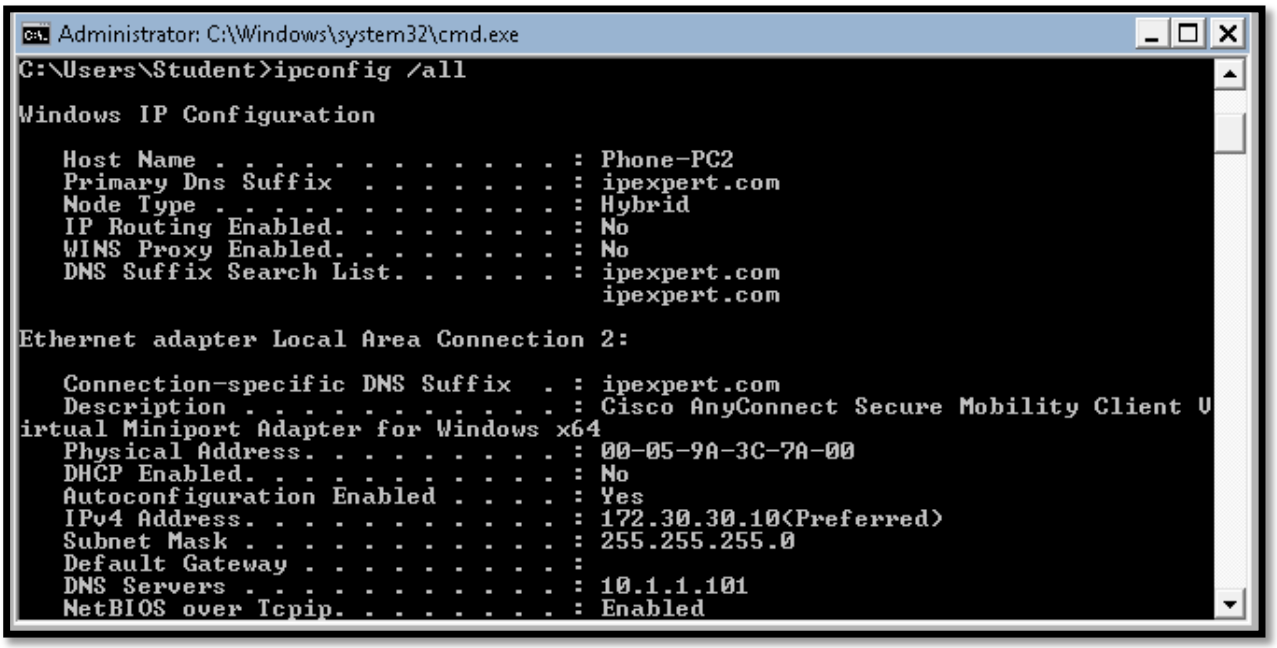













```
ASA3/act(config)# sh vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed

Username     : ipexpert               Index        : 39
Assigned IP  : 172.30.30.10           Public IP    : 192.1.12.200
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES256                 Hashing      : none SHA1
Bytes Tx     : 420                    Bytes Rx     : 74639
Pkts Tx      : 7                      Pkts Rx      : 855
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKE2VPN    Tunnel Group : IKE2VPN
Login Time   : 01:37:38 UTC Tue Jun 11 2013
Duration     : 0h:08m:47s
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    : 39.1
  Public IP    : 192.1.12.200
  Encryption   : none                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 21 Minutes
  Client Type  : AnyConnect
  Client Ver   : 3.0.10057

IKEv2:
  Tunnel ID    : 39.2
  UDP Src Port : 61634                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES256                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 85871 Seconds
  PRF          : SHA1                   D/H Group    : 5
  Filter Name  :
  Client OS    : Windows
```

```
IPsecOverNatT:
  Tunnel ID    : 39.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 172.30.30.10/255.255.255.255/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28271 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607928 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 30 Minutes
  Bytes Tx     : 420                   Bytes Rx     : 74639
  Pkts Tx      : 7                     Pkts Rx      : 855

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 530 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

Task 4.2: L2L (4 Points)

- Encrypt traffic between R4 & R8 using the following parameters :
  - Authentication is PSK
  - Use default policy for the ISAKMP parameters
  - Use ESP-AES192 for encryption and ESP-SHA-HMAC for Data Authentication
  - Use the tunnel network 10.4.8.0/24
- The VPN should not use GRE or crypto maps
- VLAN 100 should be able to reach VLAN 49 over the tunnel
- You can use one static routes on R4 and one on R8 to accomplish this
- Make sure R1 does not learn the default route from R8

Detailed Solution

R8

```
cry isa key ipexpert add 192.1.24.4
```

```
crypto ipsec transform-set SET1 esp-aes 192 esp-sha-hmac

crypto ipsec profile IPSEC_PROF
 set transform-set SET1

interface Tunnel48
 ip address 10.4.8.8 255.255.255.0
 tunnel source F0/1
 tunnel destination 192.1.24.4
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF

ip route 192.1.49.0 255.255.255.0 10.4.8.4

access-list 49 permit 192.1.49.0 0.0.0.255

route-map R49 permit 10
 match ip address 49

router rip
 redistribute static route-map R49
```

R4

```
cry isa key ipexpert add 192.1.12.8

crypto ipsec transform-set SET1 esp-aes 192 esp-sha-hmac

crypto ipsec profile IPSEC_PROF
 set transform-set SET1

interface Tunnel48
 ip address 10.4.8.4 255.255.255.0
 tunnel source s0/0/0
 tunnel destination 192.1.12.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF

ip route 10.1.1.0 255.255.255.0 10.4.8.8
```

ASA3

```
object network R8
 host 192.168.5.8
 nat (DMZ,outside) static 192.1.12.8

access-list OUTSIDE_IN permit udp host 192.1.24.4 host 192.168.5.8 eq
isakmp
access-list OUTSIDE_IN permit udp host 192.1.24.4 host 192.168.5.8 eq 4500
```

We have a few limitations in this question, the first is to create an IPSec tunnel without using GRE or crypto maps. This seems a good fit for a Static Virtual Tunnel Interface in IPSec mode. It's very similar to how you would create a GRE tunnel, but the main difference is we place the tunnel into IPSec v4 mode. We can then use tunnel protection with an IPSec Profile to encrypt the tunnel.

Only being able to use two static routes is our next problem. So we use these on R4 and R8 pointing towards the tunnel network. We then need to redistribute the R8 static for 192.1.49.0/24 into RIP, so R1 knows about this network. Here note in order to avoid also redistributing a default route we need to add a route-map to the "redistribute" line, only allowing the network for VLAN 49.

Verification

```
R8#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.5.8     192.1.24.4      QM_IDLE           1001 ACTIVE

R4#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.

1001  192.1.24.4      192.1.12.8              ACTIVE aes  sha  psk  5
23:56:09 N
       Engine-id:Conn-id =  SW:1

IPv6 Crypto ISAKMP SA


R8#ping 192.1.49.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.49.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 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: Tunnel48
Uptime: 00:01:36
Session status: UP-ACTIVE
Peer: 192.1.24.4 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.1.24.4
      Desc: (none)
  IKEv1 SA: local 192.168.5.8/4500 remote 192.1.24.4/4500 Active
          Capabilities:N connid:1001 lifetime:23:57:52
  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 15 drop 0 life (KB/Sec) 4578452/3503
        Outbound: #pkts enc'ed 19 drop 0 life (KB/Sec) 4578454/3503

R4#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 = 4/7/8 ms

R4#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: Tunnel48
Uptime: 00:02:35
Session status: UP-ACTIVE
Peer: 192.1.12.8 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 192.168.5.8
      Desc: (none)
  IKEv1 SA: local 192.1.24.4/4500 remote 192.1.12.8/4500 Active
          Capabilities:N connid:1001 lifetime:23:56:53
  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 21 drop 0 life (KB/Sec) 4515473/3444
        Outbound: #pkts enc'ed 15 drop 0 life (KB/Sec) 4515478/3444

R1#sh ip rip data
1.0.0.0/8    auto-summary
1.0.0.0/8    directly connected, Loopback0
8.0.0.0/8    auto-summary
8.0.0.0/8
    [1] via 10.2.2.8, 00:00:19, FastEthernet0/1.111
10.0.0.0/8    auto-summary
10.1.1.0/24    directly connected, FastEthernet0/1.100
10.2.2.0/24    directly connected, FastEthernet0/1.111
10.4.8.0/24
    [1] via 10.2.2.8, 00:00:19, FastEthernet0/1.111
192.1.49.0/24    auto-summary
192.1.49.0/24
    [1] via 10.2.2.8, 00:00:19, FastEthernet0/1.111
```

Task 4.3: GETVPN (5 Points)

- Configure GET VPN between R5 & R6 with R2 as the Key Server
- Use the following parameters :
  - Authentication is pre-shared key
  - Use AES, SHA, DH5 for Phase 1
  - Use ESP-AES256 for encryption and ESP-SHA-HMAC for data authentication
  - Rekeying should use multicast transport type
  - Rekey should occur every 10 minutes using AES 192
  - Encrypt ICMP traffic between R9 Loopback 0 and CAT4

Detailed Solution

R5

```
router ospf 1
 network 10.5.5.5 0.0.0.0 ar 0

crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5

crypto isakmp key ipexpert address 2.2.2.2

crypto gdoi group GET
 identity number 1
 server address ipv4 2.2.2.2

crypto map MAP1 10 gdoi
 set group GET

int s0/1/0
 crypto map MAP1

ip access-list extended OUTSIDE_IN
 no deny ip any any log
 permit udp host 2.2.2.2 eq 848 host 239.0.1.2 eq 848
 permit esp host 192.1.6.140 host 9.9.9.9
```

```
 permit pim host 192.1.25.2 host 224.0.0.13
 permit pim host 192.1.25.2 host 192.1.25.5
 permit igmp host 192.1.25.2 host 224.0.0.1
 deny   ip any any log
```

R6

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5

crypto isakmp key ipexpert address 2.2.2.2

crypto gdoi group GET
 identity number 1
 server address ipv4 2.2.2.2

crypto map MAP1 10 gdoi
 set group GET

int s0/1/0
 crypto map MAP1
```

R2

```
cry key gen rsa lab GETKEY mod 1024

ip access-list extended GETACL
 permit icmp host 9.9.9.9 host 192.1.6.140
 permit icmp host 192.1.6.140 host 9.9.9.9

ip access-list extended REKEY
 permit udp host 2.2.2.2 eq 848 host 239.0.1.2 eq 848

crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
```

```
crypto isakmp key ipexpert address 192.1.25.5
crypto isakmp key ipexpert address 192.1.26.6

crypto ipsec transform-set GETSET esp-aes 256 esp-sha-hmac

crypto ipsec profile GET_PROFILE
 set transform-set GETSET

crypto gdoi group GET
 identity number 1
 server local
  rekey algorithm aes 192
  rekey address ipv4 REKEY
  rekey lifetime seconds 600
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa GETKEY
  sa ipsec 1
   profile GET_PROFILE
   match address ipv4 GETACL
   replay counter window-size 64
```

Just a little bit of troubleshooting in the beginning – note that R6 does not know about R9's loopback so OSPF should be fixed between R5 and R9.

If your network does not support multicast traffic, your only option will obviously be unicast rekeys. If you have a mix of unicast and multicast clients, in your GETVPN environment, then you will need to use multicast rekeying, since mixed mode is not yet supported. The rekeying is used to provide periodic updates for the vpn policies, preventing the need for each GM to re-register.

The main difference between Unicast and Multicast Rekeying configuration is the addition of an ACL, to define the multicast group address. This includes the source of the key server and the Multicast destination running over GDOI UDP 848 - the multicast group was not given so you can configure any multicast address you want.

The other ACL is our proxy ACL to define interesting traffic to be encrypted. We also adjust the rekey encryption algorithm to AES 192, as well as the rekey timers.

The group member configurations are fairly simple, since the phase 2 policy and proxy ACLs are defined in the policy provided by the key server.

As R5 has CBAC configured facing the Frame cloud, we need to allow the VPN and PIM traffic into through the CBAC ACL on S0/1/0.

Verification

```
R2#sh cry gdoi ks members

Group Member Information :

Number of rekeys sent for group GET : 0

Group Member ID    : 192.1.25.5
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 192.1.26.6
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

R2#sh cry gdoi ks policy
Key Server Policy:
For group GET (handle: 2147483650) server UNKNOWN (handle: 2147483650):

  # of teks : 1  Seq num : 0
  KEK POLICY (transport type : Multicast)
    spi : 0x9BE24300B9875604479A5E701C5E3FBD
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 24
    orig life(sec): 600         remaining life(sec): 481
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : GETKEY

  TEK POLICY (encaps : ENCAPS_TUNNEL)
```

```
    spi                : 0x42F784E6
    access-list        : GETACL
    transform          : esp-256-aes esp-sha-hmac
    alg key size       : 32            sig key size          : 20
    orig life(sec)     : 3600          remaining life(sec)   : 3594
    tek life(sec)      : 3600          elapsed time(sec)     : 6
    override life (sec): 0             antireplay window size: 64


R5#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.

1004  239.0.1.2       2.2.2.2                  ACTIVE aes  sha  rsig 0  0
       Engine-id:Conn-id =  SW:4

1003  192.1.25.5      2.2.2.2                  ACTIVE aes  sha  psk  5
23:58:41
       Engine-id:Conn-id =  SW:3

IPv6 Crypto ISAKMP SA


R6#sh cry gd gm acl
Group Name: GET
 ACL Downloaded From KS 2.2.2.2:
   access-list  permit icmp host 9.9.9.9 host 192.1.6.140
   access-list  permit icmp host 192.1.6.140 host 9.9.9.9
 ACL Configured Locally:


CAT4#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 = 33/62/159 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: 00:00:44
Session status: UP-ACTIVE
Peer: 0.0.0.0 port 848 fvrf: (none) ivrf: (none)
      Phase1_id: 2.2.2.2
      Desc: (none)
  IKEv1 SA: local 192.1.25.5/848 remote 2.2.2.2/848 Active
          Capabilities:(none) connid:1005 lifetime:23:59:15
  IKEv1 SA: local 192.1.25.5/848 remote 2.2.2.2/848 Inactive
          Capabilities:(none) connid:1003 lifetime:0
  IKEv1 SA: local 239.0.1.2/848 remote 2.2.2.2/848 Active
          Capabilities:(none) connid:1006 lifetime:6w4d
  IPSEC FLOW: permit 1 host 192.1.6.140 host 9.9.9.9
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/3246
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/3246
  IPSEC FLOW: permit 1 host 9.9.9.9 host 192.1.6.140
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/3246
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/3246



R6#
*Jun 11 16:38:28.313: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GET
from 2.2.2.2 to 239.0.1.2 with seq # 3

R6#sh cry gd gm reke
```

```
   Group GET (Multicast)
       Number of Rekeys received (cumulative)       : 1
       Number of Rekeys received after registration : 1
```

5.0 Identity Management (12 points)

Task 5.1: IPv6 Initialization (2 Points)

- Configure G0/1 on ISE for IPv6
- ISE should learn the IPv6 prefix from R1
- Use 2100::/64

Detailed Solution

R1

```
interface FastEthernet0/1.100
 ipv6 address 2100::1/64
```

ISE

```
int gigabitEthernet 1
 ipv6 address autoconfig
```

As of the current code version ISE does not support IPv6 configuration – only the interfaces can be configured for IPv6.

Verification

Start verification of MAB for the IP Phone :

```
R1#sh ipv int f0/1.100 prefix
IPv6 Prefix Advertisements FastEthernet0/1.100
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar

PD default [LA] Valid lifetime 2592000, preferred lifetime 604800
```

```
AD 2100::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800

pod124ise/admin# sh int gigabitEthernet 1
GigabitEthernet 1
          Link encap:Ethernet  HWaddr 00:0C:29:A7:FD:B1
          inet addr:10.1.1.150  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: 2100::20c:29ff:fea7:fdb1/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fea7:fdb1/64 Scope:Link
          inet6 addr: 2100::944b:f82d:46bc:1ebe/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:251325 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50836 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22664249 (21.6 MiB)  TX bytes:4359356 (4.1 MiB)

R1#ping 2100::20c:29ff:fea7:fdb1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2100::20C:29FF:FEA7:FDB1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/12 ms
```

Task 5.2: Proxy Authentication (5 Points)

- The AAA server is located at 10.1.1.150. It communicates to the ASA using RADIUS and a key of "ipexpert"
- All outbound Telnet and HTTP Requests have to authenticate against the AAA server, same as a custom application that uses TCP port 4515
- Allow R2 to telnet into R1 F0/1.111 only after successful authentication - use virtual telnet with an IP address of 192.1.12.99
- The username to use is "cutproxy" with a password of "ipexpert". Use the same username and password for all authentication attempts and don't download an ACL for outbound access

Detailed Solution

ASA3

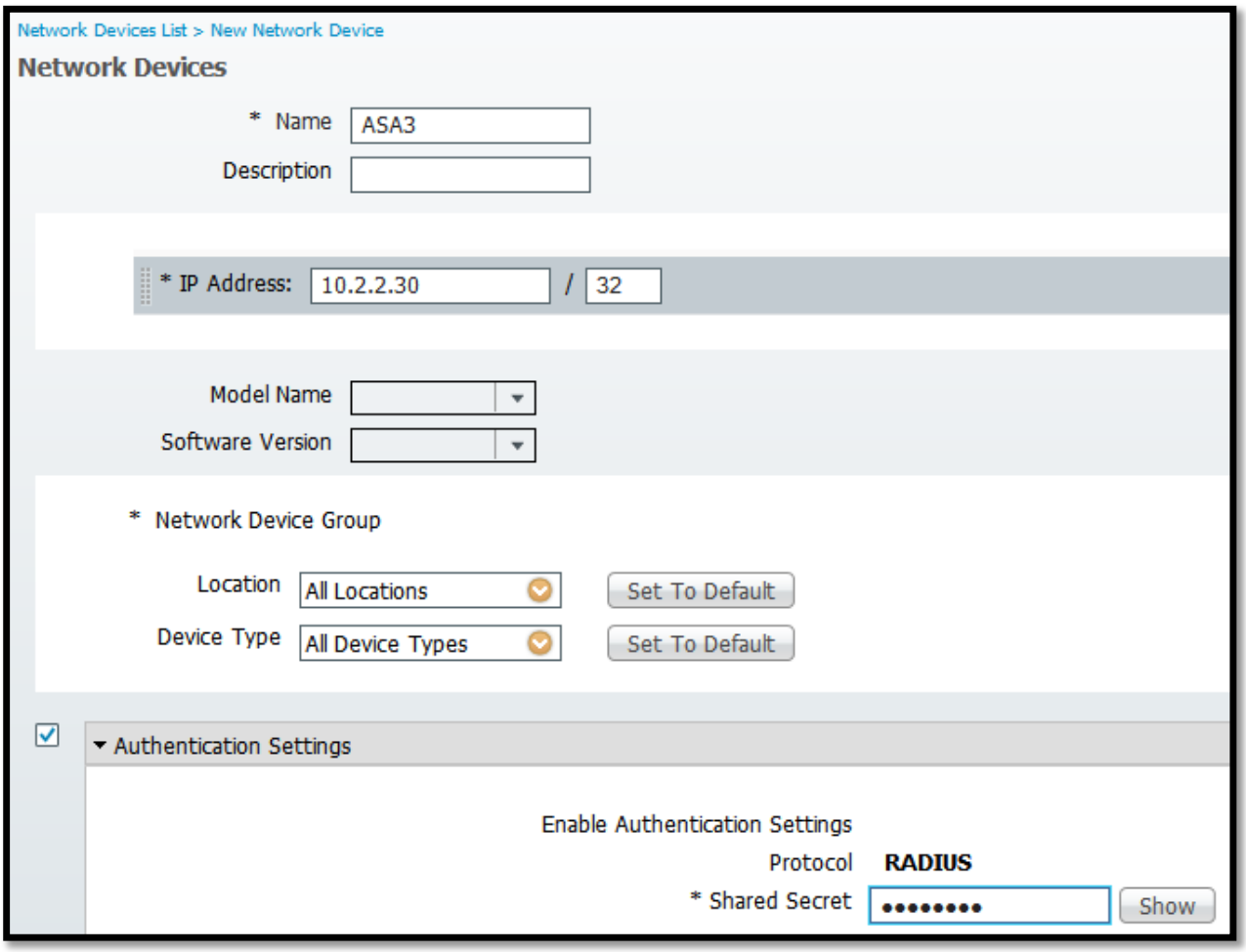
```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.1.1.150
 key ipexpert

access-list OUTSIDE_IN permit tcp host 192.1.12.2 host 192.1.12.99 eq
telnet
access-group OUTSIDE_IN in interface outside per-user-override

access-list CUTPIN permit tcp host 192.1.12.2 host 192.1.12.99 eq telnet
access-list CUTPIN permit tcp host 192.1.12.2 host 192.1.12.1 eq telnet

access-list CUTPOUT permit tcp any any eq www
access-list CUTPOUT permit tcp any any eq telnet
access-list CUTPOUT permit tcp any any eq 4515

aaa authentication match CUTPIN outside ISE
aaa authentication match CUTPOUT inside ISE

virtual telnet 192.1.12.99
```

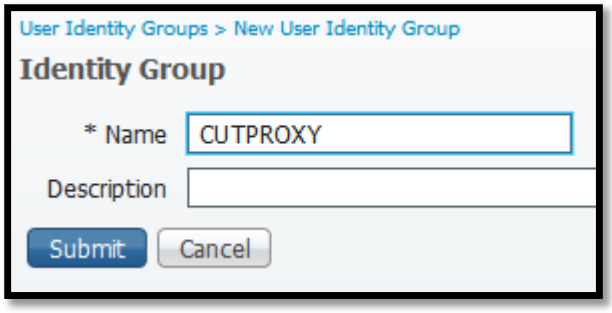
```
object network VIP
 host 192.1.12.99
 nat (i,o) static 192.1.12.99
```

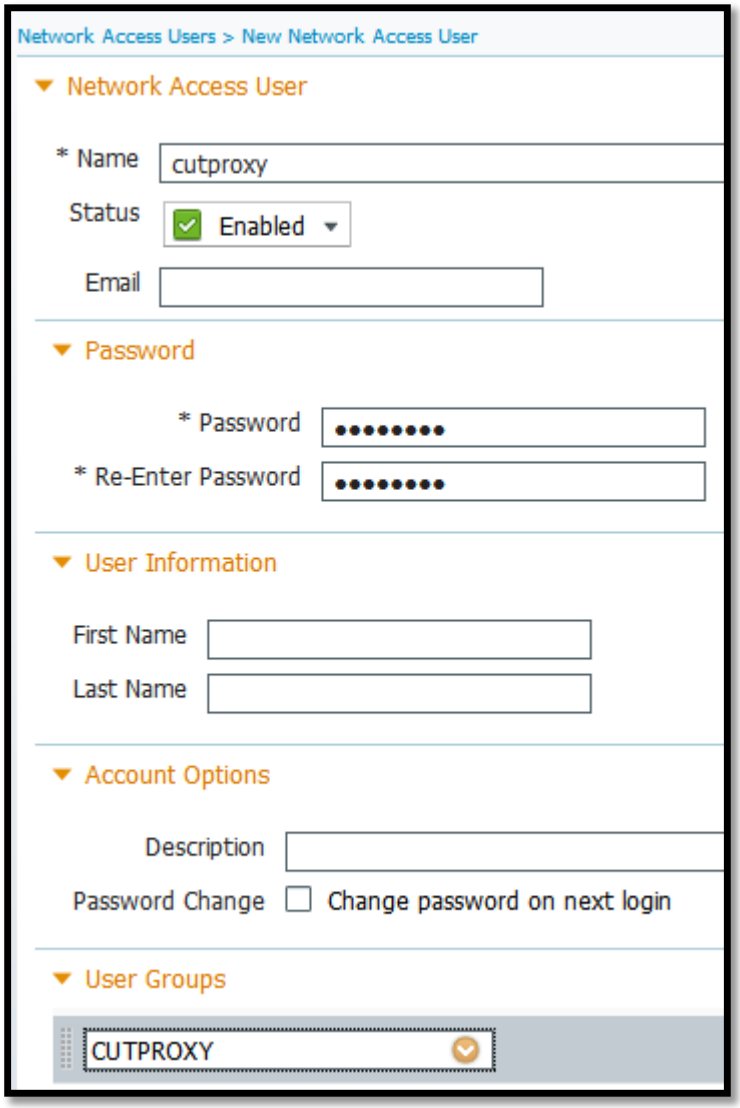
ISE

```
ip route  10.2.2.0 255.255.255.0 gateway 10.1.1.1
```

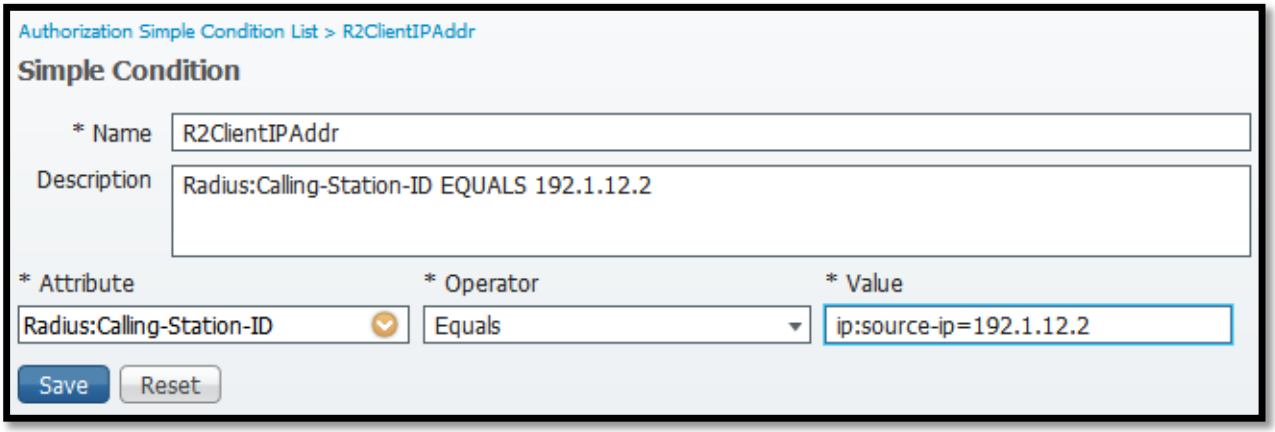
Add ASA3 as a AAA Client, configure a group and user :

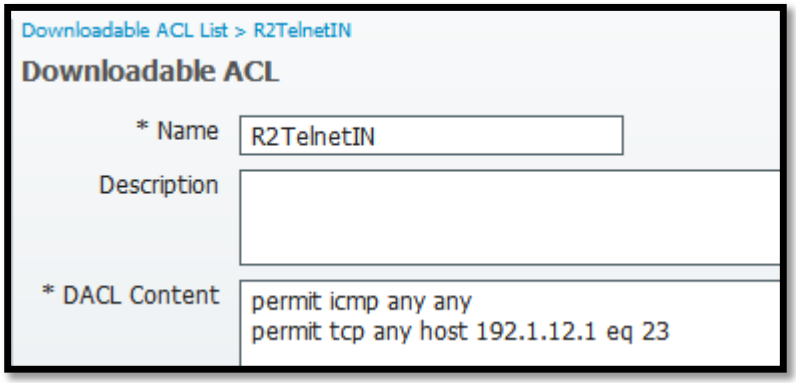


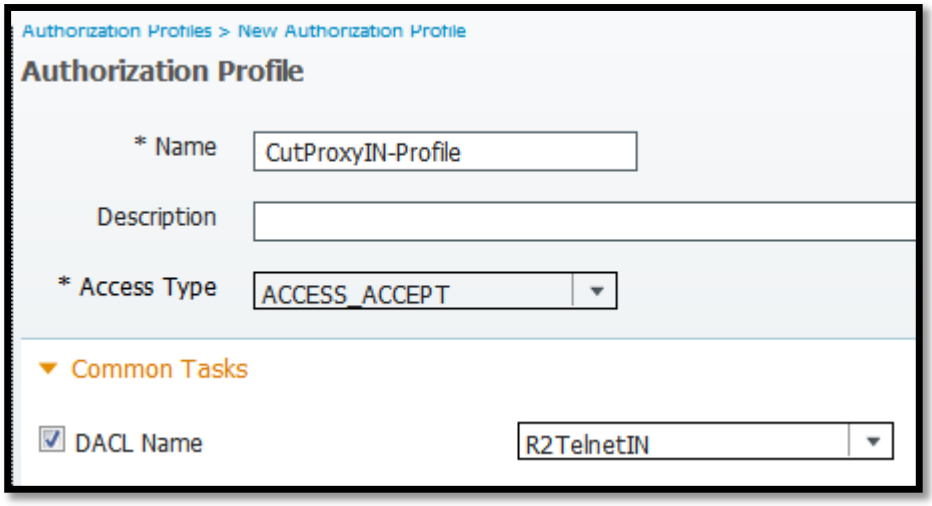


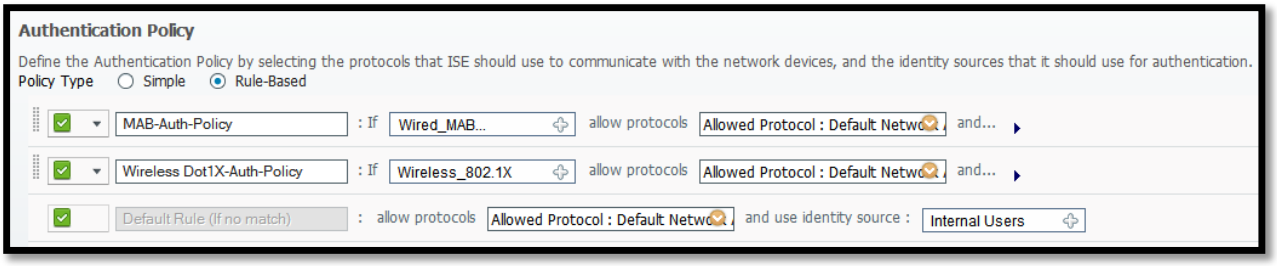


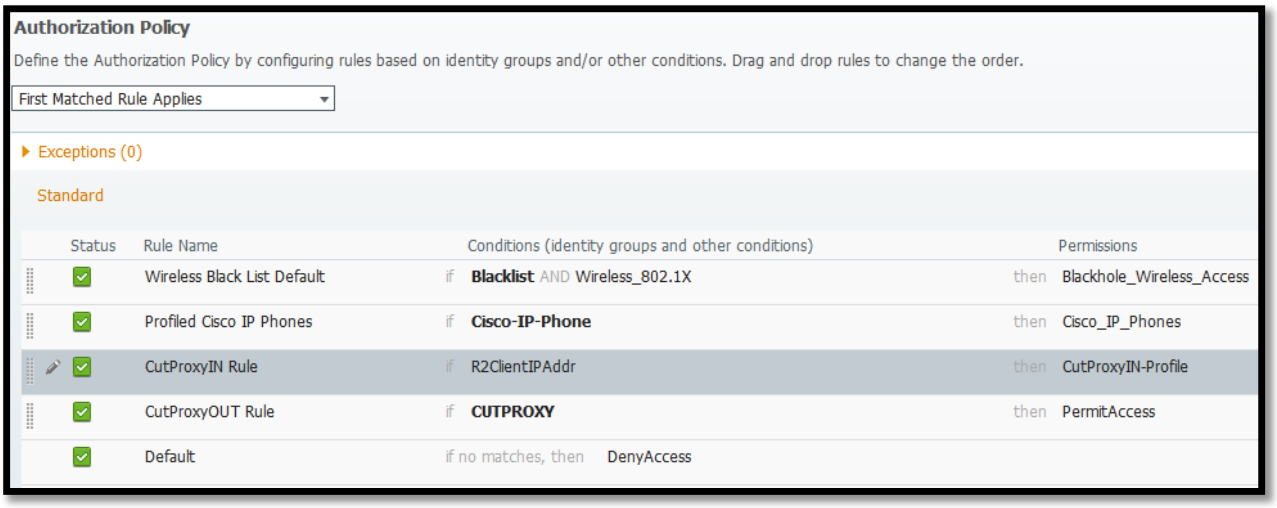
Then the policy condition, elements, Profile and AuthC & AuthZ rules :











This task demonstrates two different ways we can use to trigger Cut Proxy on the ASA – this is either gonna be direct authentication (Virtual Telnet/HTTP), or the indirect version with four supported protocols being Telnet, FTP, HTTP and HTTPs. Any other protocol cannot be used to trigger the authentication prompt.

Since we are supposed to authenticate using a single user (cutproxy) for outbound and inbound Proxy (two rules) we need to differentiate between the AuthZ Profiles we will then download for the user. For outbound access we only need Access-Accept since traffic going from higher->lower is allowed by default – no need to download any ACLs. For inbound we must download an ACL because the interface access-list blocks telnet access to R1.

Verification

Before you authenticate with the ASA telnet to R1 fails :

```
R2#telnet 192.1.12.1
Trying 192.1.12.1 ...
% Connection timed out; remote host not responding


R2#telnet 192.1.12.99
Trying 192.1.12.99 ... Open

LOGIN Authentication

Username: cutproxy

Password:


Error:  acl authorization denied

[Connection to 192.1.12.99 closed by foreign host]
```

Now it is OK since we have successfully authenticated :

```
R2#telnet 192.1.12.1
Trying 192.1.12.1 ... Open

R1>

ASA3/act(config)# sh ua
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'cutproxy' at 192.1.12.2, authenticated
   access-list #ACSACL#-IP-R2TelnetIN-51b76ef4 (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00

ASA3/act(config)# sh access-l | in R2TelnetIN
access-list #ACSACL#-IP-R2TelnetIN-51b76ef4; 2 elements; name hash:
0xc0f084ad (dynamic)
```

```
access-list #ACSACL#-IP-R2TelnetIN-51b76ef4 line 1 permit icmp any any
(hitcnt=0) 0xcd1b394f
access-list #ACSACL#-IP-R2TelnetIN-51b76ef4 line 2 permit tcp any host
192.1.12.1 eq telnet (hitcnt=1) 0xe2ba0068
```

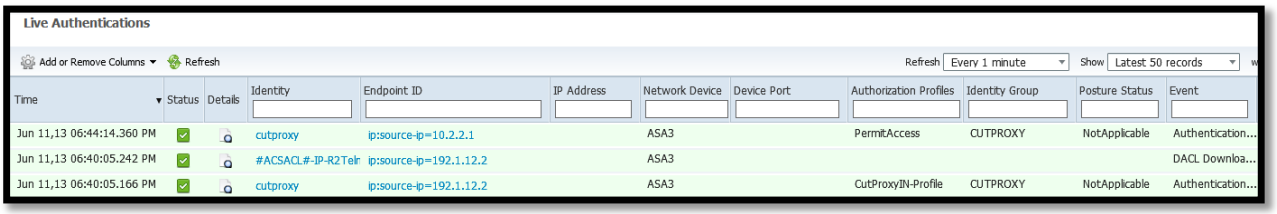
And the other direction – outbound connections :

```
R1#telnet 192.1.12.2 4515
Trying 192.1.12.2, 4515 ... Open


Error:  Must authenticate before using this service.

[Connection to 192.1.12.2 closed by foreign host]
```

OK so now we telnet – Telnet can trigger the authentication prompt as opposed to TCP port 4515 so after we authenticate we should be able to access both services :

```
R1#telnet 192.1.12.2
Trying 192.1.12.2 ... Open

Username: cutproxy

Password:


Password required, but none set


R1#telnet 192.1.12.2 4515
Trying 192.1.12.2, 4515 ...
% Connection refused by remote host
```

Note the correct AuthZ Profile was matched, as intended :



```
ASA3/act(config)# sh ua
                        Current    Most Seen
Authenticated Users       2          2
Authen In Progress        0          1
user 'cutproxy' at 10.2.2.1, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
user 'cutproxy' at 192.1.12.2, authenticated
   access-list #ACSACL#-IP-R2TelnetIN-51b76ef4 (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Task 5.3: Port Authentication (5 Points)

- Port G1/0/12 on CAT3 should be configured for 802.1x
- Only two devices are allowed to connect through this port – a Phone and PC
- Enable RADIUS Profiling along with Device Sensor feature
- Enable SNMP Query Profiling
- Authenticated user (“dot1xuser”, password “ipexpert”) should be placed into VLAN 5; MAB-authenticated Phone should go into Voice VLAN 499
- Unless the port is authenticated no user traffic should be allowed through it
- After authentication allow IP access to VLAN 49 and TFTP
- Also the connecting user’s station should obtain an IP address via DHCP
- Protect RADIUS communication with key “IntoDarkness”

Detailed Solution

CAT4

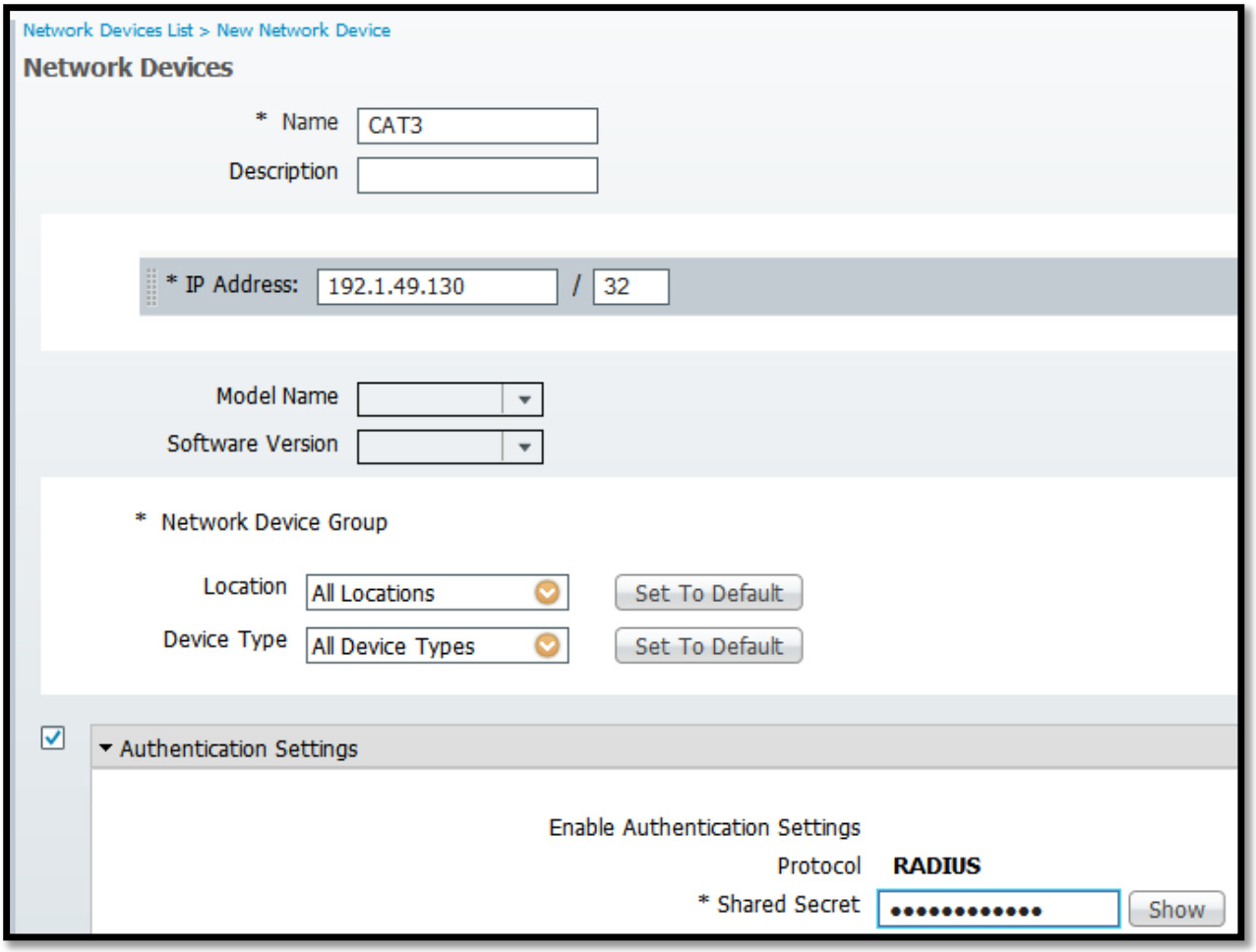
```
vlan 499
```

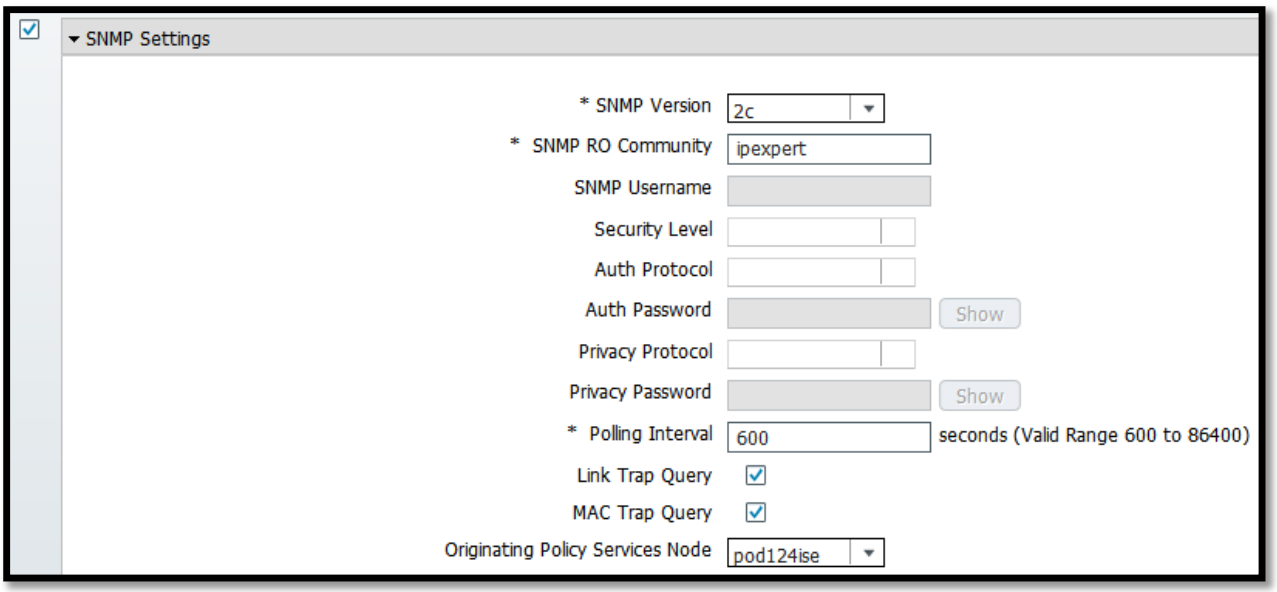
CAT3

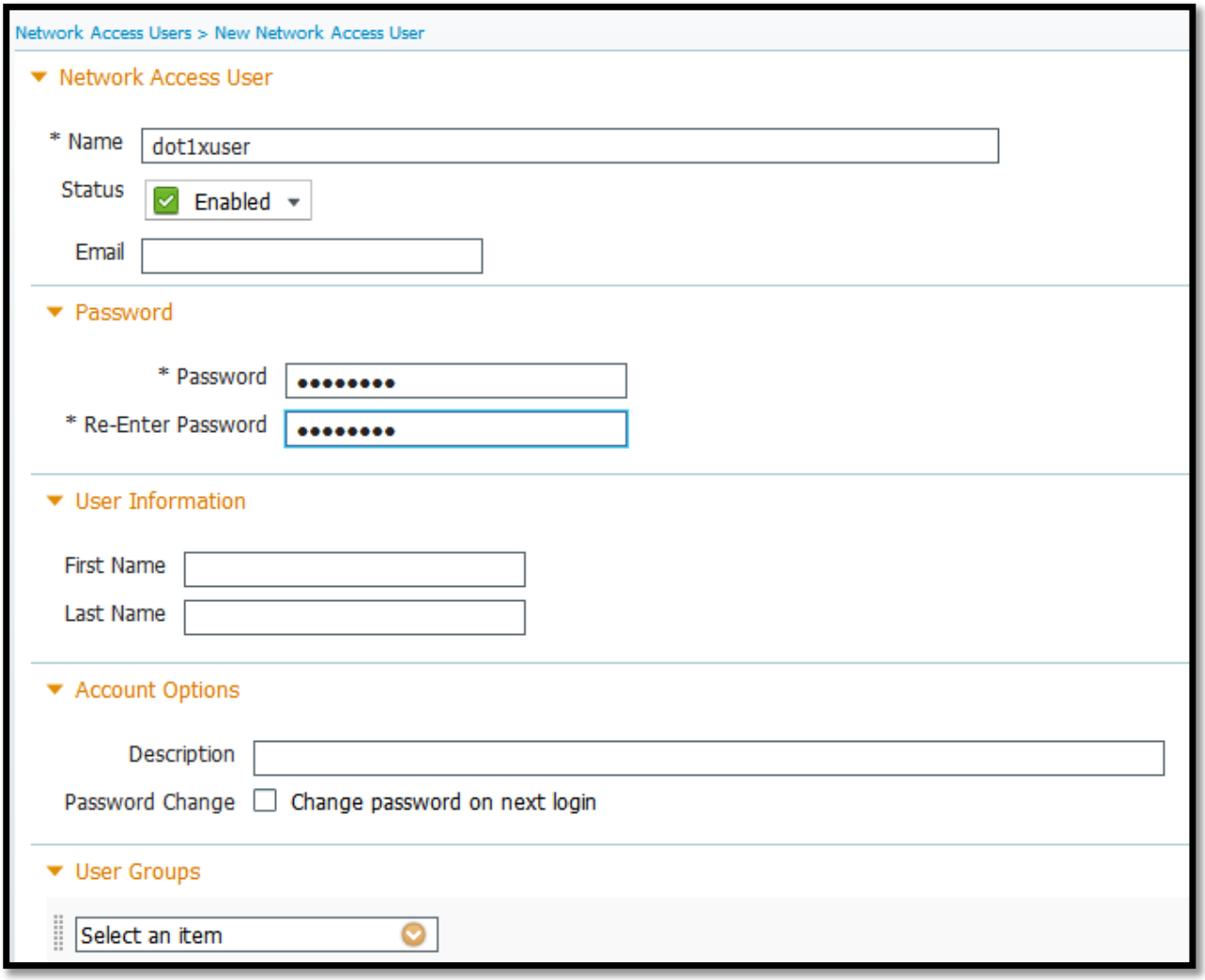
```
aaa new-model
aaa authentication login default none
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

```
radius server ISE
 address ipv4 10.1.1.150 auth-port 1645 acct-port 1646
 key IntoDarkness
radius-server vsa send accounting

device-sensor accounting
device-sensor notify all-changes

snmp-server community ipexpert RO

dot1x system-auth-control

ip device tracking

interface G1/0/12
 switchport mode access
 switchport voice vlan 499
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-domain
 dot1x pae authenticator
 dot1x timeout tx-period 10
 mab

ISE
ip route 192.1.49.0 255.255.255.0 gate 10.1.1.1
```

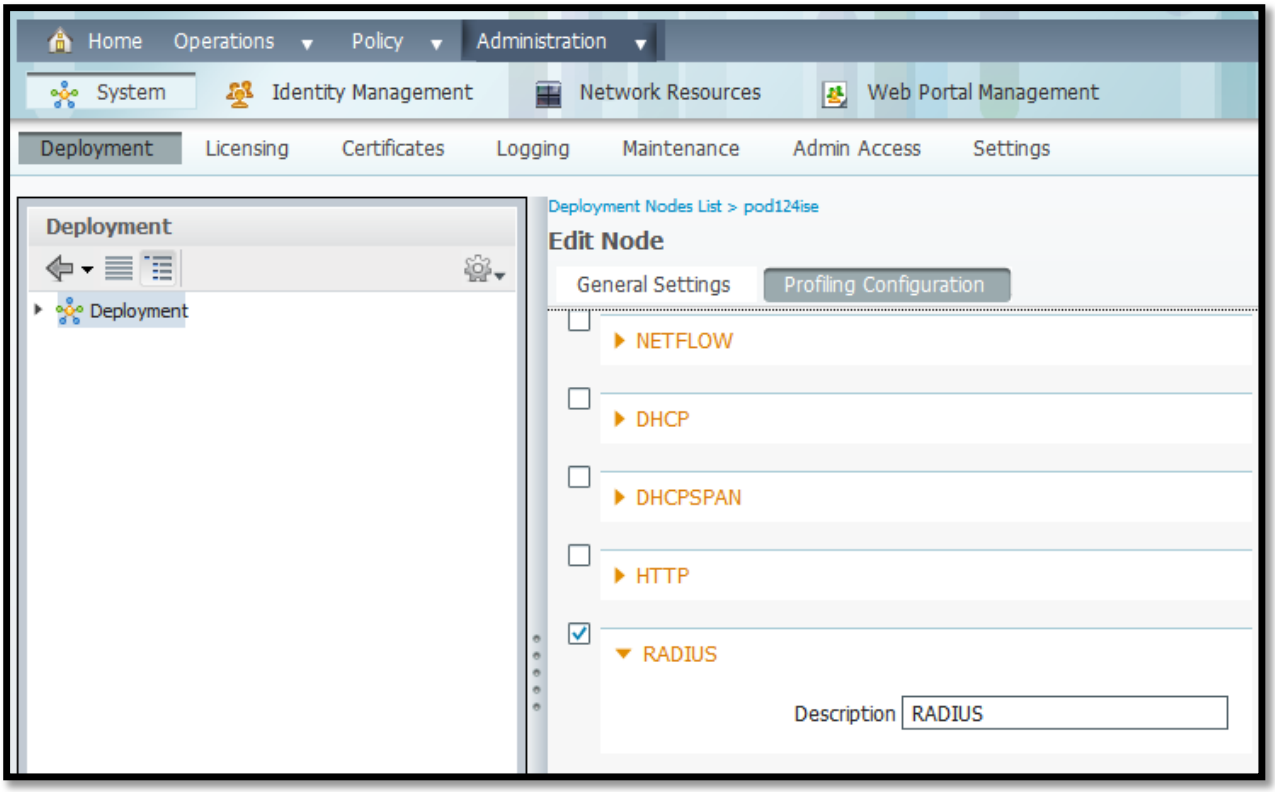
This time when you add CAT3 as a AAA Client also configure SNMP settings for Profiling purposes :

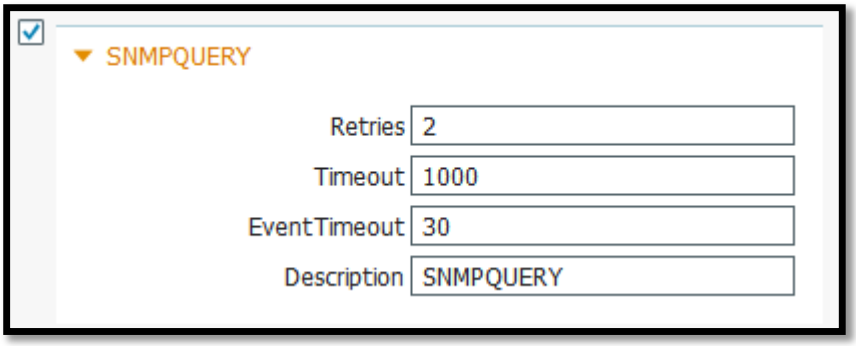




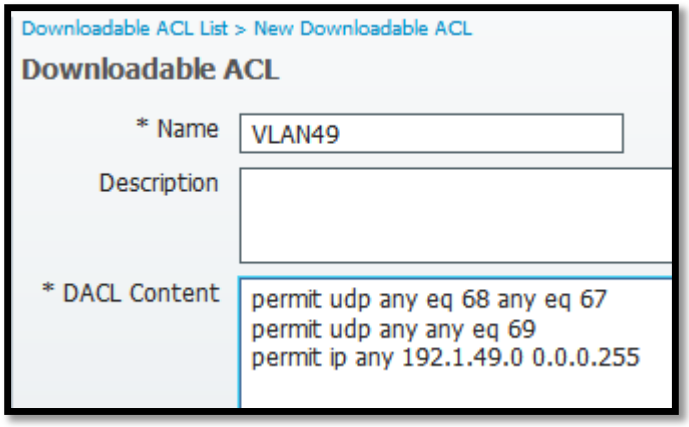


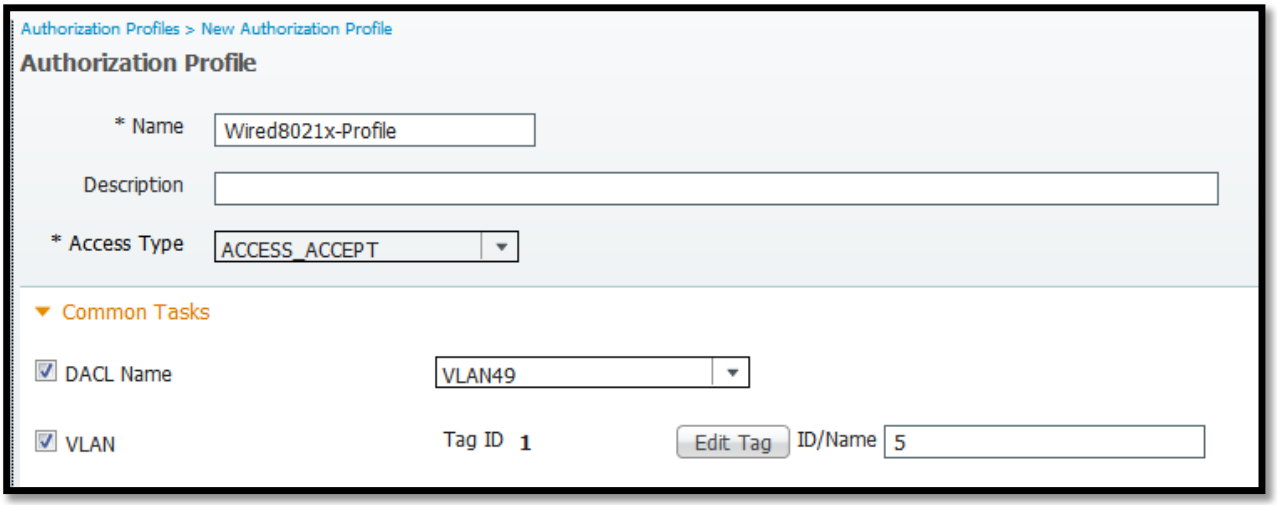
Now go under Administration -> System -> Deployment and enable RADIUS & SNMP Query Profiling :



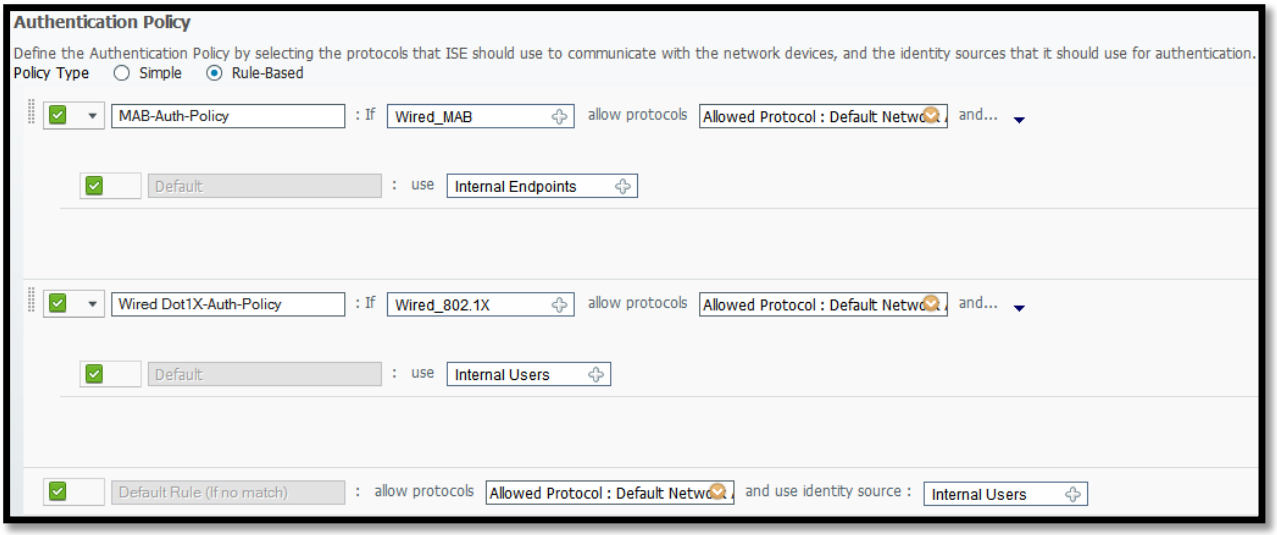


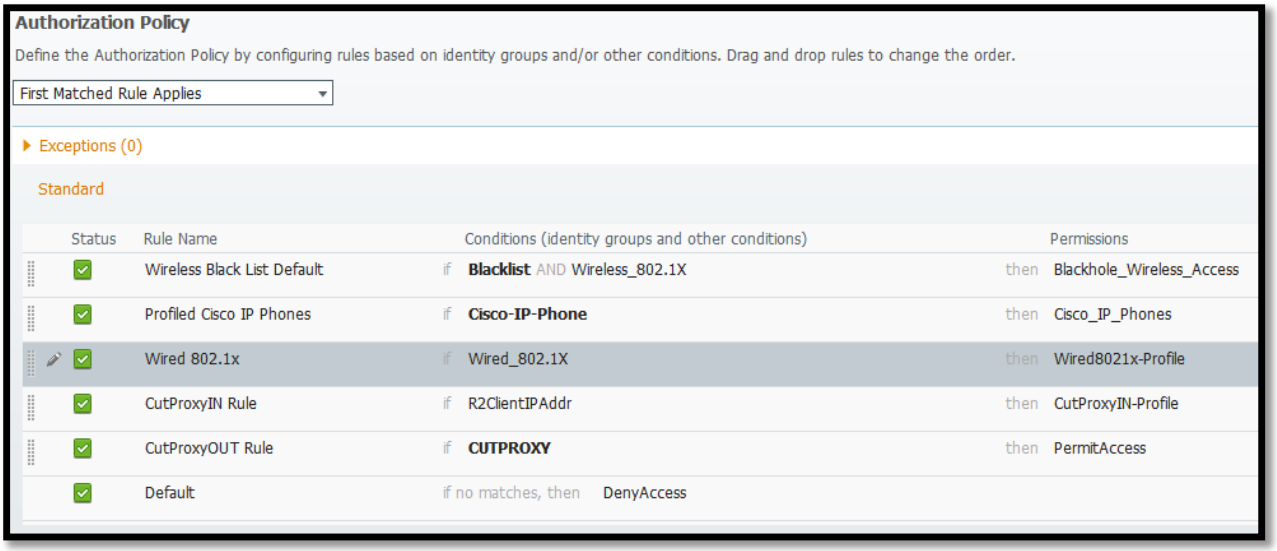
Next are Policy Elements and Policies :



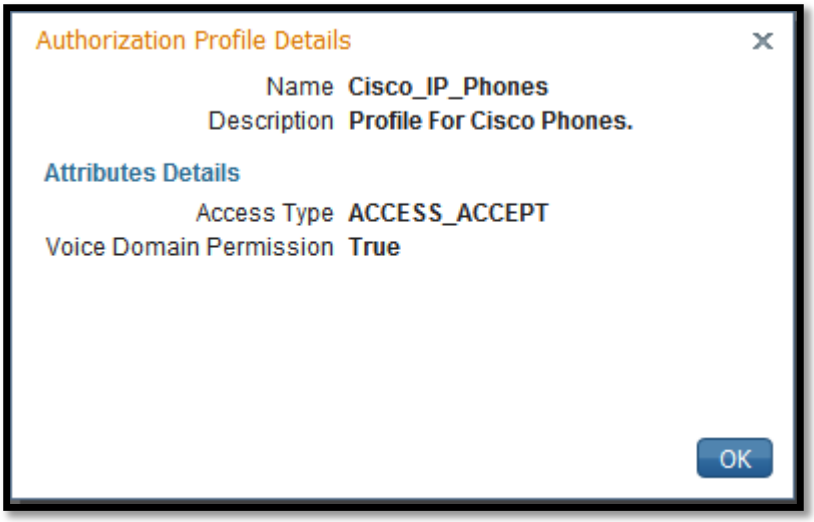


Conditions for MAB, Wired & Wireless 802.1x are pre-defined so this is an easy part :





Make sure the “Cisco_IP_Phones” prebuilt Profile gives Voice Permission :



It appears that this particular IOS version on CAT3 does not support Device Sensor feature. The Cache is populated but this information is not send in RADIUS Accounting packets although the configuration is correct (CDP information under the Endpoint Profile was populated from a SNMP Probe).

Verification

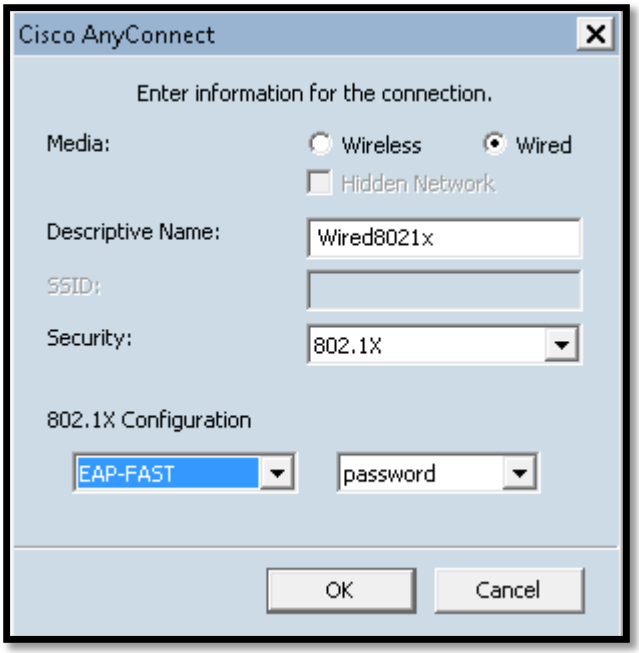
Start verification of MAB for the IP Phone :

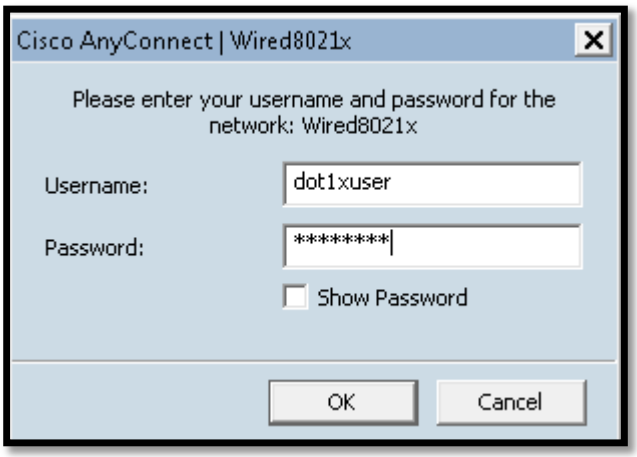
```
CAT3#sh device-sensor cache mac 001b.d4c6.1509
Device: 001b.d4c6.1509 on port GigabitEthernet1/0/12
-------------------------------------------------
Proto Type:Name                           Len Value
cdp     16:power-type                       6 00 10 00 06 18 9C
cdp     11:duplex-type                      5 00 0B 00 05 01
cdp      6:platform-type                   23 00 06 00 17 43 69 73 63 6F 20 49
50 20 50 68 6F
                                              6E 65 20 37 39 36 30
cdp      5:version-type                    16 00 05 00 10 50 30 30 33 30 37 30
32 30 34 30 30
cdp      4:capabilities-type                8 00 04 00 08 00 00 00 90
cdp      3:port-id-type                    10 00 03 00 0A 50 6F 72 74 20 31
cdp      1:device-name                     19 00 01 00 13 53 45 50 30 30 31 42
44 34 43 36 31
```

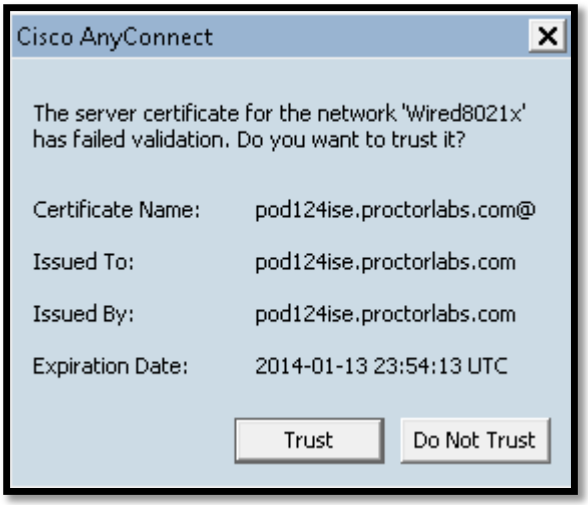
```
                                          35 30 39

CAT3#
%AUTHMGR-5-START: Starting 'mab' for client (001b.d4c6.1509) on Interface
Gi1/0/12 AuditSessionID C00131820000010B111FB80A
*Mar  4 07:56:20.567: %MAB-5-SUCCESS: Authentication successful for client
(001b.d4c6.1509) on Interface Gi1/0/12 AuditSessionID
C00131820000010B111FB80A
*Mar  4 07:56:20.567: %AUTHMGR-7-RESULT: Authentication result 'success'
from 'mab' for client (001b.d4c6.1509) on Interface Gi1/0/12
AuditSessionID C00131820000010B111FB80A
CAT3#
*Mar  4 07:56:21.549: %AUTHMGR-5-SUCCESS: Authorization succeeded for
client (001b.d4c6.1509) on Interface Gi1/0/12 AuditSessionID
C00131820000010B111FB80A


CAT3#sh authen sessions int g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4c6.1509
           IP Address:  Unknown
            User-Name:  00-1B-D4-C6-15-09
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C00131820000010B111FB80A
      Acct Session ID:  0x00000033
               Handle:  0xA900010C

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success

CAT3#sh int g1/0/12 sw | in Voice
Voice VLAN: 499 (VLAN0499)
```

CPMSessionID	C00131820000010B111FB80A
Called-Station-ID	C4-64-13-D1-C5-8C
Calling-Station-ID	00-1B-D4-C6-15-09
Class	CACS:C00131820000010B111FB80A:pod124ise/149398264/1072
DestinationIPAddress	10.1.1.150
DestinationPort	1645
Device IP Address	192.1.49.130
Device Port	1645
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	notRegistered
EndPointMACAddress	00-1B-D4-C6-15-09
EndPointMatchedProfile	Cisco-IP-Phone-7960
EndPointPolicy	Cisco-IP-Phone-7960
EndPointProfilerServer	pod124ise
EndPointSource	RADIUS Probe
Framed-MTU	1500
IdentityGroup	Cisco-IP-Phone
IdentityPolicyMatchedRule	Default
Location	Location#All Locations
MACAddress	00:1B:D4:C6:15:09
MatchedPolicy	Cisco-IP-Phone-7960

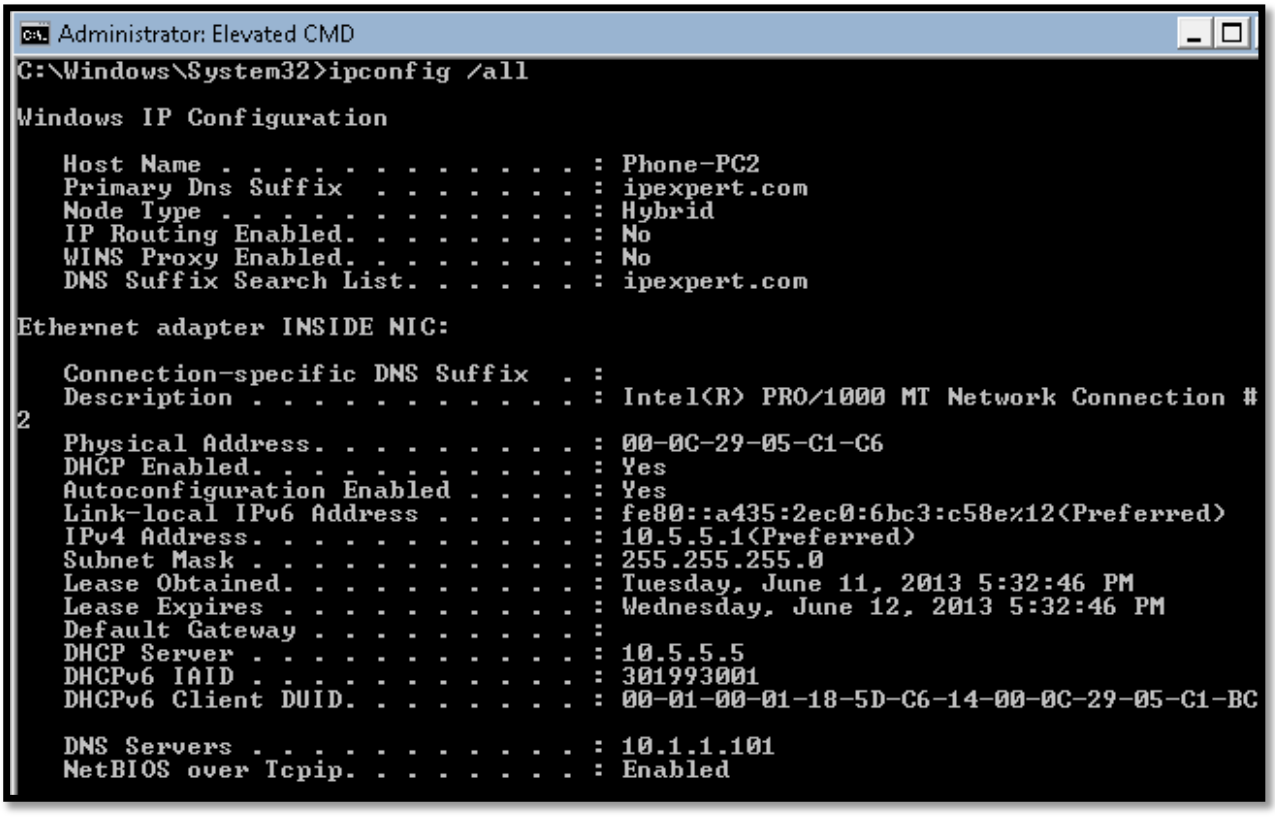
Now test 802.1x auhthentication. Create a new entry in the “Advanced” window of AnyConnect and then select it as a Profile for connection :

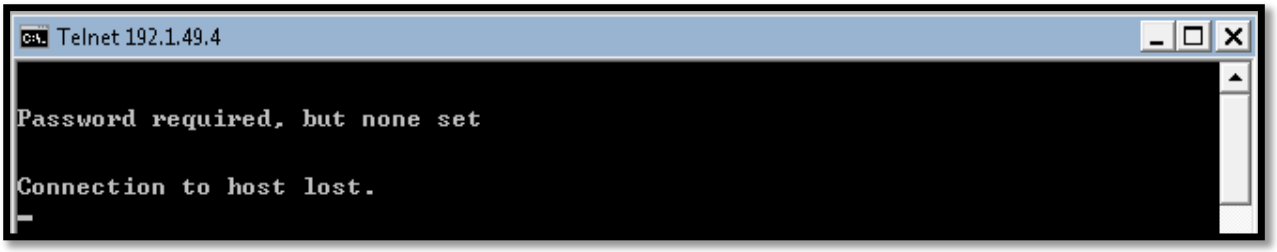


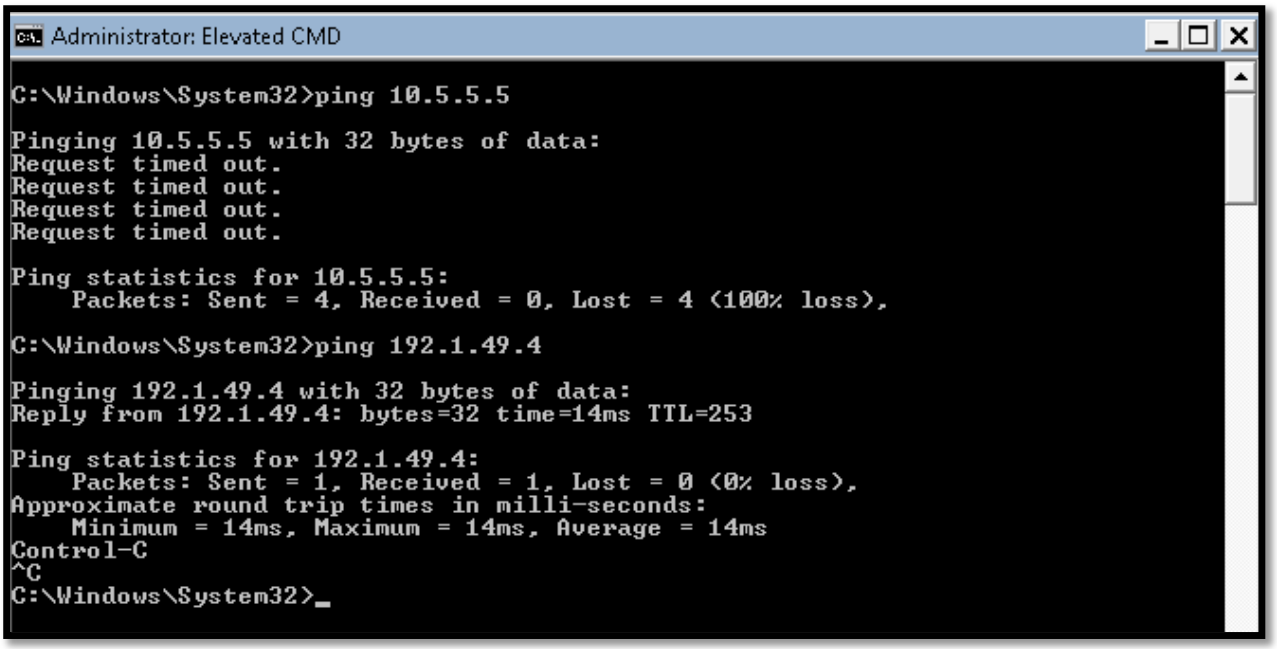




An IP address was assigned. If you add a route to VLAN49 Test PC will be able to access those networks but not local destinations for anything else than DHCP and TFTP :








```
*Mar  4 08:26:28.639: %AUTHMGR-7-RESULT: Authentication result 'success'
from 'dot1x' for client (000c.2905.c1c6) on Interface Gi1/0/12
AuditSessionID C0013182000011011424D33
CAT3(config-if)#
*Mar  4 08:26:28.648: %AUTHMGR-5-VLANASSIGN: VLAN 5 assigned to Interface
Gi1/0/12 AuditSessionID C0013182000011011424D33
*Mar  4 08:26:28.958: %AUTHMGR-5-SUCCESS: Authorization succeeded for
client (000c.2905.c1c6) on Interface Gi1/0/12 AuditSessionID
C0013182000011011424D33
```

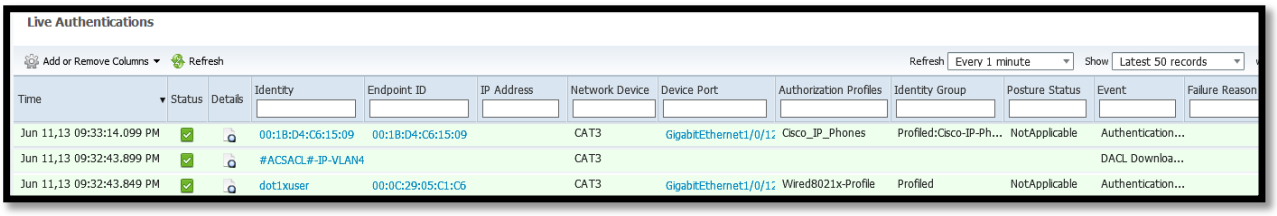
```
CAT3#sh authen sess int g1/0/12
            Interface:  GigabitEthernet1/0/12
          MAC Address:  000c.2905.c1c6
```

```
             IP Address:  Unknown
              User-Name:  dot1xuser
                 Status:  Authz Success
                 Domain:  DATA
        Security Policy:  Should Secure
        Security Status:  Unsecure
         Oper host mode:  multi-domain
       Oper control dir:  both
          Authorized By:  Authentication Server
            Vlan Policy:  5
                ACS ACL:  xACSACLx-IP-VLAN49-51b783d2
        Session timeout:  N/A
           Idle timeout:  N/A
      Common Session ID:  C0013182000011011424D33
        Acct Session ID:  0x00000038
                 Handle:  0x28000111

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run


----------------------------------------
            Interface:  GigabitEthernet1/0/12
          MAC Address:  001b.d4c6.1509
           IP Address:  Unknown
            User-Name:  00-1B-D4-C6-15-09
               Status:  Authz Success
               Domain:  VOICE
        Security Policy:  Should Secure
        Security Status:  Unsecure
         Oper host mode:  multi-domain
       Oper control dir:  both
          Authorized By:  Authentication Server
        Session timeout:  N/A
           Idle timeout:  N/A
      Common Session ID:  C00131820000010F11424513
        Acct Session ID:  0x00000037
                 Handle:  0x42000110
```

```
Runnable methods list:
       Method    State
       dot1x     Failed over
       mab       Authc Success
```

The Default ACL (“Auth-Default-ACL”) was automatically created by the switch since there was no ACL applied to the port and we want to use dACLs. Its purpose is to allow DHCP traffic through the port.

```
CAT3#sh access-l
Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348 (30
matches)
    20 permit udp any any range bootps 65347
    30 deny ip any any
Extended IP access list xACSACLx-IP-VLAN49-51b783d2 (per-user)
    10 permit udp any eq bootpc any eq bootps
    20 permit udp any any eq tftp
    30 permit ip any 192.1.49.0 0.0.0.255
```



6.0 Advanced Security (16 points)

Task 6.1: BGP (4 Points)

- Authenticate all iBGP peerings using MD5 authentication with a password of "ccie"
- Configure eBGP peering between R1 and R2 through the ASA
- R1 sees R2 as 192.1.12.2 and R2 should see R1 on AS1 as 1.1.1.1
- Authenticate this peering same way as iBGP
- Two Static routes are allowed for this task

Detailed Solution

ASA3

```
route inside 1.0.0.0 255.0.0.0 10.2.2.1

tcp-map BGP
  tcp-options range 19 19 allow

class-map BGP
 match port tcp eq bgp

policy-map global_policy
 class BGP
  set connection random-sequence-number disable
  set connection advanced-options BGP

access-list OUTSIDE_IN permit tcp host 192.1.12.2 host 1.1.1.1 eq bgp
```

R1

```
router bgp 1
 neighbor 192.1.12.2 remote-as 245
 neighbor 192.1.12.2 ebgp-multihop 255
 neighbor 192.1.12.2 pass ccie
 neighbor 192.1.12.2 update-source l0
```

R2

```
router bgp 245
 neighbor 4.4.4.4 password ccie
 neighbor 5.5.5.5 password ccie
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 password ccie
 neighbor 1.1.1.1 ebgp-multihop 255

ip route 1.0.0.0 255.0.0.0 192.1.12.30
```

R4

```
router bgp 245
 neighbor 2.2.2.2 pass ccie
```

R5

```
router bgp 245
 neighbor 2.2.2.2 pass ccie
```

IPS

```
service signature-definition sig1
signatures 1306 0
 status
  enabled false
```

What seems like a simple task here has a sting in the tail. We should all be familiar with running authenticated BGP through an ASA and the issues it causes.

A TCP Map is used to allow the md5 signature option 19 in the TCP header, and is enabled by being assigned to an MPF policy. Also be sure that the address is not translated, as this will also cause the MD5 authentication to fail (in our case 1.1.1.1 and 192.1.12.2 are not so we are good here).

The problem comes with the peering of R1 and R2. As this traffic passes through the IPS, the addition of the MD5 auth triggers the TCP option other signature 1306, which has an action of modifying the packet inline, by removing the MD5 option 19 from the TCP packet.

This signature is low, and is one that can be safely disabled if the traffic is legitimate within your network.

Verification

You configured the peering, passwords, ASA so it allows for BGP authentication and the peering R1-R2 still does not come up. Remember that we still have a Transparent Firewall and inline IPS between VLAN 11 and R1. If you take a look at the IPS you should notice “TCP Option Other Detected” signature fires :

```
R1#
*Jun 11 22:55:04.079: %TCP-6-BADAUTH: No MD5 digest from 192.1.12.2(21848)
to 1.1.1.1(179)



evIdsAlert: eventId=1041379286523810154 severity=low vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/11 22:48:16 2013/06/11 22:48:16 UTC
  signature: description=TCP Option Other id=1306 created=20050304
type=anomaly version=S272
    subsigId: 0
    sigDetails: TCP Option Other Detected
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.1.12.2
      port: 47546
    target:
      addr: locality=OUT 1.1.1.1
      port: 179
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
60
  threatRatingValue: 60
  interface: ge0_0
```

```
    protocol: tcp
```

If you now go under signature configuration (sig1, not sig0 – vs0 will only show you an alert but it won't modify the packet since it runs on a promiscuous interface) and verify what action is taken for this signature you will notice this is a Normalizer engine sig with "Modify Packet Inline" action – this is what breaks BGP MD5 :

```
IPS(config)# service signature-definition sig1
IPS(config-sig)# signatures 1306 0

IPS(config-sig-sig)# show settings
   <protected entry>
   sig-id: 1306
   subsig-id: 0
   ------------------------------------------------
      alert-severity: low <defaulted>
      sig-fidelity-rating: 100 <defaulted>
      promisc-delta: 0 <defaulted>
      sig-description
      ------------------------------------------------
         sig-name: TCP Option Other <defaulted>
         sig-string-info: TCP Option Other Detected <defaulted>
         sig-comment:  <defaulted>
         alert-traits: 0 <defaulted>
         release: S272 <defaulted>
         sig-creation-date: 20050304 <defaulted>
         sig-type: Anomaly <defaulted>
      ------------------------------------------------
      engine
      ------------------------------------------------
         normalizer
         ------------------------------------------------
            event-action: produce-alert|modify-packet-inline <defaulted>
            event-action-settings
```

After you disable the signature the peering should come up :

```
R1#
*Jun 11 22:56:30.111: %BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
```

```
R1#sh ip bgp su
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
192.1.12.2      4          245       4       4        1    0    0 00:00:26
0
```

All other peerings should be fine as well :

```
R5#clear ip bgp *
R5#
*Jun 11 22:52:27.739: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Down User reset
*Jun 11 22:52:27.743: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 IPv4
Unicast topology base removed from session  User reset
*Jun 11 22:52:27.875: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (5.5.5.5:21958) -- responder (2.2.2.2:179)
R5#
*Jun 11 22:52:27.927: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Up

R4#clear ip bgp *
R4#
*Jun 11 22:58:39.467: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Down User reset
*Jun 11 22:58:39.467: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 IPv4
Unicast topology base removed from session  User reset
*Jun 11 22:58:40.375: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Up
R2#debug tcp transactions
*Jun 11 22:59:21.129: TCP0: received md5 string: F6 2F F5 C4 5C FE 03 26
8A 34 36 78 FA 96 4D 7F
*Jun 11 22:59:21.129: digesting pseudo-header: src 704A9B50 dst 704A9B70
proto 0006 tcplen 003B
*Jun 11 22:59:21.129:   and tcp header:
        55 C6 00 B3 5E 92 E5 87 D3 15 7E 40 A0 18 3E 71 00 00 00 00
*Jun 11 22:59:21.129:   and 19 more bytes at 2B413DB4 (tcp 2B413D8C): FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF
*Jun 11 22:59:21.129: 00 13 04
*Jun 11 22:59:21.129:
*Jun 11 22:59:21.129:   and key 'ccie'
*Jun 11 22:59:21.129: TCP0: calculated md5 string: F6 2F F5 C4 5C FE 03 26
8A 34 36 78 FA 96 4D 7F
```

Task 6.2: BGP Traffic Filtering (4 Points)

- R5 should be receiving the following routes from the R9 :
  - 199.99.99.0 /24
- Devices within your topology should see the route learned from R9 with a next hop of 192.0.1.5, and if traffic is directed to these networks, it should be silently dropped locally
- You can add four static routes in this task

Detailed Solution

R9

```
route-map SETHOP permit 10
 set ip next-hop 192.0.1.5

router bgp 9
 neighbor 5.5.5.5 ebgp-multihop 2
 neighbor 5.5.5.5 update-source Loopback0
 neighbor 5.5.5.5 route-map SETHOP out
```

R1, R4, R5

```
ip route 192.0.1.5 255.255.255.255 null0

int null0
 no ip unreachables
```

R2

```
ip route 192.0.1.5 255.255.255.255 null0

int null0
 no ip unreachables

route-map SETHOP permit 10
 set ip next-hop 192.0.1.5

router bgp 245
```

```
 neighbor 1.1.1.1 route-map SETHOP out
```

Our example deploys a form of destination RTBH by manually manipulating the Next Hop attribute for 199.99.99.0/24 network (after R9 – R5 peering is fixed – two commands were missing on R9 to get this work).

We simply define a route map, changing the next hop to an address that is directed to Null0 on each BGP peer. The catch here is that this not only has to be configured on R9 (trigger router), but on R2 as well, since the next hop will not be preserved when advertising the route to an external AS.

Setting “no ip unreachables” fulfills the task of dropping the packets silently.

Verification

```
R5#sh ip bgp 199.99.99.0
BGP routing table entry for 199.99.99.0/24, version 3
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     4
  9
    192.0.1.5 from 9.9.9.9 (9.9.9.9)
      Origin IGP, metric 0, localpref 100, valid, external, best

R2#sh ip bgp 199.99.99.0
BGP routing table entry for 199.99.99.0/24, version 4
Paths: (1 available, best #1, table default)
Flag: 0x820
  Advertised to update-groups:
     1
  9, (Received from a RR-client)
    192.0.1.5 from 5.5.5.5 (5.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best

R1#sh ip bgp
BGP table version is 4, local router ID is 1.1.1.1
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
*> 199.99.99.0      192.0.1.5                              0 245 9 i
```

If you were to enable IP Unreachables on Null0 e.g. on R2 – it would be sending ICMP packets back to the source telling it the destination is not reachable :

```
ASA3/act(config)# ping 199.99.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 199.99.99.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)

R2# debug ip icmp
*Jun 12 16:30:10.793: ICMP: dst (199.99.99.1) host unreachable sent to
192.1.12.30
*Jun 12 16:30:16.789: ICMP: dst (199.99.99.1) host unreachable sent to
192.1.12.30


CAT3#ping 199.99.99.1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 199.99.99.1, timeout is 2 seconds:
..........
Success rate is 0 percent (0/10)

R4#sh int null0
Null0 is up, line protocol is up
  Hardware is Unknown
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 0 usec,
     reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10 packets output, 1140 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Task 6.3: Management (4 Points)

- CAT4 has a management interface belonging to VLAN 6
- Allow management access to this switch from VLANs 5 & 6 only
- VLAN 5 should see CAT4 as 192.1.16.140
- This NAT should be carried out on R6
- Configure SSH on R2
- SSH authentication should be done locally
- Create a user “admin” with a password of “cisco”
- Allow Management traffic (SSH/Telnet/HTTP/HTTPS) to Interface Gi0/1 only, logging dropped packets. Do not use ACLs to accomplish this

Detailed Solution

CAT4

```
access-list 6 permit 192.1.6.0 0.0.0.255
access-list 6 permit 10.5.5.0 0.0.0.255
access-list 6 deny   any log

line vty 0 4
 access-class 6 in
 password ipexpert
 login

enable secret ipexpert
```

R6

```
access-list 109 deny   ip host 192.1.6.140 host 9.9.9.9
access-list 109 permit ip host 192.1.6.140 any

route-map SW4NAT permit 10
 match ip address 109

ip nat pool CAT4POOL 192.1.16.140 192.1.16.140 prefix-length 24 add-route
ip nat ins source static 192.1.6.140 192.1.16.140 route-map SW4NAT
reversible

interface FastEthernet0/1
 ip nat inside

interface Serial0/1/0
 ip nat outside

router ospf 1
 redistribute static subnets
```

R2

```
username admin password cisco

line vty 0 15
 login local

class-map type logging match-any LOG_CLASS
 match packets dropped

policy-map type logging LOG_POL
 class LOG_CLASS
    log

control-plane host
 management-interface GigabitEthernet0/1 allow http https ssh telnet
 service-policy type logging input LOG_POL
```

Use an access-class feature to restrict access to SW4's VTY lines.

We now need to be careful with the NAT, as this will break the GETVPN encrypted traffic requirements. Be sure to use an ACL to deny the VPN interesting traffic from being NATed, and add this ACL to a route map. This will be used in the static NAT line. The "reversible" command can be added to ensure the outside to inside logic reversal occurs due to the assignment of the ACL in the route map.

The next issue here lies with the address used for NAT. It is not currently advertised to the rest of the network. Create a NAT pool using the post-NAT address with the keyword "add-route". We can then propagate this address to the rest of the network by redistributing statics in OSPF.

On R2, we need to tie down management to Gi0/1, and the best way to do this is by using a feature called Management Plane Protection. This allows us to be relatively granular in the management protocols that we allow to it. Just keep in mind that when using this feature it accounts for both inbound and outbound management traffic.

We finish this off by using another feature, Control Plane Logging, which is similar to the inspection policies or MQC. This time we are using a specific class and policy type of "logging" that we use to match on dropped packets by the Control Plane. Without this very useful feature it's very difficult to see what exactly is being dropped.

Verification

```
R5#sh ip ro 192.1.16.140
Routing entry for 192.1.16.0/24
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward
metric 128
  Last update from 192.1.25.2 on Serial0/1/0, 00:11:09 ago
  Routing Descriptor Blocks:
  * 192.1.25.2, from 6.6.6.6, 00:11:09 ago, via Serial0/1/0
      Route metric is 20, traffic share count is 1

R5#telnet 192.1.16.140
Trying 192.1.16.140 ...
% Connection refused by remote host

R5#telnet 192.1.16.140 /source-interface f0/1
Trying 192.1.16.140 ... Open
```

```
User Access Verification

Password:

CAT4>

R6#sh ip nat t
Pro Inside global      Inside local       Outside local      Outside
global
tcp 192.1.16.140:23    192.1.6.140:23     10.5.5.5:64676
10.5.5.5:64676
tcp 192.1.16.140:23    192.1.6.140:23     192.1.25.5:49771
192.1.25.5:49771
--- 192.1.16.140       192.1.6.140        ---                ---



R6#deb ip nat de
IP NAT detailed debugging is on

R9#telnet 192.1.16.140 /so l0
Trying 192.1.16.140 ...
% Connection timed out; remote host not responding

R6#
*Jun 12 16:59:22.759: NAT(acl): name 109 failed

R9#telnet 192.1.16.140
Trying 192.1.16.140 ... Open

User Access Verification

Password:



R5#telnet 192.1.12.2
Trying 192.1.12.2 ...
```

```
R2#
*Jun 12 17:04:07.517: %CP-6-TCP: DROP Management-Interface
192.1.25.5(25664) -> 192.1.12.2(23)


R8#telnet 192.1.12.2
Trying 192.1.12.2 ... Open


User Access Verification

Username: admin
Password:
R2>
```

Note that the return management traffic is also subject to the Management Plane Protection feature :

```
R2#telnet 192.1.24.4
Trying 192.1.24.4 ...
*Jun 12 17:10:53.133: %CP-6-TCP: DROP Management-Interface  192.1.24.4(23)
-> 192.1.24.2(35874)

R2#sh management-interface
Management interface GigabitEthernet0/1
        Protocol        Packets processed
            http                 0
           https                 0
             ssh                 0
          telnet                24


R2#sh policy-map type logging control-plane host

 Control Plane Host

  Service-policy logging input: LOG_POL

    Class-map: LOG_CLASS (match-any)
```

```
    5 packets, 236 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match:  packets dropped
      0 packets, 0 bytes
      5 minute rate 0 bps
    log

  Class-map: class-default (match-any)
    163 packets, 12457 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

Task 6.4: DHCP (4 Points)

- Enable R2 as a DHCP Server with the following information :
  - IP ADDRESS : 192.1.49.0/24
  - WINS ADDRESS : 192.1.49.135
  - DNS ADDRESS : 192.1.49.53
  - DEFAULT GATEWAY : 192.1.49.4
  - LEASE TIME : 6 Days
- Enable DHCP Relay function on R4 F0/1 (so it forwards DHCP requests to R2)
- Configure CAT2 for DHCP snooping for R2
- Rate Limit DHCP packets to R2 to 50pps

Detailed Solution

R2

```
ip dhcp excluded-address 192.1.49.4
ip dhcp excluded-address 192.1.49.53
ip dhcp excluded-address 192.1.49.130
ip dhcp excluded-address 192.1.49.135
ip dhcp pool R2DP
   network 192.1.49.0 255.255.255.0
   netbios-name-server 192.1.49.135
   dns-server 192.1.49.53
```

```
   default-router 192.1.49.4
   lease 6
```

R4

```
int f0/1
 ip helper-address 192.1.24.2
```

CAT2

```
ip dhcp snooping vlan 49
ip dhcp snooping

no ip dhcp snooping information option

interface FastEthernet0/4
 ip dhcp snooping limit rate 50
 ip dhcp snooping trust
```

IOS has the ability of providing DHCP server functionality to the network, although it is not meant to act as an enterprise DHCP service. We create a pool to define the network for which we will be serving IP addresses automatically. The pool also contains numerous other attributes that will be assigned along with the address. For this task, we are asked to include the DNS server, NetBIOS or WINS name server, the default gateway of R4 F0/1, and the duration that the address will be leased for. As we already have hosts using static addresses on VLAN 49, we need to exclude these addresses from the DHCP pool. Remember to include the DNS and WINS servers in the exclusion, too.

To forward the DHCP request to the DHCP server from R4 we need to configure an IP helper address on F0/1. This allows the forwarding of UDP broadcasts outside the local broadcast domain.

DHCP Snooping is the weapon of choice for mitigating DHCP-related attacks in the network. It does this by filtering out untrusted DHCP traffic, while maintaining a binding database of all static and dynamically assigned hosts and their IP/MAC addresses. For this feature to function correctly, each DHCP server must be connected to a DHCP Snooping trusted interface. To enable this we must assign DHCP Snooping to a VLAN and then enable the feature using 'ip dhcp snooping.' The interface of the DHCP server, or in our case the forwarding device (R4), is made a trusted interface and the rate of DHCP packets on the interface is limited to 50pps.

We also need to configure the switch to stop inserting DHCP option 82 into DHCP DISCOVERY packets so when the DHCP Relay Agent receives them it can process them and forward to the real DHCP Server.

Verification

Test on CAT3 – temporarily change IP address on VLAN 49 interface to be assigned via DHCP.

```
R2#debug ip dhcp server packet
*Jun 12 18:01:32.137: DHCPD: No default domain to append - abort update
*Jun 12 18:01:32.137: DHCPD: Sending DHCPACK to client
0063.6973.636f.2d63.3436.342e.3133.6431.2e63.3563.312d.566c.3439
(192.1.49.1).
*Jun 12 18:01:32.137: DHCPD: no option 125
*Jun 12 18:01:32.137: DHCPD: unicasting BOOTREPLY for client
c464.13d1.c5c1 to relay 192.1.49.4.


CAT3#
*Mar  5 04:54:19.691: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan49 assigned
DHCP address 192.1.49.1, mask 255.255.255.0, hostname CAT3

CAT3(config-if)#do sh ip int br | e una
Interface              IP-Address      OK? Method Status
Protocol
Vlan49                 192.1.49.1      YES DHCP   up                    up

CAT3(config-if)#do ping 192.1.49.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.49.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms


CAT2#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
```

```
49
DHCP snooping is operational on following VLANs:
49
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: 001b.d4c1.5400 (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    Allow option    Rate limit (pps)
-----------------------     -------    ------------    ----------------
FastEthernet0/4             yes        yes             50
  Custom circuit-ids:

CAT2#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----  ----
----------------
C4:64:13:D1:C5:C1   192.1.49.1       518137      dhcp-snooping   49
FastEthernet0/15
Total number of bindings: 1
```

7.0 Attack Mitigation (11 points)

Task 7.1: IP Options Attacks (2 Points)

- On R4 do not allow packets with IP options - do not use an ACL for this
- R6 should drop any IP packets containing the timestamp & IP Option 82 from the frame cloud
- Log all packets with any other IP Option

Detailed Solution

R4

```
ip options drop
```

R6

```
ip access-list extended OP_BLOCK
 deny   ip any any option timestamp
 deny   ip any any option traceroute
 permit ip any any option any-options log
 permit ip any any

interface Serial0/1/0
 ip access-group OP_BLOCK in
```

The “ip option drop” on R2 will prevent all packets that contain IP Options to be dropped (transit and to the device).

Option 82 is the traceroute option (use the “?” to figure that out); then “any-options” matches packets with any IP Option set so that’s what we want to log based on what the question calls for.

Verification

```
R5#ping
Protocol [ip]:
Target IP address: 192.1.6.6
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]: timestamp
Number of timestamps [ 9 ]: 5
Loose, Strict, Record, Timestamp, Verbose[TV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 192.1.6.6, 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)

Unreachable from 192.1.26.6.  Received packet has 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)

Success rate is 0 percent (0/2)
```

Then generate a similar ping but this time with a Route Record option :

```
R6#
*Jun 12 18:31:38.938: %SEC-6-IPACCESSLOGDP: list OP_BLOCK permitted icmp
192.1.25.5 -> 192.1.6.6 (0/0), 1 packet

R6#sh access-l OP_BLOCK
Extended IP access list OP_BLOCK
    10 deny ip any any option timestamp (2 matches)
    20 deny ip any any option traceroute
    30 permit ip any any option any-options log (5 matches)
    40 permit ip any any (25 matches)
```

Then test R4 :

```
R5#ping
Protocol [ip]:
Target IP address: 192.1.49.4
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]: record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.49.4, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
```

```
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)

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)

R4#sh ip traffic |  in options
         0 security failures, 0 bad options, 5 with options
         5 options denied
```

Task 7.2: TCP SYN Floods (3 Points)

- The 192.1.6.0 network is experiencing SYN attacks from the Frame cloud to your web servers (HTTP and HTTPs)
- R6 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets
- Limit TCP intercept to only watch packets coming from 192.1.26.0, 192.1.24.0 or the 192.1.25.0 networks for Web traffic towards R6
- Configure TCP intercept such that the router drops embryonic connections if they reach 1050. It should stop dropping the embryonic connections once the number reaches 850

Detailed Solution

R6

```
access-list 106 permit tcp 192.1.24.0 0.0.0.255 192.1.6.0 0.0.0.255 eq www
access-list 106 permit tcp 192.1.24.0 0.0.0.255 192.1.6.0 0.0.0.255 eq 443
access-list 106 permit tcp 192.1.25.0 0.0.0.255 192.1.6.0 0.0.0.255 eq www
access-list 106 permit tcp 192.1.25.0 0.0.0.255 192.1.6.0 0.0.0.255 eq 443
access-list 106 permit tcp 192.1.26.0 0.0.0.255 192.1.6.0 0.0.0.255 eq www
access-list 106 permit tcp 192.1.26.0 0.0.0.255 192.1.6.0 0.0.0.255 eq 443
```

```
ip tcp intercept list 106
ip tcp intercept watch-timeout 20
ip tcp intercept max-incomplete low 850 high 1050
ip tcp intercept mode watch
```

Although now classified as more of a legacy feature, TCP Intercept is still a valid lab topic, for protecting against common TCP attacks - mostly SYN floods.

First you need to define an ACL of interesting traffic. The 'ip tcp intercept list 106' line is then used to globally enable TCP Intercept.

As we are asked to watch the traffic and not proxy it, we need to switch to Watch Mode and use the watch timeout, not the connection timeout.

Verification

Telnet to CAT4's original IP from R2 over port 80 :

```
R2#telnet 192.1.6.140 80
Trying 192.1.6.140, 80 ...

R6#sh tcp intercept stat
Watching new connections using access-list 106
1 incomplete, 0 established connections (total 1)
0 connection requests per minute

R6#sh tcp intercept conn
Incomplete:
Client                Server                State    Create   Timeout
Mode
192.1.26.2:43667      192.1.6.140:80        SYNSENT  00:00:05 00:00:14 W

Established:
Client                Server                State    Create   Timeout
Mode

R6#sh access-l 106
Extended IP access list 106
```

```
    10 permit tcp 192.1.24.0 0.0.0.255 192.1.6.0 0.0.0.255 eq www
    20 permit tcp 192.1.24.0 0.0.0.255 192.1.6.0 0.0.0.255 eq 443
    30 permit tcp 192.1.25.0 0.0.0.255 192.1.6.0 0.0.0.255 eq www
    40 permit tcp 192.1.25.0 0.0.0.255 192.1.6.0 0.0.0.255 eq 443
    50 permit tcp 192.1.26.0 0.0.0.255 192.1.6.0 0.0.0.255 eq www (12
matches)
    60 permit tcp 192.1.26.0 0.0.0.255 192.1.6.0 0.0.0.255 eq 443
```

Task 7.3: Fragmentation & L2 Attacks (3 Points)

- Configure R6's FastEthernet interface to block inbound non-initial fragments with a destination of R2's G0/1
- Log those fragments and make sure information about source MAC address of the device sending fragments is also included
- Other traffic should not be affected
- Prevent VLAN Hopping attacks on CAT2 Port F0/2
- Prevent a MAC Flooding attack on CAT4 Port G1/0/1. Allow no more than 2 MAC addresses, and ensure that learned MAC's are saved to startup config

Detailed Solution

R6

```
ip access-list extended NOFRAGS
 deny ip any host 192.1.12.2 fragments log-input
 permit ip any any

interface FastEthernet0/1
 ip access-group NOFRAGS in
```

CAT2

```
interface FastEthernet0/2
 switchport nonegotiate
```

```
vlan dot1q tag native
```

CAT4

```
interface G1/0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky

kron occurrence WRITE_MEM in 10 recurring
 policy-list WRITE_MEM
kron policy-list WRITE_MEM
 cli write memory
```

For R6, we used an extended ACL to match, drop and log any fragmented packets inbound on the interface. When dropping fragments in an ACL, be sure to have the fragments line at the top of the ACL. Having the fragment line below the "ip any any" would result in all fragments being permitted.

To prevent VLAN Hopping we need to make sure that the port is in access mode and is not capable of auto negotiating the port mode to trunk. The Native VLAN tagging will assist in ensuring that the other version of this attack, double-tagging, cannot be implemented as well.

The MAC Flooding or CAM Table Overflow attack is prevented by using port security. Setting port security maximum to 2 will only allow 2 MAC addresses from that switchport, while the sticky command dynamically learns the MAC addresses and writes them to the running config.

Now to copy the running configuration to startup so the configuration is not lost we used KRON to schedule the copy of running-configuration to startup-configuration. It isn't perfect but saving the configuration every 10 minutes should be sufficient.

Verification

```
CAT4#ping 192.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/18/26 ms
```

```
CAT4#ping 192.1.12.2 size 1501 rep 2
Type escape sequence to abort.
Sending 2, 1501-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
..
Success rate is 0 percent (0/2)

R6#
*Jun 12 19:33:34.790: %SEC-6-IPACCESSLOGDP: list NOFRAGS denied icmp
192.1.6.140 (FastEthernet0/1 0007.7dbc.c6c1) -> 192.1.12.2 (0/0), 1 packet

CAT4#sh int vlan 6 | in bia
  Hardware is EtherSVI, address is 0007.7dbc.c6c1 (bia 0007.7dbc.c6c1)

R6#sh access-l NOFRAGS
Extended IP access list NOFRAGS
    10 deny ip any host 192.1.12.2 fragments log-input (2 matches)
    20 permit ip any any (9 matches)


CAT2#sh int f0/2 sw | in Negotiation
Negotiation of Trunking: Off

CAT4#sh kron schedule
Kron Occurrence Schedule
WRITE-MEM inactive, will run again in 0 days 00:09:36


CAT4#show port-security int g1/0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0023.3353.b769:100
```

```
Security Violation Count   : 0


CAT4#sh port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
---
Vlan    Mac Address       Type                          Ports   Remaining
Age
                                                                    (mins)
----    -----------       ----                          -----   ----------
---
 100    0023.3353.b769    SecureSticky                  Gi1/0/1      -
-----------------------------------------------------------------------------
---
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

After 10 minutes elapses :

```
CAT4#sh startup-config | in port-security
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0023.3353.b769
```

Task 7.4: IPv6 Attacks (3 Points)

- Make sure the ASA only allows one ICMPv6 Reply to come in for every single Request being allowed to go through
- Block and log all IPv6 fragments flowing through the ASA's inside interface
- Don't use Virtual Reassembly to accomplish this
- Drop IPv6 fragments received on R8's F0/0 interface

Detailed Solution

ASA3

```
fixup proto icmp

policy-map type inspect ipv6 IP6_POL
  match header fragment
  drop log

class-map IP6
 match any

policy-map INPOL
 class IP6
  inspect ipv6 IP6_POL

service-policy INPOL interface inside
```

R8

```
ipv6 access-list BLOCK6
 deny ipv6 any any fragments
 permit ipv6 any any

int f0/0
 ipv6 traffic-filter BLOCK6 in
```

There are two ways to drop IPv6 fragmented traffic on the ASA – the “fragment chain” command and IPv6 inspection. On IOS you can use an ACL or the Virtual Fragmentation & Reassembly feature along with the “drop” keyword.

ASA’s IPv6 inspection with the code version we have in ProctorLabs does not appear to work correctly with ICMP packets (“fragment chain” does) – use UDP probes instead for verification.

Verification

```
R1#ping 2012::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2012::2, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

ASA3/act(config)# sh service-policy global | in icmp
      Inspect: icmp, packet 5, lock fail 0, drop 0, reset-drop 0
```

Temporarily add a route to the DMZ on R1 via R8 (ipv6 route 2005::/64 2002::8) and test :

```
R1#ping 2005::8 size 1501

Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 2005::8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R8#sh ipv6 access-l
IPv6 access list BLOCK6
    deny ipv6 any any fragments (5 matches) sequence 10
    permit ipv6 any any (44 matches) sequence 20
```

Now the ASA :

```
R1#ping ipv
Target IPv6 address: 2012::2
Repeat count [5]:
Datagram size [100]: 1501
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 5, 1501-byte UDP Echos to 2012::2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ASA3/act(config)#
%ASA-4-325004: IPv6 Extension Header fragment denied and logged by
configuration. UDP from inside:2002::1/55948 to outside:2012::2/7

ASA3/act(config)# sh service-policy ins ipv

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default

Interface inside:
  Service-policy: INPOL
    Class-map: IP6
      Inspect: ipv6 IP6_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 fragment
          drop log, packet 10
        match header routing-type
          drop, packet 0
          log, packet 0
```

Fragments not going through the inside are not affected (to test this you need to allow UDP over IPv6 on the outside) :

```
R2#ping ipv
Target IPv6 address: 2005::8
Repeat count [5]:
Datagram size [100]: 1501
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 5, 1501-byte UDP Echos to 2005::8, timeout is 2 seconds:
PPPPP
Success rate is 0 percent (0/5)
```

Lab 5

Please look at the provided diagrams and read through the whole lab before you start. Read the directions very carefully to make sure you are doing what is being asked of you. This concept is very important when you take the CCIE lab administered by Cisco

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. You may add static routes on your Test PCs, AD Server, ISE, ACS and WSA to reach any networks.

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

NOTE: Unicast static/default routes are NOT allowed (except on Test PCs, AD server, ISE, ACS and WSA) unless otherwise stated in the task

NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device

NOTE: Unless explicitly prohibited in a section, you may permit ICMP for connectivity testing

NOTE: Any reference to a password that is not defined should use "ipexpert"

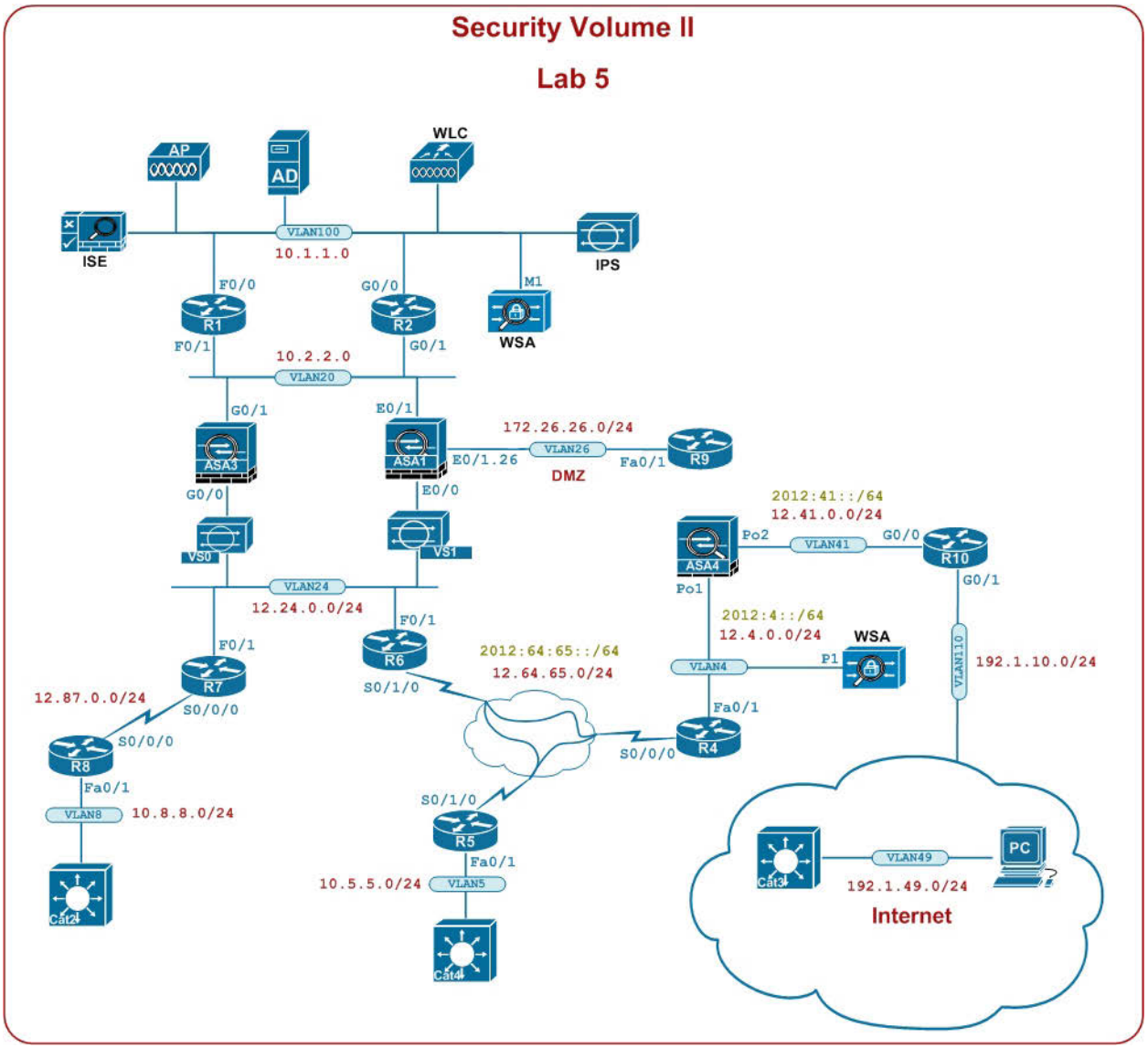
Estimated Time to Complete: **12 Hours**

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
R1	FastEthernet0/0	100	10.1.1.1/24
	FastEthernet0/1	20	10.2.2.1/24
	Loopback0		1.1.1.1/32
R2	GigabitEthernet0/0	10	10.1.1.2/24
	GigabitEthernet0/1	20	10.2.2.2/24
	Loopback0		2.2.2.2/32
R4	FastEthernet0/1	4	12.4.0.4/24 2012:4::4/64
	Serial0/0/0		12.64.65.4/24 2012:64:65::4/64
	Loopback0		4.4.4.4/32
R5	Serial0/1/0		12.64.65.5/24 2012:64:65::5/64
	FastEthernet0/1	5	10.5.5.5/24
	Loopback0		5.5.5.5
R6	FastEthernet0/1	24	12.24.0.6/24
	Serial0/1/0		12.64.65.6/24 2012:64:65::6/64
	Loopback0		6.6.6.6/32
R7	FastEthernet0/1	24	12.24.0.7/24
	Serial0/0		12.87.0.7/24
	Loopback0		7.7.7.7/24
R8	FastEthernet0/1	8	10.8.8.8/24
	Serial0/0		12.87.0.8/24
	Loopback0		8.8.8.8/32

R9	FastEthernet0/1	26	172.26.26.9/24
	Loopback0		9.9.9.9/32
R10	G0/0 G0/1	41 110	12.41.0.10/24 2012:41::10/64 192.1.10.10/24
ASA1	Ethernet0/0 - outside	24	12.24.0.10/24
	Ethernet0/1 - inside	20	10.2.2.10/24
	Ethernet0/1.26 – DMZ(sec 50)	26	172.26.26.10/24
ASA3	G0/0 - outside	24	12.24.0.30/24
	G0/1 - inside	20	10.2.2.30/24
ASA4	Po1 - inside Po2 - outside	4 41	12.4.0.40/24 2012:4::40/64 12.41.0.40/24 2012:41::40/64
Cat2	FastEthernet0/22 (DHCP)	8	10.8.8.120/24
Cat3	FastEthernet0/23	4	192.1.49.130/24
Cat4	VLAN5	5	10.5.5.140/24
ISE	Student NIC	100	10.1.1.150/24
AD	Student NIC	100	10.1.1.101/24
IPS	Mgmt	100	10.1.1.15/24
WSA	M1 P1	100 4	10.1.1.180/24 12.4.0.180/24
WLC	Port1 (G0/0)	100	10.1.1.250/24



Solutions

1.0 ASA Firewalls (21 points)

Task 1.1: ASA Basic Configuration (2 Points)

- Configure ASA1 and ASA3 IP addressing according to the lab diagram and Lab 2 Addressing Table
- Modify any of the switches necessary to ensure that you can ping all of the directly connected devices from both ASA1 and ASA3
- You may allow ICMP for testing through the ASAs

Detailed Solution

ASA1

```
hostname ASA1

interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 12.24.0.10 255.255.255.0
 no sh

interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.10 255.255.255.0
 no sh

interface Ethernet0/1.26
 vlan 26
 nameif DMZ
 security-level 50
 ip address 172.26.26.10 255.255.255.0
 no sh
```

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

ASA3

```
hostname ASA3

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 12.24.0.30 255.255.255.0
 no sh

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.30 255.255.255.0
 no sh

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

CAT3

```
int g1/0/7
 sw tru nat vlan 20
```

This task is not difficult, however it is important to watch the configuration of the switches. Since the switches were no configured properly, or just weren't finished, you have to make some modifications there. Also, if the VLANs for the outside interface of the ASAs are left to vlan 24 the pings will work, but you'll need to verify this again after you configure the the virtual sensors.

Verification

```
ASA1(config)# ping 10.2.2.30
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.2.2.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1(config)# ping 172.26.26.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.26.26.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3(config)# ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA3(config)# ping 12.24.0.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.24.0.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Task 1.2: ASA4 Setup (3 Points)

- Configure ASA4 according to the IP addressing table and directions below
- Interfaces G0/0 and G0/1 should be bundled into a single logical link
- Interfaces G0/2 and G0/3 should form another logical link
- This configuration should provide fault tolerance and traffic load-balancing capabilities
- ASA's first bundle should load-balance traffic according to source & destination port numbers
- CAT4 should load-balance based on source IP address
- Don't use any negotiation protocol to accomplish this task
- Enable inspection of ICMP traffic

Detailed Solution

CAT4

```
int range g1/0/19 – 20
 sw host
 sw acc vlan 4
 channel-group 1 mode on

int range g1/0/21 – 22
 sw host
 sw acc vlan 41
 channel-group 1 mode on

port-channel load-balance src-ip
```

ASA4

```
hostname ASA4

interface GigabitEthernet0/0
 channel-group 1 mode on
 no sh
interface GigabitEthernet0/1
 channel-group 1 mode on
 no sh
interface GigabitEthernet0/2
 channel-group 2 mode on
 speed 1000
 no sh
interface GigabitEthernet0/3
 channel-group 2 mode on
 speed 1000
 no sh

interface Port-channel1
 port-channel load-balance src-dst-port
 nameif inside
 security-level 100
 ip address 12.4.0.40 255.255.255.0
 ipv6 address 2012:4::40/64
```

```
interface Port-channel2
 nameif outside
 security-level 0
 ip address 12.41.0.40 255.255.255.0
 ipv6 address 2012:41::40/64

fixup protocol icmp
```

A good practice when dealing with EtherChannels is to first shutdown the ports you will be configuring. Then once all the configuration is in place you can try to bring up the interfaces in about the same time on both sides.

Verification

```
CAT4#sh etherchannel summary  | be Group
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
------
1      Po1(SU)          -        Gi1/0/19(P) Gi1/0/20(P)
2      Po2(SU)          -        Gi1/0/21(P) Gi1/0/22(P)

ASA4(config)# sh port-channel 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: 2
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
------
1      Po1(U)             -      Gi0/0(P)   Gi0/1(P)
2      Po2(U)             -      Gi0/2(P)   Gi0/3(P)

ASA4(config)# sh port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-port
```

```
EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination TCP/UDP (layer-4) port number
  IPv6: Source XOR Destination TCP/UDP (layer-4) port number


CAT4#test ether load-balance interface port-channel 1 ip 12.64.65.4
12.4.0.40
Would select Gi1/0/19 of Po1

CAT4#test ether load-balance interface port-channel 1 ip 12.64.65.5
12.4.0.40
Would select Gi1/0/20 of Po1

ASA4(config)# ping 12.4.0.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.4.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA4(config)# ping 12.41.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.41.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA4(config-if)# ping 2012:41::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2012:41::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA4(config-if)# ping 2012:4::4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2012:4::4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Task 1.3: ASA Routing (5 Points)

- Configure OSPF on ASA1 and ASA3
- ASA3 should be the primary route out of the internal network
- ASA1 should be the secondary route out of the network
- Inject a default route into the internal network
- Do not pass internal routes to R7 and R6
- Make sure that the routing updates are secured using the most secure method available
- Advertise the DMZ network into the inside network but not the outside
- Configure EIGRP on ASA4
- Secure routing protocol updates
- Configure R4 so OSPF and EIGRP domains can communicate with each other
- Ensure the firewall has full IPv6 reachability – you can add a single static route

Detailed Solution

ASA1

```
router ospf 1
 network 10.2.2.0 255.255.255.0 area 0
 network 172.26.26.0 255.255.255.0 area 0
 default-information originate always metric 20

router ospf 2
 network 12.24.0.0 255.255.255.0 area 0

interface Ethernet0/0
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest

interface Ethernet0/1
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest
```

ASA3

```
router ospf 1
 network 10.2.2.0 255.255.255.0 area 0
```

```
 redistribute ospf 2 subnets
 default-information originate always metric 10

router ospf 2
 network 12.24.0.0 255.255.0.0 area 0

interface G0/0
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest

interface G0/1
 ospf message-digest-key 1 md5 ipexpert
 ospf authentication message-digest
```

ASA4

```
router eigrp 4
 no auto-summary
 network 12.4.0.40 255.255.255.255
 network 12.41.0.40 255.255.255.255

interface port-channel 1
 authentication key eigrp 4 ipexpert key-id 1
 authentication mode eigrp 4 md5

interface port-channel 2
 authentication key eigrp 4 ipexpert key-id 1
 authentication mode eigrp 4 md5

ipv route inside 2012:64:65::/64 2012:4::4
```

R1, R6, R7

```
interface FastEthernet0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert
```

R2

```
interface GigabitEthernet0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ipexpert
```

R4

```
key chain EIGRP
 key 1
  key-string ipexpert

int F0/1
 ip authentication key-chain eigrp 4 EIGRP
 ip authentication mode eigrp 4 md5

router eigrp 4
 redistribute ospf 1 metric 1 1 1 1 1

router ospf 1
 redistribute eigrp 4 subnets
```

R10

```
key chain EIGRP
 key 1
  key-string ipexpert

int g0/0
 ip authentication key-chain eigrp 4 EIGRP
 ip authentication mode eigrp 4 md5
```

Even that both ASAs advertise a default route only ASA3 will be preferred due to a lower metric.

Almost all authentication settings are configured under the interfaces.

Verification

```
ASA3(config)# sh ospf ne

Neighbor ID     Pri   State           Dead Time   Address
Interface
6.6.6.6           1   FULL/BDR        0:00:32     12.24.0.6       outside
12.24.0.10        1   FULL/DR         0:00:36     12.24.0.10      outside
7.7.7.7           1   2WAY/DROTHER    0:00:37     12.24.0.7       outside
2.2.2.2           1   2WAY/DROTHER    0:00:38     10.2.2.2        inside
1.1.1.1           1   FULL/BDR        0:00:33     10.2.2.1        inside
172.26.26.10      1   FULL/DR         0:00:34     10.2.2.10       inside

ASA4(config)# sh ei ne
EIGRP-IPv4 neighbors for process 4
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
1   12.41.0.10              Po2              10  00:15:27 86   516   0   7
0   12.4.0.4                Po1              14  00:15:36 1    200   0   8


R1#sh ip ro os | be Gate
Gateway of last resort is 10.2.2.30 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/10] via 10.2.2.30, 00:20:57, FastEthernet0/1
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 10.2.2.2, 19:53:17, FastEthernet0/1
                 [110/2] via 10.1.1.2, 19:53:17, FastEthernet0/0
      4.0.0.0/32 is subnetted, 1 subnets
O E2     4.4.4.4 [110/75] via 10.2.2.30, 00:00:24, FastEthernet0/1
      5.0.0.0/32 is subnetted, 1 subnets
O E2     5.5.5.5 [110/75] via 10.2.2.30, 00:00:24, FastEthernet0/1
      6.0.0.0/24 is subnetted, 1 subnets
O E2     6.6.6.0 [110/20] via 10.2.2.30, 00:00:24, FastEthernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
O E2     7.7.7.0 [110/20] via 10.2.2.30, 00:00:24, FastEthernet0/1
      8.0.0.0/24 is subnetted, 1 subnets
O E2     8.8.8.0 [110/20] via 10.2.2.30, 00:00:24, FastEthernet0/1
      12.0.0.0/24 is subnetted, 5 subnets
```

```
O E2     12.4.0.0 [110/20] via 10.2.2.30, 00:00:24, FastEthernet0/1
O E2     12.24.0.0 [110/10] via 10.2.2.30, 00:00:24, FastEthernet0/1
O E2     12.41.0.0 [110/20] via 10.2.2.30, 00:00:24, FastEthernet0/1
O E2     12.64.65.0 [110/74] via 10.2.2.30, 00:00:24, FastEthernet0/1
O E2     12.87.0.0 [110/74] via 10.2.2.30, 00:00:24, FastEthernet0/1
      172.26.0.0/24 is subnetted, 1 subnets
O        172.26.26.0 [110/11] via 10.2.2.10, 00:25:14, FastEthernet0/1
O E2  192.1.10.0/24 [110/20] via 10.2.2.30, 00:00:24, FastEthernet0/1

ASA1(config)# sh route | be Gate
Gateway of last resort is not set

O    1.1.1.1 255.255.255.255 [110/11] via 10.2.2.1, 0:17:08, inside
O    2.2.2.2 255.255.255.255 [110/11] via 10.2.2.2, 0:17:08, inside
O IA 4.4.4.4 255.255.255.255 [110/75] via 12.24.0.6, 0:16:32, outside
O IA 5.5.5.5 255.255.255.255 [110/75] via 12.24.0.6, 0:16:32, outside
O E2 6.6.6.0 255.255.255.0 [110/20] via 12.24.0.6, 0:07:15, outside
O E2 192.1.10.0 255.255.255.0 [110/20] via 12.24.0.6, 0:07:15, outside
C    172.26.26.0 255.255.255.0 is directly connected, DMZ
O E2 7.7.7.0 255.255.255.0 [110/20] via 12.24.0.7, 0:07:15, outside
O E2 8.8.8.0 255.255.255.0 [110/20] via 12.24.0.7, 0:07:15, outside
O    10.1.1.0 255.255.255.0 [110/11] via 10.2.2.2, 0:17:08, inside
                            [110/11] via 10.2.2.1, 0:17:08, inside
C    10.2.2.0 255.255.255.0 is directly connected, inside
O E2 12.4.0.0 255.255.255.0 [110/20] via 12.24.0.6, 0:07:15, outside
O IA 12.64.65.0 255.255.255.0 [110/74] via 12.24.0.6, 0:16:32, outside
C    12.24.0.0 255.255.255.0 is directly connected, outside
O E2 12.41.0.0 255.255.255.0 [110/20] via 12.24.0.6, 0:07:15, outside
O IA 12.87.0.0 255.255.255.0 [110/74] via 12.24.0.7, 0:16:32, outside

ASA4(config)# sh route | be Gate
Gateway of last resort is not set

D EX 4.4.4.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21, inside
D EX 5.5.5.5 255.255.255.255 [170/2560000512] via 12.4.0.4, 0:06:21,
inside
D EX 6.6.6.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21, inside
D    192.1.10.0 255.255.255.0 [90/3072] via 12.41.0.10, 0:07:38, outside
D EX 7.7.7.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21, inside
D EX 8.8.8.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21, inside
```

```
C    12.4.0.0 255.255.255.0 is directly connected, inside
D EX 12.64.65.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21,
inside
D EX 12.24.0.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21,
inside
C    12.41.0.0 255.255.255.0 is directly connected, outside
D EX 12.87.0.0 255.255.255.0 [170/2560000512] via 12.4.0.4, 0:06:21,
inside

R4#ping 2012:41::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2012:41::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

ASA4(config)#  ping 12.24.0.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.24.0.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/18/20 ms

ASA3(config)# ping 192.1.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/18/20 ms
```

Task 1.4: Advanced ACLs and NAT (4 Points)

- In the near future your company will be installing a new server located at 10.1.1.160.
- The Server will only support SSH and HTTP
- Ensure that this server is seen as 12.24.0.160 for SSH and traverses ASA3
- For HTTP ensure that this server appears to be 12.24.0.60 and traverses ASA1
- Configure HTTP access to the loopback of R9. This address should be translated to 12.24.0.9
- Allow telnet into R9's f0/1 interface. This should also appear to be 12.24.0.9
- There are additional servers that will be accessed by organizations from the Internet (192.1.49.0/24). The IP Addresses of these servers are as follows :
  - 172.26.26.80
  - 172.26.26.22
  - 172.26.26.25
  - 172.26.26.161
  - 172.26.26.110
- The last octet of the server is also the service that should be allowed to it. Do this with one ACL statement to the outside interface on the ASA. Allow connections from "any" source address. Do this by adding only a single line to the outside ACL
- You may add 1 static route to complete this task

Detailed Solution

ASA1

```
static (DMZ,out) tcp 12.24.0.9 telnet 172.26.26.9 telnet
static (DMZ,out) tcp 12.24.0.9 www 9.9.9.9 www
static (DMZ,out) tcp interface www 172.26.26.80 www
static (DMZ,out) tcp interface ssh 172.26.26.22 ssh
static (DMZ,out) tcp interface smtp 172.26.26.25 smtp
static (DMZ,out) tcp interface pop3 172.26.26.110 pop3
static (DMZ,out) udp interface snmp 172.26.26.161 snmp
static (inside,out) 12.24.0.60 10.1.1.160

nat (out) 1 0.0.0.0 0.0.0.0 outside
global (inside) 1 interface
global (DMZ) 1 interface
```

```
object-group service PARTNER_SERVICES
 service-object tcp eq www
 service-object tcp eq ssh
 service-object tcp eq smtp
 service-object tcp eq pop3
 service-object udp eq snmp

access-list OUTSIDE_IN permit tcp any host 12.24.0.60 eq www
access-list OUTSIDE_IN permit tcp any host 12.24.0.9 eq telnet
access-list OUTSIDE_IN permit tcp any host 12.24.0.9 eq www
access-list OUTSIDE_IN perm object-gr PARTNER_SERVICES any interface
outside

access-list DMZ_IN permit icmp any any
access-group DMZ_IN in int DMZ

route DMZ 9.9.9.9 255.255.255.255 172.26.26.9
```

ASA3

```
object network SERVER
 host 10.1.1.160
 nat (inside,outside) static 12.24.0.160

access-list OUTSIDE_IN extended permit tcp any object SERVER eq ssh
```

This task is an interesting one because there are two ASAs involved. The default route points back to ASA3 (same as the more specific routes) so outside NAT is required to "pull in" all return traffic for ASA1. When you do the outside NAT it would be really easy to forget about the DMZ interface which will fail if you don't have a global for it.

Another thing this task clearly demonstrates is a difference between addresses being added to the interface ACLs when address translation is involved. In 8.2 and earlier you call out the translated address versus in 8.3+ it is real IP. This is why with Auto-NAT you can simply add object to the ACL and not the individual IP address.

Verification

In the real lab what you could do is to configure an SVI in VLAN 100 with IP address 10.1.1.160 on one of the switches. Then you could see the traffic actually hits the service – in the verification below I just focus on ACL counters :

```
R6#telnet 12.24.0.160 22
Trying 12.24.0.160, 22 ...
% Connection timed out; remote host not responding

R6#telnet 12.24.0.60 80
Trying 12.24.0.60, 80 ...
% Connection timed out; remote host not responding

ASA1(config)# sh access-l | in www
access-list OUTSIDE_IN line 2 permit tcp any host 12.24.0.60 eq www
(hitcnt=2) 0xaa0a7436
access-list OUTSIDE_IN line 4 extended permit tcp any host 12.24.0.9 eq
www (hitcnt=0) 0x9feba83a
  access-list OUTSIDE_IN line 5 extended permit tcp any interface outside
eq www (hitcnt=0) 0x7c40f258

ASA3(config)# sh access-l | in ssh
access-list OUTSIDE_IN line 2 extended permit tcp any object SERVER eq ssh
(hitcnt=0) 0x3f7ec66a
  access-list OUTSIDE_IN line 2 extended permit tcp any host 10.1.1.160 eq
ssh (hitcnt=1) 0x3f7ec66a
```

Now telnet from R6 on ports 23 and 80 to 12.24.0.9. Then test access to the DMZ servers; again look at the counters :

```
R9#sh tcp br
TCB        Local Address               Foreign Address             (state)
484AD6D4   9.9.9.9.80                  172.26.26.10.43496          ESTAB
49665158   172.26.26.9.23              172.26.26.10.4145           ESTAB


ASA1(config)# sh access-l | be PARTNER
access-list OUTSIDE_IN line 5 extended permit object-group
PARTNER_SERVICES any interface outside 0xa262d831
  access-list OUTSIDE_IN line 5 extended permit tcp any interface outside
eq www (hitcnt=1) 0x7c40f258
```

```
  access-list OUTSIDE_IN line 5 extended permit tcp any interface outside
eq ssh (hitcnt=1) 0x40dc2035
  access-list OUTSIDE_IN line 5 extended permit tcp any interface outside
eq smtp (hitcnt=1) 0x78037910
  access-list OUTSIDE_IN line 5 extended permit tcp any interface outside
eq pop3 (hitcnt=0) 0x1192dbbd
  access-list OUTSIDE_IN line 5 extended permit udp any interface outside
eq snmp (hitcnt=0) 0x42f47fd7

ASA1(config)# sh nat DMZ outside
  match tcp DMZ host 172.26.26.9 eq 23 outside any
    static translation to 12.24.0.9/23
    translate_hits = 0, untranslate_hits = 3
  match tcp DMZ host 9.9.9.9 eq 80 outside any
    static translation to 12.24.0.9/80
    translate_hits = 0, untranslate_hits = 1
  match tcp DMZ host 172.26.26.80 eq 80 outside any
    static translation to 12.24.0.10/80
    translate_hits = 0, untranslate_hits = 1
  match tcp DMZ host 172.26.26.22 eq 22 outside any
    static translation to 12.24.0.10/22
    translate_hits = 0, untranslate_hits = 1
  match tcp DMZ host 172.26.26.25 eq 25 outside any
    static translation to 12.24.0.10/25
    translate_hits = 0, untranslate_hits = 1
  match tcp DMZ host 172.26.26.110 eq 110 outside any
    static translation to 12.24.0.10/110
    translate_hits = 0, untranslate_hits = 0
  match udp DMZ host 172.26.26.161 eq 161 outside any
    static translation to 12.24.0.10/161
    translate_hits = 0, untranslate_hits = 0
```

Task 1.5: ASA MPF (4 Points)

- Internal users should use ASA3 to get to the Internet
- They should be translated to the address pool rage 12.24.0.112-126
- Ensure that you do not stop allocating addresses if the pool is saturated
- Make sure that they cannot access www.juniper.com, www.myspace.com, and www.facebook.com during business hours
- Business hours are Monday through Friday from 8 am to 5pm and Saturday from 9 am to 2 pm
- The policy should only apply to the inside interface.
- You can use Test PC for verification of this task. Create host entries to these three websites pointing to R7 Loopback0. When completed http://7.7.7.7 should work but http://www.juniper.com and the others should be unsuccessful

Detailed Solution

ASA3

```
object network NATPOOL
 range 12.24.0.112 12.24.0.125
object network PATIP
 host 12.24.0.126

object network INSIDE_10-1-1-0_24
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic NATPOOL
object network PAT_10-1-1-0_24
 subnet 10.1.1.0 255.255.255.0
 nat (inside,outside) dynamic pat-pool PATIP

regex domainslist1 "www\.myspace\.com"
regex domainslist2 "www\.juniper\.com"
regex domainslist3 "www\.facebook\.com"

time-range WEBTIME
 periodic weekdays 8:00 to 17:00
 periodic weekend 9:00 to 14:00

access-list webfilter permit tcp any any eq www time-range WEBTIME
```

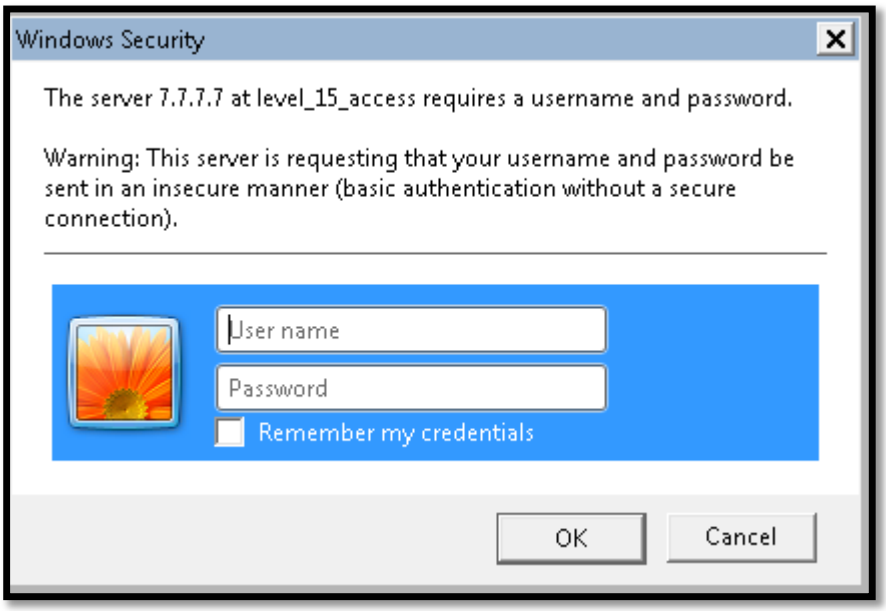
```
class-map type regex match-any DomainBlockList
 match regex domainslist1
 match regex domainslist2
 match regex domainslist3

class-map type inspect http match-all BlockDomainsClass
 match request header host regex class DomainBlockList

class-map HTTP
 match access-list webfilter

policy-map type inspect http WEBPOL
 parameters
 class BlockDomainsClass
  drop-connection log

policy-map IN_POL
 class HTTP
  inspect http WEBPOL

service-policy IN_POL interface inside
```

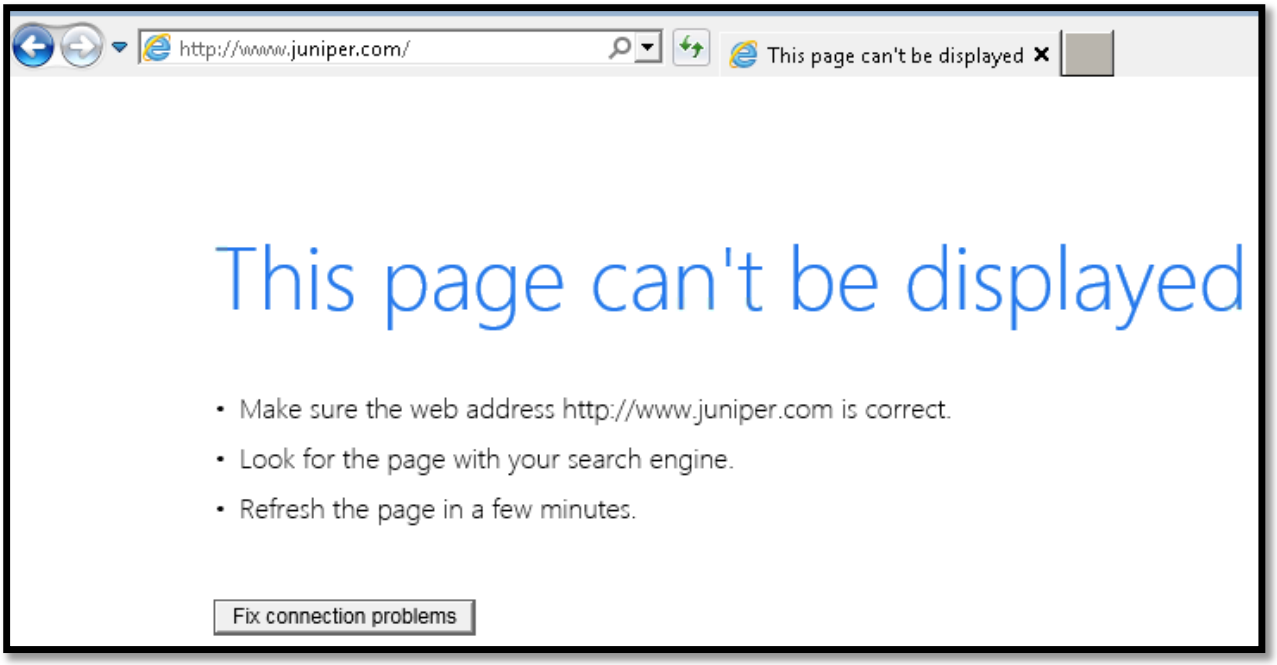
We have previously redistributed OSPF 2 into internal domain on ASA3 so it will be always preferred to reach the "Internet".

Verification

```
ASA3(config)# sh nat det

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static SERVER 12.24.0.160
    translate_hits = 0, untranslate_hits = 1
    Source - Origin: 10.1.1.160/32, Translated: 12.24.0.160/32
2 (inside) to (outside) source dynamic INSIDE_10-1-1-0_24 NATPOOL
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 12.24.0.112-12.24.0.125
3 (inside) to (outside) source dynamic PAT_10-1-1-0_24 pat-pool PATIP
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated (PAT): 12.24.0.126/32
```

```
ASA3(config)# sh x
2 in use, 9 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T -
twice
NAT from inside:10.1.1.160 to outside:12.24.0.160
    flags s idle 1:02:08 timeout 0:00:00
NAT from inside:10.1.1.200 to outside:12.24.0.121 flags i idle 0:00:16
timeout 3:00:00
```






```
ASA3(config)# %ASA-4-507003: tcp flow from inside:10.1.1.200/62101 to
outside:7.7.7.7/80 terminated by inspection engine, reason - disconnected,
dropped packet.
%ASA-4-507003: tcp flow from inside:10.1.1.200/62104 to outside:7.7.7.7/80
terminated by inspection engine, reason - disconnected, dropped packet.
```

```
ASA3(config)# sh service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default

Interface inside:
  Service-policy: IN_POL
    Class-map: HTTP
      Inspect: http WEBPOL, packet 54, lock fail 0, drop 7, reset-drop 0
        protocol violations
          packet 0
        class BlockDomainsClass
          drop-connection log, packet 7
```

Now change the time to be outside the configured range and re-test :

```
ASA3(config)# sh clo
18:03:21.953 UTC Mon Jun 3 2013
```

Task 1.6: Advanced ASA Configuration (3 Points)

- Rate Limit all ICMP traffic to the ISE server via ASA3 (NAT ISE to 12.24.0.150)
- Traffic exceeding 8000 BPS should be dropped
- Configure Secure Logging to the ISE Server on ASA1. Make sure that traffic flows if the Syslog server is down and ensure timestamps are sent
- Deny ICMP Echo Requests on the outside interface of ASA3. The ASA should still be able to ping and traceroute

Detailed Solution

ISE

```
ip route 12.0.0.0 255.0.0.0 gateway 10.1.1.1
ip route 10.2.2.0 255.255.255.0 gateway 10.1.1.1
```

ASA1

```
logging enable
logging timestamp
logging trap debugging
logging host inside 10.1.1.150 TCP/1470 secure
logging permit-hostdown
```

ASA3

```
object network ISE
 host 10.1.1.150
 nat (inside,outside) static 12.24.0.150

access-list RATELIMIT permit icmp any host 10.1.1.150

class-map POLICE_ISE_CLASS
 match access-list RATELIMIT

policy-map IN_POL
 class POLICE_ISE_CLASS
  police output 8000

icmp permit any echo-reply outside
icmp permit any unreachable outside
icmp permit any time-exceeded outside
```

Even ISE does not collect Syslog packets traffic will be still allowed through the ASA thanks to the “permit-hostdown” option.

Verification

```
ASA3(config)# traceroute 12.64.65.4

Type escape sequence to abort.
Tracing the route to 12.64.65.4

 1  12.24.0.6 0 msec 0 msec 0 msec
 2  12.64.65.4 10 msec *  0 msec
```

```
R6#ping 12.24.0.30 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 12.24.0.30, timeout is 2 seconds:
.
Success rate is 0 percent (0/1
%ASA-3-313001: Denied ICMP type=8, code=0 from 12.24.0.6 on interface
outside

R6#ping 12.24.0.150 rep 10 size 800

Type escape sequence to abort.
Sending 10, 800-byte ICMP Echos to 12.24.0.150, timeout is 2 seconds:
!!!.!!.!!!
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/2/4 ms

ASA1(config)# sh loggi setting
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: level warnings, 3 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level debugging, facility 20, 12 messages logged
        Logging to inside 10.1.1.150 tcp/1470 SECURE retry: Attempt 1
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

2.0 IOS Firewall (8 points)

Task 2.1: Cisco IP Session Filtering (3 Points)

- Configure R8 for firewall services
- You may not use CBAC or IOS Zone Based Firewall technologies in this task
- Watch all TCP, ICMP and UDP traffic from the private network to the public network and allow for its return
- Make sure that all networks in the topology cannot see the real addresses of vlan 8

Detailed Solution

R8

```
interface FastEthernet0/1
 ip nat inside

interface Serial0/0/0
 ip access-group BLOCK_IN in
 ip access-group REFLECT out
 ip nat outside

ip access-list extended TO_NAT
 permit ip 10.8.8.0 0.0.0.255 any

ip nat inside source list TO_NAT interface Serial0/0/0 overload

ip access-list extended BLOCK_IN
 evaluate MIRROR
 permit ospf host 12.87.0.7 host 12.87.0.8
 permit ospf host 12.87.0.7 host 224.0.0.5
 permit icmp any any
 100 deny   ip any any log

ip access-list extended REFLECT
 permit tcp any any reflect MIRROR
 permit udp any any reflect MIRROR
```

```
 permit icmp any any reflect MIRROR
 100 deny   ip any any log
```

There is not much that can go wrong here. You have to use Reflexive ACLs and NAT on R8 and about the only thing that I would watch for is that you don't forget about OSPF.

Verification

```
CAT2#traceroute 12.64.65.4

Type escape sequence to abort.
Tracing the route to 12.64.65.4

  1 10.8.8.8 0 msec 9 msec 0 msec
  2 12.87.0.7 0 msec 0 msec 8 msec
  3 12.24.0.6 0 msec 0 msec 9 msec
  4 12.64.65.4 8 msec 9 msec *

CAT2#ping 12.24.0.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.24.0.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/16 ms

CAT2#telnet 12.64.65.5
Trying 12.64.65.5 ... Open


Password required, but none set

R8#sh access-l
Extended IP access list BLOCK_IN
    10 evaluate MIRROR
    20 permit ospf host 12.87.0.7 host 12.87.0.8
    30 permit ospf host 12.87.0.7 host 224.0.0.5 (46 matches)
    40 permit icmp any any (8 matches)
    100 deny ip any any log
Reflexive IP access list MIRROR
```

```
     permit udp host 12.64.65.4 eq 33445 host 12.87.0.8 eq 39303 (1 match)
(time left 229)
     permit udp host 12.64.65.4 eq 33444 host 12.87.0.8 eq 41730 (1 match)
(time left 229)
     permit udp host 12.64.65.4 eq 33443 host 12.87.0.8 eq 41392 (1 match)
(time left 220)
     permit udp host 12.64.65.4 eq 33442 host 12.87.0.8 eq 34803 (1 match)
(time left 220)
     permit udp host 12.64.65.4 eq 33441 host 12.87.0.8 eq 35597 (1 match)
(time left 220)
     permit udp host 12.64.65.4 eq 33440 host 12.87.0.8 eq 41630 (1 match)
(time left 211)
     permit udp host 12.64.65.4 eq 33439 host 12.87.0.8 eq 36694 (1 match)
(time left 211)
     permit udp host 12.64.65.4 eq 33438 host 12.87.0.8 eq 41935 (1 match)
(time left 211)
     permit udp host 12.64.65.4 eq 33437 host 12.87.0.8 eq 37747 (1 match)
(time left 202)
     permit tcp host 12.24.0.5 eq telnet host 12.87.0.8 eq 51704 (4
matches) (time left 166)
     permit icmp host 12.24.0.6 host 12.87.0.8  (18 matches) (time left
168)
Extended IP access list REFLECT
    10 permit tcp any any reflect MIRROR (14 matches)
    20 permit udp any any reflect MIRROR (9 matches)
    30 permit icmp any any reflect MIRROR (9 matches)
    100 deny ip any any log
Extended IP access list TO_NAT
    10 permit ip 10.8.8.0 0.0.0.255 any (13 matches)
Extended IP access list loops
    10 permit ip 8.0.0.0 0.255.255.255 any (2 matches)
```

Task 2.2: Cisco IOS Firewall (5 Points)

- It's been decided that R4 will be configured as an additional line of defense against outside attacks. Configure the Firewall with the following parameters :
  - Fa0/1 is the outside zone
  - S0/0/0 is the inside zone
  - Allow all pertinent traffic from the outside to the inside zone
  - Inspect TCP and UDP out of the network
  - Pass and Log all ICMP
  - Log dropped packets
- Internal server 10.1.1.160 is running an ERP application on TCP port 51000. Make sure this is allowed and inspected as a custom application
- Ensure that TCP half-open sessions on your internal devices are aggressively dropped if they reach a total of 800 connections and that aggressive dropping stops when the number of connections falls below 400. Do this within a 1 minute period also
- All TCP-based sessions initiated from the outside should be session-logged

Detailed Solution

ASA3

```
access-list OUTSIDE_IN per tcp any object SERVER eq 51000
```

ASA4

```
object-group service DMZ_PORTS
 service-object tcp destination eq www
 service-object tcp destination eq ssh
 service-object tcp destination eq smtp
 service-object tcp destination eq pop3
 service-object udp destination eq snmp

access-list OUTSIDE_IN extended permit tcp any host 12.24.0.160 eq 51000
access-list OUTSIDE_IN permit object-group DMZ_PORTS any host 12.24.0.10
access-list OUTSIDE_IN extended permit tcp any host 12.24.0.9 eq telnet
access-list OUTSIDE_IN per icmp any any

access-group OUTSIDE_IN in interface outside
```

R4

```
parameter-map type inspect global
 log dropped-packets enable

ip port-map user-CUSTOM-ERP port tcp 51000

parameter-map type inspect TCP_IN_PARAMS
 audit-trail on
 max-incomplete low  400
 max-incomplete high 800
 one-minute low 400
 one-minute high 800

class-map type inspect match-all ZFW_ICMP_CLASS
 match protocol icmp

class-map type inspect match-any ZFW_TCP_UDP_OUT_CLASS
 match protocol tcp
 match protocol udp

class-map type inspect match-any ZFW_TCP_PROTO_IN_CLASS
 match protocol ssh
 match protocol telnet
 match protocol smtp
 match protocol http
 match protocol pop3

class-map type inspect match-any ZFW_UDP_PROTO_IN_CLASS
 match protocol snmp

class-map type inspect match-any ZFW_CUST_CLASS
 match protocol user-CUSTOM-ERP

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ZFW_CUST_CLASS
  inspect TCP_IN_PARAMS
 class type inspect ZFW_TCP_PROTO_IN_CLASS
  inspect TCP_IN_PARAMS
 class type ZFW_UDP_PROTO_IN_CLASS
  inspect
```

```
 class type inspect ZFW_ICMP_CLASS
  pass log
 class class-default
  drop log

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_TCP_UDP_OUT_CLASS
  inspect
 class type inspect ZFW_ICMP_CLASS
  pass log
 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
zone-pair security OUTIN source OUT destination IN
 service-policy type inspect ZFW_OUTIN_POL

interface FastEthernet0/1
 zone-member security OUT
interface Serial0/0/0
 zone-member security IN
```

Keep track on what addresses should be added to the ACL where (real vs. translated). Here since we're "in front" of the servers that were already NATed we play with translated addresses.

Verification

```
CAT3#telnet 12.24.0.9 23
Trying 12.24.0.9 ... Open

R9>

CAT3#telnet 12.24.0.160 51000
Trying 12.24.0.160, 51000 ...
```

```
% Connection reset by user

R4#sh policy-firewall session
      Half-open Sessions = 1
        Session 49EE22A0 (192.1.49.130:12441)=>(12.24.0.160:51000) user-
CUSTOM-ERP:tcp SIS_OPENING/TCP_SYNSENT
          Created 00:00:24, Last heard 00:00:24
          Bytes sent (initiator:responder) [0:0]

CAT3#telnet 12.24.0.10 110
Trying 12.24.0.10, 110 ...
% Connection reset by user

CAT3#telnet 12.24.0.10 22
Trying 12.24.0.10, 22 ...
% Connection reset by user

ASA4(config)# sh access-l | ex hitcnt=0
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTSIDE_IN; 8 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit tcp any host 12.24.0.160 eq
51000 (hitcnt=1) 0x2a12a81b
access-list OUTSIDE_IN line 2 extended permit object-group DMZ_PORTS any
host 12.24.0.10 (hitcnt=2) 0x53c0b5ed
  access-list OUTSIDE_IN line 2 extended permit tcp any host 12.24.0.10 eq
ssh (hitcnt=1) 0xb6560781
  access-list OUTSIDE_IN line 2 extended permit tcp any host 12.24.0.10 eq
pop3 (hitcnt=1) 0xcb8f9cb7
access-list OUTSIDE_IN line 3 extended permit tcp any host 12.24.0.9 eq
telnet (hitcnt=1) 0x78daf723



R4(config)#

*Jun  3 21:27:18.662: %FW-6-SESS_AUDIT_TRAIL: (target:class)-
(OUTIN:ZFW_TCP_PROTO_IN_CLASS):Stop telnet session: initiator
(192.1.49.130:18460) sent 36 bytes -- responder (12.24.0.9:23) sent 44
bytes
```

```
*Jun  3 21:27:49.758: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-
(OUTIN:ZFW_TCP_PROTO_IN_CLASS):Start pop3 session: initiator
(192.1.49.130:40715) -- responder (12.24.0.10:110)

*Jun  3 21:27:53.274: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-
(OUTIN:ZFW_TCP_PROTO_IN_CLASS):Start ssh session: initiator
(192.1.49.130:17634) -- responder (12.24.0.10:22)

CAT3#ping 12.24.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.24.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/21/25 ms

R4#
*Jun  3 21:30:31.746: %FW-6-PASS_PKT: (target:class)-
(OUTIN:ZFW_ICMP_CLASS) Passing icmp pkt 192.1.49.130:0 => 12.24.0.10:0
with ip ident 0

R5#telnet 192.1.49.130
Trying 192.1.49.130 ... Open


User Access Verification

Password:

R4#sh policy-firewall ses
      Established Sessions = 1
        Session 49EE29A0 (12.64.65.5:40454)=>(192.1.49.130:23) tcp
SIS_OPEN/TCP_ESTAB
          Created 00:00:08, Last heard 00:00:08
          Bytes sent (initiator:responder) [33:63]


R4#sh policy-firewall config all
Zone: self
  Description: System defined zone

Zone: IN
  Member Interfaces:
    Serial0/0/0
```

```
Zone: OUT
  Member Interfaces:
    FastEthernet0/1

Zone-pair              : INOUT
Source Zone            : IN
Destination Zone       : OUT
Service-policy inspect : ZFW_INOUT_POL
  Class-map : ZFW_TCP_UDP_OUT_CLASS(match-any)
   Match protocol tcp
   Match protocol udp
  Action : inspect
   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              : OUTIN
Source Zone            : OUT
Destination Zone       : IN
Service-policy inspect : ZFW_OUTIN_POL
  Class-map : ZFW_CUST_CLASS(match-any)
   Match protocol user-CUSTOM-ERP
  Action : inspect
   Parameter-map : TCP_IN_PARAMS

  Class-map : ZFW_TCP_PROTO_IN_CLASS(match-any)
   Match protocol ssh
   Match protocol telnet
   Match protocol smtp
   Match protocol http
   Match protocol pop3
```

```
    Action : inspect
     Parameter-map : TCP_IN_PARAMS

    Class-map : ZFW_UDP_PROTO_IN_CLASS(match-any)
     Match protocol snmp
    Action : inspect
     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

  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

R4#sh policy-firewall config parameter-map TCP_IN_PARAMS
 parameter-map type inspect TCP_IN_PARAMS
 audit-trail on
 alert on
 max-incomplete low 400
 max-incomplete high 800
 one-minute low 400
 one-minute high 800
 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
```

3.0 Cisco IPS and Content Security (24 points)

Task 3.1: IPS Initialization (2 Points)

- Initialize the IPS sensor with the IP addressing listed in Lab 2 Address Table
- HTTPS management should be done via port 8888
- Allow the 10.1.1.0/24 and 10.21.21.0/24 network to manage the appliance
- Create a banner that says: "Welcome to IPexpert!"

Detailed Solution

CAT4

```
int g1/0/1
 sw host
 sw acc vlan 100
```

IPS

```
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: 10.1.1.0/24
Permit: 10.21.21.0/24
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
access-list 10.21.21.0/24
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]: 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 ---

Complete the advanced setup using CLI or IDM.
To use IDM,point your web browser at https://<sensor-ip-address>.
```

```
conf t
service host
 network-settings
  login-banner-text "Welcome to IPexpert!"
  exit
  exit

service web-server
 enable-tls true
 port 8888
 exit
```

The setup of an IPS sensor should be second nature by now. You can either configure the port in option 3 of the setup menu or you can do it directly in the CLI. Either way make sure you test it.

Verification

```
sensor# exit

"Welcome to IPexpert!"
IPS login: cisco
Password:

IPS# sh interfaces brief
CC   Interface            Sensing State   Link   Inline Mode   Pair Status
     GigabitEthernet0/0   Disabled        Down   Unpaired      N/A
*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Disabled        Down   Unpaired      N/A
     GigabitEthernet0/2   Disabled        Down   Unpaired      N/A
     GigabitEthernet0/3   Disabled        Down   Unpaired      N/A

IPS# ping 10.1.1.200
PING 10.1.1.200 (10.1.1.200): 56 data bytes
64 bytes from 10.1.1.200: icmp_seq=0 ttl=128 time=2.0 ms
64 bytes from 10.1.1.200: icmp_seq=1 ttl=128 time=1.5 ms

pod124ise/admin# telnet 10.1.1.15 port 8888
```

```
Trying 10.1.1.15...
Connected to 10.1.1.15.
Escape character is '^]'.
get /
FConnection closed by foreign host.
pod124ise/admin#
```

Task 3.2: Virtual Sensors (3 Points)

- Use two Virtual Sensors, vs0 and vs1
- Configure vs1 to be inline between ASA1 and VLAN 24
- Configure vs0 to be inline between ASA3 and VLAN 24
- Configure the switches as needed
- Enable the ICMP echo and echo reply signatures on both sensors but only configure it once
- The signatures should fire a medium severity event
- Verify events are generated by both virtual sensors

Detailed Solution

CAT4

```
vlan 241,243

interface GigabitEthernet1/0/2
 switchport access vlan 243
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/3
 switchport access vlan 24
 switchport mode access
 spanning-tree portfast

interface GigabitEthernet1/0/4
 switchport access vlan 241
 switchport mode access
```

```
 spanning-tree portfast

interface GigabitEthernet1/0/5
 switchport access vlan 24
 switchport mode access
 spanning-tree portfast
```

CAT3

```
int g1/0/6
 sw acc vlan 241

int g1/0/19
 sw acc vlan 243
```

IPS

```
service interface
 physical-interfaces GigabitEthernet0/0
  admin-state enabled
 physical-interfaces GigabitEthernet0/1
  admin-state enabled
 physical-interfaces GigabitEthernet0/2
  admin-state enabled
 physical-interfaces GigabitEthernet0/3
  admin-state enabled
 inline-interfaces Pair1
  interface1 GigabitEthernet0/0
  interface2 GigabitEthernet0/1
 inline-interfaces Pair2
  interface1 GigabitEthernet0/2
  interface2 GigabitEthernet0/3

service signature-definition sig0
 signatures 2000 0
  alert-severity medium
  status
   enabled true
 signatures 2004 0
 alert-severity medium
```

```
 status
  enabled true

service analysis-engine
 virtual-sensor vs0
  logical-interface Pair1
 virtual-sensor vs1
  logical-interface Pair2
```

Just because the task relates to the IPS you must not forget about the switches. Make sure that you check the VLANS even though the lab has a basic configuration already. There may be errors or it may just be incomplete.

Also, understand that just because you created a second virtual sensor you can still reference sig0, rules0, and ad0. Unless you require different policies there is no reason to create new ones.

Verification

```
ASA3(config)# ping 12.24.0.6 rep 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 12.24.0.6, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms

IPS# show events alert

evIdsAlert: eventId=1041379286523803357 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/03 22:32:31 2013/06/03 22:32:31 UTC
  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 12.24.0.30
    target:
      addr: locality=OUT 12.24.0.6
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
  interface: ge0_0
  protocol: icmp


evIdsAlert: eventId=1041379286523803358 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/03 22:32:31 2013/06/03 22:32:31 UTC
  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 12.24.0.6
    target:
      addr: locality=OUT 12.24.0.30
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
  interface: ge0_1
  protocol: icmp

ASA1(config)# ping 12.24.0.7 rep 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 12.24.0.7, timeout is 2 seconds:
!
```

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


evIdsAlert: eventId=1041379286523803359 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/03 22:33:25 2013/06/03 22:33:25 UTC
  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 12.24.0.10
    target:
      addr: locality=OUT 12.24.0.7
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
  interface: ge0_2
  protocol: icmp


evIdsAlert: eventId=1041379286523803360 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/03 22:33:25 2013/06/03 22:33:25 UTC
  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 12.24.0.7
    target:
      addr: locality=OUT 12.24.0.10
      os: idSource=unknown relevance=relevant type=unknown
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium
85
  threatRatingValue: 85
  interface: ge0_3
  protocol: icmp

IPS# sh interfaces brief
CC   Interface            Sensing State   Link   Inline Mode
Pair Status
     GigabitEthernet0/0   Enabled         Up     Paired with interface
GigabitEthernet0/1   Up
*    Management0/0        Disabled        Up
     GigabitEthernet0/1   Enabled         Up     Paired with interface
GigabitEthernet0/0   Up
     GigabitEthernet0/2   Enabled         Up     Paired with interface
GigabitEthernet0/3   Up
     GigabitEthernet0/3   Enabled         Up     Paired with interface
GigabitEthernet0/2   Up
```

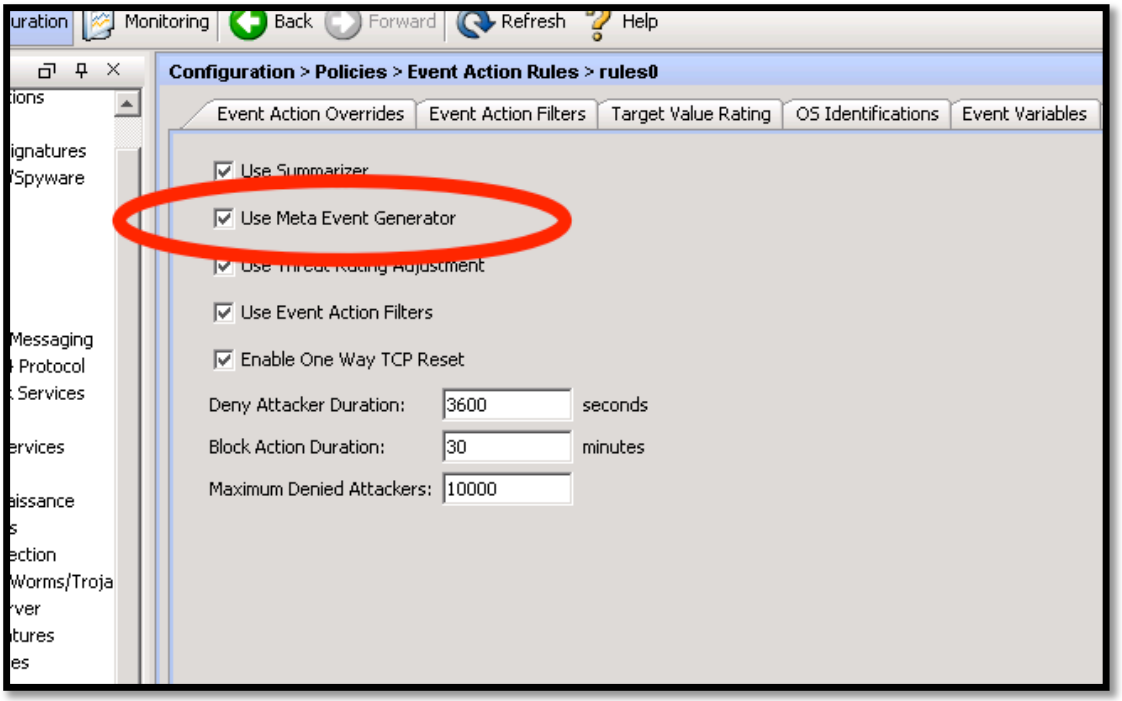
Task 3.3: Custom IPS Signature (4 Points)

- It's been determined that an attack may occur that is seen by a correlation of 5 separate signatures. These signatures are not enabled by default and determining when each of these 5 signatures fired within a specific period of time is not an option with the overwhelming amount of information IT is collecting
- Configure Signatures 3221, 3222, 3223, 3224 and 3225 as a compound signature
- The event should fire if 5 of the signatures fire within 90 seconds in the following order :
  - 3225
  - 3222
  - 3224
  - 3223
  - 3221
- The alert Severity should be high and the attacker should be denied inline

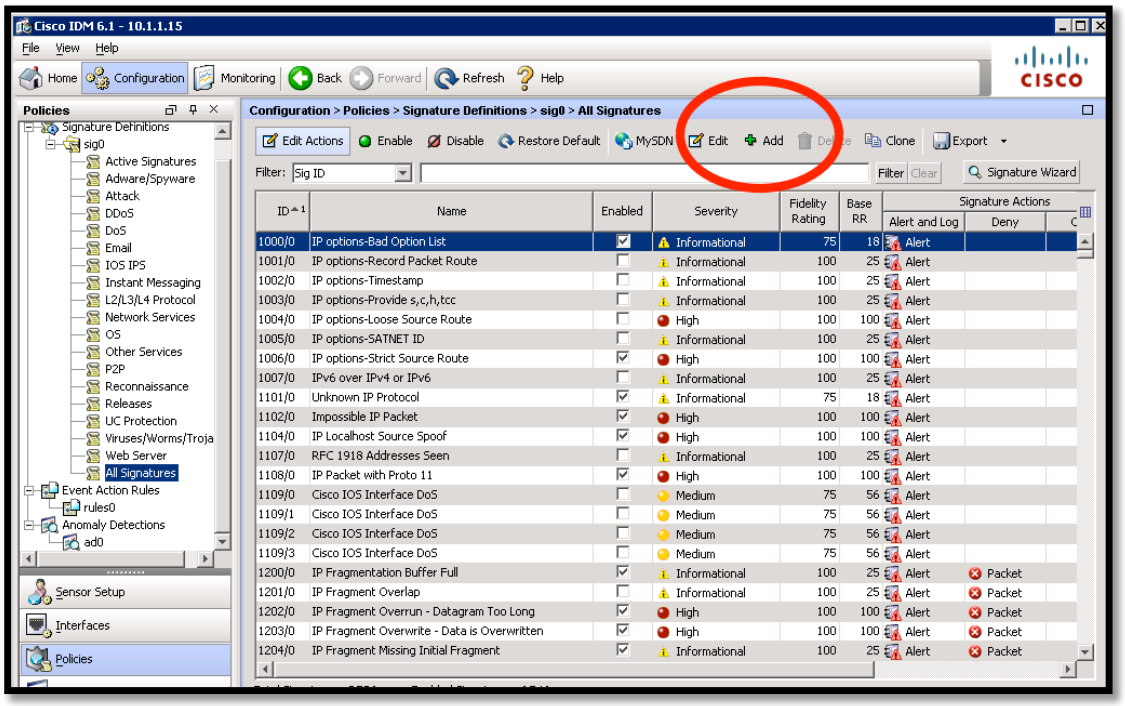
Detailed Solution

IPS

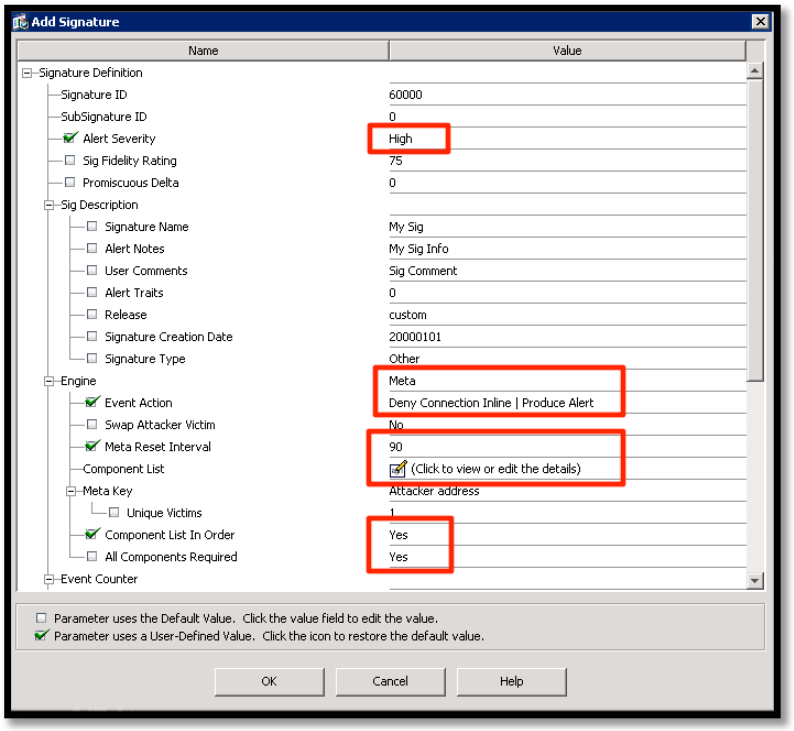
Ensure the Meta Event Generator is enabled :



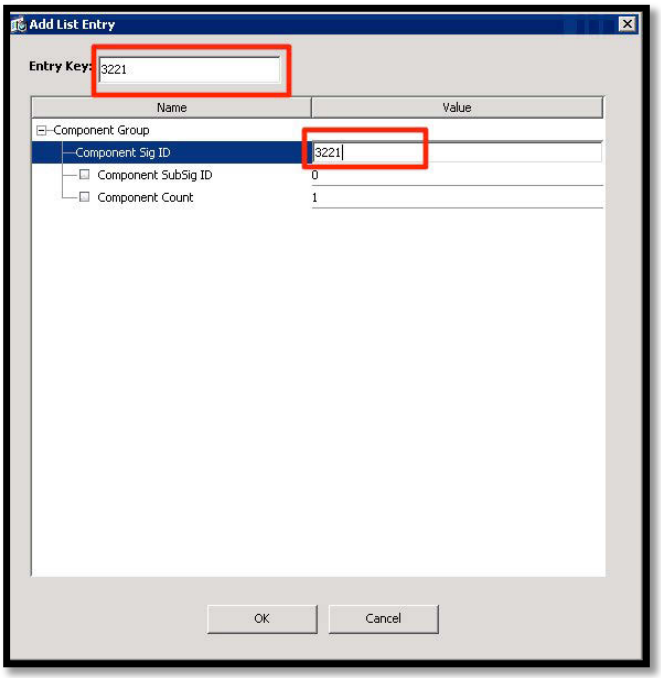
Select All Signatures -> Add :



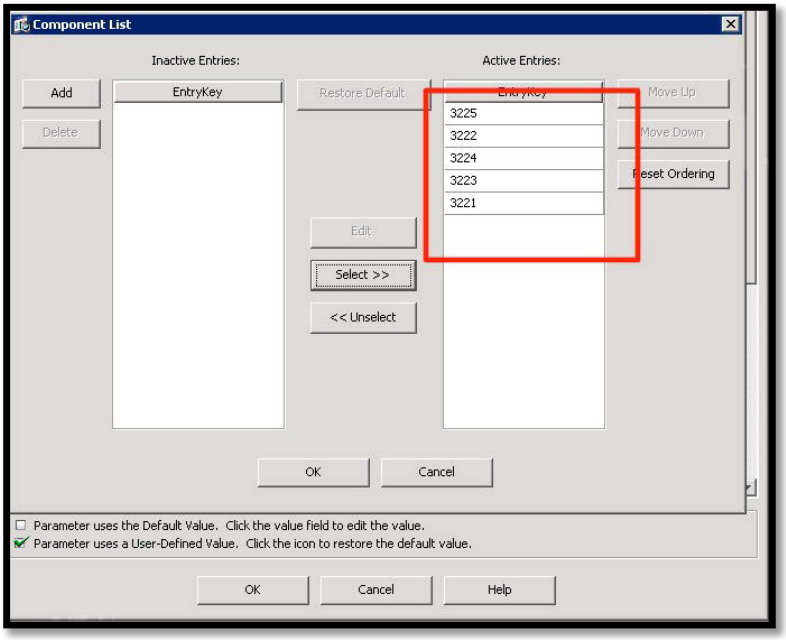
Define the parameters as listed in the lab requirements. These are highlighted in the screenshot below :



Click the Component List and Add Entry Keys :



Add the Entry Keys in the order required then, click OK :



Click OK again and apply the signature.

Here you want to see 5 signatures in a specific period of time. This is a perfect situation to allow the Meta Event generator to do the work for us. The Meta event Generator is what allows a correlation of events within a specific period of time and in a certain order.

Verification

For verification here we will simply ensure that the signature is created.

Task 3.4: IOS IPS (4 Points)

- Configure R8 to enable IPS inbound on the Serial Interface
- The Signature file located in flash should be used
- Enable the signature for ICMP Echo Request
- When completed you should obtain the following results :

```
R6#ping 8.8.8.8 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4
ms

R8#sh ip ips statistics
Signature statistics [process switch:fast switch]
  signature 2004:0: packets checked [0:100] alarmed [0:100] dropped
[0:0]
Interfaces configured for ips 1
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
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
```

Detailed Solution

R8

```
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
```

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
quit

mkdir flash:/IPS_CONFIG
ip ips config location flash:/IPS_CONFIG

ip ips signature-category
 category all
  retired true
 category ios_ips basic
  retired false
  enabled true

ip ips name IPS

int s0/0/0
 ip ips IPS in

copy flash:/IOS-S376-CLI.pkg idconf

ip ips signature-definition
 signature 2004 0
  status
   retired false
   enabled true

interface GigabitEthernet1/0/2
```

This task is an example of what you would do using Cisco documentation instead of trying to remember all the commands and steps off top of your head.

This feature is documented under Data Plane Security Configuration Guide, Intrusion Prevention, “Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements”. This is also where you will find the Cisco’s public key used to validate the signature package.

Verification

```
R8#sh cry key pubkey-chain rsa
Codes: M - Manually configured, C - Extracted from certificate

Code Usage         IP-Address/VRF         Keyring          Name
M    Signing                              default          realm-cisco.pub


R8#sh ip ips configuration

IPS Signature File Configuration Status
    Configured Config Locations: flash:/IPS_CONFIG
    Last signature default load time: 11:00:25 UTC Jun 4 2013
    Last signature delta load time: 11:01:15 UTC Jun 4 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: 2132

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name IPS
```

```
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Obsolete tuning is disabled
    Regex compile threshold (MB) 9
    Interface Configuration
      Interface Serial0/0/0
        Inbound IPS rule is IPS
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
        Enable: True

IPS License Status:             Not Required
        Current Date:           Jun 4 2013
        Expiration Date:        Not Available
        Extension Date:         Not Available
        Signatures Loaded:      Jan 12 2009     S376.0
        Signature Package:      Jan 12 2009     S376.0


R8#sh ip ips signatures 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
      Nd: signature is disallowed
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   Y     A      INFO     0     1    0    200   30  FA  N 100
S1
      sig-name: ICMP Echo Request
      sig-string-info: My Sig Info
      sig-comment: Sig Comment
      sig-type: Other
      Engine atomic-ip params:
           fragment-status :
           icmp-type : 8
           l4-protocol : icmp


R6#ping 8.8.8.8 rep 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms

*Jun  4 11:04:21.159: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo
Request [12.24.0.6:8 -> 8.8.8.8:0] VRF:NONE RiskRating:25
*Jun  4 11:04:21.163: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo
Request [12.24.0.6:8 -> 8.8.8.8:0] VRF:NONE RiskRating:25

R8#sh ip ips stat
Signature statistics [process switch:fast switch]
  signature 2004:0: packets checked [0:100] alarmed [0:100] dropped [0:0]
Interfaces configured for ips 1
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
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
```

Task 3.5: WSA Basic Setup (3 Points)

- Configure WSA interfaces according to the topology & addressing table
- Use 10.1.1.101 as the NTP and DNS server
- Password MUST BE SET TO “ironport”
- Use a separate interface for management and proxy functions
- Set default gateways to 10.1.1.1 and 12.4.0.40

Detailed Solution

CAT3

```
int g1/0/3
 sw host
 sw acc vlan 100

int g1/0/4
 sw host
 sw acc vlan 4
```

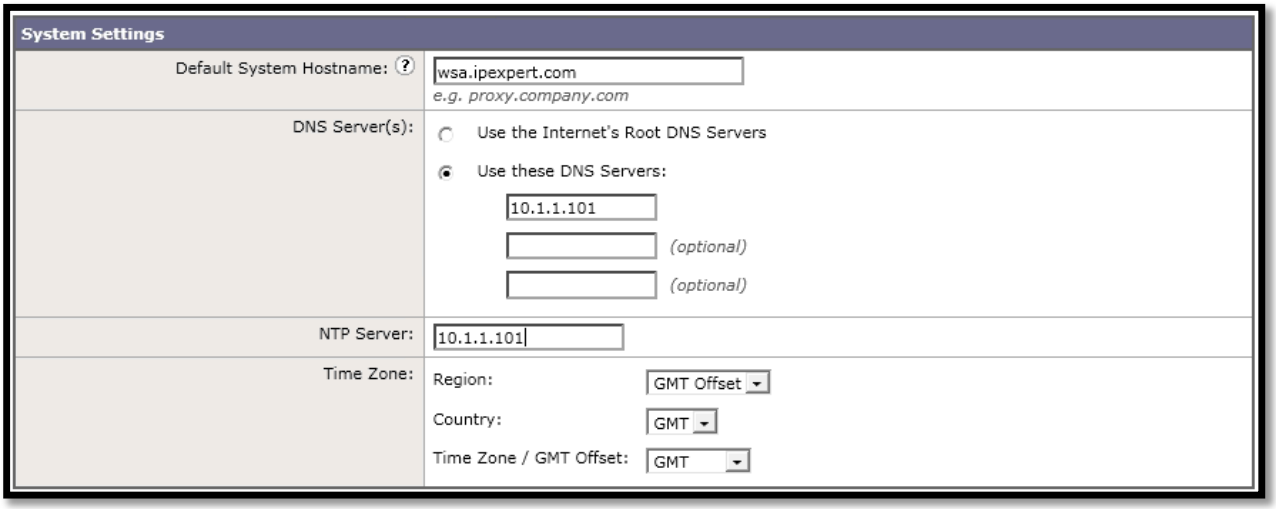
WSA

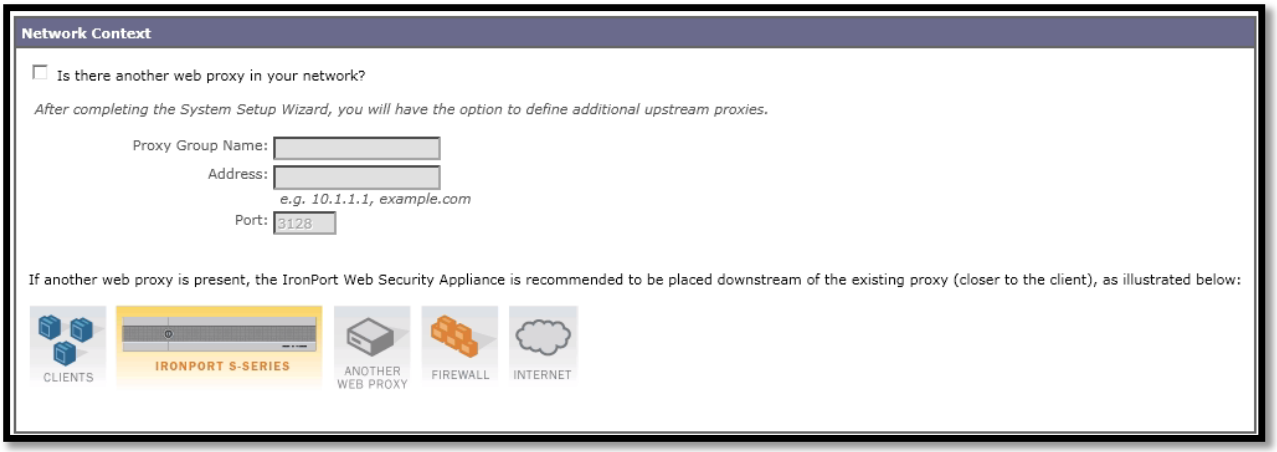
```
ironport.example.com> interfaceconfig

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> edit
```

```
Enter the number of the interface you wish to edit.
[]> 1

IP Address (Ex: 192.168.1.2):
[192.168.42.42]> 10.1.1.180

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.0

Hostname:
[ironport.example.com]> wsam.ipexpert.com

Do you want to enable FTP on this interface? [Y]>

Which port do you want to use for FTP?
[21]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?
[22]>

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?
[8080]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?
[8443]>

You have not entered an HTTPS certificate.  To assure privacy, run
"certconfig" first.  You may use the demo, but this will not be secure.
Do you really wish to use a demo certificate? [Y]>

Both HTTP and HTTPS are enabled for this interface, should HTTP requests
redirect to the secure service? [Y]>
```

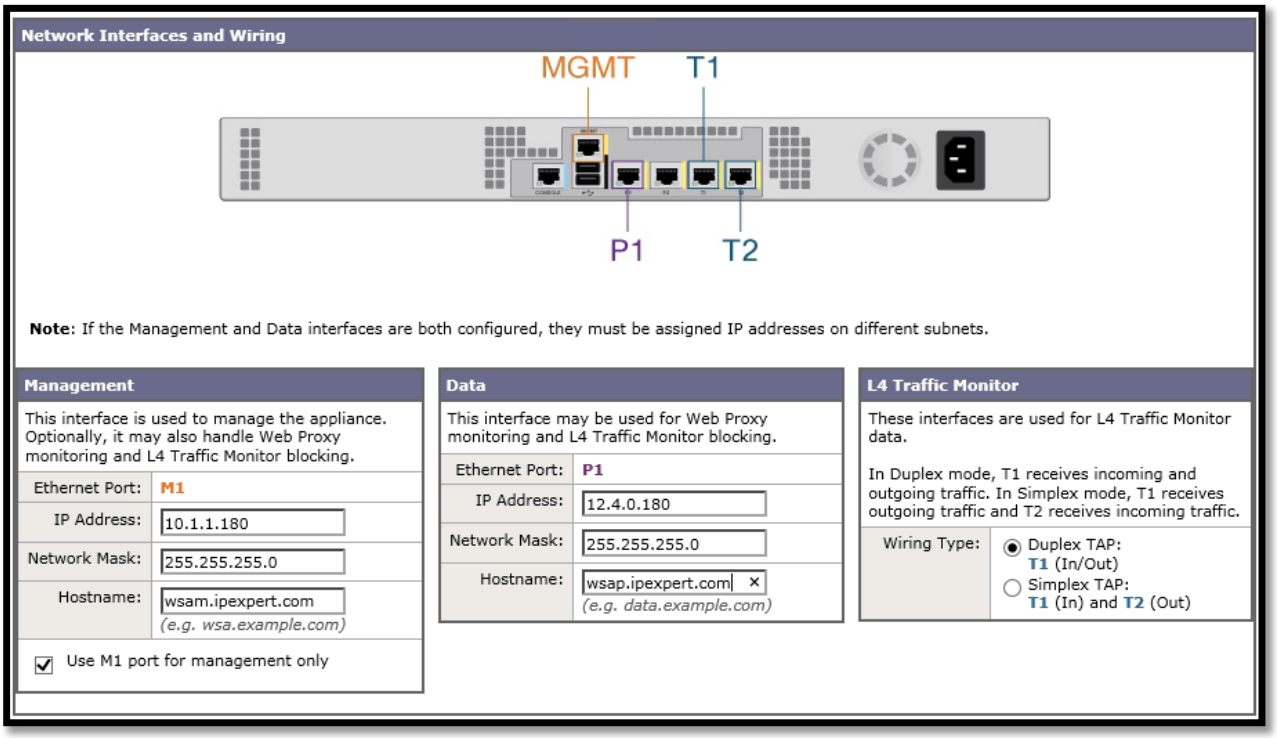
```
The interface you edited might be the one you are currently logged into.
Are
you sure you want to change it? [Y]>


ironport.example.com> commit

Please enter some comments describing your changes:
[]>

Changes committed: Tue Jun 04 11:31:41 2013 GMT
Please run System Setup Wizard at http://192.168.42.42:8080
```

Now connect to 10.1.1.180 using port 8080 (HTTP) or 8443 (HTTPs) and run the System Setup Wizard (under "System Administration"). Configure hostname, DNS & NTP Servers and basic interface settings :

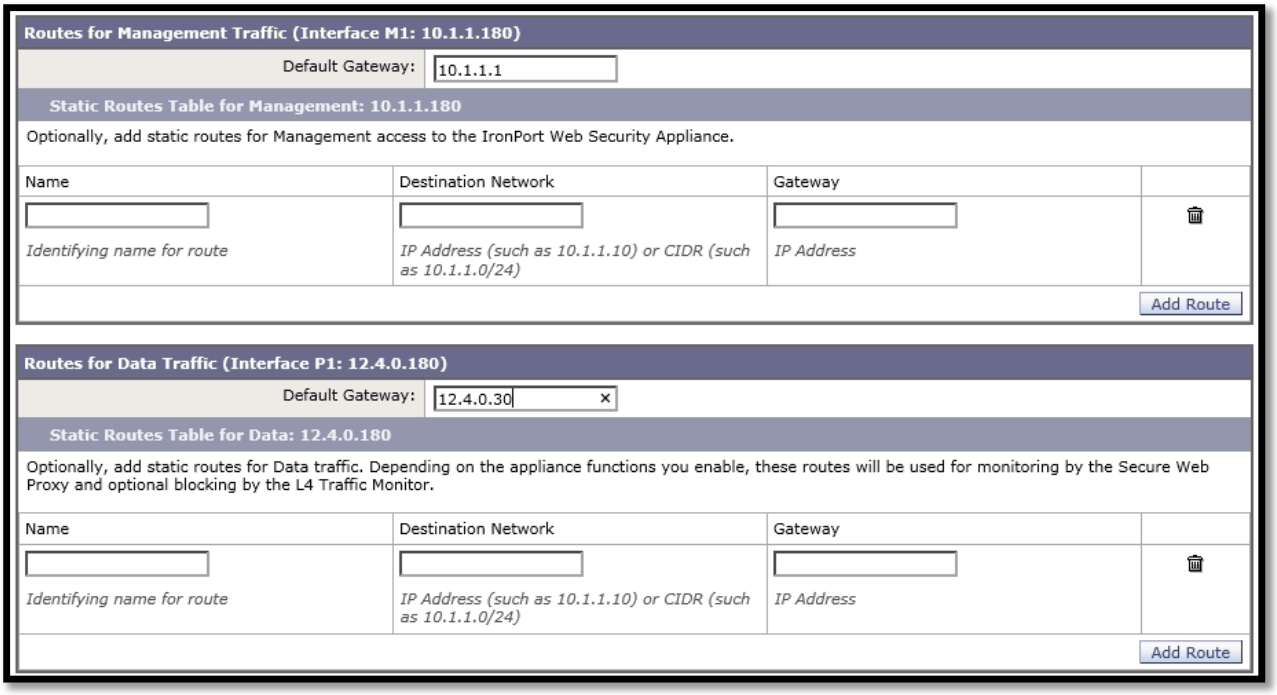


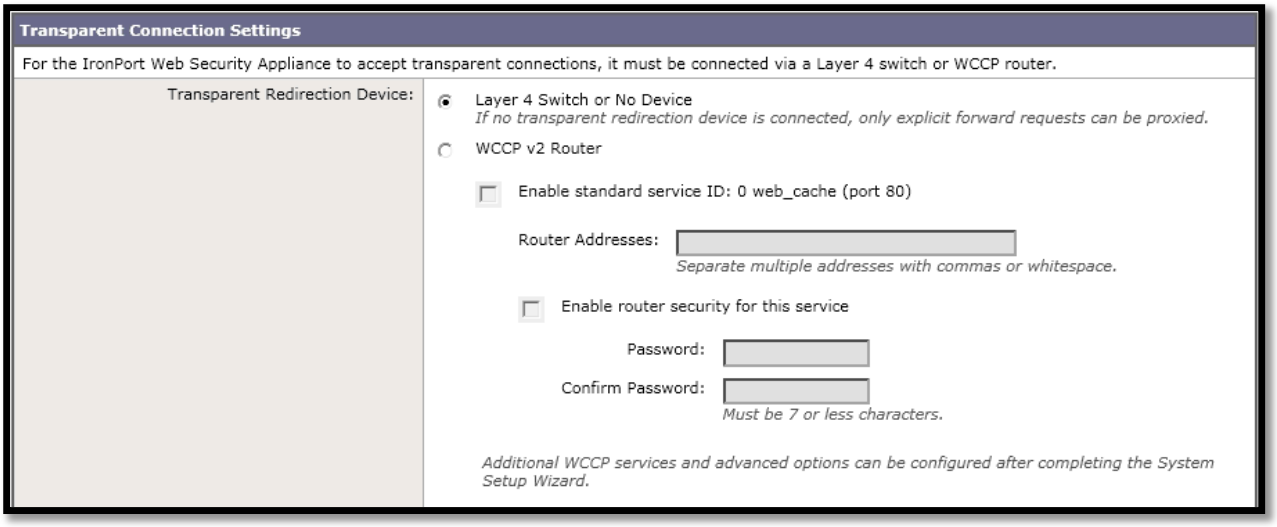


M1 will be only used for management :

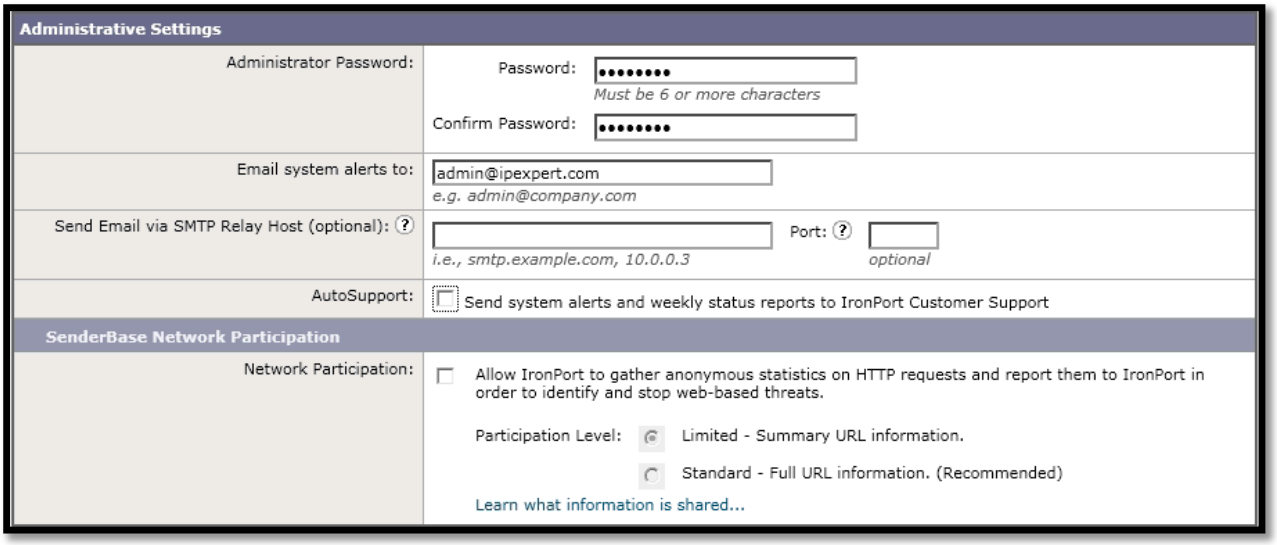


Specify default gateways (10.1.1.1 and 12.4.0.40) – any additional routes you may want to add you can do it later on :

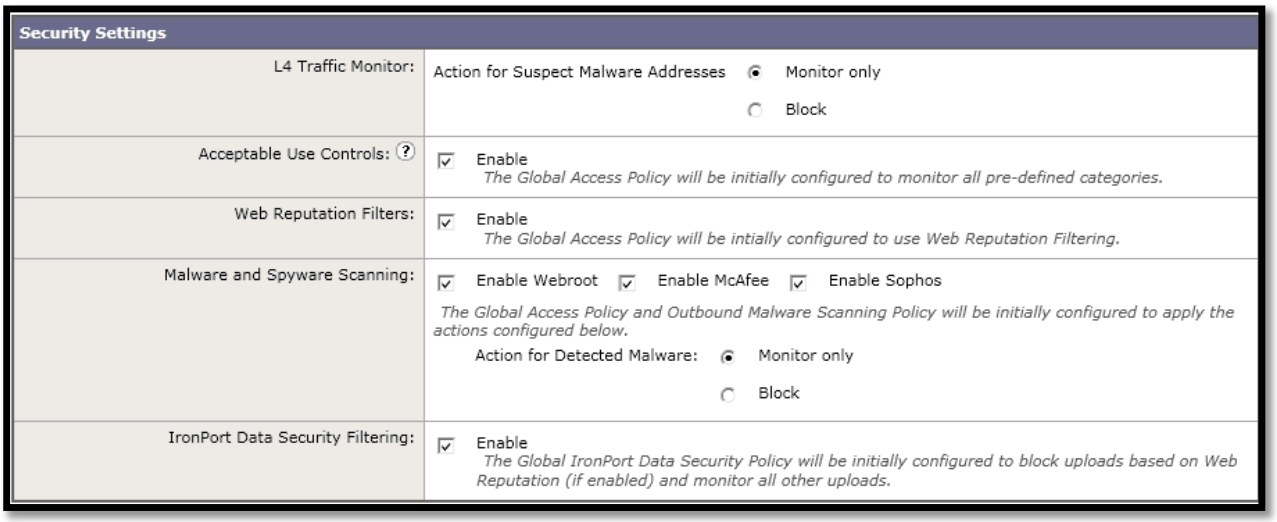




Password MUST BE SET TO "ironport" :



Leave all security features enabled :



Double check L2 first, then assign an IP address to the management interface and use a setup wizard to initialize remaining WSA settings.

Since the management port is not to be used for proxy functions we need to specify two default gateways – one for M1 and the other one for P1 interface.

Verification

```
wsa.ipexpert.com> ping

Which interface do you want to send the pings from?
1. Auto
2. Management (10.1.1.180/24: wsam.ipexpert.com)
3. P1 (12.4.0.180/24: wsap.ipexpert.com)
[1]> 3

Please enter the host you wish to ping.
[]> 192.1.49.130

Press Ctrl-C to stop.
PING 192.1.49.130 (192.1.49.130) from 12.4.0.180: 56 data bytes
36 bytes from 12.4.0.4: Redirect Network(New addr: 12.4.0.40)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 a6cf   0 0000  3f  01 d69e 12.4.0.180  192.1.49.130

64 bytes from 192.1.49.130: icmp_seq=0 ttl=253 time=3.590 ms
36 bytes from 12.4.0.4: Redirect Network(New addr: 12.4.0.40)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 a6d3   0 0000  3f  01 d69a 12.4.0.180  192.1.49.130

64 bytes from 192.1.49.130: icmp_seq=1 ttl=253 time=8.225 ms
36 bytes from 12.4.0.4: Redirect Network(New addr: 12.4.0.40)
^C
--- 192.1.49.130 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.348/5.054/8.225/2.244 ms
```

Task 3.6: WSA Configuration (3 Points)

- Enable Transparent Proxy for HTTP on WSA
- ASA4 should redirect all HTTP packets received on its inside interface destined to port 80 to WSA
- Integrate the Proxy with AD Server 10.1.1.101
- Use "Administrator" // "IPexpert123" to join IPEXPERT.COM domain

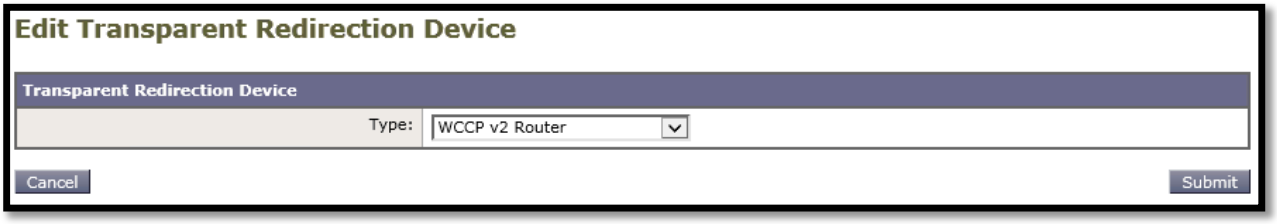
Detailed Solution

ASA4

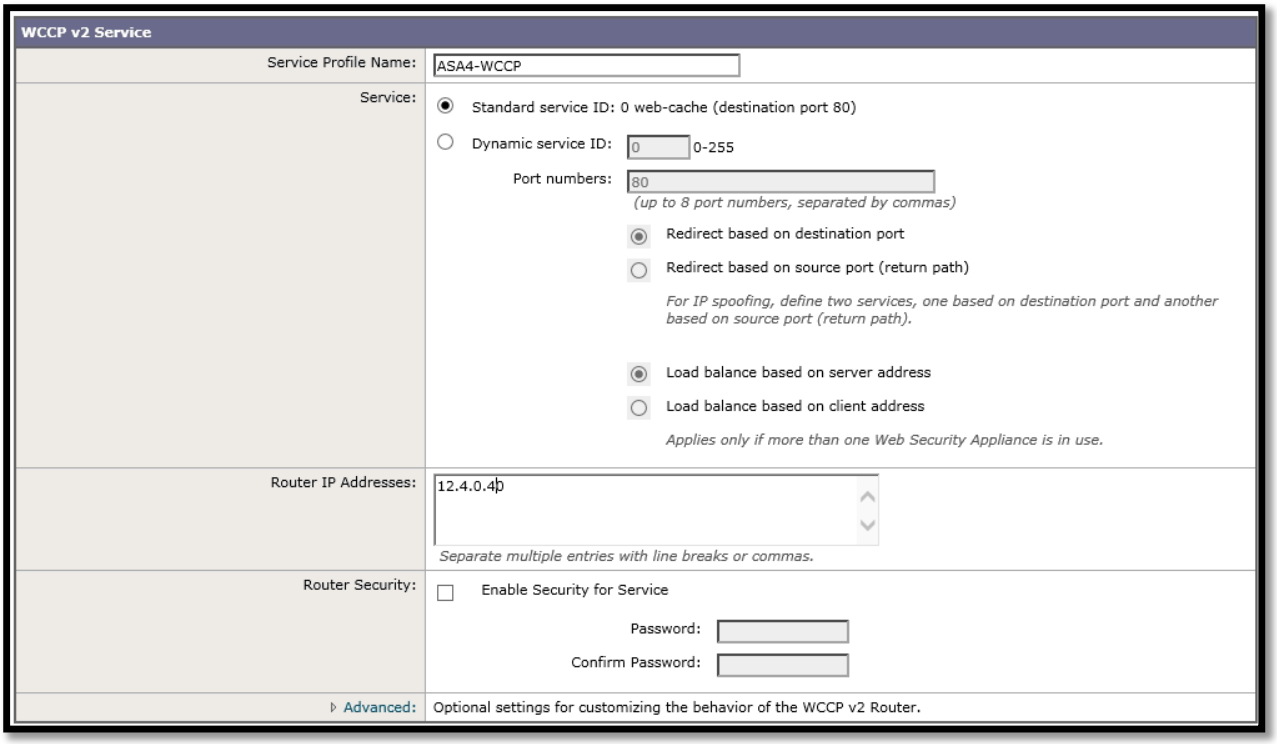
```
wccp web-cache
wccp interface inside web-cache redirect in
```

WSA

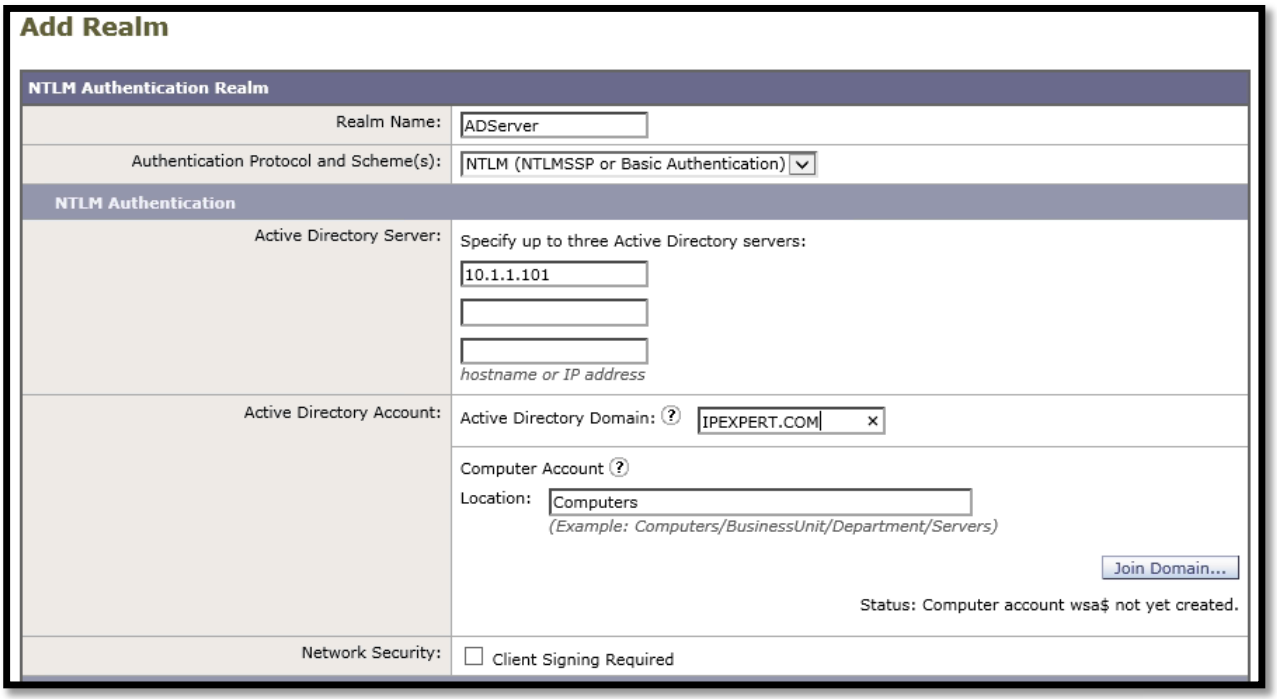
Go under Network -> Transparent Redirection, select WCCP v2 Router :



Choose a Standard service ID and specify IP address of the ASA's inside interface :

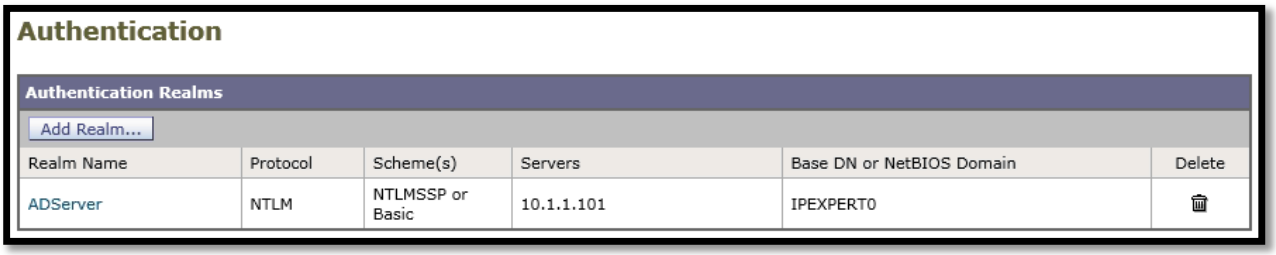


Now go under Network -> Authentication and add the AD server :



Click on “Join Domain”, provide correct credentials and when it creates an AD account click on “Submit” at the bottom of the page. Finally commit the changes.

This is what you should see under “Authentication” :



Web Proxy was enabled automatically during Initial Setup so we don’t have to worry about. If the question was talking about non-standard HTTP ports you would want to modify the Proxy settings but by default ports 80 and 3128 are enabled so we don’t care.

Verification

```
ASA4(config)# sh wccp web-cache det

WCCP Cache-Engine information:
        Web Cache ID:          12.4.0.180
        Protocol Version:      2.0
        State:                 Usable
        Initial Hash Info:     00000000000000000000000000000000
                               00000000000000000000000000000000
        Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                               FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:        256 (100.00%)
        Packets Redirected:    0
        Connect Time:          00:00:32

ASA4(config)# sh wccp  web-cache view

    WCCP Routers Informed of:
        12.41.0.40
```

```
        WCCP Cache Engines Visible:
            12.4.0.180

        WCCP Cache Engines NOT Visible:
            -none-
```

Telnet from R4 to CAT3 over port 80 and see if ASA redirects packets :

```
ASA4(config)# sh wccp web-cache

Global WCCP information:
    Router information:
        Router Identifier:                  12.41.0.40
        Protocol Version:                   2.0

    Service Identifier: web-cache
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           9
        Redirect access-list:               -none-
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
```

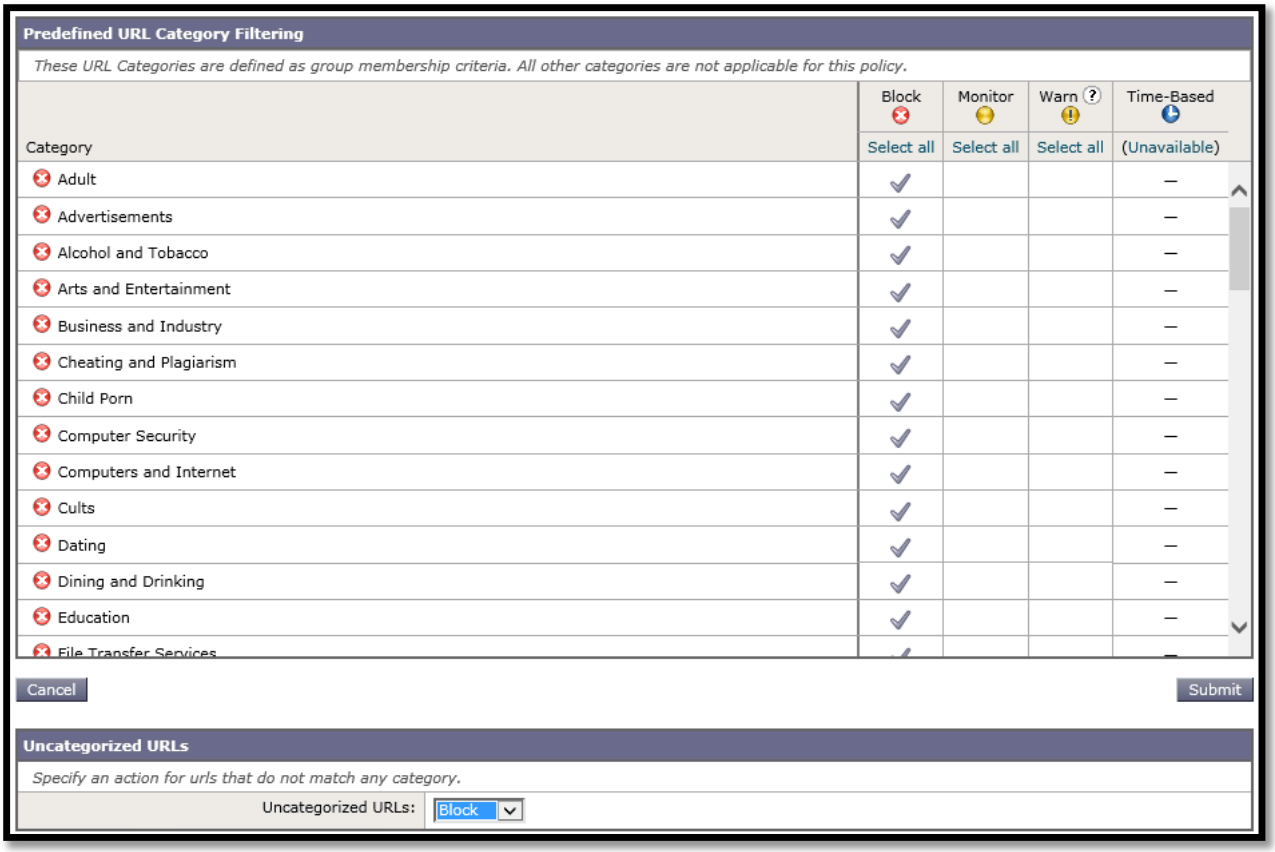
Task 3.7: Guest Access & Policies (5 Points)

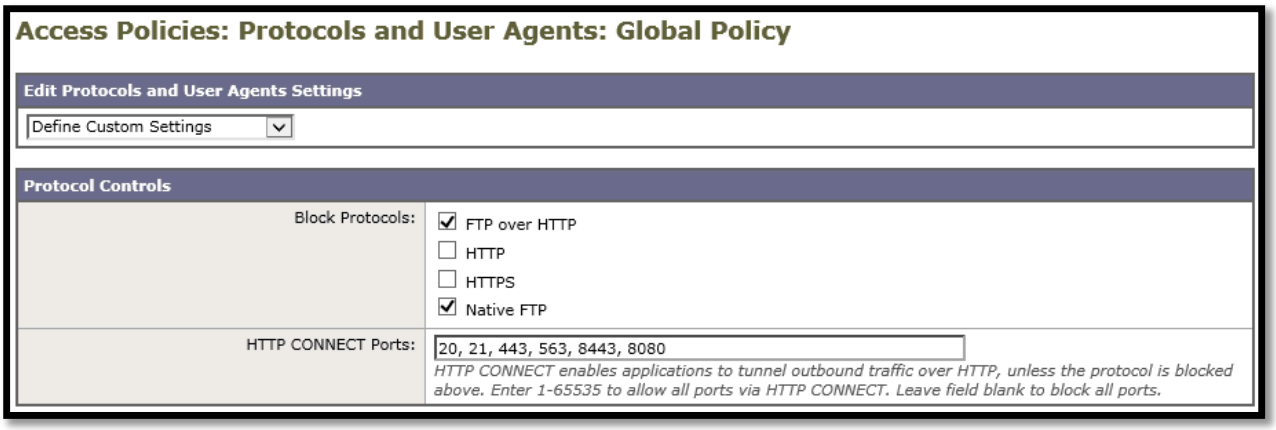
- Your company has a very strict security policy – access to all websites should be blocked by default along with any FTP requests
- Only authenticated employees (group IPX_EMP) located in VLAN 24 should be granted full HTTP access and FTP connections to the Internet but according to the policy below :
  - When they try to use search engines that don't support Safe Search function, this should be blocked
  - WSA should display a warning when Adult-Oriented Content is tried to be accessed on YouTube
  - Native FTP connections should be allowed to transfer data in Active mode if Passive mode fails
- Any VLAN 24 client who fails authentication should be only given Guest Access to www.guestportal.com hosted on R10 – this site is trusted and all other security features should be bypassed for it
- Also when "Guests" try to connect to any server in the ipexpert.com domain they should be redirected to CAT3 – all other websites should be blocked
- Log Guest access based on the name entered by the user
- User "IPXEMP1", password "cisco", is part of the IPX_EMP group on AD

Detailed Solution

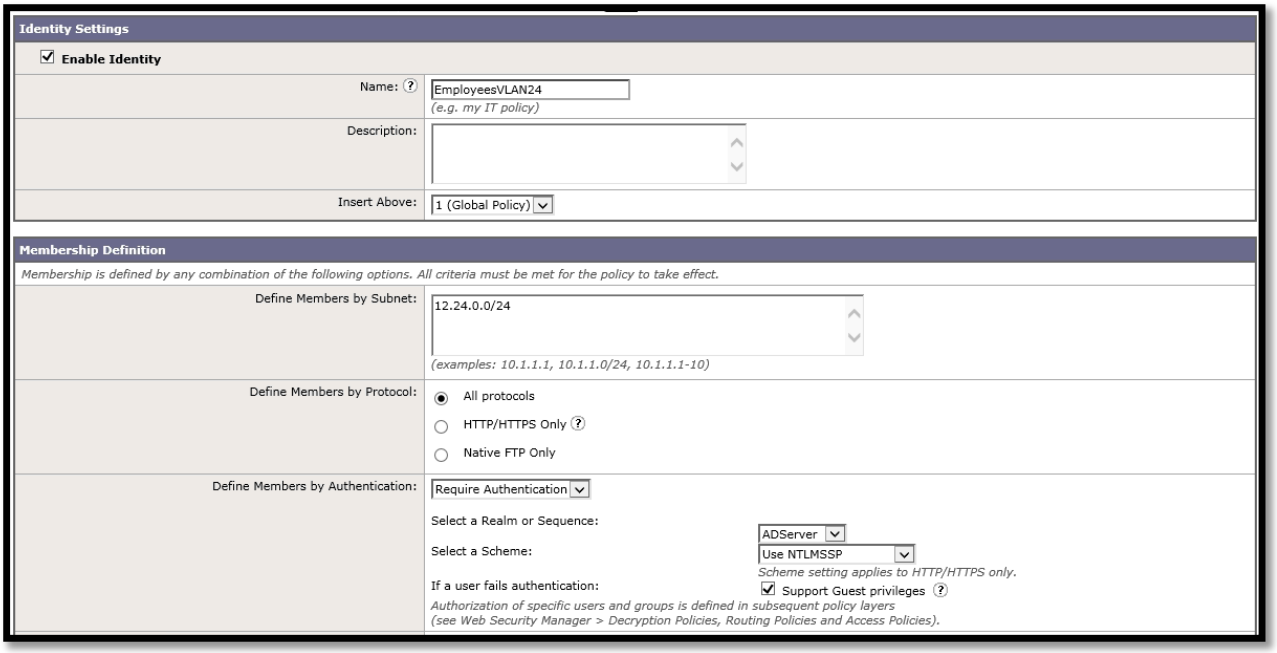
WSA

First thing we want to edit Global Access Policy – block all URLs, including Uncategorized. Then we want to block FTP over HTTP and Native FTP :

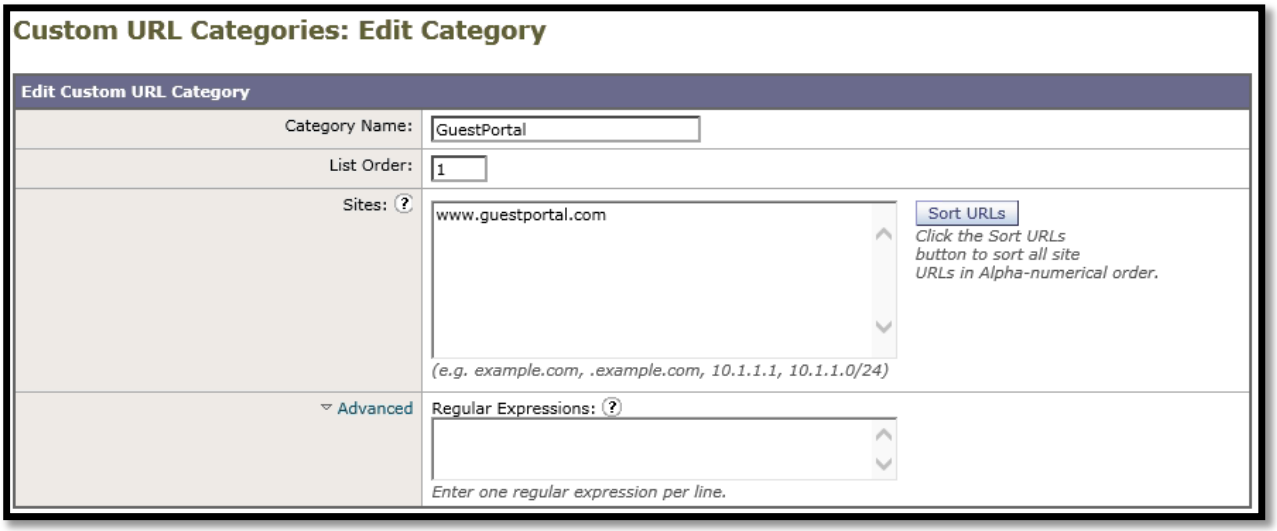


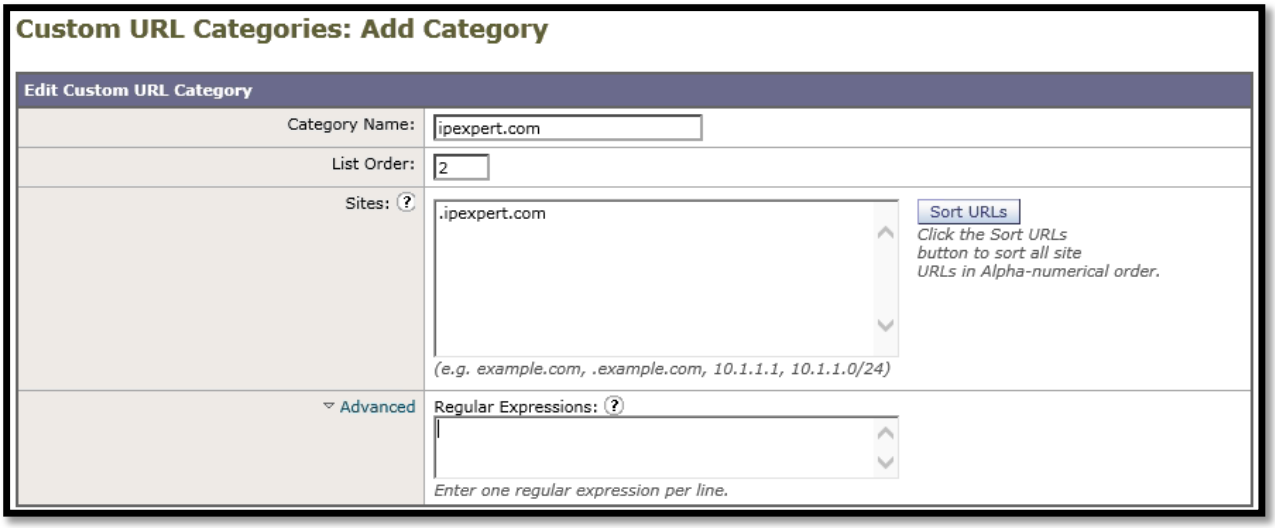


Next Create an Identity for Employees in VLAN 24. Select AD Server for authentication and enable support for Guest Access :

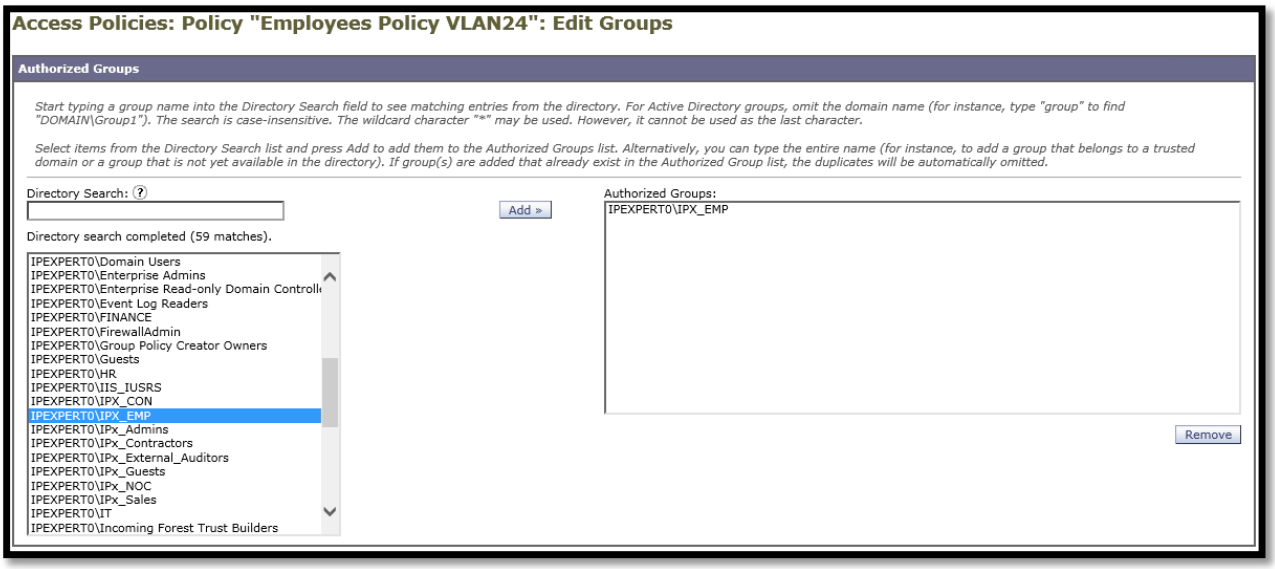


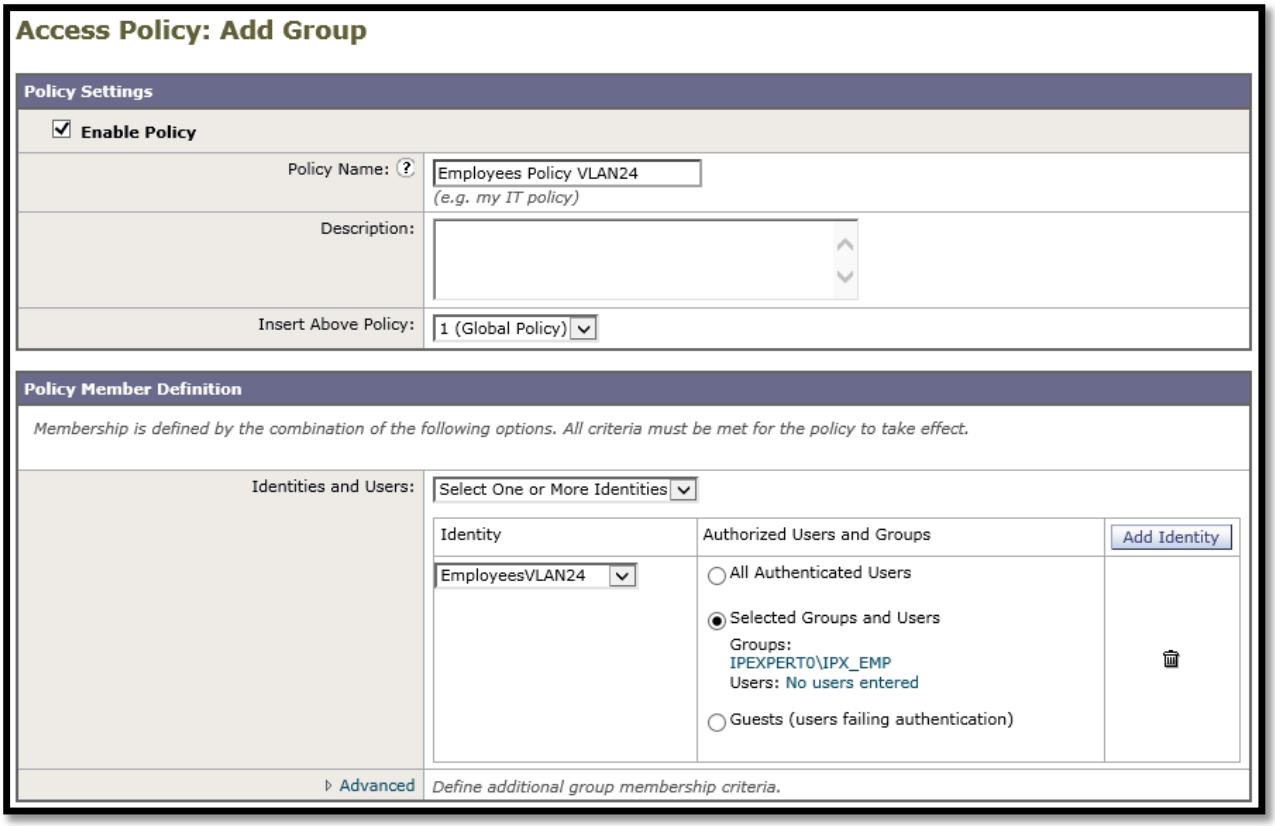
Before we move on we will now create two Custom Categories that will be used in the Guest Policy :



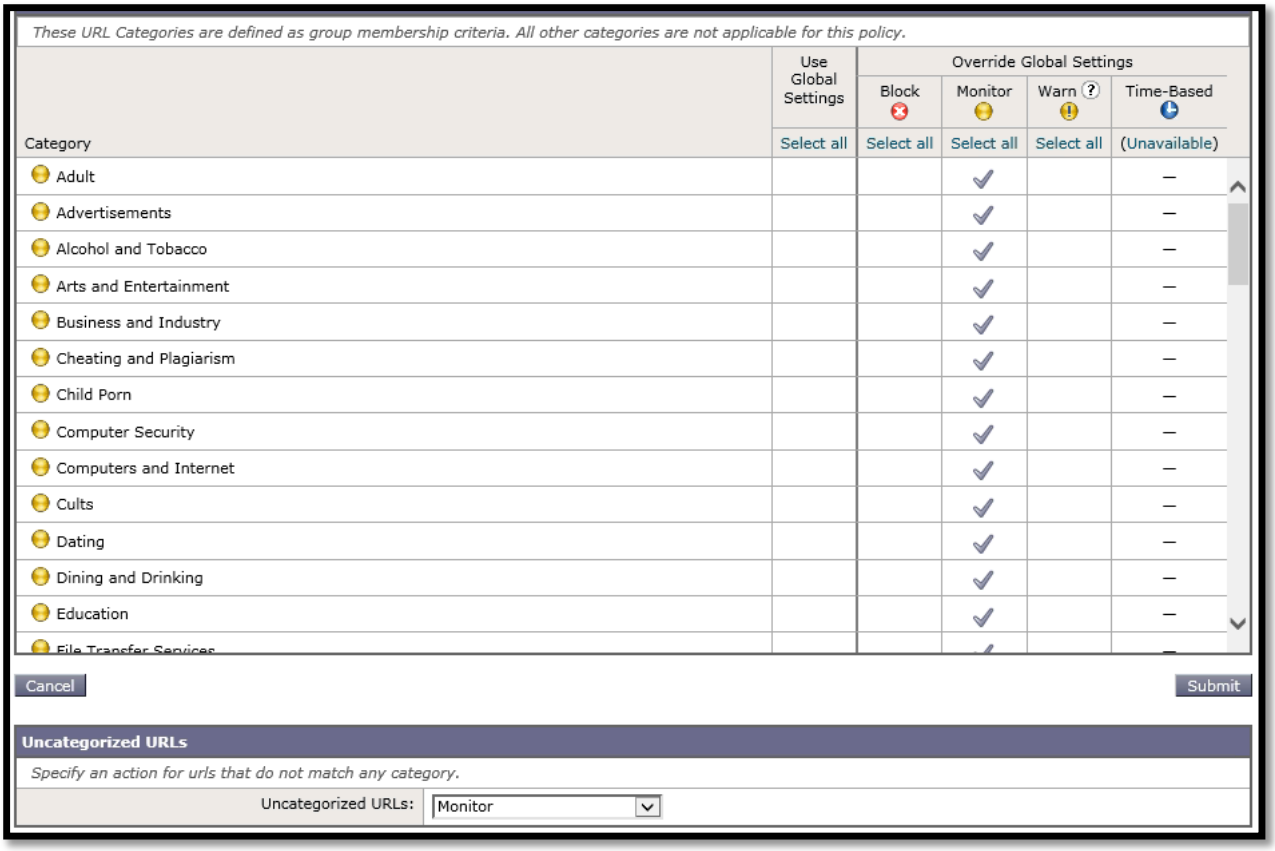


Now add an Access Policy for Employees. Select Employee Identity and under Authentication narrow down the scope of this policy to users who belong to AD group IPX_EMP :

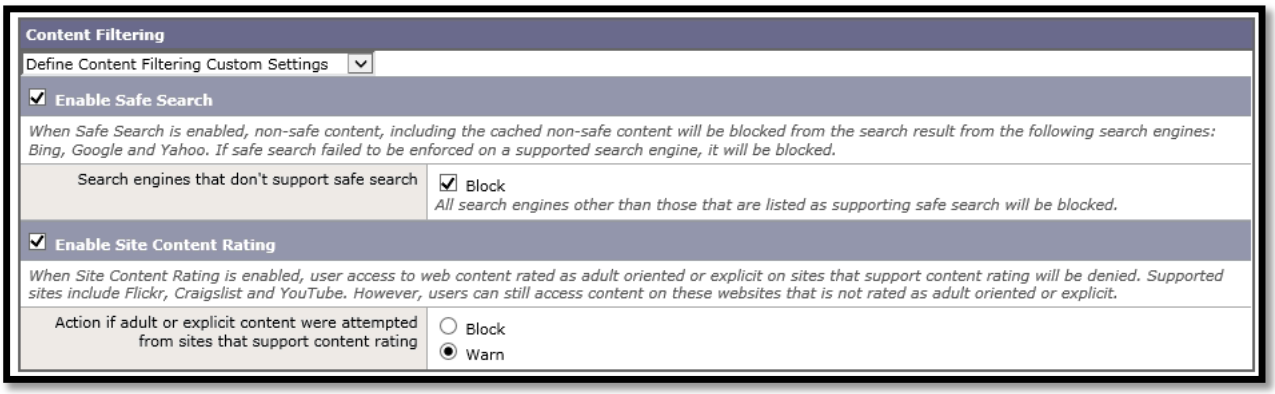


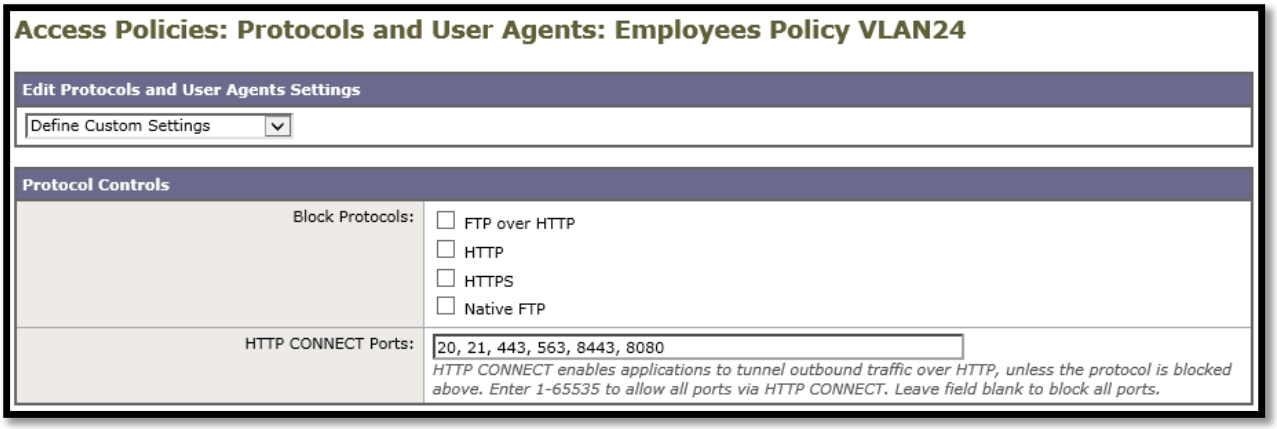


Allow for all Web Categories (Select all), including Uncategorized URLs :

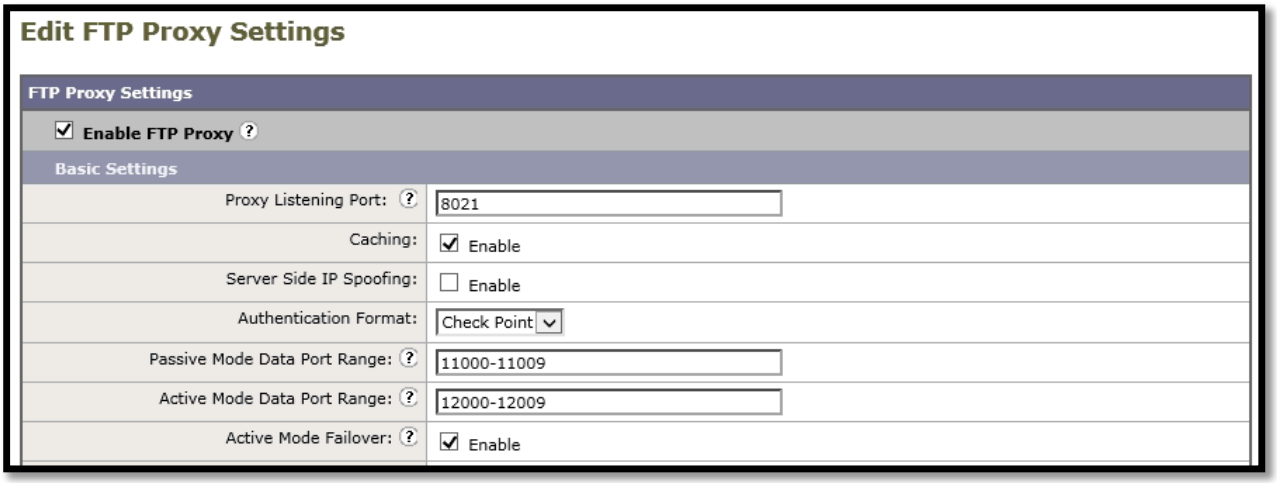


Enable Safe Search (Block), Site Content Rating (Warn) and unblock FTP :

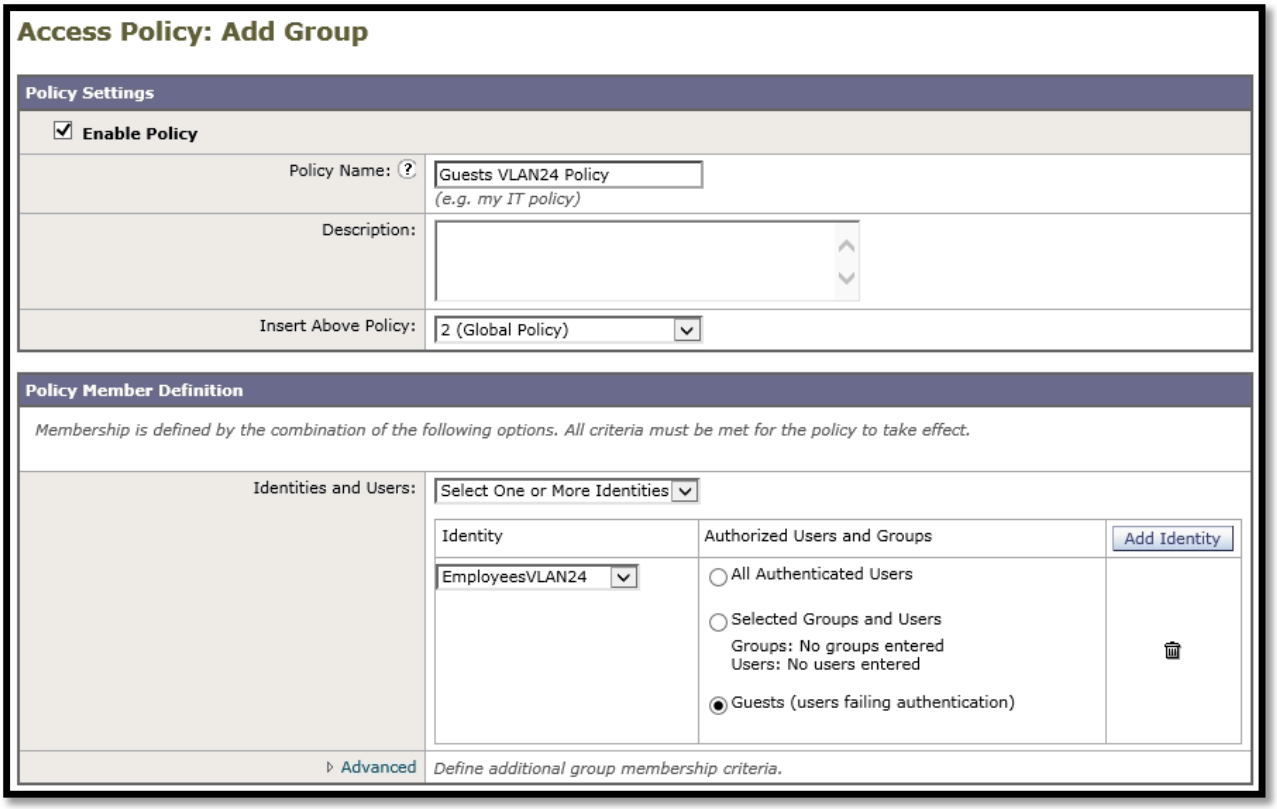




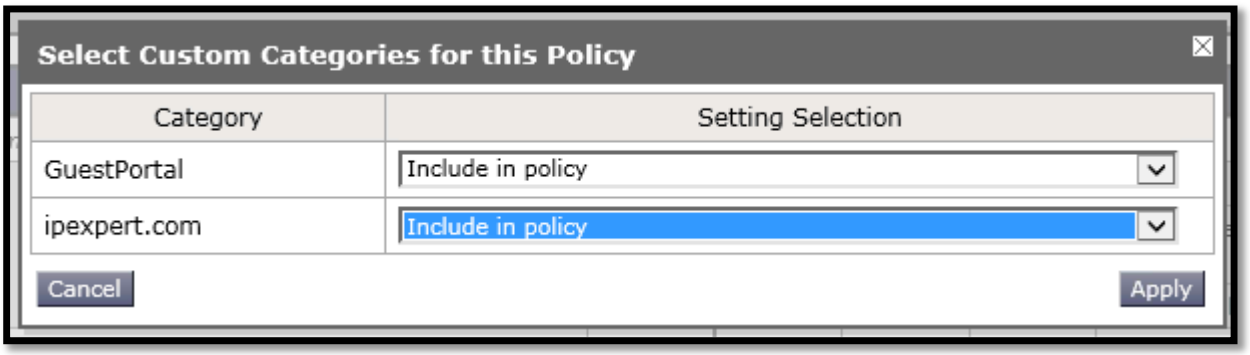
Another thing we want to make sure is enabled FTP Proxy and Active FTP for data transfer (Security Services -> FTP Proxy) :

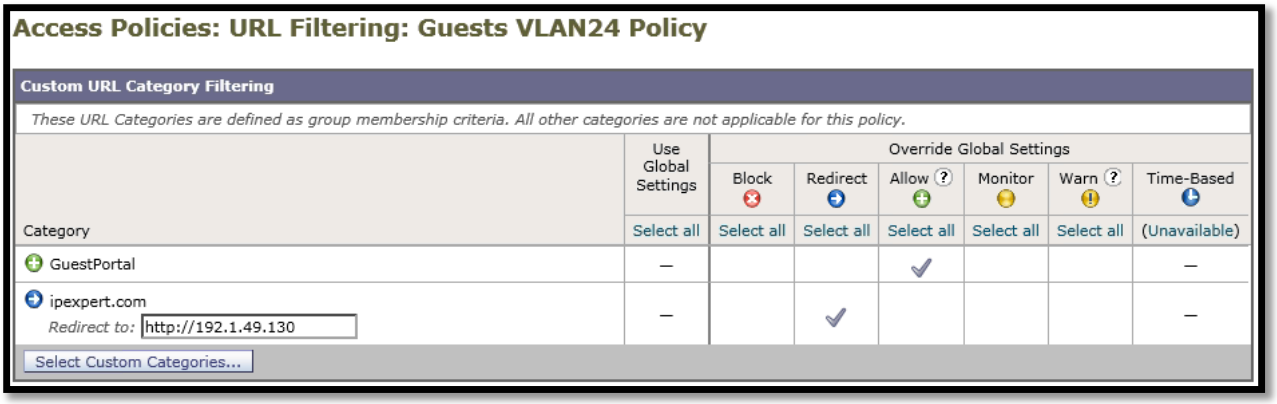


Moving on we should define a policy for Guests. Add a new one, above Global Policy, select Employee Identity and specify this is for users failing authentication (Guests) :

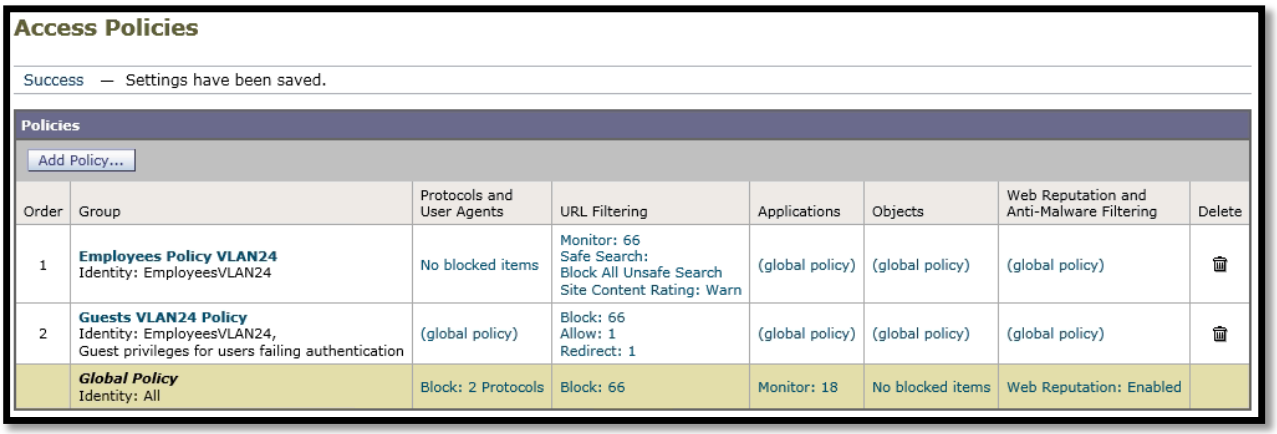


Modify the Policy. Add our Custom Categories and configure as per task requirements :

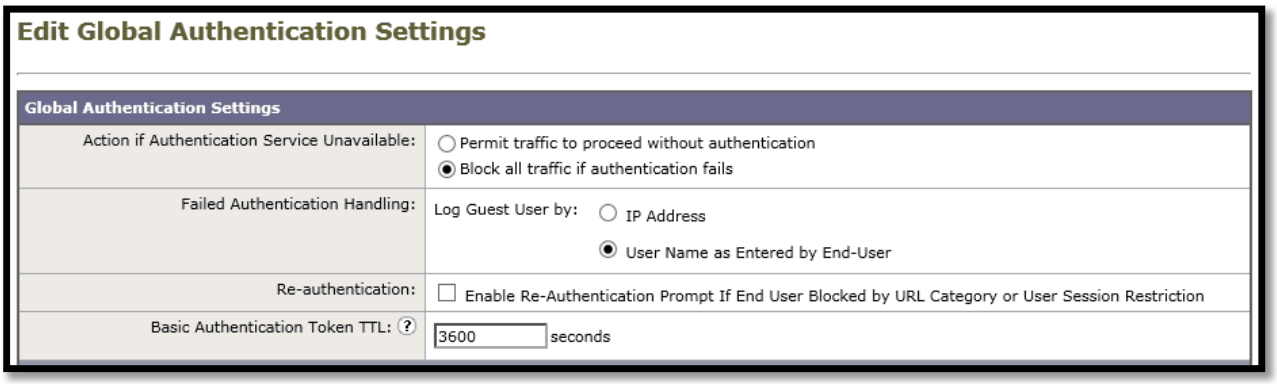




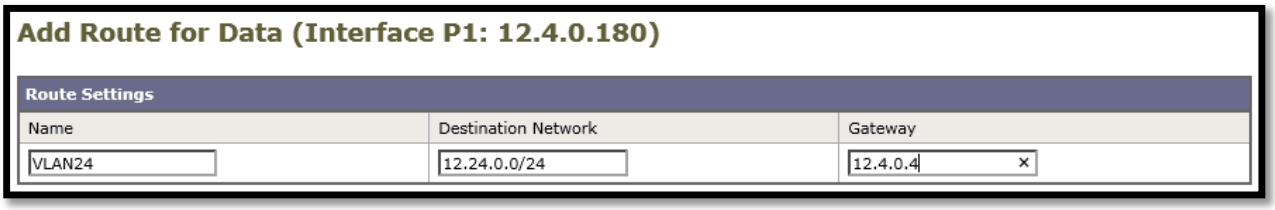
This is the structure of the entire Access Policy we will be using :



Two more things we want to configure are changing the way Guest access is logged :



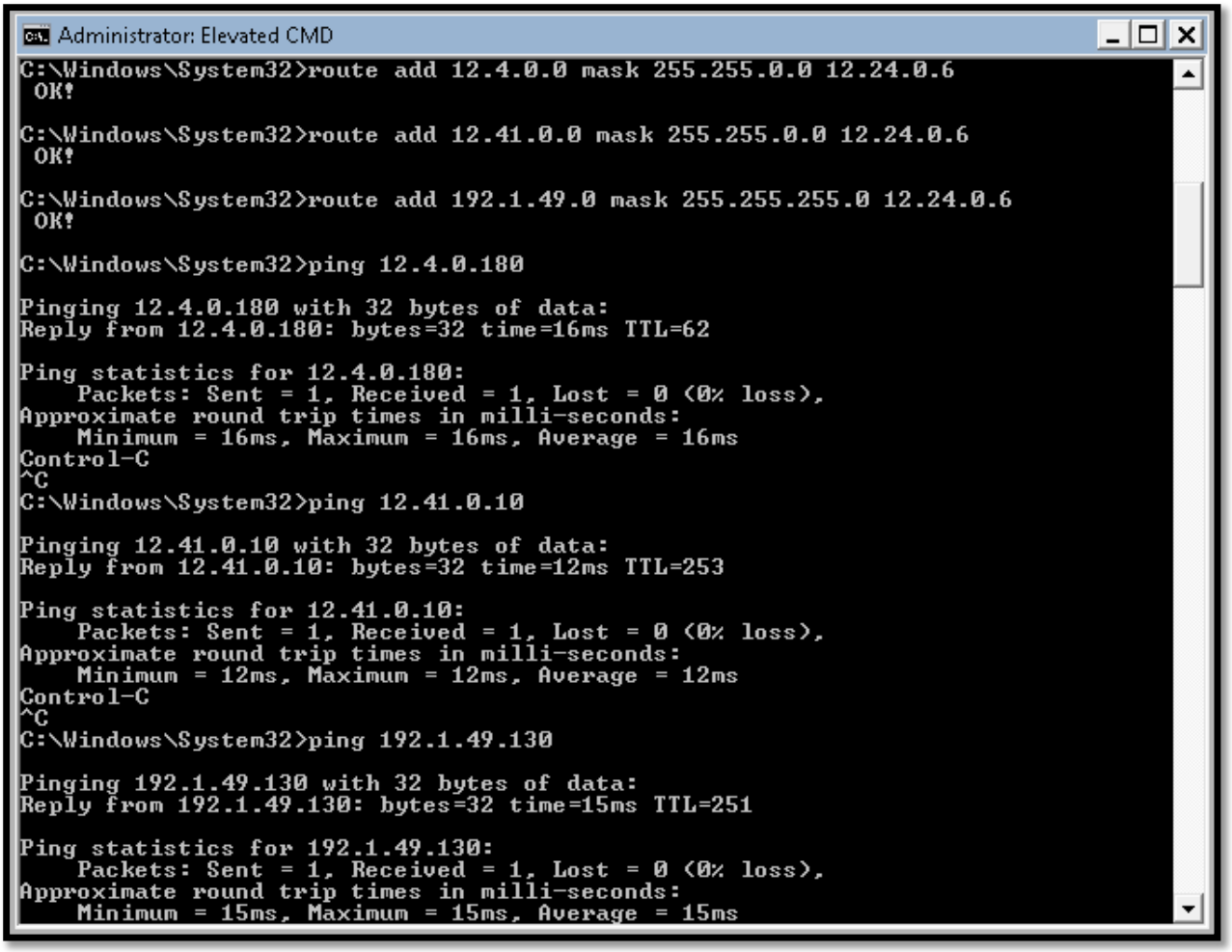
And finally we want to make sure WSA knows how to reach clients in VLAN 24 (Network -> Routes) :



Remember all Policy Settings are by default inherited from the Global Policy. Whenever you want to modify those, you need to select “Customize” option from the drop down menu for a particular Security Component.

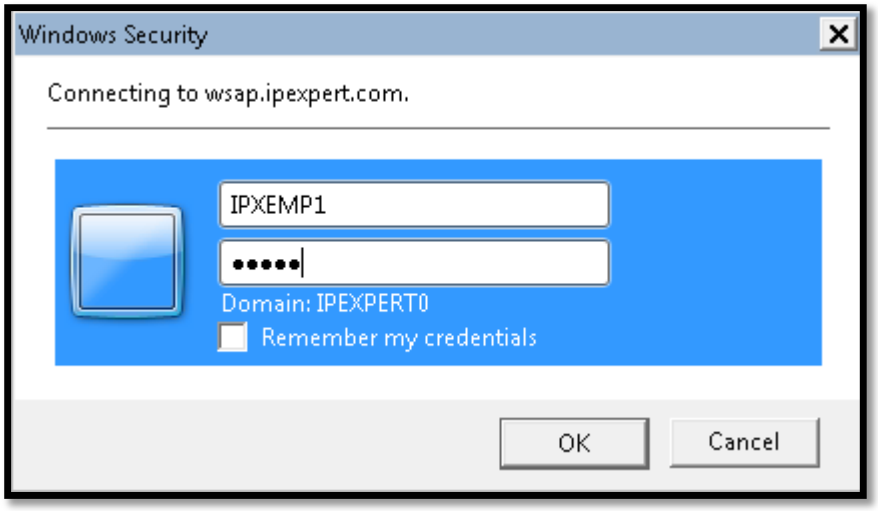
Verification

On the Test PC configure IP address from VLAN 24, add routes and then 4 entries to the Windows hosts file :




```
12.4.0.180 wsap.ipexpert.com
12.41.0.10 www.guestportal.com
192.1.49.99 cciesec.ipexpert.com
192.1.49.130 www.facebook.com
```

Technically speaking it for the ipexpert.com domain it can be any IP address that is reachable via the ASA (so traffic gets redirected) and it can be any hostname (here it is “cciesec”). Now try to connect to www.facebook.com :



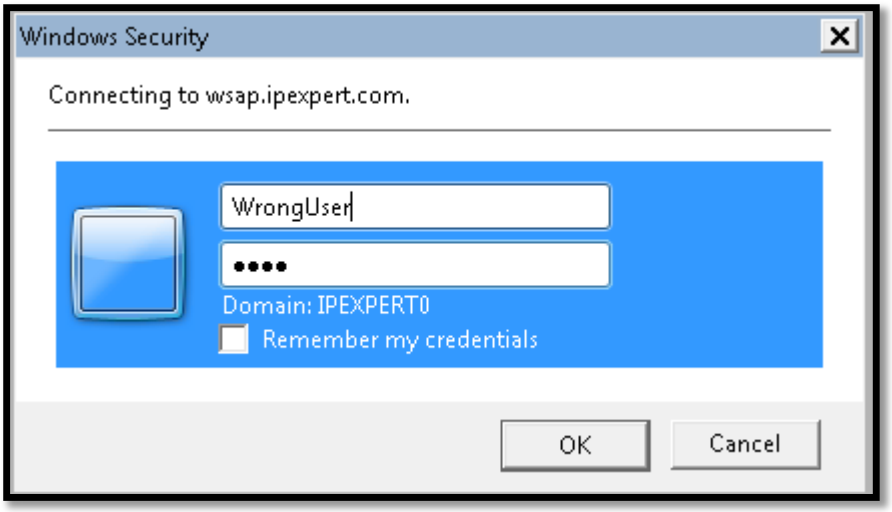

```
1370379983.640 13 12.24.0.200 TCP_MISS/401 247 GET
http://www.facebook.com/ "IPEXPERT0\ipxemp1@ADServer"
DIRECT/www.facebook.com - ALLOW_WBRS_11-Employees_Policy_VLAN24-
EmployeesVLAN24-NONE-NONE-NONE-DefaultGroup <IW_snet,7.0,"1","-",-,-,-,"-
","-",-,-,-,"-","-",-,"-","-",-,-,IW_snet,-,"-","-","Unknown","Unknown","-
","-",152.00,0,-,"-","-"> -
```

```
wsa.ipexpert.com> authcache
```

```
Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
[]> list

List may print a lot of entries. Are you sure? [Y]> y

IPEXPERT0\ipxemp1@ADServer


1 entries in authentication cache

Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
```

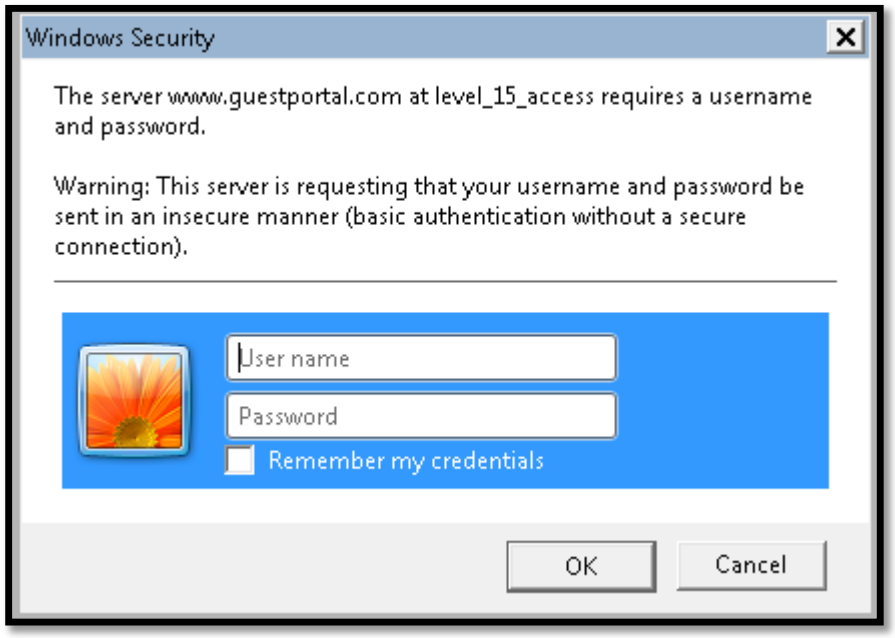
We will now clear authentication cache and fail authentication :

```
wsa.ipexpert.com> authcache


Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
[]> flushall

Are you sure that you want to flush all entries? [Y]> y

1 entries in authentication cache flushed
```




```
1370380162.742 0 12.24.0.200 TCP_DENIED/403 1795 GET
http://www.facebook.com/favicon.ico "(Unauthenticated)WrongUser" NONE/- -
BLOCK_WEBCAT_11-Guests_VLAN24_Policy-EmployeesVLAN24-NONE-NONE-NONE-NONE
<IW_snet,7.0,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,IW_snet,-
,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-">


wsa.ipexpert.com> authcache


Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
[]> list

List may print a lot of entries. Are you sure? [Y]> y

(Unauthenticated)WrongUser@__guest_realm__

1 entries in authentication cache
```

Since we are now "authenticated" as a Guest we will test two remaining things – www.guestportal.com and redirection :



Note WBRS was not checked for this site – access is allowed based on Custom Category we have created and the "Allow" action :

```
1370380320.302 90 12.24.0.200 TCP_MISS/401 247 GET
http://www.guestportal.com/ "(Unauthenticated)WrongUser"
DIRECT/www.guestportal.com - ALLOW_CUSTOMCAT_11-Guests_VLAN24_Policy-
EmployeesVLAN24-NONE-NONE-NONE-DefaultGroup <C_Gues,-,"-","-",-,-,-,"-","-
",-,-,-,"-","-",-,"-","-",-,-,-,-,"-","-","-","-","-","-",21.96,0,-,"-","-
"> -
```

And http://cciesec.ipexpert.com is blocked because 192.1.49.130 (redirected URL; original packet was sent to 192.1.49.99 according to the DNS entry on the Test PC) is Uncategorized which is blocked as well.

This Page Cannot Be Displayed

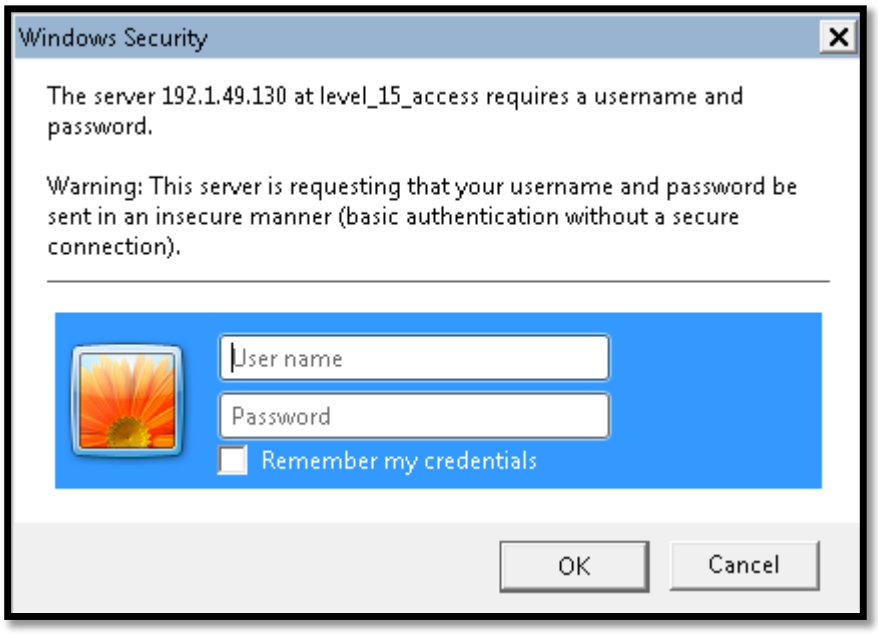
Based on your corporate access policies, access to this web site (http://192.1.49.130/) has been blocked because the web category "Uncategorized URLs" is not allowed.
If you have questions, please contact your corporate network administrator and provide the codes shown below.

Notification codes: (1, WEBCAT, BLOCK-WEBCAT, 0x0000002b, 1370380499.517, QAAAAQAAAAAAAAAAQQEAEAEAAAABAAAAAQAAQAAAAAE=, http://192.1.49.130/)

```
1370380499.341 0 12.24.0.200 TCP_DENIED/302 1693 GET
http://cciesec.ipexpert.com/ "(Unauthenticated)WrongUser" NONE/- -
REDIRECT_CUSTOMCAT_11-Guests_VLAN24_Policy-EmployeesVLAN24-NONE-NONE-NONE-
```

```
NONE <C_ipex,-,"-","-",-,-,-,"-","-",-,-,-,"-","-",-,"-","-",-,-,-,-,"-
","-","-","-","-","-",0.00,0,-,"-","-"> -
```

Temporarily enable Uncategorized URLs and re-test :




```
1370380709.270 16 12.24.0.200 TCP_MISS/401 247 GET http://192.1.49.130/
"(Unauthenticated)WrongUser" DIRECT/192.1.49.130 text/plain
DEFAULT_CASE_11-Guests_VLAN24_Policy-EmployeesVLAN24-NONE-NONE-NONE-
DefaultGroup <nc,-3.5,"1","-",-,-,-,"1","-",-,-,-,"-","1",-,"-","-",-,-
,nc,nc,"-","-","Unknown","Unknown","-","-",123.50,0,-,"-","-"> -
```

4.0 Cisco VPN Solutions (26 points)

Task 4.1: GET VPN Key Server (5 Points)

- Configure R1 as the GET VPN Key Server
- R6, R5, and R4 should register with this server
- The Policy should Apply Encryption to traffic that flows from 10.66.x.x to 10.66.x.x and to 172.27.x.x (as well as between 172.27.x.x)
- Rekey Using Multicast Group address 239.1.66.66
- You may add a tunnel interface on R1 using the IP address 10.101.101.1 if needed
- The Replay Counter Window size should be set to 64
- Use Pre-shared keys for ISAKMP. You may use a wildcard for the address on the KS only
- The ISAKMP & IPSec Policies should reflect the following :
  - ISAKMP AES 128 encryption
  - ISAKMP DH Group 2
  - IPSec AES 128 encryption
  - IPSec MD5 Hash
- Use ASA3 for access to the Key Server

Detailed Solution

R1

```
cry key gen rsa lab GETKEY mod 1024

crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2

crypto isakmp keepalive 15 periodic

crypto keyring GET
  pre-shared-key address 0.0.0.0 0.0.0.0 key ipexpert

crypto isakmp profile GET_PROF
   match identity address 0.0.0.0
```

```
    keyring GET

ip access-list extended GET_ENCRYPT
 permit ip 10.66.0.0 0.0.255.255 10.66.0.0 0.0.255.255
 permit ip 10.66.0.0 0.0.255.255 172.27.0.0 0.0.255.255
 permit ip 172.27.0.0 0.0.255.255 10.66.0.0 0.0.255.255
 permit ip 172.27.0.0 0.0.255.255 172.27.0.0 0.0.255.255

ip access-list extended GET_REKEY
 permit ip host 1.1.1.1 host 239.1.66.66

crypto ipsec transform-set GETSET esp-aes esp-md5-hmac

crypto ipsec profile GET_PROF
 set transform-set GETSET
 set isakmp-profile GET_PROF

crypto gdoi group GET
 identity number 1
 server local
  rekey address ipv4 GET_REKEY
  rekey authentication mypubkey rsa GETKEY
  sa ipsec 1
   profile GET_PROF
   match address ipv4 GET_ENCRYPT
   replay counter window-size 64

ip multicast-routing

interface Loopback0
 ip pim sparse-mode

interface Tunnel100
 ip address 10.101.101.1 255.255.255.0
 ip pim sparse-mode
 tunnel source Loop0
 tunnel destination 12.24.0.6

ip pim rp-address 1.1.1.1
```

ASA3

```
access-list OUTSIDE_IN per gre host 12.24.0.6 host 1.1.1.1
```

Reading ahead we know the GMs are already configured but the Key Server is not. In configuring the Key Server you may create a GRE tunnel between R6 and R1 since there is an ASA in the path and we are doing multicast rekeying (the other solution is to configure ASA for multicast).

Verification

Verification is done in the next task.

Task 4.2: GETVPN over DMVPN Troubleshooting (5 Points)

- R6 is a DMVPN Hub
- R5 and R4 are DMVPN Spokes
- R6, R5, and R4 are all GET VPN Group Members
- R1 is the KS that was configured in the last task
- You can add a single static route in this task
- Fix any issues with the GET VPN or DMVPN Configuration on the Group Members such that you obtain the following results :

```
R1#sh cry gdoi
GROUP INFORMATION

    Group Name               : GET (Multicast)
    Group Identity           : 1
    Group Members            : 3
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 83725 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : GET_PROF
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 926 secs
      ACL Configured         : access-list
GET_ENCRYPT

     Group Server list       : Local
```

```
R1#sh cry gdoi ks mem

Group Member Information :

Number of rekeys sent for group GET : 0

Group Member ID    : 12.64.65.4
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 12.64.65.5
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 12.64.65.6
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0
```

```
R6#sh cry gdoi gm

Group Member Information For Group GET:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GET_temp_acl

    Group member            : 12.64.65.6       vrf:
None
        Registration status   : Registered
        Registered with       : 1.1.1.1
        Re-registers in       : 3418 sec
        Succeeded registration: 1
        Attempted registration: 1
        Last rekey from       : 1.1.1.1
        Last rekey seq num    : 0
        Multicast rekey rcvd  : 2
```

```
R5#sh cry gdoi gm acl
Group Name: GET
 ACL Downloaded From KS 1.1.1.1:
   access-list  permit ip 10.66.0.0 0.0.255.255 10.66.0.0
0.0.255.255
   access-list  permit ip 10.66.0.0 0.0.255.255 172.27.0.0
0.0.255.255
   access-list  permit ip 172.27.0.0 0.0.255.255 10.66.0.0
0.0.255.255
   access-list  permit ip 172.27.0.0 0.0.255.255 172.27.0.0
0.0.255.255

 ACL Configured Locally:
```

```
R4#sh cry gd gm

Group Member Information For Group GET:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GET_temp_acl

    Group member             : 12.64.65.4       vrf:
None
       Registration status   : Registered
       Registered with       : 1.1.1.1
       Re-registers in       : 3393 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 1.1.1.1
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 2
```

Detailed Solution

ASA3

```
route inside 1.1.1.1 255.255.255.255 10.2.2.1 1

router ospf 2
 redistribute static subnets

access-list OUTSIDE_IN permit udp host 12.64.65.6 host 1.1.1.1 eq 848
access-list OUTSIDE_IN permit udp host 12.64.65.5 host 1.1.1.1 eq 848
access-list OUTSIDE_IN permit udp host 12.64.65.4 host 1.1.1.1 eq 848
```

R6

```
crypto map GET local-address Serial0/1/0

crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

```
router eigrp 1
 network 10.66.66.0 0.0.0.255
 network 172.27.0.6 0.0.0.0

int tu 654
 ip nhrp map multicast dynamic

ip mroute 1.1.1.1 255.255.255.255 tu100
```

R5

```
crypto map GET local-address Serial0/1/0

int tu 654
 no ip nhrp nhs 172.17.0.6
 ip nhrp nhs 172.27.0.6

router eigrp 1
 network 10.66.55.0 0.0.0.255
 network 172.27.0.5 0.0.0.0

ip mroute 1.1.1.1 255.255.255.255 172.27.0.6
```

R4

```
crypto map GET local-address Serial0/0/0

interface Tunnel654
 ip address 172.27.0.4 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication ipexpert
 ip nhrp map multicast 12.64.65.6
 ip nhrp map 172.27.0.6 12.64.65.6
 ip nhrp network-id 654
 ip nhrp nhs 172.27.0.6
 tunnel source Serial0/0/0
```

```
 tunnel mode gre multipoint

ip mroute 1.1.1.1 255.255.255.255 172.27.0.6
```

Before you start verification make sure devices know how to reach KS (ASA part).

Verification

Before you made the allowances on the ASA3's ACL you should have noticed devices were trying to register using the tunnel address. We need to change the crypto maps to source traffic off the physical interfaces. After this is done we can start testing – here on R6 first :

```
R6#
*Jun  5 09:47:44.977: %CRYPTO-5-GM_REGSTER: Start registration to KS
1.1.1.1 for group GET using address 12.64.65.6
*Jun  5 09:47:44.985: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of
Informational mode failed with peer at 1.1.1.1

R6#sh cry isa pol

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128
bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
--- Omitted ---
```

OK, looks R6 does not have the policy in place. Fix it.

```
*Jun  5 09:50:38.089: %GDOI-5-SA_TEK_UPDATED: SA TEK was updated
*Jun  5 09:50:38.105: %GDOI-5-GM_REGS_COMPL: Registration to KS 1.1.1.1
complete for group GET using address 12.64.65.6
```

Now let's move on to R5 :

```
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
```

And nothing happens. Do we have a crypto map configured and applied?

```
R5#sh cry map
Crypto Map: "GET" idb: Serial0/1/0 local address: 12.64.65.5

Crypto Map "GET" 10 gdoi
        Group Name: GET
            identity number 1
            server address ipv4 1.1.1.1
        Interfaces using crypto map GET:
```

OK, apply the map :

```
*Jun  5 09:52:47.301: %GDOI-5-SA_TEK_UPDATED: SA TEK was updated
*Jun  5 09:52:47.385: %GDOI-5-GM_REGS_COMPL: Registration to KS 1.1.1.1
complete for group GET using address 12.64.65.5
```

Looks good, now R4 :

```
*Jun  5 10:00:48.293: %GDOI-5-SA_TEK_UPDATED: SA TEK was updated
*Jun  5 10:00:48.345: %GDOI-5-GM_REGS_COMPL: Registration to KS 1.1.1.1
complete for group GET using address 12.64.65.4
```

No problems related to GET VPN here. We will now check DMVPN part – back to R6 (Hub):

```
R6#sh ip nhrp br
   Target             Via            NBMA           Mode   Intfc   Claimed
```

```
R5#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
172.27.0.6/32        172.27.0.6      12.64.65.6      static   Tu654   <
>

R4#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
```

Looks like R6 did not get any Registration messages; R4 does not even have a mapping. But we will start on R5 – I want to enable "debug nhrp" to see if Registrations are even sent from R5 :

```
R5#
*Jun  5 09:59:22.685: NHRP: Setting retrans delay to 32 for nhs  dst
172.17.0.6
*Jun  5 09:59:54.017: NHRP: Setting retrans delay to 64 for nhs  dst
172.17.0.6
```

OK it says it is retransmitting but to 172.17.0.6 – wrong IP. Correct this.

```
R6#sh ip nhrp br
   Target             Via             NBMA           Mode   Intfc   Claimed
172.27.0.5/32        172.27.0.5      12.64.65.5      dynamic  Tu654   <
>
```

So what about R4?

```
R4#sh ip nhrp traffic

R4#sh run int tu 654
Building configuration...

Current configuration : 80 bytes
!
interface Tunnel654
 ip address 172.27.0.4 255.255.255.0
 crypto map GET
```

Copy config from R5 to notepad and change IP address to fit R4.

```
R6#sh ip nhrp br
```

```
   Target             Via             NBMA            Mode   Intfc   Claimed
172.27.0.4/32        172.27.0.4      12.64.65.4       dynamic  Tu654   <
>
172.27.0.5/32        172.27.0.5      12.64.65.5       dynamic  Tu654   <
>
```

Much better.

```
R6#ping 172.27.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

R6#ping 172.27.0.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.0.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/62/64 ms

R6#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: Tunnel654
Uptime: 00:18:21
Session status: UP-ACTIVE
Peer: 0.0.0.0 port 848 fvrf: (none) ivrf: (none)
      Phase1_id: 1.1.1.1
      Desc: (none)
  IKEv1 SA: local 12.64.65.6/848 remote 1.1.1.1/848 Active
          Capabilities:(none) connid:1001 lifetime:23:41:38
  IKEv1 SA: local 239.1.66.66/0 remote 1.1.1.1/848 Active
          Capabilities:(none) connid:1002 lifetime:6w3d
```

```
  IPSEC FLOW: permit ip 172.27.0.0/255.255.0.0 10.66.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
  IPSEC FLOW: permit ip 10.66.0.0/255.255.0.0 172.27.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
  IPSEC FLOW: permit ip 172.27.0.0/255.255.0.0 172.27.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
        Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
  IPSEC FLOW: permit ip 10.66.0.0/255.255.0.0 10.66.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey
Disabled/2498

R5#ping 172.27.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/36 ms
```

So the tunnel networks are protected. Now we want to make sure 10.66.0.0 is protected as well, that rekey is working and that the verification outputs match. If you go over the interfaces for 10.66 you will notice R4 uses 10.66.44.0/24, R5 10.66.55.0/24 and R6 10.66.66.0/24 :

```
R6#sh ip int br | in 10.66
Loopback55                10.66.66.6      YES manual up
up

R6#sh ip ro 10.66.44.4
```

```
% Subnet not in table
```

But only R4 tries to advertise this prefix using EIGRP :

```
R4#sh run | s router
router eigrp 1
 network 10.66.44.0 0.0.0.255
 network 172.27.0.4 0.0.0.0
router eigrp 4
 network 12.4.0.4 0.0.0.0
 redistribute ospf 1 metric 1 1 1 1 1
router ospf 1
 redistribute eigrp 4 subnets
 network 4.0.0.0 0.255.255.255 area 2
 network 12.64.65.0 0.0.0.255 area 2
ipv6 router eigrp 12
 redistribute static metric 1 1 1 1 1
```

Enable EIGRP 1 on R5 and R6 and test.

```
R6#
*Jun  5 10:23:25.277: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.27.0.4
(Tunnel654) is up: new adjacency
*Jun  5 10:23:32.145: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.27.0.5
(Tunnel654) is up: new adjacency

R6#sh ip ro eigrp | be Gate
Gateway of last resort is not set

R5#sh ip route eigrp 1 | be Gate
Gateway of last resort is not set

R4#sh ip eigrp 1 int
EIGRP-IPv4 Interfaces for AS(1)
                       Xmit Queue   Mean   Pacing Time   Multicast
Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer
Routes
Tu654              0        0/0         0       6/6            0
0
```

```
Lo55                0         0/0           0        0/1               0
0
```

No routes on the Hub and Spokes even that EIGRP is running on the loopbacks as well. And in addition to that it looks like Hub has some problems with the adjacencies :

```
R6#
*Jun  5 10:26:04.461: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.27.0.4
(Tunnel654) is down: retry limit exceeded
*Jun  5 10:26:06.329: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.27.0.4
(Tunnel654) is up: new adjacency

R6#sh ip ei ne
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
0   172.27.0.4              Tu654             11 00:00:08    1  4500  1  0
1   172.27.0.5              Tu654             14 00:01:18    1  5000  1  0

R6#sh run int tu 654
Building configuration...

Current configuration : 307 bytes
!
interface Tunnel654
 ip address 172.27.0.6 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication ipexpert
 ip nhrp network-id 654
 ip nhrp redirect
 no ip split-horizon eigrp 1
 tunnel source Serial0/1/0
 tunnel mode gre multipoint
 crypto map GET
```

One command related to multicasts is missing here (“ip nhrp map multicast dynamic”). When you add it and shut/no shut tunnels routes should start being received :

```
R5#sh ip ro ei | be Gate
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D        10.66.44.0/24 [90/28288000] via 172.27.0.6, 00:00:42, Tunnel654
D        10.66.66.0/24 [90/27008000] via 172.27.0.6, 00:00:44, Tunnel654

R4#sh ip route eigrp 1 | be Gate
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D        10.66.55.0/24 [90/28288000] via 172.27.0.6, 00:01:09, Tunnel654
D        10.66.66.0/24 [90/27008000] via 172.27.0.6, 00:01:09, Tunnel654

R4#ping 10.66.66.6 so l55

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.66.66.6, timeout is 2 seconds:
Packet sent with a source address of 10.66.44.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/36 ms

R4#ping 10.66.55.5 so l55

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.66.55.5, timeout is 2 seconds:
Packet sent with a source address of 10.66.44.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/93/96 ms
```

Data Plane is fine. What’s left is GET VPN Control Plane (Rekeys) and verification outputs.

```
R6#sh ip pim ne
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
```

```
Neighbor          Interface                Uptime/Expires    Ver   DR
Address
Prio/Mode
172.27.0.4        Tunnel654                00:09:30/00:01:34 v2    1 / S P
G
172.27.0.5        Tunnel654                00:09:36/00:01:31 v2    1 / S P
G
10.101.101.1      Tunnel100                00:01:29/00:01:44 v2    1 / S P
G
```

All the PIM adjacencies are through the tunnel. Rekeys will be sent from 1.1.1.1 so we want to make sure routers will accept them :

```
R6#sh ip ro 1.1.1.1
Routing entry for 1.1.1.1/32
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward
metric 1
  Last update from 12.24.0.30 on FastEthernet0/1, 01:06:36 ago
  Routing Descriptor Blocks:
  * 12.24.0.30, from 10.2.2.30, 01:06:36 ago, via FastEthernet0/1
      Route metric is 20, traffic share count is 1

R5#sh ip ro 1.1.1.1
Routing entry for 1.1.1.1/32
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward
metric 65
  Last update from 12.64.65.6 on Serial0/1/0, 01:06:42 ago
  Routing Descriptor Blocks:
  * 12.64.65.6, from 10.2.2.30, 01:06:42 ago, via Serial0/1/0
      Route metric is 20, traffic share count is 1
```

R1 loopback is obviously reachable via the physical ports so RPF will fail. Fix with mroutes (only unicast static routes were prohibited).

```
R6(config)#do sh ip rpf 1.1.1.1
RPF information for ? (1.1.1.1)
  RPF interface: Tunnel100
  RPF neighbor: ? (10.101.101.1)
  RPF route/mask: 1.1.1.1/32
  RPF type: multicast (static)
```

```
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base

R4(config)#do sh ip rpf 1.1.1.1
RPF information for ? (1.1.1.1)
  RPF interface: Tunnel654
  RPF neighbor: ? (172.27.0.6)
  RPF route/mask: 1.1.1.1/32
  RPF type: multicast (static)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base
```

All DMVPN routers received rekey :

```
*Jun  5 10:54:25.073: %GDOI-5-GM_RECV_REKEY: Received Rekey for group GET
from 1.1.1.1 to 239.1.66.66 with seq # 3
```

```
R1#sh cry gdoi
GROUP INFORMATION

    Group Name               : GET (Multicast)
    Group Identity           : 1
    Group Members            : 3
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 83725 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : GET_PROF
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
```

```
          Remaining Lifetime  : 926 secs
       ACL Configured         : access-list GET_ENCRYPT

     Group Server list        : Local


R1#sh cry gdoi ks mem

Group Member Information :

Number of rekeys sent for group GET : 0

Group Member ID    : 12.64.65.4
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 12.64.65.5
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 12.64.65.6
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

R6#sh cry gdoi gm

Group Member Information For Group GET:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GET_temp_acl

    Group member             : 12.64.65.6       vrf: None
       Registration status   : Registered
       Registered with       : 1.1.1.1
       Re-registers in       : 3418 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 1.1.1.1
```

```
        Last rekey seq num    : 0
        Multicast rekey rcvd  : 2

R5#sh cry gdoi
GROUP INFORMATION

    Group Name               : GET
    Group Identity           : 1
    Rekeys received          : 2
    IPSec SA Direction       : Both

     Group Server list       : 1.1.1.1

    Group member             : 12.64.65.5       vrf: None
       Registration status   : Registered
       Registered with       : 1.1.1.1
       Re-registers in       : 3405 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 1.1.1.1
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 2
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 2
       After latest register : 2
       Rekey Rcvd(hh:mm:ss)  : 00:00:48

 ACL Downloaded From KS 1.1.1.1:
   access-list  permit ip 10.66.0.0 0.0.255.255 10.66.0.0 0.0.255.255
   access-list  permit ip 10.66.0.0 0.0.255.255 172.27.0.0 0.0.255.255
   access-list  permit ip 172.27.0.0 0.0.255.255 10.66.0.0 0.0.255.255
   access-list  permit ip 172.27.0.0 0.0.255.255 172.27.0.0 0.0.255.255

KEK POLICY:
    Rekey Transport Type     : Multicast
    Lifetime (secs)          : 86400
```

```
      Encrypt Algorithm        : 3DES
      Key Size                 : 192
      Sig Hash Algorithm       : HMAC_AUTH_SHA
      Sig Key Length (bits)    : 1024

  TEK POLICY for the current KS-Policy ACEs Downloaded:
    Tunnel654:
      IPsec SA:
          spi: 0x1A63973D(442734397)
          transform: esp-aes esp-md5-hmac
          sa timing:remaining key lifetime (sec): (3491)
          Anti-Replay :  Disabled

      IPsec SA:
          spi: 0x36C76E01(919039489)
          transform: esp-aes esp-md5-hmac
          sa timing:remaining key lifetime (sec): (3507)
          Anti-Replay :  Disabled

      IPsec SA:
          spi: 0x961E72C(157411116)
          transform: esp-aes esp-md5-hmac
          sa timing:remaining key lifetime (sec): (3551)
          Anti-Replay :  Disabled

  R4#sh cry gd gm

  Group Member Information For Group GET:
      IPSec SA Direction       : Both
      ACL Received From KS     : gdoi_group_GET_temp_acl

      Group member             : 12.64.65.4       vrf: None
         Registration status   : Registered
         Registered with       : 1.1.1.1
         Re-registers in       : 3393 sec
         Succeeded registration: 1
         Attempted registration: 1
         Last rekey from       : 1.1.1.1
         Last rekey seq num    : 0
         Multicast rekey rcvd  : 2
```

Task 4.3: IKEv2 L2L (5 Points)

- Configure a site-to-site VPN tunnel between ASA3 and ASA4
- Use the new version of IKE protocol for negotiation
- Protect VLANs 20, 100 and 41
- Use SHA-256 for IKE tunnel and SHA-1 to secure data traffic
- Authentication method must be Pre-Shared Key ("ipexpert")
- You can add two static routes on the ASA4
- Block access to WSA M1 interface through the tunnel
- You should be able to ping R1 from R10 after finishing this task

Detailed Solution

R4

```
ip access-list extended ESP
 permit esp any any

class-map type inspect match-all ZFW_IKE_CLASS
 match protocol isakmp
class-map type inspect match-all ZFW_ESP_CLASS
 match access-group name ESP

policy-map type inspect ZFW_OUTIN_POL
 class type inspect ZFW_ESP_CLASS
  pass
 class type inspect ZFW_IKE_CLASS
  inspect

policy-map type inspect ZFW_INOUT_POL
 class type inspect ZFW_ESP_CLASS
  pass
```

ASA3

```
crypto ikev2 policy 40
 encryption aes
 integrity sha256
 group 5
```

```
 prf sha256
 lifetime seconds 86400

access-list VPN_BLOCK deny ip any host 10.1.1.180
access-list VPN_BLOCK permit ip any any

group-policy L2LPOL internal
group-policy L2LPOL attributes
 vpn-filter value VPN_BLOCK

tunnel-group 12.4.0.40 type ipsec-l2l
tunnel-group 12.4.0.40 general-attributes
 default-group-pol L2LPOL
tunnel-group 12.4.0.40 ipsec-attributes
 ikev2 remote-authentication pre-shared-key ipexpert
 ikev2 local-authentication pre-shared-key ipexpert

access-list PROXYACL permit ip 10.1.1.0 255.255.255.0 12.41.0.0
255.255.255.0
access-list PROXYACL permit ip 10.2.2.0 255.255.255.0 12.41.0.0
255.255.255.0

object-group network VPN_NETWORKS
 network-object 12.41.0.0 255.255.255.0
object-group network VPN_INTERNAL
 network-object 10.1.1.0 255.255.255.0
 network-object 10.2.2.0 255.255.255.0

nat (i,o) sou sta VPN_INTERNAL VPN_INTERNAL des sta VPN_NETWORKS
VPN_NETWORKS
```

ASA4

```
crypto ikev2 policy 40
 encryption aes
 integrity sha256
 group 5
 prf sha256
 lifetime seconds 86400

tunnel-group 12.24.0.30 type ipsec-l2l
```

```
tunnel-group 12.24.0.30 ipsec-attributes
 ikev2 remote-authentication pre-shared-key ipexpert
 ikev2 local-authentication pre-shared-key ipexpert

access-list PROXYACL permit ip 12.41.0.0 255.255.255.0 10.1.1.0
255.255.255.0
access-list PROXYACL permit ip 12.41.0.0 255.255.255.0 10.2.2.0
255.255.255.0

crypto ipsec ikev2 ipsec-proposal SET4
 protocol esp encryption aes
 protocol esp integrity sha-1

crypto map MAP1 10 match address PROXYACL
crypto map MAP1 10 set peer 12.24.0.30
crypto map MAP1 10 set ikev2 ipsec-proposal SET4
crypto map MAP1 interface inside
crypto ikev2 enable inside

route inside 10.1.1.0 255.255.255.0 12.4.0.4 1
route inside 10.2.2.0 255.255.255.0 12.4.0.4 1
```

Hopefully you did not forget about R4 being configured as ZFW and PAT being in place on ASA3 for VLAN100. The ACL on R4 for ESP could be more specific – it could only allow ASAs but here we are OK with “any any” (you could also add an ACL to the IKE class to narrow down its scope).

VPN Filter works on the traffic that comes from the tunnel so we block any traffic to 10.1.1.180 on ASA3.

Verification

```
R10#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 80 percent (4/5), round-trip min/avg/max = 28/29/32 ms

ASA4(config)# sh cry ikev2 sa det
```

```
IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status
Role
  4684897         12.4.0.40/500        12.24.0.30/500      READY
INITIATOR
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/86 sec
      Session-id: 4
      Status Description: Negotiation done
      Local spi: DBFAFCCE349CA0F7       Remote spi: E6E7A5102831F257
      Local id: 12.4.0.40
      Remote id: 12.24.0.30
      Local req mess id: 4              Remote req mess id: 2
      Local next mess id: 4             Remote next mess id: 2
      Local req queued: 4               Remote req queued: 2
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  12.41.0.0/0 - 12.41.0.255/65535
          remote selector 10.1.1.0/0 - 10.1.1.255/65535
          ESP spi in/out: 0xb2135338/0xcb374b52
          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 det l2l

Session Type: LAN-to-LAN Detailed

Connection   : 12.4.0.40
Index        : 13                    IP Addr      : 12.4.0.40
Protocol     : IKEv2 IPsec
Encryption   : AES128                Hashing      : SHA256 SHA1
Bytes Tx     : 400                   Bytes Rx     : 400
Login Time   : 14:59:54 UTC Wed Jun 5 2013
```

```
Duration     : 0h:01m:46s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 13.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES128                 Hashing      : SHA256
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86294 Seconds
  PRF          : SHA256                 D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 13.2
  Local Addr   : 10.1.1.0/255.255.255.0/0/0
  Remote Addr  : 12.41.0.0/255.255.255.0/0/0
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28694 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 28 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)   : 107 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :

R10#ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/29/32 ms
```

```
ASA4(config)#sh cry ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:2

Tunnel-id                 Local                 Remote     Status
Role
  4684897         12.4.0.40/500        12.24.0.30/500      READY
INITIATOR
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/249 sec
Child sa: local selector  12.41.0.0/0 - 12.41.0.255/65535
          remote selector 10.2.2.0/0 - 10.2.2.255/65535
          ESP spi in/out: 0xf23e1ba3/0xb0f2be4
Child sa: local selector  12.41.0.0/0 - 12.41.0.255/65535
          remote selector 10.1.1.0/0 - 10.1.1.255/65535
          ESP spi in/out: 0xb2135338/0xcb374b52


R10#ping 10.1.1.180
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.180, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

%ASA-4-106103: access-list VPN_BLOCK denied icmp for user '<unknown>'
outside/12.41.0.10(8) -> inside/10.1.1.180(0) hit-cnt 1 first hit
[0x80b38ae3, 0x0]

R10#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 = 28/29/32 ms
```

Task 4.4: ASA Remote Access VPN (6 Points)

- Configure ASA4 for EasyVPN with external group parameters as follows :
  - DNS Server = 10.1.1.101
  - Tunneling Protocol = IPSec
  - IPSec-Authentication = RADIUS
  - IPSec Banner = "You are on the Private Network!"
  - Split Tunneling for 10.1.1.0/24 and 10.2.2.0/24
  - The user ezuser should be locked into the group EZVPN
  - The address pool should be 10.3.3.10-20 and the assignment of the pool should come from the RADIUS Server (ISE)
  - The external group-policy is EZPOL with password "IPexpert123"
- Create a user on ISE with the username ezuser and password of "IPexpert123"
- All the user VPN attributes should come through RADIUS
- RADIUS traffic should be encrypted and authenticated through the public & WAN networks
- The VPN connections will be coming from the Internet
- You can add one static route for this task

Detailed Solution

ASA4

```
access-list PROXYACL extended permit ip interface inside host 10.1.1.150
access-list PROXYACL per ip 10.3.3.0 255.255.255.224 10.1.1.0
255.255.255.0
access-list PROXYACL per ip 10.3.3.0 255.255.255.224 10.2.2.0
255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.1.1.150
 key ipexpert

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
```

```
access-list SPLIT standard permit 10.1.1.0 255.255.255.0
access-list SPLIT standard permit 10.2.2.0 255.255.255.0

ip local pool EZPOOL 10.3.3.10-10.3.3.20 mask 255.255.255.0

group-policy EZPOL external server-group ISE password IPexpert123

tunnel-group EZVPN type remote-access
tunnel-group EZVPN general-attributes
 authentication-server-group ISE
 default-group-policy EZPOL
tunnel-group EZVPN ipsec-attributes
 pre-shared-key ipexpert

crypto ipsec transform-set SET2 esp-aes esp-sha-hmac

crypto dynamic-map DYNMAP2 1 set transform-set SET2
crypto dynamic-map DYNMAP2 1 set reverse-route

crypto map MAP2 1 ipsec-isakmp dynamic DYNMAP2
crypto map MAP2 interface outside
crypto ikev1 enable outside
```

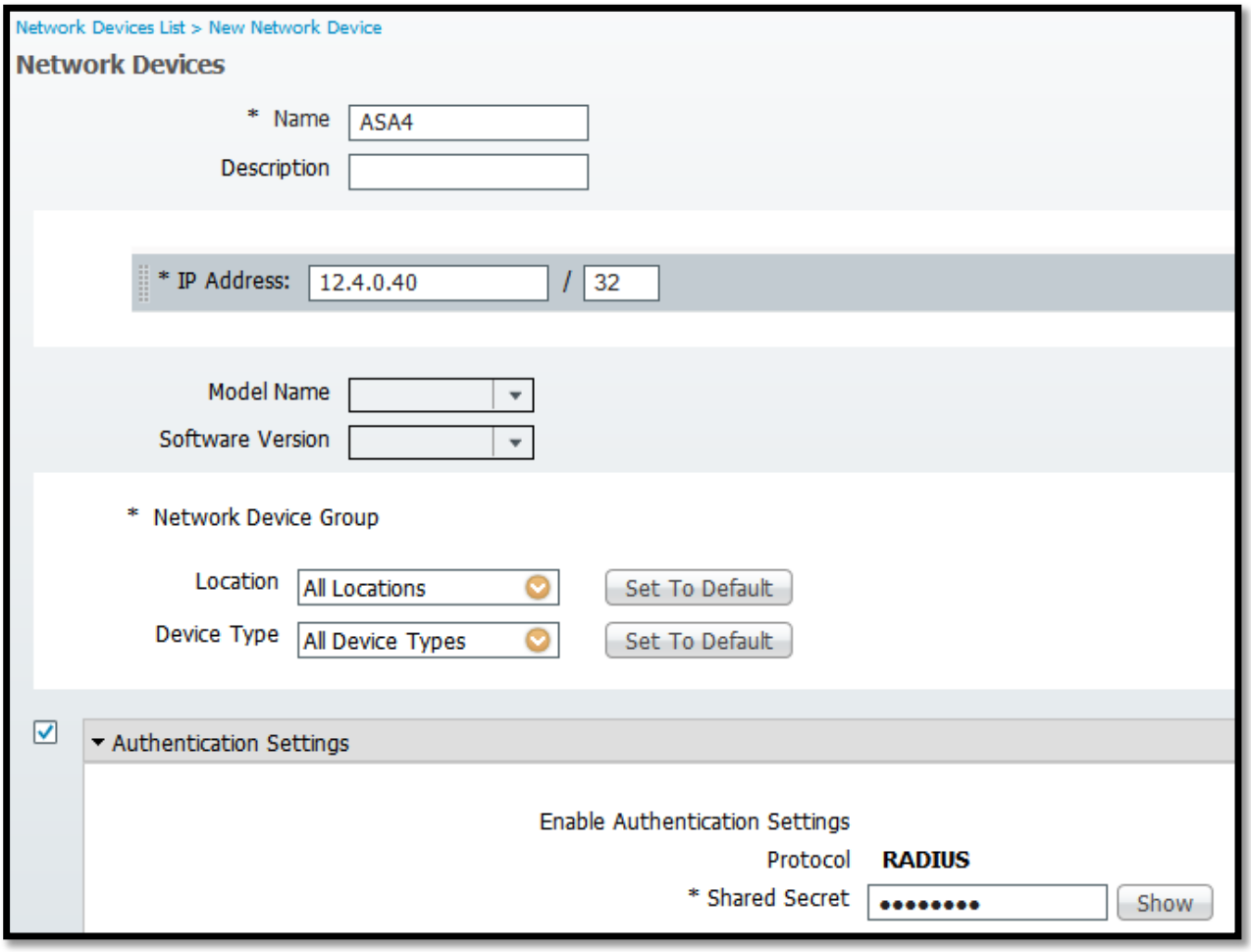
ASA3

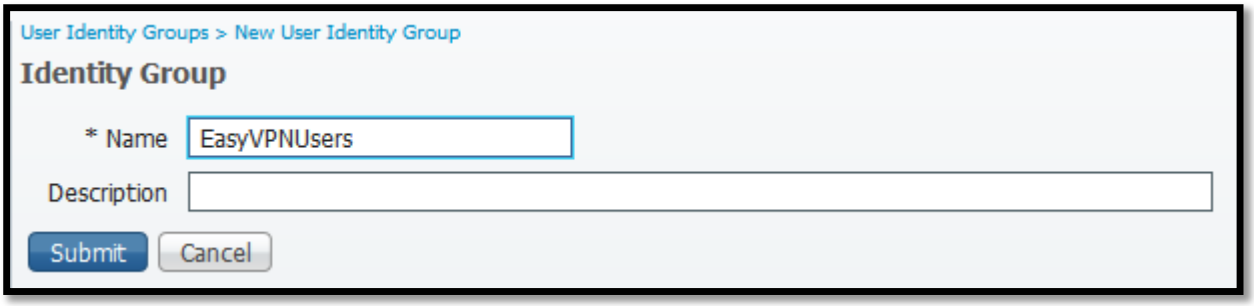
```
access-list PROXYACL per ip host 10.1.1.150 host 12.4.0.40
access-list PROXYACL per ip 10.1.1.0 255.255.255.0 10.3.3.0
255.255.255.224
access-list PROXYACL per ip 10.2.2.0 255.255.255.0 10.3.3.0
255.255.255.224


object-group network VPN_NETWORKS
 network-object host 12.4.0.40
 network-object 10.3.3.0 255.255.255.224

prefix-list VPNNET seq 5 permit 10.3.3.0/27

route-map NOVPN deny 10
```

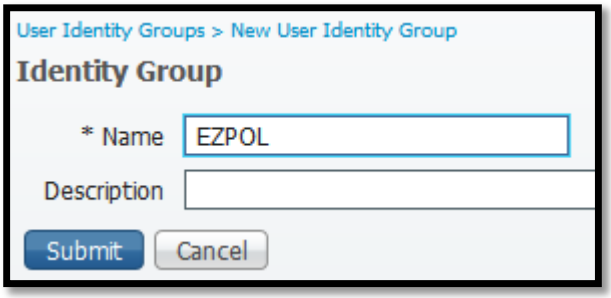
```
 match ip address prefix-list VPNNET
route-map NOVPN permit 20

router ospf 2
 no redi static subnets
 redistribute static subnets route-map NOVPN

route outside 10.3.3.0 255.255.255.224 12.4.0.40 1
```

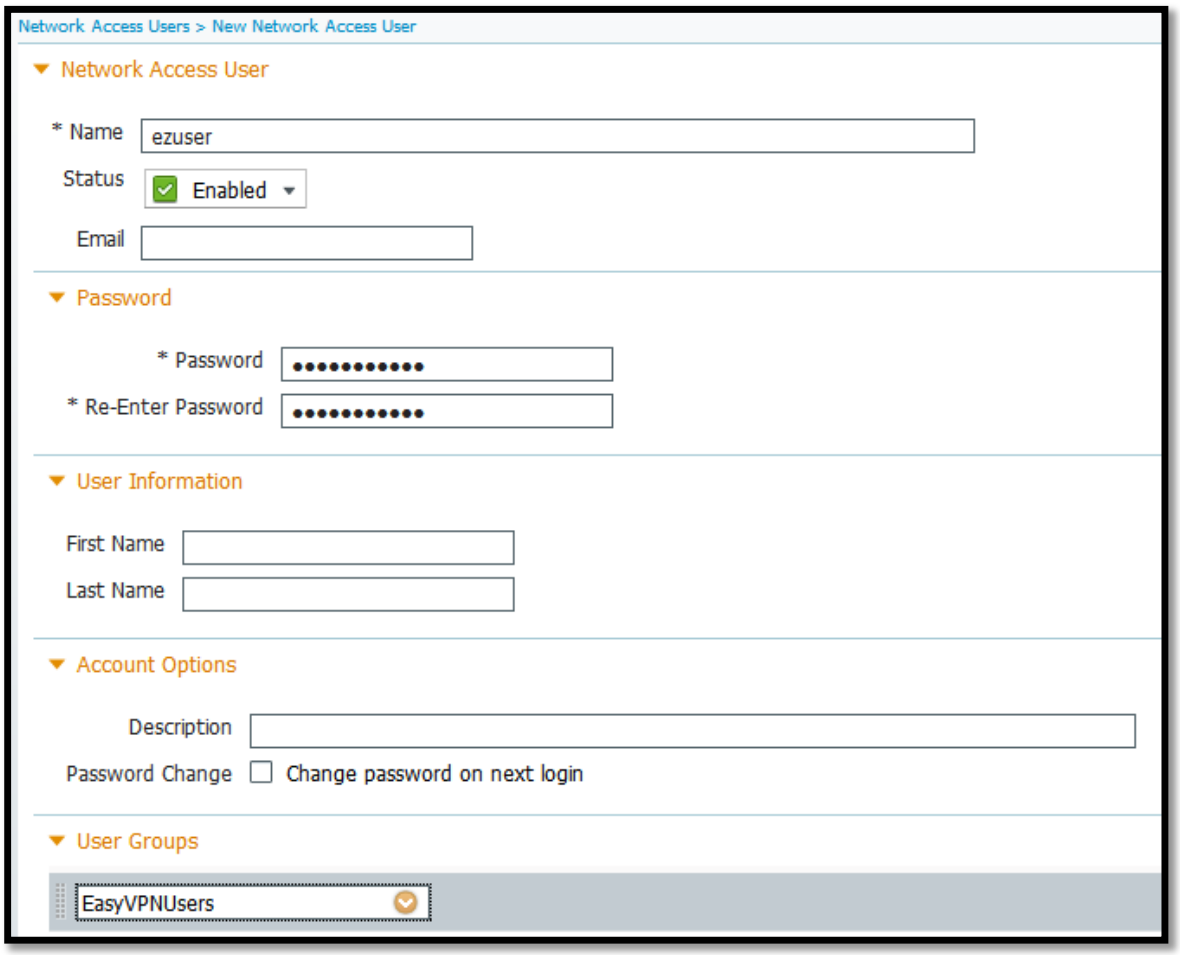
ISE

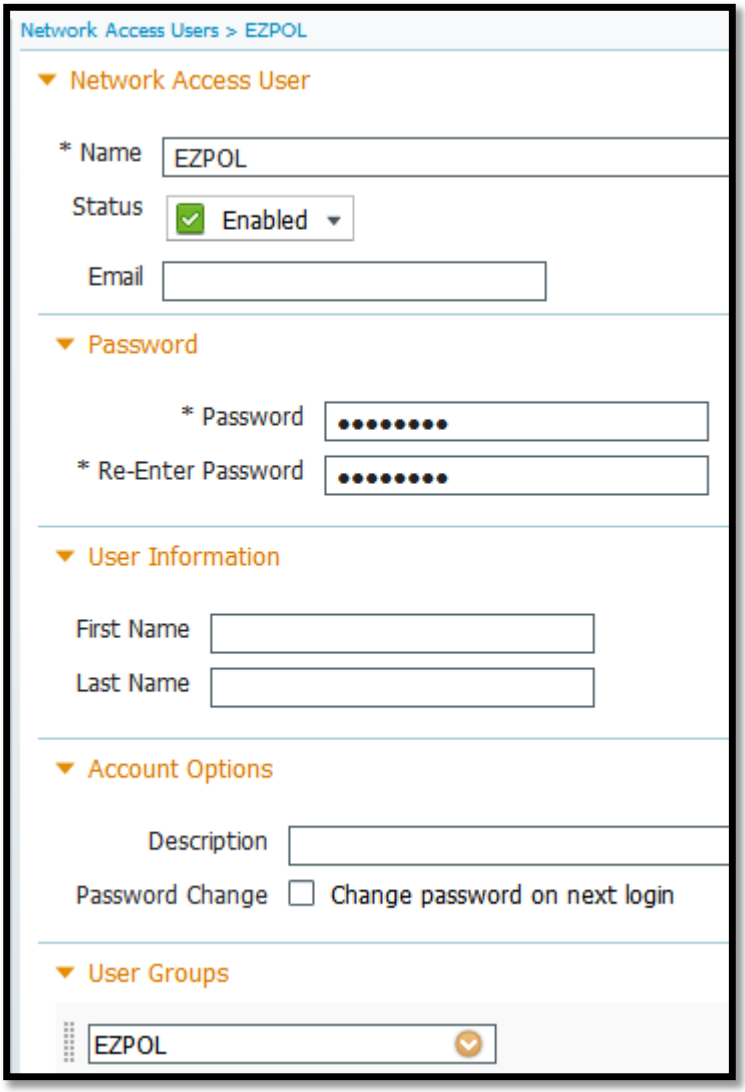
Add ASA4 as a AAA Client, configure groups and users :



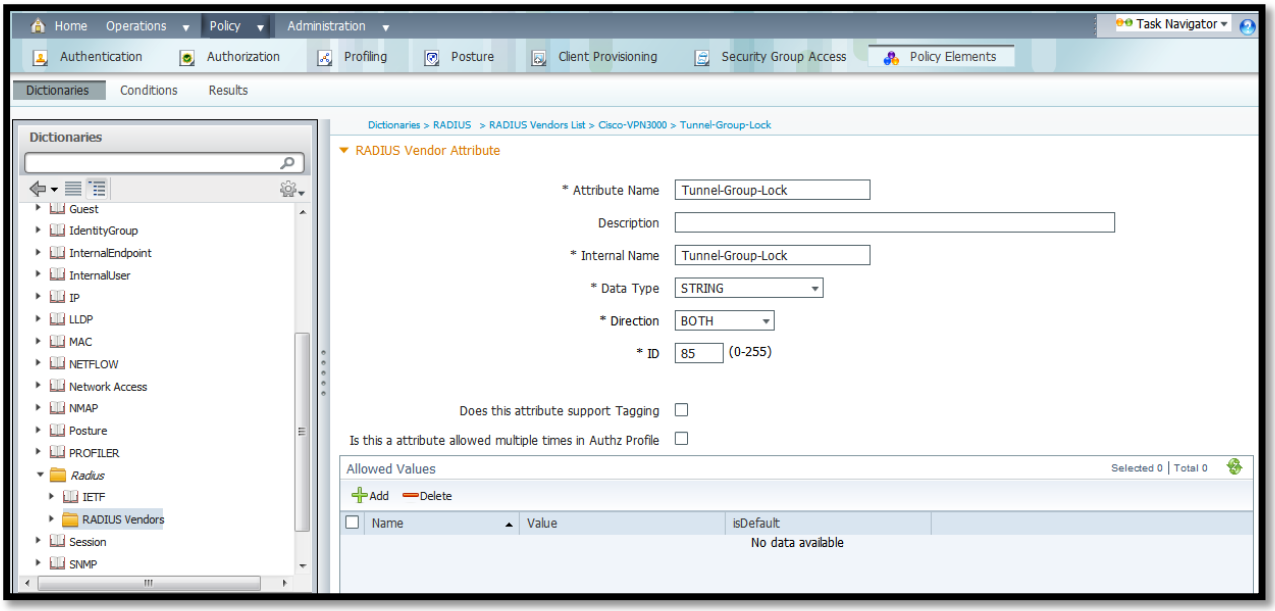


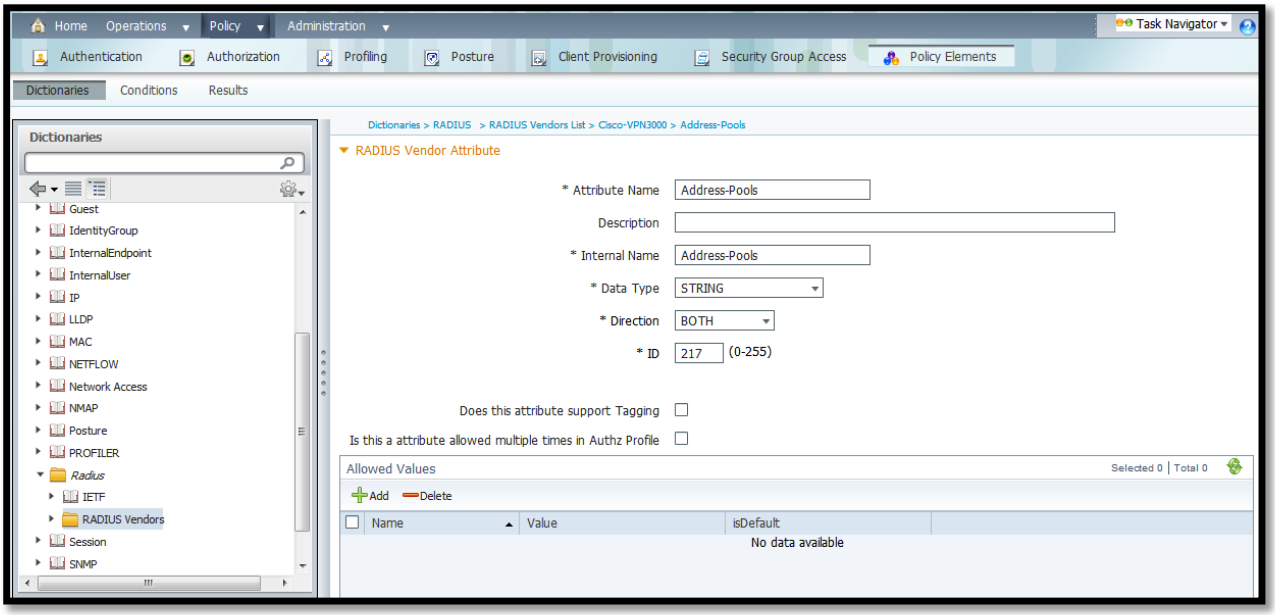




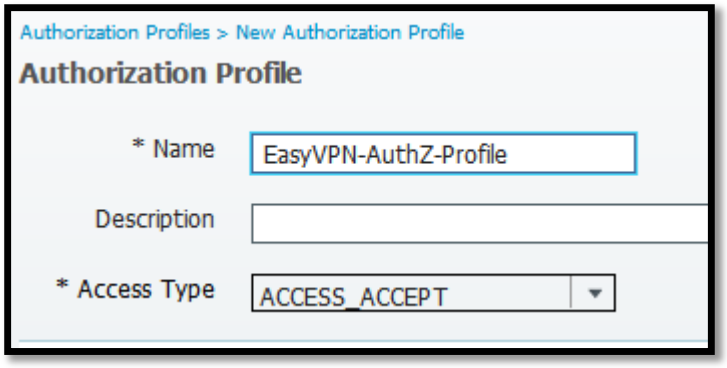


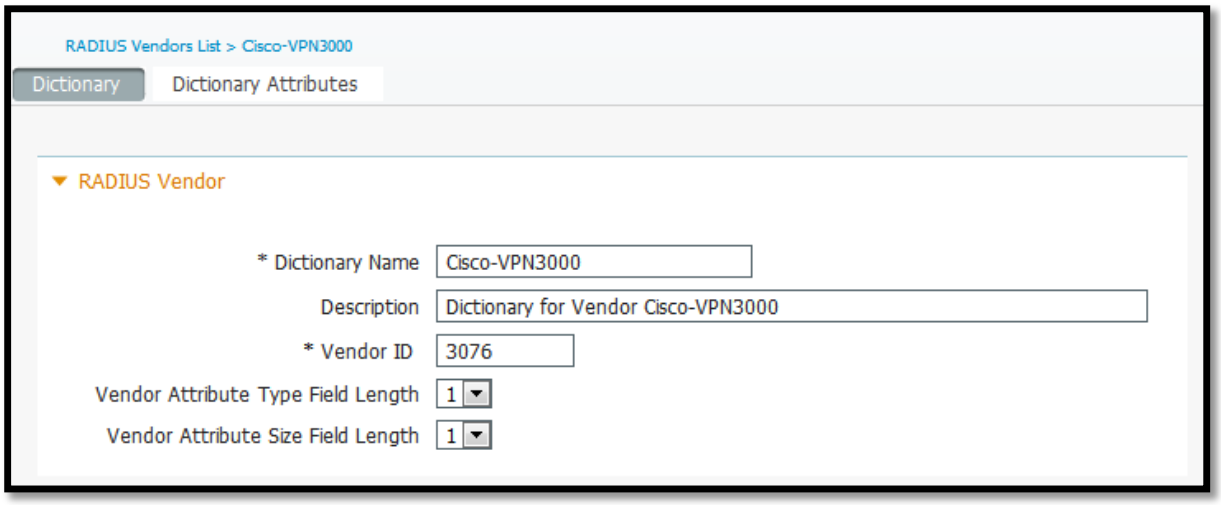
We should now define two missing attributes – Tunnel-Group-Lock and Address-Pools:



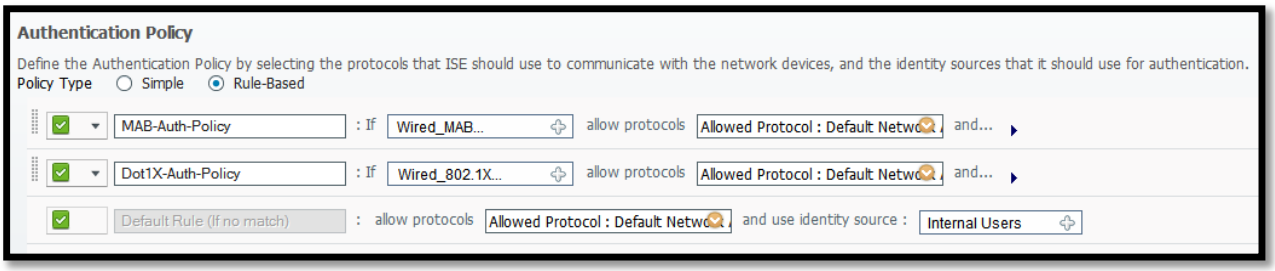


Next we need an AuthZ Profile where we will store all required attributes. This is gonna be VPN300 Dictionary :

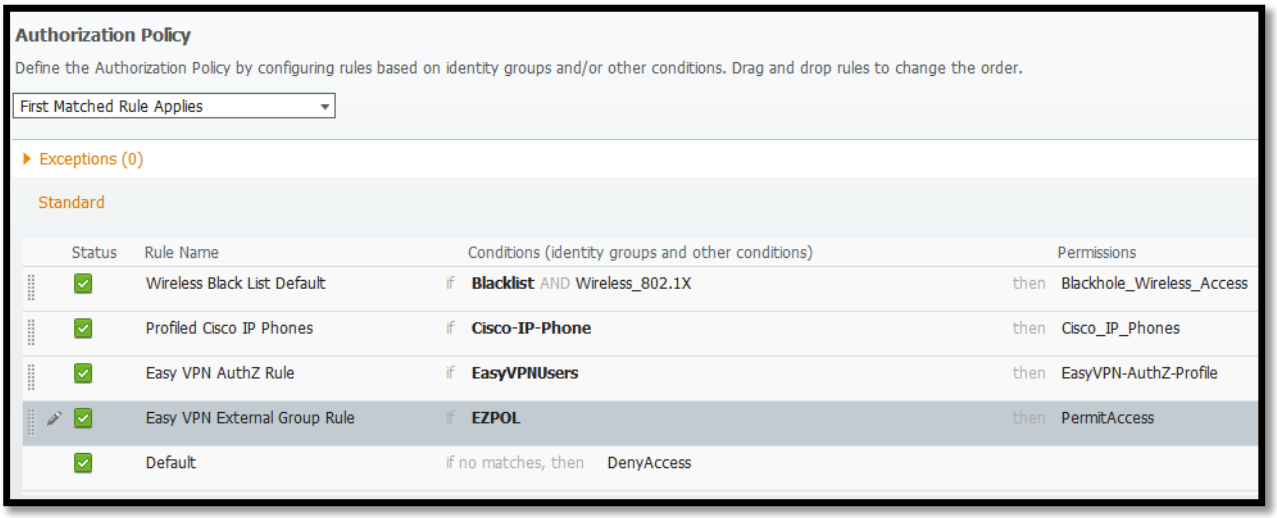




Next comes the Authentication Policy – no modifications are required since Internal User Identity Store is used in the Default Rule that will catch VPN connections :



In the AuthZ Policy we need to create two rules – one for External Group Policy lookup and other for the authenticated user :

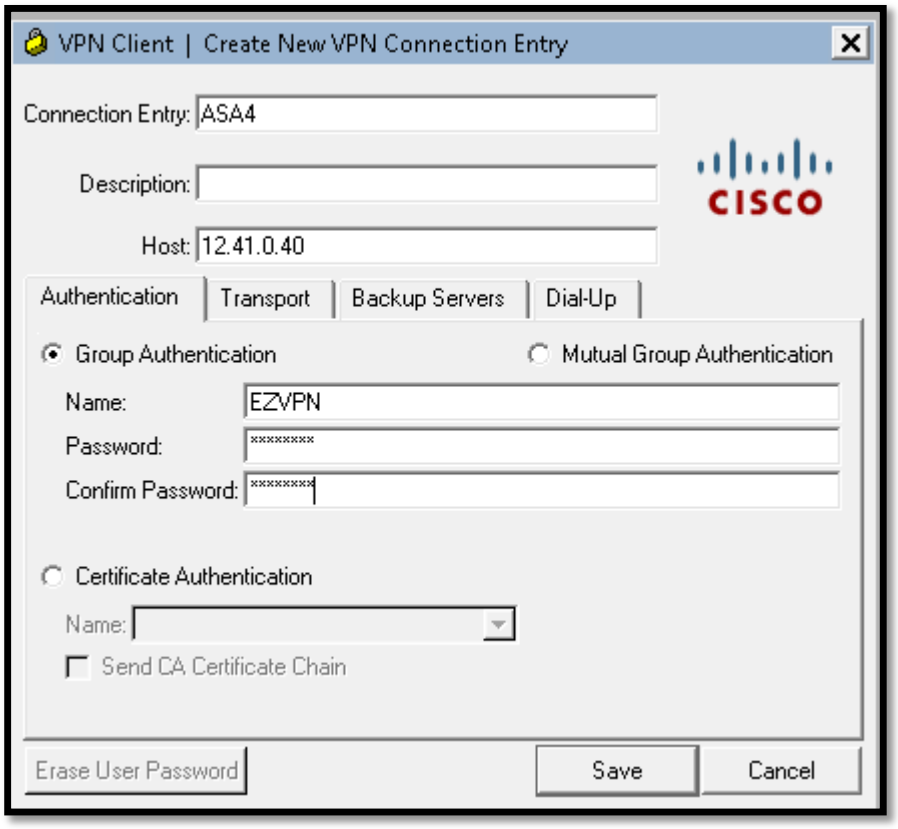


Since we need to use some of the attributes that are not predefined in Cisco's VPN 3000 Dictionary, we need to create them first (this Dictionary will be most useful for any type of RADIUS authorization on the ASA). The full list of RADIUS Authorization attributes for ASA (and their types/numbers) can be found in ASA's documentation under "Reference" -> "Configuring an External Server for Security Appliance User Authorization" -> "ASA RADIUS Authorization Attributes".

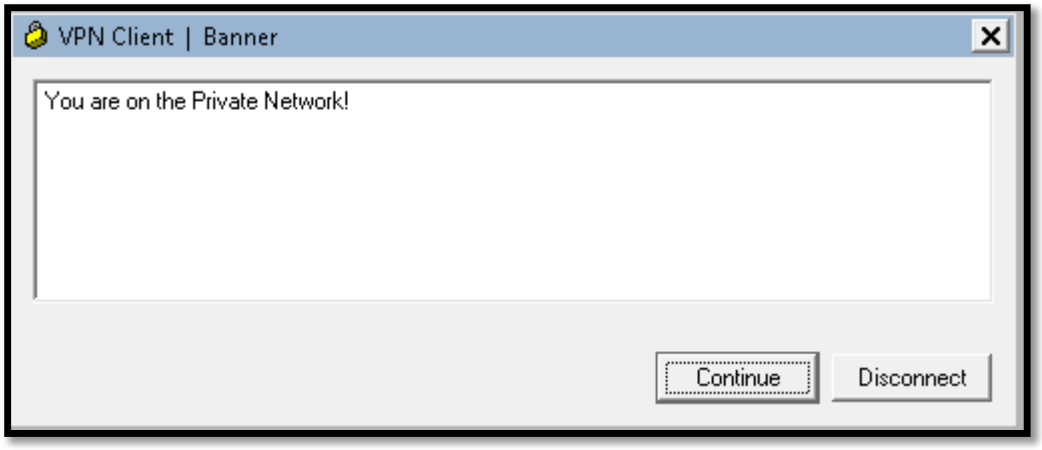
Verification

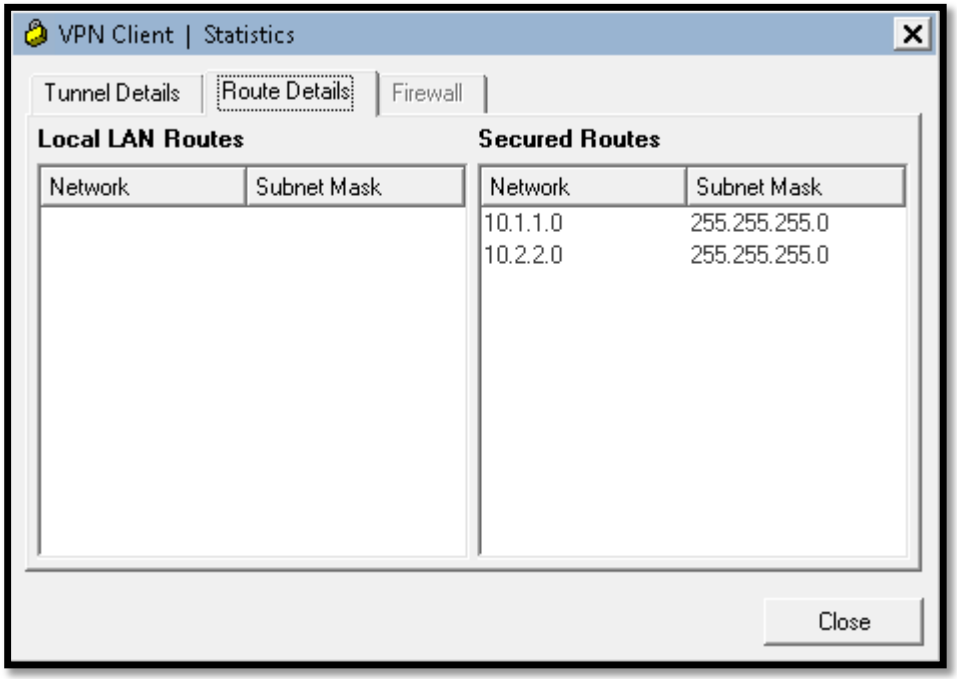
```
ASA4(config)# ping 10.1.1.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.150, timeout is 2 seconds:
%ASA-4-752011: IKEv1 Doesn't have a transform set specified
?!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/27/30 ms

ASA4(config)# test aaa authe ISE host 10.1.1.150
Username: ezuser
Password: ***********
INFO: Attempting Authentication test to IP address <10.1.1.150> (timeout:
12 seconds)
INFO: Authentication Successful
```

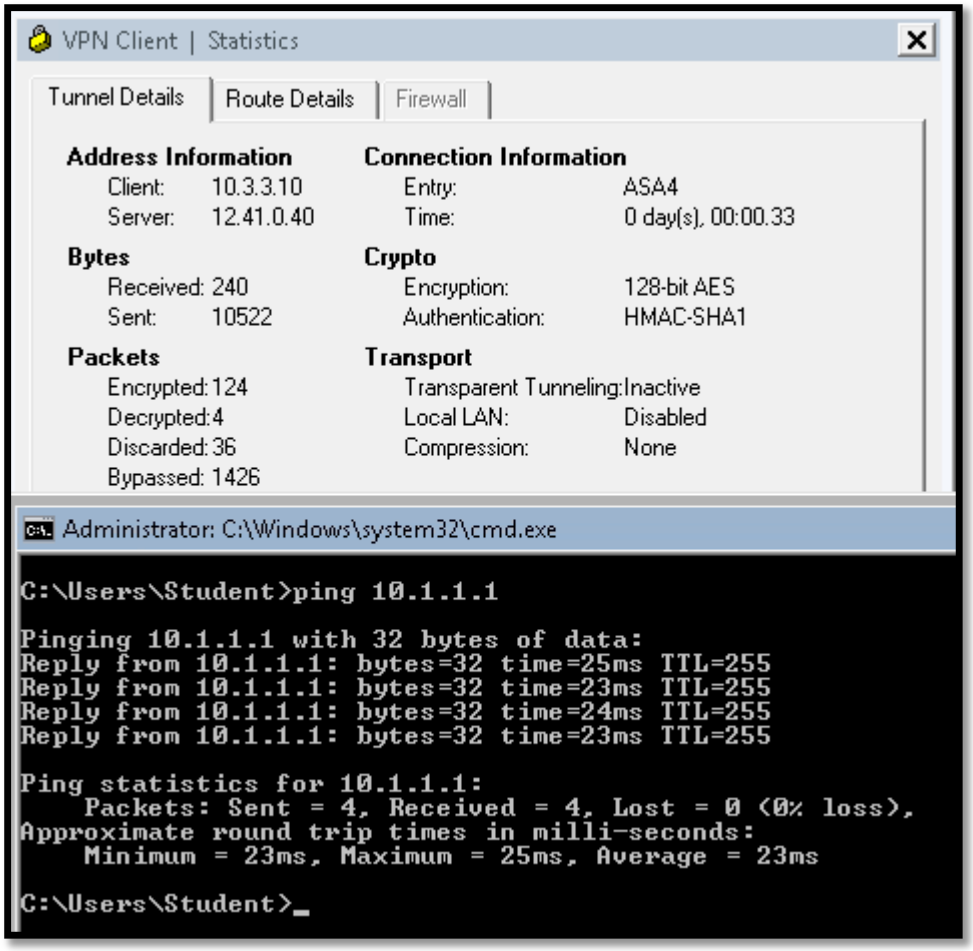
Create a VPN Profile on the Test PC :

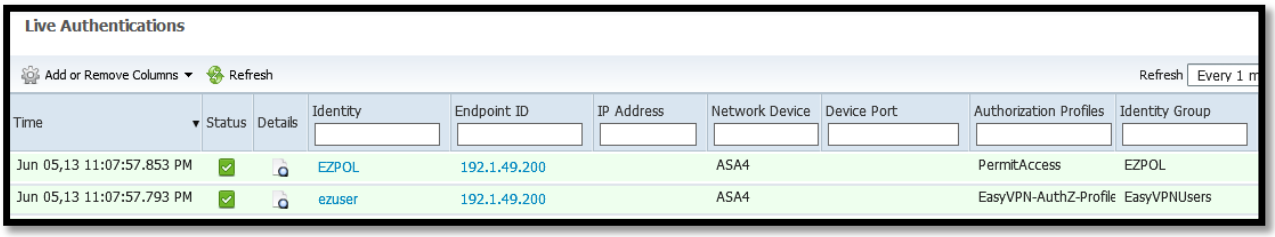


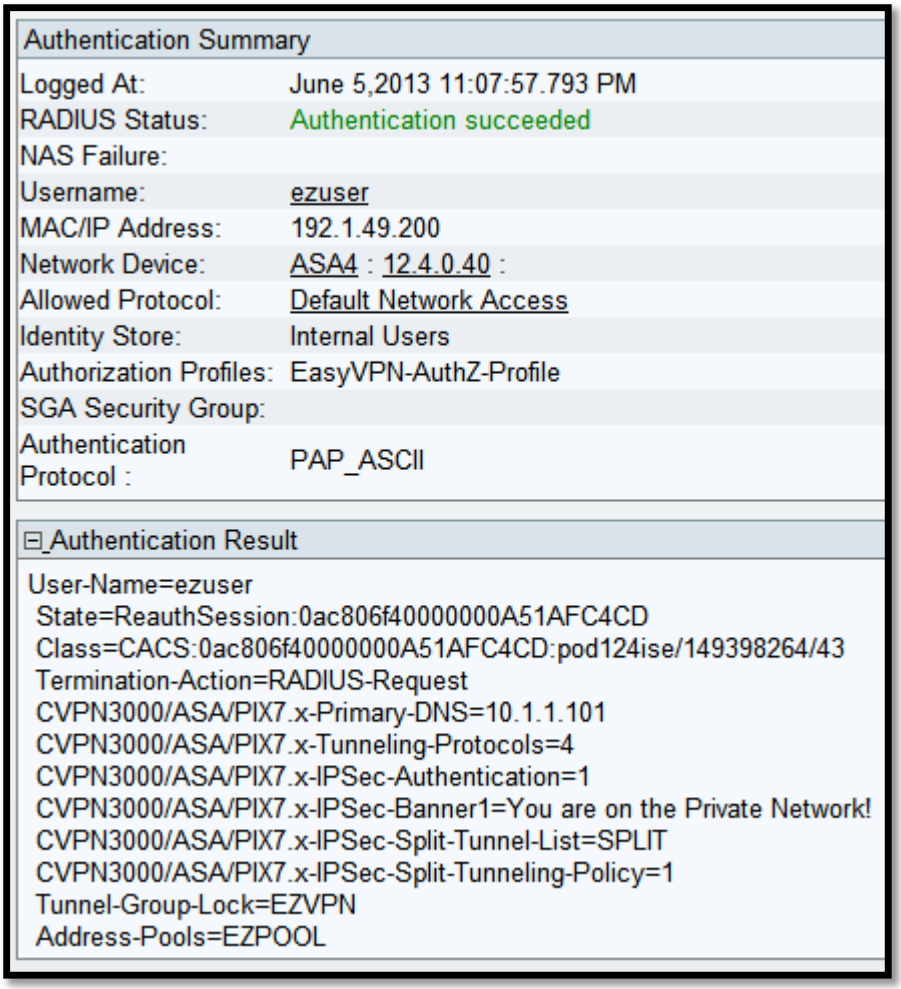
Now connect, authenticate and do a ping test :











Authentication Summary	
Logged At:	June 5,2013 11:07:57.793 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	ezuser
MAC/IP Address:	192.1.49.200
Network Device:	ASA4 : 12.4.0.40 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	EasyVPN-AuthZ-Profile
SGA Security Group:	
Authentication Protocol :	PAP_ASCII

Authentication Result

User-Name=ezuser
State=ReauthSession:0ac806f40000000A51AFC4CD
Class=CACS:0ac806f40000000A51AFC4CD:pod124ise/149398264/43
Termination-Action=RADIUS-Request
CVPN3000/ASA/PIX7.x-Primary-DNS=10.1.1.101
CVPN3000/ASA/PIX7.x-Tunneling-Protocols=4
CVPN3000/ASA/PIX7.x-IPSec-Authentication=1
CVPN3000/ASA/PIX7.x-IPSec-Banner1=You are on the Private Network!
CVPN3000/ASA/PIX7.x-IPSec-Split-Tunnel-List=SPLIT
CVPN3000/ASA/PIX7.x-IPSec-Split-Tunneling-Policy=1
Tunnel-Group-Lock=EZVPN
Address-Pools=EZPOOL

```
Jun 05 23:10:35 [IKEv1 DEBUG]Group = EZVPN, Username = ezuser, IP =
192.1.49.200, Obtained IP addr (10.3.3.10) prior to initiating Mode Cfg
(XAuth enabled)
Jun 05 23:10:35 [IKEv1 DEBUG]Group = EZVPN, Username = ezuser, IP =
192.1.49.200, Sending subnet mask (255.255.255.0) to remote client
```

```
ASA4(config)# sh vpn-sessiondb de ra-ikev1-ipsec

Session Type: IKEv1 IPsec Detailed

Username     : ezuser                 Index        : 34
Assigned IP  : 10.3.3.10              Public IP    : 192.1.49.200
Protocol     : IKEv1 IPsec
License      : Other VPN
```

```
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 240                    Bytes Rx     : 1230
Pkts Tx      : 4                      Pkts Rx      : 15
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : EZPOL                  Tunnel Group : EZVPN
Login Time   : 23:10:30 UTC Wed Jun 5 2013
Duration     : 0h:02m:48s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 34.1
  UDP Src Port : 64708                  UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeys
  Encryption   : AES128                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86237 Seconds
  D/H Group    : 2
  Filter Name  :
  Client OS    : WinNT                  Client OS Ver: 5.0.07.0290

IPsec:
  Tunnel ID    : 34.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 10.3.3.10/255.255.255.255/0/0
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28635 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 240                    Bytes Rx     : 1645
  Pkts Tx      : 4                      Pkts Rx      : 20

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Task 4.5: ASA SSL Clientless VPN (5 Points)

- Configure ASA1 for clientless SSL VPN connections from Internet on port 4443
- The User ("ssluser" with password "IPexpert123") should be authenticated via RADIUS with ISE and he/she should be able to do the following :
  - Enter URLs
  - Telnet to R1
  - See a drop down list of groups to authenticate to
- The Group Policy should be configured locally but assigned by ISE Server and this way override the default Group Policy on the ASA

Detailed Solution

R4

```
ip port-map user-SSLVPN port tcp 4443
```

ASA4

```
access-list OUTSIDE_IN permit tcp any host 12.24.0.10 eq 4443
```

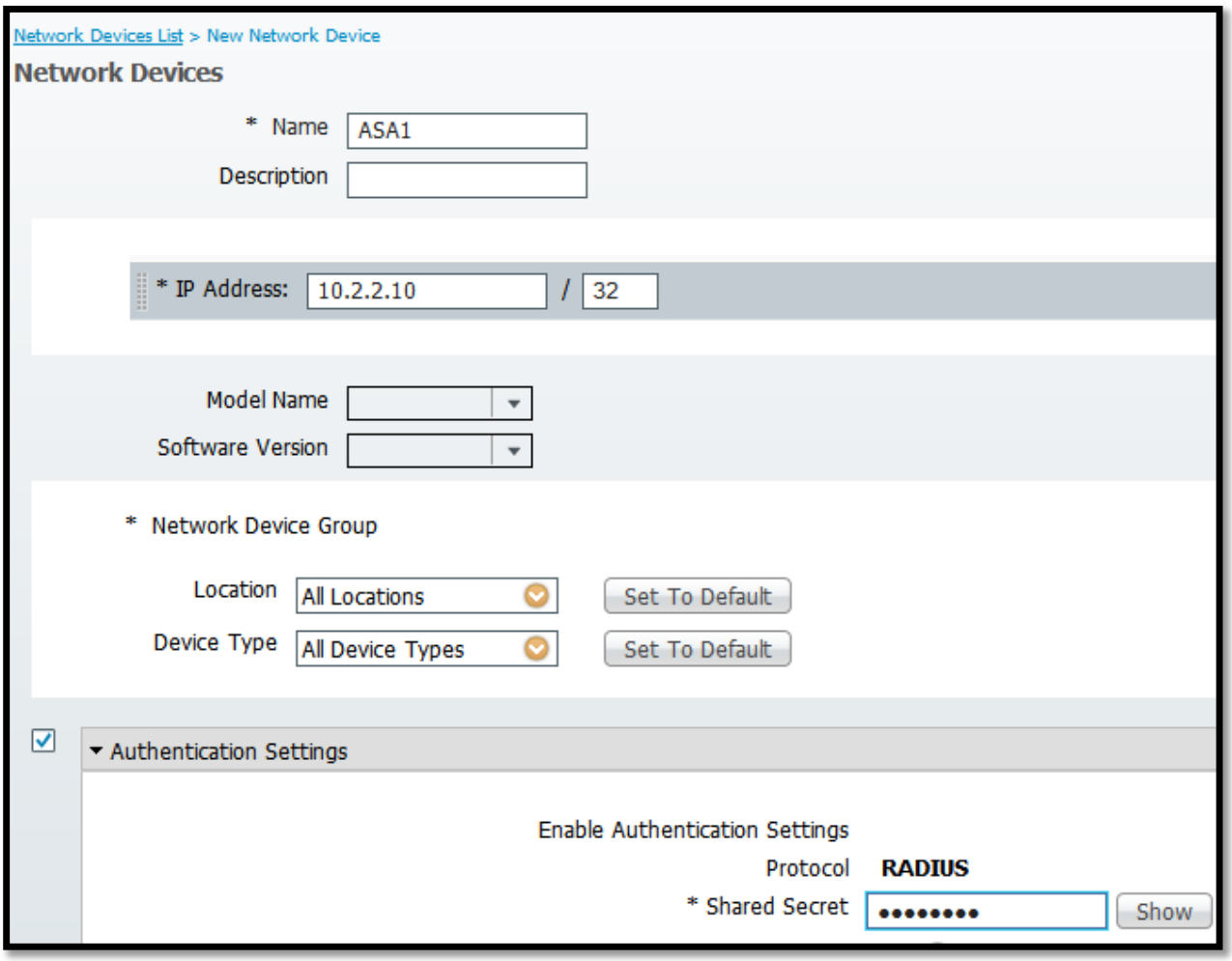
ASA1

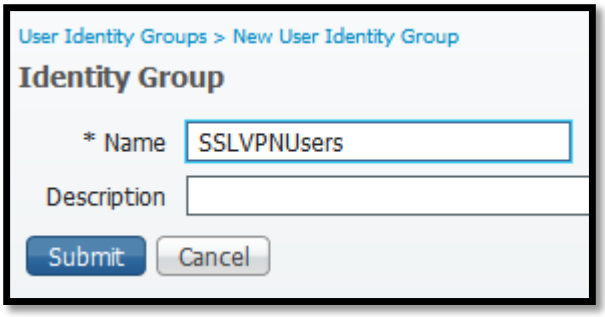
```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.1.1.150
 key ipexpert

webvpn
 port 4443
 enable outside
 port-forward R1 2023 1.1.1.1 telnet TELNET to R1
 tunnel-group-list enable

group-policy WEBPOL internal
group-policy WEBPOL attributes
 vpn-tunnel-protocol webvpn
 webvpn
  port-forward enable R1
```

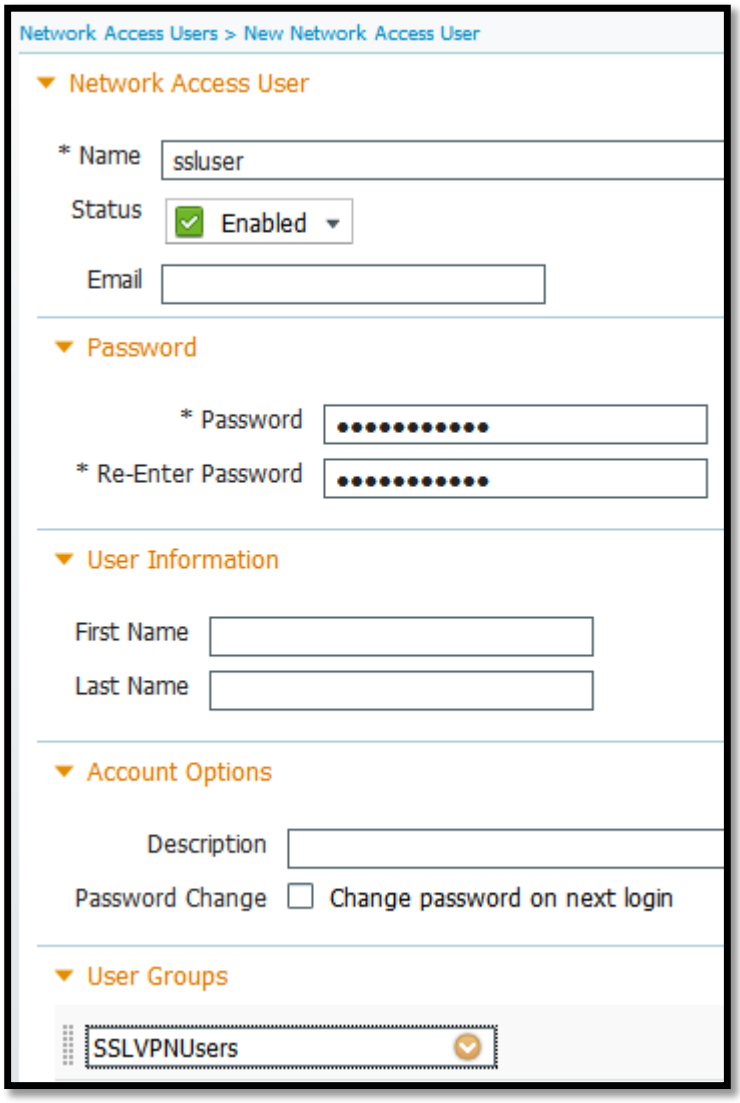
```
     url-entry enable

   tunnel-group webvpn type remote-access
   tunnel-group webvpn general-attributes
    authentication-server-group ISE
   tunnel-group webvpn webvpn-attributes
    group-alias webvpn enable
```

ISE

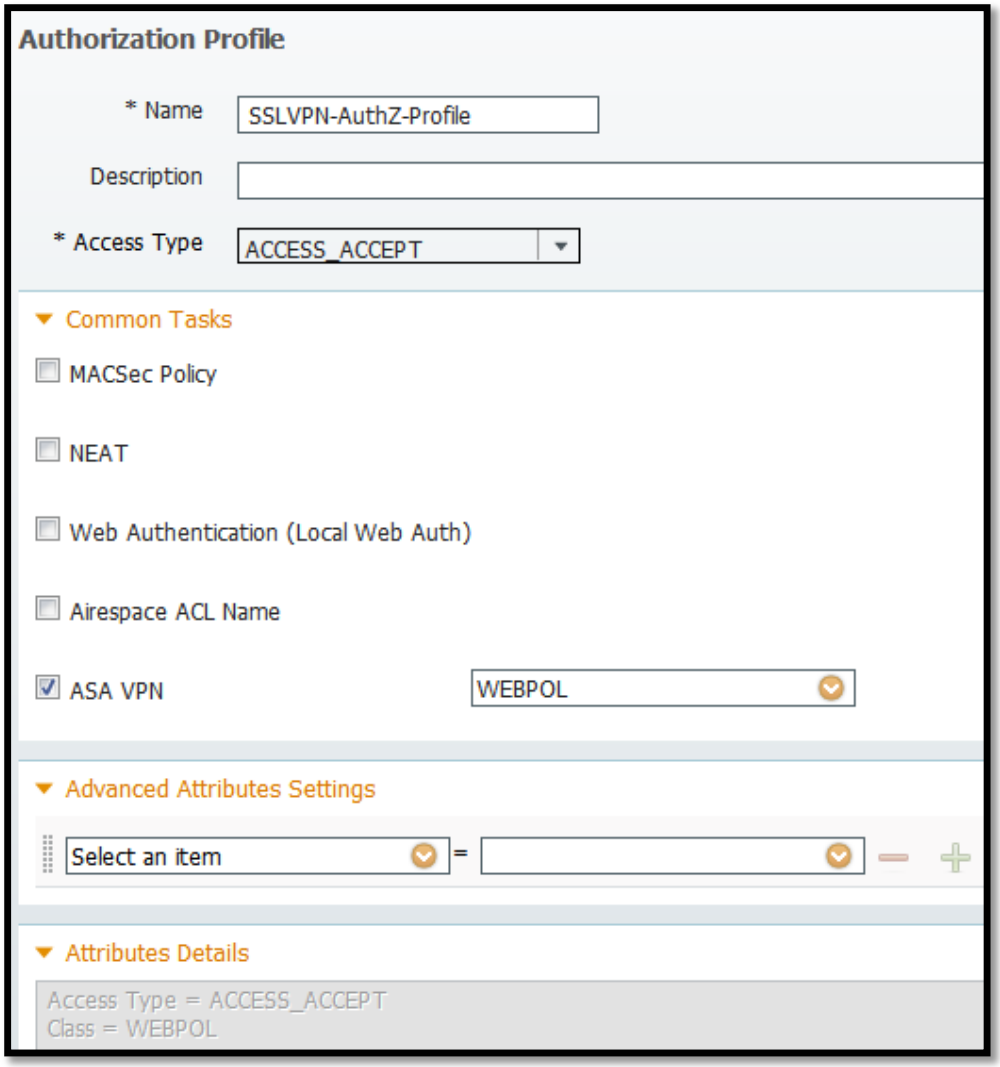
The beginning is the same as in the previous task – new Network Device, Group and User :

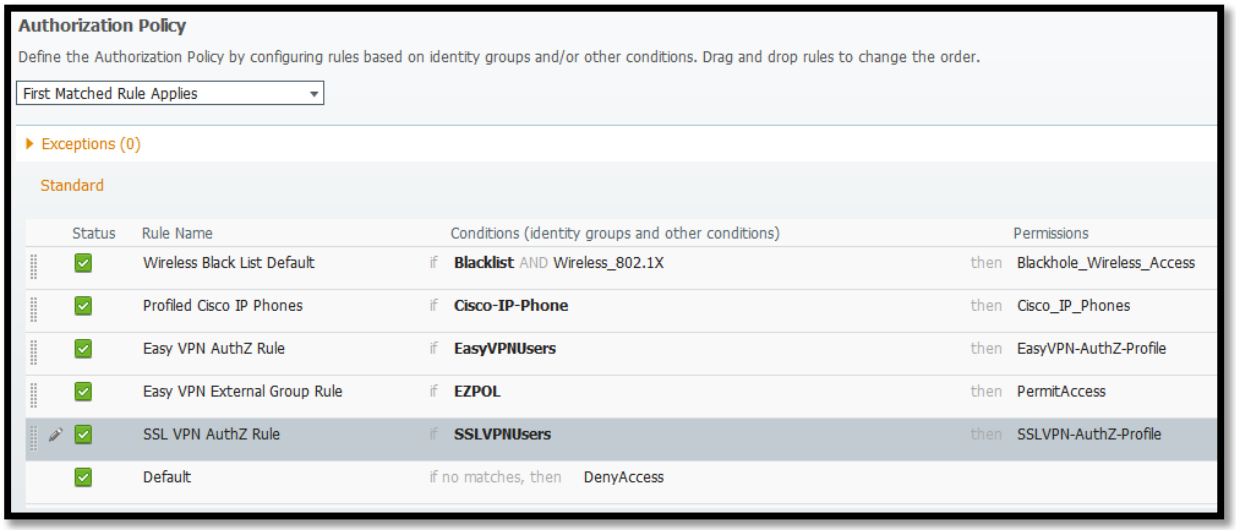






What remains is the AuthZ Profile and the AuthZ Policy Rule :





For ASAs configuration, the challenge is to identify IP addresses that should be inserted in ACL for direction of traffic flows. If NAT was not used you would also have to make permissions on the INSIDE_IN ACL on ASA3 for returning ESP packets.

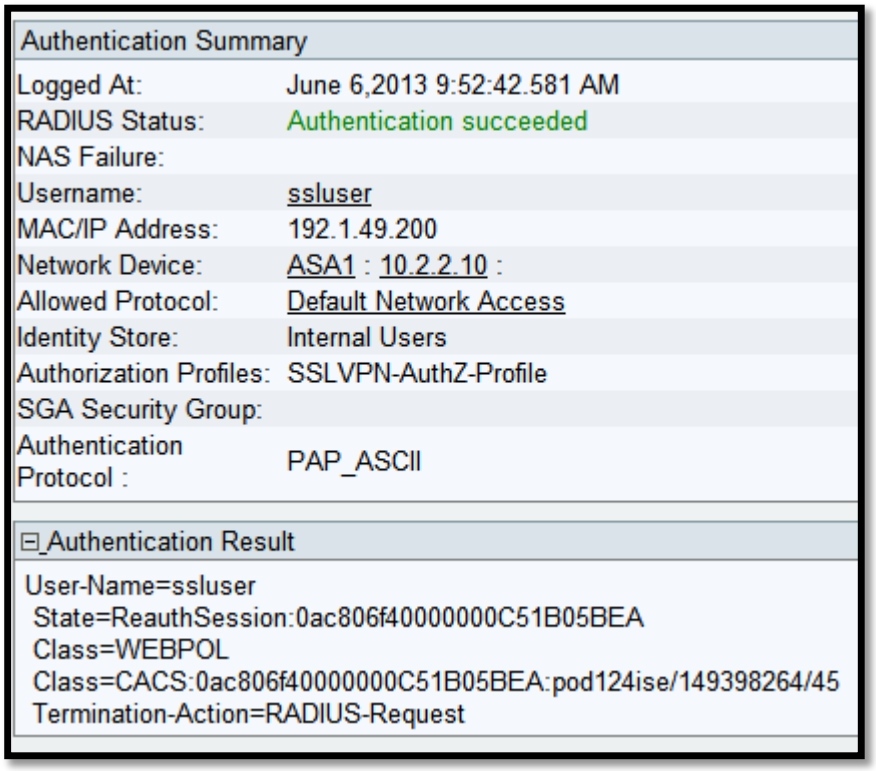
Verification

Add route to 12.24.0.0/24 on the Test PC. Connect through the browser :


```
ASA1(config)# sh vpn-sessiondb de webvpn

Session Type: WebVPN Detailed

Username     : ssluser                Index        : 1
Public IP    : 192.1.49.200
Protocol     : Clientless
License      : SSL VPN
Encryption   : RC4                    Hashing      : SHA1
Bytes Tx     : 56969                  Bytes Rx     : 13842
Pkts Tx      : 5                      Pkts Rx      : 1
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : WEBPOL                 Tunnel Group : webvpn
Login Time   : 09:38:07 UTC Thu Jun 6 2013
Duration     : 0h:00m:21s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

Clientless Tunnels: 1
```

```
Clientless:
  Tunnel ID    : 1.1
  Public IP    : 192.1.49.200
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Dst Port : 4443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client Type  : Web Browser
  Client Ver   : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0)
  Bytes Tx     : 56969                  Bytes Rx     : 13842

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 23 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :


R4#sh policy-firewall session zone-pair OUTIN
 Zone-pair: OUTIN
  Service-policy inspect : ZFW_OUTIN_POL
    Class-map : ZFW_CUST_CLASS(match-any)
    Class-map : ZFW_TCP_PROTO_IN_CLASS(match-any)
    Class-map : ZFW_UDP_PROTO_IN_CLASS(match-any)
    Class-map : ZFW_ICMP_CLASS(match-all)
    Class-map : ZFW_ESP_CLASS(match-all)
    Class-map : ZFW_IKE_CLASS(match-all)
      Established Sessions =  1
        Session 49EEDC20 (12.4.0.40:500)=>(12.24.0.30:500) isakmp:udp
SIS_OPEN
          Created 03:23:52, Last heard 00:00:01
          Bytes sent (initiator:responder) [175840:175840]
    Class-map : ZFW_SSLVPN_CLASS(match-all)
      Established Sessions =  4
        Session 49A62320 (192.1.49.200:53269)=>(12.24.0.10:4443) user-
SSLVPN:tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:19, Last heard 00:00:17
          Bytes sent (initiator:responder) [1164:4248]
```

```
        Session 49A634A0 (192.1.49.200:53274)=>(12.24.0.10:4443) user-
SSLVPN:tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:18, Last heard 00:00:17
          Bytes sent (initiator:responder) [1004:2764]
        Session 49A63120 (192.1.49.200:53273)=>(12.24.0.10:4443) user-
SSLVPN:tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:18, Last heard 00:00:17
          Bytes sent (initiator:responder) [561:5368]
        Session 49A62A20 (192.1.49.200:53271)=>(12.24.0.10:4443) user-
SSLVPN:tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:18, Last heard 00:00:17
          Bytes sent (initiator:responder) [540:3105]
    Class-map : class-default(match-any)
```

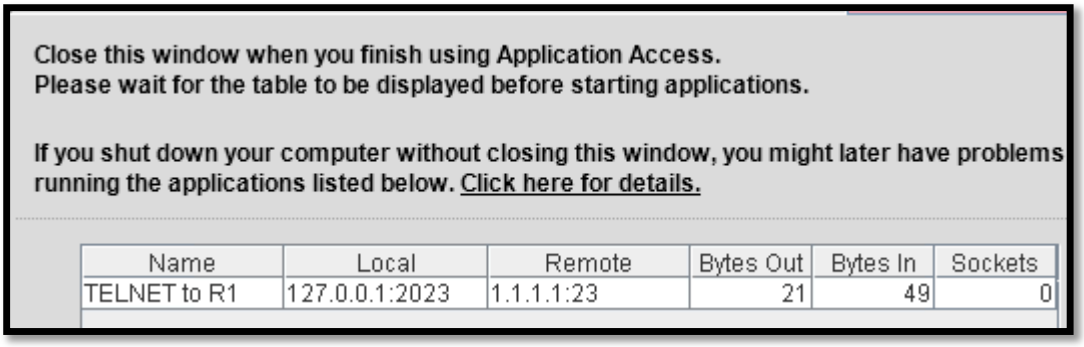


Authentication Summary	
Logged At:	June 6,2013 9:52:42.581 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	ssluser
MAC/IP Address:	192.1.49.200
Network Device:	ASA1 : 10.2.2.10 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	SSLVPN-AuthZ-Profile
SGA Security Group:	
Authentication Protocol :	PAP_ASCII

⊟ Authentication Result

User-Name=ssluser
State=ReauthSession:0ac806f40000000C51B05BEA
Class=WEBPOL
Class=CACS:0ac806f40000000C51B05BEA:pod124ise/149398264/45
Termination-Action=RADIUS-Request

Now go to “Application Access” and start Port Forwarding. Telnet to 127.0.0.1 :



Then go to the URL bar and type 1.1.1.1:80 :

5.0 Identity Management (15 points)

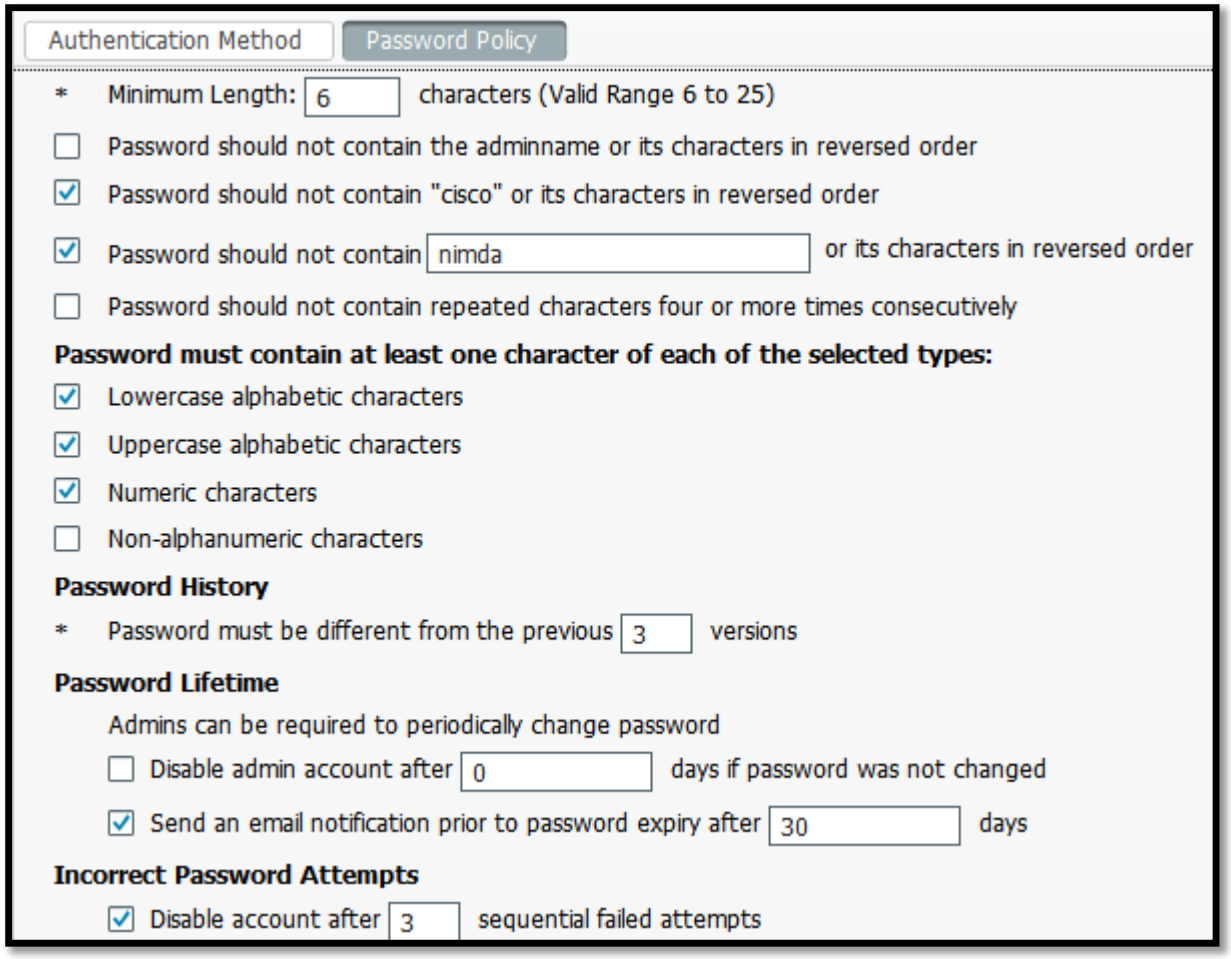
Task 5.1: ISE General Setup (3 Points)

- Create a new password policy for ISE Administrators :
  - Password must be at least 6 character long
  - It cannot contain words “cisco” or “nimda” or their characters in reversed order
  - At least one alphabetic (Upper & Lower -case) and numeric character must be part of the password
  - Disable account after 3 unsuccessful login attempts
- Create a new password policy for Users :
  - Password must be at least 6 character long
  - It cannot contain words “cisco” or “nimda” or their characters in reversed order
  - At least one alphabetic (Upper & Lower –case) and numeric character must be part of the password
  - Password must be different from the previous one
- Generate a Certificate Signing Request (CSR). Use CN of ISE-Podxxx where xxx is your pod number, Organization should be set to “IPexpert” and Organizational Unit to “Instructors”
- Create a repository for backups. Use TFTP
- Files will be stored on 10.1.1.99 under ISE-BACKUPS directory

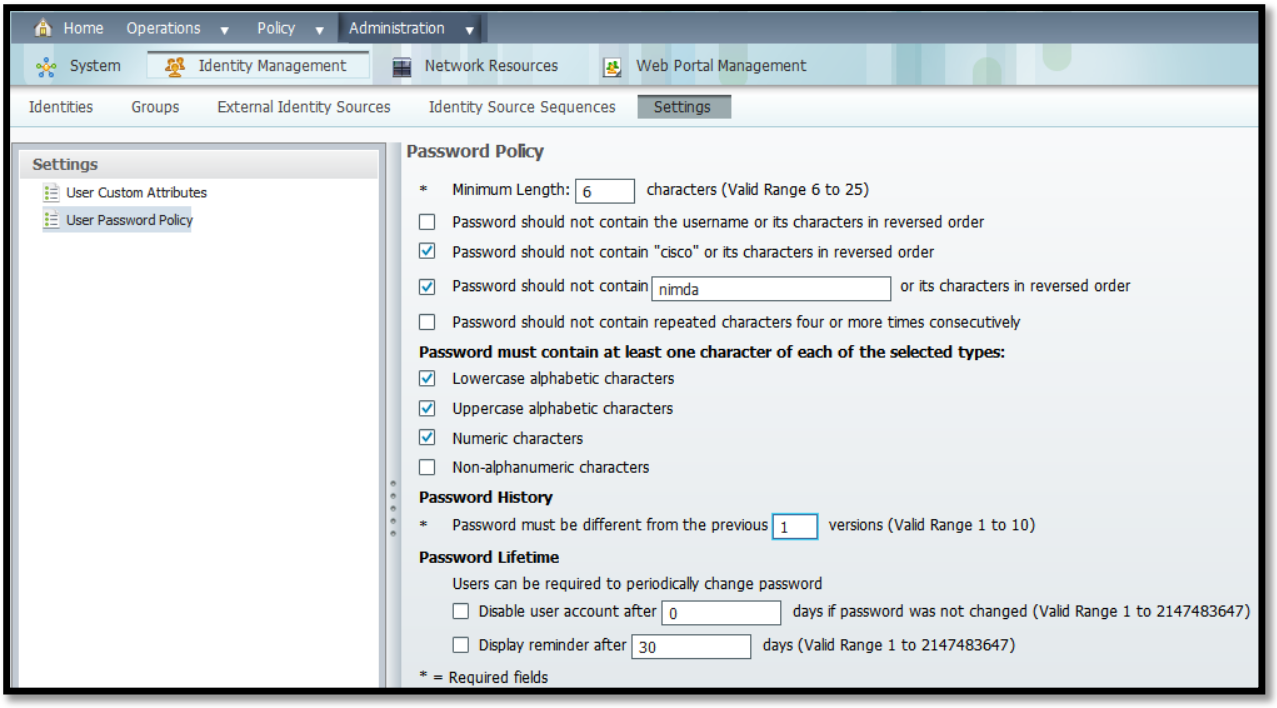
Detailed Solution

ISE

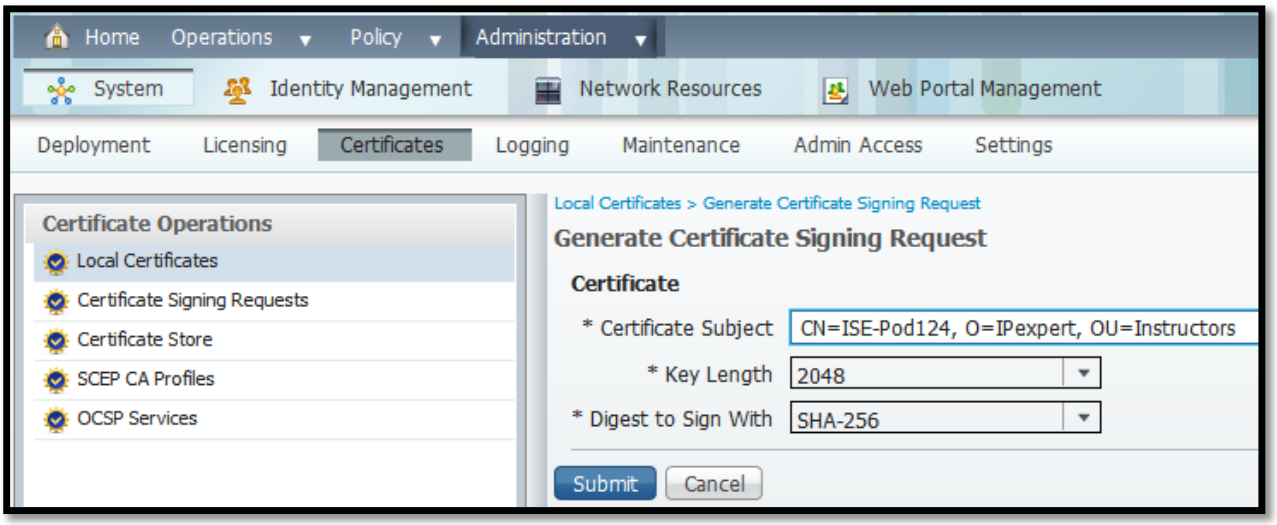
Go under Administration -> Admin Access and choose Password Policy tab :



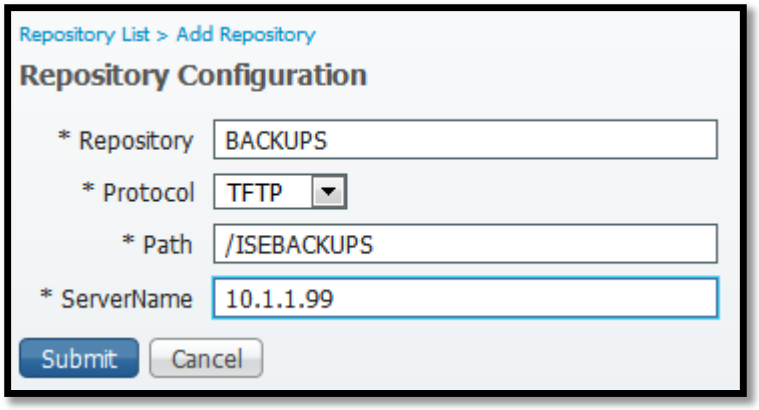
For the user Policy it is under Administration -> Identity Management -> Settings :



Now the certificate part :

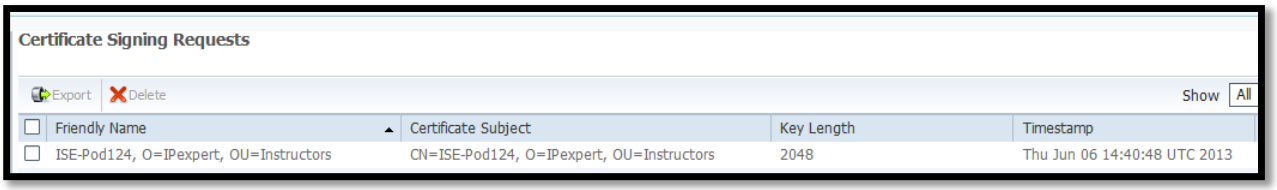


And finally the Repository for backups (Administration -> Maintenance) :

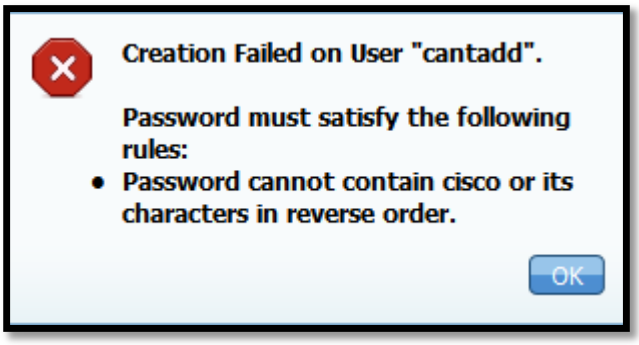


Just be familiar with where certain things can be configured on the GUI.

Verification



You can also try to add a user/admin who's password does not meet the policy. A similar message will show up :



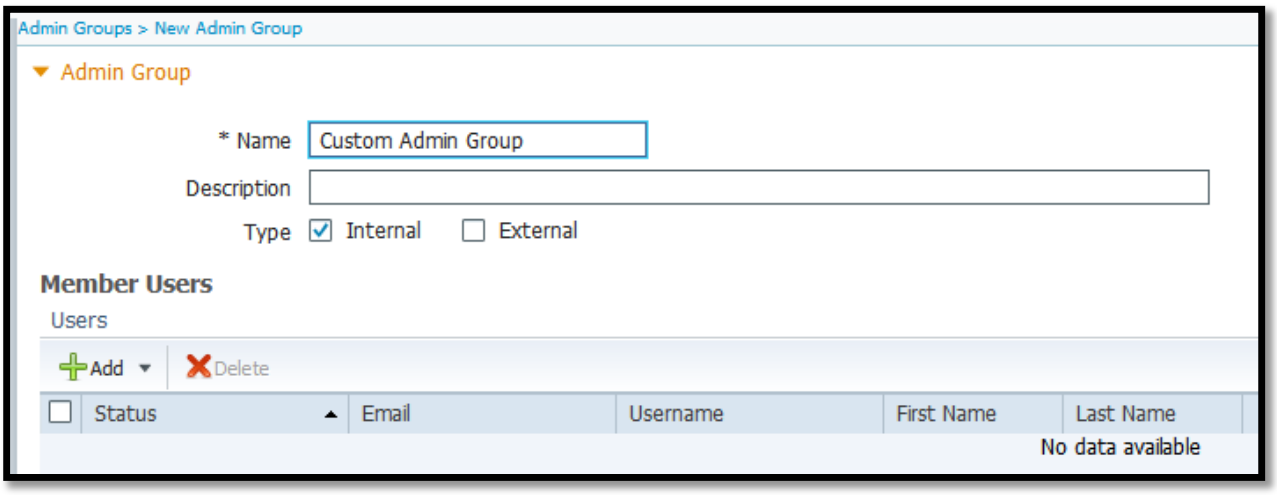
Task 5.2: ISE Administrative Access (3 Points)

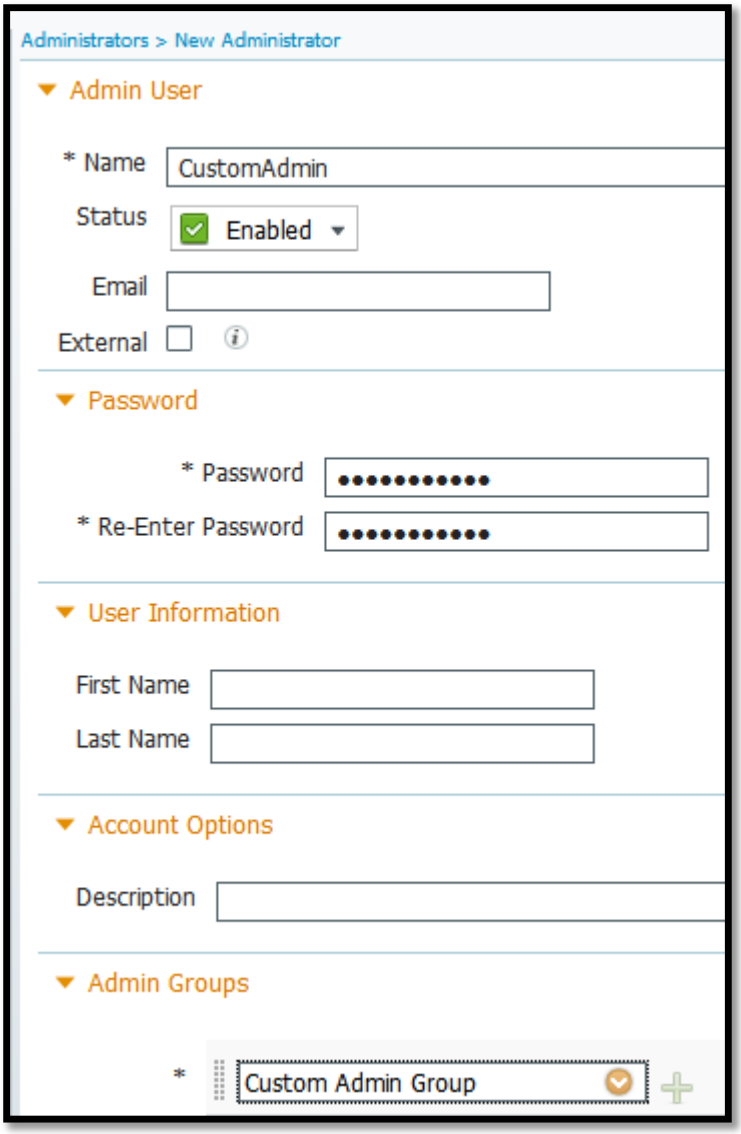
- Configure a new Administrator ("CustomAdmin", password "IPexpert123") who will be able to see all Identity Groups and all Network Devices
- Read/write access to any other Menus & Data should be denied
- Restrict management access to ISE to IP address you are using to connect to the device and VLAN 100 subnet

Detailed Solution

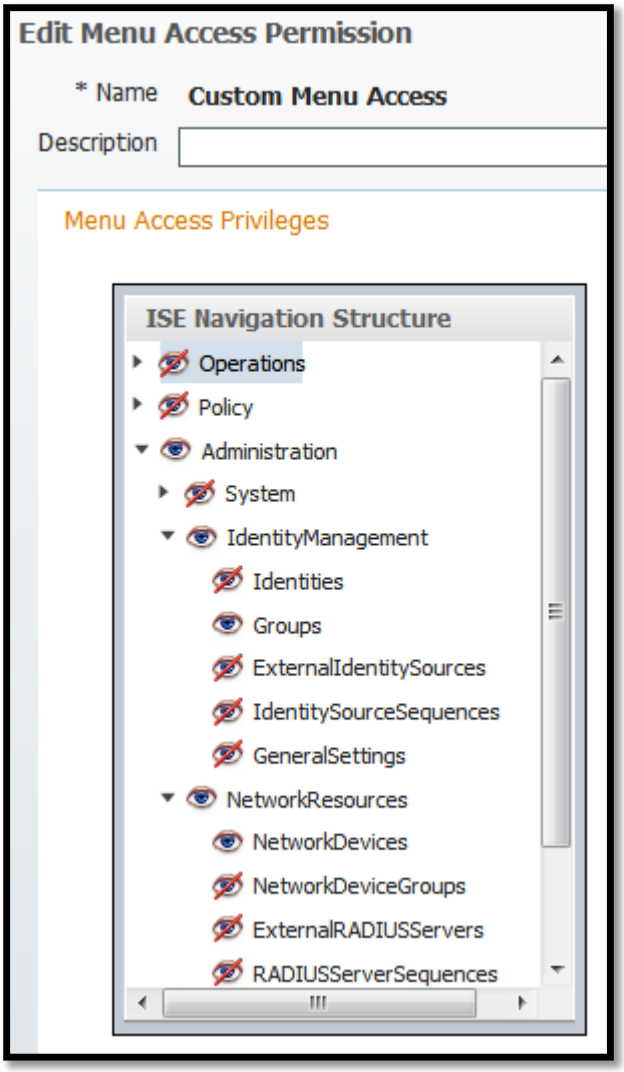
ISE

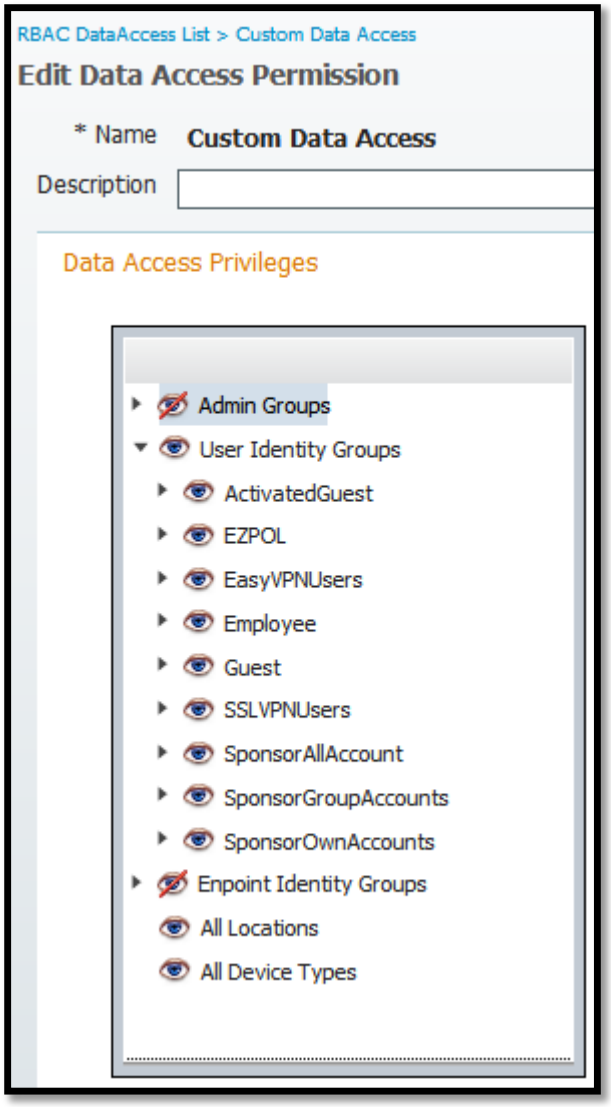
We need to first create an Admin Group where the Administrator will belong to (then make sure CustomAdmin is part of that Group). This is all configured under Administration -> Admin Access -> Administrators :



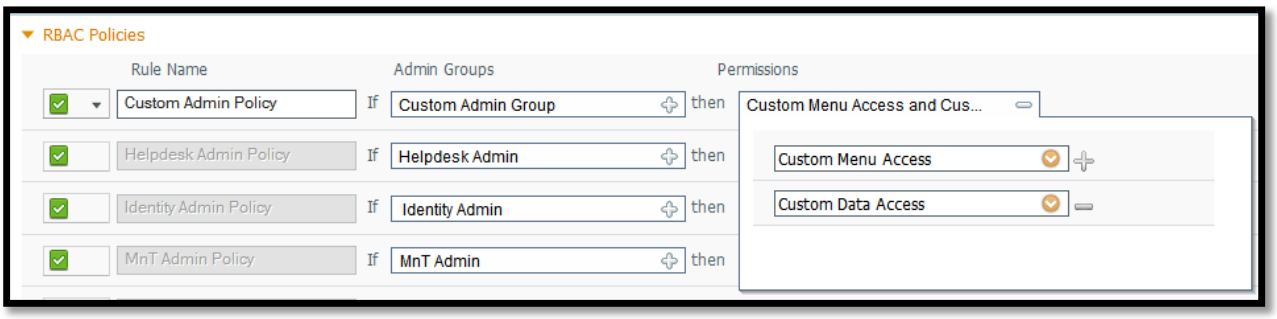


Now we need to define Menu and Data Permissions :

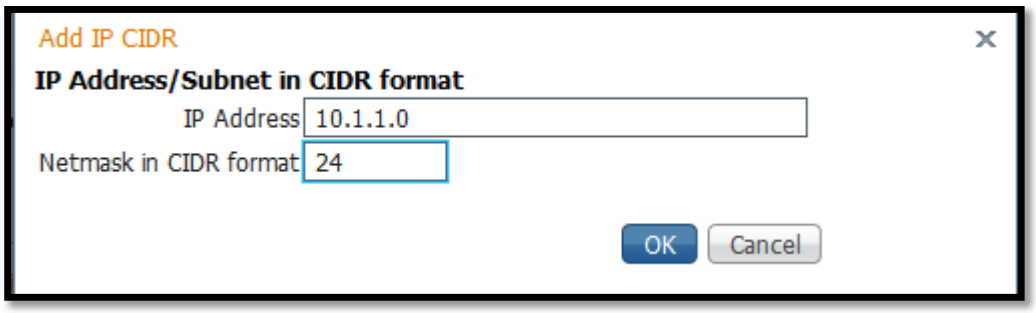


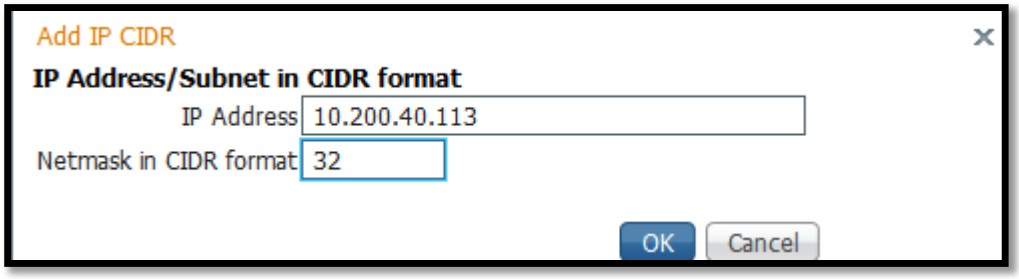


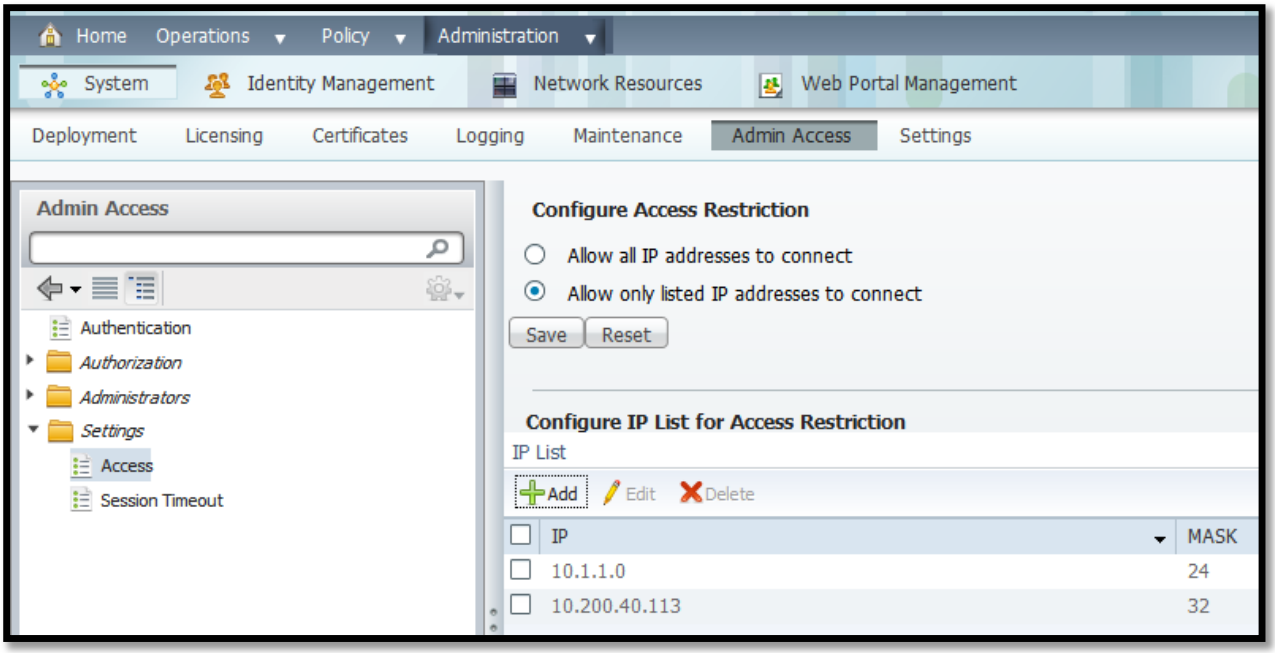
RBAC Policy Rule must be created next. It says that for Administrators who belong to our Custom Admin Group we want to give them the level of access defined by our Permissions :



And finally we want to limit management access to certain IP addresses :







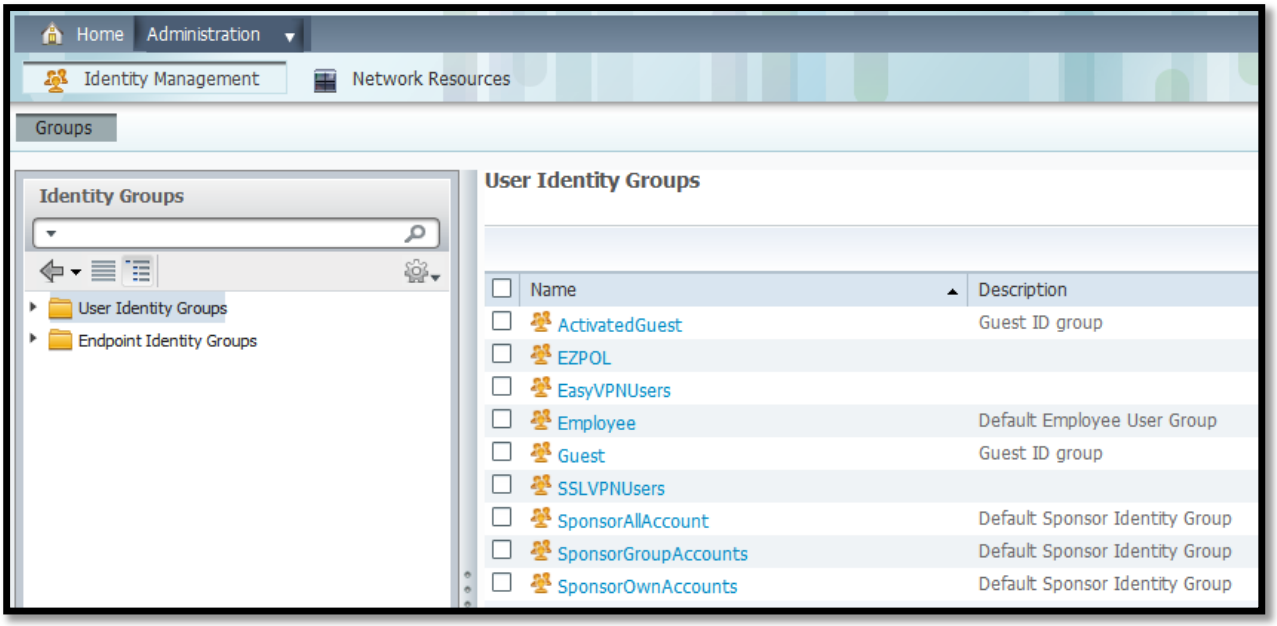
Menu Permissions is what gives Administrator access to certain GUI components, such as “Operations” tab or maybe “Network Devices” as the only element available out of whole “Network Resources”.

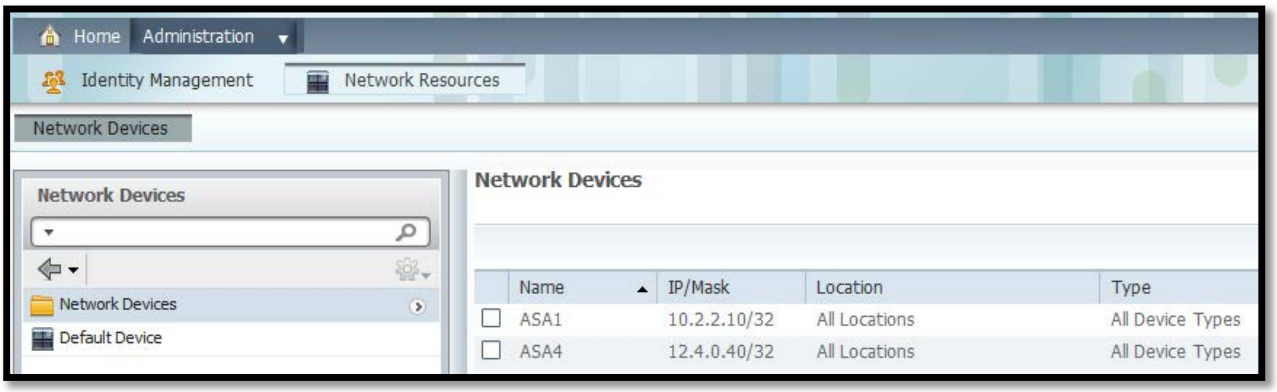
Data Permissions is where you say what data (configured elements like Users or Endpoint Groups) you want the Administrator to be able to see.

RBAC Policy is what defines access for Administrators. The condition is an Admin Group and then what the members of the group can see/do are the Menu and/or Data Permissions. You can create multiple entries for a single group and all Permissions will be then combined (permits override denies).

Verification

Login as “CustomAdmin” and verify access this user has :





Task 5.3: Wireless 802.1x (6 Points)

- Initialize WLC with a management IP address according to the addressing table
- Username MUST be "**admin**" and password MUST be set to "**IPexpert123**"
- Configure WLC to act as a DHCP Server for VLANs 100 (AP) and VLAN 20 (clients) – a pool of ten or so IP addresses will suffice in both cases
- Create WLAN "Corp-Access-xxx" where xxx is your pod number
- This wireless network should only grant access to 802.1x-authenticated users
- Users who successfully pass authentication should end up in VLAN 20 and be able to reach all 12.x.x.x networks via ASA3
- Use ISE as a source of authentication and authorization information
- Authenticate with user "wireless" password "IPexpert123"
- Secure RADIUS communication using password "ipexpert"

Detailed Solution

CAT4

```
int g1/0/13
 sw tru encap dot
 sw mode trunk
```

CAT2

```
int f0/22
 sw host
 sw acc vlan 100
```

ASA3

```
object network INSIDE_10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
 nat (inside,outside) dynamic NATPOOL
```

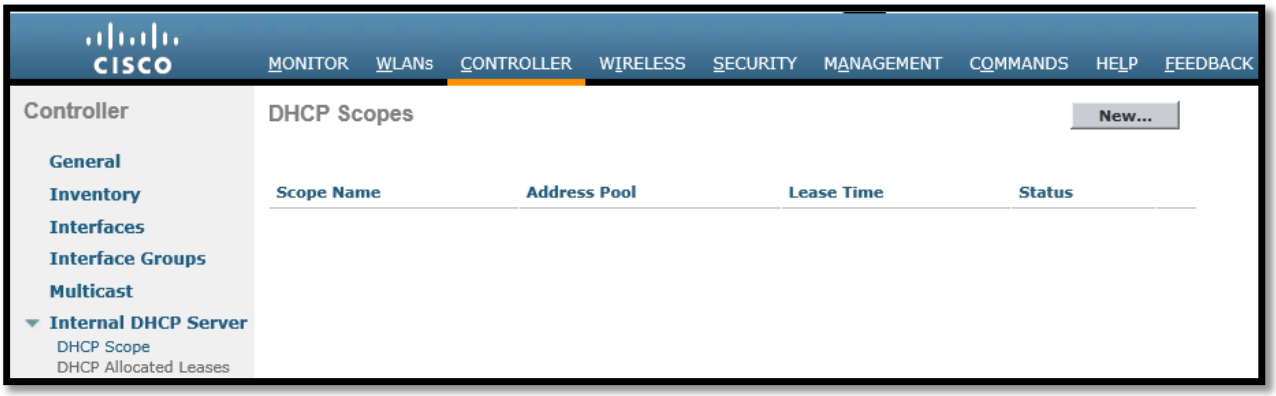
WLC

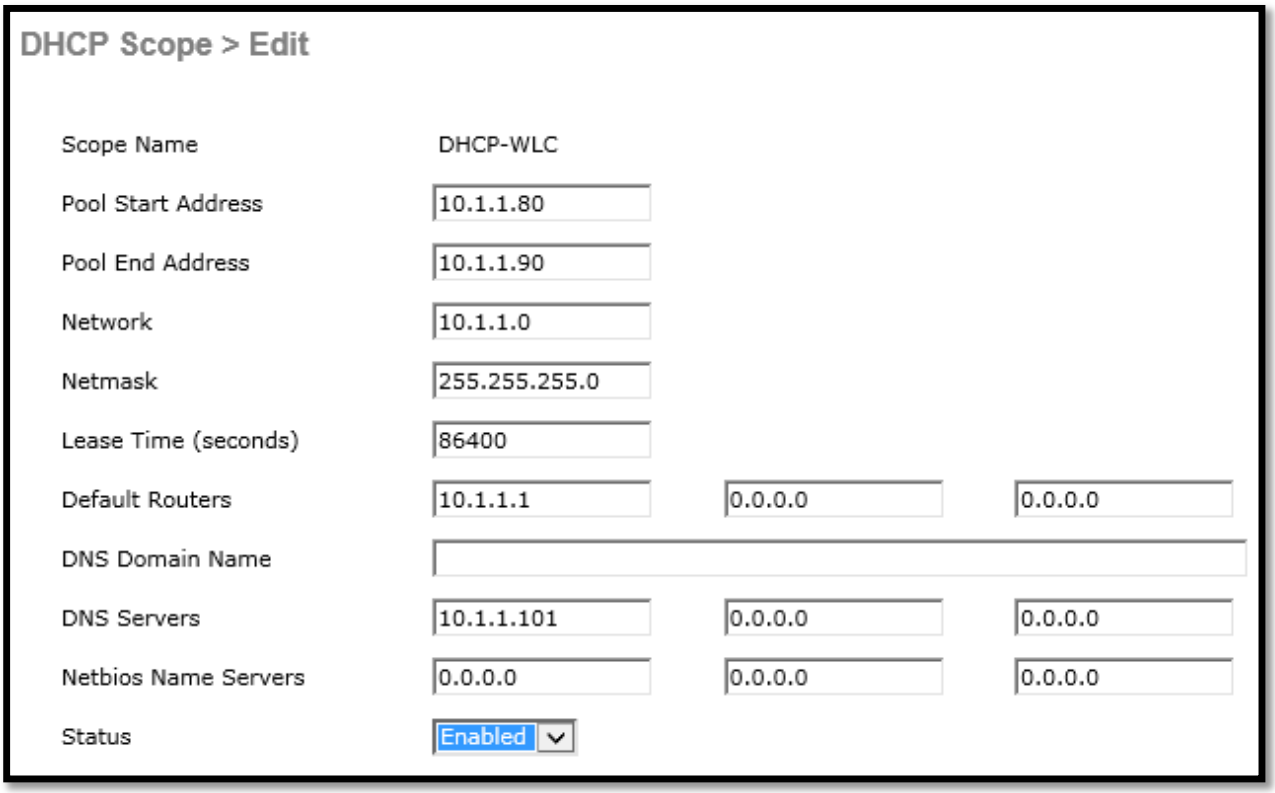
```
Would you like to terminate autoinstall? [yes]:
```

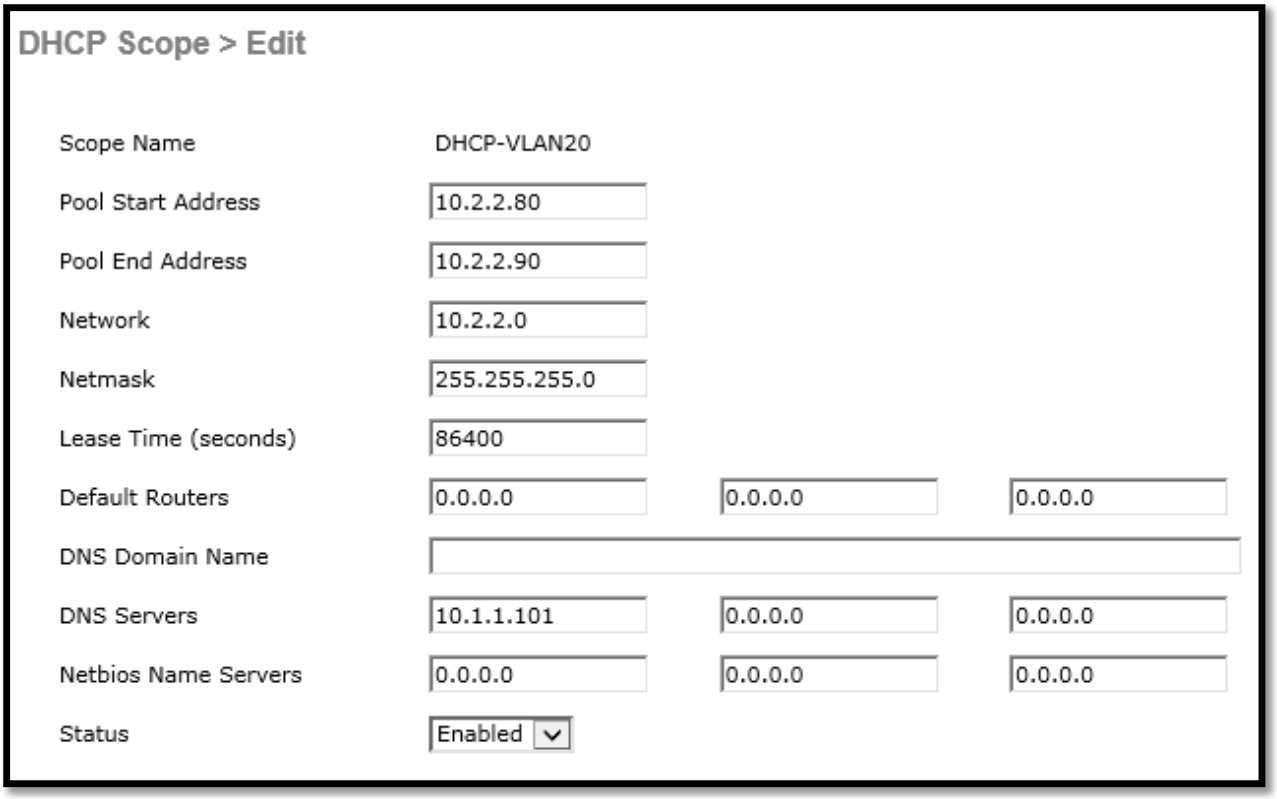
```
System Name [Cisco_b6:3d:84] (31 characters max): WLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): IPexpert123
Re-enter Administrative Password                  : IPexpert123

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: 99.99.99.99
route: SIOC[ADD|DEL]RT: File exists

Mobility/RF Group Name: RFG

Network Name (SSID): Mgmt-Sec-124

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]:

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
```

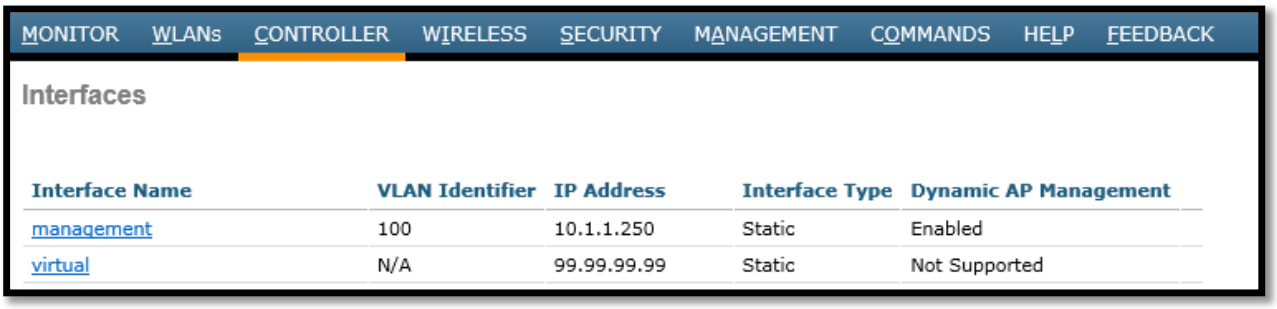
We want to define two DHCP pools – one for VLAN 100, other for VLAN20. Don't specify a default router for VLAN 20 :

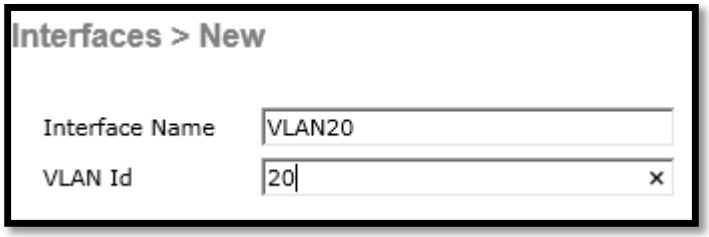




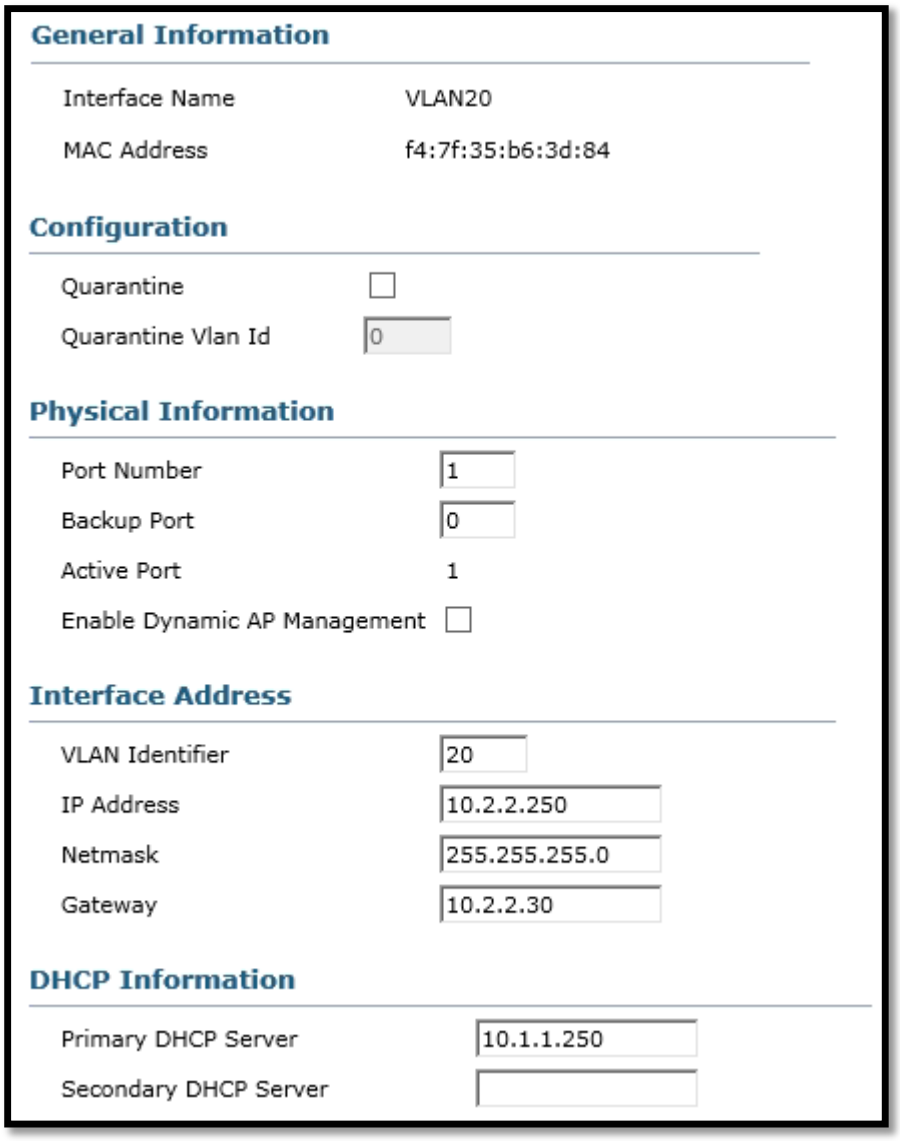


Next step is to define a subinterface for VLAN 20 :

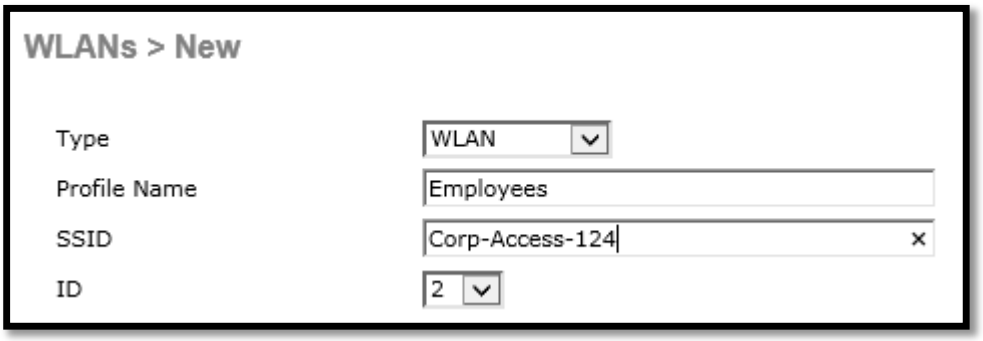




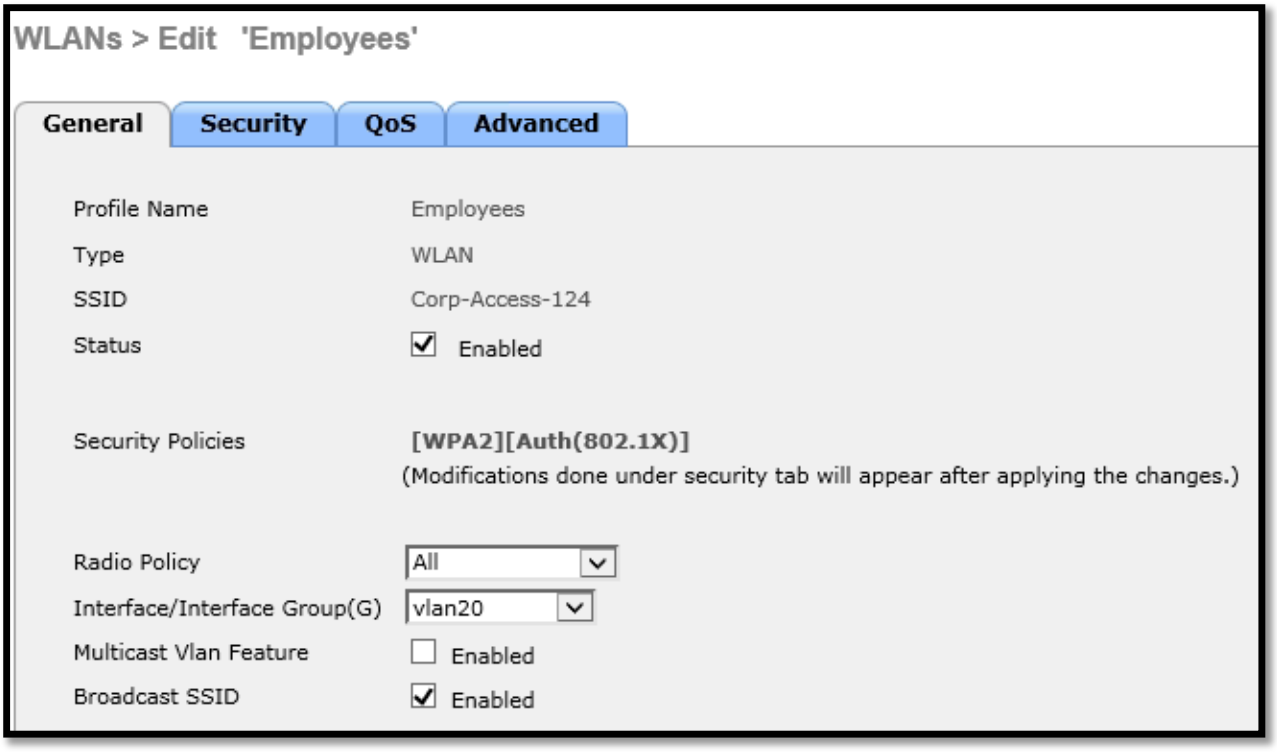
Note the Primary DHCP Server must point to the management IP address of WLC :



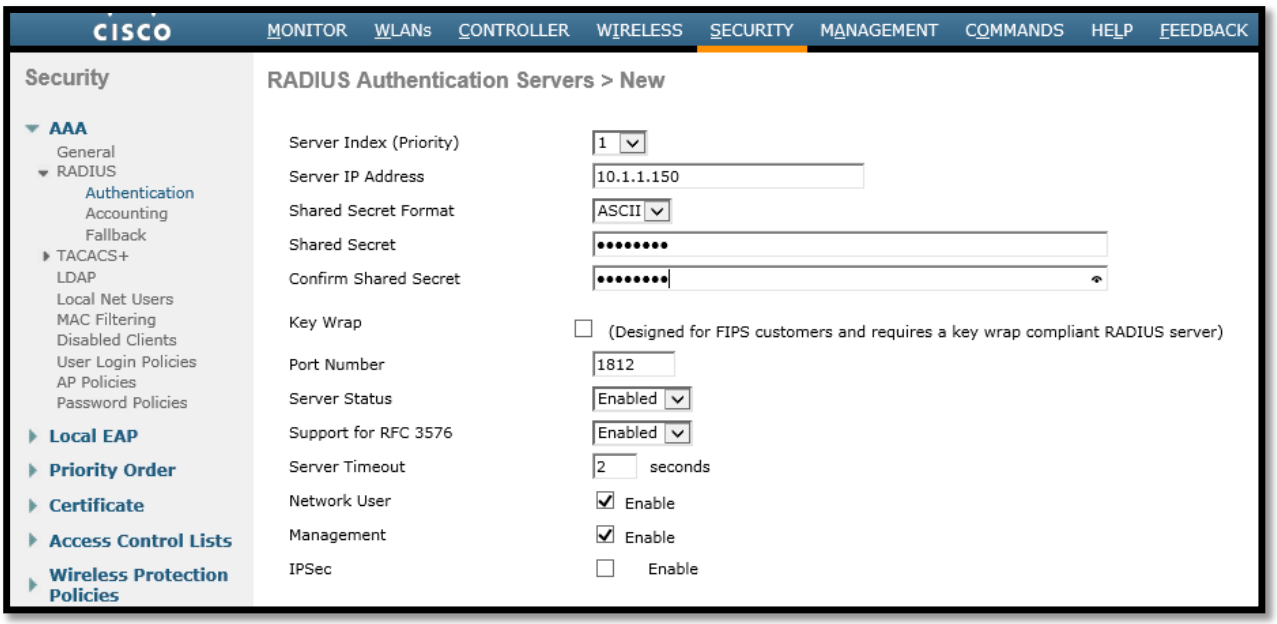
Once we have that, we should add a new WLAN :



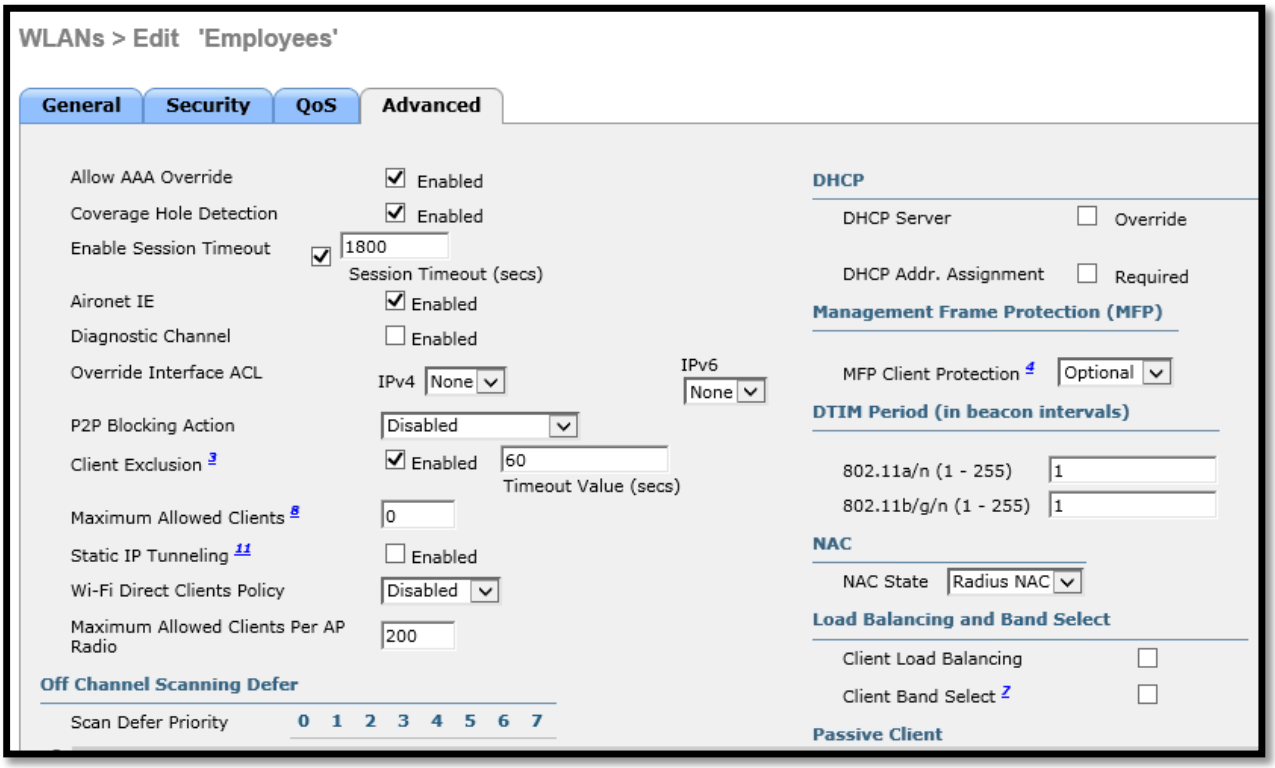
Make sure it is enabled, that you selected a proper subinterface and that SSID is broadcast :



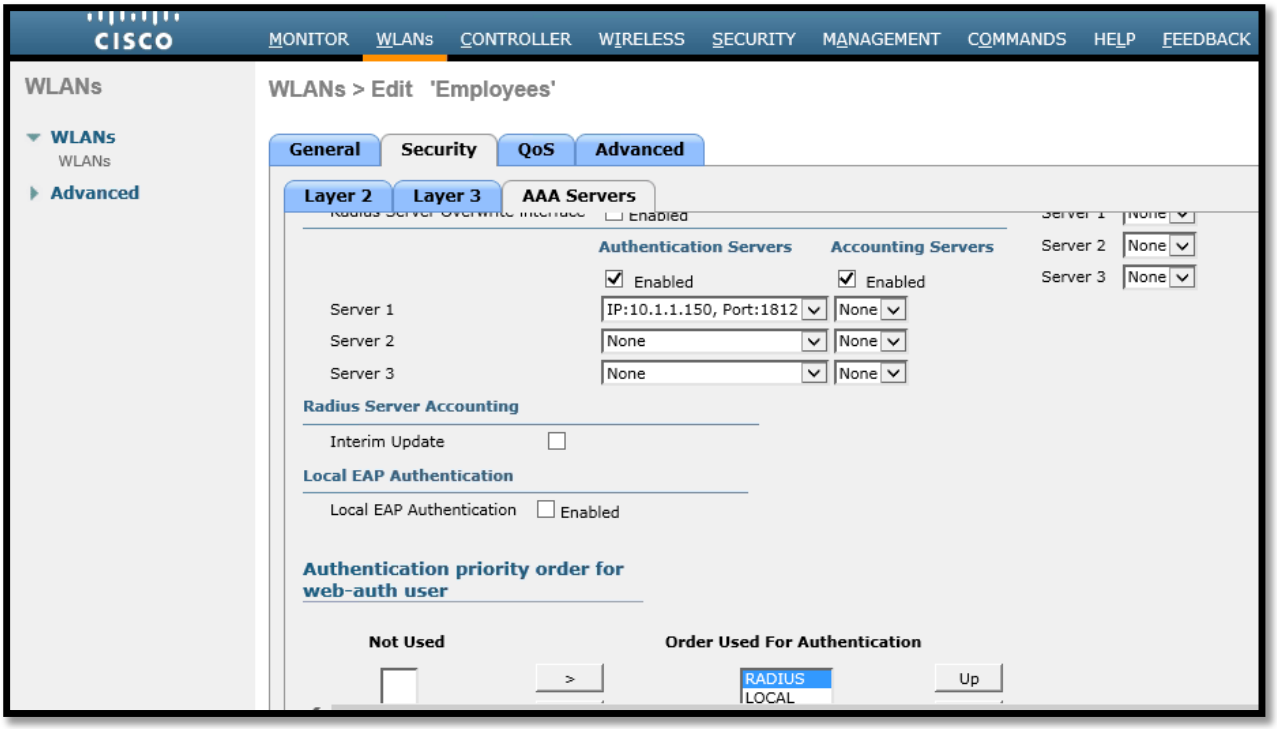
We also have to define an authentication server (ISE) – this can be done from under "Security" tab, "RADIUS" and "Authentication" :



Go back to the WLAN and check “Allow AAA Override” and choose “NAC State” to be “RADIUS NAC” :



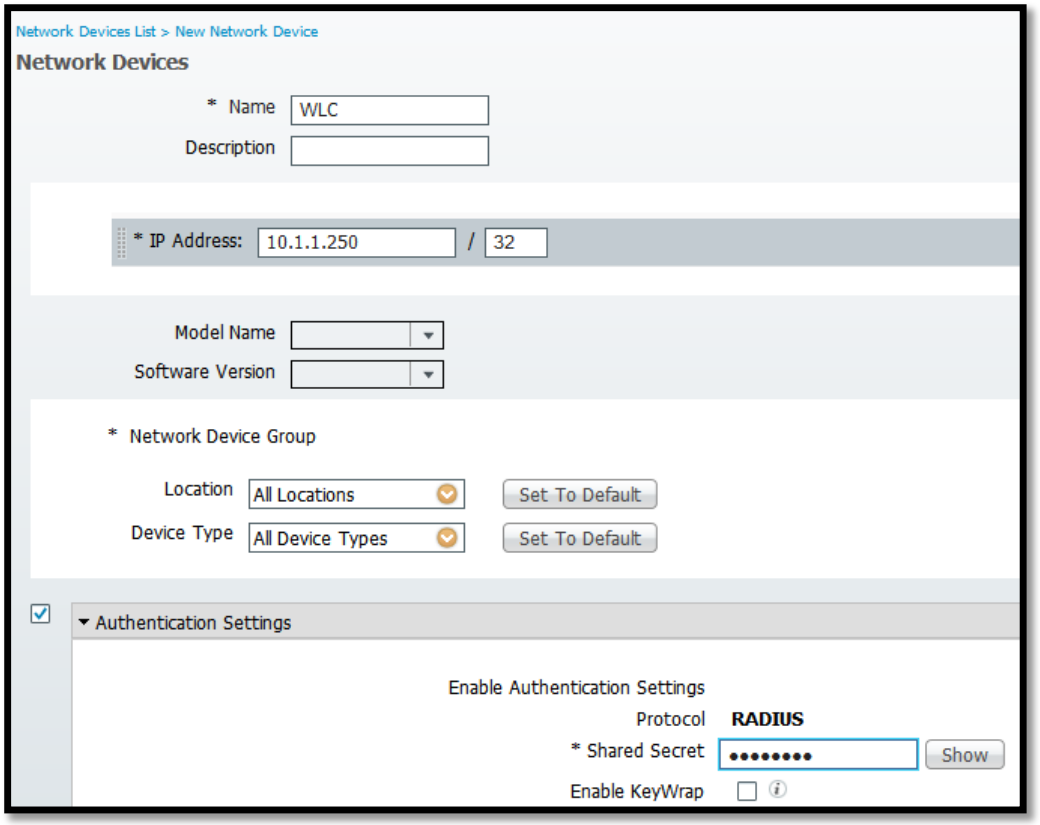
Then select ISE as an authentication AAA Server :

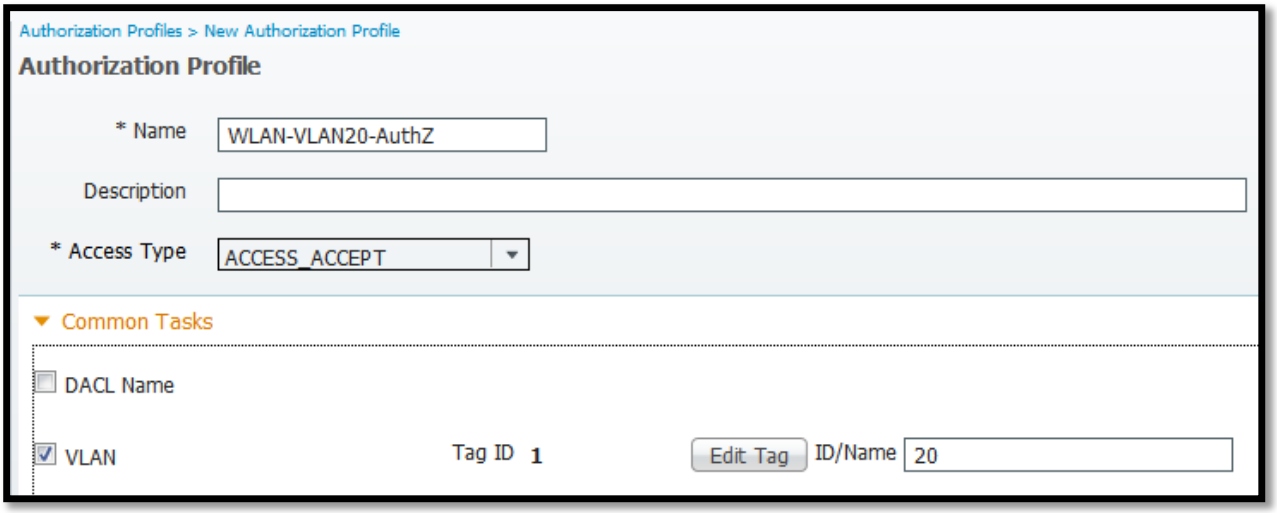


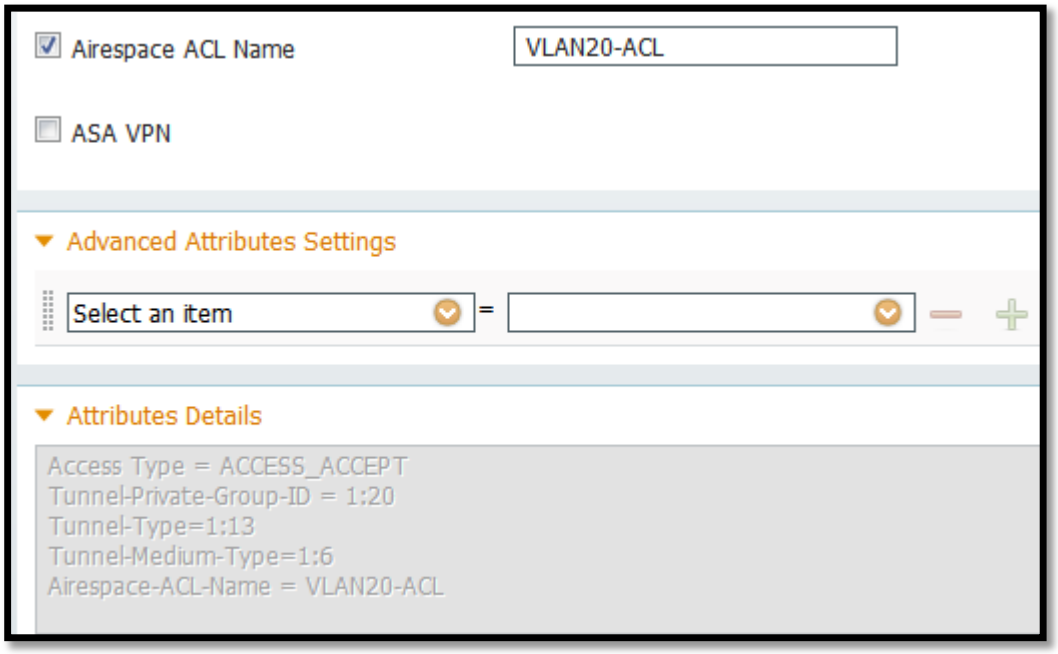
Finally we need an ACL that will be assigned to the authenticated clients :

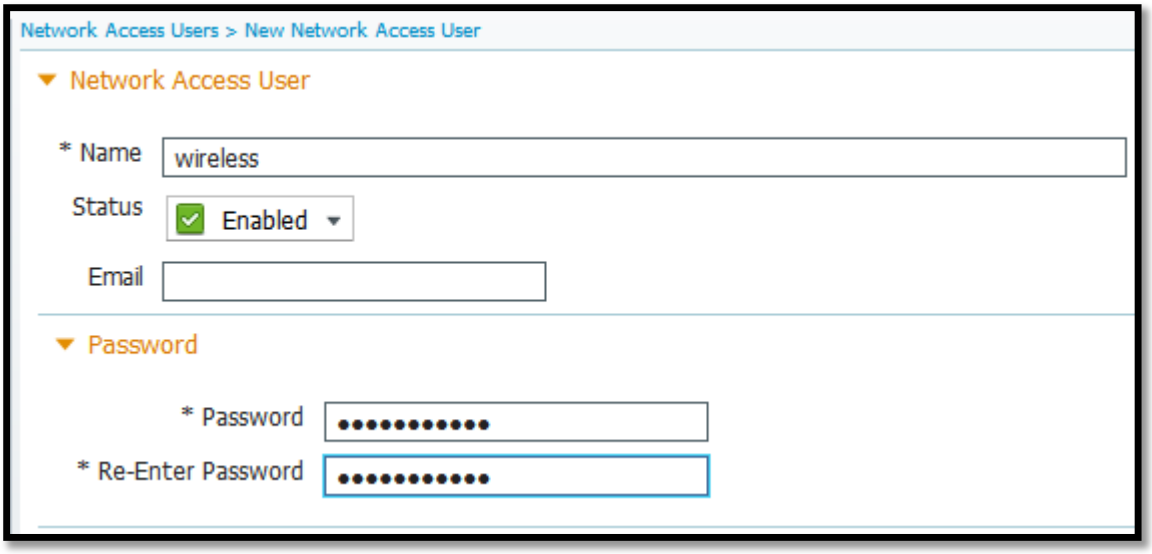
ISE

Add WLC to AAA Clients, create Authorization Profile and add a user :

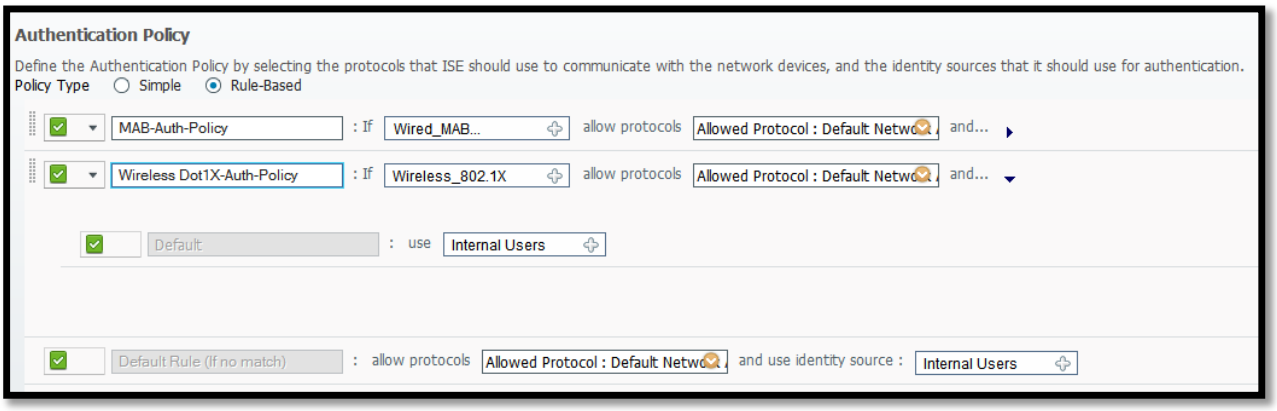


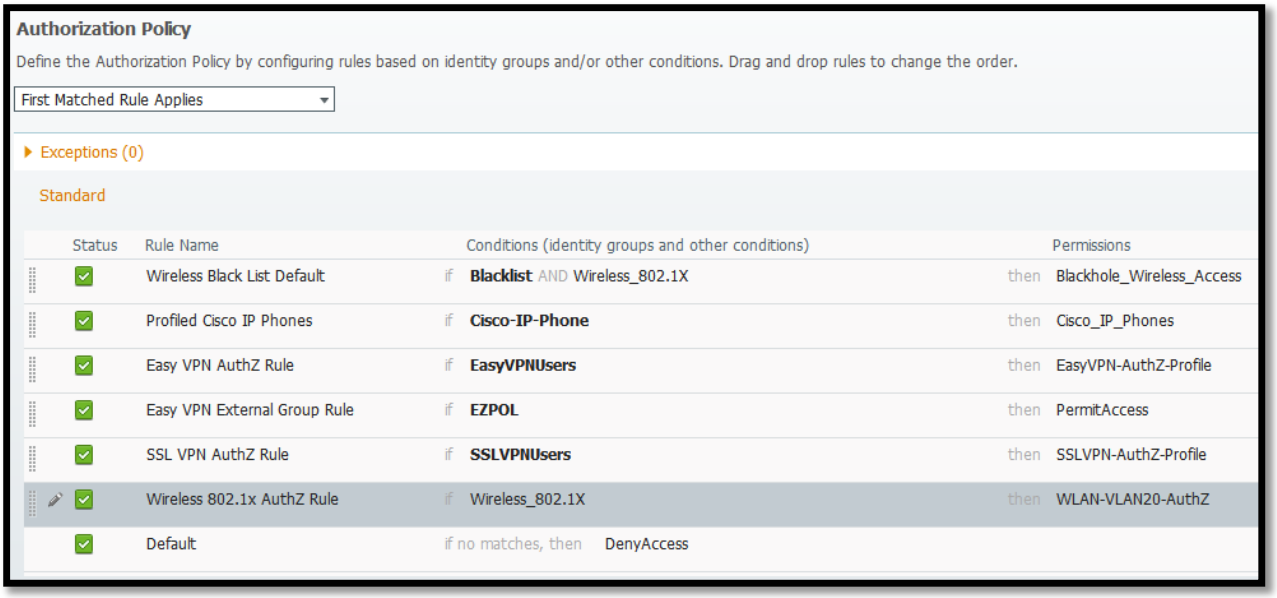






Both policies will use the “Wireless_802.1X” pre-built condition :





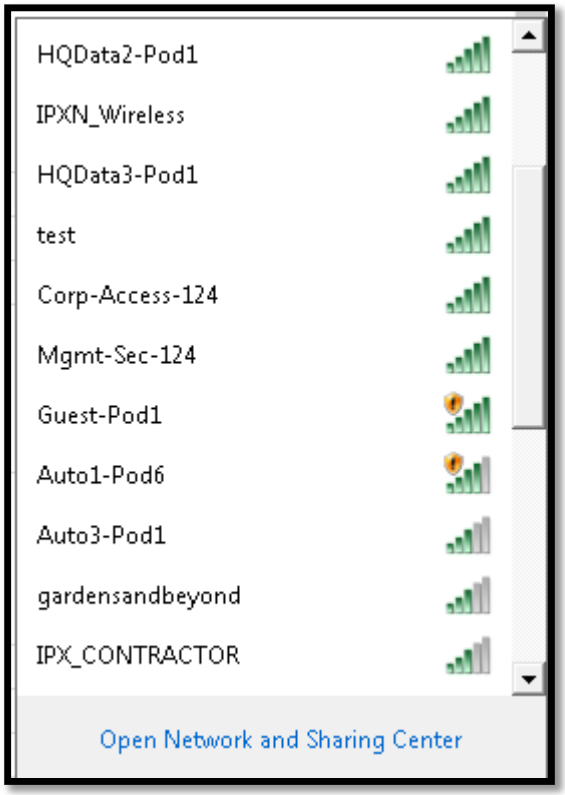
There were a lot of things to go through here. Always try to approach configuration in a step-by-step fashion without jumping between the configurations. Start on WLC or ISE and finish this part; then move on.

NAT on the ASA3 is required so the users could access 12.0.0.0 – an existing pool was used (same as for VLAN 100) which is fine in our case.

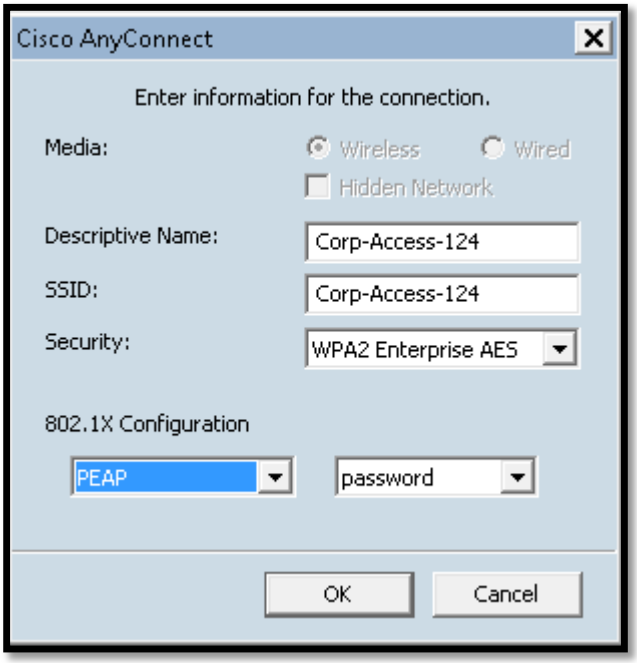
Verification

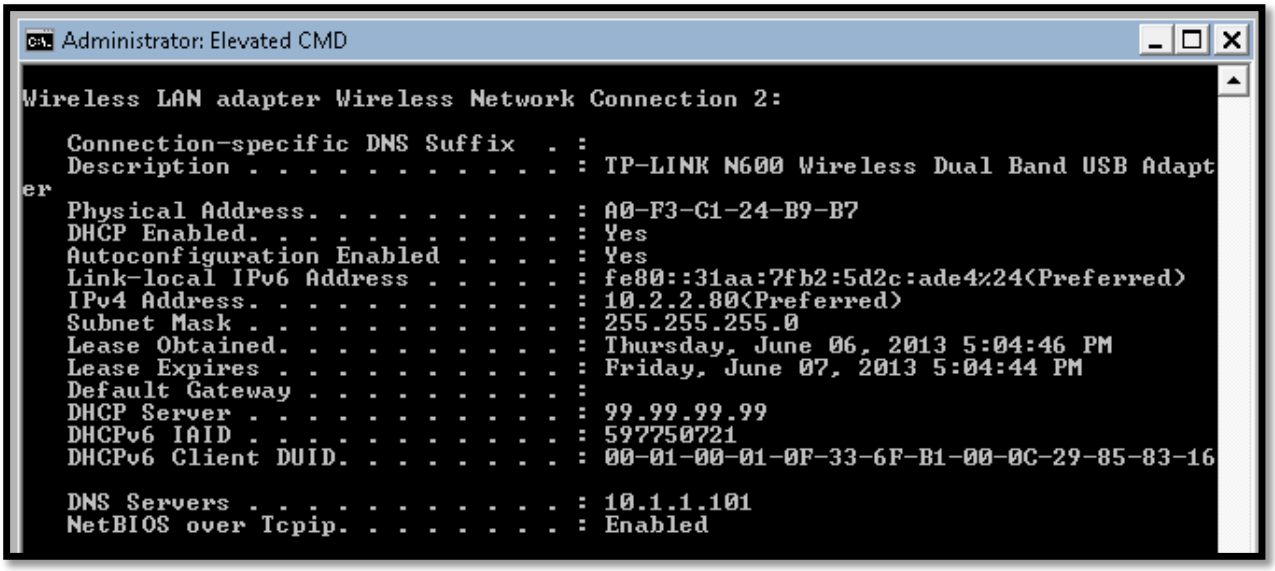
```
(Cisco Controller) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name              Slots  AP Model              Ethernet MAC
Location          Port  Country  Priority
------------------  -----  --------------------  -----------------  ------
----------  ----  -------  ------
LWAP4                 2     AIR-LAP1242AG-A-K9    00:18:73:cf:ef:0e
default location  1        US       1
```

```
(Cisco Controller) >show dhcp leases

       MAC                IP          Lease Time Remaining
00:18:73:cf:ef:0e    10.1.1.80    23 hours 49 minutes 35 seconds


(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      99.99.99.99     Static  No
No
vlan20                           1    20       10.2.2.250      Dynamic No
No
```



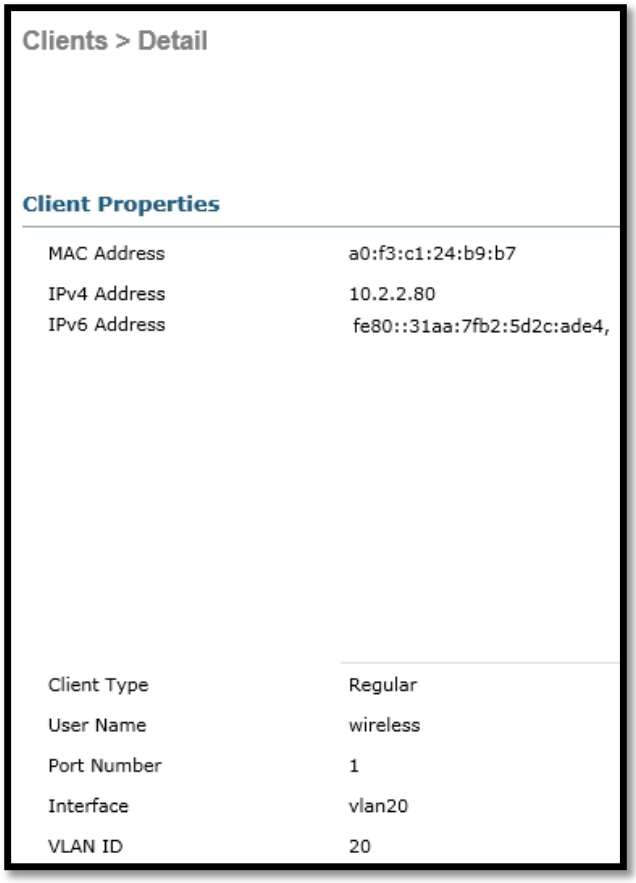
Now change the EAP method to PEAP, connect to the Corp-Access WLAN and authenticate :





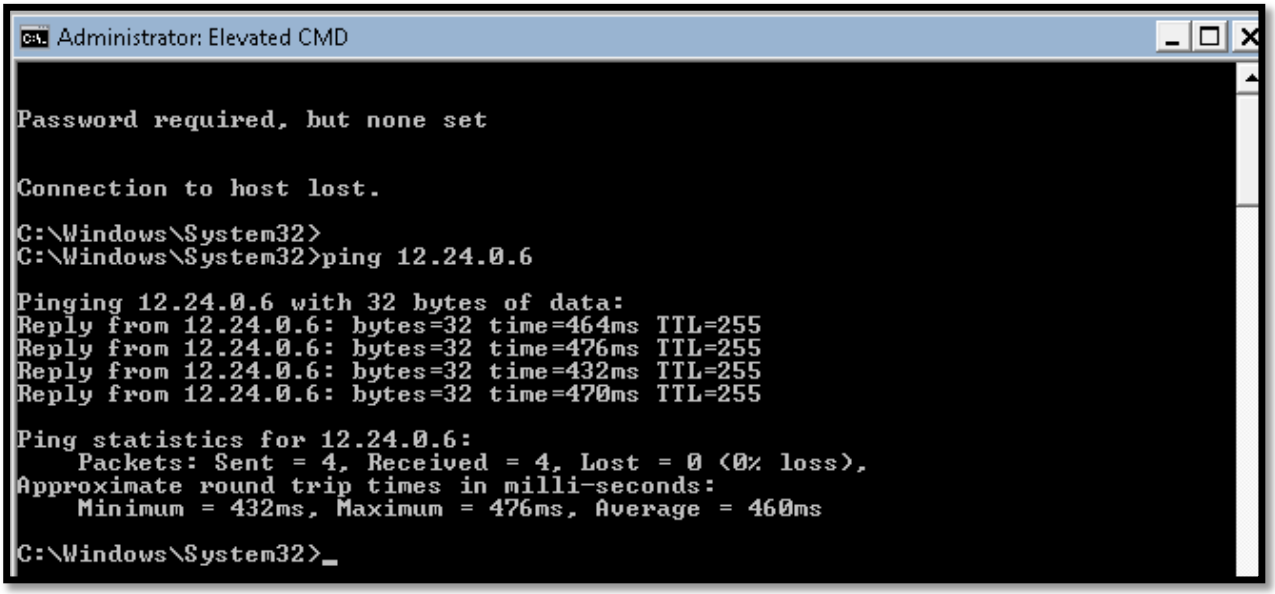

```
(Cisco Controller) >show dhcp leases

        MAC                IP          Lease Time Remaining
a0:f3:c1:24:b9:b7     10.2.2.80     23 hours 48 minutes 5 seconds
00:18:73:cf:ef:0e     10.1.1.80     22 hours 51 minutes 25 seconds
```

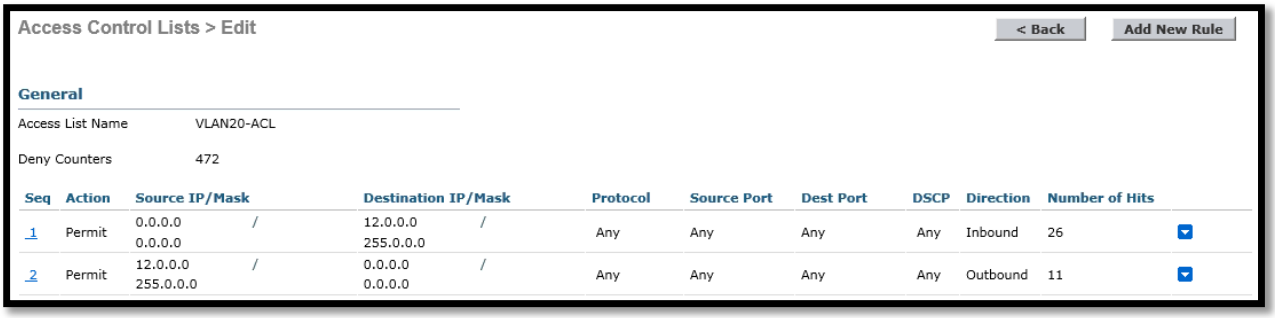
Under Monitor -> Clients you can take a look at some detailed information about associated client :



Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
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	VLAN20-ACL
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable





Access Control Lists > Edit

< Back | Add New Rule

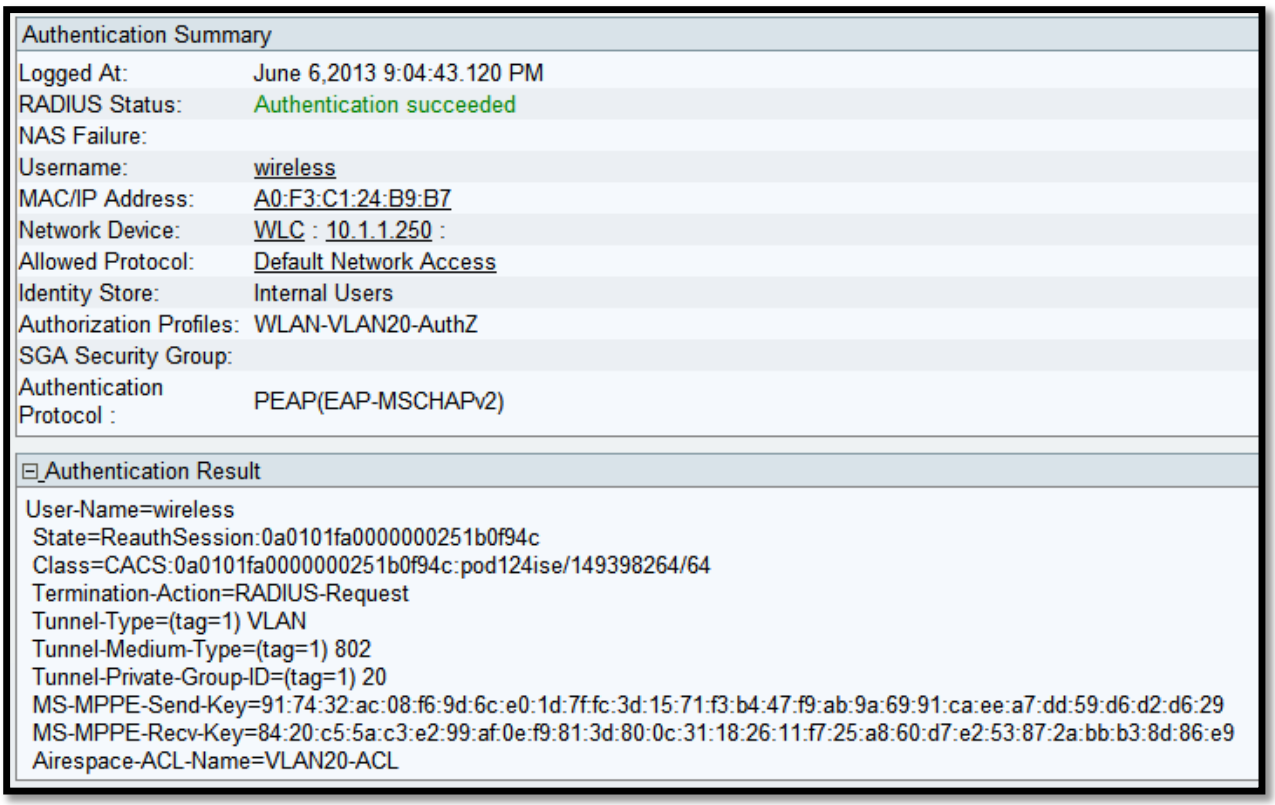
General

Access List Name: VLAN20-ACL

Deny Counters: 472

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	/	12.0.0.0 255.0.0.0	/	Any	Any	Any	Any	Inbound	26
2	Permit	12.0.0.0 255.0.0.0	/	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	Outbound	11

Don’t forget about ISE Live Logs :



Authentication Summary

Logged At:	June 6,2013 9:04:43.120 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	wireless
MAC/IP Address:	A0:F3:C1:24:B9:B7
Network Device:	WLC : 10.1.1.250 :
Allowed Protocol:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	WLAN-VLAN20-AuthZ
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

Authentication Result

User-Name=wireless
State=ReauthSession:0a0101fa0000000251b0f94c
Class=CACS:0a0101fa0000000251b0f94c:pod124ise/149398264/64
Termination-Action=RADIUS-Request
Tunnel-Type=(tag=1) VLAN
Tunnel-Medium-Type=(tag=1) 802
Tunnel-Private-Group-ID=(tag=1) 20
MS-MPPE-Send-Key=91:74:32:ac:08:f6:9d:6c:e0:1d:7f:fc:3d:15:71:f3:b4:47:f9:ab:9a:69:91:ca:ee:a7:dd:59:d6:d2:d6:29
MS-MPPE-Recv-Key=84:20:c5:5a:c3:e2:99:af:0e:f9:81:3d:80:0c:31:18:26:11:f7:25:a8:60:d7:e2:53:87:2a:bb:b3:8d:86:e9
Airespace-ACL-Name=VLAN20-ACL

Task 5.4: Access Control (3 Points)

- On R9 Create a view called “limited”
- This view should be accessed by any user that telnets into R9 and uses the username “limited” with a password “cisco”
- The user should automatically be placed in the view
- Make sure that the user can only enter the following commands :
  - Show clock
  - Show ip interface brief
- The console should not be affected

Detailed Solution

R9

```
enable secret ipexpert

aaa new-model
aaa authentication login limited local
aaa authorization exec LIMITED local

username ipexpert privilege 15 password 0 ipexpert
username limited view limited password 0 cisco

parser view limited
 secret ipexpert
 commands exec include show ip interface brief
 commands exec include show clock

line vty 0 4
 password cisco
 authorization exec LIMITED
 login authentication limited
```

Role Based CLI Access is the tool you can use locally to mimic real command authorization that can be only performed with TACACS+.

To configure this feature you need to first define enable secret password (it was not given so use “ipexpert” according to the General Rules) and then access the so-called Root View which is where you can define other views. And a view is simply a set of commands you want to make accessible to a particular user – this parameter is then assigned as a Shell attribute “view”.

User “ipexpert” was created as a safeguard – if you messed up with AAA configuration you could lock yourself out of the console (note in this case we did not apply “none” method list to the console line – just to show you the other way of doing things).

Verification

First telnet as “limited”, then as “ipexpert” :

```
R6#telnet 12.24.0.9
Trying 12.24.0.9 ... Open


User Access Verification

Username: limited
Password:

R9>sh parser view
Current view is 'limited'

R9>show ?
  clock   Display the system clock
  flash:  display information about flash: file system
  ip      IP information
  parser  Show parser commands

R9>show clock

*22:29:49.028 UTC Thu Jun 6 2013
R9>sh ip ?
  interface  IP interface status and configuration

R9>sh ip int br
```

```
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  administratively down
down
FastEthernet0/1        172.26.26.9     YES manual up                    up
Serial0/2/0            unassigned      YES unset  administratively down
down
Serial0/2/1            unassigned      YES unset  administratively down
down
Loopback0              9.9.9.9         YES manual up                    up

R9>?
Exec commands:
  <1-99>      Session number to resume
  credential  load the credential info from file system
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information

R9>


R1#telnet 172.26.26.9
Trying 172.26.26.9 ... Open


User Access Verification

Username: ipexpert
Password:

R9#sh pars view
No view is active ! Currently in Privilege Level Context

R9#sh priv
Current privilege level is 15
```

6.0 Advanced Security (4 points)

Task 6.1: FPM (4 Points)

- Create an FPM policy on R6 that matches the following :
  - IP
  - TCP port 80
  - Offset 0
  - Size 32
  - Downloaded filename (using GET method) starts with "%"
- This should be applied to Fa0/1 and dropped and logged if detected

Detailed Solution

R6

```
load protocol system:fpm/phdf/ip.phdf
load protocol system:fpm/phdf/tcp.phdf

class-map type stack match-all HTTP_STACK
 match field IP protocol eq 0x6 next TCP
 match field TCP dest-port eq 0x50 next TCP

class-map type access-control match-all EXPLOIT_CLASS
 match start TCP payload-start offset 0 size 32 regex "GET /%.*"

policy-map type access-control FPM_HTTP
 class EXPLOIT_CLASS
   drop
   log

policy-map type access-control FPM_POL
 class HTTP_STACK
  service-policy FPM_HTTP

interface Fa0/1
 service-policy type access-control input FPM_POL
```

The ".*" part was put at the end of regex to account for anything else after the sought string. Also note that regex is fully case-sensitive.

Verification

First one goes fine since it does not match our offending characteristic :

```
R7#copy http://12.64.65.5/FileOK null0
Destination filename [null0]?
Accessing http://12.64.65.5/FileOK...
%Error opening http://12.64.65.5/FileOK (No such file or directory)
```

This one, however, gets dropped :

```
R7#copy http://12.64.65.5/%FileOK null0
Destination filename [null0]?
Accessing http://12.64.65.5/%...

R6#
*Jun  6 22:49:04.016: %SEC-6-IPACCESSLOGP: list EXPLOIT_CLASS denied tcp
12.24.0.7(40069) (FastEthernet0/1 ) -> 12.64.65.5(80), 1 packet


R6#show policy-map type access-control int f0/1
 FastEthernet0/1

  Service-policy access-control input: FPM_POL

    Class-map: HTTP_STACK (match-all)
      75 packets, 5765 bytes
      5 minute offered rate 0 bps
      Match: field IP protocol eq 0x6 next TCP
      Match: field TCP dest-port eq 0x50 next TCP

      Service-policy access-control : FPM_HTTP

        Class-map: EXPLOIT_CLASS (match-all)
          11 packets, 1925 bytes
          5 minute offered rate 0 bps
          Match: start TCP payload-start offset 0 size 32 regex "GET /%.*"
      drop
```

```
    log

      Class-map: class-default (match-any)
        64 packets, 3840 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any

  Class-map: class-default (match-any)
    210 packets, 24262 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

7.0 Attack Mitigation (2 points)

Task 7.1: IP Address Spoofing Protection (2 Points)

- Configure the ASA4 such that it prevents anyone on the outside from spoofing the internal Network
- Configure R8 for RFC2827 filtering on the Serial interface, however do not configure an ACL to do this. You should be as strict as possible
- On R8 the IPS should not fire off signature 1102 when you test to yourself

Detailed Solution

ASA4

```
ip verify reverse-path interface outside
```

R8

```
int s0/0/0
 ip verify unicast source reachable-via rx allow-self-ping

ip ips signature-definition
 signature 1102 0
  status
   enabled false
   retired true
```

If R8 was running Frame-Relay you would have to create a mapping for itself.

Verification

Before you disable the signature :

```
R8#ping 12.87.0.8 rep 1
```

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 12.87.0.8, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 4/4/4 ms
R8#
*Jun  6 21:51:54.600: %IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:100
Impossible IP Packet [12.87.0.8:8 -> 12.87.0.8:0] VRF:NONE RiskRating:100
*Jun  6 21:51:54.600: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo
Request [12.87.0.8:8 -> 12.87.0.8:0] VRF:NONE RiskRating:25
*Jun  6 21:51:54.604: %IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:100
Impossible IP Packet [12.87.0.8:0 -> 12.87.0.8:8] VRF:NONE RiskRating:100
```

After :

```
R8#ping 12.87.0.8 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 12.87.0.8, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 8/8/8 ms
R8#
*Jun  6 21:55:03.684: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo
Request [12.87.0.8:8 -> 12.87.0.8:0] VRF:NONE RiskRating:25

R8#sh ip int s0/0/0 | s veri
  IP verify source reachable-via RX, allow self-ping
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate

ASA4(config)# sh ip verify statistics interface outside
interface outside: 0 unicast rpf drops
```