

IPexpert's Lab Preparation Workbook

for the Cisco® CCIE™ Security Volume 1
Complete Workbook



Table of Contents

Section 1	12
ASA Firewall	12
Lab-1: ASA Initialization Overview	12
General Rules	12
Pre-setup	13
Lab 1: Configuration Tasks	15
Task 1: Initialization ASA-3	15
Task 2: Initialization ASA-1	16
Lab 2: ASA IPv4 Unicast Routing Overview	17
General Rules	17
Pre-setup	17
Lab 2: Configuration Tasks	20
Task 1: Static Routes on ASA-3 for internal networks	20
Task 2: Floating static default routes with object tracking	20
Task 3: OSPFv2 on the ASA	20
Task 4: EIGRP on ASA	21
Task 5: RIPv2 on the ASA	21
Task 6: DMZ Communication	21
Lab 3 ASA System Management and IP Services	22
General Rules	22
Pre-setup	22
Lab 3: Configuration Tasks	23
Task 1: NTP server and client configuration on ASA-3 and R4	23
Task 2: NTP server and client configuration on ASA-1 and R5	23
Task 3: DNS configuration on ASA-3	23
Task 4: DHCP server configuration on ASA-3	23
Task 5: DHCP relay services configuration on ASA-1	23
Task 6: Logging configuration on ASA-3	24
Task 7: Logging configuration on ASA-1	24
Task 8: SNMPv3 configuration on ASA-3	24
Task 9: SNMPv2c configuration on ASA-1	24
Task 10: Management access configuration on ASA-1 and ASA-3	25
Lab 4: Address translations and access control on the ASA	26
General Rules	26
Pre-setup	26
Lab 4: Configuration Tasks	27

Task 1: Static auto NAT for dmz1 on ASA-3.....	27
Task 2: Dynamic auto NAT/PAT for dmz1 on ASA-3.....	27
Task 3: Static auto NAT for the dmzserver interface on ASA-3.....	28
Task 4: Static object NAT between dmz1 and dmzserver on ASA-3.....	28
Task 5: DNS rewrite using static auto NAT for the inside interface on ASA-3.....	29
Task 6: Static auto NAT for INSIDE on ASA-3	29
Task 7: Static PAT/port redirection using auto NAT for INSIDE on ASA-3.....	29
Task 8: Static PAT/port redirection using auto NAT for INSIDE on ASA-3.....	29
Task 9: Dynamic PAT and DNS rewrite on ASA-3	30
Task 10: Manual dynamic NAT on ASA-3	30
Task 11: Manual dynamic PAT on ASA-3	30
Task 12: Manual static identity NAT on ASA-3.....	30
Task 13: Manual static identity NAT on ASA-3.....	31
Task 14: Twice NAT on ASA-3	31
Task 15: NAT control on ASA-1.....	31
Task 16: Dynamic NAT/PAT on ASA-1	31
Task 17: Policy Dynamic PAT on ASA-1	31
Task 18: Static NAT on ASA-1	31
Task 19: Static Identity NAT on ASA-1.....	32
Task 20: Static PAT on ASA-1.....	32
Task 21: Static PAT on ASA-1.....	32
Task 22: Identity NAT on ASA-1	32
Task 23: NAT Exception on ASA-1	32
Task 24: Outside/Destination Static NAT on ASA-1.....	33
Task 25: DNS doctoring using NAT.....	33
Task 26: Enhanced Service Object-Groups.....	33
Task 27: ICMP Filters on ASA-1.....	33
Task 28: uRPF and fragmented packets on ASA-1	33
Task 29: ACL Logging on ASA-1	34
Task 30: Control Plane ACL on ASA-1	34
Task 31: Management access for ASA-1	34
Lab 5: High Availability and Modular Policy Framework on the ASA	35
General Rules	35
Pre-setup.....	35
Lab 5: Configuration Tasks	37
Task 1: Basic Initialization ASA-3.....	37
Task 2: Configure Active/Standby Failover	37
Task 3: Routing ASA-3.....	38
Task 4: Static Auto-NAT for INSIDE on ASA-3	38
Task 5: Dynamic PAT for INSIDE on ASA-3.....	38

Task 6: IPS Software module traffic diversion on ASA-3	39
Task 7: ICMP inspection on ASA-3	39
Task 8: DNS inspection on ASA-3	39
Task 9: FTP inspection on ASA-3	39
Task 10: HTTP inspection and content filtering on ASA-3	39
Task 11: ESMTP inspection on ASA-3	40
Task 12: IM inspection on ASA-3	40
Task 13: IP Options inspection on ASA-3	40
Task 14: IPSec passthrough inspection on ASA-3	40
Task 15: BGP through ASA-3	40
Task 16: TCP normalization on ASA-3	41
Task 17: Traceroute through ASA-3	41
Task 18: Netflow/NSEL on ASA-3	41
Task 19: LLQ on ASA-3	42
Task 20: Management Traffic Connection Limits on ASA-3	42
Task 21: Threat Detection on ASA-3	42
Lab 6: Transparent Firewall.....	43
General Rules	43
Pre-setup	43
Lab 6: Configuration Tasks	46
Task 1: Basic Initialization ASA-3	46
Task 2: ACLs on ASA-3	46
Task 3: Basic Initialization the ASA-1	46
Task 4: ACLs on ASA-1	47
Task 5: Transparent Firewall NAT/PAT on ASA-1	47
Task 6: Ethertype ACLs on ASA-1	47
Task 7: Dynamic ARP inspection on ASA-1	47
Task 8: Prevent MAC Spoof attacks on ASA-1	47
Lab 7: Active/Standby Transparent Firewall	48
General Rules	48
Pre-setup	48
Lab 7: Configuration Tasks	51
Task 1: Basic VLAN Setup	51
Task 2: Failover Configuration	51
Task 3: Basic Initialization ASA-3	51
Task 4: ACLs on ASA-3	52
Task 5: Transparent firewall NAT on ASA-3	52
Lab 8: Routed Mode Multi-Context and Active/Active Failover	53
General Rules	53
Pre-setup	53

Lab 8: Configuration Tasks	55
Task 1: Basic VLAN Setup	55
Task 2: Firewall Mode on ASA-3	55
Task 3: VLAN Sub-interface creation on ASA-3	55
Task 4: Context creation on ASA-3	55
Task 5: Admin context configuration on ASA-3	56
Task 6: f2 context configuration on ASA-3	57
Task 7: F1 context configuration on ASA-3	57
Task 8: Basic VLAN Setup	59
Task 9: Failover Configuration	59
Task 10: Active/Active Failover Configuration on ASA-3	59
Task 11: Re-configure Active and Standby IP address	59
Lab 9: Multi-Mode Transparent Firewall with Active/Active Failover	60
General Rules	60
Pre-setup	60
Lab 9: Configuration Tasks	64
Task 1: Basic VLAN Setup	64
Task 2: Firewall Mode on ASA-3	64
Task 3: VLAN Sub-interface creation on ASA-3	64
Task 4: Context and failover group creation on ASA-3	64
Task 5: T1 context configuration	65
Task 6: T2 context configuration	66
Lab 10: Routed Mode IPv6 on ASA	68
General Rules	68
Pre-setup	68
Lab 10: Configuration tasks	70
Task 1: Initialization of ASA-3	70
Task 2: Routing on ASA-3	70
Task 3: IPv6 and IPv4 filters on ASA-3	70
Task 4: IPv6 Management access to ASA-3	70
Task 5: Configure IPv6 Active/Standby Failover	71
Task 6: IPv6 inspection using MPF	71
Lab 11: Transparent Mode using IPv6	72
General Rules	72
Pre-setup	72
Task 1: Basic Initialization ASA-3	74
Task 2: IPv4 and IPv6 ACLs	74
Section 2	75
IOS Firewall	75

General Rules	75
Pre-setup	76
Lab-2 Configuration tasks	78
Task 1: IOS NAT	78
Task 2: IOS Access-Lists	78
Task 3: Reflexive Access-Lists	79
Task 4: CBAC	79
Task 5: CBAC Application Inspection & Tuning	79
Task 6: Zone-Based Firewall	80
Task 7: Zone-Based Firewall Inspection & Tuning	80
Task 8: User-Based Firewall	80
Section 3	82
Ironport S-Series: WSA	82
Lab-1: WSA Initialization Overview	82
General Rules	82
Pre-setup	83
Lab 1: Configuration Tasks	85
Task 1: Initialization WSA	85
Task 2: Enable basic web and FTP proxy function and PAC file hosting	86
Task 3: Configure acknowledgement and custom end-user notifications	86
Task 4: Configuring Active Directory authentication for users	87
Lab-2: Configuring Acceptable Use Policies on WSA for HTTP and FTP	87
General Rules	87
Pre-setup	88
Task 1: Configure Access Policies	89
Task 2: Configure Guest privileges and Custom URL policy - 1	92
Task 3: Configure Custom URL policy - 2	92
Task 4: Configure Custom URL policy - 3	92
Task 5: Configure Custom URL policy - 4	93
Task 6: Configure Custom URL policy - 5	93
Task 7: Configure Custom URL policy - 6	93
Task 8: Configure Custom URL policy - 7	93
Lab-3: Configuring Acceptable Use Policies on WSA for HTTPS	94
General Rules	94
Pre-setup	94
Task 1: Configure WSA for HTTPS Proxy	95
Task 2: Decryption Policies - 1	95
Task 3: Decryption Policies - 2	95
Task 4: Decryption Policies - 3	96

Task 5: Decryption Policies – 4	96
Task 6: Decryption Policies – 5	96
Task 7: Decryption Policies – 6	96
Task 8: Decryption Policies – 7	96
Task 9: Decryption Policies – 8	96
Lab-4: Configuring advanced access policies for downloads	96
General Rules	97
Pre-setup	97
Task 1: Configure download bandwidth limits and object download blocking.....	97
Task 2: Configure Application visibility and control for web traffic.....	97
Lab-5: Configuring data transfer policies.	98
General Rules	98
Pre-setup	98
Task 1: Configure outbound malware scanning	99
Task 2: Configure data transfer policies.....	99
Lab-6: Configuring WCCP and transparent proxy mode with Single Sign On.	99
General Rules	99
Pre-setup	100
Task 1: Configure transparent proxy bypass	100
Task 2: Configure transparent proxy bypass	100
Task 3: SSO using Mozilla.....	100
Lab-7: Configuring L4TM on WSA	101
General Rules	101
Pre-setup	101
Task 1: Configure SPAN/RSPAN	101
Task 2: Configure transparent proxy bypass	101
Task 3: Configure L4TM.	102
Section 4	102
ISE: Identity Services Engine	102
Lab-1: Basic Configuration of ISE.....	103
General Rules	103
Pre-setup	103
Lab 1: Configuration Tasks	105
Task 1: Basic Setup of ISE	105
Lab-2: Configuring network resources and profiling on ISE	106
General Rules	106
Pre-setup	106
Task 1: Configure NDG's and AAA clients on ISE and switches.....	107
Task 2: Configure profiling.....	107

Lab-3: Configuring ISE and Switches for MAB and 802.1x	108
General Rules	108
Pre-setup	108
Task 1: Configuring AAA clients for wired MAB and 802.1x with low impact mode....	109
Task 2: Configuring ISE for wired MAB and 802.1x with low impact mode.....	109
Task 3: Configuring ISE with specific authorization policies.	110
Task 3: Configuring WLC and ISE for Wireless 802.1x	114
Lab-4: Configuring CWA and guest access	120
General Rules	120
Pre-setup	120
Task 1: Configuring Wired CWA	121
Task 2: Configuring Guest Access.....	122
Task 3: Configuring Wireless Guest Access and CWA	125
Lab-5: Configuring MACSec.....	128
General Rules	128
Pre-setup	128
Task 1: Configuring MACSec Switch-Host	129
Task 2: Configuring MACSec Switch-Switch	129
Section 5	130
ACS: Cisco Access Control System 5.3	130
General Rules	130
Pre-setup	131
Lab 1: Configuration Tasks	133
Task 1: Basic Setup of ACS.....	133
Lab-2: Configuring AAA clients for authentication and EXEC authorization	136
General Rules	136
Pre-setup.....	136
Task 1: Configure Switches (SW1 to SW4) for authentication and EXEC authorization.	137
Task 2: Configure Routers (R1 and R2) for authentication and EXEC authorization...	137
Task 3: Configure R4 for Role Based CLI.....	138
Task 4: Configure R5 for Role Based CLI.....	138
Task 5: Configure ASA for authentication.....	139
Task 6: Configure ACS for EXEC authorization TACACS+ Device Admin access service for routers.....	139
Task 7: Configure ACS for authorization rules in TACACS+ Device Admin access service for ASA.....	140
Task 8: Configure ACS for EXEC authorization RADIUS Device Admin access service for switches	140

Task 9: Advanced authorization rules for RADIUS and TACACS+ Device Admin access policies.....	141
Lab-3: Configuring AAA clients for command authorization and accounting	142
General Rules	142
Pre-setup.....	142
Task 1: Configure R1 and R2 for command authorization.....	143
Task 2: Configure ACS for command authorization.....	143
Task 3: Configure ASA and ACS for command authorization.....	144
Task 4: Configure EXEC Accounting.....	144
Task 5: Configure R1 and R2 for command Accounting.....	144
Task 6: AAA configuration removal on ASA.....	144
Lab-4: Configuring Authentication proxy and cut-through proxy.....	144
General Rules	145
Pre-setup.....	145
Task 1: Remove AAA configuration.....	146
Task 2: ASA Cut through proxy using RADIUS.....	146
Task 3: IOS Authentication proxy using RADIUS.....	146
Section 6.....	147
IPS: Intrusion Prevention System.....	147
General Rules	147
Pre-setup.....	148
Lab 6: Cisco IPS.....	150
Task 1: Sensor Setup and Administration	150
Task 2: Password Protection.....	150
Task 3: Network Time Protocol	150
Task 4: Miscellaneous Configuration.....	150
Task 5: Creating Virtual Sensors.....	151
Task 6: Monitoring Traffic with IDS	151
Task 7: IPS Inline Interface Pair	151
Task 8: IPS Inline VLAN Pair.....	151
Task 9: Tuning Signatures, Variables and Custom Signatures.....	152
• Configure a custom signature for VS1 called “AtomicIP2” to detect telnet traffic. The telnet traffic must have a source IP of 10.7.7.7 and destination IP of 10.8.8.8. IPS should drop the connection and produce an alert. The signature should fire every time with severity of High.	153
• Configure a custom signature for VS2 called “TCPFLAGFILTER” to detect TCP traffic which has the SYN flag set and the ACK flag not set. IPS should produce verbose alert. Change the event count key and summary key to attacker and victim address and the alert type as fire all. Do not use dynamic summarization.....	153

• Configure a custom signature for VS1 called “CustHTTPsig1” to detect HTTP traffic which has “facebook” anywhere in the URI. IPS should deny packets inline and produce alerts with high severity.....	153
• Configuring a custom signature to deny ARP packets with a broadcast address in the Source IP field. Apply this to VS2 and change the alert severity to high. The custom signature should have a name of CustomARP.	153
• Configure a custom signature for VS2 called “CustomAICsig” to detect HTTP traffic based on AIC engine which has max-outstanding-request of 10. IPS should deny packets inline and produce alerts with high severity.....	153
Task 10: Advanced IPS and Anomaly Detection	153
Task 11: Blocking using the Security Appliance.	153
Task 12: Blocking using IOS Devices.....	154
Task 13: Rate Limiting	154
Task 14: IOS IPS	154
Task 15: IOS IPS Tuning.....	154
Section 7	155
Virtual Private Networks.....	155
General Rules	155
Pre-setup.....	156
Lab-7 Configuration tasks	159
Task 1: IOS CA Server	159
Task 2: IOS – ASA L2L.....	159
Task 3: IPv6 L2L IOS	159
Task 4: IPv6 VRF-Aware L2L.....	159
Task 5: IPsec Remote Access IOS	160
Task 6: IPsec Remote Access IOS with RADIUS	160
Task 7: IPsec Remote Access ASA	160
Task 8: IPsec Remote Access ASA with RADIUS.....	161
Task 9: DMVPN Phase I.....	161
Task 10: DMVPN Phase II.....	161
Task 11: DMVPN Phase III.....	161
Task 12: Redundant GETVPN.....	161
Task 13: SSL Remote Access IOS.....	162
Task 14: SSL Remote Access IOS - AnyConnect.....	162
Task 15: SSL Remote Access ASA	162
Task 16: IPv6 SSL Remote Access ASA - AnyConnect.....	162
Task 17: IKEv2 L2L IOS ASA.....	163
Task 18: IKEv2 Remote Access IPsec ASA (AnyConnect).....	163
Task 19: IPv6 FlexVPN L2L.....	163

Task 20: FlexVPN IPSec Remote Access	163
Task 21: FlexVPN Hub & Spoke.....	164
Task 22: FlexVPN EAP Authentication.....	164
Section 8.....	165
Wireless.....	165
General Rules	165
Pre-setup.....	166
Lab-8 Configuration tasks.....	168
Task 1: WLC Initialization.....	168
Task 2: WLC Basic Configuration	168
Task 3: DHCP Proxy Mode.....	168
Task 4: DHCP Bridging Mode	168
Task 5: WLAN Security	168
Section 9.....	170
Advanced Security	170
General Rules	170
Pre-setup.....	171
Lab-9 Configuration tasks.....	173
Task 1: IP Routing & Route Filtering.....	173
Task 2: Routing Protocol Authentication.....	173
Task 3: Basic Device Access Configurations	173
Task 4: Controlling Device Access.....	174
Task 5: Management Restrictions.....	174
Task 6: ASA Control Plane protection	174
Task 7: Control Plane Policing.....	174
Task 8: Control Plane Protection.....	174
Task 9: Management Plane Protection	175
Task 10: NTP	175
Task 11: SNMP & CPU Statistical Gathering.....	175
Task 12: DHCP & DHCPv6.....	175
Task 13: Unnecessary Services & Hardening.....	176
Task 14: IP Accounting.....	176
Task 15: Core Dumps.....	176
Task 16: Memory Checks	176
Task 17: CPU, Memory Protection & NVGEN Enhancement.....	177
Task 18: Managing Configuration Files	177
Section 10	178

Network Attack Mitigation.....	178
General Rules	178
Pre-setup	179
Lab-10 Configuration tasks.....	182
Task 1: Traffic Marking & Classification.....	182
Task 2: NBAR & NBAR Next Generation	182
Task 3: Policy Based Routing	183
Task 4: CAR	183
Task 5: Flexible NetFlow	183
Task 6: ICMP & UDP Flooding Attacks	183
Task 7: Fragmentation Attacks.....	184
Task 8: IP Options Attacks.....	184
Task 9: Layer 3 Spoofing Attacks.....	184
Task 10: TCP SYN Attacks.....	184
Task 11: Application Attacks & FPM	185
Task 12: DDoS Attacks & RTBH.....	185
Task 13: Layer 2 Security & Attacks.....	185
Task 14: Spanning-Tree Attacks	186
Task 15: DHCP Attacks & First Hop Security.....	186
Task 16: ARP & L2 Spoofing Attacks.....	186
Task 17: ND Cache Poisoning Attacks & SEND	186

Section 1

ASA Firewall

Lab-1: ASA Initialization Overview

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

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

General Rules

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

Estimated Time to Complete: **1 Hour**

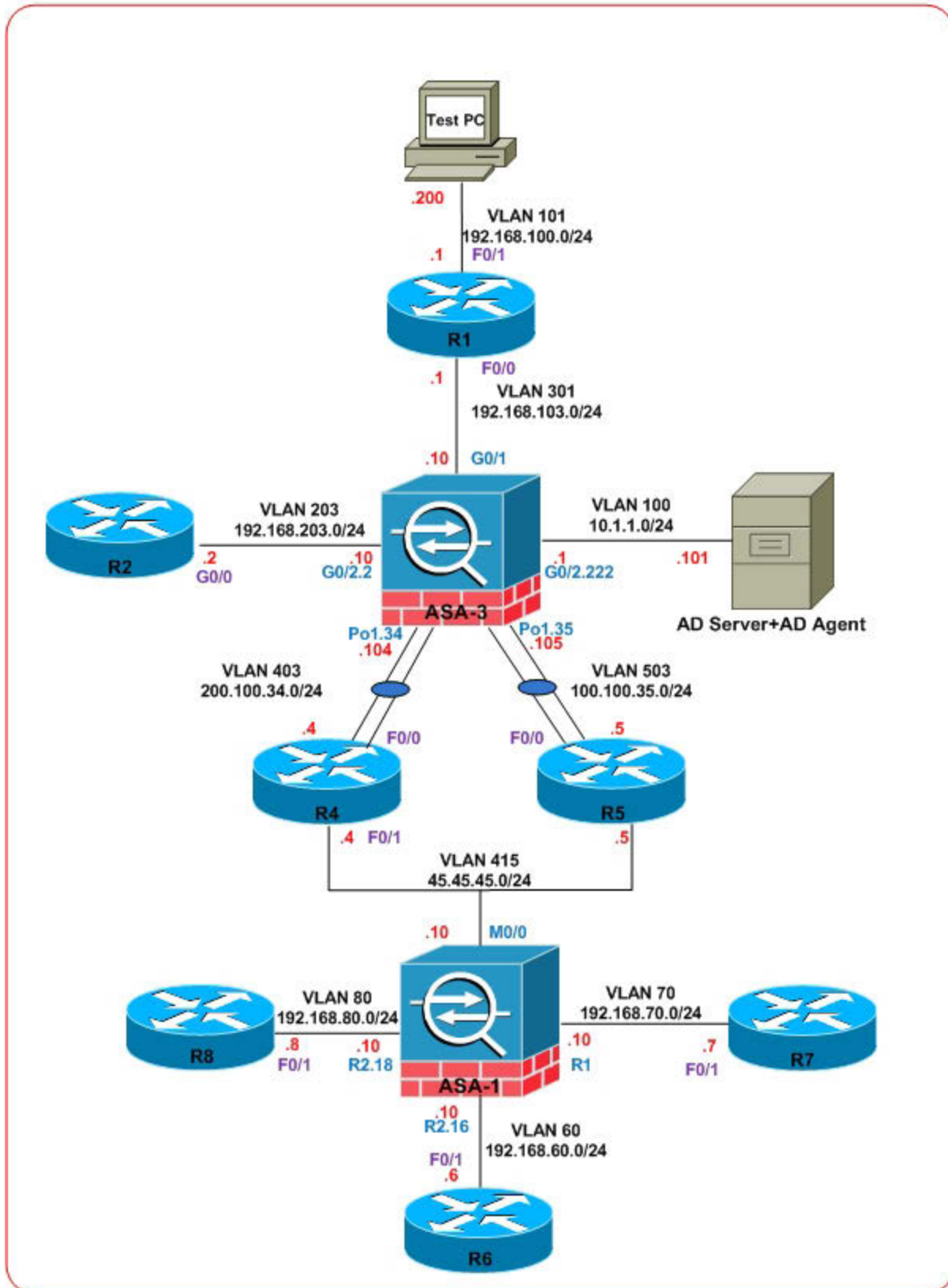
Pre-setup

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

NOTE: *Do not make additional configuration on the routers, unless explicitly asked for in the task; some switching configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 1.1 and refer to the general physical connectivity. Ensure that your ASA is in single context routed mode before you start the configuration. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.1 (Logical)



Lab 1: Configuration Tasks

Task 1: Initialization ASA-3

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

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

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

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

NOTE: Configure exact interface numbers and names

Task 2: Initialization ASA-1

- Configure a hostname of “ASA-001fw” on ASA-1
- ASA-003fw should have a domain name of ipexpert.com
- Configure the ASA-001fw outside interface and the appropriate switchports on the Catalyst with the specifications below. The management interface should be made a normal routed interface. After you perform this task, ensure that you can ping your directly connected neighbors R4 and R5.

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

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

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

NOTE: Configure exact interface numbers and names

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

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

NOTE: The names and interface numbers should be exact as stated in the tasks

Lab 2: ASA IPv4 Unicast Routing Overview

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

General Rules

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

Estimated Time to Complete: **2 Hours**

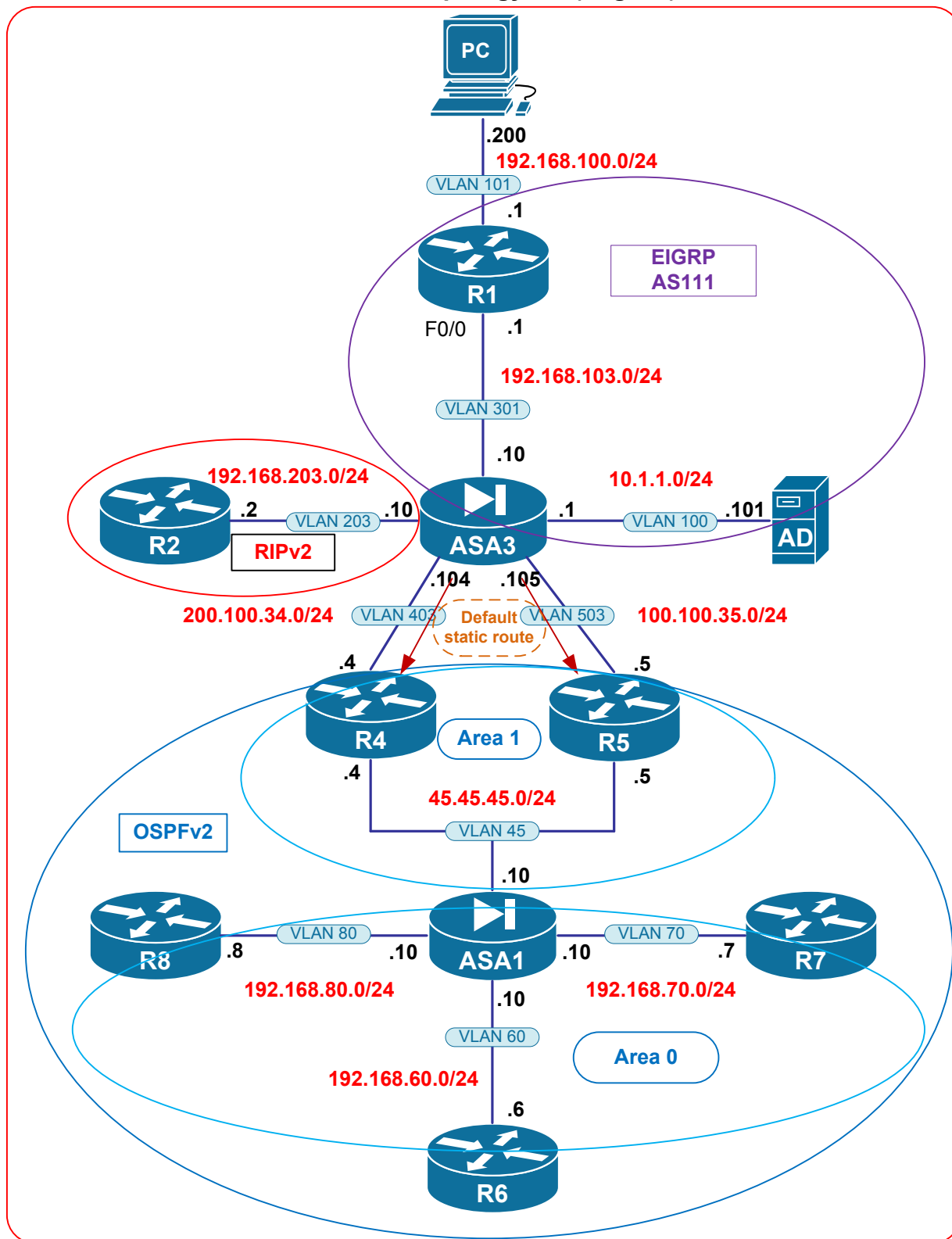
Pre-setup

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

NOTE: Routing has been pre-configured on the routers

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

Network Topology 1.1 (Logical)



LAB 2: IP Address Table of Routers

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

Lab 2: Configuration Tasks

NOTE: This Lab is built on the previous lab. Make sure you have completed Lab 1 and have direct L3 connectivity with the appropriate neighbors.

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

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

Task 2: Floating static default routes with object tracking

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

Task 3: OSPFv2 on the ASA

- Configure OSPFv2 on ASA-001fw. The Router-ID should be configured as 11.45.45.11. The outside interface should be in Area 1 and the internal interfaces (i.e. DMZs and inside interfaces) should be in Area 0.
- Authenticate all the adjacencies with MD5 authentication. The key number should be 1 and the pre-shared secret key should be "C1SC0123".
- Network statements should be as specific as possible.
- Do not advertise the R6 Loopback1 interface into OSPF area 1.
- Routers have been pre-configured. No additional configurations are required on the routers. Do not modify any configurations on the routers.
- Ensure you are able to ping the Loopbacks on R6, R7, R8, R4, R5, and the outside interfaces of ASA-003fw.

Task 4: EIGRP on ASA

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

Task 5: RIPv2 on the ASA

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

Task 6: DMZ Communication

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

Lab 3 ASA System Management and IP Services

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

General Rules

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

Estimated Time to Complete: **2 Hours**

Pre-setup

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

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

Lab 3: Configuration Tasks

NOTE: This lab is built on the previous lab. Make sure you have completed Lab 2 and have appropriate routes in the routing table.

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

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

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

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

Task 3: DNS configuration on ASA-3

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

Task 4: DHCP server configuration on ASA-3

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

Task 5: DHCP relay services configuration on ASA-1

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

Task 6: Logging configuration on ASA-3

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

Task 7: Logging configuration on ASA-1

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

Task 8: SNMPv3 configuration on ASA-3

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

Task 9: SNMPv2c configuration on ASA-1

- Configure a global community string of "SECURITY" and set the location to Moon.
- Only the NMS server IP of 192.168.60.100 can poll the ASA. Use a community string of "SECUR1TY".
- Send all traps except syslog to 192.168.60.101. Use a community string of "SECUR1TY".

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

- Configure ASDM and Telnet access on the inside interface from any hosts.
- Configure SSH access on the outside interface from any hosts for ASA-3.
- Configure SSH access on the outside interface to allow only 200.100.34.111 and 100.100.35.111 for ASA-1. (This will work after LAB 4 Translations/NAT).
- Change the Telnet password to "CC1E123" on both the ASAs.
- Use SSH version 2 only.
- Configure the above tasks on both of the ASAs. You are allowed to modify the VLAN on the switch to test ASDM access. The test PC should be in VLAN 101 only.
- You may create any local user account using local AAA authentication to test on ASA-1. You may test this after the NAT and ACL configuration given in LAB 4.
- Test the ASDM access to ASA-3 from the test PC.

Lab 4: Address translations and access control on the ASA

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

General Rules

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

Estimated Time to Complete: **4 Hours**

Pre-setup

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

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

Lab 4: Configuration Tasks

NOTE: This lab is built on the previous lab. Make sure you have completed Lab-3 and have routes in the routing table.

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

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

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

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

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

Real IP/ Subnet	Mapped IP / Subnet	Real Interface	Mapped Interface
192.168.203.0/24	200.100.34.203	Dmz1	Outside-1
192.168.203.0/24	100.100.35.203	Dmz1	Outside-2
Range 192.168.203.60 to 192.168.203.70	NAT Pool Range - 200.100.34.60 200.100.34.70 Backup PAT - 200.100.34.71	Dmz1	Outside-1
Real IP/ Subnet	Mapped IP / Subnet	Real Interface	Mapped Interface

Range 192.168.203.60 to 192.168.203.70	NAT Pool Range - 100.100.35.60 100.100.35.70 Backup PAT - 100.100.35.71	Dmz1	Outside-2
2.2.2.0/24	PAT Pool Range 200.100.34.80 to 200.100.34.85 Use round robin method	Dmz1	Outside-1
2.2.2.0/24	PAT Pool Range 100.100.35.80 to 100.100.35.85 Use round robin method	Dmz1	Outside-2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Task 10: Manual dynamic NAT on ASA-3

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

Task 11: Manual dynamic PAT on ASA-3

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

Task 12: Manual static identity NAT on ASA-3

- Create a loopback on R2 with an IP address of 222.222.222.222/32. Configure static identity NAT such that only outside users can ping that IP address. Use global ACLs to allow access.

- Advertise the new loopback into RIPv2 on R2 and create appropriate static routes on R4 and R5.

Task 13: Manual static identity NAT on ASA-3

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

Task 14: Twice NAT on ASA-3

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

Task 15: NAT control on ASA-1

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

Task 16: Dynamic NAT/PAT on ASA-1

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

Task 17: Policy Dynamic PAT on ASA-1

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

Task 18: Static NAT on ASA-1

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

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

Task 19: Static Identity NAT on ASA-1

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

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

Task 20: Static PAT on ASA-1

- Create a new loopback on R7 with an IP address of 177.177.177.177/32 and advertise that into OSPF.
- Any Telnet request that is sent to the ASA's outside interface should be redirected to 177.177.177.177.
- Create a new loopback on R8 with an IP address of 188.188.188.188/32 and advertise that into OSPF.
- Redirect all HTTP requests sent to 45.45.45.80 to 188.188.188.188.
- Redirect all Telnet requests sent to 45.45.45.81 to 188.188.188.188.
- Redirect all SSH requests sent to 45.45.45.82 to 188.188.188.188.
- Redirect all DNS requests sent to 45.45.45.83 to 188.188.188.188.
- Configure appropriate ACLs to allow access.

Task 21: Static PAT on ASA-1

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

Task 22: Identity NAT on ASA-1

- Configure Identity NAT for 77.77.77.77 for outbound connections only.

Task 23: NAT Exception on ASA-1

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

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

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

Task 25: DNS doctoring using NAT

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

Task 26: Enhanced Service Object-Groups

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

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

Task 27: ICMP Filters on ASA-1

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

Task 28: uRPF and fragmented packets on ASA-1

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

Task 29: ACL Logging on ASA-1

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

Task 30: Control Plane ACL on ASA-1

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

Task 31: Management access for ASA-1

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

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

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

General Rules

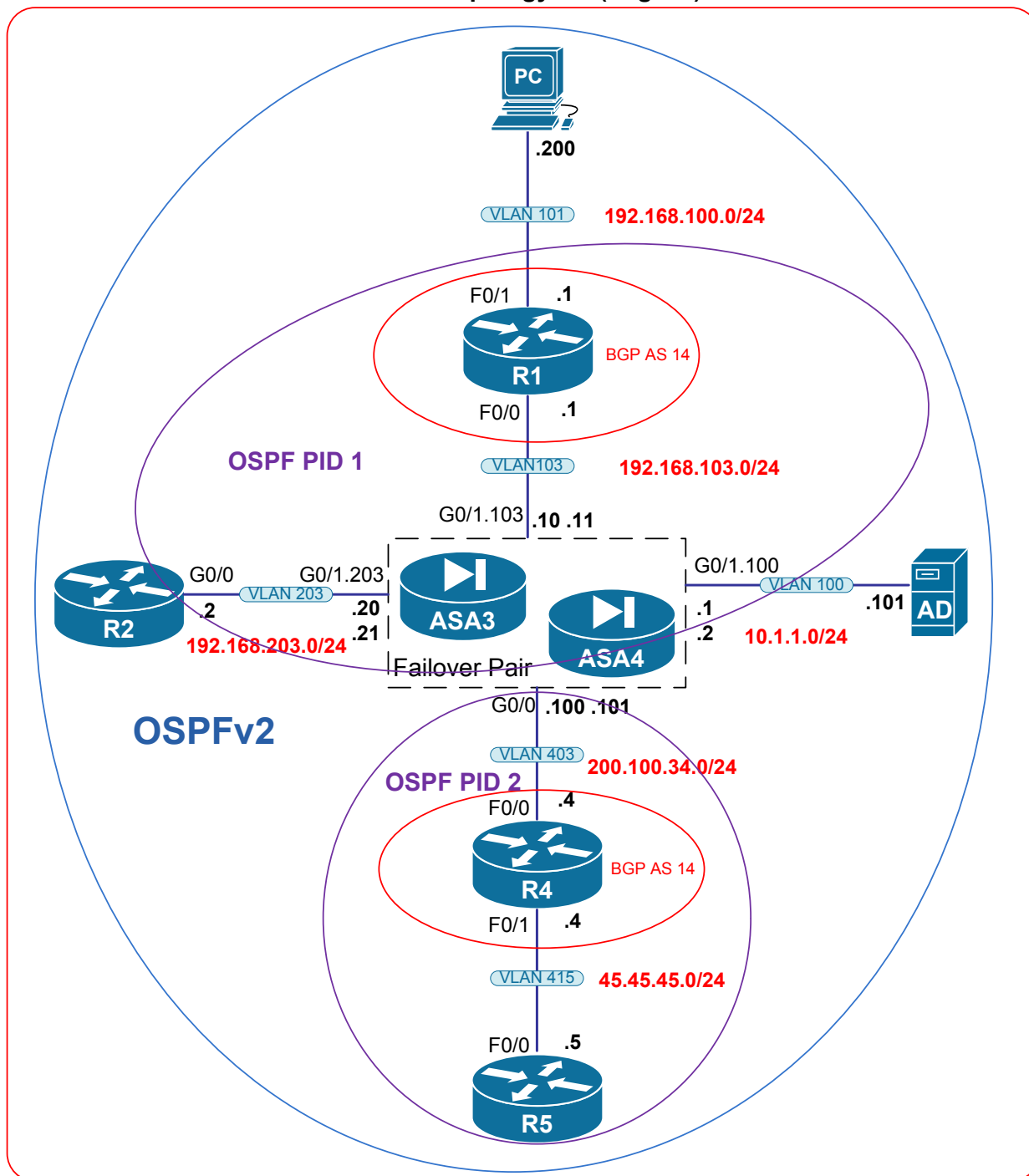
- By now you should understand how NAT works in 8.6/8.4 and 8.2 versions and how ACLs work on the ASA.
- You should understand the new logical topology (Network Topology 1.3).
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time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

Estimated Time to Complete: **3 Hours**

Pre-setup

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

Network Topology 1.3 (Logical)



Lab 5: Configuration Tasks

NOTE: Load the initial configuration before starting this lab.

Task 1: Basic Initialization ASA-3

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

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

Task 2: Configure Active/Standby Failover

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

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

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

Stateful Link – Gi0/3

Primary IP – 40.1.1.1/24
Standby IP – 40.1.1.2/24
Interface Name - 5STATE

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

Task 3: Routing ASA-3

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

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

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

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

Task 5: Dynamic PAT for INSIDE on ASA-3

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

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

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

Task 7: ICMP inspection on ASA-3

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

Task 8: DNS inspection on ASA-3

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

Task 9: FTP inspection on ASA-3

- Configure a policy to prevent web browsers from sending embedded commands in FTP requests. Configure this policy globally.
- 200.100.34.21 is an FTP server running on port 2121. Do not allow users to delete or rename any files on this server. Mask banner and syst command replies. Users should not be able to download any file starting with a string of "confidential". Configure this policy and apply this globally. Allow outside access to this server. Do not use Global ACLs.
- Drop all file executable file types. Apply this globally.

Task 10: HTTP inspection and content filtering on ASA-3

- Globally enable HTTP inspection and also enable HTTP inspection on port 8888 globally.
- Filter all outbound active-x and java contents on HTTP port 8888 from the VLAN101 to any destination.
- A Websense server is located in dmz1. The IP address of the server is 10.1.1.16. Configure URL (HTTP-80,8888 and HTTPS) filtering from VLAN 101 on port HTTP port 80. Use fail open options if the Websense server is down. Users should not be allowed to use a proxy server.
- 200.100.34.80 is a webserver running on a non-standard port of 8080. Create an HTTP deep packet inspection policy to match all the parameters below and reset the connection. Log all protocol violations. Apply this policy globally. Create an interface specific ACL to allow access to this server from the outside.

Request Header Host should contain "200.100.34.80"
Request URI containing "exec" string

Request Method GET

- 200.100.34.81 is a webserver. Create an HTTP deep packet inspection policy to match any of the parameters below and reset and log the connection. Set the maximum number of simultaneous connections to 3000, half opened embryonic connections to 300, and idle timeout to 30 minutes. Apply this policy globally. Create an interface specific ACL to allow access to this server from the outside.

Content Type Mismatch
Header length greater than 500 bytes
Via count greater than 0
Users should not be able to upload any files to this server
Users should not be able to use Mozilla browsers when accessing this server

- Do not allow any Active-X/ Java applets in the HTTP response from 200.111.111.80. Apply this policy on the outside interface. Use the MPF only.

Task 11: ESMTP inspection on ASA-3

- 200.100.34.25 is an SMTP server. Drop all emails with a size greater than 9 MB. Also drop any emails which have a recipient count greater than 1000. Only allow internal emails that contain domain names of “@ipexpert.com”, “@ipexpert.in” and “@proctorlabs.com”. Apply this policy globally in the “inspection_default” class-map.

Task 12: IM inspection on ASA-3

- Only allow MSN and Yahoo IM chat. Drop all other services in MSN and Yahoo IM. Apply this policy globally. VLAN 101 should be exempted from this policy.

Task 13: IP Options inspection on ASA-3

- Configure a global policy to ensure ASA does not conform to RFC 2113.

Task 14: IPSec passthrough inspection on ASA-3

- Configure a global policy to limit the number of simultaneous ESP tunnels from the same host to 10 tunnels with an idle time of 30 minutes.

Task 15: BGP through ASA-3

- Configure the appropriate policy and ACLs to ensure the BGP adjacency between R4 and R1 is established successfully.

Task 16: TCP normalization on ASA-3

- 200.100.34.1 is a Telnet and SSH server. Configure ASA to either drop, or allow, or normalize TCP packets using the TCP normalizer feature destined to that server from the outside as per the parameters below :

Check-retransmission	Enforce
Checksum-Verification	Enforce
Exceed-mss	drop
Invalid-ack	Drop
Reserve-bits	clear
Synack-data	Allow
Syn-data	Allow (Default)
Tcp-options timestamp	clear

- Set TCP idle timeout to 60 seconds. Enable DCD for connections to this server. Probes should be sent every 5 seconds.
- Maximum number of simultaneous connections per host should be set to 1 and maximum number of simultaneous connection should be set to 2.
- Configure appropriate interface ACLs to allow access to this server. Apply the policy on the outside interface.

Task 17: Traceroute through ASA-3

- Configure ACLs such that R5's Loopback0 can traceroute to R1 loopback0. Ensure R1 is able to see the ASA in the traceroute output. Apply this policy globally. Do not create any new class map to accomplish this task.

Task 18: Netflow/NSEL on ASA-3

- Configure the ASA such that all events related to any BGP traffic is sent to a NSEL collector. The Collector is located in the dmz1 interface with an IP address of 10.1.1.100 running on UDP port 10000. Disable all syslog messages that have become redundant due to the NSEL configuration.

Task 19: LLQ on ASA-3

- Enable LLQ for VoIP traffic marked with a DSCP value of af31 (Signal) and ef (Voice-RTP) on the outside interface. Set the allowed number of packets queued at the tx-ring for the priority-queues to 300 and the depth of the software priority queue to 800 (i.e. number of packets queued at the priority-queues). Apply this policy for the outside interface.

Task 20: Management Traffic Connection Limits on ASA-3

- Enable ASDM access on the outside interface such that anyone can connect to the ASA.
- Set the simultaneous maximum number of ASDM connections on the outside interface to 2 and maximum embryonic connections to 8. Apply this policy on the outside interface.

Task 21: Threat Detection on ASA-3

- Enable advanced threat detection to gather statistics about suspicious activity based on access-list denies and host scanning (8 hours interval).
- Ensure ASA shuns any network scan or sweeps. Make sure ASA does not shun the AD server. Shun duration should be half of the default value.

Lab 6: Transparent Firewall

Lab 6: Transparent Firewall– This lab is intended to let you be familiar with the transparent firewall feature on the ASA. This lab consists of two ASAs. One of the ASA is loaded with 8.6 code and other is loaded with 8.2 version. There are several changes in configuring the transparent firewall between different software versions.

General Rules

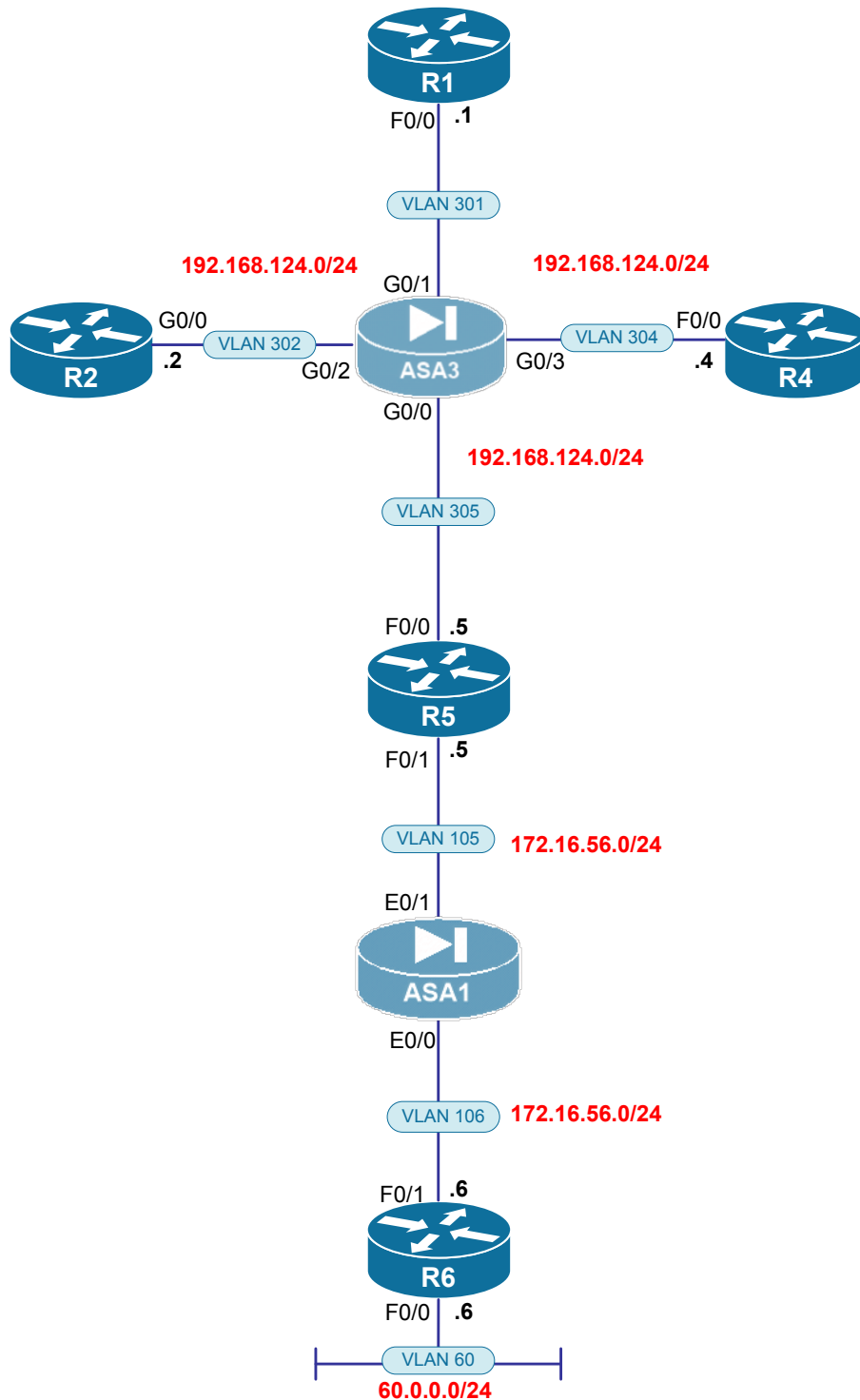
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **3 Hours**

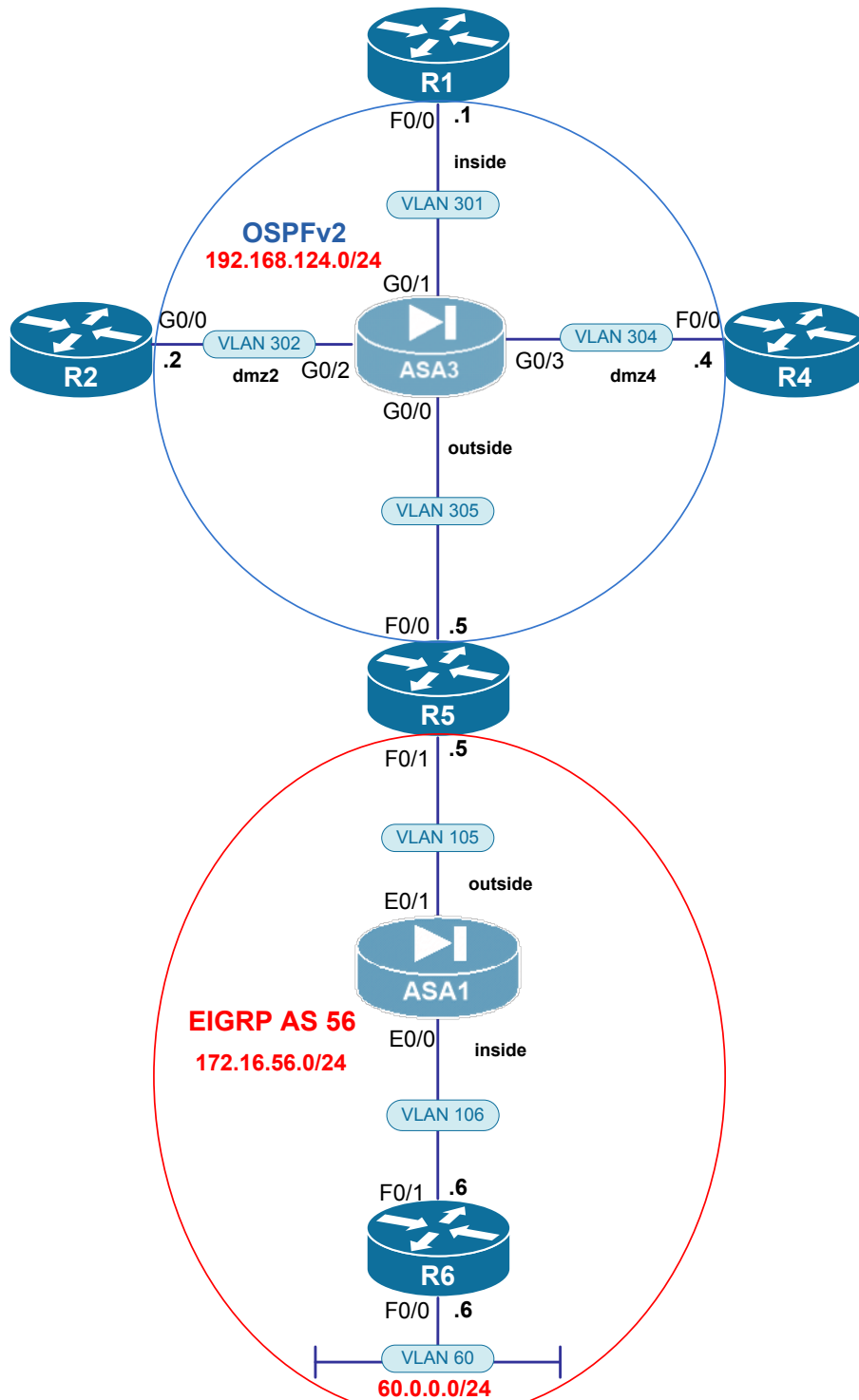
Pre-setup

Load the initial configuration for Lab 6. Routers are pre-configured. Use the logical topology drawing - Network Topology 1.4 and 1.5 to understand the logical topology and routing when transparent firewall is introduced. Double-check the loaded pre-configuration before starting the Lab. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.4 (Logical)



Network Topology 1.5 (Logical)



Lab 6: Configuration Tasks

Task 1: Basic Initialization ASA-3

- Change the mode to Transparent. Configure a hostname of “FwtASA3” on ASA-3.
- FwtASA3 should have a domain name of ipexpert.com.
- Configure the FwtASA3 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	Bridge Group	VLAN	Security Level	Name
G0/0	100	305	0	outside
G0/1	100	301	100	inside
G0/2	100	302	50	dmz2
G0/3	100	304	60	dmz4
M0/0	None	444	100	mgt

- Configure a BVI address of 192.168.124.100 and management IP of 192.168.1.100.

Task 2: ACLs on ASA-3

- The 192.168.124.0/24 subnet has been configured for OSPF. Configure Global ACLs to permit any OSPF traffic from R1, R2, R4, R5.
- Allow all SSH, Telnet, GRE, SMTP, FTP, TFTP, IPSEC, HTTP, DNS, HTTPS, ICMP, ISAKMP (UDP - Src 500 and Dst 500) traffic from 192.168.124.0/24 subnet. Use a single ACL to accomplish this task.
- Allow HTTP, HTTPS, Telnet, SSH, and ICMP access from VLAN 60 to the 192.168.124.0/24 subnet. Apply this ACL on the outside interface.
- Globally inspect ICMP traffic.

Task 3: Basic Initialization the ASA-1

- Configure a hostname of “FwtASA1” on ASA-1.
- Telnet password should be set to “ipexpert”.
- FwtASA1 should have a domain name of ipexpert.com.
- Configure the FwtASA1 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	VLAN	Security Level	Name
E0/0	106	100	inside
E0/1	105	0	outside

- Configure a Global IP address of 172.16.56.100.

Task 4: ACLs on ASA-1

- Configure ACLs to allow EIGRP traffic between R6 and R5.
- Allow all inbound SSH, Telnet, GRE, SMTP, FTP, TFTP, IPSEC, HTTP, DNS, HTTPS, ICMP, ISAKMP (UDP - Src 500 and Dst 500) traffic from 192.168.124.0/24 to the VLAN60 subnet. Use a single ACL to accomplish this task.
- Allow all outbound ICMP, Telnet, SSH, HTTP and HTTPS traffic from VLAN60 to 192.168.124.0/24.

Task 5: Transparent Firewall NAT/PAT on ASA-1

- Configure static NAT for R6 Lo16 (16.16.16.16). It should be translated to 60.0.0.16.
- Configure PAT for R6 Lo0 (6.6.6.6) to 160.0.0.6.
- Configure appropriate static routes on ASA and R5.
- Configure appropriate ACLs to allow R6 Lo0 to Telnet to R1 Lo0
- Ensure 192.168.124.0/24 can ping 60.0.0.16. Use an ACL to accomplish this task. Do not use MPF to accomplish this task.

Task 6: Ethertype ACLs on ASA-1

- Configure Ethertype ACLs to allow TRILL (TRILL TE) and MPLS unicast and MPLS multicast frames to pass through ASA-1.

Task 7: Dynamic ARP inspection on ASA-1

- Configure DAI on ASA-1 such that no ARP traffic passes through the firewall without checking the static MAC to IP binding table. If none of the ARP packets match an entry then the ASA should drop that packet. Create the appropriate MAC to IP bindings.

Task 8: Prevent MAC Spoof attacks on ASA-1

- Disable MAC learning on the outside and inside interfaces and create static bindings for R5 and R6.

Lab 7: Active/Standby Transparent Firewall

Lab 7: Active/Standby Transparent Firewall – This lab is intended to let you be familiar with the transparent firewall feature on ASA on 8.6 using multiple bridge groups in single context mode with stateful failover.

General Rules

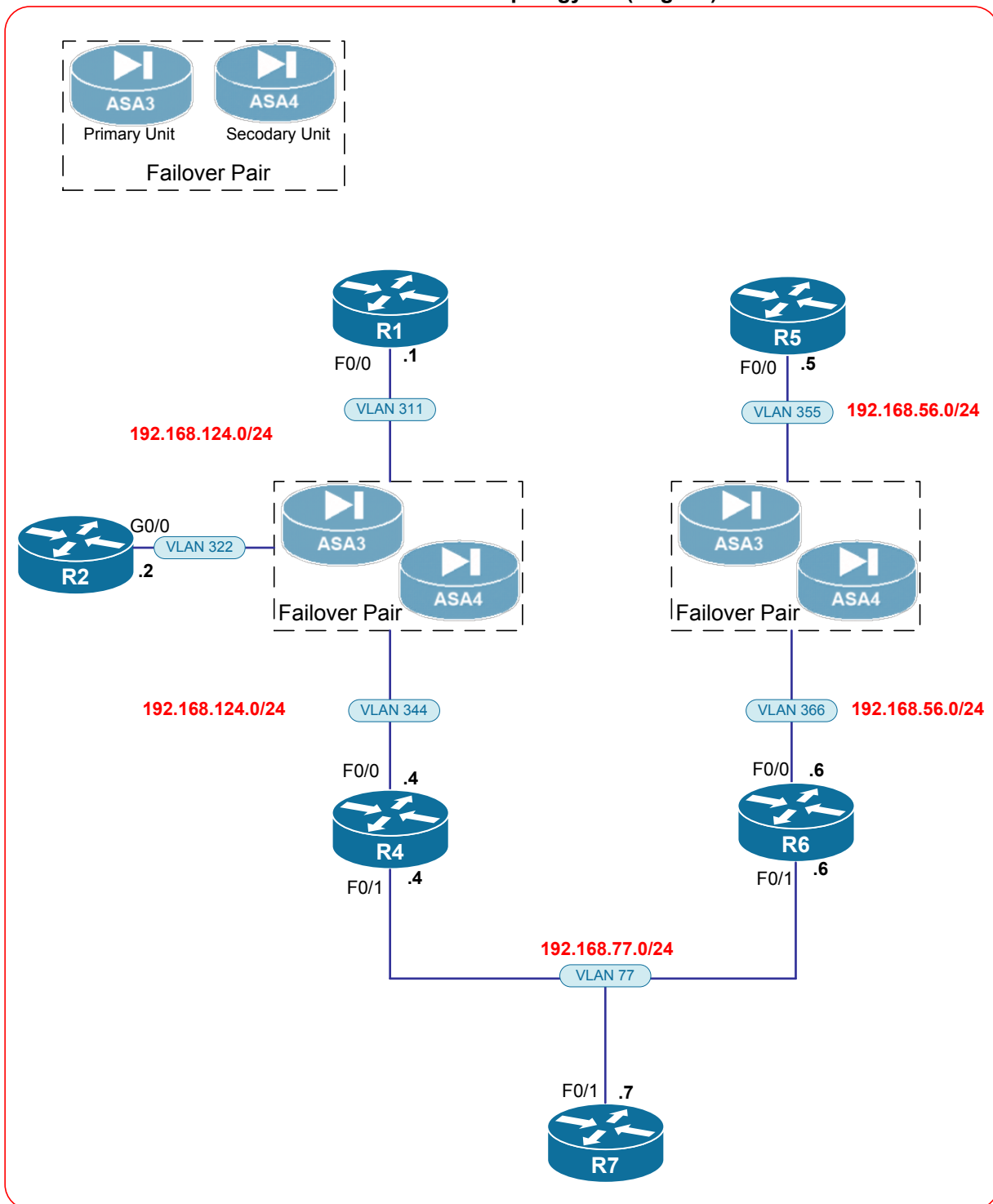
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular chapter.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: **2.5 Hours**

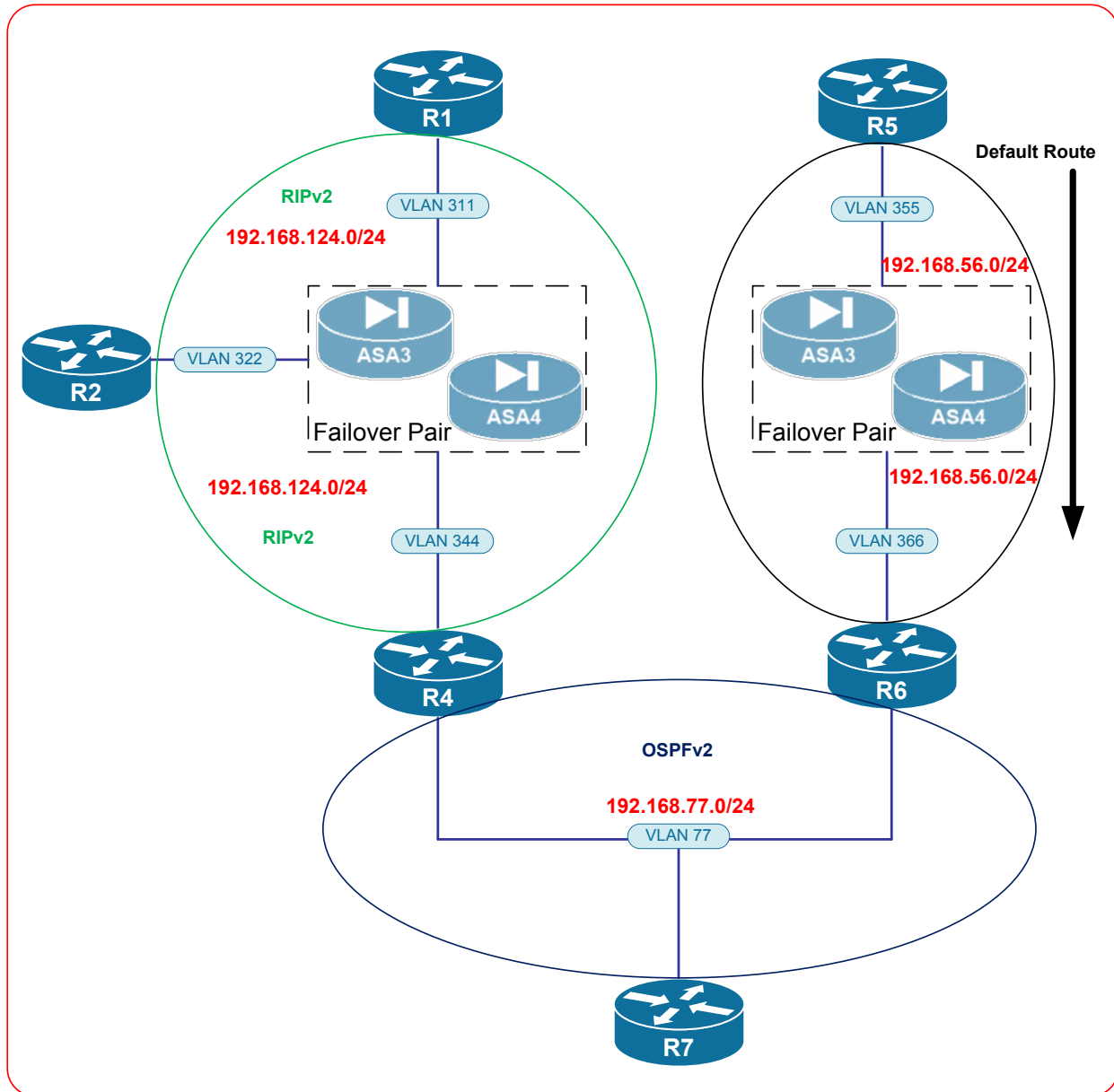
Pre-setup

Load the initial configuration for Lab 7. Routers are pre-configured. Use the logical topology drawing (Network Topology 1.6 and 1.7) to understand the logical topology and routing when Transparent firewall is introduced. Double-check the loaded pre-configuration before starting the Lab. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.6 (Logical)



Network Topology 1.7 (Logical)



Lab 7: Configuration Tasks

NOTE: Load the initial configuration before starting this lab.

Task 1: Basic VLAN Setup

- Configure the Catalyst switch with the appropriate VLANs for ports and trunks for the firewall as per topology diagram 1.6.

Task 2: Failover Configuration

- Change the firewall mode to transparent.
- Configure ASA-3 and ASA-4 for device level HA using the failover feature on the ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the parameters below for the failover configuration. Configure the switch such that the Gi0/2 interface of the firewall (failover port) should be in VLAN 300. Share the Gi0/2 interface for stateful link failover.

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

Task 3: Basic Initialization ASA-3

- Configure a hostname of “ASA3TFW” on ASA-3.
- ASA3 should have a domain name of ipexpert.com.
- Configure the ASA3 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	Bridge Group	VLAN	Security Level	Name
G0/0.311	10	311	100	inside
G0/0.322	10	322	50	dmz
G0/0.344	10	344	0	outside
G0/1.355	20	355	100	in
G0/1.366	20	366	0	out

- Configure a BVI 10 address of 192.168.124.100 and a standby IP of 192.168.124.101.
- Configure a BVI 20 address of 192.168.56.100 and a standby IP of 192.168.56.101.

- Ensure all interfaces are monitored.

Task 4: ACLs on ASA-3

- Configure interface specific ACL's to allow RIPv2 traffic between R1,R2 and R4.
- Allow all outbound HTTP, HTTPS, FTP, telnet and DNS traffic on BVI 10 group for all dmz and inside hosts.
- Do not configure any ACL's for BVI 20 group. Do not use Global ACL's.

Task 5: Transparent firewall NAT on ASA-3

- Configure Object Static NAT for R5 Lo0 to 192.168.56.55.
- You are allowed to create one static route to accomplish this task.
- R5 Lo0 should be able to telnet and ping R1 Lo0. Ensure that you match the below output.

```
R5#ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#telnet 1.1.1.1 /source-interface lo0
Trying 1.1.1.1 ... Open

R1#who
      Line      User      Host(s)      Idle      Location
*514 vty 0      idle      idle      00:00:00  192.168.56.55

      Interface      User      Mode      Idle      Peer Address

R1#exi

[Connection to 1.1.1.1 closed by foreign host]
R5#
```

- You are allowed to configure ACL's to allow access on BVI 10 outside interface only.
- No ACL's should be configured on any BVI 20 group of interfaces. Do not use Global ACL.

Lab 8: Routed Mode Multi-Context and Active/Active Failover

Lab 8: Routed Mode Multi-Context and Active/Active Failover – This lab is intended to let you be familiar with configuring ASA in multi-context routed mode with failover. Using multicontext you can configure Active/Active failover or Active/Standby failover. If both the device loadshare traffic, then it's called Active/Active. This is a very key topic and you will understand how order of operation is important when configuring Active/Active failover. Hence to begin with we shall start with just configuring one ASA 5515-X series with Multi-context and then advance to Active/Active failover.

General Rules

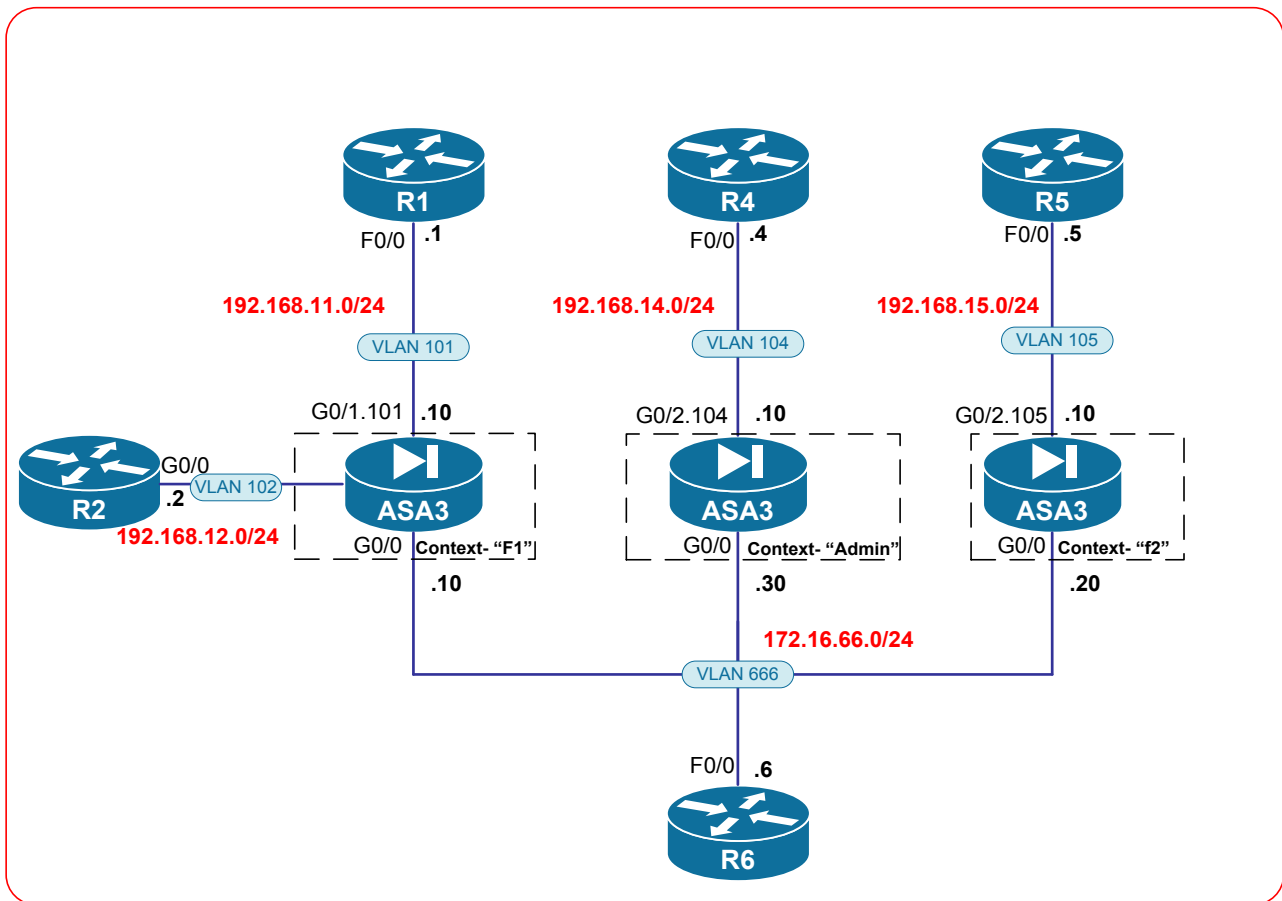
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: **3 Hours**

Pre-setup

Load the initial configuration for Lab 8. Routers are pre-configured. Use the logical topology drawing - Network Topology 1.8 - to understand the logical topology when Multi-Context firewall is introduced. Use the logical topology drawing - Network Topology 1.9 - to understand the logical topology when Multi-Context firewall with Active/Active failover is introduced. Double-check the loaded pre-configuration before starting the Lab.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.8 (Logical)

Lab 8: Configuration Tasks

NOTE: Load the initial configuration before starting this lab.

Task 1: Basic VLAN Setup

- Configure the Catalyst switch with the appropriate VLANs for ports and trunks for the firewall as per topology diagram 1.8.

Task 2: Firewall Mode on ASA-3

- Change the firewall mode on ASA-3 to multi-mode to support multi-context.
- Configure a hostname of “ASA003” on ASA-3.
- ASA003 should have a domain name of ipexpert.com.
- Administratively enable all interfaces.

Task 3: VLAN Sub-interface creation on ASA-3

- Configure VLAN sub-interfaces on ASA3 as per the parameters below:

ASA Interface	VLAN
G0/1.101	101
G0/1.102	102
G0/2.104	104
G0/2.105	105

Task 4: Context creation on ASA-3

- Remove any existing context configuration and delete any .cfg files from flash.
- Configure contexts as per the table below. Designate “Admin” to be the admin context.
- Gi0/0 will be shared between all the contexts.
- Allocate the default virtual sensor to the Admin context.
- Use the “mac-address auto” with any prefix of your choice for auto generation of MAC address.

Context	Interface Allocation	Interface name	Configuration file (Flash/Disk0)
Admin	G0/0	A_OUT	Admin.cfg
Admin	G0/2.104	A_IN	
f1	G0/0	-----	F1.cfg
f1	G0/1.101	-----	
f1	G0/1.102	-----	
f2	G0/0	F2_OUT	F2.cfg
f2	G0/2.105	F2_IN	

- Limit the resource allocation for the f2 context as per the parameters below:

Resource	Limits
Connections	2000
Xlate	200
Telnet,SSH,ASDM	2 each

NOTE: Configure exact names and numbers for interfaces and contexts

Task 5: Admin context configuration on ASA-3

- The Admin context should have a domain name of ipexpert.com.
- Configure interfaces with the parameters below. After you perform this task, ensure that you can ping your directly connected neighbors.

ASA Interface	IP Address	Security Level	Name
A_OUT	172.16.66.30/24	0	outside
A_IN	192.168.14.10/24	100	inside

- Configure a static default route toward R6 and a static route for R4 Lo0 (4.4.4.4).
- Enable Telnet on the inside interface from anyone.
- Enable SSH and ASDM access on the outside interface from anyone.
- Create username cisco password cisco123 and enable SSH, Telnet, and ASDM authentication locally.
- Create an inter-context static route to R5 Lo0 (5.5.5.5).
- Configure an ACL to allow all traffic between R4 Lo0 and R5 Lo0. Apply this on the outside interface.

Task 6: f2 context configuration on ASA-3

- Configure interfaces with the parameters below. After you perform this task, ensure that you can ping your directly connected neighbors.

ASA Interface	IP Address	Security Level	Name
F2_OUT	172.16.66.20/24	0	OUT
F2_IN	192.168.15.10/24	100	IN

- Configure a static default route toward R6 and a static route for R5 Lo0 (5.5.5.5).
- Create an inter-context static route to R4 Lo0 (4.4.4.4).
- Configure an ACL to allow all traffic between R4 Lo0 and R5Lo0. Configure Global ACLs.
- Configure Static Identity NAT using Manual NAT for R5 Lo0 when it communicates with R4 Lo0.
- All other outbound traffic should be PATed to the interface IP using Auto NAT.
- Allow all outbound telnet traffic from VLAN 105. Configure Global ACLs.

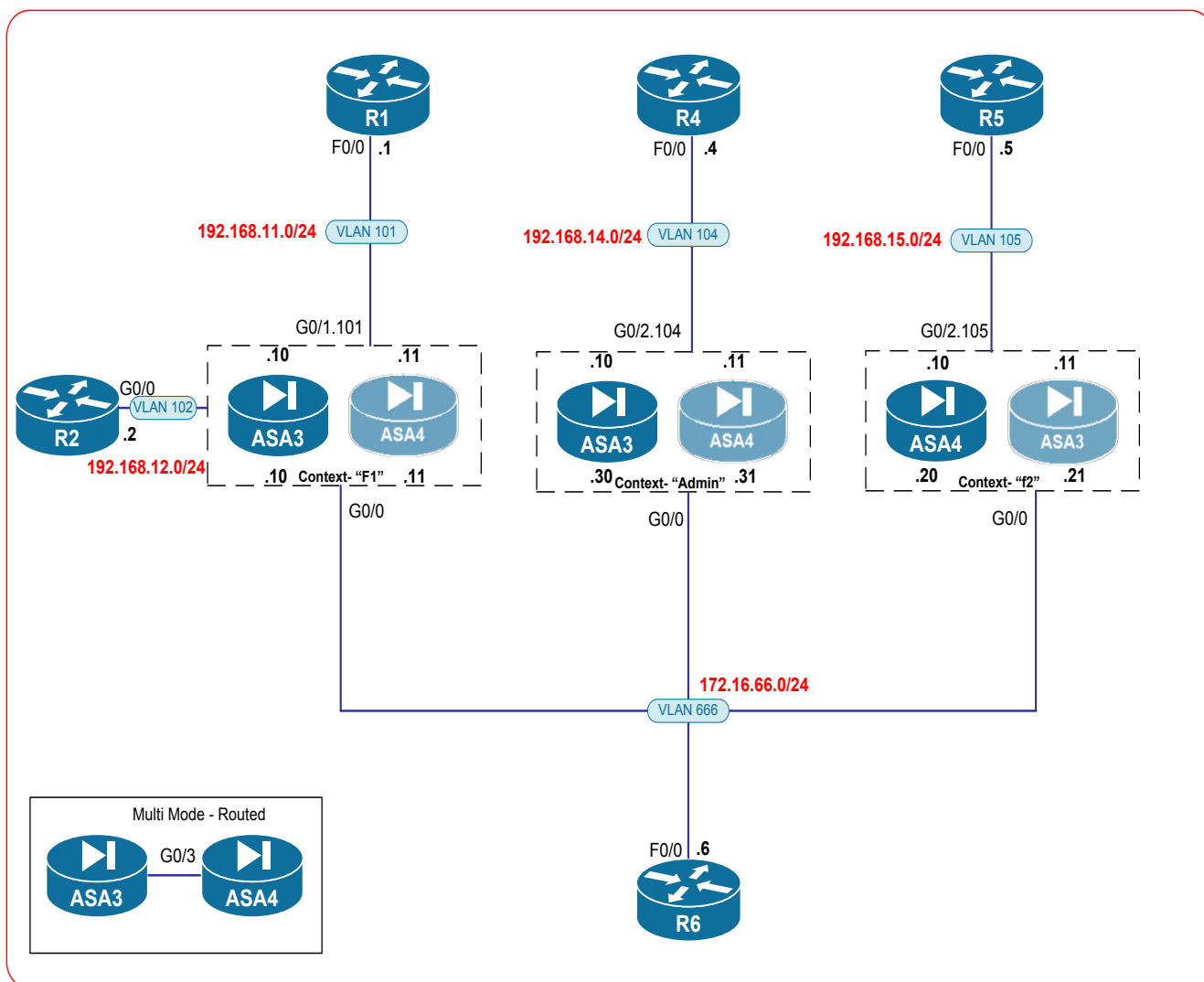
Task 7: F1 context configuration on ASA-3

- Configure interfaces with the parameters below. After you perform this task ensure that you can ping your directly connected neighbors.

ASA Interface	IP Address	Security Level	Name
G0/0	172.16.66.10/24	0	outside
G0/1.101	192.168.11.10/24	100	inside
G0/1.102	192.168.12.10/24	50	dmz

- Configure static default route towards R6 and a static route for R2 (2.2.2.2) and R1 Lo0 (1.1.1.1)
- Configure Static Auto NAT and translate 1.1.1.1 to 172.16.66.80 on the outside and 2.2.2.2 to 172.16.66.23.
- Allow all ICMP traffic to pass through from the outside
- Allow HTTP access to 172.16.66.80 and telnet access to 172.16.66.23 anyone from the outside. Telnet from R5 and R4 f0/0 to 172.16.66.23 should be successful.
- Do not use global ACL's

Network Topology 1.9 (Logical)



NOTE: The lighter color/transparent icon of the ASA indicate on that particular ASA the mentioned context is in standby state i.e. not forwarding traffic. ASA3 is the primary unit and ASA4 is the secondary unit for failover configuration.

Task 8: Basic VLAN Setup

- Configure the catalyst switch with the appropriate VLAN's for ports and trunks for the firewall to support topology diagram 1.9.

NOTE: Refer Network Topology Diagram 1.9

Task 9: Failover Configuration

- Change the mode to routed multi-mode on ASA-4
- Configure ASA-3 and ASA-4 for device level HA using failover feature on ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the below parameters for the failover configuration. Configure Switch such that G0/3 interface of the firewall should be in VLAN 333. Share G0/3 for stateful link failover. **DO NOT ENABLE FAILOVER IN THIS TASK.**

Failover interface – G0/3
Primary IP – 30.1.1.1/24
Standby IP – 30.1.1.2/24
Interface Name - FA1LOVER
Key - C1SCO

Task 10: Active/Active Failover Configuration on ASA-3

- Admin and F1 context should be active on ASA-3 and f2 context should be active on ASA-4. Configure failover groups with pre-empt option.
- Configure failover accordingly and now enable failover.

Task 11: Re-configure Active and Standby IP address.

- Since failover is enabled. Re-configure each context with standby IP Address as per the network diagram 1.9 on the appropriate active ASA.
- Configure a static MAC address for A_OUT interface of Admin context. 0011.0011.0011 should be the active and 0022.0022.0022 should be the standby MAC address.

Lab 9: Multi-Mode Transparent Firewall with Active/Active Failover

Lab 9: Transparent Mode Multi-Context – This lab is intended to let you be familiar with configuring ASA in multi-context transparent mode since there is a significant difference in configuring transparent firewall in Multi-context between 8.2 and 8.4/8.6 code of the ASA. This lab focuses on 8.6 version of the ASA. In version 8.2 only two unique interfaces can be added per context. This is, however, not the same in 8.6 version

General Rules

- By now you should have understood how to configure Failover and the order of operation when configuring Active/Active failover.
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

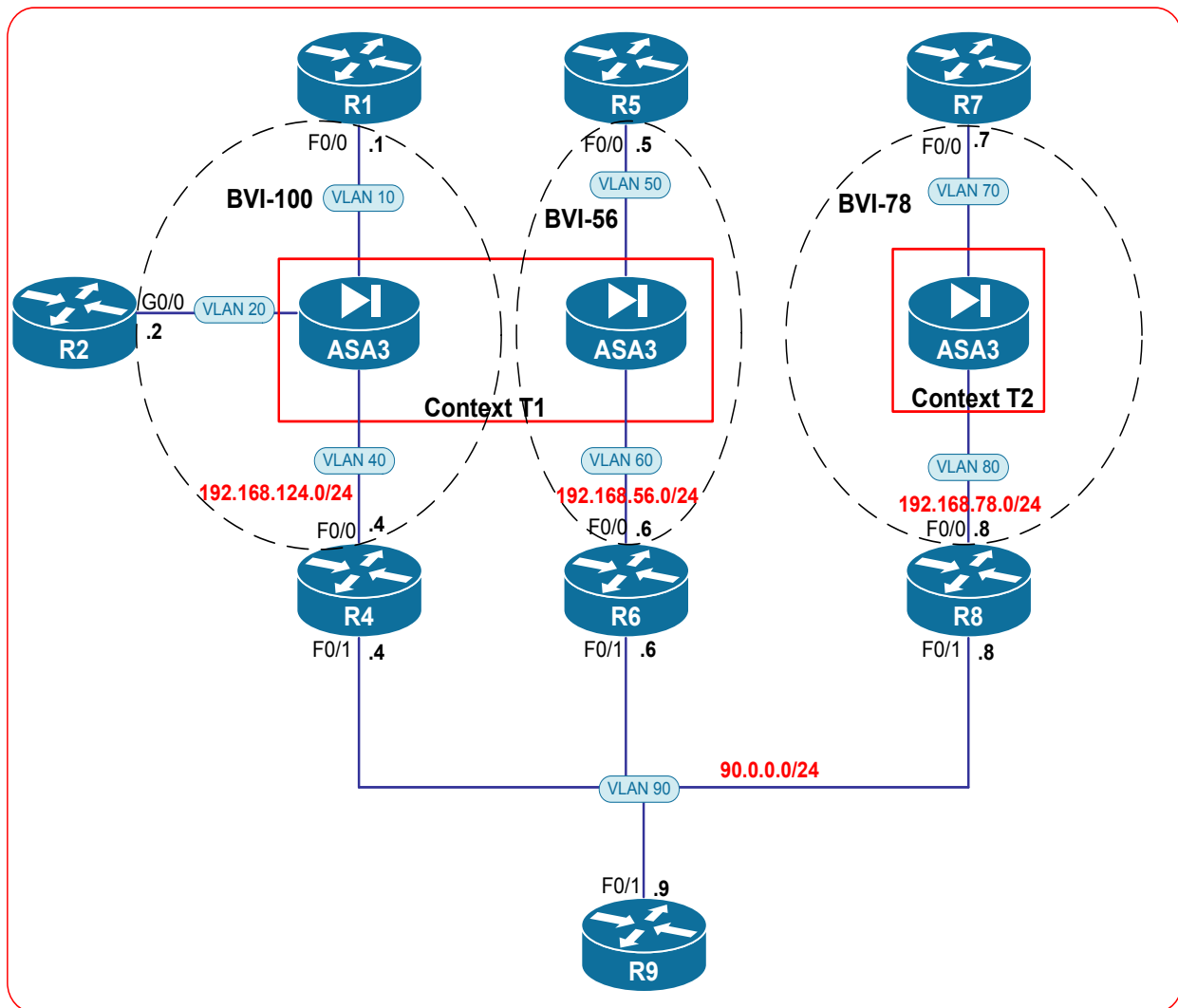
Estimated Time to Complete: **3 Hours**

Pre-setup

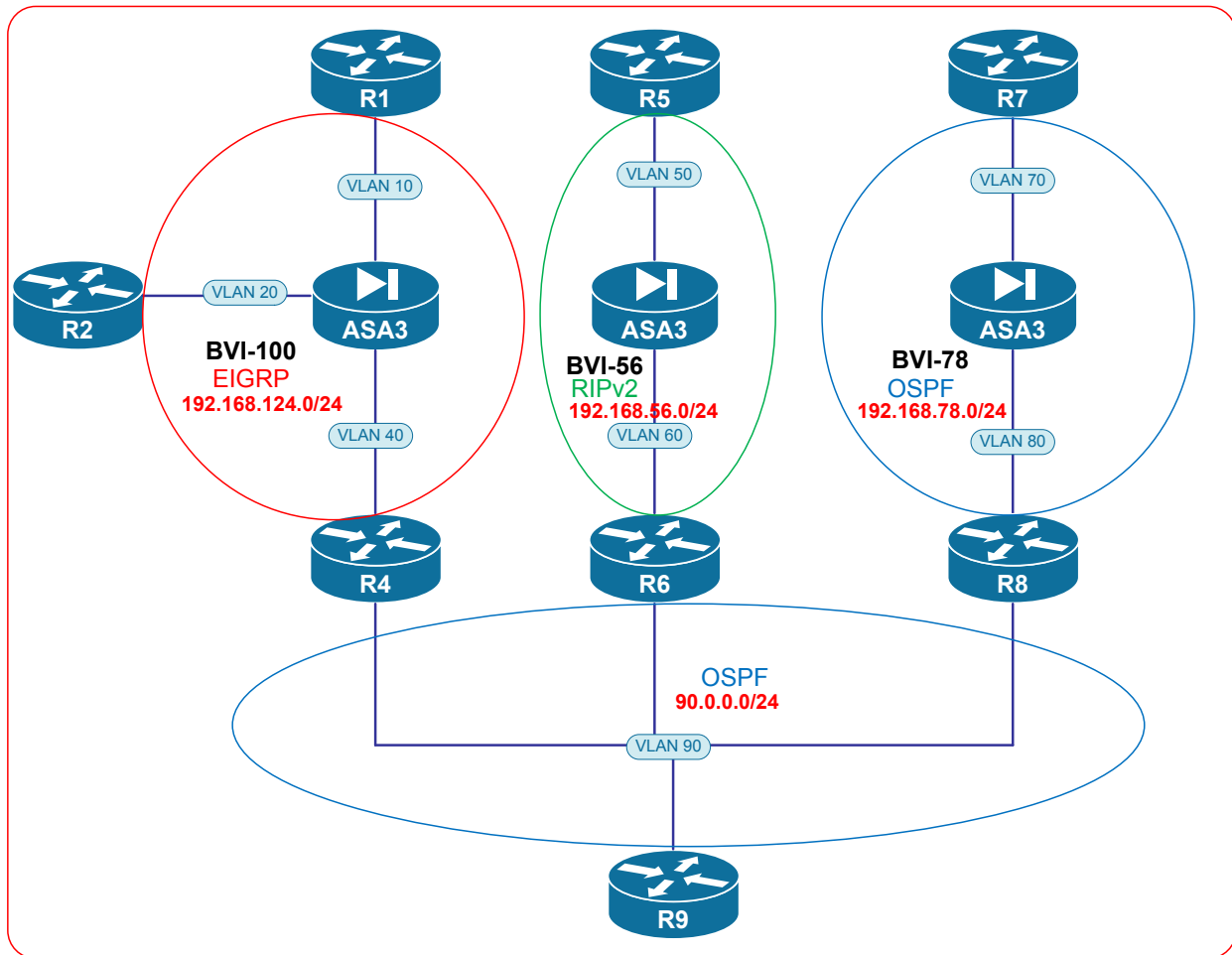
Load the initial configuration for Lab-9 Routers are pre-configured with routing. Use the logical topology drawing - Network Topology 1.10, 1.11 and 1.12 to understand the logical topology and routing topology when Multi-Context transparent firewall is introduced with Active/Active failover. Double check the loaded pre-configuration before starting the Lab.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

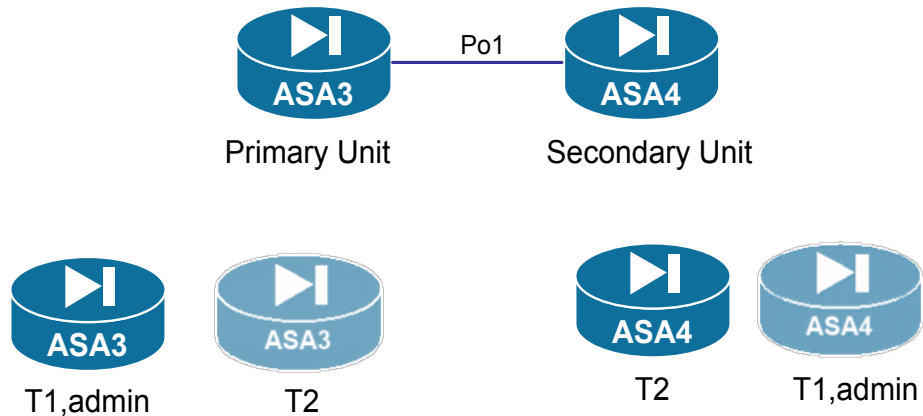
Network Topology 1.10 (Logical)



Network Topology 1.11 (Logical)



Network Topology 1.12 (Logical)



T1, admin Context - Active on ASA-3
T1, admin Context - Standby on ASA-4

T2 Context - Active on ASA-4
T2 Context - Standby on ASA-3

NOTE: The lighter color/transparent icon of the ASA indicate on that particular ASA the mentioned context is in standby state.

Lab 9: Configuration Tasks

NOTE: Load the initial configuration before starting this lab.

Task 1: Basic VLAN Setup

- Configure the catalyst switches with the appropriate VLAN's for ports and trunks for the firewall as per topology diagram 1.10 and 1.11.

Task 2: Firewall Mode on ASA-3

- Change the mode to Multi context transparent mode on ASA-3
- Configure a hostname of "ASA003" on ASA-3
- ASA003 should have a domain name of ipexpert.com
- Un shut all the interfaces

Task 3: VLAN Sub-interface creation on ASA-3

- Configure VLAN sub-interfaces on ASA3 as per the below parameters

ASA Interface	VLAN
G0/0.10	10
G0/0.20	20
G0/0.40	40
G0/0.50	50
G0/0.60	60
G0/0.70	70
G0/0.80	80

Task 4: Context and failover group creation on ASA-3

- Create contexts as per the below table

Context	Interface Allocation	Configuration file (Flash/Disk0)	Failover Group
admin	M0/0	admin.cfg	1
T1	G0/0.10	T1.cfg	1
	G0/0.20		
	G0/0.40		
	G0/0.50		

	G0/0.60		
T2	G0/0.70	T2.cfg	2
	G0/0.80		

- The failover groups should be configured with pre-emption option. Failover group 2 should be secondary mode on ASA-3. Configure ASA-3 accordingly.
- Limit the resource allocation for T2 context as per the below parameters

Resource	Limits
Connections	5000
Mac-address	500

Task 5: T1 context configuration

- Configure BVI interface 100 with a primary IP address of 192.168.124.100 and standby IP address of 192.168.124.101.
- Configure BVI interface 56 with a primary IP address of 192.168.56.56 and standby IP address of 192.168.56.57.
- Configure T1 context as per the below parameters

ASA Interface	BVI	Security Level	Name
G0/0.40	100	0	outside
G0/0.10	100	100	inside
G0/0.20	100	50	dmz
G0/0.50	56	50	IN
G0/0.60	56	0	OUT

- Configure global ACL to permit any EIGRP traffic
- Configure global ACL to allow RIP traffic between R5 and R6. The ACL should be host specific and should not have 224.0.0.9 in the destination.
- Allow all ICMP traffic in the global ACL
- Ensure routing adjacency is established as per the network diagram

Task 6: T2 context configuration

- Configure BVI interface 78 with a primary IP address of 192.168.78.78 and standby IP address of 192.168.78.79.
- Configure T2 context as per the below parameters

ASA Interface	BVI	Security Level	Name
G0/0.80	78	0	outside
G0/0.70	78	100	inside

- Configure interface specific ACL's to allow OSPF traffic. ACL's should be as specific as possible. Do not use any global ACL's.
- Allow ICMP traffic to pass through in the ACL's. Do not use global ACL's.
- Ensure routing adjacency is established as per the network diagram
- Ensure you are able to accomplish the below from R7.

```

R7#ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 5.5.5.5 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 2.2.2.2 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

Task 7: Failover Configuration

- Configure Failover – use G0/1 as a failover link. Use VLAN 100
- Change the mode to Transparent Multi-mode on ASA-4
- Configure ASA-3 and ASA-4 for Active/Active failover. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the below parameters for the failover configuration. Share G0/1 for stateful link failover.

Failover interface – G0/1
Primary IP – 30.1.1.1/24
Standby IP – 30.1.1.2/24
Interface Name - FA1LOVER
Key - C1SCO

Lab 10: Routed Mode IPv6 on ASA

Lab 10: Routed Mode IPv6 on ASA – This lab is intended to let you be familiar with configuring ASA using IPv6 and IPv4 dual stack. Although 8.6 has limited features when compared with Version 9.0 of the ASA, it is necessary to be familiar with configuring ASA using IPv6 protocol. This section will focus on interface addressing, ACL's, Filters, Failover and MPF.

General Rules

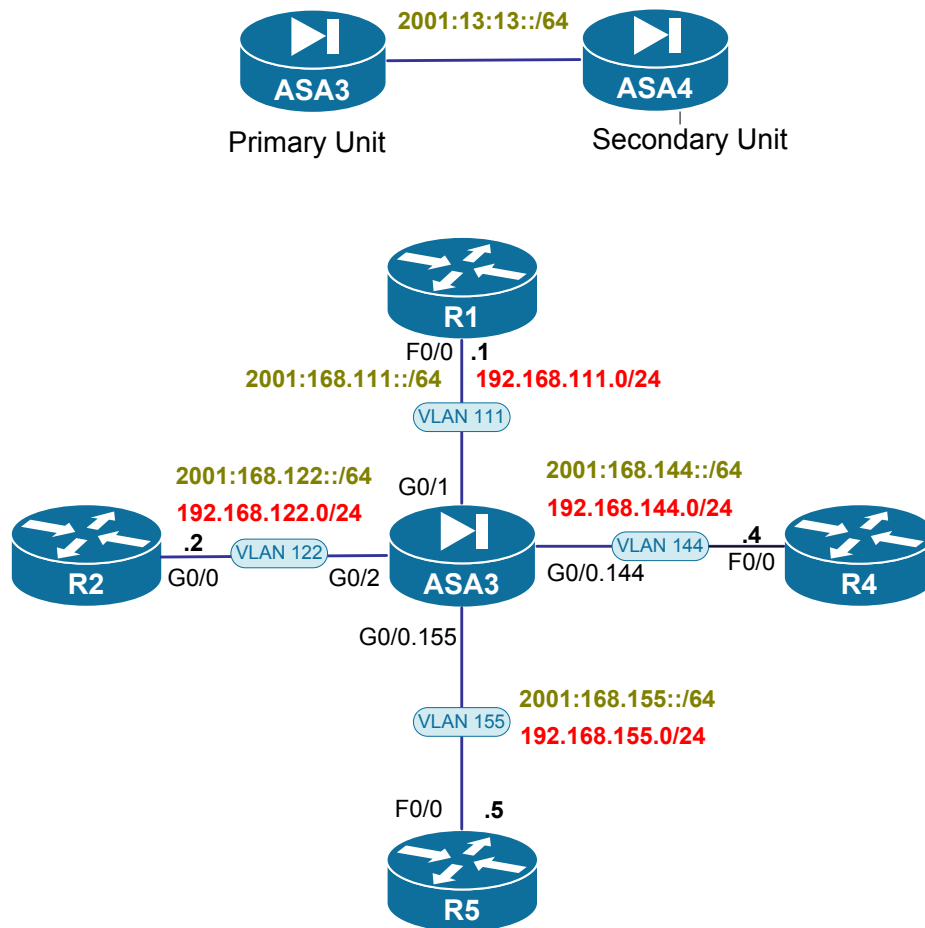
- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

Estimated Time to Complete: 2 Hours

Pre-setup

Load the initial configuration for Lab 10. Routers are pre-configured with routing. Use the logical topology drawing - Network Topology 1.13. Double-check the loaded pre-configuration before starting the Lab. This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.13 (Logical)



Lab 10: Configuration tasks

Task 1: Initialization of ASA-3

- Configure a hostname of “ASA-003fw” on ASA-3.
- ASA-003fw should have a domain name of ipexpert.com.
- Configure ASA-003fw interfaces. Ensure that you can ping your directly connected neighbors.
- Suppress IPv6 router advertisements on the outside interface.

ASA Interface	VLAN Tag	Security Level	Name	IPv4 Address Active and Standby IP	IPv6 Address Active and Standby IP
G0/1	-----	100	Inside	192.168.111.10 192.168.111.11	2001:168:111::10/64 2001:168:111::11/64
G0/2	-----	20	dmz2	192.168.122.10 192.168.122.11	2001:168:122::10/64 2001:168:122::11/64
G0/0.144	144	40	dmz4	192.168.144.10 192.168.144.11	2001:168:144::10/64 2001:168:144::11/64
G0/0.155	155	0	outside	192.168.155.10 192.168.155.11	2001:168:155::10/64 2001:168:155::11/64

Task 2: Routing on ASA-3

- Configure OSPF on all the interfaces using a single network statement.
- Configure an IPv6 static default route towards R5.
- Configure IPv6 static routes for all the loopback in dmzs and inside networks.

Task 3: IPv6 and IPv4 filters on ASA-3

- Configure global ACLs to allow all ICMP traffic for IPv4 and IPv6 traffic.
- Configure interface specific ACLs on the outside to allow Telnet traffic to R2 Lo0, SSH traffic to R4 Lo0, and HTTP traffic to R1 Lo0. This should apply both for IPv4 and IPv6 traffic.
- No one should be able to ping the outside interface using IPv6

Task 4: IPv6 Management access to ASA-3

- Configure a username of cisco and password of cisco123.
- Allow SSH access from IPv6 outside subnet. Authenticate using local AAA
- Allow telnet access from IPv6 inside subnet. Authenticate using local AAA

Task 5: Configure IPv6 Active/Standby Failover

- Configure ASA-3 and ASA-4 for device level HA using failover feature on ASA. ASA-3 will be the primary unit and ASA-4 will be the secondary unit. Use the parameters below for the failover configuration. Configure Switch such that G0/3 interface of the firewall should be in VLAN 999. Enable stateful failover on the same interface G0/3.

Failover interface – G0/3
Primary IP – 2001:13:13::10/64
Standby IP – 2001:13:13::11/64
Interface Name - FA1LOVER
Key - C1SCO

Task 6: IPv6 inspection using MPF

- Drop all fragments in the header extension using MPF. Apply this in the default policy map under the inspection_default class.

Lab 11: Transparent Mode using IPv6

Lab-11: Transparent Mode IPv6 on ASA– This lab is intended to let you be familiar with configuring ASA using IPv6 and IPv4 dual stack. Although 8.6 has limited features when compared with Version 9.0 of the ASA, it is necessary to be familiar with configuring ASA using IPv6 protocol for transparent mode on 8.6 version of the ASA.

General Rules

- Understand the new logical topology.
- Make a very close read of the tasks to ensure you do not miss details.
- Take your time; this is not a Mock Lab, so no time constraints are in place for finishing this particular lab.
- Practice multiple times to improve on speed and accuracy.

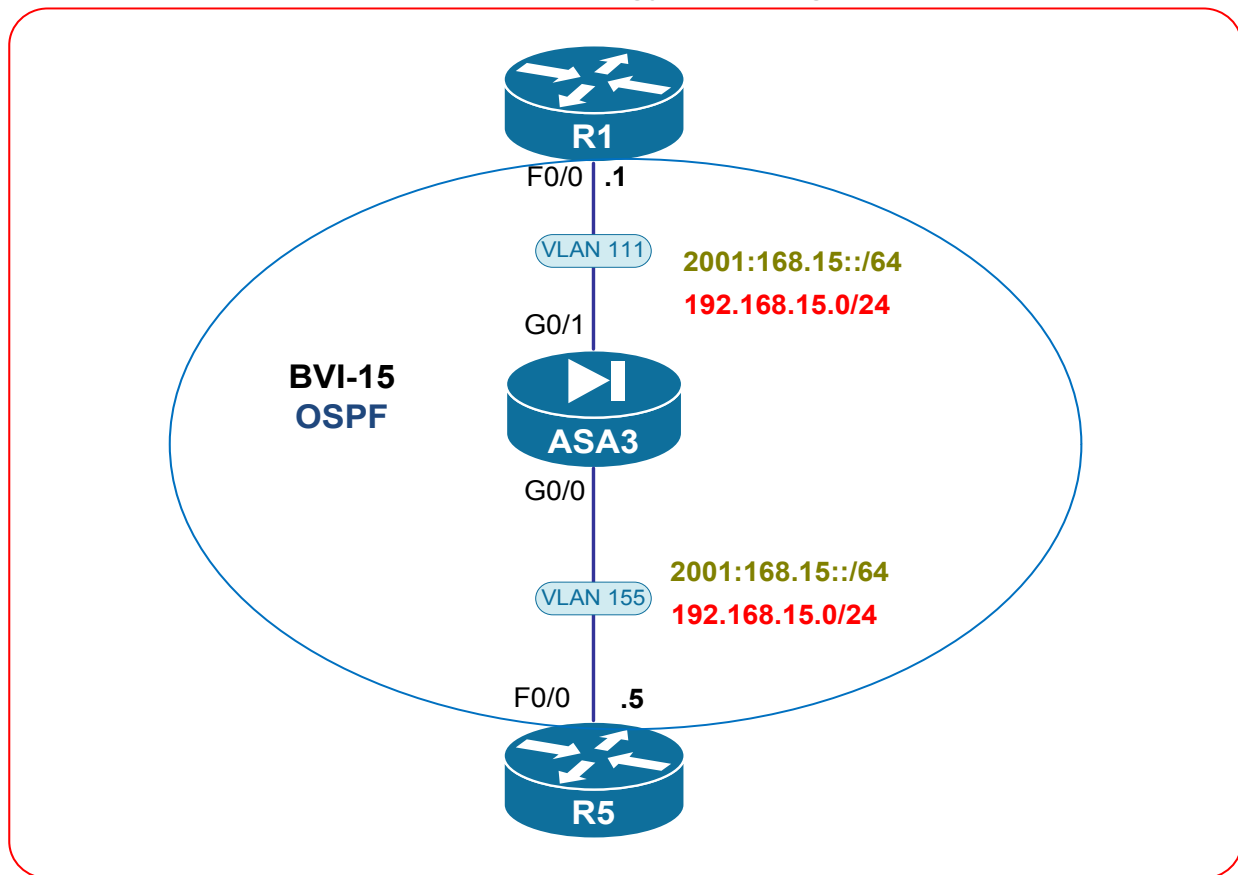
Estimated Time to Complete: 1 Hour

Pre-setup

Load the initial configuration for Lab 11. Routers are pre-configured with routing. Use the logical topology drawing - Network Topology 1.14. Double-check the loaded pre-configuration before starting the Lab.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 1.14 (Logical)



Task 1: Basic Initialization ASA-3

- Configure a hostname of “FwtASA3” on ASA-3.
- FwtASA3 should have a domain name of ipexpert.com.
- Configure FwtASA3 interfaces and the appropriate switchports on the Catalyst with the specifications below.

ASA Interface	Bridge Group	VLAN	Security Level	Name
G0/0	15	115	100	inside
G0/1	15	111	0	outside

- Configure a BVI 15 address of 192.168.15.10/24 and 2001:168:15::10/64.

Task 2: IPv4 and IPv6 ACLs

- Configure global ACLs to allow OSPF adjacency to occur between R1 and R5.

Section 2

IOS Firewall

Section 2: IOS Firewall is intended to let you be familiar with the NAT & firewall technologies that are available on IOS. You will be configuring Network Address Translations, Access-Lists, Zone Based Firewall and other filtering technologies along with some advanced features related to those.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on the IOS Firewall feature set. You will need to pre-configure the network with the base configuration files

NOTE: *Static/default routes are NOT allowed unless otherwise stated in the task*

NOTE: *ICMP and ICMPv6 traffic can be allowed everywhere unless otherwise stated*

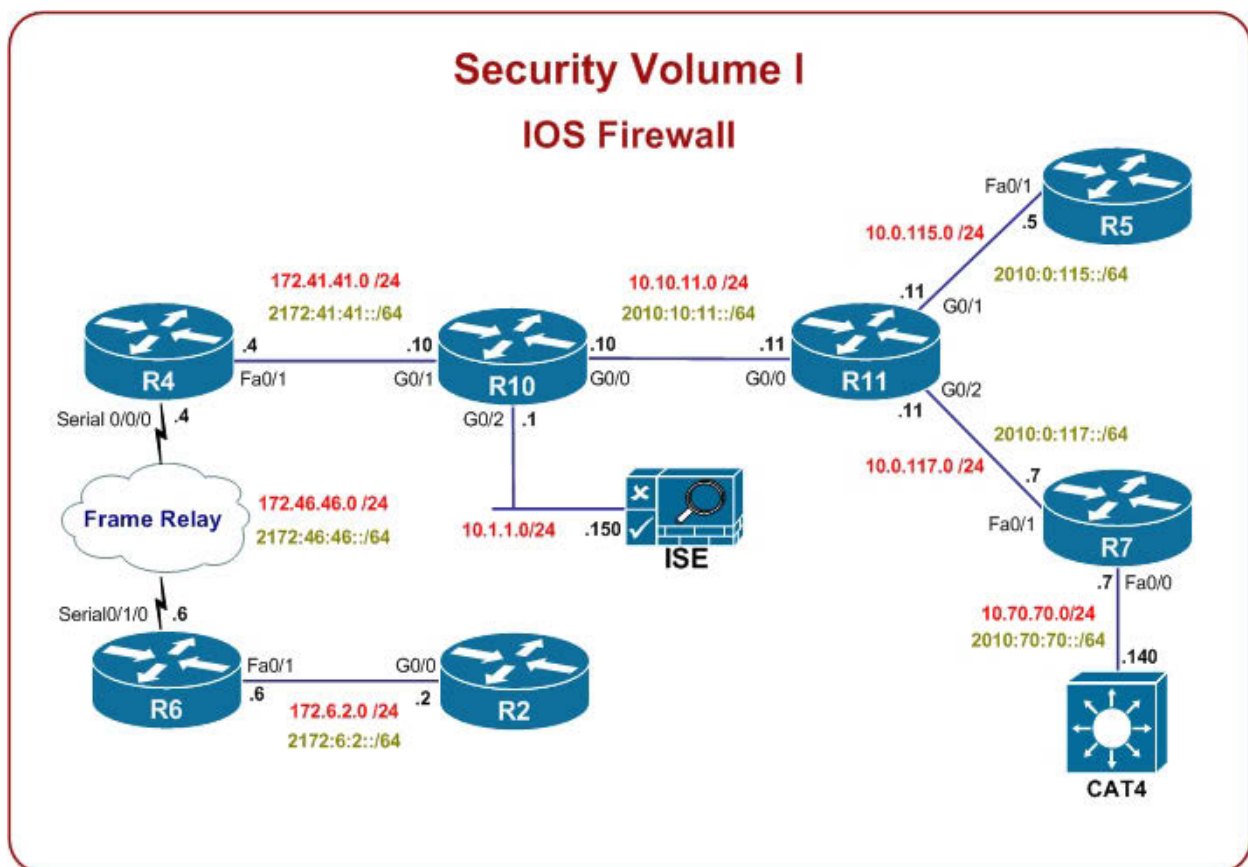
Estimated Time to Complete: **5 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R2	G0/0	62	172.6.2.2/24
			2172:6:2::2/64
	Loop0		2.2.2.2/24
			2::2/64
R4	F0/1	41	172.41.41.4/24
			2172:41:41::4/64
	S0/0/0		172.46.46.0/24
	Loop0		2172:46:46::4/64
			4.4.4.4/24
			4::4/64
R5	F0/1	115	10.0.115.5/24
			2010:0:115::5/64
	Loop0		5.5.5.5/24
			5::5/64
R6	F0/1	62	172.6.2.6/24
			2172:6:2::6/64
	S0/1/0		172.46.46.6/24
	Loop0		2172:46:46::6/64
			6.6.6.6/24
			6::6/64
R7	F0/0	70	10.70.70.7/24
	F0/1	117	10.0.117.7/24
			2010:0:117::7/64
	Loop0		7.7.7.7/24
			7::7/64
R10	G0/2	100	10.1.1.1/24
	G0/1	41	172.41.41.10/24
			2172:41:41::10/64
	G0/0	101	10.10.11.10/24
			2010:10:11::10/64
	Loop0		100.100.100.10/24
			10::10/64
R11	G0/0	101	10.10.11.11/24

G0/1	115	2010:10:11::11/64 10.0.115.11/24
G0/2	117	2010:0:115::11/64 10.0.117.11/24
Loop0		2010:0:117::11/64 11.11.11.11/24 11::11/64



Lab-2 Configuration tasks

Task 1: IOS NAT

- Configure R11 to NAT R7's F0/1 to 10.10.11.7
- Configure a pool using 10.10.11.60 – 10.10.11.80 for the rest of the devices in VLAN 117
- R5's F0/1 should be translated to 10.10.11.50 if attempting to connect to R10's loop0
- For any other destinations the translated address should be 10.10.11.5
- Outside to Inside traffic should be allowed but only to the respective addresses
- Allow the rest of the IPs in VLAN 115 to be translated to R11's G0/0
- Configure R11 to keep these translations for ICMP traffic for 3 seconds, UDP for 60 seconds and TCP for 40 seconds
- If a TCP packet does not complete communication for either FIN or SYN state R11 should remove the translation after 20 seconds
- Enable NAT on R10. Don't specify "inside" or "outside" domains
- Configure R10 to translate all VLAN 101 addresses to a pool 172.99.99.60 – 172.99.99.80
- If the addresses are exhausted allow for PAT
- As a result VLAN 101 devices should be able to communicate with public networks
- Limit the maximum number of NAT translations for any given host on R10 to 25
- Log R11's translations to the Syslog server 10.10.11.100

Task 2: IOS Access-Lists

- On R2 allow HTTP and HTTPs destined to a webserver located at 2.2.2.2
- The above mentioned webserver will be taken down for maintenance and backups
- Every Wednesday between 1am and 3am traffic to this device should be blocked
- The maintenance schedule will come into effect March 1st 2013 and will last for the next 2 months
- New TCP sessions should not be allowed to/through R2. Log all attempts
- Devices from behind R2 including the router must be able to establish new TCP sessions.
- There should be an explicit entry in the ACL allowing it. Also permit all other traffic
- There are multiple servers located in VLAN 70 behind R7:
 - 10.70.70.22 & 2010:70:70::22 (SSH, Syslog, HTTPs)
 - 10.70.70.53 & 2010:70:70::53 (DNS, Kerberos, LDAP SSL)
 - 10.70.70.153 & 2010:70:70::153 (DNS, Kerberos, LDAP SSL)
- Create access-lists that will allow for communication to those servers from any source
- IPv4 ACL should only have three "permit" entries
- All other unnecessary traffic should be explicitly blocked but not logged
- You should be as specific as possible in both ACLs. Apply them inbound on R7's F0/1

Task 3: Reflexive Access-Lists

- On R6 allow uses from VLAN 62 to reach external networks. Allow the following :
 - SSH to routers R4 and R10
 - SMTP
 - DNS
 - HTTP and HTTPs
- The return entries should be automatically created for the above mentioned traffic
- These entries should expire after 3 minutes for TCP-based protocols
- DNS entries (TCP & UDP) should expire after 1 minute
- Global Reflexive Timeout should be set to 100 seconds
- You are allowed to make any other necessary permissions and permit ICMP but all other traffic should be dropped
- Configure the same policy for IPv6 traffic
- Don't use CBAC or ZFW to accomplish this task

Task 4: CBAC

- Allow all TCP and UDP based traffic to go out and return from the “external” networks (172.x.x.x) on R10
- Inbound and outbound traffic should be inspected using CBAC
- Also inspect router-generated packets
- Make sure CBAC engine can properly inspect fragmented traffic
- Log all the denies. Only permit traffic as required by the lab
- Configure the same policy for IPv6 traffic

Task 5: CBAC Application Inspection & Tuning

- R10 configuration should be modified to meet some additional requirements
- The router should delete TCP connections if they have been idle for 10 minutes
- For web traffic only allow Java applets to be downloaded from web servers 2.2.2.2 and 6.6.6.6
- POP3 inspection should be enabled. Make sure the firewall requires secure authentication by the clients
- Turn on logging of all TCP sessions for IPv4
- After FIN exchange was detected, session should be managed for no longer than 10 seconds
- Optimize firewall's performance by adjusting CBAC memory structure to ~2000 sessions
- IPv6 CBAC Alerts should be only enabled for TCP; UDP idle timeout should be 2 minutes
- Internal web servers 10.10.11.198 & .199 should be protected from SYN-Flood attacks
- These servers are reachable from the public network via 172.41.41.198 & .199 and are configured to listen for HTTP traffic at ports 80, 8080 and 10080
- R10 should start deleting half open sessions if they are at 800. This behavior should cease when this number drops below 600

- Also if there have been 100 new half-open connections detected within the last one
- Minute, router should start deleting them. When the number of these sessions drops below 50, this process should stop
- If there is more than 450 TCP half-opened sessions hanging on a single server drop all of them and don't allow for any new connections for the next 2 minutes

Task 6: Zone-Based Firewall

- Configure Zone-Based Firewall on R11
- Create three zones – IN (towards R7), OUT (towards R10) and DMZ (towards R5)
- All TCP and UDP traffic from inside should be allowed to go out OUT and DMZ
- Router 5's loopback0 (5.5.5.5 and 5::5) emulates an IPv4 VPN gateway & IPv4/IPv6 HTTP server (port 9080)
- Make sure these services will be accessible to anyone coming from the "outside"
- Don't use an ACL to classify HTTP traffic
- ICMP is allowed to pass freely between the zones
- Deploy the same policy for IPv6 traffic (except for VPN)
- Packets that are dropped by ZFW should be logged
- Make sure routing is still working after you are done with this section

Task 7: Zone-Based Firewall Inspection & Tuning

- R11 configuration should be modified to meet some additional requirements
- Sessions originated on the "inside" destined to the "outside" should be managed in the following way:
 - TCP connections should be removed after 15 minutes of inactivity
 - TCP sessions should be kept for 12 seconds after FIN-exchange was detected
 - If a TCP session does not fully establish within 20 seconds it should be removed
 - UDP idle timeout should be set to 90 seconds
 - Change the DoS thresholds to 500/300 (total) and 100/50 (one minute)
 - Packets with Routing Extension Header should be inspected
- Tune configuration of the firewall for packets flowing in the "outside" -> "dmz" direction
- Java applets should not be downloaded
- Don't allow users to send HTTP requests with a URI greater than 30 Bytes
- Log any violations

Task 8: User-Based Firewall

- Configure R4 with User-Based Firewall
- Create two zones – internal (F0/1) and external (s0/0/0)
- Prior to accessing the network connecting users should successfully authenticate using
- Authentication Proxy and RADIUS. Use ISE as an AAA server

- Authenticated users trying to access external networks through R4 should be subject to the following policy:
 - Members of the Sales department should be able to access all TCP applications on a server located at 6.6.6.6. Don't permit any other traffic for those users
 - Administrators should be able to access any outside destinations using TCP and ICMP, including the Sales server
- Dropped inside -> outside packets should be logged
- All other traffic, including ICMP packets coming from the external networks, should be blocked

Section 3

Ironport S-Series: WSA

Lab-1: WSA Initialization Overview

Lab-1: WSA Initialization – This lab is intended to familiarize you with the initialization of the WSA to act as a web proxy, customizing EUN, testing basic proxy functions using PAC files for Firefox and integrating WSA with Active Directory for user authentication. We shall start configuring WSA initially in explicit forward proxy mode and later labs will focus on transparent mode.

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

General Rules

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

Estimated Time to Complete: **1.5 Hour**

Pre-setup

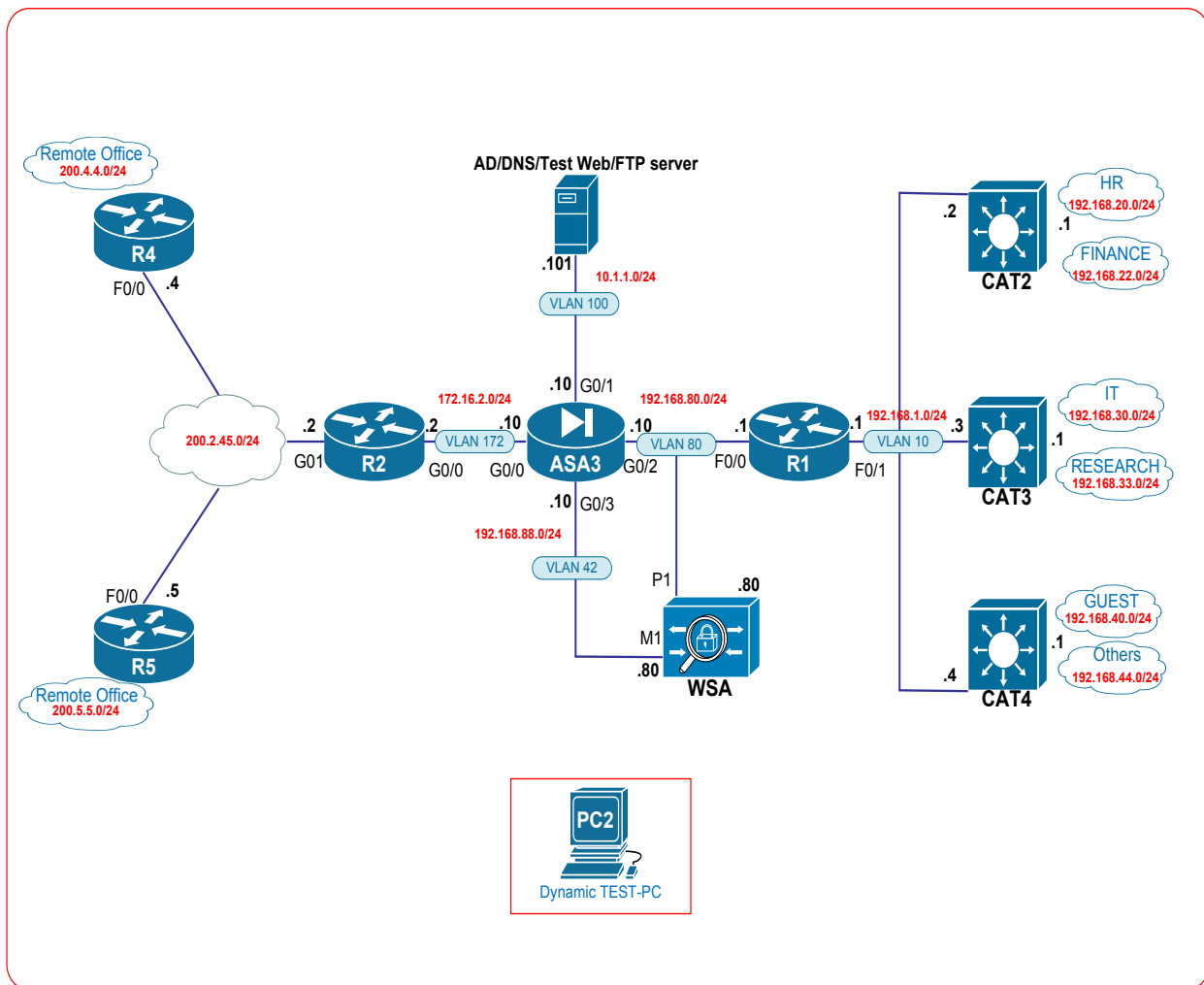
Load the initial configurations for the ASA, routers and switches. Note that routers and switches are pre-configured with these initial configurations.

NOTE: *Do not make additional configuration on the ASA and routers, unless explicitly asked for in the task; some switching configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 3.1 (Logical)



Lab 1: Configuration Tasks

Task 1: Initialization WSA

- Configure appropriate VLAN's on the switch for WSA as per topology diagram 3.1.
- Bootstrap WSA using GUI with system setup wizard. Therefore place TEST-PC in VLAN-42 and connect to the WSA using the factory default IP address and port. Use any IP for the TEST-PC to match the factory default subnet of WSA.
- Configure the below parameters when the system setup starts.

Network Settings		
Default System Hostname		wsa.ipexpert.com
DNS Servers		10.1.1.101
Network Time Protocol (NTP)		(Default)
Time Zone		America/New_York
Upstream proxy		none
Interface Management (M1): Address and Hostname	IP	192.168.88.80/24 wsam1.ipexpert.com
M1 Management Access		Use M1 only for Management Access
Interface Proxy (P1): Address and Hostname	IP	192.168.80.80/24 wsa.ipexpert.com
L4 Traffic Monitor		Duplex TAP: T1 (In/Out)
Default Gateway		M1 - 192.168.88.10 P1 - 192.168.80.10
Static Routes for P1		Network-192.168.0.0/16 Gateway-192.168.80.1
Transparent Connection Settings		None- Only explicit forward proxy
Email System Alerts To		admin@ipexpert.com
Internal SMTP Relay Hosts		mail.ipexpert.com
Administrator Password		"ironport" (Uncheck Autosupport and sender base participation)

Security Settings	
L4 Traffic Monitor	Monitoring
Acceptable Use Controls	Enabled
Active Acceptable Use Controls Engine	Cisco IronPort Web Usage Controls
Web Reputation Filters	Enabled
IronPort DVS™ Engine	Webroot: Enabled McAfee: Enabled Sophos: Enabled
IronPort Data Security Filtering	Enabled

NOTE: After you install the above configuration you will lose access to the WSA since the IP address of WSA changes from the factory default IP.

Task 2: Enable basic web and FTP proxy function and PAC file hosting

- Place the TEST-PC in VLAN 20 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally, configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW2 SVI VLAN 20 as the next hop.

NOTE: Do not set the default gateway when you change the IP address else you will lose RDP access.

- Use Internet explorer or chrome for configuring WSA. Firefox will be used as the web browser to test explicit web proxy feature of WSA.
- Connect to the M1 interface and ensure Web proxy and FTP proxy is enabled on the proxy default ports. Configure a FTP banner of "IT FTP POLICY"
- Configure WSA to host PAC files on TCP port 9001
- Create a simple PAC file using notepad such that the web browsers should use wsa.ipexpert.com and TCP proxy port 3128 as the web proxy server for any URL's.
- Configure Firefox to use WSA as the proxy server. It should download the PAC file from the WSA automatically. Verify that the PAC file is downloaded to the Firefox using from log files (pacd_logs)
- Ensure you can connect to www.ipexpert.com using Firefox. Verify using that Firefox is using WSA from log files using accesslogs.

Task 3: Configure acknowledgement and custom end-user notifications

- Configure WSA to send EUA to users before they are allowed web access. Add any custom message. Use Iron port logo. Do not change the default timeout values.

- Configure WSA to send Ironport notification and warning messages to users.
- WSA should send the below message/custom EUN when there is a DNS resolution error for a URL to the users. Test this by entering a wrong URL. “Re-Check your URL. Wrong URL entered”

Task 4: Configuring Active Directory authentication for users

- Set the time and date manually on the WSA to match the AD server
- Configure WSA with an AD realm “ADServer”
- The authentication protocol would be NTLMSSP.
- The AD server IP is 10.1.1.101 and the AD domain is IPEXPERT.COM
- Join the Domain using username of “Administrator” and password “IPexpert123”.
- Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction. IP Surrogate cache time out should be set to 5 minutes.
- Enable authentication in the global identity policy. Use IP surrogates only.
- Test by browsing to www.google.com or www.ipexpert.com using a username of “HRUSER1” with a password of “cisco”. Verify from log files using accesslogs.

Lab-2: Configuring Acceptable Use Policies on WSA for HTTP and FTP

Lab-2: Configuring AUP's for HTTP and FTP – This lab is intended to familiarize you with configuring various access and identity policies for HTTP and FTP traffic. You will also configure fall back policies using guest privilege feature, custom URL categories and authentication bypass for certain web traffic.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.

- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **4 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure Access Policies

- Your network has a very strict web access policy. Configure the Global policy such any authenticated user is allowed web access as per the below policy. Block any FTP requests. Test from the TEST-PC and check the access logs.
- Set to monitor for uncategorized URL's.
- Set URL content filtering to block for Search engines that don't support safe search and set site content rating to block web content which is explicitly rated as adult oriented.

URL Filtering	
Global Policy	Configure Monitor only the below categories and block all other URL categories.
	Business and Industry Computer Security Computers and Internet Education Government and Law News Streaming Media Search Engines and Portals

- Remote office LAN subnets users from 200.4.4.0/24 and 200.5.5.0/24 connect to the ASA main office for web access. They should be denied any streaming media access since it consumes bandwidth. The global policy permits streaming media. Hence configuring a new access policy, which denies streaming media access for those subnets.
- HR department needs additional access, which is blocked by the global policy. They need access to various job search engines, social networking sites and conduct investigations of any mis-conduct by the employees. Configure a new access policy such that HR group and user IPEXPERT0\HRUSER1 user from 192.168.20.0/24 subnet can have additional web access as per the below table. Test by connecting to www.facebook.com. Verify using accesslog entries.

URL Filtering	
HR Policy	Besides the Global policy monitor the below URL categories based on giving warning/Splash page before they access those sites.
	Cheating and Plagiarism
	Illegal Activities
	Job Search
	Social Networking

- Finance department needs additional access, which is blocked by the global policy. They need access to various financial and trading sites. Configure a new access policy such that Finance group and user IPEXPERT0\FINUSER1 user from 192.168.22.0/24 subnet can have additional web access as per the below table. Test by connecting to www.ft.com. Verify using accesslog entries.

URL Filtering	
Finance Policy	Besides the Global policy monitor the below URL categories based on time based condition – Weekdays 9 AM to 5 PM.
	Finance – With time range – Monitor else Warn
	Online Trading – With time range – Monitor else block
	Real Estates – With time range – Monitor else block

NOTE: To test you will need to reconfigure the switch and the Test PC.

Place the TEST-PC in VLAN 22 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW2 SVI VLAN 22 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

- IT department needs additional access, which is blocked by the global policy. Configure a new access policy such that IT group and user IPEXPERT0\ITUSER1 user from 192.168.30.0/24 subnet can have additional web access as per the below table. IT users will need to use FTP. Hence allow FTP protocols. Test by connecting to www.gmail.com and also to the FTP server [ftp.ipexpert.com](ftp://ftp.ipexpert.com).
- Use Filezilla client on TEST-PC to point to WSA for FTP proxy and configure checkpoint format for on the Native FTP client for FTP proxy authentication.

URL Filtering	
IT Policy	Besides the Global policy monitor the below URL categories. WSA should present warning only for File Transfer Services.
	File Transfer Series (WARN) Software Updates Web Hosting Web Page Translation Web-based Chat Web-based Email

NOTE: To test you will need to reconfigure the switch and the Test PC.

Place the TEST-PC in VLAN 30 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW3 SVI VLAN 30 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

- Research department users require complete web access for R&D purposes. Configure a new access policy such that Research group and user IPEXPERT0\RUSER1 from 192.168.33.0/24 research subnet can have full access to the web. Monitor all categories and allow FTP protocols. Do not enforce URL content filtering inherited from the global policy.
- Unless WBRS or other scanners block a website, the user should have complete access to the web. Test by connecting to www.facebook.com, www.google.com. You should be presented with a block page when you connect to www.ieplugin.com or www.ihaveabadreputation.com based on WBRS.

- 192.168.33.33 should bypass AD authentication. You are allowed to configure a new Identity and access policy for this. This policy should be effective any time during weekdays and between 10 AM to 4 PM during weekends.

NOTE: To test you will need to reconfigure the switch and the Test PC.

Place the TEST-PC in VLAN 33 and use IP of 192.168.33.33. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 and 192.168.0.0/16 with SW3 SVI VLAN 33 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

Task 2: Configure Guest privileges and Custom URL policy -1

- Users failing the authentication should be treated as guest users. All the guest users will connect from VLAN 44.
- Create a new identity policy for the guest subnet and enable guest privileges.
- Create a new access policy that matches guest users allow access (Monitor) only to www.ipexpert.com and block all other URL categories.
- You are allowed to create one custom URL category to accomplish this task.
- Place this access policy just above the global policy.
- Block uncategorized URL's.
- Test this policy from VLAN 44. You may need to reconfigure TEST-PC and switch accordingly.

Task 3: Configure Custom URL policy - 2

- All users except guests should be allowed access (Monitor) to host URL and all subdomains of files.com
- You are allowed to create one custom URL category to accomplish this task.

Task 4: Configure Custom URL policy - 3

- Authentication is breaking Microsoft windows update for the IT users.
- You are allowed to create one custom URL category for the below URL's
 - download.windowsupdate.com
 - update.microsoft.com
 - windowsupdate.com
 - windowsupdate.microsoft.com
 - download.microsoft.com
 - download.windowsupdate.com
 - ntservicepack.microsoft.com
 - stats.update.microsoft.com
 - windowsupdate.microsoft.com
- Configure a new Identity policy which disables authentication for the newly created MS update custom URL's. Additionally, the HTTP requests to these URL's should also contain windows update user agent.

- Configure a new access policy, which explicitly allows access to windows update only for those URL's with a windows update user agent string from the IT subnet.

Task 5: Configure Custom URL policy – 4

- Configure a new identity policy, which disables authentication for adobe acrobat and iTunes software updates.

Task 6: Configure Custom URL policy – 5

- Only IT subnet users should be able to remotely manage R4 (HTTP-8888) and R5 on HTTP port 80. Create custom URL policy to allow access to R4 and R5. The custom URL should include the below URL's only. Test from the TEST-PC. R4 and R5 have been pre-configured for this task. Use a username of cisco and password of cisco for R4 local HTTP authentication of the routers.
 - 4.4.4.4
 - 5.5.5.5
 - r4.ipexpert.com
 - r5.ipexpert.com

NOTE: To test you will need to reconfigure the switch and the Test PC.

Place the TEST-PC in VLAN 30 and use any IP address from that subnet for the PC. 10.1.1.101 should be the DNS server for the PC. Additionally configure appropriate static routes on the PC for 10.1.1.101/32 4.4.4.4/32, 5.5.5.5/32 and 192.168.0.0/16 with SW3 SVI VLAN 30 as the next hop. DO NOT CONFIGURE ANY DEFAULT GATEWAY.

Task 7: Configure Custom URL policy – 6

- IT users should not be able to view images when they access www.ipexpert.com. Create a custom URL policy that blocks any jpeg files from www.ipexpert.com.
- Do not use object blocking.
- Test from test PC. You should be able to see the image when you browse into <http://ipexpert.com> and the image filtered when you browse to www.ipexpert.com if your custom URL category creation is correct.
- Configure the access policy appropriately.

Task 8: Configure Custom URL policy – 7

- If any research user tries to access R4 and R5 routers they should be redirected to <http://block.ipexpert.com>. You are allowed to use custom URL categories in the access policy to accomplish this task.
- To test you may need to reconfigure the switch and TEST-PC accordingly.

Lab-3: Configuring Acceptable Use Policies on WSA for HTTPS

Lab-3: Configuring AUP's for HTTPS– This lab is intended to familiarize you with configuring WSA as a HTTPS proxy and configuring various decryption policies.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- To test a task you may need to re-configure the TEST-PC and the switch accordingly. DO not explicitly set the default gateway on the TEST-PC.

Estimated Time to Complete: **1.5 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-2 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure WSA for HTTPS Proxy

- Enable HTTPS proxy services on the WSA. The WSA should act as a self-signed root authority when acting as man in the middle for HTTPS proxy. Use the below parameters for creating the self-signed root certificate. Enable decryption for AVC. Invalid certificate handling should be set to monitor.
 - Common name: WSA
 - Organization: NETSEC
 - Organizational Unit: IPEXPERT
 - Country: US
 - Expiration Date: 36 Months

Task 2: Decryption Policies – 1

- Configure decryption for the below URL categories so that access policies can be applied for them. WSA should drop all other SSL connections even for sites have no WBRS scores.
 - Business and Industry
 - Cheating and Plagiarism
 - Computer Security
 - Computers and Internet
 - Education
 - File Transfer Services
 - Finance
 - Government and Law
 - Illegal Activities
 - Job Search
 - News
 - Online Trading
 - Real Estate
 - Science and Technology
 - Search Engines and Portals
 - Streaming Media
 - Web Hosting
 - Web Page Translation
 - Web-based Chat
 - Web-based Email

Task 3: Decryption Policies – 2

- All traffic destined to Microsoft update server should pass through without decryption. Configure a new decryption policy that is applicable only for IT subnet for the above-mentioned traffic.

Task 4: Decryption Policies – 3

- Research user subnet should be allowed HTTPS access for all URL's based on WBRs. WBRs should either drop or decrypt based on WBRs score. Sites with no WBRs scores should be dropped. You are allowed to modify WBRs. However do not change the WBRs drop threshold.

Task 5: Decryption Policies – 4

- Create a decryption policy to explicitly decrypt HTTPS traffic destined to R4 and R5 for only IT users/Subnet. All requests from others should be dropped.

Task 6: Decryption Policies – 5

- Drop all HTTPS requests to streaming media sites from the remote office LAN users.

Task 7: Decryption Policies – 6

- All software updates with user agent of iTunes and Adobe Acrobat updater should pass through without decryption. This should apply for the IT subnet only.

Task 8: Decryption Policies – 7

- Create decryption policies, which allow all users to directly connect to <https://www.ipexpert.com> without the need for a proxy in the middle.
- Guest users should be allowed access to only to <https://www.ipexpert.com> subject to other scanning verdicts. Drop all other URL categories for guest users.

Task 9: Decryption Policies – 8

- WSA should decrypt all traffic for the research subnet. Ensure that they can directly connect to <https://www.ipexpert.com>

Lab-4: Configuring advanced access policies for downloads

Lab-4: Configuring advanced access policies– This lab is intended to familiarize you with configuring access policies with protocol & object download rules, AVS and DVS-Virus/Malware scanning for downloads.

General Rules

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

Estimated Time to Complete: **1.5 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-3 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Task 1: Configure download bandwidth limits and object download blocking

- Globally configure an overall download limit to 100 Mbps.
- Each group should be allowed a maximum download limit for HTTP/HTTPS to 20 MB and 5 MB for FTP. Configure this in the Global Policy.
- IT group should be allocated 50 MB download limit for HTTP/HTTPS and FTP.
- Research subnet user traffic and MS update traffic is should not be subject to any download limits
- Configure a global policy to block downloads of any archives, windows EXE files, audio, video and bit torrent links/files.
- Disable object blocking for MS update traffic, IT subnet users and Research subnet users.

Task 2: Configure Application visibility and control for web traffic

- Configure the global policy to block P2P file sharing and block files sent through IM chat, which uses web browsers.
- Globally configure media bandwidth limits per user to 512 Kbps
- 192.168.33.33 should not be subject to the above policies.

Lab-5: Configuring data transfer policies.

Lab-5: Configuring DLP's and outbound malware scanning– This lab is intended to familiarize you with configuring outbound data transfer policies/DLP's and outbound malware scanning.

General Rules

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

Estimated Time to Complete: **1 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-4 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure outbound malware scanning

- Configure outbound malware scanning using Webroot and Sophos globally. Block any uploads of malware files.
- Research subnet traffic should use Webroot and MacAfee for scanning outbound data transfers. Block any uploads of malware files. Create a new policy to accomplish this.

Task 2: Configure data transfer policies

- Configure the global policy to block uploads of any Archives, Windows and UNIX executable files, Installers, Audio, Video and bit torrent links.
- Globally block all uploads of documents types except PDF/MS office files below 5 MB size and XML below 2 MB.
- Maximum upload limit for HTTP/HTTPS and FTP should be 5 Mbps globally.
- Research and IT subnet users should not be subject to the above upload blocking policies. Create a new policy to accomplish this.
- WBRs blocking threshold for IT and research users should be between -10 to -5.

Lab-6: Configuring WCCP and transparent proxy mode with Single Sign On.

Lab-6: Configuring WCCP and transparent mode— This lab is intended to familiarize you with configuring WSA for transparent mode using WCCP on the ASA. It also focuses on proxy bypass feature and Single Sign on.

General Rules

- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.

- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.

Estimated Time to Complete: **1 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-5 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure transparent proxy bypass

- Configure transparent proxy bypass for 192.168.88.80 and cisco WebEx traffic.

Task 2: Configure transparent proxy bypass

- Configure WCCPv2 using dynamic service ID of 90 for HTTP/HTTPS traffic (TCP-80 and 443) on the ASA. The ASA should redirect traffic all HTTP/HTTPS traffic arriving on the inside interface to the WSA. Use password of “1PEXPERT”
- Configure WSA accordingly for transparent redirection using WCCPv2
- Test from the internal LAN.

Task 3: SSO using Mozilla.

- Configure WSA with a short hostname of “wsa” as the redirect hostname for SSO.
- Login as one of the domain users on the TEST-PC and test SSO. You are allowed to re-configure Mozilla and host file entries on the TEST-PC accordingly for SSO to work.
- To test you may need to reconfigure the TEST-PC and switch accordingly.

Lab-7: Configuring L4TM on WSA

Lab-7: Configuring L4TM on WSA– This lab is intended to familiarize you with configuring WSA with L4TM blade.

General Rules

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

Estimated Time to Complete: **1 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-6 successfully. Use the logical topology drawing – Network Topology 3.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure SPAN/RSPAN

- Configure SPAN/RSPAN to mirror traffic from VLAN 200 to T1 port of WSA.

Task 2: Configure transparent proxy bypass

- Configure transparent proxy bypass for the host wikipedia.org and all subdomains of wikipedia.org

Task 3: Configure L4TM.

- L4TM should be enabled on all ports except web ports. T1 should be in duplex mode.
- Configure L4TM to block all suspected malware. Traffic destined to manage R4 and R5 should be explicitly allowed using White/Allow list.

Section 4

ISE: Identity Services Engine

Lab-1: Basic Configuration of ISE

Lab-1: ISE Basic Setup – This lab is intended to familiarize you with the basic configuration of the ISE. The VM appliance of ISE has already been initialized. The focus is to modify basic parameters and configure basic features on ISE. The basic features cover configuring a new self-signed certificate, RBAC for administrative control, repository configuration, routing configuration, NTP configuration, Integration with active directory.

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

General Rules

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

Estimated Time to Complete: **2 Hours**

Pre-setup

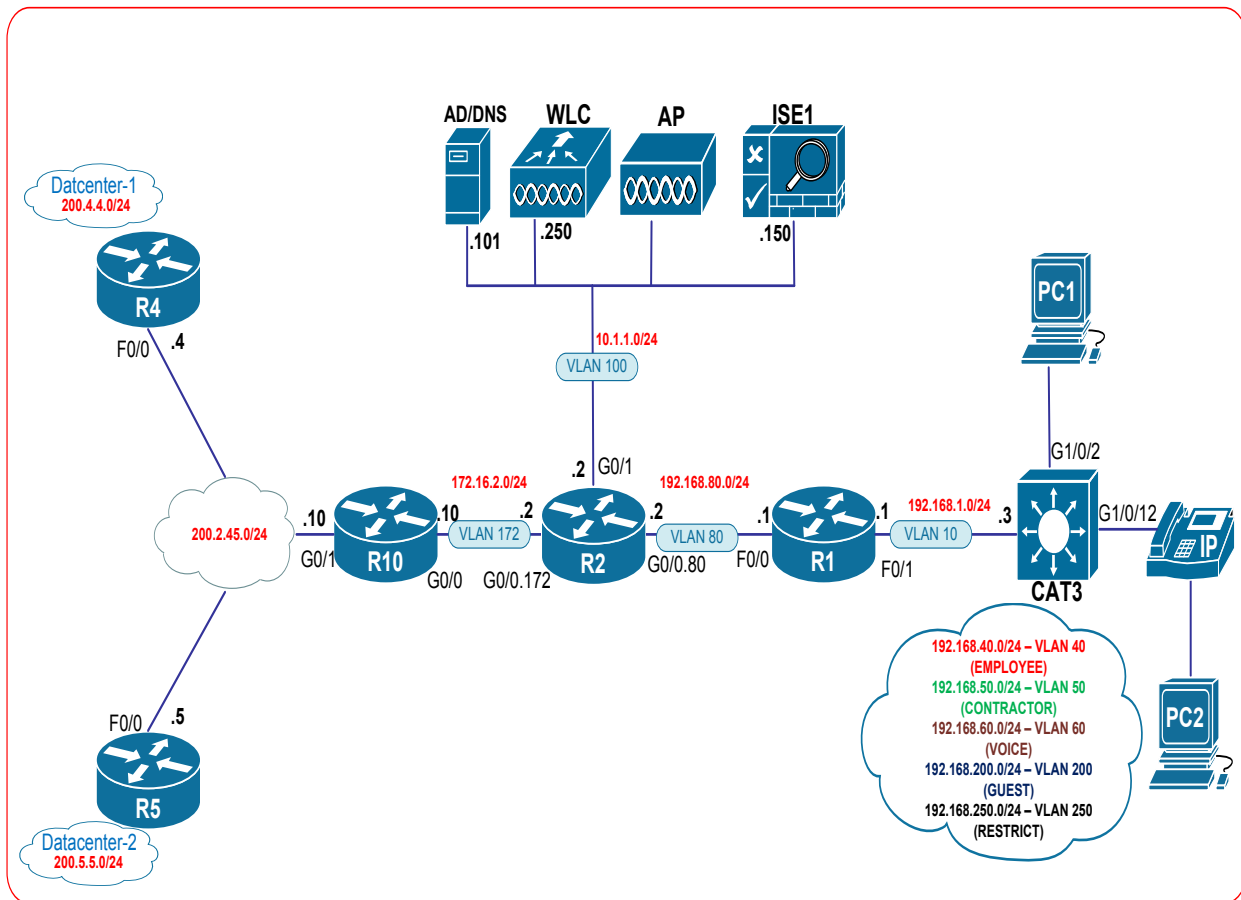
Load the initial configurations for the routers and switches. Note that routers and switches are pre-configured with these initial configurations.

NOTE: *Do not make additional configuration on the routers, unless explicitly stated in the task; some switching configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 4.1 (Logical)



Lab 1: Configuration Tasks

Task 1: Basic Setup of ISE

- Configure appropriate VLAN's on the switch for ISE as per topology diagram 4.1.
- R2 has been pre-configured to be the NTP server, make sure that R2 and the AD server has the same time settings.
- Add a static route for 192.168.0.0/16 with R2 as the next-hop on the ISE.
- Configure UTC as the time zone and set AD server and R2 as the NTP servers on ISE. Make sure R2 and AD have the same time.
- Configure AD server as the repository using FTP protocol. The repository name should be "AD_FTP". The URL should be configured as <ftp.ipexpert.com>. Use "administrator/IPexpert123" for the ftp login.
- Use "show application status ise" in the CLI and make sure all processes are running before you login to the GUI using the IP address of the ISE.
- Integrate ISE with active directory. Use a name of "AD1". The AD domain name should be ipexpert.com. Use "administrator/IPexpert123" to join the domain.
- Enable Password Change, Enable Machine Authentication and Enable Machine Access Restrictions for AD connection settings.
- Retrieve "IPX_EMP", "IPX_CON" and "Domain Computers" from the AD group attributes. These will be used for creating authorization policies in the later section.
- Configure Identity Source sequence called "AD_LOCAL" such that users are first authenticated with AD server, if this server is not accessible or users are not found in the database then the internal user endpoint database will be used for authentication as the second method.
- Use predefined RBAC policies for administrative access. Create a new user operator/IPexpert321. Assign operator user to a pre-defined group of helpdesk, which can view only the operations menu.
- Configure a new RBAC policy and group called "Policy_Admin" with the below parameters. Create a new user called policyadmin/IPexpert123 and test this admin policy. This user should be allowed to create/modify policies and view AAA clients/NDG's.

RBAC Policy and Group – "Policy_Admin"		
RBAC Menu Access policy	Allow – Operations (Allow All) Allow – Policy (Allow All) Limited - Administration	Only show "Networkresources"
RBAC Data Access Policy	Use pre-defined policy – "Network Admin Data Access"	

Lab-2: Configuring network resources and profiling on ISE

Lab-2: Configuring network resources and profiling – This lab is intended to familiarize you with configuring AAA clients, NDG's, enabling profiling services and modifying existing profiling policies.

General Rules

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

Estimated Time to Complete: **1.5 Hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully. Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure NDG's and AAA clients on ISE and switches.

- Create new NDG called "WLC" and "SWITCH" under "All device type".
- Add SW3 as the AAA client. SW3 will use VLAN 10 IP address as the source for sending RADIUS packets. Use a radius key of cisco123. Assign these switches to "SWITCH" NDG under All Device type
- Add WLC as the AAA client. Use a radius key of cisco123 and assign this device to "WLC" NDG under All Device type.
- Configure ISE (10.1.1.150) as the radius server on the switches
- SW3 should use test/cisco123 to test the connectivity between switch and ISE automatically every 1 hour. You are allowed to create a new network access user to accomplish this.
- Change the dead timer criteria for the AAA server on the switches such that if no valid response from the ISE within 15 seconds, the server should be marked as dead.
- Make sure G1/0/2 G1/0/13 and G1/0/12 interfaces on SW3 are in shutdown state.

Task 2: Configure profiling.

- Enable profiling services on ISE. It should use DHCP probes, HTTP probes, RADIUS probes, DNS probes, SNMPQUERY probes and SMTPTRAP (all) probes on all interfaces for profiling.
- Configure SNMP version 2c for AAA clients on ISE and on the NAD's with a community string of "ipexpert". Change the polling interval on ISE to the minimum possible.
- Enable SNMP traps for linkup, linkdown, mac-notification change, mac-notification move on the NDA's/AAA clients. The SNMP trap and informs should be sourced from VLAN 10 interface.
- Configure additional DHCP helper address on SW3 pointing to the ISE server IP of 10.1.1.150 for SVI interfaces of VLAN 40, 50, 60, 200 and 250. AD has been preconfigured to be the DHCP servers for these VLAN's.
- Re-configure existing profiling policy to make sure that existing profiling policy "Cisco-IP-Phone" "Windows7-Workstation" and "Cisco-Access-Point" creates a matching end point identity group when devices match the profiling policy.
- Change the CoA for profiling to re-auth on the ISE globally.
- Un-shut G1/0/13, G1/0/12, G1/0/2 on SW3 to test profiling policy.

Lab-3: Configuring ISE and Switches for MAB and 802.1x

Lab-3: Configuring ISE and switches for MAB and 802.1x– This lab is intended to familiarize you with configuring ISE with authentication and authorization policies for MAB and 802.1x for wired and wireless access. You will also be configuring switches for 802.1x with low impact mode, MAB and flex-auth and WLC for 802.1x authentication for wireless clients.

General Rules

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

Estimated Time to Complete: **5 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-2 successfully. Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configuring AAA clients for wired MAB and 802.1x with low impact mode.

- Configure 802.1x globally on SW3.
- Configure Access VLAN of 250 for SW3 G1/0/2 and G1/0/12 and VLAN 100 for G1/0/13. The voice VLAN for port G1/0/12 on SW3 should be set to 60.
- Enable 802.1x and MAB on G1/0/12, G1/0/13 and G1/0/2 on SW3.
- Configure Flex-auth for the above mention ports and change the order of authentication first to MAB and then to 802.1x method, however 802.1x authentication should have higher priority than MAB.
- Change the host mode to multi-auth and violation action to restrict.
- Configure low impact mode and configure a port ACL that allows only DHCP, DNS, ICMP traffic. Log all the packets that are denied.
- Configure periodic re-authentication and the timeout values for re-authentication should be obtained from the ISE for G1/0/12 and G1/0/2 interfaces of SW3.
- Idle timeout value should be obtained from ISE for G1/0/2 of SW3
- Change the 802.1x transmit timer to 10 seconds on all the ports configured for 802.1x.
- Switches should be configured to process RADIUS VSA for authentication and accounting
- Switches should include RADIUS attributes 6,8 and 25 in the RADIUS requests
- Configure CoA on the switches and enable device tracking.

Task 2: Configuring ISE for wired MAB and 802.1x with low impact mode.

- Create a new authentication protocol result called “MAB” that allows only host lookup for MAB.
- Create a new authentication protocol result called “PEAP_MSCHAPv2” that allows only PEAP as the outer/tunneling method and the EAP-MS-CHAPv2 as the inner method for 802.1x authentications.
- Configure authentication policies as per the below table

Name		Condition		Protocols		Identity Source
MAB-Auth-Policy_WIRED	IF	Wired_MAB AND Device:Device Type = Device Type#All Device Types#SWITCH	allow protocols	MAB	and use	Internal Endpoints
Dot1X-Auth-Policy_WIRED	IF	Wired_802_1X AND Device:Device Type =	allow protocols	PEAP_MSCHAPv 2	and use	AD_LOCAL

Name	Condition		Protocols		Identity Source
	Device Type#All Device Types#SWITCH				
Default Rule (if no match)		allow protocols	Default Network Access	and use	AD_LOCAL

- To test MAB and 802.1x configure authorization policies as per the below table

Name		Identity Group		Conditions		Authorization
Profiled Cisco IP Phones	IF	Cisco-IP-Phone	AND	-	THEN	Cisco_IP_Phone
Profiled APs	IF	Cisco-Access-Point	AND	-	THEN	PermitAccess
Default	IF	no matches			THEN	PermitAccess

- Test the policies from SW3. MAB should be successful and the IP Phone should join the voice domain based on “Cisco_IP_Phone” pre-defined authorization profile.
- RDP into TEST-PC2 and configure it for 802.1x.
- Configure anyconnect profile using NAM profile editor called “IPX_EMPLOYEE” and test 802.1 x authentications. Test using “IPXEMP1/cisco” as the login details for 802.1x. Make sure anyconnect always prompts the user for username and password and does not store the credentials.
- For testing purposes you are allowed to configure static routes on the PC. Do not set the default gateway. PC will automatically get the IP address from the pre-configured DHCP server.

Task 3: Configuring ISE with specific authorization policies.

- Configure policies for employees in your network. Employees belong to “IPX_EMP” group in the AD. After successful authentication/authorization they should be given complete access with a change of VLAN from 250 to 40. VLAN 250 is the default restricted configured on the switchport and VLAN 40 is the employee VLAN.
- Configure dACL for employees as per the below table.

Downloadable ACL

Name	EMPLOYEE_dACL
DACL Content	permit ip any any

- Configure Authorization profile for employees as per the below table.

Authorization Profile	
Name	EMPLOYEE_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	EMPLOYEE_dACL
VLAN	40

- Configure Authorization policies for employees as per the below table

Name		Identity Group		Conditions		Authorization
IPEXPERT_EMPLOYEES	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/ IPX_EMP	THE N	EMPLOYEE_AP
Default	IF	no matches			THE N	DenyAccess

- RDP into TEST-PC2 and login as "IPXEMP1/cisco" and test the above-created rule.
- Configure policies for Machine Authentication for Domain Computers.
- Configure dACL for authenticated domain computers as per the below table.

Downloadable ACL	
Name	DOMAIN_COMP_dACL

DACL Content	permit udp any eq bootpc any eq bootps permit udp any any eq domain permit icmp any any permit ip any host 10.1.1.101
--------------	--

- Configure Authorization profile for domain computers as per the below table.

Authorization Profile	
Name	DOMAIN_COMP_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	DOMAIN_COMP_dACL

- Configure Authorization policy for machine authentication as per the below table

Name		Identity Group		Conditions		Authorization
DOMAIN_COMP	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/ Domain Computers	THE N	DOMAIN_COMP_A P

- Configure policies for contractors in your network. Contractors belong to "IPX_CON" group in the AD. After successful authentication/authorization they should be given complete access except to the data centers. Configure a change of VLAN from 250 to 50. VLAN 250 is the default restricted configured on the switchport and VLAN 50 is the Contractor's VLAN. Configure Machine access restriction for contractors when they are connecting via wired network i.e. switch. They should re-authenticate every 8 hours
- Configure dACL for employees as per the below table. They should not be given access to the data centers.

Downloadable ACL

Name	CONTRACTORS_dACL
DACL Content	deny ip any host 4.4.4.4 deny ip any host 5.5.5.5 deny ip any 20.4.4.0 0.0.0.255 deny ip any 20.5.5.0 0.0.0.255 permit ip any any

- Configure Authorization profile for contractors as per the below table.

Authorization Profile	
Name	CONTRACTORS_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	CONTRACTORS_dACL
VLAN	50
REAUTHENTICATION	28800
Radius: Termination-Action	RADIUS-Request

- Configure Authorization policy for contractors as per the below table.

Name		Identity Group		Conditions		Authorization
IPEXPERT_CONTRACTORS	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/IPX_CON	THEN	CONTRACTORS_AP

Name	Identity Group	Conditions	Authorization
		AND Network Access: WasMachineAuthenticated EQUALS True AND DEVICE: Device Type EQUALS All Device Types# SWITCH	

Task 3: Configuring WLC and ISE for Wireless 802.1x

- WLC should be configured to support 802.1x authentication for employees and contractors connecting through the wireless network. Create the appropriate interfaces, ACL's and WLAN's to accomplish this task.
- Create a new interfaces on the WLC for employee and contractors as per the below table.

Employee Interface	
Interface Name	ipx_employee
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	40
IP Address	192.168.40.2
Netmask	255.255.255.0
Gateway	192.168.40.1
Primary DHCP Server	10.1.1.101

Secondary DHCP Server	-
ACL Name	none

Contractor Interface	
Interface Name	ipx_contractors
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	50
IP Address	192.168.50.2
Netmask	255.255.255.0
Gateway	192.168.50.1
Primary DHCP Server	10.1.1.101
Secondary DHCP Server	-
ACL Name	none

- Create WLAN's on the WLC for employee and contractors as per the below table.

EMPLOYEE WLAN	
Type	WLAN
Profile Name	IPX_EMPLOYEE
SSID	IPX_EMPLOYEE

Status	✓ Enabled
Radio Policy	All
Interface / Group	ipx_employee
Broadcast SSID	✓ Enabled
Security – Layer 2	
Layer 2 Security	802.1X
Security – Layer 3	
Layer 3 Security	None
Web Policy	(Not checked)
Security – AAA Servers	
Authentication Server #1	10.1.1.150, Port:1812
Accounting Server #1	10.1.1.150, Port:1813
Advanced	
Allow AAA Override	✓ Enabled
NAC State	Radius NAC

IPX_CONTRACTOR	
Type	WLAN
Profile Name	IPX_CONTRACTOR
SSID	IPX_CONTRACTOR
Status	✓ Enabled

Radio Policy	All
Interface / Group	ipx_contractors
Broadcast SSID	✓ Enabled
Security – Layer 2	
Layer 2 Security	802.1X
Security – Layer 3	
Layer 3 Security	None
Web Policy	(Not checked)
Security – AAA Servers	
Authentication Server #1	10.1.1.150, Port:1812
Accounting Server #1	10.1.1.150, Port:1813
Advanced	
Allow AAA Override	✓ Enabled
NAC State	Radius NAC

- Configure wireless authentication policies as per the below table

Name		Condition		Protocols		Identity Source
MAB-Auth-Policy_WIRELESS	IF	Wireless_MAB AND Device:Device Type = Device Type#All	allow protocols	MAB	and use	Internal Endpoints

Name		Condition		Protocols		Identity Source
		Device Types#WLC				
Dot1X-Auth-Policy_WIRELESS	IF	Wireless_802_1X AND Device:Device Type = Device Type#All Device Types#WLC	allow protocols	PEAP_MSCHAPv2	and use	AD_LOCAL

- Re-Configure Authorization profile for employees as per the below table.

Authorization Profile	
Name	EMPLOYEE_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	EMPLOYEE_dACL
VLAN	40
AIRSPACE ACL NAME	EMPLOYEE_dACL

- Configure the appropriate ACL on the WLC for the employee policy from ISE to be applied.
- Contractors should be given access through wireless. The session should be re-authenticated every 2 hours. Create a new Authorization profile and policy as per the below tables. Machine access restrictions should not apply when contractors connect through the wireless.
- Configure Authorization profile for wireless contractors as per the below table.

Authorization Profile	
Name	CONTRACTORS_WLC_AP

Access Type	ACCESS_ACCEPT
Common Tasks	
VLAN	50
AIRSPACE ACL NAME	CONTRACTORS_dACL
Advanced RADIUS Attribute Settings	
Radius: Session-Timeout and Termination-Action	2 hours / Radius-Request

- Configure Authorization policy for contractors as per the below table. Make sure you place this policy in the table below the wired policy of contractors.

Name		Identity Group		Conditions		Authorization
IPEXPERT_CONTRACTOR S_Wireless	IF	Any	AND	AD1:ExternalGroups EQUALS ipexpert.com/Users/ IPX _CON AND DEVICE: Device Type EQUALS All Device Types# WLC	THEN	CONTRACTORS_ WLC_AP

- Configure the appropriate ACL on the WLC for the contractor policy from ISE to be applied.
- RDP into TEST-PC1 and configure it for 802.1x.
- Configure anyconnect profiles using NAM profile editor and test wireless 802.1x for employee and contractor WLAN's. Test using "IPXEMP1/cisco" (Employee) or "IPXCON1/cisco" (Contractor) as the login details for 802.1x. Make sure anyconnect always prompts the user for username and password and does not store the credentials.

- For testing purposes you are allowed to configure static routes on the PC. Do not set the default gateway. PC will automatically get the IP address from the pre-configured DHCP server.

Lab-4: Configuring CWA and guest access

Lab-4: Configuring CWA and guest access – This lab is intended to familiarize you with configuring wired and wireless CWA and guest access. You will also configure guest portal, sponsor portal, sponsor group, sponsor group policies and appropriate authentication and authorization policies required for CWA and guest access.

General Rules

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

Estimated Time to Complete: **4 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-3 successfully. Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configuring Wired CWA

- Enable employees and contractors to login through guest web portal on ISE when they do not have supplicant installed on their devices.
- Re-configure wired MAB authentication policy to support wired CWA.
- When users connect to the wired network, they should be automatically placed in VLAN 250 with a restricted dACL being downloaded until they are re-authenticated and re-authorized using CWA.
- Add new authorization policy to support Wired CWA with the appropriate authorization profile.
- Configure a restricted dACL to be downloaded to the unauthenticated users as per the below table

Downloadable ACL	
Name	RESTRICT_dACL
DACL Content	deny ip any host 4.4.4.4 deny ip any host 5.5.5.5 deny ip any 20.4.4.0 0.0.0.255 deny ip any 20.5.5.0 0.0.0.255 deny ip any 192.168.1.0 0.0.0.255 deny ip any 192.168.40.0 0.0.0.255 deny ip any 192.168.50.0 0.0.0.255 deny ip any 192.168.60.0 0.0.0.255 deny tcp any any eq 80 deny tcp any any eq 443 deny ip any host 10.1.1.101 permit ip any any

- Configure a CWA authorization profile as per the below table.

Authorization Profile	
Name	CWA_GUEST_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
VLAN	250
dACL	RESTRICT_dACL
WEB AUTHENTICATION	Centralized/ ACL=REDIRECT

- Configure a new authorization policy to support CWA as per the below table.

Name	Identity Group	Conditions		Authorization
Default	IF no matches	-----	THEN	CWA_GUEST_AP

- Configure the default guest portal on ISE to support CWA and guest access using the identity source sequence created earlier. Enable VLAN DHCP release.
- Configure the switch to support CWA. Generate a new RSA key pair of length 2048. Enable HTTP / HTTPS server and configure the “REDIRECT” ACL.
- You may test this configuration from any test PC.

Task 2: Configuring Guest Access

- Configure ISE to provide guest access for visitors. IPX employees should be able to create guest accounts and act like sponsors. Visitors should also be allowed create their own guest account. After successful authentication and authorization the guest users should be given only Internet access and any traffic destined to the internal network of 192.168.0.0/16 should be dropped. Also configure a VLAN change from the default restricted VLAN 250 to the guest VLAN of 200.
- Create a new Identity group called “Guests” on the ISE
- Configure the guest portal to support self-service and guest must agree the AUP on every login. Map the guest users who use self-service to “Guest” role/identity group. They should be given access for 1 hour from the account creation.
- Sponsor should be authenticated using the identity source sequence created earlier.
- Create a new time profile called “8hours” which provides 8 hours of access from the first login.

- Create sponsor policy as per the below table

Employee Sponsor Group	
General	
Name	EMPLOYEE_SPONSOR_GROUP
Authorization Levels	
Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	No
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	Own Accounts
Suspend/Reinstate Accounts	Own Accounts
Account Start Time	1 day
Maximum Duration of Account	1 day
Guest Roles	
	Guest
Time Profiles	
Pick:	DefaultStartEnd

	8Hours
--	--------

- When creating guest accounts only the first name, last name, company name and time zone details are mandatory.
- Configure sponsor group policy as per the below table and remove all other pre-defined policies. Only IPX_EMP group can create guest accounts.

Rule Name	Identity Groups	Other Conditions	Sponsor Groups
EMPLOYEE_POLICY	Any	AD1:ExternalGroups EQUALS ipexpert.com/Users/IPX_EMP	EMPLOYEE_SPONSOR_GROUP

- Configure dACL and Authorization policies for the guest account and map it to the appropriate Guest identity group in the authorization policy.
- Create a dACL as per the below table.

Downloadable ACL	
Name	GUEST_dACL
DACL Content	deny ip any 192.168.0.0 0.0.255.255 permit ip any any

- Create a guest authorization profile as per the below table

Authorization Profile	
Name	GUEST_AP
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	GUEST_dACL
VLAN	250

Advanced Attribute Settings	
Idle-Timeout	30 minutes
Radius: Termination-Action	Default / 0 (Terminate)

- Create a the guest authorization policy as per the below table

Name		Identity Group		Conditions		Authorization
GUEST	IF	Guest	AND	-----	THEN	GUEST_AP

Task 3: Configuring Wireless Guest Access and CWA

- Configure ISE and WLC to provide guest access and CWA.
- Configure the WLC with new interfaces and WLAN's on WLC to support guest access. Guest user prior to successful authentication should be placed in restricted VLAN/interface (VLAN 250) on the WLC and after successful authentication should be placed in VLAN 200 i.e. the Guest VLAN/interface on the WLC with the same restrictions used for the wired users.
- Create new interfaces on the WLC as per the below table.

Restrict Interface	
Interface Name	restrict
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	250
IP Address	192.168.250.2
Netmask	255.255.255.0
Gateway	192.168.250.1

Primary DHCP Server	10.1.1.101
Secondary DHCP Server	-
ACL Name	none

Guest Interface	
Interface Name	ipx_guest
Quarantine	(unchecked)
Port Number	1
VLAN Identifier	200
IP Address	192.168.200.2
Netmask	255.255.255.0
Gateway	192.168.200.1
Primary DHCP Server	10.1.1.101
Secondary DHCP Server	-
ACL Name	none

- Create a new WLAN for guests to connect as per the below table.

IPX_GUEST	
Type	WLAN
Profile Name	IPX_GUEST
SSID	IPX_GUEST
Status	✓ Enabled

Radio Policy	All
Interface / Group	ipx_guest
Broadcast SSID	✓ Enabled
Security – Layer 2	
Layer 2 Security	None/MAC-Filtering
Security – Layer 3	
Layer 3 Security	None
Web Policy	(Not checked)
Security – AAA Servers	
Authentication Server #1	10.1.1.150, Port:1812
Accounting Server #1	10.1.1.150, Port:1813
Advanced	
Allow AAA Override	✓ Enabled
NAC State	Radius NAC

- Configure the WLC with appropriate ACL's to support the guest access, CWA and restricted access.
- Re-configure the appropriate authorization profiles to support dACL (Airspace ACL names).
- You may test the configuration from TEST-PC1. Use anyconnect to connect to the network. You are allowed to create new profile for the guest access using NAM profile editor.

Lab-5: Configuring MACSec

Lab-5: Configuring MACsec – This lab is intended to familiarize you with configuring MACSec switch-to-host and MACSec Switch-to-Switch.

General Rules

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

Estimated Time to Complete: **1 hour**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-4 successfully. Use the logical topology drawing – Network Topology 4.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configuring MACSec Switch-Host

- Enable MACSec on the G1/0/2 of SW3 with a MACSec policy of “must-secure”.
- RDP into TEST-PC1 and configure anyconnect NAM to use MACSec with AES-GCM-128 as the encryption algorithm for 802.1x wired connections.
- Re-Configure the employee authorization profile on the ISE to send a MACSec policy of “must-secure” in the RADIUS AV pair.

Task 2: Configuring MACSec Switch-Switch

- Enable MACSec link encryption on the trunk links between SW3 and SW4. Use a manual encryption key of “123456789” with GCM-AES-128 encryption algorithm. ISE should not be used for this task.

Section 5

ACS: Cisco Access Control System 5.3

Lab-1: ACS Basic Setup – This lab is intended to familiarize you with the basic configuration of the ACS. The VM appliance of ACS has already been initialized. The focus is to modify basic parameters and configure basic features on ACS. The basic feature cover setting the NTP server, routing, AD integration, Identity source sequence NDG setup, user and NDG schema modification, user and identity group configuration, custom attribute modification, TACACS+ general settings, modifying access policies and SSP. The focus of section 5/ACS is primarily related to AAA device administration. It also has few network access AAA tasks like Cut-through proxy and Authentication-proxy. However, generally it is recommended to configure any network access AAA policies using ISE.

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

General Rules

- It is recommended to use internet explorer version 9 browser or IE-9 compatible mode (Developers tool option) when you access the GUI of the ACS.
- Understand the physical and logical topologies.
- Try to diagram out the task - draw your own connections the way you prefer to diagram.
- Create a checklist to aid as you work through the lab.
- Perform a very close read of the tasks to ensure you do not miss details.
- Take your time - this is not a Mock Lab, so no time constraints are in place for finishing this particular section.
- Practice this section multiple times to improve on your speed and accuracy.
- Make it a common practice to verify the pre-configurations loaded on the devices.

Estimated Time to Complete: **3 Hours**

Pre-setup

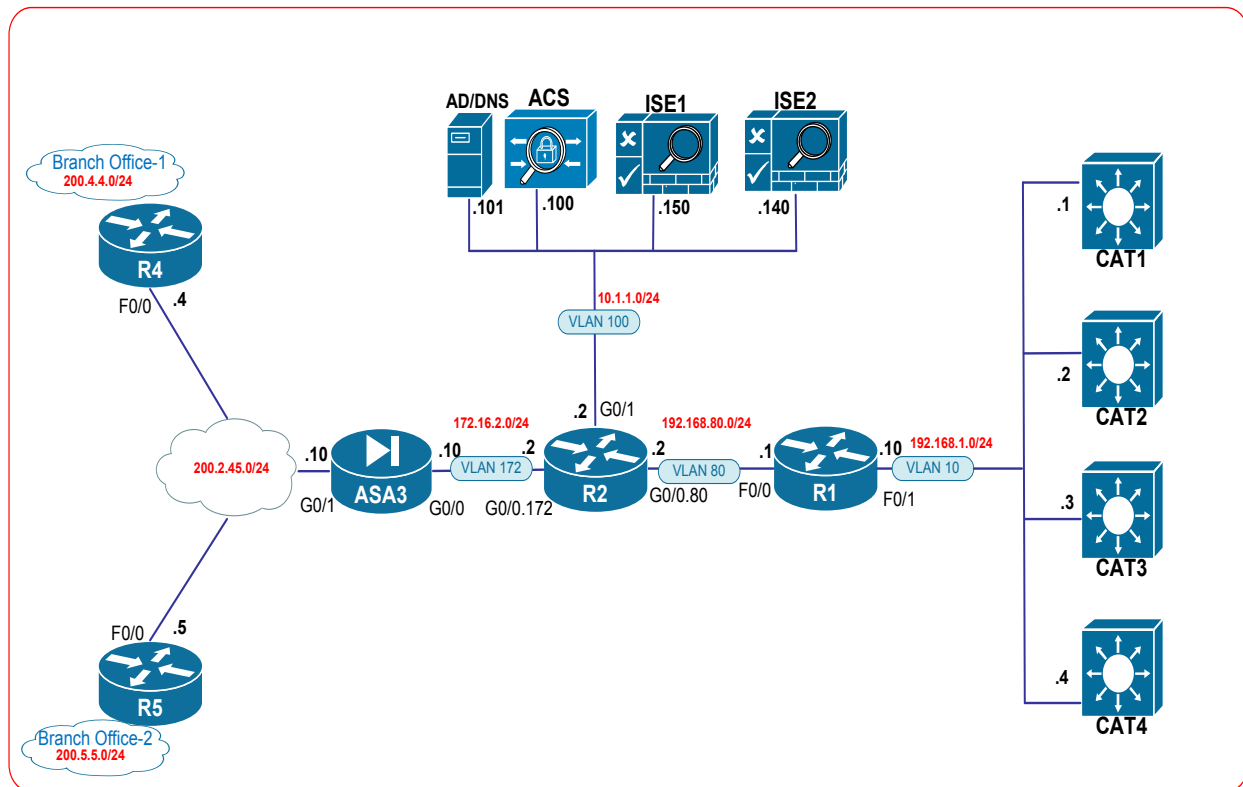
Load the initial configurations for the ASA, routers and switches. Note that ASA, routers and switches are pre-configured with these initial configurations.

NOTE: *Do not make additional configuration on the routers, unless explicitly stated in the task; some switching and firewall configuration must be performed as per the task requirements.*

Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Network Topology 5.1 (Logical)



Lab 1: Configuration Tasks

Task 1: Basic Setup of ACS

- Configure appropriate VLAN's on the switch for ACS as per topology diagram 5.1.
- SSH into ACS CLI from R2 use the credentials of admin/IPexpert123. Configure AD as the NTP server and make sure that the clock and time zone match the AD.
- Add a static route for 192.168.0.0/16, 172.16.2.0/24 and 200.2.45.0/24 with R2 as the next-hop on the ACS.
- Configure AD server as the repository using FTP protocol. The repository name should be "AD_FTP". The URL should be configured as <ftp.ipexpert.com>. Use "administrator/IPexpert123" for the ftp login.
- Use "show application status acs" in the CLI and make sure all processes are running before you login to the GUI of the ACS.
- Integrate ACS with active directory. The AD domain name should be ipexpert.com. Use "administrator/IPexpert123" to join the domain.
- Enable Password Change, Enable Machine Authentication and Enable Machine Access Restrictions for AD connection settings.
- Retrieve "NetworkAdmin", "RouterAdmin", "SwitchAdmin", "FirewallAdmin" and "Operator" groups from the AD.
- Configure Identity Source sequence called "LOCAL_AD" such that users are authenticated with the Local User database and the ACS retrieves additional information/attributes about that user from the AD.
- Create a new user with the credentials of helpdesk/IPexpert123 for ACS GUI administration. Assign this user to a pre-defined group of "ReadOnlyAdmin" which has read only access to the ACS GUI.
- Configure TACACS+ general settings such that the username and password prompt is changed to the below:
 - "Enter your User-ID:"
 - "Enter your Password:"
- Change the user schema to support a new field/attribute called "PrivilegeLevel" whose value (Integer) should be between 1 to 15. The default value should be 1.
- Add another user attribute called "RadiusShellAttribute". The value should return a string. Do not configure any default value.
- Rename the AD1:ExternalGroups condition to a simple name of "ADGroup"
- Create a new NDG called Vendor. Under the Vendor hierarchy add two more NDG's – "CiscoDevice" and "NonCiscoDevice"
- Create a new NDG under the existing Location hierarchy called "HQ" and "BranchOffice"
- Create a new NDG under the existing Device Type hierarchy called "Switch" "Router" and "Firewall"
- Configure AAA clients on the ACS as per the below table. All AAA clients should use a shared key of "cisco123"

SW1-192.168.1.1-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
SW2-192.168.1.2-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
SW3-192.168.1.3-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
SW4-192.168.1.4-RADIUS	NDG-Device Type-Switch NDG-Location-HQ NDG-Vendor-CiscoDevice
R1-192.168.1.10-TACACS+	NDG-Device Type-Router NDG-Location-HQ NDG-Vendor-CiscoDevice
R2-10.1.1.2-TACACS+	NDG-Device Type-Router NDG-Location-HQ NDG-Vendor-CiscoDevice
R4-200.2.45.4-TACACS+	NDG-Device Type-Router NDG-Location-BranchOffice NDG-Vendor-CiscoDevice
R5-200.2.45.5-RADIUS	NDG-Device Type-Router NDG-Location- BranchOffice NDG-Vendor-CiscoDevice
ASA3-172.16.2.10-RADIUS and TACACS+	NDG-Device Type-Firewall NDG-Location- HQ NDG-Vendor-CiscoDevice

- Configure local User's and User Identity group as per the below table. All passwords should be set to "cisco". Set enable password of "cisco" only for "FWadmin" and "NetAdmin" user. These users are preconfigured on the AD and mapped to certain AD groups, which you have retrieved when you joined the ACS to the AD domain.

USER	IDENTITY GROUP	PrivilegeLevel	RadiusShellAttribute
Radmin1	RAdmin	15	---
Radmin2	RAdmin	7	---
SWAdmin1	SWAdmin	15	shell:priv-lvl=15

SWAdmin2	SWAdmin	7	shell:priv-lvl=7
FWAdmin	FWAdmin	--	---
NetAdmin	NetAdmin	15	shell:priv-lvl=15
NetOps	Ops	1	shell:priv-lvl=1
SecOps	Ops	15	---
AOps	Ops	15	---

- Rename the existing access services. Change “Default Device Admin” to “TACACS+ Device Admin” and “Default Network Access” to “RADIUS Network Access”. Remove any descriptions.
- Configure a new access service called “RADIUS Device Admin” the access type should be network access in the policy structure. Allowed protocol should be PAP/ASCII.
- Create a Service Selection Policy (SSP) rule to match IETF RADIUS attributes related to RADIUS device administration and map those conditions/rules to “RADIUS Device Admin” access service.
- Make sure you re-order the SSP rules accordingly.

Lab-2: Configuring AAA clients for authentication and EXEC authorization

Lab-2: Configuring AAA clients for authentication and EXEC authorization – This lab is intended to familiarize you with configuring AAA clients for authentication and EXEC authorization using privilege levels and role based CLI.

General Rules

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

Estimated Time to Complete: **4 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully. Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure Switches (SW1 to SW4) for authentication and EXEC authorization.

- Configure a enable password of “ipexpert”
- Configure a domain name of ipexpert.com and generate RSA keys for SSH.
- Create a local username and password of Sadmin1/cisco and NetAdmin/cisco. Assign a privilege level of 15 to these users.
- Create a local username and password of Sadmin2/cisco. Assign a privilege level of 7 to this user.
- Create a local username and password of NetOps/cisco. Assign a privilege level of 1 to this user.
- Change the privilege level of the below commands to level 7.
 - Show running-config
 - Configure terminal
 - Vlan
 - ip routing
 - ip route
- Add ACS as the RADIUS AAA server. It should process RADIUS VSA's and send attribute 6, 8 and 25 in the request packet.
- Configure AAA authentication and exec authorization for the VTY lines and HTTP. Make sure console is not affected with this configuration. Do not use the default list.
- If the RADIUS server is not reachable then AAA should fallback to the local database.
- Limit the VTY lines to SSH only version 2.
- Configure the switches (SW3 and SW4) with a AAA login banner of “Unauthorized Access Prohibited”
- Configure the switches (SW3 and SW4) to display “Failed login. Try again” for any login failures
- Configure switches such that the username and password prompt is changed to the below:
 - “Enter your User-ID:”
 - “Enter your Password:”

Task 2: Configure Routers (R1 and R2) for authentication and EXEC authorization.

- Configure a domain name of ipexpert.com and generate RSA key's for SSH
- Create a local username and password of RAdmin1/cisco and NetAdmin/cisco. Assign a privilege level of 15 to these users.
- Create a local username and password of RAdmin2/cisco. Assign a privilege level of 7 to this user.
- Create a local username and password of NetOps/cisco. Assign a privilege level of 1 to this user.
- Change the privilege level of the below commands to level 7.
 - Show running-config
 - Configure terminal

- ip cef
- mpls label protocol
- mpls router-id
- vrf definition and all its sub commands
- ip route
- router and all its sub commands
- interface and all its sub commands
- Add ACS as the TACACS+ AAA server. Configure the appropriate source interface for TACACS+ packets.
- Configure AAA authentication and exec authorization for the VTY lines and HTTP. Make sure console and aux is not authenticated. Do not use the default list.
- If the ACS is not reachable then AAA should fallback to the local database.

Task 3: Configure R4 for Role Based CLI

- Configure a enable secret of "ipexpert"
- Create a local username and password of NetAdmin/cisco.
- Create a local username and password of NetOps/cisco, SecOps/cisco and AOps/cisco
- NetAdmin should be assigned to root view and should be given access to all commands
- NetOps should be assigned to NetOps view. The NetOps view should have a password of "netops". This view should be able to view all show commands, ping, telnet, SSH and static routes and configure any dynamic routing protocols
- SecOps should be assigned to SecOps view. The SecOps view should have a password of "secops". This view should be able to view all show crypto commands, ping, telnet, SSH and configure any crypto commands in the global config mode. Make sure NetOps view does not have access to any show crypto commands.
- Configure a superview called AOps, which includes SecOps and NetOps view. The view password should be "aops".
- Configure a Static Object NAT for the ACS on ASA3. Translate ACS to 200.2.45.100.
- Configure appropriate ACL's on ASA3 for communication between R5 and ACS.
- Add ACS as the TACACS+ AAA server. Configure F0/0 as the source interface for TACACS+ packets.
- Configure AAA authentication and exec authorization for the VTY lines. Make sure console and AUX lines are not authenticated. Do not use the default list.
- If the ACS is not reachable then AAA should fallback to the local database.

Task 4: Configure R5 for Role Based CLI

- Do not configure enable password or secret. The root view should use a password of "cisco". You are allowed to modify the ACS server for switching to the root view.
- Create a local username and password of NetAdmin/cisco.
- Create a local username and password of NetOps/cisco, SecOps/cisco and AOps/cisco
- NetAdmin should be assigned to root view and should be given access to all commands

- NetOps should be assigned to NetOps view. The NetOps view should have a password of “netops”. This view should be able to view all show commands, ping, telnet, SSH and static routes configure routing protocols
- SecOps should be assigned to SecOps view. The SecOps view should have a password of “secops”. This view should be able to view all show crypto commands, ping, telnet, SSH and configure any crypto commands in the global config mode. Make sure NetOps view does not have access to any show crypto commands.
- Configure a superview called AOps, which includes SecOps and NetOps view. The view password should be “aops”.
- Configure appropriate ACL’s on ASA3 for communication between R5 and ACS.
- Add ACS as the RADIUS AAA server. Configure F0/0 as the source interface for RADIUS packets.
- Configure AAA authentication and exec authorization for the VTY lines. Make sure console and AUX lines are not authenticated after switching to the root view. Do not use the default list.
- If the ACS is not reachable then AAA should fallback to the local database.
- Configure R5 such that the username and password prompt is changed to the below
 - “Enter your User-ID:”
 - “Enter your Password:”
- Configure the R5 to display “Failed login. Try again” for any login failures

Task 5: Configure ASA for authentication

- Configure an enable password of “ipexpert” on ASA3. Configure a domain name of ipexpert.com
- Configure a local username and password of “FWadmin/cisco”. Set the service type to admin.
- Configure ASA3 to authenticate all logins to console, telnet, SSH and ASDM sessions using the ACS. If the ACS is unavailable then the ASA should use its local database.
- Configure enable authentication using the ACS and should fall back to the local database if ACS is not reachable/down.
- EXEC authorization should be done using the ACS.
- Only allow management from anyone on the inside interface.

Task 6: Configure ACS for EXEC authorization TACACS+ Device Admin access service for routers

- Change the authentication method to “LOCAL_AD” identity sequence for “TACACS+ Device Admin” access service.
- Create a Shell Profile called “TACACS+ShellProfile”. Configure the default privilege level in this profile to use a dynamic value. The value for that attribute should be dynamically derived from the user attribute called “PrivilegeLevel”. This attribute is present in the internal user store.

- Radmin1 user should be given complete access to any router in the HQ. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of RouterAdmin.
- Radmin2 user should be given access to routers in the HQ for all commands at privilege-level 7 and below. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of RouterAdmin.
- Configure only one authorization rule to reflect the above policy requirement.
- Policy conditions should include date and time, NDG location, NDG Device type, Identity Group and ADGroup.
- Re-configure the default rule with DenyAccess shell profile.

Task 7: Configure ACS for authorization rules in TACACS+ Device Admin access service for ASA

- Create a Shell Profile called “FWShellProfile” configure the privilege level to 15.
- Add another authorization rule for accessing the ASA in TACACS+ Device Admin access policy.
- Only users from FWAdmin group should be given access to the ASA. Policy should include local identity group as one of the condition and also check if users belong to an AD group of FirewallAdmin. Use “FWShellProfile” as the authorization result.

Task 8: Configure ACS for EXEC authorization RADIUS Device Admin access service for switches

- Change the authentication method to “LOCAL_AD” identity sequence for “RADIUS Device Admin” access service.
- Create a new authorization profile called “UserShell” to send Cisco-AV pair to assign a user to the appropriate shell privilege. The value for that attribute should be dynamically derived from the user attribute called “RadiusShellAttribute”. This attribute is present in the internal user store.
- SWAdmin1 user should be given complete access to switches in the HQ for commands at privilege-level 15 and below. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of SwitchAdmin.
- SWAdmin2 user should be given access to switches in the HQ for all commands at privilege-level 7 and below. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of SwitchAdmin.
- Policy conditions should include date and time, NDG location, NDG Device type, Identity Group and ADGroup.
- Configure only one authorization rule to reflect the above policy requirement.
- Re-configure the default policy result to “DenyAccess”.

Task 9: Advanced authorization rules for RADIUS and TACACS+ Device Admin access policies.

- NetAdmin user should be given complete access to any device in the network.
- Create a new Shellprofile called "NetAdmin" Assign a TACACS+ custom attribute used for role base CLI view of "root". Assign the appropriate privilege level for this user.
- Create a new authorization profile called "NetAdmin" and configure the appropriate RADIUS A/V pairs.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for NetAdmin user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of NetworkAdmin.
- NetOps user should not be able to make any configuration changes for devices in the HQ. This user can only execute privilege level 1 commands for any devices in the HQ except ASA3. This user should be able to login to branch routers with a view of "NetOps".
- Create a new Shellprofile called "NetOps" Assign a TACACS+ custom attribute used for role base CLI view of "NetOps". Assign the appropriate privilege level for this user.
- Create a new authorization profile called "NetOps" and configure the appropriate RADIUS A/V pairs.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for NetOps user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of Operator.
- SecOps user can only access branch routers.
- Create a new Shellprofile called "SecOps" Assign a TACACS+ custom attribute used for role base CLI view of "SecOps".
- Create a new authorization profile called "SecOps" and configure the appropriate RADIUS A/V pair.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for SecOps user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of Operator.
- AOps user can only access branch routers.
- Create a new Shellprofile called "AOps" Assign a TACACS+ custom attribute used for role base CLI view of "AOps".
- Create a new authorization profile called "AOps" and configure the appropriate RADIUS A/V pair.
- Create the appropriate authorization rules in the RADIUS and TACACS+ Device Admin access policy for AOps user. Policy should include local identity group as one of the condition and also check if this belongs to an AD group of Operator.
- All Ops/operator users should be able to login to the network only during weekdays between 8 AM to 6 PM. Limit maximum number of sessions to 1 for Ops/Operator group
- You are allowed to add extra condition of username in the authorization rules to accomplish task 9.

Lab-3: Configuring AAA clients for command authorization and accounting

Lab-3: Configuring AAA clients for command authorization and accounting – This lab is intended to familiarize you with configuring AAA clients for command authorization using the ACS and EXEC/command accounting.

General Rules

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

Estimated Time to Complete: **3 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-2 successfully. Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Configure R1 and R2 for command authorization.

- Configure R1 and R2 for command authorization for all commands when a user connects via telnet or SSH. Configure appropriate fallback policy.
- Configure such that only privilege level 15 commands should to be authorized for HTTP sessions using the ACS on R1 and R2.

Task 2: Configure ACS for command authorization.

- Add a Command Sets as additional result in the TACACS+ Device Admin access policy in the authorization rules.
- Configure a command set call “PermitALLCMD” and permit all the commands for Radmin1 user. You are allowed to modify or change the authorization rules.
- Configure a command set called “Priv7CMD” and permit commands given in the below table for Radmin2 user. Create additional authorization rule for this.

Command	Argument
show	running-config
configure	terminal
ip	cef
mpls	(ANY)
vrf	definition
ip	route
router	(ANY)
network	(ANY)
interface	(ANY)
ip	address
no	(ANY)
exit	(ANY)
ping	(ANY)
telnet	(ANY)
ssh	(ANY)

- NetAdmin user should be assigned “PermitALLCMD” command set.
- NetOps user should be able to view only basic show commands available at privilege level 1 and be able to exit/log-off. You are allowed to create a new command set to accomplish this and modify existing authorization rule. You may also need to make some additional configuration change on R1 and R2 for NetOps user to execute show commands.

Task 3: Configure ASA and ACS for command authorization.

- Configure command authorization on the ACS. Before you configure this make sure you SSH into ACS as FWadmin user.
- Modify or change existing authorization rule such that FWadmin user can get complete access to the ASA.
- Configure additional authorization rule such that SecOps is allowed to execute all commands except reload. You are allowed to create new shell profile and command set. The authorization profile should have NDG's (Location and Device Type), identity group, AD group and username as conditions. Do not enforce date and time condition for this rule.

Task 4: Configure EXEC Accounting.

- Configure all devices to log telnet/SSH sessions to the ACS.

Task 5: Configure R1 and R2 for command Accounting.

- Configure R1 and R2 for accounting all command executed by the user when they have logged in through telnet or SSH.
- Account only privilege level 15 commands when executed through HTTP on R1 and R2.
- Configure command account on the ASA.

Task 6: AAA configuration removal on ASA

- Remove any existing AAA configs on ASA3. Execute "clear config aaa" and save the configs.

Lab-4: Configuring Authentication proxy and cut-through proxy

Lab-4: Configuring Authentication proxy and cut-through proxy– This lab is intended to familiarize you with the configuration of IOS Authentication Proxy and ASA's Cut through proxy to implement AAA network access.

General Rules

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

Estimated Time to Complete: **2 Hours**

Pre-setup

This lab is built on the previous lab. Ensure you have completed Lab-1 successfully. Use the logical topology drawing – Network Topology 5.1 and refer to the general physical connectivity.

This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below.

Task 1: Remove AAA configuration.

- Remove AAA configurations on R1.

Task 2: ASA Cut through proxy using RADIUS

- Configure ASA as a RADIUS client.
- Configure ASA for cut-through proxy authentication using dACL's for any inbound HTTP and RDP connections and configure cut-through-proxy accounting.
- Use a virtual telnet IP address of 200.2.45.23
- Configure the ASA and the ACS accordingly. Use "RADIUS Network Access" access service on the ACS. Test using any user. You are allowed to modify the VLAN's on the switch for the test PC. Do not set the default gateway on the test PC.

Task 3: IOS Authentication proxy using RADIUS

- Re-configure R1 as a radius client on the ACS. R1 should source the RADIUS packets from 192.168.80.1 (F0/0) interface. The key should be cisco123.
- Configure R1 as the RADIUS client. R1 should process RADIUS VSA's and include attribute 6 in the RADIUS request packet.
- Configure Authentication proxy such that a user needs to be authenticated, authorized and accounted before they are allowed any outbound access on TCP ports 23,80,8080 and for ICMP packets.
- Apply the Authentication proxy on F0/1 interface. R1 should directly authenticate any TCP 80 and 23 packets.
- Configure the ACS with appropriate authorization profile using cisco A/V pair's and authorization policy rule. Use "RADIUS Network Access" access service.
- Test using any user. Make sure that the default policy of RADIUS Network Access service has a DenyAccess. You are allowed to modify the VLAN's on the switch for the test PC. Do not set the default gateway on the test PC.

Section 6

IPS: Intrusion Prevention System

Section 6: Cisco IPS is intended to let you be familiar with the IPS technologies that are available on IPS appliance and the IOS software. You will be configuring basic initialization, various deployment modes, virtual sensor creation, signature tuning, anomaly detection, even action rules some advanced features related to those technologies.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

General Rules

- This lab will focus strictly on the Cisco IPS. You will need to pre-configure the network with the base configuration files

NOTE: Static/default routes are NOT allowed unless otherwise stated in the task

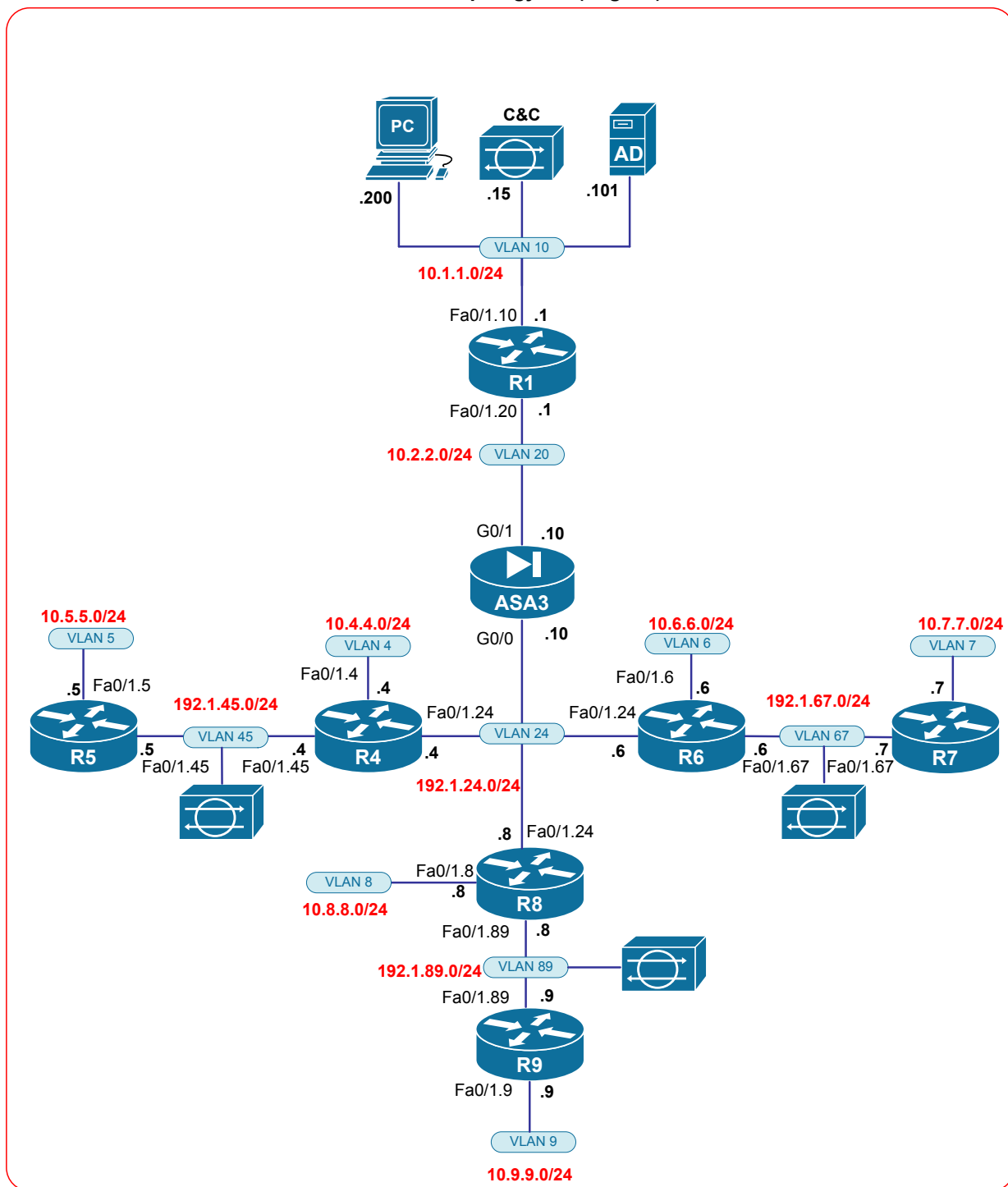
Estimated Time to Complete: **7 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R1	Fa0/1.10	10	10.1.1.1/24
	Fa0/1.20	20	10.2.2.1/24
	Loopback0	-	1.1.1.1/24
R4	Fa0/1.4	4	10.4.4.4/24
	Fa0/1.24	24	192.1.24.4/24
	Fa0/1.45	45	192.1.45.4/24
	Loopback0	-	4.4.4.4/24
R5	Fa0/1.5	5	10.5.5.5/24
	Fa0/1.45	45	192.1.45.5/24
	Loopback0	-	5.5.5.5/24
R6	Fa0/1.6	6	10.6.6.6/24
	Fa0/1.24	24	192.1.24.6/24
	Fa0/1.67	67	192.1.67.6/24
	Loopback0	-	6.6.6.6/24
R7	Fa0/1.7	7	10.7.7.7/24
	Fa0/1.67	67	192.1.67.7/24
	Loopback0	-	7.7.7.7/24
R8	Fa0/1.8	8	10.8.8.8/24
	Fa0/1.89	89	192.1.89.8/24
	Fa0/1/24	24	192.1.24.8/24
	Loopback0	-	8.8.8.8/24
R9	Fa0/1.9	9	10.9.9.9/24
	Fa0/1.89	89	192.1.89.9/24
	Loopback0	-	9.9.9.9/24
ASA's (ASA3 & 4)	G0/0 (outside)	24	192.1.24.10/24
	G0/1 (inside)	20	10.2.2.10/24
IPS	C&C	10	10.1.1.15/24

Network Topology 6.1 (Logical)



Lab 6: Cisco IPS

Task 1: Sensor Setup and Administration

- Before you begin erase the current configuration on the sensor using “erase current-config”.
- From the console, configure the hostname as “IPS” and the command-and-control interface of the sensor with an IP address of 10.1.1.15/24 and a default gateway of 10.1.1.1
- Configure the sensor to listen for HTTPS requests on port 10443 instead of the default of 443.
- From this point on, you may use either the command-line or IDS Device Manager (IDM) to configure the sensor. Note that IDM is specifically mentioned in the Blueprint, so you should be familiar with its use.

Task 2: Password Protection

- Your corporate security policy states that all passwords must be at least 10 characters in length, and must contain at least one uppercase letter, one non-alphanumeric character (such as # or \$), and at least two numbers. The previous 2 passwords should also be remembered. Configure the sensor to enforce this policy.
- Your corporate security policy requires that accounts be locked after 5 invalid login attempts. Configure the sensor to implement this requirement.
- The operations team needs read-only access to the sensor to view events. Create a new user for their use called “nocadmin” with password “NOCread123#”.

Task 3: Network Time Protocol

- Configure R1 to act as an NTP master.
- Set the time zone to EST (GMT -5) and account for daylight saving
- Configure NTP authentication with MD5 key #1 and value “ipexpert”
- Configure the sensor to sync its clock to R1 using NTP

Task 4: Miscellaneous Configuration

- Although telnet is an inherently insecure protocol, the NOC requires it to be enabled for management purposes. The NOC will connect to the sensor from R1. Configure the sensor to allow this.
- Configure the sensor to allow SNMP management using the read-only community string “IPSro” and the read-write community string “IPSrw”. Set the system location to “IPexpert HQ” and the system contact to IPS@ipexpert.com. Traps should also be enabled to the ACS Server using read only community.

- When users log into the sensor, they should see a login banner indicating that access is restricted to authorized personnel only.

Task 5: Creating Virtual Sensors

- Create a new virtual sensor, vs1
- Set the description to “Inline Pair IPS monitoring for R6 and R7”
- Create new policy objects for vs1, sig1, rules1, and ad1. These should be exact copies of the policy objects in vs0.
- Create a new virtual sensor, vs2
- Set the description to “VLAN Pair IPS monitoring for R8 and R9”
- Create new policy objects for vs2, sig2, rules2, and ad2. These should be exact copies of the policy objects in vs0

Task 6: Monitoring Traffic with IDS

- Configure switches to copy all traffic between VLAN 4 and VLAN 5 to the Gi0/0 interface on the IPS sensor. If required, you may create VLAN 450 to complete this task.
- The sensor should be able to send TCP resets to VLAN 45.
- Configure interface Gi0/0 on the sensor to monitor traffic in promiscuous mode
- Add this interface to virtual sensor to vs0.
- Set the description to “IDS monitoring for R4 and R5”
- Enable the IP Echo Request and IP Echo Reply signatures under the default Signature Definition Policy.
- Tune the above two signatures so that they produce a medium-severity alert.
- Verify that pings between R4 & R 5 generate events. Also generate alerts with a severity of high fragmented ICMP packets.

Task 7: IPS Inline Interface Pair

- Create a new inline interface on the sensor called INLINE67.
- Set the description to “R6 and R7 Monitoring Interface”.
- Add the ge0/1 and ge0/2 interfaces.
- R7 should belong to VLAN 670.
- Add the new interface to virtual sensor vs1.
- Verify that you can ping from R6 to R7.
- Verify that pings between R6 & R7 generate events. Also generate alerts with a severity of high fragmented ICMP packets.

Task 8: IPS Inline VLAN Pair

- Configure the port on Cat4 connecting to the sensor’s ge0/3 interface to be a dot1q trunk.
- Configure this trunk port to only permit VLANs 89 and 890.

- Create a new sub-interface on the sensor's ge0/3 interface. Use sub-interface #89.
- Set the description to "R8 and R9 Monitoring Interface".
- Add the new interface to virtual sensor vs2.
- Verify that you can ping from R8 to R9.
- Verify that pings between R8 & R9 generate events. Also generate alerts with a severity of high fragmented ICMP packets.

Task 9: Tuning Signatures, Variables and Custom Signatures

- For each of the Virtual Sensors make sure that the networks behind the ASA are viewed with the highest priority.
- In the previous sections you tuned the signatures for ICMP Pings. For traffic between VLAN 6 and VLAN 7, tune the Echo Request signature to generate a high-severity event, and for Echo Replies to not generate an event at all.
- Configure an existing signature that will fire a high severity alert when ICMP packets with a size of between 8000-50000 bytes, are detected between R8 & R9. Drop the packet inline. The alert should fire every 4th event, and be summarized every 5th event.
- Configure the sensor to block traffic between R7 and R8 if it detects the Code Red Worm traffic hitting a web server on VLAN 8. For the purpose of this task, consider URLs containing any of the following, to be Code Red traffic: "cmd.exe" "default.ida" or "root.exe". This task should account for the URL's using any case. Send an SNMP trap when this event is generated.
- Configure the sensor to alert when it detects a file being deleted on the FTP server at 10.4.4.100 from Vlan 5. A low-priority IPS event should also be logged.
- A custom TCP application is running in Vlan 5 on port 40004. This application should only be accessed from Vlan 7. An SNMP trap should be sent to the ACS Server in Vlan 10 if this traffic is detected being sourced from any other location. Standard severity and Risk Ratings should be used. Do not use IP or IP ranges for defining Vlan 7 when configuring this task.
- Configure a custom stream signature for VS1 called "CustTCPstring1" to detect traffic that contains the word "ccna" (Case-insensitive). The traffic must be destined to TCP port 23 or TCP port 3001. IPS should produce an alert only. The signature should change to summary alert if the alert fires more than 4 times in 40 seconds for the same attacker. The signature should trigger a global summary if it fires more than 10 times.

- Configure a custom signature for VS1 called “AtomicIP2” to detect telnet traffic. The telnet traffic must have a source IP of 10.7.7.7 and destination IP of 10.8.8.8. IPS should drop the connection and produce an alert. The signature should fire every time with severity of High.
- Configure a custom signature for VS2 called “TCPFLAGFILTER” to detect TCP traffic which has the SYN flag set and the ACK flag not set. IPS should produce verbose alert. Change the event count key and summary key to attacker and victim address and the alert type as fire all. Do not use dynamic summarization.
- Configure a custom signature for VS1 called “CustHTTPsig1” to detect HTTP traffic which has “facebook” anywhere in the URI. IPS should deny packets inline and produce alerts with high severity.
- Configuring a custom signature to deny ARP packets with a broadcast address in the Source IP field. Apply this to VS2 and change the alert severity to high. The custom signature should have a name of CustomARP.
- Configure a custom signature for VS2 called “CustomAICsig” to detect HTTP traffic based on AIC engine which has max-outstanding-request of 10. IPS should deny packets inline and produce alerts with high severity.

Task 10: Advanced IPS and Anomaly Detection

- Due to potential asymmetric traffic flows for VLAN 5 disable AD for Sensor vs0, and set the Normalizer mode accordingly.
- AD for Virtual Sensor 2 should be set to learning mode, the learning period should be 72hrs. The learning action should be so that after the learning period the new Knowledge Base is saved and loaded, replacing the initial KB.
- Ensure that Vlan 6 and 8 are seen as the Internal networks in their respective AD policies.
- You have some unallocated dark ip that will eventually be reachable via R6, 10.16.16.0/24, 10.66.66.0/24 & 10.166.166.0/24, these subnets should not be present in any traffic flows and should be handled accordingly. The scanner thresholds should be reduced to 100 for both TCP and UDP.
- In vs1 restrict the OS fingerprinting to the 10.0.0.0/8 network. Add two mappings one for the ACS server, so it is always seen as type WinNT, and one for a Linux Server called RedHat1 with an ip of 10.7.7.100.

Task 11: Blocking using the Security Appliance.

- A host on VLAN 5 is carrying out an access attack on R1 using telnet with a username of “Admin”.
- Make sure this attack is detected as high severity, and the triggered event contains as much information as possible.
- When the event is triggered the IPS should connect to the ASA using SSH and perform a shun.

- Use the ASA local database for authentication with user "IPS_Admin" and password "ipexpert". Enable password should also be "ipexpert".

Task 12: Blocking using IOS Devices

- FTP & HTTP traffic is required to be inspected on vs1.
- If malicious traffic is tunneled through HTTP from Vlan 4 to Vlan 7 a block should be placed on R6's f0/1.24 interface, and all the traffic should be logged.
- Use SSH to connect to R6 from the IPS
- R6 should have a local user "R6Admin" with password "ipexpert".

Task 13: Rate Limiting

- An ICMP Flood is being generated by multiple hosts on Vlan 6 destined for Vlan 9.
- Tune an existing signature in vs2 to place a rate limit on R8's F0/1.24 interface.
- Login to R8 using Telnet and the local user "R8Admin" password "ipexpert".
- The rate limit should be set to 2% when more than 25 pings occur within a 1 second period

Task 14: IOS IPS

- Configure R1 to enable the IPS feature set inbound on vlan 10 and 20 interfaces.
- The IPS v5 signature package is contained in the path: flash:/IOS-Sxxx-CLI.pkg
- Be sure to follow the documented prerequisites.
- Enable only basic signature set
- Once completed enable ICMP Echo Request signature and ensure that the IPS is monitoring successfully

Task 15: IOS IPS Tuning

- Set the event notification method to syslog.
- Create the AD as a mission critical device.
- Configure Sig ID 2150 to drop and alarm on receipt of the fragmented icmp traffic.
- Enable the ICMP Flood category.

Section 7

Virtual Private

Networks

Section 7: Virtual Private Networks is intended to help you master the VPN technologies that are available on IOS and the ASA. You will be configuring Site-to-Site, Remote Access, and Flex VPNs along with some advanced features related to these technologies.

It is recommended that you create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on the Virtual Private Networks. You will need to pre-configure the network with the base configuration files.

NOTE: Static/default routes are NOT allowed unless otherwise stated in a task.

Estimated Time to Complete: **7 Hours**

Pre-setup

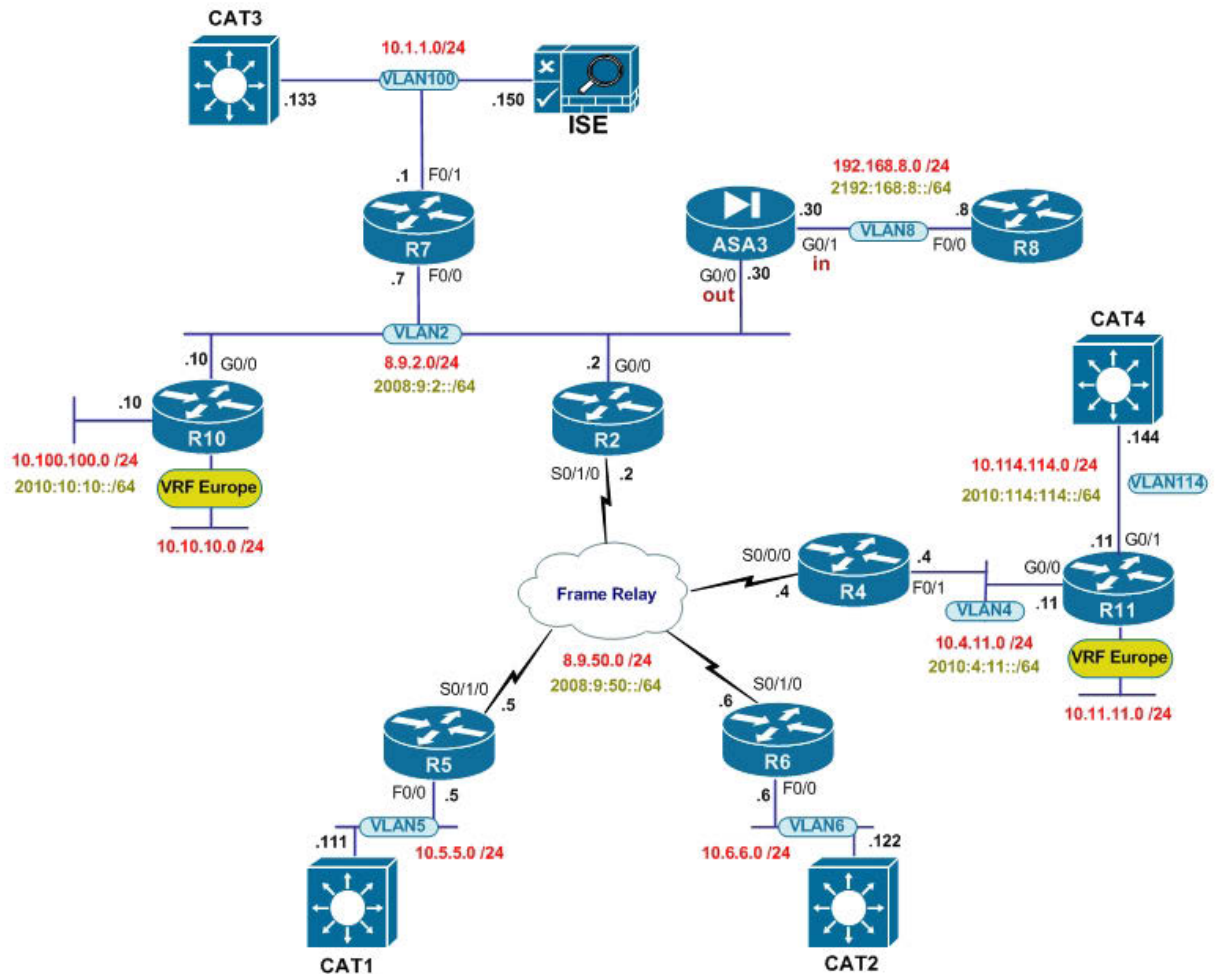
- Please login to your Security vRack at ProctorLabs.com and load the initial conf. files
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram, and the Physical Topology.
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below:

Device	Port	VLAN	IP Address
R2	G0/0	2	8.9.2.2/24 2008:9:2::2/64
	Ser0/1/0		8.9.50.2/24 2008:9:50::2/64
R4	Fa0/1	4	10.4.11.4/24 2010:4:11::4/64
	Ser0/0/0		8.9.50.4/24 2008:9:50::4/64
R5	Fa0/0	5	10.5.5.5/24
	Ser0/1/0		8.9.50.5/24 2008:9:50::5/64
R6	Fa0/0	6	10.6.6.6/24
	Ser0/1/0		8.9.50.6/24 2008:9:50::6/64
R7	Fa0/0	2	8.9.2.7/24
	Fa0/1	100	10.1.1.1/24
R8	F0/0	8	192.168.8.8/24
R10	G0/0	2	8.9.2.10/24 2008:9:2::10/64
R11	G0/0	4	10.4.11.11/24 2010:4:11::11/64
CAT1	VLAN5	5	10.5.5.111/24
CAT2	VLAN6	6	10.6.6.122/24
CAT3	VLAN100	100	10.1.1.133/24
ASA3	G0/0 (outside)	2	8.9.2.30/24

	G0/1 (inside)	8	192.168.8.30/24
ISE	Internal NIC	100	10.1.1.150/24

Security Volume I

Section #7 – Topology 1



Lab-7 Configuration tasks

Task 1: IOS CA Server

- Make R2 start acting as an IOS CA & CDP Server.
- Use key-pair CAKEYS for this purpose.
- Make sure CA keys can be further archived.
- Automatically rollover the Root Certificate 30 days prior to expiration.
- Certificates should be granted automatically.
- CRLs should be obtained through CDP.
- Configure R2 as an NTP Server.
- Synchronize R10 and R11 with the NTP Server.
- R2, R10, and R11 should be in time zone GMT+1.
- Daylight Savings Time (DST) should be enabled.
- Use the domain name of ipexpert.com.

Task 2: IOS – ASA L2L

- Create a VPN Tunnel on ASA3 and R5 protecting all IP traffic between VLANs 8 and 5.
- For Phase I, create an ISAKMP policy 30 on the ASA and use its default values. Use a PSK of “ipexpert”. For Phase II use the 3DES and SHA algorithms.
- On ASA3, ensure that ICMP traffic is not allowed across the tunnel.
- Create an additional loopback 30 on R5. Assign it an IP address of 10.30.30.5/24.
- Add traffic sourced from this newly created loopback into the existing tunnel.
- Give priority treatment to all Telnet packets flowing between VLAN5 and VLAN8 across the VPN tunnel on R5 and restrict this traffic to 200 Kbps. Loopback 30 traffic should not be subject to this policy.
- You are allowed to use two static routes in this task.

Task 3: IPv6 L2L IOS

- Create a site-to-site IPv6 VPN tunnel between R10 and R11.
- Protect communication between the Loopback 100 interfaces.
- Use AES 128 encryption, SHA-1 HMAC, DH group 5, and RSA-SIG for Phase I.
- Use R2 as the CA.
- Use the same encryption and authentication/integrity algorithms for Phase II and also make sure that any further session keys will not be derived based on previous ones.
- You are allowed to configure two static routes in this task.

Task 4: IPv6 VRF-Aware L2L

- Create a site-to-site IPv6 VPN tunnel between R10 and R11.
- Use Pre-Shared Keys for authentication.

- Protect all communication between devices that belong to the VRF “Europe”.
- You are not allowed to configure any static routes in this task.

Task 5: IPSec Remote Access IOS

- Configure R7 as an Easy VPN Server.
- Use 3DES and MD-5 algorithms for both phases.
- Perform local authentication and authorization for remote users. Use the following parameters:
 - Username “ipexpert” with password “ipexpert”
 - Group name “LONDON”
 - Key should be set to “SkyFall”
 - Domain name should be “ipexpert.com”
 - Users should only access VLAN 100 through the tunnel
 - Do not configure any IP address pool
- R7 should see the route to remote clients with a distance of 15.
- Configure R8 as an Easy VPN Client.
- Create Loopback 8 interface (8.8.8.8/24) that will emulate an internal network and client.
- Make sure your credentials are stored on the device so you do not have to type them whenever you connect.
- For configuration of both the client and the server, use a method that allows you to apply additional features for only the tunneled packets.

Task 6: IPSec Remote Access IOS with RADIUS

- Modify the configuration from the previous task.
- Authentication and Group Policy information should now be stored on ISE.
- Use “outofcontrol” as the RADIUS shared secret.
- Connecting users should now get an IP address assigned from the 172.16.70.0/24 range.
- You can add two static routes.
- Re-configure R7 and R8 to meet these requirements.

Task 7: IPSec Remote Access ASA

- Configure ASA3 to accept remote VPN connections.
- Use AES encryption and SHA-1 hashing for both phases.
- Group Policy should be stored locally.
- Use the following parameters for the Group configuration:
 - VPN group name “MIAMI”
 - Key should be set to “MiamiVice”
 - IP address pool should be 172.16.30.30/24
 - DNS Server should be 192.168.8.30
 - VPN connection should be terminated after 10 minutes of inactivity

- Users should only access VLAN 8 through the tunnel
- Make sure user “cisco” (password “cisco”) can only access the “MIAMI” group
- Configure the Cisco VPN Client to test this setup (use PC#1)

Task 8: IPSec Remote Access ASA with RADIUS

- Modify the configuration from the previous task.
- Authentication and Group Policy information should be now stored on ISE.
- Use “outofcontrol” as the RADIUS shared secret.
- User “cisco” should now be always assigned an IP address 172.16.30.100.
- Use password of “cisco1” for this user.
- Other settings/requirements from the previous task still apply.

Task 9: DMVPN Phase I

- Configure DMVPN between R5, R6, and R8.
- R8 should be seen as 8.9.2.8 on VLAN 2 and should act as a hub in this configuration.
- The hub should switch traffic between VLAN 5 and VLAN 6.
- Only one tunnel network is allowed for this task – 172.16.100.0/24.
- Run the EIGRP process to advertise both private networks to the hub. Use AS 100.
- Protect the DMVPN network using IPSec.
- Use AES 192 and SHA-1 for Phase I. Use 3DES and MD5 for Phase II.
- The PSK “cisco” should be used for authentication.

Task 10: DMVPN Phase II

- Migrate the DMVPN configuration from the previous task to Phase II.
- Traffic between VLANs 5 and 6 should be no longer going through the hub.

Task 11: DMVPN Phase III

- Migrate the DMVPN configuration from the previous task to Phase III.
- Enable summarization.
- Routing information should be summarized as efficiently as possible.

Task 12: Redundant GETVPN

- Configure GET VPN between R2, R5, and R6.
- R2 should act as primary KS.
- Protect the ICMP traffic between GMs.
- Use AES 192 and SHA-1 for both phases.
- Use a pre-shared key “ipexpert” for authentication.
- Rekey messages should be sent as multicast to 239.5.5.5.
- Secure the re-key transmission.

- Configure R4 as a redundant KS.

Task 13: SSL Remote Access IOS

- Configure R7 to provide WebVPN connections on the F0/0 interface port 443.
- HTTP connections should be redirected to HTTPS automatically.
- Create user “john” with password “matrix”.
- That user should authenticate in domain “VALVERDE”.
- Remote users should be able to access CAT3 via Telnet using local port 5000.
- Remote users should be able to WWW to CAT3 through a link on the portal page.

Task 14: SSL Remote Access IOS - AnyConnect

- Configure R7 to provide Full Client connections for remote users.
- Create a separate context “ISLAND” - make sure only AnyConnect clients are permitted.
- Use local IP address pool 10.140.140.0/24 for the connecting clients.
- Tunnel only traffic going to VLAN 100.
- Assign the clients the domain-name of “ipexpert.com” and a DNS server of 10.1.1.101.

Task 15: SSL Remote Access ASA

- Configure ASA3 to provide WebVPN connections on the G0/0 interface port 443.
- Create user “mad” with password “max”.
- That user should authenticate to group AUSTRALIA.
- Remote users should be able to access R8’s console using Putty.
- Disable the ability to enter any HTTP/HTTPS URL on the portal page.

Task 16: IPv6 SSL Remote Access ASA - AnyConnect

- Configure ASA3 to provide SSL (AnyConnect) connections on G0/0 interface port 443.
- Initial clientless connection (client download) should be redirected to HTTPs.
- Use a local IPv4 address pool of 10.170.170.0/24.
- The ASA should only allow access to VLAN8.
- User “mad” should authenticate to group “DESERT”.
- For SSL connections use the protocol that avoids latency and bandwidth problems.
- IPv6 access should be also included – use 2192:168:8::0/64 in VLAN8.
- You can add a default route on R8.

BEFORE YOU BEGIN WORKING ON THE REMAINING TASKS:

Unless you started with “fresh” config files, you may want to reload initial configurations on R10, R11, and ASA3. This is so the crypto components from the previous tasks do not interfere with the IKEv2 configuration.

Task 17: IKEv2 L2L IOS ASA

- Configure an IKEv2 L2L VPN between R10 and ASA3.
- Protect traffic between VLAN 8 and 10.100.100.0/24.
- R10 should authenticate using digital certificates. Setup R2 as a CA if needed.
- ASA3 should authenticate using a PSK of "ipexpert".
- AES 256 should be used for AUTH SA along with SHA384 hashing and DH Group 14.
- IKEv2 policy should be bound to G0/0 on R10.
- The AES 128 encryption and SHA-1 integrity algorithms should protect IPSec tunnels.
- The IKE lifetime on ASA3 should be set to 1 hour and 40 minutes.
- PFS should be enabled with a recommended key size.
- DPD Keepalives should be enabled with the interval set to 15 seconds. Retries should be sent every 3 seconds.
- Enable NAT-Traversal Keepalives.
- You are allowed to add two static routes to accomplish this task.

Task 18: IKEv2 Remote Access IPSec ASA (AnyConnect)

- Configure IKEv2 Remote Access IPSec VPN with ASA3.
- AnyConnect should be the client used to test this configuration.
- ASA should authenticate to the client using certificates.
- Clients should authenticate with user "total" and password "recall".
- Use IP pool 10.210.210.0/24.
- The DNS server should be set to 192.168.8.8.
- Clients should only be able to access 192.168.8.0/24 (VLAN 8).

Task 19: IPv6 FlexVPN L2L

- Configure an IKEv2 L2L VPN between R10 and R11.
- Protect IPv6 traffic between 2010:10:10::/64 and 2010:114:114::/64.
- Use Smart Defaults for this configuration.
- R10 should authenticate using PSK "Warsaw".
- R11 should authenticate using PSK "SanFrancisco".
- Devices should be identifying themselves as "R10_ID" (R10) and "R11_ID" (R11).

Task 20: FlexVPN IPSec Remote Access

- Configure R11 as a FlexVPN Server and R10 as a FlexVPN Client.
- You can use Smart Defaults and/or policies from the previous task.
- Use PSK "AncientPersia" for authentication.
- Devices should identify each other using their FQDNs.
- Group Policy on R11 should be stored locally.
- Only access to VLAN 114 should be granted.
- Use the IP pool 10.190.190.0/24.
- R11 should see client-assigned IP addresses with AD set to 3 and a tag value of 99.

- R10 should be able to reach CAT4 through the tunnel.
- No static routes are allowed to be added to accomplish this task.

Task 21: FlexVPN Hub & Spoke

- Configure an IKEv2 VPN between R10 and R11.
- This should be a hub (R11) and spoke (R10) deployment.
- Use digital certificates for authentication. R2 acts as a CA.
- Use IKEv2 routing to protect traffic between 10.100.100.0/24 and VLAN114 behind R11.
- Create an additional loopback interface on R10 – 10.251.251.10/24.
- This subnet should be dynamically advertised to the hub using OSPF.
- Hub should be able to reach this network through the VPN tunnel.
- You are only allowed to use Smart Default configurations.

Task 22: FlexVPN EAP Authentication

- Modify the configuration from the previous task.
- Use EAP as the authentication method.
- Authenticate as “Prince” with a password “OfPersia”.
- RADIUS communication should be protected with a key of “ipexpert”.

Section 8

Wireless

Section 8: Wireless is intended to let you be familiar with the Wireless technologies that are available on AP & WLC. You will be configuring WLC and features related to Wireless Security.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab. Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on Wireless technologies. You will need to pre-configure the network with the base configuration files

NOTE: *Static/default routes are NOT allowed unless otherwise stated in the task*

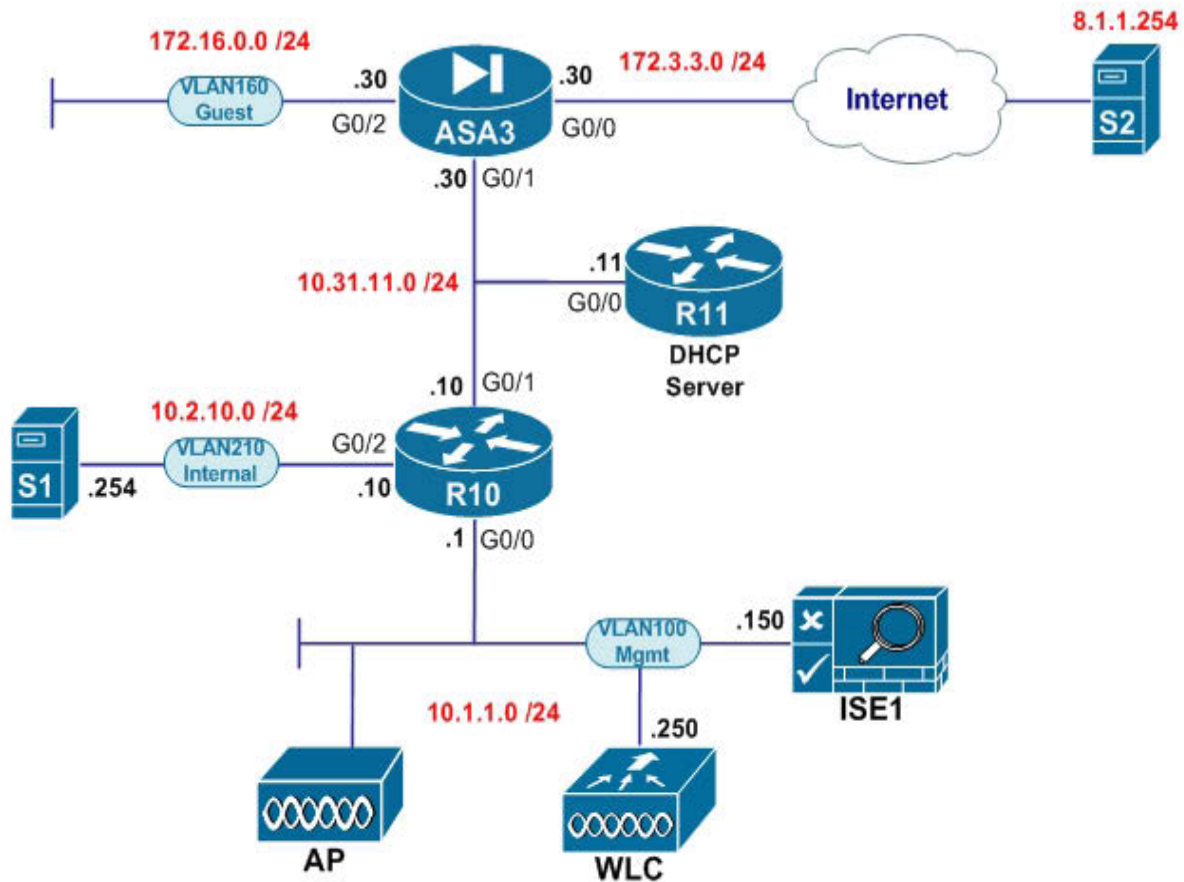
Estimated Time to Complete: **4 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below:

Device	Port	VLAN	IP Address
R10	G0/0	100	10.1.1.1/24 2010:1:1::10/64
	G0/1	311	10.31.11.10/24
	G0/2	210	10.2.10.10/24
R11	G0/0	311	10.31.11.11/24
ASA3	G0/0	33	172.3.3.30/24
	G0/1	311	10.31.11.30/24
	G0/2	160	172.16.0.30/24
ISE	G0/0	100	10.1.1.150/24
WLC	Mgmt	100	10.1.1.250/24

Security Volume I Wireless Topology



Lab-8 Configuration tasks

Task 1: WLC Initialization

- Initialize WLC using CLI
- Administrator name should be “admin”, password “IPexpert123”
- Management interface (Port #1) IP address should be set to 10.1.1.250
- DHCP Server IP address should be set to 10.1.1.250
- Virtual Gateway IP should be 1.250.250.250
- User Mobility/RF Group name “RFGROUP”

Task 2: WLC Basic Configuration

- Make sure you can access Controller using GUI
- Enable HTTP access to WLC
- Configure WLC to use NTP Server 10.1.1.101
- Any device in the management VLAN should be able to poll WLC using SNMP v1/2c
- AP should obtain an IP address from the internal DHCP pool (10.1.1.81-10.1.1.90)
- Create WLAN with SSID “IPx_Sec_Internal”. Users connecting to this network should be placed in VLAN 210
- Create WLAN with SSID “IPx_Sec_Guests”. Users connecting to this network should be placed in VLAN 160

Task 3: DHCP Proxy Mode

- Clients connecting to the Internal WLAN should obtain an IP address via DHCP
- Configure WLC to support this requirement
- WLC should act as a Proxy for client messages
- Treat R10 as a DHCP Server

Task 4: DHCP Bridging Mode

- Clients connecting to Guest WLAN should obtain an IP address via DHCP
- Configure WLC to support this requirement
- WLC should act as a Bridge for client messages
- Treat R11 as a DHCP Server

Task 5: WLAN Security

- Use WPA2 to protect communication in the Internal WLAN
- Clients should be authenticating using key “outofcontrol”
- Communication should be encrypted using AES

- Apply an ACL to the Internal WLAN that restricts traffic in the following way:
 - Blocks all Telnet connections initiated by wireless clients
 - Blocks all HTTP connections from the wired network to wireless clients
 - Permits all other traffic
- Hit counters should be enabled for this ACL
- This ACL should not be applied to the dynamic interface
- Guest WLAN connections should be authenticated based on MAC address of the client
- Only known Endpoints should be given access to the network
- Use ISE as the source of Endpoint information
- RADIUS shared secret used should be “ipexpert”

Section 9

Advanced Security

Section 9: Advanced Security is intended to let you be familiar with System Hardening and Advanced Security technologies that are available on IOS & the ASA. You will be configuring features related to Traffic Plane protection, Services protection and general System Hardening & Availability.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on Advanced Security technologies. You will need to pre-configure the network with the base configuration files

NOTE: Static/default routes are NOT allowed unless otherwise stated in a task.

NOTE: You can allow ICMP for testing throughout the network

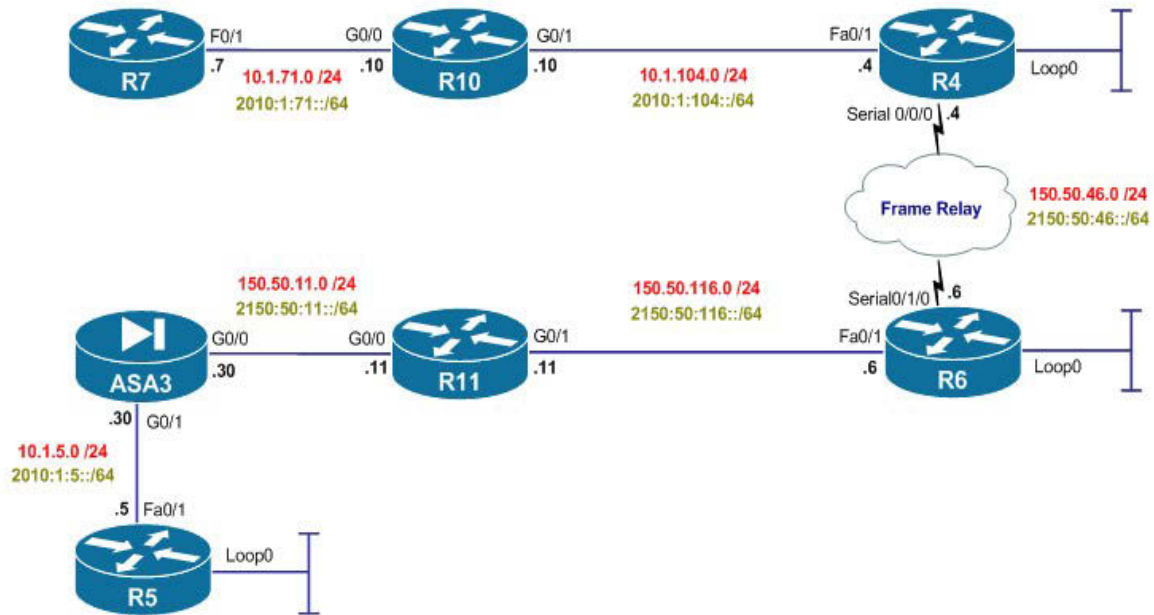
Estimated Time to Complete: **6 Hours**

Pre-setup

- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R4	F0/1	104	10.1.104.4/24
			2010:1:104::4/64
	S0/0/0		150.50.46.4/24
	Loop0		2150:50:46::4/64 4.4.4.4/24
R5	F0/1	305	10.1.5.5/24
	Loop0		2010:1:5::5/64 5.5.5.5/24
R6	F0/1	116	150.50.116.6/24
			2150:50:116::6/64
	S0/1/0		150.50.46.6/24
	Loop0		2150:50:46::6/64 6.6.6.6/24
R7	F0/1	71	10.1.71.7/24 2010:1:71::7/64
R10	G0/0	71	10.1.71.10/24
	G0/1	104	2010:1:71::10/64 10.1.104.10/24 2010:1:104::10/64
R11	G0/0	501	150.50.11.11/24
	G0/1	116	2150:50:11::11/64 150.50.116.11/24 2150:50:116::11/64
ASA3	G0/0	501	150.50.11.30/24
	G0/1	305	2150:50:11::30/64 10.1.5.30/24 2010:1:5::30/64

Security Volume I Advanced Security



Lab-9 Configuration tasks

Task 1: IP Routing & Route Filtering

- Configure IPv6 on all devices according to the table and lab topology
- Enable EIGRPv6 between R11 and R6's F0/1
- Enable OSPFv3 between R7, R10 and R4's F0/1
- Enable BGP for IPv6 over the Frame Relay cloud
- Use AS numbers 400 (R4) and 600 (R6)
- Make sure 2010:1:5::/64 is reachable in AS 600. Exchange all IPv6 routes between ASes. Ensure full IPv6 connectivity.
- You are allowed to add one default route on R5 and the ASA
- You are allowed to add one static route on R11
- Make sure RFC1918 subnets are not advertised to AS 600 devices. You can modify
- OSPF configuration on routers R4, R7 and R10 to accomplish this
- Advertise loopback of R5 into OSPF (IPv4) but not the 10.1.5.0/24 network
- Create loopback0 (7.7.7.7/24) on R7 and advertise it to OSPF as /24

Task 2: Routing Protocol Authentication

- Authenticate OSPF adjacencies in area 0 using MD5
- Area 1 should be secured using clear-text password
- Authentication on R10 can be only enabled for the entire area; link to R7 should be exempted from clear-text / MD5 authentication
- Enable authentication for EIGRPv6
- Secure OSPFv3 adjacencies using SHA-1 and AES 128
- IPv6 BGP peerings should be authenticated as well
- Use "ipexpert" for all passwords

Task 3: Basic Device Access Configurations

- Configure a domain of ipexpert.com on R5, R7, R10 and R11
- Use a username of "ipexpert" and a password of "cisco" unless otherwise specified
- Make sure any username password in this lab is not easily decrypted
- Configure a message on R5 that will appear before the password prompt when connecting via Telnet/SSHv2 (only allow SSH version 2)
- Configure a message that will appear after the session is interacting with the EXEC
- Connecting users should see the VTY line number the session terminates on
- VTY connections should timeout after 15 minutes of inactivity and should be disconnected after 1 hour regardless of activity

Task 4: Controlling Device Access

- The administrator of R7 wants to reserve a VTY line for himself. Accomplish this by
- changing the TCP port for VTY 15 to 2015. Only allow SSH version 2 connections on VTY 15
- The administrator of R7 does not want anybody to telnet from R7. Disable outbound telnet on R7. Do not make any changes in global configuration to accomplish this task
- When anyone else Telnets to R7, they should not have the ability to access the CLI.
- Instead, they should receive a menu that only allows them the ability to perform the following commands :
 - Show ip interface brief
 - Show ip route
 - Show ip ospf neighbor
 - Exit

Task 5: Management Restrictions

- Configure R10 to only allow inbound SSH sessions to the VTYS. Accomplish this without the use of an ACL
- Configure R10 to drop all SSH connections except from 10.1.71.0/24 & 2010:1:71::/64
- The administrator of R4 does not want anybody to telnet outbound from this device – you must accomplish this task using a single line ACL on R4
- Outbound telnet traffic from R6 should be sent to Null0
- Telnet and SSH traffic through the routers should not be affected

Task 6: ASA Control Plane protection

- Configure ASA3 to allow VPN connections coming from IP address 11.11.11.11
- Tunnel establishment attempts coming from any other address should be blocked
- Transit traffic should not be affected

Task 7: Control Plane Policing

- R11 should be configured to protect its CPU using CoPP feature
- Rate-limit all ICMP packets to 15 per second
- Rate-limit all ICMPv6 packets to 70000 bps
- All HTTP packets sent from 5.5.5.5 should be dropped
- Outbound telnet packets destined to 7.7.7.7 should be dropped
- Make sure OSPF packets are not affected by this configuration

Task 8: Control Plane Protection

- R10 should be configured to protect its CPU using CPPr
- Packets destined to non-listening ports should be dropped
- Telnet connections on port 3020 to VTY line 16 should be allowed

- Input queue of R10 should not be overwhelmed by any single protocol traffic
- No more than 100 BGP and 4 Telnet packets should be seen in the queue
- No more than 30 packets for all other TCP/UDP enabled protocols enabled on the router should be seen in the queue
- Allowed and over the limit Telnet packets should be logged
- All packets allowed by the Host subinterface should be logged and rate-limited to no more than one message every 5 seconds

Task 9: Management Plane Protection

- Only allow SSH and HTTP packets to R4
- Don't use any access-list or VTY line modification to accomplish this task
- Management traffic should be only allowed through the F0/1 interface

Task 10: NTP

- All involved routers except R5 should source NTP requests from their Loop 0 interface
- Set R4 as NTP master with a stratum of 2
- R6 should get its time from R4 and send NTP log messages to 150.50.116.200
- R6 should periodically update the hardware clock from NTP time source
- Configure R10 as NTP server (stratum 4); R5 & R11 should act as NTP Clients
- NTP packets exchanged between those three routers should be using IPv6 for transport
- If one of the clients loses connectivity to the server it should obtain time from its peer
- All devices should account for daylight savings time
- All NTP communication should be authenticated (use key "ipexpert")

Task 11: SNMP & CPU Statistical Gathering

- Configure R5 to allow SNMP polls from 10.1.5.0/24 using version 2c
- Only allow SNMP GET packets to be processed – use community string "ipexpert"
- To find the source of the problem configure R5 to send a SNMP Trap to 2010:1:5::100 any time the total CPU utilization hits 65%
- Encrypt & authenticate SNMP packets using 3DES and SHA; use "ipexpert" as keys
- You will also want it to inform you once it falls back below 50% to allow you to do trend analysis. Use a 5 second polling interval
- Only gather statistics for processes that use at least 3% of processor time. Gather the last 400 seconds of history

Task 12: DHCP & DHCPv6

- Enable R5 as a DHCP Server with the following information :
 - Network 10.1.5.0 /24
 - WINS address 10.1.5.135
 - DNS address 10.1.5.53

- Default Gateway 10.1.5.30
 - Lease Time 3 days 12 hours
- Enable Conflict Logging
- Enable option 19 to configure clients to do IP layer packet forwarding
- Make sure the router securely updates the ARP Table
- Specify five ping attempts by the DHCP server before ceasing any further ping attempts
- Configure CAT3 as a DHCPv6 Server for VLAN 116
- Assign a domain-name "ipexpert.com"
- CAT4 should obtain an IPv6 address from CAT3 on its SVI 116

Task 13: Unnecessary Services & Hardening

- Disable unnecessary services on R7:
 - PAD
 - DHCP
 - BOOTP
 - HTTP
 - DNS Client
- R7 should not send any IPv6 Router Advertisements
- This should account for messages sent in response to Router Solicitations
- No more than five ICMPv6 error messages should be sent by R7 per two seconds

Task 14: IP Accounting

- You would like to gather traffic statistics for the traffic received by R6 on both interfaces
- This accounting should be based on IP precedence
- The maximum number of accounting entries to be created should be 500
- Maximum number of transit entries should be 50
- Don't account for 7.7.7.7 in the transit table

Task 15: Core Dumps

- Configure R5 to send a Core Dump to a RCP Server located at 10.1.5.100
- Rename the files to "R5-crashinfo", and set the dump size to 32768
- Use the username "ipexpert"

Task 16: Memory Checks

- R5's current IOS has a memory block overflow problem in the packet memory
- Configure R5 to recover from this error unless it happens twice in less than 10 seconds
- The maximum number of error connections before a reboot should be set to 200

- Also, enable the chunk validation to see if it can give further information as to what is causing the io memory corruption
- After setting up this protection on R5 you have noticed you are filling up the flash too quickly. Configure a maximum number of 20 crash dump files before old files are overwritten

Task 17: CPU, Memory Protection & NVGEN Enhancement

- With the memory problem you are having on R6 you have also noticed it is running low on memory over time and requires a reboot. Configure R6 to send a Syslog message to 150.50.116.200 when the packet memory available falls below 2 MB free
- In addition if this occurs make sure there is still 2 MB reserved for critical management processes
- If all else fails make sure there is still 4MB free memory, to console into R6 so you can gather debug/crashinfo to further troubleshoot the problem
- Enable the feature that reduces the amount of time required for running configuration management
- Once enabled, interface configuration should be cached in the system memory

Task 18: Managing Configuration Files

- Configure R7 to automatically archive its running configuration twice per day
- Save this file to the local flash as R7-archived-config. Save no more than 5 of these files
- Configure R7 to store a secure copy of the boot-config
- On R11 you have been running into issues with multiple administrators making changes at the same time
- Configure R11 to prevent from happening by locking the configuration automatically
- Configure R11 to archive any config changes made
- Keep it below 75 lines and do not log passwords
- Send a message to the logging server whenever a configuration change occurs

Section 10

Network Attack

Mitigation

Section 10: Network Attack Mitigation & Prevention is intended to let you be familiar with common network attacks and methods/tools that can be used to prevent them. You will be configuring features related to attack detection, QoS techniques, L2 security, IPv6 security & attack-specific scenarios.

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab.

Multiple topology drawings are available for this chapter.

General Rules

- This lab will focus strictly on Network Attack Mitigation technologies. You will need to pre-configure the network with the base configuration files

NOTE: Static/default routes are NOT allowed unless otherwise stated in a task.

NOTE: You can allow ICMP for testing throughout the network

Estimated Time to Complete: **6 Hours**

Pre-setup

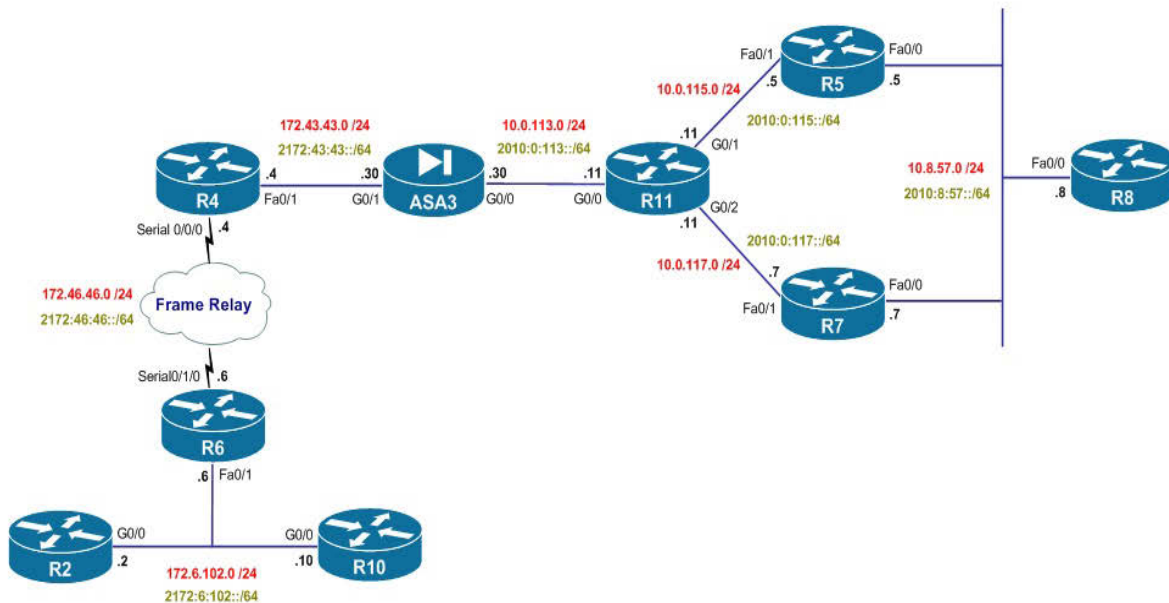
- Please login to your Security vRack at ProctorLabs.com and load the initial Configuration
- Verify basic L2/L3 connectivity. Use IP Addressing Table, Lab Diagram and the Physical Topology
- This lab is intended to be used with online rack access provided by our partner Proctor Labs (www.proctorlabs.com). Connect to the terminal server and complete the configuration tasks as detailed below

Device	Port	VLAN	IP Address
R2	G0/0	102	172.6.102.2/24 2172:6:102::2/64
	Loop0		2.2.2.2/24 2::2/64
R4	F0/1	43	172.43.43.4/24 2172:43:43::4/64
	S0/0/0		172.46.46.0/24 2172:46:46::4/64
	Loop0		4.4.4.4/24 4::4/64
R5	F0/0	857	10.8.57.5/24 2010:8:57::5/64
	F0/1	115	10.0.115.5/24 2010:0:115::5/64
	Loop0		5.5.5.5/24 5::5/64
R6	F0/1	102	172.6.102.6/24 2172:6:102::6/64
	S0/1/0		172.46.46.6/24 2172:46:46::6/64
	Loop0		6.6.6.6/24 6::6/64
R7	F0/0	857	10.8.57.7/24 2010:8:57::7/64
	F0/1	117	10.0.117.7/24 2010:0:117::7/64
	Loop0		7.7.7.7/24 7::7/64
R8	F0/0	857	10.8.57.8/24
R8	F0/0		2010:8:57::8/64
	Loop0		8.8.8.8/24 8::8/64
R10	G0/0	102	172.6.102.10/24 2172:6:102::10/64

	Loop0		100.100.100.10/24 10::10/64
R11	G0/0	113	10.0.113.11/24 2010:0:113::11/64
	G0/1	115	10.0.115.11/24 2010:0:115::11/64
	G0/2	117	10.0.117.11/24 2010:0:117::11/64
	Loop0		11.11.11.11/24 11::11/64
ASA3	G0/0	113	10.0.113.30/24 2010:0:113::30/24
	G0/1	43	172.43.43.30/24 2172:43:43::30/64

Security Volume I

Network Attack Mitigation & Prevention



Lab-10 Configuration tasks

Task 1: Traffic Marking & Classification

- Configure R6 so that all IPv4 Telnet packets are marked with IP Precedence 4
- HTTP packets (IPv4) should be colored with DSCP 31
- ICMPv6 traffic should be marked with IP Precedence 4
- All other IPv6 packets should be transported over FR cloud with the DE bit set
- On R4 all IPv4 packets with IP Precedence 4 received on DLCI 406 should be re-marked as IP Precedence 0
- IPv6 traffic with IP Precedence 4 should be marked with DSCP value 11
- Don't use an ACL to accomplish this
- IPv4 packets received with DSCP 31 should be now colored with DSCP cs4
- All traffic received with FR DE bit set should be marked as IP Precedence 7

Task 2: NBAR & NBAR Next Generation

- Using NBAR create and apply a policy outbound on R11's G0/0 interface to drop the Slammer worm
- The Slammer worm uses UDP port 1434; its packets are exactly 404B in length
- Also all HTTP packets with string "attack" in the URL should be dropped but only when sent to/coming from 4.4.4.4
- The "attack" string should not be case-sensitive

- Using the same policy-map drop all terminal-related traffic except PCANYWHERE
- Also implement a policy for Peer-to-Peer traffic:
 - All clear-text packets should be rate-limited to 200kbps
 - All encrypted traffic should be dropped
- Enable classification of IPv6 traffic that is carried over Teredo tunnels

Task 3: Policy Based Routing

- Use Policy-Based Routing on R6 to drop MSBlaster worm traffic
- Offending packets are coming from VLAN 102 using IPv6 and TCP port 135 for transport
- Also make sure IPv6 Telnet connections to port 135 cannot be initiated from R6

Task 4: CAR

- Rate-limit inbound ICMP traffic on R6's Serial interface to 16kbps. Use the minimum burst values available
- Conforming traffic should be transmitted and exceeding traffic should be dropped
- Other IPv4 traffic should be rate-limited to 64kbps. Use 64kbps for both of the burst values
- Conforming traffic should have the DSCP set to AF21 and exceeding traffic should be transmitted unchanged

Task 5: Flexible NetFlow

- Configure R11 to detect SYN Flooding attack coming from VLAN 113 network
- During this initial phase of monitoring you are only interested in the IPv4 addresses of target devices being under attack (VLANs 115, 117 and 857)
- You want to know the number of packets sent to a particular device and the time attack has started (based on System Uptime)
- The collected information should be never removed from the Cache
- No more than 200 entries should be cached
- R11 should be also monitoring unicast IPv6 traffic received on G0/1 and G0/2 interfaces
- Cache entries should depend on the input interface, destination address and name of the application used
- You want to know the number of bytes seen for the flow and also the first 20 bytes of the payload from the first packet matching the flow
- Cache information should be exported to the Collector Engine with an IP address 2010:8:57::100 over UDP port 90
- Don't analyze every IPv6 packet; only one out of 5 packets should be processed

Task 6: ICMP & UDP Flooding Attacks

- Modify the configuration on the ASA to increase protection against ICMP Floods

- Make sure only one Echo Reply packet is allowed through the firewall for every single Echo Request seen
- Recently there were several incidents of high-volume traffic (Echo Requests) coming from the FR cloud destined to 172.6.102.255
- Configure R6 so those packets never get to other routers in VLAN 102
- Use only one command to accomplish this
- R8 appears to be vulnerable to IPv6 Fraggle attacks and can be used as an amplifier
- Configure R11 to rate-limit Fraggle Echos to 24kbps when destined to 2010:8:57::/64
- Processing of those packets on R8 should be disabled

Task 7: Fragmentation Attacks

- Router 6's F0/1 interface should be configured to prevent Buffer Overflow fragment attack
- No more than 25 packets should be in the process of reassembly at any point in time
- Ensure that a packet of up to 13 fragments can be reassembled successfully
- R11 should be blocking IP fragments on its G0/1 interface
- Configure ASA3 to physically reassemble all IP fragments

Task 8: IP Options Attacks

- Router 6's should be configured to drop packets with Route-Record option on S0/1/0
- Traffic with Home Test (HoT) messages should be also blocked
- R11 should be configured to prevent attacks that use RHO
- In addition packets with any IPv4 Option set should be blocked
- ASA3 should stop traffic with Hop-by-Hop EH; traffic with Router Alert option should be forwarded
- Make sure IPv6 Extensions are ordered according to the RFC; otherwise drop the packet

Task 9: Layer 3 Spoofing Attacks

- Implement RFC 2827 on R6's FR interface
- Make sure RFC 1918 ranges are blocked as well
- RFC 3330 should be implemented for IPv6 – only account for the multicast range
- Prevent IP Spoofing Attacks on R4
- Only traffic received from a network that exists in the routing table for a given network should be allowed
- Default route should be considered as a valid route for IPv6 packets but the interface the packet is received on must match egress interface from the entry in the RIB

Task 10: TCP SYN Attacks

- Routers 5 and 7 should protect VLAN 857 from SYN Flooding attack
- Use TCP Intercept as a protection tool
- Routers should not act as a proxy for the connections

- Aggressive mode should start when there is more than 500 half-open connections detected total or 60 during last minute
- Aggressive mode should cease once the number of half-open sessions falls below 250 total or 30 within the last 60 seconds
- ASA should limit the number of simultaneous TCP and/or UDP connections to 1000
- Embryonic connection limit should be set to 400 with a per-device limit of 50
- ASA's limits should also apply to IPv6 traffic

Task 11: Application Attacks & FPM

- Use Flexible Packet Matching to drop malicious traffic
- Packets containing the string of characters „BADCC1E” within 100 bytes from the start of the UDP header should be blocked
- Those packets are destined to the well-known UDP port 53
- This policy should be applied to R7's F0/0 interface inbound
- You are allowed to use Protocol Header Definition Files to implement this
- R5 should be configured to drop and log ICMP packets with “AZ” in the payload
- Those packets will be carried in an IP-IP tunnel
- You are only interested in dropping Echo packets only

Task 12: DDoS Attacks & RTBH

- AS 600 needs to be configured with RTBH to protect itself against potential attacks
- All traffic sent to R2's loopback 20 interface should be blackholed at the edge of AS
- Use R10 as the trigger router
- Don't inform attacker packets never make their way to the victim
- You are allowed to use static routes in this task

Task 13: Layer 2 Security & Attacks

- Prevent MAC Spoofing & Flooding attacks on the L2 port connected to R11's G0/1
- On the same interface limit the amount of unicast packets to 5000 per second
- Broadcast traffic should be restricted to 1Mbps; once the threshold is crossed packets should stop to be dropped after broadcast rate falls below 700kbps
- CAT1 should be configured to black-hole frames with MAC address 00ba.dbad.cc1e seen in VLAN 857
- On CAT1's F0/7 only allow non-IP packets from MAC address R7 uses on F0/0
- Don't use Port Security to accomplish this
- Protect CAT4's CPU from ARP & IGMP flooding attacks
- When the number of offending ARP/IGMP packets exceeds 25 per second the offending VLAN should be shutdown on a port
- After a minute interfaces should be put back into the normal state automatically

Task 14: Spanning-Tree Attacks

- Prevent STP Root attack on CAT4
- If a Superior BPDU is received on G1/0/23 or G1/0/24 the port should be put into Root-Inconsistent state
- Make sure devices connected to PortFast-enabled ports on CAT3 cannot affect STP
- Enable BPDU Guard to accomplish this
- On CAT2 port connected to R10 should be put into err-disabled state if a BPDU is detected

Task 15: DHCP Attacks & First Hop Security

- There will be a DHCP server put into use on the network connected to CAT1's port F0/13
- The DHCP server will hand out IPv4 addresses to VLAN 857 clients
- Configure the switch to protect against DHCP Starvation and Rouge Server attacks
- Rate-limit the potential client ports to only allow 6 DHCP packets per second
- Make sure frames with spoofed MAC addresses will be dropped in DHCP Requests
- R11's G1/0/11 will be configured with DHCPv6 services in the future
- Configure one of the First Hop Security features to protect DHCP communication in VLAN 115
- DHCP Server packets should be only allowed to come from R11's IPv6 address
- Enable IPv6 Snooping for VLAN 115

Task 16: ARP & L2 Spoofing Attacks

- Prevent ARP MiTM attacks in VLAN 857
- Routers R5, R7 and R8 should be still able to successfully communicate
- ARP packets generated by those devices should be logged
- Also enable source and destination MAC address validation
- Prevent L2 & L3 IPv4 spoofing attacks on port F0/8 on CAT1
- You are not allowed to modify the DHCP Snooping database in this task
- CAT3 should be configured to protect against spoofed IPv6 packets on its L2 ports
- Configure Source Guard on G1/0/10 and G1/0/11 interfaces

Task 17: ND Cache Poisoning Attacks & SEND

- Prevent ND Cache Poisoning attacks in VLAN 102
- Two routers (R2 and R6) should have their IPv6 addresses cryptographically secured
- Addresses used by routing protocol updates should be protected as well
- The highest level of protection against brute-force attacks must be ensured
- All non-SEND messages seen by R2 and R6 devices should be dropped