ipexpert

IPexpert's Lab Preparation Workbook

for the Cisco® CCIE™ Security Volume 2

Complete Workbook

LAB 1

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

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

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

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

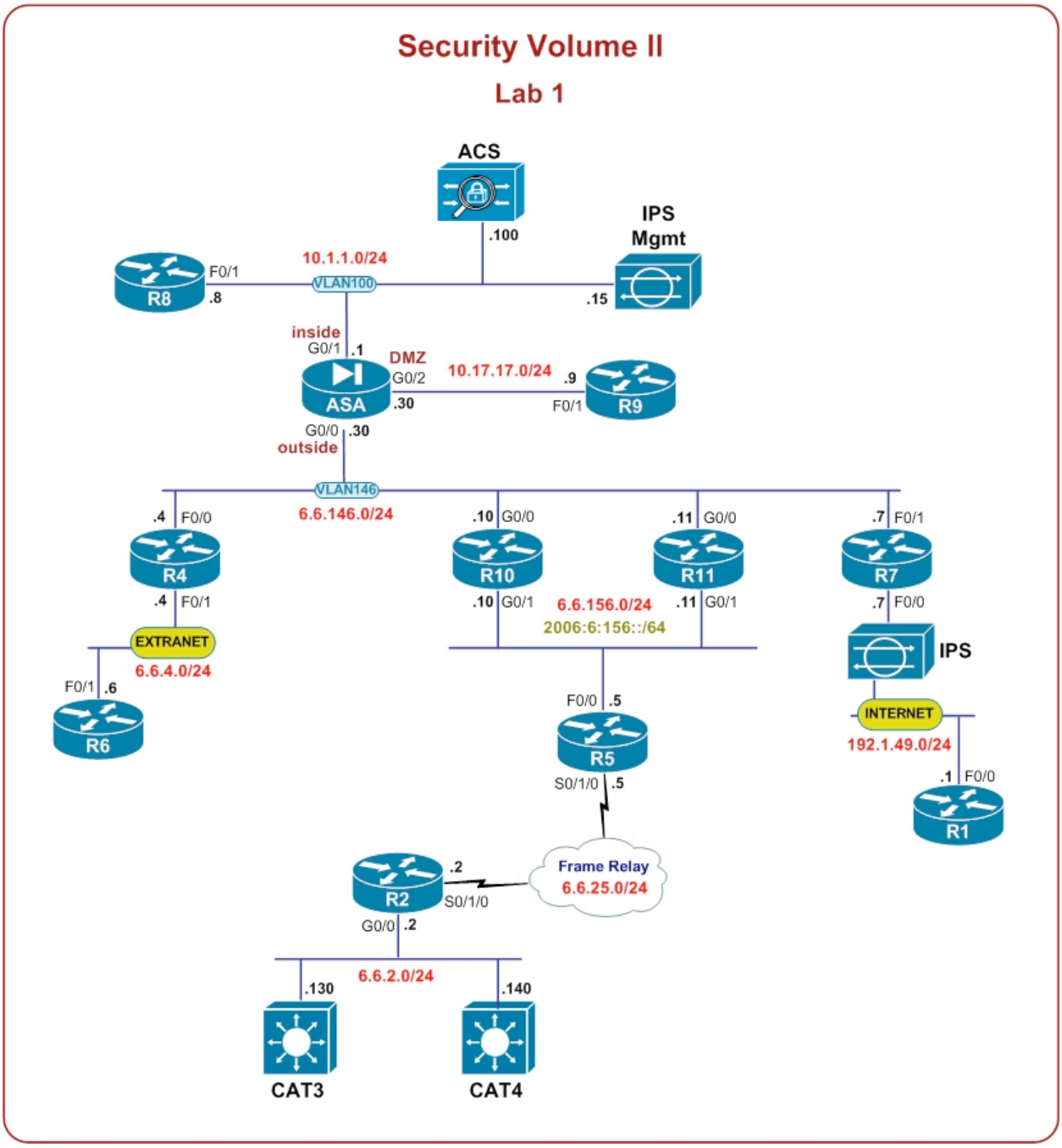
***NOTE**: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device*

Estimated Time to Complete: **8-10 Hours**

Pre-setup

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

Device	Port	VLAN	IP Address
R1	F0/1	49	192.1.49.1/24
	Loop0		6.6.99.1/32
R2	G0/0	2	6.6.2.2/24
	S0/1/0		6.6.25.2/24
	Loop0		6.6.99.2/32
R4	F0/0	146	6.6.146.4/24
	F0/1	4	6.6.4.4/24
	Loop0	160	6.6.99.4/32
R5	F0/0	156	6.6.156. 5/24
			2006:6:156::5/64
	S0/1/0		6.6.25.5/24
	Loop0		6.6.99.5/32
R6	F0/1	4	6.6.4.6/24
	Loop0		6.6.99.6/32
R7	F0/0	49	192.1.49.7/24
	F0/1	146	6.6.146.7/24
	Loop0		6.6.99.7/32
R8	F0/1	100	10.1.1.8/24
	Loop0		6.6.99.8/32
R9	F0/1	17	10.17.17.9/24
	Loop0		6.6.99.9/32
R10	G0/0	146	6.6.146.10/24
	G0/1	156	6.6.156.10/24
	Loop0		2006:6:156::10/64
			6.6.99.10/32
R11	G0/0	146	6.6.146.11/24
	G0/1	156	6.6.156.11/24
			2006:6:156::11/64
	Loop0		6.6.99.11/32
CAT3	VLAN2	2	6.6.2.130/24
CAT4	VLAN2	2	6.6.2.140/24
ASA	G0/0	146	6.6.146.30/24
	G0/1	100	10.1.1.1/24
	G0/2	17	10.17.17.30/24
ACS		100	10.1.1.100/24
IPS	Mgmt	100	10.1.1.15/24



1.0 ASA Firewalls (20 points)

Task 1.1: ASA Setup (4 Points)

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

Task 1.2: Source Protection (4 Points)

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

Task 1.3: Traffic Filtering (4 Points)

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

Task 1.4: Routing (4 Points)

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

Task 1.5: Filtering Techniques (4 Points)

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

2.0 IOS Firewall (12 points)

Task 2.1: IOS Firewall (4 Points)

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

Task 2.2: Zone-Based Firewall (4 Points)

- Configure R7 for ZBF
- Treat networks behind F0/0 as outside zone and networks behind F0/1 as inside
- Allow all outbound HTTP, ICMP, TCP, and UDP traffic
- Allow traffic back in as required for tasks in this lab
- Enable logging of dropped packets and log summaries

Task 2.3: Zone-Based Firewall (4 Points)

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

3.0 Cisco IPS and Content Security (8 points)

Task 3.1: IPS Initialization (4 Points)

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

Task 3.2: Blocking Attacks (4 Points)

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

4.0 Cisco VPN Solutions (18 points)

Task 4.1: Site to Site (4 Points)

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

Task 4.2: Stateful HA IPSec (5 Points)

- All traffic behind R2 Serial0/1/0 and VLAN146 should be encrypted
- R10 and R11 should act as a failover IPSec pair
- In the event of a host failure the IPSec tunnel should remain active without requiring a new SA negotiation
- A Failure should be detected in less than 300 msec
- DH exchange should take place every Quick Mode negotiation
- Disable Anti-Reply checks on R2
- Tune OSPF timers on all devices in VLAN 146 to speed up the convergence
- Make sure IPSec peers verify if the tunnel is actually operational. It should only occur when traffic is actively traversing the IPSec tunnel

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

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

Task 4.4: GRE (4 Points)

- Configure R4 and R2 to encrypt traffic between the Extranet and VLAN 2

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

5.0 Identity Management (18 points)

Task 5.1: Cut-Through Proxy (4 Points)

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

Task 5.2: Authentication Proxy (4 Points)

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

Task 5.3: Device Management (6 Points)

- Configure R1 for Telnet & SSH management using TACACS+ for authentication
- All TACACS+ Shell Login requests coming from R1 should result in Privilege Level 15 access. Create a separate Access Service just for this purpose with a specific condition to meet this requirement
- Use TACACS+ to authorize each and every command
- User “admin” (pw “cisco”) should be able to issue all commands
- User “oper” (pw “cisco”) should be able to issue all show commands except “show memory”
- Connecting user should see the following prompt when authenticating : “T-username:”, “T-password:”
- Send accounting information to ACS as well
- Configure a backup solution so user “admin” can login to the router when the ACS is not available
- This configuration should not affect console access

Task 5.4: Access Control with LDAP (4 Points)

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

6.0 Advanced Security (12 points)

Task 6.1: OSPFv3 Authentication Troubleshooting (4 Points)

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

Task 6.2: DHCP (4 Points)

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

Task 6.3: Port Protection (4 Points)

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

7.0 Attack Mitigation (12 points)

Task 7.1: FPM (4 Points)

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

Task 7.2: Preventing Network Attacks (4 Points)

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

Task 7.3: Preventing Network Attacks (4 Points)

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

LAB 2

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

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

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

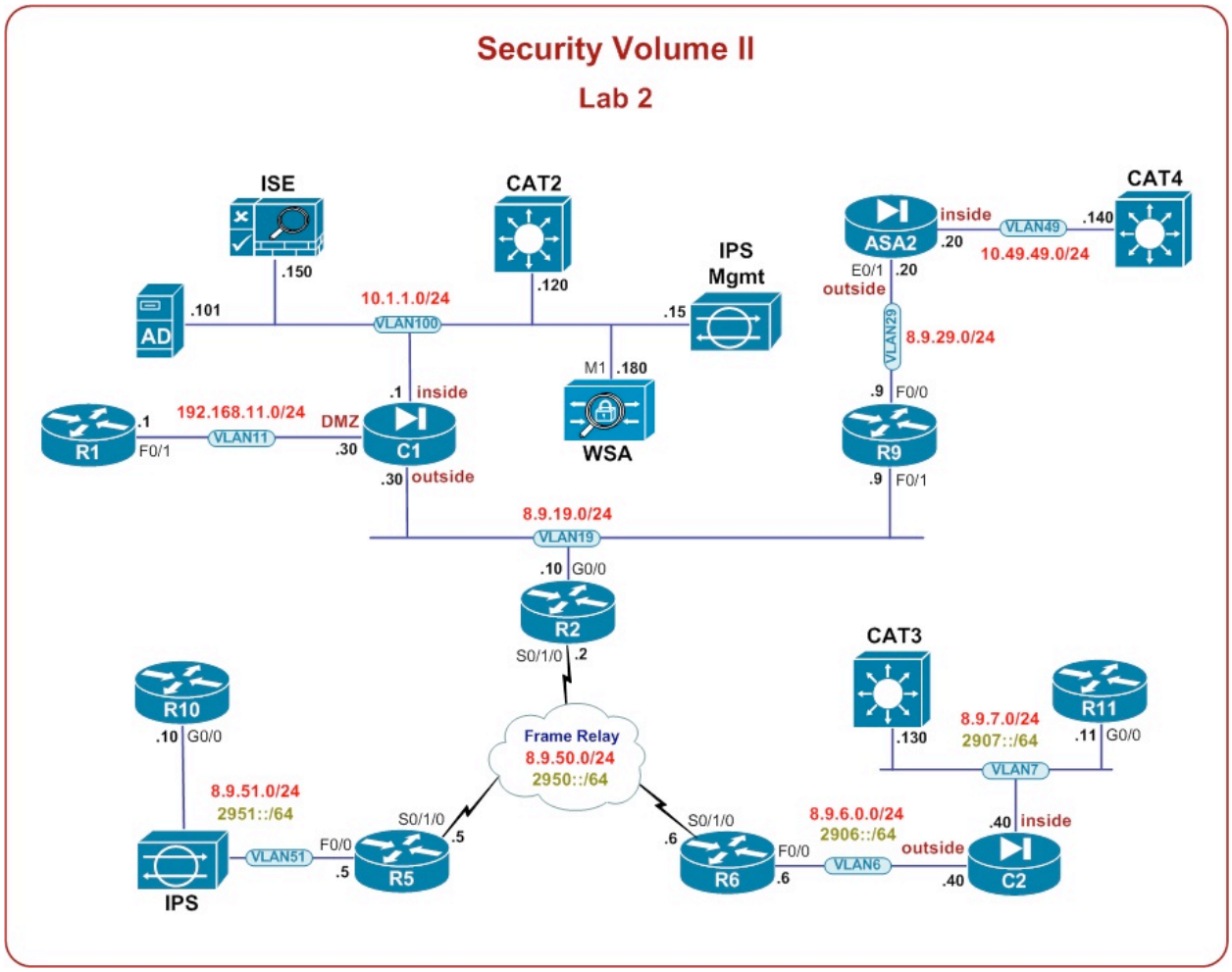
NOTE: Static/default routes are NOT allowed unless otherwise stated in the task
NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device

Estimated Time to Complete: 8-10 Hours

Pre-setup

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

Device	Port	VLAN	IP Address
R1	F0/1	11	192.168.11.1/24
	Loop0		8.9.100.1/32
R2	G0/0	19	8.9.19.2/24
	S0/1/0		8.9.50.2/24
			2950::2/64
	Loop0		8.9.100.2/32
R5	F0/0	51	8.9.51.5/24
			2951::5/64
	S0/1/0		8.9.50.5/24
	Loop0		2950::5/64
			8.9.100.5/32
R6	F0/0	6	8.9.6.6/24
			2906::6/64
	S0/1/0		8.9.50.6/24
			2950::6/64
	Loop0		8.9.100.6/32
R9	F0/0	29	8.9.29.9/24
	F0/1	19	8.9.19.9/24
	Loop0		8.9.100.9/32
R10	G0/0		8.9.51.10/24
			2951::10/64
	Loop0		8.9.100.10/32
R11	G0/0	7	8.9.7.11/24
			2907::11/64
	Loop0		8.9.100.11/32
CAT2	VLAN100	100	10.1.1.120/24
CAT3	VLAN7	7	8.9.7.130/24
CAT4	VLAN49	49	10.49.49.140/24
ASA2	Redundant1	49	10.49.49.20/24
	E0/1	29	8.9.29.20/24
ASA – C1	PortChannel1.100	100	10.1.1.1/24
	PortChannel1.11	11	192.168.11.30/24
	PortChannel1.19	19	8.9.19.30/24
ASA – C2	G0/3.6	6	8.9.6.40/24
			2906::40/24
	G0/3.7	7	8.9.7.40/24
			2907::40/64
ISE		100	10.1.1.150/24
IPS	Mgmt	100	10.1.1.15/24
WSA	M1	100	10.1.1.180/24
AD		100	10.1.1.101/24



1.0 ASA Firewalls (28 points)

Task 1.1: ASA Setup (4 Points)

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

Task 1.2: ASA2 Setup (3 Points)

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

Task 1.3: Failover (4 Points)

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

Task 1.4: NAT & Routing (3 Points)

- PAT all internal and DMZ networks to the outside's interface IP address on context C1
- ISE should be always seen as 8.9.19.150 on the outside
- CAT2 should be translated to 8.9.19.120 unless it communicates with R5's loopback – then the address should be changed to 8.9.19.220

- NAT R1 to 8.9.19.1. Hosts on the DMZ using an outside DNS server should see R1's original IP address in the DNS replies
- Enable OSPF on ASA's outside interface
- Add a default route on C1 pointing to R2; also configure a route to R1's loopback0 and a route to R1's loopback 99 (99.99.99.0/24) in the DMZ

Task 1.5: Access Control (2 Points)

- Allow the following traffic to ISE & CAT2 on C1 :
- HTTP standard port + port 8081
- HTTPs standard port + port 8443
- SSH
- RADIUS (both RFCs)
- Accomplish this with just one ACL entry
- ICMP Echos should be allowed across all ASAs/contexts
- Enable ACL optimization on C1

Task 1.6: BGP Authentication (3 Points)

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

Task 1.7: HTTP Inspection (3 Points)

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

Task 1.8: Traffic Control (3 Points)

- Permit the following ICMP and ICMPv6 traffic to the ASA C2 interfaces :
- Echo Replies
- Time-Exceed messages
- Unreachables
- All other unnecessary ICMP & ICMPv6 traffic should be explicitly dropped & logged

- Users on VLAN 7 are using a telnet application. Sometimes they leave the sessions open for 2 hours, and when they return they are forced to reestablish the session. Configure the ASA to keep all the Telnet sessions alive for more than 2 hours
- Only invalid/expired sessions should be removed from the connection table
- This configuration should only apply to Telnet traffic

Task 1.9: Logging (3 Points)

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

2.0 IOS Firewall (11 points)

Task 2.1: CBAC (3 Points)

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

Task 2.2: Firewall Tuning (3 Points)

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

Task 2.3: User-based Firewall (5 Points)

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

3.0 Cisco IPS and Content Security (18 points)

Task 3.1: IPS Initialization (3 Points)

- Configure the IPS Sensor's Command and Control Interface through the CLI to allow HTTPS access to the Sensor only from VLAN 100 based on the Network Diagram
- Use IP address 10.1.1.15/24 and gateway 10.1.1.1
- You would like to monitor all traffic inline between R5 and R10
- Use a single interface on IPS and configure the switches to support this deployment
- Synchronize time on the sensor with the AD Server

Task 3.2: Custom Signature (4 Points)

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

Task 3.3: ASA IPS (5 Points)

- Initialize the IPS module on the ASA
- Create an additional Virtual Sensor that will be monitoring all traffic coming from VLAN7 through C2
- The C1 firewall should be inspecting packets using the default vs0 – only look at packets sourced in the DMZ
- Block all ICMP & ICMPv6 Echos traversing C2. Make sure you will see an alert in the console for every dropped packet
- ICMP Echos going through C1 should be allowed but an alert must be generated whenever 5 Echos are seen within 15 seconds
- Since the first alert was generated no more alerts should fire for the next 25 seconds for a particular Attacker/Victim address pair
- If there is more than 50 alerts generated you only want to see one alert message generated per interval no matter who the Attacker/Victim is

Task 3.4: WSA Basic Configuration (3 Points)

- Perform basic WSA Initialization. Configure addresses according to the topology
- Make sure the device is listening for incoming HTTP connections on port 8080

- Use 10.1.1.101 as the NTP and DNS server
- Password MUST BE SET TO "**ironport**"
- Set default gateway to 10.1.1.1

Task 3.5: WCCP (3 Points)

- WSA should act as a proxy to HTTP (port 80 & 8081) and HTTPs (port 443) connections
- Clients will reside in VLAN 100 and ASA C1 should be configured to redirect the traffic coming from the 10.1.1.192/26 subnet
- Make sure the ASA only accepts packets from the WSA and not any other Content Engine
- Protect the WCCP communication with a password "ipx123"

4.0 Cisco VPN Solutions (14 points)

Task 4.1: DMVPN Troubleshooting (4 Points)

- There is a broken DMVPN between R2, R5 and R6
- You are supposed to fix the configuration so DMVPN verification gives outputs similar to those below (packet counters, timers etc. don't have to match) :

```
R2#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W -->
Waiting
        UpDn Time --> Up or Down Time for a Tunnel
============================================================================

Interface Tunnel100 is up/up, Addr. is 172.16.100.2, VRF ""
   Tunnel Src./Dest. addr: 8.9.100.2/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "IPSEC_PROF41"
   Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target
Network
----- --------------- --------------- ----- -------- ----- ---------------
--
    1      8.9.100.5    172.16.100.5    UP 00:22:30    D
172.16.100.5/32

    1      8.9.100.6    172.16.100.6    UP 00:14:22    D
172.16.100.6/32



Crypto Session Details:
--------------------------------------------------------------------------
------
```

```
Interface: Tunnel100
Session: [0x712CF3E0]
  IKEv1 SA: local 8.9.100.2/500 remote 8.9.100.5/500 Active
          Capabilities:(none) connid:1004 lifetime:23:37:29
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.5
  IPSEC FLOW: permit 47 host 8.9.100.2 host 8.9.100.5
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 309 drop 0 life (KB/Sec) 4416442/2249
        Outbound: #pkts enc'ed 317 drop 0 life (KB/Sec) 4416441/2249
   Outbound SPI : 0x1D1E11A1, transform : esp-3des esp-md5-hmac
    Socket State: Open

Interface: Tunnel100
Session: [0x712CF2F0]
  IKEv1 SA: local 8.9.100.2/500 remote 8.9.100.6/500 Active
          Capabilities:(none) connid:1006 lifetime:23:45:36
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 8.9.100.6
  IPSEC FLOW: permit 47 host 8.9.100.2 host 8.9.100.6
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 180 drop 0 life (KB/Sec) 4594523/2737
        Outbound: #pkts enc'ed 208 drop 0 life (KB/Sec) 4594520/2737
   Outbound SPI : 0x20C8F68F, transform : esp-3des esp-md5-hmac
    Socket State: Open

Pending DMVPN Sessions:

R2#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                            (sec)         (ms)       Cnt
Num
1   172.16.100.5            Tu100             12 00:14:48 1334  5000  0  8
0   172.16.100.6            Tu100             10 00:14:48  292  1752  0  7

R5#sh ip route eigrp | be Gateway
Gateway of last resort is not set

D     192.168.2.0/24 [90/27008000] via 172.16.100.2, 00:15:05, Tunnel100
```

```
D     192.168.6.0/24 [90/28288000] via 172.16.100.6, 00:14:59, Tunnel100

R6#sh ip route eigrp | be Gateway
Gateway of last resort is not set

D     192.168.2.0/24 [90/27008000] via 172.16.100.2, 00:15:19, Tunnel100
D     192.168.5.0/24 [90/28288000] via 172.16.100.5, 00:15:14, Tunnel100

R5#ping 192.168.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/52/56 ms

R5#traceroute 192.168.6.6

Type escape sequence to abort.
Tracing the route to 192.168.6.6

  1 172.16.100.6 36 msec *  36 msec
```

Task 4.2: FlexVPN with ASA (5 Points)

- A FlexVPN session should be established with ASA2
- ASA2 should act as the Initiator of this connection
- Protect the traffic between VLAN 49 and Loopback10 of R10
- Use AES-128, the strongest supported DH Group and SHA-256 for IKE_SA_INIT
- Authentication method selected should be PSK with a key “ipexpert”
- Use AES-128 and SHA-1 to protect CHILD_SA
- R10 should install a route to VLAN 49 with a tag of 100. Don’t use a crypto map
- You are allowed to add one static route to accomplish this task

Task 4.3: IPv6 FlexVPN (5 Points)

- Configure a FlexVPN tunnel between R10 and R11
- VPN traffic should be transported using IPv6
- Protect packets exchanged between Loopback10 interfaces of those devices
- Use Smart Defaults on R11
- Authenticate the tunnel using PSK “ipexpert1011”

5.0 Identity Management (12 points)

Task 5.1: Cut-Through Proxy (5 Points)

- Users in VLAN 51 should be authenticated prior to reaching HTTP, MS SQL and Oracleservices hosted in VLAN 49
- The following devices should be accessible to authenticated users :
- 10.49.49.51 (HTTP & MS SQL)
- 10.49.49.52 (Oracle)
- ISE should be used as a source of authentication and authorization information
- You are expected to use a granular feature-specific condition in your policies – use Client-Type VSA to accomplish this
- Authenticate using Telnet as “cutproxy” with password “cisco1”
- Protect RADIUS communication with a key “ipexpert”

Task 5.2: 802.1x (4 Points)

- Deploy 802.1x authentication on G1/0/12 interface of CAT3
- Only two devices are allowed to connect through this port – Phone and PC
- All Profiling Services should be turned off
- If ISE becomes unreachable make sure the Phone gets assigned to the Voice VLAN (599)
- Authenticated user should be placed into VLAN 29
- Unless the port is authenticated no user traffic should be allowed through it
- Use AD database for authentication (e.g. IPXEMP1//cisco)
- Protect RADIUS communication with key “ipexpert”

Task 5.3: Basic Wireless (3 Points)

- Initialize WLC with the following information :
- Administrator name MUST be “admin” and password “IPexpert123”
- SSID IPX-XXX where XXX is your pod number
- Management IP address should be 10.1.1.250
- Virtual Gateway IP should be 1.250.250.250
- Set User Mobility/RF Group name “RFGROUPXXX” where XXX is your pod number
- Use NTP Server 10.1.1.101
- Create a wireless network “IPX-EMP-XXX” where XXX is your pod number
- This WLAN should map to VLAN 29 and require 802.1x authentication
- Also enable WPA2 encryption (AES) and CCKM Fast Secure Roaming
- AP should obtain an IP address from the C1 ASA

6.0 Advanced Security (9 points)

Task 6.1: CPPr (3 Points)

- Configure early dropping of packets that are directed toward closed or non-listened TCP/UDP ports on R6
- Ensure ISAKMP packets are not affected
- Limit the total number of BGP and Telnet packets allowed in the control-plane input queue to 100

Task 6.2: OSPF Security (2 Points)

- Authenticate OSPFv2 adjacencies between routers R2, R5 and R6
- Use OSPF Type 2 authentication
- Protect OSPF neighbor sessions from CPU-based attacks – only accept OSPF packets if they come from the local L2 network

Task 6.3: SNMP (4 Points)

- Configure R2 for SNMP Support. Create two SNMP views – one which includes all objects in the MIB "internet" and the other which includes entire "cisco" MIB
- Create SNMP Group FULL with read/write access to the "internet" view for users in VLAN 7 only and security model allowing for encryption and authentication
- Create SNMP Group PART with read access to the "internet" view and write access to the "cisco" view. Security model for this group should allow for authentication
- LinkUp and LinkDown SNMP Traps sent to a management station in VLAN 100
- (10.1.1.200) should be encrypted and authenticated using 3DES and SHA algorithms with password "cisco"
- BGP SNMP Traps sent should be authenticated using SHA algorithm with password "cisco"
- Interface indexes should remain constant after a reboot

7.0 Attack Mitigation (8 points)

Task 7.1: RTBH (4 Points)

- You have detected a DoS attack coming from AS 11 (99.99.99.11)
- Attacks are targeted at subnet 5.5.5.0/24 which is part of your AS 256
- Use BGP to stop this activity at the edge of your AS
- Ensure legitimate clients can still access the services provided by devices in 5.5.5.0/24
- Treat R6 as the main controlling device
- You can use 3 static routes to complete this task

Task 7.2: IPv6 Attacks (4 Points)

- R5 should drop IPv6 fragments coming from the FR cloud
- Configure R10's g0/0 interface so the router is always capable of properly dealing with IPv6 fragments
- If more than 10 fragments are received for a packet or if the reassembly takes longer than 10 seconds all currently received data for the packet should be dropped
- Configure ASA C2 to drop & log IPv6 packets with RH Type 0
- All other RHs should be allowed and logged

Lab 3

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

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

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

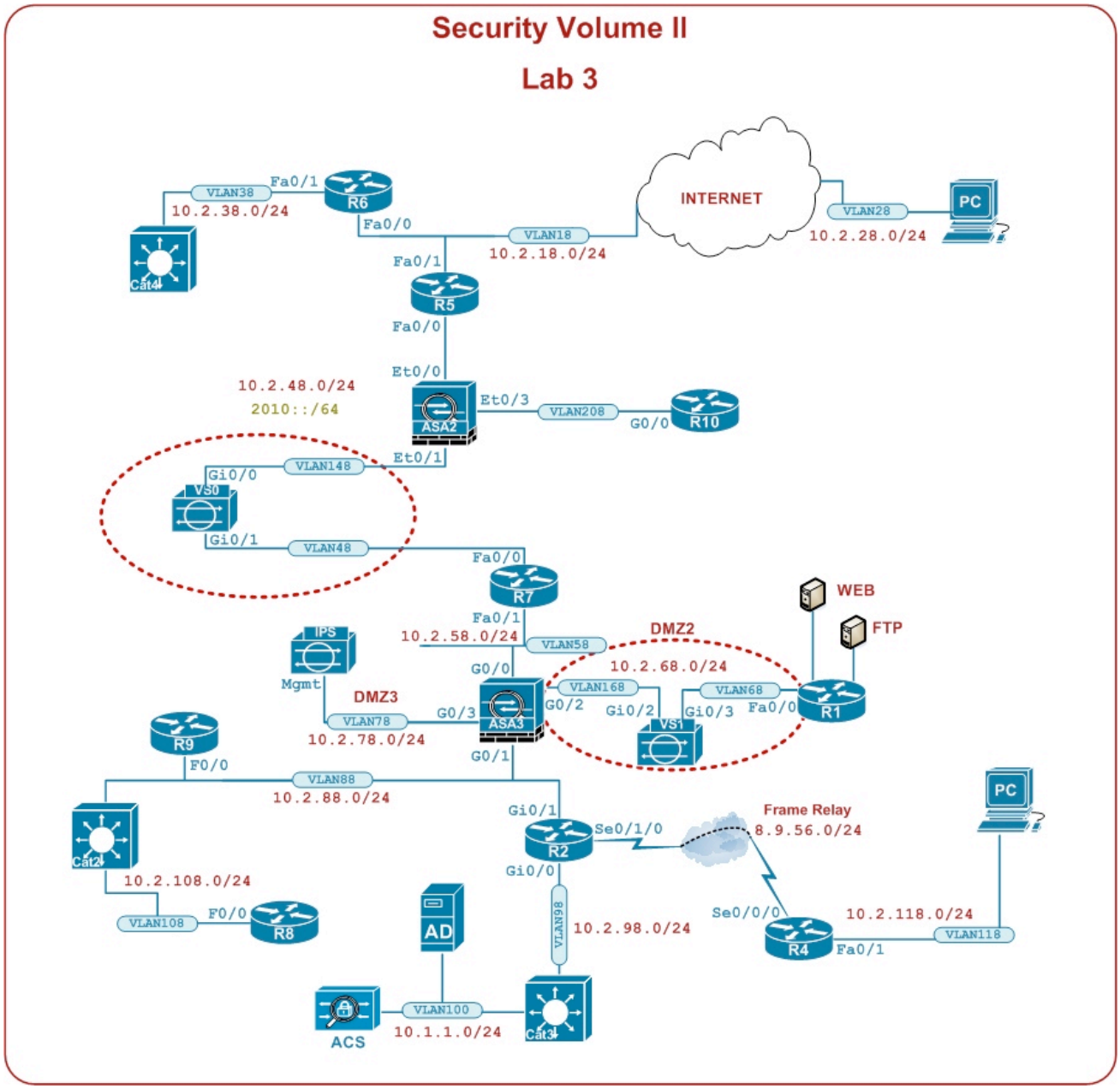
NOTE: Static/default routes are NOT allowed unless otherwise stated in the task
NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device
NOTE: Unless explicitly prohibited in a section, you may permit ICMP for connectivity testing

Estimated Time to Complete: **10 Hours**

Pre-setup

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

Device	Port	VLAN	IP Address
R1	FastEthernet0/0	68	10.2.68.1/24
	Loopback0		10.10.10.1/32
	Loopback12		10.3.68.1/24
	Loopback11		11.11.11.11/24
R2	GigabitEthernet0/0	98	10.2.98.2/24
	GigabitEthernet0/1	88	10.2.88.2/24
	Serial0/1/0.2		8.9.56.2/24
	Loopback0		22.22.22.22/32
	Loopback1		2.2.2.2/32
R4	FastEthernet 0/1	118	10.2.118.4/24
	Loopback0		44.44.44.44/32
	Serial0/0/0.2		8.9.56.4/24
R5	FastEthernet 0/0	158	10.2.48 5/24 2010::5/64
	FastEthernet 0/1	18	10.2.18.5/24
	Loopback0		55.55.55.55/32
	Loopback1		52.52.52.52/32
R6	FastEthernet 0/0	18	10.2.18.6/24
	FastEthernet 0/1	38	10.2.38.6/24
	Loopback0		66.66.66.66/24
R7	FastEthernet 0/0	48	10.2.48.7/24 2010::7/64
	FastEthernet 0/1	58	10.2.58.7/24
	Loopback0		77.77.77.77/32
R8	FastEthernet 0/0	108	10.2.108.8/24
R9	FastEthernet 0/0	88	10.2.88.9/24
R10	Gig 0/0	48	10.2.48.10/24 2010::10/64
CAT4	VLAN38		10.2.38.24/24
CAT2	VLAN88	88	10.2.88.22/24
	VLAN108	108	10.2.108.22/24
CAT3	VLAN98	98	10.2.98.23/24
	VLAN100	100	10.1.1.1/24
ASA2	Ethernet0/0 (outside)	158	
	Ethernet0/1 (inside)	148	
	Ethernet0/3 (DMZ)	208	
ASA3	Gig0/0 (outside)	58	10.2.58.30/24
	Gig0/1 (inside)	88	10.2.88.30/24
	Gig0/2 (DMZ2)	168	10.2.68.30/24
	Gig0/3 (DMZ3)	78	10.2.78.30/24
IPS	Management	78	10.2.78.15/24
ACS		100	10.1.1.100/24
AD		100	10.1.1.101/24



1.0 ASA Firewalls (16 points)

Task 1.1: ASA2 Configuration (4 Points)

- Configure ASA2 according to the IP addressing table and the diagram
- Configure the host name to be ASA2
- Enable ARP inspection on outside interface and specify that packets that do not exactly match a static ARP entry are dropped
- Configure ACLs so that any ICMP & ICMPv6 traffic is permitted through the ASA
- Ensure you are able to ping between routers R5, R7 and R10
- Ensure EIGRP and OSPFv3 adjacencies come up

NOTICE: this question 1.1 depends on the configuration of Question 3.1 "Cisco IPS section" which requires configuration of Cisco IPS inline on the inside network as shown in diagram.

Task 1.2: ASA3 Setup (4 Points)

- Configure ASA3 according to the IP addressing table below and the diagram above
- Configure the host name to be ASA3
- Configure ACLs so that any ICMP traffic is permitted on any interface through the ASA
- You must configure an inbound access-list for inside interface (specific)
- Configure OSPF area 50 on inside interface
- You must authenticate OSPF neighbors using MD5 with key "1" and the password "ipexpert"
- Configure EIGRP AS 55 on ASA2 on the outside interface
- You must authenticate EIGRP neighbors using MD5 and the password "ipexpert"
- Ensure you are able to ping R6 from ASA3
- Ensure that you are able to ping R6 from R1, R2 and IPS

NOTICE: this question 1.1 depends on the configuration of Question 3.1 "Cisco IPS section" which requires configuration of Cisco IPS inline on the inside network as shown in diagram

ASA3	10.2.58.30/24	outside	0
ASA3	10.2.78.30/24	DMZ3	60
ASA3	10.2.68.30/24	DMZ2	50
ASA3	10.2.88.30/24	inside	100

Task 1.3: NAT (4 Points)

- A web server (10.3.68.1) is configured on loopback 2 of R1. Configure ASA3 such that the server is seen on the outside interface of ASA3 as 10.2.58.1
- On the same server IP address an telnet service is also running on port 3021, configure ASA3 such that incoming telnet traffic (port 23) is redirected to the telnet server on port 3021
- Configure ASA3 to translate 10.2.108.0/24 network behind the outside interface of ASA3
- Configure static translation on ASA3 for ACS server (10.1.1.100) to 10.2.58.100 on the outside network
- Verify that CAT2 can ping the original IP address of ACS server from its interface VLAN108
- Configure ASA3 such that R1 for its interface F0/0, R2 for its interface Gi0/1 and R4 for its interface s0/0/0.2 are not translated when they connect to R7 on interface F0/1, but are translated respectively to 10.2.58.31, 10.2.58.32 and 10.2.58.34 for all others outside destinations
- You are authorized to add two static routes on the ASA to achieve this task
- To test ping reachability from CAT2 to ACS server you are allowed to add a static route on the ACS

Task 1.4: Redundant Interface (4 Points)

- Configure the interfaces Ethernet 0/0 and Ethernet 0/2 of ASA2 as members of the redundant interface 1, so that you have the following output :

```
ASA2(config)# sh int red 1 | be Information
  Redundancy Information:
        Member Ethernet0/2(Active), Ethernet0/0
        Last switchover at 16:38:50 UTC May 27 2013
```

2.0 IOS Firewall (4 points)

Task 2.1: CBAC (4 Points)

- After recent network security internal issues, you have been requested to secure connection to VLAN 38 by implementing CBAC using the following parameters :
    - Treat the link to VLAN 38 as the inside; Internet interface as the outside
    - Allow TCP and UDP sessions initiated from the inside to return into the outside interface and generate alert and audit messages
    - Permit outside PC host to connect via SSH and Telnet to CAT4 for management and inspect this traffic. Log and enable alerts for these two protocols
    - Idle TCP sessions should timeout after 30 minutes
    - UDP sessions should be timed out after 180 seconds

3.0 Cisco IPS and Content Security (12 points)

Task 3.1: IPS Initialization (4 Points)

- Configure the IPS according to the diagram and IP Addressing table
- Allow the networks 10.2.48.0/24, 10.2.78.0/24 and 10.2.118.0/24 to manage the IPS
- Configure two inline interfaces pairs using the interfaces GigabitEthernet0/0 and GigabitEthernet0/1 as Pair1 and GigabitEthernet0/2 and GigabitEthernet0/3 as Pair2
- Create a second virtual sensor named vs1
- Inline Pair1 should be configured to be used by vs0 sensor
- Inline Pair2 should be configured to be used by vs1 sensor
- Configure Anomaly Detection Configuration, Signature Definition Configuration and Event Action Rules Configuration according to the table below
- Configure IPS to be managed through HTTP (no encryption) on port 8181
- Enable telnet on the IPS

Inline interface pair	Pair1	Gi0/0 Gi0/1	vs0	sig0	ad0
Inline interface pair	Pair2	Gi0/2 Gi0/3	vs1	sig1	ad1

Task 3.2: Signatures (4 Points)

- Configure IPS to synchronize to NTP server installed on R7 using “cisco” as authentication password
- Configure the IPS to trigger an alert in event store for traffic that generates an “ICMP echo request” and “ICMP echo reply” events. Also, start to log packets containing the attacker-victim address pair
- Configure IPS to send a detailed alert each time a signature with risk rating superior to fired. Don't take any other actions (besides what was configured under the signature itself)
- Make sure the detailed alert appears on the management console
- Ping R7 from R5 and R1 from R7 to ensure you have the alerts generated
- Do not translate any IP address to 10.2.58.0/24 network for this task

Task 3.3: Custom IPS Signature (4 Points)

- Create a custom signature with the ID 60009

- This signature should trigger when a HTTP session is initiated from IP address “10.2.18.5” to the web server on R1. The IPS will generate a High severity detailed alert
- Create another signature with ID 60010
- This signature will trigger if a Telnet session is opened from IP address “10.2.18.5” to R1. The IPS will generate a High Severity detailed alert
- When signatures 60009 and 60010 fire within a 20s interval in any order, then trigger a detailed alert and do not transmit this packet and future packets originating from the attacker address for 25 minutes
- Apply the signatures 60009, 60010 and 60011 to sensor vs0
- Do not modify ASA2 or ASA3 configuration for this task

4.0 Cisco VPN Solutions (20 points)

Task 4.1: PKI Server (4 Points)

- Create an exportable RSA key on R6 with the default key size labeled “iosca”
- Configure R6 as a IOS Server using the following parameters :
- Common name of cisco1.ipexpert.com, Locality of NY and country of US
- CRL lifetime – 24 hours
- Export key to non-volatile RAM (NVRAM) with the following parameters :
- Encryption : 3des
- Password : cisco123
- Configure R6 to synchronize its clock to NTP server on R7; configure ASA2 accordingly
- NTP password is “cisco”

Task 4.2: GETVPN (4 Points)

- R7 is configured as GETVPN key server and group members are R1 and R2
- One (1) fault has been inserted in pre-configuration files
- Configure R2 (Gi0/1) and R1 (F0/0) as GETVPN group members of the key server R7
- You are allowed to use two static routes for this task

Task 4.3: SSL VPN (4 Points)

- The IPS administrator needs to access remotely the IPS management interface in a secure way from PC host. After thorough research, SSL VPN solutions have been selected to do so
- Configure a SSL VPN access on R5 with the following parameters :
- Use a SSL certificate issued by R6, configured as a CA server in task 4.1
- Authentication : local
- Create two local accounts admin/cisco and cisco/cisco
- URL link label to access the IPS management interface is “IPS management”
- Use https://R5.ipexpert.com to access to Web VPN portal page
- After being authenticated to SSL VPN, manage the IPS through link http://127.0.0.1:8181
- Allow a maximum of ten (10) users to connect to the router through SSL VPN
- If needed NTP authentication password is “cisco” and NTP server is R7
- Make the necessary modifications on access-lists on ASA2 and ASA3 firewalls
- You are allowed to modify the PC host file to achieve this task
- Make sure that there is no authentication on console access

- Ensure that you are able to access IPS management interface after login on WebVPN
- Portal
- To make the test, change the VLAN of PC Host to VLAN 28, configure network IP address as 10.2.28.200 without a default gateway and add the following route in DOS command: route add 10.2.0.0 mask 255.255.0.0 10.2.28.23

Task 4.4: Troubleshooting Remote Access IPSec VPN (4 Points)

- An easy VPN with IPSec Dynamic Virtual Tunnel Interface have been configured on R4 to allow remote access VPN from PC host
- Two (2) faults have been inserted into R4 pre-configuration
- Correct the inserted faults and configure ASA2 and ASA3 in order to make the easy VPN connection working
- You're not authorized to modify the NAT config; also make sure that there no authentication on console access
- You should be able to ping the F0/1 interface of R4 from PC host once the VPN connection is up

Task 4.5: Troubleshooting Site-to-Site VPN (4 Points)

- A site-to-site IPSec tunnel is preconfigured on R5 to run between ASA3 on its "outside"
- interface and R5 on its Fa0/0 interface, but three (3) faults have been inserted into pre-
- configuration
- Configure ASA3 for L2L tunnel and fix the inserted faults following these guidelines :
- ISAKMP authentication is RSA-Sig. IPSec should use 3DES and SHA-1
- You are required to use certificates issued by R6 configured as a CA server
- Protected network are R5 loopback0 and CAT2 interface VLAN88
- You are not authorized to modify ASA3 outside access-list
- You are not allowed to add static route on ASA3 for this task
- You should be able to ping between CAT2 VLAN88 and R5 loopback0 from either side.
- All other IP traffic should be allowed as well

5.0 Identity Management (16 points)

Task 5.1: ACS Management (4 Points)

- Create a new password policy for ACS Administrators :
- Password must be at least 6 character long and must be changed every 30 days
- It cannot contain words “cisco” or “nimda” or their characters in reversed order
- At least one alphabetic and numeric character must be part of the password
- Disable account after 3 unsuccessful login attempts
- Create a new password policy for Users :
- Password must be at least 6 character long
- It cannot contain words “cisco” or “nimda” or their characters in reversed order
- At least one alphabetic and numeric character must be part of the password
- Generate a self-signed certificate for ACS Management (only) with CN=ACS-Mgmt and O=IPexpert. Hashing function used should be SHA-1 and key size used 1024 bits
- Create a new Administrator “ReadConfig” password “IPexpert123”
- This user should be only able to read ACS configuration without the ability of configuring anything
- Restrict management connections to the ACS to only Test PC 10.2.28.200
- Make sure Test PC 10.2.28.200 can access the ACS

Task 5.2: Remote Management (4 Points)

- Configure ASA3 so that users connecting using SSH will be authenticated using TACACS.
- Use “ipexpert” as the TACACS+ password. On ACS, configure the user “adminssh” with the password “IPexpert123”
- Also, configure CAT3 for telnet access such that :
- The first session will authenticate with only password for EXEC (“ipexpert”)
- The second sessions will be prompted for username and password on ACS server – username “admincat3” and password “IPexpert123” using TACACS+
- The third session will be authenticated locally. Use “adminloc” with password for this purpose “ipexpert”
- No matter what session was used to access the device a user should be able to connect to the Privileged-EXEC mode using password “ipexpert”
- From R2 start a SSH session on ASA3 inside interface and verify that you are connected with “adminssh”
- From R2 start a telnet session on CAT3 and verify that you are prompted for password only. Then start another telnet session and verify that you are authenticating with the user: “admincat3” from ACS server

- Establish again a third session and verify that you are connecting using the account: “adminloc” with password: ipexpert

Task 5.3: Proxy Authentication - IOS (4 Points)

- Configure R4 (F0/1) to perform auth-proxy when candidate PC is trying to manage the IPS on URL link: http://10.2.78.15:8181
- Configure the auth-proxy banner to say “IPS management authentication”
- Configure a auth-proxy cache time of 10 minutes
- Use interface F0/1 of R4 for RADIUS client
- Create a username : adminips and password : IPexpert123
- After successful authentication access to the IPS should be granted
- To test the IPS management access through the auth-proxy, change the VLAN of PC Host to VLAN 118, configure network IP address as 10.2.118.200 without a default gateway and add the following route in DOS command: route add 10.2.0.0 mask 255.255.0.0 10.2.118.4

Task 5.4: Lightweight Directory Access Protocol - IOS (4 Points)

- After a major migration by system administrators, a new powerful Microsoft LDAP server has been installed in your company so, you have been asked to authenticate and authorize incoming VPN users on the ASA3 according to the following parameters :
- LDAP server IP : 10.1.1.101
- LDAP Administrator : Administrator
- LDAP Administrator password: IPexpert123
- Finance department (Group) : CN=FINANCE,CN=Users,DC= ipexpert,DC=com
- Technical department (Group): CN=IPx_Admins,CN=Users,DC= ipexpert,DC=com
- Finance users (e.g. FINUSER1//cisco) should be assigned to the ASA3 group policy “FINANCE”
- Technical users (e.g. IPx_admin1//IPexpert123) should be assigned to the ASA3 group policy “ADMIN”
- Deactivate the LDAP server after 4 failed attempts to authenticate to the LDAP server; the reactivation will occurs after 30 seconds
- Add a static route on the AD server so it can talk to the ASA

6.0 Advanced Security (16 points)

Task 6.1: Resource Protection (4 Points)

- Configure R6 to stamp log messages with a sequence number
- Configure R6 to display up to 7200 messages an hour on console
- Configure R1 to accept management traffic only through interface F0/0
- Configure R1 to accept only SSH as management protocol - do not configure lines or access-list to do that
- Configure R1 to log all incoming management traffic from VLAN68, every 20 seconds
- Ensure that you have SSH access to R1 from R4

Task 6.2: Troubleshooting NTP (4 Points)

- For time synchronization purposes, an NTP server has been configured on R7
- R1, R2 and R4 have been configured as NTP clients but they will not synchronize with R7
- There were few faults introduced to their config and you are supposed to fix them
- NTP authentication password is “cisco”
- Do not modify any NTP or NTP-related configuration on the time server R7

Task 6.3: Control Network Flooding Using MQC (4 Points)

- After the IT department has experienced a huge TCP flooding on ACS server, it has been determined that attacks came from CAT4
- Therefore, the managing IT director asked you to drop all TCP requests from CAT4 toward the ACS
- Configurations for this task should be done only on R5 and R2 (on both routers)
- Dropping packets should be done only on R2 GigabitEthernet0/0 interface
- Do not apply an access-group on any interface for this task

Task 6.4: IOS NAT (4 Points)

- The network administrator has asked to be authorized to manage CAT4 from his home, so you have been asked to configure the access with the following guidelines :
- Only SSH and Telnet access is authorized from IP address 10.2.38.200 and 10.2.28.200
- Configure R6 such as when PC host attempts connection to VLAN38, its IP address is translated to 10.2.38.200

- Configure CAT4 such that it will respond also to requests directed to IP address 10.2.38.34
- Configure R6 such that IP address 10.2.38.34 will be seen always as 10.2.18.34 on outside interface for SSH and Telnet protocols
- Create a local account for testing purposes on CAT4 : username : “admin” with password “ipexpert”
- From PC host issue a SSH session to CAT4 and then do a “who” command to ensure that the connected IP address is 10.2.38.200
- From PC host issue a SSH session to IP address 10.2.18.34 and then a “who” command to ensure that the connected IP address is 10.2.28.200
- For the test, change the VLAN of PC Host to VLAN 28, configure network IP address as 10.2.28.100 without a default gateway and add the following route in DOS command: route add 10.2.0.0 mask 255.255.0.0 10.2.28.23

7.0 Attack Mitigation (16 points)

Task 7.1: Filtering Malicious Traffic (4 Points)

- It's been found out that spoofed addresses are initiating sessions from behind R5
- You have been asked to filter this traffic within these guidelines :
- All configurations should be done on F0/1 interface of R5
- Path to the source IP address must be through the same interface as that on which the packet arrived
- Router should be allow to ping its own interface IP
- Packets sourced from 10.1.1.0/24 subnet arriving at F0/1 and failing the anti-spoofing check are logged and dropped
- Packets sourced from 172.16.1.0/24 subnet arriving at F0/0 and failing the anti-spoofing check are logged and forwarded

Task 7.2: Preventing Network Attacks (4 Points)

- After dealing with huge DoS attack that leads to crash ASA2, your manager asked you to configure ASA2 in order to meet the following requirements :
- ASA should send a Syslog message when the number of denied packets by denial by access-lists is up to 300drops/second over the last 15 minutes
- Another Syslog should be sent when the number of dropped packets caused by an incomplete session, is up to 500drops/second with a burst of 2000drops/second over the last 20 second period
- ASA2 should automatically shun detected attackers from host performing a scan, except for hosts on the 10.2.0.0/16 network
- Do not use Modular Policy Framework or ACL to configure this task

Task 7.3: Layer 2 Attacks (4 Points)

- Configure CAT3 to block any Ethernet traffic on VLAN268 that is originating from and destined to 0015.C5B7.818C MAC address
- A DHCP server will be connected to the switch on port G1/0/14
- Configure DHCP snooping on VLAN268
- Configure ARP inspection on VLAN268
- Another VLAN is to be added in the future to the network (399) along with two servers which will be made part of that VLAN
- Those servers will be connected to ports F0/20 and F0/21 on CAT1 and they should not be able to talk to each other at L2

- Make sure no matter what type of the traffic server #1 sends will not be received by the
- second server and vice-versa

Task 7.4: RA Spoofing (4 Points)

- Your security policy states that the only legitimate source of RA messages in VLANs 48, 148, 158 & 208 should be R5
- Configure R5 and R7 to implement this policy
- Disable Router Advertisements on R7 and R10
- NTP password is “cisco”
- Use R10 as a CA; cert signatures should be created with SHA-1
- Make sure R10 will be still able to communicate with R5 and R7 using IPv6

Lab 4

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

It is recommended to create your own diagram at the beginning of each lab so any potential information you find useful during your preparations can be reflected on this drawing, making it much easier when you step into the real lab. You may add static routes on your Test PCs, AD Server, ISE, ACS and WSA to reach any networks.

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

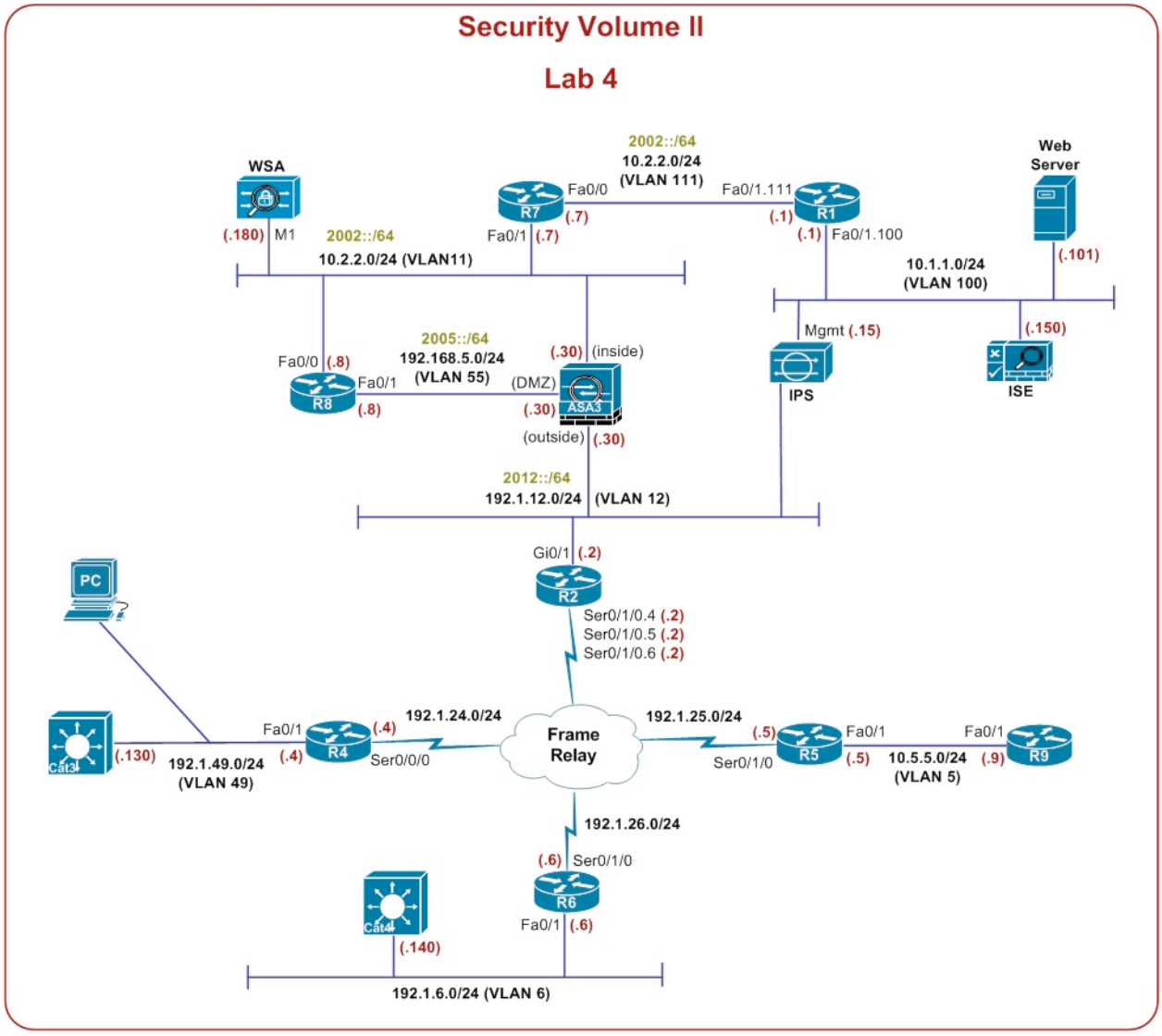
NOTE: Unicast static/default routes are NOT allowed (except on Test PCs, AD server, ISE, ACS and WSA) unless otherwise stated in the task
NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device
NOTE: Unless explicitly prohibited in a section, you may permit ICMP for connectivity testing
NOTE: Any reference to a password that is not defined should use "ipexpert"

Estimated Time to Complete: **8 Hours**

Pre-setup

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

Device	Port	VLAN	IP Address
R1	Fa0/1.100	100	10.1.1.1/24
	Fa0/1.111	111	10.2.2.1/24 2002::1/64
	Loopback0		1.1.1.1/8
R2	Gi0/1	12	192.1.12.2/24 2012::2/64
	Serial0/1/0.4		192.1.24.2/24
	Serial0/1/0.5		192.1.25.2/24
	Serial0/1/0.6		192.1.26.2/24
	Loopback0		2.2.2.2/8
R4	Fa0/1	49	192.1.49.4/24
	Serial0/0/0		192.1.24.4/24
	Loopback0		4.4.4.4/8
R5	Fa0/1	5	10.5.5.5/24
	Serial0/1/0		192.1.25.5/24
	Loopback0		5.5.5.5/8
R6	Fa0/1	6	192.1.6.6/24
	Serial0/1/0		192.1.26.6/24
	Loopback0		6.6.6.6/8
R7	BVI		10.2.2.7
R8	Fa0/0	11	10.2.2.8 2002::8/64
	Fa0/1	55	192.168.5.8/24 2005::8/64
	Loopback0		8.8.8.8/8
R9	Fa0/1	5	10.5.5.9/24
	Loopback0		9.9.9.9/8
ASA3	outside	12	192.1.12.30/24 2012::30/64
	inside	11	10.2.2.30/24 2002::30/64
	DMZ	55	192.168.5.30/24 2005::30/64
Cat3	VLAN49	49	192.1.49.130/24
Cat4	VLAN6	6	192.1.6.140/24
IPS	Management	100	10.1.1.15/24
WSA	M1	11	10.2.2.180/24
ISE		100	10.1.1.150/24
Web Server		100	10.1.1.101/24
PC		49	192.1.49.200



1.0 ASA Firewalls (15 points)

Task 1.1: ASA3 Configuration (4 Points)

- Configure ASA3 as per the diagram and table above
- Create a sub-interface off of G0/0 interface, G0/0.55
- The subinterface should belong to VLAN 55. The main interface belongs to the outside
- VLAN. Assign the new sub-interface a name of DMZ and a security level of 55
- Configure the switch to allow the ASA to communicate to the rest of the network
- Assign IP addresses to the Interfaces
- The inside interfaces should account for redundancy

Task 1.2: Failover and ASA routing (4 Points)

- Configure IP & IPv6 default route on the ASA3 pointing towards R2
- Configure a static route for the network behind R1
- Configure ASA4 as a failover device for ASA3
- Once the devices are synchronized the output should match as per below :

```
ASA3/act(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: FAIL GigabitEthernet0/3.98 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 2 seconds, holdtime 10 seconds
Interface Policy 1
Monitored Interfaces 3 of 114 maximum
Version: Ours 8.6(1)2, Mate 8.6(1)2
Last Failover at: 18:23:14 UTC Jun 9 2013
        This host: Primary - Active
                Active time: 3955 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
This host: Primary - Active
                Active time: 4321 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                Interface outside (192.1.12.30/fe80::30): Normal
(Monitored)
                Interface DMZ55 (192.168.5.30/fe80::30): Normal
(Monitored)
```

```
                Interface inside (10.2.2.30/fe80::30): Normal (Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/8.6(1)2) status (Up Sys)
                Interface outside (192.1.12.31/fe80::31): Normal
(Monitored)
                Interface DMZ55 (192.168.5.31/fe80::31): Normal
(Monitored)
                Interface inside (10.2.2.31/fe80::31): Normal (Monitored)
                slot 1: IPS5515 hw/sw rev (N/A/7.1(4)E4) status (Up/Up)
                  IPS, 7.1(4)E4, Up

Stateful Failover Logical Update Statistics
        Link : STATE GigabitEthernet0/3.99 (up)
Stateful Obj    xmit       xerr       rcv        rerr

--- OUTPUT TRUNCATED ---
```

Task 1.3: NAT (4 Points)

- Configure PAT on ASA3 for all RFC 1918 networks
- Addresses should be translated to the outside interface IP
- R1 is configured with Loopback125 and has an IP Address 195.1.1.1/24. This is a network with a public address
- Allow this network to go out without getting translated
- R2 should be able to ping this network. You are allowed a static route on R2 and the ASA to accomplish this step
- Create a static NAT entry for the AAA server at 10.1.1.150. Translate it to 192.1.12.150
- Allow R2 Gi0/1 interface to communicate with ISE using RADIUS
- Create a static NAT entry for R1 Fa0/1.111 10.2.2.1. Translate it to 192.1.12.1

Task 1.4: Management Access (3 Points)

- Configure ASDM access to the ASA
- Only allow access to users in VLANs 11 and 100
- Authenticate as “ipexpert” with password “ipexpert”
- Use local database for authentication

2.0 IOS Firewall (8 points)

Task 2.1: IOS Firewall (4 Points)

- Inspect all TCP, UDP, and ICMP traffic going towards the Frame networks on R5
- Only allow relevant traffic coming in
- ACL should be set to inbound on the Serial interface
- Log all session based information, but do not log suspicious activity for ICMP
- Set the maximum embryonic connections per host to 75 and block for 15 minutes if this limit is exceeded

Task 2.2: Transparent Firewall (4 Points)

- Configure R7 as a zone-based transparent Firewall between VLAN 11 (outside) and VLAN 111 (inside). Deny all ICMP traffic, other than Echo and Echo Reply. Allow all other traffic
- Ensure any DHCP traffic is forwarded without inspection
- Log all session based information
- Limit the amount of inspected sessions per class to 125
- Police the allowed ICMP inbound traffic to 56k, using the minimum burst value

3.0 Cisco IPS and Content Security (24 points)

Task 3.1: Basic IPS (4 Points)

- Configure the IPS Sensor's Management Interface through the CLI to allow access to the Sensor from VLAN 100 based on the Network Diagram
- Make sure you ping the IPS from R1 and manage the IPS via HTTPS port 4433
- You would like to monitor all traffic received in VLAN 12
- Configure the switches to copy all relevant traffic to the monitoring port G0/0
- Assign G0/0 to virtual sensor 0 and set G0/2 as an alternate reset interface

Task 3.2: Signatures (4 Points)

- Create a new virtual sensor called vs1, while also cloning the existing policy objects to create sig1, rules1 and ad1 that will be assigned to that sensor
- Using interface G0/1 create a VLAN pair between VLAN 11 and R7
- Use VLAN 211 as the additional VLAN for R7
- Configure the signatures so you can see a similar output on IPS CLI :

```
IPS# show events alert

evIdsAlert: eventId=1041379286523809524 severity=informational vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 413
  time: 2013/06/10 12:06:56 2013/06/10 12:06:56 UTC
  signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
    subsigId: 0
    marsCategory: Info/AllSession
  interfaceGroup: vs1
  vlan: 211
  participants:
    attacker:
      addr: locality=OUT 10.2.2.1
    target:
      addr: locality=OUT 192.1.12.2
```

```
        os: idSource=unknown relevance=relevant type=unknown
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
    threatRatingValue: 35
    interface: ge0_1
    protocol: icmp


evIdsAlert: eventId=1041379286523809525 severity=informational vendor=Cisco
    originator:
      hostId: IPS
      appName: sensorApp
      appInstanceId: 413
    time: 2013/06/10 12:06:56 2013/06/10 12:06:56 UTC
    signature: description=ICMP Echo Request id=2004 created=20001127 type=other
version=S1
      subsigId: 0
      marsCategory: Info/AllSession
    interfaceGroup: vs0
    vlan: 0
    participants:
      attacker:
        addr: locality=OUT 192.1.12.1
      target:
        addr: locality=OUT 192.1.12.2
        os: idSource=unknown relevance=relevant type=unknown
    riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 35
    threatRatingValue: 35
    interface: ge0_0
protocol: icmp
```

Task 3.3: Custom IPS Signature (3 Points)

- For vs0 create a custom string signature that detects the word “cmd.exe” anywhere in a HTTP URL. Allow for any case in the string
- Set the Alarm Severity to High, and reset the TCP connection
- When R2 does a broadcast DNS lookup, signature 4620 fires on the IDS sensor.
- Configure R2 to not send DNS broadcasts. Also, disable signature 4620 on the IDS sensor

Task 3.4: ASA IPS (3 Points)

- Configure the ASA to send message to the SYSLOG server 10.1.1.190
- Configure Console Logging to level 4. Configure Trap logging level to debugging
- Configure ASA3 IPS with the following parameters :
- Send an alarm for Info signatures
- Send an alarm and drop packets for Attack signatures
- Enable the IPS sensing on the outside interface of the ASA
- There are a large amount of false positives for DNS Zones Transfers, prevent these alarms from being generated regardless of the port used

Task 3.5: WSA Setup (4 Points)

- Configure WSA interfaces according to the topology & addressing table
- Initialize Web Security Appliance with the following settings :
    - Use 10.1.1.101 as the NTP and DNS server
    - Password MUST BE SET TO “ironport”
    - Use a single interface for management and proxy functions
    - Web Reputation should be disabled
    - Disable McAfee and Webroot scanning engines
- Set default gateway to ASA3
- Make sure Test PC in VLAN 100 can manage WSA

Task 3.6: WSA Advanced Configuration (6 Points)

- Integrate WSA with the AD Server. The domain name is “IPEXPERT.COM”
- Use “Administrator” with password “IPexpert123” to join the domain
- Enable End-User Notifications
- Create a custom Policy which ensures that access to the following websites/domains never requires authentication :
- update.microsoft.com (domain)
- windowsupdate.com (domain)
- mirrorlist.centos.com (domain)
- mirror.centos.org (server)
- Configure WSA to limit the overall bandwidth for downloaded content to 50Mbps
- All Media applications except QuickTime should be limited to 5Mbps each (don’t set a limit for QuickTime)
- Restrict users who try to upload files through WSA :
- A maximum size of uploaded files should be 2Mbps for HTTP/HTTPs and 10Mbps when they use FTP

- Microsoft Office docs can be only uploaded when they are smaller than 1Mb
- PDF files should never go through the WSA

4.0 Cisco VPN Solutions (14 points)

Task 4.1: IKEv2 Remote Access (5 Points)

- ASA3 should act as a IPSec Remote Access gateway for clients connecting from
- the outside
- IKEv2 should be the protocol used for tunnel negotiation
- Use the following parameters when configuring the VPN :
- R8 should act as a CA for the ASA
- AnyConnect clients should authenticate as “ipexpert” with password “ipexpert”
- Only VLANs 11 and 100 should be reachable via the tunnel
- Assign the connecting clients an IP address from the following pool : 172.30.30.10 – 172.30.30.20
- DNS server should be 10.1.1.101 and the domain is “ipexpert.com”

Task 4.2: L2L (4 Points)

- Encrypt traffic between R4 & R8 using the following parameters :
- Authentication is PSK
- Use default policy for the ISAKMP parameters
- Use ESP-AES192 for encryption and ESP-SHA-HMAC for Data Authentication
- Use the tunnel network 10.4.8.0/24
- The VPN should not use GRE or crypto maps
- VLAN 100 should be able to reach VLAN 49 over the tunnel
- You can use one static routes on R4 and one on R8 to accomplish this
- Make sure R1 does not learn the default route from R8

Task 4.3: GETVPN (5 Points)

- Configure GET VPN between R5 & R6 with R2 as the Key Server
- Use the following parameters :
- Authentication is pre-shared key
- Use AES, SHA, DH5 for Phase 1
- Use ESP-AES256 for encryption and ESP-SHA-HMAC for data authentication
- Rekeying should use multicast transport type
- Rekey should occur every 10 minutes using AES 192
- Encrypt ICMP traffic between R9 Loopback 0 and CAT4

5.0 Identity Management (12 points)

Task 5.1: IPv6 Initialization (2 Points)

- Configure G0/1 on ISE for IPv6
- ISE should learn the IPv6 prefix from R1
- Use 2100::/64

Task 5.2: Proxy Authentication (5 Points)

- The AAA server is located at 10.1.1.150. It communicates to the ASA using RADIUS and a key of “ipexpert”
- All outbound Telnet and HTTP Requests have to authenticate against the AAA server, same as a custom application that uses TCP port 4515
- Allow R2 to telnet into R1 F0/1.111 only after successful authentication - use virtual telnet with an IP address of 192.1.12.99
- The username to use is “cutproxy” with a password of “ipexpert”. Use the same username and password for all authentication attempts and don’t download an ACL for outbound access

Task 5.3: Port Authentication (5 Points)

- Port G1/0/12 on CAT3 should be configured for 802.1x
- Only two devices are allowed to connect through this port – a Phone and PC
- Enable RADIUS Profiling along with Device Sensor feature
- Enable SNMP Query Profiling
- Authenticated user (“dot1xuser”, password “ipexpert”) should be placed into VLAN 5; MAB-authenticated Phone should go into Voice VLAN 499
- Unless the port is authenticated no user traffic should be allowed through it
- After authentication allow IP access to VLAN 49 and TFTP
- Also the connecting user’s station should obtain an IP address via DHCP
- Protect RADIUS communication with key “IntoDarkness”

6.0 Advanced Security (16 points)

Task 6.1: BGP (4 Points)

- Authenticate all iBGP peerings using MD5 authentication with a password of “ccie”
- Configure eBGP peering between R1 and R2 through the ASA
- R1 sees R2 as 192.1.12.2 and R2 should see R1 on AS1 as 1.1.1.1
- Authenticate this peering same way as iBGP
- Two Static routes are allowed for this task

Task 6.2: BGP Traffic Filtering (4 Points)

- R5 should be receiving the following routes from the R9 :
- 199.99.99.0 /24
- Devices within your topology should see the route learned from R9 with a next hop of 192.0.1.5, and if traffic is directed to these networks, it should be silently dropped locally
- You can add four static routes in this task

Task 6.3: Management (4 Points)

- CAT4 has a management interface belonging to VLAN 6
- Allow management access to this switch from VLANs 5 & 6 only
- VLAN 5 should see CAT4 as 192.1.16.140
- This NAT should be carried out on R6
- Configure SSH on R2
- SSH authentication should be done locally
- Create a user „admin” with a password of “cisco”
- Allow Management traffic (SSH/Telnet/HTTP/HTTPS) to Interface Gi0/1 only, logging dropped packets. Do not use ACLs to accomplish this

Task 6.4: DHCP (4 Points)

- Enable R2 as a DHCP Server with the following information :
- IP ADDRESS : 192.1.49.0/24
- WINS ADDRESS : 192.1.49.135
- DNS ADDRESS : 192.1.49.53
- DEFAULT GATEWAY : 192.1.49.4
- LEASE TIME : 6 Days
- Enable DHCP Relay function on R4 F0/1 (so it forwards DHCP requests to R2)
- Configure CAT2 for DHCP snooping for R2
- Rate Limit DHCP packets to R2 to 50pps

7.0 Attack Mitigation (11 points)

Task 7.1: IP Options Attacks (2 Points)

- On R4 do not allow packets with IP options - do not use an ACL for this
- R6 should drop any IP packets containing the timestamp & IP Option 82 from the frame cloud
- Log all packets with any other IP Option

Task 7.2: TCP SYN Floods (3 Points)

- The 192.1.6.0 network is experiencing SYN attacks from the Frame cloud to your web servers (HTTP and HTTPs)
- R6 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets
- Limit TCP intercept to only watch packets coming from 192.1.26.0, 192.1.24.0 or the 192.1.25.0 networks for Web traffic towards R6
- Configure TCP intercept such that the router drops embryonic connections if they reach 1050. It should stop dropping the embryonic connections once the number reaches 850

Task 7.3: Fragmentation & L2 Attacks (3 Points)

- Configure R6's FastEthernet interface to block inbound non-initial fragments with a destination of R2's G0/1
- Log those fragments and make sure information about source MAC address of the device sending fragments is also included
- Other traffic should not be affected
- Prevent VLAN Hopping attacks on CAT2 Port F0/2
- Prevent a MAC Flooding attack on CAT4 Port G1/0/1. Allow no more than 2 MAC addresses, and ensure that learned MAC's are saved to startup config

Task 7.4: IPv6 Attacks (3 Points)

- Make sure the ASA only allows one ICMPv6 Reply to come in for every single Request being allowed to go through
- Block and log all IPv6 fragments flowing through the ASA's inside interface
- Don't use Virtual Reassembly to accomplish this
- Drop IPv6 fragments received on R8's F0/0 interface

Lab 5

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

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

Multiple topology drawings are available for this chapter.

General Rules

- You will need to pre-configure the network with the base configuration files

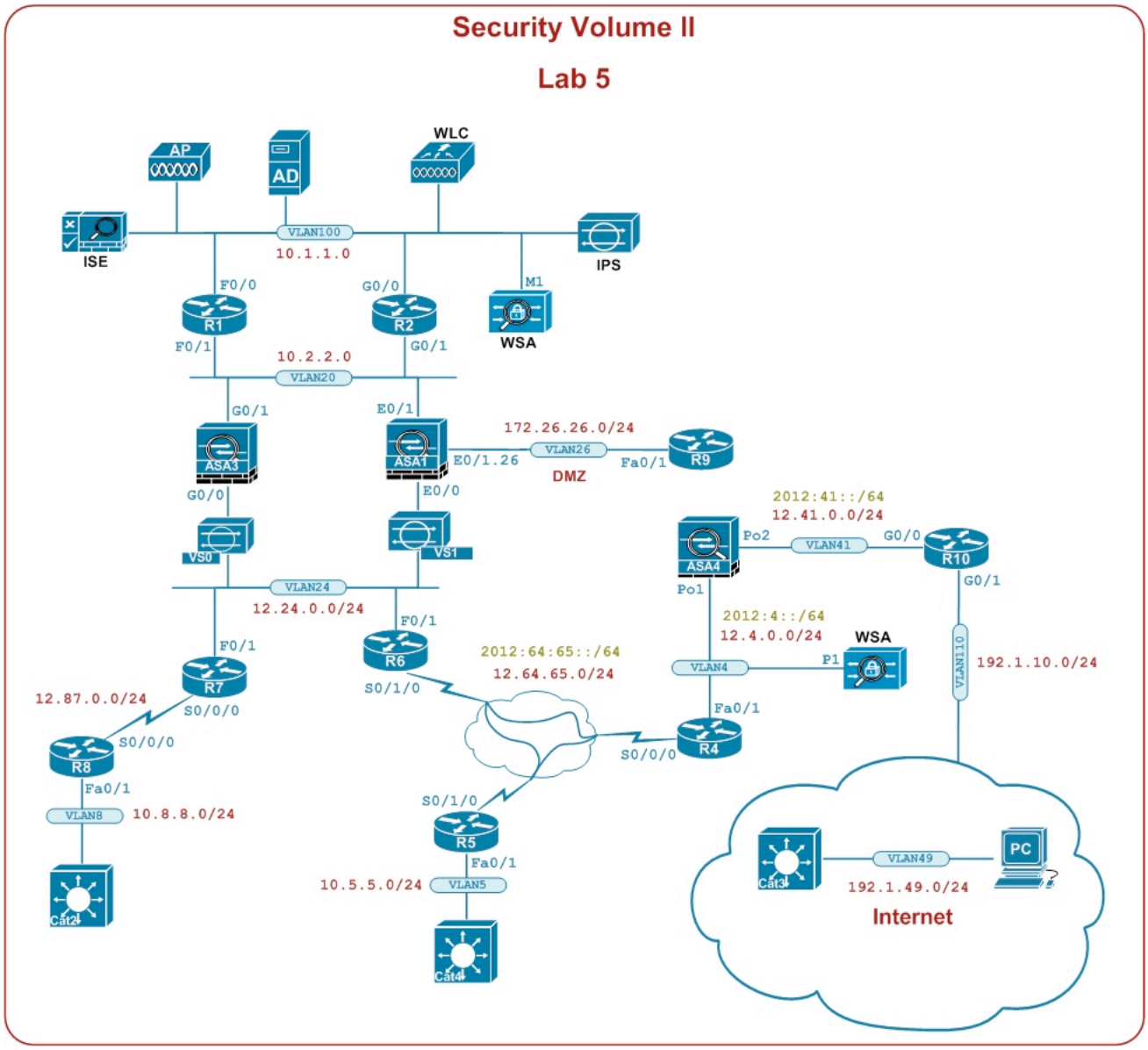
NOTE: Unicast static/default routes are NOT allowed (except on Test PCs, AD server, ISE, ACS and WSA) unless otherwise stated in the task
NOTE: Unless otherwise noted in the task you can add user "cisco" pw "cisco" to the local database to test management access to the device
NOTE: Unless explicitly prohibited in a section, you may permit ICMP for connectivity testing
NOTE: Any reference to a password that is not defined should use "ipexpert"

Estimated Time to Complete: **12 Hours**

Pre-setup

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

Device	Port	VLAN	IP Address
R1	FastEthernet0/0	100	10.1.1.1/24
	FastEthernet0/1	20	10.2.2.1/24
	Loopback0		1.1.1.1/32
R2	GigabitEthernet0/0	10	10.1.1.2/24
	GigabitEthernet0/1	20	10.2.2.2/24
	Loopback0		2.2.2.2/32
R4	FastEthernet0/1	4	12.4.0.4/24 2012:4::4/64
	Serial0/0/0		12.64.65.4/24 2012:64:65::4/64
	Loopback0		4.4.4.4/32
R5	Serial0/1/0		12.64.65.5/24 2012:64:65::5/64
	FastEthernet0/1	5	10.5.5.5/24
	Loopback0		5.5.5.5
R6	FastEthernet0/1	24	12.24.0.6/24
	Serial0/1/0		12.64.65.6/24 2012:64:65::6/64
	Loopback0		6.6.6.6/32
R7	FastEthernet0/1	24	12.24.0.7/24
	Serial0/0		12.87.0.7/24
	Loopback0		7.7.7.7/24
R8	FastEthernet0/1	8	10.8.8.8/24
	Serial0/0		12.87.0.8/24
	Loopback0		8.8.8.8/32
R9	FastEthernet0/1	26	172.26.26.9/24
	Loopback0		9.9.9.9/32
R10	G0/0 G0/1	41 110	12.41.0.10/24 2012:41::10/64 192.1.10.10/24
ASA1	Ethernet0/0 - outside	24	12.24.0.10/24
	Ethernet0/1 - inside	20	10.2.2.10/24
	Ethernet0/1.26 – DMZ(sec 50)	26	172.26.26.10/24
ASA3	G0/0 - outside	24	12.24.0.30/24
	G0/1 - inside	20	10.2.2.30/24
ASA4	Po1 - inside Po2 - outside	4 41	12.4.0.40/24 2012:4::40/64 12.41.0.40/24 2012:41::40/64
Cat2	FastEthernet0/22 (DHCP)	8	10.8.8.120/24
Cat3	FastEthernet0/23	4	192.1.49.130/24
Cat4	VLAN5	5	10.5.5.140/24
ISE	Student NIC	100	10.1.1.150/24
AD	Student NIC	100	10.1.1.101/24
IPS	Mgmt	100	10.1.1.15/24
WSA	M1 P1	100 4	10.1.1.180/24 12.4.0.180/24
WLC	Port1 (G0/0)	100	10.1.1.250/24



1.0 ASA Firewalls (21 points)

Task 1.1: ASA Basic Configuration (2 Points)

- Configure ASA1 and ASA3 IP addressing according to the lab diagram and Lab 2 Addressing Table
- Modify any of the switches necessary to ensure that you can ping all of the directly connected devices from both ASA1 and ASA3
- You may allow ICMP for testing through the ASAs

Task 1.2: ASA4 Setup (3 Points)

- Configure ASA4 according to the IP addressing table and directions below
- Interfaces G0/0 and G0/1 should be bundled into a single logical link
- Interfaces G0/2 and G0/3 should form another logical link
- This configuration should provide fault tolerance and traffic load-balancing capabilities
- ASA's first bundle should load-balance traffic according to source & destination port numbers
- CAT4 should load-balance based on source IP address
- Don't use any negotiation protocol to accomplish this task
- Enable inspection of ICMP traffic

Task 1.3: ASA Routing (5 Points)

- Configure OSPF on ASA1 and ASA3
- ASA3 should be the primary route out of the internal network
- ASA1 should be the secondary route out of the network
- Inject a default route into the internal network
- Do not pass internal routes to R7 and R6
- Make sure that the routing updates are secured using the most secure method available
- Advertise the DMZ network into the inside network but not the outside
- Configure EIGRP on ASA4
- Secure routing protocol updates
- Configure R4 so OSPF and EIGRP domains can communicate with each other
- Ensure the firewall has full IPv6 reachability – you can add a single static route

Task 1.4: Advanced ACLs and NAT (4 Points)

- In the near future your company will be installing a new server located at 10.1.1.160

- The Server will only support SSH and HTTP
- Ensure that this server is seen as 12.24.0.160 for SSH and traverses ASA3
- For HTTP ensure that this server appears to be 12.24.0.60 and traverses ASA1
- Configure HTTP access to the loopback of R9. This address should be translated to 12.24.0.9
- Allow telnet into R9's f0/1 interface. This should also appear to be 12.24.0.9
- There are additional servers that will be accessed by organizations from the Internet (192.1.49.0/24). The IP Addresses of these servers are as follows :
    - 172.26.26.80
    - 172.26.26.22
    - 172.26.26.25
    - 172.26.26.161
    - 172.26.26.110
- The last octet of the server is also the service that should be allowed to it. Do this with one ACL statement to the outside interface on the ASA. Allow connections from "any" source address. Do this by adding only a single line to the outside ACL
- You may add 1 static route to complete this task

Task 1.5: ASA MPF (4 Points)

- Internal users should use ASA3 to get to the Internet
- They should be translated to the address pool rage 12.24.0.112-126
- Ensure that you do not stop allocating addresses if the pool is saturated
- Make sure that they cannot access www.juniper.com, www.myspace.com, and www.facebook.com during business hours
- Business hours are Monday through Friday from 8 am to 5pm and Saturday from 9 am to 2 pm
- The policy should only apply to the inside interface.
- You can use Test PC for verification of this task. Create host entries to these three websites pointing to R7 Loopback0. When completed http://7.7.7.7 should work but http://www.juniper.com and the others should be unsuccessful

Task 1.6: Advanced ASA Configuration (3 Points)

- Rate Limit all ICMP traffic to the ISE server via ASA3 (NAT ISE to 12.24.0.150)
- Traffic exceeding 8000 BPS should be dropped
- Configure Secure Logging to the ISE Server on ASA1. Make sure that traffic flows if the Syslog server is down and ensure timestamps are sent
- Deny ICMP Echo Requests on the outside interface of ASA3. The ASA should still be able to ping and traceroute

2.0 IOS Firewall (8 points)

Task 2.1: Cisco IP Session Filtering (3 Points)

- Configure R8 for firewall services
- You may not use CBAC or IOS Zone Based Firewall technologies in this task
- Watch all TCP, ICMP and UDP traffic from the private network to the public network and allow for its return
- Make sure that all networks in the topology cannot see the real addresses of vlan 8

Task 2.2: Cisco IOS Firewall (5 Points)

- It's been decided that R4 will be configured as an additional line of defense against outside attacks. Configure the Firewall with the following parameters :
    - Fa0/1 is the outside zone
    - S0/0/0 is the inside zone
    - Allow all pertinent traffic from the outside to the inside zone
    - Inspect TCP and UDP out of the network
    - Pass and Log all ICMP
    - Log dropped packets
- Internal server 10.1.1.160 is running an ERP application on TCP port 51000. Make sure this is allowed and inspected as a custom application
- Ensure that TCP half-open sessions on your internal devices are aggressively dropped if they reach a total of 800 connections and that aggressive dropping stops when the number of connections falls below 400. Do this within a 1 minute period also
- All TCP-based sessions initiated from the outside should be session-logged

3.0 Cisco IPS and Content Security (24 points)

Task 3.1: IPS Initialization (2 Points)

- Initialize the IPS sensor with the IP addressing listed in Lab 2 Address Table
- HTTPS management should be done via port 8888
- Allow the 10.1.1.0/24 and 10.21.21.0/24 network to manage the appliance
- Create a banner that says: “Welcome to IPexpert!”

Task 3.2: Virtual Sensors (3 Points)

- Use two Virtual Sensors, vs0 and vs1
- Configure vs1 to be inline between ASA1 and VLAN 24
- Configure vs0 to be inline between ASA3 and VLAN 24
- Configure the switches as needed
- Enable the ICMP echo and echo reply signatures on both sensors but only configure it once
- The signatures should fire a medium severity event
- Verify events are generated by both virtual sensors

Task 3.3: Custom IPS Signature (4 Points)

- It’s been determined that an attack may occur that is seen by a correlation of 5 separate signatures. These signatures are not enabled by default and determining when each of these 5 signatures fired within a specific period of time is not an option with the overwhelming amount of information IT is collecting
- Configure Signatures 3221, 3222, 3223, 3224 and 3225 as a compound signature
- The event should fire if 5 of the signatures fire within 90 seconds in the following order :
    - 3225
    - 3222
    - 3224
    - 3223
    - 3221
- The alert Severity should be high and the attacker should be denied inline

Task 3.4: IOS IPS (4 Points)

- Configure R8 to enable IPS inbound on the Serial Interface
- The Signature file located in flash should be used
- Enable the signature for ICMP Echo Request
- When completed you should obtain the following results :

```
R6#ping 8.8.8.8 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4
ms

R8#sh ip ips statistics
Signature statistics [process switch:fast switch]
  signature 2004:0: packets checked [0:100] alarmed [0:100] dropped
[0:0]
Interfaces configured for ips 1
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
Last statistic reset never
TCP reassembly statistics
  received 0 packets out-of-order; dropped 0
  peak memory usage 0 KB; current usage: 0 KB
  peak queue length 0
```

Task 3.5: WSA Basic Setup (3 Points)

- Configure WSA interfaces according to the topology & addressing table
- Use 10.1.1.101 as the NTP and DNS server
- Password MUST BE SET TO “ironport”
- Use a separate interface for management and proxy functions

Task 3.6: WSA Configuration (3 Points)

- Enable Transparent Proxy for HTTP on WSA
- ASA4 should redirect all HTTP packets received on its inside interface destined to port 80 to WSA
- Integrate the Proxy with AD Server 10.1.1.101
- Use “Administrator” // “IPexpert123” to join IPEXPERT.COM domain

Task 3.7: Guest Access & Policies (5 Points)

- Your company has a very strict security policy – access to all websites should be blocked by default along with any FTP requests
- Only authenticated employees (group IPX_EMP) located in VLAN 24 should be granted full HTTP access and FTP connections to the Internet but according to the policy below :
    - When they try to use search engines that don’t support Safe Search function, this should be blocked
    - WSA should display a warning when Adult-Oriented Content is tried to be accessed on YouTube
    - Native FTP connections should be allowed to transfer data in Active mode if Passive mode fails
- Any VLAN 24 client who fails authentication should be only given Guest Access to www.guestportal.com hosted on R10 – this site is trusted and all other security features should be bypassed for it
- Also when “Guests” try to connect to any server in the ipexpert.com domain they should be redirected to CAT3 – all other websites should be blocked
- Log Guest access based on the name entered by the user
- User “IPXEMP1”, password “cisco”, is part of the IPX_EMP group on AD

4.0 Cisco VPN Solutions (26 points)

Task 4.1: GET VPN Key Server (5 Points)

- Configure R1 as the GET VPN Key Server
- R6, R5, and R4 should register with this server
- The Policy should Apply Encryption to traffic that flows from 10.66.x.x to 10.66.x.x and to 172.27.x.x (as well as between 172.27.x.x)
- Rekey Using Multicast Group address 239.1.66.66
- You may add a tunnel interface on R1 using the IP address 10.101.101.1 if needed
- The Replay Counter Window size should be set to 64
- Use Pre-shared keys for ISAKMP. You may use a wildcard for the address on the KS only
- The ISAKMP & IPSec Policies should reflect the following :
    - ISAKMP AES 128 encryption
    - ISAKMP DH Group 2
    - IPSec AES 128 encryption
    - IPSec MD5 Hash
- Use ASA3 for access to the Key Server

Task 4.2: GETVPN over DMVPN Troubleshooting (5 Points)

- R6 is a DMVPN Hub
- R5 and R4 are DMVPN Spokes
- R6, R5, and R4 are all GET VPN Group Members
- R1 is the KS that was configured in the last task
- You can add a single static route in this task
- Fix any issues with the GET VPN or DMVPN Configuration on the Group Members such
- that you obtain the following results :

```
R1#sh cry gdoi
GROUP INFORMATION

    Group Name               : GET (Multicast)
    Group Identity           : 1
    Group Members            : 3
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 83725 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : GET_PROF
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 926 secs
      ACL Configured         : access-list
GET_ENCRYPT

     Group Server list       : Local
```

```
R1#sh cry gdoi ks mem

Group Member Information :

Number of rekeys sent for group GET : 0

Group Member ID    : 12.64.65.4
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 12.64.65.5
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0

Group Member ID    : 12.64.65.6
 Group ID          : 1
 Group Name        : GET
 Key Server ID     : 0.0.0.0
```

```
R6#sh cry gdoi gm

Group Member Information For Group GET:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GET_temp_acl

    Group member            : 12.64.65.6       vrf:
None
        Registration status   : Registered
        Registered with       : 1.1.1.1
        Re-registers in       : 3418 sec
        Succeeded registration: 1
        Attempted registration: 1
        Last rekey from       : 1.1.1.1
        Last rekey seq num    : 0
        Multicast rekey rcvd  : 2
```

```
R5#sh cry gdoi gm acl
Group Name: GET
 ACL Downloaded From KS 1.1.1.1:
   access-list  permit ip 10.66.0.0 0.0.255.255 10.66.0.0
0.0.255.255
   access-list  permit ip 10.66.0.0 0.0.255.255 172.27.0.0
0.0.255.255
   access-list  permit ip 172.27.0.0 0.0.255.255 10.66.0.0
0.0.255.255
   access-list  permit ip 172.27.0.0 0.0.255.255 172.27.0.0
0.0.255.255

 ACL Configured Locally:
```

```
R4#sh cry gd gm

Group Member Information For Group GET:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_GET_temp_acl

    Group member             : 12.64.65.4       vrf:
None
       Registration status   : Registered
       Registered with       : 1.1.1.1
       Re-registers in       : 3393 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 1.1.1.1
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 2
```

Task 4.3: IKEv2 L2L (5 Points)

- Configure a site-to-site VPN tunnel between ASA3 and ASA4
- Use the new version of IKE protocol for negotiation
- Protect VLANs 20, 100 and 41
- Use SHA-256 for IKE tunnel and SHA-1 to secure data traffic

- Authentication method must be Pre-Shared Key (“ipexpert”)
- You can add two static routes on the ASA4
- Block access to WSA M1 interface through the tunnel
- You should be able to ping R1 from R10 after finishing this task

Task 4.4: ASA Remote Access VPN (6 Points)

- Configure ASA4 for EasyVPN with external group parameters as follows :
    - DNS Server = 10.1.1.101
    - Tunneling Protocol = IPSec
    - IPSec-Authentication = RADIUS
    - IPSec Banner = “You are on the Private Network!”
    - Split Tunneling for 10.1.1.0/24 and 10.2.2.0/24
    - The user ezuser should be locked into the group EZVPN
    - The address pool should be 10.3.3.10-20 and the assignment of the pool should come from the RADIUS Server (ISE)
    - The external group-policy is EZPOL with password “IPexpert123”
- Create a user on ISE with the username ezuser and password of “IPexpert123”
- All the user VPN attributes should come through RADIUS
- RADIUS traffic should be encrypted and authenticated through the public & WAN networks
- The VPN connections will be coming from the Internet
- You can add one static route for this task

Task 4.5: ASA SSL Clientless VPN (5 Points)

- Configure ASA1 for clientless SSL VPN connections from Internet on port 4443
- The User (“ssluser” with password “IPexpert123”) should be authenticated via RADIUS with ISE and he/she should be able to do the following :
    - Enter URLs
    - Telnet to R1
    - See a drop down list of groups to authenticate to
- The Group Policy should be configured locally but assigned by ISE Server and this way override the default Group Policy on the ASA

5.0 Identity Management (15 points)

Task 5.1: ISE General Setup (3 Points)

- Create a new password policy for ISE Administrators :
  - Password must be at least 6 character long
  - It cannot contain words “cisco” or “nimda” or their characters in reversed order
  - At least one alphabetic (Upper & Lower -case) and numeric character must be part of the password
  - Disable account after 3 unsuccessful login attempts
- Create a new password policy for Users :
  - Password must be at least 6 character long
  - It cannot contain words “cisco” or “nimda” or their characters in reversed order
  - At least one alphabetic (Upper & Lower –case) and numeric character must be part of the password
  - Password must be different from the previous one
- Generate a Certificate Signing Request (CSR). Use CN of ISE-Podxxx where xxx is your pod number, Organization should be set to “IPexpert” and Organizational Unit to “Instructors”
- Create a repository for backups. Use TFTP
- Files will be stored on 10.1.1.99 under ISE-BACKUPS directory

Task 5.2: ISE Administrative Access (3 Points)

- Configure a new Administrator (“CustomAdmin”, password “IPexpert123”) who will be able to see all Identity Groups and all Network Devices
- Read/write access to any other Menus & Data should be denied
- Restrict management access to ISE to IP address you are using to connect to the device and VLAN 100 subnet

Task 5.3: Wireless 802.1x (6 Points)

- Initialize WLC with a management IP address according to the addressing table
- Username MUST be “**admin**” and password MUST be set to “**IPexpert123**”
- Configure WLC to act as a DHCP Server for VLANs 100 (AP) and VLAN 20 (clients) – a pool of ten or so IP addresses will suffice in both cases
- Create WLAN “Corp-Access-xxx” where xxx is your pod number
- This wireless network should only grant access to 802.1x-authenticated users
- Users who successfully pass authentication should end up in VLAN 20 and be able to reach all 12.x.x.x networks via ASA3
- Use ISE as a source of authentication and authorization information

- Authenticate with user “wireless” password “IPexpert123”
- Secure RADIUS communication using password “ipexpert”

Task 5.4: Access Control (3 Points)

- On R9 Create a view called “limited”
- This view should be accessed by any user that telnets into R9 and uses the username “limited” with a password “cisco”
- The user should automatically be placed in the view
- Make sure that the user can only enter the following commands :
    - Show clock
    - Show ip interface brief
- The console should not be affected

6.0 Advanced Security (4 points)

Task 6.1: FPM (4 Points)

- Create an FPM policy on R6 that matches the following :
  - IP
  - TCP port 80
  - Offset 0
  - Size 32
  - Downloaded filename (using GET method) starts with “%”
- This should be applied to Fa0/1 and dropped and logged if detected

7.0 Attack Mitigation (2 points)

Task 7.1: IP Address Spoofing Protection (2 Points)

- Configure the ASA4 such that it prevents anyone on the outside from spoofing the internal Network
- Configure R8 for RFC2827 filtering on the Serial interface, however do not configure an ACL to do this. You should be as strict as possible
- On R8 the IPS should not fire off signature 1102 when you test to yourself