IEWB-SC-VOL2 Lab 1

Difficulty Rating (10 highest): 7

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/en/US/support/index.html.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information and routing protocols configuration.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the IPS sensor is either cisco/cisco or cisco/ciscoids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.INE.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
ASA Firewall	24
IOS Firewall	9
VPN	17
Identity Management	15
Ctrl/Mgmt Plane Security	7
IPS	14
Advanced Security	7
Network Attacks	7

GOOD LUCK!

1. ASA Firewall

1.1. ASA Addressing

- Configure the IP addresses for the inside (E0/1) and the outside (E0/0) interfaces of the ASA1 according to the diagram provided and using the last octet value of ".12".
- Configure RackXASA as the unit's hostname.

2 Points

1.2. ASA OSPF Routing

- Configure OSPF area 51 between the ASA SW2, and BB2.
- The ASA should advertise a default route to its OSPF neighbors.
- This default route should be valid only if the ASA can reach R5.

4 Points

1.3. Stateful Failover

- Configure ASA1 as the primary failover unit and ASA2 as the secondary.
- Use the DMZ interface (E0/2) on both units for stateful LAN failover; you are allowed to create an additional VLAN for this task.
- Use any IP addresses for ASA2 and the failover link.
- Configure so that only the outside interface is monitored.
- Interface failure should be detected with the minimum delay possible.

3 Points

1.4. Address Translation

- Allow the users behind the ASA firewall to access the rest of the network.
- You should use the firewall's IP address to accomplish this task.

2 Points

1.5. Modular Policy Framework

- Permit returning ICMP packets that are sent in response to outbound ICMP packets across the ASA failover pair. Do not configure an access-list entry to accomplish this.
- Allow for a maximum of 5000 simultaneous TCP connections and 1000 UDP connections; per-host limits should be 1000 and 500 for TCP/UDP respectively.
- Permit TCP Option 19 to be used in TCP connections.

3 Points

1.6. Traffic Policy

- Configure the ASA firewall so that SW2 is translated to the IP address 183.X.125.8 on the outside interface.
- Configure the ASA firewall to permit inbound **`ping`**, **`traceroute`** (UNIX variant), and telnet traffic to the protected networks.
- Make sure that **`traceroute`** responses do not reveal the inside addresses for translated subnets.
- Configure the ASA to limit ICMP traffic rate on the outside interface to 56Kbps.

4 Points

1.7. Traffic Management

- Users on the inside of the ASA have complained that they are unable to do **`traceroute`** to IP addresses on the outside.
- Configure the ASA to allow the inside users to successfully **`traceroute`** to the outside destinations.
- Only use only a single line ACL to accomplish this.
- Assume the UNIX variant of **`traceroute`** is in use.

2 Points

1.8. Port Redirection

- Configure the ASA to redirect inbound telnet sessions terminated on the outside interface to BB2.

2 Points

1.9. Destination NAT

- After the recent incorrect changes being made to the company's DNS server a host in VLAN 125 with the IP address of 183.X.125.200 now incorrectly resolves to 183.X.125.20.
- To resolve this problem in the interim configure the ASA to redirect packet going to 183.X.125.20 to the true IP address.
- Do not use the **`static`** command to achieve this task.

2 Points

2. IOS Firewall

2.1. Zone-Based Firewall

- Recently it was discovered that hosts behind BB3 were attempting to gain access to one of the company's main file servers. In order to prevent this problem in the future your manager has requested that R1 be secured according to the following requirements:

    - Treat interface connected to BB3 as the outside zone and the Frame-Relay connection as the inside zone.
    - Allow TCP and UDP sessions initiated from the inside to the outside.
    - Permit HTTP and HTTPS access to an internal web server with the IP address of 183.X.46.100
    - Permit **`traceroute`** replies coming into the outside interface
    - Drop all other traffic

- Use Zone-Based Firewall feature to accomplish this task.

4 Points

2.2. Traffic Filtering

- In order to reduce filtering overhead on R1 your manager has requested that all packets destined to TCP port 139 be dropped prior to reaching R1's connection to BB3.
- Do not make any changes to R1's configuration to accomplish this task.

2 Points

2.3. Traffic Filtering

- The network administrator has voiced concerns that R6's connection to BB1 is not secure, and would like to only allow packets in from BB1 that were initiated from behind R6.
- Configure R6 to monitor TCP and UDP traffic as it flows out its interface to BB1 and dynamically permit the return packets inbound.
- Statically permit the BGP peering session with BB1 and ICMP echo-replies inbound.
- All other traffic should be silently dropped.
- Do not use any stateful inspection technology to accomplish this and expire inactive session in two minutes.

3 Points

3. VPN

3.1. Overlapping Addressing Space

- The network administrator has requested that the network be configured to allow communication between hosts in VLAN 4 and 41.
- Hosts in VLAN 4 should appear to be in the 10.4.4.0/24 network to hosts in VLAN 41.
- Hosts in VLAN 41 should appear to be in the 10.7.7.0/24 network to hosts in VLAN 4.
- The use of static routes is permitted for this task.

3 Points

3.2. IPsec VPN

- Create a LAN-to-LAN VPN between VLAN 4 and 41 over the Frame Relay cloud on R3 and R4 using the following parameters:

    - ISAKMP Authentication Method: RSA-SIG
    - ISAKMP Hash: MD5
    - ISAKMP Encryption: 3DES
    - CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
    - ESP Encryption: AES-256
    - ESP Authentication: HMAC-MD5

- This configuration should continue to function if R4 loses its connection to the Frame Relay cloud.

3 Points

3.3. Easy VPN Server

- Configure R2 to support VPN connections for Cisco's EzVPN client as outlined below:

    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: SHA
    - ISAKMP Encryption: 3DES
    - ESP Encryption/Hash: 3DES/ HMAC-SHA
    - Address Pool: 192.168.0.1-192.168.0.50
    - Group Name: IELAB
    - Group Password: CISCO
    - DNS/WINS Server: 183.X.46.100
    - Domain: ine.com

- Allow for split tunneling to destinations not in the 183.X.0.0/16 network.
- Configure the router to probe for the dead remote peer every 10 seconds.
- Configure R2 to inject the VPN client's IP address into its routing table to ensure IP reachability; do not use a manual static route for this task.
- Use the VTI feature to accomplish this task.

3 Points

3.4. IPsec VPN

- Create a LAN-to-LAN VPN on the R5 and ASA between the 10.8.8.0/24 and the 10.5.5.0/24 subnets using the following parameters:

    - ISAKMP Authentication Method: Pre-Shared
    - ISAKMP Hash: MD5
    - ISAKMP Encryption: 3DES
    - ESP Encryption: 3DES
    - ESP Authentication: HMAC-MD5

- Configure the ASA such that hosts in the 10.8.8.0/24 subnet can not ping hosts in the 10.5.5.0/24 subnet through this VPN tunnel.
- You are allowed to use one static route to accomplish this task.

3 Points

3.5. VPN QoS

- The maximum available bandwidth in the path between the ASA and R5 is 2Mbps.
- Configure a QoS policy in the ASA to limit overall VPN traffic bandwidth such that the transit path does not become oversaturated.
- Additionally provide priority treatment for voice packets which are routed through the VPN tunnel to R5.
- Assume that VoIP traffic has been pre-marked with the DSCP value of EF.

3 Points

3.6. VPN QoS

- Configure the IPsec LAN-to-LAN tunnel on R5 such that a QoS policy applied to its Frame Relay interface is able to recognize and classify IPsec tunneled traffic.

2 Points

4. Identity Management

4.1. Service Authentication

- Recently a W32.Blaster.Worm variant infected Windows servers located in VLAN 255 and propagated itself to other servers using TCP port 135.
- In order to stop the spread of the worm, but still permit legitimate TCP port 135 traffic, users will be required to authenticate to the ASA prior to being permitted out of VLAN 255 on TCP port 135.
- Configure the ASA to require users to authenticate by opening an HTTP connection to 192.10.X.100 and entering the username USER1 along with the password of CISCO prior to permitting TCP port 135 connections through.
- The ASA should authenticate this user against the AAA server.

3 Points

4.2. Authentication Proxy

- When users in VLAN 46 need to connect on TCP port 135 through R4 these users should be required to create a HTTP connection to R4 and authenticate prior to R4 permitting the TCP port 135 traffic through.
- R4 should only allow TCP port 135 connections inbound on the Frame-Relay interface for sessions that have been authenticated.
- R4 should use TACACS+ with the AAA server for authenticating these sessions.
- Users will be authenticating using the username TCP135 along with the password of CISCO.

3 Points

4.3. Authorization & Accounting

- The network administrator would like to enable NOC users to perform basic administrative tasks on R5 according to the following requirements:
    - Authenticate telnet sessions using the username NOC and the password CISCO
    - This authentication should occur against the local username and password database
    - The NOC user's password should be stored as an MD5 hash in R5's configuration
    - Place the NOC user in privilege level 5 upon logging in
    - Do not use the **`username`** command with **`privilege`** option or the **`privilege level`** line command for this task
    - Give the NOC user access to the **`clear line`** and **`clear counters`** commands
- Account for the privilege level 5 commands using TACACS+ with the AAA server
- Source the TACACS+ session off R5's Loopback 0 interface

3 Points

4.4. 802.1x Authentication

- In order to improve security in the access layer of the network your security team has suggested that hosts connecting to the network should use 802.1x username and password authentication. In order to test out this setup before deploying it network-wide a Windows® XP host has been connected to port Fa0/17 of SW1.
- The Windows® XP host will be sending the username HOST and a password of CISCO.
- Configure SW1 to forward this authentication request on to the RADIUS server at 10.0.0.100.
- If authentication is successful the host should be allowed access to the network; if authentication fails the host should be placed into VLAN 200.
- If a clientless host connects, is should be placed into VLAN201.
- SW1 should authenticate to the RADIUS server using the password CISCO and should send the authentication request using the source IP address 150.X.7.7.

3 Points

4.5. 802.1x Authorization

- Configure SW1 and the ACS server so that a host authenticating with the credentials “HOST”/”CISCO” is assigned into VLAN 255 automatically.

3 Points

5. Control/Management Plane Security

5.1. OSPF Authentication

- Authenticate all OSPF adjacencies within area 0 using a secure hash value of the password CISCO.
- The OSPF adjacency between R3 and R5 should use a hash value based off the password CISCO35.
- The OSPF adjacency between R4 and R5 should use a hash value based off the password CISCO45.

2 Points

5.2. SNMP

- Configure the ASA for SNMP management using the community string “CISCO”.
- Configure the firewall to send all SNMP IPsec traps to the AAA/CA server; do not permit this host to poll the ASA firewall via SNMP.
- In addition to this configure the firewall to send all critical syslog messages and below to the e-mail address admin@ine.com.
- Use the AAA/CA server for SMTP transactions and send e-mails from the address asa-lab1@ine.com.

3 Points

5.3. VTP Security

- Configure the VTP domain CCIE_SECURITY between SW1 and SW2.
- Authenticate the VTP domain with the password CISCO.

2 Points

6. IPS

Read the access instructions for the IPS Sensor in the introduction for this lab prior to starting this section.

6.1. IPS Sensor Initialization

- Configure the IP address for the command and control interface of the IPS according to the diagram provided.
- Configure RackXIPS as the sensor's hostname.
- Disable the IPS's telnet server.
- The IPS should use the R1 as its default gateway.

2 Points

6.2. Traffic Monitoring

- Only allow management of the IPS sensor via HTTPS from the IP addresses 204.12.X.200 and 10.0.0.100.
- Configure the HTTPS server to listen on port 10443 and use the HTTP server-id "IPS Web Server".
- Configure the IPS to inspect the traffic captured from VLAN125. Use a dedicated virtual sensor to process just this VLAN's traffic.
- You should be able to monitor the IPS sensor using the IPS Manager Express application in the AAA server.

3 Points

6.3. Shunning

- Configure a manual block on the IPS sensor to deny all packets inbound on the outside interface of the ASA sourced from 183.X.46.120.
- This manual blocking rule should never timeout.

3 Points

6.4. Telnet Traffic Monitoring

- The network administrator would like to be notified whenever someone changes a password through a telnet connection.
- Create a custom signature to trigger an alarm of maximum fidelity and high severity whenever a telnet session contains the strings “password” or “Password”.

3 Points

6.5. IOS IPS

- In addition to your manager's earlier request to secure R6's connection to BB1 your manager has requested that R6 perform intrusion detection inbound on this interface.
- Configure R6 to meet the following requirements:

    - Log alarms to a syslog server located at 10.0.0.100
    - Retire all signatures with except to "IOS IPS Basic" category.
    - Enable the ICMP echo and ICMP echo reply signatures.
    - Assign the mission-critical TVR to the network 183.X.46.0/24

3 Points

7. Advanced Security

7.1. Syslog

- The network administrator has requested that R4 be configured to log all messages with a severity of 6 and below messages to the syslog server located at 10.0.0.100.
- To help guard against tampering with the syslog messages on the server itself R4 should include a sequence number with each log message.

2 Points

7.2. Secure Access

- A new corporate policy dictates that management through the CLI on R4 and R6 be performed using SSH and telnet access should be disabled.
- Users will be connecting using the username SSH along with the password CISCO.
- Only allow SSH connections sourced from any 183.X.0.0/16 IP address.

2 Points

7.3. QoS Features for VPN

- Configure a QoS policy on R5's VLAN125 interface to limit the VPN traffic to 2Mbps.
- Ensure that voice traffic flowing through the VPN tunnel at R5 is given priority treatment up to 128Kbps.
- Assume that VoIP packets are marked with the DSCP value of EF.
- Your configuration should only affect the tunneled traffic.

3 Points

8. Network Attacks

8.1. Remotely Triggered Blackhole

- An attacker behind the backbone routers is flooding your network with packets sourced from spoofed source addresses.
- The ultimate target of the attacks is a server with the IP address 183.X.37.200 located in VLAN37.
- Configure your BGP routers to filter out this traffic at the edge of your network.
- Set up R2 as a “trigger” router using BGP AS number 100 and instruct “edge” routers (R1 and R6) to drop the offending packets.
- You are allowed to configure static routes to Null0 at R1, R2 and R6 for this task.

4 Points

8.2. Traffic Sinkhole

- In order to assist with attack analysis, configure R2 to track the entry points (border routers) of the packets involved in the attack.
- The network 112.0.0.0/8 is suspected to be the main source of the attack; divert packets destined for this network to the sinkhole router.
- You should be able to monitor “ICMP unreachable” messages for dropped packets at R4 by using the **`show logging`** CLI command;
- Every single packet should be logged.
- You are allowed to configure a static route to Null0 on R2 for this task.

3 Points