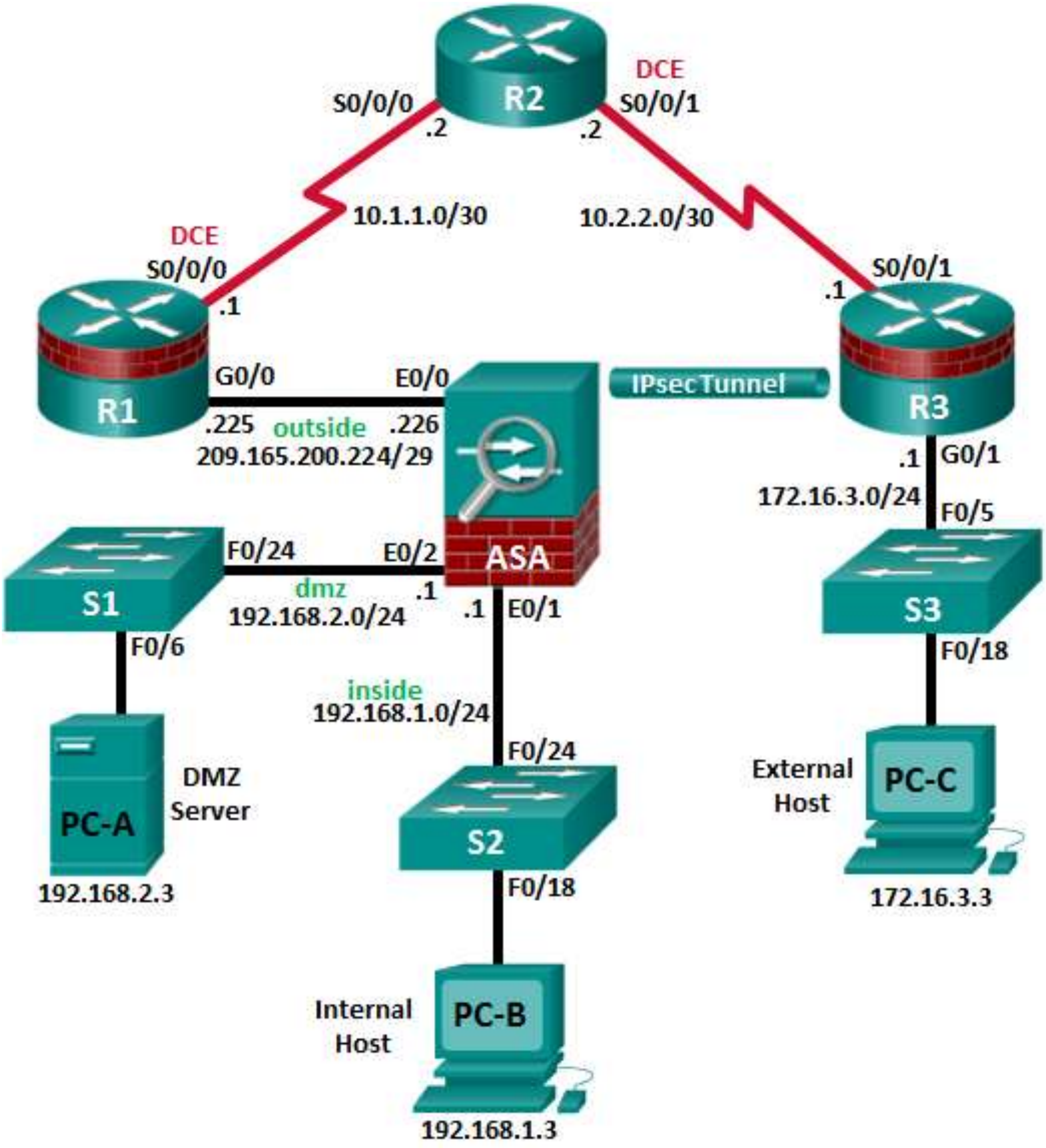
CCNA Security

Chapter 11 - CCNA Security Comprehensive Lab

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
	Loopback 1	172.20.1.1	255.255.255.0	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
S1	VLAN 1	192.168.2.11	255.255.255.0	192.168.2.1	N/A
S2	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1	N/A
S3	VLAN 1	172.16.1.11	255.255.255.0	172.30.3.1	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	N/A	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	N/A	R1 G0/0
	VLAN 2 (E0/2)	192.168.2.1	255.255.255.0	N/A	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Create a Basic Technical Security Policy

Part 2: Configure Basic Device Settings

Part 3: Configure Secure Router Administrative Access

- Configure encrypted passwords and a login banner.
- Configure the EXEC timeout value on console and VTY lines.
- Configure login failure rates and VTY login enhancements.
- Configure Secure Shell (SSH) access and disable Telnet.
- Configure local authentication, authorization, and accounting (AAA) user authentication.
- Secure the router against login attacks, and secure the IOS image and the configuration file.
- Configure a router NTP server and router NTP clients.
- Configure router syslog reporting and a syslog server on a local host.

Part 4: Configure a Zone-Based Policy Firewall and Intrusion Prevention System

- Configure a Zone-Based Policy Firewall (ZPF) on an ISR using the CLI.
- Configure an intrusion prevention system (IPS) on an ISR using the CLI.

Part 5: Secure Network Switches

- Configure passwords and a login banner.

- Configure management VLAN access.
- Secure access ports.
- Protect against Spanning Tree Protocol (STP) attacks.
- Configure port security and disable unused ports.

Part 6: Configure ASA Basic Settings and Firewall

- Configure basic settings, passwords, date, and time.
- Configure the inside and outside VLAN interfaces.
- Configure port address translation (PAT) for the inside network.
- Configure a Dynamic Host Configuration Protocol (DHCP) server for the inside network.
- Configure administrative access via Telnet and SSH.
- Configure a static default route for the Adaptive Security Appliance (ASA).
- Configure Local AAA user authentication.
- Configure a DMZ with a static NAT and ACL.
- Verify address translation and firewall functionality.

Part 7 Configure a DMZ, Static NAT, and ACLs on an ASA

Part 8: Configure ASA Clientless SSL VPN Remote Access Using ASDM

- Configure a remote access SSL VPN using the Cisco Adaptive Security Device Manager (ASDM).
- Verify SSL VPN access to the portal.

Part 9: Configure a Site-to-Site VPN between the ASA and ISR

- Configure an IPsec site-to-site VPN between the ASA and R3 using ASDM and the CLI.
- Activate and verify the IPsec site-to-site VPN tunnel between the ASA and R3.

Background/Scenario

This comprehensive lab is divided into nine parts. The parts should be completed sequentially. In Part 1, you will create a basic technical security policy. In Part 2, you will configure the basic device settings. In Part 3, you will secure a network router using the command-line interface (CLI) to configure IOS features, including AAA and SSH. In Part 4, you will configure a ZPF and IPS on an ISR. In Part 5, you will configure a network switch using the CLI. In Parts 7 and 8, you will configure the ASA firewall functionality and clientless SSL VPN remote access. In Part 9, you will configure a site-to-site VPN between the ASA and R3.

Note: The router commands and output in this lab are from a Cisco 1941 router with Cisco IOS Release 15.4(3)M2 (with a Security Technology Package license). The switch commands and output are from Cisco WS-C2960-24TT-L switches with Cisco IOS Release 15.0(2)SE4 (C2960-LANBASEK9-M image). Other routers, switches, and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router, or switch model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5505 with an 8-port integrated switch, running OS version 9.2(3) and the Adaptive Security Device Manager (ASDM) version 7.4(1) and comes with a Base license that allows a maximum of three VLANs.

Note: Before beginning, ensure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 1 ASA 5505 (OS version 9.2(3) and ASDM version 7.4(1) and Base license or comparable)

- 3 routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology package license)
- 3 switches (Cisco 2960 or comparable) (not required)
- 3 PCs (Windows 7 or Windows 8.1, SSH Client, and WinRadius)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

Part 1: Create a Basic Technical Security Policy (Chapters 1 and 11)

In Part 1, you will create a Network Device Security Guidelines document that can serve as part of a comprehensive network security policy. This document addresses specific router and switch security measures and describes the security requirements to be implemented on the infrastructure equipment.

Task 1: Identify Potential Sections of a Basic Network Security Policy.

A network security policy should include several key sections that can address potential issues for users, network access, device access, and other areas. List some key sections you think could be part of a basic security policy.

Task 2: Create a "Network Equipment Security Guidelines" Document As a Supplement to a Basic Security Policy

Step 1: Review the objectives from previous CCNA Security labs.

a. Open each of the labs completed from chapters 1 to 9, and review the objectives listed for each one.

b. Copy the objectives to a separate document and use it as a starting point. Focus on the objectives that involve security practices and device configuration.

Step 2: Create a "Network Device Security Guidelines" document for router and switch security.

Create a high-level list of tasks to include for network access and device security. This document should reinforce and supplement the information presented in a basic security policy. It is based on the content of previous CCNA Security labs and on the networking devices present in the course lab topology.

Note: The "Network Device Security Guidelines" document should be no more than two pages, and will be the basis for the equipment configuration in the remaining parts of the lab.

Step 3: Submit the "Network Device Security Guidelines" to your instructor.

Provide the "Network Device Security Guidelines" document to your instructor for review before starting Part 2 of this lab. You can send the document as an e-mail attachment or put it on removable storage media, such as a flash drive.

Part 2: Configure Basic Device Settings (Chapters 2 and 6)

Step 1: Cable the network as shown in the topology.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for all routers.

a. Configure hostnames, as shown in the topology.

b. Configure the interface IP addresses, as shown in the IP addressing table.

c. Configure a serial interface DCE clock rate of **128000** for the routers, if using routers other than those specified with this lab.

d. Disable DNS lookup on each router.

Step 3: Configure static default routes on R1 and R3.

a. Configure a static default route from R1 to R2 and from R3 to R2.

b. Configure static routes from R2 to the R1 simulated LAN (Loopback 1), the R1 Fa0/0-to-ASA subnet, and the R3 LAN.

Step 4: Configure basic settings for each switch.

a. Configure hostnames, as shown in the topology.

b. Configure the VLAN 1 management address on each switch, as shown in the IP Addressing table.

c. Configure the IP default gateway for each of the three switches.

d. Disable DNS lookup on each switch.

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for each PC, as shown in the IP Addressing table.

Step 6: Verify connectivity between PC-C and R1 G0/0.

Step 7: Save the basic running configuration for each router and switch.

Part 3: Configure Secure Router Administrative Access (Chapters 2 and 3)

You will use the CLI to configure passwords and device access restrictions.

Task 1: Configure Settings for R1 and R3

Step 1: Configure a minimum password length of 10 characters.

Step 2: Encrypt plaintext passwords.

Step 3: Configure a login warning banner.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says: **Unauthorized access strictly prohibited and prosecuted to the full extent of the law!**.

Step 4: Configure the enable secret password.

Use **cisco12345** as the **enable secret** password. Use the strongest encryption type available.

Step 5: Configure the local user database.

Create a local user account of **Admin01** with a secret password of **Admin01pa55** and a privilege level of **15**. Use the strongest encryption type available.

Step 6: Enable AAA services.

Step 7: Implement AAA services using the local database.

Create the default login authentication method list. Use case-sensitive local authentication as the first option and the enable password as the backup option to be used if an error occurs in relation to local authentication.

Step 8: Configure the console line.

Configure the console line for privilege level 15 access on login. Set the **exec-timeout** value to log out after 15 minutes of inactivity. Prevent console messages from interrupting command entry.

Step 9: Configure the VTY lines.

Configure the VTY lines for privilege level 15 access on login. Set the **exec-timeout** value to log out a session after **15** minutes of inactivity. Allow for remote access using SSH only.

Step 10: Configure the router to log login activity.

a. Configure the router to generate system logging messages for successful and failed login attempts. Configure the router to log every successful login. Configure the router to log every second failed login attempt.

b. Issue the **show login** command. What additional information is displayed?

Step 11: Enable HTTP access.

a. Enable the HTTP server on R1 to simulate an Internet target for later testing.

b. Configure HTTP authentication to use the local user database on R1.

Task 2: Configure the SSH Server on R1 and R3

Step 1: Configure the domain name.

Configure a domain name of **ccnasecurity.com**.

Step 2: Generate the RSA encryption key pair.

Configure the RSA keys with **1024** as the number of modulus bits.

Step 3: Configure the SSH version.

Specify that the router accept only **SSH version 2** connections.

Step 4: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive. Configure SSH timeout to **90** seconds and the number of authentication attempts to **2**.

Step 5: Verify SSH connectivity to R1 from PC-C.

a. Launch the SSH client on PC-C, enter the R1 S0/0/0 IP address (**10.1.1.1**), and log in as **Admin01** with the password **Admin01pa55**. If prompted by the SSH client with a security alert regarding the server's host key, click **Yes.**

b. Issue the **show run** command from the SSH session on PC-C. The configuration for R1 should be displayed.

Task 3: Secure against Login Attacks and Secure the IOS and Configuration File on R1

Step 1: Configure enhanced login security.

If a user experiences two failed login attempts within a **30**-second time span, disable logins for **1** minute. Log all failed login attempts.

Step 2: Secure the Cisco IOS image and archive a copy of the running configuration.

a. The **secure boot-image** command enables Cisco IOS image resilience, which hides the file from the **dir** and **show** commands. The file cannot be viewed, copied, modified, or removed using EXEC mode commands. (It can be viewed in ROMMON mode.)

b. The **secure boot-config** command takes a snapshot of the router running configuration and securely archives it in persistent storage (flash).

Step 3: Verify that your image and configuration are secured.

a. You can use only the **show secure bootset** command to display the archived filename. Display the status of configuration resilience and the primary bootset filename.

What is the name of the archived running config file and on what is the name based?

b. Save the running configuration to the startup configuration from the privileged EXEC mode prompt.

Step 4: Restore the IOS and configuration files back to the default setting.

You have verified the Secure IOS and configuration file settings. Now, use the **no secure boot-image** and **no secure boot config** commands to restore the default settings for these files.

Task 4: Configure a Synchronized Time Source Using NTP

R2 will be the master NTP clock source for R1 and R3.

Step 1: Set up the NTP master using Cisco IOS commands.

R2 is the master NTP server in this lab. All other routers and switches learn the time from it, either directly or indirectly. For this reason, you must ensure that R2 has the correct UTC set.

a. Use the **show clock** command to display the current time set on the router.

b. Use the **clock set** *time* command to set the time on the router.

c. Configure NTP authentication by defining the authentication key number **1** with **md5** hashing, and a password of **NTPpassword**. The password is case sensitive.

d. Configure the trusted key that will be used for authentication on R2.

e. Enable the NTP authentication feature on R2.

f. Configure R2 as the NTP master using the **ntp master** *stratum-number* command in global configuration mode. The stratum number indicates the distance from the original source. For this lab, use a stratum number of **3** on R2. When a device learns the time from an NTP source, its stratum number becomes one greater than the stratum number of its source.

Step 2: Configure R1 and R3 as NTP clients using the CLI.

a. Configure NTP authentication by defining the authentication key number **1** with **md5** hashing, and a password of **NTPpassword**.

b. Configure the trusted key that will be used for authentication. This command provides protection against accidentally synchronizing the device with a time source that is not trusted.

c. Enable the NTP authentication feature.

d. R1 and R3 will become NTP clients of R2. Use the **ntp server** *hostname* global configuration mode command. Use R2's serial IP address for the hostname. Issue the **ntp update-calendar** command on R1 and R3 to periodically update the calendar with the NTP time.

e. Use the **show ntp associations** command to verify that R1 has made an association with R2. You can also use the more verbose version of the command by adding the *detail* argument. It might take some time for the NTP association to form.

f. Verify the time on R1 and R3 after they have made NTP associations with R2.

Task 5: Configure Syslog Support on R3 and PC-C

Step 1: Install the syslog server on PC-C.

a. The Tftpd32 software from jounin.net is free to download and install, and it includes a TFTP server, TFTP client, and a syslog server and viewer. If not already installed, download Tftpd32 at http://tftpd32.jounin.net and install it on PC-C.

b. Run the **Tftpd32.exe** file, click **Settings**, and ensure that the **syslog serve**r check box is checked. In the **SYSLOG** tab, you can configure a file for saving syslog messages. Close the settings and in the main Tftpd32 interface window, note the server interface IP address and select the **Syslog server** tab to bring it to the foreground.

Step 2: Configure R3 to log messages to the syslog server using the CLI.

a. Verify that you have connectivity between R3 and PC-C by pinging the R3 G0/1 interface IP address **172.16.3.1**. If it is unsuccessful, troubleshoot as necessary before continuing.

b. NTP was configured in Task 2 to synchronize the time on the network. Displaying the correct time and date in syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it can be difficult to determine what network event caused the message.

   Verify that the timestamp service for logging is enabled on the router by using the **show run** command. Use the **service timestamps log datetime msec** command if the timestamp service is not enabled.

c. Configure the syslog service on the router to send syslog messages to the syslog server.

Step 3: Configure the logging severity level on R3.

Logging traps can be set to support the logging function. A trap is a threshold that triggers a log message. The level of logging messages can be adjusted to allow the administrator to determine what kinds of messages are sent to the syslog server. Routers support different levels of logging. The eight levels range from 0 (emergencies), which indicates that the system is unstable, to 7 (debugging), which sends messages that include router information.

Note: The default level for syslog is 6 (informational logging). The default for console and monitor logging is 7 (debugging).

a. Use the **logging trap** command to set the severity level for R3 to level 4 (**warnings)**.

b. Use the **show logging** command to see the type and level of logging enabled.

Part 4: Configure a Zone-Based Policy Firewall and Intrusion Prevention System (Chapters 4 and 5)

In Part 4, you will configure a ZPF and IPS on R3 using the CLI.

Task 1: Configure a ZPF on R3 using the CLI

Step 1: Creating the security zones.

a. Create the **INSIDE** and **OUTSIDE** security zones.

b. Create an inspect class-map to match the traffic to be allowed from the **INSIDE** zone to the **OUTSIDE** zone. Because we trust the **INSIDE** zone, we allow all the main protocols. Use the **match-any** keyword to instruct the router that the following **match** protocol statements will qualify as a successful match. This results in a policy being applied. Match for **TCP**, **UDP,** or **ICMP** packets.

c. Create an inspect policy-map named **INSIDE-TO-OUTSIDE**. Bind the **INSIDE-PROTOCOLS** class-map to the policy-map. All packets matched by the **INSIDE-PROTOCOLS** class-map will be inspected.

d. Create a zone-pair called **INSIDE-TO-OUTSIDE** that allows traffic initiated from the internal network to the external network but does not allow traffic originating from the external network to reach the internal network.

e. Apply the policy-map to the zone-pair.

f. Assign R3's G0/1 interface to the **INSIDE** security zone and the S0/0/1 interface to the **OUTSIDE** security zone.

g. Verify your ZPF configuration by using the **show zone-pair security**, **show policy-map type inspect zone-pair,** and **show zone security** commands.

Task 2: Configure IPS on R3 using the CLI.

Step 1: Prepare router R3 and the TFTP server.

To configure Cisco IOS IPS 5.x, the IOS IPS signature package file and public crypto key files must be available on the PC with the TFTP server installed. R3 uses PC-C as the TFTP server. Ask your instructor if these files are not on the PC.

a. Verify that the **IOS-Sxxx-CLI.pkg** signature package file is in the default TFTP folder. The *xxx* is the version number and varies depending on which file was downloaded from Cisco.com.

b. Verify that the **realm-cisco.pub.key.txt** file is available and note its location on PC-C. This is the public crypto key used by Cisco IOS IPS.

c. Verify or create the IPS directory (**ipsdir**) in router flash on R3. From the R3 CLI, display the content of flash memory and check to see if the **ipsdir** directory exists.

d. If the **ipsdir** directory is not listed, create it in privileged EXEC mode, using the **mkdir** command.

   Note: If the IPSDIR directory is listed and there are files in it, contact your instructor. This directory must be empty before configuring IPS. If there are no files in it, you may proceed to configure IPS.

Step 2: Verify the IOS IPS signature package location and TFTP server setup.

a. Use the **ping** command to verify connectivity between R3, PC-C, and the TFTP server.

b. Start Tftpd32 (or another TFTP server) and set the default directory to the one with the IPS signature package in it. Note the filename for use in the next step.

Step 3: Copy and paste the crypto key file into R3's configuration.

In global configuration mode, select and copy the crypto key file named **realm-cisco.pub.key.txt**. Paste the copied crypto key content at the global configuration mode prompt.

Note: The contents of the realm-cisco.pub.key.txt file have been provided below:

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
```

Step 4: Configure the IPS settings on R3 from the CLI.

a. Create an IPS rule, and name the rule **IOSIPS**.

b. Set the IPS Signature storage location to the **IPSDIR** directory you created in flash in step 1d.

c. Enable HTTP server and IPS SDEE event notification.

d. Configure IOS IPS to use one of the pre-defined signature categories.

   Note: When configuring IOS IPS, it is required to first retire all the signatures in the "all" category and then unretire selected signature categories.

   After you have retired all signatures in the **all** category, unretire the **ios_ips basic** category.

e. Apply the IPS rule to inbound traffic to R3's S0/0/1 interface.

Step 5: Start the TFTP server on PC-C and verify the IPS file directory.

Verify that PC-C has the IPS Signature package file in a directory on the TFTP server. This file is typically named IOS-S*xxx*-CLI.pkg. The *xxx* is the signature file version.

Note: If this file is not present, contact your instructor before continuing.

Step 6: Copy the signature package from the TFTP server to R3.

a. Use the **copy tftp** command to retrieve the signature file and load it into the Intrusion Detection Configuration. Use the **idconf** keyword at the end of the **copy** command.

   Note: Signature compiling begins immediately after the signature package is loaded to the router. You can see the messages on the router with logging level 6 or above enabled.

b. Use the **dir flash** command to see the contents of the **IPSDIR** directory you created earlier in this lab. There should be six files, as shown here.

c. Use the **show ip ips signature count** command to see the counts for the compiled signature package.

```
R3# show ip ips signature count
```

Note: You may see an error message during signature compilation, such as "%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)". The message means the public crypto key is invalid. Refer to Task 3, Configure the IPS Crypto Key, to reconfigure the public crypto key.

d. Use the **show ip ips all** command to view the IPS configuration status summary.

Part 5: Secure Network Switches (Chapter 6)

Note: Not all security features in this part of the lab will be configured on all switches. However, in a production network all security features would be configured on all switches.

Step 1: Configure basic security settings on S1

a. HTTP access to the switch is enabled by default. Prevent HTTP access by disabling the HTTP server and HTTP secure server.

Use an enable secret password of **cisco12345**. Use the strongest encryption available.

b. Encrypt plaintext passwords.

c. Configure a warning to unauthorized users with an MOTD banner that says **"Unauthorized access strictly prohibited!"**.

Step 2: Configure SSH server settings on S1.

a. Configure a domain name.

b. Configure username **Admin01** in the local database with a password of **Admin01pa55**. Configure this user to have the highest possible privilege level. The strongest encryption method available should be used for the password.

c. Configure the RSA keys with 1024 modulus bits.

d. Enable SSH version 2.

e. Set the SSH time-out to **90** seconds and the number of authentication retries to **2**.

Step 3: Configure the console and VTY lines.

a. Configure a console to use the local database for login. If the user has the highest privileges, then automatically enable privilege exec mode upon login. Set the **exec-timeout** value to log out after five minutes of inactivity. Prevent console messages from interrupting command entry.

b. Configure VTY lines to use the local database for login. If the user has the highest privileges, then automatically enable privilege exec mode upon login. Set the **exec-timeout** value to log out after five minutes of inactivity. Allow remote SSH access to all VTY lines

Step 4: Configure Port Security and Disable Unused Ports

Note: Configuration changes made in step 4 to interface F0/6 in a NETLAB+ environment may have an adverse effect on lab results because of a hidden control switch between S1 and PC-A. If you are performing this lab on a NETLAB+ pod, it is recommended that you perform configuration changes to F0/7 (an inactive port) instead of F0/6 for this step only.

a. Disable trunking on port F0/6.

b. Enable PortFast on F0/6.

c. Enable BPDU guard on F0/6.

d. Apply basic default port security on F0/6. This sets the maximum MAC addresses to 1 and the violation action to shut down. Use the sticky option to allow the secure MAC address that is dynamically learned on a port to the switch running configuration.

e. Disable unused ports on S1.

Step 5: Set loop guard as the default for all non-designated ports on S1.

Step 6: Save the running configuration to the startup configuration for each switch.

Part 6: Configure ASA Basic Settings and Firewall (Chapter 9)

Task 1: Prepare the ASA for ASDM Access

Step 1: Clear the previous ASA configuration settings.

a. Use the **write erase** command to remove the **startup-config** file from flash memory.

b. Use the **reload** command to restart the ASA.

Step 2: Bypass Setup Mode and configure the ASDM VLAN interfaces using the CLI.

a. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with **no**.

b. Enter privileged EXEC mode. The password should be blank (no password) at this point.

c. Enter global configuration mode. Respond with **no** to the prompt to enable anonymous reporting.

d. The VLAN 1 logical interface will be used by PC-B to access ASDM on ASA physical interface E0/1. Configure interface **VLAN 1** and name it **inside**. The Security Level should be automatically set to the highest level of 100. Specify IP address **192.168.1.1** and subnet mask **255.255.255.0**.

e. Enable physical interface **E0/1**.

f. Preconfigure interface **VLAN 2**, name it **outside**, assign IP address **209.165.200.226**, and the subnet mask **255.255.255.248**. Notice that the VLAN is automatically assigned a 0 as the security level.

g. Assign **VLAN 2** to the physical interface **E0/0** and enable the interface.

h. Configure VLAN 3, which is where the public access web server will reside. Assign it IP address **192.168.2.1/24**, name it **dmz**, and assign it a security level of **70**.

   Note: If you are working with the ASA 5505 base license, you will see the error message shown in the output below. The ASA 5505 Base license allows for the creation of up to three named VLAN interfaces. However, you must disable communication between the third interface and one of the other interfaces using the **no forward** command. This is not an issue if the ASA has a Security Plus license, which allows 20 named VLANs.

   Because the server does not need to initiate communication with the inside users, disable forwarding to interface VLAN 1.

i. Assign **VLAN 3** to the interface **E0/2** and enable the interface.

j. Display the status of all ASA interfaces by using the **show interface ip brief** command.

k. Display the information for the Layer 3 VLAN interfaces by using the **show ip address** command.

l. Display the VLANs and port assignments on the ASA by using the **show switch vlan** command.

Step 3: Configure and verify access to the ASA from the inside network.

a. From PC-B, ping the ASA's inside interface (192.168.1.1). Pings should be successful.

b. Use the **http** command to configure the ASA to accept HTTPS connections and to allow access to ASDM from any host on the inside network (192.168.1.0/24).

c. Open a browser on PC-B and test the HTTPS access to the ASA by entering **https://192.168.1.1**.

d. From the ASDM Welcome page, click **Run ASDM**. When prompted for a username and password, leave them blank and click **OK**.

Task 2: Configure Basic ASA Settings Using the ASDM Startup Wizard

Step 1: Access the Configuration menu and launch the Startup wizard.

At the top left of the screen, click **Configuration** > **Launch Startup wizard**.

Step 2: Configure the hostname, domain name, and the enable password.

a. On the first Startup wizard screen, select the **Modify Existing Configuration** option.

b. On the Startup Wizard Step 2 screen, configure the ASA hostname **CCNAS-ASA** and domain name **ccnasecurity.com**. Change the enable mode password from blank (no password) to **cisco12345**.

Step 3: Verify the VLAN and interface settings.

a. On the Startup Wizard Step 3 screen, do not change the current settings; these were previously defined using the CLI.

b. On the Startup Wizard Step 4 screen, verify that port **Ethernet 0/1** is allocated to inside VLAN 1 and that port **Ethernet 0/0** is allocated to Outside VLAN 2.

c. On the Startup Wizard Step 5 screen verify the Outside and Inside IP address settings are correct. Click **Next**.

Step 4: Configure DHCP, address translation, and administrative access.

a. On the Startup Wizard Step 6 screen – DHCP Server, select **Enable DHCP server on the Inside Interface** and specify a starting IP address of **192.168.1.5** and an ending IP address of **192.168.1.30**. Enter the DNS Server 1 address of **10.3.3.3** and enter **ccnasecurity.com** for the domain name. Do **NOT** check the box to enable auto-configuration from interface.

b. On the Startup Wizard Step 7 screen – Address Translation (NAT/PAT), configure the ASA to **Use Port Address Translation (PAT)** and select the **Use the IP address of the outside interface** option.

c. On the Startup Wizard Step 8 screen – Administrative Access, HTTPS/ASDM access is currently configured for hosts on the inside network (192.168.1.0/24). Add **SSH** access to the ASA for the **inside** network (**192.168.1.0**) with a subnet mask of **255.255.255.0**.

d. Finish the wizard and deliver the commands to the ASA.

Note: When prompted to log in again, leave the **Username** field blank and enter **cisco12345** as the password.

Task 3: Configuring ASA Settings from the ASDM Configuration Menu

Step 1: Set the ASA date and time.

At the **Configuration** > **Device Setup** screen, click **System Time** > **Clock.** Set the time zone, current date and time, and apply the commands to the ASA.

Step 2: Configure a static default route for the ASA.

a. At the **Configuration** > **Device Setup** screen, click **Routing** > **Static Routes**. Click the **IPv4 only** button and then add a static route for the **outside** interface. Specify **any4** for the Network and a Gateway IP of **209.165.200.225** (R1 G0/0). **Apply** the static route to the ASA.

b. On the ASDM **Tools** menu, select **Ping** and enter the IP address of router R1 S0/0/0 (**10.1.1.1**). The ping should succeed.

Step 3: Test access to an external website from PC-B.

Open a browser on PC-B and enter the IP address of the R1 S0/0/0 interface (**10.1.1.1**) to simulate access to an external website. The R1 HTTP server was enabled in Part 2 of this lab. You should be prompted with a user authentication login dialog box from the R1 GUI device manger. Exit the browser.

Note: You will be unable to ping from PC-B to R1 S0/0/0 because the default ASA application inspection policy does not permit ICMP from the internal network.

Step 4: Configure AAA for SSH client access.

a. At the **Configuration** > **Device Management** screen, click **Users/AAA** > **User Accounts** > **Add**. Create a new user named **Admin01** with a password of **Admin01pa55**. Allow this user **Full access** (ASDM, SSH, Telnet, and console) and set the privilege level to **15**. Apply the command to the ASA.

b. At the **Configuration** > **Device Management** screen, click **Users/AAA** > **AAA Access**. On the Authentication tab, require authentication for **HTTP/ASDM** and **SSH** connections and specify the **LOCAL** server group for each connection type. Click **Apply** to send the commands to the ASA.

   Note: The next action you attempt within ASDM will require that you log in as **Admin01** with the password **Admin01pa55**.

c. From PC-B, open an SSH client and attempt to access the ASA inside interface at **192.168.1.1**. You should be able to establish the connection. When prompted to log in, enter username **Admin01** and the password **Admin01pa55**.

d. After logging in to the ASA using SSH, enter the **enable** command and provide the password **cisco12345**. Issue the **show run** command in order to display the current configuration you have created using ASDM. Close the SSH session.

Task 4: Modify the Default Modular Policy Framework using ASDM.

Step 1: Modify the MPF application inspection policy.

The default global inspection policy does not inspect ICMP. To enable hosts on the internal network to ping external hosts and receive replies, ICMP traffic must be inspected.

a. From PC-B, select the ASDM **Configuration** screen > **Firewall** menu. Click **Service Policy Rules**.

b. Select the **inspection_default** policy and click **Edit** to modify the default inspection rules. In the Edit Service Policy Rule window, click the **Rule Actions** tab and select the **ICMP** check box. Do not change the other default protocols that are checked. Click **OK** > **Apply** to send the commands to the ASA.

   Note: If prompted, log in as **Admin01** with the password **Admin01pa55**.

Step 2: Verify that returning ICMP traffic is allowed.

From PC-B, attempt to ping the R1 G0/0 interface at IP address **209.165.200.225**. The pings should be successful because ICMP traffic is now being inspected.

Part 7: Configuring a DMZ, Static NAT, and ACLs (Chapter 10)

In Part 6 of this lab, you configured address translation using PAT for the inside network using ASDM. In this part, you will use ASDM to configure the DMZ, Static NAT, and ACLs on the ASA.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned (209.165.200.224/29). R1 G0/0 and the ASA outside interface already use 209.165.200.225 and .226. You will use public address **209.165.200.227** and static NAT to provide address translation access to the server.

Step 1: Configure static NAT to the DMZ server using a network object.

a. From PC-B, select the ASDM **Configuration** screen > **Firewall** menu. Click the **Public Servers** option and click **Add** to define the DMZ server and services offered. In the Add Public Server dialog box, specify the Private Interface as **dmz**, the Public Interface as **outside**, and the Public IP address as **209.165.200.227**.

b. Click the ellipsis button to the right of Private IP Address. In the Browse Private IP Address window, click **Add** to define the server as a **Network Object**. Enter the name **DMZ-SERVER**, select **Host** for the Type**,** enter the Private IP Address of **192.168.2.3**, and a Description of **PC-A.**

c. From the Browse Private IP Address window, verify that the DMZ-Server appears in the Selected Private IP Address field and click **OK**. You will return to the Add Public Server dialog box.

d. In the Add Public Server dialog, click the ellipsis button to the right of Private Service. In the Browse Private Service window, double-click to select the following services: **tcp/ftp**, **tcp/http** and **icmp/echo** (scroll down to see all services). Click **OK** to continue and return to the **Add Public Server** dialog.

e. Click **OK** to add the server. Click **Apply** at the Public Servers screen to send the commands to the ASA

Step 2: View the DMZ Access Rule (ACL) generated by ASDM.

With the creation of the DMZ server object and selection of services, ASDM automatically generates an Access Rule (ACL) to permit the appropriate access to the server and applies it to the outside interface in the incoming direction.

View this Access Rule in ASDM by clicking **Configuration** > **Firewall** > **Access Rules**. It appears as an outside incoming rule. You can select the rule and use the horizontal scroll bar to see all of the components.

Step 3: Test access to the DMZ server from the outside network.

a. From PC-C, ping the IP address of the static NAT public server address (**209.165.200.227**). The pings should be successful.

b. You can also access the DMZ server from a host on the inside network because the ASA inside interface (VLAN 1) is set to security level 100 (the highest) and the DMZ interface (VLAN 3) is set to 70. The ASA acts like a router between the two networks. Ping the DMZ server (PC-A) internal address (**192.168.2.3**) from PC-B. The pings should be successful due to the interface security level and the fact that ICMP is being inspected on the inside interface by the global inspection policy.

c. The DMZ server cannot ping PC-B because the DMZ interface VLAN 3 has a lower security level and because it was necessary to specify the **no forward** command when the VLAN 3 interface was created. Try to ping from the DMZ server PC-A to PC-B. The pings should not be successful.

Part 8: Configure ASA Clientless SSL VPN Remote Access (Chapter 10)

In Part 8 of this lab, you will use ASDM's Clientless SSL VPN wizard to configure the ASA to support clientless SSL VPN remote access. You will verify your configuration by using a browser from PC-C.

Step 1: Start the VPN wizard.

Using ASDM on PC-B, click **Wizards** > **VPN Wizards** > **Clientless SSL VPN wizard**. The SSL VPN wizard Clientless SSL VPN Connection screen displays.

Step 2: Configure the SSL VPN user interface.

On the SSL VPN Interface screen, configure **VPN-PROFILE** as the Connection Profile Name and specify **outside** as the interface to which outside users will connect.

Step 3: Configure AAA user authentication.

On the User Authentication screen, click **Authenticate Using the Local User Database** and enter the username **VPNuser** with a password of **Remotepa55**. Click **Add** to create the new user.

Step 4: Configure the VPN group policy.

On the Group Policy screen, create a new group policy named **VPN-GROUP**.

Step 5: Configure the bookmark list.

a. From the Clientless Connections Only – Bookmark List screen, click **Manage** to create an HTTP server bookmark in the bookmark list. In the Configure GUI Customization Objects window, click **Add** to open the Add Bookmark List window. Name the list **WebServer.**

b. Add a new bookmark with **Web Mail** as the Bookmark Title. Enter the server destination IP address of **192.168.1.3** (PC-B is simulating an internal web server) as the URL.

c. Click OK to complete the wizard and **Apply** to the ASA

Step 6: Verify VPN access from the remote host.

a. Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (**https://209.165.200.226**). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA.

   Note: Accept security notification warnings.

b. The Login window should display. Enter the previously configured username **VPNuser**, enter the password **Remotepa55**, and click **Logon** to continue.

Step 7: Access the web portal window.

After the user authenticates, the ASA SSL web portal webpage will be displayed. This webpage lists the bookmarks previously assigned to the profile. If the bookmark points to a valid server IP address or hostname that has HTTP web services installed and functional, the outside user can access the server from the ASA portal.

Note: In this lab, the web mail server is not installed on PC-B.

Part 9: Configure a Site-to-Site IPsec VPN between R3 and the ASA. (Chapters 8 & 10)

In Part 9 of this lab, you will use the CLI to configure an IPsec VPN tunnel on R3 and use ASDM's Site-to-Site Wizard to configure the other side of the IPsec tunnel on the ASA.

Task 1: Configure the Site-to-Site IPsec VPN Tunnel on R3

Step 1: Enable IKE and configure the ISAKMP policy parameters.

a. Verify that IKE is supported and enabled.

b. Create an ISAKMP policy with a priority number of **1**. Use **pre-shared key** as the authentication type, **3des** for the encryption algorithm, **sha** as the hash algorithm, and the Diffie-Helman group **2** key exchange.

c. Configure the pre-shared key of **Site2SiteKEY1** and point it to the ASA's outside interface IP address.

d. Verify the IKE policy with the **show crypto isakmp policy** command.

Step 2: Configure the IPsec transform set and lifetime.

Create a transform set with tag **TRNSFRM-SET** and use an ESP transform with an AES 256 cipher with ESP and the SHA hash function.

Step 3: Define interesting traffic.

Configure the IPsec VPN interesting traffic ACL. Use extended access list number **101.** The source network should be R3's LAN (172.16.3.0/24), and the destination network should be the ASA's LAN (192.168.1.0/24).

Step 4: Create and apply a crypto map.

a. Create the crypto map on R3, name it **CMAP**, and use **1** as the sequence number.

b. Use the **match address <access-list>** command to specify which access list defines which traffic to encrypt.

c. Set the peer address to the ASA's remote VPN endpoint interface IP address (**209.165.200.226**).

d. Set the transform set to **TRNSFRM-SET.**

e. Apply the crypto map to R3's S0/0/1 interface.

Step 5: Verify IPsec configuration on R3.

Use the **show crypto map** and **show crypto ipsec sa** commands to verify R3's IPsec VPN configuration.

Task 2: Configure Site-to-Site VPN on ASA using ASDM

Step 1: Use a browser on PC-B to establish an ASDM session to the ASA.

a. After the ASDM is established, use the **Site-to-Site VPN Wizard** to configure the ASA for IPsec site-to-site VPN.

b. Set the Peer IP Address to R3's S0/0/1 IP address (**10.2.2.1**). Verify that **outside** is selected for the VPN Access Interface.

c. Identify the traffic to protect. Set the Local Network to **inside-network/24** and the Remote Network to **172.16.3.0/24**.

d. Configure the pre-shared key. Enter the Pre-shared Key of **Site2SiteKEY1**.

e. Enable NAT exemption. Check the **Exempt ASA side host/network from address translation** box and verify that the **inside** interface is selected.

Step 2: Apply IPsec configuration to the ASA.

Click **Finish** to apply the site-to-site configuration to the ASA.

Task 3: Test the Site-to-Site IPsec VPN Connection between the ASA and R3

Step 1: From PC-B, ping R3's LAN interface.

This should access the IPsec Site-to-site VPN connection between the ASA and R3.

Step 2: Verify the IPsec Site-to-Site VPN session is active.

a. From ASDM on PC-B, click the **Monitoring**>**VPN** menu. A connection profile IP address of 10.2.2.1 should be displayed in the middle of the screen. Click the **Details** button to see IKE and IPsec session details.

b. Issue the **show crypto isakmp sa** command to verify that an IKE security association (SA) is active.

c. From PC-C, issue the command **tracert 192.168.1.3**. If the site-to-site VPN tunnel is working correctly, you will not see traffic being routed through R2 (10.2.2.2).

d. Issue the **show crypto ipsec sa** command on R3 to view the number of packets that have been encapsulated and decapsulated. Verify that there are no failed packet attempts or send and receive errors.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1700	Fast Ethernet 0 (F0)	Fast Ethernet 1 (F1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				