Cisco | Networking Academy®
Mind Wide Open™

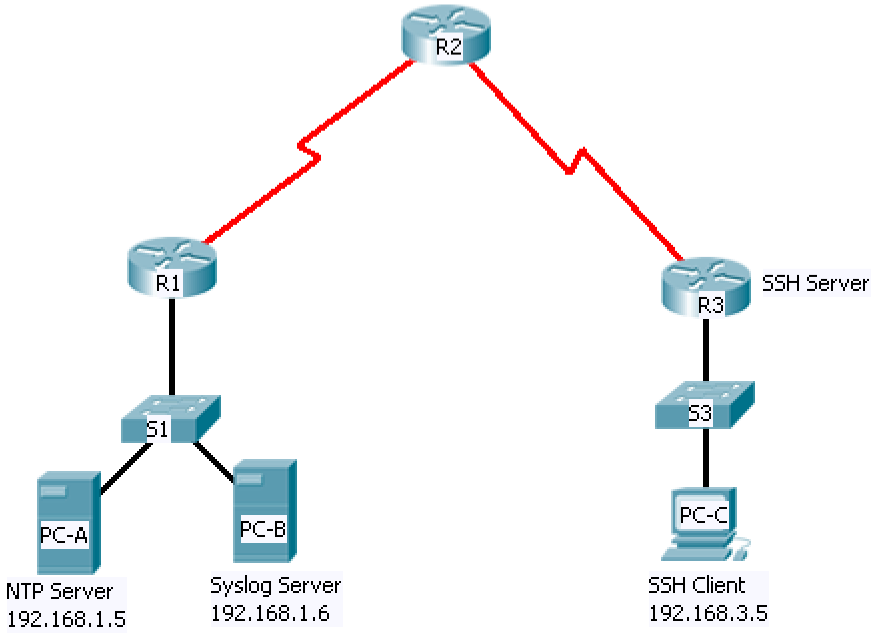
CCNA Security 1.0.1

Instructor Packet Tracer Manual

PT Activity: Configure Cisco Routers for Syslog, NTP, and SSH Operations

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	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	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 FA0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 FA0/6

Learning Objectives

- Configure routers as NTP clients.
- Configure routers to update the hardware clock using NTP.
- Configure routers to log messages to the syslog server.
- Configure routers to timestamp log messages.
- Configure local users.
- Configure VTY lines to accept SSH connections only.
- Configure RSA key pair on SSH server.
- Verify SSH connectivity from PC client and router client.

Introduction

The network topology shows three routers. You will configure NTP and Syslog on all routers. You will configure SSH on R3.

Network Time Protocol (NTP) allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings and Syslog messages generated can be analyzed more easily. This can help when troubleshooting issues with network problems and attacks. When NTP is implemented in the network, it can be set up to synchronize to a private master clock, or to a publicly available NTP server on the Internet.

The NTP Server is the master NTP server in this lab. You will configure the routers to allow the software clock to be synchronized by NTP to the time server. Also, you will configure the routers to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift) and the software clock and hardware clock may become out of synchronization with each other.

The Syslog Server will provide message logging in this lab. You will configure the routers to identify the remote host (Syslog server) that will receive logging messages.

You will need to configure timestamp service for logging on the routers. 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.

R2 is an ISP connected to two remote networks: R1 and R3. The local administrator at R3 can perform most router configurations and troubleshooting; however, since R3 is a managed router, the ISP needs access to R3 for occasional troubleshooting or updates. To provide this access in a secure manner, the administrators have agreed to use Secure Shell (SSH).

You use the CLI to configure the router to be managed securely using SSH instead of Telnet. SSH is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

The servers have been pre-configured for NTP and Syslog services respectively. NTP will not require authentication. The routers have been pre-configured with the following:

- Enable password: **ciscoenpa55**
- Password for vty lines: **ciscovtypa55**
- Static routing

Task 1: Configure routers as NTP Clients.

Step 1. Test Connectivity

- Ping from PC-C to R3.
- Ping from R2 to R3.
- Telnet from PC-C to R3. Exit the Telnet session.
- Telnet from R2 to R3. Exit the Telnet session.

Step 2. Configure R1, R2 and R3 as NTP clients.

```
R1(config)# ntp server 192.168.1.5
R2(config)# ntp server 192.168.1.5
R3(config)# ntp server 192.168.1.5
```

Verify client configuration using the command **show ntp status**.

Step 3. Configure routers to update hardware clock.

Configure R1, R2 and R3 to periodically update the hardware clock with the time learned from NTP.

```
R1(config)# ntp update-calendar
R2(config)# ntp update-calendar
R3(config)# ntp update-calendar
```

Verify that the hardware clock was updated using the command **show clock**.

Step 4. Configure routers to timestamp log messages.

Configure timestamp service for logging on the routers.

```
R1(config)# service timestamps log datetime msec
R2(config)# service timestamps log datetime msec
R3(config)# service timestamps log datetime msec
```

Task 2: Configure routers to log messages to the Syslog Server.

Step 1. Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.

```
R1(config)# logging host 192.168.1.6
R2(config)# logging host 192.168.1.6
R3(config)# logging host 192.168.1.6
```

The router console will display a message that logging has started.

Step 2. Verify logging configuration using the command show logging.

Step 3. Examine logs of the Syslog server.

From the **Config** tab of the Syslog server's dialogue box, select the **Syslog services** button. Observe the logging messages received from the routers.

Note: Log messages can be generated on the server by executing commands on the router. For example, entering and exiting global configuration mode will generate an informational configuration message.

Task 3: Configure R3 to support SSH connections.

Step 1. Configure a domain name.

Configure a domain name of **ccnasecurity.com** on R3.

```
R3(config)# ip domain-name ccnasecurity.com
```

Step 2. Configure users for login from the SSH client on R3.

Create a user ID of **SSHadmin** with the highest possible privilege level and a secret password of **ciscosshpa55**.

```
R3(config)# username SSHadmin privilege 15 secret ciscosshpa55
```

Step 3. Configure the incoming VTY lines on R3.

Use the local user accounts for mandatory login and validation. Accept only SSH connections.

```
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

Step 4. Erase existing key pairs on R3.

Any existing RSA key pairs should be erased on the router.

```
R3(config)#crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: `% No Signature RSA Keys found in configuration.`

Step 5. Generate the RSA encryption key pair for R3.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Configure the RSA keys with a modulus of **1024**. The default is 512, and the range is from 360 to 2048.

```
R3(config)# crypto key generate rsa [Enter]
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Note: The command to generate RSA encryption key pairs for R3 in Packet Tracer differs from those used in the lab.

Step 6. Verify the SSH configuration.

Use the **`show ip ssh`** command to see the current settings. Verify that the authentication timeout and retries are at their default values of 120 and 3.

Step 7. Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive. Set the timeout to **90** seconds, the number of authentication retries to **2**, and the version to **2**.

```
R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
R3(config)# ip ssh version  2
```

Issue the **`show ip ssh`** command again to confirm that the values have been changed.

Step 8. Attempt to connect to R3 via Telnet from PC-C.

Open the Desktop of PC-C. Select the Command Prompt icon. From PC-C, enter the command to connect to R3 via Telnet.

```
PC> telnet 192.168.3.1
```

This connection should fail, since R3 has been configured to accept only SSH connections on the virtual terminal lines.

Step 9. Connect to R3 using SSH on PC-C.

Open the Desktop of PC-C. Select the Command Prompt icon. From PC-C, enter the command to connect to R3 via SSH. When prompted for the password, enter the password configured for the administrator **ciscosshpa55**.

```
PC> ssh –l SSHadmin 192.168.3.1
```

Step 10. Connect to R3 using SSH on R2.

In order to troubleshoot and maintain the R3 router, the administrator at the ISP must use SSH to access the router CLI. From the CLI of R2, enter the command to connect to R3 via SSH version 2 using the SSHadmin user account. When prompted for the password, enter the password configured for the administrator: **ciscosshpa55**.

```
R2# ssh –v 2 –l SSHadmin 10.2.2.1
```

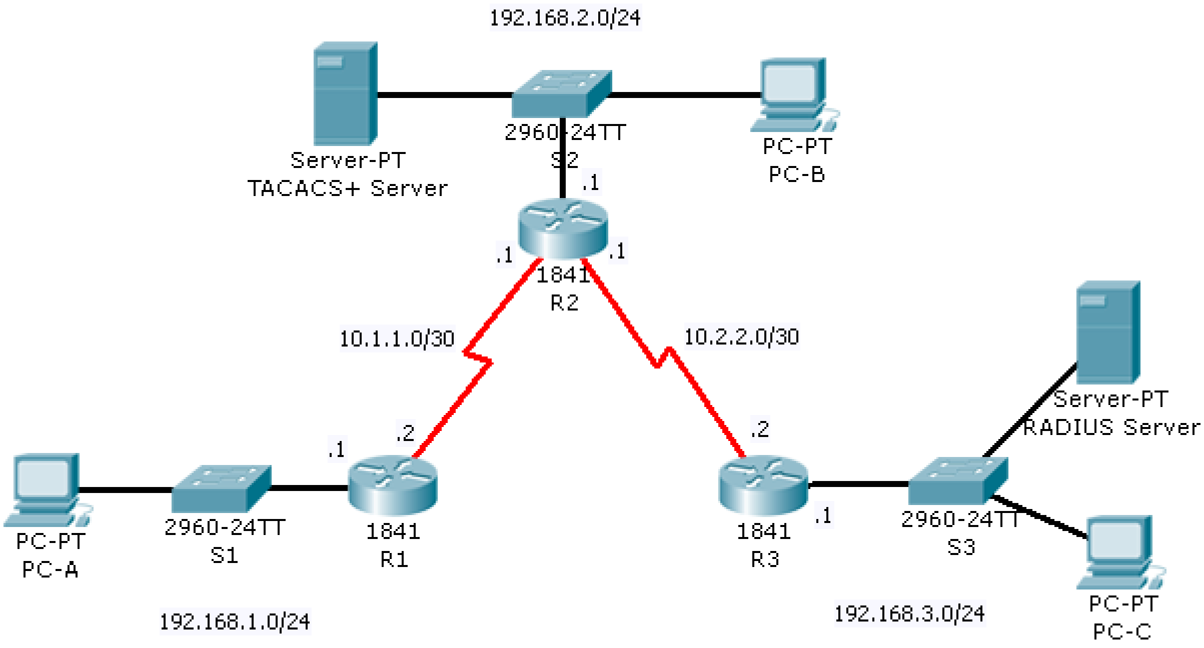
Step 11. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Configure AAA Authentication on Cisco Routers

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.1.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
R2	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.2.1	255.255.255.0
	S0/0/1	10.2.2.1	255.255.255.252
R3	S0/0/1	10.2.2.2	255.255.255.252
	Fa0/0	192.168.3.1	255.255.255.0
TACACS+ Server	NIC	192.168.2.2	255.255.255.0
RADIUS Server	NIC	192.168.3.2	255.255.255.0
PC-A	NIC	192.168.1.3	255.255.255.0
PC-B	NIC	192.168.2.3	255.255.255.0
PC-C	NIC	192.168.3.3	255.255.255.0

Learning Objectives

- Configure a local user account on R1 and authenticate on the console and VTY lines using local AAA.
- Verify local AAA authentication from the R1 console and the PC-A client.
- Configure a server-based AAA authentication using TACACS+.
- Verify server-based AAA authentication from PC-B client.
- Configure a server-based AAA authentication using RADIUS.
- Verify server-based AAA authentication from PC-C client.

Introduction

The network topology shows routers R1, R2 and R3. Currently all administrative security is based on knowledge of the enable secret password. Your task is to configure and test local and server-based AAA solutions.

You will create a local user account and configure local AAA on router R1 to test the console and VTY logins.

- User account: **Admin1** and password **admin1pa55**

You will then configure router R2 to support server-based authentication using the TACACS+ protocol. The TACACS+ server has been pre-configured with the following:

- Client: **R2** using the keyword **tacacspa55**
- User account: **Admin2** and password **admin2pa55**

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol. The RADIUS server has been pre-configured with the following:

- Client: **R3** using the keyword **radiuspa55**
- User account: **Admin3** and password **admin3pa55**

The routers have also been pre-configured with the following:

- Enable secret password: **ciscoenpa55**
- RIP version 2

Note: The console and VTY lines have not been pre-configured.

Task 1: Configure Local AAA Authentication for Console Access on R1

Step 1. Test connectivity.

- **Ping** from PC-A to PC-B.
- **Ping** from PC-A to PC-C.
- **Ping** from PC-B to PC-C.

Step 2. Configure a local username on R1.

Configure a username of **Admin1** and secret password of **admin1pa55**.

```
R1(config)# username Admin1 password admin1pa55
```

Step 3. Configure local AAA authentication for console access on R1.

Enable AAA on R1 and configure AAA authentication for console login to use the local database.

```
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
```

Step 4. Configure the line console to use the defined AAA authentication method.

Enable AAA on R1 and configure AAA authentication for console login to use the default method list.

```
R1(config)# line console 0
R1(config-line)# login authentication default
```

Step 5. Verify the AAA authentication method.

Verify the user EXEC login using the local database.

```
R1(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# exit

R1 con0 is now available
Press RETURN to get started.

************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin1
Password: admin1pa55
R1>
```

Task 2: Configure Local AAA Authentication for VTY Lines on R1

Step 1. Configure a named list AAA authentication method for VTY lines on R1.

Configure a named list called **TELNET-LOGIN** to authenticate logins using local AAA.

```
R1(config)# aaa authentication login TELNET-LOGIN local
```

Step 2. Configure the VTY lines to use the defined AAA authentication method.

Configure the VTY lines to use the named AAA method.

```
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
R1(config-line)# end
```

Step 3. Verify the AAA authentication method.

Verify the Telnet configuration. From the command prompt of PC-A, Telnet to R1.

```
PC> telnet 192.168.1.1


************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin1
Password: admin1pa55
R1>
```

Task 3: Configure Server-Based AAA Authentication Using TACACS+ on R2

Step 1. Configure a backup local database entry called Admin.

For backup purposes, configure a local username of **Admin** and secret password of **adminpa55**.

```
R2(config)# username Admin password adminpa55
```

Step 2. Verify the TACACS+ Server configuration.

Select the TACACS+ Server. From the Config tab, click on **AAA** and notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

Step 3. Configure the TACACS+ server specifics on R2.

Configure the AAA TACACS server IP address and secret key on R2.

```
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
```

Step 4. Configure AAA login authentication for console access on R2.

Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server and if not available, then use the local database.

```
R2(config)# aaa new-model
R2(config)# aaa authentication login default group tacacs+ local
```

Step 5. Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

```
R2(config)# line console 0
R2(config-line)# login authentication default
```

Step 6. Verify the AAA authentication method.

Verify the user EXEC login using the AAA TACACS+ server.

```
R2(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R2# exit

R2 con0 is now available
Press RETURN to get started.

************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin2
Password: admin2pa55
R2>
```

Task 4: Configure Server-Based AAA Authentication Using RADIUS on R3

Step 1. Configure a backup local database entry called Admin.

For backup purposes, configure a local username of **Admin** and secret password of **adminpa55**.

```
R3(config)# username Admin password adminpa55
```

Step 2. Verify the RADIUS Server configuration.

Select the RADIUS Server. From the Config tab, click on **AAA** and notice that there is a Network configuration entry for R3 and a User Setup entry for Admin3.

Step 3. Configure the RADIUS server specifics on R3.

Configure the AAA RADIUS server IP address and secret key on R3.

```
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55
```

Step 4. Configure AAA login authentication for console access on R3.

Enable AAA on R3 and configure all logins to authenticate using the AAA RADIUS server and if not available, then use the local database.

```
R3(config)# aaa new-model
R3(config)# aaa authentication login default group radius local
```

Step 5. Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

```
R3(config)# line console 0
R3(config-line)# login authentication default
```

Step 6. Verify the AAA authentication method.

Verify the user EXEC login using the AAA TACACS+ server.

```
R3(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R3# exit

R3 con0 is now available
Press RETURN to get started.

************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin3
Password: admin3pa55
R3>
```

Step 7. Check results.

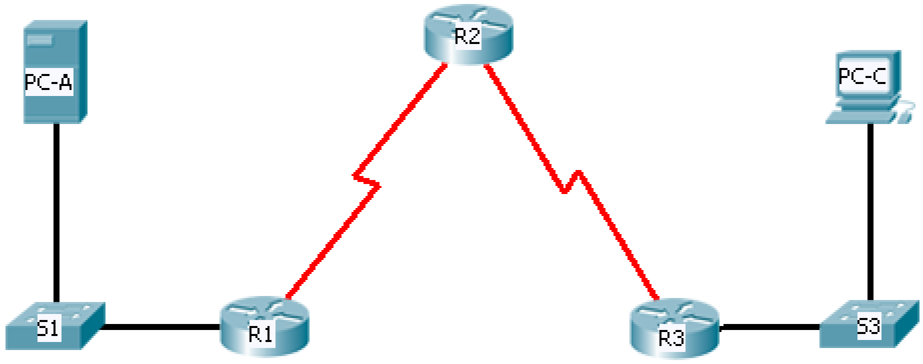
Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

Cisco | Networking Academy®
Mind Wide Open™

PT Activity: Configure IP ACLs to Mitigate Attacks

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1(DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality.

Introduction

Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R3 to achieve this goal. You then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

- Enable password: **ciscoenpa55**
- Password for console: **ciscoconpa55**
- Username for VTY lines: **SSHadmin**
- Password for VTY lines: **ciscosshpa55**
- IP addressing
- Static routing

Task 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

Step 1. From the PC-C command prompt, ping the PC-A server.

Step 2. From the PC-C command prompt, SSH to the router R2 Lo0 interface. Exit the SSH session.

Step 3. From PC-C, open a web browser to the PC-A server (using the IP address) to display the web page. Close the browser on PC-C.

Step 4. From the PC-A server command prompt, ping PC-C.

Task 2: Secure Access to Routers

Step 1. Configure ACL 10 to block all remote access to the routers except from PC-C.

Use the **access-list** command to create a numbered IP ACL on R1, R2, and R3.

```
R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0

R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0

R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```

Step 2. Apply ACL 10 to ingress traffic on the VTY lines.

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

```
R1(config-line)# access-class 10 in

R2(config-line)# access-class 10 in

R3(config-line)# access-class 10 in
```

Step 3. Verify exclusive access from management station PC-C.

SSH to 192.168.2.1 from PC-C (should be successful). SSH to 192.168.2.1 from PC-A (should fail).

```
PC> ssh –l SSHadmin 192.168.2.1
```

Task 3: Create a Numbered IP ACL 100

On R3, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step 1. Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the **access-list** command to create a numbered IP ACL.

```
R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)# access-list 100 permit ip any any
```

Step 2. Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

```
R3(config)# interface s0/0/1
R3(config-if)# ip access-group 100 in
```

Step 3. Confirm that the specified traffic entering interface Serial 0/0/1 is dropped.

From the PC-C command prompt, ping the PC-A server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

Step 4. Remove the ACL from interface Serial 0/0/1.

Remove the ACL. Otherwise, all traffic from the outside network (being addressed with private source IP addresses) will be denied for the remainder of the PT activity.

Use the **no ip access-group** command to remove the access list from interface Serial 0/0/1.

```
R3(config)# interface s0/0/1
R3(config-if)# no ip access-group 100 in
```

Task 4: Create a Numbered IP ACL 110

Deny all outbound packets with source address outside the range of internal IP addresses.

Step 1. Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any
```

Step 2. Apply the ACL to interface F0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/1.

```
R3(config)# interface fa0/1
R3(config-if)# ip access-group 110 in
```

Task 5: Create a Numbered IP ACL 120

Permit any outside host to access DNS, SMTP, and FTP services on server PC-A, deny any outside host access to HTTPS services on PC-A, and permit PC-C to access R1 via SSH.

Step 1. Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server PC-A.

Step 2. Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

```
R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq
22
```

Step 3. Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 120 in
```

Step 4. Verify that PC-C cannot access PC-A via HTTPS using the web browser.

Task 6: Modify An Existing ACL

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

Step 1. Verify that PC-A cannot successfully ping the loopback interface on R2.

Step 2. Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

```
R1(config)# access-list 120 permit icmp any any echo-reply
R1(config)# access-list 120 permit icmp any any unreachable
R1(config)# access-list 120 deny icmp any any
R1(config)# access-list 120 permit ip any any
```

Step 3. Verify that PC-A can successfully ping the loopback interface on R2.

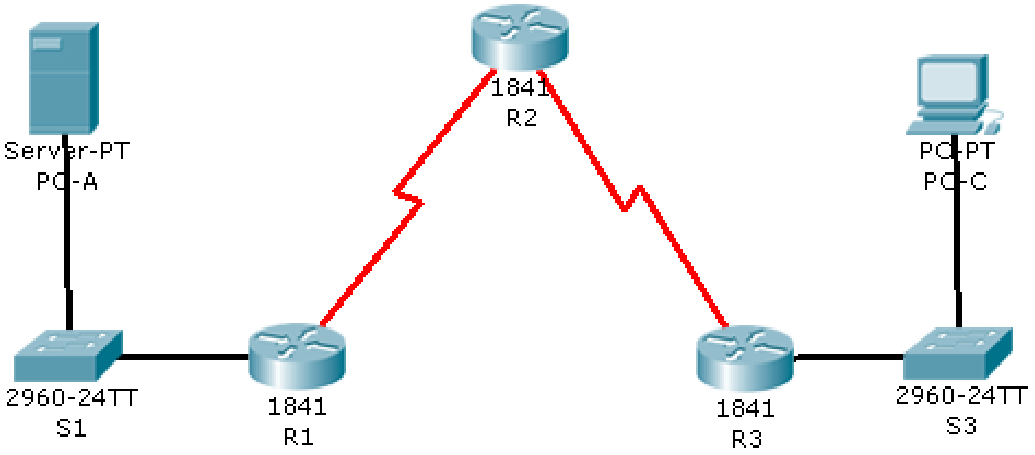
Step 4. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Configuring Context-Based Access Control (CBAC)

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Learning Objectives

- Verify connectivity among devices before firewall configuration.
- Configure an IOS firewall with CBAC on router R3
- Verify CBAC functionality using ping, Telnet, and HTTP.

Introduction

Context-Based Access Control (CBAC) is used to create an IOS firewall. In this activity, you will create a basic CBAC configuration on edge router R3. R3 provides access to resources outside of the network for hosts on the inside network. R3 blocks external hosts from accessing internal resources. After the configuration is complete, you will verify firewall functionality from internal and external hosts.

The routers have been pre-configured with the following:

- Enable password: **ciscoenpa55**
- Password for console: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- IP addressing
- Static routing
- All switch ports are in VLAN 1 for switches S1 and S3.

Task 1: Block Traffic From Outside

Step 1. Verify Basic Network Connectivity.

Verify network connectivity prior to configuring the IOS firewall.

- From the PC-C command prompt, ping the PC-A server.
- From the PC-C command prompt, Telnet to the Router R2 S0/0/1 interface: IP address 10.2.2.2. Exit the Telnet session.
- From PC-C, open a web browser to the PC-A server to display the web page. Close the browser on PC-C.
- From the PC-A server command prompt, ping PC-C.

Step 2. Configure a named IP ACL on R3 to block all traffic originating from the outside network.

Use the **ip access-list extended** command to create a named IP ACL.

```
R3(config)# ip access-list extended OUT-IN
R3(config-ext-nacl)# deny ip any any
R3(config-ext-nacl)# exit
```

Step 3. Apply the ACL to interface Serial 0/0/1.

```
R3(config)# interface s0/0/1
R3(config-if)# ip access-group OUT-IN in
```

Step 4. Confirm that traffic entering interface Serial 0/0/1 is dropped.

From the PC-C command prompt, ping the PC-A server. The ICMP echo replies are blocked by the ACL.

Task 2: Create a CBAC Inspection Rule

Step 1. Create an inspection rule to inspect ICMP, Telnet, and HTTP traffic.

```
R3(config)# ip inspect name IN-OUT-IN icmp
R3(config)# ip inspect name IN-OUT-IN telnet
R3(config)# ip inspect name IN-OUT-IN http
```

Step 2. Turn on time-stamped logging and CBAC audit trail messages.

Use the **ip inspect audit-trail** command to turn on CBAC audit messages to provide a record of network access through the firewall, including illegitimate access attempts. Enable logging to the syslog server, 192.168.1.3, with the **logging host** command. Make sure that logged messages are timestamped.

```
R3(config)# ip inspect audit-trail
R3(config)# service timestamps debug datetime msec
R3(config)# logging host 192.168.1.3
```

Step 3. Apply the inspection rule to egress traffic on interface S0/0/1.

```
R3(config-if)# ip inspect IN-OUT-IN out
```

Step 4. Verify that audit trail messages are being logged on the syslog server.

- From PC-C, test connectivity to PC-A with ping, Telnet, and HTTP. Ping and HTTP should be successful. Note that PC-A will reject the Telnet session.
- From PC-A, test connectivity to PC-C with ping and Telnet. All should be blocked.
- Review the syslog messages on server PC-A: click the **Config** tab and then click the **SYSLOG** option.

Task 3: Verify Firewall Functionality

Step 1. Open a Telnet session from PC-C to R2.

The Telnet should succeed. While the Telnet session is active, issue the command **show ip inspect sessions** on R3. This command displays the existing sessions that are currently being tracked and inspected by CBAC.

```
R3# show ip inspect sessions
Established Sessions
 Session 100424296 (192.168.3.3:1031)=>(10.1.1.2:23) telnet SIS_OPEN
```

What is the source IP address and port number? 192.168.3.3:1031 (port 1031 is random)

What is the destination IP address and port number? 10.1.1.2:23 (Telnet = port 23)

Exit the Telnet session.

Step 2. From PC-C, open a web browser to the PC-A server web page using the server IP address.

The HTTP session should succeed. While the HTTP session is active, issue the command **show ip inspect sessions** on R3.

```
R3# show ip inspect sessions
Established Sessions
 Session 104637440 (192.168.3.3:1032)=>(192.168.1.3:http SIS_OPEN
```

Note: If the HTTP session times out before you execute the command on R3, you will have to click the **Go** button on PC-C to generate a session between PC-C and PC-A.

What is the source IP address and port number? 192.168.3.3:1027 (port 1032 is random)

What is the destination IP address and port number? 192.168.1.3:80 (HTTP web = port 80)

Close the browser on PC-C.

Step 3. View the interface configuration and inspection rule timers.

Enter the **show ip inspect** interfaces command on R3.

The output shows existing sessions that are currently being tracked and inspected by CBAC.

```
R3# show ip inspect interfaces
Interface Configuration
 Interface Serial0/0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is IN-OUT-IN
    icmp alert is on audit-trail is off timeout 10
    telnet alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
  Inbound access list is OUT-IN
  Outgoing access list is not set
```

Task 4: Review CBAC Configuration

Step 1. Display CBAC configuration.

Enter the **show ip inspect config** command on R3 to display the complete CBAC inspection configuration.

```
R3# show ip inspect config
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited]
connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo
bytes
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name IN-OUT-IN
    icmp alert is on audit-trail is off timeout 10
    telnet alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
```

Step 2. Display real-time output that can be used for troubleshooting.

Enter the **debug ip inspect detailed** command on R3 to display detailed messages about CBAC software events, including information about CBAC packet processing.

From PC-C, open a web browser on PC-C; enter the PC-A (server) IP address: 192.168.1.3.

```
R3# debug ip inspect detailed
INSPECT Detailed Debug debugging is on
*Mar 01, 02:37:28.3737:  %FW-6-SESS_AUDIT_TRAIL_START: Start http session:
initiator (192.168.3.3:1039) -- responder (192.168.1.3:80)
*Mar 01, 02:37:28.3737: CBAC: Finding pregen session for src_tableid:0,
src_addr:192.168.3.3, src_port:1039, dst_tableid:0, dst_addr:192.168.1.3,
dst_port:80
*Mar 01, 02:37:38.3737:  %FW-6-SESS_AUDIT_TRAIL_STOP: Stop http session:
initiator (192.168.3.3:1041) -- responder (192.168.1.3:80)
```

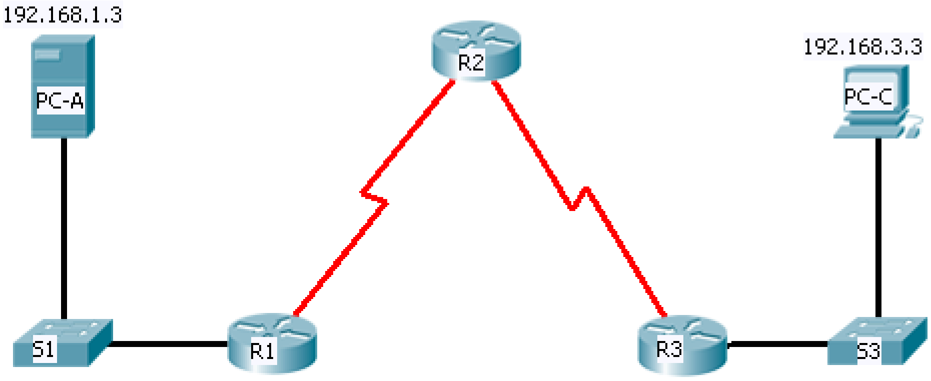
Step 3. Check Results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Configuring a Zone-Based Policy Firewall (ZPF)

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Learning Objectives

- Verify connectivity among devices before firewall configuration.
- Configure a zone-based policy (ZPF) firewall on router R3
- Verify ZPF firewall functionality using ping, Telnet and a web browser.

Introduction

Zone-based policy (ZPF) firewalls are the latest development in the evolution of Cisco firewall technologies. In this activity, you configure a basic ZPF on an edge router R3 that allows internal hosts access to external resources and blocks external hosts from accessing internal resources. You then verify firewall functionality from internal and external hosts.

The routers have been pre-configured with the following:

- Console password: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- Host names and IP addressing
- Static routing

Task 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the zone-based policy firewall.

Step 1. From the PC-A command prompt, ping PC-C at 192.168.3.3.

Step 2. From the PC-C command prompt, Telnet to the Router R2 S0/0/1 interface at 10.2.2.2. Exit the Telnet session.

Step 3. From PC-C, open a web browser to the PC-A server.

Click the **Desktop** tab and click the **Web Browser** application. Enter the PC-A IP address 192.168.1.3 as the URL. The Packet Tracer 5.x welcome page from the web server should be displayed.

Close the browser on PC-C.

Task 2: Create the Firewall Zones on Router R3

Note: For all configuration tasks, be sure to use the exact names as specified.

Step 1. Create an internal zone.

Use the **zone security** command to create a zone named **IN-ZONE**.

```
R3(config)# zone security IN-ZONE
```

Step 2. Step 2. Create an external zone.

Use the **zone security** command to create a zone named **OUT-ZONE**.

```
R3(config-sec-zone)# zone security OUT-ZONE
R3(config-sec-zone)# exit
```

Task 3: Define a Traffic Class and Access List

Step 1. Create an ACL that defines internal traffic.

Use the **access-list** command to create extended ACL **101** to permit all IP protocols from the **192.168.3.0/24** source network to any destination.

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

Step 2. Create a class map referencing the internal traffic ACL.

Use the **class map type inspect** command with the match-all option to create a class map named **IN-NET-CLASS-MAP**. Use the **match access-group** command to match ACL **101**.

```
R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit
```

Note: Although not supported in this Packet Tracer exercise, individual protocols (HTTP, FTP, etc.) can be specific to be matched using the **match-any** option in order to provide more precise control over what type of traffic is inspected.

Task 4: Specify Firewall Policies

Step 1. Create a policy map to determine what to do with matched traffic.

Use the **policy-map type inspect** command and create a policy map named **IN-2-OUT-PMAP**.

```
R3(config)# policy-map type inspect IN-2-OUT-PMAP
```

Step 2. Specify a class type of inspect and reference class map IN-NET-CLASS-MAP.

```
R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
```

Step 3. Specify the action of inspect for this policy map

The use of the **inspect** command invokes context-based access control (other options include pass and drop).

```
R3(config-pmap-c)# inspect

%No specific protocol configured in class IN-NET-CLASS-MAP for inspection.
All protocols will be inspected.
```

Issue the **exit** command twice to leave **config-pmap-c** mode and return to **config** mode.

```
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

Task 5: Apply Firewall Policies

Step 1. Create a pair of zones.

Using the **zone-pair security** command, create a zone pair named **IN-2-OUT-ZPAIR**. Specify the source and destination zones that were created in Task 1.

```
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination
OUT-ZONE
```

Step 2. Specify the policy map for handling the traffic between the two zones.

Attach a policy-map and its associated actions to the zone pair using the **service-policy type inspect** command and reference the policy map previously created, **IN-2-OUT-PMAP**.

```
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)# exit
R3(config)#
```

Step 3. Assign interfaces to the appropriate security zones.

Use the **zone-member security** command in interface config mode to assign Fa0/1 to **IN-ZONE** and S0/0/1 to **OUT-ZONE**.

```
R3(config)# interface fa0/1
R3(config-if)# zone-member security IN-ZONE
R3(config-if)# exit

R3(config)# interface s0/0/1
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)# exit
```

Step 4. Copy the running config to the startup config.

Task 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE

Verify that internal hosts can still access external resources after configuring the zone-based policy firewall.

Step 1. From internal PC-C, ping the external PC-A server.

From the PC-C Command Prompt, ping PC-A at 192.168.1.3. The ping should succeed.

Step 2. From internal PC-C, Telnet to the router R2 S0/0/1 interface.

From the PC-C Command Prompt, telnet to R2 at 10.2.2.2 and provide the vty password **ciscovtypa55**. The telnet should succeed. While the Telnet session is active, issue the command **show policy-map type inspect zone-pair sessions** on R3 to view established sessions.

```
R3# show policy-map type inspect zone-pair sessions

Zone-pair: IN-ZONE-OUT-ZONE

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect
        Established Sessions
         Session 139644744 (192.168.3.3:1025)=>(10.2.2.2:23) telnet:tcp
SIS_OPEN
          Created 00:00:02, Last heard 00:00:00
          Bytes sent (initiator:responder) [0:0]
```

What is the source IP address and port number? 192.168.3.3:1025 (port 1025 is random)

What is the destination IP address and port number? 10.2.2.2:23 (Telnet = port 23)

Step 3. From PC-C, exit the Telnet session on R2 and close the Command Prompt window.

Step 4. From internal PC-C, open a web browser to the PC-A server web page.

Enter the server IP address 192.168.1.3 in the browser URL field and click **Go**. The HTTP session should succeed. While the HTTP session is active, issue the command **show policy-map type inspect zone-pair sessions** on R3 to view established sessions.

Note: If the HTTP session times out before you execute the command on R3, you will have to click the **Go** button on PC-C to generate a session between PC-C and PC-A.

```
R3# show policy-map type inspect zone-pair sessions
 Zone-pair: IN-ZONE-OUT-ZONE

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect
        Established Sessions
               Session 139142400 (192.168.3.3:1027)=>(192.168.1.3:80)
               http:tcp SIS_OPEN
```

```
          Created 00:00:02, Last heard 00:00:00
          Bytes sent (initiator:responder) [0:0]
```

What is the source IP address and port number? 192.168.3.3:1027 (port 1027 is random)

What is the destination IP address and port number? 192.168.1.3:80 (HTTP web = port 80)

Step 5. Close the Browser on PC-C.

Task 7: Test Firewall Functionality from OUT-ZONE to IN-ZONE

Verify that external hosts CANNOT access internal resources after configuring the zone-based policy firewall.

Step 1. From the PC-A server command prompt, ping PC-C.

From the PC-A Command Prompt, ping PC-C at 192.168.3.3. The ping should fail.

Step 2. From router R2, ping PC-C.

From R2, ping PC-C at 192.168.3.3. The ping should fail.

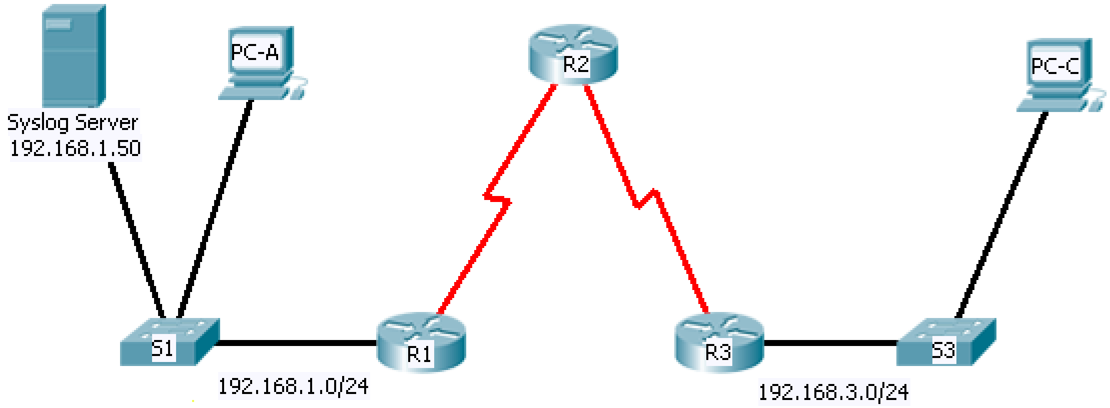
Step 3. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Configure IOS Intrusion Prevention System (IPS) using CLI

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	FA0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.0	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.0	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.0	N/A
R3	FA0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	10.2.2.2	255.255.255.0	N/A
Syslog Server	NIC	192.168.1.50	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Learning Objectives

- Enable IOS IPS.
- Configure logging.
- Modify an IPS signature.
- Verify IPS.

Introduction

Your task is to configure router R1 for IPS in order to scan traffic entering the 192.168.1.0 network.

The server labeled ‘Syslog Server’ is used to log IPS messages. You must configure the router to identify the syslog server in order to receive logging messages. Displaying the correct time and date in syslog messages is vital when using syslog to monitor the network. Set the clock and configure timestamp service for logging on the routers. Finally, enable IPS to produce an alert and drop ICMP echo reply packets inline.

The server and PCs have been preconfigured. The routers have also been preconfigured with the following:

- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**
- EIGRP 101

Task 1: Enable IOS IPS

Note: Within Packet Tracer, the routers already have the signature files imported and in place. They are the default xml files in flash. For this reason, it is not necessary to configure the public crypto key and complete a manual import of the signature files.

Step 1. Verify network connectivity.

- **Ping** from PC-C to PC-A. The ping should be successful.
- **Ping** from PC-A to PC-C. The ping should be successful.

Step 2. Create an IOS IPS configuration directory in flash.

On R1, create a directory in flash using the **`mkdir`** command. Name the directory **`ipsdir`**.

```
R1#mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir
```

Step 3. Configure the IPS signature storage location.

On R1, configure the IPS signature storage location to be the directory you just created.

```
R1(config)#ip ips config location flash:ipsdir
```

Step 4. Create an IPS rule.

On R1, create an IPS rule name using the **`ip ips name`** *`name`* command in global configuration mode. Name the IPS rule **iosips**.

```
R1(config)# ip ips name iosips
```

Step 5. Enable logging.

IOS IPS supports the use of syslog to send event notification. Syslog notification is enabled by default. If logging console is enabled, you see IPS syslog messages.

Enable syslog if it is not enabled.

```
R1(config)# ip ips notify log
```

Use the **clock set** command from privileged EXEC mode to reset the clock if necessary.

```
R1# clock set 01:20:00 6 january 2009
```

Verify that the timestamp service for logging is enabled on the router using the **show run** command. Enable the timestamp service if it is not enabled.

```
R1(config)# service timestamps log datetime msec
```

Send log messages to the Syslog server at IP address 192.168.1.50.

```
R1(config)# logging host 192.168.1.50
```

Step 6. Configure IOS IPS to use the signature categories.

Retire the **all** signature category with the **retired true** command (all signatures within the signature release). Unretire the **IOS_IPS Basic** category with the **retired false** command.

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-cateogry)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Step 7. Apply the IPS rule to an interface.

Apply the IPS rule to an interface with the **`ip ips`** *`name direction`* command in interface configuration mode. Apply the rule outbound on the Fa0/0 interface of R1. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

Note: The direction **`in`** means that IPS inspects only traffic going into the interface. Similarly, **`out`** means only traffic going out the interface.

```
R1(config)# interface fa0/0
R1(config-if)# ip ips iosips out
```

Task 2: Modify the Signature

Step 1. Change the event-action of a signature.

Un-retire the echo request signature (signature 2004, subsig ID 0), enable it and change the signature action to alert, and drop.

```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Step 2. Use show commands to verify IPS.

Use the **`show ip ips all`** command to see an IPS configuration status summary.

To which interfaces and in which direction is the iosips rule applied? Fa 0/0 outbound.

Step 3. Verify that IPS is working properly.

From PC-C, attempt to **ping** PC-A. Were the pings successful? Why or why not?

The pings should fail. This is because the IPS rule for event-action of an echo request was set to “deny-packet-inline.

From PC-A, attempt to **ping** PC-C. Were the pings successful? Why or why not?

The ping should be successful. This is because the IPS rule does not cover echo reply. When PC-A pings PC-C, PC-C responds with an echo reply.

Step 4. View the Syslog messages.

Click on the **Syslog** server. Select the **Config** tab. In the left navigation menu, select **SYSLOG** to view the log file.

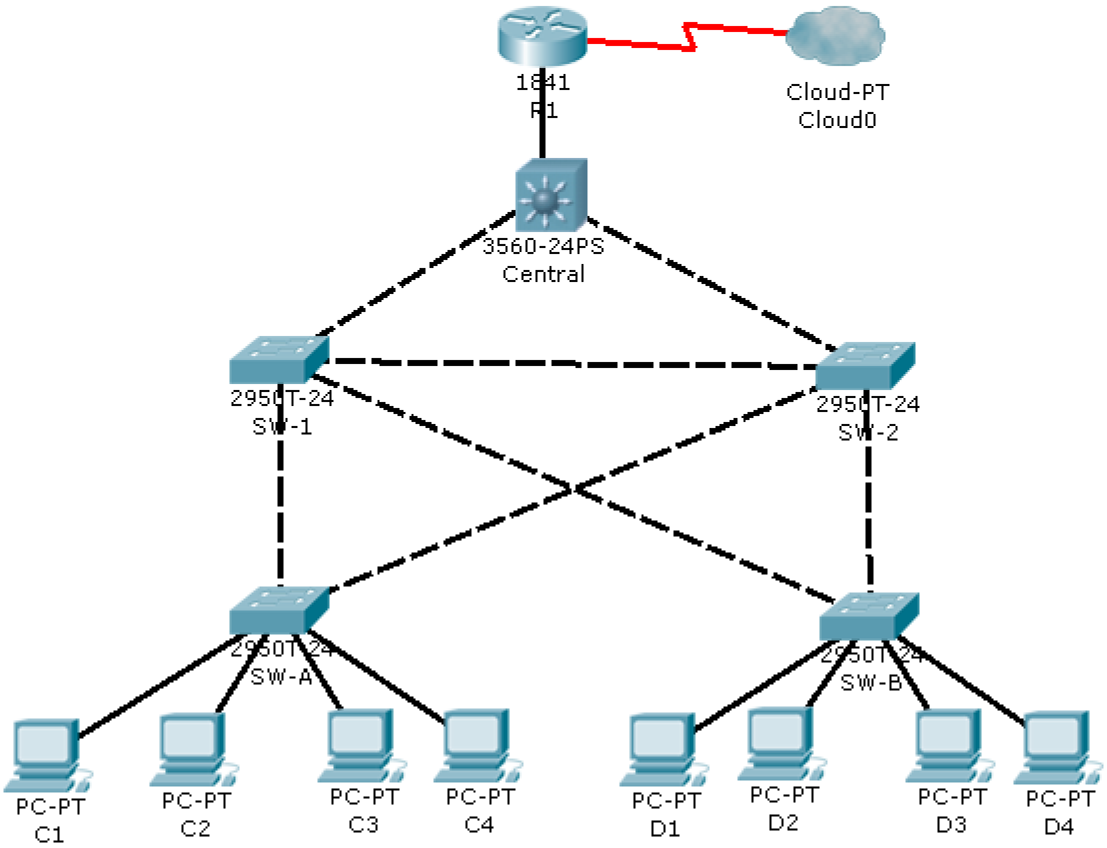
Step 5. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Layer 2 Security

Instructor Version

Topology Diagram



Objectives

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable storm control to prevent broadcast storms.
- Enable port security to prevent MAC address table overflow attacks.

Introduction

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent against spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. In addition, the network administrator would like to enable storm control to prevent broadcast storms. Finally, to prevent against MAC address table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses that can be learned per switch port. If the number of MAC addresses exceeds the set limit, the administrator would like for the port to be shutdown.

All switch devices have been preconfigured with the following:

- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

Task 1: Configure Root Bridge

Step 1. Determine the current root bridge.

From Central, issue the **show spanning-tree** command to determine the current root bridge and to see the ports in use and their status.

Which switch is the current root-bridge? Current root is SW-1

Based on the current root-bridge, what is the resulting spanning-tree? (Draw the spanning-tree topology.)

Step 2. Assign Central as the primary root bridge.

Using the **spanning-tree vlan 1 root primary** command, assign the 3560 Central switch as the root bridge.

```
Central(config)# spanning-tree vlan 1 root primary
```

Step 3. Assign SW-1 as a secondary root bridge.

Assign SW-1 as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

```
SW-1(config)# spanning-tree vlan 1 root secondary
```

Step 4. Verify the spanning-tree configuration.

Issue the **show spanning-tree** command to verify that 3560 Central switch is the root bridge.

Which switch is the current root-bridge? Current root is Central

Based on the new root-bridge, what is the resulting spanning-tree? (Draw the spanning-tree topology.)

Task 2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

Step 1. Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the SW-A and SW-B switches, use the **spanning-tree portfast** command.

```
SW-A(config)# interface range fastethernet 0/1 - 4
SW-A(config-if-range)# spanning-tree portfast

SW-B(config)# interface range fastethernet 0/1 - 4
SW-B(config-if-range)# spanning-tree portfast
```

Step 2. Enable BPDU guard on all access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on SW-A and SW-B access ports.

```
SW-A(config)# interface range fastethernet 0/1 - 4
SW-A(config-if-range)# spanning-tree bpduguard enable
```

```
SW-B(config)# interface range fastethernet 0/1 - 4
SW-B(config-if-range)# spanning-tree bpduguard enable
```

Note: Spanning-tree bpduguard can be enabled on each individual port using the command **`spanning-tree bpduguard enable`**, or in global configuration mode with the command **`spanning-tree portfast bpduguard default`**. For grading purposes, in this activity please use the **`spanning-tree bpduguard enable`** command.

Step 3. Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the **`show spanning-tree`** command to determine the location of the root port on each switch.

On switch SW-1, enable root guard on ports Fa0/23 and Fa0/24. On switch SW-2, enable root guard on ports Fa0/23 and Fa0/24.

```
SW-1(config)# interface fa0/23
SW-1(config-if)# spanning-tree guard root
SW-1(config-if)# interface fa0/24
SW-1(config-if)# spanning-tree guard root

SW-2(config)# interface fa0/23
SW-2(config-if)# spanning-tree guard root
SW-2(config-if)# interface fa0/24
SW-2(config-if)# spanning-tree guard root
```

Task 3: Enable Storm Control

Step 1. Enable storm control for broadcasts.

Enable storm control for broadcasts on all ports connecting switches (trunk ports). Set a **50** percent rising suppression level using the **`storm-control broadcast`** command. Enable storm-control on interfaces connecting Central, SW-1, and SW-2.

```
Example:
SW-1(config)# interface gi1/1
SW-1(config-if)# storm-control broadcast level 50
SW-1(config-if)# interface fa0/1
SW-1(config-if)# storm-control broadcast level 50
SW-1(config-if)# interface fa0/23
SW-1(config-if)# storm-control broadcast level 50
SW-1(config-if)# interface fa0/24
SW-1(config-if)# storm-control broadcast level 50

**Repeat on SW-2 (gig1/1, fa0/1, fa0/23, and fa0/24) and Central (gig0/1,
gig0/2, fa0/1) connection to other switches
```

Step 2. Verify storm control configuration.

Verify your configuration with the **`show storm-control broadcast`** command and the **`show run`** command.

Task 4: Configure Port Security and Disable Unused Ports

Step 1. Configure basic port security on all ports connected to host devices.

This procedure should be performed on all access ports on SW-A and SW-B. Set the maximum number of learned MAC address to **2**, allow the MAC address to be learned dynamically, and set the violation to **shutdown**.

Keep in mind that a switch port must be configured as an access port to enable port security.

```
Example:
SW-A(config)# interface FastEthernet 0/1
SW-A(config-if)# switchport mode access
SW-A(config-if)# switchport port-security
SW-A(config-if)# switchport port-security maximum 2
SW-A(config-if)# switchport port-security violation shutdown
SW-A(config-if)# switchport port-security mac-address sticky

**Repeat on other ports in SW-A and SW-B
```

Why would you not want to enable port-security on ports connected to other switches or routers?

Ports connected to other switch devices and routers can, and should, have a multitude of MAC addresses learned for that single port. Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality.

Step 2. Verify port security.

On SW-A, issue the **`show port-security interface fa0/1`** command to verify that port security has been configured.

Step 3. Disable unused ports.

Disable all ports that are currently unused. For efficiency purposes, the Activity Wizard will only grade Fa0/5 and Fa0/6 on SW-A and SW-B.

```
Example:
SW-A(config)# interface FastEthernet 0/5
SW-A(config-if)# shutdown

**Repeat on other ports on SW-A and SW-B
```

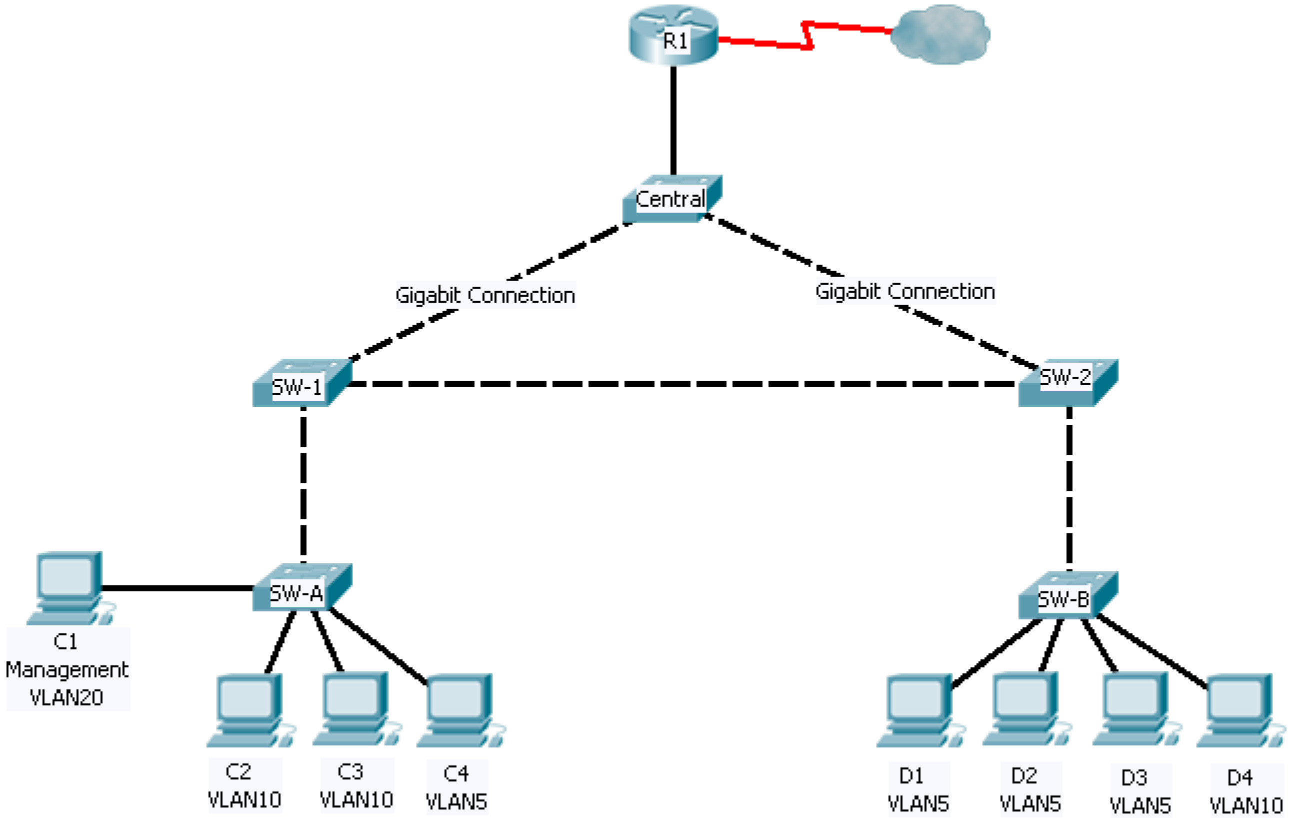
Step 4. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Layer 2 VLAN Security

Instructor Version

Topology Diagram



Objectives

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Introduction

A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to allow the management PC to be able to connect to all switches and the router, but does not want any other devices to be able to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

All devices have been preconfigured with:

- Enable secret password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

Task 1: Verify Connectivity

Step 1. Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

Step 2. Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

Note: If using the simple PDU GUI packet, be sure to **ping** twice to allow for ARP.

Task 2: Create a Redundant Link Between SW-1 and SW-2

Step 1. Connect SW-1 and SW-2.

Using a crossover cable, connect port Fa0/23 on SW-1 to port Fa0/23 on SW-2.

Step 2. Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both SW-1 and SW-2, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

```
SW-1(config)# interface fa0/23
SW-1(config-if)# no shutdown
SW-1(config-if)# switchport mode trunk
SW-1(config-if)# switchport trunk native vlan 15
SW-1(config-if)# switchport nonegotiate

SW-2(config)# interface fa0/23
SW-2(config-if)# no shutdown
SW-2(config-if)# switchport mode trunk
SW-2(config-if)# switchport trunk native vlan 15
SW-2(config-if)# switchport nonegotiate
```

Task 3: Enable VLAN 20 as a Management VLAN

The network administrator would like to be able to access all switch and routing devices using a management PC. For security, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1. Enable a management VLAN (VLAN 20) on SW-A.

Enable VLAN 20 on SW-A and use the default name of VLAN0020.

```
SW-A(config)# vlan 20
SW-A(config-vlan)# exit
```

Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

```
SW-A(config)# interface vlan 20
SW-A(config-if)# ip address 192.168.20.1 255.255.255.0
```

Step 2. Enable the same management VLAN on all other switches.

Be sure to create the VLAN on all switches: SW-B, SW-1, SW-2 and Central.

```
SW-B(config)# vlan 20
SW-B(config-vlan)# exit
SW-B(config)# interface vlan 20
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)# vlan 20
SW-1(config-vlan)# exit
SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0

SW-2(config)# vlan 20
SW-2(config-vlan)# exit
SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

Central(config)# vlan 20
Central(config-vlan)# exit
Central(config)# interface vlan 20
Central(config-if)# ip address 192.168.20.5 255.255.255.0
```

Step 3. Configure the management PC and connect it to SW-A port Fa0/1.

Ensure that the management PC is assigned an IP address within the 192.168.20.0/24 network. Connect the management PC to SW-A port Fa0/1.

Step 4. On SW-A, ensure the management PC is part of VLAN 20

Interface Fa0/1 must be part of VLAN 20.

```
SW-A(config)# interface fa0/1
SW-A(config-if)# switchport access vlan 20
SW-A(config-if)# no shutdown
```

Step 5. Verify connectivity of the management PC to all switches.

The management PC should be able to **ping** SW-A, SW-B, SW-1, SW-2 and Central.

Task 4: Enable the Management PC to Access Router R1

Step 1. Enable a new subinterface on router R1.

Create subinterface Fa0/0.3 and assign an IP address within the 192.168.20.0/24 network. Be sure to set encapsulation to dot1q 20 to account for VLAN 20.

```
R1(config)# interface fa0/0.3
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 192.168.20.100 255.255.255.0
```

Step 2. Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3. Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

Create an ACL(s) that denies any network from accessing the 192.168.20.0/24 network, but permits all other networks to access one another.

```
Example: (may vary from student configuration)
R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255
R1(config)# access-list 101 permit ip any any
```

Apply the ACL to the proper interface(s).

```
Example: (may vary from student configuration)
R1(config)# int fa0/0.1
R1(config-subif)# ip access-group 101 in
R1(config-subif)# int fa0/0.2
R1(config-subif)# ip access-group 101 in
```

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4. Verify Security.

From the management PC, **ping** SW-A, SW-B, and R1. Was the **ping** successful?

The ping should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.

From D1, **ping** the management PC. Was the **ping** successful?

The ping should have failed. This is because in order for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

Step 5. Check results.

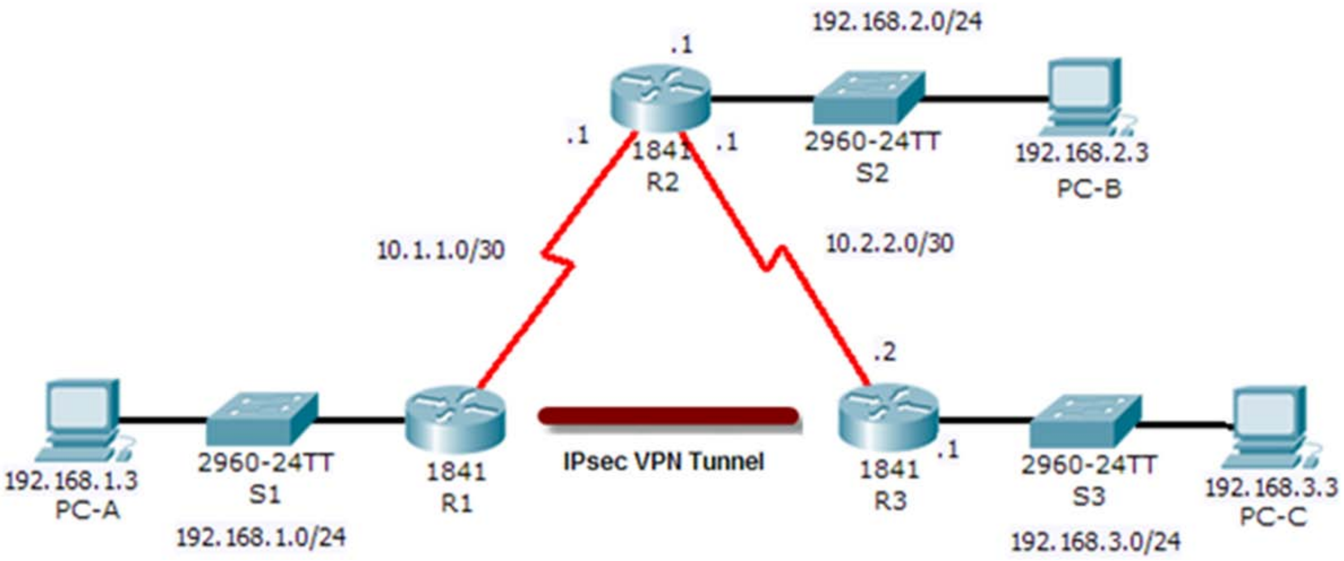
Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

Keep in mind that if all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.

PT Activity: Configure and Verify a Site-to-Site IPsec VPN using CLI

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.1.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
R2	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.2.1	255.255.255.0
	S0/0/1	10.2.2.1	255.255.255.252
R3	S0/0/1	10.2.2.2	255.255.255.252
	Fa0/0	192.168.3.1	255.255.255.0
PC-A	NIC	192.168.1.3	255.255.255.0
PC-B	NIC	192.168.2.3	255.255.255.0
PC-C	NIC	192.168.3.3	255.255.255.0

Learning Objectives

- Verify connectivity throughout the network.
- Configure router R1 to support a site-to-site IPsec VPN with R3.

Introduction

The network topology shows three routers. Your task is to configure routers R1 and R3 to support a site-to-site IPsec VPN when traffic flows from their respective LANs. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key distribution method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption algorithm	**DES**, 3DES, or AES	AES	AES
Hash algorithm	MD5 or **SHA-1**	**SHA-1**	**SHA-1**
Authentication method	Pre-shared keys or **RSA**	pre-share	pre-share
Key exchange	DH Group **1**, 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key		vpnpa55	vpnpa55

Note: Bolded parameters are defaults. Only unbolded parameters have to be explicitly configured.

IPsec Phase 2 Policy Parameters

Parameters	R1	R3
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24
Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

The routers have been pre-configured with the following:

- Password for console line: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- RIP version 2

Task 1: Configure IPsec parameters on R1

Step 1. Test connectivity.

Ping from PC-A to PC-C.

Step 2. Identify interesting traffic on R1.

Configure ACL **110** to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Remember that due to the implicit deny all, there is no need to configure a **deny any any** statement.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Step 3. Configure the ISAKMP Phase 1 properties on R1.

Configure the crypto ISAKMP policy **10** properties on R1 along with the shared crypto key **vpnpa55**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured therefore only the encryption, key exchange method, and DH method must be configured.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

Step 4. Configure the ISAKMP Phase 2 properties on R1.

Create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Step 5. Configure the crypto map on the outgoing interface.

Finally, bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface. Note: This is not graded.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Task 2: Configure IPsec Parameters on R3

Step 1. Configure router R3 to support a site-to-site VPN with R1.

Now configure reciprocating parameters on R3. Configure ACL **110** identifying the traffic from the LAN on R3 to the LAN on R1 as interesting.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Step 2. Configure the ISAKMP Phase 1 properties on R3.

Configure the crypto ISAKMP policy **10** properties on R3 along with the shared crypto key **vpnpa55**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

Step 3. Configure the ISAKMP Phase 2 properties on R1.

Like you did on R1, create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Step 4. Configure the crypto map on the outgoing interface.

Finally, bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/1 interface. Note: This is not graded.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Task 3: Verify the IPsec VPN

Step 1. Verify the tunnel prior to interesting traffic.

Issue the **show crypto ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.

Step 2. Create interesting traffic.

From PC-A, **ping** PC-C.

Step 3. Verify the tunnel after interesting traffic.

On R1, re-issue the **show crypto ipsec sa** command. Now notice that the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.

Step 4. Create uninteresting traffic.

From PC-A, **ping** PC-B.

Step 5. Verify the tunnel.

On R1, re-issue the **show crypto ipsec sa** command. Finally, notice that the number of packets has not changed verifying that uninteresting traffic is not encrypted.

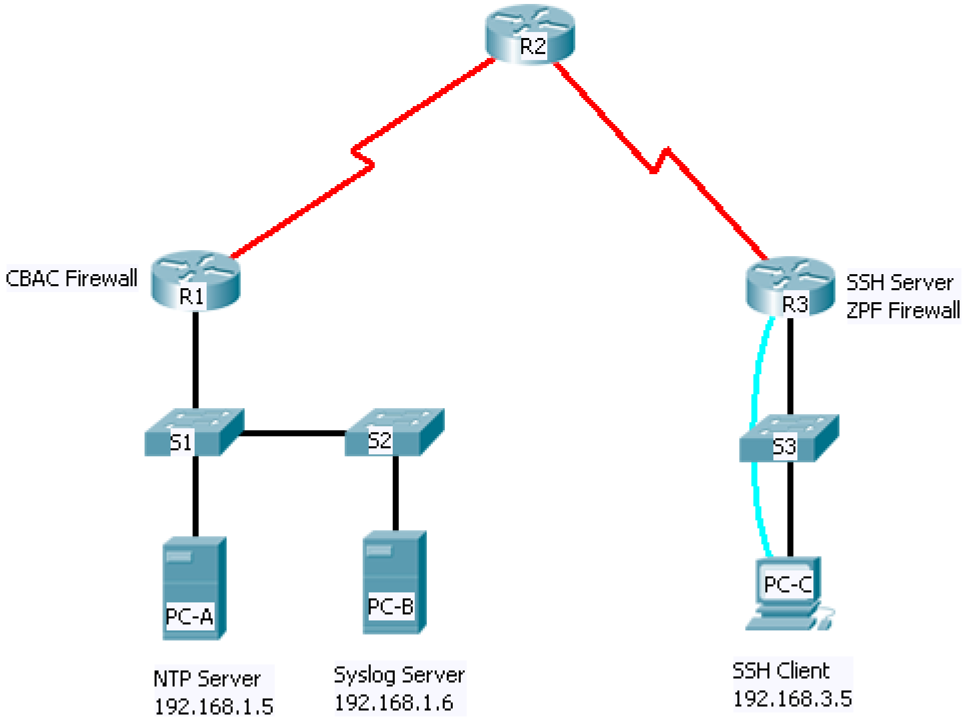
Step 6. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

PT Activity: Configure a Network for Secure Operation

Instructor Version

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	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	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 FA0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 FA0/6

Learning Objectives

- Secure the routers with strong passwords, password encryption and a login banner.
- Secure the console and VTY lines with passwords.
- Configure local AAA authentication.
- Configure SSH server.
- Configure router for syslog.
- Configure router for NTP.
- Secure the router against login attacks.
- Configure CBAC and ZPF firewalls.
- Secure network switches.

Introduction

In this comprehensive practice activity, you will apply a combination of security measures that were introduced in the course. These measures are listed in the objectives.

In the topology, R1 is the edge outer for the Company A while R3 is the edge router for Company B. These networks are interconnected via the R2 router which represents the ISP. You will configure various security features on the routers and switches for Company A and Company B. Not all security features will be configured on R1 and R3.

The following preconfigurations have been made:

- Hostnames on all devices
- IP addresses on all devices
- R2 console password: ciscoconpa55
- R2 password on VTY lines: ciscovtypa55
- R2 enable password: ciscoenpa55
- Static routing
- Syslog services on PC-B
- DNS lookup has been disabled
- IP default gateways for all switches

Task 1: Test Connectivity and Verify Configurations

Step 1. Verify IP addresses.

```
R1# show ip interface brief
R1# show run
```

Step 2. Verify routing tables.

```
R1# show ip route
```

Step 3. Test connectivity.

From PC-A, **ping** PC-C at IP address 192.168.3.5.

Task 2: Secure the Routers

Step 1. Set minimum a password length of 10 characters on router R1 and R3.

```
R1(config)# security passwords min-length 10
```

```
R3(config)# security passwords min-length 10
```

Step 2. Configure an enable secret password on router R1 and R3.

Use an enable secret password of **ciscoenpa55.**

```
R1(config)# enable secret ciscoenpa55
```

```
R3(config)# enable secret ciscoenpa55
```

Step 3. Encrypt plaintext passwords.

```
R1(config)# service password-encryption
```

```
R3(config)# service password-encryption
```

Step 4. Configure the console lines on R1 and R3.

Configure a console password of **ciscoconpa55** and enable login. Set the **`exec-timeout`** to log out after **5** minutes of inactivity. Prevent console messages from interrupting command entry.

```
R1(config)# line console 0
R1(config-line)# password ciscoconpa55
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

```
R3(config)# line console 0
R3(config-line)# password ciscoconpa55
R3(config-line)# exec-timeout 5 0
R3(config-line)# login
R3(config-line)# logging synchronous
```

Step 5. Configure vty lines on R1.

Configure a vty line password of **ciscovtypa55** and enable login. Set the **`exec-timeout`** to log out after **5** minutes of inactivity. Set the login authentication to use the default AAA list to be defined later.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypa55
R1(config-line)# exec-timeout 5 0
R1(config-line)# login authentication default
```

Note: The vty lines on R3 will be configured for SSH in a later task.

Step 6. Configure login banner on R1 and R3.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says: “`No Unauthorized Access!`”.

```
R1(config)# banner motd $No Unauthorized Access!$
```

```
R3(config)# banner motd $No Unauthorized Access!$
```

Task 3: Configure Local Authentication on R1 and R3

Step 1. Configure the local user database.

Create a local user account of **Admin01** with a secret password of **Admin01pa55**.

```
R1(config)# username Admin01 privilege 15 secret Admin01pa55
```

```
R3(config)# username Admin01 privilege 15 secret Admin01pa55
```

Step 2. Enable AAA services.

```
R1(config)# aaa new-model
```

```
R3(config)# aaa new-model
```

Step 3. Implement AAA services using the local database.

Create the default login authentication method list using local authentication with no backup method.

```
R1(config)# aaa authentication login default local none
```

```
R3(config)# aaa authentication login default local none
```

Task 4: Configure NTP

Step 1. Enable NTP authentication on PC-A.

On PC-A, choose the **Config** tab, and then the **NTP** button. Select **On** for NTP service. **Enable** authentication and enter a Key of **1** and a password of **ciscontppa55**.

Step 1. Configure R1 as an NTP Client.

Configure NTP authentication Key **1** with a password of **ciscontppa55**. Configure R1 to synchronize with the NTP server and authenticate using Key **1**.

```
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 ciscontppa55
R1(config)# ntp trusted-key 1
R1(config)# ntp server 192.168.1.5 key 1
```

Step 2. Configure routers to update hardware clock.

Configure routers to periodically update the hardware clock with the time learned from NTP.

```
R1(config)# ntp update-calendar
```

Task 5: Configure R1 as Syslog Client

Step 1. Configure R1 to timestamp log messages.

Configure timestamp service for logging on the routers.

```
R1(config)# service timestamps log datetime msec
```

Step 2. Configure R1 to log messages to the syslog server.

Configure the routers to identify the remote host (syslog server) that will receive logging messages.

```
R1(config)# logging 192.168.1.6
```

You should see a console message similar to the following:

```
SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514 started
- CLI initiated
```

Step 3. Check for syslog messages on PC-B.

On R1, exit config mode to generate a syslog message. Open the syslog server on PC-B to view the message sent from R1. You should see a message similar to the following on the syslog server:

```
%SYS-5-CONFIG_I: Configured from console by console
```

Task 6: Secure Router Against Login Attacks

Step 1. Log unsuccessful login attempts to R1.

```
R1(config)# login on-failure log
```

Step 2. Telnet to R1 from PC-A.

Telnet from PC-A to R1 and provide the username **Admin01** and password **Admin01pa55**. The Telnet should be successful.

Step 3. Telnet to R1 from PC-A and check syslog messages on the syslog server.

Exit from the current Telnet session and Telnet again to R1 using the username of **baduser** and any password. Check the syslog server on PC-B. You should see an error message similar to the following that is generated by the failed login attempt.

```
SEC_LOGIN-4-LOGIN_FAILED:Login failed [user:baduser] [Source:192.168.1.5]
[localport:23] [Reason:Invalid login] at 15:01:23 UTC Wed June 17 2009
```

Task 7: Configure SSH on R3

Step 1. Configure a domain name.

Configure a domain name of **ccnasecurity.com** on R3.

```
R3(config)# ip domain-name ccnasecurity.com
```

Step 2. Configure the incoming vty lines on R3.

Use the local user accounts for mandatory login and validation and accept only SSH connections.

```
R3(config)# line vty 0 4
R3(config-line)# exec-timeout 5 0
R3(config-line)# login local
R3(config-line)# transport input ssh
```

Step 3. Configure RSA encryption key pair for R3.

Any existing RSA key pairs should be erased on the router. If there are no keys currently configured a message will be displayed indicating this. Configure the RSA keys with a modulus of 1024.

```
R3(config)# crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

R3(config)# crypto key generate rsa [Enter]
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take a
few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Step 4. Configure SSH timeouts and authentication parameters.

Set the SSH timeout to **90** seconds, the number of authentication retries to **2**, and the version to **2**.

```
R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
```

```
R3(config)# ip ssh version  2
```

Task 8: Configure CBAC on R1

Step 1. Configure a named IP ACL.

Create an IP ACL named **OUT-IN** to block all traffic originating from the outside network.

```
R1(config)# ip access-list extended OUT-IN
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
```

Apply the access list to incoming traffic on interface Serial 0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group OUT-IN in
```

Step 2. Step 3. Confirm that traffic entering interface Serial 0/0/0 is dropped.

From the PC-A command prompt, **ping** PC-C. The ICMP echo replies are blocked by the ACL.

Step 3. Create an inspection rule to inspect ICMP, Telnet and HTTP traffic.

Create an inspection rule named **IN-OUT-IN** to inspect **ICMP**, **Telnet** and **HTTP** traffic.

```
R1(config)# ip inspect name IN-OUT-IN icmp
R1(config)# ip inspect name IN-OUT-IN telnet
R1(config)# ip inspect name IN-OUT-IN http
```

Step 4. Apply the inspect rule to the outside interface.

Apply the IN-OUT-IN inspection rule to the interface where traffic exits to outside networks.

```
R1(config)# interface s0/0/0
R1(config-if)# ip inspect IN-OUT-IN out
```

Step 5. Test operation of the inspection rule.

From the PC-A command prompt, **ping** PC-C. The ICMP echo replies should be inspected and allowed through.

Task 9: Configure ZPF on R3

Step 1. Test connectivity.

Verify that the internal host can access external resources.

- From PC-C, test connectivity with **ping** and Telnet to R2; all should be successful.
- From R2 **ping** to PC-C. The pings should be allowed.

Step 2. Create the firewall zones.

Create an internal zone named **IN-ZONE**.

```
R3(config)# zone security IN-ZONE
```

Create an external zone named **OUT-ZONE**.

```
R3(config)# zone security OUT-ZONE
```

Step 3. Create an ACL that defines internal traffic.

Create an extended, numbered ACL that permits all IP protocols from the 192.168.3.0/24 source network to any destination. Use **101** for the ACL number.

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

Step 4. Create a class map referencing the internal traffic ACL.

Create a class map named **IN-NET-CLASS-MAP** to match ACL 101.

```
R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit
```

Step 5. Specify firewall policies.

Create a policy map named **IN-2-OUT-PMAP** to determine what to do with matched traffic.

```
R3(config)# policy-map type inspect IN-2-OUT-PMAP
```

Specify a class type of **inspect** and reference class map **IN-NET-CLASS-MAP**.

```
R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
```

Specify the action of **inspect** for this policy map

```
R3(config-pmap-c)# inspect
```

You should see the following console message:

```
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection.
All protocols will be inspected.”
```

Exit to the global config prompt.

```
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

Step 6. Apply firewall policies.

Create a zone pair named **IN-2-OUT-ZPAIR**. Specify the source and destination zones that were created earlier.

```
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination
OUT-ZONE
```

Attach a policy map and actions to the zone pair referencing the policy map previously created, **IN-2-OUT-PMAP**.

```
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
```

Exit to the global config prompt and assign the internal and external interfaces to the security zones.

```
R3(config)# interface fa0/1
R3(config-if)# zone-member security IN-ZONE

R3(config-if)# interface s0/0/1
R3(config-if)# zone-member security OUT-ZONE
```

Step 7. Test firewall functionality.

Verify that the internal host can still access external resources.

- From PC-C, test connectivity with **ping** and Telnet to R2; all should be successful.
- From R2 **ping** to PC-C. The pings should now be blocked.

Task 10: Secure the Switches

Step 1. Configure an enable secret password on all switches.

Use an enable secret password of **ciscoenpa55.**

```
S1(config)# enable secret ciscoenpa55
```

Step 2. Encrypt plaintext passwords.

```
S1(config)# service password-encryption
```

Step 3. Configure the console lines on all switches.

Configure a console password of **ciscoconpa55** and enable login. Set the **exec-timeout** to log out after **5** minutes of inactivity. Prevent console messages from interrupting command entry.

```
S1(config)# line console 0
S1(config-line)# password ciscoconpa55
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
S1(config-line)# logging synchronous
```

Step 4. Configure vty lines on all switches.

Configure a vty line password of **ciscovtypa55** and enable login. Set the **exec-timeout** to log out after **5** minutes of inactivity. Set the basic login parameter.

```
S1(config)# line vty 0 4
S1(config-line)# password ciscovtypa55
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
```

Step 5. Secure trunk ports on S1 and S2.

Configure port Fa0/1 on S1 as a trunk port.

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode trunk
```

Configure port Fa0/1 on S2 as a trunk port.

```
S2(config)# interface FastEthernet 0/1
S2(config-if)# switchport mode trunk
```

Verify that S1 port Fa0/1 is in trunking mode.

```
S1# show interfaces trunk
```

Set the native VLAN on S1 and S2 trunk ports to an unused VLAN 99.

```
S1(config)# interface Fa0/1
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end

S2(config)# interface Fa0/1
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# end
```

Set the trunk ports on S1 and S2 so that they do not negotiate by turning off the generation of DTP frames.

```
S1(config)# interface Fa0/1
S1(config-if)# switchport nonegotiate

S2(config)# interface Fa0/1
S2(config-if)# switchport nonegotiate
```

Enable storm control for broadcasts on the S1 and S2 trunk ports with a 50 percent rising suppression level.

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# storm-control broadcast level 50
```

```
S2(config)# interface FastEthernet 0/1
S2(config-if)# storm-control broadcast level 50
```

Step 6. Secure access ports.

Disable trunking on S1, S2 and S3 access ports.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# switchport mode access

S1(config-if)# interface FastEthernet 0/6
S1(config-if)# switchport mode access

S2(config)# interface FastEthernet 0/18
S2(config-if)# switchport mode access

S3(config)# interface FastEthernet 0/5
S3(config-if)# switchport mode access

S3(config-if)# interface FastEthernet 0/6
S3(config-if)# switchport mode access
```

Enable PortFast on S1, S2, and S3 access ports.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# spanning-tree portfast

S1(config-if)#interface FastEthernet 0/6
S1(config-if)# spanning-tree portfast

S2(config)# interface FastEthernet 0/18
S2(config-if)# spanning-tree portfast

S3(config)# interface FastEthernet 0/5
S3(config-if)# spanning-tree portfast

S3(config-if)# interface FastEthernet 0/6
S3(config-if)# spanning-tree portfast
```

Enable BPDU guard on the switch ports previously configured as access only.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# spanning-tree bpduguard enable

S1(config-if)# interface FastEthernet 0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface FastEthernet 0/18
S2(config-if)# spanning-tree bpduguard enable

S3(config)# interface FastEthernet 0/5
S3(config-if)# spanning-tree bpduguard enable

S3(config-if)# interface FastEthernet 0/6
S3(config-if)# spanning-tree bpduguard enable
```

Enable basic default port security on all end-user access ports that are in use. Use the **`sticky`** option. Re-enable each access port to which port security was applied.

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# shutdown
```

```
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# no shutdown

S1(config-if)# interface FastEthernet 0/6
S1(config-if)# shutdown
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# no shutdown

S2(config)# interface FastEthernet 0/18
S2(config-if)# shutdown
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security mac-address sticky
S2(config-if)# no shutdown

S3(config)# interface FastEthernet 0/5
S3(config-if)# shutdown
S3(config-if)# switchport port-security
S3(config-if)# switchport port-security mac-address sticky
S3(config-if)# no shutdown

S3(config-if)# interface FastEthernet 0/6
S3(config-if)# shutdown
S3(config-if)# switchport port-security
S3(config-if)# switchport port-security mac-address sticky
S3(config-if)# no shutdown
```

Disable any ports not being used on each switch.

```
S1(config)# interface range Fa0/2 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range Fa0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range gigabitethernet1/1 - 2
S1(config-if-range)# shutdown

S2(config)# interface range Fa0/2 - 17
S2(config-if-range)# shutdown
S2(config-if-range)# interface range Fa0/19 - 24
S2(config-if-range)# shutdown
S3(config-if-range)# interface range gigabitethernet1/1 - 2
S2(config-if-range)# shutdown

S3(config)# interface range Fa0/1 - 4
S3(config-if-range)# shutdown
S3(config-if-range)# interface range Fa0/7 - 24
S3(config-if-range)# shutdown
S3(config-if-range)# interface range gigabitethernet1/1 - 2
S3(config-if-range)# shutdown
```

Task 11: Verification

Step 1. Test SSH configuration.

Attempt to connect to R3 via Telnet from PC-C.

From PC-C, enter the command to connect to R3 via Telnet at IP address 192.168.3.1.

This connection should fail, since R3 has been configured to accept only SSH connections on the virtual terminal lines.

From PC-C, enter the **ssh –l Admin01 192.168.3.1** command to connect to R3 via SSH.

When prompted for the password, enter the password **Admin01pa55** configured for the local administrator.

Use the **show ip ssh** command to see the configured settings.

```
R3# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
```

Step 2. Verify timestamps, NTP status for R1 and PC-A.

```
R1# show clock
*17:28:49.898 UTC Tue May 19 2009

R1# show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**19
reference time is CD99AF95.0000011B (15:00:37.283 UTC Tue May 19 2009)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```

Step 3. Test CBAC firewall on R1.

- **Ping** from PC-A to R2 at 10.2.2.2 (should succeed)
- Telnet from PC-A to R2 10.2.2.2 (should succeed)
- **Ping** from R2 to PC-A at 192.168.1.3 (should fail)

Step 4. Test ZPF firewall on R3.

- **Ping** from PC-C to R2 at 10.2.2.2 (should succeed)
- Telnet from PC-C to R2 at 10.2.2.2 (should succeed)
- **Ping** from R2 to PC-C at 192.168.3.5 (should fail)
- Telnet from R2 to R3 at 10.2.2.1 (should fail – only SSH is allowed)

Step 5. Verify port security.

On S2, use the **show run** command to confirm that S2 has added a sticky MAC address for Fa0/18. This should be the MAC address of PC-B. Record the MAC address for later use.

```
S2#show run
Building configuration...
<output omitted>
interface FastEthernet0/18
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.435D.3057
 spanning-tree portfast
 spanning-tree bpduguard enable
<output omitted>
```

Select PC-B. Go to the **Config** tab. Select **FastEthernet** under the Interface section. Edit the MAC address field. For example, change it from 0001.435D.3057 to 0001.435D.AAAA.

This should cause a port security violation and S2 should shut down port Fa0/18.

Use the **show interface Fa0/18** command to view the status of the port. The port should be in the err-disabled state.

```
S2#show int fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
<output omitted>

S2#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
      Fa0/18        1           1                 1         Shutdown
----------------------------------------------------------------------
```

On PC-B, go to the **Config** tab. Select **FastEthernet** under the Interface section. Change the MAC address to another address. For example, change it from 0001.435D.AAAA to 0001.435D.BBBB.

From interface configuration mode on switch S2 for Fa0/18, use the **no switchport port-security mac-address sticky *address*** command to remove the original PC-B learned address.

```
S2(config)# int fa0/18
S2(config-if)# no switchport port-security mac-address sticky
0001.435D.3057
```

Shutdown and then re-enable the Fa0/18 interface.

```
S2(config)# int fa0/18
S2(config-if)# shutdown
S2(config-if)# no shutdown
```

On S2, use the **show run** command to confirm that the port comes up and that the new MAC address has been learned.

```
S2#show run
Building configuration...
<output omitted>
interface FastEthernet0/18
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.435D.BBBB
 spanning-tree portfast
 spanning-tree bpduguard enable
<output omitted>
```

Note: If it is desired to reconnect the PC with the original MAC address, you can simply change the MAC address on the PC back to the original one and issue the **shutdown** and **no shut down** commands on port Fa0/18. If the PC or a NIC is being replaced and will have a new MAC address, you must first remove the old learned address.

Step 6. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.