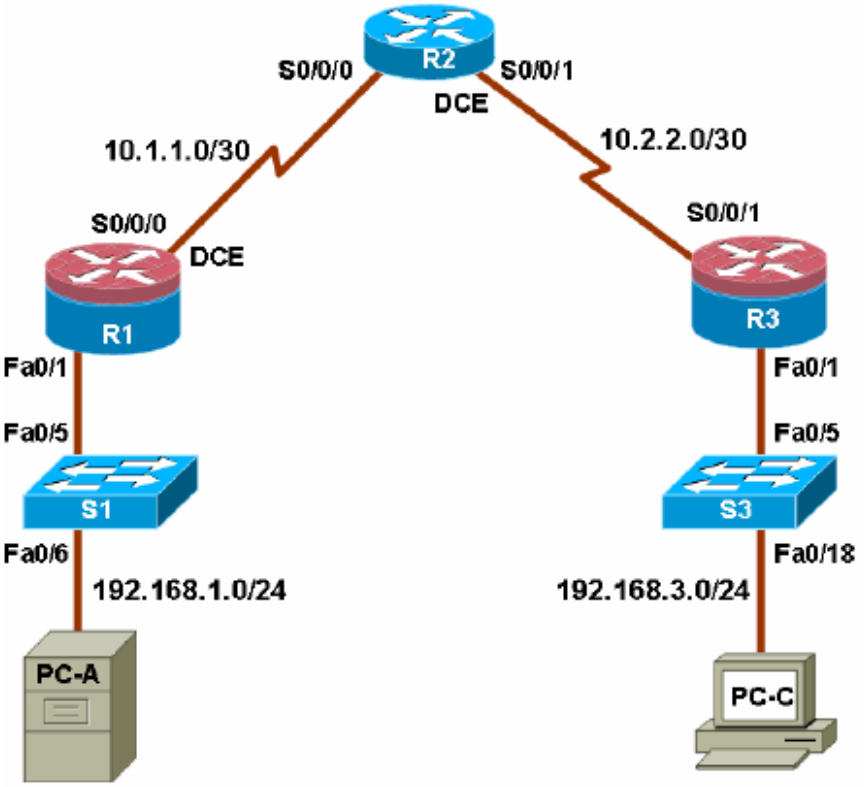
Lab: Chapter 5 Lab A, Configuring an Intrusion Prevention System (IPS) Using the CLI and SDM

Topology



IP 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	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Objectives

Part 1: Basic Router Configuration
• Configure hostname, interface IP addresses and access passwords.
• Configure the static routing.

Part 2: Configuring an IOS Intrusion Prevention System (IPS) using CLI
• Configure IOS IPS using CLI.

• Examine the resulting IPS configuration.
• Verify IPS functionality.
• Log IPS messages to a Syslog server.

Part 3: Use the Nmap port scanner to test for vulnerabilities.

Background

In this lab, you configure the Cisco IOS Intrusion Prevention System (IPS), which is part of the Cisco IOSFirewall feature set. IPS examines certain attack patterns and alerts or mitigates when those patterns occur.

IPS alone is not enough to make a router into a secure Internet firewall, but in addition to other securityfeatures, it can be a powerful defense.
You will configure the IPS using the Cisco IOS CLI on one router
Depending on the model of the router and Cisco IOS version, the available commands and the output produced might vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Part 1: Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings such as host names, interface IP addresses, static routing, device access, and passwords.
Note: Perform all tasks on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

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

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

Step 2: Configure the basic settings for each router.

a. Configure the host names as shown in the topology.
b. Configure the interface IP addresses as shown in the IP addressing table.
c. Configure a clock rate for serial router interfaces with a DCE serial cable attached.

```
R1(config)#interface S0/0/0
R1(config-if)#clock rate 64000
```

d. To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Step 3: Configure static routing on the routers.

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

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IPaddressing table.

Step 5: Verify basic network connectivity.

a. Ping from R1 to R3.
Were the results successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.
Were the results successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the static routing protocol is configuredand functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct,use the **show run** and **show ip route** commands to identify routing protocol-related problems.

Step 6: Configure and encrypt passwords.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

a. Configure a minimum password length using the **security passwords** command to set a minimum password length of 10 characters.

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

b. Configure a console password and enable login for router R1. For additional security, the **exectimeout**
command causes the line to log out after 5 minutes of inactivity. The **logging synchronous**command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered to be a good security practice.

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

c. Configure a password for the aux port for router R1.

```
R1(config)#line aux 0
R1(config-line)#password ciscoauxpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
```

d. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
```

```
R1(config-line)#login
```
e. Encrypt the console, aux, and vty clear text passwords.
```
R1(config)#service password-encryption
```
f. Issue the **show run** command. Can you read the console, aux, and vty passwords? Why or why not? _____

Step 7: Save the basic configurations for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.
```
R1#copy running-config startup-config
```

Part 2: Configuring IPS Using the Cisco IOS CLI

In Part 2 of this lab, you configure IPS on R1 using the Cisco IOS CLI. You then review and test the resultingconfiguration.

Task 1: Verify Access to the R1 LAN from R2

In this task, you verify that without IPS configured, the external router R2 can ping the R1 S0/0/0 interface andPC-A on the R1 internal LAN.

Step 1: Ping from R2 to R1.

a. From R2, ping R1 interface S0/0/0 at IP address 10.1.1.1.
```
R2#ping 10.1.1.1
```
b. Were the results successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Ping from R2 to PC-A on the R1 LAN.

a. From R2, ping PC-A on the R1 LAN at IP address 192.168.1.3.
```
R2#ping 192.168.1.3
```
b. Were the results successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 3: Display the R1 running config prior to configuring IPS.

a. Issue the **show run** command to review the current basic configuration on R1.
b. Are there any security commands related to IPS?

Task 2: Configure IPS

Step 1: Create an IPS rule.

a. On R1, create an IPS rule name using the **ip ips name** *name* command in global configuration mode. Name the IPS rule iosips. This will be used later on an interface to enable IPS.
The rule will use the inspection signatures contained in the attack-drop.sdf file stored in flash.
The file contains high fidelity (or "high probability") IPS signatures. More can be deducted from:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps3990/product_data_sheet0900aecd803ac128.html

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

b. You can specify an optional extended or standard access control list (ACL) to filter the traffic that will
be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

c. To see the options available for specifying an ACL with the rule name, use the **ipips name** command and the CLI help function (**?**).
```
R1(config)#ip ips name ips list ?
<1-199>Numbered access list
WORD Named access list
```

Step 3: Enable IPS SDEE event notification.

The Cisco Security Device Event Exchange (SDEE) server is a Simple Object Access Protocol (SOAP)based, intrusion detection system (IDS) alert format and transport protocol specification. SDEE replaces Cisco RDEP.

To use SDEE, the HTTP server must be enabled with the **`ip http server`** command. If the HTTP server isnot enabled, the router cannot respond to the SDEE clients because it cannot see the requests. SDEEnotification is disabled by default and must be explicitly enabled.

Note: SDM Monitor uses HTTP and SDEE to capture IPS events.
To enable SDEE, use the following command.

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

Step 4: Enable IPS syslog support.

IOS IPS also supports the use of syslog to send event notification. SDEE and syslog can be used independently or enabled at the same time to send IOS IPS event notification. Syslog notification is enabledby default.

a. If logging console is enabled, you see IPS syslog messages. Enable syslog if it is not enabled.

```
R1(config)#ip ips signature 2001 disable
(In order to prevent logs of ICMP events during this lab.)
R1(config)#ip ips notify log
```

b. Use the **`show clock`** command to verify the current time and date for the router. Use the **`clock set`**command from privileged EXEC mode to reset the clock if necessary. The following is an example of how to set the clock.

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

c. 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
```

d. To send log messages to the syslog server on PC-A, use the following command:

```
R1(config)#logging 192.168.1.3
```

e. To see the type and level of logging enabled on R1, use the **`show logging`** command.

```
R1#show logging
```

Note: Verify that you have connectivity between R1 and PC-A by pinging from PC-A to the R1 Fa0/1 interface
IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.

Step 5: Start the syslog server. (Kiwi)

If a syslog server is not currently available on PC-A, you can download the latest version of Kiwi from http://www.kiwisyslog.com or Tftpd32 from http://tftpd32.jounin.net/. If the syslog server is available on thePC, go to Step 6.

Step 7: Apply the IPS rule to an interface.

a. Apply the IPS rule to an interface with the **`ip ips`** *`name direction`* command in interface configuration mode. Apply the rule you just created inbound on the S0/0/0 interface. 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. To enable IPS to inspect both in and out traffic, enter the IPS rule name for in and out separately on the same interface.

```
R1(config)#interface serial0/1/0
R1(config-if)#ip ips iosips in
```

```
Jan 6 03:03:30.495: %IPS-6-ENGINE_BUILDS_STARTED: 03:03:30 UTC Jan 6
2008
Jan 6 03:03:30.495: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1
of 13 engines
Jan 6 03:03:30.511: %IPS-6-ENGINE_READY: atomic-ip - build time 16 ms –
packets for this engine will be scanned
Jan 6 03:03:30.511: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16 ms
```
The message also displays on the syslog server if it is enabled.

b. Although the R1 Fa0/1 interface is an internal interface, it might be desirable to configure it with IPS to respond to internal attacks. Apply the IPS rule to the R1 Fa0/1 interface in the inbound direction.
```
R1(config)#interface fa0/1
R1(config-if)#ip ips iosips in
```

Step 8: Save the running configuration.

Enter privileged EXEC mode using the **enable** command and provide the enable password cisco12345.
```
R1#copy run start
```

Step 4: Verify that the signature package is properly compiled.

a. Use the **show ip ips statistics** command to see the counts for the signature package.

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? _____

```
(R1#show ip ips all)
```

Part 3: Test IPS with NMAP

From PC-C

Start NMAP: C:\Program Files\Nmap\zenmap.exe

Run an intense scan towards PC-A

TCP SYN FIN is probably the best known illegal combination. Remember that SYN is used to start a connection, while FIN is used to end an existing connection. It is nonsensical to perform both actions at the same time. Many scanning tools use SYN FIN packets, because many intrusion detection systems did not catch these in the past, although most do so now. You can safely assume that any SYN FIN packets you see are malicious.

An attacker uses a TCP NULL scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with no flags in the packet header, generating packets that are illegal based on RFC 793.

Observe the Syslog messages on R1.

a. What is the IPS risk rating or severity level (Sev:) of the TCP SYN/FIN, signature 3041? _____

b. What is the IPS risk rating or severity level (Sev:) of the TCP NULL, signature 3040? _____

c. In Nmap, click the topology tab. What OS is most probable to be running on the host 192.168.1.3? _____

d. Click the host details tab and look at the TCP-sequence. What difficulty level is determined? ____