



Lab 2.1.6 Configure a Router with the IOS Intrusion Prevention System

Objective

In this lab, the students will complete the following tasks:

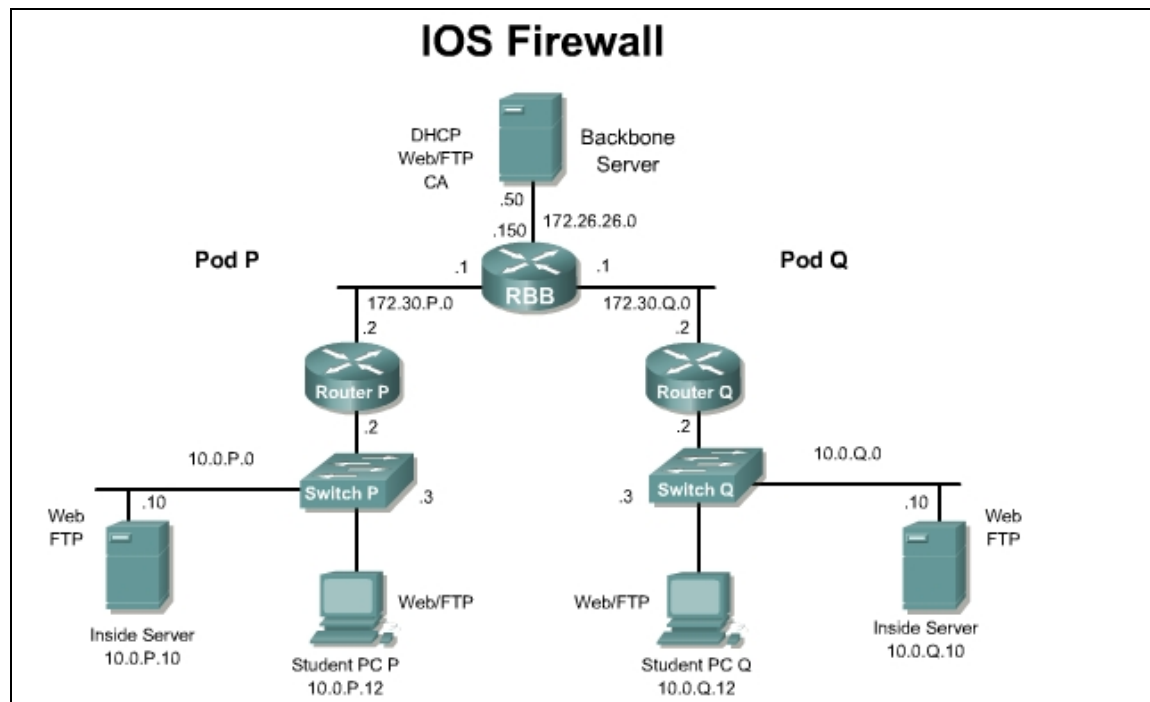
- Initialize the Intrusion Protection System (IPS) on the router.
- Disable signatures.
- Merge signature definition files.
- Verify the IPS configuration.
- Generate a test message.

Scenario

A company wants additional network protection beyond stateful inspection at the perimeter. The security policy has been updated to require basic intrusion prevention at the perimeter of the network. This will allow the perimeter router to take appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the Student Lab Orientation if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- The signature definition file, attack-drop.sdf

Additional materials

The latest attack-drop.sdf file can be downloaded from the following URL. A valid CCO login is required to access the site.

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>

Command List

In this lab exercise, the following switch commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Router Commands

Command	Description
<code>ip ips <i>ips-name</i> {in out} [list <i>acl</i>]</code>	To apply an IPS rule to an interface, use the <code>ip ips</code> command in interface configuration mode.
<code>ip ips fail closed</code>	To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the <code>ip ips fail closed</code> command in global configuration mode.
<code>ip ips name <i>ips-name</i></code>	To specify an IPS rule, use the <code>ip ips name</code> command in global configuration mode.
<code>ip ips signature <i>signature-id[:sub-signature-id]</i> {delete disable list <i>acl-list</i>}</code>	To attach a policy to a signature, use the <code>ip ips signature</code> command in global configuration mode.
<code>ip ips sdf location <i>url</i></code>	To specify the location in which the router will load the signature definition file (SDF), use the <code>ip ips sdf location</code> command in global configuration mode.
<code>show ip ips {[all] [configuration] [interfaces] [name <i>name</i>] [statistics [reset]] [sessions [details]] [signatures [details]]}</code>	To display IPS information such as configured sessions and signatures, use the <code>show ip ips</code> command in privileged EXEC mode.

Step 1 Initialize the IPS on the Router

Complete the following steps to initialize IPS on the router:

- a. From the student PC, access the router console.

- b. Switch to privileged-EXEC mode:

```
RouterP> enable
```

(Where P = pod number)

```
Password: cisco
```

- c. Switch to global configuration mode:

```
RouterP# configure terminal
```

```
RouterP(config)#
```

- d. Configure the router to use the built in signature definition file (SDF).

```
RouterP(config)# ip ips sdf builtin
```

- e. Create an IPS rule named **SECURIPS**.

```
RouterP(config)# ip ips name SECURIPS
```

- f. Enter interface configuration mode for Fa 0/1.

```
RouterP(config)# interface fastEthernet 0/1
```

- g. Apply the IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.

```
RouterP(config-if)# ip ips SECURIPS in
```

Note	The router prompt is suspended while the signature engines are being built. The router prompt will be available again after the engines are built.
-------------	--

- h. If the NetBIOS name service is running on the student PC, it may trigger an IPS signature in the router. The debug message for the signature will be similar to the following example:

```
*May 19 22:56:40.884: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP  
Bomb [10.0.P.12:137 -> 10.0.P.255:137]
```

Disable this signature with the **ip ips signature 4050 disable** command in global configuration mode.

- i. Exit to global configuration mode.

```
RouterP(config-if)# exit
```

- j. Configure logging to the student PC.

```
RouterP(config)# logging 10.0.P.12
```

- k. Configure a trap level to log messages at the level of 4 or lower.

```
RouterP(config)# logging trap warnings
```

- l. Turn on logging.

```
RouterP(config)# logging on
```

- m. Exit to privileged mode using **Ctrl+Z** or the **end** command.

```
RouterP(config)# ^Z
```

- n. Display the IPS configuration.

```
RouterP# show ip ips configuration
```

```
Configured SDF Locations: none
Builtin signatures are enabled and loaded
Last successful SDF load time: 22:30:12 UTC May 19 2005
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is disabled
Total Active Signatures: 132
Total Inactive Signatures: 0
Signature 4050:0 disable
Signature 1107:0 disable
IPS Rule Configuration
  IPS name SECURIPS
Interface Configuration
  Interface FastEthernet0/1
    Inbound IPS rule is SECURIPS
    Outgoing IPS rule is not set
```

1. How many active signatures are configured?

2. What IPS signatures are disabled?

Step 2 Load Signatures

Complete the following steps to replace the existing signatures in the router with the latest IPS signature file, attack-drop.sdf.

- a. Verify that the attack-drop.sdf file is present in the flash memory of the pod router. If the file is present, proceed to sub-step c.

```
RouterP# show flash
```

```
System flash directory:
```

File	Length	Name/status
1	16077820	c2600-advsecurityk9-mz.123-14.T1.bin
2	1038	home.shtml
3	1654	sdmconfig-26xx.cfg
4	113152	home.tar
5	820224	common.tar
6	3085312	sdm.tar
7	93095	attack-drop.sdf

```
[20192748 bytes used, 12837392 available, 33030140 total]
```

```
32768K bytes of processor board System flash (Read/Write)
```

- b. If necessary, load the SDF file into the flash memory of the router.

```
RouterP# copy tftp://10.0.P.12/attack-drop.sdf flash:attack-drop.sdf
Destination filename [attack-drop.sdf]?<Enter>
Accessing tftp://10.0.P.12/attack-drop.sdf...
Erase flash: before copying? [confirm]n
Loading attack-drop.sdf from 10.0.P.12 (via FastEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!
[OK - 93095 bytes]
```

- c. Enter global configuration mode and create an IPS rule

```
RouterP# configure terminal
RouterP(config)# ip ips name SECURIPS
```

- d. Specify the location where the router will load the SDF. If this command is not issued, the router will load the default SDF.

```
RouterP(config)# ip ips sdf location flash:attack-drop.sdf
```

- e. View the IPS configuration and answer the following questions.

```
RouterP# show ip ips configuration
```

1. What are the configured SDF locations?

2. What information is provided about the built in signatures?

- f. Configure the router to drop all packets until the signature engine is built and ready to scan traffic with the **ip ips fail closed** command. If this command is issued, one of the following scenarios will occur:

- If IPS fails to load the SDF, all packets will be dropped unless the user specifies an ACL for packets to send to IPS.
- If IPS successfully loads the SDF but fails to build a signature engine, all packets that are destined for that engine will be dropped.

If this command is not issued, all packets will be passed without scanning if the signature engine fails to build.

```
RouterP(config)# ip ips fail closed
```

- g. Enter interface configuration mode for Fa 0/1.

```
RouterP(config)# interface fastEthernet 0/1
```

- h. Remove the existing IPS rule at the interface.

```
RouterP(config-if)# no ip ips SECURIPS in
```

- i. Apply an IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.

```
RouterP(config-if)# ip ips SECURIPS in
```

Note	Whenever signatures are replaced or merged, the router prompt is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.
-------------	---

- j. Exit configuration mode.

```
RouterP(config-if)# ^Z
```

- k. View the IPS configuration and answer the following questions.

```
RouterP# show ip ips configuration
Configured SDF Locations:
  flash:attack-drop.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 00:20:07 UTC May 20 2005
IPS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is disabled
Total Active Signatures: 82
Total Inactive Signatures: 0
IPS Rule Configuration
  IPS name SECURIPS
Interface Configuration
  Interface FastEthernet0/1
    Inbound IPS rule is SECURIPS
    Outgoing IPS rule is not set
```

1. What are the configured SDF locations?

2. What information is provided about the built in signatures?

3. What is the total number of active signatures?

- l. Review the IPS signature engine configuration.

```
RouterP# show ip ips signatures
```

Step 3 Merge the attack-drop.sdf File with the Default, Built-in Signatures

It may be necessary to merge the built-in signatures with the attack-drop.sdf file if the built-in signatures are not providing the network with adequate protection from security threats. Complete the following steps to add the SDF and to change default parameters for a specific signature within the SDF or signature engine.

- a. Reload the built-in signatures.

```
RouterP(config)# no ip ips sdf location flash:attack-drop.sdf
RouterP(config)# int fastEthernet 0/1
RouterP(config-if)# no ip ips SECURIPS in
RouterP(config-if)# ip ips SECURIPS in
```

- b. From privileged EXEC mode, merge the flash-based SDF file, attack-drop.sdf, with the built-in signatures.

```
RouterP(config-if)# end
```

```
RouterP# copy flash:attack-drop.sdf ips-sdf
```

This command is used to merge the SDF with the signatures that are already loaded in the router, unless the /erase keyword is issued.

- c. Save the newly merged signatures in a new file.

```
RouterP# copy ips-sdf flash:my-signatures.sdf
```

- d. Configure the router to use new file.

```
RouterP(config)# ip ips sdf location flash:my-signatures.sdf
```

- e. Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.

```
RouterP(config)# interface fastEthernet 0/1
```

```
RouterP(config-if)# no ip ips SECURIPS in
```

- f. Reapply the rule set to interface.

```
RouterP(config-if)# ip ips SECURIPS in
```

- g. Leave interface configuration mode:

```
RouterP(config-if)# exit
```

- h. Leave global configuration mode:

```
RouterP(config)# exit
```

- i. View the IPS configuration and answer the following questions.

```
RouterP# show ip ips configuration
```

```
Configured SDF Locations:
```

```
flash:my-signatures.sdf
```

```
Builtin signatures are enabled but not loaded
```

```
Last successful SDF load time: 00:31:50 UTC May 20 2005
```

```
IPS fail closed is enabled
```

```
Fastpath ips is enabled
```

```
Quick run mode is enabled
```

```
Event notification through syslog is enabled
```

```
Event notification through SDEE is disabled
```

```
Total Active Signatures: 183
```

```
Total Inactive Signatures: 0
```

```
Signature 4050:0 disable
```

```
Signature 1107:0 disable
```

```
IPS Rule Configuration
```

```
IPS name SECURIPS
```

```
Interface Configuration
```

```
Interface FastEthernet0/1
```

```
Inbound IPS rule is SECURIPS
```

```
Outgoing IPS rule is not set
```

1. What are the configured SDF locations?

2. What information is provided about the built in signatures?

3. What is the total number of active signatures?

Step 4 Verify the Configuration

Complete the following steps to verify the configuration.

- a. Display the IPS configuration:

```
RouterP# show ip ips configuration
```

The parameters that were just configured along with several default settings are displayed.

- b. Display the IPS interface configuration:

```
RouterP# show ip ips interface
```

```
Interface Configuration
```

```
Interface FastEthernet0/1
```

```
Inbound IPS rule is SECURIPS
```

```
Outgoing IPS rule is not set
```

Step 5 Generate a Test Message

Complete the following steps to generate a test message.

- a. Start the Syslog server on the Student PC.
- b. Send multiple fragmented packets to the perimeter router of the peer pod using the following special technique:

```
RouterP# ping
```

```
Protocol [IP] <Enter>
```

```
Target IP address: 172.30.Q.2
```

```
Repeat count [5]: 20
```

```
Datagram size [100]: 2000
```

```
Timeout in seconds [2]: <Enter>
```

```
Extended commands [n]: <Enter>
```

```
Sweep range of sizes [n]: <Enter>
```

(Where Q = peer pod number)

The router will now send multiple fragmented packets to the peer router. This will cause the audit rules to generate events to the Syslog server.

- c. Analyze the Syslog messages on the Syslog server. The following messages should also appear on the router console session:
 1. What signatures are shown in the Syslog server messages?
