CHAPTER 23

# Implementing Cisco IDS and IPS

A good network security boundary is designed to prevent unauthorized access by malicious attackers. Although network security has evolved in recent years, so have the attacks. Today, various attacks are actually delivered inside of innocent-looking packets. Consequently, security has advanced well beyond a policy to permit some packets and deny the rest.

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) allow a network to examine packets and decide whether to simply notify an administrator or take some sort of corrective or preventative action. IDS and IPS are often used together to provide additional layers of protection for the network.

This chapter first explains the differences between and unique attributes of IDS and IPS. The different types of IDS and IPS are explored, as well as the various signatures used by the two systems. The chapter then details how to configure IDS and IPS in a Cisco environment.

## "Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 10-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 23-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

**Table 23-1** *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

| Foundation Topics Section | Questions Covered in This Section | Score |
|---|---|---|
| IDS and IPS Functions and Operations | 1–2 | |
| Categories of IDS and IPS | 3–4 | |
| IDS and IPS Signatures | 5 | |

*continues*

**Table 23-1** *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping (Continued)*

| Foundation Topics Section | Questions Covered in This Section | Score |
|---|---|---|
| Signature Reaction | 6 | |
| Cisco IOS Configuration | 7–8 | |
| SDM Configuration | 9–10 | |
| **Total Score** | | |

1. Where are IDS and IPS devices located in a network?
   a. An IDS device sits in the path of traffic, while an IPS device sits outside traffic flows.
   b. Both the IDS and IPS devices sit in the path of network traffic.
   c. An IPS device sits in the path of traffic, while an IDS device sits outside of traffic flows.
   d. Both IDS and IPS devices sit outside traffic flowing through the network.
   e. IDS or IPS devices can sit either in the path of traffic or outside the path of traffic. The location determines the functionality.
2. How can an IDS block unsafe network traffic?
   a. An IDS cannot block network traffic.
   b. An IDS can communicate configuration information to other network devices, such as routers and firewalls.
   c. Because the IDS sits in the path of network traffic, it can easily block the traffic itself.
   d. The IDS tells the IPS to block the traffic.
   e. When the IDS sends an alert, other network devices dynamically react according to the alert message.
3. Which of the following are characteristics of NIDS and NIPS (select all that apply)?
   a. Can examine encrypted traffic
   b. Handles additional hosts without additional resources
   c. Can assess the success or failure of an attack
   d. Can detect network reconnaissance attacks
   e. Can detect DoS attacks
   f. Ensures that proper use credentials are used, either from the local database or the AAA server

4. In an anomaly-based system, what is considered statistical information?
   a. Dynamically learned information
   b. Default rules in the IDS and IPS
   c. Statically configured rules in the IDS and IPS
   d. Manually learned information
   e. Information that is transferred into the router via TFTP
5. Which of the following are categories of IDS and IPS signatures (select all that apply)?
   a. Honeypot
   b. Exploit
   c. Anomaly
   d. Connection
   e. String
6. Which of the following actions of an IDS or IPS device is normally not the only action performed?
   a. Send an alarm
   b. Drop the packet
   c. Reset the connection
   d. Block the source IP address
   e. Block the connection
7. What is the purpose of the Cisco IOS command **ip ips name** *ipsname* **list** *ACL#*?
   a. It applies an ACL to all signatures in the IPS indicated, but the IPS must already exist.
   b. It applies an ACL to all signatures in the IPS indicated, and creates the IPS if it does not already exist.
   c. It applies an ACL to a subset of the signatures in the IPS indicated.
   d. It applies an ACL to the interface that the IPS indicated is configured on.
   e. It creates a new ACL for the IPS indicated, and enters ACL configuration mode.
8. Which command is used to display the number of active signatures?
   a. **show ip ips signatures**
   b. **show ip ips signatures active**
   c. **sh ip ips active signatures**
   d. **show ip ips configuration**
   e. **show ip ips configuration active**

9. When creating a new rule in SDM (via the Create IPS tab), what functions are possible (select all that apply)?
   a. Select the interface to which to apply the IPS rule
   b. Create an ACL for use with the IPS rules
   c. Select the traffic flow direction for IPS rule inspection
   d. Merge SDFs together
   e. Specify the location of the SDF
10. In the SDF Locations window, what is the purpose of checking the Use Built-In Signatures (as backup) checkbox?
   a. It adds the default signatures to the SDF.
   b. It causes the IPS to use only the default signatures.
   c. It causes the IPS to use the default signatures only when the selected SDF is unavailable.
   d. It causes the IPS to use the default signatures instead of those in the selected SDF.
   e. It changes the default signature file to be the selected SDF.

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **6 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **7 or 8 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

# Foundation Topics

## IDS and IPS Functions and Operations

There are two types of intrusion systems that are typically deployed in networks today: intrusion detection systems (IDS) and intrusion prevention systems (IPS). Each type of system consists of either hardware or software that first detects network anomalies. How a particular system responds to anomalies determines its true role.

An IDS device does not sit in the path of active network traffic. Instead, traffic is copied out to the IDS device for inspection. If the IDS device determines that a series of packets does not have the best of intentions, it sends an alert to a management station for further action. The IDS can also actively configure network devices (such as routers and firewalls) to block or quarantine the mischievous packet flows.

Remember that the IDS itself cannot block any packets, because it does not sit in the data path. So, if the IDS discovers an issue, the first few packets are already in the network. At best, the IDS can block further packets from getting into the network and reaching their target.

An IPS, on the other hand, sits directly in the path of network traffic. All packets must travel through the IPS device as they cross the segment that the IPS lives on. When the IPS detects some sort of anomaly, it can both alert a management station and block the questionable packets. Because all packets are flowing through the IPS, you do not need to configure other network devices to block the bad packets.

An IPS is useful for detecting viruses, worms, malicious applications, and vulnerability exploits, none of which should be permitted into the network at all. Because the IPS can immediately block packets deemed bad, it can shield the network from such exploits.

As a quick review:

- **Virus**—A virus is one type of malicious code that tries to propagate itself across a network. It is normally attached to other programs and executes a particular unwanted function on a user workstation when that program executes. A virus propagates itself by infecting other programs on the same computer. It can do serious damage, such as erasing files or erasing an entire disk. It can also be a simple annoyance, such as popping up a message. A virus cannot spread to a new computer without human assistance, such as opening an infected file in an e-mail attachment or through file sharing.

- **Worm**—A worm is another type of malicious code that executes arbitrary code and installs copies of itself in the memory of the infected computer. It can then spread to and infect other hosts from the infected computer. Like a virus, a worm is also a program that propagates itself. Unlike a virus, a worm can spread itself automatically over the network from one computer to the next. Worms simply take advantage of automatic file sending and receiving features found on many computers, or it uses its own e-mail code to send infected files to mail recipients.
- **Trojan horse**—A general term that refers to a program that appears desirable but actually contains something harmful; for example, a downloaded game that contains code to erase files. The malicious contents could also hold a virus or a worm.
- **Vulnerability exploit**—An attack that specifically targets a known device vulnerability.

The IDS and IPS can be used together to provide tighter network security. An IPS blocks traffic that it considers unsafe. If the traffic in question is legitimate, however, then the IPS could be doing more harm than good. Such traffic is commonly called "gray area" traffic. Instead of forcing the IPS to make a yes or no decision on it, gray area traffic can be sent off to the IDS for further inspection and analysis.

## Categories of IDS and IPS

There are two ways to categorize IDS and IPS systems. The first category is the scope of the system. The two IDS and IPS scopes are

- Network
- Host

An IDS or IPS can sit in the network (as a hardware appliance or a software module in an existing network device) and thus provide protection to the entire network or segments of the network. Such systems are called either network intrusion detection systems (NIDS) or network intrusion protection systems (NIPS). One appliance can monitor multiple hosts, and additional hosts can be added without increasing the number of NIDS or NIPS devices. A network-based system can monitor and detect buffer overflows, network reconnaissance, and denial of service (DoS) attacks. The ability to see attacks against the network offers the opportunity to determine the extent of the attack.

As a reminder, consider the following attacks:

- **Denial of Service (DoS)**—Where one device overloads the network access to or CPU utilization of a target system
- **Distributed Denial of Service (DDoS)**—Where multiple devices overload the network access to or CPU utilization of a target system

- **Recon**—An attempt to gather important network information from a device, such as accounts, passwords, host names, other IP addresses in use, and operating systems (to name a few)

Network-based systems can only detect and prevent intrusive activity. If a single packet does sneak through, the network-based system cannot assess the success or failure of the attack. Also, network-based systems cannot inspect encrypted traffic. As networks continue to grow, the need for additional network sensors could become cost prohibitive.

The second scope category of an IDS or IPS is at the host level. Such systems are typically software modules that reside on a workstation or server and provide anomaly detection and prevention services for that single device. These systems are called either host intrusion detection systems (HIDS) or host intrusion prevention systems (HIPS). When encrypted traffic flows across a network, only the HIPS or HIDS can see the plaintext contents of the packets. Virtually all implementations of host-based intrusion systems are HIPS versus HIDS. Cisco Security Agent is an example of a HIPS.

Another way to categorize IDS and IPS systems is the approach they take to identify malicious traffic. The three different identity approach mechanisms are as follows:

- **Signature-based**—Signature-based systems match for a specific byte pattern or content in a packet. Such pattern matching is typically combined with particular IP address, protocol, and/or port combinations to perform very precise matches. Attacks, such as Trojan horses, tend to change port numbers regularly, which can invalidate a pure signature-based system. Also, because signature patterns are preprogrammed into an IDS and IPS device, day-zero attacks (attacks that exploit a vulnerability in a new system patch) are difficult to defend against.

- **Policy-based**—Policy-based systems use algorithms to examine strings of packets to determine patterns and behavior. For example, such an approach might detect a ping sweep, whereas a signature-based system would see only individual ping packets. Additional restrictions, such as IP addresses, protocols, or ports, can be applied (as can be done with signature-based systems). Some policies, such as restricting the ability to browse certain websites, typically involve communication with some type of blacklist database to ensure up-to-date information.

- **Anomaly-based**—Anomaly-based systems look for behavior that deviates from the "norm." This implies that some definition of "normal" is dynamically learned by (statistical) or preprogrammed into (nonstatistical) the system before it can detect anything abnormal. Such systems tend to work well in small networks, where normal behavior can be easily defined. However, in larger networks, the definition of normal can easily be too expansive and complex to adequately define.

A honeypot is a common term heard in the threat prevention and protection environment. A honeypot is simply a sacrificial network device. Such a machine is left on the network to attract attackers, and thus pull the malicious packets away from important network resources. Packet flows captured on the honeypot device can be used to analyze the attack and construct an appropriate defense. Because the desire is to collect the devious packets, honeypots tend to be considered IDS instead of IPS. It is important to remember that any device that is used as a honeypot is not returned to the general network population, because the honeypot device is quite likely infected with all sorts of interesting malware.

## IDS and IPS Signatures

For the purpose of IDS and IPS, a signature is a pattern of data or traffic that should cause a reaction when it passes through the IDS or IPS. As described earlier in this chapter, this action can be either to send some type of alert or to actively block the offending traffic.

An IDS and IPS uses microengines to match signatures against packets and packet flows. In other words, each signature constitutes its own microengine. There are four categories of IDS and IPS signatures:

- **Exploit**—An exploit signature typically identifies malicious traffic by matching a traffic pattern. Usually, each exploit has a unique signature (either packet flows or packet contents). Thus, each attack requires a signature for detection. If the exploit is modified in any way, a new signature is needed to be able to match the modified attack.
- **Connection**—A connection signature is aware of valid network connections and protocols. The behavior of accepted connections and protocols is known in advance, and any actions that occur beyond the normal circumstances are considered suspect. Note that *normal* is also a subjective definition of acceptable network traffic and behavior.
- **String**—String signatures typically use regular expressions to match patterns. This is similar to how exploit signatures work, except a regular expression can be used to match many conditions, whereas an exploit signature usually matches a single exploit.
- **DoS**—DoS signatures examine behavior typical of a DoS attack. Because there are many forms and flavors of DoS attacks, there are a variety of DoS signatures used. As with exploit signatures, a behavioral change in a DoS attack would require an update to the DoS signature engine.

A Cisco IOS router can act as an inline NIPS device. By default, there are 100 signatures embedded in Cisco IOS Software (132 total with all of the subsignatures). Additional signature definition files (SDFs) can be downloaded from Cisco.com. Individual signatures within an SDF can be enabled and disabled.

## Signature Reaction

Once a signature is matched, the IDS and IPS device reacts immediately. On a Cisco IDS and IPS device, alert messages can be sent with either syslog or the Security Device Event Exchange (SDEE) protocol. SDEE is considered more secure than syslog. IDS and IPS signature reactions include the following:

- **Send an alarm to a syslog or centralized management server**—Normally, an alarm notification is not the only action.
- **Drop the packet**—This action should not affect a legitimate user if the source IP address is spoofed, as is often the case in DoS attacks.
- **Reset the connection**—This action works only on connection-oriented protocols, such as TCP. This action has no effect on UDP packet flows.
- **Block network traffic from the source IP address for a specified amount of time**—This effectively imposes a penalty on the attacking traffic, and permits time for attack analysis to occur. Blocking traffic should be done only if IP addresses are spoofed; otherwise, legitimate traffic is likely affected.
- **Block network traffic on the connection for a specified amount of time**—This introduces a penalty on the attacking traffic. Connection-oriented attacks typically do not employ IP spoofing, due to the two-way communications needed for such traffic. But if the ability to establish a connection is blocked, the attacker still could use other attack methods, or combinations of attacks.

For fully functional real-time monitoring of IDS and IPS events, the Cisco Security Monitoring, Analysis and Response System (CS-MARS) can be used. CiscoWorks Monitoring Center for Security, which is a component of CiscoWorks VPN/Security Management Solution (VMS), can also be used to collect logs and alert messages.

## Cisco IOS IPS Configuration

Only a few steps and Cisco IOS IPS configuration commands are needed to establish a basic Cisco IOS NIPS setup:

**Step 1** **Specify the location of the SDF**—Various SDFs can exist in the Cisco IOS device, but only one can be referenced.

**Step 2** **Configure the failure parameter**—This tells the Cisco IOS device what to do if the signature microengine (SME) is not available to scan the traffic.

**Step 3** **Create an IPS rule**—This creates a name that is later applied to an interface. The rule uses the SDF previously defined. Optionally, an access control list (ACL) can be applied to restrict which traffic is scanned.

**Step 4** **Apply the IPS rule to an interface**—Once the rule has been created, it must be applied to an interface to become operational.

Example 23-1 shows a sample Cisco IOS configuration of the four basic IPS setup steps from the preceding list. Comments have been added in the sample output to describe the function of each command. Also, options of each command are shown where appropriate.

**Example 23-1** *Cisco IOS IPS Configuration Commands*

```
! step 1 – define the location of the SDF
Router(config)#ip ips sdf ?
  builtin   Use the built in signature definition file
  location  Location of the signature definition file
Router(config)#ip ips sdf builtin
! step 2 – define the behavior if an SME fails
Router(config)#ip ips fail ?
  closed  Do not forward traffic of the failed module.
Router(config)#ip ips fail closed
! step 3 – create an IPS rule, and optionally apply an ACL
Router(config)#ip ips name ?
  WORD  Name of IPS rule
Router(config)#ip ips name testips ?
  list  Specify an access list to match
  <cr>
Router(config)#ip ips name testips list 123
! step 4 – apply the IPS rule to an interface
Router(config)#interface fastethernet 0/0
Router(config-if)#ip ips testips ?
  in   Inbound IPS
  out  Outbound IPS
Router(config-if)#ip ips testips in
Router(config-if)#
```

The **ip ips sdf builtin** command does not appear in the configuration file because this is a default command. This command appears only if a nondefault SDF is used.

The **ip ips fail closed** command instructs the IPS to drop packets if an SME is not available to scan traffic. Use the **no ip ips fail closed** command to forward all traffic that is not scanned.

The **ip ips name testips list 123** command creates an IPS rule called **testips** and applies extended ACL 123 for further scrutiny of scanned packets. The ACL is not shown. A standard access list can also be used if granular packet selection is not desired.

The **ip ips testips in** command applies the IPS rule **testips** to the FastEthernet 0/0 interface. Although an IPS rule can be applied both inbound and outbound, it is best to apply the rules inbound. This ensures that packets are inspected before they enter the router.

Additional IPS configurations are also possible (and desired). Other IPS configuration parameters include the ability to do the following:

- Merge SDFs
- Disable, delete, and filter selected signatures within an SDF
- Change the default location of the SDF

Example 23-2 shows each of these additional configuration parameters. As with Example 23-1, comments and options are shown where applicable.

**Example 23-2** *Additional Cisco IOS IPS Configuration Commands*

```
! optional step 1 – merge SDFs
Router#copy flash:attack-drop.sdf ips-sdf
Router#copy ips-sdf flash:newsignatures.sdf
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip ips sdf location ?
  WORD  URL of the signature definition file
Router(config)#ip ips sdf location flash:newsignatures.sdf
! optional step 2 – disable, delete, and filter selected signatures
Router(config)#ip ips signature 1107 ?
  <0-65535>  Sub signature id
  delete     Delete the specified signature
  disable    Disable the specified signature
  list       Specify an access list to match
Router(config)#ip ips signature 5037 0 delete
%IPS Signature 5037:0 is marked for deletion
%IPS The signature will be deleted when signatures are reloaded or saved
Router(config)#ip ips signature 1107 0 disable
%IPS Signature 1107:0 is disabled
Router(config)#ip ips signature 6190 0 list 152
%IPS Signature 6190:0 will use acl 152
! optional step 3 – change the location of the SDF
Router(config)#ip ips name newips list 123
Router(config)#interface fastethernet 0/0
Router(config-if)#ip ips newips in
Router(config-if)#
```

The command **copy flash:attack-drop.sdf ips-sdf** merges the *attack-drop.sdf* file with the default SDF stored in memory. The **copy ips-sdf flash:newsignatures.sdf** command creates a new SDF

in flash that can be used when the router boots. Within configuration mode, the location of the SDF that is used by the router is modified with the command **ip ips sdf location flash:newsignatures.sdf**. This location must be changed before any modifications to the SDF can be performed.

The ability to disable, delete, and filter selected signatures is shown in optional step 2 configuration commands. Note that signature 1107 is disabled (but remains in the SDF), while signature 5037 is deleted from the SDF. Signature 6190 has its own ACL applied to it for specific packet scanning.

In optional step 3, a new IPS name is created and applied to the FastEthernet 0/0 interface. The original IPS name from Example 23-1 could be used, but the **ip ips name** command must be executed again to map the new SDF into the IPS. If the original IPS name is remapped, it does not need to be reapplied to the interface.

Once the IPS has been configured in the Cisco IOS device, you can use the **show ip ips configuration** command to examine the IPS configuration, as demonstrated in Example 23-3.

**Example 23-3** *Cisco IOS IPS Verification*

```
Router#show ip ips configuration
Configured SDF Locations: none
Builtin signatures are enabled and loaded
Last successful SDF load time: 01:51:57 UTC Sep 22 2006
IDS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through Net Director is disabled
Event notification through SDEE is enabled
Total Active Signatures: 132
Total Inactive Signatures: 0
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
          :Curr Event Buf Size:0  Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
 IPS name testips
    acl list 123
Interface Configuration
 Interface FastEthernet0/0
  Inbound IPS rule is testips
    acl list 123
  Outgoing IPS rule is not set
Router#
```

Example 23-3 shows the IPS configuration on the Cisco IOS device using the initial configuration (Example 23-1). At the top of the output, only the built-in signatures are used, and the location is not set (in other words, the default location is used). There are a total of 132 active signatures, which are the 100 default signatures and 32 default subsignatures. And the IPS uses the name testips. Example 23-4 shows the IPS configuration after optional configurations have been applied.

**Example 23-4** *Cisco IOS IPS Verification*

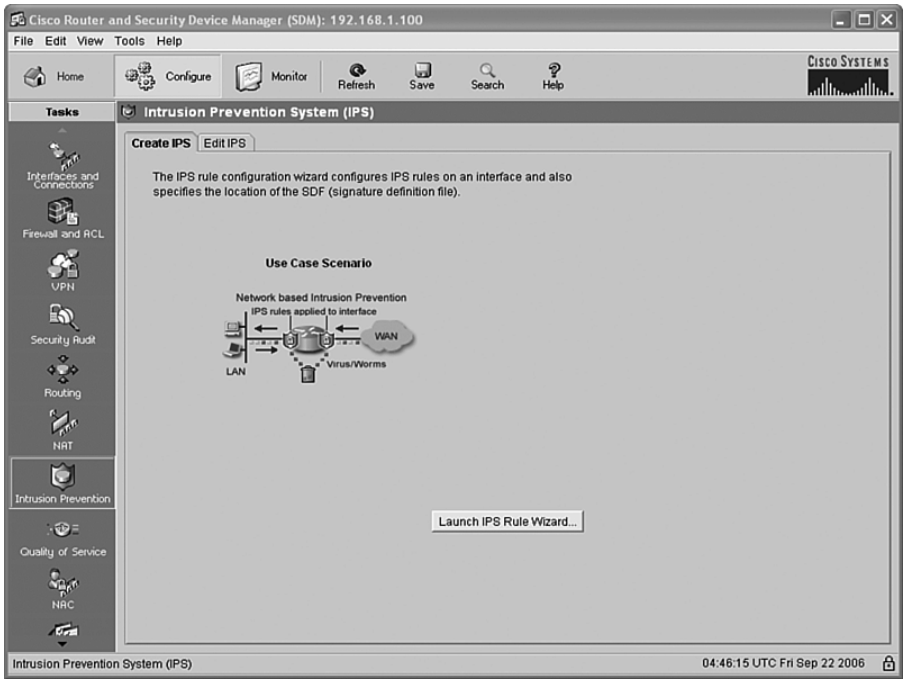
```
Router#show ip ips configuration
Configured SDF Locations:
 flash:newsignatures.sdf
Builtin signatures are enabled and loaded
Last successful SDF load time: 02:15:08 UTC Sep 22 2006
IDS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through Net Director is disabled
Event notification through SDEE is enabled
Total Active Signatures: 183
Total Inactive Signatures: 0
Signature 6190:0 list  152
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
          :Curr Event Buf Size:0  Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
 IPS name testips
    acl list 123
 IPS name newips
    acl list 123
Interface Configuration
 Interface FastEthernet0/0
  Inbound IPS rule is newips
    acl list 123
  Outgoing IPS rule is not set
Router#
```

In Example 23-4, the SDF location uses the new signature file created in Example 23-2 (*newsignatures.sdf*). The number of active signatures has increased to 183, and the signatures that were modified (1107 and 6190) are shown. At the bottom of the output, the new IPS name is created and applied to FastEthernet 0/0.

## SDM Configuration

As has been shown throughout this book, SDM is a powerful web-based tool that permits point-and-click configuration of virtually any Cisco IOS feature. Among its many wizards, SDM provides a useful set of wizards to configure IPS options. To access the IPS configuration wizards in SDM, click the **Configure** button at the top of the window, and then click the **Intrusion Prevention** button in the Tasks bar on the left side of the window. Figure 23-1 shows this initial entry point into IPS configuration within SDM.

**Figure 23-1** *SDM IPS Wizard*




As shown in Figure 23-1, there are two tabs at the top of this window:

- **Create IPS**—Offers the opportunity to launch the IPS Rule Wizard, which permits you to create new IPS rules.
- **Edit IPS**—Grants access to all existing IPS policies, signatures, and interface configurations. This tab is explored later in this section.

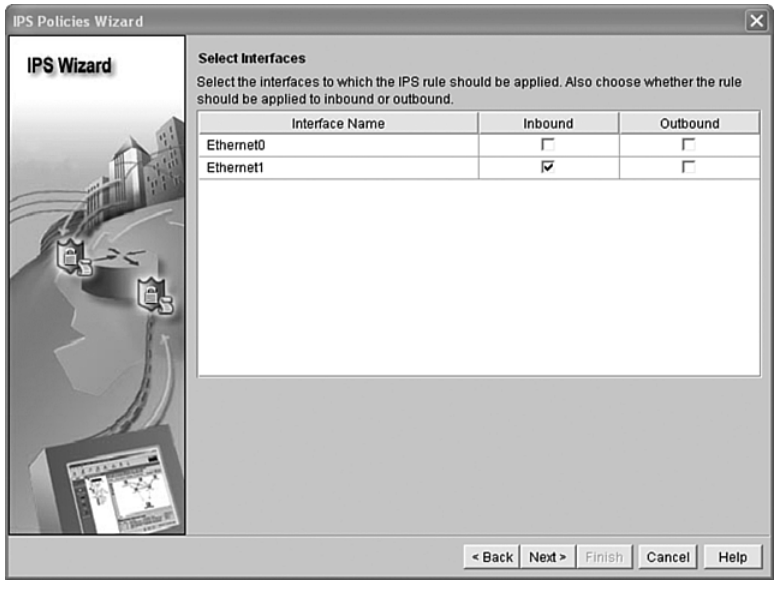
To create a new IPS rule, click the **Launch IPS Rule Wizard** button on the Create IPS tab. The wizard starts with a welcome window, which reminds you that the purpose of the wizard is to help you do the following:

- Select the interface to apply the IPS rule to
- Select the traffic flow direction that should be inspected by the IPS rules
- Specify the location of the SDF to be used by the router

Click **Next** at the bottom of the window to continue into the wizard.

The first configuration window in the IPS Wizard is the Select Interfaces window, as shown in Figure 23-2. All interfaces that are not currently configured for IPS operations are displayed. If this is your first IPS configuration in this Cisco IOS device, all interfaces should be displayed.

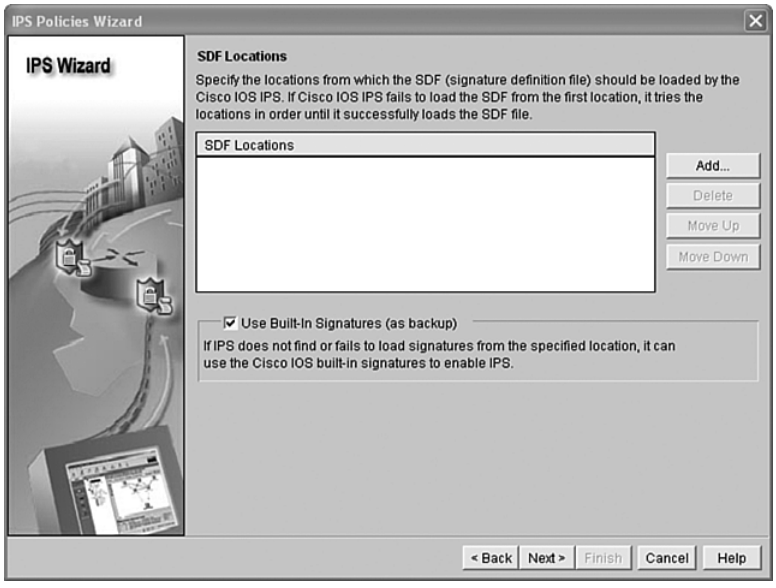
**Figure 23-2** *SDM IPS Wizard Select Interfaces Window*




Although both Inbound and Outbound options exist for each interface, it is best to check only the Inbound check box when IPS rules are applied. This triggers the IPS as packets arrive and does not give them access to the router before first being inspected. Notice that the interfaces are listed only by their name and not by their function or role. You must be aware of which interface is attached to which segment (for example, inside or outside) before you continue with this wizard. In Figure 23-2, interface Ethernet1 is selected for IPS operations. Click **Next** to continue.

Next, you must select the SDF location from the wizard. Figure 23-3 shows the SDF Locations window with only the default signature selected.

**Figure 23-3** *SDM IPS Wizard SDF Locations Window*




If you want to add signatures (another SDF) to the default SDF, click the **Add** button on the right side of the window. The Add a Signature Location dialog box appears, as shown in Figure 23-4. Click the **Specify SDF onflash** radio button, and click the drop-down arrow to view SDFs in flash.

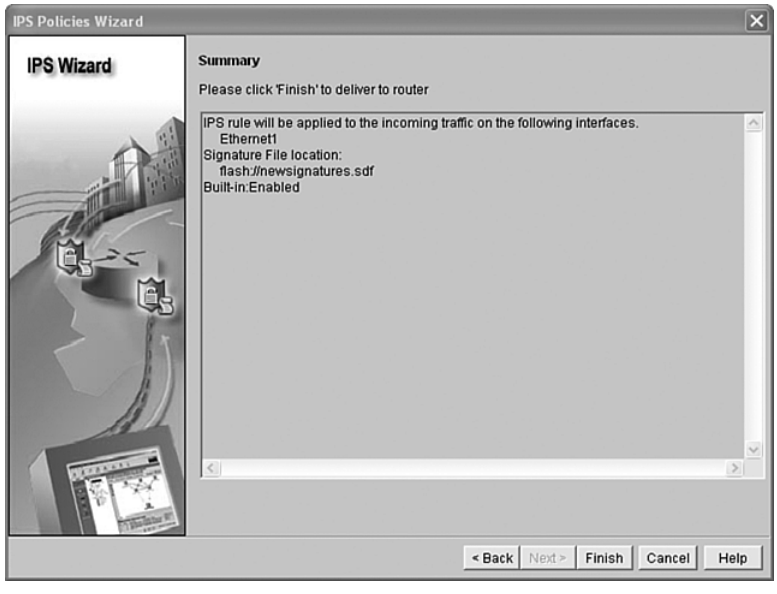
**Figure 23-4** *SDM IPS Wizard Add a Signature Location Dialog Box*

In Figure 23-4, the *newsignatures.sdf* file is highlighted in the drop-down menu. Click the desired SDF in the drop-down menu to enter it in the File Name onflash field. Click **OK** to add the specified file to the SDF locations. It is possible to add multiple SDFs in the SDF Locations window. Simply click the **Add** button again and repeat the process.

In the middle of the SDF Locations window, shown previously in Figure 23-3, is a Use Built-In Signatures (as backup) checkbox, which should be checked. This option allows the IPS to use the default SDF if the specified SDFs are unavailable for any reason (accidentally erased from flash, for example). When the necessary additional files are listed in the SDF Locations window, click **Next>** to continue.

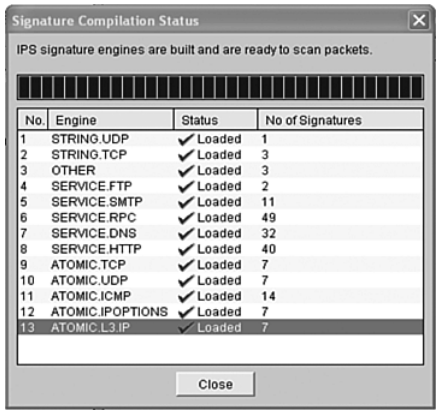
A Summary window appears that simply reminds you of your accomplishments over the last few windows. In Figure 23-2, you selected an interface, and in Figure 23-4, you added a new SDF. Figure 23-5 shows the results of these actions.

**Figure 23-5** *SDM IPS Wizard Summary Window*




Click **Finish** to complete the creation of a new SDF. SDM then pushes the configuration out to the router and compiles the new signatures into the Cisco IOS IPS. Figure 23-6 shows the results after the new signatures have been added to the Cisco IOS IPS.

**Figure 23-6** *SDM IPS Signature Compilation Status*




Click **Close** at the bottom of the Signature Compilation Status window. You are returned to the IPS Configuration window, but this time to the Edit IPS tab. The Edit IPS tab has the following four selection bars on the left of the tab, as shown in Figure 23-7:

- **IPS Policies**—Allows you to enable and/or disable the IPS on any interface in the router. You can also set the direction of the IPS (inbound is suggested). And, you can add an access list to the IPS interface configuration so that only certain packets are inspected.
- **Global Settings**—Shows a summary of current IPS settings, and allows you to add SDFs to and delete SDFs from the IPS.
- **SDEE Messages**—Shows the SDEE events.
- **Signatures**—Displays all signatures, by category, that are currently loaded. Individual signatures can be added, deleted, enabled, disabled, and edited (by applying an ACL to an individual signature).

From the Edit IPS tab, you can select each interface and modify the direction of the IPS (although inbound is suggested). The Edit button at the top of the tab allows you to apply an ACL to the IPS on the interface, and thus restrict which packets are actually inspected by the IPS. When there is no ACL applied, a warning message is displayed at the bottom of the window, as Figure 23-7 depicts.

Figure 23-8 shows the Signatures pane of the Edit IPS tab.

**Figure 23-7** *SDM IPS Policies*

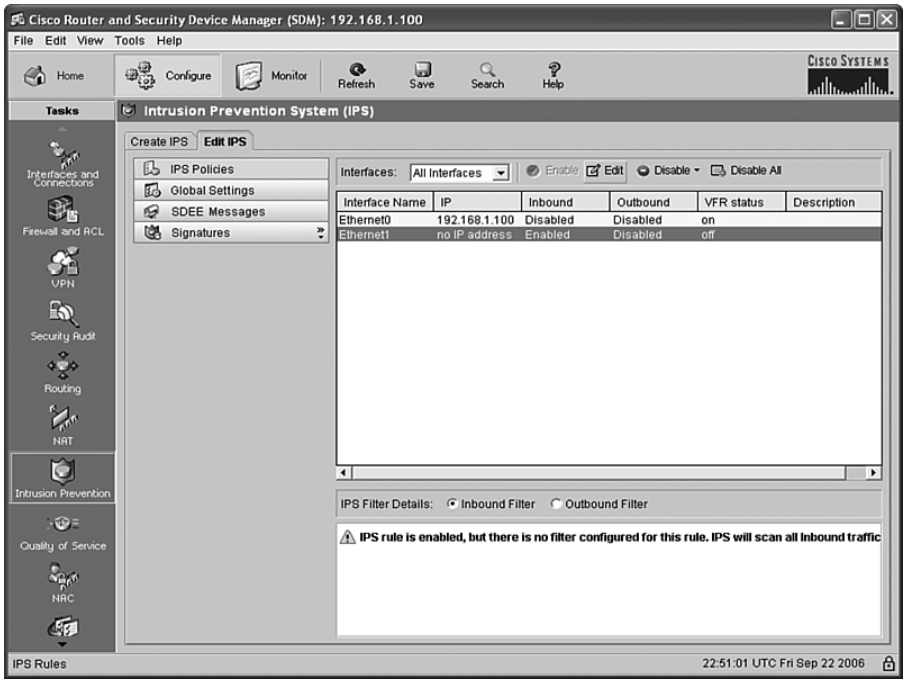
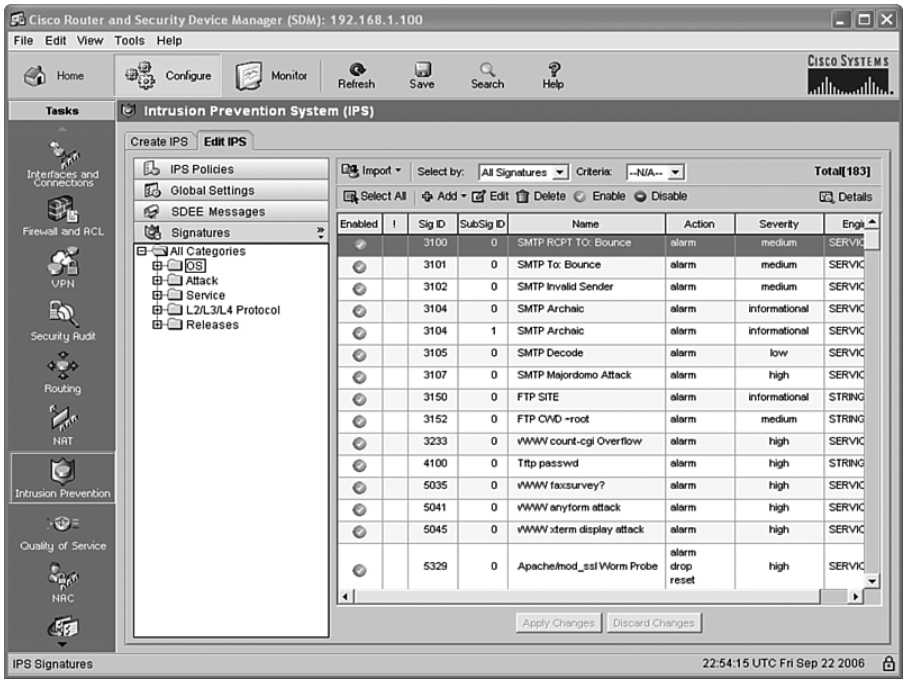



**Figure 23-8** *SDM IPS Signatures*



You can view signatures by category (for example, OS or Attack), or you can list all signatures together (All Categories). You can add, delete, enable, and disable individual signatures. Also, you can add an ACL to an individual signature by clicking the Edit button. This enables you to restrict the traffic that is actually scanned by the signature.

Note that once you complete the Create IPS tab (as described earlier), the IPS is operational. There is no need to *apply* the configuration to make it active. All operations performed from the Edit IPS tab are applied to the working configuration. Remember that in SDM, groups of configurations are created offline and applied to the router in batches. Typically, each time you click the OK button in a configuration window, the configuration is pushed out to the router.

# Foundation Summary

There are two types of intrusion systems:

- Intrusion Detection System, which is characterized by the following attributes:
  - Does not sit in the path of network traffic
  - Can send alerts when problems are detected
  - Cannot block packets itself
  - Can direct other network devices to block or quarantine mischievous packets
  - Can be used to inspect gray area traffic that the IPS avoids
- Intrusion Prevention System, which is characterized by the following attributes:
  - Sits in the path of network traffic
  - Can send alerts when problems are detected
  - Can block mischievous packets if needed
  - Is useful for detecting viruses, worms, malicious applications, and vulnerability exploits
  - Can send gray area traffic to the IDS for further inspection

There are two ways to categorize an IPS or IPS:

- Scope
- Approach to identify malicious traffic

There are two scopes for IDS and IPS:

- Network
- Host

NIDS and NIPS:

- Sits in the network as a hardware appliance or software module on an existing network device
- Provides protection to an entire network segment, and one appliance can monitor multiple hosts

- Can monitor and detect buffer overflows, network reconnaissance, and DoS attacks
- Cannot determine whether an attack is successful or not
- Cannot inspect encrypted traffic

HIDS and HIPS:

- Are typically software modules on host systems
- Can inspect encrypted traffic once it is decrypted on the host

There are three mechanisms to identify malicious traffic:

- Signature-based:
  - Match for specific byte patterns or content in packets
  - Combine such pattern matching with IP address, protocol, and port information to perform more precise matches
  - Are preprogrammed into IDS and IPS devices
  - Are not good at detecting day-zero attacks
- Policy-based:
  - Use algorithms to examine strings of packets to determine patterns and behavior
  - Can also restrict by IP address, protocol, and port numbers
  - Might require access to databases to ensure up-to-date information
- Anomaly-based:
  - Look for behavior that deviates from the "norm"
  - A definition of "normal" must first exist
  - Statistical = dynamically learned information
  - Nonstatistical = preprogrammed information
  - Tend to work better in smaller networks, where normal behavior is better defined and controlled

A honeypot is

- A sacrificial network device
- Used to attract attackers away from important network devices

- Captures packet flows for future attack analysis
- Tend to be IDS devices rather than IPS devices

There are four categories of IDS and IPS signatures:

- **Exploit**—An exploit signature typically identifies traffic by matching a traffic pattern. Each attack requires a different signature.
- **Connection**—A connection signature is aware of valid network connections and protocols. Abnormal behavior is considered suspect.
- **String**—String signatures typically use regular expressions to match many patterns.
- **DoS**—DoS signatures examine behavior that is typical of DoS attacks (of which there are many).

When a signature is matched, the IDS and IPS device can react by one or more of the following:

- Sending an alarm
- Dropping the packet
- Resetting the connection
- Blocking traffic from the source IP address
- Blocking traffic on the connection

Cisco IOS IPS configuration commands:

- **ip ips sdf builtin**—Uses the built-in SDF, but does not appear in the configuration file because it is a default command
- **ip ips sdf location** *name*—Uses the SDF *name*
- **ip ips fail closed**—Drops packets if an SME is not available to scan the traffic
- **ip ips name** *name* [**list** *num*]—Creates an IPS rule called *name* and optionally applies ACL *num* to it to refine packet selection
- **ip ips name in** | **out**—Applies the IPS to an interface in either the inbound or outbound direction
- **copy flash:***name1* **ips-sdf**—Merges the file *name1* in flash with the active SDF
- **copy ips-sdf flash:***name2*—Copies the new SDF back into flash so that it is available upon boot
- **show ip ips configuration**—Verifies the entire IPS configuration

SDM offers the IPS Wizard to create and edit IPS rules. The Create IPS tab allows you to

- Select the interface
- Select the traffic direction to inspect
- Specify the SDF

Screens within the Create IPS tab include

- **Select Interfaces window**—Lists all interfaces that are currently not enabled for IPS, and allows you to select inbound or outbound IPS direction.
- **SDF Locations window**—Shows all IPS SDFs. You can add additional SDFs or remove ones from the list displayed. This window also has the Use Built-In Signatures (as backup) check box, which, when checked, permits the default SDF to be used if the selected SDFs are unavailable.
- **Add a Signature Location dialog box**—Used to add another SDF to the IPS rule.
- **IPS Summary window**—Displays all the options configured from the IPS Wizard.

The Edit IPS tab offers access to

- **IPS Policies**—Allows you to edit an existing IPS configuration. You can enable/disable IPS on an interface, and you can add an ACL to IPS to be more selective when scanning packets.
- **Global Settings**—Shows a summary of IPS settings, and allows you to add/delete SDFs.
- **SDEE Messages**—Shows SDEE events.
- **Signatures**—Displays all signatures, and allows you to add, delete, enable, disable, and edit individual signatures.

# Q&A

The questions and scenarios in this book are designed to be challenging and to make sure that you know the answer. Rather than allowing you to derive the answers from clues hidden inside the questions themselves, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

You can find the answers to these questions in Appendix A. For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. What are the two types of intrusion systems deployed in networks today?
2. How does an IDS differ from an IPS?
3. What are the differences between network-based IDS and IPS and host-based IDS and IPS?
4. What are the three mechanisms to identify malicious traffic?
5. Of the identity mechanisms, which one may need access to a blacklist database for further information?
6. What are the four categories of IDS and IPS signatures?
7. What happens when a signature is matched?
8. Which IOS configuration command is used to apply a nondefault SDF?
9. In which direction should an IDS or IPS be applied?
10. What Cisco IOS command is used to display the number of active signatures?
11. What are the two tabs in the SDM IPS Wizard?