CHAPTER 6

Network Security Using Cisco IOS IPS

Intrusion detection system (IDS) and intrusion prevention system (IPS) solutions form an integral part of a robust network defense solution. Maintaining secure network services is a key requirement of a profitable IP-based business. Using Cisco products and technologies as examples, this chapter defines IDS and IPS and how these systems work.

Introducing IDS and IPS

IDS and IPS work together to provide a network security solution. An IDS captures packets in real time, processes them, and can respond to threats, but works on copies of data traffic to detect suspicious activity by using signatures. This is called *promiscuous mode*. In the process of detecting malicious traffic, an IDS allows some malicious traffic to pass before the IDS can respond to protect the network. An IDS analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating on a copy of the traffic is that the IDS does not affect the packet flow of the forwarded traffic. The disadvantage of operating on a copy of the traffic is that the IDS cannot stop malicious traffic from single-packet attacks from reaching the target system before the IDS can apply a response to stop the attack. An IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack.

An IPS works inline in the data stream to provide protection from malicious attacks in real time. This is called *inline mode*. Unlike an IDS, an IPS does not allow packets to enter the trusted side of the network. An IPS monitors traffic at Layer 3 and Layer 4 to ensure that their headers, states, and so on are those specified in the protocol suite. However, the IPS sensor analyzes at Layer 2 to Layer 7 the payload of the packets for more sophisticated embedded attacks that might include malicious data. This deeper analysis lets the IPS identify, stop, and block attacks that would normally pass through a traditional firewall device. When a packet comes in through an interface on an IPS, that packet is not sent to the outbound or trusted interface until the packet has been determined to be clean. An IPS builds upon previous IDS technology; Cisco IPS platforms use a blend of detection technologies, including profile-based intrusion detection, signature-based intrusion detection, and protocol analysis intrusion detection.

The key to differentiating an IDS from an IPS is that an IPS responds immediately and does not allow any malicious traffic to pass, whereas an IDS allows malicious traffic to pass before it can respond.

Key Topic

IDS:

- Analyzes copies of the traffic stream
- Does not slow network traffic
- Allows some malicious traffic into the network

IPS:

- Works inline in real time to monitor Layer 2 through Layer 7 traffic and content
- Needs to be able to handle network traffic
- Prevents malicious traffic from entering the network

IDS and IPS technologies share several characteristics:

- IDS and IPS technologies are deployed as sensors. An IDS or an IPS sensor can be any of the following devices:
  - A router configured with Cisco IOS IPS Software
  - An appliance specifically designed to provide dedicated IDS or IPS services
  - A network module installed in an adaptive security appliance, switch, or router
- IDS and IPS technologies typically monitor for malicious activities in two spots:
  - Malicious activity is monitored at the network to detect attacks against a network, including attacks against hosts and devices, using network IDS and network IPS.
  - Malicious activity is monitored on a host to detect attacks that are launched from or on target machines, using host intrusion prevention system (HIPS). Host-based attacks are detected by reading security event logs, checking for changes to critical system files, and checking system registries for malicious entries.
- IDS and IPS technologies generally use yes, signatures to detect patterns of misuse in network traffic, although other technologies will be introduced later in this chapter A signature is a set of rules that an IDS or IPS uses to detect typical intrusive activity. Signatures are usually chosen from a broad cross section of intrusion detection signatures, and can detect severe breaches of security, common network attacks, and information gathering.
- IDS and IPS technologies look for the following general patterns of misuse:
  - **Atomic pattern:** In an atomic pattern, an attempt is made to access a specific port on a specific host, and malicious content is contained in a single packet. An IDS is particularly vulnerable to an atomic attack because until it finds the attack, malicious single packets are being allowed into the network. An IPS prevents these packets from entering at all.
  - **Composite pattern:** A composite pattern is a sequence of operations distributed across multiple hosts over an arbitrary period of time.

Note: Note that sensors, even inline, might not be completely successful at drop packets of an attack. It is possible that an attack be on its way, if only partially, before even an inline sensor starts dropping packets matching a composite pattern signature. The drop action is much more effective for atomic signatures because the sensor makes a single packet match.

Figure 6-1 shows a sensor deployed in IDS mode and a sensor deployed in IPS mode.

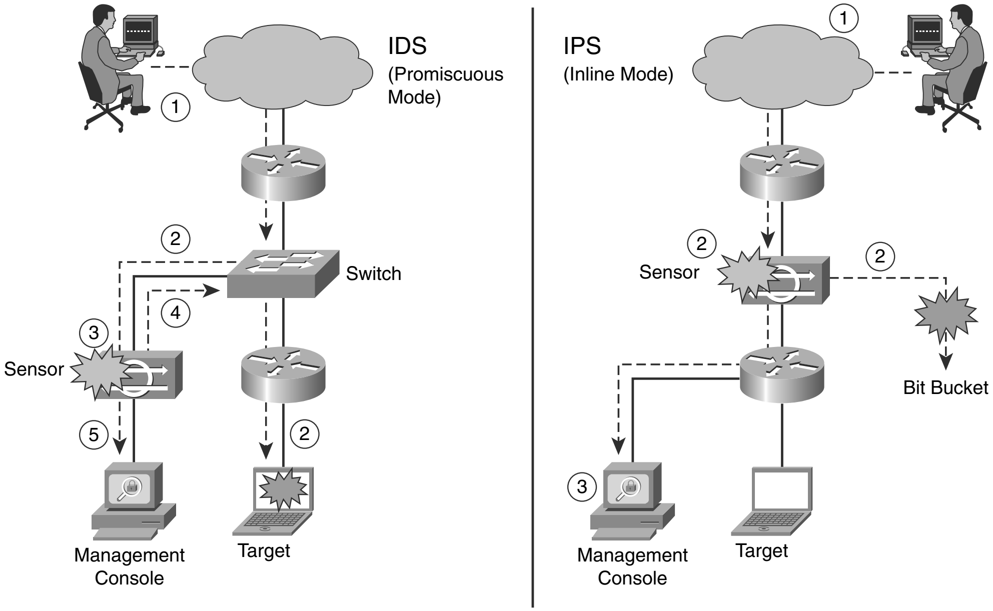


Figure 6-1 *IDS and IPS Operational Differences*

The following are the steps that occur when an attack is launched in an environment monitored by an IDS:

Step 1. An attack is launched on a network that has a sensor deployed in IDS mode.

Step 2. The switch sends copies of all packets to the IDS sensor (configured in promiscuous mode, which is explained later in this section) to analyze the packets. At the same time, the target machine experiences the malicious attack.

Step 3. The IDS sensor, using a signature, matches the malicious traffic to the signature.

Step 4. The IDS sensor sends the switch a command to deny access to the malicious traffic.

Step 5. The IDS sends an alarm to a management console for logging and other management purposes.

The following are the steps that occur when an attack is launched in an environment monitored by an IPS:

Step 1. An attack is launched on a network that has a sensor deployed in IPS mode (configured in inline mode, which is explained later in this section).

Step 2. The IPS sensor analyzes the packets as soon as they come into the IPS sensor interface. The IPS sensor, using signatures, matches the malicious traffic to the signature and the attack is stopped immediately. Traffic in violation of policy can be dropped by an IPS sensor.

Step 3. The IPS sensor can send an alarm to a management console for logging and other management purposes.

Key Topic

Promiscuous Versus Inline Mode

A sensor can be deployed either in promiscuous mode or inline mode. In promiscuous mode, the sensor receives a copy of the data for analysis, while the original traffic still makes its way to its ultimate destination. By contrast, a sensor working inline analyzes the traffic live and therefore can actively block the packets before they reach their destination.

It is worth mentioning that Cisco appliances, such as the Cisco ASA AIP SSM (discussed later in the section, “Cisco ASA AIP SSM”), although advertised as IPS device, can work either in promiscuous mode or in inline mode.

Key Topic

Management Console

The term *management console*, used in this chapter and seen in Figure 6-1, requires some explanation. A management console is a separate workstation equipped with software to configure, monitor, and report on events. The section, “Monitoring IOS IPS,” introduces some of Cisco’s IPS management solutions.

Table 6-1 lists some of the advantages and limitations of deploying an IDS platform in promiscuous mode.

Table 6-1 *Advantages and Limitations of Deploying an IDS in Promiscuous Mode*

Advantage	Limitation
Deploying the IDS sensor does not have any impact on the network (latency, jitter, and so on).	IDS sensor response actions cannot stop the trigger packet and are not guaranteed to stop a connection. IDS response actions are typically better at stopping an attacker more than a specific attack itself.
The IDS sensor is not inline and, therefore, a sensor failure cannot affect network functionality.	IDS sensor response actions are less helpful in stopping email viruses and automated attackers such as worms.

Table 6-1 *Advantages and Limitations of Deploying an IDS in Promiscuous Mode*

Advantage	Limitation
Overrunning the IDS sensor with data does not affect network traffic; however, it does affect the capability of the IDS to analyze the data.	Users deploying IDS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IDS deployments. Users must spend time to correctly tune IDS sensors to achieve expected levels of intrusion detection.
	Being out of band (OOB), IDS sensors are more vulnerable to network evasion techniques, which are the process of totally concealing an attack.

Table 6-2 lists some of the advantages and limitations of deploying an IPS platform in inline mode.

Table 6-2 *Advantages and Limitations of Deploying an IPS in Inline Mode*

Advantage	Limitation
You can configure an IPS sensor to perform a packet drop that can stop the trigger packet, the packets in a connection, or packets from a source IP address.	An IPS sensor must be inline and, therefore, IPS sensor errors or failure can have a negative effect on network traffic.
Being inline, an IPS sensor can use stream normalization techniques to reduce or eliminate many of the network evasion capabilities that exist.	Overrunning IPS sensor capabilities with too much traffic does negatively affect the performance of the network.
	Users deploying IPS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IPS deployments.
	An IPS sensor will affect network timing because of latency, jitter, and so on. An IPS sensor must be appropriately sized and implemented so that time-sensitive applications, such as VoIP, are not negatively affected.

Traffic normalization includes techniques such as fragmentation reassembly to check the validity of the transmission.

Note: Packets that are dropped based on false alarms can result in network disruption if the dropped packets are required for mission-critical applications downstream of the IPS sensor. Therefore, do not be overly aggressive when assigning the drop-action to signature. Also, "drop" discards the packet without sending a reset. Cisco recommends using "drop and reset" in conjunction with alarm.

Table 6-3 summarizes some of the advantages and limitations of an IDS in promiscuous mode and an IPS in inline mode explained earlier.

Table 6-3 *Summary of Advantages and Limitations of IDS and IPS Modes*

	Advantages	**Limitations**
IDS (Promiscuous Mode)	No impact on network (latency, jitter) No network impact if there is a sensor failure No network impact if there is sensor overload	Response action cannot stop trigger packets Correct tuning required for response actions Must have a well-thought out security policy More vulnerable to network evasion techniques
IPS (Inline Mode)	Stops trigger packets Can use stream normalization techniques	Sensor issues might affect network traffic Sensor overloading impacts the network Must have a well-thought out security policy Some impact on network (latency, jitter)

Types of IDS and IPS Systems

Table 6-4 summarizes the advantages and limitations of the various types of IDS and IPS sensors available.

Table 6-4 *Types of IDS and IPS Sensors*

	Advantages	**Limitations**
Signature Based	Easy configuration Fewer false positives Good signature design	No detection of unknown signatures Initially a lot of false positives Signatures must be created, updated, and tuned
Policy Based	Simple and reliable Customized policies Can detect unknown attacks	Generic output Policy must be created
Anomaly Based	Easy configuration Can detect unknown attacks	Difficult to profile typical activity in large networks Traffic profile must be constant
Honeypot Based	Window to view attacks Distract and confuse attackers Slow down and avert attacks Collect information about attack	Dedicated honeypot server Honeypot server must not be trusted

Key Topic

- **False negative:** Occurs when the IDS/IPS fails to report an actual intrusive action.
- **False positive:** Occurs when the IDS/IPS classifies an action as anomalous when in fact it is a legitimate action.

  These terms and others are discussed at length in the upcoming section “Signature Alarms.”
- **Honeypot:** A system deployed to entice a hacker to attack it and therefore track the hacker’s maneuvers and technique.

The sections that follow describe these IDS and IPS sensors in more detail.

Signature-Based IDS/IPS Systems

A signature-based IDS or IPS sensor looks for specific, predefined patterns (signatures) in network traffic. It compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match is found. The signature can be based on a single packet or a sequence of packets. New attacks that do not match a signature do not result in detection. For this reason, the signature database needs to be constantly updated.

Note: Protocol analysis-based intrusion detection relies on signature-based intrusion detection where the signature performs a check to ensure that the date unit header, flags, payload, and so on respect the protocol.

Signature-based pattern matching is an approach that is rigid but simple to employ. In most cases, the pattern is matched against only if the suspect packet is associated with a particular service or, more precisely, destined to and from a particular port. This matching technique helps to lessen the amount of inspection done on every packet. However, it makes it more difficult for systems to deal with protocols that do not reside on well-defined ports, such as Trojan horses and their associated traffic, which can move at will.

At the initial stage of incorporating signature-based IDS or IPS, before the signatures are tuned, there can be many false positives (traffic generating an alert which is no threat for the network). After the system is tuned and adjusted to the specific network parameters, there will be fewer false positives than with the policy-based approach.

Policy-Based IDS/IPS Systems

In policy-based systems, the IDS or IPS sensor is preconfigured based on the network security policy. You must create the policies used in a policy-based IDS or IPS. Any traffic detected outside the policy will generate an alarm or will be dropped. Creating a security policy requires detailed knowledge of the network traffic and is a time-consuming task.

Policy-based signatures use an algorithm to determine whether an alarm should be fired. Often, policy-based signature algorithms are statistical evaluations of the traffic flow. For example, in a policy-based signature used to detect a port sweep, the algorithm issues an alarm when the threshold number of unique ports is scanned on a particular machine. Policy-based signature algorithms can be designed to analyze only specific types of packets (for example, SYN packets, where the SYN bit is turned on during the handshaking process at the beginning of the session).

The policy itself might require tuning. For example, you might have to adjust the threshold level of certain types of traffic so that the policy conforms to the utilization patterns on the network that it is monitoring. Polices can be used to look for very complex relationships.

Anomaly-Based IDS/IPS Systems

Anomaly-based or profile-based signatures typically look for network traffic that deviates from what is seen "normally." The biggest issue with this methodology is that you first must define what *normal* is. If during the *learning phase* your network is the victim of an attack and you fail to identify it, the anomaly-based IPS systems will interpret that malicious traffic as normal, and no alarm will be triggered next time this same attack takes place. Some systems have hard-coded definitions of normal traffic patterns and, in this case, could be considered heuristic-based systems.

Other systems are built to learn normal traffic behavior; however, the challenge with these systems is eliminating the possibility of improperly classifying abnormal behavior as normal. Also, if the traffic pattern being learned is assumed normal, the system must contend with how to differentiate between allowable deviations, and those deviations that are not allowed or that represent attack-based traffic. Normal network traffic can be difficult to define.

The technique used by anomaly-based IDS/IPS systems is also referred as *network behavior analysis* or *heuristics analysis*.

Honeypot-Based IDS/IPS Systems

Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns. You can use this analysis to tune your sensor signatures to detect new types of malicious network traffic.

Honeypot systems are used in production environments, typically by large organizations that come across as interesting targets for hackers, such as financial enterprises, governmental agencies, and so on. Also, antivirus and other security vendors tend to use them for research.

Tip: Many security experts preach the use of honeypots as an early-warning system to be deployed with your IDS/IPS system, not in lieu of. *Honeyd* is an example of a popular open-source honeypot software. Although honeypots are often found as dedicated servers, it is possible to set up virtual honeypots using VMWare or Virtual PC. Keep in mind that should the honeypot be successfully hacked and used as a launching platform for an attack on a third party, the honeypot's owner could incur downstream liability.

IPS Actions

When an IPS sensor detects malicious activity, it can choose from any or all the following actions:

- **Deny attacker inline:** This action terminates the current packet and future packets from this attacker address for a specified period of time. The sensor maintains a list of the attackers currently being denied by the system. You can remove entries from the list or wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset, and attacker A remains on the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
- **Deny connection inline:** This action terminates the current packet and future packets on this TCP flow. This is also referred to as deny flow.
- **Deny packet inline:** This action terminates the packet.
- **Log attacker packets:** This action starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the

event store, which is local to the IOS router, even if the produce-alert action is not selected. Produce alert is discussed later in a bullet.

- **Log pair packets:** This action starts IP logging on packets that contain the attacker and victim address pair. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.
- **Log victim packets:** This action starts IP logging on packets that contain the victim address and sends an alert. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.
- **Produce alert:** This action writes the event to the event store as an alert.
- **Produce verbose alert:** This action includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.
- **Request block connection:** This action sends a request to a blocking device to block this connection.
- **Request block host:** This action sends a request to a blocking device to block this attacker host.
- **Request SNMP trap:** This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. This action causes an alert to be written to the event store, even if produce-alert action is not selected.
- **Reset TCP connection:** This action sends TCP resets to hijack and terminate the TCP flow.

Note: IP logging and verbose alert traces use a common capture file writing code called libpcap. This is the same format used by the famous packet-capture tool Wireshark (formerly Ethereal); by Snort, a famous freeware IDS; by NMAP, a well-known fingerprinting tool; and by Kismet, a famous wireless sniffing tool.
You can use the reset TCP connection action in conjunction with deny-packet and deny-flow actions. However, deny-packet and deny-connection actions do not automatically cause TCP reset actions to occur.

Event Monitoring and Management

Event monitoring and management can be divided into the following two needs:

- The need for real-time event monitoring and management
- The need to perform analysis based on archived information (reporting)

These functions can be handled by a single server, or the functions can be placed on separate servers to scale the deployment. The number of sensors that should forward alarms to a single IPS management console is a function of the aggregate number of alarms per second that are generated by those sensors.

Reporting: Analysis based on archive information
Event monitoring: Real-time monitoring

Key Topic

Experience with customer networks has shown that the number of sensors reporting to a single IPS management console should be limited to 25 or fewer. These customers use a mixture of default signature profiles and tuned signatures. The number of alarms generated by each sensor is determined by how sensitively the sensor is tuned; the more sensitive the tuning, the fewer the alarms that are generated, and the larger the number of sensors that can report to a single IPS management console.

Note: Obviously with the evolution of technology, the limit of 25 sensors reporting to a single IPS management console is constantly being pushed. Check with your vendor for the latest information.

It is essential to tune out false positives to maximize the scalability of the network IPS deployment. Sensors that are expected to generate a large number of alarms, such as those sitting outside the corporate firewall, should log in to a separate IPS management console, because the number of false alarms raised dramatically increases the noise-to-signal ratio and makes it difficult to identify otherwise valid events.

- False positives happen when the IDS/IPS mistakenly takes legitimate traffic for an attack.
- False negatives happens when the IDS/IPS sensor misses an attack.

Key Topic

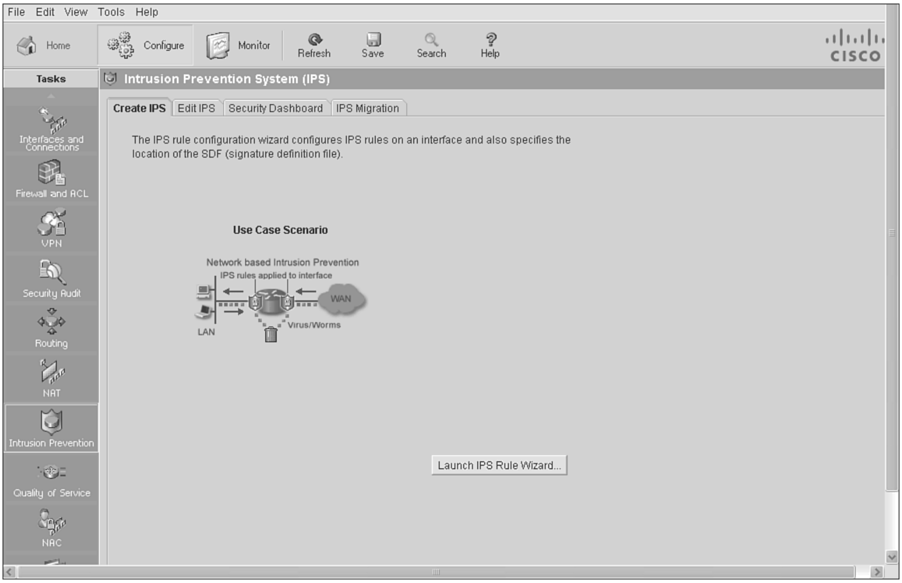
When implementing multiple IPS management consoles, implement either separate monitoring domains or a hierarchical monitoring structure.

Cisco IPS Management Software

You can use the command-line interface (CLI) to configure an IPS solution, but it is simpler to use a graphical user interface (GUI)-based device manager. The following describes the Cisco device management software available to help you manage an IPS solution.

Cisco Router and Security Device Manager

Cisco Security Device Manager (SDM), shown in Figure 6-2, is a web-based device management tool for Cisco routers that can improve the productivity of network managers, simplify router deployments, and help troubleshoot complex network and virtual private network (VPN) connectivity issues. Cisco SDM supports a wide range of Cisco IOS Software releases and is available free on Cisco router models from the Cisco 850 Series Integrated Services Router to the Cisco 7301 Router.



The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

Figure 6-2 *Cisco Router and Security Device Manager*

Cisco Security Monitoring, Analysis, and Response System

Cisco Security Monitoring, Analysis, and Response System (MARS), shown in Figure 6-3, is an appliance-based, all-inclusive solution that enables network and security administrators to monitor, identify, isolate, and counter security threats. This family of high-performance appliances enables organizations to more effectively use their network and security resources.

Figure 6-3 *Cisco Security Monitoring, Analysis, and Response System*

Cisco Security MARS can monitor security events and information from a wide variety of sources, including third-party devices and hosts. With its correlation engine, vector analysis, and hotspot identification, Cisco Security MARS can identify anomalous behavior and security threats, and recommend precision removal of those elements, which leads to rapid threat mitigation. In addition, Cisco Security MARS incorporates a comprehensive reporting engine that provides easy access to information for compliance reporting.

Cisco IDS Event Viewer

Cisco IDS Event Viewer (IEV), referred to also as Cisco IPS Event Viewer, is a Java-based application that enables you to view and manage alarms for up to five sensors. With Cisco IEV, you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms. You can also import and export event data for further analysis.

Cisco IEV offers a no-cost monitoring solution for small-scale IPS deployments. Monitoring up to five individual IPS devices, Cisco IEV is easy to set up and use, and provides the user with the following:

- Support for Cisco IPS Sensor Software Version 5.x through Security Device Event Exchange (SDEE) compatibility
- Customizable reporting
- Visibility into applied response actions and threat rating

Note: Cisco IEV is being phased out and replaced by Cisco IPS Express manager (http://tinyurl.com/5td7f2).

Cisco Security Manager

Cisco Security Manager is a powerful, but very easy-to-use solution, to centrally provision all aspects of device configurations and security policies for Cisco firewalls, VPNs, and IPS. The solution is effective for managing even small networks that consist of fewer than 10 devices, but also scales to efficiently manage large-scale networks that are composed of thousands of devices. Scalability is achieved through intelligent policy-based management techniques that can simplify administration.

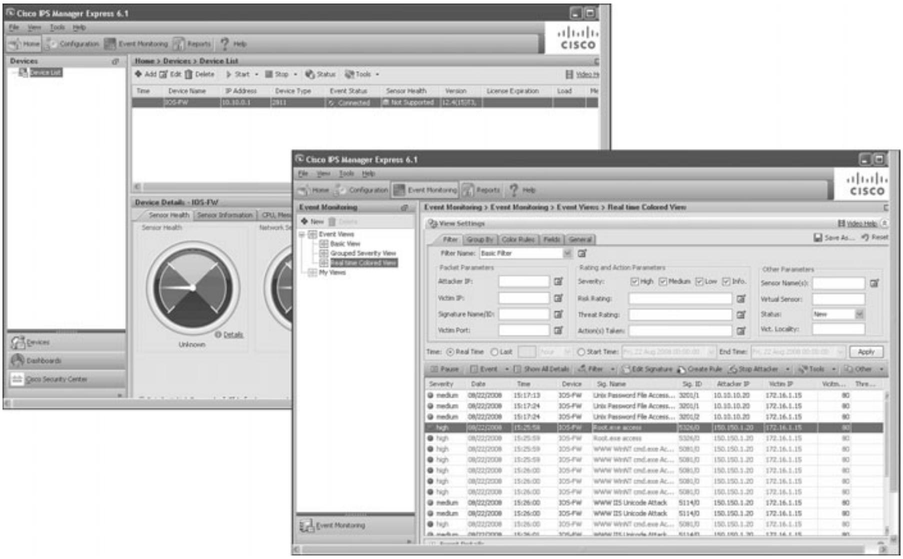
Features of CSM include the following:

- Auto update for Cisco IOS Release 12.4(11)T2 or later
- Custom signature templates
- Signature wizards to create and update signatures

Cisco IPS Device Manager

Cisco IPS Device Manager (IDM) is a web-based configuration tool for network IPS appliances. It is shipped at no additional cost with the Cisco IPS Sensor Software. Cisco IDM implements a web-based GUI.

Note: In May 2008, Cisco announced the release of a new product called Cisco IPS Manager Express. The new Cisco IPS Manager Express (IME), shown in Figure 6-4, is a powerful yet easy-to-use all-in-one IPS management application for up to five IPS sensors. Cisco IME can be used to provision, monitor, troubleshoot, and provide reports for IPS 4200 series sensors, ASA 5500 IPS solution, AIM-IPS on ISRs, and IDSM2 on Catalyst 6500s. To have access to all the capabilities of Cisco IME, it has to be used with sensors running Cisco IPS Software 6.1. With IPS Software Versions 5.1 or 6.0, or IOS IPS, you can use IME to monitor and provide reports only, with limited dashboard support.
Some of the features of Cisco IPS Manager Express are a customizable dashboard, powerful monitoring with real-time and historical viewing, integrated policy provisioning with risk rating, a flexible reporting tool, RSS feed integration, email notification, 75 events per second, and up to five IPS sensors.


Cisco IPS Manager Express 6.1
File View Tools Help
Home Configuration Event Monitoring Reports Help
Devices
Device List
Home > Devices > Device List
Add Edit Delete Start Stop Status Tools
Video Help
Device Details - IOS-FW
Sensor Health Sensor Information CPU, Memory
Unknown
Details
Devices
Dashboards
Cisco Security Center
Event Monitoring
New Delete
Event Views
Basic View
Grouped Severity View
Real time Colored View
My Views
Event Monitoring > Event Monitoring > Event Views > Real time Colored View
View Settings
Filter Group By Color Rules Fields General
Save As... Reset
Packet Parameters
Rating and Action Parameters
Other Parameters
Pause Event Show All Details Filter Edit Signature Create Rule Stop Attacker Tools Other
Apply

Time	Device Name	IP Address	Device Type	Event Status	Sensor Health	Version	License Expiration	Load
	IOS-FW	10.10.0.1	2811	Connected	Not Supported	12.4(15)T3,		

Filter Name: Basic Filter

Attacker IP:
Victim IP:
Signature Name/ID:
Victim Port:

Severity: ☑ High ☑ Medium ☑ Low ☑ Info.
Risk Rating:
Threat Rating:
Action(s) Taken:

Sensor Name(s):
Virtual Sensor:
Status: New
Vict. Locality:

Time: ● Real Time ○ Last Hour ○ Start Time: Fri, 22 Aug 2008 00:00:00 End Time: Fri, 22 Aug 2008 00:00:00

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Victim...	Thre...
medium	08/22/2008	15:17:13	IOS-FW	Unix Password File Access...	3201/1	10.10.10.20	172.16.1.15	80	
medium	08/22/2008	15:17:24	IOS-FW	Unix Password File Access...	3201/1	10.10.10.20	172.16.1.15	80	
medium	08/22/2008	15:17:24	IOS-FW	Unix Password File Access...	3201/2	10.10.10.20	172.16.1.15	80	
high	08/22/2008	15:25:58	IOS-FW	Root.exe access	5326/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:25:59	IOS-FW	Root.exe access	5326/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:25:59	IOS-FW	WWW WinNT cmd.exe Ac...	5081/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:25:59	IOS-FW	WWW WinNT cmd.exe Ac...	5081/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:26:00	IOS-FW	WWW WinNT cmd.exe Ac...	5081/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:26:00	IOS-FW	WWW WinNT cmd.exe Ac...	5081/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:26:00	IOS-FW	WWW WinNT cmd.exe Ac...	5081/0	150.150.1.20	172.16.1.15	80	
medium	08/22/2008	15:26:00	IOS-FW	WWW IIS Unicode Attack	5114/0	150.150.1.20	172.16.1.15	80	
medium	08/22/2008	15:26:00	IOS-FW	WWW IIS Unicode Attack	5114/0	150.150.1.20	172.16.1.15	80	
high	08/22/2008	15:26:00	IOS-FW	WWW WinNT cmd.exe Ac...	5081/0	150.150.1.20	172.16.1.15	80	
medium	08/22/2008	15:26:01	IOS-FW	WWW IIS Unicode Attack	5114/0	150.150.1.20	172.16.1.15	80	

Figure 6-4 *Cisco IPS Manager Express*

Host and Network IPS

IPS technology can be network based and host based. There are advantages and limitations to HIPS compared with network-based IPS. In many cases, the technologies are thought to be complementary.

Host-Based IPS

HIPS audits host log files, host file systems, and resources. A significant advantage of HIPS is that it can monitor operating system processes and protect critical system resources, including files that may exist only on that specific host. HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls, and application firewalls in one package. Note that the Cisco HIPS solution, Cisco Security Agent (CSA), is signature-free that reduces the maintenance required to be performed on that software.

A simple form of HIPS enables system logging and log analysis on the host. However, this approach can be extremely labor intensive. When implementing HIPS, the CSA software should be installed on each host to monitor all activity performed on, and against, the host. CSA performs the intrusion detection analysis and protects the host.

A Cisco HIPS deployment using CSA provides proactive security by controlling access to system resources. This approach avoids the race to update defenses to keep up with the latest exploit, and protects hosts even on day zero of a new attack. For example, the Nimda and SQL Slammer worms did millions of dollars of damage to enterprises on the first day of their appearance, before updates were even available; however, a network protected with a CSA stopped these attacks without any updates by identifying their behavior as malicious.

Host-based IPS operates by detecting attacks that occur on a host on which it is installed. HIPS works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.

More precisely, HIPS functions according to the following steps, as shown in Figure 6-5:

Step 1. An application calls for system resources.

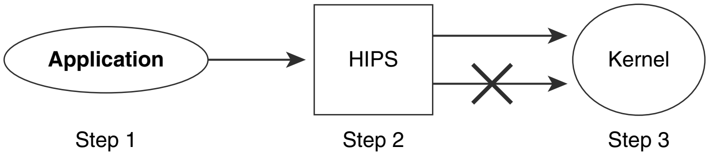


Figure 6-5 *HIPS Operations Steps*

Step 2. HIPS checks the call against the policy.

Step 3. Requests are allowed or denied.

HIPS uses rules that are based on a combination of known attack characteristics and a detailed knowledge of the operating system and specific applications running on the host. These rules enable HIPS to determine abnormal or out-of-bound activity and, therefore, prevent the host from executing commands that do not fit the correct behavior of the operating system or application.

HIPS improves the security of hosts and servers by using rules that control operating system and network stack behavior. Processor control limits activity such as buffer overflows, Registry updates, writes to the system directory, and the launching of installation programs. Regulation of network traffic can help ensure that the host does not participate in accepting or initiating FTP sessions, can rate-limit when a denial-of-service (DoS) attack is detected, or can keep the network stack from participating in a DoS attack.

The topology in Figure 6-6 shows a typical Cisco HIPS deployment. CSA is installed on publicly accessible servers, corporate mail servers, application servers, and on user desktops. CSA reports events to a central console server that is located inside the corporate firewall. CSA is managed from a central management console.

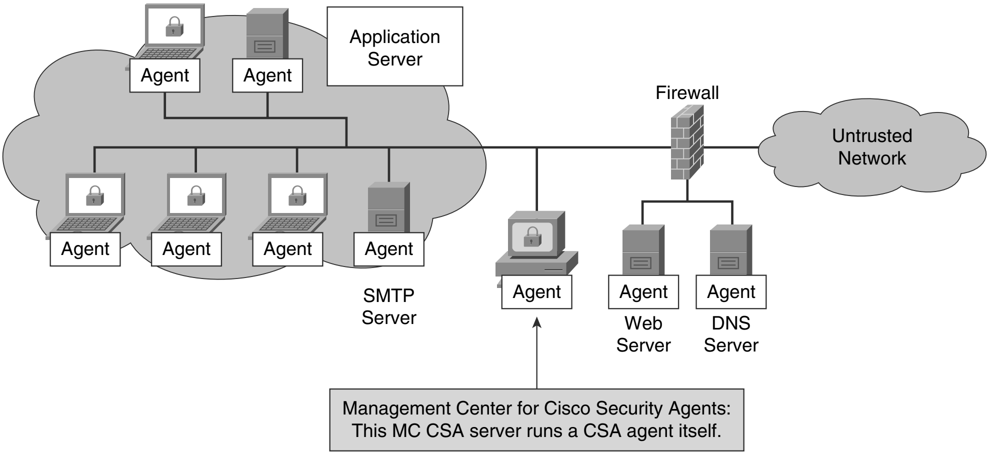


Figure 6-6 *HIPS deployment*

The advantages and limitations of HIPS are as follows:

- **Advantages of HIPS:** The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.

- **Limitations of HIPS:** There are two major drawbacks to HIPS:
  - **HIPS does not provide a complete network picture:** Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network.
  - **HIPS has a requirement to support multiple operating systems:** HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network.

Network-Based IPS

Network IPS involves the deployment of monitoring devices, or sensors, throughout the network to capture and analyze the traffic. Sensors detect malicious and unauthorized activity in real time and can take action when required. Sensors are deployed at designated network points that enable security managers to monitor network activity while it is occurring, regardless of the location of the attack target.

Network IPS sensors are usually tuned for intrusion prevention analysis. The underlying operating system of the platform on which the IPS software is mounted is stripped of unnecessary network services, and essential services are secured (that is, hardened). The hardware includes the following components:

- **Network interface card (NIC):** Network IPS must be able to connect to any network (Ethernet, Fast Ethernet, Gigabit Ethernet).

- **Processor:** Intrusion prevention requires CPU power to perform intrusion detection analysis and pattern matching.

- **Memory:** Intrusion detection analysis is memory intensive. Memory directly affects the capability of a network IPS to efficiently and accurately detect an attack.

Network IPS gives security managers real-time security insight into their networks regardless of network growth. Additional hosts can be added to protected networks without needing more sensors. When new networks are added, additional sensors are easy to deploy. Additional sensors are required only when their rated traffic capacity is exceeded, when their performance does not meet current needs, or when a revision in security policy or network design requires additional sensors to help enforce security boundaries.

Figure 6-7 shows a typical network IPS deployment. The key difference between this network IPS deployment example and the previous HIPS deployment example is that there is no CSA software on the various platforms. In this topology, the network IPS sensors are deployed at network entry points that protect critical network segments. The network segments have internal and external corporate resources. The sensors report to a central management and monitoring server that is located inside the corporate firewall.

The advantages and limitations of network IPS are as follows:

- **Advantages of network IPS:** A network-based monitoring system has the benefit of easily seeing attacks that are occurring across the entire network. Seeing the attacks against the entire network gives a clear indication of the extent to which the network is being attacked. Furthermore, because the monitoring system is examining

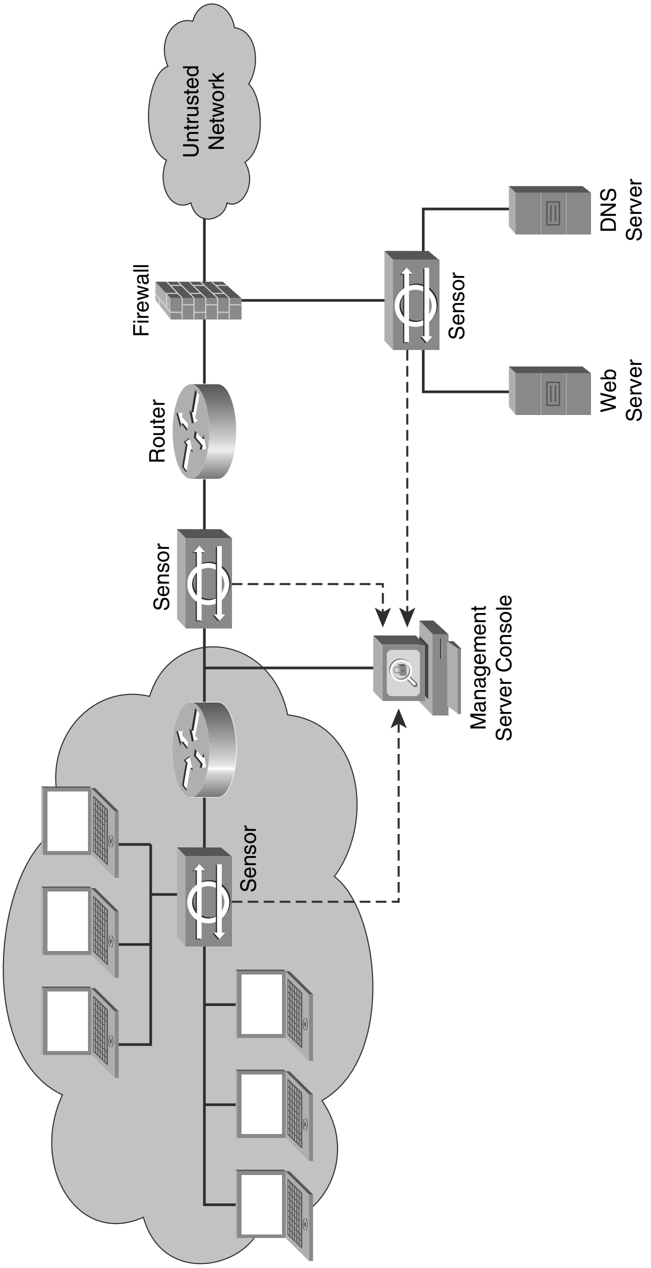


Figure 6-7 *Network-Based IPS Deployment*

only traffic from the network, it does not have to support every type of operating system that is used on the network.

- **Limitations of network IPS:** Encryption of the network traffic stream can essentially blind network IPS. Reconstructing fragmented traffic can also be a difficult problem to solve. Possibly the biggest drawback to network-based monitoring is that as networks become larger (with respect to bandwidth), it becomes more difficult to place network IPS at a single location in the network and successfully capture all the traffic. Eliminating this problem requires the use of more sensors throughout the network. However, this solution increases costs.

Caution: It is recommended that applications responsible for the management of security, such as syslog servers, IPS alarms, and so on be separated from the main corporate network by a firewall, in essence creating a network management network. Figure 6-8 shows the details of the Enterprise Campus architecture as envisioned by the Cisco SAFE Blueprint. For more information, visit http://www.cisco.com.

Comparing HIPS and Network IPS

Table 6-5 compares the advantages and limitations of HIPS and network IPS.

Table 6-5 *Advantages and Limitations of Host-Based IPS and Network-Based IPS*

	Advantages	**Limitations**
HIPS	Is host specific Protects host after decryption Provides application-level encryption protection	Operating system dependent Lower-level network events not seen Host is visible to attackers
Network IPS	Cost-effective Not visible on the network Operating system independent Lower-level network events seen	Cannot examine encrypted traffic Does not know whether an attack was successful

A host-based monitoring system examines information at the local host or operating system. Network-based monitoring systems examine packets that are traveling through the network for known signs of intrusive activity. As you move down the feature list toward network IPS, the features describe network-based monitoring features; application-level encryption protection is a HIPS feature, whereas DoS prevention is a network IPS feature.

Note: Network-based monitoring systems do not assess the success or failure of the actual attacks. They only indicate the presence of intrusive activity.
That is where Cisco MARS can be useful. Different sensors might report an intrusion; however, if all those sensors send their individual alarms to a Cisco MARS appliance, it could perform correlation analysis on those different alarms and discover that they are all part, let's say, of a common attack.

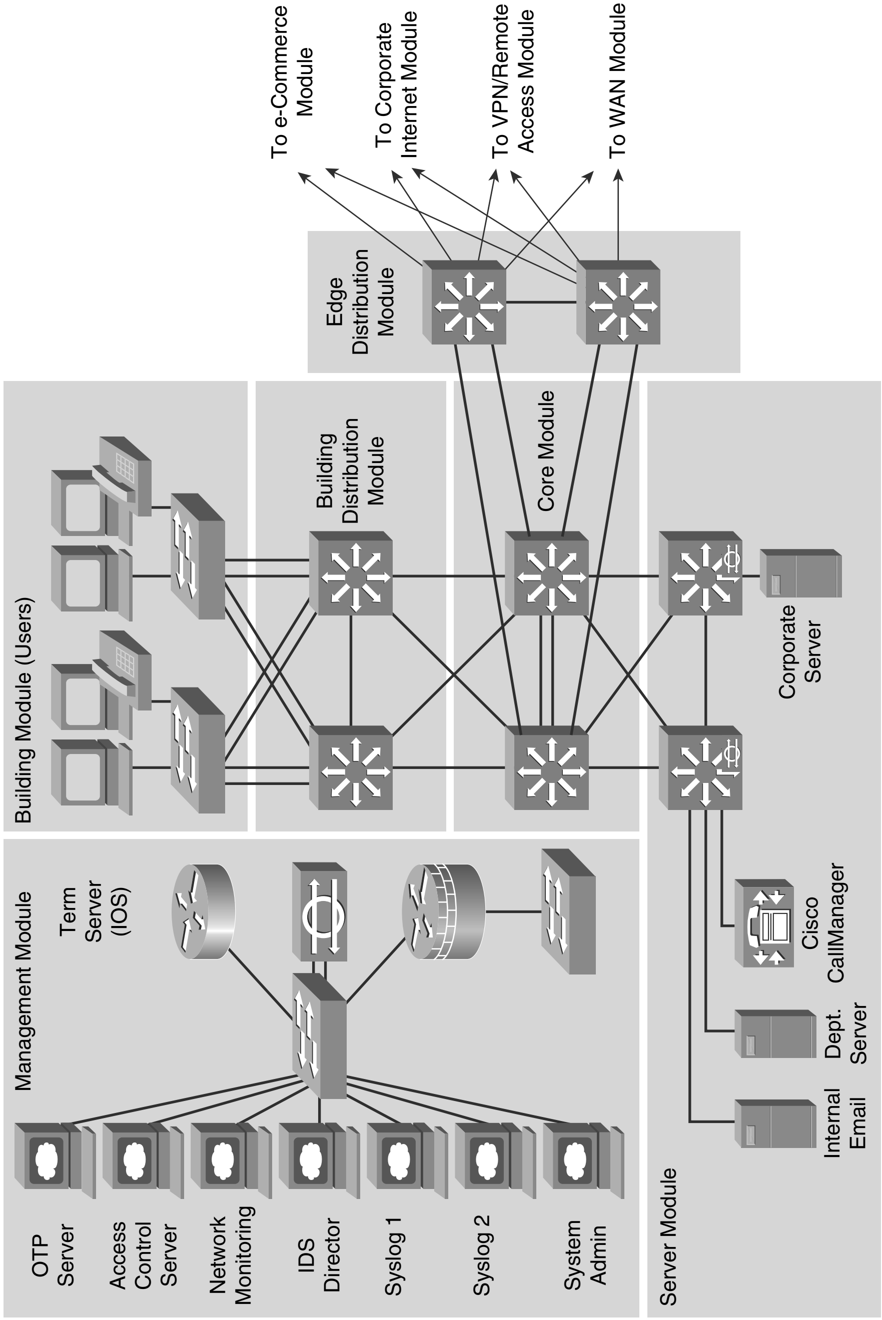


Figure 6-8 *Enterprise Campus Topology with Its Management Module*

Introducing Cisco IPS Appliances

Cisco IPS solutions run on a variety of devices, either as standalone sensors or as a module inserted into another appliance. The following is a brief description of the available Cisco IPS appliances. Each appliance is introduced further later in this section:

- **Cisco Adaptive Security Appliance Advanced Inspection and Prevention Security Services Module (ASA AIP SSM):** The Cisco ASA AIP SSM uses advanced inspection and prevention technology to provide high-performance security services, such as intrusion prevention services and advanced anti-x services, defined as antivirus and antispyware. The Cisco ASA AIP SSM products include a Cisco ASA AIP SSM-10 module with a 1-GB memory, a Cisco ASA SSM AIP-20 module with a 2-GB memory, and a Cisco ASA SSM AIP-40 module.
- **Cisco IPS 4200 series sensors:** Cisco IPS 4200 series sensors offer significant protection to your network by helping to detect, classify, and stop threats, including worms, spyware and adware, network viruses, and application abuse. Using Cisco IPS Sensor Software Version 5.1, the Cisco IPS solution combines inline intrusion prevention services with innovative technologies that improve accuracy. As a result, more threats can be stopped without the risk of dropping legitimate network traffic. Cisco IPS Sensor Software includes enhanced detection capabilities and improved scalability, resiliency, and so forth.
- **Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM-2):** The Catalyst 6500 Series IDSM-2 is part of the Cisco IPS solution. It works in combination with the other components to efficiently protect your data infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.
- **Cisco IPS Advanced Integration Module (AIM):** Cisco offers a variety of IPS solutions; the Cisco IPS AIM for the Cisco 1841 Integrated Services Router and the Cisco 2800 and 3800 Series Integrated Services Routers is made for small and medium-sized business (SMB) and branch-office environments. Cisco IPS Sensor Software running on the Cisco IPS AIM provides advanced, enterprise-class IPS functions and meets the ever-increasing security needs of branch offices. The Cisco IPS AIM can scale in performance to match branch office WAN bandwidth requirements today and in the future, because IPS functionality is run on its dedicated CPU, thus not hogging the router CPU. At the same time, the integration of IPS onto a Cisco Integrated Services Router keeps the solution cost low and effective for business of all sizes.

Cisco IPS 4200 Series Sensors

The Cisco IPS 4200 series sensors, shown in Figure 6-9, are market-leading dedicated appliances for intrusion detection and prevention, with the highest performance and lowest false alarm rates of the industry. The Cisco IPS 4200 series sensors are focused on protecting network devices, services, and applications. They are capable of detecting sophisticated attacks such as the following:

Figure 6-9 *Cisco IPS 4200 Series Sensors*

- Network attacks
- Application attacks
- DoS attacks
- Fragmented attacks
- Whisker (deprecated in favor of Nikto) attacks using IDS-evasive techniques

Cisco ASA AIP SSM

The Cisco ASA AIP SSM, shown in Figure 6-10, provides the intrusion detection and prevention security feature set for the Cisco 5500 series adaptive security appliances. It runs the same Cisco IPS Sensor Software Version 6.0 or later software image as the sensor appliances and, therefore, provides the same security features as the sensor appliance.

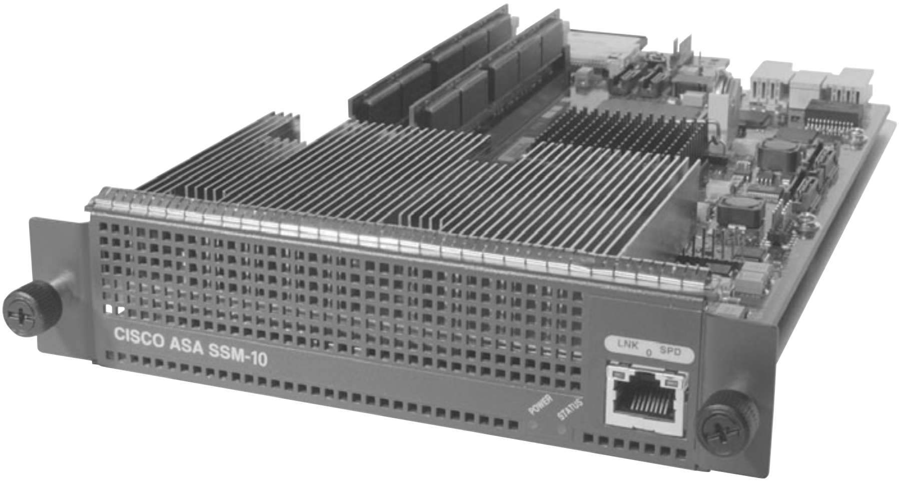


Figure 6-10 *Cisco ASA AIP SSM*

The Cisco ASA AIP SSM is available in three models:

- The Cisco ASA AIP SSM-10
- The Cisco ASA AIP SSM-20
- The ASA AIP SSM-40

The Cisco ASA AIP SSM-20 has a faster processor and more memory than the Cisco ASA AIP SSM-10. The Cisco ASA AIP SSM-40 works only in the Cisco ASA 5520 and 5540 and has a maximum throughput of 650 Mb/s.

Tip: Although Cisco markets the AIP SSM as "full-featured intrusion prevention services," it is worth noting that the sensor can operate as an IDS or IPS device. As shown in Figure 6-11, the AIP SSM can be configured in either IDS mode (promiscuous) or in IPS mode (inline).

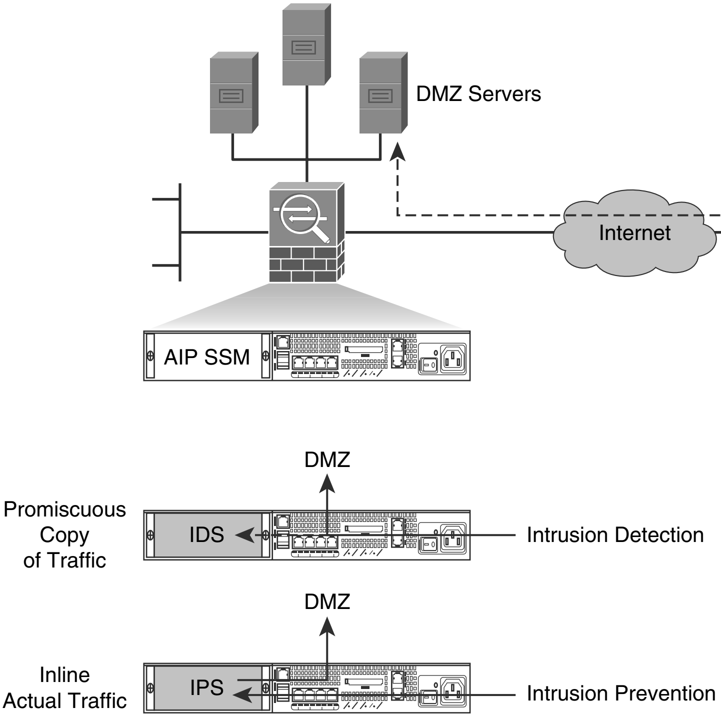


Figure 6-11 *Modes of Operation for Cisco ASA AIP SSM*

Cisco Catalyst 6500 Series IDSM-2

The Cisco Catalyst 6500 Series IDSM-2, shown in Figure 6-12, provides full-featured intrusion protection in the core network fabric device. The Cisco Catalyst 6500 Series IDSM-2 is specifically designed to address switched environments by integrating the IDS functionality directly into the switch. The Cisco Catalyst 6500 Series IDSM-2 runs the same software image as the sensor appliances and can be configured to perform intrusion prevention.

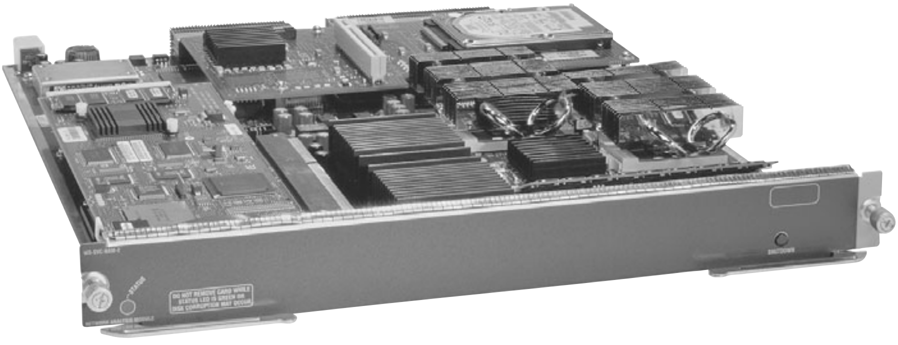


Figure 6-12 *Cisco Catalyst 6500 Series ISDM-2 Module*

Cisco IPS AIM

The Cisco IPS AIM for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers, shown in Figure 6-13, is an internal security service module that provides dedicated CPU and memory to offload inline and promiscuous intrusion prevention processing. The AIM runs the Cisco IPS Sensor Software Version 6.0 to provide feature parity with Cisco IPS 4200 series sensors and Cisco ASA 5500 series adaptive security appliances.

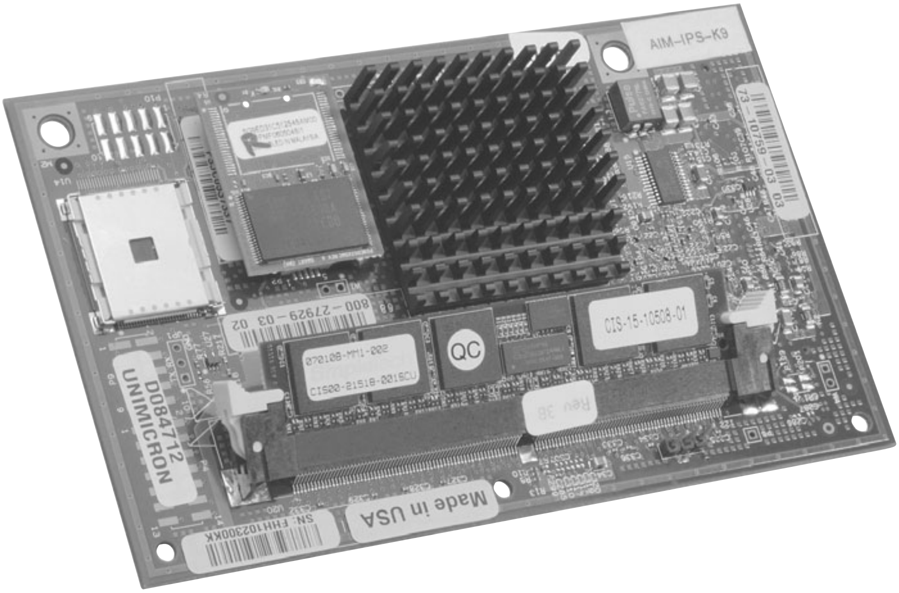


Figure 6-13 *Cisco IPS AIM*

By integrating IPS and branch-office routing, Cisco Integrated Services Routers can secure remote branch networks from threats originating from the Internet and reduce the WAN link overload from infected hosts at the branch. The integration of IPS into the branch-office router provides numerous important customer benefits:

- **Physical space savings:** The Cisco IPS AIM occupies the internal AIM slot on the router motherboard and can possibly saves space in the wiring closet.
- **Inline and promiscuous modes:** Both inline and promiscuous IPS inspection modes are supported. Inline mode places the IPS module in the packet path and can be configured to drop violated packets.
- **Common management tool for Cisco IPS solution:** Cisco Security Manager supports Cisco IPS AIM, with the same management tool used on Cisco IPS 4200 series sensors, enabling you to use one centralized management system for both appliance and router sensors.
- **Flexibility in monitoring interfaces:** The Cisco IPS AIM connects directly to the router backplane and can monitor packets coming in and going out of any router interface, including T1, T3, DSL, ATM, Fast Ethernet, and Gigabit Ethernet.
- **In-band management:** An internal Gigabit Ethernet port is used for in-band management of the Cisco IPS AIM CLI and for the web-based management application, Cisco IDM. Access to the IPS AIM can be done through the router console port or through the Secure Shell (SSH) protocol to any Layer 3 interface. No physical management port is required.
- **Simple power and cable management:** Cisco IPS AIM takes advantage of the power options of the router, including DC power and redundant power.
- **Dedicated processor to maximize performance:** Cisco IPS AIM has its own CPU and DRAM for all IPS functions. It offloads the router CPU from processor-intensive tasks, such as deep packet inspection from the host router.
- **Performance:** The Cisco IPS AIM can monitor up to 45 Mb/s of traffic and is suitable for T1, E1, and up to T3 environments.
- **Security in depth:** The Cisco IPS AIM interoperates with security and WAN optimization features such as VPN, firewall, Network Address Translation (NAT), Web Cache Control Protocol (WCCP), and Cisco Wide Area Application Services, and all common Cisco IOS Software functions.

Note: Cisco IOS IPS and the Cisco IPS AIM cannot be used together. Cisco IOS IPS must be disabled when the AIM IPS is installed. Cisco IOS IPS is discussed in the next section of this chapter.

Signatures and Signature Engines

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks. You can easily install signatures using IDS and IPS management software such as Cisco IDM. Sensors enable you to modify existing signatures and define new ones.

As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. A malicious packet flow has a specific type of activity and signature, and an IDS or IPS sensor examines the data flow using many different signatures. When an IDS or IPS sensor matches a signature with a data flow, the sensor takes action, such as logging the event or sending an alarm to IDS or IPS management software, such as the Cisco SDM.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous Internet Control Message Protocol (ICMP) messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your sensors. You can tune built-in signatures (tuned signatures) by adjusting the many signature parameters.

Examining Signature Micro-Engines

A signature micro-engine is a component of an IDS and IPS sensor that supports a group of signatures that are in a common category. Each engine is customized for the protocol and fields that it is designed to inspect and defines a set of legal parameters that have allowable ranges or sets of values. The signature micro-engines look for malicious activity in a specific protocol. Signatures can be defined for any of the supported signature micro-engines using the parameters offered by the supporting micro-engine. Packets are scanned by the micro-engines that understand the protocols contained in the packet.

Cisco signature micro-engines implement parallel scanning. All the signatures in a given signature micro-engine are scanned in parallel fashion, rather than serially. Each signature micro-engine extracts values from the packet and passes portions of the packet to the regular expression engine. The regular expression engine can search for multiple patterns at the same time (in parallel). Parallel scanning increases efficiency and results in higher throughput.

When IDS (promiscuous mode) or IPS (inline mode) is enabled, a signature micro-engine is loaded (or built) on to the router. When a signature micro-engine is built, the router may need to compile the regular expression found in a signature. Compiling a regular expression requires more memory than the final storage of the regular expression. Be sure to determine the final memory requirements of the finished signature before loading and merging signatures.

Note: A regular expression is a systematic way to specify a search for a pattern in a series of bytes.

As an example, a regular expression to be used to prevent data containing .exe or .com or .bat from crossing the firewall could look like this: **“.*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])”.**

Note: For the list of currently supported signature micro-engines, refer to the “Lists of Supported Signature Engines” section in the *Cisco IOS Security Guide, Release 12.4* available at http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a00804453cf.html. This information requires a Cisco.com login.

Table 6-6 summarizes the types of signature engines available in Cisco IOS Release 12.4(6)T. Table 6-7 provides more details on signature engines.

Table 6-6 *Summary of Supported Signature Engines*

Signature Engine	Description
Atomic	Signatures that examine simple packets, such as ICMP and UDP
Service	Signatures that examine the many services that are attacked
String	Signatures that use regular expression-based patterns to detect intrusions
Multi-string	Supports flexible pattern matching and supports Trend Labs signatures
Other	Internal engine to handle miscellaneous signatures

Table 6-7 *Details on Signature Micro-Engines*

Signature Micro-Engine	Description
ATOMIC.IP	Provides simple Layer 3 IP alarms
ATOMIC.ICMP	Provides simple ICMP alarms based on these parameters: type, code, sequence, and ID
ATOMIC.IPOPTIONS	Provides simple alarms based on the decoding of Layer 3 options
ATOMIC.UDP	Provides simple UDP packet alarms based on these parameters: port, direction, and data length
ATOMIC.TCP	Provides simple TCP packet alarms based on these parameters: port, destination, and flags
SERVICE.DNS	Analyzes the Domain Name System (DNS) service

Table 6-7 *Details on Signature Micro-Engines*

Signature Micro-Engine	Description
SERVICE.RPC	Analyzes the remote procedure call (RPC) service
SERVICE.SMTP	Inspects Simple Mail Transfer Protocol (SMTP)
SERVICE.HTTP	Provides HTTP protocol decode-based string engine; includes anti-evasive URL de-obfuscation
SERVICE.FTP	Provides FTP service special decode alarms
STRING.TCP	Offers TCP regular expression-based pattern inspection engine services
STRING.UDP	Offers UDP regular expression-based pattern inspection engine services
STRING.ICMP	Provides ICMP regular expression-based pattern inspection engine services
MULTI-STRING	Supports flexible pattern matching and supports Trend Labs signatures
Other	Provides internal engine to handle miscellaneous signatures

Note: It is recommended that you run Cisco IOS Release 12.4(11)T or later when using Cisco IOS IPS.

Note: Cisco IOS IPS and the Cisco IPS AIM cannot be used together. Cisco IOS IPS must be disabled when the AIM IPS is installed. Cisco IOS IPS is an IPS application that provides inspection capabilities for traffic flowing through the router. Although it is included in the Cisco IOS Advanced Security feature set, it uses the router CPU and shared memory pool to perform the inspection. Cisco IOS IPS also runs a subset of IPS signatures. The Cisco AIM IPS, discussed earlier in this chapter, runs with a dedicated CPU and memory, offloading all processing of IPS signatures from the router CPU. It can load a full signature set and provide enhanced IPS features not available on Cisco IOS IPS.

Signature Alarms

The capability of IDS and IPS sensors to accurately detect an attack or a policy violation and generate an alarm is critical to the functionality of the sensors. Attacks can generate the following types of alarms:

- **False positive:** A false positive is an alarm triggered by normal traffic or a benign action. Consider this scenario: A signature exists that generates alarms if the enable password of any network devices is entered incorrectly. A network administrator attempts to log in to a Cisco router but enters the wrong password. The IDS cannot distinguish between a rogue user and the network administrator, and it generates an alarm.

- **False negative:** A false negative occurs when a signature is not fired when offending traffic is detected. Offending traffic ranges from someone sending confidential documents outside of the corporate network to attacks against corporate web servers. False negatives are bugs in the IDS and IPS software and should be reported. A false negative should be considered a software bug only if the IDS and IPS have a signature that has been designed to detect the offending traffic.
- **True positive:** A true positive occurs when an IDS and IPS signature is correctly fired, and an alarm is generated, when offending traffic is detected. For example, consider a Unicode attack. Cisco IPS sensors have signatures that detect Unicode attacks against Microsoft Internet Information Services (IIS) web servers. If a Unicode attack is launched against Microsoft IIS web servers, the sensors detect the attack and generate an alarm.
- **True negative:** A true negative occurs when a signature is not fired when nonoffending traffic is captured and analyzed. In other words, the sensor does not fire an alarm when it captures and analyzes “normal” network traffic.

Table 6-8 provides a summary of the alarm types. To understand the terminology, think in terms of “Was the alarm triggered?” A positive means that the alarm was triggered and a negative means that the alarm was not triggered. Thus the expression *false alarm*, which is the same as *false positive* (positive because the alarm was triggered, but false because the intrusion did not happen or the intrusion was not detected by the sensor).

Table 6-8 *Alarm Types*

	Intrusion Occurred/Detected	Intrusion Did Not Occur / Not Detected
Alarm was triggered	True positive	False positive
Alarm was not triggered	False negative	True negative

Alarms fire when specific parameters are met. You must balance the number of incorrect alarms that you can tolerate with the capability of the signature to detect actual intrusions. If you have too few alarms, you might be letting in more suspect packets, but network traffic will flow more quickly. If IPS systems use untuned signatures, they will produce many false positive alarms. You should consider the following factors when implementing alarms that a signature uses:

- The level assigned to the signature determines the alarm severity level.
- A Cisco IPS signature is assigned one of four severity levels:

    - **Informational:** Activity that triggers the signature is not considered an immediate threat, but the information provided is useful information.
    - **Low:** Abnormal network activity is detected that could be perceived as malicious, but an immediate threat is not likely.
    - **Medium:** Abnormal network activity is detected that could be perceived as malicious, and an immediate threat is likely.
    - **High:** Attacks used to gain access or cause a DoS attack are detected, and an immediate threat is extremely likely.

- You can manually adjust the severity level that an alarm produces.

- To minimize false positives, study your existing network traffic patterns and then tune your signatures to recognize intrusion patterns that are atypical (out of character) for your network traffic patterns. Do not base your signature tuning on traffic patterns that are based only on industry examples. Use an industry example as a starting point, determine what your own network traffic patterns are, and use them in your signature alarm tuning efforts.

Retiring Signatures

Router memory and resource constraints might prevent a router from loading all Cisco IOS IPS signatures. Therefore, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a "top-down" order, you should first retire all signatures, followed by "unretiring" specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate. However, be aware that retiring and reinstating signatures are a CPU-intensive process. For more information about this topic, refer to http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ips_v5.html.

IPS Best Practices

You should follow some configuration best practices to improve IPS efficiency when deploying IPS in your network.

When setting up a large deployment of sensors, automatically update signature packs rather than manually upgrading every sensor. Then security operations personnel have more time to analyze events. When new signature packs are available, download the new signature packs to a secure server within the management network.

Place the signature packs on a dedicated FTP server within the management network. If a signature update is not available, a custom signature can be created to detect and mitigate a specific attack. You should configure the FTP server to allow read-only access to the files within the directory on which the signature packs are placed only from the account that the sensors will use. The sensors can then be configured to automatically check the FTP server periodically, such as once a week on a certain day, to look for the new signature packs and to update the sensors. You can use an IPS to protect this server from attack by an outside party.

You should stagger the time of day when the sensors check the FTP server for new signature packs, perhaps through a predetermined change window. This prevents multiple sensors from overwhelming the FTP server by asking for the same file at the same time. The need to upgrade sensors with the latest signature packs must be balanced against the momentary downtime—and, therefore, the vulnerability to attack—incurred while upgrading them. Finally, the signature levels supported on the management console must remain synchronized with the signature packs on the sensors themselves.

You should group IPS sensors together under a few larger profiles. Every signature upgrade requires that all new signatures be appropriately tuned on every sensor. Tuning signatures for groups of sensors rather than for each sensor on the network significantly reduces configuration time. This administrative advantage must be balanced against the ability to finely tune sensor configuration by establishing a separate profile for each sensor.

Refer to the release notes of signatures to confirm that the new update will not overwrite the tuning you might have performed on a signature.

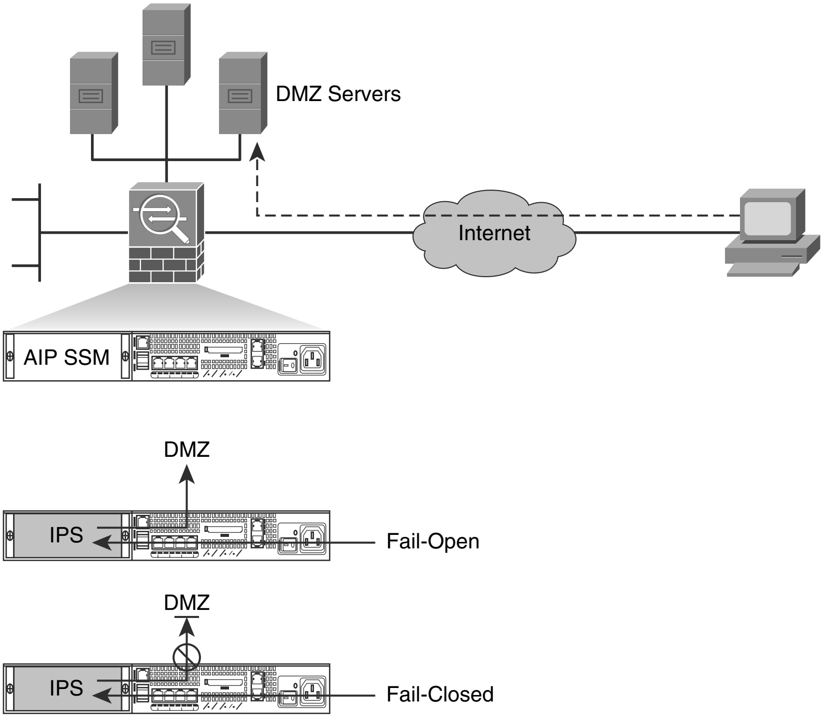


Figure 6-14 *Fail-Open or Fail-Close Approach*

A Great Debate: Fail-Close or Fail-Open?

This is a philosophical debate in which you need to get engaged in for your organization: Should the IPS sensor stop working, do you let the traffic go through or do you stop the traffic? The two opposing philosophies are represented in Figure 6-14, where the network administrator needs to decide whether the traffic will be allowed to flow into the demilitarized zone (DMZ) should the Cisco ASA AIP SSM fail.

It seems that the balance is tilting in favor of the "fail-open" approach with security experts, but each organization has to define and enforce their own policy in this topic.

Note: Readers interested in learning more about generic topics regarding IDS/IPS should consider visiting http://www.searchsecurity.com, more precisely the "Security School," which offers free training modules on different security topics.

Configuring Cisco IOS IPS

Configuring Cisco IOS Intrusion Prevention System (IPS) is a core competency for a network security administrator. In this section, you will learn how to configure Cisco IOS IPS on routers using the Cisco Router and Security Device Manager (SDM). You will also discover that Cisco SDM makes it easy to configure and manage Cisco IOS IPS on routers and security devices.

Cisco IOS IPS Features

Cisco has implemented IPS functions into its Cisco IOS Software. Cisco IOS IPS uses technology from Cisco Intrusion Detection System (IDS) and IPS sensor product lines, including Cisco IPS 4200 series sensors, and Cisco Catalyst 6500 series Intrusion Detection System Services Module (IDSM). Cisco IOS IPS combines existing Cisco IDS and IPS product features with the following three intrusion detection techniques:

- **Profile-based intrusion detection:** Profile-based intrusion detection generates an alarm when activity on the network goes outside a defined profile. With anomaly detection, profiles are created for each user or user group on your system. These profiles are then used as a baseline to define normal user and network activity. A profile could be created to monitor web traffic.

- **Signature-based intrusion detection:** Signature-based intrusion detection is less prone to triggering a false alarm when detecting unauthorized activity. A signature is a set of rules pertaining to typical intrusion activity. Signature-based intrusion detection uses signatures that are based on values in IP, TCP, UDP, and ICMP headers. Network engineers research known attacks and vulnerabilities and then develop signatures to detect these attacks and vulnerabilities on the network. These attack signatures encompass specific traffic or activity that is based on known intrusive activity.

  Cisco IOS IPS implements signatures that can look at every packet going through the network and generate alarms when necessary. A Cisco IOS IPS generates alarms when a specific pattern of traffic is matched or a signature is triggered. You can configure a Cisco IOS IPS to exclude signatures and modify signature parameters to work optimally in your network environment.

A pattern-matching approach searches for a fixed sequence of bytes in a single packet. Pattern matching is a rigid approach but is simple to employ. In most cases, the pattern is matched against a packet only if the suspect packet is associated with a particular service or, more precisely, destined to or from a particular port. For example, a signature might be based on a simple pattern-matching approach such as the following: If <the packet is IPv4 and TCP> and <the destination port is 2222> and <the payload contains the string "foo"> then <fire an alarm>.

- **Protocol analysis-based intrusion detection:** Protocol analysis-based intrusion detection is similar to signature-based intrusion detection, but it performs a more in-depth analysis of the protocols specified in the packets. A deeper analysis examines the payloads within TCP and UDP packets, which contain other protocols. For example, a protocol such as DNS is contained within TCP or UDP, which itself is contained within IP.

  The first step of protocol analysis is to decode the packet IP header information and determine whether the payload contains TCP, UDP, or another protocol. For example, if the payload is TCP, some of the TCP header information within the IP payload is processed before the TCP payload is accessed (for example, DNS data). Similar actions are mapped for other protocols.

  Protocol analysis requires that the IPS sensor knows how various protocols work so that it can more closely analyze the traffic of those protocols to look for suspicious or abnormal activity. For each protocol, the analysis is based not only on protocol standards, particularly the RFCs, but also on how things are implemented in the real world. Many implementations violate protocol standards. It is important that signatures reflect common and accepted practice rather than the RFC-specified ideal; otherwise, false results can be reported.

The following attributes describe the primary benefits of the Cisco IOS IPS solution:

- Cisco IOS IPS uses the underlying routing infrastructure to provide an additional layer of security with investment protection.
- Because Cisco IOS IPS is inline and is supported on a broad range of routing platforms, attacks can be effectively mitigated to deny malicious traffic from both inside and outside the network.
- When used in combination with Cisco IDS, Cisco IOS Firewall, virtual private network (VPN), and Network Admission Control (NAC) solutions, Cisco IOS IPS provides superior threat protection at all entry points to the network.
- Cisco IOS IPS is supported by easy and effective management tools, such as Cisco SDM, Cisco Security MARS, and Cisco Security Manager.
- Whether threats are targeted at endpoints, servers, or the network infrastructure, Cisco offers pervasive intrusion prevention solutions that are designed to integrate smoothly into the network infrastructure and to proactively protect vital resources.
- Cisco IOS IPS supports around 2000 attack signatures from the same signature database that is available for Cisco IPS appliances.

Table 6-9 describes the features of Cisco IOS IPS-based signatures.

Table 6-9 *Cisco IOS IPS Signature Features*

Cisco IOS IPS Signature Feature	Description
Regular expression string pattern matching	Enables the creation of string patterns using regular expressions.
Response actions	Enables the sensor to take an action when the signature is triggered.
Alarm summarization	Enables the sensor to aggregate alarms. It does this to limit the number of times an alarm is sent when the signature is triggered.
Threshold configuration	Enables a signature to be tuned to perform optimally in a network.
Anti-evasive techniques	Enables a signature to defeat evasive techniques used by an attacker.

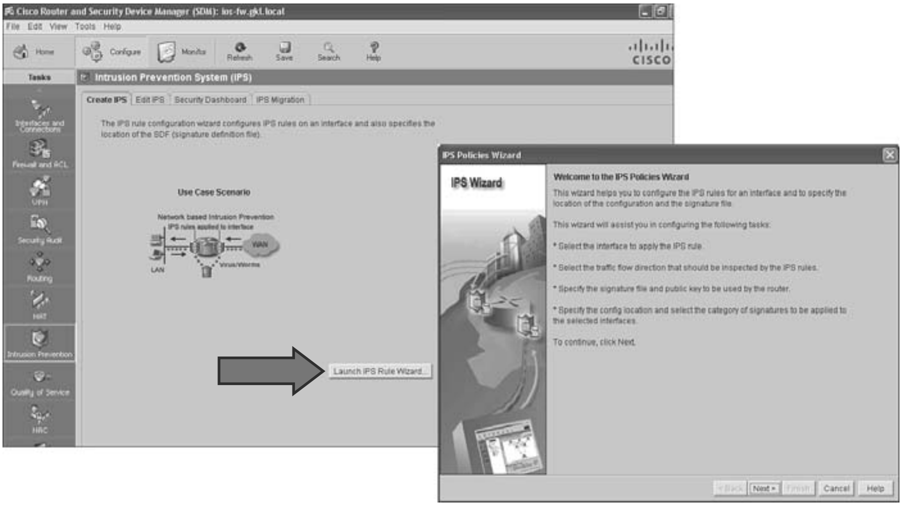
Configuring Cisco IOS IPS Using Cisco SDM

Cisco IOS IPS allows you to manage intrusion prevention on routers that use Cisco IOS Software Release 12.3(8)T4 or later. Cisco IOS IPS monitors and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected. Cisco SDM lets you control the application of Cisco IOS IPS on interfaces, import and edit signature files from Cisco.com, and configure the action that Cisco IOS IPS should take if a threat is detected.

The tasks associated with managing routers and security devices are displayed in a task pane on the left side of the Cisco SDM home page, as shown in Figure 6-15. Choose **Configure > Intrusion Prevention** to reveal the intrusion prevention options in Cisco SDM. You can use Cisco SDM to configure Cisco IOS IPS on routers and security devices.

Use the tabs at the top of the Intrusion Prevention System (IPS) window to navigate to the area you want to configure or monitor:

- **Create IPS:** This tab contains the IPS Rule wizard that you use to create a new Cisco IOS IPS rule.
- **Edit IPS:** This tab allows you to edit Cisco IOS IPS rules and apply or remove them from interfaces.
- **Security Dashboard:** This tab allows you to view the Top Threats table and deploy signatures associated with those threats.
- **IPS Migration:** If the router runs a Cisco IOS Software Release 12.4(11)T or later, you can use this tab to migrate Cisco IOS IPS configurations that were created using earlier releases of the Cisco IOS Software.



The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

Welcome to the IPS Policies Wizard

This wizard helps you to configure the IPS rules for an interface and to specify the location of the configuration and the signature file.

This wizard will assist you in configuring the following tasks:

* Select the interface to apply the IPS rule.

* Select the traffic flow direction that should be inspected by the IPS rules.

* Specify the signature file and public key to be used by the router.

* Specify the config location and select the category of signatures to be applied to the selected interfaces.

To continue, click Next.

Figure 6-15 *Cisco SDM and IPS Wizard*

Tip: In Cisco SDM, when you see the words *the IPS rule configuration* substitute *the IPS signature configuration*.

Cisco SDM enables you to create a new rule on a Cisco router in two ways: manually through the Edit IPS tab or automatically using the IPS Rule Wizard. The Cisco IOS IPS Deployment Guide recommends using the IPS Rule Wizard. The wizard that is launched does more than just configure a rule; it performs all the Cisco IOS IPS configuration steps.

Follow these steps to configure Cisco IOS IPS on the router or security device using Cisco SDM:

Step 1. Choose **Configure > Intrusion Prevention > Create IPS.**

Step 2. Click the **Launch IPS Rule Wizard** button.

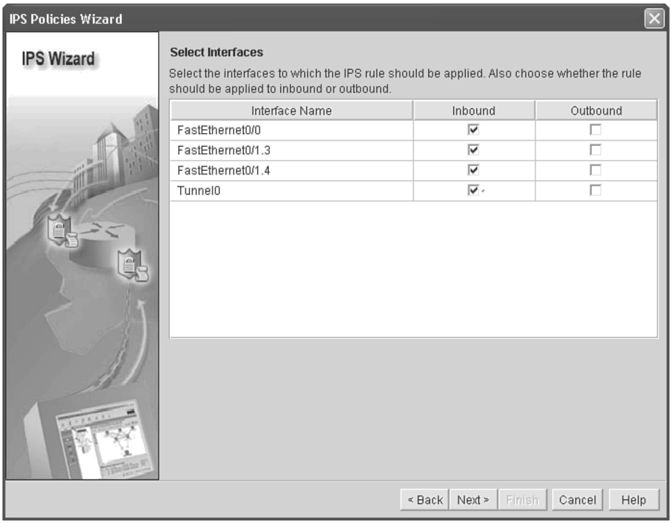
Step 3. Read the Welcome to the IPS Policies Wizard screen, and then click **Next.**

Step 4. Next, you must choose the interfaces on which you want to apply the Cisco IOS IPS rule by specifying whether the rule is to be applied to inbound traffic or outbound traffic, as shown in Figure 6-16. If you check both the Inbound and the Outbound check boxes, the rule applies to traffic flowing in both directions.

Step 5. From the Select Interfaces dialog window, choose the router interfaces to which you want to apply the IPS rule by checking either the Inbound check box, Outbound check box, or both, that is next to the desired interface.

Step 6. Click **Next.**

Step 7. Cisco IOS IPS examines traffic by comparing it against signatures contained in a signature file. The signature file can be located in router flash memory or on



Select Interfaces

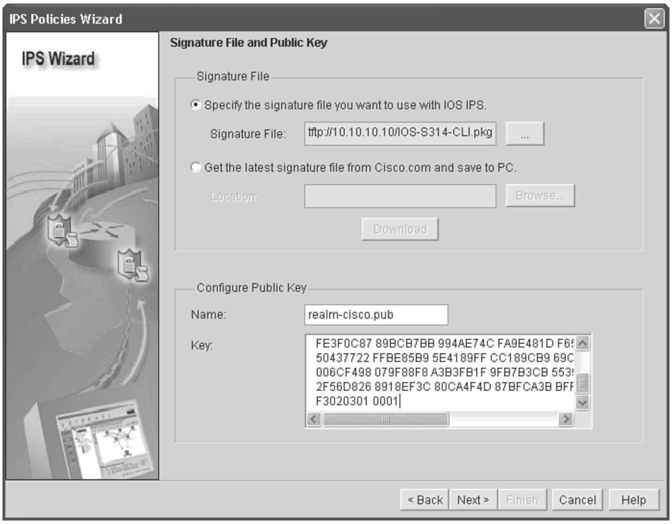
Select the interfaces to which the IPS rule should be applied. Also choose whether the rule should be applied to inbound or outbound.

Interface Name	Inbound	Outbound
FastEthernet0/0	☑	□
FastEthernet0/1.3	☑	□
FastEthernet0/1.4	☑	□
Tunnel0	☑	□

Figure 6-16 *IPS Wizard: Applying Cisco IOS IPS Rule to an Interface*

a remote system that the router can reach. You can specify multiple signature file locations so that if the router is unable to contact the first location, it can attempt to contact other locations until it obtains a signature file.

Step 8. From the Signature File and Public Key dialog window, in the Signature File pane, click either the **Specify the Signature File You Want to Use with the IOS IPS** or **Get the Latest Signature File from Cisco.com and Save to PC** option and fill in the Signature File or Location text box as appropriate, as shown in Figure 6-17.



Signature File and Public Key

Signature File

● Specify the signature file you want to use with IOS IPS.

Signature File: tftp://10.10.10.10/IOS-S314-CLI.pkg

○ Get the latest signature file from Cisco.com and save to PC.

Location:

Configure Public Key

Name: realm-cisco.pub

Key:

```
FE3F0C87 89BCB7BB 994AE74C FA9E481D F6
50437722 FFBE85B9 5E4189FF CC189CB9 69C
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 553
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF
F3020301 0001
```

Figure 6-17 *IPS Wizard—Example of Signature File and Public Key*

Note: The appropriate signature file will be in the form of an IOS IPS update package with the naming convention of IOS-S*xxx*-CLI.pkg (where *xxx* is the number of the signature set).

Step 9. If you chose to download the latest signature file from Cisco.com, you will need to click **Download** when you are ready to download the signature file.

The Cisco IOS IPS signature file contains the default signature information present in each update to the file on Cisco.com. Any changes made to this configuration are saved in a delta file. For security, the delta file must be digitally signed. Follow these steps to place the public-key information in the Name and Key fields.

Step 10. Go to the following link to obtain the public key: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup.

Step 11. Download the key to your PC.

Step 12. Open the key in a text editor and copy the text after the phrase *named-key* into the Name field. For example, if the line of text is "named-key realm-cisco.pub signature" copy "realm-cisco.pub signature" to the Name field.

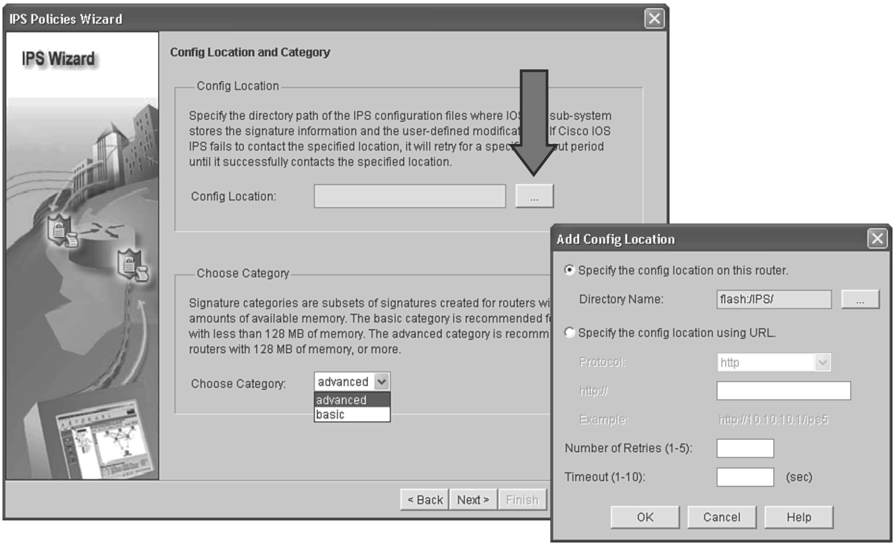
Step 13. Copy the text between the phrase *key-string* and the word *quit* into the Key field. The following output shows what this text might look like:

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

Step 14. Click **Next**.

For Cisco IOS Release 12.4(11) or later, you can specify the following additional options:

- **Config location:** This information specifies where to store files that contain changes to the Cisco IOS IPS configuration. This information consists of the signature file and the delta file that is created when changes are made to the signature information, as shown in Figure 6-18.



IPS Policies Wizard

Config Location and Category

Config Location

Specify the directory path of the IPS configuration files where IO sub-system stores the signature information and the user-defined modificat If Cisco IOS IPS fails to contact the specified location, it will retry for a speci ut period until it successfully contacts the specified location.

Config Location:

Choose Category

Signature categories are subsets of signatures created for routers wi amounts of available memory. The basic category is recommended f with less than 128 MB of memory. The advanced category is recomm routers with 128 MB of memory, or more.

Choose Category: advanced

Add Config Location

● Specify the config location on this router.

Directory Name: flash:/IPS/

○ Specify the config location using URL.

Protocol: http

http://

Example: http://10.10.10.1/ips5

Number of Retries (1-5):

Timeout (1-10): (sec)

Figure 6-18 *IPS Wizard: Config Location and Category*

- **Signature category:** The basic signature category is appropriate for routers with less than 128 MB of flash memory, and the advanced signature category is appropriate for routers with more than 128 MB of flash memory.

Follow these steps to specify a location for storing the signature information and what signature category you would like the router to use:

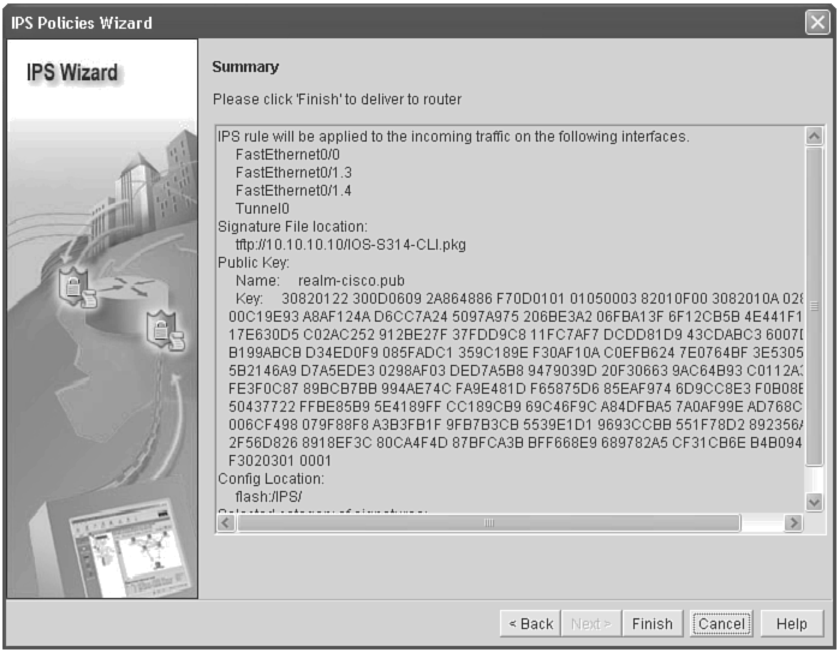
Step 15. From the Config Location and Category window, in the Config Location section, click the ellipsis (...) button to the right of the Config Location field to display a dialog that allows you to specify a location. After you enter information in this dialog, Cisco SDM displays the path to the location in this field.

Step 16. Because router memory and resource constraints can prevent the use of all the available signatures, there are two categories of signatures: basic and advanced. In the Choose Category field, choose the category that will allow the Cisco IOS IPS to function efficiently on the router.

Step 17. Click **Finish.** The IPS Policies Wizard confirms configuration as follows:

```
IPS rule will be applied to the incoming traffic on the
following interfaces.
     FastEthernet0/0
     FastEthernet0/1.3
     FastEthernet0/1.4
     Tunnel0
Signature File location:
     tftp://10.10.10.10/IOS-S314-CLI.pkg
Public Key:
    Name:    realm-cisco.pub
    Key:    30820122 300D0609 2A864886 F70D0101
01050003 82010F00 3082010A
 02820101
<output omitted>
Config Location
     flash:/IPS/
Selected category of signatures:
     Basic
```

Figure 6-19 shows actual Wizard Summary windows



Summary

Please click 'Finish' to deliver to router

```
IPS rule will be applied to the incoming traffic on the following interfaces.
   FastEthernet0/0
   FastEthernet0/1.3
   FastEthernet0/1.4
   Tunnel0
Signature File location:
   tftp://10.10.10.10/IOS-S314-CLI.pkg
Public Key:
   Name:    realm-cisco.pub
   Key:    30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02
  00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F1
  17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007
  B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E5305
  5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A
  FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08
  50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C
  006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356
  2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094
  F3020301 0001
Config Location:
   flash:/IPS/
```

Figure 6-19 *IPS Wizard: IPS Policy Summary*

Configuring Cisco IOS IPS Using CLI

To use the command-line interface (CLI) to specify an IPS rule, use the **ip ips name** *name* command in global configuration mode as follows:

```
router(config)# ip ips name sdm_ips_rule
```

To specify the location of the IPS configuration, use the **ip ips config location** *location* global configuration command, as demonstrated here:

```
router(config)# ip ips config location flash:/ipsdir/retries 1
```

To specify the method of event notification, use the **ip ips notify** global configuration command. The following is an example of event notification sent using Security Device Event Exchange (SDEE), which is a standard developed to communicate an event generated by security devices:

```
router(config)# ip ips notify SDEE
```

Note: Examples in this section of the chapter dealing with Cisco IOS IPS CLI configuration assume that the signature files are already on the router.

To configure the router to support the default basic signature set use the **ip ips signature-category** global configuration command as follows:

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
```

To apply an IPS rule to an interface, use the **ip ips** *ips_rule_name* command in interface configuration mode as demonstrated here:

```
router(config)# interface Serial0/0/0
router(config-if)# ip ips sdm_ips_rule in
```

Virtual Fragment Reassembly

Virtual Fragment Reassembly (VFR) enables the Cisco IOS Firewall to examine out-of-sequence fragments and reorder the packets into the order. It examines the number of fragments from a same single IP address. When VFR is enabled on a Cisco IOS Firewall, it creates the appropriate dynamic ACLs, thereby protecting the network from various fragmentation attacks. To enable VFR on an interface, use the **ip virtual-reassembly** command in interface configuration mode, as demonstrated here:

```
Router(config)# interface Serial0/0/0
Router(config-if)# ip virtual-reassembly
```

Example 6-1 provides a combined view of the commands shown in the preceding paragraphs.

Example 6-1 *Cisco IOS IPS CLI Configuration*

```
Router(config)# ip ips name sdm_ips_rule
Router(config)# ip ips config location flash:/ipsdir/ retries 1
Router(config)# ip ips notify SDEE
!
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
!
Router(config)# interface Serial0/0/0
Router(config-if)# ip ips sdm_ips_rule in
Router(config-if)# ip virtual-reassembly
```

Configuring IPS Signatures

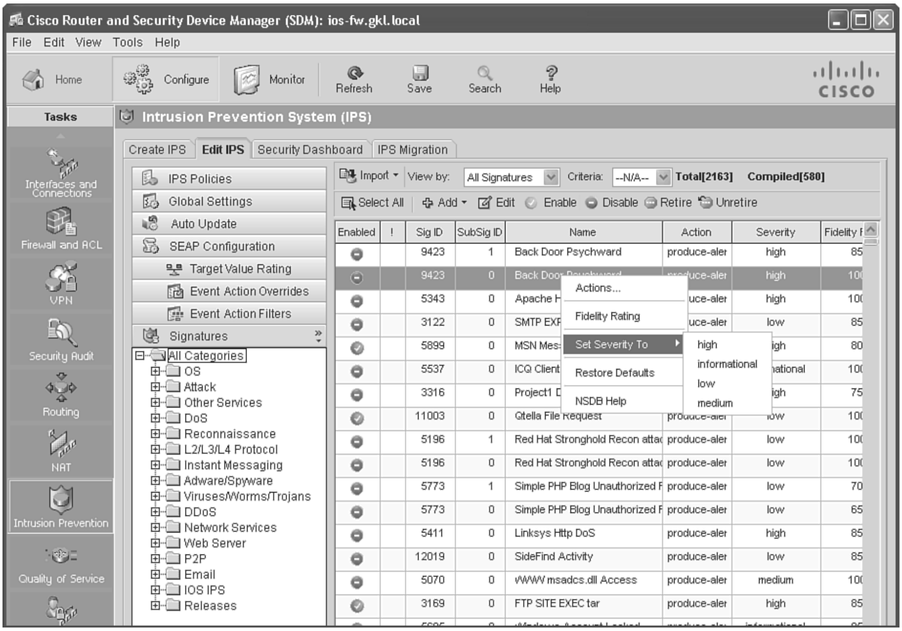
Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IOS IPS have built-in signatures that the router can use, and you can import signatures for the router to use. Imported signatures are stored in a signature file.

IPS signatures are loaded as part of the procedure to create a Cisco IOS IPS rule using the IPS rule wizard. To view the configured Cisco IOS IPS signatures on the router, choose **Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories**. Because signatures optimize your configuration, confirm that all the correct signatures are loaded on the router or security device. From this window, you can add customized signatures or import signatures that are downloaded from Cisco.com. You can also edit, delete, enable, and disable signatures.

Note: You can import signatures from the router only if the router has a DOS-based file system.

Note: Signature files are available from Cisco at http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup-sdm. A Cisco.com login is required for this site.

The signature tree enables you to filter the signature list according to the type of signature that you want to view. To modify a signature, right-click the signature and choose an option from the pop-up menu, as shown in Figure 6-20. To change the severity of the signature, choose **Set Severity To**.



Enabled	!	Sig ID	SubSig ID	Name	Action	Severity	Fidelity F
⊖		9423	1	Back Door Psychward	produce-aler	high	85
⊖		9423	0	Back Door	produce-aler	high	10(
⊖		5343	0	Apache H	uce-aler	high	10(
⊖		3122	0	SMTP EXF	uce-aler	low	85
✓		5899	0	MSN Mes		igh	80
⊖		5537	0	ICQ Client		ational	10(
⊖		3316	0	Project1 D		igh	75
✓		11003	0	Qtella File Request	produce-aler	low	10(
⊖		5196	1	Red Hat Stronghold Recon attac	produce-aler	low	10(
⊖		5196	0	Red Hat Stronghold Recon attac	produce-aler	low	10(
⊖		5773	1	Simple PHP Blog Unauthorized F	produce-aler	low	70
⊖		5773	0	Simple PHP Blog Unauthorized F	produce-aler	low	65
⊖		5411	0	Linksys Http DoS	produce-aler	high	85
⊖		12019	0	SideFind Activity	produce-aler	low	85
⊖		5070	0	WWW msadcs.dll Access	produce-aler	medium	10(
✓		3169	0	FTP SITE EXEC tar	produce-aler	high	85

Figure 6-20 *Setting Signature Severity*

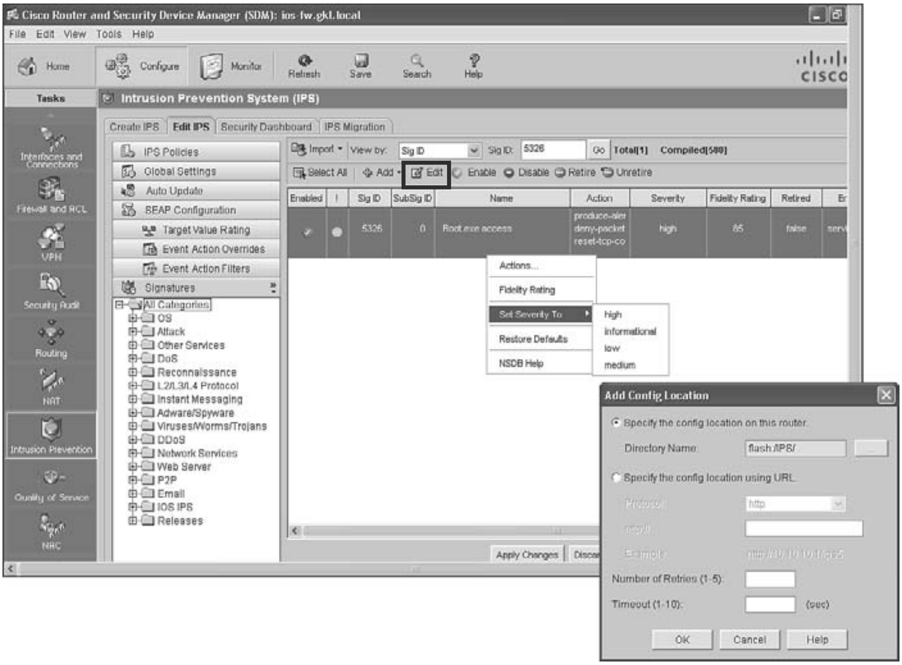
> **Note:** Cisco maintains an alert center that provides information about emerging threats. See the Cisco Security Center for more information at http://tools.cisco.com/security/center/home.x.

You can tune a signature configuration using Cisco SDM. To tune a signature, choose **Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories**. A list of available signatures appears.

To modify a signature action, right-click the signature and choose **Actions** from the pop-up menu. The Assign Actions window appears, as shown in Figure 6-21, and displays the actions that can be taken upon a signature match. The available actions depend on the signature, but the following are the most common actions:

- **Deny Attacker Inline:** Create an ACL that denies all traffic from the IP address that is considered the source of the attack by the Cisco IOS IPS system.
- **Deny Connection Inline:** Drop the packet and all future packets from this TCP flow.
- **Deny Packet Inline:** Do not transmit this packet (inline only).
- **Produce Alert:** Generate an alarm message.
- **Reset TCP Connection:** Send TCP resets to terminate the TCP flow.

To access and configure signature parameters, choose the signature and then click the **Edit** button in the Cisco SDM Configure Signatures window, as shown in Figure 6-22.



View by: Sig ID Sig ID: 5326 Go Total[1] Compiled[580]

Enabled	!	Sig ID	SubSig ID	Name	Action	Severity	Fidelity Rating	Retired	Er
✓	●	5326	0	Root.exe access	produce-aler deny-packet reset-tcp-co	high	85	false	serv

Add Config Location

◉ Specify the config location on this router.

Directory Name: flash:/IPS/

○ Specify the config location using URL.

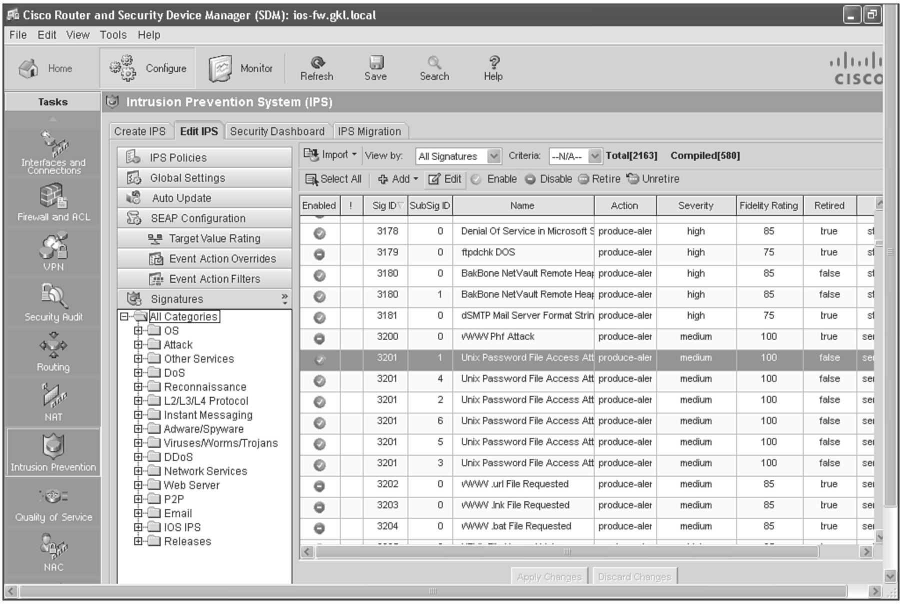
Protocol: http

Example: http://10.10.10.1/sdf5

Number of Retries (1-5):

Timeout (1-10): (sec)

Figure 6-21 *Configuring Signature Actions*

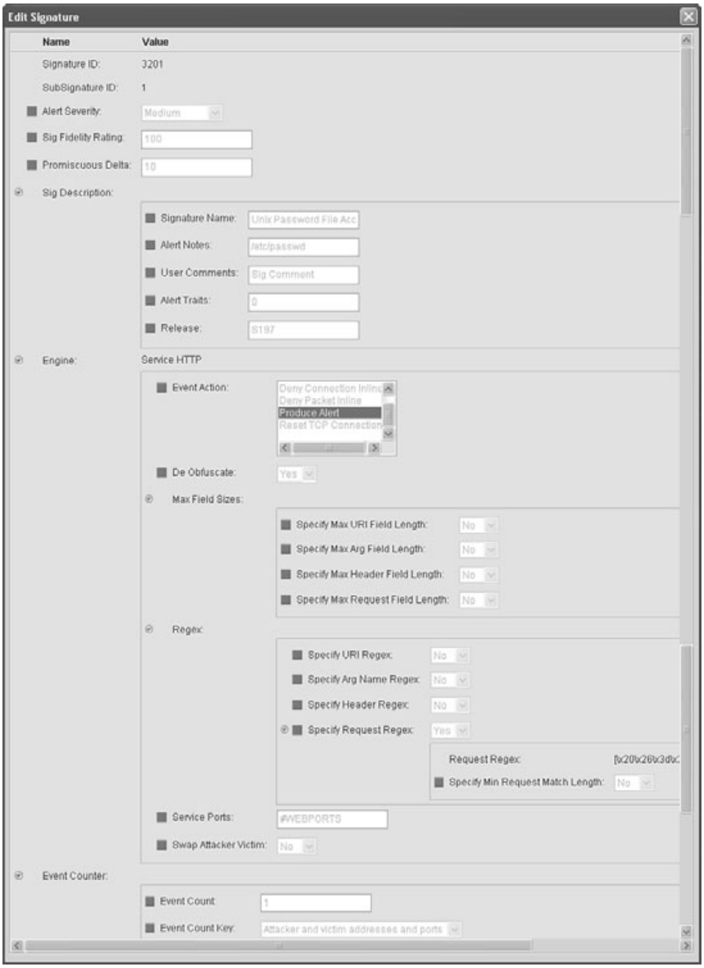


View by: All Signatures Criteria: --N/A-- Total[2163] Compiled[580]

Enabled	!	Sig ID	SubSig ID	Name	Action	Severity	Fidelity Rating	Retired	
✓		3178	0	Denial Of Service in Microsoft S	produce-aler	high	85	true	st
⊖		3179	0	ftpdchk DOS	produce-aler	high	75	true	st
✓		3180	0	BakBone NetVault Remote Hea	produce-aler	high	85	false	st
✓		3180	1	BakBone NetVault Remote Hea	produce-aler	high	85	false	st
✓		3181	0	dSMTP Mail Server Format Strin	produce-aler	high	75	true	st
⊖		3200	0	WWW Phf Attack	produce-aler	medium	100	true	sei
✓		3201	1	Unix Password File Access Att	produce-aler	medium	100	false	sei
✓		3201	4	Unix Password File Access Att	produce-aler	medium	100	false	sei
✓		3201	2	Unix Password File Access Att	produce-aler	medium	100	false	sei
✓		3201	6	Unix Password File Access Att	produce-aler	medium	100	false	sei
✓		3201	5	Unix Password File Access Att	produce-aler	medium	100	false	sei
✓		3201	3	Unix Password File Access Att	produce-aler	medium	100	false	sei
⊖		3202	0	WWW .url File Requested	produce-aler	medium	85	true	sei
⊖		3203	0	WWW .lnk File Requested	produce-aler	medium	85	true	sei
⊖		3204	0	WWW .bat File Requested	produce-aler	medium	85	true	sei

Figure 6-22 *Preparing to Edit the Cisco IOS IDS Signatures*

In the dialog box that results from clicking the **Edit** button in the Cisco SDM Configure Signatures window, shown in Figure 6-23, configure the signature parameters.



Name	Value
Signature ID:	3201
SubSignature ID:	1
■ Alert Severity:	Medium
■ Sig Fidelity Rating:	100
■ Promiscuous Delta:	10
Sig Description:	
■ Signature Name:	Unix Password File Acc
■ Alert Notes:	/etc/passwd
■ User Comments:	Sig Comment
■ Alert Traits:	0
■ Release:	S197
Engine:	Service HTTP
■ Event Action:	Deny Connection Inline Deny Packet Inline Produce Alert Reset TCP Connection
■ De Obfuscate:	Yes
Max Field Sizes:	
■ Specify Max URI Field Length:	No
■ Specify Max Arg Field Length:	No
■ Specify Max Header Field Length:	No
■ Specify Max Request Field Length:	No
Regex:	
■ Specify URI Regex:	No
■ Specify Arg Name Regex:	No
■ Specify Header Regex:	No
■ Specify Request Regex:	Yes
Request Regex:	[\x20\x26\x3d\x
■ Specify Min Request Match Length:	No
■ Service Ports:	#WEBPORTS
■ Swap Attacker Victim:	No
Event Counter:	
■ Event Count:	1
■ Event Count Key:	Attacker and victim addresses and ports

Figure 6-23 *Editing Signatures Using Cisco SDM*

Different signatures will have different parameters that you can modify. The following are common fields.

- **Signature ID:** This field displays a unique numerical value that is assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.
- **SubSignature ID:** This field displays a unique numeric value that is assigned to this subsignature. A subsig ID identifies a more granular version of a broad signature.
- **Alert Severity:** This field displays the severity of the alert for this signature.

- **Sig Description:** This section includes the signature name, alert notes, user comments, alert traits, and release number.
- **Engine:** This section contains information about what engine the signature uses and characteristics about how the engine operates.
- **Event Counter:** This section displays the event count, the event count key, and whether an alert interval is to be specified. An alert interval allows you to define special handling for timed events.
- **Alert Frequency:** (Not shown in Figure 6-23.) This section has settings to define the frequency of the alert.
- **Status:** (Not shown in Figure 6-23) This section shows whether the signature is enabled and whether the signature is retired.

Monitoring IOS IPS

Figure 6-24 shows how you can use the Security Device Event Exchange (SDEE) protocol and a syslog-based approach to send Cisco IPS alerts. The sensor generates an alarm when an enabled signature is triggered. Alarms are stored on the sensor. A host can pull the alarms from the sensor using SDEE. Pulling alarms from a sensor allows multiple hosts to subscribe to the event "feed" to allow a host or hosts to subscribe on an as-needed basis.

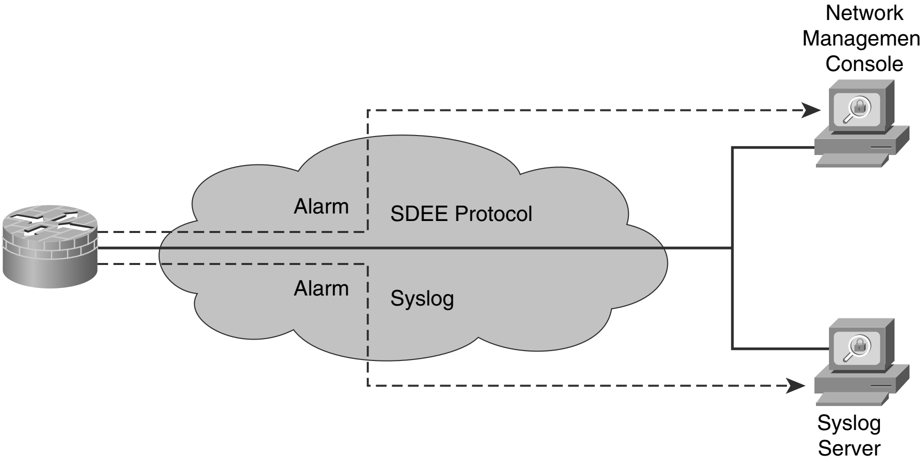


Figure 6-24 *Support for SDEE and Syslog*

The support for SDEE and syslog in the Cisco IOS IPS solution is as follows:

- Cisco IOS Software supports the SDEE protocol. When Cisco SDEE notification is enabled (by using the **ip ips notify sdee** command), by default 200 events can be stored in the event buffer, whose size can be increased to hold a maximum of 1000 events. When you disable Cisco SDEE notification, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

- SDEE uses a pull mechanism. That is, requests come from the network management application, and the IDS and IPS router responds.
- SDEE becomes the standard format for all vendors to communicate events to a network management application.
- You must also enable HTTP or HTTPS on the router, using the **ip http server** command, when you enable SDEE. The use of HTTPS ensures that data is secured as it traverses the network.
- The Cisco IOS IPS router still sends IPS alerts via syslog.

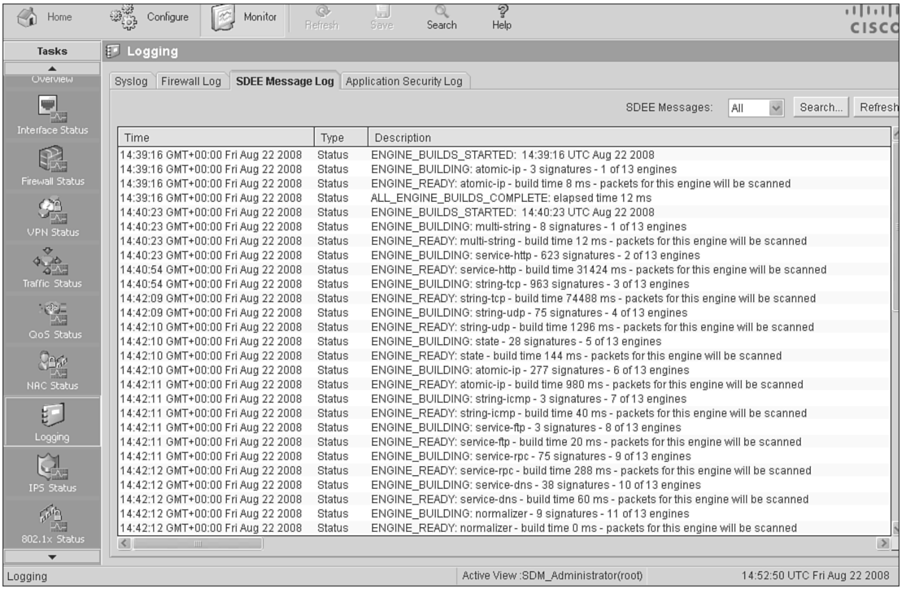
When you use Cisco SDM, you can keep track of alarms that are common in SDEE system messages, including IPS signature alarms. The following is an example of an SDEE system alarm message:

```
%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address
[192.168.121.1:137 ->192.168.121.255:137]
```

The preceding alarm was triggered by the fact that a packet with a private addresses, as listed in RFC 1918, traversed the IPS sensor.

Note: For a complete list of the Cisco IOS IPS system messages, refer to the "Interpreting Cisco IPS System Messages" section in the *Cisco IOS Security Configuration Guide, Release 12.4* available at http://tinyurl.com/3ufo6j.

To view SDEE alarm messages in Cisco SDM, choose **Monitor > Logging > SDEE Message Log**, as shown in Figure 6-25.



SDEE Messages: All

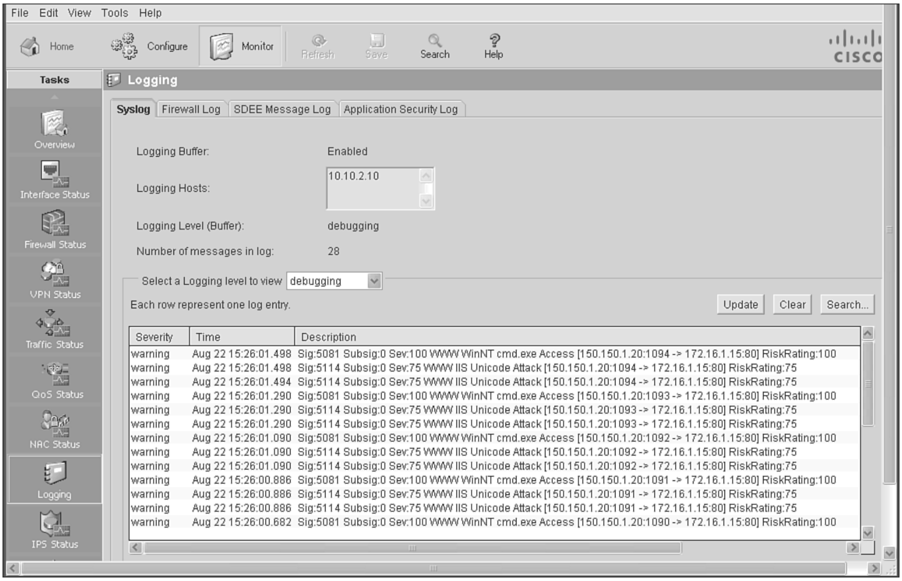
Time	Type	Description
14:39:16 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDS_STARTED: 14:39:16 UTC Aug 22 2008
14:39:16 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
14:39:16 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
14:39:16 GMT+00:00 Fri Aug 22 2008	Status	ALL_ENGINE_BUILDS_COMPLETE: elapsed time 12 ms
14:40:23 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDS_STARTED: 14:40:23 UTC Aug 22 2008
14:40:23 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13 engines
14:40:23 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: multi-string - build time 12 ms - packets for this engine will be scanned
14:40:23 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: service-http - 623 signatures - 2 of 13 engines
14:40:54 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: service-http - build time 31424 ms - packets for this engine will be scanned
14:40:54 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: string-tcp - 963 signatures - 3 of 13 engines
14:42:09 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: string-tcp - build time 74488 ms - packets for this engine will be scanned
14:42:09 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
14:42:10 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: string-udp - build time 1296 ms - packets for this engine will be scanned
14:42:10 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
14:42:10 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: state - build time 144 ms - packets for this engine will be scanned
14:42:10 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: atomic-ip - 277 signatures - 6 of 13 engines
14:42:11 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: atomic-ip - build time 980 ms - packets for this engine will be scanned
14:42:11 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
14:42:11 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: string-icmp - build time 40 ms - packets for this engine will be scanned
14:42:11 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
14:42:11 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: service-ftp - build time 20 ms - packets for this engine will be scanned
14:42:11 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13 engines
14:42:12 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: service-rpc - build time 288 ms - packets for this engine will be scanned
14:42:12 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
14:42:12 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: service-dns - build time 60 ms - packets for this engine will be scanned
14:42:12 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
14:42:12 GMT+00:00 Fri Aug 22 2008	Status	ENGINE_READY: normalizer - build time 0 ms - packets for this engine will be scanned

Active View :SDM_Administrator(root)

14:52:50 UTC Fri Aug 22 2008

Figure 6-25 *Viewing an SDDE Alarm Message*

To view alarms generated by Cisco IOS IPS, choose **Monitor > Logging > Syslog**, as shown in Figure 6-26.



Logging

Logging Buffer: Enabled

Logging Hosts: 10.10.2.10

Logging Level (Buffer): debugging

Number of messages in log: 28

Select a Logging level to view: debugging

Each row represent one log entry.

Severity	Time	Description
warning	Aug 22 15:26:01.498	Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [150.150.1.20:1094 -> 172.16.1.15:80] RiskRating:100
warning	Aug 22 15:26:01.498	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1094 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:01.494	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1094 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:01.290	Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [150.150.1.20:1093 -> 172.16.1.15:80] RiskRating:100
warning	Aug 22 15:26:01.290	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1093 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:01.290	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1093 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:01.090	Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [150.150.1.20:1092 -> 172.16.1.15:80] RiskRating:100
warning	Aug 22 15:26:01.090	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1092 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:01.090	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1092 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:00.886	Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [150.150.1.20:1091 -> 172.16.1.15:80] RiskRating:100
warning	Aug 22 15:26:00.886	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1091 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:00.886	Sig:5114 Subsig:0 Sev:75 WWW IIS Unicode Attack [150.150.1.20:1091 -> 172.16.1.15:80] RiskRating:75
warning	Aug 22 15:26:00.682	Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [150.150.1.20:1090 -> 172.16.1.15:80] RiskRating:100

Figure 6-26 *Viewing a Syslog IPS Alarm*

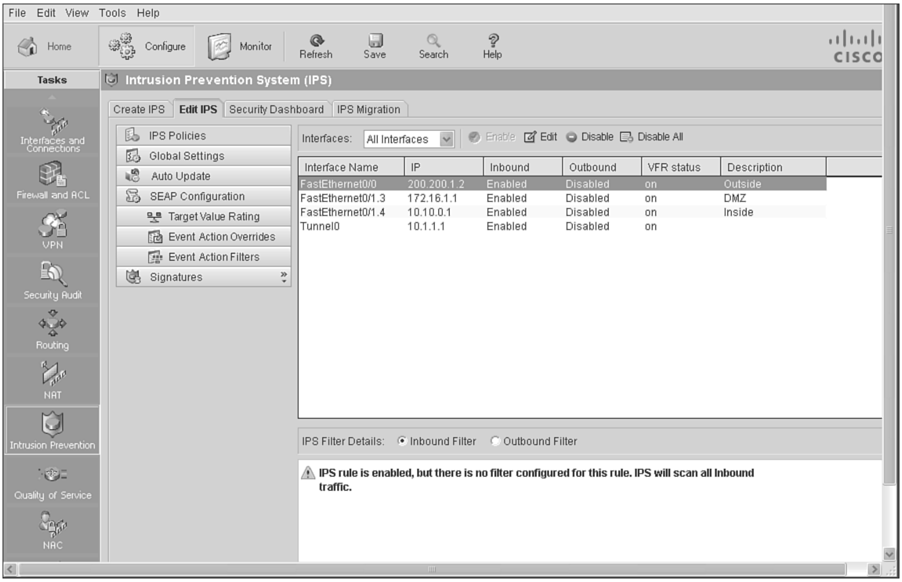
Verifying IPS Operation

To verify the IPS configuration on the router, choose **Configure > Intrusion Prevention > Edit IPS**, as shown in Figure 6-27. The Edit IPS tab shows all the interfaces on the router and whether they are configured for Cisco IOS IPS. If *Enabled* appears in either the Inbound or the Outbound column, Cisco IOS IPS is enabled for that direction of traffic on that interface. If *Disabled* appears in either the Inbound or the Outbound column, Cisco IOS IPS is disabled for that direction on the interface.

Cisco IOS IPS cannot identify the contents of IP fragments when VFR is not enabled, and it cannot gather port information from the fragment to match it with a signature. Therefore, fragments can pass through the network without being examined or without a dynamic ACL being created on the Cisco IOS Firewall. You will remember that VFR enables the Cisco IOS Firewall to examine out-of-sequence fragments. VFR can create the dynamic ACLs necessary to protect against fragment attacks

The VFR status field shows the status of VFR on an interface. If VFR is enabled on the interface, the column displays *On*. If VFR is disabled on the interface, the column displays *Off*.

The Edit IPS tab also contains buttons that enable you to configure and manage Cisco IOS IPS policies, security messages, signatures, and more.



Interfaces: All Interfaces

Interface Name	IP	Inbound	Outbound	VFR status	Description
FastEthernet0/0	200.200.1.2	Enabled	Disabled	on	Outside
FastEthernet0/1.3	172.16.1.1	Enabled	Disabled	on	DMZ
FastEthernet0/1.4	10.10.0.1	Enabled	Disabled	on	Inside
Tunnel0	10.1.1.1	Enabled	Disabled	on	

IPS Filter Details: ● Inbound Filter ○ Outbound Filter

⚠ **IPS rule is enabled, but there is no filter configured for this rule. IPS will scan all Inbound traffic.**

Figure 6-27 *Verifying IPS Policies*

Use the **show ip ips configuration** command to display additional configuration data that is not displayed with the **show running-config** command. Example 6-2 shows some sample output from the **show ip ips configuration** command.

Example 6-2 *show ip ips configuration Command Output*

```
Router# show ip ips configuration
IPS Signature File Configuration Status
    Configured Config Locations: flash:/ipsdir/
    Last signature default load time: 04:39:33 UTC Dec 14 2007
    Last signature delta load time: -none-
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 353
    Total Inactive Signatures: 1783

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name sdm_ips_rule
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface FastEthernet0/0
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set
      Interface FastEthernet0/1
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
    Category ios_ips:
        Enable: True
    Category ios_ips advanced:
       Enable: True
```

Use the **show ip ips interface** command to display interface configuration data. Example 6-3 displays output from the **show ip ips interface** command, revealing that the inbound IPS audit rule **sdm_ips_rule** is applied to FastEthernet 0/0 and FastEthernet 0/1. There is no rule applied for outgoing traffic on either interface.

Example 6-3 *show ip ips interface Command Output*

```
Router# show ip ips interfaces
Interface Configuration
      Interface FastEthernet0/0
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set
      Interface FastEthernet0/1
        Inbound IPS rule is sdm_ips_rule
       Outgoing IPS rule is not set
```

Use the **show ip ips all** command to display additional configuration data that is not displayed with the **show ip ips configuration** command.

In Example 6-4, the output from the **show ip ips all** command shows that syslog and SDEE notification is enabled, and that there are 693 active signatures and 1443 inactive signatures on the router.

Example 6-4 *show ip ips all Command Output*

```
Router# show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsstore/
    Last signature default load time: 00:25:35 UTC Dec 6 2007
    Last signature delta load time: -none-
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 693
    Total Inactive Signatures: 1443

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name myips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface FastEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is myips

IPS Category CLI is not configured

IPS Category CLI is not configured
```

Summary

This chapter described how intrusion detection system (IDS) and intrusion prevention system (IPS) technology embedded in Cisco host- and network-based IDS and IPS solutions fight Internet worms and viruses in real time. More precisely, you have learned how

- A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity.
- To use Cisco SDM to configure Cisco IOS IPS on the router or security device, choose **Configure > Intrusion Prevention > Create IPS** in Cisco SDM and click the **Launch IPS Rule Wizard** button.
- Cisco IOS IPS combines existing Cisco IDS and IPS product features.
- To configure Cisco IOS IPS on the router or security device, click the **Launch IPS Rule Wizard** button in Cisco SDM.
- Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks.
- Cisco IOS IPS alarms are communicated using SDEE and syslog.
- The command **show ip ips all** displays all the available IPS information.

References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco Intrusion Prevention System: Introduction*, http://www.cisco.com/go/ips

Cisco Systems, Inc. *Cisco Security Monitoring, Analysis and Response System: Introduction*, http://www.cisco.com/go/mars

Cisco Systems, Inc. *Cisco Security Agent: Introduction*, http://www.cisco.com/go/csa

Cisco Systems, Inc. Cisco Intrusion Detection System Event Viewer 3DES Cryptographic Software Download, http://www.cisco.com/cgi-bin/tablebuild.pl/ids-ev

Cisco Systems, Inc. *Cisco IOS Intrusion Prevention System (IPS): Cisco IOS IPS Supported Signature List in 4.x Signature Format*, http://www.cisco.com/en/US/partner/products/ps6634/products_white_paper0900aecd8039e2e4.shtml

Cisco Systems, Inc. Software Download: Cisco IOS IPS, http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco Systems, Inc. Software Download: Cisco IDS Management Center - Version *4.x* Signature Updates, http://www.cisco.com/cgi-bin/tablebuild.pl/idsmc-ids4-sigup

Cisco Systems, Inc. *Cisco IOS Security Configuration Guide, Release 12.4: Configuring Cisco IOS Intrusion Prevention System* (IPS), http://tinyurl.com/3ufo6j

Cisco System, Inc. Tools & Resources: Software Download, Cisco IOS IPS Signature Package for SDM 2.4, http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup-sdm

Cisco System, Inc. Cisco Security Center, http://tools.cisco.com/security/center/home.x

Cisco Systems, Inc. *Cisco IOS Security Configuration Guide, Release 12.4: Configuring Cisco IOS Intrusion Prevention System (IPS)*, http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804453cf.html

SearchSecurity.com. http://searchsecurity.techtarget.com/