

## Understanding Intrusion Prevention and Detection

Cisco provides intrusion detection and prevention in a variety of ways in its current security portfolio. You might add this powerful tool to your network via a dedicated hardware appliance known as a sensor, or you might add this functionality using a network module inserted into a router or a switch. However you decide to implement the technology, the goal is the same: to take some action based on an attack introduced to your network. This action might be to alert the network administrator via an automated notification, or it might be to prevent the attack from dropping the packet at a device.

## Intrusion Prevention Versus Intrusion Detection

Intrusion detection is powerful in that you can be notified when potential problems or attacks are introduced into your network. Note, however, that detection cannot prevent these attacks from occurring. Detection cannot prevent the attacks because it operates on copies of packets. Often, these copies of packets are received from another Cisco device (typically a switch). Sensors operating using intrusion detection are said to be running in promiscuous mode.

Intrusion prevention is more powerful in that potential threats and attacks can be stopped from entering your network, or a particular network segment. Prevention is possible by the sensor because it is operating inline with packet flows.

## IPS/IDS Terminology

You should be aware of many security terms that are related to intrusion detection and prevention technologies.

## Vulnerability

A vulnerability is a weakness that compromises the security or functionality of a particular system in your network. An example of a vulnerability is a web form on your public website that does not adequately filter inputs and guard against improper data entry. An attacker might enter invalid characters in an attempt to corrupt the underlying database.

## Exploit

An exploit is a mechanism designed to take advantage of vulnerabilities that exist in your systems. For example, if you have poor passwords in use in your network, a password-cracking package might be the exploit aimed at this vulnerability.

## False alarms

False alarms are IPS events that you do not want occurring in your implementation. There are two types of these alarms: false positive and false negative. Both are undesirable.

### False positive

A false positive means that an alert has been triggered, but it was for traffic that does not constitute an actual attack. This type of traffic is often referred to as benign traffic.

### False negative

A false negative occurs when attack traffic does not trigger an alert on the IPS device. This is often viewed as the worst type of false alarm, for obvious reasons.

## True alarms

There are two types of true alarms in IPS terminology. Both true positives and true negatives are desirable.

### True positive

A true positive means that an attack was recognized and responded to by the IPS device.

### True negative

This means that nonoffending or benign traffic did not trigger an alarm.

## Promiscuous Versus Inline Mode

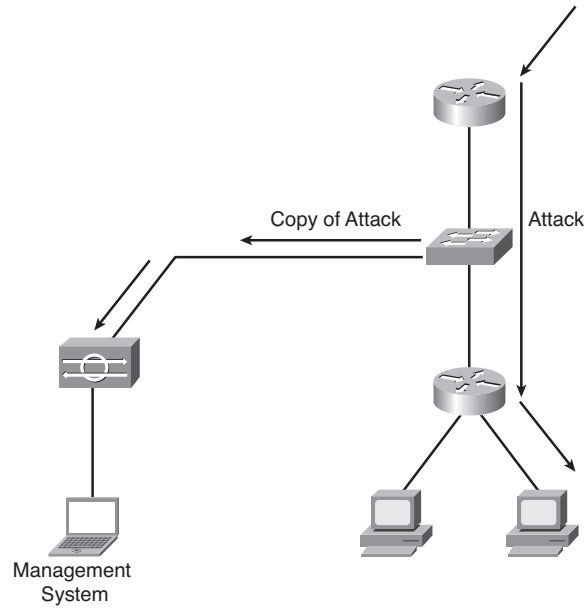
IDS/IPS sensors operate in promiscuous mode by default. This means that a device (often a switch) captures traffic for the sensor and forwards a copy for analysis to the sensor. Because the device is working with a copy of the traffic, the device is performing intrusion detection. It can detect an attack and send an alert (and take other actions), but it does not prevent the attack from entering the network or a network segment. It cannot prevent the attack, because it is not operating on traffic “inline” in the forwarding path. Figure 5-1 shows an example of a promiscuous mode IDS implementation.

If a Cisco IPS device is operating in inline mode, it can do prevention as opposed to mere detection. This is because the IPS device is in the actual traffic path. This makes the device more effective against worms and atomic attacks (attacks that are carried out by a single packet). Figure 5-2 shows an example of inline mode IPS.

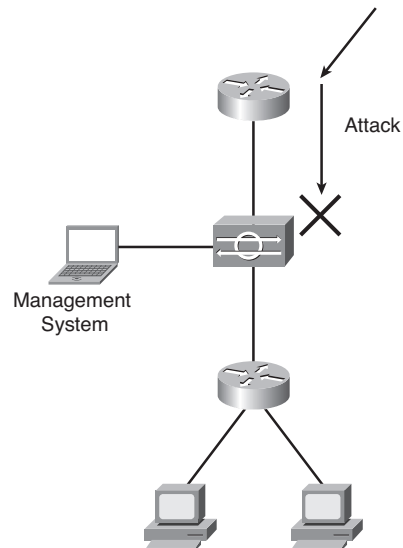
# CHAPTER 5

## Cisco IOS IPS

**FIGURE 5-1**  
Promiscuous mode  
(IDS)



**FIGURE 5-2**  
Inline mode (IPS)



To configure inline mode, you require two monitoring interfaces that are defined in the sensor as an inline pair. This pair of interfaces acts as a transparent Layer 2 structure that can drop an attack that fires a signature.

Keep in mind that a sensor could be configured inline but could be set up so that it only alerts and doesn't drop packets. This is an example of an inline configuration in which only intrusion detection is performed.

Cisco Intrusion Prevention System (IPS) Version 6.0 software permits a device to do promiscuous mode and inline mode simultaneously. This allows one segment to be monitored for intrusion detection only, whereas another segment features intrusion prevention protection.

## Approaches to Intrusion Prevention

A device can take many different approaches to securing the network using IPS. This section describes these various approaches.

### Signature-based

Although Cisco uses a blend of detection and prevention technologies, signature-based IPS is the primary tool used by Cisco IPS solutions. Cisco releases signatures that are added to the device that identify a pattern that the most common attacks present. This is much less prone to false positives and ensures that IPS devices are stopping common threats. This type of approach is also known as pattern matching. As different types of attacks are created, these signatures can be added, tuned, and updated to deal with the new attacks.

### Anomaly-based

This type of IPS technology is often called profile-based. It attempts to discover activity that deviates from what an engineer defines as "normal" activity. Because it can be so difficult to define what is normal activity for a given network, this approach tends to be prone to a high number of false positives.

There are two common types of anomaly-based IPS: statistical anomaly detection and nonstatistical. The statistical approach learns about the traffic patterns on the network itself, and the nonstatistical method uses information coded by the vendor.

## Policy-based

With this type of technology, the security policy is “written” into the IPS device. Alarms are triggered if activities are detected that violate the security policy coded by the organization. Notice how this differs from signature-based. Signature-based focuses on stopping common attacks, whereas policy-based is more concerned with enforcing the security policy of the organization.

## Protocol-analysis-based

Although this approach is similar to signature based, it looks deeper into packets thanks to a protocol-based inspection of the packet payload that can occur. Most signatures examine rather common settings, but the protocol-analysis-based approach can do much deeper packet inspection and is more flexible in finding some types of attacks.

## Exploring Evasive Techniques

Because attackers are aware of IPS technologies, they have developed ways to counter these devices in an attempt to continue attacks on network systems.

## String match

In this type of attack, strings in the data are changed in minor ways in an attempt to evade detection.

Obfuscation is one way in which control characters, hexadecimal representation, or Unicode representation help to disguise the attack. Another string match type of evasive technique is to just change the case of the string.

## Fragmentation

With this evasive measure, the attacker breaks the attack packets into fragments so that they are more difficult to recognize. Fragmentation adds a layer of complexity for the sensor, which now must engage in the resource-intensive process of reassembling the packets.

## Session

In this type of attack, the attacker spreads around the attack using a large number of very small packets, not using fragmentation in the approach. TCP segment reassembly can be used to combat this evasive measure.

## Insertion

In this evasive technique, the attacker inserts data that is harmless along with the attack data. The IPS sensor does not fire an alert based on the harmless data. The end system ignores the harmless data and processes only the attack data.

## Evasion

With this type of evasive technique, the attacker has the sensor see a different data stream than the intended victim. Unlike the insertion attack, the end system sees more data than the sensor, which results in an attack.

## TTL-based

One way to implement an insertion attack is to manipulate the Time-to-Live value of fragments. With this evasive procedure, the IPS sensor sees a different data stream than the end system thanks to the manipulation of the TTL field in the IP header.

## Encryption-based

This is an effective means of having attacks enter the network. The attacker sends the attack via an encrypted session. The encrypted attack cannot be detected by the IPS device. Because this method of foiling the IPS device exists, care must be taken to ensure that encrypted sessions cannot be established by attackers.

## Resource exhaustion

Another evasive approach is to just overwhelm the sensor. Often, attackers simply try to overwhelm the physical device or the staff in charge of monitoring by flooding the device with alarm conditions.

## Cisco Solutions and Products

Cisco offers many products and solutions that address your need for intrusion detection/prevention in your network infrastructure. This *CCNA Security Quick Reference* focuses on Cisco products that can run version 6.0 of the Cisco IPS Sensor Software. This 6.0 version adds many new features, including the following:

- **Virtualization support:** Allowing different policies for different segments that are being monitored by a single sensor.
- **New signature engines:** Additions to cover Server Message Block and Transparent Network Substrate traffic.

- **Passive operating system fingerprinting:** A set of features that enables Cisco IPS to identify the OS of the victim of an attack.
- **Improved risk- and threat-rating system:** The risk rating helps with alerts and is now based on many different components to improve the performance and operation of the sensor.
- **External product interface:** Allows sensors to subscribe for events from other devices.
- **Enhanced password recovery:** Password recovery no longer requires reimaging.
- **Improved Cisco IPS Device Manager (IDM):** New and improved GUI for management.
- **Anomaly detection:** Designed to detect worm-infested hosts.

## Cisco Sensor family

The Cisco Sensor family includes the following devices:

- Cisco IOS IPS
- Cisco IDS Network Module
- Cisco IDS 4215 Sensor
- Cisco IDS 4240 Sensor
- Cisco ASA AIP-SSM
- Cisco IPS 4255 Sensor
- Cisco Catalyst 6500 Series IDSM-2
- Cisco IPS 4260 Sensor

The following legacy devices can also run IPS 6.0 software:

- Cisco IDS 4235 Sensor
- Cisco IDS 4250 XL Sensor

## Sensor Software Solutions

Many options are available for configuration and management of Cisco sensors. Also, the sensor operating systems and overall architecture is worth exploring for the certification exam and beyond.

### IPS Sensor Software architecture

IPS Sensor Software Version 6.0 runs on the Linux OS. The components include the following:

- Event Store (provides storage for all events)
- SSH and Telnet (by default, Telnet is disabled)
- Intrusion Detection Application Programming Interface (IDAPI)
- MainApp
- SensorApp (for packet capture and analysis)
- Sensor interfaces

## Management options

For single-device (element) management, options include the following:

- Command-line interface (CLI)
- Cisco IDM (a graphical user interface)

For multiple-device management (enterprise management), options include the following:

- Cisco IPS Event Viewer
- Cisco Security Manager
- Cisco Security MARS (Cisco Security Monitoring, Analysis, and Response System)

## Network IPS

Network IPS refers to the deployment of devices (typically sensors) in the network that capture and analyze traffic as it traverses the network. Because the sensor is analyzing network traffic, it can protect many hosts at the same time.

## Host IPS

A host IPS solution features software installed on servers and workstations. Note that this solution does not require additional hardware (sensors). The Cisco host IPS is called Cisco Security Agent. It complements network IPS by protecting the integrity of applications and operating systems.

## Deploying Sensors

Technical factors to consider when selecting sensors for deployment in an organization include the following:

- The network media in use
- The performance of the sensor
- The overall network design
- The IPS design (Will the sensor analyze and protect many systems or just a few?)
- Virtualization (Will multiple virtual sensors be created in the sensor?)

Important issues to keep in mind in an IPS design include the following:

- **Your network topology:** Size and complexity, connections, and the amount and type of traffic.
- **Sensor placement:** It is recommended that these be placed at those entry and exit points that provide sufficient IPS coverage.
- **Your management and monitoring options:** The number of sensors often dictates the level of management you need.

Locations that generally need to be protected include the following:

- **Internet:** Sensor between your perimeter gateway and the Internet
- **Extranet:** Between your network and extranet connection
- **Internal:** Between internal data centers
- **Remote access:** Hardens perimeter control
- **Server farm:** Network IPS at the perimeter and host IPS on the servers

## Configuring Cisco IOS IPS Using Security Device Manager (SDM)

Cisco IOS IPS signatures include the following advanced features:

- Regular-expression string pattern matching
- Support for various response actions
- Alarm summarization
- Threshold configuration
- Anti-evasive techniques

To configure IPS using the SDM, choose **Configure > Intrusion Prevention**.

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**.

To view SDEE alarm messages in Cisco SDM, choose **Monitor > Logging > SDEE Message Log**.

To view alarms that are generated by Cisco IOS IPS, choose **Monitor > Logging > Syslog**.