Upon completion of this chapter, you will be able to perform the following tasks:

- Define the major features of Cisco intrusion protection solution
- Identify the different Cisco sensor platforms
- Explain Cisco Threat Response
- Identify the major sensor placement locations
- Explain the sensor deployment considerations

CHAPTER 4

Cisco Intrusion Protection

The Cisco intrusion protection system (IPS) is a comprehensive system that enables you to actively defend your network against network attacks, misuse, and unauthorized access. The system incorporates sensors and agents that perform real-time monitoring of traffic at locations throughout your network, from the network level all the way to the host level. Supporting a large base of sensor types enables you to easily and effectively integrate Cisco intrusion detection system (IDS) into almost any network topology.

Sensors monitor network traffic for alarms in real time through a monitoring interface. All alarms are then retrieved via the command and control interface by your management platform.

When your Cisco IDS analyzes network data, it looks for traffic patterns that represent attacks. Patterns can be as simple as an attempt to access a specific port on a specific host, or as complex as sequences of operations directed at multiple hosts over an arbitrary period of time. Besides relying solely on predefined attack patterns and protocol analysis, some Cisco IDS components are beginning to incorporate anomaly detection to enhance their attack detection capability. Furthermore, the Cisco Threat Response (CTR) product reduces your analysis task by performing intelligent threat investigation on the alarms generated by your Cisco IDS.

This chapter examines the Cisco intrusion protection solution by focusing on the following major topics:

- Cisco IDS solution overview
- Cisco IDS sensors
- Cisco Threat Response
- Cisco sensor management
- Cisco alarm monitoring and reporting
- Deploying Cisco IDS

Cisco Intrusion Detection System (IDS) Solution Overview

Cisco IDS enhances the security of your network by providing a comprehensive solution. Cisco IDS is comprised of various components that each enhance the security of your network. Combined into a single solution, these components secure your network by providing the following:

- Intrusion protection
- Active defense
- Defense in depth

Intrusion Protection

Incorporating intrusion protection into your network enables you to take an active role in defending your network against attack, misuse, and unauthorized access. Intrusion protection provides the following key capabilities:

- Enhanced security over classic solutions
- Advanced technology to meet changing threats
- Increased application attack resistance
- Effective attack mitigation
- Broad network visibility
- Greater protection against published and unpublished threats

Enhanced Security over Classic Solutions

Classic IDS solutions passively monitored the network. These systems generated alarms when intrusive activity was detected, but did not provide a comprehensive security solution. Many of these IDSs were not hybrid systems and focused only on specific aspects of your network as opposed to providing monitoring capabilities for every segment of your network. Cisco IDS provides the capability to easily monitor virtually every segment of your network topology. Along with monitoring every facet of your network, the Cisco IDS solution can respond to attacks by resetting TCP connections and blocking traffic from an offending host. Furthermore, the Cisco Security Agent software can actually prevent attacks against the individual hosts on your network.

Advanced Technology to Meet Changing Threats

The threats against your network are continually changing and evolving. Your IDS must evolve to meet these threats. By incorporating the latest IDS technology, Cisco IDS provides an advanced intrusion detection solution that is capable of addressing the changing threats that your network will face. The incorporation of the Intrusion Detection System Module (IDSM), host-based agents, and CTR are just a few examples of how Cisco is continually adding new technology to their IPS solution.

Increased Application Attack Resistance

Providing multiple layers of defense makes it more difficult for an attacker to gain access to the applications on your network without detection. Host-based agents can even prevent attacks from reaching the applications on your servers and desktop systems. These multiple security barriers increase the attack resistance of the applications on your network.

Effective Attack Mitigation

Cisco IDS provides a variety of signature responses to defend against attacks launched at your network. Combined with easily tunable signatures and multiple signature engines that facilitate the creation of custom signatures, Cisco IDS provides an environment to very effectively mitigate attacks against your network. The responses include the following:

- TCP reset
- Blocking
- IP logging

Broad Network Visibility

Supporting a wide range of sensors, you can deploy Cisco IDS throughout your entire network. These sensors enable you to achieve a very broad view of the activity on your network. By monitoring your network at numerous network segments, the chances of an attacker avoiding detection are greatly minimized.

Greater Protection Against Known and Unpublished Threats

With a signature database of approximately 1,000 signatures, Cisco IDS protects against a wide range of known security vulnerabilities at the network level. Combined with anomalous detection at the host level, Cisco IPS also provides protection against previously unpublished attacks. CTR enhances this protection capability by reducing your alarm analysis through intelligent threat investigation to identify valid attacks against vulnerable targets.

Active Defense

Traditionally, security administrators secured their networks by patching known vulnerabilities and defining security requirements such as password policies. This approach is similar to installing locks on the doors and windows of your house to keep burglars out. The problem with this approach is that it represents a passive approach to security.

Because networks are very dynamic entities, a passive approach to security does not provide enough protection in the constantly changing threat-ridden landscape. The Cisco IPS focuses on the following key components:

- Detection
- Prevention
- Reaction

Detection

Before you can do anything in response to an attack, you must detect that someone is attacking your network. Detection is a crucial component of your active defense because it forms the foundation to your security defenses. You can have a dozen different attack responses, but if an attacker can avoid detection, these responses will never be activated.

Another facet of detection is accurately determining the validity of the attacks being launched against your network. CTR performs intelligent threat investigation to help you determine which attacks are being launched at vulnerable targets along with the likelihood of the attack being successful. Combined with signature responses, you can efficiently protect your network while minimizing the impact on your normal network traffic.

Intelligent Threat Investigation

Many IDS systems generate alarms based solely on known attack traffic. The severity of these alarms is based on the damage that the attack can inflict on your network. Intelligent threat investigation goes beyond this by incorporating other factors into the equation, such as the target operating system, patches installed on the target, and target system analysis. By examining these additional factors, the severity of a specific alarm can be adjusted based on the likelihood of the attack being successful.

Prevention

Prevention comes into play after an attack is detected. Just detecting an attack informs you that someone is potentially attacking your network, but it does not necessarily prevent that attack from causing damage to your network. This is similar to an alarm going off because of a burglar breaking a window. Although the alarm is activated, the burglar might still be able to steal your property before the police arrive. By having an effective prevention capability, you actually prevent the attack from executing. Cisco host-based sensors can prevent intrusive traffic from gaining access to the applications on the servers and desktops throughout your network.

Reaction

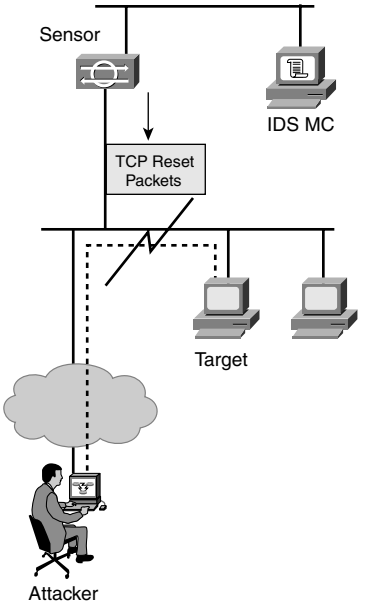
The final component of an active defense is your ability to react to intrusive activity and halt future attacks from a malicious source. One way to protect your network is to continually watch for malicious traffic on your network and then prevent it from causing damage to your network after it has been detected. Using this approach, however, you keep letting the attacker try new attacks against your network until the attacker potentially finds one that succeeds. A more effective approach is to eliminate all traffic from a specific source address when you determine that the source is malicious. By blocking all traffic from the malicious source (the attacker's IP address), you can be confident that the attacker's traffic can't cause further damage to your network.

You can program your sensors to respond in various ways when different attacks are detected. This response is configurable per signature (usually based on the severity of the attack discovered). The possible responses are as follows:

- TCP reset
- Blocking
- IP logging

The Transmission Control Protocol (TCP) reset response essentially terminates the current TCP connection from the attacker by sending a *TCP reset packet* (see Figure 4-1). This response is effective only for TCP-based connections. UDP traffic, for example, is unaffected by TCP resets.

Figure 4-1 *TCP Reset Response*

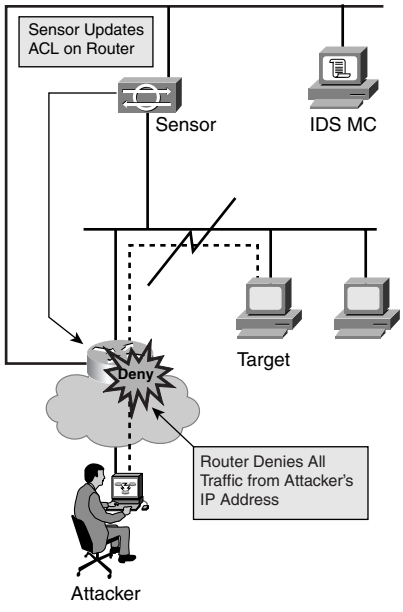


TCP Reset Packet

TCP provides a connection-oriented communication mechanism. The connection is established through a three-way handshake. To terminate a connection, each side of the connection can send a packet with the FIN bit set, signaling the end of the connection. It is also possible, however, for one side of the connection to abruptly terminate the connection by sending a reset packet (packet with the RST flag set) to the other side. The sensor uses this approach to terminate an attacker TCP connection. For a detailed explanation of TCP/IP protocols, refer to *The Protocols (TCP/IP Illustrated, Volume 1)*, by Richard Stevens (Addison-Wesley, 1994).

With the blocking option, the sensor updates the access control lists (ACLs) on one of your routers (or initiates a shun on one of your PIX firewalls) to deny all traffic from the offending IP address (see Figure 4-2). This response prevents the attacker from sending any further traffic into your protected network. (See Chapter 12, "Signature Response" for a detailed description of blocking.)

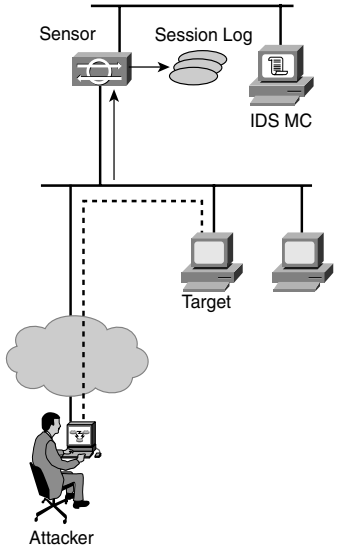
Figure 4-2 *IP Blocking Response*



CAUTION Blocking requires careful review before it is deployed, whether it is used as an automatic response or through operational guidelines for the operators. To implement blocking, the sensor dynamically reconfigures and reloads a Cisco IOS router's ACL (or initiates a shun on a PIX firewall). This type of automated response by the sensor should be configured only for attack signatures with a low probability of false positive detection (or in conjunction with CTR). It is also important not to enable automatic blocking on signatures in which an attacker can easily spoof the source address of the attack. In case of any suspicious activity that does not trigger automatic blocking, you can use the management platform to manually block the attacker. Cisco IDS can be configured to never block specific hosts or networks. This safety mechanism prevents denial-of-service attacks against the Cisco IDS and other critical components.

The third response, IP logging, only records what the attacker is doing (after triggering a signature with logging enabled) in a log file (see Figure 4-3). This option is passive and does not prevent the attacker from continuing the attack. With logging, the actual packets that the attacker is sending are captured on the sensor. You can then examine these packets to determine exactly what traffic the attacker was able to send against your network.

Figure 4-3 *IP Logging Response*



NOTE Do not confuse the traditional alarm logging with IP logging. Whenever a signature is triggered, an alarm event is generated and stored on the sensor. This is known as *alarm logging* and should not be confused with IP logging, which is a configurable alarm response. Alarm logging occurs for every signature that has not been disabled.

Defense in Depth

Any comprehensive security solution needs to contain numerous layers. Breaking through multiple security barriers is definitely harder than having to break through only a single barrier. Cisco IDS protects a broad spectrum of security boundaries by supporting sensors from the host level up through the network level. Some of the major features include the following:

- Application-level encryption protection
- Security policy enforcement (resource control)
- Web application protection
- Buffer overflow detection
- Network attack detection
- Network reconnaissance detection
- Denial-of-service detection
- Multiple monitoring locations

Cisco IDS Sensors

Sensors form the workhorses of your Cisco IDS. They constantly monitor network traffic looking for potential attacks. Each network sensor checks network traffic looking for a match against one of the attack signatures in its signature database. The host-based agents use a behavior-based model to identify traffic that lies outside the traffic considered normal for a given user. The wide variety of sensors enables you to deploy your Cisco IDS to effectively create a robust defense and an in-depth solution to secure your network.

All Cisco IDS network sensors use two types of interfaces:

- Monitoring interface
- Command and control interface

Multiple Monitoring Interfaces

To monitor multiple network segments simultaneously, it is beneficial in some environments to have network sensors support multiple monitoring interfaces (multiple NIC cards). Beginning with Cisco IDS version 4.1, multiple monitoring interfaces are supported. Initially this functionality will be available on the IDS 4215 appliance sensor (the replacement for the 4120 sensor).

The Cisco IDS solution incorporates a wide variety of sensors. These sensors fall into the following categories:

- Network sensors
- Switch sensors
- Router sensors
- Firewall sensors
- Host agents

These different types of sensors also provide different levels of functionality. Table 4-1 outlines the basic capabilities provided by some of the various sensor platforms available for Cisco IDS versions 3.x and 4.x.

Table 4-1 *Sensor Capabilities*

Feature	Appliance Sensor	IDS Module	IDS Network Module
TCP reset	3.x/4.x	4.x	4.x
IP session logging	3.x/4.x	4.x	4.x
Shun/Blocking	3.x/4.x	3.x/4.x	4.x
Active updates	3.x/4.x	3.x/4.x	4.x
Signature language	3.x/4.x	3.x/4.x	4.x
Analysis support	3.x/4.x	3.x/4.x	4.x

Network Sensors

Each network sensor uses at least two network interfaces. One or more of these interfaces monitor network traffic while the other is a command and control interface. All communication with the management platform occurs over the command and control interface. For further information on basic sensor configuration, see Chapter 7, "Cisco IDS Network Sensor Installation."

When network data triggers a signature, the sensor logs the event. Your management platform regularly connects to the sensor to retrieve these events. This pull mechanism prevents the management system from being overwhelmed by a flood of alarm traffic.

NOTE Having the monitoring platform pull the alarm events from the sensor is new to Cisco IDS 4.0. In previous versions, the sensors pushed the alarm events to the monitoring platform. The push technique could lead to missed events if the monitoring platform was temporarily unreachable.

All network sensors are hardware appliances tuned for optimum performance. The hardware, including CPU and memory, for each appliance provides optimal IDS performance, while maintaining ease of maintenance. To protect the sensors, the appliance's host operating system is configured securely. Known security vulnerabilities are patched, and unneeded services are removed.

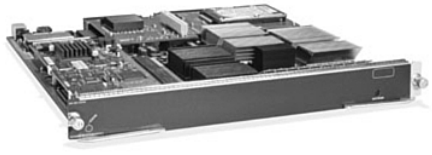
The 4200 series sensors come in six versions: IDS-4210 (being replaced by the 4215), IDS-4220, IDS-4230, IDS-4235, IDS-4250, and IDS-425-XL.

NOTE Although the IDS-4220 and IDS-4230 will operate with the Cisco IDS 4.0 software, these sensor models have reached end of sale (EOS). They are no longer sold and may no longer be supported.

Switch Sensors

The IDS Module (IDSM) for the Catalyst 6500 family of switches is designed specifically to address switched environments by integrating IDS functionality directly into a Catalyst 6500 series switch. The IDSM receives traffic right off the switch backplane, thus combining both switching and security functionality into the same chassis (see Figure 4-4).

Figure 4-4 *Catalyst 6500 IDS Module*



Some of the major features of IDSM include the following:

- Fully integrated line card
- Multi-VLAN visibility
- Full signature set
- Common configuration and monitoring
- No switching performance impact

There are two versions of IDSM. The original version is supported on Cisco IDS version 2.x and 3.x. A second-generation IDSM blade (IDSM-2) is the only version of IDSM that works with Cisco IDS 4.x.

Intrusion Detection System Module (IDSM)

The original IDSM placed a highly functional IDS sensor directly into the network switch, capturing data directly from the switch's backplane. IDSM can process 150 Mb worth of traffic. Similar to the 4200 series sensor, IDSM detects unauthorized activity on the network and sends alarms to your management platform. It does not, however, provide all of the functionality of the appliance sensor because it is based on a different code base.

IDSM is supported in both Cisco IDS versions 2.x and 3.x. It is not, however, supported by Cisco IDS 4.0 and greater.

Intrusion Detection System Module 2 (IDSM-2)

Unlike the original IDSM, IDSM-2 runs the same code that a Cisco IDS 4.x appliance sensor uses. This means that the IDSM-2 provides the identical functionality as the network sensors. The only differentiating factor is the bandwidth that the different network sensors can process. IDSM-2 can process 500 Mb worth of traffic.

For detailed information on configuration of IDSM-2, see Chapter 8, "Cisco IDS Module Configuration."

Router Sensors

Cisco IDS 4.x supports the following two types of router sensors:

- Cisco IOS IDS
- IDS network module

With Cisco IOS-based router sensors, the IDS functionality is incorporated into the actual Cisco IOS Software. This IDS functionality, however, is limited. The IDS Network Module is a card that you install on your router that has all the functionality of a Cisco IDS 4.0 appliance sensor.

Cisco Internetworking Operating System (IOS) IDS

The Cisco IOS-based router sensor integrates intrusion detection into Cisco IOS software. This Cisco IOS IDS can detect a limited subset of attacks compared to the network or switch sensors and is targeted for lower-risk environments. Some of the features of Cisco IOS IDS include the following:

- The latest software release includes 100 signatures.
- Alarms can be sent to a syslog server or PostOffice-aware device.
- Routers can drop packets and terminate TCP sessions in response to attacks.

If you want to use a Cisco IOS-based device to perform intrusion detection, your Cisco IOS device must meet the following software and hardware requirements:

- IOS Software Release 12.0(5)T or higher
- 1700, 2600, 3600, 3700, 7100, 7200, and 7500 series routers and the Catalyst 5000 series Route Switch Module (RSM)

NOTE The original IDS functionality in Cisco IOS provided 59 signatures. With Cisco IOS Release 12.2(15)T, the number of signatures increases to 100.

IDS Network Module

The IDS Network Module incorporates the existing appliance sensor code base into a router's network module card. This provides a unique form factor to deploy Cisco IDS sensors on your existing infrastructure equipment. Because it runs the same code base as the appliance sensor, it offers the same management options, and provides a fully functional IDS sensor at a competitive price.

If you want to use an IDS Network Module to perform intrusion detection, your IOS device must have an available slot and be one of the following hardware platforms:

- 2600XM
- 2691
- 3660
- 3725
- 3745

Firewall Sensors

The firewall sensor integrates IDS functionality into the PIX firewall. Like the Cisco IOS-based IDS sensor, the PIX IDS functionality is limited compared to a network or switch sensor. The PIX IDS functionality is intended to add an extra measure of protection for lower-risk environments. Some of the features of the firewall sensor include the following:

- The latest software release includes 55 signatures.
- Alarms can be sent to syslog server.
- It can drop packets and terminate TCP sessions in response to attacks.

If you want to use a firewall sensor to perform intrusion detection, your firewall must meet the following software and hardware requirements:

- PIX firewall 5.2 or higher
- PIX firewall 506E, 515E, 525, and 535

Host Agents

To provide a comprehensive IDS solution, Cisco IDS provides sensors that you can deploy throughout your network. Agents at the host level provide a key component to this solution.

Originally, Cisco host-based agents used Entercept (based on a system call interception technique) provided through a partner agreement with Entercept Security Technologies. This capability has since been replaced by the acquisition of Okena and their Stormwatch product. The current host-based solution (Cisco Security Agent) uses a behavior-based approach to provide a valuable new addition to Cisco IDS functionality.

Cisco Threat Response

Common drawbacks to many IDS systems are the time and resources required to investigate the multitude of alarms representing possible attacks. Network-level sensors trigger alarms based on known attack signatures. These network sensors, however, can't determine whether the attack will succeed against its intended target. (For instance, the host might be patched against the given attack.) Analyzing *false alarms* wastes your valuable and limited security resources.

False Alarm

When an attack is launched against a system that is not vulnerable to the exploit being used, it is known as a false alarm. A common type of false alarm is running a Windows exploit against a Linux system. Many attacks are OS-specific because the vulnerabilities are related to unique OS characteristics. Running one of these attacks against another OS will not produce the same results as running it against the correct OS. Another type of false alarm is attacking the correct OS when the OS has been patched against the attack being used.

CTR enables you to identify false alarms. After eliminating false alarms through its analysis, CTR can vary the severity of alarms that represent actual attacks against valid targets. For instance, you might set the default severity of an alarm to low. Then, when CTR locates an instance of this alarm that is not a false alarm, it can increase the severity of the alarm generated to high to indicate that the attack is being launched against a vulnerable target.

NOTE Currently, CTR and the sensor are not tightly integrated (meaning that the sensor generates an alarm, CTR modifies its severity, and then this modified alarm is retrieved by your monitoring software). Instead, your monitoring console and CTR both retrieve alarm information from your sensor. Then, CTR updates the severity of the alarms that it receives based on its analysis, but does not change the severity of the alarms retrieved directly from your sensor by your monitoring software.

Cisco Sensor Management

You may deploy multiple types of Cisco IDS sensors on your network to provide complete IDS coverage. Manually monitoring the alarms on each of these sensors is inefficient. The management and monitoring platforms provide the software interface necessary to configure, log, and display alarms (generated by your sensors) to effectively use your Cisco IDS to protect your network from attack. Furthermore, a single management system can

consolidate all the alarms from multiple sensors into a single user-friendly interface. Cisco IDS provides the following management and monitoring options:

- Cisco Intrusion Detection Manager (IDM)
- Cisco IDS Event Viewer (IEV)
- Cisco IDS Management Center (IDS MC)
- Cisco IDS Security Monitor
- Cisco Secure Policy Manager (IDS version 3.x only)
- Cisco Intrusion Detection Director (IDS version 3.x only)

NOTE This book does not provide information on Cisco Secure Policy Manager (CSPM) or Cisco Intrusion Detection Director (CIDD) because the focus here is mainly on Cisco IDS 4.x. These management platforms were described in detail in my previous book on Cisco IDS, *Cisco Secure Intrusion Detection System* (Cisco Press, 2001). These platforms are not supported with Cisco IDS version 4.x.

Cisco IDS 4.0 supports two graphical sensor management platforms:

- Cisco IDS Device Manager
- Cisco IDS Management Center

NOTE Cisco IDS 4.x sensors also support a command-line interface that you can use to configure your Cisco IDS sensor. This command line is similar to the Cisco IOS command line that you use to configure Cisco routers. For more information on the command-line interface, see Chapter 7.

Cisco IDS Device Manager

Beginning with Cisco IDS version 3.1, you could manage your network sensors using a web-based interface. The Cisco IDS Device Manager (IDM) enables you to manage a single network sensor via an easy-to-use, graphical, web-based interface.

The following web browsers are compatible with IDM:

- Netscape (version 4.79 or later)
- Internet Explorer (version 5.5 Service Pack 2 or later)

NOTE Although other web browsers can work with IDM, Cisco has only tested and verified two browsers (Netscape and Internet Explorer).

Cisco IDS Management Center

Managing your network sensors individually using IDM can be time-consuming if you have a large number of sensors deployed on your network. To manage larger numbers of network sensors, you can use Cisco IDS Management Center (IDS MC). This product enables you to manage up to 300 sensors across your network from a single management system (via a series of web-based screens).

IDS MC is a component of the CiscoWorks2000 VPN/Security Management Solution (VMS) product. You can deploy IDS MC in the following operating environments:

- Windows 2000 Server (Service Pack 3)
- Windows 2000 Professional (Service Pack 3)
- Solaris (version 2.8)

Cisco Alarm Monitoring and Reporting

Cisco IDS version 4.x supports two mechanisms to analyze the alarms generated by your network-based sensors:

- Cisco IDS Event Viewer
- Cisco IDS Security Monitor

Cisco IDS Event Viewer

Before Cisco IDS version 3.1, your only way to effectively analyze IDS alarms was through a director platform, such as CSPM or IDD. Cisco IDS version 3.1 introduced the Cisco IDS Event Viewer (IEV). IEV is a software application provided with your sensor that enables you to analyze the alarm traffic for up to five network sensors.

You can install IEV on the following two platforms:

- Windows NT 4 Service Pack 6
- Windows 2000 Service Pack 2

Cisco IDS Security Monitor

The Security Monitor is a component of the CiscoWorks2000 VMS product. Unlike IEV, Security Monitor enables you to consolidate events from up to 300 IDS devices.

Deploying Cisco IDS

One of the keys to successfully deploying Cisco IDS to protect your network involves understanding how to effectively deploy intrusion detection sensors throughout your network. The major factors impacting your placement of IDS sensors are as follows:

- Sensor selection
- Sensor placement
- Sensor deployment considerations
- Sensor deployment scenarios

Sensor Selection

Many factors will affect your decision on which Cisco IDS sensors to use throughout your network. Political, financial, and technical issues will impact your sensor selection. Political and financial issues are beyond the scope of this book so this section focuses on the technical factors that you need to consider when choosing Cisco IDS sensors to deploy on your network. You need to consider the following technical factors when choosing sensors:

- Network media
- Performance of intrusion detection analysis
- Network environment

Network Media

To capture network traffic on your network, your Cisco IDS appliance sensors use a NIC. This NIC must match the network media in use on your network. Cisco IDS supports the following common network media types:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet

NOTE The Gigabit Ethernet support is provided through both fiber (1000BASE-SX) as well as copper interfaces (10/100/1000BASE-TX).

Performance of Intrusion Detection Analysis

As your Cisco IDS sensor captures traffic, it must have enough processing power to analyze that traffic for intrusive activity. The performance of a sensor is rated by the amount of data per second that the sensor can capture and accurately analyze. Cisco provides sensors that have performance ratings from 45 Mbps to 1 Gbps. Cisco IDS provides the high-performance sensors, shown in Table 4-2.

Table 4-2 *Network Sensor Performance Ratings*

Sensor	Performance
IDS Network Module	45 Mbps
IDS 4215	80 Mbps
IDS 4235	250 Mbps
IDS 4250	500 Mbps
IDSM-2	600 Mbps
IDS 4250XL	1000 Mbps

Network Environment

The final factor impacting your sensor selection is your network environment. Different Cisco IDS sensors can handle various traffic loads. Cisco IDS sensors support the following network environments:

- Single T1/E1 environment
- Switched environment
- Multiple T3/E3 environment
- OC-12 environment
- Gigabit environment

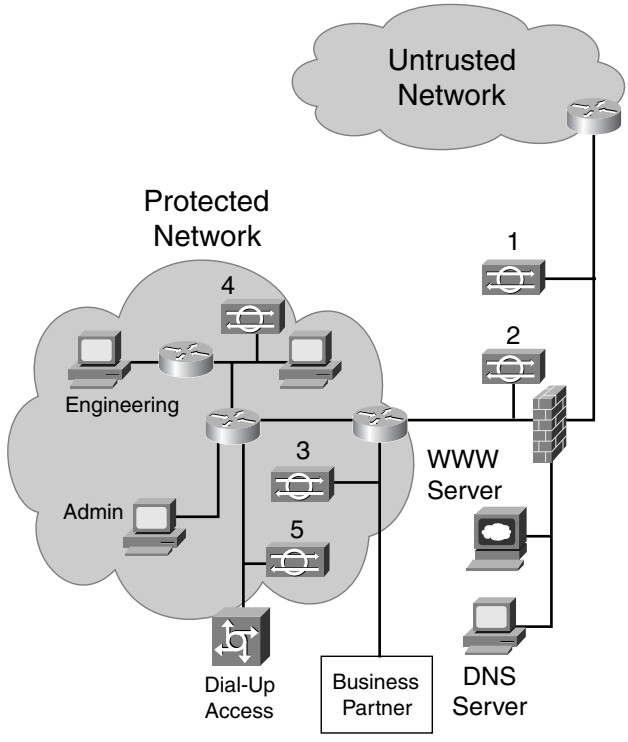
Sensor Placement

Cisco IDS supports a variety of different sensor platforms. Each of these platforms has varying capabilities and is designed to operate in a specific network environment. You need to consider the following factors when deciding where to place sensors on your network:

- Internet boundaries
- Extranet boundaries
- Intranet boundaries
- Remote-access boundaries
- Servers and desktops

Figure 4-5 shows a sample network with IDS sensors monitoring key functional boundaries in the network.

Figure 4-5 *Deploying Sensors at Common Functional Boundaries*



By carefully analyzing your network topology, you can identify the locations at which you want your Cisco IDS to monitor the traffic flow. Then you can determine which Cisco IDS sensor is appropriate for each monitoring location that you have identified.

Internet Boundaries

Sensor 1 in Figure 4-5 monitors the perimeter of the network. All traffic traveling to and from the untrusted network is visible to this sensor. In most networks, the perimeter protection refers to the link between your network and the Internet. Instead of monitoring the traffic outside the firewall, Sensor 2 examines only the traffic that actually passes through the firewall. This can reduce the amount of traffic that the sensor needs to process.

NOTE Be sure to locate all Internet connections to your network. Many times, administrators forget that remote sites contain Internet connections. Sometimes, departments within your network have their own Internet connection (separate from the corporate Internet connection). Any connection to the Internet needs to be properly monitored.

Extranet Boundaries

Sensor 3 in Figure 4-5 is positioned so that it can monitor the traffic traversing the link between your network and your business partner's network. This extranet link is only as strong as the security applied to both of the networks that it connects. If either network has weak security, the other network becomes vulnerable as well. Therefore, extranet connections need to be monitored. Because the IDS sensor monitoring this boundary can detect attacks in either direction, you might consider sharing the expense of this sensor with your business partner.

Intranet Boundaries

Sensor 4 in Figure 4-5 monitors traffic between the engineering network and the finance network. This is an example of a sensor monitoring traffic between separate network segments within your network. Many times, you use intranets to divide your network into functional areas, such as engineering, research, finance, and human resources. At other times, organizations drive the boundary definitions. For instance, a company might be divided into several product or business units. Each of these business units can in turn also have functional boundaries such as engineering and research. Sometimes, both of these classifications define intranet boundaries.

In this example, the engineering network is separated from the finance network (and the router that separates the other networks) by its own router. For more protection, a firewall is also commonly used. In either situation, you can use a sensor to monitor the traffic between the networks and verify that the security configuration (for the firewall or router) is defined correctly. Traffic that violates the security configuration generates IDS alarms, which you can use as a signal to update the configuration of the firewall or router because it is enforcing the security policy.

Remote-Access Boundaries

Sensor 5 in Figure 4-5 monitors traffic coming from the dialup access server. Numerous war dialers are freely available on the Internet. Therefore, do not think that dialup lines are safe by assuming a hacker cannot determine the phone numbers of your dialup modems. Some common war dialers include the following:

- **Toneloc**—http://www.securityfocus.com/tools/48
- **Modem Finder**—http://packetstormsecurity.org/Win/mfsetup.zip

NOTE Modems installed on desktop systems also represent a risk to your network. Attacks against these modems will not be detected by your network-based IDS.

Threats Posed by War Dialers

A *war dialer* is a tool that dials a specified range of phone numbers looking for modem connections. An attacker can start a war dialer on the computer and let it run for days, attempting to locate potential modem connections. Later, the attacker attempts to connect to the phone numbers that are listed as modems from the output of the war dialer program. If any of these modem connections has weak authentication mechanisms, the attacker easily infiltrates the network.

Many remote users also use home computers that are continuously connected to the Internet through high-speed Internet connections. If an attacker compromises one of these home systems, it can easily lead to an attack through your remote-access server.

Servers and Desktops

The current Cisco host-based agents enable you to deploy intrusion detection protection on your servers and desktop systems. Each host-based agent is actually a software application that runs on the individual systems on your network, serving as a security barrier around that individual host. These agents provide a final security blanket that can help protect your network from attack. These agents, like the network sensors, can report events to a centralized monitoring center.

Sensor Deployment Considerations

Deploying Cisco IDS on your network requires a well-thought-out design to maximize its effectiveness. Besides the basic sensor capabilities and placement, you must also consider the following important design issues when deploying Cisco IDS on your network:

- Sensor management
- Number of sensors
- Database management
- Software updates

NOTE The use of encrypted protocols can also impact the deployment of your network sensors. If you use virtual private networks (VPNs), for instance, you need to place your network sensors after the VPN traffic is unencrypted. Otherwise, attacks can go unnoticed in the encrypted data stream.

Sensor Management

Each of your Cisco IDS sensors is monitoring network traffic at a specific location in your network. You must also, however, be able to communicate with your sensors using their command and control interface. This communication path enables you to configure and manage your sensors, as well as retrieve alarm events for monitoring and reporting. Cisco IDS 4.0 uses a communication protocol that uses Transport Layer Security (TLS) / Secure Sockets Layer (SSL) and Extensible Markup Language (XML) to provide a standardized interface between devices. You have two options with respect to your sensor management:

- Out-of-band management network
- In-band management network

An out-of-band management network isolates the management traffic on a separate network. This isolation minimizes the chances of an attacker attacking your management systems, because the separate network contains only management traffic. With an in-band management system, access to the management systems is performed through the normal data network. In this situation, access to the management systems is usually limited to specific hosts using access controls on the systems being managed. Although an in-band management network is harder to secure, it is still commonly used.

Number of Sensors

The number of sensors that you plan to deploy on your network dictates how many management consoles that you need to deploy to configure and manage your Cisco IDS sensors. Each management solution is designed to effectively manage a specific number of sensors. The current two management solutions for Cisco IDS 4.0 are as follows:

- IDS Device Manager (IDM)
- IDS Management Center (IDS MC)

IDM enables you to configure a single sensor. This software is provided with Cisco IDS sensors that provide full IDS functionality. IDS MC, on the other hand, enables you to configure up to a maximum of 300 sensors from one management and monitoring system. The effective ratio depends on the number of alarms generated by your sensors. In normal operation, a more realistic ratio is probably in the range of 20 to 30 sensors per monitoring system.

Along with the actual management software, the number of sensors that you deploy on your network dictates the number of personnel that you need to employ to effectively manage your Cisco IDS devices.

Database Management

Your management system stores your sensor configuration information, along with event data from all of your sensors. You have a fixed amount of space on your management system database. Therefore, you need to determine how many days' worth of alarm data you can maintain on your management system without needing to archive the information out of your main system database. Periodically, you need to move these archive files to another system. When you know the frequency at which you need to back up your event data, you can then decide on an appropriate schedule to perform the data archival and backup.

Software Updates

New signatures are continually being added to Cisco IDS. It is vital that you have a well-defined plan on how to regularly update the software on your Cisco IDS devices. Some of the main questions that you need to consider include the following:

- How frequently are signature updates released?
- How frequently are software updates released?
- Where will the updates be stored locally?
- How will the updates be rolled out?

Sensor Deployment Scenarios

All the points where data enters your network represent potential locations at which an attacker can gain access to your network. You need to verify that each entry point is adequately monitored. Not monitoring an entry point into your network allows an attacker to penetrate your network undetected by your IDS. Common entry points into most networks that require protection include the following:

- Internet
- Extranet
- Intranet
- Remote access
- Server farm

Internet Protection

Your network's Internet connection makes your network visible to the entire Internet. Attackers worldwide can attempt to gain access to your network through this entry point. With many corporate networks, access to the Internet is directed through a single router. This device is known as a *perimeter router*. By placing a sensor behind this device, you can monitor all traffic (including attacks) destined for your corporate network. If your network contains multiple perimeter routers, you might need to use multiple sensors, one to watch each Internet entry point into your network.

NOTE Current estimates project that 171 million hosts are connected to the Internet, with more than 665 million Internet users worldwide. Any of these users can potentially attack your network through your Internet connection. (Sources are "Internet Domain Survey Number of Hosts," by the Internet Software Consortium, http://www.isc.org/ds/host-count-history.html; and "USA Tops 160M Internet Users," by Computer Industry Almanac Inc., http://www.c-i-a.com/pr1202.htm.)

Extranet Protection

Many corporate networks have special connections to business partners' networks. Traffic from these business partners' networks does not always travel through your network's perimeter device; therefore, it is important to make sure that these entry points are also monitored effectively. These connections have an implied level of trust, but that trust can't be assured. By penetrating your business partners' networks, an attacker can use the extranet to infiltrate your network. You usually have little or no control over the security of your business partners' networks. Furthermore, if an attacker penetrates your network and then uses the extranet link to attack one of your business partners, you are faced with a potential liability issue.

Intranet Protection

Intranets represent internal divisions within your network. These divisions might be organizational or functional. Sometimes, different departments within your network require different security considerations, depending on the data and resources that they need to access or protect. Usually, these internal divisions are already separated by a firewall, signaling different security levels between the different networks. Other times, the network administrator uses ACLs on the router between network segments to enforce separate security zones. Placing a sensor between these networks (in front of the firewall or router) enables you to monitor the traffic between the separate security zones and verify compliance with your defined security policy.

Sometimes you also might want to install a sensor between network segments that have complete access to each other. In this situation, you want the sensor to monitor the types of traffic between the different networks, even though by default you have not established any physical barriers to traffic flow. However, any attacks between the two networks are quickly detected.

Remote-Access Protection

Most networks provide a means to access the network through a dialup phone line. This access allows corporate users to access network functionality, such as e-mail, when away from the office. Although this enhanced functionality is useful, it also opens up another avenue for an attacker to exploit. You probably need to use a sensor to monitor the network traffic from your remote-access server, just in case an attacker can defeat your remote-access authentication mechanism.

Many remote users use home systems that connect continuously through high-speed Internet connections, such as cable modems. Because these systems are usually minimally protected, attackers frequently target and compromise these home systems, which might also lead to a compromise of your remote-access mechanism. Other times, stolen laptops reveal a wealth of information on how to access your network. Therefore, even if you trust your users and remote-access mechanisms, it is beneficial to monitor your remote-access servers with IDS.

Desktop and Server Protection

Monitoring and protecting the various boundaries on your network is crucial to developing a strong security solution. The majority of the attacks currently available are written to exploit vulnerabilities in the common host operating systems, so the final security barrier is actually the hosts on your network. Cisco host-based agents enable you to monitor and protect traffic at the individual operating system level on all the hosts on your network.

Summary

Cisco IDS is a comprehensive IPS that uses signatures, protocol analysis, and anomaly detection to trigger intrusion alarms. It supports sensors from the network level all the way through the host level. Besides detecting intrusive traffic, Cisco IDS provides an active defense that focuses on the following three factors:

- Detection
- Prevention
- Reaction

Deploying sensors at multiple locations throughout your network enables you to develop a strong defense in depth solution. Besides detecting intrusive activity, sensors can also respond to attacks through the following three mechanisms:

- TCP reset
- Blocking
- IP logging

Cisco IDS sensors represent the eyes of your security solution. The more eyes that you have looking at your network, the less likely that it is that an attack will be able to sneak through your network undetected. You can deploy the following type of sensors throughout your network:

- Network sensors
- Switch sensors
- Router sensors
- Firewall sensors
- Host agents

Each sensor has a monitoring interface and a command and control interface. Using the monitoring interface, the sensor compares network traffic against the signatures in its signature database. If unauthorized activity is detected, your management system uses the sensor's command and control interface to communicate with the sensor and retrieve alarm events. Cisco IDS supports many different sensor platforms. The three sensors based on the Cisco IDS 4.0 appliance sensor code base are as follows:

- 4200 series appliance sensors
- IDSM-2
- IDS Network Module

The 4200 series sensors are PC appliances that can be placed at various locations throughout your network. The 4200 series sensors come in six varieties: IDS-4210 (to be replaced by the IDS 4125), IDS-4220, IDS-4230, IDS-4235, IDS-4250, and IDS-425-XL.

NOTE The IDS-4220 and IDS-4230 have reached end of sale. They are no longer sold and may no longer be supported.

IDSM is an actual integrated line card that operates directly on the Catalyst switch. It receives packets directly from the switch's backplane. The switch's performance is not

impacted, however, because the IDSM operates on copies of the network packets. With the second generation of IDSM (IDSM-2), this sensor runs the same code base as the appliance sensors. This makes both sensor platforms equal in functionality. Only IDSM-2 is supported by Cisco IDS 4.0 and greater.

The final Cisco IDS sensor based on the Cisco IDS 4.0 appliance sensor code base is the IDS Network Module. This sensor is a network module (card) that you insert into your router (similar to the IDSM being used in your Catalyst 6000 series switch).

To configure your sensors, you need to use some type of management platform. Cisco IDS 4.x supports the following two management platforms:

- IDS Device Manager (IDM)
- IDS Management Center (IDS MC)

IDM enables you to configure a single sensor. If you deploy many sensors on your network, IDM is not an effective solution. IDS MC enables you to manage up to 300 sensors from a single management system.

After configuring your Cisco IDS sensors, you also need a mechanism to view the alarms generated by your sensors. Cisco IDS 4.x supports the following two reporting and monitoring platforms:

- IDS Event Viewer (IEV)
- IDS Security Monitor

IEV enables you to monitor up to five sensors and is designed for small sensor deployments. If your Cisco IDS uses more sensors, you can use the Security Monitor product to monitor up to 300 sensors.

When deploying your Cisco IDS solution, you must consider the following major factors:

- Sensor selection
- Sensor placement

Some other considerations that you need to analyze include the following factors:

- Sensor management
- Number of sensors
- Database management
- Software updates

Finally, to be a true comprehensive security solution, your Cisco IDS needs to monitor the various boundaries on your network. Watching the multiple boundaries throughout your

network reduces the risk of an attacker sneaking through your defenses undetected. Your Cisco IDS needs to provide protection at the following areas on your network:

- Internet protection
- Extranet protection
- Intranet protection
- Remote-access protection
- Desktop and server protection

Review Questions

The following questions test your retention of the material presented in this chapter. The answers to the review questions are in Appendix B, "Answers to Chapter Review Questions."

1. What are the two monitoring and reporting options available with Cisco IDS version 4.0?
2. What are the two programs that you can use to configure and manage your sensors with Cisco IDS version 4.0?
3. How many different types of sensor platforms are supported by Cisco IDS?
4. Which 4200 series sensors can process the most traffic?
5. What are the three types of responses that a sensor can perform in reply to an attack?
6. What is IDSM?
7. What is Cisco Threat Response?
8. What is a false alarm?
9. Where are the common network boundaries at which you need to deploy Cisco IDS sensors?
10. How many sensors can be managed by IDS MC?
11. You can use IEV to view the alarms from how many sensors?
12. If you are going to deploy 100 Cisco IDS sensors on your network, what management solution would you probably use?
13. If your Cisco IDS solution consists of two sensors, what monitoring and reporting tool would you probably use?

14 Cisco IDS provides an active defense for your network that focuses on what three factors?

15 What is IP logging?

16 How does the TCP reset response work?