About This Guide

This preface includes the following sections:

- Document Objective
- Audience
- Document Organization
- Document Conventions
- Cisco Connection Online
- Cisco Documentation CD-ROM

Document Objective

This guide describes intrusion detection technology and provides basic design considerations and scenarios for deployment.

Audience

The information in this guide is meant for system administrators or network security personnel that wish to learn more about intrusion detection and how to deploy it successfully in various network environments.

Document Organization

This guide is organized into the following chapters and appendixes:

- Chapter 1, "Introduction," provides background information on intrusion detection.

- Chapter 2, "Design Considerations," provides general information on network design considerations when implementing intrusion detection.

- Chapter 3, "Scenarios," provides various scenarios for deploying intrusion detection in different network environments.

- Appendix A, "Resources and Recommended Reading," provides a listing of printed and online resources on intrusion detection.

Document Conventions

This guide uses the following conventions:

- Important terminology, and variable input for commands is shown in *italics*.

- Command names, buttons, and keywords are shown in **boldface**.

- Examples depict screen displays in `screen` font.

- Information you need to enter in examples is shown in **`boldface screen`** font.

- Variables for which you must supply a value are shown in *`italic screen`* font.

- Choosing a menu item is indicated by the following convention:

    Click **Show>Context** on the **Security** menu.

Note   Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO services a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Cisco Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or an annual subscription. You can also access Cisco Documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Introduction

This chapter contains the following sections:

- Defining the Need for Intrusion Detection
- What is Intrusion Detection?
- Intrusion Detection as a Complementary Technology
- Cisco Intrusion Detection Product Overview

Defining the Need for Intrusion Detection

Without a doubt, cyberspace attacks have grabbed lots of headlines.

According to usnews.com, the online version of *U.S. News and World Report*, the past twelve months have seen dozens of hacks perpetated against high-profile targets, including newspapers, telephone companies, Internet startups, computer hardware manufacturers, and even government agencies. In 1997 an East Coast hacker disabled operations at a regional telephone utility and radio transmissions at a local airport. Dozens of other cases involve disgruntled employees inflicting major damage to their former employer's proprietary data and hardware.

These attacks are perpetated for a variety of reasons, including extortion, fraud, espionage, sabotage, or mere curiosity. The acts themselves can involve a range of activity, including misuse of authorized systems, system break-ins, equipment theft, interception of network traffic, and reconfiguration of victim systems to allow future access. Because of the nature of global networks, these attacks can (and often do) cross network and national boundaries.

To counter these security threats, various commercial vendors have brought security products to the market, such as firewalls, encryption and authentication, and access control lists. These products, although providing a certain measure of security, contain certain limitations that may allow attackers to get past them.

Complex security threats require complex security countermeasures, so there is a definite need for a complementary security technology, one that:

- Can intelligently monitor the network for ongoing, real-time intrusions

- Can be reconfigured easily and dynamically in response to intrusions

- Can respond to intrusions in a variety of user-configurable ways

The technology previously described is known as intrusion detection. The remainder of this guide provides background information, design considerations, and scenarios for deploying intrusion detection systems.

What is Intrusion Detection?

Intrusion detection, put simply, is the ability to analyze data in real time to detect, log, and stop misuse or attacks as they occur. In practice, intrusion detection is more complex than this simple definition, and various types of intrusion detection systems (IDSs) go about their activity in different ways.

Host-based IDSes, for example, are used to secure critical network servers or other systems containing sensitive information. In a typical implementation, agents are loaded on each protected asset (see Figure 1-1). These agents make use of system resources—disk space, RAM, CPU time—to analyze operating system, application, and system audit trails. The collected information is compared to a set of rules to determine if a security incident has occurred. These agents are tailored to detect host-related activity and can track these types of events with a fine degree of granularity (for example, which user accessed which file at what time).

Host-based agents can be self-contained, sending alarm information to the local console, or remotely managed by a manager/collector that receives periodic updates and security data. A host-based implementation that includes a centralized management platform makes it easier to upgrade the software. These systems are ideal if a limited number of critical systems need protection, and are complementary to *network-based IDSes*, but they do not scale well if an enterprise-wide solution is needed.

Figure 1-1   Host-based IDS Agents Deployed on a Network
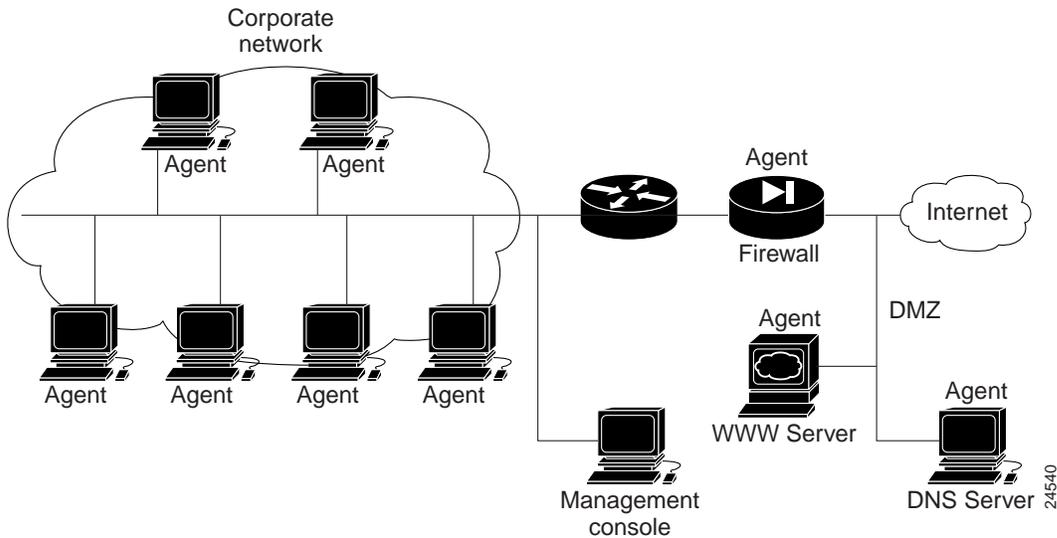
Network-based IDSes monitor activity on a specific network segment. Unlike host-based agents, network-based systems are usually dedicated platforms with two components: a sensor, which passively analyzes network traffic, and a management system, which displays alarm information from the sensor and allows security personnel to configure the sensors (see Figure 1-2). Implementations vary: some vendors sell separate sensor and management platforms; others offer a self-contained sensor/manager.

The sensors in a network-based IDS capture network traffic in the monitored segment and perform rules-based or expert system analysis of the traffic using configured parameters. The sensors analyze packet headers to determine source and destination addresses and type of data being transmitted, and analyze the packet payload to discover information in the data being transmitted. Once the sensor detects misuse, it can perform various security-related actions: log the event, send an alarm to the management console, reset the data connection, or instruct a router to shun (deny) any future traffic from that host or network.

Figure 1-2   Typical Network-based IDS Deployment
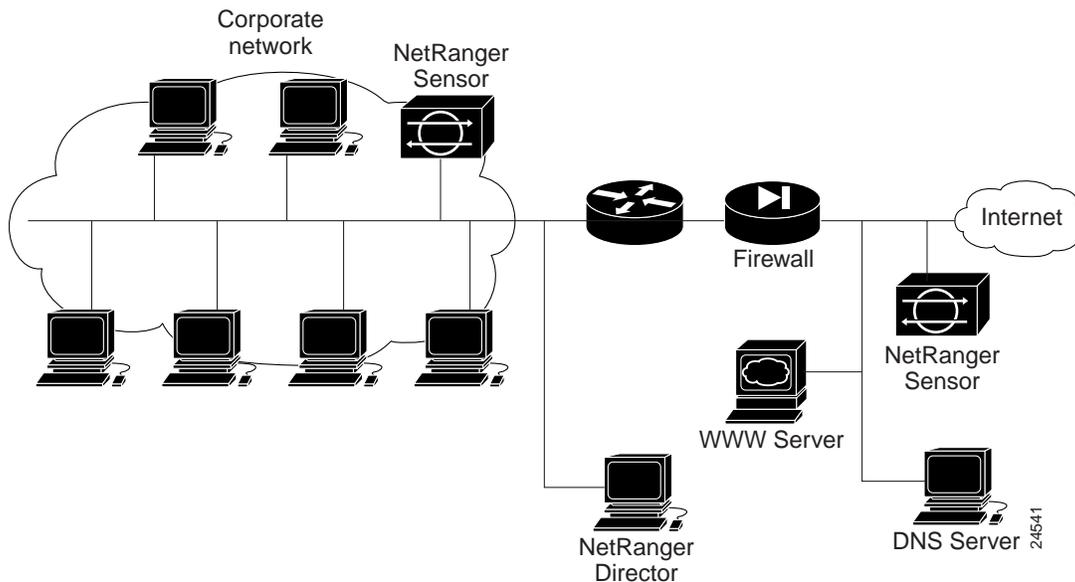
Note   Because Cisco offers network-based IDSes, the remainder of this guide will focus on network-based intrusion detection methodology and practices.

The types of rules that an IDS uses to detect misuse can vary, but there are two primary ways of detecting misuse: profile-based and signature-based detection.

Profile-based detection (also known as *anomaly-based detection*) involves building statistical profiles of user activity and then reacting to any activity that falls outside these established profiles. A user's profile can contain attributes such as files and servers frequently accessed, time spent logged onto the network, location of network access, and so forth.

There are two major hurdles that so far have kept profile-based detection an impractical, cost-prohibitive solution. First, users change the way they use the network on a regular basis. Projects begin and end, employees are transferred to other departments, or they go on the road or work from home, thus changing their point of entry into the network. Second, there is as yet no cost-effective way to build a sensor with enough memory and processing power to maintain even a small percentage of the ever-changing user profiles. Thus, due to current limitations on memory and processing power, profile-based intrusion detection often leads to a large number of *false positives*, or alarms deriving from non-threatening events.

Signature-based detection, on a very basic level, can be compared to virus checking programs. Vendors produce a list of *signatures* that the IDS uses to compare against activity on the network or host. When a match is found, the IDS takes some action, such as logging the event or sending an alarm to a management console. Although many vendors allow users to configure existing signatures and create new ones, for the most part customers are dependent on vendors to provide the latest signatures to keep the IDS up to date with the latest attacks.

Signature-based detection can also produce false positives, as certain normal network activity can be construed as malicious. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system may interpret as an attempt by an attacker to map out a network segment.

Chapter 2, "Design Considerations," provides more information on analyzing users and traffic patterns, as well as other network considerations, which should help minimize false positives.

Intrusion Detection as a Complementary Technology

As stated previously, intrusion detection technology is a complimentary tool that can be used alongside traditional security products. In other words, intrusion detection is another part of the total end-to-end security solution. How do IDSes compare with other security products? This section discusses the following types of products and how IDSes can complement them:

- Firewalls

- Encryption and Authentication

- Access Control Lists

Firewalls

Firewalls, one of the most popular security products, are based on the customer defining a very comprehensive policy (authorized traffic flows and services) that is enforced by the firewall. Generally speaking, there are two types of policies:

1 That which is not specifically authorized is denied.

2 That which is not specifically denied is authorized.

The first type of policy is by far the most prevalent, but it requires that the customer know the risks involved before authorizing services to pass through the firewall. For instance, if the firewall allows Web traffic to pass, then an attacker can send a command that exercises a buffer overflow in the web browser application. The firewall will not stop these packets from reaching the victim system.

IDS vendors, on the other hand, research and define the vulnerabilities inherent in different types of services. In the previous example, a countermeasure that detects the buffer overflow command on specific types of traffic (TCP port 80, for example) could be developed and deployed in a matter of hours.

Another difference between IDSes and firewalls is their impact on network performance. Firewalls typically are used as access control devices on a network, and could impact throughput on a local link. IDSes are typically passive monitors; a few, like Cisco's IOS IDS implementation, are inline devices that inspect packets as they cross a router's interface.

One way to effectively use firewalls and IDSes together is to place the IDS sensor in the *demilitarized zone* (DMZ), in front of the firewall. In the DMZ, the sensor monitors all traffic that enters and leaves the protected network. The sensor can detect attacks that may be of interest to the organization, such as competitors trying to map the network. Another scenario involves placing the sensor inside the firewall, and connecting it to the protected LAN. The firewall can then protect the perimeter, and the IDS sensor monitors internal users and acts as a verifier of firewall policies.

These and other scenarios are covered in Chapter 3, "Scenarios."

Encryption and Authentication

Encryption and *authentication* are also very popular and very effective ways to secure information and resources. However, each of these has associated problems that keep them from being the end-all be-all security solution.

Encryption provides point-to-point confidentiality of data. The points involved can be client-to-client, client-to-server, or router-to-router. The data on any given network segment can be bulk-encrypted—in other words, every packet between the end points is encrypted—or encrypted by session.

For example, a web server on an e-commerce site might be configured to allow customers to enter confidential information (credit card numbers and other personal data) via an SSL (Secure Socket Layer) session. At the same time, there might be thousands of customers merely browsing the online catalog, an activity that does not require encryption.

In this situation, the web site's data and hard disk are both unprotected because only the user sessions are encrypted. Once the data from these sessions is stored on the server (such as in a database) it is stored in an unencrypted manner. An attacker could conceivably find a vulnerability in the web server that would allow access; once logged on, the attacker could browse the confidential consumer information without any roadblocks. No one would be the wiser.

Of course, an attacker may not be interested in browsing the data, but in erasing it or shutting down the server (the latter is termed a *denial-of-service attack*). In either case, even host-based encryption schemes protecting the server's data would be unable to prevent this activity.

Authentication schemes are in wide use in these security-conscious days. Just about every machine on the network requires a user to log on and provide a password. However, this requirement cannot protect against users creating weak or easily guessed passwords. Furthermore, some attackers can bypass the authentication safeguard and install services on a system that give them future uncontested access.

Although IDSes normally are not used to enforce authentication or encryption schemes, they would be able to detect many of the common attacks used by the hacker community to exploit network server vulnerabilities. The attempts to break in to a server would trigger an alarm, alerting security personnel that some malicious activity is going on.

Access Control Lists

Access control lists, or sets of rules that routers and firewalls use to permit or deny certain traffic, are an effective measure against unauthorized traffic entering a network. Access control lists are commonly applied to router or firewall interfaces, and can be configured to control which data sessions can pass and which fail.

The main problem with access control lists is that unless the system administrator instructs the router to log any instances in which traffic is denied, then nobody has a clear picture of ongoing *policy violations*. Knowing about policy violations, or intrusion attempts that fail, is just as important as detecting successful attacks. If configured correctly, a router or firewall can log policy violations and send this information to a management console.

Cisco Intrusion Detection Product Overview

Cisco Systems currently uses a centralized management console known as the NetRanger Director, to gather alarm data from various sources, among them the NetRanger Sensor, the Cisco IOS IDS feature of the Cisco IOS Firewall Feature Set, and access control lists (see Figure 1-3).

Figure 1-3   Director Data Sources
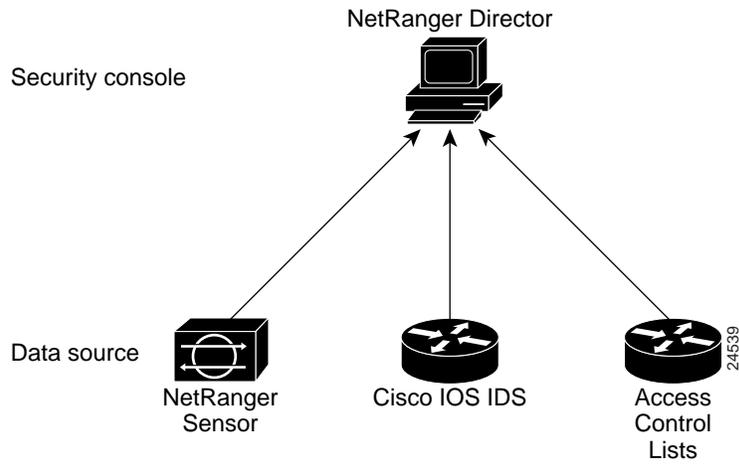
NetRanger Director

The NetRanger Director (see Figure 1-4) provides a centralized graphical interface for the management of security across a distributed network. It can also perform other important functions:

— Remote monitoring and management of Sensors.

— The ability to load NetRanger data files to third-party relational database systems, such as Oracle, through which users can generate reports.

— Access to the Network Security Database (NSDB), an HTML encyclopedia of network vulnerabilities and exploits.

— The ability to send pages or e-mail to security personnel when security events occur.

NetRanger Sensor

The NetRanger Sensor (see Figure 1-4) is a network appliance that is easy to install and maintain on a network. It uses a rules-based engine to distill large volumes of IP network traffic into meaningful security events, which it forwards to a Director. The Sensor can also log security data, reset TCP sessions, and dynamically manage a router's access control lists to shun intruders.

NetRanger Post Office

The NetRanger Post Office (see Figure 1-4) is a proprietary fault-tolerant communication infrastructure that allows Sensors and Directors to communicate with each other. The Post Office also facilitates the transfer of files, such as configuration and log files, between NetRanger nodes.

Figure 1-4   NetRanger Components

Cisco IOS Firewall Intrusion Detection System

The Cisco IOS Firewall Feature Set includes intrusion detection technology for mid-range and high-end router platforms along with firewall support. The Cisco IOS intrusion detection capabilities are ideal for monitoring intranet, extranet, and branch office Internet perimeters for network violations (see Figure 1-5). It is available on the following platforms: Cisco 2600, Cisco 3600, Cisco 7100, and Cisco 7200.

Figure 1-5   Cisco IOS Firewall Intrusion Detection
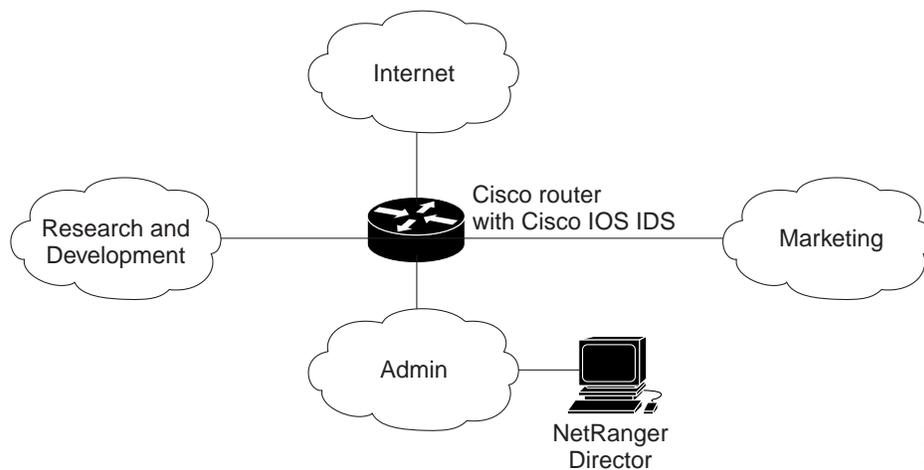
The Cisco IOS Intrusion Detection System (IDS) uses signatures to identify some of the most common attacks and can protect the network via three mechanisms:

— sending an alarm to a syslog or NetRanger Director console

— dropping the offending packet

— resetting the TCP connection

Cisco IOS IDS signatures can be deployed alongside or independent of other Cisco IOS Firewall Feature Set features. The Cisco IOS IDS does not have a full set of intrusion detection signatures, and thus does not provide the same level of intrusion detection and performance as does Cisco's NetRanger Sensor. It cannot dynamically configure an access list and shun (deny) a host or network as a reaction to an attack. Finally, it cannot be configured by the NetRanger Director.

Access Control Lists

Cisco's IOS architecture relies on Access Control Lists (ACLs) tied to physical interface ports for security. These ACLs permit or deny passage of data packets through those physical interface ports. Each numbered or named ACL contains permit and deny conditions that apply to IP addresses or types of traffic. Cisco's software tests these criteria against the conditions in an access list one at a time. The first match determines whether the packets are accepted or rejected. The first match is also a signal to stop testing conditions; therefore, the order of the entries is critical.

Before an ACL can send syslog data back to a NetRanger Director, it must be configured to trap all log information. Furthermore, each ACL deny rule must have the word *log* appended to the end of the line. This way, all policy violations that fail the ACL test are reported to the NetRanger Director alarm console.

Design Considerations

This chapter contains the following sections:

- Intrusion Detection Requires Planning
- Cisco's Comprehensive Security Solution

Intrusion Detection Requires Planning

The following scenario might be a fairly typical occurrence at a company deploying intrusion detection technology for the first time. Not long after purchasing and installing a network-based IDS on an internal network segment, security personnel notice a barrage of alarms on the management console. These alarms provide a frightening picture of the state of the network segment's security. Apparently, there are ping sweeps, port scans, DNS queries, registry hacks, and attempts to mount remote drives occurring on the network.

After further analysis, however, the network security personnel discover that several hosts running Windows NT and HP OpenView are the cause of the ping sweeps and "registry hacks." This is all expected behavior and does not constitute a security threat—or what is known as *false positives*. The IDS rules need to be tuned to minimize alarms from these sources.

The other occurrences are less benign. The port scans, DNS queries, and the drive mounting attempts are coming from outside the protected segment; in fact, from a common source across the Internet. Checking with the InterNIC, the security personnel discover that the attacking network is owned by a business competitor.

The security manager is called in to confer on possible plans of action, and no doubt, the following questions come up:

- Was the IP address of the source of the attack spoofed (falsified)?

- Besides notifying us of the activity, what other actions has the IDS taken?

- Has there been activity from this network in the past?

- Do we have a standard response process for this type of activity?

- Do we have a legal precedent or process for contacting the attacking network's owner?

- What is our next course of action?

Very quickly, the security personnel begin to see the need not only for network analysis (this would have helped them identify possible false positives), but also for operational procedures in case of an incident. Intrusion detection brings new security capabilities, and along with these capabilities comes knowledge of what occurs in the data stream and the liability of having to act on the new knowledge.

Building, maintaining, and retaining a cadre of trained security personnel who can respond effectively to security incidents is a serious commitment of time and resources. For many organizations, this is too much of a commitment. Maybe the best option is to install IDS components on the network and outsource the monitoring and response functions.

As you can see, implementing intrusion detection on your network requires some forethought. This chapter seeks to address these issues and questions to better help organizations deploy intrusion detection technology.

Cisco's Comprehensive Security Solution

This section discusses the following topics:

- Security Wheel
- Developing a Strong Security Policy
- Securing Your Network
- Monitoring the Network
- Testing Security
- Improving Security

Security Wheel

The Cisco security solution is based on an operational perspective rather than on separate products or policies. This security philosophy is reflected in the image of the Security Wheel (as shown in Figure 2-1). The premise of this philosophy is that like network management, security management is a dynamic, ever-changing process.

Figure 2-1   Security Wheel
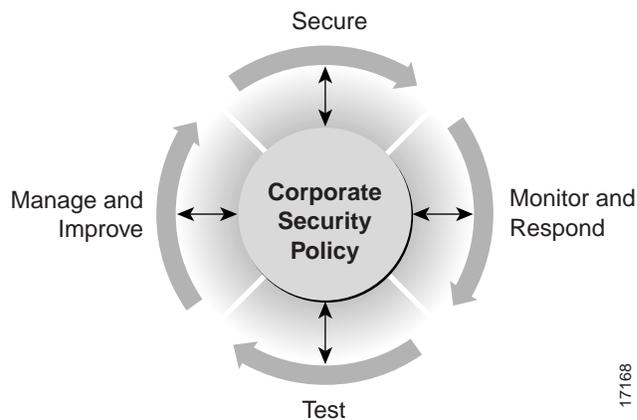
The Security Wheel is cyclical to ensure security diligence and improvement. The paradigm incorporates the following five steps:

Step 1   Develop a strong security policy.

Step 2   Secure the network.

Step 3   Monitor the network and respond to attacks.

Step 4   Test existing security safeguards.

Step 5   Manage and improve corporate security.

The results or data obtained in Steps 2 through 5 always need to be compared to the security policy developed in Step 1 to ensure that high-level security objectives are being met.

The remainder of this chapter provides detailed explanations for each of these steps.

Developing a Strong Security Policy

To develop a strong security policy, you need to take into account the following issues:

- What assets need protecting?

- What is the risk to those assets?

- What is the impact (in terms of reputation, revenues, profits, research) of a successful break-in?

- How much sensitive information is online? What is the impact if this information is damaged or stolen?

- Which users have access to those assets?

- What do users (and this includes business partners and/or customers) expect in the way of security control procedures and mechanisms?

- Should you trust your users?

- Are your users mostly accessing assets locally or remotely, or a mixture of both?

- Do you need different levels of security for different parts of the organization?

- What types of traffic exist on your network?

- Are the needs of security consistent with the business/operational needs of the organization?

- Is there a strong commitment from management to provide sufficient resources to implement security policies and technologies?

- Is there a strong commitment for security awareness training?

A strong security policy should be clearly defined, implemented, and documented, yet simple enough that users can easily go about their business within its parameters. A policy of strong password creation does no good if users consistently choose weak passwords and there is no system in place to validate password choices.

In many ways the security policy is a risk management plan—it documents the risk threshold an organization is willing to accept. Because no security technology provides 100 percent protection, and in most cases organizations do not have the budget to implement all the security elements required, the security policy rates assets and applies commensurable levels of security.

A critical element often overlooked is the policy on incident response. What is the official organization response if a policy is violated?

Securing Your Network

After developing a security policy, secure your network using a variety of point products (firewalls, intrusion detection, etc.). Before you can secure your network, however, you need to combine your understanding of your users, the assets needing protection, and the network's topology.

This section discusses the following topics:

- Understand Your Network Topology
- Understand How the Sensor Devices Function

Understand Your Network Topology

To help prevent possible miscalculations in deploying and configuring an IDS, you should carefully examine these aspects of your network:

- The size and complexity of your network
- Locations of critical resources (file servers, hosts, etc.) on the network
- Connections between your network and other networks, both Internet and extranets
- The amount and type of network traffic on your network

Consideration of these points will help you determine the number of sensors required, the hardware configuration for each sensor (for example, the capacity and type of network interface cards), and the number of management consoles needed.

The NetRanger Sensor is designed to monitor all traffic crossing a given network segment. With that in mind, you should consider all connections to the network you want to protect. These connections fall into four basic categories, or locations as illustrated in Figure 2-2.

Figure 2-2   Major Types of Network Connections
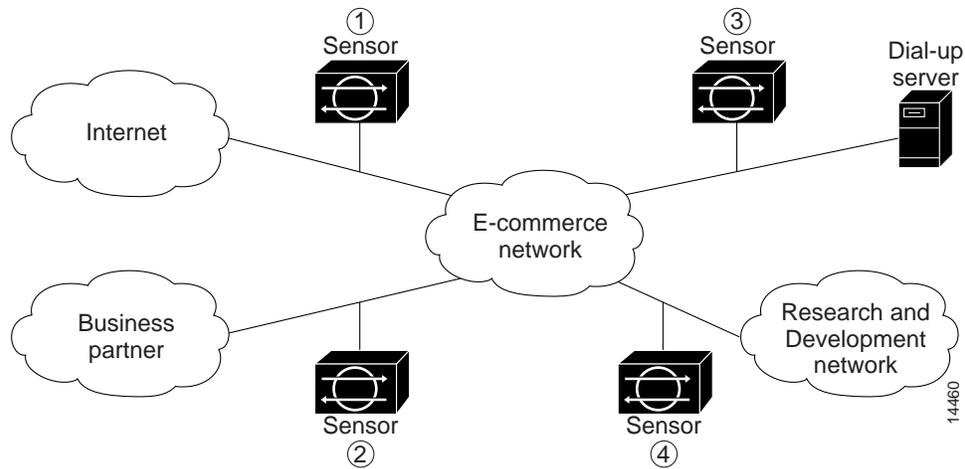
1 In location one, the NetRanger Sensor is placed to monitor traffic between the protected network and the Internet. This is commonly referred to as "perimeter protection" and is the most common deployment for a Sensor.

Because many companies use a firewall to help protect a network perimeter, there are several options for placing a Sensor in relation to the firewall. Placing a Sensor in front of a firewall allows the Sensor to monitor all incoming and outgoing network traffic. However, when deployed in this manner, the Sensor will not normally detect traffic that is internal to the network, as this traffic is behind the firewall. An internal attacker taking advantage of vulnerabilities in network services would remain undetected by the external Sensor.

Placing a Sensor behind a firewall shields the Sensor from any policy violations that the firewall rejects. For example, if the firewall is configured to deny passage of ping sweeps, then the Sensor would not detect this activity or generate any alarms.

The solution is to take advantage of the Sensor's two interfaces: place the Sensor's monitoring interface (which runs in promiscuous mode without an IP address) directly in front of the firewall, and use the second Sensor interface to communicate with the Director or router through the firewall. This configuration is illustrated in Figure 2-3.

Figure 2-3 **Preferred Sensor-Network Device Deployment**
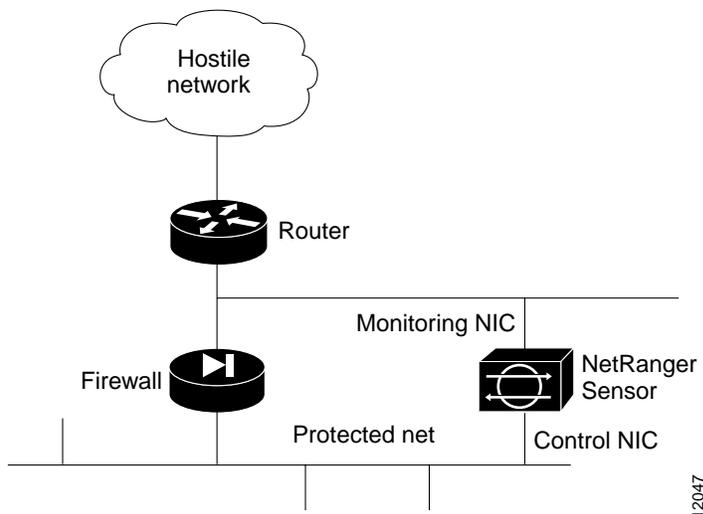
For the Sensor to effectively defend a network using the router and firewall configuration, you must do the following:

(a) Enable Telnet services on the router.

(a) Add the router to the Sensor's device management list.

(a) Configure the firewall to allow Telnet traffic from the Sensor's primary interface to the router; syslog (UDP port 514) traffic from the router to the Sensor; and NetRanger communications (UDP port 45000) between the Sensor and any Director, if the firewall comes between them.

Essentially, the firewall implements policy filtering. The Sensor captures packets between the Cisco router and the firewall, and can dynamically update the Cisco router's access control lists to deny unauthorized activity. Because the Sensor's monitoring NIC has no IP address, it can not be detected, nor can packets be sent to it.

2 In location two, the Sensor is monitoring an extranet connection with a business partner. Although most companies have defined policies on the use and security of this type of connection, there is no guarantee that the partner's network is adequately protected. Consequently, an outsider may enter your network through this type of connection. These extranet connections may be firewalled as well.

3 In location three, the Sensor is monitoring the network side of a remote access server. Although this connection may be only for employee use, it could be vulnerable to external attack.

4 In location four, the Sensor is monitoring an intranet connection. The protected network in this case is a research and development network containing proprietary engineering information requiring additional security.

Figure 2-4   Cisco IOS IDS as Perimeter Intrusion Detection Defense
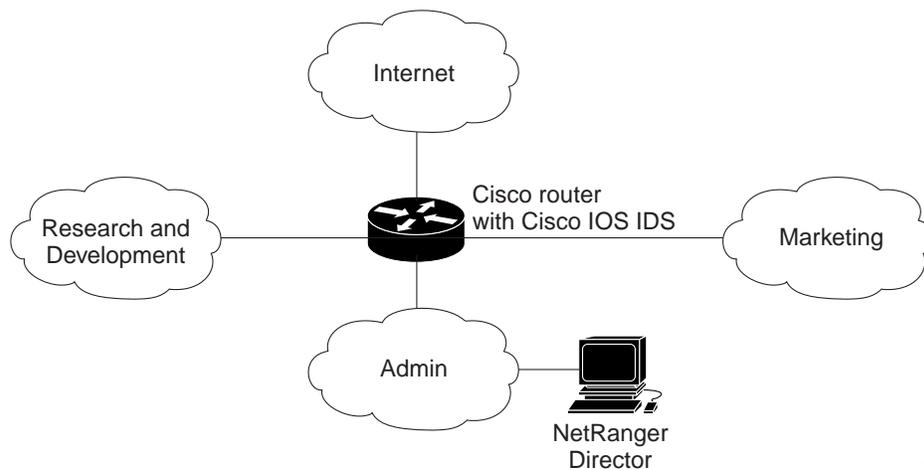
The Cisco IOS IDS feature of the IOS Firewall Feature Set bundled on certain Cisco routers makes for an ideal, lightweight, perimeter intrusion detection defense. Because Cisco IOS IDS contains only a subset of signatures found on the NetRanger Sensor, it will not detect all attacks, but combined with strong access control lists and a firewall, it should provide a fairly robust security service.

With this information, you should now consider the network you want to protect. Determine which segments should be monitored. Keep in mind that each Sensor and Cisco IOS IDS component maintains a security policy configured for the segment it is monitoring. These can be standard across the organization or unique for each IDS sensor device. You may consider changing your network topology to force traffic across a given monitored

network segment. There are always operational trade-offs when going through this process. The end result should be a rough idea of the number of IDS sensors required to protect the desired network.

Understand How the Sensor Devices Function

The next step in protecting your network is understanding how the NetRanger Sensor and Cisco IOS IDS component captures network traffic. We will discuss the NetRanger Sensor first, and then Cisco IOS IDS.

Each NetRanger Sensor comes with two interfaces. In a typical installation, one interface is used for monitoring the desired network segment, and the other interface is used for communication with the Director and other network devices. The monitoring interface is usually in promiscuous mode, meaning it has no IP address and is not visible on the monitored segment. The monitoring interface can currently monitor Ethernet, Fast Ethernet, FDDI, and Token Ring segments (you must select the type of interface when you purchase a Sensor).

The control interface will always be Ethernet. This interface has an assigned IP address, which allows it to communicate with the Director or network devices (typically a Cisco router). Although this interface is "hardened" from a security perspective, it is visible on the network and must be protected.

When responding to attacks, the Sensor inserts TCP Resets via the monitoring interface and ACL changes or shunning via the control interface.

The last step in understanding how a NetRanger Sensor functions is the data speed or load on the monitored network. Because the Sensor is not in the data path, it has a negligible impact on network performance. However, there are limitations on the data speeds it can monitor. Cisco currently offers a Sensor that can monitor Ethernet and Token Ring segments, and a Sensor that can monitor Fast Ethernet and Single/Dual FDDI connections.

Because the Sensor captures packets directly from the network:

- Your company does not have to purchase or maintain an additional router or packet filter.

- Your network administrators have more options for placing the Sensor on the network, because the Sensor can be in many positions relative to an existing router and still capture packets from the network.

There are some fundamental differences between Cisco IOS IDS and the NetRanger Sensor. First, Cisco IOS IDS is an in-line device, and will therefore have an impact on network throughput. Second, the procedure for detecting alarms is slightly different from the NetRanger Sensor.

The Cisco IOS IDS signature-matching procedure is as follows:

1 You create an audit rule, which specifies the signatures that should be applied to packet traffic and the actions to take when a match is found. The signature list can have just one signature, all signatures, or any number of signatures in between. Signatures can be disabled in case of false positives or the needs of the network environment.

2 You apply the audit rule to an interface on the router, specifying a traffic direction (*in* or *out*).

3 If the audit rule is applied to the *in* direction on the interface, packets passing through the interface are audited before the inbound ACL has a chance to discard them. This allows an administrator to be alerted if an attack or information-gathering activity is underway even if the router would normally reject the activity.

4 If the audit rule is applied to the *out* direction on the interface, packets are audited after they enter the router through another interface. In this case, the inbound ACL of the other interface may discard packets before they are audited. This may result in the loss of IDS alarms even though the attack or information-gathering activity was thwarted.

5 Packets going through the interface that match the audit rule are audited by a series of modules, starting with IP; then either ICMP, TCP, or UDP (as appropriate); and finally, the Application level.

6 If a signature match is found in a module, then the following user-configured action(s) occur:

— If the action is **alarm**, then the module completes its audit, sends an alarm, and passes the packet to the next module.

— If the action is **drop**, then the packet is dropped from the module, discarded, and not sent to the next module.

— If the action is **reset**, then the packets are forwarded to the next module, and packets with a reset flag set are sent to both participants of the session, if the session is TCP.

> **Note**   It is recommended that you use the **drop** and **reset** actions together.

If there are multiple signature matches in a module, only the first match fires an action. Additional matches in other modules fire additional alarms, but only one per module.

Monitoring the Network

Once the network has been secured, monitor activity on the network with the NetRanger Director, which can receive security information from NetRanger Sensors and Cisco IOS IDS.

When security incidents occur, respond appropriately. With both NetRanger and Cisco IOS IDS, you can take a variety of actions, such as logging the event, resetting the TCP connection, dropping the offending packets, and dynamically reconfiguring a router's ACLs to shun the attacker. These types of responses need to match the security policy.

Testing Security

Use NetSonar to periodically scan the network for new vulnerabilities. In a growing, changing network environment, new "security holes" are inevitable. Find the vulnerabilities before an attacker does. Vulnerabilities may arise because of new systems or networks. You will also need to test new security products on the network, including NetRanger Sensors, firewalls, access control lists, etc.

Improving Security

Analyze all the metrics you have obtained through the other parts of the security cycle and keep abreast of any new network threats by improving your network security policy. Continue implementing the Security Wheel cycle.

Scenarios

This chapter provides sample scenarios in which intrusion detection technology is deployed in a variety of environments:

- Scenario 1—Using Cisco IOS Firewall Intrusion Detection System
- Scenario 2—Sending Syslogs to a NetRanger Sensor
- Scenario 3—Managing a Router with NetRanger
- Scenario 4—NetRanger Tiered Hierarchy

Scenario 1—Using Cisco IOS Firewall Intrusion Detection System

This section discusses the following topics:

- Objective
- Limitations
- What You Need
- Network Diagram
- General Setup
- Common Problems and Troubleshooting

Objective

The objective of this scenario is to configure the Cisco IOS Firewall Intrusion Detection System (Cisco IOS IDS) on a router. The protected subnet contains sensitive research and development systems. The scenario also features various modifications, including signature tuning for false positives and network redesign.

Limitations

The main limitations of this scenario are throughput and coverage. Because Cisco IOS IDS is an in-line device, it inspects packets as they traverse the router's interfaces. This may impact network performance to some extent. Also, depending on the speed of the segment and the processing power of the router, some packets may not trigger signatures.

Furthermore, because Cisco IOS IDS has fewer signatures than the NetRanger Sensor appliance, it may not detect as many attacks.

What You Need

A Cisco 2600, Cisco 3600, Cisco 7100, or Cisco 7200 router with the Cisco IOS Firewall Feature Set and Cisco IOS Firewall Intrusion Detection System (Cisco IOS IDS) enabled is required for this scenario. You also need a NetRanger Director to receive alarms from the Cisco IOS IDS platform.

Network Diagram

For this scenario, use Figure 3-1 as the initial network diagram.

Figure 3-1   Cisco IOS IDS Network Configuration
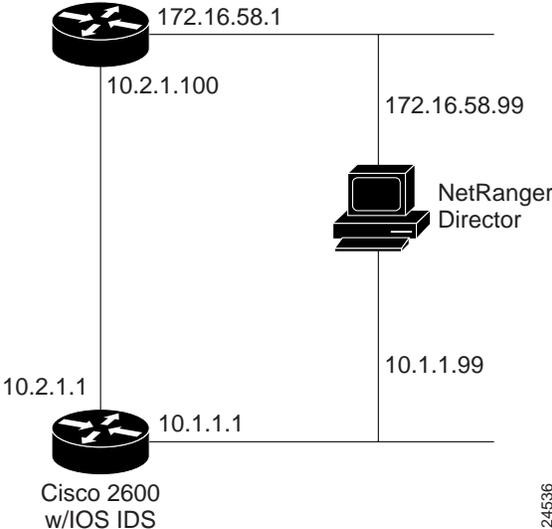
General Setup

The following primary tasks must be taken for initial setup:

1 Initialize Cisco IOS IDS

2 Add Cisco IOS IDS Information to NetRanger

3 Verify the Setup

Initialize Cisco IOS IDS

The Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion. When a packet, or a number of packets in a session, match a signature, the Cisco IOS IDS can perform the following configurable actions:

- **Alarm**—Sends an alarm to a syslog server or NetRanger Director
- **Drop**—Drops the packet
- **Reset**—Resets the TCP connection

In Example 3-1, Cisco IOS IDS is initialized. Notice that the router is set up to use two routes to communicate with the NetRanger Director. This configuration is optional, but provides extra fault tolerance for alarm notifications.

Example 3-1   Cisco IOS IDS Initialized

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2
ip audit name AUDIT.1 info action alarm
ip audit name AUDIT.1 attack action alarm drop reset

interface e0
ip address 10.1.1.1 255.255.255.0
ip audit AUDIT.1 in

interface e1
ip address 10.2.1.1 255.255.0.0
```

Add Cisco IOS IDS Information to NetRanger

Notice that the Cisco IOS IDS router is given a NetRanger Host ID of 55, and its Organization ID (orgid) matches the Director's Organization ID (123).

This NetRanger communication data must be added to the Director in order for the two components to communicate. Use nrConfigure on the NetRanger Director to add the Cisco IOS IDS router's information to the Director:

Step 1   On the Director, start nrConfigure by clicking **Configure** on the **Security** menu.

Step 2   Double-click the name of your Director machine on the displayed list.

Step 3   Double-click the currently applied configuration version (the one that is bolded).

Step 4   Double-click **System Files**.

Step 5   Double-click **Hosts**.

The **Hosts** dialog box opens.

Step 6   Click **Add** and type the host name, host ID, and organization ID for the IDS router.

Step 7   Click **OK** to close the **Hosts** dialog box.

Step 8   Double-click **Routes**.

Step 9   The **Routes** dialog box opens.

Step 10   Click **Add** and type in the route to the IDS router.

Step 11   Click **OK**.

Step 12   The **Routes** dialog box closes.

Step 13   Select the newly created transient version of the configuration and click **Apply**.

Verify the Setup

You can verify that the Director has the Cisco IOS IDS router's information by opening a terminal session on the Director and using the UNIX **more** command to view the actual configuration files (see Example 3-2 and Example 3-3).

Example 3-2   /usr/nr/etc/hosts File on the NetRanger Director

```
$ more /usr/nr/etc/hosts
14.123 localhost
14.123 director.xyzcorp
55.123 ids2600.xyzcorp
```

Example 3-3   /usr/nr/etc/routes File on the NetRanger Director

```
$ more /usr/nr/etc/routes
ids2600.xyzcorp 1 10.1.1.1 45000 1
ids2600.xyzcorp 2 10.2.1.1 45000 1
```

You can verify that Cisco IOS IDS is properly configured on the router with the **show ip audit configuration** command (see Example 3-4). Notice that communication route 1 has a status of established (ESTAB), while communication route 2 has a status of listen (LISTEN). If communication route 1 were to go down, then communication route 2 would automatically become established. After communication route 1 was reestablished, the router would automatically revert to using it instead of route 2.

Example 3-4   Output from show ip audit configuration Command

```
ids2600# show ip audit configuration
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm drop reset
Default threshold of recipients for spam signature is 25
PostOffice:HostID:55 OrgID:123 Msg dropped:0
          :Curr Event Buf Size:100  Configured:100
HID:14 OID:123 S:1 A:2 H:82 HA:49 DA:0 R:0 Q:0
 ID:1 Dest:10.1.1.99:45000 Loc:10.1.1.1:45000 T:5 S:ESTAB *
 ID:2 Dest:172.16.58.99:45000 Loc:10.2.1.1:45000 T:5 S:LISTEN

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
    attack actions alarm drop reset
```

You can verify which interfaces have audit rules applied to them with the **show ip audit interface** command (see Example 3-5).

Example 3-5   Output from show ip audit interface Command

```
ids2600# show ip audit interface
Interface Configuration
 Interface Ethernet0
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
    attack actions alarm drop reset
  Outgoing IDS audit rule is not set
 Interface Ethernet1
  Inbound IDS audit rule is not set
  Outgoing IDS audit rule is not set
```

Alarms deriving from the Cisco IOS IDS platform appear on the NetRanger Director's IOS IDS submap (see Figure 3-2).

**Figure 3-2   Cisco IOS IDS Submap on the NetRanger Director**
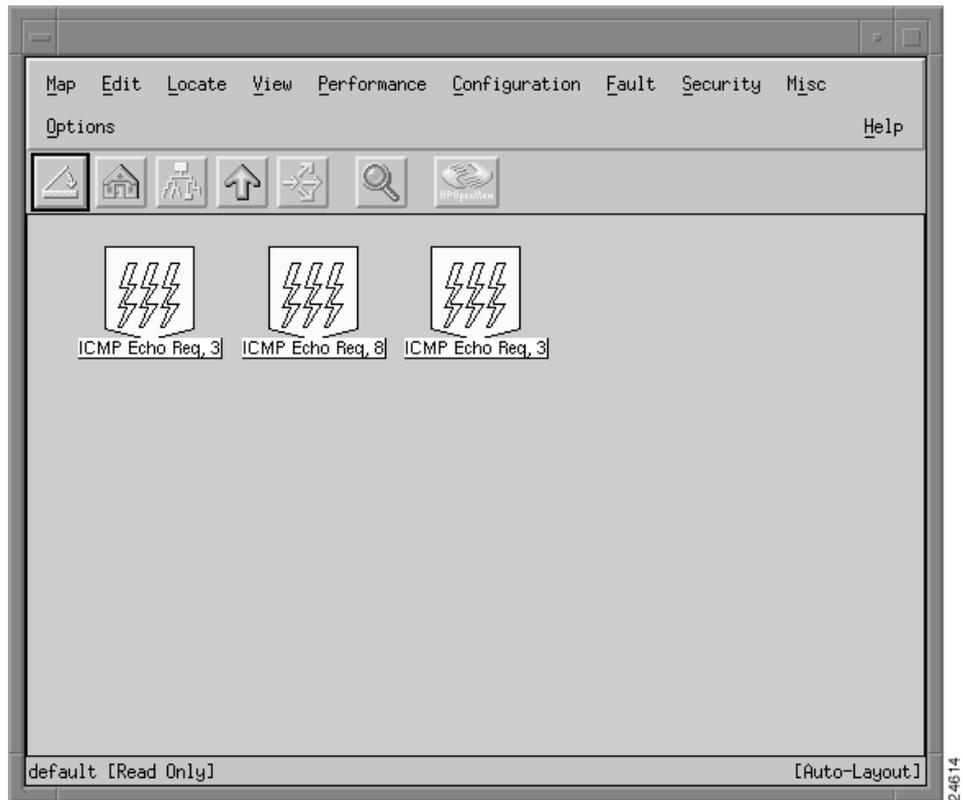
Common Problems and Troubleshooting

One common problem with deploying intrusion detection technologies is false positives, which is otherwise benign or expected behavior that triggers alarms.

For example, in Figure 3-3, a NetSonar device with an IP address of 10.1.1.65 is mapping out various internal subnets, and the audit rule applied to the router's Ethernet0 interface (10.1.1.1) is detecting this activity and sending alarms to the NetRanger Director.

Figure 3-3   NetSonar Device Causing False Positives
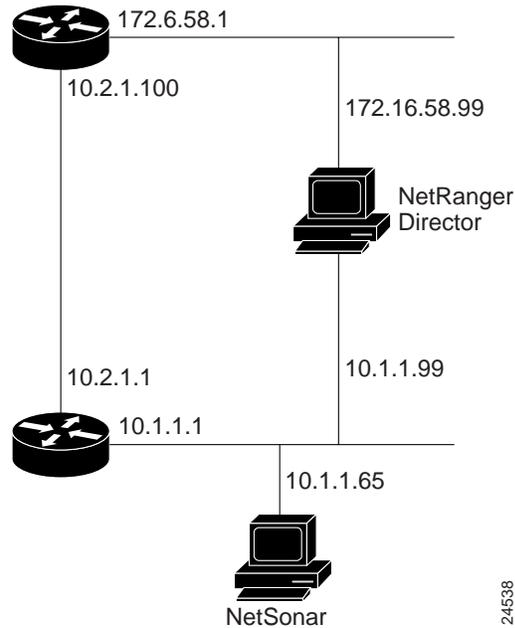
Because the NetSonar device is set to scan the internal subnets on a regular basis, there is no need to generate alarms on this activity. To solve this problem, you can add an access control list (ACL) to the audit rule that keeps traffic originating from the NetSonar device from being audited (see Example 3-6).

Example 3-6   Adding an ACL to the Audit Rule

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop reset

interface e0
ip address 10.1.1.1 255.255.255.0
ip audit AUDIT.1 in

interface e1
ip address 10.2.1.1 255.255.0.0

access-list 90 deny 10.1.1.65
access-list 90 permit any
```

Another way to deal with false positives is to disable the individual signatures that are being triggered. For example, you notice that the router is generating a lot of false positives for signatures 1234, 2345, and 3456. You know that there is an application on the network that is causing signature 1234 to fire, and it is not an application that should cause security concerns. This signature can be disabled, as illustrated in Example 3-7.

Example 3-7   Disabling a Signature

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2

ip audit signature 1234 disable

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop reset

interface e0
ip address 10.1.1.1 255.255.255.0
ip audit AUDIT.1 in

interface e1
ip address 10.2.1.1 255.255.0.0

access-list 90 deny 10.1.1.65
access-list 90 permit any
```

Yet another way to stop false positive alarms is to attach an ACL to the signatures in question. For example, after further investigation, you discover that the false positives for signatures 2345 and 3456 are caused by specific applications on hosts 10.1.1.155 and 10.1.1.2, as well as by some workstations using DHCP on the 172.16.58.0 subnet.

Example 3-8 shows the ACL attached to the signatures.

Example 3-8   Adding an ACL to Signatures

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2

ip audit signature 1234 disable
ip audit signature 2345 list 91
ip audit signature 3456 list 91

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop reset

interface e0
ip address 10.1.1.1 255.255.255.0
ip audit AUDIT.1 in

interface e1
ip address 10.2.1.1 255.255.0.0

access-list 90 deny 10.1.1.55
access-list 90 permit any
access-list 91 deny host 10.1.1.155
access-list 91 deny host 10.1.1.2
access-list 91 deny 172.16.58.0 0.0.0.255
access-list 91 permit any
```

Other common problems are created when a company reorganizes its networks. For instance, in Figure 3-4, the company has now reorganized by adding two subnets, a serial connection to the Internet, and by placing only trusted users on the 10.2.0.0 and 10.3.0.0 networks. Audit rules have been added to the 10.2.1.1, 10.3.1.1, and 192.168.1.1 interfaces. The work done by the employees on the trusted networks must not be disrupted by Cisco IOS IDS, so attack signatures in the AUDIT.1 audit rule now will only alarm on a match.

For sessions that originate from the Internet (via the 192.168.1.1) interface, any attack signature matches (other than the false positive ones that are being filtered out) are to be dealt with in the following manner: send an alarm, drop the packet, and reset the TCP session.

This dual-tier method of signature response is accomplished by configuring two different audit specifications and applying each to a different ethernet interface, as illustrated in Example 3-9.

Figure 3-4   Reorganized Corporate Network
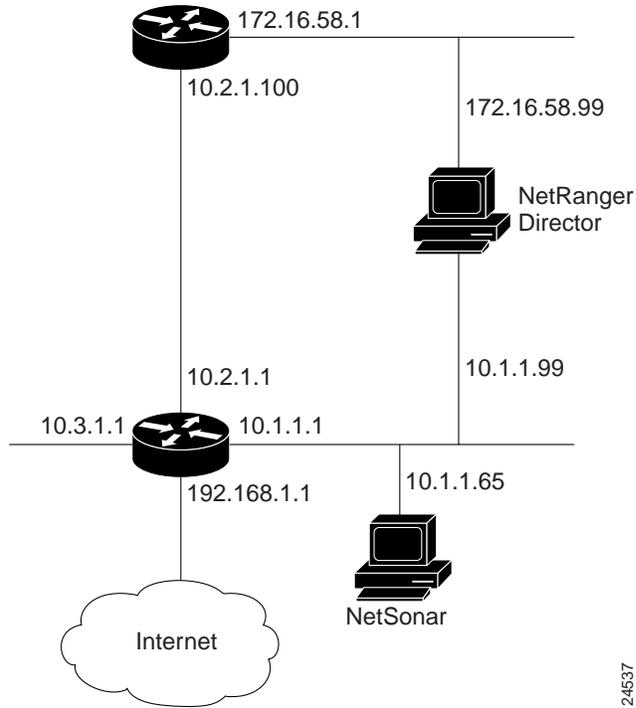
Example 3-9   Dual-Tier Signature Response

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2


ip audit signature 1234 disable
ip audit signature 2345 list 91
ip audit signature 3456 list 91

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm
ip audit name AUDIT.2 info action alarm
ip audit name AUDIT.2 attack alarm drop reset

interface e0
ip address 10.1.1.1 255.0.0.0
ip audit AUDIT.1 in

interface e1
ip address 10.2.1.1 255.255.255.0
ip audit AUDIT.1 in

interface e2
ip address 10.3.1.1 255.255.255.0
ip audit AUDIT.1 in

interface s0
ip address 192.168.1.1 255.0.0.0
ip audit AUDIT.2 in

access-list 90 deny host 10.1.1.65
access-list 90 permit any
access-list 91 deny host 10.1.1.155
access-list 91 deny host 10.1.1.2
access-list 91 deny 172.16.58.0 0.0.0.255
access-list 91 permit any
```

Scenario 2—Sending Syslogs to a NetRanger Sensor

This section discusses the following topics:

- Objective
- Limitations
- What You Need
- Network Diagram
- General Setup
- Common Problems and Troubleshooting

Objective

This scenario illustrates the use of syslog messages to report policy violations (in other words, activity that matches an ACL's deny rule) to a NetRanger Sensor, which can then send the alarm data to a NetRanger Director.

Limitations

The main limitation of this scenario is the number of packets that are denied by the router's ACL, and consequently, the number of syslog messages sent to the NetRanger Sensor.
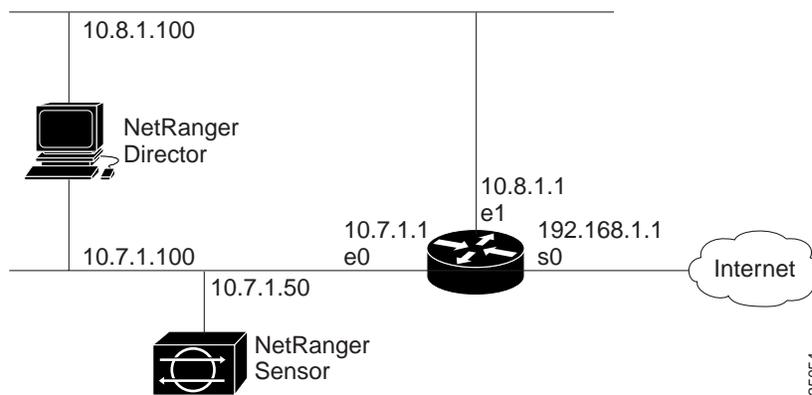
What You Need

This scenario requires that you have a Cisco router running any Cisco IOS software version from Release 10.3 through Release 12.0, and a properly installed and configured NetRanger Sensor and Director.

Network Diagram

For this scenario, use the network diagram in Figure 3-5.

Figure 3-5   Using Syslog to Send Policy Violations to a NetRanger Sensor

General Setup

This section discusses the following topics:

- Initializing the Director and Sensor

- Setting up Syslog on the Router

- Configuring the ACLs to Log Policy Violations

- Configuring the Sensor to Accept Syslog Messages

Initializing the Director and Sensor

For this scenario, initialize the Sensor and Director with the communication parameters listed in Table 3-1.

Table 3-1   NetRanger Setup Parameters

Parameter	Director	Sensor
IP Address	10.7.1.100	10.7.1.50
	10.8.1.100	
Host ID	100	50
Host Name	director	sensor
Organization ID	500	500
Organization Name	xyzcorp	xyzcorp

Refer to the *NetRanger User Guide* for complete installation and setup information.

To verify the configuration of the Director and Sensor, see Example 3-10 through Example 3-13. Notice that because the Director is dual homed on both the 10.7.0.0 and 10.8.0.0 networks, that the Sensor can have both a primary and secondary route to the Director.

Example 3-10   Entries in the Director's /usr/nr/etc/hosts File

```
$ more /usr/nr/etc/hosts
100.500 localhost
100.500 director.xyzcorp
50.500 sensor.xyzcorp
```

Example 3-11   Entry in the Director's /usr/nr/etc/routes File

```
$ more /usr/nr/etc/routes
sensor.xyzcorp 1 10.7.1.50 45000 1
```

Example 3-12   Entries in the Sensor's /usr/nr/etc/hosts File

```
$ more /usr/nr/etc/hosts
50.500 localhost
50.500 sensor.xyzcorp
100.500 director.xyzcorp
```

Example 3-13   Entry in the Sensor's /usr/nr/etc/routes File

```
$ more /usr/nr/etc/routes
director.xyzcorp 1 10.7.1.100 45000 1
director.xyzcorp 2 10.8.1.100 45000 1
```

Setting up Syslog on the Router

To set up syslog notification on the router, enter configuration mode on the router with the **conf t** command and type the following commands:

```
logging sensor_ip_address
logging trap info
```

where *sensor_ip_address* is the IP address of the Sensor's command and control interface.

Note   For this scenario, the IP address of the Sensor is 10.7.1.50.

Exit configuration mode by pressing Ctrl+Z and make the changes permanent on the router with the **wr mem** command.

Configuring the ACLs to Log Policy Violations

After setting up syslog notification, you need to manually configure the ACLs to log policy violations. In this scenario, an ACL has been applied to the router's Serial 0 interface (192.168.1.1) to deny all inbound FTP and Telnet traffic from the Internet. The ACL in question is listed in Example 3-14.

Example 3-14   ACL Denying Specific Types of Traffic

```
interface serial 0
ip address 192.168.1.1 255.255.0.0
ip access-group 199 in

access-list 199 deny tcp any any eq 21
access-list 199 deny tcp any any eq 23
access-list 199 permit ip any any
```

To report violations of this ACL, append the string "log" at the end of each deny rule, as illustrated in Example 3-15.

Example 3-15   Using the log Feature

```
access-list 199 deny tcp any any eq 21 log
access-list 199 deny tcp any any eq 23 log
access-list 199 permit ip any any
```

Note   To make this change permanent on the router, be sure to type **wr mem** after setting the log argument.

Configuring the Sensor to Accept Syslog Messages

The final step in sending syslog notifications to a Sensor is to configure the Sensor to accept the syslog messages.

To configure the Sensor to accept *syslogd* traffic from the router, follow these steps:

Step 1   On the Director interface, click the Sensor's icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version (the folder that is bolded), double-click **Intrusion Detection**.

Step 3   Click the **Data Sources** tab.

Step 4   In the **Data Sources** field, ensure that the IP address and netmask of the router sending the syslog information is present.

Step 5   Click the **Profile** tab and ensure that **Setup Method** is set to **Manual Configuration**.

Step 6   Click **Modify Sensor** and scroll down to the "Security Violations" signature and click **Expand**.

Step 7   Click **Add** to add the name/number of the Cisco ACL that sends syslog data to the Sensor (in this case, 199).

Step 8 Choose an action from the list in response to the policy violation alarm, and enter the alarm's severity level for the destination (the NetRanger Director).

Step 9 Click **OK** on each dialog box to close them.

Step 10 Select the newly created transient version and click **Apply**.

When you click **Apply**, the NetRanger Director updates the Sensor's configuration. The Sensor can now accept syslog traffic from the router and send policy violation alarms to the Director.

Common Problems and Troubleshooting

A common problem with this type of scenario involves insufficient protection. For example, although FTP and Telnet traffic is being denied and logged to the Sensor, an attacker may also try to enter the network via other methods, such as rlogin, HTTP, or TFTP.

In this scenario, other alarms on unauthorized activity are all being generated by a group of hosts on a specific network (hosts 172.31.10.10-13). It seems that all the traffic (except the FTP and Telnet attempts) from these specific attackers is getting through the router's interfaces.

The easiest solution is to adjust the ACL to deny the specific hosts (see Example 3-16).

Example 3-16   Denying Specific Hosts with an ACL

```
access-list 199 deny host 172.31.10.10 log
access-list 199 deny host 172.31.10.12 log
access-list 199 deny host 172.31.10.13 log
access-list 199 deny tcp any any eq 21 log
access-list 199 deny tcp any any eq 23 log
access-list 199 permit ip any any
```

Another problem with this scenario is based largely on the amount of syslog traffic sent to the Sensor (and the subsequent alarms sent to the Director). If the amount of syslog notifications is undesirable (either for reasons of performance or alarm management), then you have two options:

1 Continue to deny traffic, but do not log the policy violations. Simply remove "log" from the end of any deny rule you no longer want logged.

2 Reconfigure the ACLs to pinpoint and deny specific traffic instead of denying all traffic of a certain type or source.

   For example, instead of denying traffic from all hosts on a network, deny only certain hosts from that network.

For example, instead of disallowing all incoming FTP and Telnet traffic from the Internet, selectively deny this type of traffic from certain hosts or networks known to be hostile.

Scenario 3—Managing a Router with NetRanger

This section discusses the following topics:

- Objective
- Limitations
- What You Need
- Network Diagram
- General Setup
- Common Problems and Troubleshooting

Objective

The objective of this scenario is to deploy a Cisco router, firewall, and Sensor in such a way that the Sensor can dynamically update the router's ACLs to shun attackers.

Limitations

For this scenario, there are two major limitations:

- If no ACLs are currently being applied, then you might notice an immediate impact on router performance once the NetRanger dynamic ACL is imposed.

- If ACLs are already in place on a certain interface and direction, then the NetRanger dynamic ACL might replace it. You will need to move the existing ACL to another interface in order to save it.
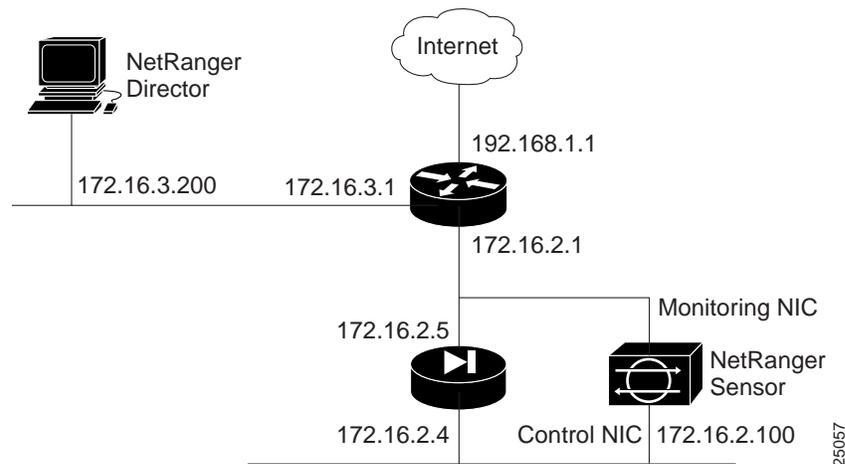
What You Need

A Cisco router running any Cisco IOS software version from Release 10.3 through Release 12.0, a PIX Firewall, and a NetRanger Director and Sensor.

Network Diagram

For this scenario, use Figure 3-6 as the network diagram.

Figure 3-6   NetRanger Sensor Managing a Cisco Router

General Setup

This section discusses the following topics:

- Initializing the Director and Sensor
- Configuring the Router
- Configuring the Firewall
- Setting Up Device Management

Initializing the Director and Sensor

For this scenario, initialize the Sensor and Director with the communication parameters listed in Table 3-2.

Table 3-2   NetRanger Setup Parameters

Parameter	Director	Sensor
IP Address	172.16.3.200	172.16.2.100
Host ID	200	100
Host Name	director	sensor
Organization ID	500	500
Organization Name	xyzcorp	xyzcorp

Refer to the *NetRanger User Guide* for complete installation and setup information.

To verify the configuration of the Director and Sensor, see Example 3-17 through Example 3-20.

Example 3-17   Entries in the Director's /usr/nr/etc/hosts File

```
$ more /usr/nr/etc/hosts
200.500 localhost
200.500 director.xyzcorp
100.500 sensor.xyzcorp
```

Example 3-18   Entry in the Director's /usr/nr/etc/routes File

```
$ more /usr/nr/etc/routes
sensor.xyzcorp 1 172.16.2.100 45000 1
```

Example 3-19   Entries in the Sensor's /usr/nr/etc/hosts File

```
$ more /usr/nr/etc/hosts
100.500 localhost
100.500 sensor.xyzcorp
200.500 director.xyzcorp
```

Example 3-20   Entry in the Sensor's /usr/nr/etc/routes File

```
$ more /usr/nr/etc/routes
director.xyzcorp 1 172.16.3.200 45000 1
```

Configuring the Router

The initial setup for the router in this scenario is illustrated in Example 3-21.

Example 3-21   Initial Router Configuration

```
Using 906 out of 29688 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname border-router
!
logging console informational
enable password attack
!
memory-size iomem 10
!
interface ethernet 0
ip address 172.16.2.1 255.255.0.0
!
interface ethernet 1
ip address 172.16.3.1 255.255.0.0
!
interface serial 0
ip address 192.168.1.1 255.255.0.0
```

In this scenario, you need to set up an ACL on the router to deny all traffic outside the 172.16.0.0 Class B network, thereby protecting the NetRanger Director from any possible outside attacker. The ACL is applied to the *out* direction of the router's ethernet 1 interface (see Example 3-22).

Example 3-22   Applying the ACL to the ethernet 1 Interface

```
interface ethernet 1
ip address 172.16.3.1 255.255.0.0
access-group 1 out

access-list 1 permit 172.16.0.0 0.0.255.255
```

Configuring the Firewall

Configure the PIX Firewall to allow the following traffic:

• Telnet traffic from the Sensor's control interface (172.16.2.100) to the router (172.16.2.1).

• NetRanger communications (UDP port 45000) between the Sensor and the Director (172.16.3.200).

Setting Up Device Management

Device management refers to the Sensor's ability to dynamically reconfigure the filters and access control lists on a router to shun an attacker. This functionality is provided by the *managed* service. Shunning refers to the Sensor's ability to use a network device to deny entry to a specific network host or an entire network.

NetRanger Sensors can manage the following types of Cisco routers:

• Cisco 1600

• Cisco 2500

• Cisco 3600

• Cisco 4500

• Cisco 4700

• Cisco 7200

• Cisco 7500

To configure device management on the Sensor, follow these steps:

Step 1   On the Director interface, click the Sensor's icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version (the folder that is bolded), double-click **Device Management**.

Step 3   Click the **Devices** tab.

Step 4   Add information about the router (such as it's IP address, username, password, and enable password).

Step 5   Click the **Interfaces** tab.

Step 6   Add information about each of the managed router's interfaces (such as IP address, interface name).

The IP address you enter is the IP address of the interface the Sensor uses to communicate with the router. This interface is not necessarily the same interface used for shunning.

For this scenario, the Sensor communicates with the 172.16.2.1 interface, and dynamically shuns on the 192.168.1.1 interface's *in* direction (s0 in).

Step 7   Click the **Shunning** tab.

Step 8   Add the Director, Sensor, PIX Firewall, and router to the **Addresses Never to Shun** list.

This keeps the Sensor from ever shunning those particular hosts.

Step 9   Add an entry for the Sensor under **Shunning Servers**.

Step 10   Click the **General** tab.

Step 11   Set the shunning ACL to 199.

The Sensor will use this ACL on the router to dynamically shun attackers. The Sensor will also use ACL 198 as the second ACL to write to whenever changes need to be made to the original ACL.

Step 12   Click **OK** to close the **Device Management** dialog box.

Step 13   Double-click the **Intrusion Detection** dialog box.

Step 14 Click the **Profile** tab.

Step 15 Select **Profile-based Configuration**.

Step 16 Under **Signatures to Disable**, you can disable individual signatures by selecting their check boxes.

Step 17 Under **Response**, click either **Relaxed**, **Moderate**, or **Strong**.

Step 18 You can view your settings in the **General Signatures** dialog box by clicking **View Sensor**.

Step 19 Click **OK** to close the Intrusion Detection dialog box.

Step 20 Select the newly created transient version and click **Apply**.

When this process is complete, the Sensor's /usr/nr/etc/managed.conf file should look something like Example 3-23.

Example 3-23 Entries in the Sensor's /usr/nr/etc/managed.conf File

```
$ more /usr/nr/etc/managed.conf

FilenameOfError            ../var/errors.managed

NetDevice    172.16.2.1  DefaultCisco  password  enable

NeverShunAddress 172.16.3.200 255.255.255.255  #Director
NeverShunAddress 172.16.2.100 255.255.255.255  #Sensor
NeverShunAddress 172.16.2.5 255.255.255.255    #Firewall--outer interface
NeverShunAddress 172.16.2.4 255.255.255.255    #Firewall--inner interface
NeverShunAddress 172.16.2.1 255.255.255.255    #Router

ShunInterfaceCisco 192.168.1.1 Serial0 in
ShunAclCisco 199
MaxShunEntries 100

FilenameOfError ../var/errors.managed
FilenameOfConfig ../etc/managed.conf
EventLevelOfErrors 1
EventLevelOfCommandLogs 1
EnableACLLogging 0
```

The NetRanger Sensor is now ready to initiate shunning by writing a dynamic ACL to the router's Serial0 interface. The next major step is to decide which signatures trigger a shun response. This type of automated response by the Sensor should only be configured for attack signatures with a low probability of false positive detection, such as an unambiguous SATAN attack. In case of any suspicious activity that does not trigger automatic shunning, you can use a Director menu function to shun manually.

To set up responses for signatures, follow these steps:

Step 1 On the Director interface, click the Sensor's icon and click **Configure** on the **Security** menu.

Step 2 In the current configuration version (the folder that is bolded), double-click **Intrusion Detection**.

Step 3 Click the **Profile** tab.

Step 4 Select **Manual Configuration** and click **Modify Sensor**.

Step 5 In the **General Signatures** dialog box, you can select shunning for any signature. However, the best candidates for use with shunning are known as Level 5 Signatures, and they are listed in Example 3-24.

Step 6 For this scenario, set the shun action on the following signatures:

- 3250 TCP Hijacking
- 3500 rlogin -froot
- 3600 IOS DoS
- 4053 Back Orifice
- 6001 Normal SATAN Probe
- 6002 Heavy SATAN Probe

Step 7 Click **OK** to close the General Signatures dialog box.

Step 8 Click **OK** to close the Intrusion Detection dialog box.

Step 9 Select the newly created transient version and click **Apply**.

The listing in Example 3-24 was filtered from the /usr/nr/etc/wgc/templates/packetd.conf file using the following UNIX command:

```
grep SigOfGeneral /usr/nr/etc/wgc/templates/packetd.conf | awk '{ if
(($4 ~ /5/) && ($5 ~ /5/) && ($6 ~ /5/) && ($7 ~ /5/)) { print $0 } }'
```

This command extracts all signatures that contain the numeral 5 in each of the four destination columns of the /usr/nr/etc/wgc/templates/packetd.conf file. These signatures have been identified by Cisco to have a very low incidence of false positives; in other words, these signatures fire only on actual attacks the vast majority of the time.

Example 3-24   Level 5 Signatures

```
SigOfGeneral 1004  0  5  5  5  5   # IP options - Loose source route
SigOfGeneral 1006  0  5  5  5  5   # IP options - Strict source route
SigOfGeneral 1102  0  5  5  5  5   # Impossible IP packet
SigOfGeneral 1103  0  5  5  5  5   # IP fragments overlap
SigOfGeneral 2101  0  5  5  5  5   # ICMP network sweep w/Timestamp
SigOfGeneral 2102  0  5  5  5  5   # ICMP network sweep w/Address Mask
SigOfGeneral 2154  0  5  5  5  5   # ICMP Ping Of Death
SigOfGeneral 3003  0  5  5  5  5   # TCP FRAG SYN port sweep
SigOfGeneral 3005  0  5  5  5  5   # TCP FIN port sweep
SigOfGeneral 3006  0  5  5  5  5   # TCP FRAG FIN port sweep
SigOfGeneral 3011  0  5  5  5  5   # TCP FIN High port sweep
SigOfGeneral 3012  0  5  5  5  5   # TCP FRAG High FIN port sweep
SigOfGeneral 3015  0  5  5  5  5   # TCP Null port sweep
SigOfGeneral 3016  0  5  5  5  5   # TCP FRAG Null port sweep
SigOfGeneral 3020  0  5  5  5  5   # TCP SYN FIN port sweep
SigOfGeneral 3021  0  5  5  5  5   # TCP FRAG SYN FIN port sweep
SigOfGeneral 3031  0  5  5  5  5   # TCP FRAG SYN host sweep
SigOfGeneral 3032  0  5  5  5  5   # TCP FIN host sweep
SigOfGeneral 3033  0  5  5  5  5   # TCP FRAG FIN host sweep
SigOfGeneral 3034  0  5  5  5  5   # TCP NULL host sweep
SigOfGeneral 3035  0  5  5  5  5   # TCP FRAG NULL host sweep
SigOfGeneral 3036  0  5  5  5  5   # TCP SYN/FIN host sweep
SigOfGeneral 3037  0  5  5  5  5   # TCP FRAG SYN/FIN host sweep
SigOfGeneral 3050  0  5  5  5  5   # Half-open SYN attack
SigOfGeneral 3107  0  5  5  5  5   # Majordomo exec bug
SigOfGeneral 3108  0  5  5  5  5   # MIME overflow bug
SigOfGeneral 3229  0  5  5  5  5   # WebSite win-c-sample buffer overflow
SigOfGeneral 3233  0  5  5  5  5   # WWW Count Overflow
SigOfGeneral 3250  0  5  5  5  5   # TCP Hijacking
```

```
SigOfGeneral 3251  0   5   5   5   5   # TCP Hijacking Simplex Mode
SigOfGeneral 3300  0   5   5   5   5   # NETBIOS OOB data
SigOfGeneral 3306  0   5   5   5   5   # Windows Registry Access
SigOfGeneral 3307  0   5   5   5   5   # Windows RedButton
SigOfGeneral 3500  0   5   5   5   5   # rlogin -froot
SigOfGeneral 3525  0   5   5   5   5   # Imap Authenticate Overflow
SigOfGeneral 3526  0   5   5   5   5   # Imap Login Overflow
SigOfGeneral 3550  0   5   5   5   5   # Pop Overflow
SigOfGeneral 3575  0   5   5   5   5   # Inn Overflow
SigOfGeneral 3576  0   5   5   5   5   # Inn Control Message
SigOfGeneral 3600  0   5   5   5   5   # IOS DoS
SigOfGeneral 3601  0   5   5   5   5   # IOS Command History
SigOfGeneral 4001  0   5   5   5   5   # UDP port scan
SigOfGeneral 4053  0   5   5   5   5   # Back Orifice
SigOfGeneral 4100  0   5   5   5   5   # Tftp passwd file attempt
SigOfGeneral 6001  0   5   5   5   5   # Normal SATAN probe
SigOfGeneral 6002  0   5   5   5   5   # Heavy SATAN probe
SigOfGeneral 6100  0   5   5   5   5   # RPC port registration
SigOfGeneral 6101  0   5   5   5   5   # RPC port unregistration
SigOfGeneral 6110  0   5   5   5   5   # RPC RSTATD Port Sweep
SigOfGeneral 6111  0   5   5   5   5   # RPC RUSERSD Port Sweep
SigOfGeneral 6112  0   5   5   5   5   # RPC NFS Port Sweep
SigOfGeneral 6113  0   5   5   5   5   # RPC MOUNTD Port Sweep
SigOfGeneral 6114  0   5   5   5   5   # RPC YPPASSWDD Port Sweep
SigOfGeneral 6115  0   5   5   5   5   # RPC SELECTION SVC Port Sweep
SigOfGeneral 6116  0   5   5   5   5   # RPC REXD Port Sweep
SigOfGeneral 6117  0   5   5   5   5   # RPC STATUS Port Sweep
SigOfGeneral 6118  0   5   5   5   5   # RPC TTDB Port Sweep
SigOfGeneral 6190  0   5   5   5   5   # statd buffer overflow
SigOfGeneral 6191  0   5   5   5   5   # ttdb buffer overflow
SigOfGeneral 6192  0   5   5   5   5   # mountd buffer overflow
SigOfGeneral 6200  0   5   5   5   5   # Ident buffer overflow
SigOfGeneral 6201  0   5   5   5   5   # Ident newline
SigOfGeneral 6202  0   5   5   5   5   # Ident improper request
SigOfGeneral 6300  0   5   5   5   5   # Loki ICMP tunnel
SigOfGeneral 6302  0   5   5   5   5   # Modified Loki ICMP tunneling
```

Common Problems and Troubleshooting

Many security administrators implementing this scenario may prefer to have a dual-homed Director machine so that the Sensor can communicate with it directly, instead of via the PIX Firewall and router.

In Figure 3-7, the NetRanger Director is dual-homed on the 172.16.3.0 and 172.16.2.0 networks.

Figure 3-7   Dual-homed Director
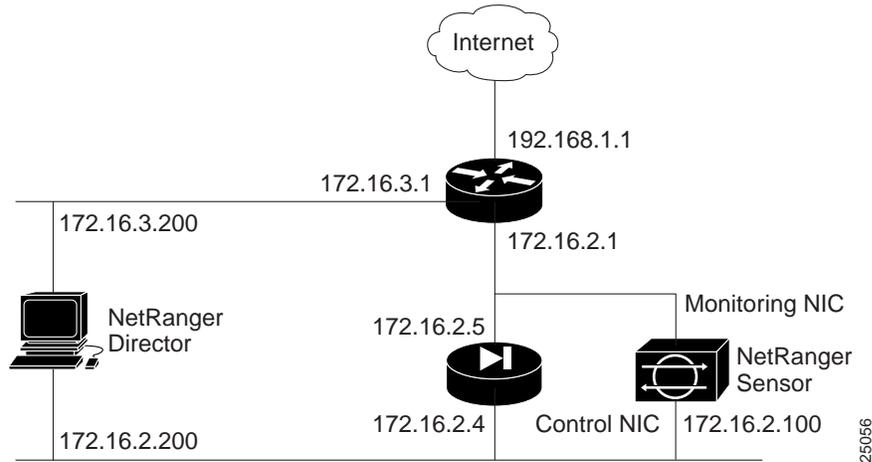
This slight change in configuration requires that you alter the entries in the Sensor's /usr/nr/etc/routes file; not only are you adding an entry for the 172.16.2.200 network address, you also decide to make this route the preferred route and the previous route secondary.

To implement this change, use nrConfigure:

Step 1   On the Director interface, click the Sensor's icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version (the folder that is bolded), double-click **System Files**.

Step 3   Double-click **Routes**.

Step 4   Select the second line, which indicates that the route to 172.16.3.200 is a primary route.

Step 5   Click **Modify**.

Step 6   Change the priority of the route to **2**.

Step 7   Click **OK**.

Step 8   Click **OK** to close the **Routes** dialog box.

Step 9   Select the newly created transient version and click **Apply**.

The Sensor's routes file should now look like Example 3-25.

Example 3-25   Changed /usr/nr/etc/routes File on the Sensor

```
$ more /usr/nr/etc/routes
director.xzycorp 1 172.16.2.200 45000 1
director.xyzcorp 2 172.16.3.200 45000 1
```

In addition, you have to add this new Director IP address to the Sensor's NeverShunAddress list:

Step 1   On the Director interface, click the Sensor's icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version (the folder that is bolded), double-click **Device Management**.

Step 3   Click the **Shunning** tab.

Step 4   Add the 172.16.2.200 IP address to the **Addresses Never to Shun** list.

Step 5   Click **OK** to close the Intrusion Detection dialog box.

Step 6   Select the newly created transient version and click **Apply**.

You can verify this change by looking at the /usr/nr/etc/managed.conf file (see Example 3-26).

Example 3-26   Changed /usr/nr/etc/managed.conf File on the Sensor

```
$ more /usr/nr/etc/managed.conf
FilenameOfError            ../var/errors.managed

NetDevice    172.16.2.1  DefaultCisco  password  enable

NeverShunAddress 172.16.3.200 255.255.255.255
NeverShunAddress 172.16.2.200 255.255.255.255
NeverShunAddress 172.16.2.100 255.255.255.255
NeverShunAddress 172.16.2.5 255.255.255.255
NeverShunAddress 172.16.2.4 255.255.255.255
NeverShunAddress 172.16.2.1 255.255.255.255

ShunInterfaceCisco 192.168.1.1 Serial0 in
ShunAclCisco 199
MaxShunEntries 100

FilenameOfError ../var/errors.managed
FilenameOfConfig ../etc/managed.conf
EventLevelOfErrors 1
EventLevelOfCommandLogs 1
EnableACLLogging 0
```

Many months later, when the corporate network is reconfigured, it is decided that outside networks should have full access to the 172.16.3.0 network. For this to occur, the ACL on the 172.16.3.1 interface must be removed (see Example 3-27). However, because there are still critical servers and systems on this subnet, it is decided that a NetRanger Sensor should be installed there for security. Figure 3-8 illustrates the new changes to the network.

Example 3-27   Removed ACL from the 172.16.3.1 Interface

```
interface ethernet 1
ip address 172.16.3.1 255.255.0.0
```

Figure 3-8   Reorganized Network
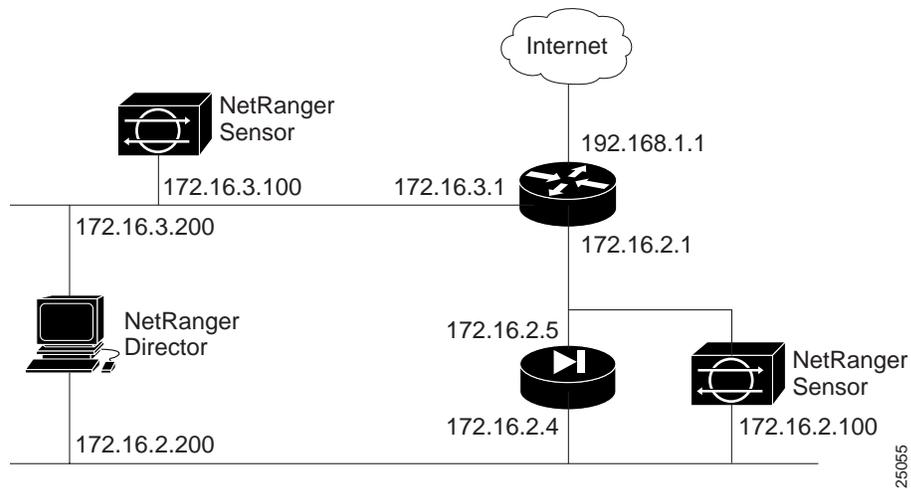
The new Sensor at 172.16.3.100 needs to be able to communicate with the Director, and vice versa. You can use nrConfigure's **Add Host Wizard** to add this Sensor (see the *NetRanger User Guide* for more information).

Use the values listed in Table 3-3 to set up the second Sensor.

Table 3-3   NetRanger Setup Parameters

Parameter	Sensor
IP Address	172.16.3.100
Host ID	300
Host Name	sensor2
Organization ID	500
Organization Name	xyzcorp

You can verify that these parameters are set on the Sensor by viewing it's configuration files. They should look like Example 3-28 and Example 3-29.

Example 3-28   /usr/nr/etc/hosts File on the New Sensor

```
$ more /usr/nr/etc/hosts
300.500 localhost
300.500 sensor2.xyzcorp
200.500 director.xyzcorp
```

Example 3-29   /usr/nr/etc/routes File on the New Sensor

```
$ more /usr/nr/etc/routes
director.xzycorp 1 172.16.3.200 45000 1
director.xyzcorp 2 172.16.2.200 45000 1
```

Note   This Sensor also has two communication routes to the Director.

The **Add Host Wizard** automatically adds the Sensor as an entry to the Director's hosts and routes files. You can verify this by checking the configuration files, which should look like Example 3-30 and Example 3-31.

Example 3-30   Changed /usr/nr/etc/hosts File on the Director

```
$ more /usr/nr/etc/hosts
200.500 localhost
200.500 director.xyzcorp
100.500 sensor.xyzcorp
300.500 sensor2.xyzcorp
```

Example 3-31   Changed /usr/nr/etc/routes File on the Director

```
$ more /usr/nr/etc/routes
sensor.xyzcorp 1 172.16.2.100 45000 1
sensor2.xyzcorp 1 172.16.3.100 45000 1
```

Scenario 4—NetRanger Tiered Hierarchy

This section discusses the following topics:

- Objective
- Limitations
- What You Need
- Network Diagram
- General Setup
- Common Problems and Troubleshooting

Objective

The objective of this scenario is to build a hierarchy of Sensor and Director systems through the use of message propagation. Instead of broadcasting events from a Sensor onto multiple hosts, information can be sent to a single Director, which can then propagate packets onto other platforms defined in its local configuration files. The Sensors will also be configured to propagate messages to more than one Director, thereby insuring fault-tolerant communication.

In addition to providing performance benefits and fault tolerance, tiered hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9AM to 5PM and then transfer control onto a central remote Director every evening.

Limitations

Although using a tiered hierarchy provides some benefits of reduced workload, using local Director hosts to forward packets to remote Director hosts may involve delays if the links connecting the segments are slow or heavily trafficked. This may result in slight delays in alarm generation on the "top-level" Director in the tiered hierarchy.

Another limitation involves using the "top-level" Director to configure Sensors and act on the copied alarms. These and other issues are discussed in the "Common Problems and Troubleshooting" section.
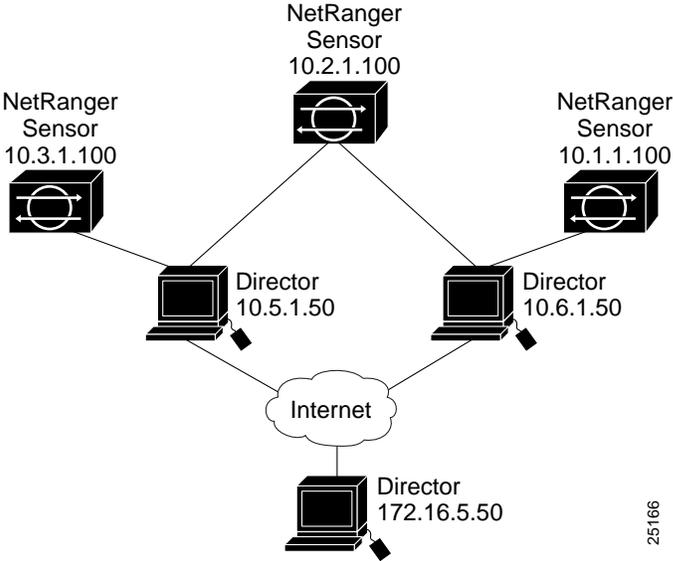
What You Need

This scenario involves the use of three Sensors and three Directors; however, any number of Sensors and Directors can be used.

Network Diagram

For this scenario, use Figure 3-9 as a reference point.

Figure 3-9   Tiered Hierarchy of NetRanger Components

General Setup

For this scenario, use nrConfigure's **Add Host Wizard** to initialize each Sensor and Director (see the *NetRanger User Guide* for more information). Use the values listed in Table 3-4.

Table 3-4   Hosts and Routes Information on Directors and Sensors

Host	Host Information	Communications Information
10.5.1.50 Director	Host ID: 10 Organization ID: 500 Host Name: director1 Organization Name: xyzcorp IP Address: 10.5.1.50	Primary routes to: • sensor3.xyzcorp (10.3.1.100) • sensor2.xyzcorp (10.2.1.100) • director3.xyzcorp (172.16.5.50)
10.6.1.50 Director	Host ID: 20 Organization ID: 500 Host Name: director2 Organization Name: xyzcorp IP Address: 10.6.1.50	Primary routes to: • sensor2.xyzcorp (10.2.1.100) • sensor1.xyzcorp (10.1.1.100) • director3.xyzcorp (172.16.5.50)
172.16.5.50 Director	Host ID: 30 Organization ID: 500 Host Name: director3 Organization Name: xyzcorp IP Address: 172.16.5.50	Primary routes to: • director1.xyzcorp (10.5.1.50) • director2.xyzcorp (10.6.1.50)
10.3.1.100 Sensor	Host ID: 300 Organization ID: 500 Host Name: sensor3 Organization Name: xyzcorp IP Address: 10.3.1.100	Primary route to: • director1.xyzcorp (10.5.1.50)

Table 3-4   **Hosts and Routes Information on Directors and Sensors (continued)**

Host	Host Information	Communications Information
10.2.1.100 Sensor	Host ID: 200 Organization ID: 500 Host Name: sensor2 Organization Name: xyzcorp IP Address: 10.2.1.100	Primary routes to: • director1.xyzcorp (10.5.1.50) • director2.xyzcorp (10.6.1.50)
10.1.1.100 Sensor	Host ID: 100 Organization ID: 500 Host Name: sensor1 Organization Name: xyzcorp IP Address: 10.1.1.100	Primary route to: • director2.xyzcorp (10.6.1.50)

After initial configuration, configure director3 to accept the alarms it receives from director1 and director2:

Step 1   On director3's interface, click the director3 icon and click **Configure** on the **Security** menu.

Step 2   Double-click **System Files**.

Step 3   Double-click **Organizations**.

Step 4   Select the organization to which director1 and director2 belong and click **OK**.

Step 5   Double-click **Hosts**.

Step 6   Add both director1 and director2 and click **OK**.

Step 7   Double-click **Routes**.

Step 8   Add the following information about both director1 and director2:

- Host name

- Connection number

- IP address

- UDP port number (45000)

- A reserved Type, which should always be 1

- Heartbeat, an amount in seconds

Step 9   Click **OK**.

Step 10   Double-click **Authorizations**.

Step 11   Make sure that director1 and director2 each have the following permissions, at minimum:

- Get

- Getbulk

Step 12   Click **OK**.

Step 13   Apply your changes by selecting the transient configuration and clicking **Apply**.

The next step is to configure director1 and director2 to forward their alarms to director3 by using nrConfigure:

Step 1   On the Director interface, click the director1 icon and click **Configure** on the **Security** menu.

Step 2   On nrConfigure, click **Add Host** on the **File** menu.

Step 3   Read the instructions and click **Next**.

Step 4   Select the organization name to which director3 belongs.

Step 5   Type in director3's Host name, Host ID, and Host IP address in the appropriate fields.

Step 6   Click **Next**.

Step 7   Select **Forward alarms to secondary Director**.

Step 8   Click **Next**.

Step 9   Click **Finish**.

Step 10   Repeat the preceding steps for director2.

If needed, you can configure the level of alarms sent to director3:

Step 1   On director1's interface, click **Configure** on the **Security** menu.

Step 2   Double-click **Director Forwarding**.

Step 3   Click the **Forwarding** tab.

An entry should exist for *loggerd* on director1 and *smid* for director3.

Step 4   To change the level of alarms sent to director3, select the director3 entry and click **Modify**.

Step 5   For **Minimum Level**, change the minimum alarm level.

Step 6   Click **OK**.

Step 7   Apply your changes by selecting the transient configuration and clicking **Apply**.

Step 8   Repeat the preceding steps for director2, if desired.

The preceding procedures write DupDestination entries in the /usr/nr/etc/smid.conf files for both director1 and director2 (see Example 3-32 and Example 3-33). These DupDestination tokens provide information on where to send duplicate alarm information—in this case, director3. Notice that in each case, only alarms that are level 3 or higher are being forwarded.

Example 3-32   DupDestination Entry in director1's /usr/nr/etc/smid.conf

```
DupDestination director3.xyzcorp smid 3 ERRORS,COMMANDS,EVENTS,IPLOGS
```

Example 3-33   DupDestination Entry in director2's /usr/nr/etc/smid.conf

```
DupDestination director3.xyzcorp smid 3 ERRORS,COMMANDS,EVENTS,IPLOGS
```

Common Problems and Troubleshooting

The first problem encountered in this scenario is duplicate alarms being sent to director3 (172.16.5.50). This duplication is occurring because sensor2 (10.2.1.100) is sending alarm data to both director1 and director2, which are in turn sending level three alarms and higher to director3.

The way to solve this problem is to use nrConfigure to edit sensor2's routes information:

Step 1   On the Director interface, click the sensor2 icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version, double-click **System Files**.

Step 3   Double-click **Routes**.

Step 4   Select the director2.xyzcorp entry and click **Modify**.

Step 5   Change the priority of the route to **2**.

Step 6   Click **OK**.

Step 7   Select the newly created transient version and click **Apply**.

The secondary route for director2.xyzcorp is to be used only when the route to director1 fails.

You can verify this change by viewing the routes file on the Sensor. It should look like Example 3-34.

Example 3-34   Edited /usr/nr/etc/routes File on sensor2

```
director1.xyzcorp 1 10.5.1.50 45000 1
director2.xyzcorp 2 10.6.1.50 45000 1
```

The second problem arises when security personnel try to use director3 (172.16.5.50) to act on alarm information sent to it by director1 and director2. director3, in it's role as "top-level" Director host of the tiered hierarchy, is only passively receiving alarms, and cannot act on the alarms because it has no entries in its hosts and routes files for the three Sensors. Additionally, director3 has no authority to make changes to any of these Sensors' configuration files or execute commands on them.

First, use nrConfigure to add the each Sensor's information to director3's hosts and routes files:

Step 1   On the Director interface, click the director3 icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version, double-click **System Files**.

Step 3   Double-click **Hosts**.

Step 4   Use the **Add** button to add the Name, Organization Name, and Host ID for sensor1, sensor2, and sensor3, one at a time.

Step 5   Click **OK** to close the **Hosts** dialog box.

Step 6   Double-click **Routes**.

Step 7   Use the **Add** button to add the Name, Connection Number, IP Address, Port Number, and Type for sensor1, sensor2, and sensor3, one at a time.

Step 8   Click **OK** to close the **Routes** dialog box.

Step 9   Select the newly created transient version and click **Apply**.

The hosts and routes files on director3 should look like Example 3-35 and Example 3-36.

Example 3-35   Edited /usr/nr/etc/hosts File on director3

```
$ more /usr/nr/etc/hosts
30.500 localhost
30.500 director3.xyzcorp
20.500 director2.xyzcorp
10.500 director1.xyzcorp
100.500 sensor1.xyzcorp
200.500 sensor2.xyzcorp
300.500 sensor3.xyzcorp
```

Example 3-36   Edited /usr/nr/etc/routes File on director3

```
$ more /usr/nr/etc/routes
director1.xyzcorp 1 10.5.1.50 45000 1
director2.xyzcorp 1 10.6.1.50 45000 1
sensor1.xyzcorp 1 10.1.1.100 45000 1
sensor2.xyzcorp 1 10.2.1.100 45000 1
sensor3.xyzcorp 1 10.3.1.100 45000 1
```

Next, use nrConfigure to allow director3 to execute commands and make configuration changes on each Sensor:

Step 1   On the Director interface, click the sensor1 icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version, double-click **System Files**.

Step 3   Double-click **Authorizations**.

Step 4   Click **Add**.

Step 5   Ensure that Get, Get Bulk, Set, Unset, and Execute are all set to **Yes**.

Step 6   Click **OK** to close the **Authorizations** dialog box.

Step 7   Select the newly created transient version and click **Apply**.

Step 8   Repeat Steps 1 through 7 for sensor2 and sensor3.

The preceding process writes entries to each Sensor's auths files (see Example 3-37).

Example 3-37   Entries in a /usr/nr/etc/auths File

```
$ more /usr/nr/etc/auths
director3.xyzcorp  GET,GETBULK,SET,UNSET,EXEC
```

The final task is to add director3 to each Sensor's hosts and routes information, using nrConfigure:

Step 1   On the Director interface, click the sensor1 icon and click **Configure** on the **Security** menu.

Step 2   In the current configuration version, double-click **System Files**.

Step 3   Double-click **Hosts**.

Step 4   Use the **Add** button to add the Name, Organization Name, and Host ID for director3.

Step 5   Click **OK** to close the **Hosts** dialog box.

Step 6   Double-click **Routes**.

Step 7   Use the **Add** button to add the Name, Connection Number, IP Address, Port Number, and Type for director3.

Step 8   Click **OK** to close the **Routes** dialog box.

Step 9   Select the newly created transient version and click **Apply**.

Step 10   Repeat Steps 1 through 9 for sensor2 and sensor3.

Resources and Recommended Reading

This appendix contains the following listings of resources on intrusion detection and network security:

- Printed Resources
- Online Resources

Printed Resources

Amoroso, E. G. *Intrusion Detection: An Introduction to Internet Surveillance, Correlations, Traps, Trace Back, and Response*. Intrusion Net Books, 1999. ISBN: 0966670078.

Barnard, R. L. *Intrusion Detection Systems*. Butterworth-Heinemann, 1988. ISBN: 0750694270.

Denning, D. *CSI Manager's Guide to Cyberspace Attacks and Countermeasures*. Computer Security Institute, 1997.

Escamilla, T. *Intrusion Detection: Network Security Beyond the Firewall*. John Wiley & Sons, 1998. ISBN: 0471290009.

Forte, D. "Intrusion-Detection Systems: Guaranteeing the Safety of a Network Beyond Using a Firewall." *;login:*, Volume 24, Number 1: February 1999.

Garfinkel, S. and G. Spafford. *Practical UNIX and Internet Security*. O'Reilly and Associates, Inc., 1996. ISBN: 1565921488.

Messmer, E. "Intrusion-Detection Tools to Stop Hackers Cold." *Network World*: February 1999.

Mukherjee, B., L. T. Heberlein, and K. N. Levitt. "Network Intrusion Detection." *IEEE Network*: May/June 1994.

Northcutt, S. *Foundations of Intrusion Detection*. SANS Institute, 1998. (Orderable from the SANS web site: http://www.sansstore.org)

Northcutt, S. *Intrusion Detection—The Big Picture*. SANS Institute, 1999. (Orderable from the SANS web site: http://www.sansstore.org)

Puketza, N., M. Chung, R. A. Olsson, and B. Mukherjee. "A Software Platform for Testing Intrusion Detection Systems." *IEEE Software*: September/October 1997.

Online Resources

SANS Institute. "SANS Network Security Roadmap." http://www.sans.org/roadmap.htm

SANS Institute. "How to Build a Successful Security Infrastructure." http://www.sans.org/securityinfra.htm

Computer Operations, Audit, and Security Technology (COAST). "Introduction to Intrusion Detection." http://www.cs.purdue.edu/coast/intrusion-detection/introduction.html

"On Computer and Network Security." *NetSurfer Focus*, Volume 1, Number 1: April 1995. http://www.netsurf.com/nsf/v01/01/nsf.01.01.html

Cisco Systems, Inc. NetRanger Product Information. http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/

Cisco Systems, Inc. NetSonar Product Information. http://www.cisco.com/warp/public/cc/cisco/mkt/security/nsonar/

Computer Security Institute. "The Cost of Computer Crime." http://www.gocsi.com/losses.htm

Computer Security Institute. Intrusion Detection Resources. http://www.gocsi.com/intrusion.htm

Computer Security Institute and FBI. *1999 CSI-FBI Survey Results*. http://www.gocsi.com/summary.htm

Freedman, D., and C. Mann. "Cracker." *U.S. News and World Report*: June 2, 1997. http://www.usnews.com/usnews/issue/970602/2crac.htm

Power, R. "CSI Roundtable: Experts Discuss Present and Future Intrusion Detection Systems." http://www.gocsi.com/roundtable.htm