CSIDS

Cisco Secure Intrusion Detection

Version 4.0

Student Guide

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

Credits

Lead Course Developer	*Jeanne Jackson*
Contributing Course Developer	*Jagdeep S. Kang*
Manager, Documentation	*Ed Rivera*
Additional Contributors	*Danny Rodriguez, Craig Hyps, Bill Chadwick, Leon Katcharian, Jeff Platzer, Ramona Boyd, Jim Kasper, Earl Carter, and Steven Hanna*

About the Course Developers

Jeanne Jackson is an Education Specialist at Cisco Systems, Inc. where she designs and develops training on Cisco's network security products. Her experience before coming to Cisco includes developing and delivering training for Microsoft products. She has over twenty years of experience in the education field as a technical instructor, instructor-mentor, technical course developer, teacher of French and English, and public school administrator.

Jeanne graduated from the University of Texas at Arlington with a BA in French and holds a Master's degree in Public School Administration from North Texas State University. Her technical certifications include CCNA, Cisco Security Specialist I, Cisco Certified Security Professional (CCSP), Microsoft Certified Systems Engineer, and Microsoft Certified Trainer.

Jagdeep S. Kang is currently a consultant with the Cisco Internet Learning and Solutions Group. He focuses on network enterprise management software and has more than five years of experience in internetworking. His technical certifications include CCSP, CCNP and MCSE. Jagdeep completed his Masters at Ohio State University and holds an MBA from India.

Table of Contents

CISCO INTRUSION DETECTION SYSTEM DEVICE MANAGER AND EVENT VIEWER 10-1

ENTERPRISE INTRUSION DETECTION SYSTEM MANAGEMENT 11-1

SENSOR CONFIGURATION 12-1

CISCO INTRUSION DETECTION SYSTEM ALARMS AND SIGNATURES 13-1

Course Introduction

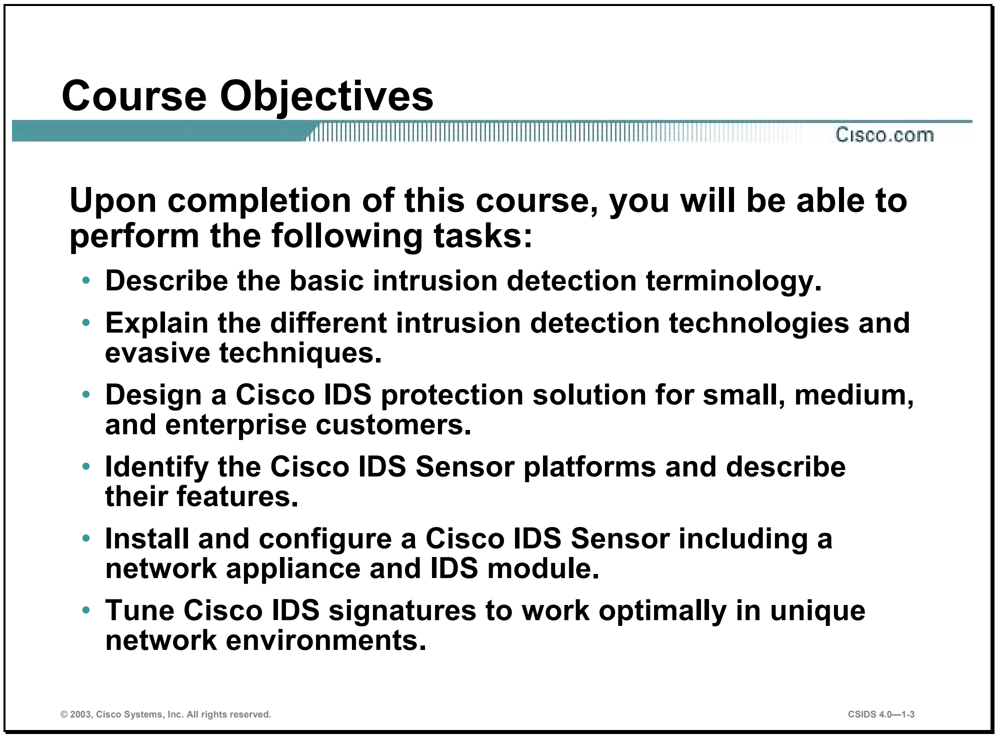
Overview

This chapter includes the following topics:

- Course objectives
- Course agenda
- Participant responsibilities
- General administration
- Graphic symbols
- Participant introductions
- Cisco security career certifications
- Lab topology overview

Course Objectives

This section introduces the course and the course objectives.



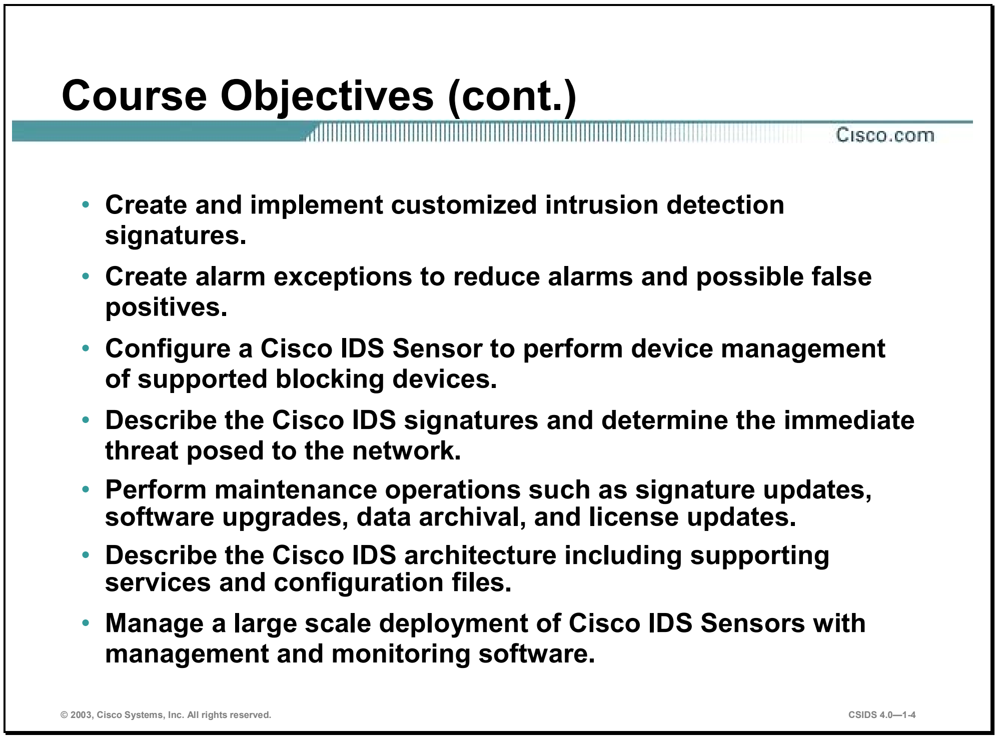
Course Objectives

Cisco.com

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

- **Describe the basic intrusion detection terminology.**
- **Explain the different intrusion detection technologies and evasive techniques.**
- **Design a Cisco IDS protection solution for small, medium, and enterprise customers.**
- **Identify the Cisco IDS Sensor platforms and describe their features.**
- **Install and configure a Cisco IDS Sensor including a network appliance and IDS module.**
- **Tune Cisco IDS signatures to work optimally in unique network environments.**

CSIDS 4.0—1-3

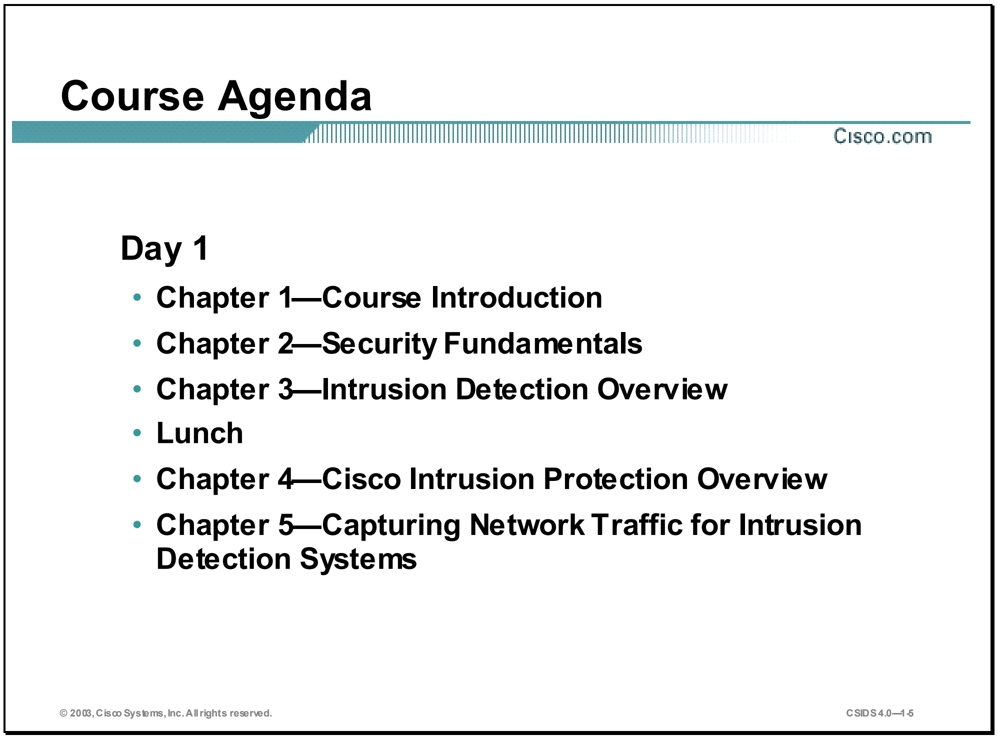


Course Objectives (cont.)

Cisco.com

- **Create and implement customized intrusion detection signatures.**
- **Create alarm exceptions to reduce alarms and possible false positives.**
- **Configure a Cisco IDS Sensor to perform device management of supported blocking devices.**
- **Describe the Cisco IDS signatures and determine the immediate threat posed to the network.**
- **Perform maintenance operations such as signature updates, software upgrades, data archival, and license updates.**
- **Describe the Cisco IDS architecture including supporting services and configuration files.**
- **Manage a large scale deployment of Cisco IDS Sensors with management and monitoring software.**

CSIDS 4.0—1-4



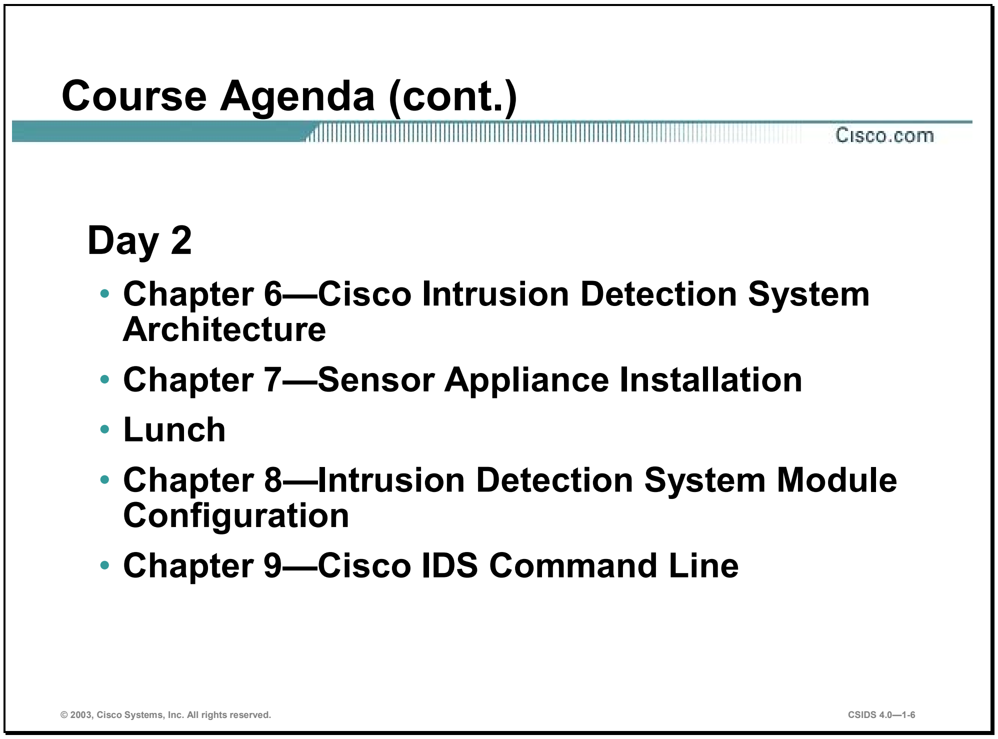
Course Agenda

Cisco.com

Day 1

- Chapter 1—Course Introduction
- Chapter 2—Security Fundamentals
- Chapter 3—Intrusion Detection Overview
- Lunch
- Chapter 4—Cisco Intrusion Protection Overview
- Chapter 5—Capturing Network Traffic for Intrusion Detection Systems

CSIDS 4.0—1-5



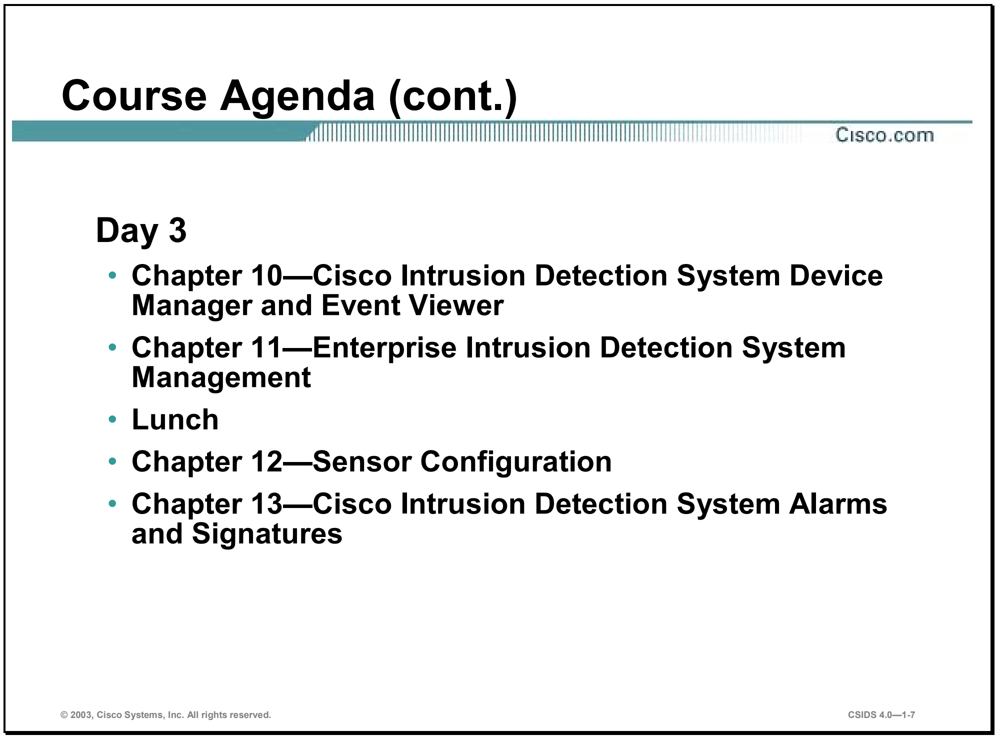
Course Agenda (cont.)

Cisco.com

Day 2

- Chapter 6—Cisco Intrusion Detection System Architecture
- Chapter 7—Sensor Appliance Installation
- Lunch
- Chapter 8—Intrusion Detection System Module Configuration
- Chapter 9—Cisco IDS Command Line

CSIDS 4.0—1-6

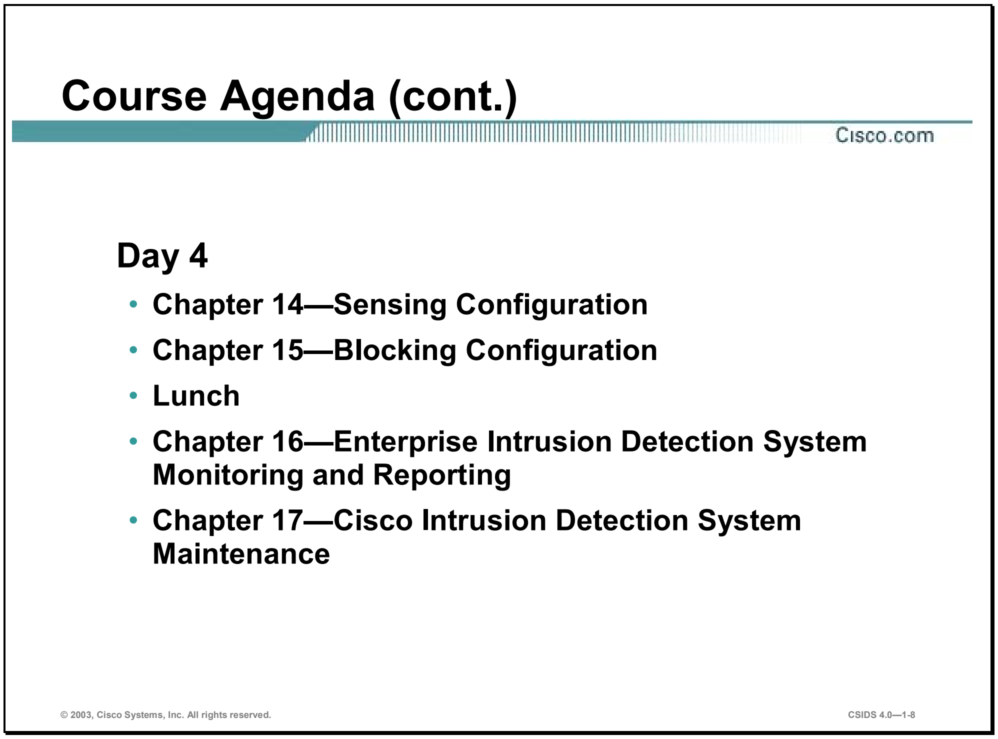


Course Agenda (cont.)

Day 3

- Chapter 10—Cisco Intrusion Detection System Device Manager and Event Viewer
- Chapter 11—Enterprise Intrusion Detection System Management
- Lunch
- Chapter 12—Sensor Configuration
- Chapter 13—Cisco Intrusion Detection System Alarms and Signatures

CSIDS 4.0—1-7

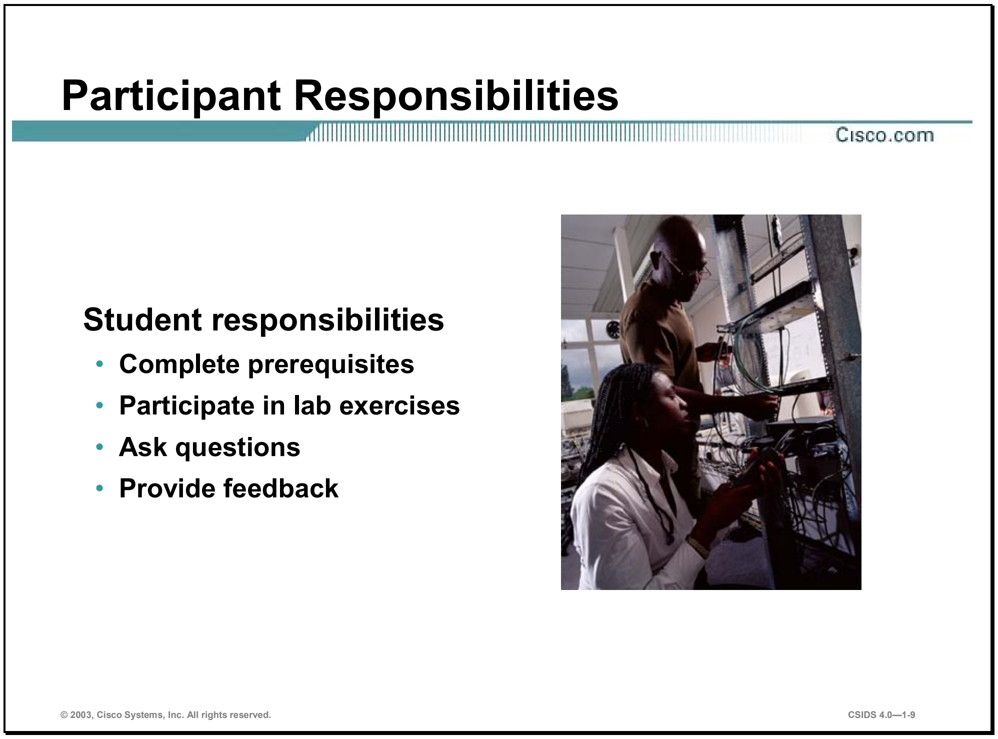


Course Agenda (cont.)

Day 4

- Chapter 14—Sensing Configuration
- Chapter 15—Blocking Configuration
- Lunch
- Chapter 16—Enterprise Intrusion Detection System Monitoring and Reporting
- Chapter 17—Cisco Intrusion Detection System Maintenance

CSIDS 4.0—1-8



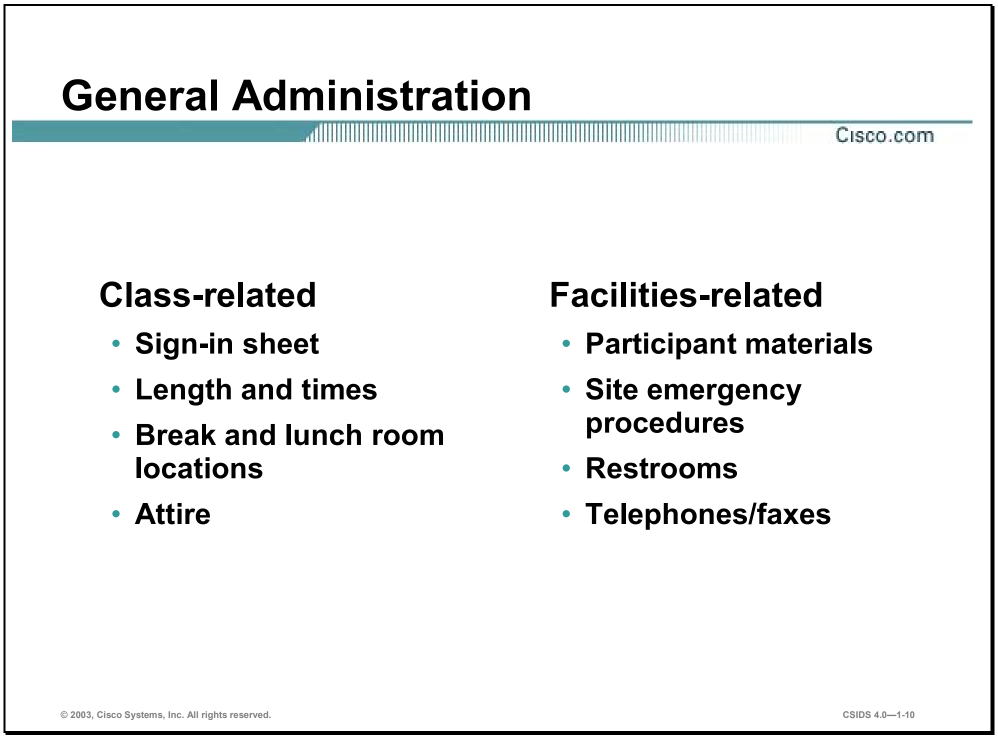
Participant Responsibilities

Cisco.com

Student responsibilities

- Complete prerequisites
- Participate in lab exercises
- Ask questions
- Provide feedback

CSIDS 4.0—1-9



General Administration

Cisco.com

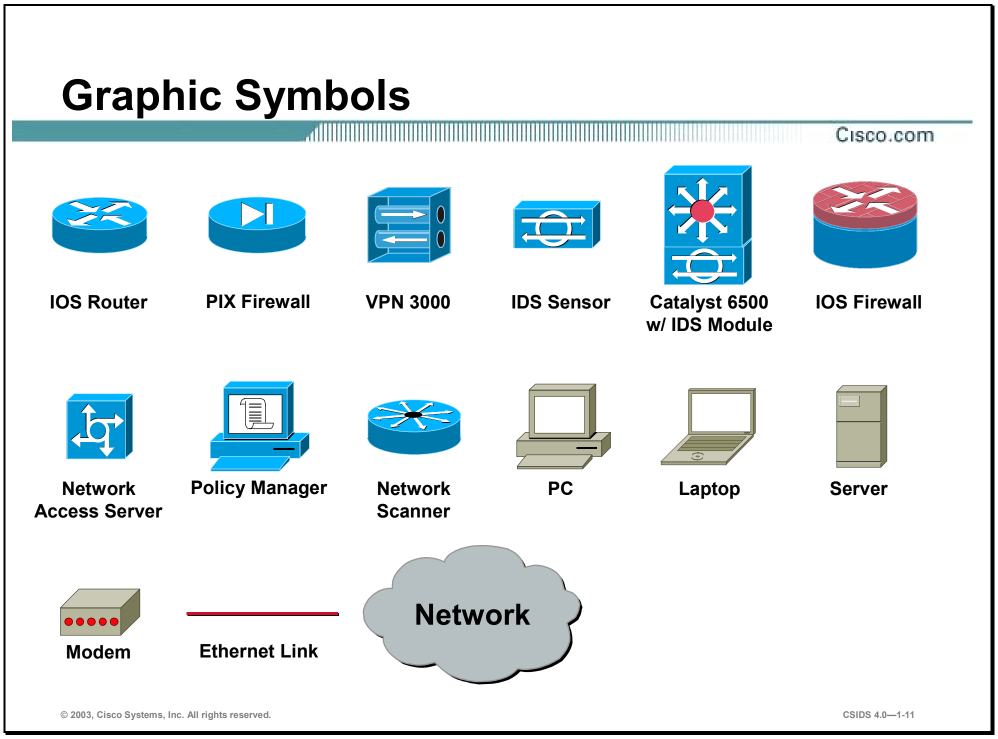
Class-related

- Sign-in sheet
- Length and times
- Break and lunch room locations
- Attire

Facilities-related

- Participant materials
- Site emergency procedures
- Restrooms
- Telephones/faxes

CSIDS 4.0—1-10



Graphic Symbols

Cisco.com

IOS Router	PIX Firewall	VPN 3000	IDS Sensor	Catalyst 6500 w/ IDS Module	IOS Firewall
Network Access Server	Policy Manager	Network Scanner	PC	Laptop	Server
Modem	Ethernet Link	Network			

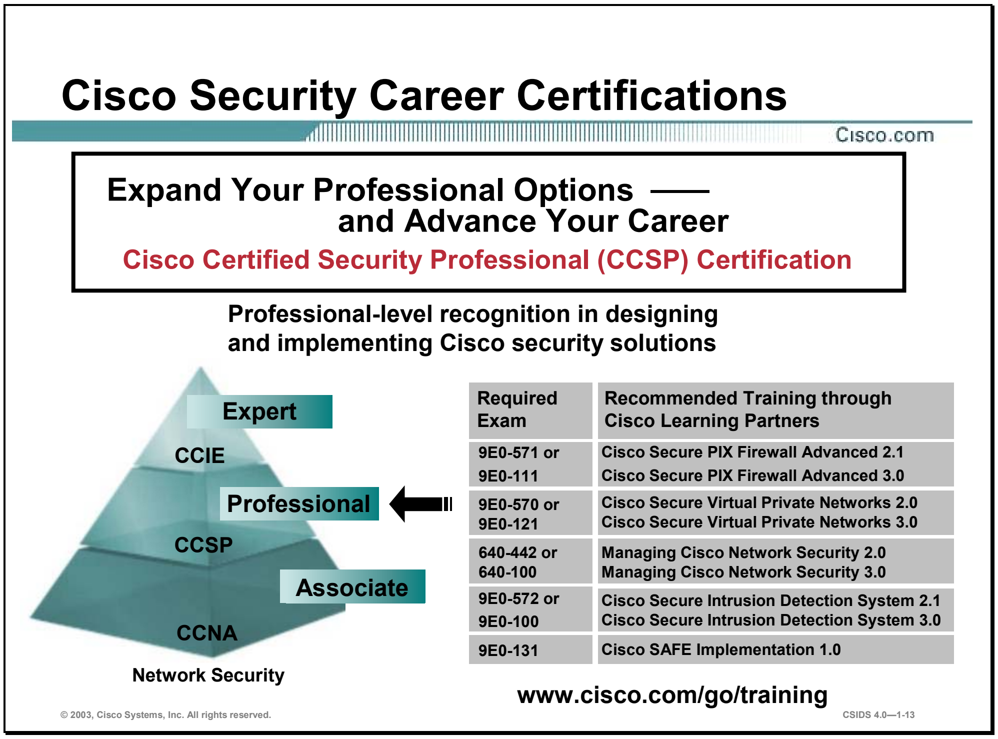
CSIDS 4.0—1-11

Participant Introductions

Cisco.com

- Your name
- Your company
- Pre-requisites skills
- Brief history
- Objective

CSIDS 4.0—1-12



Cisco Security Career Certifications

Cisco.com

Expand Your Professional Options —— and Advance Your Career

Cisco Certified Security Professional (CCSP) Certification

Professional-level recognition in designing and implementing Cisco security solutions

Expert

CCIE

Professional

CCSP

Associate

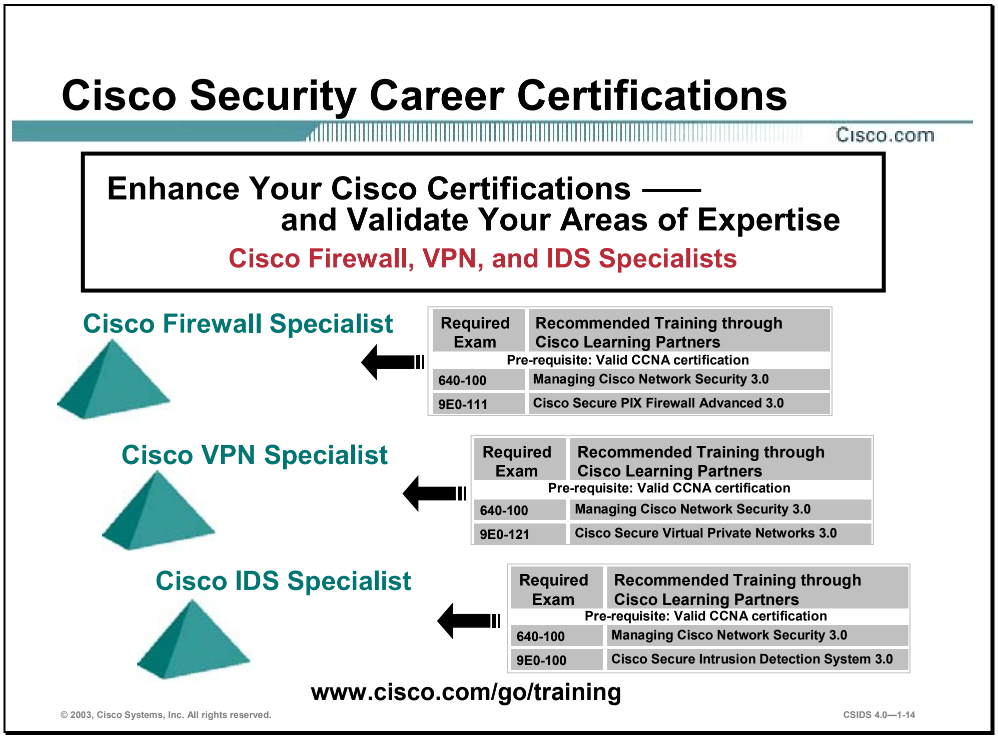
CCNA

Network Security

Required Exam	Recommended Training through Cisco Learning Partners
9E0-571 or 9E0-111	Cisco Secure PIX Firewall Advanced 2.1 Cisco Secure PIX Firewall Advanced 3.0
9E0-570 or 9E0-121	Cisco Secure Virtual Private Networks 2.0 Cisco Secure Virtual Private Networks 3.0
640-442 or 640-100	Managing Cisco Network Security 2.0 Managing Cisco Network Security 3.0
9E0-572 or 9E0-100	Cisco Secure Intrusion Detection System 2.1 Cisco Secure Intrusion Detection System 3.0
9E0-131	Cisco SAFE Implementation 1.0

www.cisco.com/go/training

CSIDS 4.0—1-13



Cisco Security Career Certifications

Cisco.com

Enhance Your Cisco Certifications —— and Validate Your Areas of Expertise

Cisco Firewall, VPN, and IDS Specialists

Cisco Firewall Specialist

Required Exam	Recommended Training through Cisco Learning Partners
Pre-requisite: Valid CCNA certification	
640-100	Managing Cisco Network Security 3.0
9E0-111	Cisco Secure PIX Firewall Advanced 3.0

Cisco VPN Specialist

Required Exam	Recommended Training through Cisco Learning Partners
Pre-requisite: Valid CCNA certification	
640-100	Managing Cisco Network Security 3.0
9E0-121	Cisco Secure Virtual Private Networks 3.0

Cisco IDS Specialist

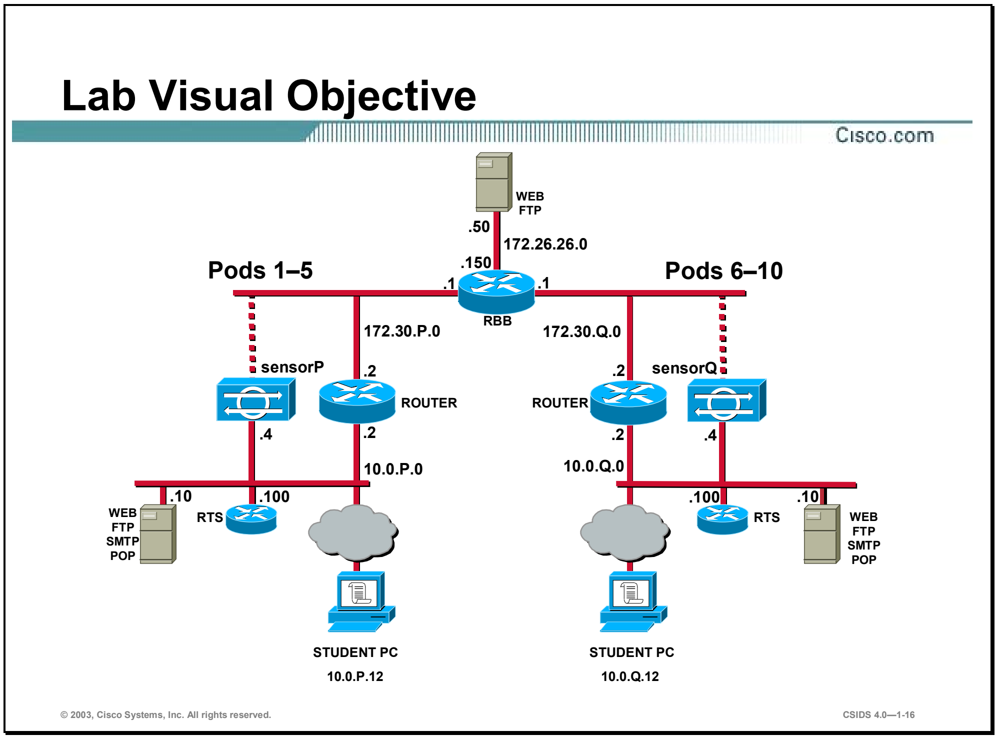
Required Exam	Recommended Training through Cisco Learning Partners
Pre-requisite: Valid CCNA certification	
640-100	Managing Cisco Network Security 3.0
9E0-100	Cisco Secure Intrusion Detection System 3.0

www.cisco.com/go/training

CSIDS 4.0—1-14

Lab Topology Overview

This section explains the lab topology that is used in this course.



Lab Visual Objective

CSIDS 4.0—1-16

Each pair of students will be assigned a pod. In general, you will be launching attacks between your pod (Pod **P**) and your assigned peer pod (Pod **Q**).

Note	The **P** in a command indicates your pod number. The **Q** in a command indicates the pod number of your peer.

2

Security Fundamentals

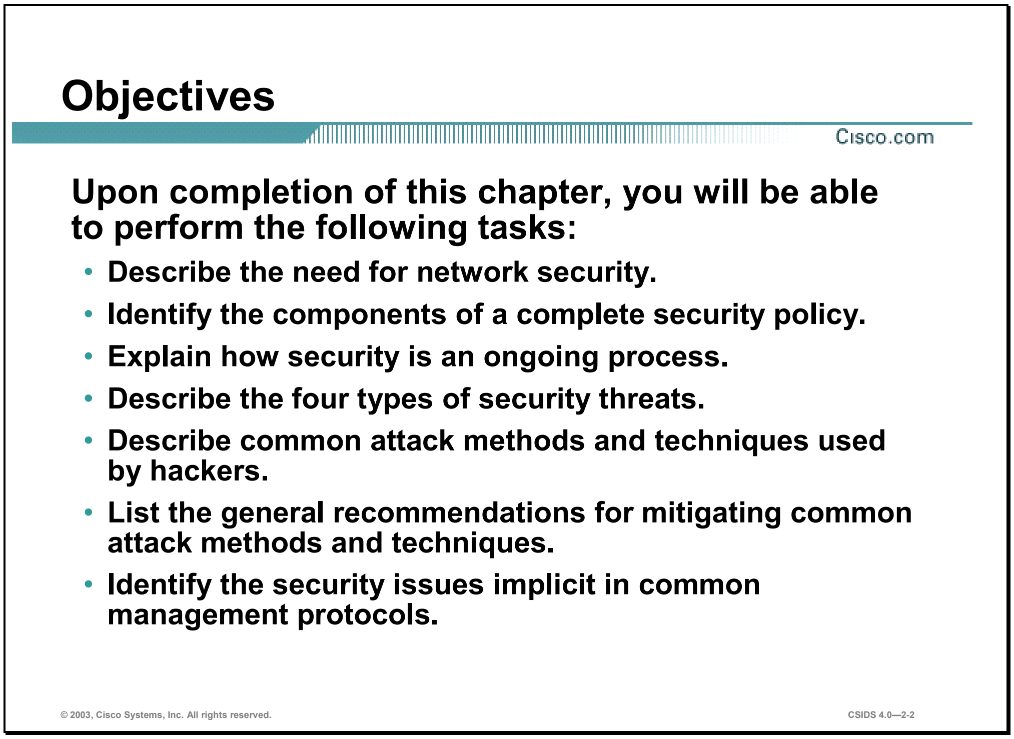
Overview

This chapter describes security fundamentals. It includes the following topics:

- Objectives
- Need for network security
- Network security policy
- The security wheel
- Network attack taxonomy
- Management protocols and functions
- Summary

Objectives

This section lists the chapter's objectives.



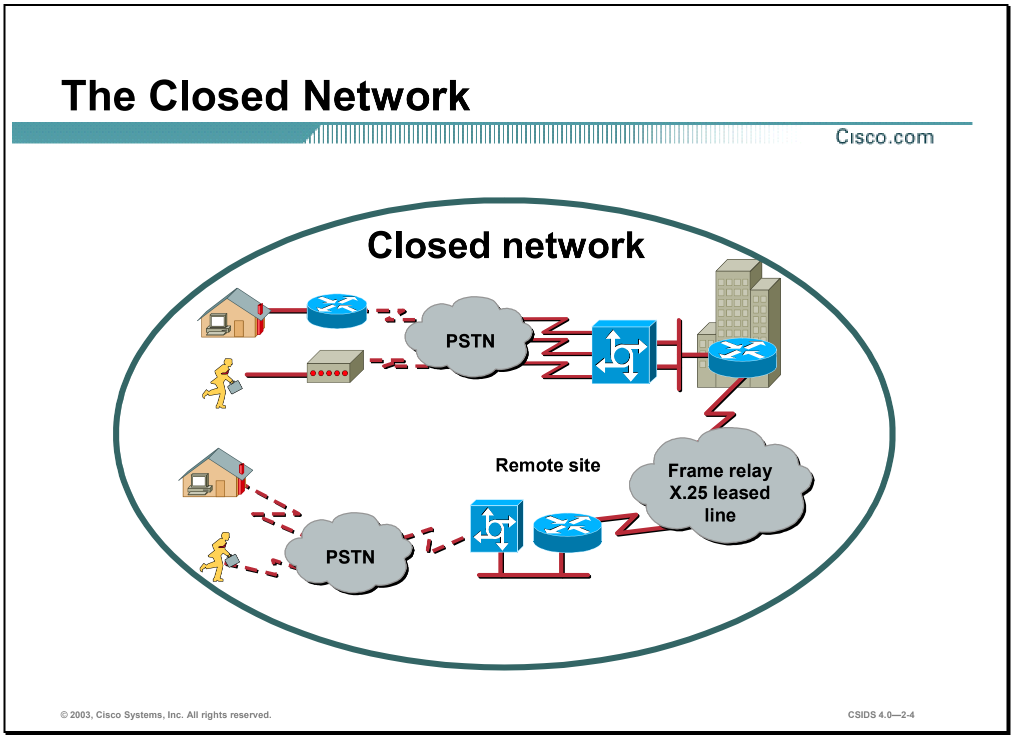
Objectives

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

- Describe the need for network security.
- Identify the components of a complete security policy.
- Explain how security is an ongoing process.
- Describe the four types of security threats.
- Describe common attack methods and techniques used by hackers.
- List the general recommendations for mitigating common attack methods and techniques.
- Identify the security issues implicit in common management protocols.

Need for Network Security

Over the past few years, Internet-enabled business, or e-business, has drastically improved companies' efficiency and revenue growth. E-business applications such as e-commerce, supply-chain management, and remote access enable companies to streamline processes, lower operating costs, and increase customer satisfaction. Such applications require mission-critical networks that accommodate voice, video, and data traffic, and these networks must be scalable to support increasing numbers of users and the need for greater capacity and performance. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. To combat those threats and ensure that e-business transactions are not compromised, security technology must play a major role in today's networks.



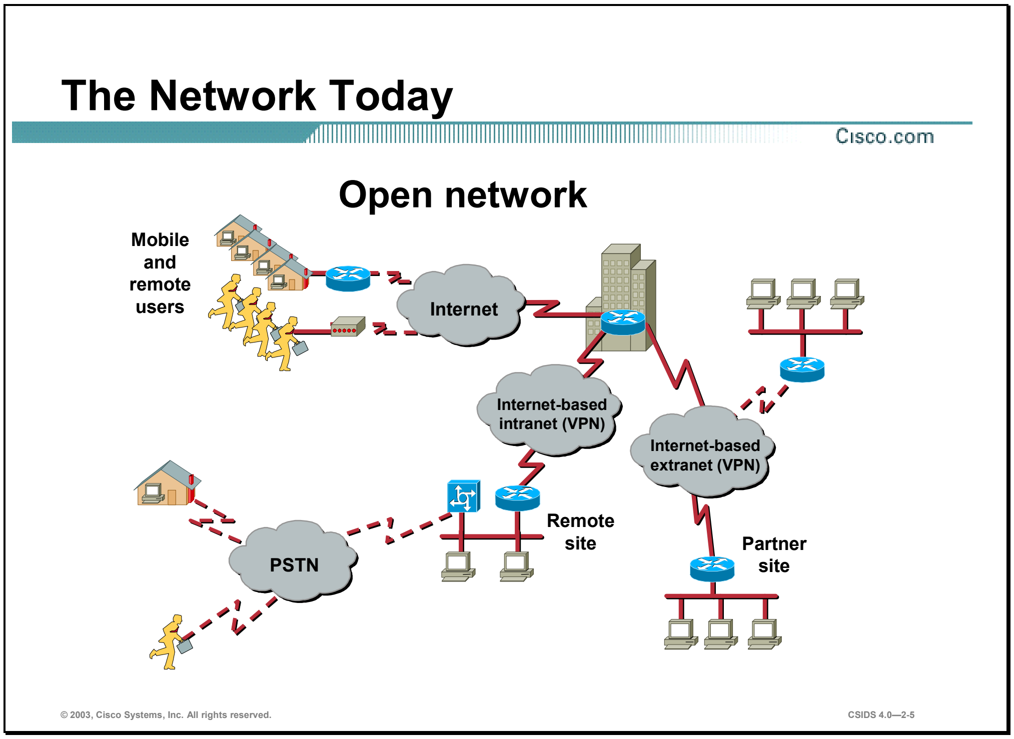
The Closed Network

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—2-4

The closed network typically consists of a network designed and implemented in a corporate environment, and provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because of no outside connectivity.

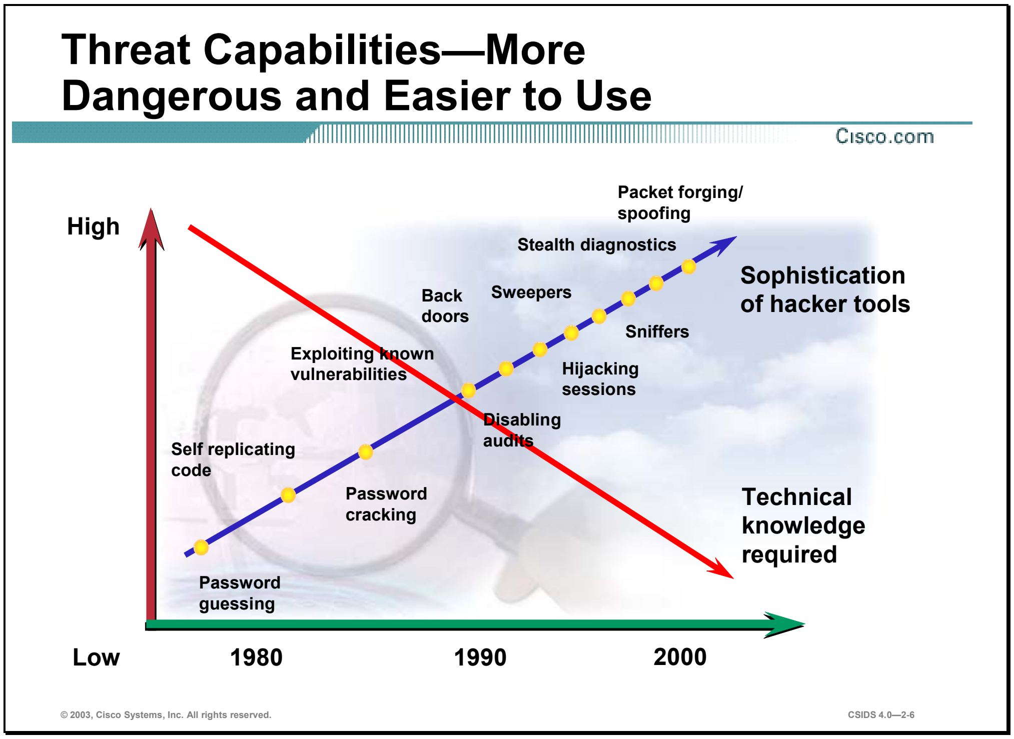


The Network Today

Open network

CSIDS 4.0—2-5

Networks of today are designed with availability to the Internet and public networks, which is a major requirement. Most of today’s networks have several access points to other networks both public and private; therefore, securing these networks has become fundamentally important.

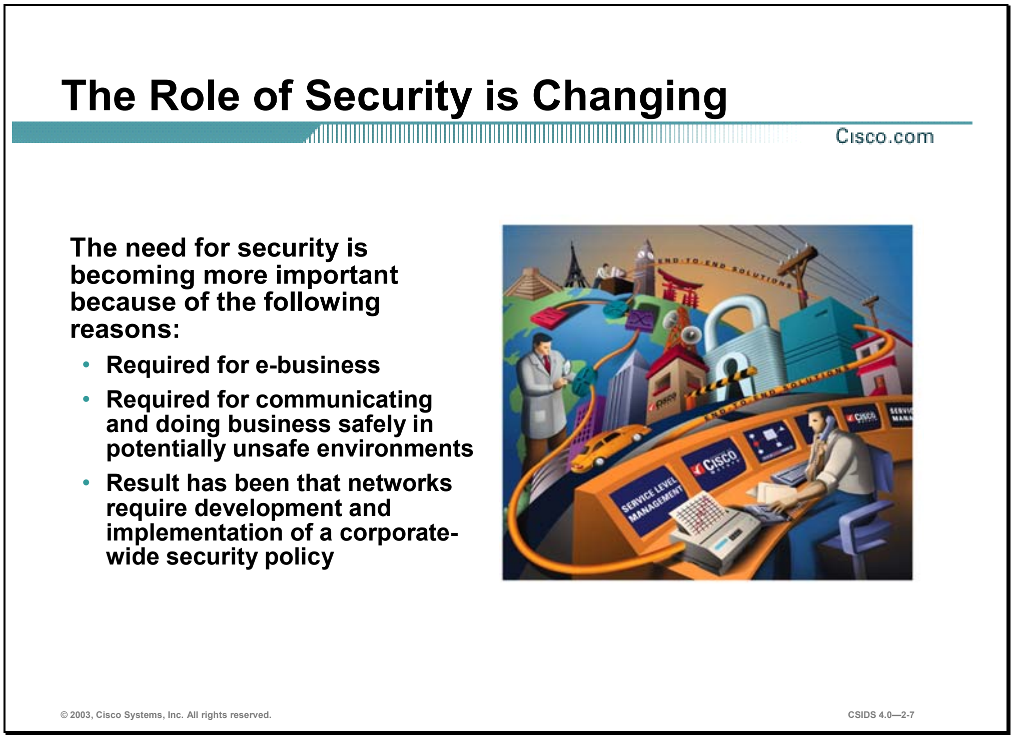


Threat Capabilities—More Dangerous and Easier to Use

Cisco.com

CSIDS 4.0—2-6

With the development of large open networks there has been a huge increase in security threats in the past twenty years. Not only have hackers discovered more vulnerabilities, but the tools used and technical knowledge required to hack a network have become simpler. There are downloadable applications available that require little or no hacking knowledge to implement. There are also inherent applications for troubleshooting a network that when used improperly can pose severe threats.



The Role of Security is Changing

Cisco.com

The need for security is becoming more important because of the following reasons:

- **Required for e-business**
- **Required for communicating and doing business safely in potentially unsafe environments**
- **Result has been that networks require development and implementation of a corporate-wide security policy**

CSIDS 4.0—2-7

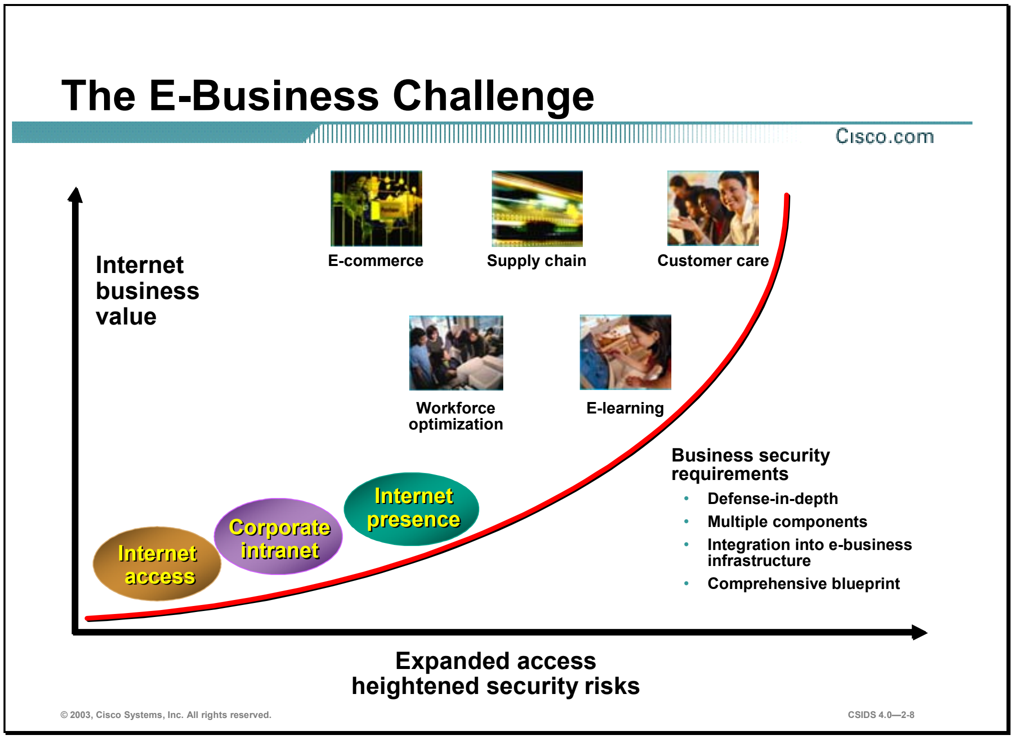
Security has moved to the forefront of network management and implementation. It is necessary for the survival of many businesses to allow open access to network resources, and ensure that the data and resources are as secure as possible.

The need for security is becoming more important because of the following:

- Required for e-business—The importance of e-business and the need for private data to traverse public networks has increased the need for network security.

- Required for communicating and doing business safely in potentially unsafe environments—Today’s business environment requires communication with many public networks and systems which increases the need for as much security as is possible when this type of communication is required.

- Networks require development and implementation of a corporate-wide security policy—Establishing a security policy should be the first step in migrating a network to a secure infrastructure.



The E-Business Challenge

Cisco.com

Internet business value

E-commerce

Supply chain

Customer care

Workforce optimization

E-learning

Internet access

Corporate intranet

Internet presence

Business security requirements

- Defense-in-depth
- Multiple components
- Integration into e-business infrastructure
- Comprehensive blueprint

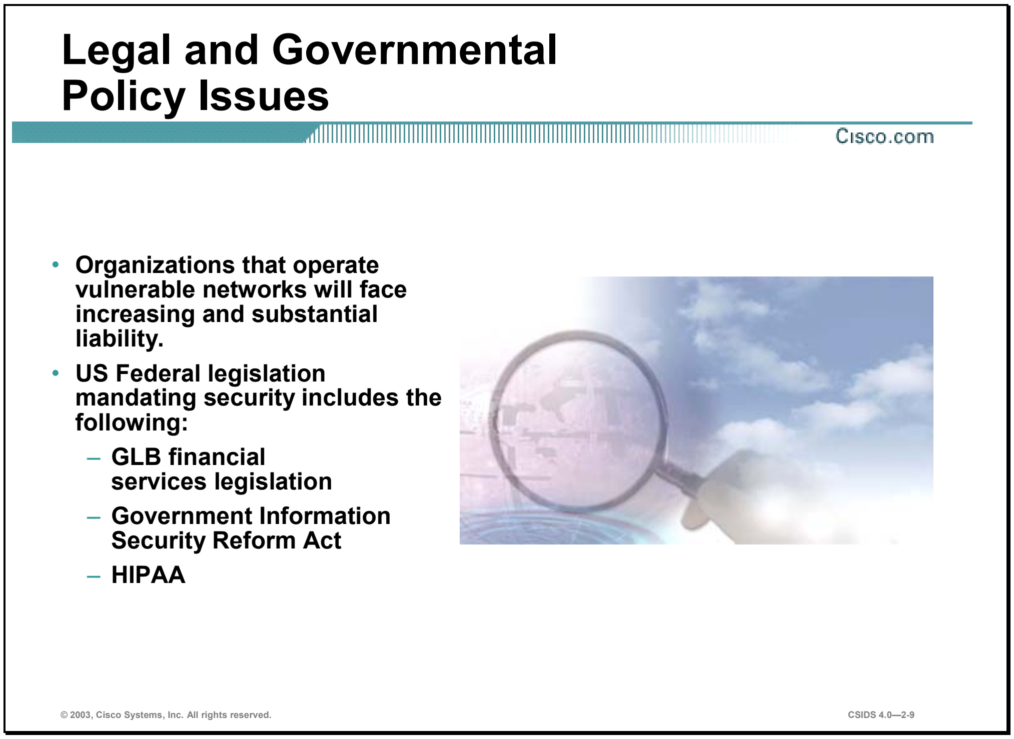
Expanded access heightened security risks

CSIDS 4.0—2-8

Security must be a fundamental component of any e-business strategy. As enterprise network managers open their networks to more users and applications, they also expose these networks to greater risk. The result has been an increase in the business security requirements.

The Internet has radically shifted expectations of companies’ abilities to build stronger relationships with customers, suppliers, partners, and employees. Driving companies to become more agile and competitive, e-business is giving birth to exciting new applications for e-commerce, supply-chain management, customer care, workforce optimization, and e-learning—applications that streamline and improve processes, speed up turnaround times, lower costs, and increase user satisfaction.

E-business requires mission-critical networks that accommodate ever-increasing constituencies and demands for greater capacity and performance. These networks also need to handle voice, video, and data traffic as networks converge into multiservice environments.



Legal and Governmental Policy Issues

- Organizations that operate vulnerable networks will face increasing and substantial liability.
- US Federal legislation mandating security includes the following:
  - GLB financial services legislation
  - Government Information Security Reform Act
  - HIPAA

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—2-9

The legal ramifications of breaches in data confidentiality and integrity can also be extremely costly for organizations. The US Government has enacted and is currently developing regulations to control the privacy of electronic information. The existing and pending regulations generally stipulate that organizations in violation could face a range of penalties. The following are some examples:

- Gramm-Leach Bliley (GLB) Act—Includes several privacy regulations for US financial institutions. These institutions could face a range of penalties from termination of their FDIC insurance to up to US $1 million in monetary penalties.

- Government Information Security Reform Act of 2000—Agencies must undergo annual self-assessments and independent assessments of their security practices and policies, which are required for submission.

- The Health Insurance Portability and Accountability Act (HIPPA) of 1996 (Public Law 104-191)—Part of a broad Congressional attempt at incremental healthcare reform. The “administrative simplification” aspect of that law requires the United States Department of Health and Human Services (DHHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients. These standards are designed to do the following:

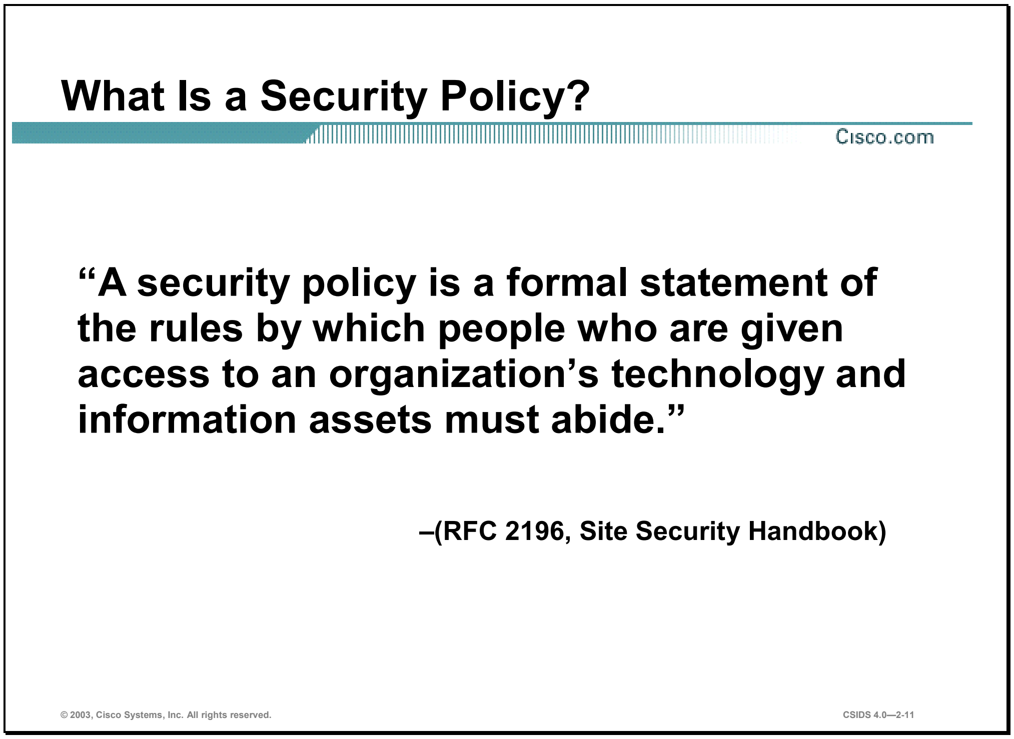
  - Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions

  - Protect the security and confidentiality of electronic health information

Even if an external hacker is the perpetrator of an attack, the company storing that information can potentially be found negligent by the courts if the information was not adequately safeguarded. Furthermore, companies that suffer breaches in data integrity might be required to defend against lawsuits initiated by customers who are negatively affected by the incorrect or offensive data and seek monetary or punitive damages.

Network Security Policy

A security policy can be as simple as an acceptable use policy for network resources or it can be several hundred pages in length and detail every element of connectivity and associated policies.



What Is a Security Policy?

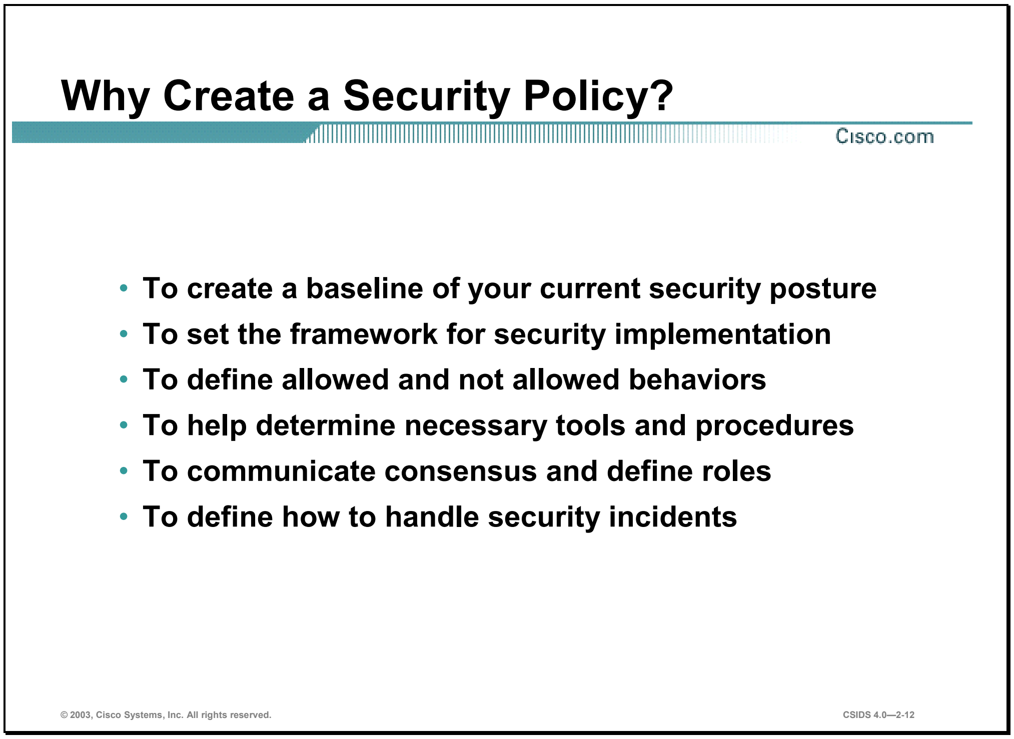
Cisco.com

“A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.”

–(RFC 2196, Site Security Handbook)

CSIDS 4.0—2-11

According to the Site Security Handbook (RFC 2196), “A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.” It further states, “A security policy is essentially a document summarizing how the corporation will use and protect its computing and network resources.”



Why Create a Security Policy?

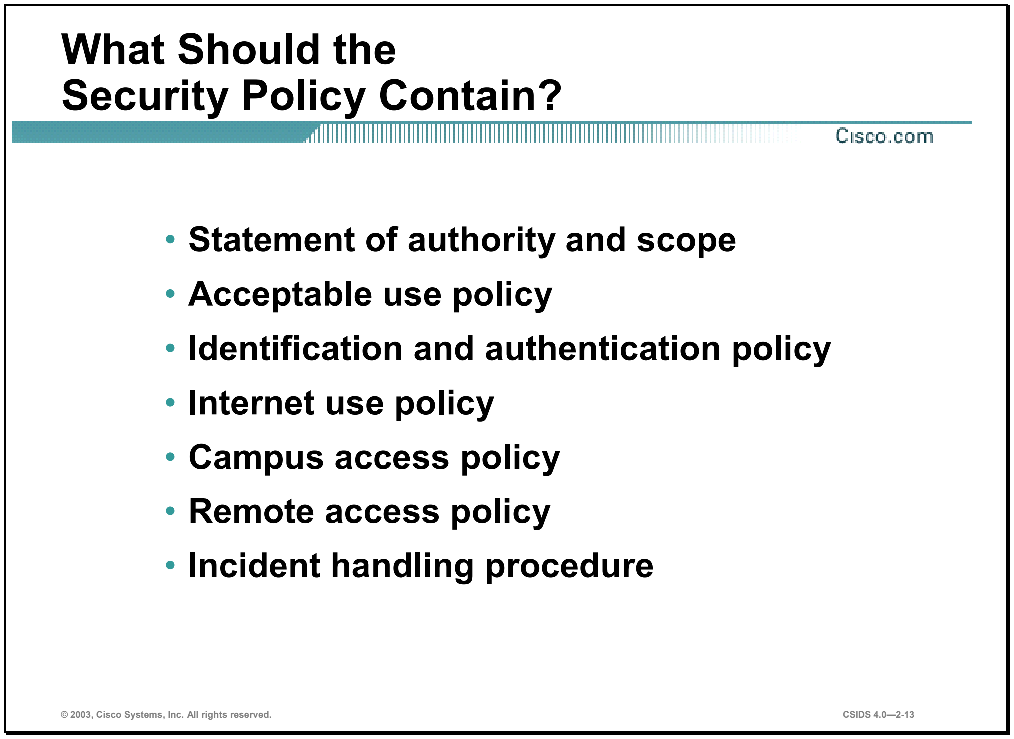
Cisco.com

- To create a baseline of your current security posture
- To set the framework for security implementation
- To define allowed and not allowed behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

CSIDS 4.0—2-12

Security policies provide many benefits and are worth the time and effort needed to develop them. Developing a security policy:

- Provides a process to audit existing network security.
- Provides a general security framework for implementing network security.
- Defines which behavior is and is not allowed.
- Helps determine which tools and procedures are needed for the organization.
- Helps communicate consensus among a group of key decision makers and define responsibilities of users and administrators.
- Defines a process for handling network security incidents.
- Enables global security implementation and enforcement. Computer security is now an enterprise-wide issue and computing sites are expected to conform to the network security policy.
- Creates a basis for legal action if necessary.



What Should the Security Policy Contain?

Cisco.com

- Statement of authority and scope
- Acceptable use policy
- Identification and authentication policy
- Internet use policy
- Campus access policy
- Remote access policy
- Incident handling procedure

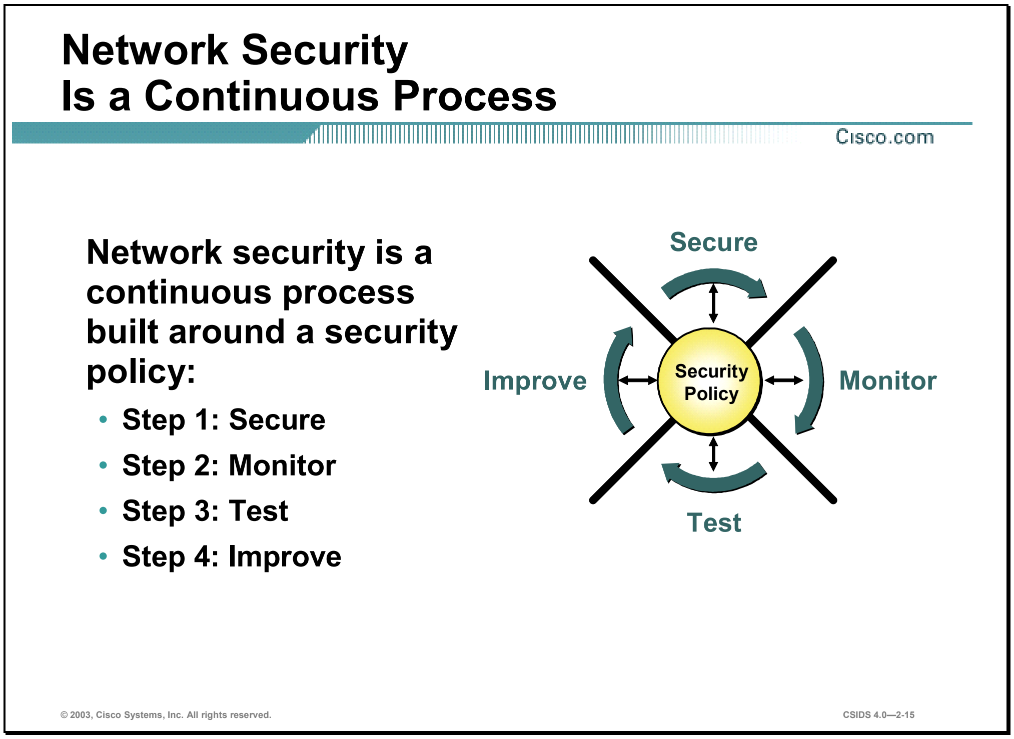
CSIDS 4.0—2-13

The following are some of the key policy components:

- Statement of authority and scope—This section specifies who sponsors the security policy and what areas the policy covers.
- Acceptable use policy—This section specifies what the company will and will not allow regarding its information infrastructure.
- Identification and authentication policy—This section specifies what technologies, equipment, or combination of the two the company will use to ensure that only authorized individuals have access to its data.
- Internet access policy—This section specifies what the company considers ethical and proper use of its Internet access capabilities.
- Campus access policy—This section specifies how on-campus users will use the company's data infrastructure.
- Remote access policy—This section specifies how remote users will access the company's data infrastructure.
- Incident handling procedure—This section specifies how the company will create an incident response team and the procedures it will use during and after and incident occurs.

The Security Wheel

Cisco is serious about network security, and about its implications for the critical infrastructures on which this and other developed nations depend. This section summarizes the view that network security is a continuous process.



Network Security Is a Continuous Process

Cisco.com

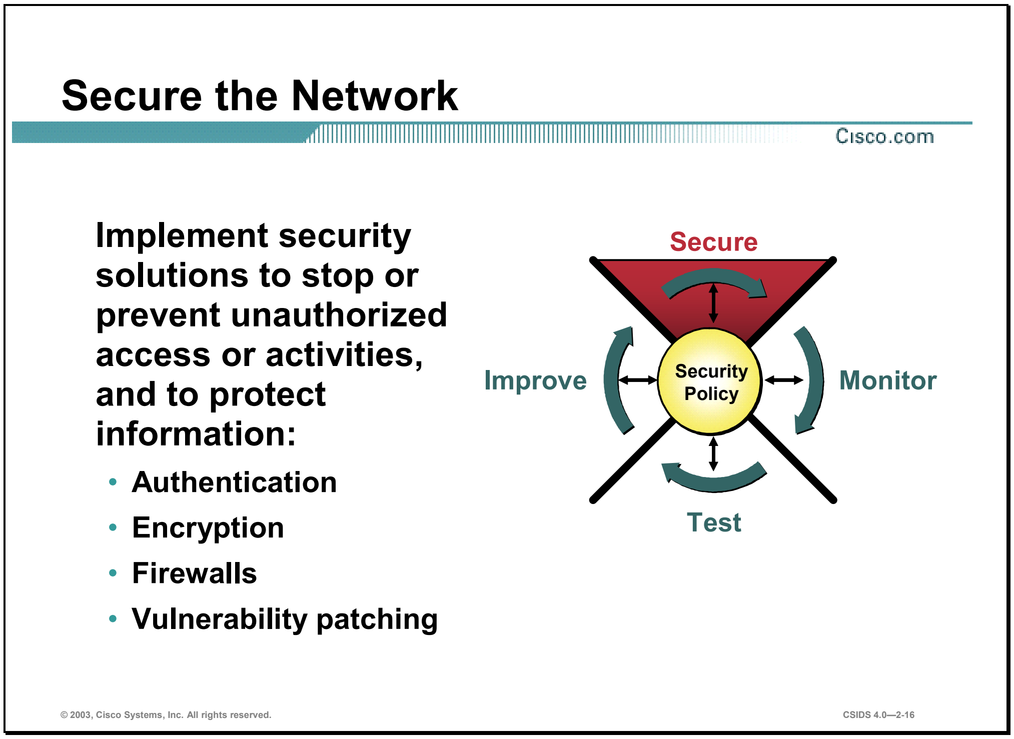
Network security is a continuous process built around a security policy:

- **Step 1: Secure**
- **Step 2: Monitor**
- **Step 3: Test**
- **Step 4: Improve**

CSIDS 4.0—2-15

After setting appropriate policies, a company or organization must methodically consider security as part of normal network operations. This could be as simple as configuring routers to not accept unauthorized addresses or services, or as complex as installing firewalls, intrusion detection systems, centralized authentication servers, and encrypted virtual private networks.

After developing a security policy, secure your network using a variety of point products (firewalls, intrusion detection, and so on.). 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.



Secure the Network

Cisco.com

Implement security solutions to stop or prevent unauthorized access or activities, and to protect information:

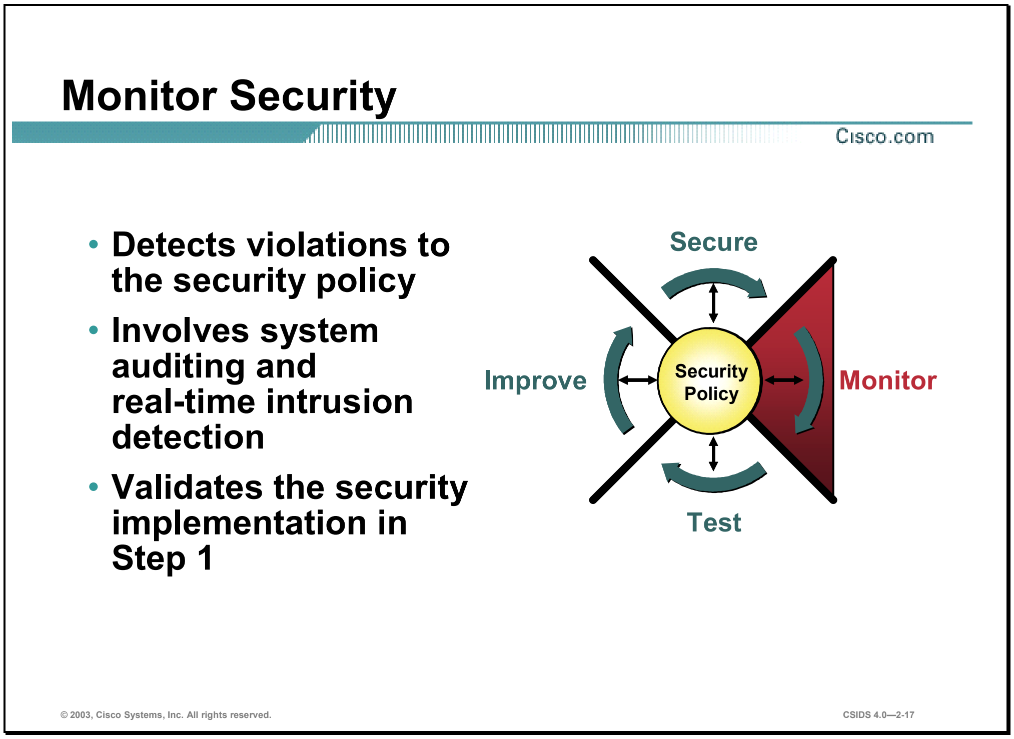
- **Authentication**
- **Encryption**
- **Firewalls**
- **Vulnerability patching**

Secure
Improve
Security Policy
Monitor
Test

CSIDS 4.0—2-16

The following are solutions identified to secure a network:

- Authentication—The recognition of each individual user, and the mapping of their identity, location, and the time to policy; and the authorization of their network services and what they can do on the network.
- Encryption—A method for ensuring the confidentiality, integrity, and authenticity of data communications across a network. The Cisco solution combines several standards, including the Data Encryption Standard (DES).
- Firewalls—A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.
- Vulnerability patching—The identification and patching of possible security “holes” that could compromise a network.



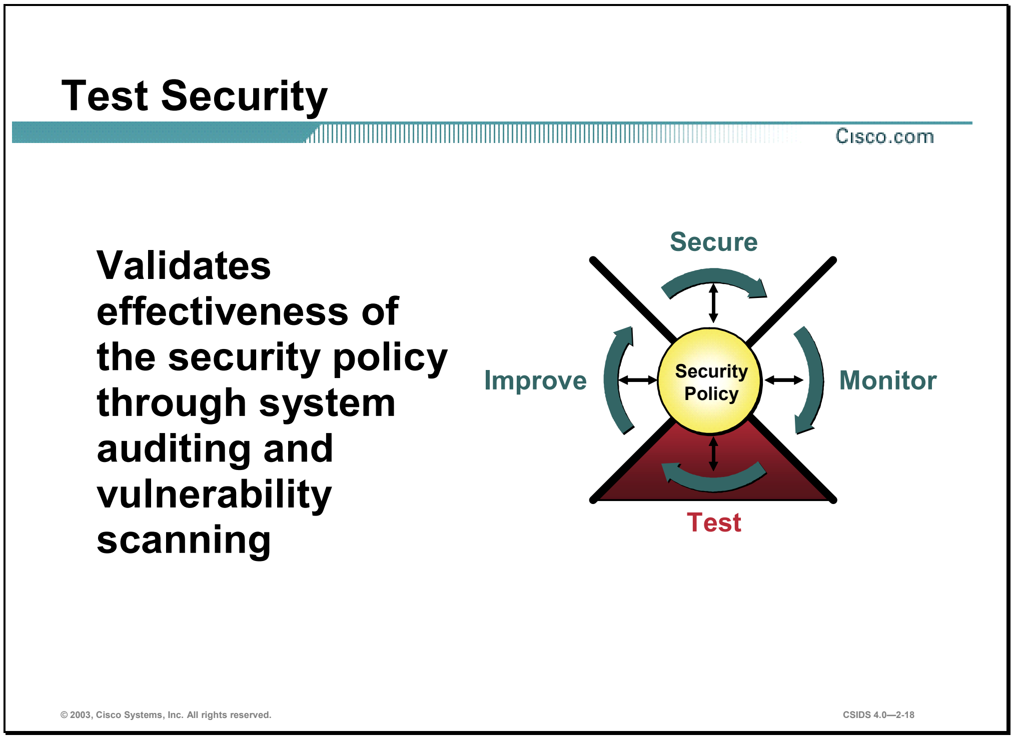
Monitor Security

Cisco.com

- Detects violations to the security policy
- Involves system auditing and real-time intrusion detection
- Validates the security implementation in Step 1

CSIDS 4.0—2-17

To ensure that a network remains secure, it is important to monitor the state of security preparation. Network vulnerability scanners can proactively identify areas of weakness, and IDSs can monitor and respond to security events as they occur. Using security monitoring solutions, organizations can obtain unprecedented visibility into both the network data stream and the security posture of the network.



Test Security

Cisco.com

Validates effectiveness of the security policy through system auditing and vulnerability scanning

Secure

Improve

Security Policy

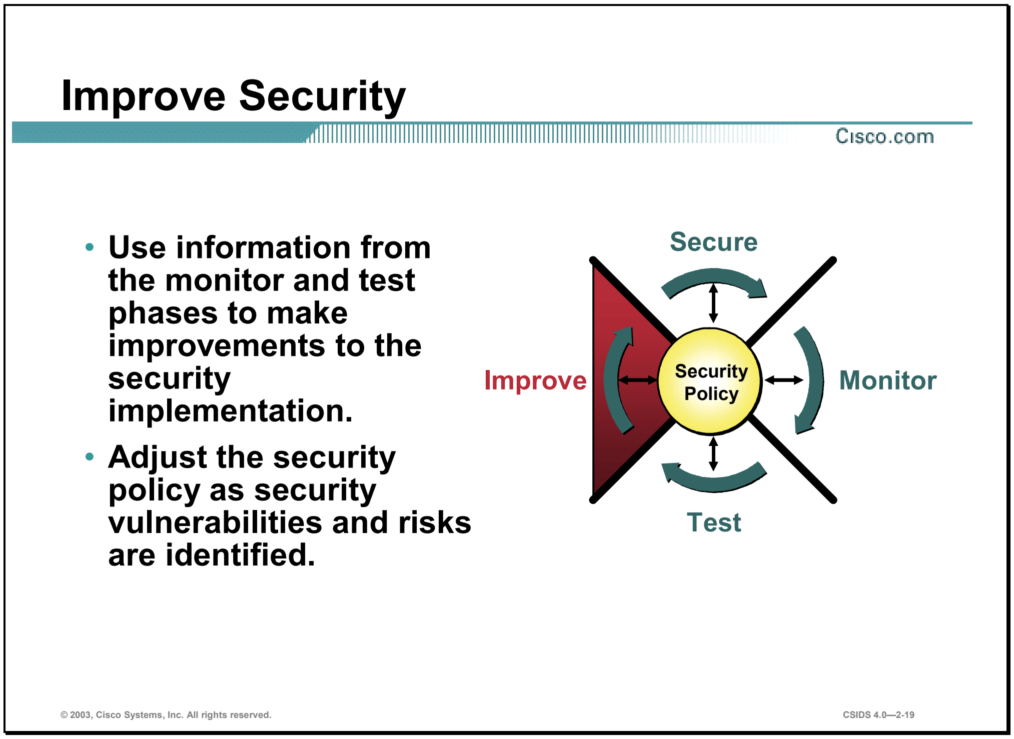
Monitor

Test

CSIDS 4.0—2-18

Testing security is as important as monitoring. Without testing the security solutions in place, it is impossible to know about existing or new attacks. The hacker community is an ever-changing environment. You can perform this testing yourself or outsource it to a third party such as the Cisco Security Posture Assessment (SPA) group.

The Cisco SPA is a premium network vulnerability assessment providing comprehensive insight into the security posture of a customer's network. Delivered by highly expert Cisco Network Security Engineers (NSEs), the Cisco SPA includes an operational, granular analysis of large-scale, distributed service provider networks from the perspective of an outside "hacker."



Improve Security

Cisco.com

- Use information from the monitor and test phases to make improvements to the security implementation.
- Adjust the security policy as security vulnerabilities and risks are identified.

Secure

Improve

Security Policy

Monitor

Test

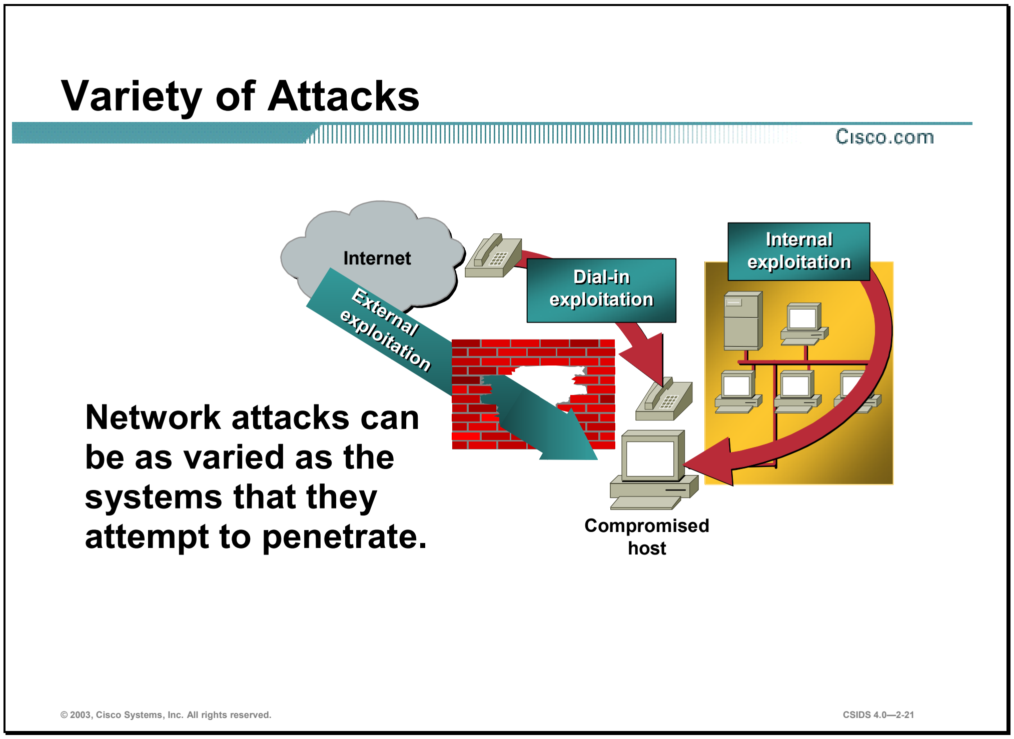
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—2-19

Monitoring and testing provides the data necessary to improve network security. Administrators and engineers should use the information from the monitor and test phases to make improvements to the security implementation as well as adjust the security policy as vulnerabilities and risks are identified.

Network Attack Taxonomy

This section provides an overview of various network attacks and affects.



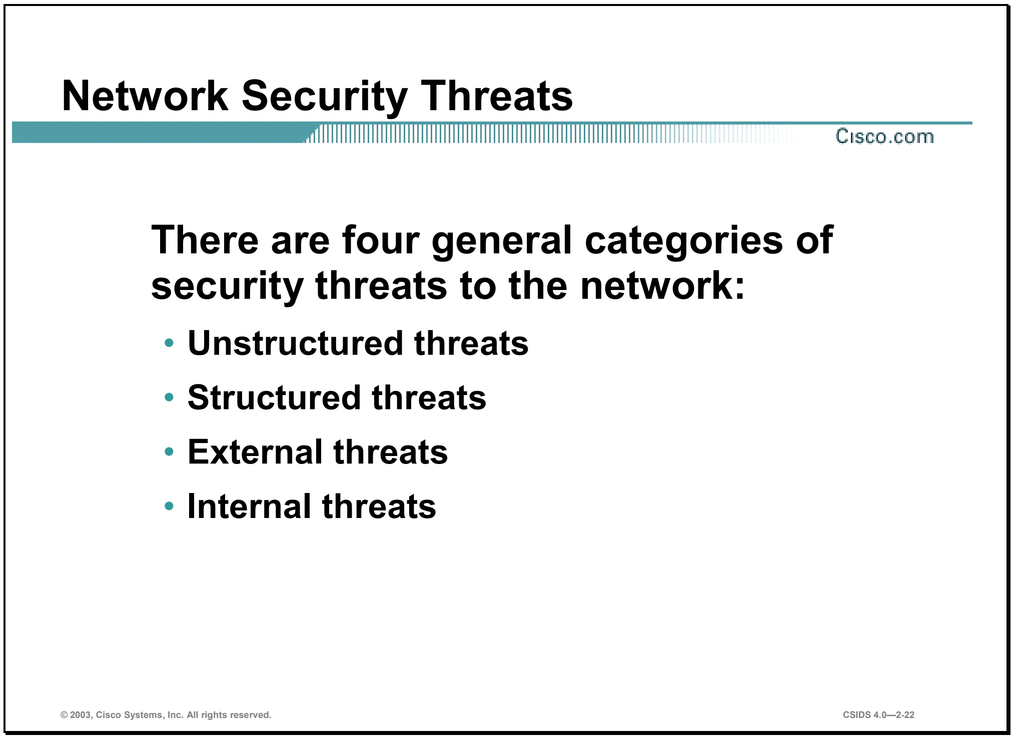
Variety of Attacks

Cisco.com

Network attacks can be as varied as the systems that they attempt to penetrate.

CSIDS 4.0—2-21

Without proper protection, any part of any network can be susceptible to attacks or unauthorized activity. Routers, switches, and hosts can all be violated by professional hackers, company competitors, or even internal employees. In fact, according to several studies, more than half of all network attacks are waged internally. The Computer Security Institute (CSI) in San Francisco estimates that between 60 and 80 percent of network misuse comes from inside the enterprises where the misuse has taken place. To determine the best ways to protect against attacks, IT managers should understand the many types of attacks that can be instigated and the damage that these attacks can cause to e-business infrastructures.



Network Security Threats

Cisco.com

There are four general categories of security threats to the network:

- **Unstructured threats**
- **Structured threats**
- **External threats**
- **Internal threats**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—2-22

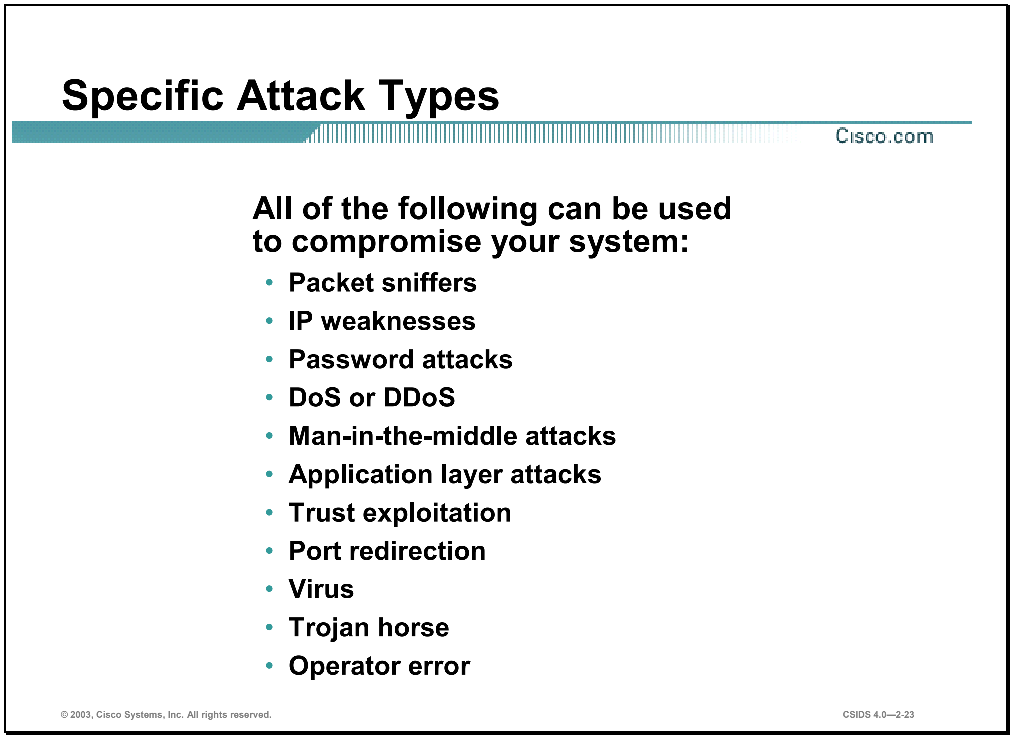
There are four general threats to network security:

- Unstructured threats—These threats primarily consist of random hackers using various common tools, such as malicious shell scripts, password crackers, credit card number generators, and dialer daemons. Although hackers in this category may have malicious intent, many are more interested in the intellectual challenge of cracking safeguards than creating havoc.

- Structured threats—These threats are created by hackers who are more highly motivated and technically competent. Typically, such hackers act alone or in small groups to understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies. Occasionally, such hackers are hired by organized crime, industry competitors, or state-sponsored intelligence collection organizations.

- External threats—These threats consist of structured and unstructured threats originating from an external source. These threats can have malicious and destructive intent, or simply be errors that generate a threat.

- Internal threats—These threats are typically from disgruntled former or current employees. Although internal threats may seem more ominous than threats from external sources, security measures are available for reducing vulnerabilities to internal threats and responding when attacks occur.



Specific Attack Types

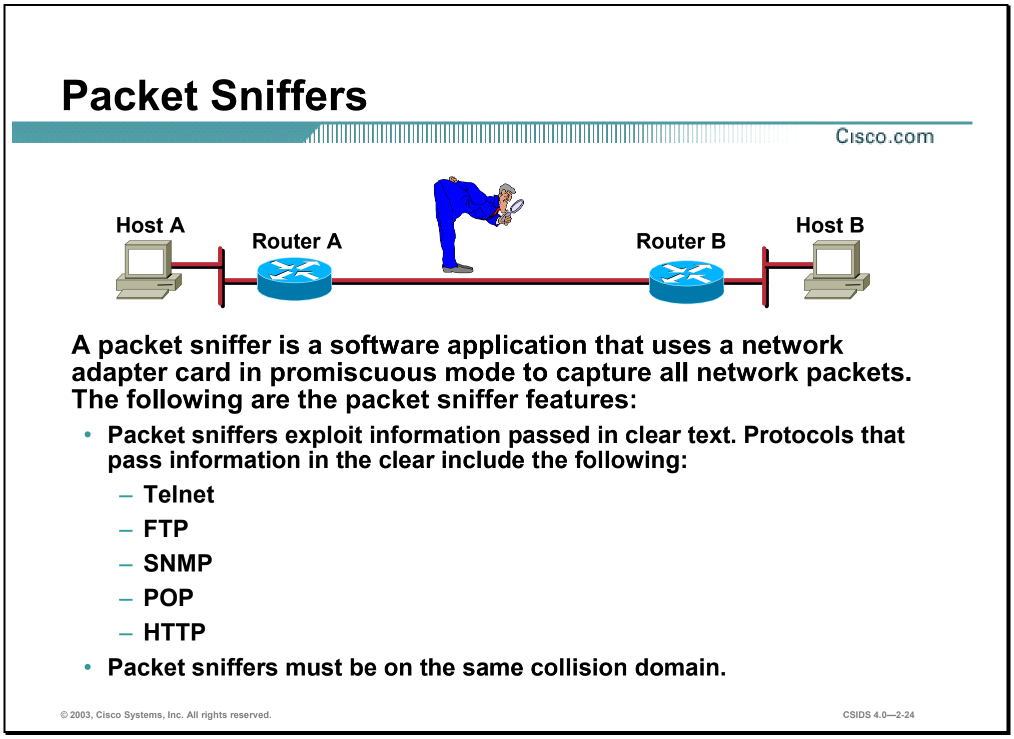
All of the following can be used to compromise your system:

- Packet sniffers
- IP weaknesses
- Password attacks
- DoS or DDoS
- Man-in-the-middle attacks
- Application layer attacks
- Trust exploitation
- Port redirection
- Virus
- Trojan horse
- Operator error

CSIDS 4.0—2-23

There are many common attacks that can occur against a network. Any of the following can be used to compromise your system:

- Packet sniffers
- IP weaknesses
- Password attacks
- Denial of service (DoS) or distributed denial of service (DDoS)
- Man-in-the-middle attacks
- Application layer attacks
- Trust exploitation
- Port redirection
- Virus
- Trojan horse
- Operator error



Packet Sniffers

A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets. The following are the packet sniffer features:

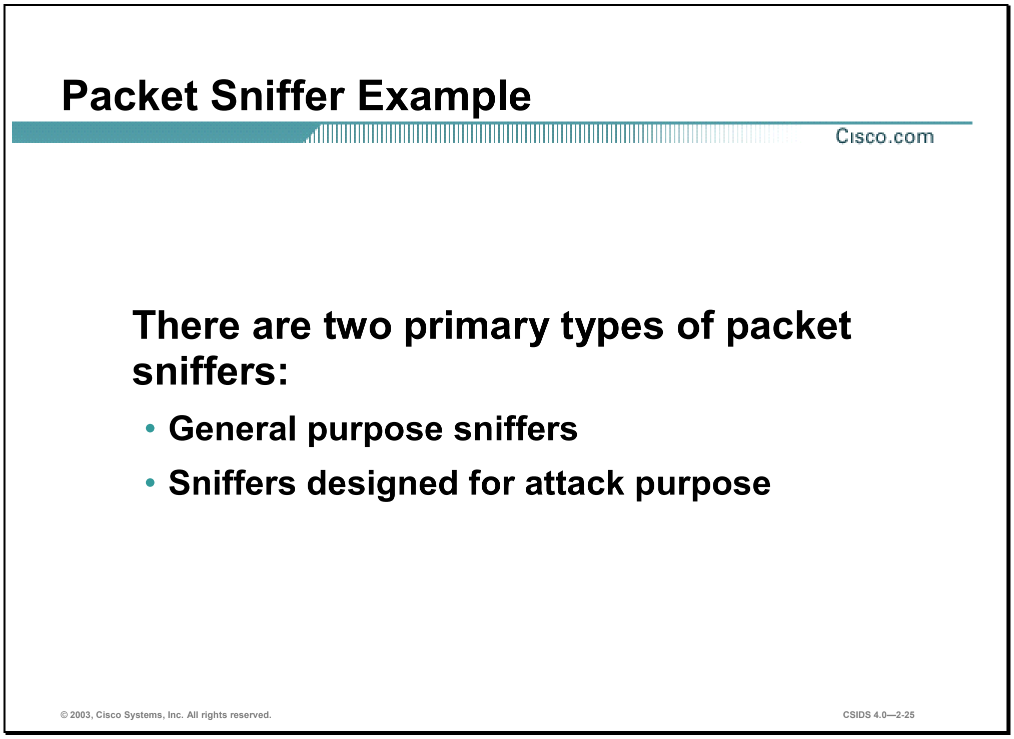
- **Packet sniffers exploit information passed in clear text. Protocols that pass information in the clear include the following:**
  - **Telnet**
  - **FTP**
  - **SNMP**
  - **POP**
  - **HTTP**
- **Packet sniffers must be on the same collision domain.**

CSIDS 4.0—2-24

A packet sniffer is a software application that uses a network adapter card in promiscuous mode (a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing) to capture all network packets that are sent across a LAN.

Several network applications distribute network packets in clear text; that is, the information sent across the network is not encrypted. Because the network packets are not encrypted, they can be processed and understood by any application that can pick them up off the network and process them.

A network protocol specifies how packets are identified and labeled, which enables a computer to determine whether a packet is intended for it. Because the specifications for network protocols, such as TCP/IP, are widely published, a third party can easily interpret the network packets and develop a packet sniffer. (The real threat today results from the numerous freeware and shareware packet sniffers that are available, which do not require the user to understand anything about the underlying protocols.)



Packet Sniffer Example

There are two primary types of packet sniffers:

- **General purpose sniffers**
- **Sniffers designed for attack purpose**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—2-25

A packet sniffer can provide its user with meaningful and often sensitive information, such as user account names and passwords. If you use networked databases, a packet sniffer can provide an attacker with information that is queried from the database, as well as the user account names and passwords used to access the database. One serious problem with acquiring user account names and passwords is that users often reuse their login names and passwords across multiple applications.

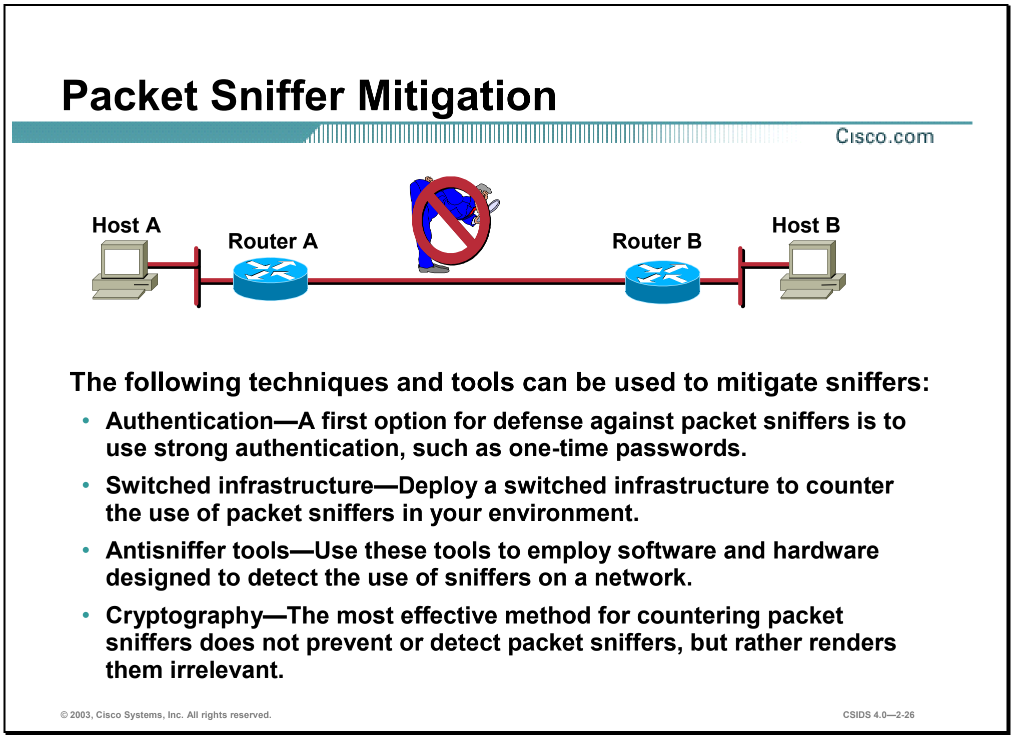
In addition, many network administrators use packet sniffers to diagnose and fix network-related problems. Because in the course of their usual and necessary duties these network administrators (such as those in a payroll department) work during regular employee hours, they can potentially examine sensitive information distributed across the network.

Many users employ a single password for access to all accounts and applications. Because attackers know and use human characteristics (attack methods known collectively as social engineering attacks), such as using a single password for multiple accounts, they are often successful in gaining access to sensitive information.

There are two primary types of packet sniffers:

- General purpose
  - Captures all packets
  - Included with some operating systems
  - Freeware and shareware versions available

- Designed for attack purpose
  - Captures first 300 to 400 bytes
  - Typically captures login sessions (File Transfer Protocol [FTP], rlogin, and Telnet)


Host A
Router A
Router B
Host B

Packet Sniffer Mitigation

The following techniques and tools can be used to mitigate sniffers:

- **Authentication—A first option for defense against packet sniffers is to use strong authentication, such as one-time passwords.**
- **Switched infrastructure—Deploy a switched infrastructure to counter the use of packet sniffers in your environment.**
- **Antisniffer tools—Use these tools to employ software and hardware designed to detect the use of sniffers on a network.**
- **Cryptography—The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but rather renders them irrelevant.**

CSIDS 4.0—2-26

The following techniques and tools can be used to mitigate packet sniffers:

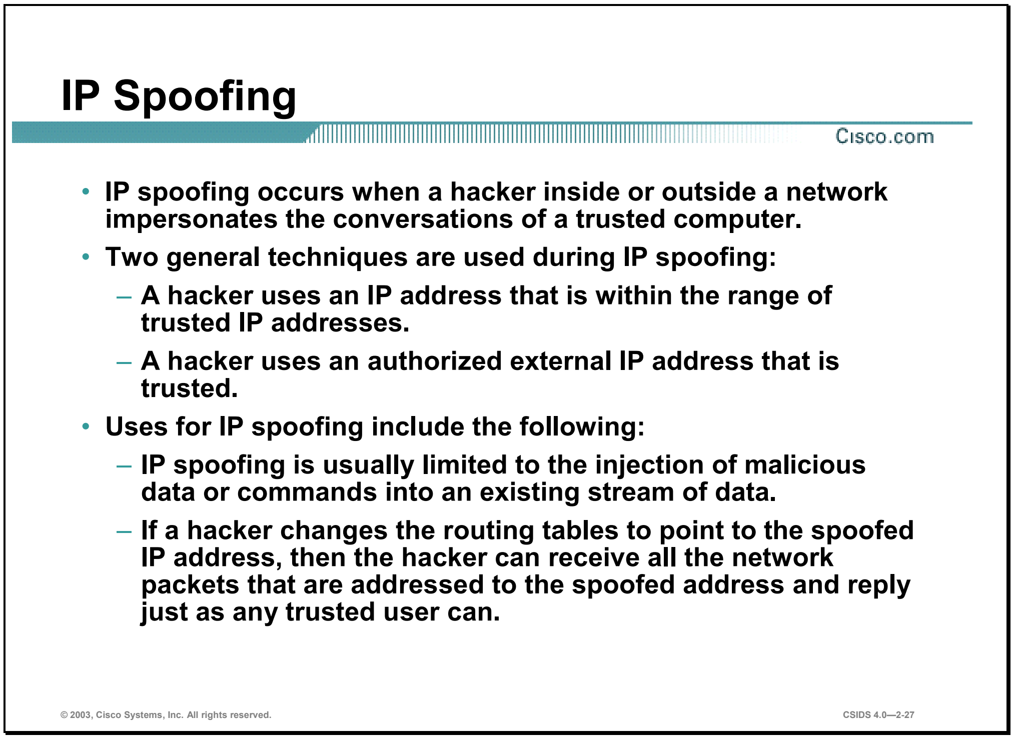
- Authentication—Using strong authentication is a first-option for defense against packet sniffers. Strong authentication can be broadly defined as a method of authenticating users that cannot easily be circumvented. A common example of strong authentication is one-time passwords (OTPs).

  An OTP is a type of two-factor authentication. Two-factor authentication involves using something you have combined with something you know. Automated teller machines (ATMs) use two-factor authentication. A customer needs both an ATM card and a personal identification number (PIN) to make transactions. With OTPs you need a PIN and your token card to authenticate to a device or software application. A token card is a hardware or software device that generates new, seemingly random, passwords at specified intervals (usually 60 seconds). A user combines that random password with a PIN to create a unique password that works only for one instance of authentication. If a hacker learns that password by using a packet sniffer, the information is useless because the password has already expired. Note that this mitigation technique is effective only against a sniffer implementation that is designed to grab passwords. Sniffers deployed to learn sensitive information (such as mail messages) will still be effective.

- Switched infrastructure—This can be used to counter the use of packet sniffers in your network environment. For example, if an entire organization deploys switched Ethernet, hackers can gain access only to the traffic that flows on the specific port to which they connect. A switched infrastructure obviously does not eliminate the threat of packet sniffers, but it can greatly reduce their effectiveness.

- Antisniffer tools—Employing software and hardware designed to detect the use of sniffers on a network. Such software and hardware does not completely eliminate the threat, but like many network security tools, they are part of the overall system. These so-called "antisniffers" detect changes in the response time of hosts to determine if the hosts are processing more traffic than their own. One such network security software tool, which is available from Security Software Technologies, is called AntiSniff.

- Cryptography—Rendering packet sniffers irrelevant, which is the most effective method for countering packet sniffers—even more effective than preventing or detecting packet sniffers. If a communication channel is cryptographically secure, the only data a packet sniffer will detect is cipher text (a seemingly random string of bits) and not the original message. The Cisco deployment of network-level cryptography is based on IPSec, which is a standard method for networking devices to communicate privately using IP. Other cryptographic protocols for network management include Secure Shell Protocol (SSH) and Secure Sockets Layer (SSL).



IP Spoofing

- IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.
- Two general techniques are used during IP spoofing:
  - A hacker uses an IP address that is within the range of trusted IP addresses.
  - A hacker uses an authorized external IP address that is trusted.
- Uses for IP spoofing include the following:
  - IP spoofing is usually limited to the injection of malicious data or commands into an existing stream of data.
  - If a hacker changes the routing tables to point to the spoofed IP address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.

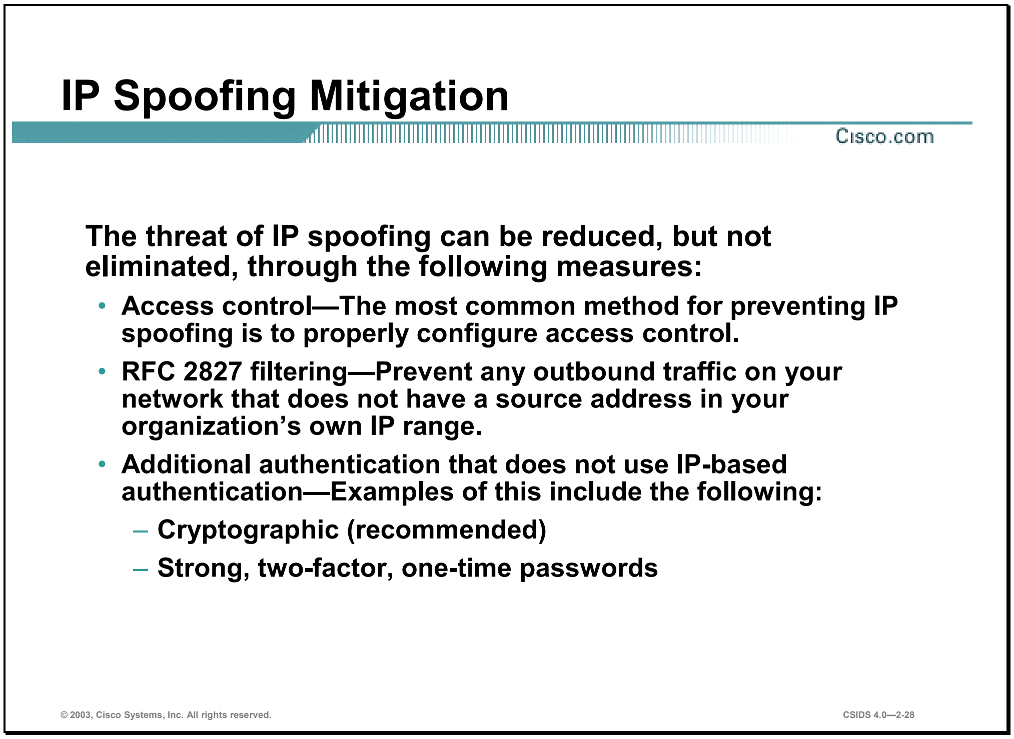
CSIDS 4.0—2-27

An IP spoofing attack occurs when an attacker outside your network pretends to be a trusted computer, either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you wish to provide access to specified resources on your network.

Normally, an IP spoofing attack is limited to the injection of data or commands into an existing stream of data passed between a client and server application or a peer-to-peer network connection. To enable bi-directional communication, the attacker must change all routing tables to point to the spoofed IP address. Another approach the attacker could take is to simply not worry about receiving any response from the applications. For example, if an attacker is attempting to get a system to mail him or her a sensitive file, application responses are unimportant.

However, if an attacker manages to change the routing tables to point to the spoofed IP address, he can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can. Like packet sniffers, IP spoofing is not restricted to people who are external to the network.

Although not as common, IP spoofing can also gain access to user accounts and passwords, and it can also be used in other ways. For example, an attacker can emulate one of your internal users in ways that prove embarrassing for your organization; the attacker could send e-mail messages to business partners that appear to have originated from someone within your organization. Such attacks are easier when an attacker has a user account and password, but they are possible by combining simple spoofing attacks with knowledge of messaging protocols.



IP Spoofing Mitigation

Cisco.com

The threat of IP spoofing can be reduced, but not eliminated, through the following measures:

- **Access control—The most common method for preventing IP spoofing is to properly configure access control.**
- **RFC 2827 filtering—Prevent any outbound traffic on your network that does not have a source address in your organization’s own IP range.**
- **Additional authentication that does not use IP-based authentication—Examples of this include the following:**
  - **Cryptographic (recommended)**
  - **Strong, two-factor, one-time passwords**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—2-28

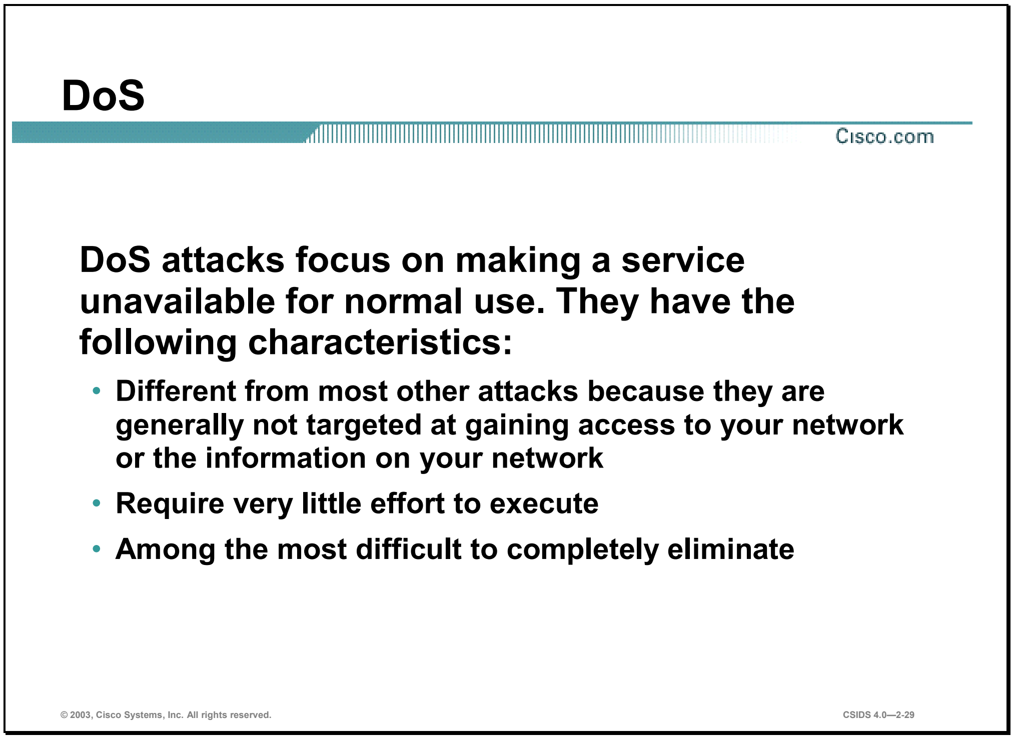
The threat of IP spoofing can be reduced, but not eliminated, through the following measures:

- Access control—The most common method for preventing IP spoofing is to properly configure access control. To reduce the effectiveness of IP spoofing, configure access control to deny any traffic from the external network that has a source address that should reside on the internal network. Note that this helps prevent spoofing attacks only if the internal addresses are the only trusted addresses. If some external addresses are trusted, this method is not effective.

- RFC 2827 filtering—You can prevent users of your network from spoofing other networks (and be a good Internet citizen at the same time) by preventing any outbound traffic on your network that does not have a source address in your organization's own IP range.

  This filtering denies any traffic that does not have the source address that was expected on a particular interface. For example, if an ISP is providing a connection to the IP address 15.1.1.0/24, the ISP could filter traffic so that only traffic sourced from address 15.1.1.0/24 can enter the ISP router from that interface. Note that unless all ISPs implement this type of filtering, its effectiveness is significantly reduced.

- Additional Authentication—The most effective method for mitigating the threat of IP spoofing is the same as the most effective method for mitigating the threat of packet sniffers: namely, eliminating its effectiveness. IP spoofing can function correctly only when devices use IP address-based authentication; therefore, if you use additional authentication methods, IP spoofing attacks are irrelevant. Cryptographic authentication is the best form of additional authentication, but when that is not possible, strong two-factor authentication using OTP can also be effective.

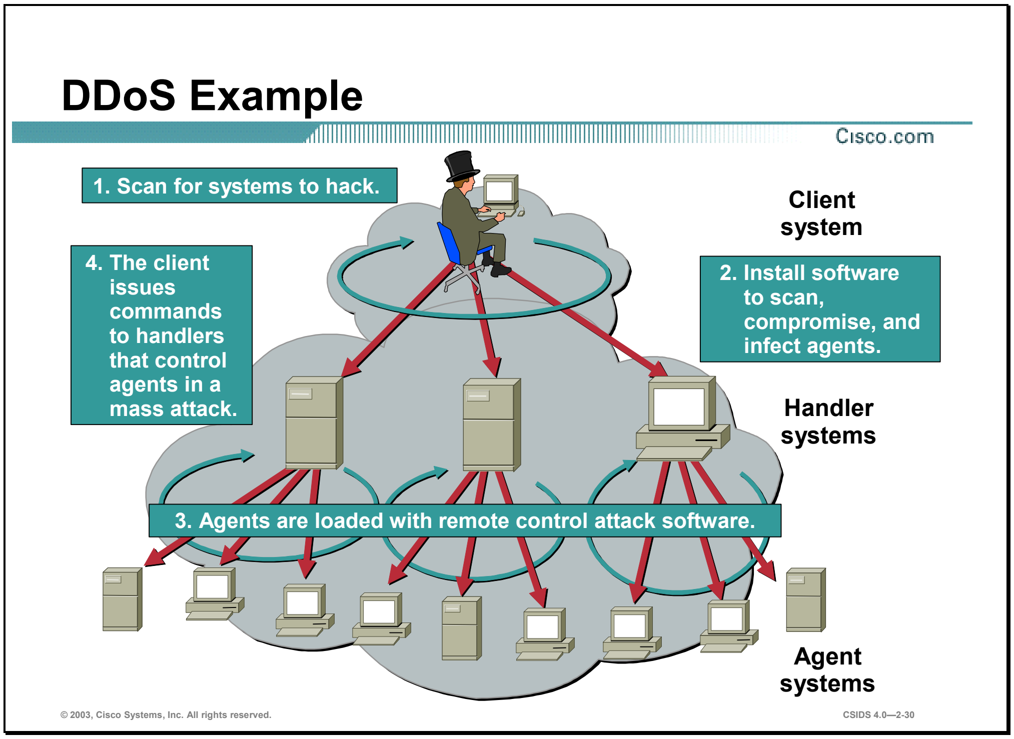


DoS

DoS attacks focus on making a service unavailable for normal use. They have the following characteristics:

- **Different from most other attacks because they are generally not targeted at gaining access to your network or the information on your network**
- **Require very little effort to execute**
- **Among the most difficult to completely eliminate**

DoS attacks are different from most other attacks because they are not targeted at gaining access to your network or the information on your network. These attacks focus on making a service unavailable for normal use, which is typically accomplished by exhausting some resource limitation on the network or within an operating system or application. These attacks require little effort to execute because they typically take advantage of protocol weaknesses or the attacks are carried out using traffic that would normally be allowed into a network. DoS attacks are among the most difficult to completely eliminate because of the way they use protocol weaknesses and “native” traffic to attack a network.



DDoS Example

Cisco.com

1. Scan for systems to hack.

2. Install software to scan, compromise, and infect agents.

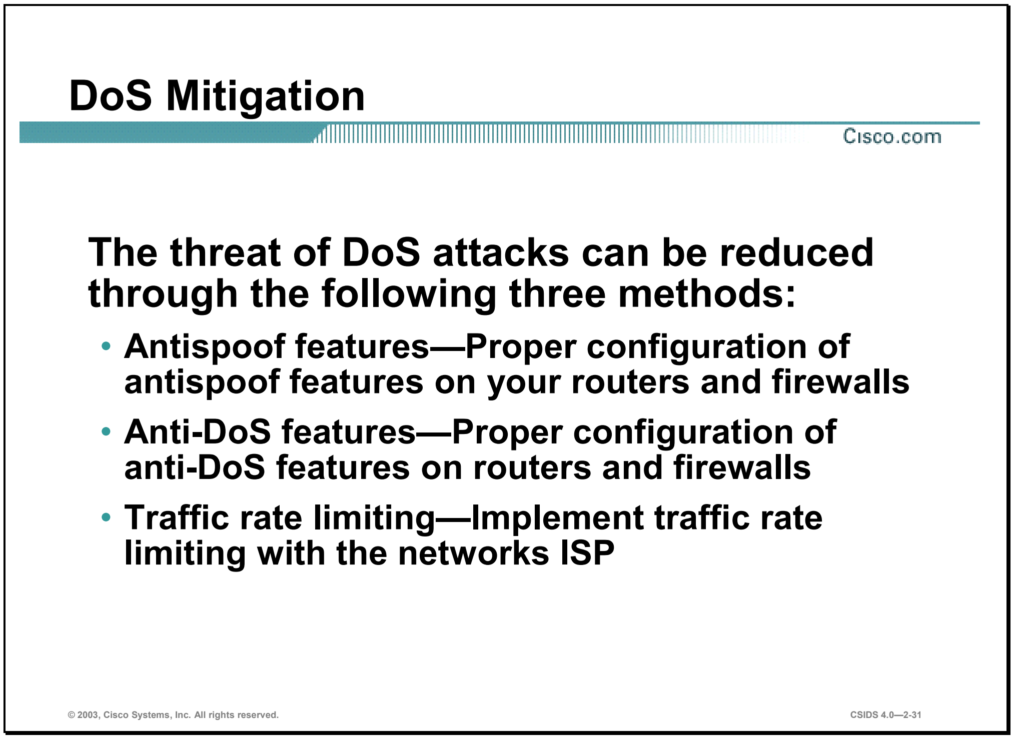
3. Agents are loaded with remote control attack software.

4. The client issues commands to handlers that control agents in a mass attack.

CSIDS 4.0—2-30

DDoS attacks are the "next generation" of DoS attacks on the Internet. This type of attack is not new—UDP and TCP SYN flooding, Internet Control Message Protocol (ICMP) echo request floods, and ICMP directed broadcasts (also known as smurf attacks) are similar—but the scope certainly is new. Victims of DDoS attacks experience packet flooding from many different sources, possibly spoofed IP source addresses, that bring their network connectivity to a grinding halt. In the past, the typical DoS attack involved a single attacker's attempt to flood a target host with packets. With DDoS tools, an attacker can conduct the same attack using thousands of systems.

In the figure the hacker uses their terminal to scan for systems to hack. When the handler systems are accessed, the hacker then installs software on them to scan for, compromise, and infect Agent systems. When the Agent systems are accessed the hacker then loads remote control attack software to carry out the DoS attack.



DoS Mitigation

The threat of DoS attacks can be reduced through the following three methods:

- **Antispoof features—Proper configuration of antispoof features on your routers and firewalls**
- **Anti-DoS features—Proper configuration of anti-DoS features on routers and firewalls**
- **Traffic rate limiting—Implement traffic rate limiting with the networks ISP**

When involving specific network server applications, such as a HTTP server or a File Transfer Protocol (FTP) server, these attacks can focus on acquiring and keeping open all the available connections supported by that server, effectively locking out valid users of the server or service. DoS attacks can also be implemented using common Internet protocols, such as TCP and ICMP. While most DoS attacks exploit a weakness in the overall architecture of the system being attacked rather than a software bug or security hole, some attacks compromise the performance of your network by flooding the network with undesired, and often useless, network packets and by providing false information about the status of network resources.

The threat of DoS attacks can be reduced through the following three methods:

- Antispoof features—Proper configuration of antispoof features on your routers and firewalls can reduce your risk. This configuration includes RFC 2827 filtering at a minimum. If hackers cannot mask their identities, they might not attack.

- Anti-DoS features—Proper configuration of anti-DoS features on routers and firewalls can help limit the effectiveness of an attack. These features often involve limits on the amount of half-open connections that a system allows open at any given time.

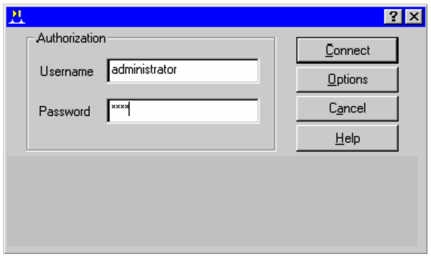
- Traffic rate limiting—An organization can implement traffic rate limiting with its ISP. This type of filtering limits the amount of nonessential traffic that crosses network segments at a certain rate. A common example is to limit the amount of ICMP traffic allowed into a network because it is used only for diagnostic purposes. ICMP-based DDoS attacks are common.

Password Attacks

Cisco.com

Hackers can implement password attacks using several different methods:

- **Brute-force attacks**
- **Trojan horse programs**
- **IP spoofing**
- **Packet sniffers**



Authorization

Username: administrator

Password: ****

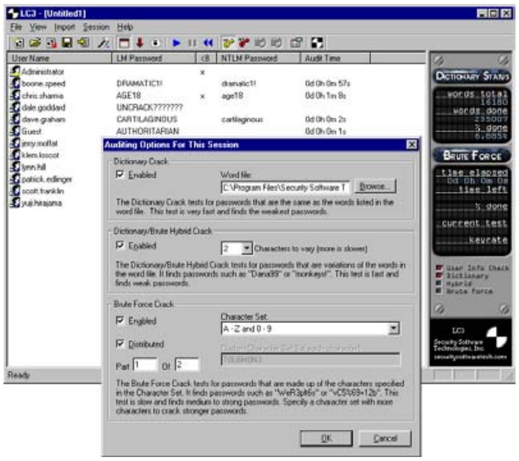
Password attacks can be implemented using several different methods, including brute-force attacks, Trojan horse programs (discussed later in the chapter), IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute-force attacks.

Often a brute-force attack is performed using a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker successfully gains access to a resource, he or she has the same rights as the user whose account has been compromised to gain access to that resource. If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account.

Password Attack Example

Cisco.com

- L0phtCrack can take the hashes of passwords and generate the clear text passwords from them.
- Passwords are computed using two different methods:
  - Dictionary cracking
  - Brute force computation



User Name	LM Password	<8	NTLM Password	Audit Time
Administrator		×		
boone.speed	DRAMATIC1!		dramatic1!	0d 0h 0m 57s
chris.sharma	AGE18	×	age18	0d 0h 1m 8s
dale.goddard	UNCRACK???????			
dave.graham	CARTILAGINOUS		cartilaginous	0d 0h 0m 2s
Guest	AUTHORITARIAN			0d 0h 0m 1s
jerry.moffat				
klem.loscot				
lynn.hill				
patrick.edlinger				
scott.franklin				
yuji.hirayama				

Auditing Options For This Session

Dictionary Crack

☑ Enabled   Word file: C:\Program Files\Security Software T   Browse...

The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

Dictionary/Brute Hybrid Crack

☑ Enabled   2   Characters to vary (more is slower)

The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.

Brute Force Crack

☑ Enabled   Character Set: A - Z and 0 - 9

☑ Distributed   Custom Character Set (list each character)

Part 1 Of 2

The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3pt6s" or "vC5%6+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.

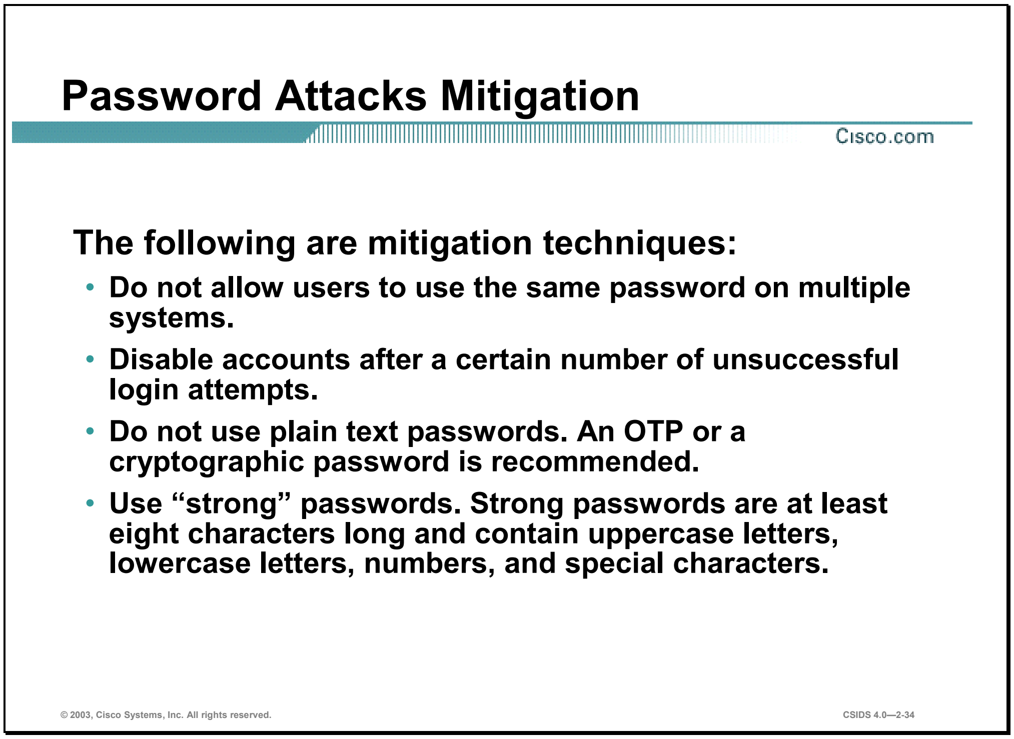
OK   Cancel

CSIDS 4.0—2-33

Just as with packet sniffers and IP spoofing attacks, a brute-force password attack can provide access to accounts that can be used to modify critical network files and services. An example that compromises your network's integrity is an attacker modifying the routing tables for your network. By doing so, the attacker ensures that all network packets are routed to him or her before they are transmitted to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

The following are the two different methods for computing passwords with L0phtCrack:

- Dictionary cracking—The password hashes for all of the words in a dictionary file are computed and compared against all of the password hashes for the users. This method is extremely fast and finds very simple passwords.
- Brute force computation—This method uses a particular character set such as A–Z, or A–Z plus 0–9 and computes the hash for every possible password made up of those characters. It will always compute the password if it is made up of the character set you have selected to test. The downside is that time is required for completion of this type of attack.



Password Attacks Mitigation

Cisco.com

The following are mitigation techniques:

- Do not allow users to use the same password on multiple systems.
- Disable accounts after a certain number of unsuccessful login attempts.
- Do not use plain text passwords. An OTP or a cryptographic password is recommended.
- Use “strong” passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.

CSIDS 4.0—2-34

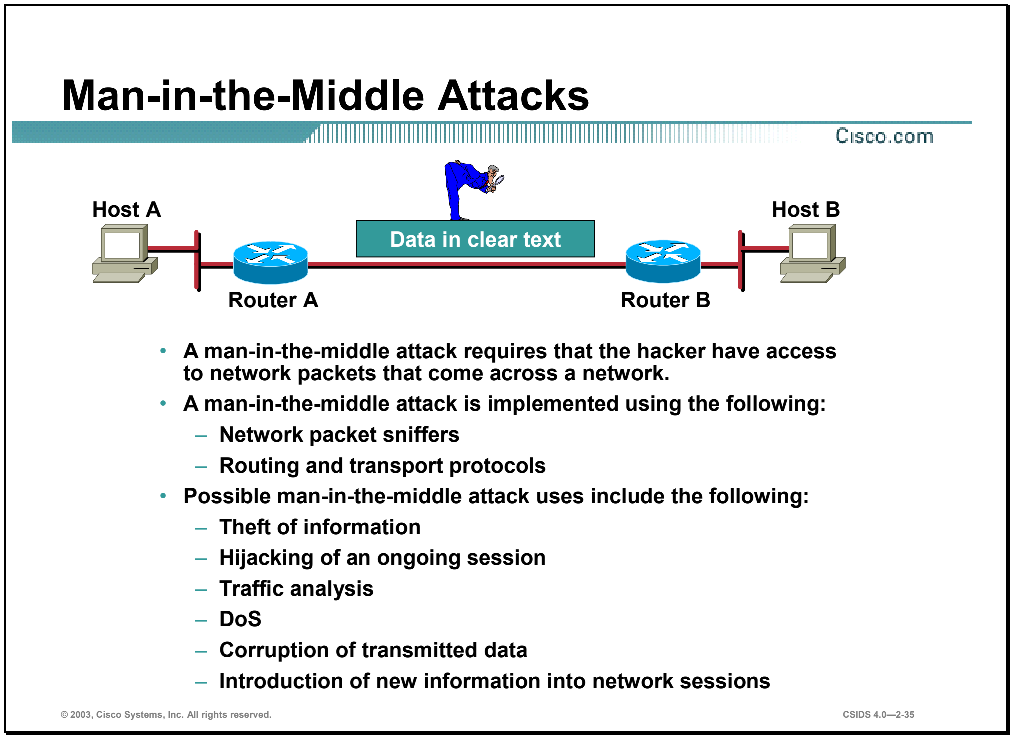
The following are password attack mitigation techniques:

- Do not allow users to have the same password on multiple systems—Most users will use the same password for each system they access, and often personal system passwords will be the same as well.

- Disable accounts after unsuccessful logins—This helps to prevent continuous password attempts.

- Do not use plain text passwords—Use of either an OTP or encrypted password is recommended.

- Use “strong” passwords—Many systems now provide strong password support and can restrict a user to only the use of strong passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.



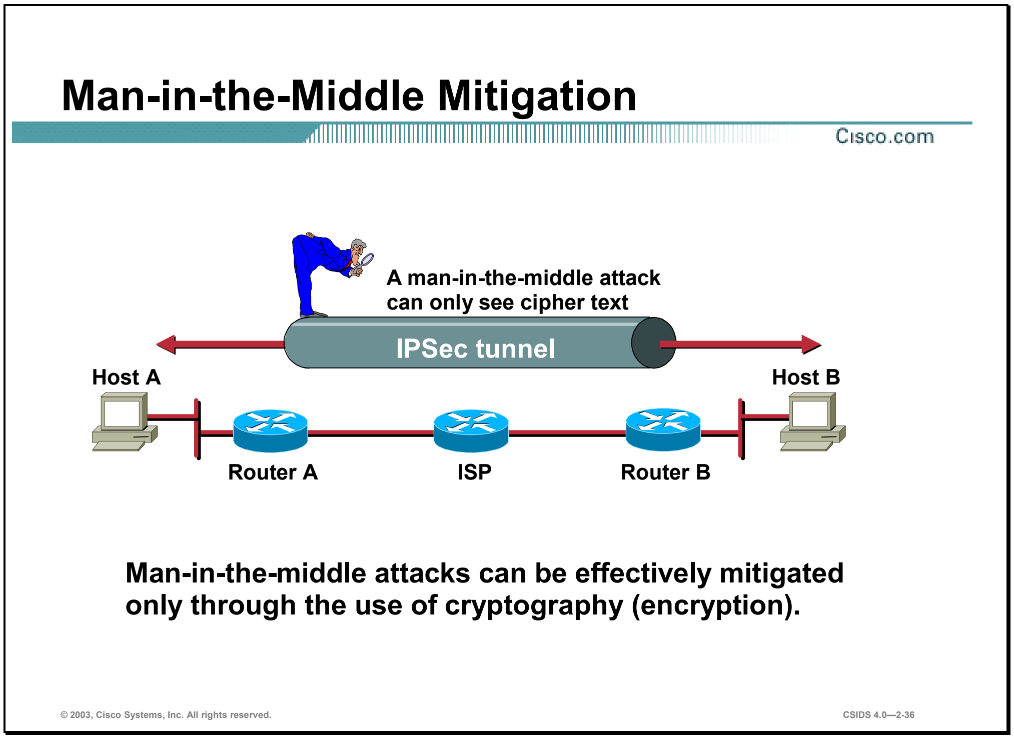
Man-in-the-Middle Attacks

- A man-in-the-middle attack requires that the hacker have access to network packets that come across a network.
- A man-in-the-middle attack is implemented using the following:
  - Network packet sniffers
  - Routing and transport protocols
- Possible man-in-the-middle attack uses include the following:
  - Theft of information
  - Hijacking of an ongoing session
  - Traffic analysis
  - DoS
  - Corruption of transmitted data
  - Introduction of new information into network sessions

CSIDS 4.0—2-35

A man-in-the-middle attack requires that the attacker have access to network packets that come across the networks. Such attacks are often implemented using network packet sniffers and routing and transport protocols. The possible uses of such attacks are theft of information, hijacking of an ongoing session to gain access to your internal network resources, traffic analysis to derive information about your network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions.

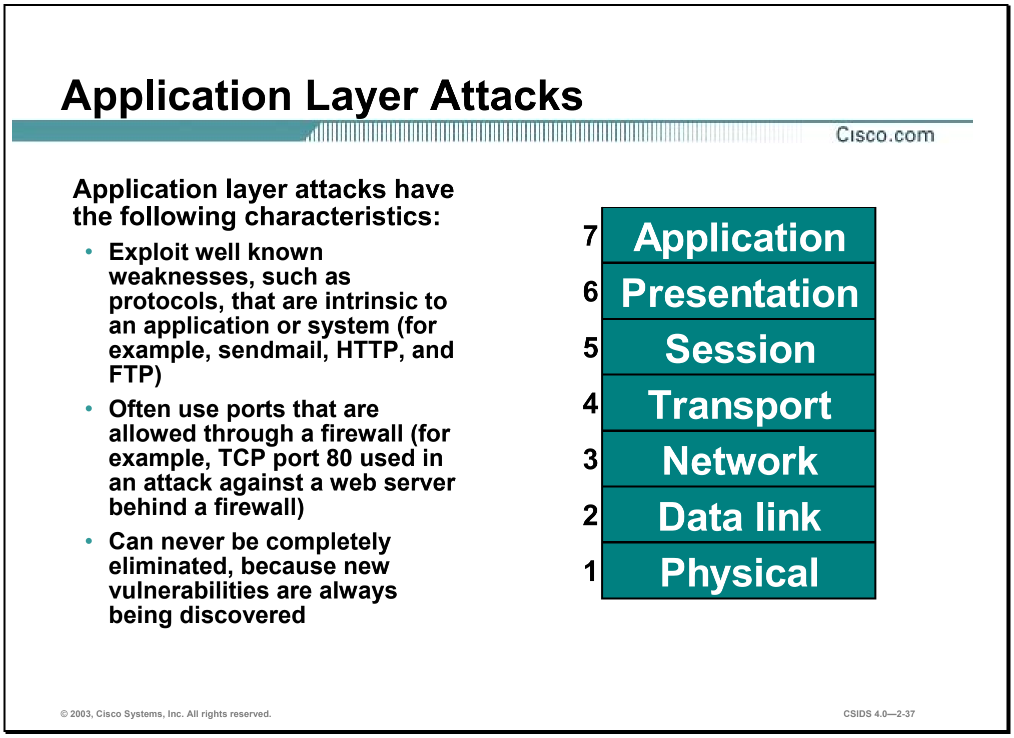
An example of a man-in-the-middle attack could be someone who is working for your ISP, who can gain access to all network packets transferred between your network and any other network.



Man-in-the-Middle Mitigation

Man-in-the-middle attacks can be effectively mitigated only through the use of cryptography (encryption).

Man-in-the-Middle attack mitigation is achieved, as shown in the figure, by encrypting traffic in an IPSec tunnel, which would only allow the hacker to see cipher text.



Application Layer Attacks

Cisco.com

Application layer attacks have the following characteristics:

- Exploit well known weaknesses, such as protocols, that are intrinsic to an application or system (for example, sendmail, HTTP, and FTP)
- Often use ports that are allowed through a firewall (for example, TCP port 80 used in an attack against a web server behind a firewall)
- Can never be completely eliminated, because new vulnerabilities are always being discovered

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data link
1 Physical

CSIDS 4.0—2-37

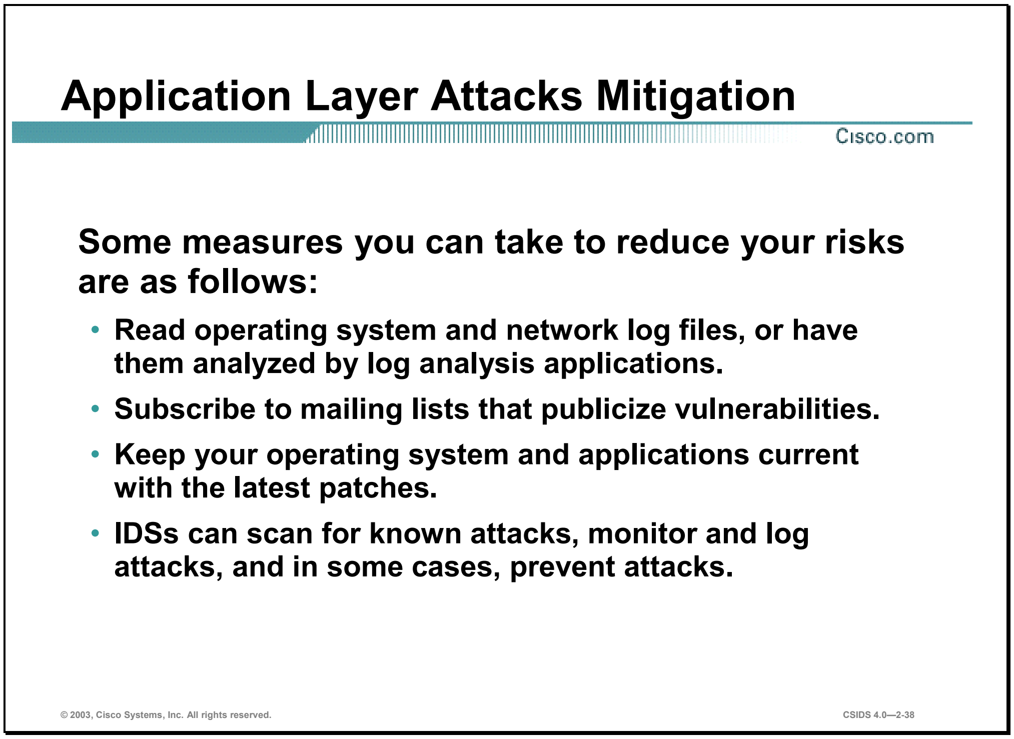
Application-layer attacks can be implemented using several different methods:

- One of the most common methods is exploiting well known weaknesses in software commonly found on servers, such as sendmail, PostScript, and FTP. By exploiting these weaknesses, attackers can gain access to a computer with the permissions of the account running the application, which is usually a privileged, system-level account.

- Trojan horse program attacks are implemented using programs that an attacker substitutes for common programs. These programs may provide all the functionality that the normal program provides, but also include other features that are known to the attacker, such as monitoring login attempts to capture user account and password information. These programs can capture sensitive information and distribute it back to the attacker. They can also modify application functionality, such as applying a blind carbon copy to all e-mail messages so that the attacker can read all of your organization's e-mail.

  One of the oldest forms of application-layer attacks is a Trojan horse program that displays a screen, banner, or prompt that the user believes is the valid login sequence. The program then captures the information that the user enters and stores or e-mails it to the attacker. Next, the program either forwards the information to the normal login process (normally impossible on modern systems), or simply sends an expected error to the user (for example, Bad Username/Password Combination), exits, and starts the normal login sequence. The user, believing that they have incorrectly entered the password (a common mistake experienced by everyone), re-enters the information and is allowed access.

- One of the newest forms of application-layer attacks exploits the openness of several new technologies: the HTML specification, web browser functionality, and HTTP. These attacks, which include Java applets and ActiveX controls, involve passing harmful programs across the network and loading them through a user's browser.



Application Layer Attacks Mitigation

Cisco.com

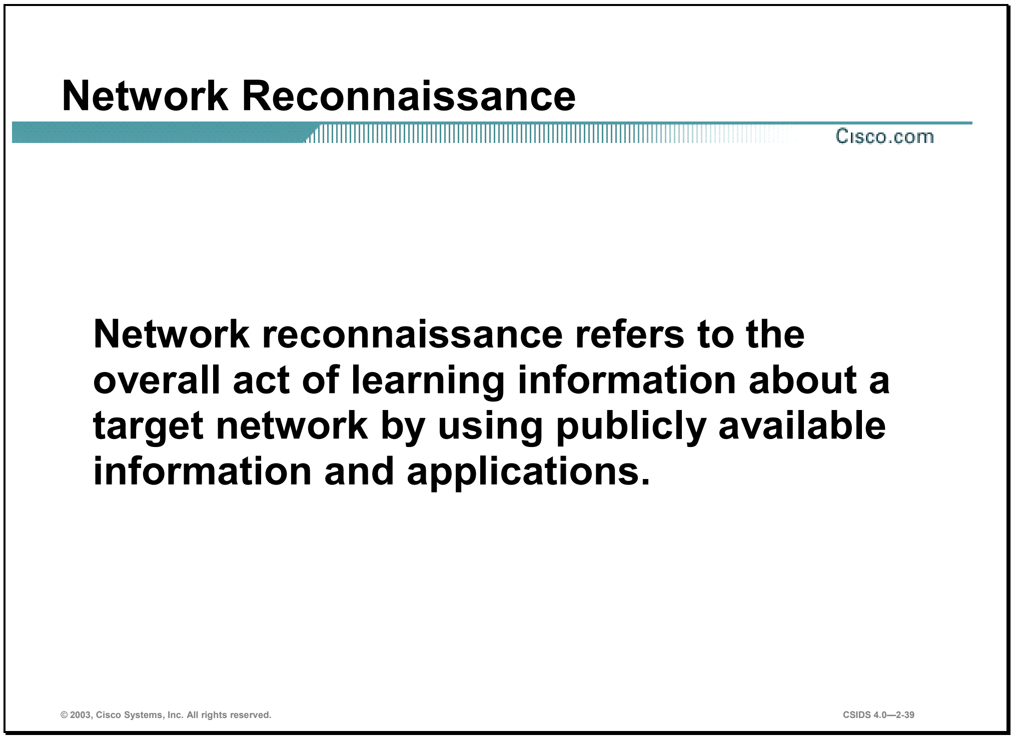
Some measures you can take to reduce your risks are as follows:

- **Read operating system and network log files, or have them analyzed by log analysis applications.**
- **Subscribe to mailing lists that publicize vulnerabilities.**
- **Keep your operating system and applications current with the latest patches.**
- **IDSs can scan for known attacks, monitor and log attacks, and in some cases, prevent attacks.**

CSIDS 4.0—2-38

The following are some measures you can take to reduce your risks for application layer attacks:

- Read operating system and network log files or have them analyzed—It is important to review all logs and take action accordingly.
- Subscribe to mailing lists that publicize vulnerabilities—Most application and operating system vulnerabilities are published on the Web at various sources.
- Keep your operating system and applications current with the latest patches—Always test patches and fixes in a non-production environment. This prevents downtime and errors from being generated unnecessarily.
- Intrusion detection systems (IDSs) can scan for known attacks, monitor and log attacks, and in some cases, prevent attacks—The use of IDSs can be essential to identifying security threats and mitigating some of those threats, and, in most cases, it can be done automatically.



Network Reconnaissance

Cisco.com

Network reconnaissance refers to the overall act of learning information about a target network by using publicly available information and applications.

© 2003, Cisco Systems, Inc. All rights reserved.

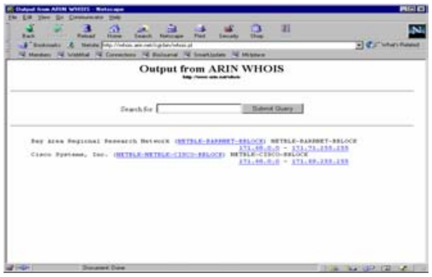
CSIDS 4.0—2-39

Network Reconnaissance refers to the overall act of learning information about a target network by using publicly available information and applications. When hackers attempt to penetrate a particular network, they often need to learn as much information as possible about the network before launching attacks. Examples include DNS queries, ping sweeps, and port scans:

- Domain Name System (DNS) queries—Reveals such information as who owns a particular domain and what addresses have been assigned to that domain.
- Ping sweeps—Presents a picture of the live hosts in a particular environment.
- Port scans—Cycles through all well known ports to provide a complete list of all services running on the hosts.

Network Reconnaissance Example

Cisco.com

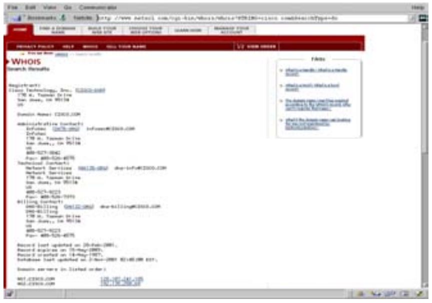


Output from ARIN WHOIS

Search for [   ] Submit Query

```
Bay Area Regional Research Network (NETBLK-BARRNET-BBLOCK) NETBLK-BARRNET-BBLOCK
                                                     171.64.0.0 - 171.71.255.255
Cisco Systems, Inc. (NETBLK-NETBLK-CISCO-BBLOCK) NETBLK-CISCO-BBLOCK
                                                     171.68.0.0 - 171.69.255.255
```

Sample IP address query



WHOIS

Search Results

```
Registrant:
[illegible]

   Domain Name: CISCO.COM

   Administrative Contact:
   [illegible]
   Technical Contact:
   [illegible]
   Billing Contact:
   [illegible]

   Domain servers in listed order:
   [illegible]
```

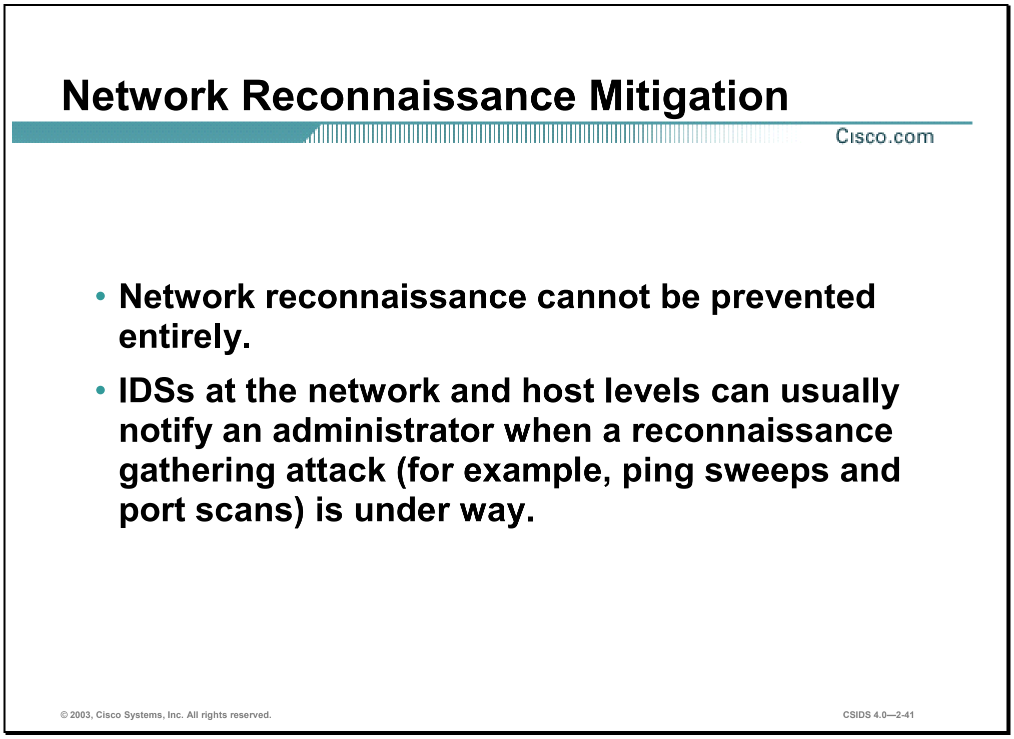
Sample domain name query

CSIDS 4.0—2-40

The figure demonstrates how existing Internet tools can be used for network reconnaissance (for example, an IP address query or a Domain Name query).

DNS queries can reveal such information as who owns a particular domain and what addresses have been assigned to that domain. Ping sweeps of the addresses revealed by the DNS queries can present a picture of the live hosts in a particular environment. After such a list is generated, port scanning tools can cycle through all well known ports to provide a complete list of all services running on the hosts discovered by the ping sweep. Finally, the hackers can examine the characteristics of the applications that are running on the hosts. This can lead to specific information that is useful when the hacker attempts to compromise that service.

IP address queries can reveal information such as who owns a particular IP address or range of addresses and what domain is associated to them.



Network Reconnaissance Mitigation

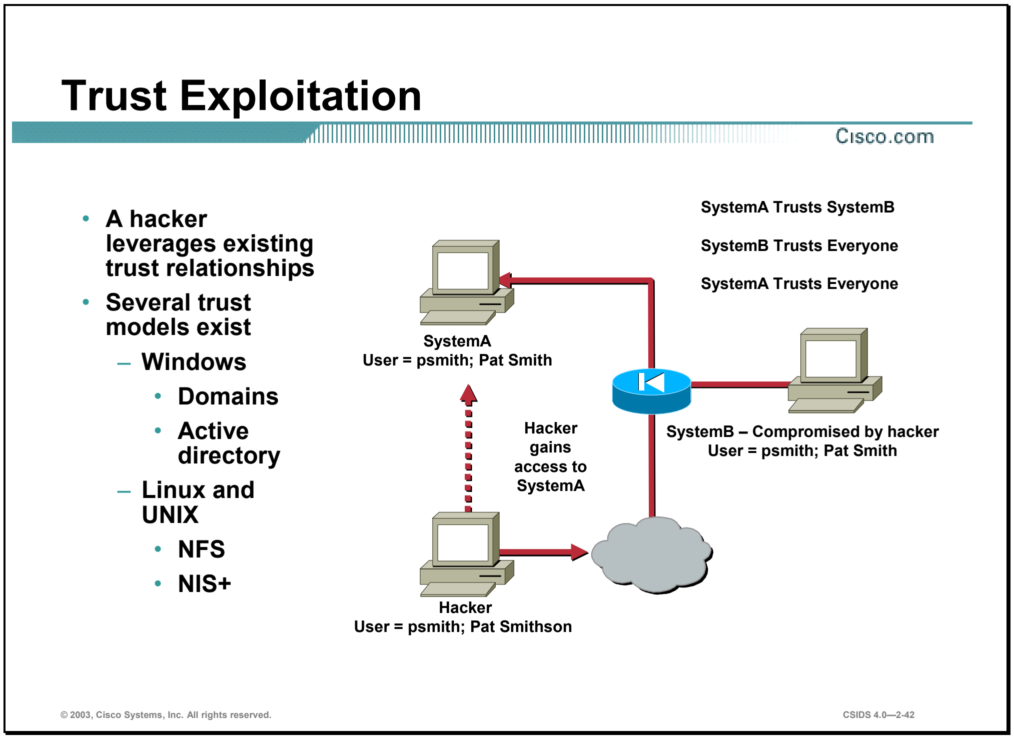
Cisco.com

- **Network reconnaissance cannot be prevented entirely.**
- **IDSs at the network and host levels can usually notify an administrator when a reconnaissance gathering attack (for example, ping sweeps and port scans) is under way.**

CSIDS 4.0—2-41

If ICMP echo and echo-reply is turned off on edge routers (for example, ping sweeps can be stopped, but at the expense of network diagnostic data), port scans can still be run without full ping sweeps They simply take longer because they need to scan IP addresses that might not be live.

IDSs at the network and host levels can usually notify an administrator when a reconnaissance gathering attack is underway. This allows the administrator to better prepare for the coming attack or to notify the ISP who is hosting the system that it is launching the reconnaissance probe.



Trust Exploitation

- A hacker leverages existing trust relationships
- Several trust models exist
  - Windows
    - Domains
    - Active directory
  - Linux and UNIX
    - NFS
    - NIS+

SystemA Trusts SystemB

SystemB Trusts Everyone

SystemA Trusts Everyone

SystemA
User = psmith; Pat Smith

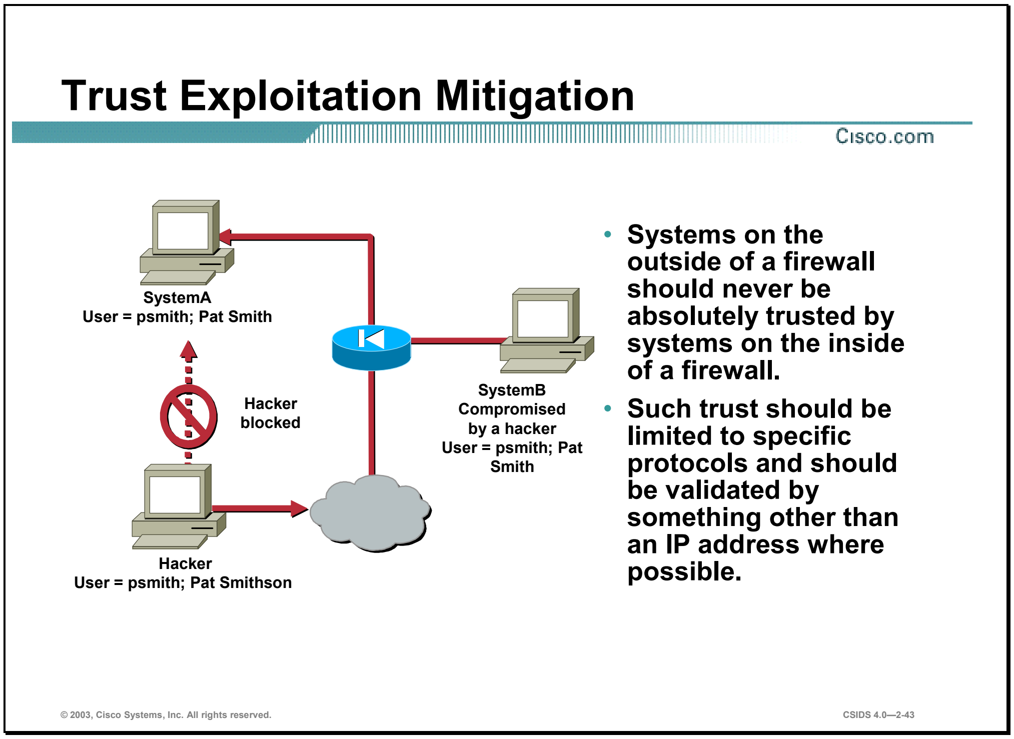
SystemB – Compromised by hacker
User = psmith; Pat Smith

Hacker gains access to SystemA

Hacker
User = psmith; Pat Smithson

CSIDS 4.0—2-42

While not an attack in and of itself, trust exploitation refers to an attack where an individual takes advantage of a trust relationship within a network. The classic example is a perimeter network connection from a corporation. These network segments often house DNS, SMTP, and HTTP servers. Because they all reside on the same segment, a compromise of one system can lead to the compromise of other systems because they might trust other systems attached to their same network. Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, it can leverage that trust relationship to attack the inside network.



Trust Exploitation Mitigation

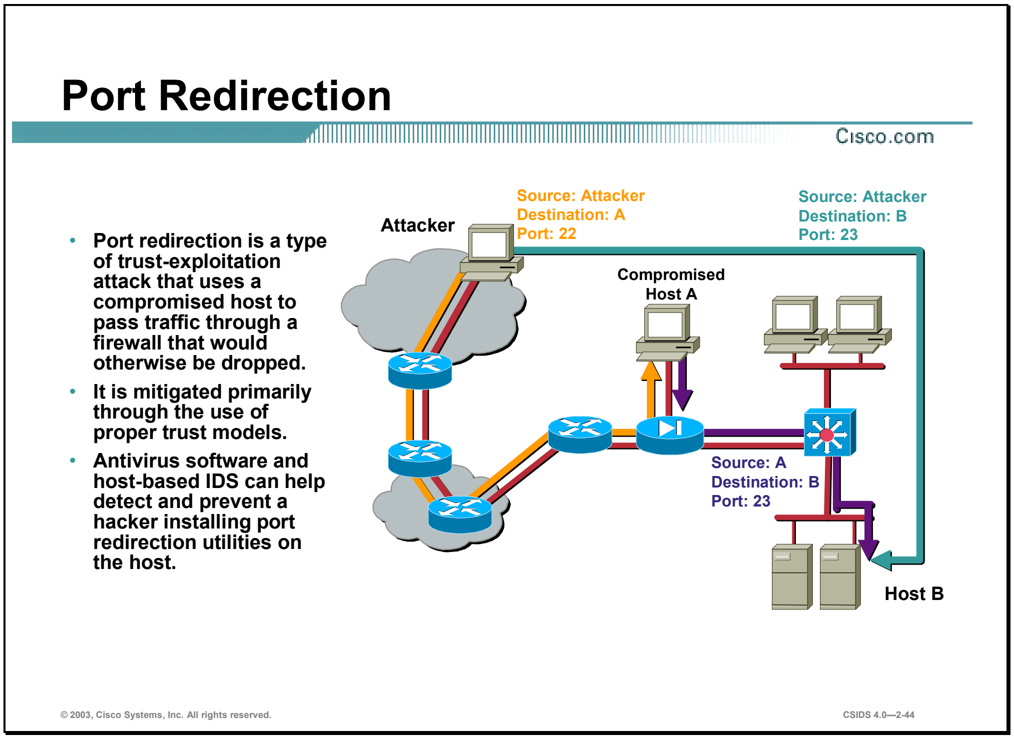
Cisco.com

SystemA
User = psmith; Pat Smith
Hacker blocked
SystemB Compromised by a hacker User = psmith; Pat Smith
Hacker
User = psmith; Pat Smithson

- Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall.
- Such trust should be limited to specific protocols and should be validated by something other than an IP address where possible.

CSIDS 4.0—2-43

You can mitigate trust and exploitation-based attacks through tight constraints on trust levels within a network. Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall. Such trust should be limited to specific protocols and should be authenticated by something other than an IP address where possible.



Port Redirection

- Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.
- It is mitigated primarily through the use of proper trust models.
- Antivirus software and host-based IDS can help detect and prevent a hacker installing port redirection utilities on the host.

CSIDS 4.0—2-44

Port redirection attacks are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. Consider a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment (commonly referred to as a Demilitarized Zone [DMZ]), but not the host on the inside. The host on the public services segment can reach the host on both the outside and the inside. If hackers were able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the inside host. Though neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of an application that can provide this type of access is netcat.

Port redirection can primarily be mitigated through the use of proper trust models, which are network specific (as mentioned earlier). Assuming a system under attack, a host-based IDS can help detect and prevent a hacker installing such utilities on a host.

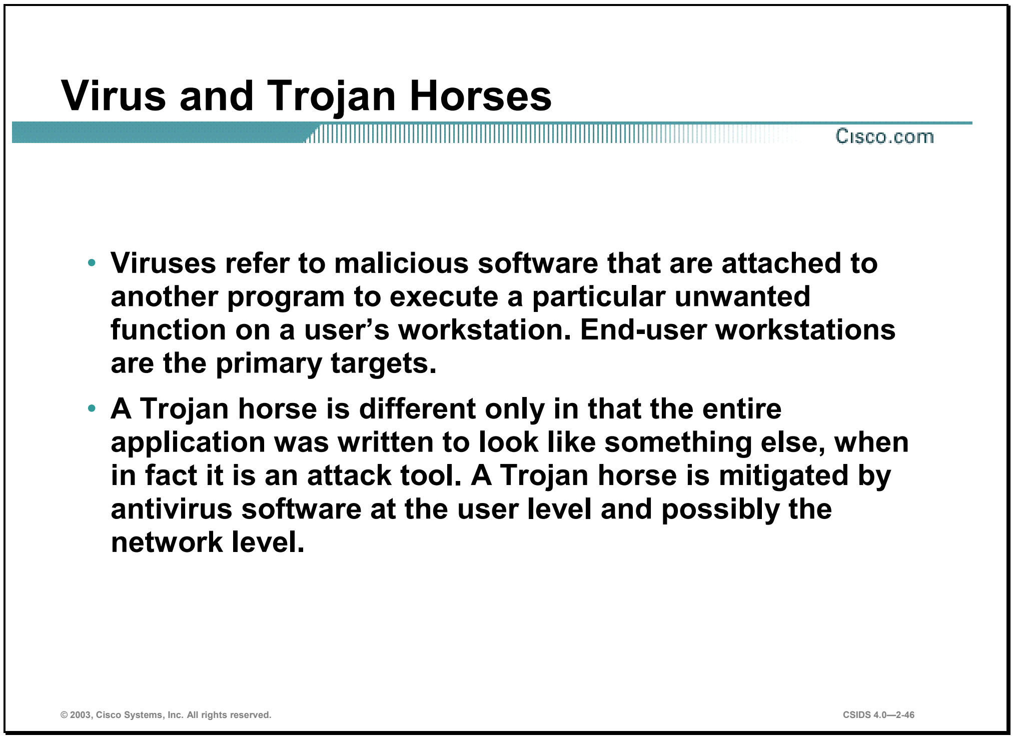
Unauthorized Access

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.

- Unauthorized access includes any unauthorized attempt to access a private resource:
  - Not a specific type of attack
  - Refers to most attacks executed in networks today
  - Initiated on both the outside and inside of a network
- The following are mitigation techniques for unauthorized access attacks:
  - Eliminate the ability of a hacker to gain access to a system
  - Prevent simple unauthorized access attacks, which is the primary function of a firewall

While not a specific type of attack, unauthorized access attacks refer to the majority of attacks executed in networks today. In order for someone to brute-force a Telnet login, they must first get the Telnet prompt on a system. Upon connection to the Telnet port, the hacker might see the message “authorization required to use this resource.” If the hacker continues to attempt access, the hacker’s actions become “unauthorized.” These kinds of attacks can be initiated both on the outside and inside of a network.

Mitigation techniques for unauthorized access attacks are very simple. They involve reducing or eliminating the ability of a hacker to gain access to a system using an unauthorized protocol. An example would be preventing hackers from having access to the Telnet port on a server that needs to provide web services to the outside. If a hacker cannot reach that port, it is very difficult to attack it. The primary function of a firewall in a network is to prevent simple unauthorized access attacks.



Virus and Trojan Horses

Cisco.com

- **Viruses refer to malicious software that are attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets.**
- **A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. A Trojan horse is mitigated by antivirus software at the user level and possibly the network level.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—2-46

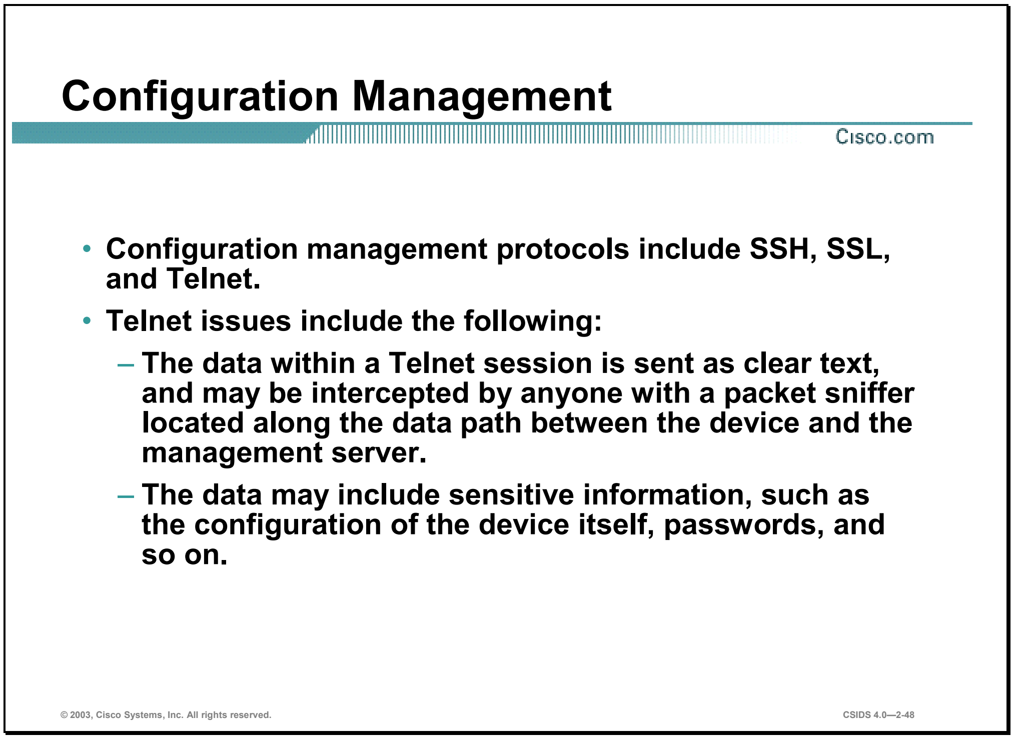
The primary vulnerabilities for end-user workstations are viruses and Trojan horse attacks. Viruses refer to malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. An example of a virus is a program that is attached to command.com (the primary interpreter for windows systems), which deletes certain files and infects any other versions of command.com that it can find.

A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. Then other users receive the game and play it, thus spreading the Trojan horse.

These kinds of applications can be contained through the effective use of antivirus software at the user level and potentially at the network level. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping up-to-date with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus or Trojan applications are released, enterprises need to keep up-to-date with the latest antivirus software, and application versions.

Management Protocols and Functions

The protocols used to manage your network can in themselves be a source of vulnerability. This section examines common management protocols and how they can be exploited.



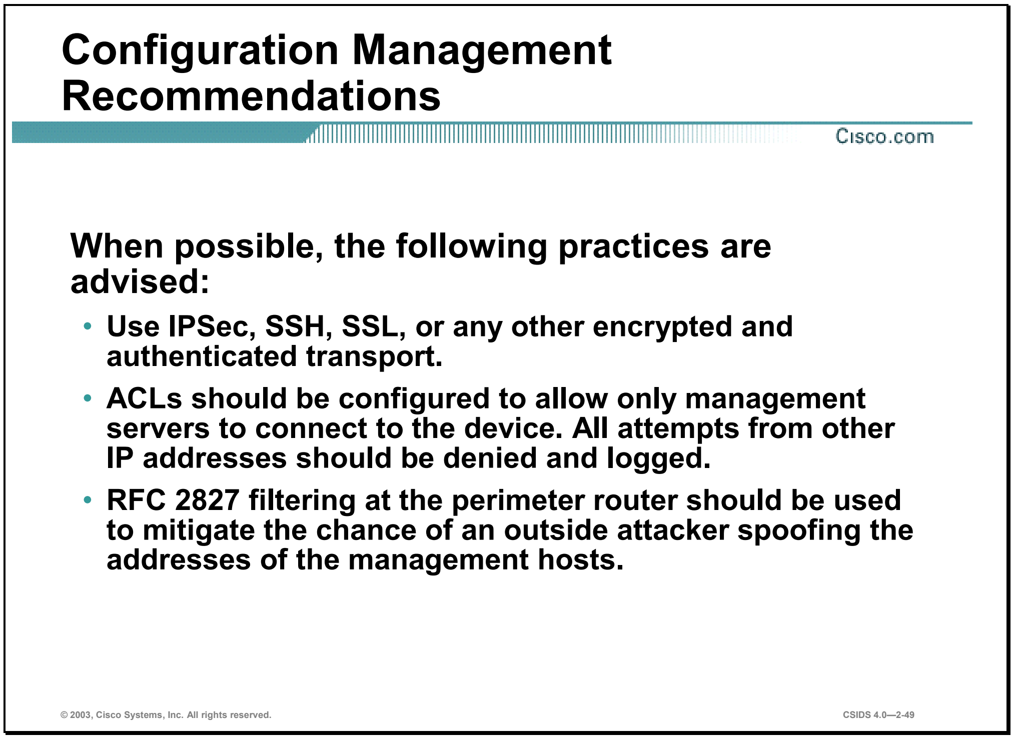
Configuration Management

Cisco.com

- Configuration management protocols include SSH, SSL, and Telnet.
- Telnet issues include the following:
  - The data within a Telnet session is sent as clear text, and may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server.
  - The data may include sensitive information, such as the configuration of the device itself, passwords, and so on.

CSIDS 4.0—2-48

If the managed device does not support any of the recommended protocols, such as SSH and SSL, Telnet may have to be used (although this protocol is not highly recommended). The network administrator should recognize that the data within a Telnet session is sent as clear text, and may be intercepted by anyone with a packet sniffer located along the data path between the managed device and the management server. The clear text may include important information, such as the configuration of the device itself, passwords, and other sensitive data.



Configuration Management Recommendations

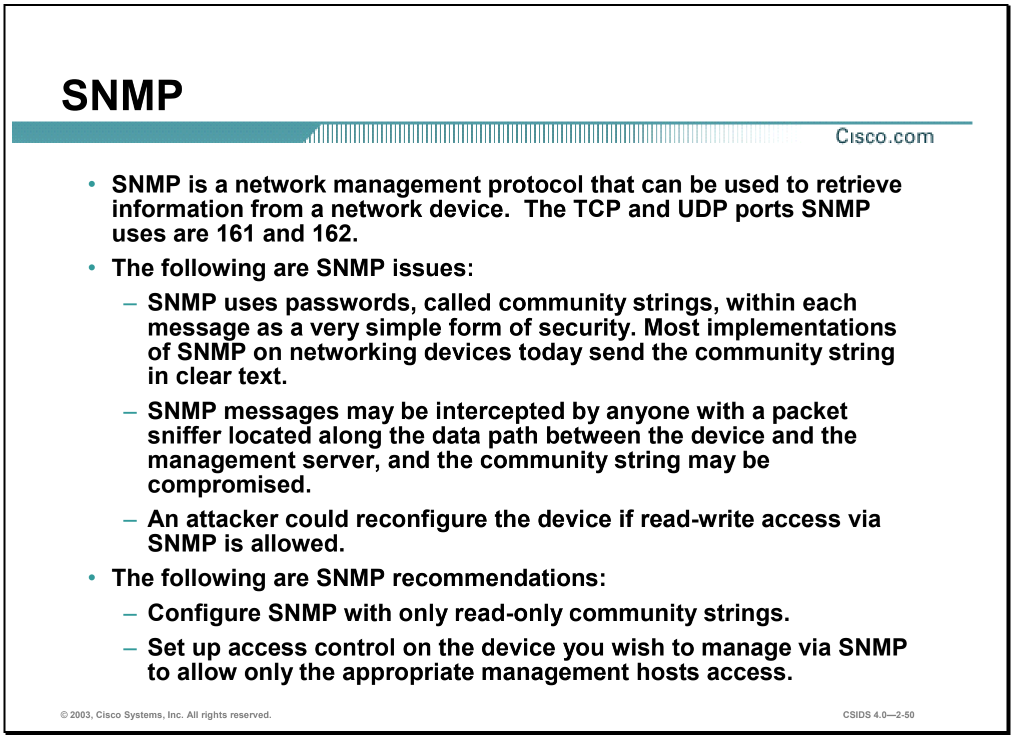
Cisco.com

When possible, the following practices are advised:

- **Use IPSec, SSH, SSL, or any other encrypted and authenticated transport.**
- **ACLs should be configured to allow only management servers to connect to the device. All attempts from other IP addresses should be denied and logged.**
- **RFC 2827 filtering at the perimeter router should be used to mitigate the chance of an outside attacker spoofing the addresses of the management hosts.**

CSIDS 4.0—2-49

Regardless of whether SSH, SSL, or Telnet is used for remote access to the managed device, access control lists (ACLs) should be configured to allow only management servers to connect to the device. All attempts from other IP addresses should be denied and logged. RFC 2827 filtering at the ingress router should also be implemented to mitigate the chance of an attacker from outside the network spoofing the addresses of the management hosts.



SNMP

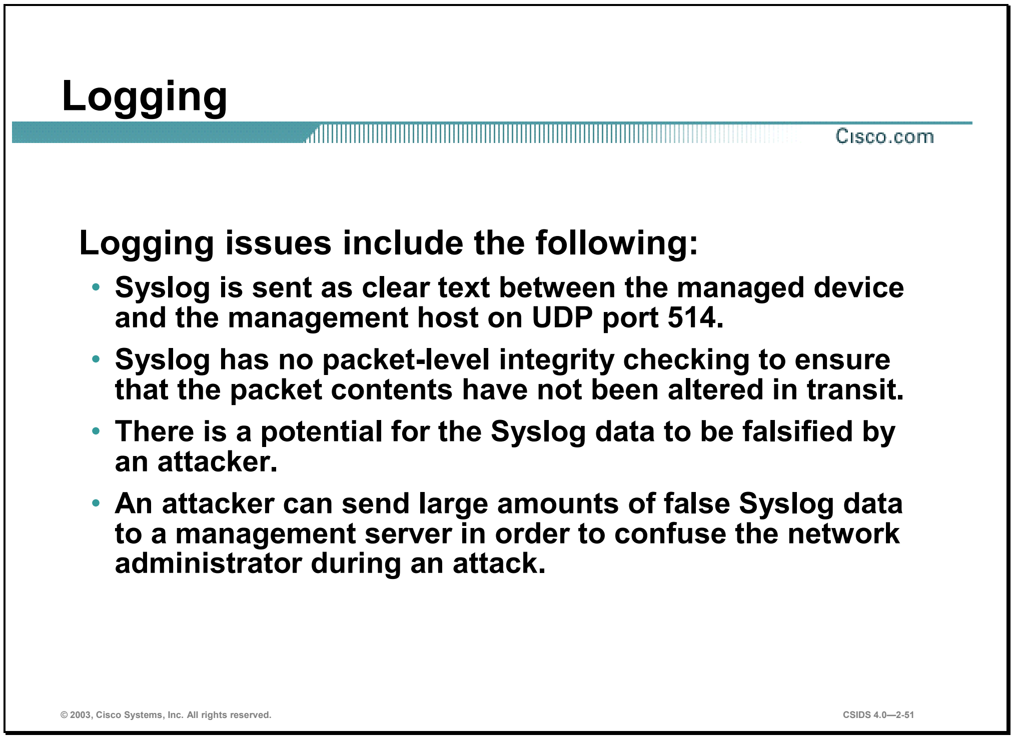
Cisco.com

- SNMP is a network management protocol that can be used to retrieve information from a network device. The TCP and UDP ports SNMP uses are 161 and 162.
- The following are SNMP issues:
  - SNMP uses passwords, called community strings, within each message as a very simple form of security. Most implementations of SNMP on networking devices today send the community string in clear text.
  - SNMP messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server, and the community string may be compromised.
  - An attacker could reconfigure the device if read-write access via SNMP is allowed.
- The following are SNMP recommendations:
  - Configure SNMP with only read-only community strings.
  - Set up access control on the device you wish to manage via SNMP to allow only the appropriate management hosts access.

CSIDS 4.0—2-50

SNMP is a network management protocol that can be used to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP uses passwords, called community strings, within each message as a very simple form of security. Unfortunately, most implementations of SNMP on networking devices today send the community string in clear text along with the message. Therefore, SNMP messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server, and the community string may be compromised.

When the community string is compromised, an attacker could reconfigure the device if read-write access via SNMP is allowed. Therefore, it is recommended that you configure SNMP with only read-only community strings. You can further protect yourself by setting up access control on the device you wish to manage via SNMP to allow only the appropriate management hosts access.



Logging

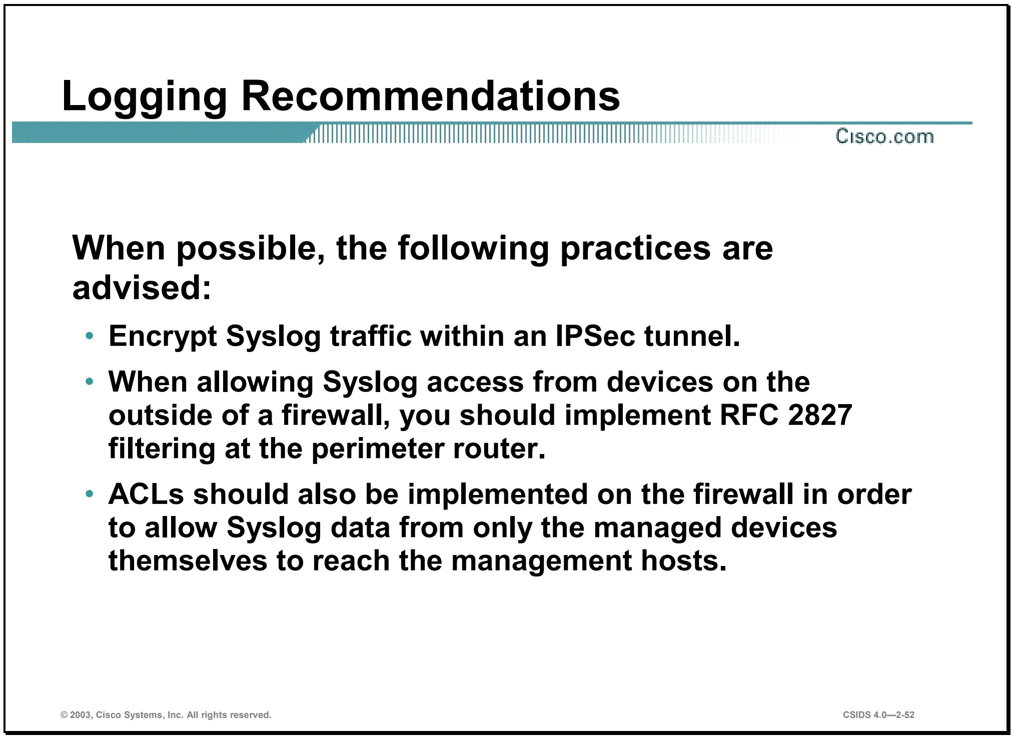
Cisco.com

Logging issues include the following:

- Syslog is sent as clear text between the managed device and the management host on UDP port 514.
- Syslog has no packet-level integrity checking to ensure that the packet contents have not been altered in transit.
- There is a potential for the Syslog data to be falsified by an attacker.
- An attacker can send large amounts of false Syslog data to a management server in order to confuse the network administrator during an attack.

CSIDS 4.0—2-51

Syslog, which is information generated by a device that has been configured for logging, is sent as clear text between the managed device and the management host. Syslog has no packet-level integrity checking to ensure that the packet contents have not been altered in transit. An attacker may alter Syslog data in order to confuse a network administrator during an attack.



Logging Recommendations

When possible, the following practices are advised:

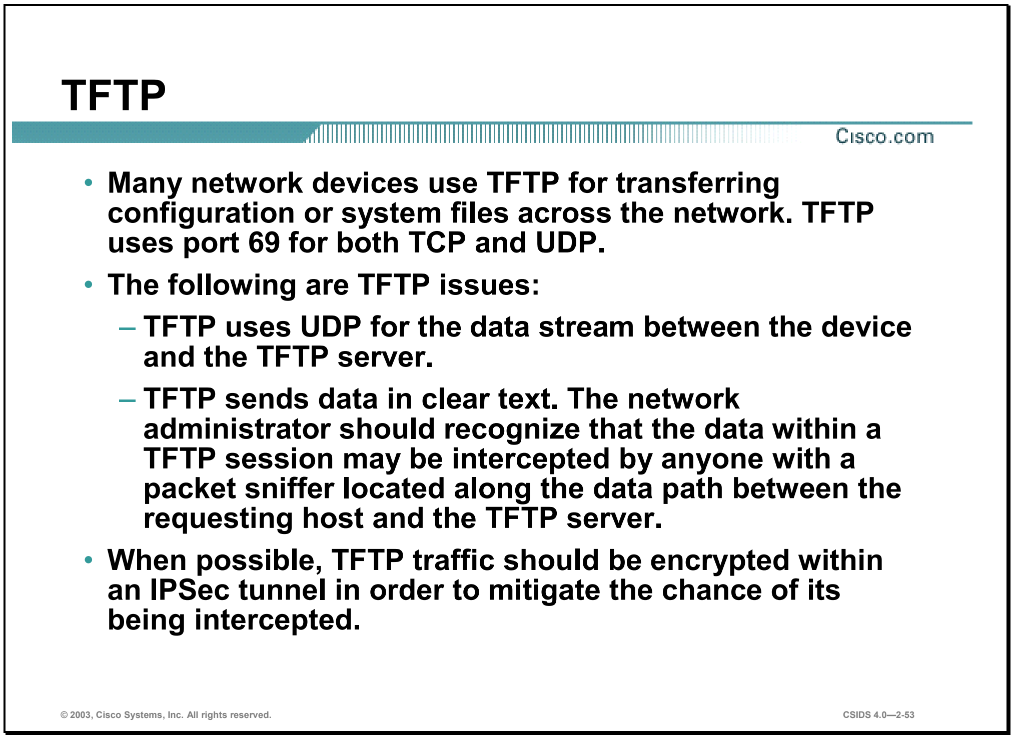
- **Encrypt Syslog traffic within an IPSec tunnel.**
- **When allowing Syslog access from devices on the outside of a firewall, you should implement RFC 2827 filtering at the perimeter router.**
- **ACLs should also be implemented on the firewall in order to allow Syslog data from only the managed devices themselves to reach the management hosts.**

CSIDS 4.0—2-52

Where possible, Syslog traffic may be encrypted within an IPSec tunnel in order to mitigate the chance of its being altered in transit. Where the Syslog data cannot be encrypted within an IPSec tunnel because of cost or the capabilities of the device itself, the network administrator should note that there is a potential for the Syslog data to be falsified by an attacker.

When allowing Syslog access from devices on the outside of a firewall, RFC 2827 filtering at the egress router should be implemented. This scenario will mitigate the chance of an attacker from outside the network spoofing the address of the managed device, and sending false Syslog data to the management hosts.

ACLs should also be implemented on the firewall in order to allow Syslog data from only the managed devices themselves to reach the management hosts. This scenario prevents an attacker from sending large amounts of false Syslog data to a management server in order to confuse the network administrator during an attack.



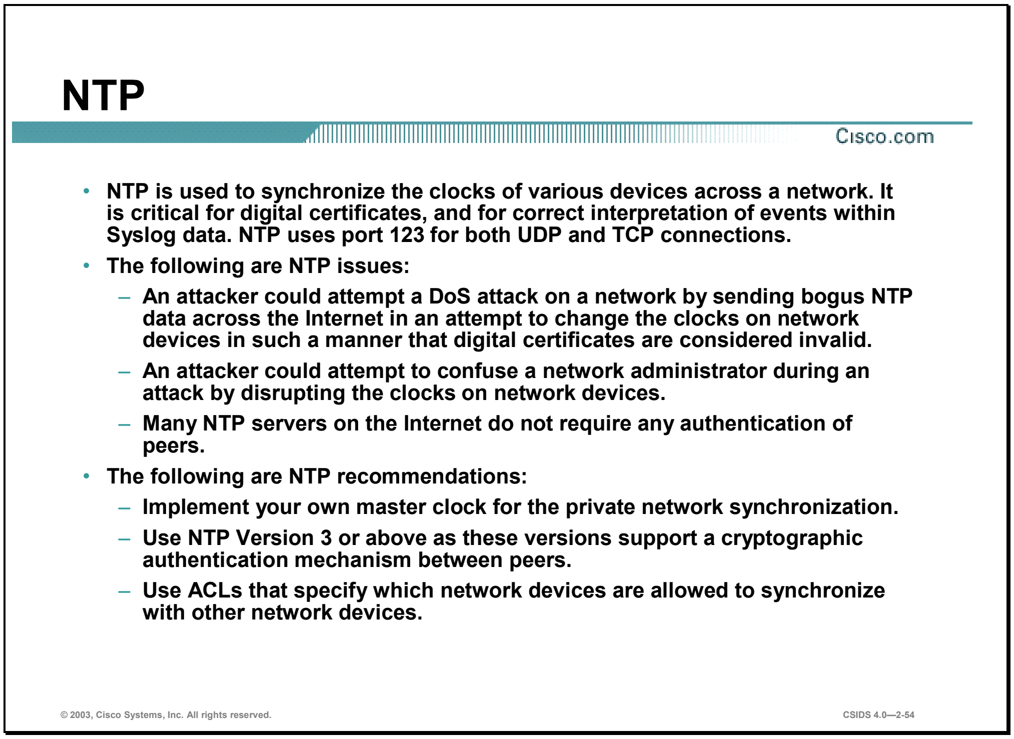
TFTP

- Many network devices use TFTP for transferring configuration or system files across the network. TFTP uses port 69 for both TCP and UDP.
- The following are TFTP issues:
  - TFTP uses UDP for the data stream between the device and the TFTP server.
  - TFTP sends data in clear text. The network administrator should recognize that the data within a TFTP session may be intercepted by anyone with a packet sniffer located along the data path between the requesting host and the TFTP server.
- When possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.

CSIDS 4.0—2-53

Many network devices use TFTP for transferring configuration or system files across the network. TFTP uses UDP for the data stream between the requesting host and the TFTP server.

As with other management protocols that send data in clear text, the network administrator should recognize that the data within a TFTP session might be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. Where possible, TFTP traffic should be encrypted within an IPSec tunnel in order to mitigate the chance of its being intercepted.



NTP

Cisco.com

- NTP is used to synchronize the clocks of various devices across a network. It is critical for digital certificates, and for correct interpretation of events within Syslog data. NTP uses port 123 for both UDP and TCP connections.
- The following are NTP issues:
  - An attacker could attempt a DoS attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices in such a manner that digital certificates are considered invalid.
  - An attacker could attempt to confuse a network administrator during an attack by disrupting the clocks on network devices.
  - Many NTP servers on the Internet do not require any authentication of peers.
- The following are NTP recommendations:
  - Implement your own master clock for the private network synchronization.
  - Use NTP Version 3 or above as these versions support a cryptographic authentication mechanism between peers.
  - Use ACLs that specify which network devices are allowed to synchronize with other network devices.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—2-54

Network Time Protocol (NTP) is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is critical for digital certificates, and for correct interpretation of events within Syslog data.

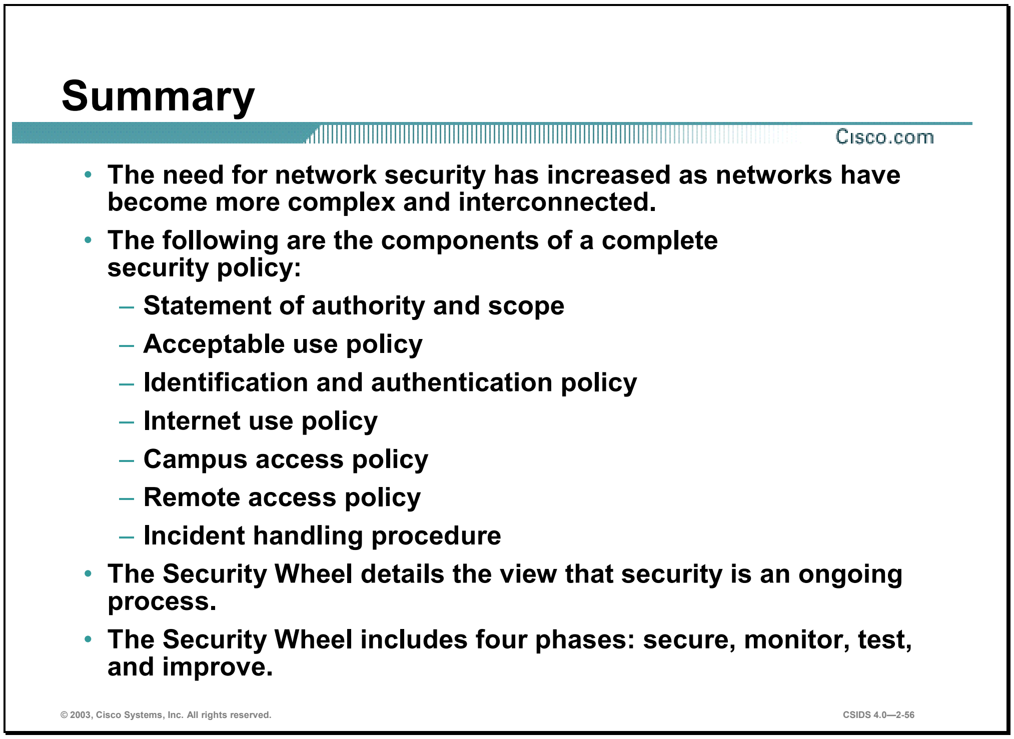
A secure method of providing clocking for the network is for the network administrator to implement their own master clock for the private network synchronized to Coordinated Universal Time (UTC) via satellite or radio. However, clock sources are available to synchronize to via the Internet, if the network administrator does not wish to implement their own master clock because of costs or other reasons.

An attacker could attempt a DoS attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices in such a manner that digital certificates are considered invalid. Further, an attacker could attempt to confuse a network administrator during an attack by disrupting the clocks on network devices. This scenario would make it difficult for the network administrator to determine the order of Syslog events on multiple devices.

Version 3 and above of NTP supports a cryptographic authentication mechanism between peers. The use of the authentication mechanism as well as ACLs that specify which network devices are allowed to synchronize with other network devices is recommended to help mitigate against such a scenario. The network administrator should weigh the cost benefits of pulling clock information from the Internet with the possible risk of doing so and allowing it through the firewall. Many NTP servers on the Internet do not require any authentication of peers. Therefore, the network administrator must trust that the clock itself is reliable, valid, and secure.

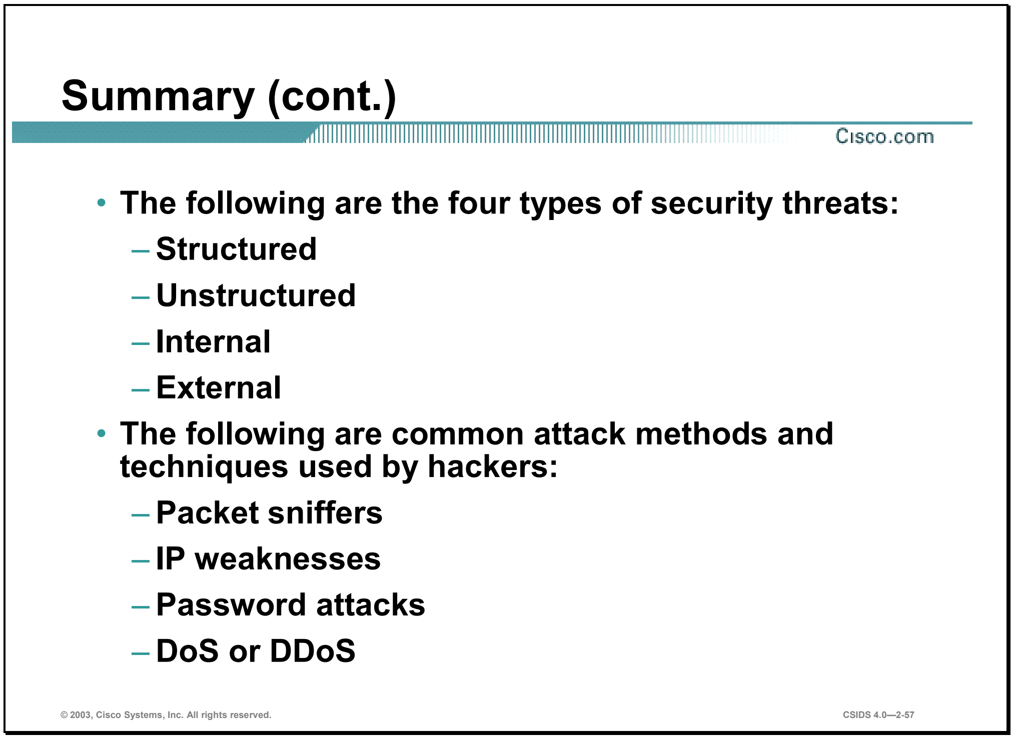
Summary

This section summarizes the information you learned in this chapter.



Summary

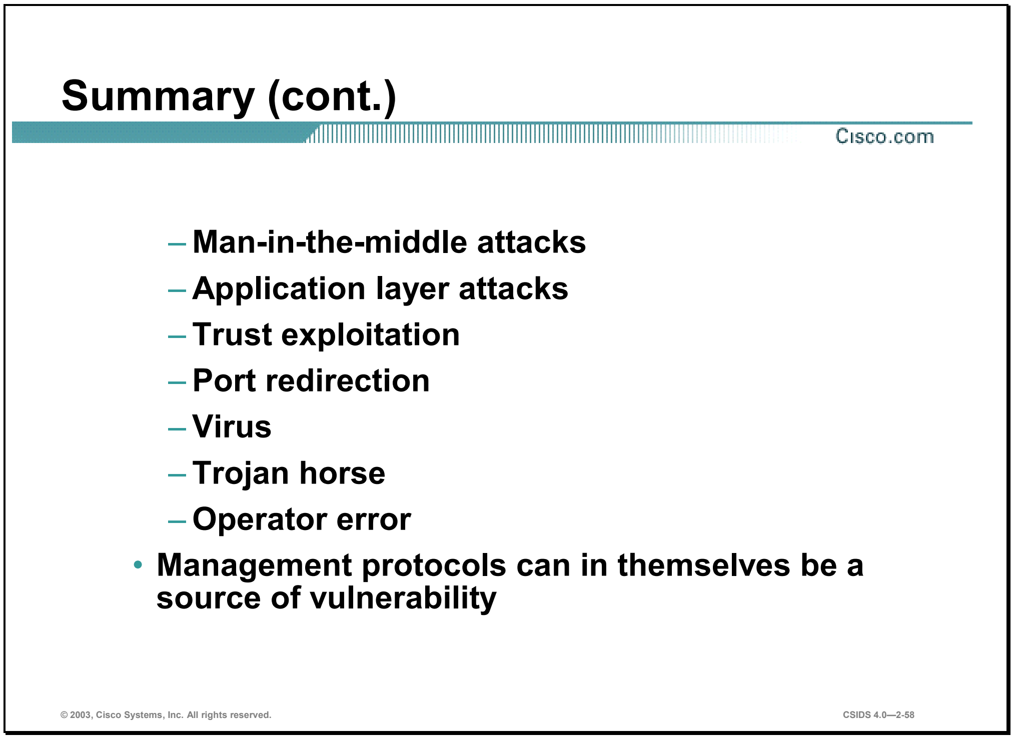
- The need for network security has increased as networks have become more complex and interconnected.
- The following are the components of a complete security policy:
  - Statement of authority and scope
  - Acceptable use policy
  - Identification and authentication policy
  - Internet use policy
  - Campus access policy
  - Remote access policy
  - Incident handling procedure
- The Security Wheel details the view that security is an ongoing process.
- The Security Wheel includes four phases: secure, monitor, test, and improve.



Summary (cont.)

- The following are the four types of security threats:
  - Structured
  - Unstructured
  - Internal
  - External
- The following are common attack methods and techniques used by hackers:
  - Packet sniffers
  - IP weaknesses
  - Password attacks
  - DoS or DDoS

CSIDS 4.0—2-57



Summary (cont.)

- Man-in-the-middle attacks
- Application layer attacks
- Trust exploitation
- Port redirection
- Virus
- Trojan horse
- Operator error

- Management protocols can in themselves be a source of vulnerability

CSIDS 4.0—2-58

3

Intrusion Detection Overview

Overview

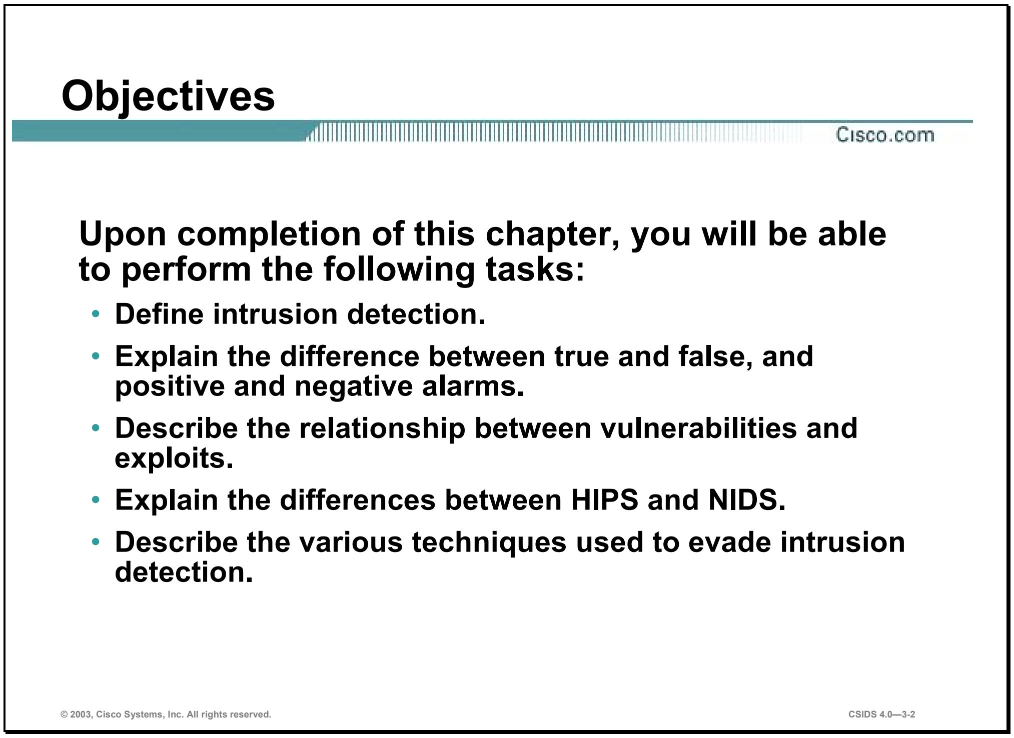
This chapter provides the fundamental knowledge required to understand an Intrusion Detection System (IDS).

This chapter includes the following topics:

- Objectives
- Intrusion detection terminology
- Intrusion detection technologies
- Host-based intrusion protection
- Network-based intrusion detection systems
- Intrusion detection evasive techniques
- Summary

Objectives

This section lists the chapter objectives.



Objectives

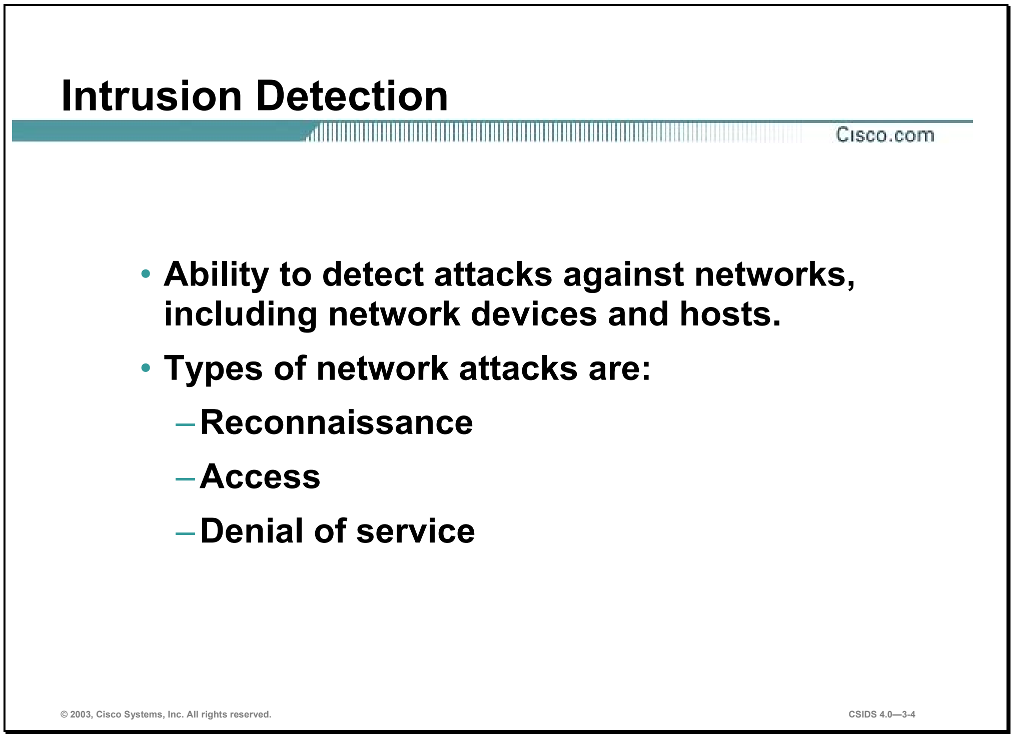
Upon completion of this chapter, you will be able to perform the following tasks:

- **Define intrusion detection.**
- **Explain the difference between true and false, and positive and negative alarms.**
- **Describe the relationship between vulnerabilities and exploits.**
- **Explain the differences between HIPS and NIDS.**
- **Describe the various techniques used to evade intrusion detection.**

CSIDS 4.0—3-2

Intrusion Detection Terminology

This sections provides definitions and explanations for commonly used terms associated with intrusion detection.



Intrusion Detection

Cisco.com

- Ability to detect attacks against networks, including network devices and hosts.
- Types of network attacks are:
  - Reconnaissance
  - Access
  - Denial of service

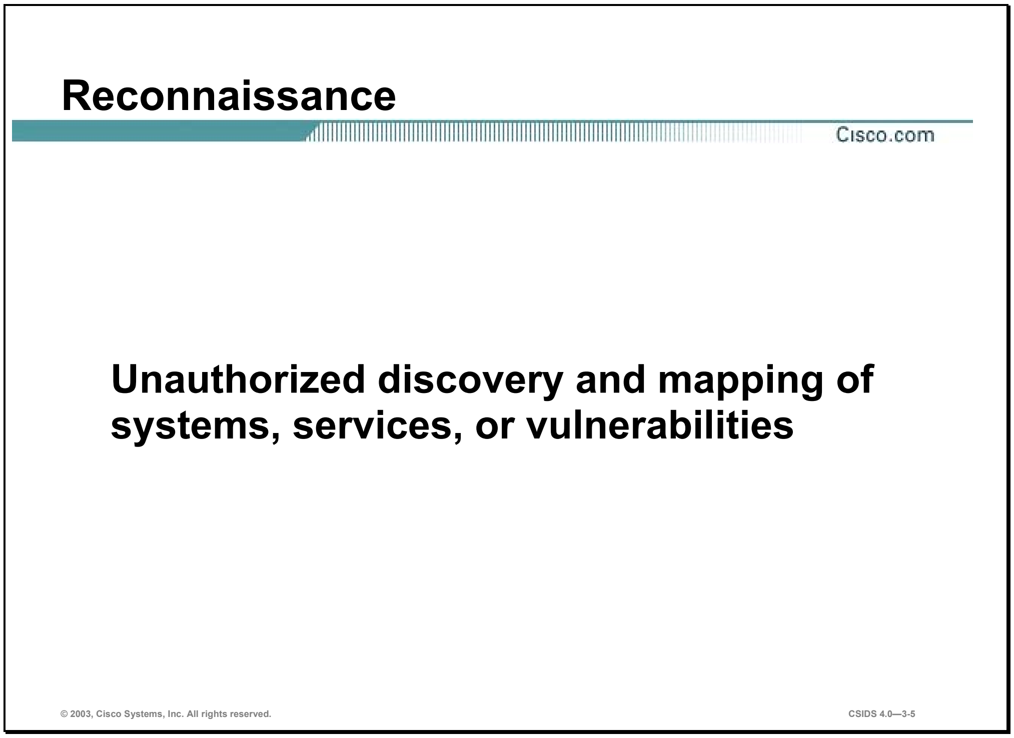
CSIDS 4.0—3-4

Intrusion detection is the ability to detect attacks against your network. The network can be made up of network devices such as routers, printers, firewalls, and servers.

Note Intrusion detection has been defined as the ability to detect misuse, abuse, and unauthorized access to networked resources.

The following are three types of network attacks:

- Reconnaissance attacks—An intruder is attempting to discover and map systems, services, or vulnerabilities.
- Access attacks—An intruder attacks networks or systems to retrieve data, gain access, or escalate their access privileges.
- Denial of service (DoS) attacks—An intruder attacks your network in a manner that damages or corrupts your computer system, or denies legitimate users access to the network, systems, or services.



Reconnaissance

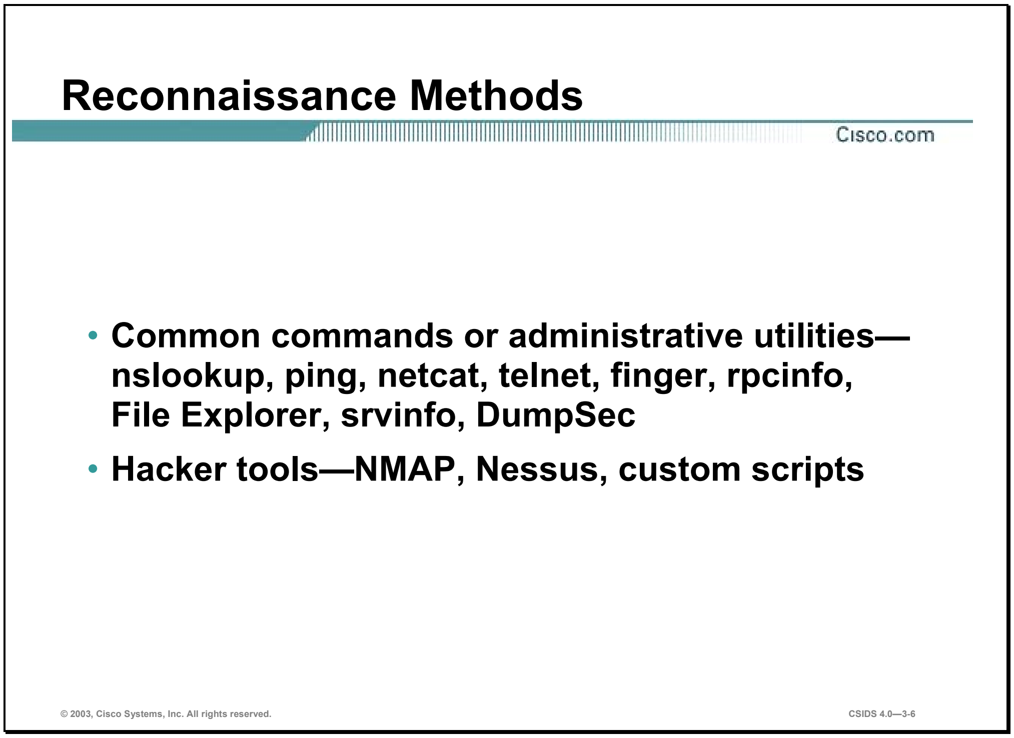
Cisco.com

Unauthorized discovery and mapping of systems, services, or vulnerabilities

CSIDS 4.0—3-5

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is known as information gathering and, in most cases, precedes an actual access or denial of service attack. The malicious intruder typically ping sweeps the target network first to determine what IP addresses are alive. After this is accomplished, the intruder determines what network services or ports are active on the live IP addresses by performing a port sweep or port scan. From this information the intruder queries the ports to determine the application type and version as well as the type and version of operating system running on the target host. Based on this information, the intruder can determine if a possible vulnerability exists that can be exploited.

Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes, such as an unoccupied residence, an easy-to-open door or window, and so on. In many cases the intruders go as far as “rattling the door handle,” not to go in immediately if open, but to discover vulnerable services that they can exploit at a later time when no one is looking.



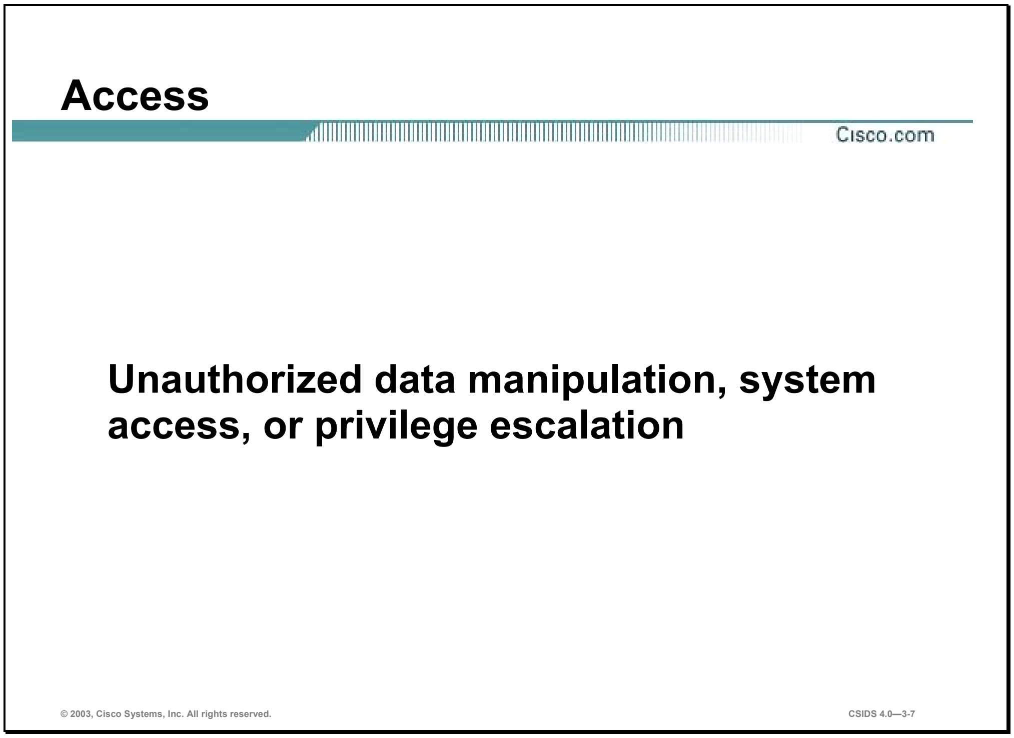
Reconnaissance Methods

- Common commands or administrative utilities—nslookup, ping, netcat, telnet, finger, rpcinfo, File Explorer, srvinfo, DumpSec
- Hacker tools—NMAP, Nessus, custom scripts

CSIDS 4.0—3-6

Performing reconnaissance involves the use of common commands or utilities available in all operating systems. For example, using the nslookup and whois utilities, the attacker can easily determine the IP address space assigned to a given corporation or entity. The **ping** command tells the attacker what IP addresses are "alive" on the network.

Hacker tools are used to perform reconnaissance. These tools make it easy for the less knowledgeable attackers to do reconnaissance since they automate the process and provide a user-friendly interface that anyone can use.



Access

Cisco.com

Unauthorized data manipulation, system access, or privilege escalation

© 2003, Cisco Systems, Inc. All rights reserved.

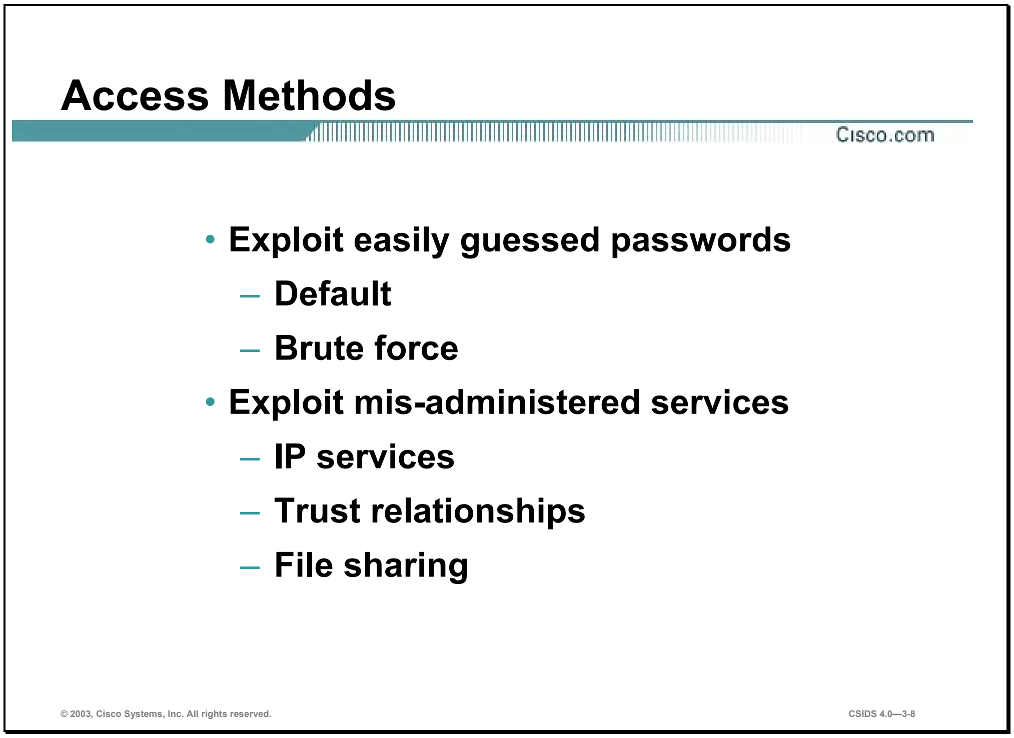
CSIDS 4.0—3-7

Access is an all-encompassing term that refers to unauthorized data manipulation, system access, or privileged escalation. Unauthorized data retrieval is simply reading, writing, copying, or moving files that are not intended to be accessible to the intruder. Sometimes this is as easy as finding shared folders in Windows or NFS exported directories in UNIX systems with read or read and write access to everyone. The intruder will have no problems getting to the files and, more often than not, the accessible information is highly confidential and completely unprotected from prying eyes, especially if the attacker is an internal user.

System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or password. Entering or accessing systems to which one does not have access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Another form of access attacks involves privilege escalation. Privilege escalation occurs when users obtain privileges or rights to objects that were not assigned by administrators. Objects can be files, commands, or other components on a network device. The intent is to gain access to information or execute procedures for which they are not authorized at their current levels of access. In many cases this involves gaining administrative privileges to systems or devices to install sniffers, create backdoor accounts, or delete log files.

In some cases intruders want to gain access without necessarily wanting to steal information—especially when the motive is intellectual challenge, curiosity, or ignorance.



Access Methods

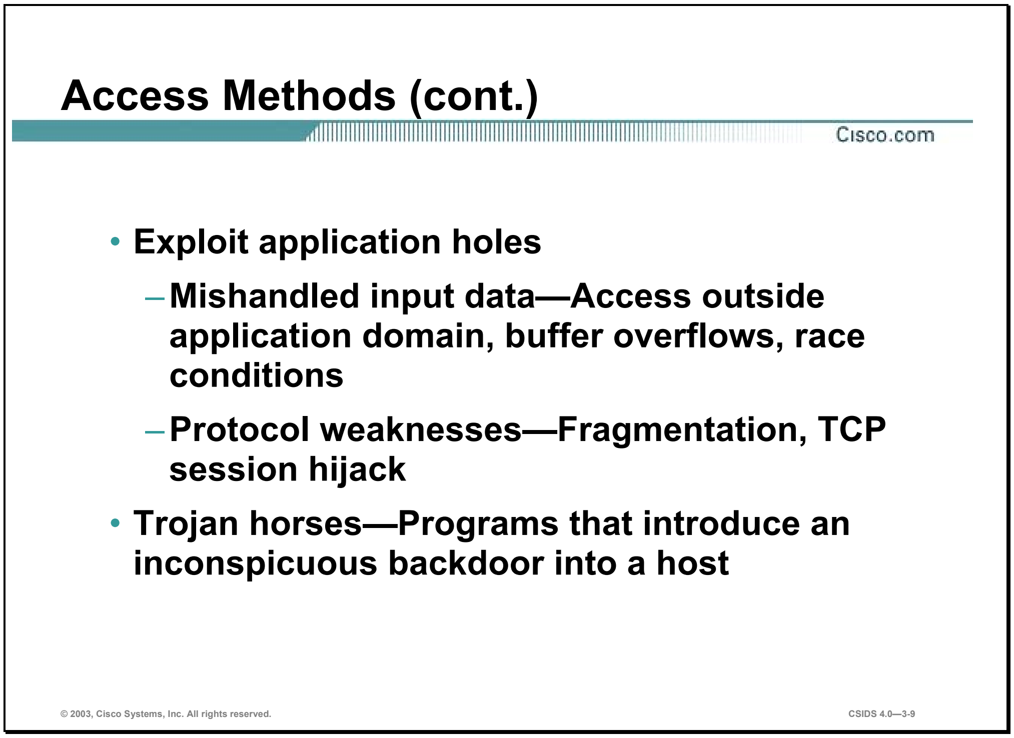
- Exploit easily guessed passwords
  - Default
  - Brute force
- Exploit mis-administered services
  - IP services
  - Trust relationships
  - File sharing

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—3-8

Access methods are varied and run the entire gamut between simple command-line hacks to sophisticated tools with nice user interfaces. Usually, the first line of defense when it comes to access attacks is strong authentication. In many cases, user passwords are too easily guessed by attempting to enter default passwords or brute force attacks. These attacks involve attempting to log onto a host with a common user name and then trying different password combinations that are commonly used. This technique is especially effective if the attacker has some prior knowledge about the user being targeted.

Exploiting mis-administered services is simply taking advantage of services that are poorly installed and administered by novice or unknowing administrators. One of the easiest services to exploit is file sharing. Too often users share their files by creating a shared folder or directory with full access to everyone, and sometimes a user does not realize that others can access the folder. This can be prevented with password-protected shares, or sharing only with intended users. Other common mis-administered services are anonymous FTP and TFTP servers, SNMP, Windows registry access, and trust relationships.



Access Methods (cont.)

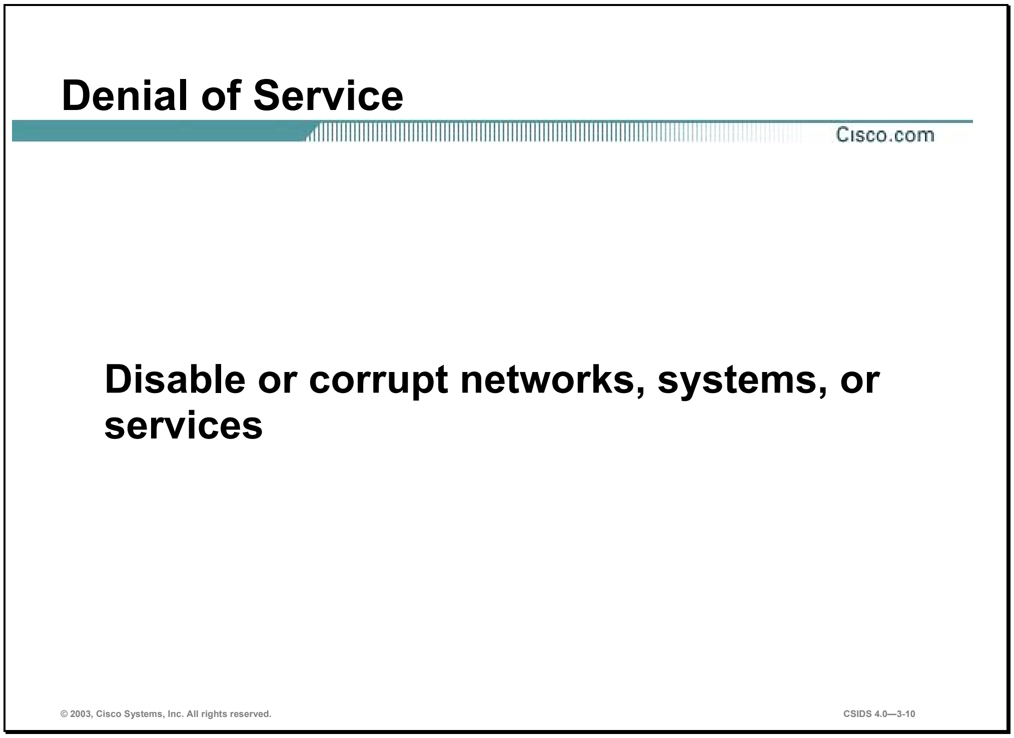
- Exploit application holes
  - Mishandled input data—Access outside application domain, buffer overflows, race conditions
  - Protocol weaknesses—Fragmentation, TCP session hijack
- Trojan horses—Programs that introduce an inconspicuous backdoor into a host

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—3-9

Application security holes have been around since the first piece of software was written. These holes are usually a result of unanticipated behavior of software code or unexpected inputs. An example of this is a program that breaks out into a root shell when receiving an out-of-band input.

Protocol weaknesses are types of application holes. Examples of this are IP fragmentation and TCP session hijack. The attacker is taking advantage of protocol design deficiencies that the original designers did not anticipate.

Finally Trojan horses are used to gain unauthorized access by tricking a legitimate user to run Trojan programs that install or open back doors for attackers to secretly break in. Then the attackers, circumventing in many cases any authentication procedures, enter through the back door.

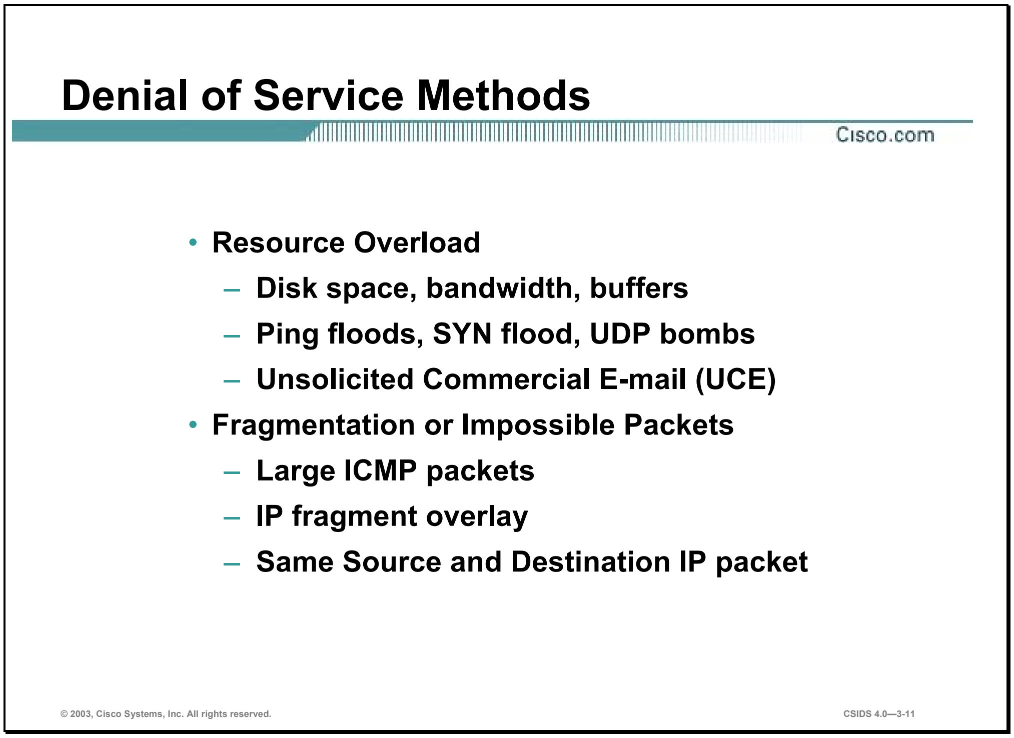


Denial of Service

Disable or corrupt networks, systems, or services

CSIDS 4.0—3-10

Denial of Service (DoS) is an attacker disabling or corrupting networks, systems, or services with the intent of denying the service to intended users. It usually involves either crashing the system or slowing it to the point that it is unusable. But DoS can be as simple as wiping out or corrupting information necessary for business. In most cases, performing the attack involves simply running a hack, script, or tool. The attacker does not need prior access to the target because all that is usually required is a way to get to it. For these reasons and because of the great damaging potential, DoS attacks are the most feared by companies conducting business that uses the Internet.



Denial of Service Methods

Cisco.com

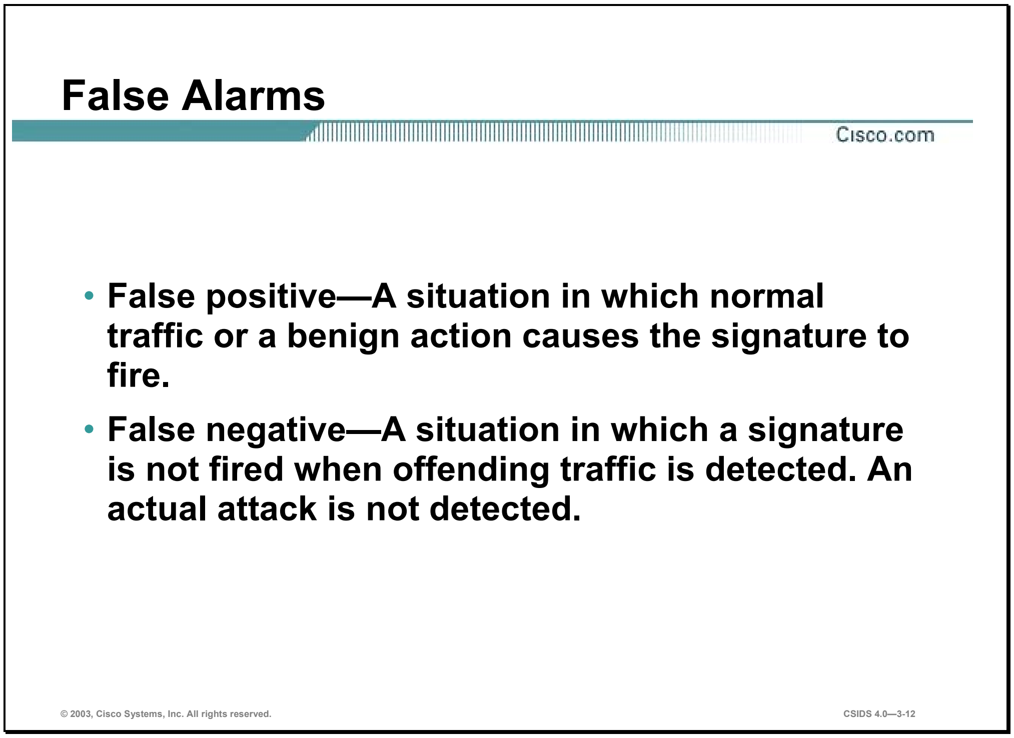
- Resource Overload
  - Disk space, bandwidth, buffers
  - Ping floods, SYN flood, UDP bombs
  - Unsolicited Commercial E-mail (UCE)
- Fragmentation or Impossible Packets
  - Large ICMP packets
  - IP fragment overlay
  - Same Source and Destination IP packet

CSIDS 4.0—3-11

Denial of Service (DoS) attack methods include everything from simple one-line commands to sophisticated programs, written by knowledgeable hackers.

Common resource overload attacks include ping floods (smurf), TCP SYN floods (neptune), and packet storms (UDP bomb and fraggle). Unsolicited Commercial E-mail (UCE), often referred to as SPAM, attempts to overload mail servers.

Some attacks to generate fragmented or impossible packets are the ping of death, winnuke, and landteardrop. One infamous hack tool, targa, combines seven attacks in one: bonk, winnuke, teardrop, land, jolt, nestea, newtear, and syndrop.



False Alarms

- False positive—A situation in which normal traffic or a benign action causes the signature to fire.
- False negative—A situation in which a signature is not fired when offending traffic is detected. An actual attack is not detected.

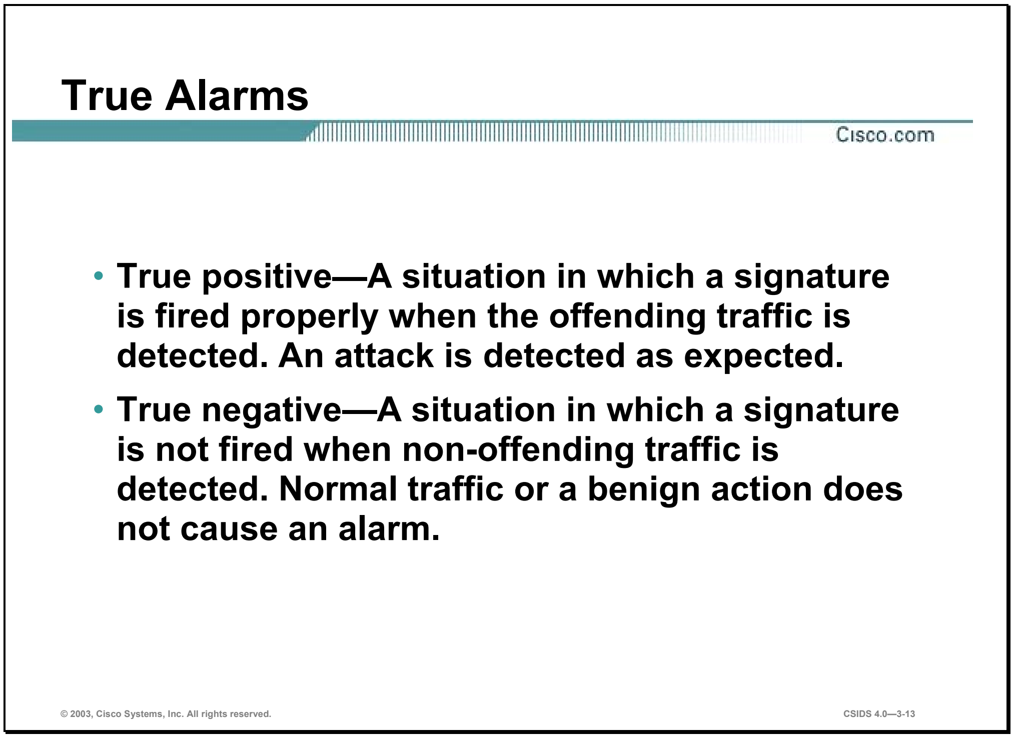
CSIDS 4.0—3-12

The ability for an intrusion detection product to accurately detect an attack or a policy violation and generate an alarm is critical to its functionality. The two forms of false alarms are false positives and false negatives.

A false positive is a situation in which normal traffic or a benign action causes the signature to fire. Consider the following scenario: a signature exists that generates alarms if any network devices' enable password is entered incorrectly. A network administrator attempts to log in to a Cisco router but mistakenly enters the wrong password. The IDS cannot distinguish between a rogue user and the network administrator, and generates an alarm.

A false negative is a situation in which a signature is not fired when offending traffic is detected. Offending traffic can be as simple as someone sending confidential documents outside of the corporate network to an attack against corporate web servers. False negatives should be considered software bugs and reported in accordance to the software license agreement.

Note A false negative should only be considered a software bug if in fact the IDS has a signature that has been designed to detect the offending traffic.



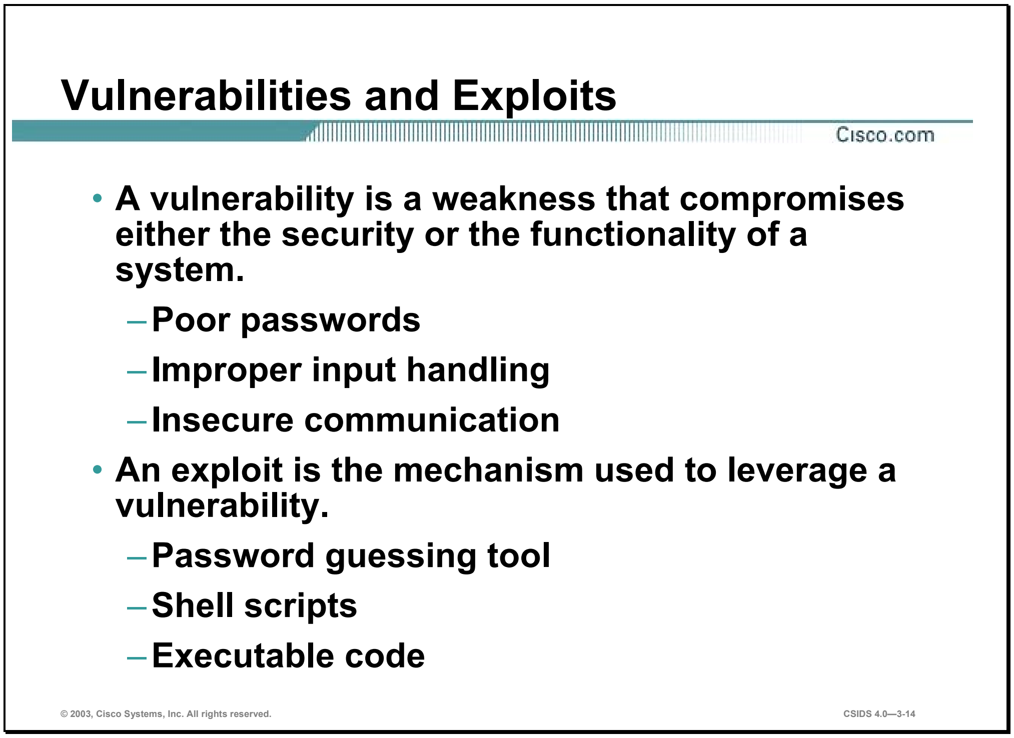
True Alarms

- True positive—A situation in which a signature is fired properly when the offending traffic is detected. An attack is detected as expected.
- True negative—A situation in which a signature is not fired when non-offending traffic is detected. Normal traffic or a benign action does not cause an alarm.

CSIDS 4.0—3-13

Like false alarms, there are two forms of true alarms. A true positive is a situation in which a signature is fired properly when offending traffic is detected and an alarm is generated. For example, Cisco IDS Sensors have signatures that detect Unicode attacks against Microsoft IIS web servers. If a Unicode attack is launched against Microsoft IIS web servers, the Sensors detect the attack and generate an alarm.

A true negative is a situation in which a signature is not fired when non-offending traffic is captured and analyzed. In other words, the Sensor does not fire an alarm when it captures and analyzes ‘normal’ network traffic.



Vulnerabilities and Exploits

Cisco.com

- A vulnerability is a weakness that compromises either the security or the functionality of a system.
  - Poor passwords
  - Improper input handling
  - Insecure communication
- An exploit is the mechanism used to leverage a vulnerability.
  - Password guessing tool
  - Shell scripts
  - Executable code

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—3-14

A vulnerability is a weakness that compromises either the security or functionality of a system. The following are examples of vulnerabilities:

- Poor passwords—Passwords are the first line of defense. Weak or easily guessed passwords are considered vulnerabilities.

- Improper input handling—Software that does not properly handle all possible input can have unexpected results. Often this leads to either a DoS or access to restricted system resources.

- Insecure communication—Data that is transferred in clear-text is susceptible to interception. The information can be system passwords, employee records, and confidential company documents are some examples of data that is vulnerable to interception.

An exploit is the mechanism used to leverage a vulnerability to compromise the security or functionality of a system. The following are examples of exploits:

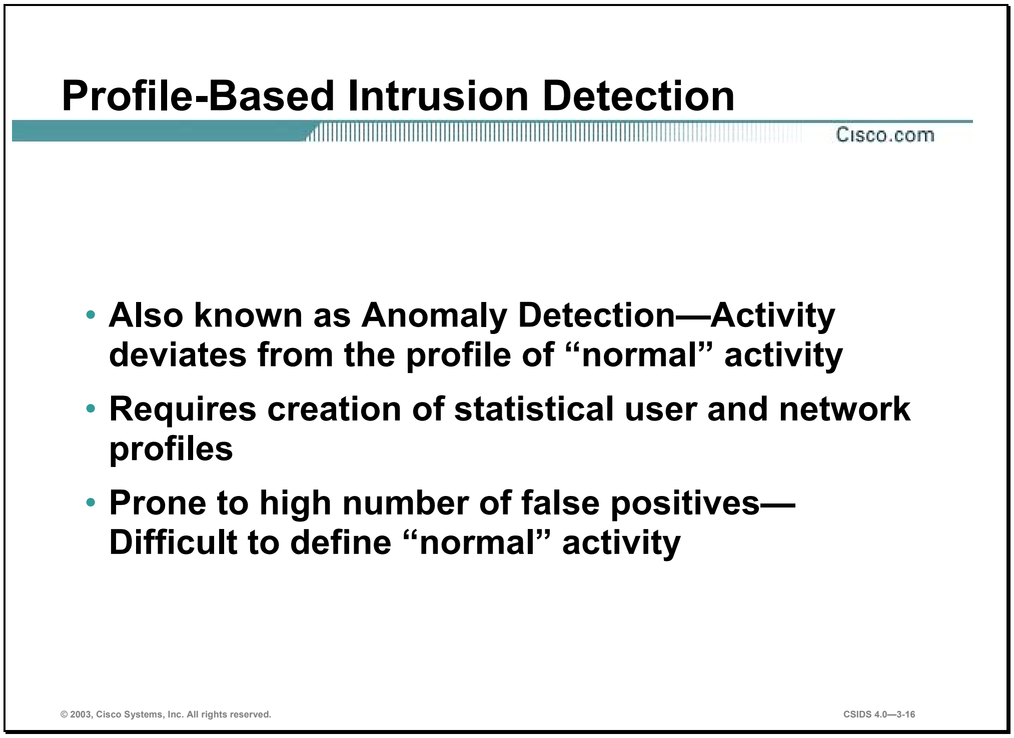
- Password guessing tools—These tools attempt to "crack" passwords by using knowledge of the algorithm used to generate the actual password or by attempting to access a system using permutations and combinations of different character sets. Some popular password cracking tools are L0phtcrack and john the ripper.

- Shell or batch scripts—These scripts are created to automate attacks or perform simple procedures known to expose the vulnerability.

- Executable code—Exploits written as executable code require programming knowledge and access to software tools such as a compiler. Consequently, executable code exploits are considered to be more advanced forms of exploitation.

Intrusion Detection Technologies

This section describes the various technologies implemented in IDSs. Cisco IDS Sensors use a blend of the technologies discussed in this section. For more information refer to the Cisco white paper, *The Science of Intrusion Detection System Attack Identification*. This white paper can be found at: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idssa_wp.htm.



Profile-Based Intrusion Detection

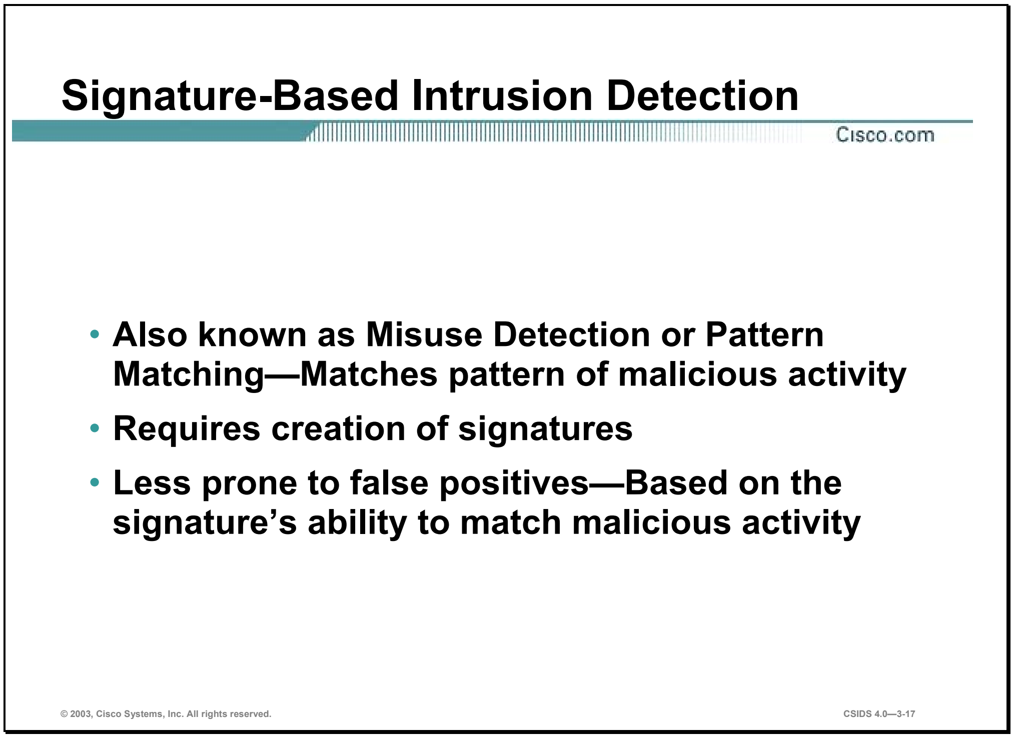
Cisco.com

- **Also known as Anomaly Detection—Activity deviates from the profile of "normal" activity**
- **Requires creation of statistical user and network profiles**
- **Prone to high number of false positives—Difficult to define "normal" activity**

CSIDS 4.0—3-16

Profile-based intrusion detection generates an alarm when activity on the network goes outside of the profile. By collecting examples of user and network activity, you can build a profile of normal activity. For example, a web server farm would typically generate web (HTTP) traffic. A profile could be created to monitor web traffic. Another example is a network segment where the users are helpdesk technicians. The help desk technician's primary function is to monitor e-mail requests. A profile could be created to monitor mail (SMTP) traffic.

The problem with this method of intrusion detection is that users do not feel a responsibility to follow a profile. Humans do not consistently keep to a normal pattern; consequently, what may be defined as normal activity today might not be normal activity tomorrow. Simply put: there is too much variation in the way users act on the network for this type of detection to be effective. For example, some help desk technicians may access the web or telnet to systems in order to troubleshoot problems. Based on the profile created, this type of network activity would trigger alarms, although the alarms are likely to be benign.



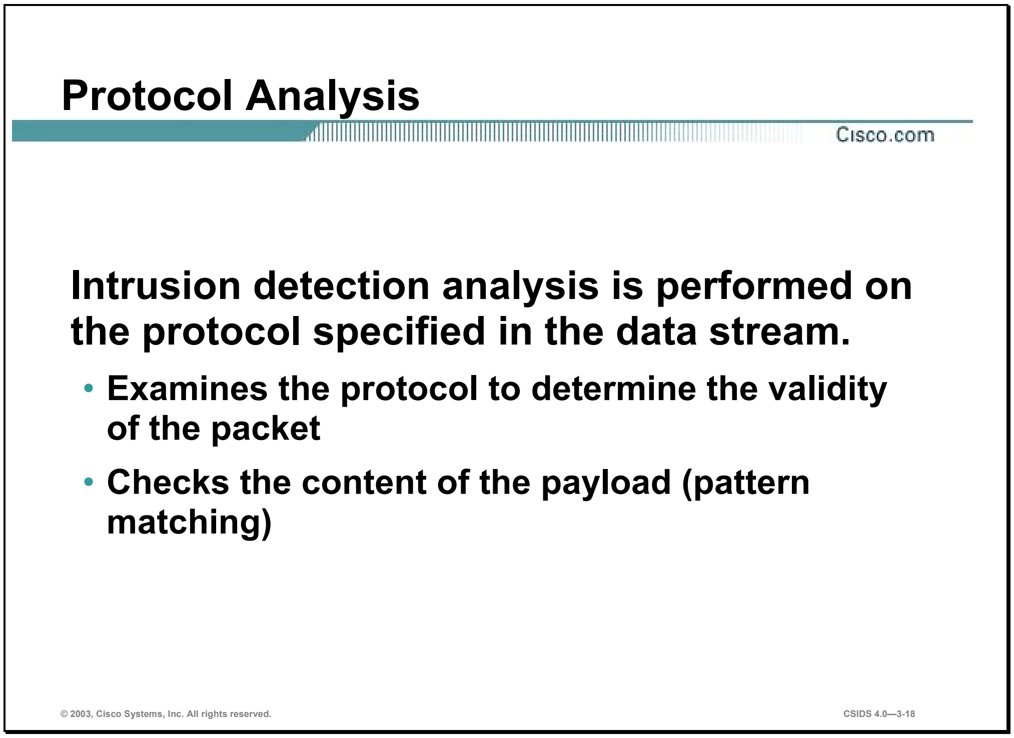
Signature-Based Intrusion Detection

- Also known as Misuse Detection or Pattern Matching—Matches pattern of malicious activity
- Requires creation of signatures
- Less prone to false positives—Based on the signature's ability to match malicious activity

CSIDS 4.0—3-17

Signature-based intrusion detection is less prone to false positives when detecting unauthorized activity. A signature is a set of rules pertaining to typical intrusion activity. Highly skilled network engineers research known attacks and vulnerabilities and can develop signatures to detect these attacks and vulnerabilities.

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



Protocol Analysis

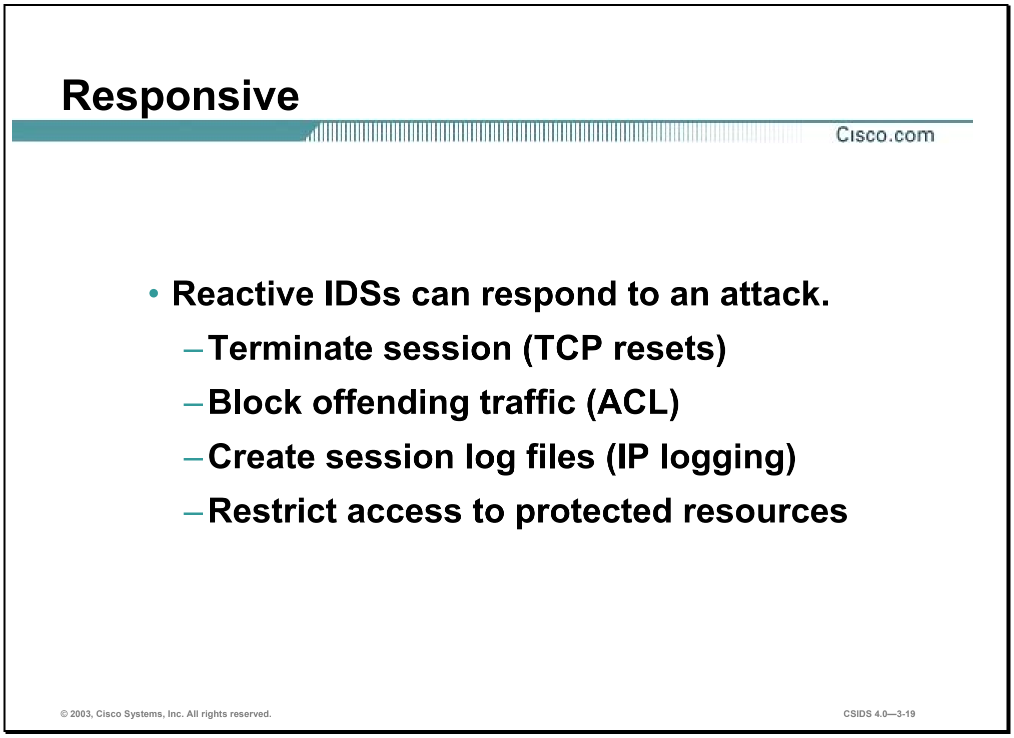
Cisco.com

Intrusion detection analysis is performed on the protocol specified in the data stream.

- **Examines the protocol to determine the validity of the packet**
- **Checks the content of the payload (pattern matching)**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—3-18

Protocol analysis-based intrusion detection is similar to signature-based, but performs a more in-depth analysis of the protocols specified in the packets. For example, an attack is launched against a server. The attacker sends an IP packet with a protocol type that, according to an RFC, should not contain any data in the payload. A protocol analysis-based IDS is able to detect this type of attack based on the knowledge of the protocol.



Responsive

- Reactive IDSs can respond to an attack.
  - Terminate session (TCP resets)
  - Block offending traffic (ACL)
  - Create session log files (IP logging)
  - Restrict access to protected resources

CSIDS 4.0—3-19

Intrusion detection technology is traditionally considered a passive monitoring tool. Earlier IDS simply monitored the network for suspicious activity or parsed system log files. Today's intrusion detection system (IDS) offers much more reactive responses and preventive measures when an intrusion or malicious activity is detected. The common reactive responses are as follows:

- Terminate the session—The IDS sends TCP packets with the reset bit set to both the source address of the attack and destination address of the target.

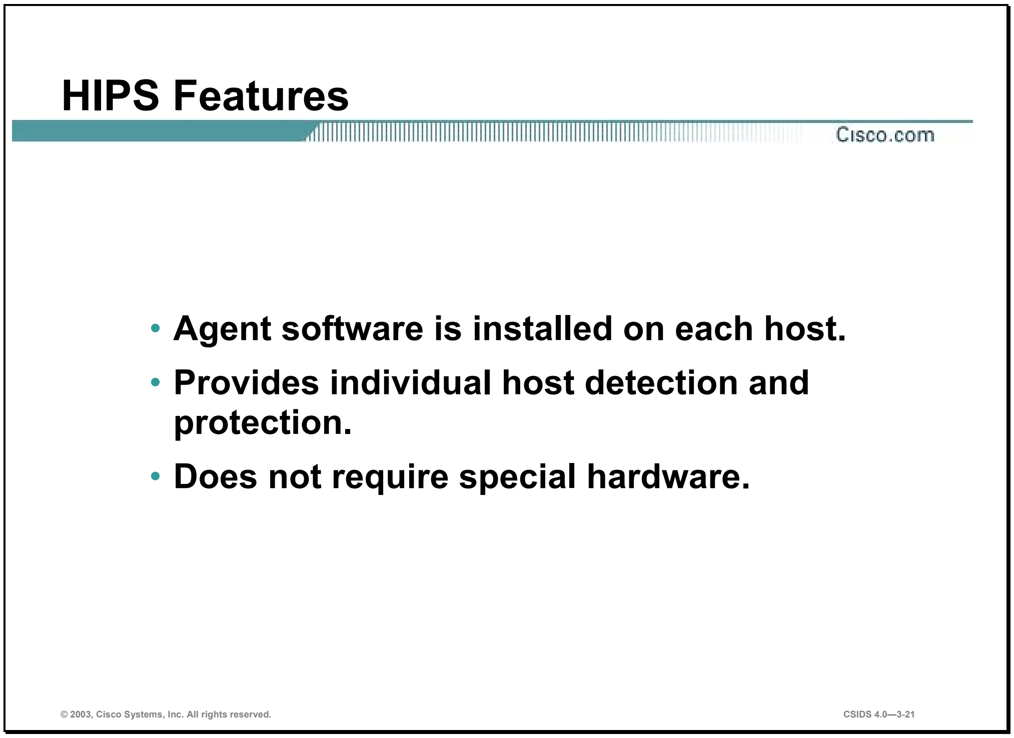
- Blocking offending traffic—The IDS communicates with the network device and applies an access control list entry specifying that the source address of the attack be denied.

- Create session log files—The IDS creates a session log file capturing the data transmitted from the source address of the attack.

- Restrict access to protected resources—The IDS prevents the attacker from accessing system resources outside the allowed realm or domain specified.

Host-Based Intrusion Protection

This section describes the features of host-based intrusion protection system (HIPS) and introduces the HIPS, which takes host-based intrusion detection a step further.



HIPS Features

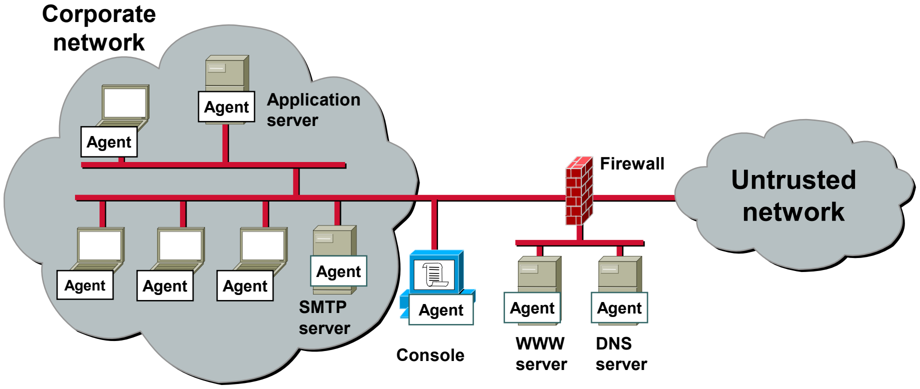
- Agent software is installed on each host.
- Provides individual host detection and protection.
- Does not require special hardware.

CSIDS 4.0—3-21

HIPS audits host log files, host file systems, and resources. An advantage of HIPS is that it can monitor operating system processes and protect critical system resources including files that may exist only on that specific host.

A simple form of HIPS is enabling system logging on the host. However, it can become manpower intensive to recover and analyze these logs. Today's HIPS software requires Agent software to be installed on each host to monitor activity performed on and against the host. The Agent software performs the intrusion detection analysis and protects the host.

Host-Based Intrusion Protection System

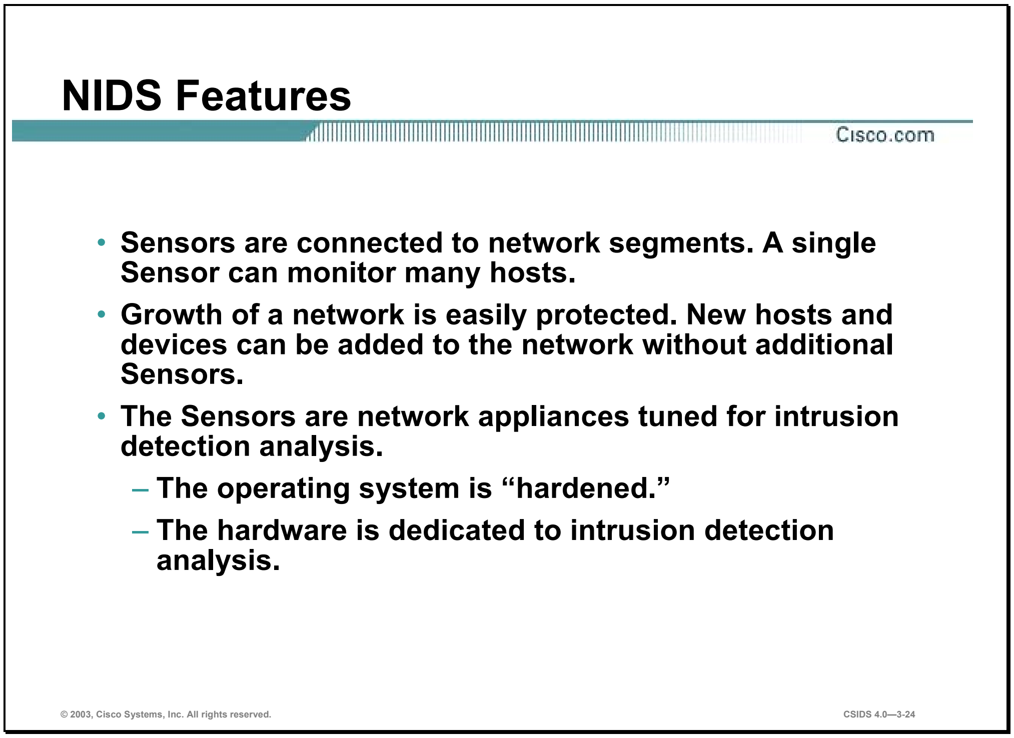


CSIDS 4.0—3-22

The figure illustrates a typical HIPS deployment. Agents are installed not only on publicly accessible servers, corporate mail servers, and application servers, but also on user desktops. The Agents report events to a central Console server located inside the corporate firewall.

Network-Based Intrusion Detection Systems

This section describes the features of network-based IDSs (NIDSs), including a pictorial of a typical NIDS deployment.



NIDS Features

- Sensors are connected to network segments. A single Sensor can monitor many hosts.
- Growth of a network is easily protected. New hosts and devices can be added to the network without additional Sensors.
- The Sensors are network appliances tuned for intrusion detection analysis.
  - The operating system is “hardened.”
  - The hardware is dedicated to intrusion detection analysis.

CSIDS 4.0—3-24

A NIDS involves the deployment of monitoring devices or “Sensors” throughout the network, which capture and analyze the traffic as it traverses the network. The Sensors detect malicious and unauthorized activity in real time and can take action when required.

Sensors can be deployed at designated network points that enable security managers to monitor network activity while it is occurring, regardless of the location of the target of the attack.

NIDS gives security managers real-time security insight into their network regardless of network growth. Network growth can occur by adding either additional hosts or new networks. Additional hosts added to existing protected networks would be covered without any new Sensors. Additional Sensors can easily be deployed to protect the new networks. Some of the factors that influence the addition of Sensors are as follows:

- Excepted traffic capacity—For example, the addition of a new gigabit network segment requires a high-capacity Sensor.
- Performance capabilities of the Sensor—The current Sensor may not be able to perform given the new traffic capacity.
- Network implementation—The security policy or network design may require additional Sensors to help enforce security boundaries.

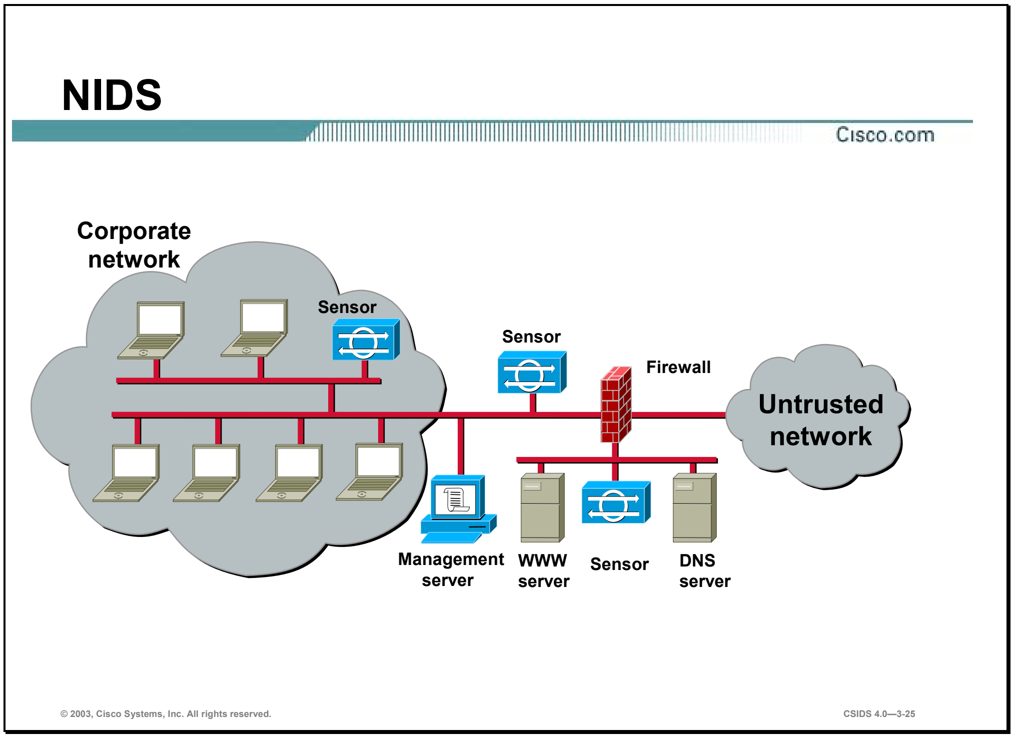
NIDS Sensors are typically tuned for intrusion detection analysis. The underlying operating system is “stripped” of unnecessary network services and essential services are secured.

The hardware chosen provides the maximum intrusion detection analysis possible for various networks. The hardware includes the following:

- Network interface card (NIC)—NIDS must be able to connect into any network. Common NIDS NICs include Ethernet, Fast Ethernet, GigEthernet, Token Ring, and FDDI.

- Processor—Intrusion detection requires CPU power to perform intrusion detection protocol analysis and pattern matching.

- Memory—Intrusion detection analysis is memory intensive. Memory directly impacts the ability of a NIDS to efficiently and accurately detect an attack.



NIDS

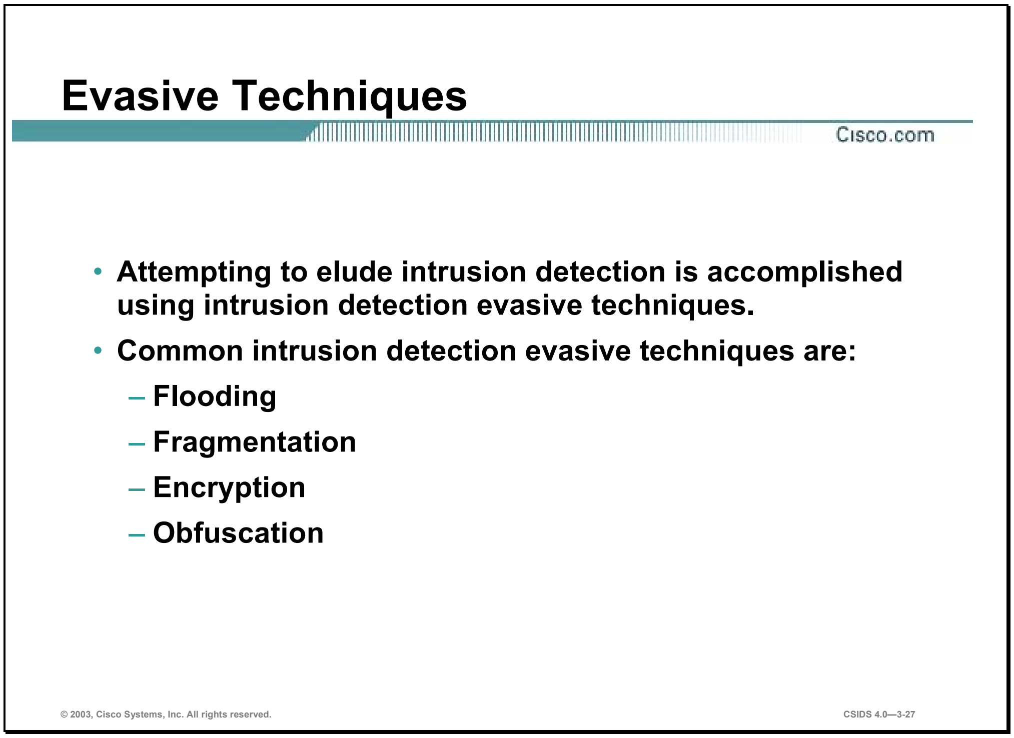
Cisco.com

CSIDS 4.0—3-25

The figure illustrates a typical NIDS deployment. Sensors are deployed at network entry points that protect critical network segments. The network segments have both internal and external corporate resources. The Sensors report to a central management and monitoring server located inside the corporate firewall.

Intrusion Detection Evasive Techniques

This section describes the common intrusion detection evasive techniques used by attackers to evade both network and host-based intrusion detection systems.



Evasive Techniques

Cisco.com

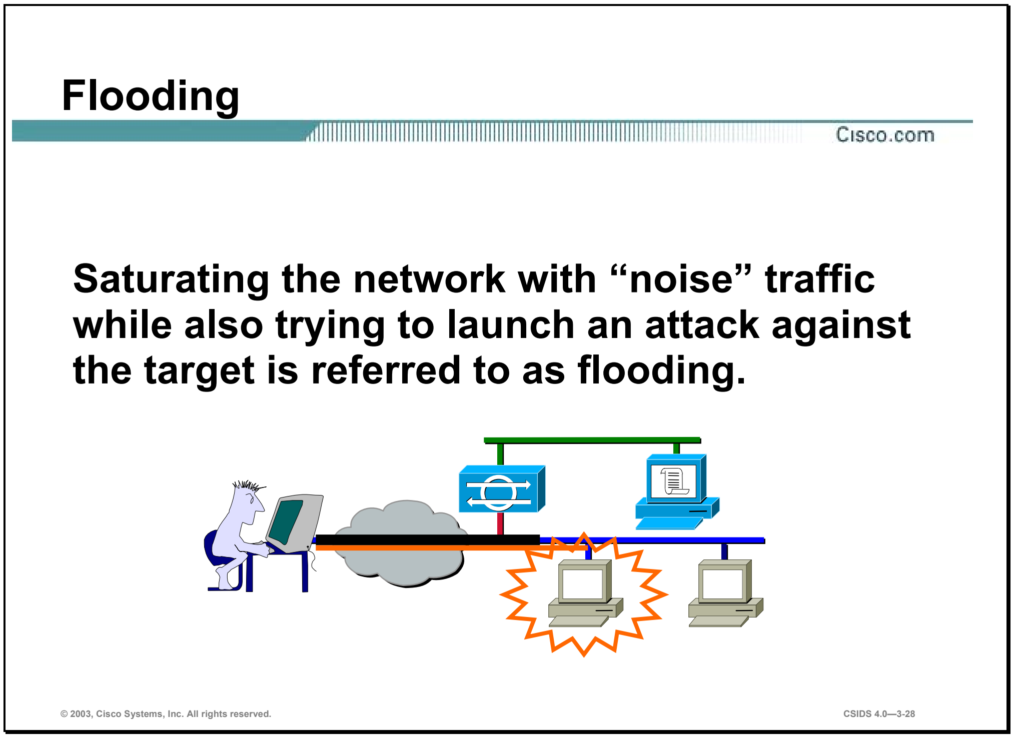
- Attempting to elude intrusion detection is accomplished using intrusion detection evasive techniques.
- Common intrusion detection evasive techniques are:
  - Flooding
  - Fragmentation
  - Encryption
  - Obfuscation

CSIDS 4.0—3-27

The hacker community is aware of the various IDS technologies used and has identified ways to evade intrusion detection. Attempting to elude intrusion detection is accomplished using intrusion detection evasive techniques. The following are common intrusion detection evasive techniques:

- Flooding
- Fragmentation
- Encryption
- Obfuscation

For more information, refer to *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection* by Ptacek and Newsham.



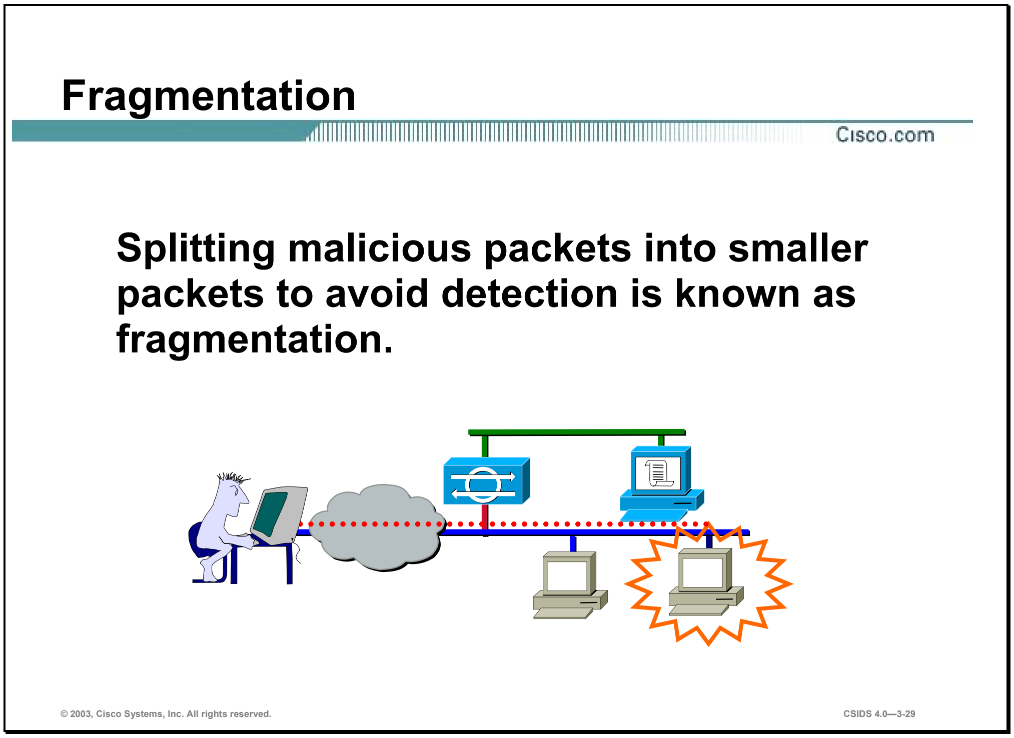
Flooding

Cisco.com

Saturating the network with “noise” traffic while also trying to launch an attack against the target is referred to as flooding.

CSIDS 4.0—3-28

Intrusion detection systems rely on their ability to capture packets off the wire and analyze them as quickly as possible. This requires the IDS has adequate memory capacity and processor speed. By flooding the network with noise traffic and causing the IDS to capture unnecessary packets, the attacker can launch an attack that can go undetected. If the attack is detected, the IDS resources may be exhausted causing a delayed response and thus is unable to respond in a timely manner. In the figure, the attacker is sending large amounts of traffic as signified by the larger pipe. Meanwhile, the actual attack is being sent to the target host, as represented by the thin pipe that reaches the target host.



Fragmentation

Cisco.com

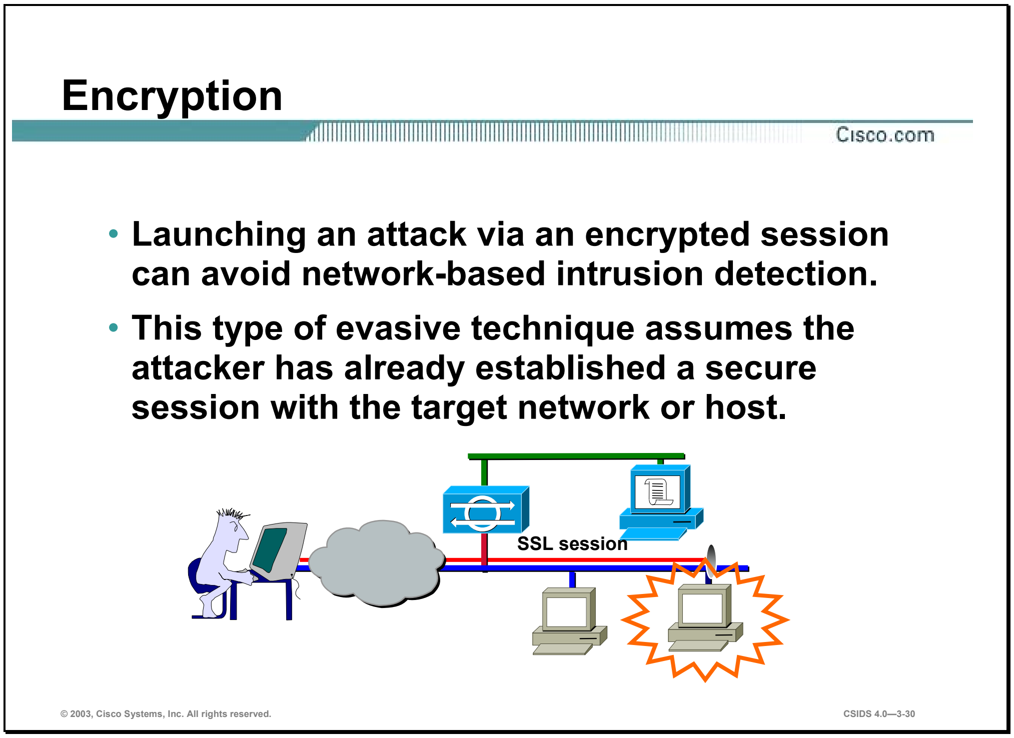
Splitting malicious packets into smaller packets to avoid detection is known as fragmentation.

CSIDS 4.0—3-29

Networks are connected via various media types such as Ethernet, FDDI, Token Ring, and ATM. Each of these technologies specifies the allowed maximum transmission unit (MTU). The MTU value is different for each technology. Consequently, fragmentation of these transmission units (packets, cells) is allowed to accommodate for differing MTU sizes.

Fragmentation adds a level of complexity that IDS must address. The IDS now must keep track of the fragmented packets and perform reassembly. Reassembly is highly processor-intensive and requires sufficient memory.

In the figure, the attacker is splitting malicious packets into smaller packets that are transmitted to the target host in an attempt to elude intrusion detection and have the target host reassemble the packets.



Encryption

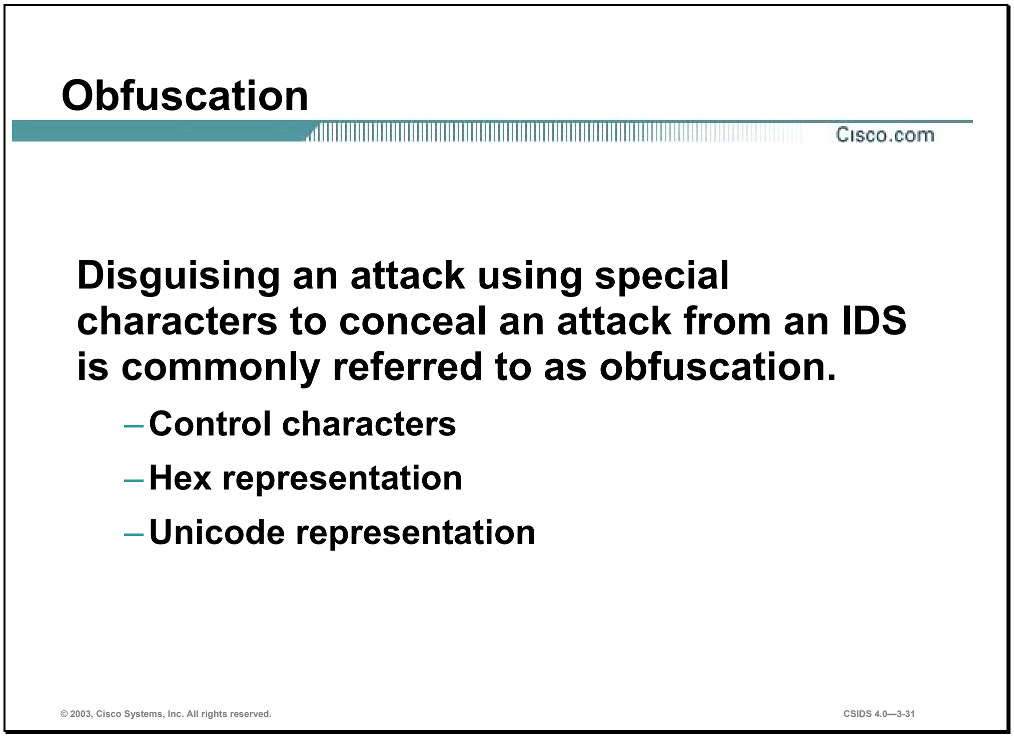
Cisco.com

- Launching an attack via an encrypted session can avoid network-based intrusion detection.
- This type of evasive technique assumes the attacker has already established a secure session with the target network or host.

CSIDS 4.0—3-30

NIDSs monitor the network and capture the packets as they traverse the network. NIDS relies on the data being transmitted in clear-text. When packets are encrypted, the NIDS captures the data but is unable to decrypt the data and cannot perform meaningful intrusion detection analysis. This type of evasive technique assumes the attacker has already established a secure session with the target network or host. Some examples of secure sessions that can be used are as follows:

- Secure Socket Layer (SSL) connection to a secure web site
- Secure Shell (SSH) connection to a SSH server
- Site-to-Site VPN tunnel
- Client-to-LAN VPN tunnel



Obfuscation

Cisco.com

Disguising an attack using special characters to conceal an attack from an IDS is commonly referred to as obfuscation.

- **Control characters**
- **Hex representation**
- **Unicode representation**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—3-31

Early intrusion detection was easily evaded by disguising an attack by using special characters to conceal an attack. The term used to describe this evasive technique is obfuscation. Obfuscation is now once again becoming a popular IDS evasive technique. The following are forms of obfuscation:

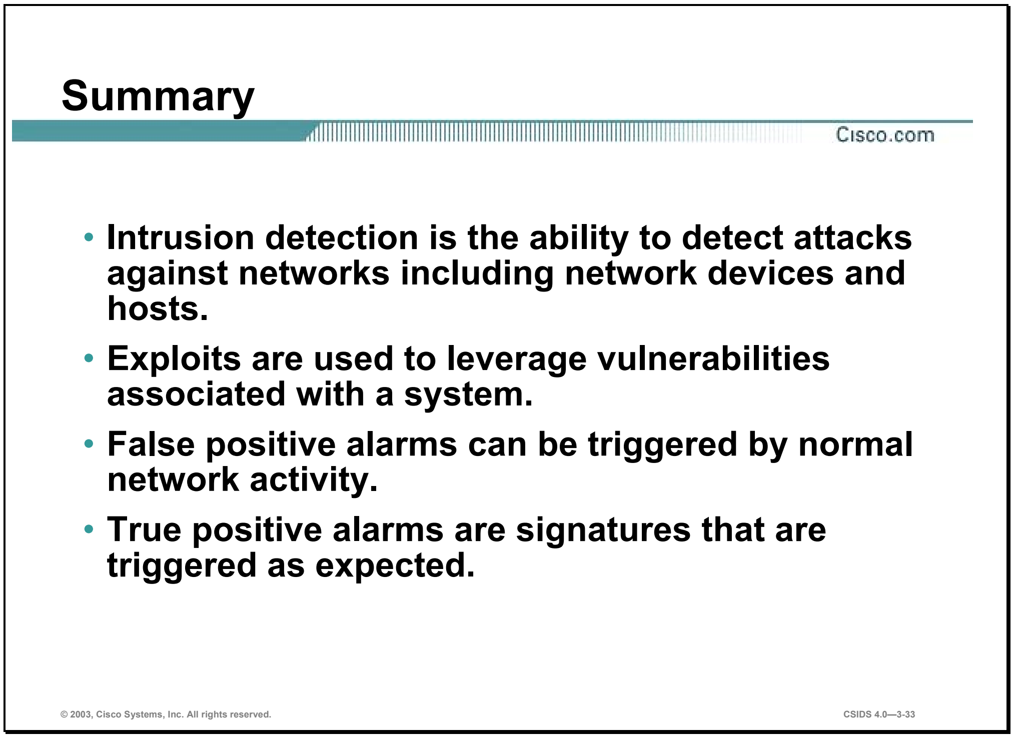
- Control characters—These characters include spaces, tabs, backspace, and delete.
- Hex representation—Each character can be represented in HEX format. For example, a space is represented by the HEX number 0x20.
- Unicode representation—Unicode provides a unique value for every character, regardless of platform, program, or language. For example, the slash character (/) is represented by the value c1.

Note The Unicode value is dependent on the Unicode encoding version used.

For more information, refer to RFC 2279, “UTF-8, a transformation format of ISO 10646” and visit http://www.unicode.org.

Summary

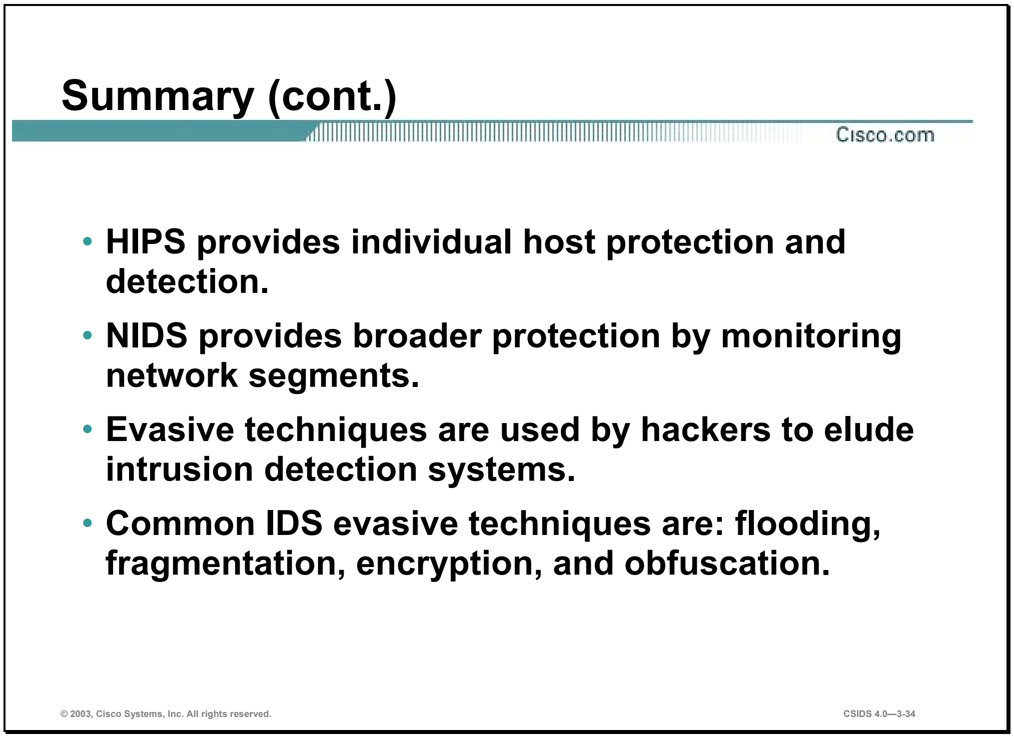
This section summarizes what you have learned in this chapter.



Summary

- Intrusion detection is the ability to detect attacks against networks including network devices and hosts.
- Exploits are used to leverage vulnerabilities associated with a system.
- False positive alarms can be triggered by normal network activity.
- True positive alarms are signatures that are triggered as expected.

CSIDS 4.0—3-33



Summary (cont.)

- HIPS provides individual host protection and detection.
- NIDS provides broader protection by monitoring network segments.
- Evasive techniques are used by hackers to elude intrusion detection systems.
- Common IDS evasive techniques are: flooding, fragmentation, encryption, and obfuscation.

CSIDS 4.0—3-34

4

Cisco Intrusion Protection Overview

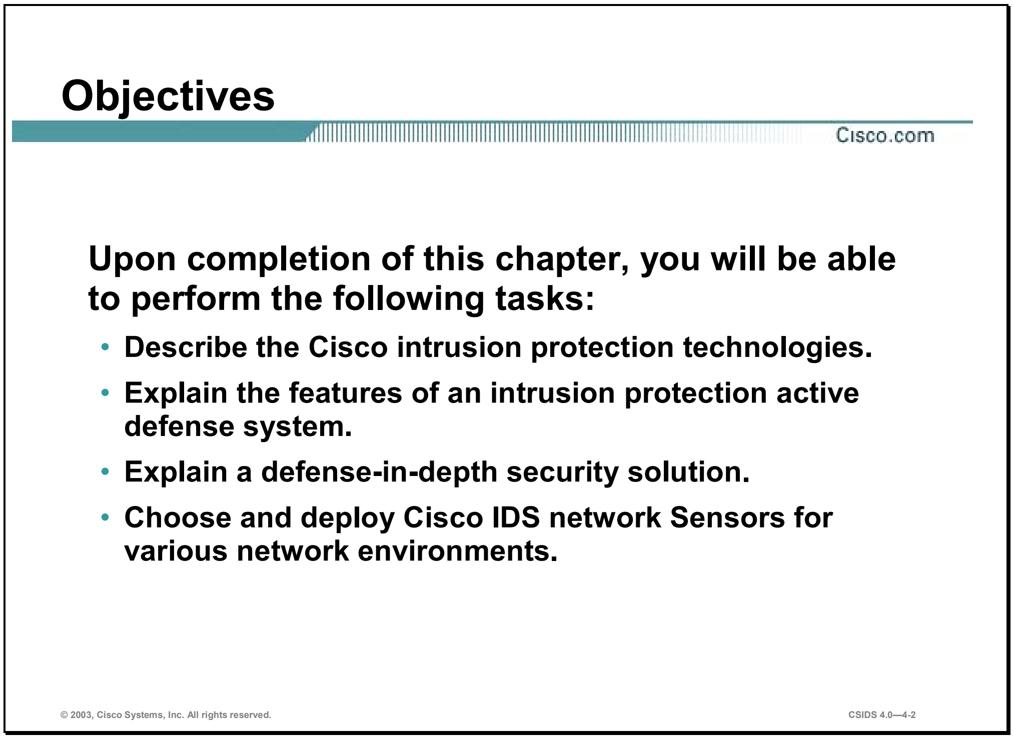
Overview

This chapter discusses the Cisco intrusion protection defense-in-depth solution and the products available to deploy the solution. This chapter includes the following topics:

- Objectives
- Intrusion protection
- Network Sensor platforms
- HIPS platforms
- Security management
- Cisco Threat Response
- Cisco IDS communication overview
- Deploying Cisco IDS
- Summary

Objectives

This section lists the chapter's objectives.



Objectives

Cisco.com

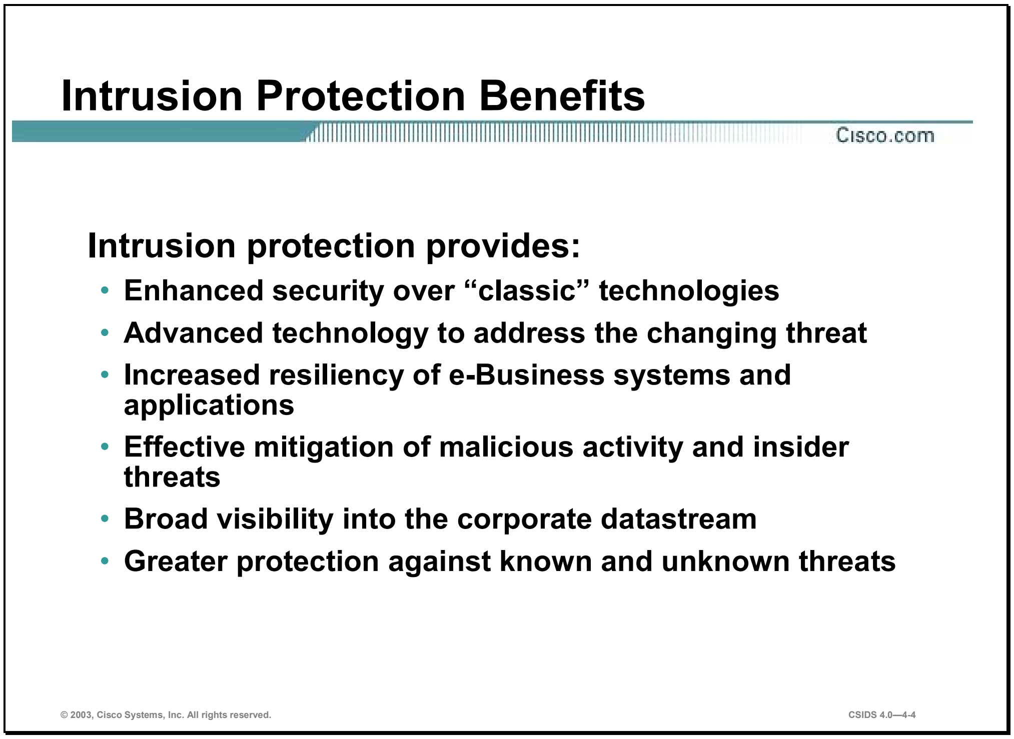
Upon completion of this chapter, you will be able to perform the following tasks:

- **Describe the Cisco intrusion protection technologies.**
- **Explain the features of an intrusion protection active defense system.**
- **Explain a defense-in-depth security solution.**
- **Choose and deploy Cisco IDS network Sensors for various network environments.**

CSIDS 4.0—4-2

Intrusion Protection

This section describes the Cisco intrusion protection technologies and solution. In addition, a defense-in-depth security strategy is discussed.



Intrusion Protection Benefits

Cisco.com

Intrusion protection provides:

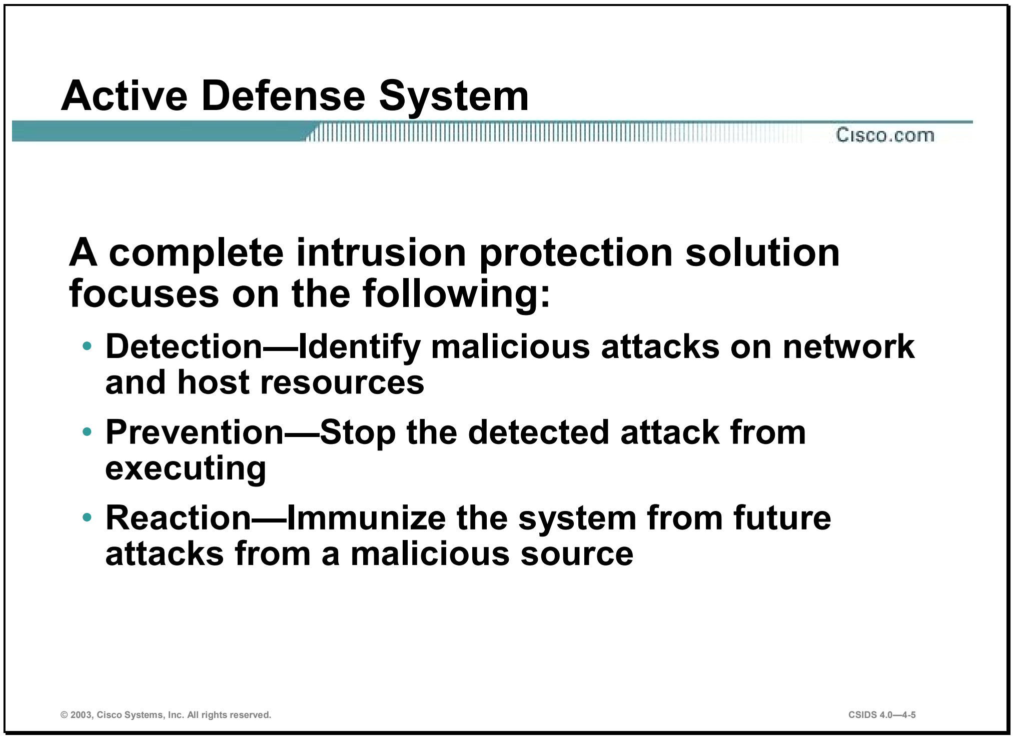
- Enhanced security over "classic" technologies
- Advanced technology to address the changing threat
- Increased resiliency of e-Business systems and applications
- Effective mitigation of malicious activity and insider threats
- Broad visibility into the corporate datastream
- Greater protection against known and unknown threats

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—4-4

The Cisco intrusion protection technologies enable a customer to actively defend their network against network attacks, misuse, and unauthorized access. Intrusion Protection provides:

- Enhanced security over classic technologies.
- Advanced technology to address the changing threat.
- Increased resiliency of e-Business systems and applications.
- Effective mitigation of malicious activity and insider threats.
- Broad visibility into the corporate datastream.
- Greater protection against known and unknown threats.



Active Defense System

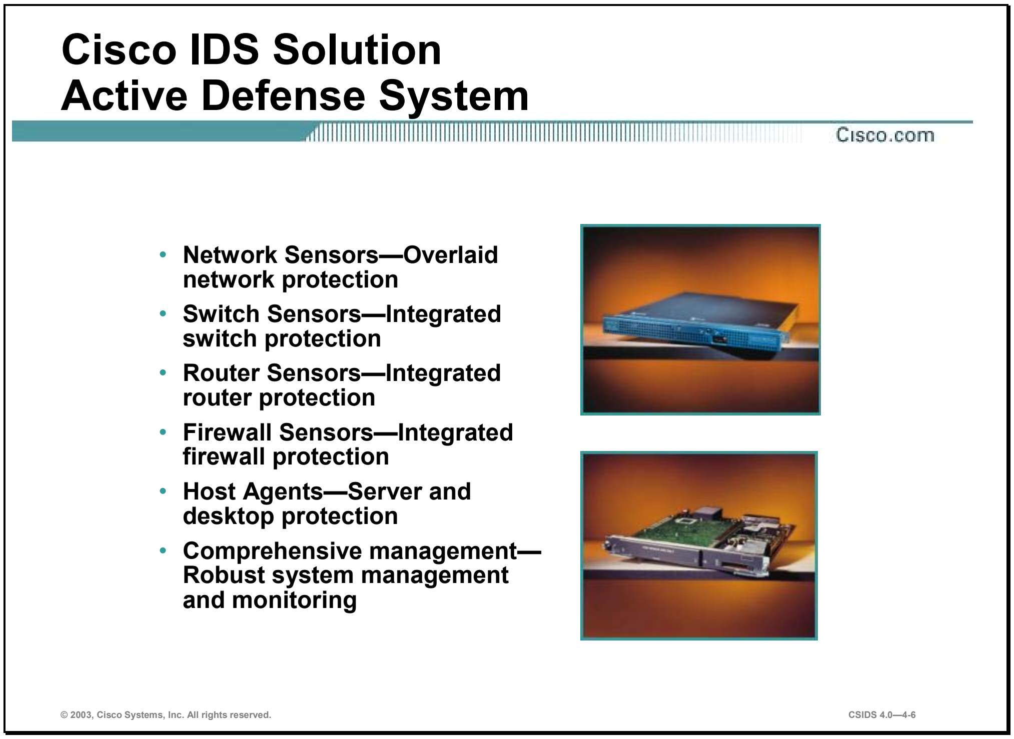
A complete intrusion protection solution focuses on the following:

- Detection—Identify malicious attacks on network and host resources
- Prevention—Stop the detected attack from executing
- Reaction—Immunize the system from future attacks from a malicious source

CSIDS 4.0—4-5

The Cisco intrusion protection solution is focused on the following active defense mechanisms:

- Detection—Identify malicious attacks on network and host resources.
- Prevention—Stop the detected attack from executing.
- Reaction—Immunize the system from future attacks from a malicious source.



Cisco IDS Solution Active Defense System

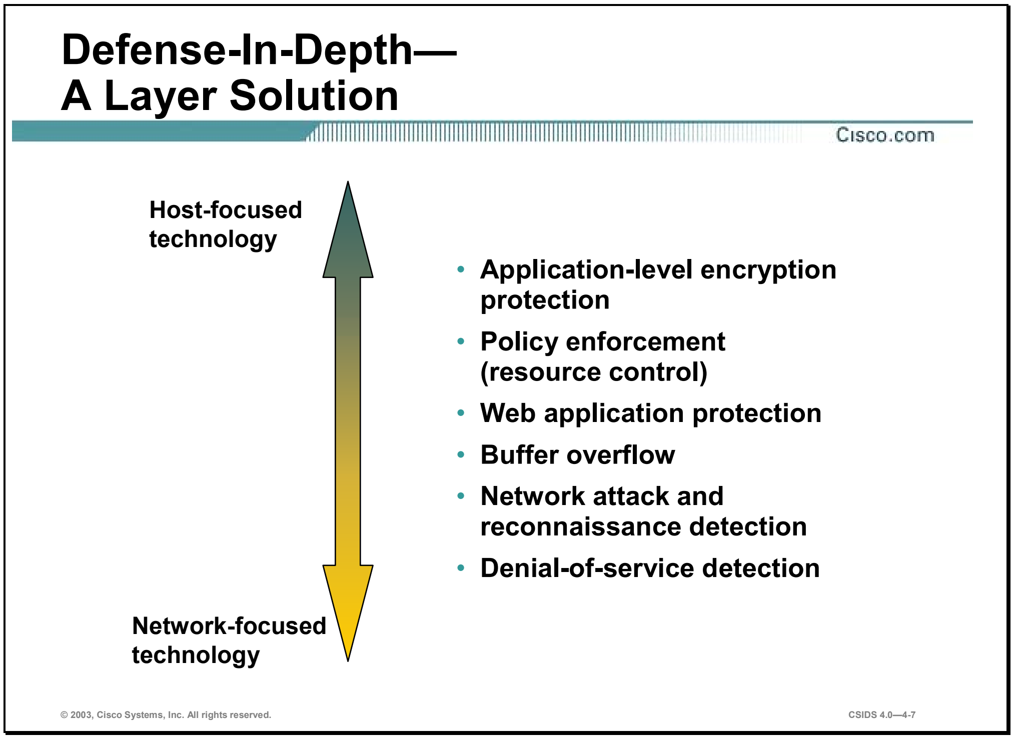
Cisco.com

- Network Sensors—Overlaid network protection
- Switch Sensors—Integrated switch protection
- Router Sensors—Integrated router protection
- Firewall Sensors—Integrated firewall protection
- Host Agents—Server and desktop protection
- Comprehensive management—Robust system management and monitoring

CSIDS 4.0—4-6

Cisco provides a complete product portfolio that enables a customer to implement and manage an active defense system. The IDS products include the following:

- Network Sensors—Network Sensors provide a dedicated intrusion detection appliance with the capabilities of monitoring and protecting network segments.
- Switch Sensors—Switch Sensors are integrated into the switch fabric to provide seamless intrusion detection.
- Router Sensors—Router Sensors provide intrusion detection for those deployments that require basic intrusion detection features.
- Firewall Sensors—Firewall Sensors provide intrusion detection for those deployments that require basic intrusion detection features.
- Host Agents—Host Agents protect critical servers and applications.
- Comprehensive Management—A comprehensive management solution that provides a robust system management and monitoring is available.



Defense-In-Depth— A Layer Solution

Cisco.com

Host-focused technology

Network-focused technology

- Application-level encryption protection
- Policy enforcement (resource control)
- Web application protection
- Buffer overflow
- Network attack and reconnaissance detection
- Denial-of-service detection

CSIDS 4.0—4-7

No single device or security technology can provide a complete security solution. A defense-in-depth security solution attempts to protect network resources by having layers of security. Intrusion detection can be implemented at both the host level and network level. Implementing both technologies provides a defense-in-depth intrusion detection solution.

Host-focused intrusion technology is designed to:

- Protect applications on the specific host.
- Enforce policy by controlling access to host resources.
- Protect web applications.
- Protect against buffer overflow attacks.

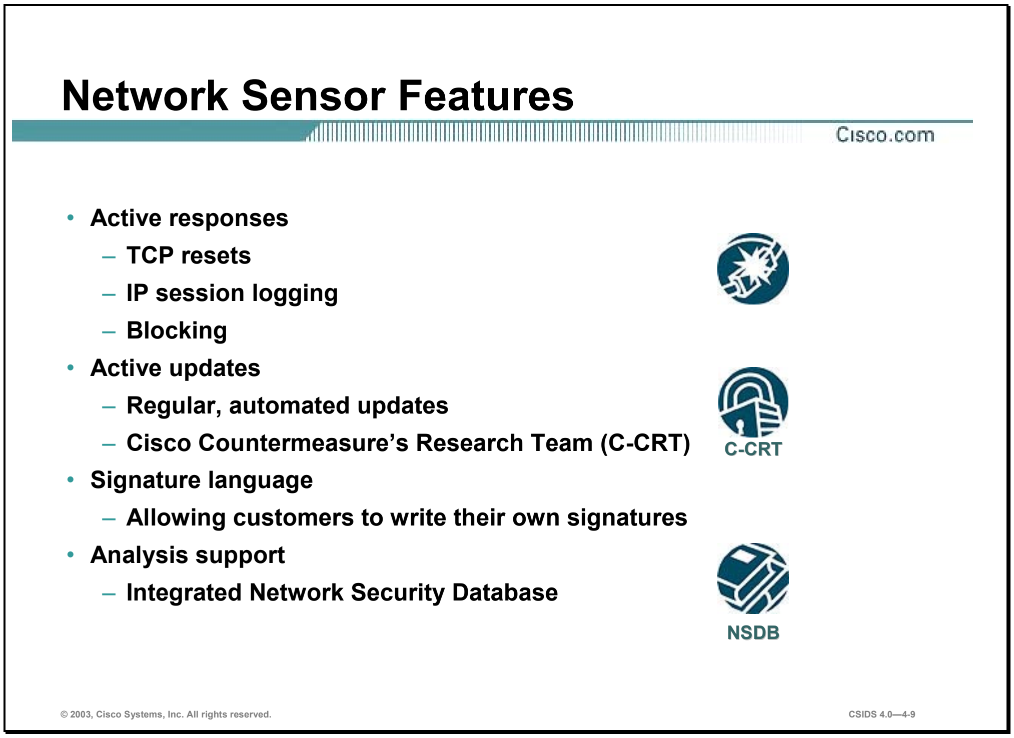
Network-focused intrusion technology is designed to:

- Detect attacks against web applications.
- Detect buffer overflow attacks.
- Detect network reconnaissance and attacks.
- Detect Denial of Service (DoS) attacks.

Notice the overlap and differences between the host-focused and network-focused intrusion detection technologies. The differences provide protection where the other technology is lacking, and the overlap provides an additional layer of protection.

Network Sensor Platforms

This section describes the Cisco IDS network Sensor features and current platforms.



Network Sensor Features

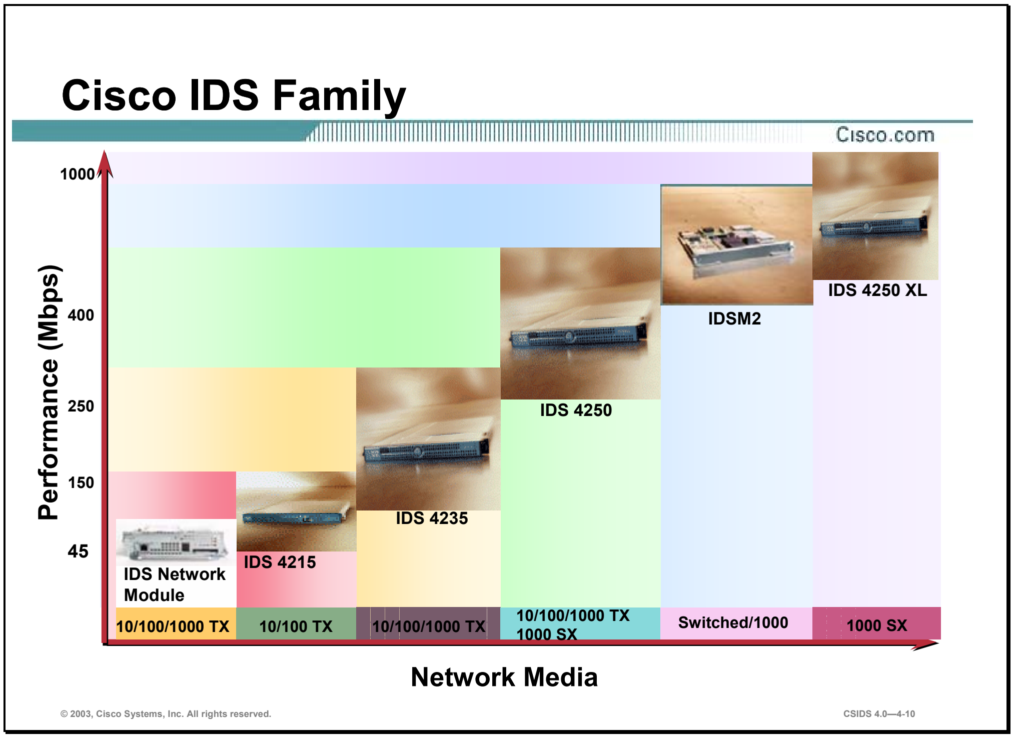
Cisco.com

- Active responses
  - TCP resets
  - IP session logging
  - Blocking
- Active updates
  - Regular, automated updates
  - Cisco Countermeasure's Research Team (C-CRT)
- Signature language
  - Allowing customers to write their own signatures
- Analysis support
  - Integrated Network Security Database

CSIDS 4.0—4-9

The Cisco IDS network Sensors have a wide range of capabilities and features. The following table identifies the features available for the Cisco IDS products:

Feature	Network Sensor	Switch Sensor	IOS-IDS	PIX-IDS
TCP reset	×	x	×	×
IP session logging	×	x		
Blocking	×	×		x
Packet drop			x	x
Active updates	×	×		
Signature language	×	×		
Analysis support	×	×	×	×



Cisco IDS Family

© 2003, Cisco Systems, Inc. All rights reserved.

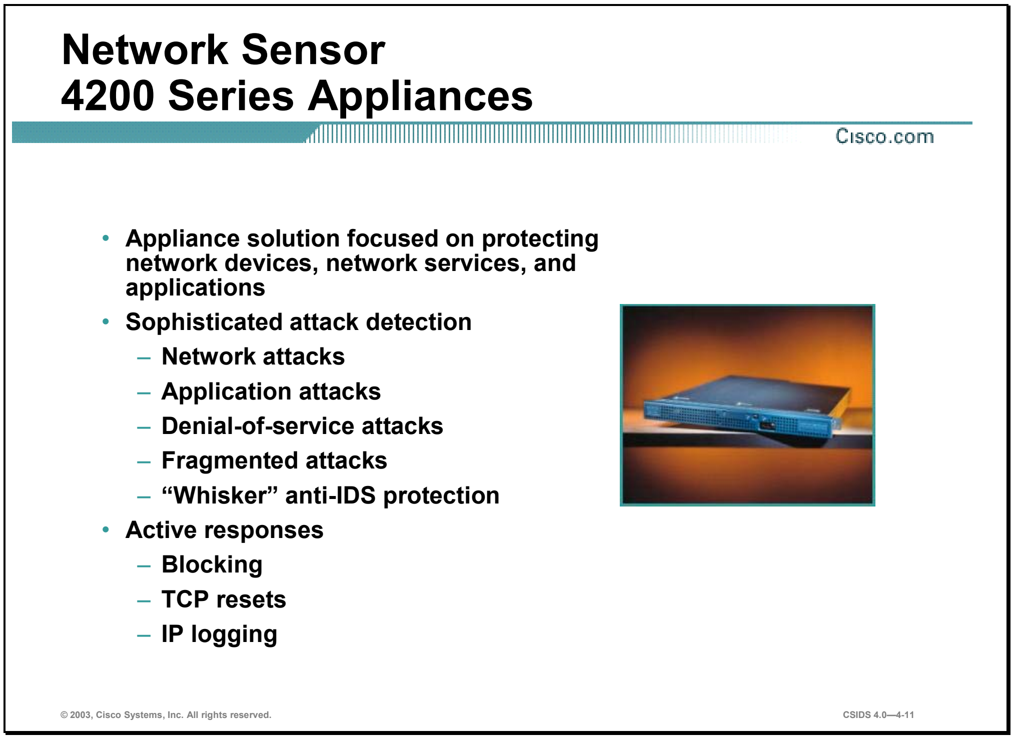
CSIDS 4.0—4-10

The following table provides a reference for all products that run IDS code 4.0 or higher:

Product	**IDS Network Module**	**4215 Sensor appliance**	**4235 Sensor appliance**	**4250 Sensor appliance**	**IDSM2**	**4250XL Sensor appliance**
Performance (Mbps)	10–45	80	200	500	600	1000
Network Media	10/100/1000 TX	10/100 TX	10/100/1000 TX	10/100/1000 TX or 1000 SX	Switched 1000	1000 SX

Note Cisco IDS Network Module for the Cisco 2600, 3600, and 3700 Series routers is part of the Cisco IDS family Sensor portfolio and the Cisco intrusion protection system. Both the IDS Network Module and the Cisco IDS 4215 Sensor appliance are delivered with IDS 4.1 software.

Caution The performance values are approximate and may vary depending on packet size. Refer to the product release notes and documentation for the most current information.



Network Sensor 4200 Series Appliances

- Appliance solution focused on protecting network devices, network services, and applications
- Sophisticated attack detection
  - Network attacks
  - Application attacks
  - Denial-of-service attacks
  - Fragmented attacks
  - “Whisker” anti-IDS protection
- Active responses
  - Blocking
  - TCP resets
  - IP logging

CSIDS 4.0—4-11

The 4200 Series Network Sensor appliances are focused on protecting network devices, services, and applications. The 4200 series appliance is capable of detecting sophisticated attacks such the following:

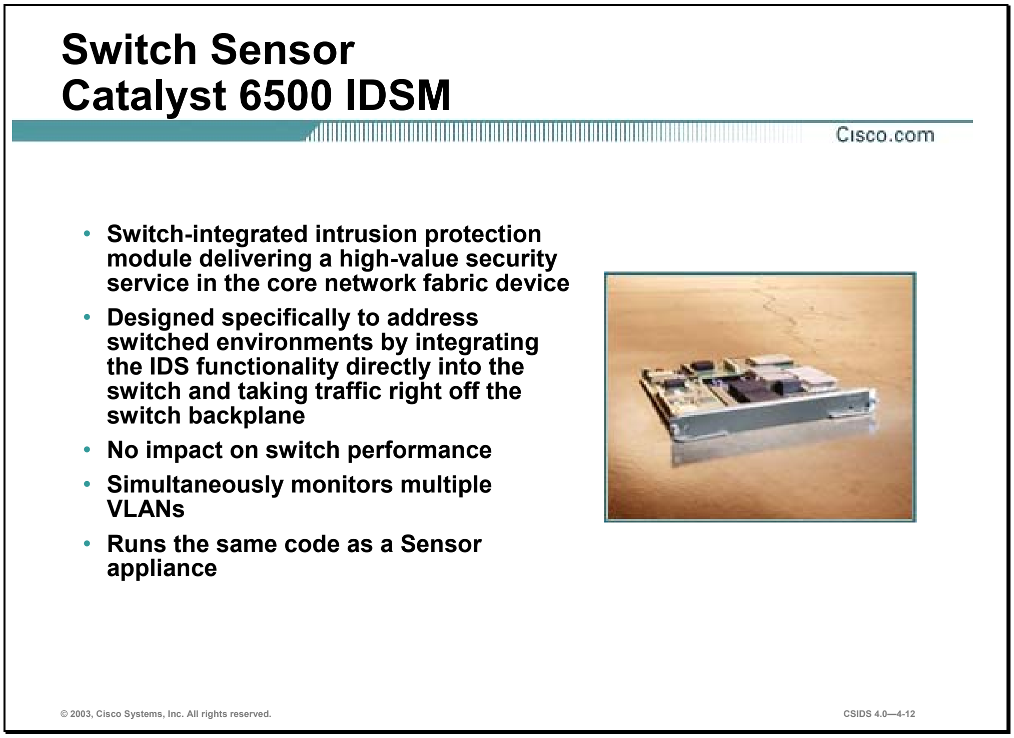
- Network attacks
- Application attacks
- DoS attacks
- Fragmented attacks
- “Whisker” attacks using IDS-evasive techniques

The 4200 series appliances are able to take the following active responses:

- Blocking—Modifies access control lists (ACLs) on routers and switches to prevent traffic from the source of the attack from entering the network.

Note The Sensor does not modify ACLs on the PIX Firewall. The **shun** command is used to enforce blocking.

- TCP Reset—Terminates a session by sending Transmission Control Protocol (TCP) packets with the reset, RST, flag to both the source and destination of the attack.
- IP Logging—Create a binary file that captures data from the source of the attack.

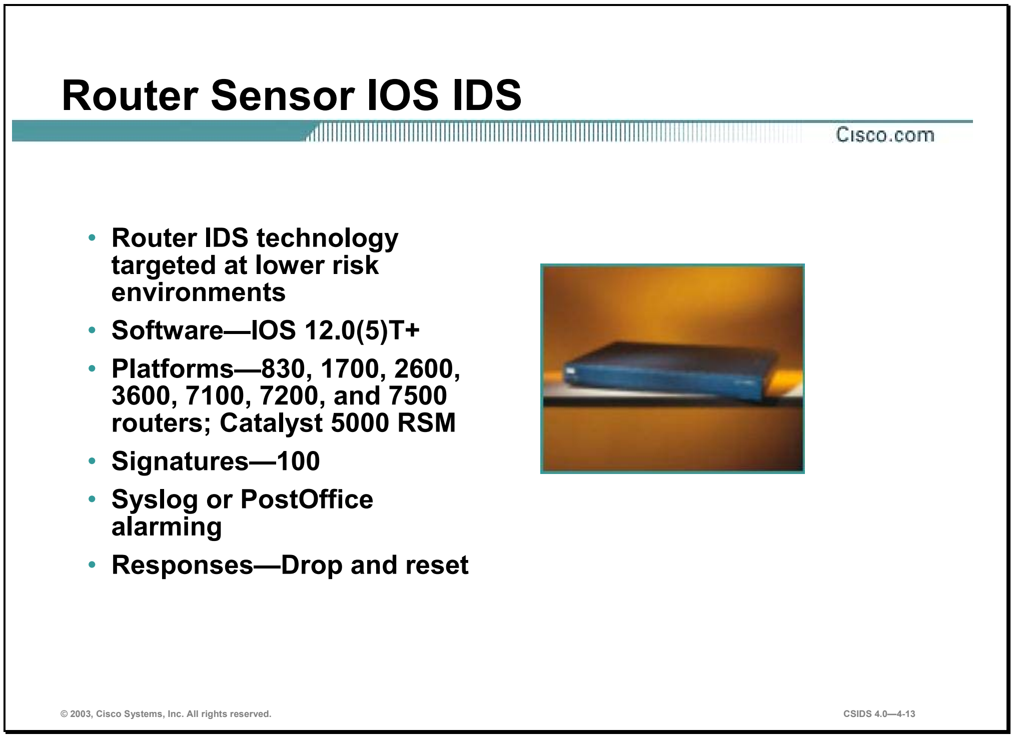


Switch Sensor Catalyst 6500 IDSM

- Switch-integrated intrusion protection module delivering a high-value security service in the core network fabric device
- Designed specifically to address switched environments by integrating the IDS functionality directly into the switch and taking traffic right off the switch backplane
- No impact on switch performance
- Simultaneously monitors multiple VLANs
- Runs the same code as a Sensor appliance

CSIDS 4.0—4-12

The Catalyst 6500 IDS Module version 2 (IDSM2) provides intrusion protection in the core network fabric device. The IDSM2 is specifically designed to address switch environments by integrating the IDS functionality directly into the switch and capturing traffic off the switch backplane. The traffic "captured" off the backplane is copied, thereby not impacting switch performance. The IDSM2 is able to monitor multiple VLANs simultaneously and provides full-featured network attack protection.



Router Sensor IOS IDS

- **Router IDS technology targeted at lower risk environments**
- **Software—IOS 12.0(5)T+**
- **Platforms—830, 1700, 2600, 3600, 7100, 7200, and 7500 routers; Catalyst 5000 RSM**
- **Signatures—100**
- **Syslog or PostOffice alarming**
- **Responses—Drop and reset**

CSIDS 4.0—4-13

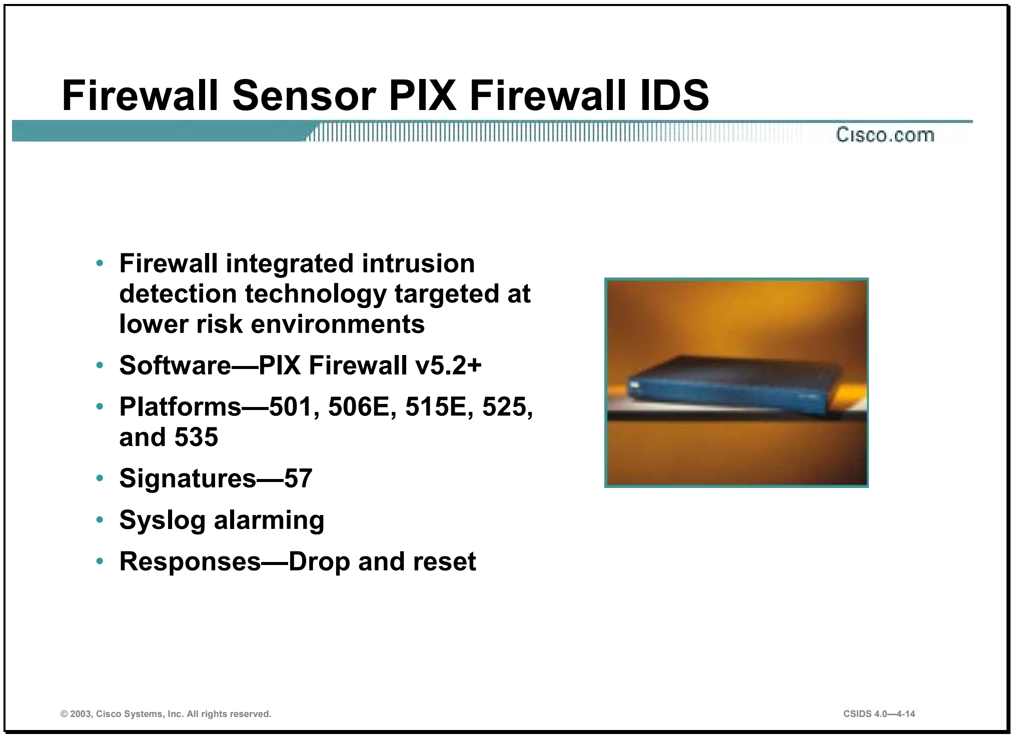
The Router Sensor integrates intrusion detection into IOS software. An IOS IDS is able to detect a limited subset of attacks compared to an IDS Sensor appliance or IDSM2. Thus it is targeted at lower risk environments.

The following are the IOS IDS features:

- Signature set—100 IDS signatures
- Reporting—Alarms can be sent to a Syslog server or another PostOffice aware device
- Responses—Drops the packet and terminates a TCP session

The software and hardware requirements of an IOS-based device to perform intrusion detection are as follows:

- Software—IOS 12.0(5)T and greater
- Hardware—Cisco 830, 1700, 2600, 3600, 7100, 7200, and 7500 series routers; and the Catalyst 5000 RSM



Firewall Sensor PIX Firewall IDS

- Firewall integrated intrusion detection technology targeted at lower risk environments
- Software—PIX Firewall v5.2+
- Platforms—501, 506E, 515E, 525, and 535
- Signatures—57
- Syslog alarming
- Responses—Drop and reset

CSIDS 4.0—4-14

The Firewall Sensor integrates IDS functionality into the PIX Firewall software. A PIX Firewall IDS is able to detect a limited subset of attacks compared to a network or switch Sensor. Thus, it is targeted for lower risk environments.

The following are the PIX Firewall IDS features:

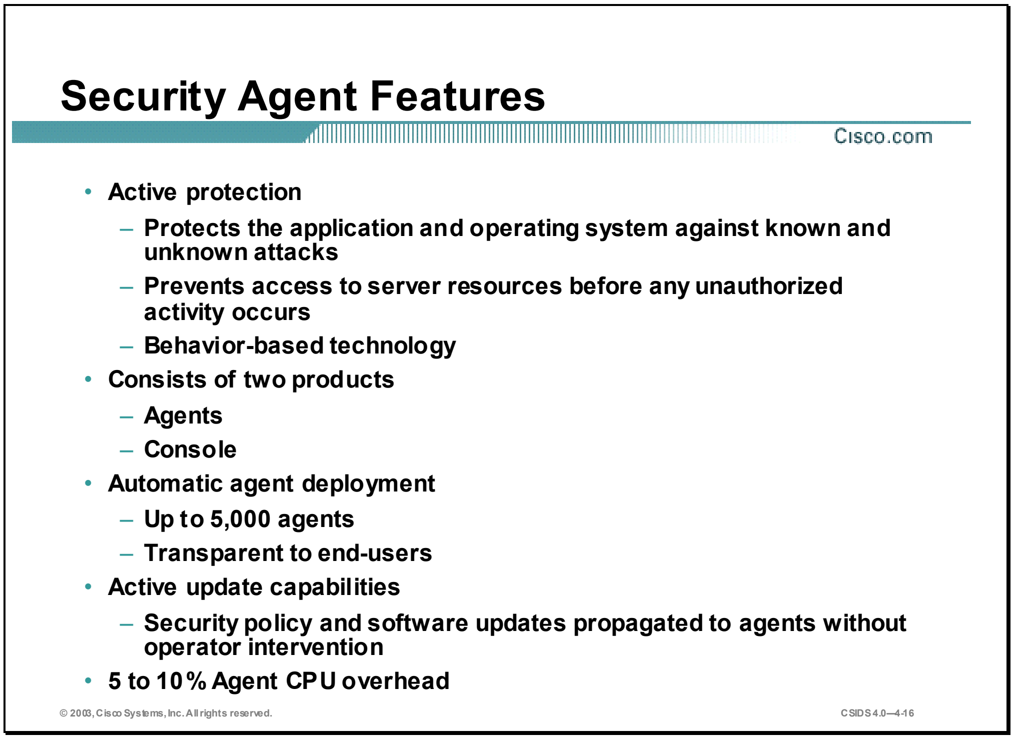
- Signature set—57 IDS signatures
- Reporting—Alarms can be sent to a Syslog server
- Responses—Drops the packet and terminate a TCP session

The following are the software and hardware requirements needed for a PIX Firewall to perform intrusion detection:

- Software—PIX Firewall 5.2 and greater
- Hardware—PIX Firewall 501, 506E, 515E, 525, and 535

HIPS Platforms

This section describes the Cisco Host-based Intrusion Protection System (HIPS) features and current platforms.



Security Agent Features

Cisco.com

- Active protection
  - Protects the application and operating system against known and unknown attacks
  - Prevents access to server resources before any unauthorized activity occurs
  - Behavior-based technology
- Consists of two products
  - Agents
  - Console
- Automatic agent deployment
  - Up to 5,000 agents
  - Transparent to end-users
- Active update capabilities
  - Security policy and software updates propagated to agents without operator intervention
- 5 to 10% Agent CPU overhead

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—4-16

The Cisco HIPS, the Cisco Security Agent, complements Cisco Network-based Intrusion Detection System (NIDS) by protecting the integrity of applications and operating systems. The Security Agent blocks malicious activity before damage is done. It protects against attacks including SYN floods, port scans, buffer overflows, Trojan horses and malformed packets. It protects against worm attacks such as Code Red, which targets Web servers, and SirCam, which targets corporate desktops, or Nimda, which targets both. By focusing on the behavior of applications, the Security Agent protects not only against known attacks such as those mentioned above but also against new attacks for which there is no known signature.

The Security Agent consists of two products:

- Management Center for Cisco Security Agent (CSA MC)
- Agents for desktops and servers

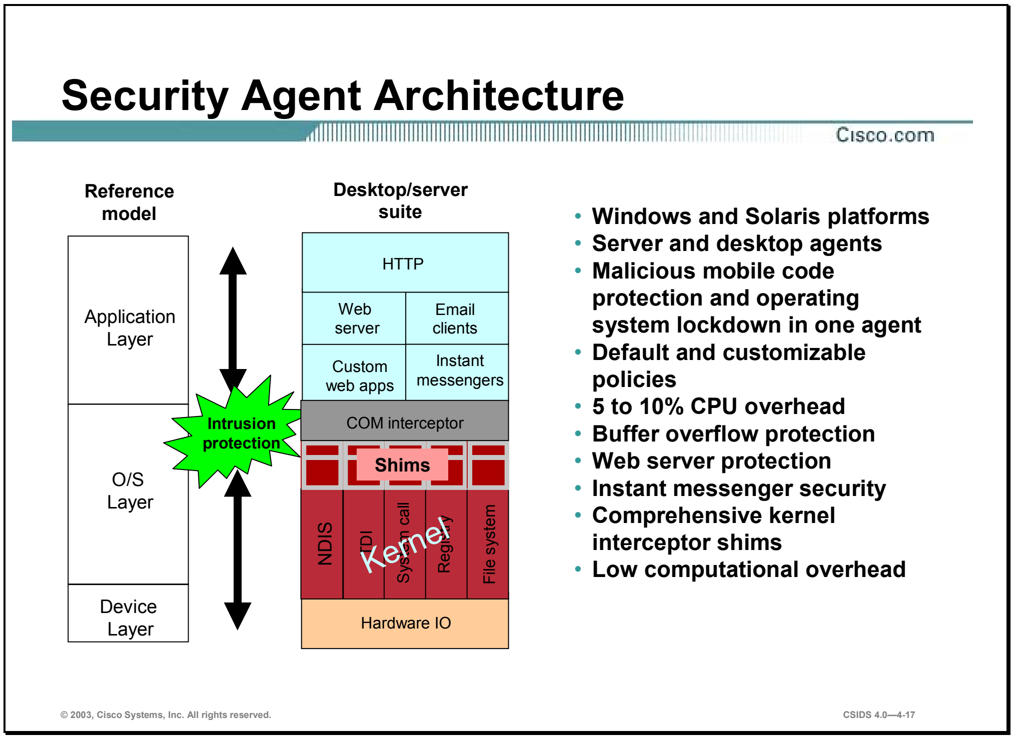
The CSA MC installation automatically builds agent kits, so it is not necessary to log into the MC to deploy agents to servers or workstations. Agent kits can be deployed to up to 5,000 agent hosts by user logon scripts, software deployment products, e-mail distribution of web link to agent kit, or software image replication. In the event that identical software images are distributed, the MC automatically ensures that each new agent is registered with a unique identifier.

Because the Security Agent offers the option for agent kits to install silently and transparently to end-users, no end user interaction is required, users do not have to answer any questions, and users do not have the ability to bypass the installation. Agents automatically register with the MC after installation, so configuration is also transparent to the end-user.

Agents communicate with the MC via SSL for rules updates with no user intervention. When agents poll into the MC at their configurable time interval, any change to the security policy is automatically propagated. Software updates are also automatically propagated to the agents without the need for operator intervention.

Note Security Agent events can be reported to the Cisco Security Monitor, a tool for capturing, storing, viewing, correlating and reporting on events. Security Monitor is covered in depth later in the course.

Note Security Agent agents can run on Windows NT, Windows 2000, Windows XP, and Solaris 2.8. The Security Agent does not inspect content, and therefore has negligible impact on performance.



Security Agent Architecture

Cisco.com

Reference model

Application Layer

O/S Layer

Device Layer

Intrusion protection

Desktop/server suite

HTTP

Web server

Email clients

Custom web apps

Instant messengers

COM interceptor

Shims

NDIS

TDI

System call

Registry

File system

Kernel

Hardware IO

- Windows and Solaris platforms
- Server and desktop agents
- Malicious mobile code protection and operating system lockdown in one agent
- Default and customizable policies
- 5 to 10% CPU overhead
- Buffer overflow protection
- Web server protection
- Instant messenger security
- Comprehensive kernel interceptor shims
- Low computational overhead

CSIDS 4.0—4-17

The Security Agent's behavior-based technology has application visibility because it resides at the kernel level within the operating system. When an application attempts an operation, the Security Agent checks the operation against the application's security policy and makes a real-time allow or deny decision on its continuation. The security policy is a set of rules that defines appropriate or acceptable behavior for a specific application. You can create your own policies and modify the default Security Agent policies in the CSA MC.

Note Because the Security Agent makes real-time allow or deny decisions within the context of the overall application behavior, it is able to minimize the number of false positives.

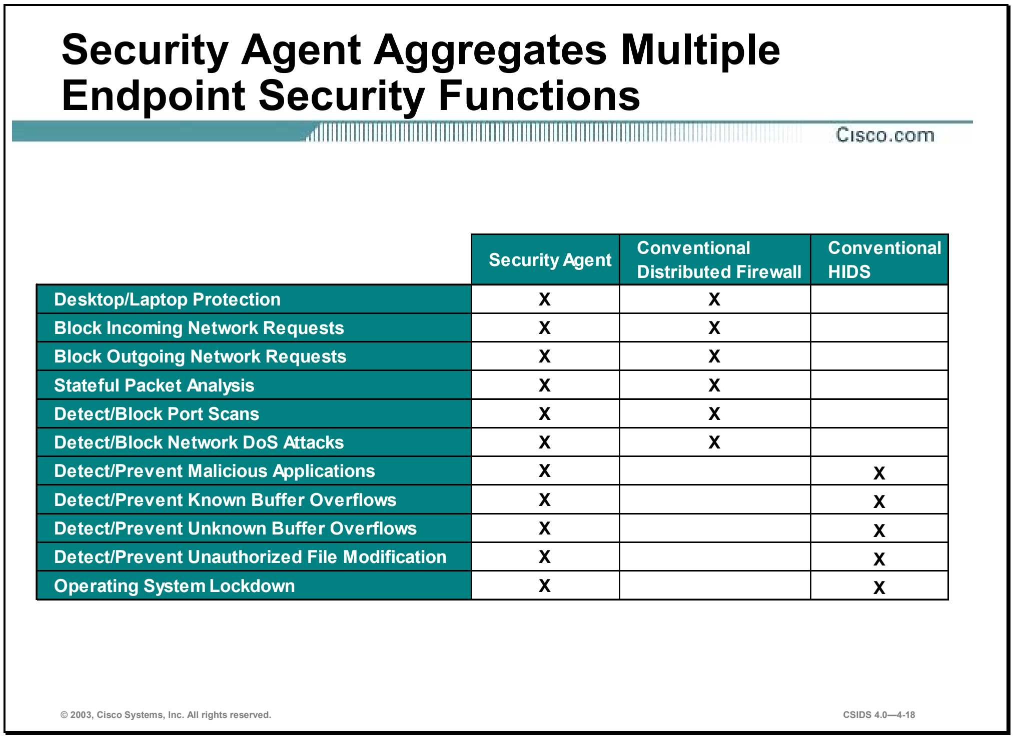
The Security Agent's Intercept Correlate Rules Engine (INCORE) architecture intercepts all system calls to file, network, COM and registry sources and then applies intelligence to correlate the behaviors of such system calls to the security policy. This correlation and understanding of an application's behavior is what allows the software to prevent new intrusions.

INCORE enables the Security Agent to act as an intrusion detection/prevention agent, a file integrity monitoring agent, and an application sandbox. It uses the following interceptors to deliver many different security capabilities:

- File System Interceptor—Intercepts all file read or write requests.
- Network Interceptor—Intercepts packet events at the network driver level and provides the same capability as traditional distributed firewall products.
- Configuration Interceptor—Intercepts read/write requests to the registry on Windows or to rc files on Unix.

- Execution Space Interceptor—Intercepts the following:
  - Requests to write to memory not owned by the requesting application
  - Attempts by one application to inject code into another process
  - Buffer overflow attacks

Note Sand boxing is a technique that prevents access to server resources not specifically allowed by the operating system or application.



Security Agent Aggregates Multiple Endpoint Security Functions

Cisco.com

	Security Agent	Conventional Distributed Firewall	Conventional HIDS
Desktop/Laptop Protection	X	X	
Block Incoming Network Requests	X	X	
Block Outgoing Network Requests	X	X	
Stateful Packet Analysis	X	X	
Detect/Block Port Scans	X	X	
Detect/Block Network DoS Attacks	X	X	
Detect/Prevent Malicious Applications	X		X
Detect/Prevent Known Buffer Overflows	X		X
Detect/Prevent Unknown Buffer Overflows	X		X
Detect/Prevent Unauthorized File Modification	X		X
Operating System Lockdown	X		X

CSIDS 4.0—4-18

The Security Agent delivers the protection of both conventional distributed firewalls and conventional host-based IDSs. The following are examples of these two functions:

- Port scan detection—The Security Agent network-wide correlation provides unique functionality in the detection of distributed port scans. Low-level port scans are used by hackers to systematically scan single ports on single agents in an alternating fashion in order to map a network. For example, server 1 would be scanned on port 1, server 2 on port 2, and so on. Each agent reports the scan activity to the CSA MC With its ability to correlate events from distributed agents, the Security Agent is able to discern that a distributed scan is taking place.

- Malicious application detection/prevention—The Security Agent can perform such difficult tasks such as catching new Trojan horses. The Security Agent does this by looking for actions that are commonly exhibited by Trojan programs to make the determination that a given application is a Trojan. Examples of such actions include writing into other processes' address space to make themselves invisible in the process table, monitoring keystrokes to capture passwords, and receiving UDP packets on high numbered ports. The Security Agent then proactively prevents the executable from executing its intrusion.

The Security Agent also complements traditional desktop anti-virus software. For example, in the case of a new attack such as an e-mail worm, the Security Agent may detect the malicious nature of the worm only after a sequence of file, network, registry, or COM operations has occurred on at least one host. Once detection has occurred, an event is sent to the management console. The management console detects and stops the malicious code at other servers and desktops by correlating the events sent from the various distributed agents. A policy is created which tells all agents not to open the offending file, effectively quarantining it and preventing further damage. The result is that you are then faced with only a few desktops that need to be rebuilt, rather than a whole network.

Note A personal firewall is a standalone product and a distributed firewall refers to a firewall on hosts that are centrally managed. In both types of firewalls, the functionality occurs on the end nodes.

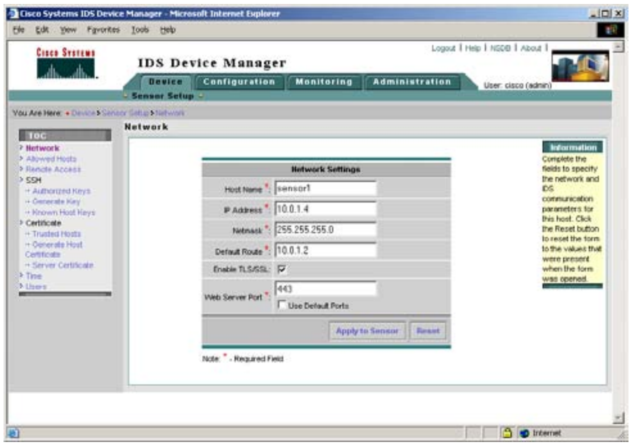
Security Management

This section describes the Cisco security management solution for intrusion detection products.

Sensor Device Management Products

Cisco.com

IDS Device Manager



Network

Network Settings

Host Name *:	sensor1
IP Address *:	10.0.1.4
Netmask *:	255.255.255.0
Default Route *:	10.0.1.2
Enable TLS/SSL:	☑
Web Server Port *:	443 □ Use Default Ports

Note: * - Required Field

Information

Complete the fields to specify the network and IDS communication parameters for this host. Click the Reset button to reset the form to the values that were present when the form was opened.

- **Web-based device configuration tool**
- **Software installed on the Sensor by default**
- **Small-scale Sensor deployments**

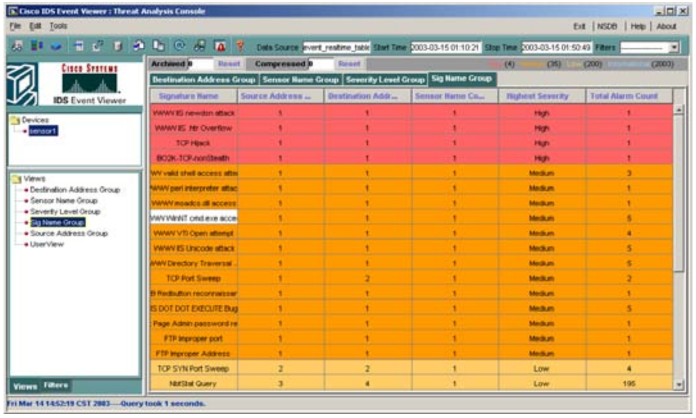
CSIDS 4.0—4-20

A network Sensor appliance can be managed via the IDS Device Manager (IDM). IDM is a web-based Sensor device configuration tool that is accessed securely via SSL and Transport Layer Security (TLS). IDM is best suited for small-scale Sensor deployments where there are no more than five Sensors.

Sensor Device Management Products (cont.)

Cisco.com

IDS Event Viewer



Data Source event_realtime_table Start Time 2003-03-15 01:10:21 Stop Time 2003-03-15 01:50:49 Filters

Archived 0 Compressed 0

Signature Name	Source Address ...	Destination Addr...	Sensor Name Co...	Highest Severity	Total Alarm Count
WWW IIS newdsn attack	1	1	1	High	1
WWW IIS .htr Overflow	1	1	1	High	1
TCP Hijack	1	1	1	High	1
BO2K-TCP-nonStealth	1	1	1	High	1
WV valid shell access atte	1	1	1	Medium	3
WWW perl interpreter attac	1	1	1	Medium	1
WWW msadcs dll access	1	1	1	Medium	1
WW WinNT cmd.exe acce	1	1	1	Medium	5
WWW VTI Open attempt	1	1	1	Medium	4
WWW IIS Unicode attack	1	1	1	Medium	5
WW Directory Traversal ...	1	1	1	Medium	5
TCP Port Sweep	1	2	1	Medium	2
B Redbutton reconnaissar	1	1	1	Medium	1
S DOT DOT EXECUTE Bug	1	1	1	Medium	5
Page Admin password re	1	1	1	Medium	1
FTP Improper port	1	1	1	Medium	1
FTP Improper Address	1	1	1	Medium	1
TCP SYN Port Sweep	2	2	1	Low	4
NbtStat Query	3	4	1	Low	195

Fri Mar 14 14:52:19 CST 2003—Query took 1 seconds.

- **Windows NT or Windows 2000**
- **Download from www.Cisco.com**
- **IDSM includes Event monitoring for up to three Sensors**

CSIDS 4.0—4-21

The IDS Event Viewer (IEV) is a windows application that is used for IDS event monitoring. IEV is a separate application from IDM and must be downloaded from www.cisco.com. IEV can monitor events for a maximum of three Sensors including the IDSM2.

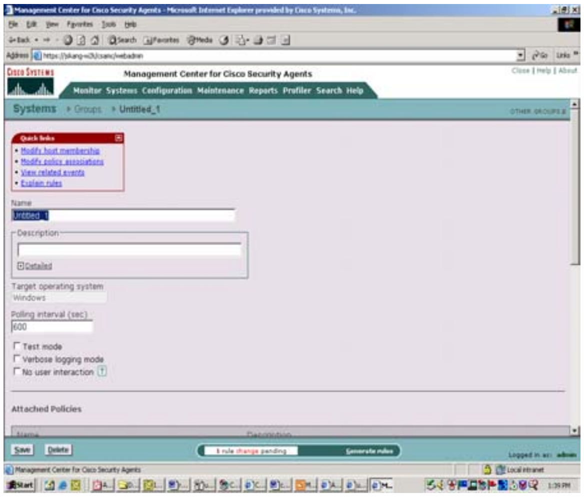
Note IEV 4.0 only works with IDS 4.0.or higher.

HIPS Management Product

Cisco.com

Management Center for Cisco Security Agent

- Runs on Windows 2000
- Provides agent management including deployment, configuration, event monitoring, and reporting


Management Center for Cisco Security Agents - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://skang-w2k/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Systems Groups Untitled_1
OTHER GROUPS
Quick links
Modify host membership
Modify policy associations
View related events
Explain rules
Attached Policies
Name
Description
Save
Delete
1 rule change pending
Generate rules
Logged in as: admin
Management Center for Cisco Security Agents
Local intranet
Start
1:39 PM

Name: Untitled_1

Description:

⊞ Detailed

Target operating system: Windows

Polling interval (sec): 600

☐ Test mode

☐ Verbose logging mode

☐ No user interaction

The CSA MC is an HTML web-based user interface required to manage and monitor Security Agent agents. This management console is able to generate e-mail and e-page notification messages, and has extensive reporting capabilities.

The security policy that will be applied by the Security Agent agents is defined in the Security Agent MC. The MC enables you to create a policy, modify it, and automatically distribute it to agents. You can manage up to 2500 security policies from one console. The Security Agent provides the following out-of-the-box policies to allow common applications to safely run on servers and desktops and control what operations they can perform:

- Microsoft IIS Web Server protection
- Microsoft SQL Server protection
- Microsoft Office protection
- Instant Messenger protection

From the Security Agent MC, you can also configure notification of security events by using any of the following strategies:

- View alerts in the web browser based GUI
- Generate e-mail messages
- Generate SNMP traps
- Dial a pager number

- Log to a flat file

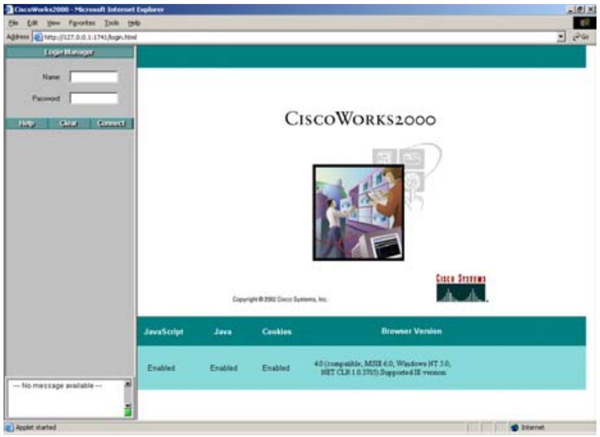
- Export alerts to 3rd party security management consoles

You can specify which alert options are to be used by which types of alerts. For example, you can have higher level alerts generate a pager notification, while lower level alerts generate SNMP traps. The Security Agent MC automatically suppresses similar events, avoiding the possibility of overloading operators with many copies of the same event message.

Security Agent alerts show that attacks have been stopped. Operators do not have to determine whether the alert represents an on-going attack and decide what to do about the situation in real time. Rather, alerts provide notification that an intrusion attempt was prevented.

VMS

Cisco.com


CiscoWorks2000 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://127.0.0.1:1741/login.html
Go
Login Manager
Name
Password
Help
Clear
Connect
CiscoWorks2000
Copyright © 2002 Cisco Systems, Inc.
Cisco Systems
— No message available —
Applet started
Internet

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible, MSIE 6.0, Windows NT 5.0, .NET CLR 1.0.3705) Supported IE version

- **An integrated management solution**
- **Provides web-based applications for the following:**
  - **Manage and monitor IDS Sensor**
  - **Security Monitor**
- **Features for configuring and monitoring firewall and IDS security**
- **Used for large-scale deployment**

CSIDS 4.0—4-23

The VPN/Security Management Solution (VMS) is an integrated management solution for VPN and security products. VMS is a suite of web-based applications targeted for large-scale deployments of Cisco security products. CiscoWorks VMS is organized into several functional areas:

- Firewall management
- Auto update server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

CiscoWorks Management Center updates for IDS Sensors and intrusion prevention include the following:

- CiscoWorks Management Center for IDS Sensors 1.2 centrally configures multiple network and switch IDS Sensors using group security profiles. Now supports IDS 4.1.

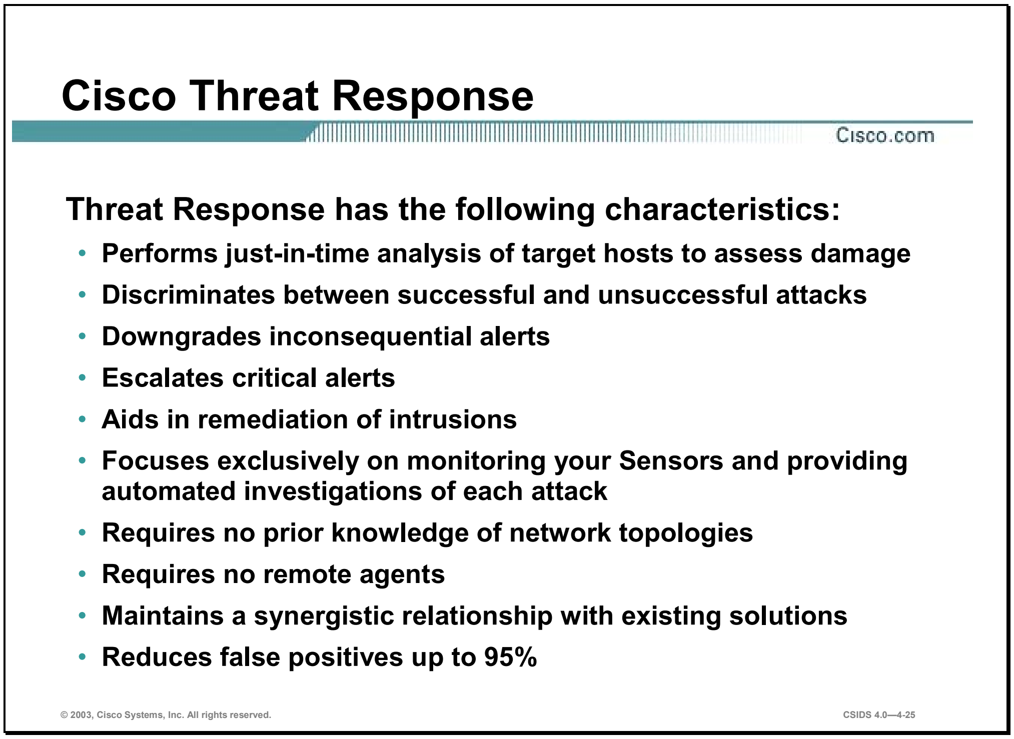
- CiscoWorks Monitoring Center for Security 1.2 identifies potential network attacks by capturing, storing and reporting on events from Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.

- CSA MC—A console providing centralized policy definitions, distribution, and software updates with constant communications to primary agents.

- Security Agents—Endpoint software that resides on servers, desktops, or laptops, and autonomously enforces local policies that prevent unauthorized access. Three server agents are provided to protect CiscoWorks VMS 2.2. Additional server or desktop agents are sold separately.

Cisco Threat Response

This section describes Cisco's Threat Response technology.



Cisco Threat Response

Cisco.com

Threat Response has the following characteristics:

- **Performs just-in-time analysis of target hosts to assess damage**
- **Discriminates between successful and unsuccessful attacks**
- **Downgrades inconsequential alerts**
- **Escalates critical alerts**
- **Aids in remediation of intrusions**
- **Focuses exclusively on monitoring your Sensors and providing automated investigations of each attack**
- **Requires no prior knowledge of network topologies**
- **Requires no remote agents**
- **Maintains a synergistic relationship with existing solutions**
- **Reduces false positives up to 95%**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—4-25

Network administrators can become so overwhelmed with the number of alerts generated by NIDS that intrusions go un-attended. Attacks that fail because they target secure systems are reported with the same severity as attacks that are successful. Administrators must decide which attacks to investigate. Often, the attacks selected for investigation are attacks that have failed, while attacks that have succeeded may go uninvestigated. This allows potentially serious threats to go unnoticed. By the time a successful attack is discovered, key forensic evidence on the targeted system may already be altered, making it difficult to successfully respond to the event.

Cisco's Threat Response technology remedies this situation by downgrading inconsequential alarms and escalating critical alerts. Threat Response works with Cisco Network IDS Sensors to increase the efficiency of Cisco IDS and is characterized by the following:

- Examines every alert your Sensor generates
- Eliminates false alarms and escalates real attacks—By inspecting the targeted host to assess what, if any damage, has been perpetrated, Threat Response is able to eliminate false and fruitless alarms. By the same token, it escalates true alarms so that they can receive the necessary attention.
- Captures forensics evidence including impacted files and logs

- Requires no remote agents—Threat Response runs independently on a single Windows system.

- Synergistic relationship with existing solutions—Threat Response works in conjunction with Cisco IDS to collect Sensor data. It uses the data to perform forensic investigative analysis and expose vulnerabilities.

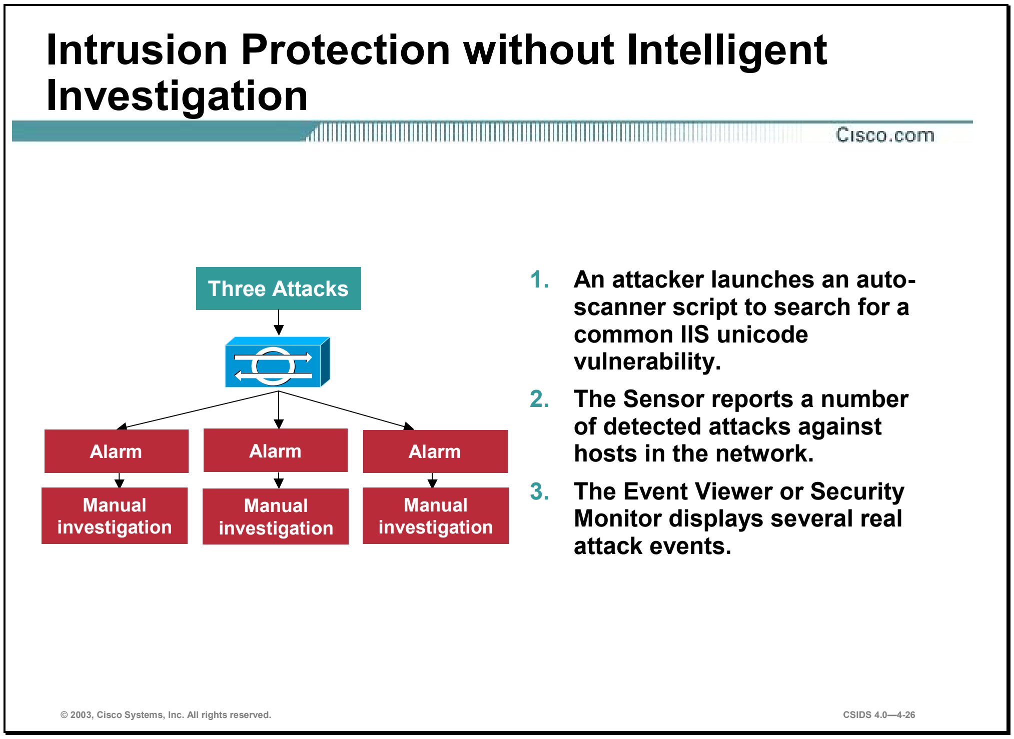
- Requires no knowledge of your network architecture other than a range of IP addresses to protect—Threat Response becomes aware of your systems only after an attack is directed against any of them.

- Wizard-based configuration

- Automatic updates

- Remote management

Cisco releases updates to keep the Threat Response IDS signature database up to date, as well as corresponding forensic signature updates to investigate IDS events. When an update is available, you are notified via the Threat Response GUI. You can use the integrated auto-update feature to keep the product current.



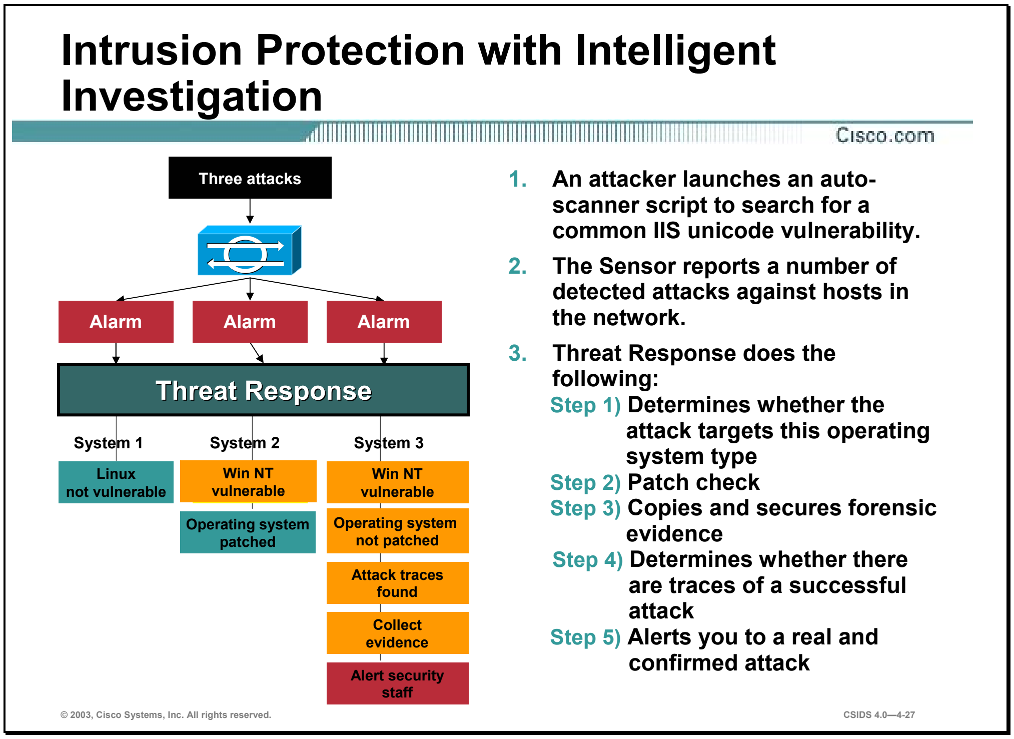
Intrusion Protection without Intelligent Investigation

1. An attacker launches an auto-scanner script to search for a common IIS unicode vulnerability.
2. The Sensor reports a number of detected attacks against hosts in the network.
3. The Event Viewer or Security Monitor displays several real attack events.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—4-26

The figure illustrates what happens when NIDS detects a number of possible attacks and the intelligent investigation provided by Threat Response is not available. Three attacks are detected and reported. Unable to discern alarms that represent successful attacks from false alarms and unsuccessful attacks, the security staff is forced to manually investigate each alarm to ensure the security of the enterprise. Their only alternative is to choose which attacks to investigate. However, if they choose the wrong alarms, the enterprise is compromised.



Intrusion Protection with Intelligent Investigation

Three attacks

Alarm

Alarm

Alarm

Threat Response

System 1

Linux not vulnerable

System 2

Win NT vulnerable

Operating system patched

System 3

Win NT vulnerable

Operating system not patched

Attack traces found

Collect evidence

Alert security staff

1. An attacker launches an auto-scanner script to search for a common IIS unicode vulnerability.
2. The Sensor reports a number of detected attacks against hosts in the network.
3. Threat Response does the following:
   - Step 1) Determines whether the attack targets this operating system type
   - Step 2) Patch check
   - Step 3) Copies and secures forensic evidence
   - Step 4) Determines whether there are traces of a successful attack
   - Step 5) Alerts you to a real and confirmed attack

CSIDS 4.0—4-27

When Cisco Threat Response receives alerts, it launches a multiphase analysis as follows:

Step 1 Level 1 investigation—Target operating system or device vulnerability check. Threat Response dispatches an agent to determine, in real time, the operating system that runs on the targeted system. Based on this information, it can rule out whether the target platform is vulnerable to the attack. The Level 1 investigation also detects any web servers that are running on the host.

Step 2 Patch check—Detailed system investigation. Threat Response logs on to the target host and uses read-access privileges to conduct a detailed system investigation based on the attack type. The investigation may include the following:

- Analysis of registry entries, system and log files (for example, a service-pack check)
- Search for specific files or directories seeking attack traces
- Other investigative methods to determine the success or failure of an attack

Step 3 Confirmed attack notification—Alerts the system administrator with information about the nature of the attack, complete details on how the investigation was conducted, and copies of the forensic evidence gathered.

Step 4 Forensic evidence retrieval—If it confirms an attack, collects forensic evidence, and copies this information to a secure location for offline analysis and to prevent tampering.

The figure demonstrates how the Threat Response technology provides an intelligent intrusion response capability for the same set of events. The NIDS detects three possible attacks, and dispatches three alarms. Threat Response receives those alarms and immediately begins its real-time investigation of each individual system. The sequence of events are as follows:

System 1—Linux operating system

Step 1 Runs a check to determine the operating system of the targeted system. Determines that this is a Linux host.

Step 2 Downgrades the alarm because it knows this attack does not target Linux hosts.

System 2—Windows NT operating system—The following are the steps if the operating system is patched:

Step 1 Runs a check to determine the operating system of the targeted system. Determines that this is a Windows NT host.

Step 2 Because it knows this attack targets Windows NT hosts, logs in to the host and checks to see if the system is patched against this attack. Determines that applicable service packs and hot fixes are installed.

Step 3 Downgrades the alarm.

System 3—Windows NT operating system—The following are the steps if the operating system is not patched:

Step 1 Runs a check to determine the operating system of the targeted system. Determines that this is a Windows NT host.

Step 2 Because it knows this attack targets Windows NT hosts, logs in to the host and checks to see if the system is patched against this attack. Determines that applicable service packs and hot fixes are not installed.

Step 3 Checks applicable Web server logs for signs of a successful attack. Determines that there are signs of a successful attack.

Step 4 Checks for other signs of intrusion. Discovers dropper files and other evidence.

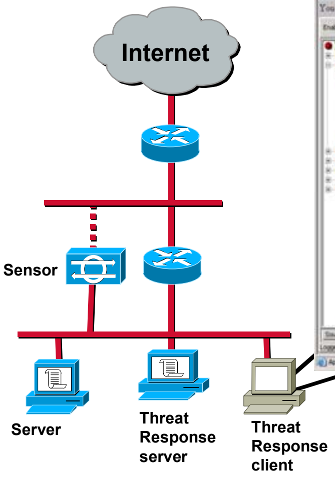
Step 5 Copies all collected forensic evidence to the central command-and-control server.

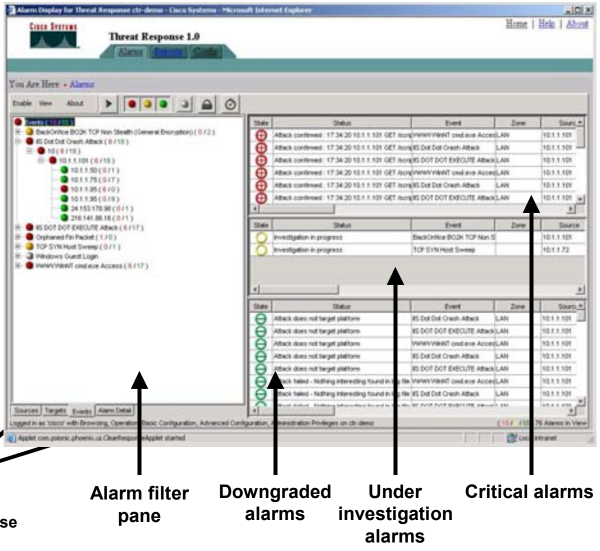
Step 6 Escalates the attack to critical status for immediate response by an administrator.

In less than five seconds, Threat Response has investigated the alarms and determined which one was successful. To aid in quick remediation, Threat Response has also obtained forensic data (such as log files) from the attacked system before an intruder could compromise the information.

Threat Response Deployment

Cisco.com





Alarm filter pane

Downgraded alarms

Under investigation alarms

Critical alarms

CSIDS 4.0—4-28

Threat Response consists of the following two components:

- The Threat Response server, which manages the alarm data and conducts investigations. The server must be a dedicated Windows 2000 Professional system with Service Pack 2 and Internet Explorer 5.5 (or later).

- The Threat Response client (or GUI), which provides users with a view of alarm data and the ability to configure the Threat Response server through a web browser. The client can be a non-dedicated Windows system with Internet Explorer 5.5 (or later) and browser access to the Threat Response server. Threat Response uses a secure socket layer (SSL) connection under Microsoft's Internet Explorer.

Note You can run the GUI on the same system as the Threat Response server, but because of performance and speed considerations, Cisco recommends that you run the GUI on a separate system.

In the GUI, you can do the following:

- Configure the CRT server.

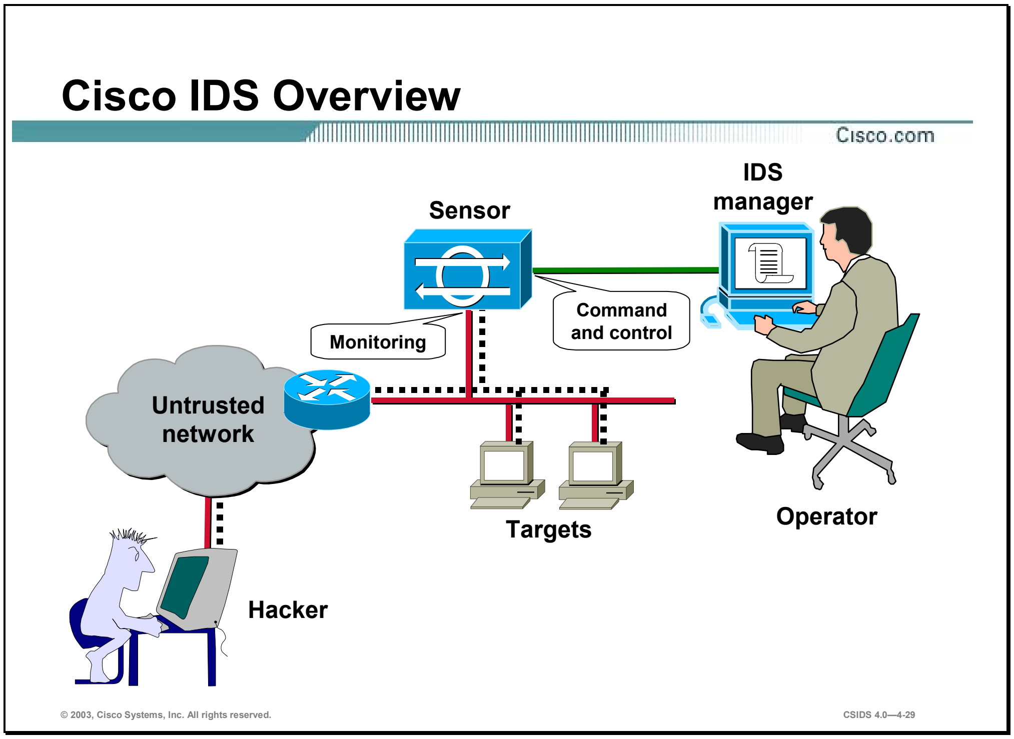
- View default reports about network activities monitored by Sensors including summary reports based on alarms, sources, or destinations. You can also create custom reports to meet the specific needs of your environment.

- View alarm data. Each alarm is placed in one of the following categories:

- Critical
- Under investigation
- Downgraded

Cisco IDS Communication Overview

This section provides an overview of the communication protocol used by Cisco IDS. The Cisco IDS communication is discussed in detail in the Cisco Intrusion Detection System Architecture chapter.

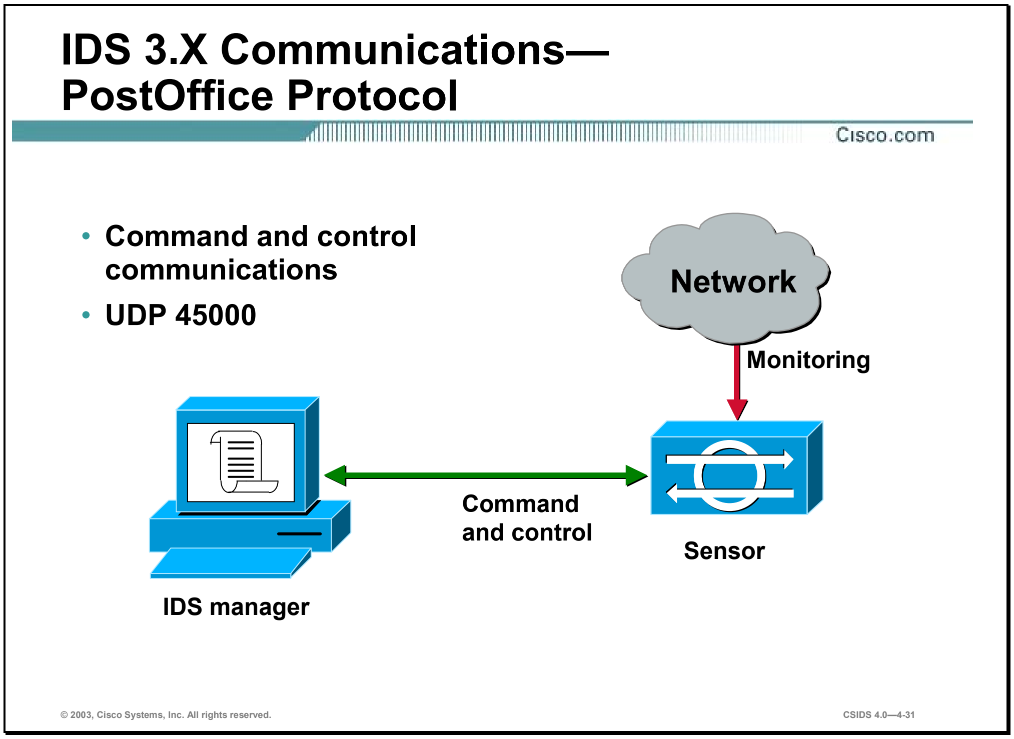


Cisco IDS Overview

Cisco.com

CSIDS 4.0—4-29

Cisco IDS involves the real-time monitoring of network packets. Sensors have a monitoring interface and a command and control interface. The monitoring interface captures the network traffic that is analyzed by the IDS Signatures Engine. Alarms and commands are sent between the Sensor and the IDS manager via the command and control interface. The IDS manager is management software used to configure the Sensor.



IDS 3.X Communications—PostOffice Protocol

- Command and control communications
- UDP 45000

Network

Monitoring

Command and control

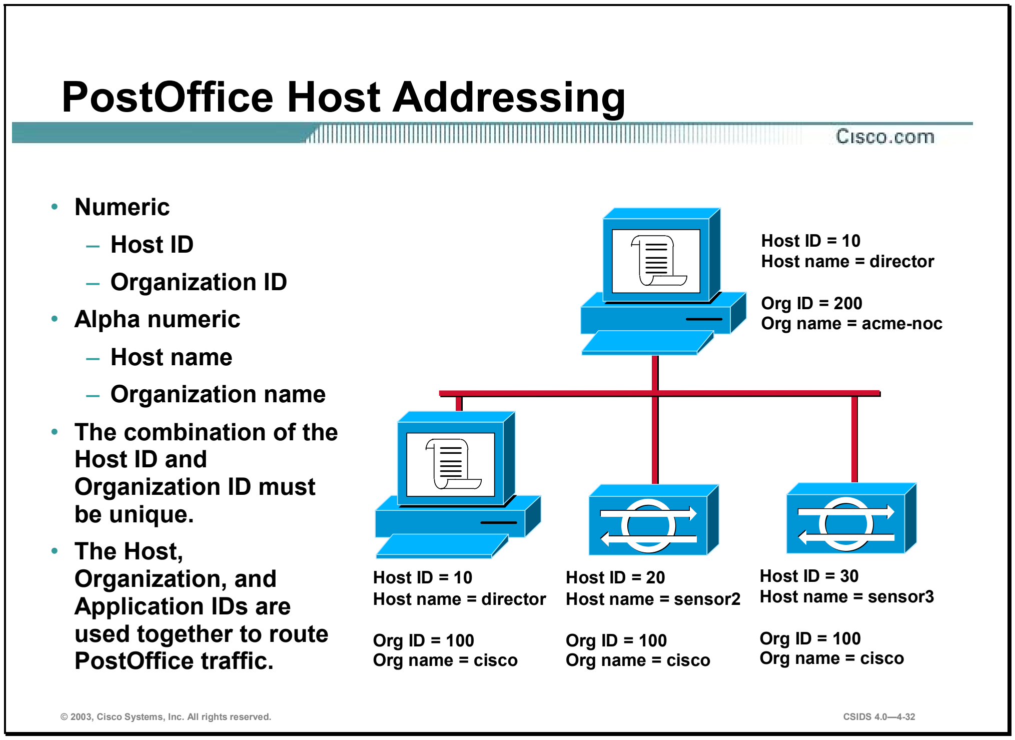
Sensor

IDS manager

CSIDS 4.0—4-31

In Sensor software version 3.X, Cisco IDS services and hosts communicate with one another using the PostOffice protocol. By default, PostOffice communication occurs over UDP port 45000. The command and control interface is assigned an IP address and is used for the following functions:

- Communication with other Cisco IDS devices—Event monitoring and device configuration
- Communication with blocking devices—IOS-based routers and PIX Firewalls
- Network access to the Sensor for management—Telnet, Secured Shell (SSH), and HTTP access



PostOffice Host Addressing

Cisco.com

- Numeric
  - Host ID
  - Organization ID
- Alpha numeric
  - Host name
  - Organization name
- The combination of the Host ID and Organization ID must be unique.
- The Host, Organization, and Application IDs are used together to route PostOffice traffic.

Host ID = 10
Host name = director

Org ID = 200
Org name = acme-noc

Host ID = 10
Host name = director

Org ID = 100
Org name = cisco

Host ID = 20
Host name = sensor2

Org ID = 100
Org name = cisco

Host ID = 30
Host name = sensor3

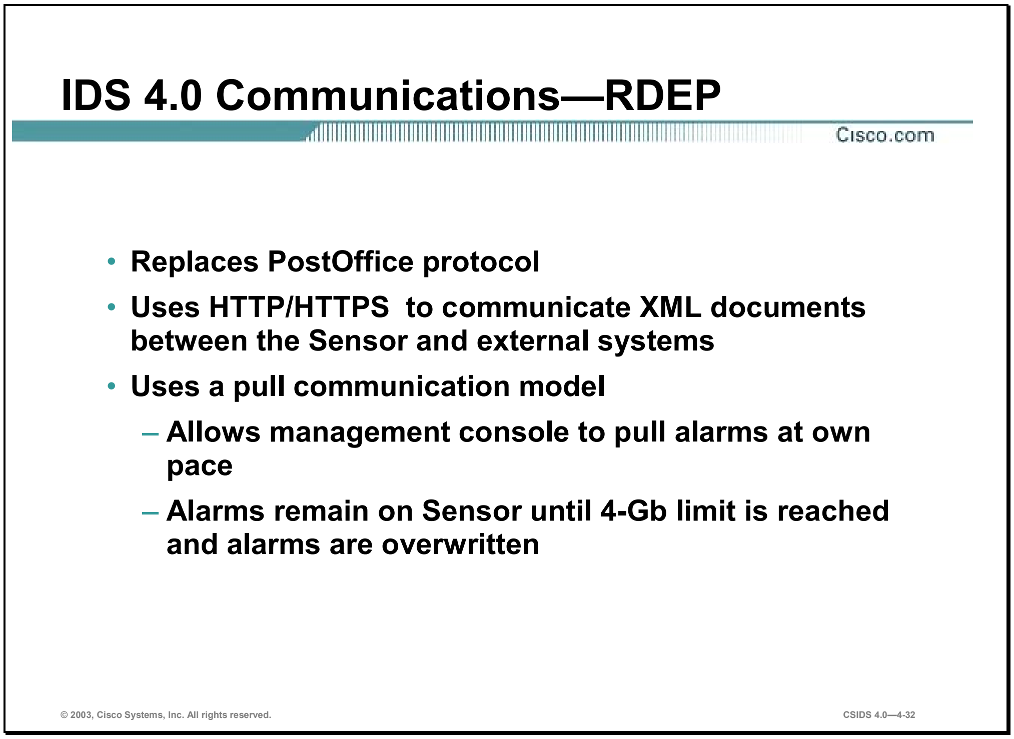
Org ID = 100
Org name = cisco

CSIDS 4.0—4-32

You must assign each Cisco IDS device a unique numeric identifier. This unique numeric identifier is a combination of a host identification and an organization identification. With every host identification and organization identification combination, there is an associated alphanumeric identifier consisting of a host name and an organization name. The following are descriptions of the individual identifiers:

- Host identification—Numeric identification for the Cisco IDS device (1–65535).
- Organization identification—Numeric identification for the Cisco IDS organization (1–65535). It can be used to group a number of Cisco IDS devices together under the same number for easy identification purposes.
- Host name—An alphanumeric identifier for a Cisco IDS device. The name chosen here is typically one that contains the word “Sensor” or “director” so you can easily identify the device type.
- Organization name—An alphanumeric identifier for a group of Cisco IDS devices. The name chosen here is typically one that describes the name of the company where the device is installed or the name of the department within the company where the device is installed.
- Application identification—A numeric identification assigned to the Cisco Secure IDS daemon.

The host and organization identifications make up two-thirds of the three-part PostOffice proprietary addressing scheme. The third part of the addressing scheme is a unique application identifier. PostOffice uses these unique identifiers to route all command and control communications.



IDS 4.0 Communications—RDEP

Cisco.com

- Replaces PostOffice protocol
- Uses HTTP/HTTPS to communicate XML documents between the Sensor and external systems
- Uses a pull communication model
  - Allows management console to pull alarms at own pace
  - Alarms remain on Sensor until 4-Gb limit is reached and alarms are overwritten

CSIDS 4.0—4-32

In IDS 4.0, the PostOffice protocol has been replaced with the Remote Data Exchange Protocol (RDEP). RDEP uses HTTP and TLS/SSL to securely pass XML documents between the Sensor and external systems. Whereas PostOffice uses a push model to push alarms across the communication channel to management applications, RDEP uses a pull model. The pull model allows the management application to pull alarms at its own pace. As soon as the management console connects to the Sensor and requests alarms, the alarms are returned to the management console without delay.

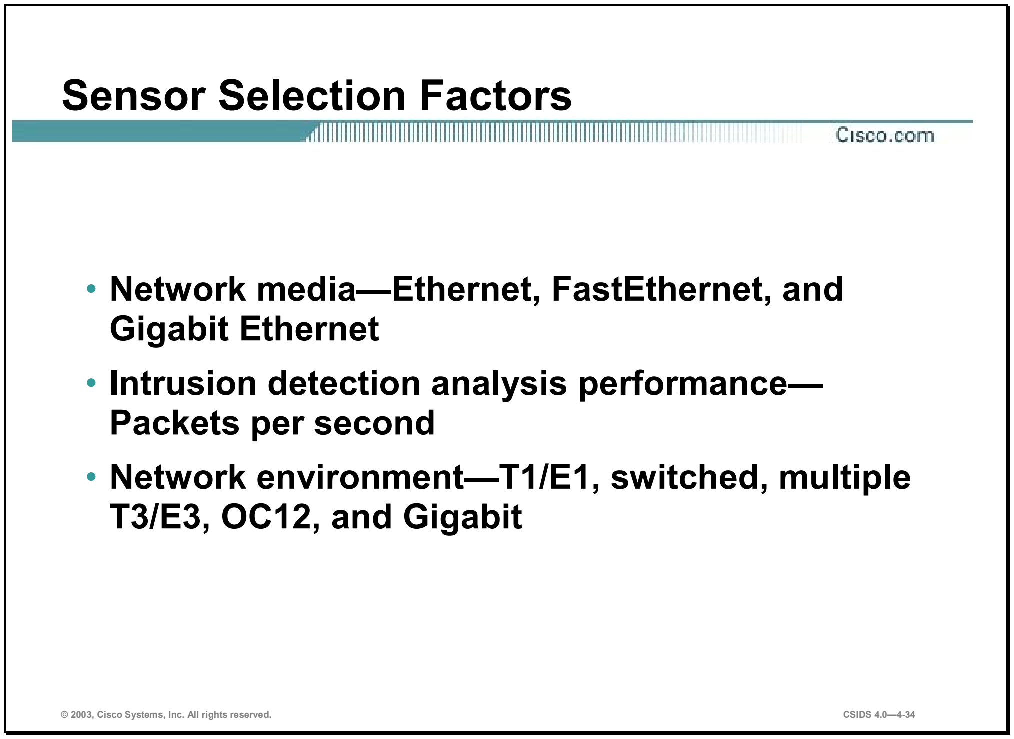
Note RDEP communications are explained in depth later in the course.

RDEP does not specify the schemas for the XML documents exchanged in RDEP messages. This is done by the Intrusion Detection Interaction and Operations Messages (IDIOM) specification.

Note See the RDEP and IDIOM specifications on CCO for more information.

Deploying Cisco IDS

This section discusses the factors to consider when deploying a Cisco IDS solution.



Sensor Selection Factors

- Network media—Ethernet, FastEthernet, and Gigabit Ethernet
- Intrusion detection analysis performance—Packets per second
- Network environment—T1/E1, switched, multiple T3/E3, OC12, and Gigabit

© 2003, Cisco Systems, Inc. All rights reserved.

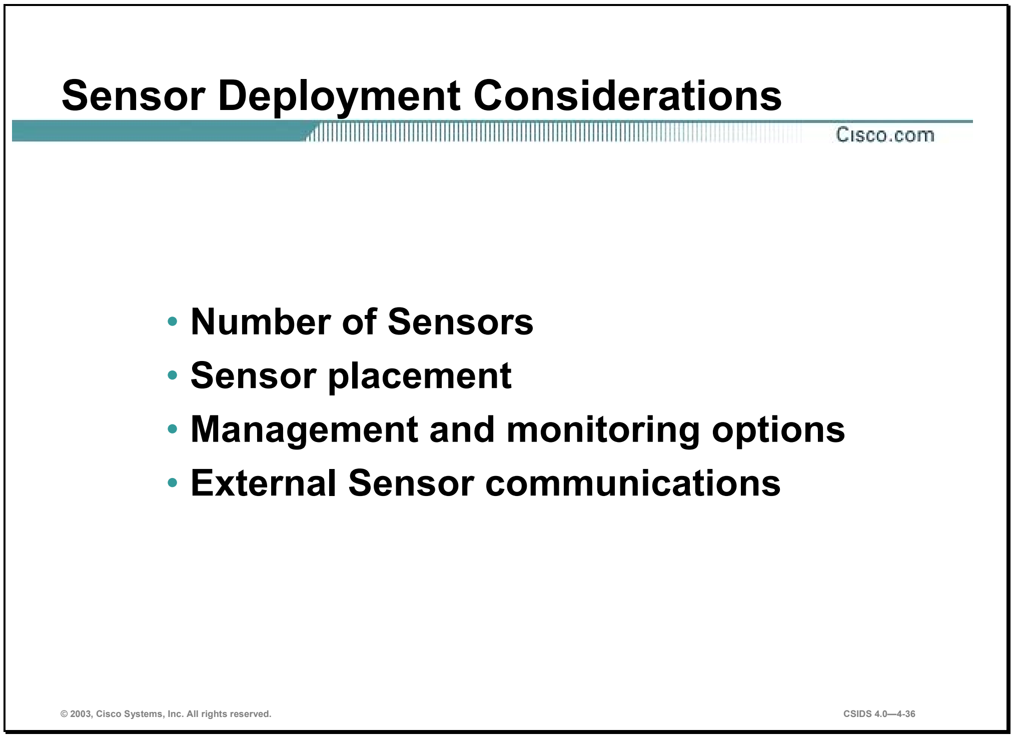
CSIDS 4.0—4-34

Several factors affect the decisions made when selecting Sensors for a Cisco IDS solution: political, financial, and technical. For the purpose of this discussion, the focus is on those technical factors to consider when selecting Sensors for a Cisco IDS solution. The following are the technical factors to consider when selecting Sensors:

- Network media—Sensor selection is affected based on the network media and environment. Cisco IDS Sensor network interface cards (NICs) range from Ethernet to Gigabit Ethernet.

- Intrusion detection analysis performance—The performance for the Sensors is rated by the number of packets per second that can be captured and accurately analyzed. Cisco IDS Sensor performance range from 45 Mbps to 1000 Mbps.

- Network environment—Cisco IDS Sensors are suited for networks that have network speeds ranging from 10/100BaseT Ethernet to Gigabit.



Sensor Deployment Considerations

- Number of Sensors
- Sensor placement
- Management and monitoring options
- External Sensor communications

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—4-36

Deploying a Cisco IDS solution requires a well thought-out design. The following are the important design issues to take into consideration:

- Your network topology—Knowledge of your network topology will help you determine how many IDS appliances are required, the hardware configuration for each IDS appliance (for example, the size and type of network interface cards), and how many IDS management workstations are needed. The IDS appliance monitors all traffic across a given network segment. With that in mind, you should consider all the connections to the network you want to protect. Before you deploy and configure your IDS appliances, you should understand the following about your network:
  - The size and complexity of your network
  - Connections between your network and other networks, including the Internet
  - The amount and type of network traffic on your network
- Sensor placement—It is recommended that Sensors be placed at those network entry and exit points that provide sufficient intrusion detection coverage. Determine the type of location you have in order to determine which segments of the network you want to monitor. Keep in mind that each IDS appliance maintains a security policy configured for the segment it is monitoring. The security policies can be standard across the organization or unique for each IDS appliance. 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 appliances required to protect the desired network. You can place an IDS appliance in front of or behind

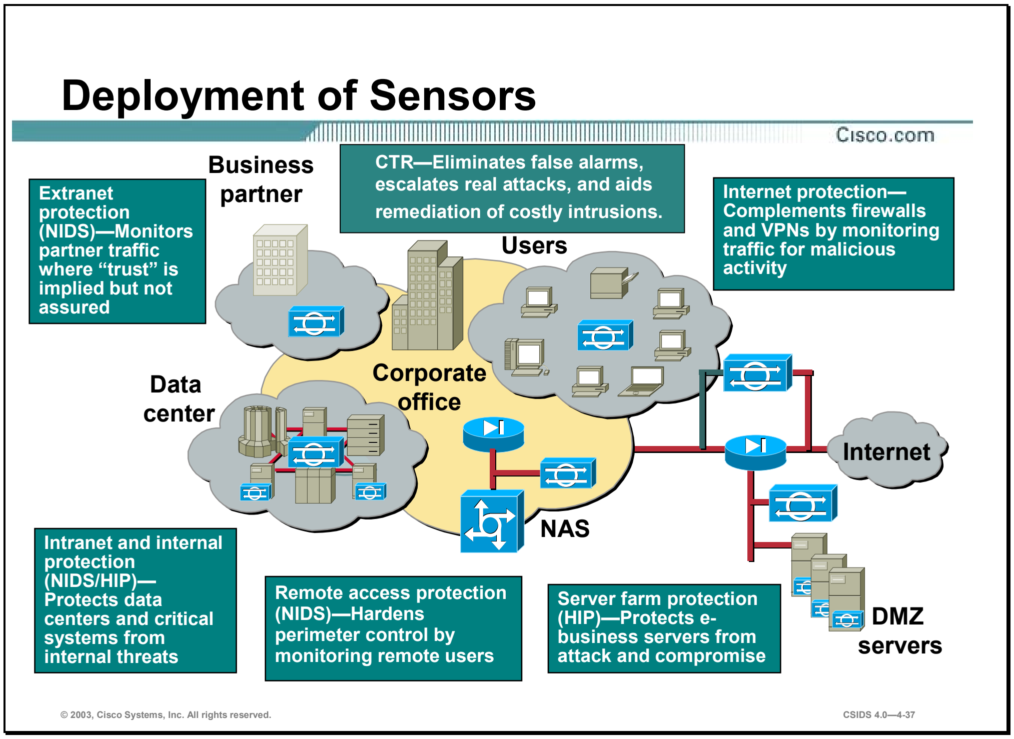
a firewall. Each position has its benefits and drawbacks. These benefits and drawbacks are discussed later in the chapter.

- Management and monitoring options—Review the management and monitoring options discussed earlier in this chapter to select those most appropriate for your network. Keep in mind that the number of Sensors that you will deploy is in direct correlation to the type of management console you select. The recommended Sensor to IEV ratio is 5:1. For the IDS MC, the ratio is 300:1.

- External Sensor communication—Traffic on the communication port between Sensors and external systems must be allowed through firewalls in order to ensure functionality. The following table shows the ports used by the various management and monitoring applications for communications with Sensors:

Management or Monitoring System	Protocol	Default Port
IDS MC	SSH	TCP 22
Security Monitor	SSL	TCP 443
IDM	SSL	TCP 443
IEV	SSL	TCP 443

Note IDS MC clients communicate with the IDS MC via SSL. Communications between the IDS MC and the Sensor use SSH.



Deployment of Sensors

CTR—Eliminates false alarms, escalates real attacks, and aids remediation of costly intrusions.

Extranet protection (NIDS)—Monitors partner traffic where "trust" is implied but not assured

Internet protection—Complements firewalls and VPNs by monitoring traffic for malicious activity

Intranet and internal protection (NIDS/HIP)—Protects data centers and critical systems from internal threats

Remote access protection (NIDS)—Hardens perimeter control by monitoring remote users

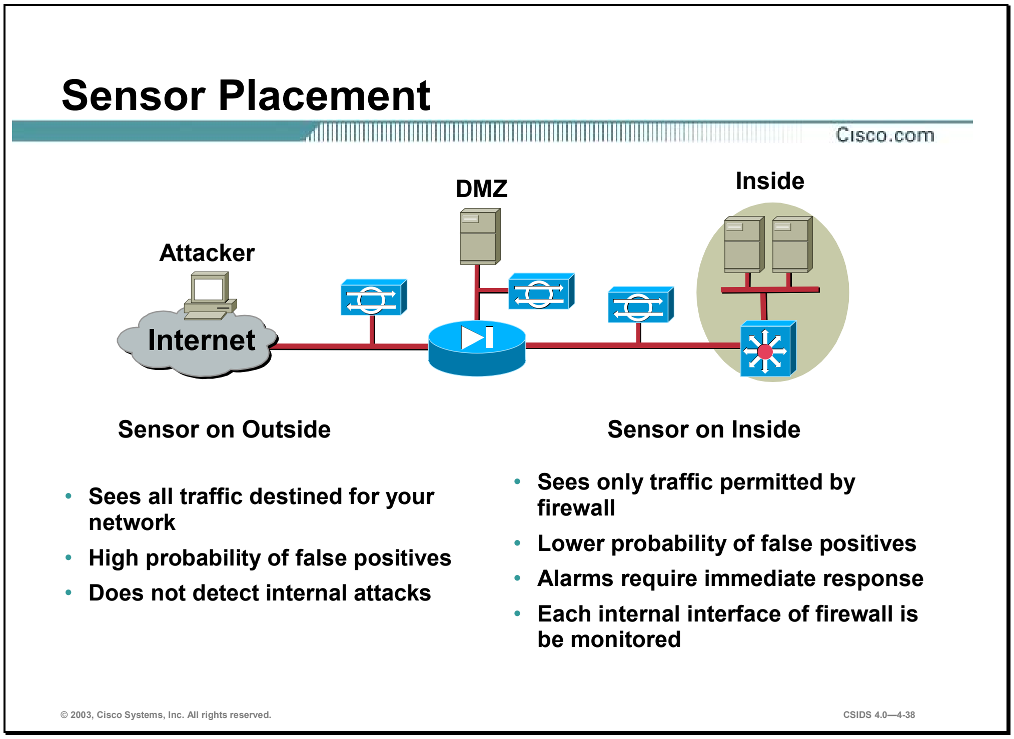
Server farm protection (HIP)—Protects e-business servers from attack and compromise

CSIDS 4.0—4-37

As you examine your network topology to determine how many IDS appliances are required, consider all connections to the network you want to protect. Locations that need to be protected generally fall into five basic categories as illustrated in the figure:

- Internet protection—A Sensor between your perimeter gateway and the Internet complements the firewall and VPN by monitoring traffic for malicious activity.
- Extranet protection—A Sensor between your network and extranet connections, such as a business partner, monitors traffic where trust is implied but not assured.
- Intranet and internal protection—Sensors on your intranet protect data centers and critical systems from internal threats.
- Remote access protection—A Sensor on your remote access network hardens perimeter control by monitoring remote access users.
- Server farm protection—Companies are deploying Internet servers on their DMZ networks. These servers offer Internet services such as Web, DNS, FTP, and SMTP. The Security Agent agents are installed on these servers. The Security Agent MC is installed on an internal network.

A complete Cisco intrusion detection solution includes the installation of both a Network-Based Intrusion Detection System (NIDS) and a Host-Based Intrusion Protection (HIP) system. NIDS Sensors are installed at network entry points to provide broader coverage, and HIP agents are installed on critical network servers.



Sensor Placement

Cisco.com

Sensor on Outside

- Sees all traffic destined for your network
- High probability of false positives
- Does not detect internal attacks

Sensor on Inside

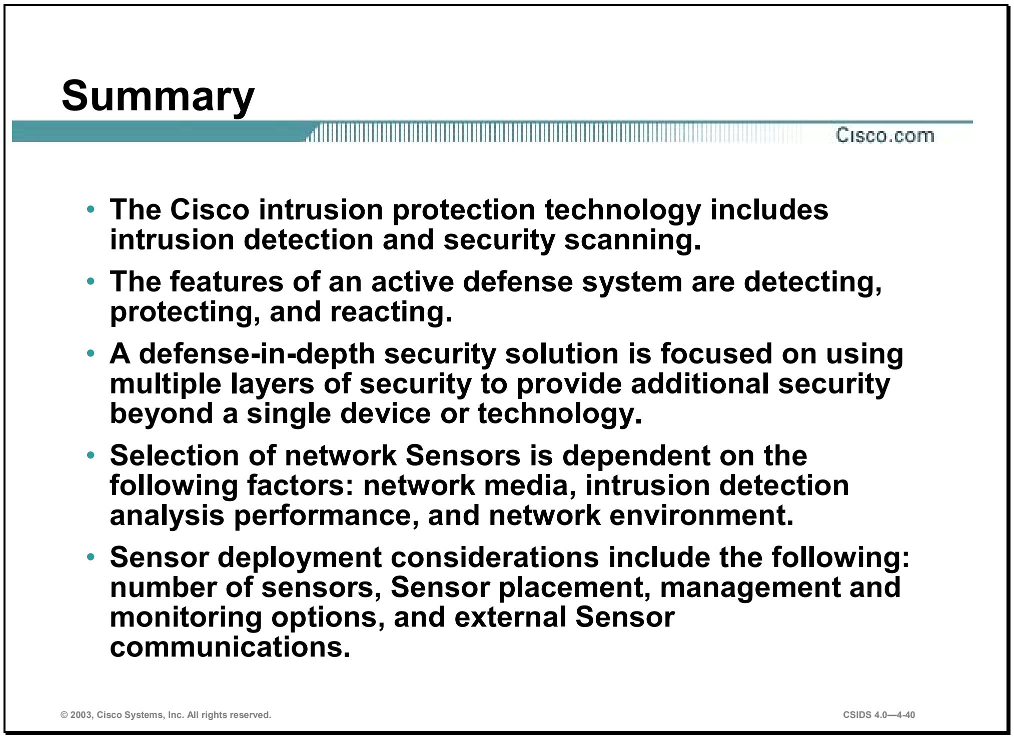
- Sees only traffic permitted by firewall
- Lower probability of false positives
- Alarms require immediate response
- Each internal interface of firewall is be monitored

CSIDS 4.0—4-38

Placing an IDS appliance in front of a firewall allows the IDS appliance to monitor all incoming and outgoing network traffic. However, when deployed in this manner, the IDS appliance does not detect traffic that is internal to the network. An internal attacker taking advantage of vulnerabilities in network services would remain undetected by the external IDS appliance. Placing an IDS appliance (a monitoring or sniffing interface) behind a firewall shields the IDS appliance from any policy violations that the firewall rejects.

Summary

This section summarizes what you have learned in this chapter.



Summary

Cisco.com

- The Cisco intrusion protection technology includes intrusion detection and security scanning.
- The features of an active defense system are detecting, protecting, and reacting.
- A defense-in-depth security solution is focused on using multiple layers of security to provide additional security beyond a single device or technology.
- Selection of network Sensors is dependent on the following factors: network media, intrusion detection analysis performance, and network environment.
- Sensor deployment considerations include the following: number of sensors, Sensor placement, management and monitoring options, and external Sensor communications.

CSIDS 4.0—4-40

5

Capturing Network Traffic for Intrusion Detection Systems

Overview

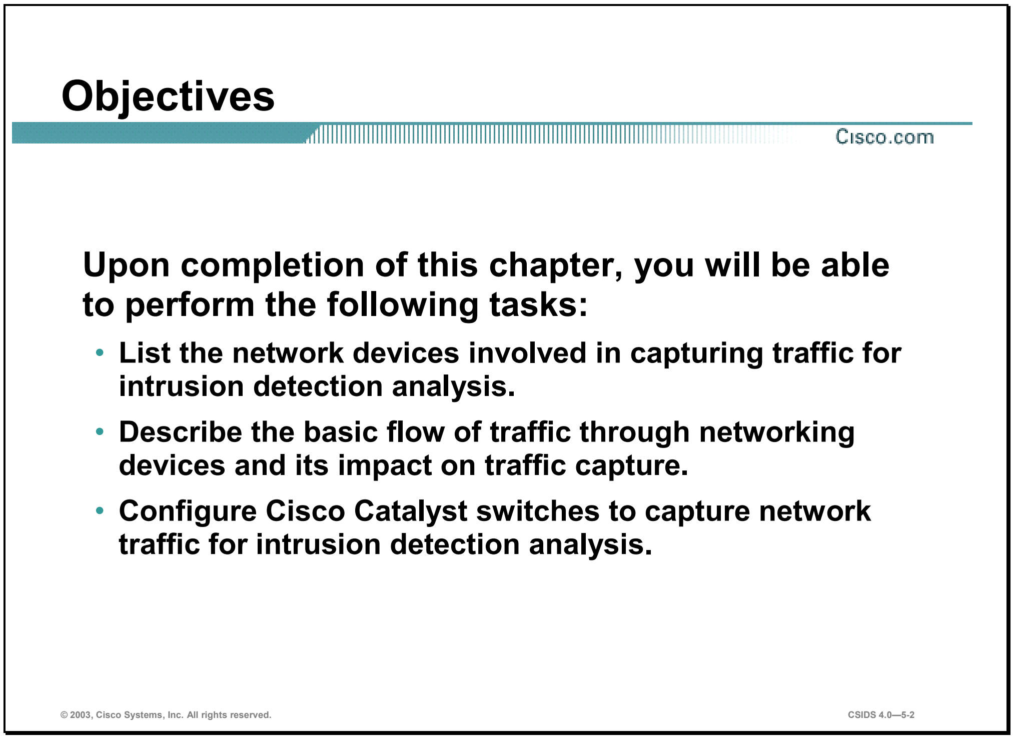
This chapter explains the methods to capture traffic for intrusion detection systems (IDSs) and how to configure Cisco Catalyst switches.

This chapter includes the following topics:

- Objectives
- Traffic capture overview
- Configuring SPAN for Catalyst 2900XL, 3500XL, 2950, and 3550 traffic capture
- Configuring SPAN for Catalyst 4000, 4500, and 6500 traffic capture
- Configuring RSPAN for Catalyst 4000 and 6500 traffic capture
- Configuring VACLs for Catalyst 6500 traffic capture
- Using the **mls ip ids** command for Catalyst 6500 traffic capture
- Advanced Catalyst 6500 traffic capturing
- Summary

Objectives

This section lists the chapter's objectives.



Objectives

Cisco.com

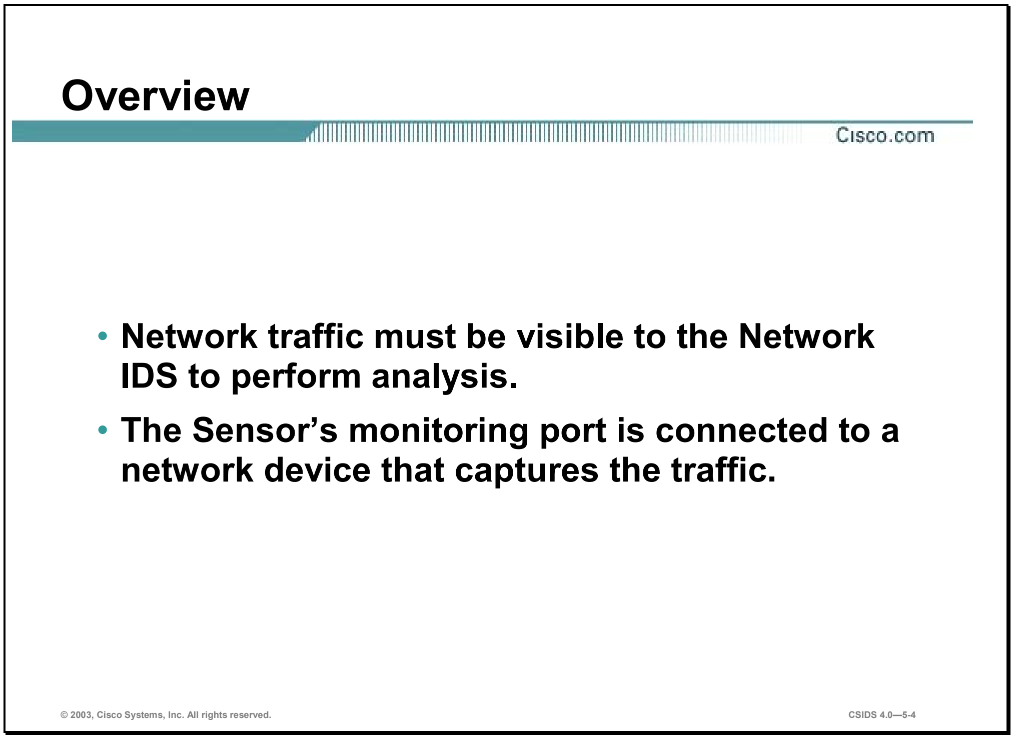
Upon completion of this chapter, you will be able to perform the following tasks:

- List the network devices involved in capturing traffic for intrusion detection analysis.
- Describe the basic flow of traffic through networking devices and its impact on traffic capture.
- Configure Cisco Catalyst switches to capture network traffic for intrusion detection analysis.

CSIDS 4.0—5-2

Traffic Capture Overview

This section discusses the network devices and methods involved in capturing network traffic for IDSs.



Overview

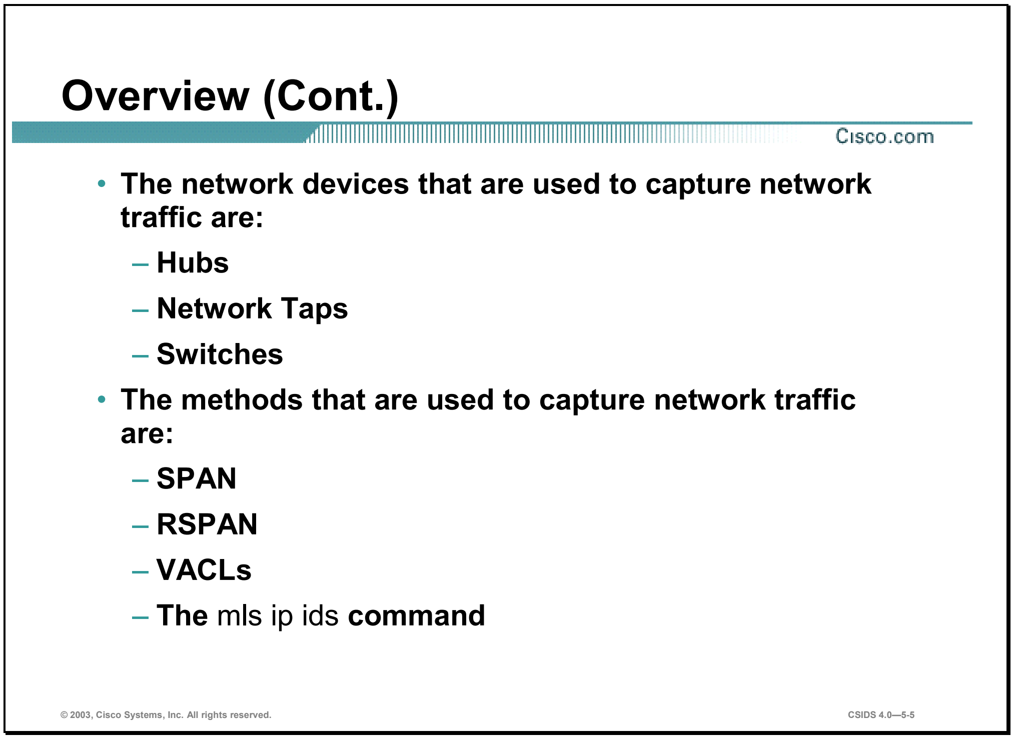
Cisco.com

- Network traffic must be visible to the Network IDS to perform analysis.
- The Sensor's monitoring port is connected to a network device that captures the traffic.

CSIDS 4.0—5-4

Network IDSs must be able to "see" network traffic in order to perform intrusion detection analysis. The term used to describe this activity is traffic capturing. The Sensor's monitoring interface is connected to a network device that captures the traffic.

Note The use of the term capture in this course encompasses any one of various methods to make network traffic visible to the Sensor. The ability to capture traffic may be inherent to a device technology or may require special features to provide this capability. For example, network hubs by their nature replicate data to all ports. Switches, on the other hand, rely on features such as port mirroring to permit the copy of specific traffic to another port.



Overview (Cont.)

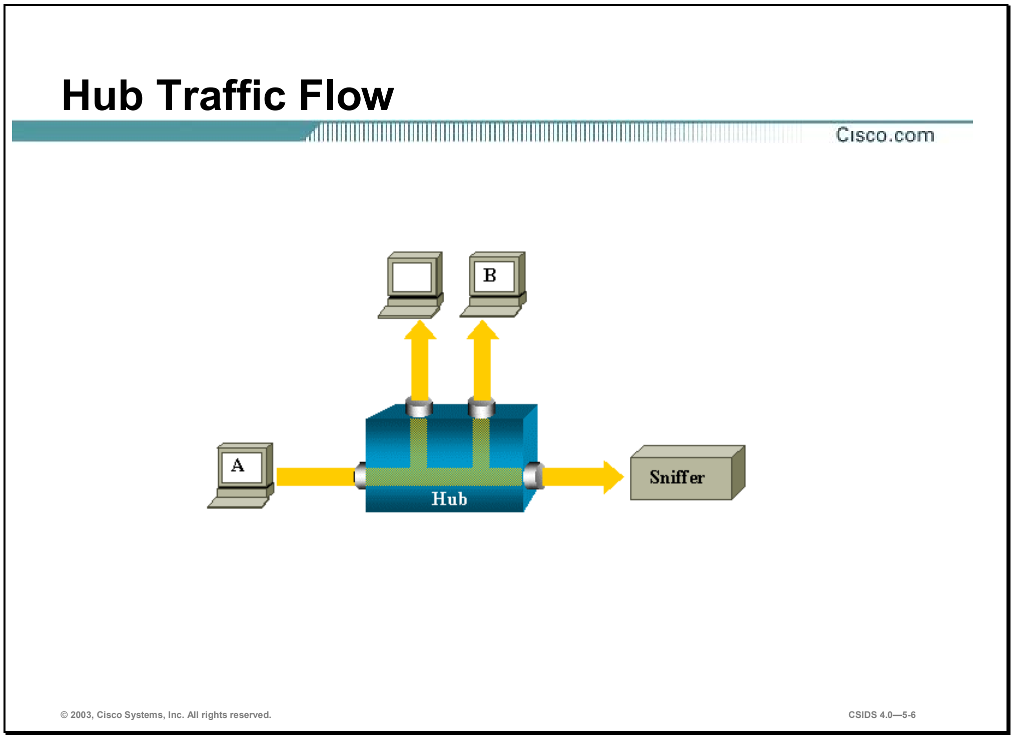
- **The network devices that are used to capture network traffic are:**
  - **Hubs**
  - **Network Taps**
  - **Switches**
- **The methods that are used to capture network traffic are:**
  - **SPAN**
  - **RSPAN**
  - **VACLs**
  - **The** mls ip ids **command**

CSIDS 4.0—5-5

The network devices that are used to capture traffic for IDSs are hubs, network taps, and switches. Methods of capturing traffic include the following:

- Switch Port Analyzer (SPAN)—Mirrors data from one or more sources (ports or VLANs) to a destination port on a local switch.
- Remote SPAN (RSPAN)—Mirrors data from one or more sources (ports or VLANs) to a destination port on a remote switch.
- VLAN access control list (VACLs)—Can selectively filter and forward VLAN traffic to the IDSM in a Catalyst 6500 switch.
- The **msl ip ids** command—The **mls ip ids** command is used instead of a VACL in situations where it is not possible to use VACLs. For example, you can use the **mls ip ids** command in the following scenarios:
  - You are running the Cisco IOS Firewall feature set on the Multilayer Switch Feature Card (MSFC) of a Catalyst 6500 switch with an Intrusion Detection System (IDS) Module (IDSM). VACLs are incompatible with (Context-based Access Control) CBAC; therefore, you cannot apply VACLs on the same VLAN in which you have applied an ip inspect rule for CBAC.
  - You are using ports as router interfaces rather than switch ports. There is no VLAN on which to apply a VACL.

Note Refer to the *Configuring Network Security* section of the Catalyst 6000 IOS documentation for more information regarding Context-Based Access Control (CBAC) and IDS.



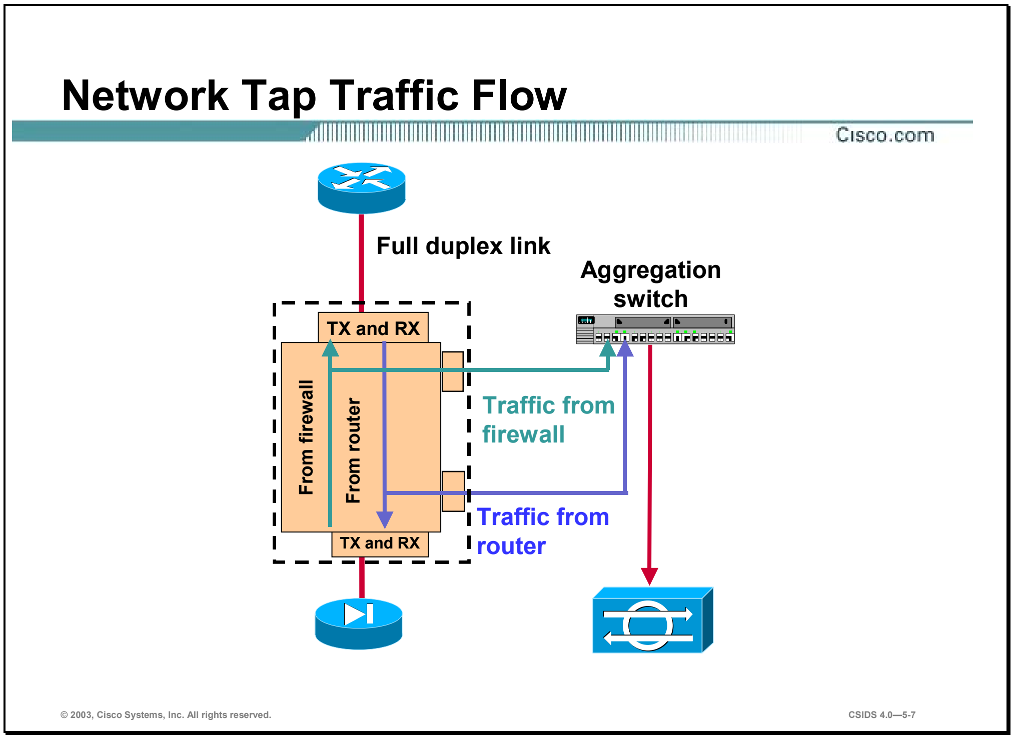
Hub Traffic Flow

Cisco.com

CSIDS 4.0—5-6

If you want to capture Ethernet traffic sent by host A to host B and both are connected to a hub, attach a sniffer to this hub as all other ports "see" the traffic between host A and B.

Note The sniffer is the network IDS.



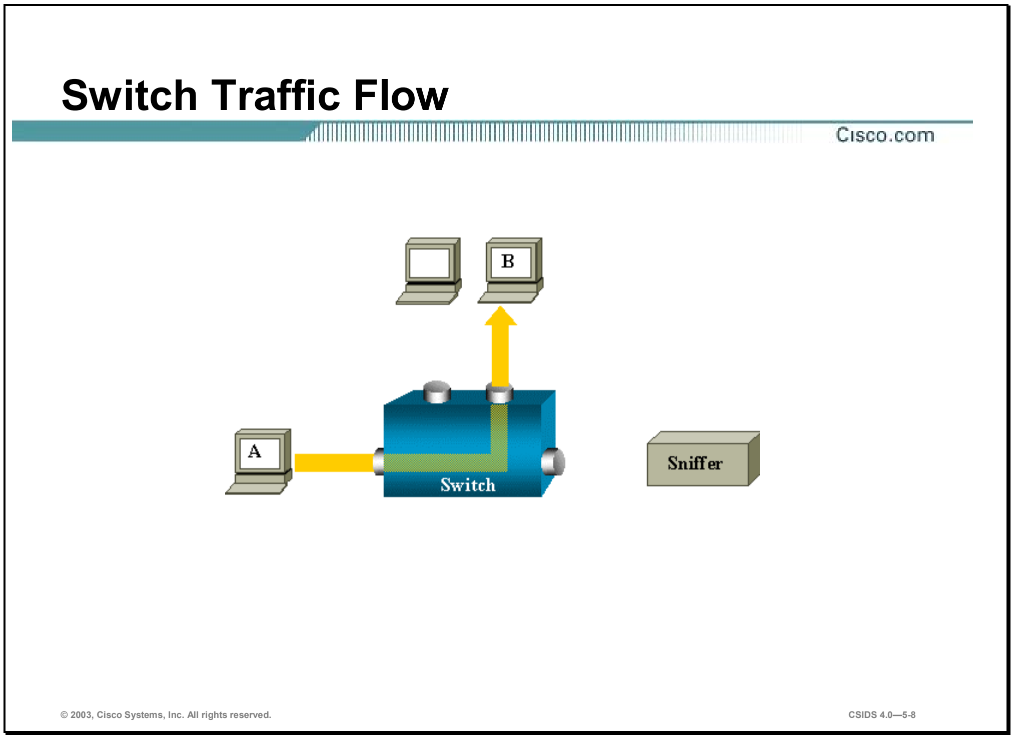
Network Tap Traffic Flow

CSIDS 4.0—5-7

A network tap is a device used to split full-duplex traffic flows into single traffic flows that can be aggregated at a switch device. The network tap has four connectors:

- Two input connectors—Traffic from a device
- Two output connectors—Traffic exiting the tap

In the figure above, a network tap is installed between a Cisco router and a Cisco PIX Firewall. The output connectors are connected to an aggregation switch. The Sensor is connected to a switch port that has been configured as a SPAN destination port.

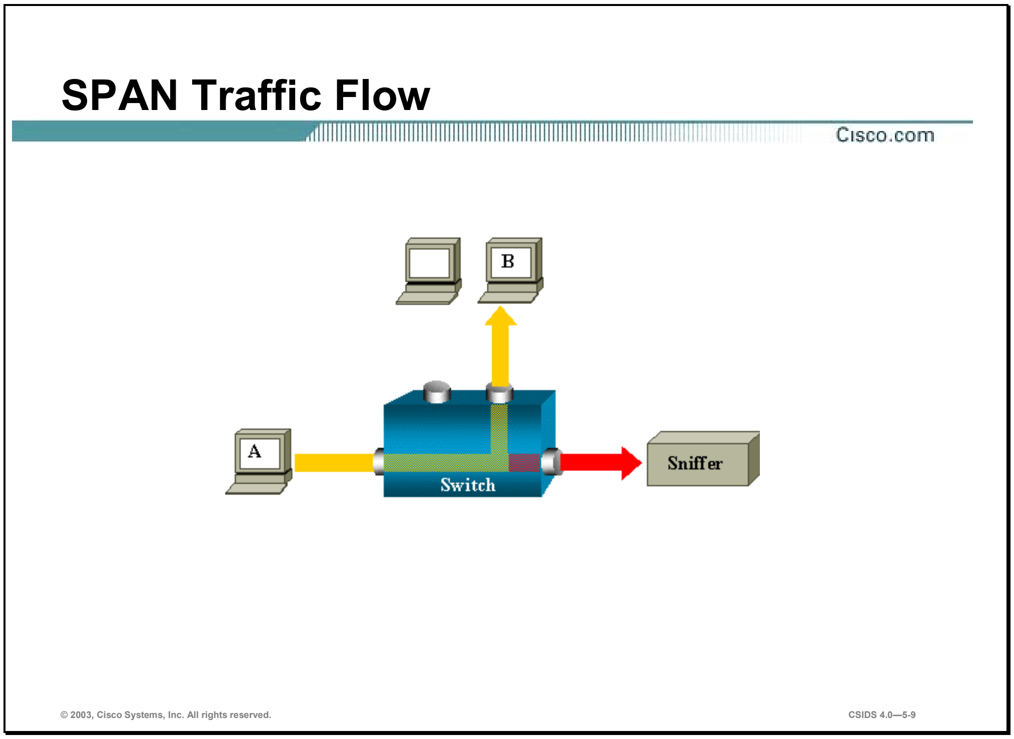


Switch Traffic Flow

CSIDS 4.0—5-8

On a switch, after host B's MAC address is learned, unicast traffic from A to B is only forwarded to B's port, and therefore not seen by the sniffer.

Note The sniffer is the network IDS.



SPAN Traffic Flow

Cisco.com

CSIDS 4.0—5-9

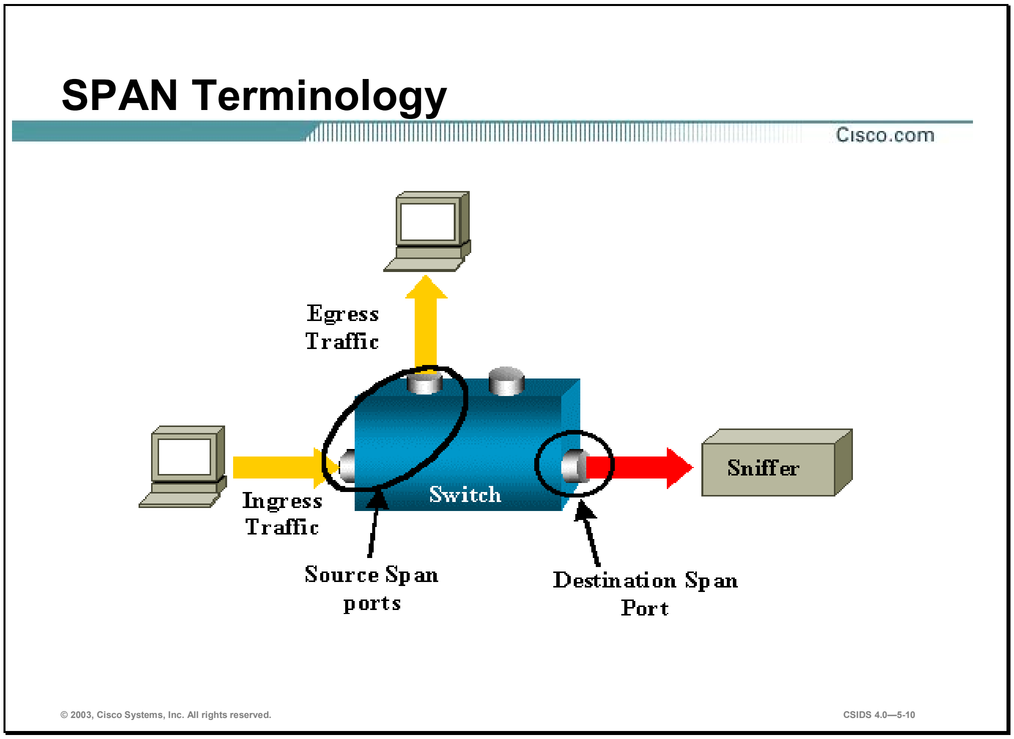
The Switched Port Analyzer (SPAN) feature, sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

The SPAN feature was introduced on switches because of a fundamental difference they have with hubs. Unlike hubs, which broadcast packets to all ports, switches learn the MAC addresses of connected devices, and therefore only forward traffic to the port of the destination device.

In the above diagram, the sniffer is attached to a port that is configured to receive a copy of every single packet that is sent by host A. This port is called a SPAN port.

Refer to *Configuring the Catalyst Switched Port Analyzer (SPAN) Feature* at http://www.cisco.com/warp/public/473/41.html for more information.

Note The sniffer is the network IDS.



SPAN Terminology

Cisco.com

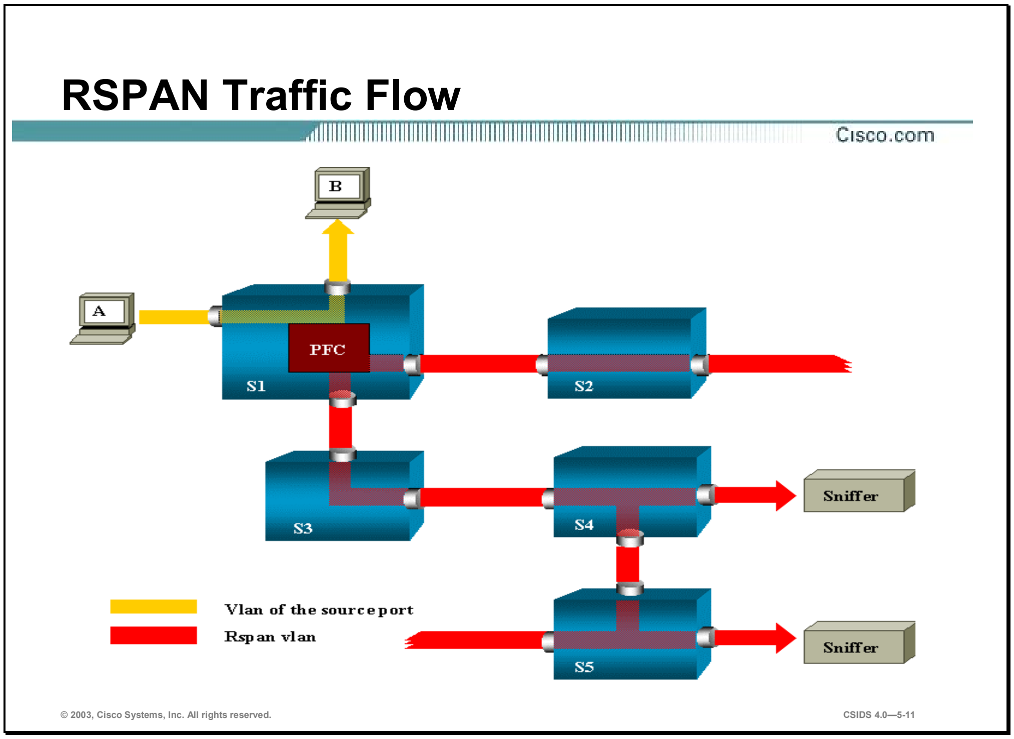
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—5-10

The following are the terms used when discussing the Cisco SPAN feature:

- Ingress traffic—Traffic enters the switch.
- Egress traffic—Traffic leaves the switch.
- Source (SPAN) Port—Port that is monitored using the SPAN feature.
- Destination (SPAN) Port—A port that is monitoring source ports, usually where a network analyzer is connected.
- Monitor Port—A monitor port is a destination SPAN port in Catalyst 2900XL/3500XL/2950 terminology.
- Local SPAN—The SPAN feature is local when the monitored ports are all located on the same switch as the destination port. This is in contrast to Remote SPAN (RSPAN) as seen below.
- RSPAN—Some source ports are not located on the same switch as the destination port. This is an advanced feature that requires a special Virtual LAN (VLAN) to carry the traffic being monitored by SPAN between switches. It is currently only available on the Catalyst 4000 switch with Catalyst OS 6.3 and on the Catalyst 6000 switch with Catalyst OS 5.3 and higher.
- Port-based SPAN (PSPAN)—The user specifies one or several source ports on the switch and one destination port.

- VLAN-based SPAN (VSPAN)—On a given switch, the user can choose to monitor all the ports belonging to a particular VLAN in a single command.



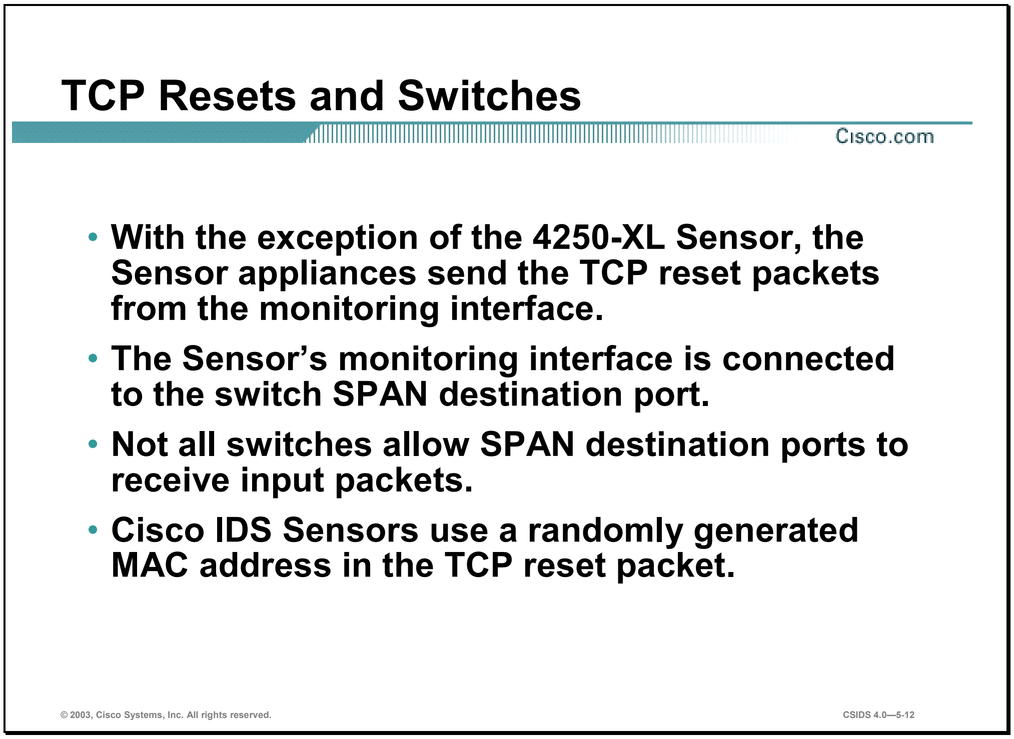
RSPAN Traffic Flow

CSIDS 4.0—5-11

Note RSPAN allows you to monitor source ports spread all over a switched network, not only locally on a switch with SPAN. The functionality works exactly as a regular SPAN session. The traffic monitored by SPAN, instead of being directly copied to the destination port, is flooded into a special RSPAN VLAN. The destination port can then be located anywhere in this RSPAN VLAN (there can even be several destination ports).

If the RSPAN is configured to monitor traffic sent by host A, when host A generates a frame destined for host B, the packet is copied by an Application-Specific Integrated Circuit (ASIC) of the Catalyst 6000 Policy Feature Card into a predefined RSPAN VLAN. From there, the packet is flooded to all other ports belonging to the RSPAN VLAN. All the interswitch links drawn in the figure are trunks; this is a requirement for RSPAN. The only access ports are destination ports, where the sniffers are connected (here on S4 and S5).

Note The sniffers are network IDSs.



TCP Resets and Switches

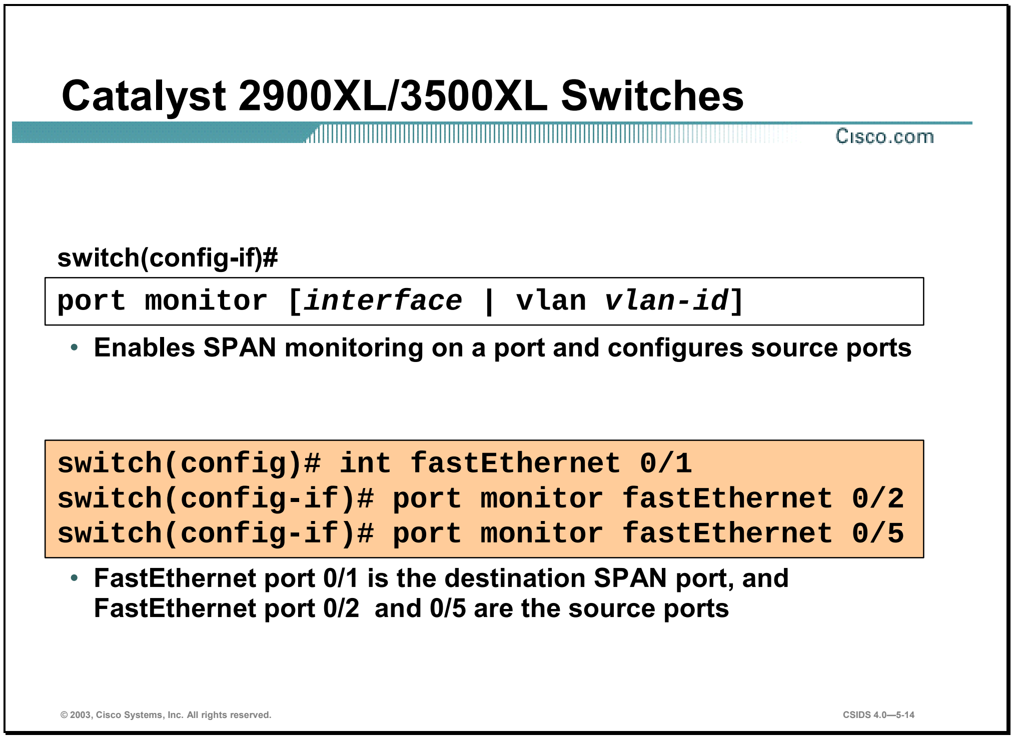
- With the exception of the 4250-XL Sensor, the Sensor appliances send the TCP reset packets from the monitoring interface.
- The Sensor's monitoring interface is connected to the switch SPAN destination port.
- Not all switches allow SPAN destination ports to receive input packets.
- Cisco IDS Sensors use a randomly generated MAC address in the TCP reset packet.

The Cisco IDS TCP reset signature action terminates a TCP session by sending TCP packets with the Reset Flag (RST) set to the offending source. The Sensor sends the TCP reset packet from the Sensor's monitoring interface. The monitoring interface is typically connected to the switch port that has been designated as the destination SPAN port. Not all switches allow the SPAN destination ports to receive incoming packets. In other words, the SPAN destination port is typically used to send mirrored packets out of the port, not to receive them in from the monitoring device. Because the Sensor sends the TCP reset packet through the monitoring interface, a switch that supports incoming packets must be used. Cisco IDS Sensors use a randomly generated MAC address in the TCP reset packet to prevent the switch (and possibly an attacker) from learning the MAC address and associating it with the Sensor.

Note The 4250-XL Sensor has a separate TCP reset interface.

Configuring SPAN for Catalyst 2900XL, 3500XL, 2950, and 3550 Traffic Capture

This section provides the switch commands used to configure the SPAN feature in Catalyst 2900XL, 3500XL, 2950 and 3550 switches.



Catalyst 2900XL/3500XL Switches

switch(config-if)#

```
port monitor [interface | vlan vlan-id]
```

- Enables SPAN monitoring on a port and configures source ports

```
switch(config)# int fastEthernet 0/1
switch(config-if)# port monitor fastEthernet 0/2
switch(config-if)# port monitor fastEthernet 0/5
```

- FastEthernet port 0/1 is the destination SPAN port, and FastEthernet port 0/2 and 0/5 are the source ports

The SPAN feature on the Catalyst 2900XL and 3500XL switches forwards both incoming and outgoing traffic of the source port(s) to another port in the same VLAN. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port (not a dynamic, trunk or multi-VLAN port). You can define any number of ports as SPAN ports, and any combination of ports can be monitored.

The **port monitor interface** configuration command is used to enable a port as a SPAN monitoring port and to configure corresponding source ports. Use the **no** form of this command to return the port to its default value.

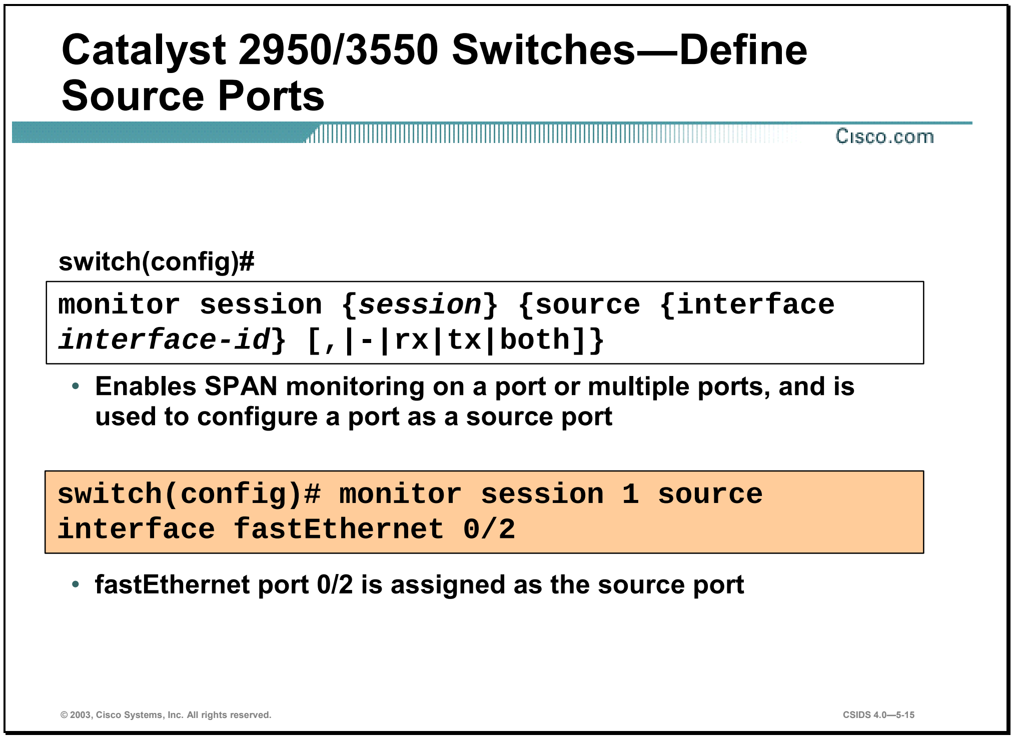
port monitor [interface | vlan vlan-id]

no port monitor [interface | vlan vlan-id]

interface	(Optional.) Module type, slot, and port number for the SPAN to be enabled. The interface specified is the port to be monitored.
vlan vlan-id	(Optional.) ID of the VLAN to be monitored. VLAN 1 is the only valid option.

Enabling port monitoring without specifying a port causes all other ports in the same VLAN to be monitored.

Entering the **port monitor vlan 1** command enables monitoring of all traffic to and from the IP address configured on VLAN 1.



Catalyst 2950/3550 Switches—Define Source Ports

switch(config)#

```
monitor session {session} {source {interface
interface-id} [,|-|rx|tx|both]}
```

- Enables SPAN monitoring on a port or multiple ports, and is used to configure a port as a source port

```
switch(config)# monitor session 1 source
interface fastEthernet 0/2
```

- fastEthernet port 0/2 is assigned as the source port

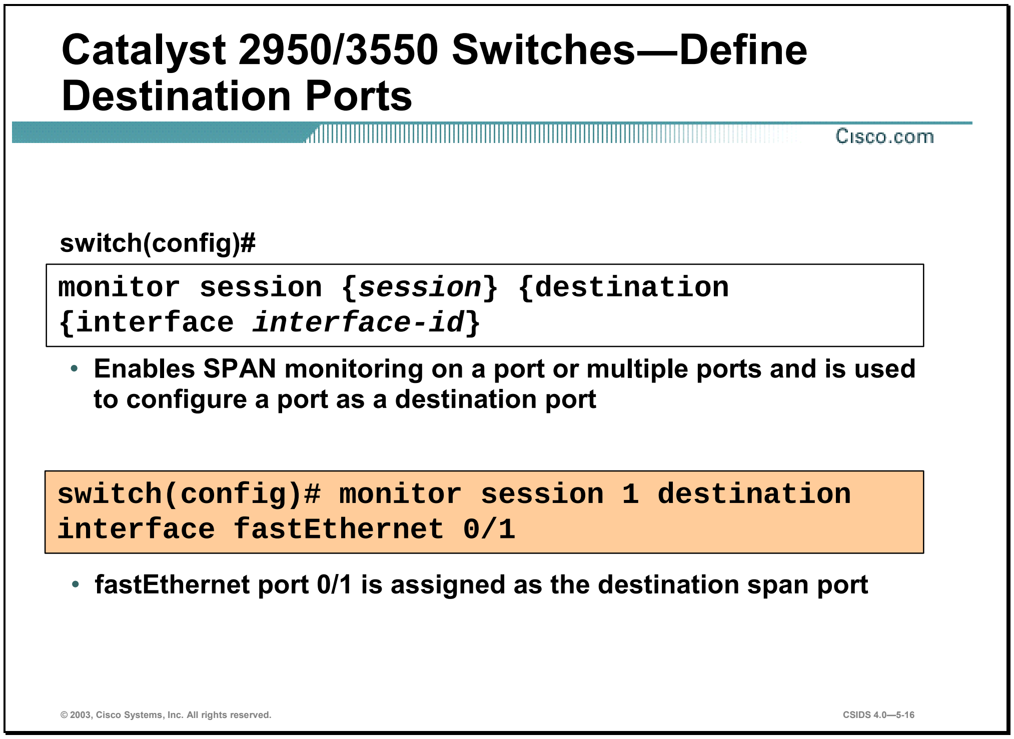
CSIDS 4.0—5-15

The **monitor session** global configuration command is used to enable SPAN monitoring on a port or multiple ports and to configure a port as a source port. Use the **no** form of this command to return the port to its default value.

monitor session {*session*} {source {interface *interface-id*} [, | - | rx | tx | both]}

no monitor session {*session*} {source {interface *interface-id*} [, | - | rx | tx | both]}

session	Number of the SPAN session. The only valid value for the 2950 is 1. For the 3550, valid values are 1 and 2.
source	Specify the SPAN source interface.
interface interface-id	Specify the interface type and number.
	(Optional.) Specify multiple ports. Enter a space after the comma.
	(Optional.) Specify a range of ports. Enter a space before and after the hyphen.
rx	(Optional.) Monitor only received traffic.
tx	(Optional.) Monitor only sent traffic.
both	(Optional.) Monitor received and sent traffic.



Catalyst 2950/3550 Switches—Define Destination Ports

switch(config)#

```
monitor session {session} {destination
{interface interface-id}
```

- Enables SPAN monitoring on a port or multiple ports and is used to configure a port as a destination port

```
switch(config)# monitor session 1 destination
interface fastEthernet 0/1
```

- fastEthernet port 0/1 is assigned as the destination span port

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—5-16

The **monitor session** global configuration command is also used to enable SPAN monitoring on a port or multiple ports and to configure a port as a destination port. Use the **no** form of this command to return the port to its default value. The syntax for the **monitor session** command is as follows:

monitor session {*session*} {destination {interface *interface-id*}}

no monitor session {*session*} {destination {interface *interface-id*}}

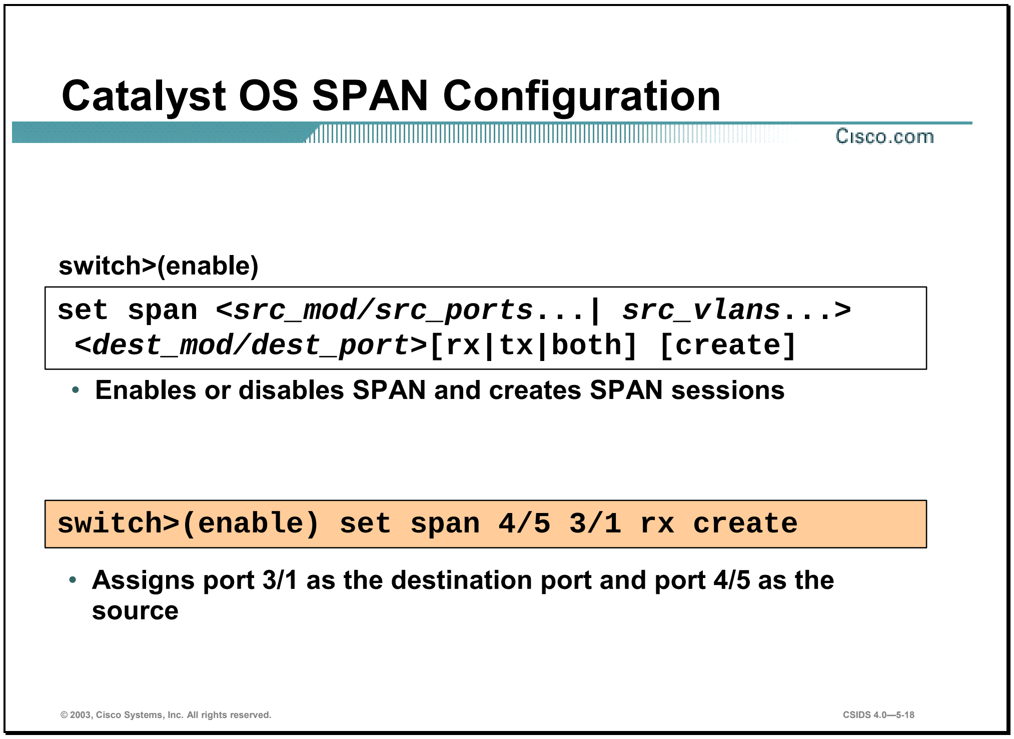
session	Number of the SPAN session. The only valid value is 1.
destination	Specify the SPAN destination interface.
interface interface-id	Specify the interface type and number.

One or more ports may be configured for a SPAN. SPAN source ports may be configured to receive incoming, outgoing or incoming and outgoing traffic.

Only **one** port may be configured as a SPAN destination port for a SPAN session. If another destination interface is added to a session that already has a destination interface configured, an error message will appear. The SPAN destination interface must be removed before changing the SPAN destination to a different interface.

Configuring SPAN for Catalyst 4000, 4500, and 6500 Traffic Capture

This section provides the commands used to configure the SPAN feature on Catalyst 4000, 4500, and 6500 switches.



Catalyst OS SPAN Configuration

Cisco.com

switch>(enable)

```
set span <src_mod/src_ports...| src_vlans...>
 <dest_mod/dest_port>[rx|tx|both] [create]
```

- Enables or disables SPAN and creates SPAN sessions

```
switch>(enable) set span 4/5 3/1 rx create
```

- Assigns port 3/1 as the destination port and port 4/5 as the source

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—5-18

The **set span** command is used to enable or disable SPAN and create SPAN sessions. The syntax for the **set span** command is as follows:

set span {*src_mod/src_ports…* | *src_vlans…* | sc0} {*dest_mod/dest_port*} [rx | tx | both] [inpkts{enable | disable}] [learning {enable | disable}] [multicast {enable | disable}] [filter *vlans...*] [create]

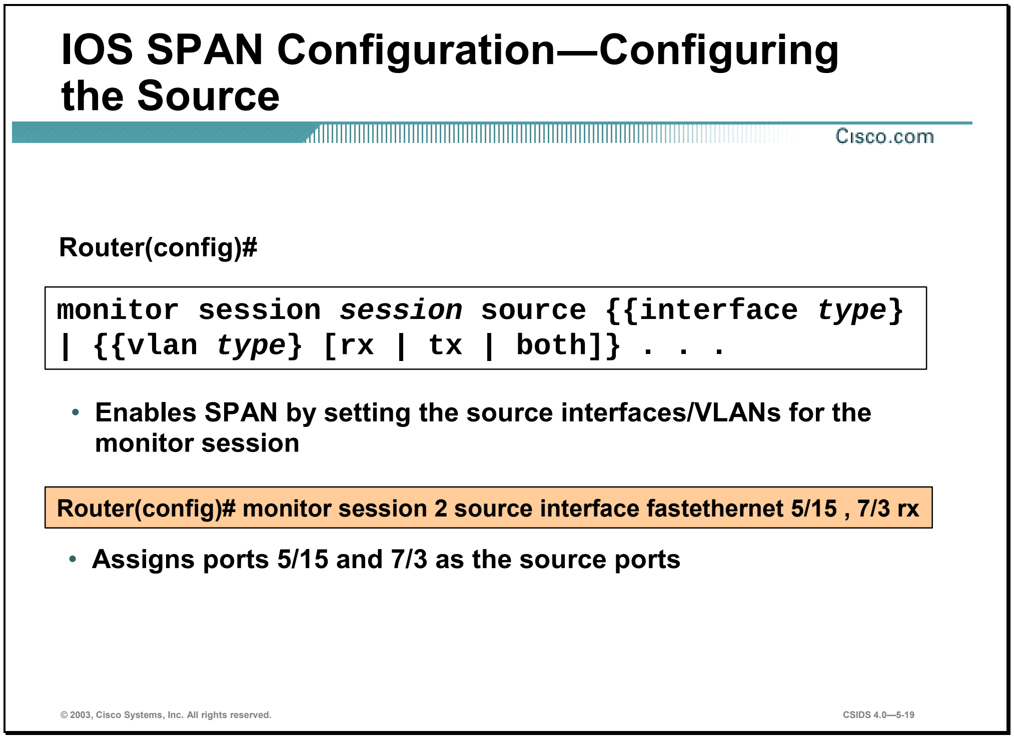
set span disable [*dest_mod/dest_port* | all]

src_mod	Monitored module (SPAN source).
src_ports…	Monitored ports (SPAN source).
src_vlans…	Monitored VLANs (SPAN source).
sc0	Keyword to specify the inbound port is a valid source.
rx	(Optional.) Keyword to specify that information received at the source (Ingress SPAN) is monitored.
tx	(Optional.) Keyword to specify that information transmitted from the source (Egress SPAN) is monitored.
both	(Optional.) Keyword to specify that information transmitted from the source (Ingress SPAN) and received (Egress SPAN) at the source is monitored.

inpkts enable	(Optional.) Keywords to enable the receiving of normal inbound traffic on the SPAN destination port.
inpkts disable	(Optional.) Keywords to disable the receiving of normal inbound traffic on the SPAN destination port.
learning enable	(Optional.) Keywords to enable learning for the SPAN destination port.
learning disable	(Optional.) Keywords to disable learning for the SPAN destination port.
multicast enable	(Optional.) Keywords to enable monitoring multicast traffic (egress traffic only).
multicast disable	(Optional.) Keywords to disable monitoring multicast traffic (egress traffic only).
filter *vlans*	(Optional.) Keyword and variable to monitor traffic on selected VLANs on source trunk ports.
create	(Optional.) Keyword to create a SPAN port.
disable	Keyword to disable SPAN.
dest_mod	(Optional.) Monitoring module (SPAN destination).
dest_port	(Optional.) Monitoring port (SPAN destination).
all	(Optional.) Keyword to disable all SPAN sessions.

If you do not specify the keyword create and you have only one session, the session is overwritten. If a matching destination port exists, the particular session is overwritten, with or without specifying create. If you specify the keyword create and there is no matching destination port, the session is created.

Note Command syntax in this section applies to the Catalyst 6500 switches. For command syntax for the other switch models, see their respective Command References.



IOS SPAN Configuration—Configuring the Source

Router(config)#

```
monitor session session source {{interface type}
| {{vlan type} [rx | tx | both]} . . .
```

- **Enables SPAN by setting the source interfaces/VLANs for the monitor session**

Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx

- **Assigns ports 5/15 and 7/3 as the source ports**

A SPAN session is an association of a set of source ports and source VLANs with one or more destination ports. You can use the **monitor session source** command for the following:

- To start a new SPAN session
- To add or delete interfaces or VLANs to or from an existing SPAN session

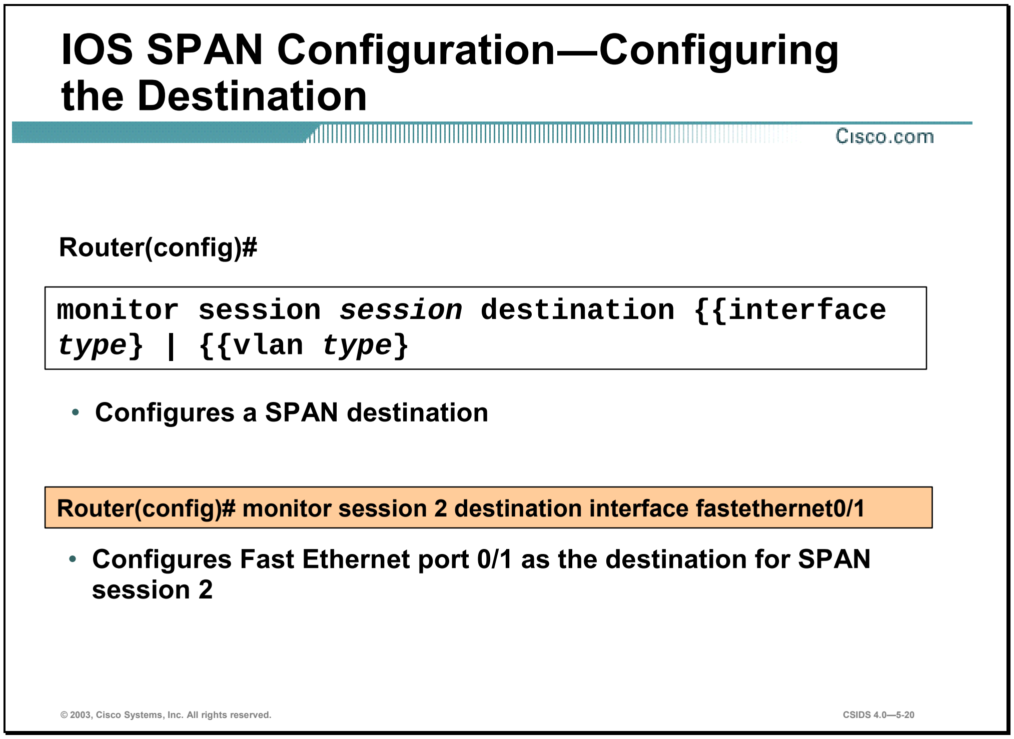
Use the **no** form of this command for the following:

- To remove one or more sources or destination interfaces from the SPAN session
- To remove a source VLAN from the SPAN session
- To delete a SPAN session

The syntax for the **monitor session** command is as follows:

monitor session ***session*** **source {{interface** ***type*****} | {vlan** ***type*****} [rx | tx | both]} . . .**

session	Number of the SPAN session; valid values are from 1 to 66.
source	SPAN source.
interface *type*	Interface type.
vlan *type*	VLAN ID.
rx	(Optional.) Monitor received traffic only.
tx	(Optional.) Monitor transmitted traffic only.
both	(Optional.) Monitor received and monitor transmitted traffic.



IOS SPAN Configuration—Configuring the Destination

Cisco.com

Router(config)#

```
monitor session session destination {{interface
type} | {{vlan type}
```

- Configures a SPAN destination

```
Router(config)# monitor session 2 destination interface fastethernet0/1
```

- Configures Fast Ethernet port 0/1 as the destination for SPAN session 2

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—5-20

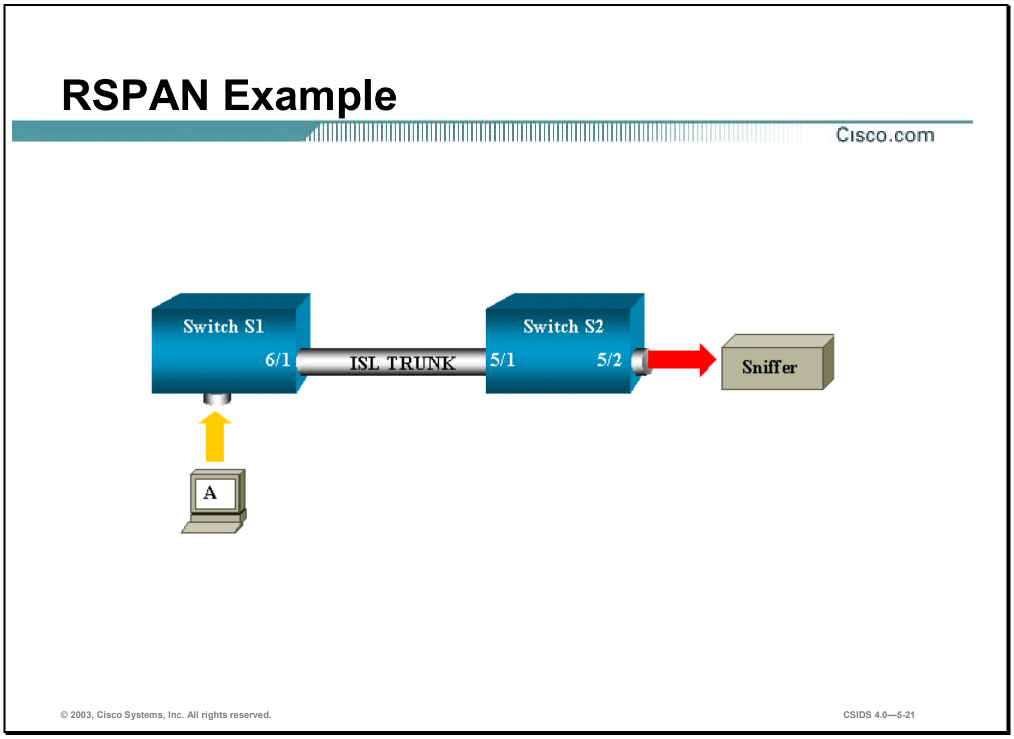
To complete the SPAN configuration, configure the SPAN destination with the **monitor session destination** command. The syntax for the **monitor session destination** command is as follows:

monitor session ***session*** **destination {{interface** ***type***} | {**vlan** ***type***}}

session	Number of the SPAN session; valid values are from 1 to 66.
destination	SPAN destination interface.
interface ***type***	Interface type. The type can represent a single interface (ethernet_type slot/port), a list of comma-separated interfaces, a range of interfaces using a hyphen, or a combination of these options.
vlan ***type***	VLAN ID. The type can represent a single VLAN, a range of VLANs using a hyphen, or combination of these options.

Configuring RSPAN for Catalyst 4000 and 6500 Traffic Capture

This section provides the commands used to configure the RSPAN feature on Catalyst 4000 and 6500 switches.



RSPAN Example

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

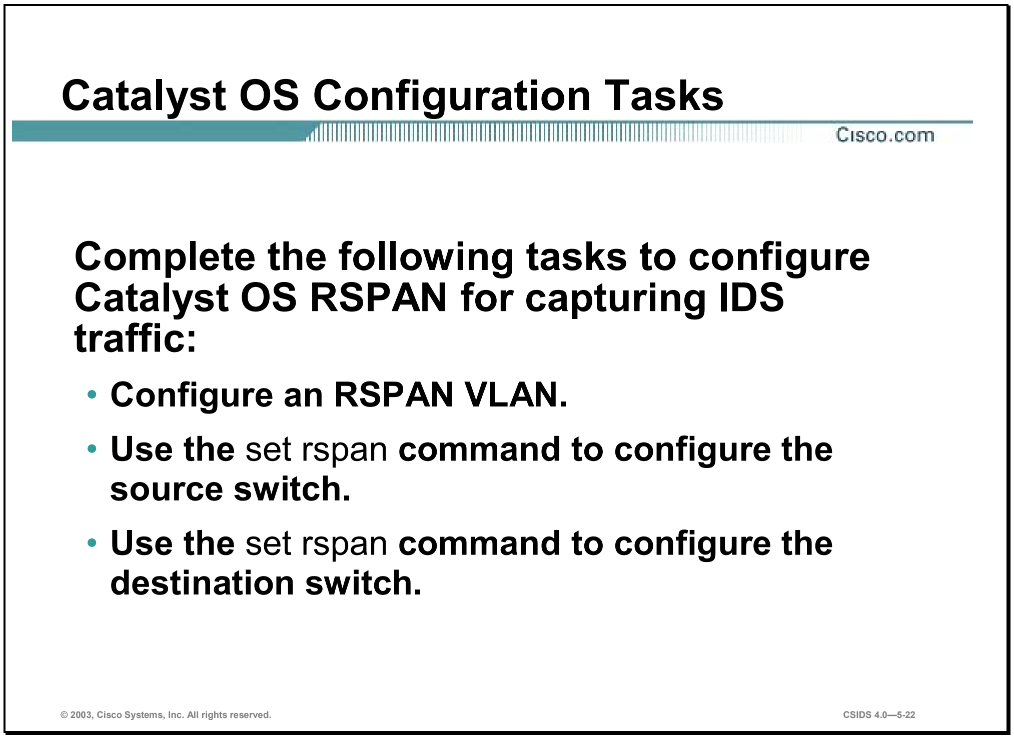
CSIDS 4.0—5-21

RSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.

The RSPAN traffic from the source ports or source VLANs is switched to the RSPAN VLAN and then forwarded to destination ports, which are in the RSPAN VLAN. The sources (ports or VLANs) in an RSPAN session can be different on different source switches but must be the same for all sources on each RSPAN source switch. Each RSPAN source switch must have either ports or VLANs as RSPAN sources.

In the figure, S1 and S2 are two Catalyst 6500 switches. A dedicated RSPAN VLAN can be configured to monitor source ports or VLANS on switch S1 from a destination port on switch S2. All inter-switch links must be trunks to carry the RSPAN VLAN. Additional configuration is required that is syntactically similar to configuring a standard SPAN session.

Note The Catalyst 4000 does not support RSPAN in IOS. The Catalyst 6500 supports RSPAN in both Catalyst OS and IOS.



Catalyst OS Configuration Tasks

Cisco.com

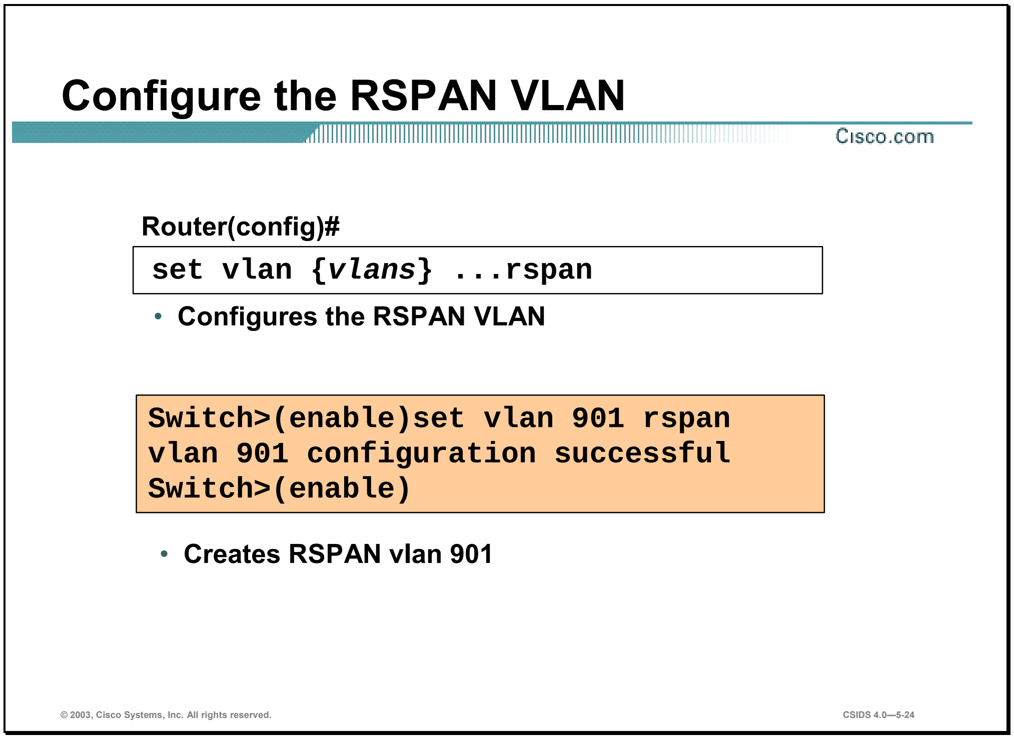
Complete the following tasks to configure Catalyst OS RSPAN for capturing IDS traffic:

- **Configure an RSPAN VLAN.**
- **Use the** set rspan **command to configure the source switch.**
- **Use the** set rspan **command to configure the destination switch.**

CSIDS 4.0—5-22

The tasks to capture traffic using Remote Span (RSPAN) are as follows:

- Configure an RSPAN VLAN. This VLAN must be configured on all source, destination, and intermediate switches and be unique across the entire switched network.
- Use the **set rspan** command with the **source** keyword to configure the source switches. This must be done on each source switch participating in RSPAN.
- Use the **set rspan** command with the **destination** keyword to configure the destination switches. This must be done on each destination switch participating in RSPAN.



Configure the RSPAN VLAN

Router(config)#

```
set vlan {vlans} ...rspan
```

- **Configures the RSPAN VLAN**

```
Switch>(enable)set vlan 901 rspan
vlan 901 configuration successful
Switch>(enable)
```

- **Creates RSPAN vlan 901**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—5-24

Use the **set vlan** command for the following:

- To group ports into a VLAN
- To set the private VLAN type
- To map or unmap VLANs to or from an instance
- To specify an 802.1x port to a VLAN

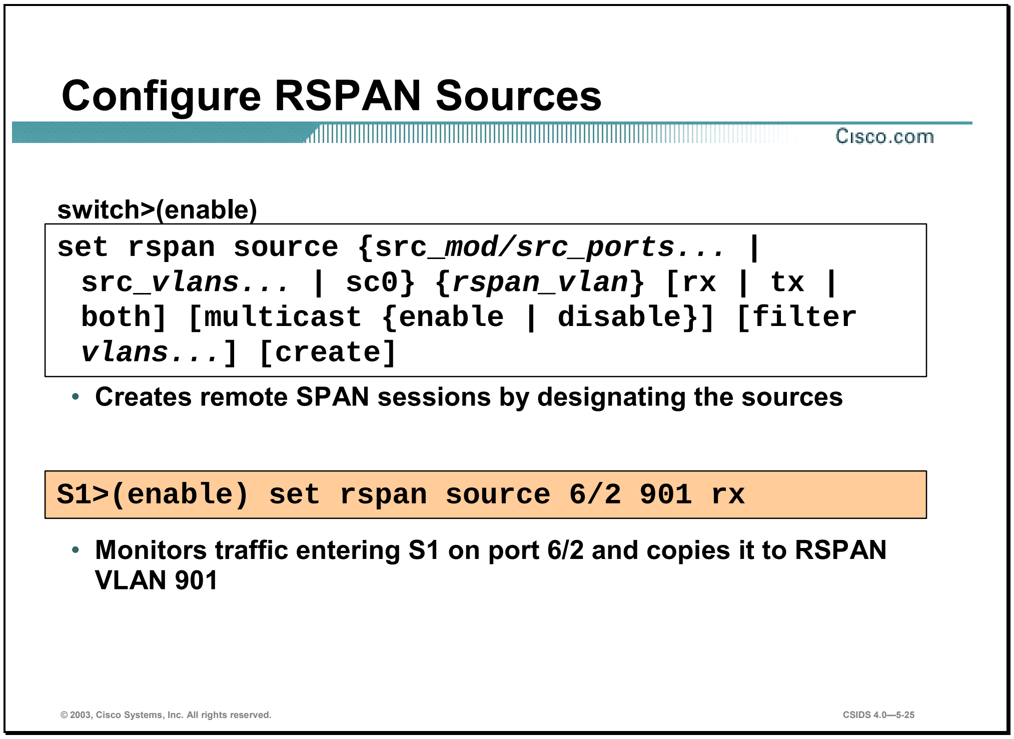
The syntax for the **set vlan** command is as follows:

set vlan {*vlans*} {*mod*/*ports*}

set vlan {*vlans*} rspan

vlans	Number identifying the VLAN; valid values are from 1 to 1000 and from 1025 to 4094.
mod/ports	Number of the module and ports on the module belonging to the VLAN.
rspan	(Optional.) Creates a VLAN for a remote SPAN.

Note Command syntax in this section applies to the Catalyst 6500 switches. For command syntax for the other switch models, see their respective Command References.



Configure RSPAN Sources

Cisco.com

switch>(enable)

```
set rspan source {src_mod/src_ports... |
 src_vlans... | sc0} {rspan_vlan} [rx | tx |
 both] [multicast {enable | disable}] [filter
 vlans...] [create]
```

- Creates remote SPAN sessions by designating the sources

```
S1>(enable) set rspan source 6/2 901 rx
```

- Monitors traffic entering S1 on port 6/2 and copies it to RSPAN VLAN 901

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—5-25

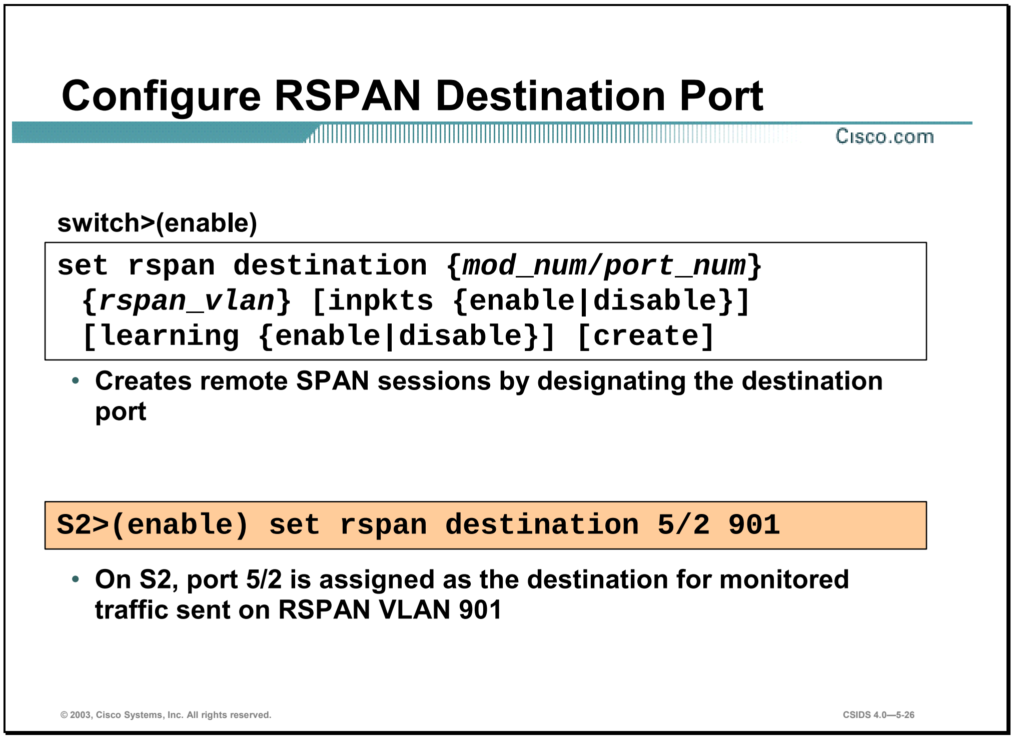
The **set rspan source** command is used to create RSPAN source sessions. The syntax for the **set rspan source** command is as follows:

set rspan disable source [*rspan_vlan* | all]

set rspan source {*src_mod/src_ports...* |*src_vlans...* | sc0} {*rspan_vlan*} [rx | tx | both] [multicast {enable | disable}] [filter *vlans...*] [create]

disable source	Keywords to disable remote SPAN source information.
rspan_vlan	(Optional.) RSPAN VLAN.
all	(Optional.) Keyword to disable all RSPAN source or destination sessions.
disable destination	Keywords to disable RSPAN destination information.
mod/port	(Optional.) RSPAN destination port.
src_mod/src_ports	Monitored ports (RSPAN source).
src_vlans	Monitored VLANs (RSPAN source).
sc0	Keyword to specify the inbound port is a valid source.
rx	(Optional.) Keyword to specify that information received at the source (Ingress SPAN) is monitored.
tx	(Optional.) Keyword to specify that information transmitted from the source (Egress SPAN) is monitored.
both	(Optional.) Keyword to specify that information transmitted from the source (Ingress SPAN) and received (Egress SPAN) at the source is monitored.
multicast enable	(Optional.) Keywords to enable monitoring multicast traffic (egress traffic only).
multicast disable	(Optional.) Keywords to disable monitoring multicast traffic (egress traffic only).

filter *vlans*	(Optional.) Keywords to monitor traffic on selected VLANs on source trunk ports.
create	(Optional.) Keyword to create a new RSPAN session instead of overwriting the previous SPAN session.



Configure RSPAN Destination Port

Cisco.com

switch>(enable)

```
set rspan destination {mod_num/port_num}
 {rspan_vlan} [inpkts {enable|disable}]
 [learning {enable|disable}] [create]
```

- Creates remote SPAN sessions by designating the destination port

```
S2>(enable) set rspan destination 5/2 901
```

- On S2, port 5/2 is assigned as the destination for monitored traffic sent on RSPAN VLAN 901

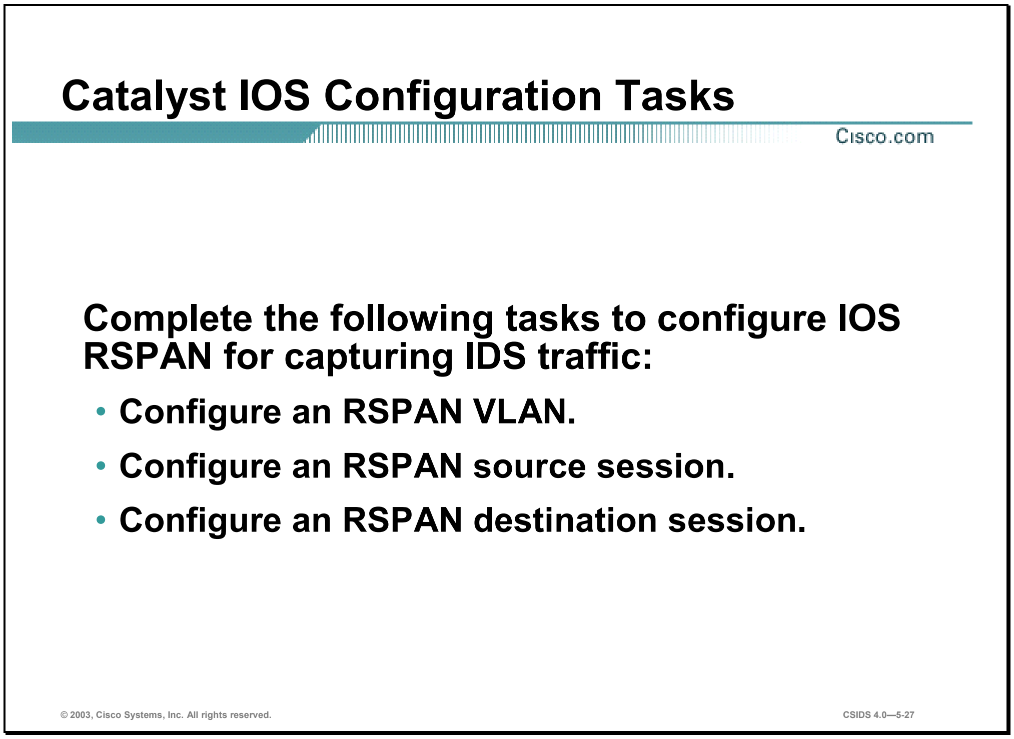
CSIDS 4.0—5-26

The set rspan **destination** command is used to create RSPAN destination sessions. The syntax for the **set rspan destination** command is as follows:

set rpsan disable destination [*mod/port* | all]

set rspan destination {*mod/port*} {*rspan_vlan*} [inpkts {enable | disable}] [learning {enable | disable}] [create]

disable destination	Keywords to disable RSPAN destination information.
mod/port	(Optional.) RSPAN destination port.
all	(Optional.) Keyword to disable all RSPAN source or destination sessions.
rspan_vlan	(Optional.) RSPAN VLAN.
inpkts enable	(Optional.) Keywords to allow the RSPAN destination port to receive normal ingress traffic (from the network to the bus) while forwarding the RSPAN traffic.
inpkts disable	(Optional.) Keywords to disable the receiving of normal inbound traffic on the RSPAN destination port.
learning enable	(Optional.) Keywords to enable learning for the RSPAN destination port.
learning disable	(Optional.) Keywords to disable learning for the RSPAN destination port.
create	(Optional.) Keyword to create a new RSPAN session instead of overwriting the previous SPAN session.



Catalyst IOS Configuration Tasks

Cisco.com

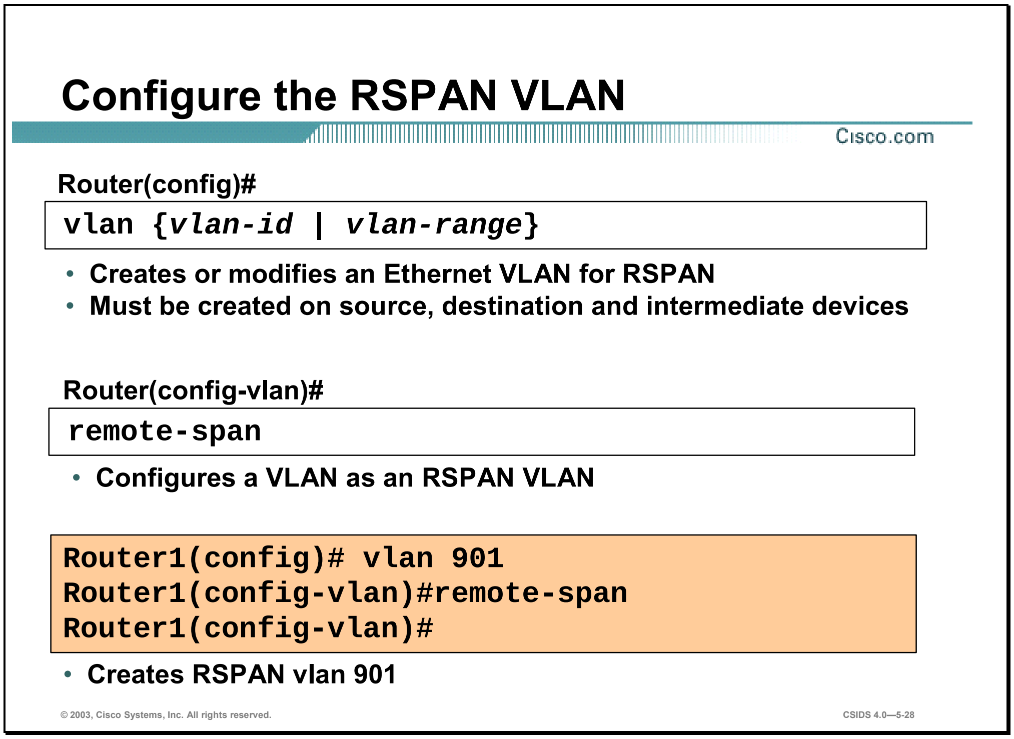
Complete the following tasks to configure IOS RSPAN for capturing IDS traffic:

- Configure an RSPAN VLAN.
- Configure an RSPAN source session.
- Configure an RSPAN destination session.

CSIDS 4.0—5-27

The following tasks must be completed to capture traffic using Remote Span (RSPAN) with IOS software:

- Configure an RSPAN VLAN on the source switch, destination switch, and any intermediate switches.
- Configure an RSPAN source session on each source switch.
- Configure an RSPAN destination session on the destination switch.



Configure the RSPAN VLAN

Cisco.com

Router(config)#

```
vlan {vlan-id | vlan-range}
```

- Creates or modifies an Ethernet VLAN for RSPAN
- Must be created on source, destination and intermediate devices

Router(config-vlan)#

```
remote-span
```

- Configures a VLAN as an RSPAN VLAN

```
Router1(config)# vlan 901
Router1(config-vlan)#remote-span
Router1(config-vlan)#
```

- Creates RSPAN vlan 901

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—5-28

Use the **vlan** command to add a VLAN and enter config-VLAN submode. Use the **no** form of this command to delete the VLAN. The syntax for the **vlan** command is as follows:

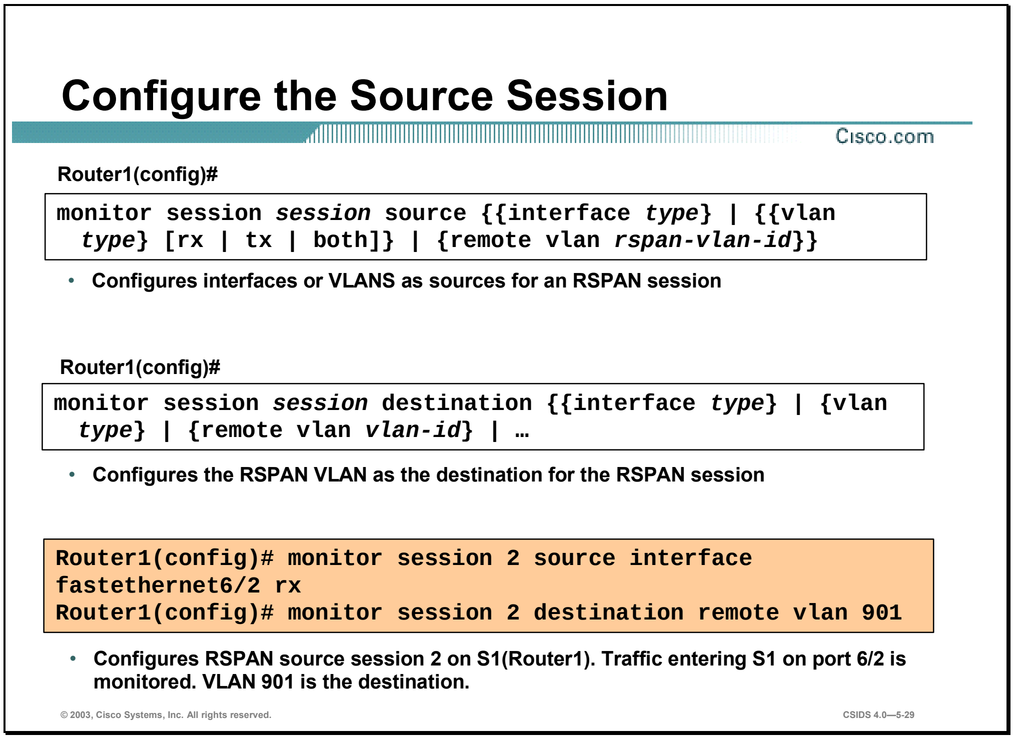
vlan {*vlan-id* | *vlan-range*}

vlan-id	Number of the VLAN. If your system is configured with a Supervisor Engine 1, valid values are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values are from 1 to 4094.
vlan-range	Range of configured VLANs. If your system is configured with a Supervisor Engine 1, valid values are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values are from 1 to 4094.

Note Extended range VLANs are not supported on systems configured with a Supervisor Engine 1. VLAN 1 parameters are factory configured and cannot be changed.

Use the **remote-span** command to configure a VLAN as an RSPAN VLAN. Use the **no** form of this command to remove the RSPAN designation. The syntax for the **remote-span** command is as follows:

remote-span



Configure the Source Session

Router1(config)#

```
monitor session session source {{interface type} | {{vlan
  type} [rx | tx | both]} | {remote vlan rspan-vlan-id}}
```

- Configures interfaces or VLANS as sources for an RSPAN session

Router1(config)#

```
monitor session session destination {{interface type} | {vlan
  type} | {remote vlan vlan-id} | …
```

- Configures the RSPAN VLAN as the destination for the RSPAN session

```
Router1(config)# monitor session 2 source interface
fastethernet6/2 rx
Router1(config)# monitor session 2 destination remote vlan 901
```

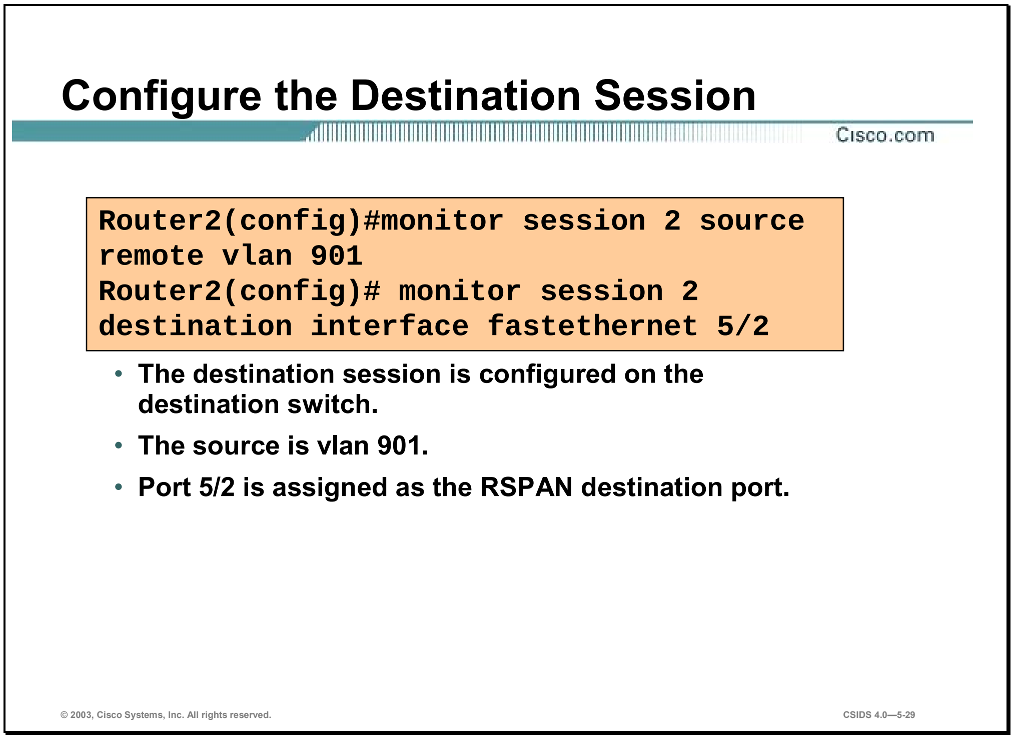
- Configures RSPAN source session 2 on S1(Router1). Traffic entering S1 on port 6/2 is monitored. VLAN 901 is the destination.

RSPAN consists of an RSPAN VLAN, an RSPAN source session, and an RSPAN destination session. You separately configure RSPAN source sessions and destination sessions on different network devices. Source sessions are configured on source switches and destination sessions are configured on destination switches. To configure an RSPAN source session, associate a set of source ports and VLANs with an RSPAN VLAN. This requires the use of the **monitor session** command as follows:

- Use the **monitor session** command with the **source** keyword to configure an RSPAN source for the session.

- Use the **monitor session** command with the **destination** keyword to configure the RSPAN VLAN as the destination for the session.

Note Use the same session number for configuring the source and the destination VLAN.



Configure the Destination Session

```
Router2(config)#monitor session 2 source
remote vlan 901
Router2(config)# monitor session 2
destination interface fastethernet 5/2
```

- **The destination session is configured on the destination switch.**
- **The source is vlan 901.**
- **Port 5/2 is assigned as the RSPAN destination port.**

CSIDS 4.0—5-29

To configure an RSPAN destination session, configure the RSPAN VLAN as the source and a port as the destination. This requires the use of the **monitor session** command as follows:

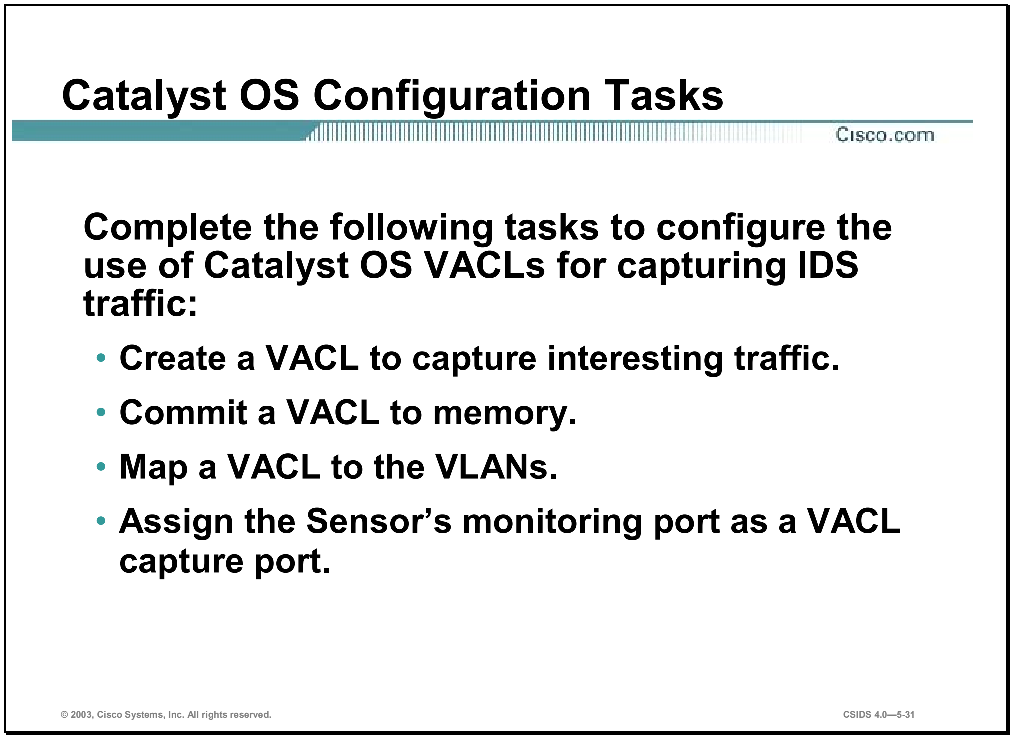
- Use the **monitor session** command with the **source** keyword to configure the RSPAN VLAN as the source for the session.

- Use the **monitor session** command with the **destination** keyword to configure a destination port for the session.

Note Use the same session number for configuring the source RSPAN VLAN and the destination port.

Configuring VACLs for Catalyst 6500 Traffic Capture

This section discusses the configuration tasks and commands used to configure the Catalyst 6500 switch capture feature.



Catalyst OS Configuration Tasks

Cisco.com

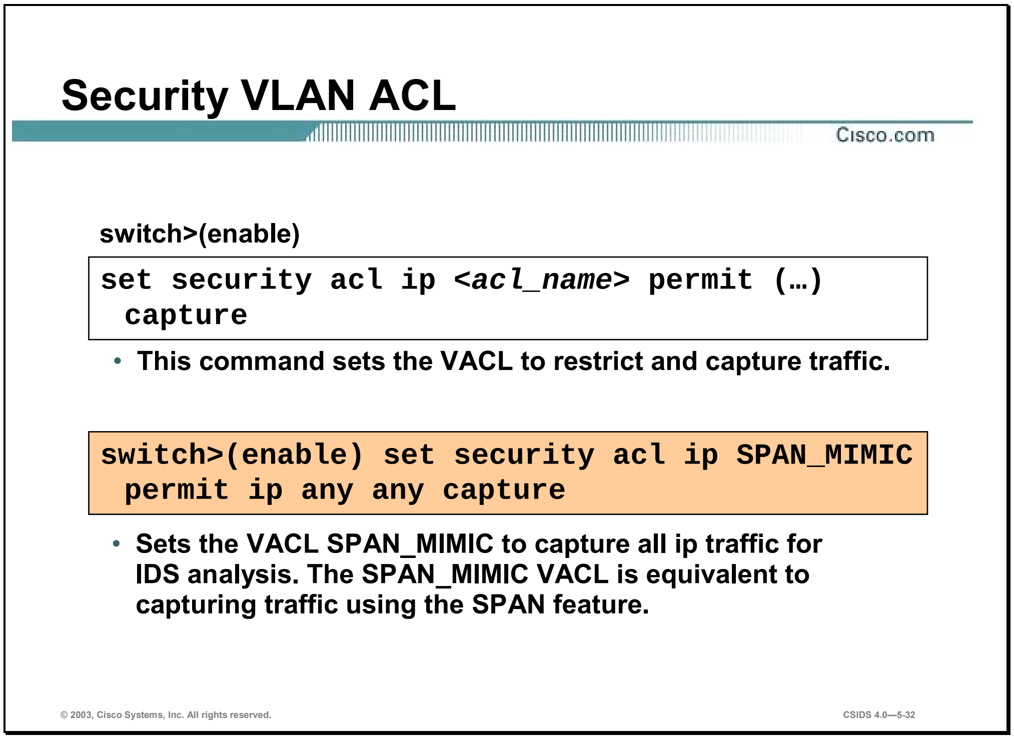
Complete the following tasks to configure the use of Catalyst OS VACLs for capturing IDS traffic:

- **Create a VACL to capture interesting traffic.**
- **Commit a VACL to memory.**
- **Map a VACL to the VLANs.**
- **Assign the Sensor's monitoring port as a VACL capture port.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—5-31

The tasks to capture traffic using VLAN Access Control Lists (VACLs) on a Catalyst 6500 switch running Catalyst OS are as follows:

- Create the VACL to capture interesting traffic.
- Commit the VACL to memory.
- MAP the VACL to VLANs.
- Assign the Sensor's monitoring port as the VACL capture port.



Security VLAN ACL

Cisco.com

switch>(enable)

```
set security acl ip <acl_name> permit (…)
 capture
```

- **This command sets the VACL to restrict and capture traffic.**

```
switch>(enable) set security acl ip SPAN_MIMIC
 permit ip any any capture
```

- **Sets the VACL SPAN_MIMIC to capture all ip traffic for IDS analysis. The SPAN_MIMIC VACL is equivalent to capturing traffic using the SPAN feature.**

CSIDS 4.0—5-32

The **set security acl ip** command is used to create VLAN ACLs to capture IP traffic for Intrusion Detection analysis. The **capture** keyword is required to capture traffic to the Sensor's monitoring port. Use the **clear security acl** command to remove specific access control entries (ACEs) or all ACEs from a VACL.

Note VACLs have an implicit **deny feature** at the end of the list. All traffic not matching the VACL will be dropped as a result.

The syntax for the **set security acl ip** command is as follows:

set security acl ip ***acl_name*** **[permit | deny]** ***src_ip_spec***

set security acl ip ***acl_name*** **[permit | deny] [ip]** ***src_ip_spec dest_ip_spec*** **[fragment] [capture]**

set security acl ip ***acl_name*****[permit | deny] [icmp | 1]** ***src_ip_spec dest_ip_spec*** **[*****icmp_type*****] [*****icmp_code*****] | [*****icmp_message*****] [capture]**

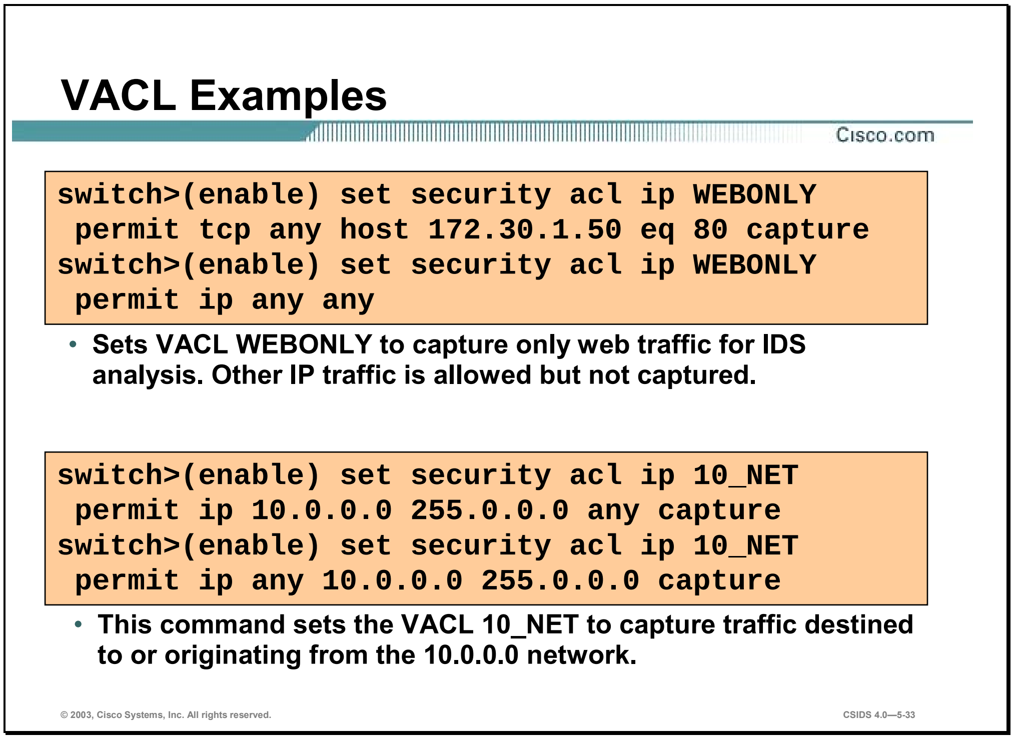
set security acl ip ***acl_name*** **[permit | deny] [tcp | 6]** ***src_ip_spec*** **[*****operator port*** **[*****port*****]]** ***dest_ip_spec*** **[*****operator port*** **[*****port*****]] [established] [capture]**

set security acl ip ***acl_name*** **[permit | deny] [udp | 17]** ***src_ip_spec*** **[*****operator port*** **[*****port*****]]** ***dest_ip_spec*** **[*****operator port*** **[*****port*****]] [capture]**

acl_name	Unique name that identifies the lists to which the entry belongs.
permit	Keyword to allow traffic from the source IP address.
deny	Keyword to deny traffic from the source IP address.
src_ip_spec	Source IP address and the source mask.
ip	(Optional.) Keyword or number to match any IP packets.

dest_ip_spec	Destination IP address and the destination mask.
fragment	(Optional.) Filters IP traffic that carries fragments.
capture	Keyword to specify packets are switched normally and captured. Permit must be enabled.
icmp | 1	(Optional.) Keyword or number to match ICMP packets.
icmp-type	(Optional.) ICMP message type name or a number.
icmp-code	(Optional.) ICMP message code name or a number.
icmp-message	ICMP message type name or ICMP message type and code name.
tcp | 6	(Optional.) Keyword or number to match TCP packets.
operator	(Optional.) Operands—Valid values include: lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).
port	(Optional.) Number or name of a TCP or UDP port. Valid port numbers are from 0–65535.
established	(Optional.) Keyword to specify an established connection. Used only for TCP protocol.
udp | 17	(Optional.) Keyword or number to match UDP packets.

The order of ACEs in a VACL is important. Each packet entering a mapped VLAN is checked against the first ACE in the VACL. If a match occurs, the appropriate action is taken to deny or permit (and optionally capture) the packet; further processing of the VACL ceases. If there is no match, the packet is applied against the next ACE in the list. If no ACEs match, the packet is implicitly denied (dropped).



VACL Examples

```
switch>(enable) set security acl ip WEBONLY
 permit tcp any host 172.30.1.50 eq 80 capture
switch>(enable) set security acl ip WEBONLY
 permit ip any any
```

- **Sets VACL WEBONLY to capture only web traffic for IDS analysis. Other IP traffic is allowed but not captured.**

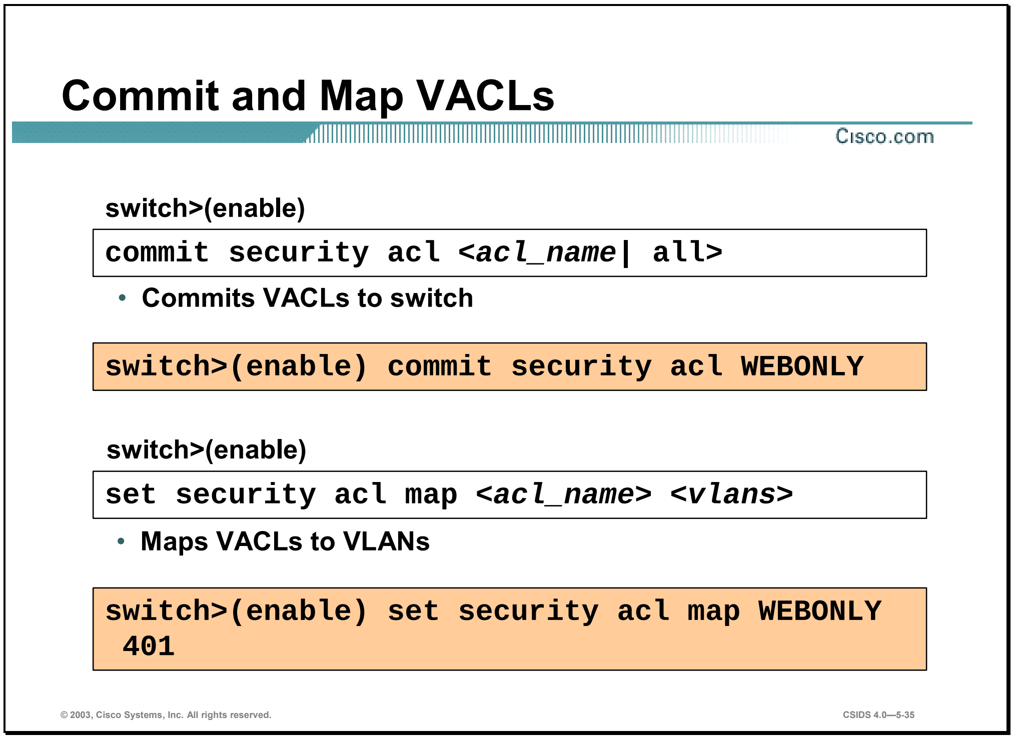
```
switch>(enable) set security acl ip 10_NET
 permit ip 10.0.0.0 255.0.0.0 any capture
switch>(enable) set security acl ip 10_NET
 permit ip any 10.0.0.0 255.0.0.0 capture
```

- **This command sets the VACL 10_NET to capture traffic destined to or originating from the 10.0.0.0 network.**

CSIDS 4.0—5-33

The WEB_ONLY VACL captures traffic destined for TCP port 80 (HTTP) for Intrusion Detection analysis. All other IP traffic is permitted, but is not captured.

The 10_NET VACL captures any IP traffic destined for or originating from the 10.0.0.0 network for Intrusion Detection analysis.



Commit and Map VACLs

switch>(enable)

```
commit security acl <acl_name| all>
```

- Commits VACLs to switch

```
switch>(enable) commit security acl WEBONLY
```

switch>(enable)

```
set security acl map <acl_name> <vlans>
```

- Maps VACLs to VLANs

```
switch>(enable) set security acl map WEBONLY
 401
```

CSIDS 4.0—5-35

The **commit security acl** command is used to save all Access Control Entries (ACEs) or a specific ACE. The syntax for the **commit security acl** command is as follows:

commit security acl ***acl_name*** | **all**

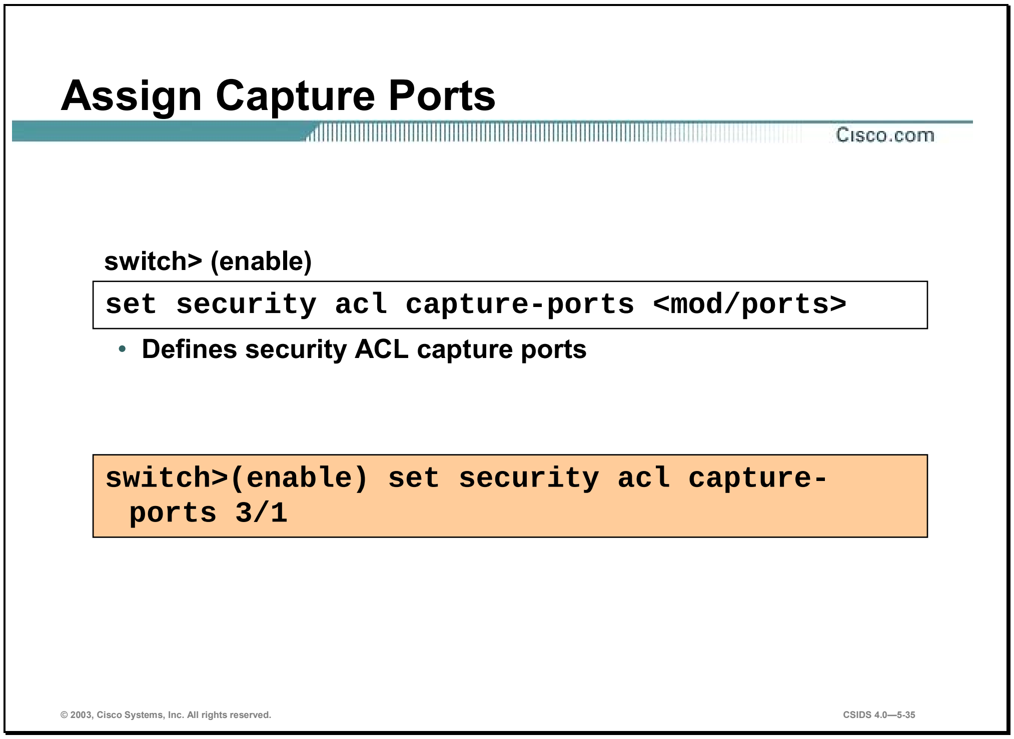
acl_name	Name that identifies the VACL whose ACEs are to be committed
all	Keyword to commit ACEs for all the ACLs

Note All changes to ACLs are stored temporarily in an edit buffer. You must use the **commit** command to commit all ACEs to NVRAM. Committed ACLs with no ACEs are deleted.

The **set security acl map** command is used to map an existing VACL to a VLAN. The **clear security acl map** command is used to remove VACL-to-VLAN mapping. The syntax for the **set security acl map** command is as follows:

set security acl map ***acl_name vlan***

acl_name	Unique name that identifies the list to which the entry belongs
vlan	Number of the VLAN to be mapped to the VACL



Assign Capture Ports

switch> (enable)

```
set security acl capture-ports <mod/ports>
```

- **Defines security ACL capture ports**

```
switch>(enable) set security acl capture-
 ports 3/1
```

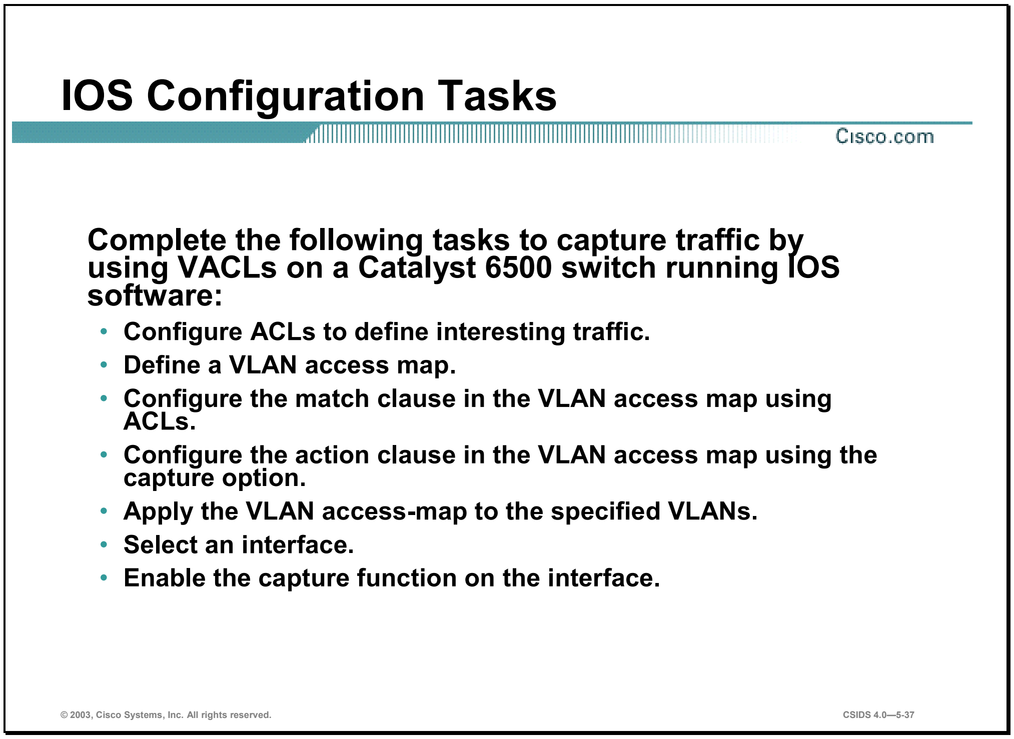
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—5-35

The **set security acl capture-ports** command is used to set the destination ports that receive the captured traffic specified in the **set security acl ip** command. The **clear security acl capture-ports** command is used to remove a port from the capture port list. The syntax for the **set security acl capture-ports** command is as follows:

set security acl capture-ports <*mod/ports*>[,<*mod/ports*>…]

mod/ports	Module and port number



IOS Configuration Tasks

Cisco.com

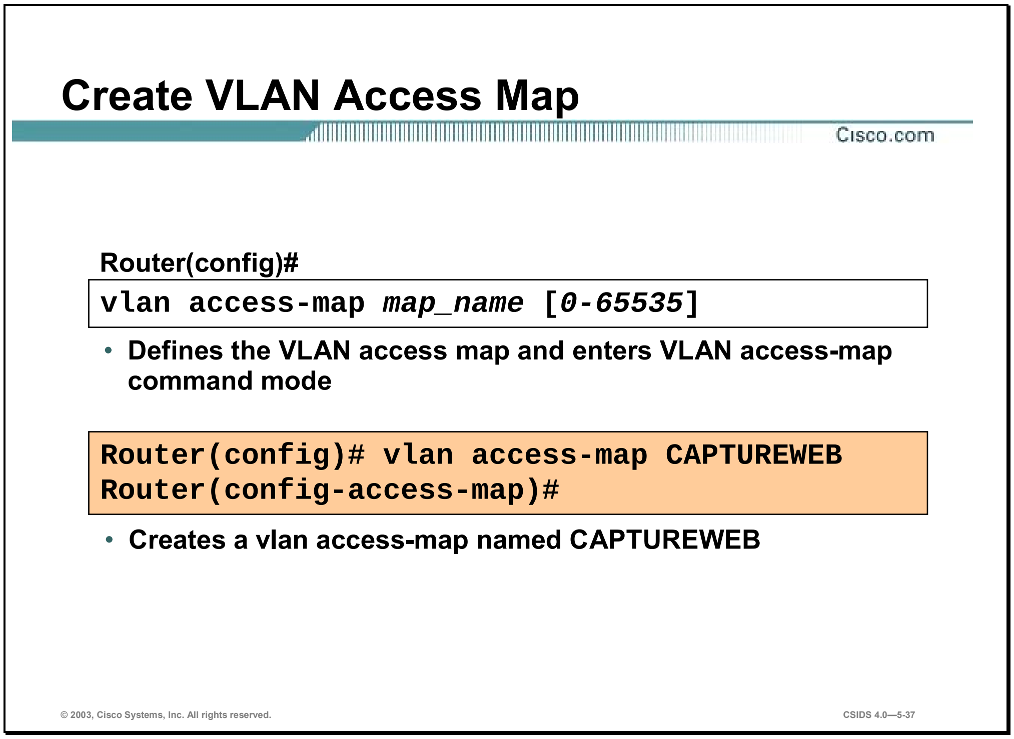
Complete the following tasks to capture traffic by using VACLs on a Catalyst 6500 switch running IOS software:

- Configure ACLs to define interesting traffic.
- Define a VLAN access map.
- Configure the match clause in the VLAN access map using ACLs.
- Configure the action clause in the VLAN access map using the capture option.
- Apply the VLAN access-map to the specified VLANs.
- Select an interface.
- Enable the capture function on the interface.

CSIDS 4.0—5-37

The tasks to capture traffic using VLAN Access Control Lists (VACLs) on a Catalyst 6500 switch running IOS are as follows:

- Configure ACLs to define interesting traffic.
- Define a VLAN access map.
- Configure the match clause in the VLAN access map using ACLs.
- Configure the action clause in the VLAN access map using the capture option.
- Apply the VLAN access-map to the specified VLANs.
- Select an interface.
- Enable the capture function on the interface.



Create VLAN Access Map

Router(config)#

```
vlan access-map map_name [0-65535]
```

- Defines the VLAN access map and enters VLAN access-map command mode

```
Router(config)# vlan access-map CAPTUREWEB
Router(config-access-map)#
```

- Creates a vlan access-map named CAPTUREWEB

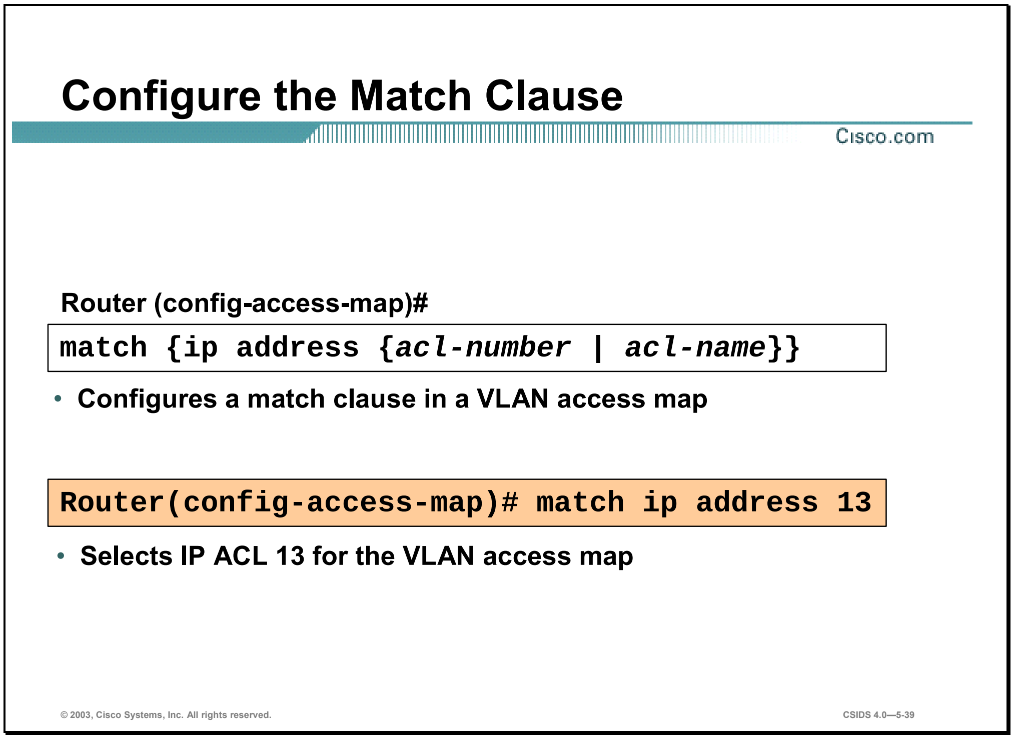
CSIDS 4.0—5-37

A VLAN access map consists of one or more map sequences, each sequence with a match clause and an action clause. The match clause specifies an ACL for traffic filtering. The action clause specifies the action to be taken when a match occurs. You can specify only one match clause and one action clause per map sequence.

You can use the **vlan access-map** command to create a VLAN access map or enter VLAN access-map command mode. Use the **no** form of this command to remove a mapping sequence or the entire map. The syntax for the **vlan access- map** command is as follows:

vlan access-map ***name*** **[*seq#*]**

name	VLAN access-map tag.
seq#	(Optional.) Map sequence number. Valid values are 0 to 65535.



Configure the Match Clause

Router (config-access-map)#

```
match {ip address {acl-number | acl-name}}
```

- **Configures a match clause in a VLAN access map**

```
Router(config-access-map)# match ip address 13
```

- **Selects IP ACL 13 for the VLAN access map**

CSIDS 4.0—5-39

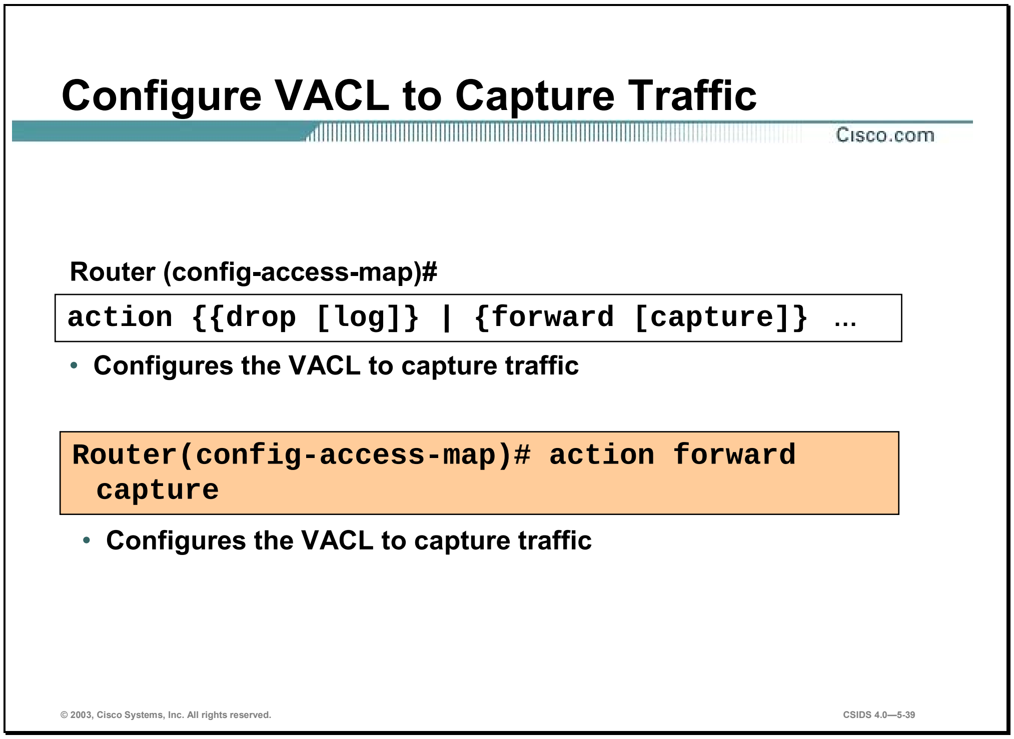
While in VLAN access-map configuration mode, use the **match** command to specify the match clause by selecting an ACL for a VLAN access-map sequence. The match clause specifies the ACLs for traffic filtering.

Use the **no** form of this command to remove the match clause. The syntax for the **match** command is as follows:

match {ip address {*acl-number* | *acl-name*}}

ip address *acl-number*	Selects one or more IP ACLs for a VLAN access map sequence; valid values are from 1 to 199 and from 1300 to 2699.
ip address acl-*name*	Selects an IP ACL by name.

If a packet matches a permit ACL entry, the specified action is taken and the packet is not checked against the remaining sequences. If a packet matches a deny ACL entry, it is checked against the next ACL in the same sequence or the next sequence. If a packet does not match any ACL entry and at least one ACL is configured for that packet type, the packet is dropped.



Configure VACL to Capture Traffic

Router (config-access-map)#

```
action {{drop [log]} | {forward [capture]} …
```

- Configures the VACL to capture traffic

```
Router(config-access-map)# action forward
 capture
```

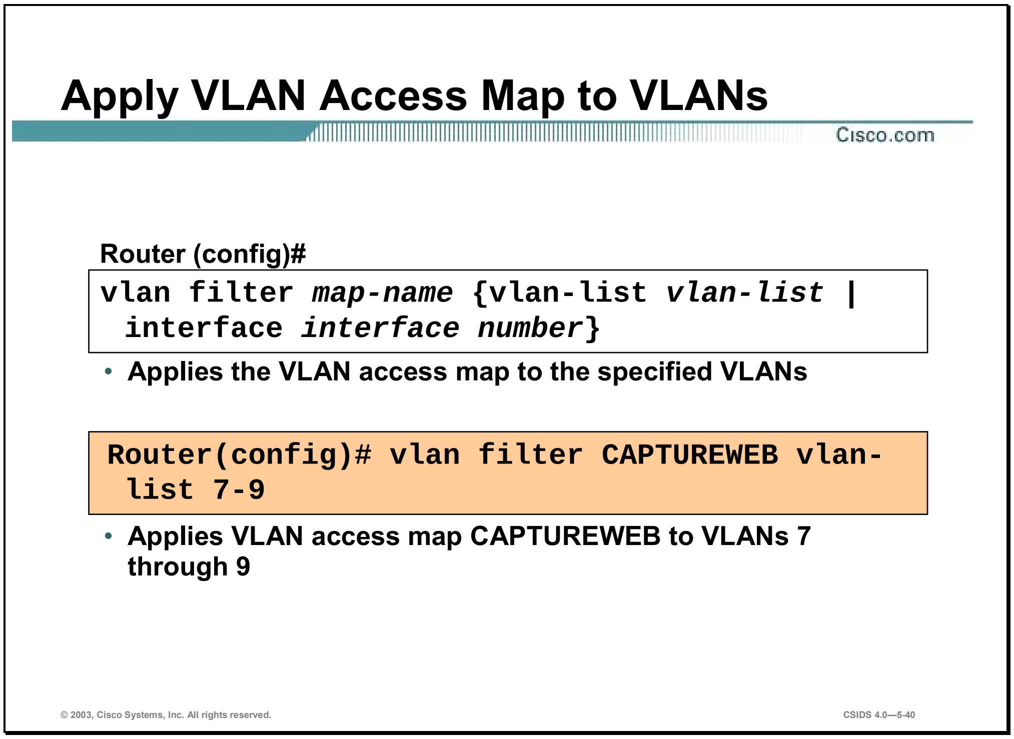
- Configures the VACL to capture traffic

CSIDS 4.0—5-39

While in VLAN access-map configuration mode, use the **action** command to set the action clause. The action clause specifies the action to be taken when a match occurs. Use the **no** form of this command to remove an action clause. The syntax for the **action** command is as follows:

action {{drop [log]} | {forward [capture]} | {redirect {interface *interface-number*}} | {port-channel *channel-id*} {interface *interface-number*} | {port-channel *channel-id*} ...}

drop	Drops the packets.
log	(Optional.) Logs the dropped packets in software.
forward	Forwards (switched by hardware) packets to their destinations.
capture	(Optional.) Sets the capture bit of forwarded packets so that ports with the capture function enabled also receive the packets.
redirect interface	Redirects packets to the specified interfaces; possible valid values are ethernet, fastethernet, gigabitethernet, tengigabitethernet, pos, atm, and ge-wan.
Interface-number	Module and port number; refer to the Usage Guidelines section for valid values.
port-channel *channel-id*	Port channel to redirect traffic; refer to the Usage Guidelines section for valid values.



Apply VLAN Access Map to VLANs

Router (config)#

```
vlan filter map-name {vlan-list vlan-list |
 interface interface number}
```

- Applies the VLAN access map to the specified VLANs

```
Router(config)# vlan filter CAPTUREWEB vlan-
 list 7-9
```

- Applies VLAN access map CAPTUREWEB to VLANs 7 through 9

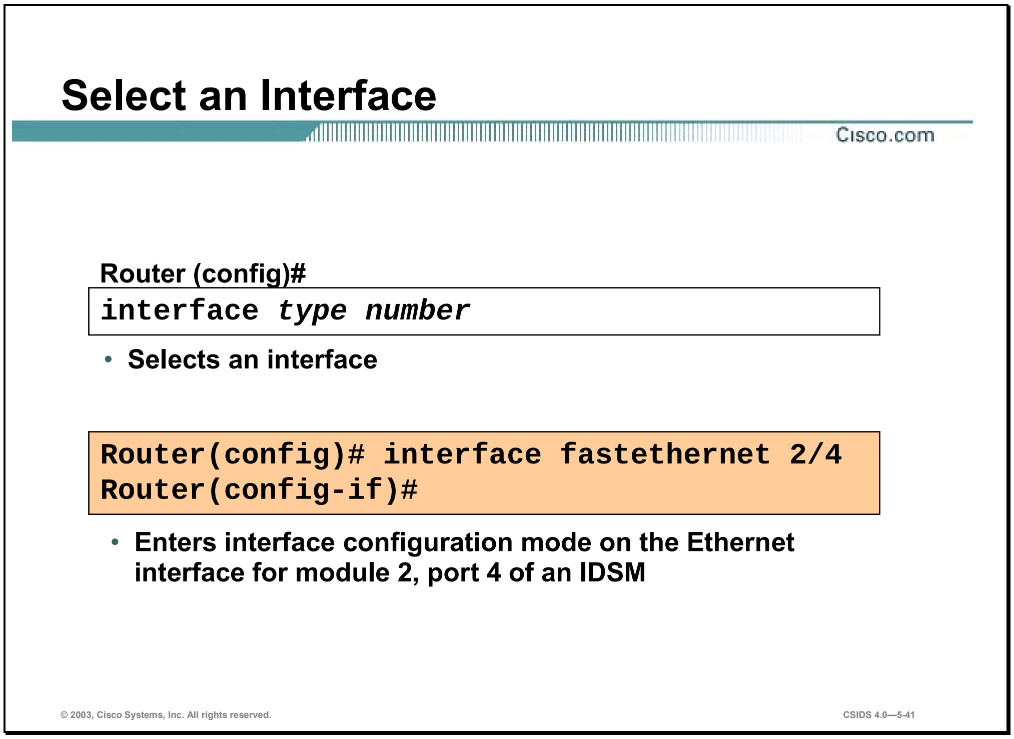
CSIDS 4.0—5-40

Use the **vlan filter** command to apply a VLAN access map. Use the **no** form of this command to clear the VLAN access maps from VLANs or interfaces. The syntax for the **vlan filter** command is as follows:

vlan filter *map-name* {**vlan-list** *vlan-list* | **interface** *interface number*}

map-name	VLAN access map tag.
vlan-list	VLAN list. Refer to the Usage Guidelines section for valid values.
interface	Specifies the WAN interface type. Valid values are pos, atm, or serial.
number	Interface number. The *interface-number* format can be *mod*/*port* or *slot*/*port_adapter*/*port*. It can include a subinterface or channel group descriptor.

You can apply the VLAN access map to one or more VLANs, but only one VLAN access map can be mapped to each VLAN or WAN interface.



Select an Interface

Cisco.com

Router (config)#

```
interface type number
```

- Selects an interface

```
Router(config)# interface fastethernet 2/4
Router(config-if)#
```

- Enters interface configuration mode on the Ethernet interface for module 2, port 4 of an IDSM

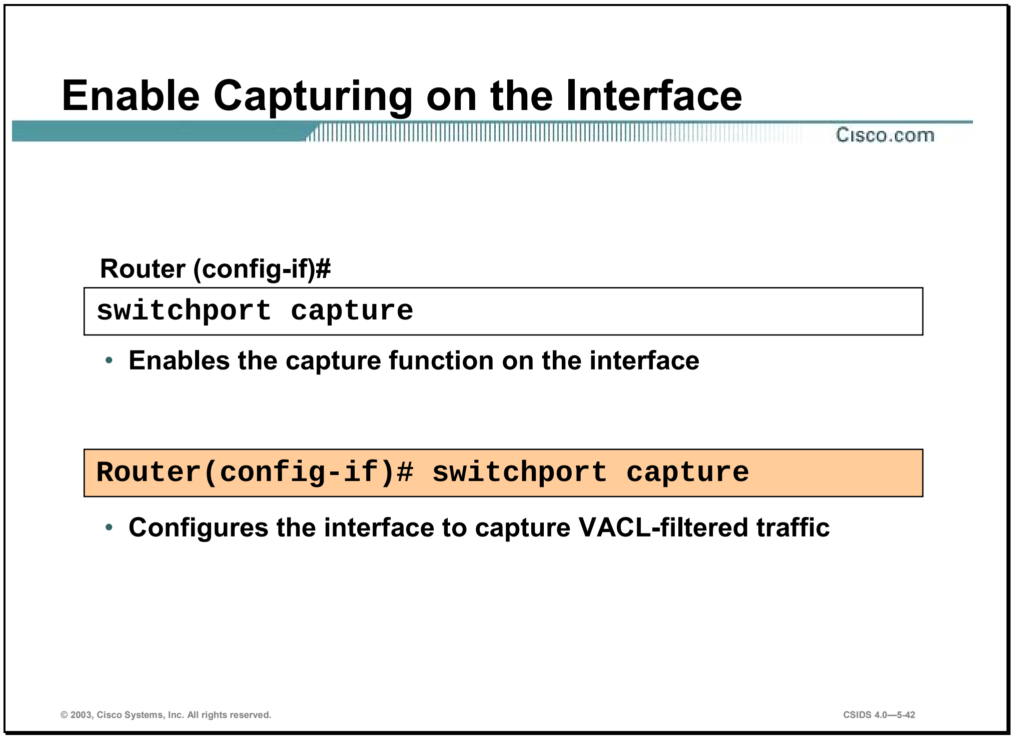
© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—5-41

Use the **interface** command to select an interface to configure, and enter interface configuration mode. The syntax for the **interface** command is as follows:

interface *type number*

type	Type of interface to be configured
number	Module and port number

Note The IDSM, including its valid interface type values, is discussed later in the course.



Enable Capturing on the Interface

Router (config-if)#

```
switchport capture
```

- Enables the capture function on the interface

```
Router(config-if)# switchport capture
```

- Configures the interface to capture VACL-filtered traffic

CSIDS 4.0—5-42

Use the **switchport capture** command to configure the port to capture VACL-filtered traffic. Use the **no** form of this command to disable the capture mode on the port.

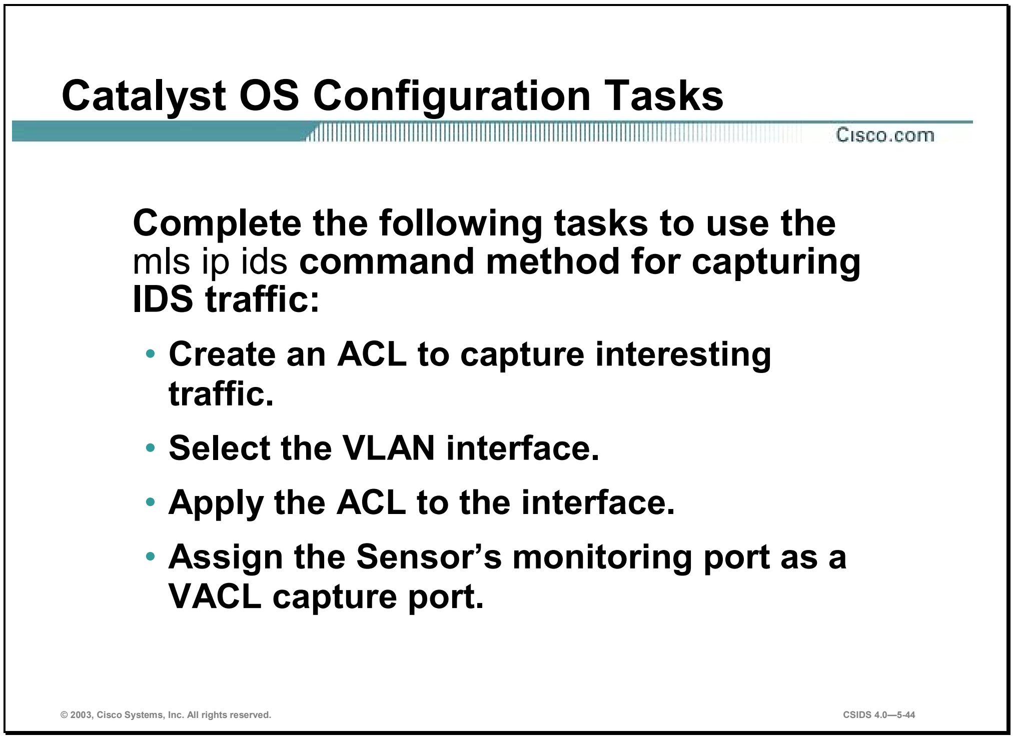
The capture port must allow the destination VLANs of the captured packets. By default, the packets are allowed from all VLANs. Use the **switchport capture allowed vlan** command to restrict capture to specific VLANS.

Once you enable capture on a port, the port changes from its originally configured mode and enters monitor mode. In monitor mode, the capture port has the following characteristics:

- Does not belong to any VLANs it was in previously.
- Does not allow incoming traffic.
- Preserves ISL or dot1q encapsulation if the capture port is a trunk port. The captured packets are encapsulated with the corresponding encapsulation type. If you enable the capture port from an access port, the captured packets are not encapsulated. Be sure to set the desired mode and encapsulation type on the capture port before entering the **switchport capture** command.
- When you enter the **no switchport capture** command to disable the capture function, the port returns to the previously configured mode (access or trunk).

Using the mls ip ids Command for Catalyst 6500 Traffic Capture

This section explains how to use the **mls ip ids** command to configure the Catalyst 6500 switch capture feature.



Catalyst OS Configuration Tasks

Complete the following tasks to use the mls ip ids **command method for capturing IDS traffic:**

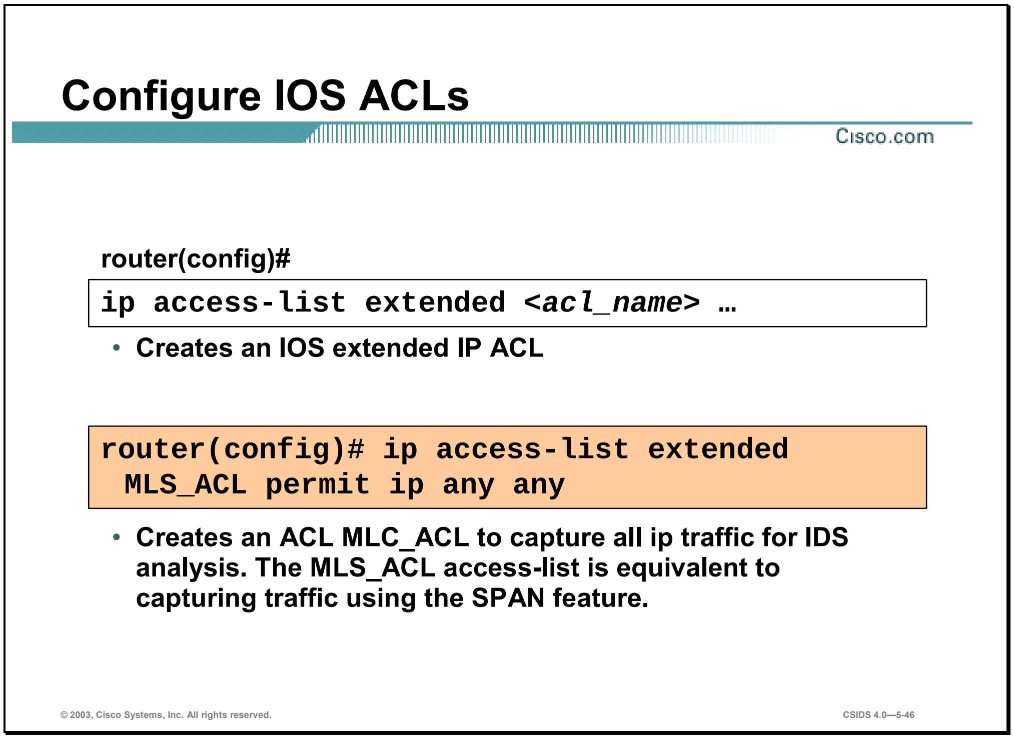
- **Create an ACL to capture interesting traffic.**
- **Select the VLAN interface.**
- **Apply the ACL to the interface.**
- **Assign the Sensor's monitoring port as a VACL capture port.**

CSIDS 4.0—5-44

When you are running the Cisco IOS Firewall on the MSFC, you cannot use VACLs to capture traffic for the IDSM, because you cannot apply VACLs to a VLAN in which you have applied an ip inspect rule for the Cisco IOS Firewall. However, you can use the **mls ip ids** command to designate which packets are captured. Packets that are permitted by the ACL are captured. Those denied by the ACL are not captured. The **permit/deny** parameter does not affect whether a packet is forwarded to destination ports. Packets coming into that router interface are checked against the IDS ACL to determine if they should be captured.

The tasks to capture traffic using the MLS IP IDS feature are as follows:

- Create the ACL to capture interesting traffic.
- Select the VLAN interface.
- Apply the ACL to the interface.
- Assign the Sensor's monitoring port as the VACL capture port.



Configure IOS ACLs

Cisco.com

router(config)#

```
ip access-list extended <acl_name> …
```

- Creates an IOS extended IP ACL

```
router(config)# ip access-list extended
 MLS_ACL permit ip any any
```

- Creates an ACL MLC_ACL to capture all ip traffic for IDS analysis. The MLS_ACL access-list is equivalent to capturing traffic using the SPAN feature.

CSIDS 4.0—5-46

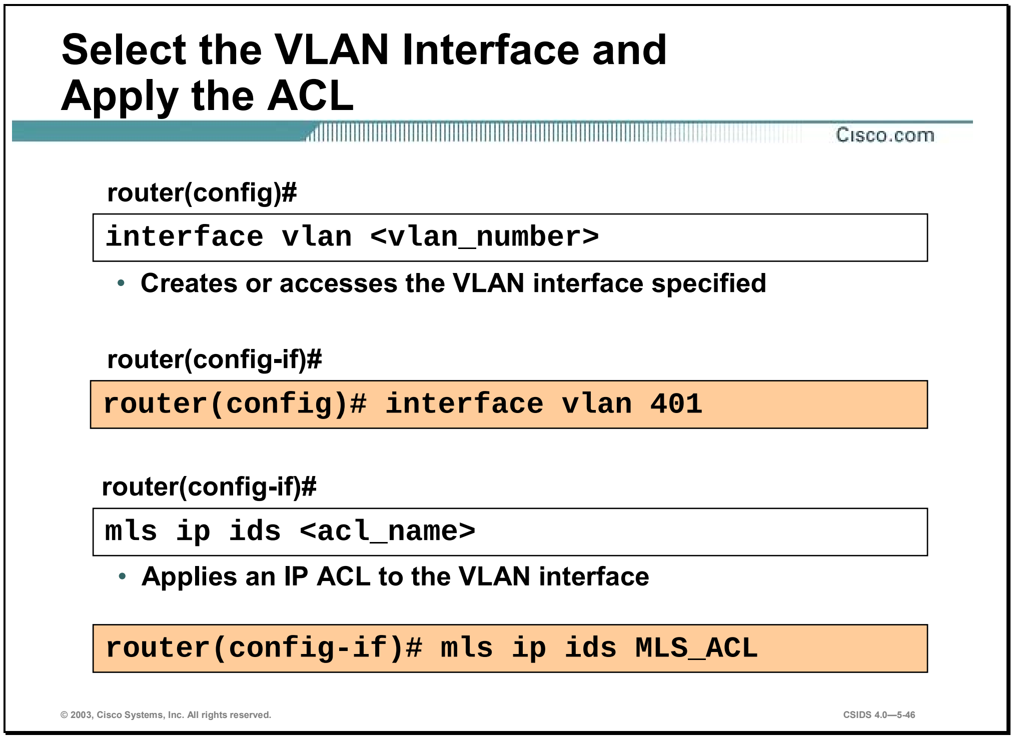
The IOS **ip access-list** command is used to create an IP ACL that is used to determine the traffic captured for intrusion detection analysis.

The extended version of the **access-list** global configuration command is used to define an extended IP access list. The syntax for the **ip access-list** command is as follows:

ip access-list extended ***acl-name*** **{deny | permit}** ***protocol source source-wildcard destination destination-wildcard***

acl-name	Name of the ACL.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an IP protocol. The name can be one of the keywords eigrp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pim, tcp, or udp, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol, (including ICMP, TCP, and UDP) use the keyword ip. Some protocols allow further qualifiers described below.
source	Number of the network or host from which the packet is being sent. Use the keyword any as an abbreviation for a source with IP address 0.0.0.0, or a source wildcard with IP address 255.255.255.255. Use host source as an abbreviation for a source or source wildcard with a source IP address of 0.0.0.0.
source-wildcard	Wildcard bits to be applied to a source. Each wildcard bit set to zero indicates that the corresponding bit position in the packet's IP address must exactly match the bit value in the corresponding bit position of the source. Each wildcard bit set to one indicates that both a zero bit and a one bit in the corresponding position of the packet's IP address will be considered a match to this access list entry. Use the keyword any as an abbreviation for a source with IP address 0.0.0.0, or a source wildcard with IP address 255.255.255.255. Use host source as an abbreviation for a source or source wildcard with a source IP address of 0.0.0.0.

destination	Number of the network or host to which the packet is being sent. Use the keyword any as an abbreviation for a destination with IP address 0.0.0.0, or a destination wildcard with IP address 255.255.255.255. Use host destination as an abbreviation for a destination or destination wildcard with a destination IP address of 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. Place ones in the bit positions you want to ignore. Use the keyword any as an abbreviation for a destination with IP address 0.0.0.0, or a destination wildcard with IP address 255.255.255.255. Use host destination as an abbreviation for a destination or destination wildcard with a destination IP address of 0.0.0.0.



Select the VLAN Interface and Apply the ACL

Cisco.com

router(config)#

```
interface vlan <vlan_number>
```

- Creates or accesses the VLAN interface specified

router(config-if)#

```
router(config)# interface vlan 401
```

router(config-if)#

```
mls ip ids <acl_name>
```

- Applies an IP ACL to the VLAN interface

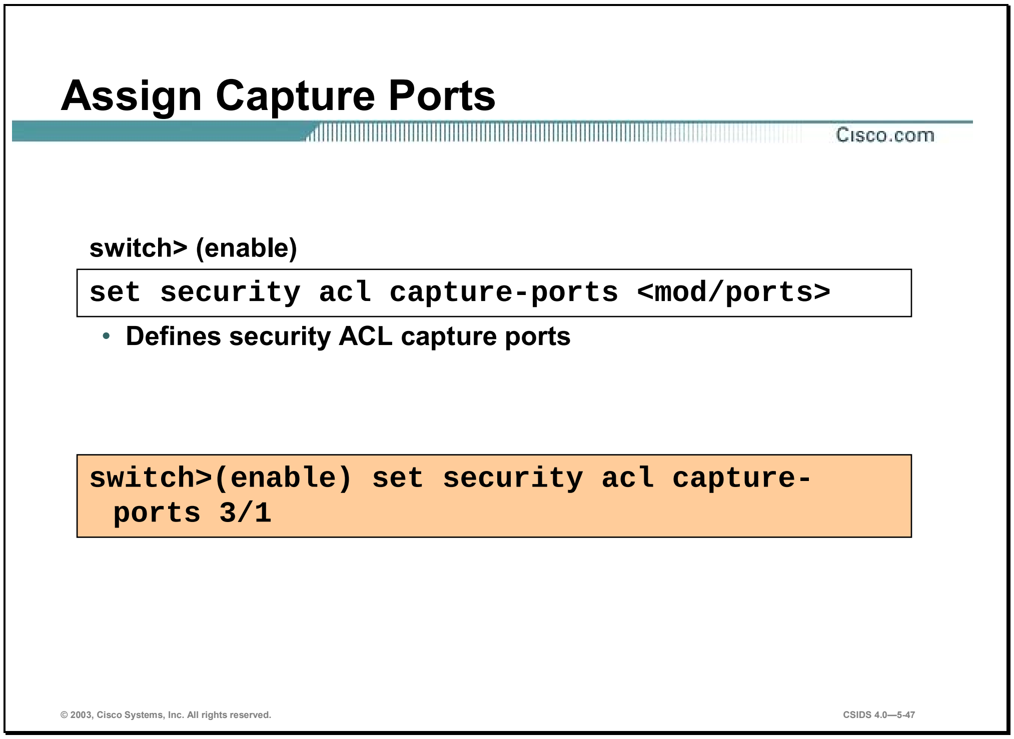
```
router(config-if)# mls ip ids MLS_ACL
```

CSIDS 4.0—5-46

The **interface vlan** command is used to create or access a VLAN interface.

The **mls ip ids** command is used to apply an extended IP access list to the VLAN interface. The **mls ip ids** command works with the **ip access-list** command to designate which packets are captured. Packets that are permitted by the ACL are captured. Packets denied by the ACL are not captured. The permit and deny parameters of the **ip access-list** command do not affect whether or not a packet is forwarded to destination ports. Packets coming into that router interface are checked against the IDS ACL to determine if they should be captured.

Note Refer to the "*Configuring Network Security"* section of the Catalyst 6000 IOS documentation for more information regarding VACLs, CBAC, and IDS.



Assign Capture Ports

Cisco.com

switch> (enable)

```
set security acl capture-ports <mod/ports>
```

- Defines security ACL capture ports

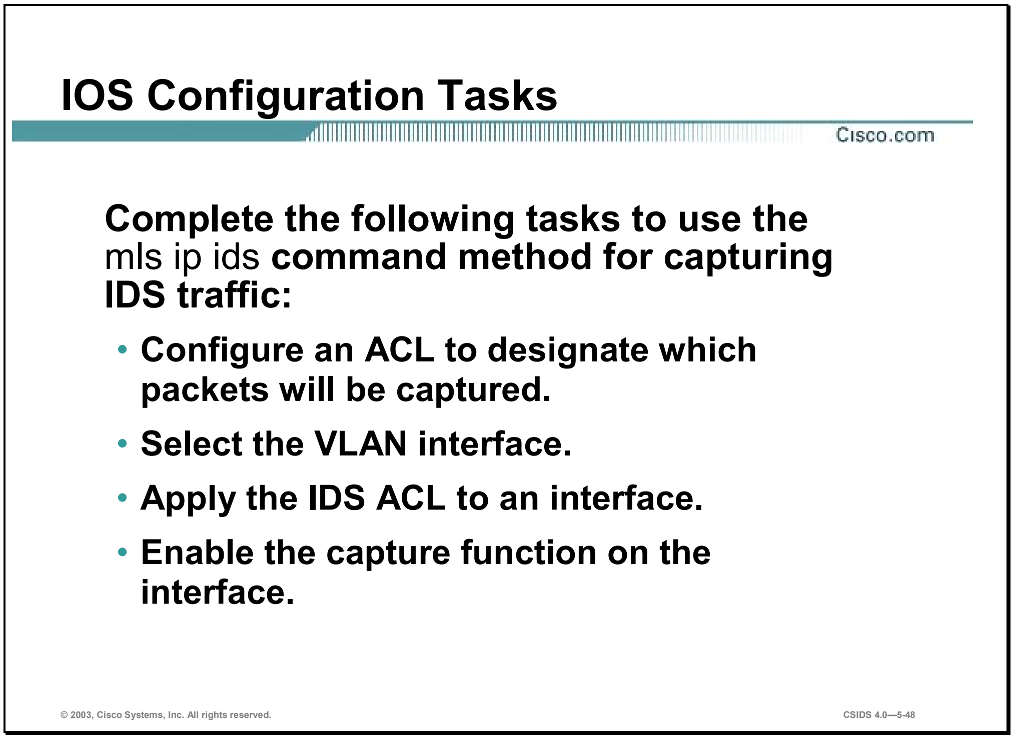
```
switch>(enable) set security acl capture-
 ports 3/1
```

CSIDS 4.0—5-47

The **set security acl capture-ports** command is used to set the destination ports that receive the captured traffic specified in the **set security acl ip** command. Use the **clear security acl capture-ports** command to remove a port from the capture port list. The syntax for the **set security acl capture-ports** command is as follows:

set security acl capture-ports <*mod/ports*>[<*mod/ports*>…]

mod/ports	Module and port number



IOS Configuration Tasks

Cisco.com

Complete the following tasks to use the mls ip ids **command method for capturing IDS traffic:**

- **Configure an ACL to designate which packets will be captured.**
- **Select the VLAN interface.**
- **Apply the IDS ACL to an interface.**
- **Enable the capture function on the interface.**

CSIDS 4.0—5-48

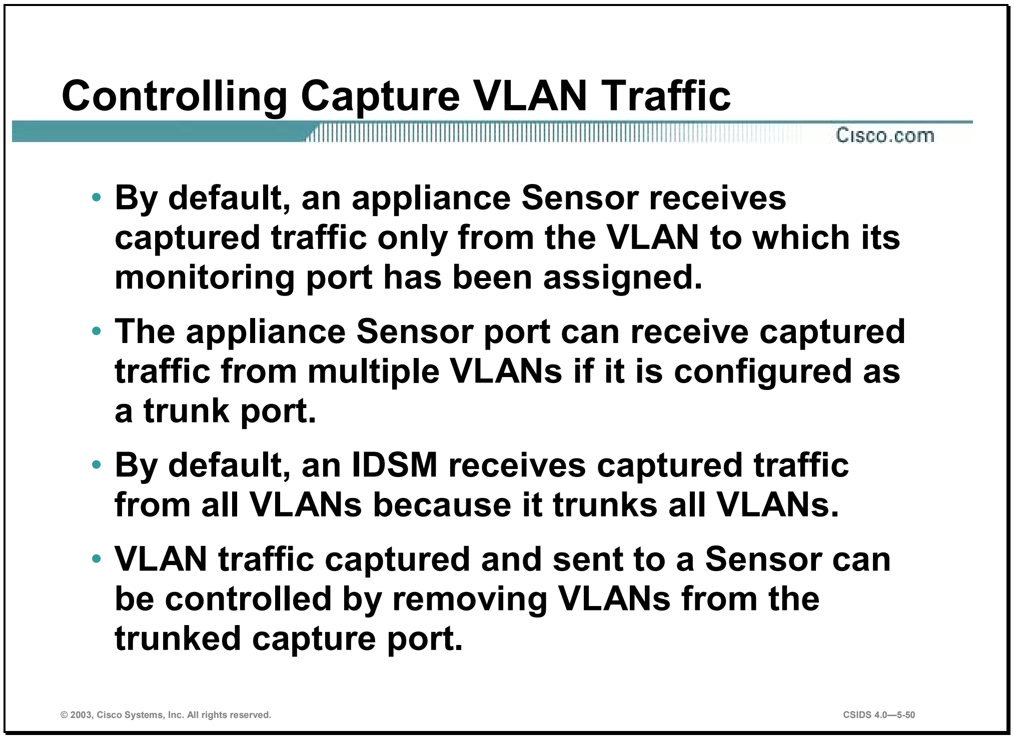
Complete the following tasks to use the **mls ip ids** command to capture IDS traffic:

- Use the IOS **ip access-list** command to configure an ACL that selects traffic for capture.
- Use the **interface vlan** command to select the VLAN interface.
- Use the **mls ip ids** command to apply the IDS ACL to an interface.
- Use the **switchport capture** command to enable the capture function on the interface so that packets with the capture bit set are received by the interface.

Note The syntax for each of these commands is presented earlier in this chapter.

Advanced Catalyst 6500 Traffic Capturing

This section explains how to limit the capture of encapsulated (trunked) traffic using the Catalyst 6500's capture features for VACLs and mls ip ids.



Controlling Capture VLAN Traffic

Cisco.com

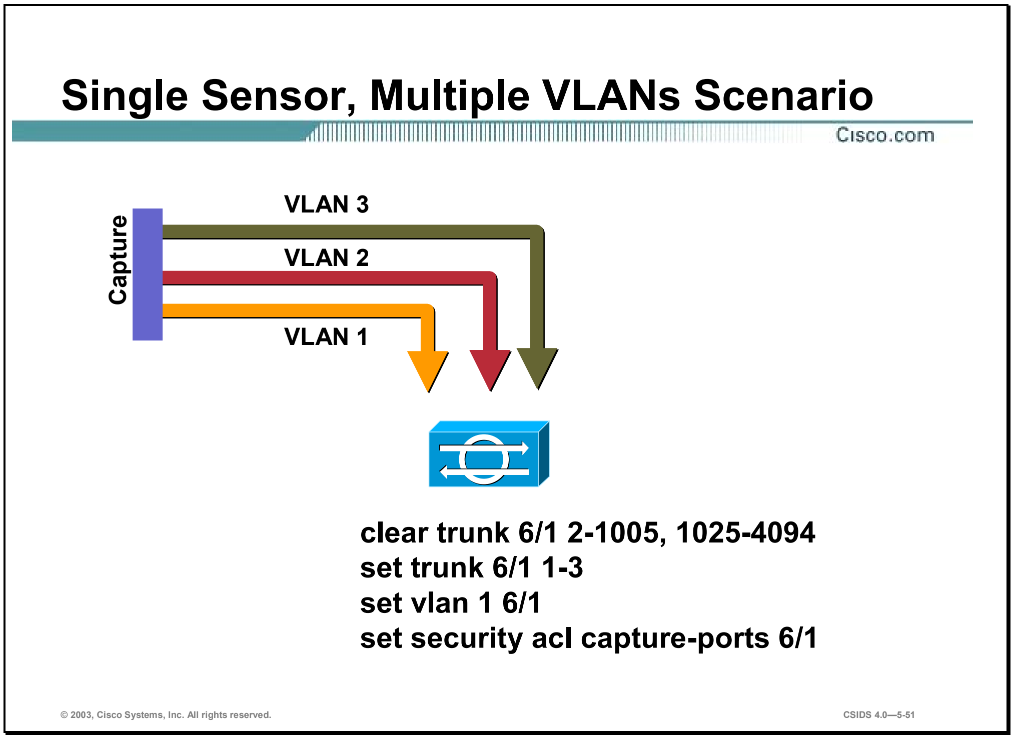
- By default, an appliance Sensor receives captured traffic only from the VLAN to which its monitoring port has been assigned.
- The appliance Sensor port can receive captured traffic from multiple VLANs if it is configured as a trunk port.
- By default, an IDSM receives captured traffic from all VLANs because it trunks all VLANs.
- VLAN traffic captured and sent to a Sensor can be controlled by removing VLANs from the trunked capture port.

CSIDS 4.0—5-50

An appliance Sensor by default receives captured traffic only from the VLAN to which its monitoring port has been assigned. The appliance Sensor's monitoring port is typically connected to an access port on a switch. The switch port must be configured as a trunk port to enable the appliance Sensor to monitor traffic from multiple VLANs.

The IDSM by default receives captured traffic from all VLANs because its monitoring port is a trunk port.

The VLAN traffic captured by the switch and sent to a Cisco IDS Sensor can be controlled by removing VLANs from the trunked capture port.



Single Sensor, Multiple VLANs Scenario

```
clear trunk 6/1 2-1005, 1025-4094
set trunk 6/1 1-3
set vlan 1 6/1
set security acl capture-ports 6/1
```

CSIDS 4.0—5-51

This scenario illustrates that the switch has been configured to send captured traffic only from VLANs 1, 2, and 3 to port 6/1. The Sensor's monitoring port is connected to port 6/1. Captured traffic from other VLANs is ignored.

Notice that the Sensor's monitoring port is a member of VLAN 1.VLAN 1 is the native VLAN for the Sensor's monitoring port.

Note The scenario is based on the use of ACLs to capture traffic.

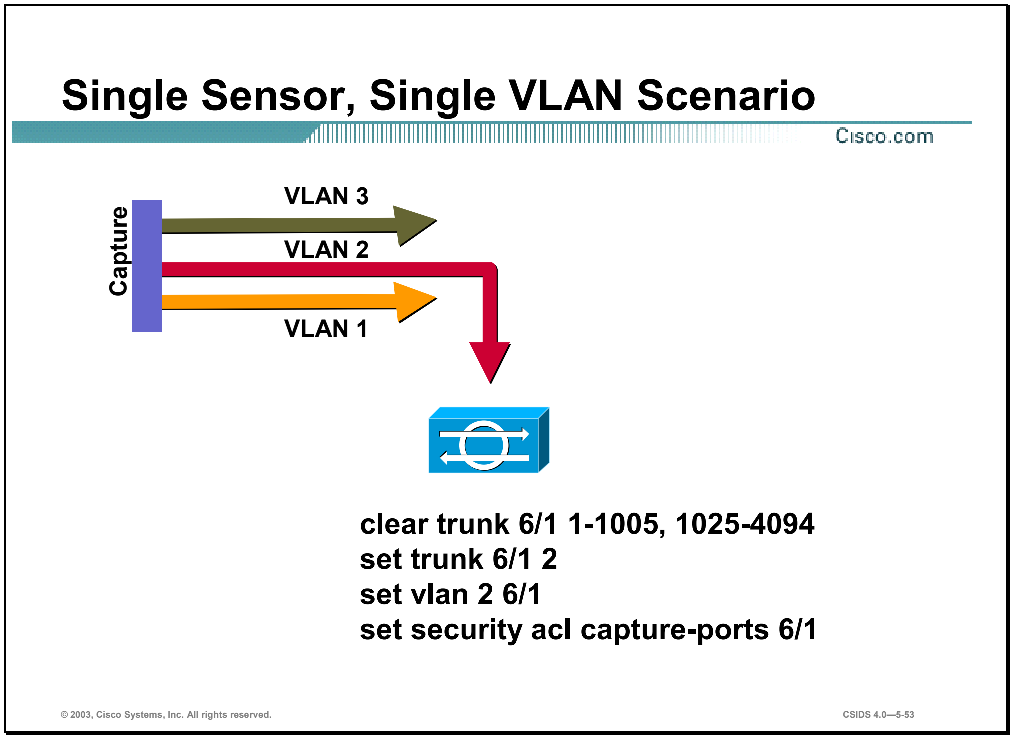
Complete the following steps to configure the switch to only capture traffic from specific vlans to a single Sensor:

Step 1 Clear all VLANs from the switch's destination capture port using the **clear trunk** command.

Step 2 Assign the VLANs of interest to the switch's destination capture port using the **set trunk** command.

Step 3 Assign the switch's destination capture port to a native VLAN using the **set vlan** command.

Step 4 Assign the switch's destination capture port as the ACL capture port using the **set security acl capture-ports** command.



Single Sensor, Single VLAN Scenario

clear trunk 6/1 1-1005, 1025-4094
set trunk 6/1 2
set vlan 2 6/1
set security acl capture-ports 6/1

CSIDS 4.0—5-53

This scenario illustrates that the switch has been configured to send capture traffic only from VLAN 2 to port 6/1. The Sensor's monitoring port is connected to port 6/1. Captured traffic from other VLANs is ignored.

Notice that the Sensor's monitoring port is a member of VLAN 2. VLAN 2 is the native VLAN for the Sensor's monitoring port.

Note The scenario is based on the use of ACLs to capture traffic.

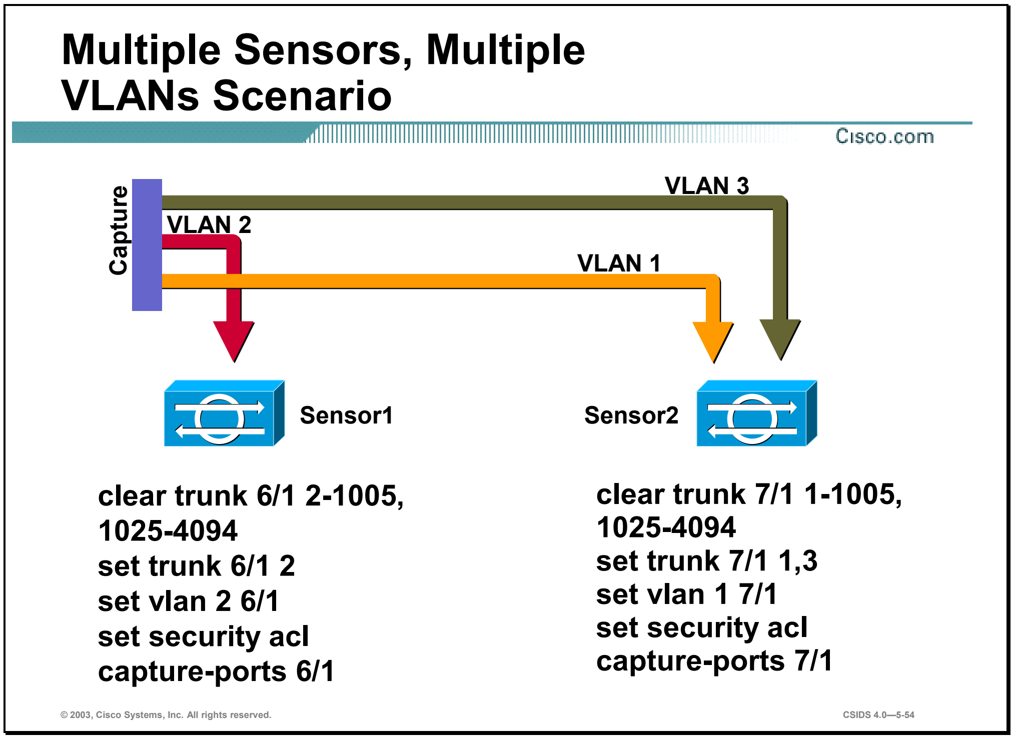
Complete the following steps to configure the switch to only capture traffic from specific VLANs to a single Sensor:

Step 1 Clear all VLANs from the switch's destination capture port using the **clear trunk** command.

Step 2 Assign the VLANs of interest to the switch's destination capture port using the **set trunk** command.

Step 3 Assign the switch's destination capture port to a native VLAN using the **set vlan** command.

Step 4 Assign the switch's destination capture port as the ACL capture port using the **set security acl capture-ports** command.



Multiple Sensors, Multiple VLANs Scenario

Cisco.com

```
clear trunk 6/1 2-1005,
1025-4094
set trunk 6/1 2
set vlan 2 6/1
set security acl
capture-ports 6/1
```

```
clear trunk 7/1 1-1005,
1025-4094
set trunk 7/1 1,3
set vlan 1 7/1
set security acl
capture-ports 7/1
```

CSIDS 4.0—5-54

This scenario illustrates that Sensor1 has been configured to capture traffic only from VLAN 2 to port 6/1, and Sensor2 has been configured to capture traffic only from VLANs 1 and 3 to port 7/1. Captured traffic from other VLANs is ignored.

Notice that Sensor1's monitoring port is a member of VLAN 2, and the Sensor2's monitoring port is a member of VLAN 1. VLAN 2 is the native VLAN for Sensor1's monitoring port, and VLAN 1 is the native VLAN for Sensor2's monitoring port.

Note The scenario is based on the use of ACLs to capture traffic.

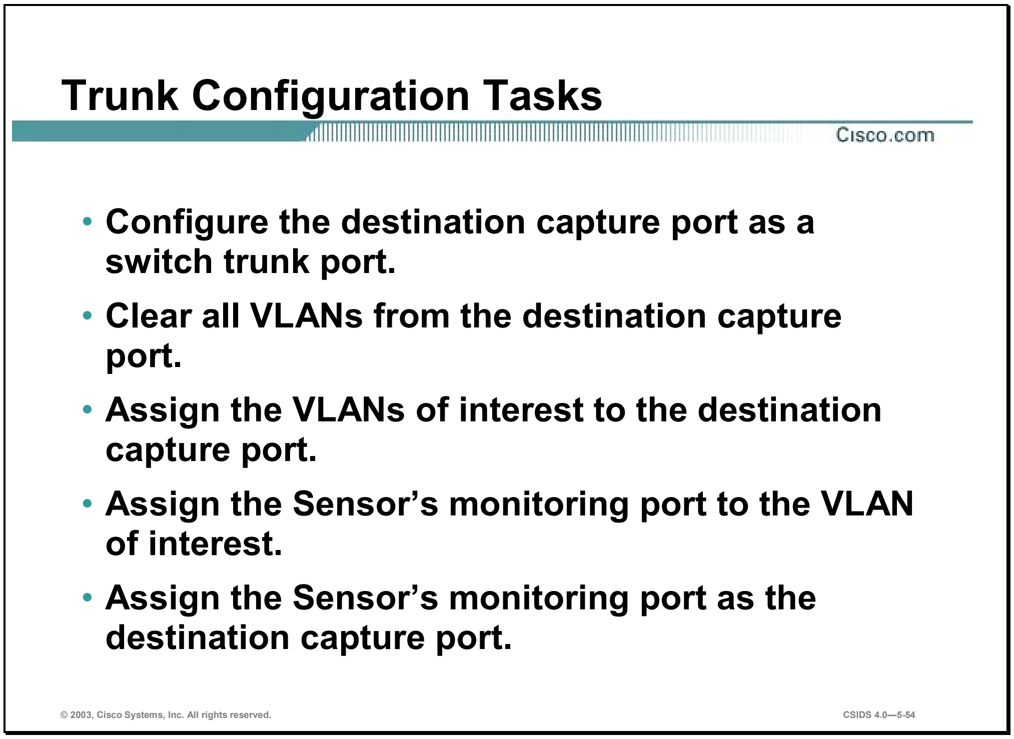
Complete the following steps to configure the switch to only capture traffic from specific VLANs to a specific Sensor:

Step 1 Clear all VLANs from the switch's destination capture port using the **clear trunk** command.

Step 2 Assign the VLANs of interest to the switch's destination capture port using the **set trunk** command.

Step 3 Assign the switch's destination capture port to a native VLAN using the **set vlan** command.

Step 4 Assign the switch's destination capture port as the ACL capture port using the **set security acl capture-ports** command.



Trunk Configuration Tasks

Cisco.com

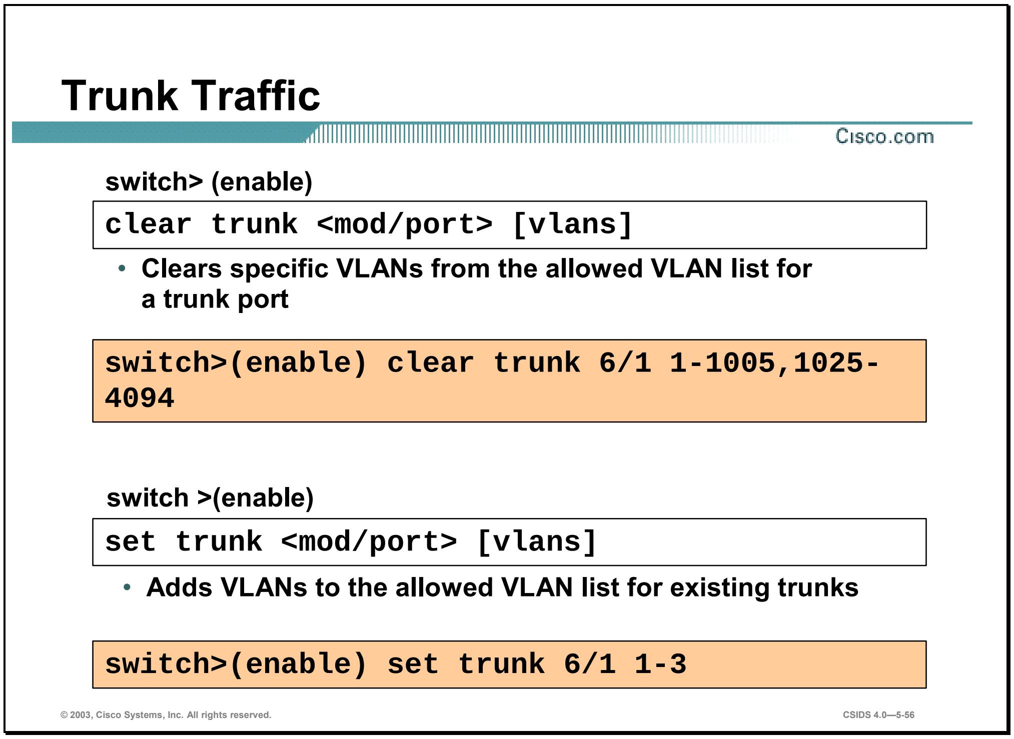
- Configure the destination capture port as a switch trunk port.
- Clear all VLANs from the destination capture port.
- Assign the VLANs of interest to the destination capture port.
- Assign the Sensor’s monitoring port to the VLAN of interest.
- Assign the Sensor’s monitoring port as the destination capture port.

CSIDS 4.0—5-54

Complete the following tasks to configure the switch to control traffic capture and to send traffic to the IDSM’s monitoring port:

- Configure the destination capture port as a switch trunk port using the **set port dot1qtunnel** command.
- Clear all VLANS from the switches destination capture port using the **clear trunk** switch command.
- Assign the VLANs of interest to the switches destination capture port using the **set trunk** switch command.
- Assign the monitoring port to the VLAN of interest using the **set vlan** command.
- Assign the switch’s monitoring port as the destination capture port using the **set security acl capture-ports** command.

Note The tasks are based on the use of VLAN ACLs to capture traffic.



Trunk Traffic

Cisco.com

switch> (enable)

```
clear trunk <mod/port> [vlans]
```

- Clears specific VLANs from the allowed VLAN list for a trunk port

```
switch>(enable) clear trunk 6/1 1-1005,1025-
4094
```

switch >(enable)

```
set trunk <mod/port> [vlans]
```

- Adds VLANs to the allowed VLAN list for existing trunks

```
switch>(enable) set trunk 6/1 1-3
```

CSIDS 4.0—5-56

The **clear trunk** command is used to restore a trunk port to its default trunk type and mode or to clear specific VLANs from the allowed VLAN list for a trunk port. The syntax for the **clear trunk** command is as follows:

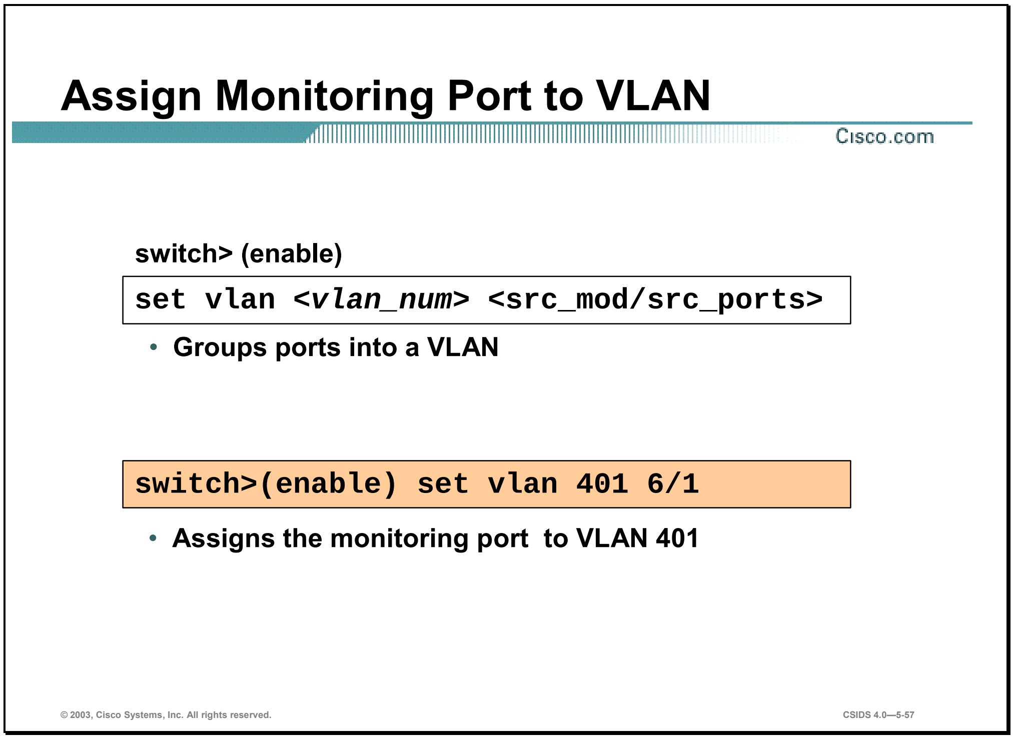
clear trunk <*mod/port*> [*vlans*]

mod/port	Number of the module and the port on the module.
vlans	(Optional.) Number of the VLAN to remove from the allowed VLAN list. Valid values range from 1 to 1005 and 1025 to 4094.

The **set trunk** command is used to configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks. The syntax for the **set trunk** command is as follows:

set trunk *<mod/port> [vlans]*

mod/port	Number of the module and the port on the module.
vlans	(Optional.) VLANs to add to the list of allowed VLANs on the trunk. Valid values range from 1 to 1000 and 1025 to 4094.



Assign Monitoring Port to VLAN

Cisco.com

switch> (enable)

```
set vlan <vlan_num> <src_mod/src_ports>
```

- Groups ports into a VLAN

```
switch>(enable) set vlan 401 6/1
```

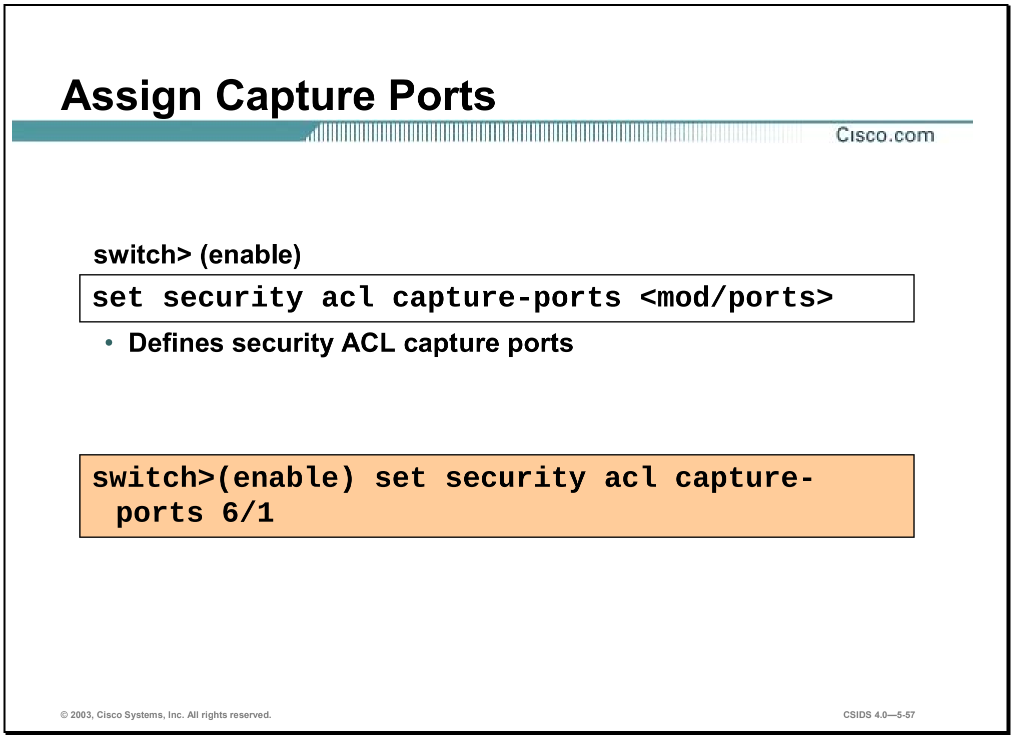
- Assigns the monitoring port to VLAN 401

CSIDS 4.0—5-57

The **set vlan** command is used to set group ports into a VLAN, or to set the private VLAN type. The syntax for the **set vlan** command is as follows:

set vlan ***vlan_num mod/ports***

vlan_num	Number identifying the VLAN
mod/ports	Number of the module and ports on the module belonging to the VLAN



Assign Capture Ports

switch> (enable)

```
set security acl capture-ports <mod/ports>
```

- Defines security ACL capture ports

```
switch>(enable) set security acl capture-
 ports 6/1
```

CSIDS 4.0—5-57

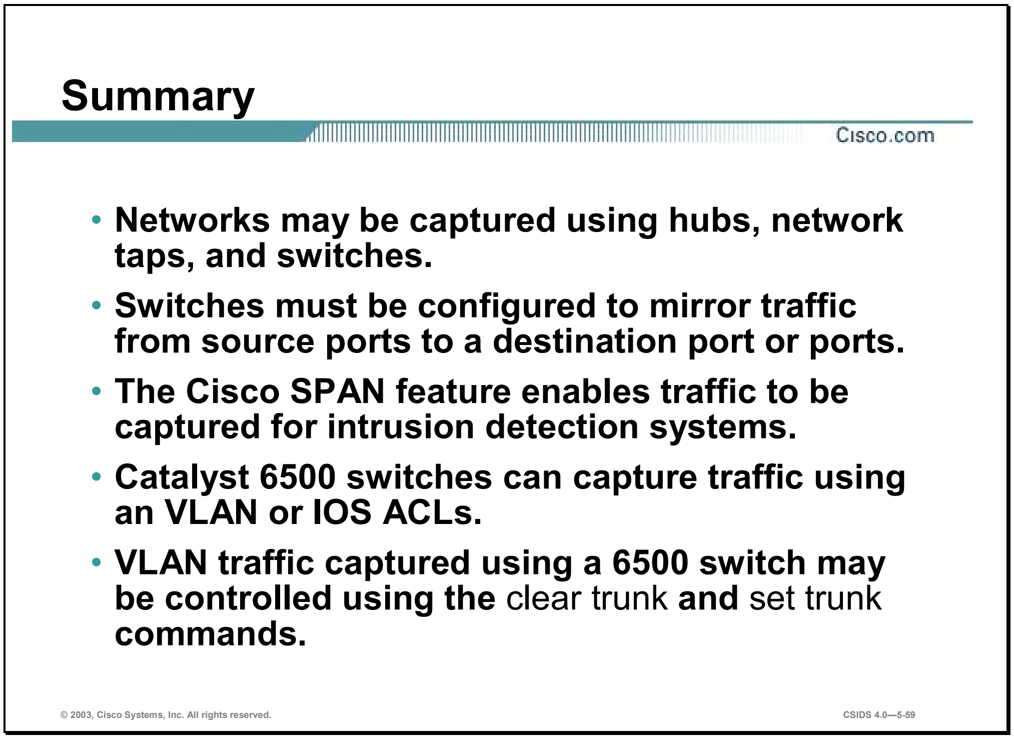
The **set security acl capture-ports** command is used to set the destination ports that receive the captured traffic specified in the **set security acl ip** command. Use the **clear security acl capture-ports** command to remove a port from the capture port list. The syntax for the **set security acl capture-ports** command is as follows:

set security acl capture-ports <*mod/ports*>[,<*mod/ports*>…]

mod/ports	Module and port number

Summary

This section summarizes what you have learned in the chapter.



Summary

- **Networks may be captured using hubs, network taps, and switches.**
- **Switches must be configured to mirror traffic from source ports to a destination port or ports.**
- **The Cisco SPAN feature enables traffic to be captured for intrusion detection systems.**
- **Catalyst 6500 switches can capture traffic using an VLAN or IOS ACLs.**
- **VLAN traffic captured using a 6500 switch may be controlled using the** clear trunk **and** set trunk **commands.**

CSIDS 4.0—5-59

Cisco Intrusion Detection System Architecture

Overview

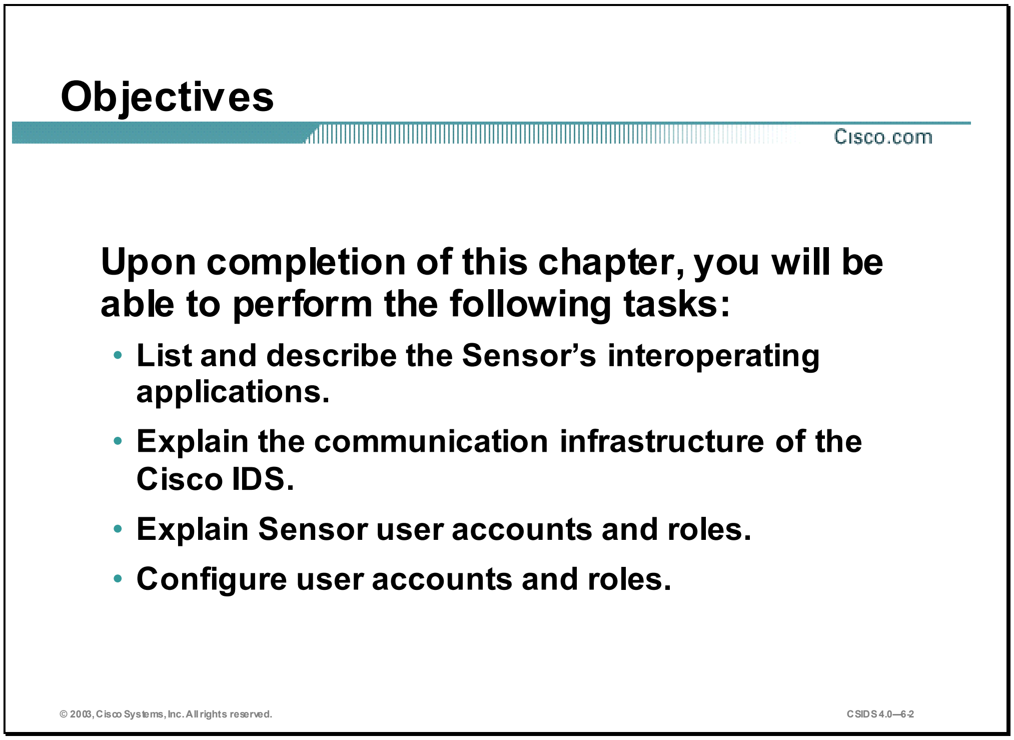
This chapter describes the Cisco Intrusion Detection System (Cisco IDS) architecture.

This chapter includes the following topics:

- Objectives
- Cisco IDS software architecture
- Cisco IDS communication
- User accounts and roles
- Summary

Objectives

This section lists the chapter's objectives.



Objectives

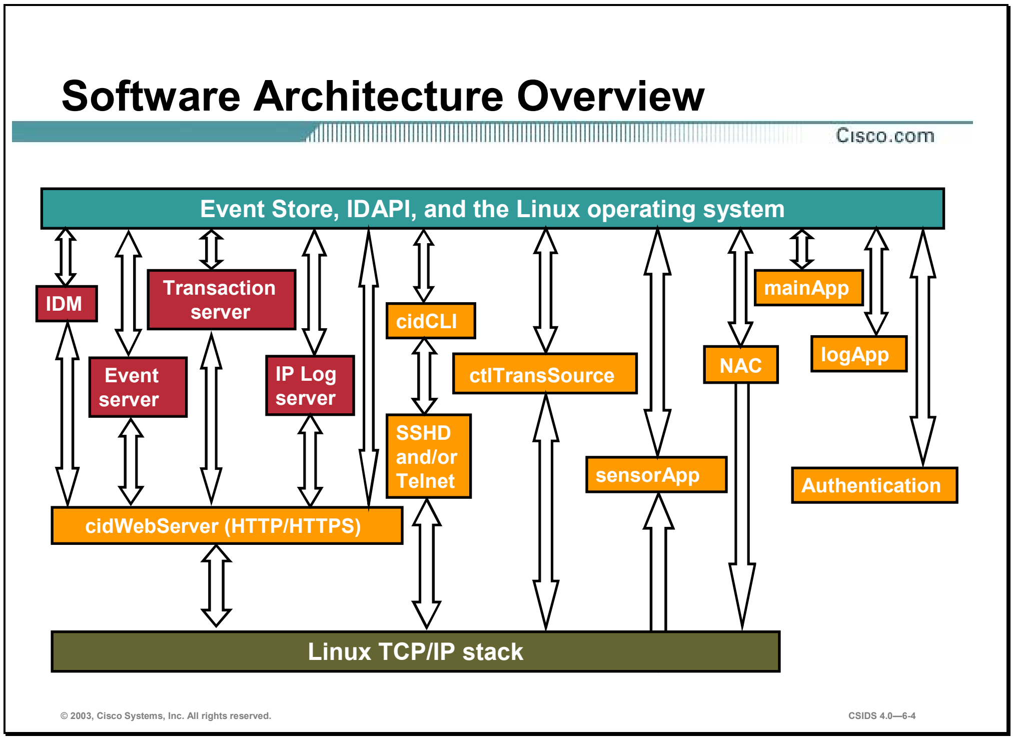
Cisco.com

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

- **List and describe the Sensor's interoperating applications.**
- **Explain the communication infrastructure of the Cisco IDS.**
- **Explain Sensor user accounts and roles.**
- **Configure user accounts and roles.**

Cisco IDS Software Architecture

This section discusses the Cisco Intrusion Detection System (Cisco IDS) Sensor architecture.



Software Architecture Overview

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—6-4

Cisco IDS 4.0 runs on the Linux operating system and is made up of the following interacting operations:

- cidWebServer—The Sensor's web server. The web server is capable of both HTTP and HTTPS communications. It provides more than static web pages. It provides the front-end server for IDM. IDM runs as a servlet inside the web server. The web server uses several other servlets to provide IDS services. These servlets are shared libraries that are loaded into the cidWebserver process at run-time. The following bullets describe the servlets:
  - IDM—Provides the IDM web-based management interface.
  - Event server—Used to serve events to external management applications such as IEV.
  - Transaction server—Allows external management applications such as the IDS MC to initiate control transactions with the Sensor. Control transactions are used to configure and control Sensors.
  - IP log server—Used to serve IP logs to external systems.

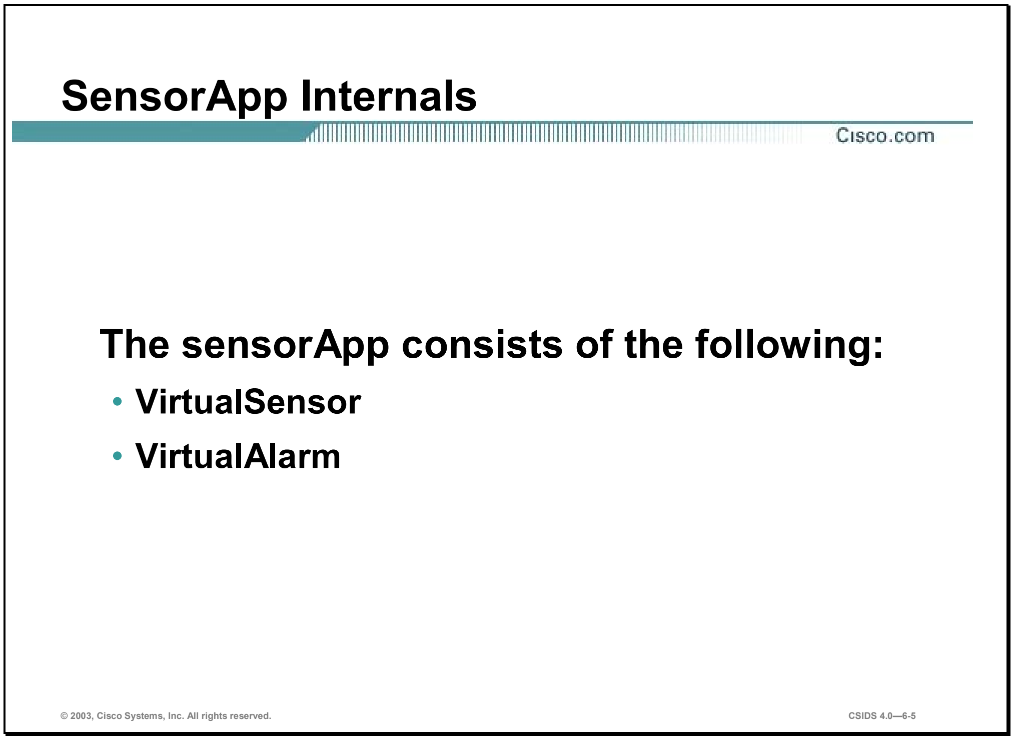
Note The Event Server, Transaction Server and IPlog Server servlets communicate using the Remote Data Exchange Protocol (RDEP). RDEP serves as the Sensor's external communication protocol.

- mainApp—The first application launched. It is responsible for configuring the Sensor's operating system configuration such as the IP address. The mainApp also starts and stops all the other IDS applications.
- logApp—Handles writing all of the application's log messages to the log file. The logApp also writes the application's error messages to the EventStore.
- Authentication—Configures and manages authentication on the Sensor. The authentication application determines a user's authentication status and role based on username and password. Each user is assigned a role on the Sensor. The user's role determines the operations that a user is allowed to perform.
- Network Access Controller (NAC)—Used to initiate Sensor shunning on network devices.
- ctlTransSource—Allows Sensors to communicate control transactions with each other. This is currently used to enable the NAC's master blocking Sensor capability. The master blocking Sensor is explained later in the course.
- sensorApp—The actual sensing engine. The sensorApp processes the signature and alarm channel configurations and generates alert events based on its configuration and the IP traffic. The sensorApp, like all applications, stores its events in the Event Store.
- Event Store—A 4 GB, shared, memory-mapped file where all events are stored. The sensorApp is the only application that writes alert events into the Event Store. All applications may write log, status and error events into the Event Store.
- cidCLI—The CLI shell application that is started when a user logs into the Sensor. A separate cidCli process is loaded for each CLI shell. In IDS 4.0, operating system shell access has been replaced with the CLI, through which most tasks can be performed. Use the CLI or the management and monitoring applications discussed in the previous chapter for configuration and troubleshooting. Shell access for configuration is no longer supported.

A Sensor running Cisco IDS 4.0 is secured by the following:

- SSH and TLS/SSL secure interfaces
- CLI access only (no operating system shell access for configuration)
- Role-based user privileges

Note Securing a Sensor running Cisco IDS 4.0 is discussed in depth later in the course.



SensorApp Internals

Cisco.com

The sensorApp consists of the following:

- **VirtualSensor**
- **VirtualAlarm**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—6-5

The sensing engine, sensorApp, consists of the following:

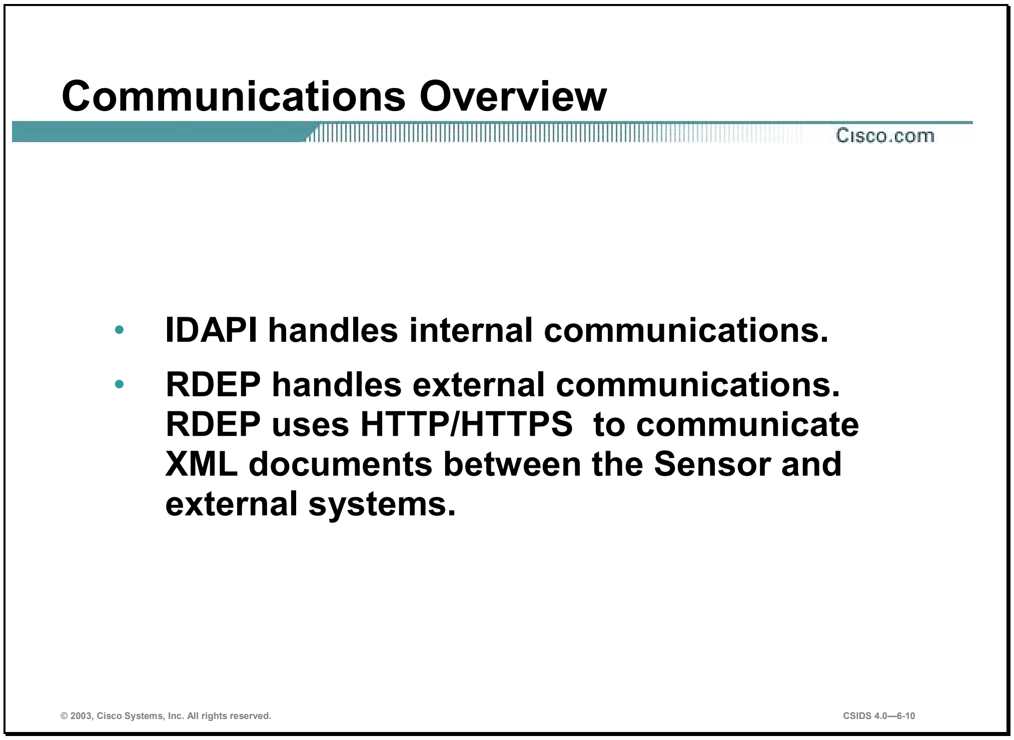
- VirtualSensor—Receives packets, processes them, and determines if they constitute an alarm or not. Various processors reside within the VirtualSensor, each of which has a specific function:
    - CaptureProducer—Receives the packets from the feed and pushes them down to other processors
    - Layer2Handler—Handles L2 inspection, dispatching, and traps for ignored packets. Processes ARP packets and passes Ethernet packets to the next processor
    - FragmentReassembler unit (FRU)—Reassembles IP Fragments
    - DatabaseHandler—Provides internal storage for tracking streams and cross packet analysis
    - StreamReassembler unit (SRU)—Reassembles and dispatches TCP streams
    - SignatureHandler—Controls and dispatches all non-stream signature engines

Note The VirtualSensor provides the ability to run multiple virtual Sensors on the same appliance, each configured with different signature behavior and traffic feeds. Although there is only one VirtualSensor in the initial release of Cisco IDS 4.0, the basic infrastructure is in place to support multiple VirtualSensors in future versions.

- VirtualAlarm (AlarmChannel)—Responsible for the output of the alarms to the downstream IdsEventStore and performing or starting the EventAction.

Cisco IDS Communication

This section discusses the Cisco Intrusion Detection System (Cisco IDS) communication protocol.



Communications Overview

Cisco.com

- IDAPI handles internal communications.
- RDEP handles external communications. RDEP uses HTTP/HTTPS to communicate XML documents between the Sensor and external systems.

© 2003, Cisco Systems, Inc. All rights reserved.

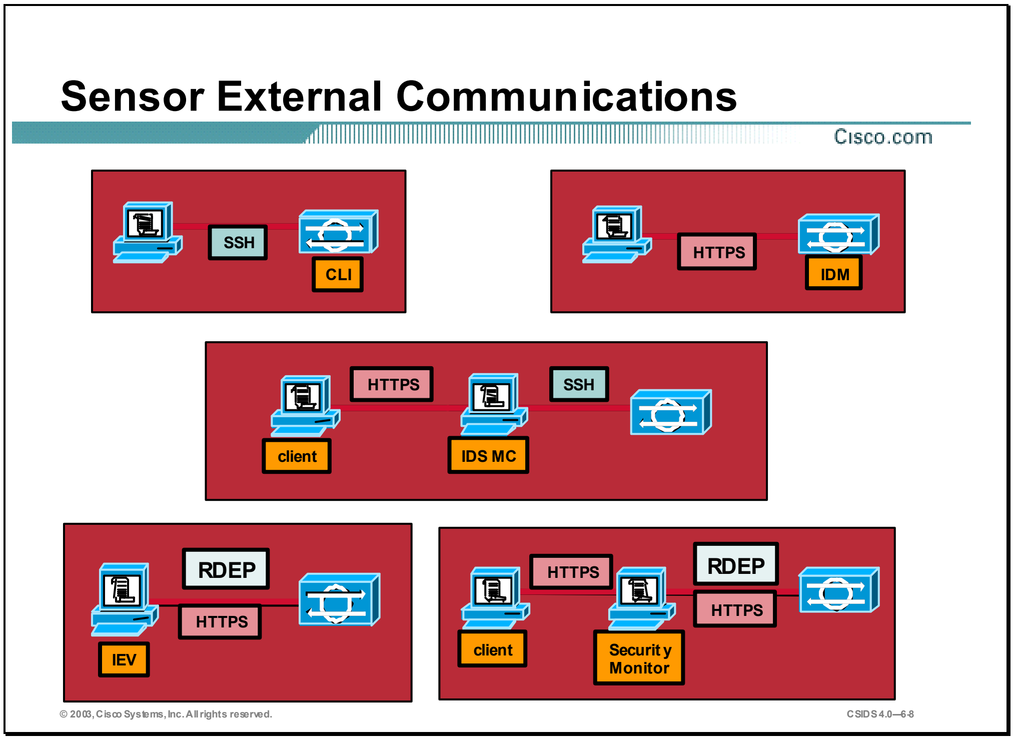
CSIDS 4.0—6-10

Cisco IDS 4.0 applications use an inter-process communication API called Intrusion Detection Application Program Interface (IDAPI) to handle internal communications. IDAPI provides a means to store and share data between IDS applications. External communications use the Remote Data Exchange Protocol (RDEP). RDEP uses HTTP and TLS/SSL to pass XML documents between the Sensor and external systems.

RDEP is an application-level communications protocol used to exchange IDS event messages and IP log messages between the Sensor and external systems. RDEP communications consist of request and response messages. RDEP defines the following classes of request and response messages:

- Event messages—Include IDS alarm, status, and error messages. Monitoring applications such as IEV and the Security Monitor use RDEP's event pull model to retrieve events from the Sensor. The pull model allows the application to pull alarms at its own pace. As soon as the monitoring application connects to the Sensor and requests alarms, the alarms are returned to the monitoring application console without delay. Alarms remain on the Sensor until a 4-GB limit is reached and they are overwritten by new alarms. Since a large number of alarms can be stored on the Sensor itself, the management application can pull alarms after being disconnected for a long period of time without losing alarms.

- IP log messages—Used by clients to retrieve IP log data from Sensors.



Sensor External Communications

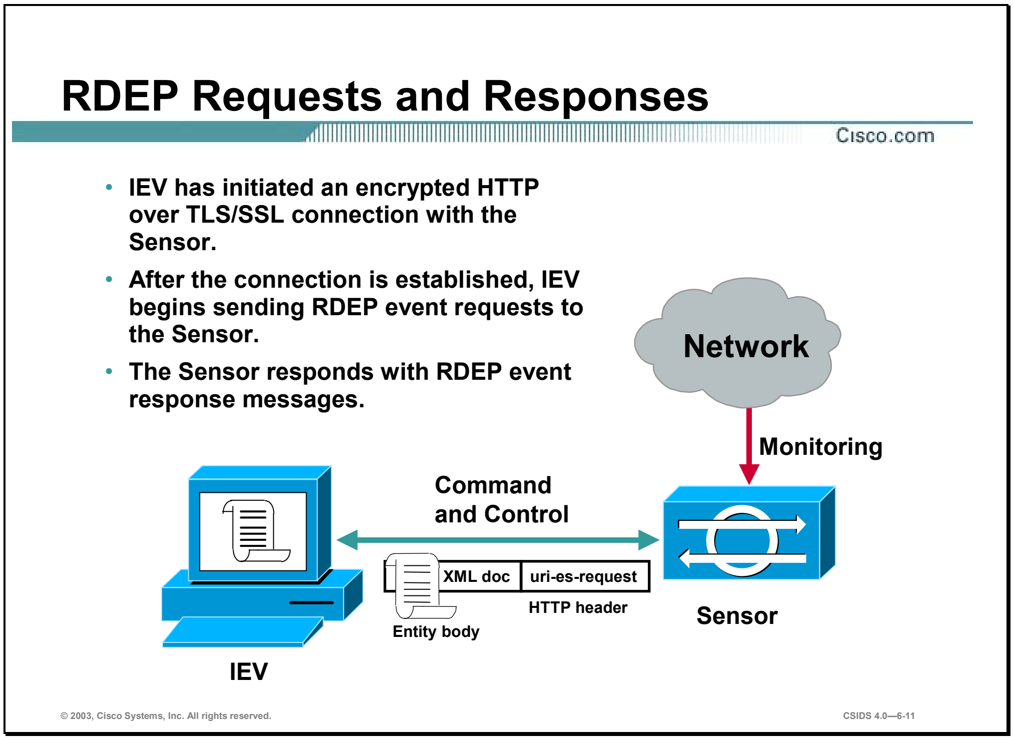
Cisco.com

CSIDS 4.0—6-8

RDEP uses the industry standard HTTPS provide a standardized interface for the exchange of XML documents between the Sensor and external systems. Another industry standard, SSH, can also be used to communicate with the Sensor. The Sensor uses these two protocols as follows:

- Communication with monitoring applications—HTTPS
- Network access to the Sensor for management—SSH and HTTPS
- Communication with blocking devices (IOS-based routers and PIX Firewalls)—SSH

The figure details the communications between the Sensor and each type of management and monitoring application with which it interacts. Also, illustrated are communications between the management and monitoring servers and the clients used to access them.



RDEP Requests and Responses

Cisco.com

- IEV has initiated an encrypted HTTP over TLS/SSL connection with the Sensor.
- After the connection is established, IEV begins sending RDEP event requests to the Sensor.
- The Sensor responds with RDEP event response messages.

CSIDS 4.0—6-11

The Sensor uses RDEP to communicate with other Cisco IDS devices via its command and control interface. RDEP operations begin with a client initiating an encrypted HTTP over TLS/SSL connection with an RDEP server. Once a connection is established, the RDEP client may initiate RDEP requests to the RDEP server. The server acts on the requests and responds back to each of the client's requests with an RDEP response.

Clients initiate RDEP requests by specifying one of the following in the request's HTTP Uniform Resource Identifier (URI):

- uri-es-request—An event request. There are two types of event requests:
  - Queries—Used to retrieve events, based on the query specification, that are currently stored on the server.
  - Subscriptions—Allow clients to establish live event feeds. The RDEP client initiates an event subscription by sending a subscription-open request to an RDEP server. Once the subscription is opened, the client sends subscription-get messages to the server to retrieve events from the subscription. The subscription-open request specifies the query criteria that restrict which events may be retrieved from the subscription.
- uri-iplog-request—An IP log request.

Each RDEP message consists of an HTTP header section followed by an optional entity (message) body. Not every request or response message contains an entity body.

Event message entity bodies consist of XML documents. RDEP does not specify the schemas for the XML documents exchanged in RDEP messages. This is done by the Intrusion Detection Interaction and Operations Messages (IDIOM) specification.

Note IP log requests do not contain entity bodies. A successful IP log response's entity body consists of IP log data. The IP log data consists of the binary IP packet data in the requested IP log. If an error occurs, the server returns a response with an HTTP error status code and an HTML document that describes the error in the response's entity body.

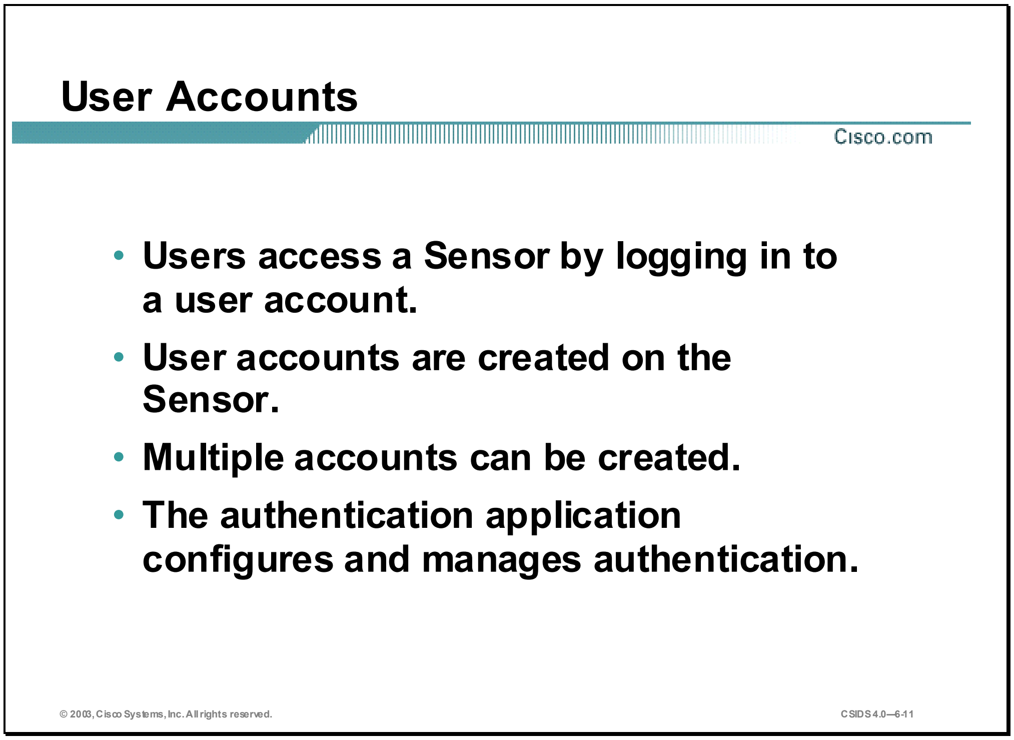
RDEP messages are securely exchanged using TLS/SSL between the Sensor and external systems. The client initiates a TCP connection to an HTTP over SSL (also known as HTTPS) server on the target host. TCP provides a reliable stream transport. The TLS/SSL protocol provides cipher and secret key negotiation, session privacy and integrity, server authentication, and optional client authentication.

The figure illustrates IEV initiating communications with the Sensor. After establishing an HTTPS connection with the Sensor, IEV sends an RDEP event request to the Sensor. The uri-es-request URI specifies the client is initiating an event transaction. The server will return a response that contains an IDIOM Response document. If an error occurs, the server will return an IDIOM Error document containing an explanation of the problem.

Note See the RDEP and IDIOM specifications on CCO for more information.

User Accounts and Roles

This section explains the Sensor's use of user accounts and roles.



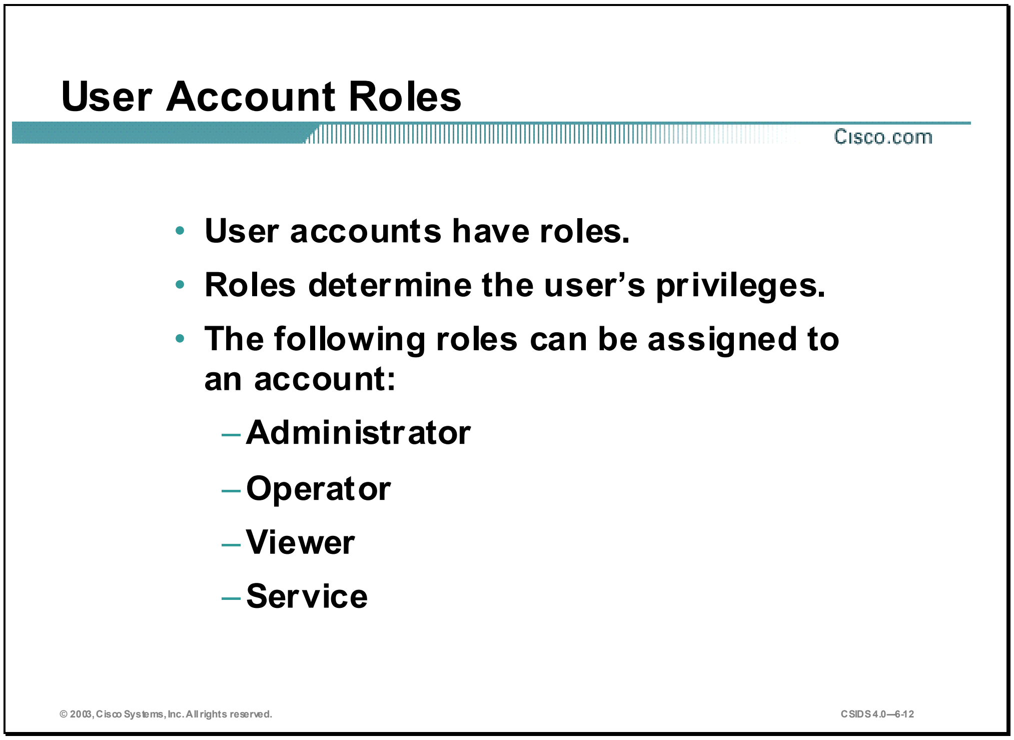
User Accounts

Cisco.com

- Users access a Sensor by logging in to a user account.
- User accounts are created on the Sensor.
- Multiple accounts can be created.
- The authentication application configures and manages authentication.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—6-11

Users access a Sensor by logging in to a user account. User accounts are created on the Sensor. Management consoles may maintain user accounts independently from Sensors. In other words, you can create and log in to accounts that exist only on a management console. The Sensor allows multiple local user accounts to be created.



User Account Roles

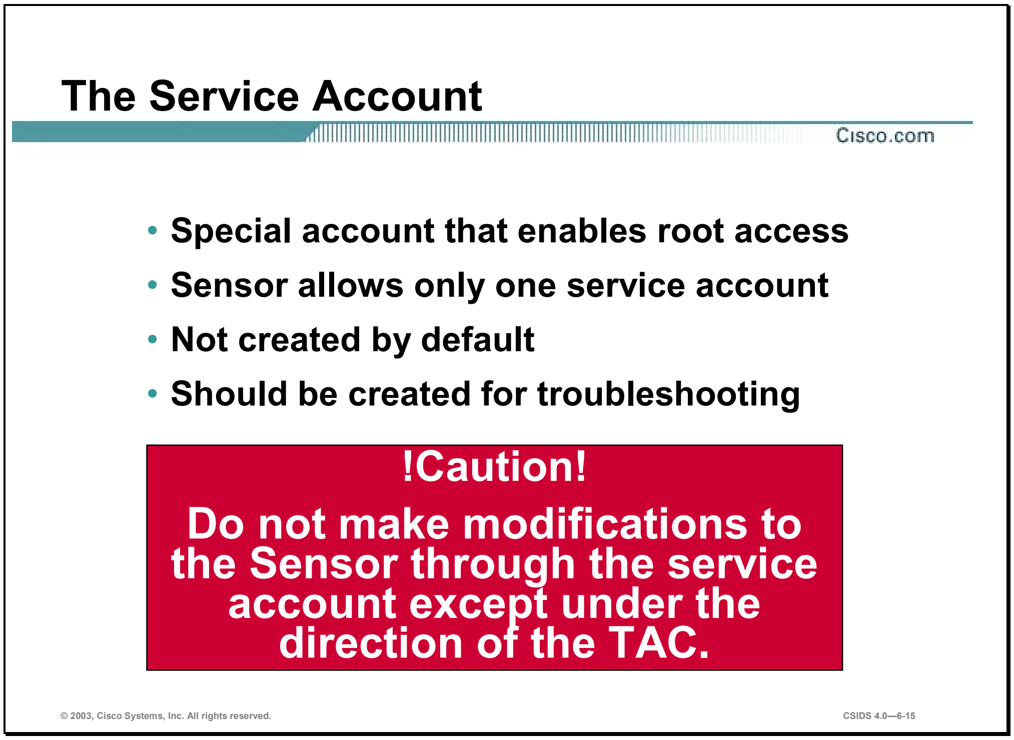
Cisco.com

- User accounts have roles.
- Roles determine the user’s privileges.
- The following roles can be assigned to an account:
  - Administrator
  - Operator
  - Viewer
  - Service

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—6-12

User accounts have roles that determine the operations the user is allowed to perform. For example, an administrative user can perform all of the operations on a Sensor, while a user with a viewer role can only view events and some Sensor configuration information. The following roles can be assigned to an account:

- Administrator—A user that can perform all operations on the Sensor.
- Operator—A user that can perform all viewing and some administrative operations on a Sensor.
- Viewer—A user that can perform all viewing operations such as viewing events and viewing some configuration files. The only administrative operation available to users with the viewer role is setting their own passwords.
- Service—A special role that allows the user to log into a native, operating system shell rather than a CLI shell. The service account and its role are discussed in the following section.



The Service Account

Cisco.com

- Special account that enables root access
- Sensor allows only one service account
- Not created by default
- Should be created for troubleshooting

!Caution!

Do not make modifications to the Sensor through the service account except under the direction of the TAC.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—6-15

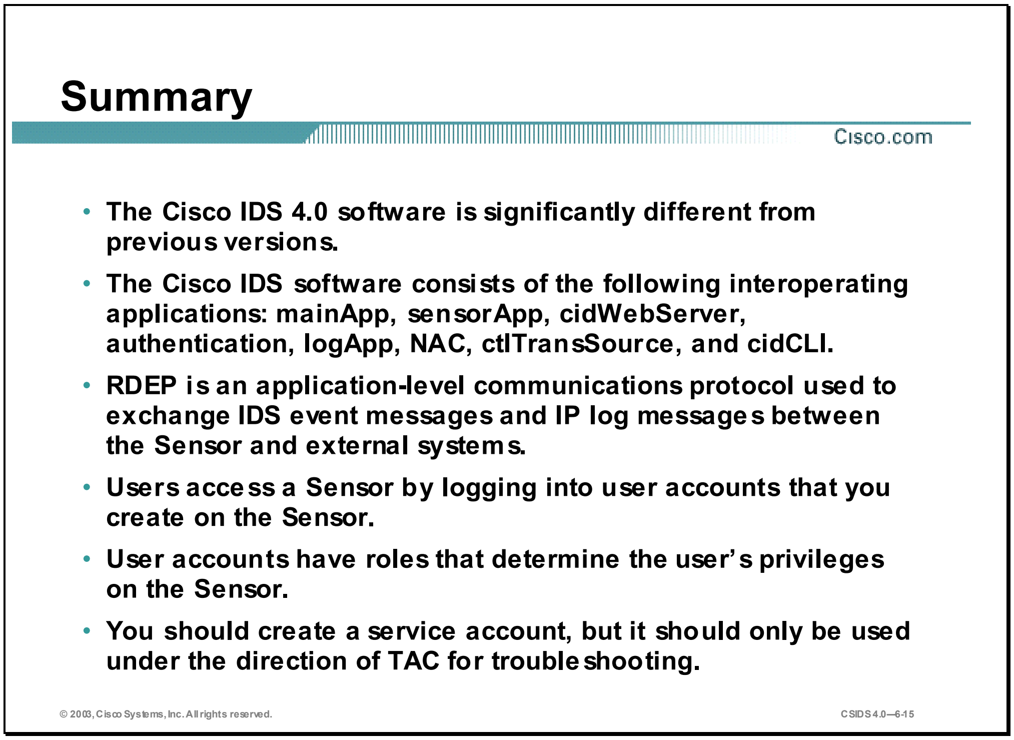
The service account is a special account that allows TAC to log into a native, operating system shell rather than a CLI shell. The purpose of the service account is not to support configuration but to support troubleshooting. By default, the service account does not exist on a Sensor; you must create it, and you should create it for TAC to use during troubleshooting. Root access to the Sensor is only possible if you log into the service account and su to the root account.

The Sensor allows only one service account. Consequently, the Sensor allows only one account to have a service role. When the service account's password is set or reset, the root account's password is automatically set to the same password. This enables the service account user to su to root using the same password. When the service account is removed, the root account's password is locked.

Do not make modifications to the Sensor through the service account except under the direction of TAC. If you use the service account to configure the Sensor, your configuration is not supported by TAC. Cisco does not support the addition or running of an additional service to the operating system through the service account, because it affects the proper performance and proper functioning of the other IDS services. To track logins to the service account, a log file named /var/log/.tac is automatically updated with a record of service account logins.

Summary

This section summarizes what you learned in this chapter.



Summary

Cisco.com

- The Cisco IDS 4.0 software is significantly different from previous versions.
- The Cisco IDS software consists of the following interoperating applications: mainApp, sensorApp, cidWebServer, authentication, logApp, NAC, ctlTransSource, and cidCLI.
- RDEP is an application-level communications protocol used to exchange IDS event messages and IP log messages between the Sensor and external systems.
- Users access a Sensor by logging into user accounts that you create on the Sensor.
- User accounts have roles that determine the user's privileges on the Sensor.
- You should create a service account, but it should only be used under the direction of TAC for troubleshooting.

CSIDS 4.0—6-15

7

Sensor Appliance Installation

Overview

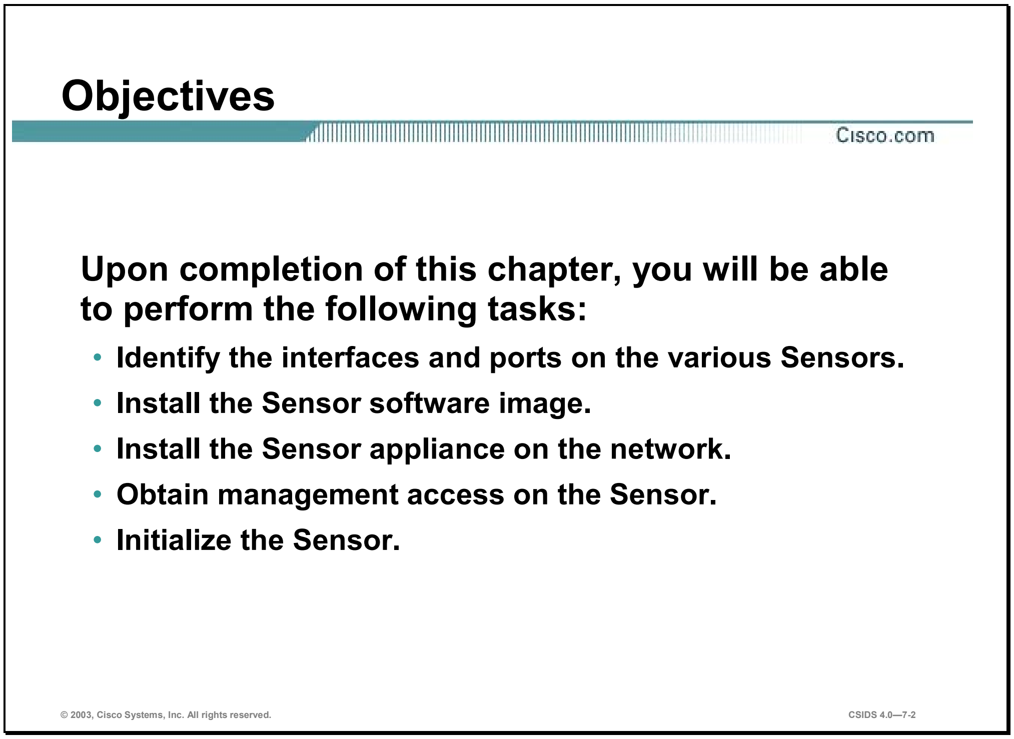
This chapter provides an overview of the Cisco Intrusion Detection System (IDS) Sensor appliances and explains the parameters that must be set to initialize the Sensor.

This chapter includes the following topics:

- Objectives
- Sensor appliances
- Sensor installation
- Sensor initialization
- Summary
- Lab exercise

Objectives

This section lists the chapter's objectives.



Objectives

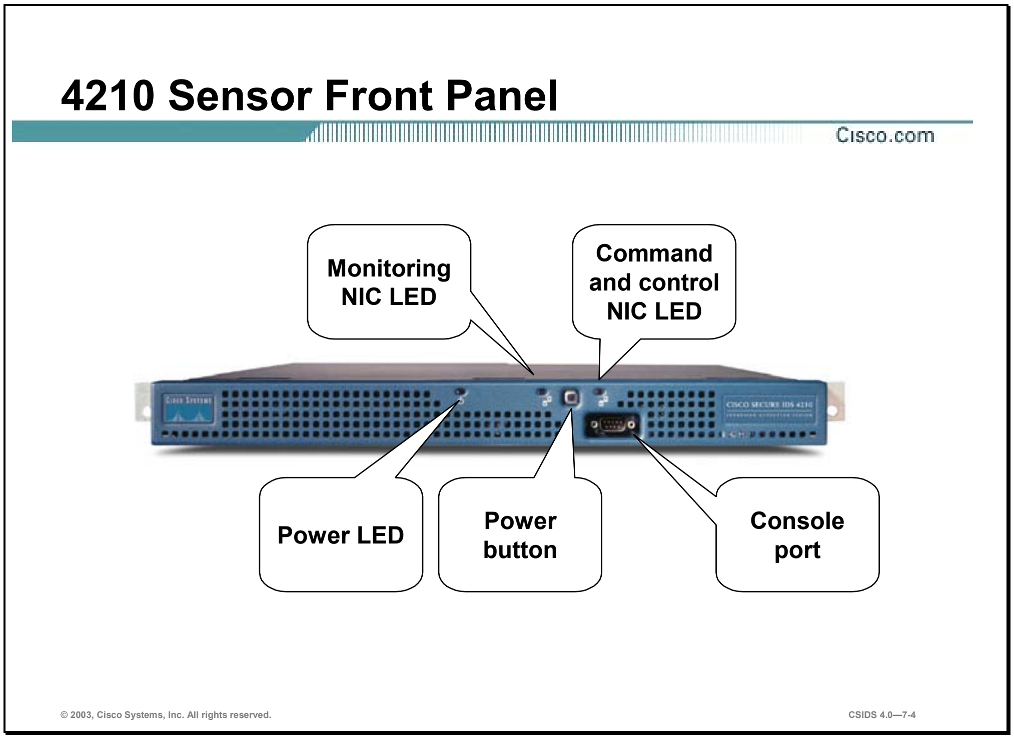
Upon completion of this chapter, you will be able to perform the following tasks:

- Identify the interfaces and ports on the various Sensors.
- Install the Sensor software image.
- Install the Sensor appliance on the network.
- Obtain management access on the Sensor.
- Initialize the Sensor.

CSIDS 4.0—7-2

Sensor Appliances

This section describes the Cisco IDS Sensor appliances features, connections, and interfaces.



4210 Sensor Front Panel

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—7-4

The following are the technical specifications for the Cisco IDS 4210 Sensor:

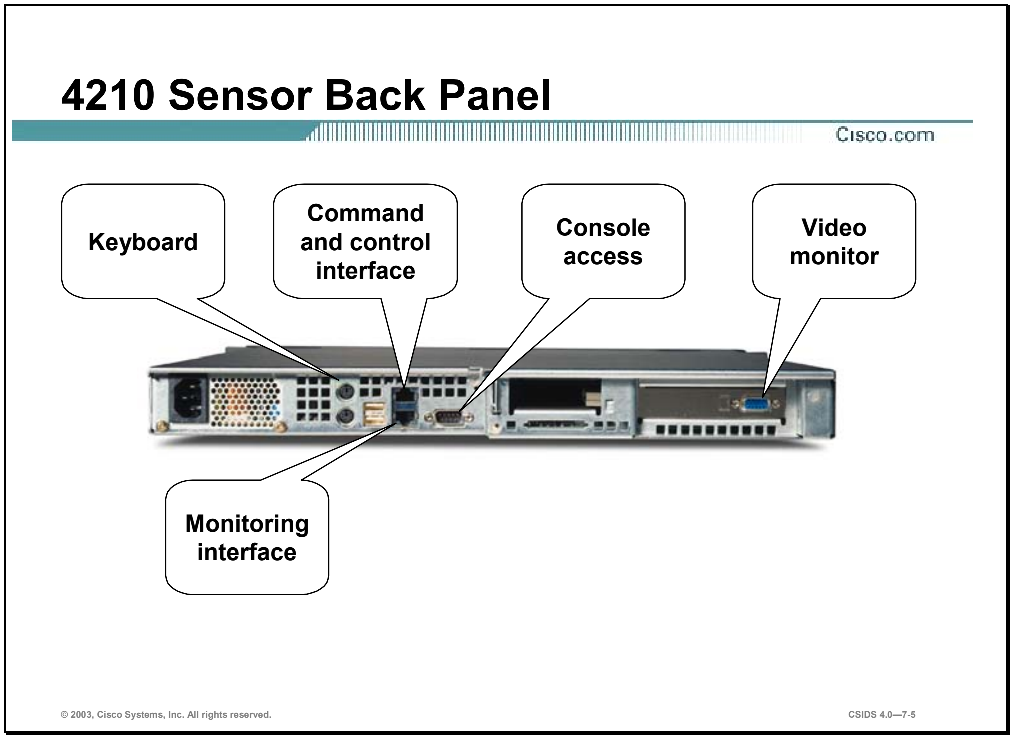
- Performance—45 Mbps
- Standard monitoring interface—10/100Base-T
- Standard command and control interface—10/100Base-T
- Optional interface—No
- Performance upgradable—Yes
- Form factor—1RU

The following are the physical dimensions for the Cisco IDS 4210 Sensor:

- Height—1.7 in. (4.32 cm)
- Width—16.8 in. (42.54 cm)
- Depth—22 in. (55.8 cm)

- Weight—23 lb (10.43 kg)

Note The interface LEDs are amber even if the Sensor is not powered on.



4210 Sensor Back Panel

Cisco.com

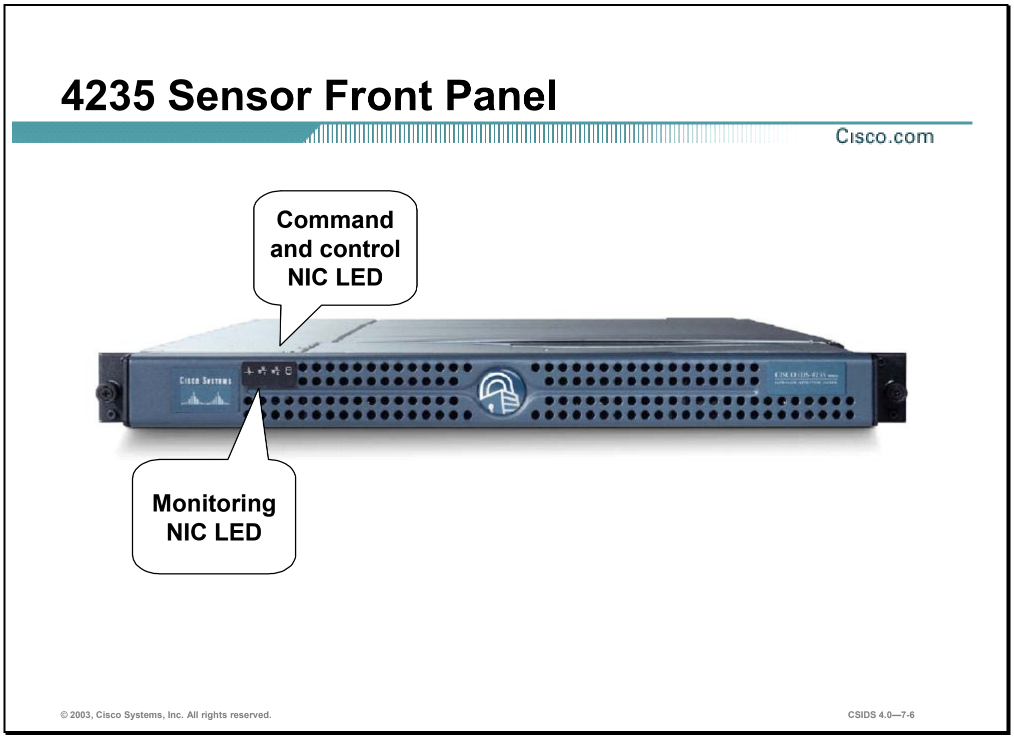
CSIDS 4.0—7-5

The back of the Cisco IDS 4210 Sensor has two Ethernet interfaces. The top interface is the command and control interface, and the bottom interface is the monitoring interface. The following is the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int0

In addition to the interfaces, the 4210 Sensors give you access to the keyboard port, the console access port, and the video monitor port.

Be sure to read and understand all safety requirements listed in the Cisco Intrusion Detection System Sensor Installation and Safety Note, which can be found at: www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/sensor/7016_04.htm.



4235 Sensor Front Panel

Cisco.com

Command and control NIC LED

Monitoring NIC LED

CSIDS 4.0—7-6

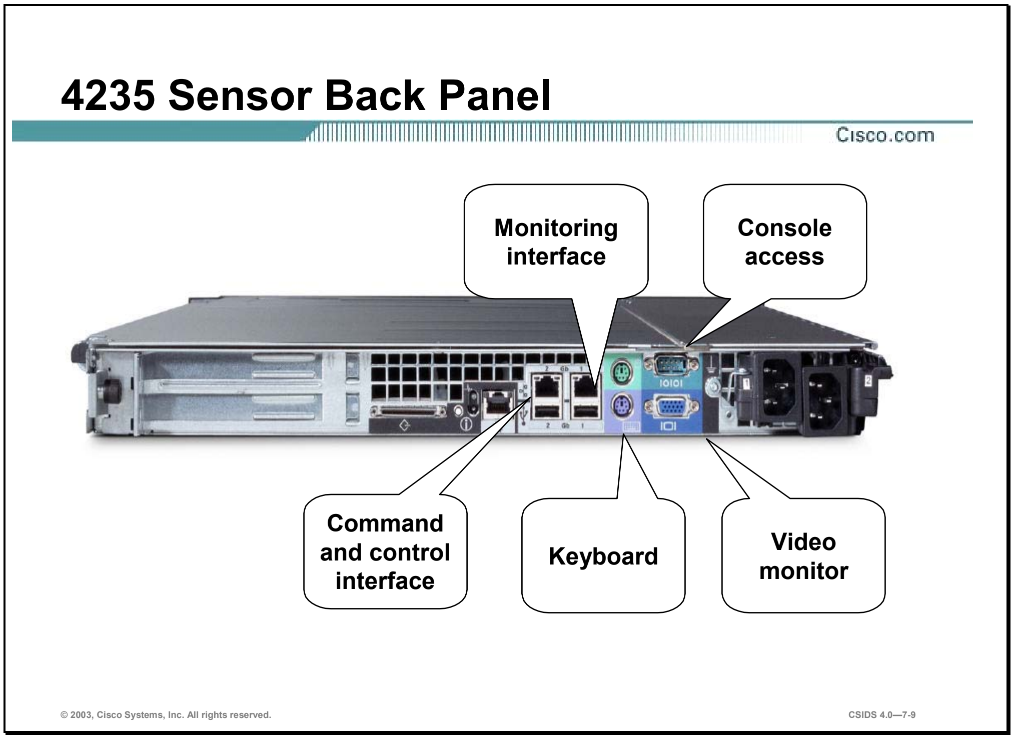
The following are the technical specifications for the Cisco IDS 4235 Sensor:

- Performance—200 Mbps
- Standard monitoring interface—10/100/1000Base-TX
- Standard command and control interface—10/100/1000Base-TX
- Optional interface—No
- Performance upgradeable—No
- Form factor—1RU

The following are the physical dimensions for the Cisco IDS 4235 Sensor:

- Height—1.67 in. (4.24 cm)
- Width—17.6 in. (44.70 cm)
- Depth—27.0 in. (68.58 cm)
- Weight—35 lb (15.88 kg)

Note The power button is under the front cover.



4235 Sensor Back Panel

Cisco.com

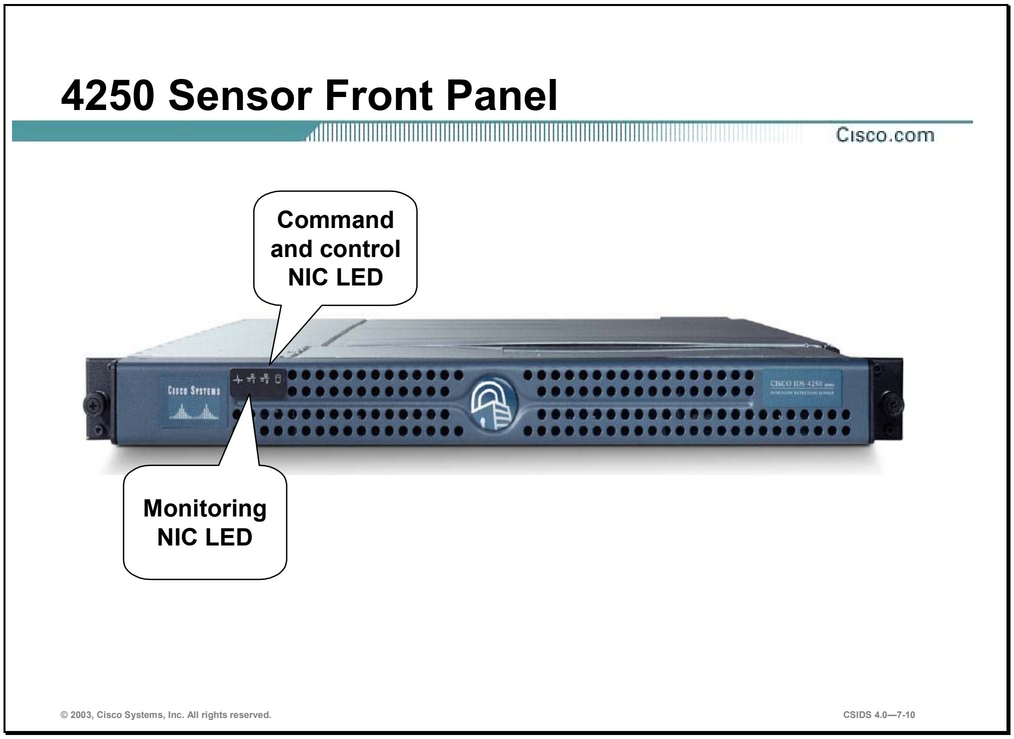
CSIDS 4.0—7-9

The back of the Cisco IDS 4235 Sensor has two Ethernet interfaces. The interface numbered 1 is the monitoring interface, and interface numbered 2 is the command and control interface. The following is the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int0

In addition to the interfaces, the 4235 Sensors give you access to the keyboard port, the console access port, and the video monitor port.

Be sure to read and understand all safety requirements listed in the Cisco Intrusion Detection System Sensor Installation and Safety Note, which can be found at: www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/sensor/7016_04.htm.



4250 Sensor Front Panel

Cisco.com

Command and control NIC LED

Monitoring NIC LED

CSIDS 4.0—7-10

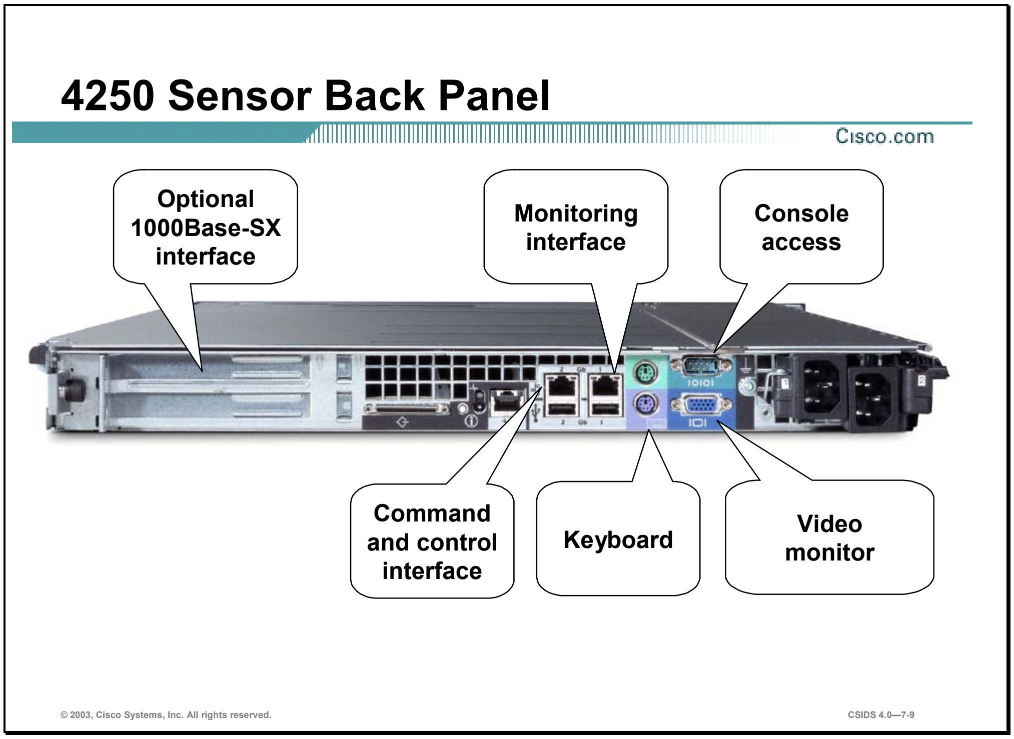
The following are the technical specifications for the Cisco IDS 4250 Sensor:

- Performance—500 Mbps
- Standard monitoring interface—10/100/1000Base-TX
- Standard command and control interface—10/100/1000Base-TX
- Optional interface—1000Base-SX (fiber)
- Performance upgradeable—Yes
- Form factor—1RU

The following are the physical dimensions for the Cisco IDS 4250 Sensor:

- Height—1.67 in. (4.24 cm)
- Width—17.6 in. (44.70 cm)
- Depth—27.0 in. (68.58 cm)
- Weight—35 lb (15.88 kg)

Note The power button is under the front cover.



4250 Sensor Back Panel

CSIDS 4.0—7-9

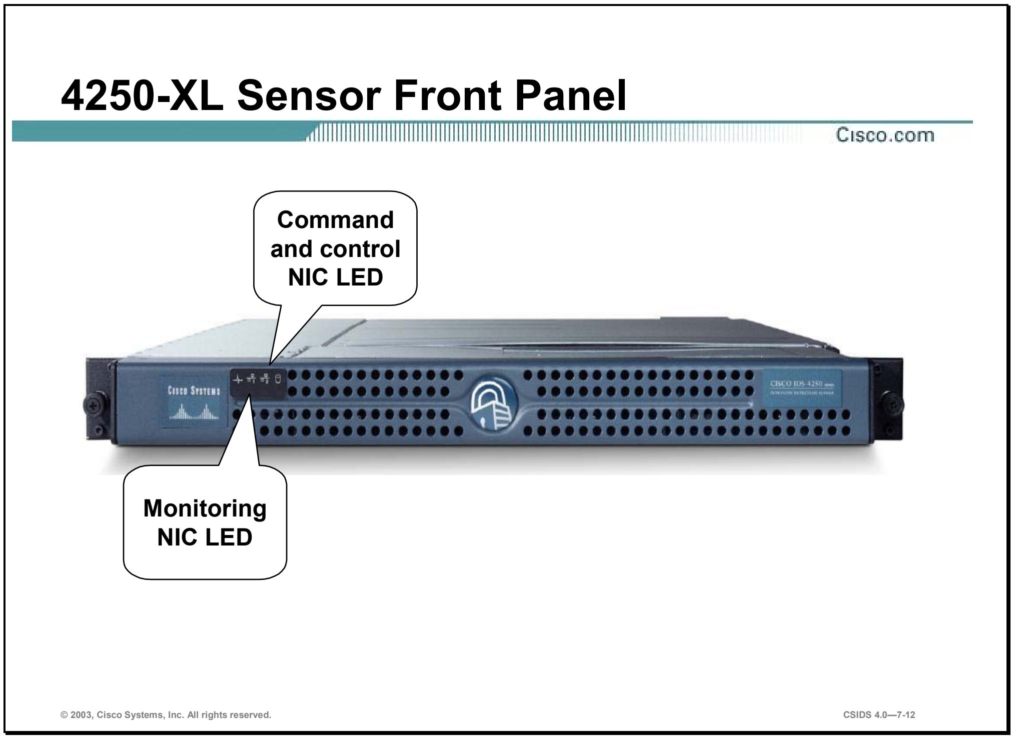
The back of the Cisco IDS 4250 Sensor has two Ethernet interfaces. The interface numbered 1 is the monitoring interface, and the interface numbered 2 is the command and control interface. The following is the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int0

In addition to the interfaces, the 4250 Sensors give you access to the keyboard port, the console access port, and the video monitor port.

Be sure to read and understand all safety requirements listed in the Cisco Intrusion Detection System Sensor Installation and Safety Note, which can be found at: www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/sensor/7016_04.htm.

Note IDS 4.0 is supported on the 4210, 4220, 4230, 4235, 4250, and 4250-XL Sensor models. However, the IDS 4220 and 4230 platforms have reached end-of-sale status; they cannot be ordered.



4250-XL Sensor Front Panel

Cisco.com

CSIDS 4.0—7-12

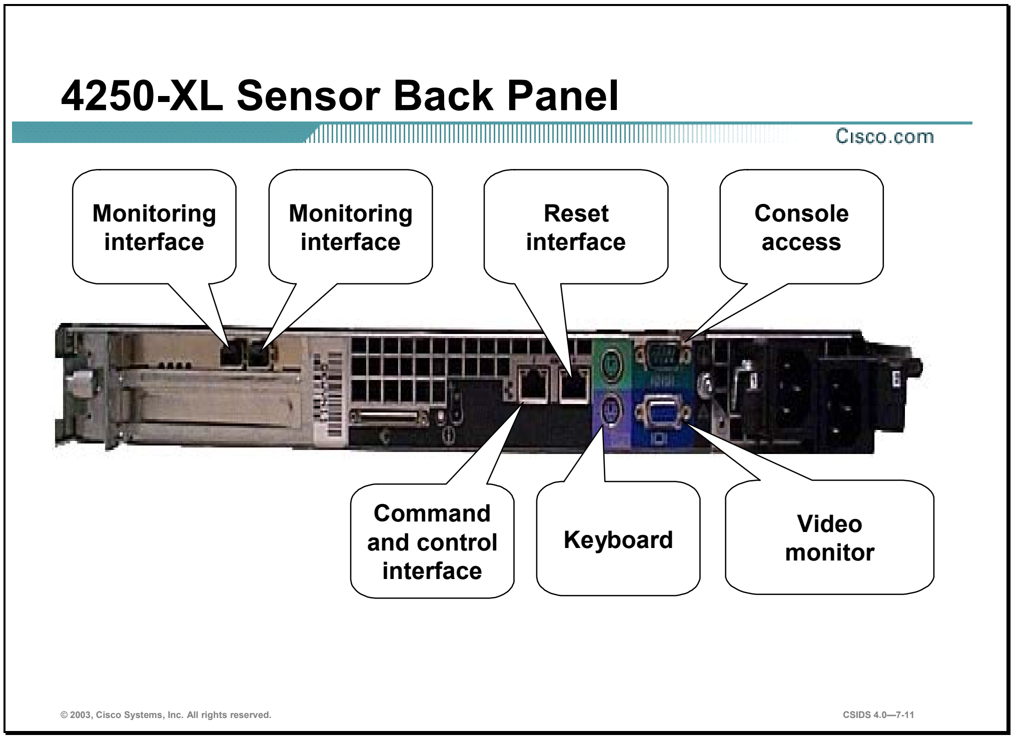
The following are the technical specifications for the Cisco IDS 4250-XL Sensor:

- Performance—1000 Mbps
- Standard monitoring interface—Dual 1000BASE-SX interface with MTRJ
- Standard command and control interface—10/100/1000Base-TX
- TCP reset interface—10/100/1000-TX
- Optional interface—1000Base-SX (fiber)
- Performance upgradeable—No
- Form factor—1RU

The following are the physical dimensions for the Cisco IDS 4250-XL Sensor:

- Height—1.67 in. (4.24 cm)
- Width—17.6 in. (44.70 cm)
- Depth—27.0 in. (68.58 cm)
- Weight—35 lb (15.88 kg)

Note The power button is under the front cover.



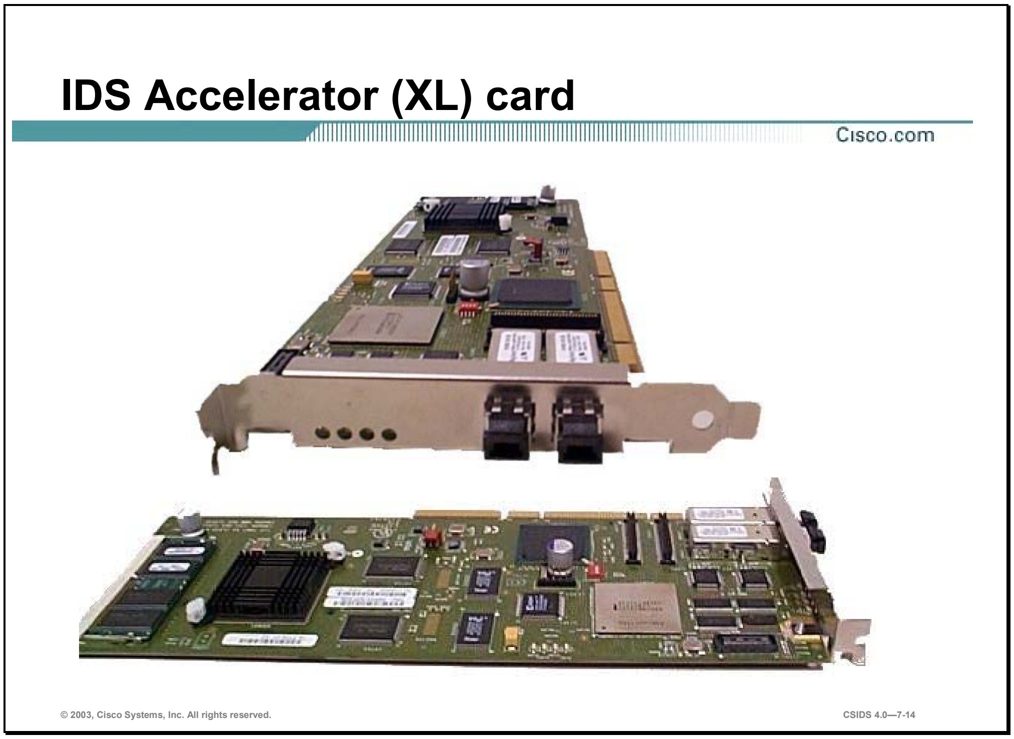
4250-XL Sensor Back Panel

CSIDS 4.0—7-11

The back of the Cisco IDS 4250-XL Sensor has four Ethernet interfaces. The interface numbered 1 is the TCP reset interface, and the interface numbered 2 is the command and control interface. The two interfaces on the XL card are monitoring interfaces. The following is the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int2 and int3

In addition to the interfaces, the 4250-XL Sensors give you access to the keyboard port, the console access port, and the video monitor port.



IDS Accelerator (XL) card

CSIDS 4.0—7-14

The 4250-XL Sensor is a 4250 appliance with an IDS Accelerator (XL) Card already installed. The XL card, which supports gigabit sensing, is a hardware acceleration option for the 4250 Sensor.

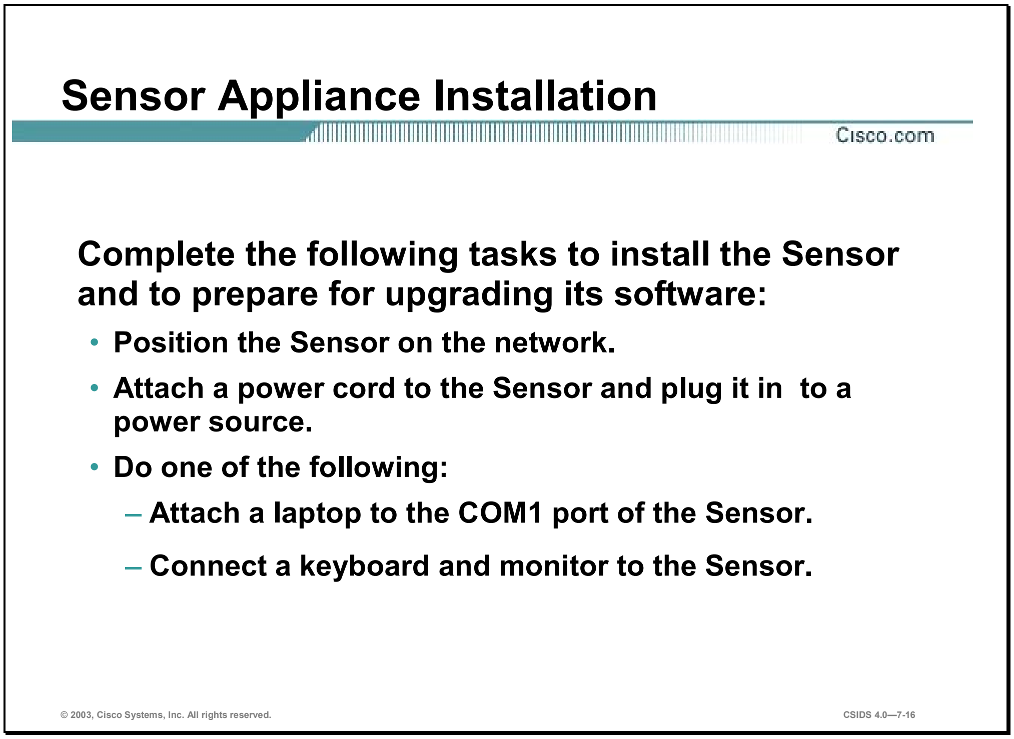
You can install the XL card in the upper PCI slot on the 4250 appliances. Placement of the XL card in the bottom PCI slot is not a supported configuration.

After you install the XL card, the monitoring interface connectors are on the XL card. The XL interface is not supported as a command and control interface.

For detailed instructions on installing the XL card in your 4250 Sensor, refer to the Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0.

Sensor Installation

This section explains how to upgrade a Sensor to IDS version 4.0.



Sensor Appliance Installation

Cisco.com

Complete the following tasks to install the Sensor and to prepare for upgrading its software:

- **Position the Sensor on the network.**
- **Attach a power cord to the Sensor and plug it in to a power source.**
- **Do one of the following:**
  - **Attach a laptop to the COM1 port of the Sensor.**
  - **Connect a keyboard and monitor to the Sensor.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—7-16

Complete the following steps to install the IDS appliance:

Step 1 Position the IDS appliance on the network.

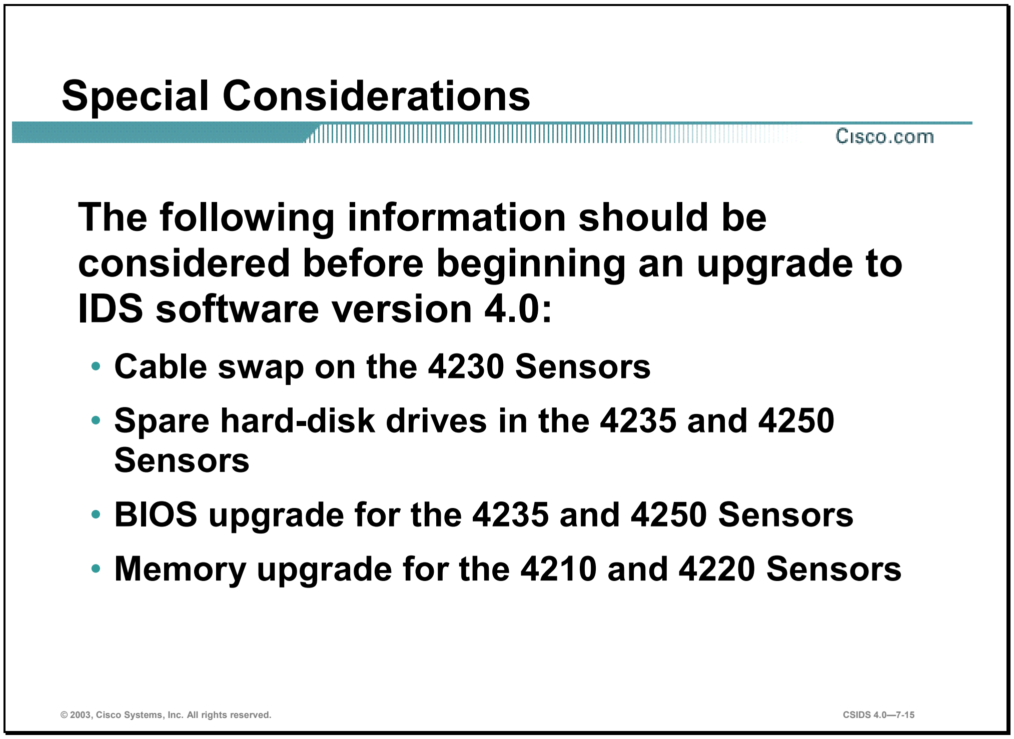
Step 2 Attach the power cord to the IDS appliance and plug it into a power source (a UPS is recommended).

Note When you first plug a 4210 appliance into a power source, it powers on momentarily and then powers off leaving the NIC link lights on. This is normal behavior. Press the power switch to boot the system into operation.

Step 3 Use the dual serial communication cable included in the accessory kit to attach a laptop to the COM1 port of the IDS appliance or connect a keyboard and monitor to the IDS appliance. It is recommended that you use the dual serial communication cable rather than a keyboard and monitor, because some keyboards and monitors are incompatible with the IDS appliance. If you use a keyboard and monitor, choose from the following recommended keyboards and monitors:

- Keyboards
  - KeyTronic E03601QUS201-C
  - KeyTronic LT DESIGNER

- Monitors
  - MaxTech XT-7800
  - Dell D1025HT



Special Considerations

Cisco.com

The following information should be considered before beginning an upgrade to IDS software version 4.0:

- **Cable swap on the 4230 Sensors**
- **Spare hard-disk drives in the 4235 and 4250 Sensors**
- **BIOS upgrade for the 4235 and 4250 Sensors**
- **Memory upgrade for the 4210 and 4220 Sensors**

CSIDS 4.0—7-15

- Cable swap on the 4230 Sensors—If you are upgrading a 4230 appliance to software version 4.0, you must swap the command and control interface cable with the sniffing interface cable before you upgrade the software. For IDS software version 4.0, the former command and control interface is now the sniffing interface. If the cables on the 4230 are not swapped, you may not be able to connect to your appliance through the network.

- Spare hard-disk drives in the 4235 and 4250 Sensors—Installing a second hard-disk drive in a 4235 or 4250 Sensor may render the Sensor unable to recognize the **recover** command used for re-imaging the appliance. Spare hard-disk drives are meant to be replacements for the original hard-disk drives and are not meant to be used along with the original hard-disk drive.

- BIOS upgrade for the 4235 and 4250 Sensors—BIOS version A04 or later is required to run IDS 4.0 on the 4235 and 4250 appliances. You must apply the BIOS upgrade before installing the 4.0 software. If the BIOS upgrade is not applied, these appliances can hang during the boot process. You cannot upgrade the BIOS from a console connection. You must connect a keyboard and monitor to the appliance so that you can see the output on the monitor.

- Memory upgrade for the 4210 and 4220 Sensors—The 4210 and 4220 Sensors require a 256 MB RAM memory upgrade, for a total of 512 MB RAM, to run IDS 4.1. This upgrade is also recommended for IDS 4.0.

Complete the following steps to create and boot the 4235 or 4250 BIOS upgrade diskette:

Step 1 Copy BIOS_A04.exe to a Windows system.

Note You can find this file in the /BIOS directory on the Cisco Intrusion Detection System 4.0 Upgrade/Recovery CD, or you can download it from Cisco.com.

Step 2 Insert a blank 1.44-MB diskette in the Windows system.

Step 3 Double-click the downloaded BIOS update file, BIOS_A04.exe, on the Windows system to generate the BIOS update diskette.

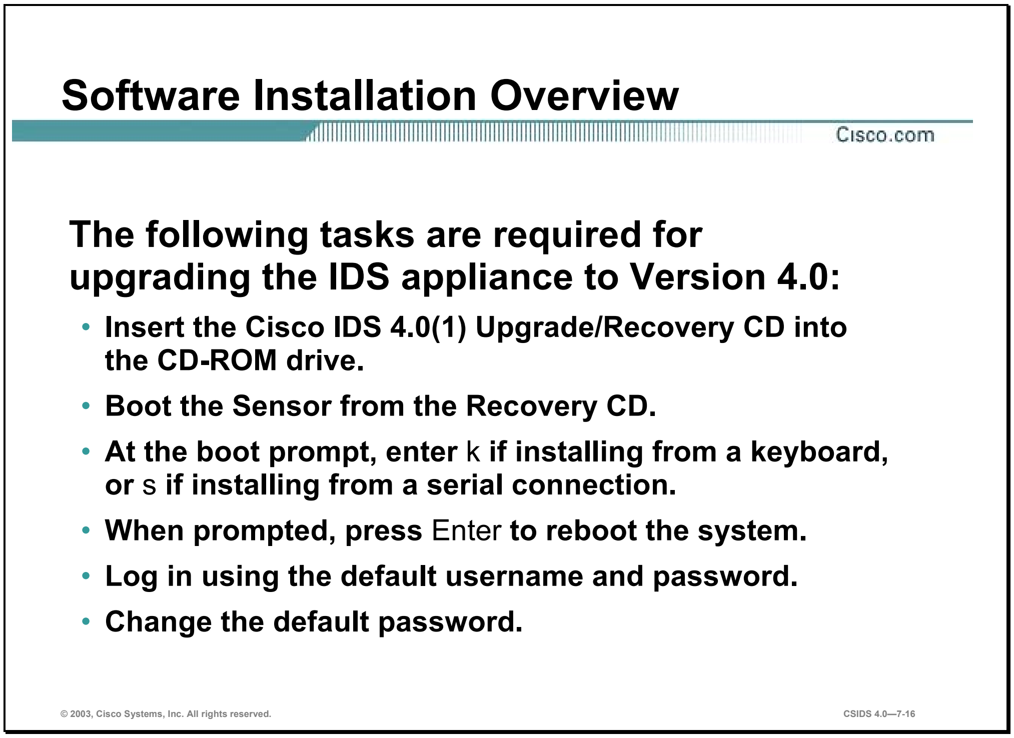
Step 4 Insert the newly created BIOS update diskette in your IDS-4235 or IDS-4250.

Caution Do not power off or manually reboot the appliance during Step 5.

Step 5 Boot the IDS appliance and follow the on-screen instructions.

Step 6 Remove the BIOS update diskette from the appliance while the appliance is rebooting, otherwise the BIOS upgrade will be started again.

Caution Do not apply this BIOS upgrade to appliance models other than the 4235 and 4250.



Software Installation Overview

Cisco.com

The following tasks are required for upgrading the IDS appliance to Version 4.0:

- **Insert the Cisco IDS 4.0(1) Upgrade/Recovery CD into the CD-ROM drive.**
- **Boot the Sensor from the Recovery CD.**
- **At the boot prompt, enter** k **if installing from a keyboard, or** s **if installing from a serial connection.**
- **When prompted, press** Enter **to reboot the system.**
- **Log in using the default username and password.**
- **Change the default password.**

CSIDS 4.0—7-16

To upgrade an IDS appliance from IDS software version 3.X to version 4.0, you must install the new 4.0 image from the 4.0 CD. Complete the following steps to upgrade from IDS 3.X software to 4.0 software:

Step 1 Insert the IDS 4.0(1) Upgrade/Recovery CD into the CD-ROM drive.

Step 2 Boot from the CD.

Step 3 When presented with a boot: prompt, enter **k** to specify that you are using a keyboard and monitor for the installation. Enter **s** if you are using a serial connection.

Step 4 Remove the CD and reboot when the process is complete.

Step 5 Log in from the console or serial terminal using the default user **cisco** with the password **cisco**.

Step 6 Change the default password. The default password must be changed on the first login. The Sensor forces the use of strong passwords at least 8 characters long.

Once the password is successfully set, you are logged into the CLI shell. From there, run the **setup** command to perform the initial configuration.

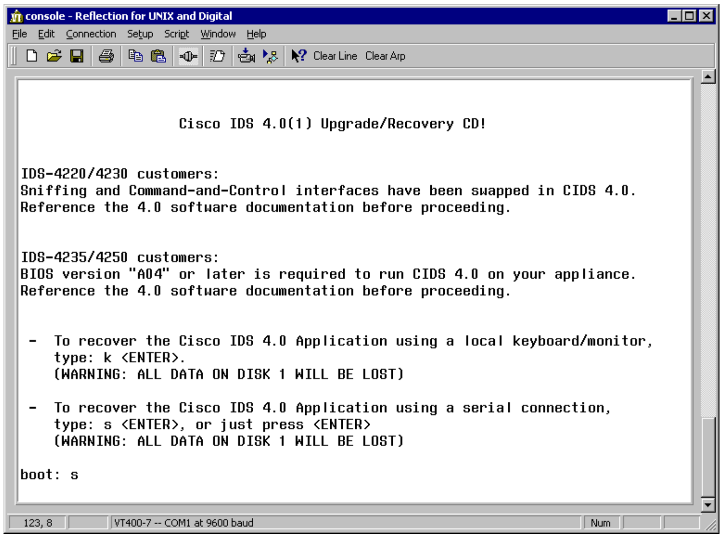
Signature updates, which include the Network Security Database (NSDB), occur every two weeks. You may not have the latest signature update on the 4.0 CD. You can find the IDS Event Viewer, signature updates, service pack updates, BIOS upgrades, Readmes, and other version 4.0 software updates on Cisco.com at the following website:

`http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/`

Signature updates and service packs occur as the product is upgraded. Check Cisco.com regularly to get the latest signature and service pack updates. You need a Cisco.com password to download updates. See the "Applying for a Cisco.com Account with Cryptographic Access" section of the Release Notes for information on obtaining a Cisco.com account with cryptographic access.

Installation from the CD overwrites all data on the drive. You will need your configuration information to initialize your appliance with the 4.0 software. The IDS MC provides an easy way to capture the configuration and data on the Sensor for import into 4.0.

Installation Options


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
123, 8
VT400-7 -- COM1 at 9600 baud
Num

```
                   Cisco IDS 4.0(1) Upgrade/Recovery CD!


IDS-4220/4230 customers:
Sniffing and Command-and-Control interfaces have been swapped in CIDS 4.0.
Reference the 4.0 software documentation before proceeding.


IDS-4235/4250 customers:
BIOS version "A04" or later is required to run CIDS 4.0 on your appliance.
Reference the 4.0 software documentation before proceeding.


 -  To recover the Cisco IDS 4.0 Application using a local keyboard/monitor,
    type: k <ENTER>.
    (WARNING: ALL DATA ON DISK 1 WILL BE LOST)

 -  To recover the Cisco IDS 4.0 Application using a serial connection,
    type: s <ENTER>, or just press <ENTER>
    (WARNING: ALL DATA ON DISK 1 WILL BE LOST)

boot: s
```

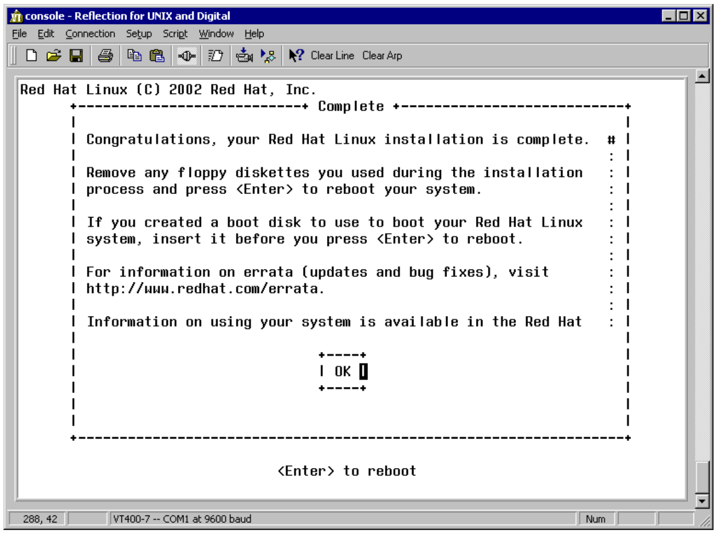
CSIDS 4.0—7-19

The figure shows the information displayed when you boot from the IDS 4.0 upgrade/recovery CD. You are required to indicate which of the following two methods you are using for the upgrade or recovery:

- Keyboard and monitor—Enter **k** and press <**Enter**> to specify that you are using a keyboard and monitor.

- Serial connection—Enter **s** and press <**Enter**>to specify that you are using a serial connection. Pressing <**Enter**> alone also specifies serial connection.

Installation Complete


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
288, 42
VT400-7 -- COM1 at 9600 baud
Num

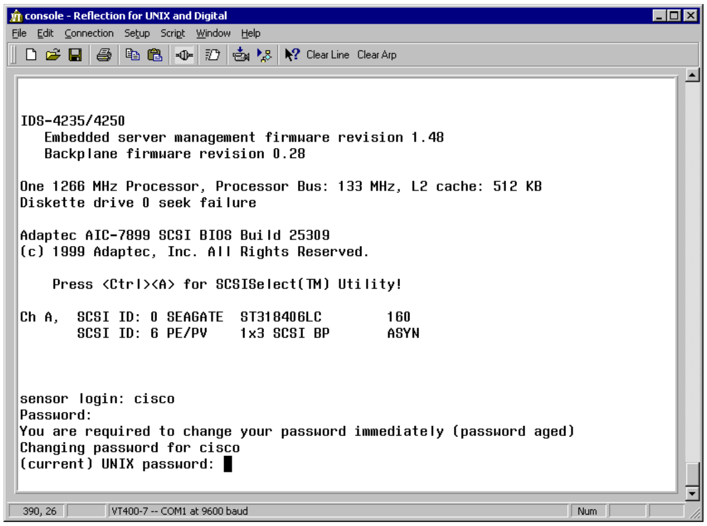
```
Red Hat Linux (C) 2002 Red Hat, Inc.
       +---------------------------+ Complete +---------------------------+
       |                                                                   |
       | Congratulations, your Red Hat Linux installation is complete.  #  |
       |                                                                :  |
       | Remove any floppy diskettes you used during the installation   :  |
       | process and press <Enter> to reboot your system.               :  |
       |                                                                :  |
       | If you created a boot disk to use to boot your Red Hat Linux   :  |
       | system, insert it before you press <Enter> to reboot.          :  |
       |                                                                :  |
       | For information on errata (updates and bug fixes), visit       :  |
       | http://www.redhat.com/errata.                                  :  |
       |                                                                :  |
       | Information on using your system is available in the Red Hat   :  |
       |                                                                   |
       |                              +----+                               |
       |                              | OK |                               |
       |                              +----+                               |
       |                                                                   |
       |                                                                   |
       +-------------------------------------------------------------------+

                             <Enter> to reboot
```

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—7-20

The screen in the figure appears when the installation is complete. Press **Enter** to reboot the Sensor.

Change Password

Cisco.com


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
390, 26
VT400-7 -- COM1 at 9600 baud
Num

```
IDS-4235/4250
   Embedded server management firmware revision 1.48
   Backplane firmware revision 0.28

One 1266 MHz Processor, Processor Bus: 133 MHz, L2 cache: 512 KB
Diskette drive 0 seek failure

Adaptec AIC-7899 SCSI BIOS Build 25309
(c) 1999 Adaptec, Inc. All Rights Reserved.

    Press <Ctrl><A> for SCSISelect(TM) Utility!

Ch A,  SCSI ID: 0 SEAGATE  ST318406LC        160
       SCSI ID: 6 PE/PV    1x3 SCSI BP       ASYN



sensor login: cisco
Password:
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password:
```

CSIDS 4.0—7-21

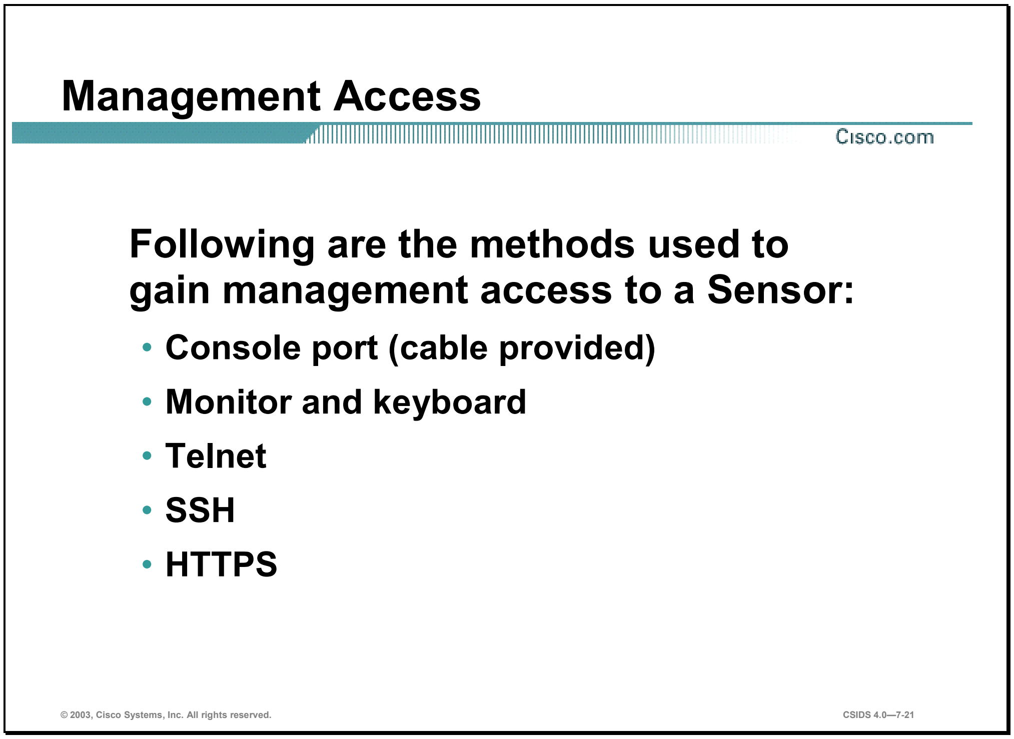
The figure shows the prompt for changing the default password. After the system reboots, log in as user **cisco** with the password **cisco**. The following prompt appears:

```
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password:
```

Enter the password **cisco** again at this prompt. You will then be allowed to enter and confirm a new password.

Sensor Initialization

This section describes how to initialize the Cisco IDS Sensor appliance.



Management Access

Cisco.com

Following are the methods used to gain management access to a Sensor:

- Console port (cable provided)
- Monitor and keyboard
- Telnet
- SSH
- HTTPS

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—7-21

Following are the methods used to gain management access to a Sensor:

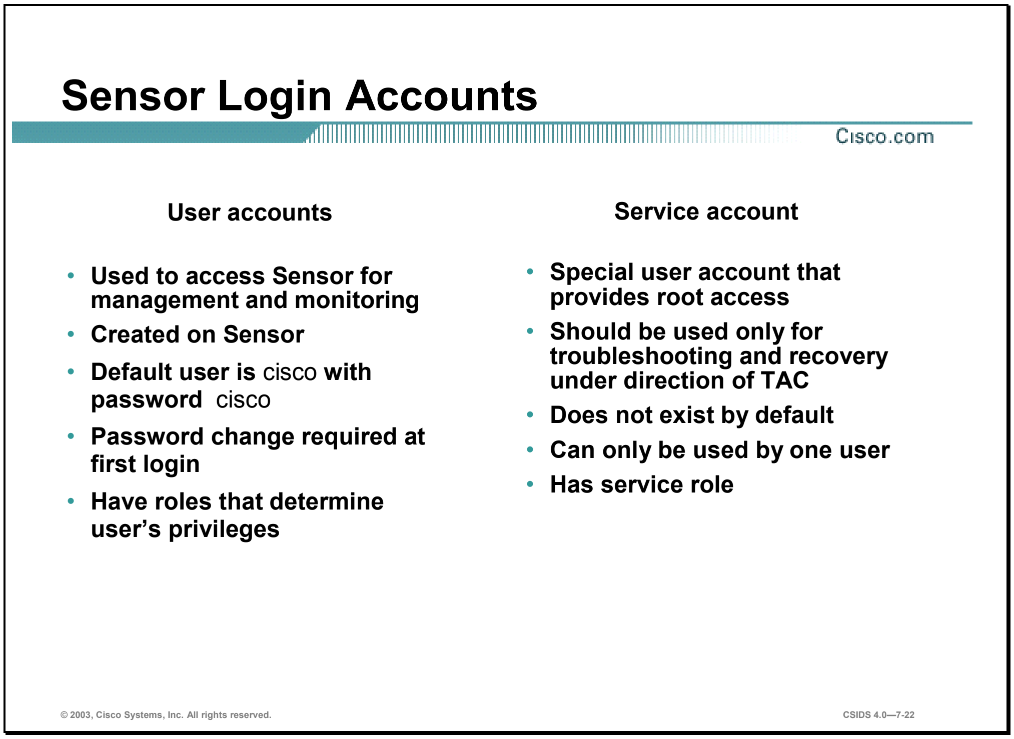
- Console port—Requires the use of the RS-232 cable provided with the Sensor and a terminal emulation program such as HyperTerminal.

- Monitor and keyboard—Requires connecting a monitor and a keyboard directly to the Sensor.

- Telnet—Requires an IP address that has been assigned to the command and control interface via the CLI **setup** command. Must be enabled to allow Telnet access. Telnet is disabled by default.

- SSH—Requires an IP address that has been assigned to the command and control interface via the CLI **setup** command and uses a supported SSH client. The SSH server in the Sensor is enabled by default.

- HTTPS—Requires an IP address that has been assigned to the command and control interface via the CLI **setup** command and uses a supported web browser. HTTPS is enabled by default but can be disabled.



Sensor Login Accounts

Cisco.com

User accounts

- **Used to access Sensor for management and monitoring**
- **Created on Sensor**
- **Default user is** cisco **with password** cisco
- **Password change required at first login**
- **Have roles that determine user's privileges**

Service account

- **Special user account that provides root access**
- **Should be used only for troubleshooting and recovery under direction of TAC**
- **Does not exist by default**
- **Can only be used by one user**
- **Has service role**

CSIDS 4.0—7-22

Following are the two types of management accounts and their characteristics:

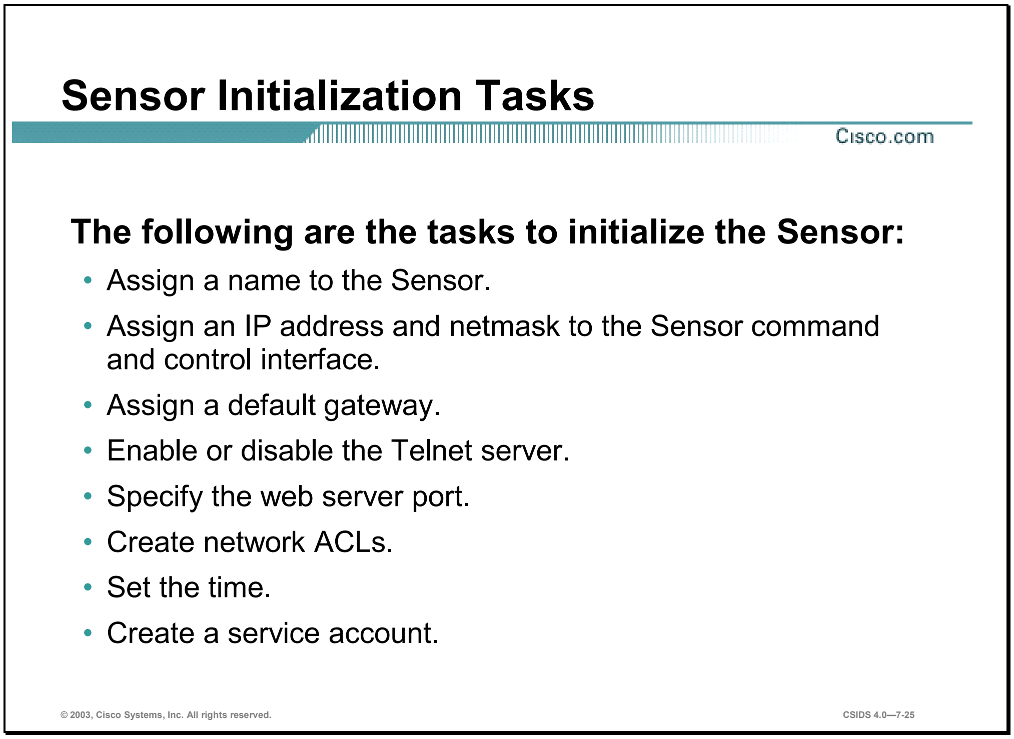
- User accounts—Enables you to access the Sensor for management and monitoring purposes. User accounts do not allow you to log in to the native, operating system shell. Logging in to a user account enables you to access the Sensor and manage or monitor it via the CLI or a management console.

User accounts can be created locally on the Sensor by using the CLI or a management console. Management consoles can also maintain user accounts independently from Sensors. For example, you can create and log in to accounts that exist only on the IDS MC. The IDS MC accesses the Sensor through a different account that is recognized by the Sensor.

The Sensor allows you to create multiple local user accounts. The default username and password is **cisco**. You are required to change the default password the first time you log on.

- Service account—Enables you to log into a native operating system shell rather than a CLI shell. This account is intended to support troubleshooting, not configuration. Only one user is allowed this privilege. When you create a user with service privileges, the service account is created and its password is set. When the service account's password is set or reset, the root account's password is automatically set to the same password. This allows the service account to access the root account using the same password.

When you log in to the service account, you obtain a bash shell. From the bash shell, you can use the **su** command to access the root account. You cannot log into the root account directly.



Sensor Initialization Tasks

Cisco.com

The following are the tasks to initialize the Sensor:

- Assign a name to the Sensor.
- Assign an IP address and netmask to the Sensor command and control interface.
- Assign a default gateway.
- Enable or disable the Telnet server.
- Specify the web server port.
- Create network ACLs.
- Set the time.
- Create a service account.

CSIDS 4.0—7-25

Some of the tasks involved in initializing the Sensor are done via an interactive dialog initiated by the **setup** command. The following are those tasks:

- Assign the Sensor a host name.
- Assign an IP address and a subnet mask to the command and control interface.
- Assign a default route.
- Enable or disable the Telnet server.
- Specify the web server port.

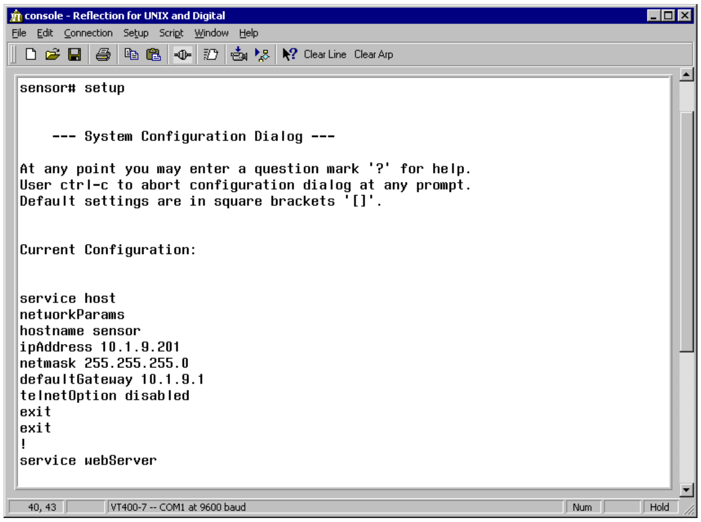
Other initialization tasks include the following:

- Modify the network ACLs to allow remote access. You can identify trusted hosts that are allowed to connect to the Sensor.
- Set the system clock.
- Create a service account for TAC to use during troubleshooting.

Note	If you later change the Sensor's IP address, you will need to generate a self-signed X.509 certificate. This certificate is needed by HTTPS communications.

setup **Command**

Cisco.com



console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
40, 43
VT400-7 -- COM1 at 9600 baud
Num
Hold

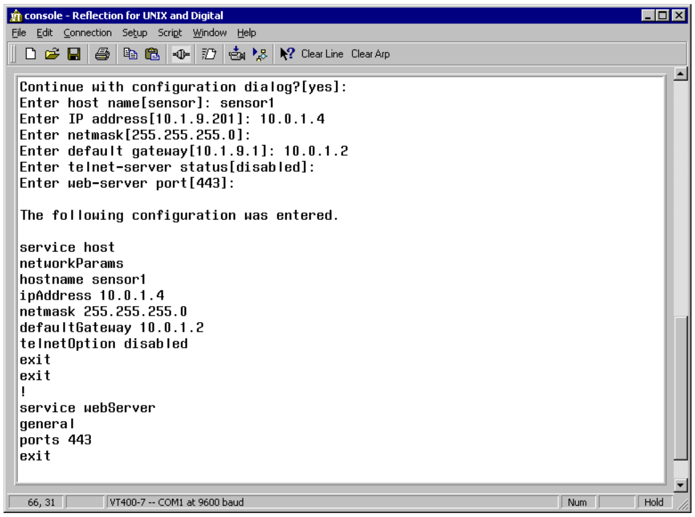
```
sensor# setup


    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
networkParams
hostname sensor
ipAddress 10.1.9.201
netmask 255.255.255.0
defaultGateway 10.1.9.1
telnetOption disabled
exit
exit
!
service webServer
```

CSIDS 4.0—7-26

Most of the initialization tasks are accomplished by using the Sensor's **setup** command. Setup replaces the pre-4.0 sysconfig-sensor script. It walks you through configuring the host name, IP address, netmask, gateway and communications options. After you enter the **setup** command, the default settings are displayed. Press the **spacebar** to continue. The following question appears: Continue with configuration dialog? [yes].

Configuration Dialog

Cisco.com


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
66, 31
VT400-7 -- COM1 at 9600 baud
Num
Hold

```
Continue with configuration dialog?[yes]:
Enter host name[sensor]: sensor1
Enter IP address[10.1.9.201]: 10.0.1.4
Enter netmask[255.255.255.0]:
Enter default gateway[10.1.9.1]: 10.0.1.2
Enter telnet-server status[disabled]:
Enter web-server port[443]:

The following configuration was entered.

service host
networkParams
hostname sensor1
ipAddress 10.0.1.4
netmask 255.255.255.0
defaultGateway 10.0.1.2
telnetOption disabled
exit
exit
!
service webServer
general
ports 443
exit
```

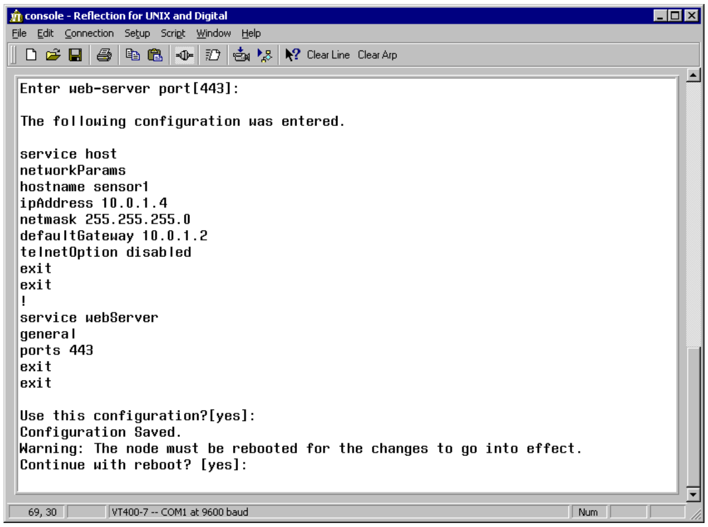
Enter **yes** to continue with the configuration dialog.

```
Continue with configuration dialog? [yes]: yes
```

The figure shows the configuration dialog presented by setup. The configuration dialog is an interactive dialog. Enter the following information:

- Host name—The host name is a case-sensitive character string up to 256 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.
- IP address—An IP address is a 32-bit address written as four octets separated by periods, X.X.X.X, where X = 0–255. The default is 10.1.9.201.
- Netmask—The netmask is a 32-bit address written as four octets separated by periods, X.X.X.X, where X = 0–255. The default for a Class C address is 255.255.255.0.
- Default gateway—The default gateway is the default router IP address for the appliance. The default is 10.1.9.1.
- Telnet server status—You can disable or enable Telnet services. The default is disabled.
- Web server port—The web server port is the TCP port used by the web server (1 to 65535). The default is 443. If you change the web server port, you must specify the port in the URL address of your browser when you connect to IDM, in the format https://sensor ip address:port (for example, https://10.1.9.201:1040).

Save and Reboot


console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
Clear Line Clear Arp
69, 30
VT400-7 -- COM1 at 9600 baud
Num

```
Enter web-server port[443]:

The following configuration was entered.

service host
networkParams
hostname sensor1
ipAddress 10.0.1.4
netmask 255.255.255.0
defaultGateway 10.0.1.2
telnetOption disabled
exit
exit
!
service webServer
general
ports 443
exit
exit

Use this configuration?[yes]:
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]:
```

After the configuration dialog is complete, you are prompted to save the configuration. The figure shows the prompts for saving the configuration and rebooting the system. If you modified the IP address, netmask, default gateway or web port, you are prompted for reboot. The system must be rebooted for the changes to go into effect. Enter **no** to avoid rebooting the Sensor at this time. After setup is complete, you still need to configure network ACLs and other settings. You can continue with this configuration and use the **reset** command to reboot the Sensor when you have finished.

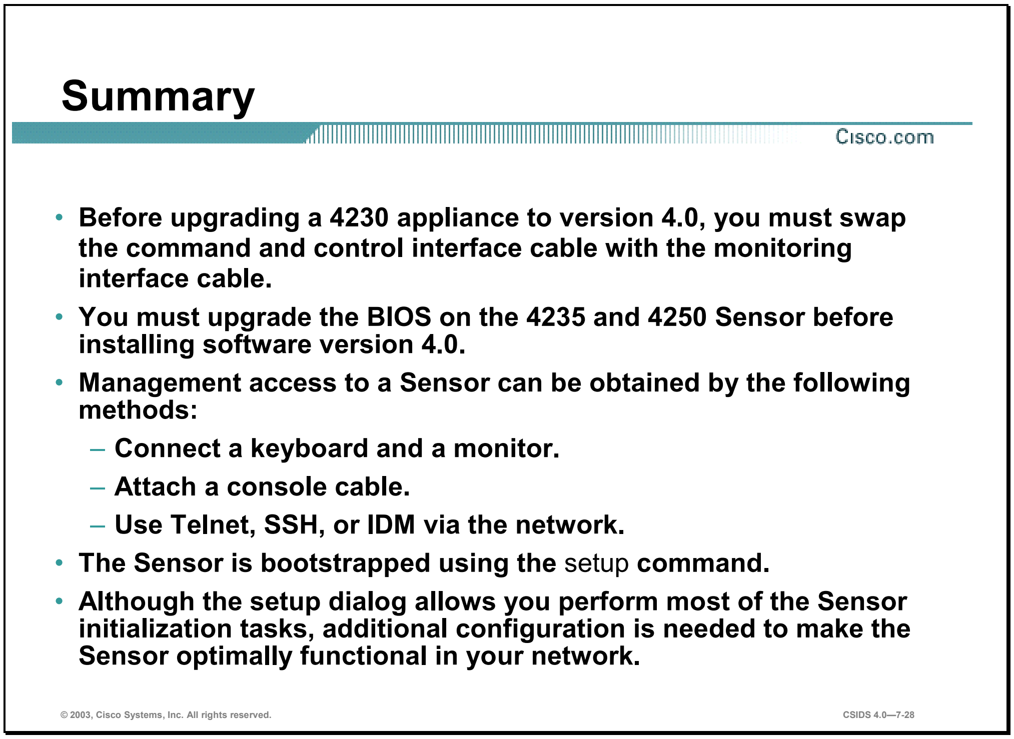
A minimal number of system reboots are required. Most configuration changes are applied immediately without reboot. Changes that are not applied immediately include the following:

- Changes made in the service configuration mode. When you exit the mode, you are prompted to apply changes. Changes are discarded if you answer **no** to applying changes.

- Changing the Sensor's IP address. You must reboot the Sensor for this change to take effect.

Summary

This section summarizes what you have learned in this chapter.



Summary

Cisco.com

- Before upgrading a 4230 appliance to version 4.0, you must swap the command and control interface cable with the monitoring interface cable.
- You must upgrade the BIOS on the 4235 and 4250 Sensor before installing software version 4.0.
- Management access to a Sensor can be obtained by the following methods:
  - Connect a keyboard and a monitor.
  - Attach a console cable.
  - Use Telnet, SSH, or IDM via the network.
- The Sensor is bootstrapped using the setup command.
- Although the setup dialog allows you perform most of the Sensor initialization tasks, additional configuration is needed to make the Sensor optimally functional in your network.

CSIDS 4.0—7-28

Lab Exercise—Sensor Appliance Initialization

Complete the following lab exercise to practice what you learned in this chapter.

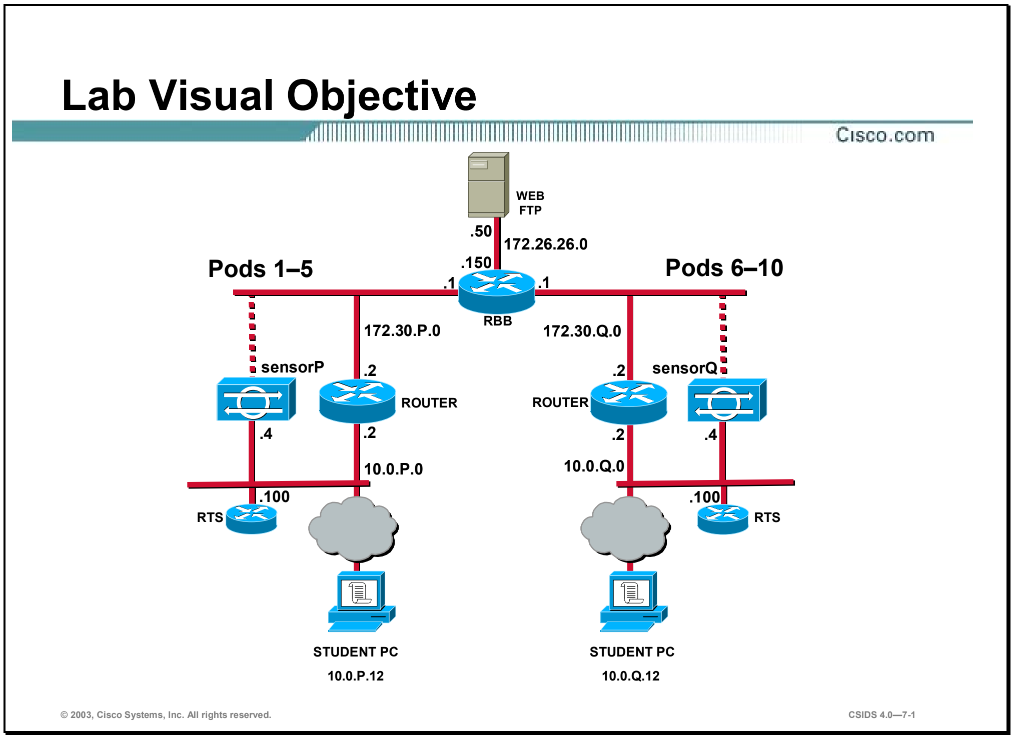
Objectives

In this lab exercise you will complete the following tasks:

- Assign the Sensor's IP network settings.
- Complete the initial configuration.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—7-1

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor.

Setup

Before starting this lab exercise, your instructor will provide you with the IP address of the terminal server and instructions to access the Sensor. Verify that your PC is able to ping the terminal server.

Task 1—Assign the Sensor's IP Network Settings

This task involves configuring the following: Sensor hostname, IP address for the Sensor's command and control interface, default route, Telnet server status, and web server port. Complete the following steps to assign the Sensor's IP network settings:

Step 1 Access the terminal server as directed by your instructor:

```
c:\telnet 10.0.P.100
```

(where P = pod number)

Step 2 Access the Sensor via its console port as directed by your instructor:

```
rts>sP
```

(where P = pod number)

Step 3 Log in to the CLI:

```
sensor login: cisco
Password: cisco
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password:
```

Step 4 When prompted, change the default password to iattacku2:

```
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password: cisco
New password: iattacku2
Type new password again: iattacku2
```

Step 5 Enter the **setup** command. The System Configuration Dialog is displayed.

```
sensor# setup
```

Step 6 Press the **Space Bar**. The following question appears:

```
Continue with configuration dialog? [yes]:
```

Step 7 Press **Enter** to continue:

```
Continue with configuration dialog? [yes]: <Enter>
```

Step 8 Assign a name to the Sensor:

```
Enter host name[sensor]: sensorP
```

(where P= pod number)

Step 9 Assign an IP address to the Sensor's command and control interface:

```
Enter IP address[10.1.9.201]: 10.0.P.4
```

(where P = pod number)

Step 10 Assign a netmask for the IP address:

```
Enter netmask[255.255.255.0]: 255.255.255.0
```

Step 11 Assign a default gateway:

```
Enter default gateway[10.1.9.1]: 10.0.P.2
```

(where P = pod number)

Step 12 Accept the default setting for Telnet services:

```
Enter telnet-server status[disabled]: <Enter>
```

Step 13 Accept the default web server port:

```
Enter web-server port[443]: <Enter>
```

Step 14 Press **Enter** to save the configuration.

```
Use this configuration? [yes]: <Enter>
```

```
Configuration Saved.
```

Step 15 Enter **no** to avoid rebooting the Sensor at this time:

```
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is rebooted. Please
use the reset command to complete the configuration.
```

Task 2—Complete the Initial Configuration

Complete the following steps to configure network access lists and set the Sensor's clock.

Note Network access lists must be configured to allow external hosts to access the Sensor.

Step 1 Enter configure terminal mode:

```
sensorP# configure terminal
sensorP(config)#
```

(where P = pod number)

Step 2 Enter host configuration mode:

```
sensorP(config)# service host
sensorP(config-Host)#
```

(where P = pod number)

Step 3 Enter network parameters configuration mode:

```
sensorP(config-Host)# networkParams
sensorP(config-Host-net)#
```

(where P = pod number)

Step 4 View the current settings:

```
sensorP(config-Host-net)# show settings
networkParams
ipAddress: 10.0.P.4
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.0.P.2
hostname: sensorP
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 1)
ipAddress: 10.0.0.0
netmask: 255.0.0.0 default: 255.255.255.255
```

(where P = pod number)

Step 5 Remove the 10.0.0.0 network from the access list:

```
sensorP(config-Host-net)# no accessList ipAddress 10.0.0.0 netmask 255.0.0.0
```

(where P = pod number)

Step 6 Add your peer pod's network to the access list:

```
sensorP(config-Host-net)# accessList ipAddress 10.0.Q.0 netmask 255.255.255.0
```

(where Q = peer pod number)

Step 7 Add your student PC to the access list:

```
sensorP(config-Host-net)# accessList ipAddress 10.0.P.12
```

(where P = pod number)

Step 8 View your changes:

```
sensorP(config-Host-net)# show settings
networkParams
ipaddress: 10.0.P.4
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.0.P.2
hostname: sensorP
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 2)
ipAddress: 10.0.P.12
netmask: 255.255.255.255 <defaulted>
```

(where P = pod number)

Step 9 Exit network parameters configuration mode:

```
sensorP(config-Host-net)# exit
sensorP(config-Host)#
```

(where P = pod number)

Step 10 Exit configure host mode:

```
sensorP(config-Host)# exit
Apply Changes:?[yes]:
```

(where P = pod number)

Step 11 Press **Enter** to apply the changes:

```
Apply Changes:?[yes]: <Enter>
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]:
```

Step 12 Enter **no** to avoid rebooting the Sensor at this time.

```
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is rebooted. Please
use the reset command to complete the configuration.
sensorP(config)#
```

(where P = pod number)

Step 13 Exit configure terminal mode:

```
sensorP(config)# exit
sensorP#
```

(where P = pod number)

Step 14 Set the clock. Enter the current time, month, day, and year:

Note Use military time, and spell out the name of the month. For example, to set the system clock to 1:32 pm, July 29, 2003, you would enter the following: clock set 13:32 July 29 2003

```
sensorP# clock set hh:mm month day year
```

(where P = pod number)

Step 15 Reboot the Sensor:

```
sensorP# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? :
```

(where P = pod number)

Step 16 Enter yes to continue rebooting the Sensor:

```
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? : yes
```

Intrusion Detection System Module Configuration

Overview

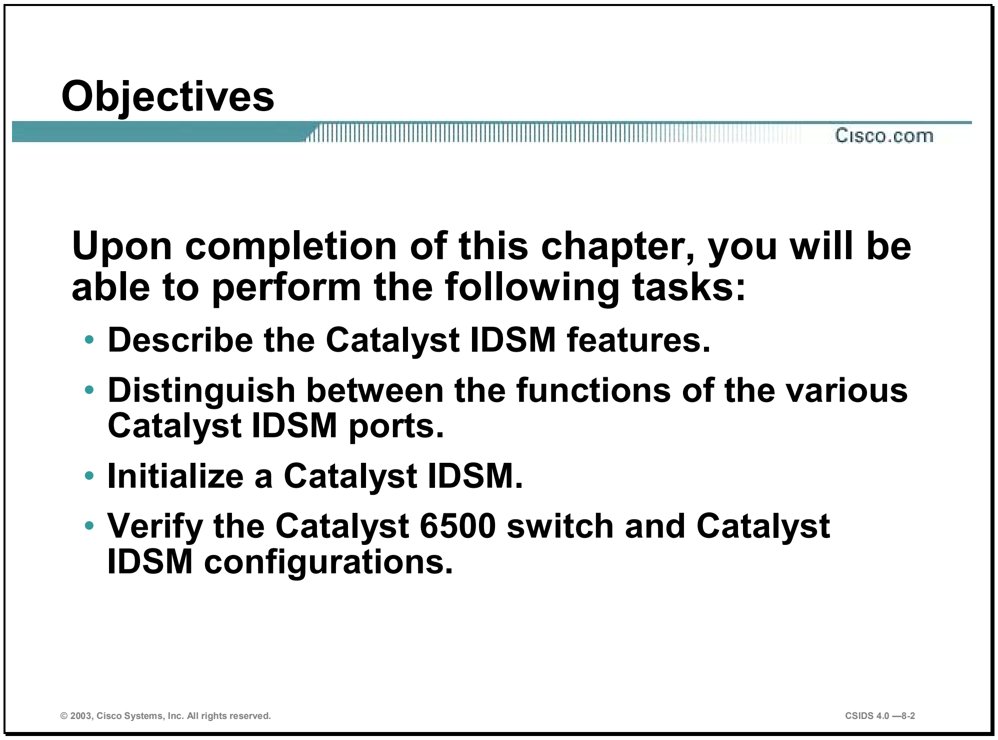
This chapter covers information on the Catalyst 6500 Intrusion Detection System (IDS) Module 2 (IDSM2) and how to configure it for intrusion detection.

This chapter includes the following topics:

- Objectives
- Introduction
- Ports and traffic
- Initialization
- Verifying IDSM2 status
- Summary

Objectives

This section lists the chapter’s objectives.



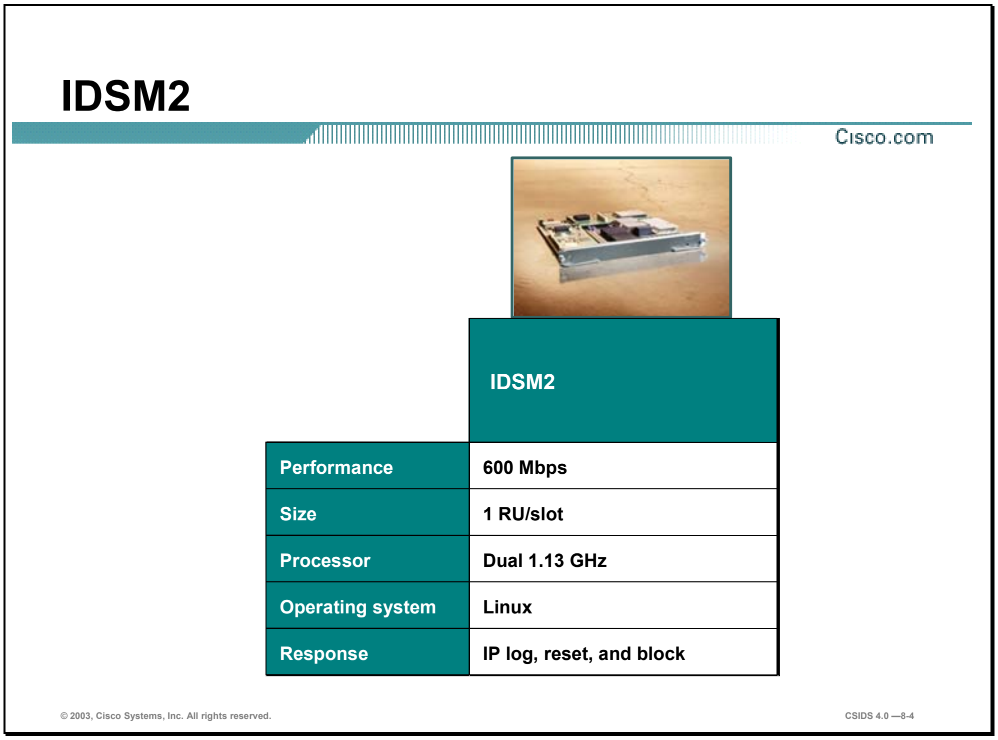
Objectives

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

- **Describe the Catalyst IDSM features.**
- **Distinguish between the functions of the various Catalyst IDSM ports.**
- **Initialize a Catalyst IDSM.**
- **Verify the Catalyst 6500 switch and Catalyst IDSM configurations.**

Introduction

This section introduces the IDSM2.



IDSM2

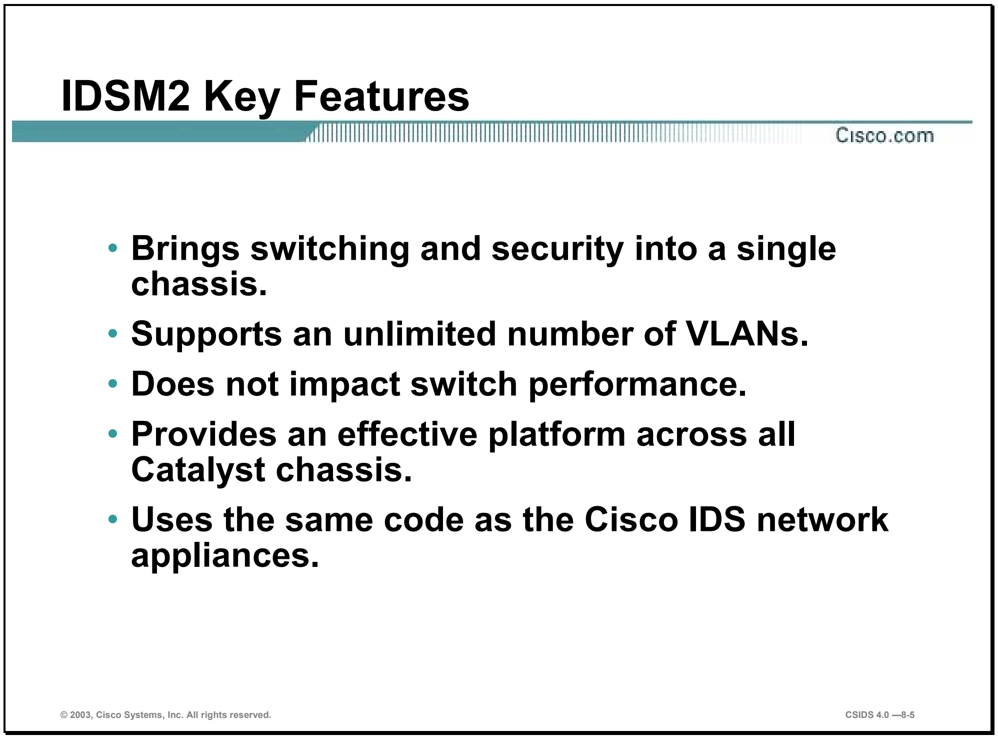
Cisco.com

	IDSM2
Performance	600 Mbps
Size	1 RU/slot
Processor	Dual 1.13 GHz
Operating system	Linux
Response	IP log, reset, and block

CSIDS 4.0 —8-4

The following are the IDSM2 technical specifications:

- Performance—600 Mbps with 450 byte packets
- Size—1 rack unit (RU)/slot
- Processor—Dual 1.13 GHz
- Operating system—Linux
- Response—IP log, reset, and block



IDSM2 Key Features

Cisco.com

- Brings switching and security into a single chassis.
- Supports an unlimited number of VLANs.
- Does not impact switch performance.
- Provides an effective platform across all Catalyst chassis.
- Uses the same code as the Cisco IDS network appliances.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0 —8-5

The following are the IDSM2 key features:

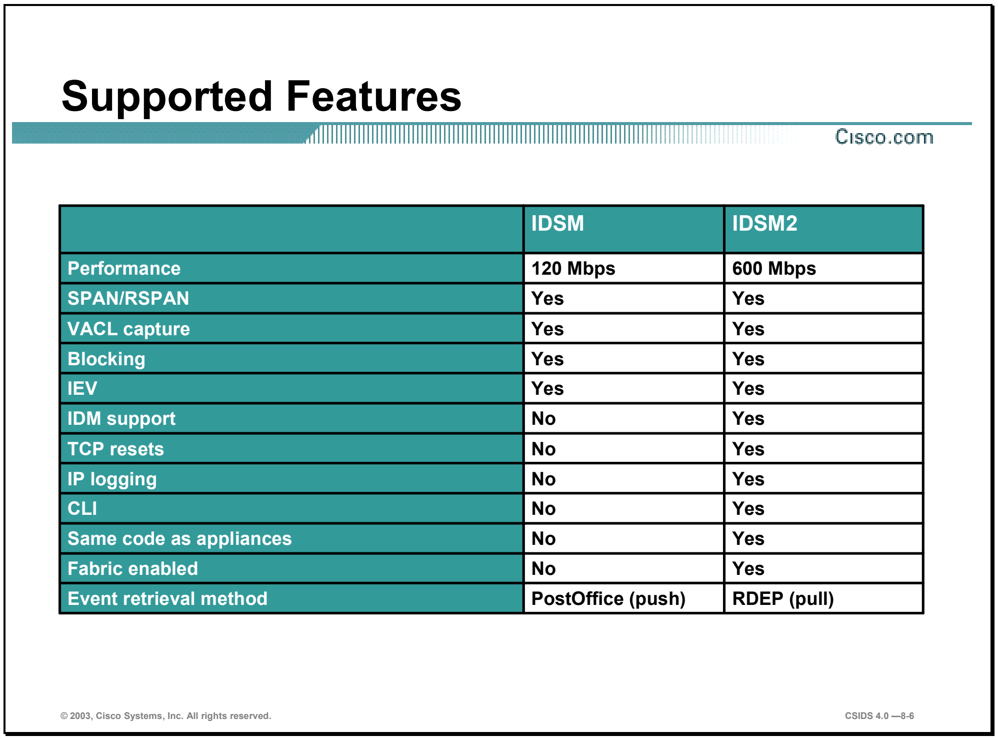
- Provides an in-switch IDS solution supplying access to the data stream via VLAN access control list (VACL) capture, SPAN, or RSPAN.

- Supports an unlimited number of VLANS.

- Transparent operation via passive, promiscuous operation that inspects copies of packets via VACL capture, Switch Port Analyzer (SPAN), and Remote SPAN (RSPAN) without exposing the network to performance degradation or downtime if the unit needs maintenance. This is possible because the IDSM2 is not in the switch forwarding path.

- Takes only a single slot in the switch chassis making it an effective platform across all Catalyst chassis, from the 3-slot Catalyst 6503 Switch to the largest chassis available. This enables you to install multiple modules and provides protection for a greater amount of traffic.

- Uses the same code as the IDS network appliances. This enables you to employ a single management technique and makes installation, training, operation, and support simpler and faster while taking advantage of Cisco IDS comprehensive attack recognition and signature coverage.



Supported Features

Cisco.com

	IDSM	IDSM2
Performance	120 Mbps	600 Mbps
SPAN/RSPAN	Yes	Yes
VACL capture	Yes	Yes
Blocking	Yes	Yes
IEV	Yes	Yes
IDM support	No	Yes
TCP resets	No	Yes
IP logging	No	Yes
CLI	No	Yes
Same code as appliances	No	Yes
Fabric enabled	No	Yes
Event retrieval method	PostOffice (push)	RDEP (pull)

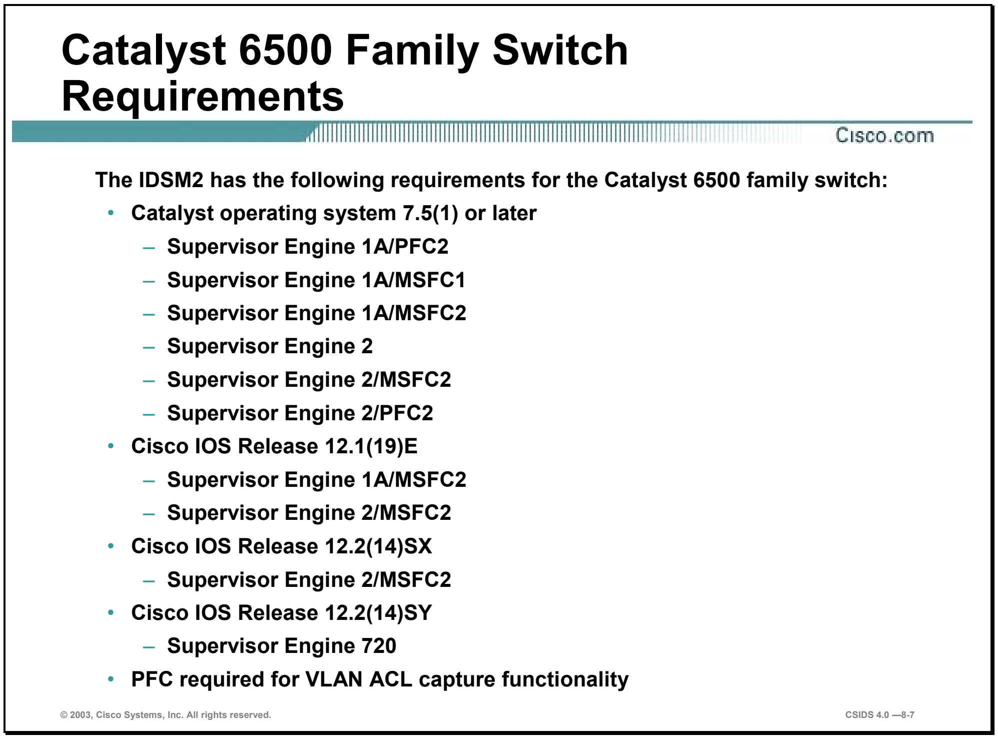
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0 —8-6

The Cisco IDSM2 is a fabric-enabled, second-generation IDSM offering more than five times the performance of the first generation module. All Cisco Catalyst 6500 Series switches and Cisco 7600 Series chasses support the Cisco IDSM2.

In addition to increased performance, the IDSM2 features the following enhancements as compared to the IDSM:

- Performance enhancement—600 Mbps
- IDS Device Manager (IDM) support
- TCP resets
- IP logging
- Command line interface (CLI)—Includes a complete CLI
- Same code as appliances
- Fabric enabled
- Event retrieval method—Pull method occurs via Remote Data Exchange Protocol (RDEP)



Catalyst 6500 Family Switch Requirements

The IDSM2 has the following requirements for the Catalyst 6500 family switch:

- Catalyst operating system 7.5(1) or later
  - Supervisor Engine 1A/PFC2
  - Supervisor Engine 1A/MSFC1
  - Supervisor Engine 1A/MSFC2
  - Supervisor Engine 2
  - Supervisor Engine 2/MSFC2
  - Supervisor Engine 2/PFC2
- Cisco IOS Release 12.1(19)E
  - Supervisor Engine 1A/MSFC2
  - Supervisor Engine 2/MSFC2
- Cisco IOS Release 12.2(14)SX
  - Supervisor Engine 2/MSFC2
- Cisco IOS Release 12.2(14)SY
  - Supervisor Engine 720
- PFC required for VLAN ACL capture functionality

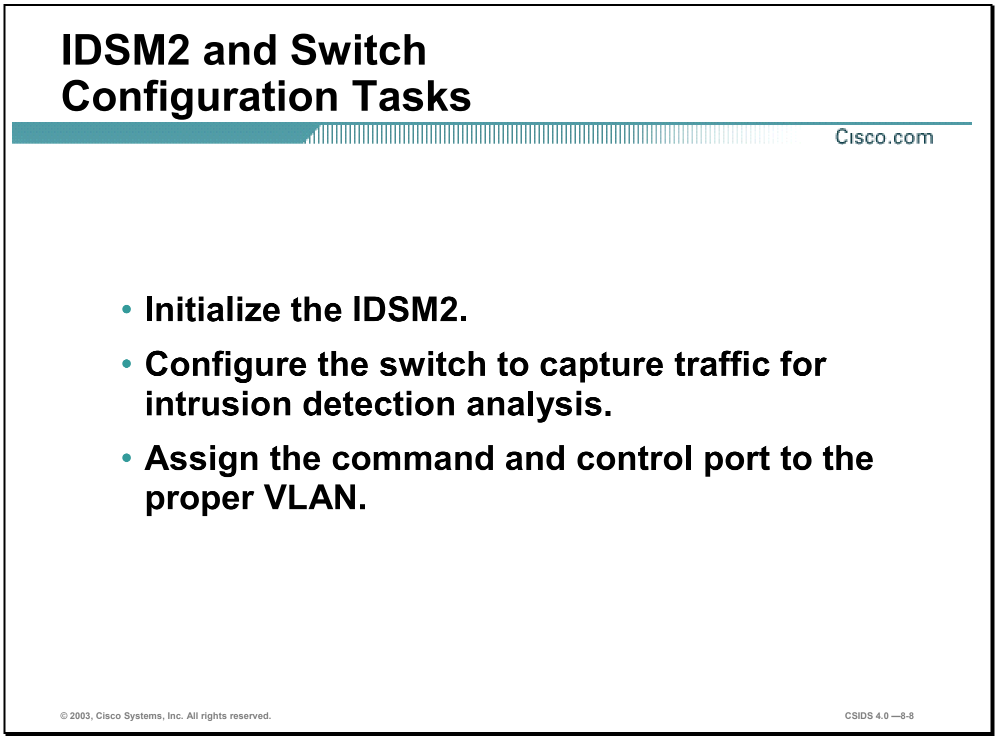
CSIDS 4.0 —8-7

The IDSM2 has the following requirements for the Catalyst 6500 Family switch:

- Catalyst operating system 7.5(1)
  - Supervisor Engine 1A
  - Supervisor Engine 1A/Policy Feature Card 2(PFC2)
  - Supervisor Engine 1A/ Multilayer Switch Feature Card MSFC1
  - Supervisor Engine 1A/MSFC2
  - Supervisor Engine 2
  - Supervisor Engine 2/MSFC2
  - Supervisor Engine 2/PFC2
- Cisco IOS Release 12.1(19)E
  - Supervisor Engine 1A/MSFC2
  - Supervisor Engine 2/MSFC2
- Cisco IOS Release 12.2(14)SX
  - Supervisor Engine 2/MSFC2

- Cisco IOS Release 12.2(14)SY
    - Supervisor Engine 720
- PFC for VACL capture feature functionality

Note Supervisor Engine 720 is not yet supported.



IDSM2 and Switch Configuration Tasks

Cisco.com

- Initialize the IDSM2.
- Configure the switch to capture traffic for intrusion detection analysis.
- Assign the command and control port to the proper VLAN.

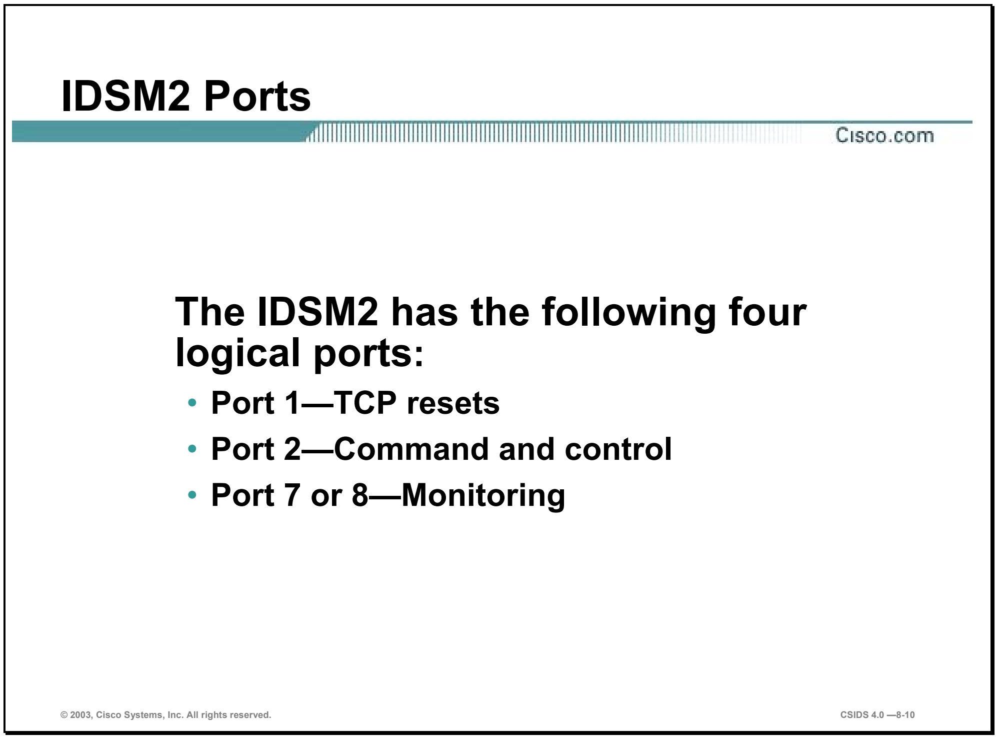
© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0 —8-8

Complete the following tasks to configure the IDSM2 and the Catalyst 6500 switch:

- Initialize the IDSM2. This includes completing the basic configuration via the **setup** command.
- Configure the switch to capture traffic for intrusion detection analysis. This includes creating SPAN sessions, RSPAN sessions, or VACL captures.
- Assign the command and control port to the correct VLAN. The command and control port should be in the same VLAN as its default gateway.

Ports and Traffic

This section discusses the ports on the IDSM2 and how traffic is captured for intrusion detection analysis.



IDSM2 Ports

The IDSM2 has the following four logical ports:

- **Port 1—TCP resets**
- **Port 2—Command and control**
- **Port 7 or 8—Monitoring**

CSIDS 4.0 —8-10

Packets are directed to the monitoring ports of the IDSM2 by using the VACL capture, SPAN, or RSPAN method of traffic capture. SPAN provides a means of sending a copy of the traffic within the switch from a spanned source port to a port designated as the SPAN port. The port being spanned is usually an Ethernet port in the chassis with interesting traffic the IDSM2 can monitor. A copy of transmit (TX), receive (RX) or both TX and RX traffic can be sent from the spanned port to an IDSM2 monitor port. The IDSM2 uses four logical ports which have the following default designations:

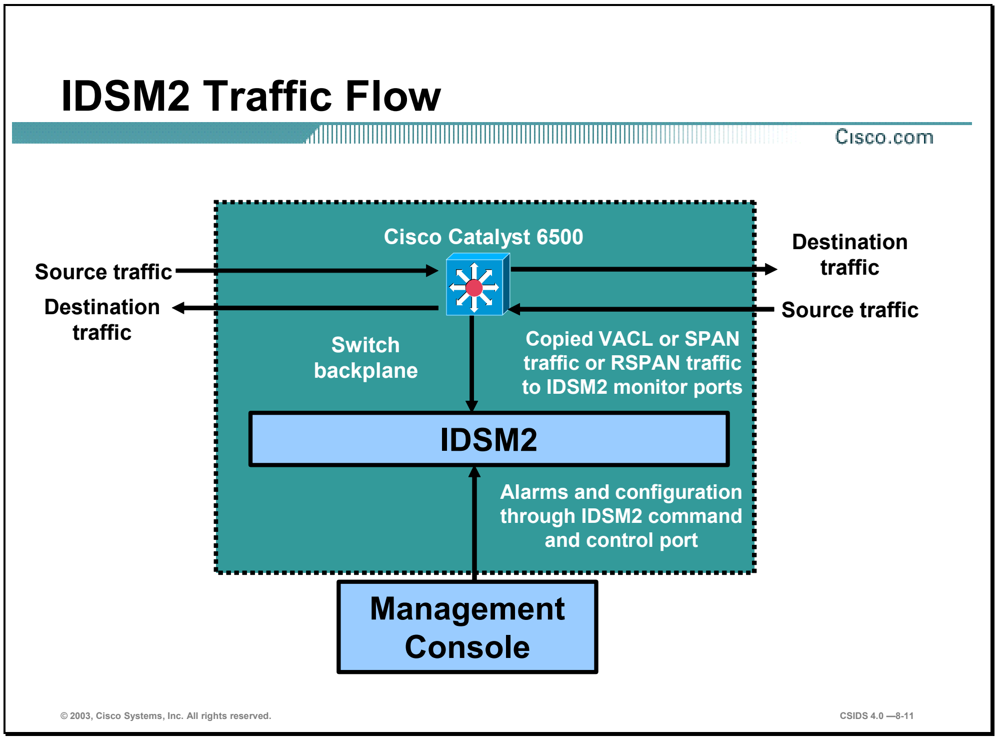
- Port 1 is used as the TCP reset port.
- Port 2 is the command and control port.
- Ports 7 and 8 are the monitoring ports. One of these ports can be configured as the SPAN monitor port.

With SPAN enabled on a source port or VLAN, a copy of all received traffic, all transmitted traffic, or all received and transmitted traffic from the SPAN source port or VLAN is sent to the SPAN destination port. On the Catalyst 6500 switch, there is a limit to the number of SPAN ports that can be configured. For RX SPAN sessions, you can have a maximum of 2 per chassis. For TX SPAN sessions, you can have a maximum of 4 sessions per chassis. For SPAN sessions that copy and send both RX and TX traffic from a port, you can configure a maximum of 2 SPAN sessions per chassis. When using SPAN, refer to the following rules:

- The total amount of spanned traffic cannot exceed the maximum throughput of the IDSM2, 600 Mbps.

- The limitation on the number of SPAN sessions limits the number of ports in the chassis that can have their traffic monitored by the IDSM2.

VACL capture is a way to leverage the hardware resources of the PFC, which resides on the Supervisor Engine of the switch. With VACL capture, traffic matching ACLs programmed into the PFC hardware are copied and sent to a configured capture port. The monitor port of the IDSM2 can be configured as the VACL capture port. Although configuring SPAN is easier, the VACL method of sending traffic to the IDSM2 may be preferable because it allows a subset of traffic to be copied and sent to the IDSM2, limiting the amount of traffic it needs to process, and also potentially allowing more traffic from more ports in the chassis to be analyzed. Other traffic flows as usual and does not add to the load of traffic that the IDSM2 has to process.



IDSM2 Traffic Flow

Cisco.com

Cisco Catalyst 6500

Source traffic

Destination traffic

Destination traffic

Source traffic

Switch backplane

Copied VACL or SPAN traffic or RSPAN traffic to IDSM2 monitor ports

IDSM2

Alarms and configuration through IDSM2 command and control port

Management Console

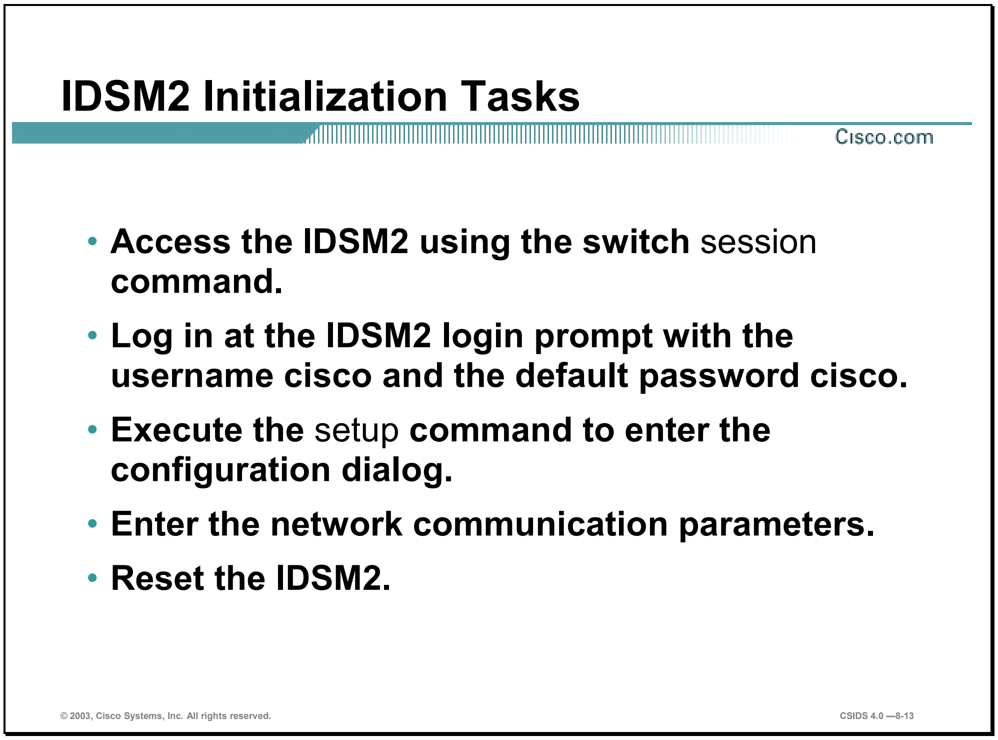
CSIDS 4.0 —8-11

The traffic flow is an important aspect of understanding how the IDSM2 captures and analyzes network traffic. The Catalyst 6500 switch must first be configured to capture traffic for intrusion detection analysis. If this is not done, the IDSM2 will never have visibility into the network traffic.

Traffic enters the Catalyst 6500 switch destined for a host or network. The traffic is captured off the switch backplane and sent to the IDSM2. The IDSM2 performs intrusion detection analysis and performs the defined actions.

Initialization

This section covers how to access and initialize the IDSM2.



IDSM2 Initialization Tasks

Cisco.com

- **Access the IDSM2 using the switch** session **command.**
- **Log in at the IDSM2 login prompt with the username cisco and the default password cisco.**
- **Execute the** setup **command to enter the configuration dialog.**
- **Enter the network communication parameters.**
- **Reset the IDSM2.**

CSIDS 4.0 —8-13

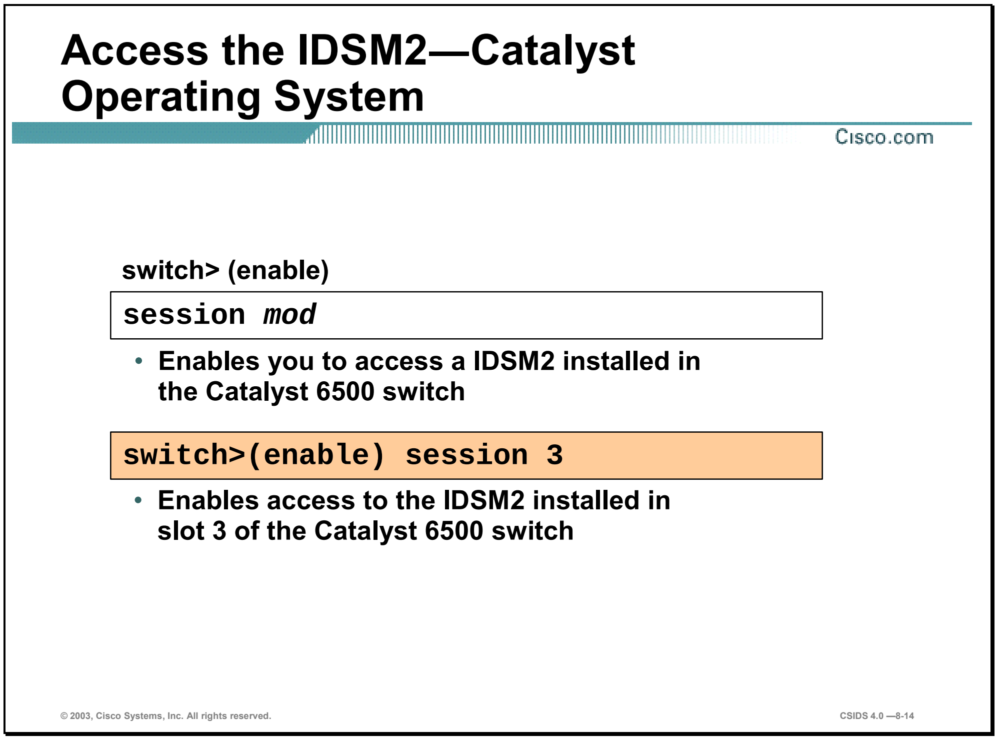
Because the IDSM2 runs the same code as the Sensor appliance, the initialization of the IDSM2 is essentially the same as that of the Sensor appliance. The main difference is the method of accessing the IDSM2 CLI. To initialize the IDSM2, complete the following steps:

Step 1 Initiate a session with the IDSM2 from the switch CLI.

Step 2 Log in to the IDSM2 using the default username cisco and the password cisco.

Step 3 Run the **setup** command and respond to its interactive prompts to complete the initial configuration.

Step 4 Reset the IDSM2 to enable and apply the configuration changes.



Access the IDSM2—Catalyst Operating System

switch> (enable)

```
session mod
```

- Enables you to access a IDSM2 installed in the Catalyst 6500 switch

```
switch>(enable) session 3
```

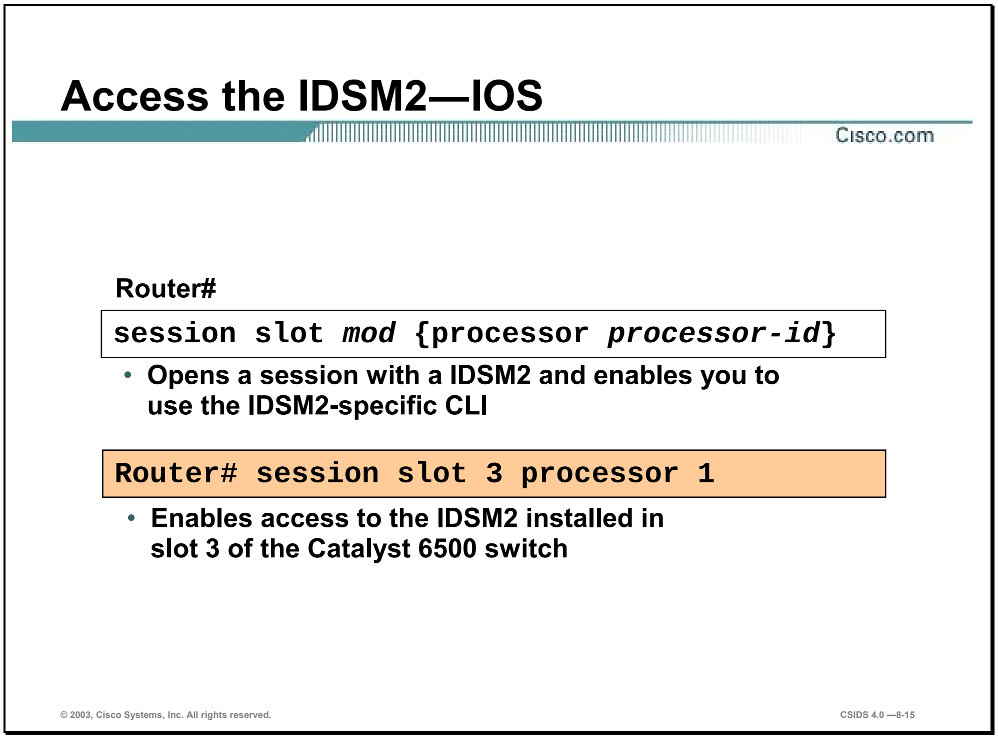
- Enables access to the IDSM2 installed in slot 3 of the Catalyst 6500 switch

CSIDS 4.0 —8-14

Using the **session** command from the Catalyst 6500 CLI to access the module gives you access to the IDSM2 CLI. The syntax for the Catalyst operating system **session** command is as follows:

session *mod*

mod	Number of the module



Access the IDSM2—IOS

Cisco.com

Router#

```
session slot mod {processor processor-id}
```

- Opens a session with a IDSM2 and enables you to use the IDSM2-specific CLI

```
Router# session slot 3 processor 1
```

- Enables access to the IDSM2 installed in slot 3 of the Catalyst 6500 switch

CSIDS 4.0 —8-15

Using the **session** command from the Catalyst 6500 CLI to access the module gives you access to the IDSM2 CLI. The syntax for the IOS **session** command is as follows:

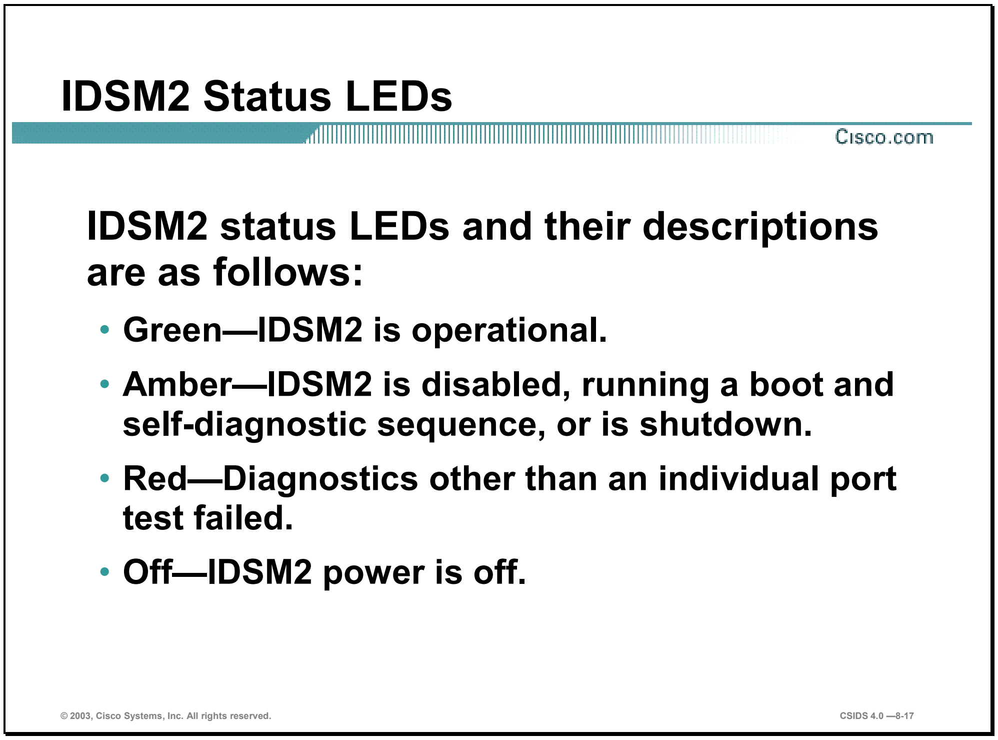
session slot ***mod*** **{ processor** ***processor-id*****}**

mod	Slot number
processor ***processor-id***	Processor ID

Note Currently, the processor for the IDSM2 is processor 1.

Verifying IDSM2 Status

This section explains how to verify the status of the IDSM2.



IDSM2 Status LEDs

IDSM2 status LEDs and their descriptions are as follows:

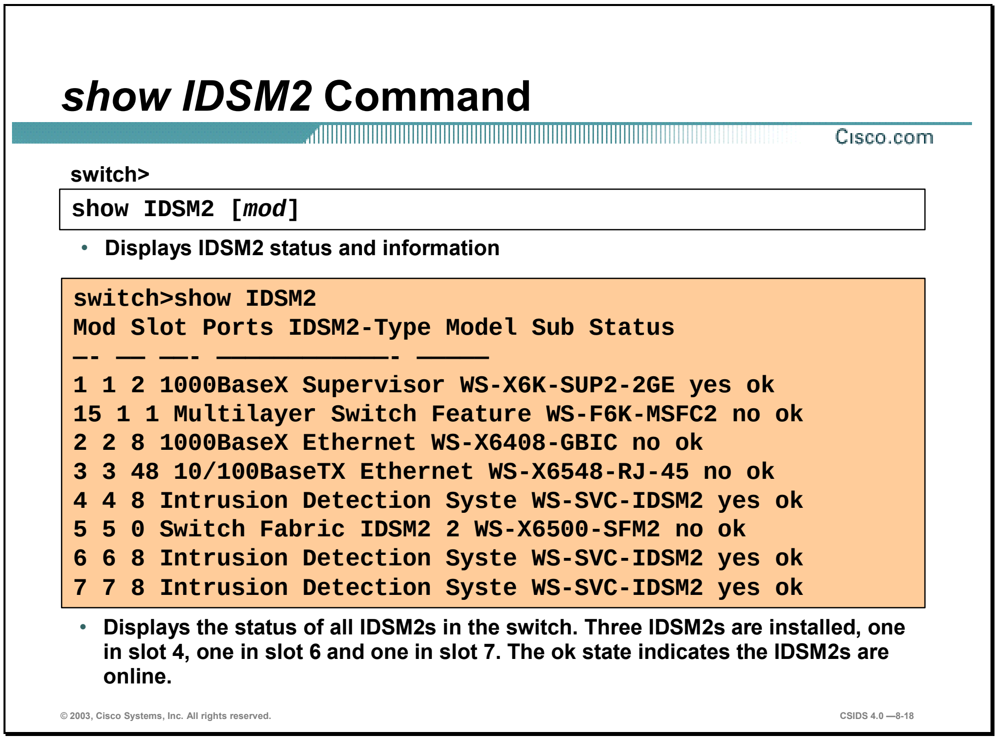
- Green—IDSM2 is operational.
- Amber—IDSM2 is disabled, running a boot and self-diagnostic sequence, or is shutdown.
- Red—Diagnostics other than an individual port test failed.
- Off—IDSM2 power is off.

CSIDS 4.0 —8-17

The status LED is a quick method to determine the state of the IDSM2. The status LED is located in the left corner of the IDSM2. LED status colors are described in the following table:

Status Color	Description
Green	IDSM2 is operational.
Amber	IDSM2 is disabled, running a boot and self-diagnostic test, or is shutdown.
Red	Diagnostics other than an individual port test failed.
Off	IDSM2 power is off.

In addition to the LED, the front panel of the IDSM2 has a shutdown switch. To prevent corruption of the IDSM2, you must shut it down properly. To properly shut it down, log in to the IDSM2 from the Catalyst 6500 series console and enter the **shutdown** command. If the IDSM2 fails to respond to the **shutdown** command, use a small pointed object, such as a paper clip, to press the **Shutdown** button. The shutdown procedure may take several minutes. The IDSM2 is hot-swappable, but you should not remove it from the switch until the IDSM2 shuts down completely. Removing the IDSM2 without going through a shutdown procedure can damage your IDSM2.



show IDSM2 Command

switch>

```
show IDSM2 [mod]
```

- Displays IDSM2 status and information

```
switch>show IDSM2
Mod Slot Ports IDSM2-Type Model Sub Status
—- —— ——- ——————————————- —————
1 1 2 1000BaseX Supervisor WS-X6K-SUP2-2GE yes ok
15 1 1 Multilayer Switch Feature WS-F6K-MSFC2 no ok
2 2 8 1000BaseX Ethernet WS-X6408-GBIC no ok
3 3 48 10/100BaseTX Ethernet WS-X6548-RJ-45 no ok
4 4 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
5 5 0 Switch Fabric IDSM2 2 WS-X6500-SFM2 no ok
6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
7 7 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
```

- Displays the status of all IDSM2s in the switch. Three IDSM2s are installed, one in slot 4, one in slot 6 and one in slot 7. The ok state indicates the IDSM2s are online.

CSIDS 4.0 —8-18

Use the **show module** command to display the module status and information. The syntax for the **show module** command is as follows:

show module [*mod*]

mod	Number of the module

The syntax for the IOS **show module** command is as follows:

show module [*mod-num* | all]

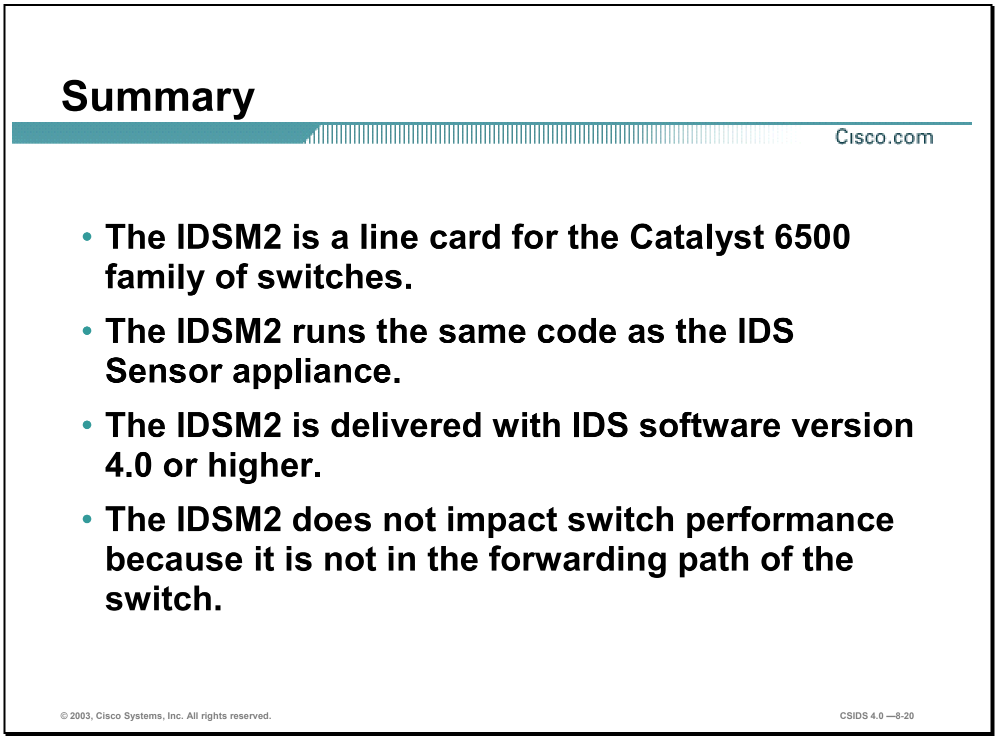
mod-num	(Optional.) Number of the IDSM2
all	(Optional.) Displays the information for all IDSM2s

The figure shows the output of the **show module** command. It is normal for the status to display "other" when the IDSM2 is first installed. After the IDSM2 completes the diagnostics routines and comes online, the status displays "ok." Allow up to 5 minutes for the IDSM2 to come online.

Note Because the IDSM2 runs the same Cisco IDS 4.0 software as the IDS network appliance, the Cisco IDS 4.0 software troubleshooting steps and commands will not be covered in this section, but will be covered in a later chapter.

Summary

This section summarizes what you have learned in this chapter.



Summary

Cisco.com

- The IDSM2 is a line card for the Catalyst 6500 family of switches.
- The IDSM2 runs the same code as the IDS Sensor appliance.
- The IDSM2 is delivered with IDS software version 4.0 or higher.
- The IDSM2 does not impact switch performance because it is not in the forwarding path of the switch.

CSIDS 4.0 —8-20

9

Cisco IDS Command Line

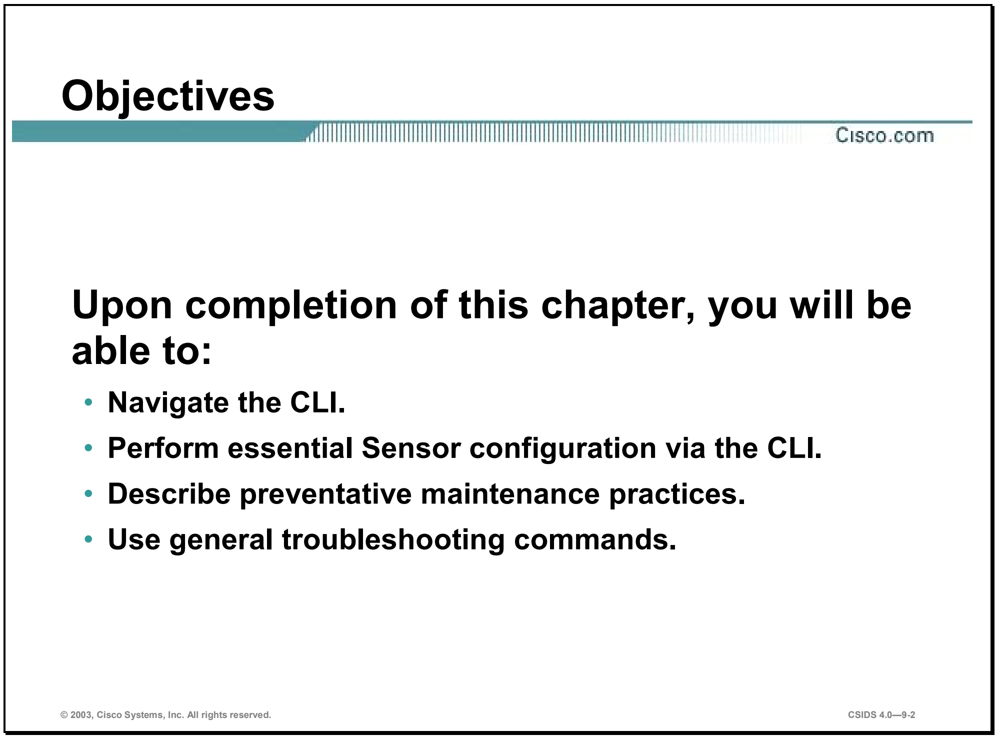
Overview

This chapter includes the following topics:

- Objectives
- Command line modes
- Initial configuration tasks
- Preventive maintenance and troubleshooting
- Summary
- Lab exercise

Objectives

This section lists the chapter's objectives.



Objectives

Cisco.com

Upon completion of this chapter, you will be able to:

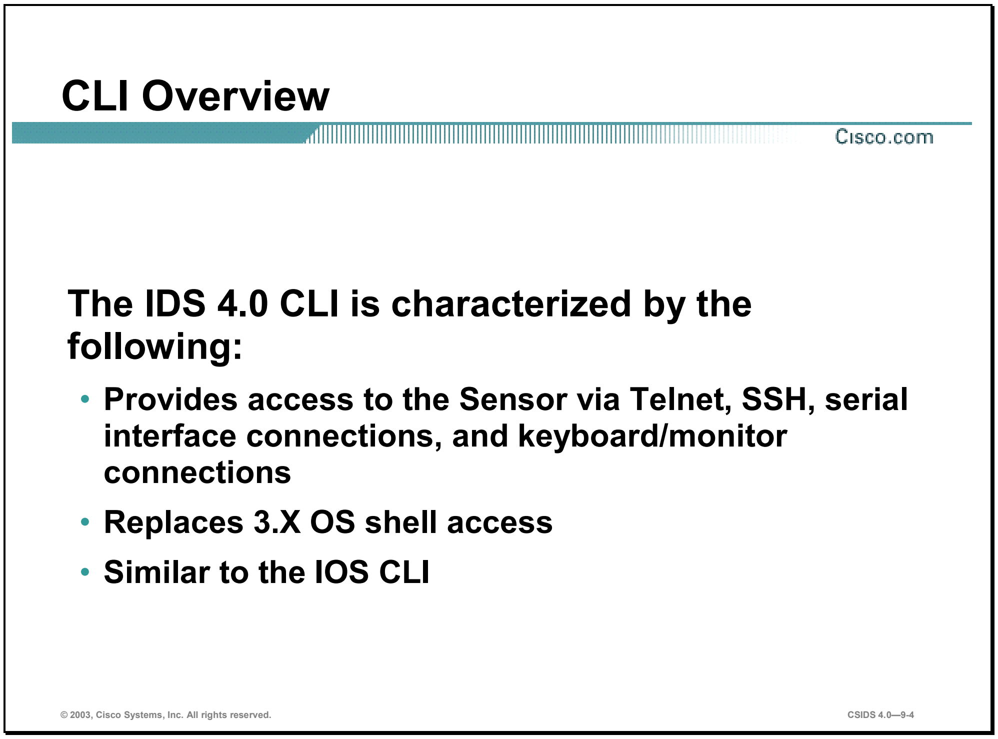
- **Navigate the CLI.**
- **Perform essential Sensor configuration via the CLI.**
- **Describe preventative maintenance practices.**
- **Use general troubleshooting commands.**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-2

Command Line Modes

This section explains the various command line interface (CLI) modes.



CLI Overview

Cisco.com

The IDS 4.0 CLI is characterized by the following:

- **Provides access to the Sensor via Telnet, SSH, serial interface connections, and keyboard/monitor connections**
- **Replaces 3.X OS shell access**
- **Similar to the IOS CLI**

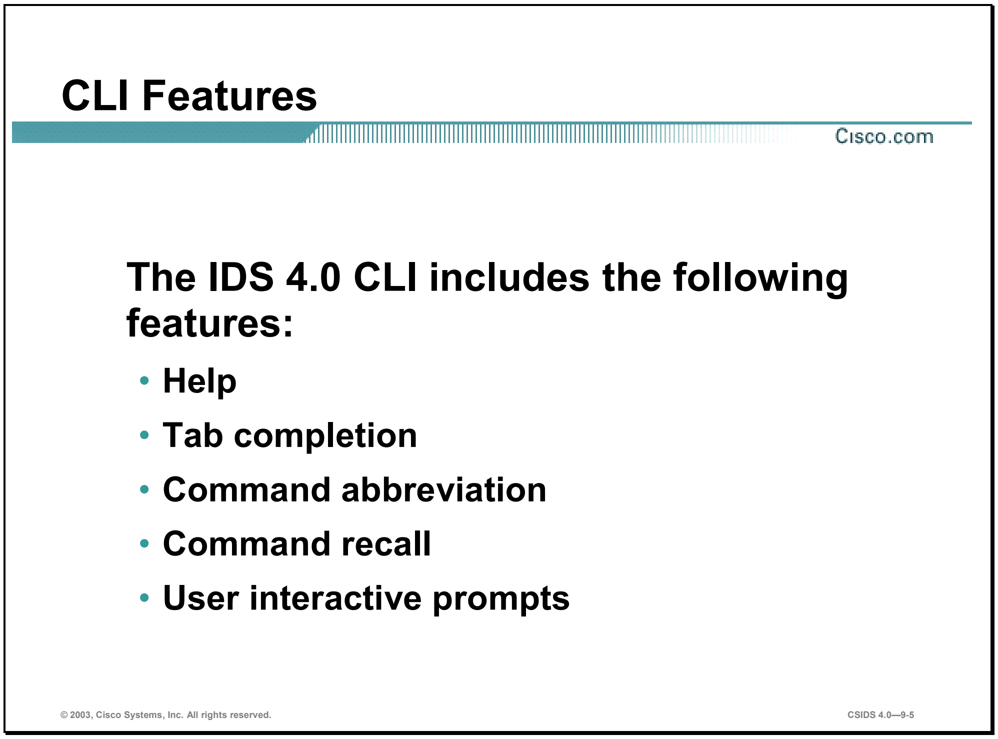
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-4

The IDS 4.0 software includes a full command line interface (CLI). The CLI for IDS version 4.0 is the user interface that enables you to access the Sensor through Telnet, SSH, and serial interface connections. Use an SSH version 1.5 client to access the CLI over the network. The following SSH clients have been tested with version 4.0 IDS Sensors:

- Windows
  - SecureCRT 3.1
  - PuTTY 0.53b
  - SSH Secure Shell for Workstations 3.2
  - Tera Term Pro 2.3 with TTSSH 1.5.4
- Solaris/HPUX/Linux
  - OpenSSH-3.4p1
  - SSH Secure Shell for Servers 3.2

The IDS CLI resembles the IOS CLI; however, it has fewer IOS configuration commands than the IOS software. It also has additional non-IOS configuration modes and commands.



CLI Features

Cisco.com

The IDS 4.0 CLI includes the following features:

- Help
- Tab completion
- Command abbreviation
- Command recall
- User interactive prompts

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-5

The IDS 4.0 CLI features the following components:

- Help—Enter **?** after the command to display command help. Help only displays commands available in the current mode.
- Tab Completion—If you are unsure of the complete syntax for a command, enter a portion of the command and press **Tab** to complete the command. If multiple commands match for tab completion, nothing is displayed. The terminal repeats the line you entered. Only commands available in the current mode are displayed by tab completion.
- Command abbreviation—The CLI recognizes shortened forms of many common commands. You only have to enter enough characters for the Sensor to recognize the command as unique. For example, **sh ver** executes the **show version** command.
- Command Recall—Use the up arrow or down arrow keys or use **Control> P** to recall the commands entered in a mode. Help and tab complete requests are not reported in the recall list.
- User interactive prompts—The CLI displays user interactive prompts when the system displays a question and waits for user input. The default input is displayed within brackets. Press **Enter** to accept the default input.

The CLI is not case sensitive, but it does echo back the text exactly as you entered it. The following steps provide an example:

Step 1 Enter **CONF** at the privileged exec prompt as follows:

```
sensor# CONF
```

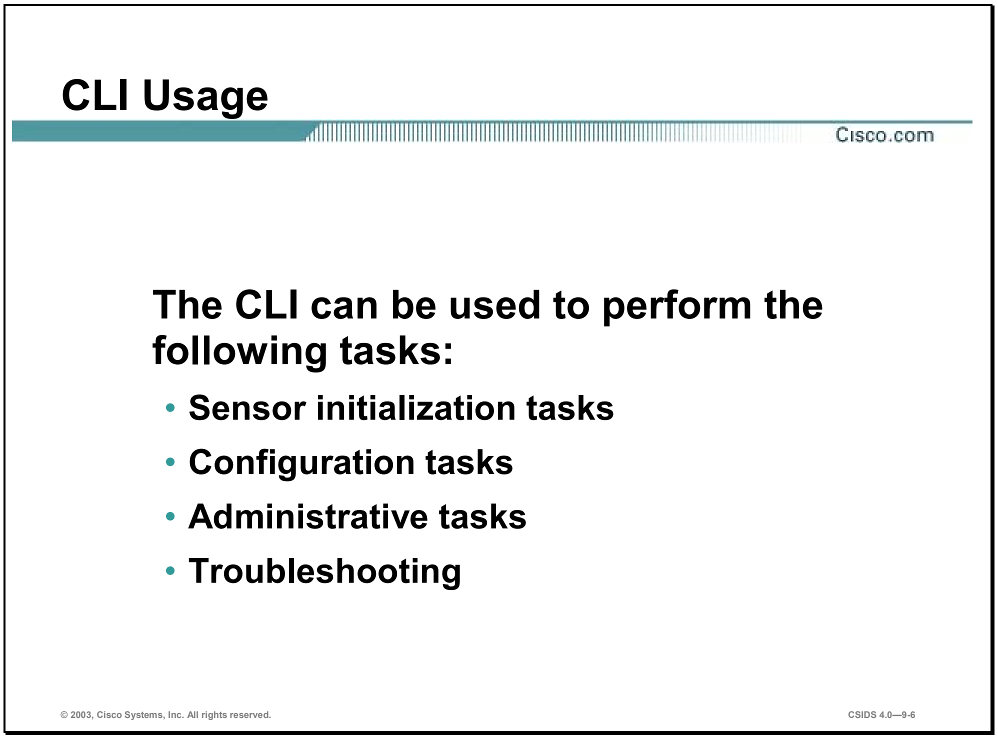
Step 2 Press **Tab**. The Sensor displays the following:

```
sensor# CONFigure
```

An interactive prompt, —More—, indicates that the terminal output exceeds the allotted display space. Press the **Space Bar** to display the next page of output, or press **Enter** to display the output one line at a time. Press **Control> C** to clear the current command line's contents and return to a blank command line.

You can usually disable features or functions by using the **no** form of a command. Use the command without the keyword no to enable a disabled feature or function. For example, the command **shutdown** disables an interface, the command **no shutdown** enables the interface. Refer to the individual commands for a complete explanation of the **no** form of that command.

Configuration commands that specify a default value in the configuration files, such as service and tune-micro-engines, can have a default form. The default form of a command returns the command setting to the default value.



CLI Usage

The CLI can be used to perform the following tasks:

- **Sensor initialization tasks**
- **Configuration tasks**
- **Administrative tasks**
- **Troubleshooting**

CSIDS 4.0—9-6

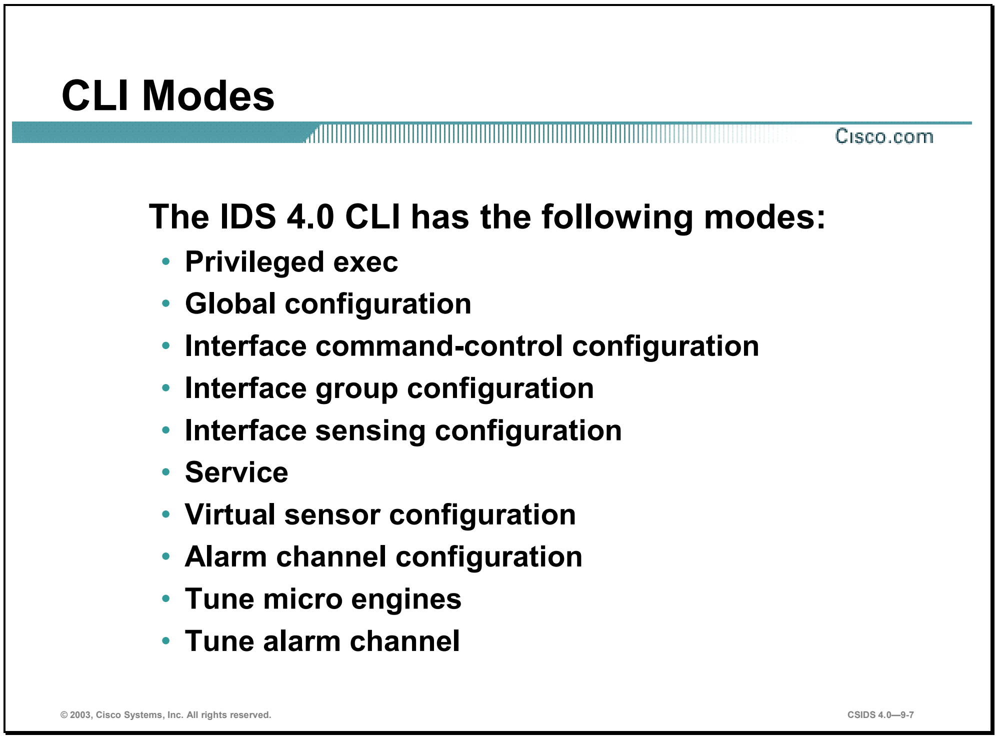
The CLI can be used to perform the following:

- Sensor initialization tasks—Sensor initialization tasks include such tasks as assigning the Sensor's IP address, specifying trusted hosts, and creating user accounts.

- Configuration tasks—Configuration tasks include such tasks as tuning signature engines and defining the ports where web servers are running.

- Administrative tasks—Administrative tasks include such tasks as backing up and restoring the current configuration file.

- Troubleshooting—Troubleshooting tasks include such tasks as verifying statistics and settings.



CLI Modes

The IDS 4.0 CLI has the following modes:

- Privileged exec
- Global configuration
- Interface command-control configuration
- Interface group configuration
- Interface sensing configuration
- Service
- Virtual sensor configuration
- Alarm channel configuration
- Tune micro engines
- Tune alarm channel

CSIDS 4.0—9-7

The command line interface (CLI) for IDS version 4.0 supports the following command modes: Each command mode provides access to a subset of commands.

- Privileged exec mode—Exec mode is the first level of the CLI. You enter exec mode by logging in to the CLI. Exec mode is denoted by the prompt sensor#.

- Global configuration mode—Global configuration mode is the second level of the CLI. You enter global configuration mode by first logging in to the CLI and then typing **configure terminal**. Global configuration mode is denoted by the prompt sensor(config)#.

- Interface command-control configuration mode—Interface command-control configuration mode is a third-level CLI mode. You enter interface command-control configuration mode by first entering global configuration mode and then typing **interface command-control**. Interface command-control configuration mode is denoted by the prompt sensor(config-if)#.

- Interface group configuration mode—Interface group configuration is a third-level CLI mode. You enter interface group configuration mode by first entering global configuration mode and then typing **interface group <*number*>,** where <number> is the group number. Interface group configuration mode is denoted by the prompt sensor(config-ifg)#.

- Interface sensing configuration mode—Interface sensing configuration is a third-level CLI mode. You enter interface sensing configuration mode by first entering global configuration mode and then typing **interface sensing <*name*>**, where <name> is the logical interface name. Interface sensing configuration mode is denoted by the prompt sensor(config-ifs)#.

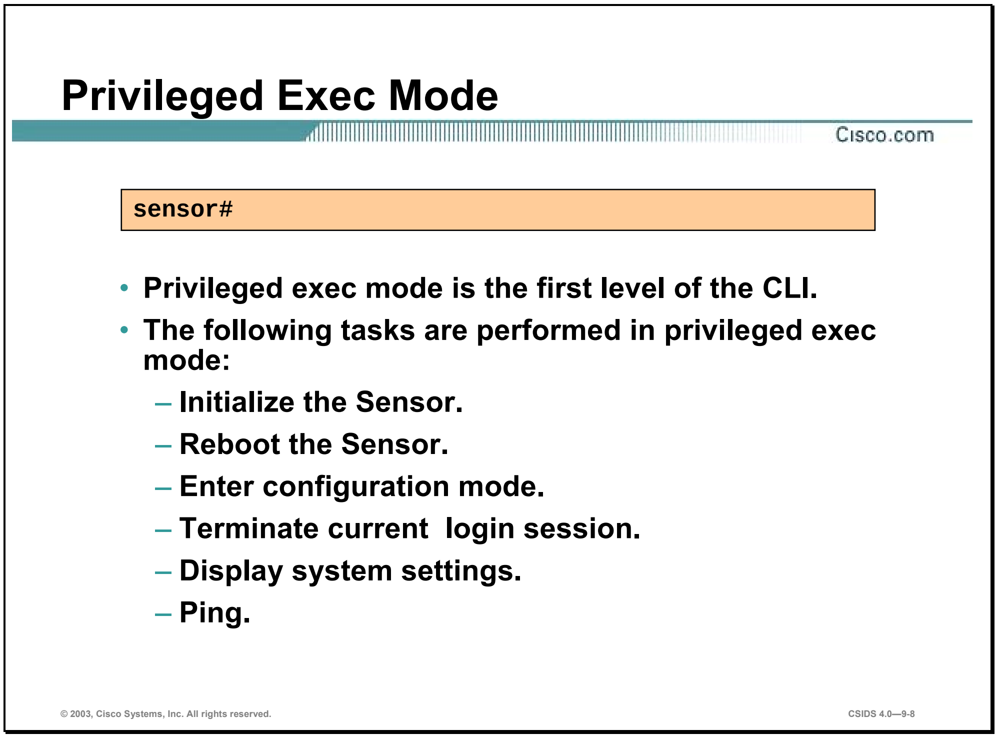
- Service mode—Service mode is a generic command mode used to edit a service's configuration. A service is a related set of functionality provided by an IDS application. An IDS application may provide more than one service. You enter service mode by first entering global configuration mode and then typing **service <*serviceName*>**, where <serviceName> identifies the actual service you are trying to access. Service mode is denoted by the prompt sensor(config-<serviceName>)#.

- Virtual sensor configuration mode—Virtual sensor configuration is a third-level CLI mode. You enter virtual sensor configuration mode by first entering global configuration mode and then typing **service virtual-sensor-configuration** followed by the logical virtual sensor configuration name. Currently, the only allowed name is virtualSensor. Virtual sensor configuration mode is denoted by the prompt sensor(config-vsc)#.

- Alarm channel configuration mode—Alarm channel configuration is a third-level CLI mode. You enter alarm channel configuration mode by first entering global configuration mode and then typing **service alarm-channel-configuration** followed by the logical alarm channel configuration name. Currently, the only allowed name is virtualAlarm. Alarm channel configuration mode is denoted by the prompt sensor(config-acc)#.

- Tune micro engines mode—Tune micro engines is a fourth-level CLI mode. You enter tune micro engines mode by first entering virtual sensor configuration mode and then typing **tune-micro-engines**. Tune micro engines mode is denoted by the prompt sensor(config-vsc-virtualSensor)#.

- Tune alarm channel—Tune alarm channel is a fourth-level CLI mode. You enter tune alarm channel mode by first entering alarm channel configuration mode and then typing **tune-alarm-channel**. Tune alarm channel mode is denoted by the prompt sensor(config-acc-virtualAlarm)#.



Privileged Exec Mode

Cisco.com

sensor#

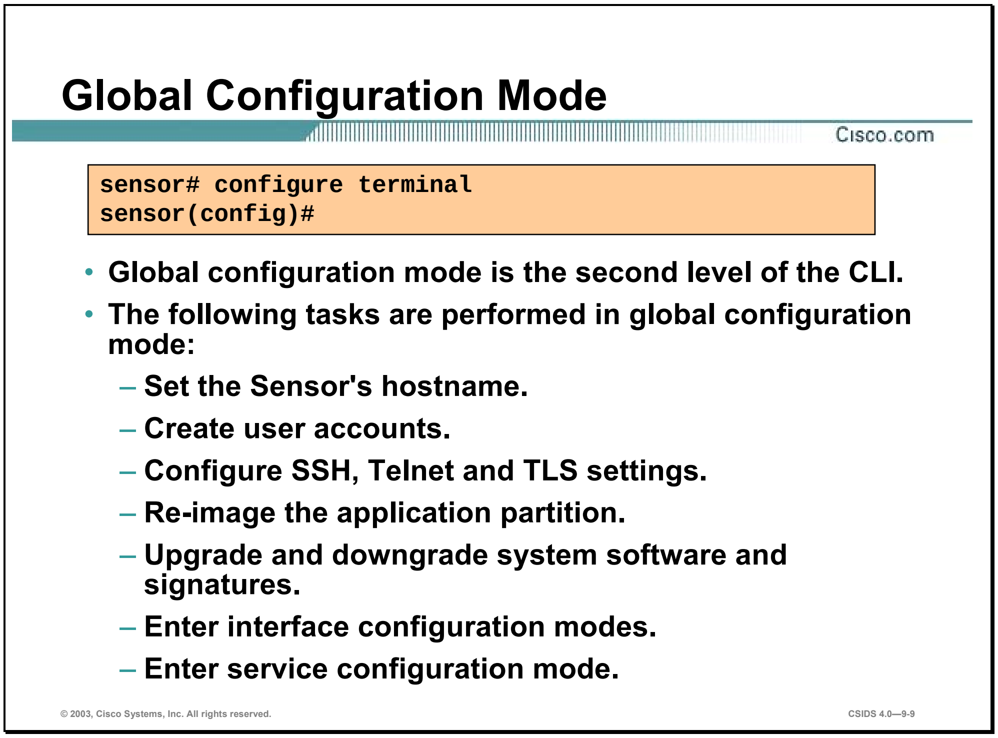
- Privileged exec mode is the first level of the CLI.
- The following tasks are performed in privileged exec mode:
  - Initialize the Sensor.
  - Reboot the Sensor.
  - Enter configuration mode.
  - Terminate current login session.
  - Display system settings.
  - Ping.

CSIDS 4.0—9-8

The first level of the CLI is the privileged exec mode. This mode enables you to perform such tasks as initialize the Sensor, and display system settings. The following example shows the commands available in privileged exec mode to a user with administrator privileges:

```
sensor1# ?
clear           Clear system settings or devices
clock           Set system clock settings
configure       Enter configuration mode
copy            Copy iplog or configuration files
erase           Erase a logical file
exit            Terminate current CLI login session
iplog           Control IP logging on the interface group
iplog-status     Display a list of IP Logs currently existing in the system
more             Display a logical file
no               Remove or disable system settings
ping             Send echo messages to destination
reset            Shutdown the sensor applications and reboot
setup            Perform basic sensor configuration
show             Display system settings and/or history information
ssh              Secure Shell Settings
terminal         Change terminal configuration parameters
tls              Configure TLS settings
trace            Display the route an IP packet takes to a destination
```

Note	The CLI supports the Administrator, Operator and Viewer user roles. The privilege levels for each role are different; therefore, the menus and available commands vary for each role. All Help command output in this section shows the commands available when logged in as a user with the Administrator role.



Global Configuration Mode

Cisco.com

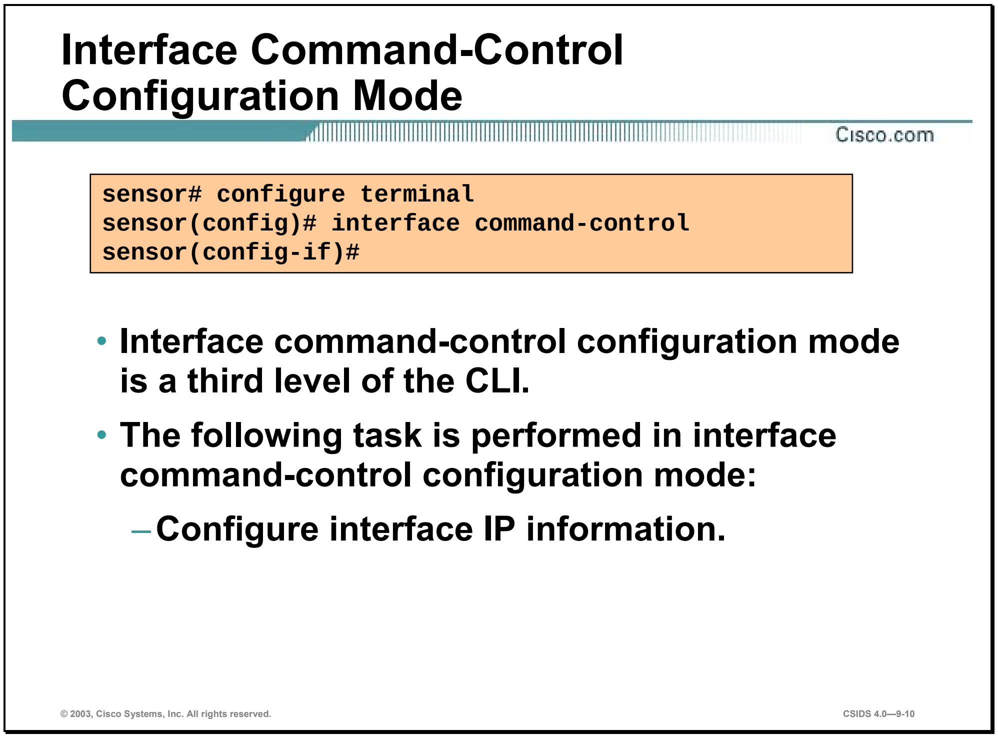
```
sensor# configure terminal
sensor(config)#
```

- Global configuration mode is the second level of the CLI.
- The following tasks are performed in global configuration mode:
  - Set the Sensor's hostname.
  - Create user accounts.
  - Configure SSH, Telnet and TLS settings.
  - Re-image the application partition.
  - Upgrade and downgrade system software and signatures.
  - Enter interface configuration modes.
  - Enter service configuration mode.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—9-9

The second level of the CLI is global configuration mode. This mode enables you to perform global configuration tasks such as setting the Sensor's hostname and creating user accounts. The following example shows the commands available in global configuration mode:

```
sensor1(config)# ?
display-serial     Re-direct all terminal output to the serial port
downgrade          Remove the last applied upgrade
end                Exit configuration mode and return to exec mode
exit               Exit configuration mode and return to exec mode
hostname           Set the sensor's hostname
interface          Enter configuration mode for system interfaces
no                 Remove configuration
password           Modify current user password on the local sensor
privilege          Modify user privilege
recover            Re-image the application partition from the recovery
                   partition
service            Enter configuration mode for node services
show               Display system settings and/or history information
ssh                Secure Shell Settings
telnet-server      Modify telnet-server settings
tls                Configure TLS settings
upgrade            Upgrade system software and signatures
username           Add a user to the local sensor
```



Interface Command-Control Configuration Mode

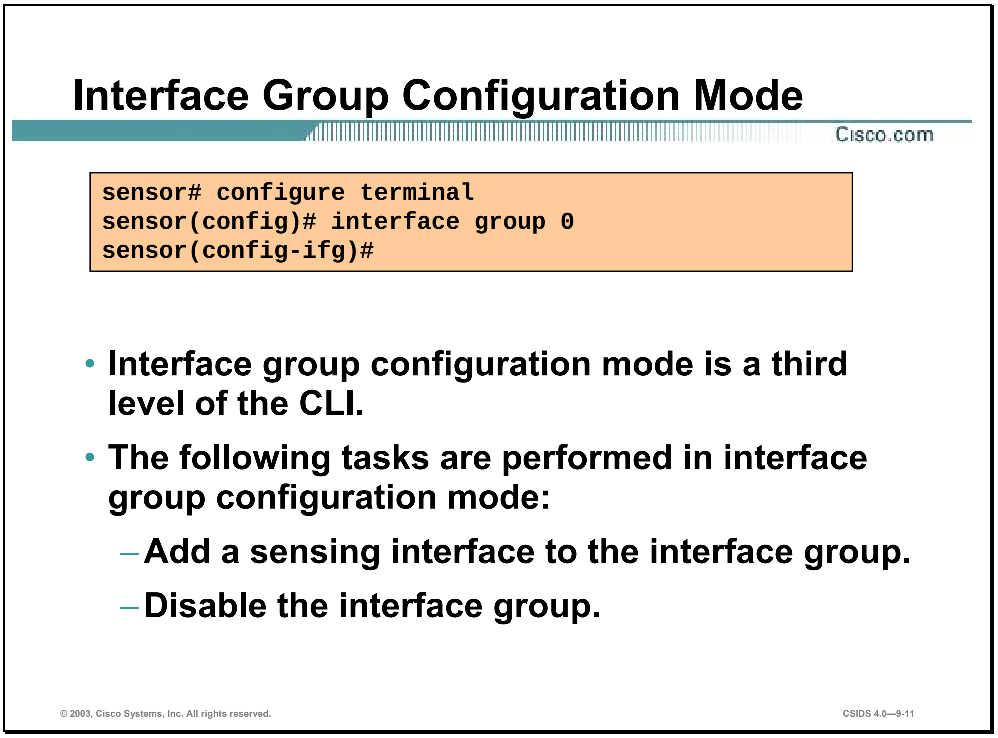
```
sensor# configure terminal
sensor(config)# interface command-control
sensor(config-if)#
```

- Interface command-control configuration mode is a third level of the CLI.
- The following task is performed in interface command-control configuration mode:
  - Configure interface IP information.

CSIDS 4.0—9-10

The interface command-control mode is a third level of the CLI. It enables you to configure IP information for the command and control interface. The following example shows the commands available in interface command-control mode:

```
sensor1(config)# interface command-control
sensor1(config-if)# ?
end      Exit interface configuration mode and return to exec mode
exit     Exit interface configuration mode and return to global configuration
         mode
ip       Configure IP information for interface
show     Display history information
```



Interface Group Configuration Mode

```
sensor# configure terminal
sensor(config)# interface group 0
sensor(config-ifg)#
```

- **Interface group configuration mode is a third level of the CLI.**
- **The following tasks are performed in interface group configuration mode:**
  - **Add a sensing interface to the interface group.**
  - **Disable the interface group.**

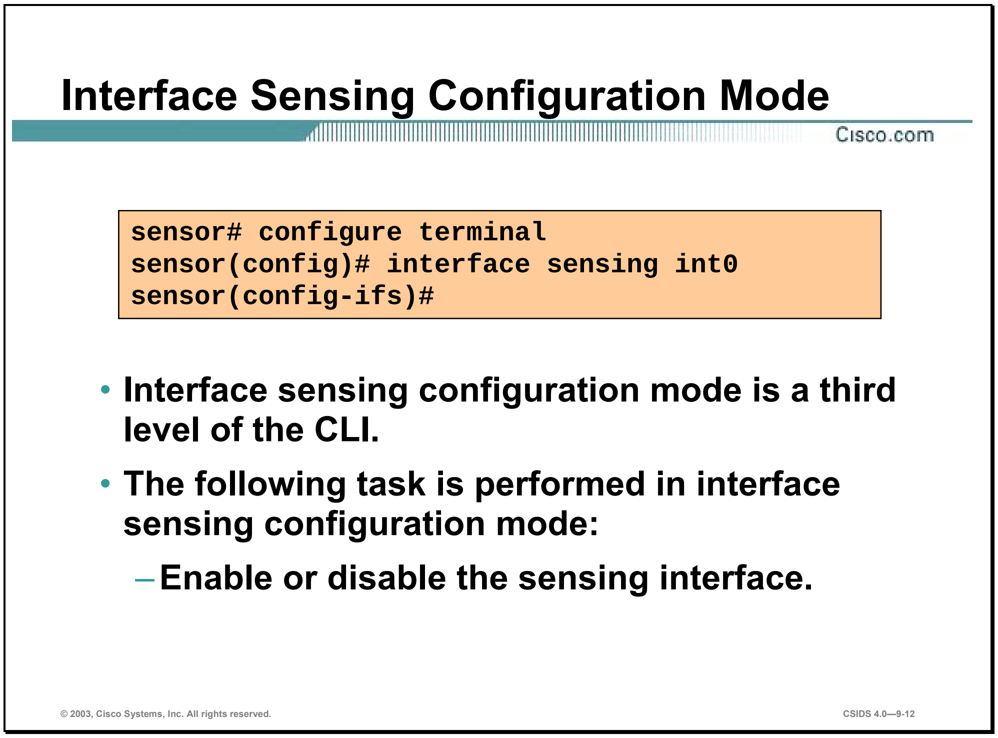
© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—9-11

The interface group configuration mode is a third level of the CLI. The **interface group** command enables you to enter a configuration mode. From this mode, you can add or remove interfaces from the group of monitoring interfaces used by sensorApp or shutdown the group, which disables monitoring on all interfaces within the group.

Note The **interface group** command functionality will be available in the 4.1 IDS software release.

The following example shows the commands available in the interface group configuration mode:

```
sensor1(config)# interface group 0
sensor1(config-ifg)# ?
end                   Exit interface group configuration mode and return to
                      exec mode
exit                  Exit interface group configuration mode and return to
                      global configuration mode
no                    Remove configuration
sensing-interface     Add a sensing interface to the interface group
show                  Display history information
shutdown              Disable the interface group
```



Interface Sensing Configuration Mode

Cisco.com

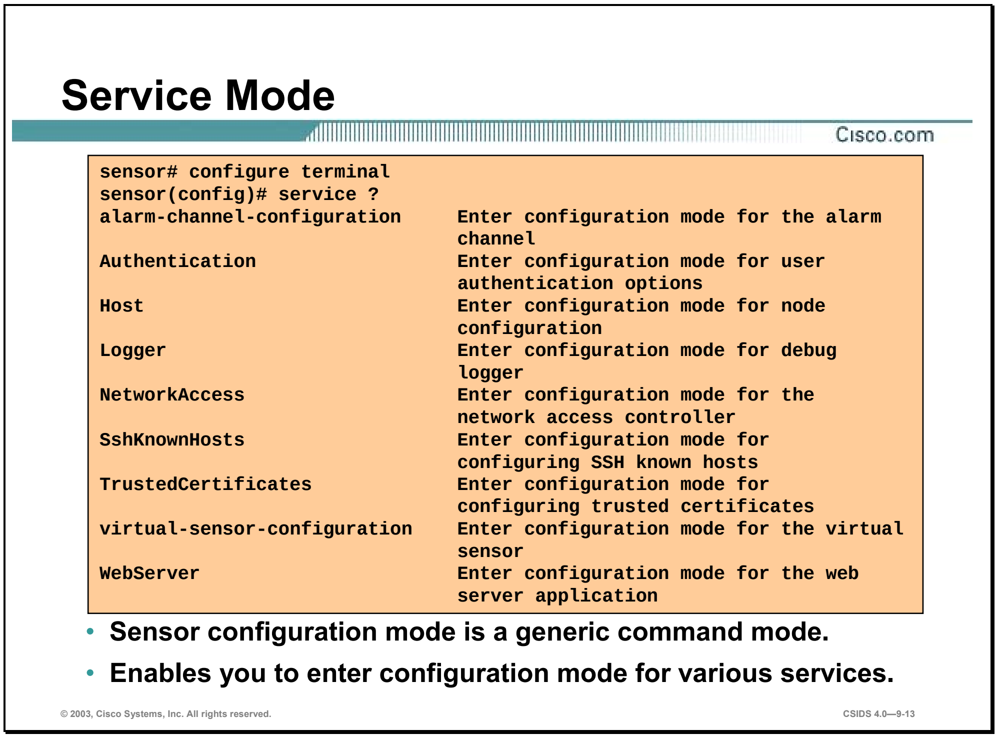
```
sensor# configure terminal
sensor(config)# interface sensing int0
sensor(config-ifs)#
```

- Interface sensing configuration mode is a third level of the CLI.
- The following task is performed in interface sensing configuration mode:
  - Enable or disable the sensing interface.

CSIDS 4.0—9-12

The interface sensing configuration mode is a third level of the CLI. It enables you to enable or disable the sensing interface. The following example shows the commands available in the interface sensing configuration mode:

```
sensor1(config)# interface sensing int0
sensor1(config-ifs)# ?
end          Exit interface sensing configuration mode and return to exec mode
exit         Exit interface sensing configuration mode and return to global
             configuration mode
no           Remove configuration
show         Display history information
shutdown     Disable the sensing interface
```



Service Mode

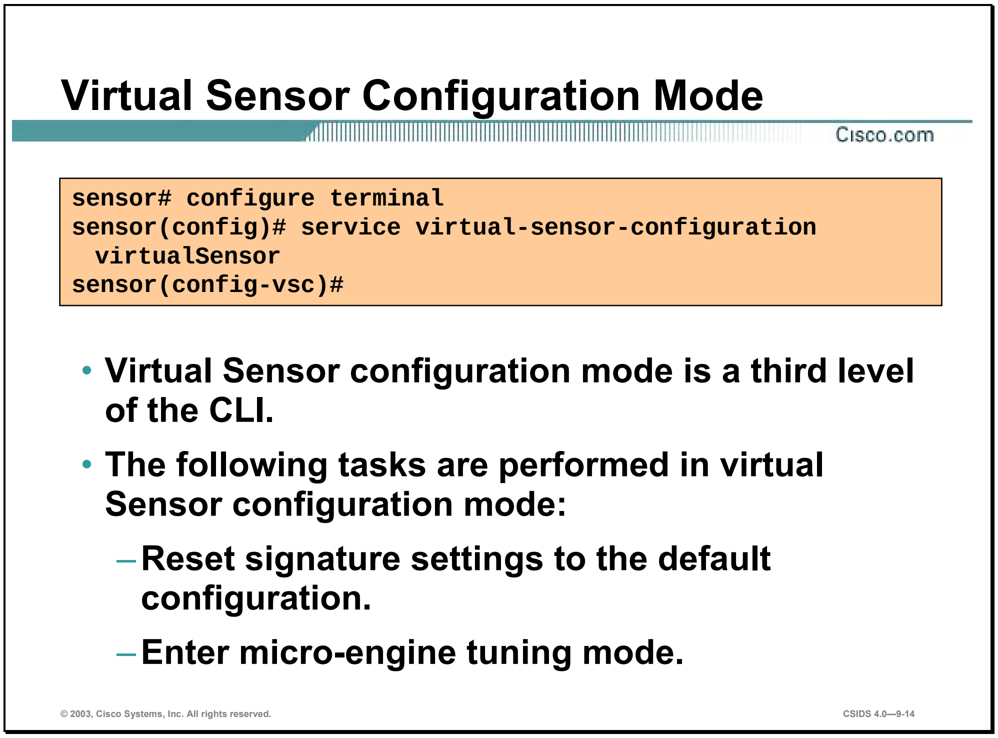
```
sensor# configure terminal
sensor(config)# service ?
alarm-channel-configuration     Enter configuration mode for the alarm
                                channel
Authentication                  Enter configuration mode for user
                                authentication options
Host                            Enter configuration mode for node
                                configuration
Logger                          Enter configuration mode for debug
                                logger
NetworkAccess                   Enter configuration mode for the
                                network access controller
SshKnownHosts                   Enter configuration mode for
                                configuring SSH known hosts
TrustedCertificates             Enter configuration mode for
                                configuring trusted certificates
virtual-sensor-configuration    Enter configuration mode for the virtual
                                sensor
WebServer                       Enter configuration mode for the web
                                server application
```

- **Sensor configuration mode is a generic command mode.**
- **Enables you to enter configuration mode for various services.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—9-13

The service mode is a generic command mode. It enables you to enter configuration mode for various services. The following example shows the commands available in service mode:

```
sensor1(config)# service ?
alarm-channel-configuration      Enter configuration mode for the alarm
                                 channel
Authentication                   Enter configuration mode for user
                                 authentication options
Host                             Enter configuration mode for node
                                 configuration
Logger                           Enter configuration mode for debug logger
NetworkAccess                    Enter configuration mode for the network
                                 access controller
SshKnownHosts                    Enter configuration mode for configuring SSH
                                 known hosts
TrustedCertificates              Enter configuration mode for configuring
                                 trusted certificates
virtual-sensor-configuration     Enter configuration mode for the virtual
                                 sensor
WebServer                        Enter configuration mode for the web server
                                 application
```



Virtual Sensor Configuration Mode

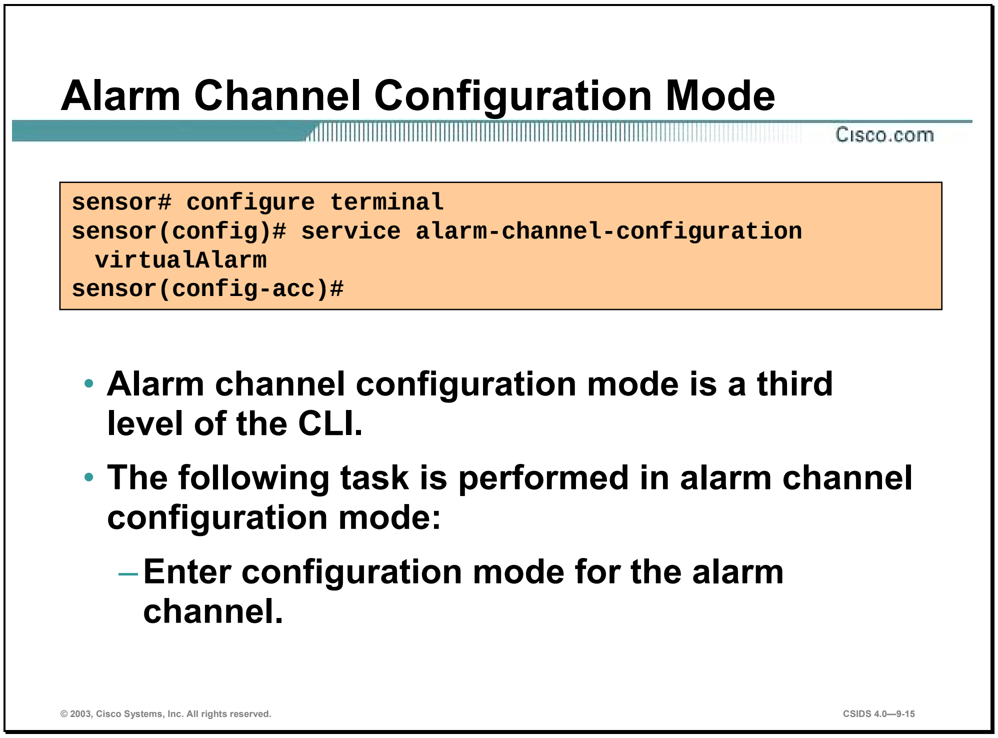
```
sensor# configure terminal
sensor(config)# service virtual-sensor-configuration
  virtualSensor
sensor(config-vsc)#
```

- Virtual Sensor configuration mode is a third level of the CLI.
- The following tasks are performed in virtual Sensor configuration mode:
  - Reset signature settings to the default configuration.
  - Enter micro-engine tuning mode.

CSIDS 4.0—9-14

The virtual sensor configuration mode is a third level of the CLI. It enables you to reset signature settings to the default configuration. The following example shows the commands available in the virtual sensor configuration mode:

```
sensor1(config)# service virtual-sensor-configuration virtualSensor
sensor1(config-vsc)# ?
exit                    Exit configuration mode and return to global
                        configuration mode
reset-signatures        Reset signatures settings back to the default
                        configuration
show                    Display system settings and/or history information
tune-micro-engines      Enter micro-engine tuning mode
```



Alarm Channel Configuration Mode

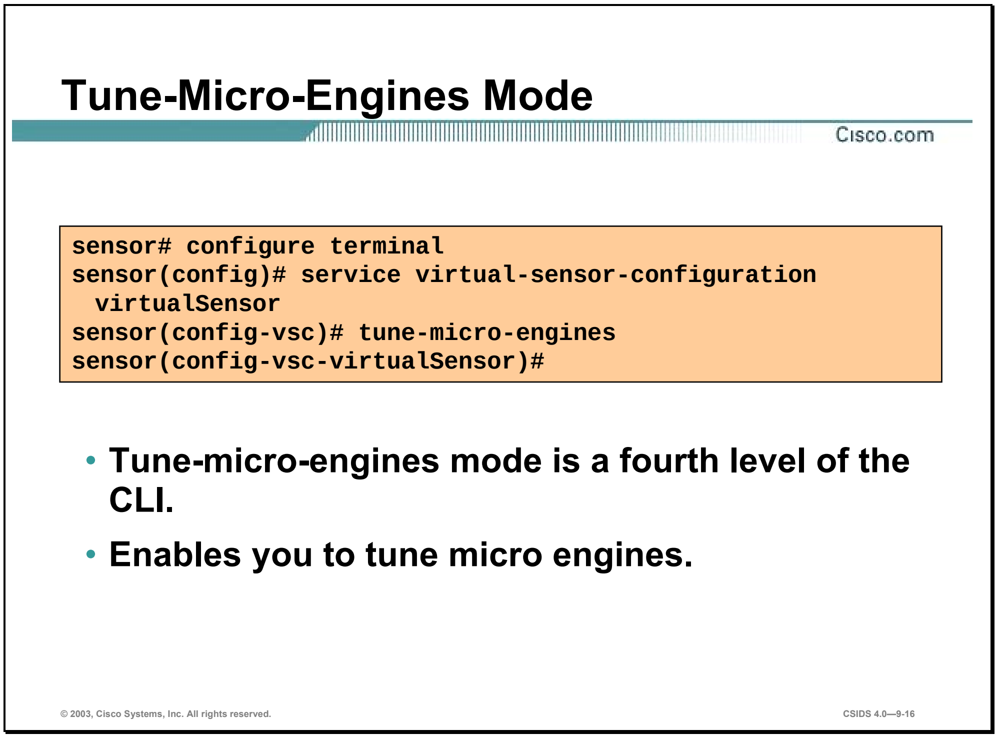
```
sensor# configure terminal
sensor(config)# service alarm-channel-configuration
 virtualAlarm
sensor(config-acc)#
```

- **Alarm channel configuration mode is a third level of the CLI.**
- **The following task is performed in alarm channel configuration mode:**
  - **Enter configuration mode for the alarm channel.**

CSIDS 4.0—9-15

The alarm channel configuration mode is a third level of the CLI. It enables you to enter configuration mode for the alarm channel. The following example shows the commands available in the alarm channel configuration mode:

```
sensor1(config)# service alarm-channel-configuration virtualAlarm
sensor1(config-acc)# ?
end                      Exit configuration mode and return to exec mode
exit                     Exit configuration mode and return to global
                         configuration mode
show                     Display history information
tune-alarm-channel       Enter configuration mode for the alarm channel
```



Tune-Micro-Engines Mode

Cisco.com

```
sensor# configure terminal
sensor(config)# service virtual-sensor-configuration
  virtualSensor
sensor(config-vsc)# tune-micro-engines
sensor(config-vsc-virtualSensor)#
```

- **Tune-micro-engines mode is a fourth level of the CLI.**
- **Enables you to tune micro engines.**

CSIDS 4.0—9-16

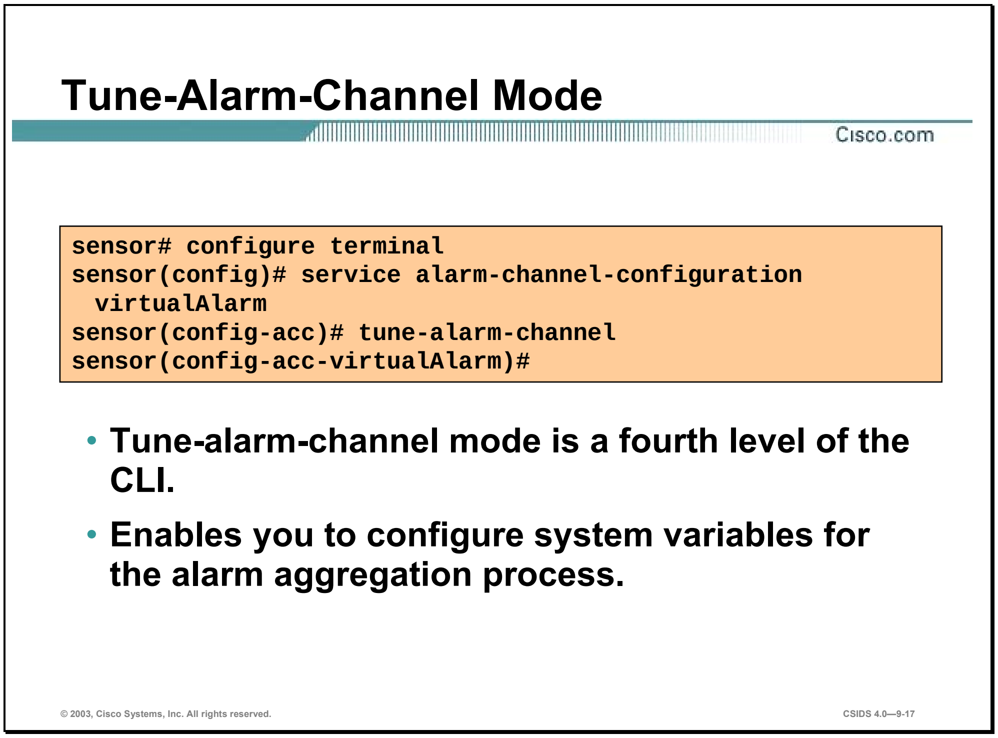
The tune-micro-engines mode is a fourth level of the CLI. It enables you to tune micro engines. The following example shows the commands available in the tune-micro-engines mode:

Note Micro-engines are explained later in the course.

```
sensor1(config)# service virtual-sensor-configuration virtualSensor
sensor1(config-vsc)# tune-micro-engines
sensor1(config-vsc-virtualSensor)# ?
ATOMIC.ARP                        Layer 2 ARP signatures.
ATOMIC.ICMP                       Simple ICMP alarms based on Type, Code, Seq,
                                  Id, etc.
ATOMIC.IPOPTIONS                  Simple L3 Alarms based on Ip Options
ATOMIC.L3.IP                      Simple L3 IP Alarms.
ATOMIC.TCP                        Simple TCP packet alarms based on TCP Flags,
                                  ports (both sides), and single packet regex.
                                  Use SummaryKey to define the address view for
                                  MinHits and Summarize counting. For best
                                  performance, use a StorageKey of xxxx.
ATOMIC.UDP                        Simple UDP packet alarms based on Port,
                                  Direction and DataLength.
exit                              Exit service configuration mode
FLOOD.HOST.ICMP                   Icmp Floods directed at a single host
FLOOD.HOST.UDP                    UDP Floods directed at a single host
FLOOD.NET                         Multi-protocol floods directed at a network
                                  segment. Ip Addresses are wildcarded for this
```

```
                                 inspection.
FragmentReassembly               Fragment Reassembly configuration tokens
IPLog                            Virtual Sensor IP log configuration tokens
OTHER                            This engine is used to group generic
                                 signatures so common parameters may be
                                 changed.  It defines an interface into common
                                 signature parameters..
SERVICE.DNS                      DNS SERVICE Analysis Engine
SERVICE.FTP                      FTP service special decode alarms
SERVICE.GENERIC                  Custom service/payload decode and analysis
                                 based on our quartet tuple programming
                                 language. EXPERT use only.
SERVICE.HTTP                     HTTP protocol decode based string search
                                 Engine. Includes anti-evasive URL
                                 deobfuscation
SERVICE.IDENT                    Ident service (client and server) alarms.
SERVICE.MSSQL                    Microsoft (R) SQL service inspection engine
SERVICE.NTP                      Network Time Protocol based signature engine
SERVICE.RPC                      RPC SERVICE analysis engine
SERVICE.SMB                      SMB Service decode inspection.
SERVICE.SMTP                     SMTP Protocol Inspection Engine
SERVICE.SNMP                     Inspects SNMP traffic
SERVICE.SSH                      SSH header decode signatures.
SERVICE.SYSLOG                   Engine to process syslogs.
show                             Display system settings and/or history
                                 information
ShunEvent                        Shun Event configuration tokens
STATE.STRING.CISCOLOGIN          Telnet based Cisco Login Inspection Engine
STATE.STRING.LPRFORMATSTRING     LPR Protocol Inspection Engine
StreamReassembly                 Stream Reassembly configuration tokens
STRING.ICMP                      Generic ICMP based string search Engine
STRING.TCP                       Generic TCP based string search Engine.
STRING.UDP                       Generic UDP based string search Engine
SWEEP.HOST.ICMP                  ICMP host sweeps from a single attacker to
many victims.
SWEEP.HOST.TCP                   TCP-based Host Sweeps from a single attacker
to                                        multiple victims.
SWEEP.MULTI                      UDP and TCP combined port sweeps.
SWEEP.OTHER.TCP                  Odd sweeps/scans such as nmap fingerprint
                                          scans.
SWEEP.PORT.TCP                   Detects port sweeps between two nodes.
SWEEP.PORT.UDP                   Detects UDP connections to multiple
                                 destination ports between two nodes.
systemVariables                  User modifiable system variables
TRAFFIC.ICMP                     Identifies ICMP traffic irregularities.
TROJAN.BO2K                      BackOrifice BO2K trojan traffic
```

TROJAN.TFN2K	TFN2K trojan/ddos traffic
TROJAN.UDP	Detects BO/BO2K UDP trojan traffic.



Tune-Alarm-Channel Mode

Cisco.com

```
sensor# configure terminal
sensor(config)# service alarm-channel-configuration
  virtualAlarm
sensor(config-acc)# tune-alarm-channel
sensor(config-acc-virtualAlarm)#
```

- Tune-alarm-channel mode is a fourth level of the CLI.
- Enables you to configure system variables for the alarm aggregation process.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—9-17

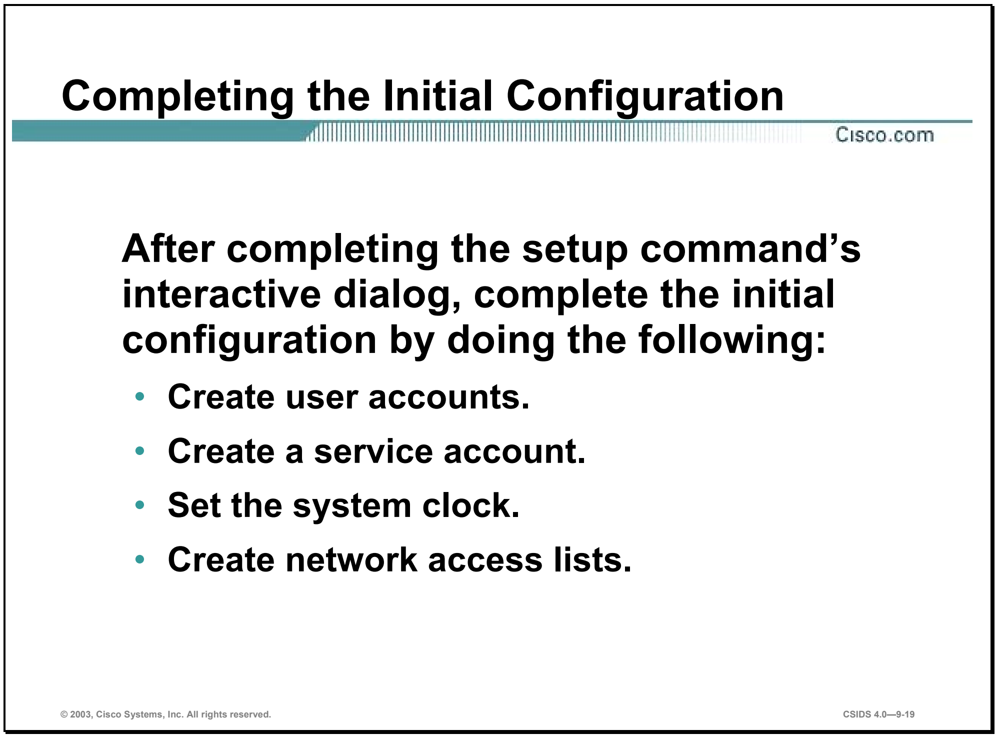
The tune-alarm-channel mode is a fourth level of the CLI. It enables you to configure system variables for the alarm aggregation process. System variables are used when configuring alarm channel event filters. When you want to use the same value within multiple filters, use a variable. When you change the value of a variable, the variables in all the filters are updated. The following example shows the commands available in the tune-alarm-channel mode:

```
sensor1(config)# service alarm-channel-configuration virtualAlarm
sensor1(config-acc)# tune-alarm-channel
sensor1(config-acc-virtualAlarm)# ?
EventFilter                         Configuration for the Event Filters
exit                                Exit service configuration mode
show                                Display history information
systemVariables                     User modifiable system variables
```

Note Event filters are explained later in the course.

Initial Configuration Tasks

This section explains the commands needed to perform the initial Sensor configuration.



Completing the Initial Configuration

Cisco.com

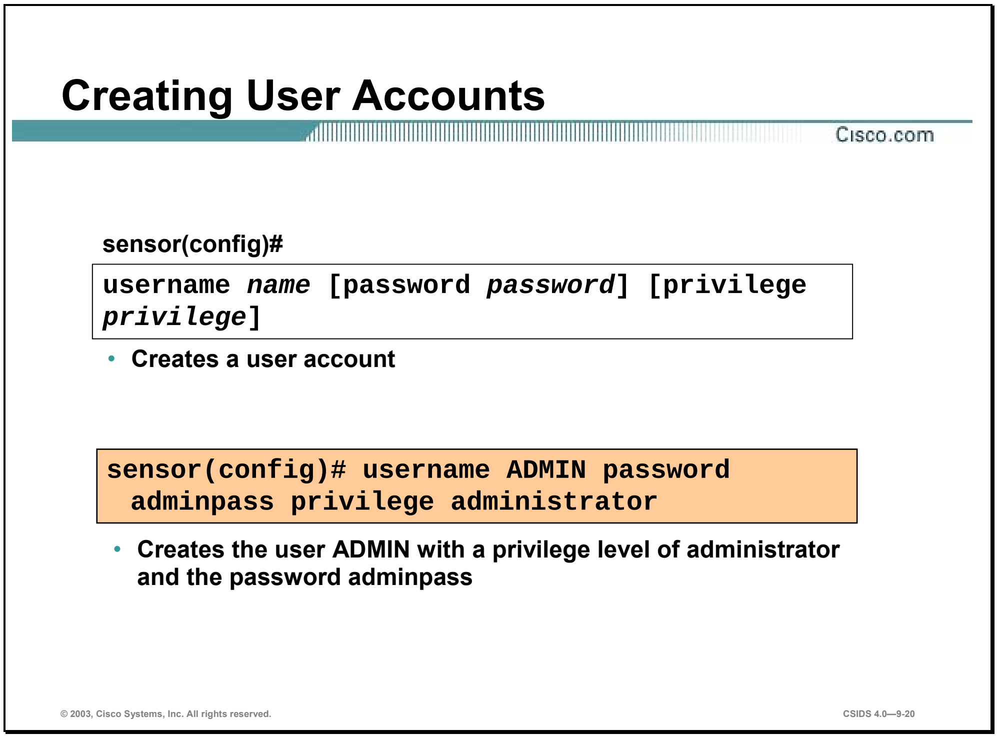
After completing the setup command's interactive dialog, complete the initial configuration by doing the following:

- **Create user accounts.**
- **Create a service account.**
- **Set the system clock.**
- **Create network access lists.**

CSIDS 4.0—9-19

After completing the setup command's interactive dialog, complete the initial configuration by doing the following:

- Create user accounts to enable users to access the Sensor.
- Create a service account for troubleshooting purposes.
- Set the system clock.
- Create network access lists to specify hosts that are allowed to connect to the Sensor.



Creating User Accounts

Cisco.com

sensor(config)#

```
username name [password password] [privilege
privilege]
```

- Creates a user account

```
sensor(config)# username ADMIN password
  adminpass privilege administrator
```

- Creates the user ADMIN with a privilege level of administrator and the password adminpass

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-20

Use the **username** command to create user accounts. The **show users all** command displays a list of all user accounts. You can use the **no username** command to delete a user and thus prevent access to the Sensor; however, Sensors do not allow the last administrative account to be removed. You can delete a user account while the user is logged in to the system, but the deletion does not take effect until the user has exited all logon sessions.

Only users with administrator privileges can add and remove user accounts. The **username** command provides username and password authentication for login purposes only.

The syntax for the **username** command is as follows:

username *name*[password *password*][privilege *privilege*]

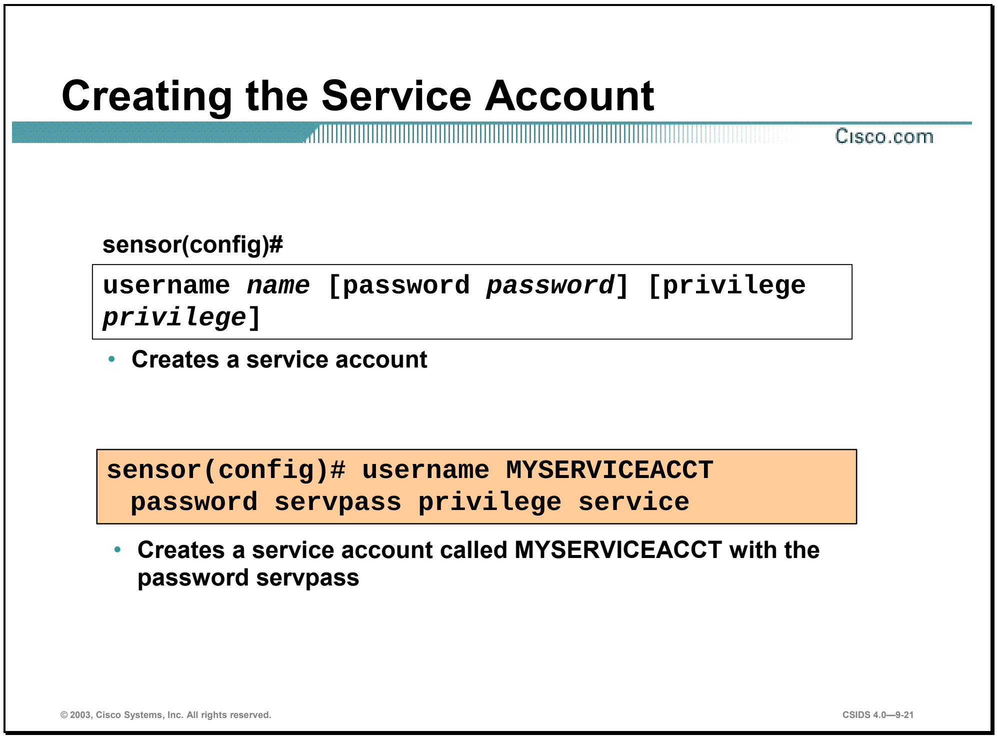
name	Specifies the username. A valid username is 1-32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).
password	Specifies the password for the user.
privilege	Sets the privilege level for the user. Allowed levels are Service, Administrator, Operator, or Viewer. The default is Viewer.

Refer to the following list to determine the privilege level you want to assign to users when creating user accounts:

- Administrator—The highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
  - Add users and assign passwords.
  - Enable and disable control of physical interfaces and interface groups.

- Assign physical sensing interfaces to interface groups.
- Modify the list of hosts allowed to connect to the Sensor as configuring or viewing agents.
- Modify Sensor address configuration.
- Tune signatures.
- Assign virtual sensor configuration to interface groups.
- Manage routers.

- Operators—This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
  - Modify their passwords.
  - Tune signatures.
  - Manage routers.
- Viewers—This user role has the lowest level of privileges. Monitoring applications, such as IDS Event Viewer, only require viewer access to the sensor. You can use the CLI to setup a user account with viewer privileges and then configure IDS Event Viewer to use this account to connect to the Sensor. Viewers can view configuration and event data and can perform the following function:
  - Modify their passwords.



Creating the Service Account

Cisco.com

sensor(config)#

```
username name [password password] [privilege
privilege]
```

- Creates a service account

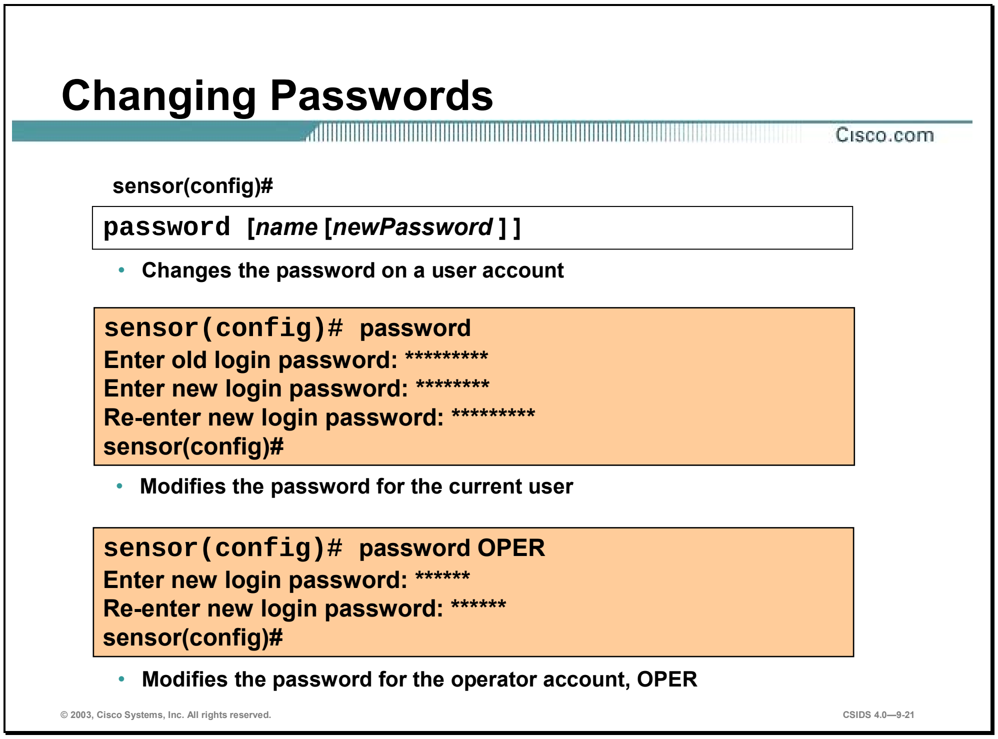
```
sensor(config)# username MYSERVICEACCT
  password servpass privilege service
```

- Creates a service account called MYSERVICEACCT with the password servpass

CSIDS 4.0—9-21

The service account is a special user role. It is created the same way you create any other user account. However, remember that this account should only be used for troubleshooting under the direction of TAC. Only one account with the service privilege can be created.

Caution Do not make modifications to the Sensor through the service account except under the direction of TAC. If you use the service account to configure the Sensor, your configuration is not supported by TAC. TAC also does not support a Sensor on which additional services have been added.



Changing Passwords

Cisco.com

sensor(config)#

```
password [name [newPassword ] ]
```

- Changes the password on a user account

```
sensor(config)# password
Enter old login password: *********
Enter new login password: ********
Re-enter new login password: *********
sensor(config)#
```

- Modifies the password for the current user

```
sensor(config)# password OPER
Enter new login password: ******
Re-enter new login password: ******
sensor(config)#
```

- Modifies the password for the operator account, OPER

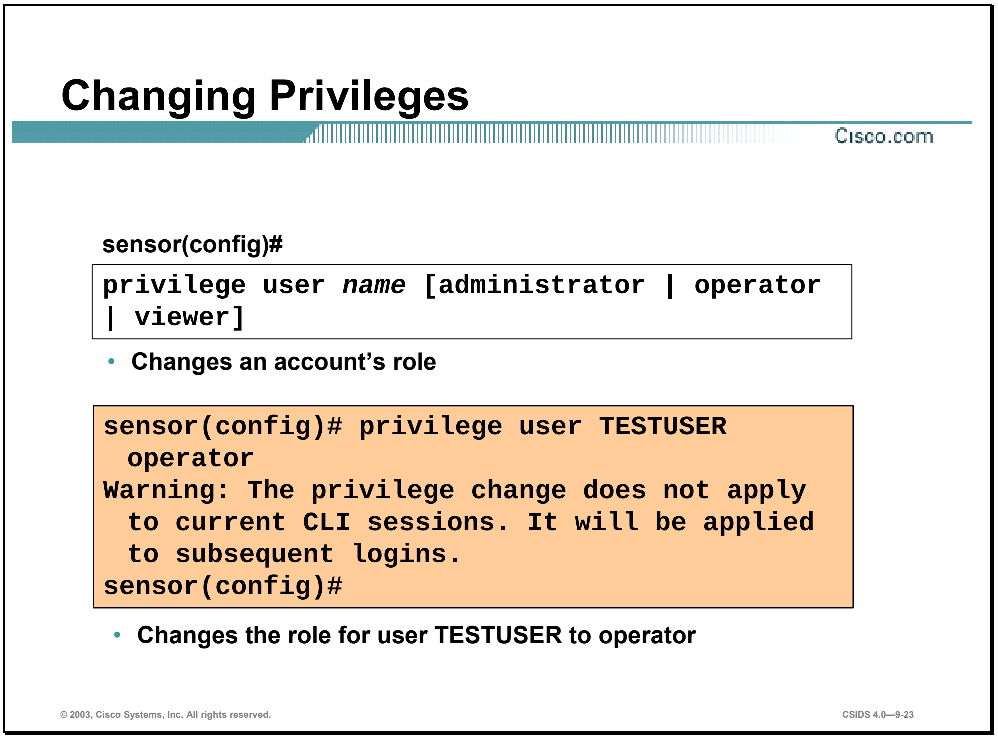
CSIDS 4.0—9-21

You can use the **password** command to change the password for an existing user. Users with administrator privileges can change the passwords of other users. Users with operator and viewer privileges can only modify their own passwords. The figure shows how to modify the password for the current user and how an administrator can modify the password of another user.

The syntax for the **password** command is as follows:

password[name**[**newPassword**]]**

name	Specifies the username. A valid username is 1-32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).
password	The password is requested when the user enters this command. A password can be any printable character, including spaces. A valid password is 6-32 characters long.



Changing Privileges

Cisco.com

sensor(config)#

```
privilege user name [administrator | operator
| viewer]
```

- Changes an account’s role

```
sensor(config)# privilege user TESTUSER
  operator
Warning: The privilege change does not apply
  to current CLI sessions. It will be applied
  to subsequent logins.
sensor(config)#
```

- Changes the role for user TESTUSER to operator

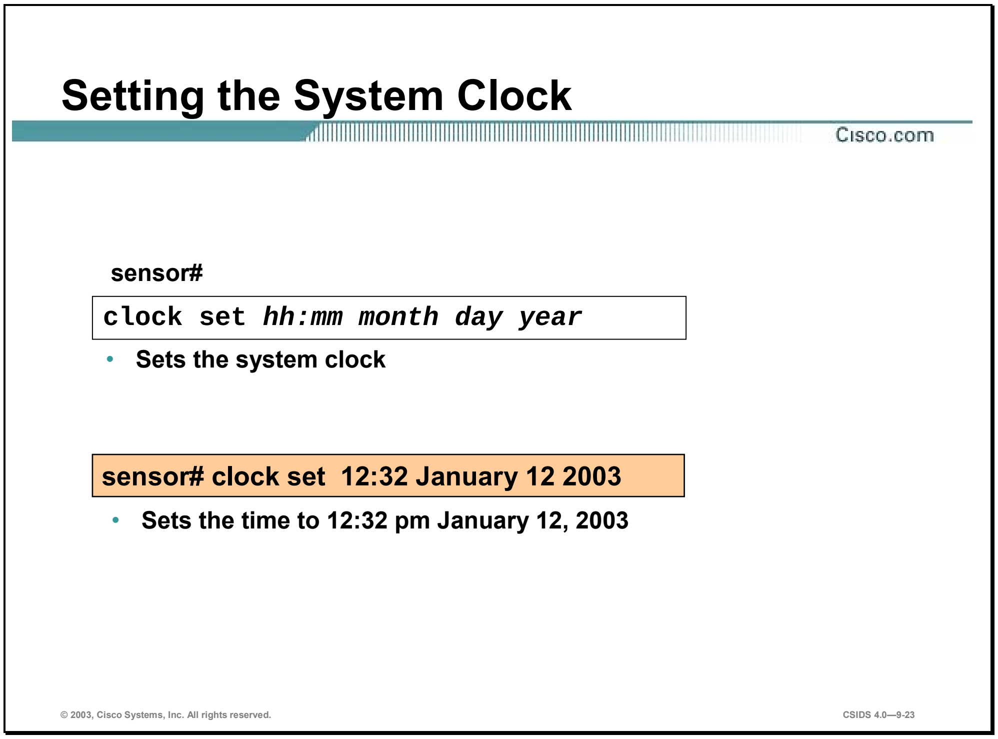
CSIDS 4.0—9-23

An account’s role is changed by using the **privilege** command. Only an administrator can change the privileges on user accounts.

The syntax for the **privilege** command is as follows:

privilege user *name*[administrator | operator | viewer]

name	Specifies the username. A valid username is 1-32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).



Setting the System Clock

Cisco.com

sensor#

```
clock set hh:mm month day year
```

- Sets the system clock

```
sensor# clock set  12:32 January 12 2003
```

- Sets the time to 12:32 pm January 12, 2003

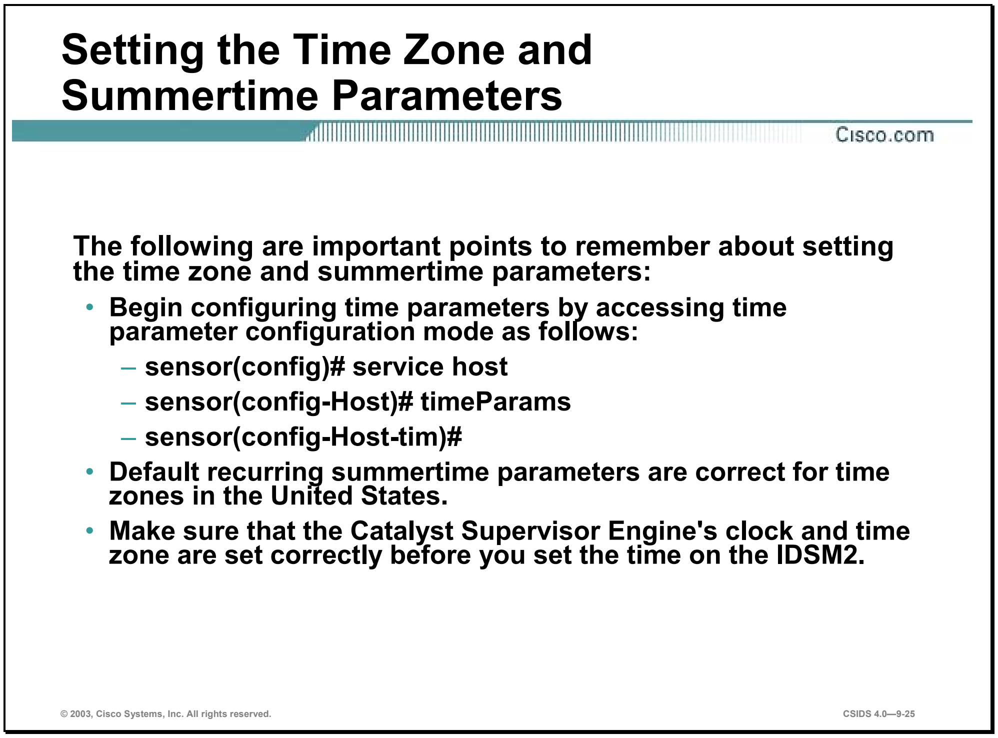
CSIDS 4.0—9-23

You can manually set the system clock of the IDS Sensor appliance. Use the **clock set** command to set the time if no other timing mechanisms are available. If you are using an NTP or VINES clock source, or if you have a router with calendar capability, you do not need to use the **clock set** command to set the system clock. Time can be set only when NTP is disabled.

You can use the **show clock** command to view the time. The syntax for the **clock set** command is as follows:

clock set ***hh:mm:***[***:ss***] ***month day year***

hh:mm [:ss]	Current time in hours (military format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name, no abbreviation).
year	Current year (no abbreviation).



Setting the Time Zone and Summertime Parameters

Cisco.com

The following are important points to remember about setting the time zone and summertime parameters:

- **Begin configuring time parameters by accessing time parameter configuration mode as follows:**
  - **sensor(config)# service host**
  - **sensor(config-Host)# timeParams**
  - **sensor(config-Host-tim)#**
- **Default recurring summertime parameters are correct for time zones in the United States.**
- **Make sure that the Catalyst Supervisor Engine's clock and time zone are set correctly before you set the time on the IDSM2.**

CSIDS 4.0—9-25

The **clock set** command sets the time without changing the time zone. The following is an example of setting the time zone and summertime parameters from the CLI:

Note For further information on setting the time zone and summertime parameters, use the CLI Help or go to the following web site: http://www.cisco.com/en/US/partner/products/sw/secursw/ps2113/products_command_reference_chapter09186a00801471c9.html#256502

Step 1 Enter host configuration mode:

```
sensor(config)# service host
```

Step 2 Enter time parameter configuration mode:

```
sensor(config-Host)# timeParams
```

Step 3 Specify the standard time offset from UTC in minutes. Negative numbers represent time zones west of the Prime Meridian.

```
sensor(config-Host-tim)# offset -360
```

Step 4 Specify the standard time zone:

```
sensor(config-Host-tim)# standardTimeZoneName CST
```

Step 5 Enter summertime parameter configuration mode:

```
sensor(config-Host-tim)# summerTimeParams
```

Step 6 Specify that summertime parameters recur at the same time each year:

```
sensor(config-Host-tim-sum)# active-selection recurringParams
```

Step 7 Enter recurring summertime parameter configuration mode:

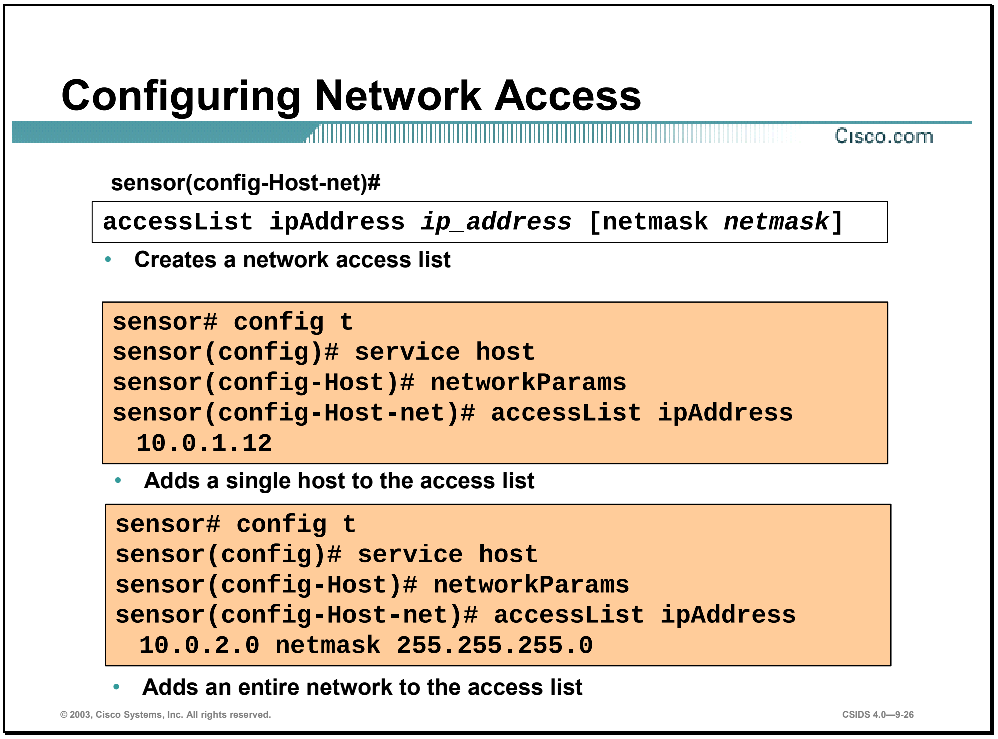
```
sensor(config-Host-tim-sum)# recurringParams
```

Step 8 Specify the summertime time zone name:

```
sensor(config-Host-tim-sum-rec)# summerTimeZoneName CDT
```

The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2 a.m. on the first Sunday in April, and a stop time of 2 a.m. on the fourth Sunday in October. The default summertime offset is 60 minutes.

Caution The IDSM2 obtains its time configuration from the Catalyst 6500 family switch. Make sure that the Catalyst Supervisor Engine's clock and time zone are set correctly (unless the IDSM2 is configured to use NTP) before you set the time on the IDSM2. The IDSM2 obtains the current UTC time from the Supervisor Engine and applies the time zone settings that are configured in the IDS configuration to calculate the local time. If the Supervisor Engine's time in incorrect, the IDSM2's local time will also be incorrect.



Configuring Network Access

sensor(config-Host-net)#

```
accessList ipAddress ip_address [netmask netmask]
```

- Creates a network access list

```
sensor# config t
sensor(config)# service host
sensor(config-Host)# networkParams
sensor(config-Host-net)# accessList ipAddress
  10.0.1.12
```

- Adds a single host to the access list

```
sensor# config t
sensor(config)# service host
sensor(config-Host)# networkParams
sensor(config-Host-net)# accessList ipAddress
  10.0.2.0 netmask 255.255.255.0
```

- Adds an entire network to the access list

CSIDS 4.0—9-26

Use the **accessList** command to modify the network access lists to allow remote access. The **accessList** command enables the network security administrator to set any number of IP addresses (either host or network) which are allowed to establish TCP connections to a Sensor. In most cases, access to the Sensor in this manner should be limited to trusted hosts, typically the IDS Manager. This allows the trusted hosts to access the Sensor to help in troubleshooting, or to transfer files when new signatures and product updates are released.

Network access lists are configured within the host service. To configure the access list, complete the following steps:

Step 1 Enter global configuration mode:

```
sensor# configure terminal
sensor(config)#
```

Step 2 Enter host configuration mode:

```
sensor(config)# service host
sensor(config-Host)#
```

Step 3 Enter network parameters configuration mode:

```
sensor(config-Host)# networkParams
sensor(config-Host-net)#
```

Step 4 Remove the default network address entry 10.0.0.0/255.0.0.0:

```
sensor(config-Host-net)# no accessList ipAddress 10.0.0.0 netmask 255.0.0.0
```

Step 5 Use the **accessList** command to add a single host or an entire network to the access list. Use the netmask parameter only if the IP address is a network address (as opposed to a host address).

```
sensor(config-Host-net)# accessList ipAddress 10.0.1.12
sensor(config-Host-net)# accessList ipAddress 10.10.10.0 netmask 255.255.255.0
```

Step 6 Repeat Step 5 for each address that you want to add to the access list.

You can view the current network parameters settings by using the **show settings** command in the network parameters configuration mode. The following is an example of the **show settings** output:

```
sensor(config-Host-net)# show settings
networkParams
——————————————————————-
ipAddress: 10.0.1.4
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.0.1.2
hostname: sensor1
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 1)
———————————————————————-
ipAddress: 10.0.1.12
netmask: 255.255.255.255 <defaulted>
———————————————————————-
ipAddress: 10.10.10.0
netmask: 255.255.255.0 default: 255.255.255.255
```

Step 7 Exit network parameters configuration mode:

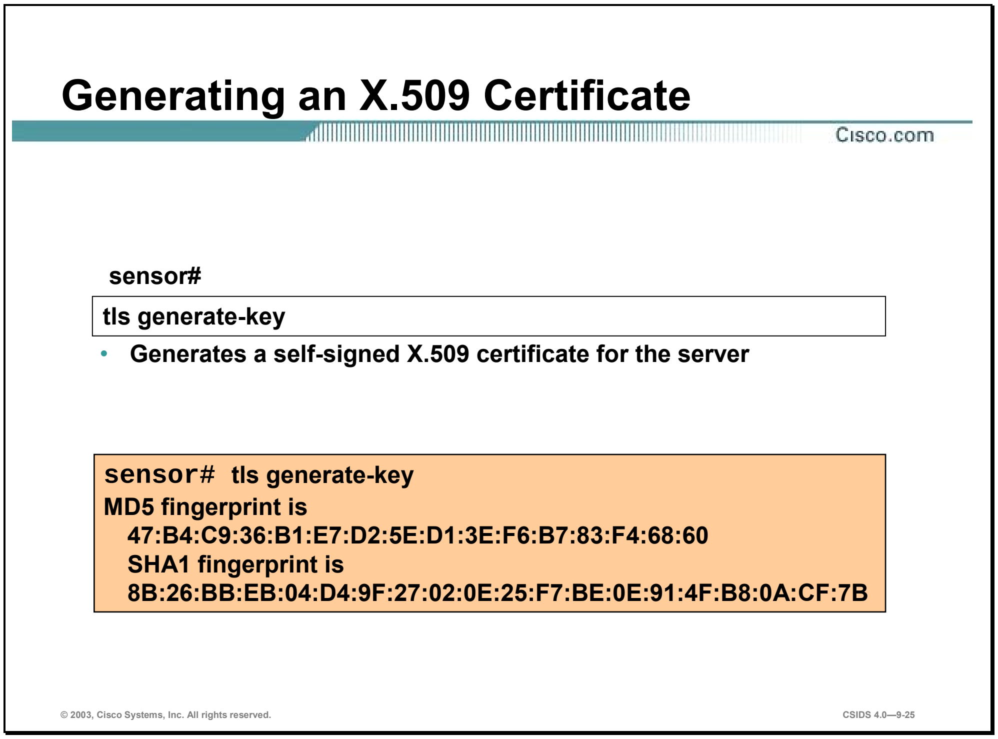
```
sensor(config-Host-net)# exit
sensor(config-Host)#
```

Step 8 Exit configure host mode. Enter **yes** when prompted to apply your changes.

The syntax for the accessList command is as follows:

accessList ipAddress ***ip_address*** **[netmask** ***netmask*****]**

ip_address	IP address of host that is allowed to access the Sensor or network address of a network that is allowed to access the Sensor.
netmask	Netmask applied to ip_address.



Generating an X.509 Certificate

sensor#

```
tls generate-key
```

- Generates a self-signed X.509 certificate for the server

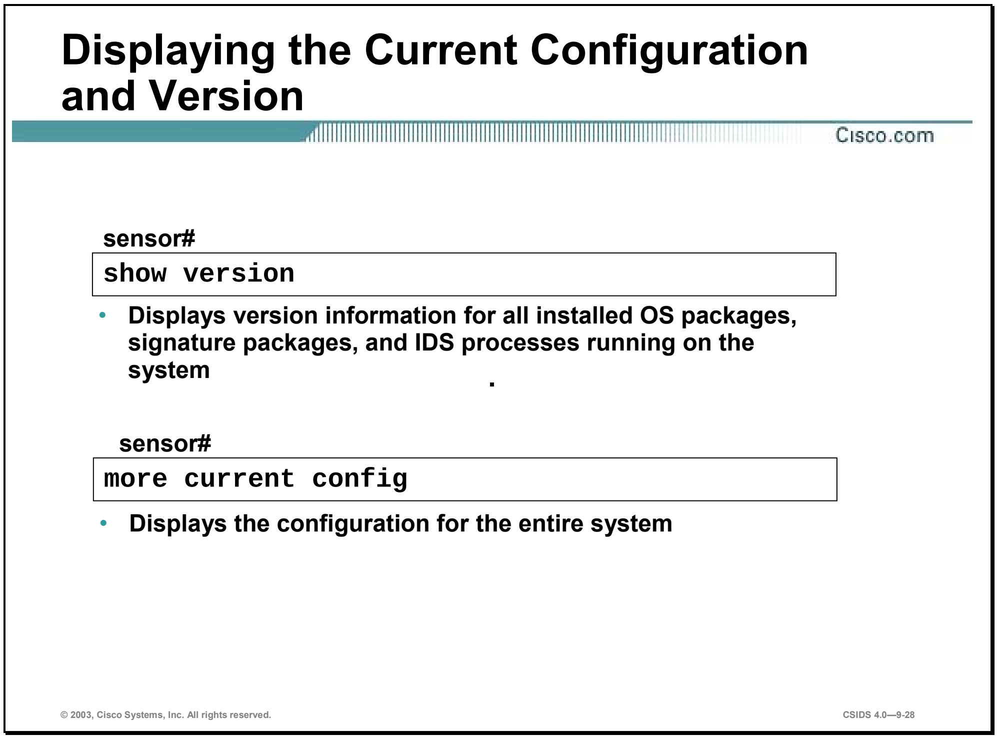
```
sensor#  tls generate-key
MD5 fingerprint is
   47:B4:C9:36:B1:E7:D2:5E:D1:3E:F6:B7:83:F4:68:60
   SHA1 fingerprint is
   8B:26:BB:EB:04:D4:9F:27:02:0E:25:F7:BE:0E:91:4F:B8:0A:CF:7B
```

CSIDS 4.0—9-25

Use the **tls generate-key** command to generate the self-signed X.509 certificate needed by TLS. Any time you change the Sensor's IP address, you will need to generate a new self-signed X.509 certificate. This certificate is needed by HTTPS communications Write down the certificate fingerprints. You will need them to check the authenticity of the certificate when connecting to this Sensor with a web browser.

Preventive Maintenance and Troubleshooting

This section describes commands that can be used for preventive maintenance and troubleshooting.



Displaying the Current Configuration and Version

Cisco.com

sensor#

```
show version
```

- Displays version information for all installed OS packages, signature packages, and IDS processes running on the system

.

sensor#

```
more current config
```

- Displays the configuration for the entire system

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-28

You can display the IDS software version and Sensor configuration. Use the **show version** command to display version information. This command also displays the following information that can be useful for troubleshooting:

- Which applications are running
- The applications' versions
- Disk and memory usage
- Upgrade history

The following is an example of the **show version** command output:

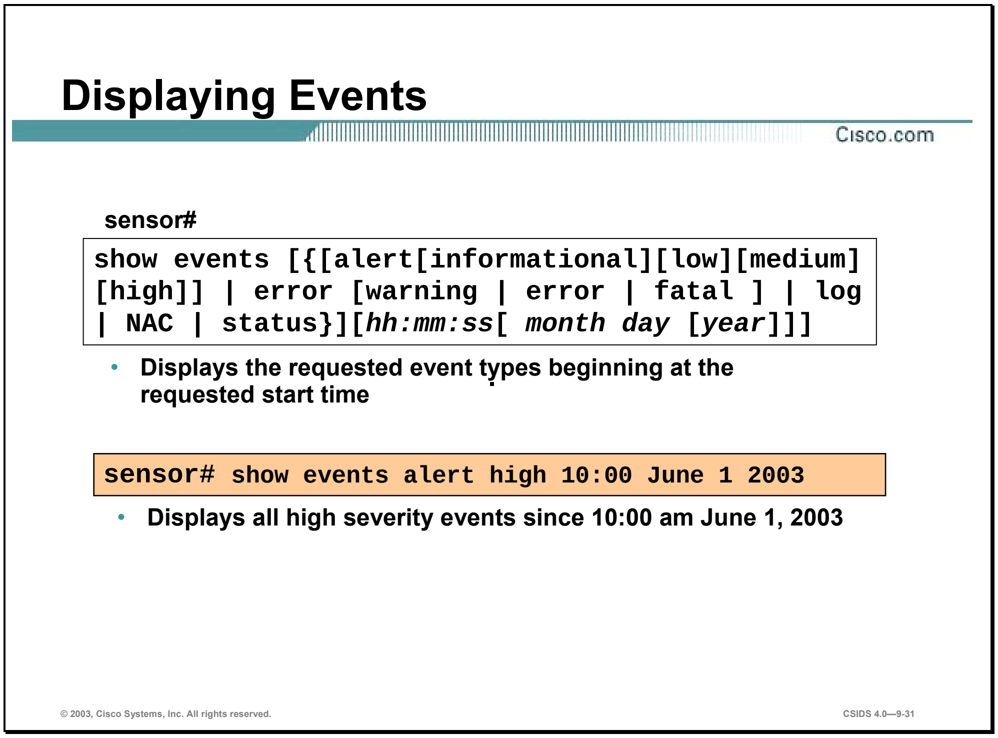
```
sensor# show version
Application Partition:


Cisco Systems Intrusion Detection Sensor, Version
4.0(1)S45


OS Version 2.4.18-5smpbigphys
Platform: IDS-4250
```

```
Sensor up-time is 6 days.
Using 406511616 out of 1846276096 bytes of available memory (22% usage)
Using 544M out of 15G bytes of available disk space (4% usage)

MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600

Upgrade History:

IDS-maj-4.0-1-S45.rpm.pkg 20:43:18 UTC Mon Feb 03 2003

Recovery Partition Version 1.1 - 4.0(1)S45
```

Use the **more current-config** command to view the configuration for the entire system. The following is an example of the **more current-config** command output:

```
sensor# more current-config
! ———————————————
service Authentication
general
attemptLimit 0
methods method Local
exit
exit
exit
! ———————————————
service Host
networkParams
ipAddress 10.0.1.4
netmask 255.255.255.255
defaultGateway 10.0.1.2
hostname sensor1
telnetOption disabled
accessList ipAddress 10.0.1.12 netmask 255.255.255.255
accessList ipAddress 10.10.10.0 netmask 255.255.255.0
exit
optionalAutoUpgrade
active-selection autoUpgradeParams
autoUpgradeParams
schedule
```

```
active-selection calendarUpgrade
calendarUpgrade
timesOfDay time 14:40:00
daysOfWeek day wed
exit
exit
ipAddress 10.89.149.10
directory var/relupdates
username netrangr
password 12345
fileCopyProtocol ftp
exit
exit
timeParams
offset -360
standardTimeZoneName CST
summerTimeParams
active-selection none
exit
exit
exit
```



Displaying Events

sensor#

```
show events [{[alert[informational][low][medium]
[high]] | error [warning | error | fatal ] | log
| NAC | status}][hh:mm:ss[ month day [year]]]
```

- Displays the requested event types beginning at the requested start time

```
sensor# show events alert high 10:00 June 1 2003
```

- Displays all high severity events since 10:00 am June 1, 2003

CSIDS 4.0—9-31

Events are the data generated by the Sensor applications such as the alerts generated by the sensorApp or errors generated by any application. There are currently five types of events:

- evAlert—Intrusion detection alerts
- evError—Application errors
- evStatus—Status changes such as an IP log being created
- evLogTransaction—Record of control transactions processed by each Sensor application
- evShunRqst—Shuns requests

All events are stored in the Sensor eventStore. Events remain in the eventStore until they are overwritten by newer events. It takes 4 GB of newer events to overwrite an existing event. Events can be retrieved through the Sensor's web server via RDEP communications. Management applications such as IEV and the Security Monitor use RDEP to retrieve events from the Sensor. Events can also be viewed from the CLI's top-level prompt using the **show events c**ommand. You can display new events, events from a specific time and events of a specific severity.

The **show events** command displays the requested event types beginning at the requested start time. If no start time is entered, the selected events are displayed beginning at the current time. If no event types are entered, all events are displayed. Events are displayed as a live feed. You can cancel the live feed by the pressing **Control>C**.

This command is helpful for troubleshooting event capture issues in which you are not seeing events in IEV or the Security Monitor, and you are trying to determine which events are being generated on the Sensor. A user with the administrator privilege can use the **clear events** command to remove all events from the eventStore.

Note The IDIOM specification describes the event types in greater detail.

The syntax for the **show events** command is as follows:

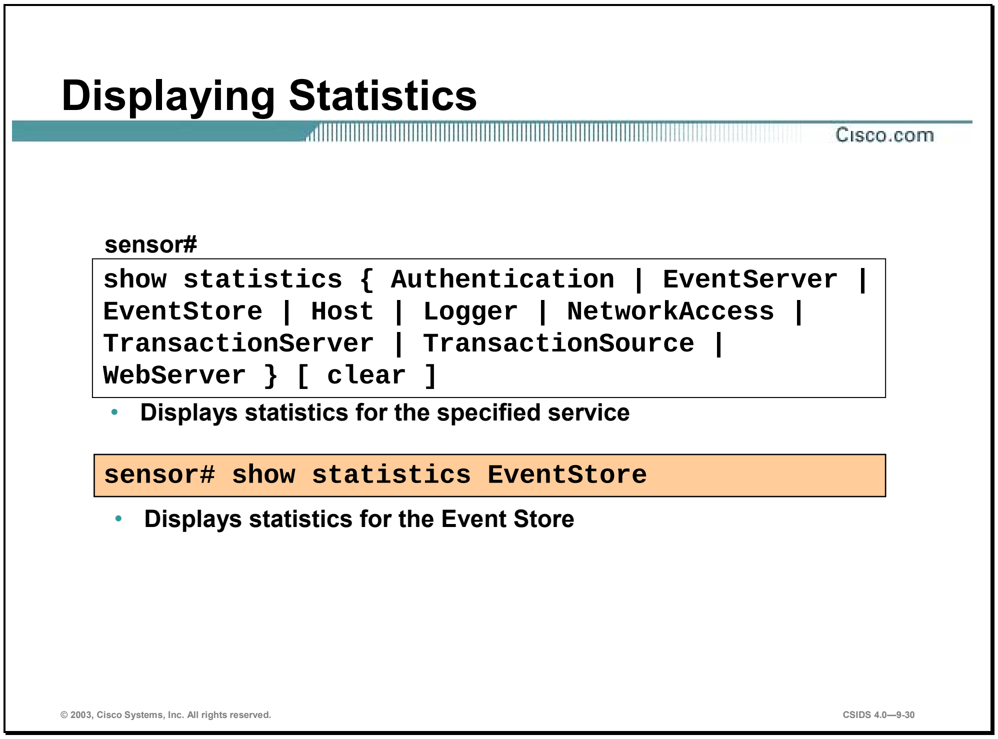
show events [{ [alert [informational] [low] [medium] [high]] | error [warning | error | fatal] | log | NAC | status}] [*hh:mm:ss[month day* [*year*]]]

alert	Display alerts. Provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis-engine whenever an IDS signature is triggered by network activity. If no level is selected (informational, low, medium, high), all alert events are displayed.
error	Display error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
log	Display log events. These events are generated whenever a transaction is received and responded to by an application. Contains information about the request, response, and success or failure of the transaction.
NAC	Display Network Access Control requests (shun requests).
status	Displays status events.
hh:mm:ss	Start time in hours (military format), minutes and seconds.
day	Start day (by date) in the month.
month	Start month (by name).
year	Start year.

The following example shows the output from the **show events** command:

```
sensor# show events 10:00:00 Dec 25 2000
evAlert: eventId=1025376040313262350 severity=high
originator:
deviceName: sensor1
appName: sensorApp
time: 2002/07/30 18:24:18 2002/07/30 12:24:18 CST
signature: sigId=4500 subSigId=0 version=1.0 IOS Embedded SNMP
Community Names
participants:
attack:
attacker: proxy=false
addr: 132.206.27.3
port: 61476
victim:
addr: 132.202.9.254
port: 161
```

```
        protocol: udp
```



Displaying Statistics

Cisco.com

sensor#

```
show statistics { Authentication | EventServer |
EventStore | Host | Logger | NetworkAccess |
TransactionServer | TransactionSource |
WebServer } [ clear ]
```

- Displays statistics for the specified service

```
sensor# show statistics EventStore
```

- Displays statistics for the Event Store

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-30

Statistics provide a snapshot of Sensor services' current internal state; therefore, they can be very useful for troubleshooting. The statistics content is specific to the service that provides it. The CLI command **show statistics ?** lists the services that provide statistics.

Use the **show statistics** command to display the requested statistics. The syntax for the show statistics command is as follows:

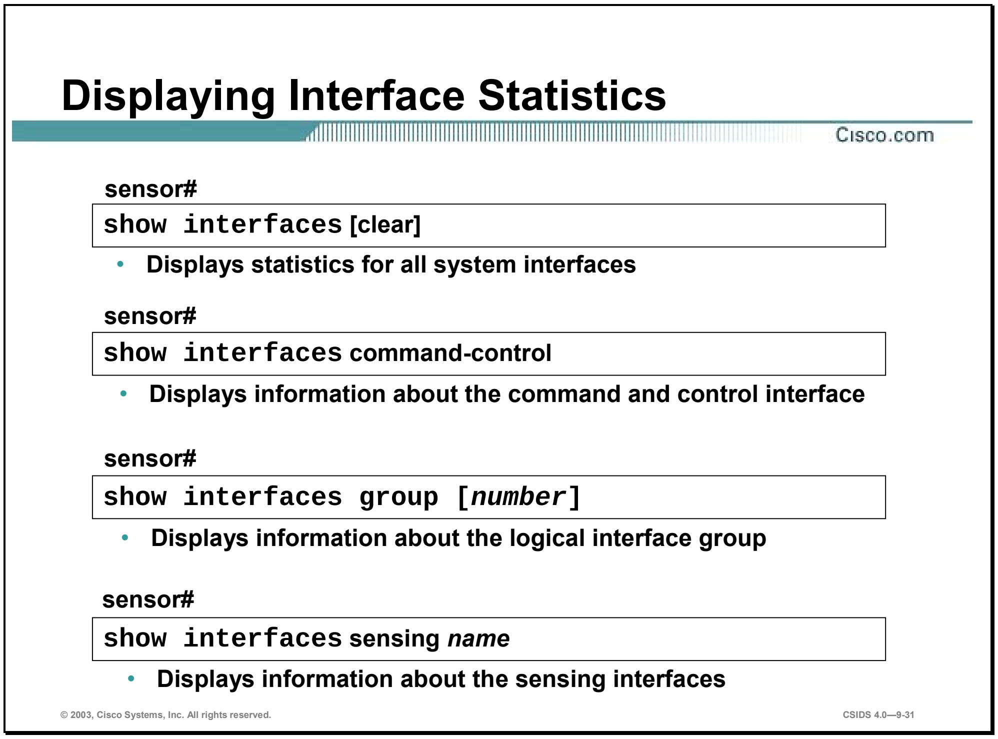
show statistics { Authentication | EventServer | EventStore | Host | Logger | NetworkAccess | TransactionServer | TransactionSource | WebServer } [clear]

Authentication	Display authorizations-authentication statistics.
EventServer	Display event server statistics.
EventStore	Display event store statistics.
Host	Display host (main) statistics.
Logger	Display logger statistics.
NetworkAccess	Display network-access-controller statistics.
TransactionServer	Display transaction server statistics.
TransactionSource	Display transaction source statistics.
WebServer	Display web-server statistics.
clear	Clear the statistics after they are retrieved. This option is not available for Host or NetworkAccess statistics.

The following is an example of **show statistics** output:

```
sensor# show statistics EventStore
Event store statistics
```

```
GENERAL INFORMATION ABOUT THE EVENT STORE
THE CURRENT NUMBER OF OPEN SUBSCRIPTIONS = 0
THE NUMBER OF EVENTS LOST BY SUBSCRIPTIONS AND QUERIES = 0
THE NUMBER OF QUERIES ISSUED = 0
THE NUMBER OF TIMES THE EVENT STORE CIRCULAR BUFFER HAS WRAPPED = 0
NUMBER OF EVENTS OF EACH TYPE CURRENTLY STORED
DEBUG EVENTS = 0
STATUS EVENTS = 8
LOG TRANSACTION EVENTS = 45
SHUN REQUEST EVENTS = 0
ERROR EVENTS, WARNING = 0
ERROR EVENTS, ERROR = 0
ERROR EVENTS, FATAL = 0
ALERT EVENTS, INFORMATIONAL = 2
ALERT EVENTS, LOW = 0
ALERT EVENTS, MEDIUM = 0
ALERT EVENTS, HIGH = 0
```



Displaying Interface Statistics

sensor#

```
show interfaces [clear]
```

- Displays statistics for all system interfaces

sensor#

```
show interfaces command-control
```

- Displays information about the command and control interface

sensor#

```
show interfaces group [number]
```

- Displays information about the logical interface group

sensor#

```
show interfaces sensing name
```

- Displays information about the sensing interfaces

CSIDS 4.0—9-31

The **show interfaces** commands display statistics for the command-control and sensing interfaces and interface groups. The **clear** option clears statistics that can be reset.

The syntax for the **show interfaces** commands is as follows:

show interfaces [clear]

show interfaces group [number**]**

show interfaces sensing [*name*]

show interfaces command-control

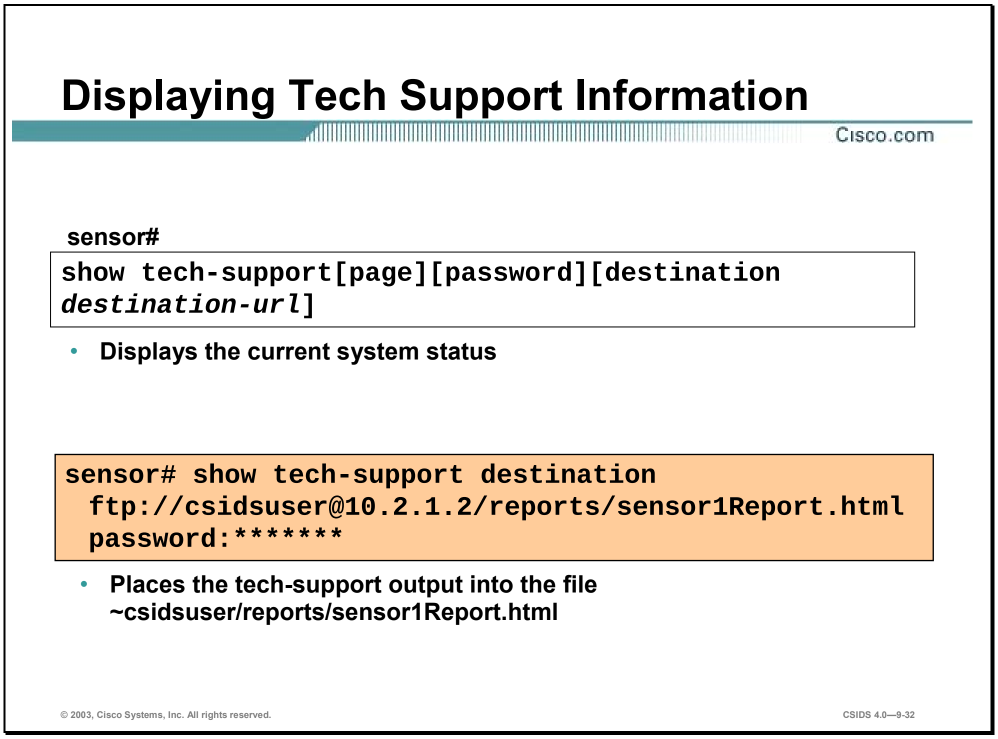
clear	Clear the diagnostics.
number	Logical number for interface group. Valid values are 0-7. If no group number is provided, the command displays information about all interface groups.
name	Logical interface name (int0, int1, and so on).

Use the **show interfaces group** command to display only information about a logical interface group. Use the **show interfaces sensing** command to display only information about the sensing interface. Use the **show interfaces command-control** command to display only information about the command and control interface. The first line of the output indicates if the interface is up or down. For IDS, the command and control interface should always be up. If the output says "command-control interface is down," there is a hardware issue, a cabling issue, or an IP address conflict.

The following is an example of the **show interfaces command-control** command output:

```
sensor#show interfaces command-control
```

```
command-control is up
Internet address is 10.0.1.4, subnet mask is
255.255.255.0, telnet is disabled.
Hardware is eth1, tx
Network Statistics
eth1 Link encap:Ethernet HWaddr 00:06:5B:0F:0E:53
inet addr:10.0.1.4 Bcast:10.0.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:49703 errors:5454 dropped:0 overruns:0
frame:289
TX packets:22928 errors:0 dropped:0 overruns:0
carrier:0
collisions:1913
RX bytes: 17140400 (16.3mb) TX bytes: 11013743
(10.5mb) txqueuelen:100
Interrupt:16 Base address:0xddc0 Memory: feb20000-
feb40000
```



Displaying Tech Support Information

sensor#

```
show tech-support[page][password][destination
destination-url]
```

- **Displays the current system status**

```
sensor# show tech-support destination
  ftp://csidsuser@10.2.1.2/reports/sensor1Report.html
  password:*******
```

- **Places the tech-support output into the file ~csidsuser/reports/sensor1Report.html**

CSIDS 4.0—9-32

The **show tech-support** command captures all status and configuration information on the Sensor. The command allows the information to be transferred to a remote system. The output can be very large. The output includes the current configuration, version information and cidDump information. The cidDump is a script that captures a large amount of information including the process list, log files, OS information, directory listings, package information and configuration files. This information is needed by developers to troubleshoot problems.

The syntax for the **show tech-support command** is as follows:

show tech-support [page][password][destination *destination-url*]

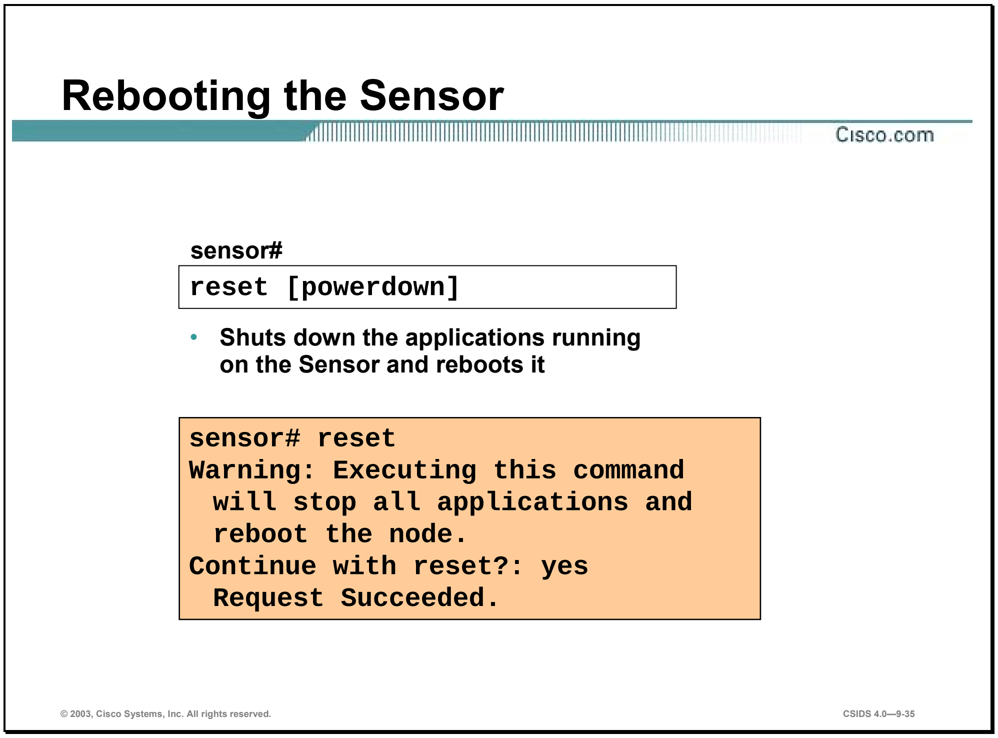
page	(Optional.) Causes the output to display one page of information at a time. Use the Enter key to display the next line of output or use the Spacebar to display the next page of information. If page is not used, the output is displayed without page breaks.
password	(Optional.) Leaves passwords and other security information in the output. If password is not used, passwords and other security sensitive information in the output are replaced with the label <removed> by default.
destination	(Optional.) Tag indicating the information should be formatted as HTML and sent to the destination following this tag.
destination-url	(Optional.) The destination for the report file. If a url is provided, the output will be formatted into an HTML file and sent to the specified destination; otherwise the output is displayed on the screen.

The exact format of the destination URL varies according to the file. You can select a filename, but it must be terminated by .html.

You can specify the following destination types:

- ftp—Destination URL for File Transfer Protocol (FTP) network server. The syntax for this prefix is ftp:[[//username@location]/relativeDirectory]/filename or ftp:[[//username@location]//absoluteDirectory]/filename

- scp—Destination URL for the Secure Copy Protocol (SCP) network server. The syntax for this prefix is scp:[[//username@]location]/relativeDirectory]/filename or scp:[[//username@]location]//absoluteDirectory]/filename



Rebooting the Sensor

sensor#

```
reset [powerdown]
```

- **Shuts down the applications running on the Sensor and reboots it**

```
sensor# reset
Warning: Executing this command
  will stop all applications and
  reboot the node.
Continue with reset?: yes
  Request Succeeded.
```

CSIDS 4.0—9-35

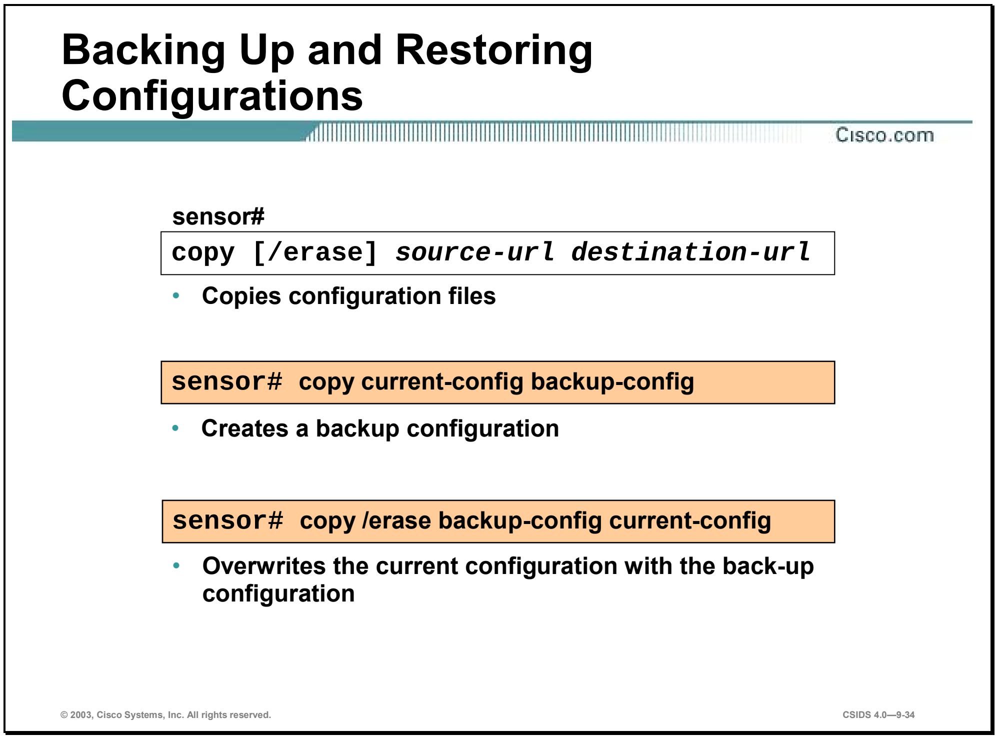
The **reset** command shuts down the applications running on the Sensor and reboots it. If the **powerdown** option is included, the appliance is powered off if possible or left in a state where the power can be turned off.

Shutdown begins immediately after the **reset** command is executed. You are asked if you want to continue with reset. Valid answers to the continue with reset question are yes or no. Y or N are not valid responses.

Because shutdown may take a little time, you may continue to access CLI commands but will be terminated without warning. The syntax for the **reset** command is as follows:

reset [powerdown]

powerdown	This option causes the Sensor to enter a state in which the power can be turned off after the applications are shutdown.



Backing Up and Restoring Configurations

Cisco.com

sensor#

```
copy [/erase] source-url destination-url
```

- Copies configuration files

```
sensor# copy current-config backup-config
```

- Creates a backup configuration

```
sensor# copy /erase backup-config current-config
```

- Overwrites the current configuration with the back-up configuration

CSIDS 4.0—9-34

You can use the **copy** command to make a snapshot of a good configuration. This enables you to copy the current configuration to a back configuration and to restore the current configuration from a back up.

The syntax for the **copy** command is as follows:

copy [/erase]*source-url destination-url*

copy iplog *log-id destination-url*

/erase	(Optional.) Erases the destination file before copying. This keyword only applies to local destinations. It is ignored for remote destinations.
source-url	The location of the source file to be copied. May be a URL or keyword.
destination-url	The location of the destination file to be copied. May be a URL or keyword.
log-id	The log ID of file to copy.

Keywords are used to designate the file location on the Sensor. The following keywords are supported.

Keyword	**Source or Destination**
current-config	The current running configuration. This configuration, unlike IOS version 12.0, becomes persistent as the commands are entered. The file format is CLI commands.

Keyword	Source or Destination
backup-config	Storage location for configuration backup. The file format is CLI commands.
iplog	An IP log contained on the system.

The copy command can be used to do any of the following:

- Transfer configuration to or from another host system using FTP or SCP.
- Copy IP log files to another host system.

Note See the CLI Reference document for the complete copy command specification.

Complete the following steps to backup and restore the Sensor's configuration using the **copy** command:

Step 1 Enter the following command at the privileged exec prompt:

```
sensor# copy current-config backup-config
```

The current configuration is saved in a backup file.

Step 2 Enter the following command to verify the backed up configuration file:

```
sensor#  more backup-config
```

The backed up configuration file is displayed.

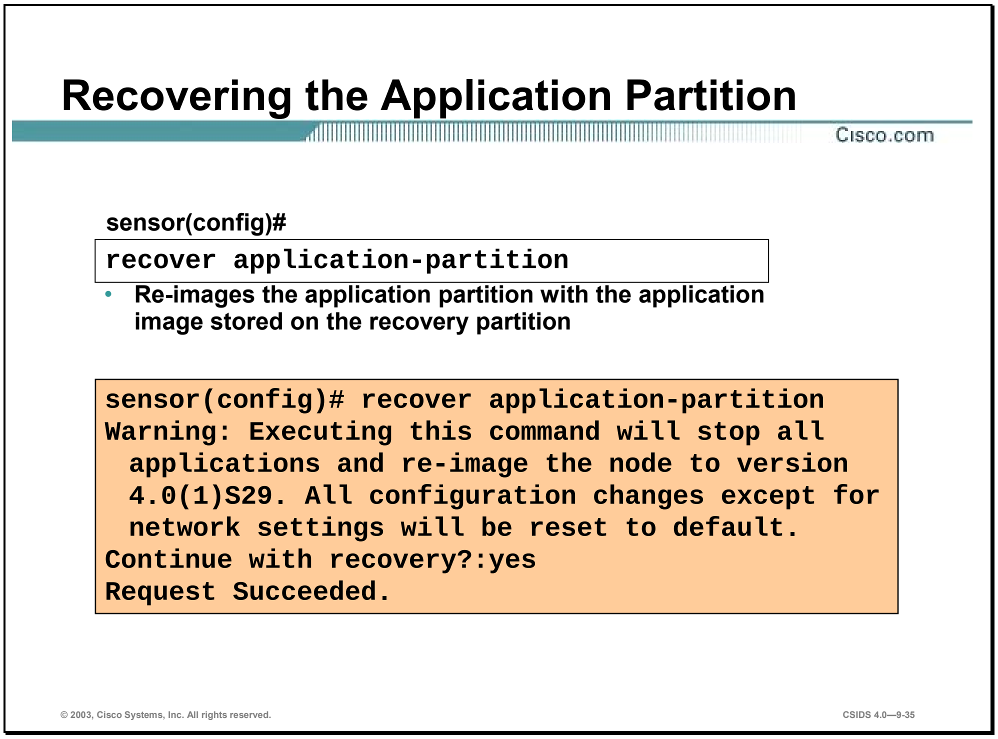
Step 3 Choose one of the following:

- Enter the following command to merge the backup configuration into the current configuration:

```
sensor# copy backup-config current-config
```

- Enter the following command to overwrite the current configuration with the back-up configuration:

```
sensor# copy/erase backup-config current-config
```



Recovering the Application Partition

sensor(config)#

```
recover application-partition
```

- Re-images the application partition with the application image stored on the recovery partition

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all
  applications and re-image the node to version
  4.0(1)S29. All configuration changes except for
  network settings will be reset to default.
Continue with recovery?:yes
Request Succeeded.
```

CSIDS 4.0—9-35

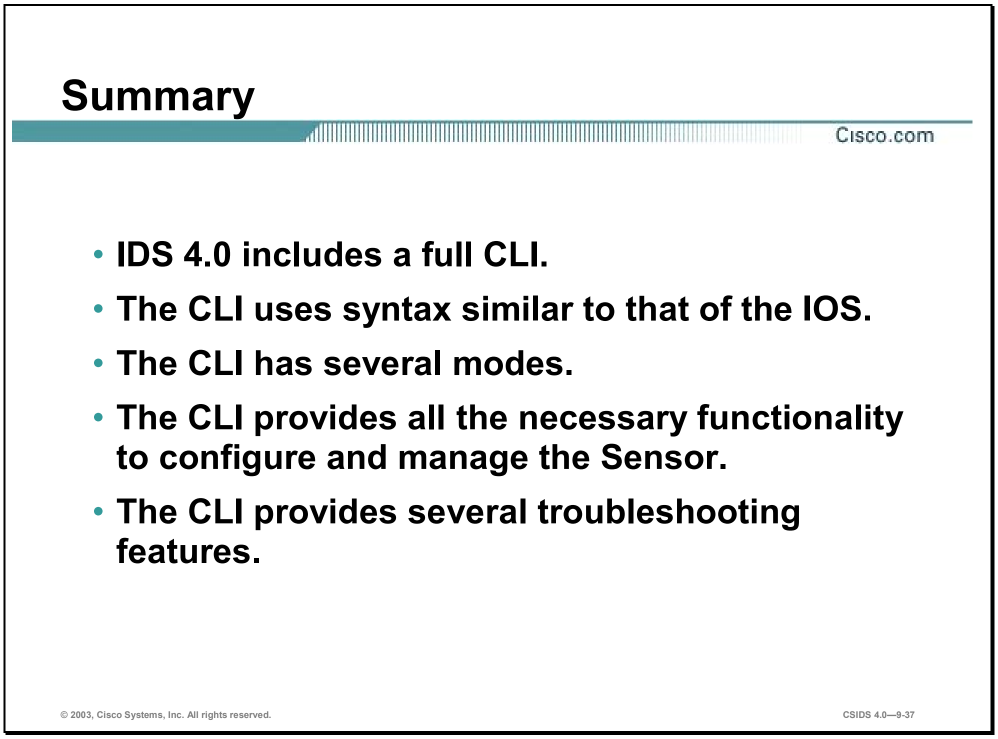
The Sensor has two partitions, application and recovery. There is no separate OS partition. The OS is the basis of the application partition.

The **recover** command re-images the application partition with the image stored on the recovery partition. The node is rebooted multiple times, and all configurations except for network will parameters are reset to default; therefore, consider backing up the current configuration before initiating recovery.

Note	This does not apply to the IDSM2. For information on recovering the software image on the IDSM2, go to the following web site: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/15620_01.htm#1034689

Summary

This section summarizes what you learned in this chapter.



Summary

Cisco.com

- IDS 4.0 includes a full CLI.
- The CLI uses syntax similar to that of the IOS.
- The CLI has several modes.
- The CLI provides all the necessary functionality to configure and manage the Sensor.
- The CLI provides several troubleshooting features.

CSIDS 4.0—9-37

Lab Exercise—Using the CLI

Complete the following lab exercises to practice what you have learned in this chapter.

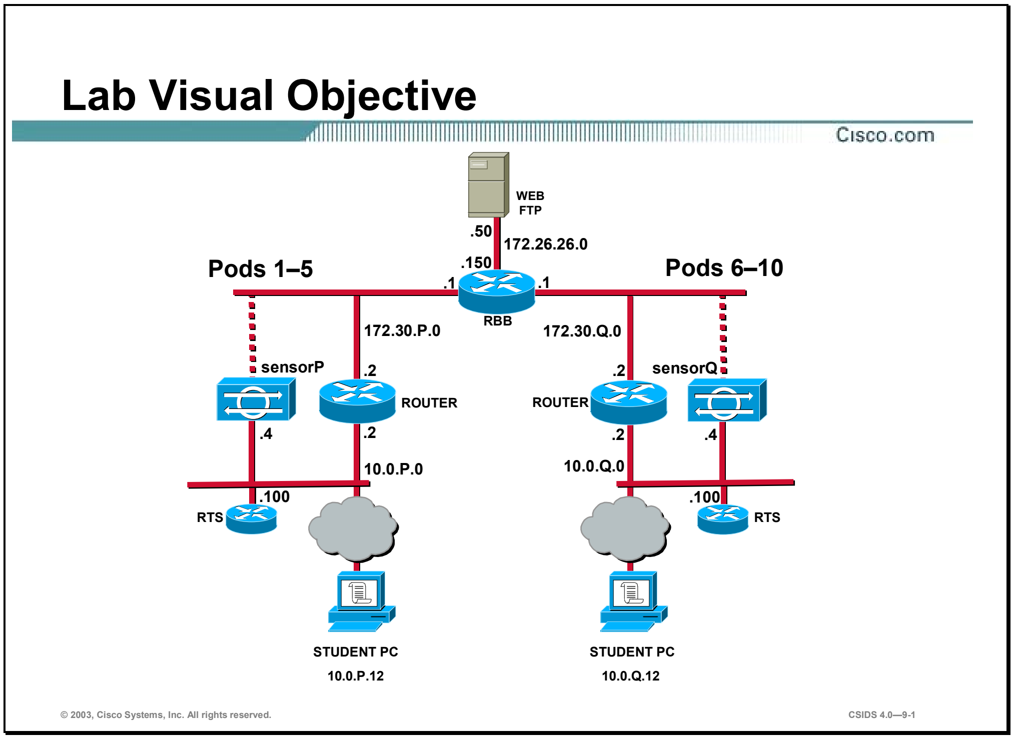
Objectives

In this lab exercise, you will complete the following tasks:

- Navigate the CLI.
- Create and test user accounts.
- Remove a user account.
- Back up and restore the current configuration.
- Display events.
- Display statistics.
- Stop and start the Sensor.

Visual Objective

The following illustration displays the lab topology for your classroom environment.



Lab Visual Objective

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—9-1

Task 1—Navigate the CLI

Complete the following steps to familiarize yourself with the command line interface. Observe the output of the commands carefully. The instructor will provide you with the procedures for access to the Sensor console port, as this will vary according to your lab connectivity. After you access the Sensor console port, the Sensor prompt appears.

Step 1 Display the command options available in the first level of the CLI, the privileged exec mode:

```
sensorP# ?
clear            Clear system settings or devices
clock            Set system clock settings
configure        Enter configuration mode
copy             Copy iplog or configuration files
erase            Erase a logical file
exit             Terminate current CLI login session
iplog            Control ip logging on the interface group
iplog-status     Display a list of IP Logs currently existing in the system
more             Display a logical file
no               Remove or disable system settings
ping             Send echo messages to destination
remove-xl        Indicate that the hardware accelerator card has been removed
                  from the system
```

```
reset            Shutdown the sensor applications and reboot
setup            Perform basic sensor configuration
show             Display system settings and/or history information
ssh              Secure Shell Settings
terminal         Change terminal configuration parameters
tls              Configure TLS settings
trace            Display the route an IP packet takes to a destination
```

(where P = pod number)

Step 2 Enter the second level of the CLI, configuration mode:

```
sensorP# configure terminal
sensorP(config)#
```

(where P = pod number)

Step 3 Display the command options available in configuration mode:

```
sensorP(config)# ?
display-serial     Re-direct all terminal output to the serial port
downgrade          Remove the last applied upgrade
end                Exit configuration mode and return to exec mode
exit               Exit configuration mode and return to exec mode
hostname           Set the sensor's hostname
interface          Enter configuration mode for system interfaces
no                 Remove configuration
password           Modify current user password on the local sensor
privilege          Modify user privilege
recover            Re-image the application partition from the recovery
                   partition
service            Enter configuration mode for node services
show               Display system settings and/or history information
ssh                Secure Shell Settings
telnet-server      Modify telnet-server settings
tls                Configure TLS settings
upgrade            Upgrade system software and signatures
username           Add a user to the local sensor
sensorP(config)#
```

Step 4 Enter a third level mode, interface command-control configuration mode:

```
sensorP(config)# interface command-control
sensorP(config-if)#
```

(where P = pod number)

Step 5 Display the command options available in interface command-control configuration mode:

```
sensorP(config-if)# ?
end      Exit interface configuration mode and return to exec mode
exit     Exit interface configuration mode and return to global configuration
         mode
```

```
ip       Configure IP information for interface
show     Display system settings and/or history information
sensorP(config-if)#
```

(where P = pod number)

Step 6 Exit interface command-control configuration mode:

```
sensorP(config-if)# exit
sensorP(config)#
```

(where P = pod number)

Step 7 Enter another third level mode, interface group configuration mode:

```
sensorP(config)# interface group 0
sensorP(config-ifg)#
```

(where P = pod number)

Step 8 Display the command options available in interface group configuration mode:

```
sensorP(config-ifg)# ?
end                    Exit interface group configuration mode and return to
                        exec mode
exit                   Exit interface group configuration mode and return to
                       global configuration mode
no                     Remove configuration
sensing-interface      Add a sensing interface to the interface group
show                   Display system settings and/or history information
shutdown               Disable the interface group
sensorP(config-ifg)#
```

(where P = pod number)

Step 9 Exit interface group configuration mode:

```
sensorP(config-ifg)# exit
sensorP(config)#
```

(where P = pod number)

Step 10 Enter another third level mode, interface sensing configuration mode:

```
sensorP(config)# interface sensing int1
sensorP(config-ifs)#
```

(where P = pod number)

Step 11 Display the command options available in interface sensing configuration mode:

```
sensorP(config-ifs)# ?
end          Exit interface sensing configuration mode and return to exec mode
exit         Exit interface sensing configuration mode and return to global
                    configuration mode
no           Remove configuration
show         Display system settings and/or history information
shutdown     Disable the sensing interface
```

```
sensorP(config-ifs)#
```

(where P = pod number)

Step 12 Exit interface sensing configuration mode:

```
sensorP(config-ifs)# exit
sensorP(config)#
```

(where P = pod number)

Step 13 Display the services that can be configured via the CLI:

```
sensorP(config)# service ?
alarm-channel-configuration      Enter configuration mode for the alarm channel
Authentication                   Enter configuration mode for user
                                    authentication options
Host                             Enter configuration mode for node
                                    configuration
Logger                           Enter configuration mode for debug logger
NetworkAccess                    Enter configuration mode for the network
                                    access controller
SshKnownHosts                    Enter configuration mode for configuring SSH
                                    known hosts
TrustedCertificates              Enter configuration mode for configuring
                                    trusted certificates
virtual-sensor-configuration     Enter configuration mode for the virtual
                                    sensor
WebServer                        Enter configuration mode for the web server
                                    application
sensorP(config)# service
```

(where P = pod number)

Step 14 Enter another third level mode, virtual-alarm-configuration mode:

```
sensorP(config)# service alarm-channel-configuration virtualAlarm
sensorP(config-acc)#
```

(where P = pod number)

Step 15 Display the command options available in virtual-alarm-configuration mode:

```
sensorP(config-acc)# ?
end                    Exit configuration mode and return to exec mode
exit                   Exit configuration mode and return to global
                             configuration mode
show                   Display system settings and/or history information
tune-alarm-channel     Enter configuration mode for the alarm channel
sensorP(config-acc)#
```

(where P = pod number)

Step 16 Exit virtual-alarm-configuration mode:

```
sensorP(config-acc)# exit
sensorP(config)#
```

(where P = pod number)

Step 17 Enter another third level mode, virtual-sensor-configuration mode:

```
sensorP(config)# service virtual-sensor-configuration virtualSensor
sensorP(config-vsc)#
```

(where P = pod number)

Step 18 Display the command options available in virtual-sensor-configuration mode:

```
sensorP(config-vsc)# ?
end                     Exit configuration mode and return to exec mode
exit                    Exit configuration mode and return to global
                              configuration mode
reset-signatures        Reset signatures settings back to the default
                              configuration
show                    Display system settings and/or history information
tune-micro-engines      Enter micro-engine tuning mode
```

(where P = pod number)

Step 19 Enter a fourth level mode, micro-engine tuning mode:

```
sensorP(config-vsc)# tune-micro-engines
sensorP(config-vsc-virtualSensor)#
```

(where P = pod number)

Step 20 Display the command options available in micro-engine tuning mode:

```
sensorP(config-vsc-virtualSensor)# ?
ATOMIC.ARP                        Layer 2 ARP signatures.
ATOMIC.ICMP                       Simple ICMP alarms based on Type, Code, Seq,
                                     Id etc.
ATOMIC.IPOPTIONS                  Simple L3 Alarms based on Ip Options
ATOMIC.L3.IP                      Simple L3 IP Alarms.
ATOMIC.TCP                        Simple TCP packet alarms based on TCP Flags,
                                     ports (both sides), and single packet
                                     regex.  Use SummaryKey to define the
                                     address view for MinHits and Summarize
                                     counting.  For best performance, use a
                                     StorageKey of xxxx.
ATOMIC.UDP                        Simple UDP packet alarms based on Port,
                                     Direction and DataLength.
exit                              Exit service configuration mode
FLOOD.HOST.ICMP                   Icmp Floods directed at a single host
FLOOD.HOST.UDP                    UDP Floods directed at a single host
FLOOD.NET                         Multi-protocol floods directed at a network
                                     segment.  Ip Addresses are wildcarded for
                                     this inspection.
FragmentReassembly                Fragment Reassembly configuration tokens
IPLog                             Virtual Sensor IP log configuration tokens
OTHER                             This engine is used to group generic
                                     signatures so common parameters may be
                                     changed.  It defines an interface into
                                     common signature parameters..
SERVICE.DNS                       DNS SERVICE Analysis Engine
SERVICE.FTP                       FTP service special decode alarms
SERVICE.GENERIC                  Custom service/payload decode and analysis
                                    based on our quartet tuple programming
                                    language. EXPERT use only.
SERVICE.HTTP                     HTTP protocol decode based string search
                                    Engine. Includes anti-evasive URL
                                    deobfuscation
SERVICE.IDENT                    Ident service (client and server) alarms.
SERVICE.MSSQL                    Microsoft (R) SQL service inspection engine
SERVICE.NTP                      Network Time Protocol based signature engine
SERVICE.RPC                      RPC SERVICE analysis engine
SERVICE.SMB                      SMB Service decode inspection.
SERVICE.SMTP                     SMTP Protocol Inspection Engine
SERVICE.SNMP                     Inspects SNMP traffic
SERVICE.SSH                      SSH header decode signatures.
SERVICE.SYSLOG                   Engine to process syslogs.
show                             Display system settings and/or history
                                    information
ShunEvent                        Shun Event configuration tokens
STATE.STRING.CISCOLOGIN          Telnet based Cisco Login Inspection Engine
STATE.STRING.LPRFORMATSTRING     LPR Protocol Inspection Engine
StreamReassembly                 Stream Reassembly configuration tokens
STRING.ICMP                      Generic ICMP based string search Engine
STRING.TCP                       Generic TCP based string search Engine.
STRING.UDP                       Generic UDP based string search Engine
SWEEP.HOST.ICMP                  ICMP host sweeps from a single attacker to
                                    many victims.
SWEEP.HOST.TCP                   TCP-based Host Sweeps from a single attacker
                                    to multiple victims.
SWEEP.MULTI                      UDP and TCP combined port sweeps.
SWEEP.OTHER.TCP                  Odd sweeps/scans such as nmap fingerprint
                                    scans.
SWEEP.PORT.TCP                   Detects port sweeps between two nodes.
SWEEP.PORT.UDP                   Detects UDP connections to multiple
                                    destination ports between two nodes.
systemVariables                  User modifiable system variables
TRAFFIC.ICMP                     Identifies ICMP traffic irregularities.
TROJAN.BO2K                      BackOrifice BO2K trojan traffic
TROJAN.TFN2K                     TFN2K trojan/ddos traffic
TROJAN.UDP                       Detects BO/BO2K UDP trojan traffic.
sensorP(config-vsc-virtualSensor)#
```

(where P = pod number)

Step 21 Exit micro-engine tuning mode:

```
sensorP(config-vsc-virtualSensor)# exit
```

(where P = pod number)

Step 22 Exit virtual-sensor-configuration mode:

```
sensorP(config-vsc)# exit
sensorP(config)#
```

(where P = pod number)

Task 2—Create and Test User Accounts

Complete the following steps to create user accounts:

Step 1 Create a user with administrative privileges:

```
sensorP(config)# username admin password adminpass privilege administrator
```

(where P = pod number)

Step 2 Create a user with viewer privileges:

```
sensorP(config)# username view password viewpass privilege viewer
```

(where P = pod number)

Step 3 Create a user with operator privileges:

```
sensorP(config)# username oper password operpass privilege operator
```

(where P = pod number)

Step 4 Exit configuration mode:

```
sensorP(config)# exit
sensorP#
```

(where P = pod number)

Step 5 Display the user accounts you created:

```
sensorP# show users all
    CLI ID   User      Privilege
*   973      cisco     administrator
             service   service
             admin     administrator
             view      viewer
             oper      operator
sensorP#
```

(where P = pod number)

Step 6 Exit privileged exec mode:

```
sensorP# exit
sensorP login:
```

(where P = pod number)

Step 7 Log in as user Viewer:

```
sensorP login: view
Password: viewpass
***NOTICE***
```

```
THIS PRODUCT CONTAINS CRYPTOGRAPHIC FEATURES AND IS SUBJECT TO UNITED STATES
AND LOCAL COUNTRY LAWS GOVERNING IMPORT, EXPORT, TRANSFER AND USE. DELIVERY
OF CISCO CRYPTOGRAPHIC PRODUCTS DOES NOT IMPLY THIRD-PARTY AUTHORITY TO IMPORT,
EXPORT, DISTRIBUTE OR USE ENCRYPTION. IMPORTERS, EXPORTERS, DISTRIBUTORS AND
USERS ARE RESPONSIBLE FOR COMPLIANCE WITH U.S. AND LOCAL COUNTRY LAWS. BY USING
THIS PRODUCT YOU AGREE TO COMPLY WITH APPLICABLE LAWS AND REGULATIONS. IF YOU
ARE UNABLE TO COMPLY WITH U.S. AND LOCAL LAWS, RETURN THIS PRODUCT IMMEDIATELY.

A SUMMARY OF U.S. LAWS GOVERNING CISCO CRYPTOGRAPHIC PRODUCTS MAY BE FOUND AT:
HTTP://WWW.CISCO.COM/WWL/EXPORT/CRYPTO

IF YOU REQUIRE FURTHER ASSISTANCE PLEASE CONTACT US BY SENDING EMAIL TO
EXPORT@CISCO.COM.
sensorP#
```

(where P = pod number)

Step 8 Display the monitoring interface:

```
sensorP# show interfaces sensing
SENSING INT0 IS UP
  HARDWARE IS ETH0, TX
  RESET PORT

MAC STATISTICS FROM THE INTELPRO INTERFACE
   LINK = UP
   SPEED = 100
   DUPLEX = FULL
   STATE = UP
   RX_PACKETS = 1964
   TX_PACKETS = 0
   RX_BYTES = 148936
   TX_BYTES = 0
   RX_ERRORS = 0
   TX_ERRORS = 0
   RX_DROPPED = 0
   TX_DROPPED = 0
   MULTICAST = 1964
   COLLISIONS = 0
   RX_LENGTH_ERRORS = 0
   RX_OVER_ERRORS = 0
   RX_CRC_ERRORS = 0
   RX_FRAME_ERRORS = 0
   RX_FIFO_ERRORS = 0
   RX_MISSED_ERRORS = 0
   TX_ABORTED_ERRORS = 0
   TX_CARRIER_ERRORS = 0
   TX_FIFO_ERRORS = 0
   TX_HEARTBEAT_ERRORS = 0
   TX_WINDOW_ERRORS = 0
   TX_ABORT_LATE_COLL = 0
   TX_DEFERRED_OK = 0
   TX_SINGLE_COLL_OK = 0
   TX_MULTI_COLL_OK = 0
   RX_LONG_LENGTH_ERRORS = 0
   RX_SHORT_LENGTH_ERRORS = 0
   RX_ALIGN_ERRORS = 0
   RX_FLOW_CONTROL_XON = 0
   RX_FLOW_CONTROL_XOFF = 0
   TX_FLOW_CONTROL_XON = 0
   TX_FLOW_CONTROL_XOFF = 0
   RX_CSUM_OFFLOAD_GOOD = 0
   RX_CSUM_OFFLOAD_ERRORS = 0
   PHY_MEDIA_TYPE = COPPER
   DROPPED PACKET PERCENT = 0

SENSING INT1 IS UP
  HARDWARE IS ETH1, TX
  RESET PORT
  COMMAND CONTROL PORT
sensorP#
```

(where P = pod number)

Step 9 Enter configuration mode:

```
sensorP# configure terminal
sensorP(config)#
```

(where P = pod number)

Step 10 Attempt to enter interface configuration mode for the command-control interface:

```
sensorP(config)# interface command-control
                 ^
% INVALID INPUT DETECTED AT '^' MARKER
sensorP(config)#
```

(where P = pod number)

Step 11 Attempt to add a TLS trusted host to the system:

```
sensorP(config)# tls
                 ^
% INVALID INPUT DETECTED AT '^' MARKER
sensorP(config)#
```

(where P = pod number)

Step 12 Observe the commands available in configuration mode when logged in with viewer privileges:

```
sensorP(config)# ?
END          EXIT CONFIGURATION MODE AND RETURN TO EXEC MODE
EXIT         EXIT CONFIGURATION MODE AND RETURN TO EXEC MODE
NO           REMOVE CONFIGURATION
PASSWORD     MODIFY CURRENT USER PASSWORD ON THE LOCAL SENSOR
SERVICE      ENTER CONFIGURATION MODE FOR NODE SERVICES
SHOW         DISPLAY SYSTEM SETTINGS AND/OR HISTORY INFORMATION
SSH          SECURE SHELL SETTINGS
sensorP(config)#
```

(where P = pod number)

Step 13 Log out of the viewer account:

```
sensorP(config)# exit
sensorP# exit
sensorP login:
```

(where P = pod number)

Step 14 Log in with the operator account, oper:

```
Sensor login: oper
Password: operpass
***NOTICE***
THIS PRODUCT CONTAINS CRYPTOGRAPHIC FEATURES AND IS SUBJECT TO UNITED STATES
AND LOCAL COUNTRY LAWS GOVERNING IMPORT, EXPORT, TRANSFER AND USE. DELIVERY
OF CISCO CRYPTOGRAPHIC PRODUCTS DOES NOT IMPLY THIRD-PARTY AUTHORITY TO IMPORT,
EXPORT, DISTRIBUTE OR USE ENCRYPTION. IMPORTERS, EXPORTERS, DISTRIBUTORS AND
USERS ARE RESPONSIBLE FOR COMPLIANCE WITH U.S. AND LOCAL COUNTRY LAWS. BY USING
THIS PRODUCT YOU AGREE TO COMPLY WITH APPLICABLE LAWS AND REGULATIONS. IF YOU
ARE UNABLE TO COMPLY WITH U.S. AND LOCAL LAWS, RETURN THIS PRODUCT IMMEDIATELY.

A SUMMARY OF U.S. LAWS GOVERNING CISCO CRYPTOGRAPHIC PRODUCTS MAY BE FOUND AT:
HTTP://WWW.CISCO.COM/WWL/EXPORT/CRYPTO

IF YOU REQUIRE FURTHER ASSISTANCE PLEASE CONTACT US BY SENDING EMAIL TO
EXPORT@CISCO.COM.
sensorP#
```

(where P = pod number)

Step 15 Enter configuration mode:

```
sensor# configure terminal
sensorP(config)#
```

(where P = pod number)

Step 16 Attempt to enter interface configuration mode for the command-control interface:

```
sensorP(config)# interface command-control
                           ^
```

```
% INVALID INPUT DETECTED AT '^' MARKER
sensorP(config)#
```

(where P = pod number)

Step 17 Attempt to change the password on the viewer account:

```
sensorP(config)# password view
                          ^
% INVALID INPUT DETECTED AT '^' MARKER
sensorP(config)#
```

(where P = pod number)

Step 18 Change the password on your own account:

```
sensorP(config)# password
Enter old login password: operpass
Enter new login password: newoperpass
Re-enter new login password: newoperpass
sensorP(config)#
```

(where P = pod number)

Step 19 Log out of the operator account:

```
sensorP(config)# exit
sensorP# exit
sensorP login:
```

(where P = pod number)

Step 20 Log in with the administrator account, admin:

```
Sensor login: admin
Password: adminpass
sensorP#
```

(where P = pod number)

Step 21 Reset the password on the operator account, oper:

```
sensorP(config)# password oper
Enter new login password: operpass
Re-enter new login password: operpass
sensorP(config)#
```

(where P = pod number)

Task 3—Remove a User Account

Complete the following steps to remove a user account:

Step 1 Remove the viewer account:

```
sensorP(config)# no username view
```

(where P = pod number)

Step 2 Exit configuration mode:

```
sensorP(config)# exit
sensorP#
```

(where P = pod number)

Step 3 Verify that the user has been removed:

```
sensorP# show users all
    CLI ID   USER      PRIVILEGE
*   1043     admin     ADMINISTRATOR
             cisco     ADMINISTRATOR
             service   SERVICE
             oper      OPERATOR
sensorP#
```

(where P = pod number)

Task 4—Back up and Restore the Current Configuration

Complete the following steps to back up and restore your Sensor's configuration.

Step 1 Back up your current configuration:

```
sensorP# copy current-config backup-config
```

(where P = pod number)

Step 2 Display the backed up configuration file:

Note You can press Control>C to return to the CLI prompt.

```
sensorP# more backup-config
! ------------------------------
SERVICE AUTHENTICATION
GENERAL
ATTEMPTLIMIT 0
METHODS METHOD LOCAL
EXIT
EXIT
EXIT
! ------------------------------
SERVICE HOST
NETWORKPARAMS
IPADDRESS 10.0.P.4
NETMASK 255.255.255.0
DEFAULTGATEWAY 10.0.P.2
HOSTNAME SENSORP
TELNETOPTION DISABLED
ACCESSLIST IPADDRESS 10.0.P.14 NETMASK 255.255.255.255
```

```
EXIT
OPTIONALAUTOUPGRADE
ACTIVE-SELECTION NONE
EXIT
TIMEPARAMS
OFFSET -360
STANDARDTIMEZONENAME CST
SUMMERTIMEPARAMS
ACTIVE-SELECTION RECURRINGPARAMS
RECURRINGPARAMS
SUMMERTIMEZONENAME CDT
STARTSUMMERTIME
```

(where P = pod number)

Step 3 Enter configuration mode:

```
sensorP# configure terminal
```

(where P = pod number)

Step 4 Enter host configuration mode:

```
sensorP(config)# service host
sensorP(config-Host)#
```

(where P = pod number)

Step 5 Enter network parameters sub-mode:

```
sensorP(config-Host)# networkParams
sensorP(config-Host-net)#
```

(where P = pod number)

Step 6 Add another host to your list of trusted hosts:

```
sensorP(config-Host-net)# accessList ipAddress 10.0.P.13
```

(where P = pod number)

Step 7 Exit network parameters sub-mode:

```
sensorP(config-Host-net)# exit
sensorP(config-Host)#
```

(where P = pod number)

Step 8 Exit host configuration mode:

```
sensorP(config-Host)# exit
Apply Changes:?[yes]
```

(where P = pod number)

Step 9 When prompted to apply changes, press **Enter** to accept the default response and save your changes:

```
Apply Changes:?[yes] <Enter>
sensorP(config)#
```

(where P = pod number)

Step 10 Exit configuration mode:

```
sensor(config)# exit
sensor#
```

(where P = pod number)

Step 11 Display the Sensor's current software version and configuration:

```
sensorP# show version
Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S37



OS Version 2.4.18-5smpbigphys
Platform: IDS-4235
Sensor up-time is 10 days.
Using 285454336 out of 1055744000 bytes of available memory (27% usage)
Using 532M out of 15G bytes of available disk space (4% usage)



MainApp             2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
AnalysisEngine      2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
Authentication      2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
Logger              2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
NetworkAccess       2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
TransactionSource   2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
WebServer           2003_Jan_23_02.00   (Release)   2003-01-23T02:00:25-0600
                      Running
CLI                 2003_Jan_17_18.33   (Release)   2003-01-17T18:33:18-0600

Upgrade History:

  IDS-K9-maj-4.0-1-S36   12:08:01 UTC Wed Feb 12 2003

Recovery Partition Version 1.1 - 4.0(1)S37
```

(where P = pod number)

Step 12 Display more configuration parameters. Notice that the trusted hosts lists contains the host you just added:

```
sensorP# more current-config
! ------------------------------
```

```
SERVICE AUTHENTICATION
GENERAL
ATTEMPTLIMIT 0
METHODS METHOD LOCAL
EXIT
EXIT
EXIT
! -----------------------------
SERVICE HOST
NETWORKPARAMS
IPADDRESS 10.0.P.4
NETMASK 255.255.255.0
DEFAULTGATEWAY 10.0.P.2
HOSTNAME SENSORP
TELNETOPTION DISABLED
ACCESSLIST IPADDRESS 10.0.P.12 NETMASK 255.255.255.255
ACCESSLIST IPADDRESS 10.0.P.13 NETMASK 255.255.255.255
EXIT
OPTIONALAUTOUPGRADE
ACTIVE-SELECTION NONE
EXIT
TIMEPARAMS
OFFSET -360
STANDARDTIMEZONENAME CST
SUMMERTIMEPARAMS
ACTIVE-SELECTION RECURRINGPARAMS
RECURRINGPARAMS
SUMMERTIMEZONENAME CDT
STARTSUMMERTIME
EXIT
ENDSUMMERTIME
```

Step 13 Press **Control>C** to return to the CLI prompt.

Step 14 Overwrite the current configuration with the back-up configuration:

```
sensor# copy /erase backup-config current-config
```

(where P = pod number)

Step 15 View your current configuration again to verify that the running configuration has been overwritten and the trusted host you just added no longer appears in the list:

```
sensorP# more current-config

! -----------------------------
SERVICE AUTHENTICATION
GENERAL
ATTEMPTLIMIT 0
METHODS METHOD LOCAL
```

```
EXIT
EXIT
EXIT
! -----------------------------
SERVICE HOST
NETWORKPARAMS
IPADDRESS 10.0.P.4
NETMASK 255.255.255.0
DEFAULTGATEWAY 10.0.P.2
HOSTNAME SENSORP
TELNETOPTION DISABLED
ACCESSLIST IPADDRESS 10.0.P.12 NETMASK 255.255.255.255
EXIT
OPTIONALAUTOUPGRADE
ACTIVE-SELECTION NONE
EXIT
TIMEPARAMS
OFFSET -360
STANDARDTIMEZONENAME CST
SUMMERTIMEPARAMS
ACTIVE-SELECTION RECURRINGPARAMS
RECURRINGPARAMS
SUMMERTIMEZONENAME CDT
STARTSUMMERTIME
```

Task 5—Display Events

Complete the following steps to practice troubleshooting the Sensor via the CLI.

Step 1 Display all events that occurred since 8:00 am June 1, 2003. The following output is displayed:

```
sensorP# show events 8:00 june 1 2003
EVLOGTRANSACTION: COMMAND=GETHOSTCONFIG EVENTID=1049799874976666001
SUCCESSFUL=TRUE
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: MAINAPP
    APPINSTANCEID: 606
  TIME: 2003/04/08 11:04:42 2003/04/08 11:04:42 UTC
  REQUESTOR:
    USER:
    APPLICATION:
      HOSTID:
      APPNAME: NAC
      APPINSTANCEID: 947

EVSTATUS: EVENTID=1049799874976666002
```

```
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: NAC
    APPINSTANCEID: 947
  TIME: 2003/04/08 11:04:42 2003/04/08 11:04:42
UTC<SHUNNINGDISABLED><DESCRIPTIO
N>SHUNNING DISABLED</DESCRIPTION></SHUNNINGDISABLED>


EVSTATUS: EVENTID=1049799874976666003
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: NAC
    APPINSTANCEID: 947
  TIME: 2003/04/08 11:04:42 2003/04/08 11:04:42
UTC<SHUNNINGENABLED><DESCRIPTION
>SHUNNING ENABLED</DESCRIPTION></SHUNNINGENABLED>


EVSTATUS: EVENTID=1049799874976666004
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: NAC
    APPINSTANCEID: 947
  TIME: 2003/04/08 11:04:42 2003/04/08 11:04:42
UTC<APPLICATIONSTARTED><DESCRIPT
ION>APP INITIALIZATION IS COMPLETE</DESCRIPTION></APPLICATIONSTARTED>


EVERROR: EVENTID=1049799874976666005 SEVERITY=WARNING
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: SENSORAPP
    APPINSTANCEID:
  TIME: 2003/04/08 11:04:43 2003/04/08 11:04:43 UTC
  ERRORMESSAGE: NAME=ERRUNCLASSIFIED GENERATING NEW ANALYSIS ENGINE
CONFIGURATION FILE.


EVSTATUS: EVENTID=1049799874976666006
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: AUTHENTICATION
    APPINSTANCEID: 945
  TIME: 2003/04/08 11:04:44 2003/04/08 11:04:44 UTC
  CERTIFICATESCHANGED:
    DESCRIPTION: A NEW SELF-SIGNED X.509 CERTIFICATE WAS GENERATED FOR 10.0.P.4
1. THE NEW CERTIFICATE MD5 FINGERPRINT IS
FF:42:14:39:C8:5E:65:91:88:86:BA:A9:18
:F8:51:15, AND THE SHA1 FINGERPRINT IS
34:D4:B5:2C:52:FF:41:74:A7:BE:EF:F7:F0:3F
```

```
:E8:16:18:BB:BB:65.


EVALERT: EVENTID=1049799874976666007 SEVERITY=INFORMATIONAL
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: SENSORAPP
    APPINSTANCEID: 949
  TIME: 2003/04/08 11:05:32 2003/04/08 11:05:32 UTC
  INTERFACEGROUP: 0
  VLAN: 0
  SIGNATURE: SIGID=994 SIGNAME=TRAFFIC FLOW STARTED SUBSIGID=1 VERSION=S37 THE
TRAFFIC THAT THE SENSOR MONITORS HAS STARTED
  PARTICIPANTS:
    ATTACK:
      ATTACKER: PROXY=FALSE
        ADDR: LOCALITY=OUT 0.0.0.0
      VICTIM:
--MORE--
```

Note You can press Control>C at any time to return to the CLI prompt.

Step 2 Display alarm events since a specified time for a specified alert level. The following output is displayed:

```
sensorP# show events alert informational 8:00 june 1 2003
EVALERT: EVENTID=1049799874976666007 SEVERITY=INFORMATIONAL
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: SENSORAPP
    APPINSTANCEID: 949
  TIME: 2003/04/08 11:05:32 2003/04/08 11:05:32 UTC
  INTERFACEGROUP: 0
  VLAN: 0
  SIGNATURE: SIGID=994 SIGNAME=TRAFFIC FLOW STARTED SUBSIGID=1 VERSION=S37 THE
TRAFFIC THAT THE SENSOR MONITORS HAS STARTED
  PARTICIPANTS:
    ATTACK:
      ATTACKER: PROXY=FALSE
        ADDR: LOCALITY=OUT 0.0.0.0
      VICTIM:
        ADDR: LOCALITY=OUT 0.0.0.0


EVALERT: EVENTID=1049806694976666007 SEVERITY=INFORMATIONAL
  ORIGINATOR:
    HOSTID: SENSORP
    APPNAME: SENSORAPP
```

```
      APPINSTANCEID: 934
    TIME: 2003/04/08 11:41:54 2003/04/08 11:41:54 UTC

--MORE--
```

(where P = pod number)

Step 3 Delete events from the Event Store:

```
sensorP# clear events

Warning: Executing this command will remove all events currently stored in the
Event Store.
Continue with clear? :
```

(where P = pod number)

Step 4 When asked if you want to continue with the clear events command, enter **yes**.

```
Warning: Executing this command will remove all events currently stored in the Event Store.

Continue with clear? : yes
```

Step 5 Verify that events have been cleared from the Event Store:

```
sensorP# show events 8:00 june 1 2003
```

(where P = pod number)

Step 6 Enter **Control>C** to return to the CLI prompt.

Task 6—Display Statistics

Complete the following steps to view Sensor statistics.

Step 1 Display the services that provide statistics:

```
sensorP# show statistics ?
AUTHENTICATION        DISPLAY AUTHENTICATION STATISTICS
EVENTSERVER           DISPLAY EVENT SERVER STATISTICS
EVENTSTORE            DISPLAY EVENT STORE STATISTICS
HOST                  DISPLAY HOST STATISTICS
LOGGER                DISPLAY LOGGER STATISTICS
NETWORKACCESS         DISPLAY NETWORK ACCESS CONTROLLER STATISTICS
TRANSACTIONSERVER     DISPLAY TRANSACTION SERVER STATISTICS
TRANSACTIONSOURCE     DISPLAY TRANSACTION SOURCE STATISTICS
WEBSERVER             DISPLAY WEB SERVER STATISTICS
sensorP# show statistics
```

(where P = pod number)

Step 2 Display the Event Store statistics:

```
sensorP# show statistics EventStore
Event store statistics
   GENERAL INFORMATION ABOUT THE EVENT STORE
      THE CURRENT NUMBER OF OPEN SUBSCRIPTIONS = 0
      THE NUMBER OF EVENTS LOST BY SUBSCRIPTIONS AND QUERIES = 0
      THE NUMBER OF QUERIES ISSUED = 0
      THE NUMBER OF TIMES THE EVENT STORE CIRCULAR BUFFER HAS WRAPPED = 0
   NUMBER OF EVENTS OF EACH TYPE CURRENTLY STORED
      DEBUG EVENTS = 0
      STATUS EVENTS = 0
      LOG TRANSACTION EVENTS = 0
      SHUN REQUEST EVENTS = 0
      ERROR EVENTS, WARNING = 0
      ERROR EVENTS, ERROR = 0
      ERROR EVENTS, FATAL = 0
      ALERT EVENTS, INFORMATIONAL = 0
      ALERT EVENTS, LOW = 0
      ALERT EVENTS, MEDIUM = 0
      ALERT EVENTS, HIGH = 0
sensorP#
```

(where P = pod number)

Step 3 Display the command-control interface view of statistics:

```
sensorP# show interfaces command-control
command-control is up
  Internet address is 10.0.P.4, subnet mask is 255.255.255.0, telnet is
disabled


  Hardware is eth1, tx


Network Statistics
   eth1      Link encap:Ethernet  HWaddr 00:06:5B:ED:0C:84
             inet addr:10.0.P.4  Bcast:10.0.P.255  Mask:255.255.255.0
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:839274 errors:0 dropped:0 overruns:0 frame:0
             TX packets:155855 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:100
             RX bytes:68850693 (65.6 Mb)  TX bytes:17619236 (16.8 Mb)
             Interrupt:16 Base address:0xdcc0 Memory:feb20000-feb40000
```

(where P = pod number)

Step 4 Display the sensing interface view of statistics:

```
sensorP# show interfaces sensing
Sensing int0 is up
  Hardware is eth0, TX
  Reset port


MAC statistics from the IntelPro interface
   Link = up
   Speed = 100
   Duplex = Full
   State = up
   Rx_Packets = 669379
   Tx_Packets = 0
   Rx_Bytes = 50710914
   Tx_Bytes = 0
   Rx_Errors = 0
   Tx_Errors = 0
   Rx_Dropped = 0
   Tx_Dropped = 0
   Multicast = 669379
   Collisions = 0
   Rx_Length_Errors = 0
   Rx_Over_Errors = 0
   Rx_CRC_Errors = 0
   Rx_Frame_Errors = 0
   Rx_FIFO_Errors = 0
   Rx_Missed_Errors = 0
   Tx_Aborted_Errors = 0
   Tx_Carrier_Errors = 0
   Tx_FIFO_Errors = 0
   Tx_Heartbeat_Errors = 0
   Tx_Window_Errors = 0
   Tx_Abort_Late_Coll = 0
   Tx_Deferred_Ok = 0
   Tx_Single_Coll_Ok = 0
   Tx_Multi_Coll_Ok = 0
   Rx_Long_Length_Errors = 0
   Rx_Short_Length_Errors = 0
   Rx_Align_Errors = 0
   Rx_Flow_Control_XON = 0
   Rx_Flow_Control_XOFF = 0
   Tx_Flow_Control_XON = 0
   Tx_Flow_Control_XOFF = 0
   Rx_CSum_Offload_Good = 0
   Rx_CSum_Offload_Errors = 0
   PHY_Media_Type = Copper
   Dropped Packet Percent = 0

Sensing int1 is up
  Hardware is eth1, TX
  Reset port
  Command control port
```

(where P = pod number)

Step 5 Display the interface group view of statistics:

```
sensorP# show interfaces group
Group 0 is up
  Sensing ports int0
  Logical virtual sensor configuration: virtualSensor
  Logical alarm channel configuration:  virtualAlarm

VirtualSensor0
   General Statistics for this Virtual Sensor
      Number of seconds since a reset of the statistics = 705972
      Total number of packets processed since reset = 669389
      Total number of IP packets processed since reset = 305132
      Total number of packets that were not IP processed since reset = 364257
      Total number of TCP packets processed since reset = 0
      Total number of UDP packets processed since reset = 0
      Total number of ICMP packets processed since reset = 0
      Total number of packets that were not TCP, UDP, or ICMP processed since
         reset = 305132
      Total number of ARP packets processed since reset = 0
      Total number of ISL encapsulated packets processed since reset = 0
      Total number of 802.1q encapsulated packets processed since reset = 0
      Total number of packets with bad IP checksums processed since reset = 0
      Total number of packets with bad layer 4 checksums processed since reset
         = 0
      Total number of bytes processed since reset = 48034360
      The rate of packets per second since reset = 0
      The rate of bytes per second since reset = 68
      The average bytes per packet since reset = 71
   Fragment Reassembly Unit Statistics for this Virtual Sensor
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
      Number of fragments received since reset = 0
      Number of complete datagrams reassembled since reset = 0
      Number of incomplete datagrams abandoned since reset = 0
      Number of fragments discarded since reset = 0
   Statistics for the TCP Stream Reassembly Unit
      Current Statistics for the TCP Stream Reassembly Unit
         TCP streams currently in the embryonic state = 0
         TCP streams currently in the established state = 0
         TCP streams currently in the closing state = 0
         TCP streams currently in the system = 0
         TCP Packets currently queued for reassembly = 0
      Cumulative Statistics for the TCP Stream Reassembly Unit since reset
         TCP streams that have been tracked since last reset = 0
         TCP streams that had a gap in the sequence jumped = 0
         TCP streams that was abandoned due to a gap in the sequence = 0
         TCP packets that arrived out of sequence order for their stream = 0
         TCP packets that arrived out of state order for their stream = 0
         The rate of TCP connections tracked per second since reset = 0
   The Signature Database Statistics.
      The Number of each type of node active in the system (can not be reset)
         Total nodes active = 8
         TCP nodes keyed on both IP addresses and both ports = 0
         UDP nodes keyed on both IP addresses and both ports = 0
         IP nodes keyed on both IP addresses = 2
      The number of each type of node inserted since reset
         Total nodes inserted = 8
         TCP nodes keyed on both IP addresses and both ports = 0
         UDP nodes keyed on both IP addresses and both ports = 0
         IP nodes keyed on both IP addresses = 2
      The rate of nodes per second for each time since reset
         Nodes per second = 0
         TCP nodes keyed on both IP addresses and both ports per second = 0
         UDP nodes keyed on both IP addresses and both ports per second = 0
         IP nodes keyed on both IP addresses per second = 0
      The number of root nodes forced to expire because of memory constraints
         TCP nodes keyed on both IP addresses and both ports = 0
   Alarm Statistics for this Virtual Sensor
      Number of alarms triggered by events = 1
      Number of alarms excluded by filters = 0
      Number of alarms removed by summarizer = 0
      Number of alarms sent to the Event Store = 1
```

(where P = pod number)

Task 7—Stop and Start the Sensor

Complete the following steps to shut down the applications running on the Sensor and reboot the Sensor:

Step 1 Start and stop the Sensor:

```
sensorP# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset?:
```

(where P = pod number)

Step 2 Enter **yes** to continue the reset:

```
Continue with reset?: yes
Request Succeeded.
sensorP#
```

(where P = pod number)

Step 3 When the Sensor finishes resetting, log back in and observe the Event Store statistics again. Notice the increment in status, log transaction, and informational alert events:

```
sensor# show statistics EventStore
    EVENT STORE STATISTICS
   GENERAL INFORMATION ABOUT THE EVENT STORE
      THE CURRENT NUMBER OF OPEN SUBSCRIPTIONS = 0
      THE NUMBER OF EVENTS LOST BY SUBSCRIPTIONS AND QUERIES = 0
      THE NUMBER OF QUERIES ISSUED = 0
      THE NUMBER OF TIMES THE EVENT STORE CIRCULAR BUFFER HAS WRAPPED = 0
   NUMBER OF EVENTS OF EACH TYPE CURRENTLY STORED
      DEBUG EVENTS = 0
      STATUS EVENTS = 12
      LOG TRANSACTION EVENTS = 50
      SHUN REQUEST EVENTS = 0
      ERROR EVENTS, WARNING = 0
      ERROR EVENTS, ERROR = 0
      ERROR EVENTS, FATAL = 0
      ALERT EVENTS, INFORMATIONAL = 3
      ALERT EVENTS, LOW = 0
      ALERT EVENTS, MEDIUM = 0
      ALERT EVENTS, HIGH = 0
sensorP#
```

(where P = pod number)

10

Cisco Intrusion Detection System Device Manager and Event Viewer

Overview

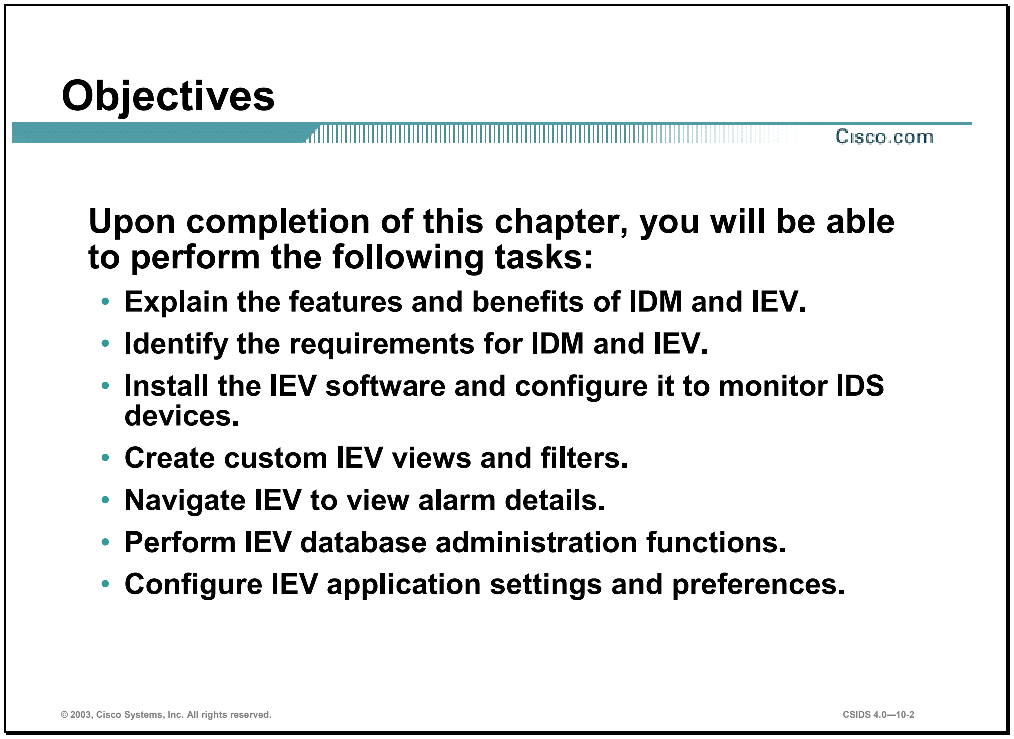
This chapter introduces the Cisco Intrusion Detection System (IDS) Device Manager (IDM) and IDS Event Viewer (IEV). The installation and use of the IEV is explained. This chapter includes the following topics:

- Objectives
- IDS Device Manager overview
- IDS Event Viewer overview
- IDS Event Viewer installation
- IDS Event Viewer views
- Network security database
- IDS Event Viewer filters
- IDS Event Viewer database administration
- IDS Event Viewer configuration

- Summary
- Lab exercise

Objectives

This section lists the chapter's objectives.



Objectives

Cisco.com

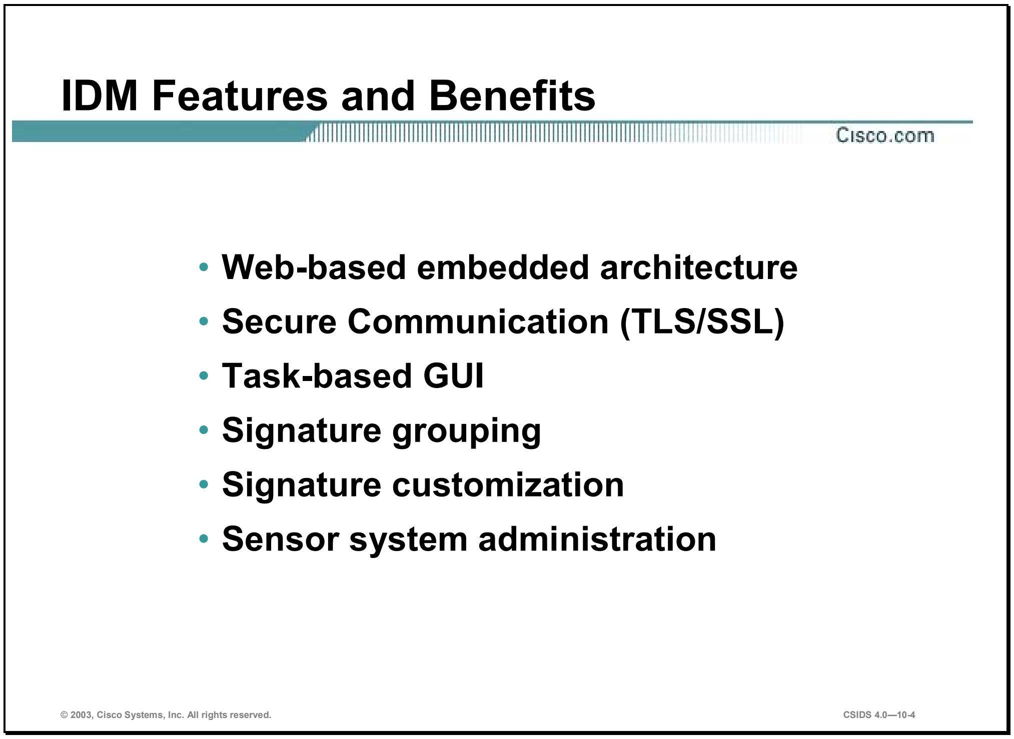
Upon completion of this chapter, you will be able to perform the following tasks:

- Explain the features and benefits of IDM and IEV.
- Identify the requirements for IDM and IEV.
- Install the IEV software and configure it to monitor IDS devices.
- Create custom IEV views and filters.
- Navigate IEV to view alarm details.
- Perform IEV database administration functions.
- Configure IEV application settings and preferences.

CSIDS 4.0—10-2

IDS Device Manager Overview

This section discusses the features and benefits of the IDS Device Manager (IDM).



IDM Features and Benefits

Cisco.com

- Web-based embedded architecture
- Secure Communication (TLS/SSL)
- Task-based GUI
- Signature grouping
- Signature customization
- Sensor system administration

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—10-4

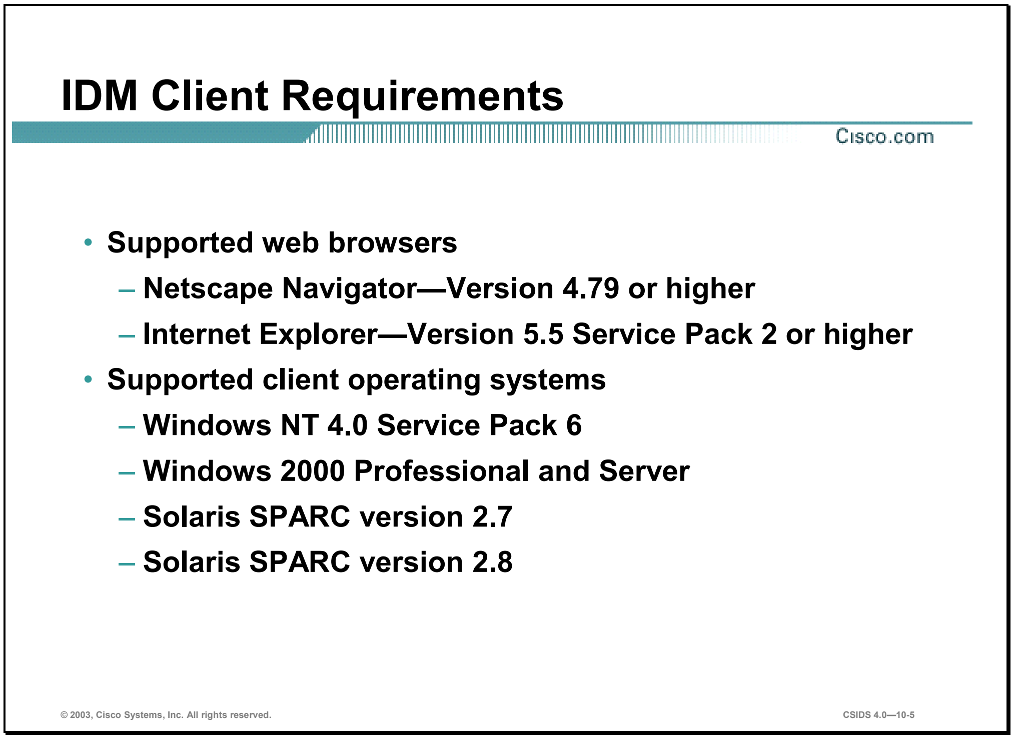
The IDM is a web-based, embedded architecture configuration tool for Cisco IDS Sensors. IDM enables a network security administrator to securely manage Sensors remotely from any workstation that has a compatible web browser.

The graphical user interface (GUI) was designed to simplify Sensor configuration tasks. For example, IDS signatures are grouped by categories such as WWW signatures. This enables the network security administrator to quickly configure all web-related signatures.

Cisco IDS signature customization is now made easier through one web page. The Custom Signature configuration page presents the network security administrator with all the parameters that can be customized for a specific signature.

IDM enables the network security administrator to remotely:

- Restart the IDS services.
- Restart the Sensor.
- Power down the Sensor.



IDM Client Requirements

Cisco.com

- Supported web browsers
  - Netscape Navigator—Version 4.79 or higher
  - Internet Explorer—Version 5.5 Service Pack 2 or higher
- Supported client operating systems
  - Windows NT 4.0 Service Pack 6
  - Windows 2000 Professional and Server
  - Solaris SPARC version 2.7
  - Solaris SPARC version 2.8

CSIDS 4.0—10-5

IDM is a web-based application running on the Sensor. The following is the supported client information:

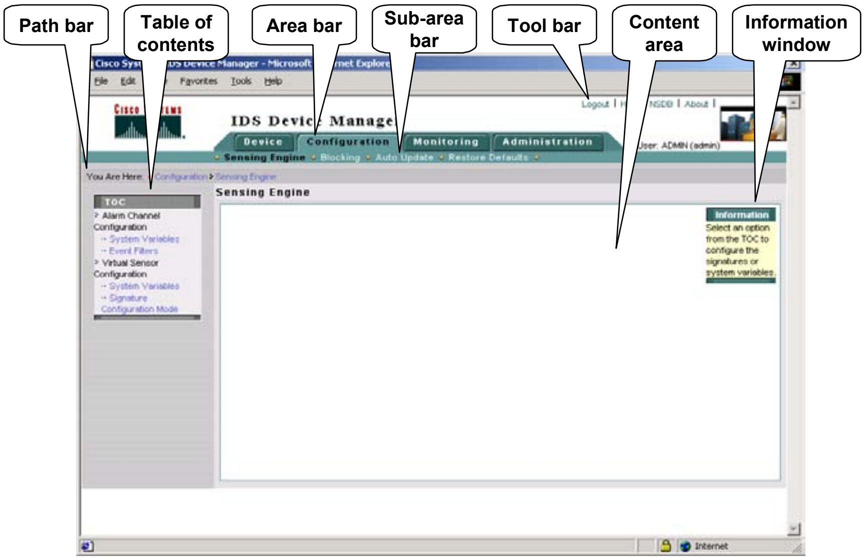
Browser	Version
Netscape Navigator	4.79 and higher
Internet Explorer	5.5 Service Pack 2 and higher

Operating System	Version
Windows NT	4.0 Service Pack 6
Windows 2000	Professional and Server
Solaris (SPARC)	2.7 and 2.8

Note The list of supported web browsers and operating systems does not imply that other browsers and operating systems will not work.

IDS Manager Interface

Cisco.com



Path bar

Table of contents

Area bar

Sub-area bar

Tool bar

Content area

Information window

Logout | Help | NSDB | About |
IDS Device Manager
Device
Configuration
Monitoring
Administration
User: ADMIN (admin)
Sensing Engine • Blocking • Auto Update • Restore Defaults •
You Are Here: Configuration > Sensing Engine
TOC
Alarm Channel Configuration
System Variables
Event Filters
Virtual Sensor Configuration
System Variables
Signature Configuration Mode
Sensing Engine
Information
Internet

Select an option from the TOC to configure the signatures or system variables.

CSIDS 4.0—10-6

The IDM GUI provides the network security administrator with an intuitive approach to configuring Sensors. The GUI has the following sections:

- Path bar—Displays the current selection. In the figure, the current path selected is Configuration>Sensing Engine.

- Table of contents (TOC)—Lists the available options for the item selected from the sub-area bar. In the figure, the TOC displays the options for the Sensing Engine.

- Area bar—Lists the available Sensor configuration items. The available Sensor configuration items are Device, Configuration, Monitoring, and Administration. Each configuration item has sub-options, which are listed in the sub-area bar.

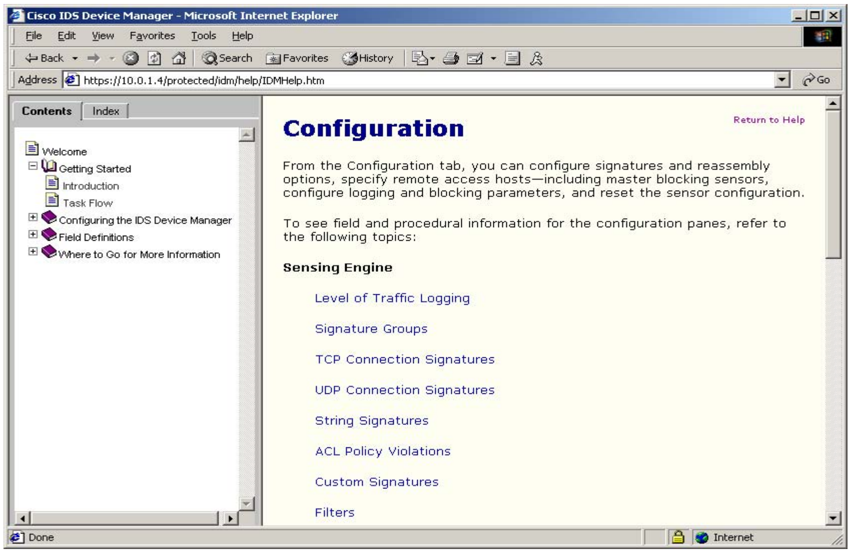
- Sub-area bar—Lists the available Sensor configuration sub-options for the item selected from the area bar. In the figure, the available configuration options are Sensing Engine, Blocking, Auto Update, and Restore Defaults.

- Tool bar—Lists the available user functions. The available user functions are Logout, Help, NSDB, and About.

- Content area—Displays the information associated with the option selected or an action associated with a user function.

- Information window—Displays a description associated with the option selected or with the instructions.

Online IDM Help


Cisco IDS Device Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
Go
Contents
Index
Welcome
Getting Started
Introduction
Task Flow
Configuring the IDS Device Manager
Field Definitions
Where to Go for More Information
Return to Help
Done
Internet

https://10.0.1.4/protected/idm/help/IDMHelp.htm

Configuration

From the Configuration tab, you can configure signatures and reassembly options, specify remote access hosts—including master blocking sensors, configure logging and blocking parameters, and reset the sensor configuration.

To see field and procedural information for the configuration panes, refer to the following topics:

Sensing Engine

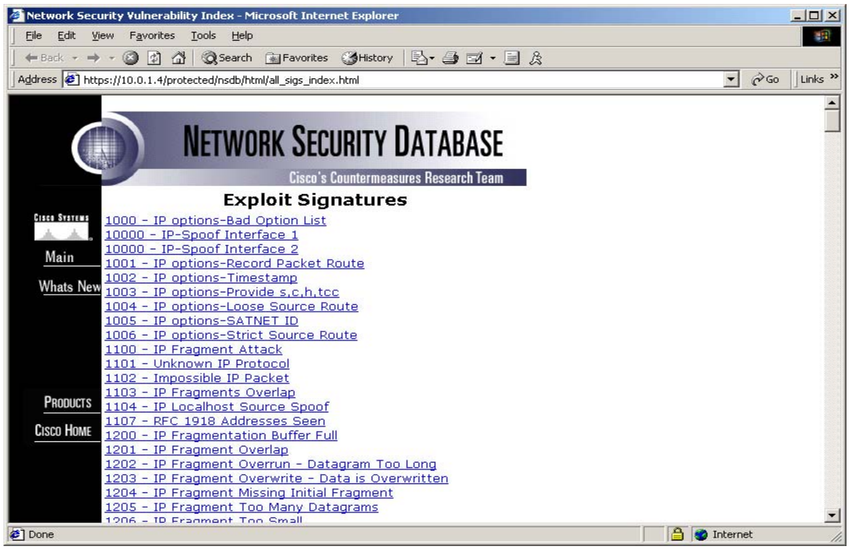
- Level of Traffic Logging
- Signature Groups
- TCP Connection Signatures
- UDP Connection Signatures
- String Signatures
- ACL Policy Violations
- Custom Signatures
- Filters

CSIDS 4.0—10-7

IDM provides online documentation to assist in the configuration of the Sensor. To access the online IDM, choose **Help** from the IDM tool bar. The IDM Help Contents are displayed in a new web browser.

NSDB Access

Cisco.com


Network Security Vulnerability Index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://10.0.1.4/protected/nsdb/html/all_sigs_index.html
Go Links
NETWORK SECURITY DATABASE
Cisco's Countermeasures Research Team
CISCO SYSTEMS
Main
Whats New
PRODUCTS
CISCO HOME
Done
Internet

Exploit Signatures

1000 - IP options-Bad Option List
10000 - IP-Spoof Interface 1
10000 - IP-Spoof Interface 2
1001 - IP options-Record Packet Route
1002 - IP options-Timestamp
1003 - IP options-Provide s,c,h,tcc
1004 - IP options-Loose Source Route
1005 - IP options-SATNET ID
1006 - IP options-Strict Source Route
1100 - IP Fragment Attack
1101 - Unknown IP Protocol
1102 - Impossible IP Packet
1103 - IP Fragments Overlap
1104 - IP Localhost Source Spoof
1107 - RFC 1918 Addresses Seen
1200 - IP Fragmentation Buffer Full
1201 - IP Fragment Overlap
1202 - IP Fragment Overrun - Datagram Too Long
1203 - IP Fragment Overwrite - Data is Overwritten
1204 - IP Fragment Missing Initial Fragment
1205 - IP Fragment Too Many Datagrams
1206 - IP Fragment Too Small

CSIDS 4.0—10-8

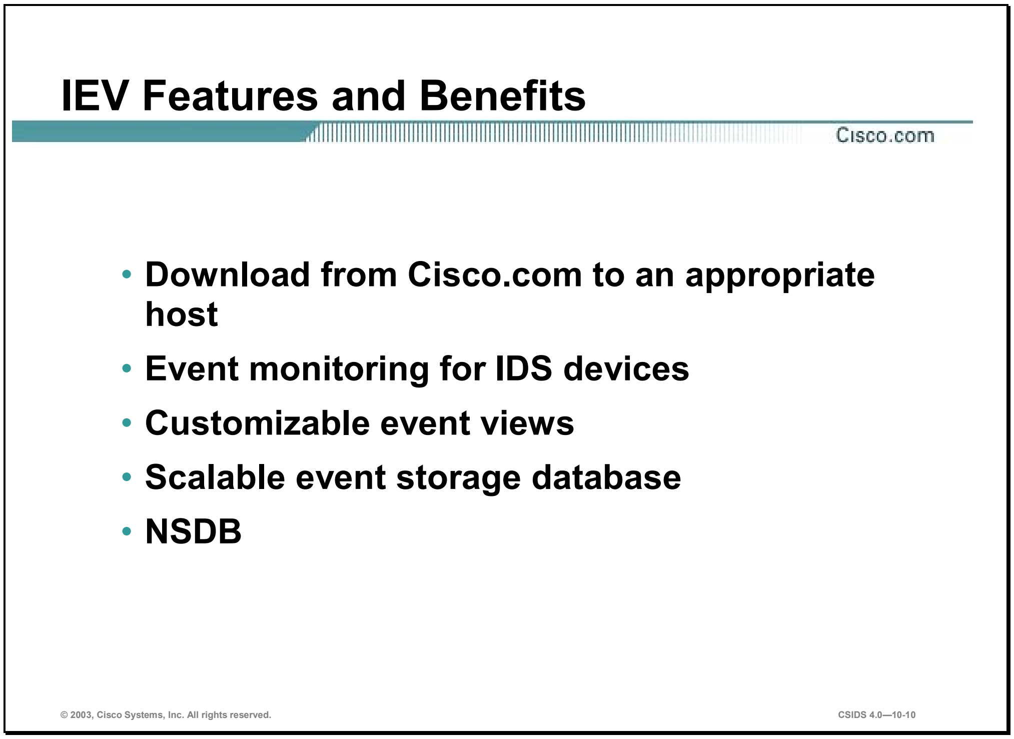
The Network Security Database (NSDB) is the Cisco HTML-based encyclopedia of network vulnerability information. You can examine the NSDB for a specific alarm. The Cisco Secure Encyclopedia (CSEC) is the online equivalent of the NSDB.

CSEC has been developed as a central warehouse of security knowledge to provide Cisco security professionals with an interactive database of security vulnerability information. CSEC contains detailed information about security vulnerabilities such as countermeasures, affected systems and software, and Cisco Secure products that can help you test for vulnerabilities or detect when malicious users attempt to exploit your systems. The CSEC can be found at http://www.cisco.com/go/csec.

Note A valid Cisco Connection Online (CCO) account is required to view the CSEC data.

IDS Event Viewer Overview

This section discusses the features and benefits of the IDS Event Viewer (IEV).



IEV Features and Benefits

Cisco.com

- Download from Cisco.com to an appropriate host
- Event monitoring for IDS devices
- Customizable event views
- Scalable event storage database
- NSDB

CSIDS 4.0—10-10

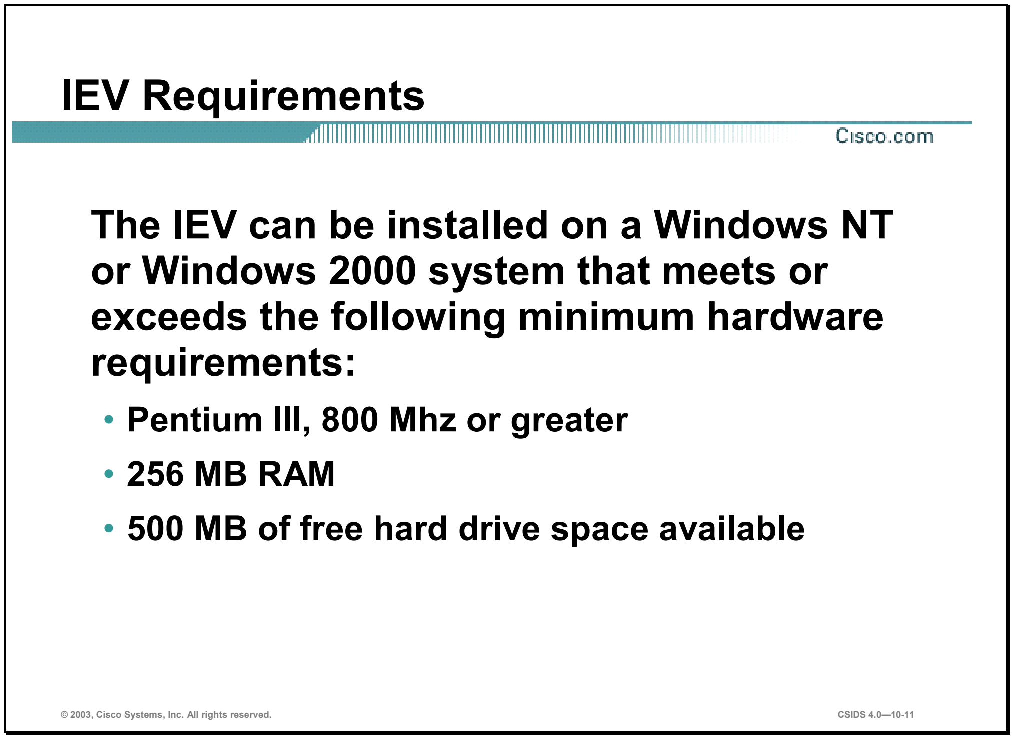
The IEV is a Java-based application that enables you to view and manage alarms for up to five Sensors. You can use the IEV to view alarms in real-time or in imported log files. You can download IEV from the following web site to any host meeting the requirements described later in this chapter:

http://www.cisco.com/cgi-bin/tablebuild.pl/ids-ev

IEV presents IDS alarm data as views. IEV has default views that can be customized to meet customer needs. IEV enables the network security administrator to create custom views.

IEV is built on a relational database, MySQL, which allows for a scalable database. Data can easily be imported, exported, and deleted from the database giving the network security administrator the ability to control the size of the database.

IEV includes the NSDB. The NSDB provides detailed IDS signature and vulnerability information. The network security administrator can use this information to assist in determining the threat posed to the network.



IEV Requirements

The IEV can be installed on a Windows NT or Windows 2000 system that meets or exceeds the following minimum hardware requirements:

- Pentium III, 800 Mhz or greater
- 256 MB RAM
- 500 MB of free hard drive space available

CSIDS 4.0—10-11

IEV can be installed on the following platforms (English version only):

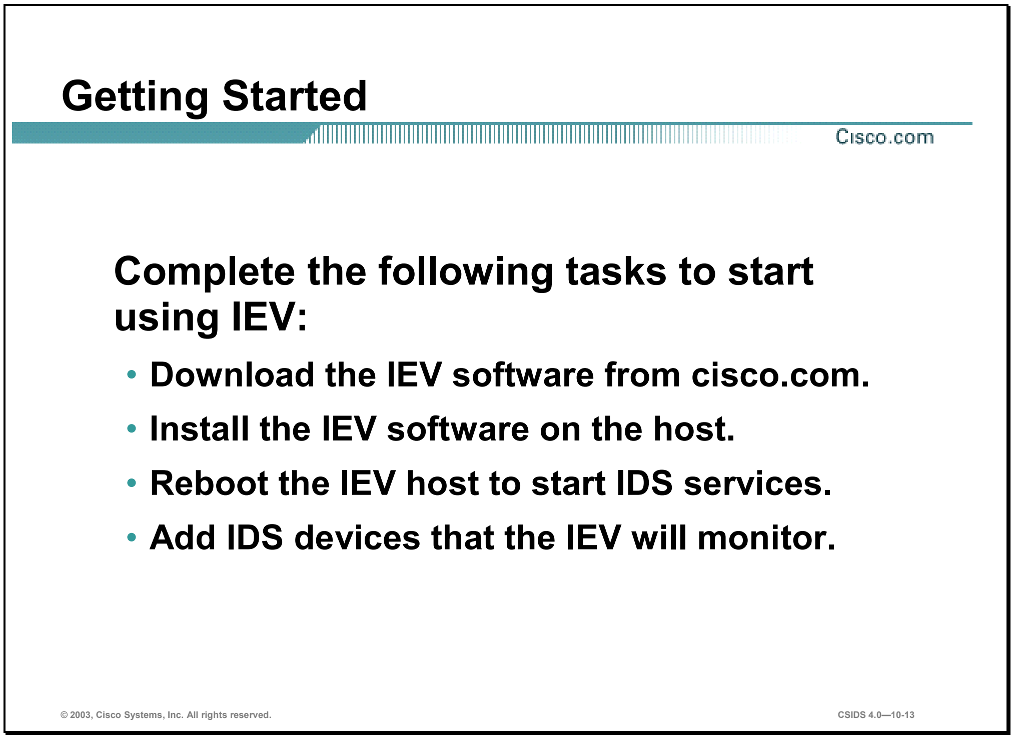
Operating System	Version
Windows NT	4.0 Service Pack 6
Windows 2000	Service Pack 2

IEV can be installed on a system that meets or exceeds the following minimum hardware requirements:

- Processor—Pentium III, 800Mhz or greater
- Memory (MB)—256
- Disk space (MB)—500

IDS Event Viewer Installation

This section describes how to install and configure the IDS Event Viewer (IEV) to monitor events from an IDS device.



Getting Started

Cisco.com

Complete the following tasks to start using IEV:

- **Download the IEV software from cisco.com.**
- **Install the IEV software on the host.**
- **Reboot the IEV host to start IDS services.**
- **Add IDS devices that the IEV will monitor.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—10-13

You must complete the following tasks to begin using IEV to monitor events from an IDS device:

Step 1 Download the IEV software from www.cisco.com.

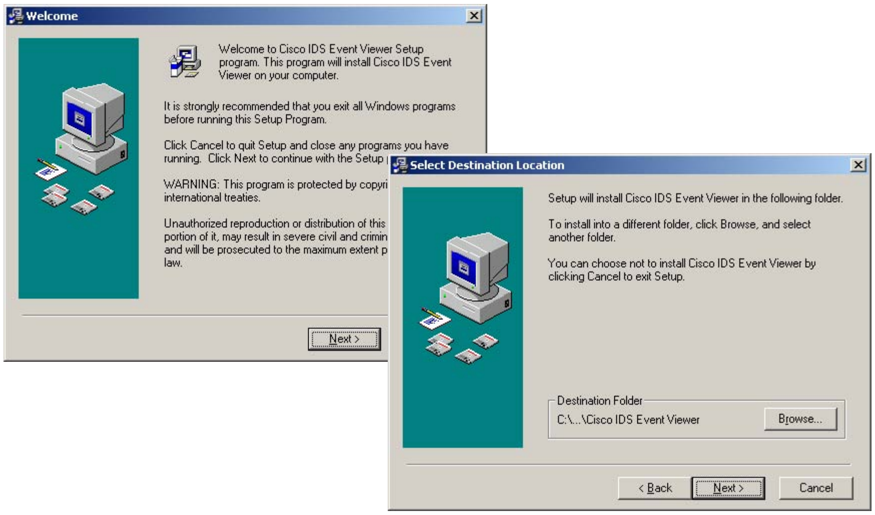
Step 2 Install the IEV software on the host—This includes starting the IEV setup program and continuing with the installation wizard.

Step 3 Reboot the IEV host to start the IDS services—This includes rebooting the IEV host in order to initialize the IDS services needed by IEV.

Step 4 Add IDS devices that the IEV is to monitor—This includes specifying the IDS devices from which the IEV application accepts events.

IEV Installation

Cisco.com



Welcome

Welcome to Cisco IDS Event Viewer Setup program. This program will install Cisco IDS Event Viewer on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup p

WARNING: This program is protected by copyri international treaties.

Unauthorized reproduction or distribution of this portion of it, may result in severe civil and crimin and will be prosecuted to the maximum extent p law.

Select Destination Location

Setup will install Cisco IDS Event Viewer in the following folder.

To install into a different folder, click Browse, and select another folder.

You can choose not to install Cisco IDS Event Viewer by clicking Cancel to exit Setup.

Destination Folder: C:\...\Cisco IDS Event Viewer

CSIDS 4.0—10-14

The IEV installation application is a wizard-based installation program. Complete the following steps to install the IEV application:

Step 1 Launch the IEV installation application from the location where it was saved. The Cisco IDS Event Viewer Welcome window opens.

Step 2 Click **Next** to continue the installation wizard process. The Select Destination Location window opens.

Step 3 Specify the destination folder if the default location is not acceptable. Click **Next** to continue with the wizard installation process. The Select Program Manager window opens.

Step 4 Enter the Program Manager group if the default location is not acceptable. Click **Next** to continue with the installation wizard process. The Start installation window opens.

Step 5 Click **Back** if any mistakes were made. Click **Next** to continue with the installation wizard process. The Installing window displays the IEV installation progress.

The IEV application files are copied to the destination location. The IEV file copy process takes approximately 5–7 minutes depending on system performance.

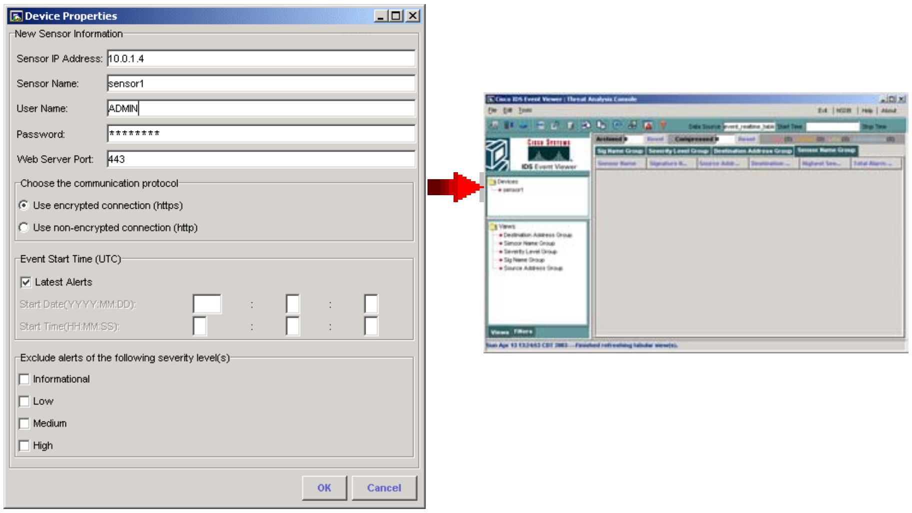
Step 6 Click **Finish** to complete the IEV installation wizard process. The Install dialog window opens.

Step 7 Click **OK** to restart the system and complete the installation process.

Add IDS Devices

Cisco.com

Choose File>New>Devices**.**



Device Properties

New Sensor Information

Sensor IP Address: 10.0.1.4

Sensor Name: sensor1

User Name: ADMIN

Password: ********

Web Server Port: 443

Choose the communication protocol

● Use encrypted connection (https)

○ Use non-encrypted connection (http)

Event Start Time (UTC)

☑ Latest Alerts

Start Date(YYYY:MM:DD): _ : _ : _

Start Time(HH:MM:SS): _ : _ : _

Exclude alerts of the following severity level(s)

□ Informational

□ Low

□ Medium

□ High

CSIDS 4.0—10-17

The IEV installation process does not prompt you to add an IDS device to monitor. Complete the following steps to add an IDS device to the IEV:

Step 1 Choose **Start>Programs>Cisco Systems>Cisco IDS Event Viewer>Cisco IDS Event Viewer** to launch the IEV. The Cisco IDS Event Viewer application opens.

Step 2 Choose **File>New>Device** from the main menu. The Device Properties window opens.

Step 3 Complete the following fields in the Device Properties window:

- Sensor IP Address
- Sensor Name
- User Name
- Password
- Web Server Port

Note The information you provide in the Device Properties panel should match the settings you entered during the initial configuration of the Sensor. If you have set up a user account with Viewer access for the IEV, specify the username and password for that account.

Step 4 To specify the communication protocol the IEV should use when connecting to the Sensor, select the **Use encrypted connection (https)** or **Use non-encrypted connection** radio button. The Use non-encrypted connection option is helpful for troubleshooting.

Step 5 Complete one of the following tasks to specify which alerts to pull from the Sensor:

- Select the **Latest Alerts** check box to pull the latest alerts from the Sensor. The IEV will receive alerts from the Sensor, starting with the first alert the Sensor receives after connecting to the IEV.

- Deselect the **Latest Alerts** check box to pull alerts from the Sensor eventStore. The IEV will receive alerts from the Sensor, starting with the first alert that matches the criteria you specify. The following criteria may be specified:

  - Start Date

  - Start Time

Step 6 Alarms that match the severity levels you select are not pulled from the Sensor eventStore and will not appear in the Statistical Graph. Select one or more of the following options to exclude alarms of specific severity levels:

- Informational

- Low

- Medium

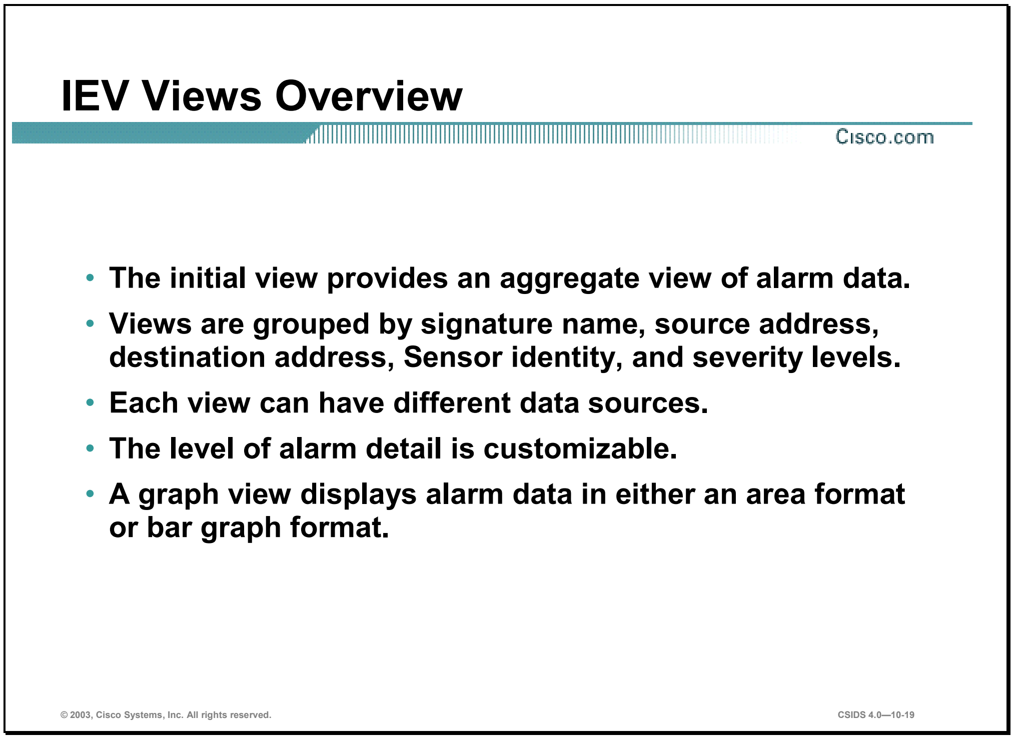
- High

Step 7 Click **OK** to close the Device Properties panel. The IEV sends a subscription request to the Sensor. This request remains open until you modify the device properties or delete the device.

Note If you specified HTTPS as the communication protocol, the IEV retrieves the certificate information from the Sensor and displays the Certificate Information dialog box. You must click **Yes** to accept the certificate and continue the HTTPS connection between the IEV and the Sensor.

IDS Event Viewer Views

This section describes the IDS Event Viewer (IEV) view concept and instructions on how to navigate, modify, and create views.



IEV Views Overview

- **The initial view provides an aggregate view of alarm data.**
- **Views are grouped by signature name, source address, destination address, Sensor identity, and severity levels.**
- **Each view can have different data sources.**
- **The level of alarm detail is customizable.**
- **A graph view displays alarm data in either an area format or bar graph format.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—10-19

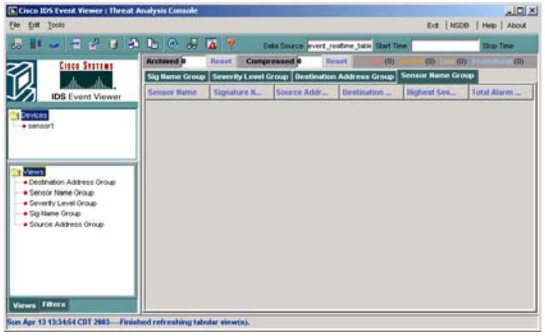
The IEV displays alarm data as views. IEV aggregates the IDS alarm data to provide the network security administrator with a high-level overview. These views are grouped by signature name, source address, destination address, Sensor name, and severity levels.

IEV uses a relational database, which enables the use of different data sources. The real-time data is stored in a database table named event_realtime_table. For example, if you import an IDS log file into the IEV database, a new table is created in the database. You can then specify this table as the data source used for any given view.

IEV views enable the network security administrator to customize the amount of alarm data detail that is displayed when selecting the alarm detail dialog.

IEV provides a graphical representation of the IDS alarm data. The graph displays alarm data in either an area format or bar graph format.

IEV Default Views



Sun Apr 13 13:34:54 CDT 2003—Finished refreshing tabular view(s).

The IEV has the following default views:

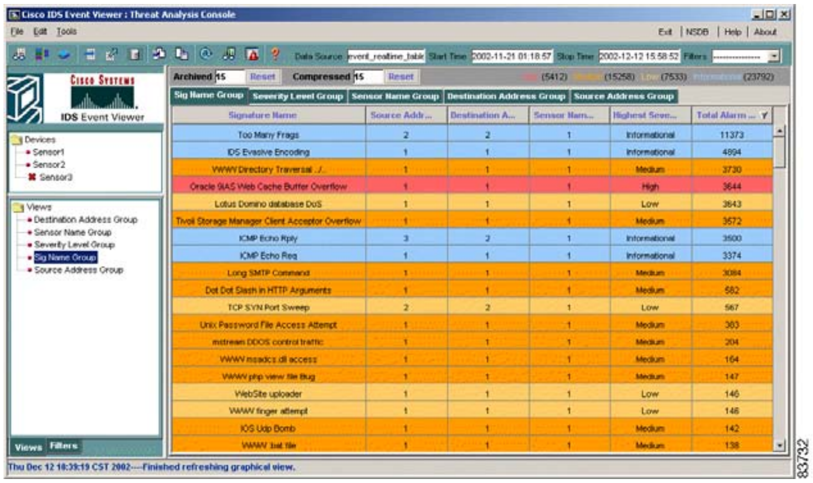
- Destination Address Group
- Sensor Name Group
- Severity Level Group
- Sig Name Group
- Source Address Group

IEV has the following default views available:

- Destination Address Group—Groups the alarm data by the destination address
- Sensor Name Group—Groups the alarm data by the Sensor name
- Severity Level Group—Groups the alarm data by the alarm severity level
- Sig Name Group—Groups the alarm data by the signature names
- Source Address Group—Groups the alarm data by the source address

Navigating Views

Cisco.com


Cisco IDS Event Viewer : Threat Analysis Console
File Edit Tools
Exit | NSDB | Help | About
Data Source event_realtime_table Start Time 2002-11-21 01:18:57 Stop Time 2002-12-12 15:58:52 Filters
Archived 15 Reset Compressed 15 Reset
(5412) (15258) Low (7533) (23792)
Sig Name Group
Severity Level Group
Sensor Name Group
Destination Address Group
Source Address Group
Cisco Systems
IDS Event Viewer
Devices
Sensor1
Sensor2
Sensor3
Views
Destination Address Group
Sensor Name Group
Severity Level Group
Sig Name Group
Source Address Group
Views Filters
83732

Signature Name	Source Addr...	Destination A...	Sensor Nam...	Highest Seve...	Total Alarm ...
Too Many Frags	2	2	1	Informational	11373
IDS Evasive Encoding	1	1	1	Informational	4894
WWW Directory Traversal ../..	1	1	1	Medium	3730
Oracle 9iAS Web Cache Buffer Overflow	1	1	1	High	3644
Lotus Domino database DoS	1	1	1	Low	3643
Tivoli Storage Manager Client Acceptor Overflow	1	1	1	Medium	3572
ICMP Echo Rply	3	2	1	Informational	3500
ICMP Echo Req	1	1	1	Informational	3374
Long SMTP Command	1	1	1	Medium	3084
Dot Dot Slash in HTTP Arguments	1	1	1	Medium	582
TCP SYN Port Sweep	2	2	1	Low	567
Unix Password File Access Attempt	1	1	1	Medium	383
mstream DDOS control traffic	1	1	1	Medium	204
WWW msadcs.dll access	1	1	1	Medium	164
WWW php view file Bug	1	1	1	Medium	147
WebSite uploader	1	1	1	Low	146
WWW finger attempt	1	1	1	Low	146
IOS Udp Bomb	1	1	1	Medium	142
WWW bat file	1	1	1	Medium	138

Thu Dec 12 18:39:19 CST 2002—Finished refreshing graphical view.

CSIDS 4.0—10-21

To display a view, double-click the view from the Views folder. The view is displayed in the right pane. The figure displays the result of selecting all of the default views. Notice that a view tab represents each view. In the figure, the signature name group view (Sig Name Group) is active.

To close a view, right-click the view tab and choose **Close <view>** from the drop-down menu, where <view> is the name assigned to the view. Closing the view does not delete the view from the database. To delete a view, right-click the view from the View folders and choose **Delete View** from the drop-down menu. This deletes the view from the database.

To change the data source used for a view, right-click the view from the Views folder and choose **Data Source** from the drop-down menu. The Change Data Source window opens. Choose the name of the database table and click **OK**. Only one database table can be selected as the data source.

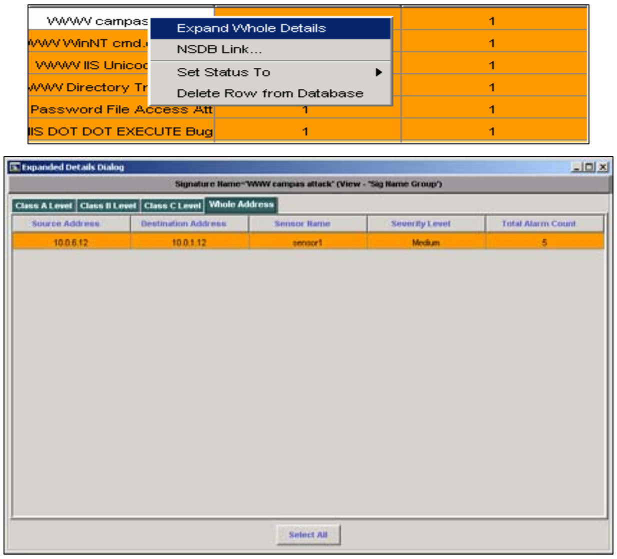
To modify the settings for a view, right-click the view from the Views folder and choose **Properties** from the drop-down menu. The View Wizard window opens.

Note Refer to the Creating Views section later in this chapter for more information.

To delete an event, right-click the event in the view and choose **Delete Row in Database**. This deletes the event from the database.

Note An event can be deleted from any view and dialog window.

Whole Details



WWW campas		1
WWW WinNT cmd.		1
WWW IIS Unicod		1
WWW Directory Tr		1
Password File Access Att	1	1
IIS DOT DOT EXECUTE Bug	1	1

Signature Name="WWW campas attack" (View - "Sig Name Group")

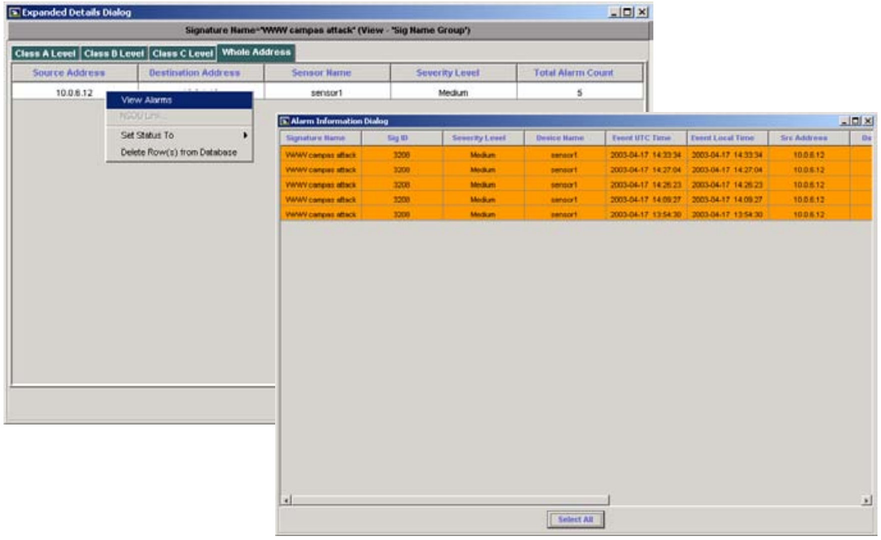
Source Address	Destination Address	Sensor Name	Severity Level	Total Alarm Count
10.0.6.12	10.0.1.12	sensor1	Medium	5

To display all of the details of an IDS event, right-click the event and choose **Expand Whole Details** from the drop-down menu. The Expanded Details Dialog window displays the alarm data by the following:

- Class A Level
- Class B Level
- Class C Level
- Whole Address

Alarm Information

Cisco.com



Source Address	Destination Address	Sensor Name	Severity Level	Total Alarm Count
10.0.6.12	[illegible]	sensor1	Medium	5

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Ds
WWW campas attack	3200	Medium	sensor1	2003-04-17 14:33:34	2003-04-17 14:33:34	10.0.6.12	
WWW campas attack	3200	Medium	sensor1	2003-04-17 14:27:04	2003-04-17 14:27:04	10.0.6.12	
WWW campas attack	3200	Medium	sensor1	2003-04-17 14:26:23	2003-04-17 14:26:23	10.0.6.12	
WWW campas attack	3200	Medium	sensor1	2003-04-17 14:09:27	2003-04-17 14:09:27	10.0.6.12	
WWW campas attack	3200	Medium	sensor1	2003-04-17 13:54:30	2003-04-17 13:54:30	10.0.6.12	

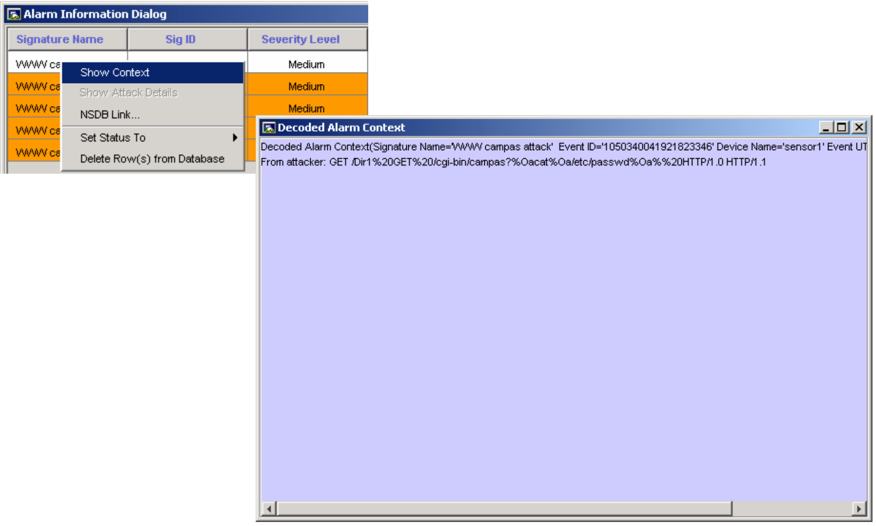
CSIDS 4.0—10-23

To view the alarm information, right-click the alarm in the Expanded Details Dialog window and choose **View Alarms**. The Alarm Information Dialog window displays each event and the associated alarm data, such as Signature Name, Source Address, and Destination Address.

To view all the data associated with an alarm, right-click a column heading and choose **Show All columns** from the drop-down menu.

Alarm Context Data

Cisco.com



Signature Name	Sig ID	Severity Level
WWW ca		Medium
WWW ca		Medium
WWW ca		Medium
WWW ca		
WWW ca		

```
Decoded Alarm Context(Signature Name='WWW campas attack'  Event ID='1050340041921823346' Device Name='sensor1' Event UT
From attacker: GET /Dir1%20GET%20/cgi-bin/campas?%0acat%0a/etc/passwd%0a%%20HTTP/1.0 HTTP/1.1
```

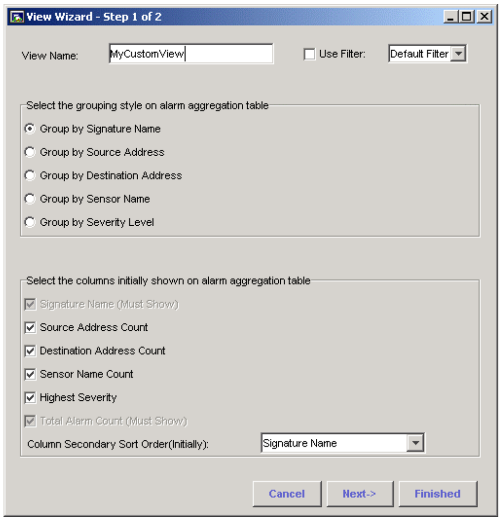
For TCP-based signatures, the Sensor captures up to 256 characters of the TCP stream, which may be examined from the Event Viewer. This is called the context data buffer and it contains keystrokes, data, or both in the connection stream around the string of characters that triggered the signature. This feature can be used to determine if the triggered alarm was from a deliberate attack or if it is an accidental set of keystrokes.

To view the captured context data buffer, right-click the alarm you wish to examine and choose **Show Context** from the drop-down menu. The Decode Alarm Context displays the signature and context information. In the figure, the context data is associated with the WWW campas attack signature. The decoded alarm data is the following:

```
GET /Dir1%20GET%20/cgi-bin/campas?%0acat%0a/etc/passwd%0a%%20HTTP/1.0 HTTP/1.1
```

Creating Views

Cisco.com



View Wizard - Step 1 of 2

View Name: MyCustomView

☐ Use Filter: Default Filter

Select the grouping style on alarm aggregation table

● Group by Signature Name
○ Group by Source Address
○ Group by Destination Address
○ Group by Sensor Name
○ Group by Severity Level

Select the columns initially shown on alarm aggregation table

☑ Signature Name (Must Show)
☑ Source Address Count
☑ Destination Address Count
☑ Sensor Name Count
☑ Highest Severity
☑ Total Alarm Count (Must Show)

Column Secondary Sort Order(Initially): Signature Name

- Assign a name to the view.
- (Optional.) Choose a filter.
- Select the grouping style on the alarm aggregation table.
- Select the columns initially shown on the alarm aggregation table.
- Choose the default secondary sort criteria.

CSIDS 4.0—10-25

Creating views enables the network security administrator to customize the data that is displayed when an event is reported. To create a view, complete the following steps:

Step 1 Choose **File>New>View** from the main menu. The View Wizard window opens.

Step 2 Assign a name to the view by entering the name in the View Name field. If a filter with the same name exists, IEV provides a prompt prior to overwriting the existing view.

Step 3 (Optional.) Enable and assign a filter to the view from the Use Filter drop-down menu.

Step 4 Select the grouping style by selecting the check boxes within the Select the grouping style on alarm aggregation table group box.

Step 5 Select the columns you want displayed on the alarm aggregation table by selecting the check boxes within the Select the columns initially shown on alarm aggregation table group box.

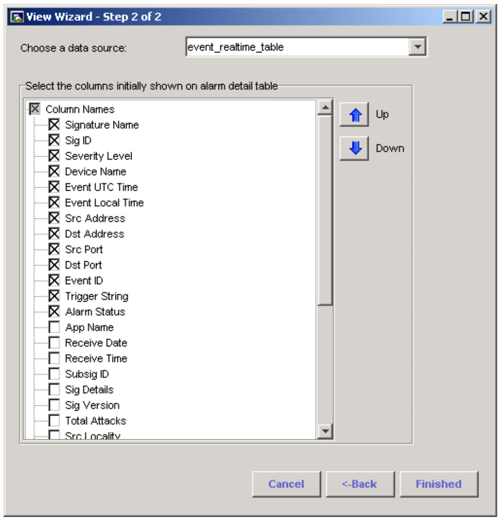
Step 6 Choose the default secondary sort order criteria from the Column Secondary Sort Order (Initially) drop-down menu.

Step 7 Click **Next** to continue. The View Wizard Step 2 Window opens.

Note If you click the Finished button, the default values in the next window are assigned to the view.

Creating Views (cont.)

Cisco.com



View Wizard - Step 2 of 2

Choose a data source: event_realtime_table

Select the columns initially shown on alarm detail table

- ☒ Column Names
  - ☒ Signature Name
  - ☒ Sig ID
  - ☒ Severity Level
  - ☒ Device Name
  - ☒ Event UTC Time
  - ☒ Event Local Time
  - ☒ Src Address
  - ☒ Dst Address
  - ☒ Src Port
  - ☒ Dst Port
  - ☒ Event ID
  - ☒ Trigger String
  - ☒ Alarm Status
  - □ App Name
  - □ Receive Date
  - □ Receive Time
  - □ Subsig ID
  - □ Sig Details
  - □ Sig Version
  - □ Total Attacks
  - □ Src Locality

- Choose the data source for the events.
- Choose the columns that are displayed in the alarm detail table.
- Choose the column display order.

CSIDS 4.0—10-26

Step 8 Choose the default data source for the events from the Choose a data source drop-down menu.

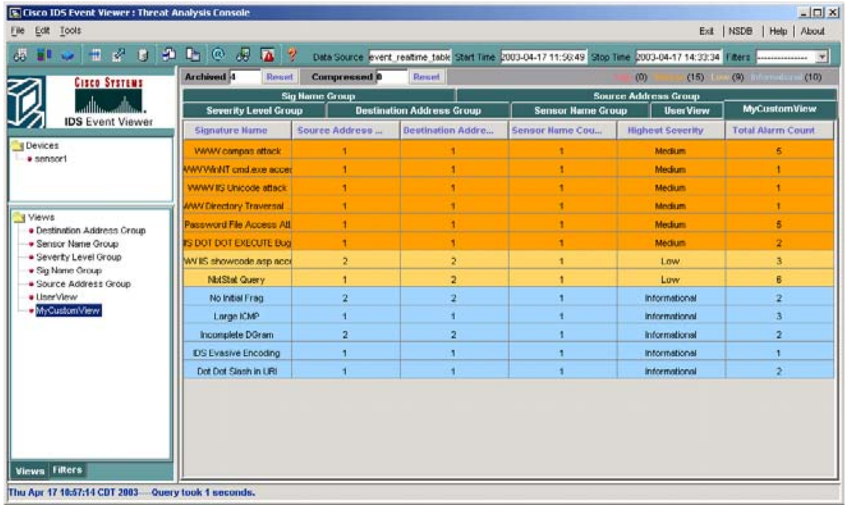
Note Select the event_realtime_table if you want to view IDS events as they occur.

Step 9 Select the columns you want displayed in the alarm detail table by selecting the check boxes within the Select the columns initially shown on alarm detail table group box.

Step 10 Choose the order of the columns you want displayed by using the Up and Down buttons.

Step 11 Click **Finished** to save the settings to the view.

Example—MyCustomView



Data Source event_realtime_table Start Time 2003-04-17 11:56:49 Stop Time 2003-04-17 14:33:34 Filters

Archived 4 Compressed 0

(0) (15) (9) (10)

Signature Name	Source Address ...	Destination Addre...	Sensor Name Cou...	Highest Severity	Total Alarm Count
WWW campas attack	1	1	1	Medium	5
WWWWinNT cmd.exe acces	1	1	1	Medium	1
WWW IIS Unicode attack	1	1	1	Medium	1
WWW Directory Traversal	1	1	1	Medium	1
Password File Access Att	1	1	1	Medium	5
IIS DOT DOT EXECUTE Bug	1	1	1	Medium	2
WWW IIS showcode.asp acce	2	2	1	Low	3
NbtStat Query	1	2	1	Low	6
No Initial Frag	2	2	1	Informational	2
Large ICMP	1	1	1	Informational	3
Incomplete DGram	2	2	1	Informational	2
IDS Evasive Encoding	1	1	1	Informational	1
Dot Dot Slash in URI	1	1	1	Informational	2

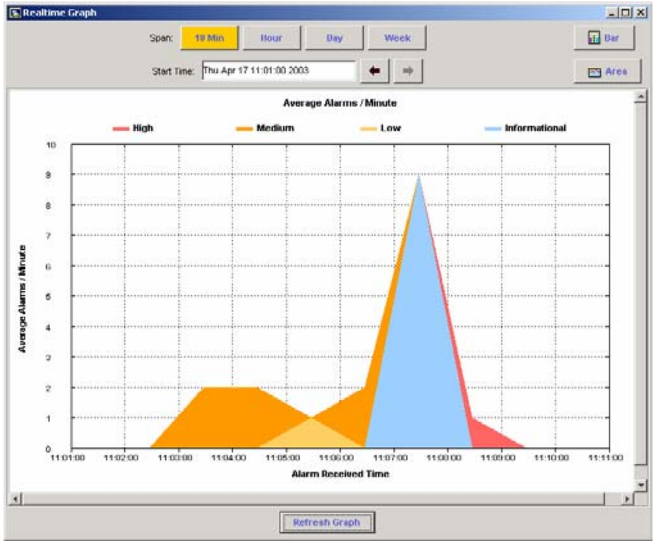
Thu Apr 17 10:57:14 CDT 2003—Query took 1 seconds.

The figure displays an example of the custom view created using the View Wizard. The following are the MyCustomView properties:

- Grouping style—Signature Name
- The columns that are displayed by default
  - Signature Name
  - Source Address Count
  - Destination Address Count
  - Sensor Name Count
  - Highest Severity
  - Total Alarm Count

Note To view the view properties, right-click the view and choose **Properties**.

Example—Realtime Graph View



Start Time: Thu Apr 17 11:01:00 2003

CSIDS 4.0—10-28

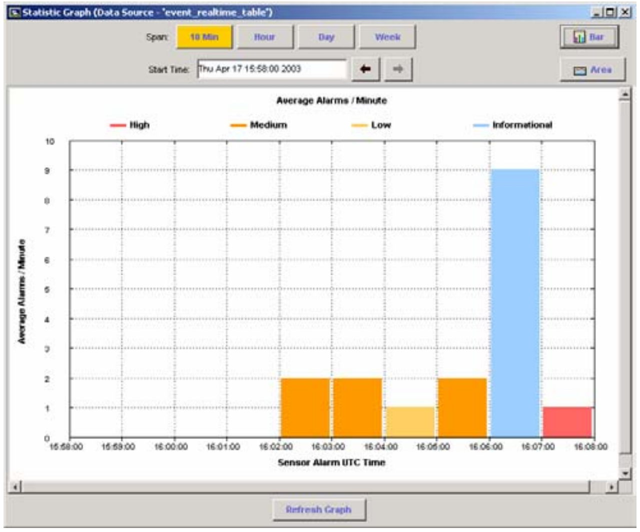
You can view events in a Realtime Graph or Statistical Graph. Each graph provides a view of the average number of alarms per minute, based on severity level. However, each graph represents a different data source and therefore a different view into the events.

The Realtime Graph is populated with events from a continuously running thread in the IEV. This thread continuously monitors and aggregates the total number of alarms the IEV receives. The events displayed in the Realtime Graph reflect the average number of alarms received by the IEV. The time stamp for these events reflects the time the IEV received the alarm, not necessarily the time the Sensor generated the alarm. To view the Realtime Graph, select **Tools>Realtime Graph.**

Note You can right-click cells within the graph to view alarm information.

Example—Statistical Graph View

Cisco.com



Statistic Graph (Data Source - 'event_realtime_table')

Span: 10 Min

Start Time: Thu Apr 17 15:58:00 2003

CSIDS 4.0—10-29

The Statistical Graph is populated with events from the data source you select. Valid data sources include the event_realtime_table, any archived table, or any imported table. The events displayed in the Statistical Graph reflect the average number of alarms received by IEV, based on the filter that is applied to the data source. Therefore, depending on the filter, the Statistical Graph may not reflect the true average number of alarms. The time stamp for these events reflects the time the Sensor generated the alarm.

Complete the following steps to view the Statistical Graph:

Step 1 Expand the Views folder and locate the view that contains the alarm data you want to display in a graph.

Step 2 Right-click the view and select **Statistical Graph**. The IEV queries the data source for the selected view and calculates the average alarms per minute. The Statistical Graph appears and displays the result.

Step 3 Complete the following sub-steps to change the range of events displayed in the graph:

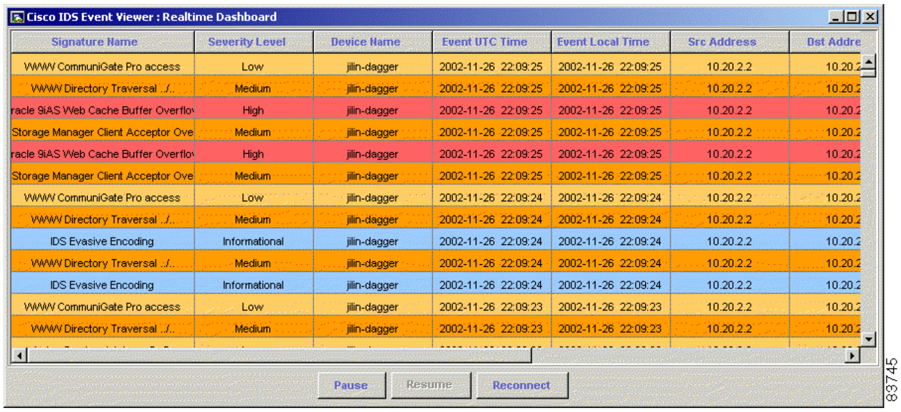
1. Click one of the Span buttons to specify the time span by which you want to advance the view.

2. Use the forward and backward arrows to adjust the start time by the interval selected with a Span button.

Step 4 Click **Bar** or **Area** to change the presentation to a bar or area graph.

Realtime Dashboard

Cisco.com



Signature Name	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst Addre
WWW CommuniGate Pro access	Low	jilin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2
WWW Directory Traversal ../..	Medium	jilin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2
racle 9iAS Web Cache Buffer Overflo	High	jilin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2
Storage Manager Client Acceptor Ove	Medium	jilin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2
racle 9iAS Web Cache Buffer Overflo	High	jilin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2
Storage Manager Client Acceptor Ove	Medium	jilin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2
WWW CommuniGate Pro access	Low	jilin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2
WWW Directory Traversal ../..	Medium	jilin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2
IDS Evasive Encoding	Informational	jilin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2
WWW Directory Traversal ../..	Medium	jilin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2
IDS Evasive Encoding	Informational	jilin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2
WWW CommuniGate Pro access	Low	jilin-dagger	2002-11-26 22:09:23	2002-11-26 22:09:23	10.20.2.2	10.20.2
WWW Directory Traversal ../..	Medium	jilin-dagger	2002-11-26 22:09:23	2002-11-26 22:09:23	10.20.2.2	10.20.2

CSIDS 4.0—10-30

You can use the Realtime Dashboard to view a continuous stream of real-time events from the Sensor. Complete the following steps to view events in the Realtime Dashboard:

Step 1 Select **Tools>Realtime Dashboard>Launch Dashboard**. The IEV opens a subscription request with the Sensor. If the connection is successful, the Realtime Dashboard appears and displays the most recent events received by the Sensor since the request was opened.

Step 2 Click **Pause** to pause the stream of real-time events. The IEV stops populating the Realtime Dashboard with events.

Step 3 Click **Resume** to resume the stream of real-time events. The IEV populates the Realtime Dashboard with events, starting with the first event that was received after the stream was paused.

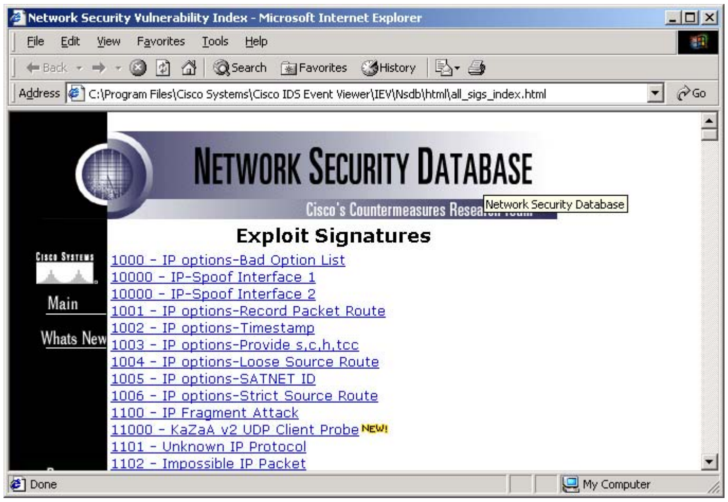
Step 4 Click **Reconnect** to clear all existing events from the Realtime Dashboard. All existing events are removed from the Realtime Dashboard and the IEV opens a new subscription with the Sensor.

Network Security Database

This section describes the Network Security Database (NSDB) and the information that exists in the database.

NSDB Signature Index

Cisco.com



Network Security Vulnerability Index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go
NETWORK SECURITY DATABASE
Cisco's Countermeasures Research Team
Network Security Database
Cisco Systems
Main
Whats New
Done
My Computer

Address C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\all_sigs_index.html

Exploit Signatures

1000 - IP options-Bad Option List
10000 - IP-Spoof Interface 1
10000 - IP-Spoof Interface 2
1001 - IP options-Record Packet Route
1002 - IP options-Timestamp
1003 - IP options-Provide s,c,h,tcc
1004 - IP options-Loose Source Route
1005 - IP options-SATNET ID
1006 - IP options-Strict Source Route
1100 - IP Fragment Attack
11000 - KaZaA v2 UDP Client Probe NEW!
1101 - Unknown IP Protocol
1102 - Impossible IP Packet

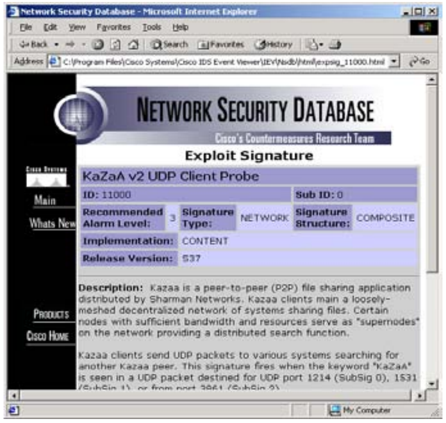
CSIDS 4.0—10-32

The NSDB is the Cisco HTML-based encyclopedia of network vulnerability information. You can examine the NSDB for a specific alarm. The Cisco Secure Encyclopedia (CSEC) is the online equivalent of the NSDB.

CSEC has been developed as a central warehouse of security knowledge to provide Cisco security professionals with an interactive database of security vulnerability information. CSEC contains detailed information about security vulnerabilities such as countermeasures, affected systems and software, and Cisco Secure products that can help you test for vulnerabilities or detect when malicious users attempt to exploit your systems. The CSEC can be found at http://www.cisco.com/go/csec.

Note	A valid Cisco Connection Online (CCO) account is required to view the CSEC data.

Signature Information


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\expsig_11000.html
Go
NETWORK SECURITY DATABASE
Cisco's Countermeasures Research Team
Main
Whats New
Products
Cisco Home
My Computer

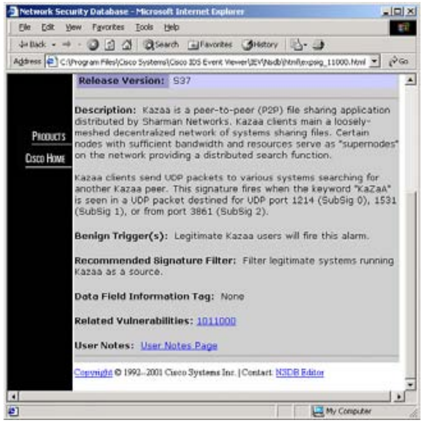
Exploit Signature

KaZaA v2 UDP Client Probe

ID: 11000				Sub ID: 0	
Recommended Alarm Level:	3	Signature Type:	NETWORK	Signature Structure:	COMPOSITE
Implementation:	CONTENT				
Release Version:	S37				

Description: Kazaa is a peer-to-peer (P2P) file sharing application distributed by Sharman Networks. Kazaa clients main a loosely-meshed decentralized network of systems sharing files. Certain nodes with sufficient bandwidth and resources serve as "supernodes" on the network providing a distributed search function.

Kazaa clients send UDP packets to various systems searching for another Kazaa peer. This signature fires when the keyword "KaZaA" is seen in a UDP packet destined for UDP port 1214 (SubSig 0), 1531 (SubSig 1), or from port 3861 (SubSig 2).


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\expsig_11000.html
Go
Products
Cisco Home
My Computer

Release Version: S37

Description: Kazaa is a peer-to-peer (P2P) file sharing application distributed by Sharman Networks. Kazaa clients main a loosely-meshed decentralized network of systems sharing files. Certain nodes with sufficient bandwidth and resources serve as "supernodes" on the network providing a distributed search function.

Kazaa clients send UDP packets to various systems searching for another Kazaa peer. This signature fires when the keyword "KaZaA" is seen in a UDP packet destined for UDP port 1214 (SubSig 0), 1531 (SubSig 1), or from port 3861 (SubSig 2).

Benign Trigger(s): Legitimate Kazaa users will fire this alarm.

Recommended Signature Filter: Filter legitimate systems running Kazaa as a source.

Data Field Information Tag: None

Related Vulnerabilities: 1011000

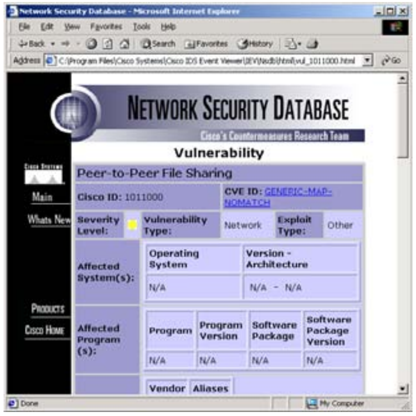
User Notes: User Notes Page

Copyright © 1992–2001 Cisco Systems Inc. | Contact: NSDB Editor

A typical NSDB Exploit Signature page contains the following information about the signature that triggered the alarm:

- Signature Name—The name of the signature.
- ID—A unique identification number for the signature.
- Sub ID—A unique sub-identification number for the sub-signature.
- Recommended Alarm Level—The alarm severity level recommended by the C-CRT.
- Signature Type—Indicates the alarm was detected on the network.
- Signature Structure—Indicates if the signature structure is either atomic or composite.
- Implementation—Indicates if the signature implementation is either content or context.
- Signature Description—A concise explanation of the signature and what exploits it detects.
- Benign Trigger(s)—An explanation of any false-positives that may appear to be an exploit but are actually normal network activity.
- Related Vulnerability—Each vulnerability information page provides background on the vulnerability and a link to any available countermeasures.
- User Notes—Link to a page with information unique to this installation and implementation.

Related Vulnerability Information


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go
Main
Whats New
Products
Cisco Home
Done
My Computer

Address: C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\vul_1011000.html

NETWORK SECURITY DATABASE

Cisco's Countermeasures Research Team

Vulnerability

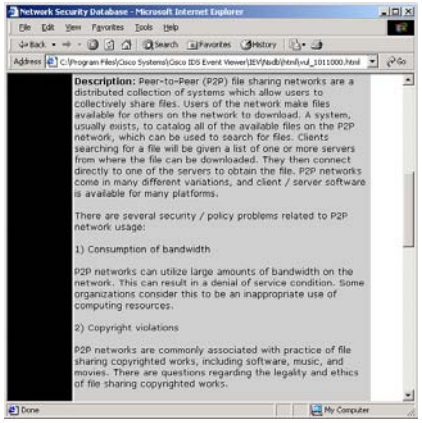
Peer-to-Peer File Sharing

Cisco ID: 1011000			CVE ID: GENERIC-MAP-NOMATCH		
Severity Level:	🟨	Vulnerability Type:	Network	Exploit Type:	Other

Affected System(s):	Operating System	Version - Architecture
	N/A	N/A - N/A

Affected Program (s):	Program	Program Version	Software Package	Software Package Version
	N/A	N/A	N/A	N/A

	Vendor	Aliases


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go
Done
My Computer

Address: C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\vul_1011000.html

Description: Peer-to-Peer (P2P) file sharing networks are a distributed collection of systems which allow users to collectively share files. Users of the network make files available for others on the network to download. A system, usually exists, to catalog all of the available files on the P2P network, which can be used to search for files. Clients searching for a file will be given a list of one or more servers from where the file can be downloaded. They then connect directly to one of the servers to obtain the file. P2P networks come in many different variations, and client / server software is available for many platforms.

There are several security / policy problems related to P2P network usage:

1) Consumption of bandwidth

P2P networks can utilize large amounts of bandwidth on the network. This can result in a denial of service condition. Some organizations consider this to be an inappropriate use of computing resources.

2) Copyright violations

P2P networks are commonly associated with practice of file sharing copyrighted works, including software, music, and movies. There are questions regarding the legality and ethics of file sharing copyrighted works.

A typical NSDB Related Vulnerability page contains the following information about the vulnerability associated with the signature that triggered the alarm:

- Vulnerability Name—The name of the vulnerability being exploited.
- Alias—Any other names used to refer to the vulnerability or exploit.
- Cisco ID—A unique identification number for the vulnerability. (It is unrelated to the Signature ID.)
- CVE ID—The Common Vulnerability and Exposures (CVE) is a list of standardized names for vulnerabilities and other information security exposures. Each vulnerability or exposure is assigned an identification number. The CVE database can be found at http://www.cve.mitre.org.
- Severity Level—A severity level associated with the vulnerability, which may or may not match the recommended alarm level.
- Vulnerability Type—Indicates this is a network vulnerability.
- Exploit Type—Indicates the type of exploit, such as Info, Recon, Access, or Denial.
- Affected System(s)—List of operating systems and their versions affected by the vulnerability.
- Affected Program(s)—List of applications and their versions affected by the vulnerability.

- Vulnerability Description—A concise explanation of the vulnerability and how to exploit it.

- Consequence(s)—What damage is done by exploiting the vulnerability.

- Countermeasures(s)—Description of what can be done to protect systems from the vulnerability.

- Advisory/Related Info Link(s)—Links to web sites that contain additional information about the vulnerability or exploit.

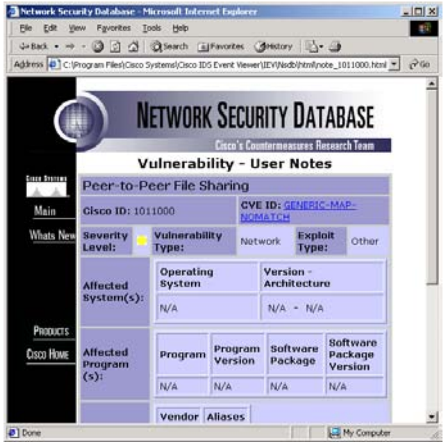
- Fix/Upgrade/Patch Link(s)—Links to web sites that contain fixes, upgrades, or patches for the vulnerability.

- Exploit Link(s)—Links to web sites where vulnerability exploits may be found.

- User Notes—Link to a page with information unique to this installation and implementation.

User Notes

Cisco.com


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Cisco Systems
Main
Whats New
Products
Cisco Home
Done
My Computer

Address: C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\note_1011000.html

NETWORK SECURITY DATABASE

Cisco's Countermeasures Research Team

Vulnerability - User Notes

Peer-to-Peer File Sharing

Cisco ID: 1011000 **CVE ID:** GENERIC-MAP-NOMATCH

Severity Level: ● **Vulnerability Type:** Network **Exploit Type:** Other

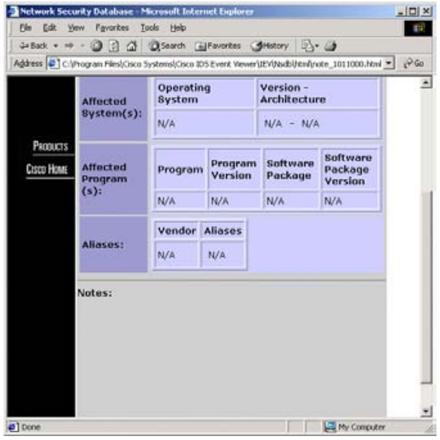
Affected System(s):

Operating System	Version - Architecture
N/A	N/A - N/A

Affected Program (s):

Program	Program Version	Software Package	Software Package Version
N/A	N/A	N/A	N/A

Vendor	Aliases


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Products
Cisco Home
Done
My Computer

Address: C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\Nsdb\html\note_1011000.html

Affected System(s):

Operating System	Version - Architecture
N/A	N/A - N/A

Affected Program (s):

Program	Program Version	Software Package	Software Package Version
N/A	N/A	N/A	N/A

Aliases:

Vendor	Aliases
N/A	N/A

Notes:

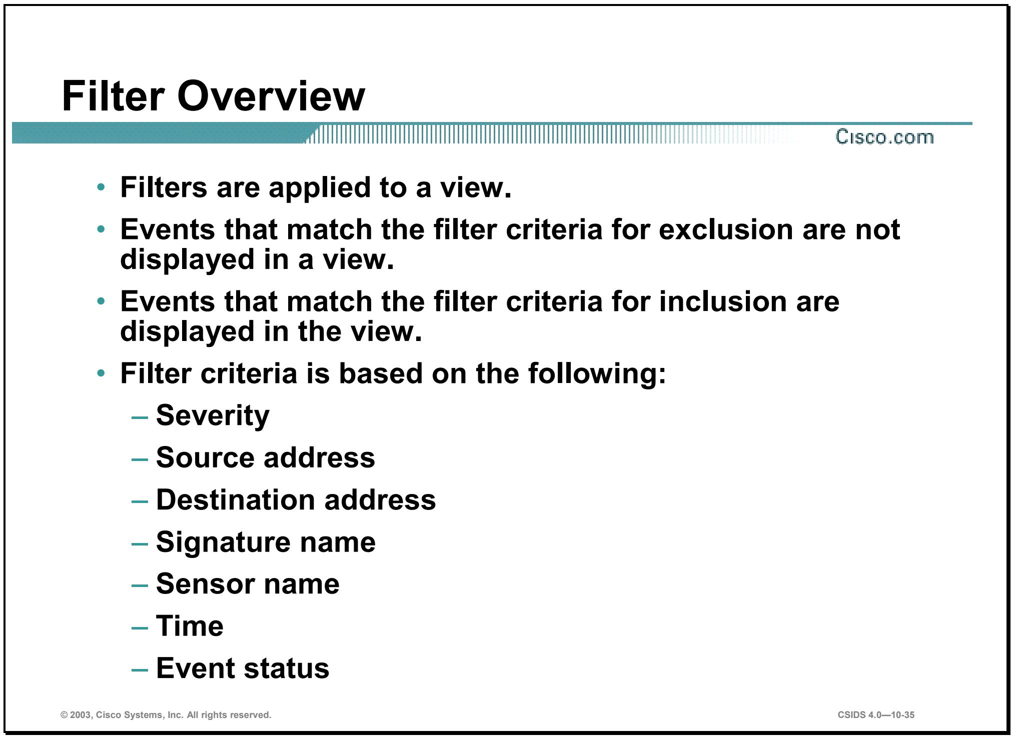
CSIDS 4.0—10-35

The User Notes page is an HTML template in which the user can provide information unique to their installation and implementation. The information can be added for both Cisco IDS signatures and vulnerabilities that exist in the NSDB. Any text or HTML editor may be used to enter the information.

The user notes HTML files are located in the IEV sub-directory (for example, C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\nsdb\html) and are named **note_id**, where id is the Cisco vulnerability or signature ID number. For example, the user notes file for the vulnerability displayed in the figure is note_324.html.

IDS Event Viewer Filters

This section describes the IDS Event Viewer (IEV) filter concept and instructions on how to modify and create filters.



Filter Overview

Cisco.com

- Filters are applied to a view.
- Events that match the filter criteria for exclusion are not displayed in a view.
- Events that match the filter criteria for inclusion are displayed in the view.
- Filter criteria is based on the following:
  - Severity
  - Source address
  - Destination address
  - Signature name
  - Sensor name
  - Time
  - Event status

CSIDS 4.0—10-35

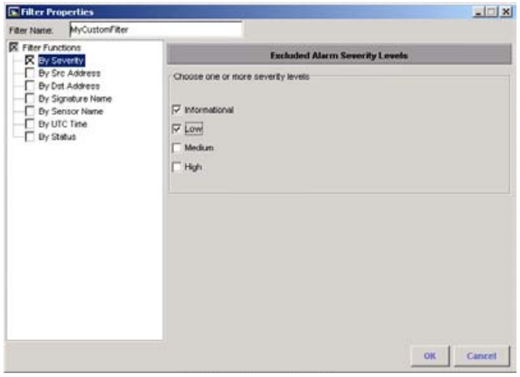
Viewing IDS alarms can be cumbersome depending on the number of IDS devices being monitored and the number of alarms the devices generate. The IEV filter feature provides the network administrator with the capability to create views that match specific criteria.

A filter is created and then applied to a view. Once applied to a view, the filter includes or excludes (according to your specification) in the view those events in the data source that match the filter criteria. The filter criteria may be based on the following:

- Alarm severity
- Source address
- Destination address
- Signature name
- Sensor name
- Time
- Event status

A default filter is included with IEV. To modify an existing filter, right-click the filter from the Filters folder and choose **Properties** from the drop-down menu. To create a new filter, choose **File>New >Filter** from the main menu.

Filter Properties—By Severity



Filter Properties

Filter Name: MyCustomFilter

- ☒ Filter Functions
  - ☒ By Severity
  - □ By Src Address
  - □ By Dst Address
  - □ By Signature Name
  - □ By Sensor Name
  - □ By UTC Time
  - □ By Status

Excluded Alarm Severity Levels

Choose one or more severity levels

- ☑ Informational
- ☑ Low
- □ Medium
- □ High

Select the alarm severity levels to add to the filter:

- **Informational**
- **Low**
- **Medium**
- **High**

CSIDS 4.0—10-38

Complete the following steps to add an alarm severity level to the filter:

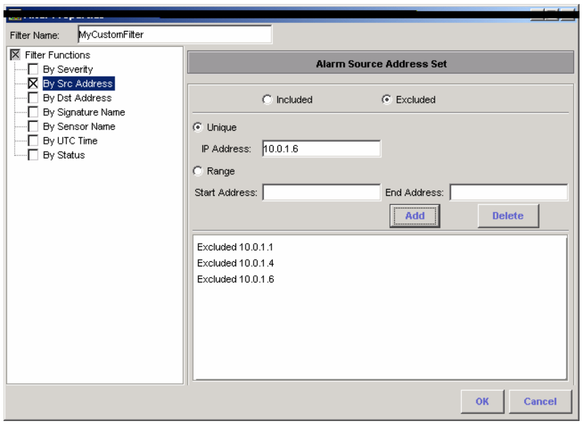
Step 1 Enable the severity function by selecting the **By Severity** check box from the Filter Functions options. The Excluded Alarm Severity Levels information is displayed. Notice the Filter Functions check box is enabled.

Step 2 Add the severity levels to the filter by selecting the appropriate check boxes within the Choose one or more severity levels group box.

Step 3 Click **OK** to save the filter settings.

Note The addition of an alarm severity level in a filter causes it to be excluded when the filter is applied to a view.

Filter Properties—By Source Address



Filter Name: MyCustomFilter

☒ Filter Functions
- ☐ By Severity
- ☒ By Src Address
- ☐ By Dst Address
- ☐ By Signature Name
- ☐ By Sensor Name
- ☐ By UTC Time
- ☐ By Status

Alarm Source Address Set

○ Included ● Excluded

● Unique

IP Address: 10.0.1.6

○ Range

Start Address: End Address:

Excluded 10.0.1.1
Excluded 10.0.1.4
Excluded 10.0.1.6

- Add unique IP addresses.
- Add a range of IP addresses:
  - Start address
  - End address

You can specify a source IP address or a range of source IP addresses to be included or excluded when the filter is applied to a view. Complete the following steps to filter properties by the source address:

Step 1 Enable the source address function by selecting the **By Src Address** check box from the Filter Functions options. The Alarm Source Address Set information is displayed. Notice the Filter Functions check box is enabled.

Step 2 Add the source address sets to the filter:

1. Select either the **Included** or **Excluded** radio button.

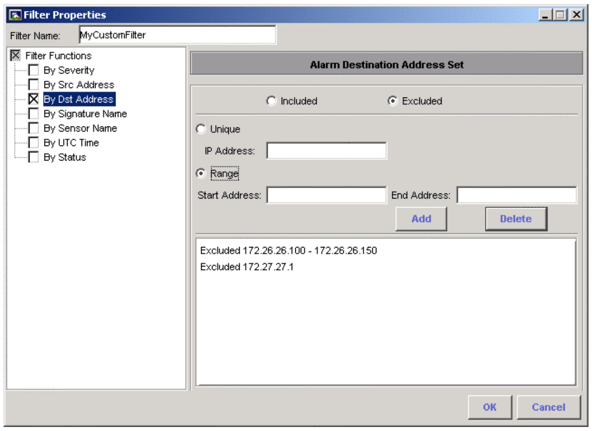
2. Select either the **Unique** or **Range** radio button.

3. If you selected the Unique radio button, enter an IP address in the IP Address field and click **Add**.

4. If you selected the Range radio button, enter the beginning IP address of the IP address range in the Start Address field, enter the ending IP address of the IP address range in the End Address field, and click **Add**.

Step 3 Click **OK** to save the filter settings.

Filter Properties— By Destination Address



Filter Properties

Filter Name: MyCustomFilter

- ☒ Filter Functions
  - □ By Severity
  - □ By Src Address
  - ☒ By Dst Address
  - □ By Signature Name
  - □ By Sensor Name
  - □ By UTC Time
  - □ By Status

Alarm Destination Address Set

○ Included ● Excluded

○ Unique

IP Address:

● Range

Start Address: End Address:

Excluded 172.26.26.100 - 172.26.26.150
Excluded 172.27.27.1

- Add unique IP addresses.
- Add a range of IP addresses:
  - Start address
  - End address

You can specify a destination IP address or a range of destination IP addresses to be included or excluded when the filter is applied to a view. Complete the following steps to filter properties by destination addresses:

Step 1 Enable the destination address function by selecting the **By Dst Address** check box from the Filter Functions options. The Excluded Alarm Destination Address Set information is displayed. Notice the Filter Functions check box is enabled.

Step 2 Add the destination address sets to the filter:

1. Select either the **Included** or **Excluded** radio button.

2. Select either the **Unique** or **Range** radio buttons.

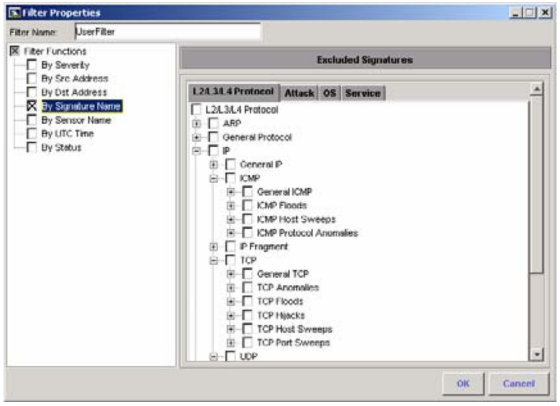
3. If you selected the Unique radio button, enter an IP address in the IP Address field and click **Add**.

4. If you selected the Range radio button, enter the beginning IP address of the IP address range in the Start Address field, enter the ending IP address of the IP address range in the End Address field, and click **Add**.

Step 3 Click **OK** to save the filter settings.

Filter Properties—By Signature Name

Cisco.com



Filter Properties

Filter Name: UserFilter

☒ Filter Functions
- ☐ By Severity
- ☐ By Src Address
- ☐ By Dst Address
- ☒ By Signature Name
- ☐ By Sensor Name
- ☐ By UTC Time
- ☐ By Status

Select a signature category or specific signatures to add in the filter.

Complete the following steps to add a signature category or specific signatures to include in the filter:

Step 1 Enable the signature name function by selecting the **By Signature Name** check box from the Filter Functions options. The Excluded Signatures information is displayed. Notice the Filter Functions check box is enabled.

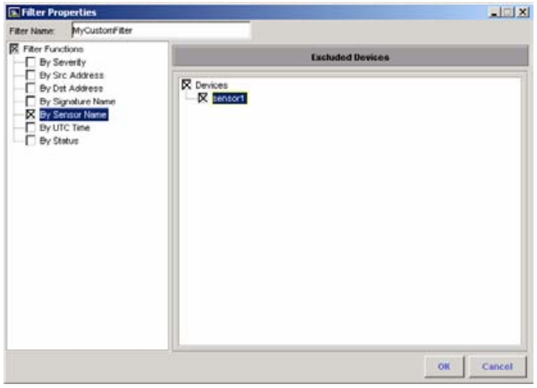
Step 2 Add the signature category or specific signature to the filter by selecting the appropriate check boxes.

Step 3 Click **OK** to save the filter settings.

Note The addition of a signature category or specific signature in a filter causes it to be excluded when the filter is applied to a view.

Filter Properties—By Sensor Name

Cisco.com



Filter Properties

Filter Name: MyCustomFilter

☒ Filter Functions
- ☐ By Severity
- ☐ By Src Address
- ☐ By Dst Address
- ☐ By Signature Name
- ☒ By Sensor Name
- ☐ By UTC Time
- ☐ By Status

Excluded Devices

☒ Devices
- ☒ sensor1

Select a Sensor to apply to the filter.

CSIDS 4.0—10-40

Complete the following steps to add a Sensor name to the filter:

Step 1 Enable the sensor name function by selecting the **By Sensor Name** check box from the Filter Functions options. The Excluded Devices information is displayed. Notice the Filter Functions check box is enabled.

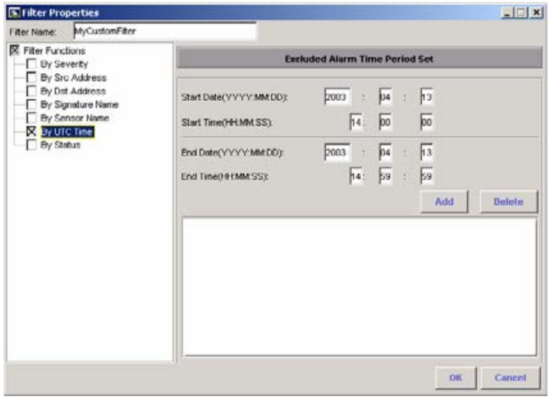
Step 2 Add the IDS devices to the filter by selecting the appropriate check boxes.

Step 3 Click **OK** to save the filter settings.

Note The addition of a Sensor in a filter causes it to be excluded when the filter is applied to a view.

Filter Properties—By Time

Cisco.com



Filter Name: MyCustomFilter

☒ Filter Functions
- ☐ By Severity
- ☐ By Src Address
- ☐ By Dst Address
- ☐ By Signature Name
- ☐ By Sensor Name
- ☒ By UTC Time
- ☐ By Status

Start Date(YYYY:MM:DD): 2003 : 04 : 13
Start Time(HH:MM:SS): 14 : 00 : 00
End Date(YYYY:MM:DD): 2003 : 04 : 13
End Time(HH:MM:SS): 14 : 59 : 59

Add an alarm time period to apply to the filter:

- **Start date and time**
- **End date and time**

CSIDS 4.0—10-41

Complete the following steps to add a date and time range to the filter:

Step 1 Enable the time function by selecting the **By UTC Time** check box from the Filter Functions options. The Excluded Alarm Time Period Set information is displayed. Notice the Filter Functions check box is enabled.

Step 2 Enter the start date and time in the appropriate fields.

Step 3 Enter the end date and time in the appropriate fields.

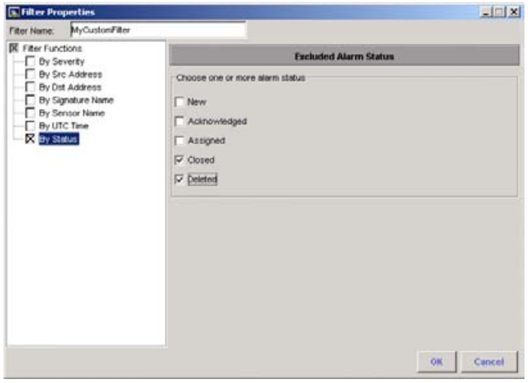
Step 4 Click **Add** to include the date and time range.

Step 5 Click **OK** to save the filter settings.

Note The addition of a time range in a filter causes it to be excluded when the filter is applied to a view.

Filter Properties—By Status

Cisco.com



Filter Name: MyCustomFilter

☒ Filter Functions
- □ By Severity
- □ By Src Address
- □ By Dst Address
- □ By Signature Name
- □ By Sensor Name
- □ By UTC Time
- ☒ By Status

Excluded Alarm Status

Choose one or more alarm status

- □ New
- □ Acknowledged
- □ Assigned
- ☑ Closed
- ☑ Deleted

Choose the status of alarms to include in the filter:

- **New**
- **Acknowledged**
- **Assigned**
- **Closed**
- **Deleted**

CSIDS 4.0—10-44

Complete the following steps to add an alarm status to the filter:

Step 1 Enable the alarm status function by selecting the **By Status** check box from the Filter Functions options. The Excluded Alarm Status information is displayed. Notice the Filter Functions check box is enabled.

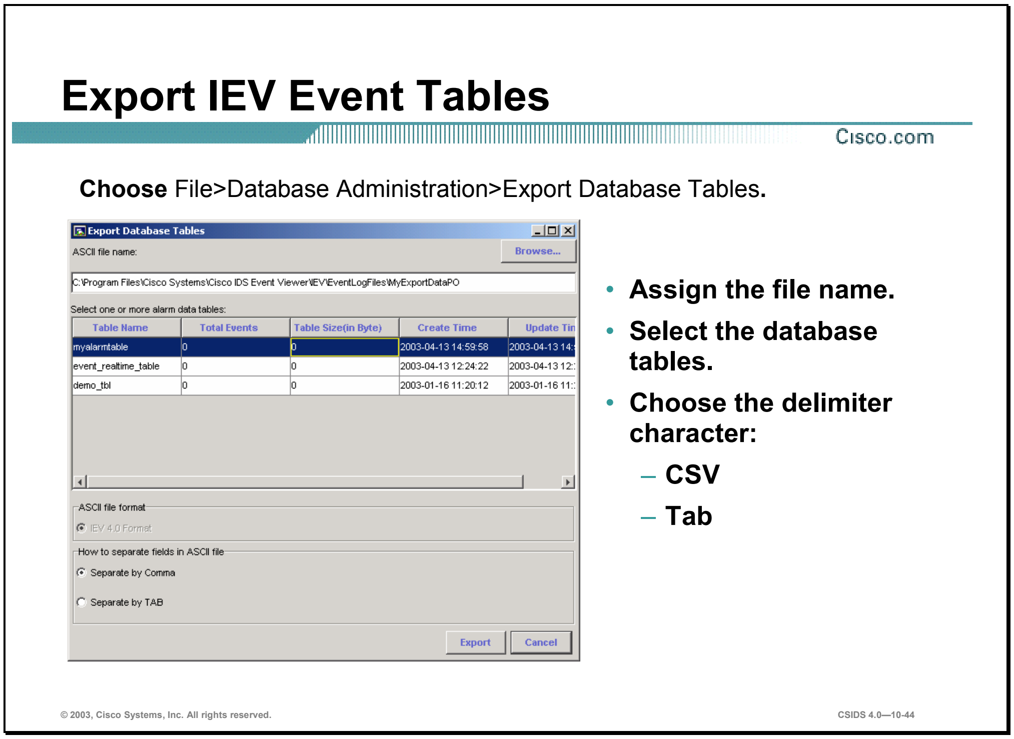
Step 2 Add an alarm status to the filter by selecting the appropriate check box within the Choose one or more alarm status group boxes.

Step 3 Click **OK** to save the filter settings.

Note The addition of an alarm status in a filter causes it to be excluded when the filter is applied to a view.

IDS Event Viewer Database Administration

This section discusses the IDS Event Viewer (IEV) database administration functions.



Export IEV Event Tables

Choose File>Database Administration>Export Database Tables.

Export Database Tables

ASCII file name:

C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\EventLogFiles\MyExportDataPO

Select one or more alarm data tables:

Table Name	Total Events	Table Size(in Byte)	Create Time	Update Tin
myalarmtable	0	0	2003-04-13 14:59:58	2003-04-13 14:
event_realtime_table	0	0	2003-04-13 12:24:22	2003-04-13 12::
demo_tbl	0	0	2003-01-16 11:20:12	2003-01-16 11::

ASCII file format

● IEV 4.0 Format

How to separate fields in ASCII file

● Separate by Comma

○ Separate by TAB

- **Assign the file name.**
- **Select the database tables.**
- **Choose the delimiter character:**
  - **CSV**
  - **Tab**

CSIDS 4.0—10-44

IEV has an export function that enables the network security administrator to export database event tables. Complete the following steps to export IDS event tables:

Step 1 Choose **File>Database Administration>Export Database Tables** from the main menu. The Export Database Tables window opens.

Step 2 Assign the destination file name where the data is to be exported by using the Browse button to locate the destination file.

Step 3 Select the database tables to export from the list of tables that exist in the database.

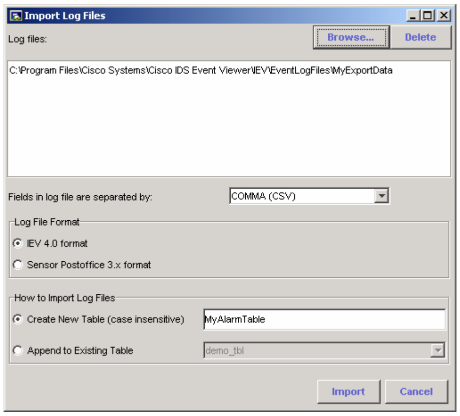
Step 4 Choose the delimiter character used when exporting the data, by selecting either **Separate by Comma** or **Separate by TAB**.

Step 5 Click **Export** to export the data to the specified table.

Import IDS Log Files

Cisco.com

Choose File>Database Administration>Import Log Files.



Import Log Files

Log files:

C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\IEV\EventLogFiles\MyExportData

Fields in log file are separated by: COMMA (CSV)

Log File Format

● IEV 4.0 format

○ Sensor Postoffice 3.x format

How to Import Log Files

● Create New Table (case insensitive) MyAlarmTable

○ Append to Existing Table demo_tbl

- **Select the log files to import into the database.**
- **Select the log file format.**
- **Import the logs into a new database table.**

or

- **Import the log files into an existing database table.**

IEV has an import function that enables a network security administrator to import archived IDS log files. The files can be in either Comma Separated (CSV) or tab-delimited format. Complete the following steps to import IDS log files into the IEV database:

Step 1 Choose **File>Database Administration>Import Log Files** from the main menu. The Import Log Files window opens.

Step 2 Select the IDS log files to import into the database by using the Browse button to locate your files. Multiple IDS log files may be specified. The log files are displayed in the Import Log Files field.

Step 3 Choose how fields in the log file are separated by selecting **COMMA (CSV)** or **TAB** from the Fields in log file are separated by drop-down menu.

Step 4 Choose the file format from the Log File Format group box.

Step 5 Choose how to import the log files by completing either of the following:

1. Select the **Create New Table** radio button, and enter a database table name in the corresponding field.

2. Select the **Append to Existing Table** radio button, and choose the name of an existing table to be appended.

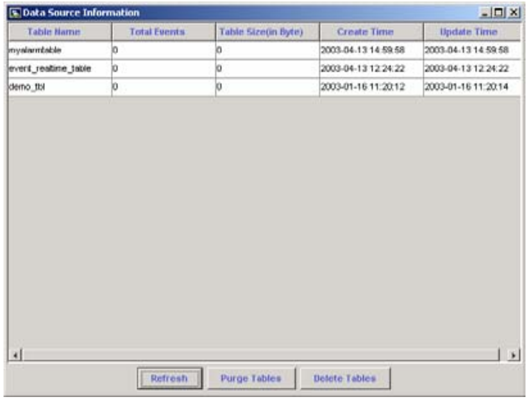
Step 6 Click **Import** to import the IDS log files into the IEV database.

Note The import function applies only to 3.x Sensors but may be useful if you are migrating from 3.x to 4.0 software. Log files with the Sensor PostOffice 3.x format are converted to IEV 4.0 format upon import.

Data Source Information

Cisco.com

Choose File>Database Administration>Data Source Information**.**



Data Source Information

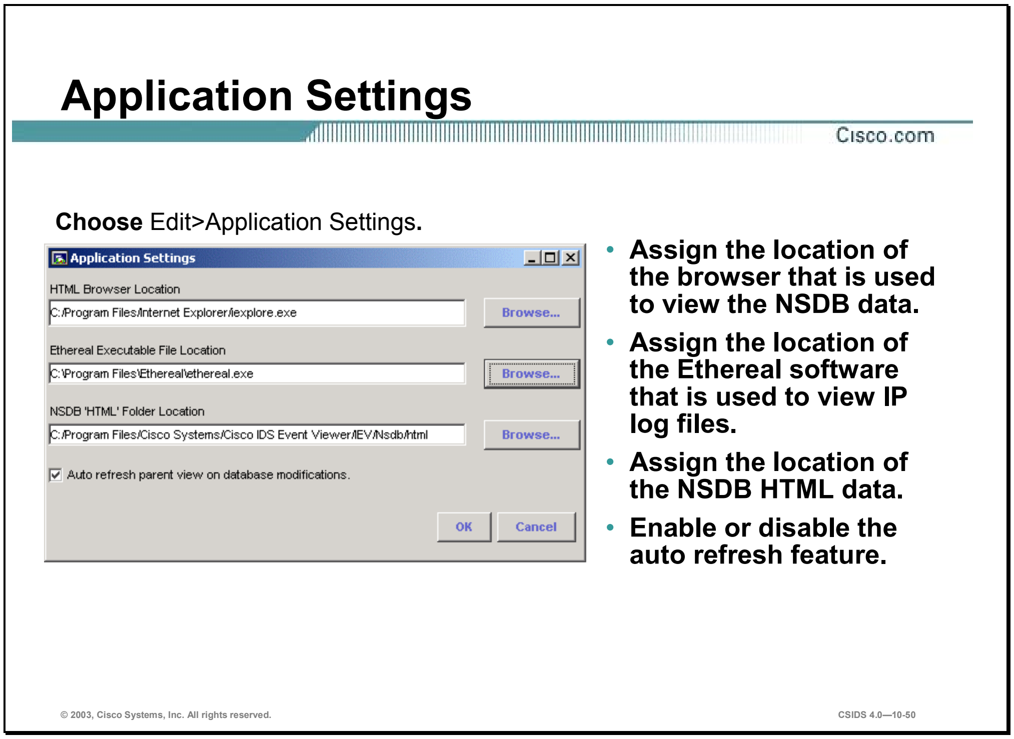
Table Name	Total Events	Table Size(in Byte)	Create Time	Update Time
myalarmtable	0	0	2003-04-13 14:59:58	2003-04-13 14:59:58
event_realtime_table	0	0	2003-04-13 12:24:22	2003-04-13 12:24:22
demo_tbl	0	0	2003-01-16 11:20:12	2003-01-16 11:20:14

- **This window lists the tables that exist in the database and table information, such as the following:**
  - **The name of the table**
  - **The total number of events**
  - **The table size (in Bytes)**
  - **The time the table was created**
  - **The time the table was updated**
- **Database tables can be purged or deleted.**

The IEV database administration utility provides the network security administrator with the information about the IEV database. To view the database information, choose **File>Database Administration>Data Source Information**. The Data Source Information window opens. The table names and detailed information for each table is listed. Purge and delete table functions are available that enable the network security administration to delete events from a table and delete the table from the database. IEV prompts you before a purge or delete action is allowed.

IDS Event Viewer Configuration

This section describes the IDS Event Viewer (IEV) configuration options.



Application Settings

Cisco.com

Choose Edit>Application Settings**.**

Application Settings

HTML Browser Location

C:/Program Files/Internet Explorer/iexplore.exe

Ethereal Executable File Location

C:\Program Files\Ethereal\ethereal.exe

NSDB 'HTML' Folder Location

C:/Program Files/Cisco Systems/Cisco IDS Event Viewer/IEV/Nsdb/html

☑ Auto refresh parent view on database modifications.

- **Assign the location of the browser that is used to view the NSDB data.**
- **Assign the location of the Ethereal software that is used to view IP log files.**
- **Assign the location of the NSDB HTML data.**
- **Enable or disable the auto refresh feature.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—10-50

During the installation of IEV, default IEV application settings are assigned. Complete the following steps to modify these settings:

Step 1 Choose **Edit>Application Settings** from the main menu. The Application Setting window opens.

Step 2 Assign the location of the HTML browser. The default system web browser is identified during the installation. If you want to assign the location of a different HTML browser, use the Browse button to locate the HTML browser.

Step 3 Assign the location of the Ethereal application used to view IP log files by using the Browse button.

Step 4 Enter the path, beginning with the drive letter, to the NSDB HTML folder in the NSDB HTML Folder Location field, or click **Browse** to locate the folder.

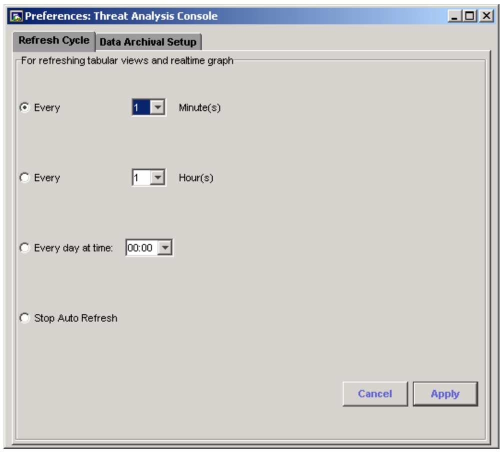
Step 5 Enable or disable the automatic refresh of a parent view on the database modifications feature by selecting or deselecting the **Auto refresh parent view on database modifications**.

Step 6 Click **OK** to save the IEV applications settings.

Preferences—Refresh Cycle

Cisco.com

Choose Edit>Preferences.



Preferences: Threat Analysis Console

For refreshing tabular views and realtime graph

● Every 1 Minute(s)

○ Every 1 Hour(s)

○ Every day at time: 00:00

○ Stop Auto Refresh

- **Choose the refresh interval for the IEV views:**
  - **Every *N* minutes**
  - **Every *N* hours**
  - **Every day at a specific time**
  - **Stop Auto Refresh**

The event views are refreshed periodically according to the parameters defined in the Refresh Cycle preferences. By default the refresh interval is every minute. Complete the following steps to modify the refresh interval:

Step 1 Choose **Edit>Preferences** from the main menu. The Preferences: Threat Analysis Console window opens.

Step 2 Select the **Refresh Cycle** tab in the Preferences window. The Refresh Cycle parameters are displayed.

Step 3 Choose a refresh interval. The interval options available are as follows:

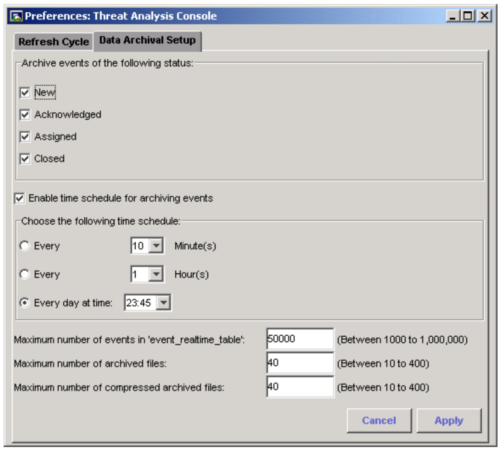
- Every *N* minutes—From the Minute(s) drop-down menu choose how many minutes until the next refresh occurs.
- Every *N* hours—From the Hour(s) drop-down menu choose how many hours until the next refresh occurs.
- Every day at time—From the Every day at time drop-down menu choose the specific time the refresh occurs every day.
- Stop Auto Refresh—Select the **Stop Auto Refresh** radio button to disable the automatic refresh feature.

Step 4 Click **Apply** to save the refresh cycle parameter settings.

Preferences—Data Archival Setup

Cisco.com

Choose Edit>Preferences**.**



Preferences: Threat Analysis Console

Archive events of the following status:

☑ New
☑ Acknowledged
☑ Assigned
☑ Closed

☑ Enable time schedule for archiving events

Choose the following time schedule:

○ Every 10 Minute(s)
○ Every 1 Hour(s)
● Every day at time: 23:45

Maximum number of events in 'event_realtime_table': 50000 (Between 1000 to 1,000,000)
Maximum number of archived files: 40 (Between 10 to 400)
Maximum number of compressed archived files: 40 (Between 10 to 400)

Assign the parameters used to determine the following:

- **Events to be archived**
- **Time events are archived**
- **Maximum number of**
  - **Events in the real-time database**
  - **Archived files**
  - **Compressed archived files**

CSIDS 4.0—10-52

The network security administrator can change the data archival parameters to meet the company's requirements. Complete the following steps to modify the data archival parameters:

Step 1 Choose **Edit>Preferences** from the main menu. The Preferences: Threat Analysis Console window opens.

Step 2 Select the **Data Archival Setup** tab in the Preferences: Threat Analysis Console window. The Data Archival Setup parameters are displayed.

Step 3 Select the status of the events to be archived by selecting the appropriate status from the Archive events of the following status group box.

Step 4 Enable or disable the time schedule for the archiving events feature by selecting or deselecting the **Enable time schedule for archiving events** check box.

Step 5 Choose the time schedule for data archival. The time schedule for the archiving events feature must be enabled. The time schedule options are as follows:

- Every *N* Minutes—From the Minute(s) drop-down menu choose how many minutes until the next data archival occurs.
- Every *N* Hour—From the Hour(s) drop-down menu choose how many hours until the next data archival occurs.
- Every day at time—From the Every day at time drop-down menu choose the specific time the data archival occurs every day.

Step 6 In the Maximum number of events in 'event_realtime_table' field, assign the maximum number of events to be recorded in the real-time database table.

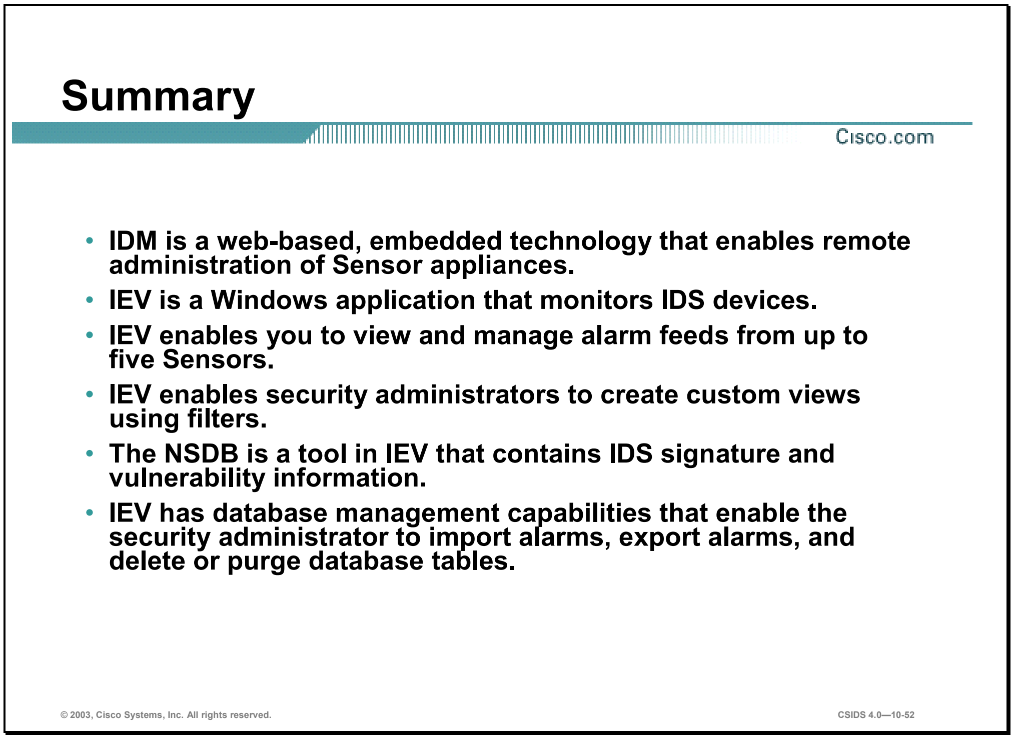
Step 7 In the Maximum number of archived files field, assign the maximum number of files to be archived.

Step 8 In the Maximum number of compressed archive files field, assign the maximum number of archived files to be compressed.

Step 9 Click **Apply** to save the data archival parameter settings.

Summary

This section summarizes what you have learned in this chapter.



Summary

Cisco.com

- IDM is a web-based, embedded technology that enables remote administration of Sensor appliances.
- IEV is a Windows application that monitors IDS devices.
- IEV enables you to view and manage alarm feeds from up to five Sensors.
- IEV enables security administrators to create custom views using filters.
- The NSDB is a tool in IEV that contains IDS signature and vulnerability information.
- IEV has database management capabilities that enable the security administrator to import alarms, export alarms, and delete or purge database tables.

CSIDS 4.0—10-52

Lab Exercise—Cisco IDS Event Viewer

Complete the following lab exercise to practice what you learned in this chapter.

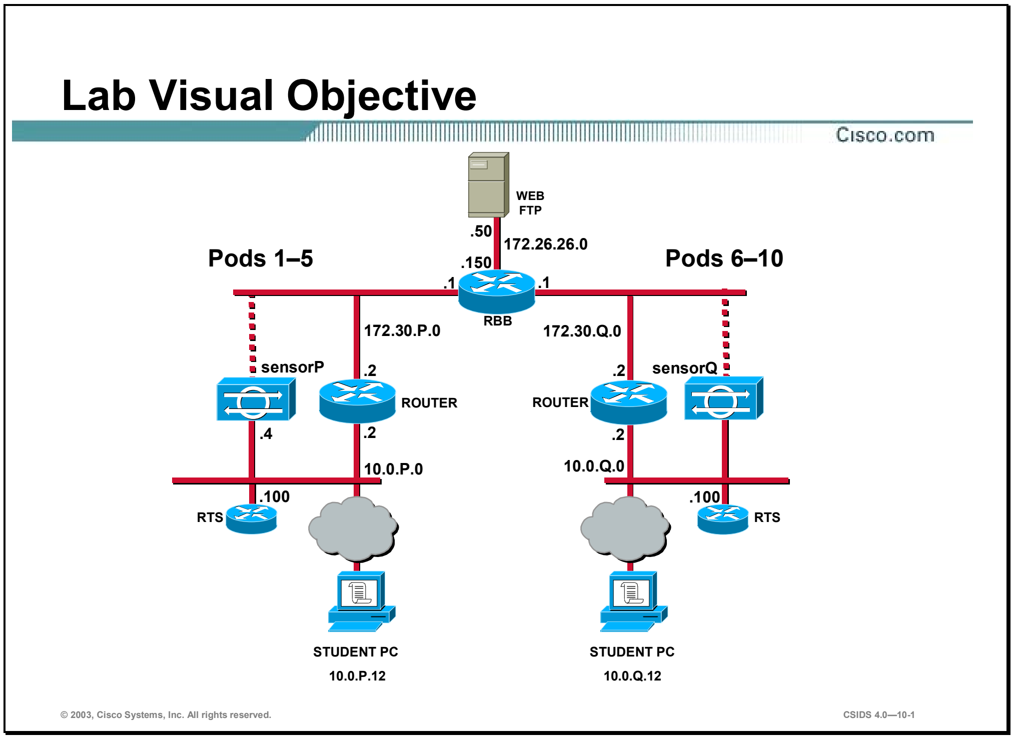
Objectives

In this lab exercise you will complete the following tasks:

- Access and navigate the IDS Device Manager (IDM).
- Install the IEV software on the student PC.
- Add the IDS devices to the list of devices monitored by the IEV.
- Monitor Cisco IDS events using the IEV.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab exercise.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor.

Setup

The Sensor should be initialized. Verify that your PC is able to ping the Sensor.

Task 1—Access and Navigate the IDM

Complete the following steps to access and navigate the IDM:

Step 1 Launch your web browser and specify the Sensor as the location. To do this, enter the following URL field in your web browser:

```
https://10.0.P.4
```

(where P = pod number)

Step 2 Click **Yes** when the Security Alert panel appears asking if you want to proceed.

Step 3 Log in to the IDM as user **admin**. The admin password is **adminpass**.

Step 4 Select **Device>Sensor Setup**.

Step 5 Select **Network** from the TOC. The network settings for your Sensor are displayed in the Network Settings group box.

Step 6 Select the **Configuration** tab and observe the configuration options that are available.

Step 7 Select the **Monitoring** tab and observe the options that are available.

Step 8 Select the **Administration** tab and observe the options that are available.

Task 2—Install the IEV Software on the Student PC

Complete the following steps to install the IEV software on your student PC:

Step 1 Locate and double-click the IDS Event Viewer executable to start the setup program. The Welcome panel of the IDS Event Viewer setup program opens.

Step 2 Click **Next** to proceed with the setup program. The Select Destination Location window opens.

Step 3 Click **Next** to accept the default location for the IDS Event Viewer files. The Select Program Manager Group window opens.

Step 4 Click **Next** to proceed with the setup program. The Start Installation window opens.

Step 5 Click **Next** to proceed with the setup program. The Installing window opens.

Step 6 Wait until the Installation Complete window opens.

Step 7 Click **Finish** to complete the IDS Event Viewer setup program. The Install popup window opens.

Step 8 Click **OK** to reboot the host.

Task 3—Add the IDS Devices to the List of Devices Monitored by the IEV

Complete the following steps to add the IDS devices to the list of devices monitored by the IEV:

Step 1 Launch IEV by selecting **Start>Programs>Cisco Systems>Cisco IDS Event Viewer>Cisco IDS Event Viewer**.

Step 2 Select **File>New>Device** from the IDS Event Viewer main menu. The Device Properties window opens.

Step 3 Enter the information the Device Properties window requires by completing the following sub-steps:

1. Enter your Sensor IP address, **10.0.P.4**, in the Sensor IP Address field.
   (where P = pod number)

2. Enter **sensorP** in the Sensor Name field.
   (where P = pod number)

3. Enter **oper** in the User Name field.

4. Enter **operpass** in the Password field.

5. Leave the default web server port (**443)** in the Web Server Port field.

6. Verify that the **Use encrypted connection (https)** radio button is selected in the Choose the communication protocol group box. The Use encrypted connection (https) is selected by default.

7. Verify that the **Latest Alerts** check box is selected within the Event Start Time (UTC) group box. The Latest Alerts check box is selected by default.

8. Click **OK** to close the Device Properties panel. The Certificate Information window opens.

9. Click **Yes** to accept the certificate. Your Sensor appears in the Devices folder on the left side of the screen.

Task 4—Monitor Cisco IDS Events Using the IEV

Complete the following steps to monitor Cisco IDS events using the IEV:

Step 1 Select **Tools>Realtime Dashboard>Launch Dashboard**. The IDS Event Viewer opens a subscription request with the Sensor.

Step 2 Minimize the Realtime Dashboard.

Step 3 Generate IDS events by completing the following sub-steps:

1. Enter the following URL in your browser to trigger the WWW IIS Showcode.asp Access signature:

```
http://target_ip_address/msadc/samples/selector/showcode.asp
```

(where target_ip_address = target IP address assigned by your instructor)

2. Enter the following URL in your browser to trigger the WWW IIS Unicode Attack signature:

```
http://target_ip_address/scripts/..%c0%af../winnt/system32
```

(where target_ip_address = target IP address assigned by your instructor)

3. Enter the following URL in your browser to trigger the WWW WinNT cmd.exe signature:

```
http://target_ip_address/scripts/..%35c../winnt/system32/cmd.exe?/c+dir
```

(where target_ip_address = target IP address assigned by your instructor)

Step 4 Generate more events by completing the following sub-steps to discover the version of IIS on your peer pod's student PC:

1. Open another Windows command prompt and telnet to port 80 on your peer pod's student PC:

```
C:\> telnet 10.0.Q.12 80
```

(where Q = peer pod number)

2. Enter the GET phf? command:

```
GET phf?
```

Note You will not see a prompt in the command prompt window.

Step 5 Maximize the Realtime Dashboard and observe the events displayed. The Realtime Dashboard displays the most recent events received by the Sensor since the request was opened.

Step 6 Close the Realtime Dashboard.

Step 7 Double-click the **Sig Name Group** view from the Views folder. The Sig Name Group View is displayed in the right pane.

Step 8 Right-click a cell in the first column in an alarm aggregation table associated with the event you want to expand, and select **Expand Whole Details**. The Expanded Details Dialog window opens with the Whole Address panel displayed.

Step 9 Right-click the alarm in the Expanded Details Dialog window and choose **View Alarms**. The Alarm Information Dialog window opens.

Step 10 Right-click a column heading and choose **Show All Columns** from the drop-down menu to display all the data associated with the alarm.

Step 11 Right-click the alarm and choose **Show Context** from the drop-down menu to view the context data associated with the alarm. The Decode Alarm Context window opens and displays the context data.

Step 12 Close the Decode Alarm Context window.

Step 13 Close the Alarm Information Dialog window.

11

Enterprise Intrusion Detection System Management

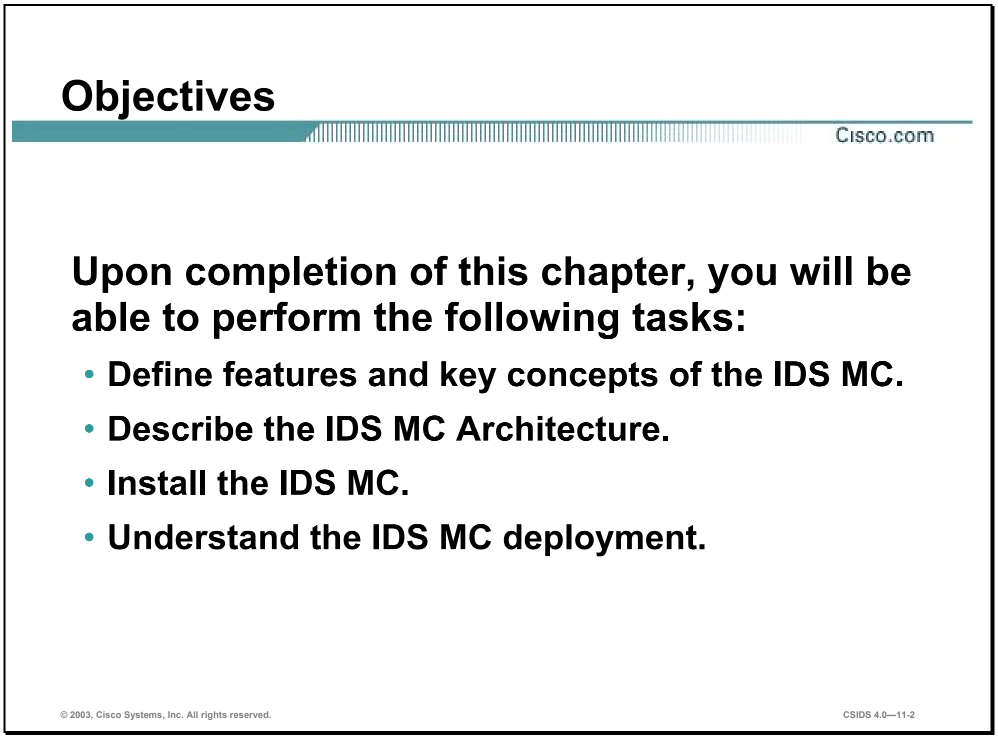
Overview

This chapter introduces the Management Center for Intrusion Detection System (IDS) Sensors (IDS MC) application to manage configurations for Cisco IDS Sensors in an enterprise network. IDS MC is a component of the CiscoWorks2000 (CiscoWorks) Virtual Private Network (VPN)/Security Management Solution (VMS) bundle. The following topics are covered in this chapter:

- Objectives
- Introduction
- Windows installation
- Solaris installation
- Architecture
- Getting started
- IDS MC Workflow
- Summary
- Lab exercise

Objectives

This section lists the chapter objectives.



Objectives

Cisco.com

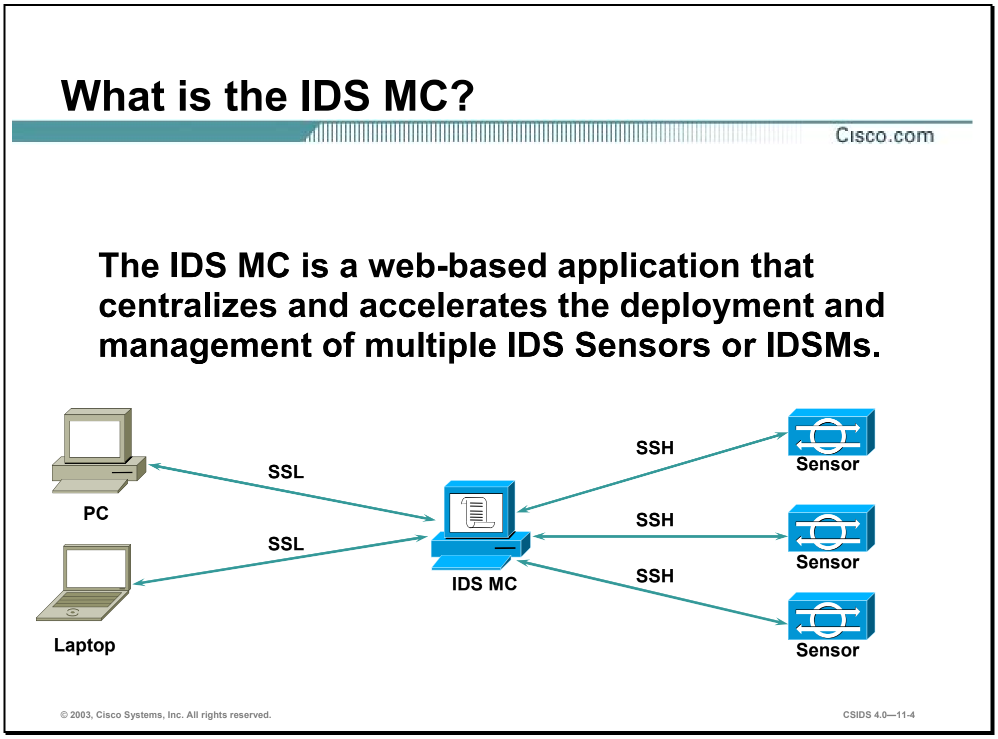
Upon completion of this chapter, you will be able to perform the following tasks:

- Define features and key concepts of the IDS MC.
- Describe the IDS MC Architecture.
- Install the IDS MC.
- Understand the IDS MC deployment.

CSIDS 4.0—11-2

Introduction

This section introduces the IDS MC.



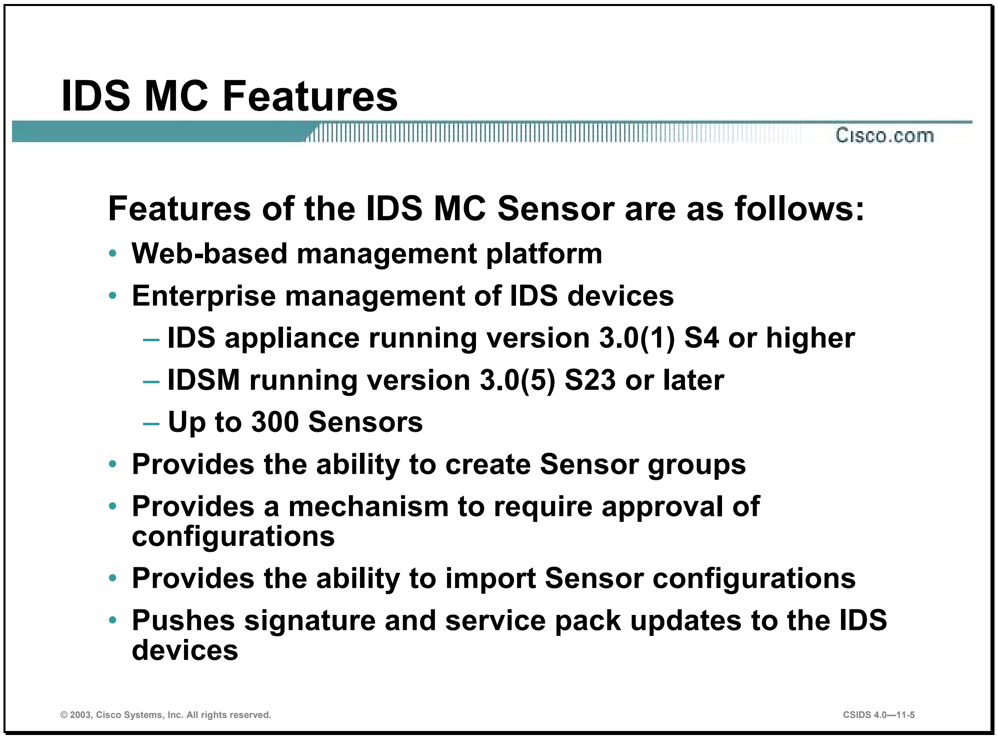
What is the IDS MC?

Cisco.com

The IDS MC is a web-based application that centralizes and accelerates the deployment and management of multiple IDS Sensors or IDSMs.

CSIDS 4.0—11-4

IDS MC is a component of the VMS bundle. The VMS bundle integrates the CiscoWorks Server with a number of individual applications such as VPN Monitor, Management Centers (MCs), and the Monitoring Center for Security to provide a comprehensive suite of security management tools. Through the CiscoWorks Common Services component, the IDS MC provides a web-based interface for configuring and managing a Sensor or Sensor Group.



IDS MC Features

Features of the IDS MC Sensor are as follows:

- Web-based management platform
- Enterprise management of IDS devices
  - IDS appliance running version 3.0(1) S4 or higher
  - IDSM running version 3.0(5) S23 or later
  - Up to 300 Sensors
- Provides the ability to create Sensor groups
- Provides a mechanism to require approval of configurations
- Provides the ability to import Sensor configurations
- Pushes signature and service pack updates to the IDS devices

CSIDS 4.0—11-5

Sensors are network devices that perform real-time monitoring of network traffic for suspicious activities and active network attacks. The IDS MC provides a web-based method to remotely manage and configure IDS Sensors.

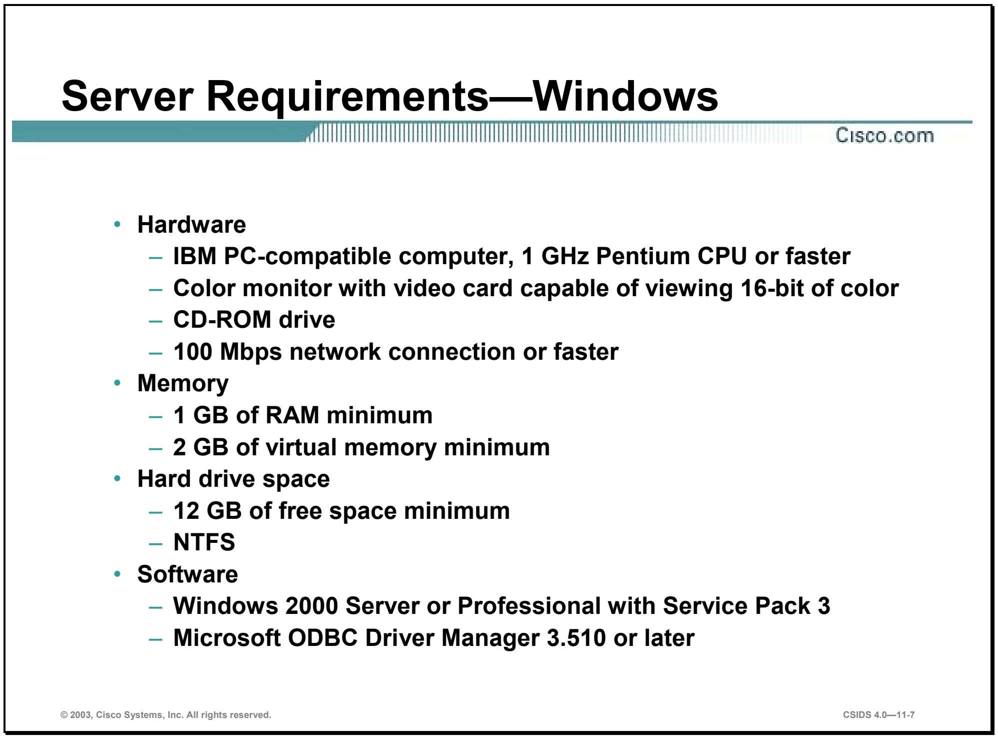
The IDS MC can manage the following types of Sensors:

- Sensor appliance—Requires software version 3.0(1) S4, 4.0, or higher
- IDS Module (IDSM)—Requires software version 3.0(5) S23 or higher

The IDS MC can manage configurations for up to 300 Sensors. You can manage individual Sensors, and groups of Sensors that have a common configuration. The IDS MC is built on the CiscoWorks framework, which enables the IDS MC to leverage the ability to define user roles. User roles define management privileges such as who can generate and deploy IDS configurations. The IDS MC can import Sensor configurations that have been configured by other IDS management tools. Additionally, the IDS MC enables you to push signature updates and Sensor software updates to Sensors or Sensor Groups.

Windows Installation

This section explains the server installation requirements, client access requirements, and provides an overview of the installation process for Windows-based machines.



Server Requirements—Windows

Cisco.com

- Hardware
  - IBM PC-compatible computer, 1 GHz Pentium CPU or faster
  - Color monitor with video card capable of viewing 16-bit of color
  - CD-ROM drive
  - 100 Mbps network connection or faster
- Memory
  - 1 GB of RAM minimum
  - 2 GB of virtual memory minimum
- Hard drive space
  - 12 GB of free space minimum
  - NTFS
- Software
  - Windows 2000 Server or Professional with Service Pack 3
  - Microsoft ODBC Driver Manager 3.510 or later

CSIDS 4.0—11-7

Before you begin, verify the Windows-based server on which you plan to install the IDS MC meets the following requirements:

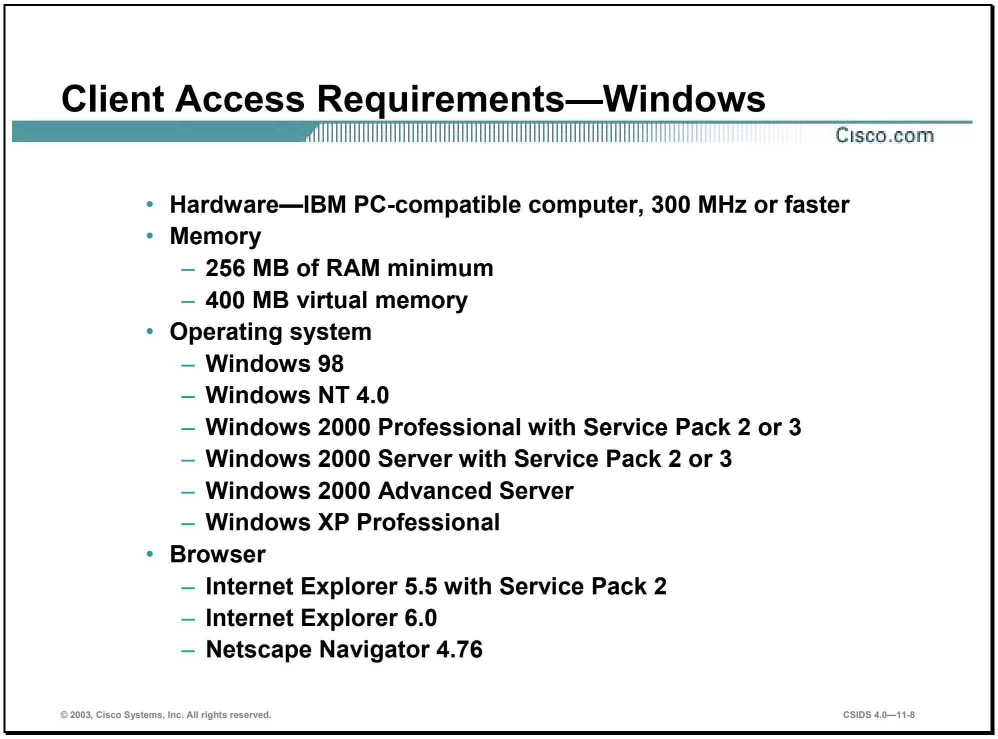
- Hardware
  - IBM PC-compatible computer, 1 GHz Pentium CPU or faster
  - Color monitor and video card capable of viewing 16-bit color
  - CD-ROM drive
  - 100 Mbps network connection or faster
- Memory
  - 1 GB of RAM minimum
  - 2 GB of virtual memory minimum
- Hard drive space

  - 12 GB minimum of free space formatted with the New Technology File System (NTFS)

- Software
  - Windows 2000 Server or Professional with Service Pack 3
  - Microsoft ODBC Driver Manager 3.510 or later

Note Single and multiprocessor systems are supported.

Note Do not attempt to install the IDS MC on a host on which the Cisco Secure Policy Manager (CSPM) has been installed.



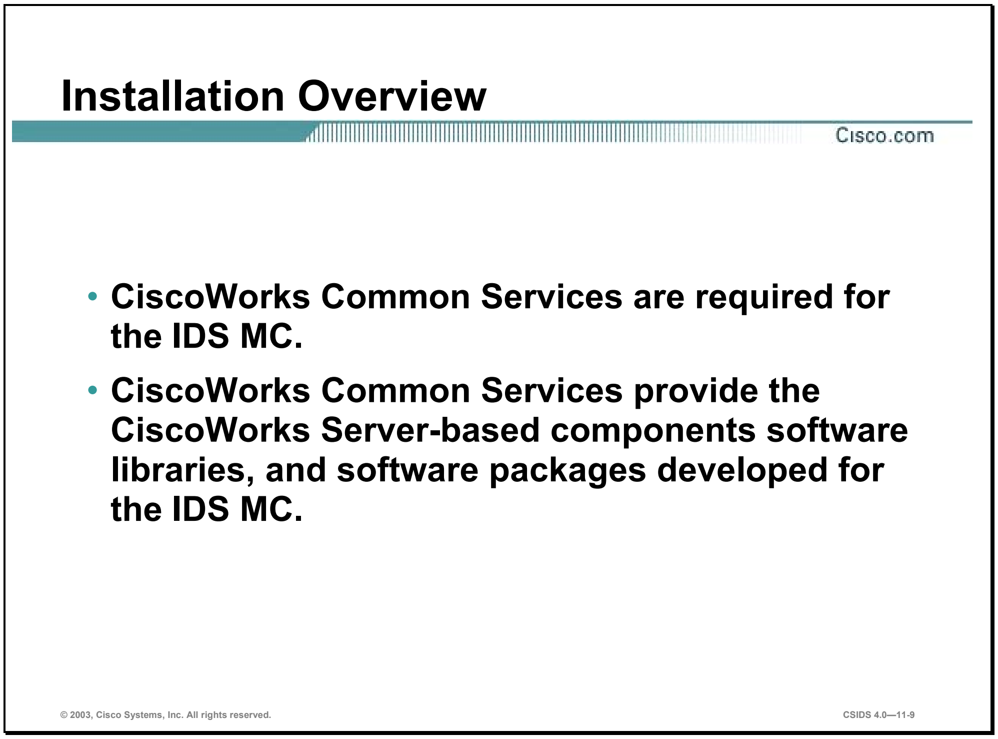
Client Access Requirements—Windows

- **Hardware—IBM PC-compatible computer, 300 MHz or faster**
- **Memory**
  - **256 MB of RAM minimum**
  - **400 MB virtual memory**
- **Operating system**
  - **Windows 98**
  - **Windows NT 4.0**
  - **Windows 2000 Professional with Service Pack 2 or 3**
  - **Windows 2000 Server with Service Pack 2 or 3**
  - **Windows 2000 Advanced Server**
  - **Windows XP Professional**
- **Browser**
  - **Internet Explorer 5.5 with Service Pack 2**
  - **Internet Explorer 6.0**
  - **Netscape Navigator 4.76**

CSIDS 4.0—11-8

Before you log in to the IDS MC, verify that the Windows-based client machine used to log in to the IDS MC meets the following requirements:

- Hardware—IBM PC-compatible computer, 300 MHz or faster
- Memory
  - 256 MB of RAM minimum
  - 400 MB of virtual memory minimum
- Operating system
  - Windows 98 and NT 4.0
  - Windows 2000 Server or Professional with Service Pack 3
  - Windows 2000 Advanced Server
- Browser
  - Microsoft Internet Explorer version 6.0 or 5.5 with Service Pack 2, and Java Virtual Machine (JVM) 5.00.3186 or later
  - Netscape Navigator 4.79 or later



Installation Overview

- CiscoWorks Common Services are required for the IDS MC.
- CiscoWorks Common Services provide the CiscoWorks Server-based components software libraries, and software packages developed for the IDS MC.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—11-9

CiscoWorks Common Services, a component of VMS, is required for the IDS MC. CiscoWorks Common Services provides the CiscoWorks2000 Server base components, software libraries, and software packages developed to support the IDS MC.

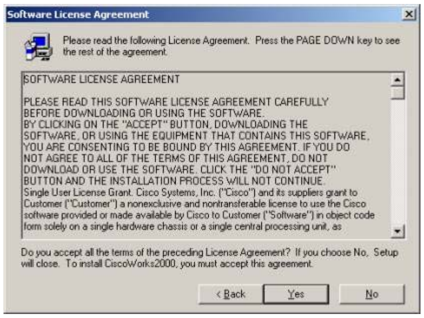
For more information on CiscoWorks Common Services, see the *Quick Start Guide for VPN Security Management Solution* or *Installing VMS Common Services on Windows 2000*.

Note CiscoWorks Common Services should not be installed on a Windows platform that is also serving as a primary domain controller (PDC), a backup domain controller (BDC), or if terminal services are running.

Note CiscoWorks Common Services may be installed on a standalone server, without CD One, or integrated into an existing CiscoWorks installation running CD One 5th Edition. If CD One is required to support other VMS components such as the Resource Manager Essentials (RME), then CD One must be installed before CiscoWorks Common Services can be installed.

Installation Process

Cisco.com



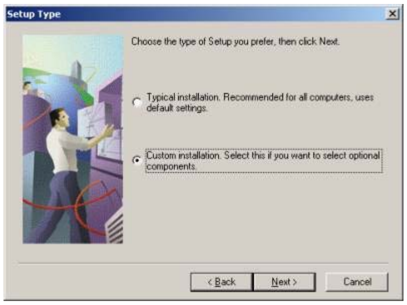
Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE.
BY CLICKING ON THE "ACCEPT" BUTTON, DOWNLOADING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT DOWNLOAD OR USE THE SOFTWARE. CLICK THE "DO NOT ACCEPT" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE.
Single User License Grant. Cisco Systems, Inc. ("Cisco") and its suppliers grant to Customer ("Customer") a nonexclusive and nontransferable license to use the Cisco software provided or made available by Cisco to Customer ("Software") in object code form solely on a single hardware chassis or a single central processing unit, as

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install CiscoWorks2000, you must accept this agreement.



Setup Type

Choose the type of Setup you prefer, then click Next.

○ Typical installation. Recommended for all computers, uses default settings.

● Custom installation. Select this if you want to select optional components.

CSIDS 4.0—11-10

Complete the following steps to install the IDS MC:

Note The typical installation installs both the IDS MC and the Monitoring Center for Security. Installation of the Monitoring Center for Security is discussed in a later chapter.

Step 1 Launch the IDS MC installation. The Welcome window opens.

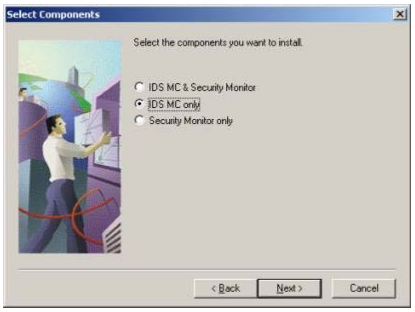
Step 2 Click **Next**. The Software License Agreement window opens.

Step 3 If you agree to the Software License Agreement, click **Yes** to proceed. The Setup Type window opens. If you click **No**, the installation process stops.

Step 4 Select **Custom Installation** as the installation type and click **Next**. The Select Components window opens.

Note If you select Typical Installation, the IDS MC and the Monitoring Center for Security will be installed on the same machine.

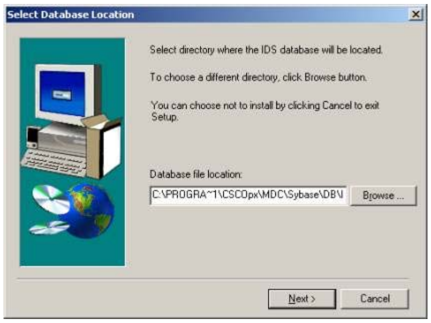
Installation Process (cont.)



Select Components

Select the components you want to install.

○ IDS MC & Security Monitor
● IDS MC only
○ Security Monitor only



Select Database Location

Select directory where the IDS database will be located.

To choose a different directory, click Browse button.

You can choose not to install by clicking Cancel to exit Setup.

Database file location: C:\PROGRA~1\CSCOpx\MDC\Sybase\DB\

CSIDS 4.0—11-11

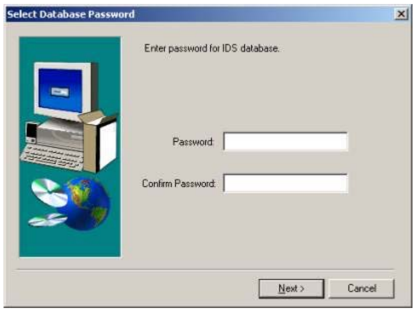
Step 5 Select **IDS MC only** and click **Next**. The Verification window opens.

Step 6 Click **Next**. The Select Database Location window opens.

Step 7 The default database location is within the directory where the CiscoWorks Common Services are installed. Click **Next** to accept the default directory. The Select Database Password window opens.

Installation Process (cont.)

Cisco.com

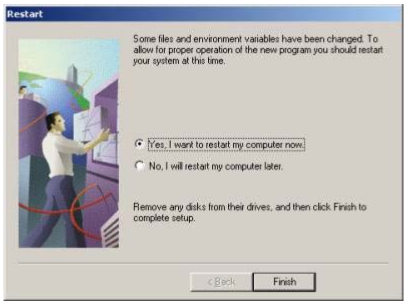


Select Database Password

Enter password for IDS database.

Password:

Confirm Password:



Restart

Some files and environment variables have been changed. To allow for proper operation of the new program you should restart your system at this time.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

CSIDS 4.0—11-12

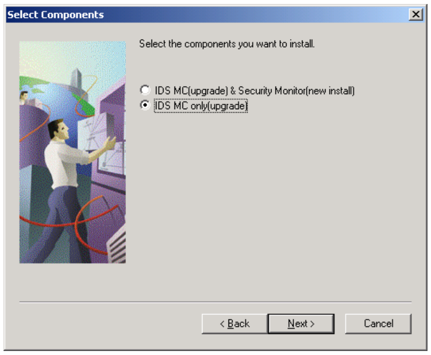
Step 8 Enter a password to secure the Sybase SQL database used by the IDS MC to store information about Sensors. Type the password again to confirm it and click **Next**. The Restart window opens.

Note The IDS MC database password must be at least 4 characters in length. If you do not enter a password of at least 4 characters in length, you will receive a pop-up error message that indicates you must enter a password of the necessary length.

Step 9 Select **Yes, I want to restart my computer now** to finish the installation.

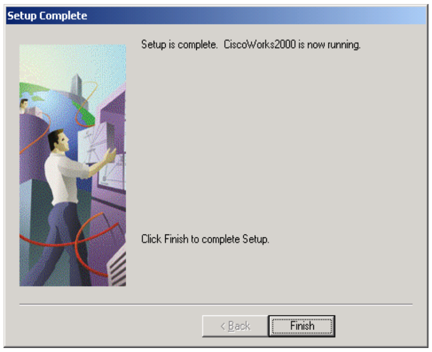
Upgrade Process

Cisco.com


Select Components

Select the components you want to install.

○ IDS MC(upgrade) & Security Monitor(new install)
● IDS MC only(upgrade)


Setup Complete

Setup is complete. CiscoWorks2000 is now running.

Click Finish to complete Setup.

CSIDS 4.0—11-13

Complete the following steps to upgrade from a previous version of the IDS MC:

Step 1 Launch the IDS MC installation. The Welcome window opens.

Step 2 Click **Next**. The Software License Agreement window opens.

Step 3 If you agree to the Software License Agreement, click **Yes** to proceed. The Setup Type window opens. If you click **No**, the installation process stops.

Step 4 Select **Custom Installation** as the installation type and click **Next**. The Select Components window opens.

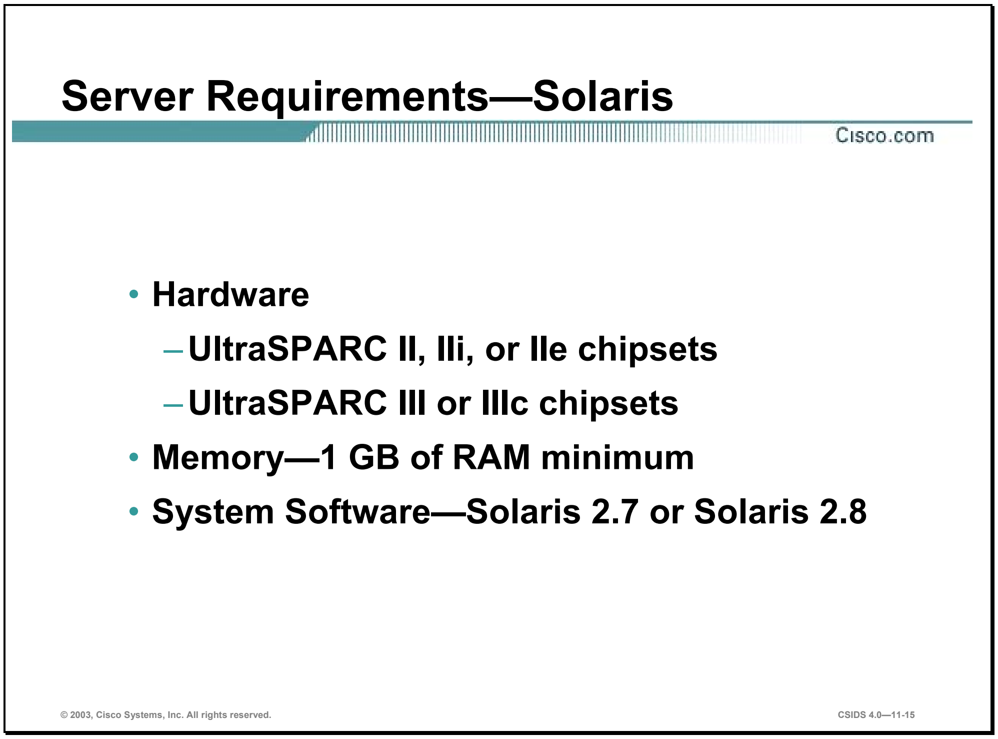
Step 5 Select **IDS MC only(upgrade)** and click **Next**. The Verification window opens.

Step 6 Verify the components that you are installing or upgrading and click **Next**. After upgrading the IDS MC, the Setup Complete window opens.

Step 7 Click **Finish**. The IDS MC processes start.

Solaris Installation

This section explains the server installation requirements, client access requirements, a brief installation overview, and the installation process for Solaris-based machines.



Server Requirements—Solaris

Cisco.com

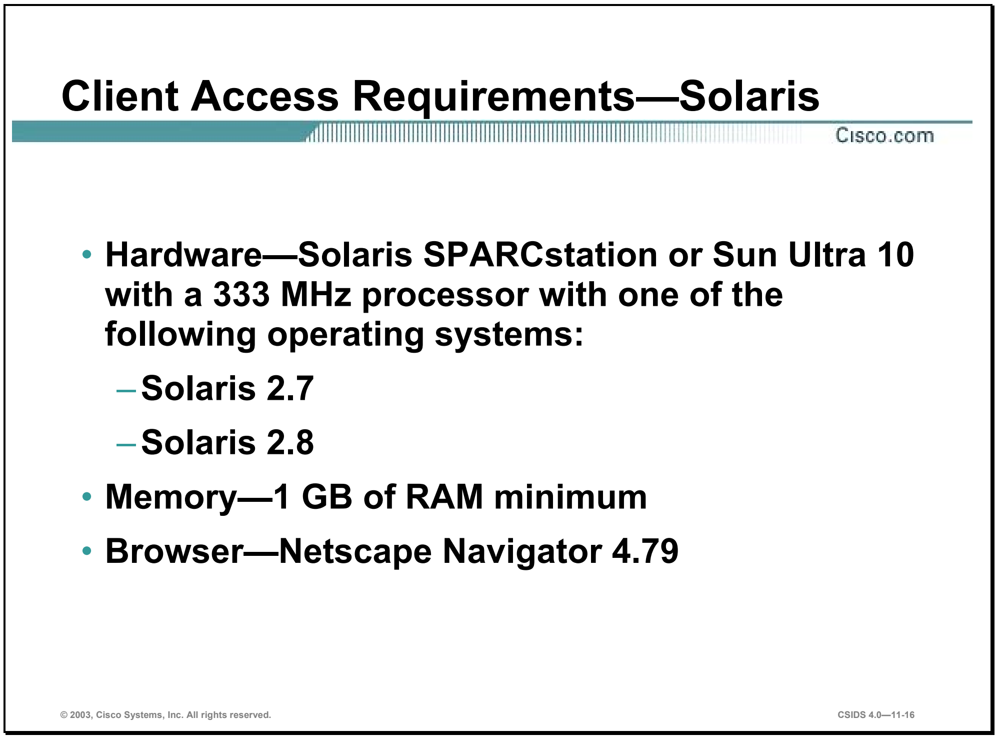
- Hardware
  - UltraSPARC II, IIi, or IIe chipsets
  - UltraSPARC III or IIIc chipsets
- Memory—1 GB of RAM minimum
- System Software—Solaris 2.7 or Solaris 2.8

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—11-15

Before you begin, verify the Solaris-based server on which you plan to install the IDS MC meets the following requirements:

- Hardware
  - UltraSPARC II, Iii, or IIe chipsets
  - UltraSPARC III or IIIc chipsets
- Memory
  - 1 GB of RAM minimum
  - 2 GB of swap space minimum
- Hard Drive Space—512 MB swap space
- System Software—Solaris 2.7 or Solaris 2.8



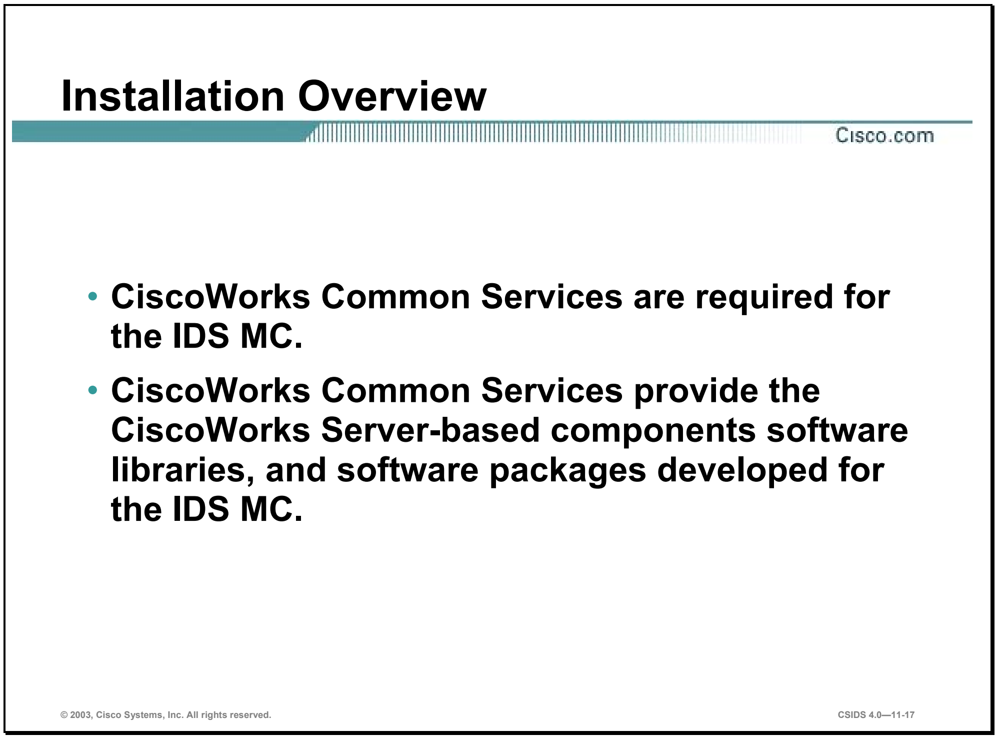
Client Access Requirements—Solaris

- Hardware—Solaris SPARCstation or Sun Ultra 10 with a 333 MHz processor with one of the following operating systems:
  - Solaris 2.7
  - Solaris 2.8
- Memory—1 GB of RAM minimum
- Browser—Netscape Navigator 4.79

CSIDS 4.0—11-16

Before you log in to the IDS MC, verify that the Solaris-based client machine used to log in to the IDS MC meets the following requirements:

- Hardware—Solaris SPARCstation or Sun Ultra 10 with a 333 MHz processor or better
- Operating System
  - Solaris 2.7
  - Solaris 2.8
- Memory
  - 1 GB of RAM minimum
  - 512 MB swap space minimum
- Browser—Netscape Navigator 4.76



Installation Overview

Cisco.com

- CiscoWorks Common Services are required for the IDS MC.
- CiscoWorks Common Services provide the CiscoWorks Server-based components software libraries, and software packages developed for the IDS MC.

© 2003, Cisco Systems, Inc. All rights reserved.

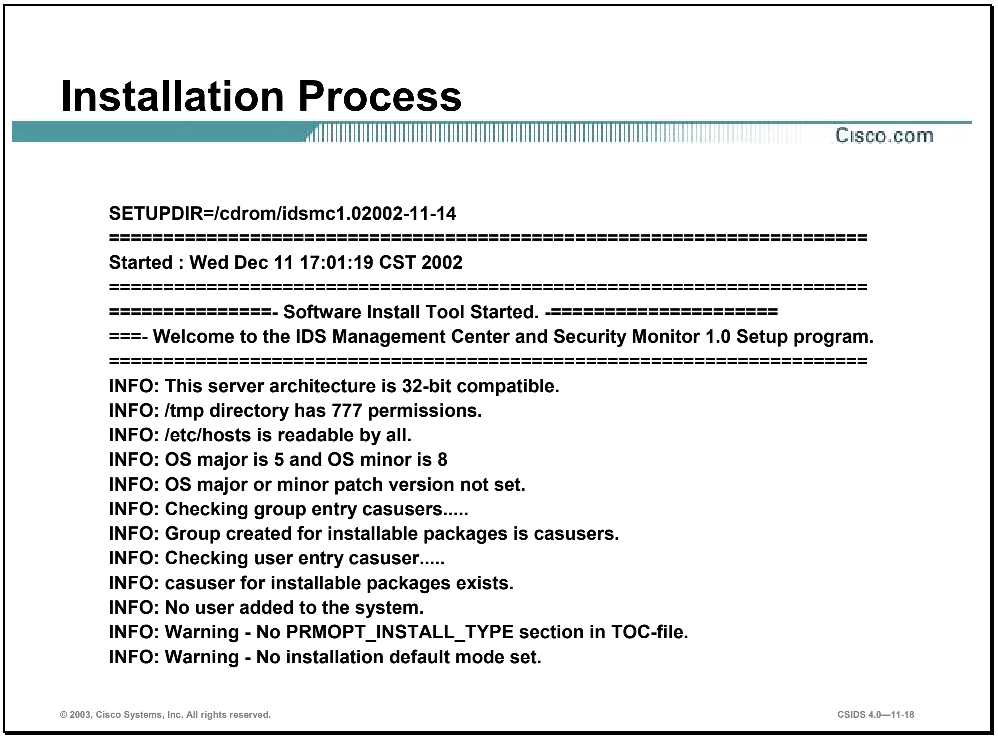
CSIDS 4.0—11-17

CiscoWorks Common Services, a component of VMS, is required for the IDS MC. CiscoWorks Common Services provides the CiscoWorks2000 Server-based components, software libraries, and software packages developed to support the IDS MC.

For more information on CiscoWorks Common Services, see the *Quick Start Guide for VPN Security Management Solution* or *Installing VMS Common Services on Windows 2000*.

Note CiscoWorks Common Services should not be installed on a Windows platform that is also serving as a PDC, BDC, or if terminal services are running.

Note CiscoWorks Common Services may be installed on a standalone server (without CD One), or integrated into an existing CiscoWorks installation running CD One 5th Edition. If CD One is required to support other VMS components such as Resource Manager Essentials (RME), then CD One *must* be installed before CiscoWorks Common Services.



Installation Process

```
SETUPDIR=/cdrom/idsmc1.02002-11-14
================================================================
Started : Wed Dec 11 17:01:19 CST 2002
================================================================
===============- Software Install Tool Started. -=====================
===- Welcome to the IDS Management Center and Security Monitor 1.0 Setup program.
================================================================
INFO: This server architecture is 32-bit compatible.
INFO: /tmp directory has 777 permissions.
INFO: /etc/hosts is readable by all.
INFO: OS major is 5 and OS minor is 8
INFO: OS major or minor patch version not set.
INFO: Checking group entry casusers.....
INFO: Group created for installable packages is casusers.
INFO: Checking user entry casuser.....
INFO: casuser for installable packages exists.
INFO: No user added to the system.
INFO: Warning - No PRMOPT_INSTALL_TYPE section in TOC-file.
INFO: Warning - No installation default mode set.
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—11-18

Complete the following steps to install the IDS MC:

Note The typical installation installs both the IDS MC and the Monitoring Center for Security. Installation of the Monitoring Center for Security is discussed in a later chapter.

Step 1 Insert the IDS MC for Solaris CD into the CD-ROM drive.

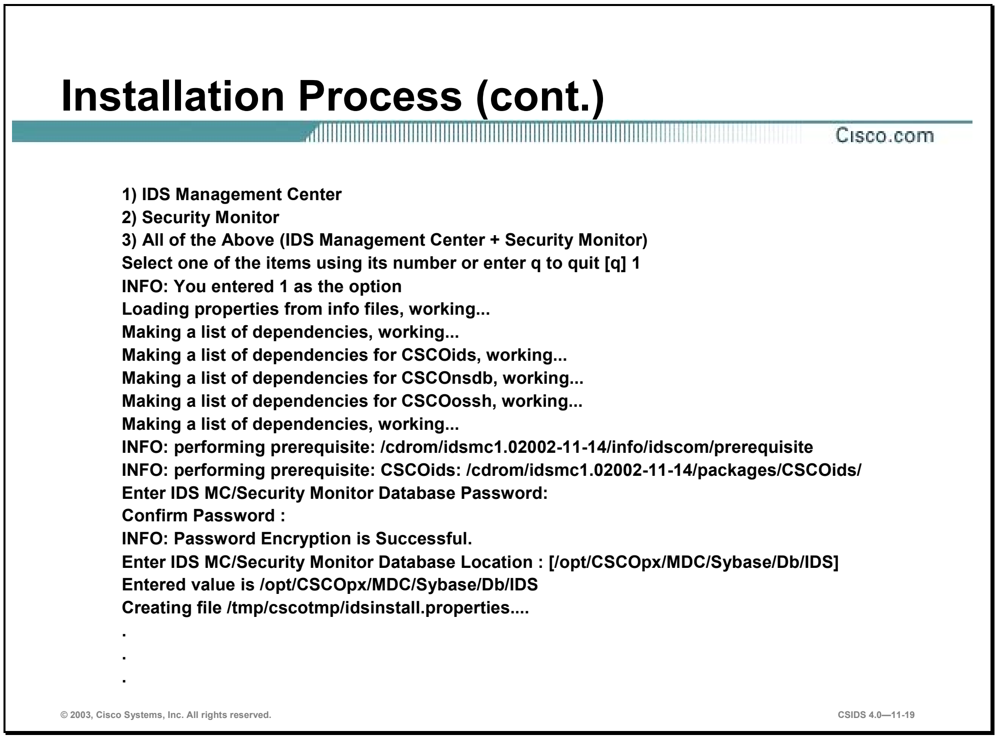
Step 2 Log into the server with an account with root level permissions.

Step 3 Locate **setup.sh** using the File Manager.

Step 4 Double-click **setup.sh** to launch the installation process. The Software Install Tool runs in a new window.

Step 5 After the Software Install Tool checks the operating system version and patches, it will prompt you to choose an installation package.

Note Be aware that the Software Install Tool must stop processes and services running in the background. It may take up to 10 minutes before you can proceed to the next step.



Installation Process (cont.)

Cisco.com

```
1) IDS Management Center
2) Security Monitor
3) All of the Above (IDS Management Center + Security Monitor)
Select one of the items using its number or enter q to quit [q] 1
INFO: You entered 1 as the option
Loading properties from info files, working...
Making a list of dependencies, working...
Making a list of dependencies for CSCOids, working...
Making a list of dependencies for CSCOnsdb, working...
Making a list of dependencies for CSCOossh, working...
Making a list of dependencies, working...
INFO: performing prerequisite: /cdrom/idsmc1.02002-11-14/info/idscom/prerequisite
INFO: performing prerequisite: CSCOids: /cdrom/idsmc1.02002-11-14/packages/CSCOids/
Enter IDS MC/Security Monitor Database Password:
Confirm Password :
INFO: Password Encryption is Successful.
Enter IDS MC/Security Monitor Database Location : [/opt/CSCOpx/MDC/Sybase/Db/IDS]
Entered value is /opt/CSCOpx/MDC/Sybase/Db/IDS
Creating file /tmp/cscotmp/idsinstall.properties....
.
.
.
```

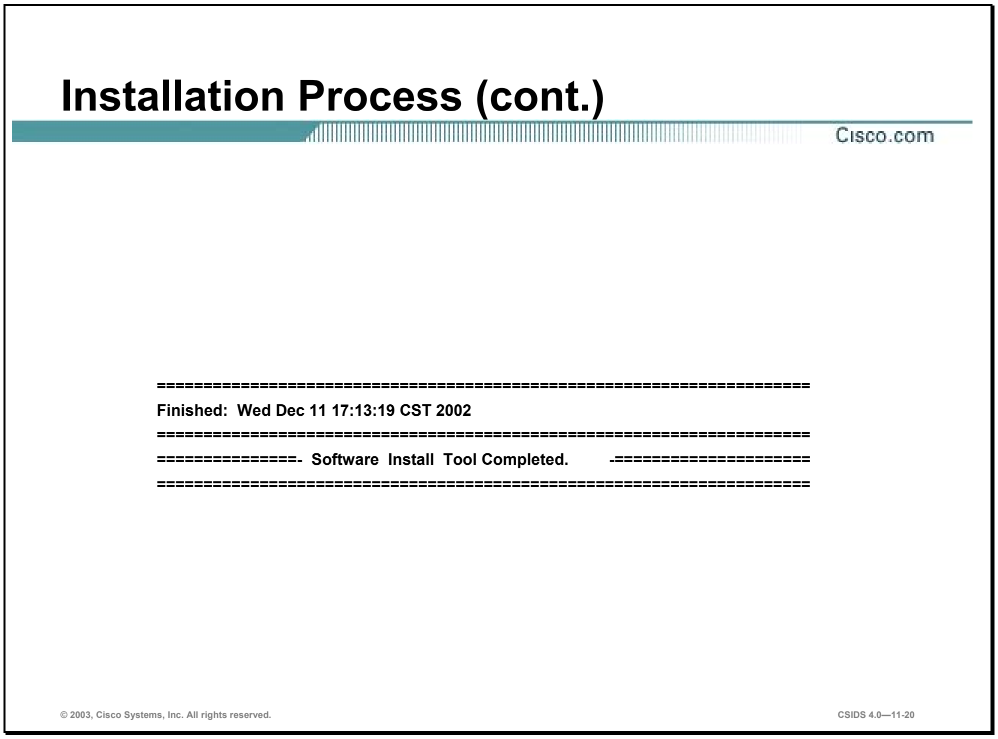
CSIDS 4.0—11-19

Step 6 Enter **1** and press **Enter**. After making a list of dependencies and performing prerequisite checks, you will be prompted to enter an IDS MC Database password.

Step 7 Enter a password to secure the Sybase SQL database used by the IDS MC to store information about Sensors. Type the password again to confirm it and press **Enter**. The Software Install Tool will prompt you to enter a database path.

Step 8 Press **Enter** to accept the default IDS MC database path: **/opt/CSCOpx/MDC/Sybase/Db/IDS**. The Software Install Tool installs the IDS MC and it components.

Note During the course of the IDS MC Solaris installation, you will receive a number of messages that indicate a portion of the installation was successful. Ignore these messages.



Installation Process (cont.)

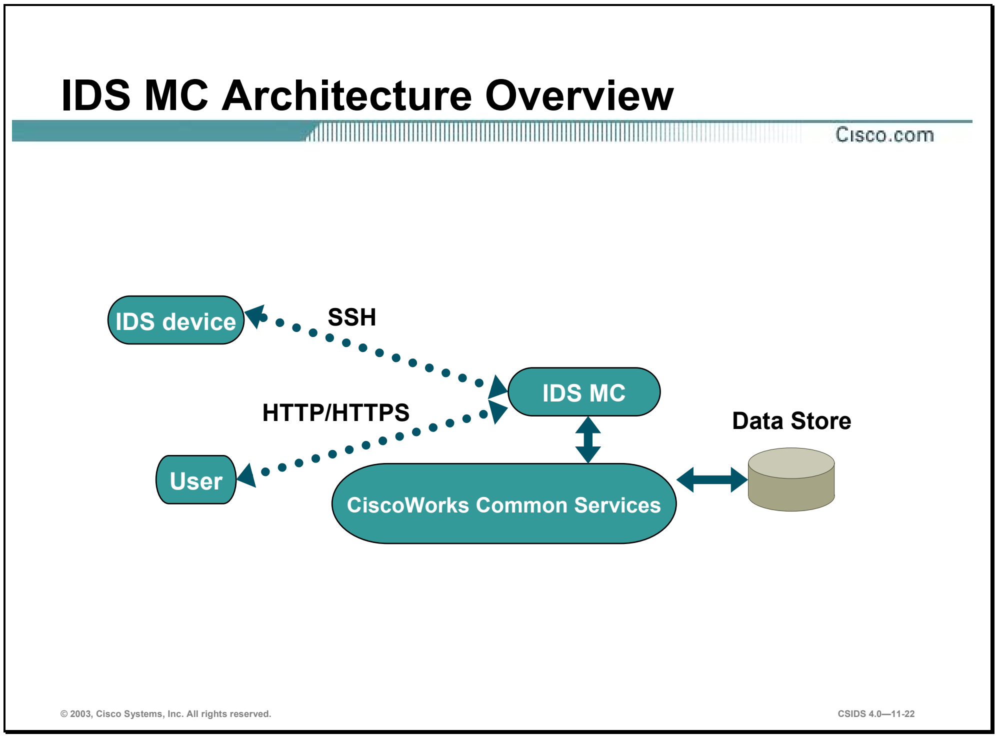
```
====================================================================
Finished:  Wed Dec 11 17:13:19 CST 2002
====================================================================
===============-  Software  Install  Tool Completed.        -=====================
====================================================================
```

CSIDS 4.0—11-20

Step 9 Close the Software Install Tool window after the IDS MC installation is complete.

Architecture

This section explains the IDS MC architecture, directories, and elements.



IDS MC Architecture Overview

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—11-22

The figure represents a high level overview of the IDS MC architecture. The IDS MC provides configuration management for multiple Sensors. It is designed to co-exist with existing CiscoWorks applications or as a standalone server.

The IDS MC depends on the framework and services provided by CiscoWorks Common Services. CiscoWorks Common Services is comprised of the following components:

- Data storage and management—The data store is contained within a Sybase SQL Anytime database. CiscoWorks Common Services provide management for this data to enable data backups and restores. Additionally, CiscoWorks Common Services provide functionality to enable automatic repairs of the database to prevent corruption.

- Web interface—This interface is provided by an Apache Web Server, which enables the user to connect to the CiscoWorks server via HTTP. Access to the IDS MC occurs via HTTPS.

- Session management—Manages user sessions to ensure that multiple users can connect to the IDS MC and performs operations without losing or corrupting data.

- User authentication and permission management—Performs permission management based upon user authorization roles. Users are assigned to a role. Each authorization role defines a set of permissions for access to various functions within VMS applications. CiscoWorks Common Services enforces the rights defined by authorization roles.

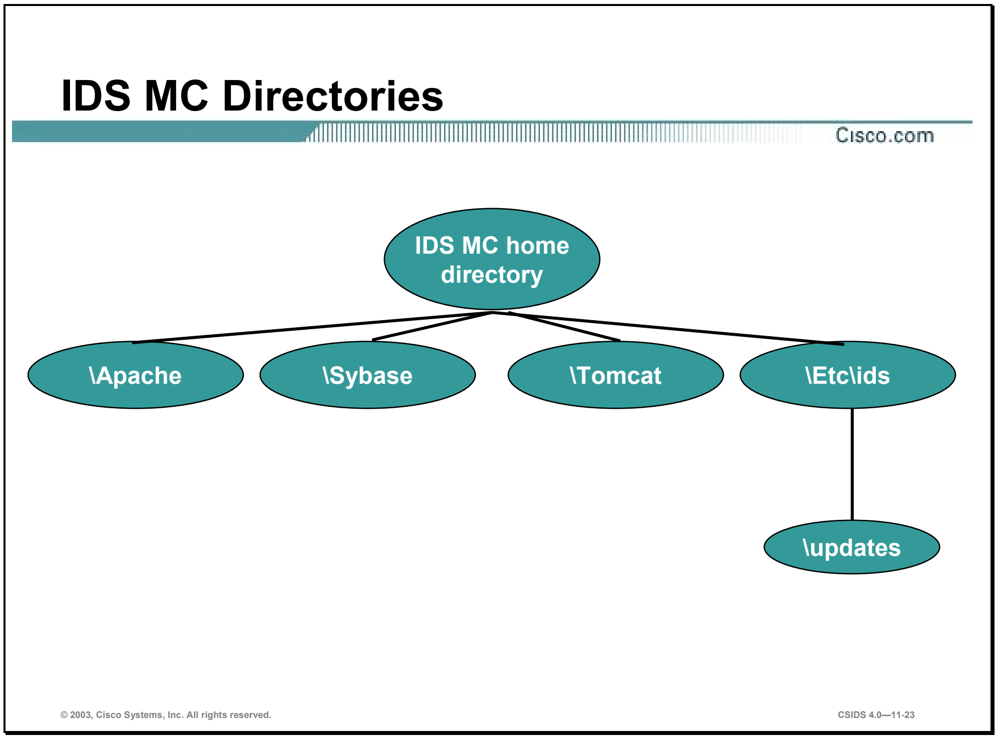
  - Common environment for the IDS MC—Enables abstraction of services by any and all Management Consoles installed on the server. Enables independent processes to function within their own range of operation.

The figure illustrates the interaction between the IDS MC and the CiscoWorks Common Services as well as the communications that occur among the user, the IDS MC server, and the Sensor. The following bullets describe those communications:

- First, the user must contact the CiscoWorks server to access the IDS MC. This initial contact with the CiscoWorks server occurs via HTTP on port 1741.

- Then, the user selects the IDS MC from within the CiscoWorks server. Encrypted communications are initiated. Thereafter, communications between the user and the IDS MC occur via HTTPS on port 443.

- The IDS MC and the Sensor communicate via SSH.



IDS MC Directories

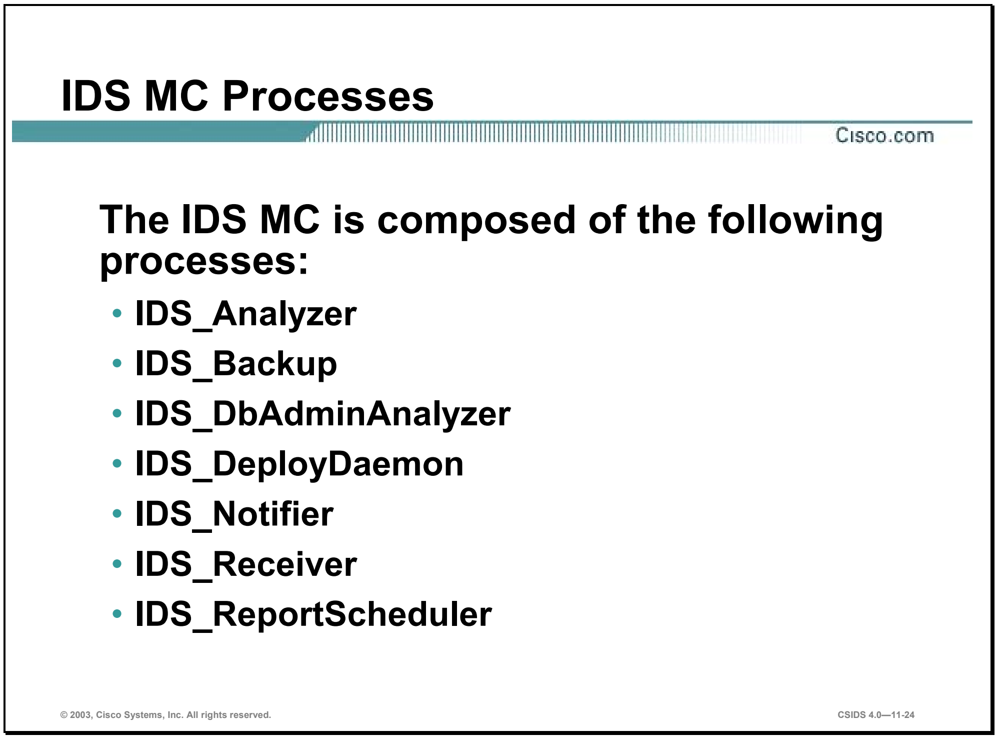
Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—11-23

By default, the IDS MC installs its components to the default directory where the CiscoWorks Common Services components have been installed. This directory is typically X:\Program Files\CSCOPx, (where X = hard drive). The IDS MC and its components are installed within the default directory as follows:

- IDS MC home directory—Is found at X:\CSCOPx\MDC, (where X = the hard drive that contains the home directory). All dependent applications are installed in this directory and the subsequent sub-directories.
  - Apache—The default directory where the Apache web server is installed. It serves the web pages that are displayed when using the IDS MC.
  - Sybase—The default directory where the Sybase SQL database is installed. Information is stored on IDS appliances and IDSMs in the Sybase SQL database.
  - Tomcat—The default directory where the Tomcat Server is installed. It is the application server that dispatches servlets to the IDS MC from Common Services.
  - Etc\ids—Directory where the IDS MC is stored.
- Etc\ids\updates—Directory where IDS update signatures are stored for the IDS MC to update Sensors or the IDS MC server itself.



IDS MC Processes

Cisco.com

The IDS MC is composed of the following processes:

- IDS_Analyzer
- IDS_Backup
- IDS_DbAdminAnalyzer
- IDS_DeployDaemon
- IDS_Notifier
- IDS_Receiver
- IDS_ReportScheduler

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—11-24

The following processes within the IDS MC enable it to perform its duties:

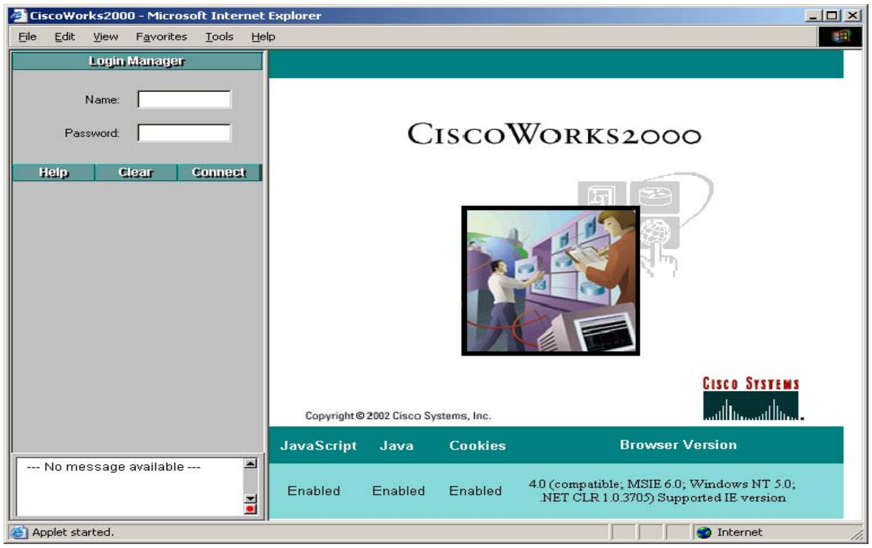
- IDS_Analyzer—Process defines event rules and requests user-specified notifications when appropriate.
- IDS_Backup—Performs a backup and restore of the database used by the IDS MC.
- IDS_DbAdminAnalyzer—Periodically applies active database rules to the current state of the server.
- IDS_DeployDaemon—Manages all configuration deployments.
- IDS_Notifier—Retrieves notification requests from other subsystems and performs the requested notification.
- IDS_Receiver—Receives Cisco IDS alarms and Syslog security events and stores them in the database.
- IDS_ReportScheduler—Generates all scheduled reports.

Getting Started

This section explains how authorization roles in CiscoWorks are responsible for the delegation of tasks and how to log in to the IDS MC.

CiscoWorks Login

Cisco.com



CiscoWorks2000 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Login Manager
Name:
Password:
Help
Clear
Connect
CiscoWorks2000
Cisco Systems
Internet

Copyright © 2002 Cisco Systems, Inc.

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.0.3705) Supported IE version

--- No message available ---

Applet started.

CSIDS 4.0—11-26

You must log in to CiscoWorks to navigate in the IDS MC. The CiscoWorks desktop is the interface for CiscoWorks network management applications, including the IDS MC.

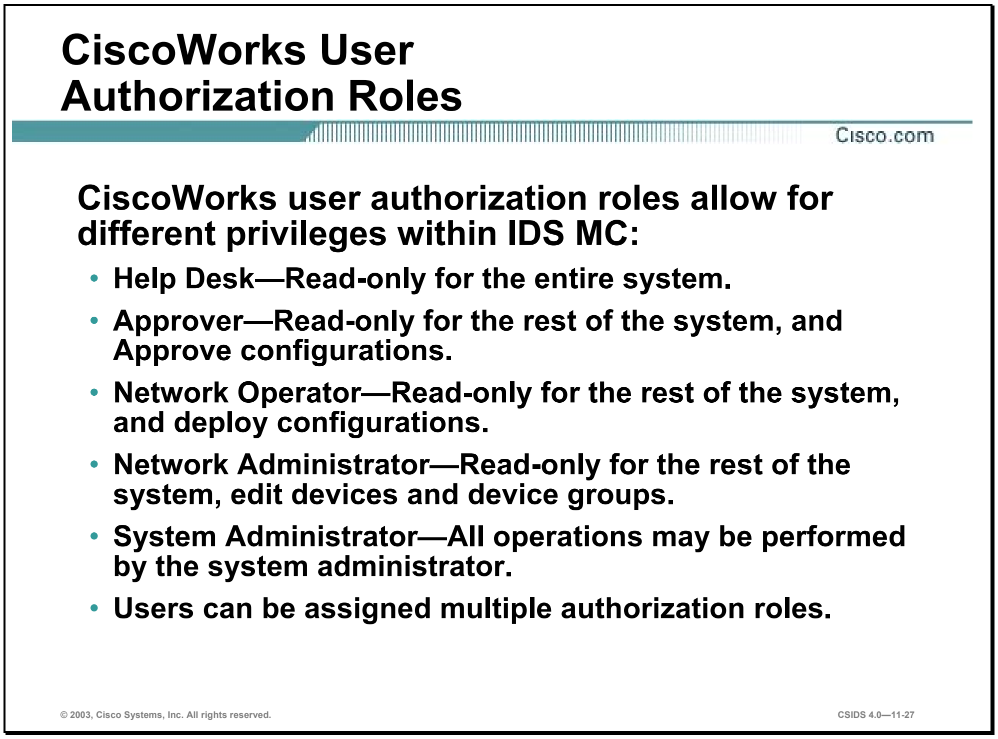
Complete the following steps to log in to CiscoWorks:

Step 1 Open a browser and point your browser to the IP address of the CiscoWorks machine with a port number of 1741. In this example the CiscoWorks server is the local machine. Enter the following web address in the browser address field:

```
http://127.0.0.1:1741
```

Step 2 Use the default administrative username and password of **admin** and **admin** to log in to CiscoWorks.

Note	It is recommended that you change the default admin account password.



CiscoWorks User Authorization Roles

CiscoWorks user authorization roles allow for different privileges within IDS MC:

- Help Desk—Read-only for the entire system.
- Approver—Read-only for the rest of the system, and Approve configurations.
- Network Operator—Read-only for the rest of the system, and deploy configurations.
- Network Administrator—Read-only for the rest of the system, edit devices and device groups.
- System Administrator—All operations may be performed by the system administrator.
- Users can be assigned multiple authorization roles.

CSIDS 4.0—11-27

There are five types of user authorization roles that are pertinent to the IDS MC. These roles can be used to delegate different responsibilities to users who log in to the IDS MC. For example, you can specify who can generate configurations or who can approve configurations. The five types of user authorization roles are as follows:

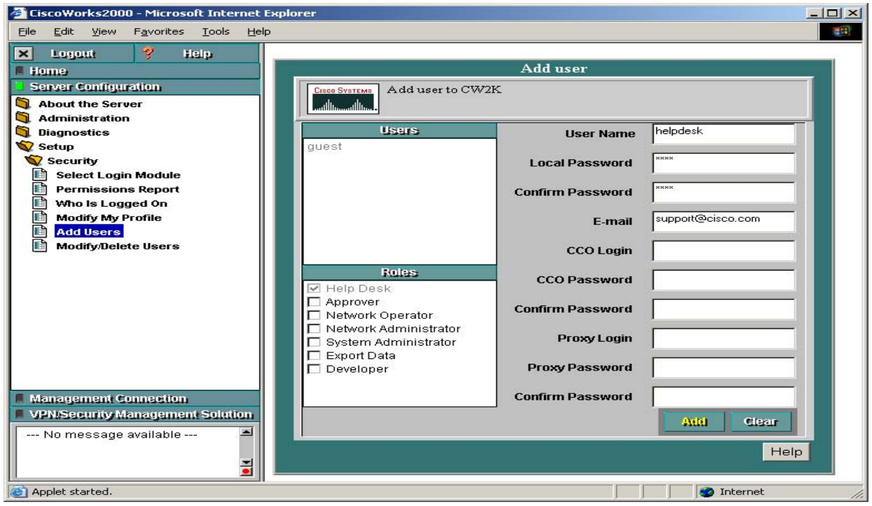
- Help Desk—Read-only for the entire system.
- Approver—Read-only for the entire system and includes approval privileges for configuration changes.
- Network Operator—Read-only for the entire system, generates reports, and includes configuration deployment privileges.
- Network Administrator—Read-only for the entire system and includes privileges to edit devices and device groups.
- System Administrator—Capable of performing all operations.

Note Users can be assigned multiple authorization roles. The roles of Export Data and Developer are not relevant to the IDS MC operations.

CiscoWorks Add User

Cisco.com

Choose Server Configuration>Setup>Security>Add Users.



Users: guest

Roles:
- ☑ Help Desk
- □ Approver
- □ Network Operator
- □ Network Administrator
- □ System Administrator
- □ Export Data
- □ Developer

User Name	helpdesk
Local Password	****
Confirm Password	****
E-mail	support@cisco.com
CCO Login	
CCO Password	
Confirm Password	
Proxy Login	
Proxy Password	
Confirm Password	

CSIDS 4.0—11-28

Complete the following steps to add users, and assign appropriate user authorization roles:

Step 1 Log in to the CiscoWorks desktop. The CiscoWorks desktop appears.

Step 2 Choose **Server Configuration>Setup>Security>Add Users**. The Add User page appears.

Step 3 Enter values for settings listed in the following table:

CiscoWorks Add User Settings	Description
User Name	User name to add.
Local Password	Password.
Confirm Password	Password confirmation.
E-mail	(Optional.) User's email address.
CCO Login	(Optional.) User's Cisco Connection Online (CCO) login.
CCO Password	(Optional.) User's CCO password.
Confirm Password	(Optional.) User's CCO password confirmation.
Proxy Login	(Optional.) Enter the user's proxy login. This is required if the CiscoWorks server is installed on a network that uses a proxy server.
Proxy Password	(Optional.) User's proxy password.
Confirm Password	(Optional.) User's proxy password confirmation.

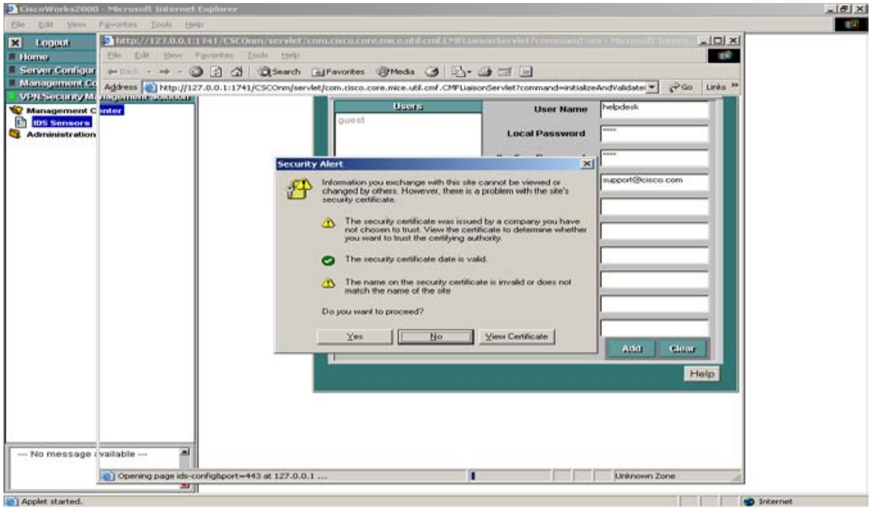
Step 4 Locate the Roles section on the lower left hand side of the Add User page. Use the check boxes to select the appropriate roles the user will fulfill.

Step 5 Click **Add** to complete the addition of the user to the CiscoWorks database.

IDS MC Launch

Cisco.com

Choose VPN/Security Management>Management Center>IDS Sensors.



CiscoWorks2000 - Microsoft Internet Explorer
Logout
Home
Server Configur
Management Co
VPN/Security Management Solution
Management Center
IDS Sensors
Administration
http://127.0.0.1:1741/CSCOnm/servlet/com.cisco.core.mice.util.cmf.CMFLiaisonServlet?command=initializeAndValidate
Users
guest
User Name
helpdesk
Local Password
support@cisco.com
Add
Clear
Help
--- No message available ---
Opening page ids-config&port=443 at 127.0.0.1 ...
Unknown Zone
Applet started.
Internet

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Yes | No | View Certificate

CSIDS 4.0—11-29

The IDS MC application is accessible from the CiscoWorks desktop. Complete the following steps to launch the IDS MC:

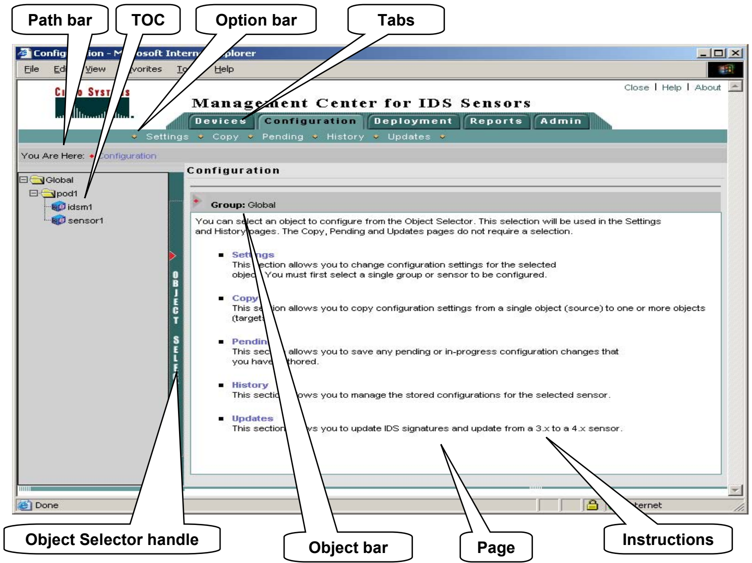
Step 1 Log in to CiscoWorks.

Step 2 Select the **VPN/Security Management** drawer to expand it and reveal the folders within the drawer.

Step 3 Click the folder named **Management Center**. The Management Center folder expands.

Step 4 Click on **IDS Sensors** to launch the IDS MC. The IDS MC launches in a new window.

Understanding the IDS MC Interface



Group: Global

You can s lect an object to configure from the Object Selector. This selection will be used in the Settings and History pages. The Copy, Pending and Updates pages do not require a selection.

- **Set ngs**
  This ection allows you to change configuration settings for the selected objec You must first select a single group or sensor to be configured.
- **Copy**
  This se ion allows you to copy configuration settings from a single object (source) to one or more objects (target
- **Pendin**
  This sec allows you to save any pending or in-progress configuration changes that you have thored.
- **History**
  This sectio ows you to manage the stored configurations for the selected sensor.
- **Updates**
  This section vs you to update IDS signatures and update from a 3.x to a 4.x sensor.

CSIDS 4.0—11-30

The figure illustrates elements of the IDS MC GUI. The elements are described as follows:

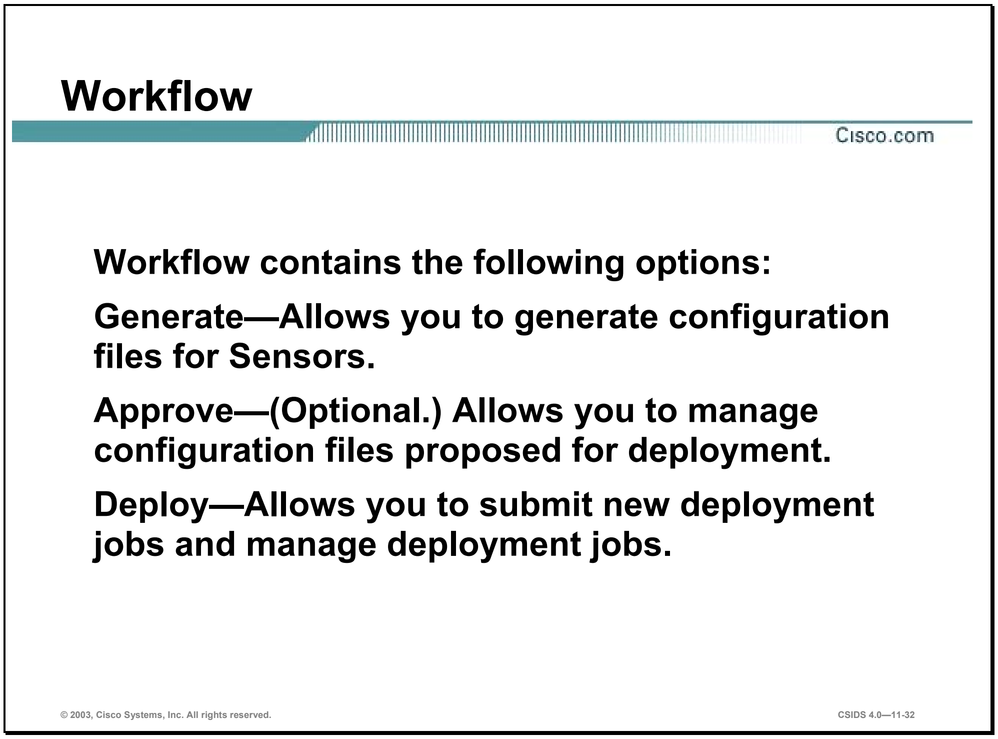
- Path bar—Provides a context for the displayed page. Shows the tabs, options, and current page.
- TOC—Displays the available sub-options, if required.
- Option bar—Displays the options available for the selected tab.
- Tabs—Provides access to product functionality:
  - Devices tab—Enables you to perform initial setup of devices to be managed by the system.
  - Configuration tab—Enables you to perform general configuration tasks.
  - Deployment tab—Enables you to generate configuration files, manage Sensor configuration files, and submit or manage new jobs.
  - Reports tab—Enables you to generate reports, view scheduled reports, and view reports.
  - Admin tab—Enables you to administer system settings.
- Instructions—Provides a brief overview of how to use the page.
- Page—Displays the area in which you perform application tasks.

- Object bar—Displays the object or objects selected in the Object Selector.

- Object Selector handle—Opens and closes the Object Selector by clicking on it. The Object Selector contains devices and device groups from which to select.

IDS MC Workflow

This section explains the workflow process of deploying IDS configuration files.



Workflow

Workflow contains the following options:

Generate—Allows you to generate configuration files for Sensors.

Approve—(Optional.) Allows you to manage configuration files proposed for deployment.

Deploy—Allows you to submit new deployment jobs and manage deployment jobs.

CSIDS 4.0—11-32

The Deployment tab is used to deploy configuration files to Sensors. Sensor configuration files should be deployed in, which is known as the workflow. The workflow is as follows:

Step 1 Generate new configuration files. This applies to Sensors for which proposed configuration changes have been committed to the database, but for which the configuration files have not been generated.

Step 2 (Optional.) Approve the configuration file changes. At this point you can approve, view, and delete proposed configuration file changes.

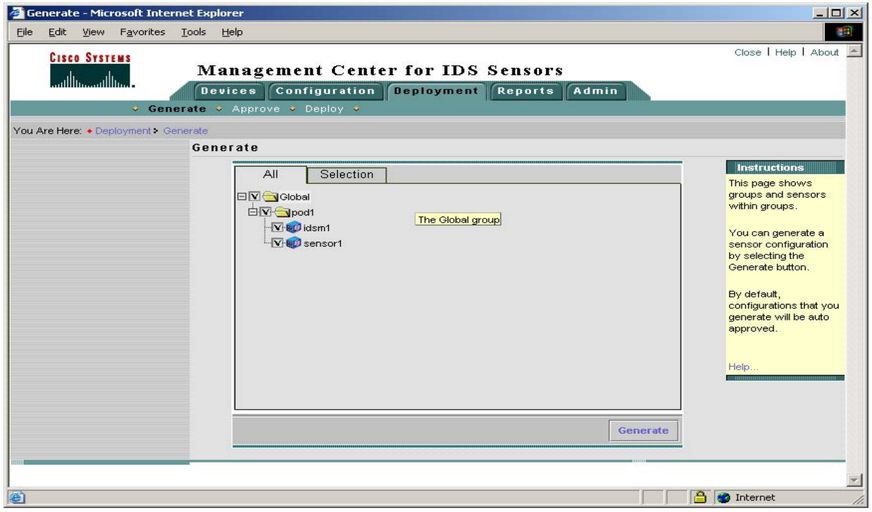
Note By default, approval is not required. Choose **Admin>System Configuration>Configuration File Management** and select **Enable Configuration file change approval** to enable the approval feature.

Step 3 Deploy approved configuration files to the Sensors.

Workflow—Generate

Cisco.com

Choose Deployment>Generate**.**


Generate - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Close | Help | About
Management Center for IDS Sensors
Devices Configuration Deployment Reports Admin
Generate Approve Deploy
You Are Here: Deployment > Generate
Generate
All Selection
Global
pod1
idsm1
sensor1
The Global group
Generate
Internet

Instructions

This page shows groups and sensors within groups.

You can generate a sensor configuration by selecting the Generate button.

By default, configurations that you generate will be auto approved.

Help...

CSIDS 4.0—11-33

Generating new configuration files applies to Sensors for which proposed configuration changes have been committed to the database, but for which the configuration files have not been generated.

You cannot generate a configuration file for proposed configuration changes until you commit them to the database, that is, until you save them. You can review proposed configuration changes to determine whether or not you have saved them.

Complete the following steps to generate configuration files for the Sensor:

Step 1 Choose **Deployment>Generate**. The Generate page appears.

Step 2 Select the Sensor’s check box and click **Generate** to generate the Sensor’s configuration. The Generate page appears.

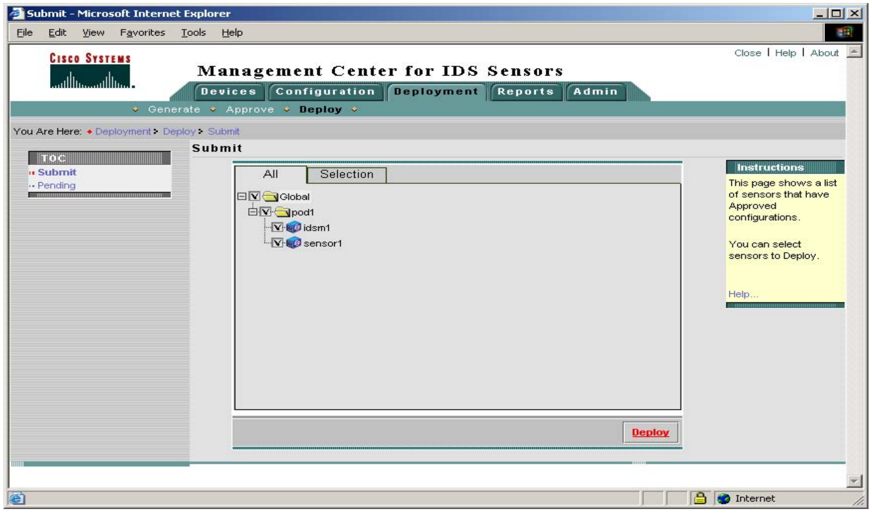
Note If there are existing changes to the configuration file that are pending, the configuration file generation will fail. Choose **Configuration>Pending** to view the existing pending changes to the Sensors.

The configuration file generations are complete and ready to be sent for deployment.

Workflow—Deploy

Cisco.com

Choose Deployment>Deploy>Submit.



Instructions

This page shows a list of sensors that have Approved configurations.

You can select sensors to Deploy.

CSIDS 4.0—11-34

The Deploy page on the Deployment tab allows you to view two activities, submit and pending. Submit allows you to create a new deployment job. Pending enables you to view pending deployment jobs.

Complete the following steps to create a new deployment job:

Step 1 Choose **Deployment>Deploy**. The Deploy page appears.

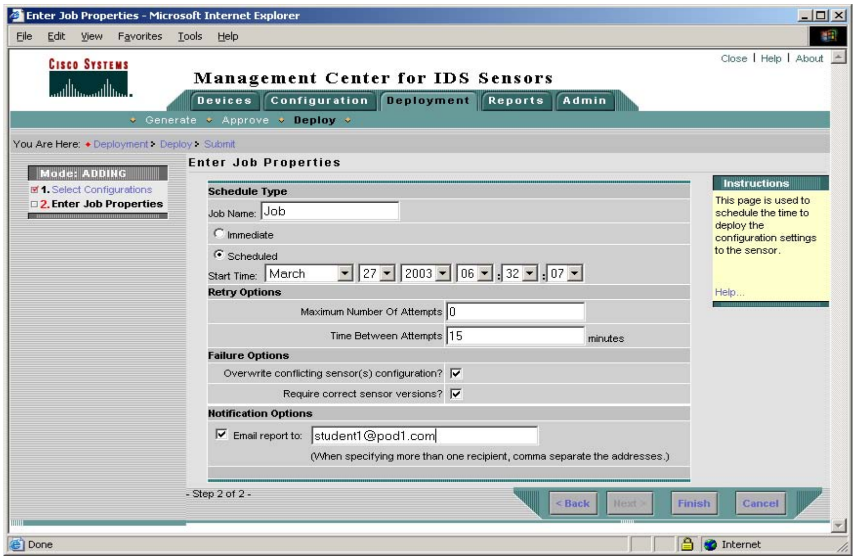
Step 2 From the TOC, select **Submit**.

Step 3 Select the Sensors for which you want to deploy configuration files and click **Deploy**. The Select Configurations page appears.

Step 4 Select the configuration files that you want to deploy to Sensors. Click **Next**. The Enter Job Properties page appears.

Workflow—Deploy (Schedule)

Cisco.com



Enter Job Properties - Microsoft Internet Explorer

Management Center for IDS Sensors

You Are Here: Deployment > Deploy > Submit

Mode: ADDING

☑ 1. Select Configurations
□ 2. Enter Job Properties

Enter Job Properties

Schedule Type

Job Name: Job

○ Immediate

● Scheduled

Start Time: March 27 2003 06 : 32 : 07

Retry Options

Maximum Number Of Attempts 0

Time Between Attempts 15 minutes

Failure Options

Overwrite conflicting sensor(s) configuration? ☑

Require correct sensor versions? ☑

Notification Options

☑ Email report to: student1@pod1.com

(When specifying more than one recipient, comma separate the addresses.)

- Step 2 of 2 -

Instructions

This page is used to schedule the time to deploy the configuration settings to the sensor.

CSIDS 4.0—11-35

Step 5 Enter values for settings listed in the following table:

IDS MC Enter Job Properties Setting	Description
Job Name	Name of the deployment job.
Immediate	Immediately deploys the configuration files to the Sensors.
Scheduled	Schedule the configuration file deployment for a later date and time.
Maximum Number Of Attempts	(Optional.) Change the number of times the IDS MC will attempt to send an update to the Sensors. The default is 0.
Time Between Attempts	(Optional.) Change the number of minutes between attempts. The default is 15.
Overwrite conflicting Sensors configuration	(Optional.) Select this check box to overwrite the Sensor’s configuration.
Require correct Sensor versions	(Optional.) Select this check box to require the Sensor version to be the same of that listed on the IDS MC.
Email report to	(Optional.) Select this check box and enter the e-mail addresses to which reports of the IDS MC Job Deployment status should be sent.

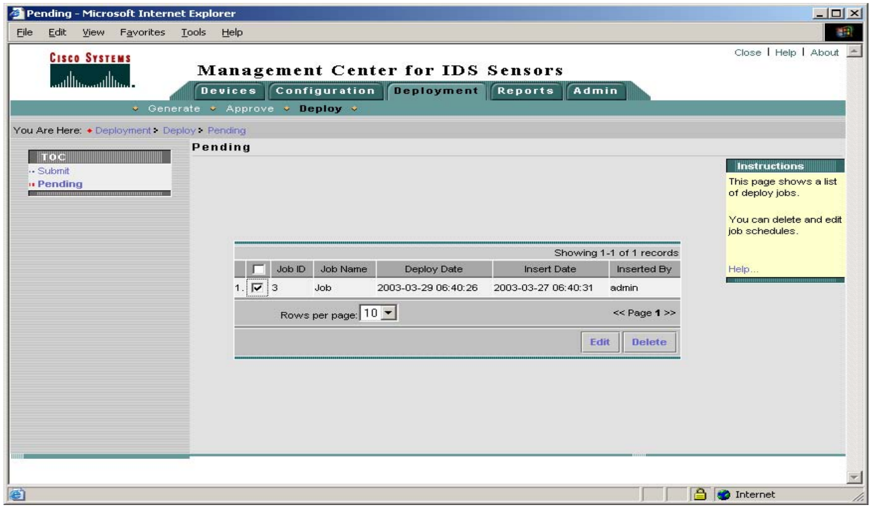
Step 6 Click **Finish**. The Submit page is displayed.

Note Verify the Sensor’s configuration deployment by generating a Sensor Configuration Deployment Report. Choose **Reports>Generate>Sensor Configuration Deployment Report** and click **Select** to start the report generation.

Workflow—Deploy (Pending)

Cisco.com

Choose Deployment>Deploy>Pending**.**



You Are Here: Deployment > Deploy > Pending

Pending

This page shows a list of deploy jobs.

You can delete and edit job schedules.

Showing 1-1 of 1 records

	□	Job ID	Job Name	Deploy Date	Insert Date	Inserted By
1.	☑	3	Job	2003-03-29 06:40:26	2003-03-27 06:40:31	admin

Rows per page: 10

<< Page 1 >>

CSIDS 4.0—11-36

During the job deployment submission process, you have the ability to schedule the deployment for a later time. If you choose a future deployment date, as opposed to an immediate deployment date, you will be able to see and edit pending job deployment schedules.

Complete the following steps to view and edit a pending job:

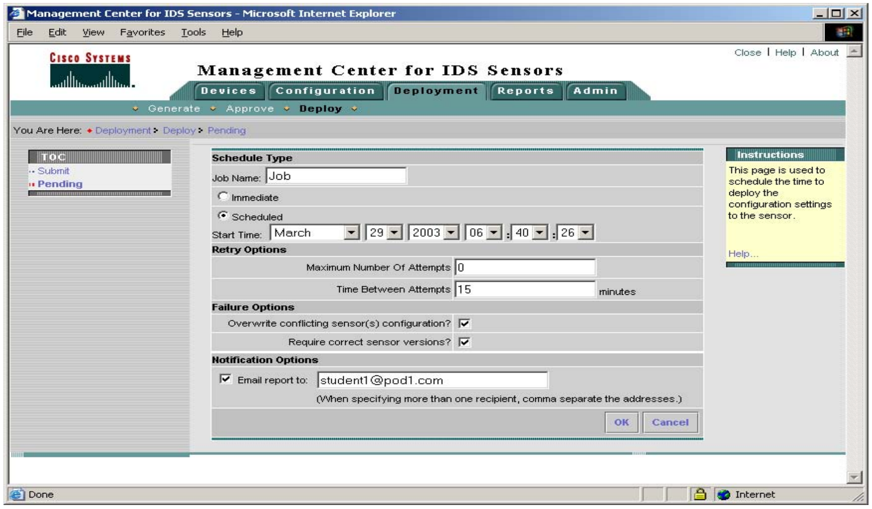
Step 1 Choose **Deployment>Deploy**. The Deploy page is displayed.

Step 2 Click **Pending** from the TOC. The Pending page is displayed.

Workflow—Deploy (Pending) (cont.)

Cisco.com

Choose Deployment>Deploy>Pending**.**



You Are Here: • Deployment > Deploy > Pending

Schedule Type

Job Name: Job

○ Immediate

● Scheduled

Start Time: March 29 2003 06 : 40 : 26

Retry Options

Maximum Number Of Attempts: 0

Time Between Attempts: 15 minutes

Failure Options

Overwrite conflicting sensor(s) configuration? ☑

Require correct sensor versions? ☑

Notification Options

☑ Email report to: student1@pod1.com

(When specifying more than one recipient, comma separate the addresses.)

OK Cancel

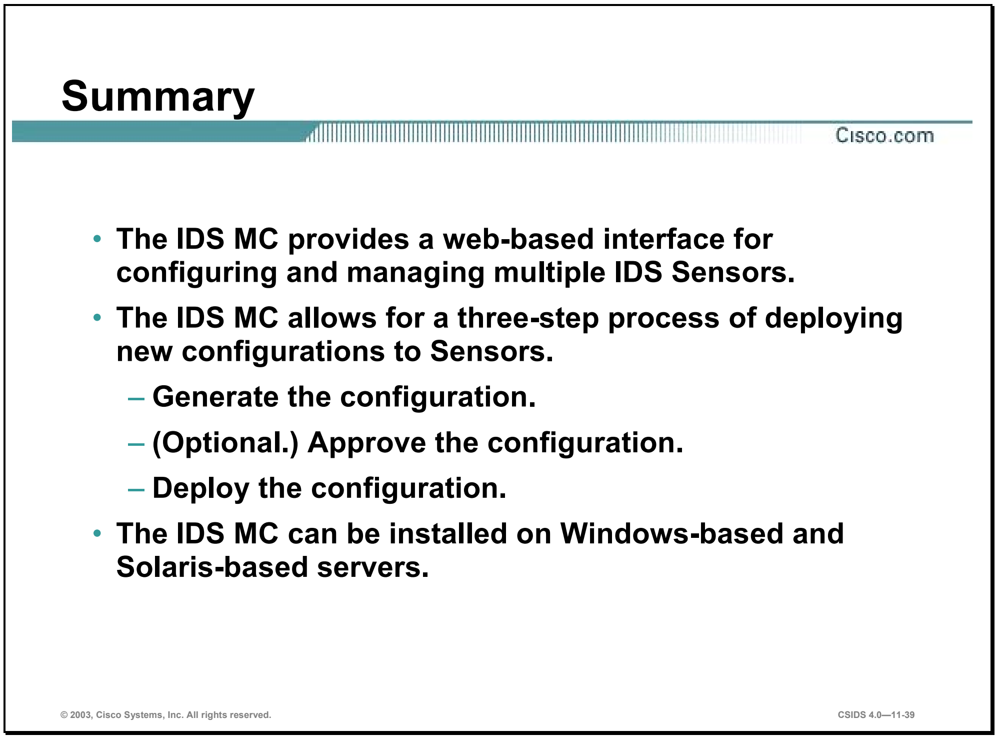
This page is used to schedule the time to deploy the configuration settings to the sensor.

CSIDS 4.0—11-37

Step 3 Select a pending job’s check box and click **Edit**. The pending job’s scheduling page is displayed.

Summary

This section summarizes what you learned in the chapter.



Summary

- The IDS MC provides a web-based interface for configuring and managing multiple IDS Sensors.
- The IDS MC allows for a three-step process of deploying new configurations to Sensors.
  - Generate the configuration.
  - (Optional.) Approve the configuration.
  - Deploy the configuration.
- The IDS MC can be installed on Windows-based and Solaris-based servers.

CSIDS 4.0—11-39

Lab Exercise—Enterprise Intrusion Detection System Management

Complete the following lab exercise to practice what you learned in this chapter.

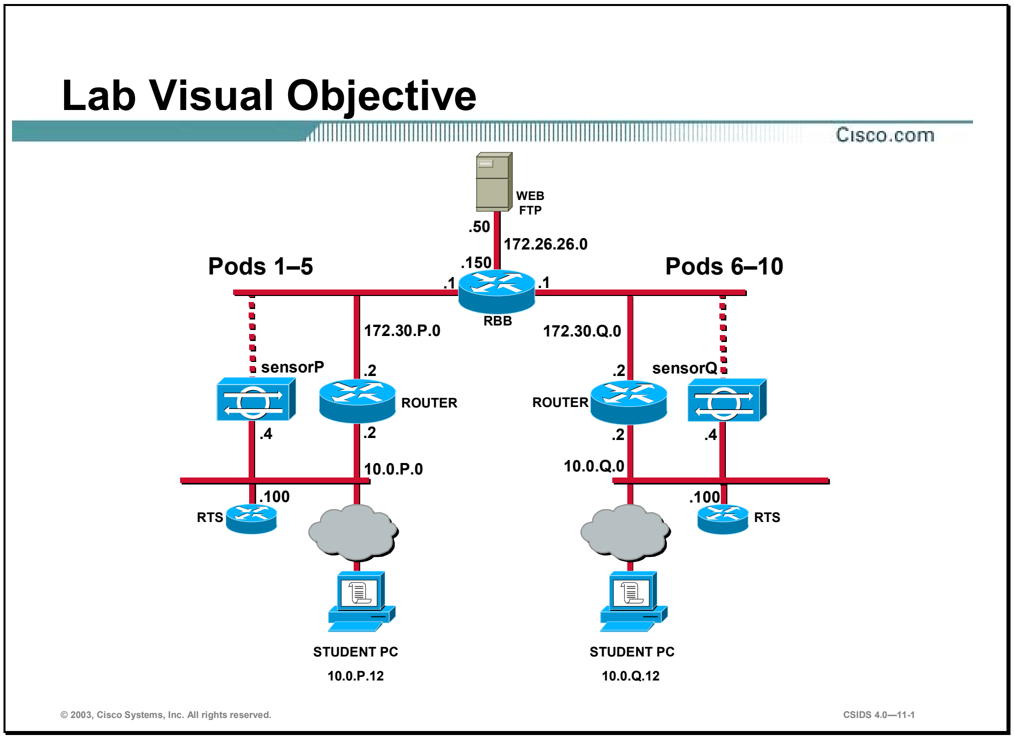
Objectives

In this lab exercise you will complete the following tasks:

- Install the IDS MC.
- Launch the IDS MC.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—11-1

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab exercise.

Note	The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor. Make sure to replace it with your peer's pod number.

Task 1—Install the IDS MC

This task involves the student installing only the Intrusion Detection System (IDS) Management Center (MC) of the Sensors product on to the student PC. Complete the following steps to install the IDS MC:

Step 1 Log in as the local administrator on the student PC.

Step 2 Uninstall the IDS Event Viewer.

Caution Do not proceed with this task until the IDS Event Viewer is uninstalled from the student PC.

Step 3 Go to **Start>Programs>CiscoWorks2000** to verify that the CiscoWorks2000 (CiscoWorks) VPN/Security Management Solution (VMS) Common Services has been installed on the student PC. Notify your instructor if the CiscoWorks Common Services are not installed.

Step 4 Locate and run the IDS MC installation files as directed by your instructor. The Welcome window opens.

Step 5 Click **Next** to begin the installation. The Software License Agreement panel is displayed.

Step 6 Click **Yes** to accept the terms of the license agreement. A window opens to give a choice of Typical or Custom installation.

Step 7 Select **Custom installation** and click **Next** to continue. The Select Components window opens.

Step 8 Select **IDS MC only** to install the IDS MC and click **Next**. The System Requirements panel is displayed.

Step 9 Click **Next** after verifying that your system meets the minimum disk space and memory requirements. The Verification window opens.

Step 10 Click **Next** after verifying the selected settings. The Select Database Location window opens.

Step 11 Click **Next** to accept the default database directory. The Select Database Password window opens.

Step 12 Enter **cisco** in the Password and Confirm Password text boxes.

Step 13 Click **Next**. The Restart window opens.

Step 14 Select **Yes, I want to restart my computer now**, and click **Finish**.

Task 2—Launch the IDS MC

This task involves accessing the CiscoWorks server to launch the IDS MC. Complete the following steps to log in to the CiscoWorks server and launch the IDS MC:

Step 1 Access the CiscoWorks server from your web browser by entering the following in the URL field:

```
http://127.0.0.1:1741
```

Be patient when connecting to the CiscoWorks server. The server requires additional software to be installed. The software is installed during the initial access. Subsequent attempts should not require the user to install additional software.

Note Select **Grant Always** when prompted to accept the Sun certificate to avoid future messages.

Step 2 Log in by entering the default username and password of **admin** and **admin**, respectively.

Note It is recommended to change the default admin account password.

Step 3 Click **Connect**. You are now logged in to the CiscoWorks desktop.

Step 4 Select the **VPN/Security Management Solution** drawer located in the left panel.

Step 5 Select the **Management Center** folder located in the VPN/Security Management Solution drawer.

Step 6 Select **IDS Sensors** from the Management Center folder. The Security Alert window opens prompting you to accept a digital certificate.

Step 7 Click **Yes**. You are now logged in to the IDS MC.

Step 8 Minimize the CiscoWorks browser window before proceeding to the next lab exercise.

12

Sensor Configuration

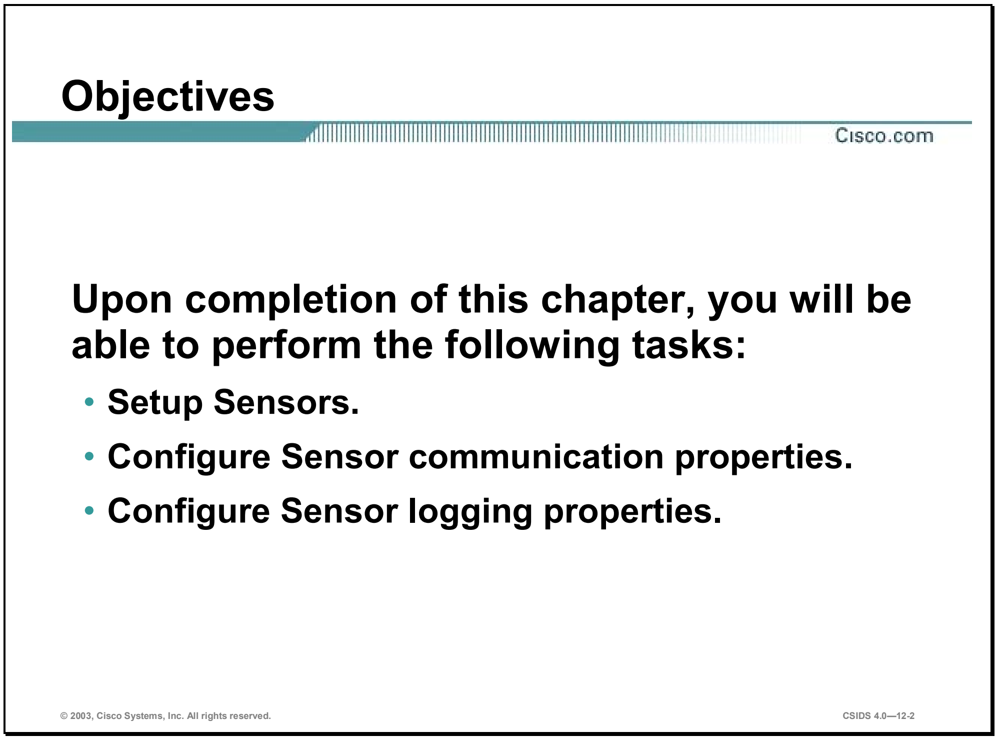
Overview

This chapter introduces the setup of Sensors in the Intrusion Detection System (IDS) Management Center (MC). The following topics are covered in this chapter:

- Objectives
- Sensors and Sensor Groups
- Communications
- Logging
- Summary
- Lab exercise

Objectives

This section lists the chapter objectives.



Objectives

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

- **Setup Sensors.**
- **Configure Sensor communication properties.**
- **Configure Sensor logging properties.**

CSIDS 4.0—12-2

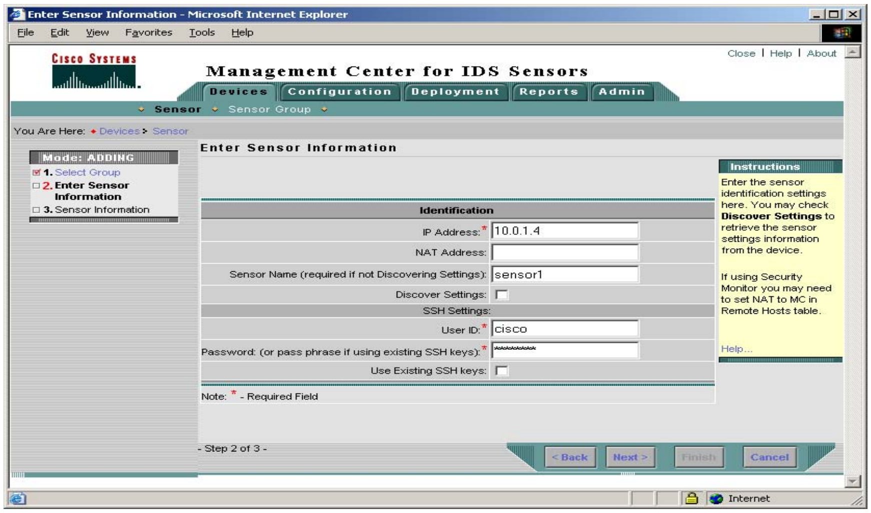
Sensors and Sensor Groups

This section explains adding Sensors and creating Sensor groups within the IDS MC.

Devices—Sensor

Cisco.com

Choose Devices>Sensor>Add.


Enter Sensor Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Management Center for IDS Sensors
Devices Configuration Deployment Reports Admin
Sensor Sensor Group
Mode: ADDING
< Back
Next >
Finish
Cancel
Internet

You Are Here: Devices > Sensor

☑ 1. Select Group
□ 2. Enter Sensor Information
□ 3. Sensor Information

Enter Sensor Information

Identification

IP Address:* 10.0.1.4
NAT Address:
Sensor Name (required if not Discovering Settings): sensor1
Discover Settings: □
SSH Settings:
User ID:* cisco
Password: (or pass phrase if using existing SSH keys):* ********
Use Existing SSH keys: □

Note: * - Required Field

- Step 2 of 3 -

Instructions

Enter the sensor identification settings here. You may check **Discover Settings** to retrieve the sensor settings information from the device.

If using Security Monitor you may need to set NAT to MC in Remote Hosts table.

Help...

CSIDS 4.0—12-4

Complete the following steps to add a Sensor to the IDS MC:

Step 1 Choose **Devices>Sensor>Add**. The Select Sensor Group page appears.

Step 2 Select the group you are going to import the Sensor into and click **Next**. The Enter Sensor Information page is displayed.

Step 3 Enter values for settings listed in the following table:

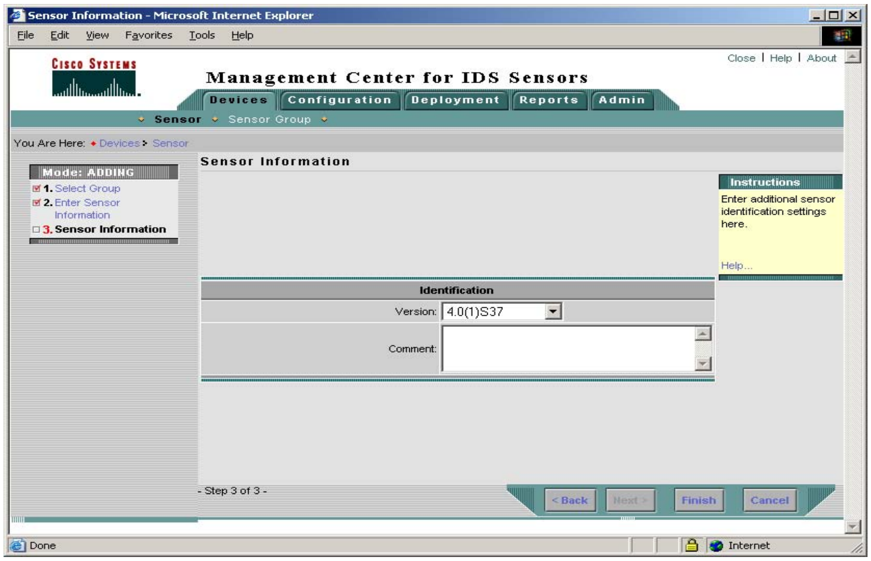
IDS MC Sensor Settings	Description
IP Address	Enter the IP address of the Sensor you want to manage.
NAT Address	(Optional.) Enter the Sensor's NAT address. This is the IP address the IDS MC server would see for the Sensor.
Sensor Name	Enter the name of the Sensor you want to manage.
Discover Settings	(Optional.) Select this check box to retrieve the Sensor settings information from the device.
User ID	Enter the username that will manage the Sensor. Use the username netrangr when you are using a Sensor appliance with a software version earlier than 4.0. Use the username cisco when you are importing a Sensor with a software version of 4.0 or later. Use the username ciscoids when using an IDSM.
Password	Enter the User ID password or pass phrase if you are using existing SSH keys. The passwords will vary according to the passwords that you assigned to the devices during the initial configuration.

IDS MC Sensor Settings	Description
Use Existing SSH Keys	(Optional.) Select this check box if you are using existing SSH keys.
Discover Settings	(Optional.) Select this check box to retrieve the Sensor settings information from the device.

Note The discover settings process may require 30 seconds to several minutes, depending upon the size and complexity of your network and its traffic, to complete.

Step 4 Click **Next**. The Sensor Information page appears.

Devices—Sensor (cont.)


Sensor Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Management Center for IDS Sensors
Devices
Configuration
Deployment
Reports
Admin
Sensor
Sensor Group
You Are Here: Devices > Sensor
< Back
Next >
Finish
Cancel
Done
Internet

Mode: ADDING

☑ 1. Select Group
☑ 2. Enter Sensor Information
□ 3. Sensor Information

Sensor Information

Instructions
Enter additional sensor identification settings here.
Help...

Identification

Version: 4.0(1)S37

Comment:

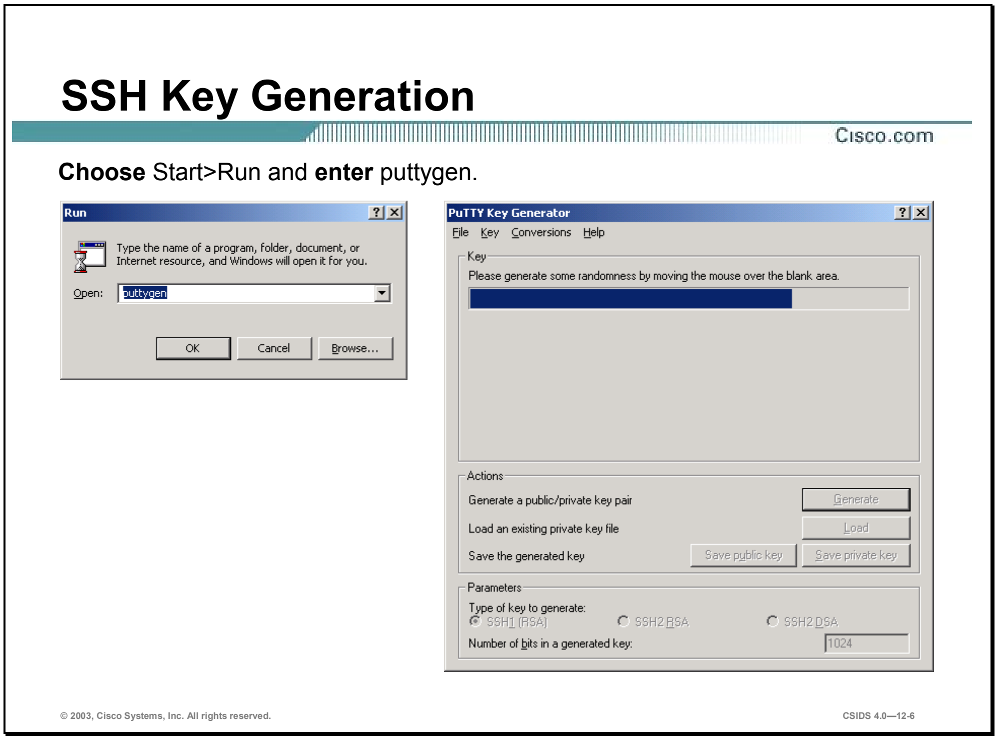
- Step 3 of 3 -

Step 5 Select the Sensor's software version from the Version drop-down menu and enter a descriptive comment in the Comment field.

Note If you chose the Discover Settings check box earlier, you will see the Sensor Information page with an Import Status message. The message displays the Sensor's name and software version.

Step 6 Click **Finish** to finish adding a Sensor to the IDS MC. The Sensor page is displayed with the new Sensor.

Note If the Sensor software version is not listed in the drop-down menu, it will be necessary to update the IDS MC with the latest version of IDS signatures.



SSH Key Generation

Cisco.com

Choose Start>Run and **enter** puttygen.

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: puttygen

PuTTY Key Generator

Please generate some randomness by moving the mouse over the blank area.

Type of key to generate:
● SSH1 (RSA) ○ SSH2 RSA ○ SSH2 DSA

Number of bits in a generated key: 1024

CSIDS 4.0—12-6

When you import the IDS Sensor into the IDS MC, you are given the option to import a Sensor using existing SSH keys. This option allows you to use the Sensor's existing SSH key and provides an additional level of security for your enterprise.

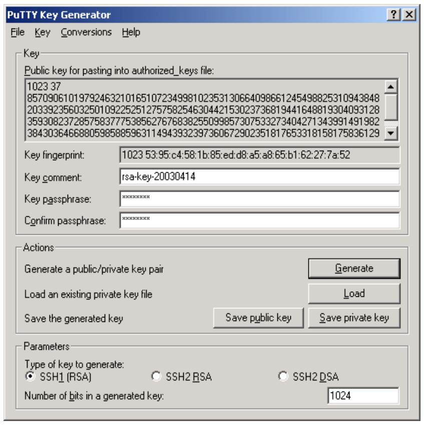
Complete the following steps to generate an SSH key, copy the SSH key to the IDS Sensor, connect to the Sensor, test the SSH key, and import the Sensor into the IDS MC:

Step 1 Complete the following sub-steps to generate an SSH key:

1. Log into the server where the IDS MC has been installed.
2. Choose **Start>Run** to access the Run command line.
3. Enter **puttygen** in the Open field and click **OK**. The PuTTY Key Generator window opens.
4. Click **Generate** to accept the default values. Drag your mouse pointer over the blank area of the PuTTY Key Generator to generate the key. The public key is displayed.

SSH Key Generation (cont.)

Cisco.com



PuTTY Key Generator

Public key for pasting into authorized_keys file:

```
1023 37
857090610197924632101651072349981023531306640986612454988253109438482033923560325010922525127575825463044215302373681944164881930409312835930823728575837775385627676838255099857307533273404271343991491982384303646688059858859631149439323973606729023518176533181581758361 29
```

Key fingerprint: 1023 53:95:c4:58:1b:85:ed:d8:a5:a8:65:b1:62:27:7a:52

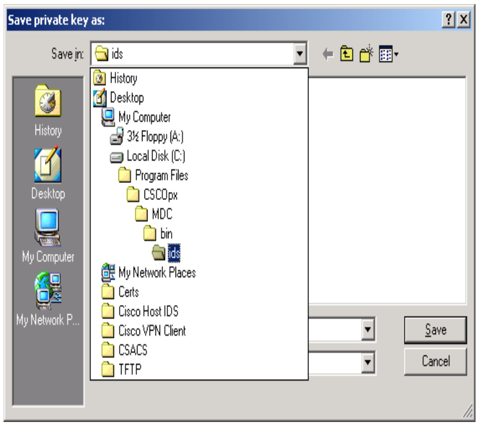
Key comment: rsa-key-20030414

Key passphrase: ********

Confirm passphrase: ********

Type of key to generate: ● SSH1 (RSA) ○ SSH2 RSA ○ SSH2 DSA

Number of bits in a generated key: 1024



Save private key as:

Save in: ids

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—12-7

5. Enter an SSH key passphrase in the Key passphrase field.

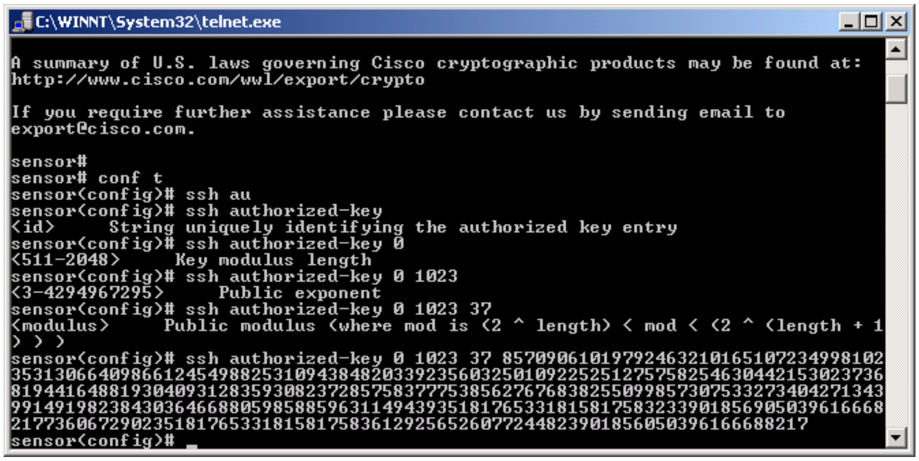
6. Enter the passphrase again in the Confirm passphrase field.

7. Click **Save private key**. The Save private key as window opens.

8. Save the private key with the hostname of the Sensor you are going to import to the X:\Program Files\CSCOpx\MDC\bin\ids directory, where X = the default drive where the IDS MC is installed.

SSH Key Import

Cisco.com



```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto

If you require further assistance please contact us by sending email to
export@cisco.com.

sensor#
sensor# conf t
sensor(config)# ssh au
sensor(config)# ssh authorized-key
<id>     String uniquely identifying the authorized key entry
sensor(config)# ssh authorized-key 0
<511-2048>     Key modulus length
sensor(config)# ssh authorized-key 0 1023
<3-4294967295>     Public exponent
sensor(config)# ssh authorized-key 0 1023 37
<modulus>     Public modulus (where mod is (2 ^ length) < mod < (2 ^ (length + 1
) ) )
sensor(config)# ssh authorized-key 0 1023 37 857090610197924632101651072349981O2
3531306640986612454988253109438482033923560325010922525127575825463044215302373б
81944164881930409312835930823728575837775385627676838255099857307533273404271343
99149198238430364668805985885963114943935181765331815817583233901856905039616668
2177360672902351817653318158175836129256526077244823901856050396166688217
sensor(config)# _
```

CSIDS 4.0—12-8

Step 2 Complete the following sub-steps to copy the SSH key to the Sensor:

1. Connect to the Sensor and enter configuration mode.
2. Enter the **ssh authorized-key** command:

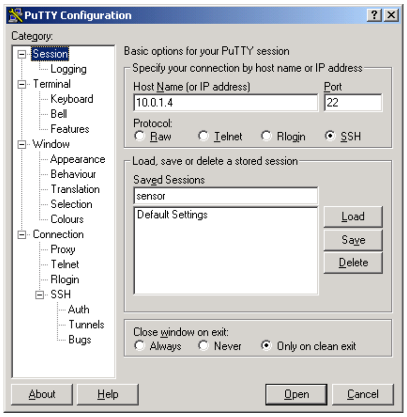
```
sensor1(config)# ssh authorized-key 0  . . .
```

Note Enter the modulus key length, public exponent, and modulus number parameters by copying them from the PuTTY Key Generator to the Sensor CLI. The first number of the public key you generated is the modulus key length, the second number is the public exponent, and the third number is the modulus number.

SSH Key Test

Cisco.com

Choose Start>Run and **enter** putty.



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 10.0.1.4

Port: 22

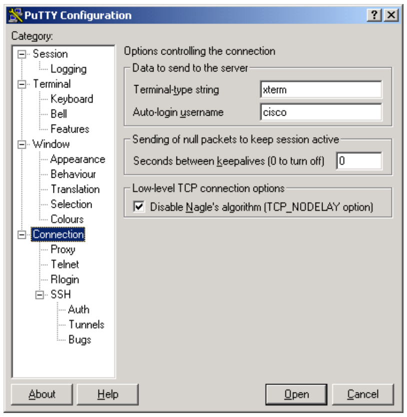
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

Saved Sessions: sensor

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



Options controlling the connection

Data to send to the server

Terminal-type string: xterm

Auto-login username: cisco

Sending of null packets to keep session active

Seconds between keepalives (0 to turn off): 0

Low-level TCP connection options

☑ Disable Nagle's algorithm (TCP_NODELAY option)

CSIDS 4.0—12-9

Step 3 Complete the following sub-steps to test the SSH key:

1. Launch the PuTTY Configuration application from the server where the IDS MC is installed.

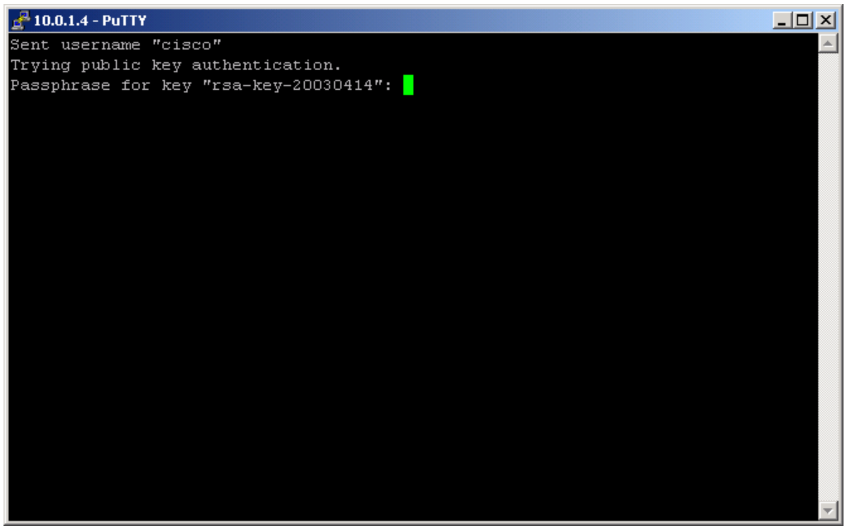
2. Enter values for settings listed in the following table:

PuTTY Settings	Description
Session>Host Name or IP Address	Enter the IP address of the Sensor you want to connect to in order to test the SSH key.
Session>Protocol	Select the **SSH** radio button.
Session>Saved Sessions	Enter the hostname of the Sensor in the Saved Sessions field. Do not click Save yet.
Connection>Auto-login username	Enter the username with which you logged in and created the session.

3. Go back to the Session page and click **Save**. The PuTTY Configuration window refreshes to display the saved session.

SSH Key Test (cont.)

Cisco.com



```
Sent username "cisco"
Trying public key authentication.
Passphrase for key "rsa-key-20030414":
```

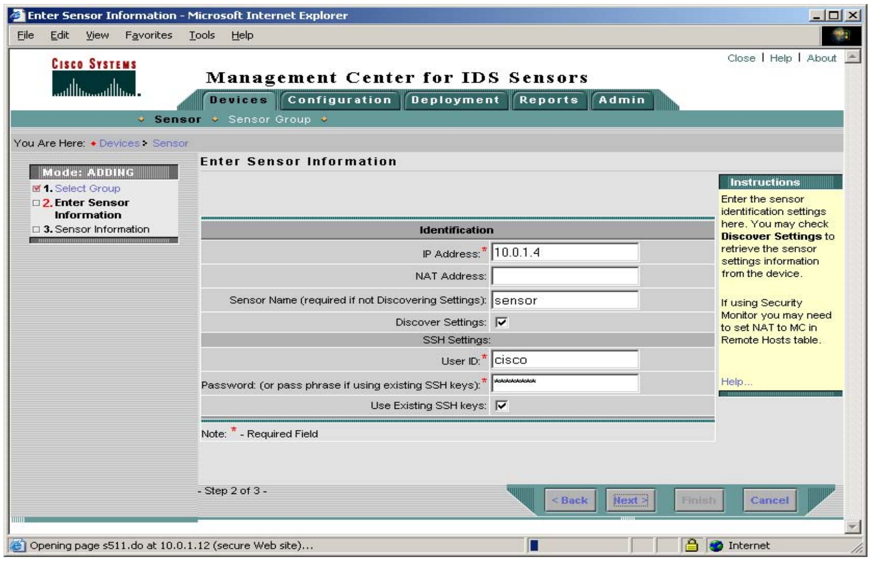
CSIDS 4.0—12-10

4. Click **Open**. The PuTTY session opens and connects to the Sensor.

5. Enter the passphrase you assigned to the private key and press **Enter**. You should be connected to the Sensor via SSH.

Devices—Existing SSH Key Import

Cisco.com



You Are Here: Devices > Sensor

☑ 1. Select Group
□ 2. Enter Sensor Information
□ 3. Sensor Information

Enter Sensor Information

Identification

IP Address:* 10.0.1.4

NAT Address:

Sensor Name (required if not Discovering Settings): sensor

Discover Settings: ☑

SSH Settings:

User ID:* cisco

Password: (or pass phrase if using existing SSH keys):* ********

Use Existing SSH keys: ☑

Note: * - Required Field

- Step 2 of 3 -

Enter the sensor identification settings here. You may check **Discover Settings** to retrieve the sensor settings information from the device.

If using Security Monitor you may need to set NAT to MC in Remote Hosts table.

Opening page s511.do at 10.0.1.12 (secure Web site)...

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—12-11

Step 4 Complete the following sub-steps to import a Sensor into the IDS MC using existing SSH keys:

1. Choose **Devices>Sensors>Add**. The Select Sensor Group page is displayed.
2. Select the group you are going to import the Sensor into and click **Next**. The Enter Sensor Information page is displayed.
3. Enter values for settings listed in the following table:

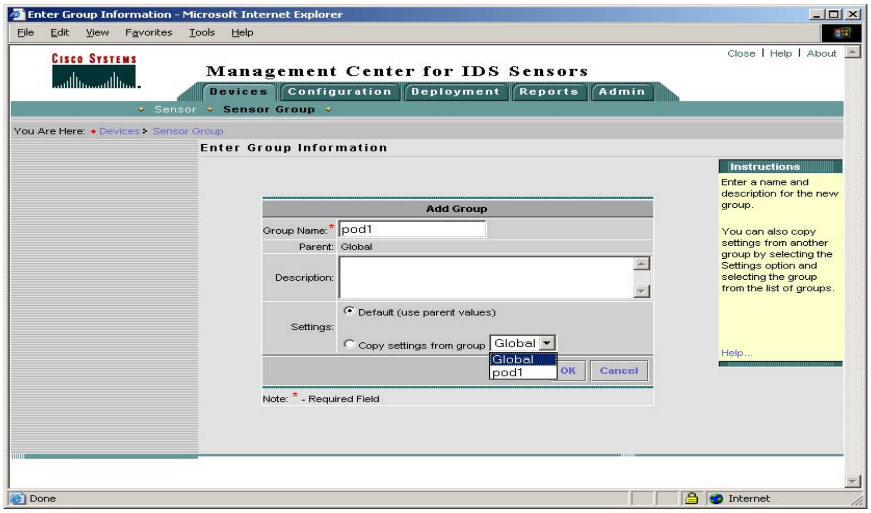
IDS MC Sensor Settings	Description
IP Address	Enter the IP address of the Sensor you want to manage.
NAT Address	(Optional.) Enter the Sensor's NAT address.
Sensor Name	Enter the hostname of the Sensor you want to manage.
Discover Settings	Select this check box to retrieve the Sensor settings information from the device.
User ID	Enter the username that will manage the Sensor. Use the username netrangr when you are using a Sensor appliance with a software version earlier than 4.0. Use the username cisco when you are importing a Sensor with a software version of 4.0 or later. Use the username ciscoids when using an IDSM.
Password	Enter the passphrase that you saved to the private key.
Use Existing SSH Keys	Select this check box to use existing SSH keys.

4. Click **Next**. The Sensor Information page is displayed with an Import Status message that displays the Sensor's name and software version.

Step 5 Click **Finish**. The Sensor page is displayed with the new Sensor.

Devices—Sensor Group

Choose Devices>Sensor Group and **Click** Create Subgroup**.**



Enter Group Information

Add Group

Group Name:* pod1

Parent: Global

Description:

Settings: ● Default (use parent values) ○ Copy settings from group Global

Note: * - Required Field

Instructions

Enter a name and description for the new group.

You can also copy settings from another group by selecting the Settings option and selecting the group from the list of groups.

Enter Group Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Management Center for IDS Sensors
Close | Help | About
Devices Configuration Deployment Reports Admin
Sensor Sensor Group
You Are Here: Devices > Sensor Group
Global
pod1
OK
Cancel
Help...
Done
Internet

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—12-12

The IDS MC uses a hierarchy of groups and Sensors. A group can contain Sensors, other groups, or a combination of Sensors and groups. When you start the IDS MC, you always have at least one active, defined group, the Global group. The IDS MC hierarchy can contain many levels of groups and Sensors, just as a folder in Windows 2000 can contain many levels of folders and files.

The IDS MC hierarchy of groups and Sensors enables you to configure more than one Sensor at a time by configuring an entire group of Sensors simultaneously. Configuring more than one Sensor at a time in this way is possible because a Sensor can acquire settings from its parent group. A Sensor must, in fact, acquire settings from its parent group if a parent defines those settings as mandatory. A child cannot override the values for such settings.

Complete the following steps to add a Sensor sub-group to the Global Group of the IDS MC:

Step 1 Choose **Devices>Sensor Group**. The Select Sensor Group page appears.

Step 2 Select the Global group and click **Create Subgroup**. The Enter Group Information page is displayed.

Step 3 Enter values for settings listed in the following table:

IDS MC Group Settings	Description
Group Name	Enter a group name to use for the subgroup that you are about to create.
Description	(Optional.) Enter an optional description.
Settings	Select the **Defaults (use parent values)** radio button to use the group parent configuration settings or the **Copy settings from group** radio button.

Note When you create subgroups, the subgroup inherits the properties of either the parent group or you may copy settings from another group to the new subgroup.

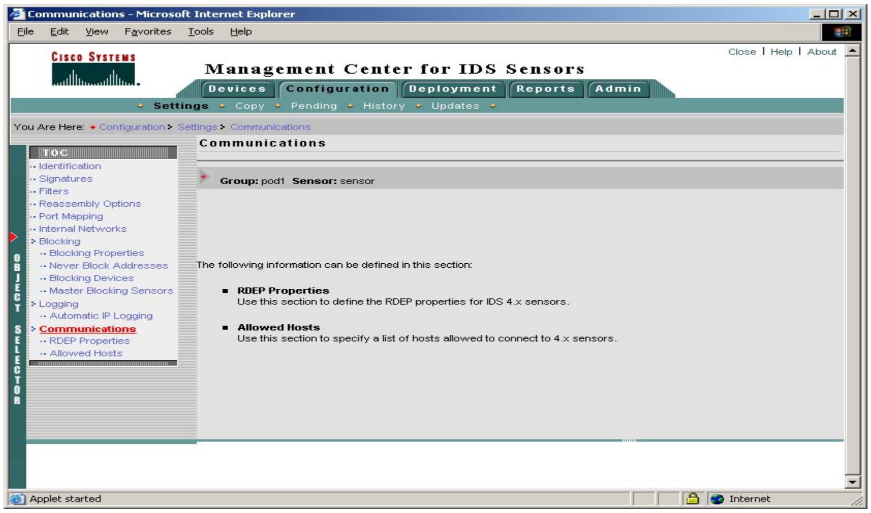
Step 4 Click **OK**. The Select Sensor Group page is displayed with the new Sensor subgroup.

Communications

This section introduces the Sensor settings used for communications, the Remote Data Exchange Protocol (RDEP) protocol and allowed host settings.

Sensor Communications

Choose Settings>Communications**.**



Communications

Group: pod1 **Sensor:** sensor

The following information can be defined in this section:

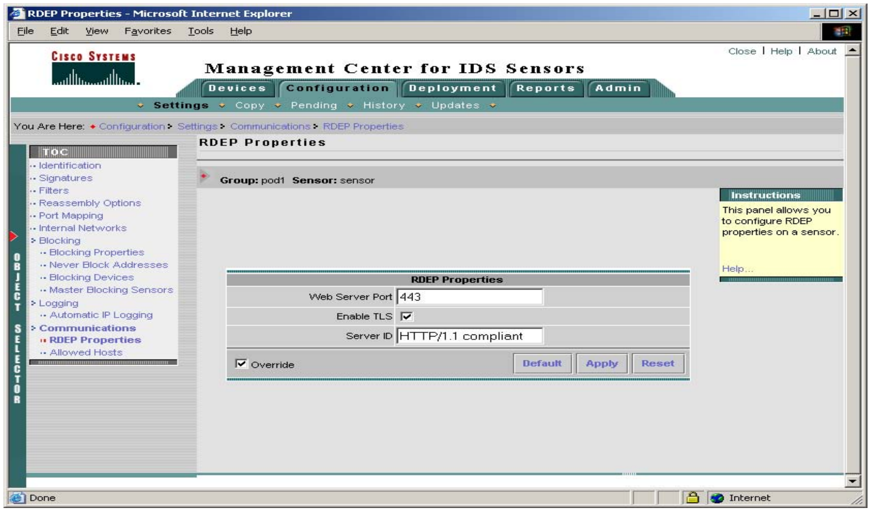
- **RDEP Properties**
  Use this section to define the RDEP properties for IDS 4.x sensors.
- **Allowed Hosts**
  Use this section to specify a list of hosts allowed to connect to 4.x sensors.

CSIDS 4.0—12-14

Choose **Configuration>Settings>Communications** to see what communication settings you may change on the Sensor.

Sensor Communications—RDEP

Choose Configuration>Settings>Communications>RDEP Properties**.**



RDEP Properties

Group: pod1 **Sensor:** sensor

This panel allows you to configure RDEP properties on a sensor.

RDEP Properties

Web Server Port	443
Enable TLS	☑
Server ID	HTTP/1.1 compliant

☑ Override

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—12-15

Version 4.x of the IDS Sensor software uses the Remote Data Exchange Protocol (RDEP) instead of PostOffice, which is used by earlier versions. RDEP, a subset of the HTTP/1.1 protocol, uses a client request and server response model. The IDS MC does not use RDEP itself to communicate with the Sensor. However, it does allow you to configure the RDEP properties on the Sensor.

Complete the following steps to configure the RDEP protocol settings:

Step 1 Choose **Configuration>Settings>Communications>RDEP Properties**. The RDEP Properties page is displayed.

Step 2 Enter a new port number that the web server listens and responds on in the Web Server Port field.

Step 3 Select or de-select the **Enable Transaction Layer Security (TLS)** check box.

Note TLS provides cipher and secret key negotiation, session privacy and integrity, and server authentication. It enables a secure exchange of data between the RDEP server and RDEP client.

Step 4 Enter the server identification in the Server ID field to identify the web server on the Sensor.

Step 5 Click **Apply**. The RDEP Properties page is refreshed to indicate the IDS MC received the changes.

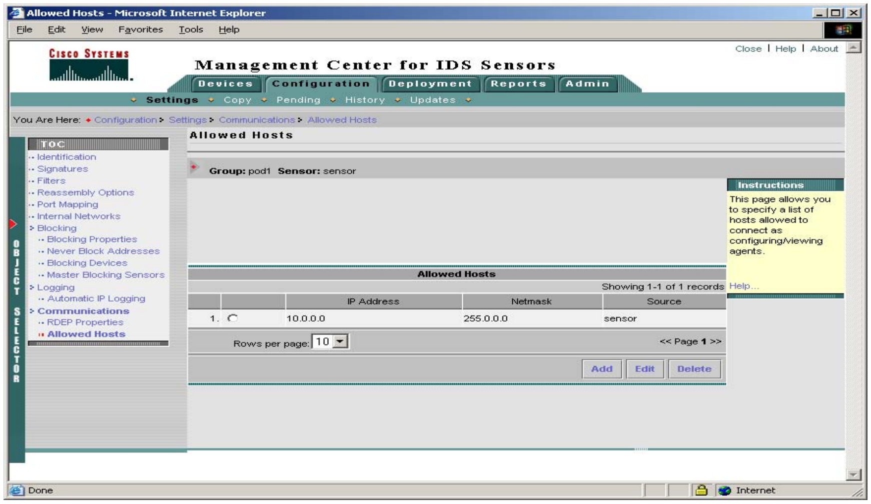
Step 6 Click **Reset** to discard your changes and restore the previous settings.

Note Click the **Default** button to reset the RDEP properties to their factory default values. Click the **Reset** button to discard any changes you have made and restore previous settings.

Sensor Communications—Allowed Hosts

Cisco.com

Choose Configuration>Settings>Communications>Allowed Hosts**.**



Allowed Hosts

Group: pod1 **Sensor:** sensor

This page allows you to specify a list of hosts allowed to connect as configuring/viewing agents.

Allowed Hosts

Showing 1-1 of 1 records

		IP Address	Netmask	Source
1.	○	10.0.0.0	255.0.0.0	sensor

During the initial setup of a Sensor, you are prompted to configure hosts or networks that are allowed to connect to and configure the Sensor. You may edit the list of networks or hosts that are allowed to connect to the Sensor.

Note If you are importing a Sensor with software version 4.0 or greater that has no previous configuration, all hosts on the local network are allowed to configure the Sensor. For security purposes, you want to turn this feature off and configure specific hosts to connect to the Sensor.

Complete the following steps to configure the Sensor to allow specific hosts:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Select **Communications>Allowed Hosts**. The Allowed Hosts page is displayed.

Step 3 Click **Add**. The Enter Allowed Host page is displayed.

Step 4 Enter the IP address of the allowed host in the IP Address field.

Note If the allowed host is using a NAT address, enter the NAT IP address.

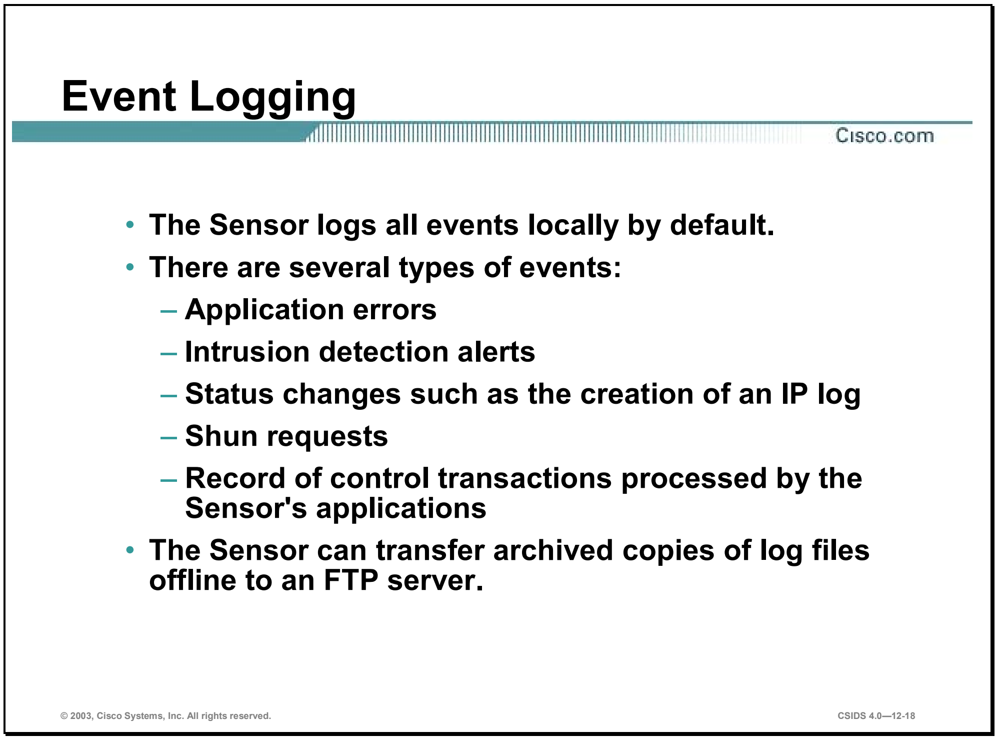
Step 5 Enter the network mask of the allowed host in the Net Mask field.

Step 6 Click **OK**. The Allowed Hosts page is displayed with the new allowed host.

Step 7 You may also delete any Allowed Hosts by selecting the radio button next to the host and clicking **Delete**.

Logging

This section explains the logging capabilities of the Sensor and how to configure logging settings via the IDS MC.



Event Logging

Cisco.com

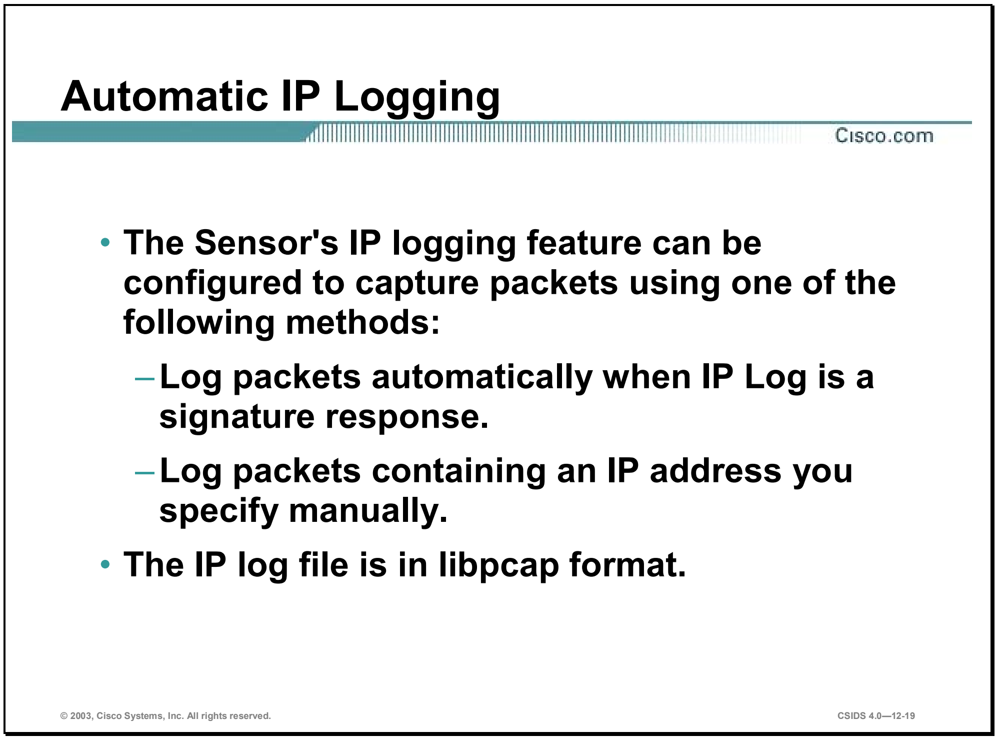
- The Sensor logs all events locally by default.
- There are several types of events:
  - Application errors
  - Intrusion detection alerts
  - Status changes such as the creation of an IP log
  - Shun requests
  - Record of control transactions processed by the Sensor's applications
- The Sensor can transfer archived copies of log files offline to an FTP server.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—12-18

The Sensor's logging service is enabled by default, and the Sensor logs events locally. The events logged may be any of the following types:

- evError events—Application errors
- evAlert—Intrusion detection alerts
- evStatus—Status changes such as the creation of an IP log
- evShunRqst—Shun requests
- evLogTransaction—Record of control transactions processed by the Sensor's applications

All events are stored locally on the Sensor in the Event Store. Management consoles such as IEV and the Security Monitor can pull events occurring after a time you specify. Whether events are pulled to a management console or not, they remain on the Sensor until the 4-GB limit is reached.



Automatic IP Logging

Cisco.com

- The Sensor's IP logging feature can be configured to capture packets using one of the following methods:
  - Log packets automatically when IP Log is a signature response.
  - Log packets containing an IP address you specify manually.
- The IP log file is in libpcap format.

CSIDS 4.0—12-19

The IP logging feature provides the ability to capture raw, unaltered IP packets. IP logs differ from alarms. They are copies of the binary packets that the Sensor sees on the network. Information from IP logs can be used for confirmation, damage assessment, and forensic evidence.

You can configure a Sensor to automatically generate an IP log when it detects an attack. Both attacker and victim addresses are added to the iplog list, and all traffic going to and from these addresses is logged for a configured period of time. If you want the Sensor to take this action, you must specify it when you configure individual signatures. You must specify how long, in minutes, IP logging will occur when the Sensor detects an attack. You can also specify the maximum number of packets or bytes to be logged. If duration, packets, and bytes are entered, logging terminates whenever the first limit (duration, packets, or bytes) is met. You can configure signatures and automatic IP logging parameters via the IDS MC or the CLI.

Note This chapter explains how to configure IP logging parameters in the IDS MC. Signature configuration is explained later in the course.

You can also use the CLI or IDM to configure the generation of IP log files for specific IP addresses. This causes the Sensor to log all traffic going to and from the specified address whether there is an attack or not.

One of the largest problems with storing information to a fixed resource like a hard drive or memory is handling all the error conditions properly. The IDS IP logging design ensures that there is always room to write a new IP log file.

When the Sensor starts, it sets up a re-usable ring of files for IP logging. After 2 GB of logs have been logged, it starts re-using these files. The Sensor re-uses files by overwriting the file with the oldest closing time. A file is closed when it reaches its configured expiry or when its full size has been used. Since the files are pre-allocated, there is no reason to delete them; however, remember that IP logging does impact performance.

Note The 2 GB limit mentioned above may vary from platform to platform.

You can use the CLI's **iplog-status** command to verify that IP logs are being created and display a description of the available IP log contents. IP log files can be retrieved from the Sensor before or after they are closed. If you try to retrieve an IP log before the file closes, you get all parts of any packet, but you may not get the last couple of packets. IP log files can be retrieved by the following methods:

- Use the CLI **copy** command to copy the IP log files to another host system using FTP or SCP.
- Download the IP log files via IDM.

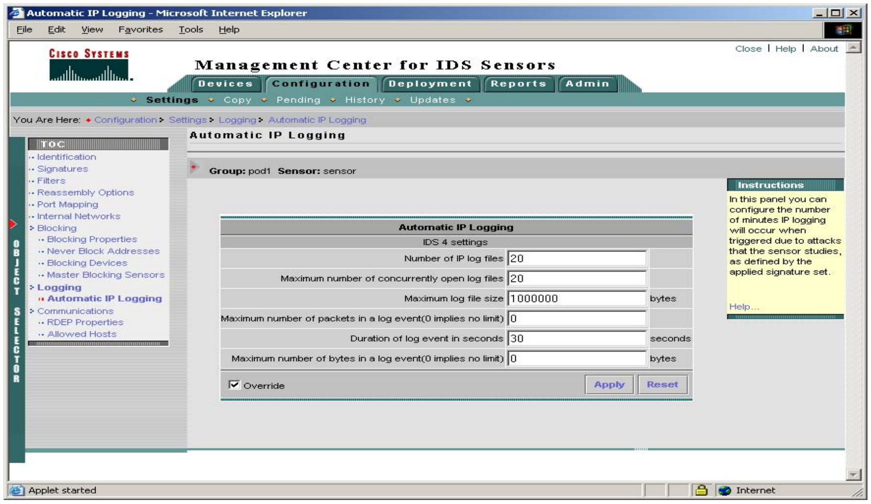
After retrieving the IP log files, you can use a network protocol analyzer to examine the data. You can use Ethereal, tcpdump, or any other reader that understands libpcap format. Libpcap format contains the data of the captured packets in binary form and is a standard used by network tools such as WinDump, Ethereal and Snort.

Caution Because of its impact on performance, IP logging should only be used temporarily for such purposes as attack confirmation, damage assessment, or forensic evidence.

Automatic IP Logging

Cisco.com

Choose Configuration>Settings>Logging>Automatic IP Logging**.**



Automatic IP Logging

Group: pod1 **Sensor:** sensor

Automatic IP Logging

IDS 4 settings

Number of IP log files	20	
Maximum number of concurrently open log files	20	
Maximum log file size	1000000	bytes
Maximum number of packets in a log event(0 implies no limit)	0	
Duration of log event in seconds	30	seconds
Maximum number of bytes in a log event(0 implies no limit)	0	bytes

☑ Override Apply Reset

Instructions

In this panel you can configure the number of minutes IP logging will occur when triggered due to attacks that the sensor studies, as defined by the applied signature set.

Help...

The IDS MC allows you to edit the Automatic IP Logging properties of Sensors. By editing the Automatic IP Logging properties, you are changing the way the Sensor logs IP sessions when it detects an attack. If you want the Sensor to automatically log IP sessions, you must specify this when you configure individual signatures.

Complete the following steps to edit automatic IP logging:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Select **Logging>Automatic IP Logging** from the TOC. The Automatic IP Logging page is displayed.

Note Since these settings are configurable at the group level, individual Sensor settings are grayed out. You must select the Override check box to edit the settings on the individual Sensor.

Step 3 Enter values for settings listed in the following table:

IDS MC Automatic IP Logging Settings	**Description**
Number of IP log files	The number of IP log files the Sensor will log IP session information into. The default is 20.
Maximum number of concurrently open log files	The number of concurrent log files into which the Sensor will log IP session information. The default is 20.
*Maximum log file size	Maximum size of the IP log file. The default is 1,000,000 bytes.
*Maximum number of packets in a log event (0 implies no limit)	Maximum number of packets that will be logged in an event. The default is 0.
*Duration of log in seconds.	Duration the IP session information is logged. The default is 30 seconds.

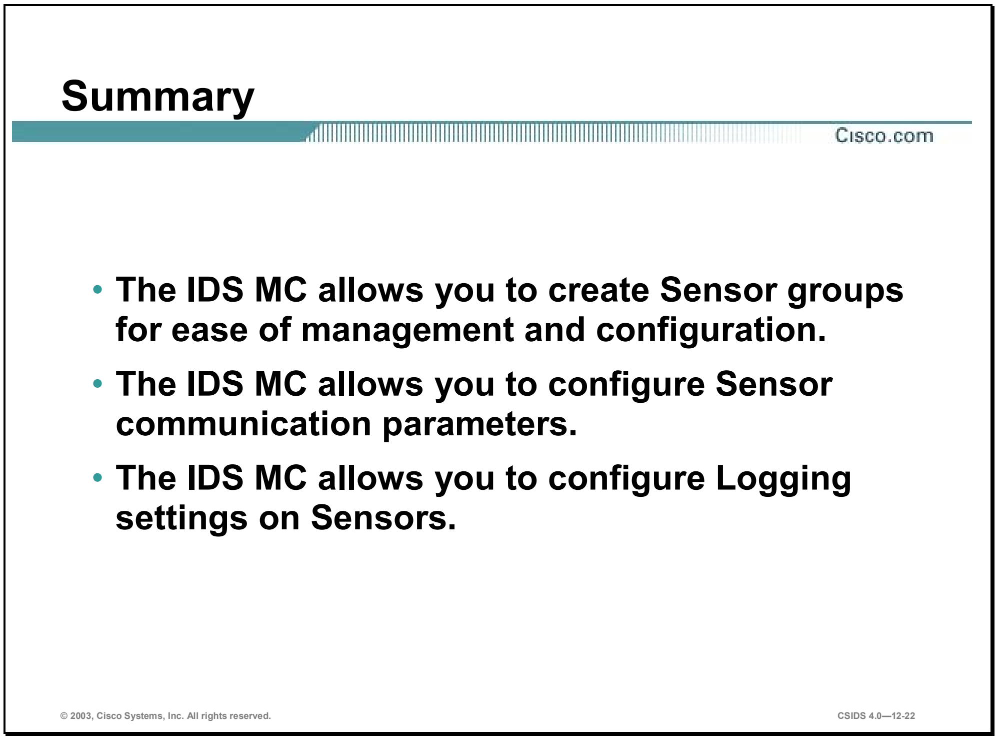
Note The defaults settings are recommended for most scenarios. There is rarely a need to modify these settings. If you do make changes, you should limit them to decreasing the value of those marked with an asterisk.

Step 4 Click **Apply**. The Automatic IP Logging page is refreshed to indicate that the IDS MC received the changes.

Note The Signature's Log setting must be enabled to allow the Sensor to log IP Session information during an attack.

Summary

This section summarizes what you learned in the chapter.



Summary

- The IDS MC allows you to create Sensor groups for ease of management and configuration.
- The IDS MC allows you to configure Sensor communication parameters.
- The IDS MC allows you to configure Logging settings on Sensors.

Lab Exercise—Sensor Configuration

Complete the following lab exercise to practice what you learned in this chapter.

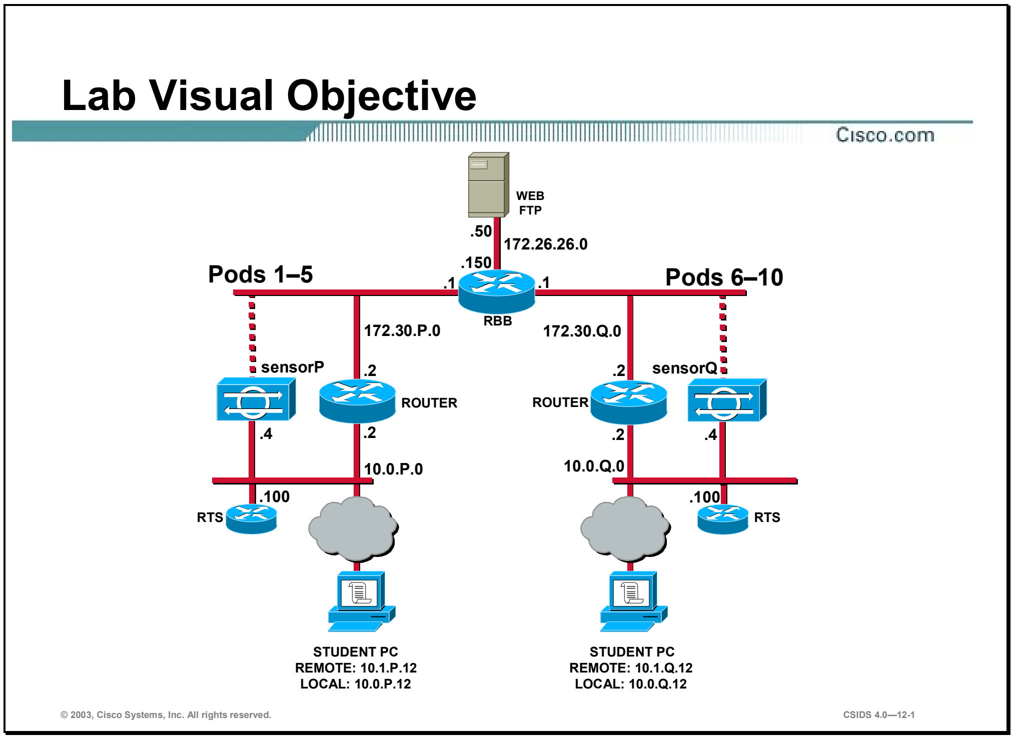
Objectives

In this lab exercise you will complete the following tasks:

- Add the Sensor to the IDS MC.
- Create Sensor groups and organize IDS devices.
- Configure RDEP communication settings.
- Deploy configurations to Sensors.
- Create a configuration deployment report.
- Test your configuration.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—12-1

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab exercise.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor. Make sure to replace it with your peer's pod number.

Task 1—Add the Sensor to the IDS MC

Complete the following steps to import a Sensor to the IDS MC:

Step 1 Choose **Devices>Sensor** from within the IDS MC. The Global Sensor Group is displayed.

Step 2 Click **Add**. The Select Sensor Group page is displayed.

Step 3 Select the **Global** group and click **Next**. The Enter Sensor Information page is displayed.

Step 4 Enter the Sensor information settings by completing the following sub-steps:

1. Enter your Sensor's IP address, **10.0.P.4**, in the IP Address field. (where P = pod number)

2. Select the **Discover Settings** check box.

3. Enter **admin** in the User ID field.

4. Enter **adminpass** in the Password field.

Step 5 Click **Next**. The Sensor Information page is displayed with the import status. The import should succeed.

Note It will take 5-15 seconds for the Sensor to discover the new settings, depending on the speed of your network and the version of your Sensor hardware. Please be patient.

Note If you enter the wrong password or username when attempting to discover the Sensor using the IDS MC, you will receive an error message indicating that system exec did not complete within watchdog time.

Step 6 Click **Finish**. The Sensor, sensorP, is listed on the Sensor page.

(where P = pod number)

Task 2—Create Sensor Groups and Organize IDS Devices

This task involves creating a Sensor group and assigning the IDS device group properties to the new group. Complete the following steps to create groups and organize IDS devices:

Step 1 Choose **Devices>Sensor Group** from within the IDS MC. The Select Sensor Group page is displayed.

Step 2 Select the **Global** group and click the **Create Subgroup** button. The Enter Group Information page is displayed.

Step 3 Enter **podP** in the Group Name field.

(where P = pod number)

Step 4 Enter a description in the Description field.

Step 5 Select the **Default (use parent values)** radio button within the Settings group box.

Step 6 Click **OK**. The podP group appears within the Select Sensor Group page.

(where P = pod number)

Step 7 Choose **Configuration>Settings** from the IDS MC. The Settings page is displayed.

Step 8 Click the **Object Selector** handle and select **sensorP**. The Sensor, sensorP, is displayed in the Settings page. Notice the Sensor's current group is Global.

(where P = pod number)

Step 9 Select **Identification** from the table of contents (TOC). The Identification page is displayed.

Step 10 Choose **podP** from the Group drop-down menu.

(where P = pod number)

Step 11 Enter the comment, **My Sensor**, in the Comment field. The comment is used to provide a description of the Sensor.

Step 12 Click **Apply**. The Identification page refreshes indicating that the IDS MC received the change. Notice that the Sensor, sensorP, now belongs to the Group, podP.

(where P = pod number)

Task 3—Configure RDEP Communication Settings

This task involves verifying that the RDEP communication settings are properly configured and a host on your subnet may access the Sensor and configure it with the IDS MC or IDM.

Step 1 Select **podP** by using the Object Selector.

Step 2 Choose **Configuration>Settings**. The Settings page is displayed.

Step 3 Choose **Communications>RDEP Properties** from the TOC. The RDEP Properties page is displayed.

Step 4 Verify the RDEP Properties settings by completing the following sub-steps:

1. Verify that 443 appears in the Web Server Port field.
2. Verify that the Enable TLS check box is selected.
3. Verify that HTTP/1.1 compliant appears in the Server ID field.

Step 5 Choose **Communications>Allowed Hosts** from the TOC. The Allowed Hosts page is displayed.

Step 6 Click **Add**. The Enter Allowed Host page is displayed.

Step 7 Enter the IP address of your peer's student PC, **10.0.Q.12**, in the IP Address field.

(where Q = peer pod number)

Step 8 Enter **255.255.255.255** in the Net Mask field.

Step 9 Click **OK**. The Allowed Hosts page is displayed with the new allowed host.

Task 4—Deploy Configurations to Sensors

Complete the following steps to deploy a configuration to your Sensor:

Step 1 Choose **Configuration>Pending**. The Pending page is displayed.

Step 2 Select all pending configuration changes by selecting their respective check boxes.

Step 3 Click **Save**. The Pending page refreshes.

Step 4 Choose **Deployment>Generate**. The Generate page is displayed.

Step 5 Select the **Global** check box.

Step 6 Click **Generate**. The Generate Status page is displayed with the configuration generation status.

Step 7 Choose **Deployment>Deploy>Submit**. The Submit page is displayed.

Step 8 Select the **Global** check box.

Step 9 Click **Deploy**. The Select Configurations page is displayed.

Step 10 Choose the configurations that you wish to deploy by selecting their respective check boxes.

Step 11 Click **Next**. The Enter Job Properties page is displayed.

Step 12 Enter **SensorDeployment** in the Job Name field and verify that the Immediate radio button is selected.

Step 13 Click **Finish**. The Submit page is displayed.

Note The time needed to deploy configuration changes will vary, and depends on the number of configuration changes made.

Task 5—Create a Deployment Report

Complete the following steps to create a deployment report:

Step 1 Choose **Reports>Generate**. The Select Report page is displayed.

Step 2 Select **Sensor Configuration Deployment Report** from the list of available reports to run and click **Selec**t. The Report Filtering page is displayed.

Step 3 Click the **Select All** button in the Event Severity group box.

Step 4 Click the **Select All** button in the Devices group box.

Step 5 Click **Next**. The Schedule Report page is displayed.

Step 6 Click **Finish**. The Notifications window opens and indicates the report will be available to view when it has been generated.

Step 7 Click **OK**. The Report View page is displayed.

Step 8 Choose **Reports>View** to refresh the View page.

Step 9 Select your report's check box and click **View**. The Report page is displayed with the generated report.

Task 6—Test Your Configuration

Complete the following steps to test your Sensor's configuration:

Step 1 Establish an SSH session to your peer pod's Sensor and log in with the administrator account, **admin**, and password, **adminpass**. Access to your peer pod's Sensor should be allowed.

Step 2 Attempt to establish an SSH session to another peer pod's Sensor. Access should be denied because your network address is not defined in the list of allowed hosts.

Cisco Intrusion Detection System Alarms and Signatures

Overview

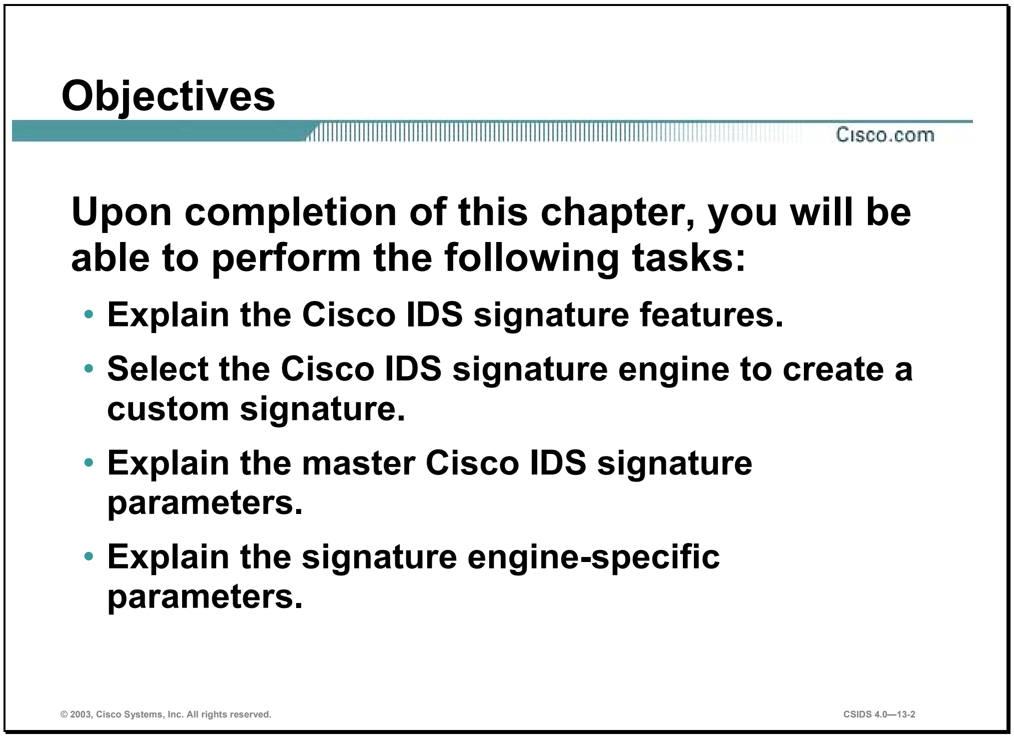
This chapter discusses how alarms and signatures are implemented in Cisco Intrusion Detection System (IDS) Sensors. The Cisco IDS signature engines usage and selection is explained. This chapter includes the following topics:

- Objectives
- Cisco IDS signatures
- Cisco IDS alarms
- Cisco IDS signature engines
- Atomic signature engines
- Flood signature engines
- Service signature engines
- State signature engines
- String signature engines
- Sweep signature engines

- Miscellaneous signature engines
- Signature engine selection
- Summary

Objectives

This section lists this chapter’s objectives.



Objectives

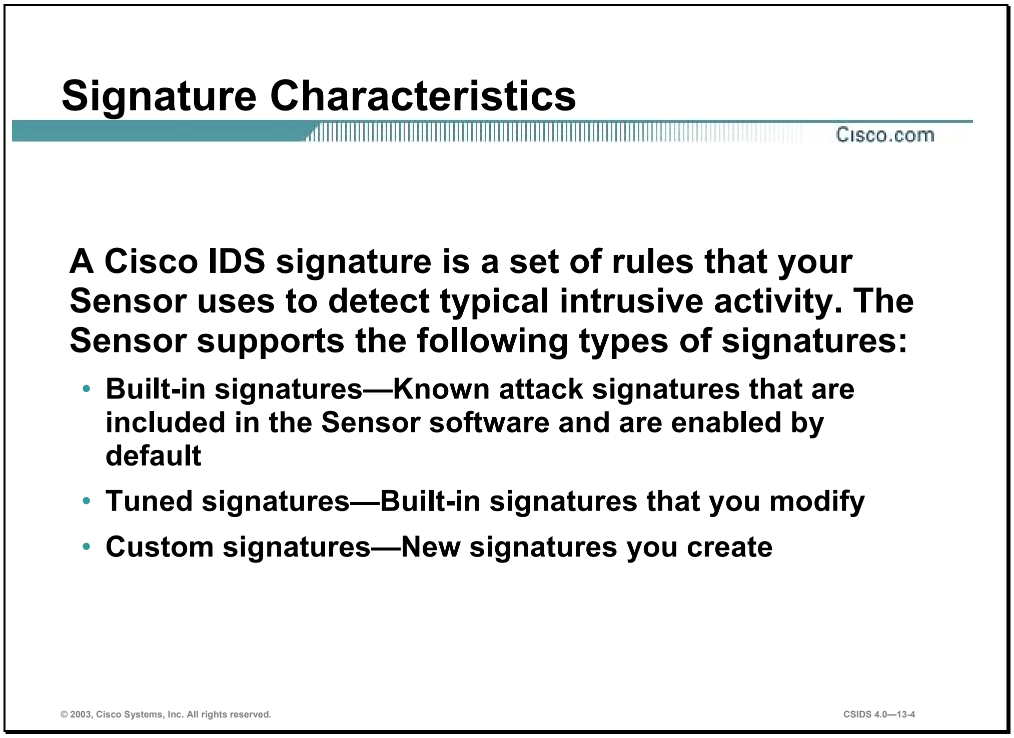
Upon completion of this chapter, you will be able to perform the following tasks:

- Explain the Cisco IDS signature features.
- Select the Cisco IDS signature engine to create a custom signature.
- Explain the master Cisco IDS signature parameters.
- Explain the signature engine-specific parameters.

CSIDS 4.0—13-2

Cisco IDS Signatures

This section highlights the features and capabilities of Cisco IDS signatures.



Signature Characteristics

Cisco.com

A Cisco IDS signature is a set of rules that your Sensor uses to detect typical intrusive activity. The Sensor supports the following types of signatures:

- **Built-in signatures—Known attack signatures that are included in the Sensor software and are enabled by default**
- **Tuned signatures—Built-in signatures that you modify**
- **Custom signatures—New signatures you create**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-4

A signature is a set of rules that your Sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. As Sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

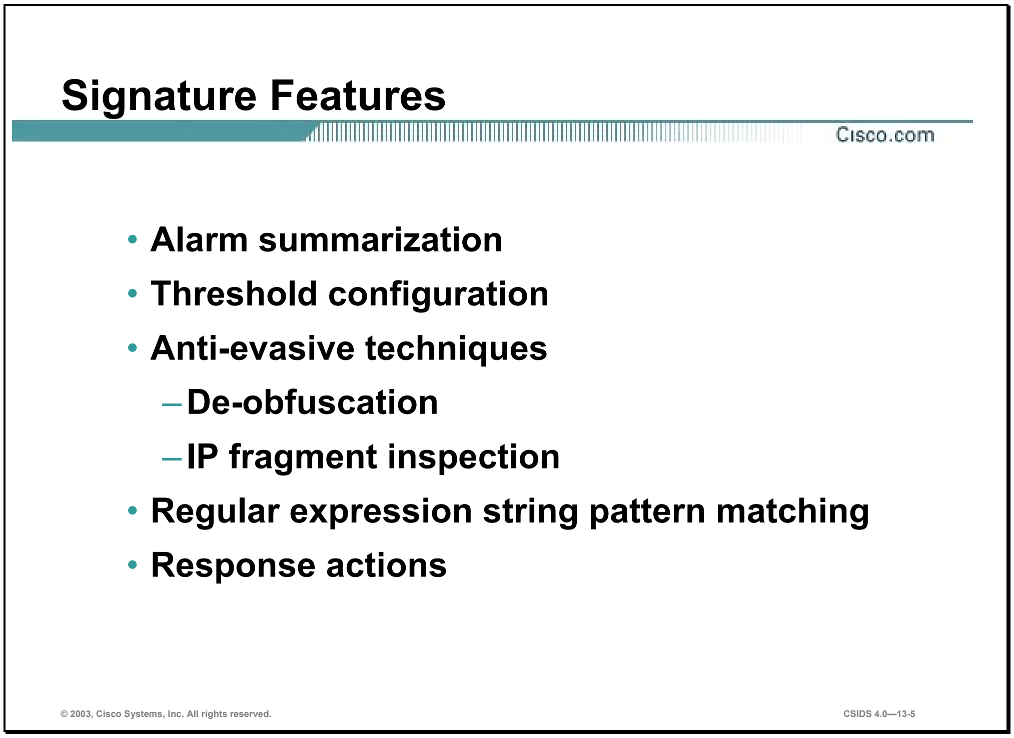
The Sensor compares the list of signatures with network activity. When a match is found, the Sensor logs an event. A Sensor enables you to modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your Sensors.

You must enable the signature to configure a Sensor to monitor network traffic for a particular signature. The most critical signatures are enabled by default. When an attack is detected that matches an enabled signature, the Sensor generates an alert event and stores it in the Event Store. The alert events, as well as other events, may be retrieved from the Event Store by web-based clients. The Sensor logs all informational alarms or higher by default.

Some signatures have sub-signatures. This means that the signature is divided into sub-categories. When you configure a sub-signature, changes made to the parameters of one sub-signature apply only to that sub-signature.

Built-in signatures are known attack signatures that are included in the Sensor software and are enabled by default. You cannot add to or delete from the list of built-in attack signatures. You also cannot rename them. You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called tuned signatures. You can also create new signatures, which are called custom signatures.



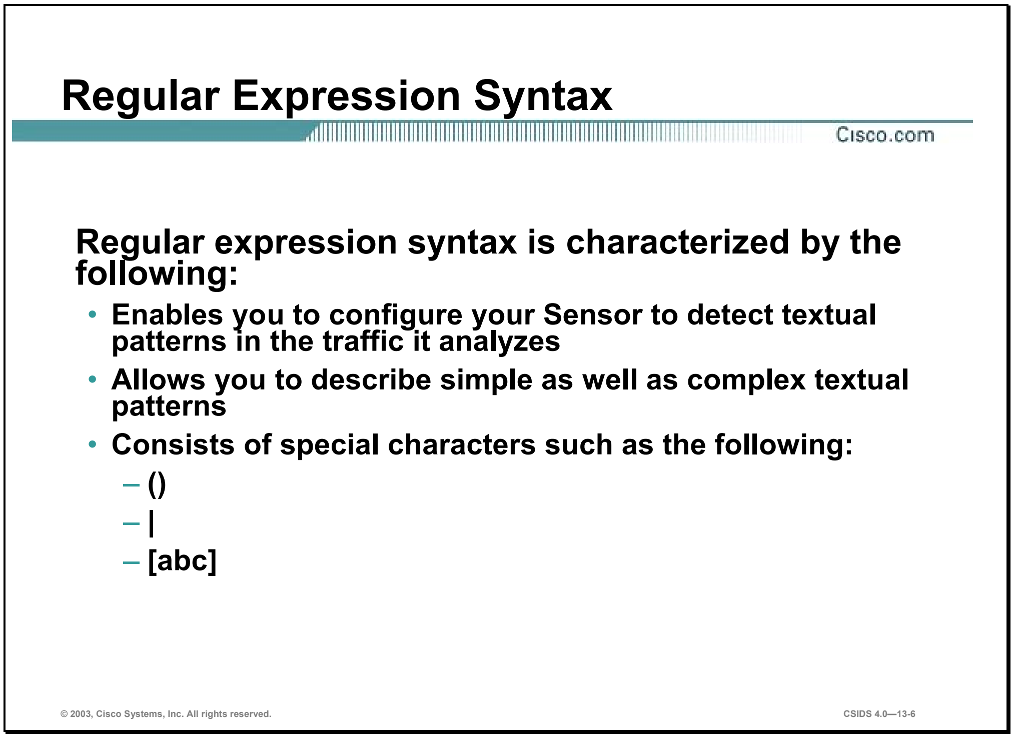
Signature Features

- Alarm summarization
- Threshold configuration
- Anti-evasive techniques
  - De-obfuscation
  - IP fragment inspection
- Regular expression string pattern matching
- Response actions

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-5

The Cisco IDS signatures have the following features and capabilities:

- Alarm summarization—This feature enables the Sensor to aggregate alarms to limit the number of times an alarm is sent when the signature is triggered.
- Threshold configuration—This capability enables a signature to be tuned to perform optimally in a network.
- Anti-evasive techniques—This feature enables a signature to defeat evasive techniques used by an attacker. The anti-evasive techniques used are de-obfuscation and IP fragment inspection.
- Regular expression string pattern matching—This capability enables the creation of string patterns using regular expressions.
- Response actions—This capability enables the Sensor to take an action when the signature is triggered.



Regular Expression Syntax

Cisco.com

Regular expression syntax is characterized by the following:

- **Enables you to configure your Sensor to detect textual patterns in the traffic it analyzes**
- **Allows you to describe simple as well as complex textual patterns**
- **Consists of special characters such as the following:**
  - **()**
  - **|**
  - **[abc]**

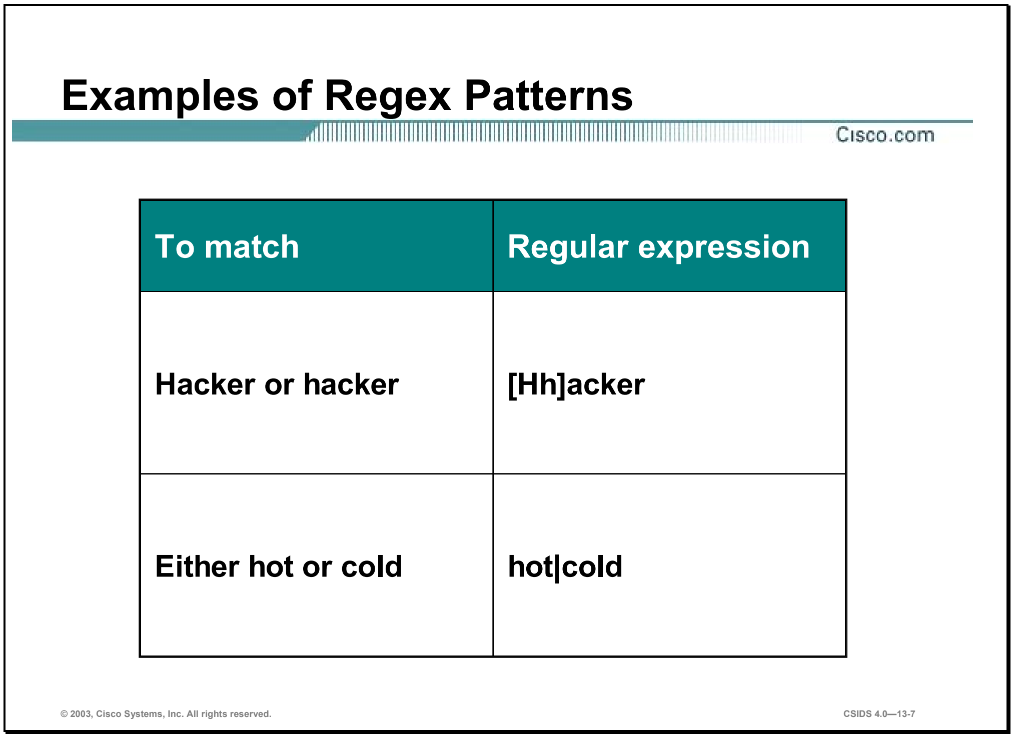
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-6

Regular expressions (Regex) constitute a powerful and flexible notational language that allows you to describe text. In the context of pattern matching, regular expressions allow a succinct description of almost any arbitrary pattern. The following table lists the IDS regular expression syntax:

Metacharacter	Name	Description
?	Question mark	Repeat 0 or 1 time
*	Star, asterisk	Repeat 0 or more times
+	Plus	Repeat 1 or more times
{x}	Quantifier	Repeat exactly X times
{x,}	Minimum quantifier	Repeat at least X times
.	Dot	Any one character except new line (0x0A)
[abc]	Character class	Any character listed
[^abc]	Negated character class	Any character not listed
[a-z]	Character range class	Any character listed inclusively in the range
( )	Parenthesis	Used to limit the scope of other metacharacters
|	Alternation, or	Matches either expression it separates
^	Caret	The beginning of the line
\char	Escaped character	When char is a metacharacter or not, matches the literal char
char	Character	When char is not a metacharacter, matches the literal char
\r	Carriage return	Matches the carriage return character (0x0D)
\n	New line	Matches the new line character (0x0A)
\t	Tab	Matches the tab character (0x09)

Metacharacter	Name	Description
\f	Form feed	Matches the form feed character (0x0C)
\xNN	Escaped hexadecimal character	Matches character with the hexadecimal code 0xNN (where 0<=N<=F)
\NNN	Escaped octal character	Matches the character with the octal code NNN (where 0<=N<=8)



Examples of Regex Patterns

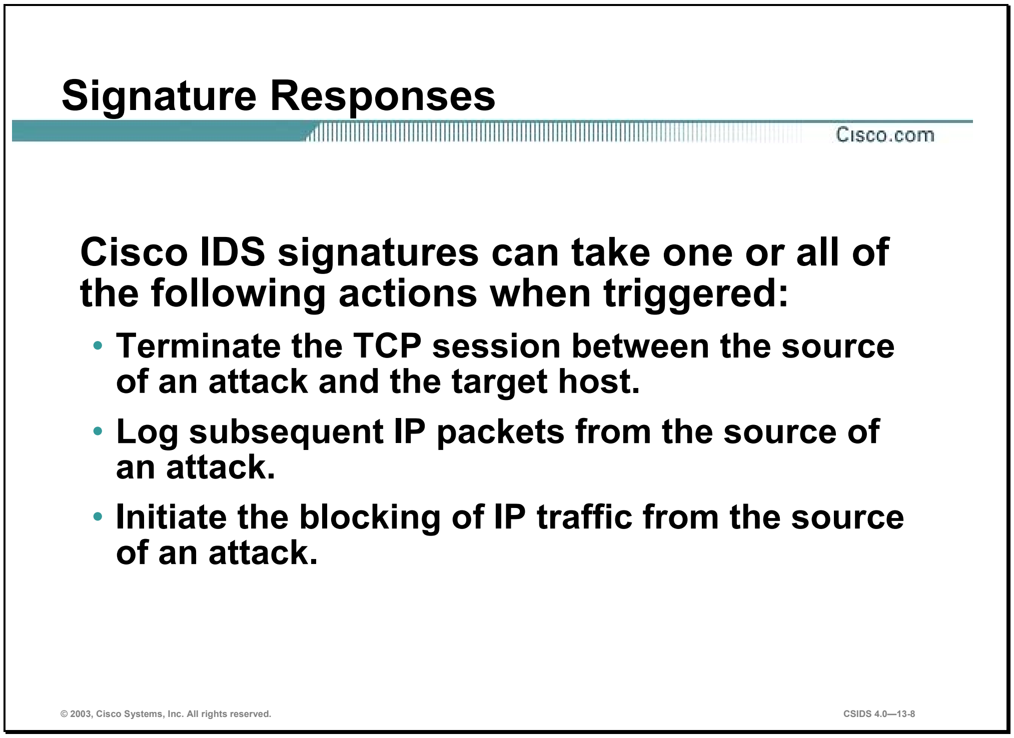
Cisco.com

To match	Regular expression
Hacker or hacker	**[Hh]acker**
Either hot or cold	**hot|cold**

CSIDS 4.0—13-7

The following table shows examples of Regex patterns:

To Match	Regular expression
Hacker	Hacker
Hacker or hacker	[Hh]acker
Variations of bananas, bananananas, bananananananas	ba(na)+s
The words hot and cold on the same line with anything except a new line between them	hot.*cold
Either hot or cold	hot|cold
Either moon or soon	(m|s)oon



Signature Responses

Cisco.com

Cisco IDS signatures can take one or all of the following actions when triggered:

- **Terminate the TCP session between the source of an attack and the target host.**
- **Log subsequent IP packets from the source of an attack.**
- **Initiate the blocking of IP traffic from the source of an attack.**

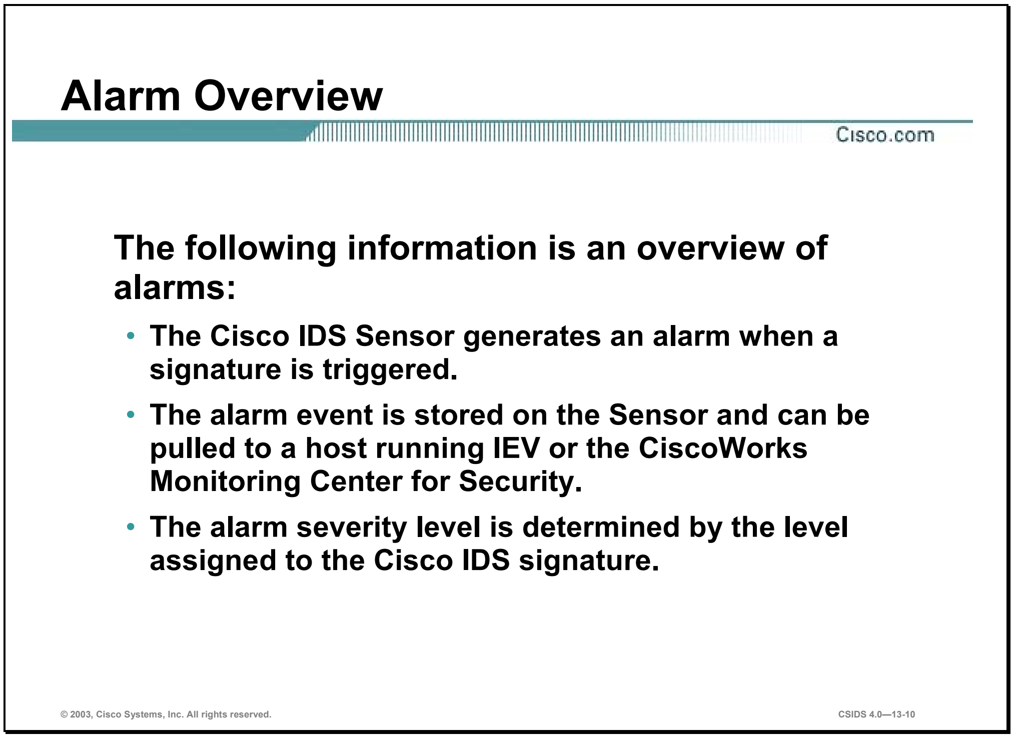
CSIDS 4.0—13-8

Cisco IDS signatures can take one or all of the following actions when triggered:

- TCP reset—Terminates the TCP session between the source of an attack and the target host
- IP log—Logs subsequent IP packets from the source of an attack
- Block—Initiates the blocking of IP traffic from the source of an attack, either a block on the host or the connection

Cisco IDS Alarms

This section discusses the relationship between Cisco IDS signatures and alarms.



Alarm Overview

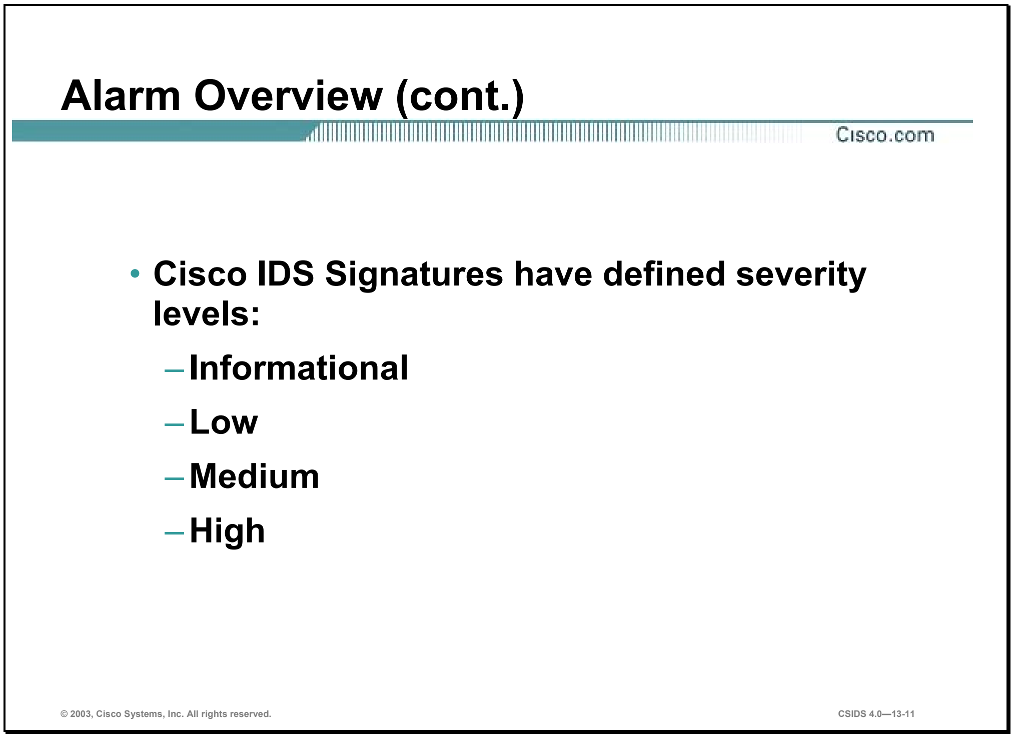
The following information is an overview of alarms:

- **The Cisco IDS Sensor generates an alarm when a signature is triggered.**
- **The alarm event is stored on the Sensor and can be pulled to a host running IEV or the CiscoWorks Monitoring Center for Security.**
- **The alarm severity level is determined by the level assigned to the Cisco IDS signature.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-10

The following information is an overview of alarms for Cisco IDS Sensors:

- The Sensor generates an alarm when an enabled signature is triggered.
- Alarms are stored on the Sensor and a host can pull the alarms off of the Sensor. Pulling alarms from a Sensor allows multiple hosts to subscribe to the event “feed”. This allows a host or hosts to subscribe on an as-needed basis.
- The level assigned to the signature determines the alarm severity level. When tuning a signature, you may assign a severity level to signature, which in turn will make the alarm the same severity level as that of the signature.



Alarm Overview (cont.)

Cisco.com

- Cisco IDS Signatures have defined severity levels:
  - Informational
  - Low
  - Medium
  - High

© 2003, Cisco Systems, Inc. All rights reserved.

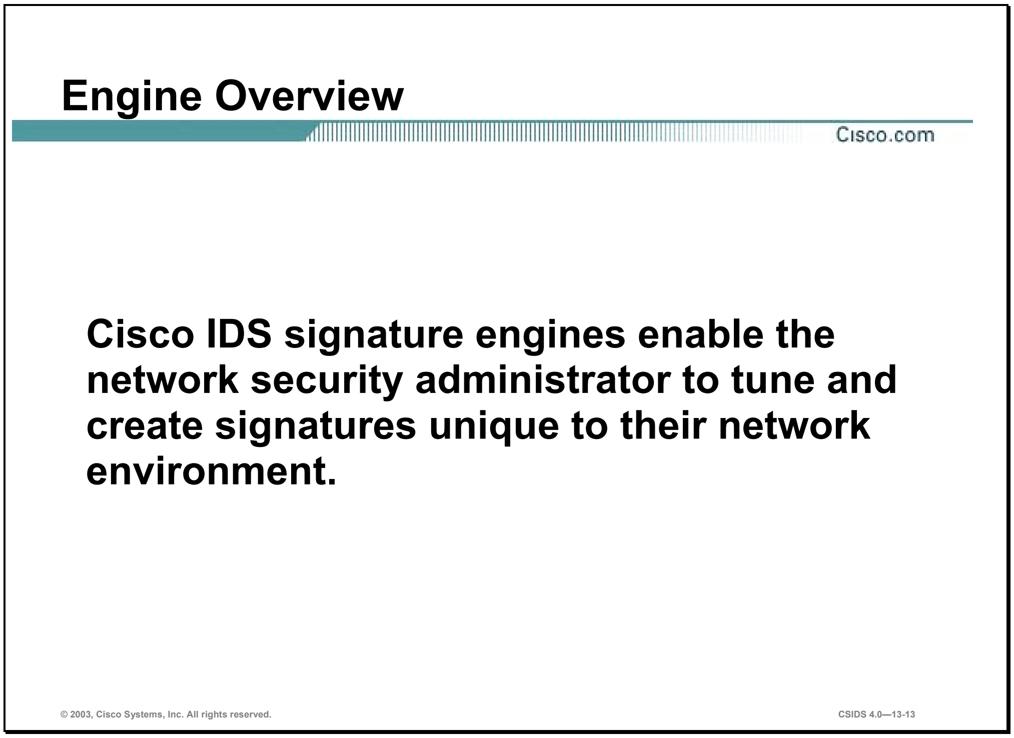
CSIDS 4.0—13-11

A Cisco IDS signature can have one of the following severity levels:

- Informational—Activity that triggered the signature is not considered an immediate threat, but does provide useful information.
- Low—Abnormal network activity was detected that could be perceived as malicious, but an immediate threat is not likely.
- Medium—Abnormal network activity was detected that could be perceived as malicious, and an immediate threat is likely.
- High—Attacks used to gain access or cause a DoS were detected, and an immediate threat is extremely likely.

Cisco IDS Signature Engines

This section introduces the signature engines used by Sensors.



Engine Overview

Cisco.com

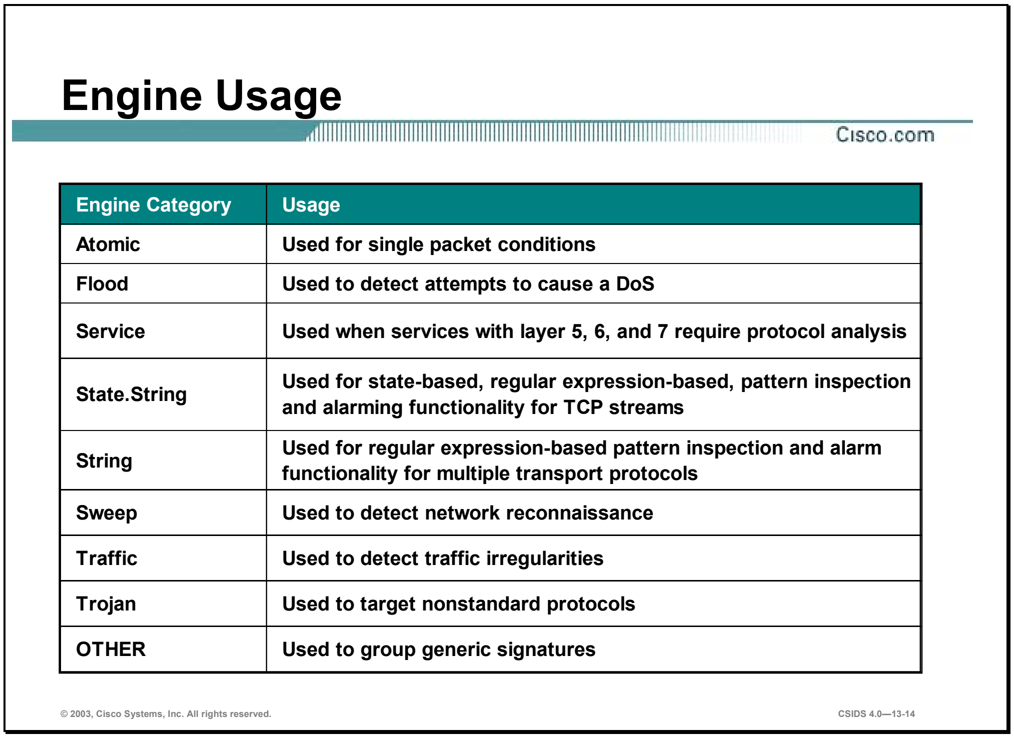
Cisco IDS signature engines enable the network security administrator to tune and create signatures unique to their network environment.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-13

Each signature is created using a signature engine specifically designed for the type of traffic being monitored. A signature engine is a component of the Sensor that supports a category of signatures. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values.

Cisco IDS signature engines enable the network security administrator to tune and create signatures unique to their network environment. Refer to the online document Cisco Intrusion Detection System - Appendix: Signature Engines for more information.



Engine Usage

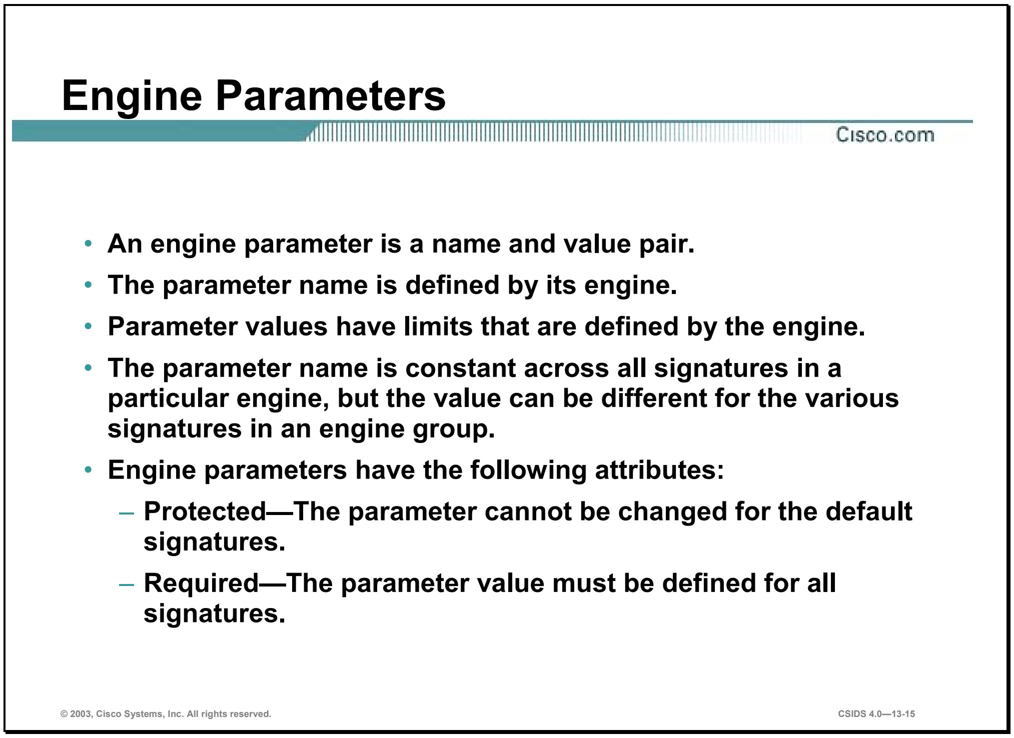
Engine Category	Usage
Atomic	Used for single packet conditions
Flood	Used to detect attempts to cause a DoS
Service	Used when services with layer 5, 6, and 7 require protocol analysis
State.String	Used for state-based, regular expression-based, pattern inspection and alarming functionality for TCP streams
String	Used for regular expression-based pattern inspection and alarm functionality for multiple transport protocols
Sweep	Used to detect network reconnaissance
Traffic	Used to detect traffic irregularities
Trojan	Used to target nonstandard protocols
OTHER	Used to group generic signatures

CSIDS 4.0—13-14

There are several general categories of Cisco IDS signature engines. The categories are as follows:

- Atomic—Used to perform per-packet inspection. The Atomic engines support signatures that trigger based on the analysis of a single packet.
- Flood—Used to detect attempts to cause a DoS
- Service—Used when services with layer 5, 6, and 7 require protocol analysis
- State.String—Used for state-based, regular expression-based, pattern inspection and alarming functionality for TCP streams
- String—Used for regular expression-based pattern inspection and alarm functionality for multiple transport protocols including TCP, UDP, and ICMP
- Sweep—Used to detect network reconnaissance
- Traffic—Identifies traffic irregularities
- Trojan—Used to detect BackOrifice Trojan traffic and Tribal Flood Network 2000 (TFN2K) Trojan or distributed denial of service (DDoS) traffic
- OTHER—Used to group generic signatures so common parameters may be changed

Note The usage and selection of signature engines is dependent on several variables. The selection of signature engines is discussed in a later section.



Engine Parameters

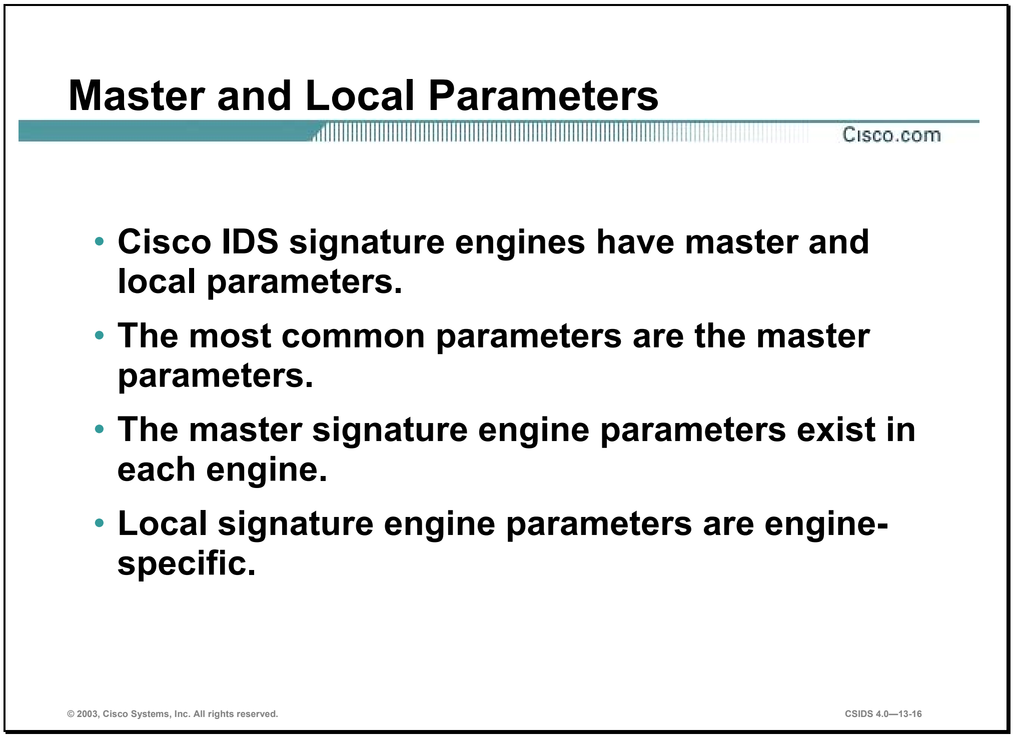
- An engine parameter is a name and value pair.
- The parameter name is defined by its engine.
- Parameter values have limits that are defined by the engine.
- The parameter name is constant across all signatures in a particular engine, but the value can be different for the various signatures in an engine group.
- Engine parameters have the following attributes:
  - Protected—The parameter cannot be changed for the default signatures.
  - Required—The parameter value must be defined for all signatures.

CSIDS 4.0—13-15

An engine parameter is a name and value pair. The name is defined by each engine. The value has limits that are defined by the engine so that only values falling in a particular range are valid. The parameter name is constant across all signatures in a particular engine, but the value can be different for the various signatures in an engine group.

Engine parameters have the following attributes:

- Protected—If a parameter is protected, you cannot change it for the default signatures. You can modify it for custom signatures.
- Required—If a parameter is required, you must define it for all signatures, both default signatures and custom signatures.



Master and Local Parameters

- Cisco IDS signature engines have master and local parameters.
- The most common parameters are the master parameters.
- The master signature engine parameters exist in each engine.
- Local signature engine parameters are engine-specific.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-16

Cisco IDS signature engines have master and local signature parameters. Master parameters are common to most signatures and exist in most signature engines. Local signature parameters are engine-specific. For example, the parameter IcmpCode exists in the Atomic.ICMP signature engine, and the parameter IPOption exists in the Atomic.IPOptions signature engine.

The following table lists the master signature parameters:

Master Signature Parameters	Value	Description
AlarmDelayTimer	1–3600	The number of seconds to delay further signature inspection after an alarm
AlarmInterval	2–1000	Special handling for time events. Use AlarmInterval Y with MinHits X for X alarms in a Y-second interval.
AlarmSeverity	■ High ■ Medium ■ Low ■ Informational	The severity of the alert reported in the alarm

Master Signature Parameters	Value	Description
AlarmThrottle	■ FireAll—Sends all alarms ■ FireOnce—Sends the first alarm and then deletes the inspector ■ Summarize—Sends an IntervalSummary alarm ■ GlobalSummarize—Sends a GlobalSummary alarm	Technique used to limit alarm firings
AlarmTraits	0–65535	User-defined traits that further describe the signature
ChokeThreshold	0–2147483647	Threshold value of alarms per interval to autoswitch AlarmThrottle modes. If ChokeThreshold is defined, the Sensor switches AlarmThrottle modes when a large volume of alarms are viewable in the ThrottleInterval.
Enabled	■ True—Enables the signature ■ False—Disables the signature	Used to enable or disable a signature
EventAction	■ Log ■ Reset ■ ShunHost ■ ShunConnection ■ ZERO	The action to perform when the alarm is fired.
FlipAddr	■ True ■ False	Swaps the source and destination information in the alarm event
MaxInspectLength	0–2147483647	Defines the maximum number of bytes to inspect
MaxTTL	0–1000	Defines the maximum number of seconds to inspect a logical stream
MinHits	0–2147483647	Defines the minimum number of times the signature is triggered before an alarm event is sent

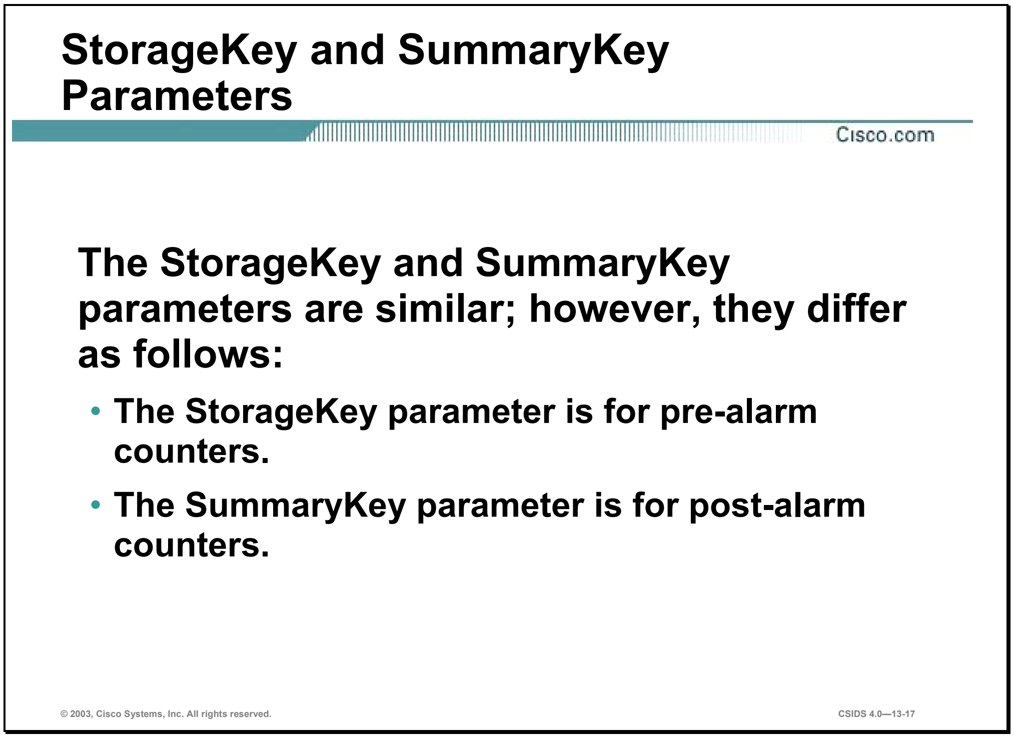
Master Signature Parameters	Value	Description
Protocol	■ Frag ■ IP ■ TCP ■ UDP ■ ICMP ■ ARP ■ Cross ■ Zero ■ Custom	Defines the protocol to be inspected
ResetAfterIdle	2–1000	Defines the number of seconds to wait to reset signature counters after the hosts were idle
ServicePorts	<set list>	Defines a list of ports or port ranges where the target service resides
SigComment	<string>	Defines miscellaneous information about the signature
SIGID	■ 993–19999—Range for default signatures ■ 20000–50000—Range for custom signatures	The numeric value assigned to the signature
SigName	<string>	The alphanumeric name assigned to the signature
SigStringInfo	<string>	Defines extra information included in the alarm message
StorageKey	■ xxxx ■ Axxx ■ xxBx ■ AxBx ■ AaBb ■ Axxb ■ STREAM DOUBLE ZERO	Type of Address Key used to store persistent data
SubSig	0–2147483647	The number assigned to the sub-signature
SummaryKey	■ AaBb ■ AxBx ■ Axxb ■ Axxx ■ xxBx	The storage type on which to summarize this signature
ThrottleInterval	0–1000	Defines the period of time used to control alarm summarization

Master Signature Parameters	Value	Description
WantFrag	■ TRUE—Only fragmented packets trigger an alarm. ■ FALSE—Only non-fragmented packets will trigger an alarm. ■ <blank>—Fragmented and non-fragmented IP traffic will trigger an alarm.	Controls the inspection of fragmented packets

The FlipAddr parameter is useful in situations in which the traffic that triggers the signature is return traffic from the target system. Normally, the traffic that triggers a signature originates from the attacker's IP address, so the source IP address in the resulting alarm is that of the attacker. However, some signatures rely on return traffic from the target to determine if an attack is taking place. For example, ResetPortSweep looks for the target sending back multiple resets from various ports to determine that a port sweep is taking place. Without the FlipAddr parameter, the source address in the resulting alarm would be that of the target. Setting the FlipAddr parameter to true causes the alarm to display the correct attacker and target addresses.

Examples of the local engine-specific signature parameters are explained in this chapter. For a complete listing and further information on the engine-specific parameter, visit the following web site:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a008014a214.html#wp803372



StorageKey and SummaryKey Parameters

The StorageKey and SummaryKey parameters are similar; however, they differ as follows:

- **The StorageKey parameter is for pre-alarm counters.**
- **The SummaryKey parameter is for post-alarm counters.**

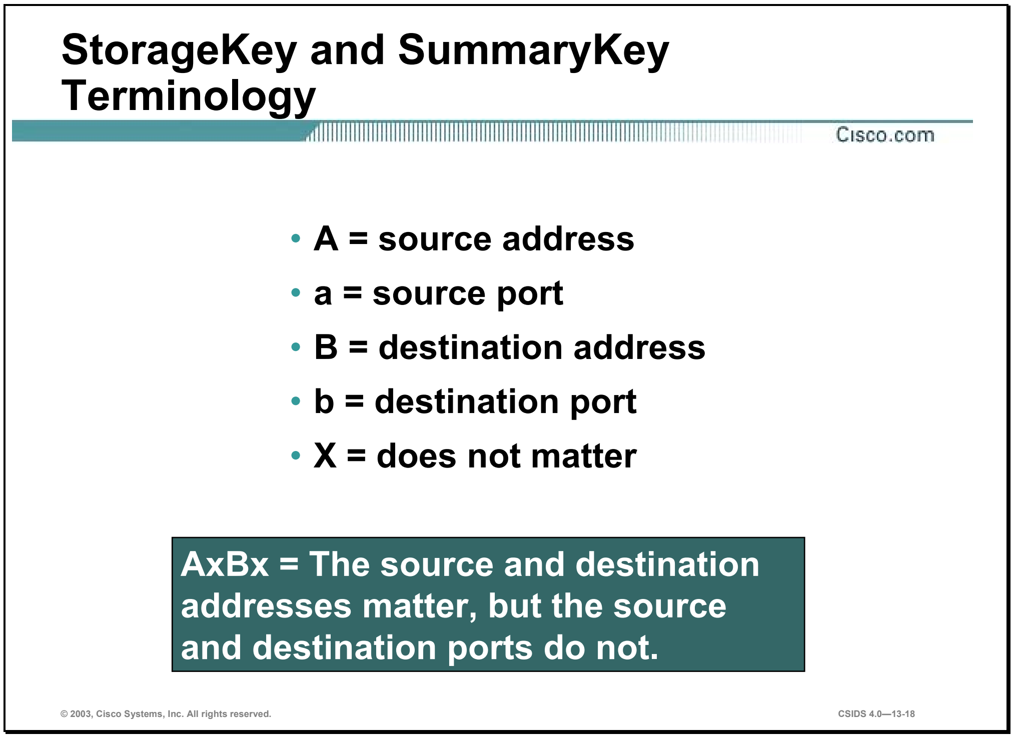
CSIDS 4.0—13-17

The StorageKey and SummaryKey parameters are defined as follows:

- StorageKey—Specifies where persistent cross-packet data for the signature is stored. This is data that influences signature alarm firing. You should not change the default value of the StorageKey, even for custom signatures.

- SummaryKey—Specifies where the results of alarms are stored. This is where the counters for summary and MinHits are stored. The SummaryKey enables you to count the number of occurrences of a signature firing on various address sets.

The StorageKey and SummaryKey parameters are similar; however, the StorageKey is for the pre-alarm counters, whereas the SummaryKey is for the post-alarm counters.



StorageKey and SummaryKey Terminology

- A = source address
- a = source port
- B = destination address
- b = destination port
- X = does not matter

AxBx = The source and destination addresses matter, but the source and destination ports do not.

© 2003, Cisco Systems, Inc. All rights reserved.

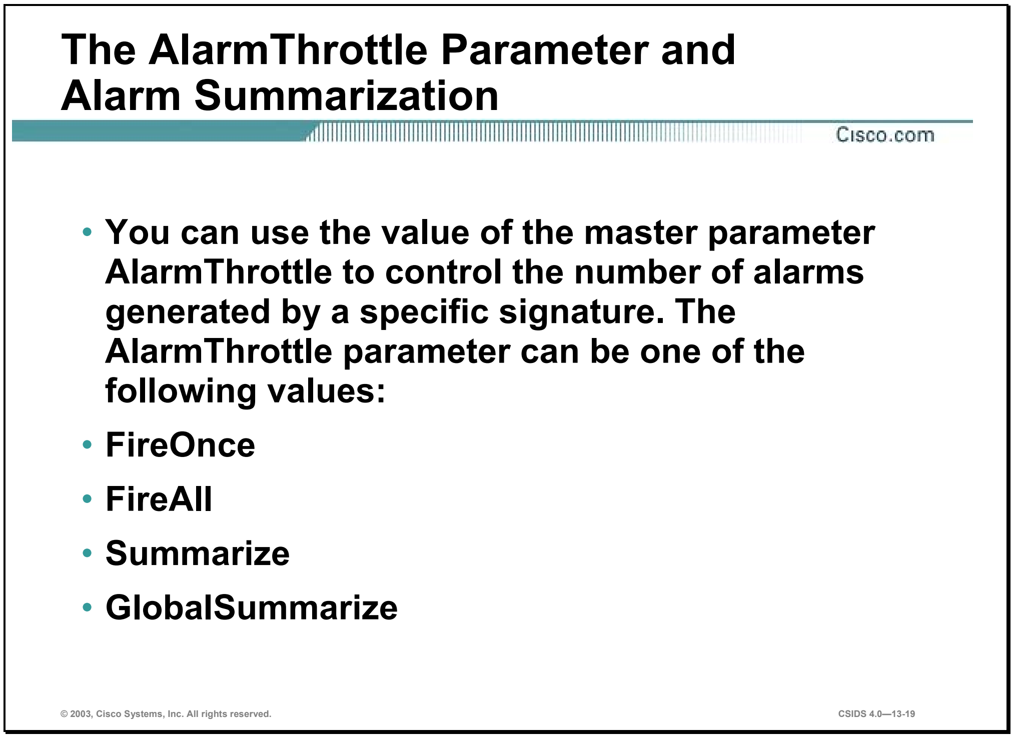
CSIDS 4.0—13-18

The StorageKey and SummaryKey parameters use A, a, B, and b to designate a source address, source port, destination address, and destination port, respectively. This terminology uses x as a wildcard. If x occupies the position of A, a, B, or b in the sequence AaBb, the value of that position is unimportant. The following are examples of using the StorageKey and SummaryKey terminology:

- Axxx—Only the source address is examined.
- AxBx—The source and destination addresses are examined, but the source and destination ports are not.
- xxBx—Only the destination address is examined.
- AaBb—The source and destination sockets are examined.

You could use AxBb for web sessions in which various pages are accessed. Every new page is a new connection. The source IP address is examined, but the source port is not. Both the destination IP addresses and the destination ports are examined.

The designation Axxb is used for service sweeps in which an attacker is sweeping port 80 across multiple hosts. The attacker port and the victim address port are not examined, but the victim port is examined.



The AlarmThrottle Parameter and Alarm Summarization

- You can use the value of the master parameter AlarmThrottle to control the number of alarms generated by a specific signature. The AlarmThrottle parameter can be one of the following values:
- FireOnce
- FireAll
- Summarize
- GlobalSummarize

CSIDS 4.0—13-19

The master parameter, AlarmThrottle, controls the number of alarms generated by a specific signature. By correctly configuring this parameter, you can reduce the ability of an attacker to consume resources on your Cisco IDS by flooding it with attacks. The AlarmThrottle can be one of the following values:

- FireOnce—Triggers a single alarm for each unique entry based on the SummaryKey parameter settings, and then waits a predefined period of time before triggering an alarm again for the same signature with the same keys. The predefined period of time is usually specified by the ThrottleInterval parameter.

- FireAll—Triggers an alarm for all activity that matches the signature characteristics. This is effectively the opposite of the FireOnce option and can generate a considerably large number of alarms during an attack.

- Summarize—Consolidates alarms for the address set specified in the SummaryKey parameter

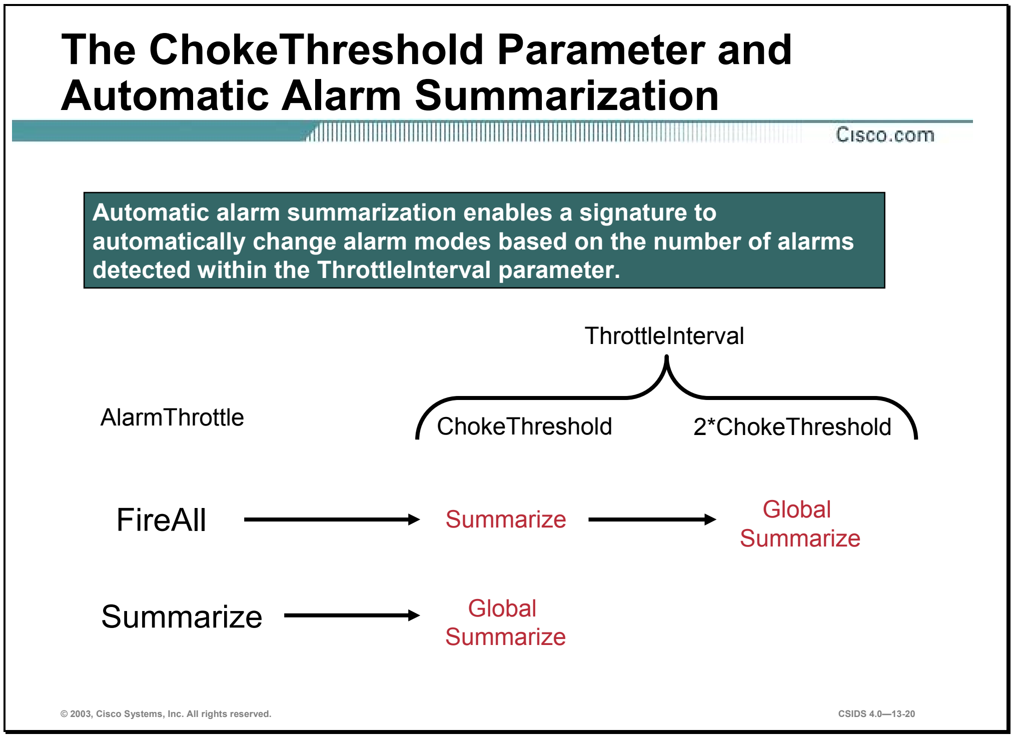
- GlobalSummarize—Consolidates alarms for all address combinations

Besides the basic alarm firing options, signatures can also take advantage of two alarm summarization modes. Like FireOnce, the Summarize and GlobalSummarize modes limit the number of alarms generated and make it difficult for an attacker to consume resources on the IDS. However, using these alarm summarization modes, the network security administrator receives information on the number of times that activity which matches a signature's characteristics was observed during a specific period of time. When using Summarize mode, the first instance of intrusive activity triggers a normal alarm. Then, other instances of the same activity, duplicate alarms, are counted until the end of the ThrottleInterval of the signature.

When the length of time specified by the ThrottleInterval has elapsed, a summary alarm is sent to the eventStore, indicating the number of alarms that occurred during the Throttle Interval.

Both alarm summarization modes operate essentially the same, except GlobalSummarize mode consolidates the alarms for all address combinations, whereas the Summarize mode only consolidates the alarms for the address set specified in the SummaryKey parameter.

Note Alarm summarization modes are available to all signatures and are handled by the master parameters.



The ChokeThreshold Parameter and Automatic Alarm Summarization

Cisco.com

Automatic alarm summarization enables a signature to automatically change alarm modes based on the number of alarms detected within the ThrottleInterval parameter.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-20

Setting the ChokeThreshold parameter enables a signature to use variable alarm summarization. The signature needs to be configured to use one of the following AlarmThrottle modes to take advantage of variable alarm summarization: FireAll, Summarize, or GlobalSummarize. When traffic causes the signature to trigger, the alarms are generated according to the original AlarmThrottle mode. If the number of alarms for the signature exceeds the value configured for the ChokeThreshold parameter, during a ThrottleInterval, the signature automatically switches to the next higher alarming mode, a mode generating less alarms. If the number of alarms for the signature exceeds twice the ChokeThreshold, during the same ThrottleInterval, the signature switches to Global Summarization, if not already at this level, since this is the maximum level of alarm consolidation. At the end of the ThrottleInterval, the signature reverts back to its configured original AlarmThrottle mode.

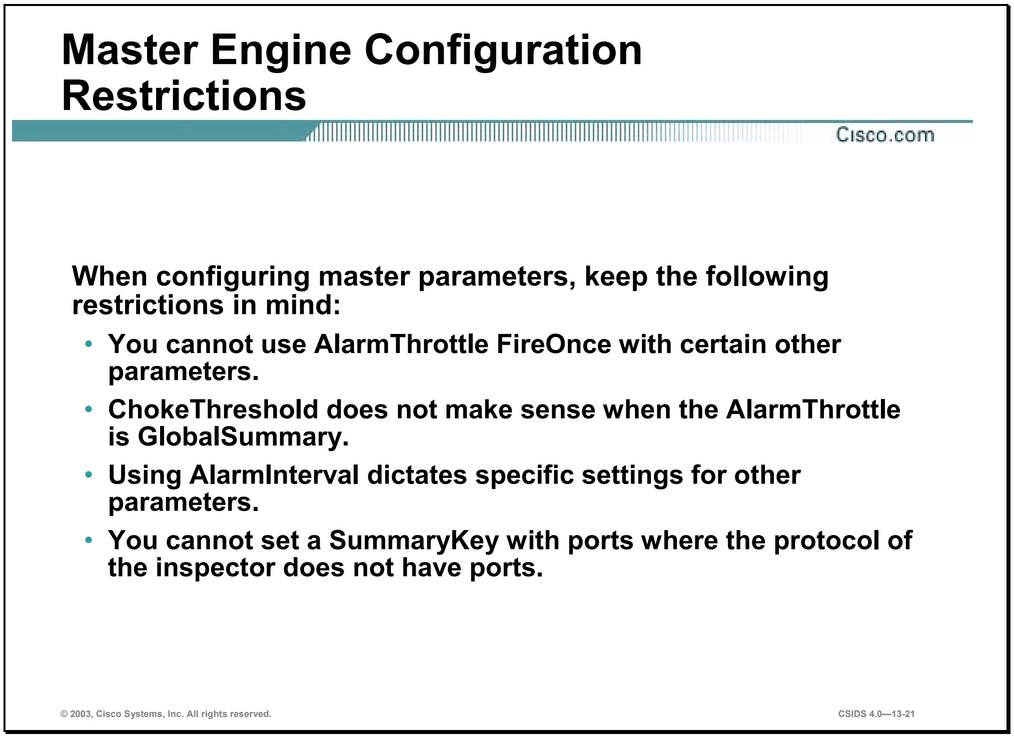
For example, if the signature starts with a original AlarmThrottle mode of FireAll, an alarm is generated every time the signature is triggered. If the number of alarms for the signature exceeds the ChokeThreshold parameter setting, during a ThrottleInterval, the signature automatically switches to Summarize mode. Finally, if the number of alarms exceeds twice the ChokeThreshold parameter, during the same ThrottleInterval, the signature automatically switches to GlobalSummarize mode. At the end of the ThrottleInterval, the signature reverts back to the FireAll alarming mode.

The variable alarming mode gives you the flexibility of having signatures fire an alarm on every instance of a signature, but reducing the number of alarms generated when the number of alarms begins to significantly impact the resources on the IDS and the ability of the network security administrator to analyze the alarms being generated. The following is an example of variable alarming mode:

```
SIG ID 20000
AlarmThrottle: FireAll
```

```
ChokeThreshold: 150
ThrottleInterval: 60
Traffic1: 100 alarms in 60 seconds
Result: 100 regular alarms
Traffic2: 160 alarms in 60 seconds
Result: 150 regular alarms and 1 IntervalSummary alarm with count 160
Traffic3: 320 alarms in 60 seconds
Result: 150 regular alarms and 1 GlobalSummary alarm with count 320
```

Note This example assumes that all alarms are on the same address set (for example, 10.0.5.12–10.0.6.12).



Master Engine Configuration Restrictions

When configuring master parameters, keep the following restrictions in mind:

- You cannot use AlarmThrottle FireOnce with certain other parameters.
- ChokeThreshold does not make sense when the AlarmThrottle is GlobalSummary.
- Using AlarmInterval dictates specific settings for other parameters.
- You cannot set a SummaryKey with ports where the protocol of the inspector does not have ports.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-21

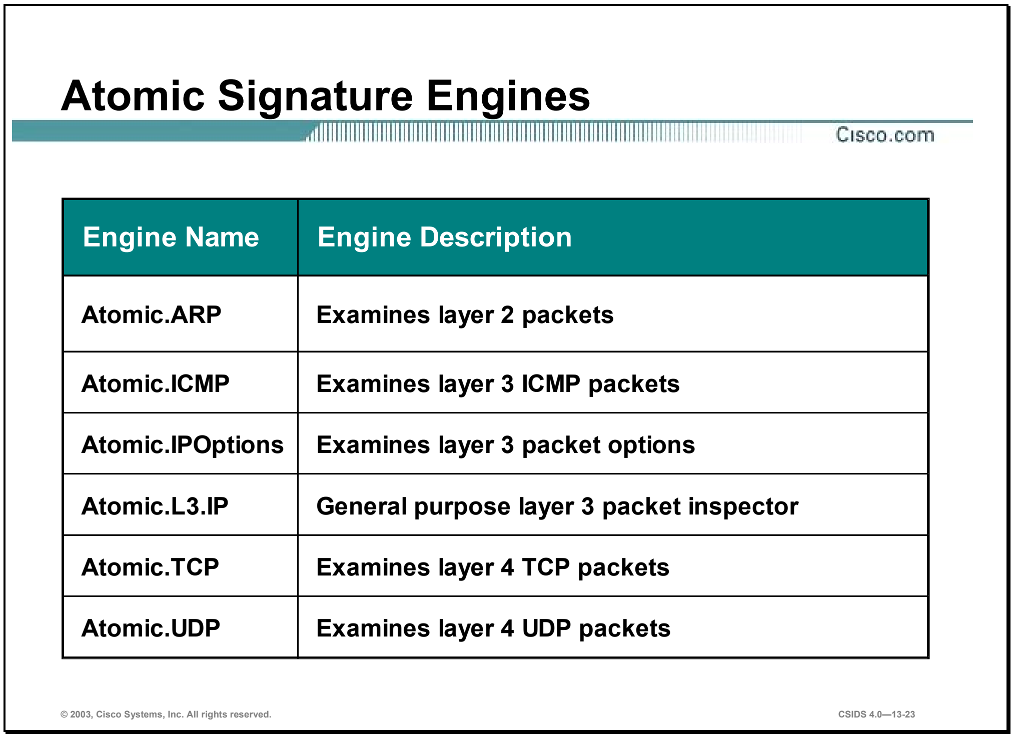
Not all Master engine parameters work together. The following are constraints on the configuration of various Master engine parameters:

- You cannot use the AlarmThrottle parameter value FireOnce with the following:
  - ChokeThreshold X (where X is not ANY)
  - Signatures that use StorageKey xxxx
  - MinHits
- A ChokeThreshold parameter does not make sense when the AlarmThrottle mode is GlobalSummary.
- If you use AlarmInterval, you must set the following parameters:
  - Set MinHits to a value less than 1.
  - Set AlarmThrottle to FireAll.
  - Set ChokeThreshold to ANY.
  - Configure a valid ThrottleInterval.
- You cannot set a SummaryKey with ports AaBb, Axxb where the protocol of the inspector does not have ports. SummaryKey attempts to return to the same default settings as the StorageKey except when the StorageKey is xxxx. In this case, you must specify a

SummaryKey. In this case, if you do not specify a SummaryKey, the summarization features will not work, and you will receive all the alarms.

Atomic Signature Engines

This section discusses the atomic signature engines and their specific configuration parameters.



Atomic Signature Engines

Engine Name	Engine Description
Atomic.ARP	Examines layer 2 packets
Atomic.ICMP	Examines layer 3 ICMP packets
Atomic.IPOptions	Examines layer 3 packet options
Atomic.L3.IP	General purpose layer 3 packet inspector
Atomic.TCP	Examines layer 4 TCP packets
Atomic.UDP	Examines layer 4 UDP packets

The Atomic signature engines support signatures that are triggered by the contents of a single packet. Since the Atomic signature engines examine single packets, they do not need to maintain a state. Therefore, the Atomic signature engines do not store any persistent data across multiple data packets.

The following are Atomic signature engines:

- Atomic.ARP—Used to examine basic layer 2 packets; and, also for more advanced detection of the ARP spoof tools dsniff and ettercap

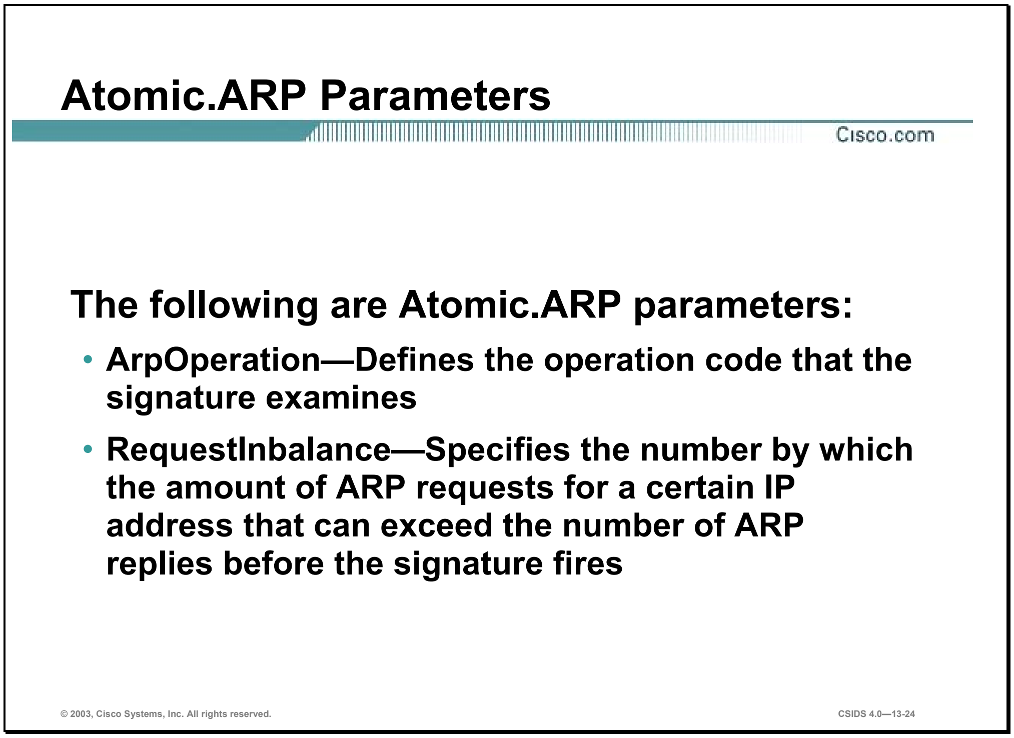
- Atomic.ICMP—Used to examine layer 3 ICMP packets

- Atomic.IPOptions—Used to examine layer 3 IP packets with a specified IP option

- Atomic.L3.IP—Used to examine layer 3 IP packets

- Atomic.TCP—Used to examine layer 4 TCP packets

- Atomic.UDP—Used to examine layer 4 UDP packets



Atomic.ARP Parameters

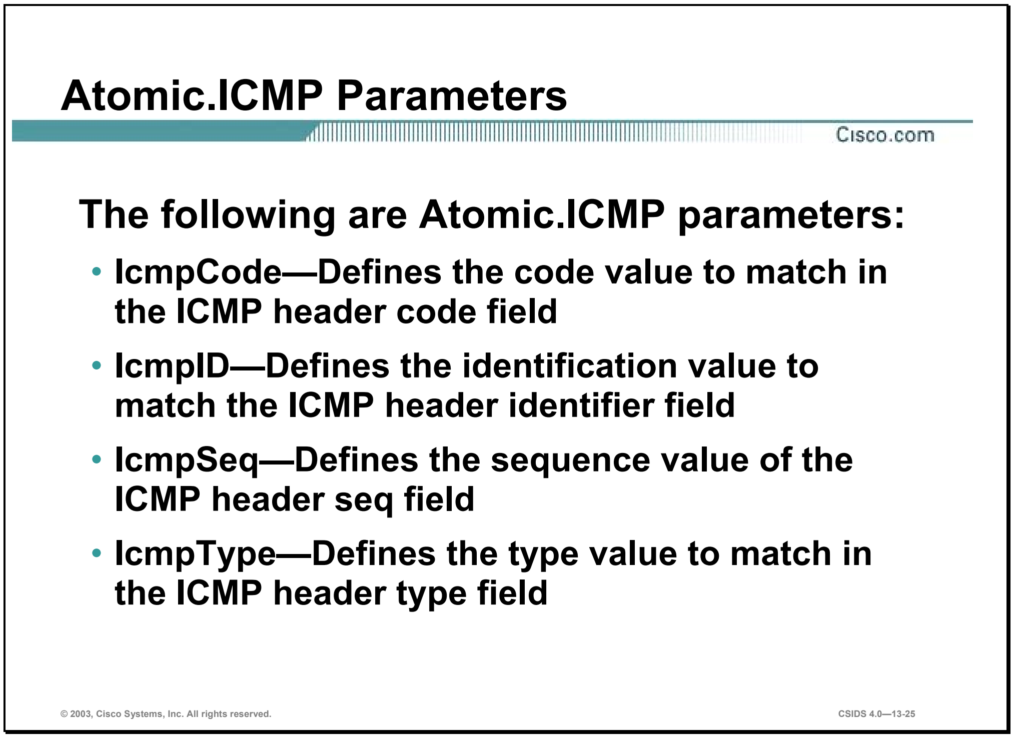
The following are Atomic.ARP parameters:

- **ArpOperation—Defines the operation code that the signature examines**
- **RequestInbalance—Specifies the number by which the amount of ARP requests for a certain IP address that can exceed the number of ARP replies before the signature fires**

CSIDS 4.0—13-24

The following table shows examples of the Atomic.ARP parameters:

Parameter	Value	Attribute	Description
ArpOperation	0–255	■ Not protected ■ Not required	Defines the operation code that the signature examines
RequestInbalance	0–65535	■ Not protected ■ Not required	Defines the number of requests for an IP address against the replies. Once the number of requests is X more than the replies, the signature fires.



Atomic.ICMP Parameters

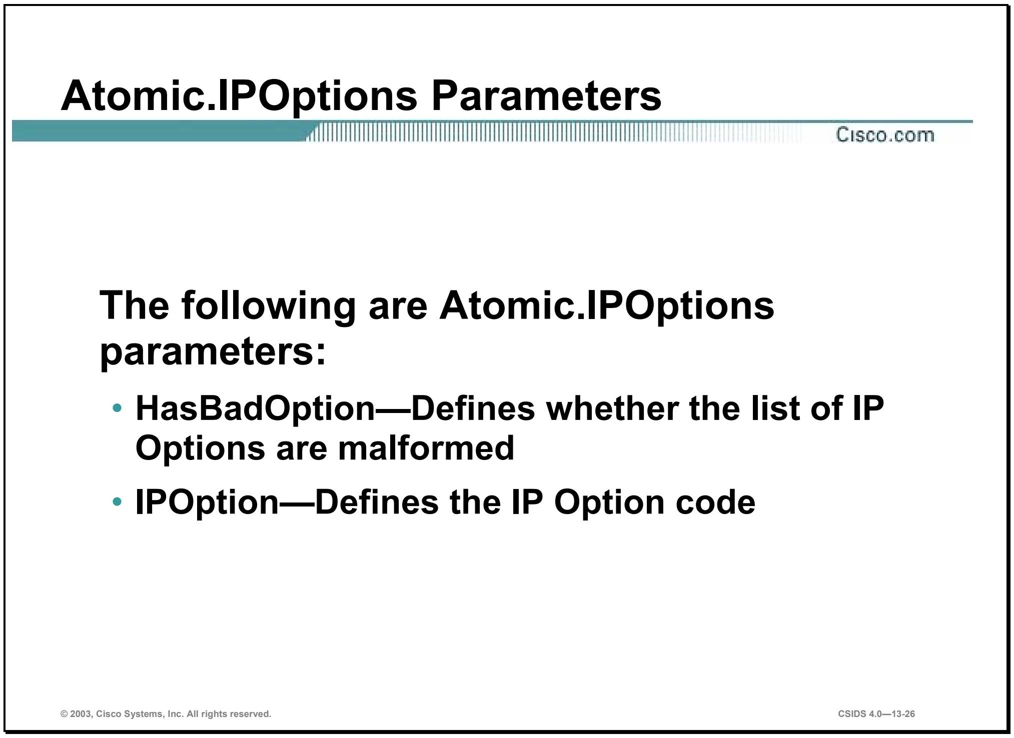
The following are Atomic.ICMP parameters:

- **IcmpCode—Defines the code value to match in the ICMP header code field**
- **IcmpID—Defines the identification value to match the ICMP header identifier field**
- **IcmpSeq—Defines the sequence value of the ICMP header seq field**
- **IcmpType—Defines the type value to match in the ICMP header type field**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-25

The following table shows examples of the Atomic.ICMP parameters:

Parameter	Value	Attribute	Description
IcmpCode	0–255	■ Not protected ■ Not required	Defines the code value to match in the ICMP header code field
IcmpID	0–65535	■ Not protected ■ Not required	Defines the identification value to match the ICMP header identifier field
IcmpSeq	0–65535	■ Not protected ■ Not required	Defines the sequence value of the ICMP header seq field
IcmpType	0–255	■ Not protected ■ Not required	Defines the type value to match in the ICMP header type field



Atomic.IPOptions Parameters

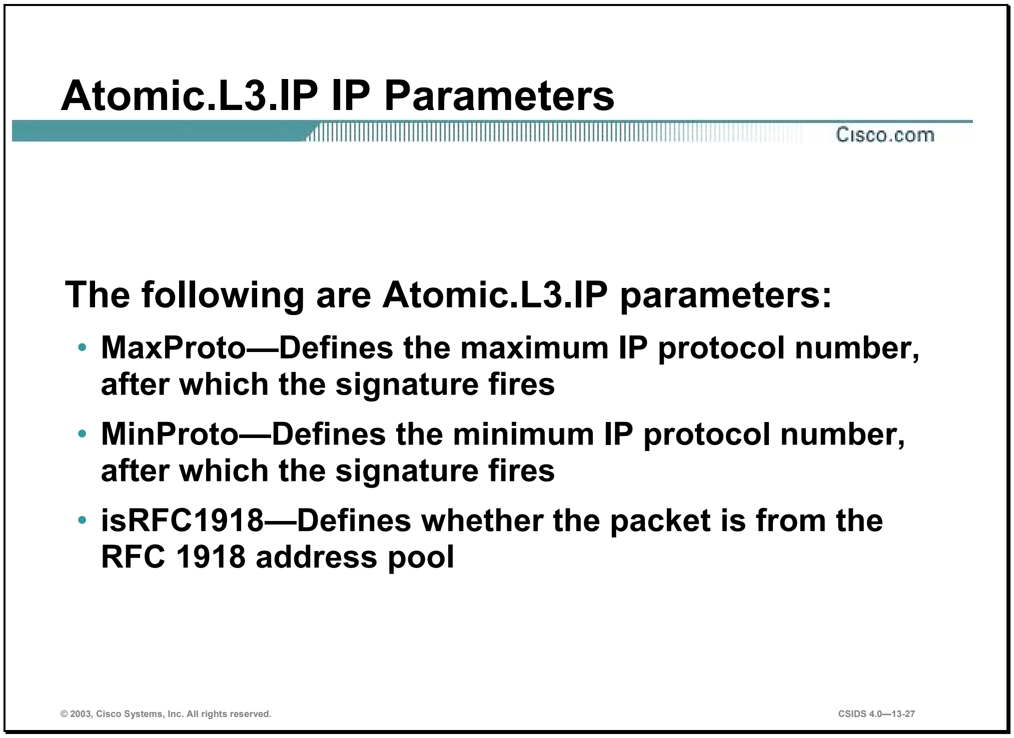
The following are Atomic.IPOptions parameters:

- **HasBadOption—Defines whether the list of IP Options are malformed**
- **IPOption—Defines the IP Option code**

CSIDS 4.0—13-26

The following table shows examples of the Atomic.IPOptions parameters:

Parameter	Value	Attribute	Description
HasBadOption	■ True ■ False	■ Not protected ■ Not required	Defines whether the list of IP Options are malformed
IPOption	0–255	■ Not protected ■ Not required	Defines the IP Option code



Atomic.L3.IP IP Parameters

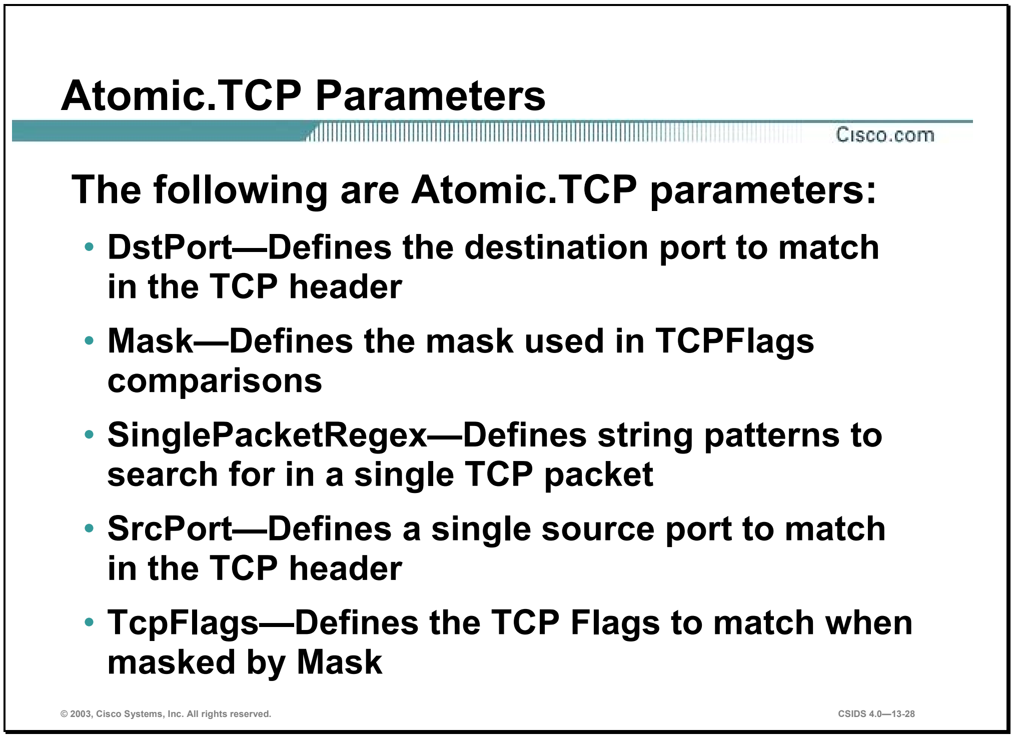
The following are Atomic.L3.IP parameters:

- MaxProto—Defines the maximum IP protocol number, after which the signature fires
- MinProto—Defines the minimum IP protocol number, after which the signature fires
- isRFC1918—Defines whether the packet is from the RFC 1918 address pool

CSIDS 4.0—13-27

The following table shows examples of the Atomic.L3.IP parameters:

Parameter	Value	Attribute	Description
MaxProto	0–255	■ Not protected ■ Not required	Triggers an alarm if the IP protocol value is greater than this value
MinProto	0–255	■ Not protected ■ Not required	Triggers an alarm if the IP Protocol value is less than this value
isRFC1918	■ True ■ False	■ Not protected ■ Not required	Defines whether the packet is from RFC 1918 address



Atomic.TCP Parameters

The following are Atomic.TCP parameters:

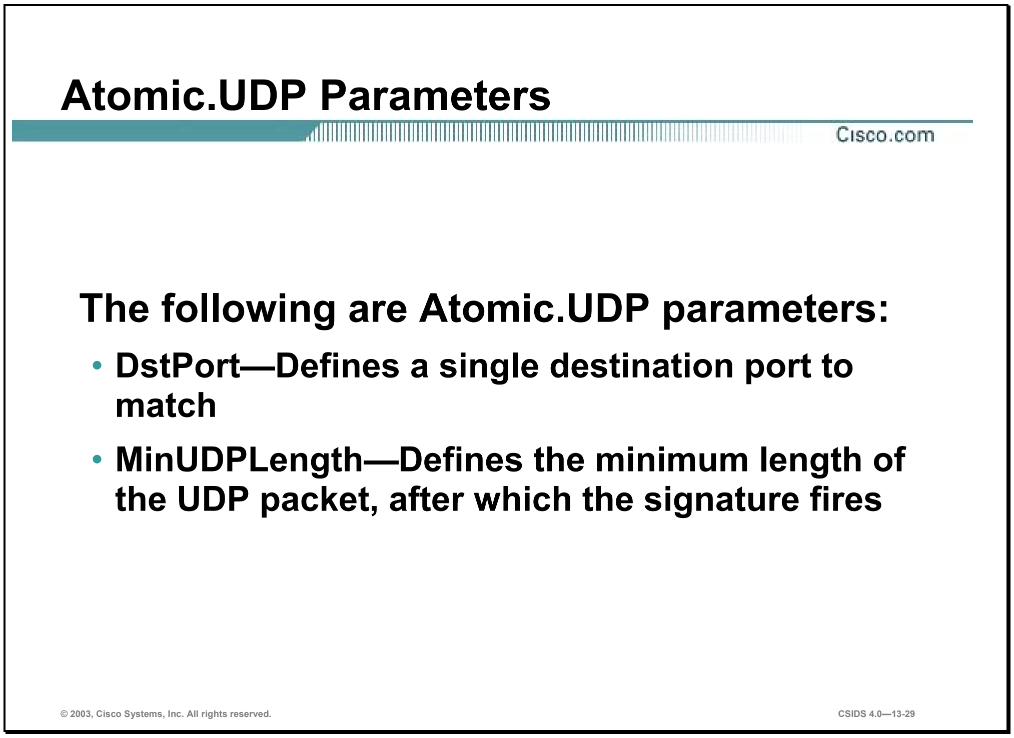
- DstPort—Defines the destination port to match in the TCP header
- Mask—Defines the mask used in TCPFlags comparisons
- SinglePacketRegex—Defines string patterns to search for in a single TCP packet
- SrcPort—Defines a single source port to match in the TCP header
- TcpFlags—Defines the TCP Flags to match when masked by Mask

CSIDS 4.0—13-28

The following table shows examples of the Atomic.TCP parameters:

Parameter	Value	Attribute	Description
DstPort	0–65535	■ Not protected ■ Not required	Defines the destination port to match in the TCP header
Mask	■ FIN ■ SYN ■ RST ■ PUSH ■ ACK ■ URG ■ Zero	■ Not protected ■ Required	Defines the mask used in TCP Flags comparison
SinglePacketRegex	<string>	■ Not protected ■ Not required	Defines string patterns to search for in a single TCP packet
SrcPort	1–65535	■ Not protected ■ Not required	Defines a single source port to match in the TCP header
TcpFlags	■ FIN ■ SYN ■ RST ■ PUSH ■ ACK ■ URG ■ Zero	■ Not protected ■ Required	Defines the TCP Flags to match when masked by Mask

You can specify what type of TCP traffic you want the signature to match by using the Mask and TcpFlags parameters. The Mask parameter identifies the TCP Flags of interest, and the TcpFlags parameter specifies which of the TCP Flags in a packet must be set to trigger the signature. Any TCP Flags that you do not include in the Mask cannot impact whether the signature triggers.



Atomic.UDP Parameters

Cisco.com

The following are Atomic.UDP parameters:

- DstPort—Defines a single destination port to match
- MinUDPLength—Defines the minimum length of the UDP packet, after which the signature fires

© 2003, Cisco Systems, Inc. All rights reserved.

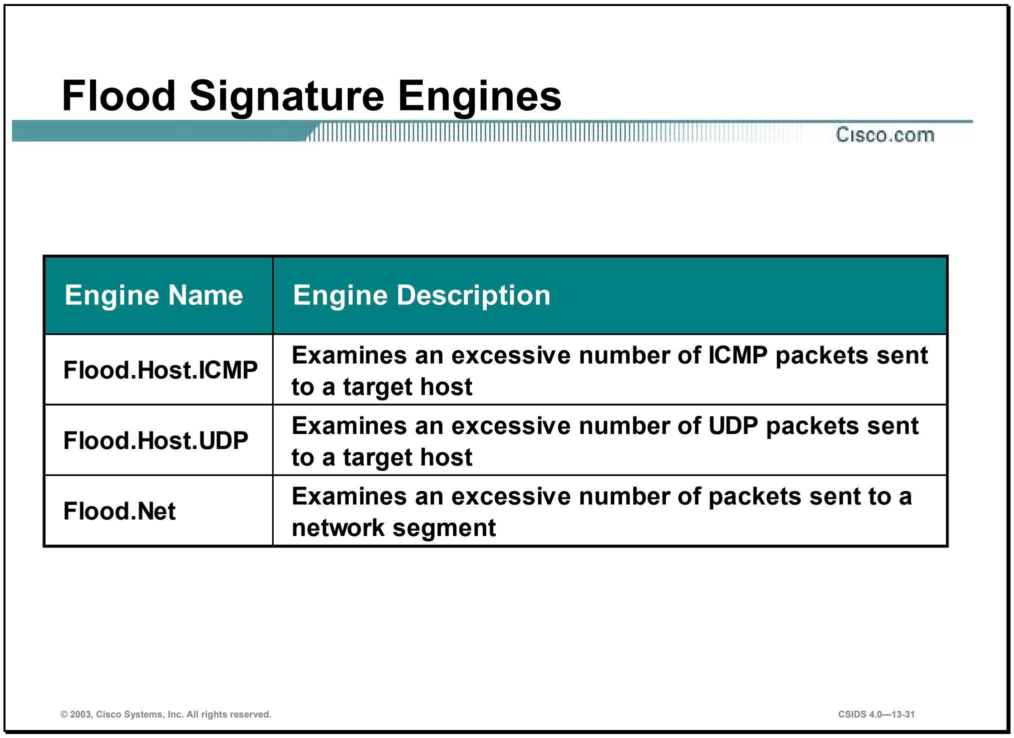
CSIDS 4.0—13-29

The following table shows examples of the Atomic.UDP parameters:

Parameter	Value	Attribute	Description
DstPort	0–65535	■ Not protected ■ Not required	Defines a single destination port to match in the UDP header
MinUDPLength	0–65535	■ Not protected ■ Not required	Defines the minimum length of the UDP packet, after which the signature fires

Flood Signature Engines

This section discusses the Flood signature engines and their specific configuration parameters.



Flood Signature Engines

Engine Name	Engine Description
Flood.Host.ICMP	Examines an excessive number of ICMP packets sent to a target host
Flood.Host.UDP	Examines an excessive number of UDP packets sent to a target host
Flood.Net	Examines an excessive number of packets sent to a network segment

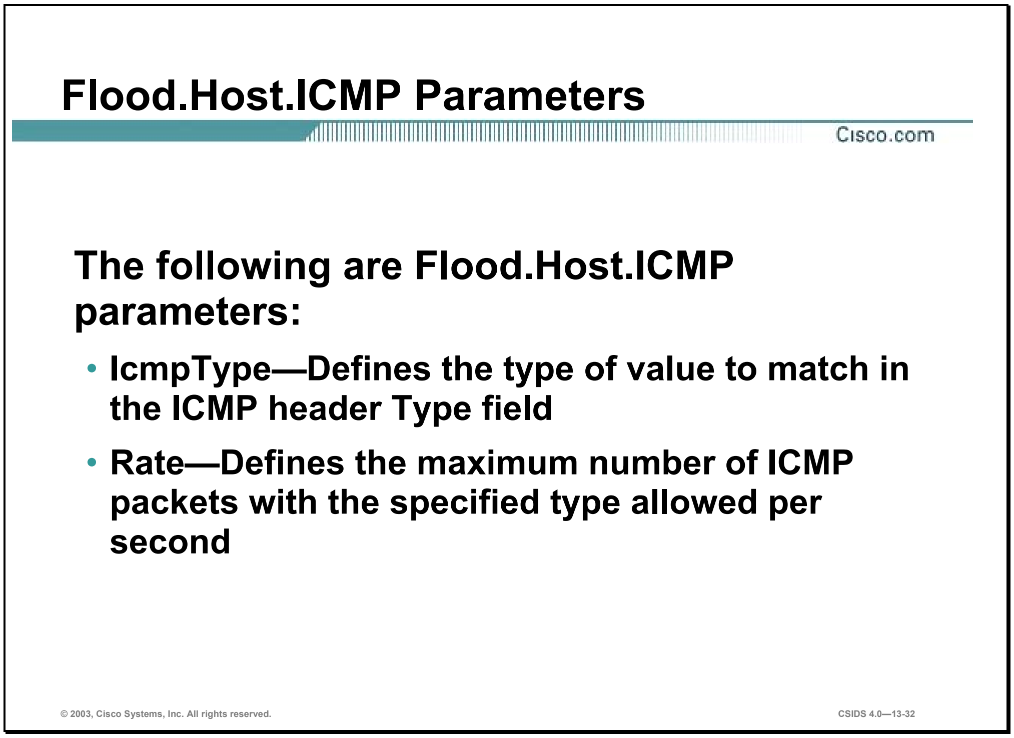
CSIDS 4.0—13-31

The Flood signature engines detect attacks in which the attacker is directing a flood of traffic to either a single host or the entire network. The following are the Flood signature engines:

- Flood.Host.ICMP—Used to examine an excessive number of ICMP packets sent to a target host
- Flood.Host.UDP—Used to examine an excessive number of UDP packets sent to a target host
- Flood.Net—Used to examine an excessive number of packets sent to a network segment

The Flood.Host.ICMP and Flood.Host.UDP signature engines support n to 1 signatures and attach a packets-per-second (PPS) rate counter to the destination address. The sampling occurs on a per-second basis.

The Flood.Net signature engine supports n to n signatures and counts the rate of packets seen by the engine on a virtual Sensor basis. It does not use addresses for counting. The Flood.Net signature engine also performs sampling on a per-second basis.



Flood.Host.ICMP Parameters

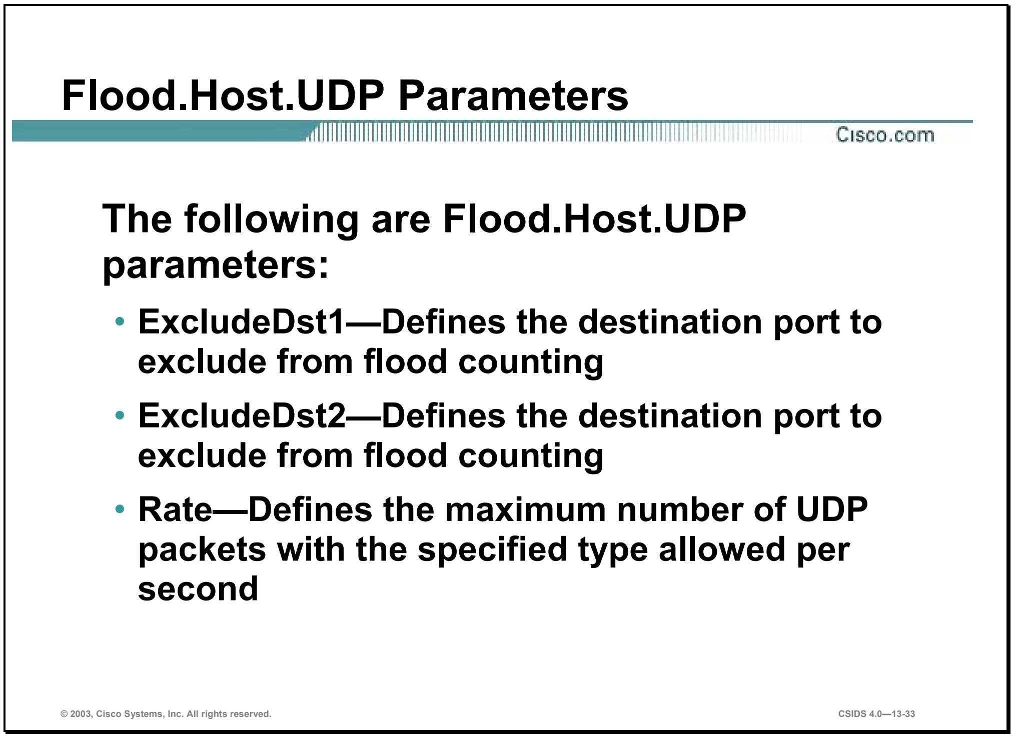
The following are Flood.Host.ICMP parameters:

- **IcmpType—Defines the type of value to match in the ICMP header Type field**
- **Rate—Defines the maximum number of ICMP packets with the specified type allowed per second**

CSIDS 4.0—13-32

The following table shows examples of the Flood.Host.ICMP parameters:

Parameter	Value	Attribute	Description
IcmpType	0–255	■ Not protected ■ Not required	Defines the type value to match in the ICMP header TYPE field
Rate	0–2147483647	■ Not protected ■ Not required	Defines the maximum number of ICMP packets with the specified type allowed per second



Flood.Host.UDP Parameters

Cisco.com

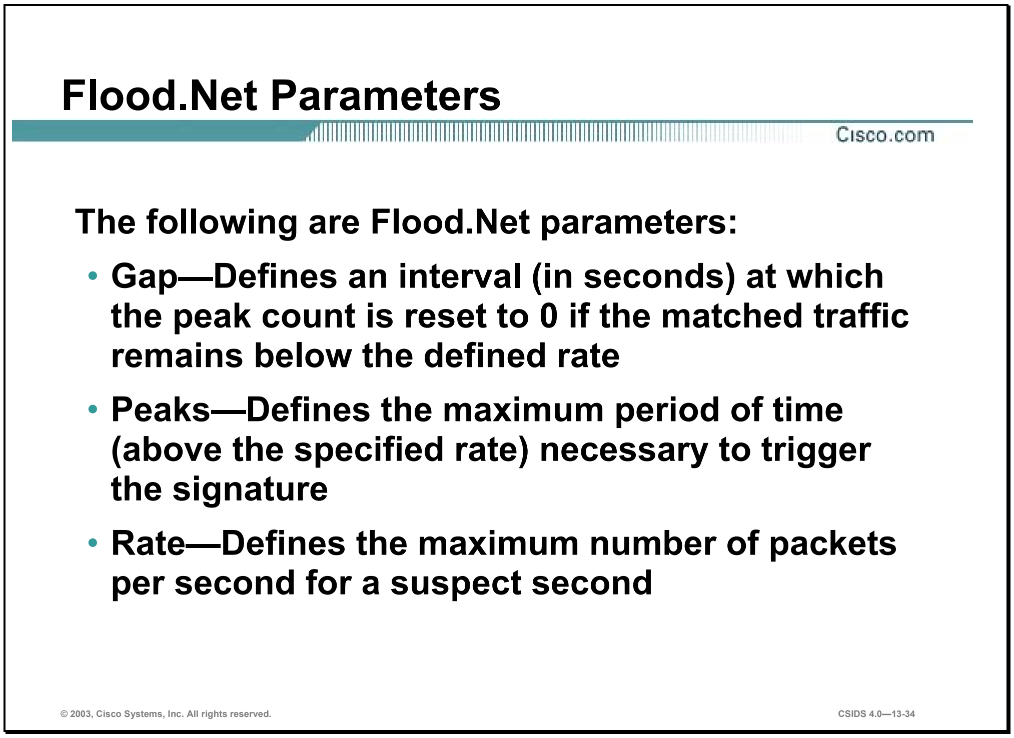
The following are Flood.Host.UDP parameters:

- **ExcludeDst1—Defines the destination port to exclude from flood counting**
- **ExcludeDst2—Defines the destination port to exclude from flood counting**
- **Rate—Defines the maximum number of UDP packets with the specified type allowed per second**

CSIDS 4.0—13-33

The following table lists the Flood.Host.UDP parameters:

Parameter	Value	Attribute	Description
ExcludeDst1	0–65535	■ Not protected ■ Not required	Defines the destination port to exclude from flood counting
ExcludeDst2	0–65535	■ Not protected ■ Not required	Defines the destination port to exclude from flood counting
Rate	0–2147483647	■ Not protected ■ Required	Defines the maximum number of UDP packets with the specified type allowed per second



Flood.Net Parameters

The following are Flood.Net parameters:

- **Gap—Defines an interval (in seconds) at which the peak count is reset to 0 if the matched traffic remains below the defined rate**
- **Peaks—Defines the maximum period of time (above the specified rate) necessary to trigger the signature**
- **Rate—Defines the maximum number of packets per second for a suspect second**

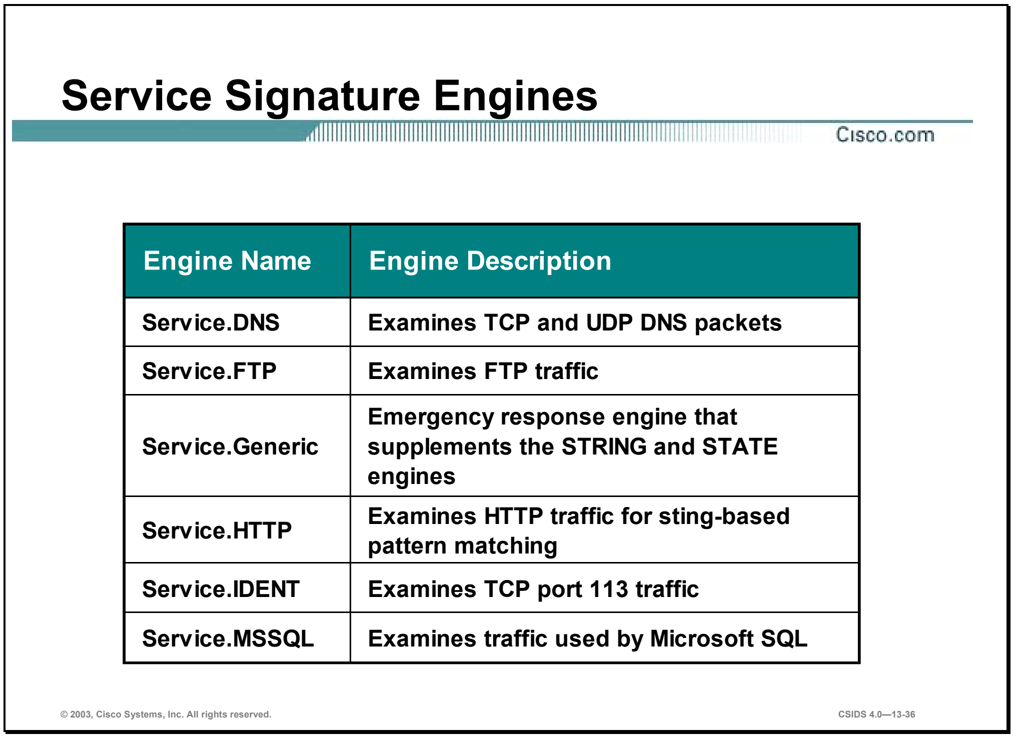
CSIDS 4.0—13-34

The following table lists the Flood.Net parameters:

Parameter	Value	Attribute	Description
Gap	0–2147483647	■ Not protected ■ Not required	Defines an interval, in seconds, at which the peak count is reset to 0 if the matched traffic remains below the defined rate
Peaks	0–2147483647	■ Not protected ■ Not required	Defines the maximum period of time, above the specified rate, necessary to trigger the signature
Rate	0–2147483647	■ Not protected ■ Not required	The maximum PPS required to trigger a flood

Service Signature Engines

This section discusses the Service signature engines and their specific configuration parameters. The RPC signature engine is the only engine discussed in detail in this section.



Service Signature Engines

Cisco.com

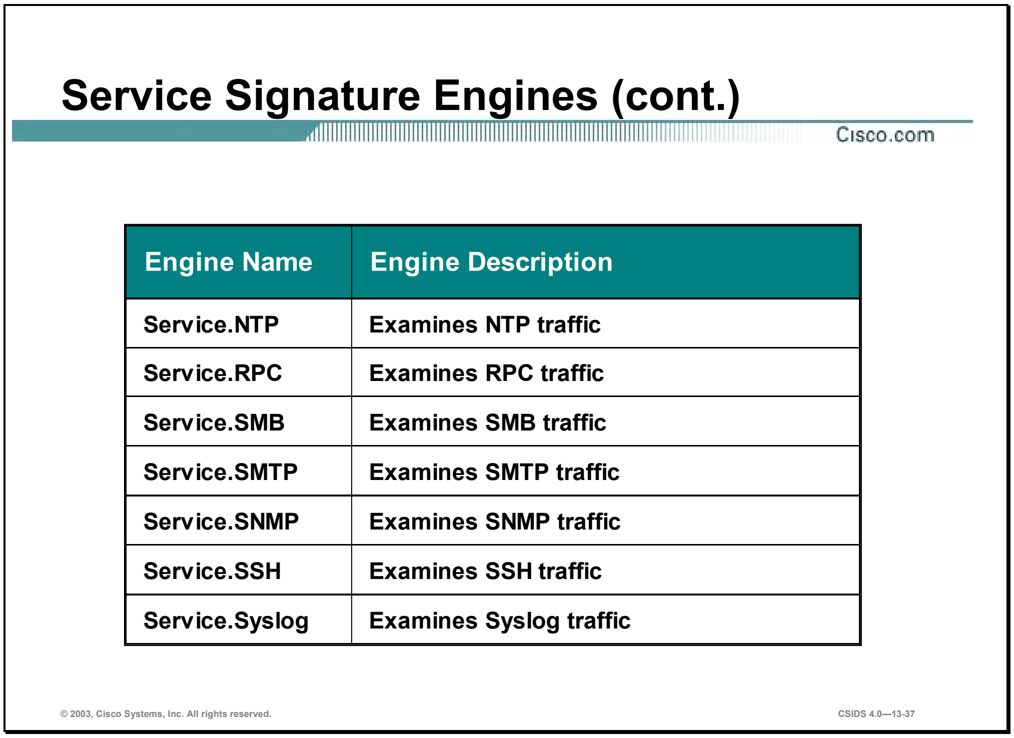
Engine Name	Engine Description
Service.DNS	Examines TCP and UDP DNS packets
Service.FTP	Examines FTP traffic
Service.Generic	Emergency response engine that supplements the STRING and STATE engines
Service.HTTP	Examines HTTP traffic for sting-based pattern matching
Service.IDENT	Examines TCP port 113 traffic
Service.MSSQL	Examines traffic used by Microsoft SQL

CSIDS 4.0—13-36

The Service signature engines analyze traffic at and above layer five of the Open Systems Interconnection (OSI) architectural model. This provides protocol decoding for numerous network protocols such as DNS, FTP, and HTTP.

The following are Service signature engines:

- Service.DNS—Examines TCP and UDP DNS packets
- Service.FTP—Examines FTP traffic
- Service.Generic—Emergency response engine that supplements the STRING and STATE engines
- Service.HTTP—Examines HTTP traffic for string-based pattern matching
- Service.IDENT—Examines TCP port 113 traffic
- Service.MSSQL—Examines traffic used by Microsoft SQL



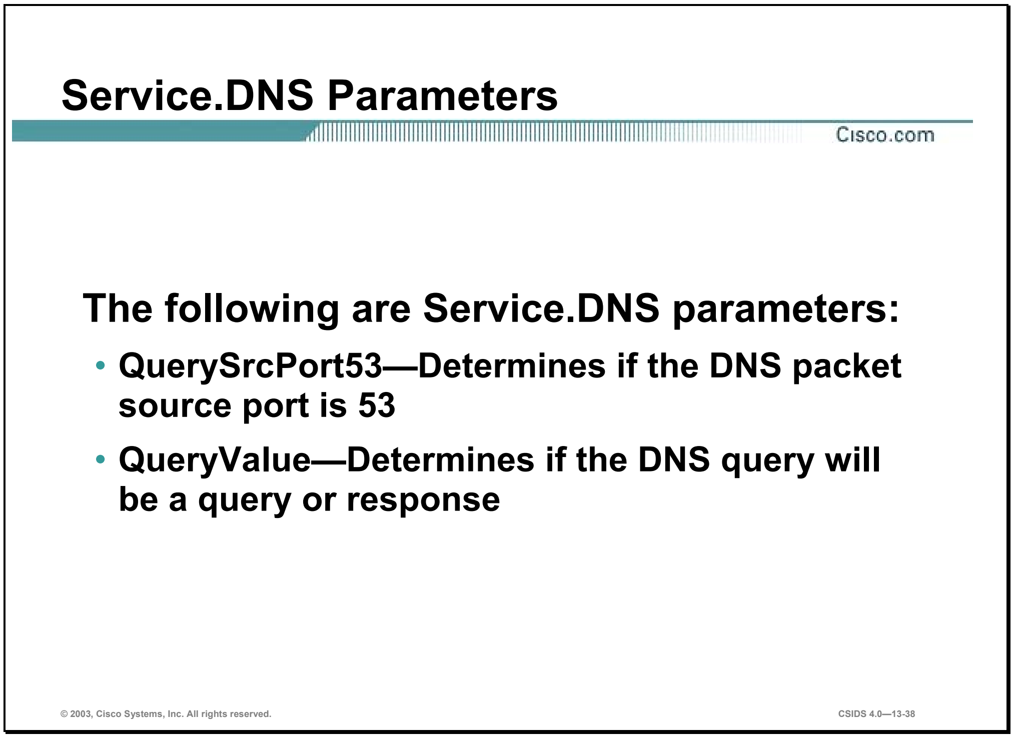
Service Signature Engines (cont.)

Engine Name	Engine Description
Service.NTP	Examines NTP traffic
Service.RPC	Examines RPC traffic
Service.SMB	Examines SMB traffic
Service.SMTP	Examines SMTP traffic
Service.SNMP	Examines SNMP traffic
Service.SSH	Examines SSH traffic
Service.Syslog	Examines Syslog traffic

CSIDS 4.0—13-37

- Service.NTP—Examines NTP traffic
- Service.RPC—Examines RPC traffic
- Service.SMB—Examines SMB traffic
- Service.SMTP—Examines SMTP traffic
- Service.SNMP—Examines SNMP traffic
- Service.SSH—Examines SSH traffic
- Service.Syslog—Examines Syslog traffic

Note The Service.SMTP signature engine is actually a pre-defined state machine that enables you to configure pattern matches for different states in the SMTP protocol. Therefore, this engine is explained in the State Signature Engines section later in this chapter.



Service.DNS Parameters

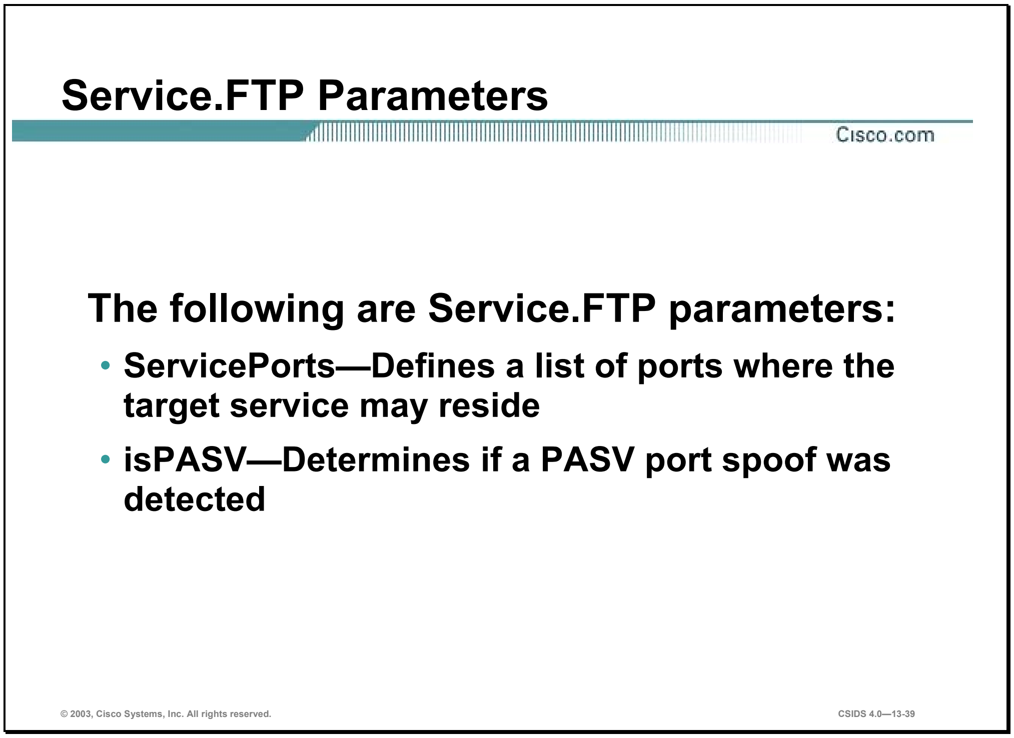
The following are Service.DNS parameters:

- **QuerySrcPort53—Determines if the DNS packet source port is 53**
- **QueryValue—Determines if the DNS query will be a query or response**

CSIDS 4.0—13-38

The following table shows examples of the Service.DNS parameters:

Parameter	Value	Attribute	Description
QuerySrcPort53	■ True ■ False	■ Not protected ■ Not required	Determines whether the DNS packet source port is port 53
Query Value	■ True ■ False	■ Not protected ■ Not required	Determines whether the DNS query will be a Query or Response



Service.FTP Parameters

Cisco.com

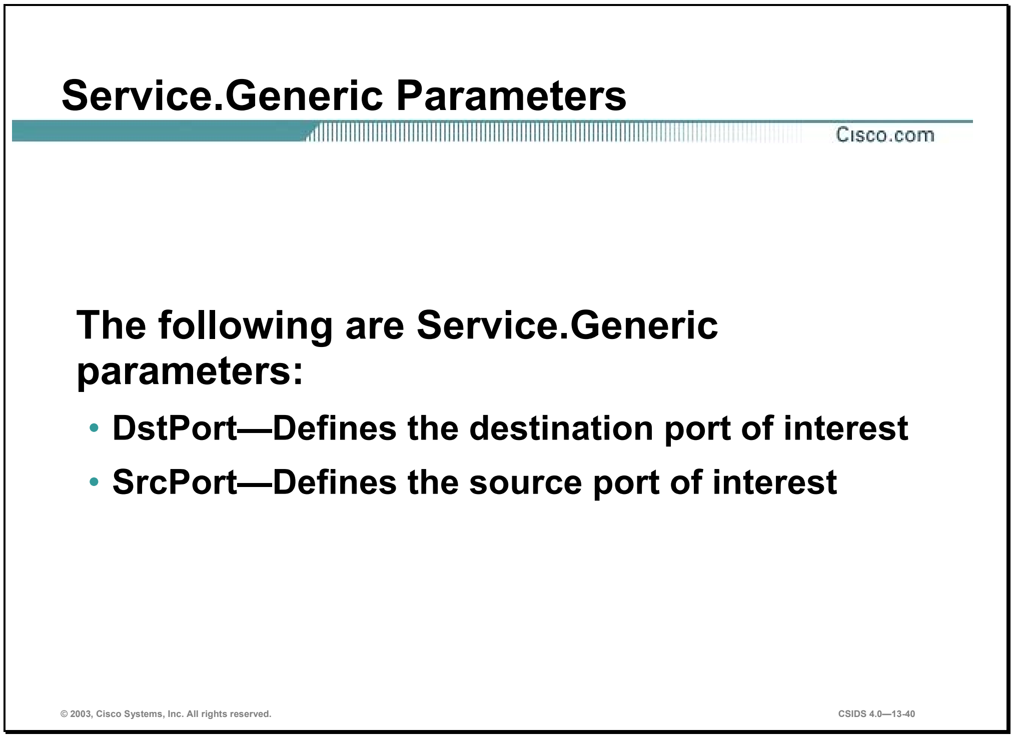
The following are Service.FTP parameters:

- **ServicePorts—Defines a list of ports where the target service may reside**
- **isPASV—Determines if a PASV port spoof was detected**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-39

The following table shows examples of the Service.FTP parameters:

Parameter	Value	Attribute	Description
ServicePorts	<set list>	■ Not protected ■ Not required	Defines a list of ports where the target service may reside
isPASV	■ True ■ False	■ Not protected ■ Not required	Determines whether a PASV port spoof was detected



Service.Generic Parameters

The following are Service.Generic parameters:

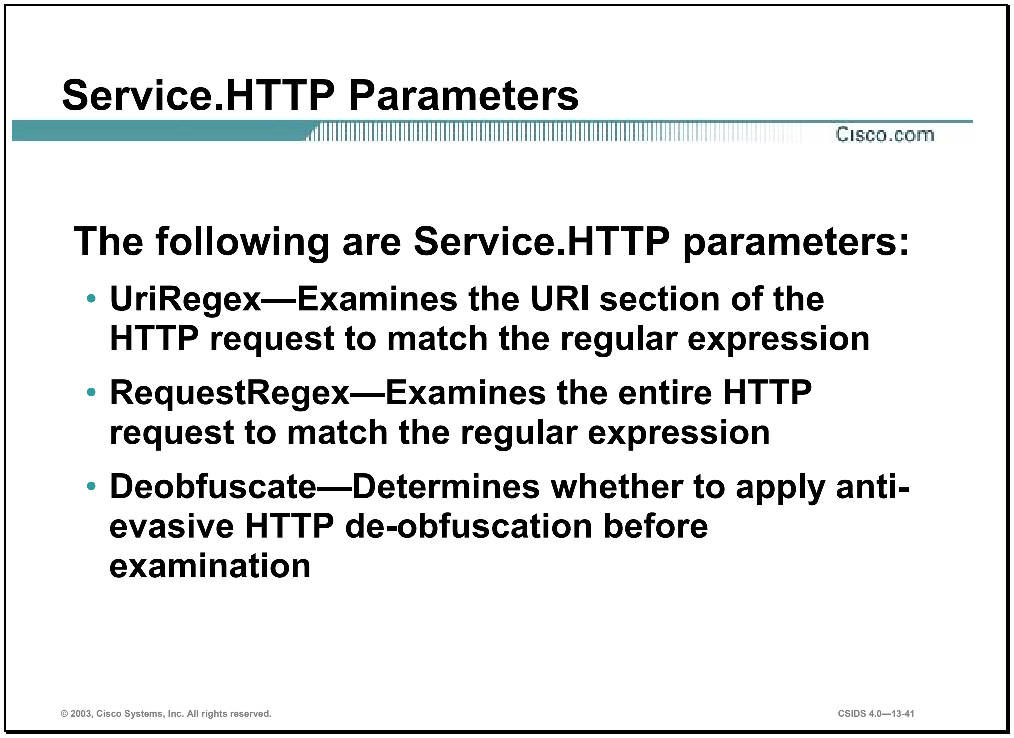
- **DstPort—Defines the destination port of interest**
- **SrcPort—Defines the source port of interest**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-40

The following table shows examples of the Service.Generic parameters:

Parameter	Value	Attribute	Description
DstPort	0–65535	■ Not protected ■ Not required	The destination port of interest for this signature
IntermediateInstructions	<string>	■ Protected ■ Not required	Assembly or machine code in string form. This field is for expert use only.

Caution Only expert users should attempt to create custom signatures with this engine.



Service.HTTP Parameters

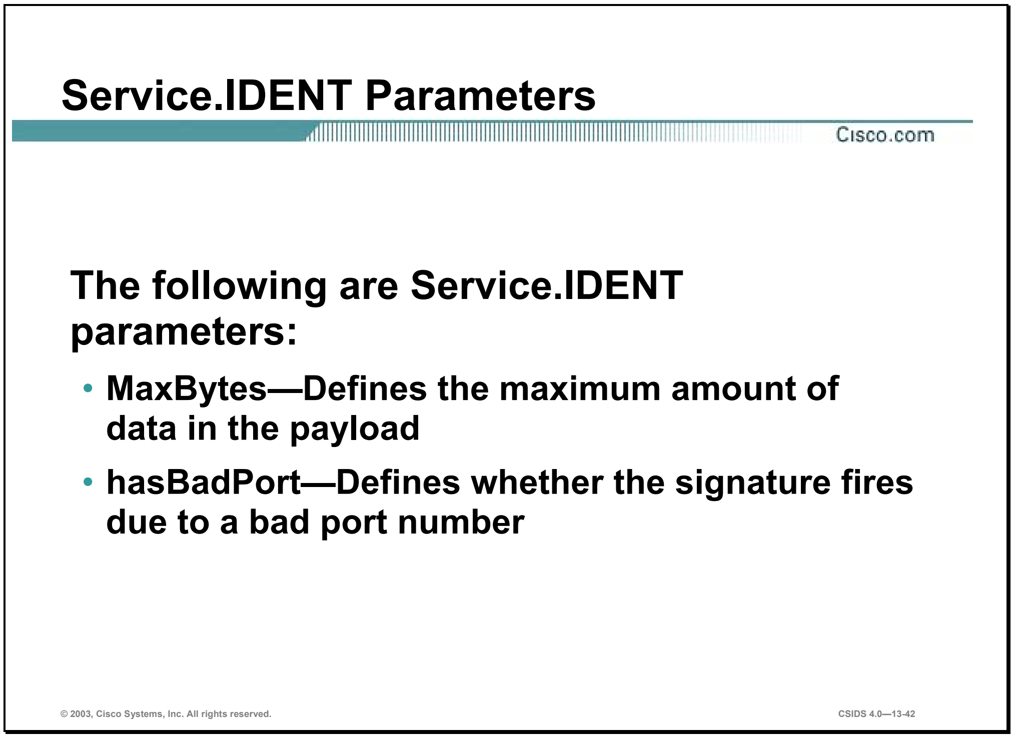
The following are Service.HTTP parameters:

- UriRegex—Examines the URI section of the HTTP request to match the regular expression
- RequestRegex—Examines the entire HTTP request to match the regular expression
- Deobfuscate—Determines whether to apply anti-evasive HTTP de-obfuscation before examination

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-41

The following table shows examples of the Service.HTTP parameters:

Parameter	Value	Attribute	Description
UriRegex	<string>	■ Protected ■ Not required	Examines the URI section of the HTTP request to match the regular expression
RequestRegex	<string>	■ Protected ■ Not required	Examines the entire HTTP request to match the regular expression
Deobfuscate	■ True ■ False	■ Not protected ■ Not required	Determines whether to apply anti-evasive HTTP de-obfuscation before examination



Service.IDENT Parameters

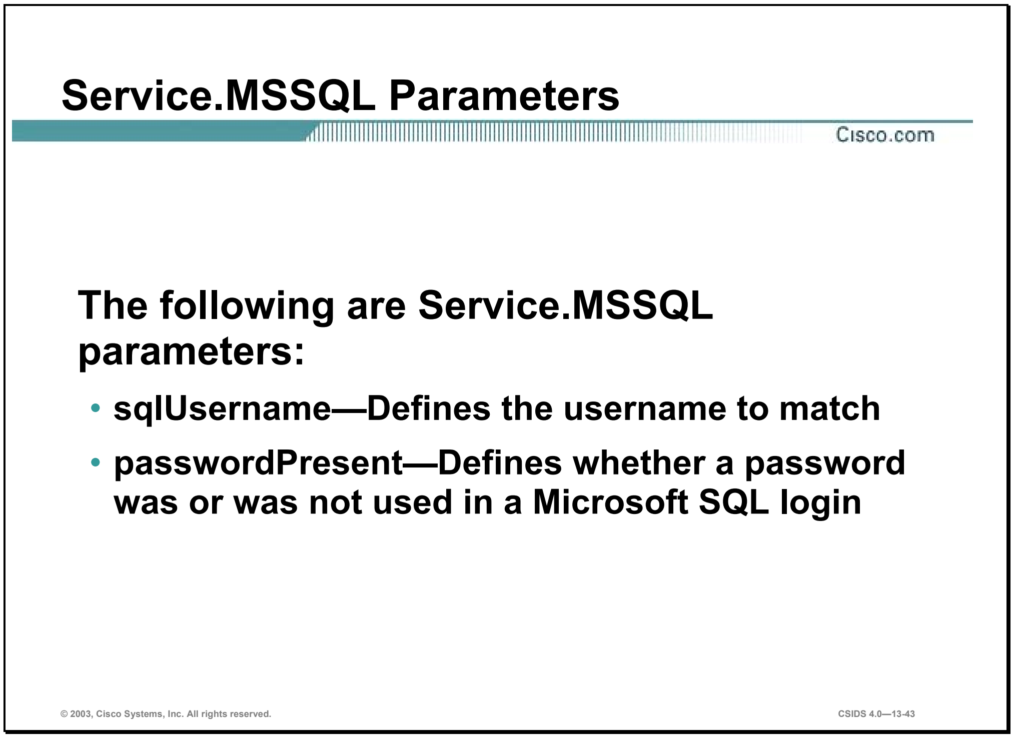
The following are Service.IDENT parameters:

- **MaxBytes—Defines the maximum amount of data in the payload**
- **hasBadPort—Defines whether the signature fires due to a bad port number**

CSIDS 4.0—13-42

The following table shows examples of the Service.IDENT parameters:

Parameter	Value	Attribute	Description
MaxBytes	0–65535	■ Not protected ■ Not required	Defines the maximum amount of data in the payload
hasBadPort	■ True ■ False	■ Not protected ■ Not required	Defines whether the signature fires due to a bad port number



Service.MSSQL Parameters

The following are Service.MSSQL parameters:

- **sqlUsername—Defines the username to match**
- **passwordPresent—Defines whether a password was or was not used in a Microsoft SQL login**

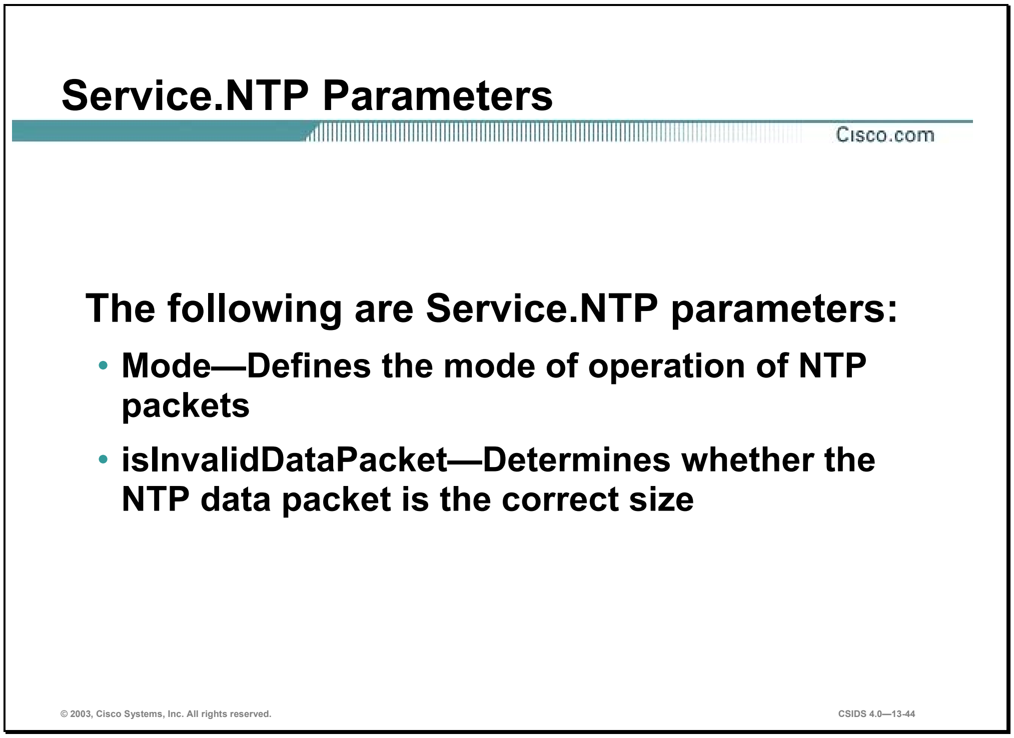
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-43

The Service.MSSQL engine inspects the protocol used by Microsoft SQL server. You can add custom signatures based on the MSSQL protocol values, such as the login username and whether a password was used.

The following table shows examples of the Service.MSSQL parameters:

Parameter	Value	Attribute	Description
sqlUsername	<string>	■ Not protected ■ Not required	Defines the username to match
passwordPresent	■ True ■ False	■ Not protected ■ Not required	Defines whether a password was or was not used in an MSSQL login



Service.NTP Parameters

The following are Service.NTP parameters:

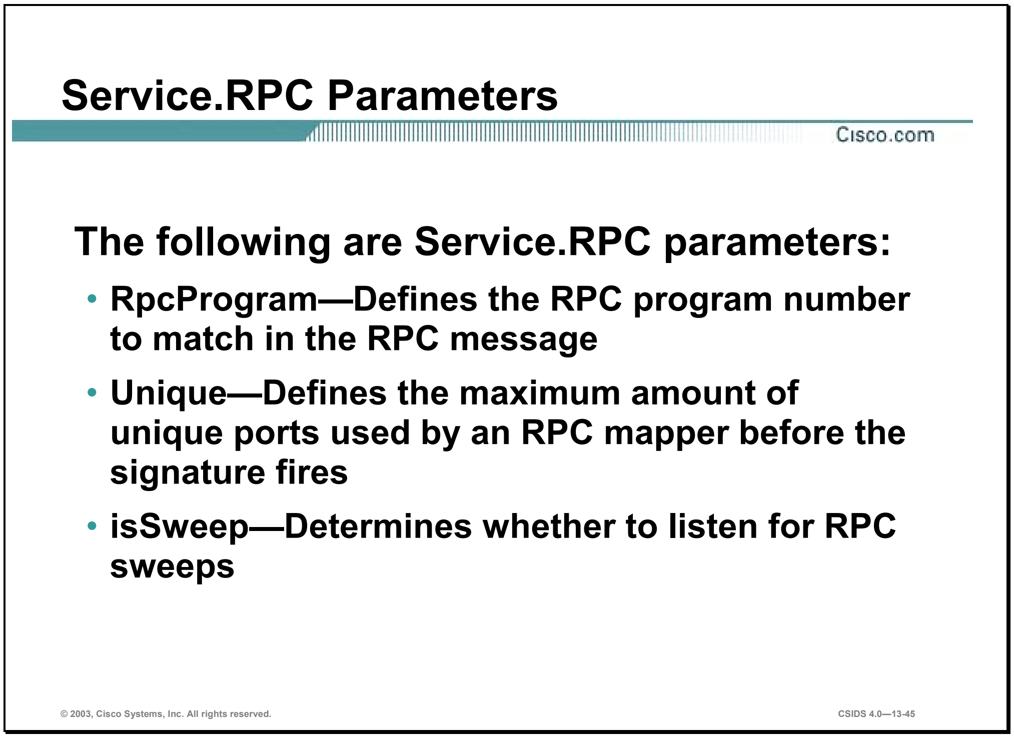
- Mode—Defines the mode of operation of NTP packets
- isInvalidDataPacket—Determines whether the NTP data packet is the correct size

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-44

The Service.NTP engine inspects the Network Time Protocol (NTP). The following table shows examples of the Service.NTP parameters:

Parameter	Value	Attribute	Description
Mode	0–7	■ Not protected ■ Not required	Defines the mode of operation of the NTP packets
isInvalidDataPacket	■ True ■ False	■ Not protected ■ Not required	Checks for incorrect NTP data packet structure



Service.RPC Parameters

Cisco.com

The following are Service.RPC parameters:

- **RpcProgram—Defines the RPC program number to match in the RPC message**
- **Unique—Defines the maximum amount of unique ports used by an RPC mapper before the signature fires**
- **isSweep—Determines whether to listen for RPC sweeps**

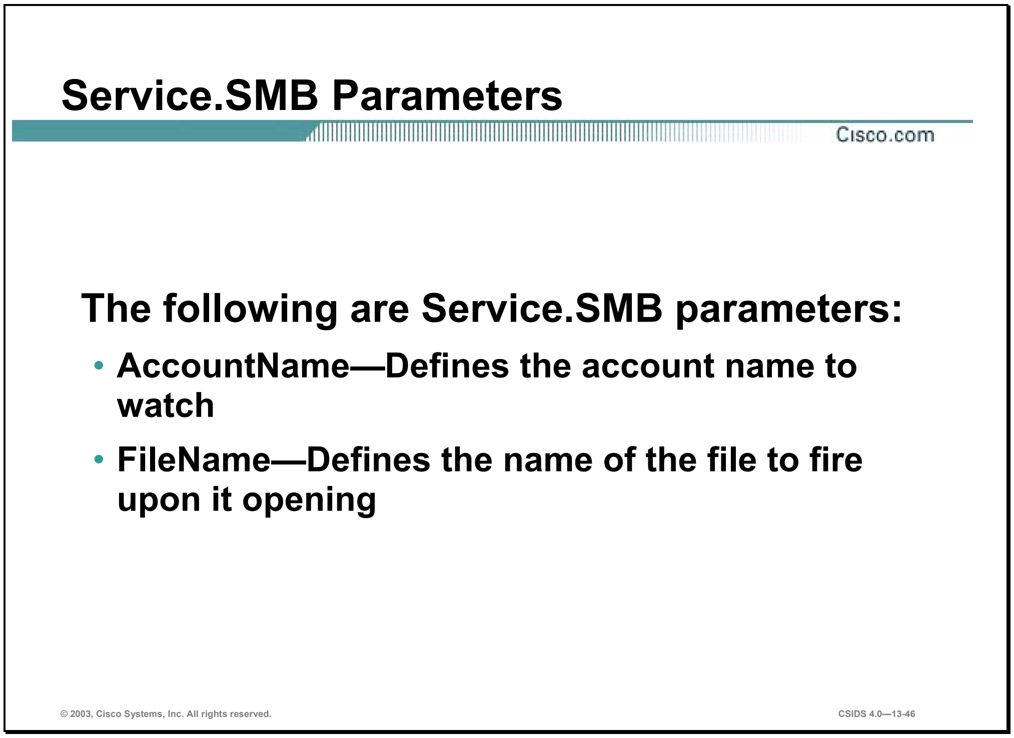
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-45

The Service.RPC signature engine decoder has the ability to fully decode an anti-evasive strategy. It can handle fragmented messages, one message in several packets, or batch messages, several messages in a single packet. The RPC port mapper operates on port 111. Regular RPC messages can be on any port greater than 550. RPC sweeps are like TCP port sweeps except that they only count unique ports when a valid RPC message is sent. They separate each RPC program type for sweep unique counting.

The following table shows examples of the Service.RPC parameters:

Parameter	Value	Attribute	Description
RpcProgram	0–99999	■ Not protected ■ Not required ■ Not required	Defines the RPC program number to match in the RPC message
Unique	2–40	■ Not protected ■ Not required	Defines the maximum number of unique ports used by an RPC mapper before the signature fires
isSweep	■ True ■ False	■ Not protected ■ Not required	Determines whether to listen for RPC sweeps. Unique must be set for this to be valid



Service.SMB Parameters

Cisco.com

The following are Service.SMB parameters:

- **AccountName—Defines the account name to watch**
- **FileName—Defines the name of the file to fire upon it opening**

CSIDS 4.0—13-46

The Service.SMB signature engine decodes the SMB protocol. The following built-in signatures are included in the Service.SMB signature engine:

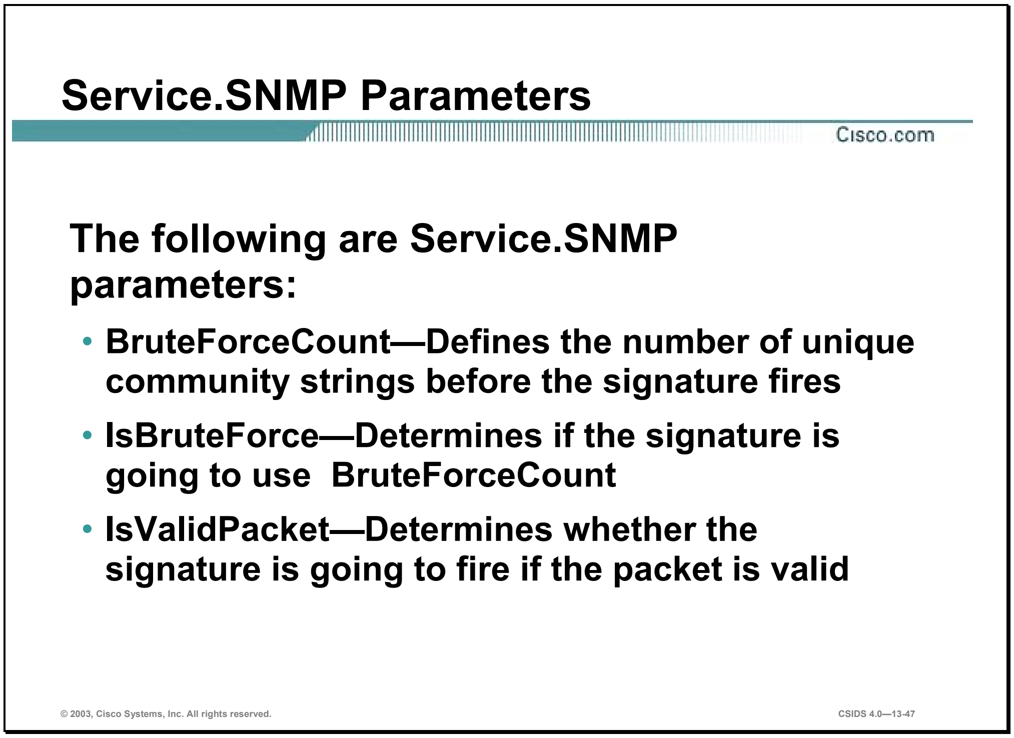
- 3303—Login successful with guest privileges
- 3304—NULL login attempt
- 3305—Windows 95, and Windows 98 password file access
- 3306—Remote registry access attempt
- 3307—RedButton reconnaissance
- 3308—Remote isarpc service access attempt
- 3309—Remote srvsvc service access attempt
- 6255—SMB login failure

Note The list of signatures changes with each signature update. This list applies to the 4.0 (S37) release.

The following table shows examples of the Service.SMB parameters:

Parameter	Value	Attribute	Description
AccountName	<string>	■ Not protected ■ Not required	Defines the account name to watch.
FileName	<string>	■ Not protected ■ Not required	Defines the file name to fire upon when this file is opened.

Caution You cannot add custom signatures to the Service.SMB signature engine. If you try to add custom signatures to the Service.SMB signature engine, you receive the following error message: Error: Array contains max entries, could not add new entry.



Service.SNMP Parameters

Cisco.com

The following are Service.SNMP parameters:

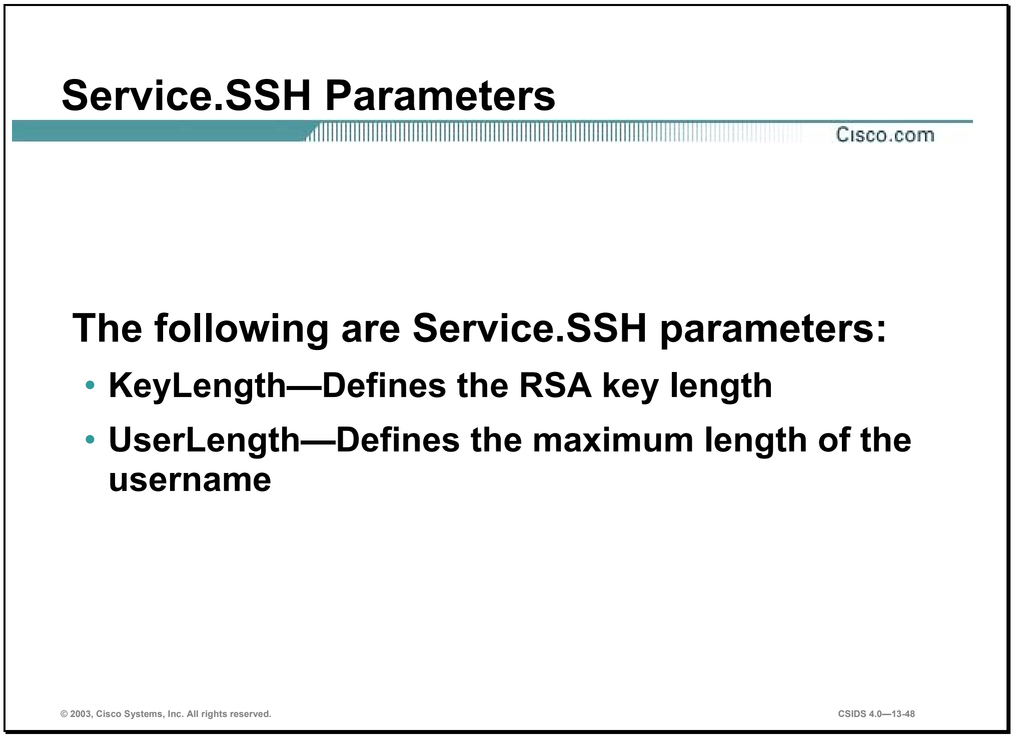
- **BruteForceCount—Defines the number of unique community strings before the signature fires**
- **IsBruteForce—Determines if the signature is going to use BruteForceCount**
- **IsValidPacket—Determines whether the signature is going to fire if the packet is valid**

CSIDS 4.0—13-47

The CommunityName strings are converted into an integer-sized hash, which speeds up the protocol decode and reduces storage space. The CommunityName decoded from the packet is also converted to an integer hash. Each CommunityName string should produce a near unique integer hash. These hashes are used to determine if the CommunityNames match. The hashes are also stored and compared to determine if a brute force attack was attempted.

The following table shows examples of the Service.SNMP parameters:

Parameter	Value	Attribute	Description
BruteForceCount	1–32	■ Not protected ■ Not required	Defines the number of unique community strings before the signature fires
IsBruteForce	■ True ■ False	■ Protected ■ Not required	Determines if the signature is going to use BruteForceCount
IsValidPacket	■ True ■ False	■ Protected ■ Required	The token that signifies an SNMP protocol violation



Service.SSH Parameters

The following are Service.SSH parameters:

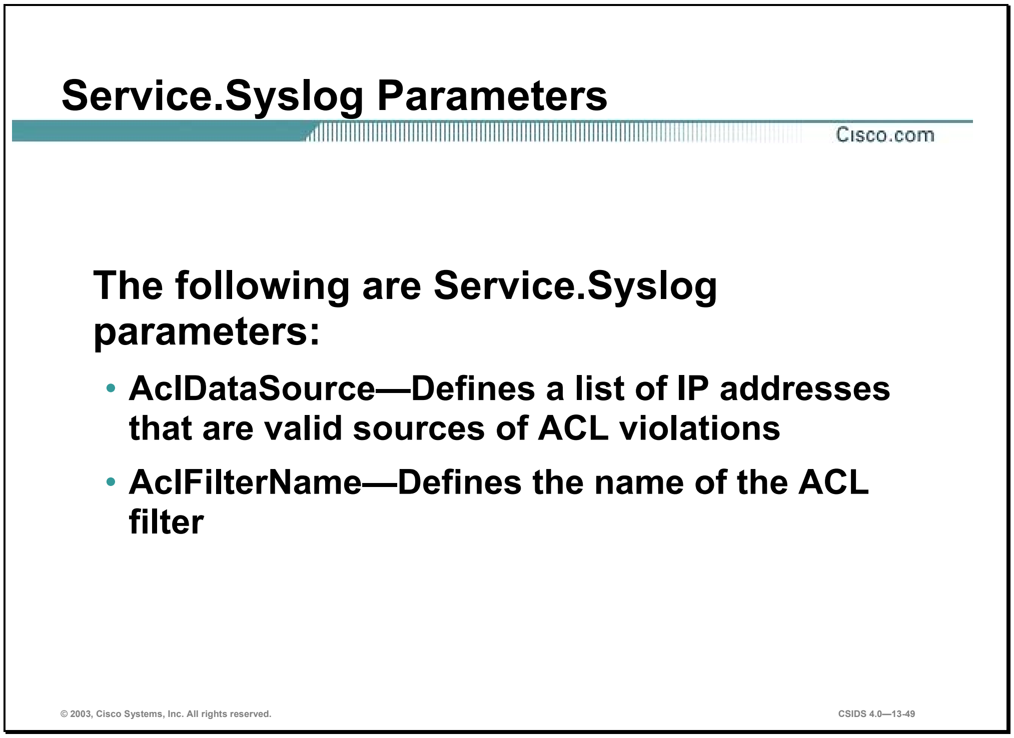
- **KeyLength—Defines the RSA key length**
- **UserLength—Defines the maximum length of the username**

CSIDS 4.0—13-48

The Service.SSH signature engine is specialized for port 22 SSH traffic. Because everything but the setup of an SSH session is encrypted, the engine only looks at the fields in the setup. There are two default signatures for SSH. You can tune these existing signatures, but you cannot add new SSH signatures.

The following table shows examples of the Service.SSH parameters:

Parameter	Value	Attribute	Description
KeyLength	0–65535	■ Not protected ■ Not required	Defines the RSA key length
UserLength	0–65535	■ Not protected ■ Not required	Defines the maximum length of the username



Service.Syslog Parameters

The following are Service.Syslog parameters:

- **AclDataSource—Defines a list of IP addresses that are valid sources of ACL violations**
- **AclFilterName—Defines the name of the ACL filter**

CSIDS 4.0—13-49

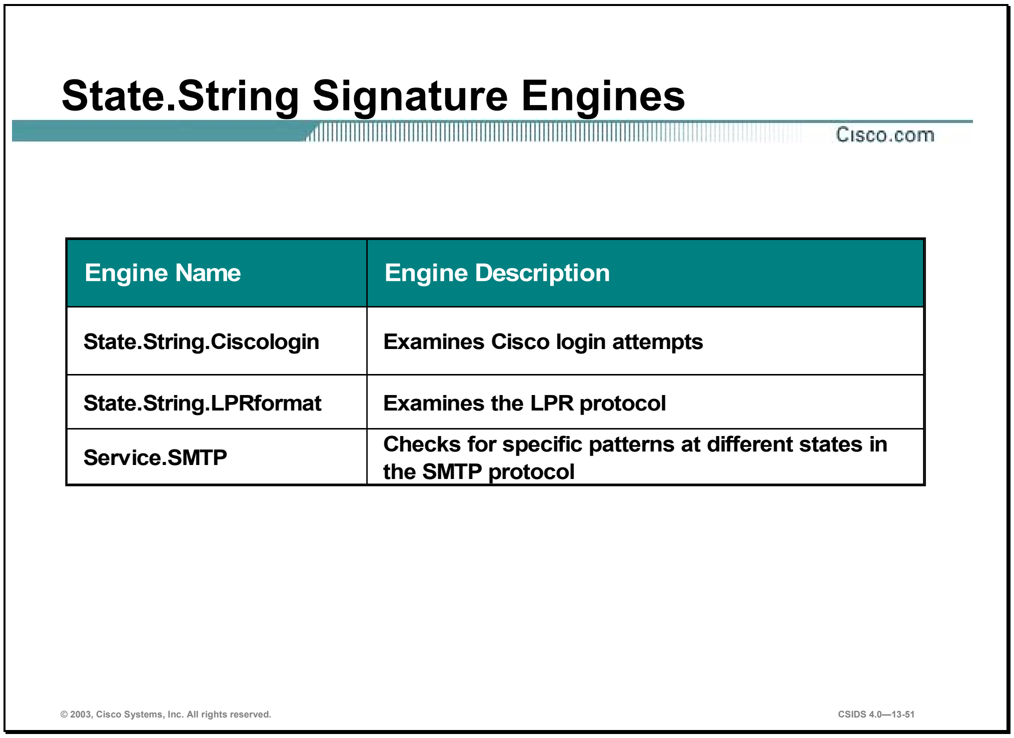
The Syslog signature engine analyzes traffic directed at the Syslog port, 514 UDP. It provides specialized handling of the contents of the Syslog data. If the contents of the Syslog match the predetermined format for a Cisco access control list (ACL) policy violation message, the contents of the Syslog are used to generate an alert. Any Syslog that does not match the ACL format is ignored.

The following table shows examples of the Service.Syslog parameters:

Parameter	Value	Attribute	Description
AclDataSource	<string>	■ Not protected ■ Not required	A comma-separated list of IP addresses that are valid sources of ACL violations
AclFilterName	<string>	■ Not protected ■ Not required	Defines the name of the ACL filter

State Signature Engines

This section discusses the State signature engines and the specific configuration parameters.



State.String Signature Engines

Cisco.com

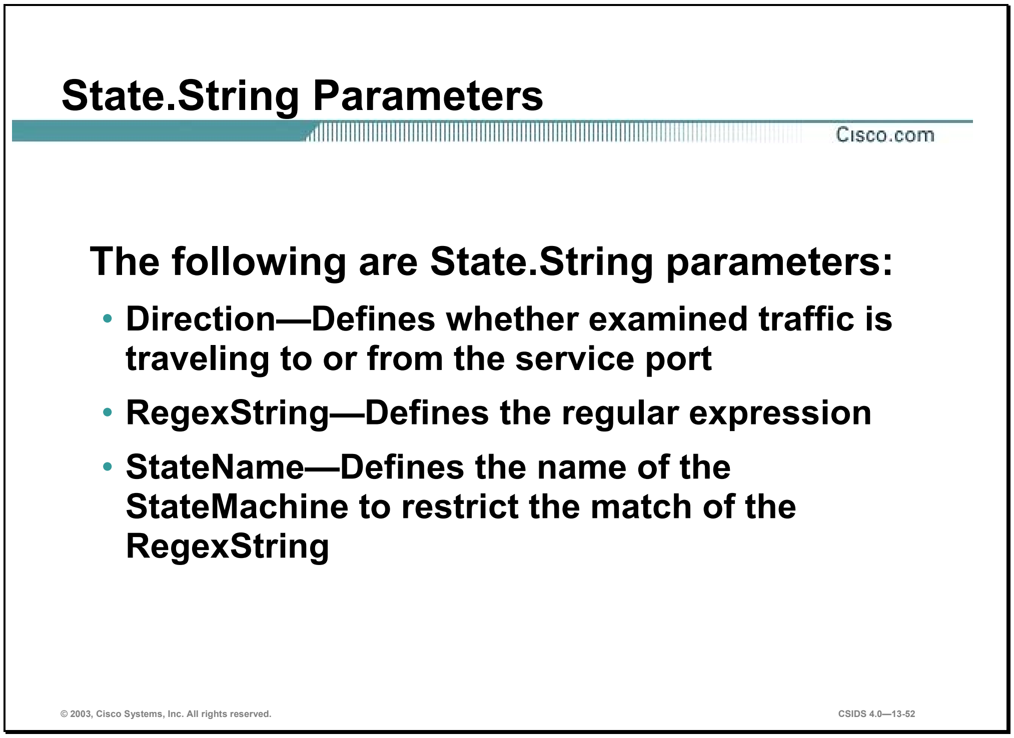
Engine Name	Engine Description
State.String.Ciscologin	Examines Cisco login attempts
State.String.LPRformat	Examines the LPR protocol
Service.SMTP	Checks for specific patterns at different states in the SMTP protocol

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-51

Some protocols have different states. Searching for specific patterns at these various states enables you to create robust signatures. State machines provide this capability. A state machine consists of a starting state and a list of valid state transitions. It stores the state of something and at a given time can operate on input to move from one state to another and/or cause an action or output to take place. State machines are used to describe a specific event that causes an output or alarm. Cisco IDS supports the following state machine engines:

- State.String.Ciscologin—Checks for specific patterns at different states in the Cisco login process
- State.String.LPRformat—Inspects the LPR protocol
- Service.SMTP—Checks for specific patterns at different states in the SMTP protocol



State.String Parameters

Cisco.com

The following are State.String parameters:

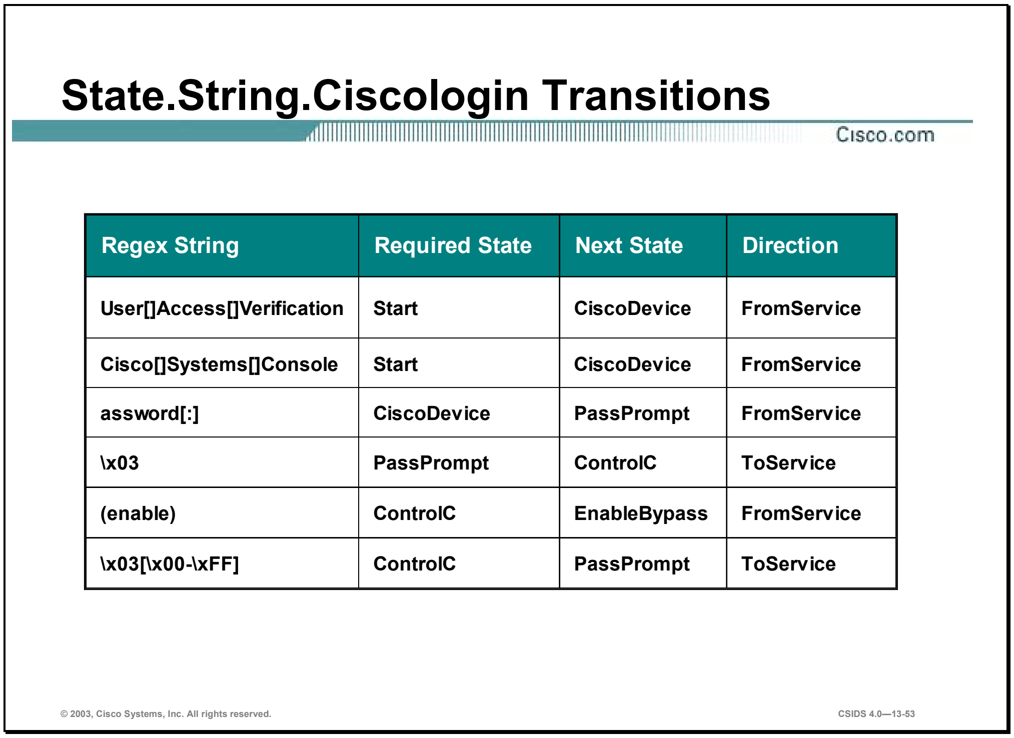
- **Direction—Defines whether examined traffic is traveling to or from the service port**
- **RegexString—Defines the regular expression**
- **StateName—Defines the name of the StateMachine to restrict the match of the RegexString**

CSIDS 4.0—13-52

All state machine engines share the parameters of the State.String signature engine. The following table shows examples of the State.String parameters:

Parameter	Value	Attribute	Description
Direction	■ ToService ■ FromService	■ Protected ■ Required	Defines whether the Sensor is listening to traffic destined to or from the service port or both
RegexString	<string>	■ Protected ■ Required	Defines the regular expression
StateName	■ CiscoLogin ■ LPRFormatString	■ Protected ■ Required	Defines the name of the StateMachine to restrict the match of the RegexString

The RegexString parameter specifies the pattern to search for. The StateName parameter specifies the state that the state machine must be in for the signature to begin the search.



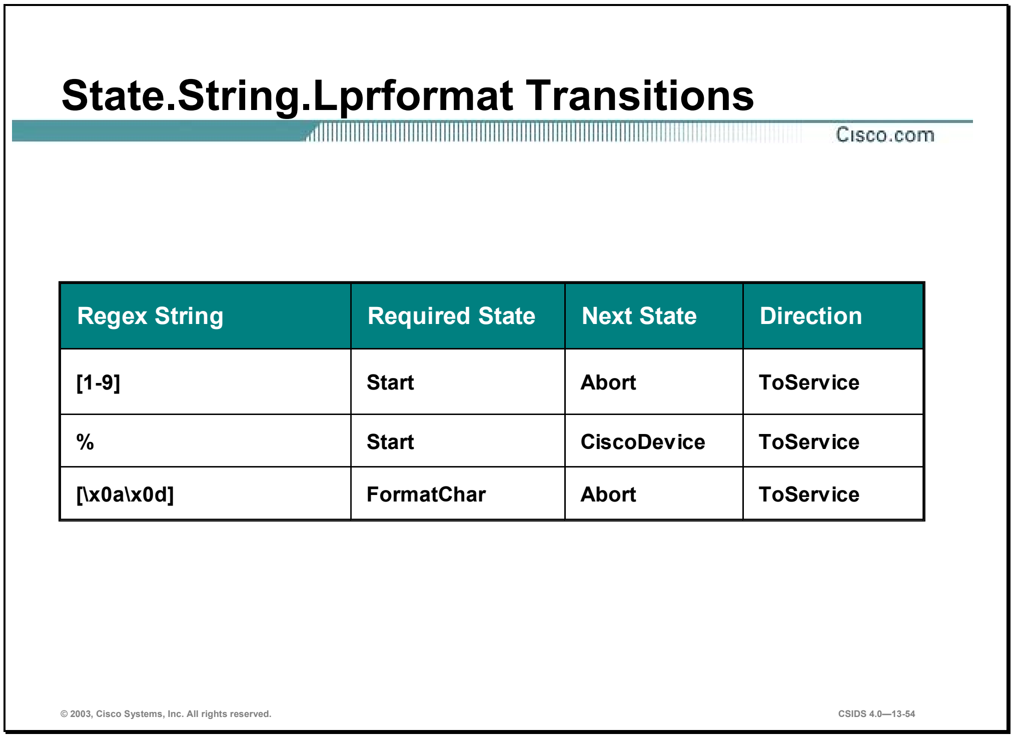
State.String.Ciscologin Transitions

Regex String	Required State	Next State	Direction
User[]Access[]Verification	Start	CiscoDevice	FromService
Cisco[]Systems[]Console	Start	CiscoDevice	FromService
assword[:]	CiscoDevice	PassPrompt	FromService
\x03	PassPrompt	ControlC	ToService
(enable)	ControlC	EnableBypass	FromService
\x03[\x00-\xFF]	ControlC	PassPrompt	ToService

CSIDS 4.0—13-53

The following table lists the State.String.Ciscologin transitions:

Regex String	Required State	Next State	Direction
UserAccessVerifiction	Start	CiscoDevice	FromService
CiscoSystemsConsole	Start	CiscoDevice	FromService
assword[:]	CiscoDevice	PassPrompt	FromService
\x03	PassPrompt	ControlC	ToService
(enable)	ControlC	EnableBypass	FromService
\x03[\x00-\xFF]	ControlC	PassPrompt	ToService



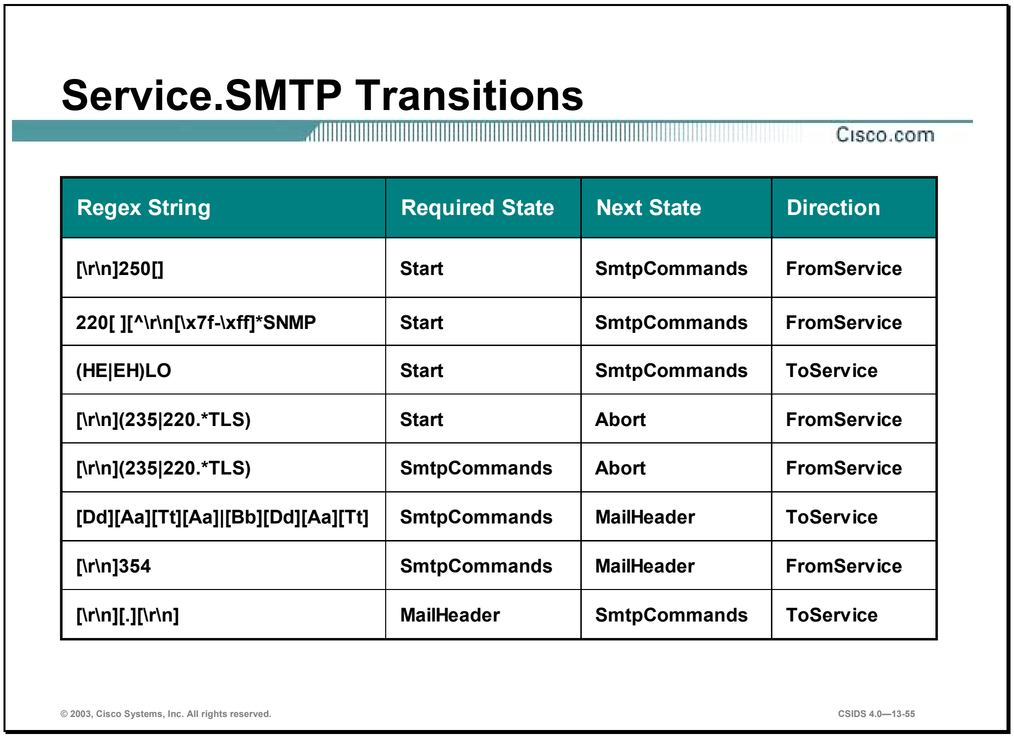
State.String.Lprformat Transitions

Regex String	Required State	Next State	Direction
[1-9]	Start	Abort	ToService
%	Start	CiscoDevice	ToService
[\x0a\x0d]	FormatChar	Abort	ToService

CSIDS 4.0—13-54

The following table lists the State.String.Lprformat transitions:

Regex String	Required State	Next State	Direction
[1-9]	Start	Abort	ToService
%	Start	CiscoDevice	ToService
[\x0a\x0d]	FormatChar	Abort	ToService



Service.SMTP Transitions

Cisco.com

Regex String	Required State	Next State	Direction
[\r\n]250[]	Start	SmtpCommands	FromService
220[ ][^\r\n[\x7f-\xff]*SNMP	Start	SmtpCommands	FromService
(HE|EH)LO	Start	SmtpCommands	ToService
[\r\n](235|220.*TLS)	Start	Abort	FromService
[\r\n](235|220.*TLS)	SmtpCommands	Abort	FromService
[Dd][Aa][Tt][Aa]|[Bb][Dd][Aa][Tt]	SmtpCommands	MailHeader	ToService
[\r\n]354	SmtpCommands	MailHeader	FromService
[\r\n][.][\r\n]	MailHeader	SmtpCommands	ToService

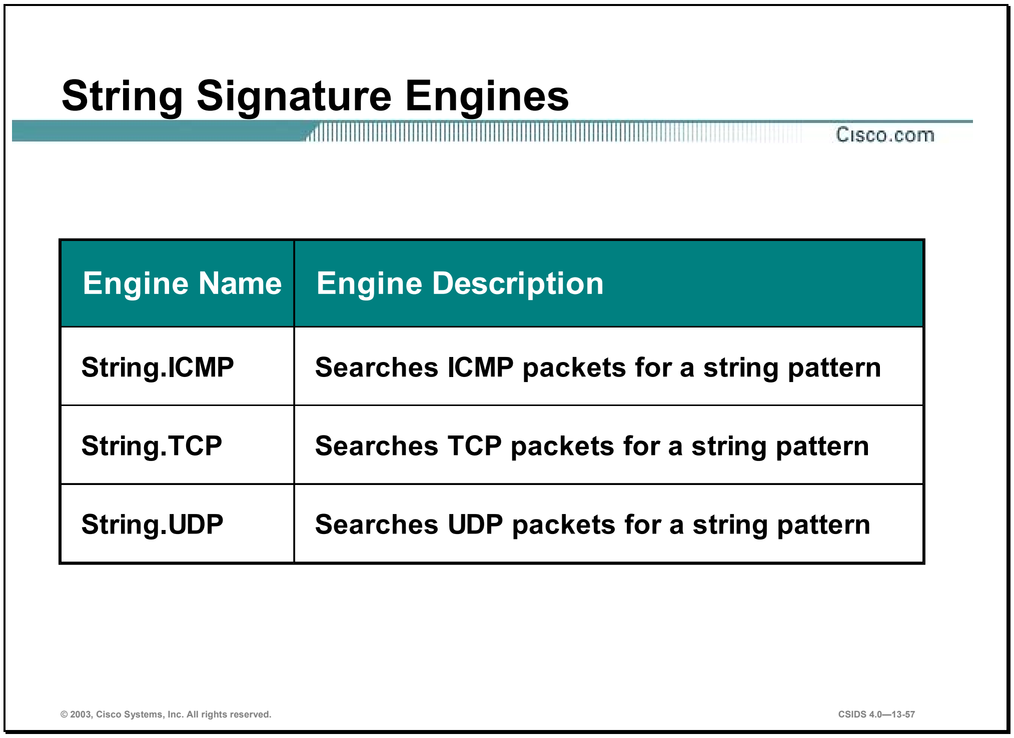
CSIDS 4.0—13-55

The following table lists the Service.SMTP transitions:

Regex String	Required State	Next State	Direction
[\r\n[250[]	Start	SmtpCommands	FromService
220[ ][^\r\n[\x7f-\xff]*SNMP	Start	SmtpCommands	FromService
(HE|EH)LO	Start	SmtpCommands	ToService
[\r\n](235|220.*TLS)	Start	Abort	FromService
[\r\n](235|220.*TLS)	SmtpCommands	Abort	FromService
[Dd][Aa][Tt][Aa]|[Bb][Dd][Aa][Tt]	SmtpCommands	MailHeader	ToService
[\r\n]354	SmtpCommands	MailHeader	FromService
[\r\n][.][\r\n]	MailHeader	SmtpCommands	ToService
[\r\n][2][0-9][0-9][ ]	MailHeader	SmtpCommands	FromService
([\r][\n]|[\n][\r]){2}	MailHeader	MailBody	ToService
[\r\n][.][\r\n]	MailBody	SmtpCommands	ToService
[\r\n][2][0-9][0-9][ ]	MailBody	SmtpCommands	FromService

String Signature Engines

This section discusses the string signature engines and their specific configuration parameters.



String Signature Engines

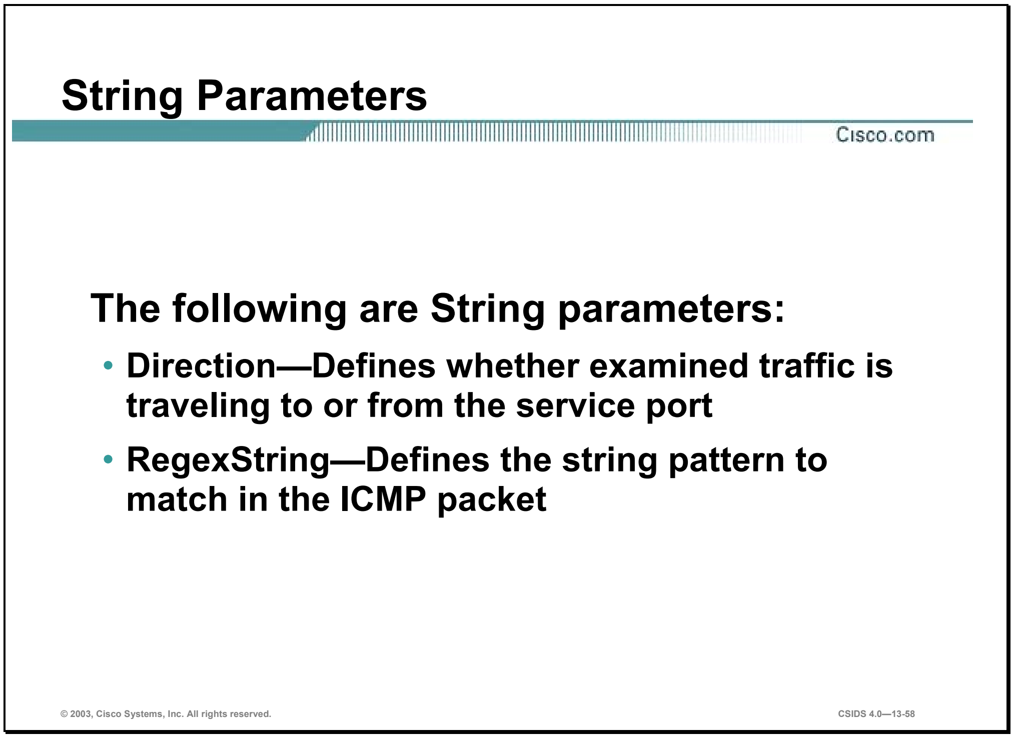
Cisco.com

Engine Name	Engine Description
String.ICMP	Searches ICMP packets for a string pattern
String.TCP	Searches TCP packets for a string pattern
String.UDP	Searches UDP packets for a string pattern

CSIDS 4.0—13-57

The String signature engines support regular expression pattern matching and alarm functionality for ICMP, UDP and TCP. The following are String signature engines:

- String.ICMP—Searches ICMP packets for a string pattern
- String.TCP—Searches TCP packets for a string pattern
- String.UDP—Searches UDP packets for a string pattern



String Parameters

The following are String parameters:

- Direction—Defines whether examined traffic is traveling to or from the service port
- RegexString—Defines the string pattern to match in the ICMP packet

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-58

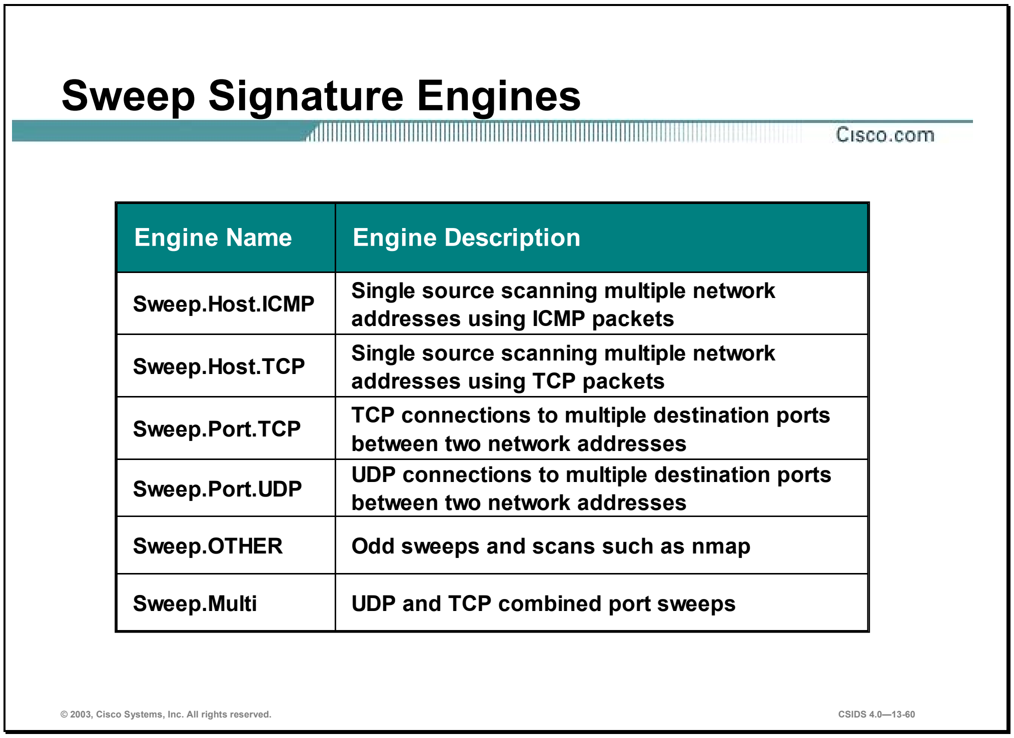
The three String signature engines share common parameters. Each engine supports signatures that search its specific protocol for configured patterns.

Examples of these parameters are shown in the following table:

Parameter	Value	Attribute	Description
Direction	■ ToService ■ FromService	■ Protected ■ Not required	Defines if examined traffic is traveling to or from the service port
RegexString	<string>	■ Protected ■ Not required	Defines the string pattern to match in the packet

Sweep Signature Engines

This section discusses the Sweep signature engines and their specific configuration parameters.



Sweep Signature Engines

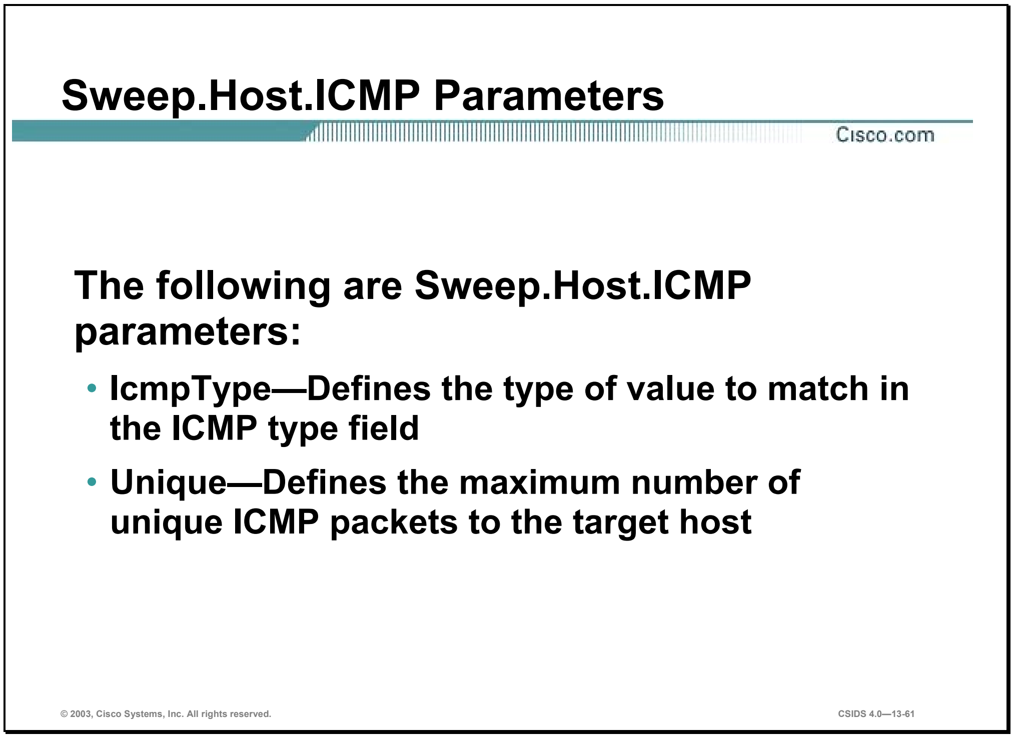
Cisco.com

Engine Name	Engine Description
Sweep.Host.ICMP	Single source scanning multiple network addresses using ICMP packets
Sweep.Host.TCP	Single source scanning multiple network addresses using TCP packets
Sweep.Port.TCP	TCP connections to multiple destination ports between two network addresses
Sweep.Port.UDP	UDP connections to multiple destination ports between two network addresses
Sweep.OTHER	Odd sweeps and scans such as nmap
Sweep.Multi	UDP and TCP combined port sweeps

CSIDS 4.0—13-60

The Sweep signature engines detect attacks in which one system makes connections to multiple hosts or multiple ports. The following are Sweep signature engines:

- Sweep.Host.ICMP—Detects a single source scanning multiple network addresses using ICMP packets
- Sweep.Host.TCP—Detects a single source scanning multiple network addresses using TCP packets
- Sweep.Port.TCP—Detects TCP connections to multiple destination ports between two network addresses
- Sweep.Port.UDP—Detects UDP connections to multiple destination ports between two network addresses
- Sweep.OTHER—Detects odd sweeps and scans (for example, nmap)
- Sweep.Multi—Detects UDP and TCP combined port sweeps



Sweep.Host.ICMP Parameters

Cisco.com

The following are Sweep.Host.ICMP parameters:

- **IcmpType—Defines the type of value to match in the ICMP type field**
- **Unique—Defines the maximum number of unique ICMP packets to the target host**

CSIDS 4.0—13-61

The following table shows examples of the Sweep.Host.ICMP parameters:

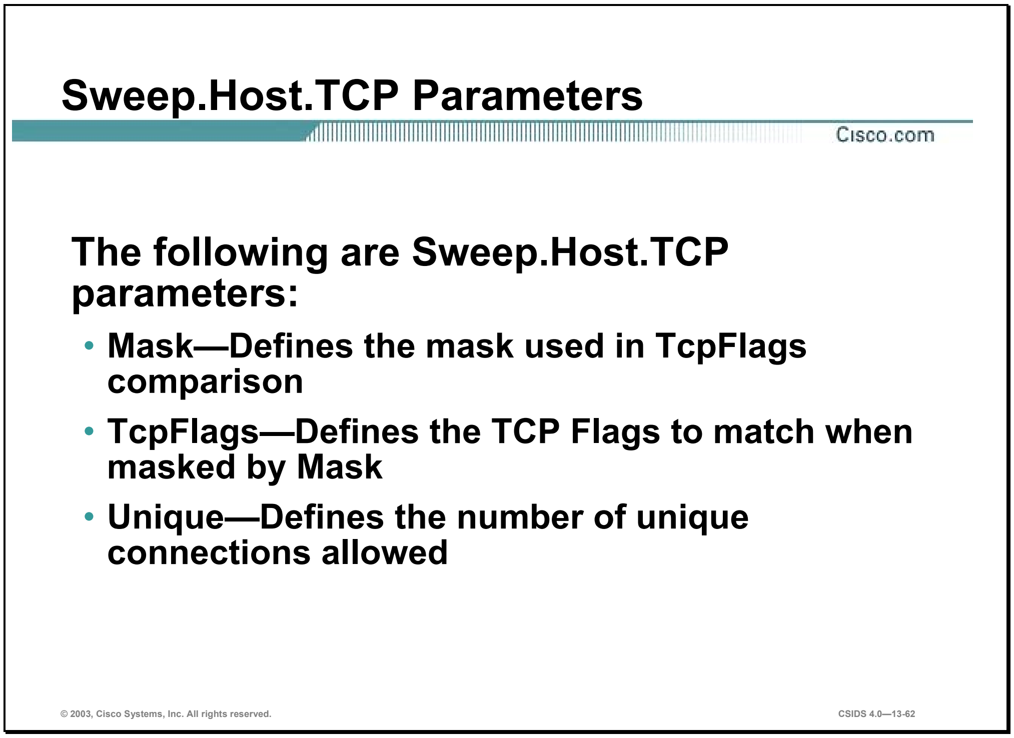
Parameter	Value	Attribute	Description
IcmpType	0–255	■ Not protected ■ Required	Defines the type value to match in the ICMP type field
Unique	2–40	■ Not protected ■ Required	Defines the maximum number of unique ICMP packets to the target host

The IcmpType parameter defines the type of ICMP traffic that can trigger the signature. The Unique parameter specifies how many instances of the ICMP traffic are required to trigger the signature. If you do not specify a value using the IcmpType parameter, the signature uses all ICMP traffic.

Each of the Sweep signature engines' alarm conditions ultimately depend on the count of the Unique parameter. The Unique parameter is the threshold parameter that triggers firing of the alarm when more than the Unique number of ports or hosts is detected on the address set within the time period. The processing of a Unique port and host tracking is called counting.

The Sweep signature engines use the ResetAfterIdle master parameter to clear the current value of the Unique counter. The value is cleared, or reset, when no traffic has passed between the hosts for the period of time specified by the ResetAfterIdle parameter. This means that the hosts being tracked on the address set did not have any traffic in the last X seconds.

Note The address set is determined by the value of the SummaryKey master parameter.



Sweep.Host.TCP Parameters

Cisco.com

The following are Sweep.Host.TCP parameters:

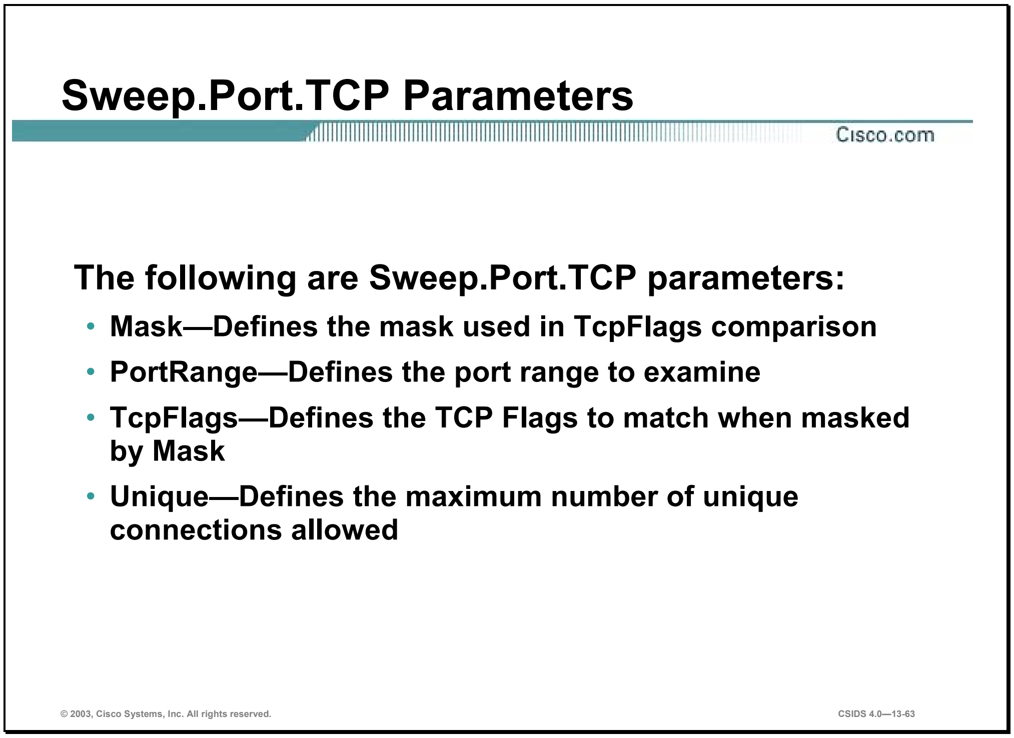
- **Mask—Defines the mask used in TcpFlags comparison**
- **TcpFlags—Defines the TCP Flags to match when masked by Mask**
- **Unique—Defines the number of unique connections allowed**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-62

The following table lists the Sweep.Host.TCP parameters:

Parameter	Value	Attribute	Description
Mask	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Required	Defines the mask used in TcpFlags comparisons
TcpFlags	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Required	Defines the TCP Flags to match as defined by Mask
Unique	2–40	■ Not protected ■ Required	Defines the number of unique connections allowed



Sweep.Port.TCP Parameters

Cisco.com

The following are Sweep.Port.TCP parameters:

- **Mask—Defines the mask used in TcpFlags comparison**
- **PortRange—Defines the port range to examine**
- **TcpFlags—Defines the TCP Flags to match when masked by Mask**
- **Unique—Defines the maximum number of unique connections allowed**

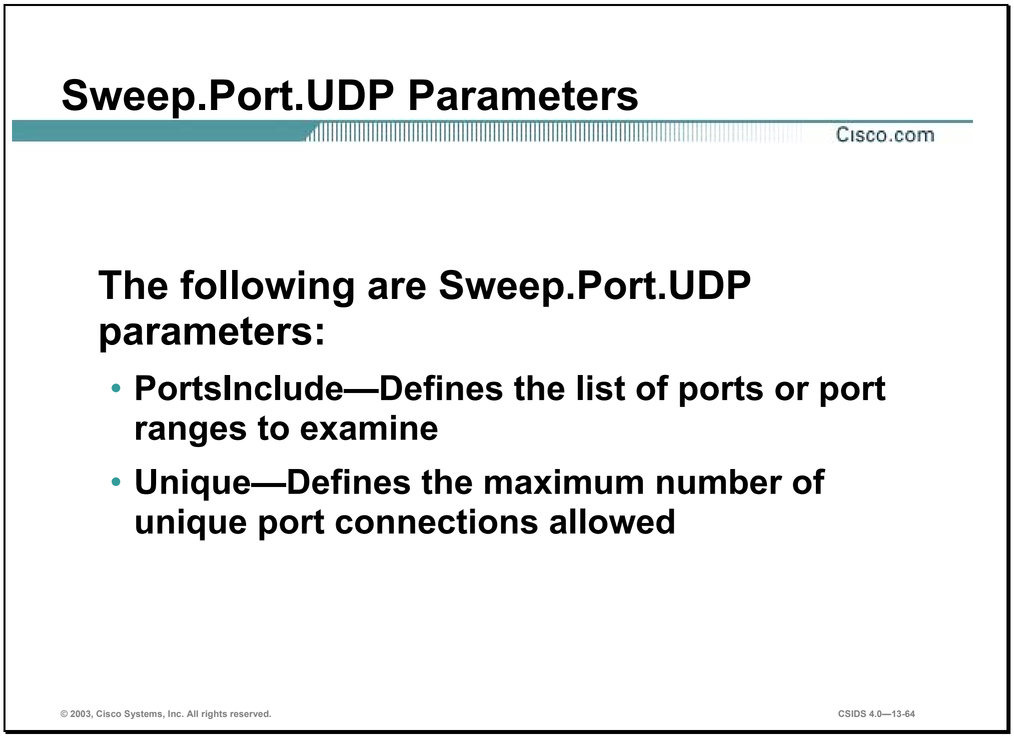
CSIDS 4.0—13-63

The Sweep.Port.TCP signature engine supports signatures that detect when a single host attempts to connect to multiple TCP ports on the same target system.

The following table shows examples of the Sweep.Port.TCP parameters:

Parameter	Value	Attribute	Description
Mask	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Required	Defines the mask used in TcpFlags comparison
PortRange	■ 1-Low ■ 2-High ■ 0-All	■ Not protected ■ Required	Defines the port range to examine
TcpFlags	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Required	Defines the TCP Flags to match as defined by Mask

Parameter	Value	Attribute	Description
Unique	2–40	■ Not protected ■ Required	Defines the maximum number of unique connections allowed



Sweep.Port.UDP Parameters

Cisco.com

The following are Sweep.Port.UDP parameters:

- PortsInclude—Defines the list of ports or port ranges to examine
- Unique—Defines the maximum number of unique port connections allowed

© 2003, Cisco Systems, Inc. All rights reserved.

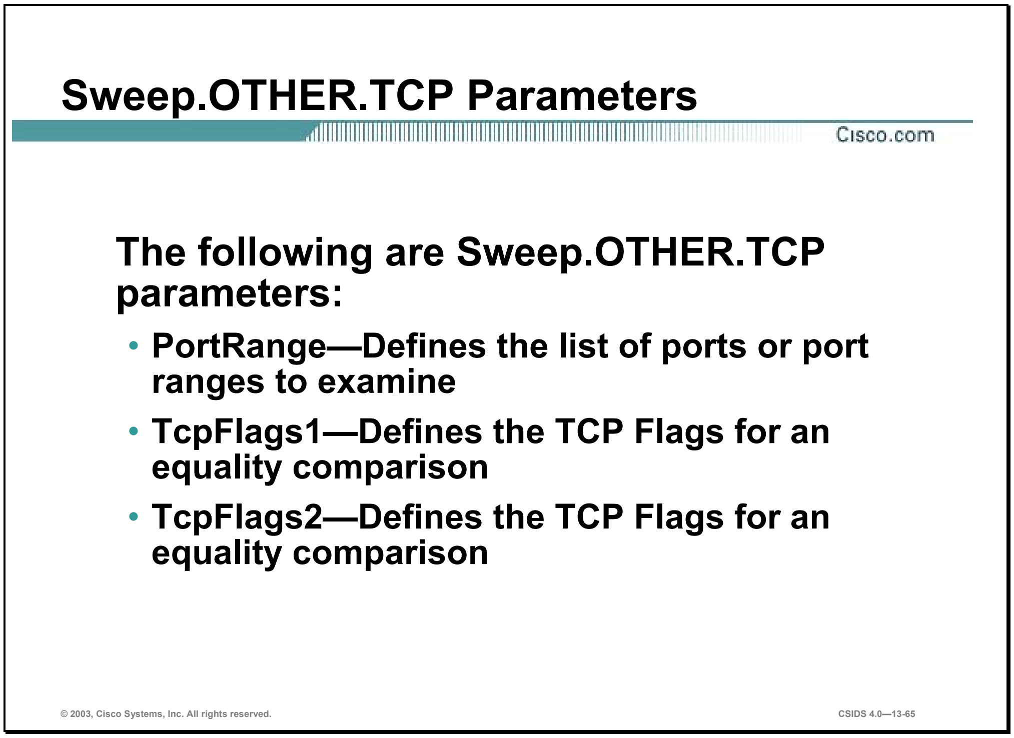
CSIDS 4.0—13-64

The Sweep.Port.UDP signature engine supports signatures that detect when a single host attempts to connect to multiple UDP ports on the same target system.

The following table shows examples of the Sweep.Port.UDP parameters:

Parameter	Value	Attribute	Description
PortsInclude	<set list>	■ Not protected ■ Not required	Defines the list of ports or port ranges to examine
Unique	2–40	■ Not protected ■ Required	Defines the maximum number of unique port connections allowed

The PortsInclude parameter enables you to specify a comma-separated list that indicates which UDP ports the signature will use when looking for unique connections. Ports not included in the list will have no impact on the signature.



Sweep.OTHER.TCP Parameters

Cisco.com

The following are Sweep.OTHER.TCP parameters:

- **PortRange—Defines the list of ports or port ranges to examine**
- **TcpFlags1—Defines the TCP Flags for an equality comparison**
- **TcpFlags2—Defines the TCP Flags for an equality comparison**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-65

The Sweep.Other.TCP signature engine supports signatures that trigger when a mixture of TCP packets, with different flags set, is detected on the network. Examples of this type of sweep are the Queso or NMAP sweeps that send odd TCP Flag combinations and attempt to fingerprint the operating system of the target machine. This engine does not do Unique counting like the other Sweep signature engines.

The following table shows examples of the Sweep.OTHER.TCP parameters:

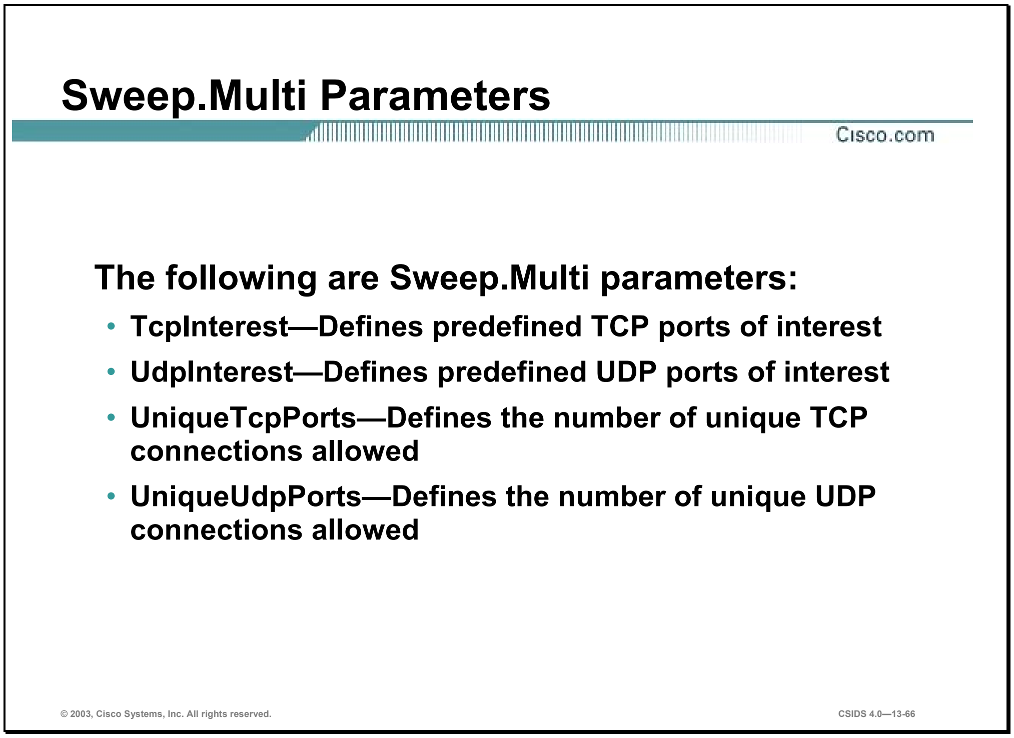
Parameter	Value	Attribute	Description
PortRange	<set list>	■ Not protected ■ Not required	Defines the list of ports or port ranges to examine
TcpFlags1	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Required	Defines the TCP Flags to match
TcpFlags2	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Not required	Defines the TCP Flags to match

Parameter	Value	Attribute	Description
TcpFlags3	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Not required	Defines the TCP Flags to match
TcpFlags4	■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO	■ Not protected ■ Not required	Defines the TCP Flags to match

The PortRange parameter identifies ports that are valid for the signature to process. You can specify any of the following as valid ports:

- 0—All ports
- 1—Low ports (1–1024)
- 2—High ports (1025–65535)

The TcpFlags1, TcpFlags2, TcpFlags3, and TcpFlags4 parameters enable you to specify up to four different sets of TCP Flag combinations. Each of the TCP Flag combinations that you specify must be detected before the signature triggers. Unlike other TCP-based engines, this engine does not have a Mask parameter. The signature looks for the flags specified in the TcpFlags parameter and ignores any other TCP Flags.



Sweep.Multi Parameters

Cisco.com

The following are Sweep.Multi parameters:

- **TcpInterest—Defines predefined TCP ports of interest**
- **UdpInterest—Defines predefined UDP ports of interest**
- **UniqueTcpPorts—Defines the number of unique TCP connections allowed**
- **UniqueUdpPorts—Defines the number of unique UDP connections allowed**

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—13-66

The Sweep.Multi signature engine detects cross-protocol sweeps, such as those perpetrated by the SATAN scanning tool. It supports signatures that trigger when sweeps involve both UDP and TCP ports.

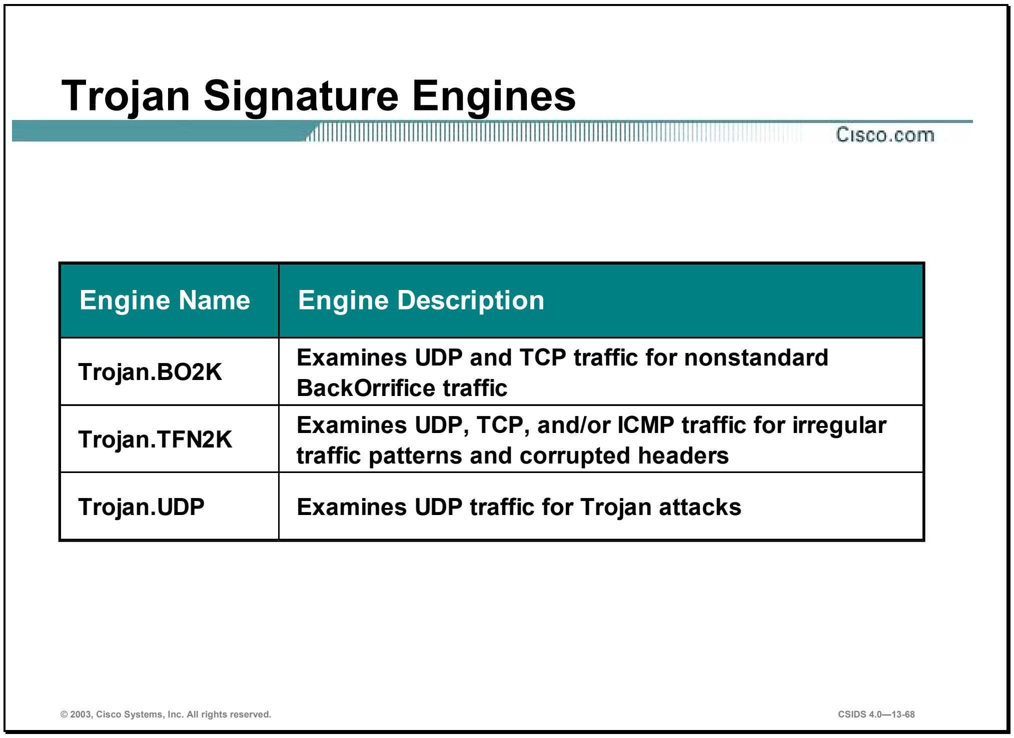
The following table lists the Sweep.Multi parameters:

Parameter	Value	Attribute	Description
TcpInterest	■ 1-SATAN Normal ■ 2-SATAN Heavy	■ Not protected ■ Not required	Defines predefined TCP ports of interest
UdpInterest	■ 1-SATAN Normal ■ 2-SATAN Heavy	■ Not protected ■ Not required	Defines predefined UDP ports of interest
UniqueTcpPorts	2–40	■ Not protected ■ Not required	Defines the number of unique TCP connections allowed
UniqueUdpPorts	2–40	■ Not protected ■ Not required	Defines the number of unique UDP connections allowed

The TcpInterest and UdpInterest parameters enable a signature to trigger when the signature detects traffic that matches the ports used by the SATAN scanning tool. The UniqueTcpPorts and UniqueUdpPorts parameters support signatures that trigger based on a mixture of TCP and UDP connections.

Miscellaneous Signature Engines

This section describes Miscellaneous signature engines that handle non-standard protocol signatures and signatures that do not fit into the other engine protocol decodes.



Trojan Signature Engines

Engine Name	Engine Description
Trojan.BO2K	Examines UDP and TCP traffic for nonstandard BackOrrifice traffic
Trojan.TFN2K	Examines UDP, TCP, and/or ICMP traffic for irregular traffic patterns and corrupted headers
Trojan.UDP	Examines UDP traffic for Trojan attacks

CSIDS 4.0—13-68

Attackers can place back door Trojan programs on systems in your network to enable them to operate from systems within your network. For example, when you download files from certain sites on the Internet, you risk downloading files that contain Trojan programs. The Trojan program can perform a variety of malicious acts such as erasing your disk or enabling the attacker to use your computer to commit DDoS attacks. The Trojan engines detect Trojan programs on your network.

The following are Trojan signature engines:

- Trojan.BO2K—Examines UDP and TCP traffic for nonstandard Back Orifice traffic
- Trojan.TFN2K—Examines UDP, TCP, and/or ICMP traffic for irregular traffic patterns, and corrupted headers
- Trojan.UDP—Examines UDP traffic for Trojan attacks

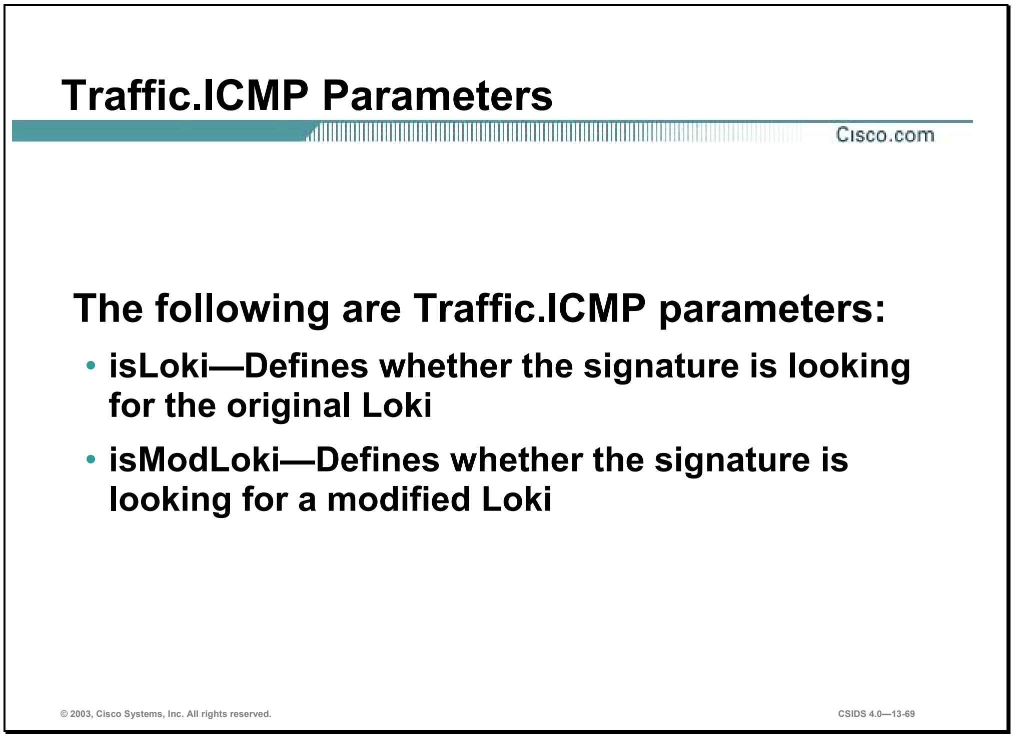
Back Orifice (BO) is the original Windows back door Trojan that runs over UDP. Back Orifice 2000 (BO2K) soon superseded it. BO2K supports UDP and TCP with basic (exclusive-OR (XOR) encryption. The Trojan.UDP signature engine handles the UDP modes of BO and BO2K. The Trojan.BO2K signature engine handles the TCP modes.

TFN2K is the newer version of the Tribal Flood Network (TFN). It is a DDoS agent that is used to control coordinated attacks by infected machines, zombies, to target a single machine or domain with fake traffic floods from hundreds or thousands of unknown attacking hosts. TFN2K also randomizes the packet header information it sends, but it has discriminators that can be used to define the signature. The following discriminators can be used to define the signature:

- The L3 checksum is incorrect.
- There are remnants of the base64 encoding at the end of each packet.

TFN2K can run on any port and can use ICMP, TCP, UDP, or a combination of these protocols for its communications.

There are no specific parameters for the Trojan engines. You can tune the engines by using the master parameters. You cannot create custom signatures with the Trojan engines. If you attempt to do so, you receive the following error message: Error: Array contains max entries, could not add new entry.



Traffic.ICMP Parameters

Cisco.com

The following are Traffic.ICMP parameters:

- **isLoki—Defines whether the signature is looking for the original Loki**
- **isModLoki—Defines whether the signature is looking for a modified Loki**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-69

There is only one Traffic signature engine, Traffic.ICMP. The Traffic.ICMP signature engine supports signatures that are triggered by non-standard usage of the ICMP protocol. Tools that exploit ICMP traffic include TFN, TFN2K, Stacheldraht, and Loki.

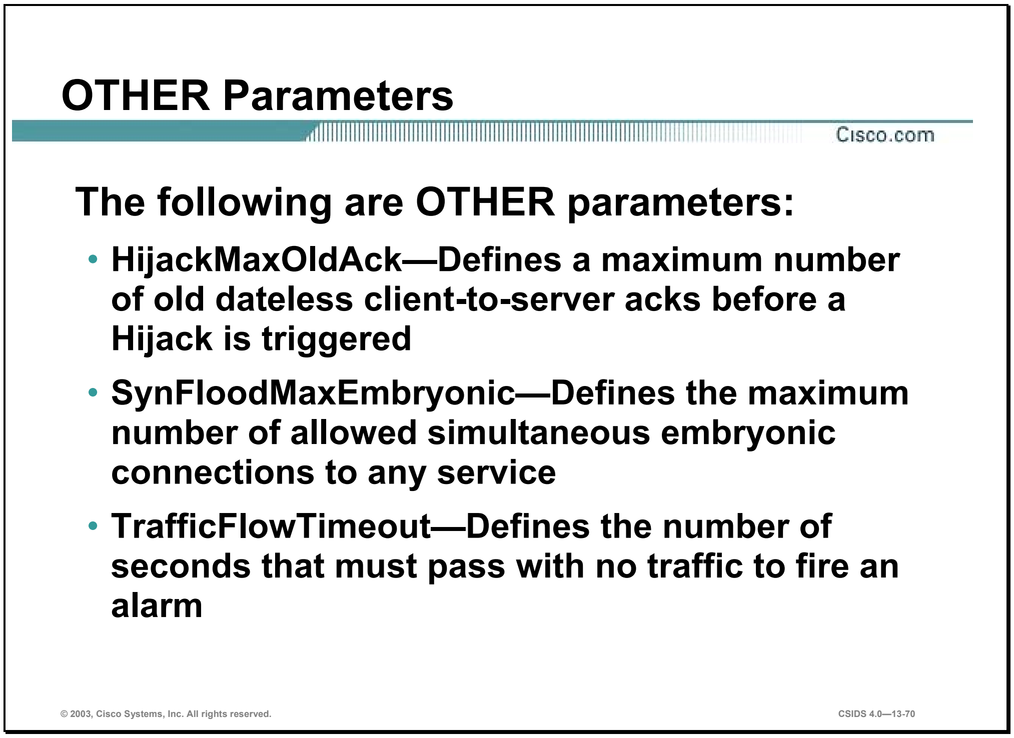
Loki is another type of back door Trojan. Once the machine is infected, the malicious code creates an ICMP tunnel that can be used to send a small payload of ICMP replies, which can travel through a firewall if the firewall is not configured to block ICMP traffic. The signature looks for an imbalance of ICMP echo requests to replies and simple IcmpCode and payload discriminators.

Most DDoS attacks, excluding TFN2K, target ICMP-based DDoS agents. The main tools are TFN and Stacheldraht. They are similar to TFN2K, but rely on ICMP only and have fixed commands, integers and strings.

The following table shows examples of the Traffic.ICMP parameters:

Parameter	Value	Attribute	Description
isLOKI	■ True ■ False	■ Not protected ■ Not required	Defines whether the signature is looking for the original Loki attack
isModLOKI	■ True ■ False	■ Not protected ■ Not required	Defines whether the signature is looking for a modified Loki attack

You cannot add custom signatures to the Traffic signature engine. If you attempt to do so, you receive the following error message: Error: Array contains max entries, could not add new entry.



OTHER Parameters

The following are OTHER parameters:

- HijackMaxOldAck—Defines a maximum number of old dateless client-to-server acks before a Hijack is triggered
- SynFloodMaxEmbryonic—Defines the maximum number of allowed simultaneous embryonic connections to any service
- TrafficFlowTimeout—Defines the number of seconds that must pass with no traffic to fire an alarm

CSIDS 4.0—13-70

The OTHER signature engine handles signatures that do not fit into the other engine protocol decoders. These signatures include Sensor status alarms that indicate changes in the flow of traffic to the Sensor. The OTHER signature engine allows you to configure parameters for built-in signatures using the same engine infrastructure as the other engines. These parameters are used by specialized processors in the system.

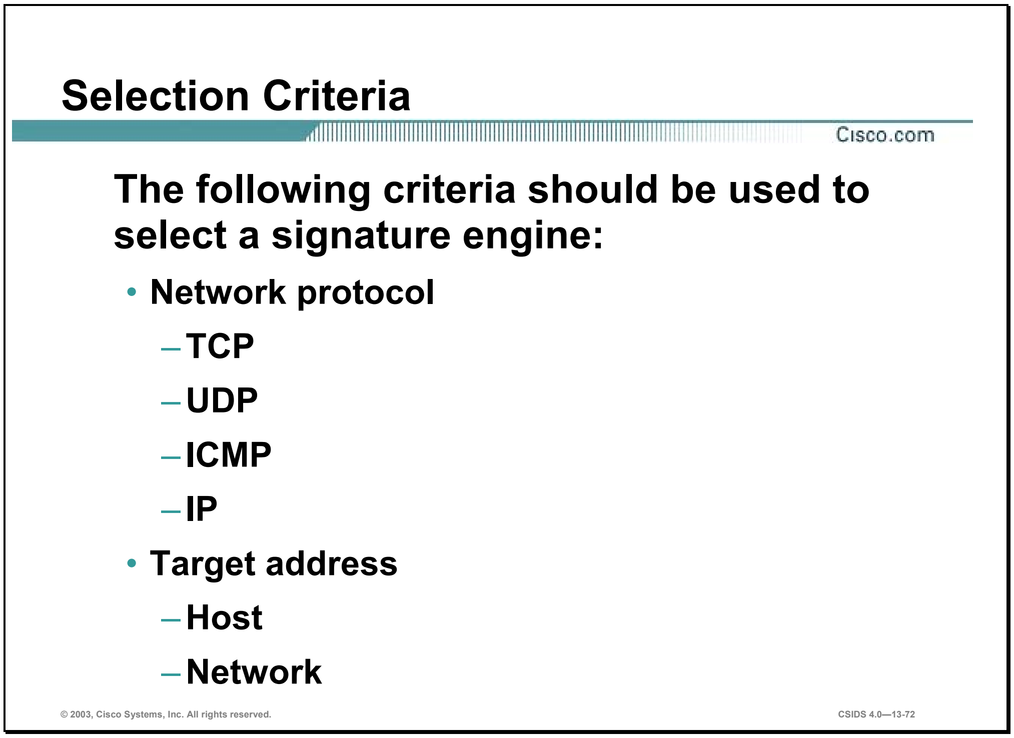
Note You cannot define custom signatures using the OTHER signature engine.

The following table shows examples of the OTHER parameters:

Parameter	Value	Attribute	Description
HijackMaxOldAck	0–2147483647	■ Not protected ■ Not required	Defines a maximum number of old dateless client-to-server acks before a hijack is triggered
SynFloodMaxEmbryonic	0–2147483647	■ Not protected ■ Not required	Defines the maximum number of allowed simultaneous embryonic connections to any service
TrafficFlowTimeout	0–2147483647	■ Not protected ■ Not required	Defines the number of seconds that must pass with no traffic to fire an alarm

Signature Engine Selection

This section provides the criteria to apply when selecting a signature engine that can be used to create custom signatures.



Selection Criteria

The following criteria should be used to select a signature engine:

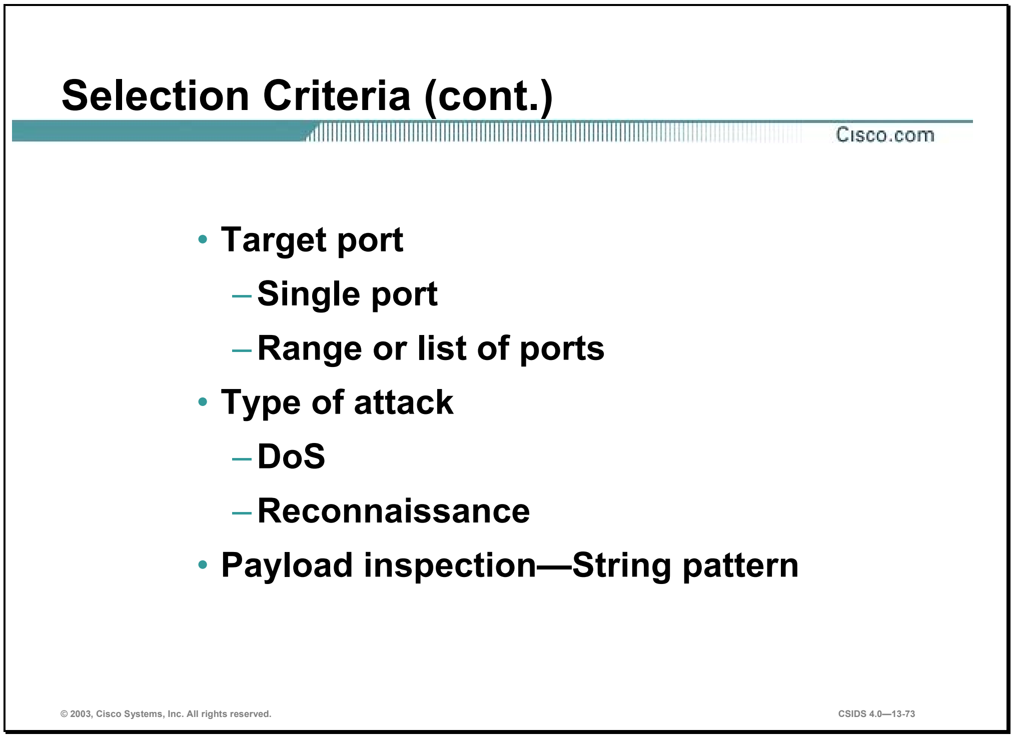
- **Network protocol**
  - **TCP**
  - **UDP**
  - **ICMP**
  - **IP**
- **Target address**
  - **Host**
  - **Network**

CSIDS 4.0—13-72

Cisco IDS signature engines enable the creation of a wide range of custom signatures. Selecting the appropriate signature engine is affected by several variables. The following criteria should be used when deciding which signature engine meets your requirements to create a custom signature:

- Network protocol—Determine the network protocol of the traffic to be examined. For example, to create a signature that examines EIGRP packets, the Atomic.L3.IP signature engine is the appropriate engine because you can specify the IP protocol number.

- Target address—Determine the anticipated target of the attack. For example, the Flood.Net signature engine is designed to detect an excessive amount of packets sent to a network.



Selection Criteria (cont.)

Cisco.com

- Target port
  - Single port
  - Range or list of ports
- Type of attack
  - DoS
  - Reconnaissance
- Payload inspection—String pattern

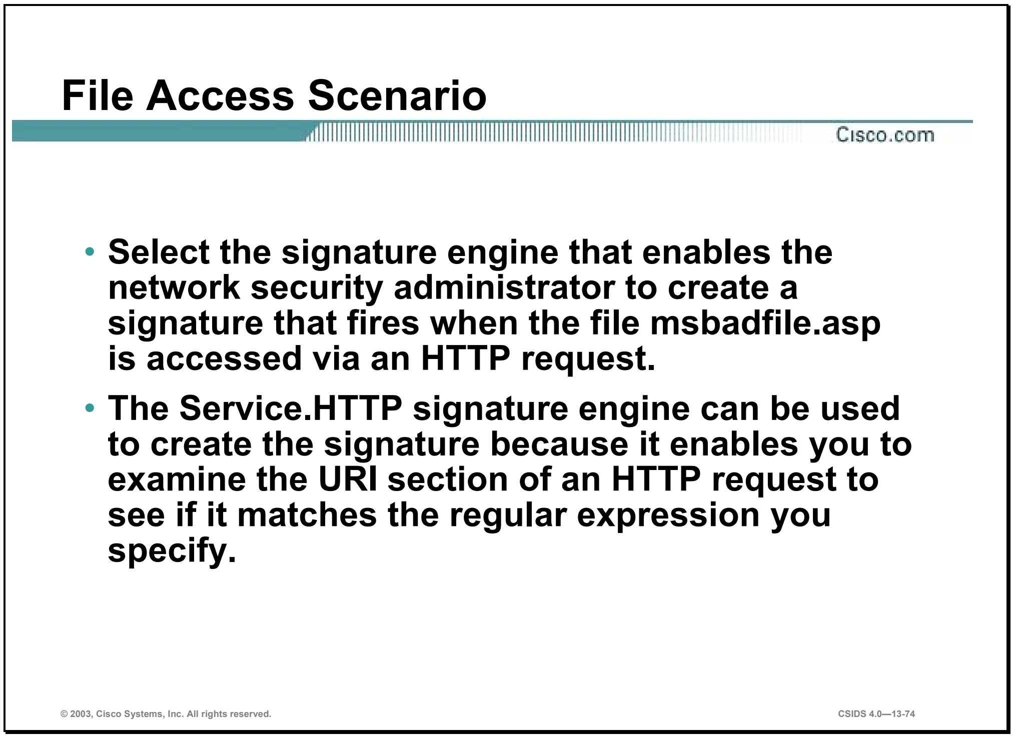
CSIDS 4.0—13-73

- Target port—Determine the anticipated target ports of the attack. For example, the Sweep.Port.UDP signature engine is designed to detect connections to either a specific UDP port or a range of UDP ports.

- Type of attack—Determine the anticipated type of attack: DoS or reconnaissance. For example, the Flood signature engines are commonly used to detect DoS attacks and the Sweep signature engines are commonly used to detect network reconnaissance attacks.

Note	Although an engine was designed to detect a certain attack, it is not limited to detecting those specific types of attacks. For example, the Sweep.Host.TCP or Atomic.TCP signature engines can also be used to detect a possible DoS attack.

- Payload inspection—Determine the need to inspect the payload of a packet for a string pattern. For example, the String.TCP signature engine is designed to detect a string pattern in a TCP packet.



File Access Scenario

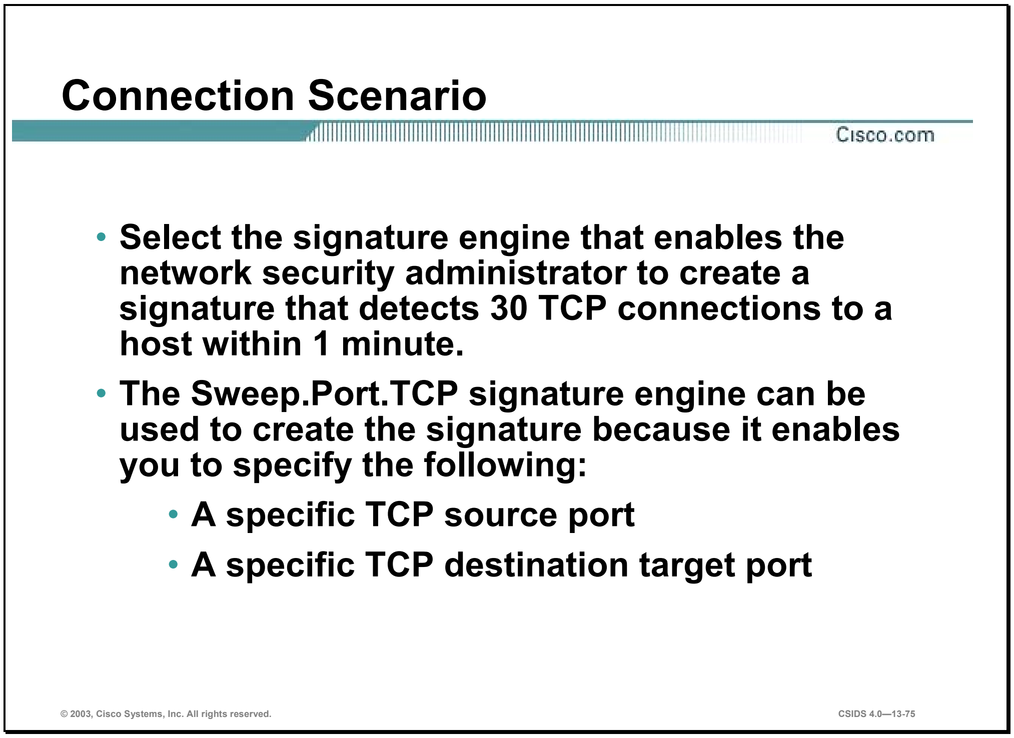
Cisco.com

- Select the signature engine that enables the network security administrator to create a signature that fires when the file msbadfile.asp is accessed via an HTTP request.
- The Service.HTTP signature engine can be used to create the signature because it enables you to examine the URI section of an HTTP request to see if it matches the regular expression you specify.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—13-74

Select the signature engine that enables the network security administrator to create a signature that detects when the file msbadfile.asp is accessed via an HTTP request.

The Service.HTTP engine can be used to create the signature. Service.HTTP's UriRegex parameter can be used to examine the URI section of the HTTP request to match the regular expression you specify.



Connection Scenario

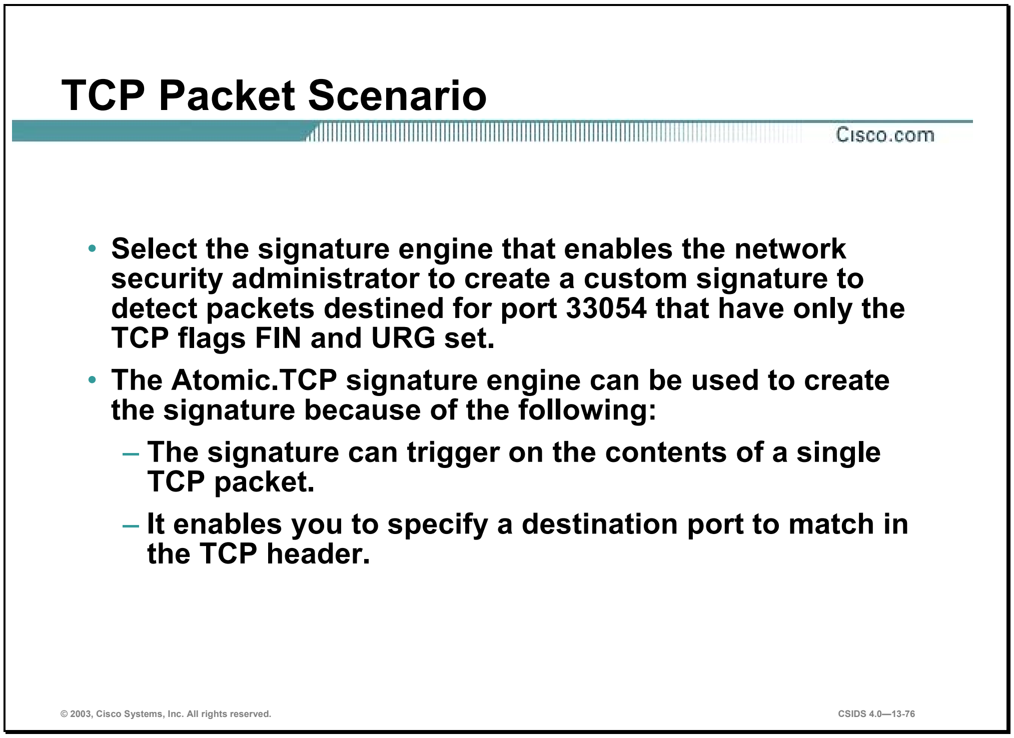
Cisco.com

- Select the signature engine that enables the network security administrator to create a signature that detects 30 TCP connections to a host within 1 minute.
- The Sweep.Port.TCP signature engine can be used to create the signature because it enables you to specify the following:
  - A specific TCP source port
  - A specific TCP destination target port

CSIDS 4.0—13-75

Select the signature engine that enables the network security administrator to create a signature that detects 30 TCP connections to a host within 1 minute.

The Sweep.Port.TCP signature engine can be used to create the signature. This engine can detect an attacker scanning from a specific source port or to a specific destination port.



TCP Packet Scenario

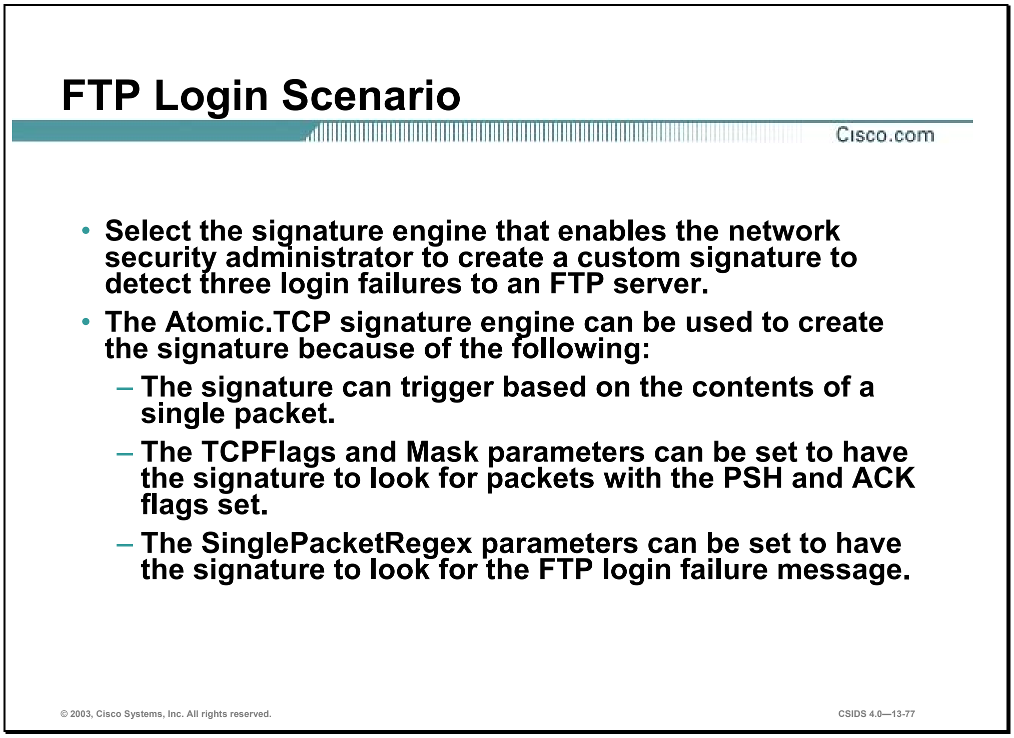
- Select the signature engine that enables the network security administrator to create a custom signature to detect packets destined for port 33054 that have only the TCP flags FIN and URG set.
- The Atomic.TCP signature engine can be used to create the signature because of the following:
  - The signature can trigger on the contents of a single TCP packet.
  - It enables you to specify a destination port to match in the TCP header.

CSIDS 4.0—13-76

Select the signature engine that enables the network security administrator to create a signature to detect packets destined for port 33054 that have only the TCP Flags FIN and URG set.

The Atomic.TCP signature engine could be used to create the signature. The signature could be created by configuring the following parameters and parameter values:

- SIGID—30001
- SubSig—0
- SigName—FIN / URG Packet
- DstPort—33054
- Mask—FIN SYN RST PSH ACK URG
- TcpFlags—FIN URG
- SigStringInfo—FIN / URG



FTP Login Scenario

- Select the signature engine that enables the network security administrator to create a custom signature to detect three login failures to an FTP server.
- The Atomic.TCP signature engine can be used to create the signature because of the following:
  - The signature can trigger based on the contents of a single packet.
  - The TCPFlags and Mask parameters can be set to have the signature to look for packets with the PSH and ACK flags set.
  - The SinglePacketRegex parameters can be set to have the signature to look for the FTP login failure message.

CSIDS 4.0—13-77

Another example of using the Atomic.TCP signature engine is for creating a custom signature to detect three login failures to an FTP server. You could configure the following parameters to create this signature:

- SIGID—30003
- SubSig—0
- Mask—FIN SYN RST PSH ACK URG
- MinHits—3
- SigName—FTP Auth Failure
- SigStringInfo—FTP Auth Failure
- SinglePacketRegex—[5][3][0]
- SrcPort—21
- TcpFlags—PSH ACK

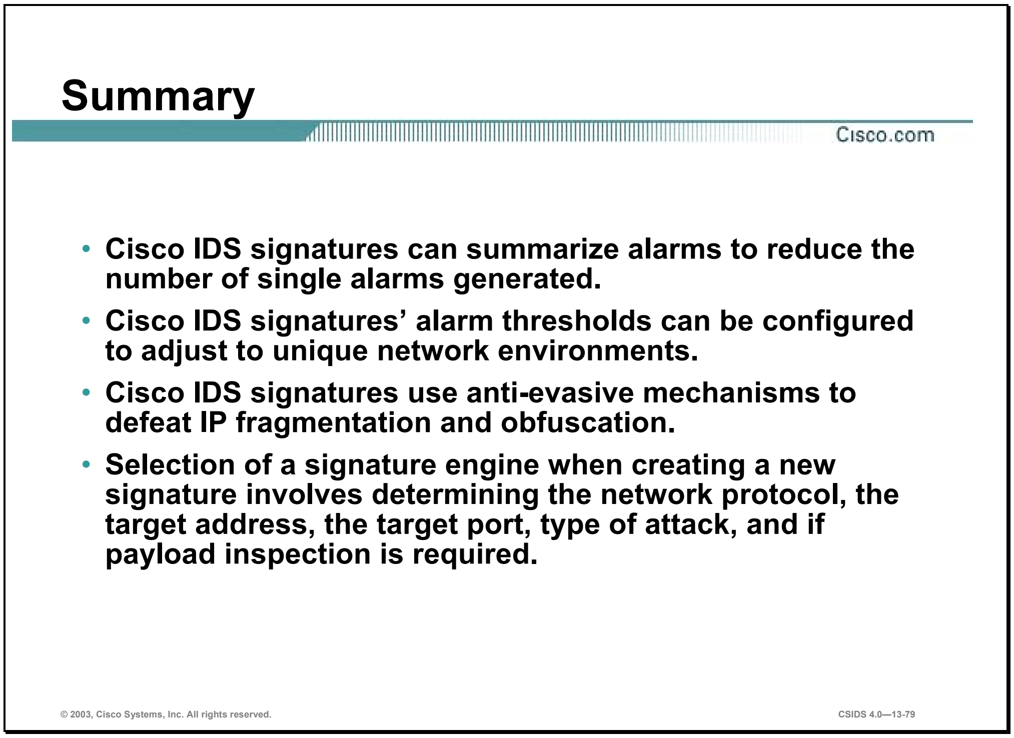
The SinglePacketRegex parameter would configure the signature to look for the FTP 530 error message, which indicates a login failure occurred. The TcpFlags and Mask parameters would configure the signature to look for the following flags in the packet:

- PSH—Indicates that the data in the packet is complete rather than segmented and should be passed immediately to the application

- ACK—Indicates that this is an acknowledgement of a previous packet

Summary

This section summarizes what you have learned in this chapter.



Summary

- Cisco IDS signatures can summarize alarms to reduce the number of single alarms generated.
- Cisco IDS signatures' alarm thresholds can be configured to adjust to unique network environments.
- Cisco IDS signatures use anti-evasive mechanisms to defeat IP fragmentation and obfuscation.
- Selection of a signature engine when creating a new signature involves determining the network protocol, the target address, the target port, type of attack, and if payload inspection is required.

CSIDS 4.0—13-79

14

Sensing Configuration

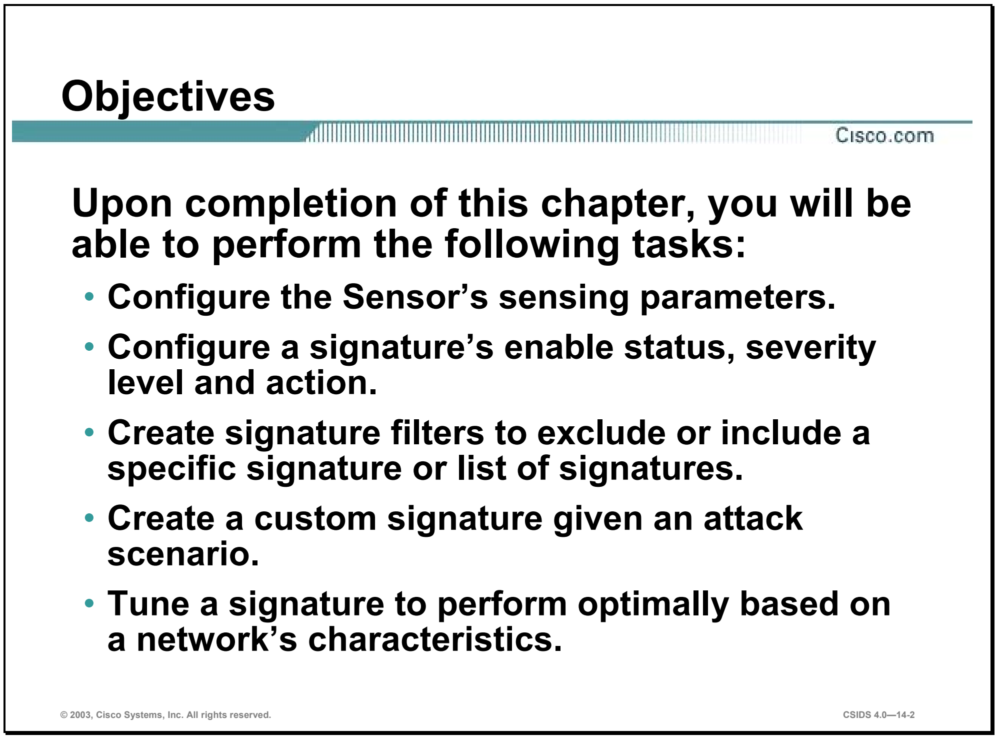
Overview

This chapter explains the Cisco Sensor's sensing configuration including custom signature creation and signature tuning. This chapter includes the following topics:

- Objectives
- Global sensing configuration
- Signature configuration
- Signature filtering
- Signature tuning
- Custom signatures
- Summary
- Lab exercise

Objectives

This section lists the chapter’s objectives.



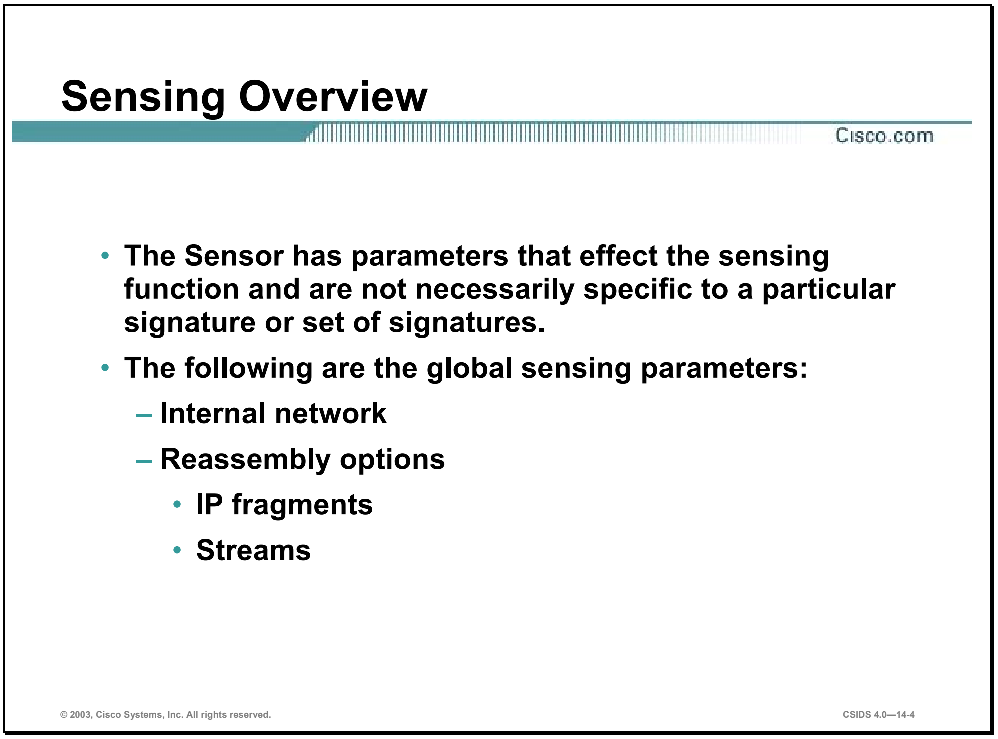
Objectives

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

- Configure the Sensor’s sensing parameters.
- Configure a signature’s enable status, severity level and action.
- Create signature filters to exclude or include a specific signature or list of signatures.
- Create a custom signature given an attack scenario.
- Tune a signature to perform optimally based on a network’s characteristics.

Global Sensing Configuration

This section discusses the configuration parameters that effect the Sensor's sensing capabilities.



Sensing Overview

Cisco.com

- The Sensor has parameters that effect the sensing function and are not necessarily specific to a particular signature or set of signatures.
- The following are the global sensing parameters:
  - Internal network
  - Reassembly options
    - IP fragments
    - Streams

CSIDS 4.0—14-4

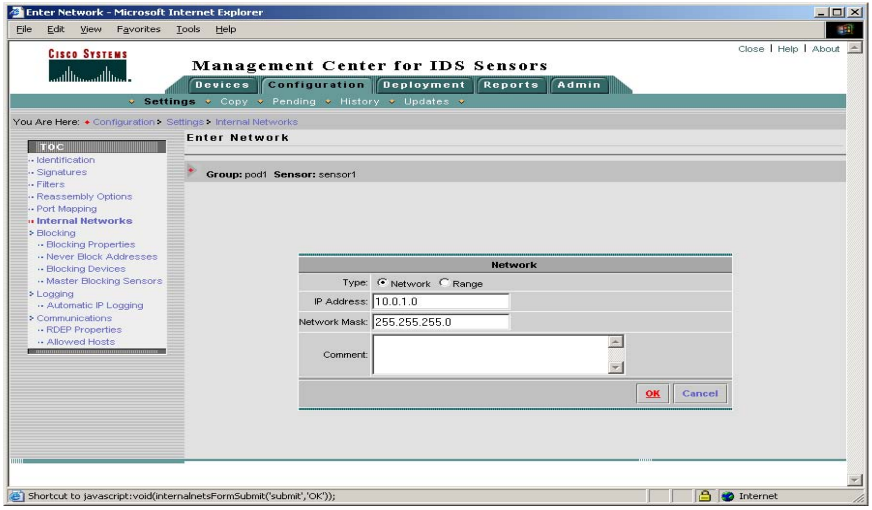
The Sensor has configuration parameters that affect the sensing function. These parameters are not necessarily specific to a particular signature or set of signatures. The following are the global sensing parameters:

- Internal network
- Reassembly options
  - IP fragments
  - Streams

Internal Networks

Cisco.com

Choose Configuration>Settings>Internal Networks>Add**.**



Enter Network

Group: pod1 **Sensor:** sensor1

Network

Type: ● Network ○ Range

IP Address: 10.0.1.0

Network Mask: 255.255.255.0

Comment:

Shortcut to javascript:void(internalnetsFormSubmit('submit','OK'));

CSIDS 4.0—14-5

The Management Center for Intrusion Detection System Sensors (IDS MC) enables an administrator to add networks that are either internal to the Sensor or are deemed trusted. Complete the following steps to add an Internal Network to the Sensor:

Step 1 Choose **Configuration>Settings>Internal Networks>Add**. The Enter network page appears.

Step 2 Enter values for settings listed in the following table:

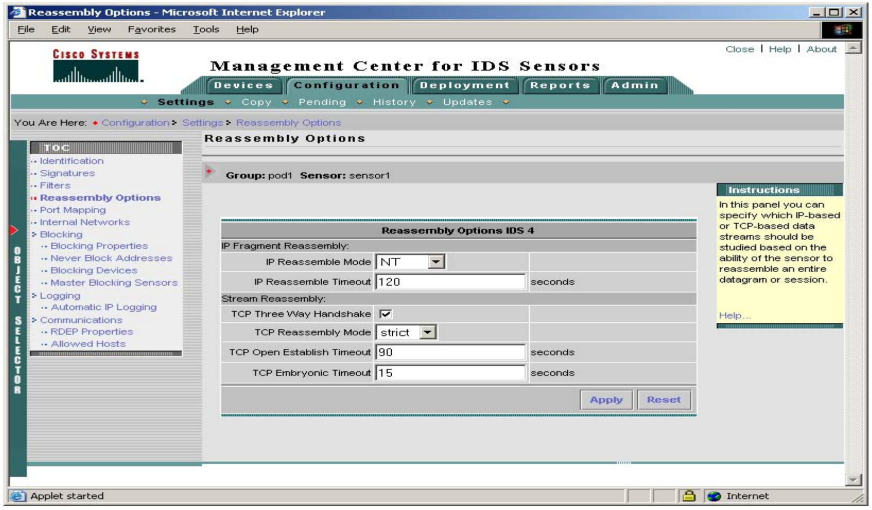
IDS MC Internal Networks Settings	Description
IP Address	The IP address of the internal network
Network Mask	The network mask of the internal network
Comments	Optional

Step 3 Click **OK**. The Internal Networks page appears.

Reassembly Options

Cisco.com

Choose Configuration>Settings>Reassembly Options**.**



You Are Here: Configuration > Settings > Reassembly Options

Reassembly Options

Group: pod1 **Sensor:** sensor1

Reassembly Options IDS 4

IP Fragment Reassembly:

IP Reassemble Mode	NT	
IP Reassemble Timeout	120	seconds

Stream Reassembly:

TCP Three Way Handshake	☑	
TCP Reassembly Mode	strict	
TCP Open Establish Timeout	90	seconds
TCP Embryonic Timeout	15	seconds

Instructions

In this panel you can specify which IP-based or TCP-based data streams should be studied based on the ability of the sensor to reassemble an entire datagram or session.

Help...

CSIDS 4.0—14-6

The IDS MC enables you to edit the IP Fragment Reassembly and TCP Session Reassembly Options for a Sensor. Complete the following steps to edit the IP Fragment or TCP Session Reassembly Options for a Sensor:

Step 1 Choose **Configuration>Settings>Reassembly Options**. The Reassembly Options page appears.

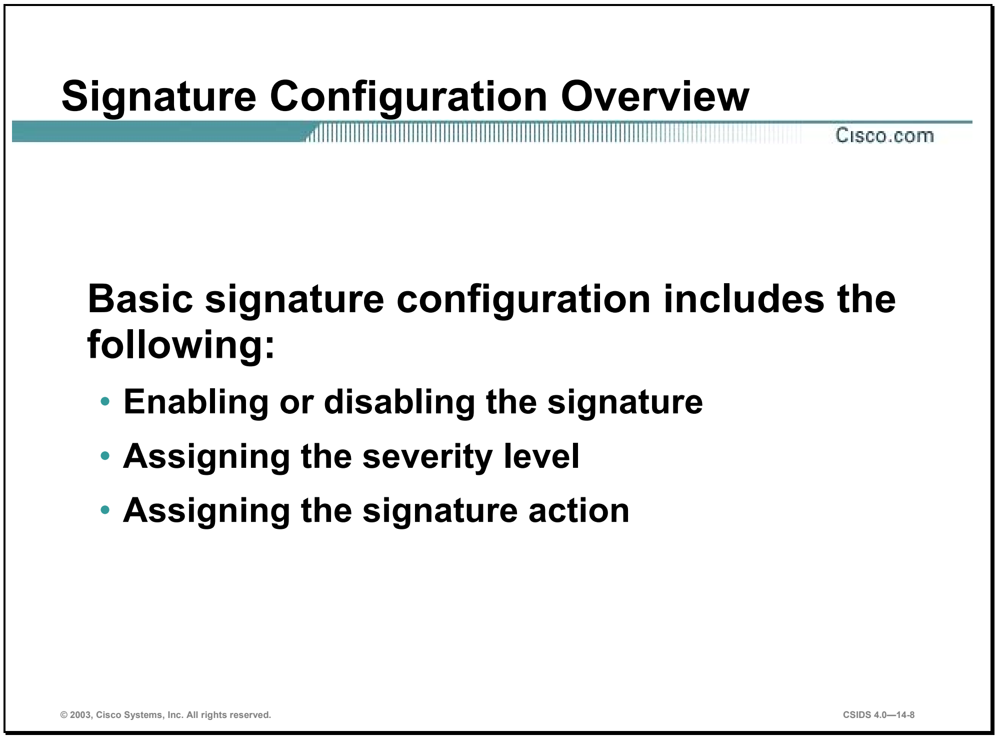
Step 2 Enter Reassembly values for settings listed in the following table:

IDS MC Reassembly Settings	Description
IP Reassemble Mode	Allows you to alter how the Sensor reassembles IP fragments. The default is NT. The following options are available: NT, Solaris, LINUX, and BSD.
IP Reassemble Timeout	Number of seconds the Sensor will wait for IP fragment to reassemble before it discards the original IP fragment. The default is 120 seconds.
TCP Three Way Handshake	Check box that if selected enables the Sensor to reassemble a TCP session that has completed the three-way handshake.
TCP Reassemble Mode	Mode by which the Sensor will reassemble TCP streams. The default is strict. The following options are available: strict or loose.
TCP Open Establish Timeout	The number of seconds a Sensor will allow an open established connection to exist without timing out. The default is 120 seconds.
TCP Embryonic Timeout	The number of seconds a Sensor will allow a partial connection to stay open before closing it. The default is 15 seconds.

Step 3 Click **Apply** to complete editing the IP Fragment and TCP Session reassembly options. The Reassembly Options will refresh to indicate that the IDS MC received the changes.

Signature Configuration

This section discusses signature categorization and explains basic signature configuration.



Signature Configuration Overview

Basic signature configuration includes the following:

- **Enabling or disabling the signature**
- **Assigning the severity level**
- **Assigning the signature action**

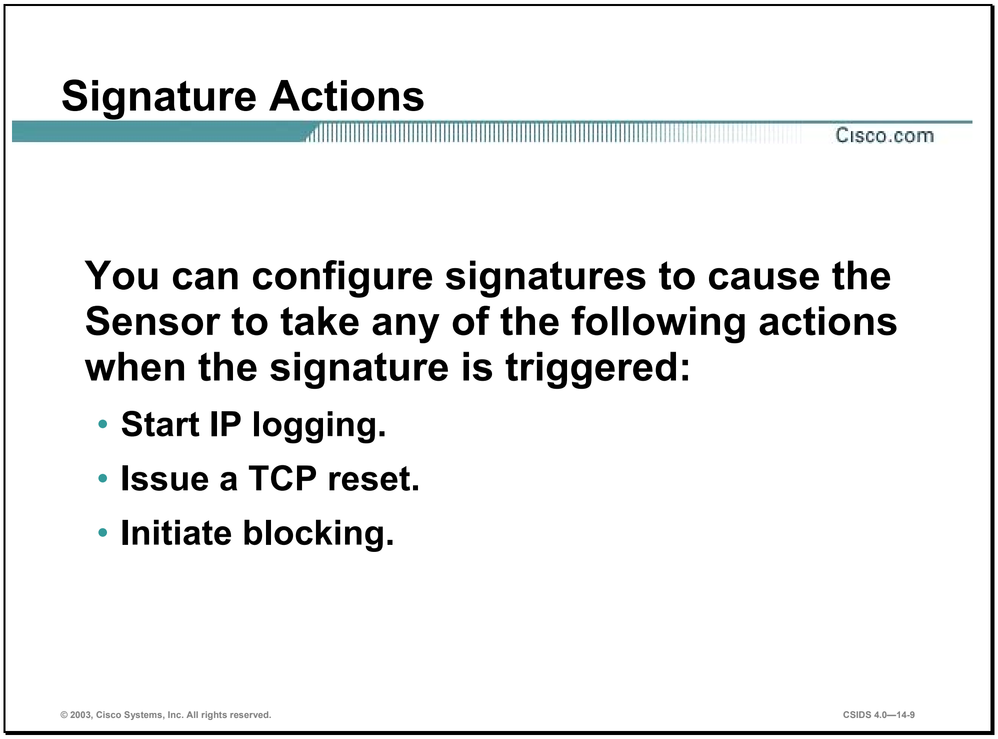
CSIDS 4.0—14-8

Known attack signatures are included in the Sensor software and are enabled by default. These are called built-in signatures. You cannot add to or delete from the list of built-in attack signatures, nor can you re-name them. However, you can tune them by adjusting their parameters. Built-in signatures that have been modified are called tuned signatures.

You can also create new signatures, which are called custom signatures. Custom signature identification numbers begin at 20000. You can configure custom signatures for many purposes such as matching strings on UDP connections, tracking network floods. Custom signatures are created using a signature engine specifically designed for the type of traffic being monitored.

Every signature belongs to a signature engine. Therefore, all signatures can be tuned. All signatures have the following basic configurable parameters:

- Enable status—Enables or disables the signature
- Severity level—Assigns the severity level (information, low, medium, or high)
- Signature action—Assigns the action to take if the signature is triggered (log, reset, block host, or block connection)



Signature Actions

You can configure signatures to cause the Sensor to take any of the following actions when the signature is triggered:

- **Start IP logging.**
- **Issue a TCP reset.**
- **Initiate blocking.**

CSIDS 4.0—14-9

You can configure signatures to cause the Sensor to take an action when the signature is triggered by selecting on of the following options:

- IP Log—Writes the IP session data to an IP log file. The IP logging feature provides the ability to capture raw, unaltered packets related to the participants of an event. Information from the logs can be used for confirmation, damage assessment, and forensic evidence.

- TCP Reset—Sends a TCP reset command to the session in which the attack signature was detected. The reset action is available only for TCP-based attack signatures.

- Block—Modifies ACLs on routers and other devices to dynamically change the access policy in response to an event. You can configure a signature for either of the following types of blocking:

  - Block host—Denies the source IP address. This denies all IP packets from the blocked address. The following is an example of the deny ACE created on the blocking device:

    ```
    deny ip host 10.1.1.1 any
    ```

  - Block connection—Denies only the IP packets from the source IP address to a specific destination IP address, destination port, and service. Block connection denies all connections of the same type to the same destination address. The following is an example of the deny ACE created on the blocking device:

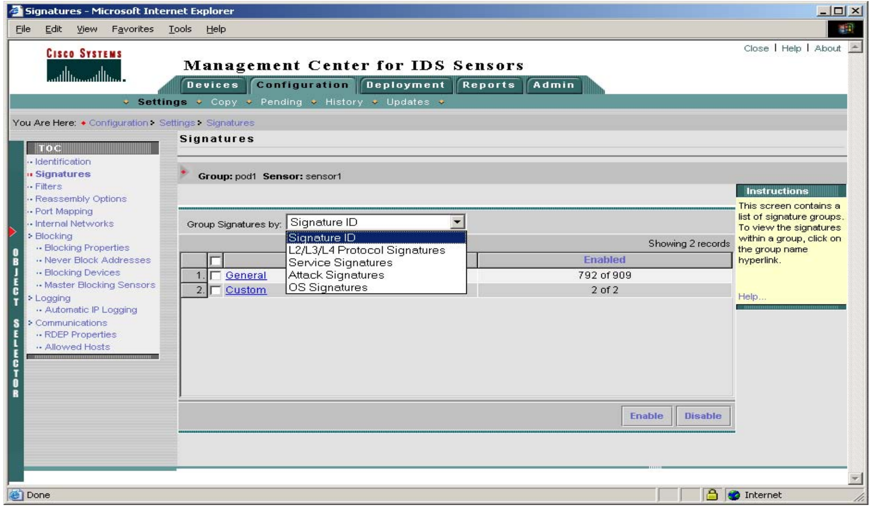
    ```
    deny tcp host 10.1.1.1 host 172.21.1.1 eq telnet
    ```

In addition to denying the connection in which the attack was executed, Block Connection denies all connections of that type to that destination address. All connections for that service from the source to the destination IP address will be denied. If an attacker executes a web attack against a web server, all web connections from the attacker's IP address to that specific web server IP address will be blocked. However, the attacker can still Telnet or FTP to that web server, and can continue to make web connections to other IP addresses.

Signature Groups

Cisco.com

Choose Configuration>Settings>Signatures.



Signatures

Group: pod1 **Sensor:** sensor1

Group Signatures by: Signature ID

Showing 2 records

	□		Enabled
1.	□	General	792 of 909
2.	□	Custom	2 of 2

Instructions

This screen contains a list of signature groups. To view the signatures within a group, click on the group name hyperlink.

Help...

Choose **Configuration>Settings>Signatures** to access the main Signatures page. From the Signatures page, you can use the Group Signatures by drop-down menu to display signatures grouped in any of the following ways:

- Signature ID
- L2/L3/L4 protocol
- Service
- Attack
- OS

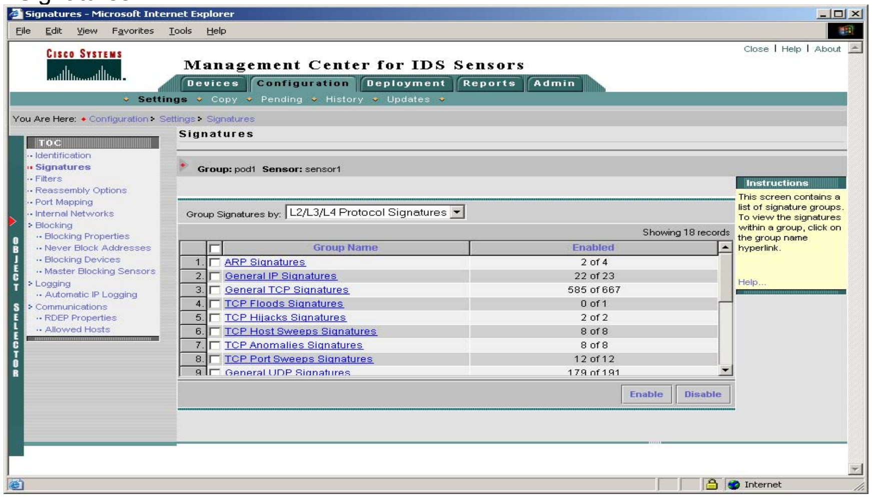
If you select Signature ID from the drop-down menu, you can then select one of the following:

- General—Enables you to access all pre-loaded signatures on the Sensor or IDSM
- Custom—Enables you to access all custom signatures that have been defined on the Sensor or IDSM

L2/L3/L4 Protocol Signatures

Cisco.com

Choose Configuration>Settings>Signatures and **select** L2/L3/L4 Protocol Signatures.



Signatures

Group: pod1 **Sensor:** sensor1

Group Signatures by: L2/L3/L4 Protocol Signatures

Showing 18 records

	☐	Group Name	Enabled
1.	☐	ARP Signatures	2 of 4
2.	☐	General IP Signatures	22 of 23
3.	☐	General TCP Signatures	585 of 667
4.	☐	TCP Floods Signatures	0 of 1
5.	☐	TCP Hijacks Signatures	2 of 2
6.	☐	TCP Host Sweeps Signatures	8 of 8
7.	☐	TCP Anomalies Signatures	8 of 8
8.	☐	TCP Port Sweeps Signatures	12 of 12
9	☐	General UDP Signatures	179 of 191

Instructions

This screen contains a list of signature groups. To view the signatures within a group, click on the group name hyperlink.

Help...

CSIDS 4.0—14-11

The figure shows signature groups as displayed if you select L2/L3/L4 Protocol Signatures from the drop-down menu on the Signatures page. Layer 2/Layer 3/Layer 4 protocol signatures are based on layers of the networking framework from the International Organization for Standardization's (IOS) Open System Interconnect (OSI).

The following table lists L2/L3/L4 Protocol Signature groups and the number of signatures that are enabled within the group:

L2/L3/L4 Signatures Group Name	Enabled
ARP Signatures	2 of 4
General IP Signatures	22 of 23
General TCP Signatures	585 of 667
TCP Floods Signatures	0 of 1
TCP Hijacks Signatures	2 of 2
TCP Host Sweeps Signatures	8 of 8
TCP Anomalies Signatures	8 of 8
TCP Port Sweeps Signatures	12 of 12
General UDP Signatures	180 of 191
UDP Floods Signatures	1 of 2
UDP Protocol Anomalies Signatures	1 of 1
UDP Port Sweeps Signatures	2 of 2
General ICMP Signatures	8 of 22
ICMP Floods Signatures	1 of 4

L2/L3/L4 Signatures Group Name	Enabled
ICMP Host Sweeps Signatures	3 of 3
ICMP Protocol Anomalies Signatures	1 of 2
Miscellaneous Protocol Signatures	5 of 5
TCP/UDP Combo Sweeps Signatures	2 of 2

Note Enabling and editing a Service Signature with the IDS MC is similar to enabling or editing other signatures on the Sensor or IDSM2.

Complete the following steps to enable and edit a General UDP signature:

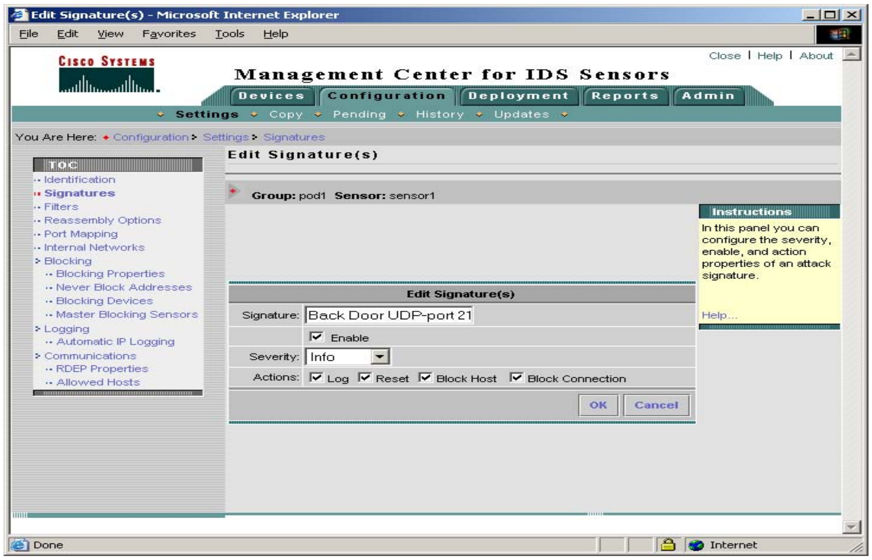
Step 1 Choose **Configuration>Settings>Signatures**. The Signatures page is displayed.

Step 2 Select **L2/L3/L4 Protocol Signatures** from the Group Signatures by drop-down menu. The Signatures page refreshes to display the L2/L3/L4 protocol signatures.

Step 3 Click the **General UDP Signatures** group name. The Signatures in Group page is displayed.

L2/L3/L4 Protocol Signatures (cont.)

Cisco.com



Edit Signature(s)

Group: pod1 **Sensor:** sensor1

Instructions

In this panel you can configure the severity, enable, and action properties of an attack signature.

Help...

Edit Signature(s)

Signature: Back Door UDP-port 21

☑ Enable

Severity: Info

Actions: ☑ Log ☑ Reset ☑ Block Host ☑ Block Connection

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—14-12

Step 4 Click the Signature's Name of the signature that you wish to edit. The Edit Signatures page is displayed.

Step 5 Enter values listed in the following table in the Edit Signatures page:

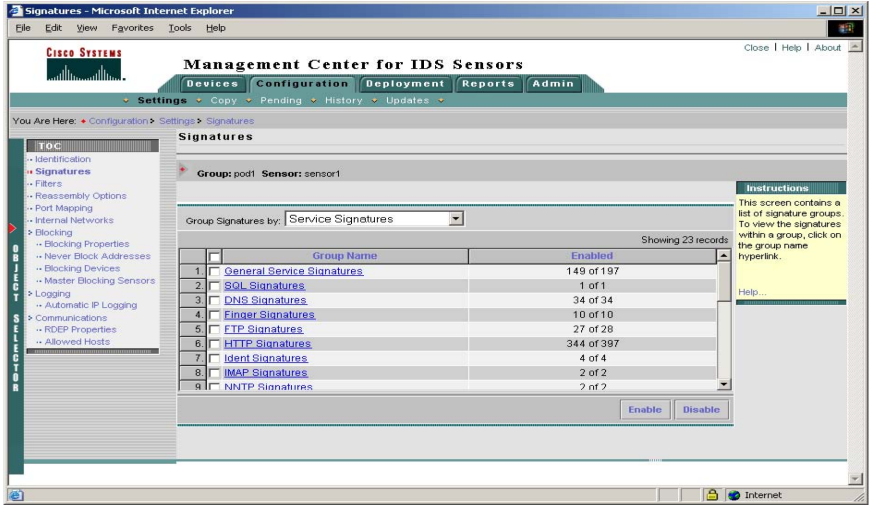
IDS MC Edit Signature Settings	Description
Enable check box	Allows you to enable or disable the signature.
Severity drop-down menu	Allows you to select a severity for the signature. The following options are available: info, low, medium, and high.
Actions check boxes	Allows you to perform an action when the signature is triggered. The following options are available: log, reset, block host, and block connection.

Step 6 Click **OK**. The Signatures in Group page is displayed.

Service Signatures

Cisco.com

Choose Configuration>Settings>Signatures and **select** Service Signatures.



You Are Here: Configuration > Settings > Signatures

Signatures

Group: pod1 **Sensor:** sensor1

Group Signatures by: Service Signatures

Showing 23 records

	□	Group Name	Enabled
1.	□	General Service Signatures	149 of 197
2.	□	SQL Signatures	1 of 1
3.	□	DNS Signatures	34 of 34
4.	□	Finger Signatures	10 of 10
5.	□	FTP Signatures	27 of 28
6.	□	HTTP Signatures	344 of 397
7.	□	Ident Signatures	4 of 4
8.	□	IMAP Signatures	2 of 2
9	□	NNTP Signatures	2 of 2

Instructions

This screen contains a list of signature groups. To view the signatures within a group, click on the group name hyperlink.

Help...

Service signatures are based on services provided on the network that are operating system independent. The following table lists service signature groups and the number of signatures that are enabled within the group:

Service Signatures Group Name	Enabled
General Service Signatures	149 of 197
SQL Signatures	1 of 1
DNS Signatures	34 of 34
Finger Signatures	10 of 10
FTP Signatures	27 of 28
HTTP Signatures	344 of 397
Ident Signatures	4 of 4
IMAP Signatures	2 of 2
NNTP Signatures	2 of 2
LPR Signatures	1 of 1
NetBIOS/SMB Signatures	18 of 18
NTP Signatures	1 of 1
POP Signatures	5 of 5
R-Services Signatures	3 of 3
RPC Signatures	66 of 70
SMTP Signatures	22 of 22
SNMP Signatures	51 of 51
SSH Signatures	2 of 2

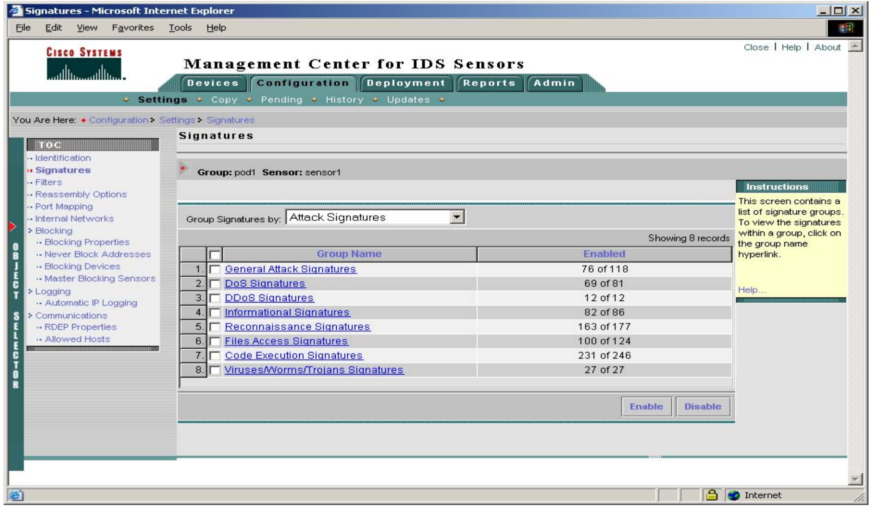
Service Signatures Group Name	Enabled
Telnet Signatures	12 of 13
SOCKS Signatures	0 of 1
TFTP Signatures	3 of 3
HTTPS Signatures	1 of 1
DHCP Signatures	0 of 1

Note Enabling and editing a Service Signature with the IDS MC is similar to enabling and editing other signatures on the Sensor or IDSM2.

Attack Signatures

Cisco.com

Choose Configuration>Settings>Signatures and **select** Attack Signatures.



Signatures

Group: pod1 **Sensor:** sensor1

Group Signatures by: Attack Signatures

Showing 8 records

	□	Group Name	Enabled
1.	□	General Attack Signatures	76 of 118
2.	□	DoS Signatures	69 of 81
3.	□	DDoS Signatures	12 of 12
4.	□	Informational Signatures	82 of 86
5.	□	Reconnaissance Signatures	163 of 177
6.	□	Files Access Signatures	100 of 124
7.	□	Code Execution Signatures	231 of 246
8.	□	Viruses/Worms/Trojans Signatures	27 of 27

Instructions

This screen contains a list of signature groups. To view the signatures within a group, click on the group name hyperlink.

CSIDS 4.0—14-14

Attack signatures are based on attacks that are preformed against networks or hosts. The following table lists attack signature groups along with the number of signatures that are enabled within the group:

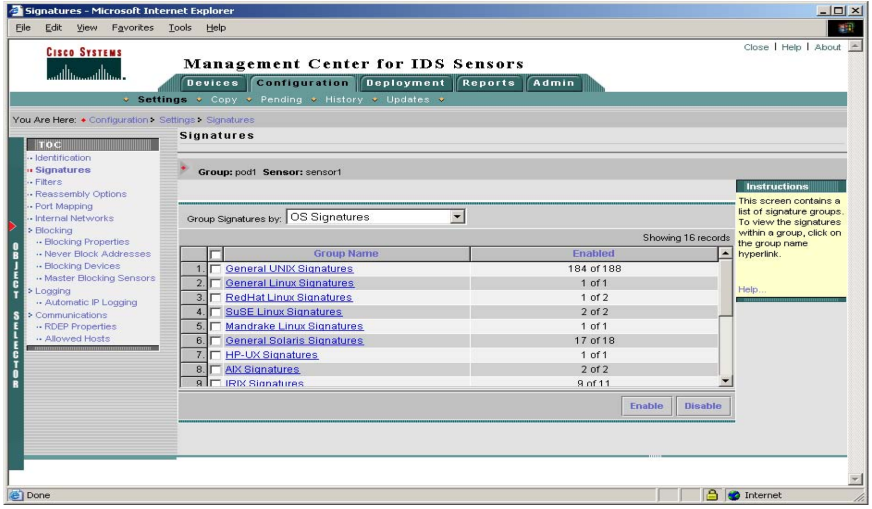
Attack Signatures Group Name	Enabled
General Attack Signatures	76 of 118
DoS Signatures	69 of 81
DDoS Signatures	12 of 12
Information Signatures	82 of 86
Reconnaissance Signatures	163 of 177
File Access Signatures	100 of 124
Code Execution Signatures	231 of 246
Viruses/Worms/Trojans Signatures	27 of 27

Note Enabling and editing an Attack Signature with the IDS MC is similar to enabling and editing other signatures on the Sensor or IDSM2.

OS Signatures

Cisco.com

Choose Configuration>Settings>Signatures and **select** OS Signatures.



You Are Here: Configuration > Settings > Signatures

Signatures

Group: pod1 **Sensor:** sensor1

Group Signatures by: OS Signatures

Showing 16 records

	□	Group Name	Enabled
1.	□	General UNIX Signatures	184 of 188
2.	□	General Linux Signatures	1 of 1
3.	□	RedHat Linux Signatures	1 of 2
4.	□	SuSE Linux Signatures	2 of 2
5.	□	Mandrake Linux Signatures	1 of 1
6.	□	General Solaris Signatures	17 of 18
7.	□	HP-UX Signatures	1 of 1
8.	□	AIX Signatures	2 of 2
9.	□	IRIX Signatures	9 of 11

Instructions

This screen contains a list of signature groups. To view the signatures within a group, click on the group name hyperlink.

Help...

CSIDS 4.0—14-15

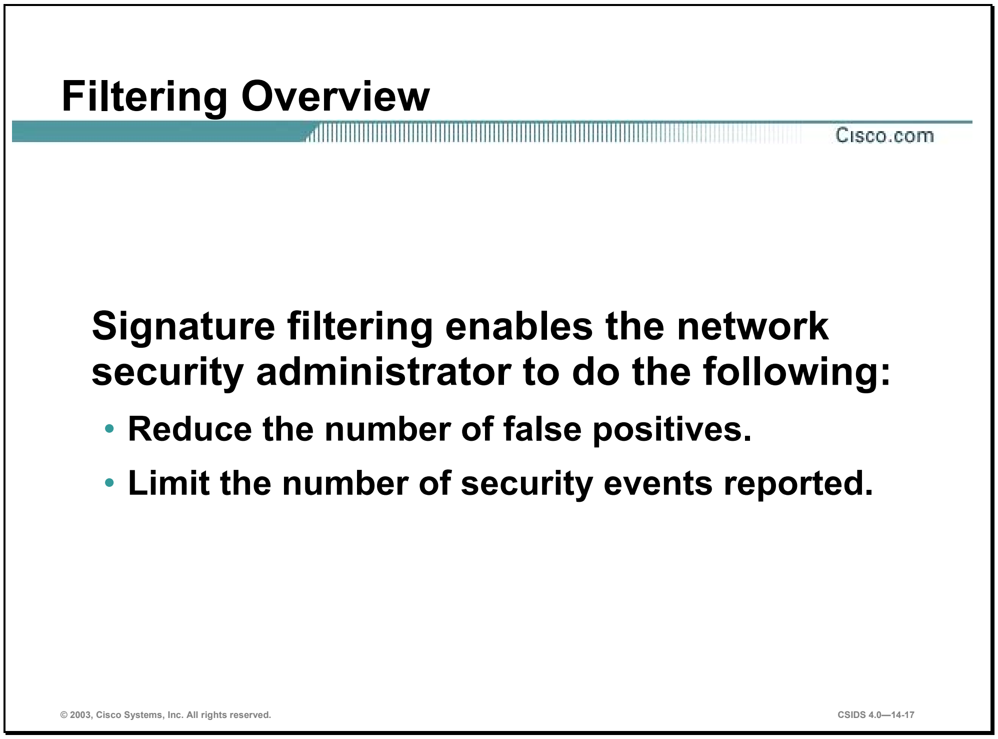
OS Signatures allow the Sensor to check traffic flows for attacks that are launched against specific operating systems. The following table lists OS signature groups and the number of signatures that are enabled within the group:

OS Attack Group Name	Enabled
General UNIX Signatures	182 of 188
General Linux Signatures	1 of 1
RedHat Linux Signatures	1 of 2
SuSE Linux Signatures	2 of 2
Mandrake Linux Signatures	1 of 1
General Solaris Signatures	17 of 18
HP-UX Signatures	1 of 1
AIX Signatures	2 of 2
IRIX Signatures	9 of 11
General Windows Signatures	108 of 124
General Windows NT Signatures	48 of 55
WinNT Signatures	13 of 14
IOS Signatures	11 of 14
General OS Signatures	353 of 431
Netware Signatures	1 of 1
MacOS Signatures	3 of 3

Note Enabling and editing an OS Signature with the IDS MC is similar to enabling and editing any other signatures on the Sensor or IDSM2.

Signature Filtering

This section explains the signature-filtering feature and how to create filters that enhance the Sensor's IDS functionality and performance.



Filtering Overview

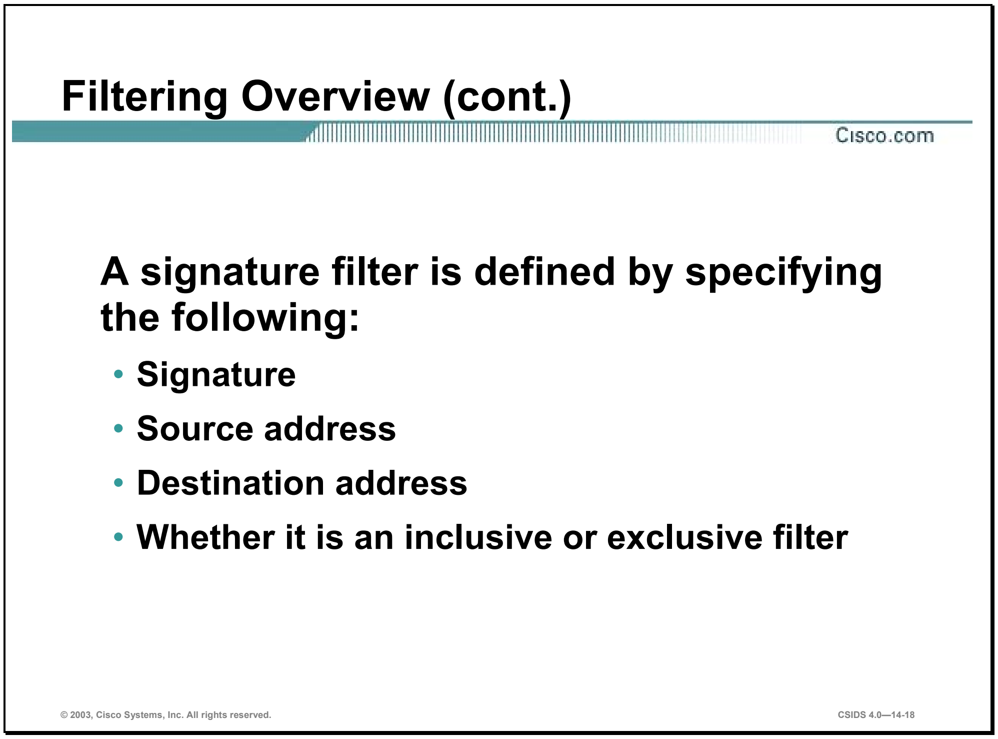
Signature filtering enables the network security administrator to do the following:

- **Reduce the number of false positives.**
- **Limit the number of security events reported.**

CSIDS 4.0—14-17

Signature filtering enables the network security administrator to do the following:

- Reduce the number of false positives.
- Reduce the number of security events reported.



Filtering Overview (cont.)

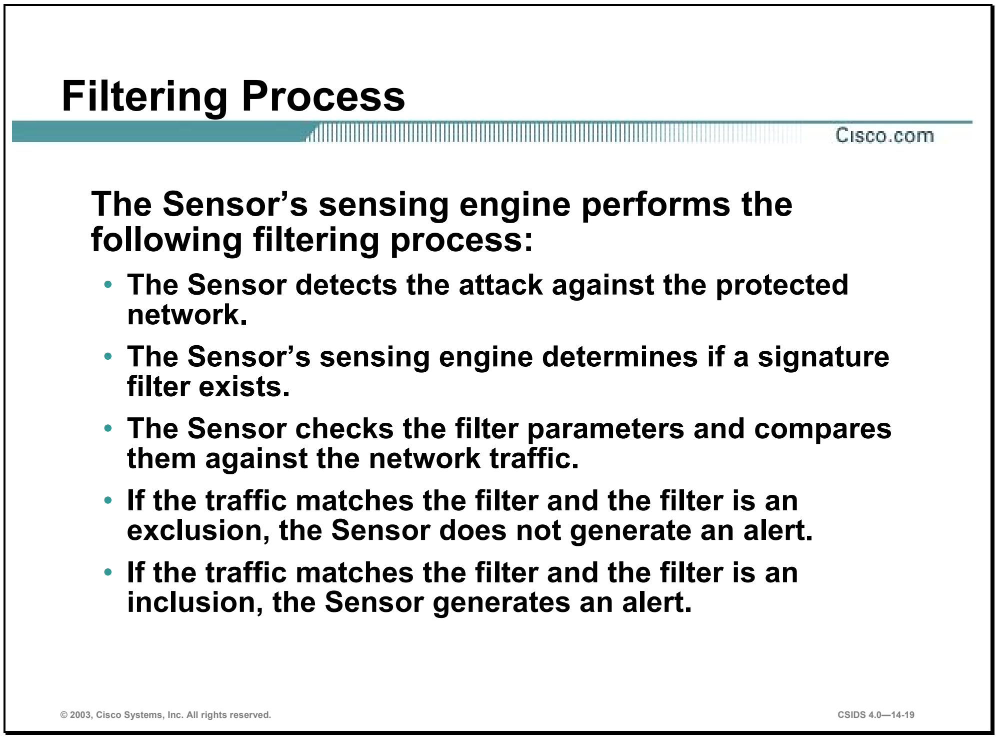
A signature filter is defined by specifying the following:

- **Signature**
- **Source address**
- **Destination address**
- **Whether it is an inclusive or exclusive filter**

CSIDS 4.0—14-18

Filtering an alarm means that the Sensor will analyze the data stream but will not generate an alarm. Filtering all alarms from a particular signature is not the same thing as disabling that signature, which results in no analysis of the data stream for that signature. A filter is defined by specifying the signature, the source address, and the destination address and whether it is an inclusive or exclusive filter.

Note IDS MC filters defined for a Sensor should not be confused with event filters that are part of a Security Monitor event rule.



Filtering Process

The Sensor's sensing engine performs the following filtering process:

- **The Sensor detects the attack against the protected network.**
- **The Sensor's sensing engine determines if a signature filter exists.**
- **The Sensor checks the filter parameters and compares them against the network traffic.**
- **If the traffic matches the filter and the filter is an exclusion, the Sensor does not generate an alert.**
- **If the traffic matches the filter and the filter is an inclusion, the Sensor generates an alert.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—14-19

The filtering process works as follows:

Step 1 The Sensor detects the attack launched against the protected network.

Step 2 The Sensor's sensing engine determines if signature filters exist.

Step 3 The Sensor checks the filter parameters and compares them against the traffic that triggered the attack.

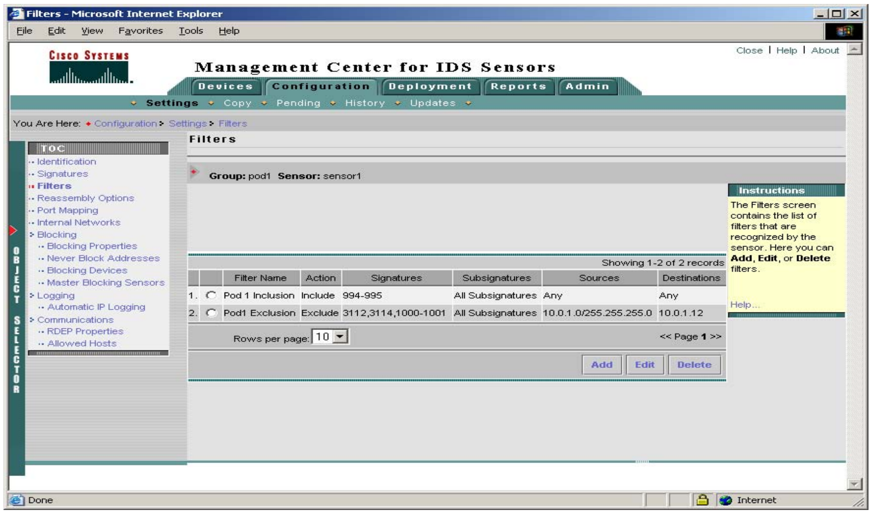
Step 4 The Sensor completes one of the following:

- If the traffic does not match the filter, the Sensor generates an alert, and the signature action is taken if configured.
- If the traffic matches the filter and the filter is an exclusion, the Sensor does not generate an alert.
- If the traffic matches the filter and the filter is an inclusion, the Sensor generates an alert and performs the signature action if configured.

Signature Filters

Cisco.com

Choose Configuration>Settings>Filters.



Filters

Group: pod1 **Sensor:** sensor1

Showing 1-2 of 2 records

		Filter Name	Action	Signatures	Subsignatures	Sources	Destinations
1.	○	Pod 1 Inclusion	Include	994-995	All Subsignatures	Any	Any
2.	○	Pod1 Exclusion	Exclude	3112,3114,1000-1001	All Subsignatures	10.0.1.0/255.255.255.0	10.0.1.12

Rows per page: 10   << Page **1** >>

Instructions

The Filters screen contains the list of filters that are recognized by the sensor. Here you can **Add**, **Edit**, or **Delete** filters.

Help...

CSIDS 4.0—14-20

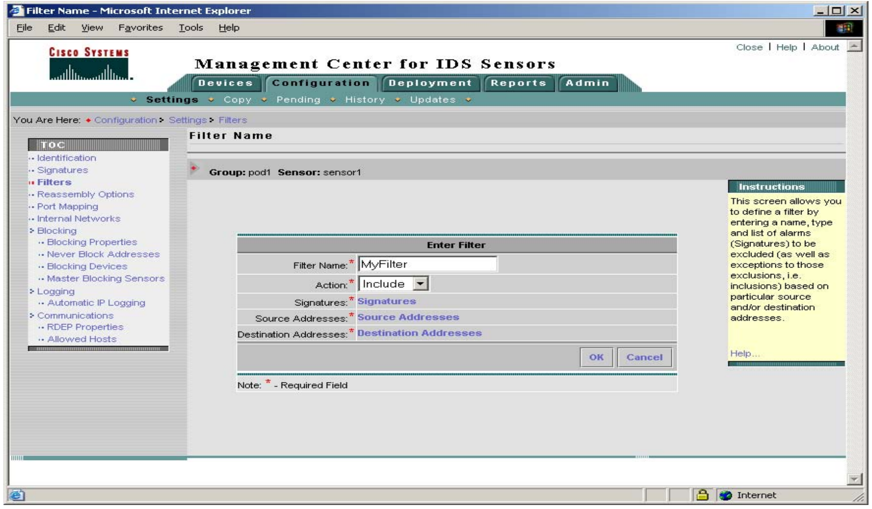
Complete the following steps to create a signature filter:

Step 1 Choose **Configuration>Settings>Filters**. The Filters page is displayed.

Step 2 Click **Add**. The Filter Name page is displayed.

Signature Filter—Add

Choose Configuration>Settings>Filters and **select** Add**.**



Filter Name

Group: pod1 **Sensor:** sensor1

Enter Filter

Filter Name:* MyFilter

Action:* Include

Signatures:* Signatures

Source Addresses:* Source Addresses

Destination Addresses:* Destination Addresses

Note: * - Required Field

Instructions

This screen allows you to define a filter by entering a name, type and list of alarms (Signatures) to be excluded (as well as exceptions to those exclusions, i.e. inclusions) based on particular source and/or destination addresses.

CSIDS 4.0—14-21

Step 3 Enter the filter’s name in the Filter Name field.

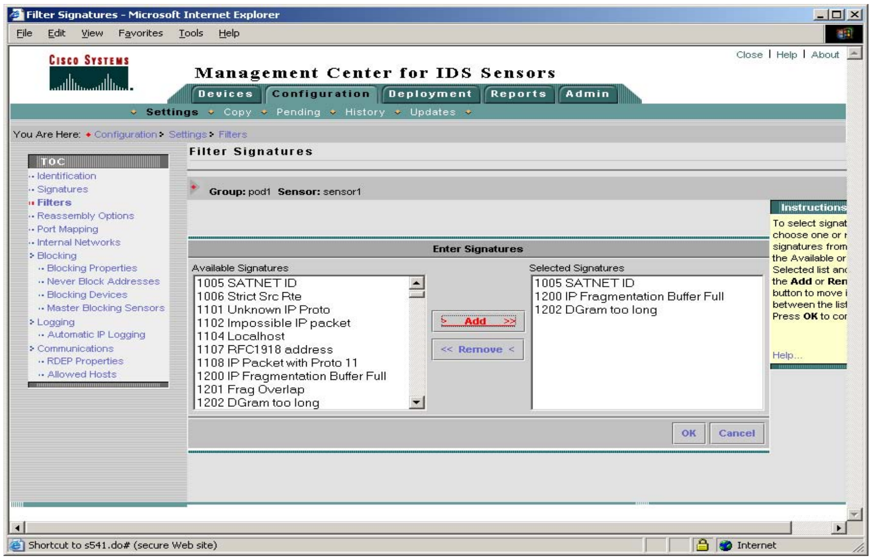
Step 4 Select **Include** or **Exclude** from the Action drop-down menu.

Step 5 Complete the following sub-steps to select signatures on which to filter:

1. Click **Signatures**. The Filter Signatures page is displayed.

Signature Filter—Add (cont.)

Cisco.com



Group: pod1 **Sensor:** sensor1

Available Signatures

1005 SATNET ID
1006 Strict Src Rte
1101 Unknown IP Proto
1102 Impossible IP packet
1104 Localhost
1107 RFC1918 address
1108 IP Packet with Proto 11
1200 IP Fragmentation Buffer Full
1201 Frag Overlap
1202 DGram too long

Selected Signatures

1005 SATNET ID
1200 IP Fragmentation Buffer Full
1202 DGram too long

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—14-22

2. Scroll through the list of Available Signatures, select a signature, and click **Add**. The signature moves to the list of Selected Signatures.

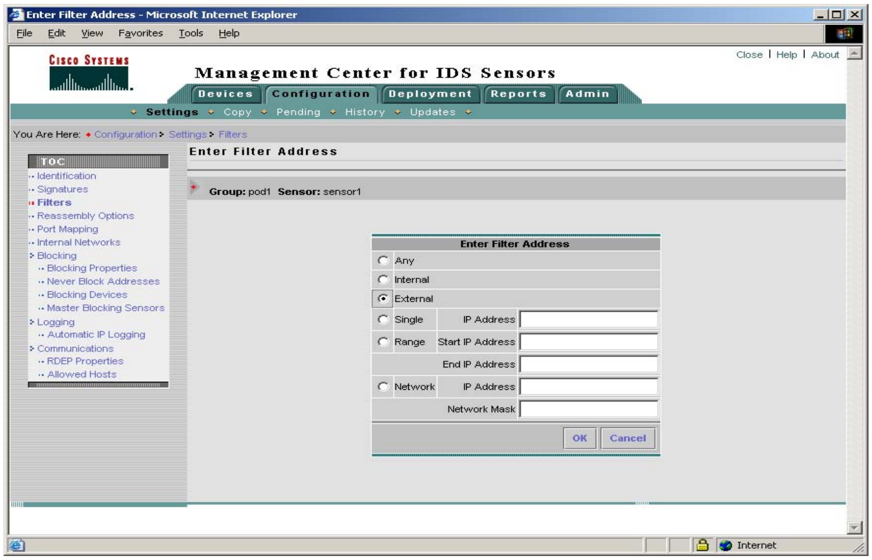
3. Click **OK**. The Filter Name page is displayed.

Step 6 Complete the following sub-steps to select source addresses on which to apply the filter:

1. Click **Source Addresses**. The Filter Source Addresses page is displayed.

2. Click **Add**. The Enter Filter Address page is displayed.

Signature Filter—Add (cont.)



You Are Here: Configuration > Settings > Filters

Enter Filter Address

Group: pod1 **Sensor:** sensor1

Enter Filter Address

○ Any		
○ Internal		
● External		
○ Single	IP Address	
○ Range	Start IP Address	
	End IP Address	
○ Network	IP Address	
	Network Mask	

OK Cancel

CSIDS 4.0—14-23

3. Select either **Any**, **Internal**, **External**, **Single**, **Range**, or **Network** as the filtered source address.

4. Click **OK**. The Filter Source Addresses page is displayed.

5. Click **OK**. The Filter Name page is displayed.

Step 7 Complete the following sub-steps to select source addresses on which to apply the filter:

1. Click **Destination Addresses**. The Filter Destination Addresses page is displayed.

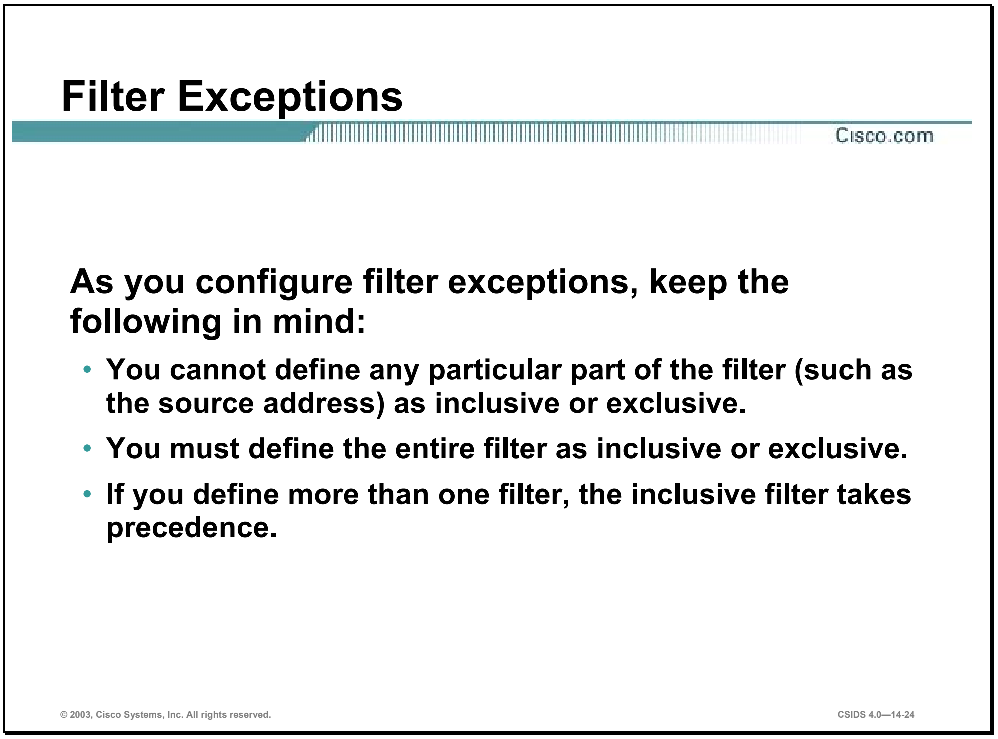
2. Click **Add**. The Enter Filter Address page is displayed.

3. Select either **Any**, **Internal**, **External**, **Single**, **Range**, or **Network** as the filtered destination address.

4. Click **OK**. The Filter Destination Addresses page is displayed.

5. Click **OK**. The Filter Name page is displayed.

Step 8 Click **OK**. The Filters page is displayed.



Filter Exceptions

As you configure filter exceptions, keep the following in mind:

- You cannot define any particular part of the filter (such as the source address) as inclusive or exclusive.
- You must define the entire filter as inclusive or exclusive.
- If you define more than one filter, the inclusive filter takes precedence.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—14-24

At times, you might need to create exceptions to filters. For example, you have a large server farm that consists of a variety of platforms. Only one of the servers on this server farm is an Apache server with the OpenSSL module (mod_ssl). Traffic from the Internet is generating a large number of 5330 alarms as someone attempts to infect servers with the Apache/mod_ssl worm. Although the attacks target many systems in your server farm, only the one running Apache with the OpenSSL module (mod_ssl) on Intel architectures is truly vulnerable. You can greatly reduce the number of alarms you receive by excluding alarms generated by the 5330 Apache/mod_ssl Worm Buffer Overflow signature and still protect your vulnerable servers by creating an exception to the exclusion. You can create an exception to the exclusion of alarms from the Internet by completing the following steps:

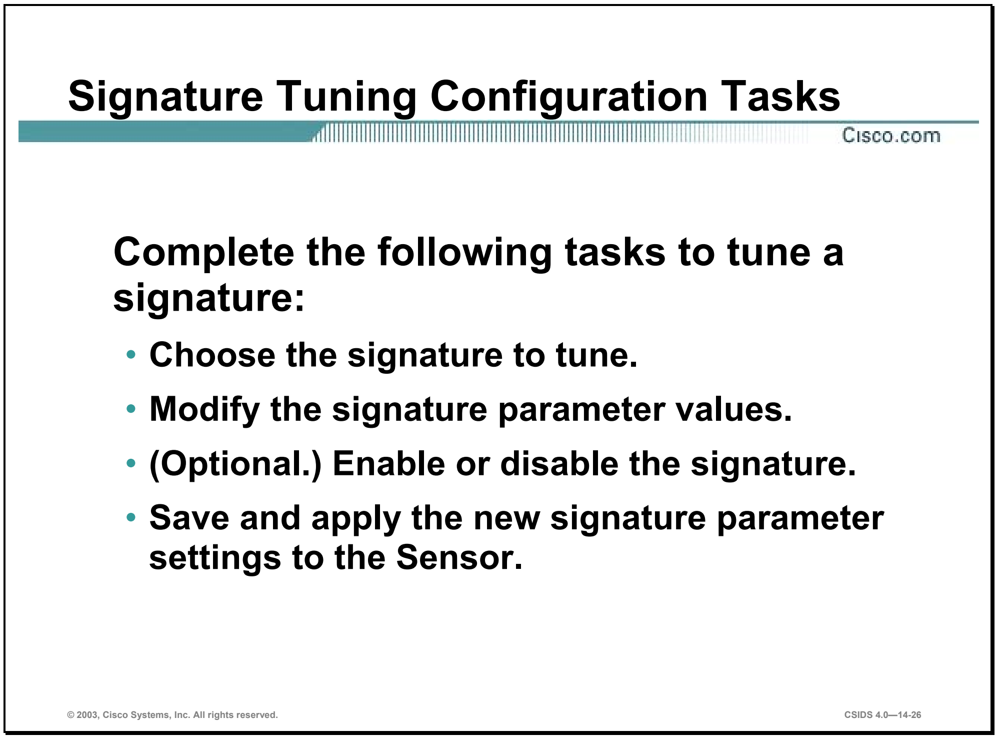
Step 1 Define an exclusive filter. Specify the source address as External, which is the network that is generating the large number of alarms. Specify the 5330 signature.

Step 2 Define an inclusive filter. Specify the same source address and the same signature. However, specify the address of your vulnerable Apache server as the destination.

By creating these two filters, you can filter out a large number alarms while allowing some of them to pass through. This is possible because the inclusion filter takes precedence when more than one filter is defined.

Signature Tuning

This section explains the tasks involved in tuning Cisco IDS signatures. A scenario in which a network security administrator would tune existing signatures is explained.



Signature Tuning Configuration Tasks

Cisco.com

Complete the following tasks to tune a signature:

- **Choose the signature to tune.**
- **Modify the signature parameter values.**
- **(Optional.) Enable or disable the signature.**
- **Save and apply the new signature parameter settings to the Sensor.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—14-26

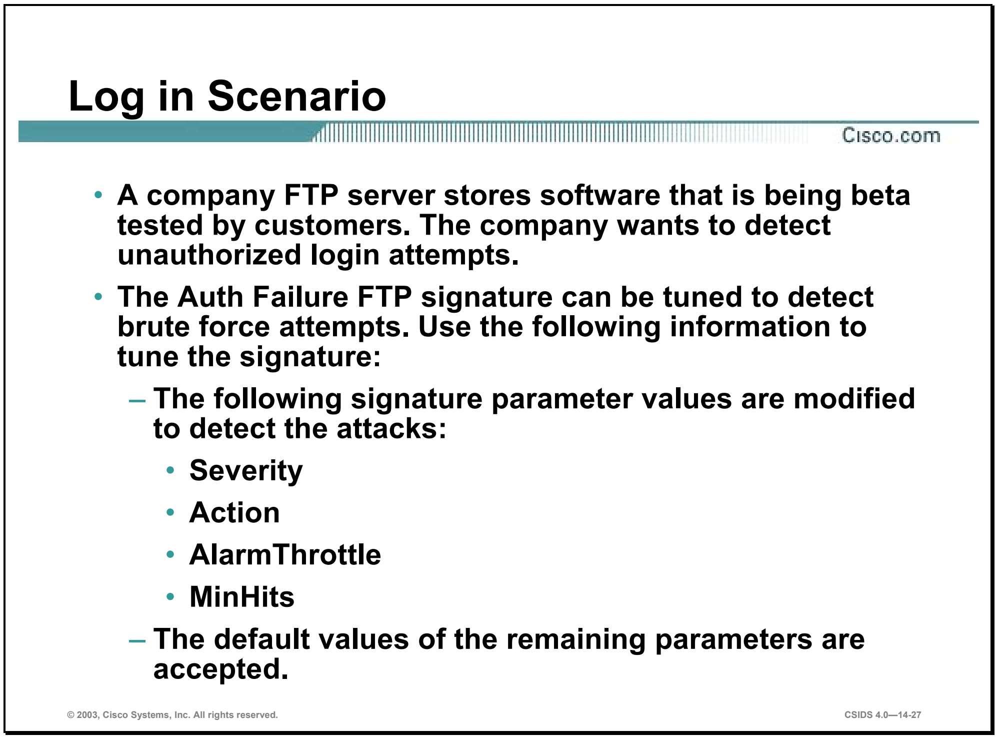
The Cisco IDS enables a network security administrator to tune existing signatures to perform optimally in their networks. Complete the following tasks to tune a signature:

- Choose the signature to tune—This task involves understanding the signature and deciding which parameter values must be modified to meet your requirements. For example, the Auth Failure FTP signature is configured to trigger if three failed login attempts are detected. The MinHits parameter controls the number of hits required to trigger the signature.

- Modify the signature parameter values—This task involves modifying the signature parameter values that are required to meet your requirements. For example, to detect two failed FTP login attempts, you would need to assign the MinHits value of 2.

- (Optional.) Enable or disable the signature—This task involves enabling or disabling the signature.

- Save and apply the new signature parameter settings to the Sensor—This task involves saving the configuration and transferring the configuration files from the IDS MC to the Sensor.



Log in Scenario

Cisco.com

- A company FTP server stores software that is being beta tested by customers. The company wants to detect unauthorized login attempts.
- The Auth Failure FTP signature can be tuned to detect brute force attempts. Use the following information to tune the signature:
  - The following signature parameter values are modified to detect the attacks:
    - Severity
    - Action
    - AlarmThrottle
    - MinHits
  - The default values of the remaining parameters are accepted.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—14-27

A company FTP server stores software that is being beta tested by customers. The company wants to detect unauthorized login attempts. The Auth Failure FTP signature can be tuned to detect these brute force attempts. Based on the threat the attack poses, the signature should meet the following requirements:

- Trigger a high severity alarm after two failed login attempts.
- Send an alarm event every time the attack is detected.
- Terminate the session.

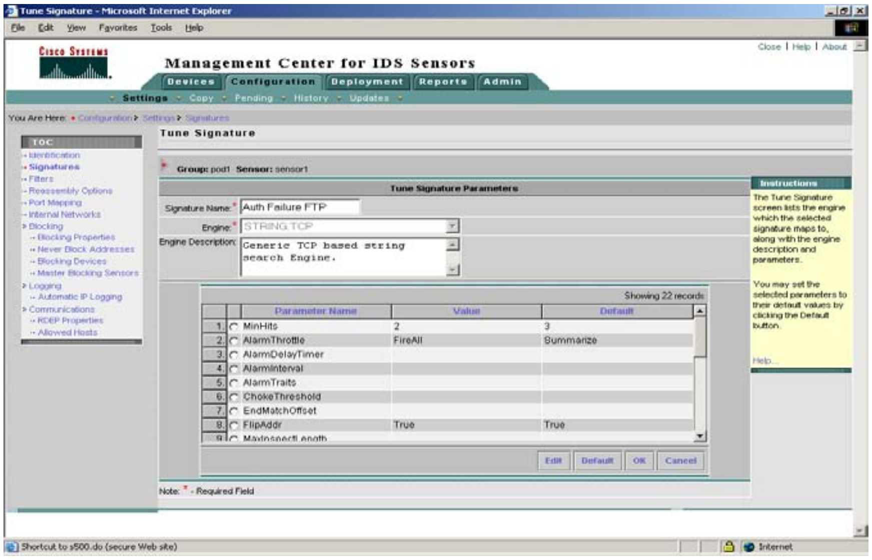
The following signature parameter values are modified based on the scenario requirements:

- Severity level
- Action
- AlarmThrottle
- MinHits

Note The default values of the remaining parameters are accepted.

Log in Scenario Configuration

Cisco.com



Tune Signature

Group: pod1 Sensor: sensor1

Tune Signature Parameters

Signature Name: * Auth Failure FTP

Engine: * STRING.TCP

Engine Description: Generic TCP based string search Engine.

Showing 22 records

		Parameter Name	Value	Default
1.	○	MinHits	2	3
2.	○	AlarmThrottle	FireAll	Summarize
3.	○	AlarmDelayTimer		
4.	○	AlarmInterval		
5.	○	AlarmTraits		
6.	○	ChokeThreshold		
7.	○	EndMatchOffset		
8.	○	FlipAddr	True	True
9.	○	MaxInspectLength		

Instructions

The Tune Signature screen lists the engine which the selected signature maps to, along with the engine description and parameters.

You may set the selected parameters to their default values by clicking the Default button.

Note: * - Required Field

Complete the following steps to tune the Auth Failure FTP signature:

Step 1 Choose **Configuration>Settings>Signatures**. The Signatures page is displayed.

Step 2 Click **General**. The Signature(s) in Group page is displayed.

Step 3 Enter **6250** in the field next to the Filter Event Source drop-down menu.

Step 4 Click **Filter**. The Signature(s) in Group page is refreshed to display the 6250 signature.

Step 5 Click the **String.TCP** engine. The Tune Signature page is displayed.

Step 6 Complete the following sub-steps to edit the minimum hits:

1. Select the **MinHits** radio button and click **Edit**. The Edit Parameters page is displayed.
2. Enter **2** in the Value Field.
3. Click **OK**. The Tune Signatures page is displayed.

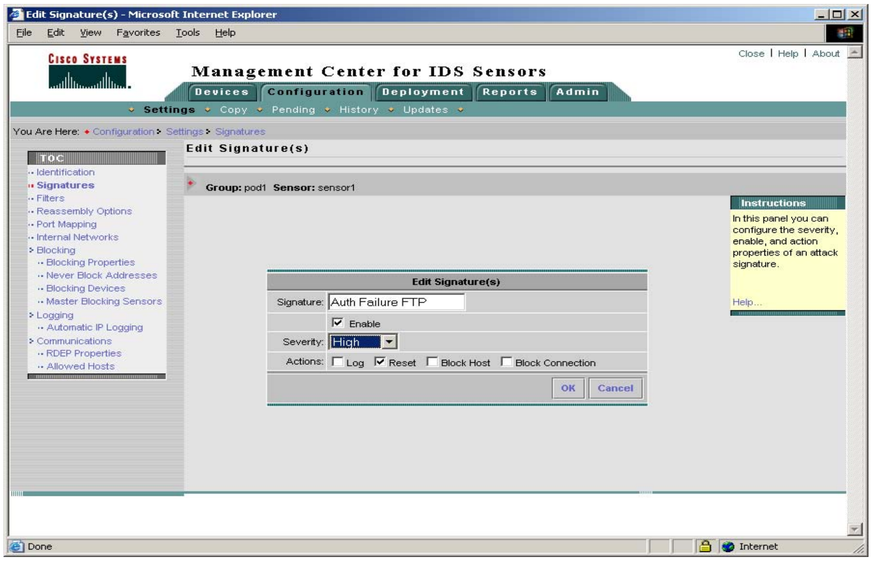
Step 7 Complete the following sub-steps to edit the alarm firings:

1. Select the **AlarmThrottle** radio button and click **Edit**. The Edit Parameters page is displayed.
2. Enter **FireAll** in the Value Field.
3. Click **OK**. The Tune Signatures page is displayed.

Step 8 Click **OK**. The Signature(s) in Group page is displayed.

Log in Scenario Configuration (cont.)

Cisco.com



Edit Signature(s)

Group: pod1 **Sensor:** sensor1

Instructions

In this panel you can configure the severity, enable, and action properties of an attack signature.

Help...

Edit Signature(s)

Signature: Auth Failure FTP

☑ Enable

Severity: High

Actions: □ Log ☑ Reset □ Block Host □ Block Connection

OK Cancel

CSIDS 4.0—14-29

Step 9 Complete the following sub-steps to edit the severity and actions:

1. Select the check box located next the signature ID 6250 and click **Edit**. The Edit Signature(s) page is displayed.

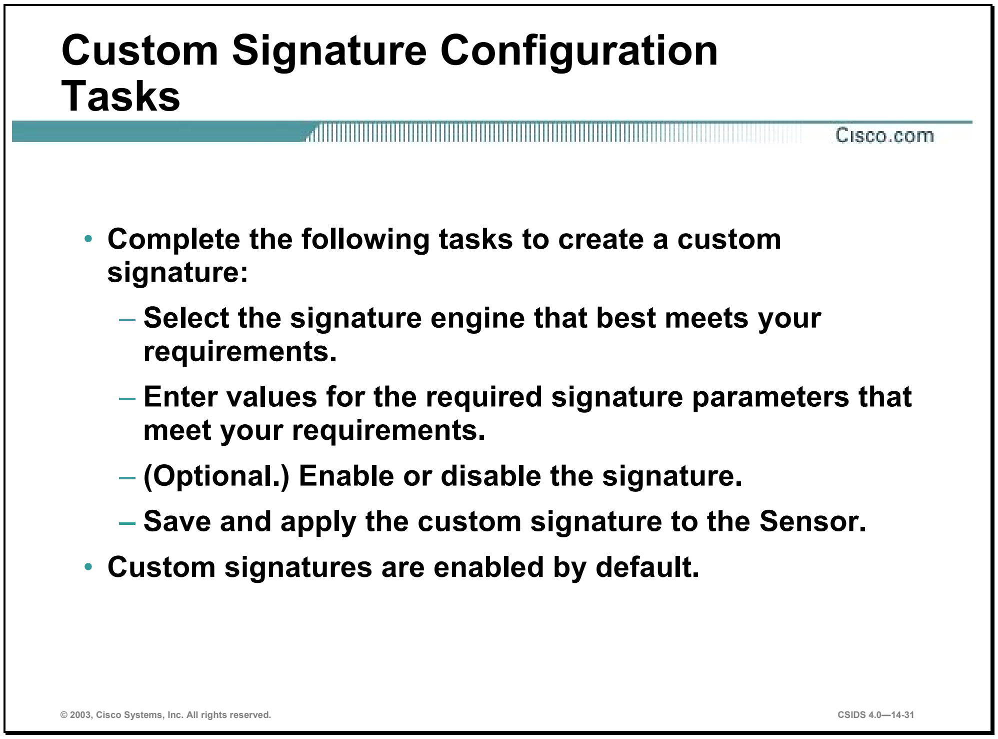
2. Select **High** from the Severity drop-down menu.

3. Select the **Reset** check box.

Step 10 Click **OK**. The Signature(s) in Group page is displayed.

Custom Signatures

This section discusses how to create custom signatures using Cisco IDS signature micro-engines. Scenarios in which a network security administrator would create custom signatures are explained.



Custom Signature Configuration Tasks

- Complete the following tasks to create a custom signature:
  - Select the signature engine that best meets your requirements.
  - Enter values for the required signature parameters that meet your requirements.
  - (Optional.) Enable or disable the signature.
  - Save and apply the custom signature to the Sensor.
- Custom signatures are enabled by default.

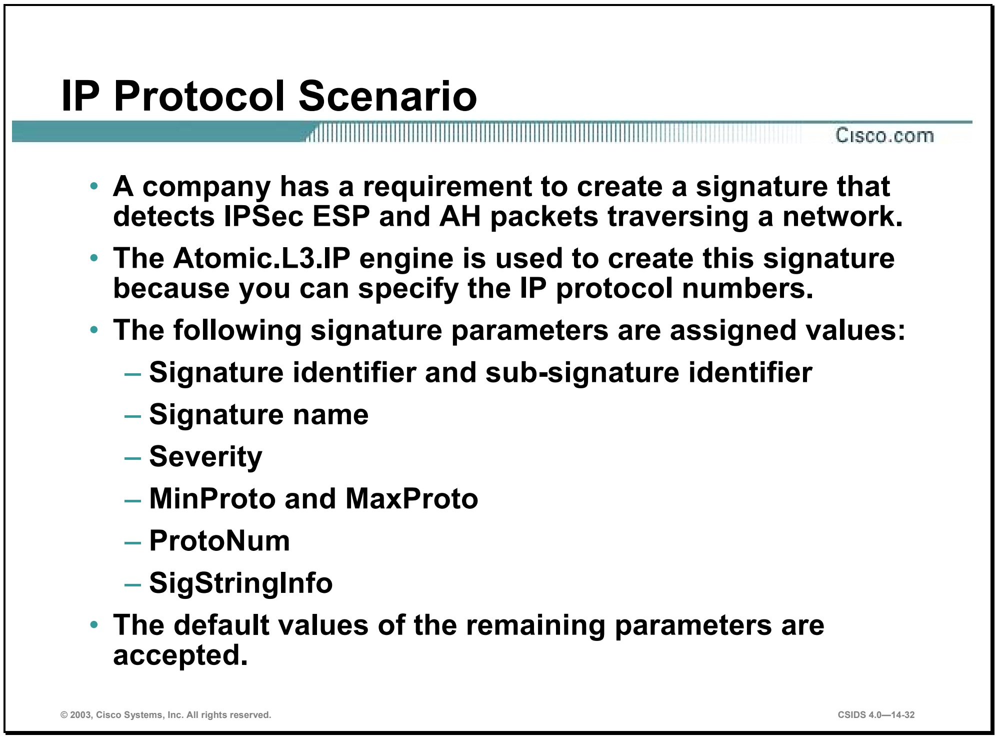
CSIDS 4.0—14-31

New vulnerabilities are discovered quicker than new signature releases can be developed and tested. The Cisco IDS enables a network security administrator to create custom signatures to detect new vulnerabilities and other unique attacks. Complete the following tasks to create a custom signature:

- Select the signature engine that best meets your requirements—This task involves understanding the signature micro-engines capabilities and deciding which engine is appropriate. For example, the String.TCP engine could not detect a UDP attack. Instead, the String.UDP engine could be selected.

- Enter the values for the signature parameters—This task involves entering the values for the signature parameters that are required and that meet your requirements. For example, to detect an SNMP attack, you would need to assign the destination port and protocol.

- Enable or disable the signature—This task involves enabling or disabling the signature. Custom signatures are enabled by default. It is recommended to test custom signatures in a non-production environment to avoid unexpected results including network disruption.



IP Protocol Scenario

- A company has a requirement to create a signature that detects IPSec ESP and AH packets traversing a network.
- The Atomic.L3.IP engine is used to create this signature because you can specify the IP protocol numbers.
- The following signature parameters are assigned values:
  - Signature identifier and sub-signature identifier
  - Signature name
  - Severity
  - MinProto and MaxProto
  - ProtoNum
  - SigStringInfo
- The default values of the remaining parameters are accepted.

CSIDS 4.0—14-32

A company has a requirement to create a signature that detects IPSec, Encapsulation Security Payload (ESP), and Authentication Header (AH) packets traversing a network.

The Atomic.L3.IP engine is used to create this signature since you can specify the IP protocol numbers.

The following signature parameters are assigned values based on the scenario requirements and those that are required by the signature engine:

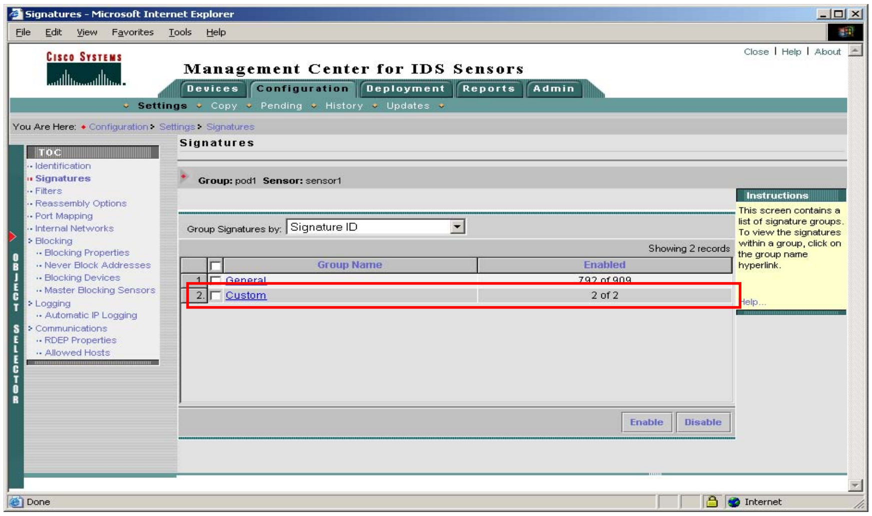
- Signature identifier
- Sub-signature identifier
- Signature name
- Severity
- MinProto
- MaxProto
- ProtoNum
- SigStringInfo

Note The default values of the remaining parameters are accepted.

Custom Signatures

Cisco.com

Choose Configuration>Signatures**.**



Signatures

Group: pod1 **Sensor:** sensor1

Group Signatures by: Signature ID

Showing 2 records

		Group Name	Enabled
	□		
1	□	General	792 of 909
2	□	Custom	2 of 2

Instructions

This screen contains a list of signature groups. To view the signatures within a group, click on the group name hyperlink.

CSIDS 4.0—14-33

Complete the following steps to begin creating a custom signature:

Step 1 Select Configuration>Settings.

Step 2 From the TOC, click the **Object Selector** handle.

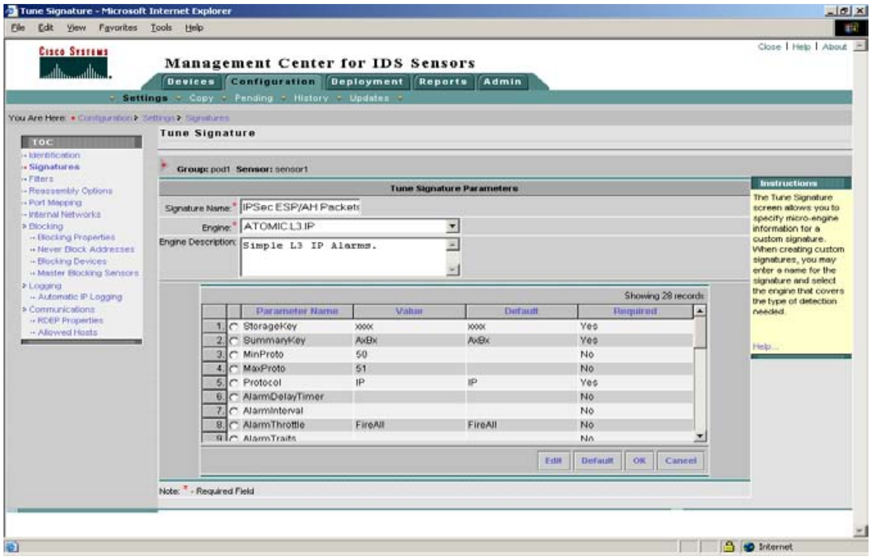
Step 3 From the Object Selector, select the Sensor for which you want to create a custom signature. The Object Selector closes.

Step 4 From the TOC, select **Signatures**. The Signatures page is displayed.

Step 5 Click the **Custom** group name. The Signatures in Group page is displayed.

Step 6 Click **Add**. The Tune Signature page is displayed.

IP Protocol Scenario Configuration



Tune Signature

Group: pod1 Sensor: sensor1

Tune Signature Parameters

Signature Name:* IPSec ESP/AH Packets

Engine:* ATOMIC.L3.IP

Engine Description: Simple L3 IP Alarms.

Showing 28 records

		Parameter Name	Value	Default	Required
1.	○	StorageKey	xxxx	xxxx	Yes
2.	○	SummaryKey	AxBx	AxBx	Yes
3.	○	MinProto	50		No
4.	○	MaxProto	51		No
5.	○	Protocol	IP	IP	Yes
6.	○	AlarmDelayTimer			No
7.	○	AlarmInterval			No
8.	○	AlarmThrottle	FireAll	FireAll	No
9.	○	AlarmTraits			No

Instructions

The Tune Signature screen allows you to specify micro-engine information for a custom signature. When creating custom signatures, you may enter a name for the signature and select the engine that covers the type of detection needed.

Note: * - Required Field

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—14-34

Complete the following steps to create the custom signature:

Step 1 Enter **IPSec ESP/AH Packets** in the Signature Name field.

Step 2 Select **Atomic.L3.IP** from the Engine drop-down menu. The Tune Signature page refreshes to indicate that you are configuring Atomic.L3.IP micro-engine parameters.

Step 3 Complete the following sub-steps to configure the signature version:

1. Select the **SigVersion** radio button and click Edit. The Edit Parameter page is displayed.
2. Enter **20002** in the Value field.
3. Click **OK**. The Tune Signatures page is displayed.

Step 4 Complete the following sub-steps to configure the maximum IP protocol number:

1. Select the **MaxProto** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Enter **51** in the Value field.
3. Click **OK**. The Tune Signatures page is displayed.

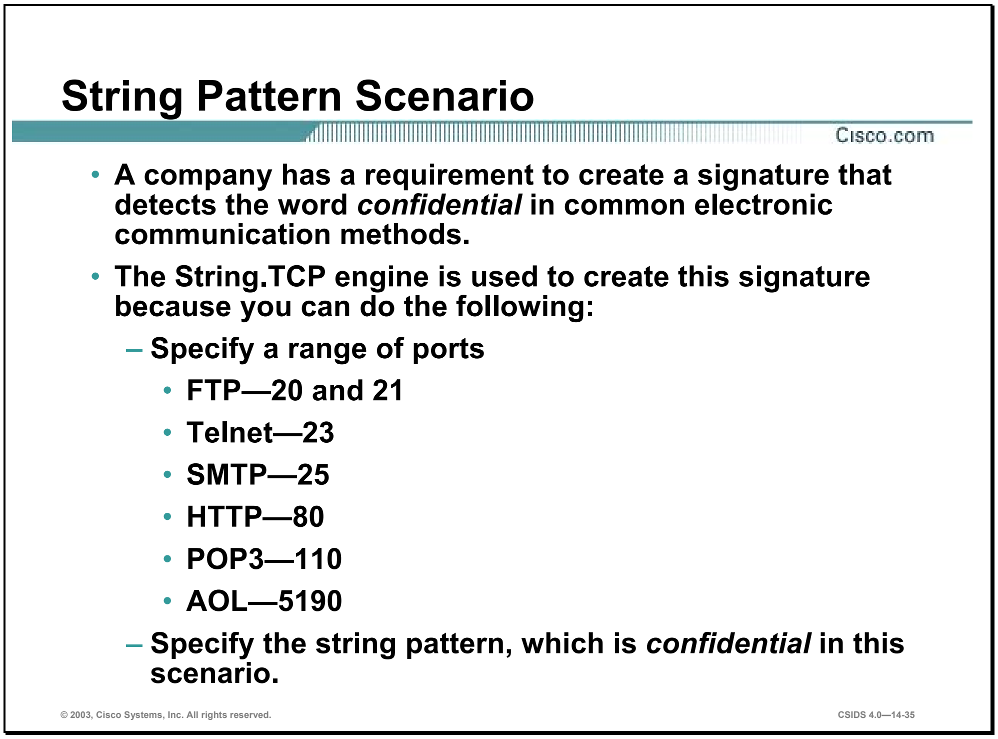
Step 5 Complete the following sub-steps to configure the minimum IP protocol number:

1. Select the **MinProto** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Enter **50** in the Value field.
3. Click **OK**. The Tune Signatures page is displayed.

Step 6 Complete the following sub-steps to configure signature string information:

1. Select the **SigStringInfo** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Enter **ESP/AH Packet** in the Value field.

Step 7 Click **OK**. The Tune Signatures page is displayed.



String Pattern Scenario

Cisco.com

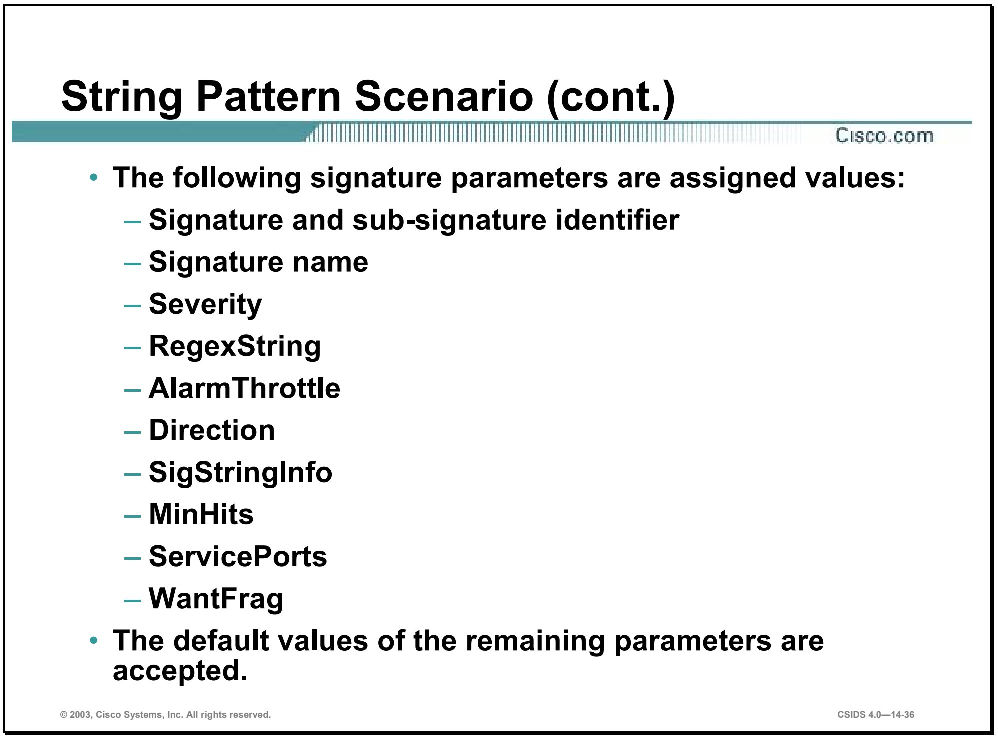
- A company has a requirement to create a signature that detects the word *confidential* in common electronic communication methods.
- The String.TCP engine is used to create this signature because you can do the following:
  - Specify a range of ports
    - FTP—20 and 21
    - Telnet—23
    - SMTP—25
    - HTTP—80
    - POP3—110
    - AOL—5190
  - Specify the string pattern, which is *confidential* in this scenario.

CSIDS 4.0—14-35

A company has a requirement to create a signature that detects the word **confidential** in common electronic communication methods.

The String.TCP engine is used to create this signature because you can to the following:

- Specify a range of ports:
  - FTP—20 and 21
  - Telnet—23
  - SMTP—25
  - HTTP—80
  - POP3—110
  - AOL—5190
- Specify the string pattern, which is confidential in this scenario.



String Pattern Scenario (cont.)

Cisco.com

- The following signature parameters are assigned values:
  - Signature and sub-signature identifier
  - Signature name
  - Severity
  - RegexString
  - AlarmThrottle
  - Direction
  - SigStringInfo
  - MinHits
  - ServicePorts
  - WantFrag
- The default values of the remaining parameters are accepted.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—14-36

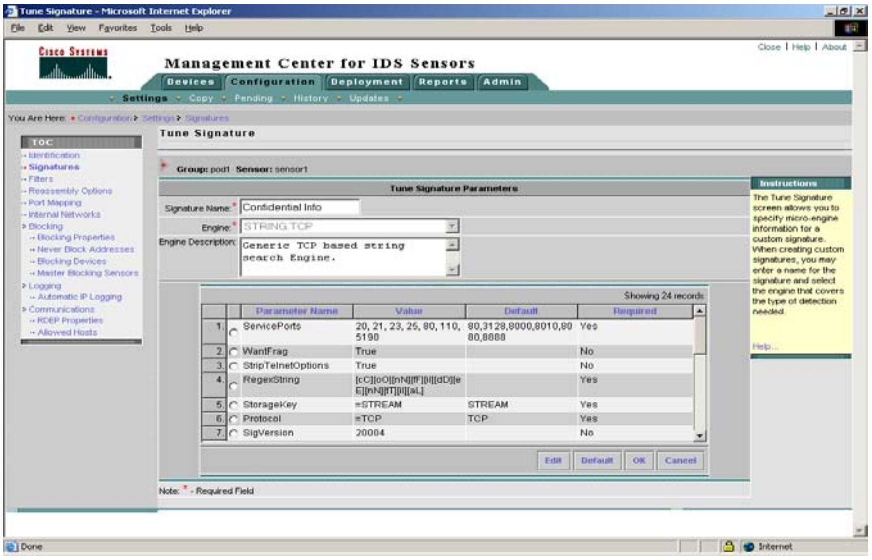
The following signature parameters are assigned values based on the scenario requirements and those that are required by the signature micro-engine:

- Signature
- Sub-signature identifier
- Signature name
- Severity
- RegexString
- AlarmThrottle
- Direction
- SigStringInfo
- MinHits
- ServicePorts
- WantFrag

Note The default values of the remaining parameters are accepted.

String Pattern Scenario Configuration

Cisco.com



Tune Signature

Group: pod1 Sensor: sensor1

Tune Signature Parameters

Signature Name:* Confidential Info

Engine:* STRING.TCP

Engine Description: Generic TCP based string search Engine.

Showing 24 records

		Parameter Name	Value	Default	Required
1.	○	ServicePorts	20, 21, 23, 25, 80, 110, 5190	80,3128,8000,8010,8080,8888	Yes
2.	○	WantFrag	True		No
3.	○	StripTelnetOptions	True		No
4.	○	RegexString	[cC][oO][nN][fF][iI][dD][eE][nN][tT][iI][aL]		Yes
5.	○	StorageKey	=STREAM	STREAM	Yes
6.	○	Protocol	=TCP	TCP	Yes
7.	○	SigVersion	20004		No

Note: * - Required Field

Instructions

The Tune Signature screen allows you to specify micro-engine information for a custom signature. When creating custom signatures, you may enter a name for the signature and select the engine that covers the type of detection needed.

Help...

CSIDS 4.0—14-37

Complete the following steps to create the custom signature:

Step 1 Select **Configuration>Settings**.

Step 2 From the TOC, click the **Object Selector** handle.

Step 3 From the Object Selector, select the Sensor for which you want to create a custom signature. The Object Selector closes.

Step 4 From the TOC, select **Signatures**. The Signatures page is displayed.

Step 5 Click **Custom**. The Signature(s) in Group page is displayed.

Step 6 Click **Add**. The Tune Signature page is displayed.

Step 7 Enter **Confidential Info** in the Signature Name field.

Step 8 Select **String.TCP** from the Engine drop-down menu. The Tune Signature page refreshes to indicate that you are configuring String.TCP micro-engine parameters.

Step 9 Complete the following sub-steps to configure the signature version:

1. Select the **SigVersion** radio button and click **Edit**. The Edit Parameter page is displayed.

2. Enter **20002** in the Value field.

3. Click **OK**. The Tune Signatures page is displayed.

Step 10 Complete the following sub-steps to configure a string pattern:

1. Select the **RegexString** radio button and click **Edit**. The Edit Parameter page is displayed.

2. Enter **[cC][oO][nN][fF][iI][dD][eE][nN][tT][iI][aA][lL]** in the Value field.

3. Click **OK**. The Tune Signatures page is displayed.

Step 11 Complete the following sub-steps to configure the signature ports:

1. Select the **ServicePorts** radio button and click **Edit**. The Edit Parameters page is displayed.
2. Enter **20, 21, 23, 25, 80, 110, 5190** in the Value field.
3. Click **OK**. The Tune Signatures page is displayed.

Step 12 Complete the following sub-steps to configure fragmentation expectations:

1. Select the **WantFrag** radio button and click **Edit**. The Edit Parameters page is displayed.
2. Enter **True** in the Value field.
3. Click **OK**. The Tune Signature page is displayed.

Step 13 Complete the following sub-steps to configure the minimum hits:

1. Select the **MinHits** radio button and click **Edit**. The Edit Parameters page is displayed.
2. Enter **1** in the Value field.
3. Click **OK**. The Tune Signature page is displayed.

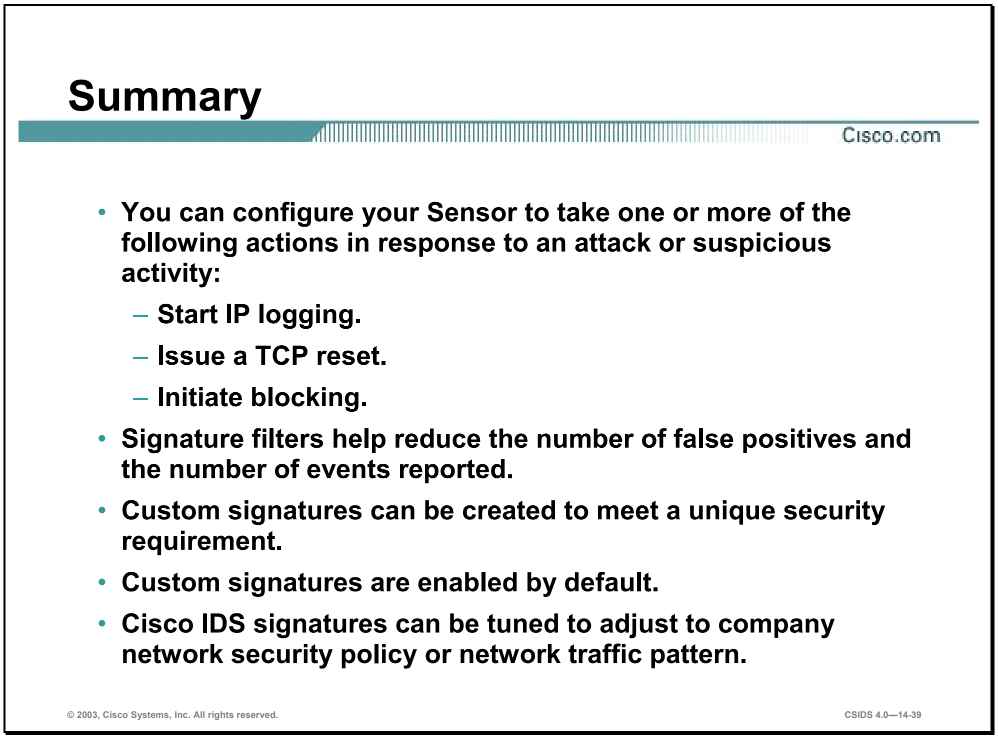
Step 14 Complete the following sub-steps to configure enable Telnet de-obfuscation:

1. Select the **StripTelnetOptions** radio button and click **Edit**. The Edit Parameters page is displayed.
2. Enter **True** in the Value field.
3. Click **OK**. The Tune Signature page is displayed.

Step 15 Click **OK**. The Signature(s) in Group page is displayed.

Summary

This section summarizes the information you learned in this chapter.



Summary

Cisco.com

- You can configure your Sensor to take one or more of the following actions in response to an attack or suspicious activity:
  - Start IP logging.
  - Issue a TCP reset.
  - Initiate blocking.
- Signature filters help reduce the number of false positives and the number of events reported.
- Custom signatures can be created to meet a unique security requirement.
- Custom signatures are enabled by default.
- Cisco IDS signatures can be tuned to adjust to company network security policy or network traffic pattern.

CSIDS 4.0—14-39

Lab Exercise—Sensing Configuration

Complete the following lab exercise to practice what you learned in this chapter.

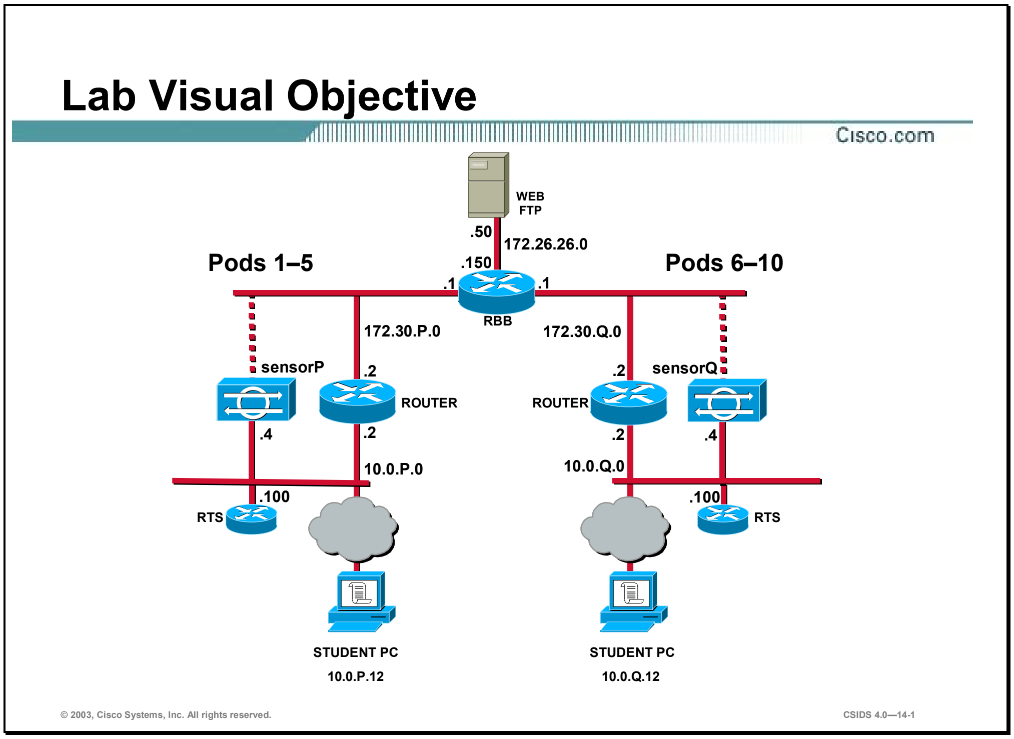
Objectives

In this lab exercise you will complete the following tasks:

- Edit the global sensing parameters.
- Create a string match signature.
- Tune a Sensor signature.
- Create a signature filter.
- Deploy the Sensor configuration.
- Test the Sensor's sensing configuration.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—14-1

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab exercise.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor. Make sure to replace it with your peer's pod number.

Task 1—Edit the Global Sensing Parameters

Complete the following steps to edit the global sensing parameters. This includes configuring automatic IP logging and reassembly options and defining internal networks.

Step 1 Use the Object Selector to select **sensorP**. The IDS MC refreshes to indicate that you are configuring sensorP settings.

(where P = pod number)

Step 2 Complete the following sub-steps to edit the internal networks:

1. Choose **Configuration>Settings>Internal Networks**. The Internal Networks page is displayed.

2. Click **Add**. The Enter Network page is displayed.

3. Select the **Network** radio button.

4. Enter **10.0.P.0** in the IP Address field and **255.255.255.0** in the Network Mask field. (where P = pod number)

5. Click **OK**. The Internal Networks page is displayed with the new internal network.

Step 3 Complete the following sub-steps to edit the reassembly options:

1. Choose **Configuration>Settings>Reassembly Options**. The Reassembly Options page is displayed.

2. Select **Solaris** from the IP Reassemble Mode drop-down menu.

3. Enter **60** in the IP Reassemble Timeout field.

4. Enter **45** in the TCP Open Establish Timeout field.

5. Enter **10** in the TCP Embryonic Timeout field.

6. Click **Apply**. The Reassembly Options page is refreshed to indicate that the IDS MC received the changes.

Task 2—Create a String Match Signature

This task involves creating a string match signature that is applied to a Sensor. Complete the following steps to create a string match signature:

Step 1 Choose **Configuration>Settings>Signatures**. The Signatures page is displayed.

Step 2 Click the **Custom** Group Name. The Signature(s) in Group page is displayed.

Step 3 Click **Add**. The Tune Signature page is displayed.

Step 4 Enter **podPStringTCP** in the Signature Name field.

(where P = pod number)

Step 5 Select **String.TCP** from the Engine drop-down menu. The Tune Signature page refreshes to indicate that you are configuring a String.TCP engine.

Step 6 Complete the following sub-steps to enter a string match pattern:

1. Select the **RegexString** radio button and click **Edit**. The Edit Parameter page is displayed.

2. Enter the string pattern to detect podP, **[pP][oO][dD]P**, in the Value field. (where P = pod number)

3. Click **OK**. The Tune Signature page is displayed.

Step 7 Complete the following sub-steps to edit the service ports:

1. Select the **ServicePorts** radio button and click **Edit**. The Edit Parameter page is displayed.

2. Clear the default values and enter **23** in the Value field.

3. Click **OK**. The Tune Signature page is displayed.

Step 8 Complete the following sub-steps to choose the direction for which we are listening to trigger this custom signature:

1. Select the **Direction** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Clear the default value and enter **ToService** in the Value field.
3. Click **OK**. The Tune Signature page is displayed.

Step 9 Click **OK**. The Signature(s) in Group page is displayed.

Step 10 Complete the following sub-steps to edit the custom signature:

1. Select the check box to the left of the new custom signature's ID and click **Edit**. The Edit Signature(s) page is displayed.
2. Choose **High** from the Severity drop-down menu.
3. Select the **Log** and **Reset Action** check boxes.
4. Click **OK**. The Signature(s) in Group page is displayed.

Task 3—Tune a Sensor Signature

This task involves modifying a built-in signature’s behavior. Complete the following steps to tune a Sensor signature:

Step 1 Choose **Configuration>Settings>Signatures**. The Signatures page is displayed.

Step 2 Click the **General Group Name**. The Signature(s) in Group page is displayed.

Step 3 Enter **2004** in the field next to the Filter Source drop-down menu and press Enter. The Signatures in Group page refreshes to display signature 2004.

Step 4 Click **Atomic.ICMP**. The Tune Signature page is displayed.

Step 5 Complete the following sub-steps to configure the alarm throttle:

1. Select the **AlarmThrottle** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Clear the default value and enter **FireAll** in the Value Field.
3. Click **OK**. The Tune Signature page is displayed.

Step 6 Complete the following sub-steps to configure the minimum hits:

1. Select the **MinHits** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Enter **3** in the Value field.
3. Click **OK**. The Tune Signatures page is displayed.

Step 7 Complete the following sub-steps to enter a comment about the signature:

1. Select the **SigComment** radio button and click **Edit**. The Edit Parameter page is displayed.
2. Enter **Three Echo Requests** in the Value field.
3. Click **OK**. The Tune Signature page is displayed.

Step 8 Click **OK**. The Signature(s) in Group page is displayed.

Step 9 Click the **ICMP Echo Req** signature name. The Edit Signature page is displayed.

Step 10 Choose the severity level, **High**, from the drop-down menu.

Step 11 Select the **Enable** check box.

Step 12 Click **OK**. The Signature(s) in Group page is displayed.

Task 4—Create a Signature Filter

This task involves creating an exclusion signature filter to exclude a signature from firing against a remote address. Complete the following steps to create a signature filter:

Step 1 Choose **Configuration>Settings>Filters**. The Filters page is displayed.

Step 2 Ensure that you are still configuring at the Sensor level by verifying that sensorP still appears in the Object Bar.

Step 3 Click **Add**. The Filter Name page is displayed.

Step 4 Enter **PodP Filter** in the Filter Name field.

(where P = pod number)

Step 5 Choose **Exclude** from the Action drop-down menu.

Step 6 Click **Signatures**. The Filter Signatures page is displayed.

Step 7 Select **2004 ICMP Echo Req** from the list of Available Signatures, and click **Add**.

Step 8 Click **OK**. The Filter Subsignatures page is displayed.

Step 9 Select **All Subsignatures** from the list of Subsignatures and click **Add**.

Step 10 Click **OK**. The Filter Name page is displayed.

Step 11 Click **Source Addresses**. The Filter Source Addresses page is displayed.

Step 12 Click **Add**. The Enter Filter Address page is displayed.

Step 13 Select **Single** and enter **10.0.Q.12** in the IP Address field.

(where Q = peer pod number)

Step 14 Click **OK**. The Filter Source Addresses page is displayed.

Step 15 Click **OK**. The Filter Name page is displayed.

Step 16 Click **Destination Addresses**. The Filter Destination Addresses page is displayed.

Step 17 Click **Add**. The Enter Filter Address page is displayed.

Step 18 Select Single and enter **10.0.P.12** in the IP Address field.

(where P = pod number)

Step 19 Click **OK**. The Filter Destination Addresses page is displayed.

Step 20 Click **OK**. The Filter Name page is displayed.

Step 21 Click **OK**. The Filters page is displayed. Notice that the filter, PodP Filter, is displayed in the list of filters.

Task 5—Deploy the Sensor Configuration

Complete the following steps to deploy the configuration to the Sensor:

Step 1 Choose **Configuration>Pending**. The Pending page is displayed.

Step 2 Select the check box to the left of the new configuration entry and click **Save**.

Step 3 Choose **Deployment>Generate**. The Generate page is displayed.

Step 4 Select the **sensorP** check box and click **Generate**. The Generate Status page is displayed.

(where P = pod number)

Step 5 Choose **Deployment>Deploy**. The Deploy page is displayed.

Step 6 Click **Submit**. The Submit page is displayed.

Step 7 Select the **sensorP** check box and click **Deploy**. The Select Configurations page is displayed.

Step 8 Select the check box to the left of the most recently generated configuration.

Step 9 Click **Next**. The Enter Job Properties page is displayed.

Step 10 Enter **Sensing Parameters** in the Job Name field.

Step 11 Select the **Email report to** check box and enter **studentP@cisco.com** in the Email reports to field.

(where P = pod number)

Step 12 Click **Finish**. The Submit page is displayed.

Step 13 Open your e-mail client and wait for the Sensor configuration deployment confirmation e-mail to arrive in your Inbox.

Note The e-mail confirmation may take awhile to deploy depending on the speed of the network and processing power of the IDS MC server.

Task 6—Test the Sensor's Sensing Configuration

Complete the following steps to test the Sensor's sensing configuration:

Step 1 Complete the following sub-steps to test the string match signature:

1. Telnet to IP address 172.26.26.150.
2. Enter **podP** at the password prompt.
   (where P = pod number)
3. The Telnet session should close because entering podP triggers the string match signature.
   (where P = pod number)

Step 2 Complete the following sub-steps to test the tuned signature:

1. Open an SSH session to **sensorP**.
   (where P = pod number)
2. Clear all events:

```
sensorP# clear events
Warning: Executing this command will remove all events currently stored in the
event store.
Continue with clear? :
```

3. Enter **yes** to continue:

```
Continue with clear? : yes
```

4. Verify that all events have been cleared:

```
sensor# show events
```

5. Open a Windows command prompt and issue the command **ping 10.0.Q.4**. (where Q = peer pod number)

6. Go back to the SSH session and verify that an event is now displayed on the console thus indicating the signature fired correctly.

7. Verify that the severity level displayed is **High**.

Step 3 Complete the following sub-steps to test the signature filter:

1. Clear all events:

```
sensorP# clear events
Warning: Executing this command will remove all events currently stored in the
event store.
Continue with clear? :
```

2. Enter **yes** to continue:

```
Continue with clear? : yes
```

3. Verify that all events have been cleared:

```
sensor# show events
```

4. Open a Windows command prompt and issue the command **ping 10.0.Q.12**. (where Q = peer pod number)

5. Return to the SSH session and verify that no events are listed in the console thus indicating that the filter is performing as expected.

Blocking Configuration

Overview

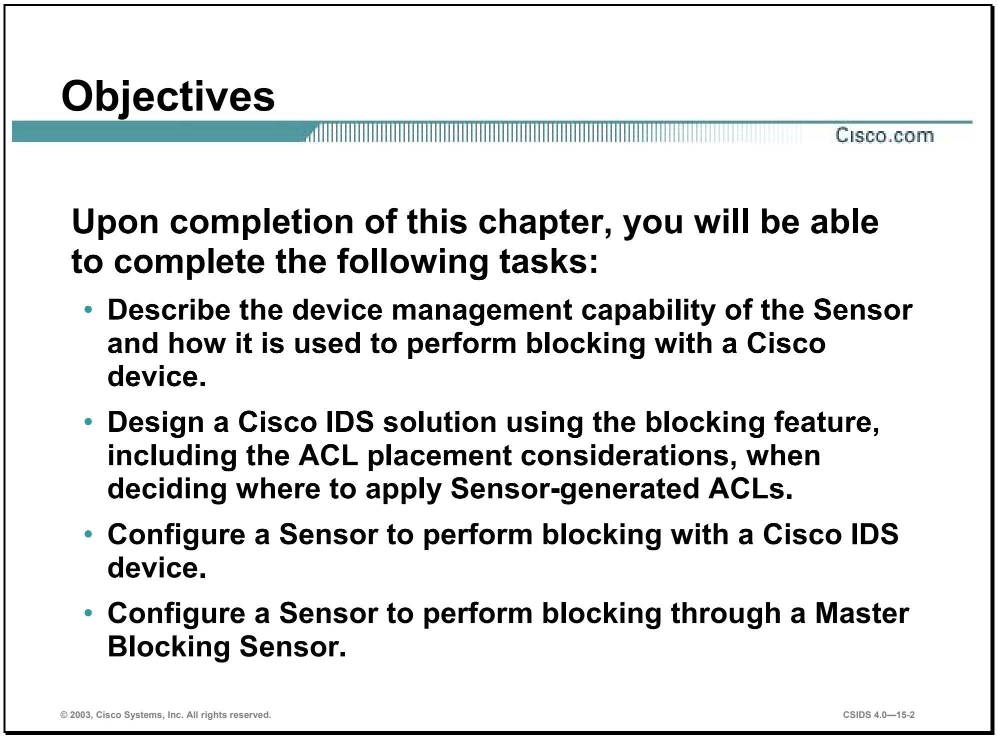
This chapter describes how to configure the blocking capability on a Cisco Intrusion Detection System (IDS) Sensor and how blocking is used. In addition, it explains considerations you need to make before you select the interface on which to apply the blocking access control lists (ACLs).

This chapter includes the following topics:

- Objectives
- Introduction
- ACL considerations
- Blocking Sensor configuration
- Master Blocking Sensor configuration
- Summary
- Lab exercise

Objectives

This section lists the chapter’s objectives.



Objectives

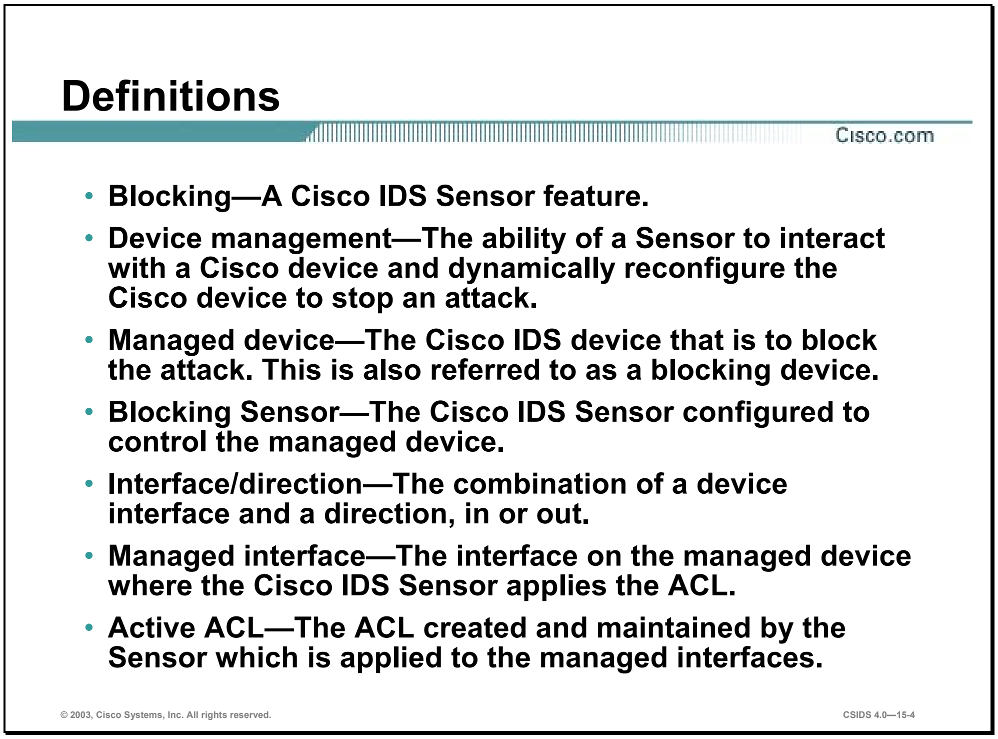
Upon completion of this chapter, you will be able to complete the following tasks:

- **Describe the device management capability of the Sensor and how it is used to perform blocking with a Cisco device.**
- **Design a Cisco IDS solution using the blocking feature, including the ACL placement considerations, when deciding where to apply Sensor-generated ACLs.**
- **Configure a Sensor to perform blocking with a Cisco IDS device.**
- **Configure a Sensor to perform blocking through a Master Blocking Sensor.**

CSIDS 4.0—15-2

Introduction

This section explains what blocking is and provides some guidelines when designing a Cisco IDS solution that incorporates the blocking feature.



Definitions

Cisco.com

- Blocking—A Cisco IDS Sensor feature.
- Device management—The ability of a Sensor to interact with a Cisco device and dynamically reconfigure the Cisco device to stop an attack.
- Managed device—The Cisco IDS device that is to block the attack. This is also referred to as a blocking device.
- Blocking Sensor—The Cisco IDS Sensor configured to control the managed device.
- Interface/direction—The combination of a device interface and a direction, in or out.
- Managed interface—The interface on the managed device where the Cisco IDS Sensor applies the ACL.
- Active ACL—The ACL created and maintained by the Sensor which is applied to the managed interfaces.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—15-4

The following are terms used when discussing the Cisco IDS blocking feature:

- Blocking—A Cisco IDS feature commonly referred to as blocking.

- Device management—The ability of a Sensor to interact with a Cisco device and dynamically reconfigure the Cisco device to block the source of an attack in real time.

- Managed device—The Cisco device that actually blocks the attack. It is also referred to as a blocking device.

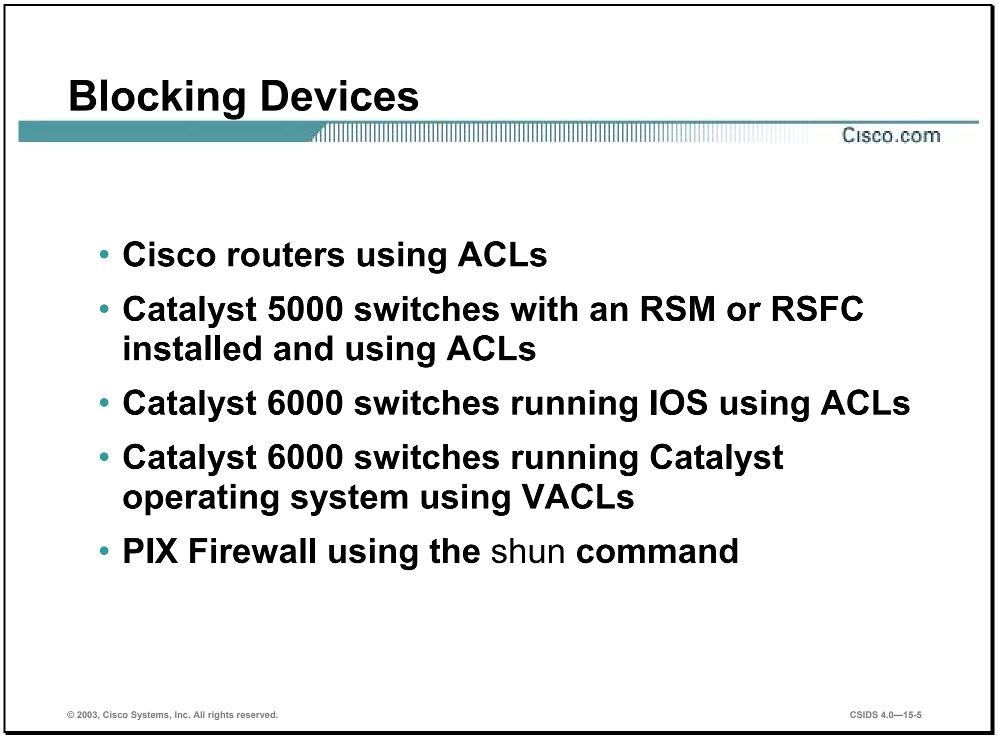
- Blocking Sensor—A Sensor that has been configured to control a managed device.

- Interface/direction (ACLs only)—The combination of a device's interface and a direction, in or out, which specifies the blocking of inbound or outbound packets on a particular interface. Blocking is configured separately for each device's interface/direction. The Sensor can be configured to block a total of 10 interface/directions across all devices.

- Managed interface/VLAN—The interface/VLAN on the managed device where the Sensor applies the dynamically created ACL or VACL. This interface/VLAN is also referred to as a blocking interface/VLAN.

Note The Cisco PIX Firewall uses the **shun** command to enforce a block. The PIX Firewall ACLs are not modified.

- Active ACL/VACL—This ACL/VACL is dynamically created and maintained by the Sensor, which is applied to the managed interface/VLAN.



Blocking Devices

Cisco.com

- Cisco routers using ACLs
- Catalyst 5000 switches with an RSM or RSFC installed and using ACLs
- Catalyst 6000 switches running IOS using ACLs
- Catalyst 6000 switches running Catalyst operating system using VACLs
- PIX Firewall using the shun command

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—15-5

The Sensor Network Access Controller (NAC) service can control up to 10 supported devices in any combination. The figure shows a list of blocking devices that have been approved and tested to work with the Sensors and device management:

- Cisco routers running Cisco IOS Release 11.2 or later using ACLs
- Catalyst 5000 switches running Cisco IOS Release 11.2(9)P or later with a Router Switch Module (RSM) or Route Switch Feature Card (RSFC) installed using ACLs
- Catalyst 6000 switches running Cisco IOS Release 12.1(13)E or later using ACLs—Requires one of the following:
  - Multilayer Switch Feature Card 1 (MSFC1)
  - MSFC2
- Catalyst 6000 switches running Catalyst operating system version 7.5(1) or later—Requires one of the following:
  - Sup1A
  - Sup1A/Policy Feature Card (PFC)
  - Sup1A/MSFC1
  - Sup1A/MSFC2

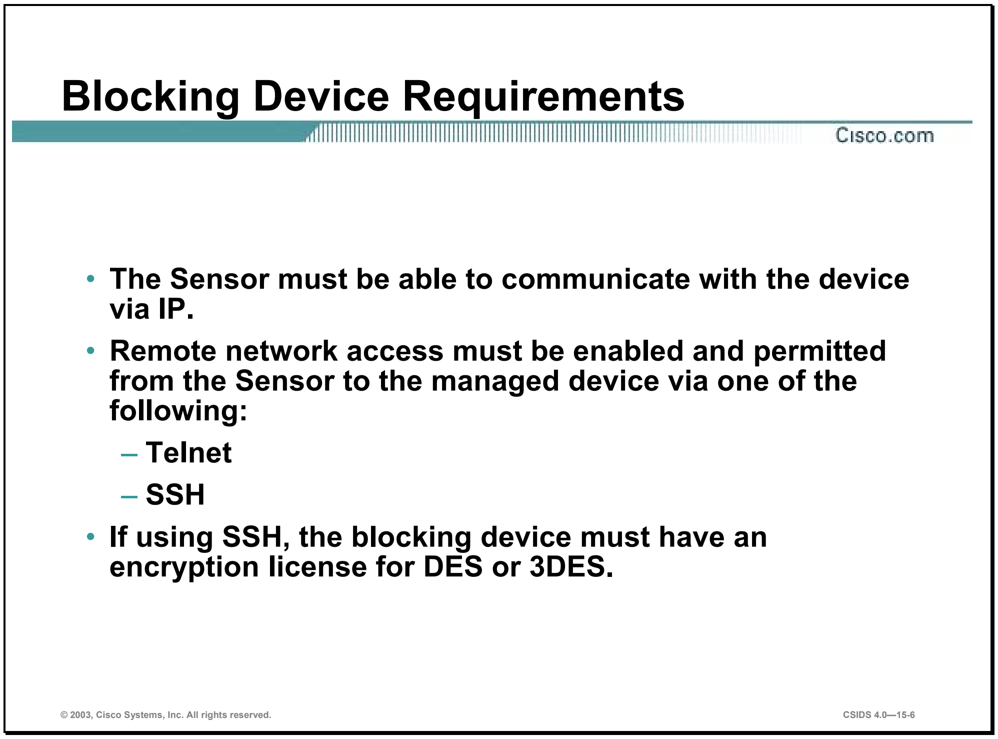
  - Sup2/MSFC2

- PIX Firewall running version 6.0 or later using the **shun** command—Requires one of the following:
  - 501
  - 506E
  - 515E
  - 525
  - 535

Blocking is configured using either ACLs, VACLs, or the **shun** command. All PIX Firewall models that support the **shun** command can be used as blocking devices. The **shun** command was introduced in PIX Firewall operating system 6.0.

The Sensor must be able to communicate with the managed device. The Sensor must have a route to or exist on the same subnet as the managed device. The Cisco device must have the following configured:

- VTY (Telnet access) should be enabled and assigned a line password on Cisco routers.
- Telnet access should be allowed from the Sensor.
- The enable password must be assigned.



Blocking Device Requirements

- The Sensor must be able to communicate with the device via IP.
- Remote network access must be enabled and permitted from the Sensor to the managed device via one of the following:
  - Telnet
  - SSH
- If using SSH, the blocking device must have an encryption license for DES or 3DES.

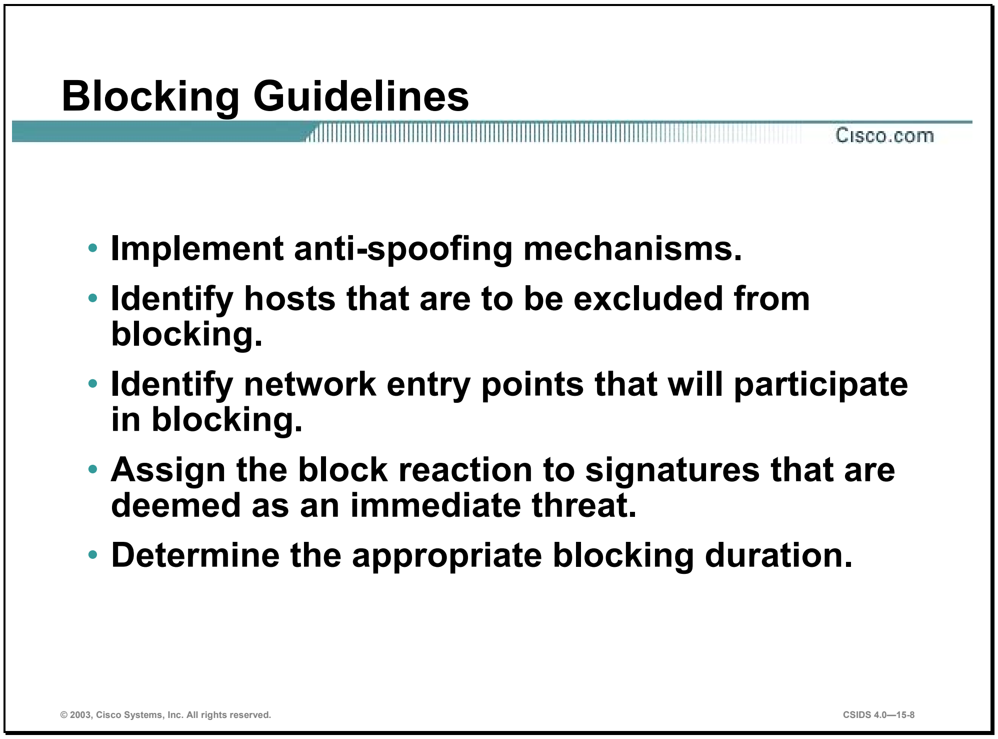
© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—15-6

The Sensor must be able to communicate with the blocking device. The Sensor must have a route to or exist on the same subnet as the managed firewall. The blocking device must have one the following configured:

- Telnet enabled—Telnet access should be allowed from the Sensor, or
- Secure shell (SSH) enabled—SSH access should be allowed from the Sensor.

Note The SSH configuration is optional but recommended. If SSH is configured, the Sensor and the blocking device must exchange keys manually using the **ssh host-key** command. The blocking device must have a software license that supports Data Encryption Standard (DES) or 3DES encryption.

As soon as the blocking device is configured on the Sensor, the Sensor attempts to log into the blocking device using the specified credentials and access protocol, Telnet or SSH. If the Sensor logs in successfully, a user connection is maintained between the Sensor and the blocking device. This persistent connection allows the Sensor to immediately and dynamically configure blocking rules on the blocking device as required.



Blocking Guidelines

Cisco.com

- Implement anti-spoofing mechanisms.
- Identify hosts that are to be excluded from blocking.
- Identify network entry points that will participate in blocking.
- Assign the block reaction to signatures that are deemed as an immediate threat.
- Determine the appropriate blocking duration.

CSIDS 4.0—15-8

The Cisco IDS blocking feature is a powerful feature that must be used after thorough planning. The automatic blocking feature generates blocking rules, ACLs, VACLs, and **shun** commands, based solely on the IP addresses of the hosts that generate the alarms. The Sensor cannot determine whether or not the attacking host should be considered a friend or foe. Consequently, it is quite possible that the blocking feature may block legitimate network traffic. The key points to remember when designing and implementing blocking are as follows:

- Anti-spoofing mechanisms—Attackers will forge packets with IP addresses that are either private addresses (RFC 1918) or addresses of your internal network. The attacker's goal may be to elude detection, to gain privileged access through the use of a trusted address, or to cause a Denial of Service (DoS) if Sensor blocking is configured. By implementing a proper anti-spoofing mechanism and network ingress and egress filtering (RFC 2827), the Sensor will not block possible valid addresses.

- Critical hosts—Each network has critical hosts that should not be blocked. It is important to identify these hosts to prevent possible network disruptions.

- Network topology—Determine which devices should be blocked by which Sensor. Two Sensors cannot control blocking on the same device.

- Entry points—Today's networks have several entry points to provide for reliability, redundancy, and resilience. These entry points are different avenues for the attacker to attack your network. It is important to identify all entry points and decide if the connecting devices should participate in blocking.

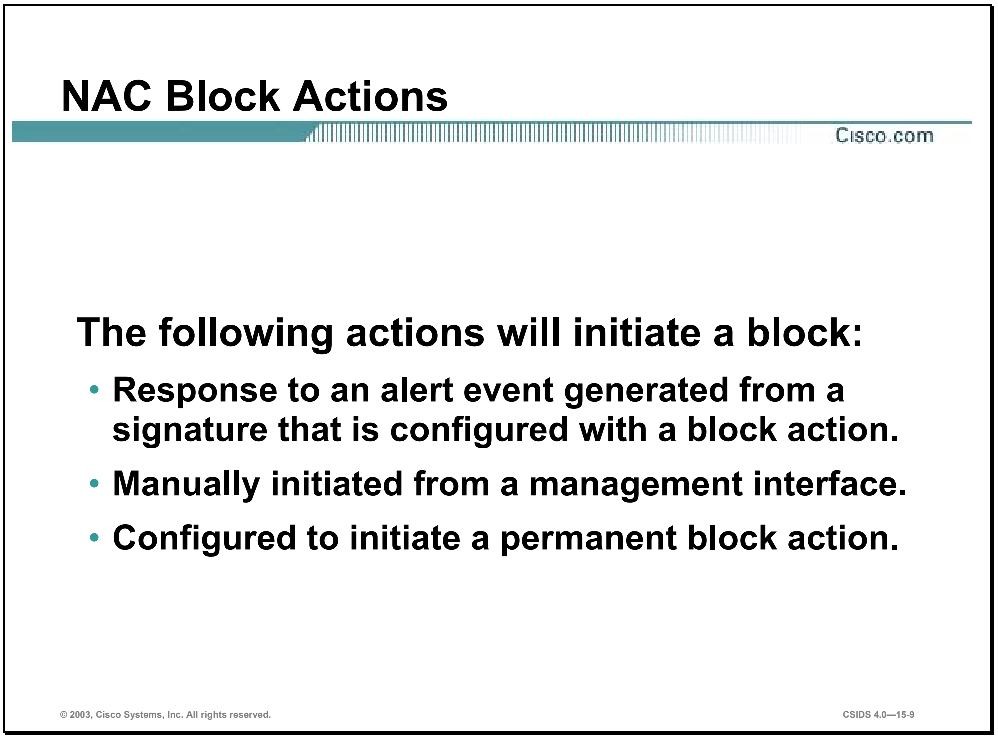
- Signature selection—Cisco IDS contains several hundred signatures that can be configured to perform blocking. It is not feasible to perform blocking on all signatures. Identify which signatures are best suited to perform blocking. For example, if you were only allowing Web traffic to your server farm, you would identify web related signatures specific to your Web server software. From this list of signatures, you would then identify those signatures whose severity is High and could potentially lead to access. These signatures would be candidates to perform blocking.

- Blocking duration—By default the Sensor will automatically block for 30 minutes. Determine the appropriate time for your network environment.

- Device login information—Before configuring blocking, you must determine any username, password, modal passwords, and connection types needed to log into each blocking device.

- Interface ACL requirements—Each interface/direction can only have one active ACL. Therefore, if an interface needs other ACL entries besides the blocking ACL entries generated by the Sensor, these entries should be configured on the blocking device in the form of a pre-block and post-block ACL. The pre-block and post-block ACLs must be configured on the blocking device independently of the Sensor. These ACLs provide a way to include access rules that a network administrator needs processed before and after the blocking rules are added by the Sensor. When the Sensor NAC service generates an ACL for a device, the NAC first includes all the entries from the Pre-block ACL. The NAC then appends its own blocking entries. Finally, the NAC appends the Post-block ACL entries to the new ACL of the device. The dynamically created ACL is applied to the specified interface with the specified direction, in/out. When blocking is not in effect, the resulting ACL applied to the interface is simply a combination of the Pre- and Post-block ACL without any blocking entries inserted.

Note It is important to understand which interfaces should and should not be blocked in order to avoid inadvertently shutting down an entire network.



NAC Block Actions

The following actions will initiate a block:

- **Response to an alert event generated from a signature that is configured with a block action.**
- **Manually initiated from a management interface.**
- **Configured to initiate a permanent block action.**

© 2003, Cisco Systems, Inc. All rights reserved.

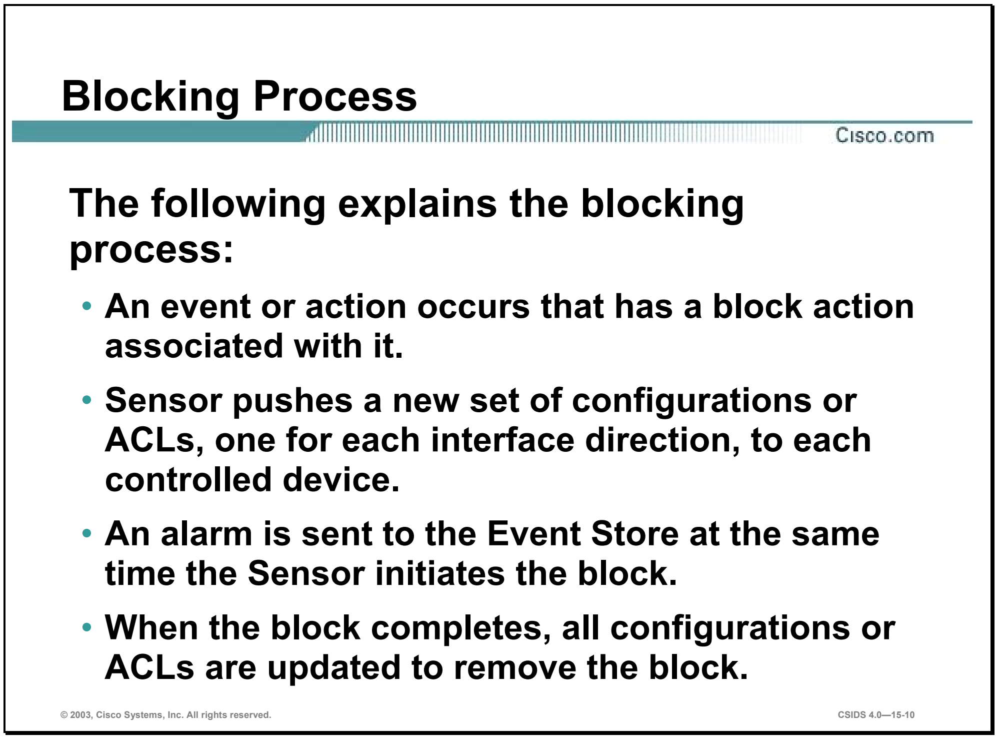
CSIDS 4.0—15-9

The Network Access Controller (NAC) is the Sensor service that performs the network access control, or blocking, function. The NAC controls starting and stopping blocks on routers, switches, and PIX Firewalls.

The following actions will initiate a block:

- The NAC can automatically initiate a block in response to an alert event generated from a signature that is configured with a block action.
- A block can be manually initiated from a management interface such as the command line interface (CLI), IDS Module (IDM), or the Management Center for IDS Sensors (IDS MC). A block can be temporary or permanent if it is configured from the CLI.
- The NAC can be configured to initiate a permanent block, whereby a host or network address is permanently blocked. Using IDM, a manual block can be configured for a specific duration.

Note The Sensor determines if a block is temporary or permanent. For managed devices, all blocks are permanent.



Blocking Process

The following explains the blocking process:

- An event or action occurs that has a block action associated with it.
- Sensor pushes a new set of configurations or ACLs, one for each interface direction, to each controlled device.
- An alarm is sent to the Event Store at the same time the Sensor initiates the block.
- When the block completes, all configurations or ACLs are updated to remove the block.

CSIDS 4.0—15-10

The following explains the blocking process:

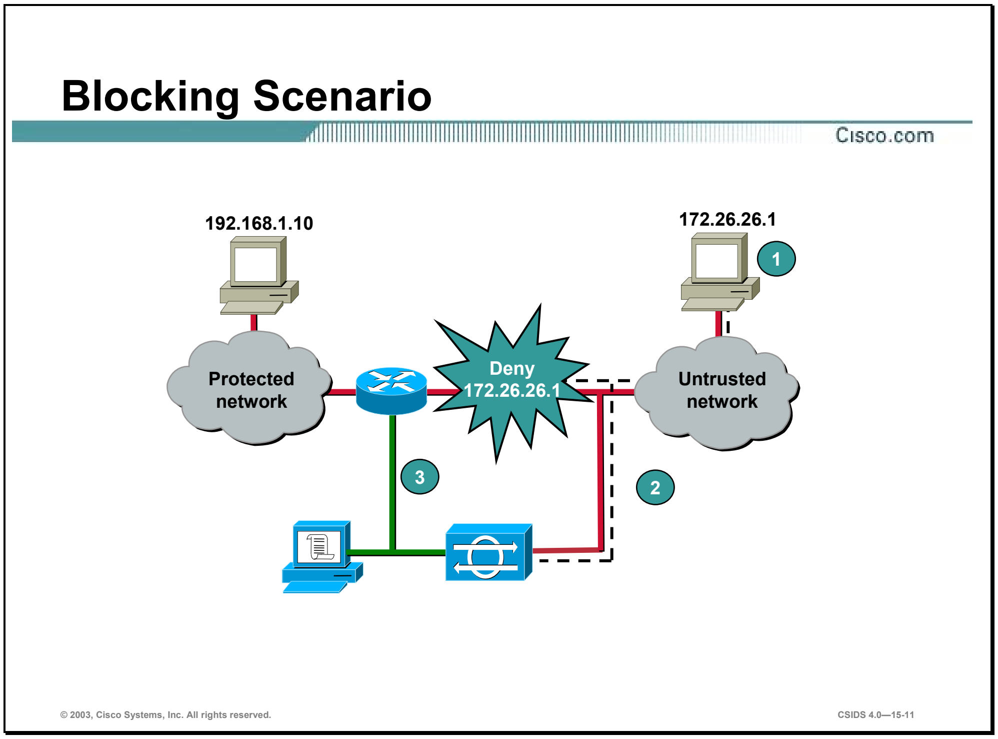
- An event or action occurs that has a block action associated with it.

Note If the NAC is configured to permanently block a specific device, the NAC initiates either a Telnet or a SSH connection with the device and maintains the connection with the device.

- The NAC pushes a new set of configurations or ACLs, one for each interface/direction, to each controlled device. It applies the blocking rules to all configured interface/directions on all devices it is configured to control.
- The alarm is sent to the Event Store at the same time the Sensor initiates the block. The block and alarm occur independently of each other.
- When the blocking event completes, all configurations or ACLs are updated to remove the Sensor’s blocking rules.

A time limit can be specified for any manual block except for a permanent block, which is in effect as long as it is configured. The duration of automatic blocks is set globally for all signatures; the default is 30 minutes.

The number of blocking entries that can be active at any given time is configurable with a default limit of 100. The number of blocking entries is not the same as the number of interface/directions. The number of interface/directions corresponds to the number of ACLs that the NAC has to update when a block state changes. The number of blocking entries corresponds to the number of entries in each ACL. The blocking entry in the ACL specifies a host address or network address to be blocked.



Blocking Scenario

CSIDS 4.0—15-11

The following steps describe the blocking process for the scenario in the figure:

Step 1 An attack starts when an attacker executes a hack to gain access to the protected network. In the figure, the attacker’s IP address is 172.26.26.1. The attacker has launched attacks against the server at 192.168.1.10.

Step 2 The Sensor detects the attack and generates an alert. The signature triggered was configured to enforce an automatic block.

Step 3 At the same time, the Sensor automatically writes a new ACL on the managed router denying traffic from the attacking host. The managed router then denies any future traffic generated by the attacking host until the block is manually removed or the default automatic block time expires. The ACL entry written to the router would be similar to the following example:

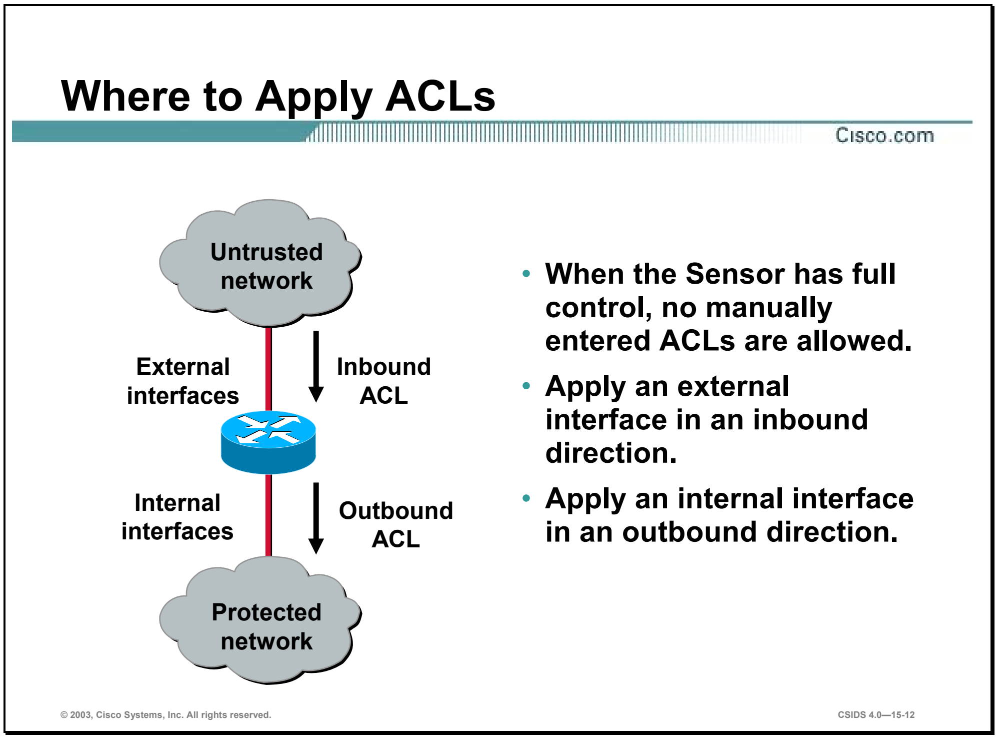
```
access-list IDS_e0/1_in_1 deny ip 172.26.26.1 any
```

The ACL name indicates the source, IDS, the interface/direction, e0/1_in, and a unique identifier, 1. The ACL is applied to the appropriate interface in the specified direction. For example:

```
interface Ethernet0/1
  ip access-group IDS_e0/1_in_1 in
```

ACL Considerations

This section describes the considerations you should make before applying access control lists (ACLs).



Where to Apply ACLs

Cisco.com

- **When the Sensor has full control, no manually entered ACLs are allowed.**
- **Apply an external interface in an inbound direction.**
- **Apply an internal interface in an outbound direction.**

CSIDS 4.0—15-12

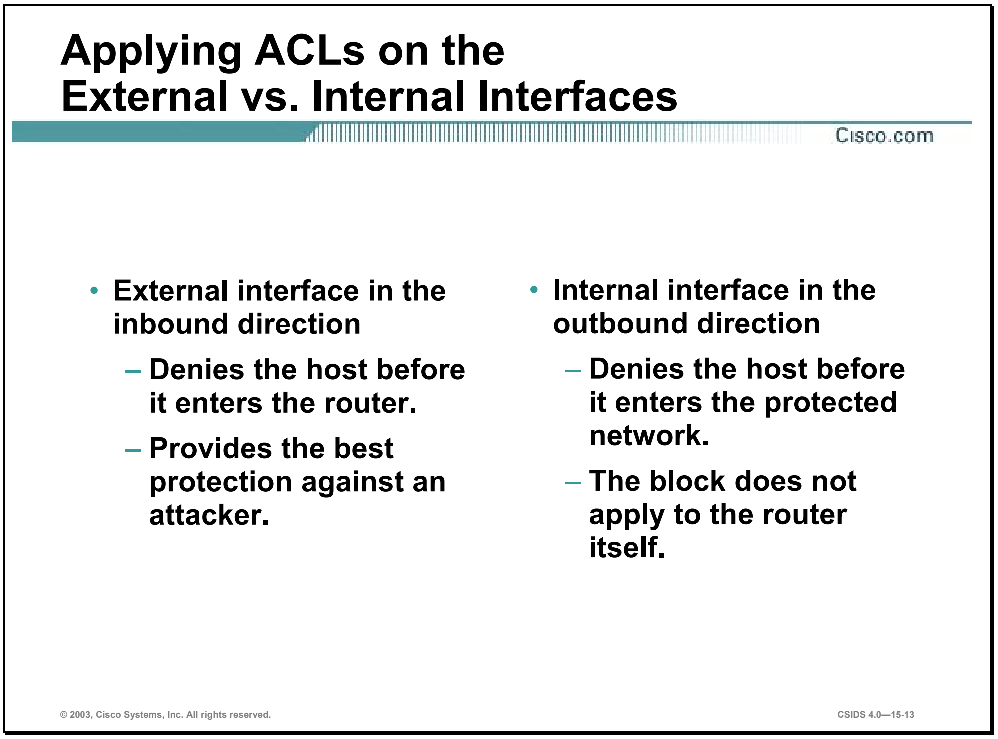
The Sensor must have full control of the assigned interface ACL. The Sensor writes ACLs and applies it to the Cisco device until the device is no longer defined as a blocking device.

Manually configured ACLs are not allowed on this interface, but may be applied to other interfaces or incorporated into the dynamically created ACL. More information about using existing ACLs is discussed later in this section.

You must decide which interface and in what direction to apply the ACL. The ACL may be applied on either the external or internal interface of the router. It can also be configured for inbound or outbound traffic on these interfaces.

When selecting an external interface as the managed interface, the recommended ACL direction is inbound. When selecting an internal interface as the managed interface, the recommended ACL direction is outbound. Either of these strategies will block attacks in the direction of the protected network.

Note Sensor blocking ACLs are incompatible with Context-Based Access Control (CBAC), a component of the IOS Firewall feature set.



Applying ACLs on the External vs. Internal Interfaces

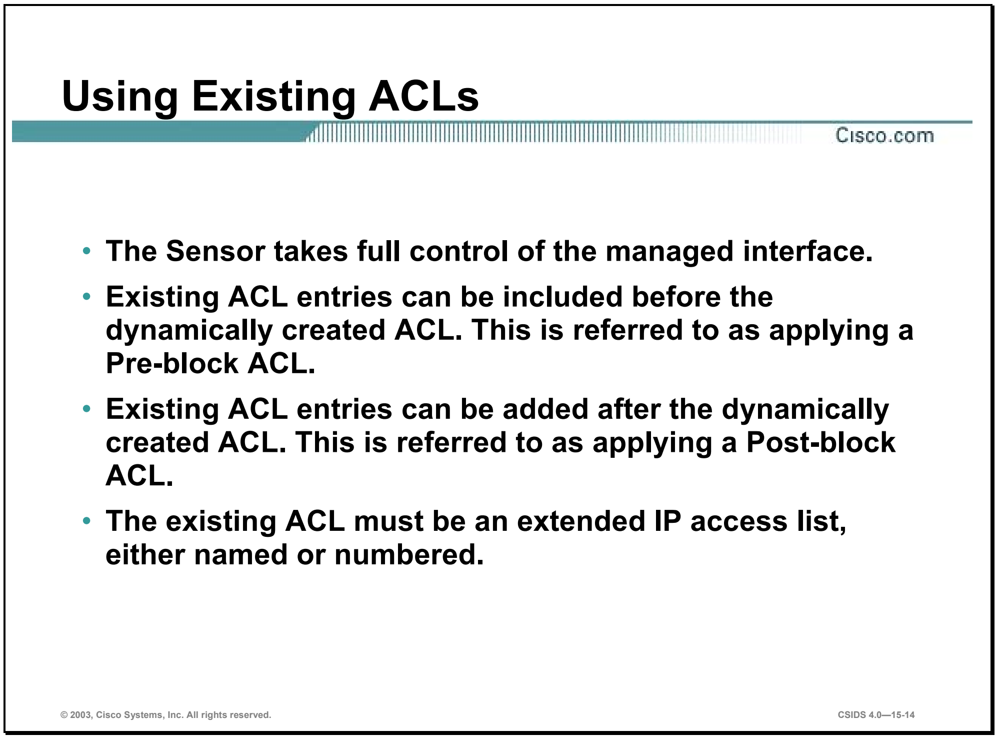
Cisco.com

- External interface in the inbound direction
  - Denies the host before it enters the router.
  - Provides the best protection against an attacker.
- Internal interface in the outbound direction
  - Denies the host before it enters the protected network.
  - The block does not apply to the router itself.

CSIDS 4.0—15-13

Applying the ACL to the external interface in the inbound direction denies a host access before the router processes packets. Applying the ACL to the internal interface in the outbound direction denies a host access to the protected network, but allows packets to be processed by the router. This scenario is less desirable, but may be required if an existing ACL is already applied to an external interface.

Based on your unique network architecture and security policy, you must decide which configuration will meet your needs for security and functionality.



Using Existing ACLs

Cisco.com

- The Sensor takes full control of the managed interface.
- Existing ACL entries can be included before the dynamically created ACL. This is referred to as applying a Pre-block ACL.
- Existing ACL entries can be added after the dynamically created ACL. This is referred to as applying a Post-block ACL.
- The existing ACL must be an extended IP access list, either named or numbered.

CSIDS 4.0—15-14

If you want to change the ACL generated by the Sensor, you can specify either Pre-block or Post-block ACLs. The Pre-block ACL designates ACL entries that the Sensor should place in the beginning of the new ACL, before the addition of any Sensor blocking, deny, entries for the addresses and, or connections being blocked. The Post-block ACL designates ACL entries that the Sensor should place after the Sensor blocking entries.

The Sensor includes an option to never block its IP address as a result of the blocking rules. If selected, then a permit entry is inserted at the beginning of the Sensor-generated ACL to prevent the Sensor IP address from being blocked. .

Note A Pre-block and Post- block ACL must be an extended IP ACL, named or unnumbered. They should be configured on the device before Sensor blocking is configured for that interface/direction.

When working with ACLs, keep in mind that if you do not use Pre-block or Post-block ACLs, you should migrate all existing ACLs for managed interfaces to another non-managed interface that provides access points before a Sensor can manage the device. The simplest alternative to migration is to specify the existing user-defined ACL on the blocking interface as the Post-block ACL.

This section provides a blocking ACL example. The following examples depict portions of a blocking configuration for an IOS router that implements Pre-block and Post-block ACLs on interface Serial0/0 for the inbound direction. The predefined Pre-block ACL is named pre-ACL and the predefined Post-block ACL is named post-ACL:

```
ip access-list extended pre-ACL
  deny   ip any host 172.16.16.200
  deny   tcp any host 192.168.2.2 eq ftp
```

```
!
ip access-list extended post-ACL
  permit tcp any any
```

The following example displays the ACL configuration before blocking is initiated, or after the blocking duration has expired on a Cisco router:

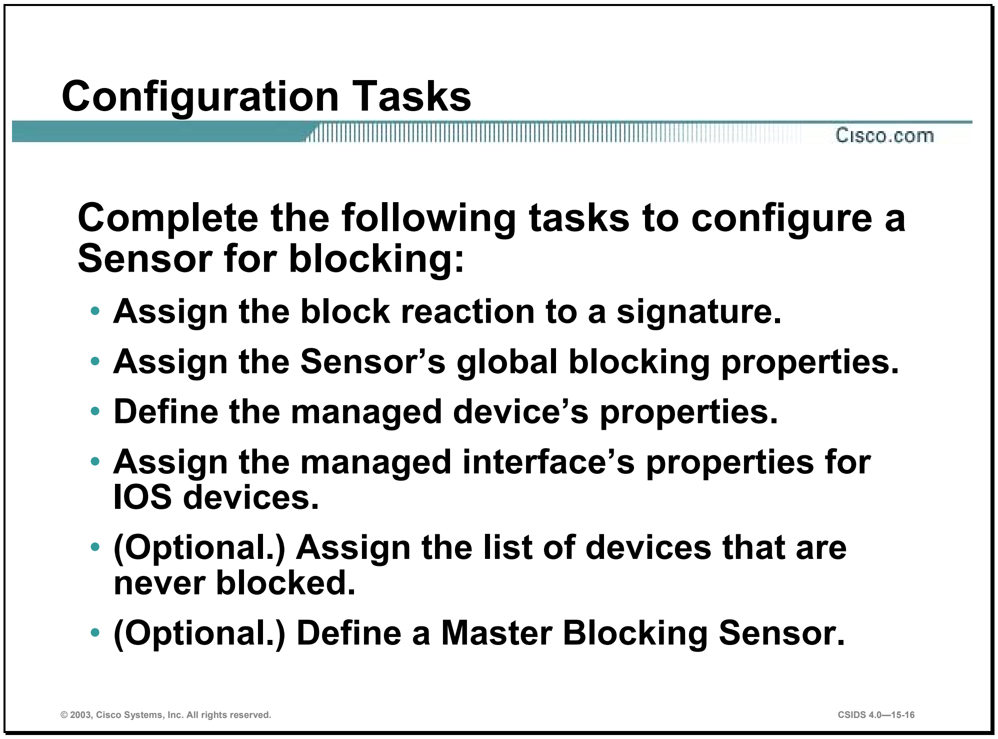
```
!
interface Serial0/0
  ip access-group IDS_Serial0/0_in_1 in       # ACL is applied to the interface in
!                                             the designated direction
ip access-list extended IDS_Serial0/0_in_1
  permit ip host 172.16.16.110 any            # Never block Sensor entry
  deny   ip any host 172.16.16.200            # Pre-block ACL entry
  deny   tcp any host 198.168.2.2 eq ftp      # Pre-block ACL entry
  permit tcp any any                          # Post-block ACL entry
```

The following example displays the ACL configuration while an active block is in progress on an IOS router. In this example, a signature was set to trigger a connection block for attacks to the Web server:

```
!
interface Serial0/0
  ip access-group IDS_Serial0/0_in_1 in        # ACL is applied to the interface in
!                                              the designated direction
ip access-list extended IDS_Serial0/0_in_1
  permit ip host 172.16.16.110 any             # Never block Sensor entry
  deny   ip any host 172.16.16.200             # Pre-block ACL entry
  deny   tcp host 200.2.2.2 any eq ftp         # Pre-block ACL entry
  deny   tcp host 10.1.1.200 host 172.16.16.100  # Blocking ACL entry with logging
          eq www log                           enabled
  permit tcp any any                           # Post-block ACL entry
```

Blocking Sensor Configuration

This section covers how to configure a Sensor to perform blocking.



Configuration Tasks

Complete the following tasks to configure a Sensor for blocking:

- **Assign the block reaction to a signature.**
- **Assign the Sensor's global blocking properties.**
- **Define the managed device's properties.**
- **Assign the managed interface's properties for IOS devices.**
- **(Optional.) Assign the list of devices that are never blocked.**
- **(Optional.) Define a Master Blocking Sensor.**

CSIDS 4.0—15-16

The following are the configuration tasks to configure a Sensor for blocking:

- Assign the block reaction to a selected signature—This task involves using the IDS MC or IDM to configure a signature's action to block.

- Assign the Sensor's global blocking properties—This task involves enabling blocking and defining blocking parameters such as the block duration, maximum blocking entries, and whether or not to allow the Sensor IP address to be blocked.

- Define the managed devices' properties—This task involves defining the blocking devices properties such as device type, IP address, username, password and communication method.

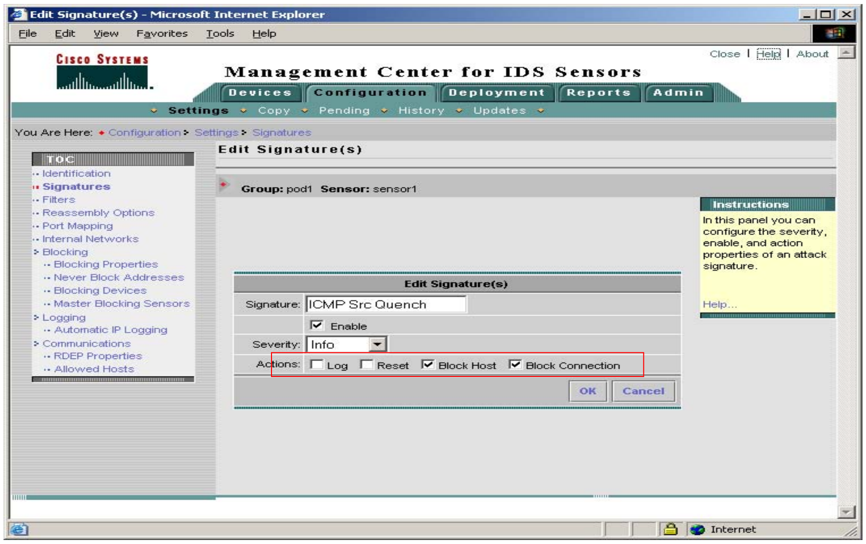
- Assign the managed interface's properties for IOS devices—This task involves selecting the blocking interface or VLAN and assign the Pre-block and Post-block ACLs or VACLs.

- (Optional.) Assign the list of devices that are never blocked—This task involves adding the networks and hosts that the Sensor will never add to the active ACL.

- (Optional.) Define a Master Blocking Sensor—This task involves adding the Sensor that will perform the blocking function for other blocking devices.

Assign Block Reaction

Cisco.com



Edit Signature(s)

Group: pod1 **Sensor:** sensor1

In this panel you can configure the severity, enable, and action properties of an attack signature.

Edit Signature(s)

Signature: ICMP Src Quench

☑ Enable

Severity: Info

Actions: □ Log □ Reset ☑ Block Host ☑ Block Connection

CSIDS 4.0—15-17

The first step to configure blocking is to select a signature and set its alarm response to block the offending host or connection. Choosing to block a host will result in all packets with the source address of the suspected intruder to be blocked. Choosing to block a connection will result in only those packets associated with the offending protocol from the offending source to its target to be blocked.

Complete the following steps to configure a signature action to block:

Step 1 Open and launch the IDS MC and select the blocking Sensor from the Object Selector.

Step 2 Choose **Configuration>Settings>Signatures**. The Signatures page is displayed.

Step 3 Click the **General Group Name** or select a group to which the signature belongs. The Signature(s) in Group page is displayed.

Step 4 Locate the desired signature and click its name. The Edit Signature(s) page is displayed.

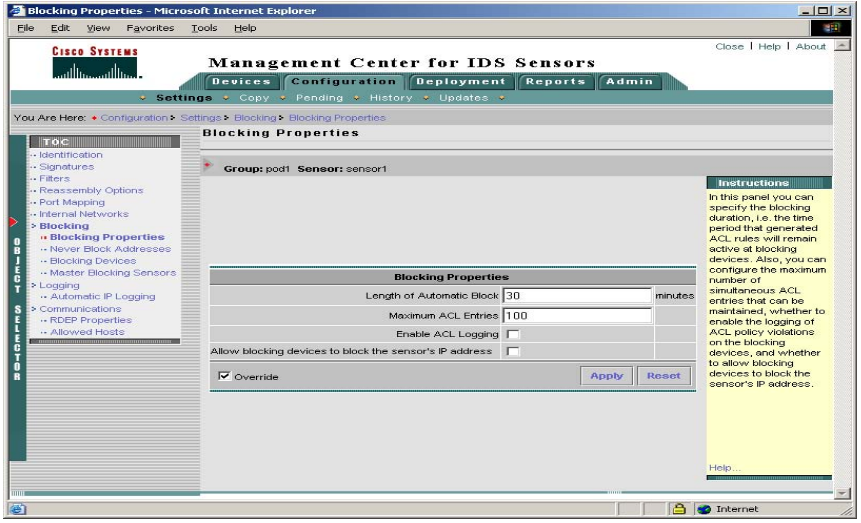
Step 5 Select the **Block Host or Block Connection** check box.

Step 6 Click **OK**. The Signature(s) in Group page is displayed.

Sensor's Blocking Properties

Cisco.com

Choose Configuration>Settings>Blocking>Blocking Properties.



Blocking Properties

Group: pod1 **Sensor:** sensor1

Blocking Properties

Length of Automatic Block 30 minutes

Maximum ACL Entries 100

Enable ACL Logging □

Allow blocking devices to block the sensor's IP address □

☑ Override

Instructions

In this panel you can specify the blocking duration, i.e. the time period that generated ACL rules will remain active at blocking devices. Also, you can configure the maximum number of simultaneous ACL entries that can be maintained, whether to enable the logging of ACL policy violations on the blocking devices, and whether to allow blocking devices to block the sensor's IP address.

Complete the following steps to configure the Sensor's global blocking properties:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Choose **Blocking>Blocking Properties** from the TOC. The Blocking Properties page is displayed.

Step 3 Enter the length that an automatic block will occur in the Length of Automatic Block field. The default length of time is 30 minutes.

Step 4 Enter the maximum number of ACL entries the Sensor will manage in the Maximum ACL Entries field. The default number of entries is 100.

Step 5 Select the **Enable ACL Logging** check box if you want the router to locally log ACL entries.

Step 6 Select the **Allow blocking devices to block the sensor's IP address** check box if you want to possibly have the Sensor's IP address blocked. Select this option only if you think there is a likely possibility that the Sensor device may be compromised and IP spoofing is unlikely. If selected, then it is possible that communications from the Sensor will be blocked, thus losing remote management, and monitoring capabilities. If not selected, which is the default, a permit entry for the Sensor IP address is inserted at the start of the blocking ACL to prevent blocking of the Sensor IP address.

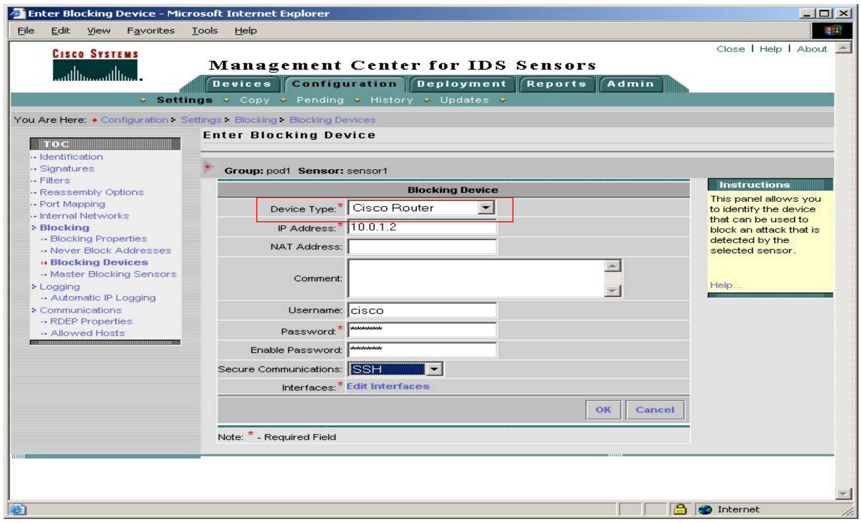
Note If you are configuring Group settings, you may specify that these settings are mandatory by selecting the Mandatory check box. If you do not want the settings to be mandatory, configure the settings and you may override these settings on a sub-group or device basis by using the Override check box.

Step 7 Click **Apply**. The Blocking Properties page is refreshed to indicate that the IDS MC received the changes.

Managed Device—Cisco Router

Cisco.com

Choose Configuration>Blocking>Blocking Devices and **select** Add**.**



You Are Here: Configuration > Settings > Blocking > Blocking Devices

Enter Blocking Device

Group: pod1 **Sensor:** sensor1

Blocking Device

Device Type:* Cisco Router

IP Address:* 10.0.1.2

NAT Address:

Comment:

Username: cisco

Password:* *******

Enable Password: *******

Secure Communications: SSH

Interfaces:* Edit Interfaces

Note: * - Required Field

Instructions

This panel allows you to identify the device that can be used to block an attack that is detected by the selected sensor.

CSIDS 4.0—15-19

The Cisco router Device Type allows you to select a blocking device type: Cisco IOS routers, Catalyst 5000 Series switches with an RSM or RSFC, and Catalyst 6000 Series switches running native IOS with an MSFC. Complete the following steps to add a Cisco Router as a blocking device:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Choose **Blocking>Blocking Devices** from the TOC. The Blocking Devices page is displayed.

Step 3 Click **Add**. The Enter Blocking Devices page is displayed.

Step 4 Enter values for the IDS MC Blocking Device settings listed in the following table:

IDS MC Blocking Device Settings	Description
Device Type	Drop-down menu that allows you to select a blocking device type
IP Address	IP address of the blocking device—Cisco router
NAT Address	NAT IP address of the blocking device—Cisco router
Comment	Optional
Username	User name that has permissions to log in and perform administration, configuration, or management functions, if the blocking device is configured for user authentication.
Password	Console level access password
Enable Password	Password that enables the logged in user to perform administration, configuration or management functions
Secure Communications	Drop-down menu that allows you to select a mode of communication between the Sensor and the blocking device. The default is None. The None option implies Telnet, which is not considered a secured communication method. The following options are available: None, SSH, or SSH-3DES.

Step 5 Click **Edit Interfaces**. The Enter Blocking Devices Interfaces page is displayed.

Step 6 Click **Add**. The Enter Blocking Device Interface page is displayed.

If SSH DES or 3DES is selected as the secure communication method, SSH password authentication will be used, not public key authentication. Also, the IOS device must have a software license that supports DES or 3DES encryption depending on the SSH option selected.

To configure the Sensor to communicate with a router blocking device using SSH, you must manually configure the SSH public key of the router to the Sensor using the **ssh host-key** ip_address command, where ip_address = the IP address of the router. The Sensor automatically retrieves the SSH parameters from the router, if properly configured for an SSH server.

The following displays a partial sample configuration for a Cisco router that supports SSH authentication from the Sensor using the local database for password authentication:

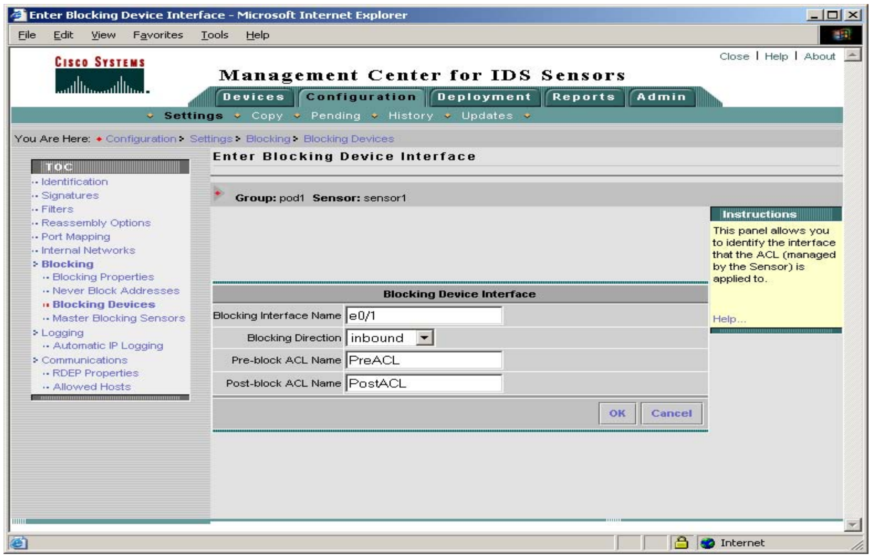
```
!
hostname router1                                 # Establish identity
!
username sensor password 0 secret                # Sensor username account for SSH
                                                 login
!
aaa new-model
aaa authentication login ssh local enable        # Define aaa profile “ssh” for local
                                                 user database authentication; enable
                                                 password as backup
!
ip domain-name company.com                       # Establish identity
ip ssh time-out 90                               # Optional (Default=60)
ip ssh authentication-retries 2                  # Optional (Default=3)
!
line vty 0 4
  login authentication ssh                       # Authenticate vty lines using aaa
                                                 profile “ssh”
  transport input ssh                            # Enable the ssh transport on the vty
                                                 line
!
```

The IOS command **crypto key generate rsa** does not appear in the static configuration, but is used to enable the SSH server and generates the server public and private keys for SSH authentication.

The IOS commands **show users** and **show ssh** can be used to verify that the Sensor has logged into the Cisco router and established an SSH connection; the encryption level is also displayed.

Managed Device—Cisco Router (cont.)

Cisco.com



You Are Here: Configuration > Settings > Blocking > Blocking Devices

Enter Blocking Device Interface

Group: pod1 **Sensor:** sensor1

This panel allows you to identify the interface that the ACL (managed by the Sensor) is applied to.

Blocking Device Interface

Blocking Interface Name: e0/1

Blocking Direction: inbound

Pre-block ACL Name: PreACL

Post-block ACL Name: PostACL

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—15-20

Step 7 Enter values for the IDS MC Blocking Device Interface settings listed in the following table:

IDS MC Blocking Device Interface Settings	Description
Blocking Interface Name	Allows you to enter the name of the interface that will perform the blocking
Blocking Direction	Drop-down menu that allows you to select the direction blocking will occur. The following options are available: inbound and outbound.
Pre-block ACL Name	Name of the ACL that includes entries to insert prior to blocking ACL entries
Post-block ACL Name	Name of the ACL that includes entries to append after the blocking ACL entries

Step 8 Click **OK**. The Enter Blocking Interfaces page is displayed.

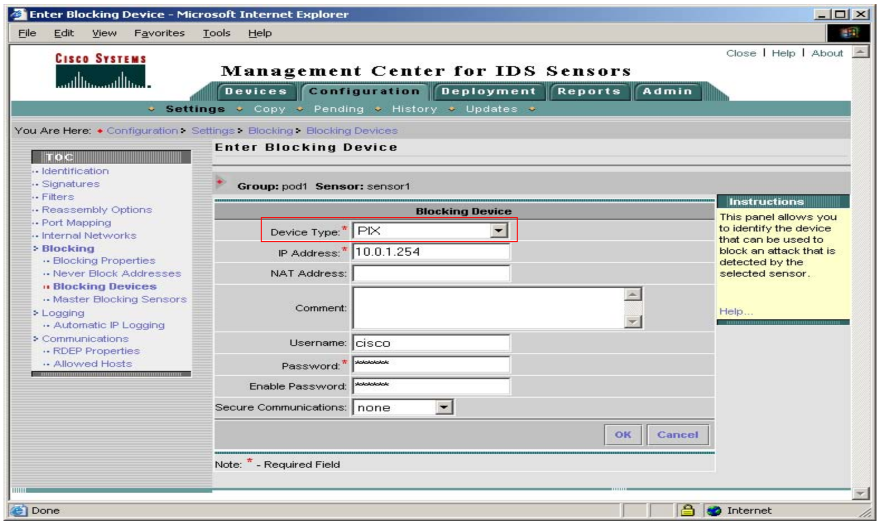
Step 9 Click **OK**. The Enter Blocking Device page is displayed.

Step 10 Click **OK**. The Blocking Device page is displayed.

Managed Device—PIX Firewall

Cisco.com

Choose Configuration>Blocking>Blocking Devices and **select** Add.



You Are Here: Configuration > Settings > Blocking > Blocking Devices

Enter Blocking Device

Group: pod1 **Sensor:** sensor1

Blocking Device

Device Type:* PIX

IP Address:* 10.0.1.254

NAT Address:

Comment:

Username: cisco

Password:* *******

Enable Password: *******

Secure Communications: none

Note: * - Required Field

Instructions

This panel allows you to identify the device that can be used to block an attack that is detected by the selected sensor.

CSIDS 4.0—15-21

PIX Firewall interfaces and ACLs do not need to be configured when the PIX Firewall is defined as a blocking device. Blocking is enforced using the PIX Firewall **shun** command. The **shun** command is limited to blocking hosts and host connections; it does not support the manual blocking of entire networks or sub-networks. The **shun** command is available in PIX software versions 6.0 and later.

Complete the following steps to add a PIX Firewall as a blocking device:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Choose **Blocking>Blocking Devices** from the TOC. The Blocking Devices page is displayed.

Step 3 Click **Add**. The Enter Blocking Devices page is displayed.

Step 4 Enter values for the IDS MC Blocking Device settings listed in the following table:

IDS MC Blocking Device Settings	Description
Device Type	Drop-down menu that allows you to select a blocking device type
IP Address	IP address of the blocking device—PIX Firewall
NAT Address	NAT IP address of the blocking device—PIX Firewall
Comment	Optional
Username	User name that has permissions to log in and perform administration, configuration, or management functions, if the blocking device is configured for user authentication. If you are using SSH and local authentication, the username is “pix”.
Password	Console level access password
Enable Password	Password that enables the logged in user to perform administration, configuration or management functions

IDS MC Blocking Device Settings	Description
Secure Communications	Drop-down menu that allows you to select a mode of communication between the Sensor and the blocking device. The default is None. The following options are available: None, SSH, or SSH-3DES.

If SSH DES or 3DES is selected as the secure communication method, the SSH password authentication will be used, not public key authentication. Also, the PIX Firewall must have a software license that supports DES or 3DES encryption depending on the SSH option selected. Use the PIX **show version** command to verify the encryption license.

To configure the Sensor to communicate with a PIX Firewall blocking device using SSH, you must manually add the PIX Firewall SSH public key to the Sensor using the **ssh host-key** ip_address command, where ip_address = the PIX IP address. The Sensor automatically retrieves the SSH parameters from the PIX Firewall, if properly configured for the SSH server.

The following displays a partial sample configuration for a PIX Firewall that supports SSH authentication from the Sensor using local password authentication, not AAA:

```
passwd secret                               # Define SSH local password
hostname pix1                               # Establish identity for key
                                            generation
domain-name company.com                     # Establish identity for key
                                            generation
ssh 172.16.1.1 255.255.255.255 inside       # Allows SSH only from host
                                            172.16.1.1 on inside network
ssh timeout 60                              # Optional
```

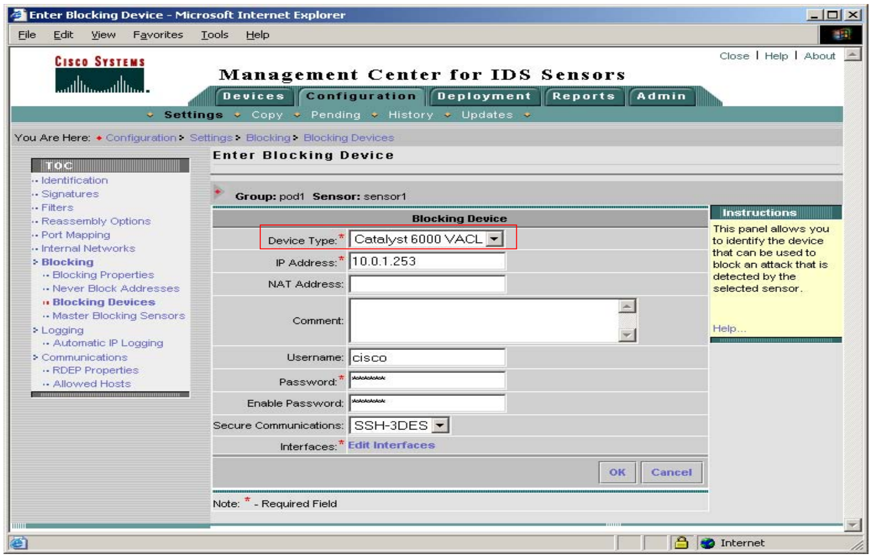
Once the hostname and domain name of the PIX Firewall are set, the **PIX ca generate rsa key** command is used to generate the server public and private keys for SSH authentication; the **ca save all** command is then used to save the RSA key pair to Flash memory.

The PIX Firewall **show ssh sessions** command can be used to verify that the Sensor has logged into the PIX Firewall and established an SSH connection. The encryption level is also displayed.

Note If local authentication, not AAA, is used for SSH on the PIX Firewall, then the SSH username is always “pix”. There is no per-user name entry.

Managed Device—Catalyst 6000 VACL

Cisco.com



You Are Here: Configuration > Settings > Blocking > Blocking Devices

Enter Blocking Device

Group: pod1 Sensor: sensor1

Blocking Device

Device Type:* Catalyst 6000 VACL

IP Address:* 10.0.1.253

NAT Address:

Comment:

Username: cisco

Password:* *******

Enable Password: *******

Secure Communications: SSH-3DES

Interfaces:* Edit Interfaces

Note: * - Required Field

Instructions

This panel allows you to identify the device that can be used to block an attack that is detected by the selected sensor.

Help...

CSIDS 4.0—15-22

Blocking is configured on a Catalyst 6000 running the Catalyst operating system using VACLs. A blocking device interface is required to complete the configuration of the blocking feature on the Catalyst 6000 using VACLs. Since Catalyst 6000 VACLs do not support direction-based ACLs, the blocking direction is not available for Catalyst 6000 VACL devices.

Complete the following steps to add a Catalyst 6000 device as a blocking device using VACLs:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Select **Blocking>Blocking Devices** from the TOC. The Blocking Devices page is displayed.

Step 3 Click **Add**. The Enter Blocking Devices page is displayed.

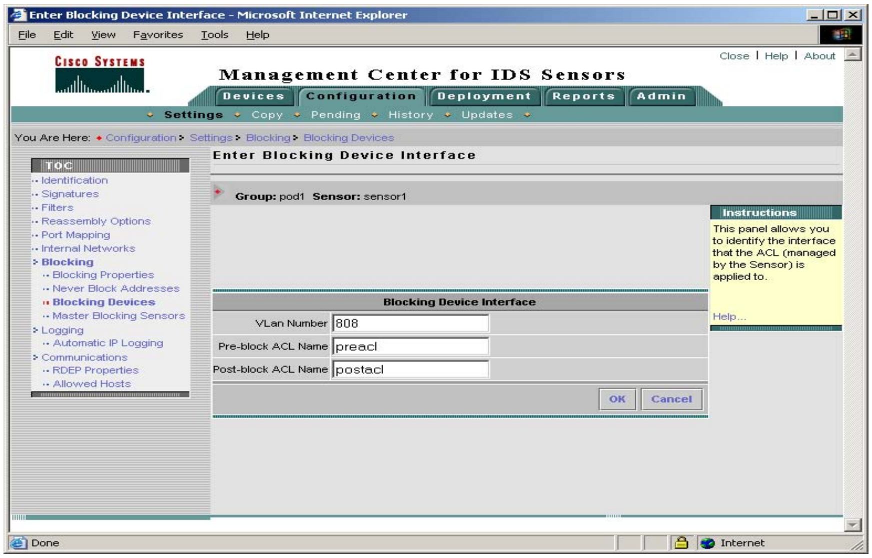
Step 4 Enter values for the IDS MC Blocking Device settings listed in the following table:

IDS MC Blocking Device Settings	Description
Device Type	Drop-down menu that allows you to select a blocking device type
IP Address	IP address of the blocking device—Catalyst 6000 switch
NAT Address	NAT IP address of the blocking device—Catalyst 6000 switch
Comment	Optional
Username	User name that has permissions to log in and perform administration, configuration, or management functions, if the blocking device is configured for user authentication
Password	Console level access password
Enable Password	Password that enables the logged in user to perform administration, configuration or management functions

IDS MC Blocking Device Settings	Description
Secure Communications	Drop-down menu that allows you to select a mode of communication between the Sensor and the blocking device. The default is None, Telnet. The following options are available: None, SSH, or SSH-3DES.

Note If the blocking device is a Catalyst 5000 RSM or RSFC, or a Catalyst 6000 with an MSFC running the native IOS, then the blocking device type is Cisco Router, which uses ACLs instead of VACLs for blocking.

Managed Device— Catalyst 6000 VACL (cont.)



Enter Blocking Device Interface

Group: pod1 **Sensor:** sensor1

This panel allows you to identify the interface that the ACL (managed by the Sensor) is applied to.

Blocking Device Interface

VLan Number 808

Pre-block ACL Name preacl

Post-block ACL Name postacl

CSIDS 4.0—15-23

Step 5 Enter values for the IDS MC Blocking Device Interface settings listed in the following table:

IDS MC Blocking Device Interface Settings	Description
VLAN Number	VLAN number that will be used to initiate blocking
Pre-block ACL Name	Name of the ACL that is used prior to blocking entries
Post-block ACL Name	Name of the ACL that is used after blocking entries

Step 6 Click **OK**. The Enter Blocking Interfaces page is displayed.

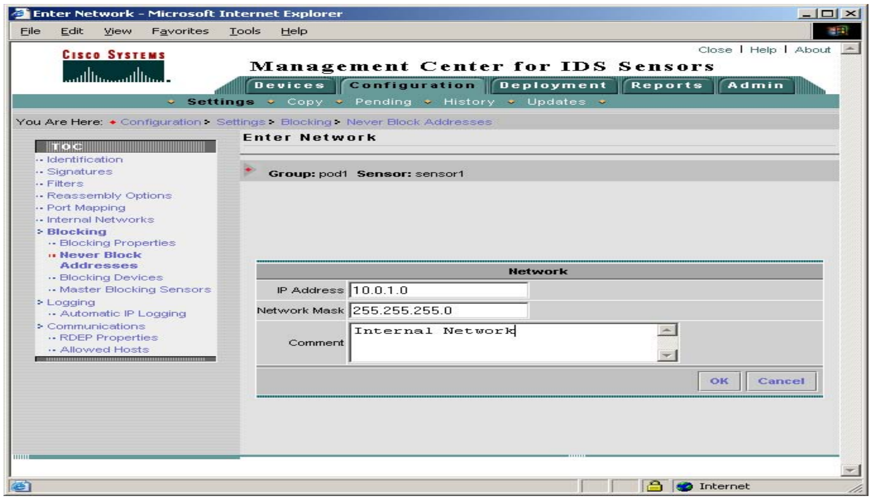
Step 7 Click **OK**. The Enter Blocking Device page is displayed.

Step 8 Click **OK**. The Blocking Device page is displayed.

Never Block Addresses

Cisco.com

Choose Configuration>Settings>Blocking>Never Block Addresses and **click** Add.



Enter Network

Group: pod1 **Sensor:** sensor1

Network

IP Address	10.0.1.0
Network Mask	255.255.255.0
Comment	Internal Network

Cisco IDS enables you to define a list of network addresses of hosts or networks that will never be blocked. These addresses may include critical servers or hosts that, if blocked, would severely impact business operations. If used, take additional cautionary measures to ensure that these hosts cannot be compromised and used as a launching point for additional attacks. The Sensor adds permit statements for these addresses in the ACL. Complete the following steps to add addresses that should never be blocked:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Choose **Blocking>Never Block Addresses** from the TOC. The Never Block Addresses page is displayed.

Step 3 Click **Add**. The Enter Network page is displayed.

Step 4 Enter the IP address of host or network that you wish to not block in the IP Address field.

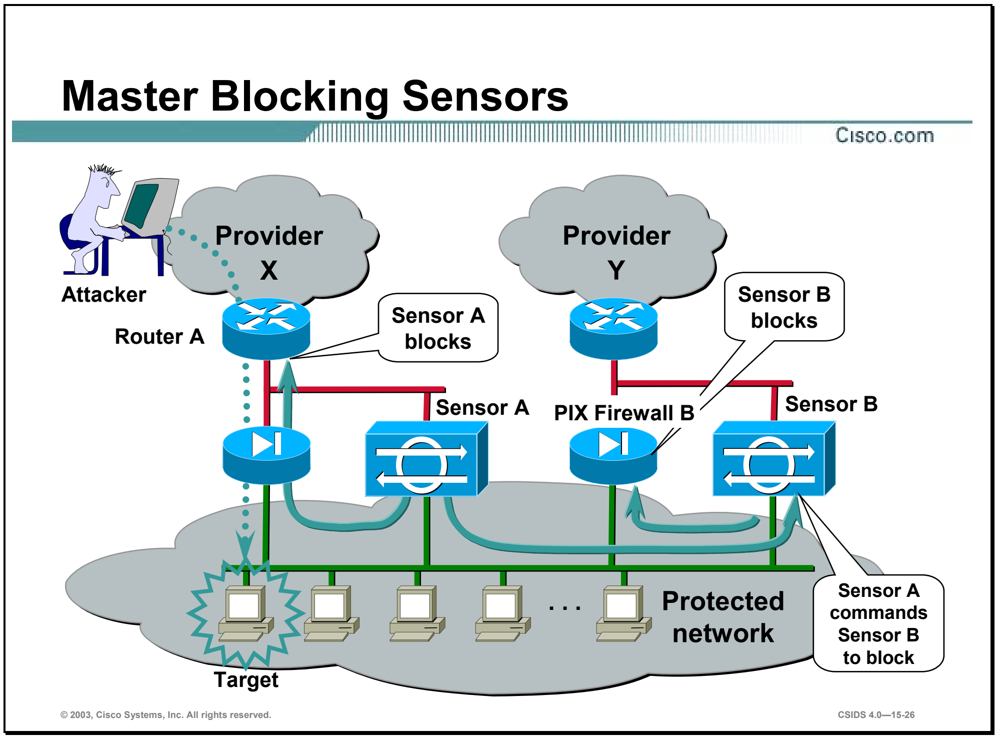
Step 5 Enter the network mask in the Network Mask field.

Step 6 Enter an optional comment in the Comment field.

Step 7 Click **OK**. The Never Block Addresses page is displayed.

Master Blocking Sensor Configuration

This section covers how to configure a Master Blocking Sensor.



Master Blocking Sensors

Cisco.com

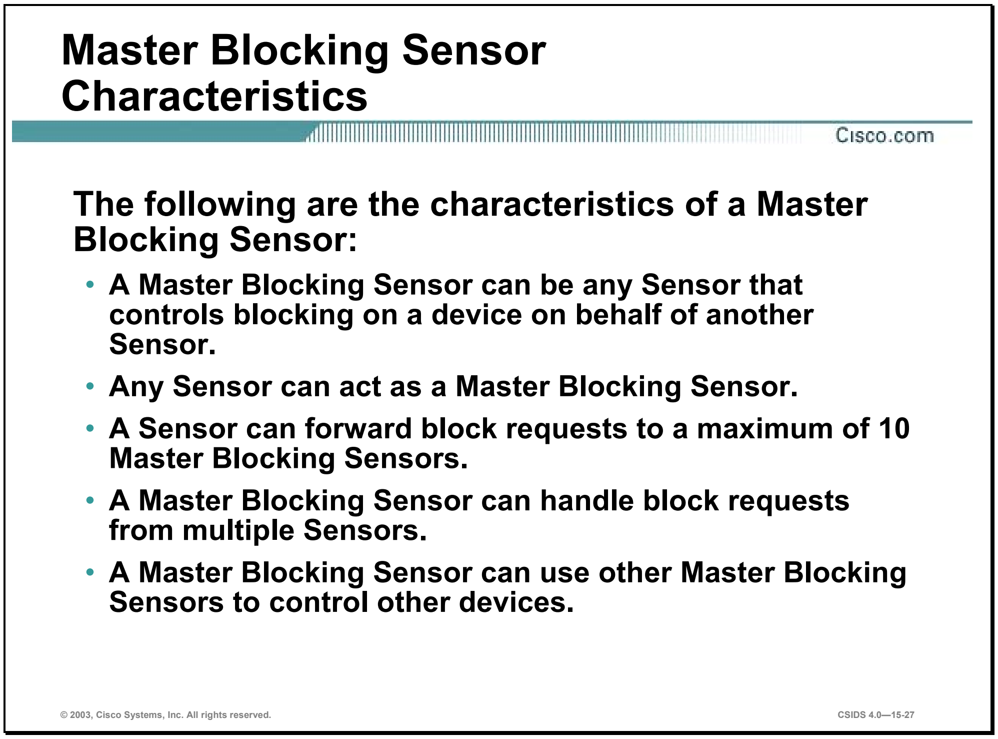
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—15-26

In some configurations it is necessary to have a proxy Sensor perform the blocking action for another Sensor on your network. These proxy Sensors are referred to as Master Blocking Sensors. The Sensors that send block requests to Master Blocking Sensors are referred to as Blocking Forwarding Sensors.

The figure illustrates an example of how to use Master Blocking Sensors. It represents a scenario where a network has two entry points from two different providers: Provider X and Provider Y. The entry point for Provider X has a Sensor configured for device management with Router A. The entry point for Provider Y has a Sensor configured for device management with the PIX Firewall B. When an attempt to penetrate a host in the protected network is detected by Sensor A, Sensor A blocks the attack at Router A. If Sensor A has not been configured to use a Master Blocking Sensor, then the Provider Y access would still be visible and the attacker could penetrate the protected network through that route.

Only one Sensor should directly control blocking on a given device. Therefore, if two Sensors need to initiate blocking to the same device, one Sensor should be designated as the Master Blocking Sensor and the other as the Blocking Forwarding Sensor. This configuration allows one Sensor to control the blocking for both Sensors. The Blocking Forwarding Sensor would not be configured to control blocking for the blocking device, but to communicate its blocks to the Master Blocking Sensor.



Master Blocking Sensor Characteristics

The following are the characteristics of a Master Blocking Sensor:

- **A Master Blocking Sensor can be any Sensor that controls blocking on a device on behalf of another Sensor.**
- **Any Sensor can act as a Master Blocking Sensor.**
- **A Sensor can forward block requests to a maximum of 10 Master Blocking Sensors.**
- **A Master Blocking Sensor can handle block requests from multiple Sensors.**
- **A Master Blocking Sensor can use other Master Blocking Sensors to control other devices.**

CSIDS 4.0—15-27

A Master Blocking Sensor is actually the NAC running on a Sensor that controls blocking on one or more devices on behalf of one or more other Sensors known as Blocking Forwarding Sensors. In other words, the NAC on a Master Blocking Sensor controls blocking on devices at the request of the NACs running on Blocking Forwarding Sensors.

Any IDS version 4.x Sensor can act as a Master Blocking Sensor for another IDS version 4.x Sensor. In IDS 3.x Sensors or earlier, PostOffice is the protocol used to communicate blocking instructions. In IDS version 4.0 Sensors and later, RDEP is used by the Blocking Forwarding Sensor to communicate blocking instructions to a Master Blocking Sensor. The block messages used to communicate from the Blocking Forwarding Sensor NAC to a Master Blocking Sensor are as follows:

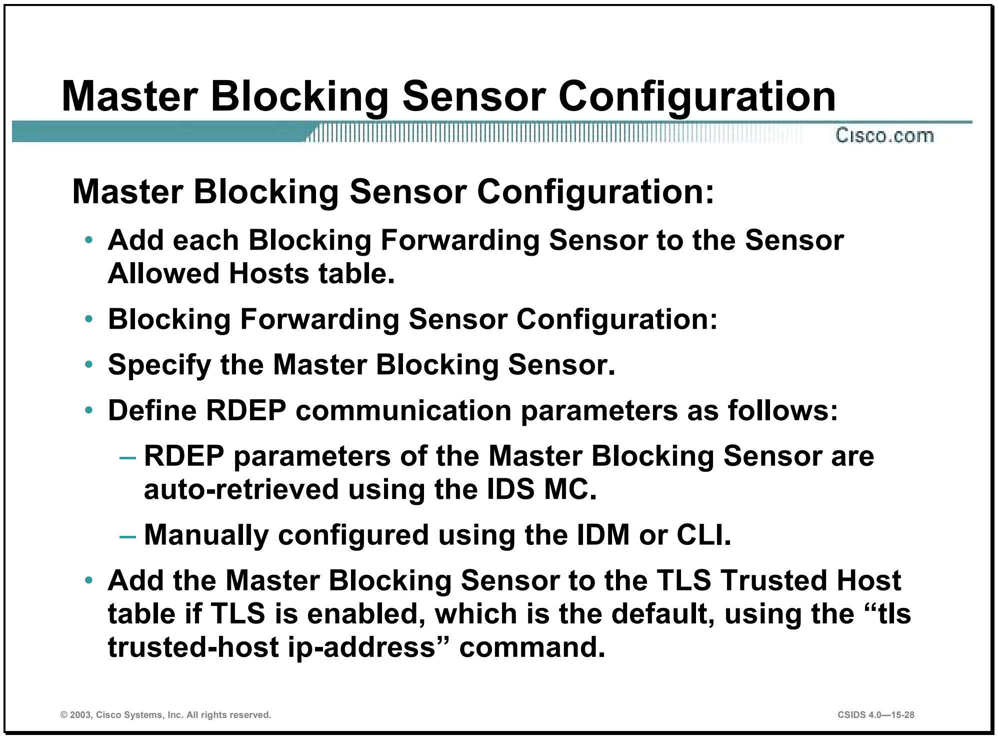
- Initiate a block—Used for manual blocks or blocks initiated in response to an event, automatic blocks
- Stop blocking—Used for manual blocks

Block timeout messages are not communicated because each Sensor handles its own blocking timeouts. Permanent blocks are also not communicated because these can only be configured for devices that a Sensor directly manages.

A Blocking Forwarding Sensor can forward block requests to a maximum of 10 Master Blocking Sensors, and a Master Blocking Sensor can handle block requests from more than one Sensor. The only Sensor blocking limitation is the total number of blocks that can be active regardless of how the blocks were initiated.

A Master Blocking Sensor can also use other Master Blocking Sensors to control other devices. However, this type of blocking configuration can become quite complex, and because Master Blocking Sensors can chain block messages, circular block messaging can occur.

Note When a Master Blocking Sensor chains block messages, the block messages are applied one right after the other. Circular block messaging occurs when chained block messages are in continuance for an extended period of time.



Master Blocking Sensor Configuration

Cisco.com

Master Blocking Sensor Configuration:

- Add each Blocking Forwarding Sensor to the Sensor Allowed Hosts table.
- Blocking Forwarding Sensor Configuration:
- Specify the Master Blocking Sensor.
- Define RDEP communication parameters as follows:
  - RDEP parameters of the Master Blocking Sensor are auto-retrieved using the IDS MC.
  - Manually configured using the IDM or CLI.
- Add the Master Blocking Sensor to the TLS Trusted Host table if TLS is enabled, which is the default, using the “tls trusted-host ip-address” command.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—15-28

On the Master Blocking Sensor, each Blocking Forwarding Sensor must be added to the Master Blocking Sensor allowed host configuration. On each Blocking Forwarding Sensor, identify the remote host that will serve as the Master Blocking Sensor. Also, if TLS is enabled for encrypted RDEP communications, then the Master Blocking Sensor must be added to the Blocking Forwarding Sensor TLS trusted host table.

For a Master Blocking Sensor to support a Master Blocking Sensor configuration, you must add each Blocking Forwarding Sensor IP address to the Sensor Allowed Hosts table.

For a Blocking Forwarding Sensor to support a Master Blocking Sensor configuration, you must complete the following:

- Define the Master Blocking Sensor. To do this, configure the Master Blocking Sensor IP address, SSL port, TLS setting, username, and password. Using the IDS MC, these parameters are automatically retrieved from the device database when the Sensor is selected from the device list. Using the IDM or CLI, these parameters are manually configured.

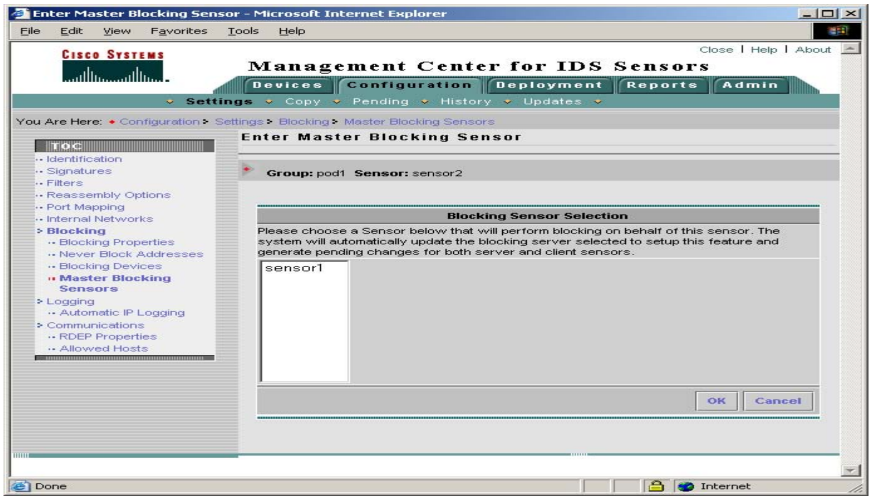
- If TLS is enabled, which is the default setting, configure the Master Blocking Sensor as a TLS trusted host using the Sensor **tls trusted-host ip-address** ip_address command, where ip_address = the Master Blocking Sensor IP address.

Note A Sensor that is configured for SSH authentication using pre-existing keys cannot currently be configured as a Master Blocking Sensor using the IDS MC. The IDS MC auto-retrieves the device credentials from the device database and assumes password authentication for device access, not public key authentication.

Configuring Master Blocking Sensors

Cisco.com

Choose Configuration>Settings>Blocking>Master Blocking Sensors and **click** Add**.**



Enter Master Blocking Sensor

Group: pod1 **Sensor:** sensor2

Blocking Sensor Selection

Please choose a Sensor below that will perform blocking on behalf of this sensor. The system will automatically update the blocking server selected to setup this feature and generate pending changes for both server and client sensors.

sensor1

CSIDS 4.0—15-29

Complete the following steps in the IDS MC on a Blocking Forwarding Sensor to add the Sensor IP addresses that will act as Master Blocking Sensors:

Step 1 From the Object Selector, select the Sensor that will forward block requests to a Master Blocking Sensor.

Step 2 Choose **Configuration>Settings**. The Settings page is displayed.

Step 3 Choose **Blocking>Master Blocking Sensors** from the TOC. The Master Blocking Sensors page is displayed.

Step 4 Click **Add**. The Enter Master Blocking Sensor page is displayed.

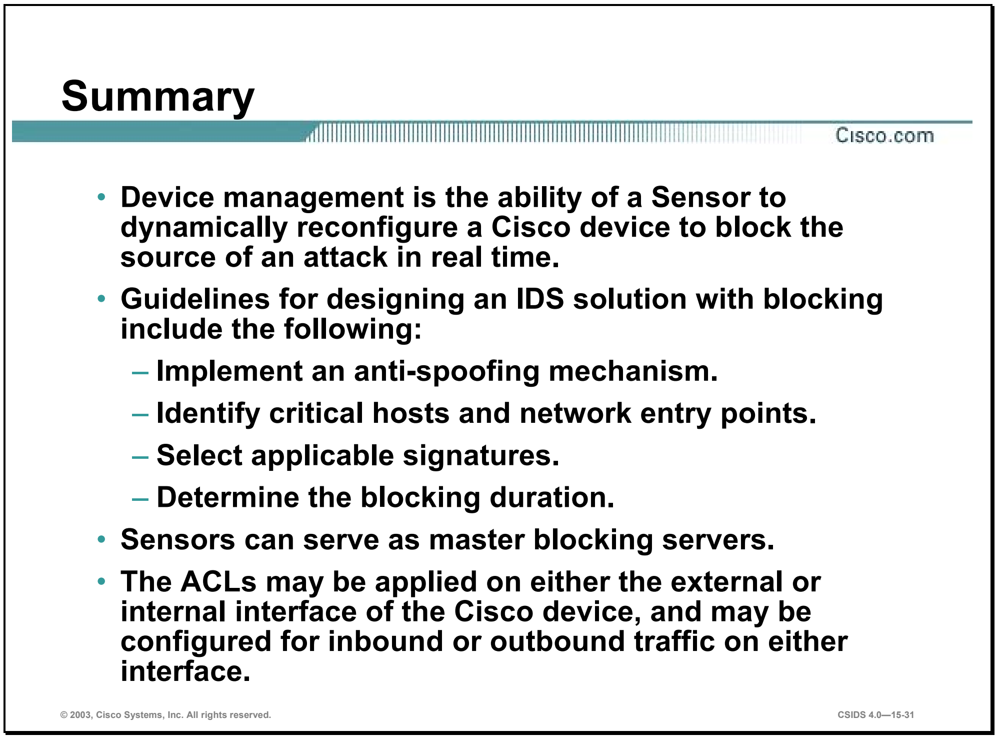
Note Only an IDS 4.0 Sensor can be a Master Blocking Sensor for another IDS 4.0 Sensor. If you have other IDS 4.0 Sensors defined within the IDS MC and they do not appear, it may be necessary to commit pending changes to the IDS MC.

Step 5 Select the Master Blocking Sensor from the list of Sensors and click **OK**. The Master Blocking Sensors page is displayed.

Note The IDS MC automatically updates the blocking server selected to setup this feature and generate pending changes for both server and client Sensors.

Summary

This section summarizes what you learned in this chapter.



Summary

- Device management is the ability of a Sensor to dynamically reconfigure a Cisco device to block the source of an attack in real time.
- Guidelines for designing an IDS solution with blocking include the following:
  - Implement an anti-spoofing mechanism.
  - Identify critical hosts and network entry points.
  - Select applicable signatures.
  - Determine the blocking duration.
- Sensors can serve as master blocking servers.
- The ACLs may be applied on either the external or internal interface of the Cisco device, and may be configured for inbound or outbound traffic on either interface.

CSIDS 4.0—15-31

Lab Exercise—Blocking Configuration

Complete the following lab exercise to practice what you learned in this chapter.

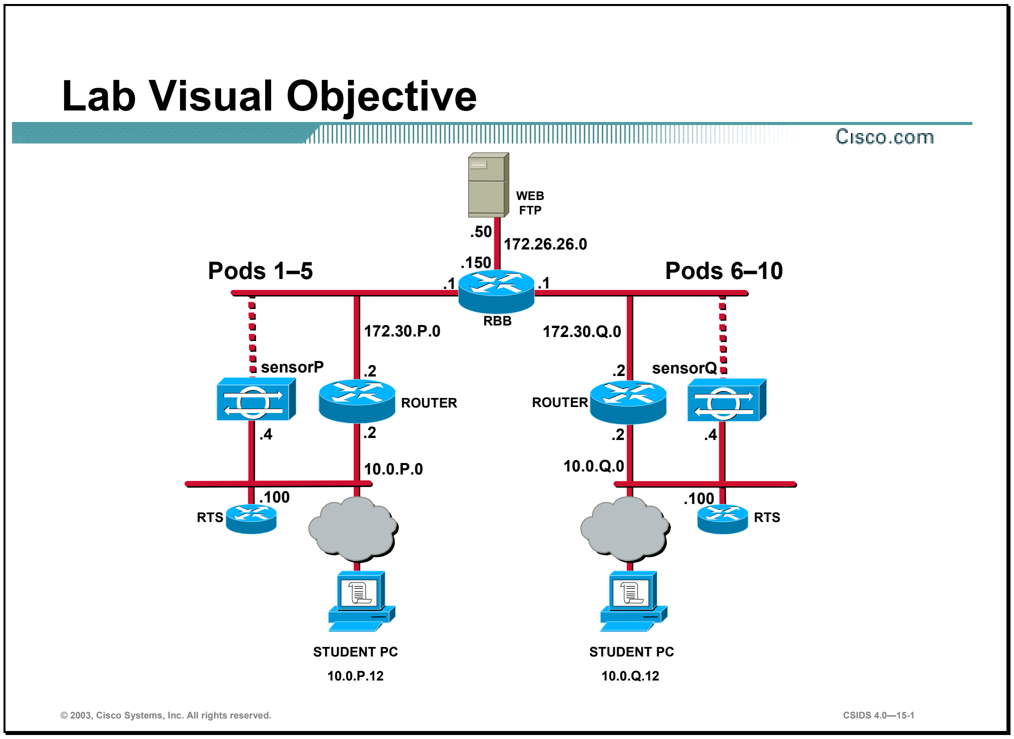
Objectives

In this lab exercise you will complete the following tasks:

- Configure blocking properties.
- Edit a signature to block a host.
- Configure never block addresses.
- Configure blocking devices.
- Deploy the Sensor configuration.
- Create a deployment report.
- Test the blocking configuration.
- Remove the blocking configuration.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab exercise.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor. Make sure to replace it with your peer's pod number.

Task 1—Configure Blocking Properties

Complete the following steps to configure blocking properties for IDS 4.0 Sensors:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Use the Object Selector to choose **sensorP**. The Settings page is refreshed and indicates you are configuring sensorP.

(where P = pod number)

Step 3 Select **Blocking>Blocking Properties**. The Blocking Properties page is displayed.

Step 4 Verify that the **Override** check box is selected.

Step 5 Enter **3** in the Length of Automatic Block field.

Step 6 Enter **50** in the Maximum ACL Entries field.

Step 7 Select the **Enable ACL Logging** check box.

Step 8 Click **Apply**. The Blocking Properties page refreshes and indicates that the IDS MC received the changes.

Task 2—Edit a Signature to Block a Host

Complete the following steps to edit a signature to block a host:

Step 1 Select **Signatures** from the TOC. The Signatures page is displayed.

Step 2 Click the **General** Group Name. The Signature(s) in Group page is displayed.

Step 3 Enter **2004** in the field to the left of the Filter button, and click **Filter**. Signature 2004 is displayed in the Signature(s) in Group page.

Step 4 Select the **Signature 2004** check box and click **Edit**. The Edit Signature(s) page is displayed.

Step 5 Select the **Block Host** check box.

Step 6 Click **OK**. The Signature(s) in Group page is refreshed and displays the actions you configured.

Task 3—Configure Never Block Addresses

Complete the following steps to configure addresses to never block:

Step 1 Select **Blocking>Never Block Addresses** from the TOC. The Never Block Addresses page is displayed.

Step 2 Click **Add**. The Enter Network page is displayed.

Step 3 Enter **10.0.P. 0** in the IP Address field.

(where P = pod number)

Step 4 Enter **255.255.255.0** in the Network Mask field.

Step 5 Click **OK**. The Never Block Addresses page is displayed.

Task 4—Configure Blocking Devices

Complete the following steps to configure a router as a blocking device:

Step 1 Select **Blocking>Blocking Devices** from the TOC. The Blocking Devices page is displayed.

Step 2 Click **Add**. The Enter Blocking Device page is displayed.

Step 3 Select **Cisco Router** from the Device Type drop-down menu.

Step 4 Enter **10.0.P.2** in the IP Address field.

(where P = pod number)

Step 5 Enter **Internet Router** in the Comment field.

Step 6 Enter **cisco** in the Password field.

Step 7 Enter **cisco** in the Enable Password field.

Step 8 Verify that **none** is selected from the Secure Communications drop-down menu by default.

Step 9 Click **Edit Interfaces**. The Enter Blocking Device Interfaces page is displayed.

Step 10 Click **Add**. The Enter Blocking Device Interface page is displayed.

Step 11 Enter **Ethernet0/1** in the Blocking Interface Name field.

Step 12 Verify that **inbound** is selected from the Blocking Direction drop-down menu by default.

Step 13 Enter **preblock** in the Pre-block ACL Name field.

Step 14 Enter **postblock** in the Post-block ACL Name field.

Step 15 Click **OK**. The Enter Blocking Device Interfaces page is displayed.

Step 16 Click **OK**. The Enter Blocking Device page is displayed.

Step 17 Click **OK**. The Blocking Devices page is displayed.

Task 5—Deploy the Sensor Configuration

Complete the following steps to deploy the configuration to the Sensor:

Step 1 Choose **Configuration>Pending**. The Pending page is displayed.

Step 2 Select the check box located next to the pending configuration and click **Save**.

Step 3 Choose **Deployment>Generate**. The Generate page is displayed.

Step 4 Select the check box to the left of **SensorP** and click **Generate**. The Generate Status page is displayed.

(where P = pod number)

Step 5 Choose **Deployment>Deploy**. The Deploy page is displayed.

Step 6 Click **Submit**. The Submit page is displayed.

Step 7 Select the **SensorP** check box and click **Deploy**. The Select Configurations page is displayed.

Step 8 Select the check box next to the most recently generated configuration.

Step 9 Click **Next**. The Enter Job Properties page is displayed.

Step 10 Enter **Sensing Parameters** in the Job Name field.

Step 11 Verify that the **Immediate** radio button is selected by default.

Step 12 Select the **Email report to:** check box and enter **studentP@cisco.com** in the Email report to field.

Step 13 Click **Finish**. The Submit page is displayed.

Step 14 Open your e-mail client and wait for the Sensor configuration deployment confirmation e-mail to appear in your Inbox.

Note The e-mail confirmation may take a while to deploy depending on the speed of the network and processing power of the IDS MC server.

Task 6—Create a Deployment Report

Complete the following steps to create a configuration deployment report:

Step 1 Choose **Reports>Generate**. The Select Report page is displayed.

Step 2 Select the **Sensor Configuration Deployment Report** radio button.

Step 3 Click **Select**. The Report Filtering page is displayed.

Step 4 Complete the following sub-steps to configure report filtering:

1. Verify that **Since the dawn of time** is selected for the Date/Time by default.
2. Click **Select All** for the Event Severity.
3. Select **SensorP** from the list of IDS Sensors.

Step 5 Click **Next**. The Schedule Report page is displayed.

Step 6 Complete the following sub-steps to configure report scheduling:

1. Enter **SensorP Deployment Report** in the Report Title field.
2. Select the **Schedule for Later** radio button and leave the Start Time at its default setting. The default setting is the present time when you start the report.
3. Select the **Repeat every** check box and select **Day** from the Repeat every drop-down menu.
4. Select the **Email report to:** check box and enter **studentP@cisco.com** in the Email report to field.
5. Click **Finish**. The Select Report page is refreshed.

Step 7 Open your e-mail client and check for new mail. You will receive the e-mail shortly after the report is generated.

Step 8 Double-click the link that is provided in the e-mail. A Security Alert window opens.

Step 9 Click **Yes** in the Security Alert window. The IDS MC browser displays an authentication prompt.

Step 10 Enter **admin** in the username field and **admin** the password field.

Step 11 Click **Login**. The Choose Completed Report page is displayed.

Step 12 Select the **SensorP Deployment Report** check box and click **View**. The Report is displayed in the open browser window.

Task 7—Test the Blocking Configuration

Complete the following steps to test the blocking configuration:

Step 1 Telnet and log in to your router at IP address 10.0.P.2.

(where P = pod number)

Step 2 Enter **cisco** at the password prompt.

```
Password: cisco
rP>
```

Step 3 Enter privileged mode:

```
rP> en
Password:
```

Step 4 Enter the password **cisco**:

```
Password: cisco
```

Step 5 Execute the **show access-lists** command:

```
rP# show access-lists
```

Step 6 From the student PC, ping your peer pod router's outside interface as assigned by your instructor. The ping is successful because the pre-shun ACL allows ICMP traffic.

```
c:\ ping 172.30.Q.2
```

(where Q = peer pod number)

Step 7 Return to your Telnet session and execute the **show access-lists** command again. Notice the ACL dynamically created by the Sensor:

```
rP# show access-lists
Extended IP access list IDS_Ethernet0/1_in_1
  permit ip host 10.0.P.4 any
  deny ip host 10.0.Q.12 any log (1 match)
  permit ip any any (4 matches)
```

(where P = pod number, and Q = peer pod number)

Step 8 From the student PC, attempt to establish a Telnet session to your peer pod router's outside interface. The connection should fail.

```
c:\telnet 172.30.Q.2
```

(where Q = peer pod number)

Step 9 Wait approximately one minute for the Sensor to apply the pre-shun access list.

Step 10 Telnet to your peer pod router's outside interface again. The connection should succeed.

Step 11 Return to your Telnet session with your router and execute the show access-lists command. Notice that the deny statement has been removed:

```
rP# show access-lists
Extended IP access list IDS_Ethernet0/1_in_1
  permit ip host 10.0.P.4 any
  permit ip any any (4 matches)
```

(where P = pod number)

Step 12 Notice that the Sensor added the following configuration to the router:

```
rP# show run
.
.
interface FastEthernet0/1
 ip address 172.30.P.2 255.255.255.0
 ip access-group IDS_FastEthernet0/1_in_0 in
 duplex auto
 speed auto
.
.
.
ip access-list extended IDS_FastEthernet0/1_in_0
```

```
 permit ip host 10.0.P.4 any
 permit ip any any
.
.
.
```

Step 13 Open a DOS prompt and enter the following command:

```
c:\ping –t 10.0.Q.12 –l 1500
```

(where Q = peer pod number)

Step 14 Telnet to IP address 10.0.P.2 and view the running configuration (where P = pod number). Notice the Sensor added the following configuration to the router:

```
rP# show run
.
.
.
interface FastEthernet0/1
 ip address 172.30.P.2 255.255.255.0
 ip access-group IDS_FastEthernet0/1_in_0 in
 duplex auto
 speed auto
.
.
.
ip access-list extended IDS_FastEthernet0/1_in_0
 permit ip host 10.0.P.4 any
 deny ip host 10.0.Q.11 any log
 permit ip any any
.
.
```

Task 8—Remove the Blocking Configuration

Complete the following steps to remove the blocking configuration:

Step 1 Choose **Configuration>Settings**. The Settings page is displayed.

Step 2 Use the Object Selector to choose **sensorP**. The Settings page is refreshed and indicates you are configuring sensorP.

(where P = pod number)

Step 3 Select **Blocking>Blocking Properties**. The Blocking Properties page is displayed.

Step 4 De-select the **Enable ACL Logging** check box.

Step 5 Click **Apply**. The Blocking Properties page refreshes and indicates that the IDS MC received the changes.

Step 6 Select **Signatures** from the TOC. The Signatures page is displayed.

Step 7 Click the **General** Group Name. The Signature(s) in Group page is displayed.

Step 8 Enter **2004** in the field to the left of the Filter button, and click **Filter**. Signature 2004 is displayed in the Signature(s) in Group page.

Step 9 Select the **Signature 2004** check box and click **Edit**. The Edit Signatures page is displayed.

Step 10 De-select the **Block Host** check box.

Step 11 De-select the **Block Connection** check box.

Step 12 Click **OK**. The Signature(s) in Group page is refreshed and displays the actions you configured.

Step 13 Select **Blocking>Blocking Devices** from the TOC. The Blocking Devices page is displayed.

Step 14 Select the radio button to the left of the blocked IP address.

Step 15 Click **Delete**.

Step 16 Choose **Configuration>Pending**. The Pending page is displayed.

Step 17 Select the check box located next to the pending configuration and click **Save**.

Step 18 Choose **Deployment>Generate**. The Generate page is displayed.

Step 19 Select the check box to the left of **SensorP** and click **Generate**. The Generate Status page is displayed.

(where P = pod number)

Step 20 Choose **Deployment>Deploy**. The Deploy page is displayed.

Step 21 Click **Submit**. The Submit page is displayed.

Step 22 Select the **SensorP** check box and click **Deploy**. The Select Configurations page is displayed.

Step 23 Select the check box next to the most recently generated configuration.

Step 24 Click **Next**. The Enter Job Properties page is displayed.

Step 25 Enter **Sensing Parameters** in the Job Name field.

Step 26 Verify that the **Immediate** radio button is selected by default.

Step 27 Select the **Email report to:** check box and enter **studentP@cisco.com** in the Email report to text box.

Step 28 Click **Finish**.

16

Enterprise Intrusion Detection System Monitoring and Reporting

Overview

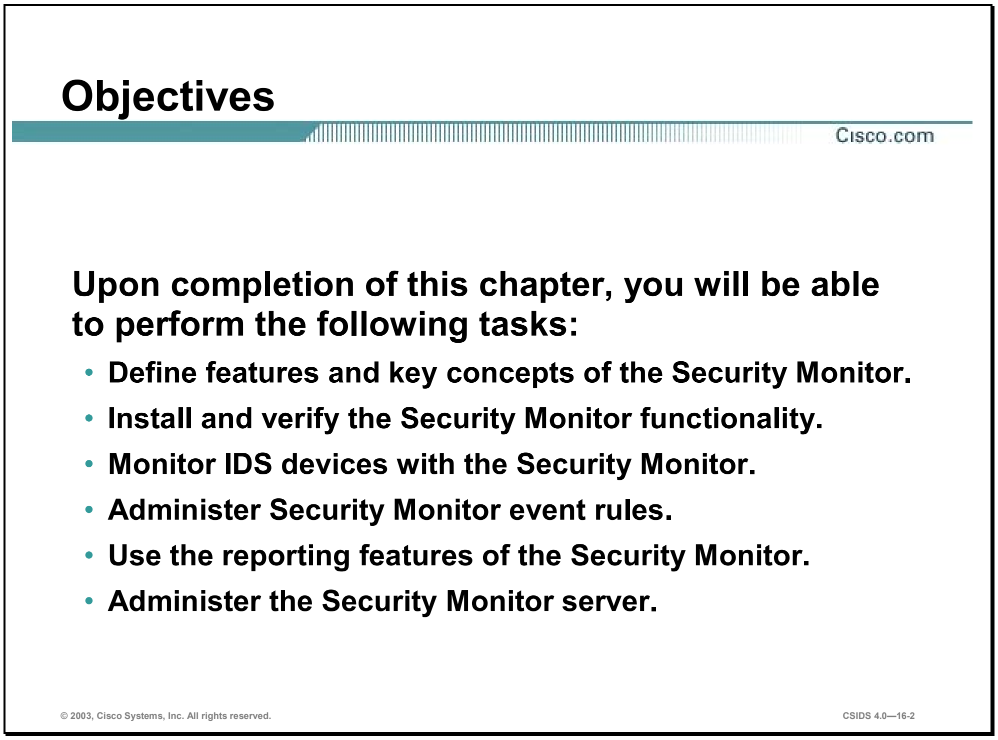
This chapter introduces Enterprise intrusion detection system (IDS) monitoring and reporting using the CiscoWorks2000 (CiscoWorks) Virtual Private Network (VPN)/Security Management Solution (VMS) Security Monitor. The following topics are covered in this chapter:

- Objectives
- Introduction
- Installation
- Getting started
- Security Monitor configuration
- Security Monitor Event Viewer
- Administration and reporting
- Summary

- Lab exercise

Objectives

This section lists the chapter's objectives.



Objectives

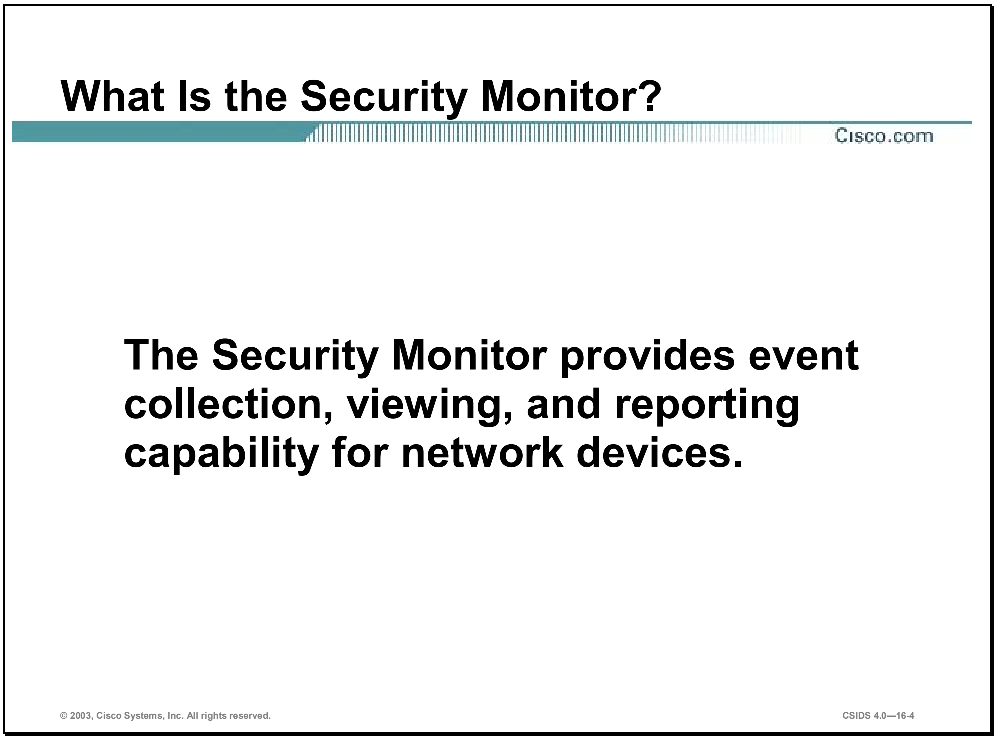
Upon completion of this chapter, you will be able to perform the following tasks:

- **Define features and key concepts of the Security Monitor.**
- **Install and verify the Security Monitor functionality.**
- **Monitor IDS devices with the Security Monitor.**
- **Administer Security Monitor event rules.**
- **Use the reporting features of the Security Monitor.**
- **Administer the Security Monitor server.**

CSIDS 4.0—16-2

Introduction

This section introduces the Security Monitor product for intrusion detection systems (IDS).



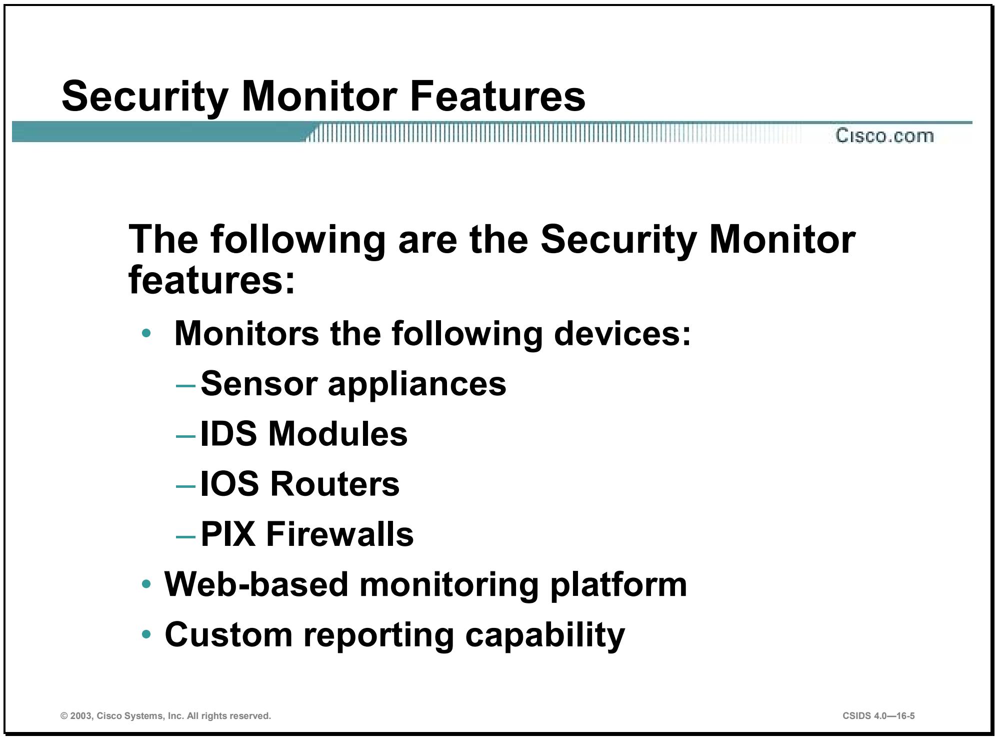
What Is the Security Monitor?

The Security Monitor provides event collection, viewing, and reporting capability for network devices.

CSIDS 4.0—16-4

The Security Monitor is a component of the Virtual Private Network (VPN)/Security Management Solution (VMS) product. The Security Monitor provides event collection, viewing, and reporting capability for network devices. The VMS product integrates numerous security applications into a single solution, such as the following:

- CiscoWorks
- Security Monitor
- VPN Monitor
- VMS Common Services.



Security Monitor Features

Cisco.com

The following are the Security Monitor features:

- **Monitors the following devices:**
  - **Sensor appliances**
  - **IDS Modules**
  - **IOS Routers**
  - **PIX Firewalls**
- **Web-based monitoring platform**
- **Custom reporting capability**

© 2003, Cisco Systems, Inc. All rights reserved.

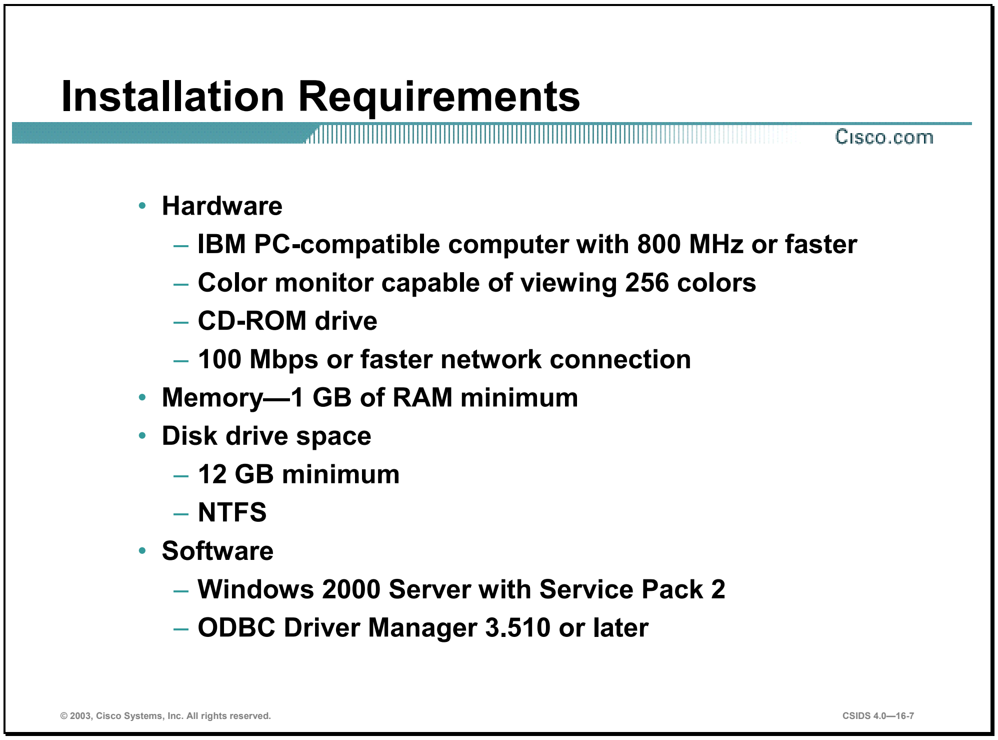
CSIDS 4.0—16-5

The Security Monitor has the following features:

- Device monitoring—The Security Monitor can receive IDS events from the following Cisco IDS capable devices:
  - Sensor appliances
  - IDS Modules (IDSM)
  - IOS routers
  - PIX Firewalls
- Web-based monitoring platform—The Security Monitor is built on web-based technology. This enables the network security administrator to view IDS events from a web browser.
- Custom reporting capability—The Security Monitor has a comprehensive list of common reports that can be customized to meet a customers needs.

Installation

This section explains the installation of the Security Monitor and discusses the requirements.



Installation Requirements

Cisco.com

- Hardware
  - IBM PC-compatible computer with 800 MHz or faster
  - Color monitor capable of viewing 256 colors
  - CD-ROM drive
  - 100 Mbps or faster network connection
- Memory—1 GB of RAM minimum
- Disk drive space
  - 12 GB minimum
  - NTFS
- Software
  - Windows 2000 Server with Service Pack 2
  - ODBC Driver Manager 3.510 or later

CSIDS 4.0—16-7

Verify that the server on which you plan to install the Security Monitor meets the following requirements:

- Hardware
  - IBM PC-compatible computer with Pentium 1 GHz minimum
  - Color monitor with video card capable of 16-bit colors
  - A CD-ROM drive
  - A 10BaseT or faster network connection
- Memory—1 GB of RAM minimum
- Disk drive space
  - 9 GB free hard drive space minimum
  - 2 GB of virtual memory

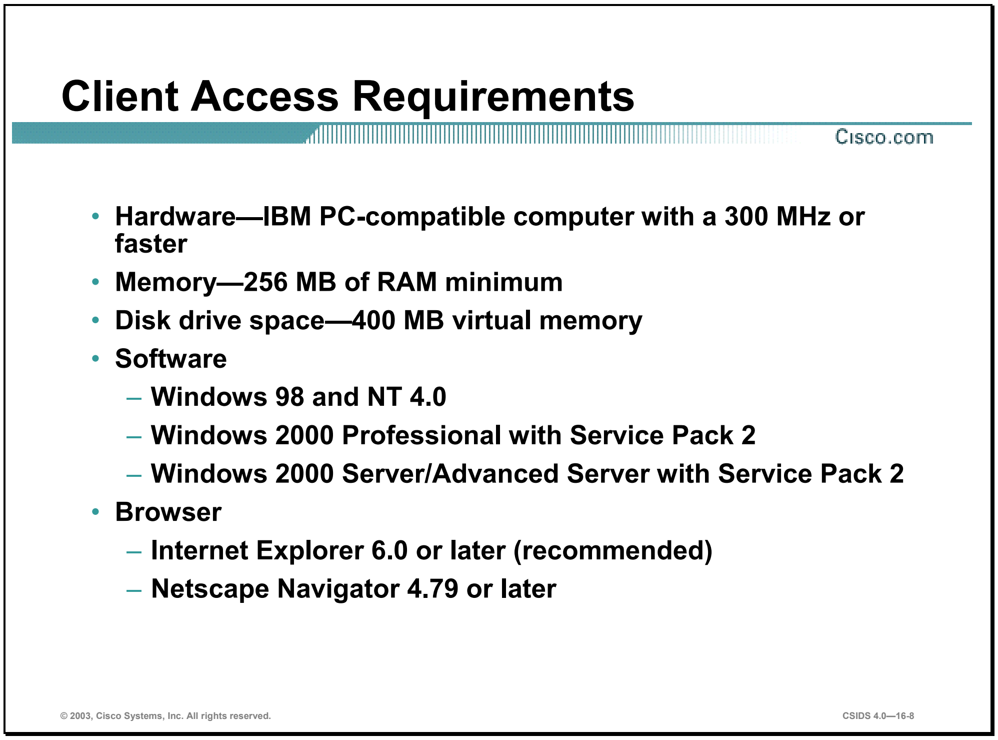
  - New Technology File System (NTFS)

- Software

  - Windows 2000 Server or Professional with Service Pack 2

  - Open Database Connectivity (ODBC) Driver Manager 3.510 or later

Caution Do not attempt to install IDS MC on a system that has Cisco Secure Policy Manager (CSPM) installed on it. The installer for Security Monitor attempts to install the Cisco IDS PostOffice software in a second location on the host causing it to function incorrectly.



Client Access Requirements

Cisco.com

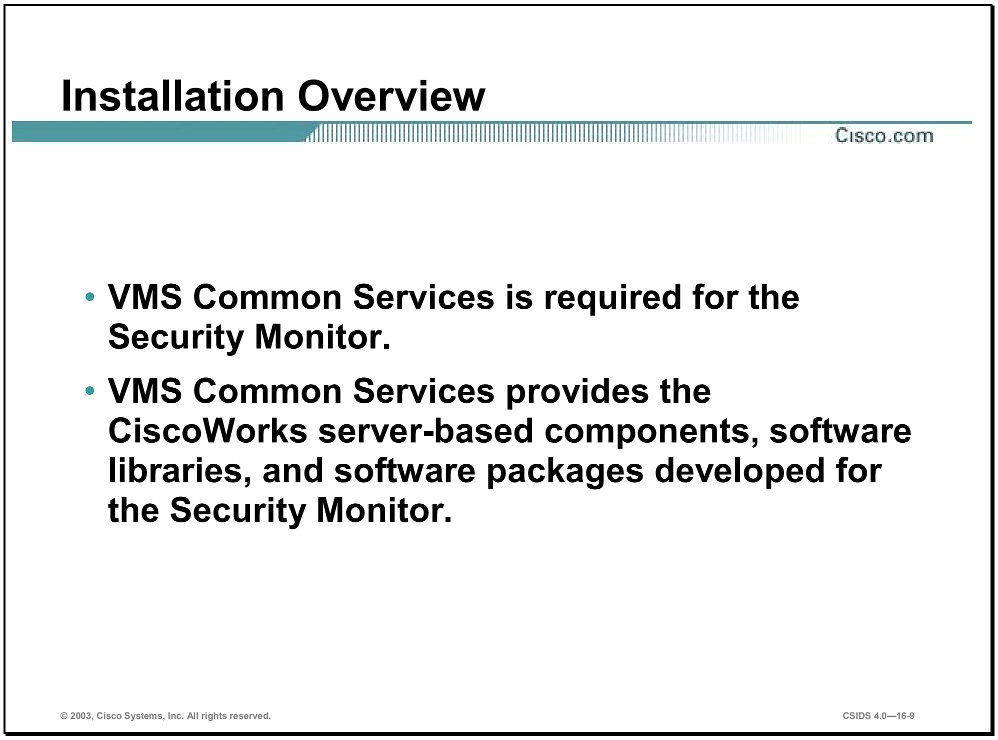
- Hardware—IBM PC-compatible computer with a 300 MHz or faster
- Memory—256 MB of RAM minimum
- Disk drive space—400 MB virtual memory
- Software
  - Windows 98 and NT 4.0
  - Windows 2000 Professional with Service Pack 2
  - Windows 2000 Server/Advanced Server with Service Pack 2
- Browser
  - Internet Explorer 6.0 or later (recommended)
  - Netscape Navigator 4.79 or later

CSIDS 4.0—16-8

Verify that the client machine used to log into the VMS Security Monitor meets the following requirements:

- Hardware—IBM PC-compatible with a 300 MHz or faster
- Memory—256 MB of RAM minimum
- Disk Drive Space
  - 400 MB virtual memory (for Windows)
  - 512 MB swap space (for Solaris)
- Software
  - Windows 98
  - Windows NT
  - Windows 2000 Professional with Service Pack 2 or Service Pack 3
  - Windows 2000 Server with Service Pack 2 or Service Pack 3
  - Windows 2000 Advanced Server
  - Solaris SPARCstation or Sun Ultra 10 with 333 MHz processor running Solaris 2.7 or Solaris 2.8

- Browser
  - Microsoft Internet Explorer version 6.0 or 5.5 with Service Pack 2, and Java Virtual Machine (JVM) 5.00.3186 or later
  - Netscape Navigator 4.79 or later (for Windows)
  - Netscape Navigator 4.76 or later (for Solaris)



Installation Overview

- **VMS Common Services is required for the Security Monitor.**
- **VMS Common Services provides the CiscoWorks server-based components, software libraries, and software packages developed for the Security Monitor.**

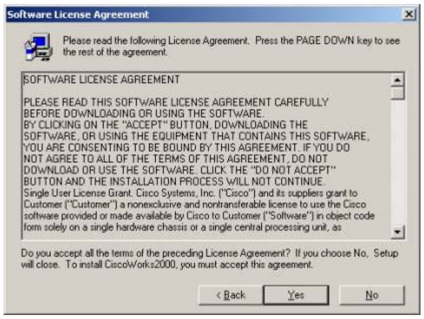
CSIDS 4.0—16-9

CiscoWorks Common Services are required for the Security Monitor. CiscoWorks Common Services provide the CiscoWorks server-based components and software developed specifically for the Security Monitor, including the necessary software libraries and packages.

For more information, see the *Quick Start Guide for VPN Security Management Solution* or *Installing VMS Common Services on Windows 2000*.

Security Monitor Installation

Cisco.com



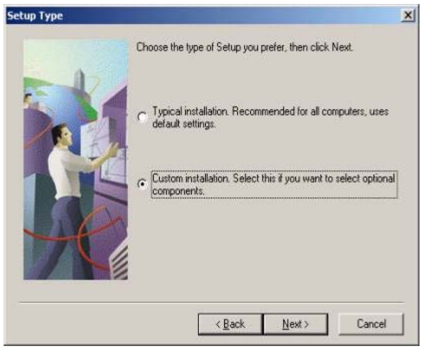
Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE. BY CLICKING ON THE "ACCEPT" BUTTON, DOWNLOADING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT DOWNLOAD OR USE THE SOFTWARE. CLICK THE "DO NOT ACCEPT" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE.
Single User License Grant. Cisco Systems, Inc. ("Cisco") and its suppliers grant to Customer ("Customer") a nonexclusive and nontransferable license to use the Cisco software provided or made available by Cisco to Customer ("Software") in object code form solely on a single hardware chassis or a single central processing unit, as

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install CiscoWorks2000, you must accept this agreement.



Setup Type

Choose the type of Setup you prefer, then click Next.

○ Typical installation. Recommended for all computers, uses default settings.

● Custom installation. Select this if you want to select optional components.

CSIDS 4.0—16-10

Complete the following steps to install the Security Monitor:

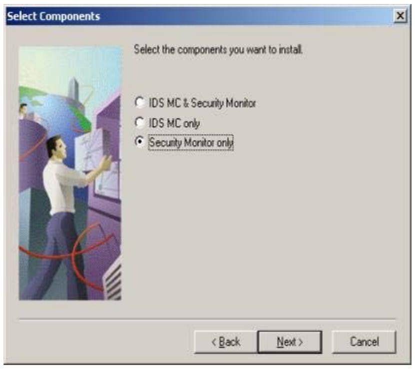
Step 1 Launch the Security Monitor installation. The Welcome Window opens.

Step 2 Click **Next**. The Software License Agreement window opens.

Step 3 If you agree with the Software License Agreement, click **Yes** to proceed. The Select Installation Type window opens. If you do not agree with the Software License Agreement, click **No** and the installation process stops.

Step 4 Select **Custom Installation** for the installation type and click **Next**. The Select Components window opens.

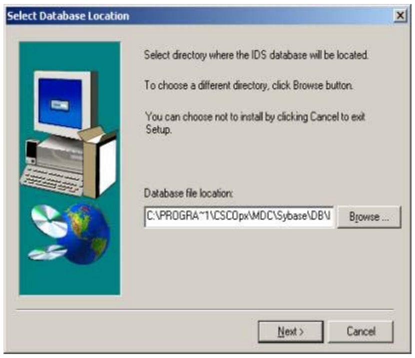
Component and Database Location Selection



Select Components

Select the components you want to install.

○ IDS MC & Security Monitor
○ IDS MC only
● Security Monitor only



Select Database Location

Select directory where the IDS database will be located.

To choose a different directory, click Browse button.

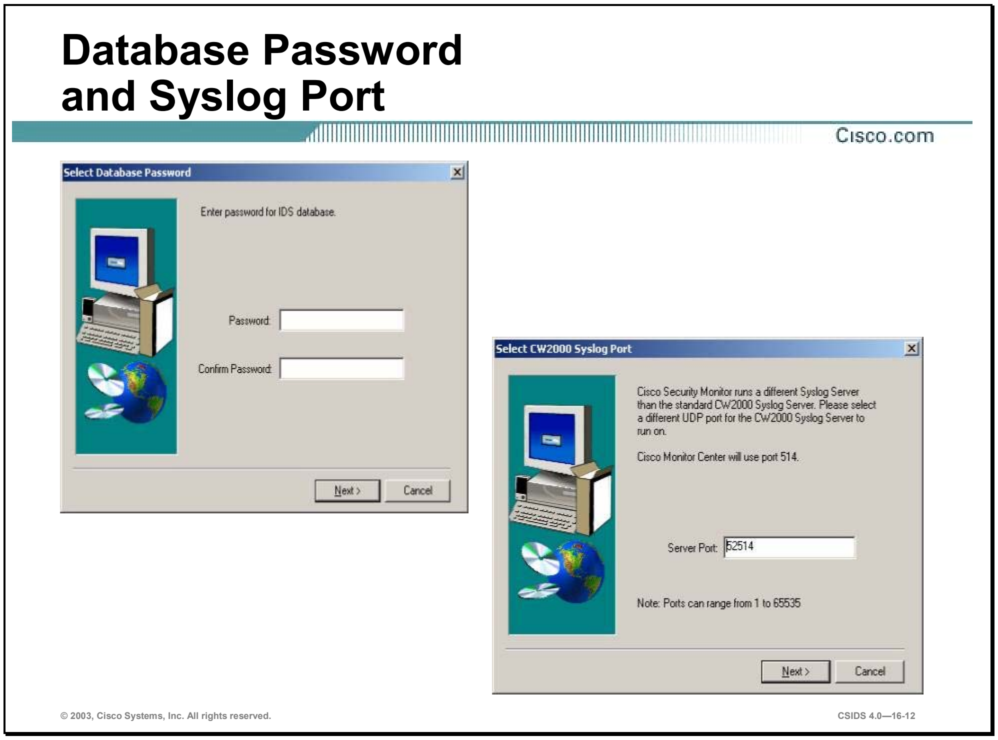
You can choose not to install by clicking Cancel to exit Setup.

Database file location: C:\PROGRA~1\CSCOpx\MDC\Sybase\DB\I

CSIDS 4.0—16-11

Step 5 Select **Security Monitor only** and click **Next**. The Select Database Location window opens.

Step 6 The default database location is located within the database where the VMS common services have been installed. To install the IDS Database to a different directory, click **Browse** and select a different directory. **Click Next**. The Select Database Password window opens.



Database Password and Syslog Port

Cisco.com

Select Database Password

Enter password for IDS database.

Password:

Confirm Password:

Select CW2000 Syslog Port

Cisco Security Monitor runs a different Syslog Server than the standard CW2000 Syslog Server. Please select a different UDP port for the CW2000 Syslog Server to run on.

Cisco Monitor Center will use port 514.

Server Port: 52514

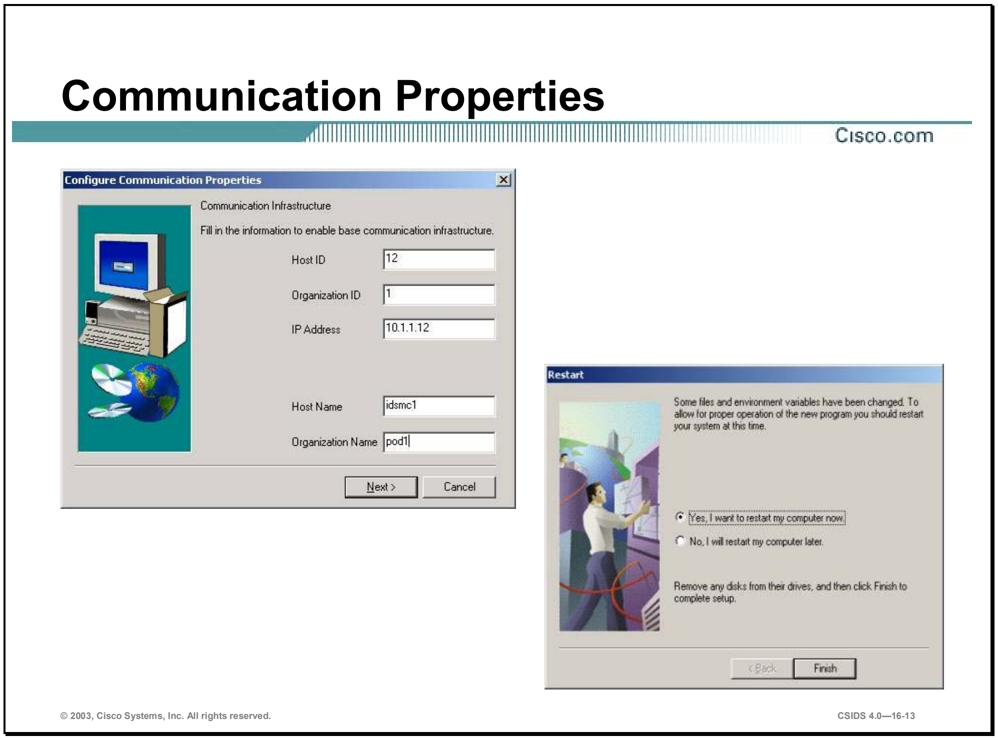
Note: Ports can range from 1 to 65535

CSIDS 4.0—16-12

Step 7 Enter a password in the Password and Confirm Password fields. This password is used to secure the Sybase SQL database that the Security Monitor uses to store information about Cisco IDS devices. Click **Next** to continue. The Select CW2000 Syslog Port window opens.

Step 8 In the Server Port field, enter a different UDP port for CiscoWorks to run on and click **Next**. The Configure Communications Properties window opens.

Note The Security Monitor runs a different Syslog server than the standard CiscoWorks Syslog server.



Communication Properties

Cisco.com

Configure Communication Properties

Communication Infrastructure

Fill in the information to enable base communication infrastructure.

Host ID: 12

Organization ID: 1

IP Address: 10.1.1.12

Host Name: idsmc1

Organization Name: pod1

Restart

Some files and environment variables have been changed. To allow for proper operation of the new program you should restart your system at this time.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

CSIDS 4.0—16-13

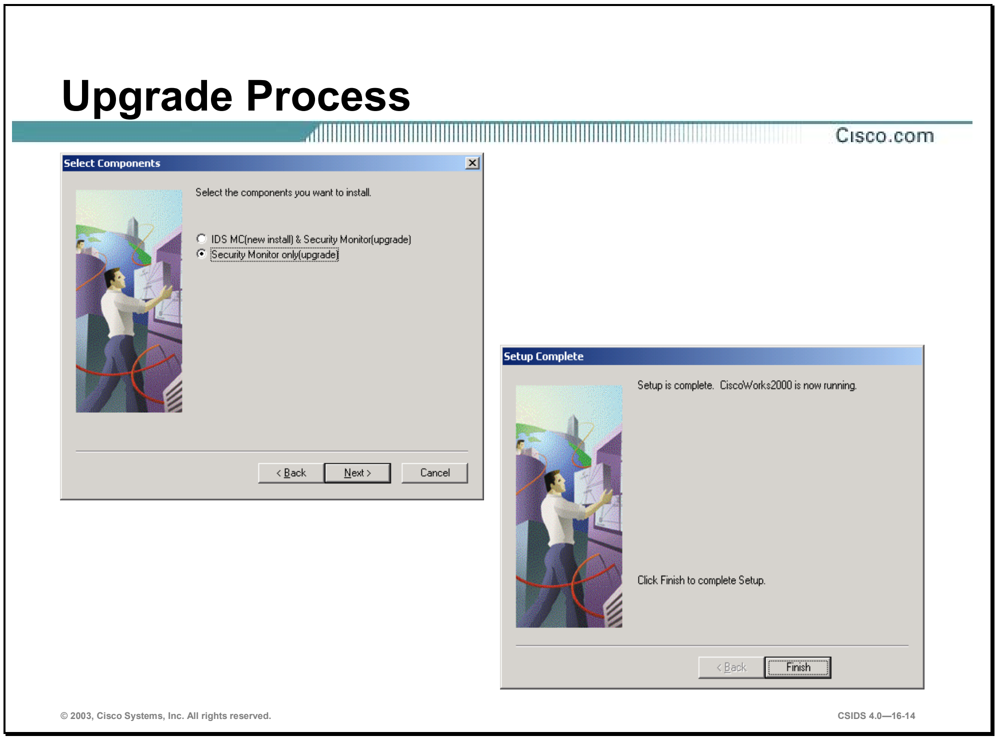
Step 9 Enter values for settings listed in the following table:

Security Monitor Installation Settings	Description
Host ID	The host identity of the Security Monitor’s PostOffice service. The default is the last octet of the IP address.
Organization ID	The organization identity of the Security Monitor’s PostOffice service. The default is 100.
IP Address	The IP address of the Security Monitor.
Host Name	The hostname of the Security Monitor.
Organization Name	The organization name of the Security Monitor.

Step 10 Click **Next**. After the installation process is complete, the Restart window opens.

Step 11 Select **Yes, I want to restart my computer now** to finish the installation.

Note The settings mentioned above are required only if you are running an IDS software version earlier than 4.0.



Upgrade Process

Cisco.com

Select Components

Select the components you want to install.

○ IDS MC(new install) & Security Monitor(upgrade)

● Security Monitor only(upgrade)

Setup Complete

Setup is complete. CiscoWorks2000 is now running.

Click Finish to complete Setup.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—16-14

Complete the following steps to upgrade a previous version of the Security Monitor:

Step 1 Launch the Security Monitor installation. The Welcome Window opens.

Step 2 Click **Next**. The Software License Agreement window opens.

Step 3 If you agree with the Software License Agreement, click **Yes** to proceed. The Select Installation Type window opens. If you do not agree with the Software License Agreement, click **No** and the installation process stops.

Step 4 Select **Custom Installation** for the installation type and click **Next**. The Select Components window opens.

Step 5 Select **Security Monitor only(upgrade)** and click **Next**. The Verification window opens.

Step 6 Verify the components that you are installing or upgrading and click **Next**. After upgrading the Security Monitor, the Setup Complete window opens.

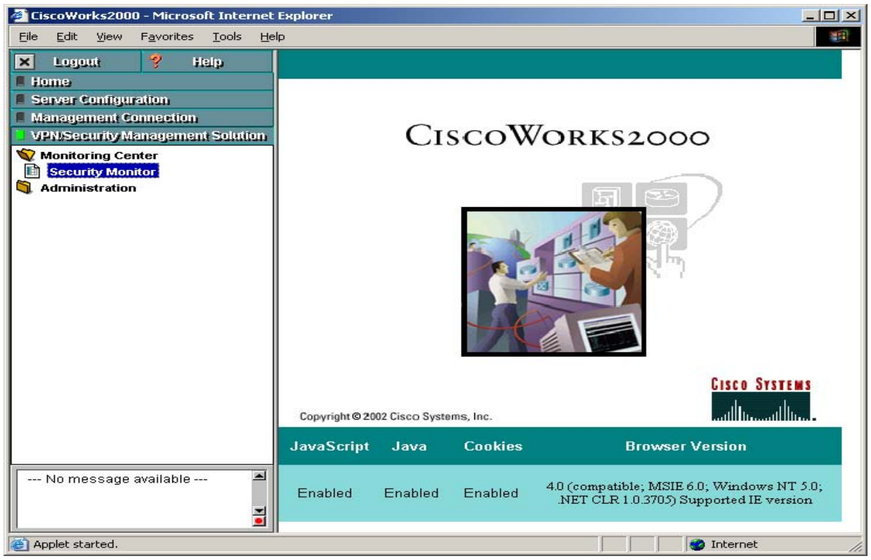
Step 7 Click **Finish**. The Security Monitor processes begin.

Getting Started

This section explains how authorization roles in CiscoWorks are responsible for delegation of tasks and how to log in to the Security Monitor.

CiscoWorks Login

Cisco.com



--- No message available ---

Copyright © 2002 Cisco Systems, Inc.

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.0.3705) Supported IE version

CSIDS 4.0—16-16

You must log in to the CiscoWorks server desktop to navigate in the Security Monitor. The CiscoWorks server desktop is the interface for the CiscoWorks network management applications, including the Security Monitor.

Complete the following steps to log in to CiscoWorks:

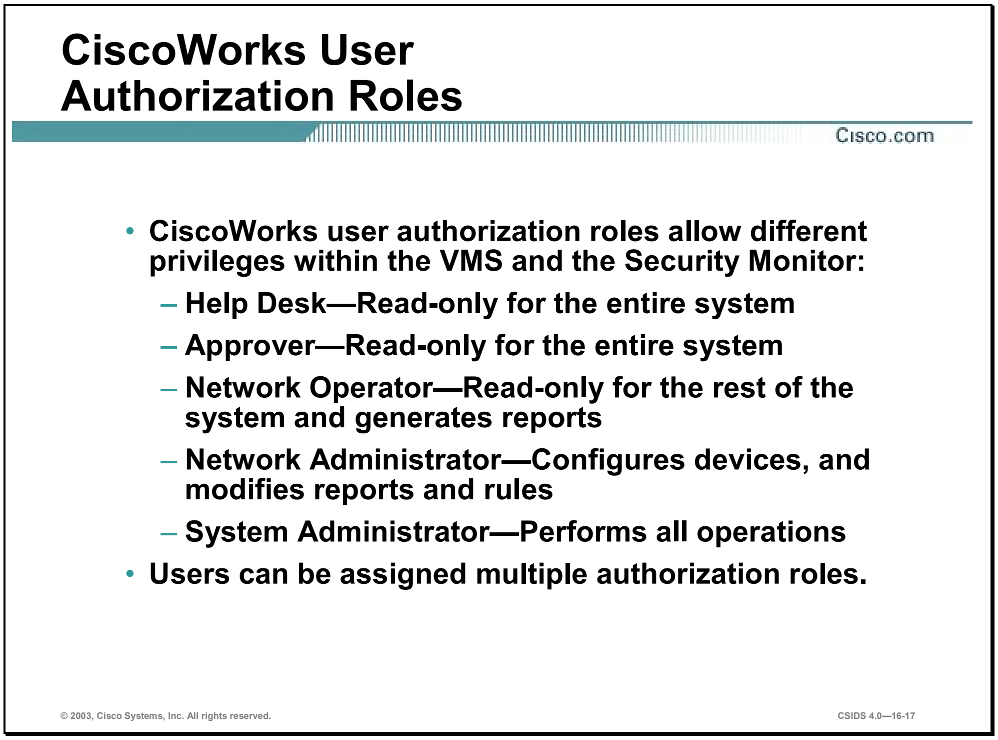
Step 1 Open a browser and point your browser to the IP address of the CiscoWorks server with a port number of 1741. In the figure, the CiscoWorks server is the local machine. Enter the following in the browser address field:

```
http://127.0.0.1:1741
```

Step 2 The CiscoWorks desktop is displayed.

Step 3 Use the default username and password of **admin** and **admin** to log in to CiscoWorks.

Note It is recommended that you change the default admin account password.



CiscoWorks User Authorization Roles

Cisco.com

- CiscoWorks user authorization roles allow different privileges within the VMS and the Security Monitor:
  - Help Desk—Read-only for the entire system
  - Approver—Read-only for the entire system
  - Network Operator—Read-only for the rest of the system and generates reports
  - Network Administrator—Configures devices, and modifies reports and rules
  - System Administrator—Performs all operations
- Users can be assigned multiple authorization roles.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—16-17

There are CiscoWorks user authorization roles that are pertinent to the Security Monitor. These roles can be used to delegate different responsibilities to users who log into the Security Monitor. For example, you specify who can generate configurations or specify who can approve configurations. The user authorization roles pertinent to the Security Monitor are as follows:

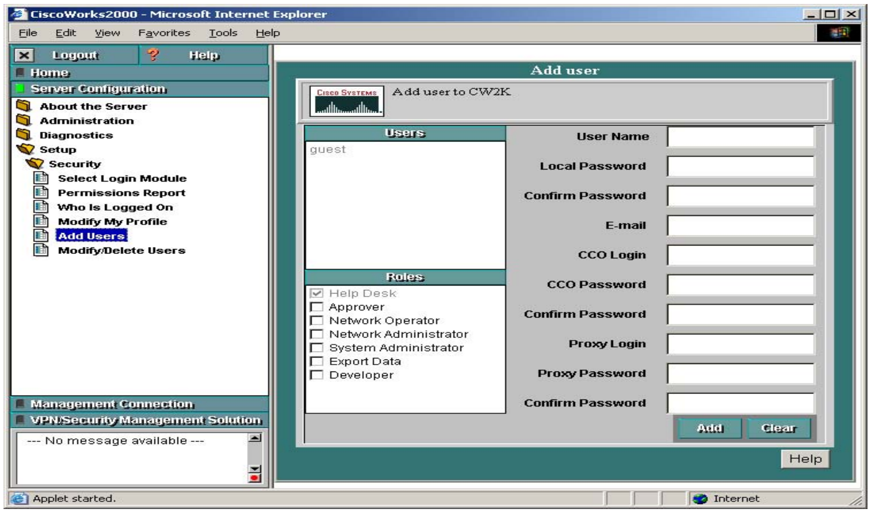
- Help Desk—Read-only for the entire system
- Approver—Read-only for the entire system
- Network Operator—Read-only for the rest of the system, and generates reports
- Network Administrator—Configures devices and modifies reports and rules
- System Administrator—Performs all operations

Note Users can be assigned multiple authorization roles.

CiscoWorks Add User

Cisco.com

Choose Server Configuration>Setup>Security>Add Users**.**



- ☑ Help Desk
- ☐ Approver
- ☐ Network Operator
- ☐ Network Administrator
- ☐ System Administrator
- ☐ Export Data
- ☐ Developer

CSIDS 4.0—16-18

Complete the following steps to add users based upon how CiscoWorks user authorization roles work:

Step 1 Log in to the CiscoWorks server desktop. The CiscoWorks server desktop is displayed.

Step 2 Choose **Server Configuration>Setup>Security>Add Users**. The Add User page is displayed.

Step 3 Enter values for settings listed in the following table:

CiscoWorks Add User Settings	Description
User Name	User name to add.
Local Password	Password.
Confirm Password	Password confirmation.
E-Mail	User’s e-mail address.
CCO Login	User’s Cisco Connection Online (CCO) login.
CCO Password	User’s CCO password.
Confirm Password	User’s CCO password confirmation.
Proxy Login	User’s proxy login. This is required if the CiscoWorks server is installed on a network that uses a proxy server.
Proxy Password	User’s proxy password.
Confirm Password	User’s proxy password confirmation.

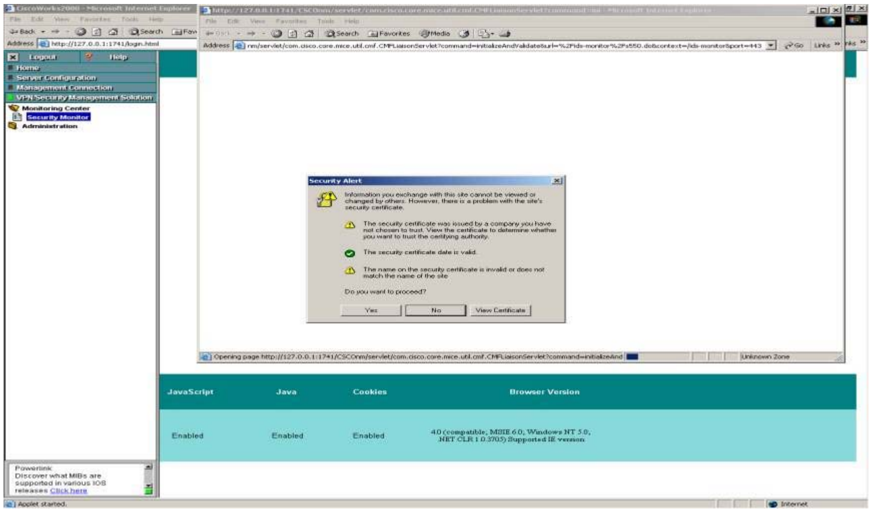
Step 4 Locate the Roles group box on the lower left hand side of the Add User page. Select the appropriate check boxes for the roles the user will fulfill.

Step 5 Click **Add** to complete the addition of the user to the CiscoWorks database.

Security Monitor Launch

Cisco.com

Choose VPN/Security Management>Management Center>Security Monitor**.**



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Opening page http://127.0.0.1:1741/CSCOnm/servlet/com.cisco.core.mice.util.cmf.CMFLiaisonServlet?command=initializeAnd

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.0.3705) Supported IE version

Powerlink
Discover what MIBs are supported in various IOS releases Click here

Applet started.

CSIDS 4.0—16-19

The Security Monitor is located within CiscoWorks. Complete the following steps to launch the Security Monitor:

Step 1 Click the **VPN Security Management Solution** drawer located on the far-left side of the CiscoWorks page. The drawer expands, and displays sets of folders.

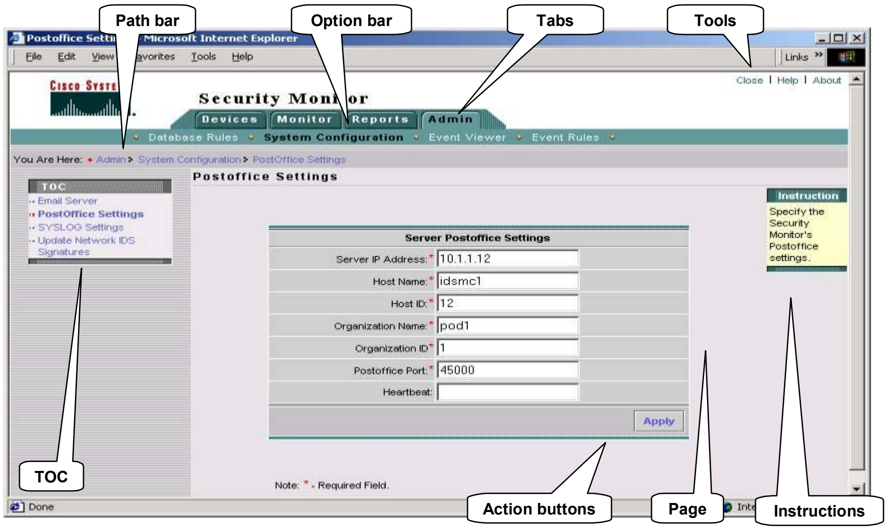
Step 2 Click the **Monitoring Center** folder. The Monitoring Center folder expands.

Step 3 Click **Security Monitor**. A Security Alert window opens.

Step 4 Click **Yes** to proceed. The Security Monitor is launched in a new browser window.

Understanding the Security Monitor Interface

Cisco.com



You Are Here: ◆ Admin ▸ System Configuration ▸ PostOffice Settings

Postoffice Settings

Server Postoffice Settings

Server IP Address:*	10.1.1.12
Host Name:*	idsmc1
Host ID:*	12
Organization Name:*	pod1
Organization ID*	1
Postoffice Port:*	45000
Heartbeat:	

Note: * - Required Field.

Instruction

Specify the Security Monitor's Postoffice settings.

CSIDS 4.0—16-20

The figure illustrates elements of the Security Monitor GUI. The elements are described as follows:

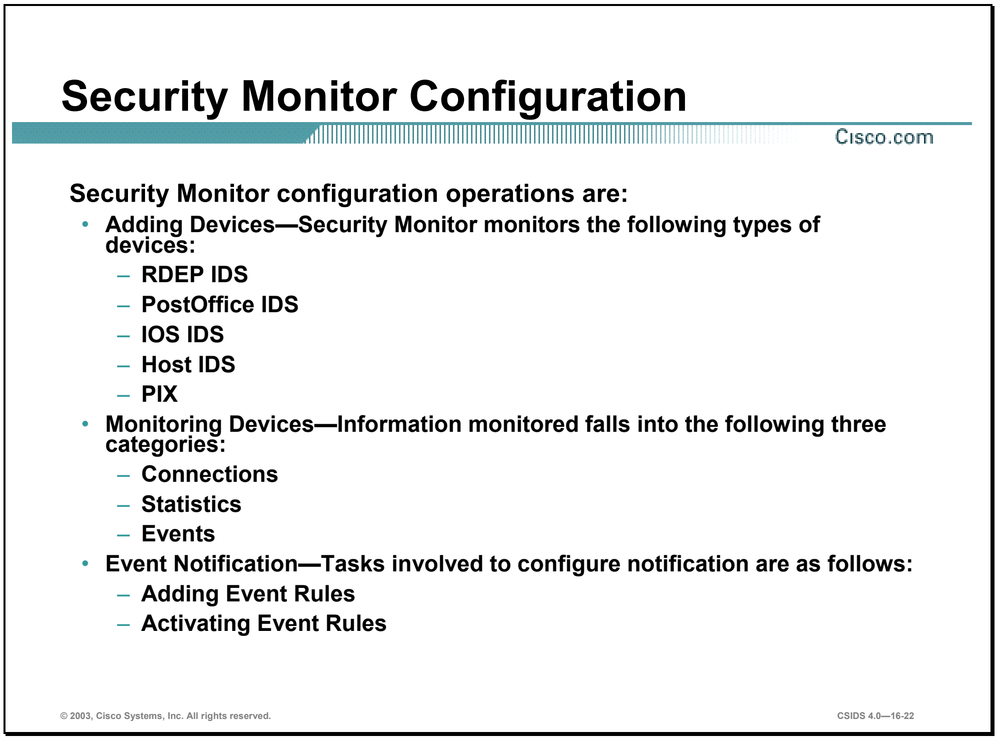
- Path bar—Provides the location of the current page.
- TOC (table of contents)—TOC is a menu of choices that is displayed down the left side of the Security Monitor interface. It represents the list of sub-options that you can select (based on the option chosen).
- Option bar—Displays the options available for the selected tab.
- Configuration Tabs—Provides access to product functionality:
  - Devices tab—Enables you to perform initial setup of devices to be monitored by Security Monitor.
  - Monitor tab—Enables you to monitor information about your devices and launch the Event Viewer.
  - Reports tab—Enables you to generate reports, view scheduled reports, and view reports.
  - Admin tab—Enables you to administer system and database settings.
- Tools—Contains the Close/Logout, Help, and About buttons. Close/Logout option enables you to close the Security Monitor program. The Help option displays Security Monitor's

help information in a separate browser window. Finally, the About option displays the Security Monitor software version.

- Instructions—Provides a brief overview of how to use the page. This information is a quick summary of information provided through the Help option on the Tools bar.
- Page—Displays the area in which you complete application tasks.
- Action buttons—Initiates actions or commands for this page. Buttons that do not work on a particular page are grayed-out.

Security Monitor Configuration

This section explains how to add security devices to the Security Monitor, monitor security devices, use the reporting feature of the Security Monitor, and administer the Security Monitor server.



Security Monitor Configuration

Security Monitor configuration operations are:

- **Adding Devices—Security Monitor monitors the following types of devices:**
  - **RDEP IDS**
  - **PostOffice IDS**
  - **IOS IDS**
  - **Host IDS**
  - **PIX**
- **Monitoring Devices—Information monitored falls into the following three categories:**
  - **Connections**
  - **Statistics**
  - **Events**
- **Event Notification—Tasks involved to configure notification are as follows:**
  - **Adding Event Rules**
  - **Activating Event Rules**

CSIDS 4.0—16-22

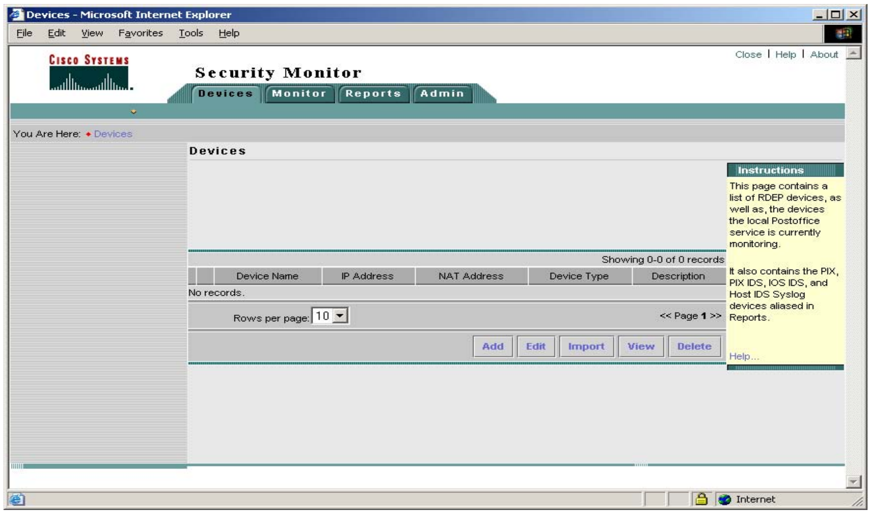
Before you can utilize Security Monitor to analyze the events from your IDS devices, you must add them to Security Monitor. You can configure the rules that Security Monitor uses to access alerts from the different devices being monitored. For RDEP devices, you can also monitor connection and statistical information. This section will focus on the following Security Monitor configuration operations:

- Adding Devices
- Monitoring Devices
- Event Notification

Devices—Add

Cisco.com

Choose Devices.



Devices

Showing 0-0 of 0 records

		Device Name	IP Address	NAT Address	Device Type	Description
No records.						

Instructions

This page contains a list of RDEP devices, as well as, the devices the local Postoffice service is currently monitoring.

It also contains the PIX, PIX IDS, IOS IDS, and Host IDS Syslog devices aliased in Reports.

Security Monitor enables you to view alerts from various Cisco IDS devices deployed throughout your network. Before you can monitor these devices, however, you must add them to Security Monitor. The Devices window shows you the devices that you have already added to Security Monitor and enables you to add or import new devices as well as performing the following operations on existing devices:

- Add
- Edit
- Import
- View
- Delete

Security Monitor monitors the following types of devices:

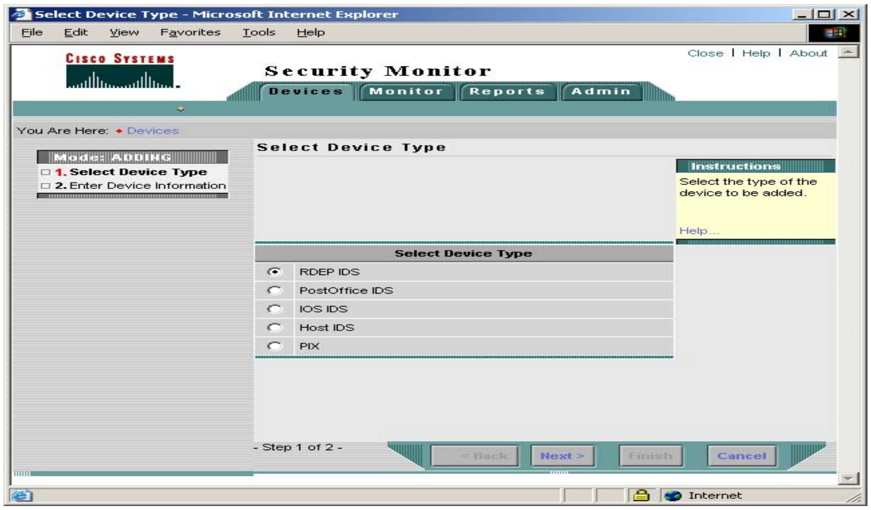
- RDEP IDS
- PostOffice IDS
- IOS IDS
- Host IDS
- PIX

Note Users can use Security Monitor to import device information from a local or remote IDS MC server.

RDEP Devices—Add

Cisco.com

Choose Devices and Select Add**.**



You Are Here: ◆ Devices

Mode: ADDING

□ **1. Select Device Type**

□ **2.** Enter Device Information

Select Device Type

Instructions

Select the type of the device to be added.

Help...

Select Device Type

● RDEP IDS

○ PostOffice IDS

○ IOS IDS

○ Host IDS

○ PIX

- Step 1 of 2 -

CSIDS 4.0—16-24

Security Monitor uses RDEP to communicate with your Cisco IDS version 4.0 sensors. Complete the following steps to add an RDEP IDS device to the Security Monitor:

Step 1 Choose **Devices>Add**. The Select Device Type page is displayed.

Step 2 Select the **RDEP IDS** radio button and click **Next**. The Enter Device Information page is displayed.

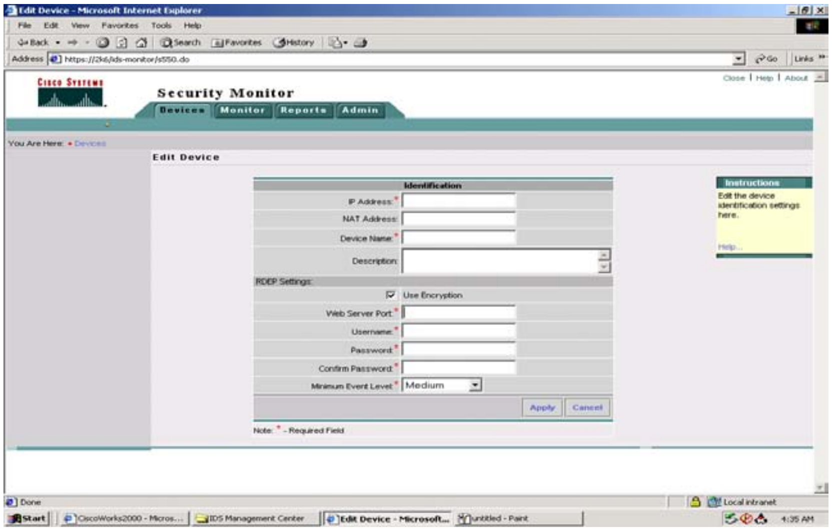
Complete the following steps to delete an IDS device from the Security Monitor:

Step 1 Select **Devices**. The Devices page is displayed.

Step 2 Choose a device to delete from the Security Monitor database. Click **Delete**.

RDEP Devices—Add (cont.)

Cisco.com


Edit Device - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://2k6/ids-monitor/s550.do
Go Links
Cisco Systems
Close | Help | About
Devices Monitor Reports Admin
Done
Local intranet
Start CiscoWorks2000 - Micros... IDS Management Center Edit Device - Microsoft... untitled - Paint
4:35 AM

Security Monitor

You Are Here: • Devices

Edit Device

Identification

IP Address: *

NAT Address:

Device Name: *

Description:

RDEP Settings:

☑ Use Encryption

Web Server Port: *

Username: *

Password: *

Confirm Password: *

Minimum Event Level: * Medium

Apply Cancel

Note: * - Required Field

Instructions

Edit the device identification settings here.

Help...

CSIDS 4.0—16-25

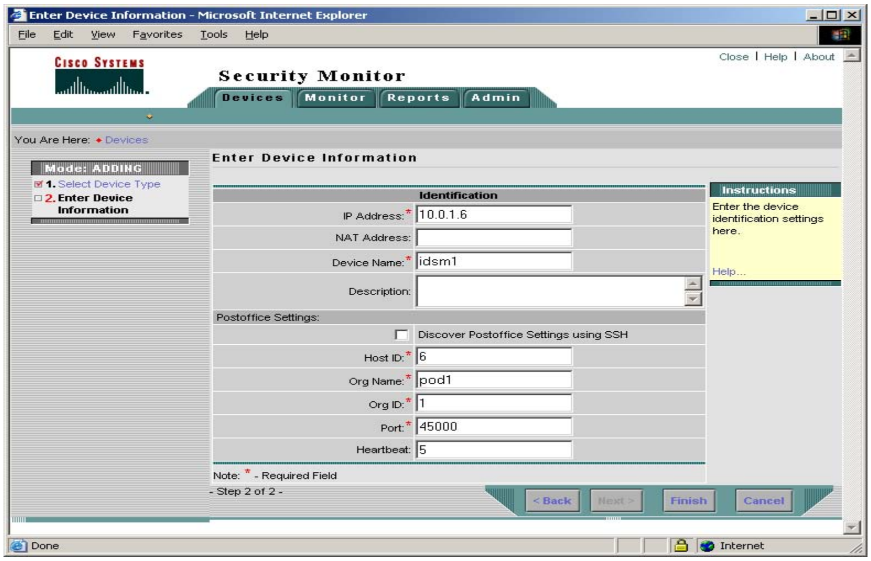
Step 3 Enter values for settings listed in the following table:

Security Monitor Device Information Settings	Description
IP Address	IP address of the security device.
NAT Address	NAT IP address of the RDEP IDS device, required if the device is using NAT.
Device Name	Name of the device.
Description	Optional.
Use Encryption	Select this check box if the device uses Transport Layer Security (TLS). This check box is selected by default.
Web Server Port	Web server port used by the RDEP device.
Username	User name used to log into the RDEP device.
Password	Password used to log into the RDEP device.
Confirm Password	Confirmation password used to log into the RDEP device.
Minimum Event Level	Minimum event level to monitor. The following options are available: Informational, Low, Medium, and High. Medium is selected by default.

Step 4 Click **Finish**. The Devices page is displayed with the RDEP device.

PostOffice Devices—Add

Cisco.com



Enter Device Information

Identification

IP Address:*	10.0.1.6
NAT Address:	
Device Name:*	idsm1
Description:	

Postoffice Settings:

□	Discover Postoffice Settings using SSH
Host ID:*	6
Org Name:*	pod1
Org ID:*	1
Port:*	45000
Heartbeat:	5

Enter the device identification settings here.

Note: * - Required Field

- Step 2 of 2 -

Security Monitor can receive events from Cisco IDS version 3.x sensors. You can add these devices selecting the PostOffice IDS radio button when adding a new device. Complete the following steps to add an IDS device that uses the PostOffice protocol:

Step 1 Choose **Devices>Add**. The Select Device Type page is displayed.

Step 2 Select the **PostOffice IDS** radio button and click **Next**. The Enter Device Information page is displayed.

Step 3 Enter values for settings listed in the following table:

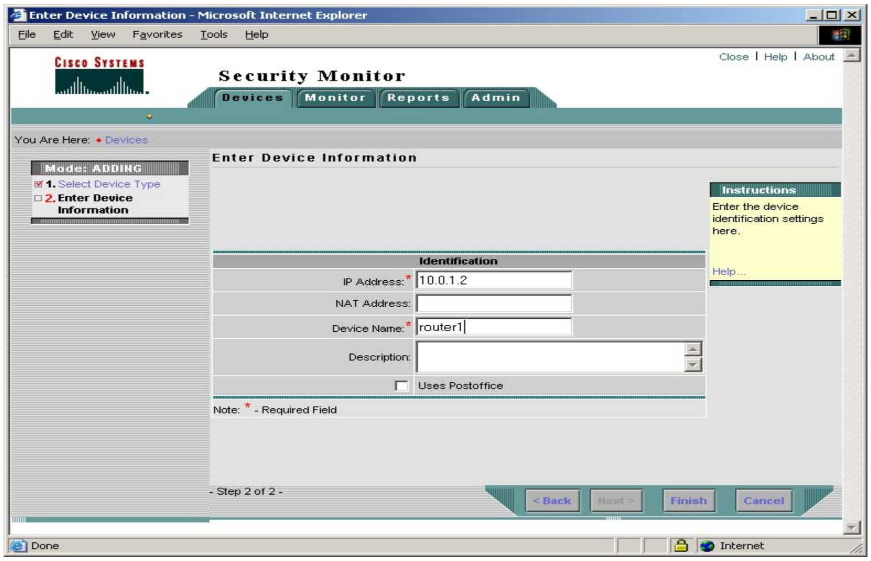
Security Monitor Device Information Settings	Description
IP Address	IP address of the security device.
NAT Address	NAT IP address of the RDEP IDS device, required if the device is using NAT.
Device Name	Name of the security device.
Description	Optional.
Discover PostOffice Settings using SSH	Check box that, if selected, enables the Security Monitor to discover the PostOffice IDS settings via Secure Shell (SSH).
Host ID	Host ID for PostOffice communications.
Org Name	Org Name for PostOffice communications.
Org ID	Org ID for PostOffice communications.
Port	Port number for PostOffice communications. The default port number is 45000.
Heartbeat	Heartbeat interval for PostOffice communications. The default heartbeat interval is 5 seconds.

Step 4 Click **Finish**. The Devices page is displayed with the PostOffice device.

Note If you select the Discover PostOffice Settings using SSH check box, the Security Monitor will take awhile to update its Devices page because of the discovery process.

IOS IDS Devices—Add

Cisco.com


Enter Device Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
You Are Here: ♦ Devices
Mode: ADDING
☑ 1. Select Device Type
□ 2. Enter Device Information
Instructions
Enter the device identification settings here.
Help...
Uses Postoffice
- Step 2 of 2 -
< Back
Next >
Finish
Cancel
Done
Internet

Enter Device Information

Identification

IP Address:* 10.0.1.2

NAT Address:

Device Name:* router1

Description:

□ Uses Postoffice

Note: * - Required Field

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—16-26

Besides receiving events from Cisco IDS Sensors, Security Monitor can also receive events from other Cisco IDS devices (such as IOS routers and PIX firewalls). You can add IOS Devices by selecting the IOS IDS radio button when adding a new device. Complete the following steps to add an IOS IDS device:

Step 1 Choose **Devices>Add**. The Select Device Type page is displayed.

Step 2 Select the **IOS IDS** radio button and click **Next**. The Enter Device Information page is displayed.

Step 3 Enter values for settings listed in the following table:

Security Monitor Device Information Settings	Description
IP Address	IP address of the security device.
NAT Address	NAT IP address of the IOS IDS device, required if the device is using NAT.
Device Name	Name of the security device.
Description	Optional.
Uses Postoffice check box	Check box that, if selected, allows you to enter PostOffice settings for a device.

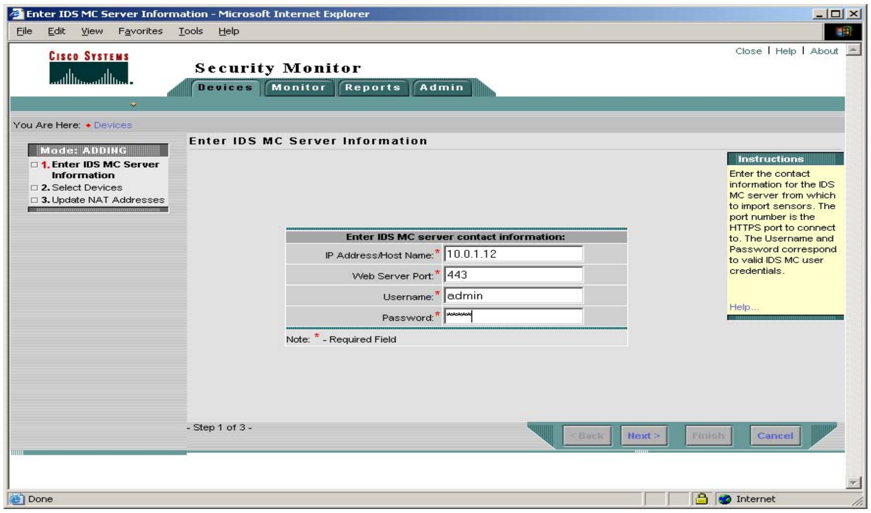
Step 4 Click **Finish**. The Devices page is displayed with the IOS IDS device.

The steps for adding a host IDS device and a PIX Firewall are similar steps to adding an IOS IDS device.

Devices—Import

Cisco.com

Choose Devices and Select Import**.**



Enter IDS MC Server Information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Close | Help | About
Security Monitor
Devices
Monitor
Reports
Admin
Done
Internet

You Are Here: ◆ Devices

Mode: ADDING

□ 1. Enter IDS MC Server Information
□ 2. Select Devices
□ 3. Update NAT Addresses

Enter IDS MC Server Information

Enter IDS MC server contact information:

IP Address/Host Name:* 10.0.1.12
Web Server Port:* 443
Username:* admin
Password:* *****

Note: * - Required Field

Instructions

Enter the contact information for the IDS MC server from which to import sensors. The port number is the HTTPS port to connect to. The Username and Password correspond to valid IDS MC user credentials.

Help...

- Step 1 of 3 -

< Back | Next > | Finish | Cancel

CSIDS 4.0—16-27

Instead of adding new devices by specifying all of the information necessary for Security Monitor to communicate with it, you can also import devices from an instance of IDS MC that is already monitoring the devices that you wish to add. Complete the following steps to import Sensors into the Security Monitor from a local or remote IDS MC server:

Step 1 Choose **Devices** and select **Import**. The Enter IDS MC Server Information page is displayed.

Step 2 Enter values for settings listed in the following table:

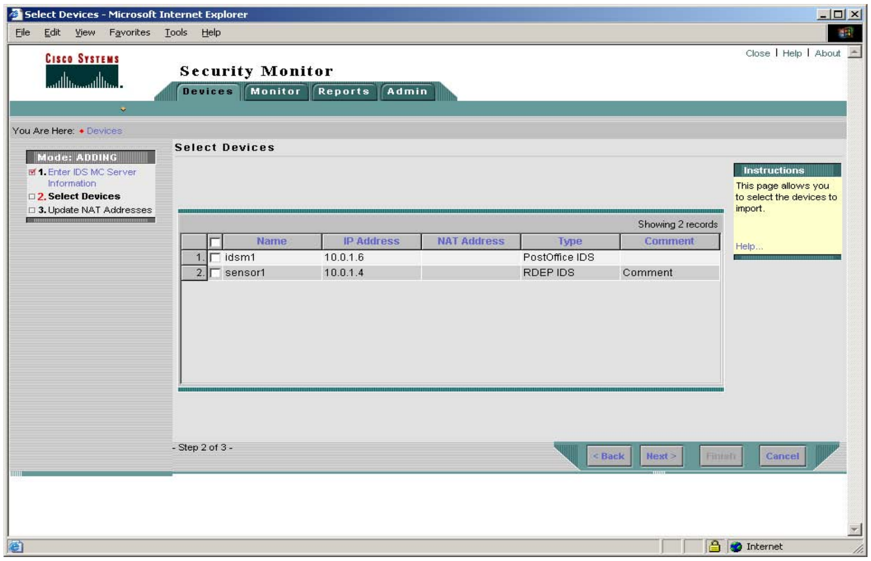
Security Monitor IDS MC Server Information Settings	Description
IP Address/Host Name	IP address or hostname of the IDS MC server.
Web Server Port	Web server port address over which communication between the Security Monitor and the IDS MC is to take place.
Username	Name of the user that will be used to log into the IDS MC.
Password	Password for the username.

Step 3 Click **Next**. The Select Devices page is displayed.

Note The Select Devices page may take awhile to appear, depending on the speed of your network.

Devices—Import (cont.)

Cisco.com


Select Devices - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
You Are Here: • Devices
Mode: ADDING
☑ 1. Enter IDS MC Server Information
□ 2. Select Devices
□ 3. Update NAT Addresses
Instructions
Help...
- Step 2 of 3 -
< Back Next > Finish Cancel
Internet

Select Devices

This page allows you to select the devices to import.

Showing 2 records

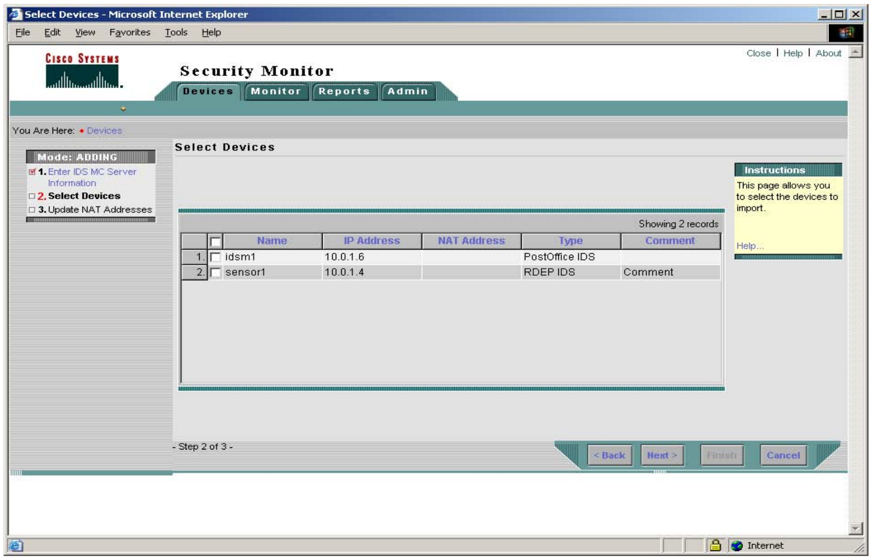
	□	Name	IP Address	NAT Address	Type	Comment
1.	□	idsm1	10.0.1.6		PostOffice IDS	
2.	□	sensor1	10.0.1.4		RDEP IDS	Comment

CSIDS 4.0—16-28

Step 4 Select the Sensors to import into the Security Monitor and click **Next**. The Update NAT addresses page is displayed.

Devices—Import (cont.)

Cisco.com



Select Devices

☒ 1. Enter IDS MC Server Information
□ 2. Select Devices
□ 3. Update NAT Addresses

This page allows you to select the devices to import.

Showing 2 records

	□	Name	IP Address	NAT Address	Type	Comment
1	□	idsm1	10.0.1.6		PostOffice IDS	
2	□	sensor1	10.0.1.4		RDEP IDS	Comment

- Step 2 of 3 -

CSIDS 4.0—16-29

Step 5 Enter the NAT addresses of the Sensors or IDSMs in the NAT Address field following the IP Address column, if applicable.

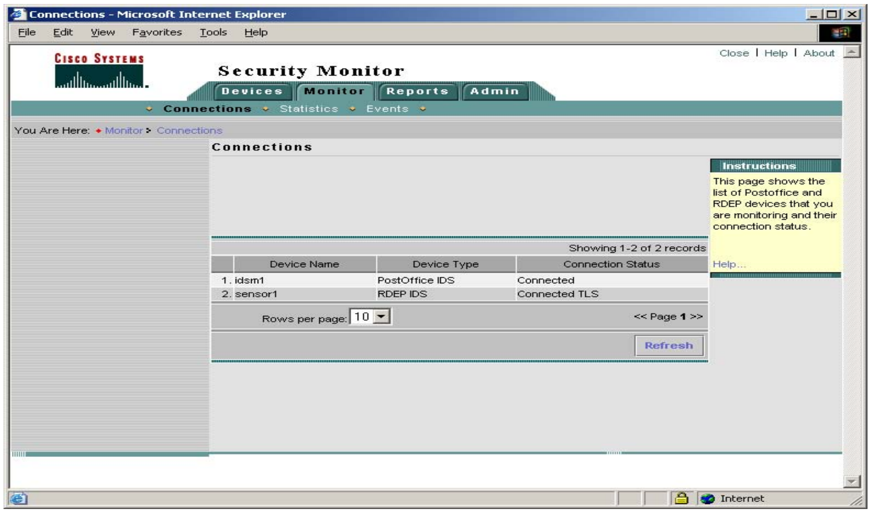
Step 6 Click **Finish**. The Summary page is displayed with the Import Status.

Step 7 Click **OK**. The Devices page is displayed with the new IDS devices.

Monitor—Connections

Cisco.com

Choose Monitor>Connections**.**


Connections - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices
Monitor
Reports
Admin
Connections
Statistics
Events
You Are Here: Monitor > Connections
Internet

Connections

Instructions

This page shows the list of Postoffice and RDEP devices that you are monitoring and their connection status.

Help...

Showing 1-2 of 2 records

	Device Name	Device Type	Connection Status
1.	idsm1	PostOffice IDS	Connected
2.	sensor1	RDEP IDS	Connected TLS

Rows per page: 10 << Page **1** >>

Refresh

CSIDS 4.0—16-30

You can monitor information about the devices that you have added to Security Monitor. This information falls into the following three categories:

- Connections
- Statistics
- Events

Monitoring connections—Security Monitor needs to communicate with all of the devices from which it receives information. With RDEP devices, Security Monitor actually connects to the sensor and retrieves the alerts. PostOffice devices actually send the information directly to Security Monitor. For RDEP and PostOffice devices, you can check the status of these connections using **Monitor>Connections**.

If the status is either "Connected" or "Connected TLS", then Security Monitor is receiving events from the device correctly. A status of "Not Connected" represents a problem and can indicate one of the following conditions:

- The device has been added to the Security Monitor, but is not yet configured to send event data. Configure the device to forward event data to the Security Monitor. This condition occurs when you configure the Security Monitor for a device that you plan to deploy later in your network.
- The device has been misconfigured. Make sure that the PostOffice or RDEP settings on the device are correct and that the events are being sent to the correct IP address, protocol, and port number.

- Security Monitor has been misconfigured. Make sure the settings in Security Monitor match those on the device. Also, make sure that NAT settings have been configured properly.

- Network connectivity between the device and Security Monitor has been lost. Try pinging the device from the Security Monitor server. CiscoWorks contains several diagnostic tools, including ping and traceroute, in the Server Configuration>Diagnostics>Connectivity Tools folder.

Note RDEP devices show additional connection information, such as the use of TLS.

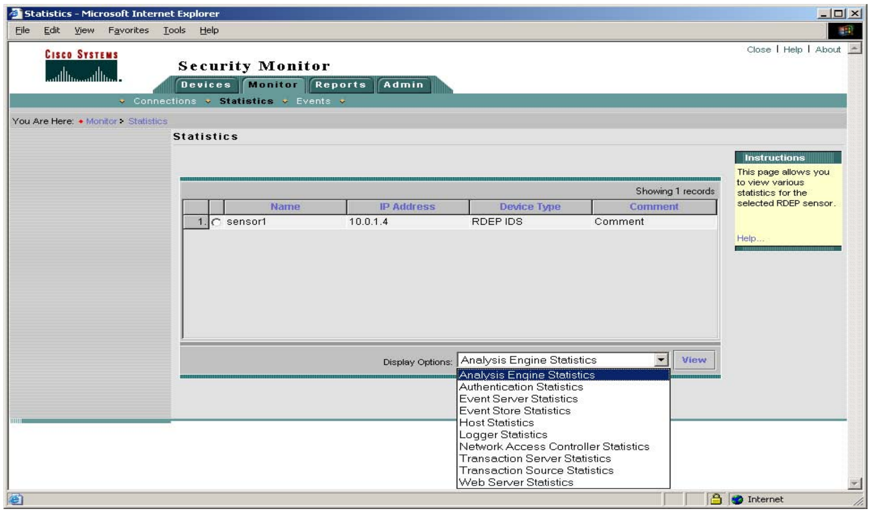
Choose **Monitor>Connections** to view the connection status of the IDS devices.

Note Only RDEP and PostOffice IDS devices will be displayed. IOS IDS devices (those not using PostOffice) and PIX firewalls, do not show up in the connection list since they send information to the Security Monitor in a connectionless fashion using Syslog messages.

Monitor—Statistics

Cisco.com

Choose Monitor>Statistics**.**



Statistics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Connections Statistics Events
You Are Here: Monitor > Statistics

Statistics

Showing 1 records

		Name	IP Address	Device Type	Comment
1.	○	sensor1	10.0.1.4	RDEP IDS	Comment

Display Options: Analysis Engine Statistics

View
Analysis Engine Statistics
Authentication Statistics
Event Server Statistics
Event Store Statistics
Host Statistics
Logger Statistics
Network Access Controller Statistics
Transaction Server Statistics
Transaction Source Statistics
Web Server Statistics
Internet

Instructions

This page allows you to view various statistics for the selected RDEP sensor.

Help...

CSIDS 4.0—16-31

Monitoring statistics—For your RDEP devices, you can view a wealth of statistical information about each device. Using the Monitor>Statistics window, you can view information about the following items:

- Analysis Engine Statistics—MAC, virtual Sensor, TCP stream reassembly, and signature database statistics.
- Authentication Statistics—Successful and failed login attempts to the RDEP device.
- Event Server Statistics—General and specific subscription information about the devices with connections to the server.
- Event Store Statistics—General and number of specific events that have occurred on the device.
- Host Statistics—Network statistics, memory usage, and swap file usage.
- Logger Statistics—Number of events, and log messages written by the Logger.
- Network Access Controller Statistics—Information about the sensor's current shunning (blocking) configuration.
- Transaction Server Statistics—Counts indicating the failed and total number of control transactions for the server.
- Transaction Source Statistics—Counts indicating the failed and total number of source control transactions.

- Web Server Statistics— Configuration information for the device web server and statistics for connections to the web server.

Complete the following steps to view statistical information about selected RDEP devices:

Step 1 Choose **Monitor>Statistics**. The Statistics page is displayed with the RDEP devices configured on the Security Monitor.

Step 2 Select the RDEP device for which you want to view the information by clicking the radio button next to the name of the sensor.

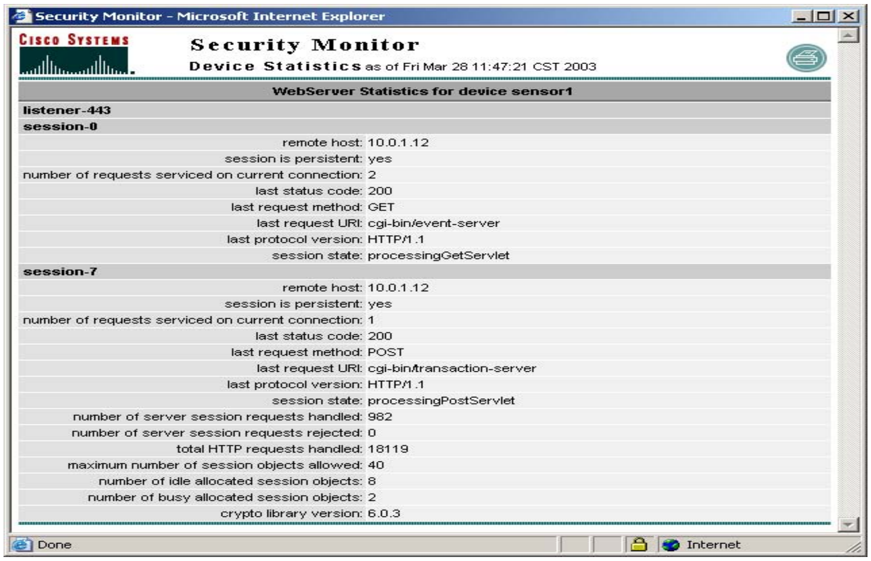
Step 3 Select statistics to view from the **Display Options** drop-down menu.

Step 4 Click **View**. A Security Monitor Device Statistics window opens and displays the requested statistical information.

Note You can view multiple statistical reports at a time since each of the reports is displayed in a new browser window. These reports are a snap shot of the information from the device and are not updated. To get updated information, you must generate another report.

Monitor—Statistics (cont.)

Cisco.com



Security Monitor

Device Statistics as of Fri Mar 28 11:47:21 CST 2003

WebServer Statistics for device sensor1

listener-443

session-0

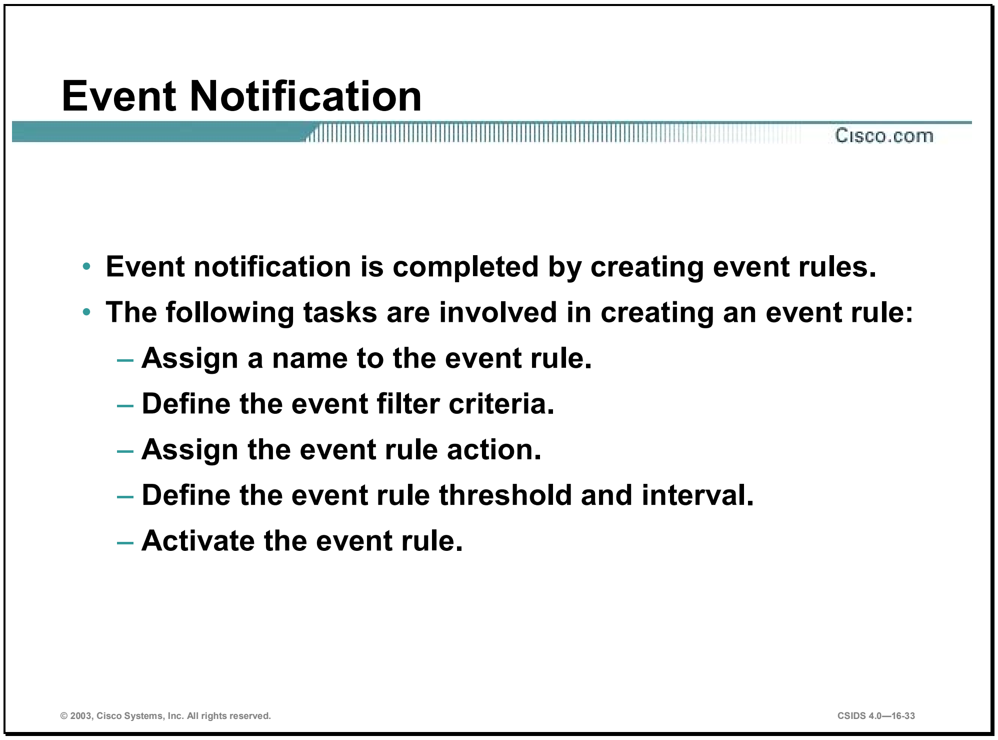
remote host: 10.0.1.12
session is persistent: yes
number of requests serviced on current connection: 2
last status code: 200
last request method: GET
last request URI: cgi-bin/event-server
last protocol version: HTTP/1.1
session state: processingGetServlet

session-7

remote host: 10.0.1.12
session is persistent: yes
number of requests serviced on current connection: 1
last status code: 200
last request method: POST
last request URI: cgi-bin/transaction-server
last protocol version: HTTP/1.1
session state: processingPostServlet
number of server session requests handled: 982
number of server session requests rejected: 0
total HTTP requests handled: 18119
maximum number of session objects allowed: 40
number of idle allocated session objects: 8
number of busy allocated session objects: 2
crypto library version: 6.0.3

CSIDS 4.0—16-32

Step 5 Click the printer icon in the upper right corner of the Security Monitor>Microsoft Internet Explorer window. A printable version of the Security Monitor>Microsoft Internet Explorer window appears that allows you to print the statistical report.



Event Notification

- Event notification is completed by creating event rules.
- The following tasks are involved in creating an event rule:
  - Assign a name to the event rule.
  - Define the event filter criteria.
  - Assign the event rule action.
  - Define the event rule threshold and interval.
  - Activate the event rule.

CSIDS 4.0—16-33

Monitoring Events—Finally, you can monitor the events that Security Monitor is receiving from all of the monitored devices. This is probably the most important feature of Security Monitor since it enables you to identify attacks against your network. You view the events that Security Monitor has collected through the Security Monitor Event Viewer which is accessed from **Monitor>Events**. Before the event viewer is launched, you need to specify the criteria on which alerts should be included in the display.

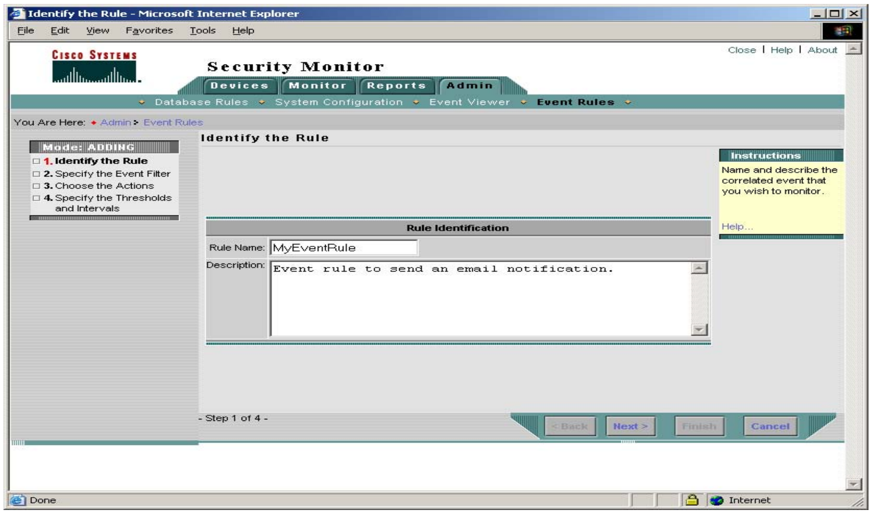
Event notification is accomplished by creating IDS MC event rules. The event rules specify the criteria that an event must meet to cause an action to occur. Complete the following tasks to create an event rule:

- Assign a name to the event rule.
- Define the event filter criteria.
- Assign the event rule action.
- Define the event rule threshold and interval.
- Activate the event rule.

Event Rules—Step 1

Cisco.com

Choose Admin>Event Rules>Add**.**



Identify the Rule

- □ 1. Identify the Rule
- □ 2. Specify the Event Filter
- □ 3. Choose the Actions
- □ 4. Specify the Thresholds and Intervals

Instructions

Name and describe the correlated event that you wish to monitor.

Help...

Rule Identification

Rule Name: MyEventRule

Description: Event rule to send an email notification.

- Step 1 of 4 -

< Back | Next > | Finish | Cancel

CSIDS 4.0—16-34

When one or more security devices are deployed to protect a network, they can generate large amounts of event data. Event rules enable you to define filters for the event data generated by your monitored devices and to specify an action to occur when filter conditions are met. Actions include sending an e-mail notification, logging a console notification to the audit log, and executing a script.

The steps for adding an event rule and editing an event rule are the same. Complete the following steps to add an event rule:

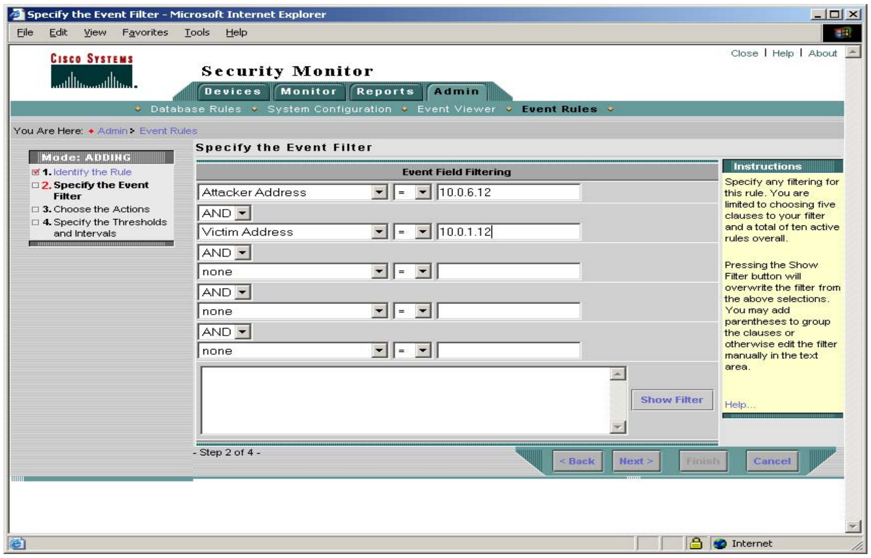
Step 1 Choose **Admin>Event Rules**. The Identify the Rule page is displayed.

Step 2 Enter a rule name in the Rule Name field. Optionally, enter a description in the Description field.

Step 3 Click **Next**. The Specify Event Filter page is displayed.

Event Rules—Step 2

Cisco.com



Specify the Event Filter

Event Field Filtering

Attacker Address = 10.0.6.12

AND

Victim Address = 10.0.1.12

AND

none =

AND

none =

AND

none =

Instructions

Specify any filtering for this rule. You are limited to choosing five clauses to your filter and a total of ten active rules overall.

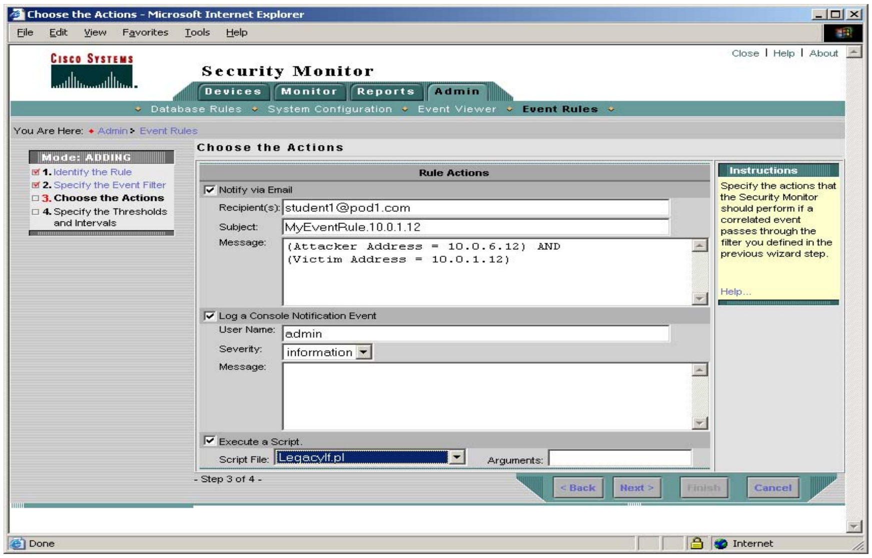
Pressing the Show Filter button will overwrite the filter from the above selections. You may add parentheses to group the clauses or otherwise edit the filter manually in the text area.

CSIDS 4.0—16-35

Step 4 Use the drop-down menu to choose the appropriate filter criteria and operators. The following options are available: Originating Device, Originating Device Address, Attack Address, Victim Address, Signature Name, Signature ID, and Severity. The following operators are available: <, <=, =, !=, >=, and >.

Step 5 Click **Next**. The Choose the Actions page is displayed.

Event Rules—Step 3



Choose the Actions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Database Rules System Configuration Event Viewer Event Rules
Done
Internet

You Are Here: Admin > Event Rules

Choose the Actions

Mode: ADDING

☑ 1. Identify the Rule
☑ 2. Specify the Event Filter
□ 3. Choose the Actions
□ 4. Specify the Thresholds and Intervals

Rule Actions

☑ Notify via Email

Recipient(s): student1@pod1.com

Subject: MyEventRule.10.0.1.12

Message:

```
(Attacker Address = 10.0.6.12) AND
(Victim Address = 10.0.1.12)
```

☑ Log a Console Notification Event

User Name: admin

Severity: information

Message:

☑ Execute a Script.

Script File: Legacylf.pl

Arguments:

- Step 3 of 4 -

< Back | Next > | Finish | Cancel

Instructions

Specify the actions that the Security Monitor should perform if a correlated event passes through the filter you defined in the previous wizard step.

Help...

CSIDS 4.0—16-36

Step 6 Enter values for settings listed in the following table:

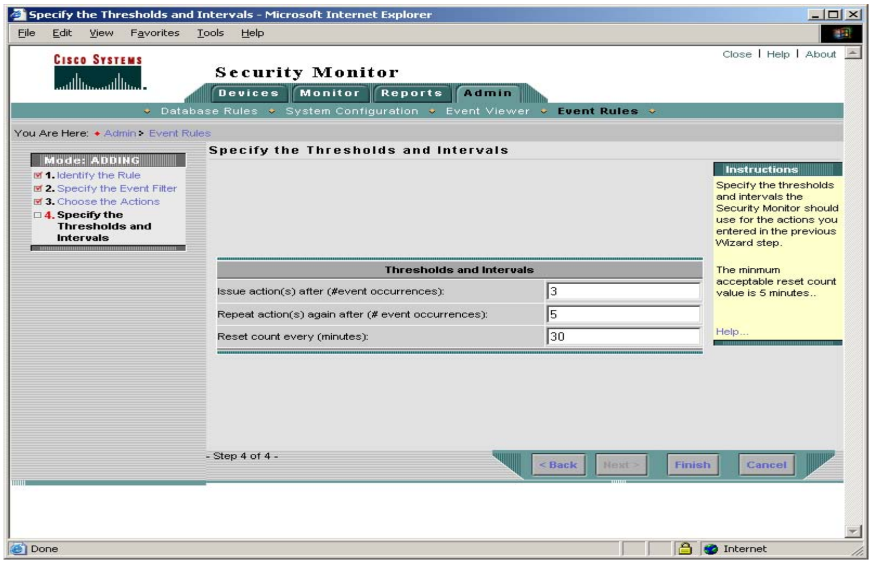
Security Monitor Rule Actions Settings	Description
Notify via Email	Check box that, if selected, enables the Security Monitor to send an e-mail when the database rule is triggered.
Recipients	People who receive an e-mail when the database rule is triggered, if the Notify via Email check box is selected. Separate multiple recipients with a comma.
Subject	Subject of the e-mail that a recipient receives when the database rule is triggered, if the Notify via Email check box is selected.
Message	Message of the e-mail that a recipient receives when the database rule is triggered, if the Notify via Email check box is selected.
Log a Console Notification Event	Check box that, if selected, enables the Security Monitor to log a notification report to the console when the database rule is triggered.
Subject	Subject of the notification report that is logged on the console when the database rule is triggered, if the Log a Console Notification Event check box is selected.
Message	Message of the notification report that is logged on the console when the database rule is triggered, if the Log a Console Notification Event check box is selected.
Execute a Script	Check box that, if selected, enables the Security Monitor to execute a script when the database rule is triggered.
Script File	Drop-down menu that enables you to choose from a list of scripts to execute when the database rule is triggered, if the Execute a Script check box is selected.

Security Monitor Rule Actions Settings	Description
Arguments	Additional arguments that can accompany a script that executes when the database rule is triggered, if the Execute a Script check box is selected.

Step 7 Click **Next**. The Specify the Thresholds and Intervals page is displayed.

Event Rules—Step 4

Cisco.com



Mode: ADDING

- ☒ **1.** Identify the Rule
- ☒ **2.** Specify the Event Filter
- ☒ **3.** Choose the Actions
- □ **4. Specify the Thresholds and Intervals**

Specify the Thresholds and Intervals

Thresholds and Intervals	
Issue action(s) after (#event occurrences):	3
Repeat action(s) again after (# event occurrences):	5
Reset count every (minutes):	30

Instructions

Specify the thresholds and intervals the Security Monitor should use for the actions you entered in the previous Wizard step.

The minmum acceptable reset count value is 5 minutes..

Help...

- Step 4 of 4 -

< Back | Next > | Finish | Cancel

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—16-37

Step 8 Enter the threshold in the Issue actions after field, the Repeat actions again after field, and the Reset count every field.

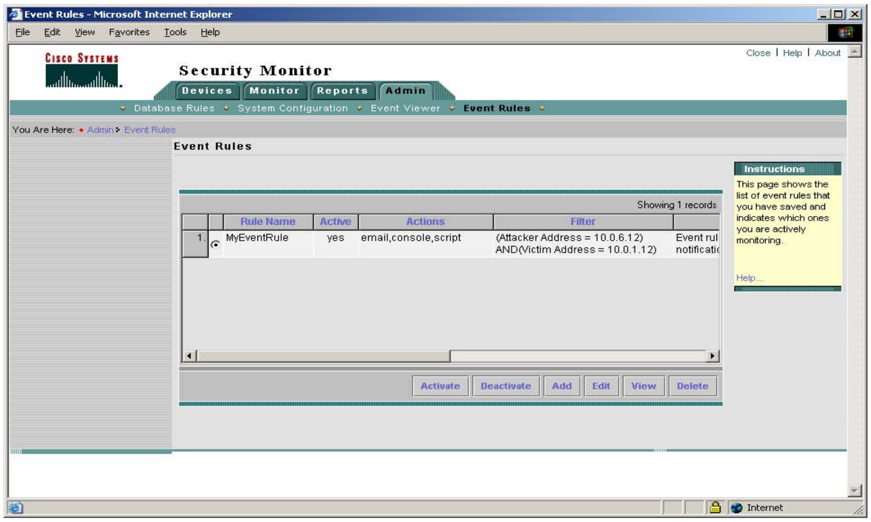
Step 9 Click **Finish**.

Note It is possible to execute scripts, against the Security Monitor database, other than those that accompany the Security Monitor. To install and use a newly created script, place the script in the default directory of the Security Monitor within the following sub-directory: \CSCOpx\MDC\etc\ids\scripts. Running some scripts against the Security Monitor database can result in unknown results. Therefore, use scripts with caution. In addition, you can edit an event rule that is currently activated. However, if your edits make the event rule invalid, the rule is automatically deactivated.

Event Rules—Activation

Cisco.com

Choose Admin>Event Rules>Activate**.**



Event Rules - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Database Rules System Configuration Event Viewer Event Rules
You Are Here: Admin > Event Rules
Activate Deactivate Add Edit View Delete
Internet

Event Rules

Showing 1 records

		Rule Name	Active	Actions	Filter	
1.	●	MyEventRule	yes	email,console,script	(Attacker Address = 10.0.6.12) AND(Victim Address = 10.0.1.12)	Event rul notificatic

Instructions

This page shows the list of event rules that you have saved and indicates which ones you are actively monitoring.

Help...

CSIDS 4.0—16-38

An event rule must be activated before the actions you specified in an event rule can occur. You can have up to ten activated event rules and each event rule can have as many as five clauses. Complete the following steps to activate an event rule:

Step 1 Choose **Admin>Event Rules**. The Event Rules page is displayed.

Step 2 Select the event that is to be activated and click **Activate**.

Note If the event rule does not contain an event filter and an action, you cannot activate it, and you will receive an error message when you attempt to activate it. Edit the event rule to complete the missing fields, and then activate it.

Complete the following steps to deactivate an event rule:

Step 1 Choose **Admin>Event Rules**. The Event Rules page is displayed.

Step 2 Select the event to activate and click **Deactivate**.

Note If an event rule is active, a check mark appears in the Active column on the Event Rules page.

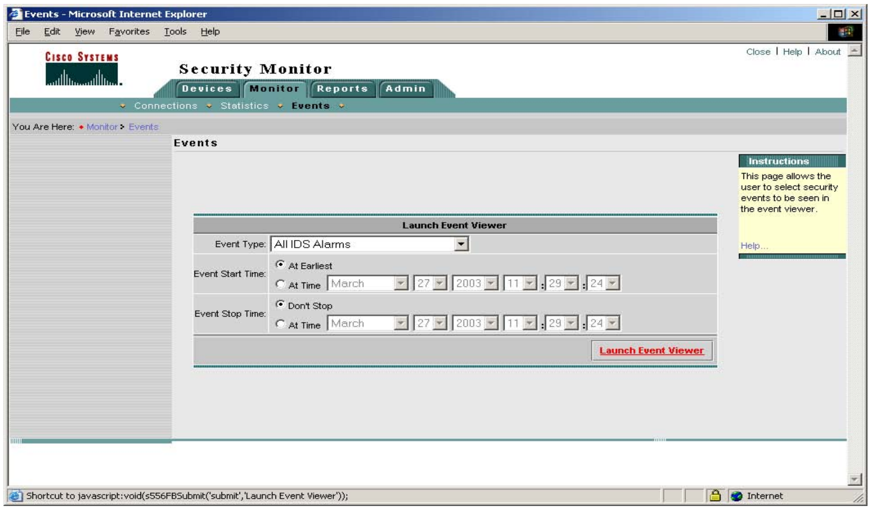
Security Monitor Event Viewer

This section discusses the Security Monitor's event viewing and reporting features.

Security Monitor—Event Viewer

Cisco.com

Choose Monitor>Events**.**



This page allows the user to select security events to be seen in the event viewer.

Launch Event Viewer

Event Type: All IDS Alarms

Event Start Time: ● At Earliest ○ At Time March 27 2003 11 : 29 : 24

Event Stop Time: ● Don't Stop ○ At Time March 27 2003 11 : 29 : 24

Shortcut to javascript:void(s556FBSubmit('submit','Launch Event Viewer'));

CSIDS 4.0—16-41

The Event Viewer combines the functionality of a spreadsheet with that of a hierarchical, drill-down directory to create a collection of event records called a drillsheet (a drill-down spreadsheet). The drillsheet displays groups of similar event records on a single row of a grid, enabling you to detect patterns in the data.

The Event Viewer contains a grid plane that organizes and displays event records. The Event Viewer can read and displays both real-time and historical events from the Security Monitor database. You can configure the grid plane to display information about alerts detected by the monitored devices in a variety of ways, thereby customizing the interface to your requirements.

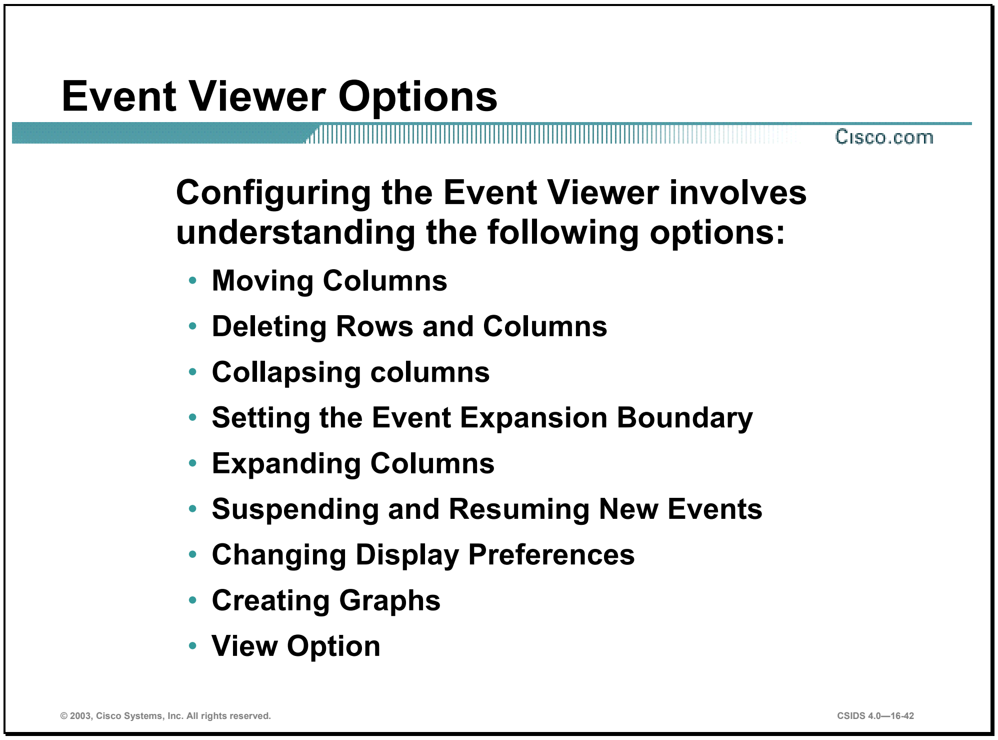
Complete the following steps to view select security events in the Event Viewer:

Step 1 Choose **Monitor>Events**. The Events page is displayed.

Step 2 Choose an Event Type from the Event type drop-down menu.

Step 3 Select the Event Start Time and Event Stop Time to view security events.

Step 4 Click **Launch Event Viewer**. The Event Viewer page is displayed.



Event Viewer Options

Configuring the Event Viewer involves understanding the following options:

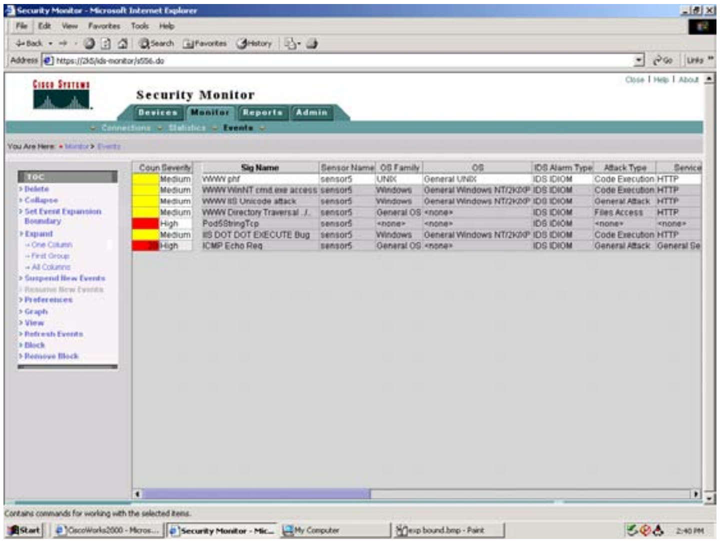
- **Moving Columns**
- **Deleting Rows and Columns**
- **Collapsing columns**
- **Setting the Event Expansion Boundary**
- **Expanding Columns**
- **Suspending and Resuming New Events**
- **Changing Display Preferences**
- **Creating Graphs**
- **View Option**

CSIDS 4.0—16-42

Configuring the Event Viewer involves understanding the following options:

- Moving Columns—To change the default order of fields within an alarm entry.
- Deleting Rows and Columns—To remove an alarm from the Event Viewer grid, columns or from the actual Security Monitor database.
- Collapsing columns—To reduce the number of lines displayed on the Event Viewer grid.
- Setting the Event Expansion Boundary—To automatically expand more fields than the default.
- Expanding Columns—To expand the amount of alarm detail shown on the Event Viewer grid.
- Suspending and Resuming New Events—Provides the capability to suspend and resume the Event Viewer from displaying new alarms.
- Changing Display Preferences—Provides different preference settings that you can use to customize in the Event Viewer.
- Creating Graphs—To create a graph of the data, or a subset of the data, shown in Event Viewer.
- View Option—Enables you to access Context Buffer, Host Names, Network Security Database and Statistics.

Event Viewer—Moving Columns


Security Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://2k5/ids-monitor/s556.do
Close | Help | About
Security Monitor
Devices
Monitor
Reports
Admin
Connections
Statistics
Events
You Are Here: Monitor > Events
TOC
Delete
Collapse
Set Event Expansion Boundary
Expand
One Column
First Group
All Columns
Suspend New Events
Resume New Events
Preferences
Graph
View
Refresh Events
Block
Remove Block
Contains commands for working with the selected items.
Start
CiscoWorks2000 - Micros...
Security Monitor - Mic...
My Computer
exp bound.bmp - Paint
2:40 PM

Coun	Severity	Sig Name	Sensor Name	OS Family	OS	IDS Alarm Type	Attack Type	Service
🟨	Medium	WWW phf	sensor5	UNIX	General UNIX	IDS IDIOM	Code Execution	HTTP
🟨	Medium	WWW WinNT cmd.exe access	sensor5	Windows	General Windows NT/2K/XP	IDS IDIOM	Code Execution	HTTP
🟨	Medium	WWW IIS Unicode attack	sensor5	Windows	General Windows NT/2K/XP	IDS IDIOM	General Attack	HTTP
🟨	Medium	WWW Directory Traversal ../	sensor5	General OS	<none>	IDS IDIOM	Files Access	HTTP
🟥	High	Pod5StringTcp	sensor5	<none>	<none>	IDS IDIOM	<none>	<none>
🟨	Medium	IIS DOT DOT EXECUTE Bug	sensor5	Windows	General Windows NT/2K/XP	IDS IDIOM	Code Execution	HTTP
🟥 20	High	ICMP Echo Req	sensor5	General OS	<none>	IDS IDIOM	General Attack	General Se

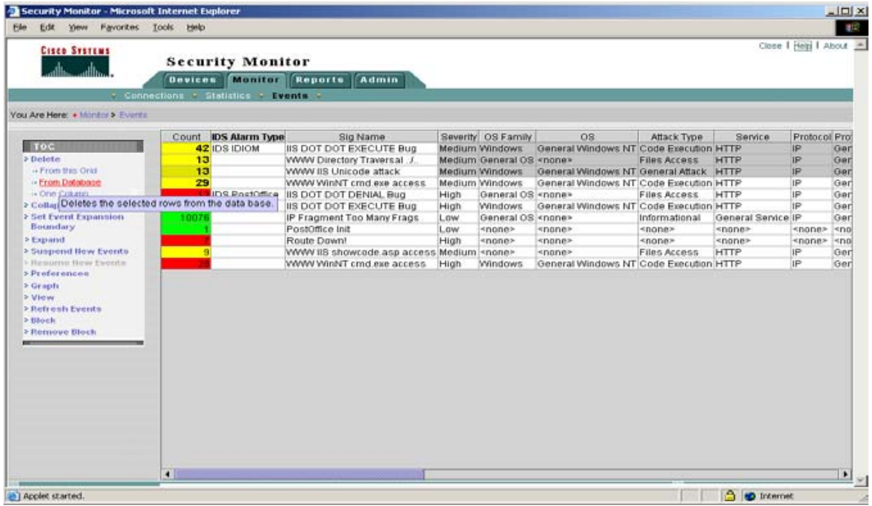
CSIDS 4.0—16-43

Moving Columns—The default order of fields within an alarm entry may not suite your operational environment. You can change the order that the columns are displayed in the Event Viewer. To move a column, click-and-drag the column header of the column that you want to move to the new position where you want it to be.

Note This is not a persistent change. This means that closing the Event Viewer and re-opening it will bring back the default column ordering.

Event Viewer—Deleting Rows and Columns

Choose Monitor>Events>Delete**.**



Count	IDS Alarm Type	Sig Name	Severity	OS Family	OS	Attack Type	Service	Protocol	Pro
42	IDS IDIOM	IIS DOT DOT EXECUTE Bug	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
13		WWW Directory Traversal ../	Medium	General OS	<none>	Files Access	HTTP	IP	Ger
13		WWW IIS Unicode attack	Medium	Windows	General Windows NT	General Attack	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
17	IDS PostOffice	IIS DOT DOT DENIAL Bug	High	General OS	<none>	Files Access	HTTP	IP	Ger
[illegible]		IIS DOT DOT EXECUTE Bug	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
10076		IP Fragment Too Many Frags	Low	General OS	<none>	Informational	General Service	IP	Ger
1		PostOffice Init	Low	<none>	<none>	<none>	<none>	<none>	<no
7		Route Down!	High	<none>	<none>	<none>	<none>	<none>	<no
9		WWW IIS showcode.asp access	Medium	<none>	<none>	Files Access	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger

CSIDS 4.0—16-44

You access the delete options by clicking on **Delete** in the TOC. The Event Viewer offers three The following delete options are available:

- Delete>From This Grid—To remove a row from the Event Viewer display, you select a specific row by clicking on a field in the row to be deleted. Then clicking on the **From This Grid** TOC option will delete the alarms from the Event Viewer where the action is being performed. It will not delete alarms from other Event Viewer instances or the Security Monitor database.

Complete the following steps to delete a security event from the current Event Viewer grid:

Step 1 Select a security event that you want to delete from the Event Viewer grid.

Step 2 Select **Delete** from the Event Viewer TOC. The Delete options are displayed.

Step 3 Select **From this Grid**. The Event Viewer Delete Events From Grid window opens.

Step 4 Click **Yes** if you want to continue with the deletion of the event from the current Event Viewer grid.

- Delete>From Database—To remove a row from the Security Monitor database, you select the specific row by clicking on a field in the row to be deleted. Then, clicking on the **From Database** TOC option deletes the selected alarm events from all of the open Event Viewers as well as the Security Monitor database. If you use this option, the alarm is completely gone and you may not display it in the Event Viewer again, even if you open another Event Viewer instance.

Complete the following steps to delete a security event from the database:

Step 1 Select a security event that you want to delete from the Event Viewer grid.

Step 2 Select **Delete** from the Event Viewer TOC. The Delete options are displayed.

Step 3 Select **From the Database**. The Event Viewer Delete Events from database window opens.

Step 4 Click **Yes** if you want to continue with the deletion of the event from the database.

- Delete>One Column—To remove columns from the Event Viewer display, you select a specific column by clicking on a field in that column. Then clicking on the **One Column** TOC option removes the selected column from the Event Viewer display.

Complete the following steps to delete a column:

Step 1 Select a column to delete from the Event Viewer grid.

Step 2 Select **Delete** from the Event Viewer TOC. The Delete options are displayed.

Step 3 Select **One Column**. The Event Viewer Delete Column window opens.

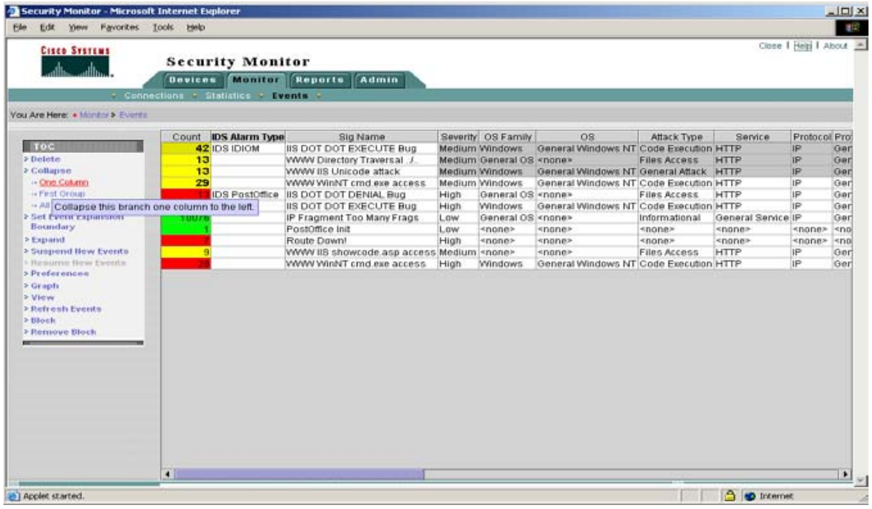
Step 4 Click **Yes** if you want to continue with the deletion of the event from the database.

Note The Sensor Name, Org Name, and Source Address fields are required for the block feature.

Event Viewer—Collapsing Columns

Cisco.com

Choose Monitor>Events>Collapse**.**



Count	IDS Alarm Type	Sig Name	Severity	OS Family	OS	Attack Type	Service	Protocol	Pro
42	IDS IDIOM	IIS DOT DOT EXECUTE Bug	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
13		WWW Directory Traversal ../	Medium	General OS	<none>	Files Access	HTTP	IP	Ger
13		WWW IIS Unicode attack	Medium	Windows	General Windows NT	General Attack	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
[illegible]	IDS PostOffice	IIS DOT DOT DENIAL Bug	High	General OS	<none>	Files Access	HTTP	IP	Ger
		IIS DOT DOT EXECUTE Bug	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
10076		IP Fragment Too Many Frags	Low	General OS	<none>	Informational	General Service	IP	Ger
1		PostOffice Init	Low	<none>	<none>	<none>	<none>	<none>	<no
7		Route Down!	High	<none>	<none>	<none>	<none>	<none>	<no
9		WWW IIS showcode.asp access	Medium	<none>	<none>	Files Access	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger

CSIDS 4.0—16-45

Collapsing columns—To reduce the number of lines displayed on the Event Viewer grid, multiple alarms are collapsed into a single row based on a specific number of fields (known as the Expansion Boundary). By default, the Expansion Boundary is only the first field. All alarm entries with the same value for the first field are consolidated into a single row on the Event Viewer display. To examine specific alarms, you may expand the display so that only a few alarms are consolidated on each row in the Event Viewer display. Although this is helpful when analyzing a specific attack, the Event Viewer grid can quickly become cluttered with more alarms than you can manage. When your Event Viewer display is too cluttered, you can collapse the display so that multiple alarms are consolidated onto a single line.

You have the following three options to collapse rows in the Event Viewer:

- Collapse>One Column—To consolidate alarm details, you must collapse the columns until only the fields that you are interested in are expanded. When you collapse columns, however, the process begins with the column (that is not already collapsed) farthest to the right on the Event Viewer display. You can't collapse specific columns only. To collapse one column, select the row that you want to consolidate and then click **Collapse>One Column** from the TOC.

- Collapse>First Group—The Event Viewer display contains numerous columns. If you happen to have expanded all columns (so that each row in the display represents a single alarm entry), you can use the Collapse>One Column TOC option many times without any visual effect (since you are collapsing columns on the far right end of the Event Viewer display). Using the **Collapse>First Group** TOC option, you can quickly collapse a selected row to the first row that causes some consolidation to occur (a reduction in the number of lines displayed in the Event Viewer).

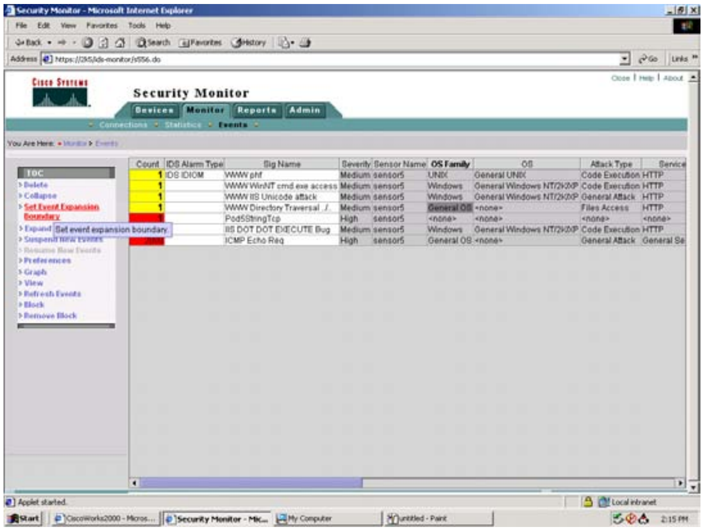
- Collapse>All Columns—The **Collapse>All Columns** TOC option enables you to quickly consolidate all of the alarm entries based on the first column in the Event Viewer display.

Note These options are not persistent changes. This means that closing the Event Viewer and re-opening it will bring back the default settings and expansion boundary.

Choose **Monitor>Events>Collapse** to collapse event columns.

Event Viewer—Setting the Event Expansion Boundary

Cisco.com



Count	IDS Alarm Type	Sig Name	Severity	Sensor Name	**OS Family**	OS	Attack Type	Service
1	IDS IDIOM	WWW phf	Medium	sensor5	UNIX	General UNIX	Code Execution	HTTP
1		WWW WinNT cmd.exe access	Medium	sensor5	Windows	General Windows NT/2K/XP	Code Execution	HTTP
1		WWW IIS Unicode attack	Medium	sensor5	Windows	General Windows NT/2K/XP	General Attack	HTTP
1		WWW Directory Traversal ../	Medium	sensor5	General OS	<none>	Files Access	HTTP
1		Pod5StringTcp	High	sensor5	<none>	<none>	<none>	<none>
[illegible]		IIS DOT DOT EXECUTE Bug	Medium	sensor5	Windows	General Windows NT/2K/XP	Code Execution	HTTP
[illegible]		ICMP Echo Req	High	sensor5	General OS	<none>	General Attack	General Se

CSIDS 4.0—16-46

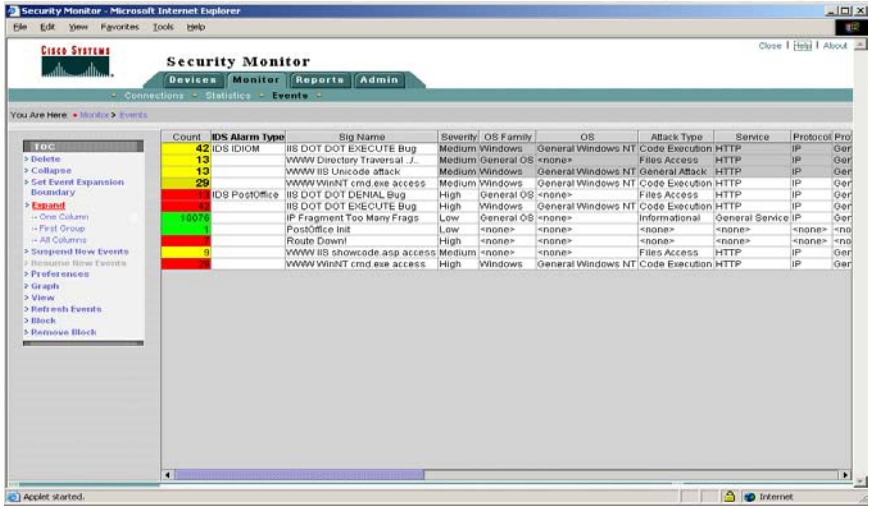
Setting the Event Expansion Boundary—By default, the Event Viewer expands the first column of the grid. If you want to automatically expand more fields than this, you need to change the Expansion Boundary. To change the expansion boundary for the current instance of the Event Viewer, you need to click on a field in the column where you want the expansion boundary to end. Then click **Set Event Expansion Boundary** from the TOC. The new expansion boundary is indicated by the column name becoming bold.

The Expansion Boundary represents the block of columns that will be automatically expanded when a new alarm entry comes into the table. The block of columns is contiguous and starts at the first column in the Event Viewer. By default the Expansion Boundary expands the first field of an alarm entry. When setting a new Expansion Boundary, you only have to specify the last column to be expanded. All columns from the first column to the column that you specify will now be expanded for new alarm entries.

Event Viewer—Expanding Columns

Cisco.com

Choose Monitor>Events>Expand**.**



Count	IDS Alarm Type	Sig Name	Severity	OS Family	OS	Attack Type	Service	Protocol	Pro
42	IDS IDIOM	IIS DOT DOT EXECUTE Bug	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
13		WWW Directory Traversal ./..	Medium	General OS	<none>	Files Access	HTTP	IP	Ger
13		WWW IIS Unicode attack	Medium	Windows	General Windows NT	General Attack	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
13	IDS PostOffice	IIS DOT DOT DENIAL Bug	High	General OS	<none>	Files Access	HTTP	IP	Ger
42		IIS DOT DOT EXECUTE Bug	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
10076		IP Fragment Too Many Frags	Low	General OS	<none>	Informational	General Service	IP	Ger
1		PostOffice Init	Low	<none>	<none>	<none>	<none>	<none>	<no
7		Route Down!	High	<none>	<none>	<none>	<none>	<none>	<no
9		WWW IIS showcode.asp access	Medium	<none>	<none>	Files Access	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger

CSIDS 4.0—16-47

Expanding Columns—Besides collapsing the entries on the display, you frequently need to expand the amount of alarm detail shown on the Event Viewer grid. Expanding columns provides more information and causes more rows to be displayed in the Event Viewer. When expanding columns, you have the following three options:

- Expand>One Column—By default, the Event Viewer consolidates or “collapses” alarms based on the first column. The rest of the fields in the alarm entry have a gray background to indicate that they have been collapsed (the collapsed fields may indicate actual field values or a ‘+’). To view these collapsed fields, you must expand the collapsed columns until the fields that you are interested in are shown. To expand fields one column at a time, select the row that you want to expand and then click **Expand>One Column** from the TOC.

Note When expanding columns in your Event Viewer, you will eventually increase the number of row entries being displayed. The count field shows you how many entries are consolidated into a single row in the Event Viewer. This consolidation is based on the columns that are currently expanded. As you expand fields, less of the alarm entries will have the same values for all of the expanded columns. When you expand all of the columns, each row will probably only represent one alarm entry (count equal to 1), since it is unlikely that two separate alarm entries will have the exact same values for every column.

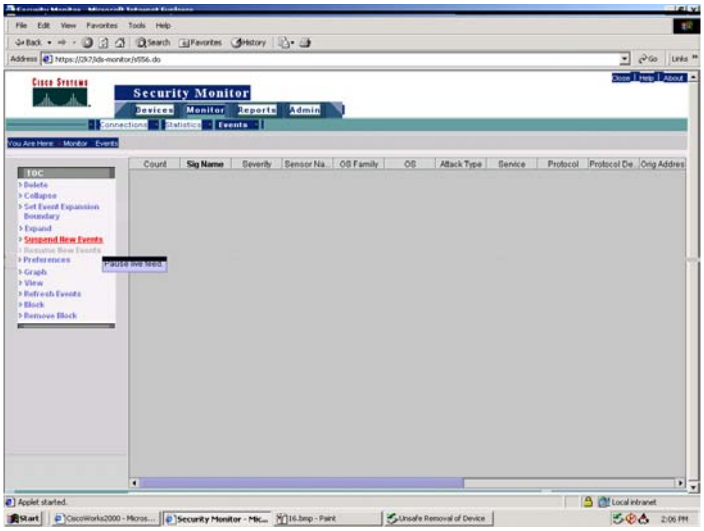
- Expand>First Group—Instead of expanding columns one at a time, you can click **Expand>First Group** from the TOC. This option expands the fields until the first field that causes more rows to be displayed. This is much easier than expanding columns one at a time.

- Expand>All Columns—Expanding an alarm entry one row at a time can be tedious, especially if the column that you are interested in is many fields away. In one click you can expand all of the fields for the currently selected row. To expand all of the columns for the current alarm entry, click **Expand>All Columns** from the TOC.

Note This is not a persistent change. This means that closing the Event Viewer and re-opening it will bring back the default settings and expansion boundary.

Choose **Monitor>Events>Expand** to expand event columns.

Event Viewer—Suspending and Resuming New Events


File Edit View Favorites Tools Help
Back Search Favorites History
Address https://2k7/ids-monitor/s556.do
Go Links
Close Help About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Connections Statistics Events
You Are Here › Monitor › Events
TOC
Delete
Collapse
Set Event Expansion Boundary
Expand
Suspend New Events
Resume New Events
Preferences
Graph
View
Refresh Events
Block
Remove Block
Pause live feed.
Applet started.
Local intranet
Start
CiscoWorks2000 - Micros...
Security Monitor - Mic...
16.bmp - Paint
Unsafe Removal of Device
2:06 PM

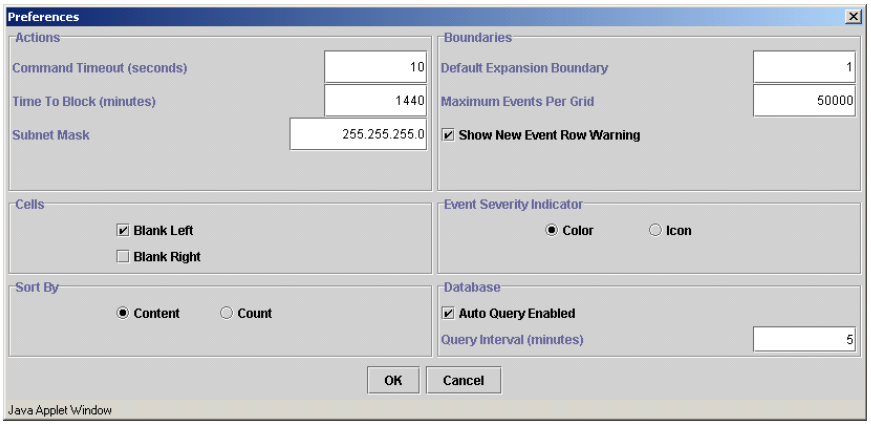
Count	Sig Name	Severity	Sensor Na..	OS Family	OS	Attack Type	Service	Protocol	Protocol De..	Orig Addres

Suspending and Resuming New Events—Sometimes you may want to freeze the Event Viewer display and temporarily not display any more alarms. This might happen during a flood of alarms. If alarms keep updating the Event Viewer, you may have difficulty analyzing what is happening. At that point, it is nice to freeze your Event Viewer window so that you can research the alarms that you already have in your window.

Security Monitor provides you the capability to suspend the Event Viewer from displaying new alarms. To suspend the Event Viewer, choose **Suspend New Events** from the TOC. To resume alarms, choose **Resume New Events** from the TOC. Only one of the options is available at a time. For instance, when you have suspended alarms, the resume option becomes available (it is no longer grayed out). Furthermore, suspending alarms does not prevent new alarms from being added to the Security Monitor database. It only prevents them from being displayed in your current Event Viewer.

Event Viewer—Changing Display Preferences

Choose Monitor>Events>Preferences**.**



Preferences

Actions

Command Timeout (seconds): 10

Time To Block (minutes): 1440

Subnet Mask: 255.255.255.0

Boundaries

Default Expansion Boundary: 1

Maximum Events Per Grid: 50000

☑ Show New Event Row Warning

Cells

☑ Blank Left

☐ Blank Right

Event Severity Indicator

● Color ○ Icon

Sort By

● Content ○ Count

Database

☑ Auto Query Enabled

Query Interval (minutes): 5

Changing Display Preferences—This section describes the different preference settings that you can use to customize in the Event Viewer. To access the Preferences window you need to click on **Preferences** from TOC. This will display the Preferences popup window. These settings fall into six basic categories:

- Actions—The Actions group box in the Preference window allows you to set the following values:

  - Command Timeout—The Command Timeout determines how long, in seconds, the Event Viewer will wait for a response from the Sensor before it concludes that it has lost communication with the Sensor. In most cases, you will not need to modify this value. If you find that you are experiencing frequent Command Timeout errors, then you might consider increasing the Command Timeout value or diagnosing the reason that your Event Viewer is experiencing such a slow response time.The Command Timeout value applies to all functions that require communication through the PostOffice infrastructure. For example, functions such as retrieving Sensor statistics, viewing Sensor block lists, and requesting that the Sensor blocks a particular IP address all must be completed within the the Command Timeout. This timeout value is not used for non-PostOffice functions, such as DNS queries. The default value is 10 seconds, with an allowable range between 1 and 3,600 seconds (one hour).

  - Time To Block—The Time to Block specifies how long (in minutes) the Sensor blocks traffic from the specified source when you issue a Block command from the Event Viewer. The block duration value that can be specified for the Sensor in the Network Topology Tree (NTT) applies only to blocks that are generated automatically by that Sensor. The Time to Block value in the Preferences dialog box applies only to manually generated blocks from the Event Viewer. The default value is 1440 minutes (one day). The allowable range is from 1 to 525,600 minutes (one year).

- Subnet Mask—The Subnet Mask is used to define the network portion of the IP address that will be used to block a range of addresses. Your Sensors use this information when they publish a blocking rule to the blocking devices on your network. The Subnet Mask is only applied to the to the Block>Network and Remove Block>Network options from the Event Viewer. The default value is 255.255.255.0 represents a class C address range.

- Cells—The Blank Left and Blank Right check boxes in the Cells section of the Preference window enable you to specify whether certain cells will be blank or filled in:
  - Blank Left—Choosing the Blank Left check box controls whether values that are suggested by a cell above a row are filled in on following rows in the Event Viewer.
  - Blank Right—Choosing Blank Right affects how the collapsed cells are displayed in the Event Viewer. When cells are collapsed their background color is gray and if the collapsed values are different a "+" sign is displayed. When Blank Right is selected, a '+' sign is displayed in a collapsed cell regardless of whether or not the cell values are different. The default setting is for Blank Right not to be selected. In this state, a plus sign is only displayed in collapsed cells if the values in the cells differ. If the values in the collapsed cell are the same, then the actual value is displayed in the Event Viewer.

- Sort By—The Sort By group box in the Preferences enables you to specify how the events are sorted in the Event Viewer. You can choose from the following two options:
  - Count—When sorting by Count, the entries in the Event Viewer are sorted by the count of alarms listed in the first column of each row.
  - Content—If you sort by Content, then the entries in the Event Viewer are sorted alphabetically by the first field that is unique (starting with the first field and moving to the right until a differing field value is found).

- Boundaries—The Boundaries group box in the Preferences window enables you to set the following values:
  - Default Expansion Boundary—The Default Expansion Boundary specifies the default number of columns in which the cells of a new event are expanded. By default, only the first field of an event is expanded.
  - Maximum Events Per Grid—The Maximum Events Per Grid defines the maximum number of alarms that can be displayed in a single Event Viewer. When the maximum value is reached, an error message is displayed. The default value is 50,000 alarms.

- Event Severity Indicator—There are two Severity Indicator options that you can select from:
  - Color—The default setting is for the severity to be indicated in the Event Viewer with colors. The color affects the background of the Count field. The following colors are used to indicate alarm severity: High severity displayed in red, Medium severity displayed in yellow and Low severity displayed in green.
  - Icon—Besides the default color severity indicator, you can also choose to display the severity of your alarms using icons. The icons used to display alarm severity are: High severity is a red exclamation point, Medium severity is a yellow flag and Low severity receives no icon.
- Database—The Database group box in the Preferences window enables you configure whether the Event Viewer automatically retrieves new events from the Security Monitor database. If you check the **Auto Query Enabled** checkbox, then you can configure how often the Event Viewer automatically retrieves events from the Security Monitor Database.

Note You can manually retrieve new events from the Security Monitor database by clicking **Refresh Events** from the TOC.

Note The display preferences specified using this option are not persistent. They are lost once you close the Event Viewer. To make persistent changes to your display preferences, refer to “Defining Event Viewer Preferences” later in this chapter.

Complete the following steps to modify the Event Viewer preferences:

Note The preferences are for the user currently using the Event Viewer. Each VMS user can have their own Event Viewer preferences.

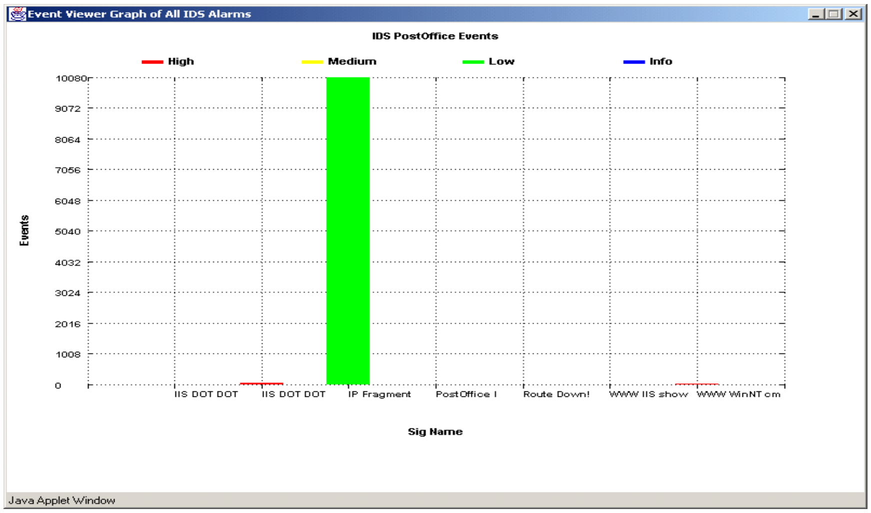
Step 1 Select **Preferences** from the Event Viewer TOC. The Preferences page opens.

Step 2 Enter values for settings (discussed above).

Step 3 Click **OK** to close the Preferences page.

Event Viewer—Creating Graph

Choose Monitor>Events>Graph**.**



CSIDS 4.0—16-50

Creating Graphs—You can create a graph of the data, or a subset of the data, shown in Event Viewer. The graphs represent a static snapshot of the information and are not updated dynamically. Choose **Graph>By Child**. The Graph of Child items is displayed in another window.

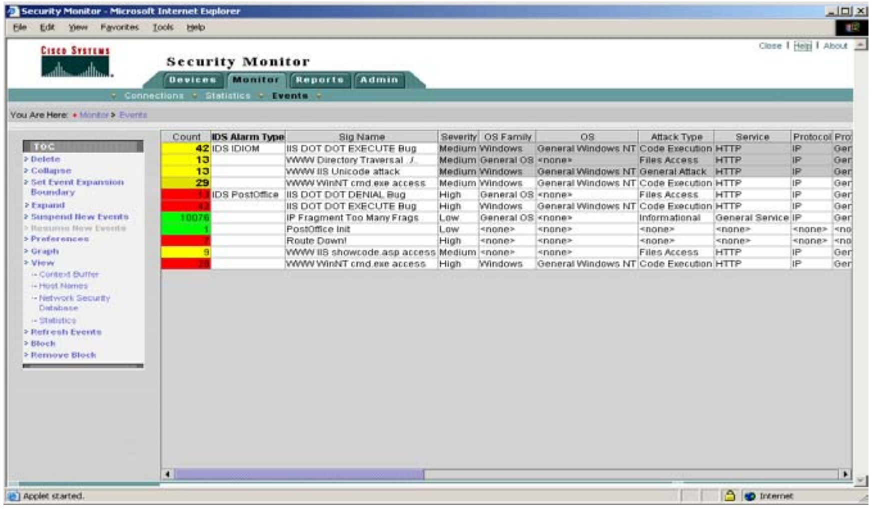
You can choose from the following two types of graphs:

- By Child—To see the distribution of children events, select **Graph>By Child** from the TOC. The graph displays the child events (the events in the column to the right of the selected node) across the X-axis of the graph and the number of occurrences along the Y-axis. Event severity is indicated by the color of the bar.

- By Time—To see how the selected events were distributed over time, select **Graph>By Time** from the TOC. The graph displays along the x-axis the range of time over which the event occurred; along the y-axis the number of occurrences. Event severity is indicated by the color of the bar.

Event Viewer—View Option

Choose Monitor>Events>View.


Security Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Connections Statistics Events
You Are Here: Monitor > Events
TOC
Delete
Collapse
Set Event Expansion Boundary
Expand
Suspend New Events
Resume New Events
Preferences
Graph
View
Context Buffer
Host Names
Network Security Database
Statistics
Refresh Events
Block
Remove Block
Applet started.
Internet

Count	IDS Alarm Type	Sig Name	Severity	OS Family	OS	Attack Type	Service	Protocol	Pro
42	IDS IDIOM	IIS DOT DOT EXECUTE Bug	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
13		WWW Directory Traversal ./.	Medium	General OS	<none>	Files Access	HTTP	IP	Ger
13		WWW IIS Unicode attack	Medium	Windows	General Windows NT	General Attack	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	Medium	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
13	IDS PostOffice	IIS DOT DOT DENIAL Bug	High	General OS	<none>	Files Access	HTTP	IP	Ger
42		IIS DOT DOT EXECUTE Bug	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger
10076		IP Fragment Too Many Frags	Low	General OS	<none>	Informational	General Service	IP	Ger
1		PostOffice Init	Low	<none>	<none>	<none>	<none>	<none>	<no
7		Route Down!	High	<none>	<none>	<none>	<none>	<none>	<no
9		WWW IIS showcode.asp access	Medium	<none>	<none>	Files Access	HTTP	IP	Ger
29		WWW WinNT cmd.exe access	High	Windows	General Windows NT	Code Execution	HTTP	IP	Ger

CSIDS 4.0—16-51

View Option—Clicking on View in the TOC enables you to access the following options:

- Context Buffer—For TCP-based signatures that trigger on patterns in the TCP data stream, the Sensor captures up to 256 characters of the TCP stream, which may be examined from the Event Viewer. These capture characters are called the context buffer and it contains keystrokes, data, or both in the connection stream around the string of characters that triggered the signature. This feature can be used to determine if the triggered alarm was from a deliberate attack or if it is an accidental set of keystrokes. To view the context information for an alarm, you need to select the alarm entry (by clicking on it) and the clicking on View>Context Buffer from the TOC.

- Host Names—By default, the alerts stored by the Event Viewer indicate the IP addresses of the systems involved in the alert. Using the View>Host Names option from the TOC, you can cause the Event Viewer to attempt to resolve the host names for the IP addresses in the selected alerts. This information is displayed in a pop-up window in the Content Area.

- Network Security Database—The NSDB is the Cisco HTML-based encyclopedia of network vulnerability information. You can examine the NSDB for information on a specific alarm.

- Statistics—You can view event statistics for a row in Event Viewer. The statistics include the following information:

  - The severity level for the row.

  - The number of child nodes for the row.

- The number of events represented by the row.

- The percentage of the total events (based on the events currently displayed by the Event Viewer) that the selected row represents.

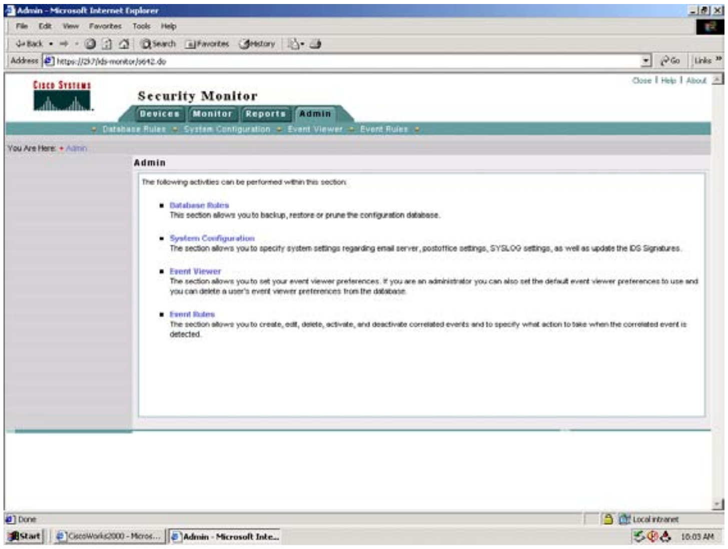
Note To access the statistics for a specific row, you select the row by clicking on a field in the row. Then you click View>Statistics from the TOC. A pop-up window appears in the Content Area indicating the statistics.

Administration and Reporting

This section describes how to administer the Security Monitor and generate reports.

Security Monitor Administration

Cisco.com



Admin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://2k7/ids-monitor/s642.do
Go Links
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Database Rules System Configuration Event Viewer Event Rules
You Are Here: Admin
Done
Local intranet
Start CiscoWorks2000 - Micros... Admin - Microsoft Inte...
10:03 AM

Admin

The following activities can be performed within this section:

- Database Rules
  This section allows you to backup, restore or prune the configuration database.
- System Configuration
  The section allows you to specify system settings regarding email server, postoffice settings, SYSLOG settings, as well as update the IDS Signatures.
- Event Viewer
  The section allows you to set your event viewer preferences. If you are an administrator you can also set the default event viewer preferences to use and you can delete a user's event viewer preferences from the database.
- Event Rules
  The section allows you to create, edit, delete, activate, and deactivate correlated events and to specify what action to take when the correlated event is detected.

CSIDS 4.0—16-53

Although a large percentage of your time will be spent using the Event Viewer functionality of Security Monitor, there are also various tasks that you may need to perform to administer and maintain your Security Monitor software. Security Monitor server administration and maintenance falls into the following categories:

- Database Maintenance—Allows you to backup, restore or prune the configuration database.

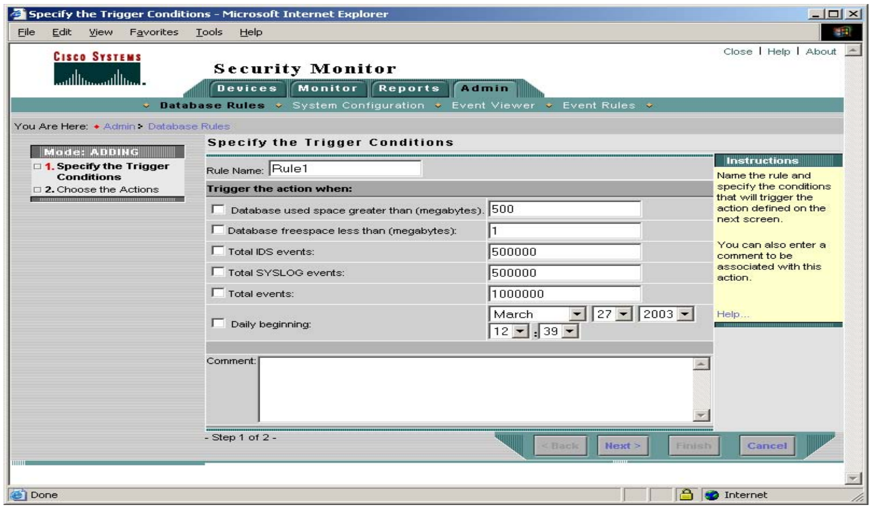
- System Configuration—Enables you to configure the communication properties as e-mail server, PostOffice settings, Syslog settings, and update network IDS signatures.

- Defining Event Viewer Preferences—Allows you to set your event viewer preferences. You can also create, edit, delete, activate, and deactivate correlated events and specify what action to take when the correlated event is detected by using Event Rules.

Admin—Database Rules

Cisco.com

Choose Admin>Database Rules>Add**.**



Specify the Trigger Conditions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Close | Help | About
Security Monitor
Devices Monitor Reports Admin
Database Rules System Configuration Event Viewer Event Rules
You Are Here: Admin > Database Rules
Mode: ADDING
1. Specify the Trigger Conditions
2. Choose the Actions
Specify the Trigger Conditions
Instructions
- Step 1 of 2 -
< Back Next > Finish Cancel
Done
Internet

Rule Name: Rule1

Trigger the action when:

□ Database used space greater than (megabytes):	500
□ Database freespace less than (megabytes):	1
□ Total IDS events:	500000
□ Total SYSLOG events:	500000
□ Total events:	1000000
□ Daily beginning:	March 27 2003 12 : 39

Comment:

Name the rule and specify the conditions that will trigger the action defined on the next screen.

You can also enter a comment to be associated with this action.

Help...

CSIDS 4.0—16-49

The Security Monitor enables you to launch a notification, trigger a script, or send an e-mail when a database rule is triggered. These database rules can be triggered when the Security Monitor database reaches a certain size, a number of events happen, or on a daily basis.

The Security Monitor comes with three predefined rules for database maintenance:

- Default pruning—Default pruning for alarm tables when the database reaches 2,000,000 total events.
- Default Syslog pruning—Default pruning for Syslog tables when the database reaches 2,000,000 total events.
- Default audit log pruning—Default pruning for audit log pruning performed on a daily basis.

Complete the following steps to add your own custom database rule:

Step 1 Choose **Admin>Database Rules>Add**. The Specify the Trigger Condition page is displayed.

Step 2 Enter values for settings listed in the following table:

Security Monitor Trigger Condition Settings	Description
Rule Name	Name that is to be assigned to the rule.
Database used space greater than (megabytes)	Check box that, if selected, triggers the database rule when the database reaches a size greater than specified. The default is 500 MB.

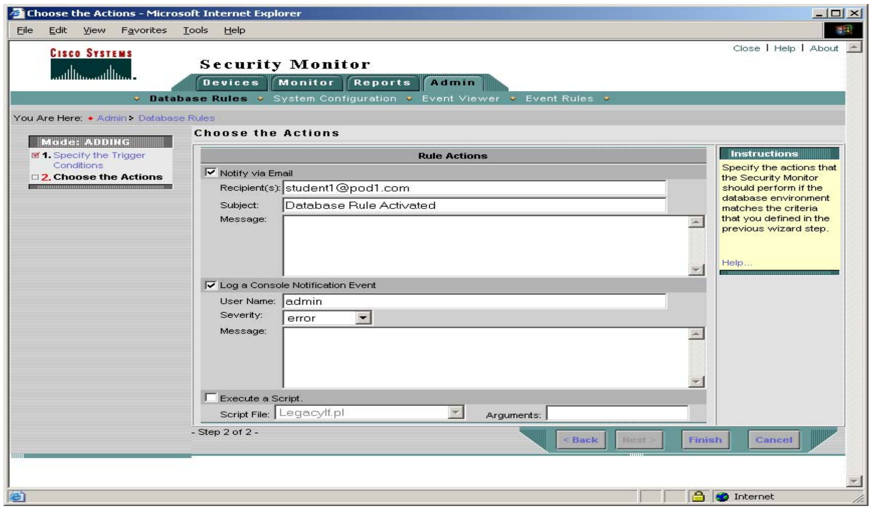
Security Monitor Trigger Condition Settings	**Description**
Database free space less than (megabytes)	Check box that, if selected, triggers the database rule when the free space on the drive to which the database has been installed falls below the specified size. The default is 1 MB.
Total IDS Events	Check box that, if selected, triggers the database rule when the total number of IDS events is more than the number specified. The default is 500,000.
Total SYSLOG Events	Check box that, if selected, triggers the database rule when the total number Syslog events are more than the number specified. The default is 500,000.
Total Events	Check box that, if selected, triggers the database rule when the combined total number of IDS and Syslog events is more than the number specified. The default is 1,000,000.
Daily Beginning	Check box that, if selected, allows the database rule to be triggered daily beginning at a specified date and time. The default is set to 24 hours from the clock on the Security Monitor server.
Comment	Optional.

Step 3 Click **Next**. The Choose the Actions page is displayed.

Admin—Database Rules (cont.)

Cisco.com

Choose Admin>Database Rules>Add>Next**.**



Choose the Actions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Database Rules System Configuration Event Viewer Event Rules

You Are Here: Admin > Database Rules

Mode: ADDING

- ☑ 1. Specify the Trigger Conditions
- □ 2. Choose the Actions

Choose the Actions

Rule Actions

☑ Notify via Email

Recipient(s): student1@pod1.com

Subject: Database Rule Activated

Message:

☑ Log a Console Notification Event

User Name: admin

Severity: error

Message:

□ Execute a Script.

Script File: Legacylf.pl Arguments:

- Step 2 of 2 -

< Back
Next >
Finish
Cancel
Internet

Instructions

Specify the actions that the Security Monitor should perform if the database environment matches the criteria that you defined in the previous wizard step.

Help...

CSIDS 4.0—16-50

Step 4 Enter values for settings listed in the following table:

Security Monitor Rule Actions Settings	Description
Notify via Email	Check box that, if selected, enables the Security Monitor to send an e-mail when the database rule is triggered.
Recipients	People who receive an e-mail when the database rule is triggered, if the Notify via Email check box is selected. Separate multiple recipients with a comma.
Subject	Subject of the e-mail that a recipient receives when the database rule is triggered, if the Notify via Email check box is selected.
Message	Message of the e-mail that a recipient receives when the database rule is triggered, if the Notify via Email check box is selected.
Log a Console Notification Event	Check box that, if selected, enables the Security Monitor to log a notification report to the console when the database rule is triggered.
Subject	Subject of the notification report that is logged on the console when the database rule is triggered, if the Log a Console Notification Event check box is selected.
Message	Message of the notification report that is logged on the console when the database rule is triggered, if the Log a Console Notification Event check box is selected.
Execute a Script	Check box that, if selected, enables the Security Monitor to execute a script when the database rule is triggered.
Script File	Drop-down menu that enables you to choose from a list of scripts to execute when the database rule is triggered, if the Execute a Script check box is selected.

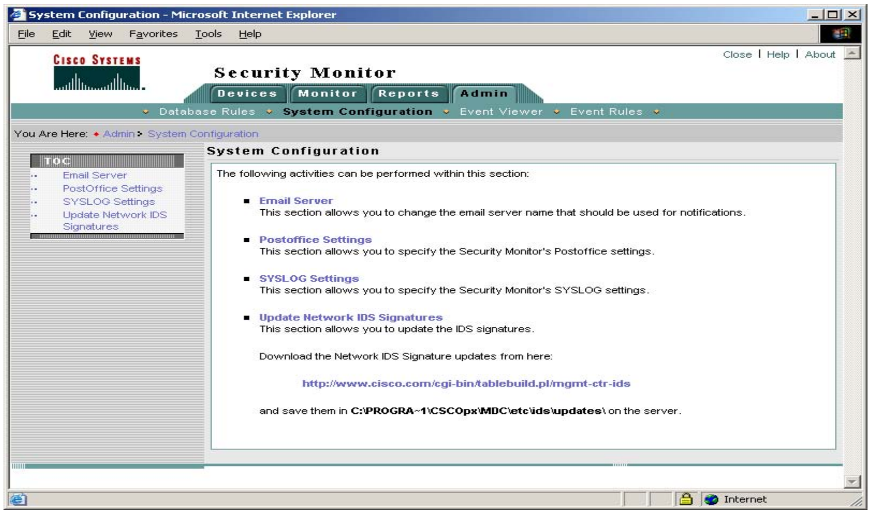
Security Monitor Rule Actions Settings	Description
Arguments	Additional arguments that can accompany a script that executes when the database rule is triggered, if the Execute a Script check box is selected.

Step 5 Click **Finish**. The Database Rules page is displayed with the rule you just created.

Note It is possible to execute scripts, against the Security Monitor database, other than those that accompany the Security Monitor. To install and use a newly created script, place the script in the default directory of the Security Monitor within the following sub-directory: \CSCOpx\MDC\etc\ids\scripts. Running some scripts against the Security Monitor database can result in unknown results. Use scripts with caution.

Admin—System Configuration Settings

Choose Admin>System Configuration**.**



System Configuration

The following activities can be performed within this section:

- **Email Server**
  This section allows you to change the email server name that should be used for notifications.
- **Postoffice Settings**
  This section allows you to specify the Security Monitor's Postoffice settings.
- **SYSLOG Settings**
  This section allows you to specify the Security Monitor's SYSLOG settings.
- **Update Network IDS Signatures**
  This section allows you to update the IDS signatures.

  Download the Network IDS Signature updates from here:

  http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids

  and save them in **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\** on the server.

CSIDS 4.0—16-56

The Security Monitor enables you to administer the Security Monitor's system configuration. The following are options to configure for the Security Monitor:

- Email Server—The Email Server enables you to specify the e-mail server that Security Monitor uses for event notifications and configure its properties.

- PostOffice Settings—Enables you to specify the settings used to establish the communication infrastructure between Security Monitor and Cisco IDS version 3.x IDS devices.

- Syslog Settings—Enables you to specify the port that Security Monitor uses to monitor Syslog messages.

- Update Network IDS Signatures—Allows you to update the IDS signatures.

Note Download the Network IDS Signature updates from http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids and save them in X:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\ on the server, where X = the default drive.

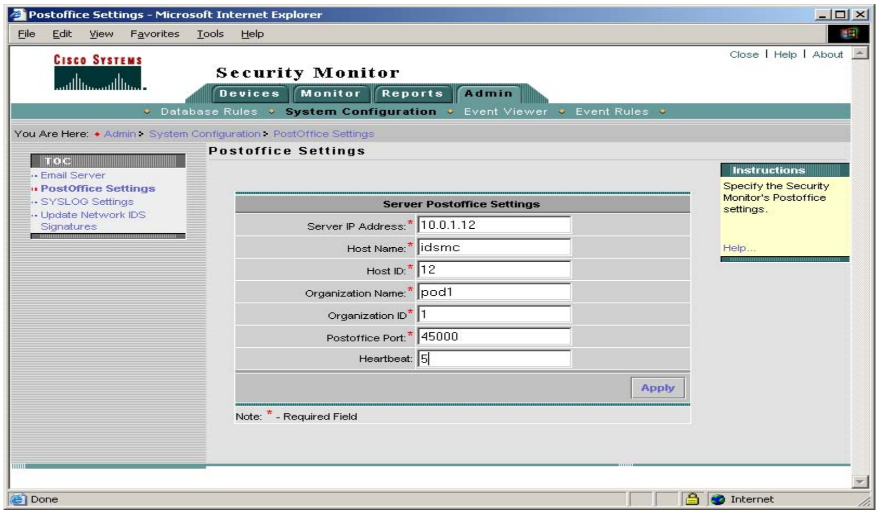
Complete the following steps to edit the e-mail server:

Step 1 Choose **Admin>System Configuration>Email Server**. The Email Server page is displayed.

Step 2 Enter the IP address of the e-mail server in the Email Server Name field and click **Apply**. The page refreshes indicating that the Security Monitor database has received the change.

Admin—PostOffice Settings

Choose Admin>System Configuration>Postoffice Settings**.**


Postoffice Settings - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Close | Help | About
Security Monitor
Devices Monitor Reports Admin
Database Rules System Configuration Event Viewer Event Rules
You Are Here: Admin > System Configuration > PostOffice Settings
TOC
Email Server
PostOffice Settings
SYSLOG Settings
Update Network IDS Signatures
Instructions
Help...
Apply
Done
Internet

Postoffice Settings

Specify the Security Monitor's Postoffice settings.

Server Postoffice Settings

Server IP Address:*	10.0.1.12
Host Name:*	idsmc
Host ID:*	12
Organization Name:*	pod1
Organization ID*	1
Postoffice Port:*	45000
Heartbeat:	5

Note: * - Required Field

Complete the following steps to edit the PostOffice settings:

Step 1 Choose **Admin>System Configuration>Postoffice Settings**. The Postoffice Settings page is displayed.

Step 2 Enter values for Postoffice settings listed in the following table:

Postoffice Settings	Description
Server IP Address	IP address of the server using PostOffice protocol.
Host Name	Hostname of the server using PostOffice protocol.
Host ID	Host ID of the server using PostOffice protocol.
Organization Name	Organization name of the server using PostOffice protocol.
Postoffice Port	Port that the PostOffice protocol uses for communication.
Heartbeat	Heartbeat interval used by the PostOffice protocol.

Step 3 Click **Apply**. The page refreshes indicating that the Security Monitor database has received the change.

Complete the following steps to configure Syslog settings:

Step 1 Choose **Admin>System Configuration>Syslog Settings**. The Syslog Settings page is displayed.

Step 2 Enter the new Syslog port number in the Listen on UDP Port entry field.

Step 3 Enter the new port to forward UDP Syslog information to in the Forward to UDP Port entry field.

Step 4 Click **Apply**. The Syslog Settings page refreshes indicating the Security Monitor received your request to edit the Syslog settings.

Complete the following steps to update the Security Monitor and Sensor signatures:

Step 1 Download the latest IDS updates for the Security Monitor from the Cisco Software center: http://www.cisco.com/cgi-bin//tablebuild.pl/ids4.

Step 2 Copy the files into the following directory: **CSCOpx\MDC\etc\ids\updates**.

Step 3 Choose **Admin>System Configuration>Update Network IDS Signatures**. The Update Network IDS Signatures page is displayed.

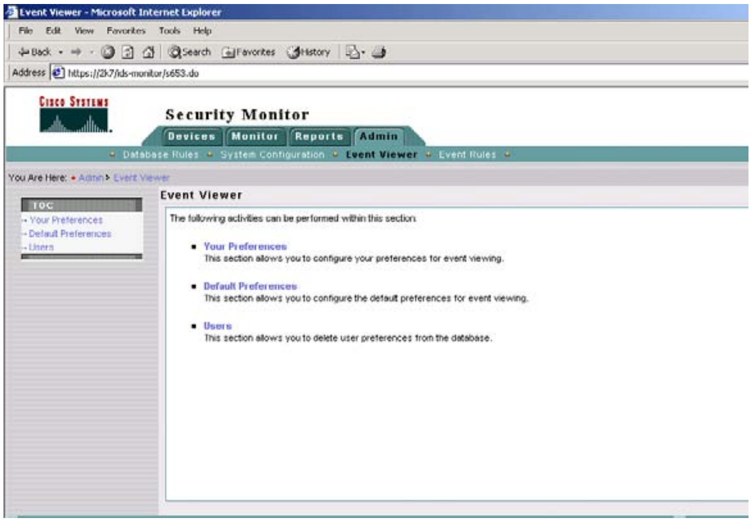
Step 4 Choose the downloaded IDS signature update for the Security Monitor from the Update File drop-down menu, and click **Apply**. If the Security Monitor needs to be updated, the Update Summary page is displayed. Proceed to Step 6. If the Security Monitor does not need to be updated, but Sensors need to be updated, the Select Sensor page is displayed. Proceed to Step 5.

Step 5 Select the Sensors that need to be updated by selecting their corresponding check boxes, and click **Next**. The Update Summary page is displayed.

Step 6 Click **Continue**. The Update Network IDS Signatures page is displayed.

Admin—Defining Event Viewer Preferences

Cisco.com


Event Viewer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://2k7/ids-monitor/s653.do
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Database Rules • System Configuration • Event Viewer • Event Rules
You Are Here: • Admin > Event Viewer
TOC
→ Your Preferences
→ Default Preferences
→ Users

Event Viewer

The following activities can be performed within this section.

- Your Preferences
  This section allows you to configure your preferences for event viewing.
- Default Preferences
  This section allows you to configure the default preferences for event viewing.
- Users
  This section allows you to delete user preferences from the database.

CSIDS 4.0—16-58

When working in the Event Viewer, you can configure your Event Viewer preferences. These changes, however, are not persistent and are lost whenever you close the Event Viewer. If you want to change your preferences so that they are applied every time that you open the Event Viewer you need to change the Event Viewer preferences using the administration options. Administratively, you can configure your Event Viewer preferences using the following two options:

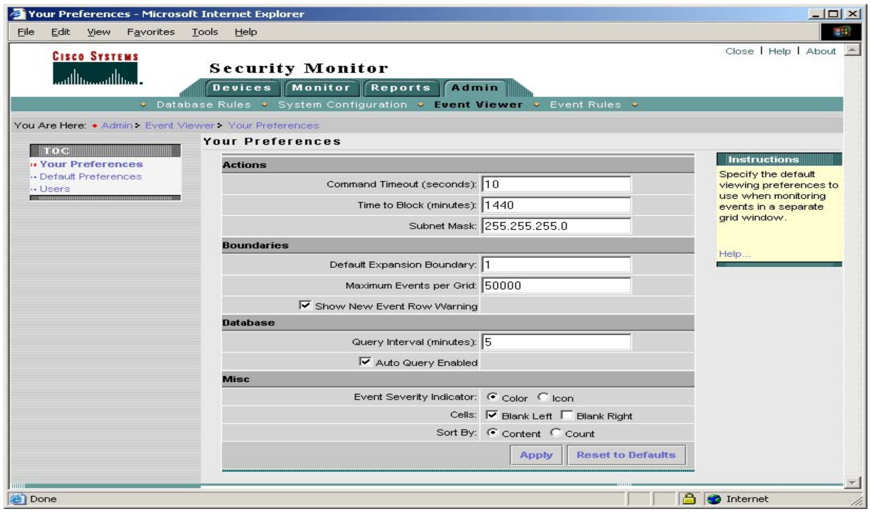
- Your Preferences—You can configure you own personal display preferences. These changes will only applied to the user that you are currently logged into Security Monitor with. These options enable you to customize the Event Viewer to your own personal preferences.

- Default Preferences—Allows you to change the default display settings for all users. You can use this option to establish display preferences that all users will benefit from.

Admin—Defining Event Viewer Preferences (cont.)

Cisco.com

Choose Admin>Event Viewer>Your Preferences**.**



Your Preferences

Actions

Command Timeout (seconds): 10

Time to Block (minutes): 1440

Subnet Mask: 255.255.255.0

Boundaries

Default Expansion Boundary: 1

Maximum Events per Grid: 50000

☑ Show New Event Row Warning

Database

Query Interval (minutes): 5

☑ Auto Query Enabled

Misc

Event Severity Indicator: ● Color ○ Icon

Cells: ☑ Blank Left □ Blank Right

Sort By: ● Content ○ Count

Instructions

Specify the default viewing preferences to use when monitoring events in a separate grid window.

Help...

CSIDS 4.0—16-59

Complete the following steps to edit your CiscoWorks account preferences:

Step 1 Choose **Admin>Event Viewer>Your Preferences**. The Your Preferences page is displayed.

Step 2 Enter values for settings listed in the following table:

Security Monitor Your Preferences Settings	Description
Command Timeout	Amount of time the Event Viewer will wait for a response from the remote Sensor or host before concluding that the remote Sensor or host is not connected. The default command timeout is 10 seconds.
Time to Block	Amount of time the Sensor blocks traffic from a specified source when you issue a block command from the Event Viewer. The default time to block is 1440 minutes.
Subnet Mask	Subnet mask of the Security Monitor.
Default Expansion Boundary	Amount of expansion that takes place when opening security event levels within the Event Viewer.
Maximum Events per Grid	Maximum number of events that populate the Event Viewer grid. Newer events push the older events off of the grid.
Auto Collapse Enabled	Check box that, if selected, enables the automatic collapsing of a cell.
Query Interval	Amount of time that the Event Viewer queries the database for new events. The default query interval time is 5 minutes.
Auto Query Enabled	Check box that, if selected, enables automatic queries of the database for new security events.
Event Security Indicator	Radio buttons that change the event security indicator from a color to an icon, or vice versa.
Cells	Check boxes that, if selected, enable the Event Viewer to display security events blank left, blank right, or both.

Security Monitor Your Preferences Settings	Description
Sort by	Radio buttons that enable you to sort the security events by content or by count. The default is by content.

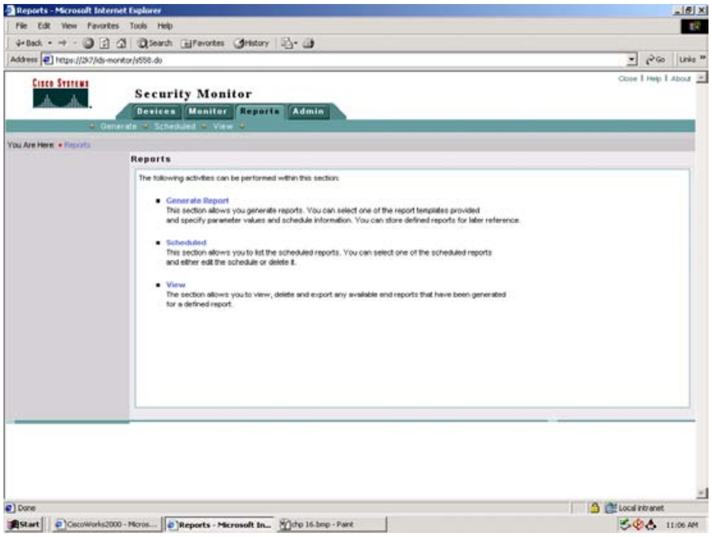
Step 3 Click **Apply**. The Your Preferences page refreshes indicating that the Security Monitor received the changes.

Changing the default preferences has the same process and entry fields that need to be completed. When you edit the default preferences, it only affects new users.

The Users section only allows you to delete the user preferences for that account, not the account itself.

Security Monitor Reports

Cisco.com


Reports - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://2k7/ids-monitor/s558.do
Go Links
Close | Help | About
Cisco Systems
Security Monitor
Devices Monitor Reports Admin
Generate Scheduled View
You Are Here • Reports
Done
Local intranet
Start CiscoWorks2000 - Micros... Reports - Microsoft In... chp 16.bmp - Paint
11:06 AM

Reports

The following activities can be performed within this section:

- Generate Report
  This section allows you generate reports. You can select one of the report templates provided and specify parameter values and schedule information. You can store defined reports for later reference.
- Scheduled
  This section allows you to list the scheduled reports. You can select one of the scheduled reports and either edit the schedule or delete it.
- View
  The section allows you to view, delete and export any available end reports that have been generated for a defined report.

CSIDS 4.0—16-60

Security Monitor enables you to generate reports based on the audit and alarm information collected by Security Monitor. These reports can be generated immediately, or you can be schedule them be generated at a later time. Creating a report using Security Monitor involves the following tasks:

Task 1—Generate reports

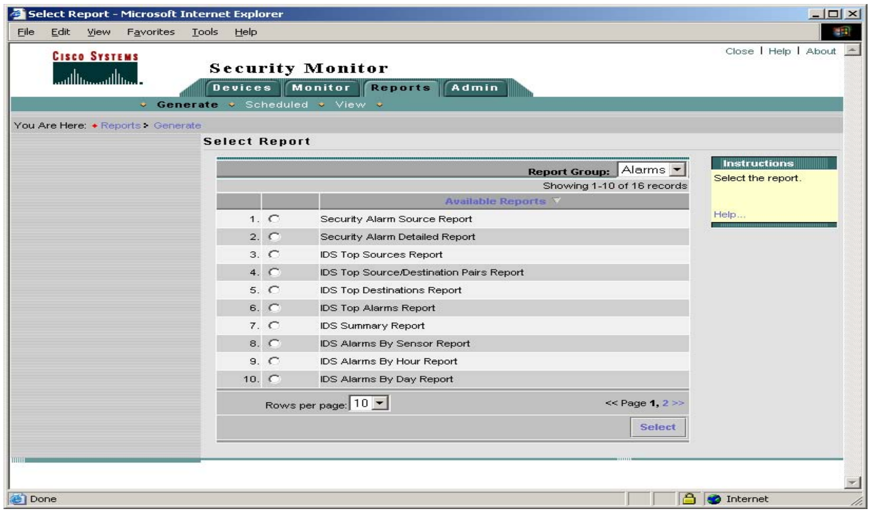
Task 2—Schedule reports

Task 3—View reports

Reports—Generate

Cisco.com

Choose Reports>Generate**.**



You Are Here: ◆ Reports > Generate

Select Report

Report Group: Alarms

Showing 1-10 of 16 records

		Available Reports
1.	○	Security Alarm Source Report
2.	○	Security Alarm Detailed Report
3.	○	IDS Top Sources Report
4.	○	IDS Top Source/Destination Pairs Report
5.	○	IDS Top Destinations Report
6.	○	IDS Top Alarms Report
7.	○	IDS Summary Report
8.	○	IDS Alarms By Sensor Report
9.	○	IDS Alarms By Hour Report
10.	○	IDS Alarms By Day Report

Rows per page: 10

<< Page **1**, 2 >>

Select

Instructions

Select the report.

Help...

The Security Monitor enables the network security administrator to generate audit and alarm reports. The report can be generated immediately or scheduled to run at a later time. The scheduled reports can run once at a specific time or at regular intervals.

Complete the following steps to generate an IDS alarm report:

Step 1 Choose **Reports>Generate**. The Select Report page is displayed.

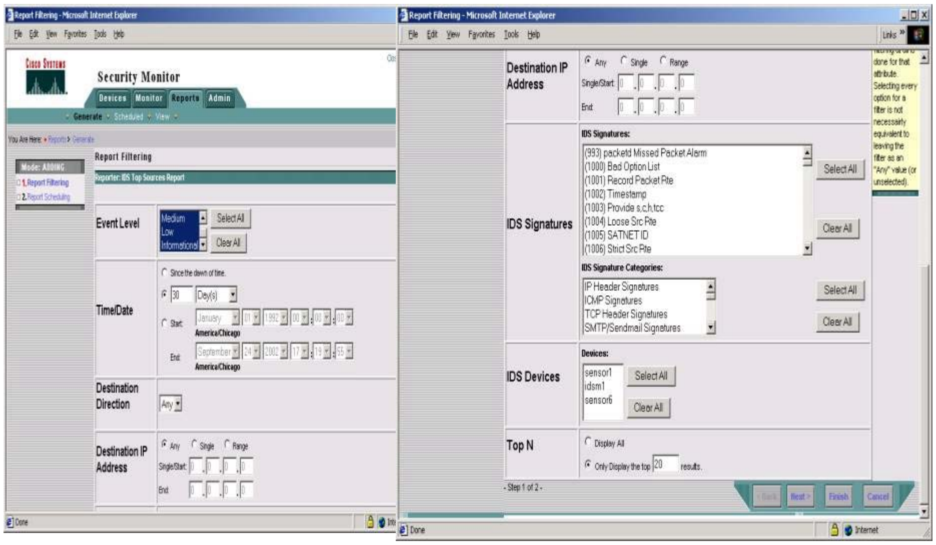
Step 2 Choose **All** from the Report Group drop-down menu. The list of Available Reports refreshes to display the reports.

Step 3 Select an IDS report radio button.

Step 4 Click **Select**. The Report Filtering page is displayed.

Reports—Generate (cont.)

Cisco.com



Report Filtering - Microsoft Internet Explorer

Security Monitor

Report Filtering

Reporter: IDS Top Sources Report

Event Level: Medium, Low, Informational

Time/Date:
○ Since the dawn of time.
● 30 Day(s)
○ Start: January 01 1992 00 : 00 : 00 America/Chicago
End: September 24 2002 17 : 19 : 55 America/Chicago

Destination Direction: Any

Destination IP Address: ● Any ○ Single ○ Range
Single/Start: 0 . 0 . 0 . 0
End: 0 . 0 . 0 . 0

IDS Signatures:
(993) packetd Missed Packet Alarm
(1000) Bad Option List
(1001) Record Packet Rte
(1002) Timestamp
(1003) Provide s,c,h,tcc
(1004) Loose Src Rte
(1005) SATNET ID
(1006) Strict Src Rte

IDS Signature Categories:
IP Header Signatures
ICMP Signatures
TCP Header Signatures
SMTP/Sendmail Signatures

IDS Devices: Devices: sensor1, idsm1, sensor6

Top N:
○ Display All
● Only Display the top 20 results.

- Step 1 of 2 -

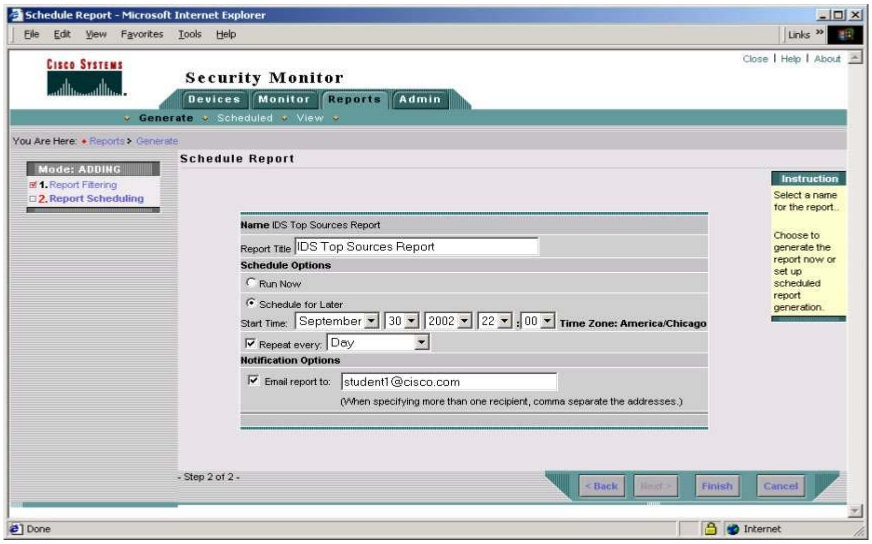
&lt; Back
Next &gt;
Finish
Cancel
done for that attribute. Selecting every option for a filter is not necessarily equivalent to leaving the filter as an "Any" value (or unselected).
Done
Internet

Step 5 Enter values for settings listed in the following table:

Security Monitor Report Filtering Settings	Description
Event Level	The event level that is displayed in the selected report. Options to choose from are: High, Medium, Low, and Informational.
Time/Date	The time and date selected in the report. Options to choose from are: Since the dawn of time, a specified number of time units, or a range of time.
Source Direction	The direction of the security violation. Options to choose from are: Any, In, or Out.
Source Address	The source address of the security violation. Options to choose from are: Any, Single, or A Range of IP Addresses.
Destination Direction	The direction of the security violation. Options to choose from are: Any, In, or Out.
Destination Address	The source address of the security violation. Options to choose from are: Any, Single, or A Range of IP Addresses.
IDS Devices	The IDS devices that are viewed in the report. You can choose all devices that have been defined in the Security Monitor.
IDS Signatures	The IDS signatures that are viewed in the report. You can choose one or multiple signatures.
IDS Signature Categories	The IDS signature categories that are viewed in the report. You can choose one or multiple signature categories.
Top N	Displays the top number of results in the report.

Reports—Generate (cont.)

Cisco.com



Schedule Report - Microsoft Internet Explorer

You Are Here: Reports > Generate

Mode: ADDING

☑ 1. Report Filtering

□ 2. Report Scheduling

Schedule Report

Name IDS Top Sources Report

Report Title: IDS Top Sources Report

Schedule Options

○ Run Now

● Schedule for Later

Start Time: September 30 2002 22 : 00 **Time Zone: America/Chicago**

☑ Repeat every: Day

Notification Options

☑ Email report to: student1@cisco.com

(When specifying more than one recipient, comma separate the addresses.)

- Step 2 of 2 -

Instruction

Select a name for the report.

Choose to generate the report now or set up scheduled report generation.

CSIDS 4.0—16-63

Note	Selecting a value, or multiple values, for a filter limits the results to those containing the selected values. Not selecting any values, or choosing the Any option on some filters, indicates that no filtering will occur for that attribute. Selecting every option for a filter is not necessarily equivalent to leaving the filter as an Any value or unselected.

Step 6 Click **Next**. The Schedule Report page is displayed.

Step 7 Enter values for settings listed in the following table:

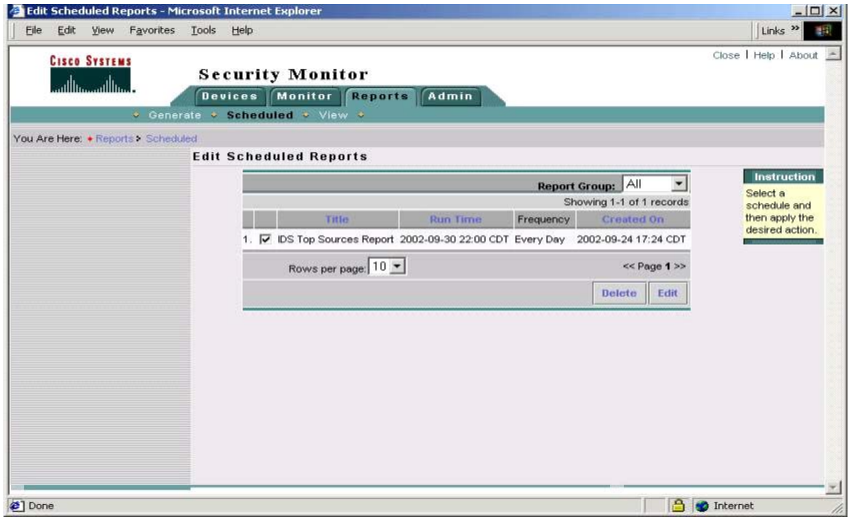
Security Monitor Schedule Report Settings	Description
Report Title	Description field that enables you to label the report that is about to be generated.
Schedule Options	Options that enable you to either run the report immediately or schedule it for a later time.
Repeat every	Check box with a drop-down menu that enables you to repeat the report at the following intervals: every day, week, weekday, weekend day, minute, and hour.
Email report to	Entry field that enables you to have the report e-mailed after it is generated.

Step 8 Click **Finish**. If the report was scheduled to run immediately, the Report View page is displayed. If not, then the Select Report page is displayed.

Reports—Scheduled

Cisco.com

Choose Reports>Scheduled**.**



You Are Here: • Reports > Scheduled

Edit Scheduled Reports

Report Group: All

Showing 1-1 of 1 records

		Title	Run Time	Frequency	Created On
1.	☑	IDS Top Sources Report	2002-09-30 22:00 CDT	Every Day	2002-09-24 17:24 CDT

Rows per page: 10

<< Page **1** >>

Delete   Edit

Instruction

Select a schedule and then apply the desired action.

CSIDS 4.0—16-64

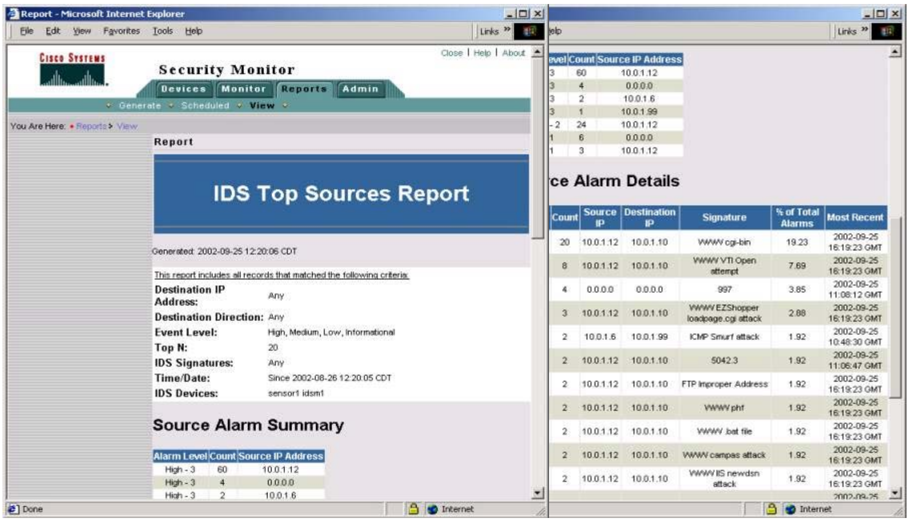
For each report that you generate, you can enter a report title and define a schedule and notification options. You enter this information on the Schedule Report page when you choose **Reports>Generate**. You can run the report immediately, or you can schedule the report to run at a later time, at regular intervals, or both.

Select **Reports>Scheduled** to view reports that have been scheduled. In addition to viewing scheduled reports, you may edit the report's schedule or delete it.

Reports—View

Cisco.com

Choose Reports>View**.**



Report

IDS Top Sources Report

Generated: 2002-09-25 12:20:06 CDT

This report includes all records that matched the following criteria:

Destination IP Address:	Any
Destination Direction:	Any
Event Level:	High, Medium, Low, Informational
Top N:	20
IDS Signatures:	Any
Time/Date:	Since 2002-08-26 12:20:05 CDT
IDS Devices:	sensor1 idsm1

Source Alarm Summary

Alarm Level	Count	Source IP Address
High - 3	60	10.0.1.12
High - 3	4	0.0.0.0
High - 3	2	10.0.1.6

evel	Count	Source IP Address
3	60	10.0.1.12
3	4	0.0.0.0
3	2	10.0.1.6
3	1	10.0.1.99
- 2	24	10.0.1.12
1	6	0.0.0.0
1	3	10.0.1.12

ce Alarm Details

Count	Source IP	Destination IP	Signature	% of Total Alarms	Most Recent
20	10.0.1.12	10.0.1.10	WWW cgi-bin	19.23	2002-09-25 16:19:23 GMT
8	10.0.1.12	10.0.1.10	WWW VTI Open attempt	7.69	2002-09-25 16:19:23 GMT
4	0.0.0.0	0.0.0.0	997	3.85	2002-09-25 11:08:12 GMT
3	10.0.1.12	10.0.1.10	WWW EZShopper loadpage.cgi attack	2.88	2002-09-25 16:19:23 GMT
2	10.0.1.6	10.0.1.99	ICMP Smurf attack	1.92	2002-09-25 10:48:30 GMT
2	10.0.1.12	10.0.1.10	5042.3	1.92	2002-09-25 11:06:47 GMT
2	10.0.1.12	10.0.1.10	FTP Improper Address	1.92	2002-09-25 16:19:23 GMT
2	10.0.1.12	10.0.1.10	WWW phf	1.92	2002-09-25 16:19:23 GMT
2	10.0.1.12	10.0.1.10	WWW .bat file	1.92	2002-09-25 16:19:23 GMT
2	10.0.1.12	10.0.1.10	WWW campas attack	1.92	2002-09-25 16:19:23 GMT
2	10.0.1.12	10.0.1.10	WWW IIS newdsn attack	1.92	2002-09-25 16:19:23 GMT
					2002-09-25

CSIDS 4.0—16-58

After generating your reports, you can view them by accessing **Reports>View.** This displays the Choose Completed Report window in the Content Area.

To view a report that you have generated, you first need to click the radio button next to the report. Then you have to choose one of the following two methods to view your reports:

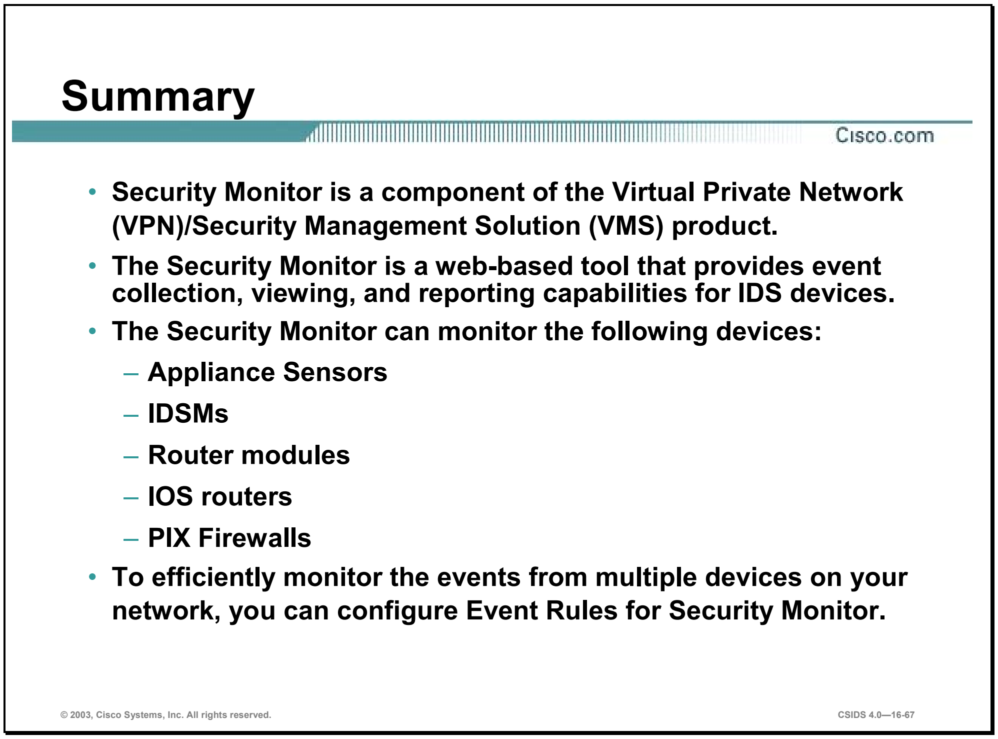
- View
- Open in Window ...

The difference between these options is that the Open in Window option causes the report to be displayed in a new browser window.

Note If the report was generated from a scheduled report template, deleting the report does not delete the associated scheduled report template.

Summary

This section summarizes the information you learned in this chapter.

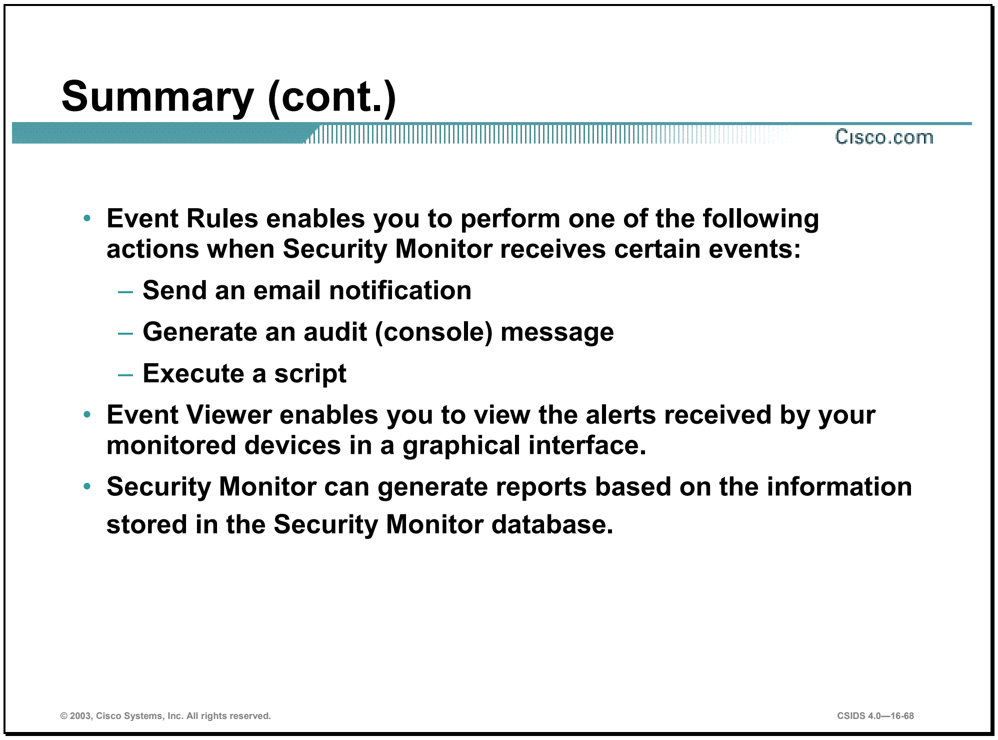


Summary

Cisco.com

- Security Monitor is a component of the Virtual Private Network (VPN)/Security Management Solution (VMS) product.
- The Security Monitor is a web-based tool that provides event collection, viewing, and reporting capabilities for IDS devices.
- The Security Monitor can monitor the following devices:
  - Appliance Sensors
  - IDSMs
  - Router modules
  - IOS routers
  - PIX Firewalls
- To efficiently monitor the events from multiple devices on your network, you can configure Event Rules for Security Monitor.

CSIDS 4.0—16-67



Summary (cont.)

- Event Rules enables you to perform one of the following actions when Security Monitor receives certain events:
  - Send an email notification
  - Generate an audit (console) message
  - Execute a script
- Event Viewer enables you to view the alerts received by your monitored devices in a graphical interface.
- Security Monitor can generate reports based on the information stored in the Security Monitor database.

Lab Exercise—Enterprise IDS Monitoring and Reporting

Complete the following lab exercise to practice what you learned in this chapter.

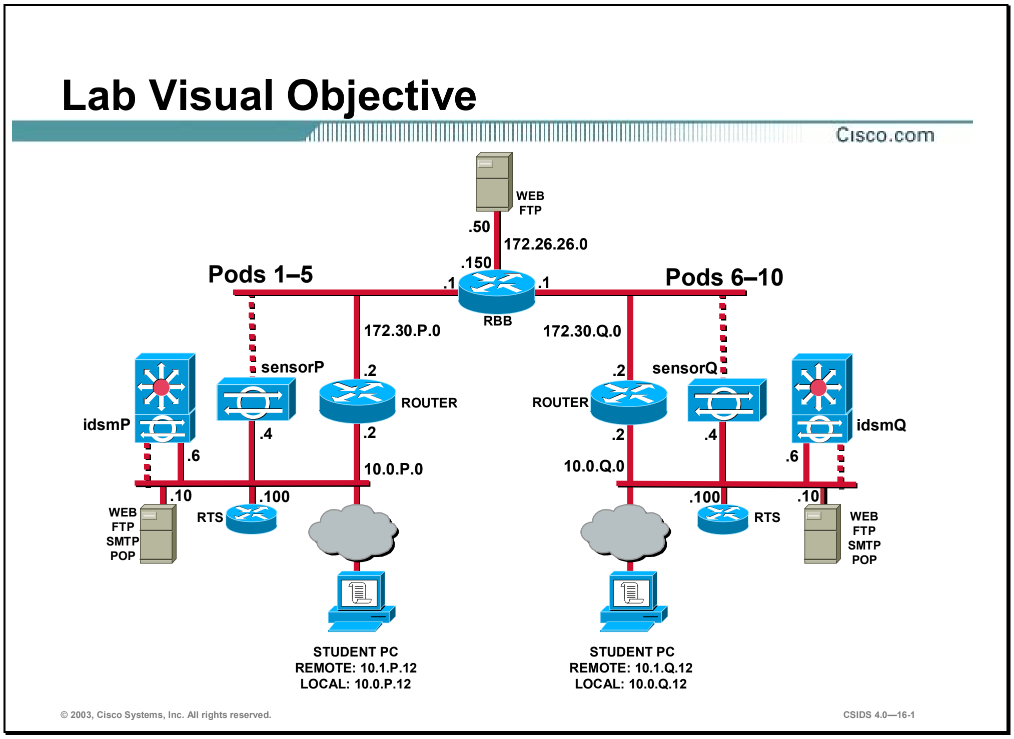
Objectives

In this lab exercise you will complete the following tasks:

- Install the Security Monitor.
- Launch the Security Monitor.
- Import and view the Cisco IDS device status.
- View IDS alarms in the Security Monitor Event Viewer.
- Create an e-mail notification event rule.
- Generate an IDS top alarms report.
- Generate an audit log report.

Visual Objective

The following figure displays the lab topology you will use to complete this lab exercise.



Lab Visual Objective

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—16-1

Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor. Make sure to replace it with your peer's pod number.

Setup

Before starting this lab exercise, the IDS Event Viewer must be uninstalled. Ensure that the CiscoWorks2000 (CiscoWorks) VPN/Security Management Solution (VMS) Common Services has been installed on the student PC. Notify your instructor if the VMS common services are not installed.

Task 1—Install the Security Monitor

Complete the following steps to install the Security Monitor:

Step 1 Log in as the local administrator on the student PC.

Step 2 Verify the CiscoWorks VMS Common services are installed on the student PC.

Step 3 Verify the IDS Event Viewer application has been uninstalled.

Step 4 Locate and execute the Security Monitor installation files as directed by your instructor. The Welcome panel is displayed.

Step 5 Click **Next** to begin the installation. The Software License Agreement panel is displayed.

Step 6 Click **Yes** to accept the terms of the license agreement. The Setup Type window opens.

Step 7 Select **Custom installation** to install the Security Monitor and click **Next**. The Select Components panel is displayed.

Step 8 Select the **Security Monitor only** radio button and click **Next**. The System Requirements panel is displayed.

Step 9 Verify that your system meets the minimum disk space and memory requirements. Click **Next**. The Verification panel is displayed.

Step 10 Verify the selected components. Click **Next**. The Select CW2000 Syslog Port panel is displayed.

Step 11 Click **Next** to accept the default port. The Configure Communication Properties panel is displayed.

Step 12 Click **Next**. The Setup Complete panel is displayed after the Security Monitor installation process finishes.

Step 13 Click **Finish**. The Install Wizard exits and the Security Monitor processes start.

Task 2—Launch the Security Monitor

This task involves the student accessing the CiscoWorks server to launch the Security Monitor. Complete the following steps to log in to the CiscoWorks server and launch the Security Monitor.

Step 1 Launch your web browser and specify the IP address of the CiscoWorks server as the location:

```
http://127.0.0.1:1741
```

Step 2 Log in to CiscoWorks as the default user **admin.** The default admin password is **admin**.

Step 3 Click **Connect**. You are now logged in to the CiscoWorks desktop.

Step 4 Select the **VPN/Security Management Solution** drawer in the left panel.

Step 5 Select the **Monitoring Center** folder located in the VPN/Security Management Solution drawer.

Step 6 Select the **Security Monitor** icon to launch the Security Monitor. The Security Alert window opens and prompts you to accept a digital certificate.

Step 7 Click **Yes**. You are now logged in to the Security Monitor.

Step 8 Minimize the CiscoWorks window before proceeding to the next task.

Task 3—Import and View the Cisco IDS Device Status

This task involves importing the intrusion detection system (IDS) devices that exist in the IDS Management Center (MC) database into the Security Monitor database, and viewing the IDS device status. Complete the following steps to import and view the Cisco IDS device status:

Step 1 Choose **Devices**. The Devices page is displayed. Currently, there are no devices defined in the Security Monitor.

Step 2 Click **Import**. The Enter IDS Server Information page is displayed.

Step 3 Enter **10.0.P.12** in the IP Address/Host Name field.

(where P = pod number)

Step 4 Verify that **443** appears in the Web Server Port field.

Step 5 Enter **admin** in the Username field.

Step 6 Enter **admin** in the Password field.

Step 7 Click **Next**. The Select Devices page is displayed.

Step 8 Select **sensorP** from the list of devices and click **Next**. The Update NAT Addresses page is displayed.

(where P = pod number)

Step 9 Click **Finish**. The Summary page is displayed.

Step 10 Click **OK**. The Devices page is displayed with the Sensor added to the Security Monitor.

Step 11 Choose **Monitor>Connections**. The Connections page is displayed and the Connection Status column reads Connected TLS.

Task 4—View IDS Alarms in the Security Monitor Event Viewer

This task involves launching an attack against the network in order to generate alarms that can be viewed in the Security Monitor Event Viewer. Complete the following steps to view IDS alarms in the Security Monitor Event Viewer:

Note The attacks that are used to generate events in the Security Monitor have been configured in previous labs.

Step 1 Complete the following sub-steps to test the string match signature you created earlier:

1. Initiate a Telnet session to the backbone router from the Windows command line:

```
C:\> telnet 172.26.26.150
User Access Verification
Password:
```

Step 2 Enter **podP** at the password prompt. The Telnet session should close due to the string match signature:

```
Password: podP
```

(where P = pod number)

Step 3 Complete the following sub-steps to test the tuned signature and signature filter:

1. Open a DOS command prompt and initiate a continuous ping to your peer pod's Sensor with an increased packet size:

```
C:\> ping –t 10.0.Q.4 –l 11500
```

(where Q = peer pod number)

2. Open another DOS command prompt and initiate a continuous ping to your peer pod's student PC with an increased packet size:

```
C:\> ping –t 10.0.Q.12 –l 11500
```

(where Q = peer pod number)

3. Open another DOS command prompt and initiate a continuous ping to your peer pod's Sensor with an increased packet size:

```
C:\> ping –t 10.0.Q.4 –l 11500
```

(where Q = peer pod number)

Step 4 Completing the following sub-steps to discover the version of IIS on your peer pod's student PC:

1. Open another DOS command prompt and telnet to port 80 on your peer pod's student PC:

```
C:\> telnet 10.0.Q.12 80
```

(where Q = peer pod number)

2. Enter the **GET phf?** command:

```
GET phf?
```

Step 5 Choose **Monitor>Events**. The Events page is displayed.

Step 6 Accept the default values and click **Launch Event Viewer**. The Event Viewer is displayed.

Step 7 Double-click in the cell beneath the Count column heading. The alarms you generated are displayed.

Task 5—Create an E-mail Notification Event Rule

The Security Monitor will notify you when a signature pattern triggers by generating a report detailing the security event. Complete the following steps to create an e-mail notification event rule:

Step 1 Choose **Admin>System Configuration**. The System Configuration page is displayed.

Step 2 Select **Email Server** from the table of contents (TOC). The Email Server page is displayed.

Step 3 Verify that the e-mail server address, **10.0.P.10**, appears in the Email Server Name field.

(where P = pod number)

Step 4 Choose **Admin>Event Rules**. The Event Rules page is displayed.

Step 5 Click **Add**. The Identify the Rule page is displayed.

Step 6 Enter **Email Alert** in the Rule Name field. Enter a brief description in the Description field.

Step 7 Click **Next**. The Specify Event Filter page is displayed.

Step 8 Enter the Event Field Filtering settings from the following table in the first row of the Event Field Filtering group box:

Event Field Filtering Settings	Value
First drop-down menu	**Severity**
Second drop-down menu	**>=**
Third drop-down menu	**Low**

Step 9 Verify that the Boolean operator, **AND**, is selected from the drop-down menu by default.

Step 10 Enter the Event Field Filtering settings from the following table in the next row of the Event Field Filtering group box:

Event Field Filtering Settings	Value
First drop-down menu	**Attacker Address**
Second drop-down menu	**=**
Third entry field	**10.0.Q.12**

(where Q = peer pod number)

Step 11 Click **Next**. The Choose the Actions page is displayed.

Step 12 Select the **Notify via Email** check box to enable e-mail notification.

Step 13 Enter the recipient, **studentP**, in the Recipients field.

(where P = pod number)

Note It is recommended to enter a fully qualified e-mail address. The e-mail server in the lab exercise is configured to accept only the recipient name.

Step 14 Enter **Severity Event Rule Alert Message** in the Subject field.

Step 15 Enter the following in the Message field: **A signature was triggered from my peer**.

Step 16 Click **Next**. The Specify the Thresholds and Intervals page is displayed.

Step 17 Enter the values from the following table in the Thresholds and Intervals group box:

Threshold and Intervals Settings	Value
Issue actions after (# event occurrences)	**1**
Repeat actions again after (# event occurrences)	**1**
Reset count every (minutes)	**5**

Step 18 Click **Finish**. The Event Rules page is displayed with the new event rule. Notice that the event rule is not active.

Step 19 Select the radio button associated with the event rule.

Step 20 Click the **Activate** button to enable the event rule. The page refreshes to indicate the rule was activated.

Step 21 Enter the URLs listed in the following table in your browser to generate IDS events:

URL	Signature Name
http://**target_ip_address**/msadc/samples/selector/showcode.asp	WWW IIS Showcode.asp Access
http://**target_ip_address**/scripts/..%c0%af../winnt/system32	WWW IIS Unicode Attack

URL	Signature Name
http://**target_ip_address**/ scripts/..%35c../winnt/system32/cmd.exe?/c+dir	WWW WinNT cmd.exe

(where target_ip_address = target host IP address assigned by your instructor)

Note No spaces should be entered in the URL.

Step 22 Choose **Monitor>Events**. The Events page is displayed.

Step 23 Accept the default values and click **Launch Event Viewer**. The Event Viewer is displayed.

Step 24 Locate and select an IDS event that was generated in the previous step.

Step 25 Choose **View>Context Buffer** from the TOC. The URL used to launch the attack is displayed in a new window.

Step 26 Log in to your e-mail client as directed by your instructor.

Step 27 Retrieve your e-mail to verify that the event rule generated e-mail notifications.

Task 6—Generate an IDS Top Alarms Report

Complete the following steps to generate an IDS top alarms report:

Step 1 Choose **Reports>Generate**. The Select Report page is displayed.

Step 2 Select **IDS Top Alarms Report** from the Available Reports list.

Step 3 Click **Select**. The Report Filtering page is displayed.

Note If this report is not available for generation, it may be necessary to scroll through the list of reports or reorder them. Use **>>**, located above Select, to scroll through the list of available reports. To list all reports that can be generated, use the **Report Group** drop-down menu and select **All**.

Step 4 Enter the Report Filtering settings from the following table:

Report Filtering Settings	Lab Settings
Event Level	**Select All**
Time/Date	**Since the dawn of time.**
Source Direction	**Any**
Source IP Address	**Any**
Destination Direction	**Any**
Destination IP Address	**Any**
IDS Devices	**sensorP**
IDS Signatures	Do not make a selection..
Top N	**10**

(where P = pod number)

Step 5 Click **Next**. The Schedule Report page is displayed.

Step 6 Enter **PodP Top IDS Alarms Report** for the Report Title.

(where P = pod number)

Step 7 Select the **Schedule for Later** Schedule option, and set the Start Time for **5** minutes later than the current time.

Step 8 Select the **Repeat every:** check box and choose the **Day** from the drop-down menu.

Step 9 Select the Notification option, **Email report to** check box, and enter **studentP@cisco.com** in the Email Report To field.

(where P = pod number)

Step 10 Click **Finish** to submit the report. The Select Report page is displayed.

Step 11 Check your e-mail in about 5 minutes to verify the report has been successfully delivered. The email will contain the URL of the Security Monitor server with a reports section of the Security Monitor appended to it.

Step 12 Double-click the URL in the email report to launch your browser and view the report. A Security Alert window opens.

Step 13 Click **Yes**. A Secure Login window opens.

Step 14 Log in to the Secure Login window as the default user admin. The default admin password is admin. The Choose Completed Report page is displayed.

Step 15 Select the **PodP Top IDS Alarms Report** and click **View**. The PodP Top IDS Alarms Report is displayed in the same browser.

(where P = pod number)

Task 7—Generate an Audit Log Report

It may be necessary to troubleshoot system processes on the Security Monitor. Complete the following steps to generate an audit log report:

Step 1 Choose **Reports>Generate**. The Select Report page is displayed.

Step 2 Select **Audit** from the Report Group drop-down menu. The Available Report page refreshes to display the available audit reports that can be generated.

Step 3 Select **Audit Log Report** from the list of Available reports and click **Select**. The Report Filtering page is displayed.

Step 4 Enter the Report Filtering settings from the following table:

Report Filtering Settings	Lab Settings
Date/Time	**Since the dawn of time.**
Event Severity	**Select All**
Applications	**Monitoring Center for Security**
Subsystem	**IDS_Notifier**
Task Type	Leave this field blank.

Step 5 Click **Next**. The Schedule Report page is displayed.

Step 6 Enter **PodP Audit Log Report** for the Report Title.

(where P = pod number)

Step 7 Select **Run Now** from the Schedule Options.

Step 8 Select the Notification option, **Email report to**, check box and enter **studentP** in the Email Report To field.

(where P = pod number)

Step 9 Click **Finish** to submit the report. The Choose Completed Report page is displayed.

Step 10 Check your email to verify the report has been successfully delivered. The email will contain the URL of the Security Monitor server with a reports section of the Security Monitor appended to it.

Step 11 Double-click the URL in the e-mail report to launch your browser and view the report. Your browser opens a Secure Login window.

Step 12 Log in to the Secure Login window as the default user admin. The default admin password is admin. The Choose Completed Report page is displayed.

Step 13 Select the **PodP Audit Log Report** and click **View**. The PodP Audit Log Report is displayed in the same browser window.

17

Cisco Intrusion Detection System Maintenance

Overview

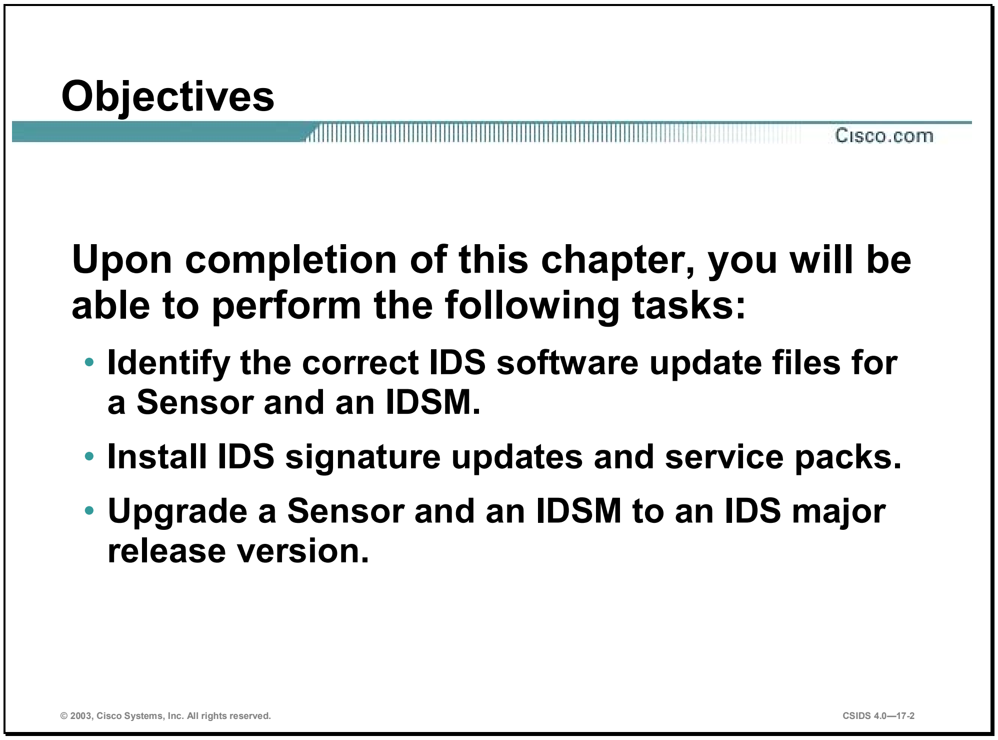
This chapter explains how to perform maintenance on a Cisco Intrusion Detection System (IDS) appliance Sensor or an IDS Module (IDSM).

This chapter includes the following topics:

- Objectives
- Software updates
- Sensor maintenance
- Summary
- Lab exercise

Objectives

This section lists this chapter's objectives.



Objectives

Cisco.com

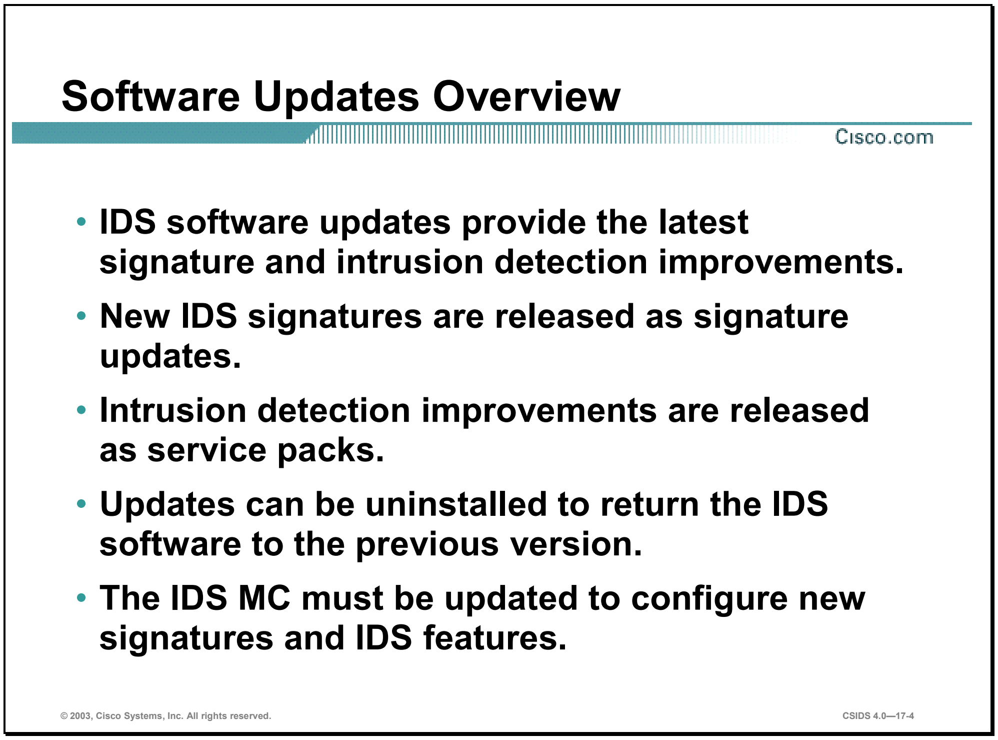
Upon completion of this chapter, you will be able to perform the following tasks:

- **Identify the correct IDS software update files for a Sensor and an IDSM.**
- **Install IDS signature updates and service packs.**
- **Upgrade a Sensor and an IDSM to an IDS major release version.**

CSIDS 4.0—17-2

Software Updates

This section provides an overview of IDS software updates and some guidelines to follow when installing software updates.



Software Updates Overview

Cisco.com

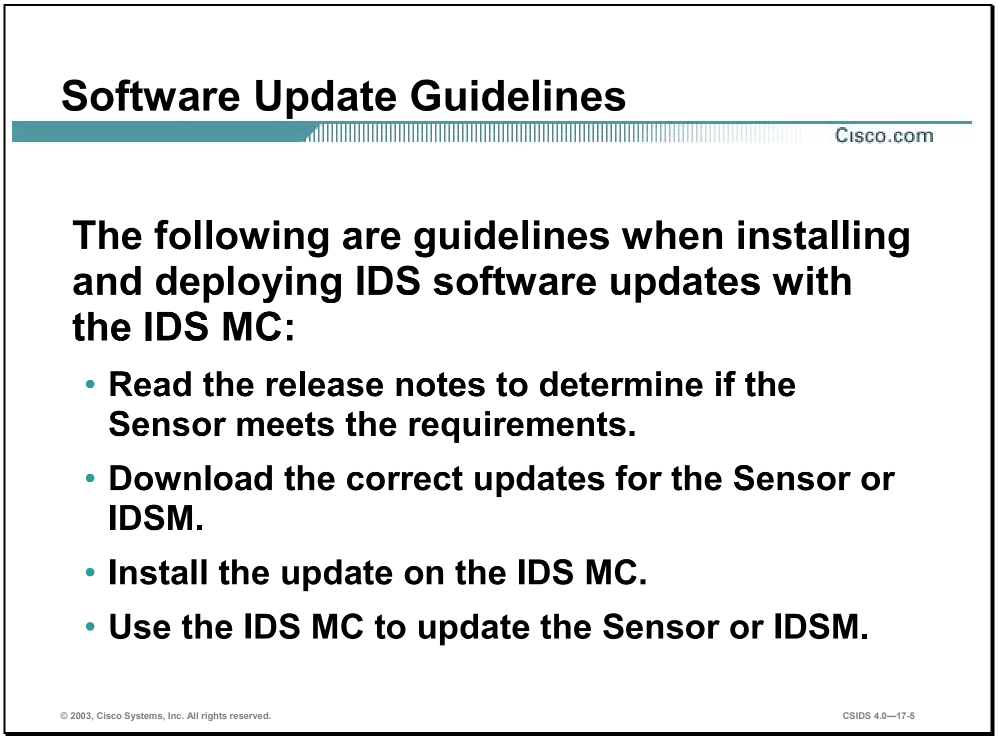
- IDS software updates provide the latest signature and intrusion detection improvements.
- New IDS signatures are released as signature updates.
- Intrusion detection improvements are released as service packs.
- Updates can be uninstalled to return the IDS software to the previous version.
- The IDS MC must be updated to configure new signatures and IDS features.

CSIDS 4.0—17-4

New vulnerabilities that pose a threat to networks and hosts are discovered everyday. Cisco releases signature updates to meet the requirements to detect attacks launched against a network using the new vulnerabilities. Cisco also releases service packs to improve the Sensor's intrusion detection capabilities.

The installation of IDS software updates can be performed from the supported management consoles or from the command line interface (CLI). Updates can be uninstalled to the previous version if needed.

In addition to updating a Sensor, you must update the IDS MC for it to be able to understand the software installed on the Sensor or IDSM.



Software Update Guidelines

Cisco.com

The following are guidelines when installing and deploying IDS software updates with the IDS MC:

- Read the release notes to determine if the Sensor meets the requirements.
- Download the correct updates for the Sensor or IDSM.
- Install the update on the IDS MC.
- Use the IDS MC to update the Sensor or IDSM.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—17-5

The following are guidelines when installing and deploying IDS software updates:

- Read the release notes to determine if the Sensor meets the requirements—The release notes contain caveats and known issues that may arise if the update is installed.
- Download the correct updates for the Sensor or the IDSM2.
- Install the update on the IDS MC—The IDS MC must be updated to configure the new signatures and IDS features.
- Use the IDS MC to update the Sensor or IDSM2—The IDS MC should be used to update the Sensor or IDSM2.

Note It is possible to update the Sensor or IDSM independently of the IDS MC; however, you must update the IDS MC with the same version of software update that you did with the IDSM or Sensor. Otherwise, you run the risk of configuration issues between the IDS MC and the Sensor or IDSM.

You can find the IDS Event Viewer, signature updates, service pack updates, BIOS upgrades, Readme files, and other IDS version 4.0 software updates in the Software Center on Cisco.com at the following URL:

`http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/`

For IDS MC software, go to the following URL:

```
http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids
```

Note You must be logged into Cisco.com to access the Software Center.

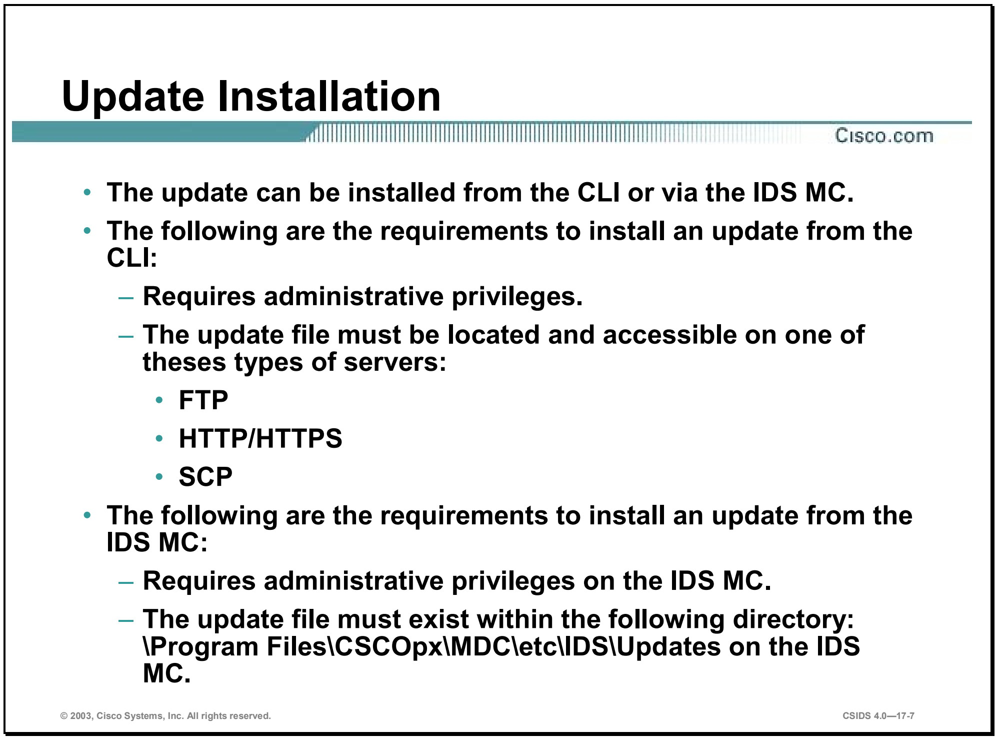
Signature updates, which also contain Network Security Database (NSDB) updates, occur every two weeks, and service packs occur as the product is upgraded. You need a Cisco.com password to download updates. Check Cisco.com regularly for the latest signature and service pack updates. You can subscribe to the Cisco IDS Active Update Notifications on Cisco.com to receive emails when signature updates and service pack updates occur.

Go to the following URL to receive notification about signature updates:

```
http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html
```

Sensor Maintenance

This section explains the installation process for Sensor signature updates and service packs. It also explains how to recover the software image if it becomes corrupted.



Update Installation

Cisco.com

- The update can be installed from the CLI or via the IDS MC.
- The following are the requirements to install an update from the CLI:
  - – Requires administrative privileges.
  - – The update file must be located and accessible on one of theses types of servers:
    - FTP
    - HTTP/HTTPS
    - SCP
- The following are the requirements to install an update from the IDS MC:
  - – Requires administrative privileges on the IDS MC.
  - – The update file must exist within the following directory: \Program Files\CSCOpx\MDC\etc\IDS\Updates on the IDS MC.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—17-7

The Sensor software can be updated using the following methods:

- CLI—This method involves using the **upgrade** command.
- IDS MC—The IDS MC pushes the update file to the Sensor.

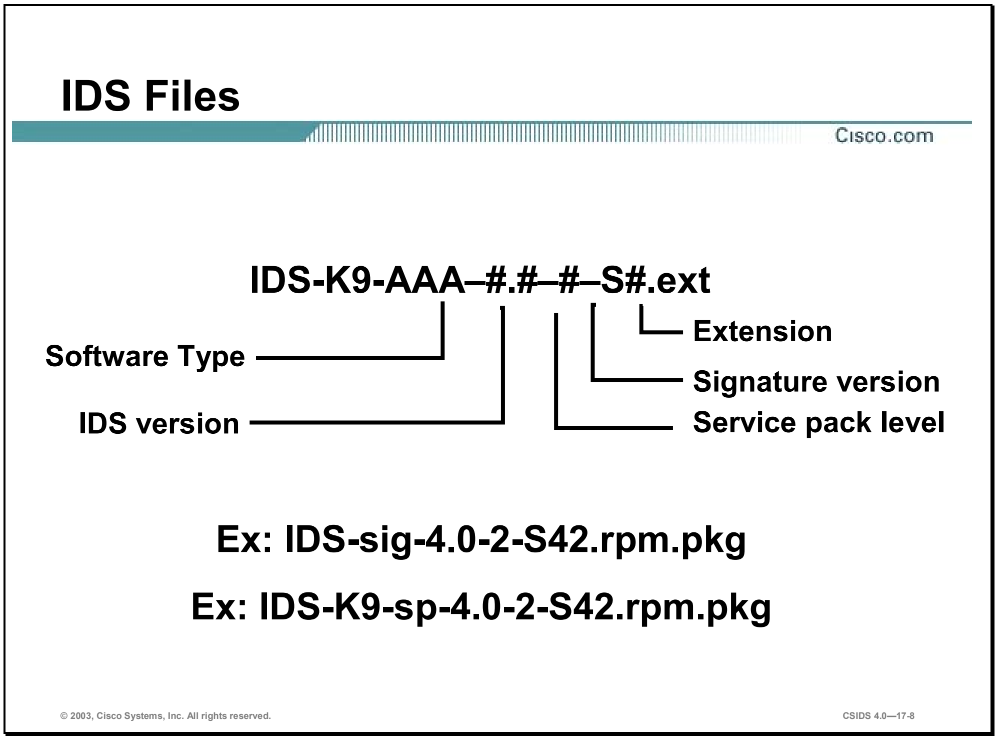
The following are the requirements to install an update from the CLI:

- Requires administrative user privileges—This involves logging in to the Sensor as a user with the necessary permissions.
- The update file must be located on one of these types of servers:
  - — FTP—Source URL for File Transfer Protocol network server.
  - — HTTPS—Source URL for web server.
  - — SCP—Source URL for the Secure Copy Protocol network server.
  - — HTTP—Source URL for web server.

The following are the requirements to install an update from the IDS MC:

- Requires administrative privileges on the IDS MC—This involves logging in to the IDS MC as a user with administrative privileges.

- The update file must exist on the IDS MC—The update files should reside on the IDS MC at X:\Program Files\CSCOpx\MDC\etc\IDS\Updates, where X: is the default drive where the IDS MC is installed.



IDS Files

Cisco.com

IDS-K9-AAA–#.#–#–S#.ext

Software Type

IDS version

Extension

Signature version

Service pack level

Ex: IDS-sig-4.0-2-S42.rpm.pkg

Ex: IDS-K9-sp-4.0-2-S42.rpm.pkg

© 2003, Cisco Systems, Inc. All rights reserved.

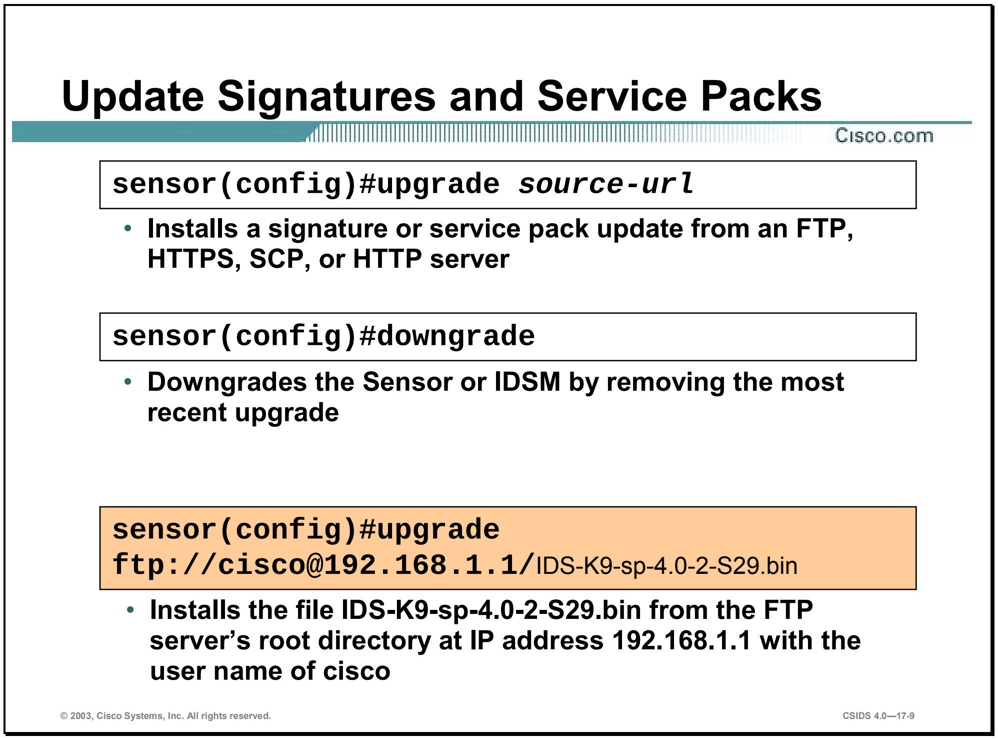
CSIDS 4.0—17-8

A Cisco IDS software filename has the following parts:

- Software type:
  - Service packs (sp)—Cisco IDS engine fixes
  - Signatures (sig)—Cisco IDS signature updates
- Cisco IDS version—The version is represented by a numeric value and is separated by a decimal. The preceding number is the major version and the later is the minor version.
- Service pack level—The service pack level identifies the level at which the IDS has been patched.
- Signature version—The signature version is the Cisco IDS major and minor release number.
- Extension—The filename extension can be one the following:
  - **rpm.pkg**—Executable file that contains signature or service pack updates.
  - **readme**—Text file containing information associated with signature or service pack updates.

An example of a Cisco IDS software file is IDS-K9-sp-4.0-2-S42.rpm.pkg This filename represents service pack update 42 for IDS major version 4.0, with service pack level 2.

Note The update files for both Sensor software versions and signatures are compressed (.zip) files. The IDS MC works with these compressed files directly; therefore, you should not unzip them or extract anything from them.



Update Signatures and Service Packs

Cisco.com

```
sensor(config)#upgrade source-url
```

- Installs a signature or service pack update from an FTP, HTTPS, SCP, or HTTP server

```
sensor(config)#downgrade
```

- Downgrades the Sensor or IDSM by removing the most recent upgrade

```
sensor(config)#upgrade
ftp://cisco@192.168.1.1/IDS-K9-sp-4.0-2-S29.bin
```

- Installs the file IDS-K9-sp-4.0-2-S29.bin from the FTP server's root directory at IP address 192.168.1.1 with the user name of cisco

CSIDS 4.0—17-9

The IDS software update can be installed or uninstalled by executing the **upgrade** command from the configuration prompt of the Sensor or IDSM.

From the command line, you can enter all necessary source and destination URL information and the username. If you enter only the command, **upgrade**, followed by a prefix, ftp or scp, you are prompted for any missing information, including a password where applicable.

Note The directory specification should be an absolute path to the desired file. The filename is optional. For recurring upgrades, a filename will not be present.

Use the following guidelines when designating the source or destination:

- FTP—Source URL for File Transfer Protocol network server. The syntax for this prefix is ftp:[[//username@]location]/relativeDirectory/filename or ftp:[[//username@]location]//absoluteDirectory/filename.

- HTTPS—Source URL for web server. The syntax for this prefix is https:[[//username@]location]/directory]/filename.

- SCP—Source URL for the Secure Copy Protocol network server. The syntax for this prefix is scp:[[//username@]location]/relativeDirectory]/filename or scp:[[//username@]location]//absoluteDirectory]/filename.

- HTTP—Source URL for web server. The syntax for this prefix is http:[[//username@]location]/directory]/filename.

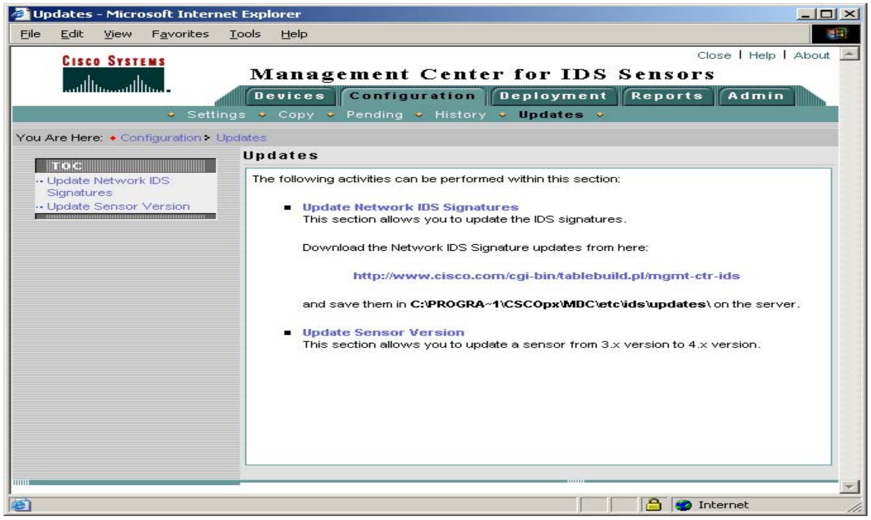
The **downgrade** command is used to remove the most recent upgrade or update to the Sensor or IDSM. The command is issued at the configuration prompt and is as follows:

```
sensor(config)#downgrade

Warning: Executing this command will reboot the system and downgrade to IDS-
K9-sp-4.0-2-S29.rpm. Configuration changes made since the last upgrade will be
lost and the system may be rebooted.

Continue with downgrade?:yes
```

IDS Software Updates

Cisco.com

Choose Configuration>Updates.


Updates - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Close | Help | About
Management Center for IDS Sensors
Devices Configuration Deployment Reports Admin
Settings Copy Pending History Updates
You Are Here: Configuration > Updates
TOC
Update Network IDS Signatures
Update Sensor Version
Internet

Updates

The following activities can be performed within this section:

- Update Network IDS Signatures
  This section allows you to update the IDS signatures.

  Download the Network IDS Signature updates from here:

  http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids

  and save them in **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates** on the server.
- Update Sensor Version
  This section allows you to update a sensor from 3.x version to 4.x version.

CSIDS 4.0—17-10

The IDS MC allows you to update IDS appliance signatures or Sensor versions through separate GUI interfaces.

Complete the following steps to update IDS signatures:

Step 1 Download the IDS MC updates from the CCO at:

http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids

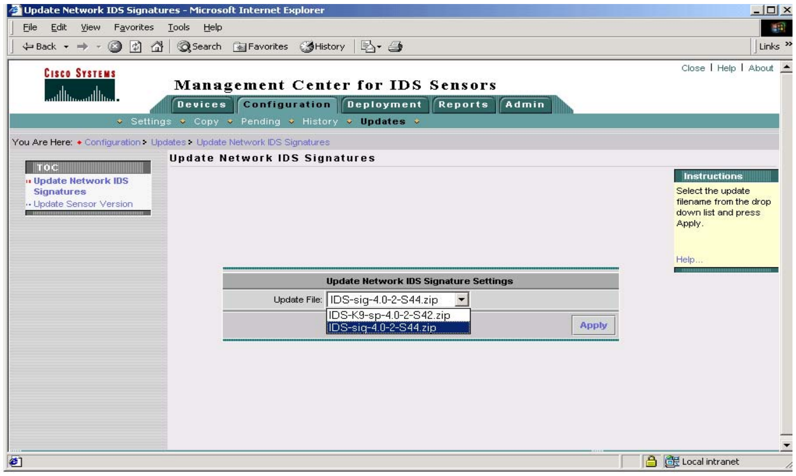
Note	Use your CCO login to download the IDS MC updates. Be aware there are other updates for IDS software located here. Read the descriptions carefully.

Step 2 After you have downloaded them, place the IDS MC updates in **X:\Program Files\CSCOpx\MDC\etc\ids\updates** (where X is the default drive letter).

Step 3 From within the IDS MC, Choose **Configuration>Updates**. The Updates page is displayed.

Step 4 Select **Update Network IDS Signatures** from the TOC. The Update Network IDS Signatures page is displayed.

IDS Signature Updates


Update Network IDS Signatures - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links
Cisco Systems
Close | Help | About
Management Center for IDS Sensors
Devices Configuration Deployment Reports Admin
Settings Copy Pending History Updates
TOC
Update Network IDS Signatures
Update Sensor Version
Instructions
Help...
Apply
Local intranet

You Are Here: Configuration > Updates > Update Network IDS Signatures

Update Network IDS Signatures

Select the update filename from the drop down list and press Apply.

Update Network IDS Signature Settings

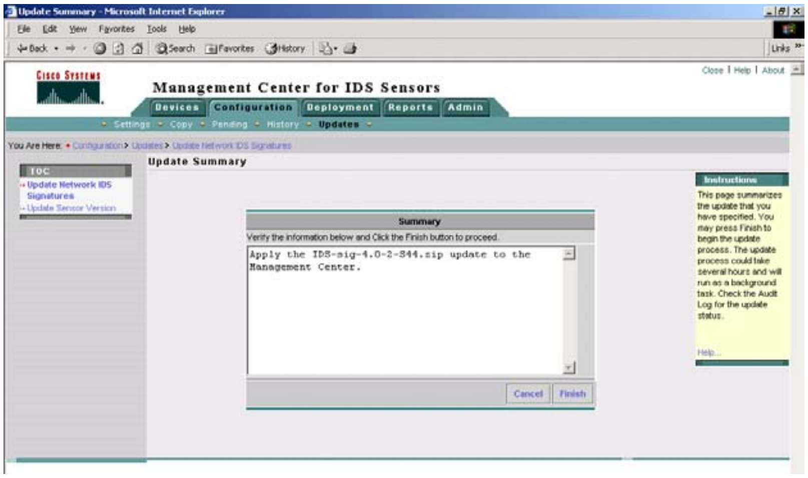
Update File: IDS-sig-4.0-2-S44.zip

IDS-K9-sp-4.0-2-S42.zip
IDS-sig-4.0-2-S44.zip

Step 5 Click **Apply**. The Update Summary page is displayed.

IDS Signature Updates (cont.)

Cisco.com


Update Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Links
Cisco Systems
Close | Help | About
Management Center for IDS Sensors
Devices Configuration Deployment Reports Admin
Settings Copy Pending History Updates
You Are Here: Configuration > Updates > Update Network IDS Signatures
TOC
Update Network IDS Signatures
Update Sensor Version
Cancel
Finish
Help...

Update Summary

Summary

Verify the information below and Click the Finish button to proceed.

```
Apply the IDS-sig-4.0-2-S44.zip update to the
Management Center.
```

Instructions

This page summarizes the update that you have specified. You may press Finish to begin the update process. The update process could take several hours and will run as a background task. Check the Audit Log for the update status.

CSIDS 4.0—17-12

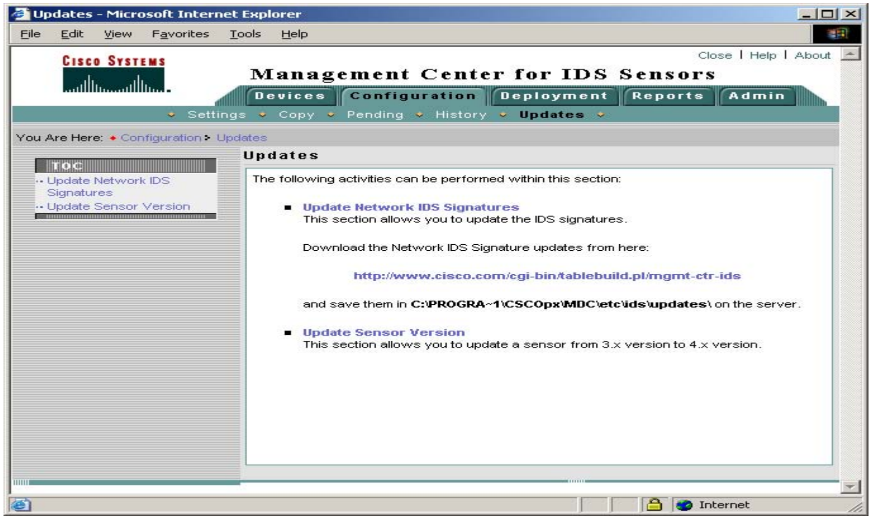
Step 6 Click **Finish**. The Update Network IDS Signatures page is displayed.

Note	Depending on the size of the signature or service pack update, the IDS MC might take a while to update.

IDS Sensor Updates

Cisco.com

Choose Configuration>Updates.


Updates - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Close | Help | About
Management Center for IDS Sensors
Devices
Configuration
Deployment
Reports
Admin
Settings
Copy
Pending
History
Updates
You Are Here: Configuration > Updates
TOC
Update Network IDS Signatures
Update Sensor Version
Internet

Updates

The following activities can be performed within this section:

- **Update Network IDS Signatures**
  This section allows you to update the IDS signatures.

  Download the Network IDS Signature updates from here:

  http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids

  and save them in **C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\** on the server.
- **Update Sensor Version**
  This section allows you to update a sensor from 3.x version to 4.x version.

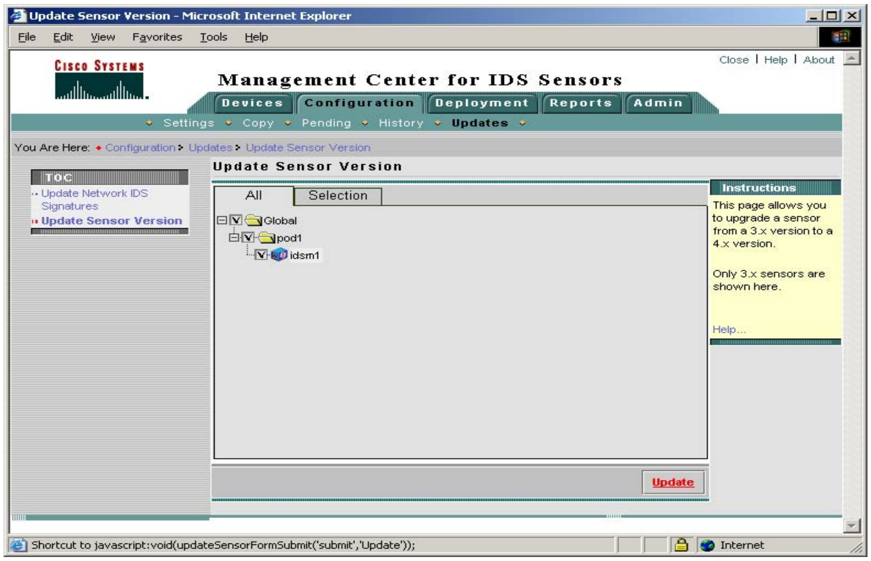
CSIDS 4.0—17-13

The other option to update a Sensor or IDSM is to update its Sensor software, a service pack. Complete the following steps to update the software version:

Step 1 Choose **Configuration>Updates**. The Updates page is displayed.

Step 2 Select **Update Network IDS Signatures** from the TOC. The Update Sensor Version page is displayed.

IDS Sensor Updates (cont.)



Update Sensor Version - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Close | Help | About
Cisco Systems
Management Center for IDS Sensors
Devices Configuration Deployment Reports Admin
Settings Copy Pending History Updates
You Are Here: Configuration > Updates > Update Sensor Version
TOC
Update Network IDS Signatures
Update Sensor Version
All Selection
Global
pod1
idsm1
Instructions
Help...
Update
Internet

Update Sensor Version

This page allows you to upgrade a sensor from a 3.x version to a 4.x version.

Only 3.x sensors are shown here.

Shortcut to javascript:void(updateSensorFormSubmit('submit','Update'));

Step 3 Select the check box next to the Sensor or IDSM that you wish to update and click **Update**. The Update Status page is displayed.

Note Only Sensors or IDSMs that may be updated through the IDS MC are shown. If you are in doubt as to whether or not the Sensor or IDSM may be updated with the IDS MC, check the IDS appliance's software version.

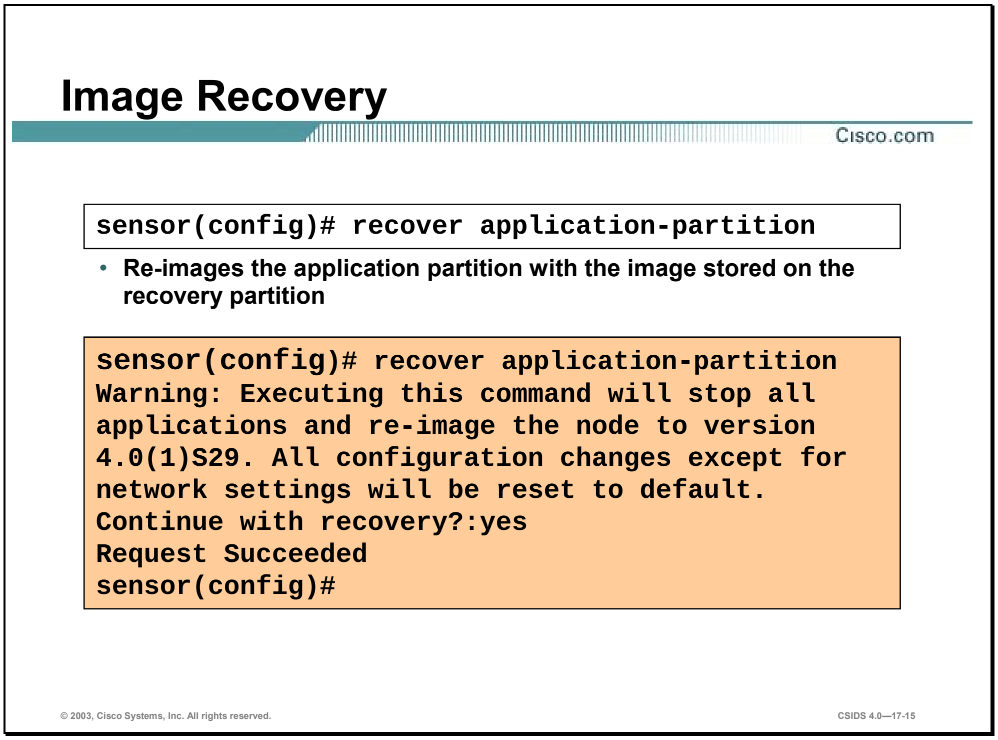


Image Recovery

```
sensor(config)# recover application-partition
```

- Re-images the application partition with the image stored on the recovery partition

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all
applications and re-image the node to version
4.0(1)S29. All configuration changes except for
network settings will be reset to default.
Continue with recovery?:yes
Request Succeeded
sensor(config)#
```

You can recover the Sensor's software image if it becomes corrupted. When you re-image the Sensor, all accounts are removed and the default cisco account is reset to use the default password cisco. After you re-image the Sensor, you must initialize it again using the **setup** command.

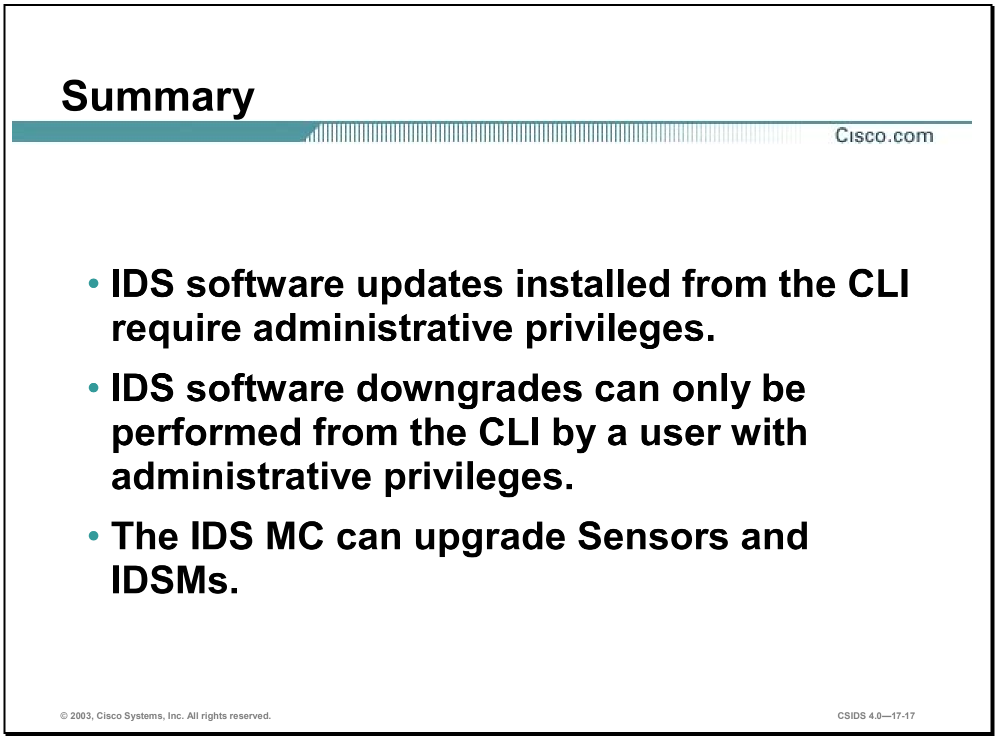
You can re-image the Sensor via the recovery partition or the upgrade and recovery CD. To re-image the Sensor via the recovery partition, use the **recover** command from the CLI. This command re-images the application partition with the application image stored on the recovery partition. The Sensor is re-booted multiple times, and all configurations except the basic network parameters such as IP address are reset to the defaults. For this reason, you should back up the current configuration before initiating a recovery.

Note If the binaries on the recovery partition were to become corrupted, you could also re-image the recovery partition from the application partition if you have a good image on the application partition.

Signature and service pack updates are not applied to the recovery partition. Therefore, you need to keep your recovery partition updated with signature and service packs or run an upgrade after you do a recovery.

Summary

This section summarizes what you have learned in this chapter.



Summary

Cisco.com

- IDS software updates installed from the CLI require administrative privileges.
- IDS software downgrades can only be performed from the CLI by a user with administrative privileges.
- The IDS MC can upgrade Sensors and IDSMs.

CSIDS 4.0—17-17

Lab Exercise—Cisco IDS System Maintenance

Complete the following lab exercise to practice what you learned in this chapter.

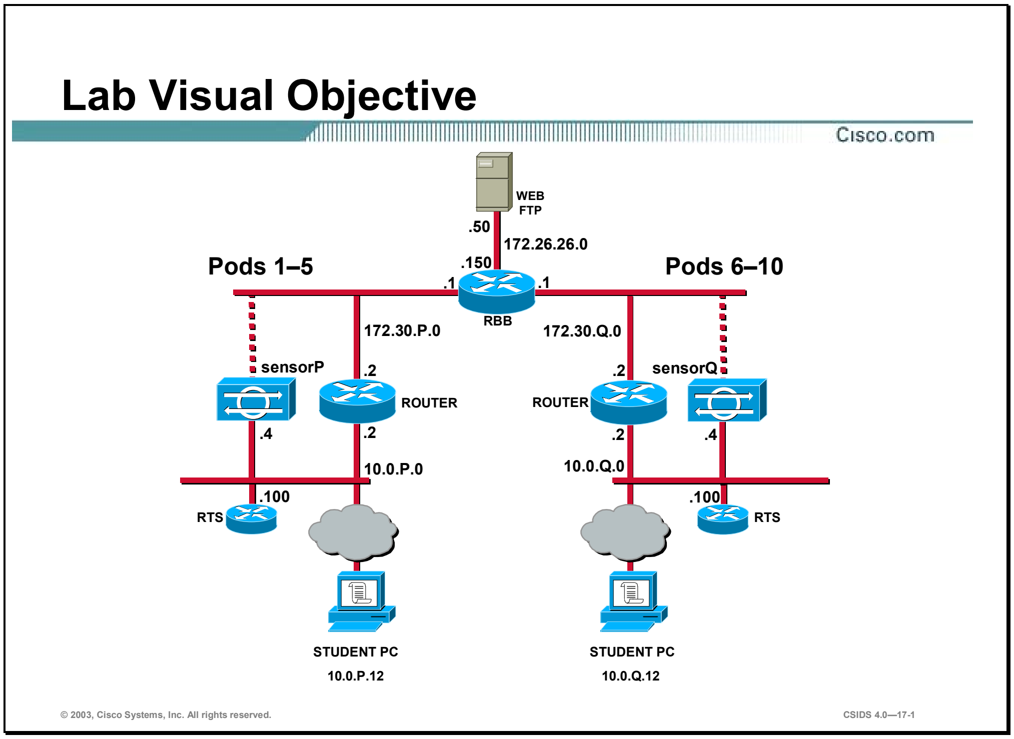
Objectives

In this lab exercise you will complete the following tasks:

- Update the IDS Sensor service pack.
- Verify that the update was applied.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Lab Visual Objective

Task 1—Update the IDS Sensor Service Pack

Complete the following steps to update the IDS Sensor service pack:

Step 1 Locate the IDS software updates as directed to by your instructor.

Step 2 Copy the updates to the following folder on your student PC: C:\Program Files\CSCOpx\MDC\etc\ids\updates.

Step 3 Log in to the IDS MC.

Step 4 Choose **Configuration>Updates**. The Updates page is displayed.

Step 5 Select **Update Network IDS Signatures** from the TOC. The Update Network IDS Signatures page is displayed.

Step 6 Select **IDS-K9-sp-4.0-2-S42.zip** from the Update File drop-down menu.

Step 7 Click **Apply**. The Select Sensors to Update page is displayed.

Step 8 Select the check box to the left of your Sensor's IP address and click **Next**. The Update Summary page is displayed.

Step 9 Click **Finish**.

Note	The Service Pack update may take up to 15 minutes to complete. Please be patient.

Task 2—Verify That the Update Was Applied

Complete the following steps to generate an Audit Log report and verify that the update was applied:

Step 1 Choose **Reports>Generate**. The Select Report page is displayed.

Step 2 Select **Audit Log Report** from the list of reports and click **Select**. The Report Filtering page is displayed.

Step 3 Complete the following sub-steps to configure report filtering:

1. Click the **Select All** button for the Event Severity.
2. Choose **Shared Service Processes** from the list of Applications.
3. Choose **Common Java System Services** from the list of Subsystems.
4. Click **Next**. The Schedule Report page is displayed.

Step 4 Select the **Run Now** radio button and click **Finish**. The Notifications window opens indicating the report will be listed on the Choose Completed Report page that appears in the back ground.

Note It may be necessary to wait while the report is generated from the IDS MC database. You can refresh the view by choosing **Reports>View**.

Step 5 Click **OK** in the Notifications window.

Step 6 Choose **Reports>View**. The Choose Completed Reports page refreshes and displays the completed report.

Step 7 Select the **Audit Log Report** check box and click **View**. The Audit Log Report is displayed in the Report page.

Step 8 Locate the update completion information in the Event Message column.

A

Cisco IOS Firewall Intrusion Detection System

Overview

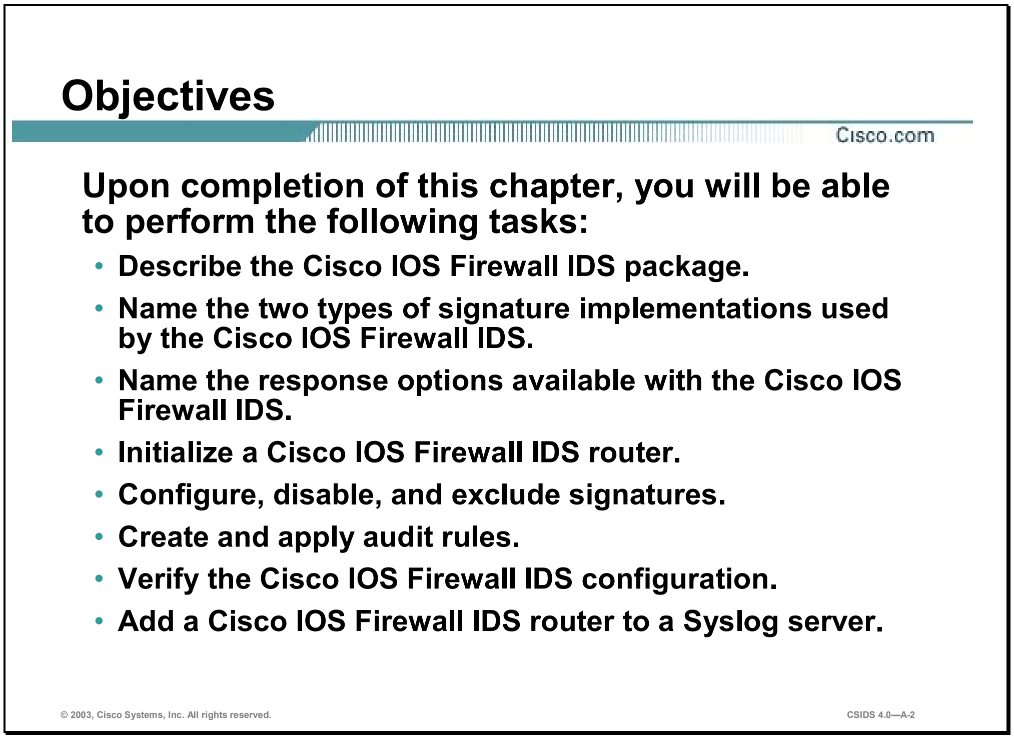
This chapter covers information on the Cisco IOS Firewall Intrusion Detection System (IDS) package for Cisco routers and how to configure it.

This chapter includes the following topics:

- Objectives
- Cisco IOS Firewall IDS introduction
- Initializing the Cisco IOS Firewall IDS
- Configuring, disabling, and excluding signatures
- Creating and applying audit rules
- Verifying the configuration
- Summary

Objectives

This section lists the chapter objectives.



Objectives

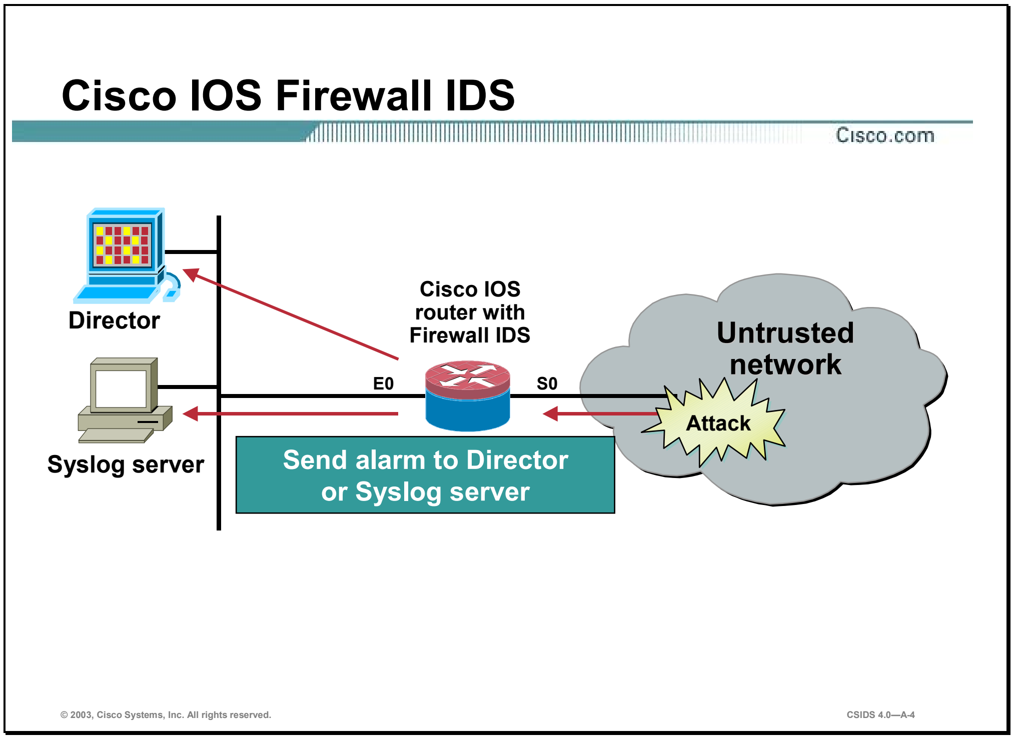
Upon completion of this chapter, you will be able to perform the following tasks:

- **Describe the Cisco IOS Firewall IDS package.**
- **Name the two types of signature implementations used by the Cisco IOS Firewall IDS.**
- **Name the response options available with the Cisco IOS Firewall IDS.**
- **Initialize a Cisco IOS Firewall IDS router.**
- **Configure, disable, and exclude signatures.**
- **Create and apply audit rules.**
- **Verify the Cisco IOS Firewall IDS configuration.**
- **Add a Cisco IOS Firewall IDS router to a Syslog server.**

CSIDS 4.0—A-2

Cisco IOS Firewall IDS Introduction

This section introduces the Cisco IOS Firewall Intrusion Detection System (IDS) feature for Cisco IOS routers.



Cisco IOS Firewall IDS

Cisco.com

Director

Syslog server

Cisco IOS router with Firewall IDS

E0

S0

Untrusted network

Attack

Send alarm to Director or Syslog server

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—A-4

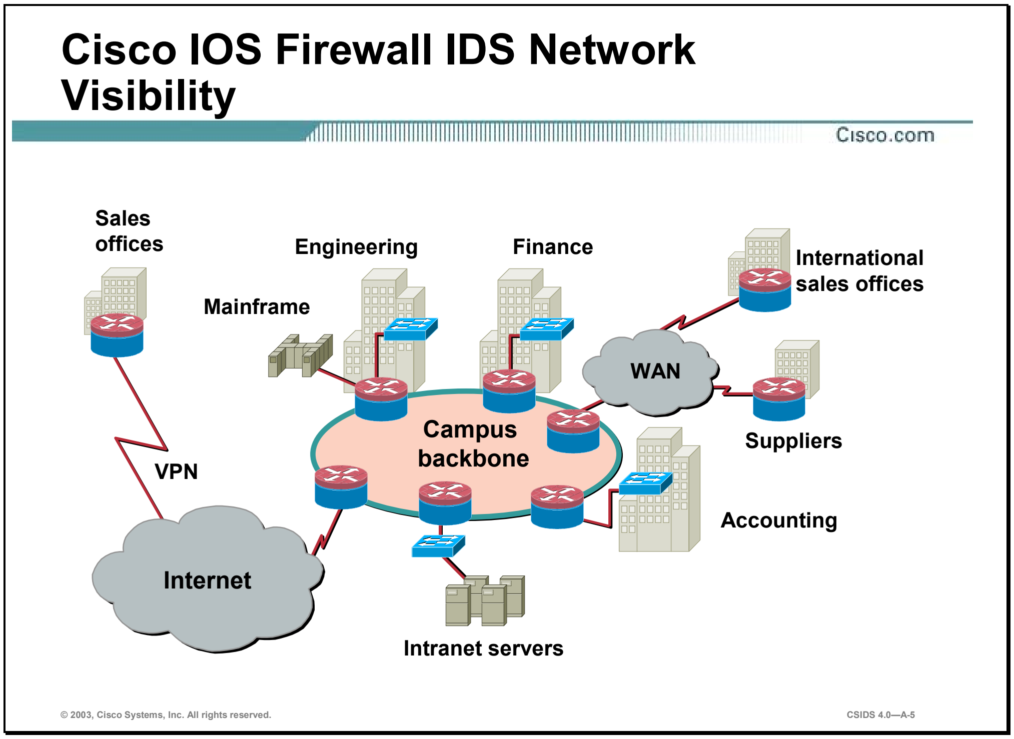
Cisco offers several non-router-based products to monitor your network including the following:

- Cisco Secure IDS Sensors—The Cisco IDS 4200 Series appliance sensors are purpose-built, high-performance network security "appliances" that protect against unauthorized, malicious activity traversing the network, such as attacks by hackers. Cisco IDS sensors analyze traffic in real time, enabling users to quickly respond to security breaches.

- Cisco Secure Intrusion Detector Director—Centrally monitors the activity of multiple Cisco Secure IDS sensors located on local or remote network segments. It is designed to address the increased requirements for security visibility, denial-of-service protection and anti-hacking detection.

The Cisco IOS Firewall IDS provides firewall and intrusion detection capabilities within a variety of Cisco IOS routers. It acts just like a Cisco Secure IDS Sensor from an intrusion detection point-of-view, and can be added to the Cisco Secure Intrusion Detector Director map as another icon to provide a consistent view of all Sensors throughout a network. The Cisco IOS Firewall IDS contains an enhanced reporting mechanism that permits logging to the router’s Syslog service in addition to the Director.

The Cisco IOS Firewall IDS provides a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. This technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.



Cisco IOS Firewall IDS Network Visibility

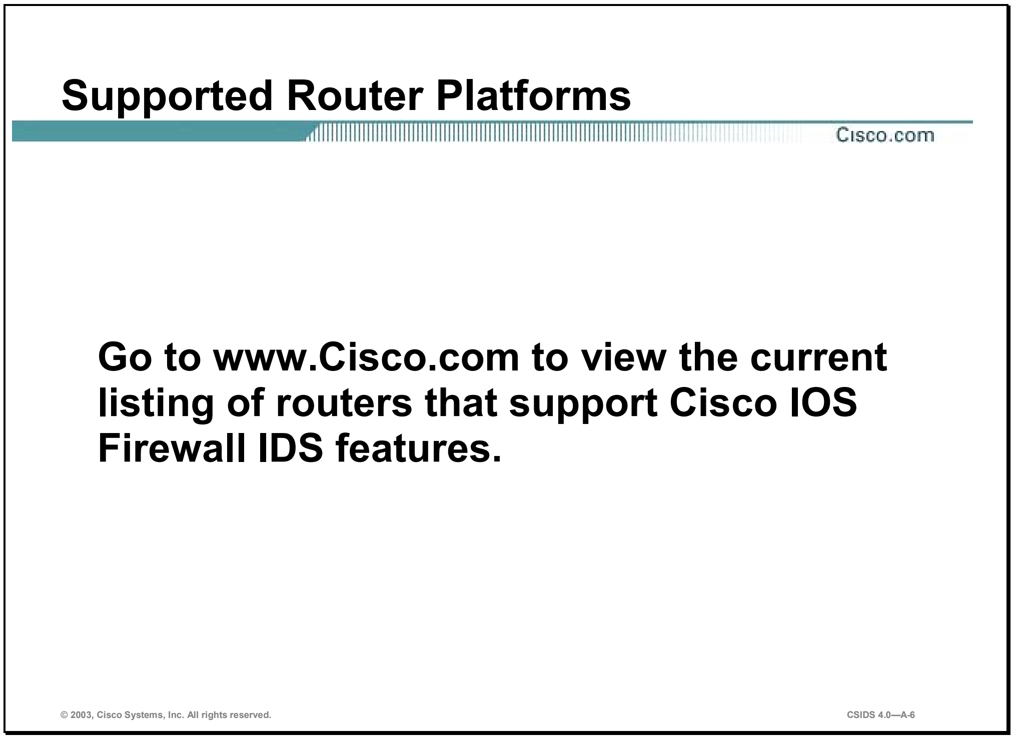
Cisco.com

CSIDS 4.0—A-5

The Cisco IOS Firewall IDS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators now have more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts. IDS signatures can be deployed alongside or independently of other Cisco IOS Firewall features. Existing Cisco IDS customers can deploy the Cisco IOS Firewall software-based IDS signatures to complement their current protection. This enables intrusion detection to be deployed to areas that may not be capable of supporting a Sensor.

The Cisco IOS Firewall IDS is intended to satisfy the security goals of all Cisco customers, and is particularly appropriate for the following:

- Enterprise customers who are interested in a cost-effective method of extending their perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters.
- Small- and medium-sized businesses that are looking for a cost-effective router that has an integrated firewall with intrusion detection capabilities.
- Service provider customers who want to set up managed services, providing firewall and intrusion detection to their customers, all housed within the necessary function of a router.

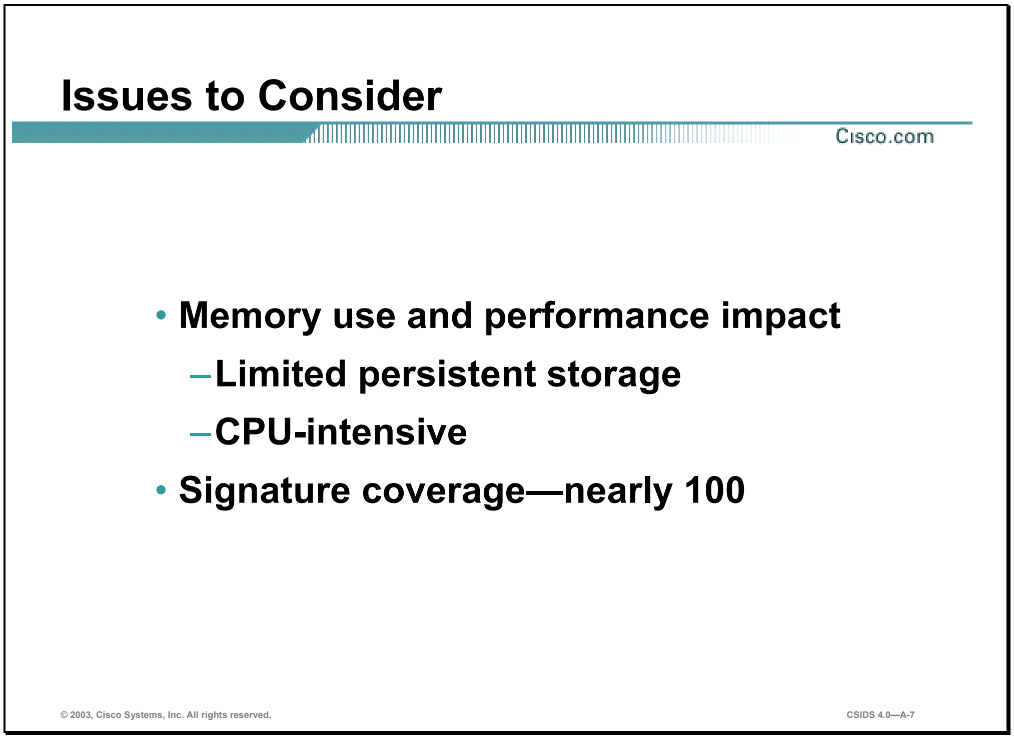


Supported Router Platforms

Go to www.Cisco.com to view the current listing of routers that support Cisco IOS Firewall IDS features.

CSIDS 4.0—A-6

Always reference the Cisco web site for up-to-date information regarding IOS Firewall IDS feature support.



Issues to Consider

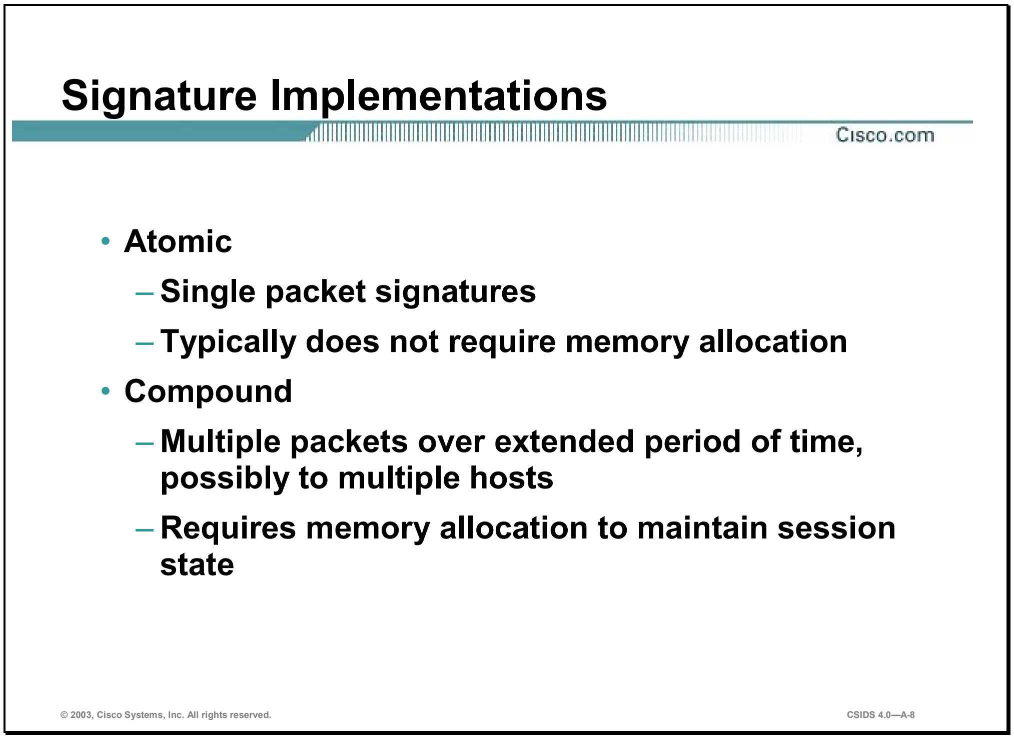
- Memory use and performance impact
  - Limited persistent storage
  - CPU-intensive
- Signature coverage—nearly 100

CSIDS 4.0—A-7

The following are issues to consider when implementing the IOS Firewall IDS:

- Memory usage and performance impact—The performance impact of intrusion detection depends on the number of signatures enabled, the level of traffic on the router, the router platform, and other individual features enabled on the router (for example, encryption and source route bridging). Because this router is being used as a security device, no packet is allowed to bypass the security mechanisms. The IDS process in the router sits directly in the packet path and thus searches each packet for signature matches. In some cases, the entire packet needs to be searched, and state information and even application state and awareness must be maintained by the router.

- Signature coverage—The Cisco IOS Firewall IDS identifies nearly 100 of the most common attacks using signatures to detect patterns of misuse in network traffic. The intrusion detection signatures were chosen from a broad cross-section of intrusion detection signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans. On the other hand, the dedicated Sensor audits over 300 signatures, providing the most comprehensive coverage on network attacks.

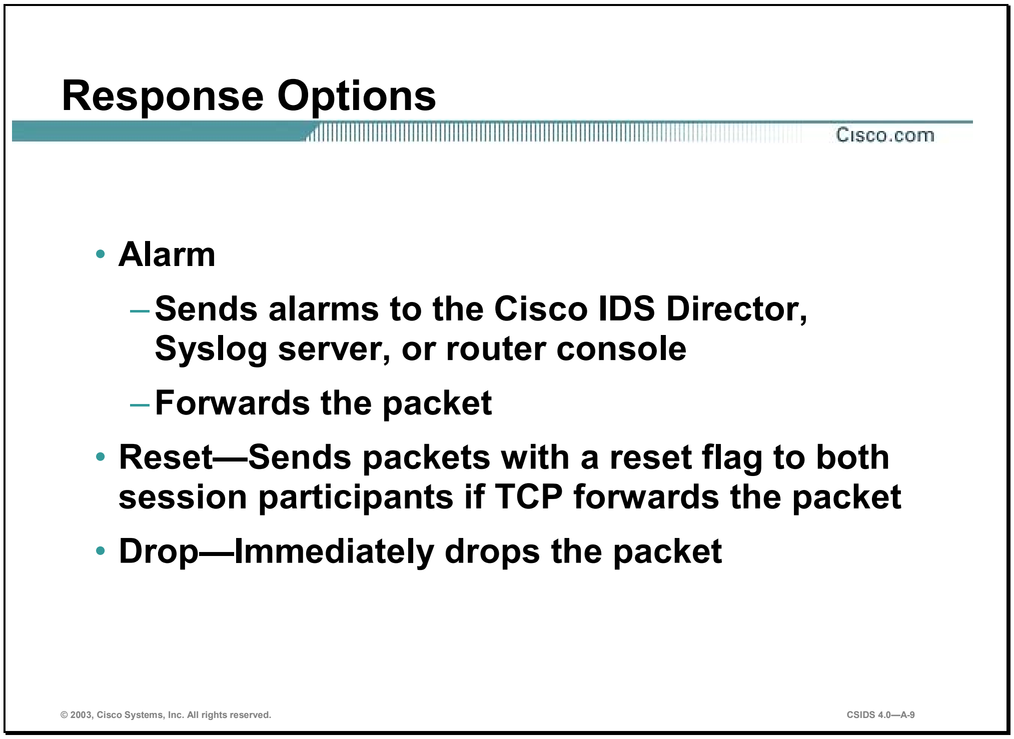


Signature Implementations

- Atomic
  - Single packet signatures
  - Typically does not require memory allocation
- Compound
  - Multiple packets over extended period of time, possibly to multiple hosts
  - Requires memory allocation to maintain session state

CSIDS 4.0—A-8

Atomic signatures are those that trigger on a single packet. For auditing atomic signatures, there is no traffic-dependent memory requirement. Compound signatures are those that trigger on multiple packets. For auditing compound signatures, the IOS Firewall IDS allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.



Response Options

- Alarm
  - Sends alarms to the Cisco IDS Director, Syslog server, or router console
  - Forwards the packet
- Reset—Sends packets with a reset flag to both session participants if TCP forwards the packet
- Drop—Immediately drops the packet

CSIDS 4.0—A-9

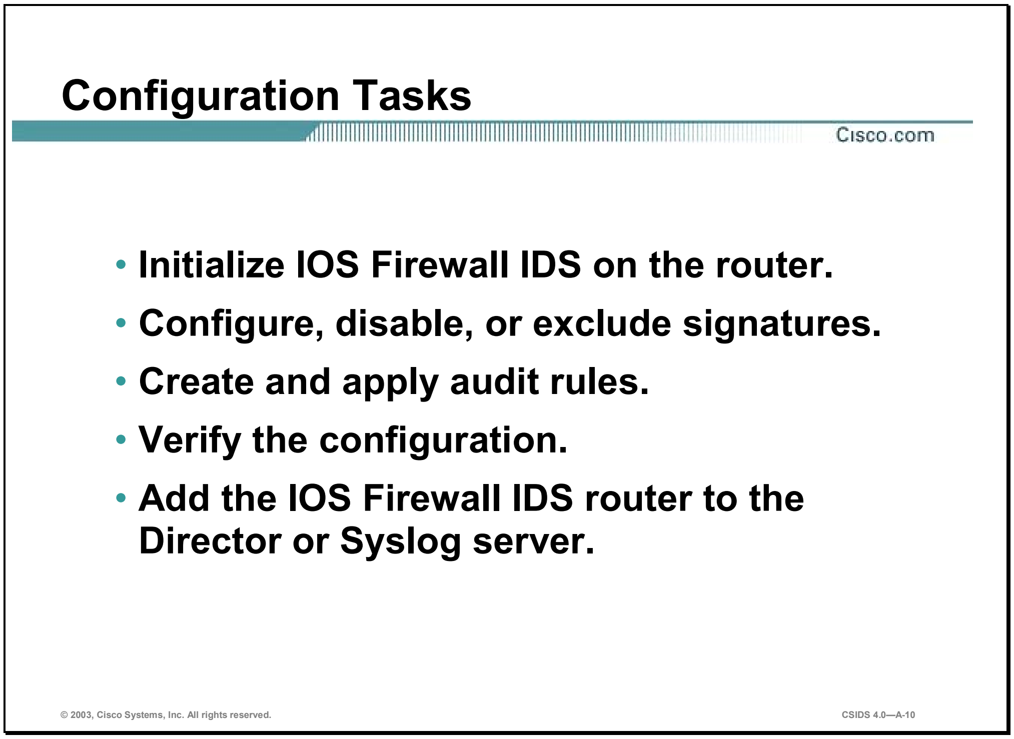
The Cisco IOS Firewall IDS acts as an in-line Sensor, watching packets as they traverse the router's interfaces, and acting upon them in a definable fashion. When a packet, or a number of packets in a session, match a signature, the IOS Firewall IDS may perform the following configurable actions:

- Alarm—Sends alarms to the Director, Syslog server, or router console, and then forwards the packet through.

- Reset—Sends packets with a reset flag to both session participants if it is a TCP session. It then forwards the packet through.

- Drop—Immediately drops the packet.

Note It is recommended that you use the drop and reset actions together to ensure that the attack is terminated.



Configuration Tasks

Cisco.com

- Initialize IOS Firewall IDS on the router.
- Configure, disable, or exclude signatures.
- Create and apply audit rules.
- Verify the configuration.
- Add the IOS Firewall IDS router to the Director or Syslog server.

CSIDS 4.0—A-10

To configure the IOS Firewall IDS on a router and to have it report alarms to a Director, complete the following tasks:

- Initialize the IOS Firewall IDS on the router—This includes setting the notification type, the router's PostOffice parameters, the Director's PostOffice parameters, the protected network definition, and the router's maximum queue size for holding alarms.

- Configure, disable, or exclude signatures—This includes setting the spam attack threshold, disabling signatures globally, and excluding signatures by host or network.

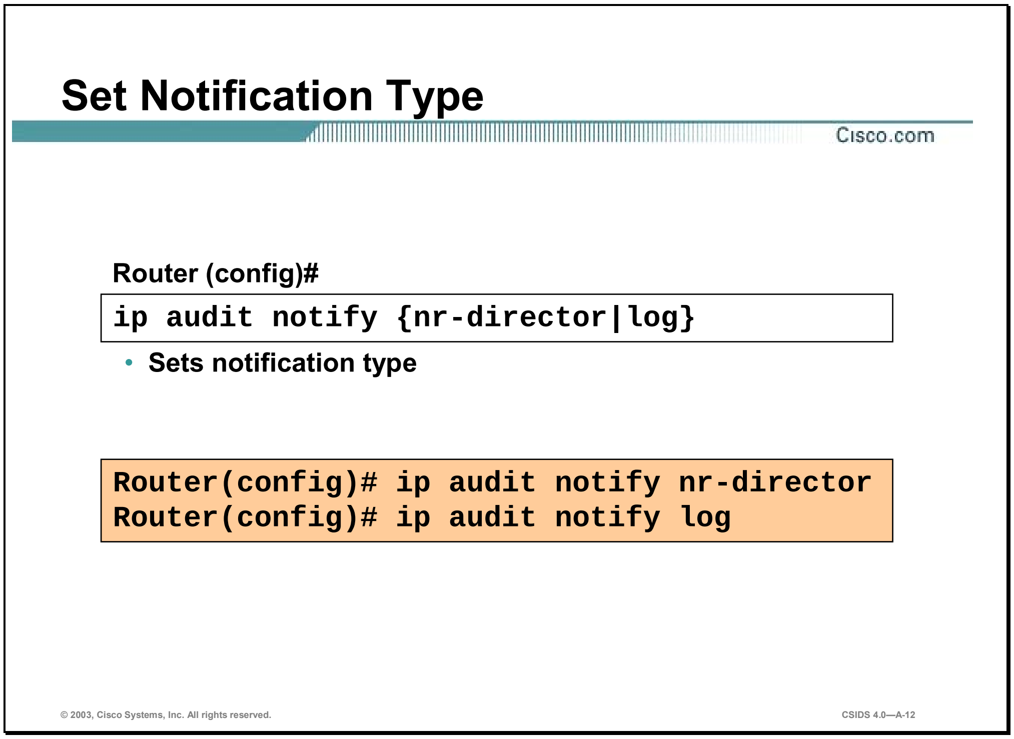
- Create and apply audit rules—This includes creating an audit rule for information or attack signatures and then applying it to an interface. Another option is to create an audit rule that excludes hosts or networks and then applying it to an interface.

- Verify the configuration—This includes using available **show**, **clear**, and **debug** commands for the IOS Firewall IDS.

- Add the IOS Firewall IDS to the Director's map—The IDS-enabled router appears as another Sensor on the Cisco IDS Home map.

Initializing the Cisco IOS Firewall IDS

This section covers the commands to set the notification type, the router's PostOffice parameters, the Director's PostOffice parameters, the protected network definition, and the router's maximum queue size for holding alarms.



Set Notification Type

Cisco.com

Router (config)#

```
ip audit notify {nr-director|log}
```

- Sets notification type

```
Router(config)# ip audit notify nr-director
Router(config)# ip audit notify log
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—A-12

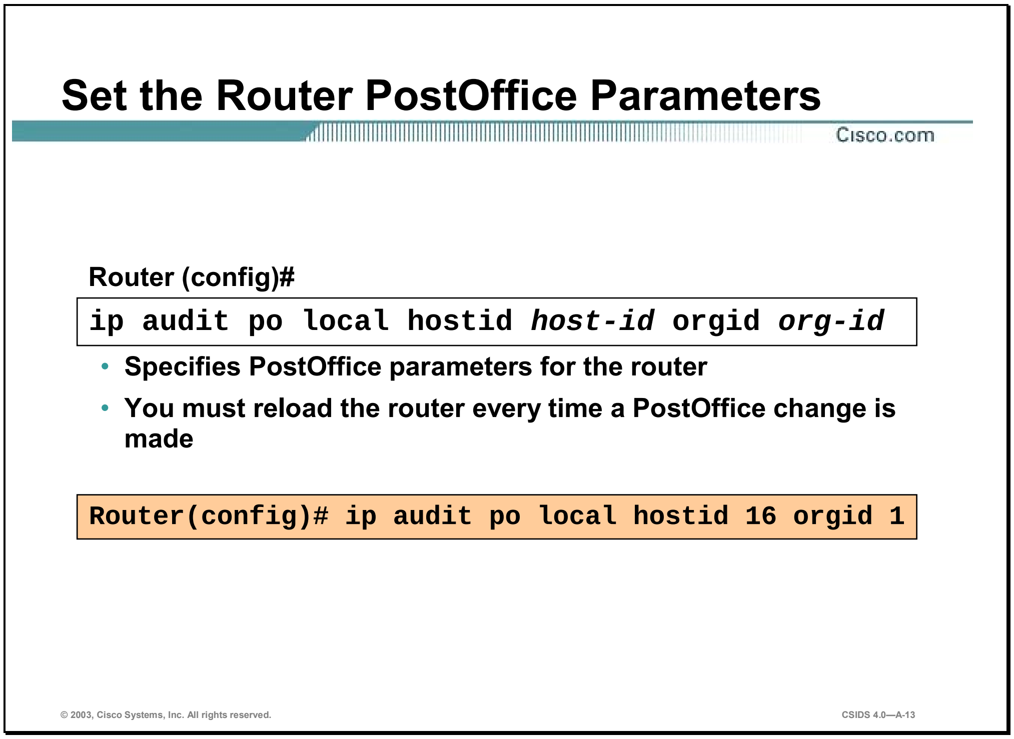
Use the **ip audit notify** global configuration command to specify the methods of alarm notification. Use the **no** form of this command to disable event notifications.

The syntax for the **ip audit notify** command is as follows:

ip audit notify {nr-director | log}

no ip audit notify {nr-director | log}

nr-director	Send messages in PostOffice format to the Director or Sensor.
log	Send messages in Syslog format to the router's console or a remote Syslog server.



Set the Router PostOffice Parameters

Router (config)#

```
ip audit po local hostid host-id orgid org-id
```

- Specifies PostOffice parameters for the router
- You must reload the router every time a PostOffice change is made

```
Router(config)# ip audit po local hostid 16 orgid 1
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—A-13

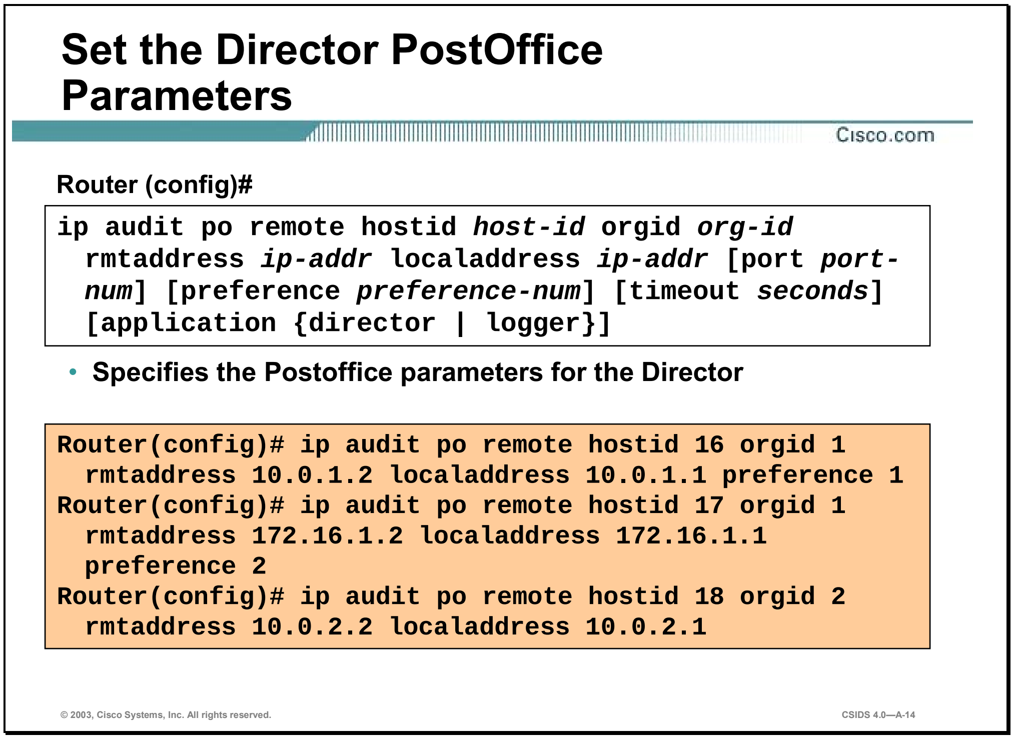
Use the **ip audit po local** global configuration command to specify the local PostOffice parameters used when sending alarm notifications to the Director. Use the **no** form of this command to set the local PostOffice parameters to their default settings.

The syntax for the **ip audit po local** command is as follows:

ip audit po local hostid ***host-id*** **orgid** ***org-id***

no ip audit po local [hostid ***host-id*** **orgid** ***org-id*****]**

hostid	Specifies a PostOffice host ID.
host-id	Unique integer in the range 1–65535 used in PostOffice communications to identify the local host. Use with the **hostid** keyword. The default host identification is 1.
orgid	Specifies a PostOffice organization ID.
org-id	Unique integer in the range 1–65535 used in PostOffice communications to identify the group to which the local host belongs. Use with the **orgid** keyword. The default organization identification is 1.



Set the Director PostOffice Parameters

Router (config)#

```
ip audit po remote hostid host-id orgid org-id
  rmtaddress ip-addr localaddress ip-addr [port port-
  num] [preference preference-num] [timeout seconds]
  [application {director | logger}]
```

- Specifies the Postoffice parameters for the Director

```
Router(config)# ip audit po remote hostid 16 orgid 1
  rmtaddress 10.0.1.2 localaddress 10.0.1.1 preference 1
Router(config)# ip audit po remote hostid 17 orgid 1
  rmtaddress 172.16.1.2 localaddress 172.16.1.1
  preference 2
Router(config)# ip audit po remote hostid 18 orgid 2
  rmtaddress 10.0.2.2 localaddress 10.0.2.1
```

Use the **ip audit po remote** global configuration command to specify one or more set of PostOffice parameters for the Director receiving alarm notifications from the router. Use the **no** form of this command to remove a Director’s PostOffice parameters as defined by host identification, organization identification, and IP address.

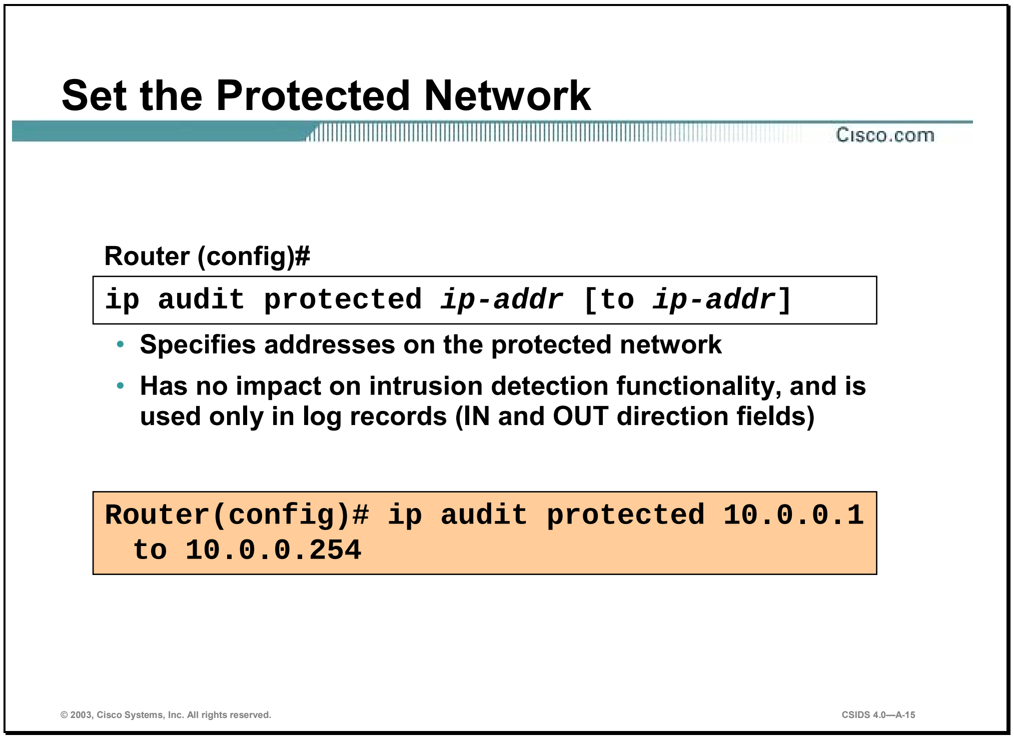
The syntax for the **ip audit po remote** command is as follows:

ip audit po remote hostid ***host-id*** **orgid** ***org-id*** **rmtaddress** ***ip-addr*** **localaddress** ***ip-addr*** **[port** ***port-num*****]** **[preference** ***preference-num*****]** **[timeout** ***seconds*****]** **[application {director | logger}]**

no ip audit po remote hostid ***host-id*** **orgid** ***org-id*** **rmtaddress** ***ip-address***

hostid	Specifies a PostOffice host identification.
host-id	Unique integer in the range 1–65535 used in PostOffice communications to identify the remote host. Use with the hostid keyword. The default host identification is 1.
orgid	Specifies a PostOffice organization identification.
org-id	Unique integer in the range 1–65535 used in PostOffice communications to identify the group to which the remote host belongs. Use with the orgid keyword.
rmtaddress	Specifies the IP address of the remote Director.
localaddress	Specifies the IP address of the Cisco IOS Firewall IDS router.
ip-addr	IP address of the Director or Cisco IOS Firewall IDS router's interface. Use with the rmtaddress and localaddress keywords.
port	Specifies a UDP port through which to send messages.
port-num	Integer representing the UDP port on which the Director is listening for alarm notifications. Use with the port keyword. The default UDP port number is 45000. The default preference is 1. The default heartbeat timeout is 5 seconds. The default application is director.

preference	Specifies an IP address preference for communication.
preference-number	Integer representing the relative priority of an IP address to a Director, if more than one IP address exists. Use with the preference keyword.
timeout	Specifies a timeout value for PostOffice communications.
seconds	Integer representing the heartbeat timeout value for PostOffice communications (the default is 5 seconds). Use with the timeout keyword.
application	Specifies the type of application that is receiving the Cisco IOS Firewall IDS alarms.
director	Specifies that the receiving application is a Director. Use with the application keyword. The default organization identification is 1.
logger	Specifies that the receiving application is a Sensor. Use with the application keyword.



Set the Protected Network

Cisco.com

Router (config)#

```
ip audit protected ip-addr [to ip-addr]
```

- Specifies addresses on the protected network
- Has no impact on intrusion detection functionality, and is used only in log records (IN and OUT direction fields)

```
Router(config)# ip audit protected 10.0.0.1
 to 10.0.0.254
```

CSIDS 4.0—A-15

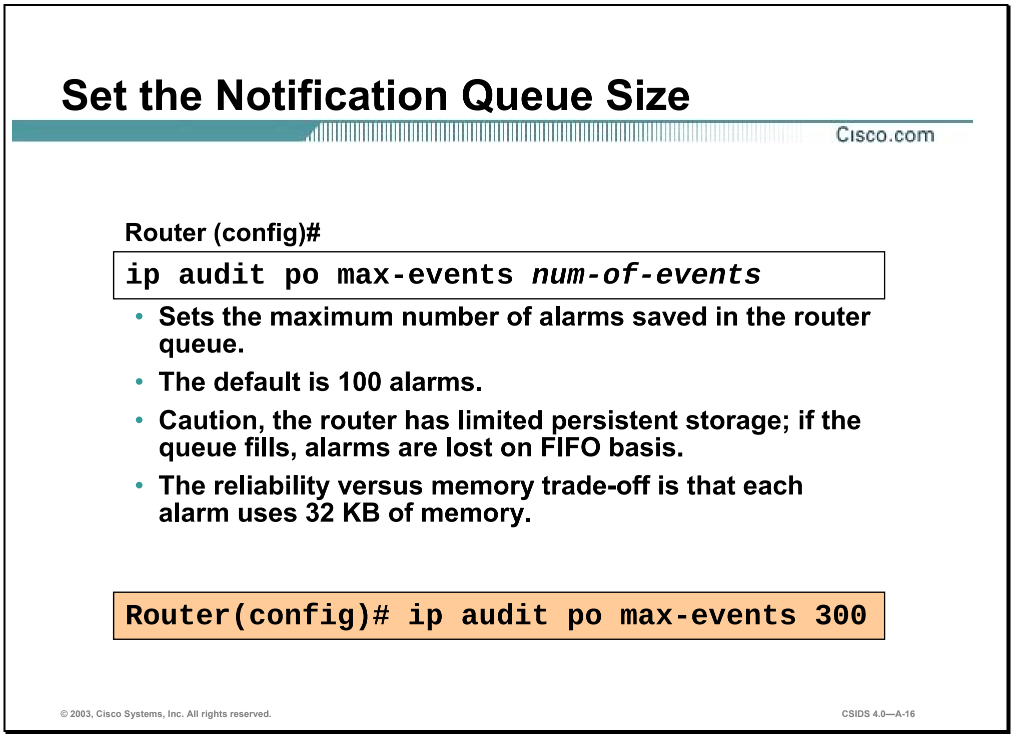
Use the **ip audit po protected** global configuration command to specify whether an IP address is on a protected network. Use the **no** form of this command to remove network addresses from the protected network list. If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

The syntax for the **ip audit po protected** command is as follows:

ip audit protected *ip-addr* [to *ip-addr*]

no ip audit protected [*ip-addr*]

to	Specifies a range of IP addresses.
ip-addr	IP address of a network host.



Set the Notification Queue Size

Cisco.com

Router (config)#

```
ip audit po max-events num-of-events
```

- Sets the maximum number of alarms saved in the router queue.
- The default is 100 alarms.
- Caution, the router has limited persistent storage; if the queue fills, alarms are lost on FIFO basis.
- The reliability versus memory trade-off is that each alarm uses 32 KB of memory.

```
Router(config)# ip audit po max-events 300
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—A-16

Use the **ip audit po max-events** global configuration command to specify the maximum number of event notifications that are placed in the router's event queue. Use the **no** version of this command to set the number of recipients to the default setting.

The syntax for the **ip audit po max-events** command is as follows:

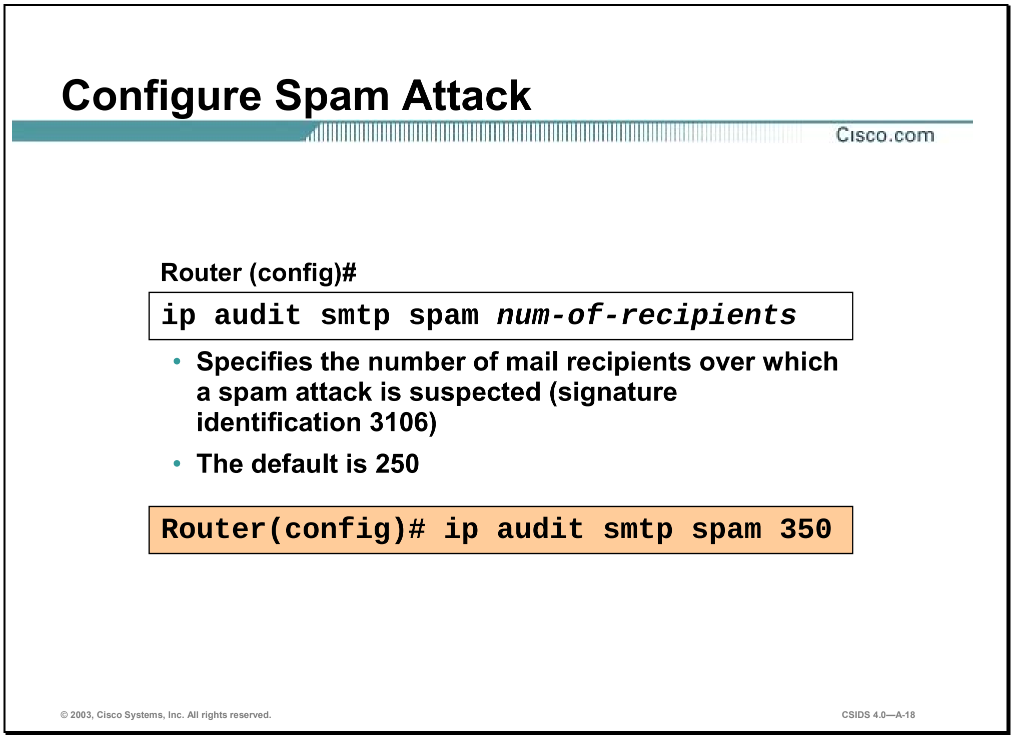
ip audit po max-events ***num-of-events***

no ip audit po max-events

number-of-events	Integer in the range of 1–65535 that designates the maximum number of events allowable in the event queue. Use with the max-events keyword. The default number of events is 100.

Configuring, Disabling, and Excluding Signatures

This section covers the commands to set the spam attack threshold, disable signatures globally, and exclude signatures by host or network.



Configure Spam Attack

Router (config)#

```
ip audit smtp spam num-of-recipients
```

- Specifies the number of mail recipients over which a spam attack is suspected (signature identification 3106)
- The default is 250

```
Router(config)# ip audit smtp spam 350
```

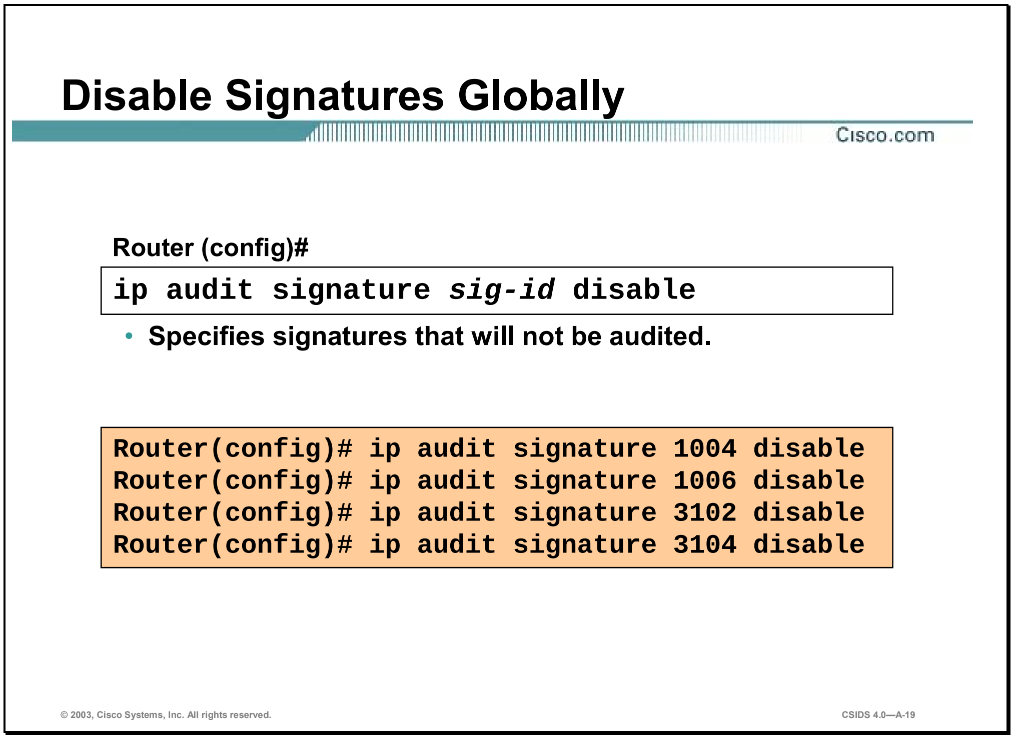
Use the **ip audit smtp spam** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected. Use the **no** version of this command to set the number of recipients to the default setting.

The syntax for the **ip audit smtp spam** command is as follows:

ip audit smtp spam ***num-of-recipients***

no ip audit smtp spam

num-of-recipients	Integer in the range of 1–65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the spam keyword. The default number of recipients is 250.



Disable Signatures Globally

Router (config)#

```
ip audit signature sig-id disable
```

- **Specifies signatures that will not be audited.**

```
Router(config)# ip audit signature 1004 disable
Router(config)# ip audit signature 1006 disable
Router(config)# ip audit signature 3102 disable
Router(config)# ip audit signature 3104 disable
```

CSIDS 4.0—A-19

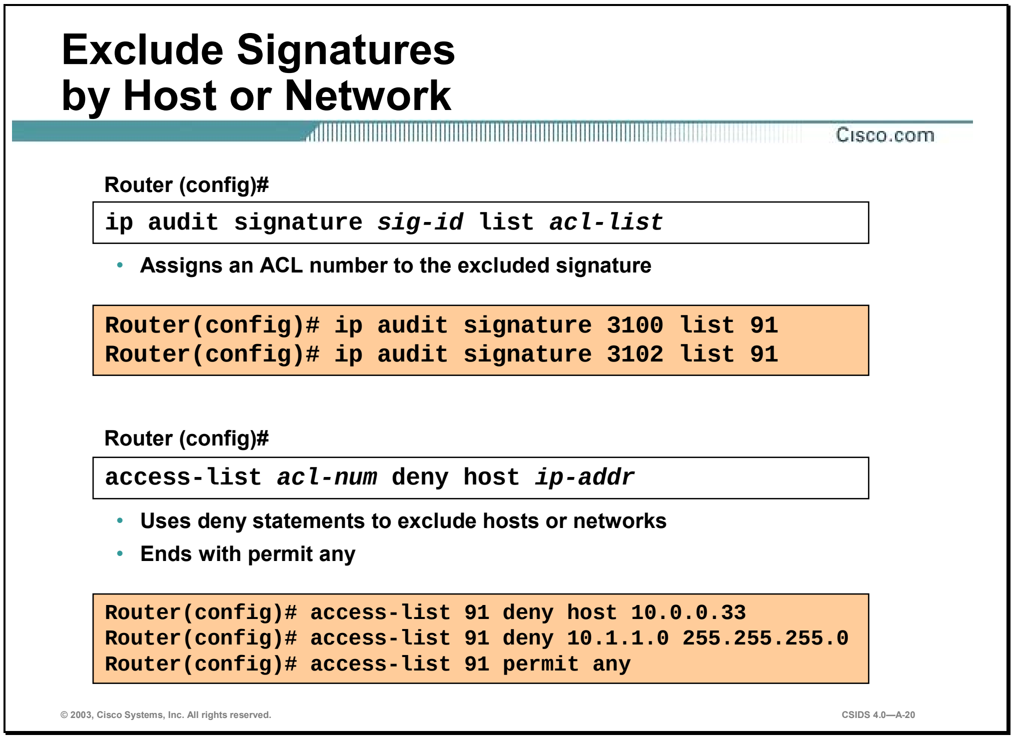
Use the **ip audit signature** global configuration command to globally disable a signature. Use the **no** form of this command to re-enable the signature.

The syntax for the **ip audit signature** command is as follows:

ip audit signature *sig-id* disable

no ip audit signature *sig-id*

sig-id	Unique integer specifying a signature as defined in the Cisco IDS Network Security Database (NSDB).
disable	Globally disables a signature from being audited by the IOS Firewall IDS router. All 59 signatures are enabled.



Exclude Signatures by Host or Network

Cisco.com

Router (config)#

```
ip audit signature sig-id list acl-list
```

- Assigns an ACL number to the excluded signature

```
Router(config)# ip audit signature 3100 list 91
Router(config)# ip audit signature 3102 list 91
```

Router (config)#

```
access-list acl-num deny host ip-addr
```

- Uses deny statements to exclude hosts or networks
- Ends with permit any

```
Router(config)# access-list 91 deny host 10.0.0.33
Router(config)# access-list 91 deny 10.1.1.0 255.255.255.0
Router(config)# access-list 91 permit any
```

CSIDS 4.0—A-20

Use the **ip audit signature** and the **access-list** global configuration commands to attach a signature to an ACL and stop the signature from triggering when generated from a given host or network. Use the **no** form of this command to remove the signature from the ACL.

The syntax for the **ip audit signature** command is as follows:

ip audit signature ***sig-id*** **list** ***acl-num***

no ip audit signature ***sig-id***

sig-id	Unique integer specifying a signature as defined in the NSDB.
list	Specifies an ACL to associate with the signature.
acl-num	Unique integer specifying a configured ACL on the router. Use with the list keyword.

The syntax for the **access-list** command is as follows:

access-list ***acl-num*** **deny [host]** ***ip-addr*** **[*wildcard*]**

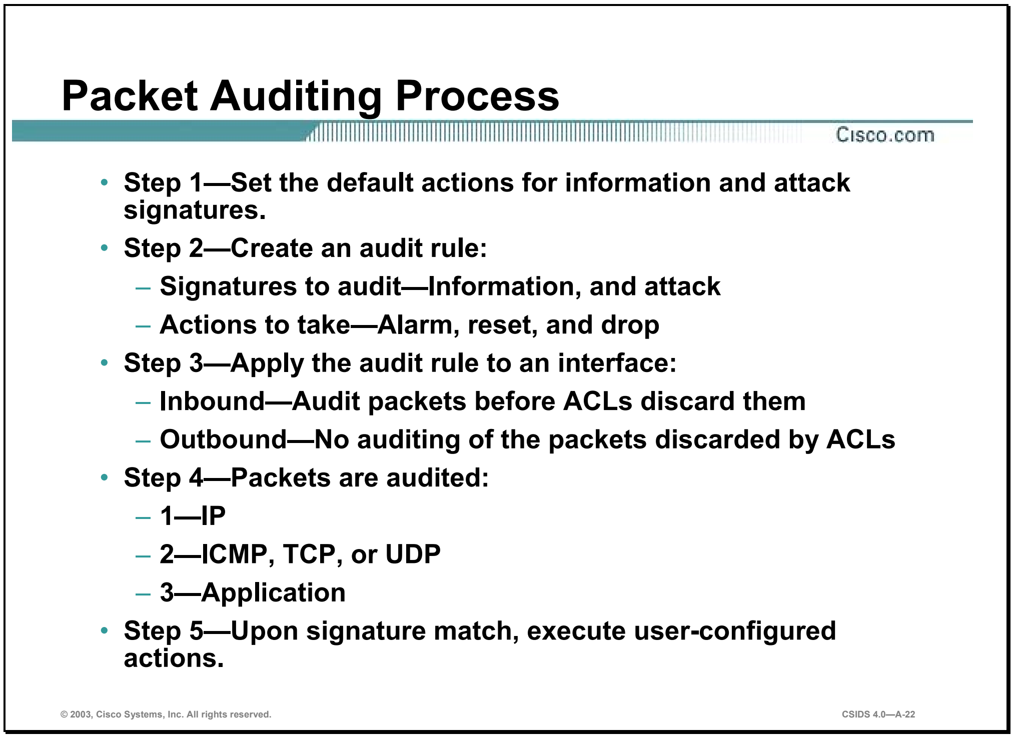
no access-list ***acl-num***

acl-num	Number of an ACL. This is a decimal number from 1 to 99.
deny	Denies signature trigger if the conditions are matched.
hosts	Identifies that the following IP address is that of a host.

ip-addr	IP address of the network or host from which the packet is being sent. There are two alternative ways to specify the source: ■ Use a four-octet, dotted-decimal IP address. ■ Use the keyword any as an abbreviation for an IP address and wildcard of 0.0.0.0 255.255.255.255.
wildcard	Wildcard bits to be applied to the IP address. There are two alternative ways to specify the source wildcard: ■ Use a four-octet, dotted-decimal format. Place ones in the bit positions you want to ignore. ■ Use the keyword any as an abbreviation for an IP address and wildcard of 0.0.0.0 255.255.255.255.

Creating and Applying Audit Rules

This section covers the commands to create the Cisco IOS Firewall IDS audit rules and apply them to an interface.



Packet Auditing Process

Cisco.com

- Step 1—Set the default actions for information and attack signatures.
- Step 2—Create an audit rule:
  - Signatures to audit—Information, and attack
  - Actions to take—Alarm, reset, and drop
- Step 3—Apply the audit rule to an interface:
  - Inbound—Audit packets before ACLs discard them
  - Outbound—No auditing of the packets discarded by ACLs
- Step 4—Packets are audited:
  - 1—IP
  - 2—ICMP, TCP, or UDP
  - 3—Application
- Step 5—Upon signature match, execute user-configured actions.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—A-22

The following describes the packet auditing process with the Cisco IOS Firewall IDS:

Step 1 Set the default actions for both information and attack signatures.

Step 2 Create an audit rule that specifies the signatures that should be applied to packet traffic and the actions to take when a match is found. An audit rule can apply information and attack signatures to network packets.

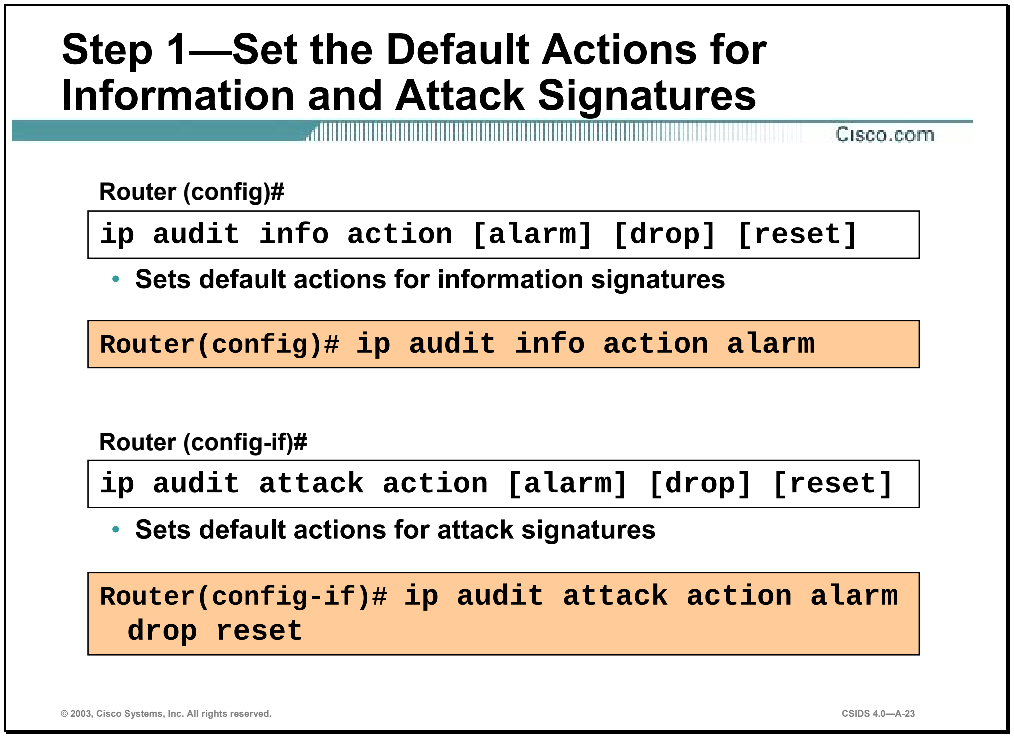
Step 3 Apply the audit rule to an interface on the router, specifying a traffic direction (in or out):

- If the audit rule is applied to the inbound direction of the interface, packets passing through the interface are audited before any inbound ACL has a chance to discard them. This enables an administrator to be alerted if an attack or reconnaissance activity is underway even if the router would normally reject the activity.

- If the audit rule is applied to the outbound 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 reconnaissance activity was thwarted.

Step 4 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.

Step 5 If a signature match is found in a module, then the user-configured actions occur.



Step 1—Set the Default Actions for Information and Attack Signatures

Router (config)#

```
ip audit info action [alarm] [drop] [reset]
```

- Sets default actions for information signatures

```
Router(config)# ip audit info action alarm
```

Router (config-if)#

```
ip audit attack action [alarm] [drop] [reset]
```

- Sets default actions for attack signatures

```
Router(config-if)# ip audit attack action alarm
  drop reset
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—A-23

Use the **ip audit info** global configuration command to specify the default actions for info signatures. Use the **no** form of this command to set the default action for info signatures.

Use the **ip audit attack** global configuration command to specify the default actions for attack signatures. Use the **no** form of this command to set the default action for attack signatures.

The syntax for the **ip audit info** command is as follows:

ip audit info action [alarm] [drop] [reset]

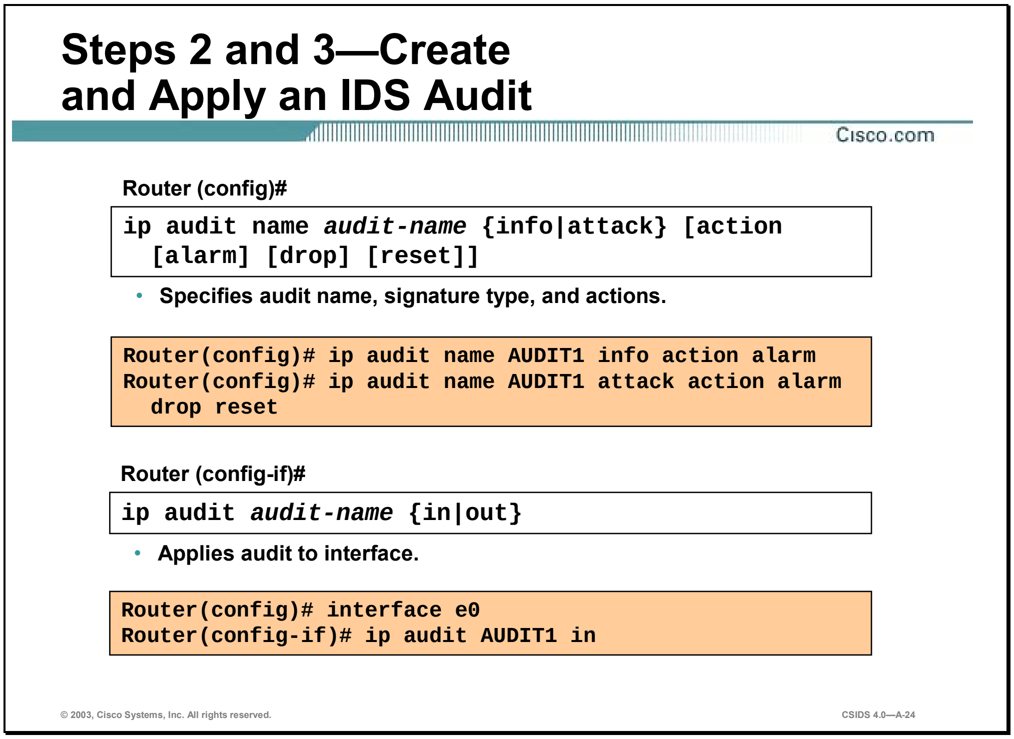
no ip audit info

The syntax for the **ip audit info** command is as follows:

ip audit attack action [alarm] [drop] [reset]

no ip audit attack

action	Sets an action for the information signature to take in response to a match. The default action is to alarm.
alarm	Sends an alarm to the console, Director, or to a Syslog server. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.



Steps 2 and 3—Create and Apply an IDS Audit

Router (config)#

```
ip audit name audit-name {info|attack} [action
  [alarm] [drop] [reset]]
```

- Specifies audit name, signature type, and actions.

```
Router(config)# ip audit name AUDIT1 info action alarm
Router(config)# ip audit name AUDIT1 attack action alarm
  drop reset
```

Router (config-if)#

```
ip audit audit-name {in|out}
```

- Applies audit to interface.

```
Router(config)# interface e0
Router(config-if)# ip audit AUDIT1 in
```

CSIDS 4.0—A-24

Use the **ip audit name** global configuration command to create audit rules for information and attack signature types. Use the **no** form of this command to delete an audit rule.

Use the **ip audit** interface configuration command to apply an audit specification created with the **ip audit name** command to a specific interface and for a specific direction. Use the **no** version of this command to disable auditing of the interface for the specified direction.

The syntax for the **ip audit name** command is as follows:

ip audit name *audit-name* {info | attack} [action [alarm] [drop] [reset]]

no ip audit name audit-name {info | attack}

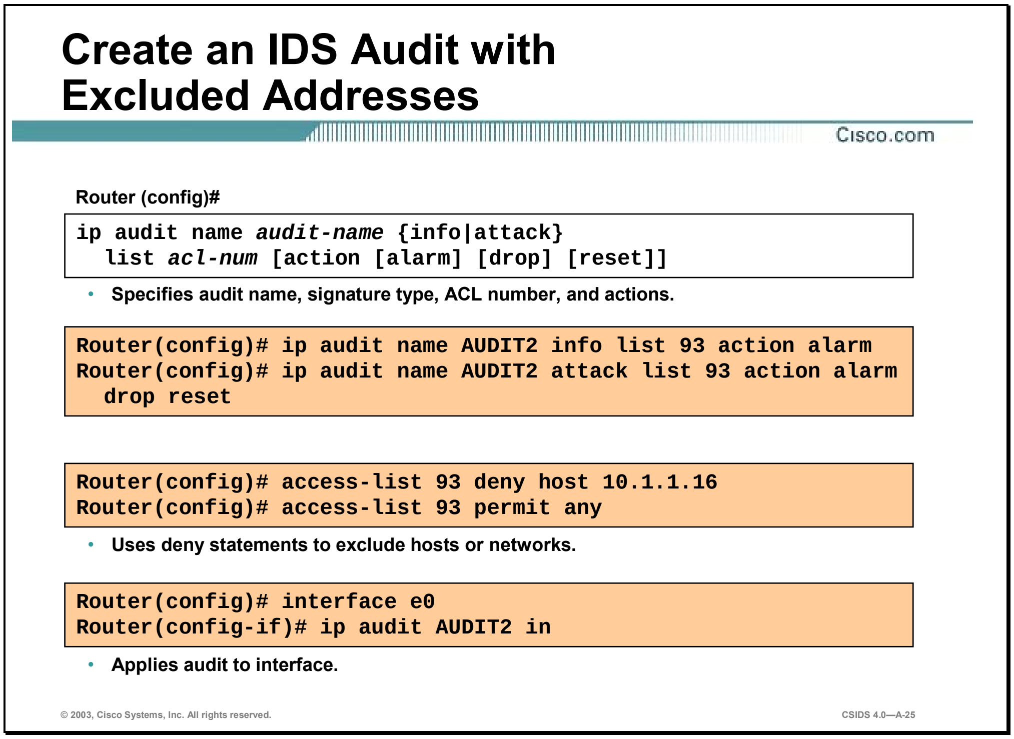
audit-name	Name for an audit specification.
info	Specifies that the audit rule is for information signatures.
attack	Specifies that the audit rule is for attack signatures.
action	Specifies an action or actions to take in response to a match. If an action is not specified, the default action is to alarm.
alarm	Sends an alarm to the console, Director, or to a Syslog server. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.

The syntax for the **ip audit** command is as follows:

ip audit *audit-name* {in | out}

no ip audit *audit-name* {in | out}

audit-name	Name for an audit specification. No audit specifications are applied to an interface or direction.
in	Apply to inbound traffic.
out	Apply to outbound traffic.



Create an IDS Audit with Excluded Addresses

Router (config)#

```
ip audit name audit-name {info|attack}
  list acl-num [action [alarm] [drop] [reset]]
```

- Specifies audit name, signature type, ACL number, and actions.

```
Router(config)# ip audit name AUDIT2 info list 93 action alarm
Router(config)# ip audit name AUDIT2 attack list 93 action alarm
  drop reset
```

```
Router(config)# access-list 93 deny host 10.1.1.16
Router(config)# access-list 93 permit any
```

- Uses deny statements to exclude hosts or networks.

```
Router(config)# interface e0
Router(config-if)# ip audit AUDIT2 in
```

- Applies audit to interface.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—A-25

The **ip audit name** and **access-list** global configuration commands can be used to create audit rules for information and attack signature types that you want to exclude from triggering when generated by a particular host or network. Use the **no** form of this command to delete an audit rule.

The syntax for the **ip audit name** command is as follows:

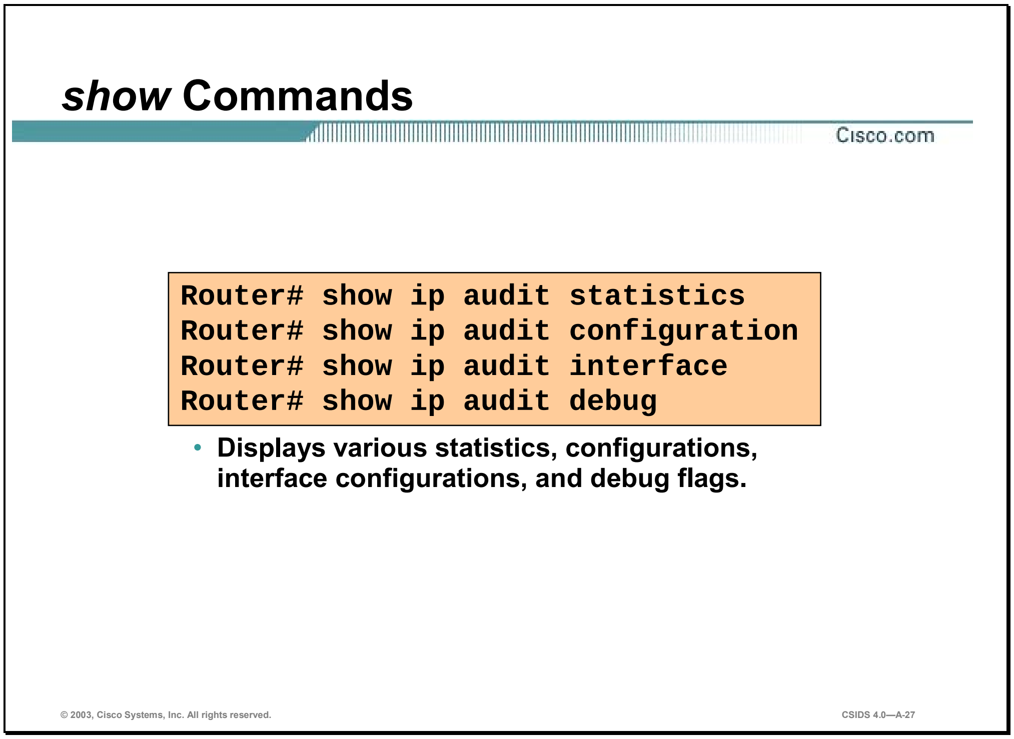
ip audit name *audit-name* {info | attack} [list *acl-num*] [action [alarm] [drop] [reset]]

no ip audit name *audit-name* {info | attack}

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for information signatures.
attack	Specifies that the audit rule is for attack signatures.
list	Specifies an ACL to attach to the audit rule.
acl-num	Unique integer specifying a configured ACL on the router. Use with the list keyword.
action	Specifies an action or actions to take in response to a match. If an action is not specified, the default action is to alarm.
alarm	Sends an alarm to the console, Director, or to a Syslog server. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.

Verifying the Configuration

This section covers the commands that allow you to verify that the configuration is correct. These include the **show**, **clear**, and **debug** commands.



show Commands

```
Router# show ip audit statistics
Router# show ip audit configuration
Router# show ip audit interface
Router# show ip audit debug
```

- **Displays various statistics, configurations, interface configurations, and debug flags.**

Use the **show ip audit statistics** command to display the number of packets audited and the number of alarms sent, among other information. The syntax for the **show ip audit statistics** command is as follows:

show ip audit statistics

Use the **show ip audit configuration** command to display additional configuration information, including default values that may not be displayed using the **show run** command. The syntax for the **show ip audit configuration** command is as follows:

show ip audit configuration

An example output of the **show ip audit configuration** command follows:

```
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:172.16.58.99:45000 T:5 S:ESTAB *

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

Use the **show ip audit interface** command to display the interface configuration. The syntax for the **show ip audit interface** command is as follows:

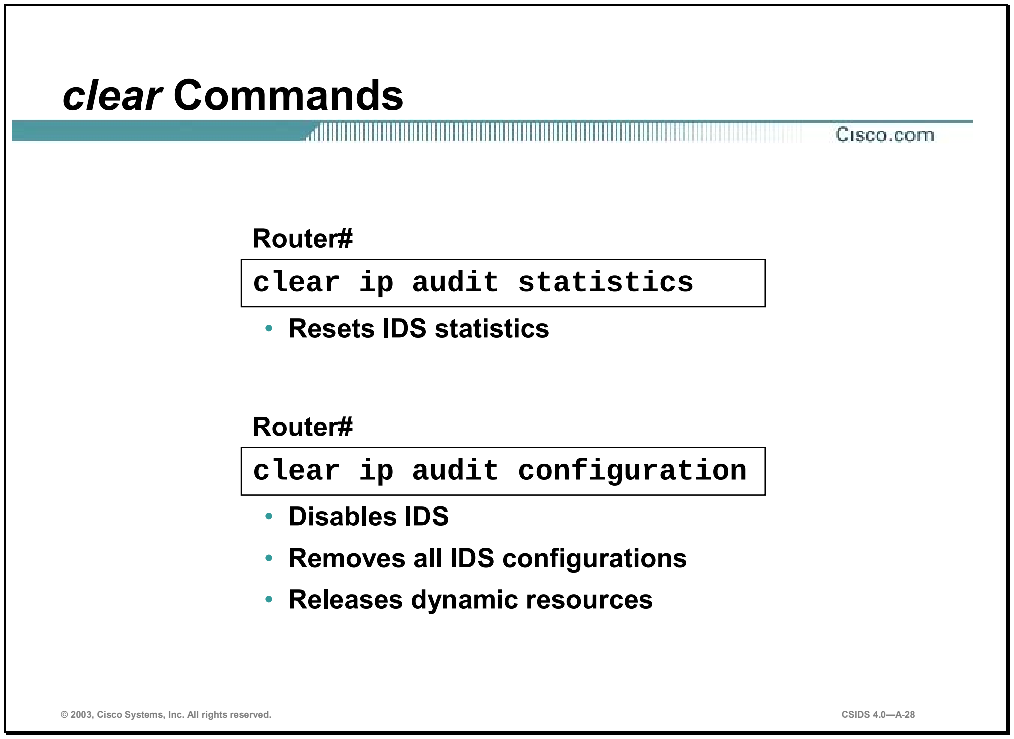
show ip audit interface

An example output of the **show ip audit interface** command follows:

```
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 AUDIT.1
    info actions alarm
    attack actions alarm drop reset
  Outgoing IDS audit rule is not set
```

Use the **show ip audit debug** command to display the enabled debug flags. The syntax for the **show ip audit debug** command is as follows:

show ip audit debug



clear Commands

Router#

```
clear ip audit statistics
```

- Resets IDS statistics

Router#

```
clear ip audit configuration
```

- Disables IDS
- Removes all IDS configurations
- Releases dynamic resources

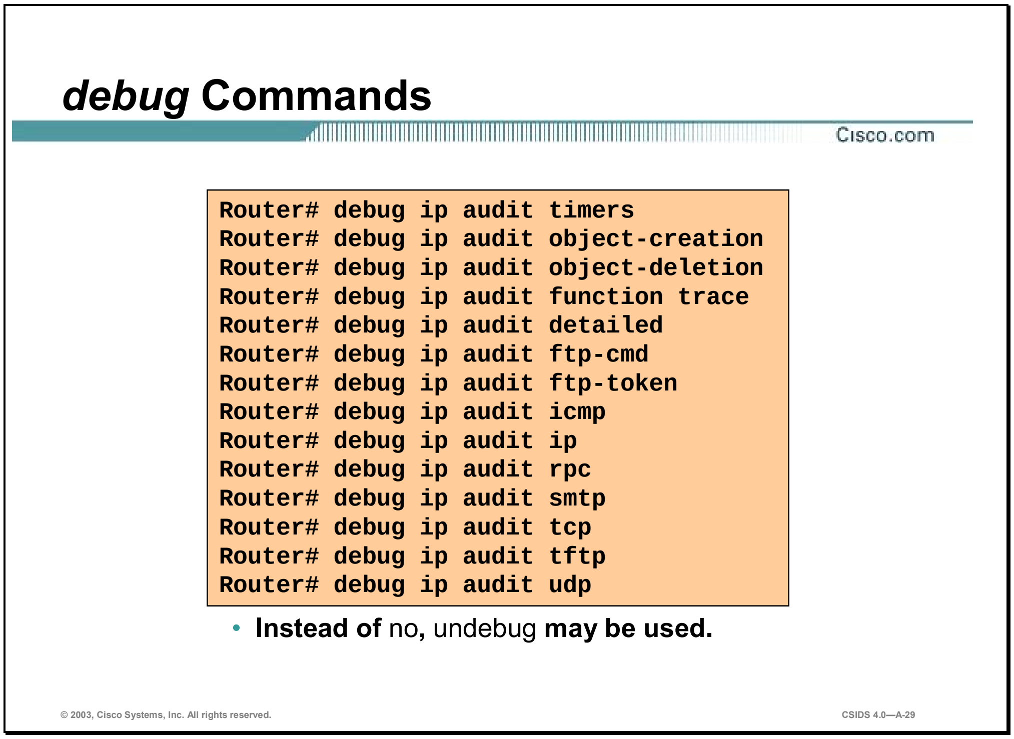
CSIDS 4.0—A-28

Use the **clear ip audit statistics** command to reset statistics on packets analyzed and alarms sent. The syntax for the **clear ip audit statistics** command is as follows:

clear ip audit statistics

Use the **clear ip audit configuration** command to disable the Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources. The syntax for the **clear ip audit configuration** command is as follows:

clear ip audit configuration



debug Commands

Cisco.com

```
Router# debug ip audit timers
Router# debug ip audit object-creation
Router# debug ip audit object-deletion
Router# debug ip audit function trace
Router# debug ip audit detailed
Router# debug ip audit ftp-cmd
Router# debug ip audit ftp-token
Router# debug ip audit icmp
Router# debug ip audit ip
Router# debug ip audit rpc
Router# debug ip audit smtp
Router# debug ip audit tcp
Router# debug ip audit tftp
Router# debug ip audit udp
```

- **Instead of** no, undebug **may be used.**

CSIDS 4.0—A-29

A plethora of debug commands are available to troubleshoot and test the Cisco IOS Firewall IDS configurations. Use the **no** form of the commands to disable debugging a given option. The following is the list of available debug commands:

debug ip audit timers

debug ip audit object-creation

debug ip audit object-deletion

debug ip audit function trace

debug ip audit detailed

debug ip audit ftp-cmd

debug ip audit ftp-token

debug ip audit icmp

debug ip audit ip

debug ip audit rpc

debug ip audit smtp

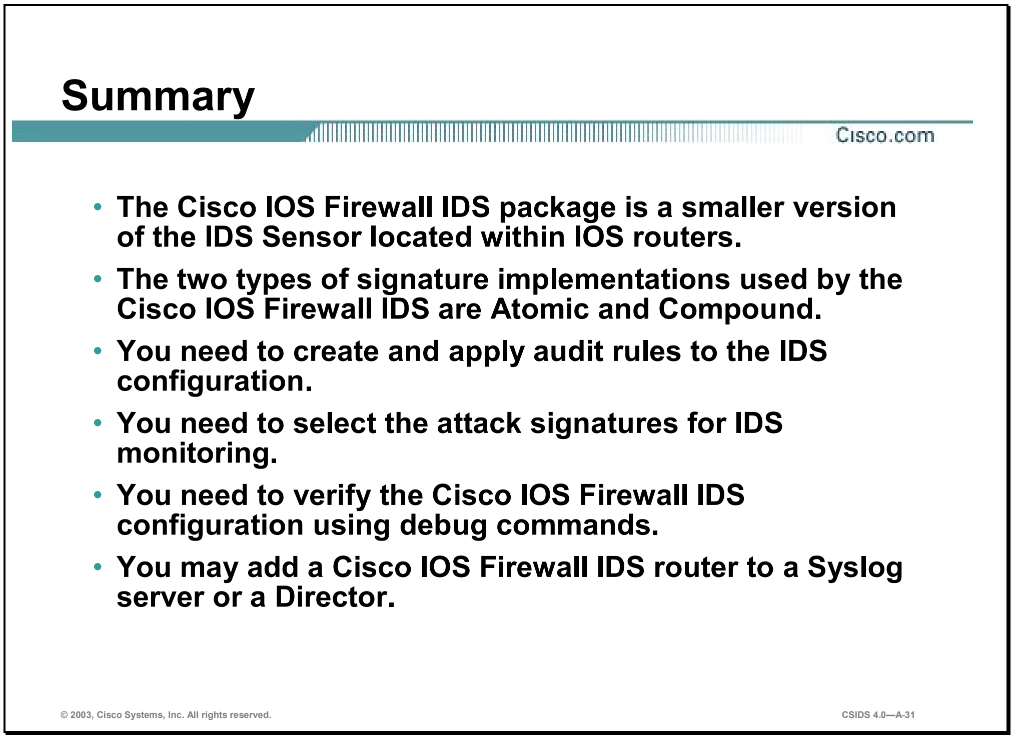
debug ip audit tcp

debug ip audit tftp

debug ip audit udp

Summary

This section summarizes what you learned in this chapter.



Summary

- The Cisco IOS Firewall IDS package is a smaller version of the IDS Sensor located within IOS routers.
- The two types of signature implementations used by the Cisco IOS Firewall IDS are Atomic and Compound.
- You need to create and apply audit rules to the IDS configuration.
- You need to select the attack signatures for IDS monitoring.
- You need to verify the Cisco IOS Firewall IDS configuration using debug commands.
- You may add a Cisco IOS Firewall IDS router to a Syslog server or a Director.

CSIDS 4.0—A-31

B

PIX Firewall Intrusion Detection and Blocking

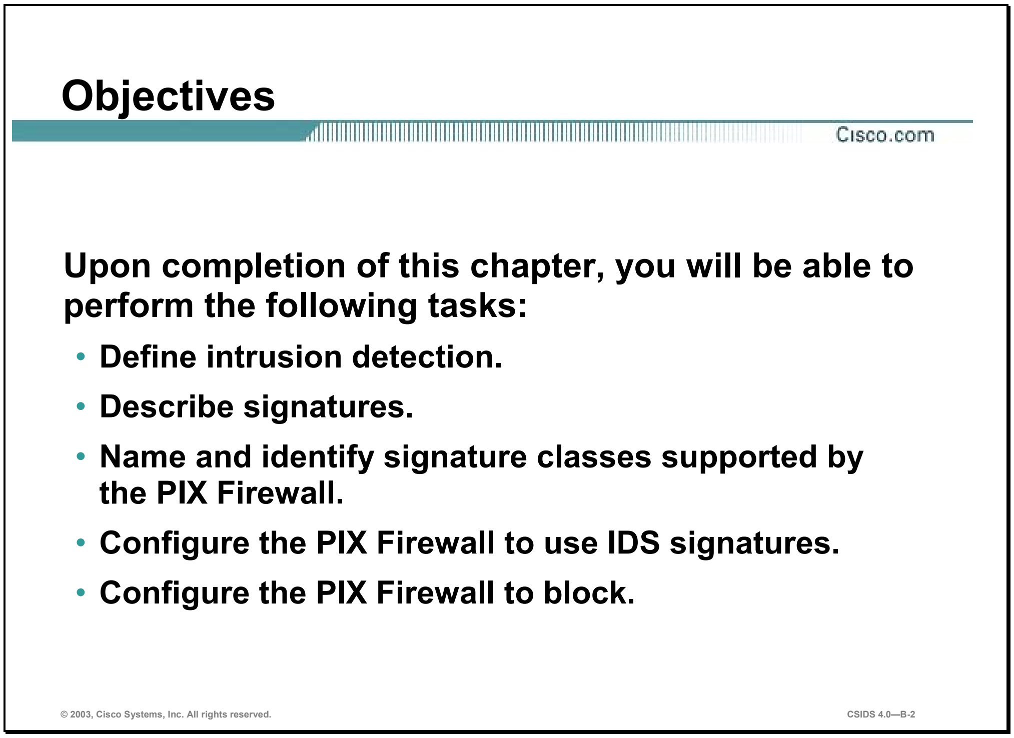
Overview

This chapter includes the following topics:

- Objectives
- Intrusion detection
- Blocking
- Summary

Objectives

This section lists the chapter's objectives.



Objectives

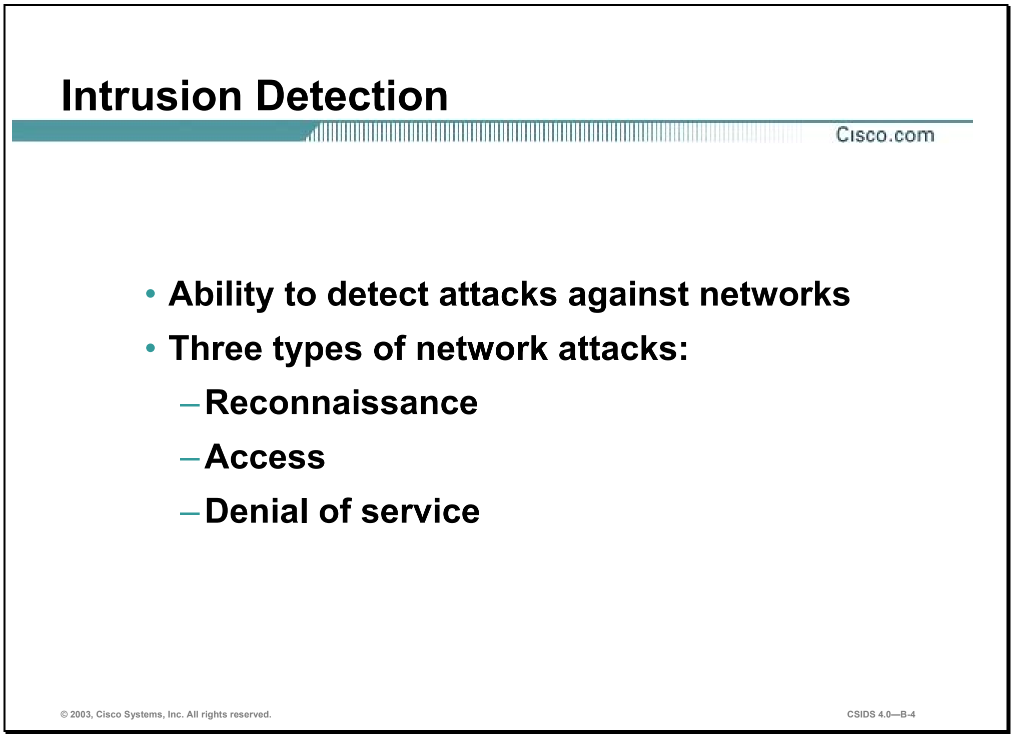
Upon completion of this chapter, you will be able to perform the following tasks:

- Define intrusion detection.
- Describe signatures.
- Name and identify signature classes supported by the PIX Firewall.
- Configure the PIX Firewall to use IDS signatures.
- Configure the PIX Firewall to block.

CSIDS 4.0—B-2

Intrusion Detection

This section explains the intrusion detection capabilities of the PIX Firewall.



Intrusion Detection

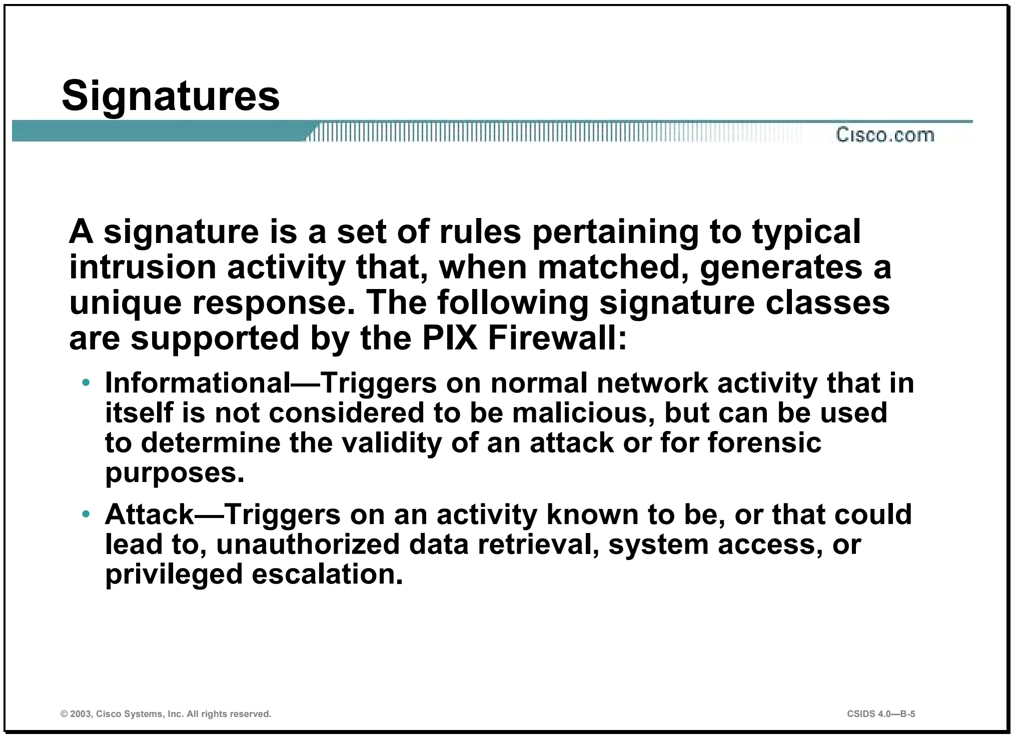
Cisco.com

- Ability to detect attacks against networks
- Three types of network attacks:
  - Reconnaissance
  - Access
  - Denial of service

CSIDS 4.0—B-4

PIX Firewall software versions 5.2 and higher have Cisco Intrusion Detection System (IDS) capabilities. Intrusion detection is the ability to detect attacks against your network. There are three types of network attacks:

- Reconnaissance attacks—An intruder is attempting to discover and map systems, services, or vulnerabilities.
- Access attacks—An intruder attacks networks or systems to retrieve data, gain access, or escalate their access privilege.
- Denial of service (DoS) attacks—An intruder attacks your network in such a way that damages or corrupts your computer system, or denies you and others access to your networks, systems, or services.



Signatures

A signature is a set of rules pertaining to typical intrusion activity that, when matched, generates a unique response. The following signature classes are supported by the PIX Firewall:

- **Informational—Triggers on normal network activity that in itself is not considered to be malicious, but can be used to determine the validity of an attack or for forensic purposes.**
- **Attack—Triggers on an activity known to be, or that could lead to, unauthorized data retrieval, system access, or privileged escalation.**

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—B-5

The PIX Firewall performs intrusion detection by using intrusion detection signatures. A signature is a set of rules pertaining to typical intrusion activity. Highly skilled network engineers research known attacks and vulnerabilities and can develop signatures to detect these attacks and vulnerabilities.

With intrusion detection enabled, the PIX Firewall can detect signatures and generate a response when this set of rules is matched to network activity. It can monitor packets for over 55 intrusion detection signatures and can be configured to send an alarm to a Syslog server, drop the packet, or reset the TCP connection. The signatures supported by the PIX Firewall are a subset of the signatures supported by the Cisco IDS product family.

The PIX Firewall can detect two different types of signatures: informational signatures and attack signatures. Information class signatures are signatures that are triggered by normal network activity that in itself is not considered to be malicious, but can be used to determined the validity of an attack or for forensics purposes. Attack class signatures are signatures that are triggered by an activity known to be, or that could lead to, unauthorized data retrieval, system access, or privileged escalation.

The following table lists examples of the IDS signatures supported by the PIX Firewall:

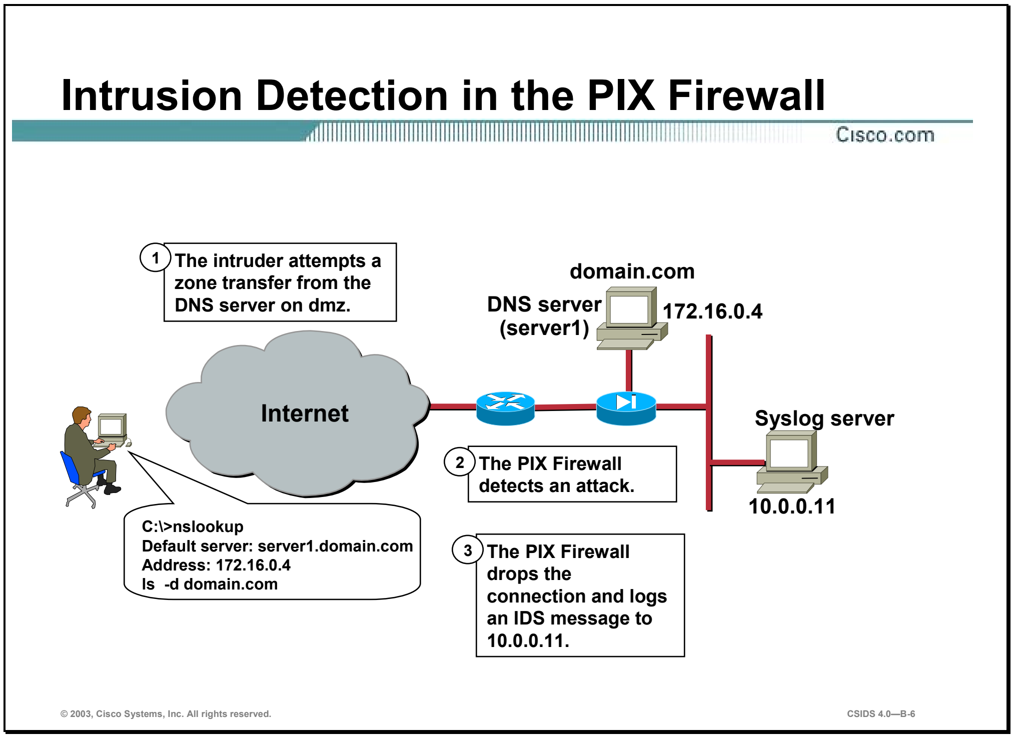
Message #	Signature ID	Signature Title	Signature Type
400000	1000	IP options-Bad Option List	Informational
400001	1001	IP options-Record Packet Route	Informational
400002	1002	IP options-Timestamp	Informational
400003	1003	IP options-Security	Informational
400007	1100	IP Fragment Attack	Attack

Message #	Signature ID	Signature Title	Signature Type
400010	2000	ICMP Echo Reply	Informational
400011	2001	ICMP Host Unreachable	Informational
400013	2003	ICMP Redirect	Informational
400014	2004	ICMP Echo Request	Informational
400023	2150	Fragmented ICMP Traffic	Attack
400024	2151	Large ICMP Traffic	Attack
400025	2154	Ping of Death Attack	Attack
400032	4051	UDP Snork Attack	Attack
400035	6051	DNS Zone Transfer	Attack
400041	6103	Proxied RPC Request	Attack

IDS Syslog messages all start with %PIX-4-4000nn and have the following format: %PIX-4-4000nn IDS:sig_num sig_msg from ip_addr to ip_addr on interface int_name. For example, %PIX-4-400013 IDS:2003 ICMP redirect from 10.4.1.2 to 10.2.1.1 on interface dmz, and %PIX-4-400032 IDS:4051 UDP Snork attack from 10.1.1.1 to 192.168.1.1 on interface outside.

Refer to System Log Messages for the Cisco Secure PIX Firewall Version 5.2 or System Log Messages for the Cisco Secure PIX Firewall Version 5.3 for a list of all supported messages. You can view these documents online at the following sites:

- www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/syslog/index.htm
- www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/index.htm



Intrusion Detection in the PIX Firewall

1 The intruder attempts a zone transfer from the DNS server on dmz.

2 The PIX Firewall detects an attack.

3 The PIX Firewall drops the connection and logs an IDS message to 10.0.0.11.

```
C:\>nslookup
Default server: server1.domain.com
Address: 172.16.0.4
ls  -d domain.com
```

CSIDS 4.0—B-6

Intrusion detection, or auditing, is enabled on the PIX Firewall with the **ip audit** commands. Using the **ip audit** commands, audit policies can be created to specify the traffic that is audited or to designate actions to be taken when a signature is detected. After a policy is created, it can be applied to any PIX Firewall interface.

Each interface can have two policies: one for informational signatures and one for attack signatures. When a policy for a given signature class is created and applied to an interface, all supported signatures of that class are monitored unless you disable them with the **ip audit signature disable** command.

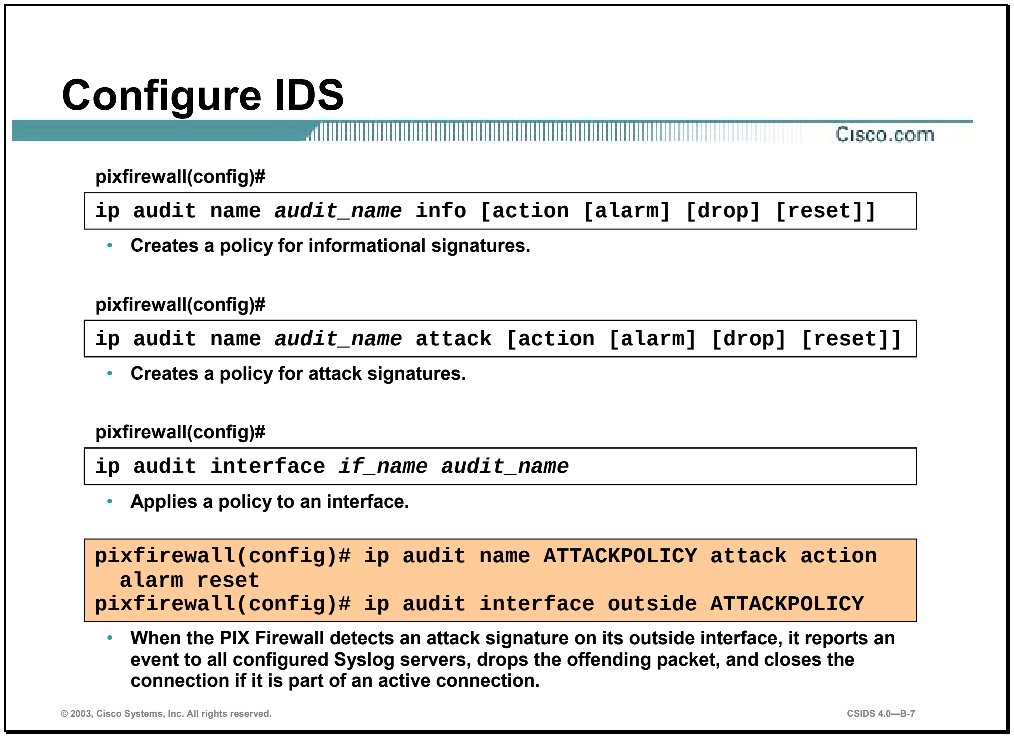
The PIX Firewall supports both inbound and outbound auditing. Auditing is performed by looking at the IP packets as they arrive at an input interface. For example, if an attack policy is applied to the outside interface, attack signatures are triggered when attack traffic arrives at the outside interface in an inward direction, either as inbound traffic or as return traffic from an outbound connection.

In the figure, the PIX Firewall has an attack policy, which contains the alarm and drop actions, applied to its outside interface. Therefore, the following series of events takes place:

Step 1 The intruder attempts to transfer a DNS zone from the DNS server on the DMZ.

Step 2 The PIX Firewall detects an attack.

Step 3 The PIX Firewall drops the connection and sends an IDS Syslog message to the Syslog server at 10.0.0.3.



Configure IDS

pixfirewall(config)#

```
ip audit name audit_name info [action [alarm] [drop] [reset]]
```

- Creates a policy for informational signatures.

pixfirewall(config)#

```
ip audit name audit_name attack [action [alarm] [drop] [reset]]
```

- Creates a policy for attack signatures.

pixfirewall(config)#

```
ip audit interface if_name audit_name
```

- Applies a policy to an interface.

```
pixfirewall(config)# ip audit name ATTACKPOLICY attack action
  alarm reset
pixfirewall(config)# ip audit interface outside ATTACKPOLICY
```

- When the PIX Firewall detects an attack signature on its outside interface, it reports an event to all configured Syslog servers, drops the offending packet, and closes the connection if it is part of an active connection.

Use the **ip audit** command to configure IDS signature use. First create a policy with the **ip audit name** command, and then apply the policy to an interface with the **ip audit interface** command.

There are two variations of the **ip audit name** command: **ip audit name info** and **ip audit name attack**. The **ip audit name info** command is used to create policies for signatures classified as informational. All informational signatures, except those disabled or excluded by the **ip audit signature** command, become part of the policy. The **ip audit name attack** command performs the same function for signatures classified as attack signatures.

The **ip audit name** commands also allow you to specify actions to be taken when a signature is triggered. If a policy is defined without actions, the default actions take effect. The default action for both attack and info signatures is alarm.

The **no ip audit name** command can be used to remove an audit policy. The **show ip audit name** command displays audit policies. To remove a policy from an interface, use the **no ip audit interface** command. To display the interface configuration, use the **show ip audit interface** command.

The syntax for these **ip audit** commands is as follows:

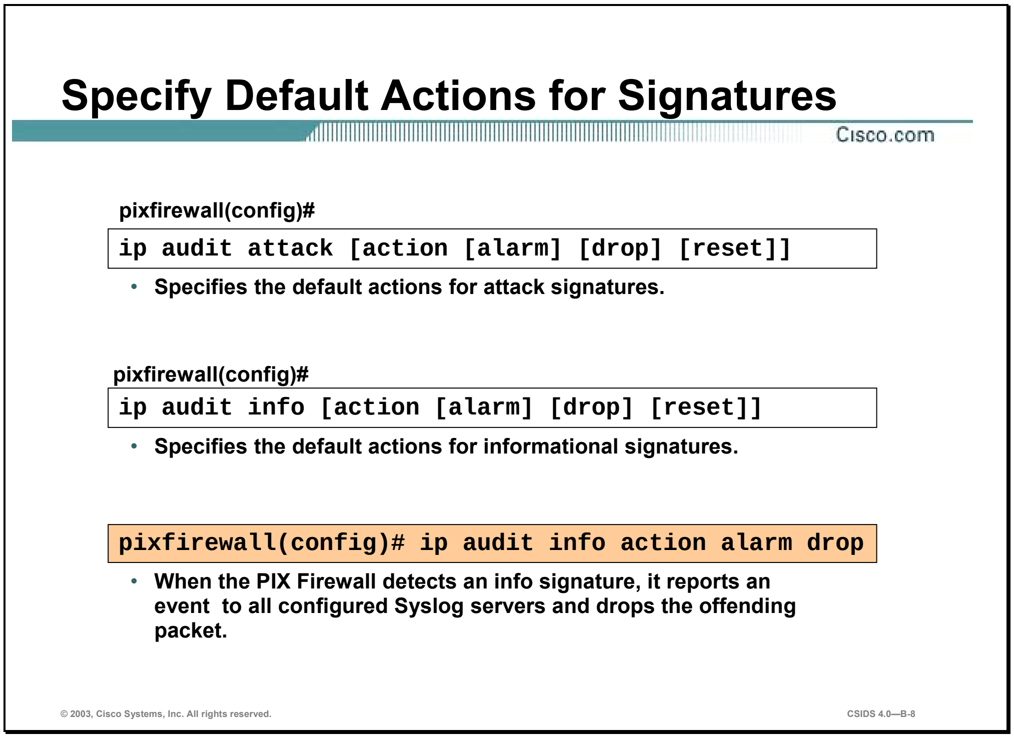
ip audit name *audit_name* info [*action* [*alarm*] [*drop*] [*reset*]]

ip audit name *audit_name* attack [*action* [*alarm*] [*drop*] [*reset*]]

ip audit interface *if_name audit_name*

audit name	Specifies signatures, except those disabled or excluded by the **ip audit signature** command, as part of the policy.
audit_name	Audits the policy name viewed with the **show ip audit name** command.

action *actions*	The alarm option indicates that when a signature match is detected in a packet, the PIX Firewall reports the event to all configured Syslog servers. The drop option drops the offending packet. The reset option drops the offending packet and closes the connection if it is part of an active connection. The default is alarm.
audit interface	Applies an audit specification or policy (via the **ip audit name** command) to an interface.
if_name	The interface to which the policy is applied.



Specify Default Actions for Signatures

Cisco.com

pixfirewall(config)#

```
ip audit attack [action [alarm] [drop] [reset]]
```

- Specifies the default actions for attack signatures.

pixfirewall(config)#

```
ip audit info [action [alarm] [drop] [reset]]
```

- Specifies the default actions for informational signatures.

```
pixfirewall(config)# ip audit info action alarm drop
```

- When the PIX Firewall detects an info signature, it reports an event to all configured Syslog servers and drops the offending packet.

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—B-8

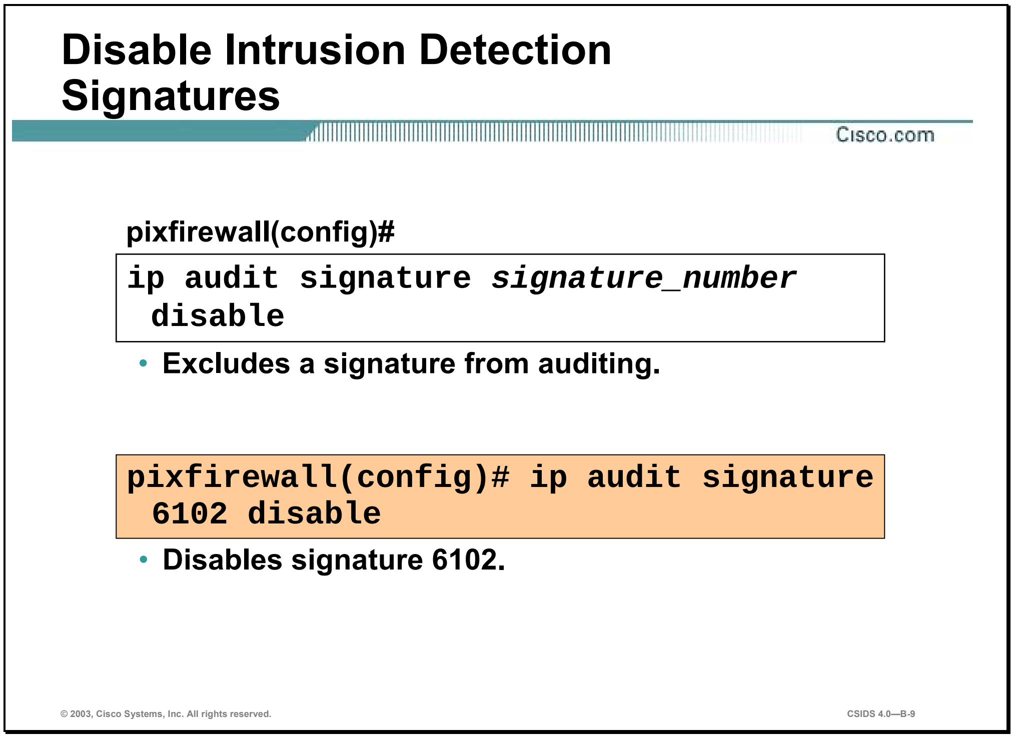
The **ip audit attack** command specifies the default actions to be taken for attack signatures. The **no ip audit attack** command resets the action to be taken for attack signatures to the default action. The **show ip audit attack** command displays the default attack actions. The **ip audit info**, **no ip audit info**, and **show ip audit info** commands perform the same functions for signatures classified as informational. To cancel event reactions, specify the **ip audit info** command without an action option.

The syntax for these **ip audit** commands is as follows:

ip audit attack [*action* [*alarm*] [*drop*] [*reset*]]

ip audit info [*action* [*alarm*] [*drop*] [*reset*]*/*

audit attack	Specifies the default actions to be taken for attack signatures.
audit info	Specifies the default actions to be taken for informational signatures.
action *actions*	The alarm option indicates that when a signature match is detected in a packet, the PIX Firewall reports the event to all configured Syslog servers. The drop option drops the offending packet. The reset option drops the offending packet and closes the connection if it is part of an active connection. The default is alarm.



Disable Intrusion Detection Signatures

Cisco.com

pixfirewall(config)#

```
ip audit signature signature_number
 disable
```

- Excludes a signature from auditing.

```
pixfirewall(config)# ip audit signature
 6102 disable
```

- Disables signature 6102.

CSIDS 4.0—B-9

If you wish to exclude a signature from auditing, use the **ip audit signature disable** command. The **no ip audit signature** command is used to re-enable a signature, and the **show ip audit signature** command displays disabled signatures.

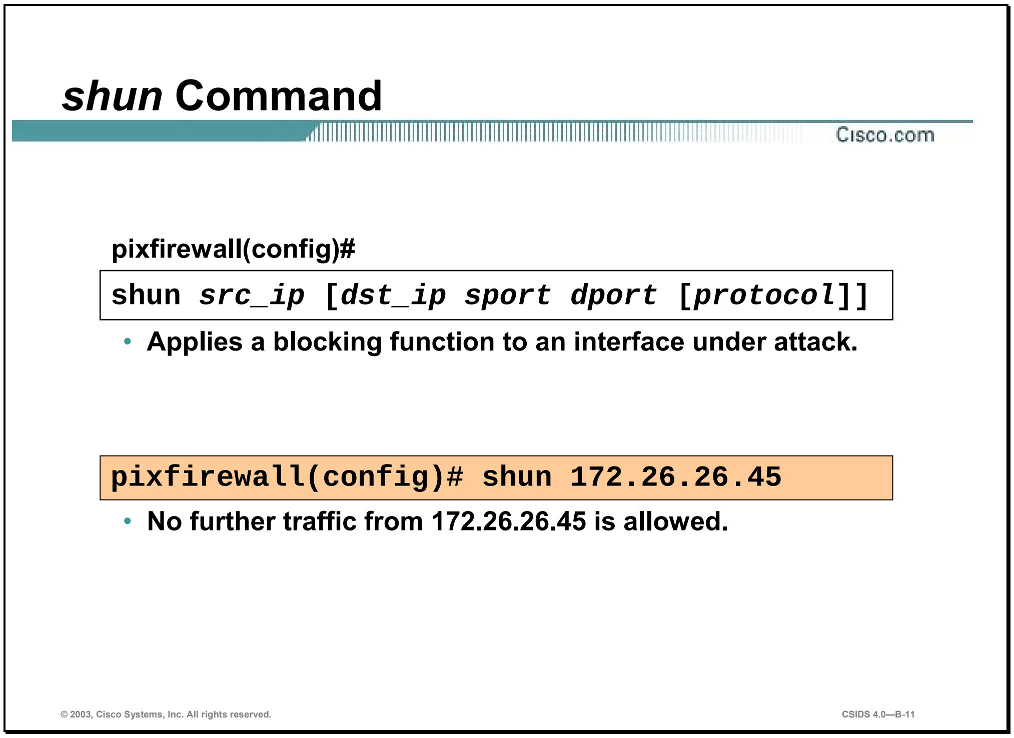
The syntax for the **ip audit signature** command is as follows:

ip audit signature *signature_number* disable

audit signature	Specifies what messages to display, attaches a global policy to a signature, and disables or excludes a signature from auditing.
signature_number	Intrusion detection signature number.

Blocking

This section explains the PIX Firewall's blocking capabilities.



shun Command

pixfirewall(config)#

```
shun src_ip [dst_ip sport dport [protocol]]
```

- **Applies a blocking function to an interface under attack.**

```
pixfirewall(config)# shun 172.26.26.45
```

- **No further traffic from 172.26.26.45 is allowed.**

CSIDS 4.0—B-11

The PIX Firewall's block feature allows a PIX Firewall, when combined with a Cisco IDS Sensor, to dynamically respond to an attacking host by preventing new connections and disallowing packets from any existing connection. A Cisco IDS device instructs the PIX Firewall to block sources of traffic when those sources of traffic are determined to be malicious.

The **shun** command, intended for use primarily by a Cisco IDS device, applies a blocking function to an interface receiving an attack. Packets containing the IP source address of the attacking host are dropped and logged until the blocking function is removed manually or by the Cisco IDS master unit. No traffic from the IP source address is allowed to traverse the PIX Firewall, and any remaining connections time out as part of the normal architecture. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

The offending host can be inside or outside of the PIX Firewall. If the **shun** command is used only with the source IP address of the host, no further traffic from the offending host is allowed.

The **show shun** command displays all blocks currently enabled in the exact format specified. The **no** form of the **shun** command disables a block based on src_ip.

Note PIX Firewall blocking is supported in Cisco IDS 3.0.

The **show shun** command displays all blocks currently enabled in the exact format specified. The **no** form of the **shun** command disables a block based on src_ip.

The syntax for the **shun** command is as follows:

shun ***src_ip* [*dst_ip sport dport* [*protocol*]]**

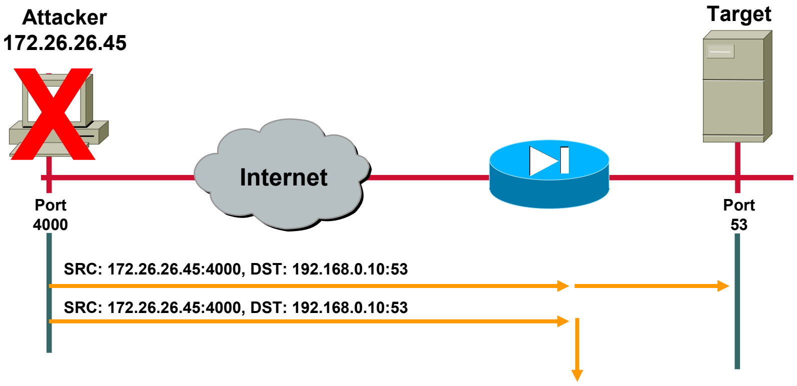
show shun ***src_ip***

clear shun [statistics]

clear	Disables all blocks currently enabled and clears block statistics. Specifying statistics only clears the counters for that interface.
dport	The destination port of the connection causing the block.
dst_ip	The address of the of the target host.
protocol	The optional IP protocol, such as UDP or TCP.
sport	The source port of the connection causing the block.
src_ip	The address of the attacking host.
statistics	Clears only interface counters.

Blocking an Attacker

Cisco.com



Attacker
172.26.26.45

Target

Internet

Port
4000

Port
53

SRC: 172.26.26.45:4000, DST: 192.168.0.10:53

SRC: 172.26.26.45:4000, DST: 192.168.0.10:53

```
pixfirewall(config)# shun 172.26.26.45
  192.168.0.10 4000 53
```

CSIDS 4.0—B-12

In the figure, host 172.26.26.45 has been attempting a DNS zone transfer from host 192.168.0.10 using a source port other than the well-known DNS port of TCP 53. The offending host (172.26.26.45) has made a connection with the victim (192.168.0.10) with TCP. The connection in the PIX Firewall connection table reads as follows:

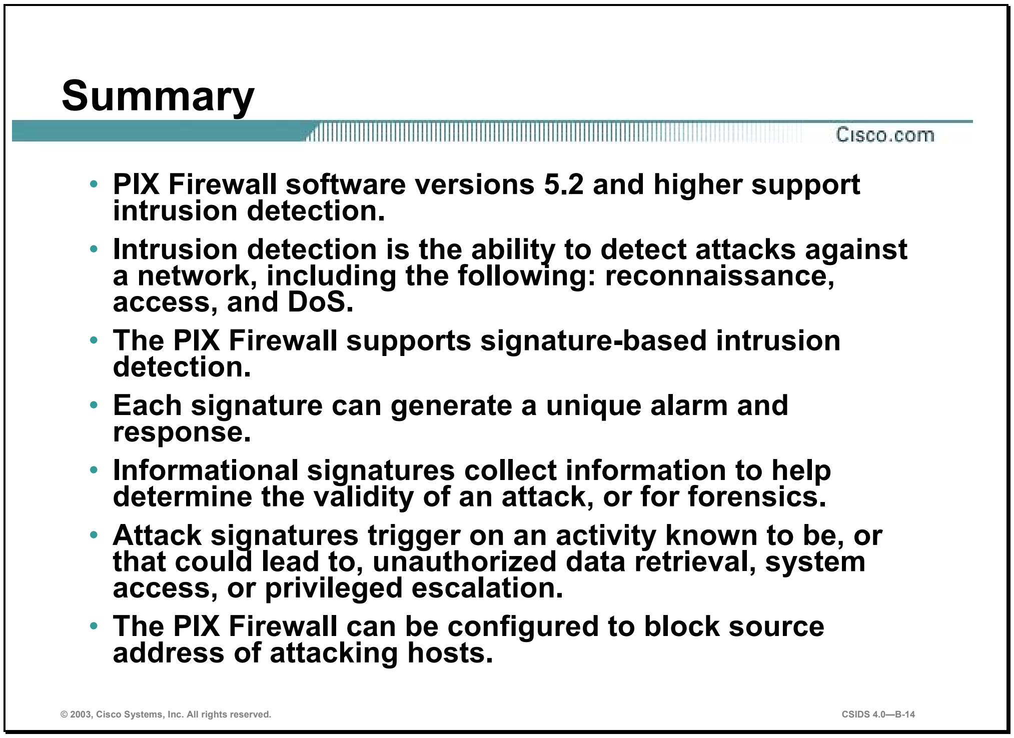
172.26.26.45, 4000-> 10.0.0.11 PROT TCP

If the **shun** command is applied as shown in the figure, the PIX Firewall deletes the connection from its connection table and prevents packets from 172.26.26.45 from reaching the inside host.

Note	The PIX Firewall configuration contains a static mapping of host 10.0.0.11 to global address 192.168.0.10.

Summary

This section summarizes what you learned in this chapter.



Summary

Cisco.com

- PIX Firewall software versions 5.2 and higher support intrusion detection.
- Intrusion detection is the ability to detect attacks against a network, including the following: reconnaissance, access, and DoS.
- The PIX Firewall supports signature-based intrusion detection.
- Each signature can generate a unique alarm and response.
- Informational signatures collect information to help determine the validity of an attack, or for forensics.
- Attack signatures trigger on an activity known to be, or that could lead to, unauthorized data retrieval, system access, or privileged escalation.
- The PIX Firewall can be configured to block source address of attacking hosts.

CSIDS 4.0—B-14

C

Cisco Intrusion Detection System 3.X Architecture

Overview

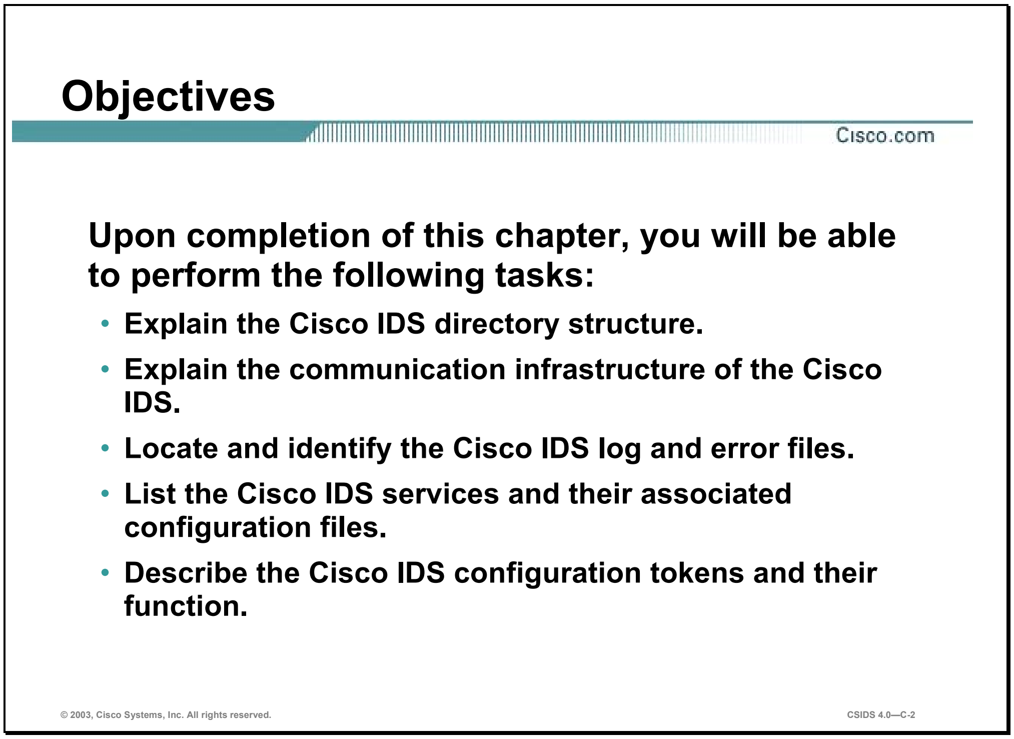
This appendix describes the Cisco Intrusion Detection System (Cisco IDS) architecture.

This appendix includes the following topics:

- Objectives
- Cisco IDS software architecture
- Cisco IDS communication
- Cisco IDS directory structure
- Cisco IDS service files
- Summary

Objectives

This section lists the chapter’s objectives.



Objectives

Cisco.com

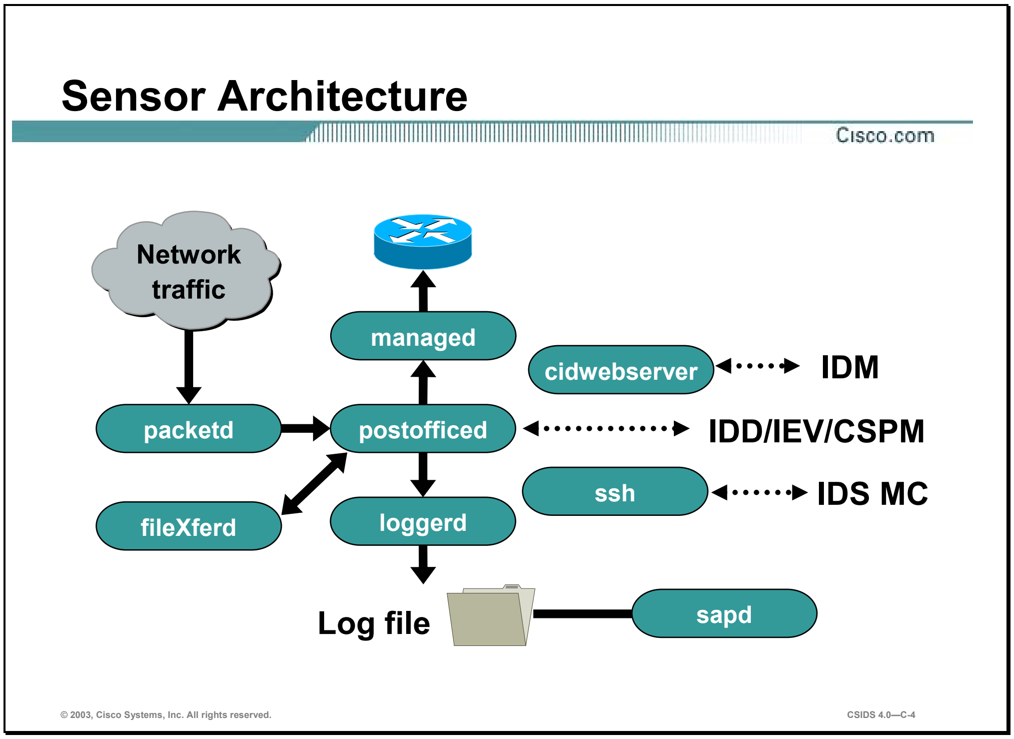
Upon completion of this chapter, you will be able to perform the following tasks:

- **Explain the Cisco IDS directory structure.**
- **Explain the communication infrastructure of the Cisco IDS.**
- **Locate and identify the Cisco IDS log and error files.**
- **List the Cisco IDS services and their associated configuration files.**
- **Describe the Cisco IDS configuration tokens and their function.**

CSIDS 4.0—C-2

Cisco IDS Software Architecture

This section discusses the Cisco Intrusion Detection System (Cisco IDS) Sensor and IDS Event Viewer (IEV) architecture.



Sensor Architecture

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-4

The Sensor, Cisco IDS Director, and PostOffice each have separate operational software components often referred to as daemons or services. Since each major Cisco IDS function is accomplished by a separate service, the result is a security system that is fast, durable, and scalable.

The following are the Sensor's services:

- postofficed—Handles communications between the Cisco IDS services and the Cisco IDS devices. PostOfficed routes the messages based on signature settings.
- packetd—Cisco IDS service that enables the Sensor to capture packets directly from the network and conduct intrusion detection analysis. Intrusion alarms are forwarded to postofficed for distribution.
- loggerd—As the Cisco IDS logging service, loggerd writes error, command, and alarm entries to log files on the Sensor. Loggerd handles the creation of IP log files.
- sapd—This is the security analysis package daemon. This service provides data and file management. It is responsible for moving the log files to the database staging areas, off-line archives, and other routine processes to prevent file systems from filling up and overwriting saved logs.

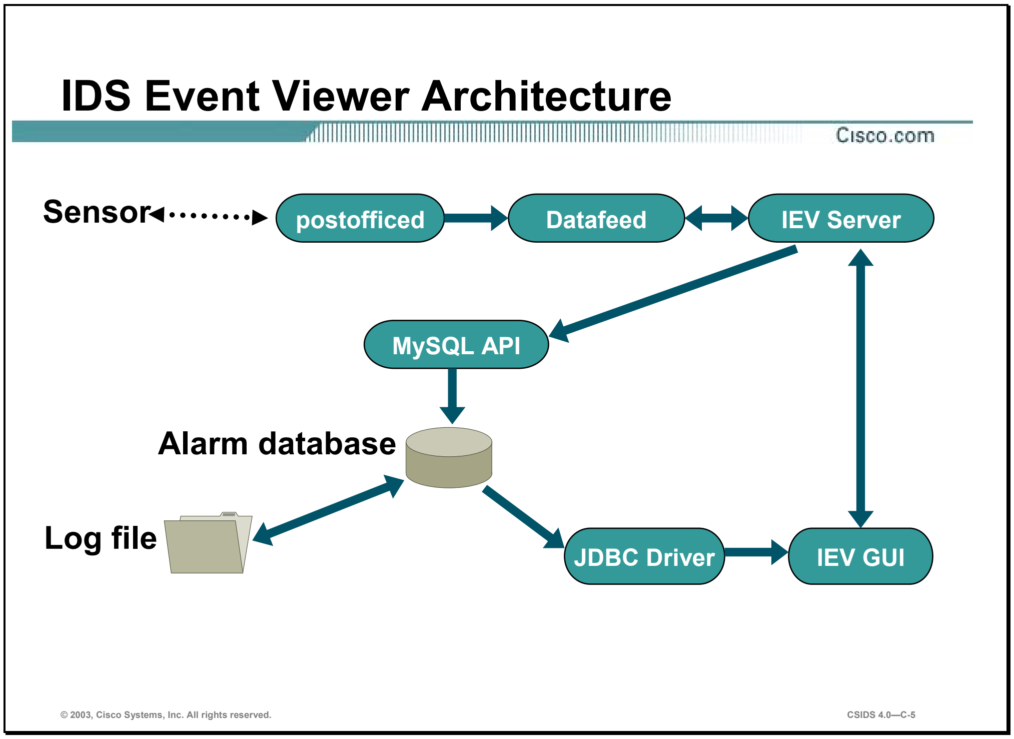
- managed—Communicates with managed Cisco devices. When packetd identifies that a certain type of attack should be blocked, it sends a block command to managed via postofficed. Managed then communicates with the blocking device and either uses the shun command or writes an Access Control List (ACL) to prohibit access into the protected network.

- fileXferd—Transfers configuration files from the Director to the Sensors using PostOffice to communicate.

- cidwebserver—Embedded web server that enables the configuration of the Sensor via a supported web browser. The configuration files are transferred via an HTTPS session.

Note Standard HTTP is supported for those network environments where HTTPS cannot be deployed.

- ssh—Secure shell (SSH) server that is used by the IDS Management Center (IDS MC) to deploy IDS configuration files.



IDS Event Viewer Architecture

Cisco.com

Sensor

postofficed

Datafeed

IEV Server

MySQL API

Alarm database

Log file

JDBC Driver

IEV GUI

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-5

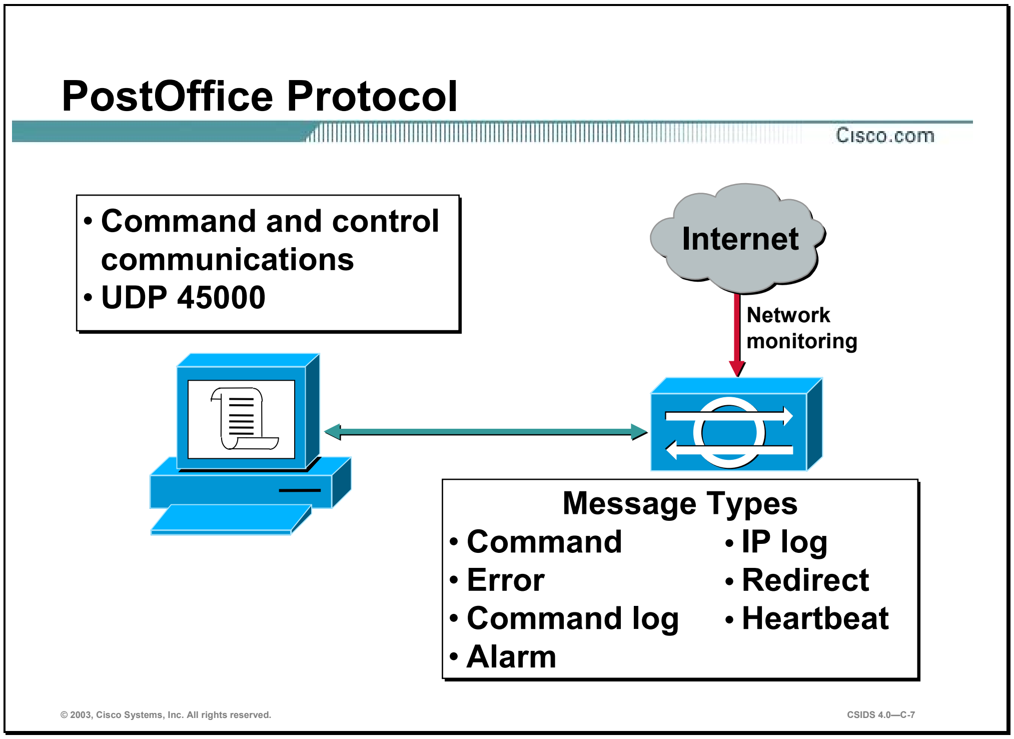
The Sensor forwards messages to the IEV host. The messages are routed to the defined services by postofficed.

The following are the IEV's services:

- postofficed—Handles communications between the Cisco IDS services and the Cisco IDS devices.
- Datafeed—Populates the alarm database when events are received from the Sensor.
- IEVServer—Stores the alarms in a MySQL database, archives the database files, and checks available disk space.
- IEV GUI—Graphical user interface used to configure IEV and display the Cisco IDS alarms from the database.
- JDBC Driver—The Java Database Connectivity driver is the Java API for communicating with databases. JDBC specifies the interface necessary to connect to a database, execute SQL commands, and interpret the results.
- MySQL—Persistently stores the alarm data and serving data when queried. The data from the database can be exported to an ASCII text file.

Cisco IDS Communication

This section discusses the Cisco Intrusion Detection System (Cisco IDS) communication protocol.



PostOffice Protocol

Cisco.com

- Command and control communications
- UDP 45000

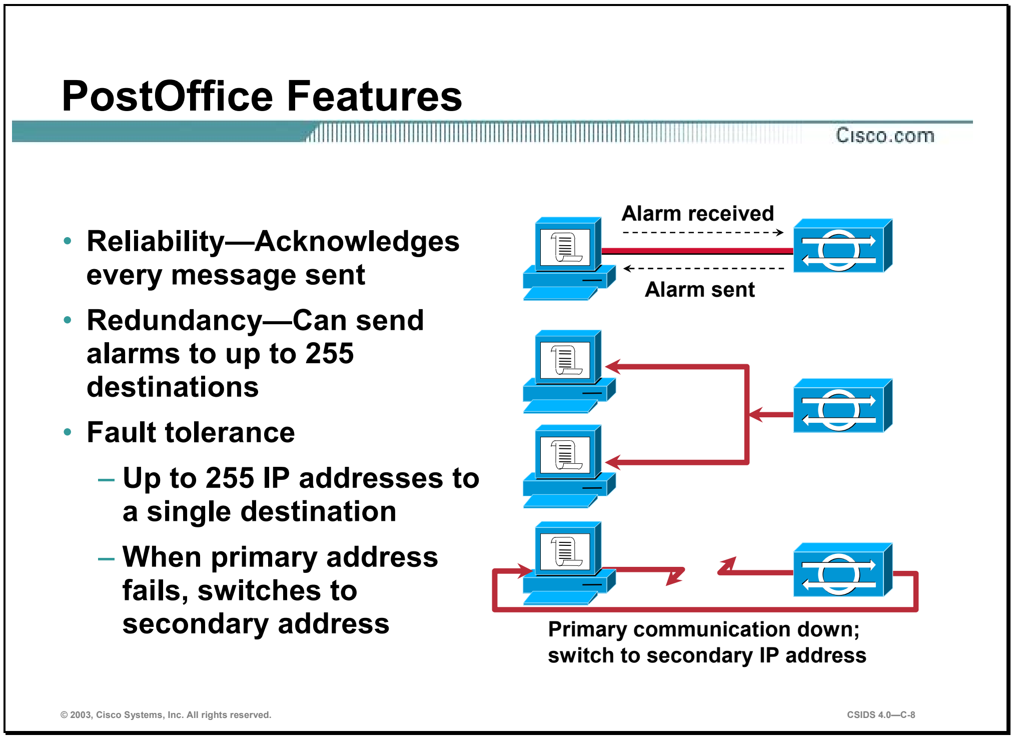
Message Types

- Command
- Error
- Command log
- Alarm
- IP log
- Redirect
- Heartbeat

CSIDS 4.0—C-7

The Cisco IDS services and hosts communicate with one another using the PostOffice protocol. PostOffice uses the User Datagram Protocol (UDP) transport on port 45000. The Sensor communicates with other Cisco IDS devices via its command and control interface. The following are the types of messages that are sent using the PostOffice protocol:

- Command messages
- Error messages
- Command log messages
- Alarm messages
- IP log messages
- Redirect messages
- Heartbeat messages



PostOffice Features

Cisco.com

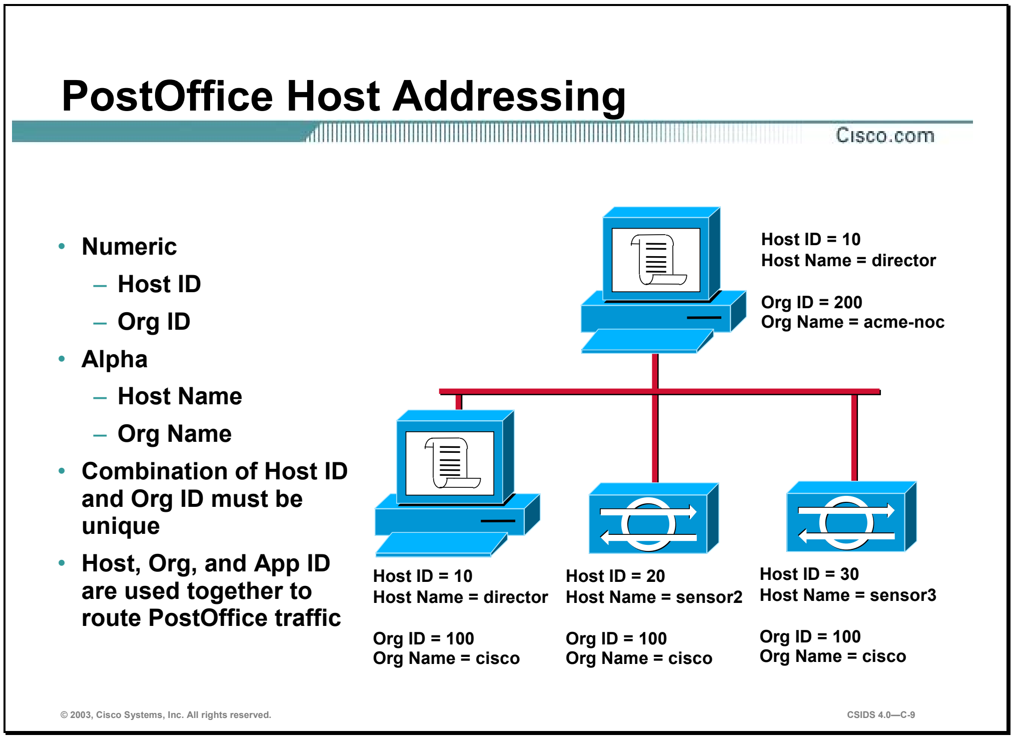
- Reliability—Acknowledges every message sent
- Redundancy—Can send alarms to up to 255 destinations
- Fault tolerance
  - Up to 255 IP addresses to a single destination
  - When primary address fails, switches to secondary address

CSIDS 4.0—C-8

PostOffice is designed to guarantee the transmission of messages to the intended recipient. PostOffice expects acknowledgement for every message sent from the receiver. If no acknowledgement is received within a predetermined length of time, the message is resent until the acknowledgement is received.

The PostOffice protocol enables Sensors to propagate messages to up to 255 destinations. This feature allows for redundant alarm notifications, which ensures the appropriate personnel are notified when an alarm is received.

Using the PostOffice protocol, up to 255 alternate IP addresses may be assigned to a single host. The alternate routing protocol automatically switches to the next IP address whenever the current connection fails. PostOffice uses a system “watchdog” to detect when a connection to the preferred IP address is reestablished, at which time PostOffice reverts back to the primary address.



PostOffice Host Addressing

- Numeric
  - Host ID
  - Org ID
- Alpha
  - Host Name
  - Org Name
- Combination of Host ID and Org ID must be unique
- Host, Org, and App ID are used together to route PostOffice traffic

Host ID = 10
Host Name = director

Org ID = 200
Org Name = acme-noc

Host ID = 10
Host Name = director

Org ID = 100
Org Name = cisco

Host ID = 20
Host Name = sensor2

Org ID = 100
Org Name = cisco

Host ID = 30
Host Name = sensor3

Org ID = 100
Org Name = cisco

Assign each Cisco IDS device a unique numeric identifier. This unique numeric identifier is a combination of a host and an organization identification. With every host identification and organization identification combination, there is an associated alphanumeric identifier consisting of a host name and an organization name. The following are descriptions of the individual identifiers:

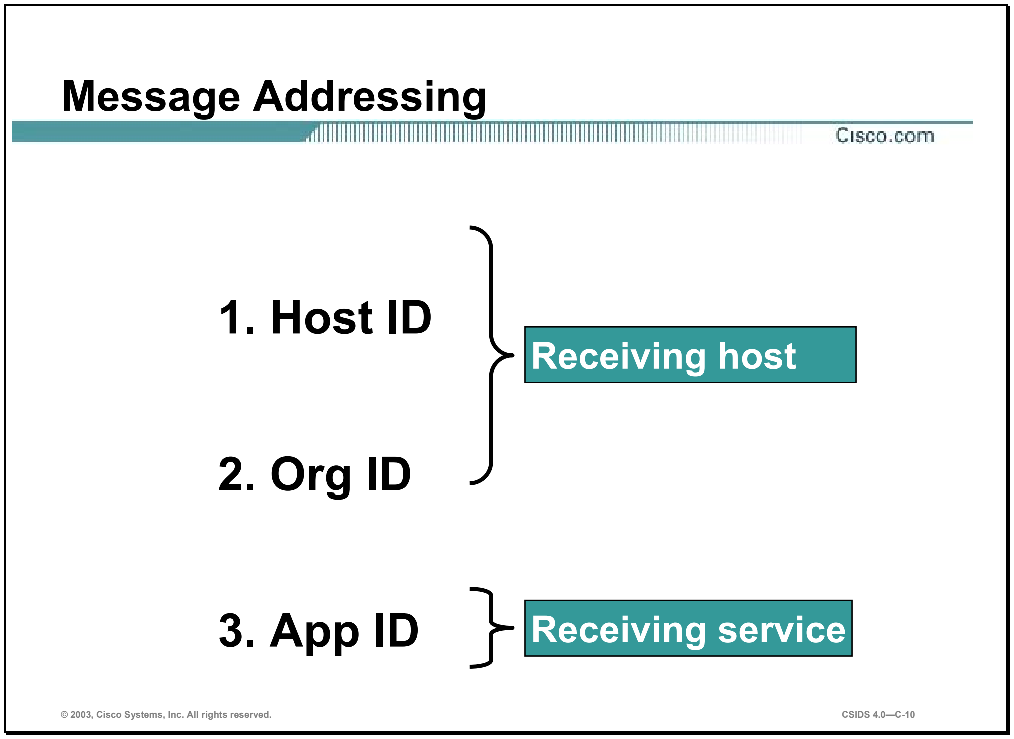
- Host identification number (Host ID)—Numeric identification for the Cisco IDS host (1–65535).

- Host name—An alphanumeric identifier for the Cisco IDS device. The name chosen here is typically one that describes the name and location where the device is installed (sensor1_Austin).

- Organization identification number (Org ID)—Numeric identification for the Cisco IDS organization (1–65535). It can be used to group a number of the Cisco IDS devices together under the same number for easy identification purposes.

- Organization name (Org name)—An alphanumeric identifier for a group of Cisco IDS devices. The name chosen here is typically one that describes the name of the company where the device is installed or the name of the department within the company where the device is installed (austin_eng).

The host and organization identifications make up two-thirds of the three-part PostOffice proprietary addressing scheme. The third part of the addressing scheme is a unique application identifier. PostOffice uses these unique identifiers to route all command and control communications.



Message Addressing

Cisco.com

1. Host ID
2. Org ID

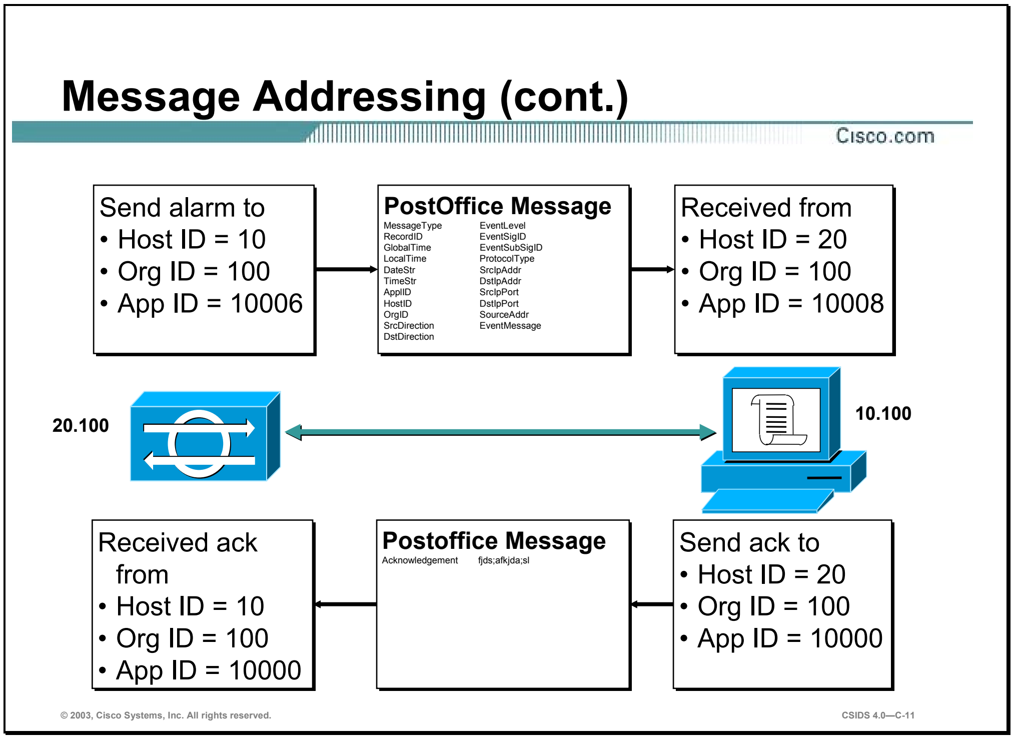
Receiving host

3. App ID

Receiving service

CSIDS 4.0—C-10

The Cisco IDS uses the PostOffice protocol to transmit messages between the Cisco IDS services. The PostOffice protocol uses a message-addressing scheme that includes a combination of the host identification, organization identification, and the application identification. The host identification is a numeric identifier of the Cisco IDS host as defined in the hosts file. The organization identification is a numeric identifier of the Cisco IDS organization to which the Cisco IDS host belongs as defined in the host file. The application identification is the numeric identifier of the Cisco IDS service as defined in the services file.



Message Addressing (cont.)

Send alarm to
- Host ID = 10
- Org ID = 100
- App ID = 10006

PostOffice Message

MessageType
RecordID
GlobalTime
LocalTime
DateStr
TimeStr
ApplID
HostID
OrgID
SrcDirection
DstDirection

EventLevel
EventSigID
EventSubSigID
ProtocolType
SrcIpAddr
DstIpAddr
SrcIpPort
DstIpPort
SourceAddr
EventMessage

Received from
- Host ID = 20
- Org ID = 100
- App ID = 10008

Received ack from
- Host ID = 10
- Org ID = 100
- App ID = 10000

Postoffice Message

Acknowledgement fjds;afkjda;sl

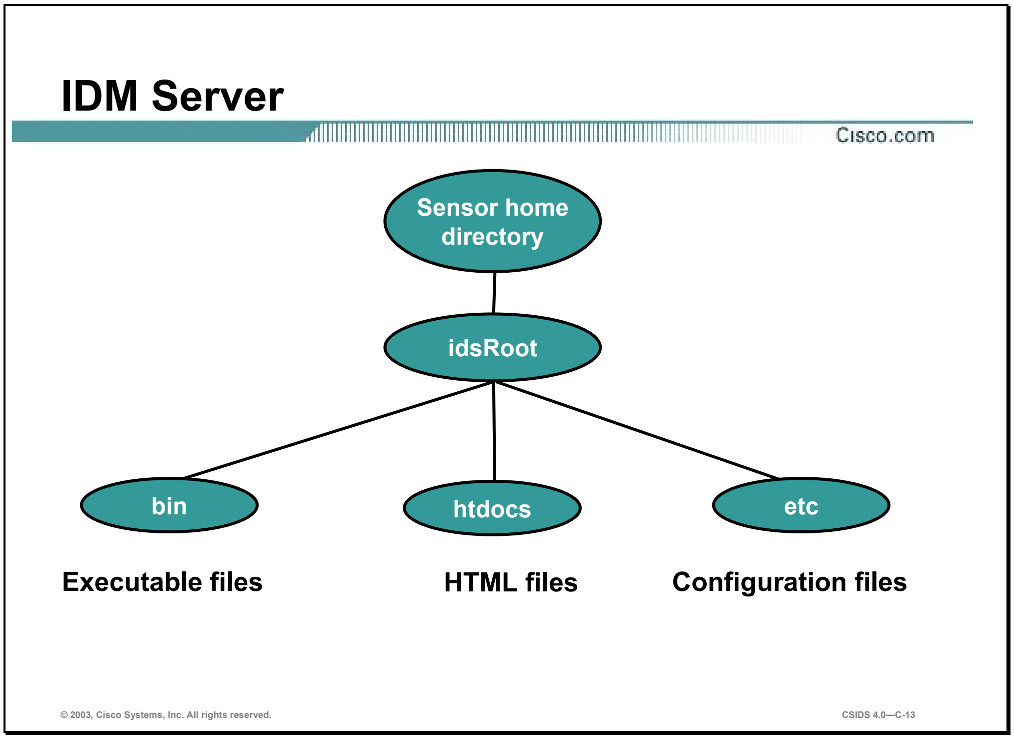
Send ack to
- Host ID = 20
- Org ID = 100
- App ID = 10000

CSIDS 4.0—C-11

In this example, Sensor 20.100 is transmitting a PostOffice message to the Director 10.100. The packetd service on the Sensor generates this message destined to the smid service on the Director. Once the Director has received the message, the Director’s postofficed service sends an acknowledgement message to the Sensor’s postofficed service.

Cisco IDS Directory Structure

This section describes the Cisco Intrusion Detection System (IDS) directory structure and IDS service files.



IDM Server

Cisco.com

Sensor home directory

idsRoot

bin

htdocs

etc

Executable files

HTML files

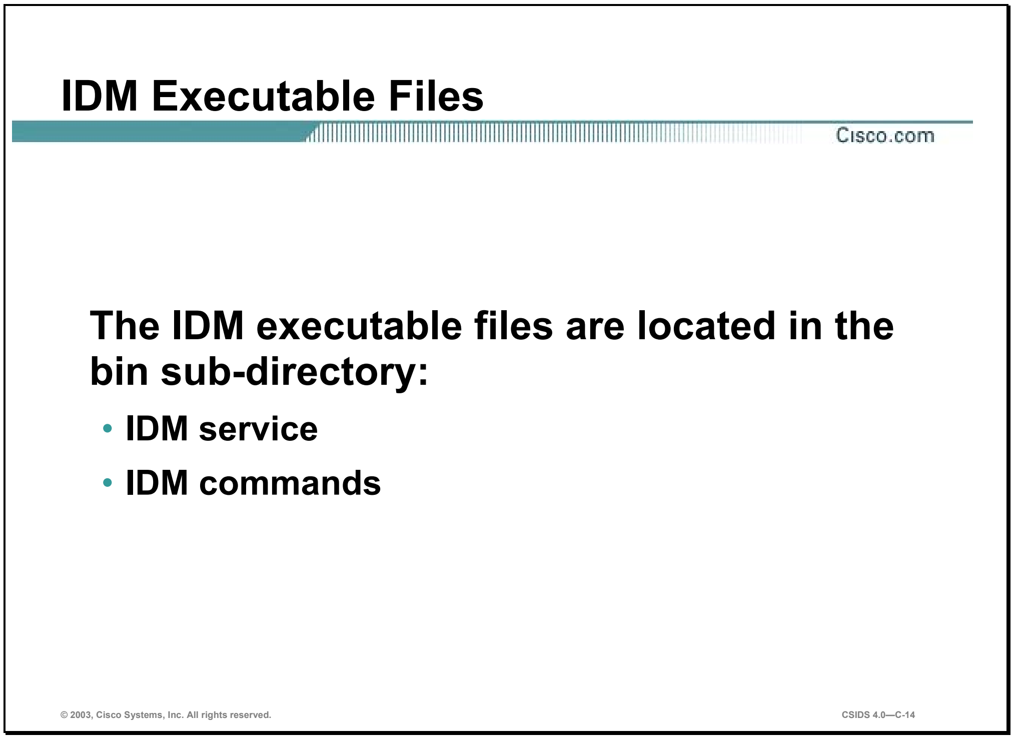
Configuration files

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-13

The IDM directory structure follows a hierarchy. The following are Cisco IDM directories:

- Sensor home directory—The 4200 series appliances Sensor directory is /usr/nr.
- idsRoot—This is the IDM home directory.
- bin—This is the executable file directory. It includes Cisco IDM services, programs, and functions.
- htdocs—This is the HTML document directory. It opens user requested HTML documents.
- etc—This is the configuration file directory. It includes configuration files for the Cisco IDM server.



IDM Executable Files

The IDM executable files are located in the bin sub-directory:

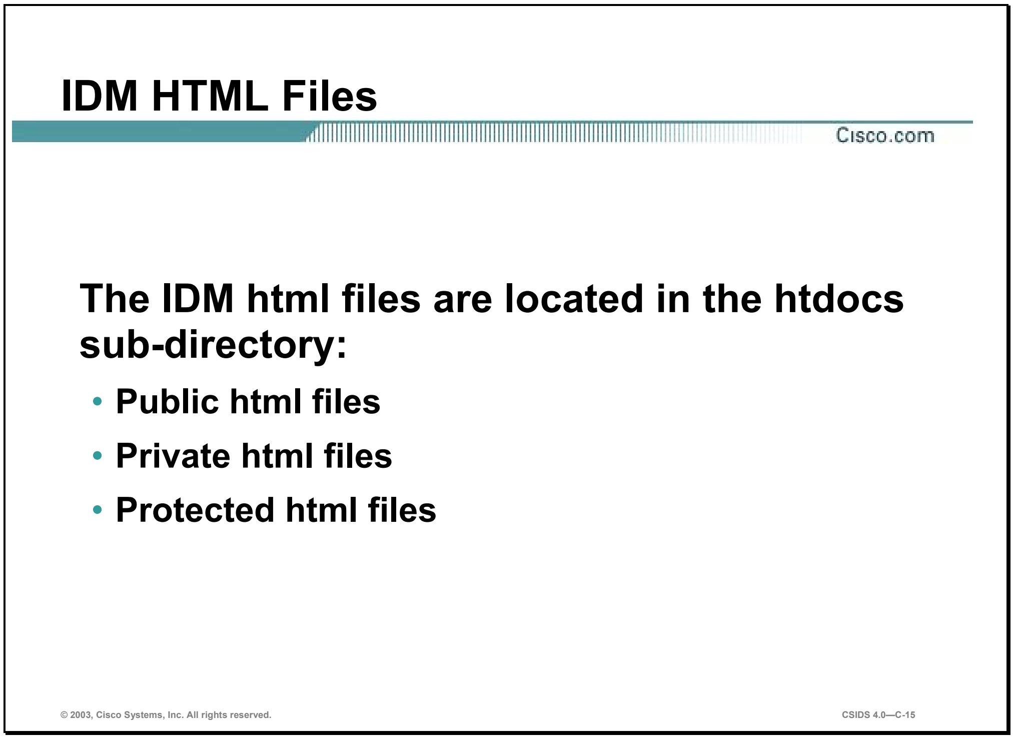
- **IDM service**
- **IDM commands**

CSIDS 4.0—C-14

The Cisco IDM services and commands are located in the bin sub-directory. The Cisco IDM service is cidwebserver.

The Cisco IDM commands include the following:

- cidServer
- fingerprint
- cidDump



IDM HTML Files

Cisco.com

The IDM html files are located in the htdocs sub-directory:

- Public html files
- Private html files
- Protected html files

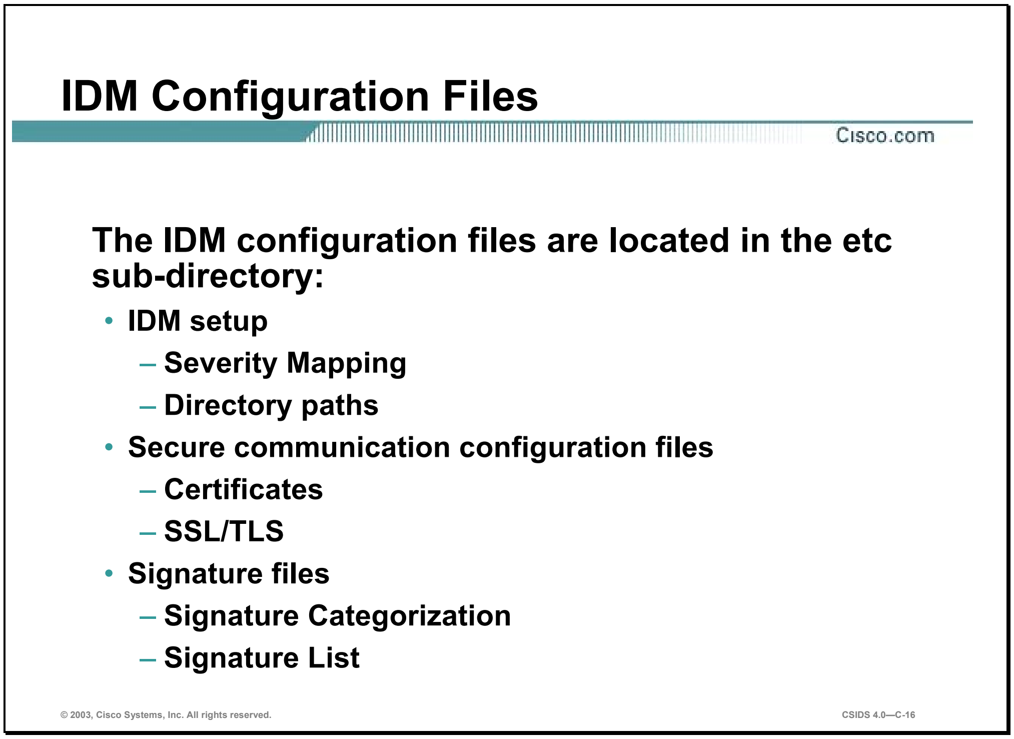
CSIDS 4.0—C-15

The Cisco IDM HTML files are located in the htdocs sub-directory. The Cisco IDM htdocs directory has the following sub-directories that contain the HTML documents:

- The public sub-directory contains the following HTML files:
  - applyingUpdate.html
  - index.html
  - logged_out.html
  - reboot.html
  - unauthorized.html
  - userlimit.html
- The private sub-directory contains the following HTML files:
  - auth/login.html
  - cidDump.html
- The protected sub-directory contains the following folders and HTML files:
  - idm/

        - help
        - templates
    - downloads/
    - nsdb/

Note Root privileges are required to access and view the contents of the protected directories.



IDM Configuration Files

Cisco.com

The IDM configuration files are located in the etc sub-directory:

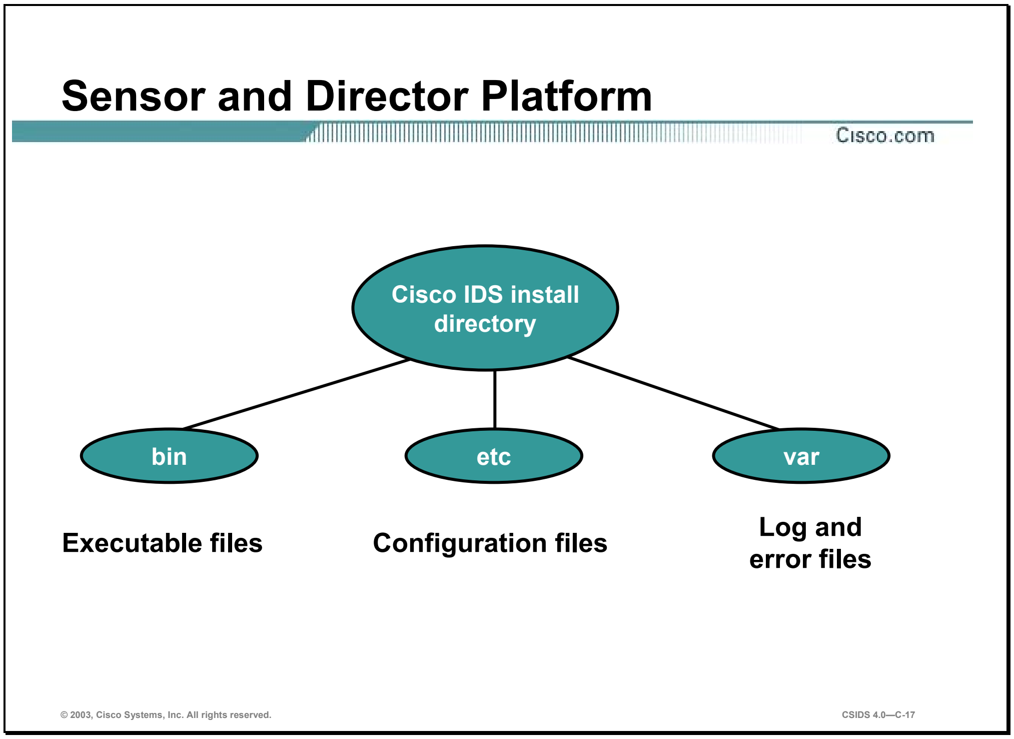
- IDM setup
  - Severity Mapping
  - Directory paths
- Secure communication configuration files
  - Certificates
  - SSL/TLS
- Signature files
  - Signature Categorization
  - Signature List

CSIDS 4.0—C-16

The Cisco IDM configuration files are located in the etc sub-directory. The Cisco IDM configuration files include the following:

- IDMSetup.xml
- SigCategory.txt
- auth.conf
- cert/
  - mytestca.priv
  - mytestca.cer
- cidwebserver.conf
- credentials.conf
- idm_conf
- selfcert.conf
- severityMapping.conf
- sigs.xml

- tls.conf



Sensor and Director Platform

Cisco.com

Cisco IDS install directory

bin

etc

var

Executable files

Configuration files

Log and error files

CSIDS 4.0—C-17

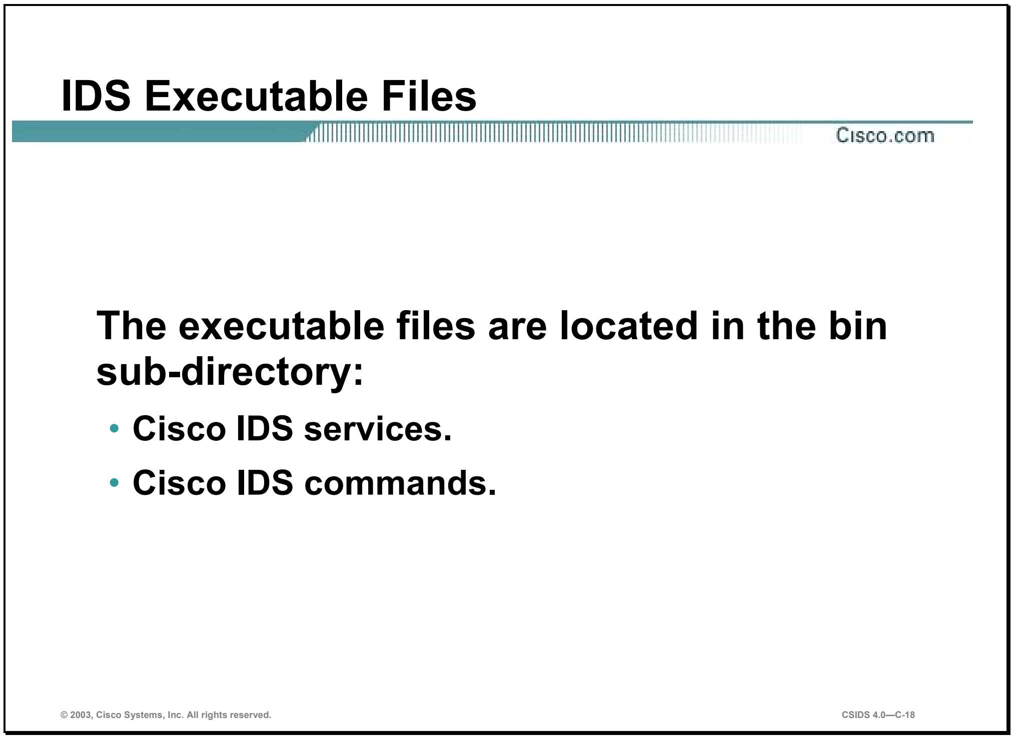
The Cisco IDS directory structure follows a hierarchy. The following are the Cisco IDS directories:

- Cisco IDS install directory—This is the installation directory. It is created during the installation phase of the Cisco IDS Director and is the main directory on the Sensor. The 4200 series appliances Cisco IDS install directory is /usr/nr. A default IEV PostOffice installation install directory is C:\Program Files\Cisco Systems\Cisco IDS Event Viewer\DataFeed.

- bin—This is the executable files directory. It includes all of the Cisco IDS services, programs, and functions.

- etc—This is the configuration files directory. It includes all configuration files for all of the Cisco IDS services.

- var—This is the log and error files directory. It includes the current and closed log files, IP session recorded files, and error files generated by the Cisco IDS services.



IDS Executable Files

The executable files are located in the bin sub-directory:

- **Cisco IDS services.**
- **Cisco IDS commands.**

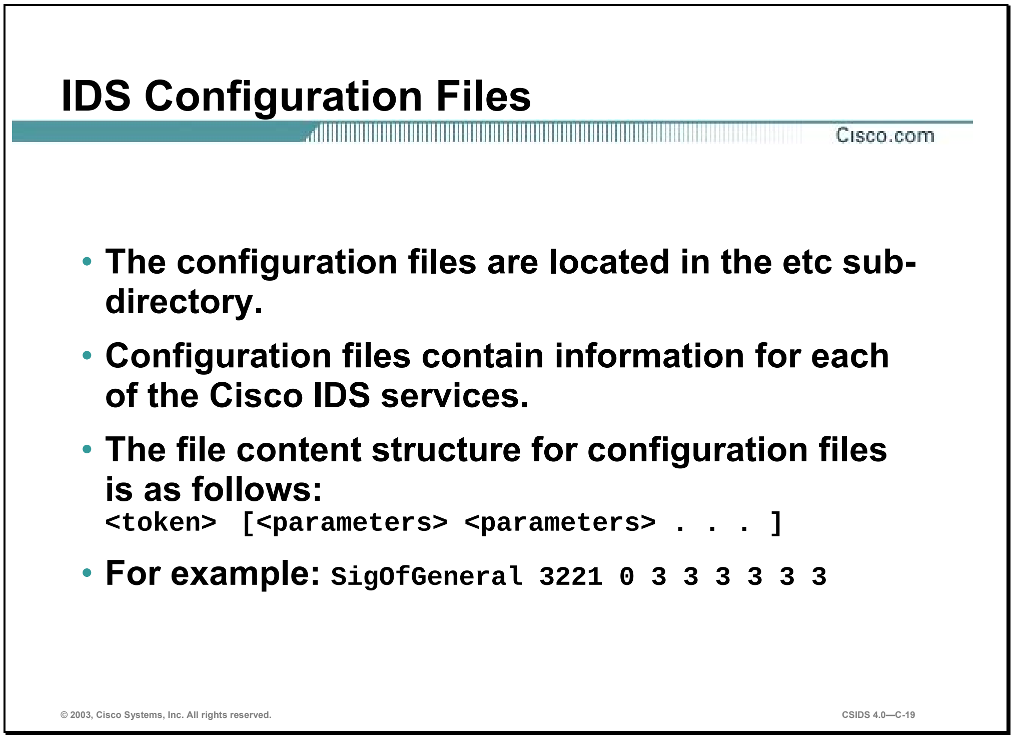
CSIDS 4.0—C-18

The Cisco IDS services and commands are located in the bin sub-directory. The Cisco IDS services include the following:

- packetd
- postofficed
- smid
- sapd
- fileXferd
- managed

The Cisco IDS commands include the following:

- idsstart
- idsstop
- idsconns
- idsvers
- idsstatus



IDS Configuration Files

- The configuration files are located in the etc sub-directory.
- Configuration files contain information for each of the Cisco IDS services.
- The file content structure for configuration files is as follows:
  `<token> [<parameters> <parameters> . . . ]`
- For example: `SigOfGeneral 3221 0 3 3 3 3 3 3`

Configuration files contain configuration information for each of the Cisco IDS services. The files are located in the etc sub-directory. The file content structure for configuration files is as follows:

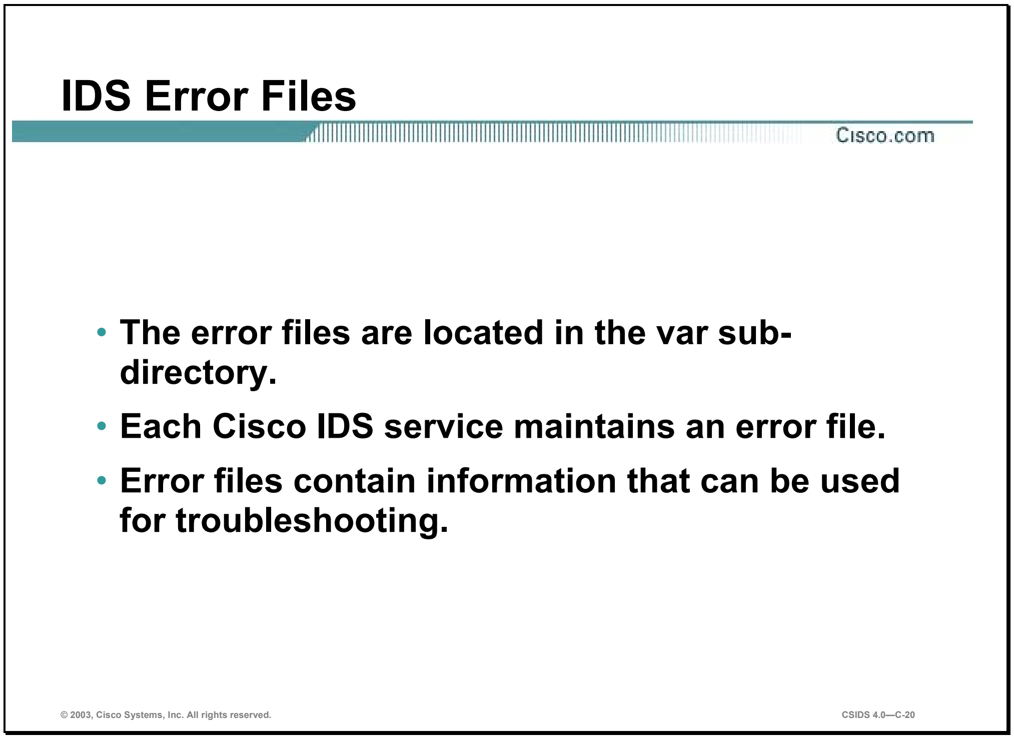
<token> [<parameters> <parameters> . . .]

token	Character string identifying a Cisco IDS service configurable item
parameters	Values associated with the Cisco IDS token

The following is an example from packetd.conf:

SigOfGeneral 3221 0 3 3 3 3 3 3

Note A pound sign precedes comments in the configuration files (#).



IDS Error Files

Cisco.com

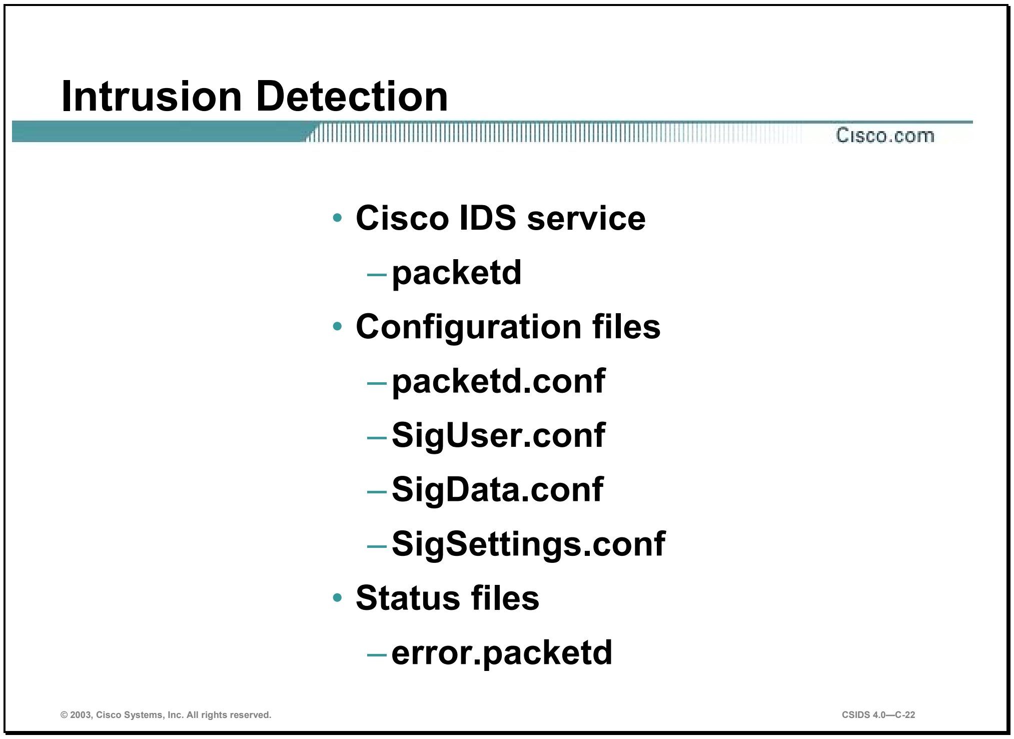
- The error files are located in the var sub-directory.
- Each Cisco IDS service maintains an error file.
- Error files contain information that can be used for troubleshooting.

CSIDS 4.0—C-20

Each Cisco IDS service that is started maintains an error file that exists in the var sub-directory. The error files are useful when troubleshooting. The files contain messages that can indicate the cause of problems associated with a service.

Cisco IDS Service Files

This section describes the Cisco Intrusion Detection System (Cisco IDS) services and files used when configuring a Cisco IDS Sensor.



Intrusion Detection

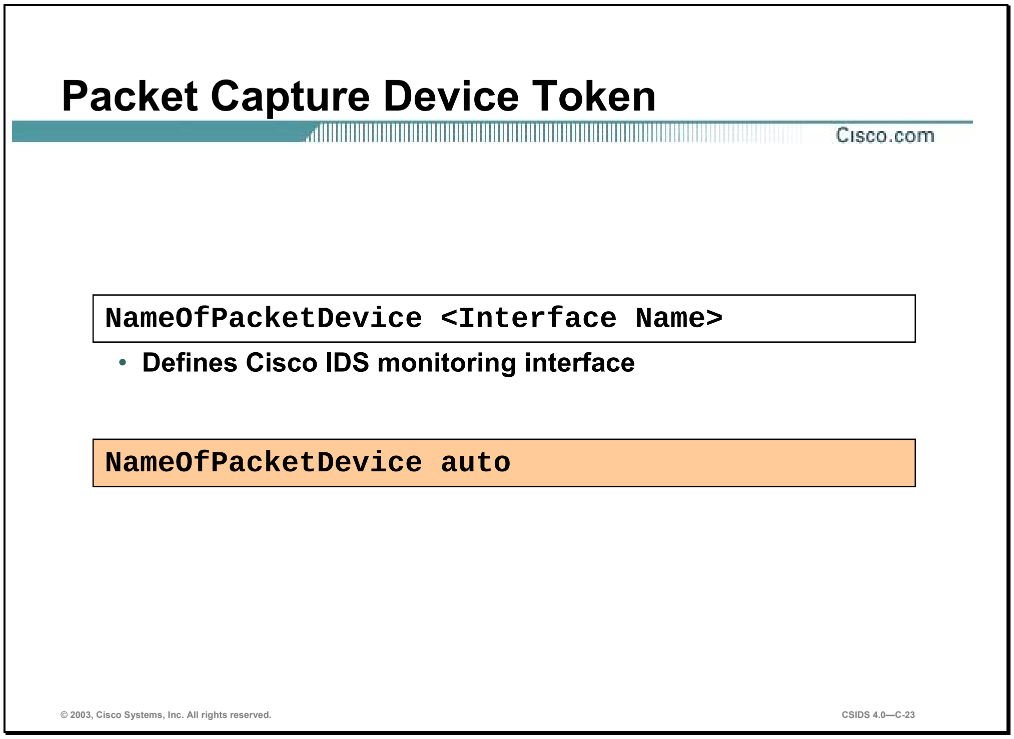
Cisco.com

- Cisco IDS service
  - packetd
- Configuration files
  - packetd.conf
  - SigUser.conf
  - SigData.conf
  - SigSettings.conf
- Status files
  - error.packetd

CSIDS 4.0—C-22

The Cisco IDS software service responsible for capturing network traffic and performing intrusion detection analysis is packetd. The Sensor intrusion detection settings are written to packetd.conf, SigUser.conf, SigData.conf, and SigSettings.conf files. The service status file is error.packetd.

Note	If the Cisco IDS is not capturing data as expected, verify that packetd is active on the Sensor using the **idsstatus** command.



Packet Capture Device Token

Cisco.com

```
NameOfPacketDevice <Interface Name>
```

- Defines Cisco IDS monitoring interface

```
NameOfPacketDevice auto
```

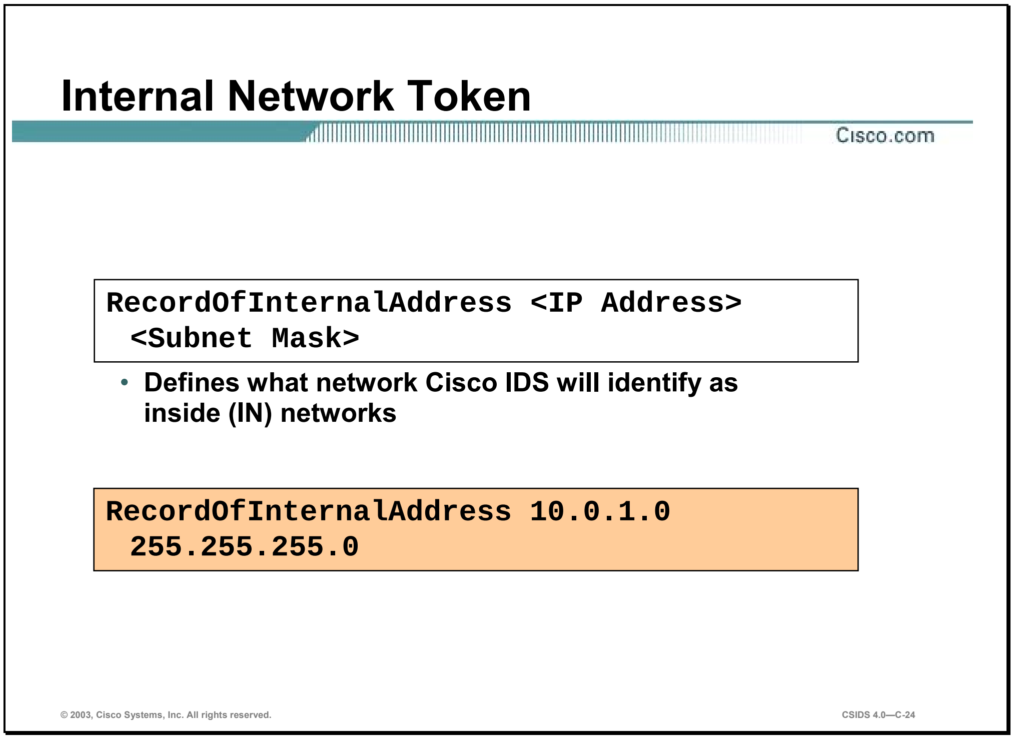
CSIDS 4.0—C-23

The NameOfPacketDevice token in the packetd.conf file defines the monitoring interface of the Sensor. The following is the token syntax:

NameOfPacketDevice <interface name>

interface name	The device name of the monitoring interface on the Sensor. The following is a list of possible values: ■ /dev/spwr0 ■ /dev/mtok0 ■ /dev/ptpci ■ /dev/iprb0 ■ /dev/e1000g0 auto

Note If the Cisco IDS is not capturing data as expected, verify that the NameOfPacketDevice token is assigned correctly based on the Sensor model.



Internal Network Token

Cisco.com

```
RecordOfInternalAddress <IP Address>
 <Subnet Mask>
```

- **Defines what network Cisco IDS will identify as inside (IN) networks**

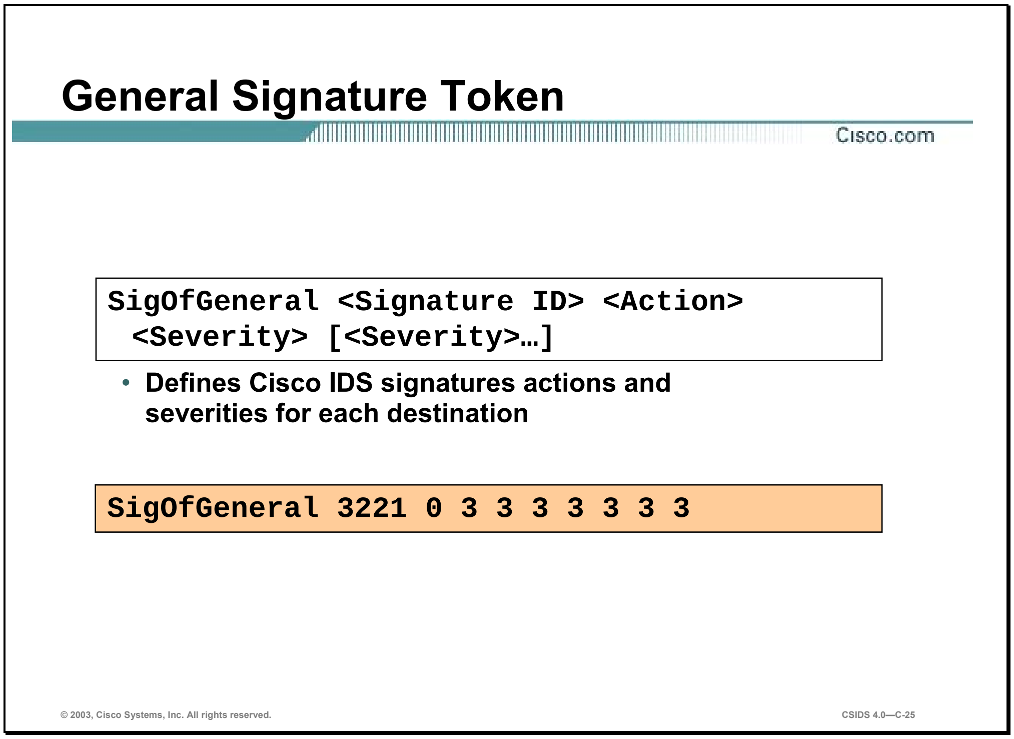
```
RecordOfInternalAddress 10.0.1.0
 255.255.255.0
```

© 2003, Cisco Systems, Inc. All rights reserved. CSIDS 4.0—C-24

The Cisco IDS enables you to define an internal network. The internal network is used to associate the source and destination location of alarms. The keywords IN and OUT signify the location in reference to the defined internal network. The following is the token syntax:

RecordOfInternalAddress <IP address> <subnet mask>

IP address	The IP address of the network or host that the Cisco IDS Sensor considers an internal network address.
Subnet mask	The network mask associated with the IP address of the network or host.



General Signature Token

Cisco.com

```
SigOfGeneral <Signature ID> <Action>
  <Severity> [<Severity>…]
```

- Defines Cisco IDS signatures actions and severities for each destination

```
SigOfGeneral 3221 0 3 3 3 3 3 3 3
```

© 2003, Cisco Systems, Inc. All rights reserved.

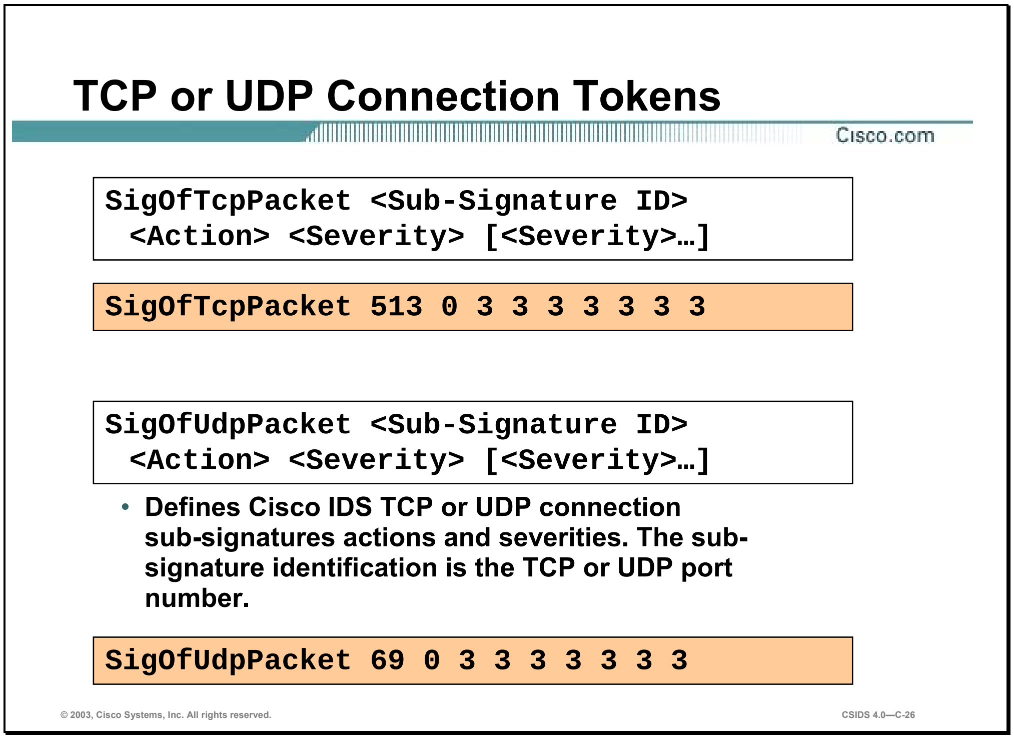
CSIDS 4.0—C-25

The SigOfGeneral token in the packetd.conf file is associated with the Cisco IDS General Signatures tab. The following is the token syntax:

SigOfGeneral <Signature ID> <Action> <Severity> [<Severity>...]

Signature ID	Numeric identification of the signature being configured (1–65535)
Action	■ 0—None ■ 1—Block ■ 2—IP log ■ 3—Block and IP log ■ 4—TCP Reset ■ 5—Block ■ 6—IP Log and TCP Reset ■ 7—Block, IP log, and TCP Reset
Severity	■ 0—Disabled Signature ■ 1—Informational ■ 2—Informational ■ 3—Low ■ 4—Medium ■ 5—High

The first severity setting represents the severity to be sent to destination 1 in the destinations file. The subsequent severities represent destination 2, destination 3, and so on, in the destinations file. The Cisco IDS supports a maximum of 32 destinations, and for every destination a severity level must be set.



TCP or UDP Connection Tokens

```
SigOfTcpPacket <Sub-Signature ID>
 <Action> <Severity> [<Severity>…]
```

```
SigOfTcpPacket 513 0 3 3 3 3 3 3 3
```

```
SigOfUdpPacket <Sub-Signature ID>
 <Action> <Severity> [<Severity>…]
```

- **Defines Cisco IDS TCP or UDP connection sub-signatures actions and severities. The sub-signature identification is the TCP or UDP port number.**

```
SigOfUdpPacket 69 0 3 3 3 3 3 3 3
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-26

The SigOfTcpPacket and SigOfUdpPacket tokens in the packetd.conf file are associated with the Cisco IDS TCP or UDP Signatures.

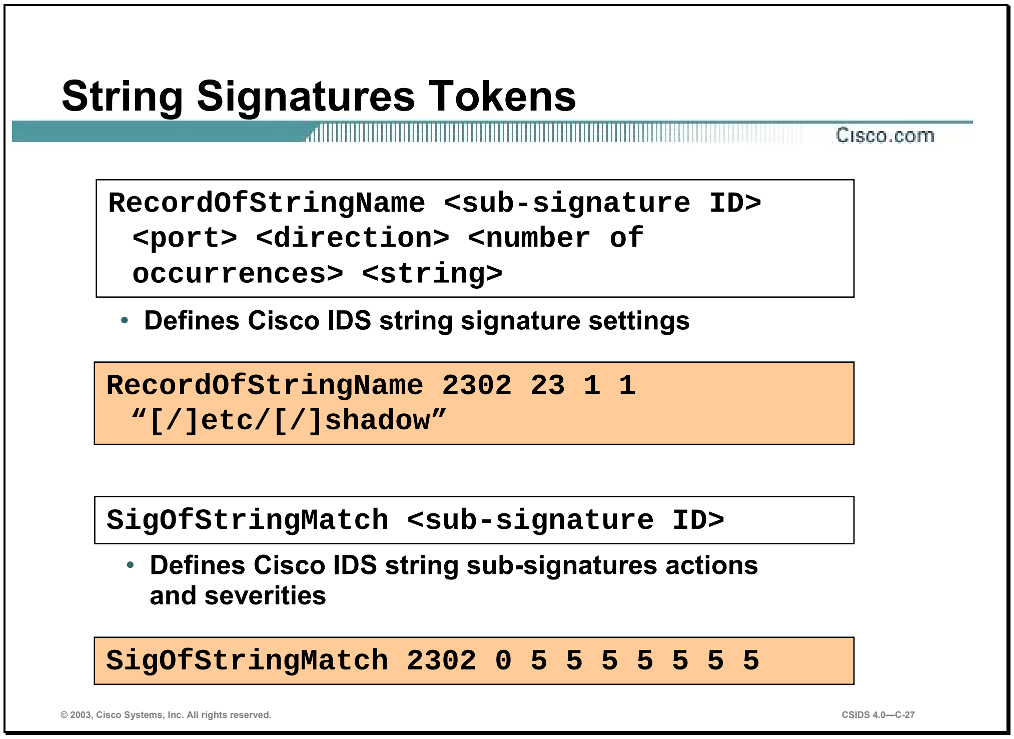
The following are the token syntax:

SigOfTcpPacket <Port> <Action> <Severity> [<Severity>...]

SigOfUdpPacket <Port> <Action> <Severity> [<Severity>...]

Port	The TCP communication request port number of the UDP traffic request port number. The port number assigned is the sub-signature identification for TCP records and UDP packet records.
Action	■ 0—None ■ 1—Block ■ 2—IP log ■ 3—Block and IP log ■ 4—TCP Reset ■ 5—Block ■ 6—IP Log and TCP Reset ■ 7—Block, IP log, and TCP Reset
Severity	■ 0—Disabled Signature ■ 1—Informational ■ 2—Informational ■ 3—Low ■ 4—Medium ■ 5—High

The first severity setting represents the severity to be sent to destination 1 in the destinations file. The subsequent severities represent destination 2, destination 3, and so on, in the destinations file. The Cisco IDS supports a maximum of 32 destinations, and for every destination a severity level must be set.



String Signatures Tokens

```
RecordOfStringName <sub-signature ID>
 <port> <direction> <number of
 occurrences> <string>
```

- Defines Cisco IDS string signature settings

```
RecordOfStringName 2302 23 1 1
 “[/]etc/[/]shadow”
```

```
SigOfStringMatch <sub-signature ID>
```

- Defines Cisco IDS string sub-signatures actions and severities

```
SigOfStringMatch 2302 0 5 5 5 5 5 5 5
```

CSIDS 4.0—C-27

The **RecordOfStringName** and **SigOfStringMatch** tokens in the packetd.conf file are associated with the Cisco IDS string signatures. The following are the token syntax:

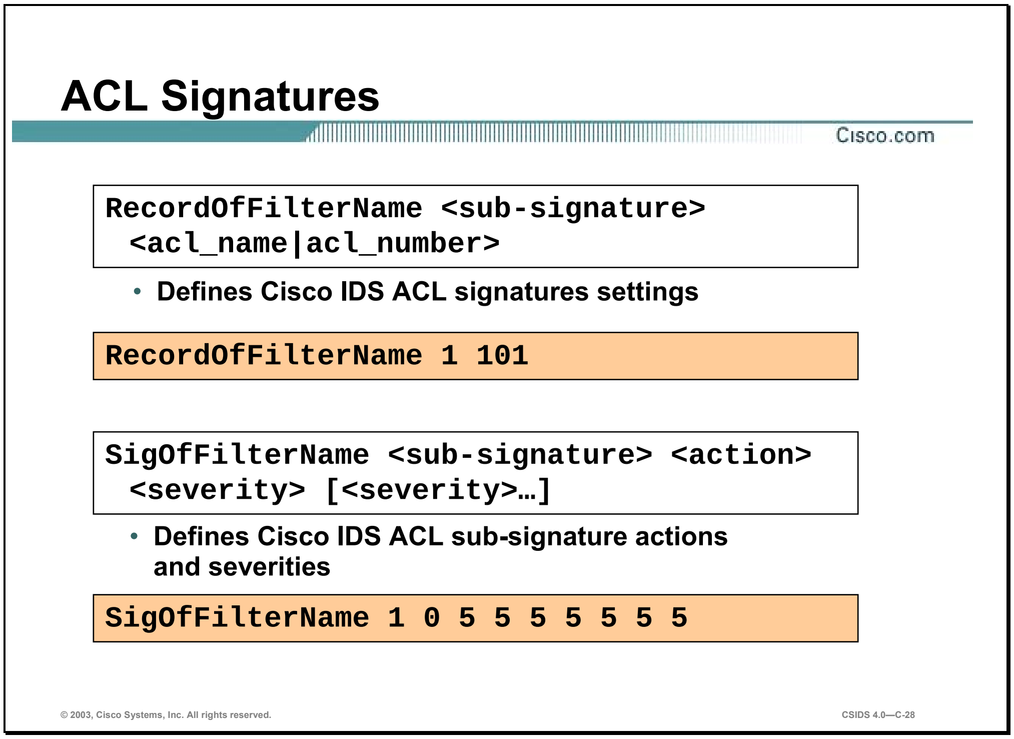
RecordOfStringName <Sub-Signature ID> <Port> <Direction> <Num of Occurrences> <String>

Sub-Signature ID	Numeric identification of the sub-signature being configured (1–65535)
Port	TCP port number that the signature examines for the given string match
Direction	1—To the specified port number 2—From the specified port number 3—Both directions
Num of Occurrences	Number of times the string occurs in the session before an alarm is triggered
String	Actual string to look for, uses regular expression format

SigOfStringMatch <Sub-Signature ID> <Action> <Severity> [<Severity>...]

Sub-Signature ID	Numeric identification of the sub-signature being configured (1–65535)
Action	■ 0—None ■ 1—Block ■ 2—IP log ■ 3—Block and IP log ■ 4—TCP Reset ■ 5—Block ■ 6—IP Log and TCP Reset ■ 7—Block, IP log, and TCP Reset
Severity	■ 0—Disabled Signature ■ 1—Informational ■ 2—Informational ■ 3—Low ■ 4—Medium ■ 5—High

The first severity setting represents the severity to be sent to destination 1 in the destinations file. The subsequent severities represent destination 2, destination 3, and so on, in the destinations file. The Cisco IDS supports a maximum of 32 destinations, and for every destination a severity level must be set.



ACL Signatures

Cisco.com

```
RecordOfFilterName <sub-signature>
  <acl_name|acl_number>
```

- Defines Cisco IDS ACL signatures settings

```
RecordOfFilterName 1 101
```

```
SigOfFilterName <sub-signature> <action>
  <severity> [<severity>…]
```

- Defines Cisco IDS ACL sub-signature actions and severities

```
SigOfFilterName 1 0 5 5 5 5 5 5 5
```

CSIDS 4.0—C-28

The RecordOfFilterName and SigOfFilterName tokens in the packetd.conf file are associated with the Cisco IDS ACL signatures. The following is the token syntax:

RecordOfFilterName <Sub-Signature ID> <acl_name|acl_number>

Sub-Signature ID	Numeric identification of the sub-signature being configured (1–65535)
acl_name	Name of the ACL list that triggers policy violation alarms
acl_number	Number of the ACL list that triggers policy violation alarms

Note The Director generates the sub-signature identification automatically.

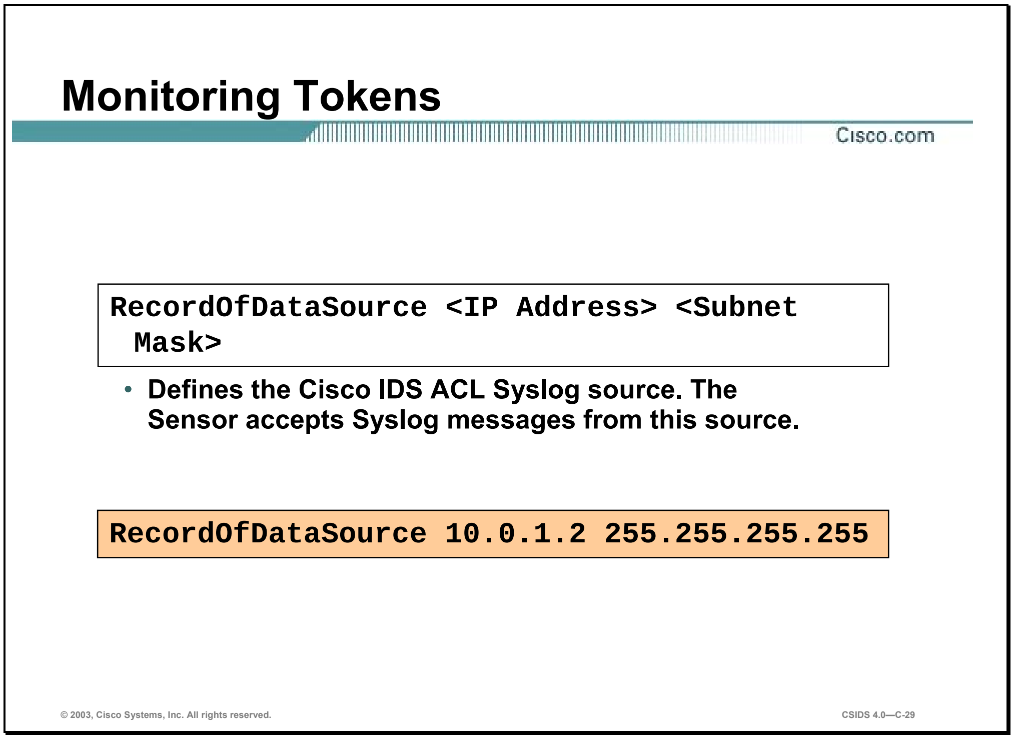
SigOfFilterName <Sub-Signature ID> <Action> <Severity> [<Severity>...]

Sub-Signature ID	Numeric identification of the sub-signature being configured (1–65535)
Action	■ 0—None ■ 1—Block ■ 2—IP log ■ 3—Block and IP log ■ 4—TCP Reset ■ 5—Block ■ 6—IP Log and TCP Reset ■ 7—Block, IP log, and TCP Reset

Severity	■ 0—Disabled Signature ■ 1—Informational ■ 2—Informational ■ 3—Low ■ 4—Medium ■ 5—High

The first severity setting represents the severity to be sent to destination 1 in the destinations file. The subsequent severities represent destination 2, destination 3, and so on, in the destinations file. The Cisco IDS supports a maximum of 32 destinations, and for every destination a severity level must be set.

Note The Director generates the sub-signature identification automatically.



Monitoring Tokens

```
RecordOfDataSource <IP Address> <Subnet
 Mask>
```

- Defines the Cisco IDS ACL Syslog source. The Sensor accepts Syslog messages from this source.

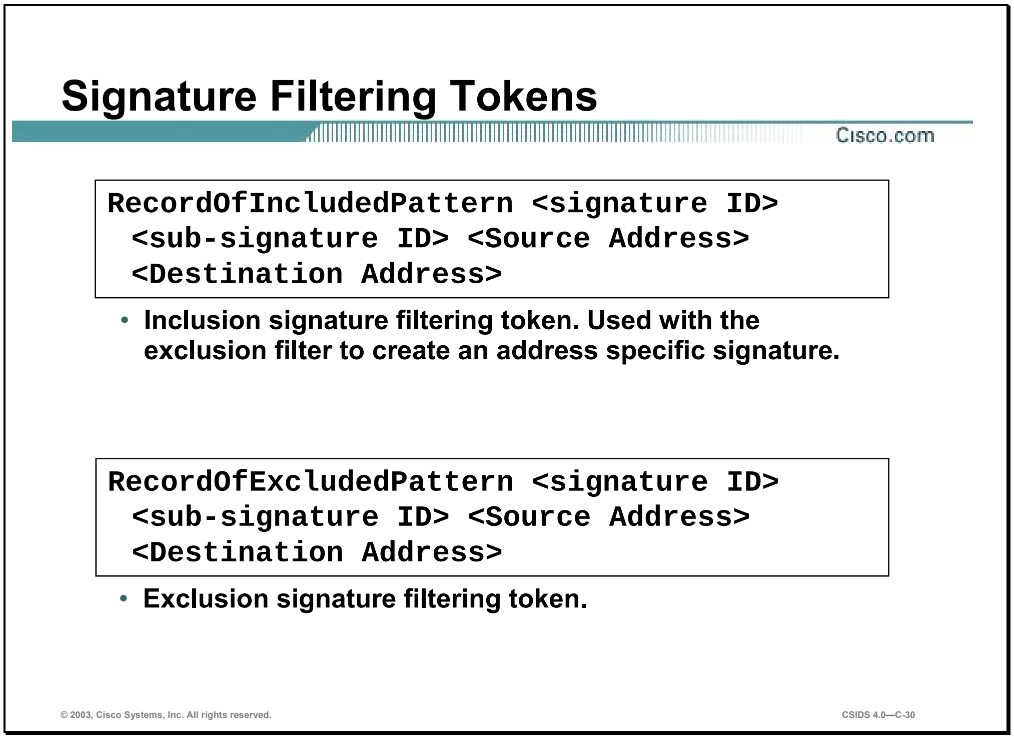
```
RecordOfDataSource 10.0.1.2 255.255.255.255
```

CSIDS 4.0—C-29

The RecordOfDataSource token in the packetd.conf file is associated with the Cisco IDS ACL signatures. The following is the token syntax:

RecordOfDataSource <IP Address> <Subnet Mask>

IP Address	IP address of the Cisco router from which the Sensor is accepting Syslog messages
Mask	Network mask associated with the IP address of the Cisco router from which the Sensor is accepting Syslog messages



Signature Filtering Tokens

```
RecordOfIncludedPattern <signature ID>
 <sub-signature ID> <Source Address>
 <Destination Address>
```

- Inclusion signature filtering token. Used with the exclusion filter to create an address specific signature.

```
RecordOfExcludedPattern <signature ID>
 <sub-signature ID> <Source Address>
 <Destination Address>
```

- Exclusion signature filtering token.

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-30

The RecordOfIncludedPattern token in the packetd.conf file is associated with signature filtering. The following is the token syntax:

RecordOfIncludedPattern <Signature ID>[,<Signature ID>…] <Sub-Signature ID>[,<Sub-Signature ID>…] <Source Address> <Destination Address>

RecordOfIncludedPattern <Signature ID>[-<Signature ID>…] <Sub-Signature ID>[-<Sub-Signature ID>…] <Source Address> <Destination Address>

Signature ID	Signature identification for which the Cisco IDS will generate an event if the given IP address is the source, destination, or both the source and destination of the traffic. An asterisk (*) can be used as a wildcard to define all signatures.
Sub-Signature ID	Subsignature ID for which the Cisco IDS will generate an event if the given IP address is the source, destination, or both the source and destination of the traffic. An asterisk (*) can be used as a wildcard to define all signatures.
Source Address	IP address or network for which the Cisco IDS will generate an event if the IP address is the source of the traffic. The IP address or network can be represented with a network mask or CIDR notation. An asterisk (*) can be used as a wildcard to define all signatures. The keywords IN and OUT can be used to define the source as either originating from inside or outside the internal work. An internal network must have been previously defined.

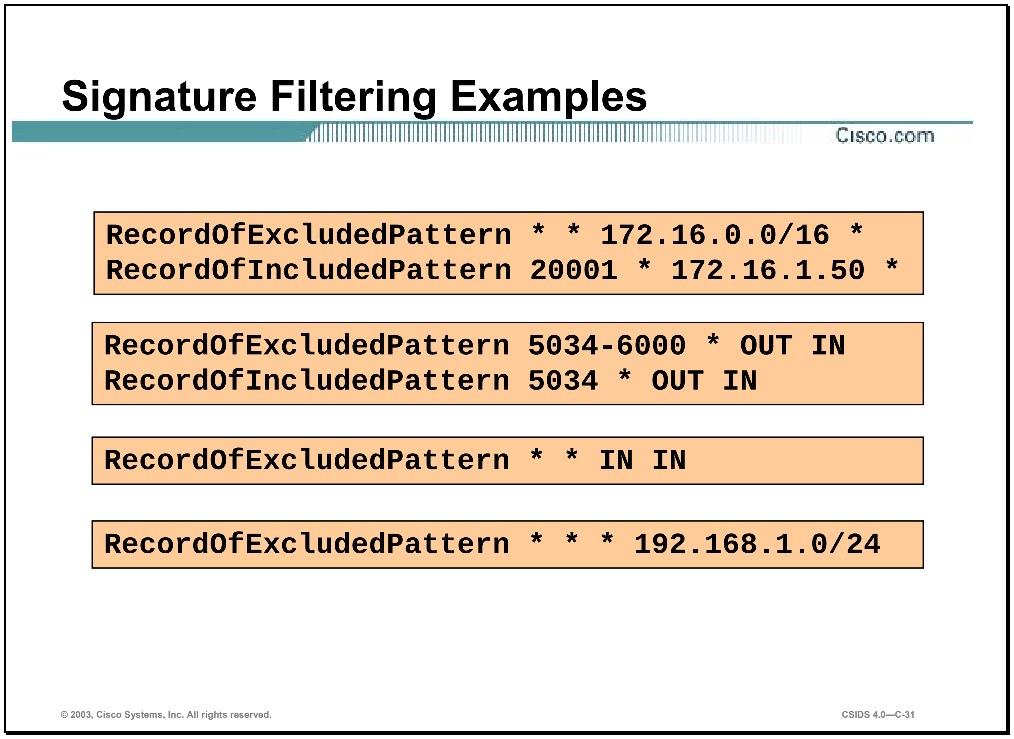
Destination Address	IP address or network for which the Cisco IDS will generate an event if the IP address is the destination of the traffic. The IP address or network can be represented with a network mask or CIDR notation. An asterisk (*) can be used as a wildcard to define all signatures. The keywords IN and OUT can be used to define the source as either originating from inside or outside the internal work. An internal network must have been previously defined.

The **RecordOfExcludedPattern** token in the packetd.conf file is associated with signature filtering. The following is the token syntax:

RecordOfExcludedPattern <Signature ID>[,<Signature ID>…] <Sub-Signature ID>[,<Sub-Signature ID>…] <Source Address> <Destination Address>

RecordOfExcludedPattern <Signature ID>[-<Signature ID>…] <Sub-Signature ID>[-<Sub-Signature ID>…] <Source Address> <Destination Address>

Signature ID	Signature identification for which the Cisco IDS will not generate an event if the given IP address is the source, destination, or both the source and destination of the traffic. An asterisk (*) can be used as a wildcard to define all signatures.
Sub-Signature ID	Subsignature ID for which the Cisco IDS will not generate an event if the given IP address is the source, destination, or both the source and destination of the traffic. An asterisk (*) can be used as a wildcard to define all signatures.
Source Address	IP address or network for which the Cisco IDS will not generate an event if the IP address is the source of the traffic. The IP address or network can be represented with a network mask or CIDR notation. An asterisk (*) can be used as a wildcard to define all signatures. The keywords IN and OUT can be used to define the source as either originating from inside or outside the internal work. An internal network must have been previously defined.
Destination Address	IP address or network for which the Cisco IDS will not generate an event if the IP address is the destination of the traffic. The IP address or network can be represented with a network mask or CIDR notation. An asterisk (*) can be used as a wildcard to define all signatures. The keywords IN and OUT can be used to define the source as either originating from inside or outside the internal work. An internal network must have been previously defined.



Signature Filtering Examples

```
RecordOfExcludedPattern * * 172.16.0.0/16 *
RecordOfIncludedPattern 20001 * 172.16.1.50 *
```

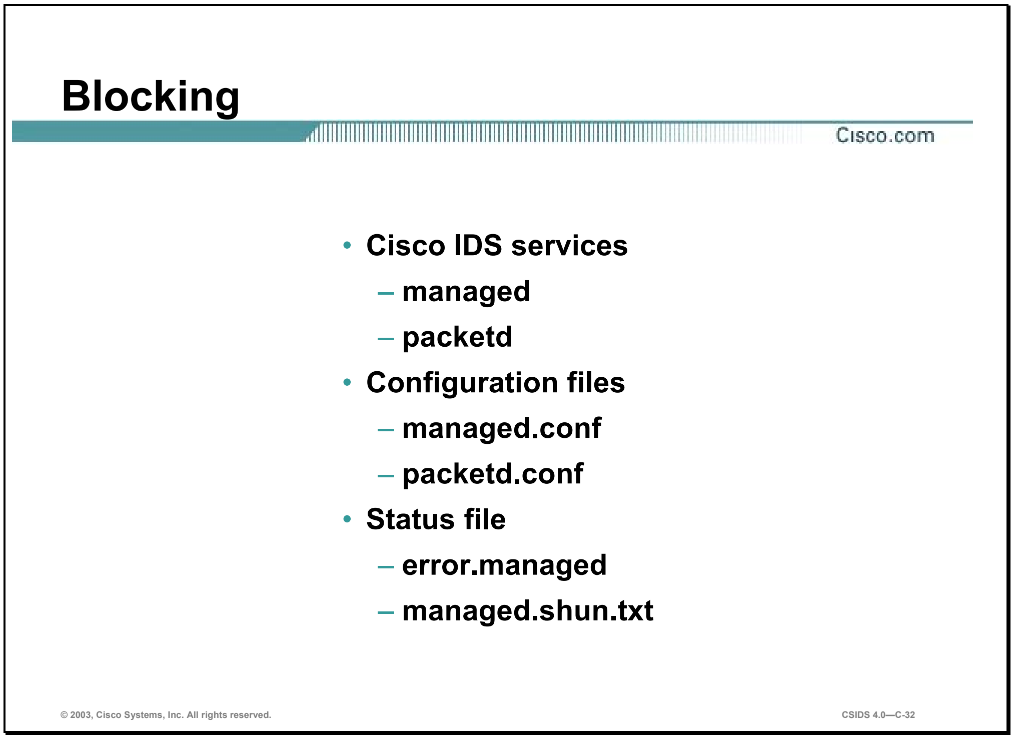
```
RecordOfExcludedPattern 5034-6000 * OUT IN
RecordOfIncludedPattern 5034 * OUT IN
```

```
RecordOfExcludedPattern * * IN IN
```

```
RecordOfExcludedPattern * * * 192.168.1.0/24
```

The following describes the example signature filtering tokens:

- RecordOfExcludedPattern * * 172.16.0.0/16—The Cisco IDS will not generate an event on all signatures and all associated subsignatures from the 172.16.0.0/16 network to any destination.
- RecordOfIncludedPattern * * 172.16.1.50—The Cisco IDS will generate an event when signature 20001 and all associated subsignatures are triggered from the host 172.16.1.50 to any destination.
- RecordOfExcludedPattern 5034-6000 * OUT IN—The Cisco IDS will not generate an event on signatures 5034 through 6000 and all associated subsignatures from the outside, OUT, destined to the defined inside, IN, networks.
- RecordOfIncludedPattern 5034 * OUT IN—The Cisco IDS will generate an event when signature 5034 and all associated subsignatures are triggered from the outside, OUT, destined to the defined inside, IN, networks.
- RecordOfExcludedPattern * * IN IN—The Cisco IDS will not generate an event on all signatures and all associated subsignatures from the internal network destined to the internal network.
- RecordOfExcludedPattern * * * 192.168.1.0/24—The Cisco IDS will not generate an event on all signatures and all associated subsignatures from any source destined to the 192.168.1.0/24 network.



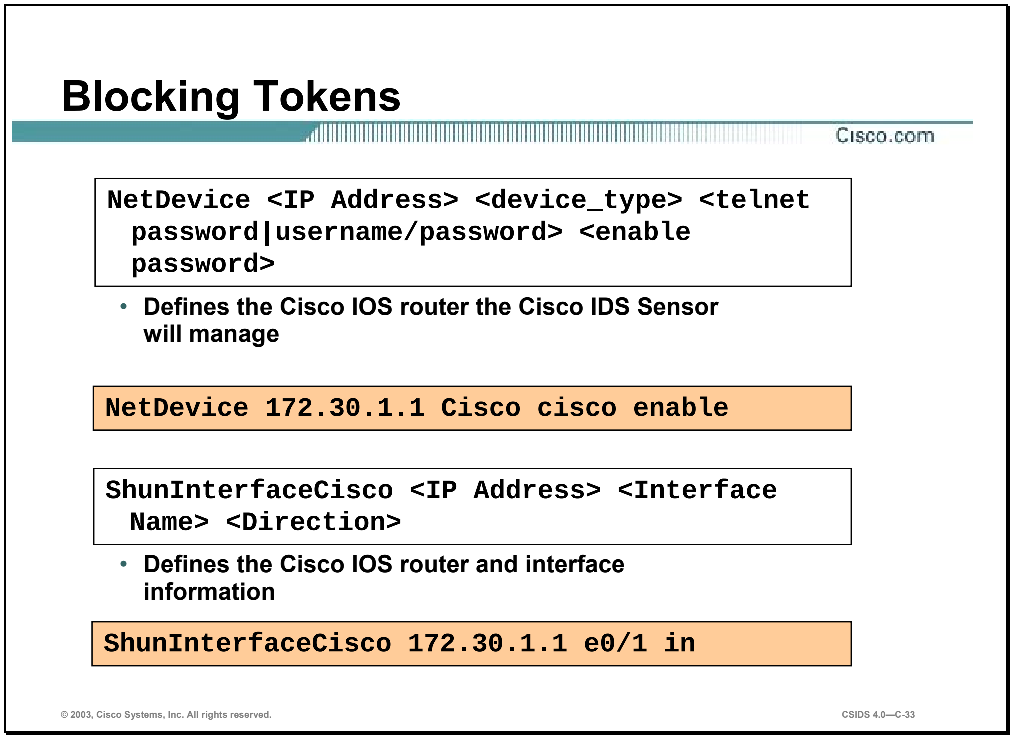
Blocking

Cisco.com

- Cisco IDS services
  - managed
  - packetd
- Configuration files
  - managed.conf
  - packetd.conf
- Status file
  - error.managed
  - managed.shun.txt

CSIDS 4.0—C-32

The managed service generates ACLs to be applied to a Cisco router or Catalyst switch and issues the shun command on a PIX Firewall. The Sensor IP blocking settings are written to the managed.conf and packetd files. The managed status files are error.managed and managed.shun.txt. The managed.shun.txt file maintains the list of blocked IP addresses.



Blocking Tokens

Cisco.com

```
NetDevice <IP Address> <device_type> <telnet
  password|username/password> <enable
  password>
```

- Defines the Cisco IOS router the Cisco IDS Sensor will manage

```
NetDevice 172.30.1.1 Cisco cisco enable
```

```
ShunInterfaceCisco <IP Address> <Interface
  Name> <Direction>
```

- Defines the Cisco IOS router and interface information

```
ShunInterfaceCisco 172.30.1.1 e0/1 in
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-33

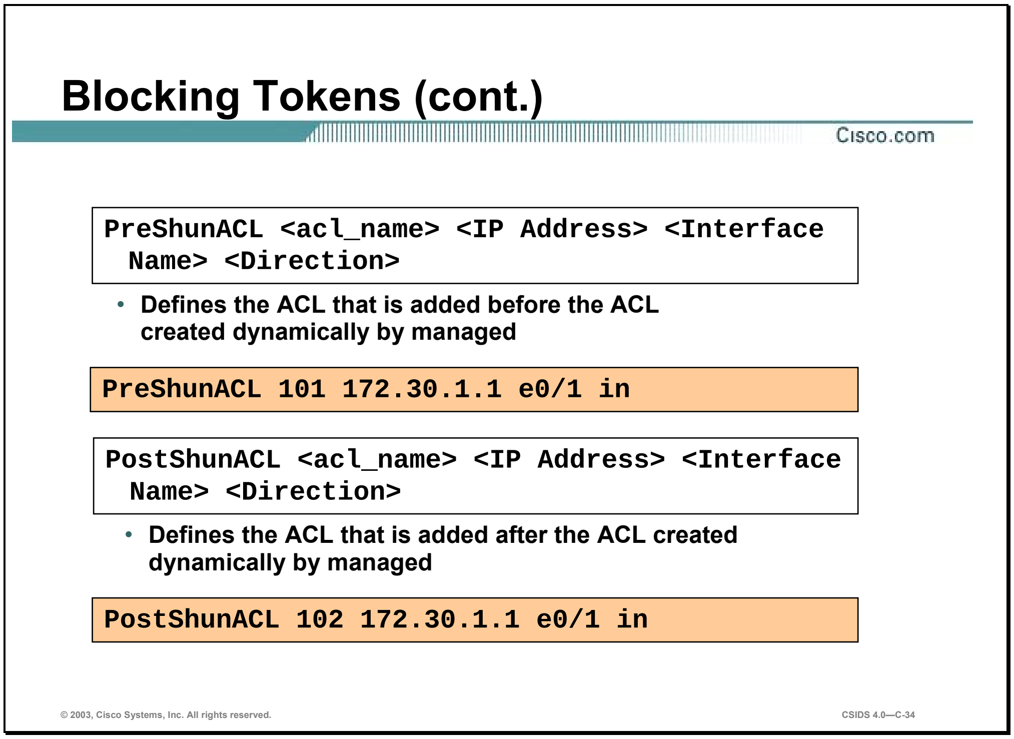
The following are the tokens in the managed.conf file associated with the blocking feature:

NetDevice <IP Address> CiscoDefault <Telnet Password>|<Telnet Username/Password> <Enable password>

IP Address	IP address the Sensor telnets to on the router
CiscoDefault	Not user configurable
Telnet Password or Telnet Username/Password	Password, or username and password combination to telnet to the router
Enable Password	Password for the router's enable mode

ShunInterfaceCisco <IP Address> <Interface Name> <Direction>

IP Address	IP address of the managed router. The Sensor should have Telnet access to this IP address.
Interface Name	Name of the interface where the ACL is applied. No space is allowed between the interface name and its number. Some examples are as follows: ■ ethernet0 ■ e0 ■ serial0/1 ■ s0/1
Direction	The direction to which the shunning ACLs are applied: IN or OUT.



Blocking Tokens (cont.)

Cisco.com

```
PreShunACL <acl_name> <IP Address> <Interface
  Name> <Direction>
```

- Defines the ACL that is added before the ACL created dynamically by managed

```
PreShunACL 101 172.30.1.1 e0/1 in
```

```
PostShunACL <acl_name> <IP Address> <Interface
  Name> <Direction>
```

- Defines the ACL that is added after the ACL created dynamically by managed

```
PostShunACL 102 172.30.1.1 e0/1 in
```

CSIDS 4.0—C-34

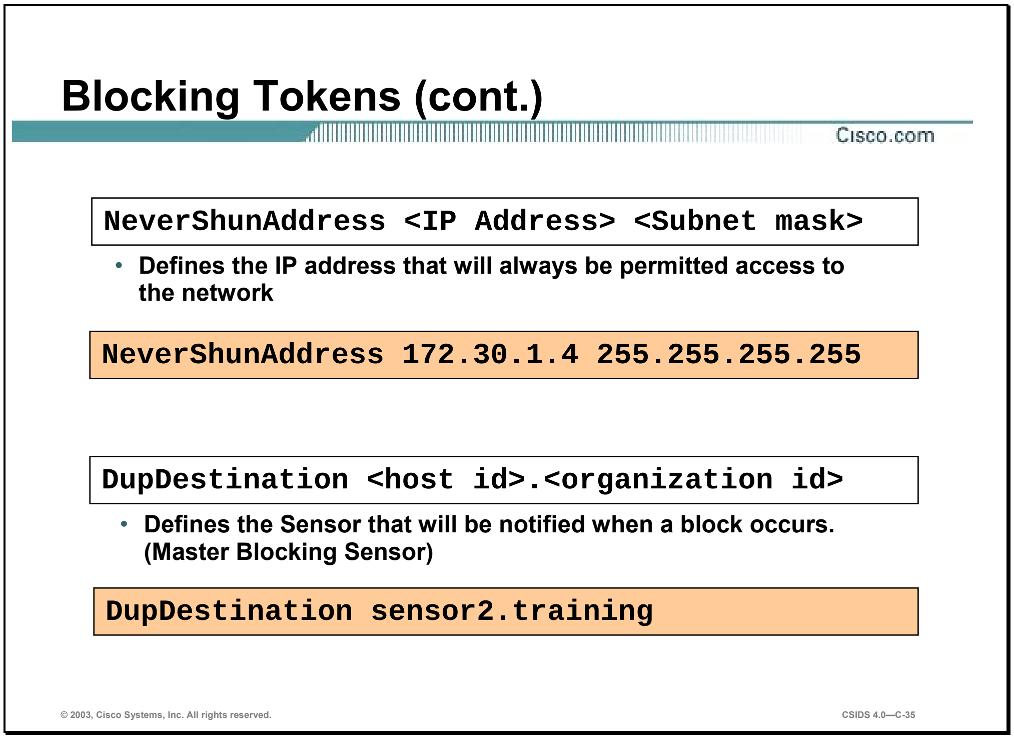
The following are the tokens in the managed.conf file associated with the blocking feature:

PreShunACL <acl_name> <IP Address> <Interface Name> <Direction>

acl_name	Name or number of an extended IP ACL
IP Address	IP address of the managed device's control interface
Interface Name	Name of the managed device's interface where the ACL is applied
Direction	The direction (IN or OUT) that the ACL is applied

PostShunACL <acl_name> <IP Address> <Interface Name> <Direction>

acl_name	Name or number of an extended IP ACL
IP Address	IP address of the managed device's control interface
Interface Name	Name of the managed device's interface where the ACL is applied
Direction	The direction (IN or OUT) that the ACL is applied



Blocking Tokens (cont.)

Cisco.com

```
NeverShunAddress <IP Address> <Subnet mask>
```

- Defines the IP address that will always be permitted access to the network

```
NeverShunAddress 172.30.1.4 255.255.255.255
```

```
DupDestination <host id>.<organization id>
```

- Defines the Sensor that will be notified when a block occurs. (Master Blocking Sensor)

```
DupDestination sensor2.training
```

CSIDS 4.0—C-35

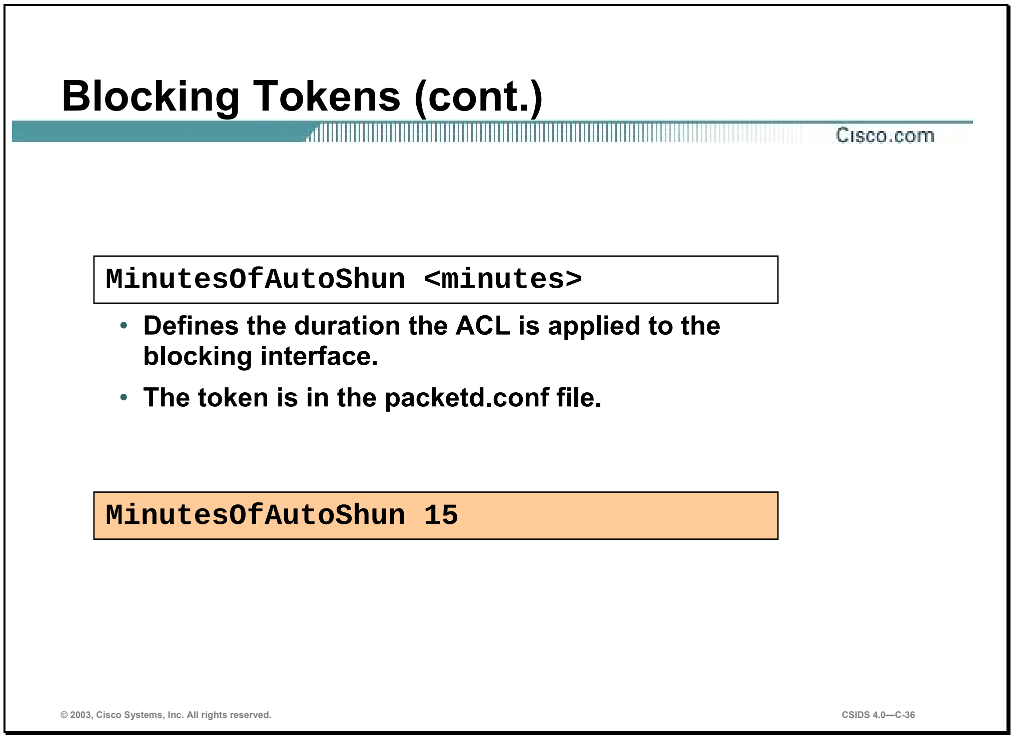
The following are the tokens in the managed.conf file associated with the blocking feature:

NeverShunAddress <IP Address> <Mask>

IP Address	IP address the Sensor telnets to on the router
Mask	Network mask associated with the IP address the Sensor telnets to on the router

DupDestination <Host Name>

Host Name	The Cisco IDS hostname (host id.organization id) of the other Sensor performing blocking on other routers that the user wants to activate when this Sensor responds with a block request. A Cisco IDS Sensor with the blocking feature is referred to as a Master Blocking Sensor.



Blocking Tokens (cont.)

Cisco.com

```
MinutesOfAutoShun <minutes>
```

- Defines the duration the ACL is applied to the blocking interface.
- The token is in the packetd.conf file.

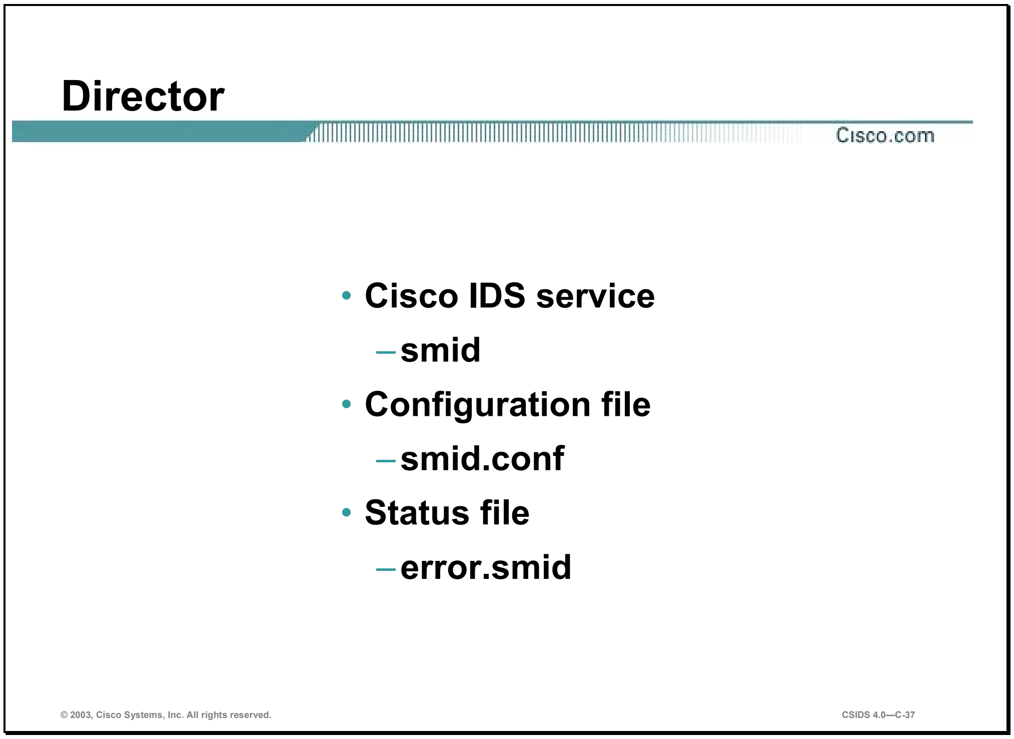
```
MinutesOfAutoShun 15
```

CSIDS 4.0—C-36

The following are the tokens in the packetd.conf file associated with the blocking feature:

MinutesOfAutoShun <Minutes>

Minutes	Number of minutes the Cisco IDS blocks an attacking host or network

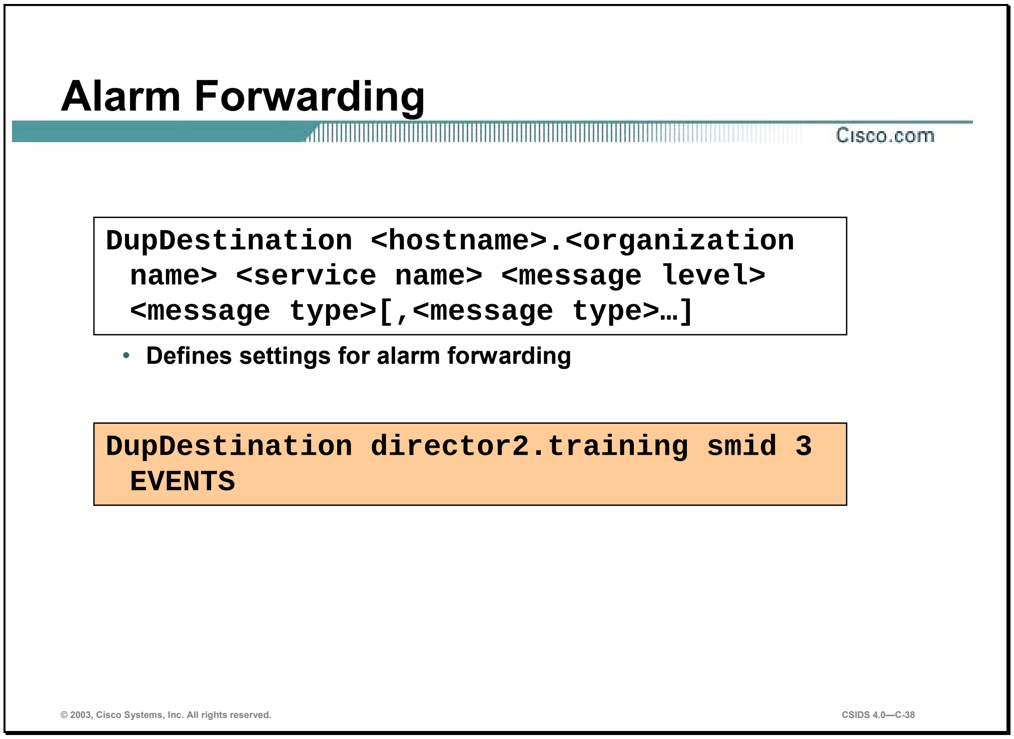


Director

- Cisco IDS service
  - smid
- Configuration file
  - smid.conf
- Status file
  - error.smid

CSIDS 4.0—C-37

The smid service is responsible for enabling alarm forwarding and interacting between the management interfaces. Director forwarding settings are written to the smid.conf file. The service status file is error.smid.



Alarm Forwarding

```
DupDestination <hostname>.<organization
 name> <service name> <message level>
 <message type>[,<message type>…]
```

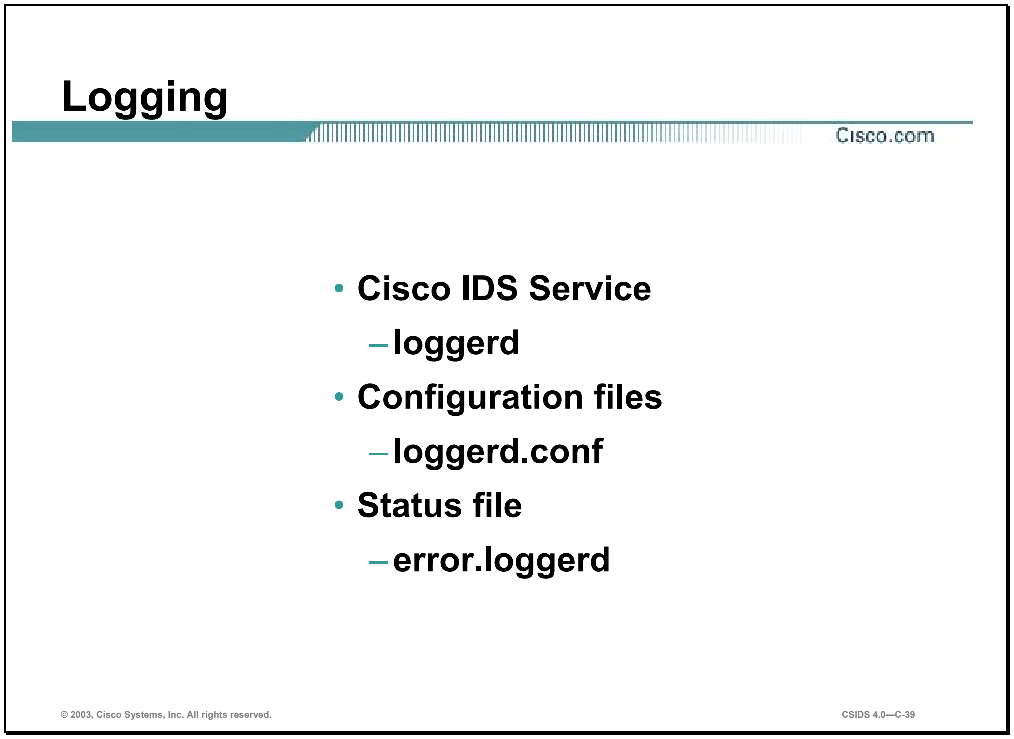
- **Defines settings for alarm forwarding**

```
DupDestination director2.training smid 3
 EVENTS
```

The following are the tokens in the smid.conf associated with the alarm-forwarding feature:

DupDestination <host name>.<organization name><service name> <message level> <message type>, [<message type>…]

Host Name	The Cisco IDS hostname of the IDS device (Director or Sensor) that will receive the forwarded message.
Organization Name	The Cisco IDS organization name of the IDS device (Director or Sensor) that will receive the forwarded message.
Service Name	The name of the service to which the messages are sent. The possible services are as follows: ■ smid ■ loggerd ■ eventd
Message level	The minimum severity level that an event must have to be forwarded. Values are 1,3, or 5 (Low, Medium, High).
Message type	Identifies the following types of messages to be forwarded: ■ ERRORS—All error messages from any Cisco IDS service. ■ COMMANDS—All command messages from any Cisco IDS service to any Cisco IDS service. ■ EVENTS—All alarms from packetd. ■ IPLOGS—All captured session data from packetd.



Logging

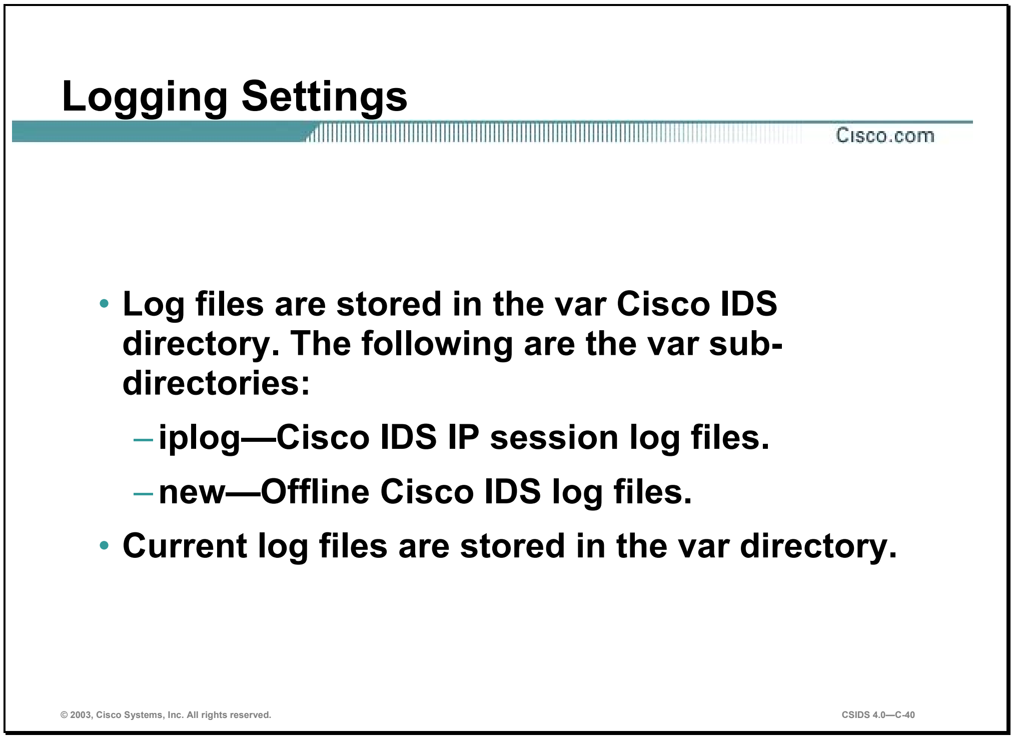
Cisco.com

- Cisco IDS Service
  - loggerd
- Configuration files
  - loggerd.conf
- Status file
  - error.loggerd

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-39

The loggerd service is responsible for performing logging functions on the Cisco IDS components. The logging settings are written to the loggerd.conf file. The service status is error.loggerd.



Logging Settings

- Log files are stored in the var Cisco IDS directory. The following are the var sub-directories:
  - iplog—Cisco IDS IP session log files.
  - new—Offline Cisco IDS log files.
- Current log files are stored in the var directory.

CSIDS 4.0—C-40

The Cisco IDS log files are stored in the var directory within the Cisco IDS sub-directory. For example, on a 4210 Sensor the log files are stored in /usr/nr/var. The Cisco IDS maintains sub-directories for the different types of possible log files. The following are the sub-directories:

- iplog—This directory stores IP session log files.
- new—This directory stores archived Cisco IDS log files.

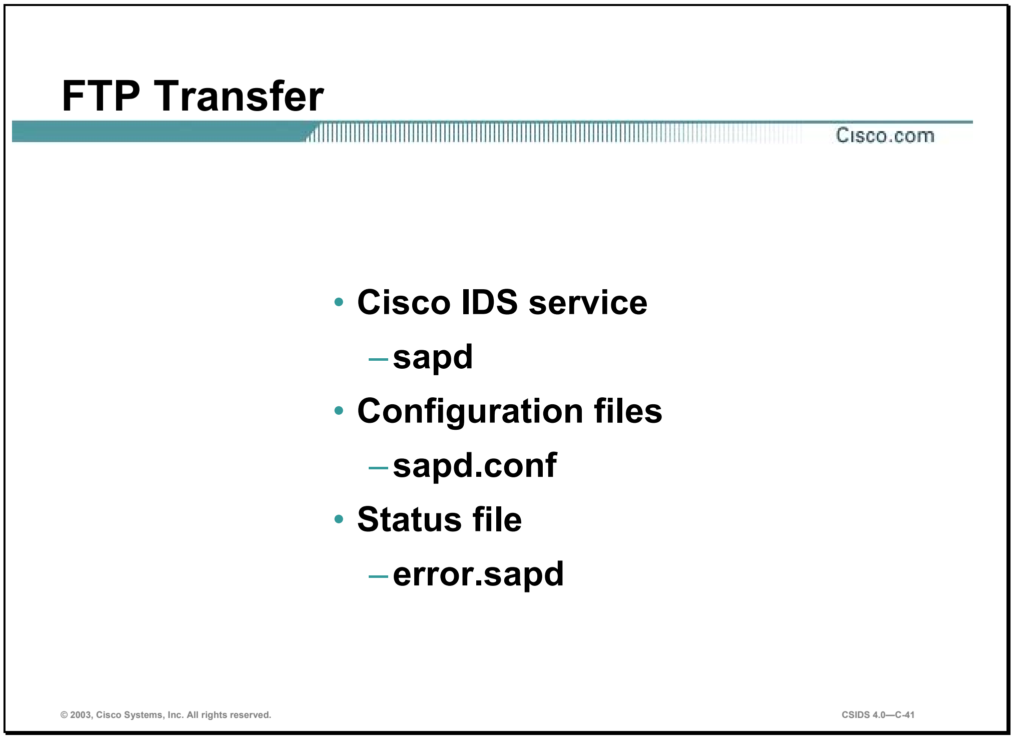
Note The IP log directory has a separate new directory for archived IP log files.

Refer to *Appendix C* for information on the Cisco IDS log files.

The active Cisco IDS log file is located in /usr/nr/var. The IP log files are located in the /usr/nr/var/iplog directory. Each Cisco IDS service maintains its own error log file and is located in /usr/nr/var. The active log files are closed and archived, and a new active log file is created when the file size or time thresholds are exceeded. By default, log files will be archived and a new one is created when the active log file reaches 1 GB or after 60 minutes have past, which ever comes first. By default, IP log files will remain active for 15 minutes or until the session that triggered the IP log action is terminated. Archived log files are located in the /usr/nr/var/new directory or the Cisco IDS log and error log files. They can also be found in the /usr/nr/var/iplog/new directory for IP session log files.

The following table contains the Cisco IDS log file naming convention:

IP log file	iplog.XXX.XXX.XXX.XXX.YYYYMMDDHHMM ■ iplog—Keyword identifying the file as a Cisco IDS IP log session file ■ XXX.XXX.XXX—The IP address of the attacking host ■ YYYY—Year the file was created ■ MM—Month the file was created ■ DD—Day the file was created ■ HH—Hour the file was created ■ MM—Minute of the hour the file was created
Cisco IDS log file	log.*YYYYMMDDHHMM* ■ log—Keyword identifying the file as a Cisco IDS log file ■ XXX.XXX.XXX—The IP address of the attacking host ■ YYYY—Year the file was created ■ MM—Month the file was created ■ DD—Day the file was created ■ HH—Hour the file was created ■ MM—Minute of the hour the file was created
Service Error log file	error.service.processid ■ error—Keyword identifying it as a Cisco IDS service log file ■ service—Cisco IDS service name ■ processid—Numeric value of the service process identification number

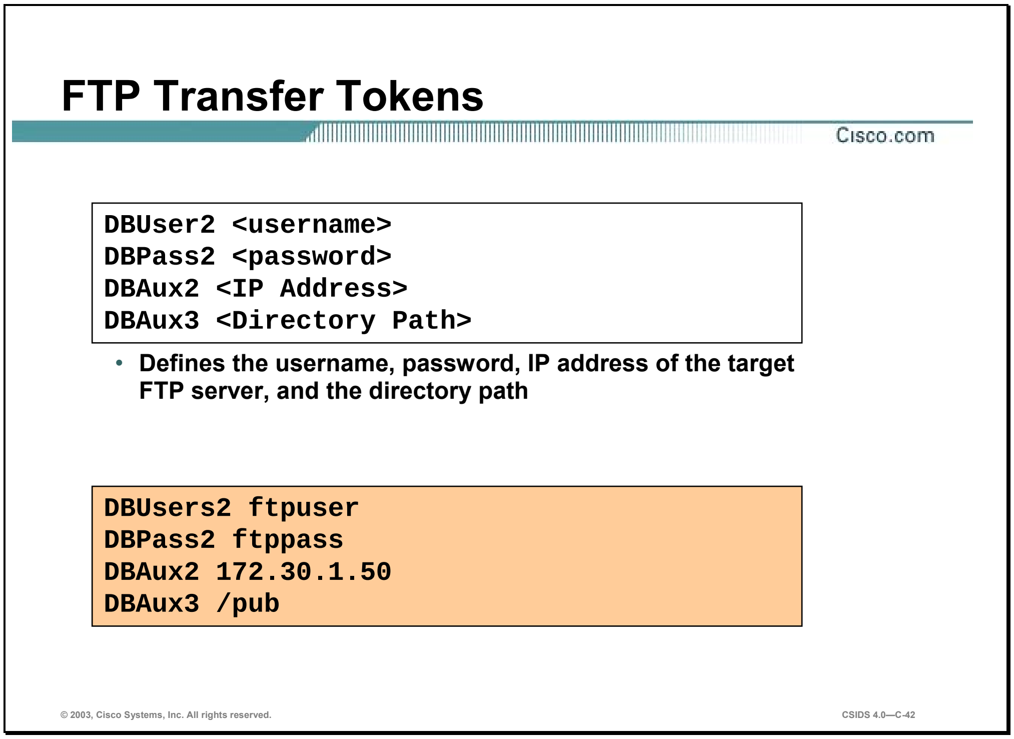


FTP Transfer

- Cisco IDS service
  - sapd
- Configuration files
  - sapd.conf
- Status file
  - error.sapd

CSIDS 4.0—C-41

The sapd service is responsible for performing database functions and offline log file transfers. The FTP transfer settings are written to the sapd.conf file. The service status file is error.sapd.



FTP Transfer Tokens

```
DBUser2 <username>
DBPass2 <password>
DBAux2 <IP Address>
DBAux3 <Directory Path>
```

- Defines the username, password, IP address of the target FTP server, and the directory path

```
DBUsers2 ftpuser
DBPass2 ftppass
DBAux2 172.30.1.50
DBAux3 /pub
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-42

The following are the tokens in sapd.conf associated with the FTP transfer of Sensor log files:

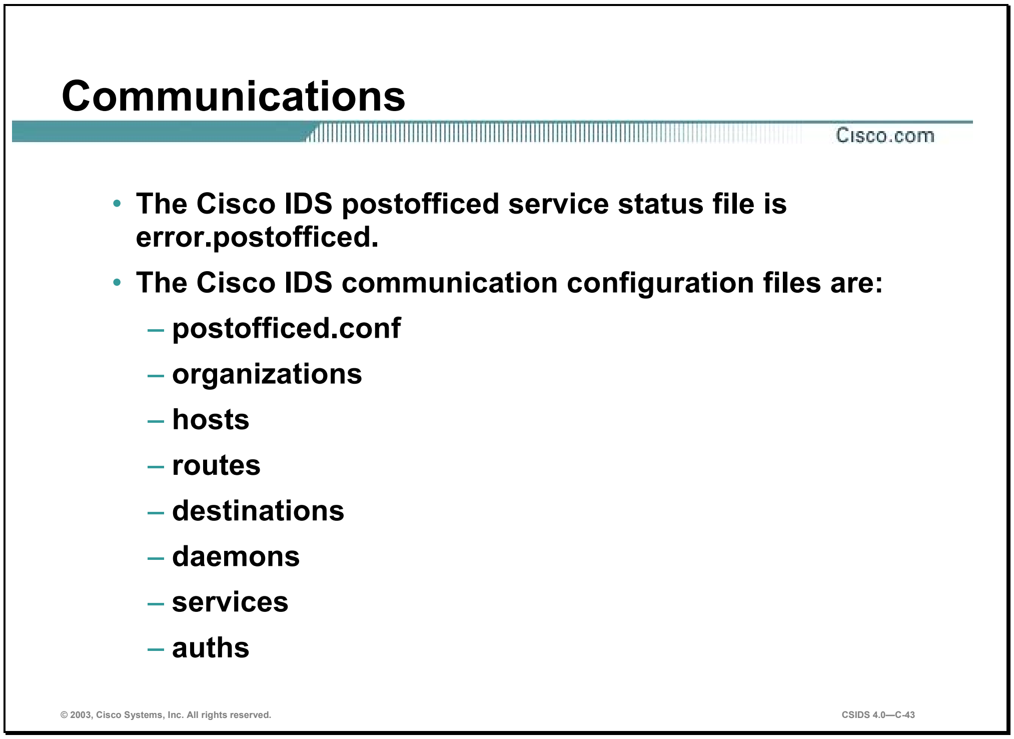
DBUser2 <Username>

DBPass2 <Password>

DBAux2 <IP Address>

DB Aux3 <Directory Path>

Username	Username for the account that will be used to log in to the FTP server.
Password	Password for the account that will be used to log in to the FTP server.
IP Address	IP address of the target FTP server.
Path	Directory path where the log files will be written. The directory must have write permission for the specified username.



Communications

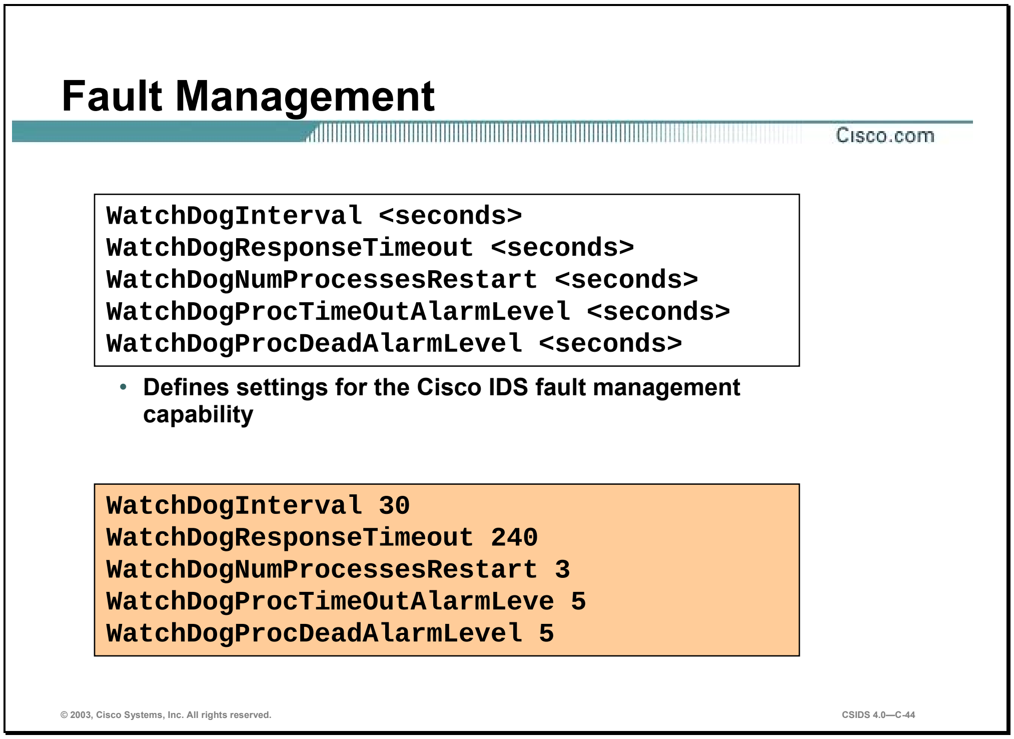
- The Cisco IDS postofficed service status file is error.postofficed.
- The Cisco IDS communication configuration files are:
  - postofficed.conf
  - organizations
  - hosts
  - routes
  - destinations
  - daemons
  - services
  - auths

CSIDS 4.0—C-43

The Cisco IDS communication configuration settings are written to the following files:

- postofficed.conf
- organizations
- hosts
- routes
- destinations
- daemons
- services
- auths

The postofficed service status file is error.postofficed.



Fault Management

Cisco.com

```
WatchDogInterval <seconds>
WatchDogResponseTimeout <seconds>
WatchDogNumProcessesRestart <seconds>
WatchDogProcTimeOutAlarmLevel <seconds>
WatchDogProcDeadAlarmLevel <seconds>
```

- **Defines settings for the Cisco IDS fault management capability**

```
WatchDogInterval 30
WatchDogResponseTimeout 240
WatchDogNumProcessesRestart 3
WatchDogProcTimeOutAlarmLeve 5
WatchDogProcDeadAlarmLevel 5
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-44

The following are the tokens in postofficed.conf associated with fault management:

WatchDogInterval <Num of Seconds>

Num of Seconds	Number of seconds between postofficed's regular status queries of the services running on the specific device

WatchDogResponseTimeOut <Num of Seconds>

Num of Seconds	Number of seconds that must pass without a given Cisco IDS service response before declaring the Cisco IDS service to be down

WatchDogNumProcessRestarts <Num of Tries>

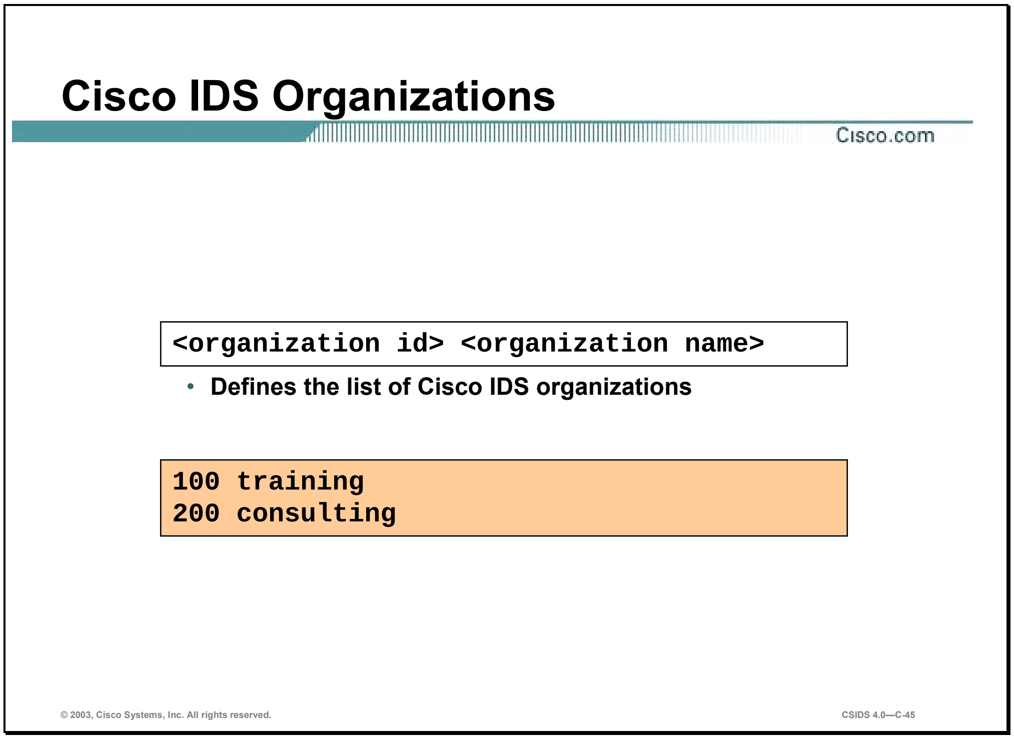
Num of Tries	The number of times that postofficed will try to restart a downed Cisco IDS service before declaring it to be down

WatchDogProcTimeOutAlarmLevel <Severity>

Severity	The severity level of the alarm that is generated when postofficed concludes that a Cisco IDS service is down

WatchDogProcDeadAlarmLevel <Severity>

Severity	The severity level of the alarm that is generated when postofficed concludes that a Cisco IDS service cannot be started



Cisco IDS Organizations

```
<organization id> <organization name>
```

- **Defines the list of Cisco IDS organizations**

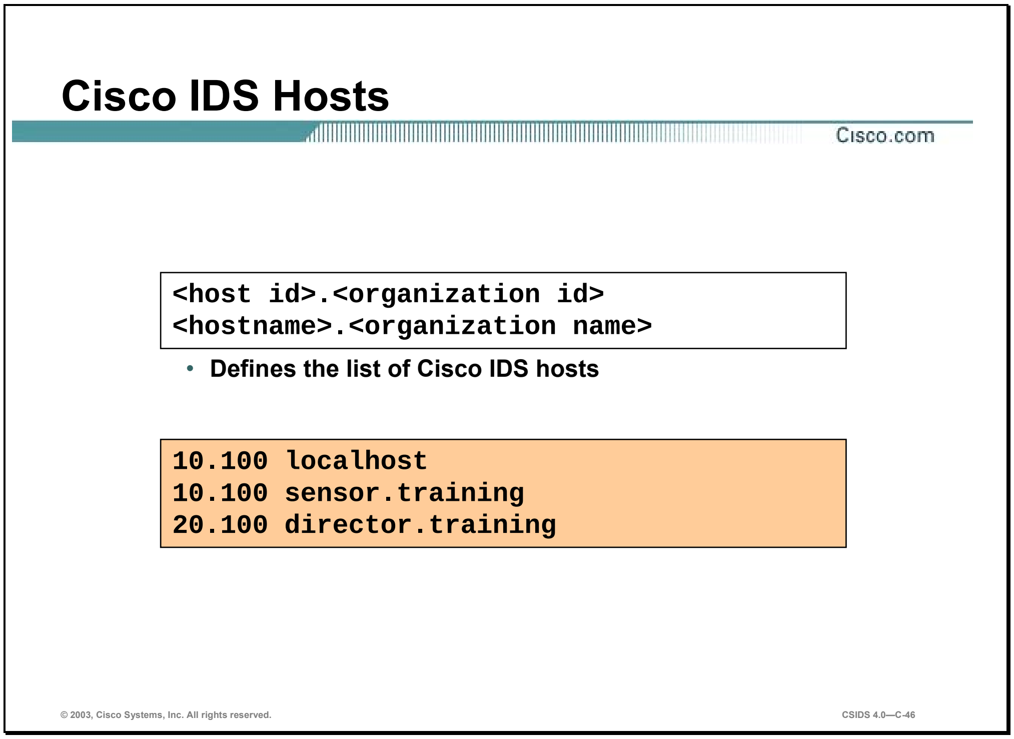
```
100 training
200 consulting
```

CSIDS 4.0—C-45

The organizations file contains PostOffice organization identifications and names. The following is the entry format for the organizations file:

<Organization ID> <Organization Name>

Organization ID	Numeric identification for a Cisco IDS organization (1–65535)
Organization Name	Alphanumeric identification associated with a Cisco IDS organization



Cisco IDS Hosts

Cisco.com

```
<host id>.<organization id>
<hostname>.<organization name>
```

- **Defines the list of Cisco IDS hosts**

```
10.100 localhost
10.100 sensor.training
20.100 director.training
```

© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-46

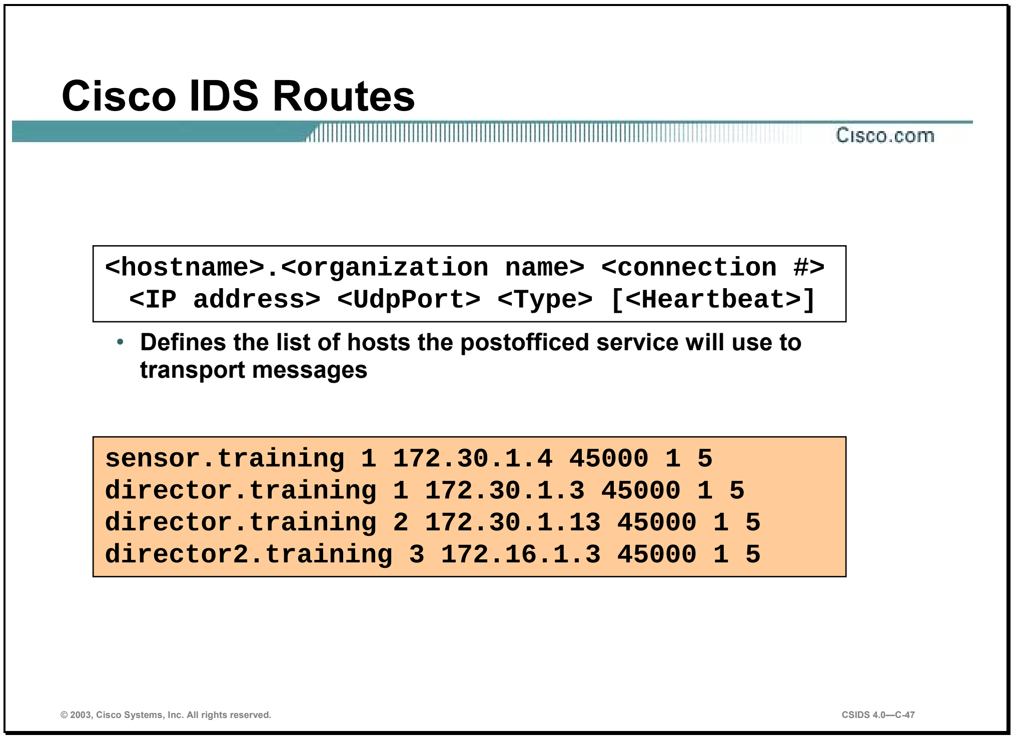
This file is much like a UNIX /etc/hosts file. In UNIX, each machine is identified by both an IP address and name. The Cisco IDS uses a more complex addressing scheme that allows for more unique addresses than the standard IP system. It enumerates the organizations and hosts that are recognized by a given Sensor or Director system in a Cisco IDS configuration. Each entry has the following form:

<host ID>.<organization ID> <host name>.<organization name>

host ID	Numeric identification for the Cisco IDS host (1–65535)
organization ID	Numeric identification for the Cisco IDS organization (1–65535)
host Name	Alphanumeric identification associated with a Cisco IDS host
organization Name	Alphanumeric identification associated with a Cisco IDS organization

Note The period between the host identification and organization identification, and the hostname and organization name is required. The exception is the localhost entry.

The combination of the host identification and organization identification must form a unique identifier throughout your entire network of Sensors and Directors. The organization identification and name must be the same in all configuration files. This file must have localhost as the first entry. The localhost must have the same host identification and organization identification as the host in which the file is maintained. On the Sensor, you should have a minimum of three entries: Localhost, Sensor, and Director. On the Director, you will have all the Sensors and Directors listed.



Cisco IDS Routes

```
<hostname>.<organization name> <connection #>
  <IP address> <UdpPort> <Type> [<Heartbeat>]
```

- Defines the list of hosts the postofficed service will use to transport messages

```
sensor.training 1 172.30.1.4 45000 1 5
director.training 1 172.30.1.3 45000 1 5
director.training 2 172.30.1.13 45000 1 5
director2.training 3 172.16.1.3 45000 1 5
```

CSIDS 4.0—C-47

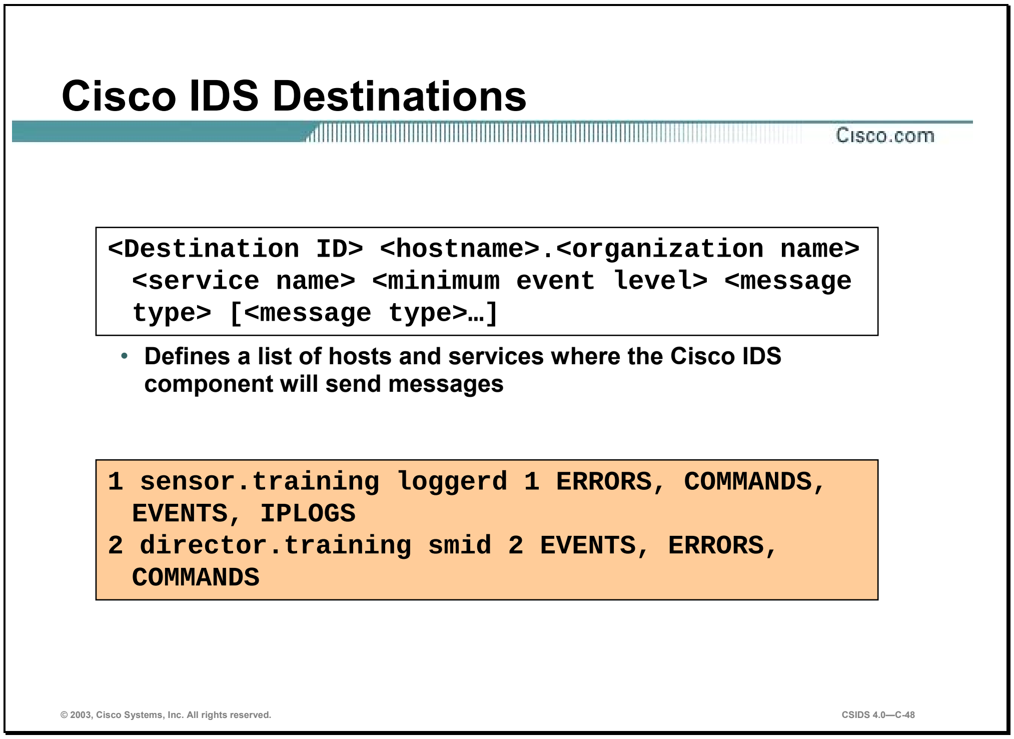
The routes file allows you to set the IP address associated with the Cisco IDS hosts. For fault-tolerance, multiple IP addresses may be defined for a single host. These multiple addresses are then used as alternate IP addresses in the event the primary IP address is not responding.

The IP address for each machine known to the host is searched for by postofficed. This file identifies the actual IP routes that postofficed uses to send messages between different hosts. The following is the entry format for the routes file:

<hostname>.<organization name> <connection #><IP address><UDP port><Type> [<Heartbeat>]

Hostname	The Cisco IDS name of the host to which messages are routed. It must already be defined in the hosts file.
Organization Name	Alphanumeric identification associated with the Cisco IDS organization.
Connection #	The numerical order in which you want the path to this machine to be tried. A lower the number, the higher the route priority. The higher number acts as a backup route in case the primary route goes down.
IP address	Identifies the IP address of the Cisco IDS device to receive the message.
UDP port	Identifies the UDP port communication services that are routed through on each host. The default setting is 45000.
Type	Identifies the connection type and is currently not used.
Heartbeat	(Optional.) The number of seconds before the route is considered down.

In the figure, the Sensor is routing to two different Directors and has a backup route for one of the Directors. Route 1 will be used to communicate with director.training at IP address 172.30.1.3 until there is a connection problem detected. As soon as the Cisco IDS detects a problem with the primary route, it automatically switches to the backup route, while at that same time trying to reestablish the primary route. The Cisco IDS automatically reverts to the primary route when the connection is re-established.



Cisco IDS Destinations

Cisco.com

```
<Destination ID> <hostname>.<organization name>
  <service name> <minimum event level> <message
  type> [<message type>…]
```

- **Defines a list of hosts and services where the Cisco IDS component will send messages**

```
1 sensor.training loggerd 1 ERRORS, COMMANDS,
  EVENTS, IPLOGS
2 director.training smid 2 EVENTS, ERRORS,
  COMMANDS
```

CSIDS 4.0—C-48

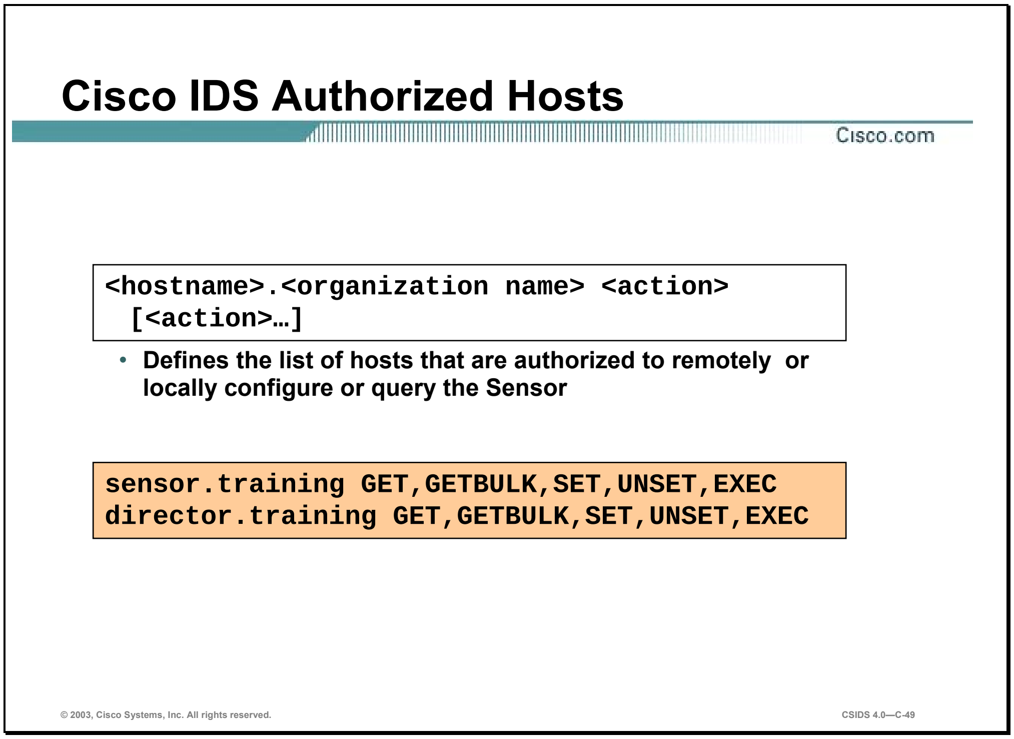
The destinations file enables you to add additional destinations to send events generated by the Cisco IDS. The routing of the messages to any other host registered in the hosts file is handled by postofficed. The destinations file identifies the severity of the messages and the type of messages that are routed to a given application on a given host. The three services that postofficed can forward messages to are loggerd, smid, and eventd. A given postofficed service may forward messages to a maximum of 32 destinations. The following is the entry format for the destinations file:

<Destination ID> <host name>.<organization name> <service name> <message level> <message type>

Destination ID	A numeric identification (1–32) for each destination.
Host Name	The Cisco IDS name of the host to send the messages. It must already be defined in the hosts file.
Organization Name	Alphanumeric identification associated with the Cisco IDS organization.
Service name	The name of the Cisco IDS service to send the messages. The possible services are as follows: ■ smid ■ loggerd ■ eventd
Message level	The minimum severity level that an event must have in order to be forwarded. Values are 1,3, or 5 (Low, Medium, High).

Message type	Identifies the following types of messages to be forwarded: ■ ERRORS—All error messages from any Cisco IDS service ■ COMMANDS—All command messages from any Cisco IDS service to any Cisco IDS service ■ EVENTS—All alarms from packetd ■ IPLOGS—All captured session data from packetd

In the example destinations file, all errors, commands, events, and IP logs destined to the loggerd service are sent to the loggerd service on the Sensor, sensor.training. All errors, commands, and events, with a level of 2 or higher are forwarded to the smid service on the Director, director.training.



Cisco IDS Authorized Hosts

```
<hostname>.<organization name> <action>
  [<action>…]
```

- **Defines the list of hosts that are authorized to remotely or locally configure or query the Sensor**

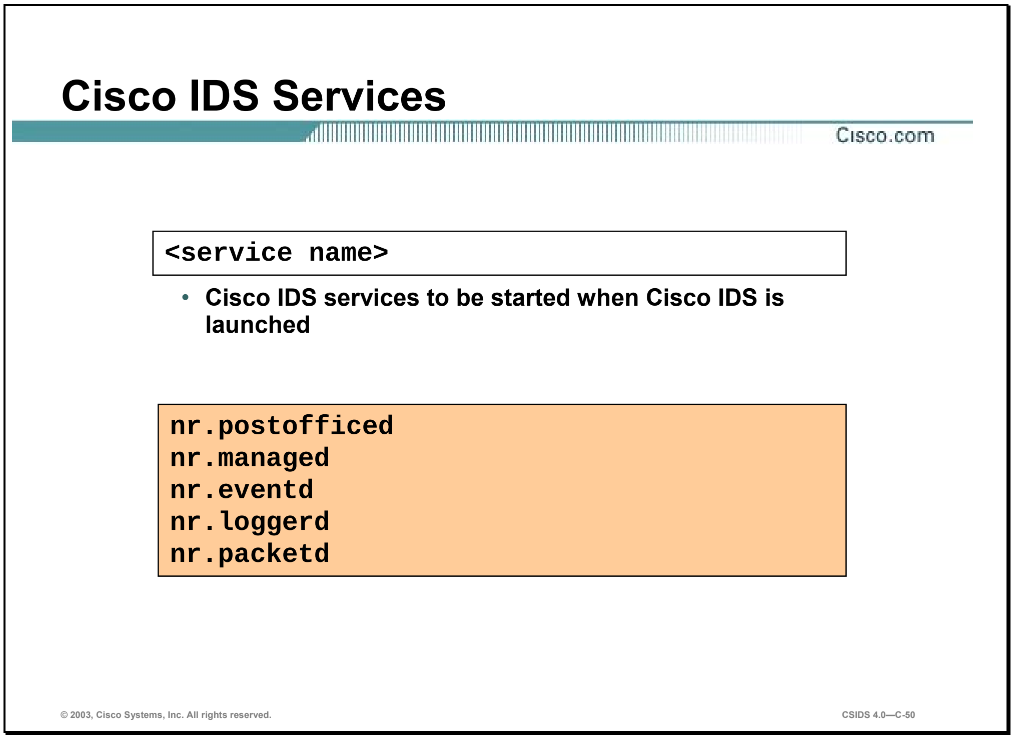
```
sensor.training GET,GETBULK,SET,UNSET,EXEC
director.training GET,GETBULK,SET,UNSET,EXEC
```

CSIDS 4.0—C-49

The auths file enables you to set appropriate permissions for other Cisco IDS components to remotely query and configure the current Cisco IDS component, Sensor or Director. The following is the entry format in the auths files:

<Host Name>.<Organization Name> <action>[,<action>…]

Host Name	The Cisco IDS host name of the Cisco IDS component being granted the permissions
Organization Name	The Cisco IDS organization name of the Cisco IDS component being granted the permissions
Action	Actions allowed from defined host are as follows: ■ GET—Allows access to single pieces of information at a time ■ GETBULK—Allows access to multiple pieces of information at a time ■ SET— Allows the remote host to set local attributes ■ UNSET— Allows the remote host to unset local attributes ■ EXEC— Allows the remote host to execute the Cisco IDS commands



Cisco IDS Services

Cisco.com

```
<service name>
```

- Cisco IDS services to be started when Cisco IDS is launched

```
nr.postofficed
nr.managed
nr.eventd
nr.loggerd
nr.packetd
```

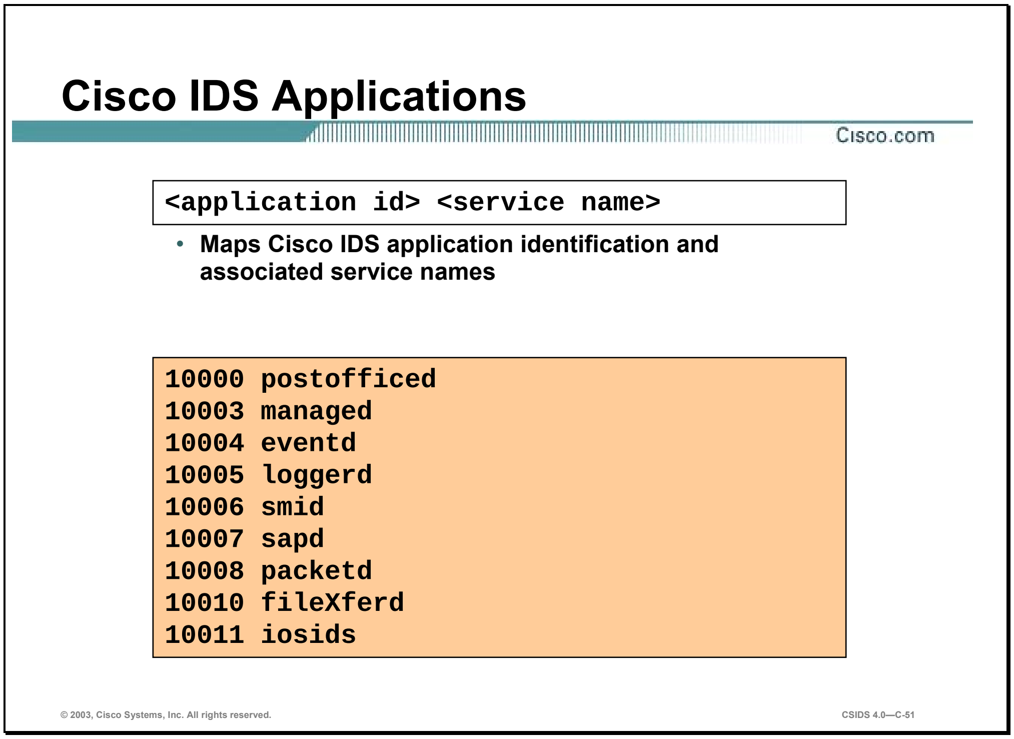
© 2003, Cisco Systems, Inc. All rights reserved.

CSIDS 4.0—C-50

The daemons file enables you to define which Cisco IDS services are started every time the Cisco IDS is launched. The following is the entry format in the daemons file:

<service name>

Service Name	The name of the daemon to be started every time the Cisco IDS is started. Service names can be one or more of the following: ■ postofficed ■ loggerd ■ sapd ■ packetd ■ fileXferd ■ managed ■ smid



Cisco IDS Applications

Cisco.com

```
<application id> <service name>
```

- **Maps Cisco IDS application identification and associated service names**

```
10000 postofficed
10003 managed
10004 eventd
10005 loggerd
10006 smid
10007 sapd
10008 packetd
10010 fileXferd
10011 iosids
```

CSIDS 4.0—C-51

The following is the entry format in the services file that defines the application ID for each Cisco IDS service:

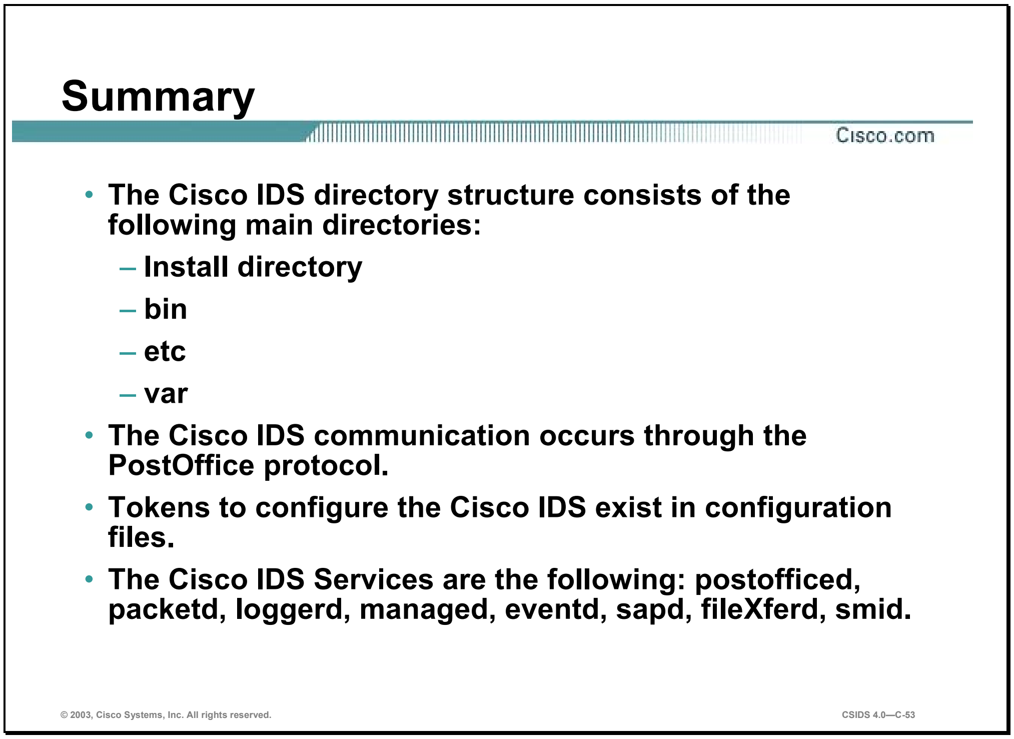
<Application ID> <Service Name>

Application ID	Numeric identification assigned to the Cisco IDS daemon.
Service Name	Name of the Cisco IDS daemon whose application identification is being set. The Cisco IDS application IDs and associated service names are as follows: ■ 10000—postofficed ■ 10003—managed ■ 10004—eventd ■ 10005—loggerd ■ 10006—smid ■ 10007—sapd ■ 10008—packetd ■ 10010—fileXferd ■ 10011—iosids

Warning Entries in the *services* file should never be changed. Changing entries could cause the Cisco IDS not to function properly.

Summary

This section summarizes what you learned in this chapter.



Summary

Cisco.com

- The Cisco IDS directory structure consists of the following main directories:
  - Install directory
  - bin
  - etc
  - var
- The Cisco IDS communication occurs through the PostOffice protocol.
- Tokens to configure the Cisco IDS exist in configuration files.
- The Cisco IDS Services are the following: postofficed, packetd, loggerd, managed, eventd, sapd, fileXferd, smid.

CSIDS 4.0—C-53