

CSIDS

Cisco Secure Intrusion Detection System

Version 4.1

Student Guide

Copyright © 2004, Cisco Systems, Inc. All rights reserved.

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 • Cyprus • 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



Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, iQ logo, the iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 1

Course Introduction	1-1
Overview	1-1
Course Objectives	1-2
Lab Topology Overview	1-8
Security Fundamentals	2-1
Overview	2-1
Objectives	2-2
Need for Network Security	2-3
Network Security Policy	2-10
Primary Network Threats and Attacks	2-13
Reconnaissance Attacks and Mitigation	2-16
Access Attacks and Mitigation	2-23
Denial of Service Attacks and Mitigation	2-31
Worm, Virus, and Trojan Horse Attacks and Mitigation	2-36
Management Protocols and Functions	2-43
Summary	2-48
Intrusion Detection Overview	3-1
Overview	3-1
Objectives	3-2
Intrusion Detection Terminology	3-4
Intrusion Detection Technologies	3-8
Network-Based Intrusion Detection Systems	3-12
Host-Based Intrusion Prevention System	3-15
Intrusion Protection Benefits	3-17
Network Sensor Platforms	3-21
Host-based Intrusion Protection System	3-28
Sensor Appliances	3-33
Deploying Cisco IDS	3-42
Summary	3-47
Cisco Intrusion Detection System Architecture	4-1
Overview	4-1
Objectives	4-2
Cisco IDS Software Architecture	4-3
Cisco IDS Communication	4-6
User Accounts and Roles	4-11
Summary	4-14
Getting Started with the IDS Command Line Interface	5-1
Overview	5-1
Objectives	5-2
Sensor Installation	5-3
Sensor Initialization	5-12
Command Line Modes	5-17
Completing the Initial Configuration	5-34
Preventive Maintenance and Troubleshooting	5-45
Summary	5-65
Sensor Management and Monitoring	6-1
Objectives	6-2
IDS Device Manager Overview	6-3
IDS Event Viewer Overview	6-8
IDS Event Viewer Installation	6-10

IDS Event Viewer Views	6-14
IDS Event Viewer Filters	6-22
Network Security Database	6-30
Summary	6-35
Using the Intrusion Detection System Device Manager to Configure the Sensor	7-1
Overview	7-1
Objectives	7-2
Configuring Basic Sensor Settings	7-3
Configuring SSH Communications	7-18
Configuring TLS Communications	7-23
Configuring Monitoring	7-30
Viewing Diagnostics and System Information	7-33
Summary	7-37
Cisco Intrusion Detection System Alarms and Signatures	8-1
Overview	8-1
Objectives	8-2
Cisco IDS Signatures	8-3
Cisco IDS Alarms	8-10
Cisco IDS Signature Engines	8-12
Atomic Signature Engines	8-27
Flood Signature Engines	8-36
Service Signature Engines	8-40
State Signature Engines	8-55
String Signature Engines	8-60
Sweep Signature Engines	8-62
Miscellaneous Signature Engines	8-71
Summary	8-75
Signature Configuration	9-1
Overview	9-1
Objectives	9-2
Signature Configuration	9-3
Signature Tuning	9-14
Custom Signatures	9-20
Custom Signature Scenarios	9-43
Summary	9-70

Table of Contents

Volume 2

Sensor Tuning	10-1
Overview	10-1
Objectives	10-2
Intrusion Detection Evasive Techniques	10-3
Tuning the Sensor	10-8
Logging	10-16
Reassembly Options	10-25
Alarm Channel System Variables	10-29
Alarm Channel Event Filtering	10-33
Summary	10-41
Blocking Configuration	11-1
Overview	11-1
Objectives	11-2
Introduction	11-3
ACL Considerations	11-12
Blocking Sensor Configuration	11-16
Master Blocking Sensor Configuration	11-30
Summary	11-35
Cisco Intrusion Detection System Maintenance	12-1
Overview	12-1
Objectives	12-2
Service Pack and Signature Updates	12-3
Image Recovery	12-13
Resetting, Powering Down, and Restoring the Default Configuration	12-17
Time Settings	12-19
Summary	12-23
Enterprise Intrusion Detection System Management	13-1
Overview	13-1
Objectives	13-2
Introduction	13-3
Windows Installation	13-6
Solaris Installation	13-14
Architecture	13-20
Getting Started with the IDS MC	13-23
Sensors and Sensor Groups	13-29
Using the IDS MC to Configure the Sensor	13-36
IDS MC Workflow	13-42
Updating the IDS MC	13-52
Reporting	13-56
Summary	13-60
Enterprise Intrusion Detection System Monitoring and Reporting	14-1
Overview	14-1
Objectives	14-2
Introduction	14-3
Installation	14-5
Getting Started	14-12
Monitoring	14-19
Customizing the Event Viewer	14-24
Reporting	14-34
Administration	14-38

Cisco Threat Response	14-52
Summary	14-58
Cisco Intrusion Detection System Network Module	15-1
Overview	15-1
Objectives	15-2
NM-CIDS Overview	15-3
How the NM-CIDS Works	15-7
Design Considerations	15-11
Installation and Configuration Tasks	15-20
Maintenance Tasks Unique to the NM-CIDS	15-46
Summary	15-62
Intrusion Detection System Module Configuration	16-1
Overview	16-1
Objectives	16-2
Introduction	16-3
Ports and Traffic	16-8
Initialization	16-11
Verifying IDSM-2 Status	16-15
Summary	16-17
Capturing Network Traffic for Intrusion Detection Systems	17-1
Overview	17-1
Objectives	17-2
Traffic Capture Overview	17-3
Configuring SPAN for Catalyst 4500 and 6500 Traffic Capture	17-12
Configuring RSPAN for Catalyst 4500 and 6500 Traffic Capture	17-16
Configuring VACLs for Catalyst 6500 Traffic Capture	17-26
Using the mls ip ids Command for Catalyst 6500 Traffic Capture	17-39
Advanced Catalyst 6500 Traffic Capture	17-45
Summary	17-54

Course Introduction

Overview

This lesson 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 topic 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.
- Describe the Cisco IDS signatures and determine the immediate threat posed to the network.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-1-3

Course Objectives (Cont.)

Cisco.com

- Describe the Cisco IDS signature engines and engine parameters.
- Tune Cisco IDS signatures to work optimally in unique network environments.
- 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-1-4

Course Objectives (Cont.)

Cisco.com

- **Perform maintenance operations such as signature and service pack upgrades.**
- **Describe the Cisco IDS architecture.**
- **Manage a large scale deployment of Cisco IDS Sensors with management and monitoring software.**
- **Install and configure Cisco IDS Sensors including the following:**
 - **A network appliance**
 - **A Network Module for Cisco 2600, 3600, and 3700 routers**
 - **An Intrusion Detection System Module 2**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-5

Course Agenda

Cisco.com

Day 1

- Lesson 1—Course Introduction
- Lesson 2—Security Fundamentals
- Lesson 3—Intrusion Detection Overview
- Lunch
- Lesson 4—Cisco Intrusion Detection System Architecture
- Lesson 5—Getting Started with the IDS Command Line Interface

Day 2

- Lesson 6—Sensor Management and Monitoring
- Lesson 7—Using the Intrusion Detection System Device Manager to Configure the Sensor
- Lunch
- Lesson 8—Cisco Intrusion Detection System Alarms and Signatures
- Lesson 9—Signature Configuration

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-6

Course Agenda (Cont.)

Cisco.com

Day 3

- Lesson 10—Sensor Tuning
- Lesson 11—Blocking Configuration
- Lunch
- Lesson 12—Cisco Intrusion Detection System Maintenance
- Lesson 13—Enterprise Intrusion Detection System Management

Day 4

- Lesson 14—Enterprise IDS Monitoring and Reporting
- Lesson 15—Cisco Intrusion Detection System Network Module
- Lunch
- Lesson 16—Intrusion Detection System Module Configuration
- Lesson 17—Capturing Network Traffic for Intrusion Detection Systems

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-7

Participant Responsibilities

Cisco.com

Student responsibilities

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-8

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-9

Graphic Symbols

Cisco.com



IOS Router



PIX Firewall



VPN 3000



IDS Sensor



Catalyst 6500
w/ IDS Module 2



IOS Router
w/IDS Network
Module



Network
Access Server



Policy Manager



CA
Server



PC



Laptop



Server
Web, FTP, etc.



Hub



Modem



Ethernet Link



VPN Tunnel



Network
Cloud

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-10

Participant Introductions

Cisco.com

- **Your name**
- **Your company**
- **Prerequisite skills**
- **Brief history**
- **Objective**



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-11

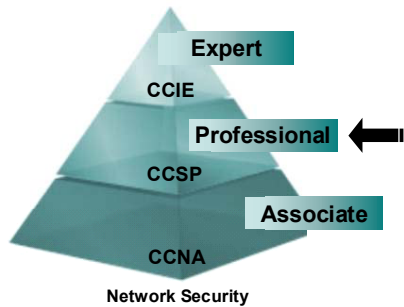
Cisco Security Career Certifications

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



Required Exam	Recommended Training through Cisco Learning Partners
642-501	Securing Cisco IOS Networks
642-511	Cisco Secure Virtual Private Networks
642-531	Cisco Secure Intrusion Detection System
642-521	Cisco Secure PIX Firewall Advanced
642-541	Cisco SAFE Implementation

www.cisco.com/go/securitytraining

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-12

Cisco Security Career Certifications (Cont.)

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	
642-501	Securing Cisco IOS Networks
642-521	Cisco Secure PIX Firewall Advanced

Cisco VPN Specialist



Required Exam	Recommended Training through Cisco Learning Partners
Pre-requisite: Valid CCNA certification	
642-501	Securing Cisco IOS Networks
642-511	Cisco Secure Virtual Private Networks

Cisco IDS Specialist



Required Exam	Recommended Training through Cisco Learning Partners
Pre-requisite: Valid CCNA certification	
642-501	Securing Cisco IOS Networks
642-531	Cisco Secure Intrusion Detection System

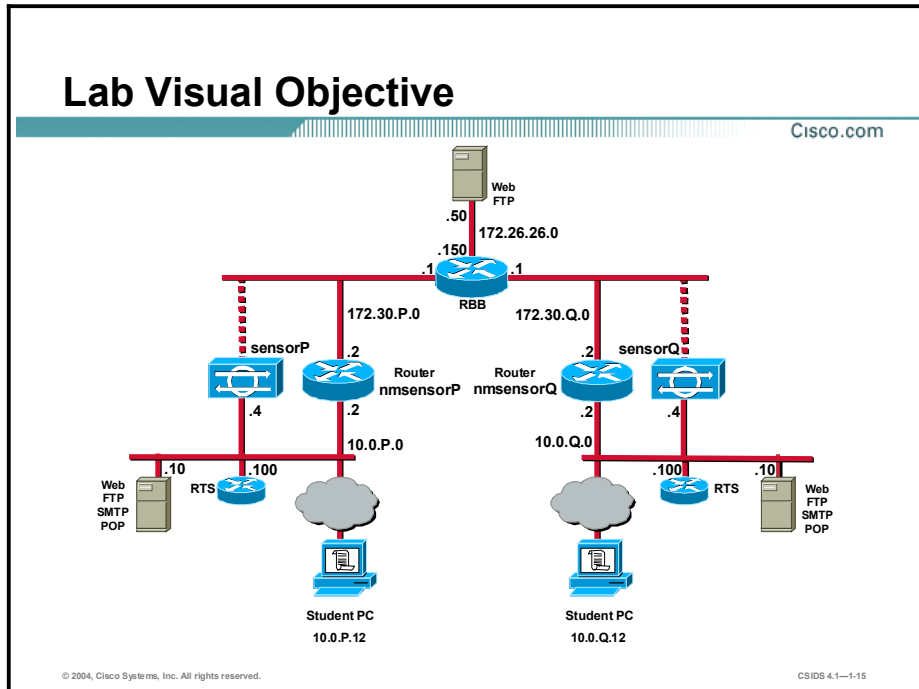
www.cisco.com/go/securitytraining

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—1-13

Lab Topology Overview

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



Each pair of students will be assigned a pod. Some lab exercises require connectivity between your pod, pod P, and your assigned peer pod, pod Q. Other lab exercises require connectivity between your pod, pod P, and your assigned secondary peer pod, pod S.

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

Security Fundamentals

Overview

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

- Objectives
- Need for network security
- Network security policy
- Primary network threats and attacks
- Reconnaissance attacks and mitigation
- Access attacks and mitigation
- Denial of service attacks and mitigation
- Worm, virus, and Trojan horse attacks and mitigation
- Management protocols and functions
- Summary

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

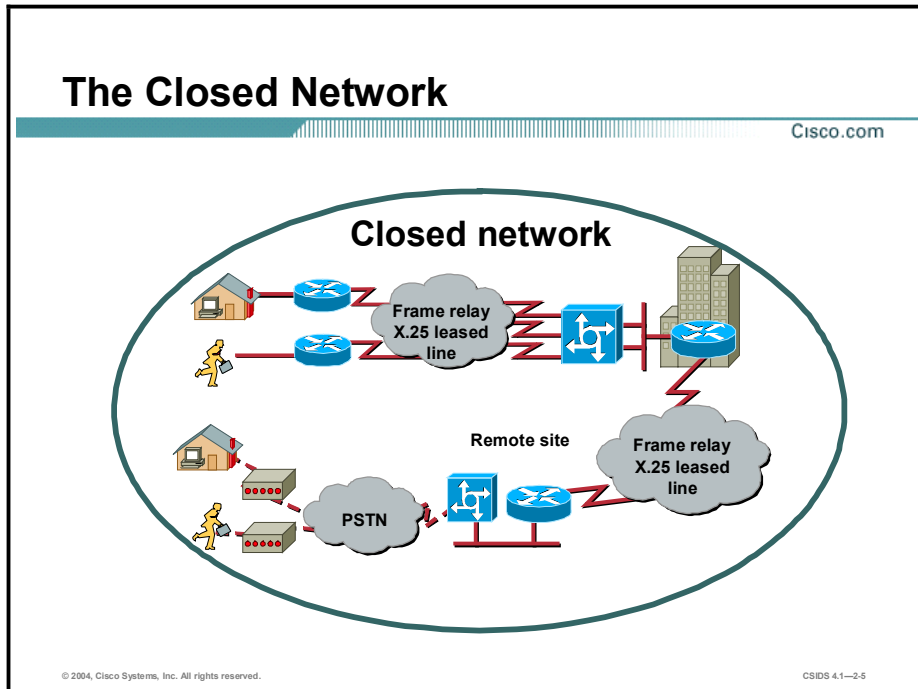
- Describe the need for network security.
- Identify the components of a complete security policy.
- Explain security as an ongoing process.
- Describe the four types of security threats.
- Describe the four primary attack categories.
- Describe the types of attacks associated with each primary attack category and their mitigation methods.
- Describe the configuration management and management protocols and the recommendations for securing them.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1--2.3

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.

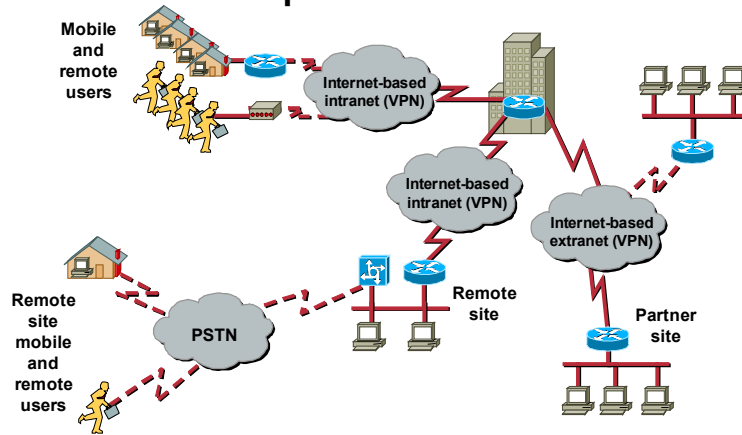


The closed network typically consists of a network designed and implemented in a corporate environment, and it provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because there was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

The Network Today

Cisco.com

Open network



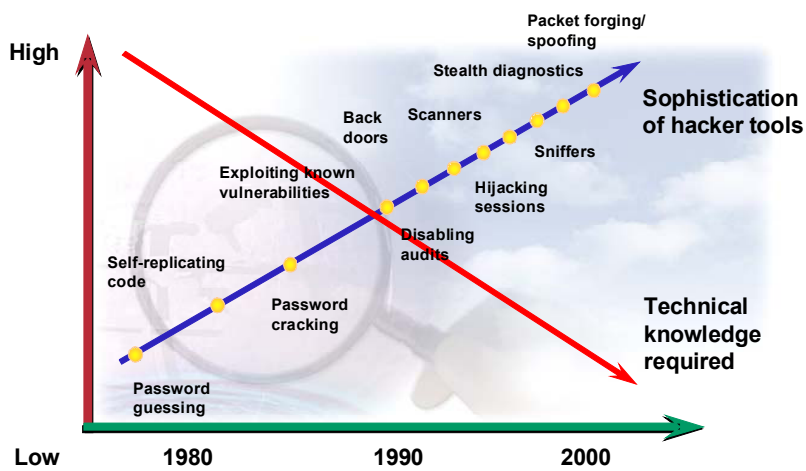
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-2.6

The 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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.7

With the development of large open networks there has been a huge increase in security threats in the past 20 years. Not only have hackers discovered more vulnerabilities, but the tools used to hack a network have become simpler and the technical knowledge required has decreased. There are downloadable applications available that require little or no hacking knowledge to implement. There are also applications intended for troubleshooting a network that when used improperly can pose severe threats.

The Role of Security Is Changing

Cisco.com

As businesses become more open to supporting Internet-powered initiatives such as e-commerce, customer care, supply-chain management, and extranet collaboration, network security risks are also increasing.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1--2.8

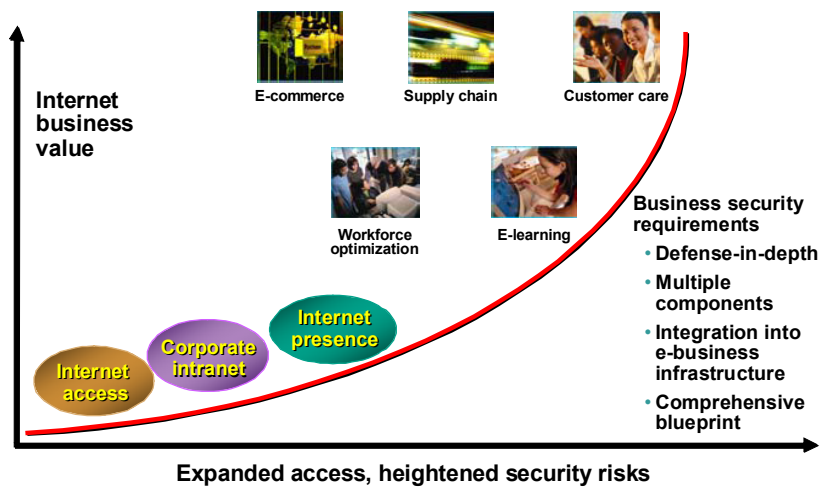
Security has moved to the forefront of network management and implementation. It is necessary for the survival of many businesses to allow open access to network resources and ensure that the data and resources are as secure as possible.

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 produces the need for as much security as is possible.
- 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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.9

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 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

Cisco.com

- **Many governments have formed cross-border task forces to deal with privacy issues.**
- **The outcome of international privacy efforts is expected to take several years to develop.**
- **National laws regarding privacy are expected to continue to evolve worldwide.**



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-10

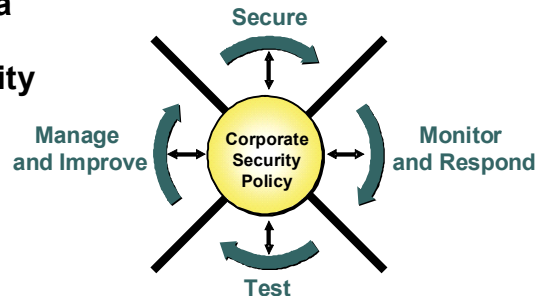
As concerns about privacy increase, many governments have formed cross-border task forces to deal with privacy issues. International privacy efforts are expected to take several years to develop and even longer to implement globally. National laws regarding privacy are expected to continue to evolve worldwide.

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.11

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

- Secure—The following are methods used to secure a network:
 - Authentication
 - Encryption
 - Firewalls
 - Vulnerability patching
- Monitor—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—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 or outsource it to a third party such as the Cisco Security Posture Assessment (SPA) group.
- Improve—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 to adjust the security policy as vulnerabilities and risks are identified.

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

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—2-13

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**
- **To inform users of their responsibilities**
- **To define assets and the way to use them**
- **To state the ramifications of misuse**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.14

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

- Provides a process for auditing 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**

© 2004, Cisco Systems, Inc. All rights reserved.

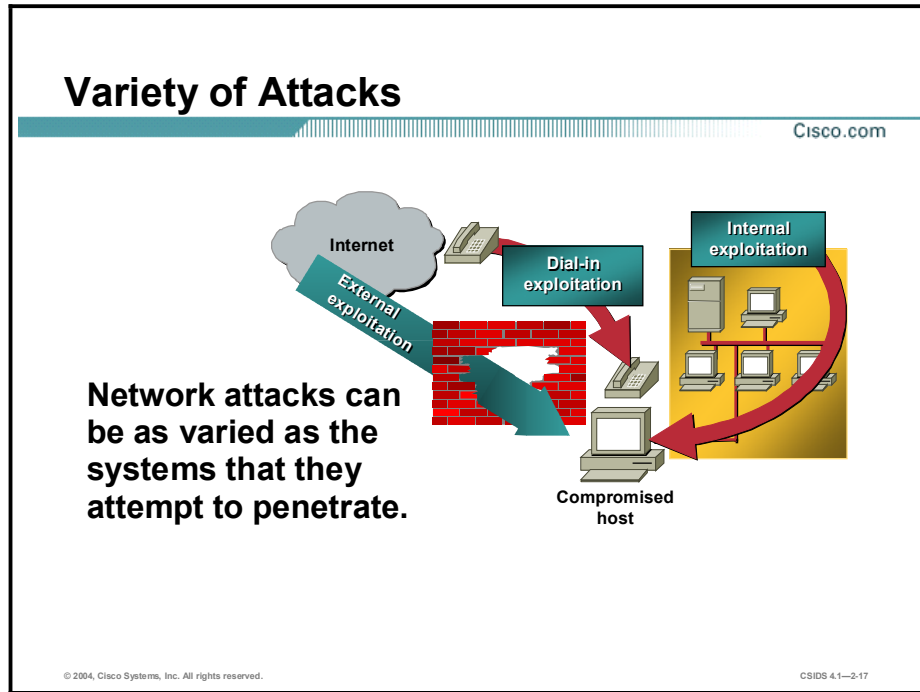
CSIDS 4.1—2-15

The following are some of the key policy components:

- **Statement of authority and scope**—This topic specifies who sponsors the security policy and what areas the policy covers.
- **Acceptable use policy**—This topic specifies what the company will and will not allow regarding its information infrastructure.
- **Identification and authentication policy**—This topic 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 topic specifies what the company considers ethical and proper use of its Internet access capabilities.
- **Campus access policy**—This topic specifies how on-campus users will use the company's data infrastructure.
- **Remote access policy**—This topic specifies how remote users will access the company's data infrastructure.
- **Incident handling procedure**—This topic specifies how the company will create an incident response team and the procedures it will use during and after an incident.

Primary Network Threats and Attacks

This topic provides an overview of primary network threats and attacks.



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, California, 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-18

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 in 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 in 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 may have malicious and destructive intent, or they may simply be errors that generate a threat.
- Internal threats—These threats typically involve 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.

The Four Primary Attack Categories

Cisco.com

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

- **Reconnaissance attacks**
- **Access attacks**
- **Denial of service attacks**
- **Worms, viruses, and Trojan horses**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.19

There are four types of network attacks:

- **Reconnaissance attacks**—An intruder attempts to discover and map systems, services, and vulnerabilities.
- **Access attacks**—An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.
- **Denial of service (DoS) attacks**—An intruder attacks your network in a way that damages or corrupts your computer system or denies you and others access to your networks, systems, or services.
- **Worms, viruses, and Trojan horses**—Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services or access to networks, systems, or services.


Reconnaissance Attacks and Mitigation

This topic describes reconnaissance attacks and their mitigation.

Reconnaissance Attacks

Cisco.com

Reconnaissance refers to the overall act of learning information about a target network by using readily available information and applications.



© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—2-21

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, precedes an actual access or DoS attack. The malicious intruder typically conducts a ping sweep of the target network first to determine which IP addresses are alive. After this has been accomplished, the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the application type and version as well as the type and version of the operating system running on the target host.

Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, a house with 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 it is opened, but to discover vulnerable services that they can exploit later when there is less likelihood that anyone is looking.

Reconnaissance attacks can consist of the following:

- Packet sniffers
- Port scans
- Ping sweeps
- Internet information queries

Packet Sniffers

Cisco.com



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.**
- **Packet sniffers can be general purpose or can be designed specifically for attack.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.22

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 Attack Mitigation

Cisco.com



The following techniques and tools can be used to mitigate sniffer attacks:

- **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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.23

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

- **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).

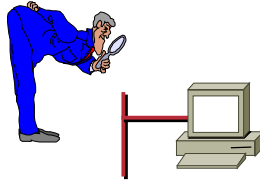
An OTP is a type of two-factor authentication. Two-factor authentication involves using something you have combined with something you know. Automated teller machines (ATMs) use two-factor authentication. A customer needs both an ATM card and a personal identification number (PIN) to make transactions. 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 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 e-mail messages) will still be effective.

- **Switched infrastructure**—This technique 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**—Software and hardware designed to detect the use of sniffers on a network can be employed. 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 whether 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 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).

Port Scans and Ping Sweeps

Cisco.com



These attacks can attempt to:

- Identify all services on the network
- Identify all hosts and devices on the network
- Identify the operating systems on the network
- Identify vulnerabilities on the network

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.24

Port scans and ping sweeps are typically applications built to run various tests against a host or device in order to identify vulnerable services. The information is gathered by examining IP addressing and port or banner data from both TCP and UDP ports.

Port Scan and Ping Sweep Attack Mitigation

Cisco.com

- **Port scans and ping sweeps cannot be prevented entirely.**
- **IDSs at the network and host levels can usually notify an administrator when a reconnaissance attack such as a port scan or ping sweep is under way.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.25

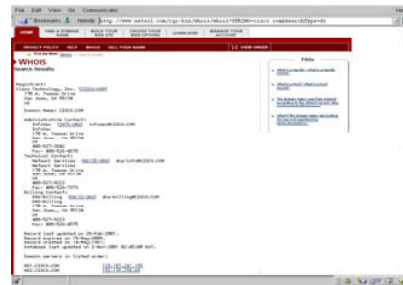
If ICMP echo and echo reply are turned off on edge routers, for example, ping sweeps can be stopped, but at the expense of network diagnostic data. However, port scans can easily be run without full ping sweeps; they simply take longer because they need to scan IP addresses that might not be live. IDSs at the network and host levels can usually notify an administrator when a reconnaissance attack is under way. This warning allows the administrator to better prepare for the coming attack or to notify the Internet service provider (ISP) that is hosting the system launching the reconnaissance probe.

Internet Information Queries

Cisco.com



Sample IP address query



Sample domain name query

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-26

The figure demonstrates how existing Internet tools can be used for network reconnaissance (for example, an IP address query or a Domain Name System [DNS] 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 step 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 with them.

Access Attacks and Mitigation


This topic describes specific access attacks and their mitigation.

Access Attacks

Cisco.com

In access attacks, intruders typically attack networks or systems to:

- Retrieve data
- Gain access
- Escalate their access privileges



© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—2.28

Access attacks exploit known vulnerabilities in authentication services, FTP services, and Web services to gain entry to Web accounts, confidential databases, and other sensitive information. Access attacks can consist of the following:

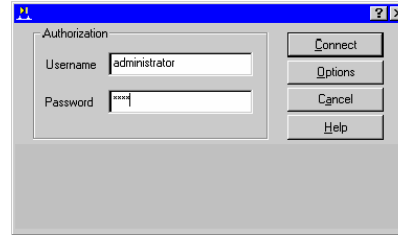
- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle attacks

Password Attacks

Cisco.com

Hackers can implement password attacks using several methods:

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.29

Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, 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 gains access to a resource, he or she has the same access rights as the user whose account has been compromised. 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 Mitigation

Cisco.com

The following are password attack 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.
- Force periodic password changes.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.30

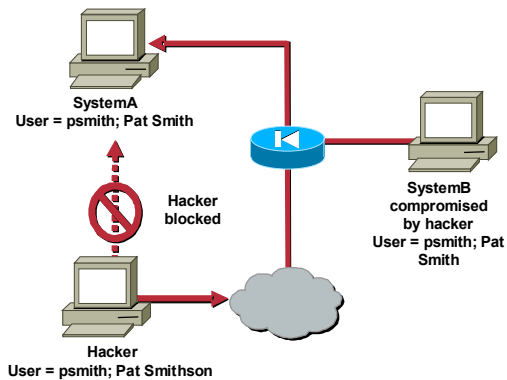
The following are password attack mitigation techniques:

- 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 a specific number of unsuccessful logins—This practice 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 the use of strong passwords only. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.
- Force periodic password changes—Forcing users to periodically change their passwords can reduce the risk of password discovery.

Trust Exploitation Attack Mitigation

Cisco.com

- 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.



© 2004, Cisco Systems, Inc. All rights reserved.

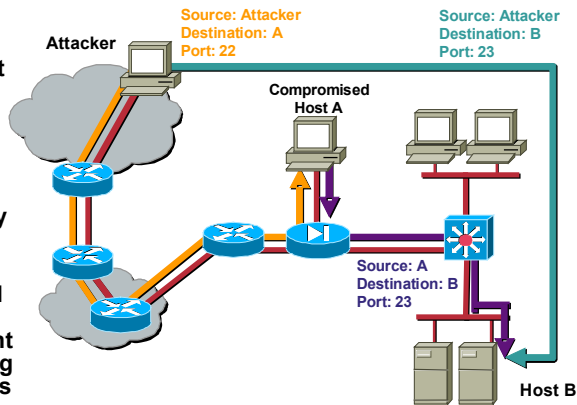
CSIDS 4.1—2.32

You can mitigate trust 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

Cisco.com

- 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 from installing port redirection utilities on the host.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-33

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

Man-in-the-Middle Attacks

Cisco.com



- 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

© 2004, Cisco Systems, Inc. All rights reserved.

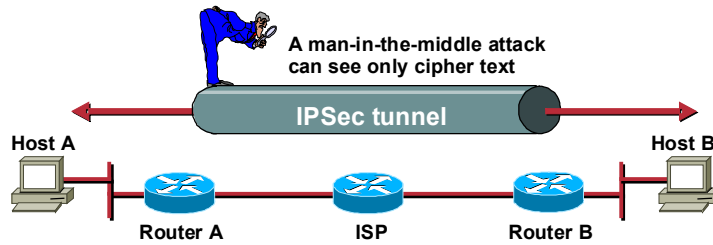
CSIDS 4.1—2.34

A man-in-the-middle attack requires that the attacker have access to network packets that come across the network. 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 and who can gain access to all network packets transferred between your network and any other network.

Man-in-the-Middle Attack Mitigation

Cisco.com



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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-35

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


Denial of Service Attacks and Mitigation

This topic describes specific DoS attacks and their mitigation.

Denial of Service Attacks

Cisco.com

Denial of service attacks occur when an intruder attacks your network in a way that damages or corrupts your computer system or denies you and others access to your networks, systems, or services.



© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1--2.37

Certainly the most publicized form of attack, DoS attacks are also among the most difficult to completely eliminate. Even within the hacker community, DoS attacks are regarded as trivial and considered bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators. If you are interested in learning more about DoS attacks, researching the methods employed by some of the better-known attacks can be useful. DoS attacks can consist of the following:

- IP spoofing
- Distributed denial of service (DDoS)

IP Spoofing

Cisco.com

- **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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-38

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 bidirectional communication, the attacker must change all routing tables to point to the spoofed IP address. Another approach the attacker could take is simply not to 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 or she 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 use is not restricted to people who are external to the network.

Although this use is not as common, IP spoofing can also provide 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 when simple spoofing attacks are combined with knowledge of messaging protocols.

IP Spoofing Attack 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.
- **Require additional authentication that does not use IP-based authentication**—Examples of this technique include the following:
 - **Cryptographic (recommended)**
 - **Strong, two-factor, one-time passwords**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.39

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 OTPs can also be effective.

DoS and DDoS Attacks

Cisco.com

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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—240

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 because 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.

DoS and DDoS Attack Mitigation

Cisco.com

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

- **Antispoof features—Proper configuration of antispoof features on routers and firewalls**
- **Anti-DoS features—Proper configuration of anti-DoS features on routers, firewalls, and Intrusion Detection Systems**
- **Traffic rate limiting—Implement traffic rate limiting with the ISP of the network**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.41

When they involve specific network server applications, such as an HTTP server or an 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, firewalls, and IDSs can help limit the effectiveness of an attack. These features often involve limits on the amount of half-open connections that a system allows 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.

Worm, Virus, and Trojan Horse Attacks and Mitigation


This topic describes worm, virus, and Trojan horse attacks and their mitigation.

Worm, Virus, and Trojan Horse Attacks

Cisco.com

The primary vulnerabilities for end-user workstations are worm, virus, and Trojan horse attacks.

- A worm executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.
- A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.
- 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.



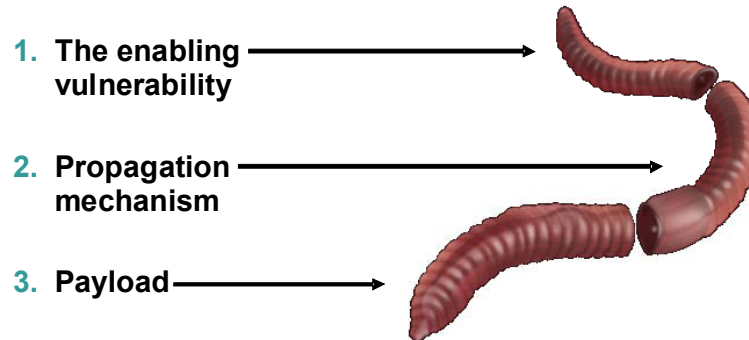
© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—2-43

The primary vulnerabilities for end-user workstations are worm, virus, and Trojan horse attacks.

- A worm executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.
- A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.
- 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.

Worm Attacks

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.44

The anatomy of a worm attack is as follows:

- **The enabling vulnerability**—A worm installs itself using an exploit vector on a vulnerable system.
- **Propagation mechanism**—After gaining access to devices, a worm replicates and selects new targets.
- **Payload**—Once the device is infected with a worm, the attacker has access to the host—often as a privileged user. Attackers could use a local exploit to escalate their privilege level to administrator.

Typically, worms are self-contained programs that attack a system and try to exploit a vulnerability in the target. Upon successful exploitation of the vulnerability, the worm copies its program from the attacking host to the newly exploited system to begin the cycle again. A virus normally requires a vector to carry the virus code from one system to another. The vector can be a word-processing document, an e-mail message, or an executable program. The key element that distinguishes a computer worm from a computer virus is that human interaction is required to facilitate the spread of a virus.

Worm Attack Mitigation

Cisco.com

- **Containment**—Contain the spread of the worm inside your network and within your network. Compartmentalize parts of your network that have not been infected.
- **Inoculation**—Start patching all systems and, if possible, scanning for vulnerable systems.
- **Quarantine**—Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.
- **Treatment**—Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—245

Worm attack mitigation requires diligence on the part of system and network administration staff. Coordination between system administration, network engineering, and security operations personnel is critical in responding effectively to a worm incident. The following are the recommended steps for worm attack mitigation:

- Containment
- Inoculation
- Quarantine
- Treatment

Typical incident response methodologies can be subdivided into six major categories. The following categories are based on the network service provider security (NSP-SEC) incident response methodology:

- Preparation—Acquire the resources to respond.
- Identification—Identify the worm.
- Classification—Classify the type of worm.
- Traceback—Trace the worm back to its origin.
- Reaction—Isolate and repair the affected systems.
- Post mortem—Document and analyze the process used for the future.

Virus and Trojan Horse Attacks

Cisco.com

- **Viruses are malicious software that is 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.46

The primary vulnerabilities for end-user workstations are viruses and Trojan horse attacks. Viruses are 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) that 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. The other users receive the game and then play it, thus spreading the Trojan horse.

Virus and Trojan Horse Attack Mitigation

Cisco.com

These kinds of applications can be contained by:

- **Effective use of antivirus software**
- **Keeping up-to-date with the latest developments in these sorts of attacks**
- **Keeping up-to-date with the latest antivirus software and application versions**
- **Effective use of Intrusion Protection**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-47

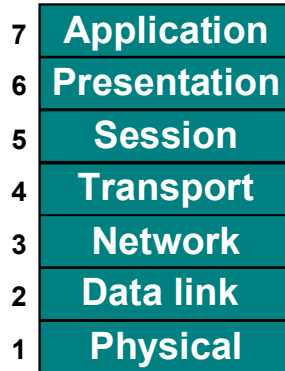
These kinds of applications can be contained through the effective use of antivirus software and intrusion protection at the user level and potentially at the network level. Both methods can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping 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.

Application-Layer Attacks

Cisco.com

Application-layer attacks have the following characteristics:

- Exploit well-known weaknesses, such as those in 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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-48

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 he or she has 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 Attack Mitigation

Cisco.com

Measures you can take to reduce your risks include the following:

- **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.**
- **Use IDSs, which can scan for known attacks, monitor and log attacks, and in some cases, prevent attacks.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—249

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 by various sources.
- Keep your operating system and applications current with the latest patches—Always test patches and fixes in a nonproduction environment. This practice prevents downtime and keeps errors from being generated unnecessarily.
- Use IDSs to 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. In most cases, it can be done automatically.

Management Protocols and Functions

The protocols used to manage your network can become a source of vulnerability. This topic 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.51

If the managed device does not support any of the recommended protocols, such as SSH and SSL, Telnet may be required (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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2-52

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 reduce the chance of an attacker from outside the network spoofing the addresses of the management hosts.

Management Protocols

Cisco.com

The following are management protocols that that can be compromised:

- **SNMP**—The community string information for simple authentication is sent in clear text.
- **Syslog**—Data is sent as clear text between the managed device and the management host.
- **TFTP**—Data is sent as clear text between the requesting host and the TFTP server.
- **NTP**—Many NTP servers on the Internet do not require any authentication of peers.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.53

Simple Network Management Protocol (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.

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.

Trivial File Transfer Protocol (TFTP) is used 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 reduce the chance of its being intercepted.

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 network administrators to implement their own master clocks for private networks synchronized to Coordinated Universal Time (UTC) via satellite or radio. However, clock sources are available for synchronization via

the Internet, for network administrators who do not wish to implement their own master clocks because of cost 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.

Management Protocol Recommendations

Cisco.com

- **SNMP recommendations:**
 - Configure SNMP with only read-only community strings.
 - Set up access control on the device you wish to manage.
 - Use SNMP Version 3 or above.
- **Logging recommendations:**
 - Encrypt Syslog traffic within an IPSec tunnel.
 - Implement RFC 2827 filtering.
 - Set up access control on the firewall.
- **TFTP recommendations:**
 - Encrypt TFTP traffic within an IPSec tunnel.
- **NTP recommendations:**
 - Implement your own master clock.
 - Use NTP Version 3 or above.
 - Set up access control that specifies which network devices are allowed to synchronize with other network devices.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—2.54

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 access by only the appropriate management hosts.
- Use SNMP Version 3 or above.

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.
- When possible, TFTP traffic should be encrypted within an IPSec tunnel in order to reduce the chance of its being intercepted.

The following are NTP recommendations:

- Implement your own master clock for private network synchronization.
- Use NTP Version 3 or above because these versions support a cryptographic authentication mechanism between peers.
- Use ACLs that specify which network devices are allowed to synchronize with other network devices.

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco.com

- **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 comprises four phases: secure, monitor, test, and improve.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—2.56

Summary (Cont.)

Cisco.com

- **The following are the four types of security threats:**
 - **Structured**
 - **Unstructured**
 - **Internal**
 - **External**
- **The following are the four primary attack categories:**
 - **Reconnaissance attacks**
 - **Access attacks**
 - **Denial of service attacks**
 - **Worms, viruses, and Trojan horses**
- **Configuration management and management protocols are an important part of securing a network.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—2.57

Intrusion Detection Overview

Overview

This lesson provides the fundamental knowledge required to understand an intrusion detection system (IDS).

This lesson includes the following topics:

- Objectives
- Intrusion detection terminology
- Intrusion detection technologies
- Network-based intrusion detection systems
- Host-based intrusion prevention system
- Intrusion protection benefits
- Network Sensor platforms
- Host-based intrusion protection system
- Sensor appliances
- Deploying Cisco IDS
- Summary

Objectives

This topic lists the lesson objectives.

Objectives

Cisco.com

Upon completion of this lesson, 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 similarities and differences among the various intrusion detection technologies.**
- **Explain the differences between HIPS and NIDS.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-2

Objectives (Cont.)

Cisco.com

- Describe the benefits of intrusion protection.
- Describe the network sensors that are currently available and their features.
- Describe the Cisco Security Agent.
- Describe the considerations necessary for selection, placement, and deployment of network intrusion protection.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-3

Intrusion Detection Terminology

This topic 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.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—3-5

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.

False Alarms

Cisco.com

- **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.**

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

CSIDS 4.0—3-12

The ability of 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 enters the wrong password. The IDS cannot distinguish between a rogue user and the network administrator, and it 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 or as complex as 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

Cisco.com

- **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 nonoffending traffic is detected. Normal traffic or a benign action does not cause an alarm.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1–3.7

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 Internet Information Server (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 tools**
 - **Shell scripts**
 - **Executable code**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-8

A vulnerability is a weakness that compromises either the security or the 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 denial of service (DoS) or access to restricted system resources.
- **Insecure communication**—Data that is transferred in clear text is susceptible to interception. 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 topic describes the various technologies implemented in IDSs. Cisco IDS Sensors use a blend of the technologies discussed in this topic. 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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-10

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 (Simple Mail Transfer Protocol [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

Cisco.com

- **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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-11

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 generate 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 intrusion detection, but it 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.

Reactive IDSs can respond to an attack in any of the following ways:

- **Terminate session (TCP resets)**
- **Block offending traffic (ACL)**
- **Create session log files (IP logging)**

Intrusion detection technology is traditionally considered a passive monitoring tool. Earlier IDSs simply monitored the network for suspicious activity or parsed system log files. Today's 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 the destination address of the target.
- **Block offending traffic**—The IDS communicates with the network device and applies an access control list (ACL) 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.

Network-Based Intrusion Detection Systems

This topic describes the features of network-based IDSs (NIDSs).

NIDS Features

Cisco.com

- **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.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—3-15

An 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 networks regardless of network growth. Network growth can occur by adding either additional hosts or new networks. Additional hosts added to 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:

- Exceeded 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.

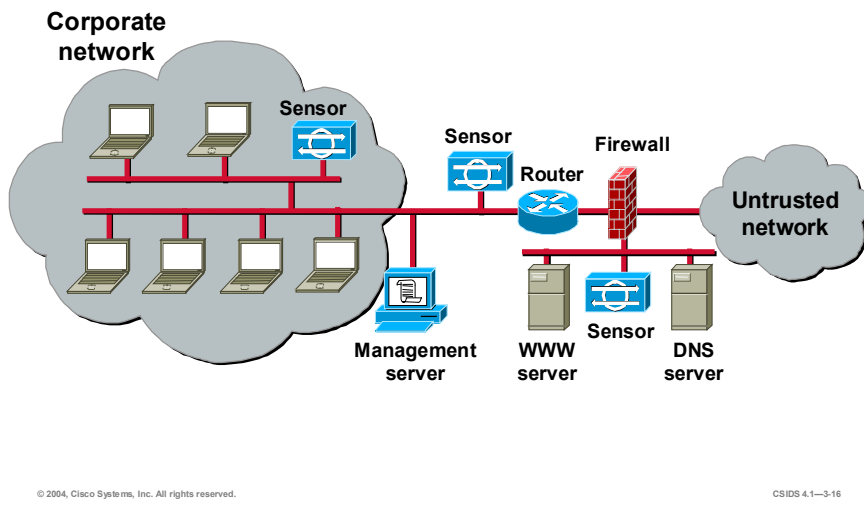
NIDS Sensors are typically tuned for intrusion detection analysis. The underlying operating system is “stripped” of unnecessary network services, and essential services are secured.

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

- Network interface card (NIC)—NIDSs must be able to connect into any network. Common NIDS NICs include Ethernet, Fast Ethernet, Gigabit Ethernet, 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



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.

Host-Based Intrusion Prevention System

This topic describes the features of a host-based intrusion prevention system (HIPS) and introduces the Cisco Security Agent (CSA).

HIPS Features

Cisco.com

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

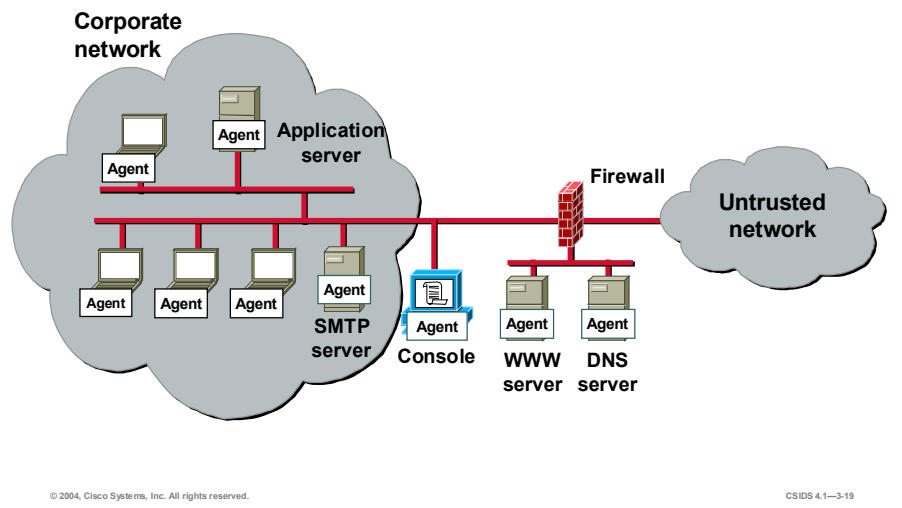
© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—3-18

A HIPS audits host log files, host file systems, and resources. An advantage of a 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 a 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.

HIPS

Cisco.com



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.

Intrusion Protection Benefits

This topic describes the Cisco intrusion protection technologies and solution. In addition, it discusses a defense-in-depth security strategy.

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 data stream**
- **Greater protection against known and unknown threats**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—3-21

The Cisco intrusion protection technologies enable customers to actively defend their networks 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 data stream
- Greater protection against known and unknown threats

Active Defense System

Cisco.com

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 against future attacks from a malicious source.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-22

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 against 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 feature**
- **Host Agents—Server and desktop protection**
- **Comprehensive management—Robust system management and monitoring**



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-23

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

- **Network Sensors**—Network Sensors provide a dedicated intrusion detection appliance with the ability to monitor and protect 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 deployments that require basic intrusion detection features.
- **Firewall Sensors**—Firewall Sensors provide intrusion detection for 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

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-24

No single device or security technology can provide a complete security solution. A defense-in-depth security solution attempts to protect network resources by providing layers of security. Intrusion detection can be implemented at both the host level and the 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 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 topic 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 Countermeasures Research Team (C-CRT)
- **Signature language**
 - Allowing customers to write their own signatures
- **Analysis support**
 - Integrated Network Security Database

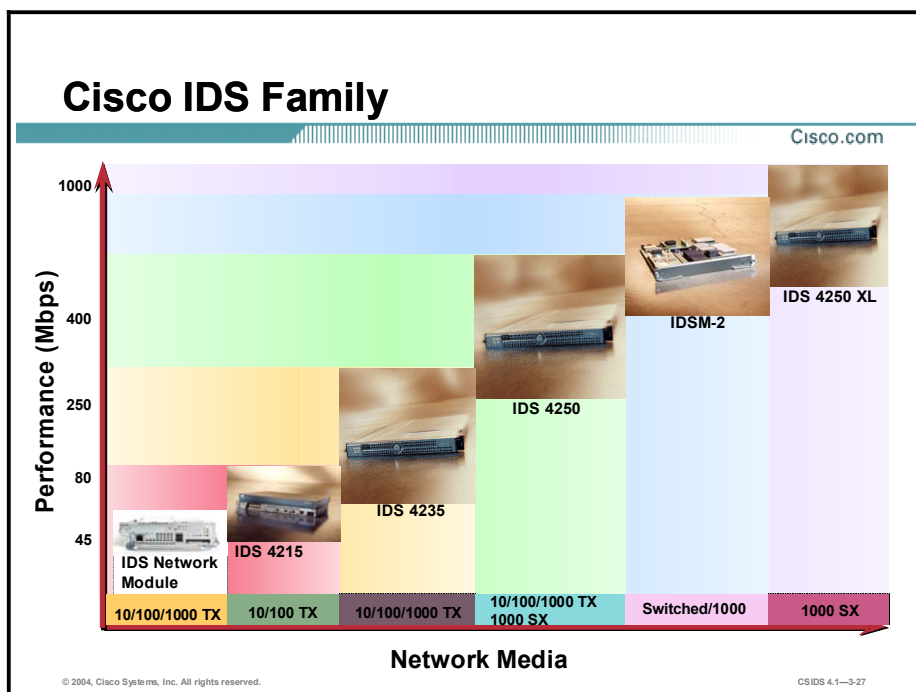




© 2004, Cisco Systems, Inc. All rights reserved.
CSIDS 4.1—3-28

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

Cisco IDS Product Features

Feature	Sensor Appliance/IDSM-2/NM-CIDS	Cisco IOS IDS	PIX Firewall IDS
TCP reset	X	X	X
IP session logging	X		
Blocking	X	X	X
Packet drop		X	X
Active updates	X		
Signature language	X		
Analysis support	X	X	X



The table provides a reference for all products that run Cisco IDS Software Versions 4.0 or higher.

Cisco IDS Product Features

	Cisco IDS Network Module	Cisco 4215 Sensor Appliance	Cisco 4235 Sensor Appliance	Cisco 4250 Sensor Appliance	IDSM-2	Cisco 4250-XL Sensor Appliance
Performance (Mbps)	10-45	80	250	500	600	1000
Network media	10/100/1000 BASE-TX	10/100 BASE-TX	10/100/1000 BASE-TX	10/100/1000 BASE-TX or 1000BASE-SX	Switched 1000	1000 BASE-SX

Note The 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 Software Version 4.1.

Note 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—Cisco 4200 Series Appliance

Cisco.com

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-28

The Cisco 4200 Series Network Sensor appliances are market-leading, dedicated appliances for intrusion prevention and detection, with the industry's highest performance and lowest false alarm rates. The 4200 Series appliances are focused on protecting network devices, services, and applications. They are capable of detecting sophisticated attacks such as the following:

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

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

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

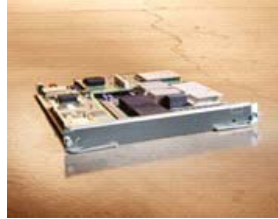
Note The Sensor does not modify ACLs on the PIX Firewall. The **shun** command is used on the PIX Firewall to enforce blocking.

- TCP reset—Terminates a session by sending TCP packets with the reset, RST, flag to both the source and destination of the attack.
- IP logging—Creates a binary file that captures data from the source of the attack.

Switch Sensor—Cisco Catalyst 6500 IDSM-2

Cisco.com

- **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**
- **Supports unlimited number of VLANs**
- **Runs same code as Sensor appliance**



© 2004, Cisco Systems, Inc. All rights reserved.

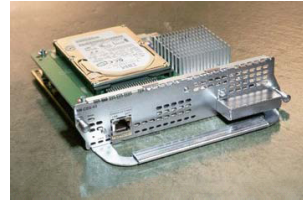
CSIDS 4.1—3-29

The Cisco Catalyst 6500 Intrusion Detection System Module 2 (IDSM-2) provides full-featured intrusion protection in the core network fabric device. The IDSM-2 is specifically designed to address switched 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; therefore, there is no impact on switch performance. The IDSM-2 has access to the data stream via VLAN access control list (VACL) capture capable of supporting an unlimited number of VLANs.

Router Sensor—IDS Network Module for Access Routers

Cisco.com

- **Integrates IDS into the 2600XM, 2691, 3660, 3725, & 3745 access router platforms**
- **Provides full-featured intrusion protection**
- **Able to monitor traffic from all router interfaces**
- **Able to inspect GRE/IPSec traffic that has been decrypted at the router**
- **Delivers comprehensive intrusion protection at branch offices, isolating threats from corporate network**
- **Runs same code as Sensor appliances**



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-30

The Network Module-Cisco IDS (NM-CIDS) can be installed in a Cisco 2600XM, 2691, 3660, or 3700 Series router to provide 45 Mbps of full-featured intrusion protection services within the router. The IDS Network Module provides the ability to inspect all traffic traversing the router and then identify and terminate unauthorized or malicious activity. The IDS Network Module leverages the current Cisco IDS Sensor technology to expand IDS support into the branch office router. It requires an encryption feature set of Cisco IOS Software Release 12.2(15)ZJ or later for the routers. Through collaboration with IPSec virtual private network (VPN) and Generic Routing Encapsulation (GRE) traffic, the module allows decryption, tunnel termination, and traffic inspection at the first point of entry into the network. Only one IDS Network Module is supported in a single router; however, it is not restricted to a specific network module slot within the router.

Router Sensor—Cisco IOS IDS

Cisco.com

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-31

The Router Sensor integrates intrusion detection into Cisco IOS software. A Cisco IOS IDS is able to detect a limited subset of attacks compared to an IDS Sensor appliance or IDSM-2. Thus, it is targeted at lower-risk environments.

The following are the Cisco IOS IDS features:

- **Signature set—100 IDS signatures**
- **Reporting—Sends alarms to a Syslog server or another PostOffice-aware device**
- **Responses—Drops the packet, blocks offending traffic, and terminates a TCP session**

The software and hardware requirements of a Cisco IOS software-based device performing intrusion detection are as follows:

- **Software—Cisco IOS Software Release 12.0(5)T and greater**
- **Hardware—Cisco 830, 1700, 2600, 3600, 7100, 7200, and 7500 Series routers and the Catalyst 5000 Route Switch Module (RSM)**

Firewall Sensor—PIX Firewall IDS

Cisco.com

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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-32

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 terminates a TCP session**

The following are the software and hardware requirements for a PIX Firewall performing intrusion detection:

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

Host-based Intrusion Protection System

This topic describes the Cisco host-based intrusion protection system (HIPS) features and current platform.

Cisco Security Agent Features

Cisco.com

- **Active protection**
 - Protects application and operating system against known and unknown attacks
 - Prevents access to server resources before unauthorized activity occurs
 - Uses behavior-based technology
- **Consists of two products**
 - Agents
 - Management Center
- **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**
- **5–10% Agent CPU overhead**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1–3-34

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

The CSA consists of two components:

- Agents—Installed on hosts
- Management Center for Cisco Security Agents (CSA MC)—Provides centralized Agent management

The CSA MC installation automatically builds Agent kits, so it is not necessary to log in to the CSAMC 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 a web link to an Agent kit, or software image replication. In the event that identical software images are distributed, the CSAMC automatically ensures that each new agent is registered with a unique identifier.

Because the CSA 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

cannot bypass the installation. Agents automatically register with the CSAMC after installation, so configuration is also transparent to the end user.

Agents communicate with the CSAMC via Secure Sockets Layer (SSL) for rules updates with no user intervention. When Agents poll into the CSAMC at a 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.

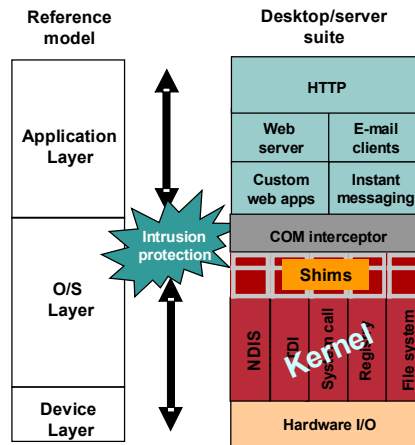
Note CSA events can be reported to the Cisco Security Monitor, a tool for capturing, storing, viewing, correlating, and reporting on events.

Note Agents can run on Windows NT, Windows 2000, Windows XP, and Solaris 2.8. CSA does not inspect content, and therefore it has a negligible impact on performance.

Cisco Security Agent Architecture

Cisco.com

- Windows and Solaris platforms
- Server and desktop agents
- Malicious mobile code protection and operating system lockdown in one Agent
- Default and customizable policies
- Approximately 2% CPU overhead
- Buffer overflow protection
- Web server protection
- Instant messenger security
- Comprehensive kernel interceptor shims
- Low computational overhead



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-3-35

The CSA behavior-based technology has application visibility because it resides at the kernel level within the operating system. When an application attempts an operation, the CSA checks the operation against the application's security policy and makes a real-time decision to allow or deny the continuation of the operation. 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 CSA policies in the CSAMC.

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

The CSA's Intercept Correlate Rules Engine (INCORE) architecture intercepts all system calls to file, network, Component Object Model (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 CSA 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 and 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 Sandboxing is a technique that prevents access to server resources not specifically allowed by the operating system or application.

CSA Aggregates Multiple Endpoint Security Functions

Cisco.com

	CSA	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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-36

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

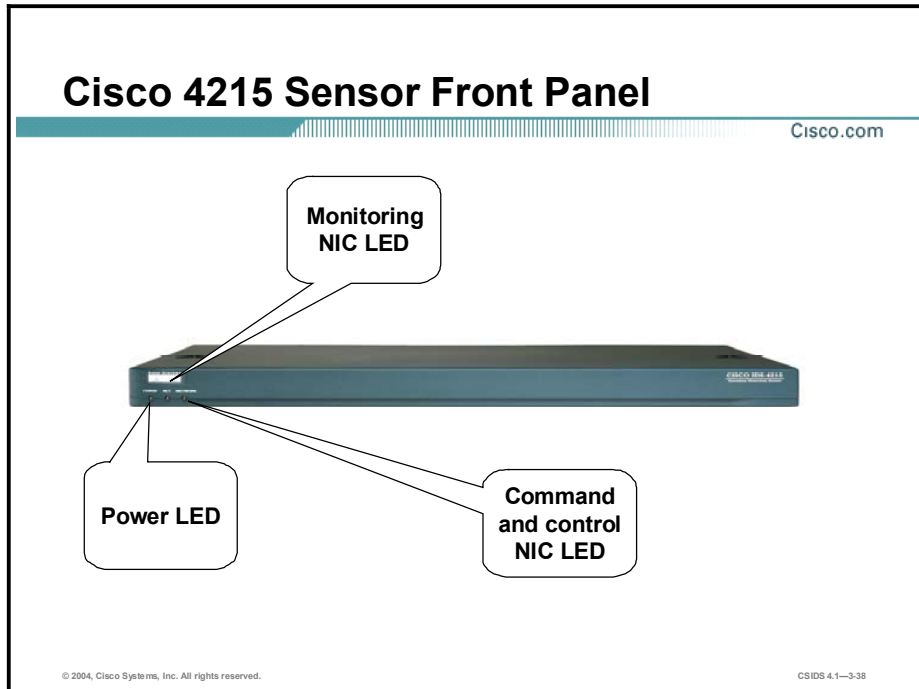
- Port scan detection—The CSA network-wide correlation provides unique functionality in the detection of distributed port scans. Low-level port scans are used by hackers to systematically scan single ports on single Agents in an alternating fashion in order to map a network. For example, server 1 would be scanned on port 1, server 2 on port 2, and so on. Each Agent reports the scan activity to the CSAMC. With its ability to correlate events from distributed Agents, the CSA is able to discern that a distributed port scan is taking place.
- Malicious application detection and prevention—The CSA can perform such difficult tasks such as catching new Trojan horse attacks. The CSA does so 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 CSA then prevents the executable file from executing its intrusion.

The CSA also complements traditional desktop antivirus software. For example, in the case of a new attack such as an e-mail worm, the CSA 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, a report of an event is sent to the CSAMC. The CSAMC 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 that tells all Agents not to open the offending file, effectively quarantining that file and preventing further damage. The result is that you are then faced with only a few desktop machines that need to be rebuilt, rather than a whole network.

Note A personal firewall is a standalone product; 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.

Sensor Appliances

This topic describes the Cisco IDS Sensor appliances features, connections, and interfaces.



The following are the technical specifications for the Cisco IDS 4215 Sensor:

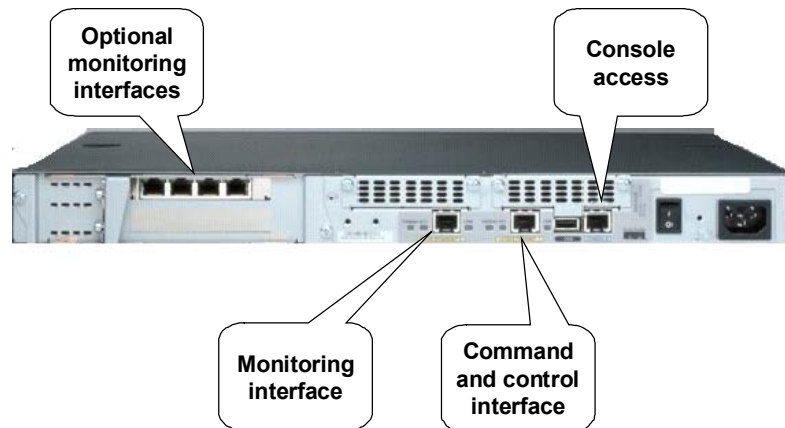
- Performance—80 Mbps
- Standard monitoring interface—10/100BASE-T
- Standard command and control interface—10/100BASE-T
- Optional interface—Four 10/100BASE-TX (4 FE) sniffing interfaces (allowing a total of five sniffing interfaces)
- Performance upgradable—No
- Form factor—1 rack unit (RU)

The following are the physical dimensions of the Cisco IDS 4215 Sensor:

- Height—1.7 in. (4.32 cm)
- Width—16.8 in. (42.54 cm)
- Depth— 11.8 in. (29.97 cm)
- Weight— 11.5 lb. (4.11 kg)

Cisco 4215 Sensor Back Panel

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-39

The back of the Cisco IDS 4215 Sensor can have up to six Ethernet interfaces, one command and control interface and five monitoring interfaces. The interface labeled int1 is the command and control interface, and the interface labeled int0 is the monitoring interface. The four additional monitoring interfaces are int2, int3, int4, and int5, from left to right. The following are the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int0

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.

Cisco 4235 Sensor Front Panel

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-40

The following are the technical specifications for the Cisco IDS 4235 Sensor:

- Performance—250 Mbps
- Standard monitoring interface—10/100/1000BASE-TX
- Standard command and control interface—10/100/1000BASE-TX
- Optional sensing interfaces—Yes
- Performance upgradable—No
- Form factor—1RU

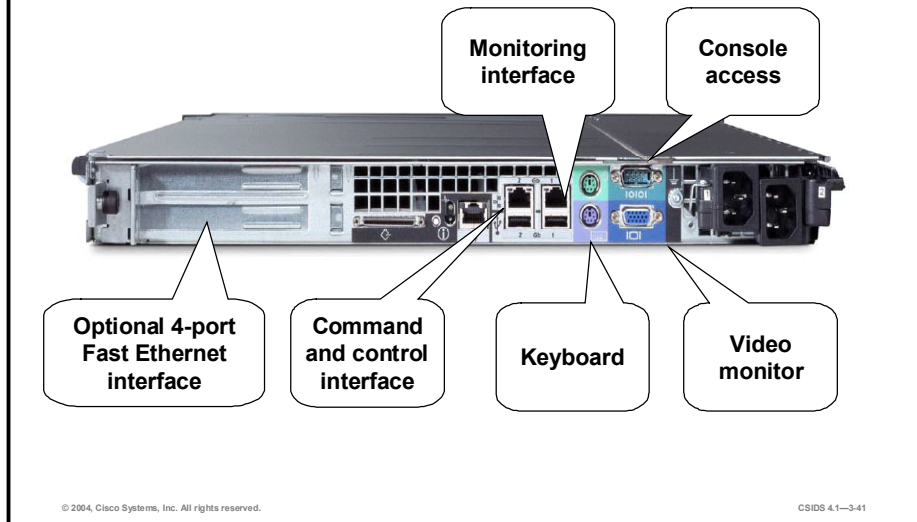
The following are the physical dimensions of the Cisco IDS 4235 Sensor:

- 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.

Cisco 4235 Sensor Back Panel

Cisco.com



The back of the Cisco IDS 4235 Sensor has two Ethernet interfaces. The interface labeled 1 is the monitoring interface, and the interface numbered 2 is the command and control interface. The following are 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 IDS 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.

Note You can install a 4-port Fast Ethernet NIC in the lower PCI slot of the IDS 4235 Sensor to add four sensing interfaces.

Cisco 4250 Sensor Front Panel

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-42

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 upgradable—Yes
- Form factor—1RU

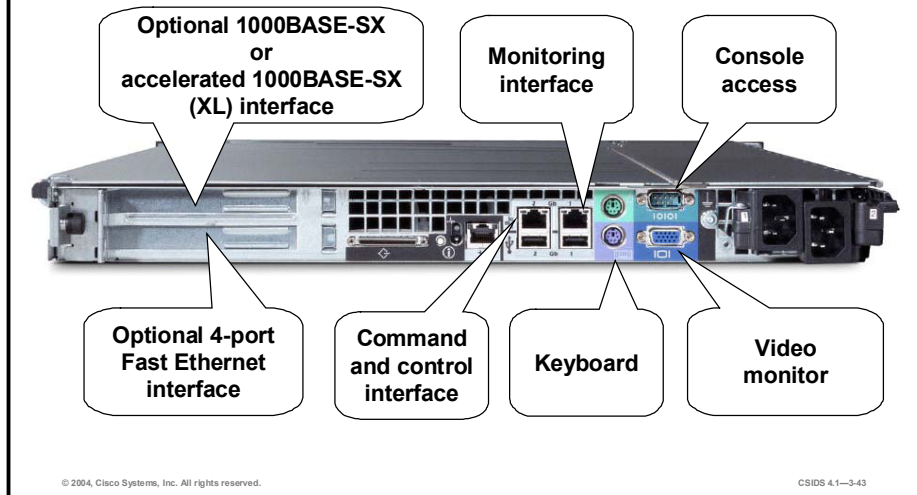
The following are the physical dimensions of the Cisco IDS 4250 Sensor:

- 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.

Cisco 4250 Sensor Back Panel

Cisco.com



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 are the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int0

The IDS 4250 Sensor supports only one of the following cards in a PCI slot:

- The SX card in the upper PCI slot—The Sensor has three interfaces when the SX card is added.
- The XL card in the upper PCI slot—The Sensor has four interfaces when the 2-port XL card is added.
- The 4-port Fast Ethernet card in the lower PCI slot—The Sensor has six interfaces when the 4-port Fast Ethernet NIC is added.

In addition to more interfaces, the IDS 4250 Sensor gives 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*. It is available at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/sensor/7016_04.htm.

Note Cisco IDS Sensor Software Version 4.1 is supported on the 4210, 4215, 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.

Cisco 4250-XL Sensor Front Panel

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-44

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—10/100/1000BASE-TX
- Performance upgradeable—No
- Form factor—1RU

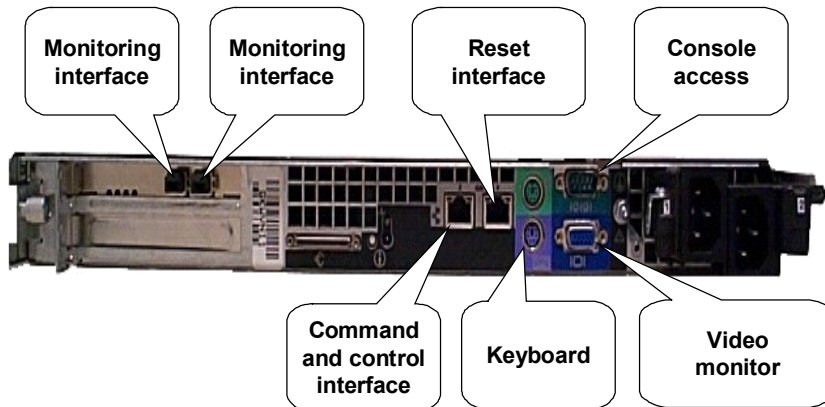
The following are the physical dimensions of the Cisco IDS 4250-XL Sensor:

- 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.

Cisco 4250-XL Sensor Back Panel

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-45

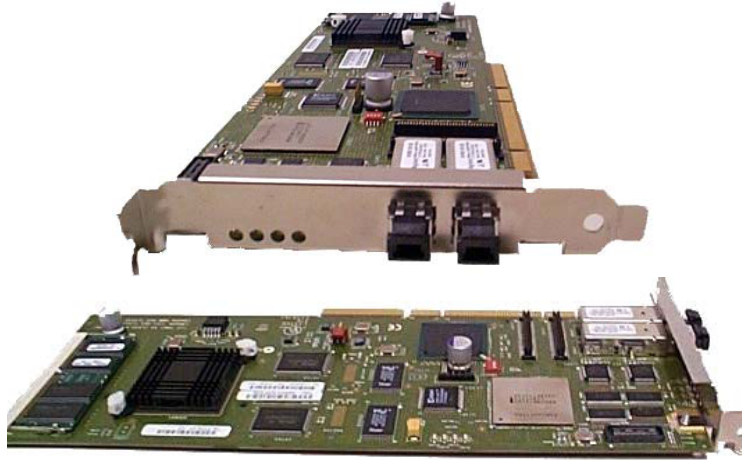
The back of the Cisco IDS 4250-XL Sensor has four Ethernet interfaces. The interface numbered 1 is the TCP reset interface, and the interface numbered 2 is the command and control interface. The two interfaces on the XL card are monitoring interfaces. The following are the type of network connection and the corresponding monitoring interface's device name:

- Network connection—Ethernet
- Device name—int0 and int3

In addition to the interfaces, the Cisco 4250-XL Sensors give you access to the keyboard port, the console access port, and the video monitor port.

Cisco IDS XL Card

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-46

The Cisco 4250-XL Sensor is a Cisco 4250 Sensor appliance with an IDS Accelerator (XL) card already installed. The XL card, which supports gigabit sensing, is a hardware acceleration option for the Cisco 4250 Sensor.

You can install the XL card in the upper PCI slot on the Cisco 4250 Sensor 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 and the original monitoring interface can no longer be used for monitoring. It can only be used for TCP resets. The XL monitoring interface is not supported as a command and control interface.

For detailed instructions on installing the XL card in your Cisco 4250 Sensor, refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide, Version 4.1*.

Deploying Cisco IDS

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

Sensor Selection Factors

Cisco.com

- **Network media—Ethernet, Fast Ethernet, and Gigabit Ethernet**
- **Intrusion detection analysis performance—Bits per second**
- **Network environment—T1/E1, switched, multiple T3/E3, OC-12, and Gigabit**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—3-48

Several factors affect the decisions to be made when selecting Sensors for a Cisco IDS solution: organizational, financial, and technical. For the purposes of this discussion, the focus is on the 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 by the network media and environment. Cisco IDS Sensor NICs range from Ethernet to Gigabit Ethernet.
- Intrusion detection analysis performance—The performance for the Sensors is rated by the number of bits per second that can be captured and accurately analyzed. Cisco IDS Sensor performance ranges from 45 Mbps to 1000 Mbps.
- Network environment—Cisco IDS Sensors are suited for networks that have network speeds ranging from 10/100BASE-T Ethernet to Gigabit Ethernet.

Sensor Deployment Considerations

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-49

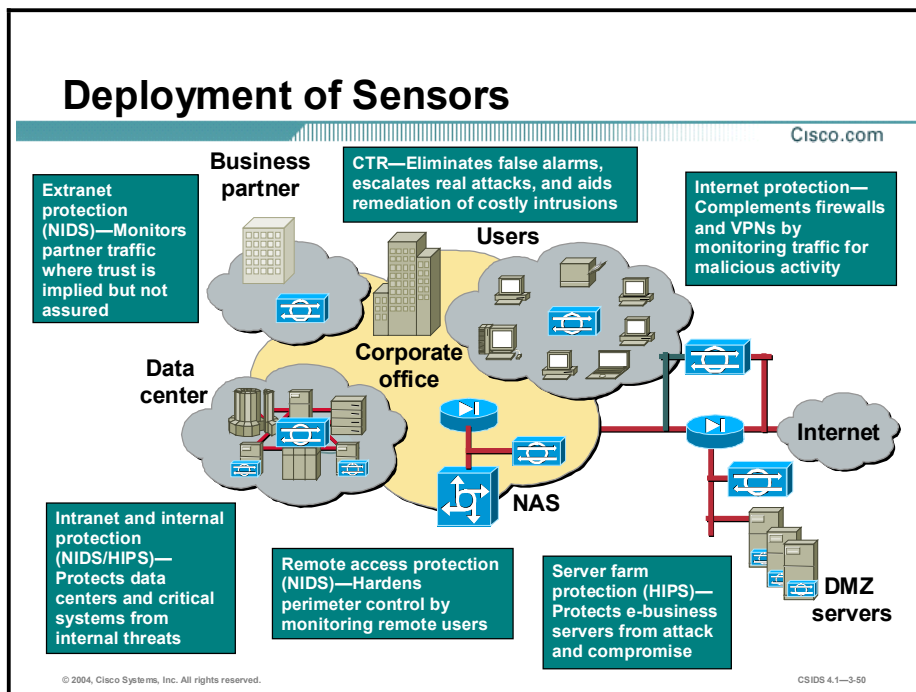
Deploying a Cisco IDS solution requires a well thought-out design. The following are the important design issues to take into consideration:

- **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 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 this lesson.
- **Management and monitoring options**—Review the management and monitoring options discussed earlier to select those most appropriate for your network. Keep in mind that the number of Sensors that you will deploy is directly correlated to the type of management console you select. The recommended Sensor-to-IDS Event Viewer (IEV) ratio is 5:1. For the Management Center for IDS Sensors (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 to ensure functionality. The table shows the ports used by the various management and monitoring applications for communications with Sensors.

Ports Used for Managing or Monitoring

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



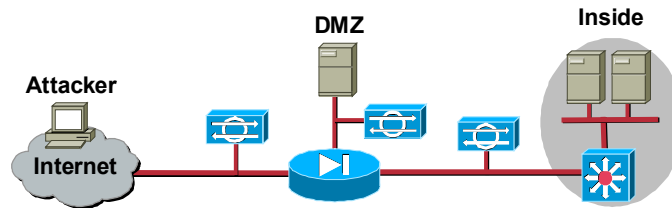
As you examine your network topology to determine how many IDS appliances are required, consider all connections to the network you want to protect. Locations that need to be protected generally fall into five basic categories, as illustrated in the figure:

- **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 connections with 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 Demilitarized Zone (DMZ) networks. These servers offer Internet services such as Web access, Domain Name System (DNS), FTP, and SMTP. The CSA agents are installed on these servers. The CSAMC is installed on an internal network.

A complete Cisco IDS includes the installation of both a NIDS and a HIPS. NIDS Sensors are installed at network entry points to provide broader coverage, and HIPS 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-51

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 topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **Intrusion detection is the ability to detect attacks against networks, including network devices and hosts.**
- **Exploits 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-53

Summary (Cont.)

Cisco.com

- **A HIPS provides individual host protection and detection.**
- **A NIDS provides broader protection by monitoring network segments.**
- **The Cisco intrusion protection technology includes intrusion detection and security scanning.**
- **The features of an active defense system are detecting, protecting, and reacting.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-54

Summary (Cont.)

Cisco.com

- **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 depends on the following factors: network media, intrusion detection analysis performance, and network environment.**
- **Sensor deployment considerations include the following: number of Sensors needed, Sensor placement, management and monitoring options, and external Sensor communications.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—3-55

Cisco Intrusion Detection System Architecture

Overview

This lesson describes the Cisco Intrusion Detection System (Cisco IDS) architecture.

This lesson includes the following topics:

- Objectives
- Cisco IDS software architecture
- Cisco IDS communication
- User accounts and roles
- Summary

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

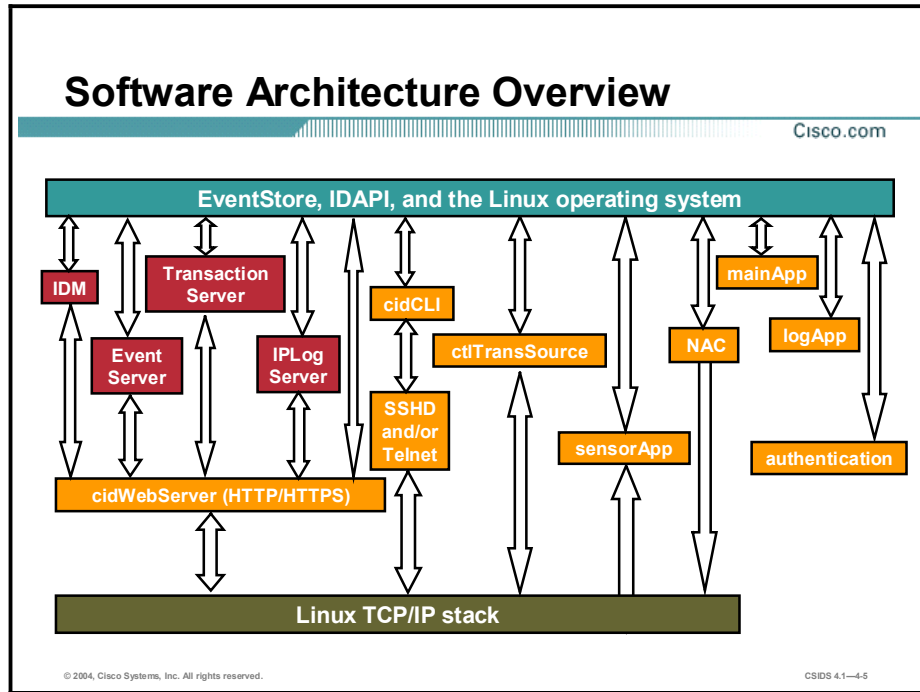
Upon completion of this lesson, you will be able to perform the following tasks:

- 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.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-4.3

Cisco IDS Software Architecture

This topic discusses the Cisco IDS Sensor software architecture.



Cisco IDS 4.x 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 IDS Device Manager (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 bullet points describe the servlets:
 - **IDM**—Provides the IDM web-based management interface.
 - **EventServer**—Used to serve events to external management applications such as IDS Event Viewer (IEV).
 - **TransactionServer**—Allows external management applications such as the Management Center for IDS Sensors (IDS MC) to initiate control transactions with the Sensor. Control transactions are used to configure and control Sensors.
 - **IPLogServer**—Used to serve IP logs to external systems.

Note The EventServer, TransactionServer and IPLogServer 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 Cisco 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 EventStore.
- EventStore—A 4-GB, shared, memory-mapped file where all events are stored. The sensorApp is the only application that writes alert events into the EventStore. All applications may write log, status, and error events into the EventStore.
- cidCLI—The command line interface (CLI) shell application that is started when a user logs into the Sensor. A separate cidCLI process is loaded for each CLI shell. In Cisco IDS 4.x, operating system shell access has been replaced with the CLI, through which most tasks can be performed. Use the CLI or the appropriate Cisco management application for configuration and troubleshooting. Shell access for configuration is no longer supported.

A Sensor running Cisco IDS 4.x is secured by the following:

- Secure Shell (SSH) and Transport Layer Security/Secure Sockets Layer (TLS/SSL) secure interfaces
- CLI access only (no operating system shell access for configuration)
- Role-based user privileges

SensorApp Internals

Cisco.com

The sensorApp consists of the following:

- **virtualSensor**
- **virtualAlarm**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—4.6

The sensing engine, sensorApp, consists of the following:

- **virtualSensor**—Receives packets, processes them, and determines whether 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 Layer 2 inspection, dispatching, and traps for ignored packets. Processes Address Resolution Protocol (ARP) packets and passes Ethernet packets to the next processor
 - **Fragment Reassembly Unit (FRU)**—Reassembles IP Fragments
 - **DatabaseHandler**—Provides internal storage for tracking streams and cross packet analysis
 - **Stream Reassembly Unit (SRU)**—Reassembles and dispatches TCP streams
 - **SignatureHandler**—Controls and dispatches all nonstream 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 only one virtualSensor is supported in Cisco IDS 4.x software, the basic infrastructure is in place to support multiple virtualSensors in future versions.

- **virtualAlarm (Alarm Channel)**—Responsible for the output of the alarms to the downstream IDS EventStore and for performing or starting the EventAction

Cisco IDS Communication

This topic discusses the Cisco IDS communication protocol.

Communications Overview

Cisco.com

- **IDAPI handles internal communications.**
- **RDEP handles external communications.**
- **RDEP uses either HTTP or HTTPS to transmit XML documents between the Sensor and external systems.**
- **RDEP uses a pull communication model.**
 - **The pull communication model allows the management console to pull alarms at its own pace.**
 - **Alarms remain on the Sensor until the 4-GB limit is met. When the limit is met, alarms are overwritten.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—4-6

Cisco IDS 4.x applications use an interprocess communication application-programming interface (API) called Intrusion Detection Application Program Interface (IDAPI) to handle internal communications. IDAPI provides a means to store and share data among Cisco IDS applications. External communications use the Remote Data Exchange Protocol (RDEP). RDEP uses HTTP and TLS/SSL to pass Extensible Markup Language (XML) documents between the Sensor and external systems.

RDEP is an application-level communications protocol used to exchange Cisco 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:

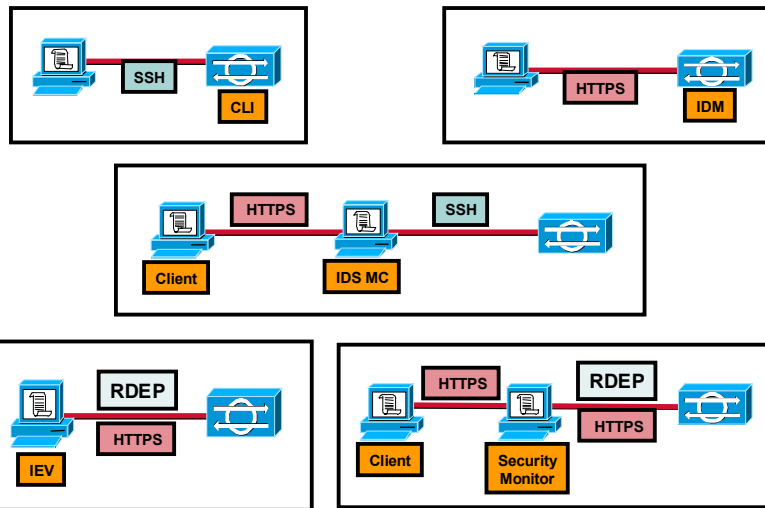
- **Event messages**—Include Cisco IDS alarm, status, and error messages. Monitoring applications such as IEV and the Security Monitor use RDEP's event pull model to retrieve events from the Sensor. The pull model allows the application to pull alarms at its own pace. As soon as the monitoring application 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. Because 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.

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 Cisco.com for more information.

Sensor External Communications

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-4-9

RDEP uses the industry-standard HTTPS to 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:

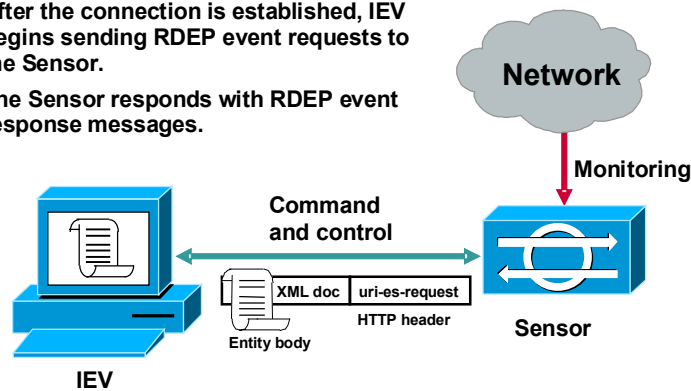
- Communication with monitoring applications—HTTPS
- Network access to the Sensor for management—SSH and HTTPS
- Communication with blocking devices (Cisco IOS software-based routers and PIX Firewalls)—Telnet or SSH

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.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—4-10

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 has been 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 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 that 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 Cisco.com for more information.

User Accounts and Roles

This topic 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.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—4-12

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 privileges.**
- **The following roles can be assigned to an account:**
 - **Administrator**
 - **Operator**
 - **Viewer**
 - **Service**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—4-13

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 topic.

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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—4-14

The service account is a special account that allows the Cisco Technical Assistance Center (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 Cisco 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 topic summarizes what you learned in this lesson.

Summary

Cisco.com

- **The Cisco IDS software consists of the following interoperating applications: mainApp, sensorApp, cidWebServer, authentication, logApp, NAC, ctiTransSource, 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 in to user accounts that you create on the Sensor.**
- **User accounts have roles that determine the privileges of the user on the Sensor.**
- **Create and use a service account only under the direction of TAC for troubleshooting.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—4-16

Getting Started with the IDS Command Line Interface

Overview

This lesson 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 lesson includes the following topics:

- Objectives
- Sensor installation
- Sensor initialization
- Command line modes
- Completing the initial configuration
- Preventive maintenance and troubleshooting
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

- **Install the Sensor software image.**
- **Install the Sensor appliance on the network.**
- **Obtain management access to the Sensor.**
- **Initialize the Sensor.**
- **Navigate the CLI.**
- **Create user accounts.**
- **Configure account lockout.**
- **Configure network access lists.**
- **Describe preventative maintenance practices.**
- **Use general troubleshooting commands.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-5.3

Sensor Installation

This topic explains how to upgrade a Sensor to IDS software version 4.x.

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 into a power source.**
- **Do one of the following:**
 - **Attach a laptop to the console port of the Sensor.**
 - **Connect a keyboard and monitor to the Sensor.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—5-5

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. An uninterruptible power supply (UPS) is recommended.
- Step 3** Use the dual serial communication cable included in the accessory kit to attach a laptop to the console 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

Note You cannot use a monitor and keyboard with the Cisco IDS 4215 Sensor appliance.

Special Considerations

Cisco.com

The following information should be considered before beginning an upgrade to IDS software version 4.x:

- **Cable swap on the 4220 and 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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1–5-6

Before starting an upgrade to IDS software version 4.0, you should be aware of the following special considerations:

- **Cable swap on the 4220 and 4230 Sensors**—If you are upgrading a 4220 or 4230 appliance to software version 4.0 or higher, you must swap the command and control interface cable with the sniffing interface cable before you upgrade the software. For IDS 4.x software, the former command and control interface is now the sniffing interface. If the cables on these models 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 or higher on the 4235 and 4250 appliances. You must apply the BIOS upgrade before installing the 4.0 or 4.1 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 upgrade, for a total of 512 MB of 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-5-7

To upgrade an IDS appliance from IDS Software Version 3.X to 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 you are 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 username **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 eight characters long.

Once the password is successfully set, you are logged into the command line interface (CLI) shell. From there, run the **setup** command to perform the initial configuration.

Signature updates, which include the Network Security Database (NSDB), occur approximately every two weeks. You may not have the latest signature update on the 4.0 CD. You can find the IDS Event Viewer (IEV), 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 are created 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 Management Center for IDS Sensors (IDS MC) provides an easy way to capture the configuration and data on the Sensor for import into 4.0.

Installation Options

Cisco.com

```
console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
[Icons] Clear Line Clear App

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

123,8 | VT400-7 -- COM1 at 9600 baud | Num
```

© 2004, Cisco Systems, Inc. All rights reserved.

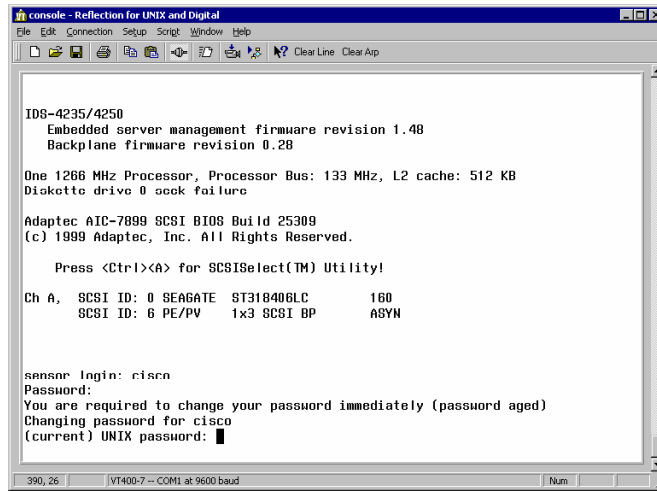
CSIDS 4.1-5-8

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.

Change Password

Cisco.com



```
console - Reflection for UNIX and Digital
File Edit Connection Setup Script Window Help
[Icons] Clear Line Clear Atp

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: █

390,26 VT400-7 -- COM1 at 9600 baud Num
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-5-10

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.

Upgrade from Software Version 4.0 to 4.1

Cisco.com

The upgrade from IDS software version 4.0 to 4.1 is characterized by the following:

- The upgrade can be applied only to 4200 Series Sensor appliances and IDSM-2s.
- The Sensor must report IDS Software Version 4.0(1)S37 or later prior to upgrade.
- The 4210 and 4220 Sensor appliances must be upgraded to 512 MB of RAM prior to upgrade.
- The upgrade can be performed via the upgrade command.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-11

IDS Sensor Software Version 4.1 is a minor update package for IDS 4.0. This update can be applied only to Cisco 4200 Series Sensor appliances and Cisco Catalyst 6500 Intrusion Detection System Modules (IDSM-2s) running software version 4.0(1)S37 or later. If you plan to apply the update to a 4210 or 4220 Sensor appliance, you must also upgrade the memory on the appliance to 512 MB of RAM before proceeding.

To update your Sensor from version 4.0 to version 4.1, complete the following steps:

- Step 1** Log in to Cisco.com using an account with cryptographic privileges.
- Step 2** Download the file `IDS-K9-min-4.1-1-S47.rpm.pkg` to an FTP, SCP, HTTP, OR HTTPS server on your network from the following site: <http://www.cisco.com/cgi-bin/tablebuild.pl/ids4>.

Note Do not change the file name. You must preserve the original file name for the Sensor to accept the update.

- Step 3** Log in to the CLI using an account with administrator privileges.
- Step 4** In global configuration mode, enter the following command (where [URL] is the uniform resource locator pointing to the location of the update package):
- ```
upgrade [URL]/IDS-K9-min-4.1-1-S47.rpm.pkg
```
- For example, to retrieve the update via FTP at 10.0.1.12, enter the following:
- ```
sensor(config)# upgrade ftp://username@10.0.1.12/IDS-K9-min-4.1-1-S47.rpm.pkg
```
- Step 5** Enter the appropriate password when prompted.
- Step 6** To complete the upgrade, type `yes` when prompted.

Sensor Initialization

This topic 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**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—5-13

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.
- **Secure Shell (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 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 date and time.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-14

Sensor initialization tasks are done via an interactive dialog initiated by the **setup** command. The following are those tasks:

- Assign the Sensor a hostname.
- 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.
- Add and remove access control list (ACL) entries that specify which hosts are allowed to connect to the Sensor.
- Set the date and time.

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

```
Tera Term - 10.1.9.201 VT
File Edit Setup Control Window Help
sensor# setup

--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Current Configuration:

networkParams
ipAddress 10.1.9.201
defaultGateway 10.1.9.1
hostname sensor
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
exit
timeParams
summerTimeParams
active-selection none
exit
service webServer
general
ports 443
exit
exit

Current time: Fri Oct 10 16:40:25 2003

Setup Configuration last modified: Fri Oct 10 16:32:28 2003
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1--5-15

Most of the initialization tasks are accomplished by using the Sensor's **setup** command. It walks you through configuring the hostname, 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

```
Tera Term - 10.1.9.201 VT
File Edit Setup Control Window Help
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]:
Modify current access list?(no): yes
Current access list entries:
  [1] 10.0.0.0 255.0.0.0
Delete: 1
Delete:
Permit: 10.0.1.12
Permit:
Modify system clock settings?(no):
The following configuration was entered.
networkParams
ipAddress 10.0.1.4
defaultGateway 10.0.1.2
hostname sensor1
accessList ipAddress 10.0.1.12 netmask 255.255.255.0
exit
timeParams
summerTimeParams
active-selection none
exit
service webServer
general
ports 443
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
Enter your selection[2]:
Configuration Saved.
*17:12:14 UTC Fri Oct 10 2003
Modify system date and time?(no): yes
Local Date[]: 2003-10-10
Local Time[]: 12:28
sensor1#
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-16

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 a series of interactive prompts that enables you to configure the following settings:

- **Hostname**—The hostname 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 IDS Device Manager (IDM), in the format https://sensor_ip_address:port (for example, <https://10.1.9.201:1040>).
- **Network access lists**—The network access list specifies hosts and networks that are allowed to access the Sensor. If you answer **yes** when prompted to modify the network access list, the current access list entries are displayed. You are then prompted to delete entries from the current list. Enter the number corresponding to the entry you want to delete. Repeat this step until you have deleted all the entries that you want to delete from the access list. The access list entries contain a default network address entry, 10.0.0.0/255.0.0.0. Remove this entry, and modify the access list to suit your network. Pressing **Enter** without entering a number retrieves the Permit prompt, which enables you to enter addresses of hosts or networks allowed to access the Sensor. Enter the IP address only to add a single host to the list. Enter the IP address and netmask to add a network

address to the list. Repeat this step until you have entered all the addresses you want to add to the access list. Pressing **Enter** at this point without entering a number retrieves the prompt to modify the system clock settings.

- System clock settings—Answering **yes** when prompted to modify the system clock settings enables you to configure Network Time Protocol (NTP), summer time settings, and the system time zone.
- System date and time—If you answer **yes** when prompted to modify the system date and time, the local date prompt is displayed. Enter the date in the format YYYY-MM-DD. When presented with the local time prompt, enter the time in 24-hour format.

After you respond to the system clock settings prompt, your configuration appears with the options below. If you select **[2]** to save your configuration, you are prompted to modify the system date and time.

- [0] Go to the command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration and exit setup.

Command Line Modes

This topic explains the various CLI modes.

CLI Overview

Cisco.com

The IDS 4.x CLI is characterized by the following:

- **Provides access to the Sensor via Telnet, SSH, serial interface connections, and keyboard/monitor connections**
- **Replaces 3.x operating system shell access**
- **Similar to the Cisco IOS software CLI**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—5-18

The IDS 4.1 software includes a full CLI. The CLI for IDS version 4.1 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 IDS version 4.1 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/HP-UX/Linux
- OpenSSH-3.4p1
- SSH Secure Shell for Servers 3.2

The IDS CLI resembles the Cisco IOS software CLI; however, it has fewer Cisco IOS configuration commands than the Cisco IOS software. It also has additional configuration modes and commands.

CLI Features

Cisco.com

The IDS 4.x CLI includes the following features:

- **Help**
- **Tab completion**
- **Command abbreviation**
- **Command recall**
- **User interactive prompts**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-19

The IDS CLI features the following components:

- **Help**—Enter **?** after the command to display command help. Help displays only 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 have to enter only enough characters for the Sensor to recognize the command as unique. For example, **sh ver** executes the **show version** command.
- **Command recall**—Press the **up arrow** or **down arrow** keys or **Ctrl-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 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 the **tab** key. The Sensor displays the following:

```
sensor# CONFigure
```

An interactive prompt, **—More—**, indicates that the terminal output exceeds the allotted display space. Press the **spacebar** to display the next page of output, or press **Enter** to display the output one line at a time. Press **Ctrl-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

Cisco.com

The CLI can be used to perform the following tasks:

- **Sensor initialization tasks**
- **Configuration tasks**
- **Administrative tasks**
- **Troubleshooting**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-20

The CLI can be used to perform the following:

- **Sensor initialization tasks**—Sensor initialization tasks include such tasks as assigning the Sensor 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

Cisco.com

The IDS 4.x 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-21

The CLI 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5.22

The first level of the CLI is the privileged EXEC mode. This mode enables you to perform such tasks as initializing the Sensor, and displaying 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 topic 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 hostname.
 - Create user accounts.
 - Configure SSH, Telnet, and TLS settings.
 - Reimage the application partition.
 - Upgrade and downgrade system software and signatures.
 - Enter interface configuration modes.
 - Enter service configuration mode.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-23

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

Cisco.com

```
sensor# configure terminal
sensor(config)# interface command-control
sensor(config-if)#
```

- Interface command-control configuration mode is a third level of the CLI.
- Interface command-control configuration mode enables you to configure interface IP information.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-24

The interface command-control configuration 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

Cisco.com

```
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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-25

The interface group configuration mode is a third level of the CLI. The interface group command enables you to enter interface group configuration mode. From this mode, you can add or remove interfaces from the group of monitoring interfaces used by sensorApp or shut down the group, which disables monitoring on all interfaces within the group.

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.
- Interface sensing configuration mode allows you to enable or disable the sensing interface.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-26

The interface sensing configuration mode is a third level of the CLI. It enables you to enable or disable the sensing interface. In IDS software version 4.1, sensing interfaces are disabled by default. You must enable at least one sensing interface to allow your Sensor to monitor traffic. 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

Cisco.com

```
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
```

- Service mode is a generic command mode.
- It enables you to enter configuration mode for various services.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-27

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

Cisco.com

```
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 tune micro engines mode.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-28

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

Cisco.com

```
sensor# configure terminal
sensor(config)# service alarm-channel-configuration
virtualAlarm
sensor(config-acc)#
```

- Alarm channel configuration mode is a third level of the CLI.
- Alarm channel configuration mode enables you to enter configuration mode for the alarm channel.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-29

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.
- It enables you to tune micro-engines.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-30

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:

```
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
                          MinHits and Summarize counting. For best
                          performance, use a StorageKey of xxxx.
for
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
                          inspection.
this
FragmentReassembly       Fragment Reassembly configuration tokens.
IPLog                     Virtual Sensor IP log configuration tokens
OTHER                     This engine is used to group generic
                          signatures so that 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 de-obfuscation.
SERVICE.IDENT	Ident service (client and server) alarms.
SERVICE.MSSQL	Microsoft (R) SQL service inspection engine.
SERVICE.NTP engine.	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.
- It enables you to configure system variables for the alarm aggregation process.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-31

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
```

Completing the Initial Configuration

This topic explains the commands needed to complete the initial Sensor configuration.

Initial Configuration Tasks

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.**
- **(Optional.) Add hosts to the network ACL.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—5-33

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.
- Create network ACLs to specify hosts that are allowed to connect to the Sensor.

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 be used by only one user
- Has service role

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-34

Following are the two types of management accounts and their characteristics:

- User accounts—Enable 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 practice 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.

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-35

Use the **username** command to create user accounts. The **show users all** command displays a list of all user accounts with the usernames of locked accounts in parentheses.

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]
```

Command	Description
<i>name</i>	Specifies the username. A valid username is 1–32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).
<i>password</i>	Specifies the password for the user.
<i>privilege</i>	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 IEV, only require viewer access to the Sensor. You can use the CLI to setup a user account with viewer privileges and then configure IEV to use this account to connect to the Sensor. Viewers can:
 - View configuration and event data.
 - 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-36

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 be used only for troubleshooting under the direction of the Cisco Technical Assistance Center (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.

Configuring Account Lockout

Cisco.com

```
sensor(config-Authentication-gen)#
```

```
attemptLimit limit
```

- Limits the number of authentication attempts before the account becomes disabled

```
sensor(config-Authentication-gen)# attemptLimit 3
```

- Sets the maximum number of authentication attempts to three

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-37

You can use the **attemptLimit** command to limit the number of times a user can attempt authentication before the account becomes disabled. Disabled accounts appear in parentheses when you execute the **show users all** command. A user with administrative privileges can unlock a disabled account by changing the account password. To use the **attemptLimit** command, complete the following steps:

- Step 1** Enter the authentication service configuration mode:
- ```
sensor(config)# service authentication
sensor(config-Authentication)#
```
- Step 2** Enter the general submode:
- ```
sensor(config-Authentication)# general  
sensor(config-Authentication-gen)#
```
- Step 3** Use the **attemptLimit** command to set the attempt limit:
- ```
sensor(config-Authentication-gen)# attemptLimit 3
sensor(config-Authentication-gen)#
```
- Step 4** Exit the general submode:
- ```
sensor(config-Authentication-gen)# exit  
sensor(config-Authentication)#
```
- Step 5** Exit the authentication service configuration mode:
- ```
sensor(config-Authentication)# exit
sensor(config)#
```
- Step 6** Press **Enter** to apply your changes:
- ```
Apply Changes:? [yes]: <Enter>
```

The syntax for the **attemptLimit** command is as follows:

attemptLimit *limit*

Command	Description
<i>limit</i>	Number of failed login attempts allowed before the account is disabled. The default is 0, which means that account locking is disabled.

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5.38

You can use the **password** command to change the password for an existing user or to re-enable a disabled account. Users with administrator privileges can change the passwords of other users. Users with operator and viewer privileges can modify only 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]]
```

Command	Description
name	Specifies the username. A valid username is 1–32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).
newPassword	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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-39

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]
```

Command	Description
<i>name</i>	Specifies the username. A valid username is 1–32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).

Configuring Network Access

Cisco.com

```
sensor(config-Host-net)#
```

```
accessList ipAddress ip_address [netmask netmask]
```

- Creates a network ACL

```
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 ACL

```
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 ACL

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-40

Use the **accessList** command to modify the network ACLs to allow remote access. The **accessList** command enables the network security administrator to set any number of IP addresses (either host or network) that 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 practice 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 ACLs are configured within the host service. To configure the ACL, 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 the network parameters submode:

```
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 ACL. 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 ACL.

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: sensor
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]
```

Command	Description
<i>ipAddress</i>	IP address of host that is allowed to access the Sensor or network address of a network that is allowed to access the Sensor.
<i>netmask</i>	Netmask applied to <i>ip_address</i> .

Preventive Maintenance and Troubleshooting

This topic describes commands that can be used for preventive maintenance and troubleshooting.

Displaying the Current Version

Cisco.com

```
sensor#  
show version
```

- Displays version information for all installed operating system packages, signature packages, and IDS processes running on the system

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—5-42

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:

- The applications that 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 4.1(1)S47
```

```
OS Version 2.4.18-5smpbigphys  
Platform: IDS-4210
```

```
Using 255578112 out of 509276160 bytes of available memory (50% usage)  
Using 603M out of 17G bytes of available disk space (4% usage)
```

```
MainApp          2003_Jun_20_06.00  (Release)  2003-06-  
20T05:53:31-0500  Running
```

AnalysisEngine	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500	Running		
Authentication	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500	Running		
Logger	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500	Running		
NetworkAccess	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500	Running		
TransactionSource	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500	Running		
WebServer	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500	Running		
CLI	2003_Jun_20_06.00	(Release)	2003-06-
20T05:53:31-0500			

Upgrade History:

* IDS-K9-maj-4.0-1-S36	11:50:24 UTC Thu Oct 09 2003
IDS-K9-min-4.1-1-S47.rpm.pkg	14:54:49 UTC Fri Oct 10 2003

Recovery Partition Version 1.1 - 4.0(1)S37

Displaying the Configuration

Cisco.com

sensor#

```
show configuration | [begin | exclude | include  
filter]
```

- Displays the current configuration for the entire system

```
sensor# show configuration | include accessList  
accessList ipAddress 10.0.1.12 netmask  
255.255.255.255  
accessList ipAddress 10.0.2.0 netmask  
255.255.255.0
```

- Displays only the accessList portions of the current configuration

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-43

Use the **show configuration** command to display all or part of the system configuration.

The syntax for the **show configuration** command is as follows:

```
show configuration | [ begin | exclude | include filter]
```

Command	Description
begin	Causes the output to start with the first line that matches the filter.
exclude	Causes the output to exclude all lines that match the filter.
include	Causes the output to include only lines that match the filter.
filter	A regular expression.

The following is an example of partial **show configuration** output when the command is used with no options:

```
sensor# show config  
! -----  
service Authentication  
general  
methods method Local  
exit  
exit  
exit  
! -----  
service Host  
networkParams  
ipAddress 10.0.1.4  
defaultGateway 10.0.1.2  
hostname sensor
```

```

accessList ipAddress 10.0.1.12 netmask 255.255.255.255
accessList ipAddress 10.0.2.0 netmask 255.255.255.0
exit
optionalAutoUpgrade
active-selection none
exit
timeParams
summerTimeParams
active-selection none
exit
exit
exit
! -----
service Logger
masterControl
enable-debug false
exit
zoneControl zoneName Cid
severity debug
exit
zoneControl zoneName AuthenticationApp
severity warning
exit
zoneControl zoneName Cli
severity warning
exit
zoneControl zoneName ctlTransSource
severity warning
exit
zoneControl zoneName IdapiCtlTrans
severity warning
exit
zoneControl zoneName IdsEventStore
severity warning
exit
zoneControl zoneName MpInstaller
severity warning
exit
zoneControl zoneName tls
severity warning
exit
exit
! -----
service NetworkAccess
general
allow-sensor-shun false
shun-enable true
exit

```

```
exit
! -----
service SshKnownHosts
exit
! -----
service TrustedCertificates
exit
! -----
service WebServer
exit
! -----
interface group 0
sensing-interface int0
exit
interface sensing int0
exit
! -----
service virtual-sensor-configuration virtualSensor
tune-micro-engines
ATOMIC.ARP
signatures SIGID 7101 SubSig 0
exit
signatures SIGID 7102 SubSig 0
exit
signatures SIGID 7104 SubSig 0
exit
signatures SIGID 7105 SubSig 0
exit
exit
ATOMIC.ICMP
signatures SIGID 2000 SubSig 0
exit
signatures SIGID 2001 SubSig 0
exit
signatures SIGID 2002 SubSig 0
--MORE--
```

Displaying the Configuration (Cont.)

Cisco.com

sensor#

```
more keyword | [begin | exclude | include filter]
```

- Displays the current or backup configuration

```
sensor# more backup-config
```

- Displays the backup configuration

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-44

You can use the **more** command to view your current or backup configuration.

The syntax for the **more** command is as follows:

```
more keyword | [ begin | exclude | include filter ]
```

Command	Description
keyword	The keyword current-config displays the current running configuration. The keyword backup-config displays the backup configuration.
begin	Causes the output to start with the first line that matches the filter.
exclude	Causes the output to exclude all lines that match the filter.
include	Causes the output to include only lines that match the filter.
filter	A regular expression.

Displaying Settings

Cisco.com

sensor(config)#

```
show settings [terse] [begin | exclude | include  
filter]
```

- Displays the contents of the configuration contained in the current submode

```
sensor(config)# show settings
```

- Displays all high-severity events since 10:00 a.m., June 1, 2003

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-45

Use the **show settings** command to display the contents of the configuration contained in the current sub-mode. This command is available in several of the service sub-modes and is useful for troubleshooting. For example, it facilitates the troubleshooting of blocking by enabling you to view all settings for the Network Access Controller (NAC).

The **show settings** command is also especially useful in the tune micro engines sub-mode. Used with no options, this command displays all signature parameter settings. When used with the **terse** option, it displays only the signature ID.

The syntax for the **show settings** command is as follows:

```
show settings [terse] [ begin | exclude | include filter]
```

Command	Description
terse	Reduces the amount of detail displayed.
begin	Causes the output to start with the first line that matches the filter.
exclude	Causes the output to exclude all lines that match the filter.
include	Causes the output to include only lines that match the filter.
filter	A regular expression.

Displaying Events

Cisco.com

sensor#

```
show events
[alert [informational] [low] [medium] [high]
[include-traits must-have-traits] [exclude-traits
must-not-have-traits] | error [warning | error |
fatal ] | log | NAC | status] [[past] hh:mm:ss
[month day [year]]] [| {begin filter | include
filter | exclude filter}]
```

- 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 a.m., June 1, 2003

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-46

Events are the data generated by the Sensor applications, such as the alerts generated by the sensorApp or errors generated by an 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—Shun 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 Remote Data Exchange Protocol (RDEP) communications. Management applications such as IEV and the Monitoring Center for Security use RDEP to retrieve events from the Sensor. Events can also be viewed from the CLI's top-level prompt using the **show events** command. 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 **Ctrl-C**.

This command is helpful for troubleshooting event capture issues in which you are not seeing events in IEV or the Monitoring Center for Security, 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 Intrusion Detection Interaction and Operations Messages (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] [include-traits must-have-traits][exclude-traits must-not-have-traits] | error [warning | error | fatal ] | log | NAC | status]
[[past] hh:mm:ss [month day [year]]] [ {begin filter | include filter | exclude filter}]
```

Command	Description
alert	Display alerts. Provides notification of some suspicious activity that may indicate that 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, or high), all alert events are displayed.
include-traits	Includes only alerts for which all of the specified traits are true. Filters evAlert events based on the alarmTraits signature tuning parameter.
must-have-traits	A list of bit numbers or ranges of bit numbers.
exclude-traits	Excludes alerts for which any of the specified traits are true. Filters evAlert events based on the alarmTraits signature tuning parameter.
must-not-have-traits	A list of bit numbers or ranges of bit numbers.
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.
past	Display events starting at the current time minus hh:mm:ss.
hh:mm:ss	Start time in hours (24-hour format), minutes, and seconds.
month	Start month (by name).
day	Start day (by date) in the month.
year	Start year.
begin	Causes the output to start with the first line that matches the filter.
exclude	Causes the output to exclude all lines that match the filter.
include	Causes the output to include only lines that match the filter.
filter	A regular expression.

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: sensor
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 EventStore

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-47

Statistics provide a snapshot of the current internal state of Sensor services; 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 ]
```

Command	Description
Authentication	Display authorization authentication statistics.
EventServer	Display Event Server statistics.
EventStore	Display EventStore statistics.
Host	Display host (main) statistics.
Logger	Display logger statistics.
NetworkAccess	Display NAC statistics.
TransactionServer	Display transaction server statistics.
TransactionSource	Display transaction source statistics.
WebServer	Display web server statistics.
clear	Clear 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-48

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
```

Command	Description
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 whether 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-49

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, operating system 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]
```

Command	Description
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 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

Cisco.com

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.
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-50

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 that question are “yes” and “no.” “Y” and “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]

Command	Description
powerdown	This option causes the Sensor to enter a state in which the power can be turned off after the applications are shut down.

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 backup configuration

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-51

You can use the **copy** command to make a snapshot of a good configuration. This practice enables you to copy the current configuration to a backup configuration and to restore the current configuration from a backup.

The syntax for the **copy** command is as follows:

```
copy [/erase]source-url destination-url
```

```
copy iplog log-id destination-url
```

Command	Description
/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 the file to copy.

Keywords are used to designate the file location on the Sensor. The following keywords are supported:

Keyword	Description
current-config	The current running configuration. This configuration, unlike Cisco IOS Software Version 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
backup-config	Storage location for configuration backup. The file format is CLI commands.

Keyword	Description
iplog	An IP log contained on the system.

The **copy** command can be used to do any of the following:

- Transfer a 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 back up 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 backup configuration:

```
sensor# copy /erase backup-config current-config
```

Recovering the Application Partition

Cisco.com

```
sensor(config)#
```

```
recover application-partition
```

- Reimages 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.
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-52

The Sensor has two partitions, application and recovery. There is no separate operating system partition. The operating system 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 parameters are reset to default; therefore, consider backing up the current configuration before initiating recovery.

Note This information does not apply to the IDSM-2. For information on recovering the software image on the IDSM-2, go to the following web site: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/15620_01.htm#1034689.

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **Obtain management access to a Sensor 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.**
- **IDS Software Versions 4.0 and higher include a full CLI.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-54

Summary (Cont.)

Cisco.com

- **The CLI uses syntax similar to that of the Cisco IOS software.**
- **The CLI provides all the necessary functionality to configure and manage the Sensor.**
- **The CLI provides several troubleshooting features.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—5-55

Sensor Management and Monitoring

This lesson introduces the Cisco Intrusion Detection System (IDS) Device Manager (IDM) and IDS Event Viewer (IEV). The installation and use of IEV is explained. This lesson includes the following topics:

- Objectives
- IDS Device Manager overview
- IDS Event Viewer overview
- IDS Event Viewer installation
- IDS Event Viewer views
- IDS Event Viewer filters
- Network Security Database
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

Upon completion of this lesson, 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.
- Describe the NSDB.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-6-2

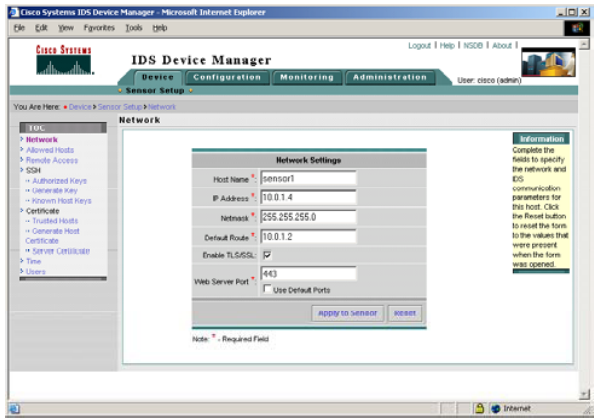
IDS Device Manager Overview

This topic discusses the features and benefits of the IDS Device Manager (IDM).

IDS Device Manager

Cisco.com

- Web-based device configuration tool
- Software installed on the Sensor by default
- For small-scale Sensor deployments



© 2004, Cisco Systems, Inc. All rights reserved. CS-IDS 4.1-6-4

A network Sensor appliance can be managed via the IDS Device Manager (IDM). IDM is a web-based tool that resides on your Sensor and enables you to configure and manage the Sensor. IDM is accessed securely via Secure Sockets Layer (SSL) and Transport Layer Security (TLS) using the Netscape or Internet Explorer web browsers. Because IDM resides on your Sensor, it can only manage one Sensor at a time. It is best suited for small-scale Sensor deployments where there are no more than five Sensors.

IDM Features and Benefits

Cisco.com

- **Web-based embedded architecture**
- **Secure communication (TLS/SSL)**
- **Task-based GUI**
- **Signature grouping**
- **Signature customization**
- **Sensor system administration**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-6-5

IDM enables you 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.

IDM enables you to remotely:

- Re-start 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**

© 2004, Cisco Systems, Inc. All rights reserved.

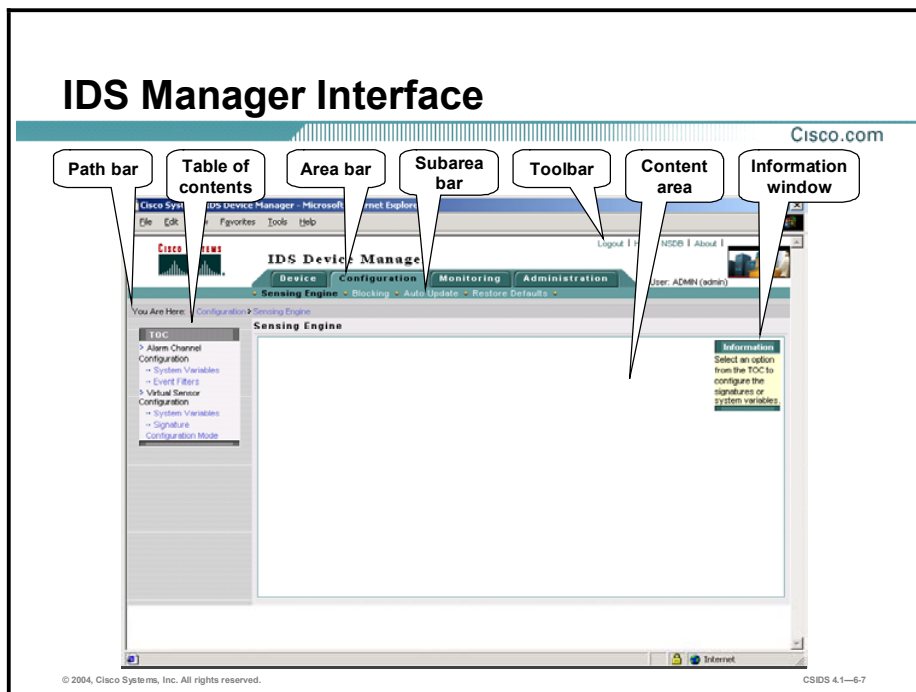
CSIDS 4.1—6.6

IDM is a web-based application running on the Sensor. The following is information about the supported clients:

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.

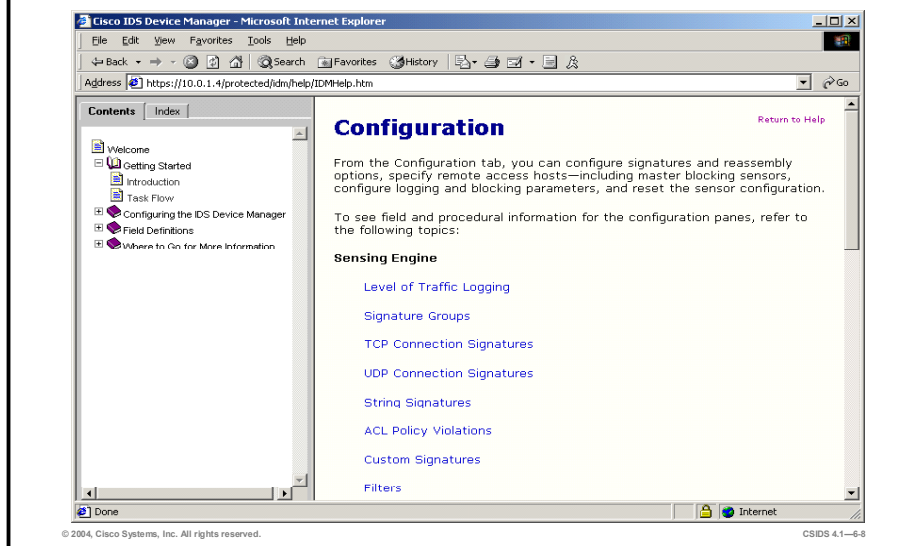


The IDM GUI provides you with an intuitive approach to configuring Sensors. The GUI has the following sections:

- Path bar—Displays the current selection. In the figure, the 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.
- Toolbar—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.com



IDM provides online documentation to assist in the configuration of the Sensor. To access the online IDM, choose **Help** from the IDM toolbar. The IDM Help Contents are displayed in a new web browser.

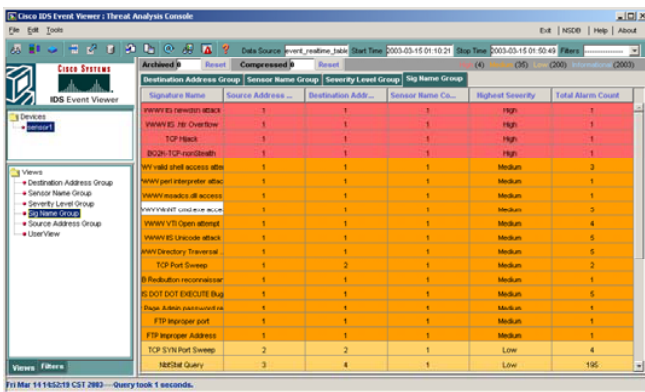
IDS Event Viewer Overview

This topic discusses the features and benefits of the IDS Event Viewer (IEV).

IDS Event Viewer

Cisco.com

- Windows NT or Windows 2000
- Download from Cisco.com
- Provides event monitoring for up to five Sensors



Signature Name	Source Address	Destination Addr.	Sensor Name Co.	Highest Severity	Total Alarm Count
Worms ES_ircdnet attack	1	1	1	High	1
Worms ES_Overflow	1	1	1	High	1
TCP flood	1	1	1	High	1
SQLM-TCP-overflow	1	1	1	High	1
WV valid shell access attack	1	1	1	Medium	3
Worms perl interpreter attack	1	1	1	Medium	1
Worms msrpc attack	1	1	1	Medium	1
Worms netcmd attack	1	1	1	Medium	3
Worms VBS Open attack	1	1	1	Medium	4
Worms ES_Unicode attack	1	1	1	Medium	5
Worms Director Traversal	1	1	1	Medium	5
TCP Port Sweep	1	2	1	Medium	2
IP Fragmentation reconstruction	1	1	1	Medium	1
IS DOT DOT EXECUTE flag	1	1	1	Medium	5
Open Admin password attack	1	1	1	Medium	1
FTP wrapper port	1	1	1	Medium	1
FTP wrapper Address	1	1	1	Medium	1
TCP SYN Port Sweep	2	2	1	Low	4
NETSOL Query	3	4	1	Low	145

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-6-10

IEV is a Java-based application that enables you to view and manage alarms for up to five Sensors. You can use 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 lesson:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ids-ev>

IEV Features and Benefits

Cisco.com

- **Downloadable from Cisco.com to an appropriate host**
- **Event monitoring for IDS devices**
- **Customizable event views**
- **Scalable event storage database**
- **NSDB**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-11

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
Windows XP	Service Pack 1

IEV can be installed on a system that meets or exceeds the following minimum hardware requirements:

- Processor—Pentium III, 800 MHz or greater
- Memory—256 MB
- Disk space—500 MB

The following table shows the browser requirements for IEV:

Browser	Version
Netscape Navigator	4.7 and higher
Internet Explorer	5.5 and higher

IEV installs and uses the following support applications:

- Java 2 Runtime Environment version 1.3.1
- MySQL Server version 3.23

IDS Event Viewer Installation

This topic describes how to install and configure IDS Event Viewer (IEV) to monitor events from an IDS device.

Getting Started

Cisco.com

Complete the following tasks to start using the IEV:

- 1. Download the IEV software from Cisco.com.**
- 2. Install the IEV software on the host.**
- 3. Reboot the IEV host to start IDS services.**
- 4. Add IDS devices that the IEV will monitor.**

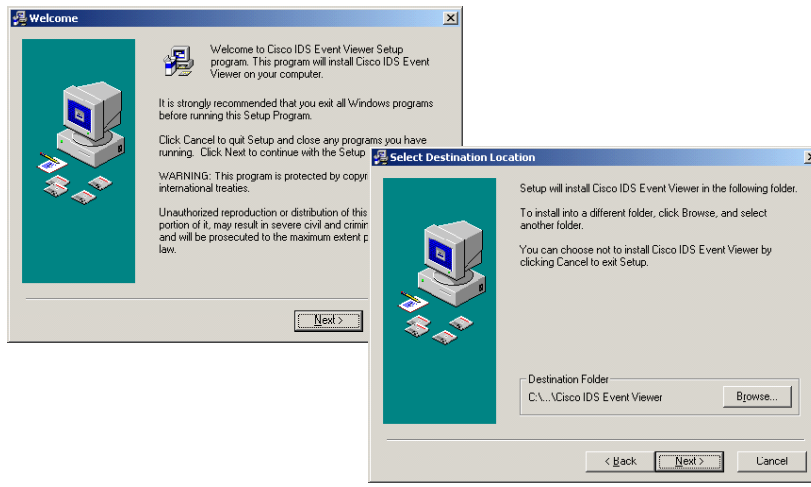
© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—6-14

Complete the following tasks to begin using IEV to monitor events from an IDS device:

- Step 1** Download the IEV software from Cisco.com.
- Step 2** Install the IEV software on the host—This step includes starting the IEV setup program and continuing with the installation wizard.
- Step 3** Reboot the IEV host to start the IDS services—This step includes rebooting the IEV host in order to initialize the IDS services needed by IEV.
- Step 4** Add IDS devices that IEV is to monitor—This step includes specifying the IDS devices from which the IEV application accepts events.

IEV Installation

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-15

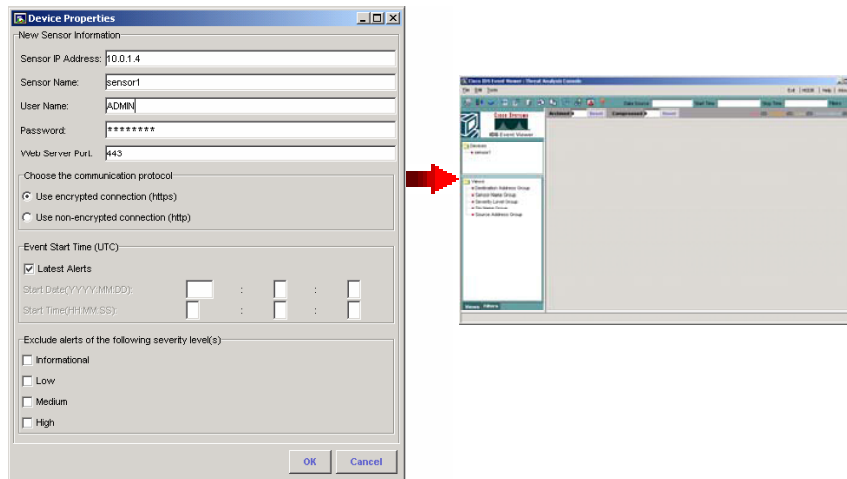
The IEV installation application is a wizard-based installation program. Complete the following steps to install the IEV application:

- Step 1** Launch the IEV installation application from the location to which 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.
- Step 6** The IEV application files are copied to the destination location. The IEV file copy process takes approximately 5 to 7 minutes, depending on system performance.
- Step 7** Click **Finish** to complete the IEV installation process. The Install dialog window opens.
- Step 8** Click **OK** to restart the system and complete the installation process.

Add IDS Devices

Cisco.com

Choose File > New > Devices.



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 IEV:

- Step 1** Choose **Start > Programs > Cisco Systems > Cisco IDS Event Viewer > Cisco IDS Event Viewer** to launch 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 IEV, specify the username and password for that account.

- Step 4** To specify the communication protocol that IEV should use when connecting to the Sensor, select either the **Use encrypted connection (https)** or the **Use non-encrypted connection (http)** radio button. The 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. IEV will receive alerts from the Sensor, starting with the first alert the Sensor receives after connecting to IEV.

- De-select the **Latest Alerts** check box to pull all alerts from the Sensor EventStore. 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 from the Exclude alerts of the following severity levels section to exclude alarms of specific severity levels:

- Informational
- Low
- Medium
- High

Step 7 Click **OK** to close the Device Properties panel. IEV sends a subscription request to the Sensor, and the Sensor appears in the Devices folder on the left side of the screen. The subscription request remains open until you modify the device properties or delete the device.

Note If you specified HTTPS as the communication protocol, 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 IEV and the Sensor.

You can check the status of your Sensor by right-clicking the Sensor icon in the Devices folder and choosing **Device Status** from the drop-down menu. The Device Status window opens and displays the connection status.

IDS Event Viewer Views

This section describes the IDS Event Viewer (IEV) view concept and provides instructions on how to navigate, modify, and create views.

IEV Views Overview

Cisco.com

- **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 a different data source.**
- **The level of alarm detail is customizable.**
- **A graph view displays alarm data in either an area format or a bar graph format.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—6-18

IEV displays alarm data as views. Views aggregate the IDS alarm data to provide you with a high-level overview. IEV has default views that can be customized to meet your needs. 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.

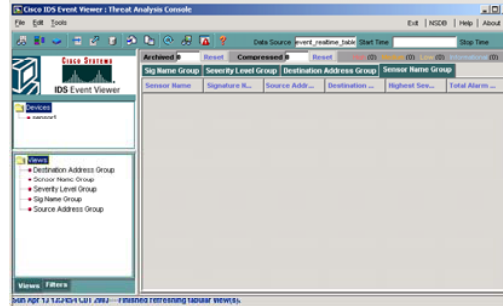
The event views are refreshed periodically according to the parameters defined in the Refresh Cycle preferences. By default, the refresh interval is every minute. To modify the refresh interval, choose **Edit > Preferences** from the main menu. Then select the **Refresh Cycle** tab in the Preferences window that opens.

IEV Default Views

Cisco.com

IEV has the following default views:

- Destination Address Group
- Sensor Name Group
- Severity Level Group
- Sig Name Group
- Source Address Group



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-19

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 name
- Source Address Group—Groups the alarm data by the source address

You can also create your own views to customize the data that is displayed when an event is reported. To create a view, choose **File > New > View** from the main menu. The View Wizard opens and leads you through creating a view.

Navigating Views

Cisco.com

The screenshot shows the Cisco IDS Event Viewer interface. The main window displays a table of security events with columns for Signature Name, Source Address, Destination Address, Service Name, Highest Severity, and Total Alarm Count. The 'Sig Name Group' view is active in the sidebar.

Signature Name	Source Addr...	Destination A...	Service Name...	Highest Seve...	Total Alarm ...
Too Many Frag...	2	2	1	Informational	11373
IDS Evasive Enc...	1	1	1	Informational	4994
WWW Directory Traversal /...	1	1	1	Medium	3730
Oracle SAS Web Cache Buffer Overflow	1	1	1	High	3644
Lotus Domino database DOS	1	1	1	Low	3643
Troil Storage Manager Client Acceptor Overflow	1	1	1	Medium	3572
ICMP Echo Reply	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	303
streamer 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	148
IOS Udp Bomb	1	1	1	Medium	142
WWW bad file	1	1	1	Medium	138

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-6-20

- 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.

Whole Details

Cisco.com

WWW campas	Expand Whole Details	1
WWW WinNT cmd.	NSDB Link...	1
WWW IIS Unicod	Set Status To	1
WWW Directory Tr	Delete Row from Database	1
Password File Access Att		1
IS DOT DOT EXECUTE Bug		1

Expanded Details Dialog

Signature Name: "WWW campas attack" (View - "Sig Name Group")

Class A Level	Class B Level	Class C Level	Whole Address		
Source Address	Destination Address	Sensor Name	Severity Level	Total Alarm Count	
10.0.0.12	10.0.1.12	sensor1	Medium	5	

Select All

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-6-21

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

The screenshot displays two windows from the Cisco Security Manager interface. The top window, titled "Expanded Details Dialog", shows a summary for a "WWW campus attack" with a severity level of "Medium" and a total alarm count of "5". A context menu is open over the source address "10.0.6.12", with "View Alarms" selected. The bottom window, titled "Alarm Information Dialog", displays a table of alarm events.

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst
WWW campus attack	3200	Medium	sensor1	2003-04-17 14:33:34	2003-04-17 14:33:34	10.0.6.12	
WWW campus attack	3200	Medium	sensor1	2003-04-17 14:27:04	2003-04-17 14:27:04	10.0.6.12	
WWW campus attack	3200	Medium	sensor1	2003-04-17 14:26:23	2003-04-17 14:26:23	10.0.6.12	
WWW campus attack	3200	Medium	sensor1	2003-04-17 14:09:27	2003-04-17 14:09:27	10.0.6.12	
WWW campus attack	3200	Medium	sensor1	2003-04-17 13:54:30	2003-04-17 13:54:30	10.0.6.12	

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-22

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 of 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

The screenshot shows the 'Alarm Information Dialog' window. It contains a table with the following data:

Signature Name	Sig ID	Severity Level
WWW cs		Medium
WWW cs		Medium
WWW cs		Medium
WWW cs		Medium
WWW cs		Medium

A context menu is open over the first row, with 'Show Context' selected. Below the table, a 'Decoded Alarm Context' window is displayed, showing the following text:

```
Decoded Alarm Context(Signature Name='WWW campas attack' Event ID='1050340041921823346' Device Name='sensor1' Event UTI  
From attacker: GET /Dir1%20GET%20/cgi-bin/campas?%0acat%0a/etc/passwd%0a%20HTTP/1.0 HTTP/1.1
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-23

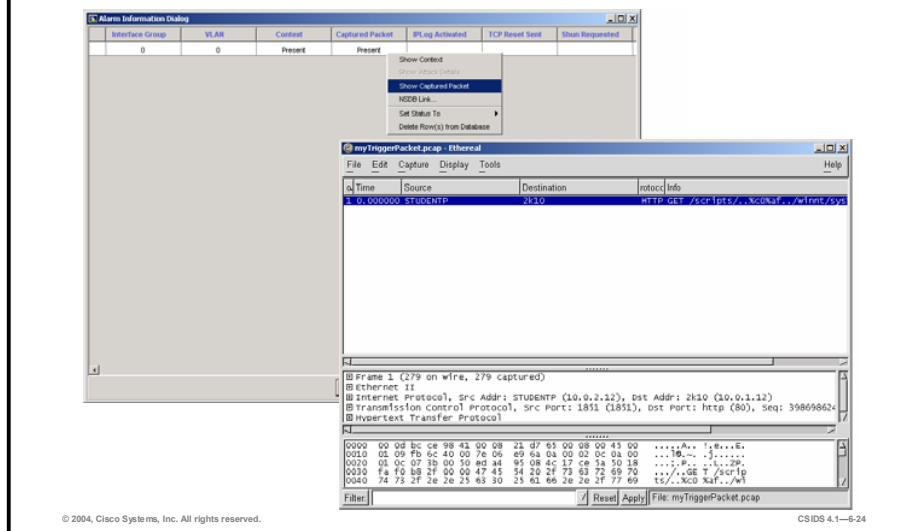
For TCP-based signatures, the Sensor captures up to 256 characters of the TCP stream, which may be examined from the Event Viewer. This is called the context data buffer and it contains keystrokes, data, or both in the connection stream around the string of characters that triggered the signature. This 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
```

Viewing the Trigger Packet

Cisco.com



If you configure the Sensor to capture the packet that triggers an alarm, the alarm will contain captured packet data that you can view. If Ethereal is installed on your system, you can view the fully decoded output, including the IP header information. If you do not have Ethereal, you can view the hexadecimal ASCII code representation of the trigger packet in IEV.

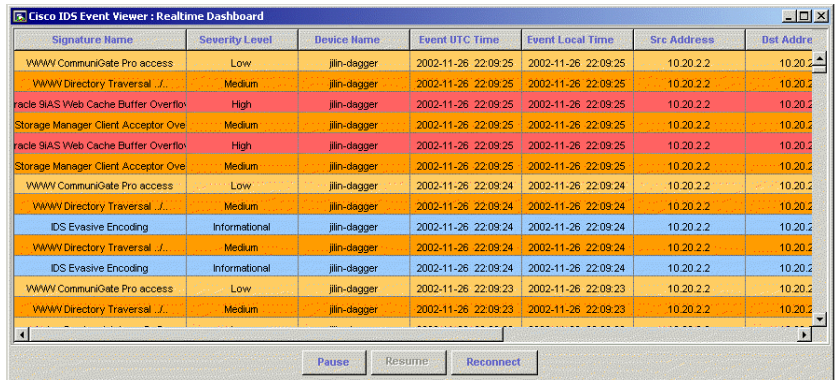
Complete the following steps to view the captured packet for an alarm:

- Step 1** From the Alarm Information Dialog or Realtime Dashboard, locate the alarm with the captured packet you want to view. If an alarm has a captured packet, the word present appears in the corresponding cell of the Captured Packet column. A blank cell indicates that no packet was captured.
- Step 2** Right-click the corresponding cell in the Captured Packet column, and select **Show Captured Packet**.
- Step 3** If Ethereal is installed on the system and the path to the Ethereal executable is set correctly in the Application Settings panel, the trigger packet is displayed in Ethereal.
- Step 4** If Ethereal is not installed on the system, an error message appears. Click **OK** to close the error message. The Captured Packet dialog appears and displays the hexadecimal ASCII code representation of the trigger packet.

Note Ethereal is a network protocol analyzer for Windows that enables you to examine data from a live network or from a captured file. You can interactively browse the captured data and view summary and detail information for each packet, including the reconstructed stream of a TCP session.

Realtime Dashboard

Cisco.com



The screenshot shows a window titled "Cisco IDS Event Viewer : Realtime Dashboard". It contains a table with the following columns: Signature Name, Severity Level, Device Name, Event UTC Time, Event Local Time, Src Address, and Dest Address. The table lists several events, including "WWW CommuniGate Pro access", "WWW Directory Traversal", "race SIAS Web Cache Buffer Overflow", and "Storage Manager Client Acceptor Ove". The severity levels range from Low to High. At the bottom of the window, there are three buttons: "Pause", "Resume", and "Reconnect".

Signature Name	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dest Address
WWW CommuniGate Pro access	Low	jlin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2.2
WWW Directory Traversal /...	Medium	jlin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2.2
race SIAS Web Cache Buffer Overflow	High	jlin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2.2
Storage Manager Client Acceptor Ove	Medium	jlin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2.2
race SIAS Web Cache Buffer Overflow	High	jlin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2.2
Storage Manager Client Acceptor Ove	Medium	jlin-dagger	2002-11-26 22:09:25	2002-11-26 22:09:25	10.20.2.2	10.20.2.2
WWW CommuniGate Pro access	Low	jlin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2.2
WWW Directory Traversal /...	Medium	jlin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2.2
IDS Evasive Encoding	Informational	jlin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2.2
WWW Directory Traversal /...	Medium	jlin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2.2
IDS Evasive Encoding	Informational	jlin-dagger	2002-11-26 22:09:24	2002-11-26 22:09:24	10.20.2.2	10.20.2.2
WWW CommuniGate Pro access	Low	jlin-dagger	2002-11-26 22:09:23	2002-11-26 22:09:23	10.20.2.2	10.20.2.2
WWW Directory Traversal /...	Medium	jlin-dagger	2002-11-26 22:09:23	2002-11-26 22:09:23	10.20.2.2	10.20.2.2

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**. 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. IEV stops populating the Realtime Dashboard with events.
- Step 3** Click **Resume** to resume the stream of real-time events. 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 IEV opens a new subscription with the Sensor.

Note You can also view events in a Realtime Graph or Statistical Graph. To view the Realtime Graph, select **Tools > Realtime Graph**. To view a Statistical Graph, right-click a view and select **Statistical Graph**.

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**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—6-27

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 you 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 one or more of 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.

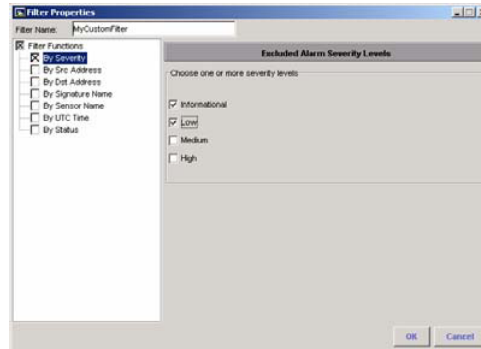
Note Only one filter can be applied to a view at a time.

Filter Properties—By Severity

Cisco.com

Select the alarm severity levels to add to the filter:

- Informational
- Low
- Medium
- High



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-28

Complete the following steps to add an alarm severity level to the filter:

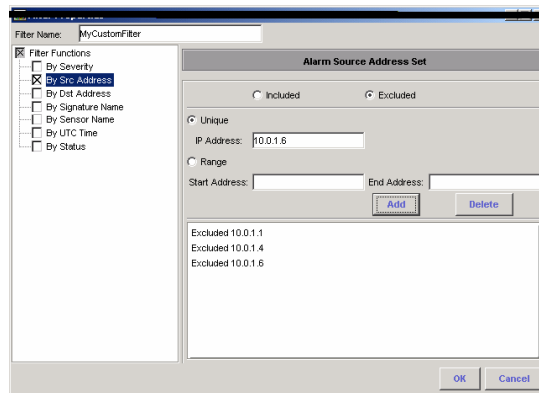
- Step 1** Enable the severity function by selecting the **By Severity** check box from the Filter Functions options. The Excluded Alarm Severity Levels information is displayed. Notice the Filter Functions check box is enabled.
- Step 2** Add the severity levels to the filter by selecting the appropriate 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

Cisco.com

- Add unique IP addresses.
- Add a range of IP addresses:
 - Start address
 - End address



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-29

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:

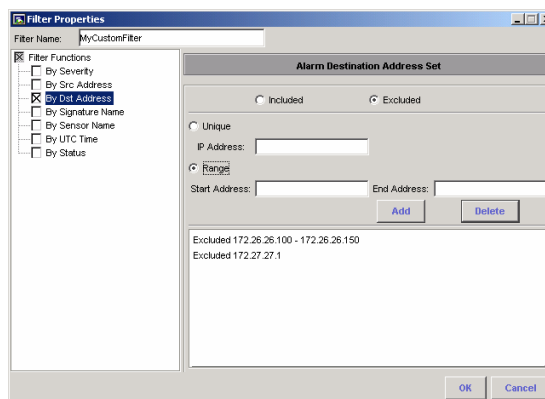
- Step 1** Enable the source address function by selecting the **By Src Address** check box from the Filter Functions options. The Alarm Source Address Set information is displayed. Notice that the Filter Functions check box is enabled.
- Step 2** Add the source address sets to the filter:
1. Select 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.

A filter based on a source address can contain both include and exclude options. When include and exclude entries are combined, include takes precedence.

Filter Properties—By Destination Address

Cisco.com

- Add unique IP addresses.
- Add a range of IP addresses:
 - Start address
 - End address



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-30

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:

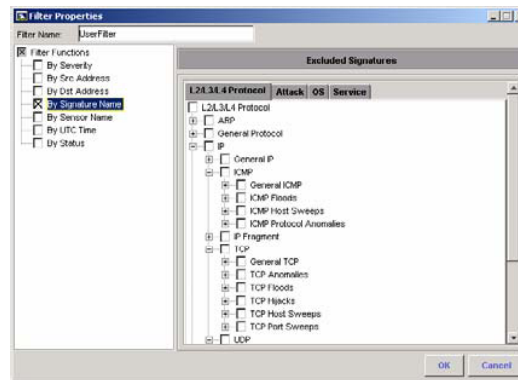
- Step 1** Enable the destination address function by selecting the **By Dst Address** check box from the Filter Functions options. The Excluded Alarm Destination Address Set information is displayed. Notice that the Filter Functions check box is enabled.
- Step 2** Add the destination address sets to the filter:
 1. Select either the **Included** or **Excluded** radio button.
 2. Select either the **Unique** or **Range** radio 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.

A filter based on a destination address can contain both include and exclude options. When include and exclude entries are combined, include takes precedence.

Filter Properties—By Signature Name

Cisco.com

Select a signature category or specific signatures to add in the filter.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-31

Complete the following steps to add a signature category or specific signatures to include in the filter:

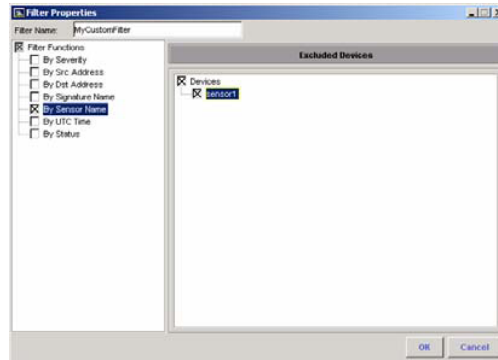
- Step 1** Enable the signature name function by selecting the **By Signature Name** check box from the Filter Functions options. The Excluded Signatures information is displayed. Notice that the Filter Functions check box is enabled.
- Step 2** Add the signature category or specific signature to the 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

Select a Sensor to apply to the filter.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-32

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 that 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.

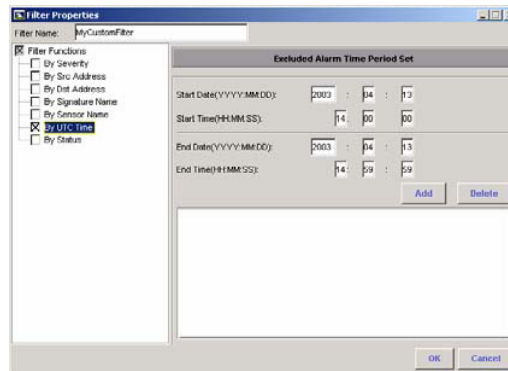
Note The addition of a Sensor in a filter causes it to be excluded when the filter is applied to a view.

Filter Properties—By Time

Cisco.com

Add an alarm time period to apply to the filter:

- **Start date and time**
- **End date and time**



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-33

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 that 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.

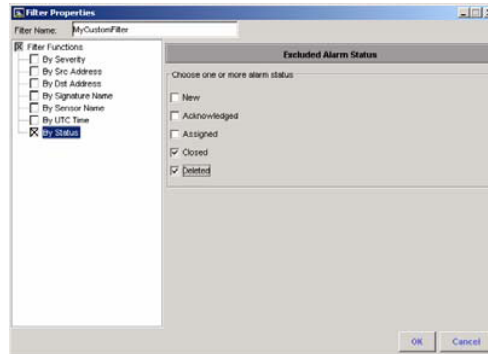
Note The addition of a time range in a filter causes it to be excluded when the filter is applied to a view.

Filter Properties—By Status

Cisco.com

Choose the status of alarms to include in the filter:

- New
- Acknowledged
- Assigned
- Closed
- Deleted



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-34

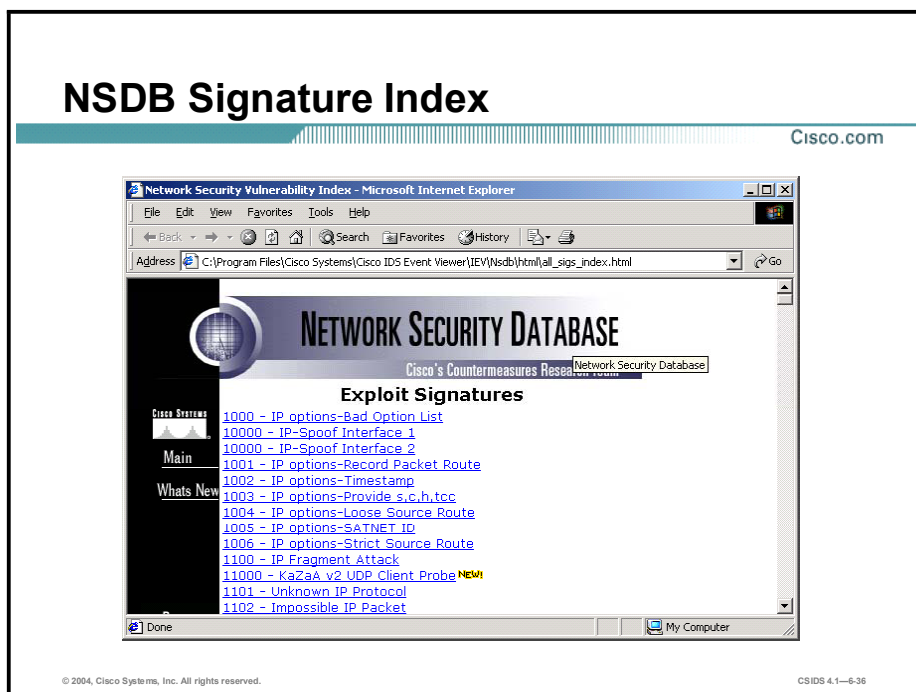
Complete the following steps to add an alarm status to the filter:

- 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 that 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.

Network Security Database

This topic describes the Network Security Database (NSDB) and the information contained in the database.



IEV includes the Network Security Database (NSDB). The NSDB provides detailed IDS signature and vulnerability information. You can use this information to assist in determining the threat posed to your network.

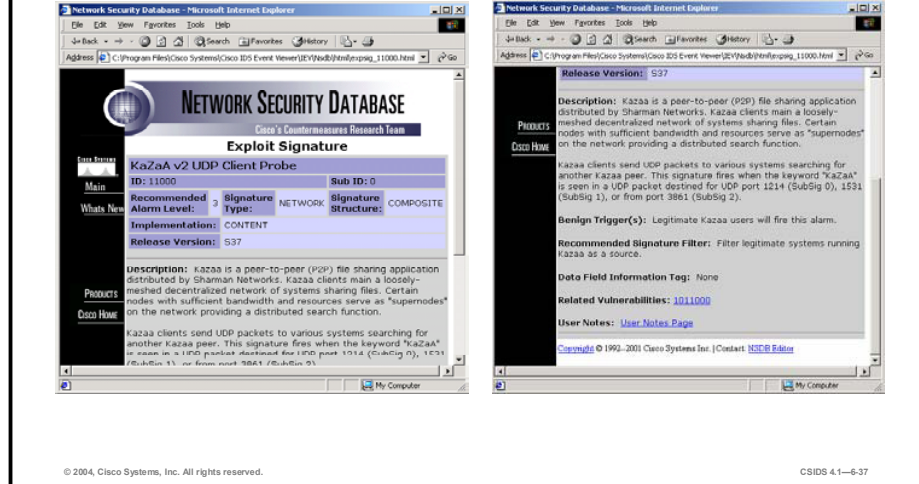
The NSDB is the Cisco HTML-based encyclopedia of network vulnerability information. You can examine the NSDB for a specific alarm. The Cisco Secure Encyclopedia (CSEC) is the online equivalent of the NSDB.

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 malicious attempts to exploit your systems. CSEC can be found at: <http://www.cisco.com/go/csec>.

Note A valid Cisco.com account is required to view the CSEC data.

Signature Information

Cisco.com



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.
- Recommended Alarm Level—The alarm severity level recommended by the Cisco Countermeasures Research Team (C-CRT).
- Description—A concise explanation of the signature and which exploits it detects.
- Benign Trigger(s)—An explanation of any false positives that may appear to be exploits but are actually normal network activity.
- Related Vulnerabilities—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

Cisco.com

The left screenshot shows the NSDB interface for the 'Peer-to-Peer File Sharing' vulnerability. It includes the following information:

- Cisco ID: 1011000
- CVE ID: **GENERIC-MAE-N/A**
- Severity Level: **Medium**
- Vulnerability Type: **Network**
- Exploit Type: **Other**
- Affected System(s): **N/A**
- Affected Program(s): **N/A**
- Vendor Aliases: **N/A**

The right screenshot shows the 'Description' section, which states: "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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-6-38

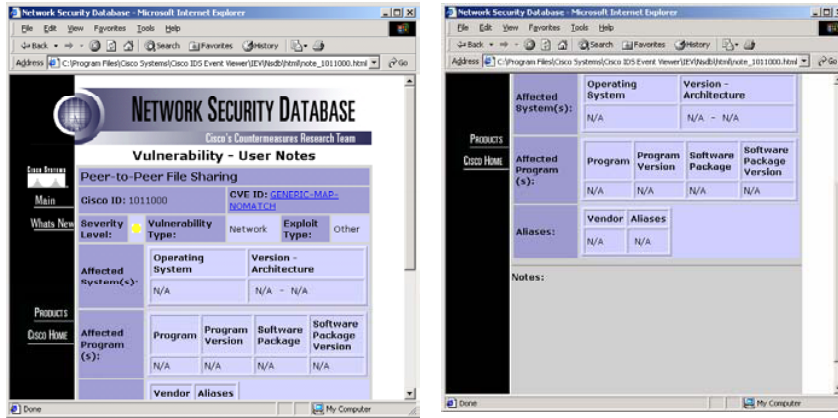
A typical NSDB Vulnerability page contains the following information about the vulnerability associated with the signature that triggered the alarm:

- **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**—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.
- **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 versions affected by the vulnerability.
- **Vulnerability Description**—A concise explanation of the vulnerability and how it can be exploited.
- **Consequence(s)**—The damage 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 offer 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



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-6-39

The User Notes page is an HTML template in which users 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 subdirectory (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.

Summary

This topic summarizes what you have learned in this lesson.

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.**
- **The NSDB is a tool in IDM and IEV that contains IDS signature and vulnerability information.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—6-41

Using the Intrusion Detection System Device Manager to Configure the Sensor

Overview

This lesson introduces the Intrusion Detection System Device Manager (IDM), which is used to manage configurations for Cisco IDS Sensors in a small to medium network. The following topics are covered in this lesson:

- Objectives
- Configuring basic Sensor settings
- Configuring SSH communications
- Configuring TLS communications
- Configuring monitoring
- Viewing diagnostics and system information
- Summary
- Lab exercise

Objectives

This topic lists the lesson objectives.

Objectives

Cisco.com

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

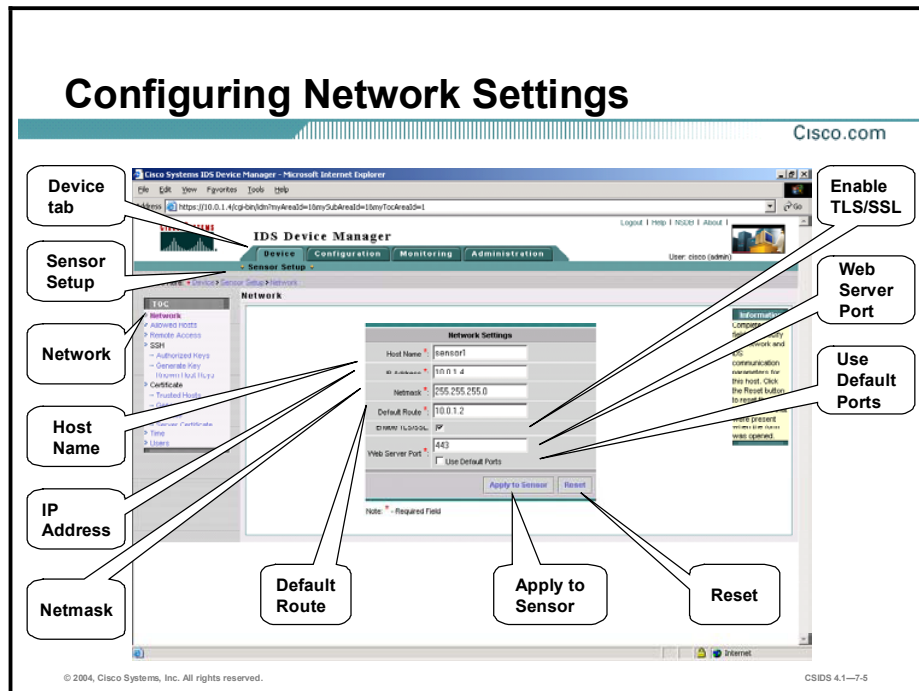
- **Configure network settings.**
- **Add allowed hosts.**
- **Set the time.**
- **Add users.**
- **Configure interfaces.**
- **Restore default settings.**
- **Configure SSH communications.**
- **Configure TLS and SSL communications.**
- **Configure the events display.**
- **View Sensor statistics.**
- **View diagnostics.**
- **View system information.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7.3

Configuring Basic Sensor Settings

This topic explains how to set up the Sensor by using the IDM.



After you use the **setup** command to initialize the Sensor, the parameter values appear on the Network Settings page in IDM. If you need to change these parameters, you can do so from the Network Settings page. Changing the network settings may disrupt your connection to the Sensor and force you to reconnect.

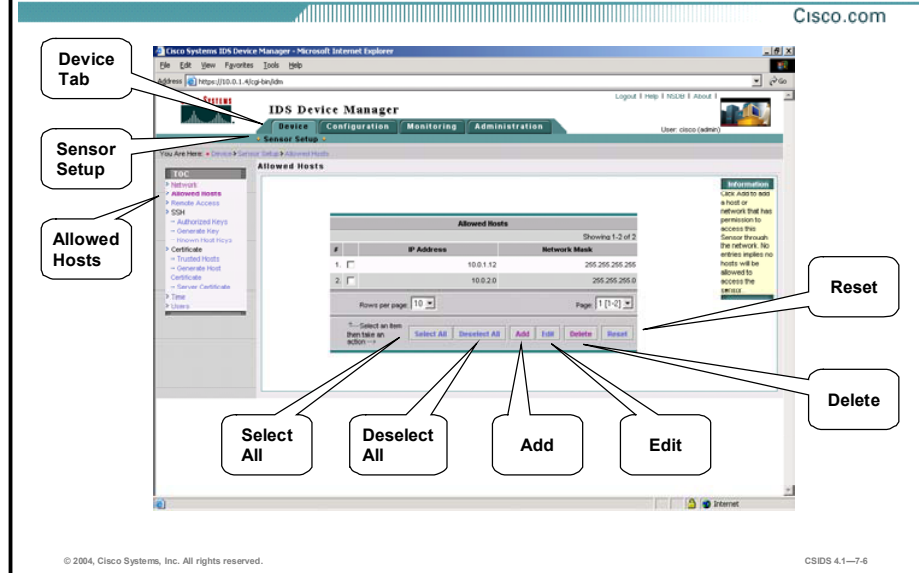
Only a user with administrator privileges can configure the network settings of the Sensor. To change the communication parameters of a Sensor, choose **Device > Sensor Setup > Network**. The **Network Settings** panel appears, enabling you to enter the following settings:

- **Sensor Name**—The name of the Sensor. The name is a case-sensitive character string up to 256 characters. Numbers, “_” and “-” are valid, but spaces are not acceptable.
- **IP Address**—The IP address of the Sensor.
- **Netmask**—The netmask for the Sensor.
- **Default Route**—The default route IP address for the Sensor.
- **Enable TLS/SSL**—Enables TLS/SSL in the web server when checked. This option is enabled by default. Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are protocols that enable encrypted communications between a web browser and a web server. When TLS/SSL is enabled, you connect to IDS Device Manager using **https://sensor_ip_address**. If you disable TLS/SSL, connect to the IDS Device Manager using **http://sensor_ip_address:port_number**.
- **Web Server Port**—The TCP port used by the web server (1 to 65535).
- **Use Default Ports**—Enables the web server to use the default port when selected. You can enter a TCP port to be used by the web server in the field above or you can select this check box to use the default port. The default port for http is 80. The default port for https 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 the IDM.

To save and apply your changes, click **Apply to Sensor**. If you want to reset the form, click **Reset**.

Configuring Allowed Hosts



You can give a host or network permission to access the Sensor through the network by adding the host or network as an allowed host. In order to use management and monitoring hosts, you must add them as allowed hosts. Otherwise, they will not be able to communicate with the Sensor. By default, only hosts on the 10.0.0.0 network are permitted access. If you delete the default network and you do not add any hosts to the list, no hosts are permitted.

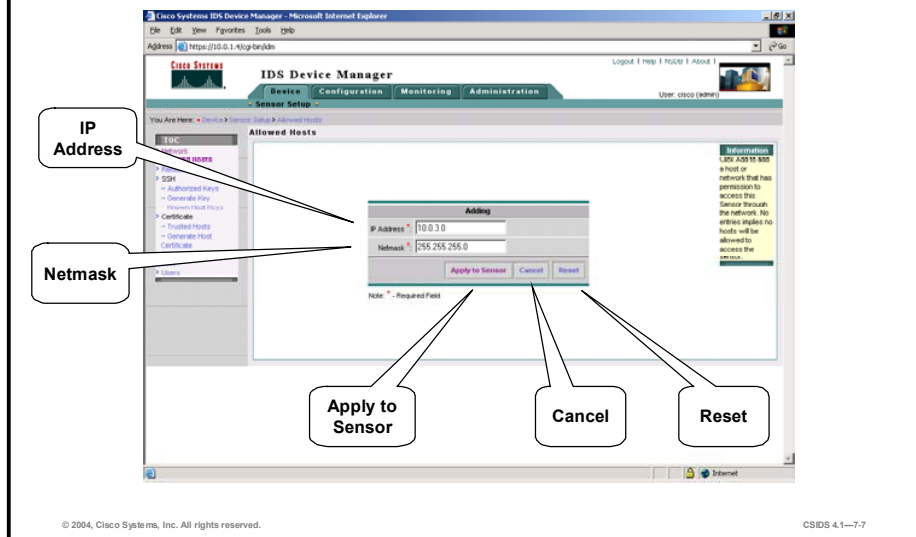
To add, edit, or delete allowed hosts, choose **Device > Sensor Setup > Allowed Hosts**. The Allowed Hosts page is displayed. This page provides the following options:

- Select All—Enables you to select all host and network entries simultaneously
- Deselect All—Enables you to deselect all host and network entries simultaneously
- Add—Enables you to access the Adding page, where you can add allowed hosts
- Edit—Enables you to edit the IP addresses and netmasks of specific hosts
- Delete—Enables you to delete hosts from the allowed list
- Reset—Enables you to reset the form

Caution When adding, editing, or deleting allowed hosts, make sure that you do not delete the IP address used for remote management of the Sensor.

Configuring Allowed Hosts (Cont.)

Cisco.com

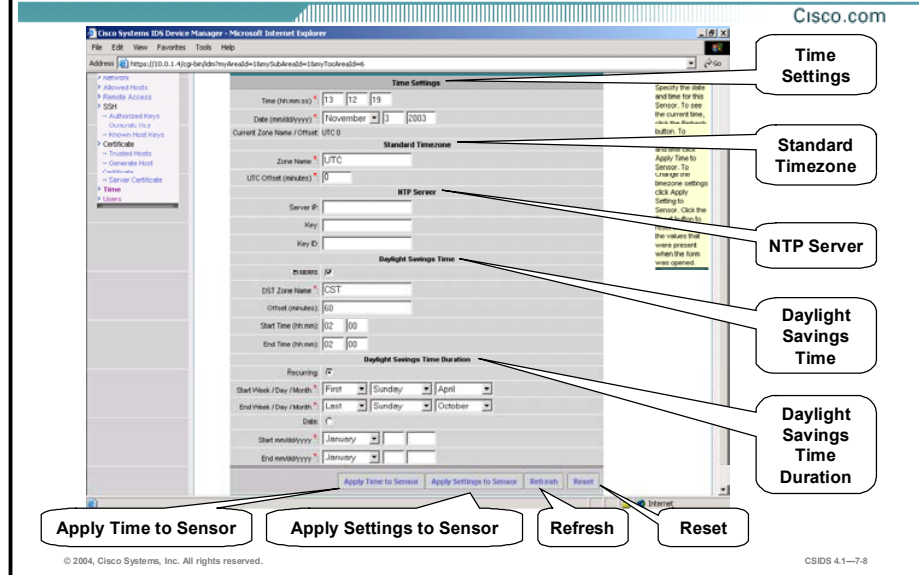


If you select Add from the Allowed Hosts page, the Adding page appears, enabling you to enter the following settings for the allowed host:

- IP Address—The IP address of the host you are permitting access to the Sensor
- Netmask—The netmask of the network or host you are permitting to access the Sensor

If you want to reset the form, click **Reset**. Otherwise, click **Apply to Sensor** to save and apply your changes. The Allowed Hosts page appears again with the host information you entered.

Setting the Time



You can define the time, time zone, and daylight savings time (DST) for the Sensor by selecting **Device > Sensor Setup > Time**. The Time Settings page appears, enabling you to configure the following settings:

■ Time Settings

- **Time**—The current time in hh:mm:ss format. Time indicates the time on the local host. To see the current time, click Refresh. If you accidentally specify the incorrect time, stored events will have the wrong time stamp. You must clear the events.
- **Date**—The current date in the format mm:dd:yyyy. Date indicates the date on the local host.

■ Standard Timezone

- **Zone Name**—The local time zone to be displayed when summer time is not in effect. The default value is Universal Coordinated Time (UTC).
- **UTC Offset**—The offset in minutes from UTC (in the format mm). The default value is 0.

■ NTP Server

- **Server IP**—The Network Time Protocol (NTP) server's IP address. Enter the IP address if you are using an NTP server to set the Sensor's time. If you define an NTP server, the Sensor's time is set by the NTP server, and the command line interface (CLI) clock set command will produce an error; however, you can still set the time zone and daylight saving time parameters.
- **Key**—The NTP server's key value. Enter this value if you specified an NTP server.
- **Key ID**—The NTP server's key ID, a value from 1 to 4294967295. Enter this value if you specified an NTP server.

- Daylight Savings Time
 - Enabled—Select the Enabled check box to enable daylight saving time (DST, or summer time). The default is Off.
 - DST Zone Name—The name of the zone (1 to 32 characters of text) to be displayed when summer time is in effect.
 - Offset—The number of minutes to add during the summer time in mm format. The default is 60 minutes.
 - Start Time—The time (in hh:mm format) to apply the summer time setting. The default is 02:00.
 - Stop Time—The time (in hh:mm format) to remove the summer time setting. The default is 02:00.
- Daylight Savings Time Duration
 - Recurring—Select the Recurring radio button to indicate that summer time should start and end on the specified days every year. The default is Off.
 - Start Week/Day/Month—The week, day, and month of the year to apply summer time. The defaults are 1, Sunday, April. Use the drop-down menus to select the week, day, and month.
 - End Week/Day/Month—The week, day, and month of the year to remove summer time. The defaults are last, Sunday, October. Use the drop-down menus to select the week, day, and month.
 - Date—Select the Date radio button to indicate that summer time should start on a specific date.
 - Start—The month, date, and year to start summer time. Use the drop-down menu to select the month. Enter the date and year in the format dd:yyyy.
 - End—The month, date, and year to stop summer time. Use the drop-down menu to select the month. Enter the date and year in the format dd:yyyy.

To reset the form, click **Reset**. Otherwise, click **Apply to Sensor** to save the settings.

Note Cisco IDS Version 4.1 has been evaluated against the Intrusion Detection System Protection Profile, V1.4, February 4, 2002, using the Common Criteria Evaluation and Validation Scheme found at the following site: <http://niap.nist.gov/cc-scheme/>. In the evaluated configuration, the Sensor must utilize internal resources for time setting and timekeeping. You cannot use an NTP server. See Common Criteria Evaluated Configuration for more information.

If you set the time incorrectly when you first configure the options in the Time page, your stored events will have the incorrect time because they are stamped with the time the event was created. The eventStore time stamp is always based on UTC. If during the original Sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events could have times older than old events.

For example, if during the initial setup, you configure the Sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m.,

and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To insure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command from the CLI.

Creating User Accounts

Cisco.com

The screenshot shows the Cisco IDS Device Manager web interface. The top navigation bar includes 'Device', 'Configuration', 'Monitoring', and 'Administration'. The 'Sensor Setup' tab is selected, and the 'Users' sub-tab is active. A table displays the following user accounts:

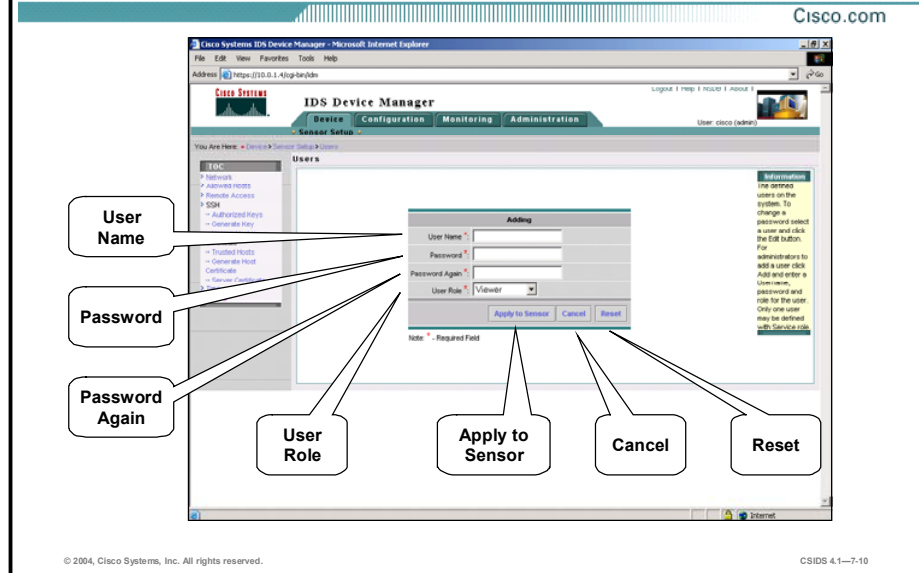
#	User Name	Role
1.	cisco	administrator
2.	admin	administrator

Below the table are buttons for 'Select All', 'Deselect All', 'Add', 'Edit', 'Delete', and 'Reset'. Callouts from the left side of the image point to the 'Device Tab', 'Sensor Setup', and 'Users' sections. Callouts from the bottom point to the 'Select All', 'Deselect All', 'Add', 'Edit', 'Delete', and 'Reset' buttons.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-7-9

To create and remove users from the local Sensor, select **Device > Sensor Setup > Users**. The Users page appears, displaying all currently configured user accounts. If you click **Add** in the Users page, the Adding page appears, enabling you to add a user.

Creating User Accounts (Cont.)



To add a user, complete the Adding page as follows:

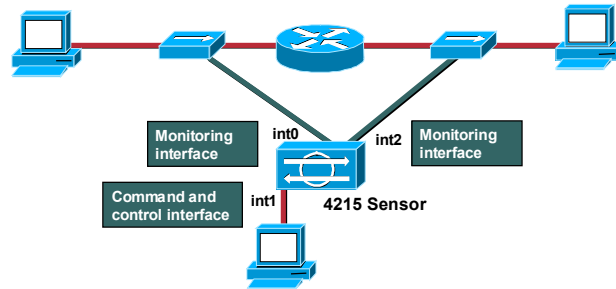
- **User Name**—The new username, which can contain 1 to 16 alphanumeric characters.
- **Password**—The password associated with the user. The password must be at least eight characters long and must not be a dictionary word.
- **Password Again**—The password associated with the user. Enter the password again in this field.
- **User Role**—Select one of the following roles for the user from the User Role drop-down menu:
 - Viewer
 - Operator
 - Administrator
 - Service

To reset the form, click **Reset**. Otherwise, click **Apply to Sensor** to save your changes.

IDM permits only one user to log in at a time. If a second user attempts to log in, a message is displayed indicating that the user limit has been reached. If the second user has equal or greater privileges than the first user, the login can be forced, but this process logs out the first user. If the first user is forced out, all unsaved changes are lost.

Sensor Interface Overview

Cisco.com



The figure illustrates the following Sensor interface characteristics:

- There is only one command and control interface per Sensor.
- You can configure up to five monitoring interfaces depending on the type of Sensor.
- Multiple monitoring interfaces enable simultaneous protection of up to five different network subnets.
- All monitoring interfaces use the same configuration.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-11

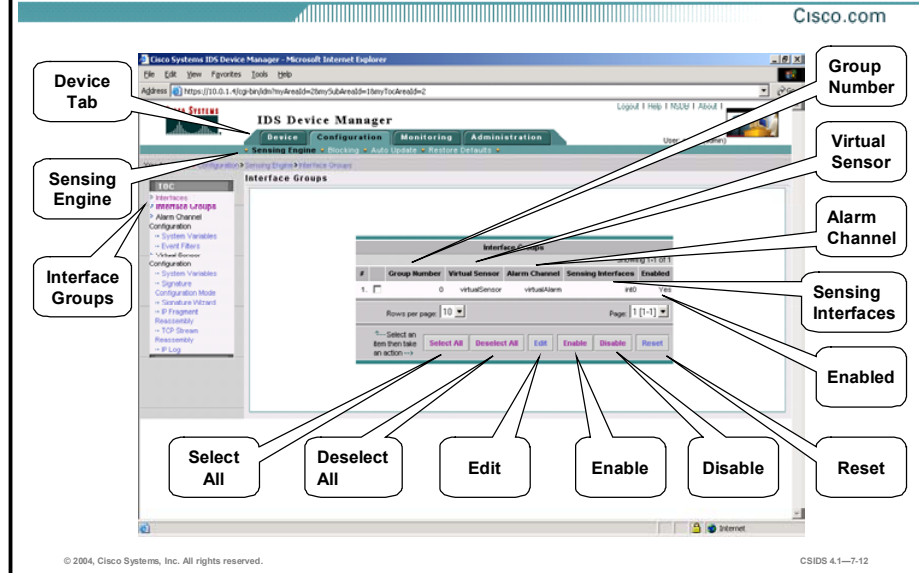
Each Sensor has only one command and control interface, but you can configure up to five monitoring interfaces depending on the type of Sensor you have. Multiple interfaces enable simultaneous protection of up to five different network subnets, which is like having five Sensors in a single appliance.

All monitoring interfaces use the same configuration. There is only one virtualSensor, so no mapping of virtualSensor configurations to interfaces is required.

A monitoring interface must be part of Interface Group 0 and must be enabled. Sensors with factory-installed Cisco IDS Version 4.1 are shipped with all monitoring interfaces added to Interface Group 0 and disabled. You must enable the monitoring interfaces in order for the Sensor to monitor your networks. Upgrades from IDS Version 4.0 to 4.1 may leave some interfaces enabled that are not assigned to a group. Either disable these interfaces or add them to Group 0 to prevent inconsistencies in reporting to the Sensor.

You do not need to enable all interfaces. Enable only those interfaces that you want to use.

Configuring the Interfaces



You can enable an interface only if the interface belongs to an interface group. You receive the following error message if you attempt to enable an interface that is not part of a group:

This operation is illegal because interface, int0, does not belong to an interface group.

An interface group provides a way to group monitoring interfaces into one logical virtualSensor. Only one interface group, Group 0, is supported. Multiple monitoring interfaces can be assigned to the interface group at any given time, but you cannot assign the command and control interface to the interface group.

Note Interface 0 (int0) on the IDS-4250-XL cannot be a monitoring interface because it is used for sending TCP resets.

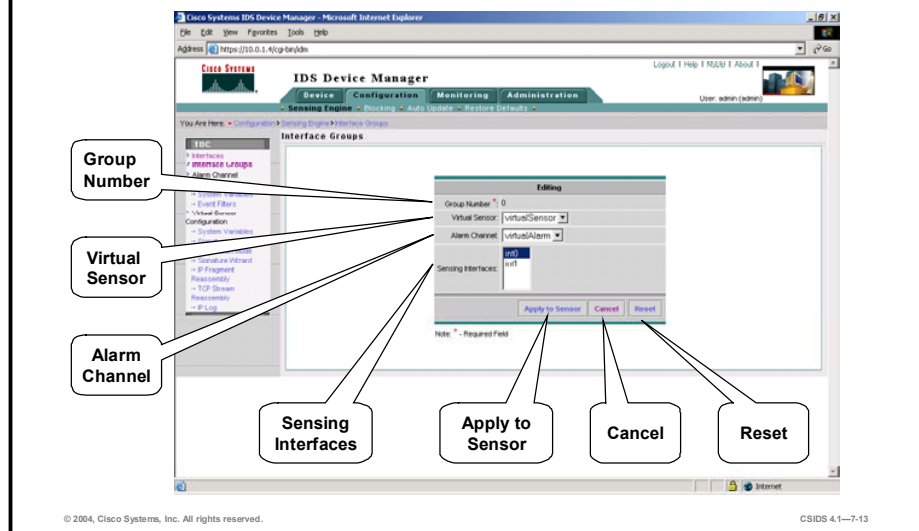
To add an interface to an interface group and to enable an interface group, select **Configuration > Sensing Engine > Interface Groups**. The Interface Groups page appears with the following information displayed:

- **Group Number**—Specifies the logical number associated with the group. You must use 0 for the current IDS software versions.
- **Virtual Sensor**—Specifies the virtualSensor assigned to this group. You must use “virtualSensor” for the current IDS software versions. Only one virtualSensor is supported.
- **Alarm Channel**—Specifies the Alarm Channel assigned to this group. You must use “alarmChannel” for current IDS software versions. Only one Alarm Channel is supported.
- **Sensing Interfaces**—Specifies the interfaces that belong to the group. There is no default.
- **Enabled**—Defines whether the group is enabled or disabled. The default is Yes.

To enable or disable the interface group, select the check box next to the group and click **Enable** or **Disable**. To add interfaces to an interface group, select the check box next to the group and click **Edit**. The Editing page appears.

Configuring the Interfaces (Cont.)

Cisco.com



In the Editing page, you can select one or more sensing interfaces to add to the group. For current IDS software versions, the only option you can edit is the Sensing Interfaces option. To select multiple interfaces, press the Ctrl key while selecting each additional interface. Selecting the command and control interface results in an invalid configuration. Do not select the command and control interface as a sensing interface. The command and control interface is int1 on most Sensors; however, it is int0 on the router network module.

To reset the form, click **Reset**. Otherwise, select **Apply to Sensor** to save and apply your changes. When you click **Apply to Sensor**, the following message is displayed:

Configuration update in progress. This page will be unavailable for a few minutes.

You can select **Configuration > Sensing Engine > Interface Groups** to display the Interface Groups page and view any changes you made.

Configuring the Interfaces (Cont.)

Cisco.com

The screenshot shows the 'Sensing Interface' configuration page in the Cisco Systems IDS Device Manager. The page contains a table with the following data:

#	Interface Name	Device Name	Enabled	Command and Control	Sniffing	Reset	Type
1	eth0	eth0	Yes	No	Yes	Yes	TX
2	eth1	eth1	No	Yes	No	Yes	TX

Below the table, there are buttons for 'Select All', 'Deselect All', 'Enable', 'Disable', and 'Reset'. Callout boxes point to these buttons with labels: 'Select All', 'Deselect All', 'Enable', 'Disable', and 'Reset'.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-14

To enable sensing interfaces, select **Configuration > Sensing Engine > Interfaces**. The Sensing Interface page appears. The Sensing Interface page lists the known interfaces and allows you to enable or disable them. The following information is displayed:

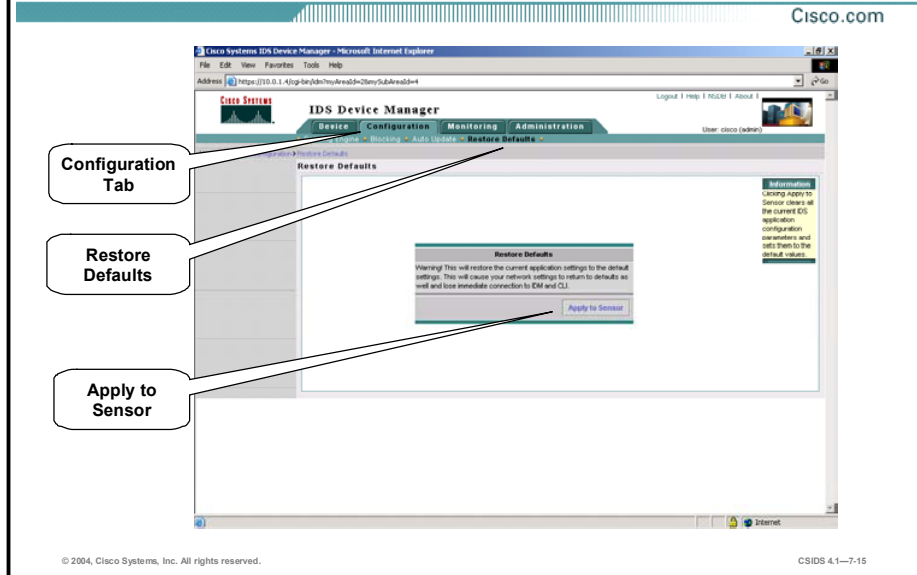
- The interface name
- The device name
- Whether the interface is enabled or disabled
- Whether the interface is command and control or monitoring (sniffing)
- Which type of interface it is (SX, TX)

To enable an interface, select the check box next to the interface and click **Enable**. To disable the interface, click **Disable**. You receive the following message while the configuration is taking place:

Configuration update is in progress. This page will be unavailable for a few minutes.

The Sensing Interface page then appears again and displays your changes.

Restoring the Default Settings



You can restore the default configuration to your Sensor. Restoring the default configuration removes the current application settings and restores the default settings. Your network settings also return to the defaults and you immediately lose connection to IDM and the CLI. The following settings, however, are not reset:

- User accounts
- Passwords
- Time

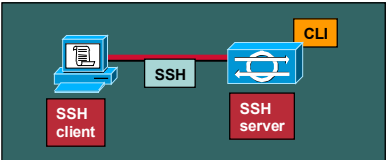
To restore the default configuration, select **Configuration > Restore Defaults**. The Restore Defaults page appears. Click **Apply to Sensor** to restore the default configuration.

Configuring SSH Communications

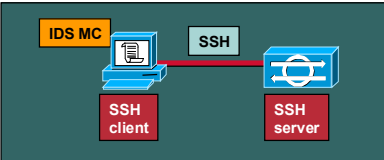
This topic explains how to configure SSH communications.

SSH Communications

Cisco.com



SSH client — SSH — SSH server (CLI)



IDS MC — SSH — SSH client — SSH server

- **The client key, SSH authorized key, enables the client to connect without password authentication.**
- **The server key, SSH host key, is used by the Sensor to prove its identity to the client.**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—7-17

When using SSH to log in to the sensor, you can use Rivest, Shamir, and Adleman (RSA) authentication rather than using passwords. IDM enables you to define the public keys used by clients to log in to the Sensor with RSA authentication. To enable RSA authentication, first use an RSA key generation tool on the client. Then display the generated public key as a set of three numbers (key modulus length, public exponent, and public modulus) and enter those numbers in IDM.

Note SSH authorized keys are user-specific.

Defining SSH Authorized Keys

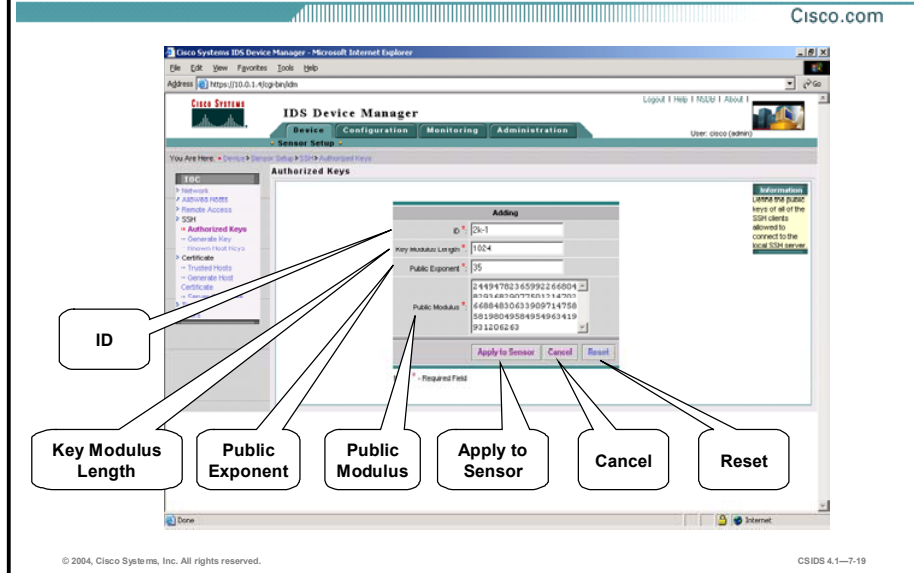
Cisco.com

The screenshot displays the Cisco IDS Device Manager web interface. The navigation path is highlighted: **Device Tab** (top menu), **Sensor Setup** (left sidebar), and **Authorized Keys** (left sidebar). The main content area shows the **SSH Authorized Keys** configuration page. A table titled **SSH Authorized Keys** is displayed, showing 1-0 of 0 rows. The table has columns for ID, Key Modulus Length, Public Exponent, and Public Modulus. Below the table are buttons for **Select All**, **Deselect All**, **Add**, **Edit**, **Delete**, and **Reset**. A callout box on the right side of the table contains the text: "Warning: Limit the public keys of all of the SSH clients allowed to connect to the local SSH server."

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—7-18

To define public authorized keys in IDM, first select **Device > Sensor Setup > Authorized Keys**. The SSH Authorized Keys page appears. Clicking **Add** in this page displays the Adding page, which enables you to enter the key information.

Defining SSH Authorized Keys (Cont.)



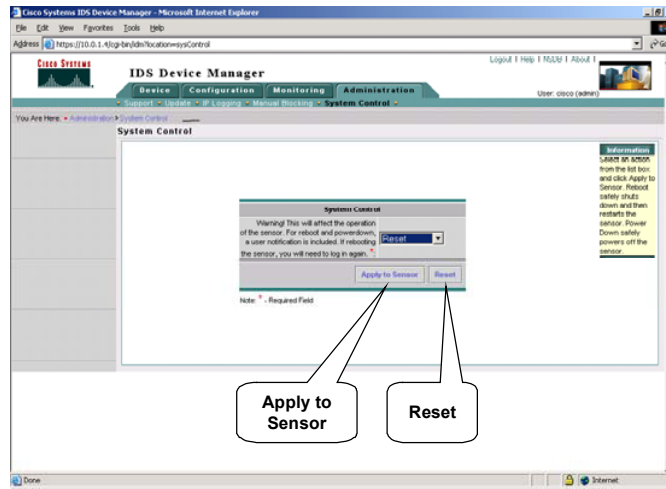
Enter the following in the Adding page:

- **ID**—A unique ID to identify the key. The ID should be a string of 1 to 256 characters that uniquely identifies the authorized key. Numbers, “_”, and “-” are valid. Spaces are not valid.
- **Key Modulus Length**—An ASCII decimal integer from 511 to 2048. The key modulus length is the number of significant bits in the modulus. The strength of an RSA key relies on the size of the modulus. The more bits the modulus has, the stronger the key.
- **Public Exponent**—An ASCII decimal integer from 3 to 4294967296. The RSA algorithm uses the public exponent to encrypt data.
- **Public Modulus**—An ASCII decimal integer in the range x , such that $(2^{[key-modulus-length-1]} < x < 2^{key-modulus-length})$. The RSA algorithm uses the public modulus to encrypt data.

If you wish to reset the form, click **Reset**. Otherwise, click **Apply to Sensor** to save your changes. The SSH Authorized Keys page displays your entry. If you need to edit the values in the fields, select the check box next to the key you want to edit and click **Edit** to begin the editing process.

Generating an SSH Host Key (Cont.)

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-21

To complete the generation of the new host key, select **Reset** from the drop-down menu and click **Apply to Sensor**. A new host key is generated and the old host key is deleted.

Configuring TLS Communications

This topic explains TLS and how to configure TLS certificates.

TLS/SSL Communications

Cisco.com

- **TLS and SSL use a process called handshaking that involves a number of coordinated exchanges between a client and server.**
- **A trusted host certificate is used by the server to verify the identity of a connecting client.**
- **A server certificate, host certificate, is used by the server to prove its identity to the client.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—7-23

The IDS Sensor software contains a web server that runs the IDM. To provide security, this web server uses an encryption protocol known as Transport Layer Security (TLS), which is closely related to Secure Sockets Layer (SSL) protocol. When you enter a URL in the web browser that starts with `https://ip_address`, the web browser responds by using either TLS or SSL to negotiate an encrypted session with the host.

The process of negotiating an encrypted session in TLS is called handshaking, because it involves a number of coordinated exchanges between client and server. The server sends its certificate to the client. The client performs the following three-part test on this certificate:

1. Is the issuer identified in the certificate trusted?—Every web browser ships with a list of trusted third-party Certificate Authorities (CAs). If the issuer identified in the certificate is among the list of CAs trusted by your browser, the first test is passed.
2. Is the date within the range of dates during which the certificate is considered valid?—Each certificate contains a Validity field, which is a pair of dates. If the date falls within this range of dates, the second test is passed.
3. Does the common name of the subject identified in the certificate match the URL hostname?—The URL hostname is compared with the subject common name. If they match, the third test is passed.

When you direct your web browser to connect with IDM, the certificate that is returned fails because the Sensor issues its own certificate. The Sensor is its own CA, and the Sensor is not already in the list of CAs trusted by your browser. When you receive the Security Alert message from your browser, you have three options:

- Disconnect from the site immediately.

- Accept the certificate for the remainder of the web browsing session.
- Add the issuer identified in the certificate to the list of trusted CAs of the web browser and trust the certificate until it expires.

The most convenient option is to permanently trust the issuer. However, before you add the issuer, use out-of-band methods to examine the fingerprint of the certificate. This prevents you from being victimized by an attacker posing as a Sensor. Confirm that the fingerprint of the certificate appearing in your web browser is the same as the one on your Sensor. If you change the hostname of the Sensor, a new certificate is generated the next time the Sensor is rebooted. The next time your web browser connects to IDM, you will receive the manual override dialog boxes. You must perform the certificate fingerprint validation again for Netscape and Internet Explorer.

Generating the Server Certificate

Cisco.com

The screenshot shows the Cisco Systems IDS Device Manager web interface. The main content area displays the 'Generate Host Certificate' page. A dialog box titled 'Generate Server Certificate' is open, showing the following information:

```
The system has the following Server Certificate:  
MD5: ED:EP:41:85:59:82:45:89:FC:CE:88:9D:9E:47:1E  
SHA1: 01:A:52:88:54:30:48:25:00:9F:20:F5:E7:8F:30:00:97:C4:F8:0C
```

Below the fingerprint, there is a button labeled 'Apply to Sensor'.

Callout boxes on the left side of the screenshot point to the following elements:

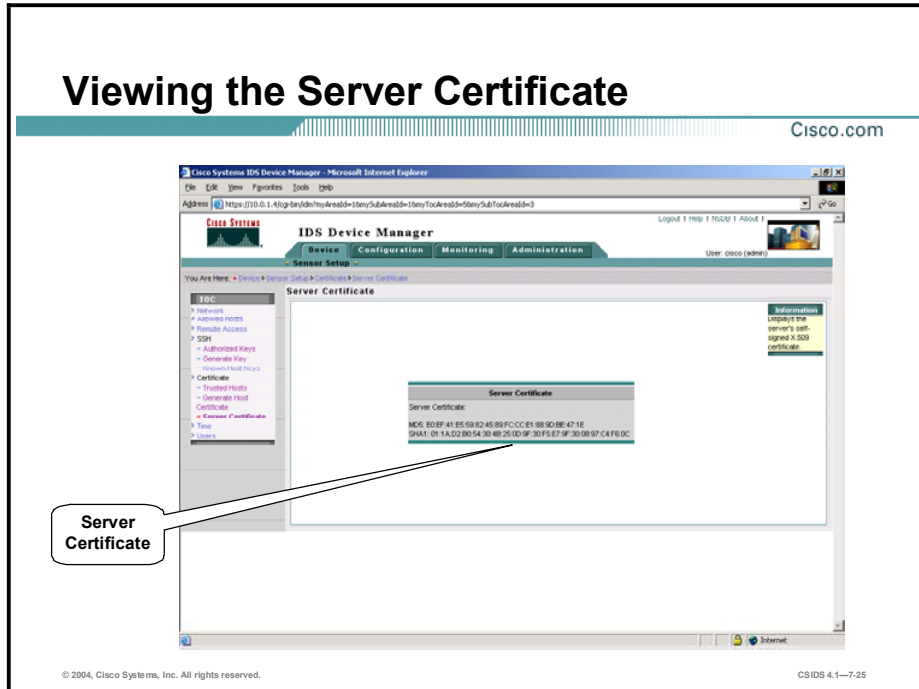
- Device Tab**: Points to the 'Device' tab in the top navigation bar.
- Sensor Setup**: Points to the 'Sensor Setup' link in the left sidebar.
- Generate Host Certificate**: Points to the 'Generate Host Certificate' link in the left sidebar.
- Apply to Sensor**: Points to the 'Apply to Sensor' button in the dialog box.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—7-24

The Sensor generates its server certificate when the Sensor is first started. The Sensor's IP address is included in its certificate. If you change the Sensor's IP address, a new certificate is generated. You can also generate a new certificate by selecting **Device > Sensor Setup > Certificate > Generate Host Certificate**. The Generate Server Certificate panel is displayed within the Generate Host Certificate page. Click **Apply to Sensor** to generate a new certificate. Write down the new fingerprint. You will need it later to verify what is displayed in your web browser when you connect.

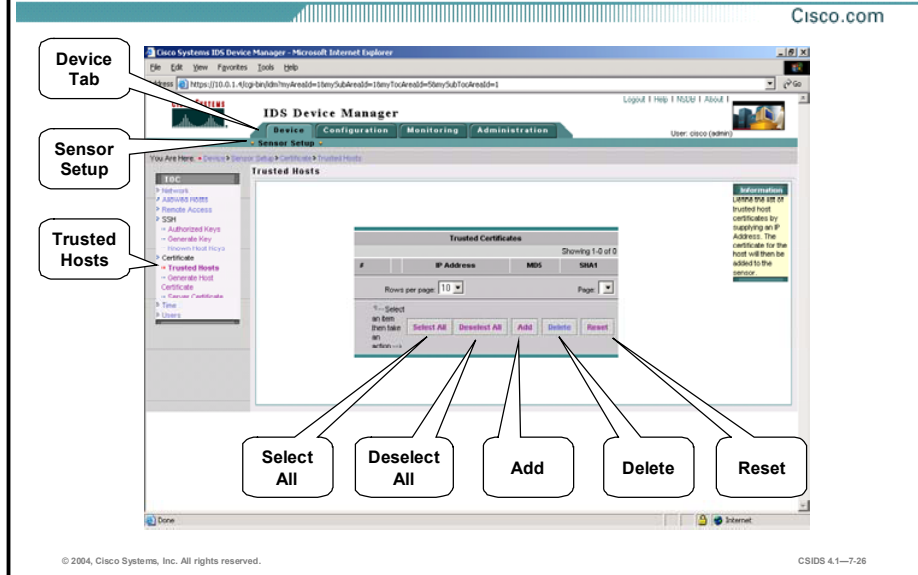
Viewing the Server Certificate

Cisco.com



To view the Sensor's server certificate, select **Device > Sensor Setup > Server Certificate**.

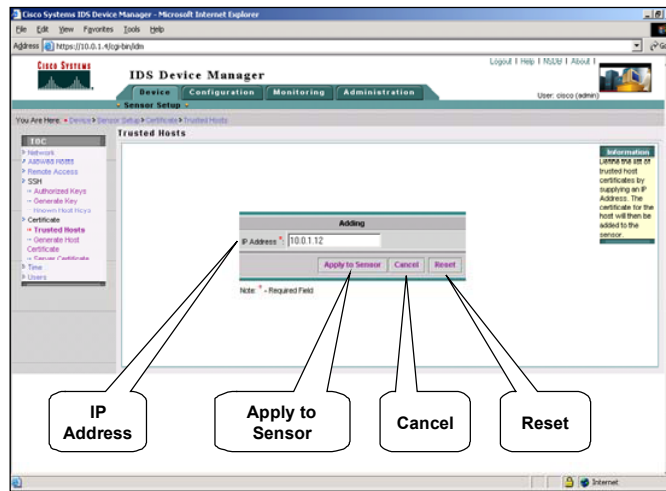
Adding Trusted Host Certificates



The Trusted Hosts page in IDM lists all trusted host certificates. Trusted Hosts certificates are required when the Sensor must communicate with another device using TLS. You can add certificates by entering the IP address of the trusted host. IDM retrieves the certificate and displays its fingerprint. If you accept the fingerprint, the certificate is trusted. To add certificates of trusted hosts, select **Device > Sensor Setup > Trusted Host**. The Trusted Certificates page is displayed. If you click **Add**, the Adding page is displayed, enabling you to add a trusted host address.

Adding Trusted Host Certificates (Cont.)

Cisco.com

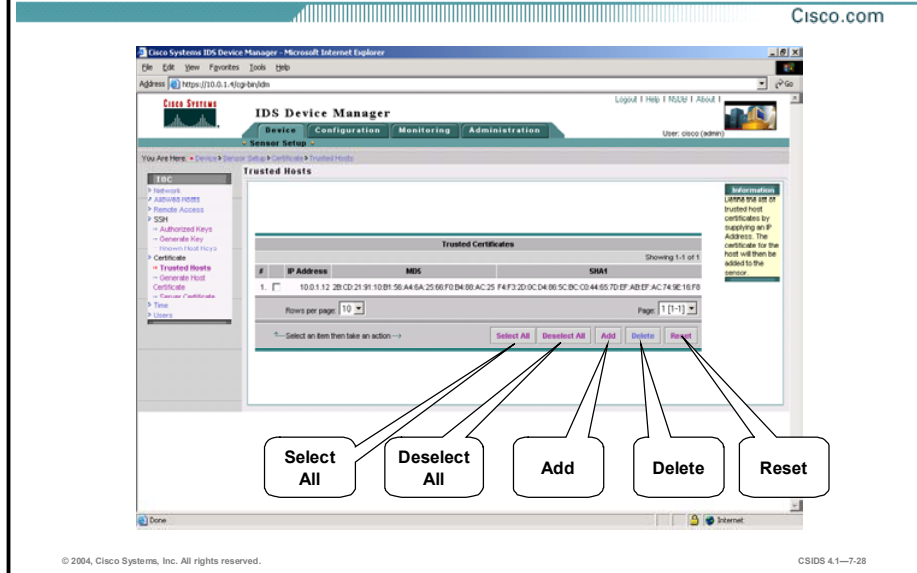


© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-27

In the IP Address field, enter the IP address of the host you want to trust. If you wish to reset the form, click **Reset**. Otherwise, click **Apply to Sensor** to save your changes. The host certificate is added to the list and is displayed in the Trusted Certificates page.

Adding Trusted Host Certificates (Cont.)



Verify the fingerprint by completing the following steps:

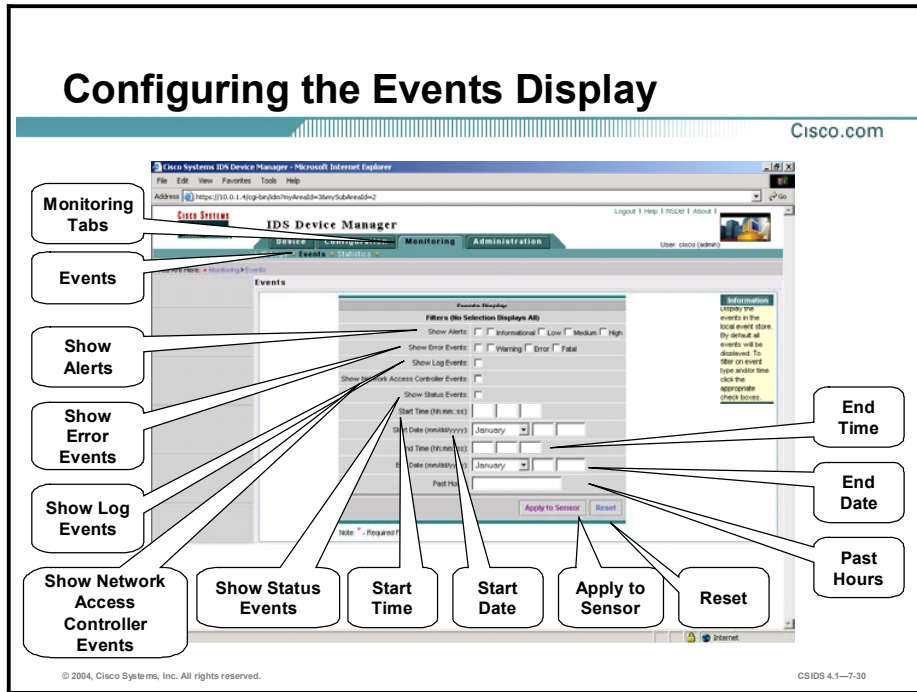
- Step 1** Obtain the fingerprint from the host by displaying it on the host console or through a direct terminal connection with the host.
- Step 2** Compare the fingerprint displayed in IDM with the fingerprint displayed on the host.

If you find any discrepancies, delete the host certificate immediately by selecting the check box next to it and clicking **Delete**.

Note IDM is enabled by default to use TLS/SSL. You can disable it by selecting **Device > Sensor Setup > Network** and then deselecting **TLS/SSL**.

Configuring Monitoring

This topic explains how to set up monitoring from the IDM Monitoring tab.



You can configure how events are displayed in IDM. You can filter events based on event type, time, or both. By default, all events are displayed. To configure the events display, select **Monitoring > Events**. The Events Display page is displayed. The following list explains the configurable options on the Events Display page:

- Show Alerts—To show alerts, select this check box. Then select the check boxes next to the level of alerts you want to see. The alert levels are as follows:
 - Informational
 - Low
 - Medium
 - High
- Show Error Events—To show error events, select this check box. Then select the check boxes next to the types of error events that you want to see. The types of error events are as follows:
 - Warning
 - Error
 - Fatal
- Show Log Events—To show log events, select this check box.
- Show Network Access Controller Events—To show network access controller (NAC) events, select this check box.
- Show Status Events—To show status events, select this check box.

- **Start Time**—To view events within a specified time frame, enter the start time in the format hh:mm:ss.
- **Start Date**—To view events within a specified time frame, enter a date in the format month:dd:yyyy.
- **End Time**—To view events within a specified time frame, enter a time in the format hh:mm:ss.
- **End Date**—To view events within a specified time frame, enter a date in the format month:dd:yyyy.

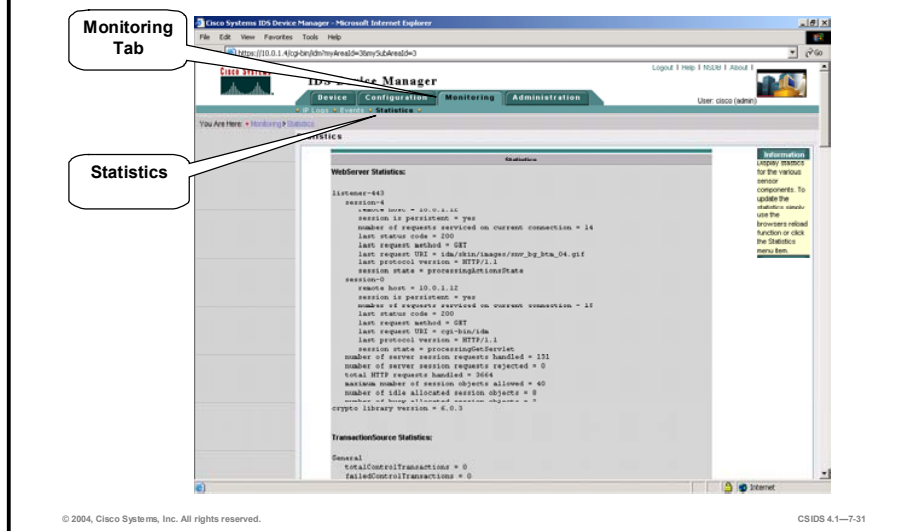
Note If you specify any part of the time frame fields, you must specify a value for all time frame fields.

- **Past Hours**—To specify past events ending now, do not specify a time frame by completing the time frame fields. Instead, enter the number of hours to go back (1-65535) in this field. For example, if you want to look at the most recent events, you can specify the number of past hours to review. Entering 2 would display the events logged during the past two hours.

To reset the form, click **Reset**. Otherwise, click **Apply to Sensor** to save your changes. The Events page lists the events you just selected.

Viewing Sensor Statistics

Cisco.com

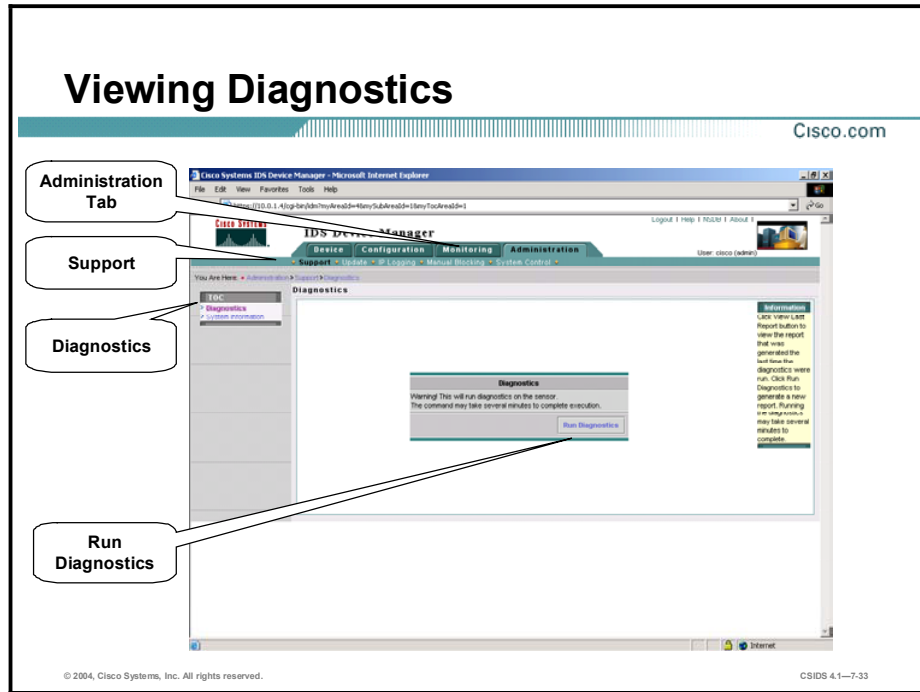


To view statistics for your Sensor, select **Monitoring > Statistics**. The Statistics page displays statistics for the following categories:

- WebServer
- TransactionSource
- TransactionServer
- NAC
- Logger
- Host
- EventStore
- EventServer
- AnalysisEngine
- Authorization

Viewing Diagnostics and System Information

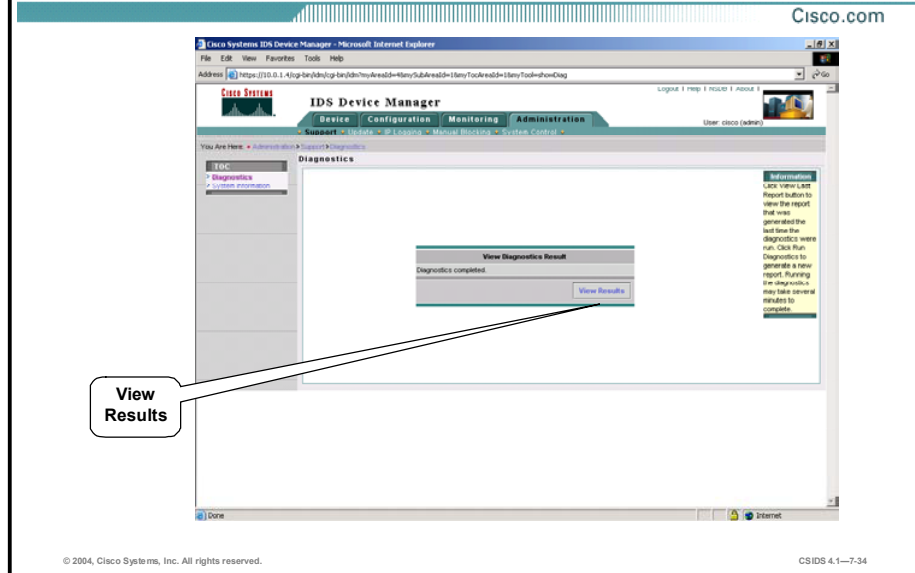
This topic explains how to view diagnostics and system information.



You can obtain diagnostics information on your Sensors for troubleshooting. To run diagnostics, select **Administration > Support > Diagnostics**. The Diagnostics page appears. If you click **Run Diagnostics**, the Cancel Diagnostics Command page appears with the following message:

Diagnostics are being generated. Please stand by.

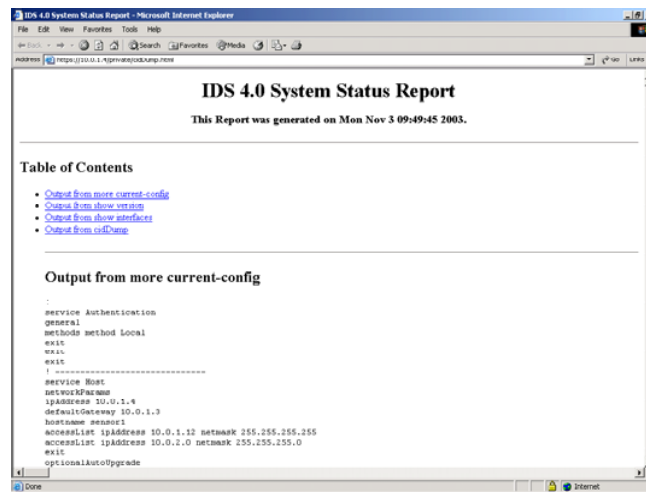
Viewing Diagnostics (Cont.)



The View Diagnostics Result page then appears. Click **View Results** to see the diagnostics report. The IDS 4.1 System Status Report appears in HTML format in another window, as shown in the figure.

Viewing Diagnostics (Cont.)

Cisco.com



The screenshot shows a web browser window displaying the "IDS 4.0 System Status Report". The report title is "IDS 4.0 System Status Report" and it states "This Report was generated on Mon Nov 3 09:49:45 2003." Below the title is a "Table of Contents" section with three links: "Output from more current-config", "Output from show version", and "Output from show interface". The main content area is titled "Output from more current-config" and displays a configuration snippet:

```
service Authentication
GENERAL
METHODS method Local
EXIT
EXIT
!
-----
service Host
networkParam
ipAddress 10.0.1.4
defaultGateway 10.0.1.3
hostname sensor1
accessList ipAddress 10.0.1.12 network 255.255.255.255
accessList ipAddress 10.0.1.0 network 255.255.255.0
EXIT
optionAutoUpgrade
```

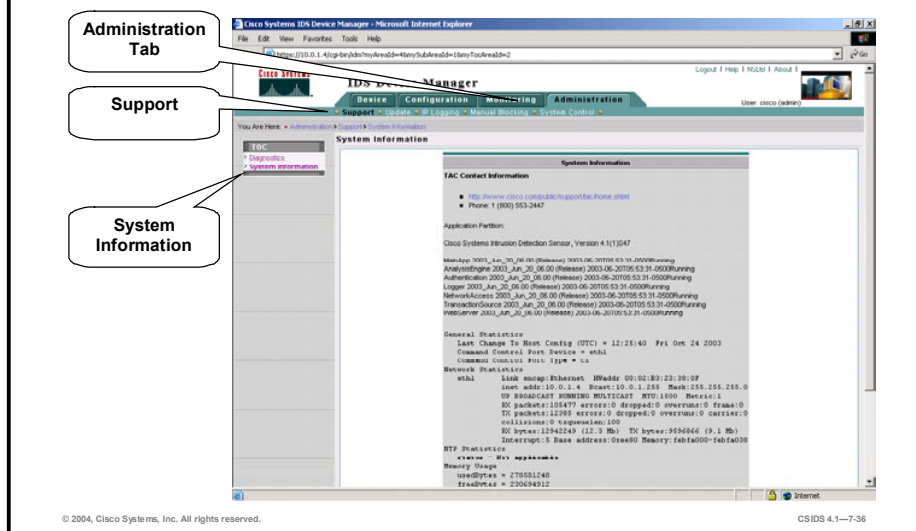
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-35

The next time you open the Diagnostics page, you will see an additional button called View Last Report. Click **View Last Report** to view the most recent report. This report is deleted when you run a new one.

Viewing System Information

Cisco.com



You can view system information by selecting **Administration > Support > System Information**. The System Information page displays the following information:

- Cisco Technical Assistance Center (TAC) contact information
- Software version
- Status of applications
- Interface information
- Resource usage

To access the Cisco Technical Support website, go to:
<http://www.cisco.com/en/US/partner/support/index.html>.

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco.com

- You can use IDM to edit the settings configured via the setup command's interactive prompts.
- You can use IDM to define the time, time zone, and daylight saving time for the Sensor.
- You can use IDM to create and remove users from the local Sensor.
- You can configure up to five monitoring interfaces depending on the type of Sensor you have.
- All monitoring interfaces use the same configuration.
- An interface group provides a way to group monitoring interfaces into one logical virtualSensor.
- A monitoring interface must be part of Group 0 and must be enabled.
- You can use RSA authentication rather than passwords to log in to the Sensor over SSH.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-38

Summary (Cont.)

Cisco.com

- You can use IDM to define the public keys used by clients to log in to the Sensor with RSA authentication.
- The Sensor uses its SSH host key to prove its identity to SSH clients.
- You can use IDM to generate a new SSH host key for the Sensor.
- The server certificate, host certificate, is used by the Sensor to prove its identity to the client.
- A trusted host certificate is used by the Sensor to verify the identity of a connecting host.
- You can use IDM to generate a new server certificate and to add certificates of trusted hosts.
- From the IDM Monitoring tab, you can view Sensor statistics and configure how events will be displayed.
- From the IDM Administration tab, you can obtain diagnostics and system information for troubleshooting.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—7-39

Cisco Intrusion Detection System Alarms and Signatures

Overview

This lesson 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 lesson 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
- Summary

Objectives

This topic lists this lesson's objectives.

Objectives

Cisco.com

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

- **Explain the Cisco IDS signature features.**
- **Explain the master Cisco IDS signature parameters.**
- **Explain the signature engine-specific parameters.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-8-3

Cisco IDS Signatures

This topic 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**
- **Tuned signatures—Built-in signatures that you modify**
- **Custom signatures—New signatures that you create**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-5

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 Internet Control Message Protocol (ICMP) messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your Sensors.

You must enable the signature to monitor network traffic. 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 EventStore. The alert events, as well as other events, may be retrieved from the EventStore by web-based clients. The Sensor logs all alarms at the informational level or higher by default.

Some signatures have subsignatures. This means that the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature.

Built-in signatures are included in the Sensor software. You cannot add to or delete from the list of built-in signatures. You also cannot rename them. Many built-in signatures are based on

known attacks, but some provide information about your Sensor. For example, signature 993 (Missed Packet Count) alerts you if the Sensor is dropping packets. It also tells the percentage dropped to help you tune the traffic level you are sending to the Sensor. If the alarms show that there are no dropped packets or a very small percentage of dropped packets, the Sensor is able to monitor the quantity of traffic being sent. If you see signature 993 alerts with a high percentage of dropped packets, your Sensor is oversubscribed. If signature 993 is firing with 100 percent packet loss, the Sensor is not generating alarms and there is a problem. Make sure that you have the most recent version of the Sensor software. If you have the most recent version, contact the Cisco Technical Assistance Center (TAC) to report the problem.

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

Cisco.com

- **Regular expression string pattern matching**
- **Response actions**
- **Alarm summarization**
- **Threshold configuration**
- **Anti-evasive techniques**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-6

The Cisco IDS signatures have the following features and capabilities:

- **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.
- **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.

Regular Expressions Syntax

Cisco.com

Regular expressions 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]**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1–8.7

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 expressions 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	Whether 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)

Metacharacter	Name	Description
\t	Tab	Matches the tab character (0x09)
\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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1--8-8

The following table shows examples of regex patterns:

To Match	Regular Expression
Hacker	Hacker
Hacker or hacker	[Hh]acker
Variations of bananas, banananas, bananananas	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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-9

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

Note The current list of IDS signatures can be found at:
<http://www.cisco.com/cgi-bin/front.x/csec/idsAllList.pl>

Cisco IDS Alarms

This topic discusses the relationship between Cisco IDS signatures and alarms.

Alarm Overview

Cisco.com

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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-11

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 a signature, which in turn will make the alarm severity level the same as that of the signature.

Alarm Overview (Cont.)

Cisco.com

- **Cisco IDS signatures have defined severity levels:**
 - **Informational**
 - **Low**
 - **Medium**
 - **High**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-12

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 the information provided is 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 topic introduces the signature engines used by Sensors.

Engine Overview

Cisco.com

- **A signature engine is a component of the Sensor that supports a category of signatures.**
- **Cisco IDS signature engines enable you to tune and create signatures unique to your network environment.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-14

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 “Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1” for more information.

Engine Usage

Cisco.com

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 and 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-15

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 and 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, User Datagram Protocol (UDP), and ICMP.
- Sweep—Used to detect network reconnaissance.
- Traffic—Identifies traffic irregularities.
- Trojan—Used to detect Back Orifice Trojan horse 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 topic.

Engine Parameters

Cisco.com

- **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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-16

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.com

- 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-17

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
<code>AlarmDelayTimer</code>	1–3000	The number of seconds to delay further signature inspection after an alarm
<code>AlarmInterval</code>	2–1000	Special handling for time events. Use <code>AlarmInterval Y</code> with <code>MinHits X</code> for <code>X</code> alarms in a <code>Y</code> -second interval.
<code>AlarmSeverity</code>	<ul style="list-style-type: none">■ High■ Medium■ Low■ Informational	The severity of the alert reported in the alarm
<code>AlarmThrottle</code>	<ul style="list-style-type: none">■ <code>FireOnce</code>—Sends the first alarm and then deletes the inspector■ <code>FireAll</code>—Sends all alarms■ <code>Summarize</code>—Sends an <code>IntervalSummary</code> alarm■ <code>GlobalSummarize</code>—Sends a <code>GlobalSummary</code> alarm	Technique used to limit alarm firings
<code>AlarmTraits</code>	0–65535	User-defined traits that further describe the signature

Master Signature Parameters	Value	Description
CapturePacket	<ul style="list-style-type: none"> ■ True ■ False 	Enables the alarm data (evAlert) to contain a copy of the packet that triggered it
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 number of alarms are viewable in the ThrottleInterval.
Enabled	<ul style="list-style-type: none"> ■ True—Enables the signature ■ False—Disables the signature 	Used to enable or disable a signature
EventAction	<ul style="list-style-type: none"> ■ Log ■ Reset ■ ShunHost ■ ShunConnection ■ ZERO 	The action to perform when the alarm is fired
FlipAddr	<ul style="list-style-type: none"> ■ True ■ False 	When true, 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
Protocol	<ul style="list-style-type: none"> ■ 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 host or 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

Master Signature Parameters	Value	Description
SIGID	<ul style="list-style-type: none"> ■ 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
SigVersion	<string>	Defines the signature version in which the signature appears.
StorageKey	<ul style="list-style-type: none"> ■ 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 subsignature
SummaryKey	<ul style="list-style-type: none"> ■ 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
WantFrag	<ul style="list-style-type: none"> ■ TRUE—Only fragmented packets trigger an alarm ■ FALSE—Only non-fragmented packets trigger an alarm ■ <blank>—Fragmented and non-fragmented IP traffic 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 whether 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.

Packet Capture—In Perspective

Cisco.com

	Context Data	Packet Capture	IP Logging
Describes	PAST TCP stream data leading up to the trigger	PRESENT Packet that triggered the alarm	FUTURE Packets that came after the trigger
Reported in	evAlert	evAlert	IP logs
Activated by	Always on for TCP stream signatures	Signature configuration (CapturePacket)	By IP address or signature configuration (EventAction=log)
Contains	Portion of Layer 5 data	Entire frame	Entire frame

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-18

The CapturePacket parameter enables the Sensor to capture the packet that triggers an alert. When packet capture is enabled, the offending packet is encoded in Base64 (a standard encoding schema used in the evAlert) and included in a field of the evAlert. The evAlert contains the entire packet.

The captured packet can be viewed as follows:

- In the command line interface (CLI) as raw hexadecimal data.
- In IDS Device Manager (IDM) as raw hexadecimal data.
- In IDS Event Viewer (IEV) if Ethereal is installed on the same system as IEV. IEV uses Ethereal to display the packet contents.

CapturePacket is different from the context data associated with certain alarms. Context data is for TCP streams only, and contains only the Layer 5 data of the TCP stream and a limited number of bytes. It provides a snapshot of the TCP traffic that preceded the triggering of the signature.

Capture Packet also differs from IP logging. Both features capture entire frames, but their main difference lies in the fact that CapturePacket captures the packet that triggered the alert while IP logging captures packets that come after the trigger.

StorageKey and SummaryKey Parameters

Cisco.com

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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-19

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

Cisco.com

- **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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-20

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.

The designation Axxb could be used for service sweeps in which an attacker is sweeping port 80 across multiple hosts. The attacker port and the victim address are not examined, but the victim port is examined.

The following values are also available for the StorageKey parameter:

- **STREAM**—Source address, source port, destination address and destination port are all examined. This value represents a TCP connection, a full AaBb with stream reassembly.
- **DOUBLE**—This value represents bi-directional AxBx. Both sides of an AxBx connection are counted in one area.
- **ZERO**—Although this value appears in the StorageKey parameter list, it is not used in IDS 4.x.

The AlarmThrottle Parameter and Alarm Summarization

Cisco.com

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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-21

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. Alarm reduction also reduces the amount of data that administrators need to analyze. 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 larger 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 or overwhelm the administrator with noise. 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.

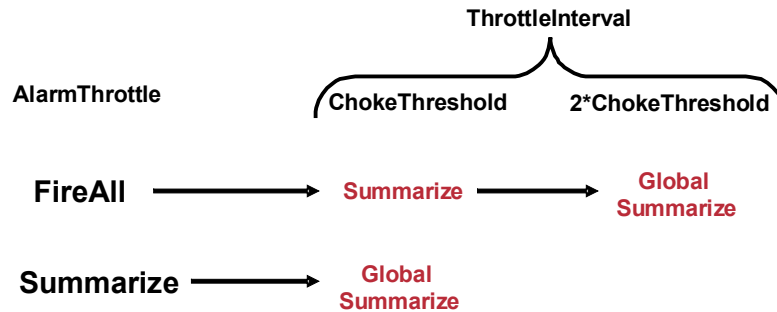
Both alarm summarization modes operate essentially the same, except GlobalSummarize mode consolidates the alarms for all address combinations, whereas the Summarize mode consolidates the alarms only for the address set specified in the SummaryKey parameter.

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 change alarm modes automatically based on the number of alarms detected within the ThrottleInterval parameter.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-9-22

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 alarm 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 GlobalSummarize, if not already at this level, since this is the maximum level of alarm consolidation. At the end of the ThrottleInterval, the signature reverts to its configured original AlarmThrottle mode.

For example, if the signature starts with an 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 to the FireAll alarm mode.

The variable alarm 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 alarm 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.

Master Engine Configuration Restrictions

Cisco.com

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 when the protocol of the inspector does not have ports.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-23

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
- You cannot use a ChokeThreshold when the AlarmThrottle mode is GlobalSummary because summarization is already at its highest level.
- You cannot set a SummaryKey with ports 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. If you do not specify a SummaryKey, the summarization features will not work, and you will receive all the alarms.
- If you use AlarmInterval, you must set the following parameters:
 - Set MinHits to a value greater than 1.
 - Set AlarmThrottle to FireAll.
 - Set ChokeThreshold to a large number such as 1000000.

The AlarmInterval parameter is used to define time-based signatures. Used with the MinHits parameter, it enables the Sensor to fire an alarm if it sees X number of events in Y seconds. The AlarmInterval parameter value supplies the Y part of the equation, while the MinHits parameter value supplies the X value. Configuring the AlarmThrottle and ChokeThreshold as shown in the bullet point enables an accurate MinHits (X) count. Setting the AlarmThrottle to FireAll tells the Sensor not to summarize. Setting the ChokeThreshold to a large number such as 1000000 tells it not to automatically start summarizing if the alarm volume increases.

Atomic Signature Engines

This topic discusses the Atomic signature engines and their specific configuration parameters.

Atomic Signature Engines	
<small>Cisco.com</small>	
Engine Name	Engine Description
Atomic.ARP	Examines ARP packets
Atomic.ICMP	Examines ICMP packets
Atomic.IPOptions	Examines the IP options list in IP packets
Atomic.L3.IP	Examines IP packets
Atomic.TCP	Examines TCP packets
Atomic.UDP	Examines UDP packets

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-25

The Atomic signature engines support signatures that are triggered by the contents of a single packet. Because 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; 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

Cisco.com

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 can exceed the number of ARP replies for a certain IP address before the signature fires

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-28

The following table shows examples of the Atomic.ARP parameters:

Parameter	Value	Attribute	Description
ArpOperation	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the operation code that the signature examines
RequestInbalance	0–65535	<ul style="list-style-type: none">■ 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-27

The following table shows examples of the Atomic.ICMP parameters:

Parameter	Value	Attribute	Description
IcmpCode	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the code value to match in the ICMP header code field
IcmpID	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the identification value to match the ICMP header identifier field
IcmpSeq	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the sequence value of the ICMP header seq field
IcmpType	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the type value to match in the ICMP header type field

Atomic.IPOptions Parameters

Cisco.com

The following are Atomic.IPOptions parameters:

- **HasBadOption**—Defines whether the list of IP options is malformed
- **IPOption**—Defines the IP option code

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-28

The following table shows examples of the Atomic.IPOptions parameters:

Parameter	Value	Attribute	Description
HasBadOption	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Defines whether the list of IP options is malformed
IPOption	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the IP option code

Atomic.L3.IP Parameters

Cisco.com

The following are Atomic.L3.IP parameters:

- **MaxProto**—Configures the signature to fire if the IP protocol value is greater than this value
- **MinProto**—Configures the signature to fire if the IP protocol number is less than this value
- **isRFC1918**—Defines whether the packet is from the RFC 1918 address pool

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-29

The following table shows examples of the Atomic.L3.IP parameters:

Parameter	Value	Attribute	Description
MaxProto	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Triggers an alarm if the IP protocol value is greater than this value
MinProto	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Triggers an alarm if the IP protocol value is less than this value
isRFC1918	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Defines whether the packet is a reserved RFC 1918 address

Atomic.TCP Parameters

Cisco.com

The following are Atomic.TCP parameters:

- **DstPort**—Defines the destination port to match in the TCP header
- **Mask**—Defines the mask used in TCP flags 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-30

The following table shows examples of the Atomic.TCP parameters:

Parameter	Value	Attribute	Description
DstPort	0–65535	<ul style="list-style-type: none"> ■ Not protected ■ Not required 	Defines the destination port to match in the TCP header
Mask	<ul style="list-style-type: none"> ■ FIN ■ SYN ■ RST ■ PUSH ■ ACK ■ URG ■ ZERO 	<ul style="list-style-type: none"> ■ Not protected ■ Required 	Defines the mask used in TcpFlags comparison
SinglePacketRegex	<string>	<ul style="list-style-type: none"> ■ Not protected ■ Not required 	Defines string patterns to search for in a single TCP packet
SrcPort	1–65535	<ul style="list-style-type: none"> ■ Not protected ■ Not required 	Defines a single source port to match in the TCP header
TcpFlags	<ul style="list-style-type: none"> ■ FIN ■ SYN ■ RST ■ PUSH ■ ACK ■ URG ■ ZERO 	<ul style="list-style-type: none"> ■ Not protected ■ Required 	Defines the TCP flags to match when masked by Mask

You can specify which 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. TCP flags that you do not include in the Mask cannot affect 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-31

The following table shows examples of the Atomic.UDP parameters:

Parameter	Value	Attribute	Description
DstPort	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines a single destination port to match in the UDP header
MinUDPLength	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the minimum length of the UDP packet, after which the signature fires

Parameters for All Atomic Engines

Cisco.com

Atomic signatures can be tuned to trigger only on specific source or destination IP addresses.

The following tuning parameters are available for each ATOMIC signature engine:

- **SrcIpAddr and SrcIpMask**
- **DstIpAddr and DstIpMask**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-32

The following parameters, which enable you to tune a signature to trigger only on specific source or destination IP addresses, apply to each ATOMIC signature engine:

- SrcIpAddr and SrcIpMask
- DstIpAddr and DstIpMask

Flood Signature Engines

This topic discusses the Flood signature engines and their specific configuration parameters.

Flood Signature Engines	
	Cisco.com
Engine Name	Engine Description
Flood.Host.ICMP	Looks for an excessive number of ICMP packets sent to a target host
Flood.Host.UDP	Looks for an excessive number of UDP packets sent to a target host
Flood.Net	Looks for an excessive number of packets sent to a network segment

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-34

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 one or many to one 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 one or many to many 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-35

The following table shows examples of the Flood.Host.ICMP parameters:

Parameter	Value	Attribute	Description
IcmpType	0-255	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the type value to match in the ICMP header type field
Rate	0-2147483647	<ul style="list-style-type: none">■ Not protected■ 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-38

The following table lists the Flood.Host.UDP parameters:

Parameter	Value	Attribute	Description
ExcludeDst1	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the destination port to exclude from flood counting
ExcludeDst2	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the destination port to exclude from flood counting
Rate	0–2147483647	<ul style="list-style-type: none">■ Not protected■ Required	Defines the maximum number of UDP packets with the specified type allowed per second

Flood.Net Parameters

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-37

The following table lists the Flood.Net parameters:

Parameter	Value	Attribute	Description
Gap	0–2147483647	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the maximum period of time, above the specified rate, necessary to trigger the signature
Rate	0–2147483647	<ul style="list-style-type: none">■ Not protected■ Not required	The threshold for PPS for a suspect second. A suspect second is defined as the case when the PPS exceeds the Rate. Set the Rate value to 0 for diagnostics/feedback mode.

Service Signature Engines

This topic discusses the Service signature engines and their specific configuration parameters.

Service Signature Engines	
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 string-based pattern matching
Service.IDENT	Examines TCP port 113 traffic
Service.MSSQL	Examines traffic used by Microsoft SQL

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-39

The Service signature engines analyze traffic at and above Layer 5 of the Open Systems Interconnection (OSI) architectural model. This provides protocol decoding for numerous network protocols such as Domain Name System (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.)

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-40

- Service.NTP—Examines Network Time Protocol (NTP) traffic
- Service.RPC—Examines Remote Procedure Call (RPC) traffic
- Service.SMB—Examines Server Message Block (SMB) traffic
- Service.SMTP—Examines Simple Mail Transfer Protocol (SMTP) traffic
- Service.SNMP—Examines Simple Network Management Protocol (SNMP) traffic
- Service.SSH—Examines Secure Shell (SSH) traffic
- Service.Syslog—Examines Syslog traffic

Note The Service.SMTP signature engine is actually a predefined 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 topic later in this lesson.

Service.DNS Parameters

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-41

The following table shows examples of the Service.DNS parameters:

Parameter	Value	Attribute	Description
QuerySrcPort53	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Determines whether the DNS packet source port is port 53
QueryValue	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Determines whether the DNS query is a query or a response

Service.FTP Parameters

Cisco.com

The following are Service.FTP parameters:

- **ServicePorts**—Defines a list of ports where the target service may reside
- **BadPortCmdPort**—Invalid port specified in the port command

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-42

The following table shows examples of the Service.FTP parameters:

Parameter	Value	Attribute	Description
ServicePorts	<set list>	<ul style="list-style-type: none">■ Not protected■ Not required	Defines a list of ports where the target service may reside
BadPortCmdPort	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Invalid port specified in the port command

Service.Generic Parameters

Cisco.com

The following are Service.Generic parameters:

- **DstPort**—Defines the destination port of interest
- **IntermediateInstructions**—Assembly or machine code in string form

Note—Only expert users should attempt to create custom signatures with the Service.Generic engine.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-43

The following table shows examples of the Service.Generic parameters:

Parameter	Value	Attribute	Description
DstPort	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	The destination port of interest for this signature
IntermediateInstructions	<string>	<ul style="list-style-type: none">■ Protected■ Not required	Assembly or machine code in string form. This field is for expert use only.

Service.HTTP Parameters

Cisco.com

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
- **De-obfuscate**—Determines whether to apply anti-evasive HTTP de-obfuscation before examination

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-44

The following table shows examples of the Service.HTTP parameters:

Parameter	Value	Attribute	Description
UriRegex	<string>	<ul style="list-style-type: none">■ Protected■ Not required	Examines the uniform resource identifier (URI) section of the HTTP request to match the regular expression
RequestRegex	<string>	<ul style="list-style-type: none">■ Protected■ Not required	Examines the entire HTTP request to match the regular expression
De-obfuscate	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Determines whether to apply anti-evasive HTTP de-obfuscation before examination

Service.IDENT Parameters

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-45

The following table shows examples of the Service.IDENT parameters:

Parameter	Value	Attribute	Description
MaxBytes	0–65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the maximum amount of data in the payload
hasBadPort	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Defines whether the signature fires due to a bad port number

Service.MSSQL Parameters

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-46

The Service.MSSQL engine inspects the protocol used by Microsoft SQL server. You can add custom signatures based on the Microsoft SQL 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>	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the username to match
passwordPresent	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Defines whether a password was or was not used in a Microsoft SQL login

Service.NTP Parameters

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-47

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	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the mode of operation of the NTP packets
isInvalidDataPacket	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-48

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, batch messages, or 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 count only 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	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the RPC program number to match in the RPC message
Unique	2-40	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the maximum number of unique ports used by an RPC mapper before the signature fires
isSweep	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ 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 that, when opened, causes an alarm to fire

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-49

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 srsvsc 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>	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the account name to watch
FileName	<string>	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the file name of the file that causes an alarm to fire when 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 whether the signature is going to use BruteForceCount
- **IsValidPacket**—Determines whether the signature is going to fire if the packet is valid

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-50

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 whether the CommunityName strings match. The hashes are also stored and compared to determine whether a brute force attack was attempted.

The following table shows examples of the Service.SNMP parameters:

Parameter	Value	Attribute	Description
BruteForceCount	1–32	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the number of unique community strings before the signature fires
IsBruteForce	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Protected■ Not required	Determines whether the signature is going to use BruteForceCount
IsValidPacket	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Protected■ Required	The token that signifies an SNMP protocol violation

Service.SSH Parameters

Cisco.com

The following are Service.SSH parameters:

- **KeyLength**—Defines the RSA key length
- **UserLength**—Defines the maximum length of the username

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-51

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 looks only 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	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the Rivest, Shamir, and Adleman (RSA) key length
UserLength	0-65535	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the maximum length of the username

Service.Syslog Parameters

Cisco.com

The following are Service.Syslog parameters:

- **AcldataSource**—Defines a list of IP addresses that are valid sources of ACL violations
- **AcldataFilterName**—Defines the name of the ACL filter

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-52

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>	<ul style="list-style-type: none">■ Not protected■ Not required	A comma-separated list of IP addresses that are valid sources of ACL violations
AcldataFilterName	<string>	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the name of the ACL filter

State Signature Engines

This topic discusses the State signature engines and the specific configuration parameters.

State.String Signature Engines	
<small>Cisco.com</small>	
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

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-54

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 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 Line Printer Remote (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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-55

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	<ul style="list-style-type: none">■ ToService■ FromService	<ul style="list-style-type: none">■ Protected■ Required	Defines whether the Sensor is listening to traffic destined to or from the service port or both
RegexString	<string>	<ul style="list-style-type: none">■ Protected■ Required	Defines the regular expression
StateName	<ul style="list-style-type: none">■ CiscoLogin■ LPRFormatString	<ul style="list-style-type: none">■ 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-56

The following table lists the State.String.Ciscologin transitions:

Regex String	Required State	Next State	Direction
UserAccessVerification	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

Cisco.com

Regex String	Required State	Next State	Direction
[1-9]	Start	Abort	ToService
%	Start	CiscoDevice	ToService
[x0a\x0d]	FormatChar	Abort	ToService

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-57

The following table lists the State.String.Lprformat transitions:

Regex String	Required State	Next State	Direction
[1-9]	Start	Abort	ToService
%	Start	FormatChar	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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-58

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 topic 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

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-60

The String signature engines support regular expression pattern matching and alarm functionality for ICMP, UDP, and TCP. String signatures match patterns based on a stream of packets, not a single atomic packet. Since network streams comprise more than one packet, matches are made in context within the state of the stream. This type of signature analysis considers the arrival order of packets in a TCP stream and handles pattern matching across packet boundaries. 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

Cisco.com

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 packet

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-61

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	<ul style="list-style-type: none">■ ToService■ FromService	<ul style="list-style-type: none">■ Protected■ Required	Defines whether examined traffic is traveling to or from the service port
RegexString	<string>	<ul style="list-style-type: none">■ Protected■ Required	Defines the string pattern to match in the packet

Sweep Signature Engines

This topic 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

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-63

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 value to match in the ICMP type field
- **Unique**—Defines the maximum number of unique ICMP packets to the target host

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-64

The following table shows examples of the Sweep.Host.ICMP parameters:

Parameter	Value	Attribute	Description
IcmpType	0–255	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the type value to match in the ICMP type field
Unique	2–40	<ul style="list-style-type: none">■ 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 depends 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 past 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-65

The following table lists the Sweep.Host.TCP parameters:

Parameter	Value	Attribute	Description
Mask	<ul style="list-style-type: none">■ FIN■ SYN■ RST■ PSH■ ACK■ URG■ ZERO	<ul style="list-style-type: none">■ Not protected■ Required	Defines the mask used in TcpFlags comparisons
TcpFlags	<ul style="list-style-type: none">■ FIN■ SYN■ RST■ PSH■ ACK■ URG■ ZERO	<ul style="list-style-type: none">■ Not protected■ Required	Defines the TCP flags to match as defined by Mask
Unique	2–40	<ul style="list-style-type: none">■ 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-66

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	<ul style="list-style-type: none">■ FIN■ SYN■ RST■ PSH■ ACK■ URG■ ZERO	<ul style="list-style-type: none">■ Not protected■ Required	Defines the mask used in TcpFlags comparison
PortRange	<ul style="list-style-type: none">■ 0—All■ 1—Low■ 2—High	<ul style="list-style-type: none">■ Not protected■ Required	Defines the port range to examine. Valid values include the following: <ul style="list-style-type: none">■ 0—All ports■ 1—Low ports (1–1023)■ 2—High ports (1024–65535)

Parameter	Value	Attribute	Description
TcpFlags	<ul style="list-style-type: none"> ■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO 	<ul style="list-style-type: none"> ■ Not protected ■ Required 	Defines the TCP flags to match as defined by Mask
Unique	2–40	<ul style="list-style-type: none"> ■ 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-67

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>	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the list of ports or port ranges to examine
Unique	2–40	<ul style="list-style-type: none">■ 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-68

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	<ul style="list-style-type: none">■ 0—All■ 1—Low■ 2—High	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the list of ports or port ranges to examine. Valid values are as follows: <ul style="list-style-type: none">■ 0—All■ 1—Low (1–1023)■ 2—High (1024–65535)
TcpFlags1	<ul style="list-style-type: none">■ FIN■ SYN■ RST■ PSH■ ACK■ URG■ ZERO	<ul style="list-style-type: none">■ Not protected■ Required	Defines the TCP flags to match

Parameter	Value	Attribute	Description
TcpFlags2	<ul style="list-style-type: none"> ■ FIN ■ SYN ■ RST ■ PSH ■ ACK ■ URG ■ ZERO 	<ul style="list-style-type: none"> ■ 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 (1–1023)
- 2—High ports (1024–65535)

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-69

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	<ul style="list-style-type: none">■ 1–SATAN Normal■ 2–SATAN Heavy	<ul style="list-style-type: none">■ Not protected■ Not required	Defines predefined TCP ports of interest
UdpInterest	<ul style="list-style-type: none">■ 1–SATAN Normal■ 2–SATAN Heavy	<ul style="list-style-type: none">■ Not protected■ Not required	Defines predefined UDP ports of interest
UniqueTcpPorts	2–40	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the number of unique TCP connections allowed
UniqueUdpPorts	2–40	<ul style="list-style-type: none">■ 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 topic describes miscellaneous signature engines that handle nonstandard protocol signatures and signatures that do not fit into the other engine protocol decodes.

Trojan Signature Engines

Cisco.com

Engine Name	Engine Description
Trojan.BO2K	Examines UDP and TCP traffic for nonstandard Back Orifice traffic
Trojan.TFN2K	Examines UDP, TCP, or ICMP traffic for irregular traffic patterns and corrupted headers
Trojan.UDP	Examines UDP traffic for Trojan attacks

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—8-71

Attackers can place backdoor 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, or ICMP traffic for irregular traffic patterns and corrupted headers
- Trojan.UDP—Examines UDP traffic for Trojan attacks

Back Orifice 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 Back Orifice 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 Layer 3 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-72

There is only one Traffic signature engine, Traffic.ICMP. The Traffic.ICMP signature engine supports signatures that are triggered by nonstandard usage of the ICMP protocol. Tools that exploit ICMP traffic include TFN, TFN2K, Stacheldraht, and Loki.

Loki is another type of backdoor attack. 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	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ Not protected■ Not required	Defines whether the signature is looking for the original Loki attack
isModLOKI	<ul style="list-style-type: none">■ True■ False	<ul style="list-style-type: none">■ 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-73

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	<ul style="list-style-type: none">■ Not protected■ Not required	Defines a maximum number of old dateless client-to-server ACKs before a hijack is triggered
SynFloodMaxEmbryonic	0–2147483647	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the maximum number of allowed simultaneous embryonic connections to any service
TrafficFlowTimeout	0–2147483647	<ul style="list-style-type: none">■ Not protected■ Not required	Defines the number of seconds that must pass with no traffic to fire an alarm

Summary

This topic summarizes this lesson.

Summary

Cisco.com

- **A signature is a set of rules that your Sensor uses to detect typical intrusive activity.**
- **The Sensor compares network activity with its enabled signatures and generates an alarm when a match is found.**
- **A signature engine is a component of the Sensor that supports a category of signatures.**
- **Each signature engine is designed for a specific type of traffic.**
- **Each engine has a set of parameters that help define the behavior of the signatures controlled by the engine.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-75

Summary (Cont.)

Cisco.com

- Parameters can be modified so that signatures meet the needs of your network environment.
- 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
- Cisco IDS signatures can summarize alarms to reduce the number of single alarms generated.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—8-76

Signature Configuration

Overview

This lesson explains how to configure signatures, including tuning signatures and creating custom signatures. This lesson includes the following topics:

- Objectives
- Signature configuration
- Signature tuning
- Custom signatures
- Custom signature scenarios
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

- **Configure a signature's enable status, severity level, and action.**
- **Tune a signature to perform optimally based on a network's characteristics.**
- **Create a custom signature given an attack scenario.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-9.3

Signature Configuration

This topic explains how to perform basic signature configuration.

Signature Configuration Tasks

Cisco.com

Basic signature configuration includes the following:

- **Enabling or disabling the signature**
- **Assigning the severity level**
- **Assigning the signature action**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—9-5

By default, the Cisco Intrusion Detection System (IDS) signatures are configured to meet the needs of most average deployments. The most critical signatures are enabled to provide you immediately with a certain level of security. Depending on your security policy and the location of your Sensor or Sensors, you may choose to enable specific signatures that are disabled by default, tune certain signatures, or even create custom signatures. Before modifying any signature settings or creating new signatures, study the built-in signatures and their default settings and consider the following:

- **Network protocols**—Consider the network protocol of the traffic to be examined. For example, if you are concerned with Enhanced Interior Gateway Routing Protocol (EIGRP) packets, you might want to examine the configurable parameters of signatures that examine IP packets and are triggered by the contents of a single packet. The Atomic.L3.IP engine supports such signatures. It could be used to create a custom signature to meet this need because it enables you to specify the IP protocol number.
- **Target address**—Consider the target of any anticipated attack. For example, if you are concerned with an excessive number of packets being sent to a specific network, you might want to examine the configurable parameters of signatures that detect an excessive volume of packets sent to a network. The Flood.Net engine supports such signatures.
- **Target port**—Consider the anticipated target ports of the attack. For example, if you are concerned with connections to a specific UDP port or a range of UDP ports, you might want to examine the configurable parameters of signatures that detect those connections. The Sweep.Port.UDP engine supports such signatures.
- **Type of attack**—Consider any anticipated type of attack. For example, if you anticipate denial of service (DoS) attacks, you might want to examine the signatures supported by the Flood engines, which are commonly used to detect DoS attacks. If you anticipate

reconnaissance attacks, you might want to examine the signatures supported by the Sweep engines, which are commonly used to detect network reconnaissance attacks.

Note Although engines are designed to detect certain attacks, they are 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—Consider the need to inspect the payload of a packet for a string pattern. For example, if you need to detect a string pattern in a TCP packet, you might want to examine the configurable parameters of the String.TCP engine, which are designed to detect a string pattern in a TCP packet.

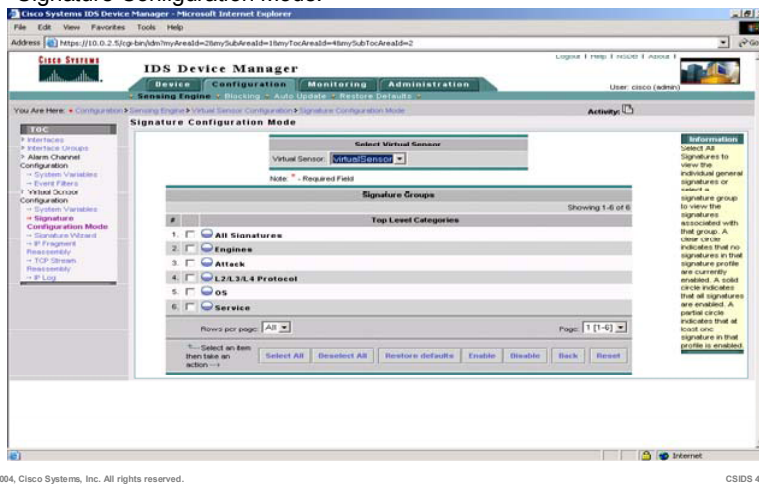
After determining the needs of your specific deployment and familiarizing yourself with the built-in signatures and their default settings, you can begin modifying signature settings as needed. All signatures have the following basic configurable parameters:

- Enable—Enables or disables the signature
- AlarmSeverity—Assigns the severity level (information, low, medium, or high)
- EventAction—Assigns the action to take if the signature is triggered (log, reset, block host, or block connection)

Accessing the Signature Configuration Page

Cisco.com

Choose **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode**.



You can access signatures of interest in a variety of ways via IDS Device Manager (IDM). Select **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode** to go to the Signature Configuration Mode page, which displays a list of top-level categories of signature groups. From this page, you can enable and disable signature groups, view all signatures, and restore defaults to signatures that you have tuned.

Each group displays its enable level (the disabled, partially enabled, or enabled icon). A clear circle indicates that no signatures in that group are enabled. A solid circle indicates that all signatures in the group are enabled. A partially filled circle indicates that at least one signature in that group is enabled. You can enable or disable all signatures in a group by selecting the group's check box and then clicking the Enable or Disable button.

You can access and view all signatures by clicking any of the following:

- All Signatures—Enables you to view all individual signatures at once.
- Engines—Enables you to view signatures grouped by engine.
- Attack—Enables you to view signatures grouped by attack types.
- L2/L3/L4 Protocol—Enables you to view signatures grouped by network protocol type.
- OS—Enables you to view signatures grouped by OS type.
- Service—Enables you to view signatures grouped by network service.

A signature can be in multiple groups. Editing a signature in one group affects it in all groups. For example, if you enable all general attack signatures in the Attack category, signature 7107 is enabled. If you disable the Atomic.ARP signatures in the Engine category, signature 7107 is disabled. The last edit that you make is the one that is applied.

All Signatures Group

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select All Signatures.

NSDB Information on signature 1001

ID	Enabled	ID	SubID	Name	Type	Severity	Action	More
1	<input type="checkbox"/>	993	0	Missed Packet Count	Dut-in	Informational		
2	<input type="checkbox"/>	994	1	Traffic Flow Started	Dut-in	Informational		
3	<input type="checkbox"/>	994	2	Traffic Flow Stopped	Dut-in	Informational		
4	<input type="checkbox"/>	995	1	Traffic Flow Stopped	Dut-in	Informational		
5	<input type="checkbox"/>	995	2	Traffic Flow Stopped	Dut-in	Informational		
6	<input type="checkbox"/>	1000	0	DND P-OPTION	Dut-in	Informational		
7	<input type="checkbox"/>	1001	0	Record Packet Rte	Dut-in	Informational		
8	<input type="checkbox"/>	1002	0	Timestamp	Dut-in	Informational		
9	<input type="checkbox"/>	1004	U	Smurfs v.v.j.joc	Dut-in	Informational		
10	<input type="checkbox"/>	1004	0	Loose Src Rte	Dut-in	high		
11	<input type="checkbox"/>	1004	0	Loose Src Rte	Dut-in	high		

Rows per page: 10 | Page: 1 of 1 (993-1004)

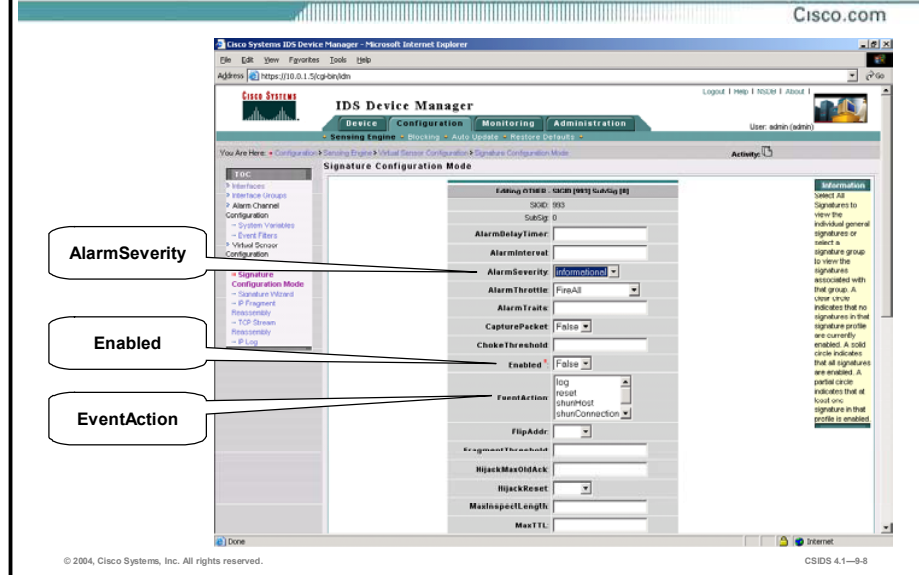
If you are looking for a particular signature, select **All Signatures** from the Signature Configuration Mode page, and use the browser's search option to find the desired string, which could be either the signature ID or the signature name. When you select All Signatures, the list of all individual signatures is displayed. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to another page by selecting one from the Page popup menu.

Selecting All Signatures from the top-level categories list takes you immediately to the individual signature level. Choosing any of the signature groups requires you to drill down to the signature level. However, after you have arrived at the individual signature level, you can enable, disable, and edit individual signatures. You can edit only one signature at a time.

To configure any signature, select the signature's check box and then click the appropriate button at the bottom of the page. Clicking the Restore Defaults button returns a single signature to its default settings. The Edit button displays the configurable parameters for the signature.

Regardless of how you access the individual signature level, you can click any signature ID number from the individual signature level and see the description of the signature in the Network Security Database (NSDB). Throughout IDM, click **Back** to return to the previous page.

Basic Signature Configuration



When you select a signature check box and click the Edit button, the configurable parameters for that signature are displayed. Although the list of parameters varies from signature to signature, the basic configurable parameters discussed earlier in this topic are available for all signatures. The following are those parameters:

- AlarmSeverity—From the drop-down menu, select one of the following severity levels for the signature:
 - Informational
 - Low
 - Medium
 - High
- Enabled—From the drop-down menu, select **True** to enable the signature or select **False** to disable it.
- EventAction—Select any of the following actions for the Sensor to take when the signature is triggered:
 - Log—This action writes the IP session data to a 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.
 - Reset—This action 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.
 - ShunHost—Denies the source IP address. This action denies all IP packets from the blocked address. The following is an example of the deny access control entry (ACE) created on the blocking device:

```
deny ip host 10.1.1.1 any
```

- **ShunConnection**—Denies only the IP packets from the source IP address to a specific destination IP address, destination port, and service. **ShunConnection** 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
```

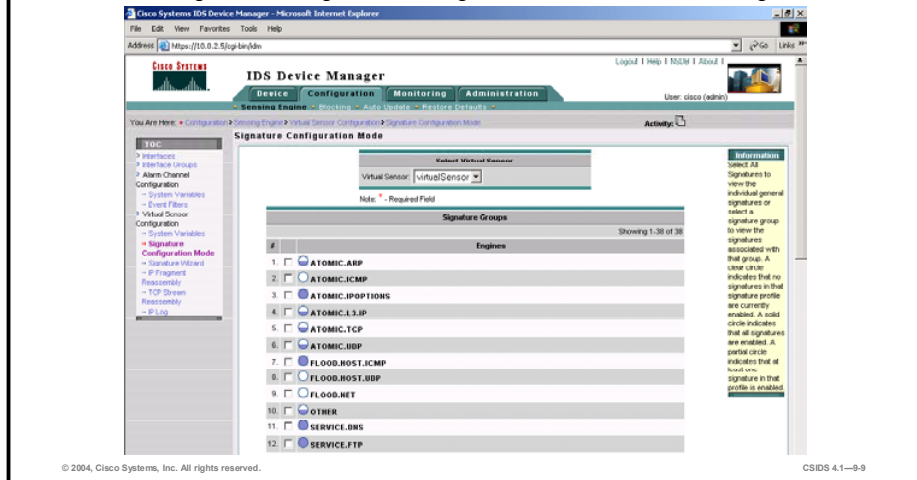
In addition to denying the connection in which the attack was executed, **ShunConnection** denies all connections of that type to that destination address. All connections for that service from the source to the destination IP address will be denied. If an attacker executes a web attack against a web 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 the attacker can continue to make web connections to other IP addresses.

Note ShunHost and ShunConnection are the blocking actions that the Sensor can perform.

Engines Group

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select Engines.



The figure shows the engines list displayed when you select the Engines category from the Signature Configuration Mode page. Selecting an engine from the engines list takes you to the individual signatures for that engine.

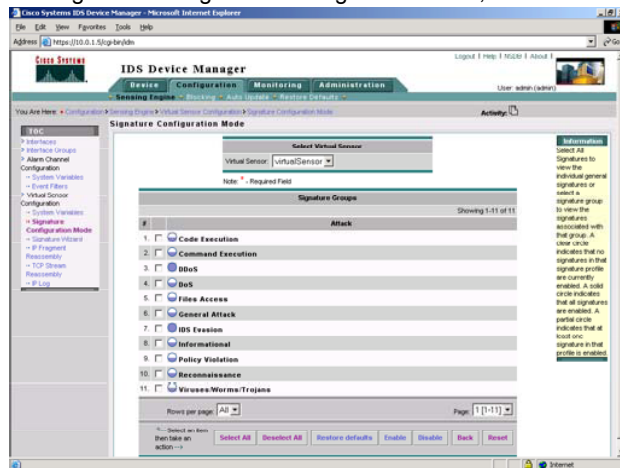
You can enable, disable, or restore defaults for all signatures within any engine by selecting the check box for that engine and then clicking the appropriate button at the bottom of the page.

Note The figure does not display the entire Engines list.

Attack Group

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select Attack.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-9-10

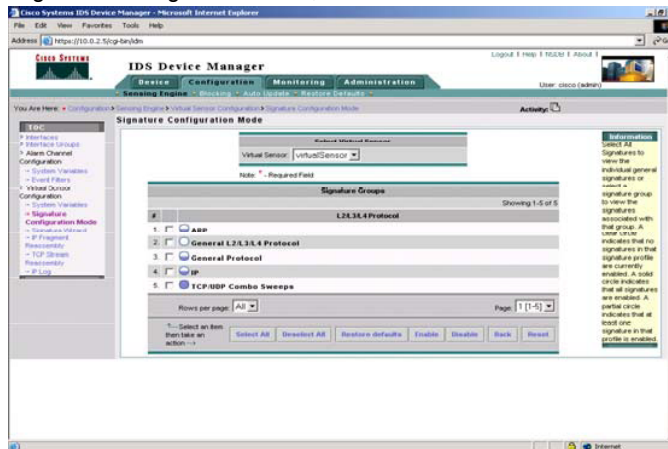
The figure shows the list of attack types displayed when you select the Attack category from the Signature Configuration Mode page. Selecting an attack type from the list takes you to the individual signatures that inspect traffic for that type of attack.

You can enable, disable, or restore defaults for all signatures for an attack type by selecting the check box for that attack type and then clicking the appropriate button at the bottom of the page.

L2/L3/L4 Protocol Group

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select L2/L3/L4 Protocol.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-11

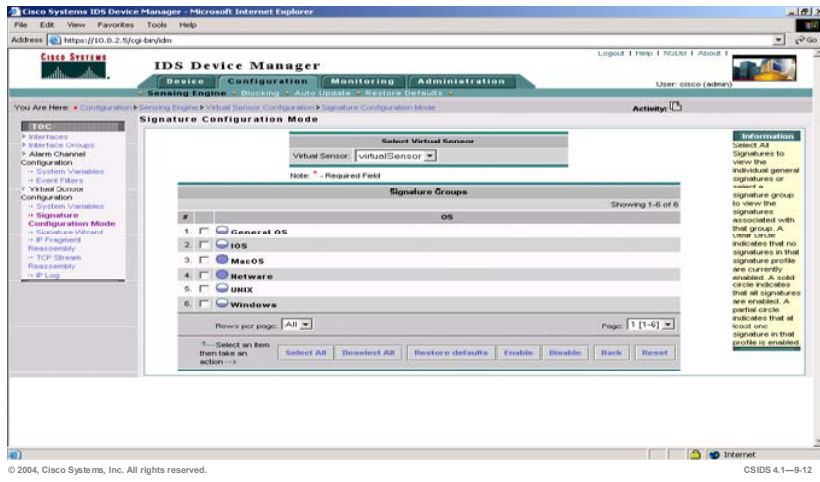
The figure shows the list of network protocols displayed when you select the L2/L3/L4 Protocol category from the Signature Configuration Mode page. Selecting a protocol from the list takes you to the individual signatures that inspect traffic for that protocol.

You can enable, disable, or restore defaults for all signatures in a protocol group by selecting the check box for that protocol and then clicking the appropriate button at the bottom of the page.

OS Group

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select OS.



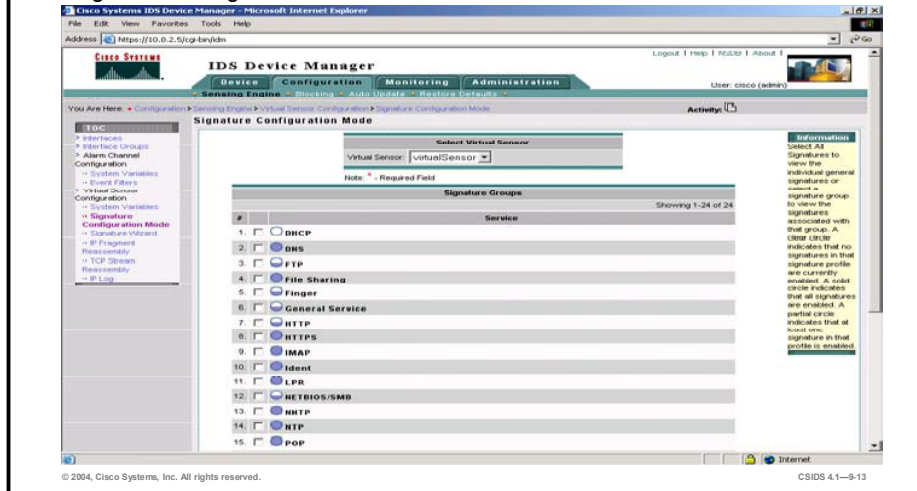
The figure shows the list of operating system types displayed when you select the OS category from the Signature Configuration Mode page. Depending on the operating system you select, you may be taken directly to the individual signatures that support that operating system, or you may be taken to a list of specific operating systems within that operating system type.

You can enable, disable, or restore defaults for all signatures for an operating system type by selecting the check box for that operating system type and then clicking the appropriate button at the bottom of the page.

Service Group

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select Service.



The figure shows the list of network services displayed when you select the Service category from the Signature Configuration Mode page. Selecting a service from the list takes you to the individual signatures that inspect traffic for that service.

You can enable, disable, or restore defaults for all signatures for a service by selecting the check box for that service and then clicking the appropriate button at the bottom of the page.

Note The figure does not display the entire list of services.

Signature Tuning

This topic explains the tasks involved in tuning Cisco IDS signatures. A scenario in which a network security administrator tunes an existing signature is used to clarify the process.

Tuning Signatures

Cisco.com

Complete the following tasks to tune a signature:

- **Choose the signature to tune.**
- **Modify the signature parameter values.**
- **Save and apply the new signature parameter settings to the Sensor.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—9-15

The Cisco IDS enables you to tune existing signatures to perform optimally in your network. 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.
- Modify the signature parameter values—This task involves modifying the signature parameter values that are required to meet your needs.
- Save and apply the new signature parameter settings to the Sensor—This task involves clicking the save changes icon in the Activity bar.

Tuning Scenario—FTP Login

Cisco.com

- **A company FTP server stores software that is being beta tested by customers. The company wants to detect unauthorized login attempts.**
- **By examining the FTP service signatures, the network security administrator discovers signature 6250, the Auth Failure FTP signature.**
- **After examining the parameters for signature 6250, the administrator decides to tune the signature to do the following:**
 - **Trigger a high-severity alarm after two failed login attempts.**
 - **Send an alarm event every time the attack is detected.**
 - **Terminate the session.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-16

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.

Tuning Scenario—FTP Login (Cont.)

Cisco.com

- The administrator decides to modify the values of the following signature parameters to satisfy the current needs:
 - AlarmSeverity—To trigger a high-severity alarm
 - AlarmThrottle—To send an alarm event every time the attack is detected
 - EventAction—To terminate the session when the signature fires
 - MinHits—To trigger the alarm after two failed login attempts
- The default values of the remaining parameters are accepted.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-17

The following signature parameter values are modified based on the scenario requirements:

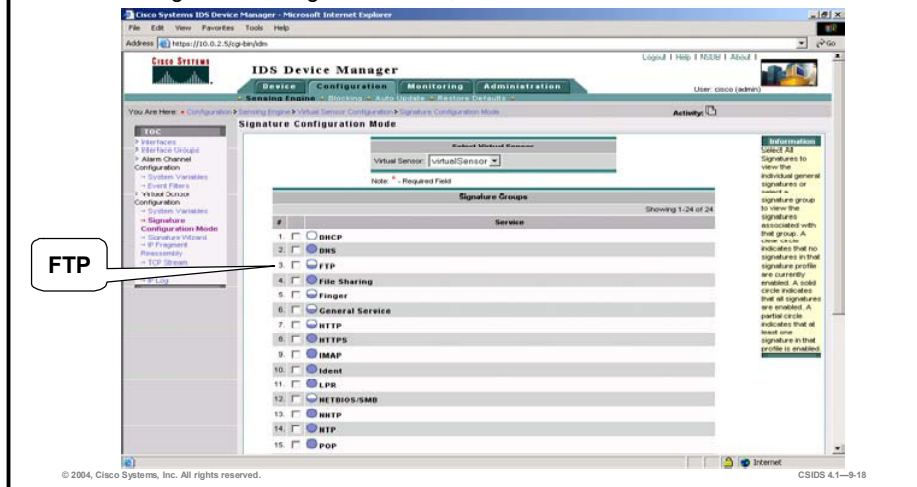
- AlarmSeverity—AlarmSeverity is set to High so that a high-severity alarm is triggered.
- AlarmThrottle—AlarmThrottle is set to FireAll so that an alarm event is sent every time the attack is detected.
- EventAction—EventAction is set to reset to terminate the session.
- MinHits—MinHits is set to 2 so that the signature fires after two failed login attempts.

Note The default values of the remaining parameters are accepted.

Login Scenario Configuration

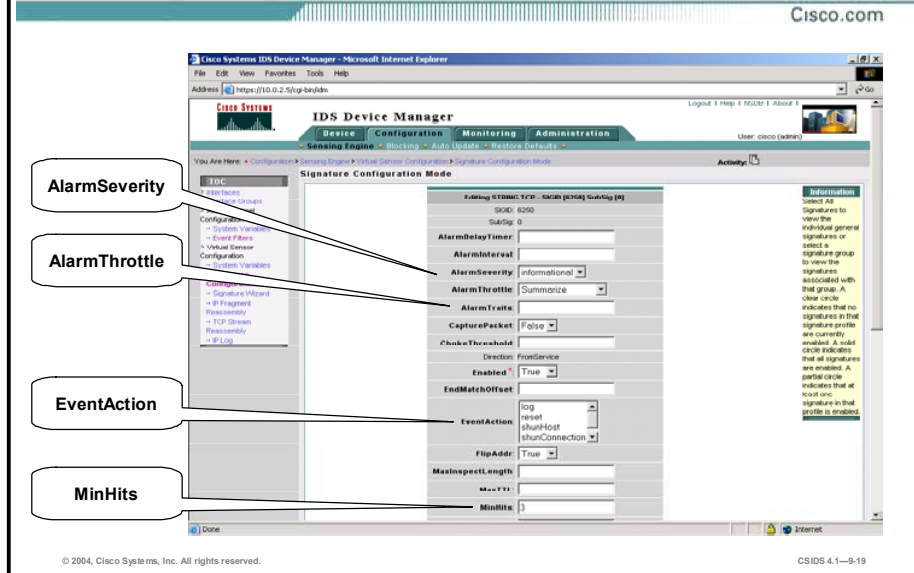
Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode, and select Service.



The Auth Failure FTP signature can be located by selecting **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode > Service** and then selecting the **FTP** check box.

Login Scenario Configuration (Cont.)

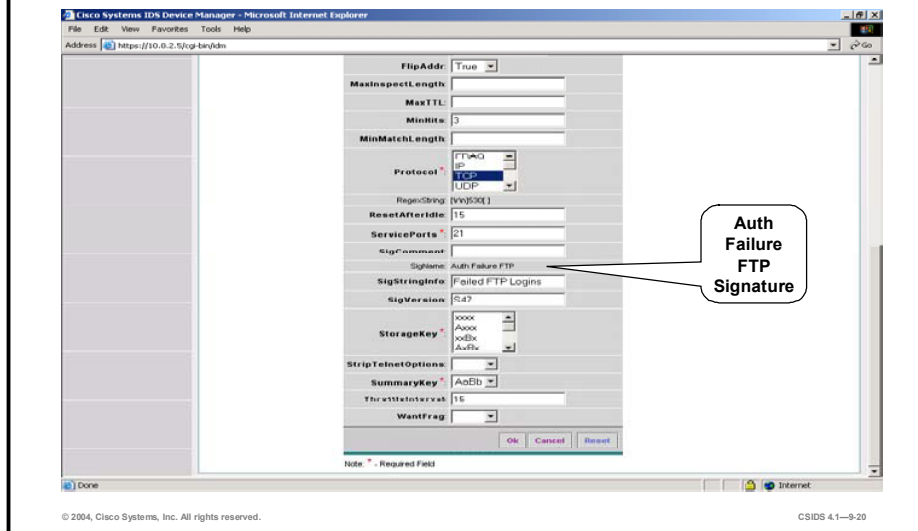


The figure shows the default settings for the parameters that are modified in this tuning scenario. The parameters are modified as follows:

- Use the AlarmSeverity drop-down menu to change the AlarmSeverity value from Informational to **High**.
- Use the AlarmThrottle drop-down menu to change the AlarmThrottle value from Summarize to **FireAll**.
- Select **reset** from the EventAction pane.
- Enter **2** in the MinHits field.

Login Scenario Configuration (Cont.)

Cisco.com



The figure shows the name of the signature as it appears in the parameters list.

Custom Signatures

This topic discusses how to create custom signatures using Cisco IDS signature micro-engines. Scenarios in which you might want to create custom signatures are used to explain the process.

Creating Custom Signatures

Cisco.com

The Signature Wizard in IDM:

- **Guides you through the process of creating custom signatures**
- **Enables you to create custom signatures without detailed knowledge of all the signature engines and their parameters**
- **Consists of six tasks:**
 - **Choosing the signature type**
 - **Identifying the signature**
 - **Setting the engine-specific parameters**
 - **Setting the alert response**
 - **Setting the alert behavior**
 - **Completing the custom signature**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-9-22

New vulnerabilities are discovered more quickly than new signature releases can be developed and tested. Cisco IDS Sensors enable you to create custom signatures to detect new vulnerabilities and other unique attacks.

The Signature Wizard in IDM provides a step-by-step procedure for configuring custom signatures. Once you are more familiar with the process, you can also configure custom signatures through Virtual Sensor Configuration mode.

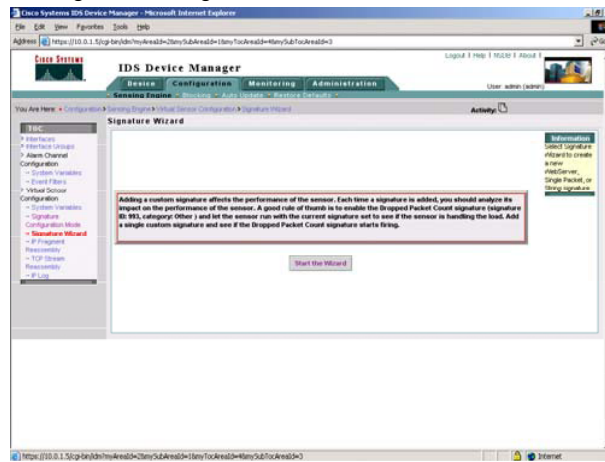
The Signature Wizard consists of the following tasks:

- Choosing the signature type (Signature Type)
- Identifying the signature (Signature Identification)
- Setting the engine-specific parameters (Engine-Specific Parameters)
- Setting the alert response (Alert Response)
- Setting the alert behavior (Alert Behavior)
- Completing the custom signature (Finish)

Start the Signature Wizard

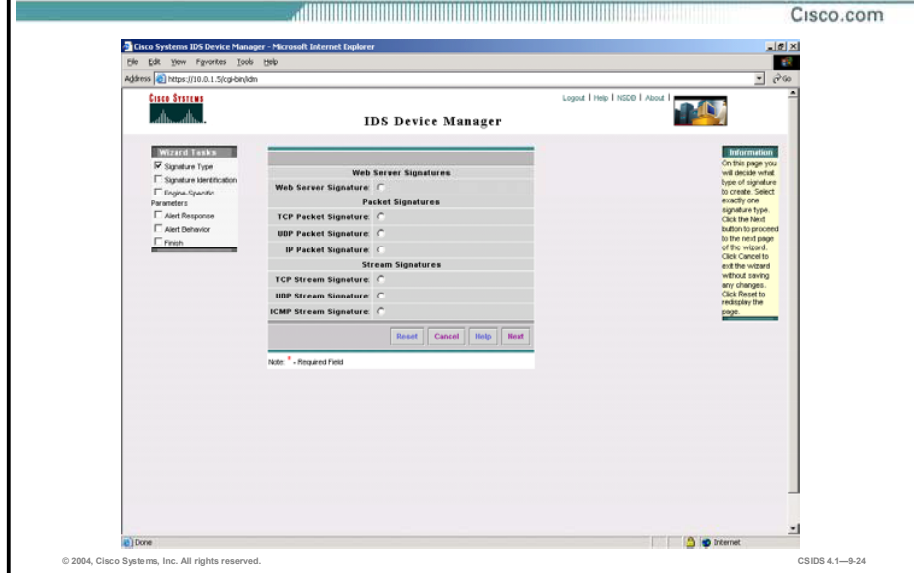
Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Wizard.



To start the Signature Wizard, select **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Wizard**. When the Signature Wizard main page is displayed, click the **Start the Wizard** button.

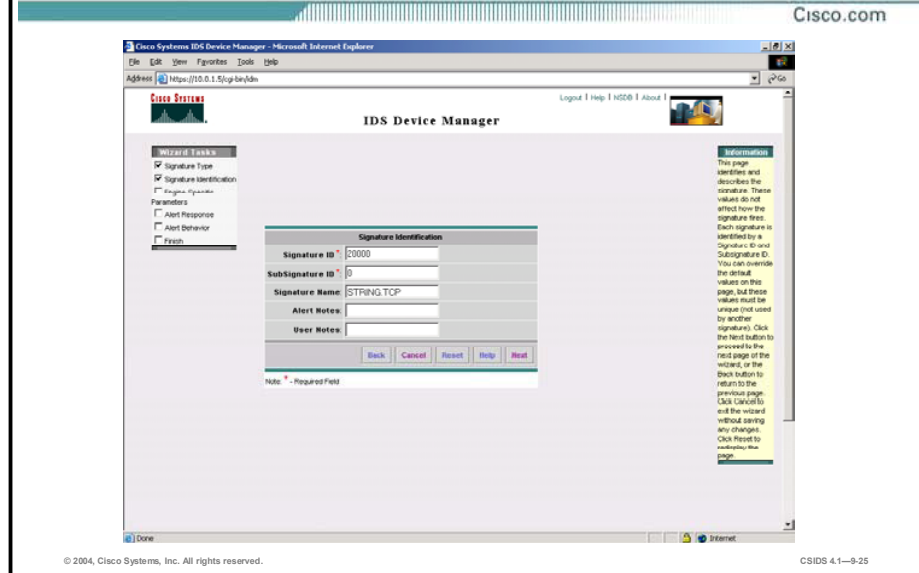
Select the Signature Type



The first wizard task for configuring a custom signature is selecting a signature type. Click **Next** after selecting a signature type. The signature types are as follows:

- **Web Server Signatures**—Capture regular expressions in web URL requests and check arguments, uniform resource identifier (URI) length, and other parameters. These signatures search traffic directed to web services or HTTP requests only. Return traffic cannot be inspected using these signatures. You can specify separate web ports of interest in each signature.
- **Packet Signatures (TCP, UDP, or IP)**—Inspect traffic by protocol and port. Packet signatures are also known as Atomic signatures.
- **Stream Signatures (TCP, UDP, or ICMP)**—Perform simple stateful expression-matching based on protocol and port.

Configure the Signature Identification Parameters

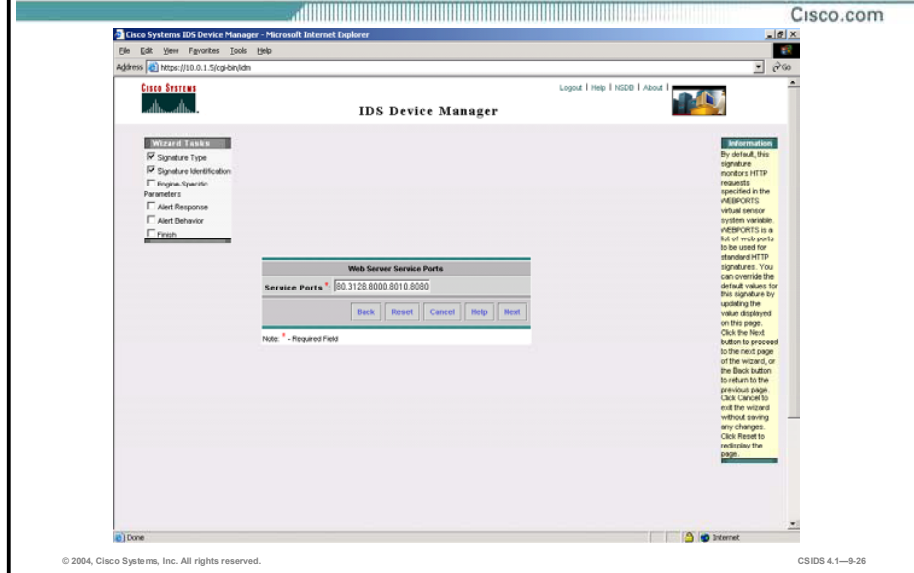


After you choose the signature type, you must configure the identification parameters. Complete the second wizard task by filling in the Signature Identification fields as follows:

- **Signature ID**—Enter a number in the range of 20,000 to 50,000.
- **SubSignature ID**—Enter a number. The default is 0. Subsignature IDs are useful if you are grouping similar signatures.
- **Signature Name**—Enter a name. By default, the signature engine name (according to the signature type that you chose) appears in the Signature Name field. Change it to a name that is more closely related to your custom signature. The signature name, along with the signature ID and subsignature ID, are reported to the IDS Event Viewer (IEV) when an alert is generated.
- **Alert Notes**—(Optional.) Enter any text you want included in alarms associated with this signature. These notes are reported to IEV when an alert is generated.
- **User Notes**—(Optional.) Enter any text that you find useful. This field does not affect the signature or alert in any way, but may include useful information that identifies the purpose and use of the custom signature.

When you have finished completing the Signature Identification fields, click **Next**. If you are creating a web server signature, you are presented with the Web Server Service Ports page, where you can enter the ports you want the signature to monitor.

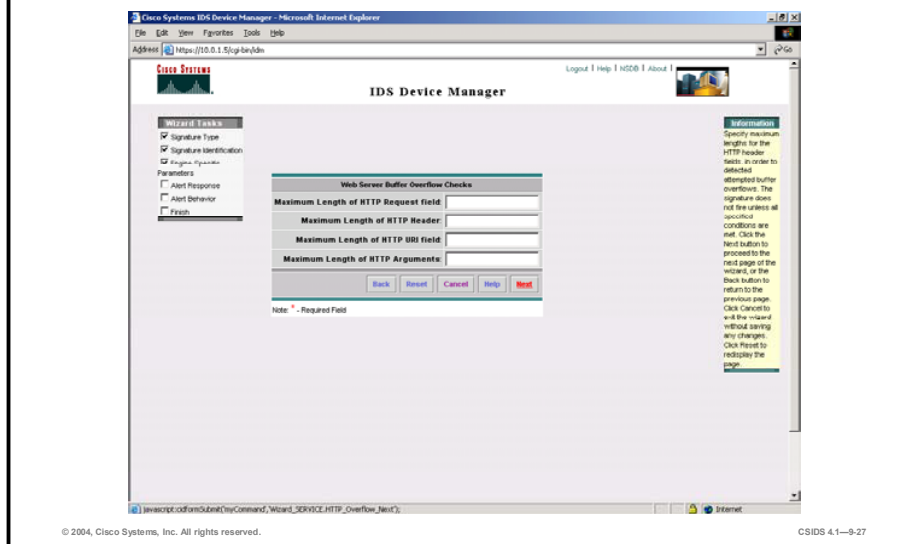
Configure Web Server Service Ports for Web Server Signatures



By default, web server signatures monitor HTTP requests specified in the WEBPORTS virtual sensor system variable. WEBPORTS is a list of web ports to be used for standard HTTP signatures. The default web ports are 80, 3128, 8000, 8010, 8080, 8888, and 24326. You can modify the ports to reflect the ports you want the signature to monitor.

Configure the Engine-Specific Parameters—Web Server Signatures

Cisco.com

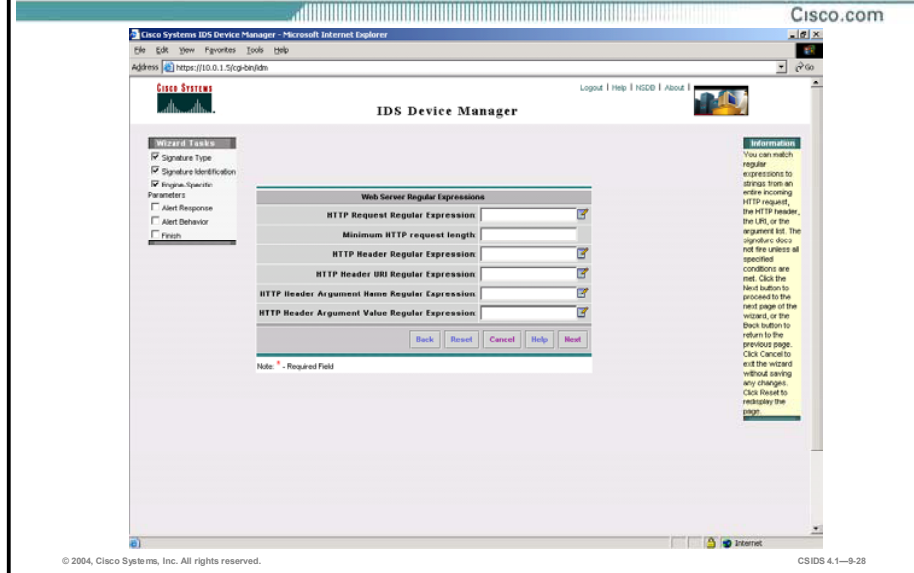


After configuring the signature identification parameters, you must configure the parameters that are specific to the type of signature you are creating. Web server signatures allow you to match regular expressions to strings from an entire incoming HTTP request, the HTTP header, the URI, or the argument list. You can also check for potential buffer overflow conditions in these fields. To do so, enter the number of bytes that indicate attempted buffer overflows in the following Web Server Buffer Overflow Checks fields:

- Maximum Length of HTTP Request—Enables you to specify a maximum length for the entire HTTP request.
- Maximum Length of HTTP Header—Enables you to specify a maximum length for the entire HTTP header.
- Maximum Length of HTTP URI—Enables you to specify a maximum length for the HTTP URI.
- Maximum Length of HTTP Arguments—Enables you to specify a maximum length for the HTTP argument list.

Note The signature does not fire unless all specified conditions are met.

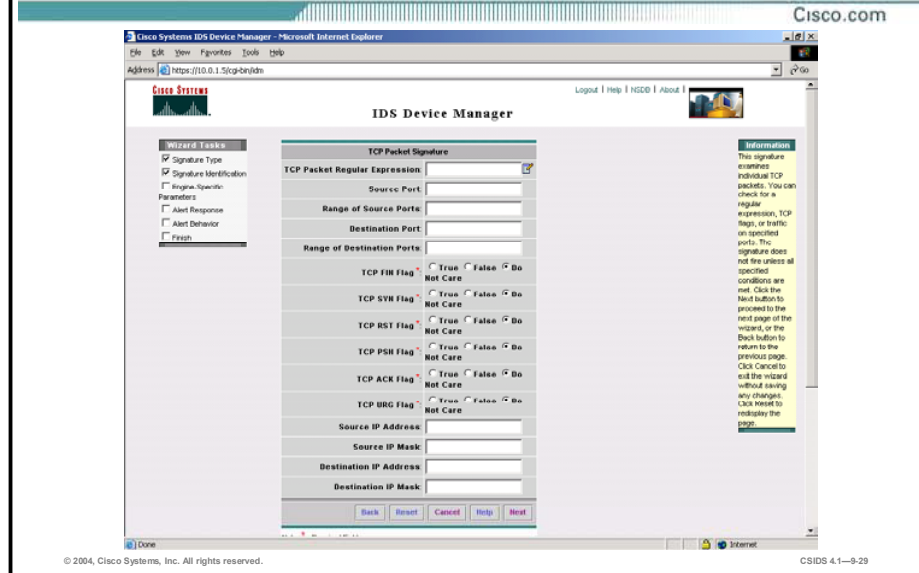
Engine-Specific Parameters—Web Server Signatures (Cont.)



You can match regular expressions to strings from an entire incoming HTTP request, the HTTP header, the URI, or the argument list. Enter any regular expressions you want to match in the Web Server Regular Expressions fields:

- HTTP Request Regular Expression—Enables you to specify a regular expression that matches text in the entire HTTP request.
- Minimum HTTP request length—Enables you to specify a minimum length for the request before the regular expression will match it. You can set the minimum length only if your request regular expression contains a * or + regular expression operator.
- HTTP Header Regular Expression—Enables you to specify a regular expression that matches text in the HTTP header.
- HTTP Header URI Regular Expression—Enables you to specify a regular expression that matches text in the HTTP header URI.
- HTTP Header Argument Name Regular Expression—Enables you to specify a regular expression that matches an HTTP header argument name.
- HTTP Header Argument Value Regular Expression—Enables you to specify a regular expression that matches an HTTP header argument value.

Configure the Engine-Specific Parameters—TCP Packet Signatures



TCP packet signatures examine individual TCP packets. They check for a regular expression, TCP flags, or traffic on specified ports. The signature does not fire unless all specified conditions are met.

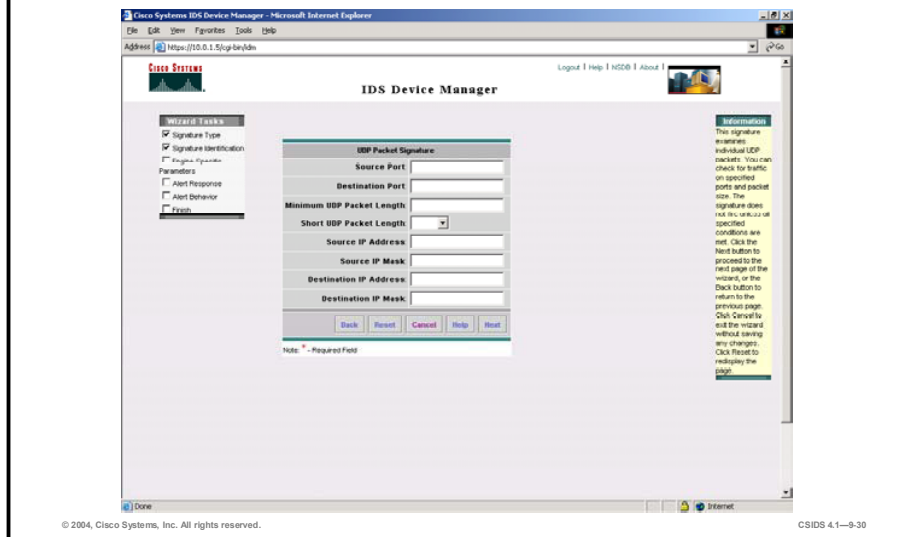
For TCP packet signatures, the following parameters are configurable:

- **TCP Packet Regular Expression**—Enables you to specify a regular expression to match in the text of the TCP packet. Clicking the icon next to the TCP Packet Regular Expression field opens the Regular Expression Builder, which can help you create regular expressions.
- **Source Port**—Enables you to specify a source port to match in the TCP packet. Allowable values are 0 to 65535.
- **Range of Source Ports**—Enables you to specify a range of source ports to match in the TCP packet. You can enter any of the following values:
 - 0—All ports
 - 1—Low ports (0 to 1023)
 - 2—High ports (1024 to 65535)
- **Destination Port**—Enables you to specify a destination port to match in the TCP packet. Allowable values are 0 to 65535.
- **Range of Destination Ports**—Enables you to specify a range of destination ports to match in the TCP packet. You can enter any of the following values:
 - 0—All ports
 - 1—Low ports (0 to 1023)
 - 2—High ports (1024 to 65535)

- TCP FIN Flag, TCP SYN Flag, TCP RST Flag, TCP PSH Flag, TCP ACK Flag, TCP URG Flag—Enable you to specify the TCP flags to match in the TCP packet. The allowable values are as follows:
 - True—The signature fires if the flag is set.
 - False—The signature does not fire if the flag is set.
 - Do Not Care—The flag is not inspected.
- Source IP Address—Enables you to specify the source host or network IP address to match in the TCP packet.
- Source IP Mask—Enables you to specify the netmask for the source host or network.
- Destination IP Address—Enables you to specify the destination host or network IP address to match in the TCP packet.
- Destination IP Mask—Enables you to specify the netmask for the destination host or network.

Configure the Engine-Specific Parameters—UDP Packet Signatures

Cisco.com

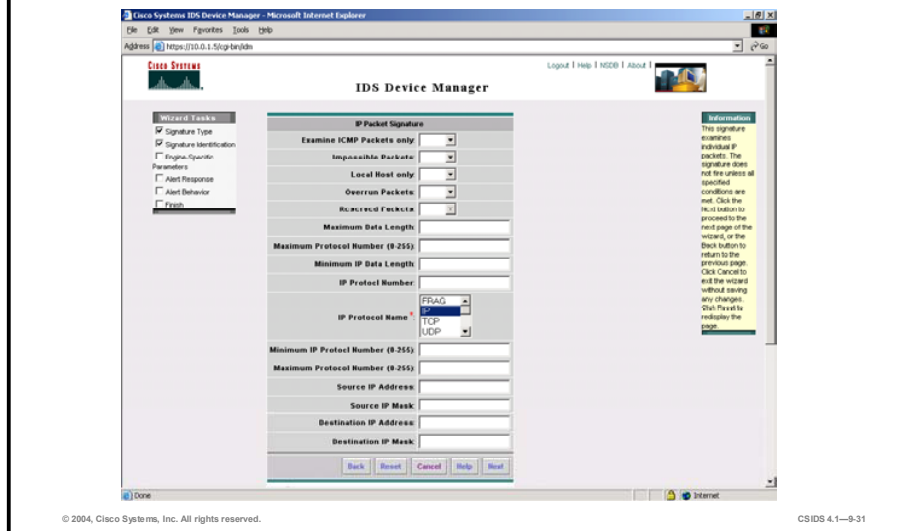


UDP packet signatures examine individual UDP packets. They check for traffic on specified ports and for packet size. The signature does not fire unless all specified conditions are met. The following parameters are configurable for UDP packet signatures:

- Source Port—Enables you to specify a source port to match in the UDP packet.
- Destination Port—Enables you to specify a destination port to match in the UDP packet.
- Minimum UDP Packet Length—Enables you to specify a minimum length for the UDP packet.
- Short UDP Packet Length—Enables you to specify an IP data length that is less than the UDP header length.
- Source IP Address—Enables you to specify the source host or network IP address to match in the UDP packet.
- Source IP Mask—Enables you to specify the netmask for the source host or network.
- Destination IP Address—Enables you to specify the destination host or network IP address to match in the UDP packet.
- Destination IP Mask—Enables you to specify the netmask for the destination host or network.

Configure the Engine-Specific Parameters—IP Packet Signatures

Cisco.com



IP packet signatures examine individual IP packets. The signature does not fire unless all specified conditions are met. The following parameters are configurable for IP packet signatures:

- Examine ICMP Packets only—Configures the signature to examine ICMP packets only.
- Impossible Packets—Configures the signature to fire only if the source and destination addresses are equal.
- Local Host only—Configures the signature to fire if the local host address (127.0.0.1) is seen in the packet.
- Overrun Packets—Configures the signature to fire if a fragment overrun occurs.
- Reserved Packets—Configures the signature to fire if it detects a reserved IP address as specified in RFC 1918.
- Maximum Data Length—Sets a maximum allowable length for the data length of an IP packet.
- Maximum Protocol Number (0–255)—Specifies the maximum allowable protocol number.
- Minimum IP Data Length—Sets a minimum allowable length for the data length of a IP packet.
- IP Protocol Number—Configures the signature to fire if the packet uses a specific protocol, as defined by number.
- IP Protocol Name—Configures the signature to fire if the packet uses a specific protocol, as defined by name. The values are FRAG, IP, TCP, UDP, ICMP, ARP, CROSS, CUSTOM, and ZERO.
- Minimum IP Protocol Number (0–255)—Sets a minimum allowable protocol number.
- Maximum Protocol Number (0–255)—Sets a maximum allowable protocol number.
- Source IP Address—Configures the signature to fire on a source host or network IP address.

- Source IP Mask—Specifies the netmask for the source host or network.
- Destination IP Address—Configures the signature to fire on a destination host or network IP address.
- Destination IP Mask—Specifies the netmask for the destination host or network.

Configure the Engine-Specific Parameters—Stream Signatures

Cisco.com

The screenshot shows the 'Stream Signature' configuration page in the Cisco Systems IDS Device Manager. The page is titled 'IDS Device Manager' and 'Stream Signature'. It contains several input fields: 'Regular Expression', 'Service Ports', 'Direction' (a dropdown menu set to 'To Port'), 'Offset in Packet to Examine(bytes)', and 'Minimum Matching String Length'. There are 'Back', 'Reset', 'Cancel', 'Help', and 'Next' buttons at the bottom of the form. A note at the bottom left indicates that the asterisk (*) denotes a required field. On the right side, there is a help text box explaining that the signature examines data streams for a specified string and that the signature does not fire unless all specified conditions are met.

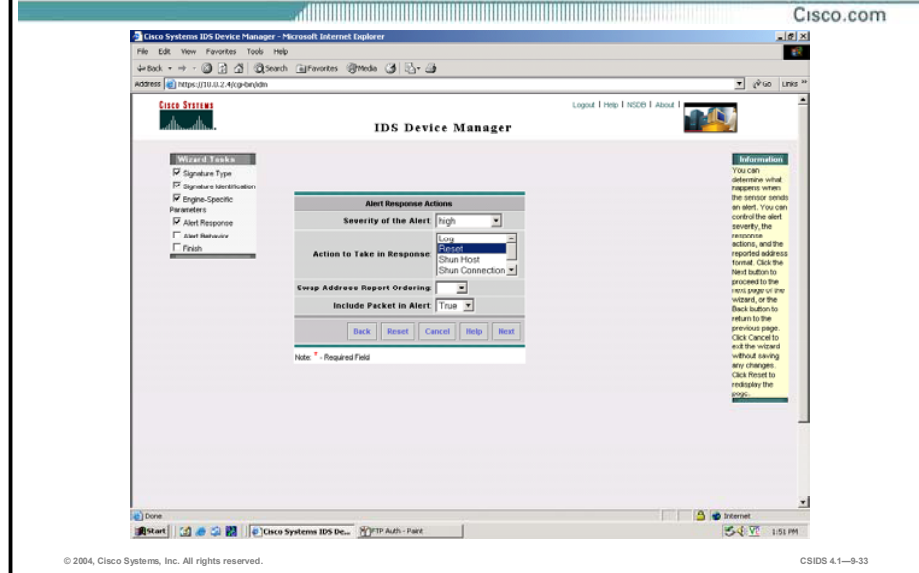
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-32

Stream signatures examine a stream of packets for a specified string. The signature does not fire unless all specified conditions are met. The following parameters are configurable for stream signatures:

- Regular Expression—Specifies a regular expression to be matched.
- Service Ports—Specifies a list or range of destination ports to check.
- Direction—Specifies whether to inspect packets going to or from the service ports. The values are To Port and From Port.
- Offset in Packet to Examine (bytes)—(Optional.) Specifies that the signature should fire only if the regular expression occurs at a specified offset in the stream.
- Minimum Matching String Length—(Optional.) Specifies that the signature should fire only if the matching string is at least this size.

Configure the Alert Response Actions

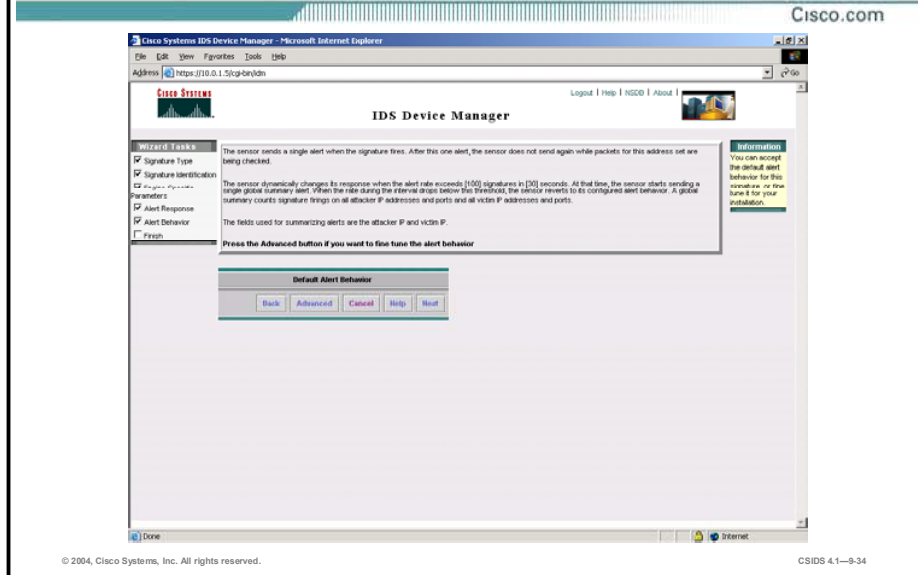


After you configure the engine-specific parameters, the wizard presents the Alert Response Actions page. The following can be configured on this page:

- **Severity of the Alert**—The severity level to be included in the alert. The following levels are available:
 - Informational
 - Low
 - Medium
 - High
- **Action to Take in Response**—An action for the Sensor to take in addition to firing the alert. Some Event Action options do not appear for all signatures. This is determined by the signature engine. The following actions can be selected:
 - Log—The Sensor logs the traffic that caused the alert.
 - Reset—The Sensor sends a TCP reset packet to the attacker to break the connection.
 - Shun Host—The Sensor dynamically configures a network device to block all packets from the attacker to the local network.
 - Shun Connection—The Sensor dynamically configures a network device to block packets from the attacker that are directed specifically at a victim IP address and port.
 - ZERO—The Sensor takes no action. This is the default.
- **Swap Address Report Ordering**—Whether to swap the source and destination addresses that are reported in the alert when this signature fires. The following options are available:
 - Yes—Swaps the address
 - No—Does not swap the address

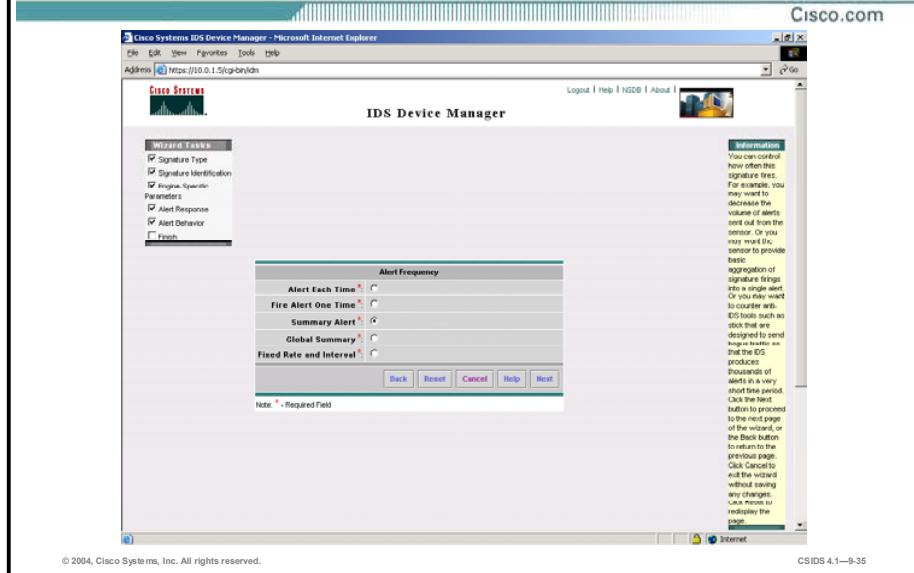
- Include Packet in Alert—Whether to include the packet that caused the signature to fire in the alert. The following options are available:
 - True—Includes the packet
 - False—Does not include the packet

Fine-Tune the Alert Behavior



Next, the wizard gives you the option to accept the default alert behavior or to fine-tune it. Click **Next** to accept the default behavior. Click **Advanced** to fine-tune it.

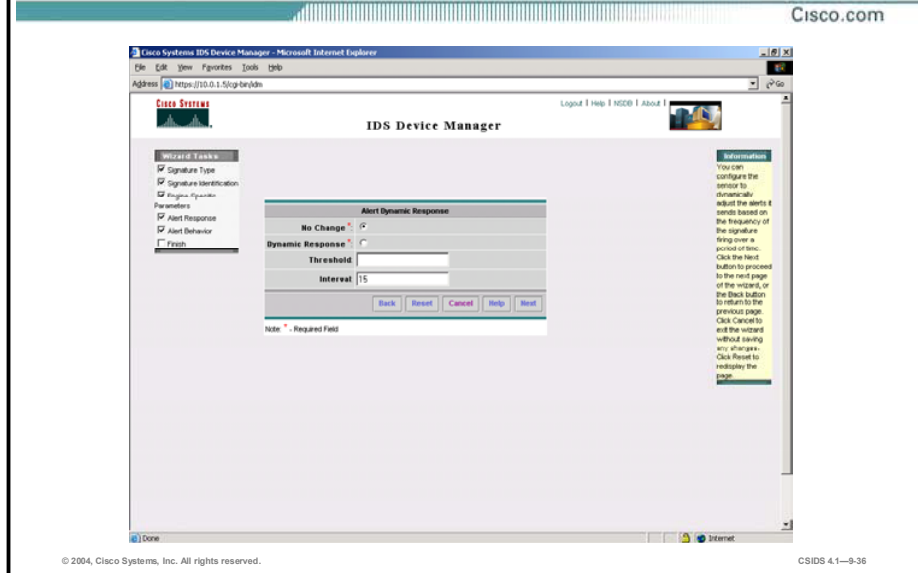
Set the Alert Frequency



The first step in fine-tuning the alert behavior is to configure the alert frequency or the value of AlarmThrottle. You can select one of the following:

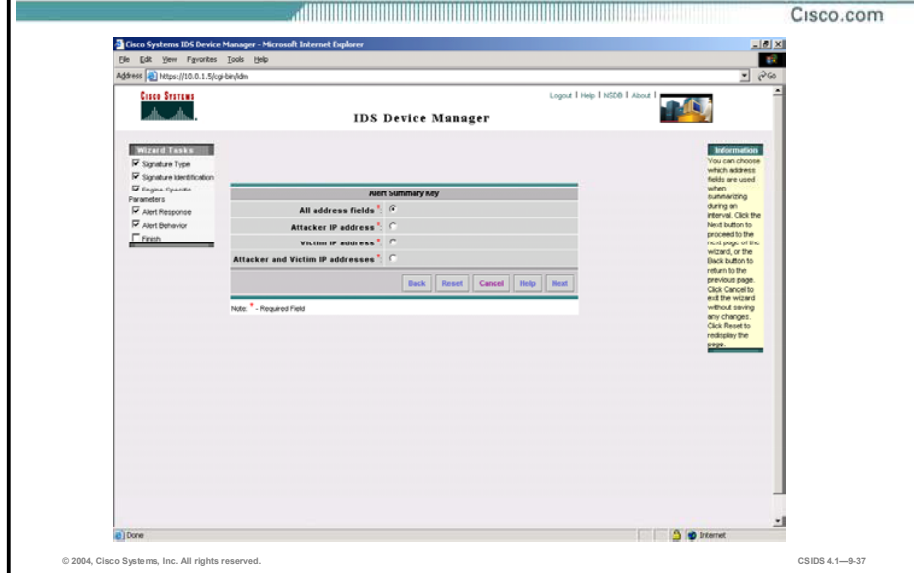
- **Alert Each Time**—Sends an alert each time the signature fires. This sets the AlarmThrottle value to FireAll.
- **Fire Alert One Time**—Sends an alert each time the signature fires but waits a predefined period of time before triggering an alert again for the same signature. This sets the AlarmThrottle value to FireOnce. The predefined period of time is usually specified by the ThrottleInterval parameter.
- **Summary Alert**—Sends the first alert for the address set and then sends a summary of all the alerts that occur on this address set over a given interval of time. This sets the AlarmThrottle value to Summarize.
- **Global Summary**—Sends the first alert and then sends a global summary of all the alerts that occur on all address sets over a specified interval of time. This sets the AlarmThrottle value to GlobalSummarize.
- **Fixed Rate and Interval**—Sends an alert if the signature fires a specified number of times in a specified number of seconds. If you choose this option, you cannot configure the Sensor to dynamically change its behavior based on signature firing frequency.

Configure the Alert Dynamic Response



After you configure the alert frequency, you are prompted to change the dynamic response. If you want to change the dynamic response, click the **Dynamic Response** radio button. Enter the threshold signature firing rate in the Threshold field. The default is 100. Enter the interval in seconds in the Interval field. The default is 30 seconds.

Configure the Alert Summary Key

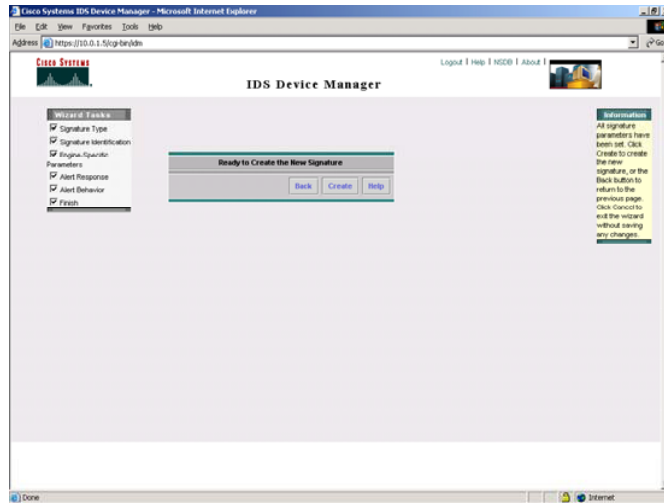


Choose one of the following address sets to configure the summary key:

- All address fields—Summarizes and inspects based on the attacker IP address and attacker port, victim IP address and victim port.
- Attacker IP address—Summarizes and inspects based on the attacker IP address.
- Victim IP address—Summarizes and inspects based on the victim IP address.
- Attacker and Victim IP addresses—Summarizes and inspects based on the attacker IP address and victim IP address.

Create the New Signature

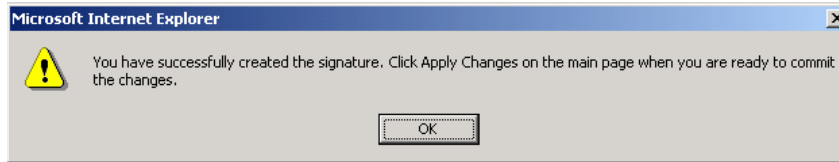
Cisco.com



When you have finished configuring the signature, you are presented with the Ready to Create the New Signature page. Click **Create** to create the custom signature.

Acknowledge Configuration Completion

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

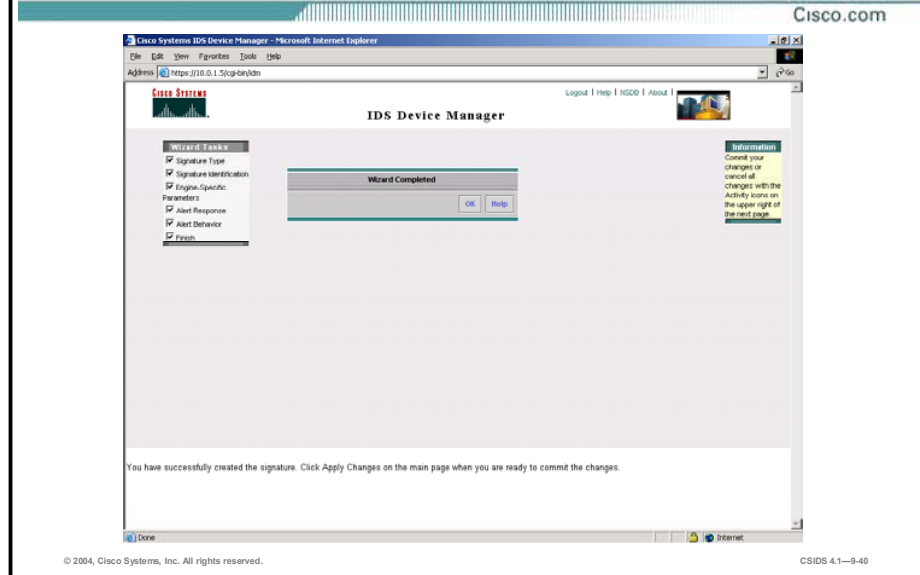
CSIDS 4.1-9-39

When you click **Create**, you receive the following message:

You have successfully created the signature. Click Apply Changes on the main page when you are ready to commit the changes.

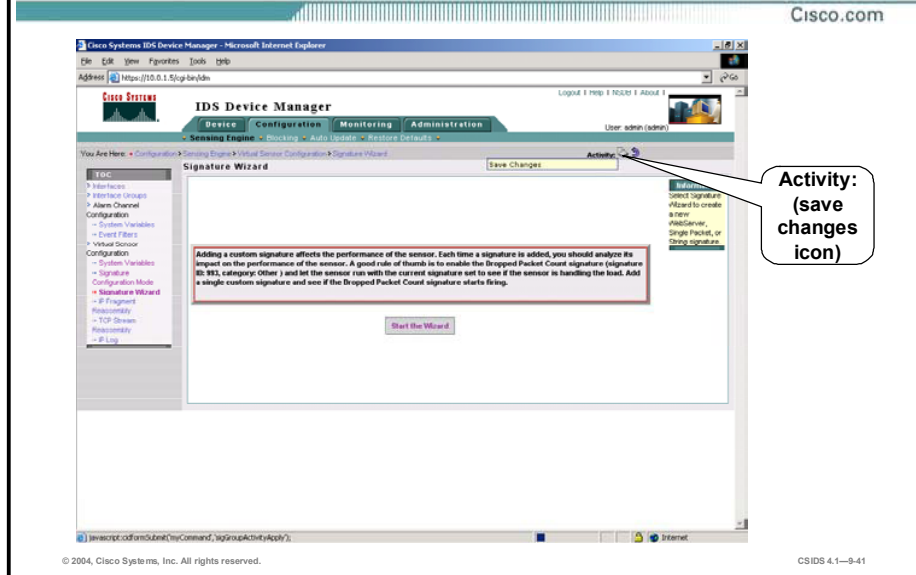
Click **OK** in the message dialog box to continue.

Wizard Complete



Clicking **OK** in the message dialog box takes you to the Wizard Completed page. Click **OK** to return to the main Signature Wizard page.

Commit Changes



Click the save changes icon in the Activity bar to save your custom signature.

Custom Signature Scenarios

This topic uses scenarios to explain custom signatures.

IP Address and Packet Capture Scenario

Cisco.com

A network security administrator wants to create a custom signature that meets the following requirements:

- **The signature should trigger on and capture all SYN packets from the 10.0.20.0/24 network, but not SYN-ACK packets.**
- **The number of alarms sent to the eventStore should be limited.**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—9-43

A company's network security administrators notice unusual traffic on the company's network coming from the 10.0.20.0/24 network. They decide to create custom signatures to protect against potential attacks from this network. Based on the type of traffic observed, the administrators decide that one of these custom signatures should detect and capture SYN packets from the 10.0.20.0/24 network, but not SYN-ACK packets. The administrators also decide to limit the number of alarms sent to the eventStore.

IP Address and Packet Capture Scenario (Cont.)

Cisco.com

The administrator determines that a custom TCP packet signature can meet this need because of the following:

- **The SrcIpAddr and SrcIpMask parameters can be used to specify the IP address of interest.**
- **The TcpFlags and Mask parameters can be used to specify the flags of interest.**
- **The AlarmThrottle, ChokeThreshold, and ThrottleInterval parameters can be used to limit the number of alarms.**
- **The CapturePacket parameter can be set to true to instruct the Sensor to capture any packet that triggers an alarm.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-44

The administrators decide to create an atomic signature so that the signature will fire based on the contents of a single packet. They further determine that this atomic signature should be of the TCP packet signature type because the TCP packet signature parameters can be used as follows:

- **SrcIpAddr and SrcIpMask**—Can be used to specify the IP address of interest, which is 10.0.20.0/24 in this scenario.
- **TcpFlags and Mask**—Can be used to specify the TCP flag of interest, which is SYN in this scenario.
- **AlarmThrottle, ChokeThreshold, and ThrottleInterval**—Can be used to limit the number of alarms.
- **CapturePacket**—Can be used to instruct the Sensor to capture any packet that triggers an alarm.

Select the Signature Type

Cisco.com

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—9-45

To begin creating this custom signature, first start the Signature Wizard. Then, when presented with the signature type selections, choose **TCP Packet Signature**.

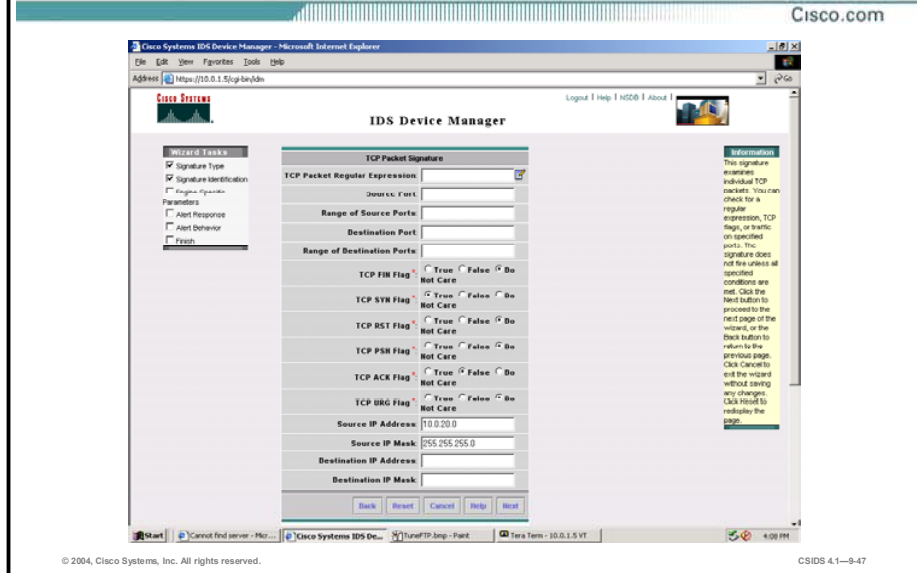
Configure the Signature Identification Parameters



Complete the following fields on the Signature Identification page and then click **Next**:

- **Signature ID**—Assign a number within the range allowed for custom signatures. For this signature use the ID number 20001.
- **Signature Name**—Assign a signature name that helps you easily recognize the signature. For this signature use the name IPAddr.

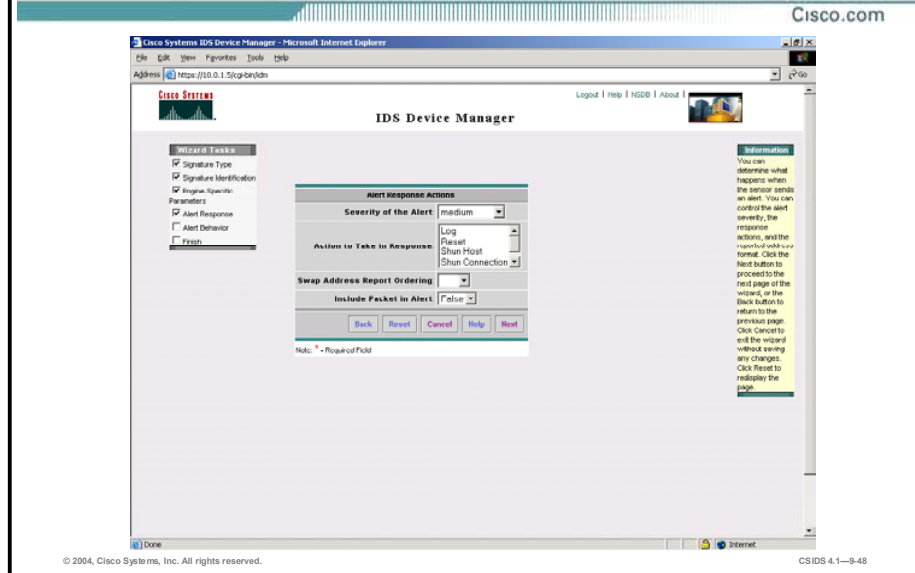
Configure the Engine-Specific Parameters



Configure the following signature parameters and then click **Next**:

- **TCP FIN Flag**—Accept the default setting, **Do Not Care**.
- **TCP SYN Flag**—Select the **True** radio button. This is the flag that must be present in the packet if the signature is to fire.
- **TCP RST Flag**—Accept the default setting, **Do Not Care**.
- **TCP PSH Flag**—Accept the default setting, **Do Not Care**.
- **TCP ACK Flag**—Select the **False** radio button. If this flag is present in the packet, the signature will not fire.
- **TCP URG Flag**—Accept the default setting, **Do Not Care**.
- **Source IP Address**—Enter **10.0.20.0**, the source network address of the anticipated attack.
- **Source IP Mask**—Enter **255.255.255.0**, the mask for the source IP address.

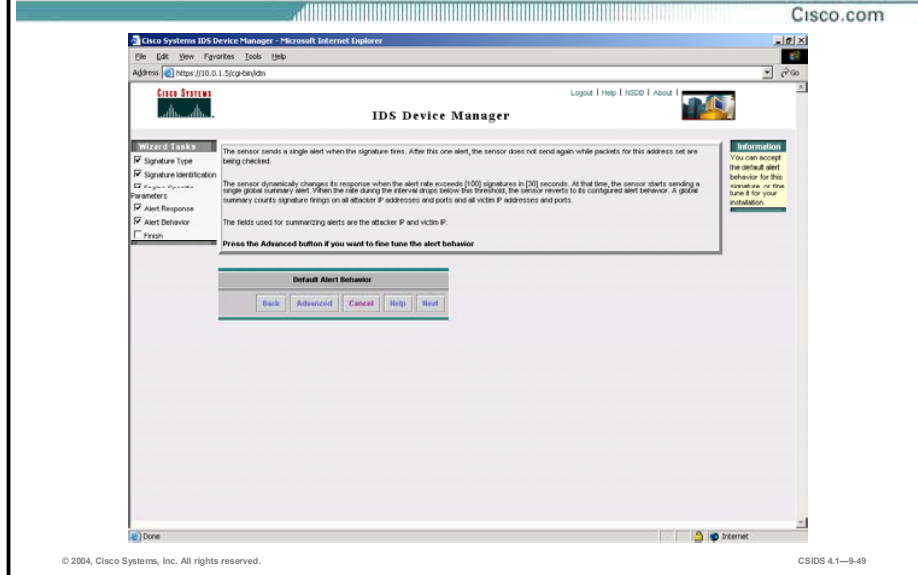
Configure the Alert Response Actions



Configure the following on the Alert Response Actions page:

- Severity of the Alert—Select **high** from the drop-down menu.
- Include Packet in Alert—Select **True** from the drop-down menu.

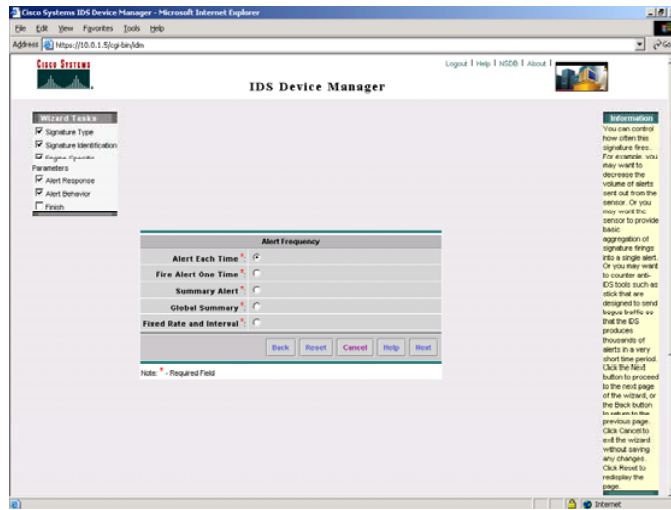
Fine-Tune the Alert Behavior



Click **Advanced** in the Default Alert Behavior box. This action enables you to access the Alert Frequency and Alert Dynamic Response pages necessary for configuring the AlarmThrottle, ChokeThreshold, and ThrottleInterval values.

Set the Alert Frequency

Cisco.com

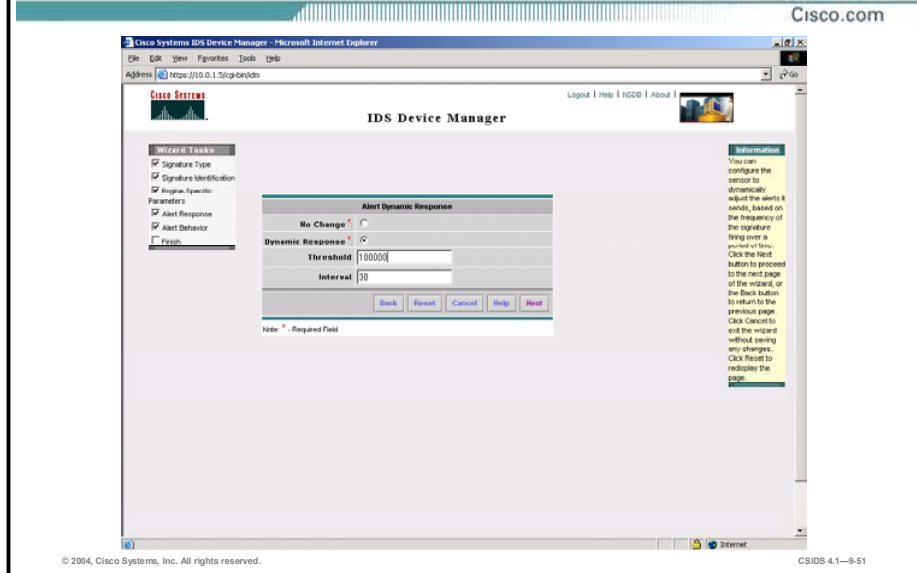


© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-50

From the Alert Frequency page, select the **Alert Each Time** radio button and click **Next**. This is the IDM equivalent of setting AlarmThrottle to FireAll.

Configure the Alert Dynamic Response



Configure the following on the Alert Dynamic Response page:

- Select the **Dynamic Response** radio button to enable alarm summarization.
- Enter **100000** in the Threshold field. This is the IDM equivalent of setting ChokeThreshold to 100000.
- Accept the default value of **30** in the Interval field. This is the IDM equivalent of setting ThrottleInterval to 30 seconds.

After configuring the alert dynamic response, click **Next** to continue. Accept the default settings as you proceed through the remainder of the Signature Wizard pages.

FTP Login Scenario

Cisco.com

A network security administrator wants to create a custom signature to detect login failures to an FTP server. The administrator knows the following about FTP and TCP:

- **The FTP server sends the “530 user access denied” error when an FTP login failure occurs.**
- **FTP uses TCP port 21.**
- **The FTP server uses the TCP PSH operation to force prompts and user input.**
- **The TCP ACK flag indicates an acknowledgment.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-52

A company’s FTP server stores software that is being beta tested by customers. The company wants to detect unauthorized login attempts. Based on the threat the attack poses, the signature should meet the following requirements:

- Trigger a high-severity alarm after a failed login attempt.
- Send an alarm event every time the attack is detected.
- Terminate the session.

The network security administrators’ knowledge of FTP, which follows, enables them to create a suitable custom signature:

- The FTP server sends the “530 user access denied” error when an FTP login failure occurs.
- FTP uses TCP port 21 as the control port for establishing connections.
- The FTP server application uses the TCP PUSH (PSH) operation to force prompts and user input.
- The TCP ACK flag indicates an acknowledgement.

FTP Login Scenario (Cont.)

Cisco.com

The network security administrator, using knowledge of TCP and FTP, determines that the signature can trigger based on the contents of a single packet.

- **The SinglePacketRegex parameter can be set to have the signature to look for the 530 error message in a packet.**
- **The TCPFlags and Mask parameters can be set to have the signature to look for packets with the PSH and ACK flags set.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-53

The administrators decide to create an atomic signature so that the signature will fire based on the contents of a single packet. They further determine that this atomic signature should be of the TCP packet signature type because the TCP packet signature parameters can be used as follows:

- **SinglePacketRegex**—Can be used to specify the 530 error message. This parameter provides a simple regular expressions (regex) match capability so you can combine ports, flags, and regex match in a single signature.
- **TcpFlags and Mask**—Can be used to specify the TCP flags of interest, which are PSH and ACK in this scenario.
- **AlarmSeverity**—Can be used to set the alarm severity level. For this scenario, the severity level is set to high.
- **AlarmThrottle**—Can be used to instruct the Sensor to send an alarm event every time the attack is detected.
- **EventAction**—Can be set to Reset to instruct the Sensor to terminate the session when the alarm is fired.

Note By setting the MinHits parameter, you could tune the signature to fire only after a certain number of failed login attempts.

FTP Login Scenario—Select the Signature Type

Cisco.com

The screenshot shows the Cisco Systems IDS Device Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL <https://170.0.1.1/SignWrdr.htm>. The page title is "IDS Device Manager". On the left, there is a "WIZARD TASKS" sidebar with the following options: Signature Type, Signature Identification, Signature Parameters, Alert Response, Alert Behavior, and Finish. The main content area is titled "Web Server Signatures" and contains three sections: "Web Server Signatures" with a "Web Server Signature:" label and a radio button; "Packet Signatures" with "TCP Packet Signature:" (checked), "UDP Packet Signature:" (unchecked), and "IP Packet Signature:" (unchecked); and "Stream Signatures" with "TCP Stream Signature:" (unchecked), "UDP Stream Signature:" (unchecked), and "ICMP Stream Signature:" (unchecked). At the bottom of the main area are "Reset", "Cancel", "Help", and "Next" buttons. A "Note" section at the bottom indicates "Note * - Required Field". On the right side, there is an "Information" box with instructions: "On this page you will decide what type of signature to create. Select exactly one signature type. Click the Next button to proceed to the next page of the wizard. Click Cancel to exit the wizard without saving any changes. Click Finish to redisplay the page."

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-54

To begin creating this custom signature, first start the Signature Wizard. Then, when presented with the signature type selections, choose **TCP Packet Signature**.

FTP Login Scenario—Configure the Signature Identification Parameters

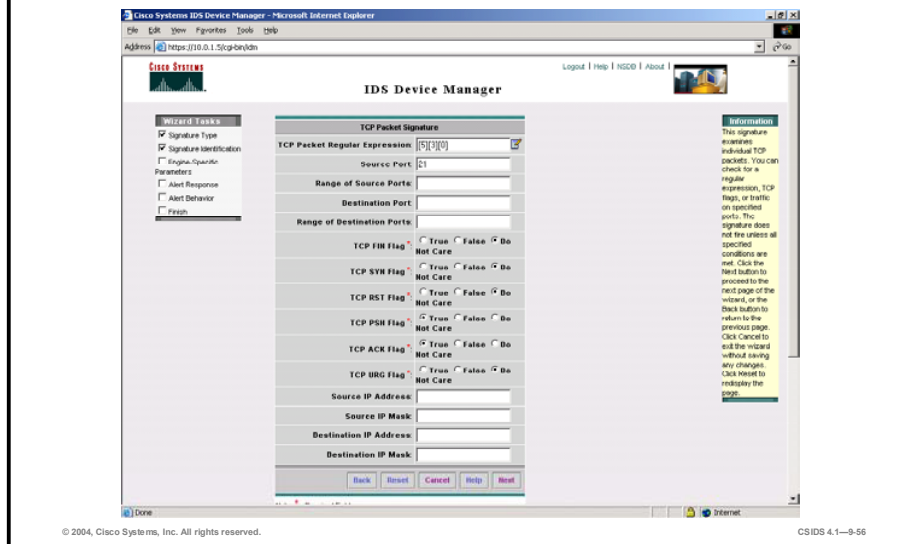


Complete the following fields on the Signature Identification page and then click **Next**:

- **Signature ID**—Assign a number within the range allowed for custom signatures. For this signature, use the ID number 20002.
- **Signature Name**—Assign a signature name that helps you easily recognize the signature. For this signature, use the name FTP Auth Failure.

FTP Login Scenario—Configure the Engine-Specific Parameters

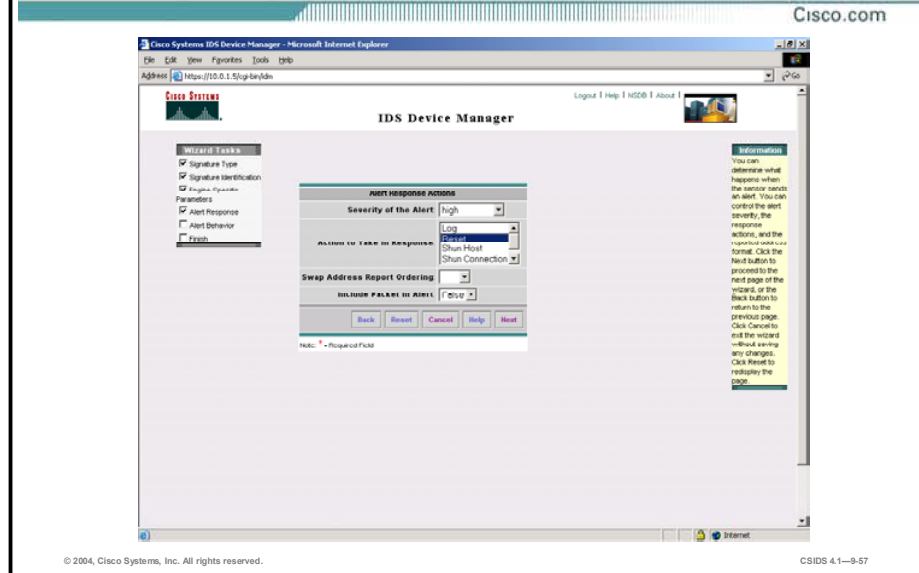
Cisco.com



Configure the following signature parameters and then click **Next**:

- **TCP Packet Regular Expression**—Enter **[5][3][0]** to set the signature to fire if 530 appears in the packet.
- **Source Port**—Enter **21** to specify that the packet that triggers the signature comes from TCP port 21.
- **TCP FIN Flag**—Accept the default setting, **Do Not Care**.
- **TCP SYN Flag**—Accept the default setting, **Do Not Care**.
- **TCP RST Flag**—Accept the default setting, **Do Not Care**.
- **TCP PSH Flag**—Select the **True** radio button. This flag must be set for the signature to fire.
- **TCP ACK Flag**—Select the **True** radio button. This flag must be set for the signature to fire.
- **TCP URG Flag**—Accept the default setting, **Do Not Care**.

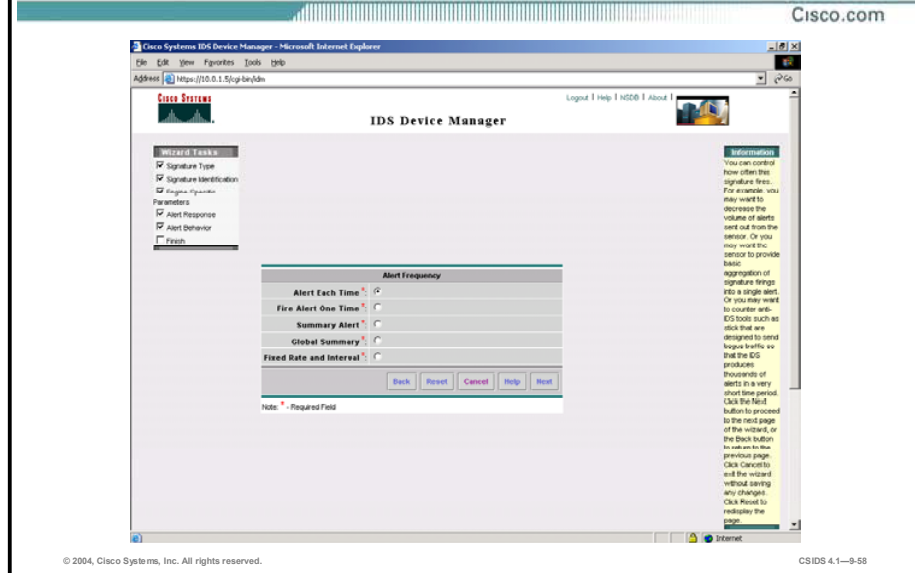
FTP Login Scenario—Configure the Alert Response Actions



Configure the following on the Alert Response Actions page:

- Severity of the Alert—Select **high** from the drop-down menu.
- Action to Take in Response—Select **Reset** from the list of actions.

FTP Login Scenario—Set the Alert Frequency



Select **Advanced** in the Default Alert Behavior box to open the Alert Frequency page. From the Alert Frequency page, select **Alert Each Time** and click **Next** to set AlarmThrottle to FireAll. Proceed through the Signature Wizard, accepting the defaults for the remaining settings.

String Pattern Scenario

Cisco.com

A network security administrator wants to create a signature that detects the word “confidential” in common electronic communication methods. The administrator knows the port numbers of the traffic to be inspected:

- **FTP—20 and 21**
- **Telnet—23**
- **SMTP—25**
- **HTTP—80**
- **POP3—110**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-59

A company’s network security administrators want to create a signature that detects the word “confidential” in common electronic methods. Other than the string for which they want the signature to search, the administrators know only the following information:

- The traffic that needs to be inspected
- The ports used by that traffic

String Pattern Scenario (Cont.)

Cisco.com

The administrator decides to create a TCP stream signature because all the protocols to be examined are TCP-based and because of the following:

- **The Regular Expression parameter can be used to specify the string pattern 'confidential'.**
- **The Service Ports parameter can be used to specify the range of ports.**
- **The Direction parameter can be used to instruct the Sensor to inspect traffic destined for the service ports specified.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-60

The administrators decide to create a TCP stream signature because all traffic to be inspected is TCP based and because stream signatures perform simple stateful expression-matching based on protocol. To create this signature, configure the parameters as follows:

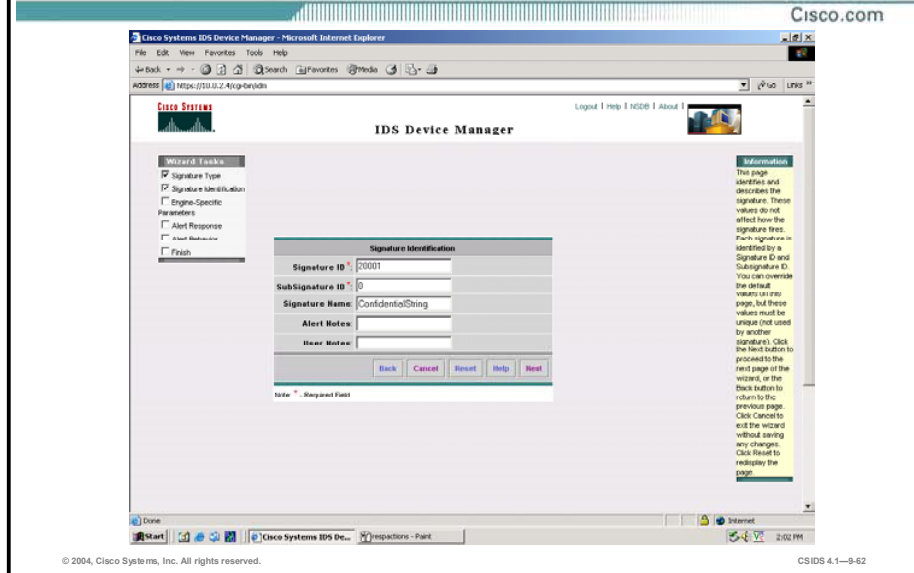
- **Regular Expression**—Can be used to configure the signature to trigger when it detects the string pattern 'confidential'.
- **Service Ports**—Can be used to specify the range of ports.
- **Direction**—Can be used to configure the signature to trigger when the traffic inspected is destined for the range of ports specified in Service Ports.

String Pattern Scenario—Select the Signature Type



To configure this signature, start the Signature Wizard and select **TCP Stream Signature** as the signature type.

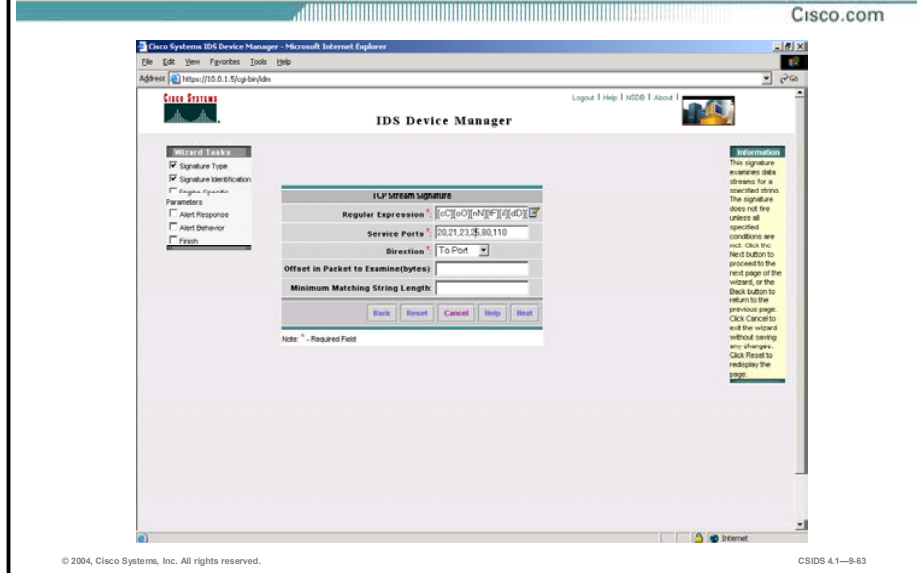
String Pattern Scenario—Configure the Signature Identification Parameters



Complete the following fields on the Signature Identification page and then click **Next**:

- **Signature ID**—Assign a number within the range allowed for custom signatures. For this scenario, the ID number 20001 is used.
- **Signature Name**—Assign a signature name that helps you easily recognize the signature. For this scenario, the name FTP Auth Failure is used.

String Pattern Scenario—Configure the Engine-Specific Parameters



Configure the following signature parameters and then click **Next**:

- Regular Expression—Enter `[cC][oO][nN][fF][iI][dD][eE][nN][fT][iI][aA][IL]` to configure the signature to fire if it detects the string 'confidential'.
- Service Ports—Enter the following port numbers to configure the signature to inspect the traffic that uses those ports: **20, 21, 23, 25, 80, 110**.
- Direction—Select **ToPort** from the drop-down menu to configure the signature to trigger when the traffic inspected is destined for the range of ports specified in Service Ports.

Proceed through the Signature Wizard, accepting the defaults for the remaining settings or modifying them as needed.

File Access Scenario

Cisco.com

- **A network security administrator wants to create a signature that fires when the file msbadfile.asp is accessed via an HTTP request.**
- **The administrator decides to create a custom web server signature because the UriRegex parameter can be used to examine the URI section of an HTTP request to see whether it matches the regular expression specified, which is msbadfile.asp in this scenario.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-64

A company's network security administrators want to create a signature that fires when the file msbadfile.asp is accessed via an HTTP request. The administrators decide to create a custom web server signature for the following reasons:

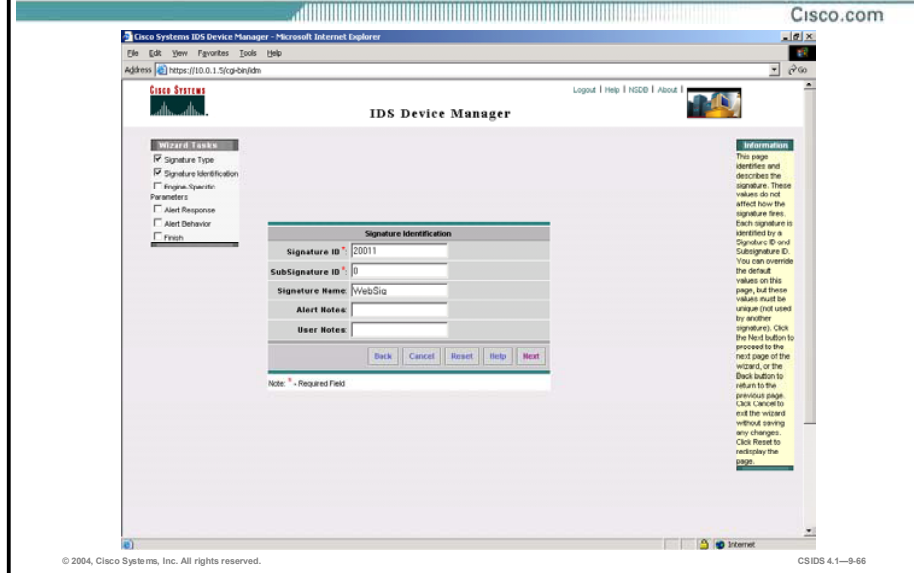
- Web server signatures can be used to detect regular expressions in web URL requests. These signatures search only traffic directed to web services or HTTP requests.
- The UriRegex parameter can be used to configure the signature to fire when it detects msbadfile.asp in the URI section of the HTTP request.

File Access Scenario—Select the Signature Type



To begin creating this custom signature, first start the Signature Wizard. Then, when presented with the signature type selections, choose **Web Server Signature**.

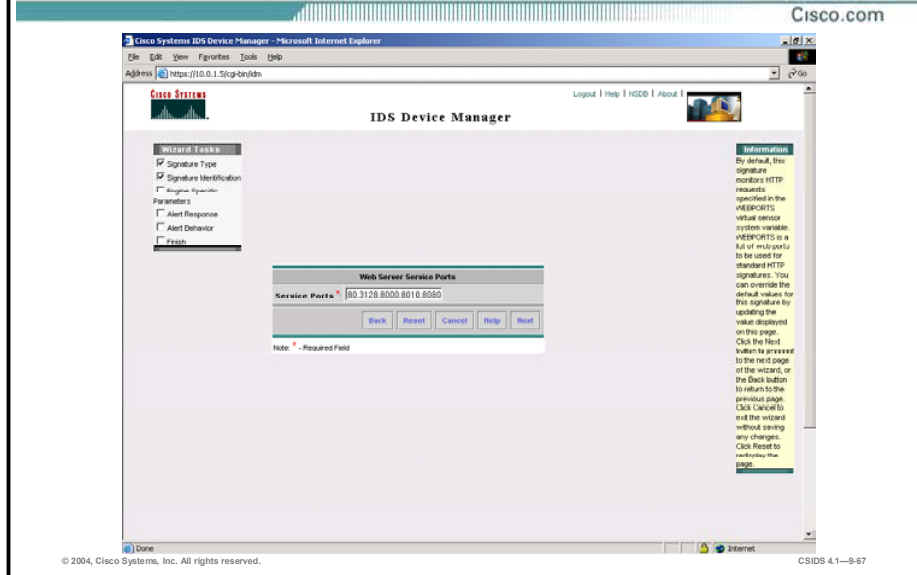
File Access Scenario—Configure the Signature Identification Parameters



Complete the following fields on the Signature Identification page and then click **Next**:

- **Signature ID**—Assign a number within the range allowed for custom signatures. For this signature, use the ID number 20011.
- **Signature Name**—Assign a signature name that helps you easily recognize the signature. For this signature, use the name WebSig.

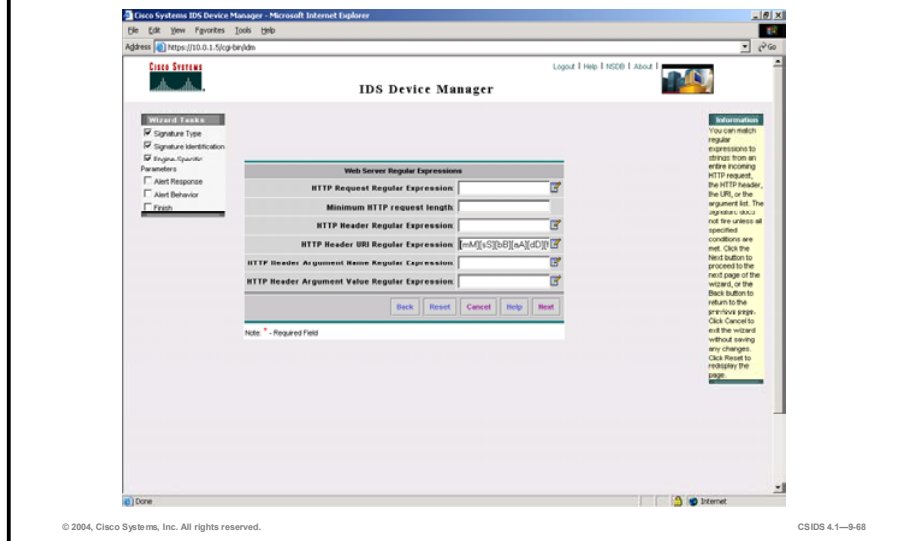
File Access Scenario—Configure the Engine-Specific Parameters



When creating a web server signature, the Signature Wizard prompts you to configure the web server service ports. By default, web server signatures monitor HTTP requests specified in the WEBPORTS virtual sensor system variable. WEBPORTS is a list of web ports to be used for standard HTTP signatures.

File Access Scenario—Configure the Engine-Specific Parameters (Cont.)

Cisco.com



After you accept or modify the web server service ports, the Signature Wizard prompts you to configure Web Server Regular Expressions. You can match regular expressions to strings from an entire incoming HTTP request, the HTTP header, the URI, or the argument list. To create the custom signature that fires when the file `msbadfile.asp` is accessed via an HTTP request, enter `[mM][sS][bB][aA][dD][fF][iI][lL][eE][.][aA][sS][pP]` in the HTTP Header URI Regular Expression field.

Port-Specific Scenario

Cisco.com

- **A network security administrator wants to create a custom signature to detect packets destined for port 33054 that have only the TCP flags FIN and URG set.**
- **The administrator determines that a custom TCP packet signature can meet this need because of the following:**
 - **The DstPort parameter can be used to specify the destination port, which is port 33054 in this scenario.**
 - **The Mask and TcpFlags parameters can be used to specify the TCP flags of interest.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-69

A company's network security administrators want to create a custom signature to detect packets that have only the TCP flags FIN and URG set and that are destined for port 33054. They determine that a custom TCP packet signature can meet this need because of the following:

- The Destination Port parameter can be used to specify the destination port, which is port 33054 in this scenario.
- The TcpFlags and Mask parameters can be used as follows to specify the TCP flags of interest:
 - TCP FIN Flag—Select the **True** radio button. This flag must be set for the signature to fire.
 - TCP SYN Flag—Select the **False** radio button. The signature will not fire if this flag is set.
 - TCP RST Flag—Select the **False** radio button. The signature will not fire if this flag is set.
 - TCP PSH Flag—Select the **False** radio button. The signature will not fire if this flag is set.
 - TCP ACK Flag—Select the **False** radio button. The signature will not fire if this flag is set.
 - TCP URG Flag—Select the **True** radio button. This flag must be set for the signature to fire.

Summary

This topic summarizes this lesson.

Summary

Cisco.com

- **All signatures have the following basic configurable parameters:**
 - **Enable**—Enables or disables the signature
 - **AlarmSeverity**—Assigns the severity level: information, low, medium, or high
 - **EventAction**—Assigns the action to take if the signature is triggered: log, reset, block host, or block connection
- **Cisco IDS signatures can be tuned to adjust to company network security policy or network traffic pattern.**
- **Custom signatures can be created to meet a unique security requirement.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-71

Summary (Cont.)

Cisco.com

- **Custom signatures can be created via the IDM Signature Wizard.**
- **Consider the following before creating a signature with the Signature Wizard:**
 - **The network protocol**
 - **The target address**
 - **The target port**
 - **The type of attack**
 - **Whether payload inspection is required**
 - **Whether the signature can be triggered on the contents of a single packet**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—9-72

Sensor Tuning

Overview

This lesson discusses how Sensors can be tuned in order to provide the most beneficial and efficient intrusion protection solution. This lesson includes the following topics:

- Objectives
- Intrusion detection evasive techniques
- Tuning the Sensor
- Logging
- Reassembly options
- Alarm channel system variables
- Alarm channel event filtering
- Summary
- Lab exercise

Objectives

This topic lists the objectives of this lesson.

Objectives

Cisco.com

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

- **Explain the evasive techniques used by hackers and how Cisco IDS defeats those techniques.**
- **Define Sensor tuning.**
- **Describe Sensor tuning methods.**
- **Explain automatic and manual IP logging.**
- **Explain IP fragment and TCP stream reassembly options.**
- **Define and configure system variables.**
- **Define and configure signature filters.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-3

Intrusion Detection Evasive Techniques

This topic describes the evasive techniques employed by hackers.

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**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—10-5

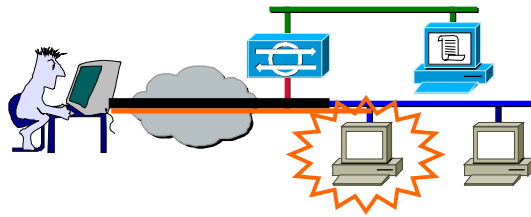
The hacker community is aware of the various intrusion detection system (IDS) technologies used and has identified ways to evade intrusion detection. Attempting to elude intrusion detection is accomplished using intrusion detection evasive techniques. The following are common intrusion detection evasive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

- Flooding
- Fragmentation
- Encryption
- Obfuscation

For more information, refer to “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection,” Thomas H. Ptacek and Timothy N. Newsham, Secure Networks, Inc., January 1998.

Flooding

Cisco.com



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

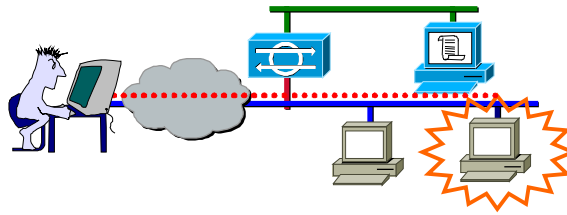
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-6

Intrusion detection systems rely on their ability to capture packets off the wire and analyze them as quickly as possible. This requires the IDS to have 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 and thus 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-7

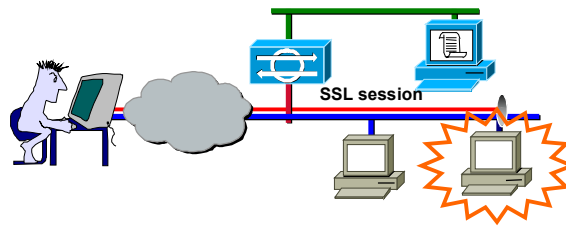
Networks are connected via various media types, such as Ethernet, FDDI, Token Ring, and ATM. Each of these technologies specifies the allowed maximum transmission unit (MTU). The MTU value is different for each technology. Consequently, fragmentation of these transmission units (packets, cells) is allowed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

Fragmentation adds a level of complexity that IDSs 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-8

IDSs monitor the network and capture the packets as they traverse the network. Network-based IDSs (NIDSs) rely 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 that 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 Sockets Layer (SSL) connection to a secure web site
- Secure Shell (SSH) connection to an SSH server
- Site-to-site virtual private network (VPN) tunnel
- Client-to-LAN VPN tunnel

Obfuscation

Cisco.com

Disguising an attack using special characters to conceal it from an IDS is commonly referred to as obfuscation. The following are forms of obfuscation:

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1–10-9

Early intrusion detection was easily evaded by using special characters to disguise 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 space, tab, backspace, and delete characters.
- **Hexadecimal representation**—Each character can be represented in hexadecimal format. For example, a space is represented by the hexadecimal 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>.


Tuning the Sensor

This topic explains how to tune the Sensor to avoid evasive techniques and provide network-specific intrusion protection.

Sensor Tuning

Cisco.com

Tuning is the process of configuring your IDS system so that it provides the desired level of information to efficiently monitor and protect your network.



© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—10-11

Tuning is a general term that is applied to the process of setting up an IDS in such a way that it provides you the correct level of information necessary for protecting your specific network. If your IDS is to serve you efficiently, you must determine what level of events you want from the Sensors as well as what you are going to do with that event information. An IDS has the ability to provide information on network events at as low a level as reporting every HTTP connection attempt or every ping sweep or port sweep, but if you have no intention of using this data, there is little reason to collect it.

One of the main purposes of the tuning process is to modify the IDS system behavior so that the alarms that are generated have a much higher fidelity (or likelihood of being correct) and a lower chance of reflecting anything other than a true event. Another purpose of tuning is to quickly and efficiently identify attacks in progress in order to respond to them.

Sensor Tuning (Cont.)

Cisco.com

- **To tune your Sensors successfully, you must have knowledge of the network and the individual devices being protected.**
- **This knowledge enables you to recognize normal versus abnormal network activity.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-12

In order for tuning to be successful, the IDS administrator must be knowledgeable about the network and the individual devices that are being protected by the IDS system. This knowledge enables you to recognize normal versus abnormal network activity.

Tuning Considerations

Cisco.com

Important information to gather before you begin tuning includes:

- **The network topology**
- **The network address space under observation**
- **Which of the inside addresses are statically assigned to servers and which are DHCP addresses**
- **The operating system running on each server**
- **Applications running on the servers**
- **The security policy**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-13

Information that you should gather before tuning your IDS includes, but is not limited to, the following:

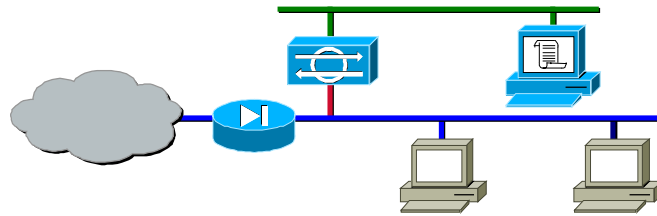
- The network topology
- The network address space under observation
- Which of the inside addresses are statically assigned to servers and which are Dynamic Host Configuration Protocol (DHCP) addresses
- The operating system running on each server
- Applications running on the servers
- The security policy

This network knowledge is important if you have to sort through events that may or may not have relevance and make decisions about how to react to each one. The decision is affected by such information as the source and destination address of each event, the operating system of a targeted server, the applications that are running on the server, and the normal behavior of the server.

For example, you might see ping sweep events coming from IP address 10.0.1.99. These might normally be considered suspicious events. However, if you know that 10.0.1.99 is a server running Hewlett-Packard OpenView network management software, which does ping sweeps as part of its normal network discovery functionality, you can tune out the event using the Sensor alarm channel filtering function so that the Sensor never again triggers that event when it comes from the 10.0.1.99 address.

Sensor Location

Cisco.com



The location of the Sensor is important to tuning for the following reasons:

- The nature of the traffic that a Sensor monitors varies.
- The security policy with which the Sensor interacts varies.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-14

The location of the Sensor typically has an important influence on how the Sensor is tuned. A typical deployment location consideration is whether the Sensor is watching traffic outside or inside the firewall. Another consideration is whether the traffic being monitored is mostly Internet traffic coming in or user traffic going out to the Internet versus predominantly internal traffic.

One reason location is important is that traffic inspected by a Sensor outside a firewall tends to be unregulated. Sensors monitoring traffic outside a firewall see scans, sweeps, and every Internet worm and attack that exists along with potentially large numbers of spoofed packets from around the globe. This makes it much more difficult to distinguish true alarms from noise or false alarms. A possible strategy for a Sensor outside a firewall is to use the event stream from the Sensor to identify trends.

When the Sensor is outside the firewall, consider tuning as follows:

- Avoid assigning a high severity level to any individual event.
- Turn off all response actions.
- Use the Sensor primarily for looking for trends on the Internet such as activity explosions, which can indicate attacks like Code Red or Nimda.

Another reason location plays an important role is that the security policy the Sensor must enforce may vary at different deployment points. A Sensor that monitors traffic outside a perimeter firewall can function independently of security policy because there is really no policy to enforce; however, a firewall on a tightly controlled Demilitarized Zone (DMZ) segment could have a much tighter policy. If Telnet and FTP are not allowed on the DMZ, it would be reasonable to set high severity levels for Telnet and FTP signatures on the DMZ Sensor so that those protocols generate a high-severity event any time they are seen.

Phases of Tuning

Cisco.com

The phases of tuning correspond to the length of time the IDS has been running at the current location. The following are the phases:

- **Deployment phase**
- **Tuning phase**
- **Maintenance phase**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-15

The phases of tuning correspond to the length of time the IDS has been running at the current location. The following are the phases:

- **Deployment phase**—This phase is completed during initial setup and deployment. During this phase, the Sensor is normally running the default configuration. The default configuration is generally close to being tuned for the average deployment. Depending on your security policy and the location of your Sensor, you may choose to turn on specific signatures for activity you want to track. This is typically done using one of the connection signatures to track activity on a specific TCP or UDP port or a type of Internet Control Message Protocol (ICMP) packet.
- **Tuning phase**—Although it could last up to several weeks, this phase usually takes place during the two weeks after the end of the deployment phase. Most of the activity and work occurs during this phase. Before starting the tuning phase, the IDS should be up and running for a continuous period so that it sees a normal sampling of the network activity. During this time, it is possible for the Sensor to fire a considerable number of events. Do not delete these events because they can be used extensively in the tuning process. Observe which alarm types are being triggered most frequently and note their source and destination addresses. Using the Cisco IDS Network Security Database (NSDB) as a reference, you can then proceed to examine each of the top alarm sources to determine whether an event worth investigating is occurring.
- **Maintenance phase**—This phase is completed periodically as tuning becomes necessary, such as each time a signature update is applied to the Sensor. Maintenance tuning could include turning alarms off, modifying their default severity levels or parameters, or creating filters either on the Sensor or on your monitoring application. This is because signature updates not only add new signatures but also modify the way existing ones fire.

Methods of Tuning

Cisco.com

Some tuning methods involve configuring the Sensor, while others involve configuring your monitoring application. The following points show tuning methods and where they are performed:

- **On the Sensor**
 - Enabling and disabling signatures
 - Changing alarm severity up or down
 - Changing the parameters of signatures
 - Creating alarm filters
- **On the monitoring application**
 - Specifying by severity level the alarms you want to view

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-16

The following are methods of tuning:

- Enabling and disabling signatures—This method is best used on a case-by-case basis. For example, you might want to enable a signature that is disabled by default because it is of interest in your particular situation. Exercise caution when disabling signatures to avoid compromising your network. Disabling signatures is usually done only when the signature is of no interest or is providing no foreseeable useful data.
- Changing alarm severity up or down—The use of this tuning mechanism is generally related either to the location of a Sensor or the policy that exists at the Sensor's location. For example, you might need to lower the severity level of a web signature on a Sensor monitoring traffic from outside a firewall because of the volume of web traffic at that location. On the other hand, you might want to raise the severity level of a NetBIOS signature for a Sensor monitoring traffic on your DMZ if your security policy states that NetBIOS traffic should not occur on the DMZ.
- Changing the parameters of the signature—This tuning mechanism is most commonly used to control the firing of signatures that have thresholds. For example, a small company may set a Sensor's ICMP Network Sweep w/Echo signature to fire if five hosts receive echo request packets within 15 seconds. Because of a higher level of benign ICMP activity, a larger company might need to set the same signature to ten hosts in 15 seconds to keep the signature from firing on benign activity.
- Creating alarm channel event filters—This is the most common method of tuning and is the best method to control benign triggers. It also helps decrease false positives. For example, by specifying the source of traffic that is triggering false positives, you can prevent the Sensor from firing the same alarm again. For another example, your Sensor has already alerted you that your Apache server is being attacked by Code Red and you no longer want to know about any Internet source that is sending Code Red attacks. You can tune out all events generated by Internet sources that are sending these attacks.
- Specifying by severity level the alarms you want to see—This tuning is part of the monitoring application initial configuration. Both Cisco IDS Event Viewer (IEV) and

Monitoring Center for Security can be configured to request alarms of a certain severity level and higher from the Sensor.

Global Sensor Tuning

Cisco.com

- **This topic provides guidelines for maximizing the efficiency of your IDS via settings for the following:**
 - Individual signatures
 - Monitoring applications
- **Other topics in this lesson provide guidelines for the following settings, which apply to the Sensor globally and ensure that valuable system resources are not wasted:**
 - IP logging
 - IP fragment reassembly
 - TCP stream reassembly

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-17

You can dramatically increase the benefits of your IDS by adhering to the guidelines presented in this topic. These guidelines apply to settings for individual signatures and monitoring applications. However, you can further increase these benefits by increasing the efficiency of your Sensor via global Sensor settings that can be used to conserve valuable system resources. The following global Sensor settings can be configured:

- IP logging
- IP fragment reassembly
- TCP stream reassembly

Logging

This topic explains the logging capabilities of the Sensor, how to configure logging settings via the Cisco IDS Device Monitor (IDM), and the effects of IP logging on the Sensor.

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**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—10-19

The Sensor 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 EventStore. Management consoles such as IEV and the Monitoring Center for Security 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.

IP Logging

Cisco.com

- **The Sensor 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-20

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 can also configure IP log files to be generated for specific IP addresses. This causes the Sensor to log all traffic going to and from the specified IP 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 reusable ring of files for IP logging. After 2 GB of data has been logged, the Sensor starts reusing these files. The Sensor reuses 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. Because the files are preallocated, there is no reason to delete them; however, remember that IP logging does impact performance.

Note The 2-GB limit mentioned may vary from platform to platform.

You can use the command line interface (CLI) **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 Secure Copy (SCP).
- Download the IP log files via IDM.

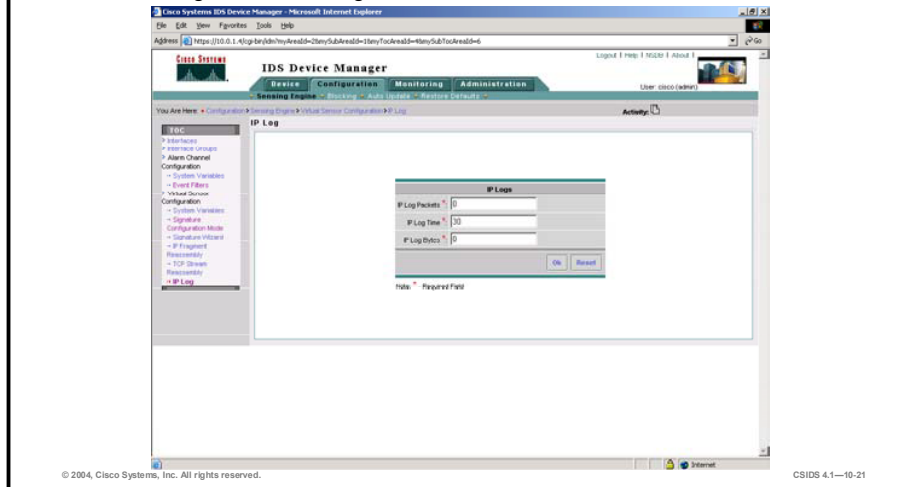
After retrieving the IP log files, you can use a network protocol analyzer to examine the data. You can use Ethereal, tcpdump, or any other reader that understands libpcap format. Libpcap format contains the data of the captured packets in binary form and is a standard used by network tools such as WinDump, 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—Global Setting

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > IP Log.



The IDM enables 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.

You can specify how long, in minutes, IP logging will continue 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 IDM, Monitoring Center for IDS Sensors (IDS MC), or the CLI.

Complete the following steps to edit automatic IP logging in the IDM:

Step 1 Choose **Configuration > Sensing Engine > Virtual Sensor Configuration > IP Log**. The IP Log page is displayed.

Step 2 Enter values for the settings listed in the following table:

IDM Automatic IP Logging Settings	Description
IP Log Packets	Maximum number of packets to be logged in an event. The default is 0.
IP Log Time	Length of the IP session during which information is logged. The default is 30 minutes.
IP Log Bytes	Maximum number of bytes that will be logged in an event. The default is 0.

Note You only need to enter one of the values listed in the table. IP logging will stop when the first condition is met.

Step 3 Click **OK**. The following message is displayed:

IP Log configuration has been updated. To commit the changes, click the save changes icon in the Activity bar.

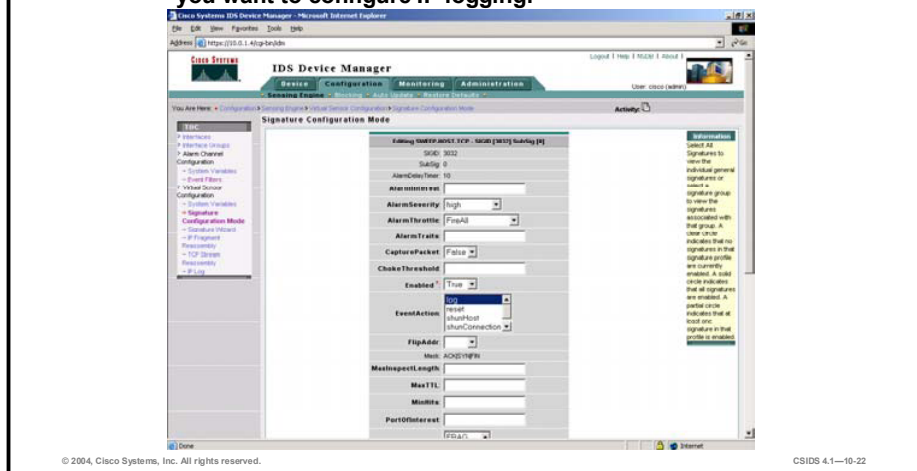
Step 4 Click **OK**. The IP Log page is refreshed.

Step 5 Click the save changes icon in the Activity bar.

Automatic IP Logging—Signature Setting

Cisco.com

Choose **Configuration > Sensing Engine > Signature Configuration Mode** and locate the signature for which you want to configure IP logging.



Complete the following steps to edit a signature to perform automatic IP logging using IDM:

Step 1 Choose **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode**. The Signature Configuration Mode page is displayed.

Step 2 Select **All Signatures** from the Signature Groups pane. The All Signatures page is displayed.

Step 3 Select the check box next to the signature to be edited or use the Page popup menu to view a list of other signatures.

Step 4 Click **Edit**. The Editing page is displayed.

Step 5 Select **log** from the EventAction pane.

Step 6 Click **OK**. The following message is displayed:

The signature has been updated. To commit the changes, click the save changes icon in the Activity bar.

Step 7 Click **OK**. The All Signatures page is refreshed. The Action column of the edited signature displays *log*.

Step 8 Click the save changes icon in the Activity bar.

Manual IP Logging

Cisco.com

Choose Administration > IP Logging.

The screenshot shows the 'IP Logging Configuration' table with the following data:

#	Log ID	IP Address	Interface Group	Status	More
1	13020700	10.0.1.12	0	completed	
2	13020700	172.26.26.150	0	completed	
3	13020700	10.0.1.12	0	completed	
4	13020700	10.0.2.2	0	completed	
5	13020700	10.0.1.12	0	completed	
6	13020700	172.26.26.150	0	completed	
7	13020704	10.0.1.12	0	completed	
8	13020704	172.26.26.150	0	completed	
9	13020706	10.0.2.2	0	completed	

Below the table, there are controls for 'Rows per page' (set to 10) and 'Page' (1 of 1). Action buttons include 'Select All', 'Deselect All', 'Add', 'Stop', and 'Reset'. A note states: 'Select an item then take an action.' An information box on the right explains: 'You can configure the Sensor to capture all traffic related to the specified hosts. Specify the IP Address of any host for which you want to log IP traffic.'

© 2004, Cisco Systems, Inc. All rights reserved.

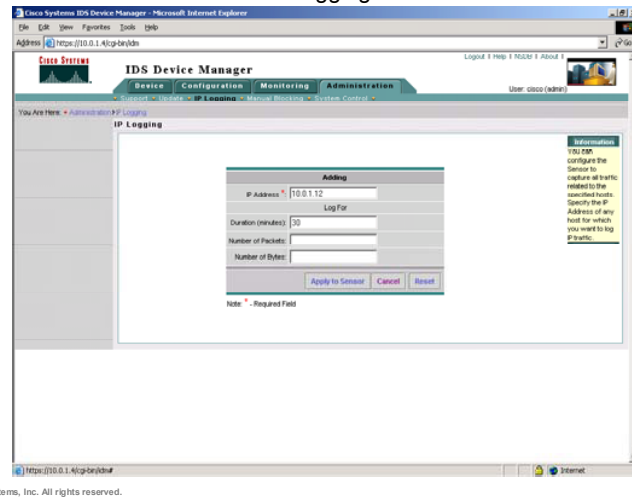
CSIDS 4.1—10-23

You can configure the Sensor to capture all IP traffic associated with the hosts you specify by IP address.

Manual IP Logging (Cont.)

Cisco.com

Choose Administration > IP Logging and select Add.



Complete the following steps to generate log files for specific IP addresses:

- Step 1** Select **Administration > IP Logging**. The IP Logging Configuration window appears.
- Step 2** Click **Add**. The Adding window is displayed.
- Step 3** Enter values for the settings listed in the following table:

IDM Manual IP Logging Settings	Description
IP Address	IP address of the host whose IP traffic you want to log
Duration (minutes)	(Optional.) The number of minutes you want the Sensor to log IP traffic
Number of Packets	(Optional.) The number of packets you want the Sensor to count
Number of Bytes	(Optional.) The number of bytes you want to log

Note When any one of the duration, number of packets, or number of bytes limits is met, the log closes.

- Step 4** Click **Apply to Sensor** to save your changes. The IP Logging Configuration page now displays the new Log ID.

Note The Sensor begins logging and creates a log file.

- Step 5** To discontinue logging IP traffic, select the check box next to the log ID, and then click **Stop**.

Viewing IP Logs

Cisco.com

Choose **Monitoring > IP Logs** and select the **Log ID**.

#	Log ID	IP Address	Interface Group	More
1	136207000	10.0.1.12	0	
2	136207001	172.26.26.190	0	
3	136207000	10.0.1.12	0	
4	136207001	10.0.2.2	0	
5	136207000	10.0.1.12	0	
6	136207000	172.26.26.190	0	
7	136207004	10.0.1.12	0	
8	136207005	172.26.26.190	0	
9	136207006	10.0.2.2	0	

You can view a log file by completing the following:

- Step 1** Select **Monitoring > IP Logs**. The IP Logs page is displayed.
- Step 2** Click the hyperlink for the log file that you want to download in the Log ID column. The File Download Window appears.
- Step 3** Click **Save As**. The file is saved in tcpdump format. Use a third-party tool that can read tcpdump files, such as Ethereal, to view the log files.

Reassembly Options

This topic describes IP fragment and TCP stream reassembly. It also explains how configuring their settings affects the Sensor.

Reassembly Overview

Cisco.com

- **You can configure Sensor reassembly settings for both of the following:**
 - IP fragments
 - TCP streams
- **Reassembly settings affect the Sensor's overall sensing function but are not necessarily specific to a particular signature or set of signatures.**
- **Reassembly settings ensure that valuable system resources are not wasted.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-10-27

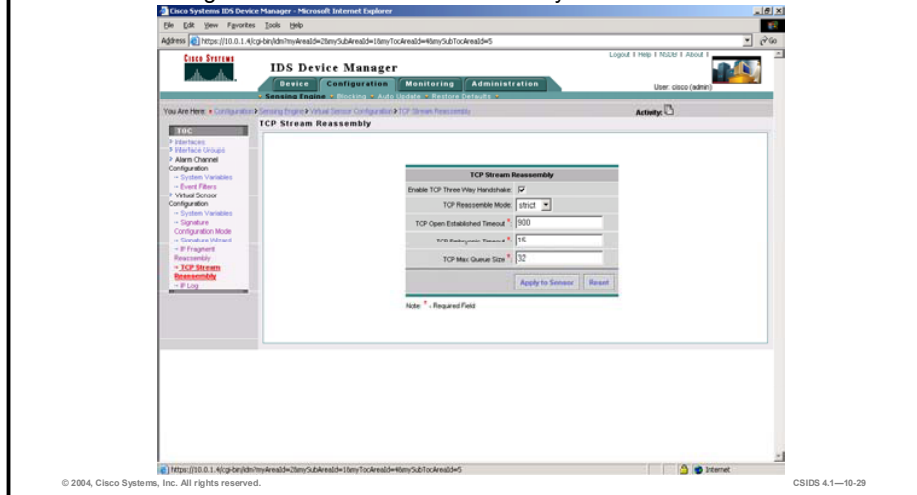
Reassembly options affect the sensing function but are not necessarily specific to a particular signature or set of signatures. Reassembly settings ensure that valuable system resources are not wasted. In IDM, you can select reassembly options for the following:

- IP fragments
- TCP streams

TCP Stream Reassembly Options

Cisco.com

Choose Configuration > Sensing Engine > Virtual Sensor Configuration > TCP Stream Reassembly.



Like IP fragment reassembly options, TCP stream reassembly options apply to Sensors globally and enable you to conserve valuable system resources. For example, you can configure the Sensor to monitor only TCP sessions that have been established by a complete three-way handshake. You can also configure how long to wait for the handshake to complete and how long to keep monitoring a connection where no more packets have been seen. The goal is to prevent the Sensor from wasting resources in situations where a valid TCP session is not established.

Complete the following steps to configure TCP stream reassembly:

- Step 1** Select **Configuration > Sensing Engine > Virtual Sensor Configuration > TCP Stream Reassembly**. The TCP Stream Reassembly page is displayed.
- Step 2** Enter reassembly values for the settings listed in the following table:

TCP Stream Reassembly Settings	Description
Enable TCP Three Way Handshake	Select the check box to specify that the Sensor only tracks sessions for which the three-way handshake is completed.
TCP Reassemble Mode	The mode of reassembly. You can select one of the following from a drop-down menu: <ul style="list-style-type: none"> ■ Strict—If a packet is missed for any reason, all packets after the missed packet are processed. ■ Loose—Use in environments where packets might be dropped.
TCP Open Established Timeout	The number of seconds that can elapse before the Sensor frees the resources allocated to a fully established TCP connection when no more packets are being seen for that connection. The default is 900.
TCP Embryonic Timeout	The number of seconds that can elapse before the Sensor frees the resources allocated for an initiated, but not fully established, TCP session.

TCP Stream Reassembly Settings	Description
TCP Max Queue Size	The number of packets that can enter the queue. The default is 32.

Note A session is considered embryonic if it has not completed the three-way handshake.

Step 3 Click **Apply to Sensor** to save your changes. The following message appears:

TCP Stream Reassembly configuration has been updated. To commit the changes please click the save changes icon in the Activity bar.

Step 4 Click the save changes icon in the Activity bar.

Alarm Channel System Variables

This topic explains alarm channel system variables and how they are used.

System Variables Overview

Cisco.com

System variables enable you to use the same value within multiple signature filters.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—10-31

Alarm channel 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 all filter variables are updated. This prevents you from having to change the variable repeatedly as you configure alarm channel filters.

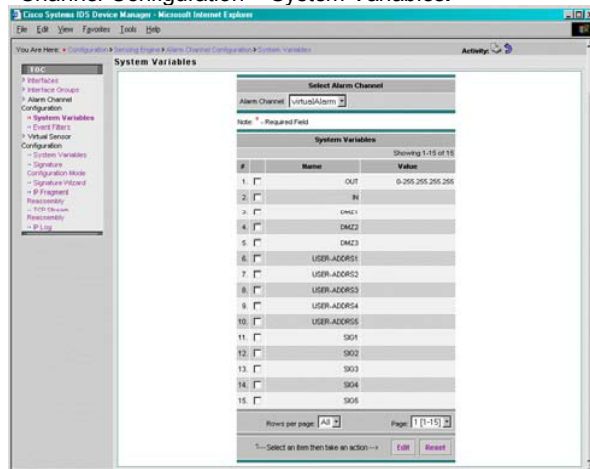
For example, assume that you have an IP address space that applies to your engineering group. Because there are no Windows systems in that group, you are not worried about Windows-based attacks. You can configure a USER-ADDR1 to be the engineering group IP address space. Then, you can use this variable on the Event Filters page to configure the filter to ignore all Windows-based attacks on USER-ADDR1.

You can change the value of an alarm channel system variable, but you cannot add or delete variables. You also cannot change the name, type, or constraints of a variable.

Alarm Channel System Variables

Cisco.com

Choose Configuration > Sensing Engine > Alarm Channel Configuration > System Variables.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-32

Complete the following steps to define alarm channel system variables:

Step 1 Choose **Configuration > Sensing Engine > Alarm Channel Configuration > System Variables**. The System Variables page is displayed.

Step 2 Select the check box next to the system variable you want to edit, and click **Edit**. The alarm channel system variables are defined in the following table:

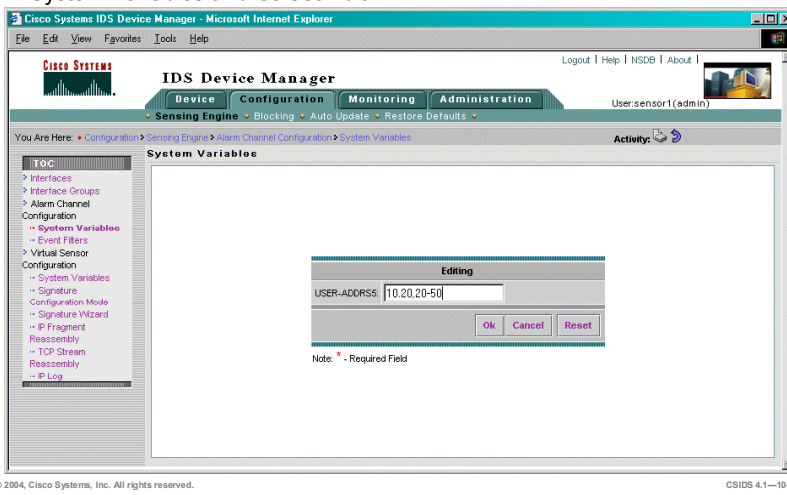
Variable	Description
OUT	Anything that is not included in IN. You cannot edit this variable. The default is 0-255.255.255.255.
IN	A list of all internal IP address spaces.
DMZ1, DMZ2, and DMZ3	Any valid IP address.
USER-ADDRS1, USER-ADDRS2, USER-ADDRS3, USER-ADDRS4, and USER-ADDRS5	Any valid IP address.
SIG1, SIG2, SIG3, SIG4, and SIG5	Any valid signature ID. You can use SIG to define popular signatures that you like to exclude for certain addresses.

Note You can reset the form by clicking **Reset**.

Alarm Channel System Variables (Cont.)

Cisco.com

Choose Configuration > Sensing Engine > Alarm Channel Configuration
> System Variables and select Edit.



When you select a system variable from the System Variables page and click **Edit**, the Editing panel for the variable you chose is displayed. Continue configuring the system variable by completing the following steps:

Step 1 Enter the values for the system variable. For example, the 192.168.1.0 network with a 255.255.255.0 netmask can be specified as follows:

- 192.168.1.0-192.168.1.255—This designates the network as a range of single IP addresses. The hyphen, "-", indicates the range of IP addresses between any two given IP addresses.
- 192.168.1.0/24—This designates the network using the numerical bit masking.
- 192.168.1.—This designates the network by leaving off the last octet. The Sensor treats IP addresses with missing octets like networks.
- 192.168.1—This also designates the network by leaving off the last octet but without the trailing period: "."

You can also designate multiple IP addresses and networks for a single variable by placing a comma, ",", between the entries. For example, entering 10.20,20-50 results in the following networks:

- 10.20—Network 10.20.0.0 with netmask 255.255.0.0
- 20-50—31 different networks (20.0.0.0 255.0.0.0, 21.0.0.0 255.0.0.0, 22.0.0.0 255.0.0.0, and so on, ending with 50.0.0.0 255.0.0.0)

Note If you use commas as delimiters, make sure there are no trailing spaces after the comma. Otherwise, you receive a Validation failed error.

Step 2 Click **OK**.

Step 3 Click the save changes icon in the Activity bar to save your system variable.

Note You can undo your changes by clicking the undo changes icon on the Activity bar.

Alarm Channel Event Filtering

This topic explains alarm channel event filtering and describes how to create filters that enhance Sensor functionality and performance.

Filtering Overview

Cisco.com

Alarm channel event filtering enables you to do the following:

- Reduce the number of false positives.
- Limit the number of security events reported.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—10-35

Alarm channel event filtering enables you to do the following:

- Reduce the number of false positives.
- Reduce the number of security events reported.

Filtering Overview (Cont.)

Cisco.com

An alarm channel event filter is defined by specifying the following:

- **Signature**
- **Source address**
- **Destination address**
- **Whether the filter constitutes an exception to another filter**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-36

Filtering an event in the alarm channel means that the Sensor will analyze the data stream but will not generate an alarm for the signature you specify in the filter. Filtering all alarms from a particular signature is not the same thing as disabling that signature; disabling results in no analysis of the data stream for that signature. A filter is defined by specifying the signature, the source address, the destination address, and whether this filter constitutes an exception to another filter.

Filtering Process

Cisco.com

The Sensor sensing engine performs the following filtering processes:

- **The Sensor detects the attack against the protected network.**
- **The Sensor sensing engine determines whether a signature filter exists.**
- **The Sensor checks the filter parameters and compares them against the network traffic.**
- **If the traffic does not match the filter, the Sensor generates an alert.**
- **If the traffic matches the filter, the Sensor does not generate an alert.**
- **If the traffic matches the filter and the filter is an exception, the Sensor generates an alert.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-37

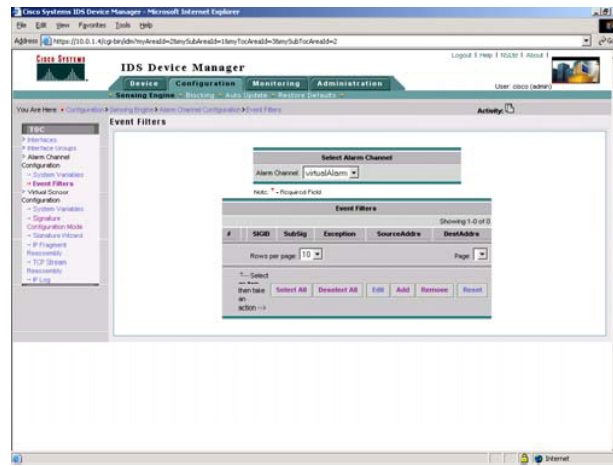
The Sensor sensing engine performs the following filtering processes:

1. The Sensor detects the attack launched against the protected network.
2. The Sensor's sensing engine determines whether signature filters exist.
3. The Sensor checks the filter parameters and compares them to the traffic that triggered the attack.
4. The Sensor does 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 not an exception, the Sensor does not generate an alert.
 - If the traffic matches the filter and the filter is an exception, the Sensor generates an alert, and the signature action is implemented if configured.

Configuring Alarm Channel Event Filters

Cisco.com

Choose **Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters**.



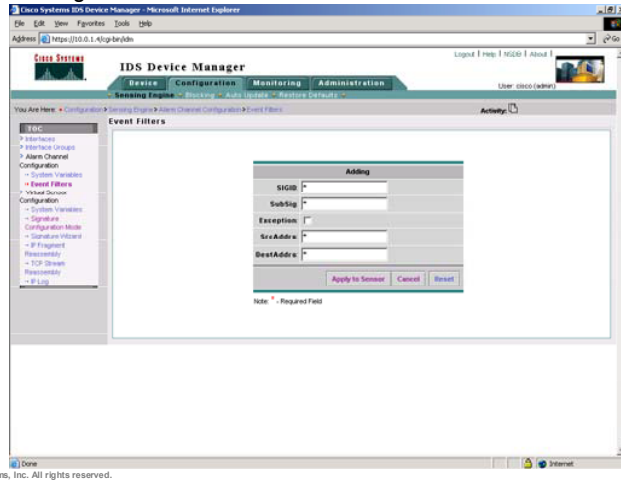
Complete the following steps to create an event filter:

- Step 1** Choose **Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters**. The Event Filters page is displayed.
- Step 2** Select **Add**. The Event Filters Adding page is displayed.

Alarm Channel Event Filter—Add

Cisco.com

Choose Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters and select Add.



Complete the following steps to finish configuring the filter:

Step 1 Enter event filter values for the settings listed in the following table:

Event Filter Settings	Description
SIGID	The signature IDs of the events to which this filter should be applied. You can use any of the following: <ul style="list-style-type: none"> ■ A list (2001, 2004) ■ A range (2001-2004) ■ An asterisk (*) for all signatures ■ An alarm channel system variable if you defined variables on the Alarm Channel System Variables page. If you use a variable, you must preface it with \$.
SubSig	The sub-signature IDs of the events to which this filter should be applied
Exception	A check box that allows you to indicate whether this filter is an exception to another filter
SrcAddr	The source addresses of events to which this filter should be applied. You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page. If you use a variable, you must preface it with \$.
DestAddr	The destination addresses of events to which this filter should be applied. You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page. If you use a variable, you must preface it with \$.

Step 2 Click **Apply to Sensor**.

Step 3 Click the save changes icon in the Activity bar to save your changes. The following message appears:

Configuration information is not available at this time. Try again in a few minutes.

Step 4 After a few minutes, click **Event Filters** again to see the filter you added. The filter is displayed on the Event Filters page.

Filter Exceptions

Cisco.com

As you configure filter exceptions, keep the following in mind:

- **If you want to define an exception to a filter, you must create two filters and define one filter as an exception to the other.**
- **If you define two filters and one constitutes an exception to the other, the exception filter takes precedence.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-40

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 defining a filter and an exception filter.

Complete the following steps to define a filter:

- Step 1** Specify the 5330 signature.
- Step 2** Specify the source address as system variable `OUT`, which is the network that is generating the large number of alarms.
- Step 3** Specify all destination addresses.

Complete the following steps to define an exception filter:

- Step 1** Specify the 5330 signature.
- Step 2** Specify the source address as system variable `OUT`, which is the network that is generating the large number of alarms.
- Step 3** Specify the address of your vulnerable Apache server as the destination.

By creating these two filters, you can filter out a large number of alarms while allowing some of them to pass through. This is possible because the exception filter takes precedence.

Alarm Channel Event Filters Versus Alarm on IP Address

Cisco.com

Alarm channel filtering compares to the Sensor alarm on IP address feature as follows:

- **Both provide the ability to limit alarms to specific IP addresses.**
- **Alarm channel filtering performs post-filtering so that the alarm is dropped only after the signature has fired and the alarm has been generated. This processing has an impact on performance.**
- **Alarm on IP address performs pre-filtering so that the signature fires only if the address in the traffic matches the address specified in the signature. Therefore, there is little impact on performance.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-41

In IDS Software Version 4.1, you can configure atomic signatures to trigger alarms only on certain source or destination IP addresses. Both the alarm on IP address feature and alarm channel event filters provide the ability to limit alarms to specific IP addresses. The difference in the two lies in their impact on Sensor performance. The alarm on IP address feature has little impact on performance because it performs pre-filtering. The signature fires only if the address in the traffic being inspected matches the address specified in the signature configuration. In contrast, alarm channel filters perform post-filtering so that the alarm is dropped only after the signature fires and the alarm is generated. The required processing creates the performance impact.

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- Cisco IDS signatures use anti-evasive mechanisms to defeat IP fragmentation and obfuscation.
- To enable your IDS to serve you most efficiently, configure the following on your Sensor according to the needs of your particular network:
 - Signature parameters
 - IP logging
 - Reassembly options
 - Alarm channel event filters
- You should also configure your monitoring application for optimal functionality in your particular network.
- IP fragment reassembly options and TCP stream reassembly options apply to Sensors globally and enable you to conserve valuable system resources.
- Alarm channel system variables facilitate the use and modification of values in alarm channel event filters.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-43

Summary (Cont.)

Cisco.com

- **Event logging is the logging of application errors, alerts, status changes, blocking requests, and records of controls transactions in the Sensor EventStore.**
- **IP logging is capturing raw, unaltered IP packets that 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 by specifying it when you configure a signature.**
- **You can also configure the Sensor to log all IP traffic going to and from a specified address whether there is an attack or not.**
- **Alarm channel event filtering enables you to reduce the number of false positives and the number of security events reported.**
- **Alarm channel event filtering causes the Sensor to analyze the data stream but not generate an alarm.**
- **An alarm channel event filter is defined by specifying a signature, a source address, a destination address, and whether this filter constitutes an exception to another filter.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—10-44

Blocking Configuration

Overview

This lesson explains 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 take into account before you select the interface on which to apply the blocking access control lists (ACLs).

This lesson includes the following topics:

- Objectives
- Introduction
- ACL considerations
- Blocking Sensor configuration
- Master Blocking Sensor configuration
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

Upon completion of this lesson, you will be able to perform 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.**
- **Configure a Sensor to perform blocking with a Cisco IDS device.**
- **Configure a Sensor to perform blocking through a Master Blocking Sensor.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-3

Introduction

This topic explains what blocking is and provides some guidelines for 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
- **Logical device**—Logical settings to be applied to blocking devices
- **Managed device**—The Cisco IDS device that is to block the attack; 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 or VLAN**—The interface or VLAN on the managed device where the Cisco IDS Sensor applies the ACL or VACL
- **Active ACL or VACL**—The ACL or VACL created and applied to the managed interfaces or VLANs by the Sensor

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-5

The following are terms used when discussing the Cisco IDS blocking feature:

- **Blocking**—A Cisco IDS feature commonly referred to as blocking that prevents packets from reaching their destination.
- **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.
- **Logical device**—Logical settings to be applied to blocking devices.
- **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, that 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 or VLAN**—The interface or VLAN on the managed device where the Sensor applies the dynamically created ACL or VLAN access control list (VACL). This interface or VLAN is also referred to as a blocking interface or blocking VLAN.

Note The Cisco PIX Firewall uses the **shun** command to enforce a block. The PIX Firewall ACLs are not modified.

- Active ACL or VACL—The ACL or VACL dynamically created and maintained by the Sensor and applied to the managed interface or VLAN.

Blocking Devices

Cisco.com

- Cisco routers
- PIX Firewalls
- Catalyst 6000 switches

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-6

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 Software Release 11.2 or later using ACLs
- PIX Firewall running version 6.0 or later using the **shun** command—You must use one of the following PIX Firewall models:
 - 501
 - 506E
 - 515E
 - 525
 - 535
- Catalyst 6000 switches—Hardware and software requirements for Catalyst 6000 switch blocking devices vary depending on the following:
 - Switch operating system—Cisco IOS software on the Supervisor/Multilayer Switch Feature Card (MSFC), called native mode, or Catalyst operating system software on the Supervisor with Cisco IOS software on the MSFC, called hybrid mode
 - Sensor type—Appliance or IDS Module 2 (IDSM2)
 - Your choice of blocking method—ACLs or VACLs

Blocking is configured using 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 Software Version 6.0.

Blocking Device Requirements

Cisco.com

- **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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-7

The Sensor must be able to communicate with the blocking device. The Sensor must have a route to or must be on the same subnet as the managed firewall. The blocking device must have one of the following configured:

- Telnet—Telnet access should be allowed from the Sensor.
- SSH—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 Triple Data Encryption Standard (3DES) encryption.

As soon as the blocking device is configured on the Sensor, the Sensor attempts to log in to 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 antispoofing 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-8

Cisco IDS blocking is a powerful feature that should be used only 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 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:

- **Antispoofing 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. If you implement a proper antispoofing mechanism and network ingress and egress filtering (RFC 2827), the Sensor will not block possibly 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 avenues for the attacker to attack your network. It is important to identify all entry points and decide whether the connecting devices should participate in blocking.
- **Signature selection**—Cisco IDS contains several hundred signatures that can be configured for blocking. It is not feasible to perform blocking on all signatures. Identify which signatures are best suited for blocking. For example, if you were allowing only 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 ranked high and could potentially lead to access. These signatures would be candidates for 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 usernames, passwords, modal passwords, and connection types needed to log in to each blocking device.
- Interface ACL requirements—Each interface/direction can have only 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 Pre-block and Post-block ACLs. 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 or out. When blocking is not in effect, the resulting ACL applied to the interface is simply a combination of the Pre- and Post-block ACLs without any blocking entries inserted.

NAC Block Actions

Cisco.com

The following events cause the NAC to initiate a block:

- **A signature configured with a block action generates an alert.**
- **You manually initiate a temporary block from a management interface such as the CLI, IDM, or IDS MC.**
- **You manually configure the NAC to permanently block a host or network address.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-9

The Network Access Controller (NAC) is the Sensor service that initiates the network access control, or blocking, function. The NAC controls starting and stopping blocks on routers, switches, and PIX Firewalls.

The following events cause the NAC to initiate a block:

- A signature configured with a block action generates an alert.
- You manually initiate a temporary block from a management interface such as the command line interface (CLI), IDS Device Manager IDM, or the Management Center for IDS Sensors (IDS MC).
- You manually configure the NAC to permanently block a host or network address.

Blocking Process

Cisco.com

The following explains the blocking process:

- An event or action occurs that has a block action associated with it.
- The Sensor pushes a new set of ACL entries, one for each interface/direction, to each managed device.
- An alarm is sent to the EventStore at the same time the Sensor initiates the block.
- When the block expires, all configurations or ACLs are updated to remove the block.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-10

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 an SSH connection with the device and maintains the connection with the device.

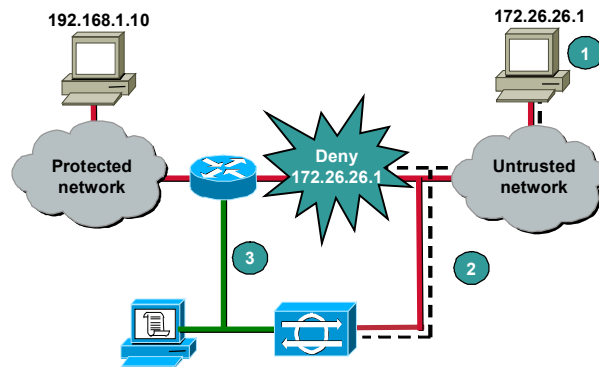
- The NAC pushes a new set of configurations or ACLs, one for each interface/direction, to each controlled device. It applies the blocking rules to all configured interface/directions on all devices it is configured to control.
- The alarm is sent to the EventStore at the same time the Sensor initiates the block. The block and alarm occur independently of each other.
- When the blocking event expires, 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

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-11

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 so that an automatic block is enforced.
- 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 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:

```
ip access-list extended IDS_e0/1_in_1
  deny ip host 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 topic describes the considerations you should take into account 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 to an external interface in an inbound direction.**
- **Apply to an internal interface in an outbound direction.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—11-13

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 topic.

You must decide on which interface and in which direction to apply the ACL. The ACL can 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 Cisco IOS Firewall feature set.

Applying ACLs on the External vs. Internal Interfaces

Cisco.com

- **External interface in the inbound direction**
 - Denies packets from the host before they enter the router.
 - Provides the best protection against an attacker.
- **Internal interface in the outbound direction**
 - Denies packets from the host before they enter the protected network.
 - The block does not apply to the router itself.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-14

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 it 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 ACLs on 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 ACL, either named or numbered.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-15

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, 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 that option is 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 numbered. The ACLs 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 nonmanaged 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 a Cisco 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 a Cisco 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 any host 192.168.2.2 eq ftp     # Pre-block ACL entry
  deny tcp host 10.1.1.200 host            # Blocking ACL entry with logging
    172.16.16.100 eq www log               enabled
  permit tcp any any                        # Post-block ACL entry

```

Blocking Sensor Configuration

This topic covers how to configure a Sensor to perform blocking.

Configuration Tasks

Cisco.com

Complete the following tasks to configure a Sensor for blocking:

- Assign the block reaction to a signature.
- Assign the Sensor global blocking properties.
- Define the logical device properties.
- Define the managed device properties.
- For Cisco IOS or Catalyst 6000 devices, assign the managed interface's properties.
- (Optional.) Assign the list of devices that are never blocked.
- (Optional.) Define a Master Blocking Sensor.

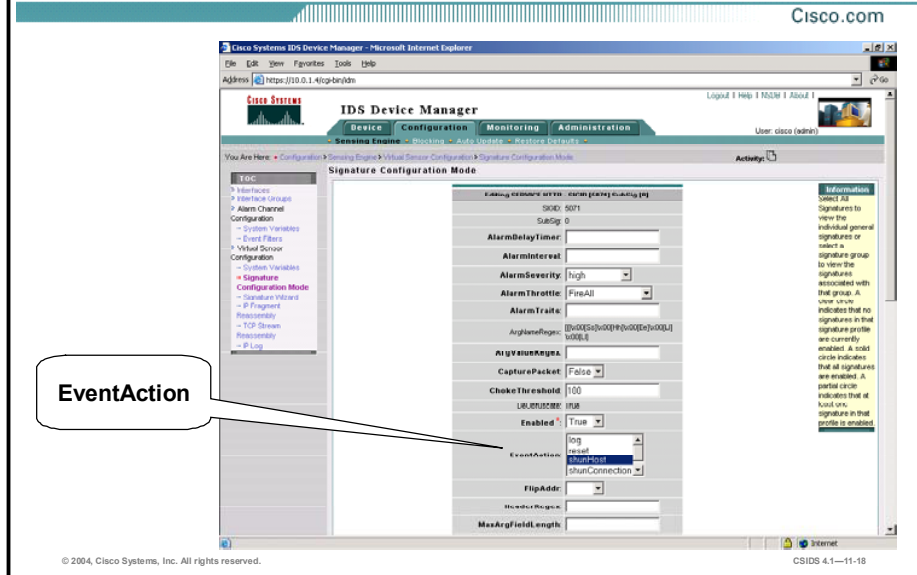
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-17

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 IDS Device Manager (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 logical device's properties—This task involves defining the username, password, and enable password for communication between the Sensor and the blocking device for the purpose of blocking.
- 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 Cisco IOS or Catalyst 6000 devices—This task involves selecting the blocking interface or VLAN and assigning 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



The first step to configure blocking is to select a signature and set its alarm response to block the offending host or connection. If you choose to block a host, all packets with the source address of the suspected intruder will be blocked. If you choose to block a connection, only those packets that are moving from the offending source to its target and are associated with the offending protocol will be blocked.

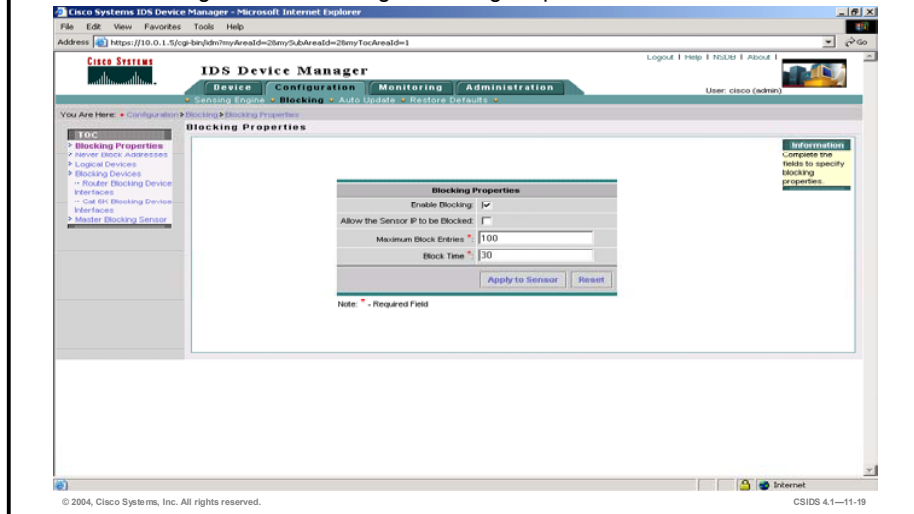
Complete the following steps to configure a signature action to block the ATOMIC.ICMP signature:

- Step 1** Open and launch the IDM and log in.
- Step 2** Choose **Configuration > Sensing Engine > Signature Configuration Mode**. The Signature Groups list is displayed.
- Step 3** Select the **Engines** category from the Top Level Categories list. The Signature Groups, Engines page is displayed.
- Step 4** Select **ATOMIC.ICMP** from the Engines list. The ATOMIC.ICMP page is displayed.
- Step 5** Select the check box for signature ID **2002**, ICMP Src Quench.
- Step 6** Click the **Edit** button. The editing ATOMIC.ICMP-SIGID [2002] Subsig [0] page is displayed.
- Step 7** Select the blocking method from the EventAction list.
- Step 8** Click the **OK** button. The following message is displayed:
The signature has been updated. To commit the changes please click the save changes icon in the Activity bar message appears.
- Step 9** Click the **OK** button. The ATOMIC.ICMP page appears and the Action for signature ID 2002 indicates shunHost.
- Step 10** Click the **save changes** icon from the Activity bar.

Sensor's Blocking Properties

Cisco.com

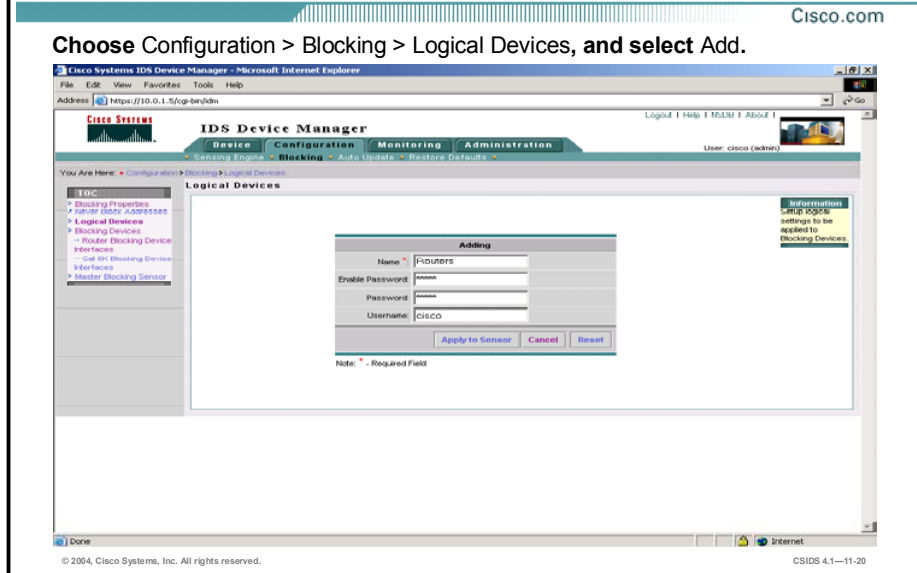
Choose Configuration > Blocking > Blocking Properties.



Complete the following steps to configure the Sensor's global blocking properties:

- Step 1** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 2** Choose **Blocking Properties** from the table of contents (TOC). The Blocking Properties page is displayed.
- Step 3** Select the **Enable Blocking** check box.
- Step 4** Select the **Allow blocking devices to block the sensor's IP address** check box if you might want to have the Sensor's IP address blocked. Select this option only if you think it is likely that the Sensor device may be compromised and that IP spoofing is unlikely. If this check box is selected, it is possible that communications from the Sensor will be blocked, thus causing loss of remote management and monitoring capabilities. If this check box is 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.
- Step 5** Enter the maximum number of ACL entries the Sensor will manage in the Maximum Block Entries field. The default number of entries is 100.
- Step 6** Enter the length of time that an automatic block will occur in the Block Time field. The default length of time is 30 minutes.
- Step 7** Click **Apply**. The Blocking Properties page is refreshed to indicate that the IDM received the changes.

Managed Device—Cisco Router



The Logical Devices page enables you to configure logical settings such as username, password, and enable password that are used to access a managed device. To configure logical device settings, complete the following steps:

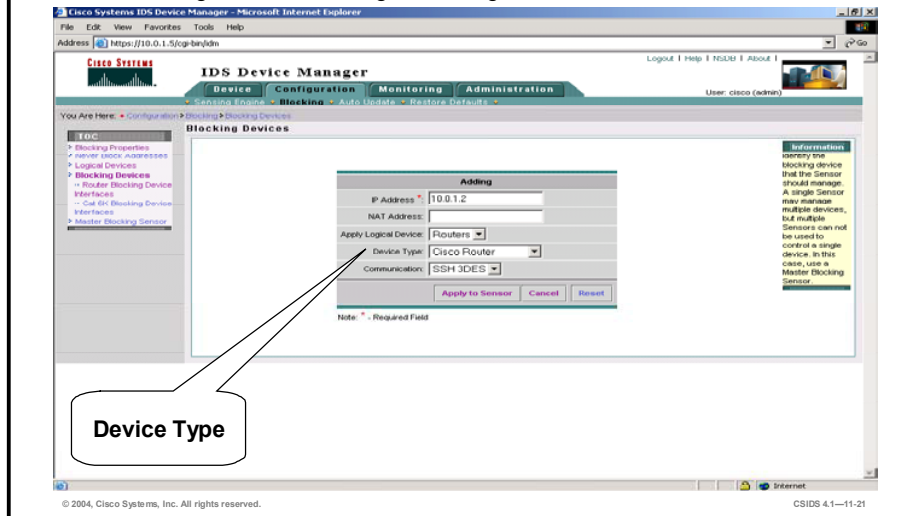
- Step 1** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 2** Choose **Logical Devices** from the TOC. The Logical Devices page is displayed.
- Step 3** Click the **Add** button. The Adding Logical Devices page is displayed.
- Step 4** Enter the name of the types of devices to be managed in the Name field.
- Step 5** Enter the enable password for the devices to be managed in the Enable Password field.
- Step 6** Enter the password for the devices being managed in the Password field.
- Step 7** Enter the username for the devices being managed in the Username field.
- Step 8** Click the **Apply to Sensor** button. The Logical Devices page refreshes, showing the new devices entry.

You must assign logical device settings to each device that the Sensor manages. Managed devices of the same type that share common usernames and passwords can use the same logical device name and settings. The figure illustrates configuring logical settings for Cisco router managed devices.

Managed Device—Cisco Router (Cont.)

Cisco.com

Choose **Configuration > Blocking > Blocking Devices**, and select **Add**.



The Blocking Devices page enables you to select the blocking device type: Router, Catalyst 6000 VACL, or PIX. The Cisco Router device type includes Cisco IOS routers and Catalyst 6000 Series switches running native Cisco IOS with an MSFC. These devices supports Sensor blocking through ACLs. Complete the following steps to add a Cisco router as a blocking device:

- Step 1** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 2** Choose **Blocking Devices** from the TOC. The Blocking Devices page is displayed.
- Step 3** Click **Add**. The Adding Blocking Devices page is displayed.
- Step 4** Enter values for the Blocking Device settings listed in the following table:

IDM Blocking Device Settings	Description
IP Address	IP address of the blocking device—Cisco router.
NAT Address	Network Address Translation (NAT) IP address of the blocking device—Cisco router.
Apply Logical Device	Drop-down menu that allows you to select the logical device to apply to this blocking device—routers.
Device Type	Drop-down menu that allows you to select a blocking device type.
Communication	Drop-down menu that allows you to select a mode of communication between the Sensor and the blocking device. The default is SSH-3DES. The options available are SSH-3DES, SSH-DES, and Telnet.

- Step 5** Click **Apply to Sensor**. The Blocking Devices page is displayed with the new device entry.

If SSH-DES or 3DES is selected as the secure communication method, SSH password authentication will be used, not public key authentication. Also, the Cisco 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  
!
```

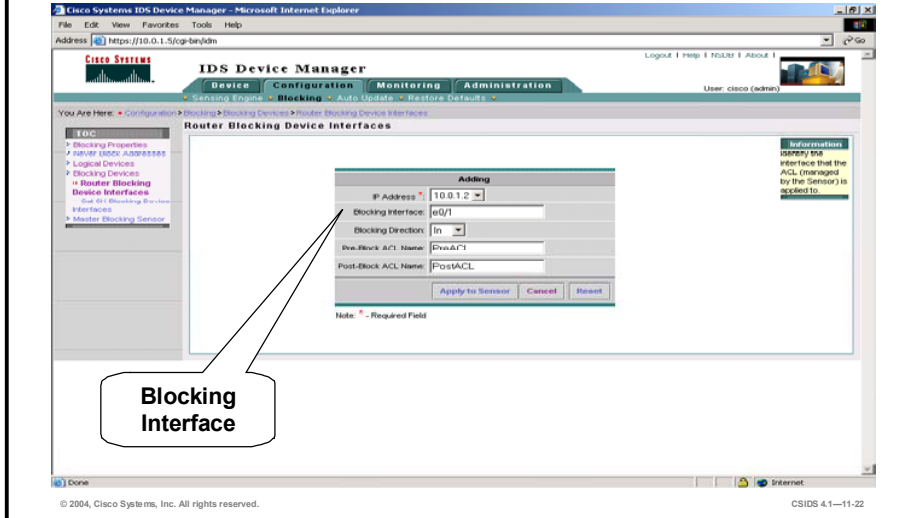
The IOS command **crypto key generate rsa** does not appear in the static configuration but is used to enable the SSH server and generates the server public and private keys for SSH authentication.

The IOS commands **show users** and **show ssh** can be used to verify that the Sensor has logged in to the Cisco router and established an SSH connection; the encryption level is also displayed.

Managed Device—Cisco Router (Cont.)

Cisco.com

Choose **Configuration > Blocking > Router Blocking Device Interfaces**, and select **Add**.



- Step 6** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 7** Choose **Blocking Devices > Router Blocking Device Interfaces** from the TOC. The Router Blocking Device Interfaces page is displayed.
- Step 8** Click **Add**. The Router Blocking Device Interfaces Adding page is displayed.
- Step 9** Enter values for the Blocking Device Interface settings listed in the following table:

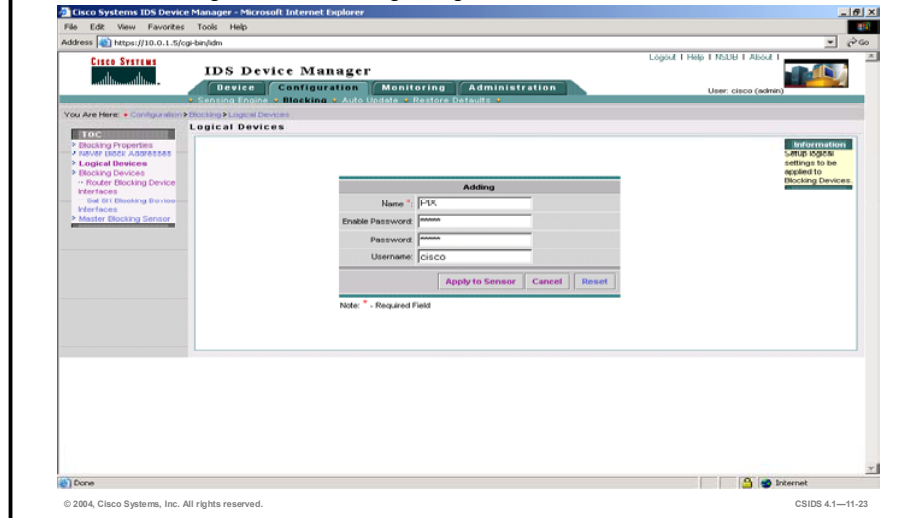
IDM Blocking Device Interface Settings	Description
IP Address	Drop-down menu that allows you to select the blocking device IP address.
Blocking Interface	Allows you to enter the name of the interface that will perform the blocking.
Blocking Direction	Drop-down menu that allows you to select the direction in which blocking will occur. The options available are in and out.
Pre-block ACL Name	Name of the ACL that includes entries to insert prior to the blocking ACL entries.
Post-block ACL Name	Name of the ACL that includes entries to append after the blocking ACL entries.

- Step 10** Click **Apply to Sensor**. The Router Blocking Device Interfaces page is displayed with the new interface entry.

Managed Device—PIX Firewall

Cisco.com

Choose Configuration > Blocking > Logical Devices, and select Add.

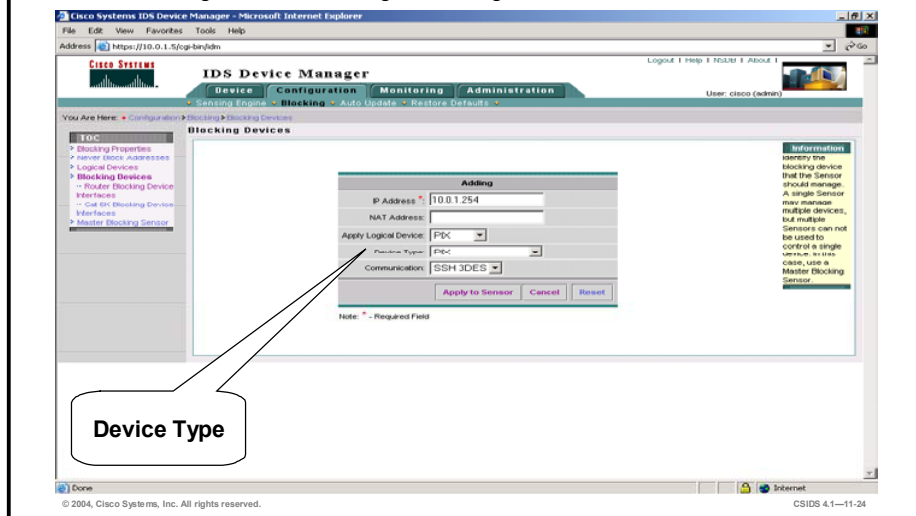


The figure illustrates configuring logical settings for a PIX Firewall managed device. The process is the same as for any other type of managed device.

Managed Device—PIX Firewall (Cont.)

Cisco.com

Choose Configuration > Blocking > Blocking Devices, and select Add.



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; it does not support the blocking of specific host connections or the manual blocking of entire networks or subnetworks. The **shun** command is available in PIX Firewall Software Versions 6.0 and later.

Complete the following steps to add a PIX Firewall as a blocking device:

- Step 1** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 2** Choose **Blocking Devices** from the TOC. The Blocking Devices page is displayed.
- Step 3** Click **Add**. The Blocking Devices Adding page is displayed.
- Step 4** Enter values for the IDM Blocking Device settings listed in the following table:

IDM Blocking Device Settings	Description
IP Address	IP address of the blocking device—PIX Firewall.
NAT Address	NAT IP address of the blocking device—PIX Firewall.
Apply Logical Device	Drop-down menu that allows you to select the logical device to apply to this blocking device—PIX.
Device Type	Drop-down menu that allows you to select a blocking device type.
Communication	Drop-down menu that allows you to select a mode of communication between the Sensor and the blocking device. The default is SSH-3DES. The options available are SSH-3DES, SSH-DES, and Telnet.

- Step 5** Click the **Apply to Sensor** button. The Blocking Devices page refreshes, showing the new blocking devices entry.

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 Firewall 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 authentication, authorization, and accounting (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        # Allow 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.

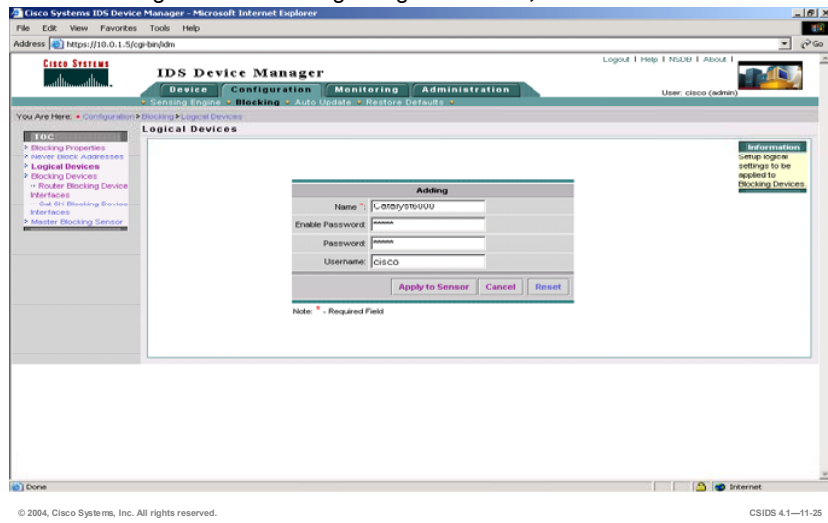
The PIX Firewall **show ssh sessions** command can be used to verify that the Sensor has logged in to the PIX Firewall and established an SSH connection. The encryption level is also displayed.

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 Switch

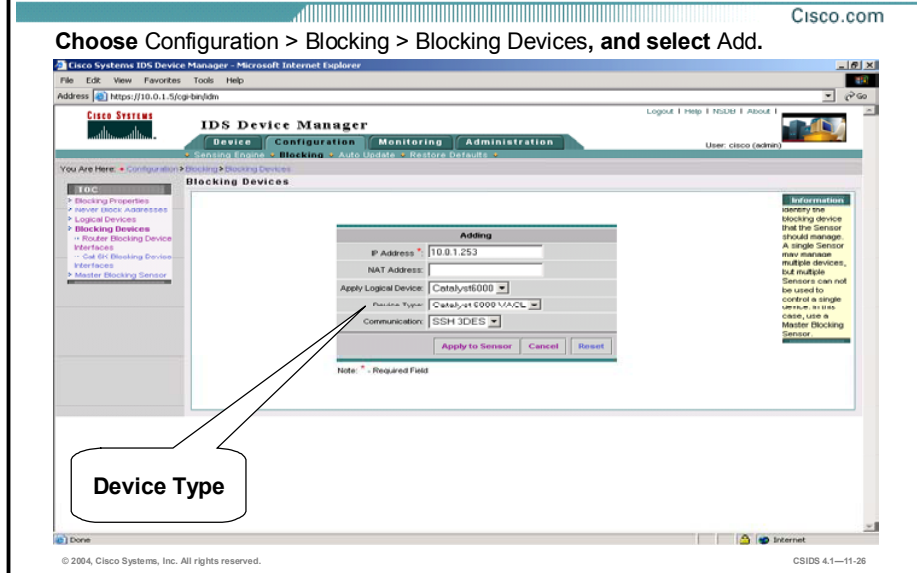
Cisco.com

Choose Configuration > Blocking > Logical Devices, and select Add.



The figure illustrates configuring logical settings for a Catalyst 6000 Series switch managed device. The process is the same as for any other type of managed device.

Managed Device—Catalyst 6000 Switch (Cont.)



Blocking is configured on a Catalyst 6000 switch 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 switch as a blocking device using VACLs:

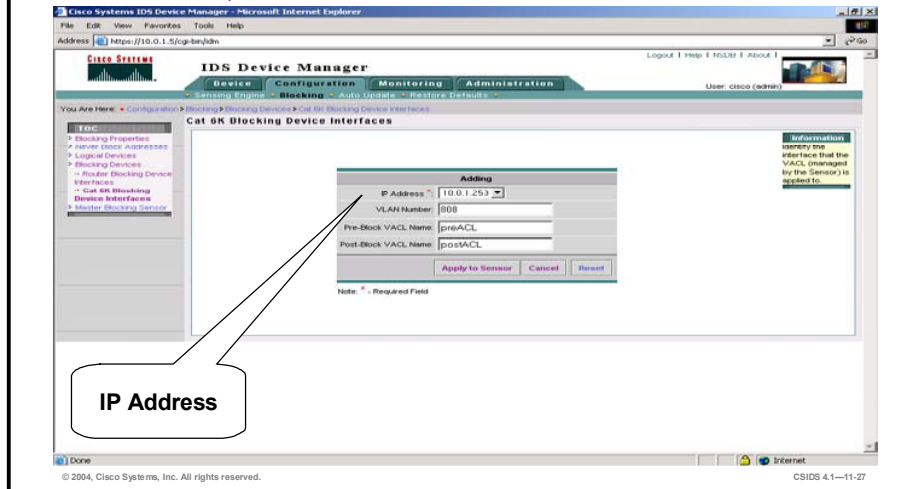
- Step 1** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 2** Select **Blocking Devices** from the TOC. The Blocking Devices page is displayed.
- Step 3** Click **Add**. The Blocking Devices Adding page is displayed.
- Step 4** Enter values for the Blocking Device settings listed in the following table:

Blocking Device Settings	Description
IP Address	IP address of the blocking device—Catalyst 6000 switch.
NAT Address	NAT IP address of the blocking device—Catalyst 6000 switch.
Apply Logical Device	Drop-down menu that allows you to select the logical device to apply to this blocking device—Catalyst6000.
Device Type	Drop-down menu that allows you to select a blocking device type.
Communication	Drop-down menu that allows you to select a mode of communication between the Sensor and the blocking device. The default is SSH-3DES. The options available are SSH-3DES, SSH-DES, and Telnet.

Managed Device—Catalyst 6000 Switch (Cont.)

Cisco.com

Choose **Configuration > Blocking > Blocking Devices > Cat 6K Blocking Device Interfaces**, and select **Add**.



Step 5 Choose **Configuration > Blocking**. The Blocking page is displayed.

Step 6 Choose **Blocking Devices > Cat 6K Blocking Device Interfaces** from the TOC. The Cat 6K Blocking Device Interfaces page is displayed.

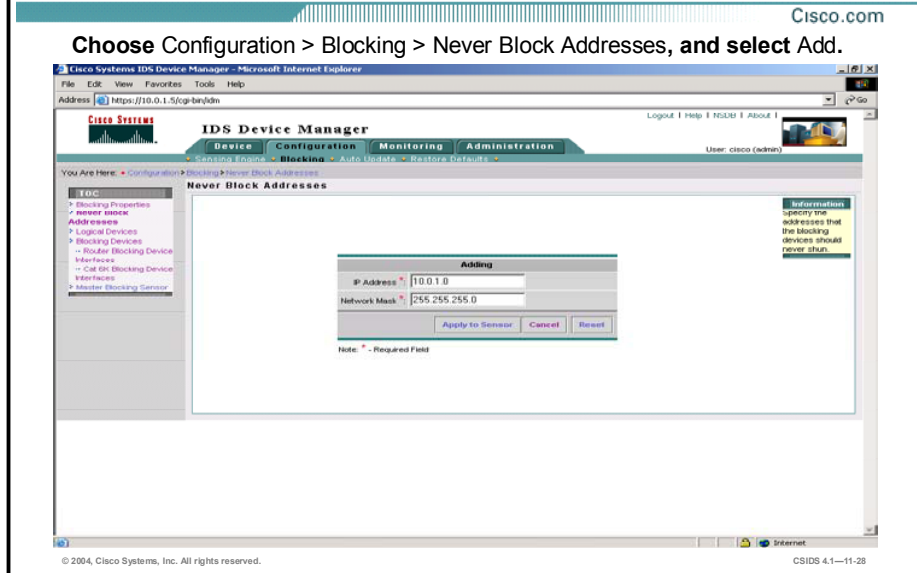
Step 7 Click **Add**. The Cat 6K Blocking Device Interfaces Adding page is displayed.

Step 8 Enter values for the Blocking Device Interface settings listed in the following table:

Blocking Device Interface Settings	Description
IP Address	Drop-down menu that allows you to select the IP address of the blocking device to be used
VLAN Number	VLAN number that will be used to initiate blocking
Pre-block VACL Name	Name of the VACL that is used prior to the blocking entries
Post-block VACL Name	Name of the VACL that is used after the blocking entries

Step 9 Click **Apply to Sensor**. The Cat 6K Blocking Device Interfaces page is displayed with the new entry.

Never-Block Addresses

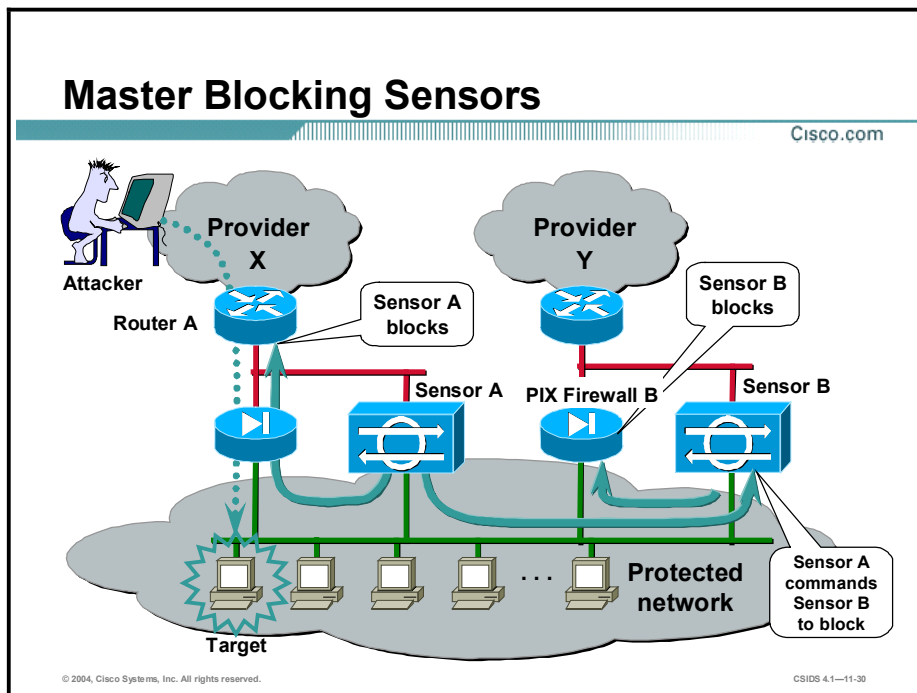


Cisco IDS enables you to define a list of network addresses of hosts or networks that will never be blocked. These addresses may include critical servers or hosts that, if blocked, would severely impact business operations. If used, take additional cautionary measures to ensure that these hosts cannot 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 > Blocking**. The Blocking page is displayed.
- Step 2** Choose **Never Block Addresses** from the TOC. The Never Block Addresses page is displayed.
- Step 3** Click **Add**. The Never Block Addresses Adding page is displayed.
- Step 4** Enter the IP address of the 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** Click **Apply to Sensor**. The Never Block Addresses page is displayed with the new entry.

Master Blocking Sensor Configuration

This topic explains how to configure a Master Blocking Sensor.



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

Cisco.com

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.**
- **A Blocking Forwarding Sensor is a Sensor that sends block requests to a Master Blocking Sensor.**
- **Any 4.x Sensor can act as a Master Blocking Sensor for any other 4.x 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 Blocking Forwarding Sensors.**
- **A Master Blocking Sensor can use other Master Blocking Sensors to control other devices.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-31

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, Post Office Protocol (POP) is the protocol used to communicate blocking instructions. In IDS version 4.0 Sensors and later, Remote Data Exchange Protocol (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 be configured only 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 continue for an extended period of time.

Configuring the Use of a Master Blocking Sensor

Cisco.com

- On the Blocking Forwarding Sensor, complete the following tasks:
 - Specify the Master Blocking Sensor.
 - Define RDEP communication parameters.
 - If you use the IDS MC for configuration, RDEP parameters of the Master Blocking Sensor are automatically retrieved.
 - If you use the IDM or CLI for configuration, you must manually configure the RDEP parameters.
 - If TLS is enabled, add the Master Blocking Sensor to the TLS trusted host table.
- On the Master Blocking Sensor, add each Blocking Forwarding Sensor to the allowed hosts table.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-32

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 Transport Layer Security (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:

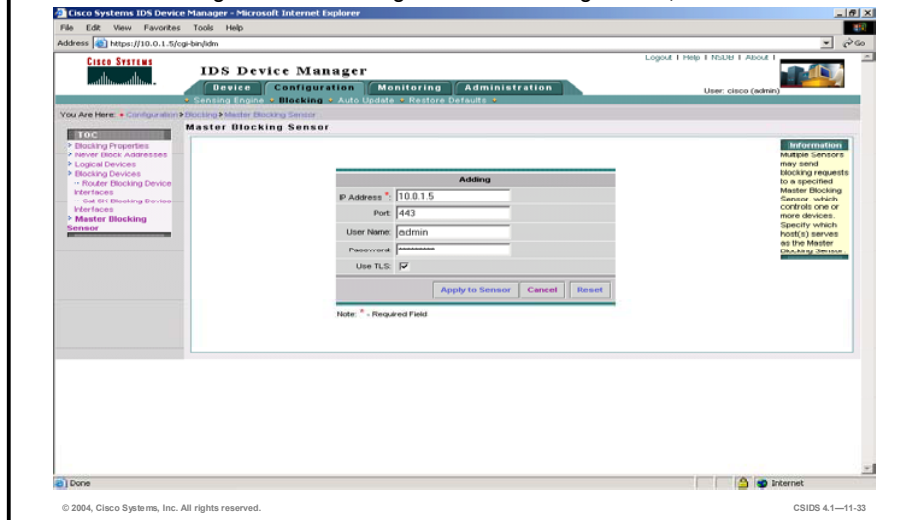
- Define the Master Blocking Sensor. To do this, configure the Master Blocking Sensor IP address, Secure Sockets Layer (SSL) port, TLS setting, username, and password. If you are using the IDS MC, these parameters are automatically retrieved from the device database when the Sensor is selected from the device list. If you are 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 automatically 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 > Blocking > Master Blocking Sensor, and select Add.



Complete the following steps in the IDM on a Blocking Forwarding Sensor to add the Sensor IP addresses that will act as Master Blocking Sensors:

- Step 1** Choose **Configuration > Blocking**. The Blocking page is displayed.
- Step 2** Choose **Master Blocking Sensors** from the TOC. The Master Blocking Sensor page is displayed.
- Step 3** Click **Add**. The Master Blocking Sensor Adding page is displayed.

Note Only an IDS 4.x Sensor can be a Master Blocking Sensor for another IDS 4.x Sensor.

- Step 4** Enter the IP address of the Master Blocking Sensor in the IP Address field.
- Step 5** Enter the communications port number to be used in the Port field.
- Step 6** Enter the user name to be used for communication in the User Name field.
- Step 7** Enter the password for the master blocking sensor in the password field.
- Step 8** Select the Use TLS check box to enable TLS for communications with the master blocking sensor.
- Step 9** Select **Apply to Sensor**. The Master Blocking Sensor page is displayed with the new entry.

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco.com

- **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 antispoofing mechanism.**
 - **Identify critical hosts and network entry points.**
 - **Select applicable signatures.**
 - **Determine the blocking duration.**
- **Sensors can serve as master blocking sensors.**
- **The ACLs may be applied on either the external or internal interface of the Cisco IOS device and may be configured for inbound or outbound traffic on either interface.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—11-35

Cisco Intrusion Detection System Maintenance

Overview

This lesson explains how to perform maintenance on a Cisco Intrusion Detection System (IDS) appliance Sensor or a Cisco Catalyst 6500 Series IDS Module 2 (IDSM-2).

This lesson includes the following topics:

- Objectives
- Service pack and signature updates
- Image recovery
- Resetting, powering down, and restoring the default configuration
- Time settings
- Summary
- Lab exercise

Objectives

This topic lists this lesson's objectives.

Objectives

Cisco.com

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

- **Explain the naming convention for IDS software update files.**
- **Install IDS signature updates and service packs.**
- **Recover the Sensor application partition.**
- **Restore the Sensor default configuration.**
- **Configure the Time Settings on the sensor via IDM.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—12-3

Service Pack and Signature Updates

This topic explains how to install service pack and signature updates via the command line interface (CLI) and IDS Device Manager (IDM).

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.**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—12-5

New attacks that pose a threat to networks are discovered every day. Cisco Systems periodically releases signature updates to enable the Sensor to detect these attacks. Cisco also releases service packs to improve the Sensor's intrusion detection capabilities.

Service pack and signature updates can be installed from the supported management consoles or from the CLI. Updates can also be uninstalled if necessary.

Software Update Guidelines

Cisco.com

The following are guidelines for installing IDS software updates:

- Read the release notes to determine whether the Sensor meets the requirements.
- Download the correct update for the Sensor appliance, IDSM, IDSM-2, or NM-CIDS.
- Use one of the following to update the Sensor:
 - IDM
 - IDS MC
 - CLI

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—12-6

The following are guidelines for 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 when the update is installed.
- Download the correct updates for the Sensor appliance, IDSM-2, or IDS Network Module (NM-CIDS) to an FTP, SCP, HTTP, or HTTPS server on your network. It is strongly recommended that you download and apply all service pack updates, in order and without exception, as they become available.
- Use one of the following to update the Sensor:
 - IDM
 - Management Center for IDS Sensors (IDS MC)
 - CLI

You can find the IDS Event Viewer (IEV), signature updates, service pack updates, BIOS upgrades, readme files, and other IDS Software Version 4.x 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 approximately every two weeks, and service packs are made available 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 e-mail messages when signature updates and service pack updates occur.

Go to the following URL to receive notification about signature updates:

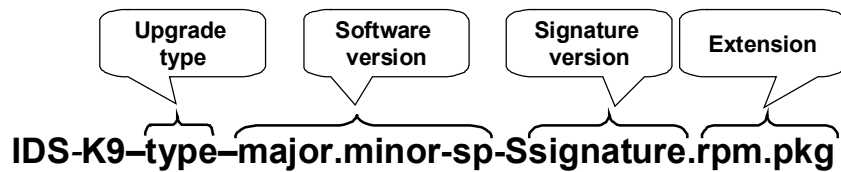
http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html

If for some reason the Sensor is unusable after installing a signature update or service pack, see the Image Recovery topic of this lesson for more information.

Note Review the release notes for every update to ascertain the sequence in which updates should be applied.

IDS Files

Cisco.com



Example: IDS-sig-4.1-3-S64.rpm.pkg

Example: IDS-K9-sp-4.1-3-S61.rpm.pkg

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—12-7

A Cisco IDS software filename has the following parts:

- Upgrade type—There are four upgrade types. All types (major version upgrades, minor version upgrades, service packs, and signature updates) are the same for all 4.x Sensors.
 - maj—Major software release
 - min—Minor upgrade
 - sp—Service pack
 - sig—Signature update
- Software version—The software version consists of numeric values representing the major release, the minor upgrade, and the service pack. The major release number and minor upgrade number are separated by a decimal. The minor upgrade number and the service pack number are separated by a hyphen.
- Signature version—The signature version is a numerical value representing the signature update.
- Extension—The filename extension is rpm.pkg.

Note The software update files used by the IDS MC are compressed (.zip) files. The IDS MC works with these compressed files directly; therefore, you should not unzip them or extract anything from them.

upgrade Command

Cisco.com

```
sensor(config)#upgrade source-url
```

- Applies a service pack, signature update, or image upgrade from an FTP, SCP, HTTP, or HTTPS server

```
sensor(config)#upgrade  
ftp://administator@10.0.1.12/IDS-K9-sp-4.1-  
3-S61.rpm.pkg
```

- Upgrades the Sensor to Service Pack 3 for IDS Software Version 4.1

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—12-8

An IDS software update can be installed by executing the **upgrade** command from the configuration prompt of the Sensor. You can enter all necessary file location (URL) information and the username in one command line entry.

Use the following guidelines when specifying the location of the update file:

- FTP—Source URL for File Transfer Protocol network server. The syntax for this prefix can be one of the following:
 - ftp:[[/username@]location]/relativeDirectory/filename
 - ftp:[[/username@]location]//absoluteDirectory/filename
- SCP—Source URL for the Secure Copy Protocol network server. The syntax for this prefix can be one of the following:
 - scp:[[/username@]location]/relativeDirectory/filename
 - scp:[[/username@]location]//absoluteDirectory/filename
- HTTP—Source URL for the web server. The syntax for this prefix is http:[[/username@]location]/directory/filename.
- HTTPS—Source URL for the web server. The syntax for this prefix is https:[[/username@]location]/directory/filename.

Note If you plan to use HTTPS for installing the update, you must first use the **tls trusted-host** command to set up a Transport Layer Security (TLS) trusted host.

The **downgrade** command can be used to remove the most recent upgrade or update from the Sensor. The following is an example of the use of the **downgrade** command:

```
sensor (config) #downgrade
```

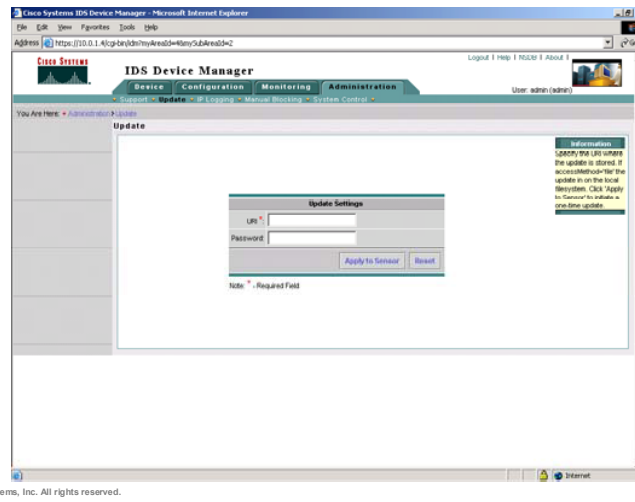
Warning: Executing this command will reboot the system and downgrade to IDS-K9-sp-4.1-1-S47.rpm. Configuration changes made since the last upgrade will be lost and the system may be rebooted.

Continue with downgrade?: **yes**

Using IDM to Install an Update

Cisco.com

Choose Administration > Update.



You can also use the Update page in IDM to apply service pack and signature updates. Complete the following steps to immediately apply a service pack or signature update to the Sensor:

- Step 1** Download the service pack or signature update from Cisco.com to your FTP, SCP, HTTP, or HTTPS server.
- Step 2** From IDM, select **Administration > Update**. The Update page is displayed.
- Step 3** In the URL field, enter the URL where the update can be found. The following URL types are supported:
 - FTP—Source URL for File Transfer Protocol network server. The syntax for this prefix can be one of the following:
 - ftp://username@location/relativeDirectory/filename
 - ftp://username@location/absoluteDirectory/filename
 - SCP—Source URL for the Secure Copy Protocol network server. The syntax for this prefix can be one of the following:
 - scp://username@]location/relativeDirectory/filename
 - scp://username@location/absoluteDirectory/filename
 - HTTP—Source URL for web server. The syntax for this prefix is http://username@location/directory/filename.
 - HTTPS—Source URL for the web server. The syntax for this prefix is https://username@location/directory/filename.

Note If you plan to use HTTPS, use the **tls trusted-host** command to set up a TLS trusted host.

- Step 4** In the Password field, enter the password for the transport protocol you are using.

Step 5 Click **Apply to Sensor** to apply the update. The Sensor applications are stopped while the update is applied. If you are applying a service pack, the installer automatically reboots the Sensor.

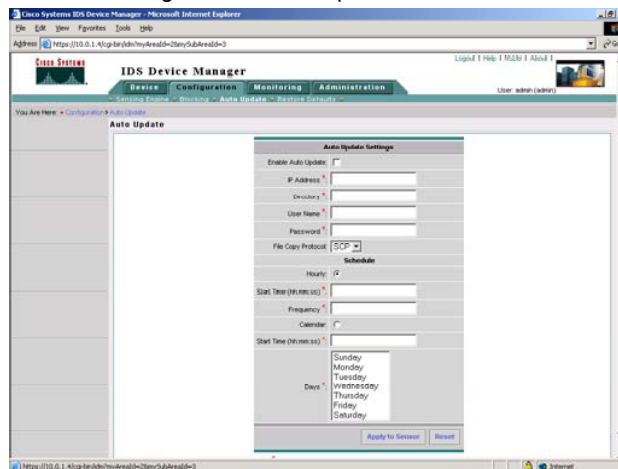
Note This procedure does not apply to updating service packs and signatures via the IDS MC. When using the IDS MC, the update file must reside on the IDS MC at X:\Program Files\CSCOp\MDC\etc\IDS\Updates, where X: is the default drive where the IDS MC is installed.

Note When you use the IDS MC to update a Sensor, you must also update the IDS MC for it to be able to understand the software installed on the Sensor.

Configuring Automatic Updates

Cisco.com

Choose Configuration > Auto Update.



You can configure automatic service pack and signature updates, so that when a service pack or signature update is loaded on a central FTP or SCP server, it is automatically downloaded and applied to your Sensor. The Sensor cannot automatically download service pack and signature updates from Cisco.com. You must download service pack or signature updates from Cisco.com to an FTP or SCP server and then configure the Sensor to download them from the FTP or SCP server.

Note After you download an update from Cisco.com, verify the integrity of the downloaded file.

Complete the following steps to configure automatic updates:

- Step 1** Select **Configuration > Auto Update**. The Auto Update page is displayed.
- Step 2** Select the **Enable Auto Update** check box to enable automatic updates.
- Step 3** Enter the IP address of the server to poll for updates in the IP Address field.
- Step 4** In the Directory field, enter the path to the directory on the server where the updates are located. The path can be up to 128 characters in length.
- Step 5** In the Username field, enter the username to use when logging in to the server. The username can be up to 16 characters in length.
- Step 6** In the Password field, enter the username password. The password can be up to 16 characters in length.
- Step 7** From the File Copy Protocol list box, select either **SCP** or **FTP**.
- Step 8** For hourly updates, select **Hourly**, and complete the following substeps:
 1. In the Start Time field, enter the time you want the updates to start. Use the format hh:mm:ss.

2. In the Frequency field, enter the hour interval at which you want every update to occur. You can enter a value from 1 to 8760. For example, if you enter 5, the Sensor looks at the directory of files on the server every 5 hours. If there is an available update file, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available files.

Step 9 For calendar updates, select **Calendar**, and complete the following steps:

1. In the Start Time field, enter the time you want the updates to start. Use the format hh:mm:ss.
2. In the Day field, select the day or days on which you want to download updates.

Step 10 Click **Apply to Sensor** to save your changes.

Note To reset the form, click **Reset**.

Image Recovery

This topic explains how to recover the Sensor's software image if it becomes corrupted.

Image Recovery Overview

Cisco.com

- **The Sensor appliance has two partitions: the application partition and the recovery partition.**
- **You can recover the application partition image from the image stored on the recovery partition.**
- **You should back up your configuration before recovering the application partition.**
- **Recovery procedures for the Sensor appliance differ from the recovery procedures for the IDSM-2 and the NM-CIDS.**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—12-12

The Sensor appliance has two partitions, the application partition and the recovery partition. The recovery partition can be used to recover the Sensor's software image if it becomes corrupted. However, you should back up the current configuration before initiating a recovery due to the following effects of recovery on the Sensor:

- The cisco account password is set back to the default (cisco).
- All user accounts except for the cisco account are removed.
- All IDS settings, such as signatures and filters, are set to the default.
- All iplogs, alerts, error messages, and status messages are cleared.

After you reimage the Sensor, you must initialize it again using the **setup** command. You must also upgrade your Sensor with the most recent signature updates and service packs and reassign the interfaces.

Image Recovery

Cisco.com

```
sensor(config)# recover application-partition
```

- Reimages 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
4.1(1)S47. All configuration changes except for
network settings will be reset to default.
Continue with recovery?:yes
Request Succeeded
sensor(config)#
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—12-13

To reimage the Sensor's application partition via the recovery partition, use the **recover application-partition** command from the CLI. After the recovery, reinstall any service pack and signature updates you have applied. This process is necessary because service pack and signature updates are not applied to the recovery partition when you apply them to the Sensor.

Upgrading the Recovery Partition

Cisco.com

- A recovery partition image file is available for every major and minor release of the IDS Software Version 4.x.
- The recovery partition image file is the only upgrade available for the recovery partition.
- It is a good idea to keep your recovery partition up to date with the latest recovery partition image so that it is ready if you need to recover the application partition on your Sensor.
- You can use the **upgrade** command to install the recovery partition image.

© 2004, Cisco Systems, Inc. All rights reserved.

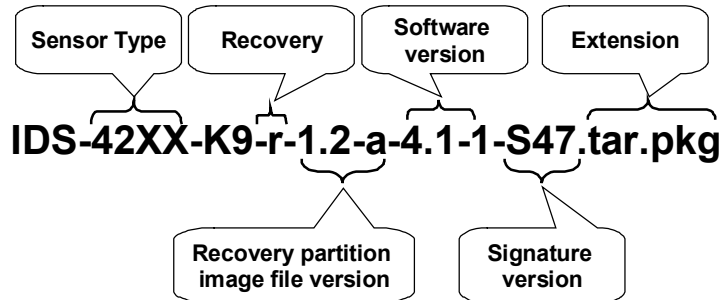
CSIDS 4.1—12-14

For every major and minor release of the IDS Software Version 4.x, a recovery partition image file is created and posted to Cisco.com. This recovery partition image file is the only upgrade available for the recovery partition. It is a good idea to keep your recovery partition up to date with the latest recovery partition image file so that it is ready if you need to recover the application partition on your Sensor. To upgrade the recovery partition, download the recovery partition image file from the Software Center on Cisco.com to an SCP or FTP server. Then use the **upgrade** command to install the package.

Note If you boot to the recovery partition during Sensor bootup, an automatic recovery is initiated.

Recovery Partition Image File Example

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

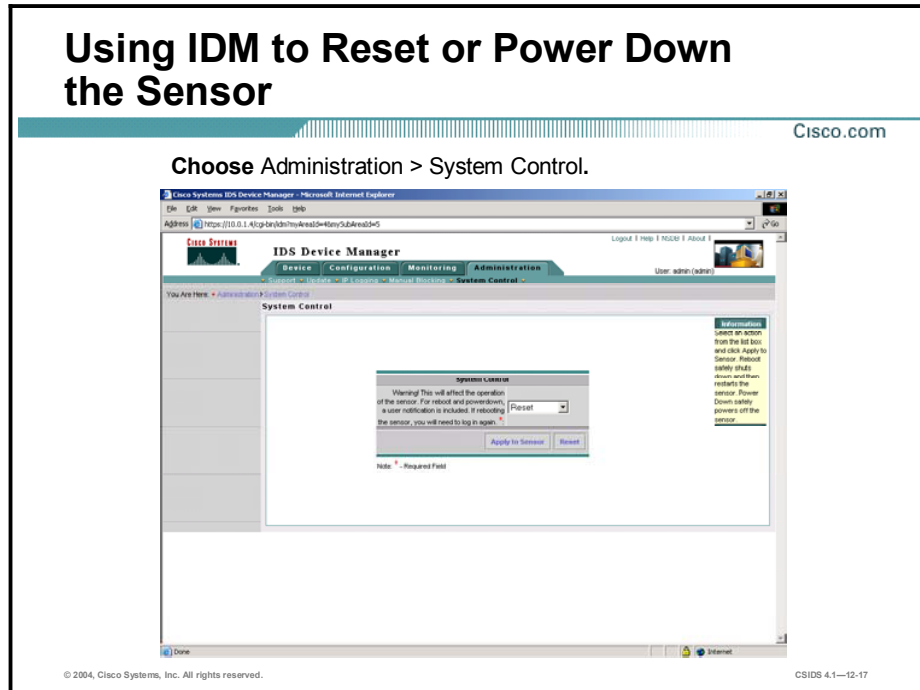
CSIDS 4.1—12-15

The figure shows an example of a recovery partition image file for a Sensor appliance. Recovery files are unique for each platform and look completely different for an IDSM-2 or NM-CIDS. The image file in the figure applies to all Cisco IDS 4200 Series Sensor Appliances except the Cisco IDS 4215. The following is an example of a recovery partition image file for a Cisco IDS 4215 Sensor:

IDS-5215-K9-r-1.1-a-4.1-1-S47.tar.pkg

Resetting, Powering Down, and Restoring the Default Configuration

This topic explains how to reset, power down, and restore the default configuration to your Sensor.



From the System Control page, you can reset the Sensor or put it in a state where it is safe to power down. Reset shuts down the Sensor safely and then restarts it. Power Down safely shuts down the Sensor to a point where it is safe to power the unit off.

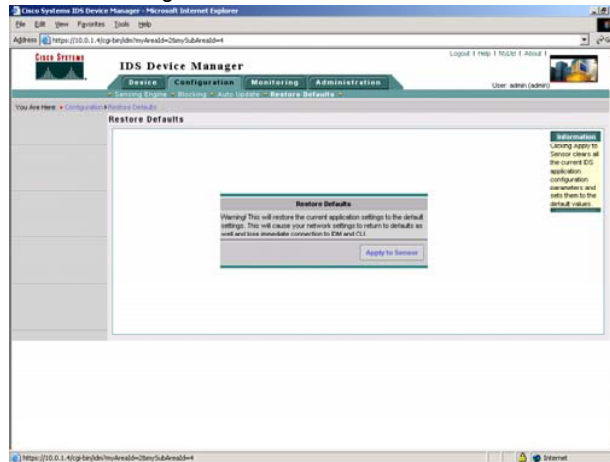
Complete the following steps to reset or power down the Sensor:

- Step 1** Select **Administration > System Control**. The System Control page is displayed.
- Step 2** Select one of the following options from the drop-down menu:
 - **Reset**—Shuts down the IDS applications and the Sensor, and then reboots. After the reboot, you must log in. There is a 30-second delay during which users who are logged in to the CLI are notified that the IDS applications and Sensor are going to shut down.
 - **Power Down**—Shuts down the IDS applications and then puts the Sensor in a state in which it is safe to power it off. There is a 30-second delay during which users who are logged in to the CLI are notified that the IDS applications and the Sensor are going to shut down.

Using IDM to Restore the Default Configuration

Cisco.com

Choose Configuration > Restore Defaults.



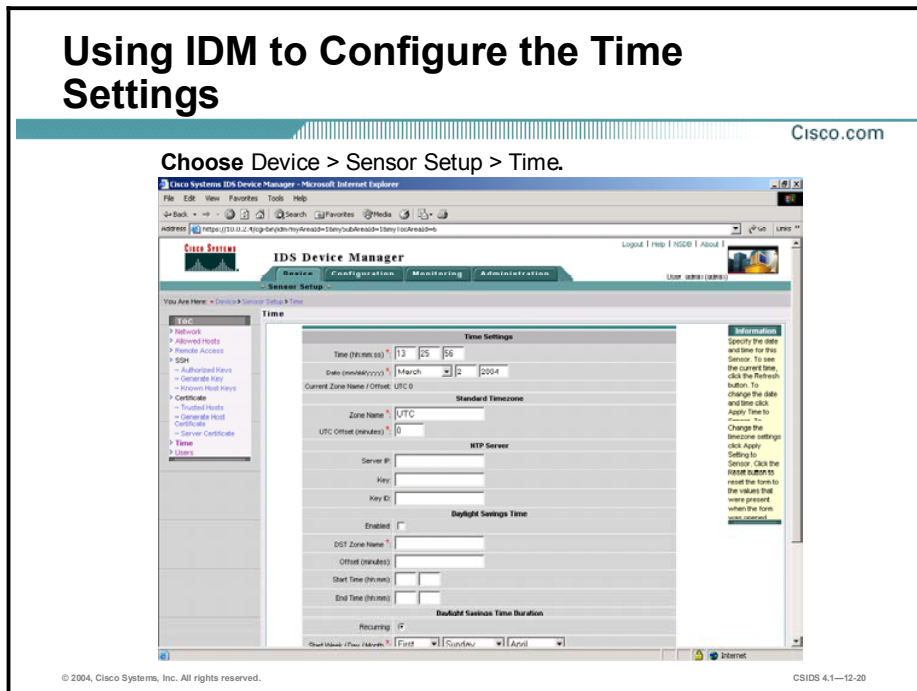
You can restore the default configuration to your Sensor. Restoring the default configuration removes the current application settings and restores the default settings. Your network settings also return to the defaults, and you immediately lose connection to IDM and the CLI. To restore the default configuration, complete the following steps:

- Step 1** Select **Device > Configuration > Restore Defaults**. The Restore Defaults page is displayed.
- Step 2** Click **Apply to Sensor** to restore the default configuration.

Note Restoring the default configuration does not restore usernames, passwords, or time settings.

Time Settings

This topic explains how to configure the time settings on your Sensor:



You can define the time, time zone, and daylight savings time (DST) for the Sensor.

Complete the following steps to set the time on the Sensor using IDM:

- Step 1** Choose **Device > Sensor Setup > Time**. The Time page is displayed.
- Step 2** In the Time field under Time Settings, enter the **current time (hh:mm:ss)**.

Note Time indicates the time on the local host. To see the current time, click **Refresh**.

Note If you accidentally specify the incorrect time, stored events will have the wrong time stamp. You must clear the events.

- Step 3** In the Date field under Time Settings, enter the **current date (mm:dd:yyyy)**.

Note Date indicates the date on the local host.

- Step 4** In the Zone Name field under Standard Timezone, enter the **local time zone** to be displayed when summer time is not in effect. The default value is UTC.

- Step 5** In the UTC Offset field under Standard Timezone, enter the **offset in minutes** from UTC (mm). The default value is 0.

Step 6 If you are using an NTP server to set the Sensor time, enter the **NTP server's IP address** in the NTP Server Server IP field.

Step 7 In the NTP Server Key field, enter the **NTP server's key value**.

Step 8 In the NTP Server Key ID field, enter the **NTP server's key ID** value: 1 to 4294967295.

Note If you define an NTP server, the Sensor time is set by the NTP server. The CLI clock set command will produce an error, but time zone and daylight saving time parameters are valid.

Step 9 Select **Enabled** under Daylight Savings Time to enable daylight savings time. The default is Off.

Step 10 In the DST Zone Name field, enter the **name of the zone**, text 1 to 32 characters, to be displayed when summer time is in effect.

Step 11 In the Offset field, enter the **number of minutes to add during the summer time (mm)**. The default is 60 minutes.

Step 12 In the Start Time field, enter the **time (hh:mm)** to apply the DST setting. The default is 02:00.

Step 13 In the Stop Time field, enter the **time (hh:mm)** to remove the DST setting. The default is 02:00.

Using IDM to Configure the Time Settings (Cont.)

Cisco.com

Choose Device > Sensor Setup > Time.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—12-21

- Step 14** Select the **Recurring** radio button under Daylight Savings Time Duration to indicate that summer time should start and end on the specified days every year. The default is Off.
- Step 15** In the Start Week/Day/Month field under Daylight Savings Time Duration enter the **week (1-5, last), day (Sunday-Saturday), and month (January-December)** of the year to apply the DST. The default is 1, Sunday, April.
- Step 16** In the End Week/Day/Month field under Daylight Savings Time Duration enter the **week (1-5, last), day (Sunday-Saturday), and month (January-December)** of the year to remove DST. The default is last, Sunday, October.
- Step 17** Select the **Date** radio button under Daylight Savings Time Duration to indicate that summer time should start on a specific date.
- Step 18** In the Start field enter the **month, date, and year (mm:hh:yyyy)** to start DST.
- Step 19** In the End field enter the **month, date, and year (mm:hh:yyyy)** to stop DST.

Note To reset the form, click **Reset**.

- Step 20** Click **Apply to Sensor** to save the settings.

The EventStore time stamp is always based on UTC time. If during the original Sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the Sensor to use central time with daylight savings time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error and the clock displays 21:00:23 CDT. You then change the

time to 9:00 a.m. Now, the clock displays 09:01:33 CDT. Because the offset from UTC has not changed, it requires the UTC time to be 14:01:33 UTC, which creates the time-stamp problem.

To ensure the integrity of the time stamp in the event records, you must clear older events from the event archive. Use the **clear events** command. See *Cisco Intrusion Detection System Command Reference Version 4.1* for more information on the **clear events** command.

Note You cannot clear individual events.

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **You can use any of the following to install service pack and signature updates on your Sensor:**
 - CLI
 - IDM
 - IDS MC
- **To install service pack and signature updates via the CLI or IDM, you must first download the correct update file to an FTP, SCP, HTTP, or HTTPS server on your network.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1–12-23

Summary (Cont.)

Cisco.com

- To install service pack and signature updates via the IDS MC, the update file must reside on the IDS MC.
- You can use either IDM or the IDS MC to configure automatic service pack and signature updates. This enables the software to be automatically applied to your Sensor after you download it to a central FTP or SCP server.
- The Sensor recovery partition can be used to recover the Sensor software image if it becomes corrupted. The recovery can be performed via the CLI.
- You can use IDM to restore the default configuration to your Sensor.
- You can use IDM to set the Sensor Time Settings.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—12-24

Enterprise Intrusion Detection System Management

Overview

This lesson 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 lesson:

- Objectives
- Introduction
- Windows installation
- Solaris installation
- Architecture
- Getting started with the IDS MC
- Sensors and Sensor groups
- Using the IDS MC to configure the Sensor
- IDS MC workflow
- Updating the IDS MC
- Reporting
- Summary
- Lab exercise

Objectives

This topic lists the lesson objectives.

Objectives

Cisco.com

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

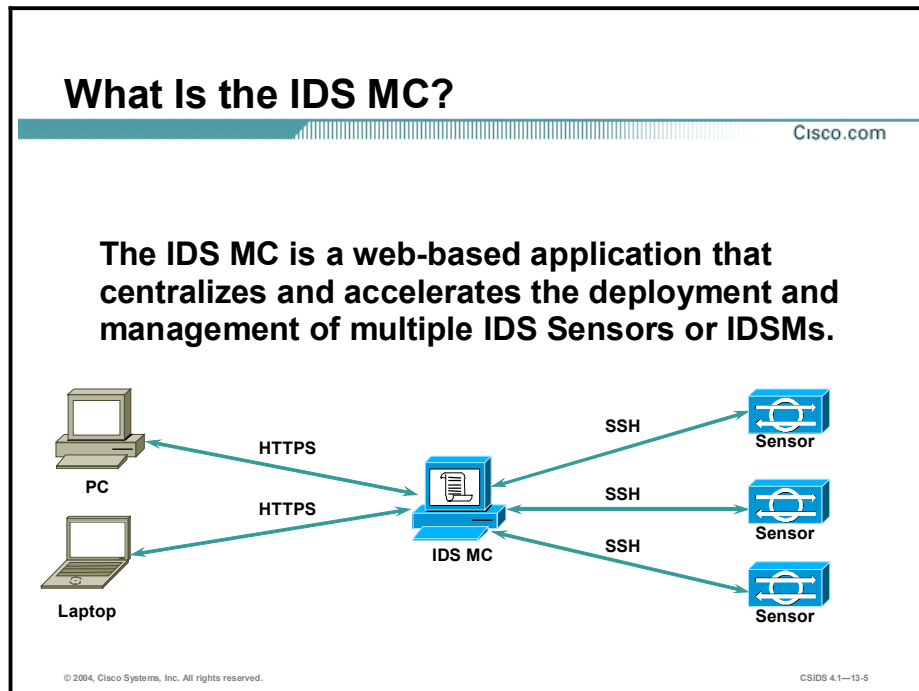
- **Define features and key concepts of the IDS MC.**
- **Describe the IDS MC architecture.**
- **Install the IDS MC.**
- **Locate the directories in which the IDS MC and its components are installed.**
- **Add Sensors and Sensor groups to the IDS MC.**
- **Use the IDS MC to tune signatures.**
- **Deploy configuration files.**
- **Update the IDS MC.**
- **Generate and view reports.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-3

Introduction

This topic introduces the IDS MC.



IDS MC is a component of the VMS bundle. The VMS bundle integrates the CiscoWorks server with a number of individual applications such as CiscoWorks VPN Monitor, CiscoWorks Management Centers (MCs), and the CiscoWorks 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.

You can access and manage your Sensor from a server running the IDS MC or you can manage the Sensor from a client computer connected to the IDS MC server. The figure illustrates communications between the client and the IDS MC and between the IDS MC and the Sensor. The following protocols are used:

- HTTPS—For communication with the monitoring application
- Secure Shell (SSH) Protocol—For network access to the Sensor

IDS MC Features

Cisco.com

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**
 - **IDS running Version 3.0(5) S23 or later**
 - **IDS-2 running Version 4.0 or higher**
 - **NM-CIDS running Version 4.1 or higher**
 - **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**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-6

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:

Type of Device	Devices Supported	Software
Cisco Network IDS Sensor Appliances	NRS-2E	IDS 3.0 and IDS 3.1
	NRS-2FE	IDS 3.0 and IDS 3.1
	NRS-TR	IDS 3.0 and IDS 3.1
	NRS-SFDDI	IDS 3.0 and IDS 3.1
	NRS-DFDDI	IDS 3.0 and IDS 3.1
	IDS-4210	IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
	IDS-4215	IDS 4.1
	IDS-4220	IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
	IDS-4230	IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
	IDS-4235	IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
	IDS-4250-TX and IDS-4250-SX	IDS 3.0, IDS 3.1, IDS 4.0, and IDS 4.1
IDS-4250-XL	IDS 4.0 and IDS 4.1	
Cisco Switch IDS Sensor Modules	IDS-M	IDS-M 3.0(5) and IDS-M 3.0(6)
	IDS-M-2	IDS 4.0 and IDS 4.1
Cisco IOS Router IDS Sensor Module	NM-CIDS	IDS 4.1

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 topic explains the server and client 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 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 Professional, Server, or Advanced Server (with Service Pack 3)

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—13-8

Before you begin, verify that 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 Professional, Server, or Advanced Server (with Service Pack 3)

The IDS MC and Security Monitor support only the US English versions of these operating systems. In addition, only the US English Regional Options setting is supported.

You should not install any of the VMS products on a Windows server if it is running Terminal Services or if it plays either of the following roles in your network:

- Primary domain controller
- Backup domain controller

Note Single-processor 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

Cisco.com

- **Hardware**—IBM PC-compatible computer, 300 MHz or faster
- **Memory**
 - 256 MB of RAM minimum
 - 400 MB virtual memory
- **Operating system**
 - Windows 2000 Professional with Service Pack 3
 - Windows 2000 Server with Service Pack 3
 - Windows XP, Service Pack 1 with Microsoft Virtual Machine
- **Browser**
 - Internet Explorer 6.0 with Service Pack 1
 - Netscape Navigator 4.79

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-9

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 2000 Server or Professional with Service Pack 3
 - Windows XP, Service Pack 1 with Microsoft Virtual Machine
- **Browser**
 - Microsoft Internet Explorer Version 6.0, Service Pack 1 for Windows operating systems with Microsoft Virtual Machine
 - Netscape Navigator 4.79

Installation Overview

Cisco.com

- **CiscoWorks Common Services is required for the IDS MC.**
- **CiscoWorks Common Services provides the CiscoWorks Server-based components, software libraries, and software packages developed for the IDS MC.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-10

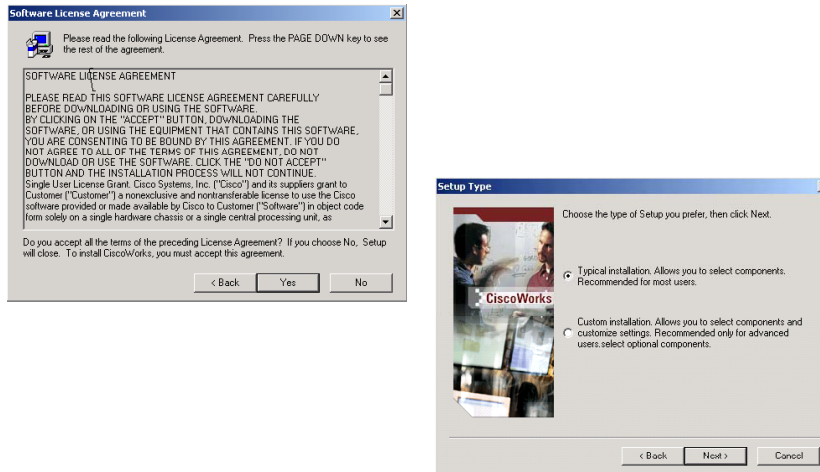
CiscoWorks Common Services, a component of VMS, is required for the IDS MC. CiscoWorks Common Services provides the CiscoWorks2000 Server base components, software libraries, and software packages developed to support the IDS MC.

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) or a backup domain controller (BDC) or if terminal services are running.

Installation Process

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-11

Complete the following steps to install the IDS MC:

Note The typical installation installs both the IDS MC and the Monitoring Center for Security.

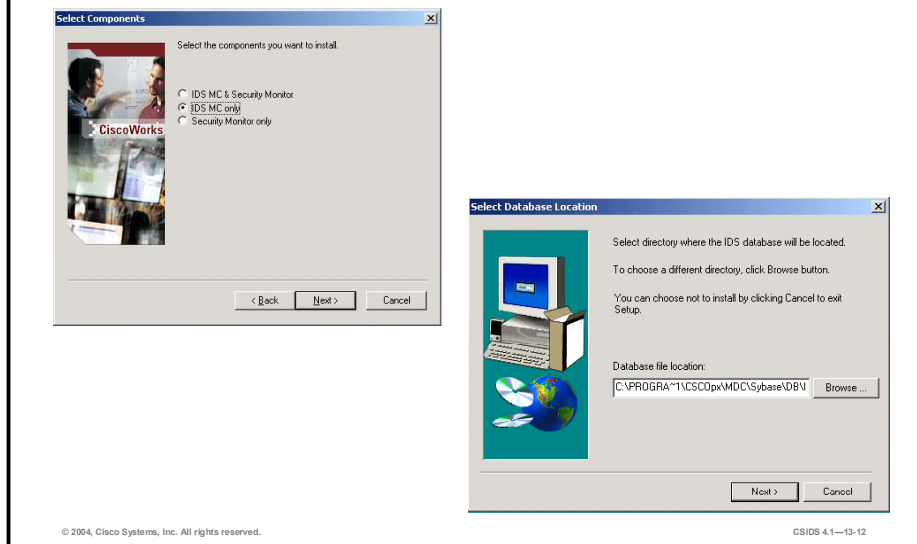
- Step 1** Launch the IDS MC installation. The following message is displayed:
- Do you really want to install IDS MC & Security Monitor?**
- Step 2** Click **Yes**. The Welcome window opens.
- Step 3** Click **Next**. The Software License Agreement window opens.
- Step 4** If you agree to the Software License Agreement, click **Yes** to proceed. The Setup Type window opens.

Note If you click **No**, the installation process stops.

- Step 5** Select **Custom installation** as the installation type and click **Next**. The Select Components window opens.

Installation Process (Cont.)

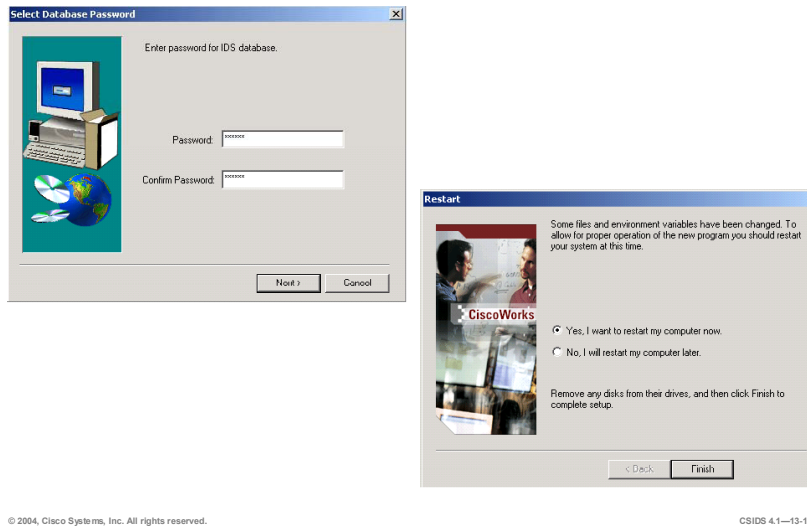
Cisco.com



- Step 6** Select **IDS MC only** and click **Next**. The System Requirements panel is displayed.
- Step 7** Click **Next** after verifying that your system meets the minimum disk space and memory requirements. The Summary window opens.
- Step 8** Click **Next** after verifying the selected settings. The Select Database Location window opens. The default database location is within the directory where the CiscoWorks Common Services is installed.
- Step 9** Click **Next** to accept the default database directory. The Select Database Password window opens.

Installation Process (Cont.)

Cisco.com



Step 10 Enter a password in the Password and Confirm Password fields. This password is used to secure the Sybase SQL database used by the IDS MC to store information about Sensors.

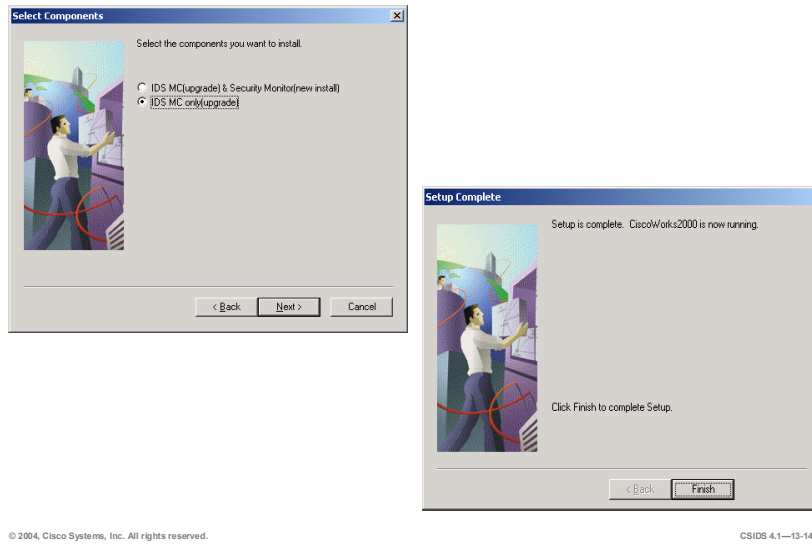
Note The IDS MC database password must be at least 4 characters in length. If you do not enter a password of at least 4 characters in length, you will receive a popup error message that indicates that you must enter a password of the necessary length.

Step 11 Click **Next**.

Step 12 When the installation is complete and the Restart window opens, select **Yes, I want to restart my computer now**, and click **Finish**.

Upgrade Process

Cisco.com



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.

Note 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 System Requirements panel is displayed.
- Step 6** Click **Next**. The Summary page is displayed.
- Step 7** Click **Next**. After the upgrade is complete, the Setup Complete window opens.
- Step 8** Click **Finish**.

Solaris Installation

This topic describes the server and client installation requirements, gives a brief installation overview, and explains the installation process for Solaris-based machines.

Server Requirements—Solaris

Cisco.com

- **Hardware**
 - **Sun UltraSPARC 60 with 440 MHz or faster processor**
 - **Sun UltraSPARC III (Sun Blade 2000 Workstation or Sun Fire 280R Server)**
- **Memory**
 - **1 GB of RAM minimum**
 - **2 GB of virtual memory**
- **System software—Solaris 2.8**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—13-16

Before you begin, verify that the Solaris-based server on which you plan to install the IDS MC meets the following requirements:

- **Hardware**
 - UltraSPARC 60 with 440 MHz or faster processor
 - UltraSPARC III (Sun Blade 2000 Workstation or Sun Fire 280R Workgroup Server)
- **Memory**
 - 1 GB of RAM minimum
 - 2 GB of virtual memory
- **Hard drive space—512 MB of swap space**
- **System software—Solaris 2.8**

Client Access Requirements—Solaris

Cisco.com

- **Hardware—Sun SPARCstation or Ultra 10 with a 333-MHz processor with the Solaris 2.8 operating system**
- **Memory—1 GB of RAM minimum**
- **Swap space—512 MB**
- **Browser—Netscape Navigator 4.76**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-17

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—Sun SPARCstation or Ultra 10 with a 333-MHz processor or better**
- **Operating system**
 - Solaris 2.8
- **Memory**
 - 1 GB of RAM minimum
 - 512 MB of swap space minimum
- **Browser—Netscape Navigator 4.76**

Installation Overview

Cisco.com

- **CiscoWorks Common Services is required for the IDS MC.**
- **CiscoWorks Common Services provides the CiscoWorks Server-based components, software libraries, and software packages developed for the IDS MC.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-18

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 can be installed on a standalone server (without CD One), or integrated into an existing CiscoWorks installation running CD One Edition 5. 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

Cisco.com

```
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.
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-19

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 lesson.

- Step 1** Insert the IDS MC for Solaris CD into the CD-ROM drive.
- Step 2** Log in to 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 can 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....
.
.
.
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-20

- Step 6** Enter **1** and press **Enter**. After making a list of dependencies and performing prerequisite checks, the Software Install Tool prompts you 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 prompts 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 its 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.)

Cisco.com

```
=====  
Finished: Wed Dec 11 17:13:19 CST 2002  
=====
```

```
===== Software Install Tool Completed. =====  
=====
```

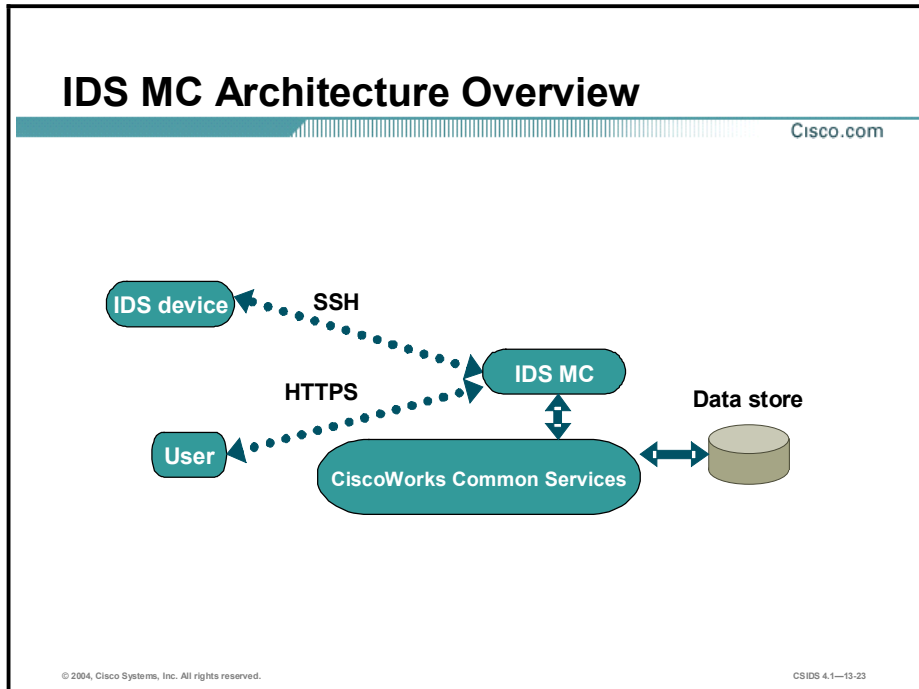
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-21

Step 9 Close the Software Install Tool window after the IDS MC installation is complete.

Architecture

This topic explains the IDS MC architecture, directories, and elements.



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 either coexist with existing CiscoWorks applications or function as a standalone server.

The IDS MC depends on the framework and services provided by CiscoWorks Common Services. CiscoWorks Common Services comprises the following components:

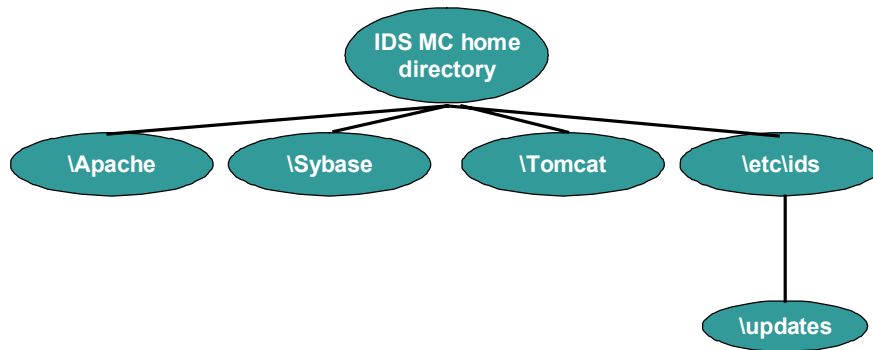
- Data storage and management—The data store is contained within a Sybase SQL Anywhere database. CiscoWorks Common Services provides management for this data to enable data backups and restores. Additionally, CiscoWorks Common Services provides functionality to enable automatic repairs of the database 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—This component 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—This component 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—This component enables abstraction of services by any and all management consoles installed on the server. It 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 points 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



© 2004, Cisco Systems, Inc. All rights reserved.

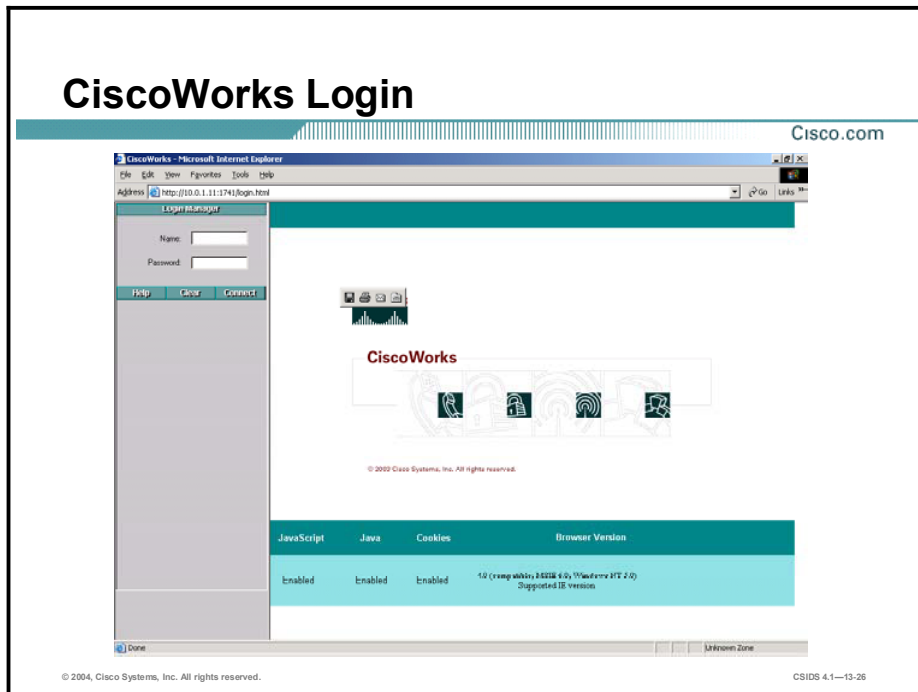
CSIDS 4.1—13-24

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—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 subdirectories.
 - 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 about 4.x Sensors is stored 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.

Getting Started with the IDS MC

This topic explains how authorization roles in CiscoWorks enable the delegation of tasks and how to log in to the IDS MC.



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 IP address of the CiscoWorks server is 10.0.1.11. Enter the following web address in the browser address field:

`http://10.0.1.11:1741`

- Step 2** Use the default administrative account, **admin**, with the password you configured during installation to log in to CiscoWorks.

CiscoWorks User Authorization Roles

Cisco.com

CiscoWorks user authorization roles allow for different privileges within the IDS MC:

- **Help Desk—Read-only privileges for the entire system.**
- **Approver—Read-only privileges for the rest of the system, and ability to approve configurations.**
- **Network Operator—Read-only privileges for the rest of the system, and ability to deploy configurations.**
- **Network Administrator—Read-only privileges for the rest of the system, and ability to edit devices and device groups.**
- **System Administrator—All operations may be performed by the system administrator.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-27

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 approve configurations. The five types of user authorization roles are as follows:

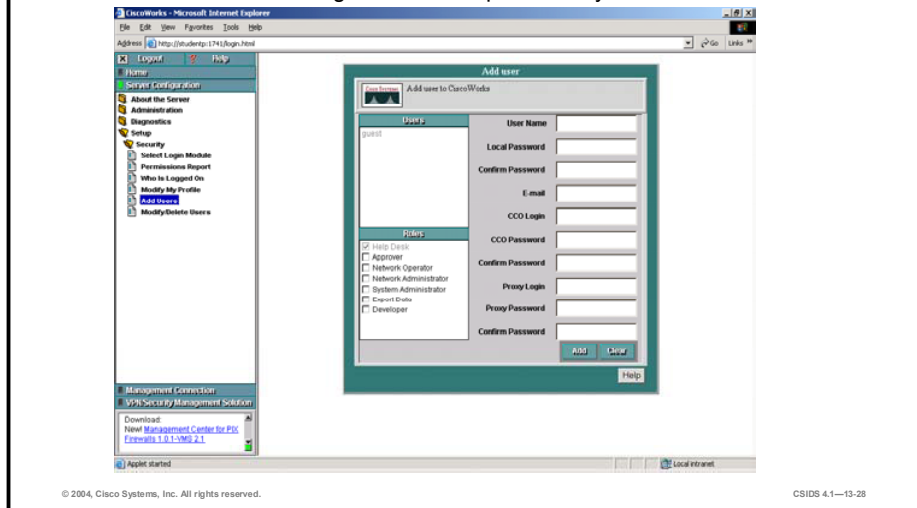
- **Help Desk—Read-only privileges for the entire system**
- **Approver—Read-only privileges for the entire system; includes approval privileges for configuration changes**
- **Network Operator—Read-only privileges for the entire system; includes privileges for generating reports and deploying configurations**
- **Network Administrator—Read-only privileges for the entire system; includes privileges for editing devices and device groups**
- **System Administrator—Capable of performing all operations**

Note Users can be assigned multiple authorization roles.

CiscoWorks Add User

Cisco.com

Choose **Server Configuration > Setup > Security > Add Users.**



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:

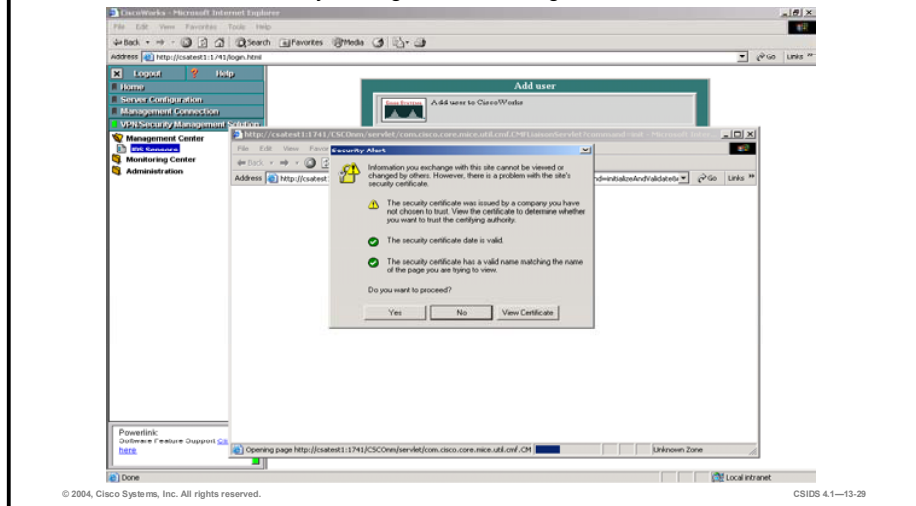
CiscoWorks Add User Settings	Description
User Name	User name to add.
Local Password	Password.
Confirm Password	Password confirmation.
E-mail	(Optional.) User's e-mail address.
CCO Login	(Optional.) User's Cisco.com login.
CCO Password	(Optional.) User's Cisco.com password.
Confirm Password	(Optional.) User's Cisco.com 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 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

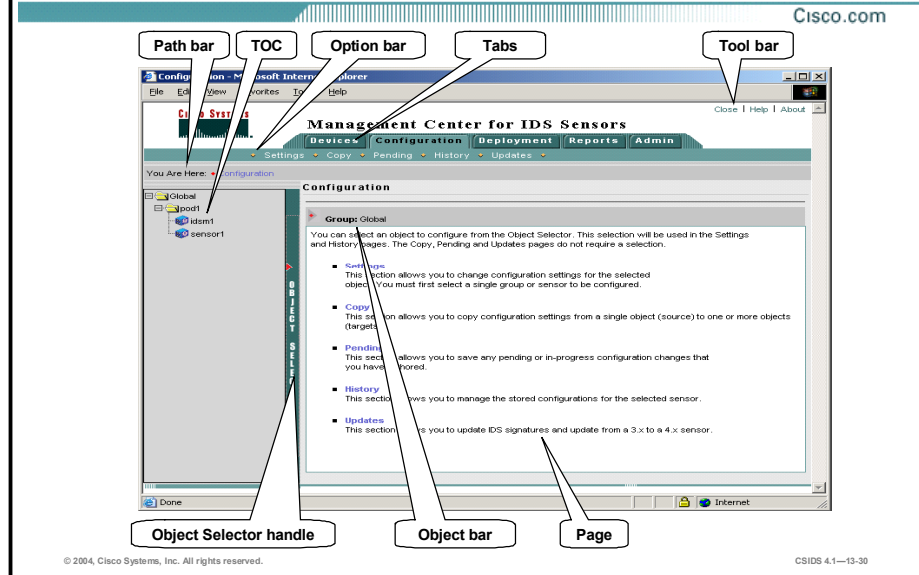
Choose VPN/Security Management > Management Center > IDS Sensors.



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 **IDS Sensors** to launch the IDS MC. The IDS MC launches in a new window.

Understanding the IDS MC Interface



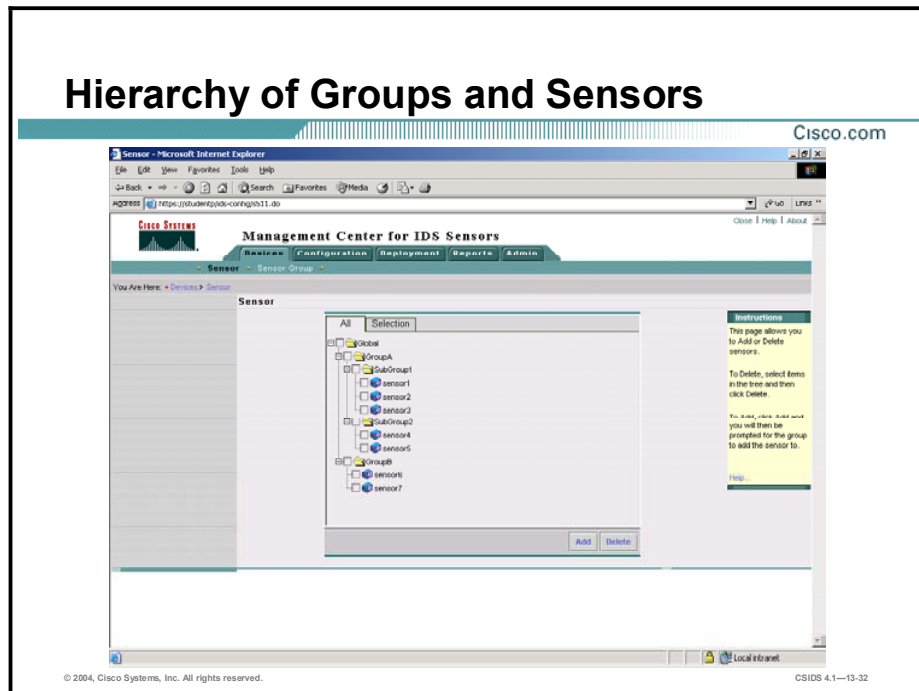
The figure illustrates elements of the IDS MC GUI. The elements are described as follows:

- **Path bar**—Provides a context for the displayed page. Shows the tabs, options, and current page.
- **TOC**—Displays the available suboptions, if required.
- **Option bar**—Displays the options available for the selected tab.
- **Tabs**—Provide 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 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.
- **Tool bar**—Contains the following options:
 - **Close**—Enables you to close the IDS MC.
 - **Help**—Provides information about the current page.
 - **About**—Provides information about the IDS MC version and copyright.
- **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. Most of the tasks for

configuring Sensors and signature settings require you to use the Object Selector to select a Sensor or Sensor group to configure.

Sensors and Sensor Groups

This topic explains adding Sensors and creating Sensor groups within the IDS MC.



The IDS MC uses the concept of groups to enable you to configure an entire group of Sensors simultaneously. A group can contain Sensors, other groups, or a combination of Sensors and groups. You can create a hierarchy that contains many levels of groups and Sensors just as a folder in Windows 2000 can contain many levels of folders and files. The hierarchy you create appears in the Object Selector, which is used to select groups or devices for configuration. The figure shows an example of an IDS MC hierarchy.

Configuring more than one Sensor at a time is possible because a Sensor can inherit settings from its parent group. By default, settings applied to a group are inherited by subgroups and devices within that group. You can, however, enable child settings to override the default settings of a parent group.

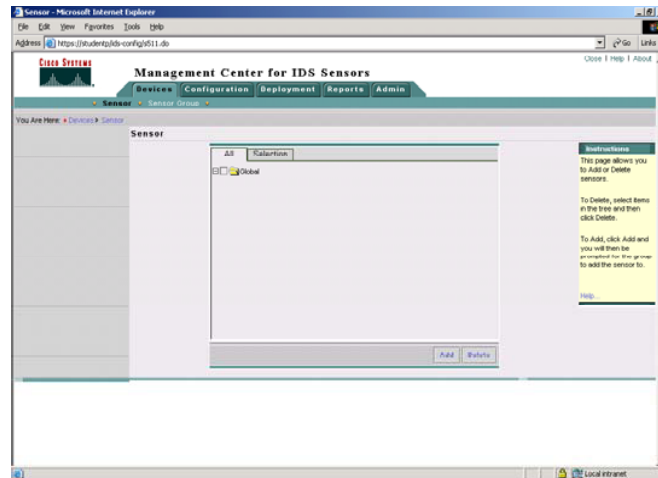
A Sensor must inherit settings from its parent group if a parent defines those settings as mandatory. When you configure a setting as mandatory, you ensure that the setting is inherited by all enclosed subgroups and devices and cannot be overridden by a subgroup or device.

Note The IDS MC has one default group, the Global group.

Adding a Sensor

Cisco.com

Choose Devices > Sensor.



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-33

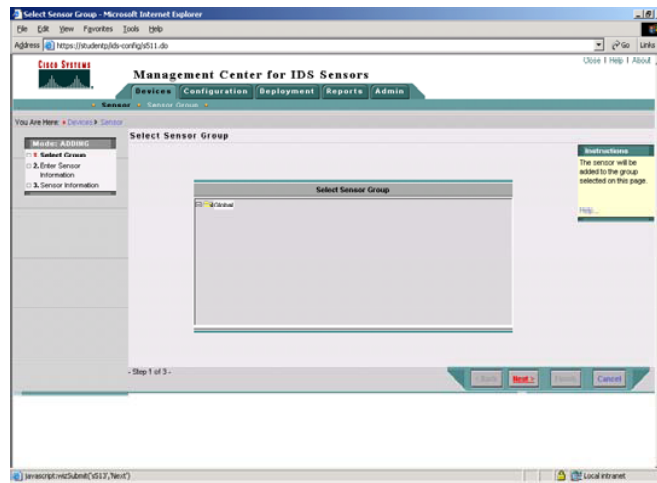
Complete the following steps to add a Sensor to the IDS MC:

Step 1 Choose **Devices > Sensor**. The Sensor page is displayed.

Step 2 Click **Add**. The Select Sensor Group page is displayed.

Adding a Sensor (Cont.)

Cisco.com

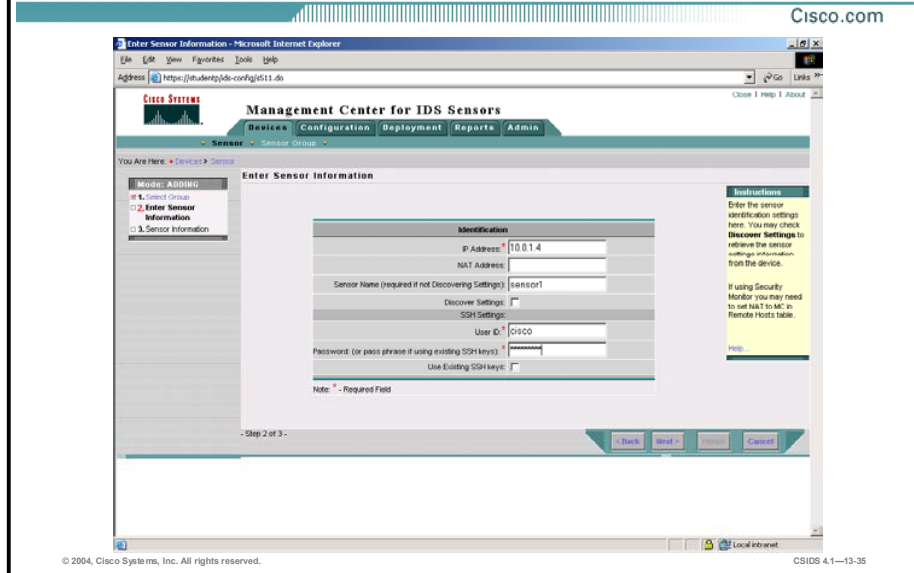


© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-34

Step 3 Select a group and click **Next**. The Enter Sensor Information page is displayed.

Adding a Sensor (Cont.)

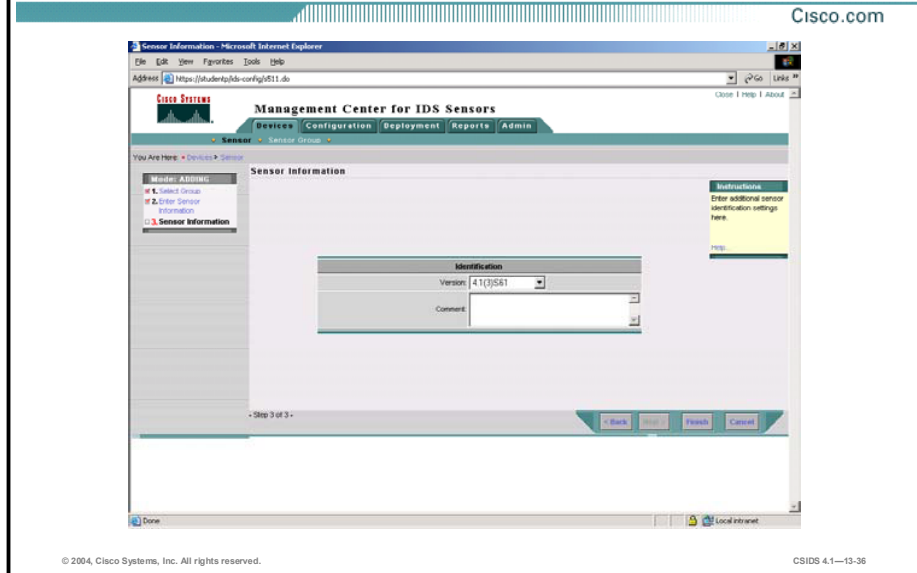


Step 4 Enter values for settings listed in the following table:

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 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 name of the user who will manage the Sensor.
Password	Enter the User ID password or passphrase if you are using existing SSH keys.
Use Existing Systems SSH Keys	(Optional.) Select this check box to use the existing SSH keys.

Step 5 Click **Next**. The Sensor Information page is displayed.

Adding a Sensor (Cont.)



Step 6 Select the version of software that the Sensor is running from the drop-down menu.

Step 7 (Optional.) Enter notes about the Sensor in the Comment field.

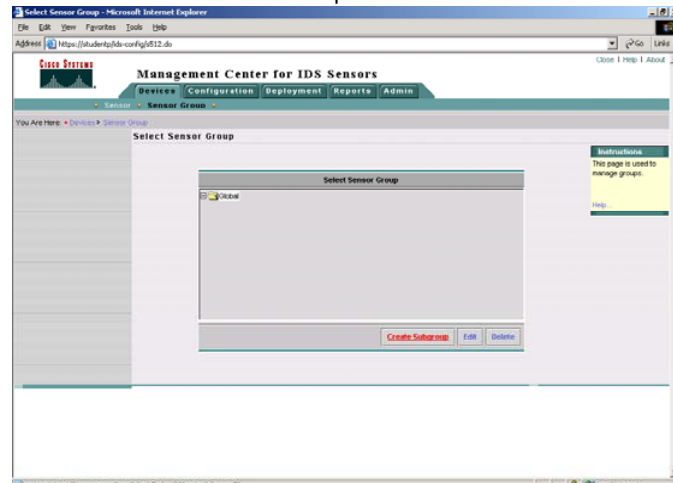
Step 8 Click **Finish** to finish adding a Sensor to the IDS MC. After the Sensor is added, it is displayed on the Sensor page.

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. The latest version that appears in this list is the version your IDS MC is currently using.

Adding a Sensor Group

Cisco.com

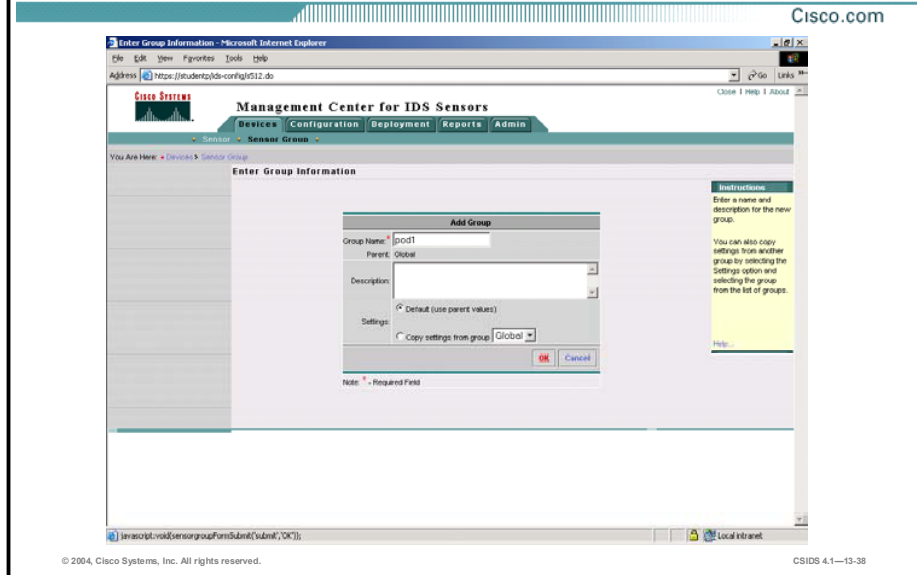
Choose Devices > Sensor Group.



Complete the following steps to add a Sensor group to the IDS MC:

- Step 1** Choose **Devices > Sensor Group**. The Select Sensor Group page is displayed.
- Step 2** Select a group, and click **Create Subgroup**. The Enter Group Information page is displayed.

Adding a Sensor Group (Cont.)



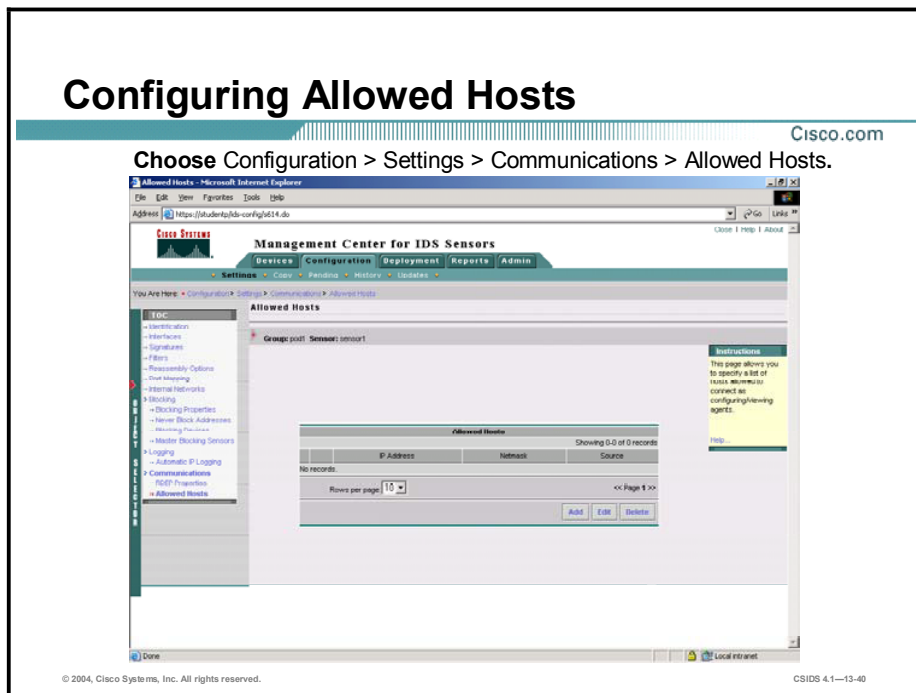
Step 3 Enter values for settings listed in the following table:

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 select the Copy settings from group radio button.

Step 4 Click **OK**. After the Sensor group is added, it is displayed on the Select Sensor Group page.

Using the IDS MC to Configure the Sensor

This topic does not attempt to thoroughly cover the use of the IDS MC to configure the Sensor. This topic explains how to use the IDS MC to configure allowed hosts and tune a signature by providing configuration examples.

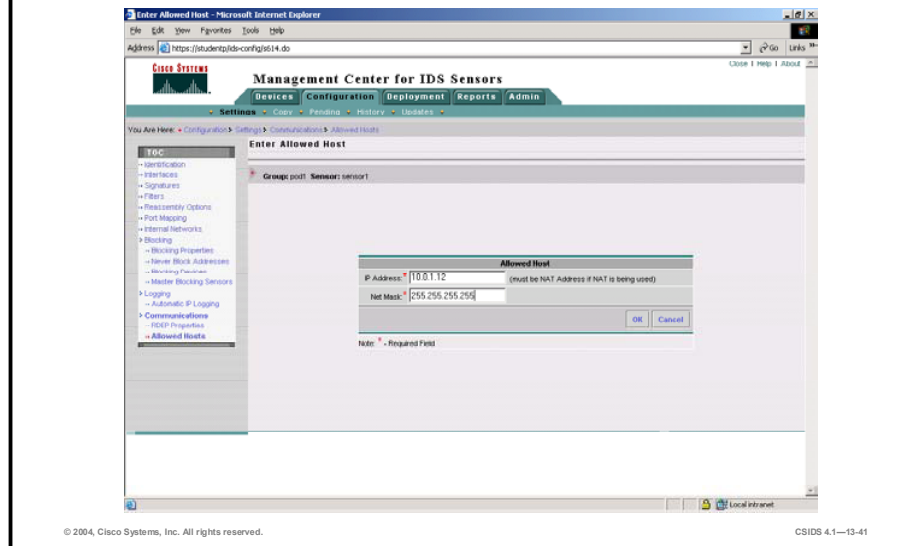


Complete the following steps to configure an allowed host:

- Step 1** Choose **Configuration > Settings**. The Settings page is displayed.
- Step 2** Use the Object Selector to select a Sensor.
- Step 3** Choose **Communications > Allowed Hosts** from the TOC. The Allowed Hosts page is displayed.
- Step 4** Click **Add**. The Enter Allowed Host page is displayed.

Configuring Allowed Hosts (Cont.)

Cisco.com



- Step 5** Enter the IP address of the allowed host or network in the IP Address field.
- Step 6** Enter the netmask in the Net Mask field. If the allowed host is a host rather than a network, enter the netmask 255.255.255.255.
- Step 7** Click **OK**. The allowed host is displayed in the Allowed Hosts page.

Tuning Signatures

Cisco.com

Choose Configuration > Settings > Signatures.

The screenshot shows the Cisco Management Center for IDS Sensors interface. The browser address bar shows 'https://studentsids-config1525.do'. The page title is 'Signatures - Microsoft Internet Explorer'. The main navigation bar includes 'Devices', 'Configuration', 'Deployment', 'Reports', and 'Admin'. The 'Configuration' tab is active, and the 'Settings > Signatures' path is highlighted. The left-hand TOC (Table of Contents) lists various configuration areas, with 'Signatures' selected. The main content area displays the 'Signatures' page for a sensor named 'sensor1'. It shows a table of signature groups with columns for 'Group Name' and 'Enabled'. Two groups are listed: 'Default' (404 of 1071) and 'CUSTOM' (0 of 0). Below the table are 'Enable' and 'Disable' buttons. A 'Help' link is visible on the right side of the page.

	Group Name	Enabled
1	Default	404 of 1071
2	CUSTOM	0 of 0

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-42

Complete the following steps to tune a signature:

- Step 1** Choose **Configuration > Settings**. The Settings page is displayed.
- Step 2** Use the Object Selector to select a Sensor.
- Step 3** Select **Signatures** from the TOC. The Signatures page is displayed.
- Step 4** Click **General**. The Signature(s) in Group page is displayed.

Tuning Signatures (Cont.)

Cisco.com

The screenshot shows the Cisco Management Center for IDS Sensors interface. The main content area displays a table of signatures for a sensor group named 'Sensors: sensor1'. The table has columns for Signature ID, Signature Name, Signature, Engine, Enabled, Severity, and Action. The first five signatures are related to traffic flow (Missed Packet Count, Traffic Flow Started, Traffic Flow Stopped) and the last five are related to packet recording (BAD IP OPTION, Record Packet Prio, Spoofing, Provide s.c.h.jcc, Loose Src Prio). A 'Filter Source' dropdown menu is set to 'General' and a 'Filter' field is empty. The table shows 10 records out of 1071 records.

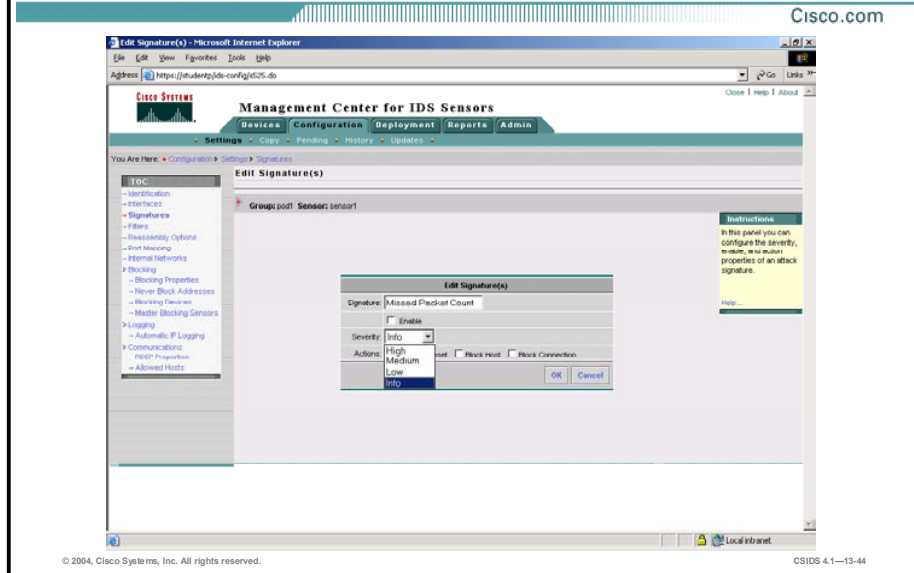
Signature ID	Signature Name	Signature	Engine	Enabled	Severity	Action
950 0	Missed Packet Count	OTHER		No	Info	None
954 1	Traffic Flow Started	OTHER		Yes	Info	None
954 2	Traffic Flow Started	OTHER		Yes	Info	None
955 1	Traffic Flow Stopped	OTHER		Yes	Info	None
955 2	Traffic Flow Stopped	OTHER		Yes	Info	None
1000 0	BAD IP OPTION	ATOMIC_PORTS		No	Info	None
1000 0	Record Packet Prio	ATOMIC_PORTS		No	Info	None
1000 0	Spoofing	ATOMIC_PORTS		No	Info	None
1000 0	Provide s.c.h.jcc	ATOMIC_PORTS		No	Info	None
1004 0	Loose Src Prio	ATOMIC_PORTS		No	High	None

Step 5 Locate the signature you want to tune, and select the check box to the left of the signature ID number.

Step 6 Click **Edit**. The Edit Signature(s) page is displayed.

Note You can locate a signature by making a selection from the Filter Source drop-down menu and entering a corresponding value in the field to its right.

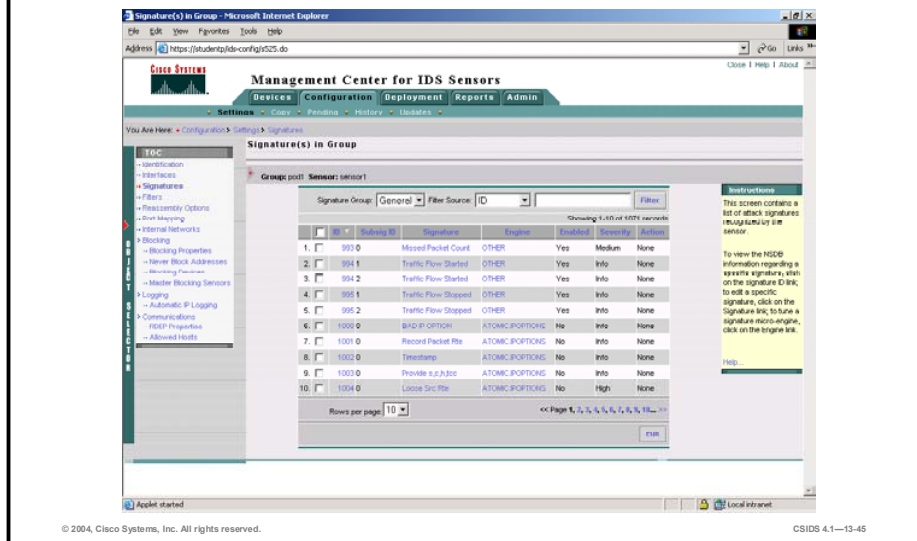
Tuning Signatures (Cont.)



- Step 7** Select the **Enable** check box.
- Step 8** Select a severity level from the Severity drop-down menu.
- Step 9** Choose an action for the Sensor to take if the signature fires by selecting one of the Action check boxes.
- Step 10** Click **OK**. The Signature(s) in Group page is displayed.

Tuning Signatures (Cont.)

Cisco.com



The new settings are displayed in the Signature(s) in Group page as shown in the figure. By viewing the signature configuration in the CLI, you can verify that the Sensor accepts the settings and the signature is configured as desired on the Sensor. To view the signature settings in the CLI, complete the following steps, which use the settings for the 3001 TCP Port Sweep signature as an example:

Step 1 Enter virtual sensor configuration mode:

```
sensor(config)# service virtual-sensor-configuration virtualSensor
sensor(config-vsc)#
```

Step 2 Enter micro-engine tuning mode:

```
sensor(config-vsc)# tune-micro-engines
sensor(config-vsc-virtualSensor)#
```

Step 3 Enter configuration mode for the engine that controls the signature:

```
sensorP(config-vsc-virtualSensor)#sweep.port.tcp
sensorP(config-vsc-virtualSensor-SWE)#
```

Step 4 Access the signature:

```
sensorP(config-vsc-virtualSensor-SWE)# signatures SIGID 3001
sensorP(config-vsc-virtualSensor-SWE-sig)#
```

Step 5 View the signature settings:

```
sensorP(config-vsc-virtualSensor-SWE-sig)# show settings
```

Note The Sensor will not operate with the new settings until the configuration is deployed as explained in the next topic.

IDS MC Workflow

This topic explains the workflow process for deploying IDS configuration files.

Workflow

Cisco.com

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**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—13-47

The Deployment tab is used to deploy configuration files to Sensors. Deploying Sensor configuration files requires you to perform certain tasks in a specific order. This 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.

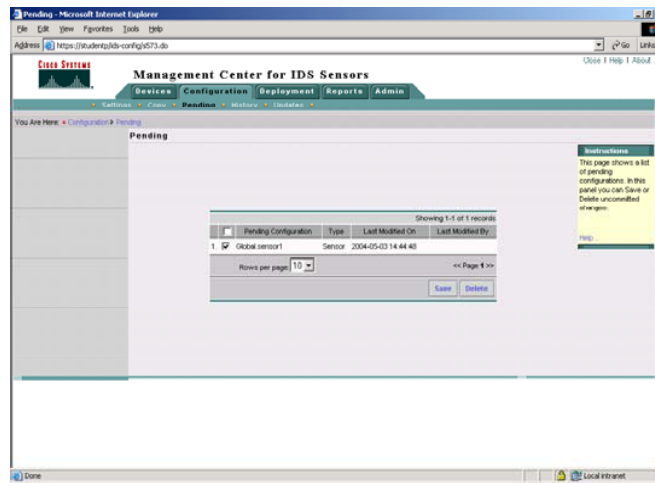
Note By default, approval is not required. Choose **Admin > System Configuration > Configuration File Management** and select **Enable Configuration file change approval** to enable the approval feature.

- Step 3** Deploy approved configuration files to the Sensors.

Saving Configuration Changes

Cisco.com

Choose Configuration > Pending.



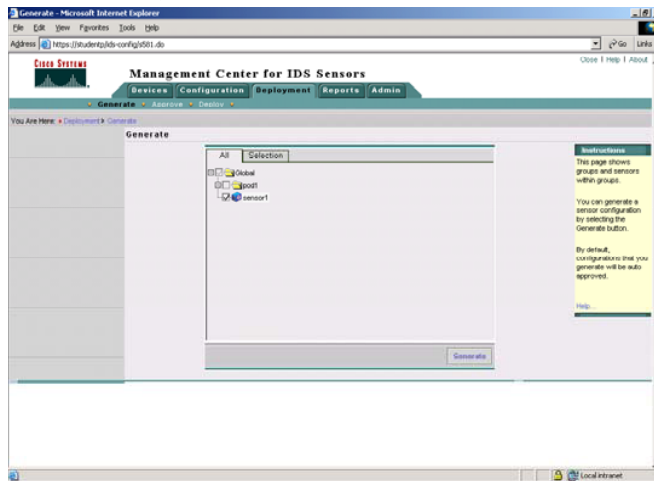
Before you can generate a configuration file for your Sensor, you must commit your proposed configuration changes to the database by saving them. To save configuration changes, complete the following steps:

- Step 1** Select **Configuration > Pending**. The Pending page is displayed.
- Step 2** Select the check box to the left of the pending configuration.
- Step 3** Click **Save**. The Pending page refreshes, and the configuration file name is no longer displayed.

Generating a Configuration File

Cisco.com

Choose **Deployment > Generate**.

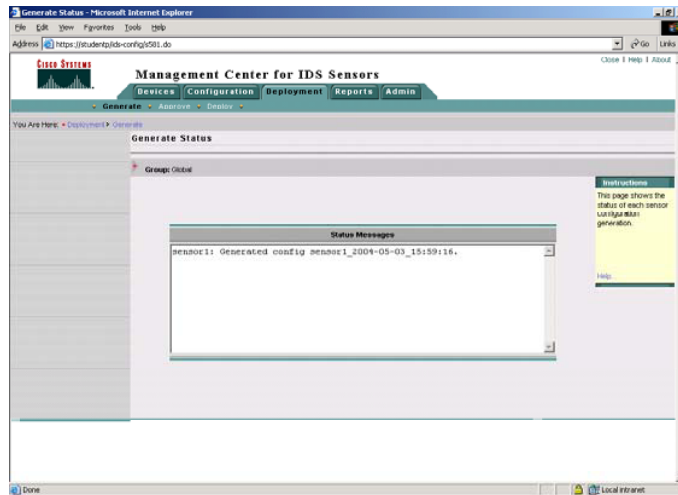


Complete the following steps to generate configuration files for the Sensor:

- Step 1** Choose **Deployment > Generate**. The Generate page is displayed.
- Step 2** Select the Sensor check box and click **Generate** to generate the Sensor configuration. The Generate Status page is displayed.

Generating a Configuration File (Cont.)

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

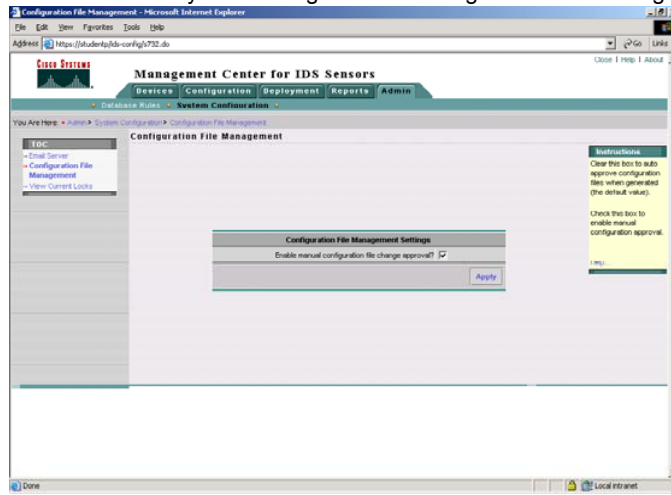
CSIDS 4.1—13-50

The configuration file name and the time at which it was generated are displayed in the Generate Status page. If configuration changes are pending, the configuration file generation will fail. Choose **Configuration > Pending** to view pending changes.

Approving a Configuration File (Optional.)

Cisco.com

Choose Admin > System Configuration > Configuration File Management.

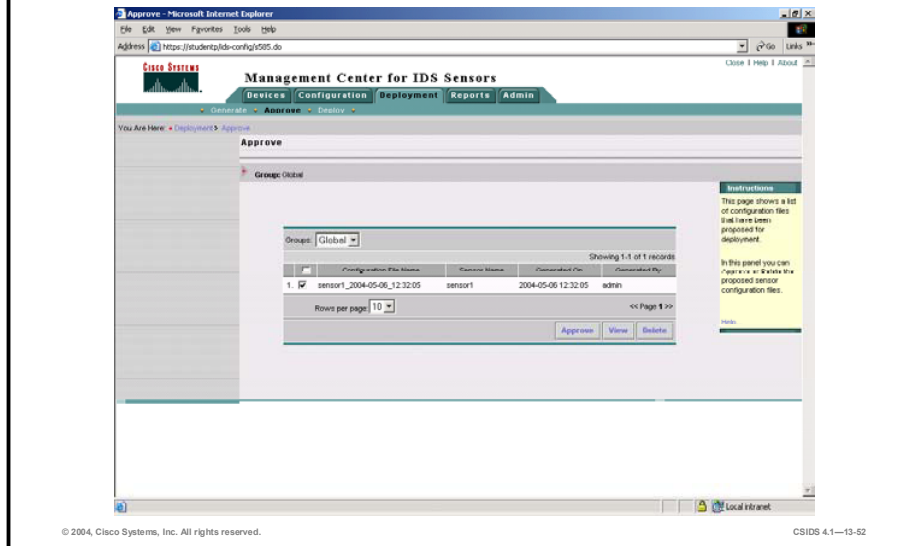


Unless you specify otherwise, the IDS MC automatically approves Sensor configurations when you generate them. To specify manual approval, complete the following steps:

- Step 1** Select **Admin > System Configuration**.
- Step 2** Select **Configuration File Management** from the TOC.
- Step 3** Select the Enable manual configuration file change approval check box.
- Step 4** Click **Apply**.

Approving a Configuration File (Cont.)

Cisco.com



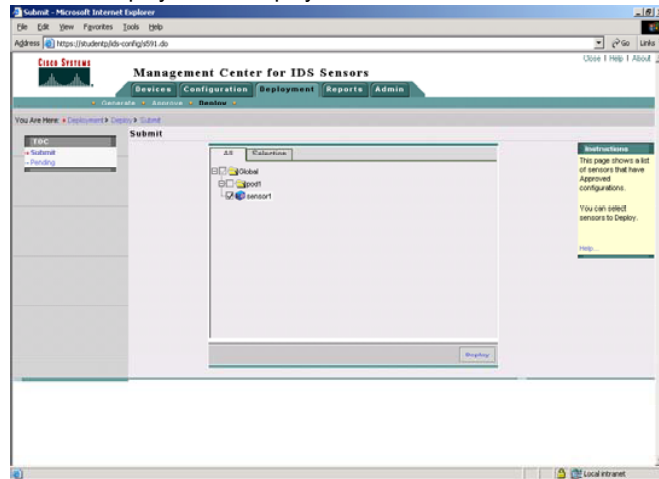
Complete the following steps to approve a Sensor configuration:

- Step 1** Select **Deployment > Approve**. The Approve page is displayed.
- Step 2** Select the check box for the configuration file you wish to approve.
- Step 3** Click **Approve**.

Deploying a Configuration File

Cisco.com

Choose **Deployment > Deploy > Submit**.

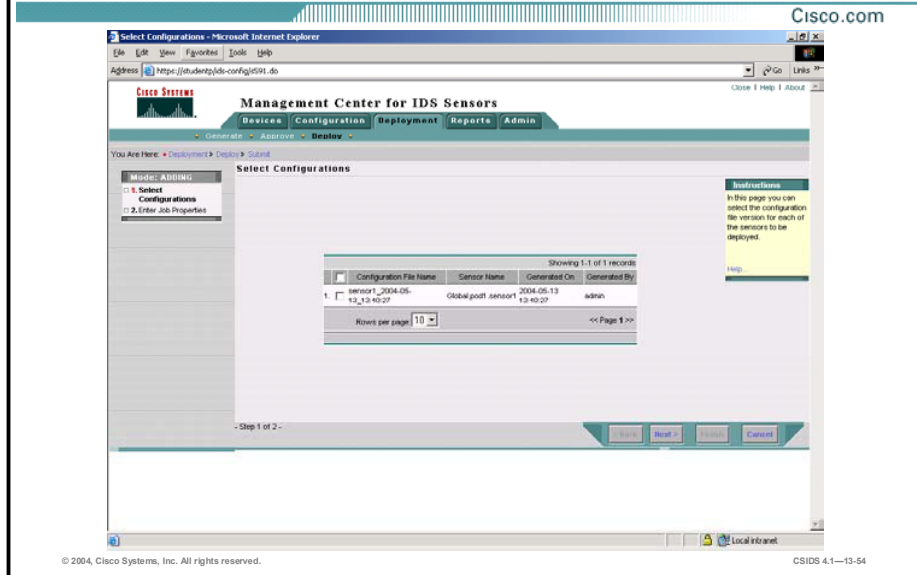


When you select **Deployment > Deploy**, two options are displayed in the TOC, submit and pending. Submit allows you to create a new deployment job. Pending enables you to view pending deployment jobs.

Complete the following steps to create a new deployment job:

- Step 1** Choose **Deployment > Deploy > Submit**. The Submit page is displayed.
- Step 2** Select the check box to the left of the Sensor for which you want to deploy a configuration.
- Step 3** Click **Deploy**. The Select Configurations page is displayed.

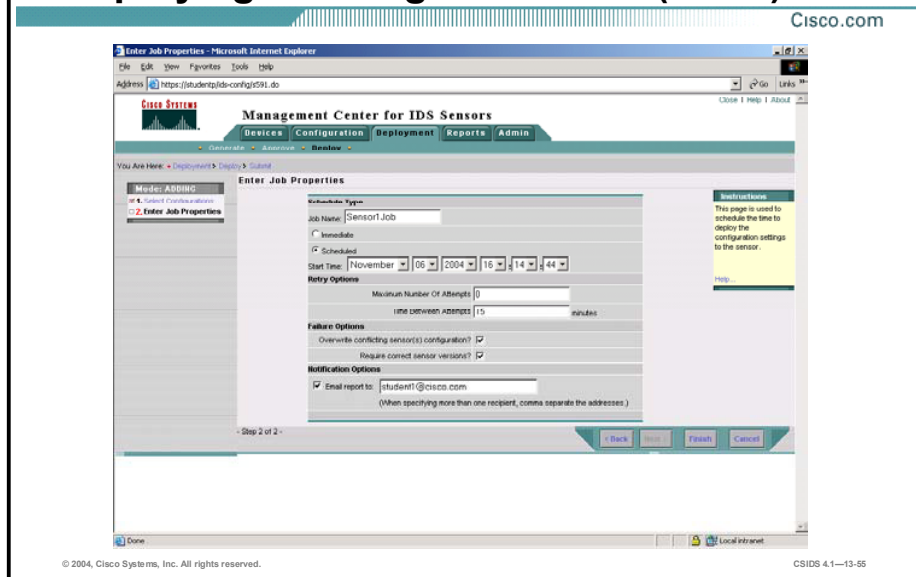
Deploying a Configuration File (Cont.)



Step 4 Select the check box to the left of the configuration file name.

Step 5 Click **Next**. The Enter Job Properties page is displayed.

Deploying a Configuration File (Cont.)



Step 6 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 Sensor(s) configuration?	(Optional.) Select this check box to overwrite the Sensor 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.

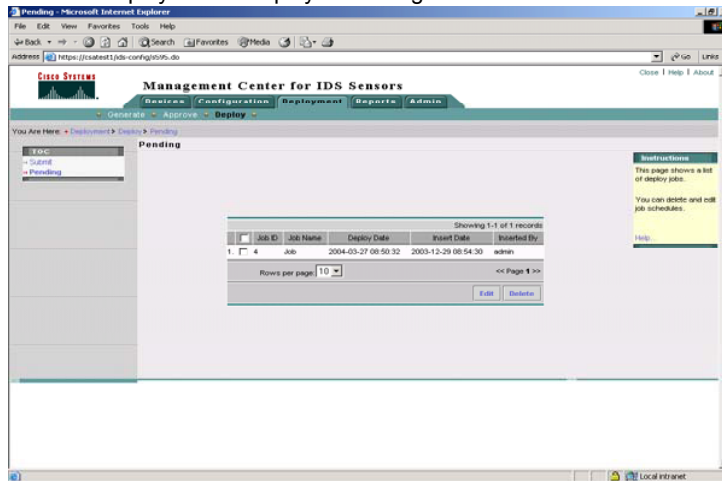
Step 7 Click **Finish**. The Submit page is displayed.

Note Verify the Sensor configuration deployment by generating a Sensor Configuration Deployment Report. Choose **Reports > Generate > Sensor Configuration Deployment Report** and click **Select** to start the report generation.

Pending Deployments

Cisco.com

Choose **Deployment > Deploy > Pending.**



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, you will be able to see and edit pending job deployments.

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.
- Step 3** Select a pending job's check box and click **Edit**. The pending job's scheduling page is displayed.

Updating the IDS MC

This topic explains how to update the IDS MC.

IDS MC Updates

Cisco.com

- **The IDS MC must operate with the same software and signature version as the Sensors it manages.**
- **When you update the Sensor, you must also update the IDS MC.**
- **A compressed (.zip) update file must be used to upgrade the IDS MC.**
- **To update the IDS MC, the update file must reside on the IDS MC server at X:\Program Files\CSCOpX\MDC\etc\ids\updates.**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1—13-58

Cisco Systems periodically releases updates of Sensor software and signatures. It is strongly recommended that you download and apply all update files, in order and without exception, as they become available. For the IDS MC to understand the software installed on the Sensor, it must operate with the same software and signature version as the Sensors it manages. Therefore, when you apply service pack and signature updates to a Sensor, you must also update the IDS MC.

The software update files used by the IDS MC are compressed (.zip) files. The IDS MC works with these compressed files directly, so you should not unzip them or extract anything from them. The update file must reside on the IDS MC server at X:\Program Files\CSCOpX\MDC\etc\ids\updates, where X is the drive where the IDS MC is installed. You can obtain the compressed update files from the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids>

Before performing updates, check the software and signature version that your Sensor and your IDS MC server are using. You can determine the Sensor software and signature version that your IDS MC server is using by following the steps for adding a Sensor to the IDS MC. When the Sensor Information page is displayed, scroll to the bottom of the Version list. The highest version listed is the version your IDS MC is using. Click **Cancel** after locating the version.

Complete the following steps to determine the software and signature version that your Sensor is using:

Step 1 Choose **Configuration > Settings**.

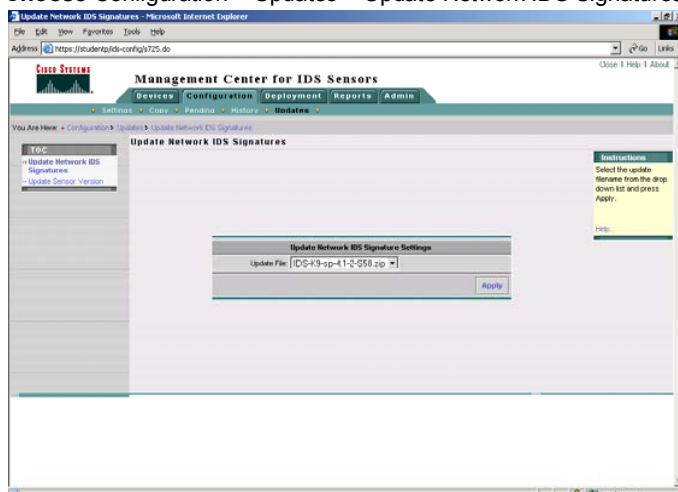
Step 2 Click the **Object Selector** handle. The Object Selector opens.

- Step 3** From the Object Selector, select the Sensor whose software and signature version you want to determine. The Object Selector closes.
- Step 4** Select **Identification** from the TOC. The Identification page is displayed. The Sensor software and signature version are displayed in the Version field.

Applying an Update

Cisco.com

Choose Configuration > Updates > Update Network IDS Signatures.



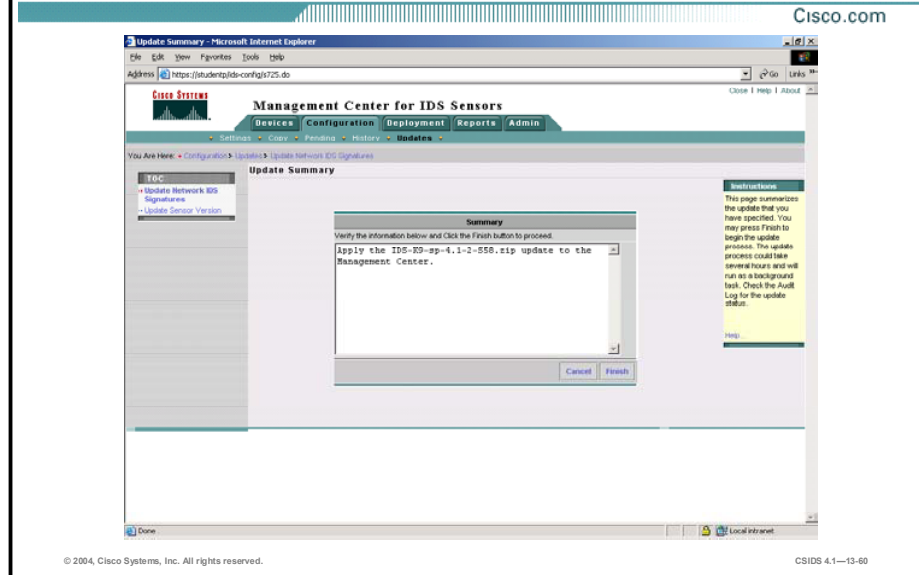
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-59

Complete the following steps to update the Sensor software and signature version of your IDS MC:

- Step 1** Download the update file to `~CSCOPx/MDC/etc/ids/updates` on the IDS MC server.
- Step 2** Select **Configuration > Updates > Update Network IDS Signatures**. The Update Network IDS Signatures page is displayed.
- Step 3** Select the update you wish to apply from the Update File drop-down menu.
- Step 4** Click **Apply**. The Update Summary page is displayed.

Applying an Update (Cont.)

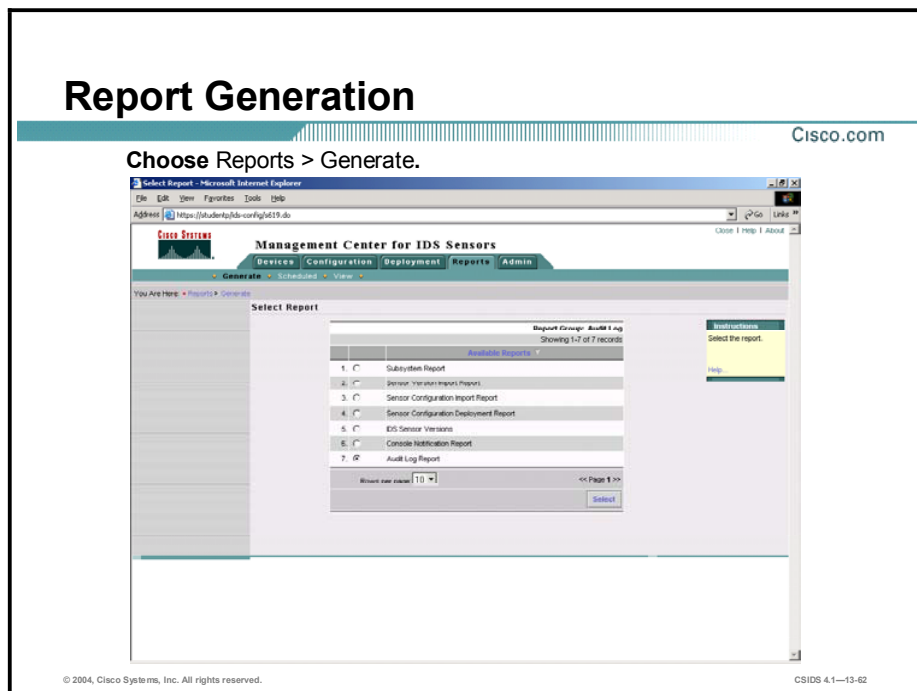


Step 5 Verify that the Update Summary page describes the update you want to apply.

Step 6 Click **Finish**.

Reporting

This topic explains using the IDS MC to create reports.



The Reports tab enables you to generate and view reports related to the IDS MC and deployment of Sensor configuration files. When you generate a report, you can run it immediately or you can schedule it to run at a later time. Scheduled reports can be run once or repeatedly.

The six types of reports that can be generated are as follows:

- Subsystem Report—Enables you to generate reports on the subsystem components of the IDS MC
- Sensor Version Import Report—Enables you to generate reports based upon the imported versions of Sensors in the IDS MC
- Sensor Configuration Import Report—Enables you to generate reports on the status of configuration imports of Sensors in the IDS MC
- Sensor Configuration Deployment Report—Enables you to generate reports on the status of configuration deployments to Sensors
- Console Notification Report—Enables you to generate reports based upon notifications that the console has received
- Audit Log Report—Enables you to generate reports based upon the audit event log stored locally on the Sensor

Complete the following steps to generate a report:

- Step 1** Choose **Reports > Generate**. The Select Report page is displayed.
- Step 2** Select one of the available reports and click **Select**. The Report Filtering page is displayed.

Report Generation (Cont.)

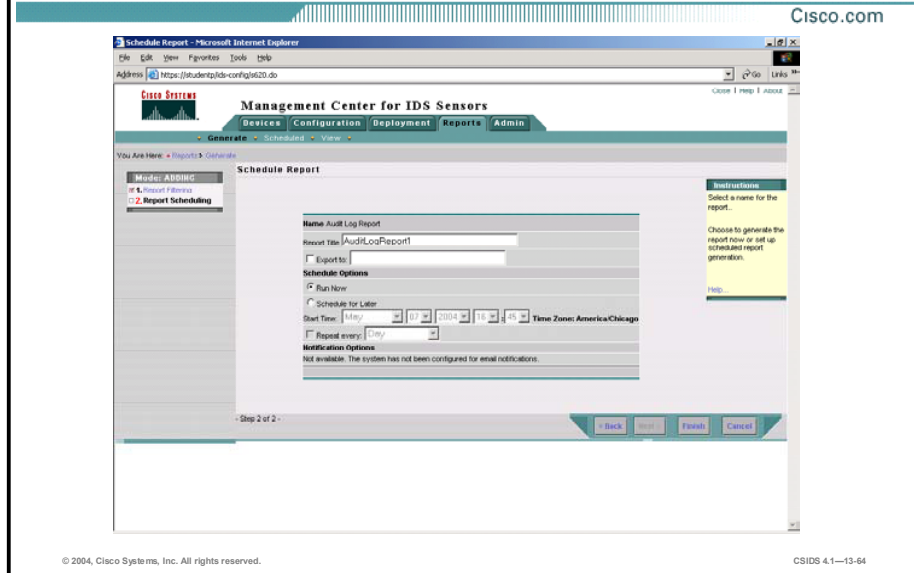
Cisco.com

The screenshot shows the 'Report Filtering' page in the Cisco Management Center for IDS Sensors. The page is titled 'Report Filtering' and is part of a 'Reports' section. The main content area is for an 'Audit Log Report'. It includes several filter categories: 'Date/Time' (with radio buttons for 'List' and 'Since the dawn of time'), 'Event Severity' (with a dropdown menu), 'Applications' (with a text input field), 'Subsystem' (with a dropdown menu), and 'Task Type' (with a dropdown menu). Each category has 'Select All' and 'Clear All' buttons. A 'Next' button is visible at the bottom right. The page also includes a 'Help' link and a 'Close' button. The footer contains the copyright information: '© 2004, Cisco Systems, Inc. All rights reserved.' and the document ID 'CSIDS 4.1-13-63'.

Step 3 Enter the report parameters for the report type you selected. The contents of the Report Filtering page will vary depending on which type of report you choose to generate.

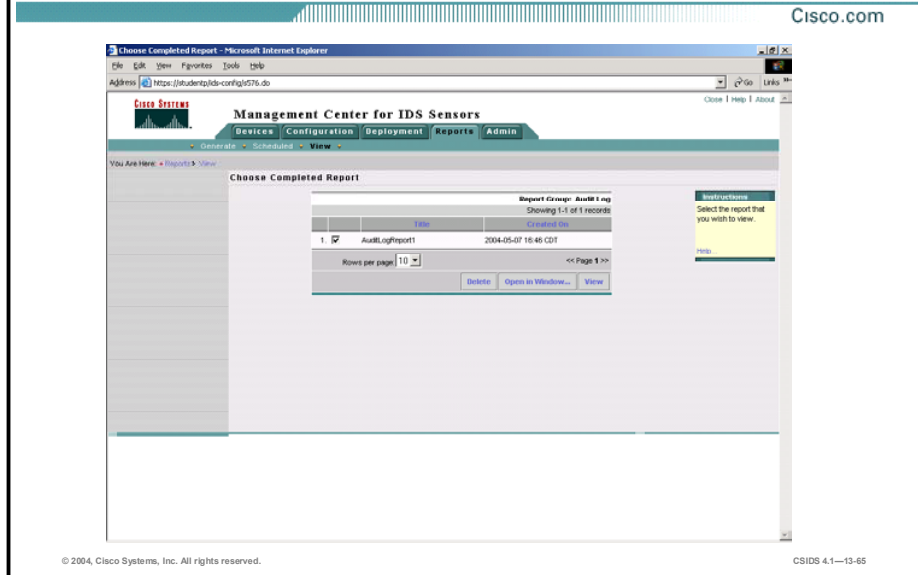
Step 4 Click **Next**. The Schedule Report page is displayed.

Report Generation (Cont.)



- Step 5** Enter a name for the report in the Report Title field.
- Step 6** If you wish to export the generated report to an HTML file, select the **Export to** check box and specify the exact path to the file that is to contain the generated report. The path should include the filename and the desired extension.
- Step 7** Click the **Run Now** or **Schedule for Later** radio button under Schedule Options. If you select Run Now, skip to Step 9. If you select Schedule for Later, configure the following settings:
1. Use the Start Time drop-down menus to specify the date and time that you want the report to run. The date is specified by month, day, and year. The time is specified in hours and minutes. The time zone used to determine the time is to the right of the Start Time drop-down menus.
 2. To run the report at regular intervals, select the Repeat every check box and make a selection from the drop-down menu. You can schedule the report to run every day, week, weekday, weekend day, hour, or minute.
- Step 8** To send an e-mail notification to someone when the report runs, select the Email report to check box and enter an e-mail address in the adjacent field. Use commas to separate multiple addresses.
- Step 9** Click **Finish**.

Viewing Reports



Complete the following steps to view a report:

- Step 1** Select **Reports > View**. The Choose Completed Report page is displayed.
- Step 2** Select the check box corresponding to the title of the report you want to view.
- Step 3** Click **View**. The report appears in the Report page. Optionally, choose **Open in Window** to view the report in a new browser window. The report appears in a new browser window.

Note If you select **Run Now**, the report runs and you can view the generated report by selecting **Reports > View**. If you select **Schedule for Later**, you can view the scheduled report template by selecting **Reports > Scheduled**.

Summary

This topic summarizes what you learned in the lesson.

Summary

Cisco.com

- **The IDS MC provides a web-based interface for configuring and managing multiple IDS Sensors.**
- **The IDS MC can be installed on Windows-based and Solaris-based servers.**
- **The IDS MC allows the grouping of Sensors into Sensor groups for ease of management and configuration.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-67

Summary (Cont.)

Cisco.com

- For the IDS MC to understand the software installed on the Sensor, it must operate with the same software and signature version as the Sensors it manages. Therefore, if you apply a service pack or signature update to a Sensor managed by the IDS MC, you must also update the IDS MC.
- The IDS MC provides a mechanism for controlling the approval and deployment of Sensor configuration files.
- The IDS MC's reporting capability provides a method for determining the status of configuration deployment.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—13-68

Enterprise Intrusion Detection System Monitoring and Reporting

Overview

This lesson introduces enterprise intrusion detection system (IDS) monitoring and reporting using the CiscoWorks Virtual Private Network (VPN)/Security Management Solution (VMS) Security Monitor. The following topics are covered in this lesson:

- Objectives
- Introduction
- Installation
- Getting started
- Monitoring
- Customizing the Event Viewer
- Reporting
- Administration
- Cisco Threat Response
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

- **Define features and key concepts of the Security Monitor.**
- **Install the Security Monitor and verify its 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.**
- **Explain the functionality and benefits of Cisco Threat Response.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-3

Introduction

This topic introduces CiscoWorks Monitoring Center for Security (Security Monitor) for the Cisco Intrusion Detection System (IDS).

What Is the Security Monitor?

Cisco.com

The Security Monitor provides event collection, viewing, and reporting capability for network devices.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—14-5

The Security Monitor is a component of the CiscoWorks Virtual Private Network (VPN)/Security Management Solution (VMS) product. The VMS product integrates numerous security applications into a single solution, including the following:

- CiscoWorks Common Services
- Security Monitor
- CiscoWorks VPN Monitor
- Management Center for IDS Sensors (IDS MC)

The Security Monitor provides event collection, viewing, and reporting capability. It benefits organizations experiencing information overload resulting from large volumes of security events. Security Monitor's event correlation capabilities increase the accuracy of threat detection by enabling you to identify attacks that are not easily recognizable from a single event. You can create event correlation rules that enable you to perform the following tasks:

- Monitor attacks against specific, high-visibility hosts such as web servers
- Monitor traffic for patterns of attacks
- Correlate IDS information from multiple security devices
- Receive early notification of emerging threats
- Trigger an automated response as a corrective action against an attack
- Reduce the number of false positives

Security Monitor Features

Cisco.com

The following are Security Monitor features:

- **Monitors the following devices:**
 - **Sensor appliances**
 - **IDS Services Modules**
 - **IDS Network Modules**
 - **Cisco IOS routers**
 - **PIX Firewalls**
 - **Firewall Services Modules**
 - **CSA MC**
- **Web-based monitoring platform**
- **Custom reporting capability**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-6

The Security Monitor has the following features:

- **Device monitoring**—The Security Monitor can receive IDS events from the following Cisco IDS-capable devices:
 - Sensor appliance
 - Intrusion Detection System Services Module (IDSM)
 - Intrusion Detection System Services Module 2 (IDSM-2)
 - Intrusion Detection System Network Module (NM-CIDS)
 - IOS router
 - PIX Firewall
 - Firewall Services Module (FWSM)
 - Management Center for Cisco Security Agents
- **Web-based monitoring platform**—The Security Monitor is built on web-based technology. This enables you 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 your needs.

Note

See the following web site for more details on supported devices:

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3991/products_data_sheet09186a00800e55b6.html

Installation

This topic explains the installation of the Security Monitor and discusses the requirements for installation.

Installation Requirements

Cisco.com

- **Hardware**
 - IBM PC-compatible computer, 1 GHz or faster
 - Color monitor with at least 800 x 600 resolution and a video card capable of 16-bit color
 - CD-ROM
 - 100-Mbps or faster network connection
- **Memory—1 GB of RAM minimum**
- **Virtual memory—2 GB minimum**
- **Disk drive space**
 - 9 GB minimum
 - NTFS
- **Software**
 - Windows 2000 Professional, Server, or Advanced Server with Service Pack 3
 - Sun Java plug-in 1.3.1-b24

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—14-8

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 color
 - A CD-ROM drive
 - A 100BASE-T or faster network connection
- **Memory—1 GB of RAM minimum**
- **Virtual memory—2 GB minimum**
- **Disk drive space**
 - 12 GB of free hard drive space minimum
 - New Technology File System (NTFS)
- **Software**
 - Windows 2000 Professional, Server or Advanced Server with Service Pack 3
 - Sun Java plug-in 1.3.1-b24

Note You must ensure that Terminal Services is turned off on the Windows system on which the Security Monitor will run.

Caution Do not attempt to install the Security Monitor 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, 300 MHz or faster**
- **Memory—256 MB of RAM minimum**
- **Disk drive space—400 MB of virtual memory**
- **Software**
 - **Windows 2000 Professional, Server, or Advanced Server with Service Pack 3**
 - **Windows XP Professional**
- **Browser**
 - **Internet Explorer 6.0 (Service Pack 1) with Microsoft Virtual Machine**
 - **Netscape Navigator 4.79**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-9

Verify that the client machine used to log in to the Security Monitor meets the following requirements:

- **Hardware—IBM PC-compatible, 300 MHz or faster**
- **Memory—256 MB of RAM minimum**
- **Disk drive space—400 MB of virtual memory**
- **Software**
 - **Windows 2000 Professional, Server, or Advanced Server with Service Pack 3**
 - **Windows XP Professional**
- **Browser**
 - **Microsoft Internet Explorer 6.0 (Service Pack 1) with Microsoft Virtual Machine**
 - **Netscape Navigator 4.79**

Note Requirements for client and server systems are frequently updated. Check Cisco.com for the latest requirements.

Installation Overview

Cisco.com

- **Common Services is required for the Security Monitor.**
- **Common Services provides the CiscoWorks server-based components, software libraries, and software packages developed for the Security Monitor.**

© 2004, Cisco Systems, Inc. All rights reserved.

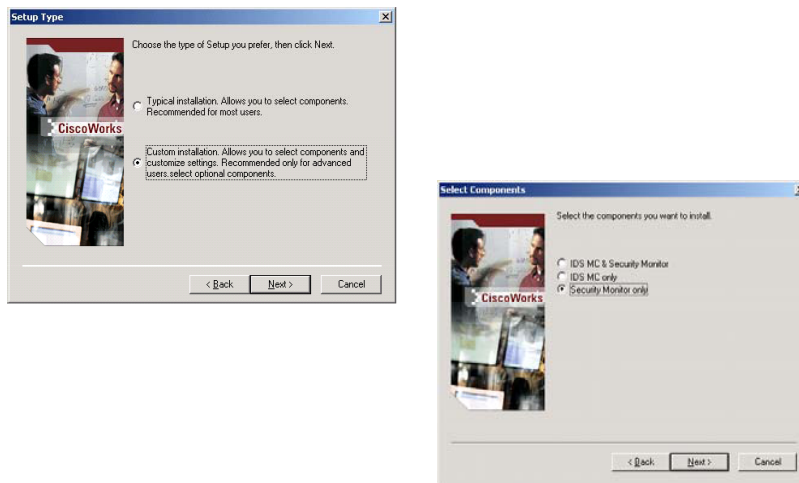
CSIDS 4.1—14-10

Common Services is required for the Security Monitor. Common Services provides 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 the VPN/Security Management Solution*.

Security Monitor Installation

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-11

Complete the following steps to install the Security Monitor:

- Step 1** Launch the Security Monitor installation. The following message is displayed:
Do you really want to install IDS MC & Security Monitor?
- Step 2** Click **Yes**. The Welcome Window opens.
- Step 3** Click **Next**. The Software License Agreement window opens.
- Step 4** Click **Yes** to accept the Software License Agreement. The Setup Type window opens.

Note If you do not accept the Software License Agreement, the installation process stops.

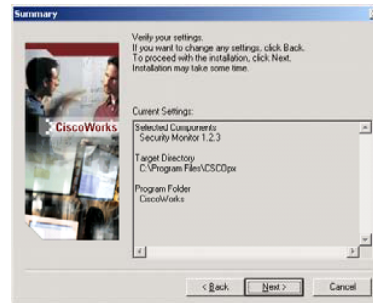
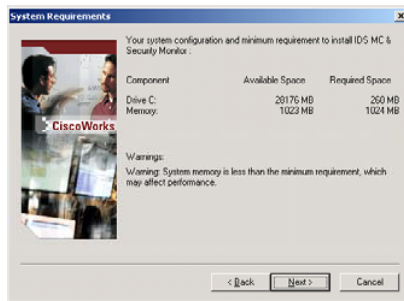
- Step 5** Select **Custom Installation** and click **Next**. The Select Components window opens.

Note To install the IDS MC and the Security Monitor simultaneously, select **Typical installation**.

- Step 6** Select the **Security Monitor only** radio button and click **Next**. The System Requirements window opens.

Verifying System Requirements and Settings During Installation

Cisco.com



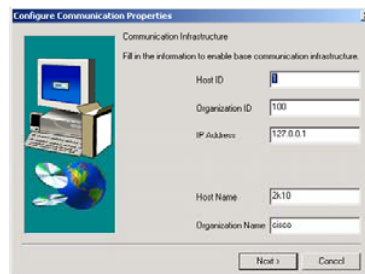
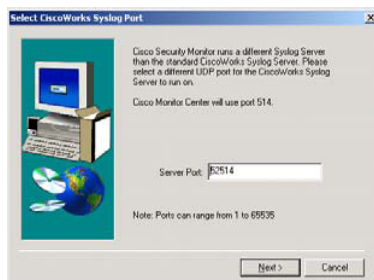
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-12

- Step 7** Verify that your system meets the requirements, and click **Next**. The Summary panel is displayed.
- Step 8** Verify the selected components, and click **Next**. The Select CiscoWorks Syslog Port panel is displayed.

Selecting the Syslog Port and Specifying Communication Properties

Cisco.com



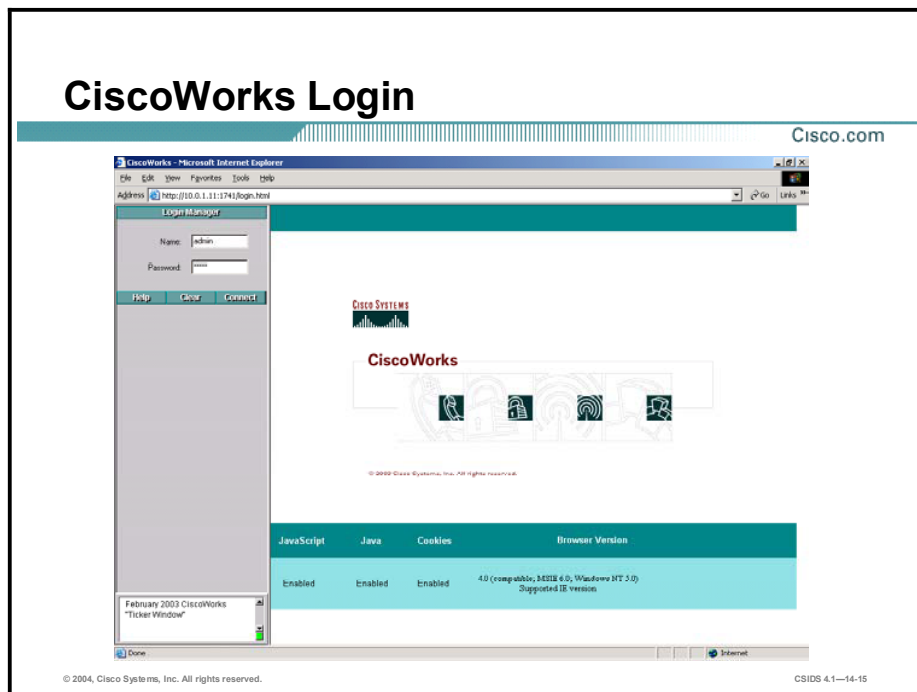
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-13

- Step 9** Specify a UDP port for the CiscoWorks Syslog server or accept the default port, and click **Next**. The Configure Communication Properties panel is displayed.
- Step 10** If your Security Monitor will monitor Sensors running 3.x software, enter values for communication infrastructure settings.
- Step 11** Click **Next**. When the Security Monitor installation is complete, the Setup Complete panel is displayed.
- Step 12** Click **Finish**. The Install Wizard exits.
- Step 13** Restart your student PC.

Getting Started

This topic explains how authorization roles in CiscoWorks are responsible for delegation of tasks and how to log in to the Security Monitor.



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:

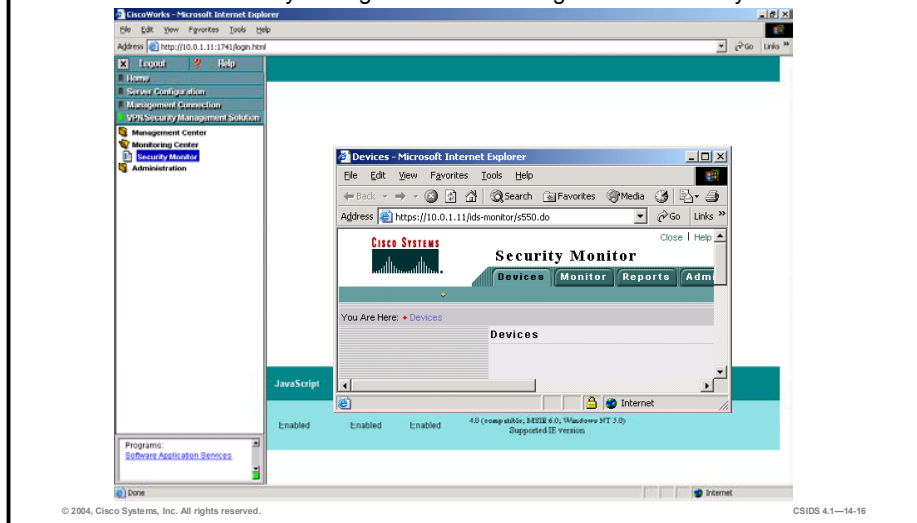
- Step 1** Open a browser and point your browser to the IP address of the CiscoWorks server with a port number of 1741. In the figure, the IP address of the CiscoWorks server is 10.0.1.11. Enter the following in the browser address field:
http://10.0.1.11:1741
- Step 2** The CiscoWorks desktop is displayed.
- Step 3** Log in with the default username of **admin** and the password you created during the CiscoWorks installation.

Note It is recommended that you change the default admin account password.

Security Monitor Launch

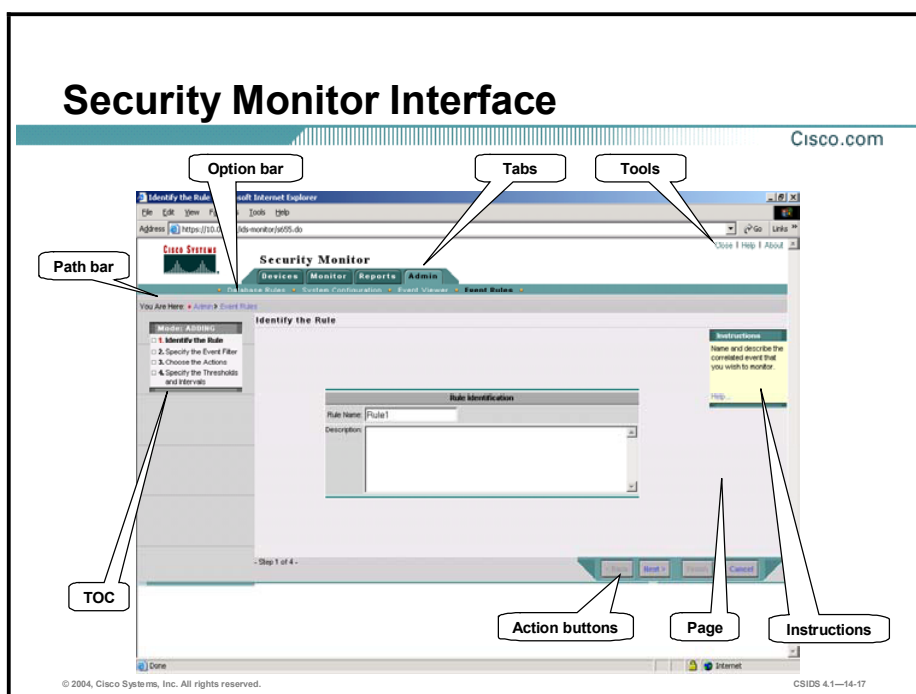
Cisco.com

Choose VPN/Security Management > Monitoring Center > Security Monitor.



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.

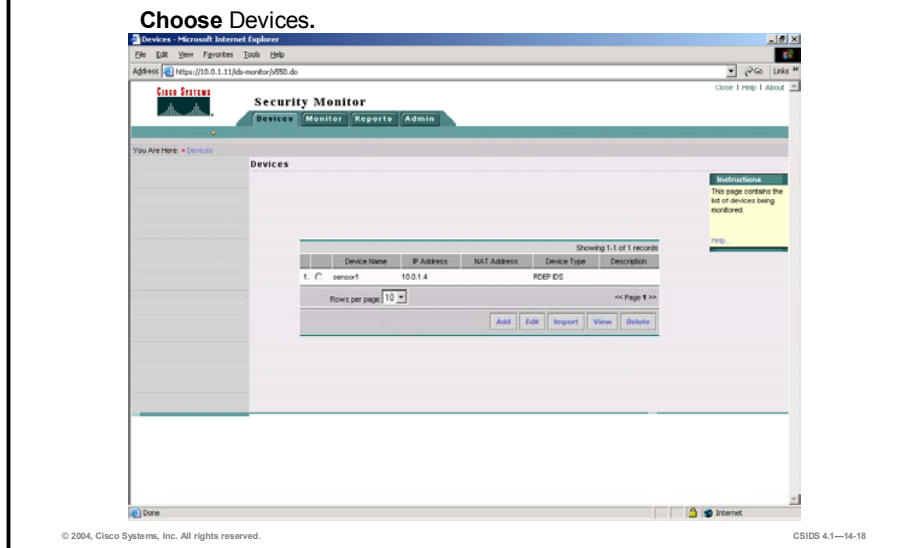


The figure illustrates elements of the Security Monitor GUI. The elements are described as follows:

- Path bar—Provides the location of the current page.
- TOC (table of contents)—A menu of choices that is displayed down the left side of the Security Monitor interface. It represents the list of suboptions that you can select.
- Option bar—Displays the options available for the selected tab.
- Configuration tabs—Provide 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. The 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—Initiate actions or commands for this page. Buttons that do not work on a particular page are grayed out.

Adding Devices

Cisco.com



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 to perform the following operations on existing devices:

- Edit
- View
- Delete

Note You can use Security Monitor to import device information from a local or remote IDS MC server.

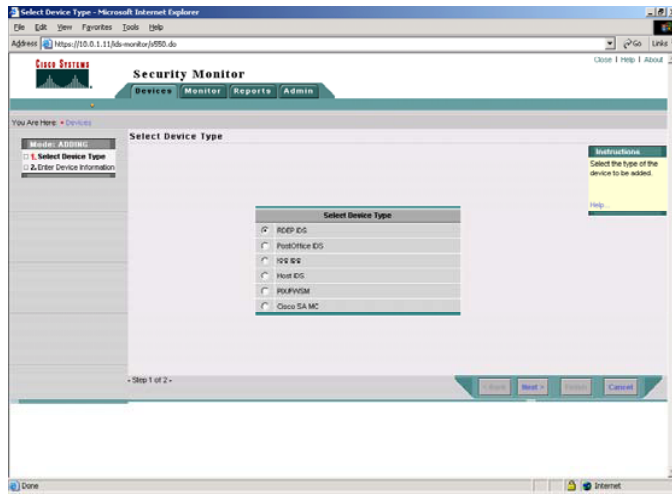
Complete the following steps to add a device to the Security Monitor:

- Step 1** Choose **Devices**. The Devices page is displayed.
- Step 2** Click **Add**. The Select Device Type page is displayed.

Adding Devices (Cont.)

Cisco.com

Choose Devices and select Add.



© 2004, Cisco Systems, Inc. All rights reserved.

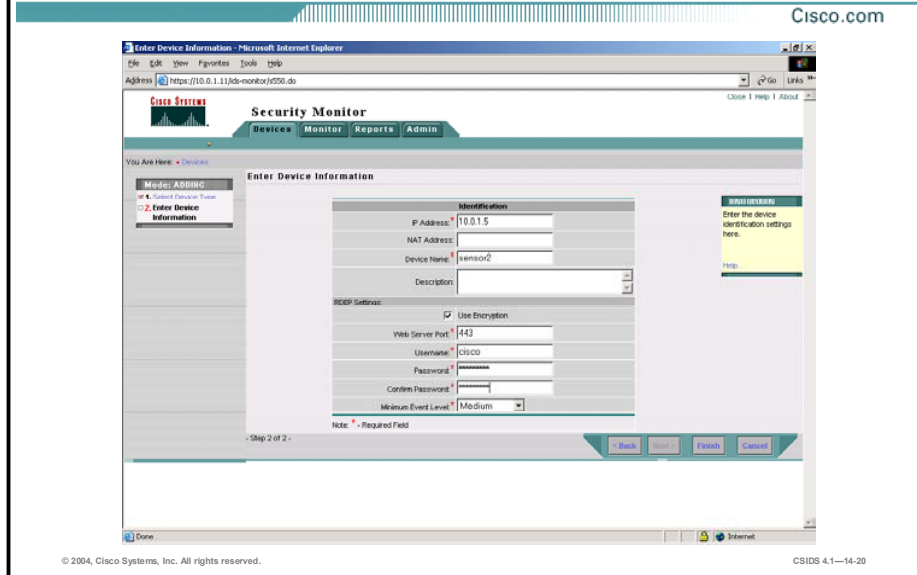
CSIDS 4.1—14-19

Step 3 Choose one of the following device types:

- RDEP IDS
- PostOffice IDS
- IOS IDS
- Host IDS
- PIX/FWSM
- Cisco SA MC

Step 4 Click **Next**. The Enter Device Information page is displayed.

Adding Devices (Cont.)



Step 5 Enter values for settings listed in the following table:

Add Device	Description
IP Address	(Required.) The IP address of the device being added.
NAT Address	Network Address Translation (NAT) IP address of the device, required if the device is using NAT.
Device Name	(Required.) The name of the device being added.
Description	(Optional.) The description for the device being added.
Protocol	(Required.) The protocol of the device being added.
Use Encryption	Select this check box if the device uses Transport Layer Security (TLS). This check box is selected by default.
Web Server Port	(Required.) The port to be used for communication with the device. The default is port 443.
Username	(Required.) The user account name to be used for the Monitoring Center for Security to access the device.
Password	(Required.) The password for the user account.
Confirm Password	(Required.) The password for the user account confirmed.
Minimum Event Level	(Required.) A drop-down menu to select the minimum event level for the device.

Step 6 Click **Finish**. The Devices page is refreshed with the new device in the table.

Note To allow a Security Monitor server to retrieve event data from an RDEP device, you must identify the Security Monitor server as an allowed host on the Sensor.

Importing Devices

Cisco.com

Choose Devices and select Import.

The screenshot shows a web browser window titled "Enter IDS MC Server Information - Microsoft Internet Explorer". The page is part of the Cisco Security Monitor interface. The main heading is "Enter IDS MC Server Information". On the left, there is a "Works Adding" section with a list of steps: "1. Enter IDS MC Server Information", "2. Select Devices", and "3. Update NAT Addresses". The current step is "1. Enter IDS MC Server Information". The main content area contains a form titled "Enter IDS MC server contact information:" with the following fields: "IP Address/Host Name" (value: 10.0.1.12), "Web Server Port" (value: 443), "Username" (value: admin), and "Password" (value: [masked]). A "Note" below the form states: "Note: * - Required Field". On the right, there is an "Instructions" box with text: "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." and a "Help" link. At the bottom of the form, there are navigation buttons: "Back", "Next", "Finish", and "Cancel". The page footer shows "© 2004, Cisco Systems, Inc. All rights reserved." and "CSIDS 4.1-14-21".

Instead of adding new devices by specifying all of the information necessary for Security Monitor to communicate with the device, you can also import devices from an instance of IDS MC. Complete the following steps to import Sensors into the Security Monitor from a local or remote IDS MC server:

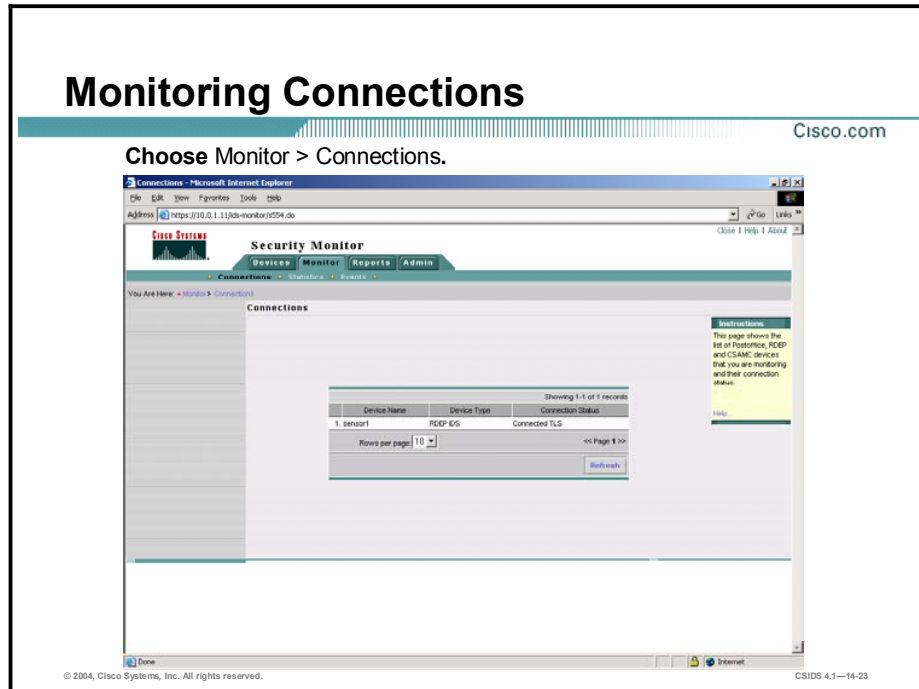
- Step 1** Choose **Devices**. The Devices page is displayed.
- Step 2** Click **Import**. The Enter IDS MC Server Information page is displayed.
- Step 3** Enter values for settings listed in the following table:

Security Monitor IDS MC Server Information Settings	Description
IP Address/Host Name	IP address or host name 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 4** Click **Next**. The Select Devices page is displayed.
- Step 5** Select the Sensors to import into the Security Monitor and click **Next**. The Update NAT addresses page is displayed.
- Step 6** Click **Finish**. The Summary page is displayed.
- Step 7** Click **OK**. The Devices page is displayed with the Sensor added to the Security Monitor.

Monitoring

This topic explains the monitoring capabilities of the Security Monitor.



You can monitor information about the devices that you have added to Security Monitor. This information can be classified in any of the following categories:

- Connections
- Statistics
- Events

The Security Monitor needs to communicate with all of the devices from which it receives information. With RDEP devices, the Security Monitor connects to the Sensor and retrieves the alerts. PostOffice devices send the information directly to Security Monitor. For RDEP and PostOffice devices, you can check the status of these connections by choosing **Monitor > Connections**.

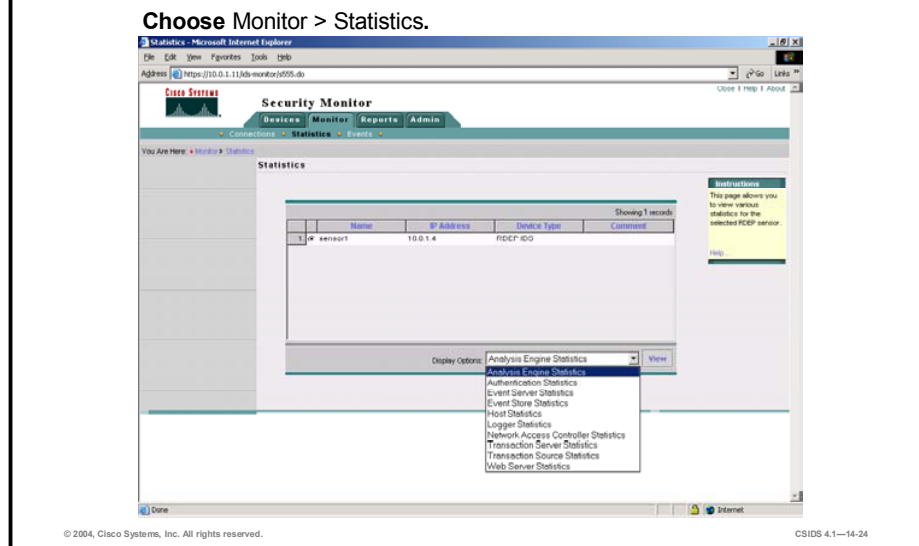
If the connection status is either Connected or Connected TLS, the Security Monitor is receiving events from the device correctly. A status of Not Connected represents a problem and may indicate one of the following conditions:

- The device has been added to the Security Monitor, but it 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. Verify 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.

- The Security Monitor has been misconfigured. Verify that the settings in the Security Monitor match those on the device. Also, verify that NAT settings have been configured properly.
- The Network connectivity between the device and the Security Monitor has been lost. Ping the device from the Security Monitor server. CiscoWorks contains several diagnostic tools, including ping and traceroute, in the Server **Configuration > Diagnostics > Connectivity Tools** folder.

Monitoring Statistics

Cisco.com

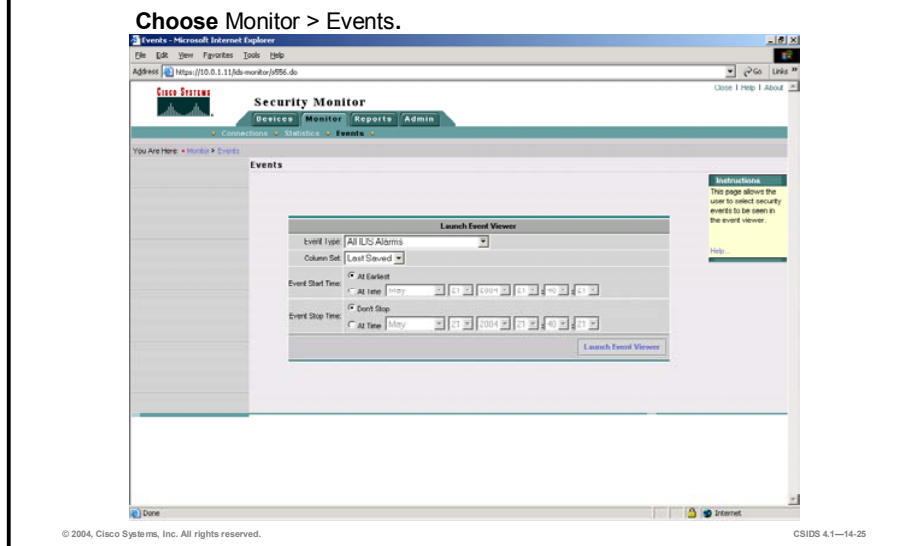


You can view a statistical report about various components of an RDEP device. The report is not updated in real time. It displays a snapshot of the device component at the time the report was run. Complete the following steps to display statistics for an RDEP device:

- Step 1** Select **Monitor > Statistics**. The Statistics page appears. All RDEP devices that you have added to Security Monitor are listed.
- Step 2** Select the device for which you want to view statistics.
- Step 3** Select the RDEP device component from Display Options list. You can select statistics from the following components:
 - 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
- Step 4** Click **View**. The report appears in a new browser window.

Monitoring Events

Cisco.com



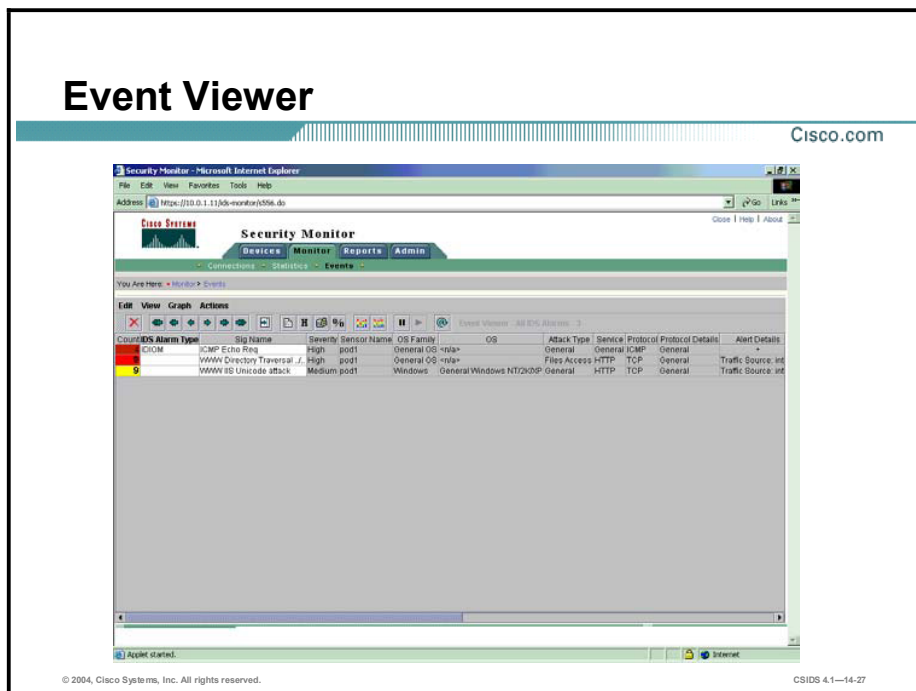
You can monitor the events that Security Monitor receives from all of the monitored devices. This is probably the most important feature of Security Monitor because it enables you to identify attacks against your network. Complete the following steps to use the Event Viewer to view the events that the Security Monitor has collected:

- Step 1** Select **Monitor > Events**. The Events page is displayed.
- Step 2** Choose the type of event you want to appear in Event Viewer by selecting an option from the Event Type list box.
- Step 3** Select one of the following options from the Column Set list box:
 - Last Saved—If you choose **Last Saved**, the Security Monitor queries the database to retrieve your customized set of columns.
 - Default—If you choose **Default**, the Security Monitor provides the set of columns provided with version 1.1 and earlier.
 - All—If you choose **All**, the Security Monitor provides all possible columns: the recommended columns and then all of the remaining columns.
- Step 4** Select one of the following options in the Event Start Time section to specify the oldest events that appear in Event Viewer.
 - Select **At Earliest** to view events starting with the oldest stored in the database.
 - Select **At Time** to specify a date and time from which you want to start displaying events.
- Step 5** Select one of the following options in the Event Stop Time section to specify the most recent events that appear in Event Viewer.
 - Select **Don't Stop** for real-time event analysis.
 - Select **At Time** to specify a date and time up to which you want to display events.
- Step 6** Click **Launch Event Viewer**. The Event Viewer appears.

Note Event start and stop times are the times at which events were stored in the database, not the time that the events were generated by the Sensor. Usually, the two times are close, if not identical. Storage and generation times differ greatly only if there are communication problems that postpone sending events from the Sensor to the database.

Customizing the Event Viewer

This topic explains how to customize the Security Monitor's Event Viewer.



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 display 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.

Customizing the Event Viewer

Cisco.com

Customizing the Event Viewer involves the following options:

- **Moving columns**
- **Deleting columns**
- **Deleting events**
- **Collapsing cells**
- **Expanding cells**
- **Setting the event expansion boundary**

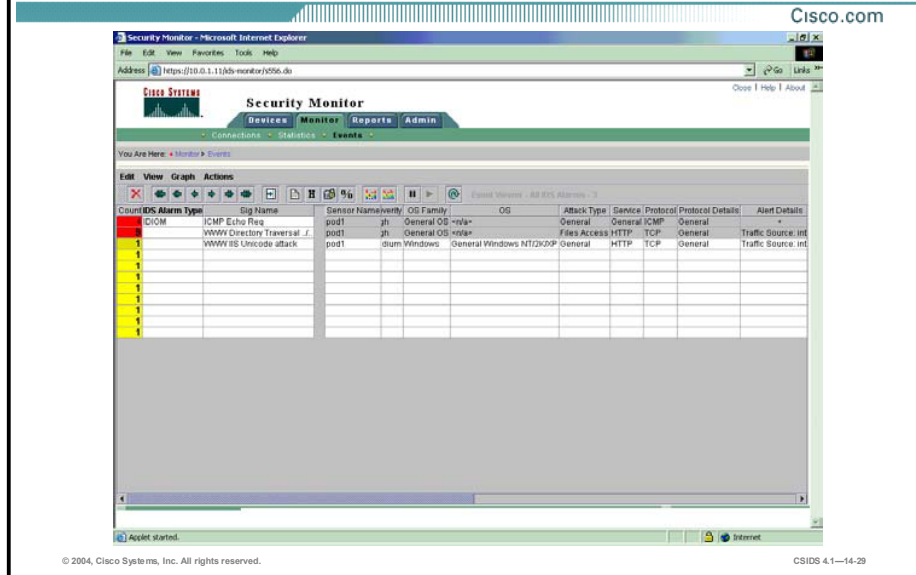
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-28

Customizing the Event Viewer involves understanding the following options:

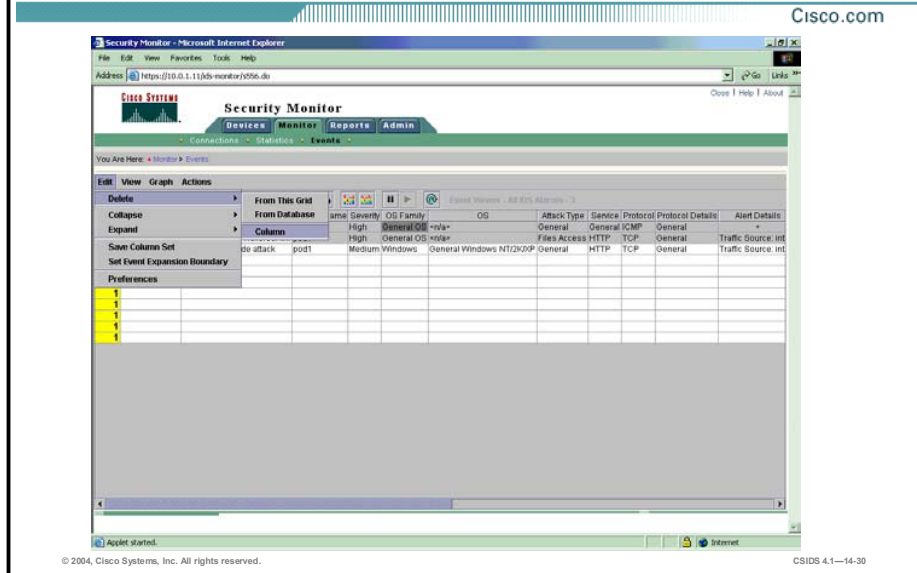
- **Moving columns**—To change the default order of fields within an alarm entry.
- **Deleting columns**—To remove columns from the Security Monitor grid.
- **Deleting events**—To remove an alarm from the Event Viewer grid or from the Security Monitor database.
- **Collapsing columns**—To reduce the number of lines displayed on the Event Viewer grid.
- **Expanding columns**—To expand the amount of alarm detail shown on the Event Viewer grid.
- **Setting the event expansion boundary**—To automatically expand more fields than the default.

Moving Columns



The default order of fields within an alarm entry may not suit 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.

Deleting Columns

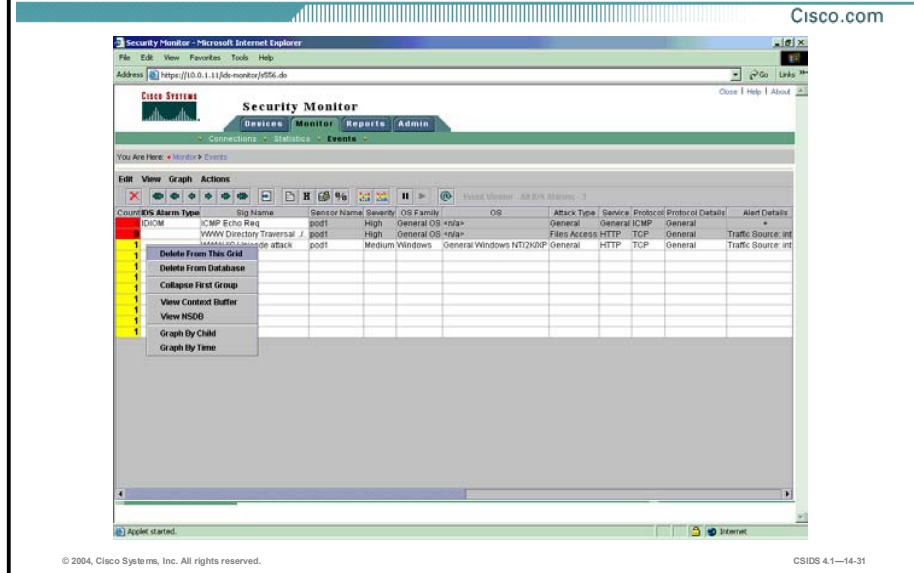


You can delete a column from the current Event Viewer display. Deleting a column from the current Event Viewer display does not delete the events in that column from the database, nor does it mark the events in that column for deletion from the database. To delete a column from the current Event Viewer display, complete the following steps:

- Step 1** Select any cell in the column that you want to delete.
- Step 2** Select **Edit > Delete > Column**. The Event Viewer display appears again, reflecting the deletion of the column that you selected.

Note You cannot delete the Count column.

Deleting Events from the Grid

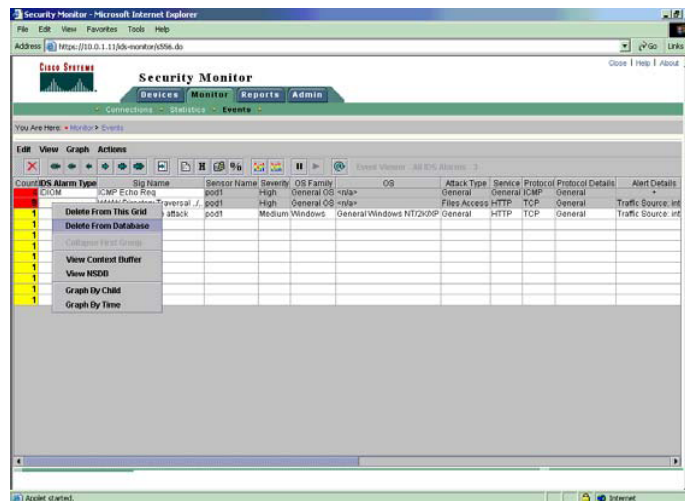


You can delete an event or set of events from the current Event Viewer display without removing these events from the database or other, concurrently running Event Viewers. To delete an event from the current Event Viewer display, complete the following steps:

- Step 1** Select a cell in the Event Viewer display.
- Step 2** Select **Edit > Delete > From this Grid**. The Event Viewer display appears again, reflecting the deletion of the cell that you selected.

Deleting Events from the Database

Cisco.com



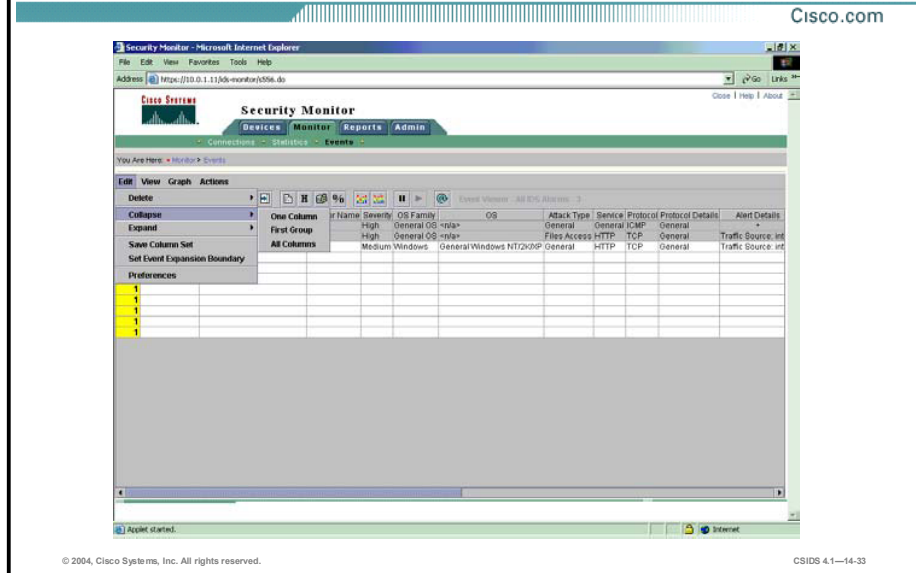
You can delete events from the database manually when you no longer need those events or when you want to reduce the size of the database. Deleting events manually involves executing a script at a command prompt. Other methods of deleting events involve using database rules, event rules, or Event Viewer.

Note Because of the way alarm data is stored in the database, there will not always be a one-to-one correspondence between the number of events deleted from the event display and number of records removed from the relational database.

Deleting events manually is the best method for deleting events that you no longer need. Manual deletion also is the best method to use when your database has grown larger than you want. Database rules and event rules can help you maintain the content and size of your database, but they are not as effective when you need to delete events because you have to wait for rules to be triggered. Deleting events through Event Viewer is best only when the number of events in the database is less than 1,000,000. To delete events through the Event Viewer, complete the following steps:

- Step 1** Select one or more cells in Event Viewer.
- Step 2** Select **Edit > Delete > From Database**.

Collapsing Cells



When a cell is collapsed, all branches that pass through the selected cell provide less detail. For each branch, the background color of the cells in the newly hidden column changes from white to gray. Also, rows are removed as necessary to conceal the appropriate data.

Note Collapsing does not delete anything; it merely hides data from view.

Events can be collapsed by one column, by first group, or all the way (all columns). If a cell is collapsed by one column, each branch through the selected cell gives one less column of detail. If a cell is collapsed by first group, Event Viewer traverses the tree from the selected node and collapses all nodes up the branch until a node with multiple child nodes is collapsed. If a cell is collapsed all the way, all branches through the selected cell are condensed into the selected cell.

To collapse a cell, complete the following steps:

- Step 1** Select a cell in Event Viewer. The selected cell is highlighted and outlined in gray.
- Step 2** Select **Edit > Collapse > One Column** to collapse a cell by one column. To collapse a cell by first group, select **Edit > Collapse > First Group**. To collapse a cell all the way, select **Edit > Collapse > All Columns**.

When a cell is expanded, all branches that pass through the selected cell provide more detail. For each branch, the background color of the cells in the newly filled-in column(s) changes from gray to white. Also, rows are created as necessary to display the exposed data.

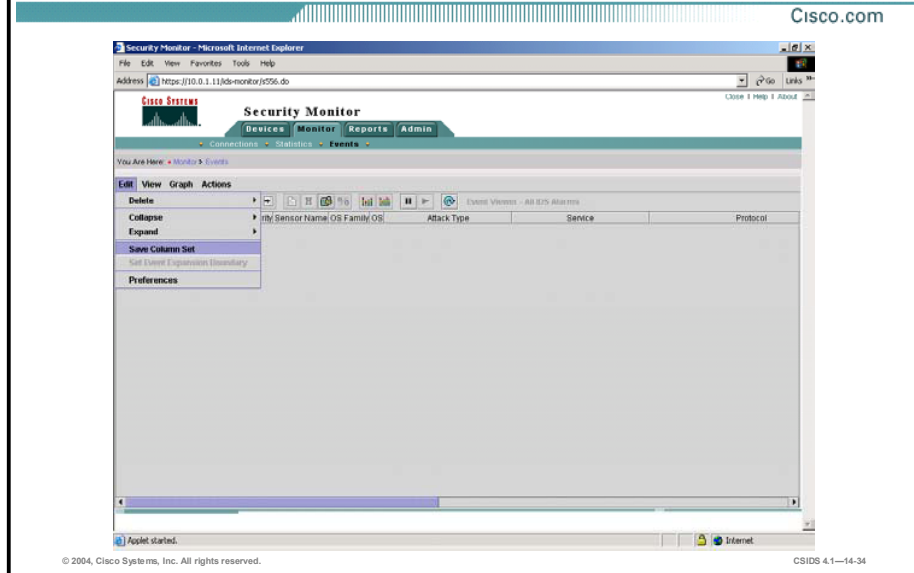
Event rows can be expanded by one column, by first group, and by all columns. If a cell is expanded by one column, each branch through the selected cell gives one more column of detail. If a cell is expanded by first group, Event Viewer traverses the tree from the selected node and expands all nodes down the branch until a node with multiple children is reached. If a cell is expanded all the way, all branches through the selected cell are fully expanded.

Sometimes expanding events can cause many rows to be created. If the number of new rows exceeds a certain maximum, a popup window asks you to confirm that you want to continue.

To expand a cell, complete the following steps:

- Step 1** Select a cell in the Event Viewer. The selected cell is highlighted and outlined in gray.
- Step 2** Select **Edit > Expand > One Column** to expand a cell by one column. To expand a cell by first group, select **Edit > Expand > First Group**. To expand a cell all the way, select **Edit > Expand > All Columns**.

Saving your Column Settings



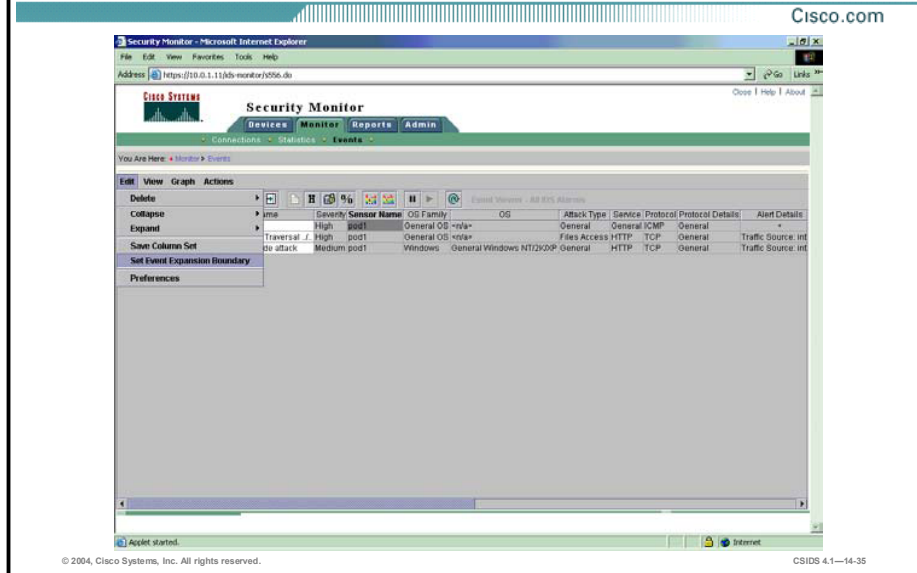
Column settings are not persistent. This means that closing the Event Viewer and re-opening it will bring back the default column ordering. However, you can save your column settings. You can specify and save the following information for a particular event type:

- Which columns are displayed
- The order in which the columns are displayed
- The sorting scheme for each column

Complete the following steps to save your column setting as your preferred column setting:

- Step 1** Start Event Viewer as explained in Starting Event Viewer. Be sure to select **Last Saved** from the Column Set list box.
- Step 2** Arrange columns as desired.
- Step 3** Select **Edit > Save Column Set**. Your current column setting is saved as your preferred column setting. It applies for the particular event type that you are monitoring.

Setting the Event Expansion Boundary



The Event Expansion Boundary represents the block of columns that will be expanded automatically 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 Event Expansion Boundary expands the first field of an alarm entry. When setting a new Event 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.

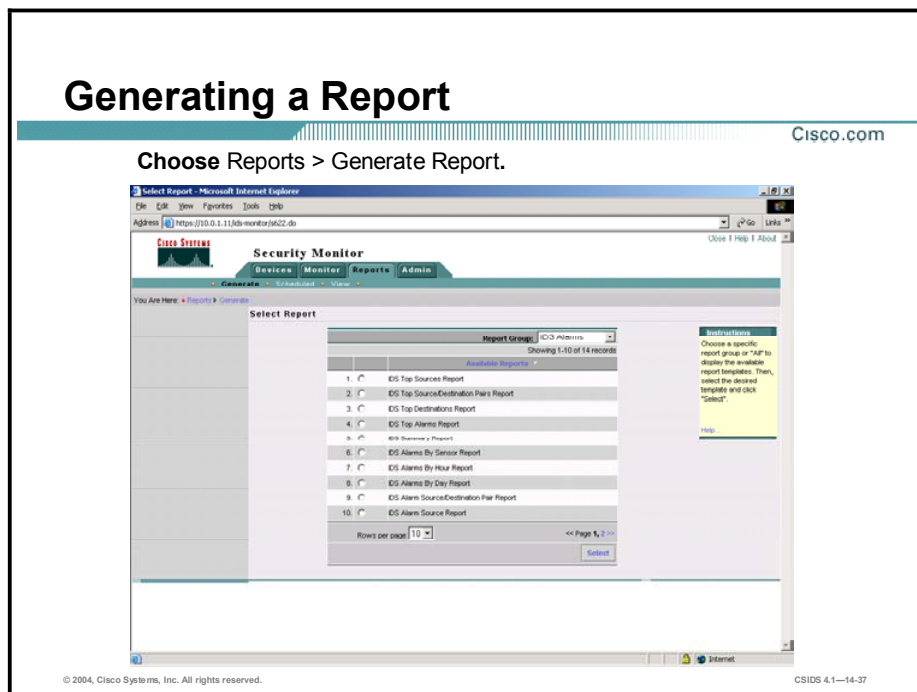
The Event Expansion Boundary represents the block of columns that will be automatically expanded when a new alarm entry comes into the table. The block of columns is contiguous and starts at the first column in the Event Viewer. By default the Event Expansion Boundary expands the first field of an alarm 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 then be expanded for new alarm entries.

Complete the following steps to set the Event Expansion Boundary:

- Step 1** To establish a column as the Event Expansion Boundary, select a cell in that column. The selected cell is highlighted and outlined in gray.
- Step 2** Select **Edit > Set Event Expansion Boundary**. The Event Expansion Boundary is set. The column heading is bold.

Reporting

This topic explains how to take advantage of the reporting capabilities of Security Monitor.



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 schedule them to be generated at a later time. Complete the following steps to generate a report:

- Step 1** Choose **Reports > Generate Report**. The Select Report page is displayed.
- Step 2** Use the Report Group drop-down menu to select one of the following report types:
 - Audit Log Reports—Provide information about system events.
 - IDS Alarms Reports—Provide information about the events being collected by the Security Monitor.
 - CSA Alarms Reports—Provide information about events generated by the Management Center for Cisco Security Agents.
 - Firewall Reports—Provide information about firewall events.
- Step 3** Select the report you want to generate.
- Step 4** Click **Select**. The Report Filtering page is displayed.

Generating a Report (Cont.)

Cisco.com

Report Filtering - Microsoft Internet Explorer
Address: https://10.0.1.1/ids-monitor/3619.do

Security Monitor
Generate | Schedule | View

You Are Here: Reports > Generate

Model: ASBING
1. Report Filtering
2. Report Scheduling

Report Filtering
Reporter: ES Top Sources Report

Event Level
Medium | Select All
Low | Clear All
Informational

Time/Date
 Since the dawn of time
 Last 30 Day(s)
Start: January 01, 2004 | America/Chicago
End: May 31, 2004 | America/Chicago

Destination Direction
Any

Destination IP Address
 Any Single Range
SingleStart: | | | | |
End: | | | | |

IDS Signatures
 Any signature
IDS Signatures:
(993-0) Missed Packet Count
(994-1) Traffic Flow Started
(994-2) Traffic Flow Stopped
(995-1) Traffic Flow Stopped
(995-2) Traffic Flow Stopped
Clear All

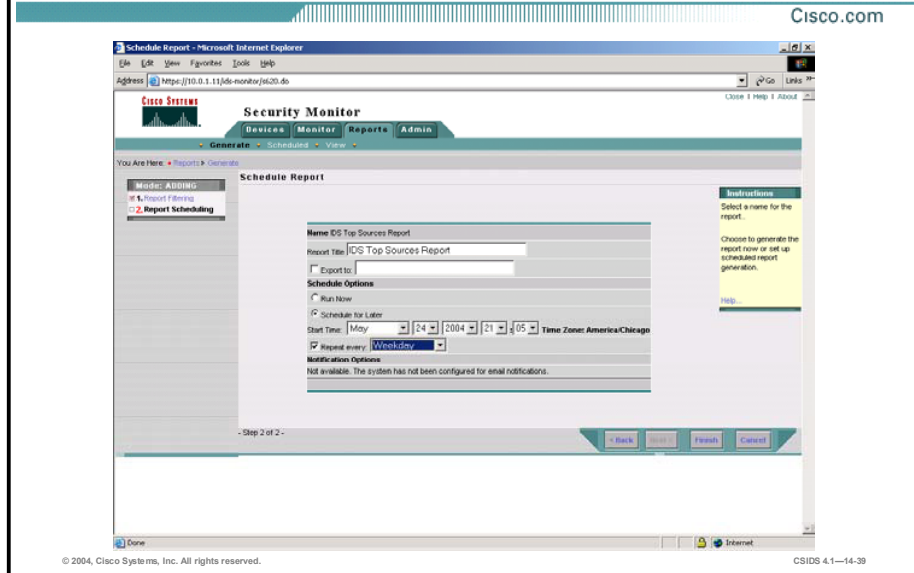
Instructions: Select any additional filtering for the report.
Tip: Selecting filter value(s) limits the results to those containing the value(s) that you select. For some filters, selecting no value or choosing filtering as all for that attribute. Selecting every filter value may not produce the same results as selecting no results (L1 ERROR) "Any".

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1-14-38

Step 5 The contents of the Report Filtering page depends on the report you choose to generate. Enter the report parameters for the report you selected.

Step 6 Click **Next**. The Schedule Report page is displayed.

Generating a Report (Cont.)

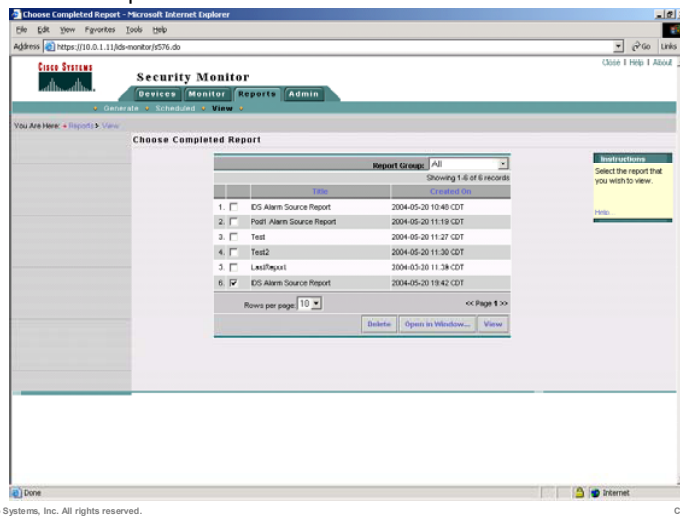


- Step 7** Enter a title for the report in the Report Title field.
- Step 8** To export the generated report to an HTML file, select the **Export to** check box. Then, specify the exact path to the file that will contain the generated report. The path should include the filename and the desired extension. No extension is appended to the filename if you do not specify an extension.
- Step 9** Click the **Run Now** or **Schedule for Later** radio button under Schedule Options. If you select Schedule for Later, specify the following options:
- Start Time—Specify the date and time that you want the report to run by using the Start Time drop-down menus.
 - Repeat every—Check the **Repeat every** check box and select one of the following options from the drop-down menu to run the report at regular intervals:
 - Day
 - Week
 - Weekday
 - Weekend day
 - Minute
 - Hour
- Step 10** To send an e-mail notification to someone when the report runs, select the **Email report to** check box and enter an e-mail address in the adjacent field. Use commas to separate multiple addresses.
- Step 11** Click **Finish** to submit the report. The following message is displayed:
Your report will be listed here when it is ready.
- Step 12** Click **OK**. The Choose Completed Report page is displayed.

Viewing Reports

Cisco.com

Choose Reports > View.



After you generate a report, you can view it. To view a report, complete the following steps:

- Step 1** Select **Reports > View**. The Choose Completed Report page is displayed.
- Step 2** Select the check box corresponding to the title of the report you want to view.
- Step 3** Click **View**. The report appears in the Report page. To view the report in a new browser window, click **Open in Window**. The report appears in a new browser window.

Administration

This topic describes how to administer the Security Monitor.



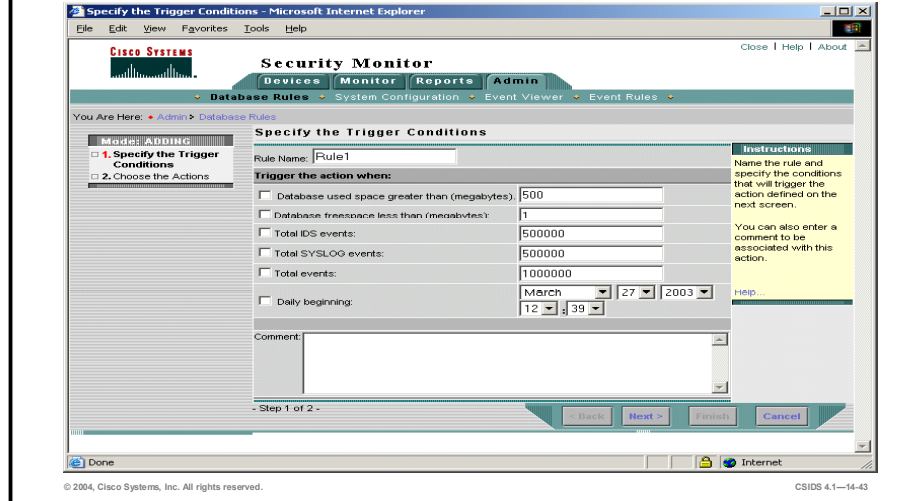
Although a large percentage of your time will be spent using the Event Viewer functionality of Security Monitor, there are also various tasks that you may need to perform to administer and maintain your Security Monitor software. Security Monitor server administration and maintenance falls into the following categories:

- Database management—This section allows you to manage the size of the database and disk files generated by the application.
- System configuration—The section allows you to manage system settings. If you are an administrator you can also update the Cisco 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—This 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.

Database Rules

Cisco.com

Choose Admin > Database Rules > Add.



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 or a certain number of events happen, or on a daily basis. The Security Monitor comes with the following 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.
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.

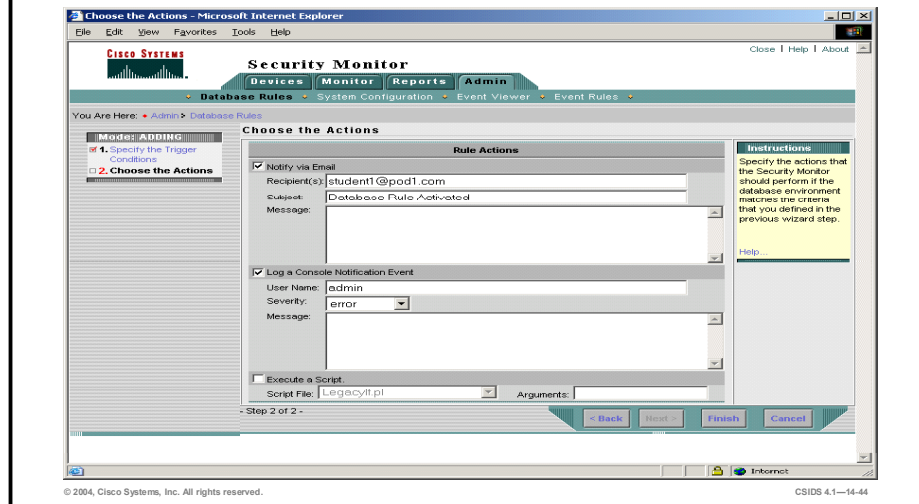
Security Monitor Trigger Condition Settings	Description
Total IDS Events	Check box that, if selected, triggers the database rule when the total number of IDS events is more than the number specified. The default is 500,000.
Total SYSLOG Events	Check box that, if selected, triggers the database rule when 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.

Database Rules (Cont.)

Cisco.com

Choose Admin > Database Rules > Add > Next.



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.

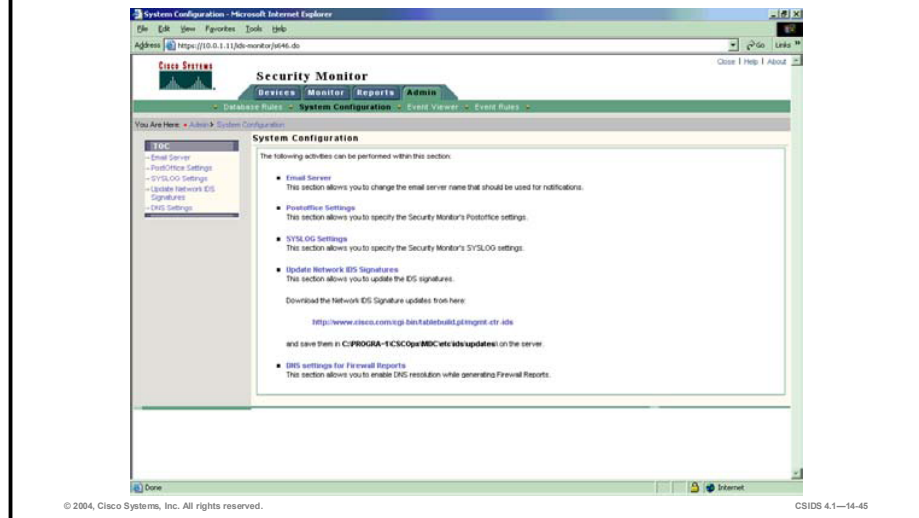
Step 5 Click **Finish**. The Database Rules page is displayed with the rule you just created.

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: `\CSCOp\MDC\etc\ids\scripts`. Running some scripts against the Security Monitor database can result in unexpected results. Use scripts with caution.

System Configuration Settings

Cisco.com

Choose Admin > System Configuration.



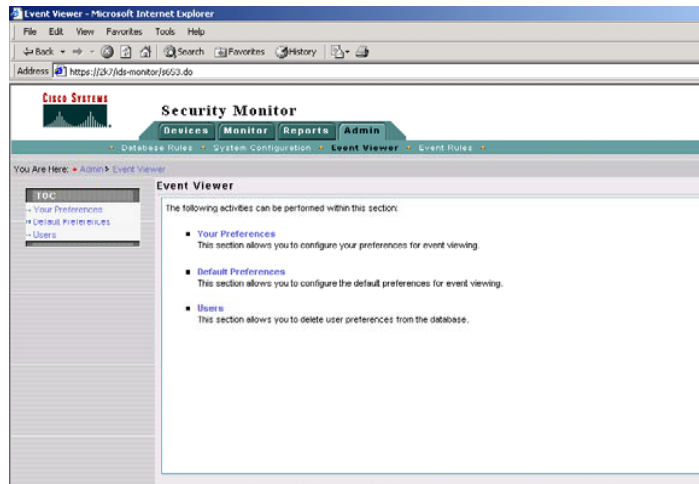
The Security Monitor enables you to administer the Security Monitor's system configuration. The following are options to configure for the Security Monitor:

- **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 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 subdirectory: `\CSCOp\MDC\etc\ids\scripts`. Running some scripts against the Security Monitor database can result in unknown results. Use scripts with caution.

Defining Event Viewer Preferences

Cisco.com



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.
- **User Preferences**—Allows you to delete user preferences from the database.

Event Notification

Cisco.com

- **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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-47

When one or more security devices are deployed to protect a network, they can generate large amounts of event data. Monitoring this data for specific events or a specific pattern of events can be difficult. Security Monitor uses event rules to monitor for specific events or patterns of events. Event rules have the following three parts:

- Event filters
- The action that you want to occur when filter conditions are met
- The thresholds and intervals for the actions you define

Event rules allow 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. The actions available are as follows:

- Sending an e-mail notification.
- Logging a console notification to the audit log.
- Executing a script.

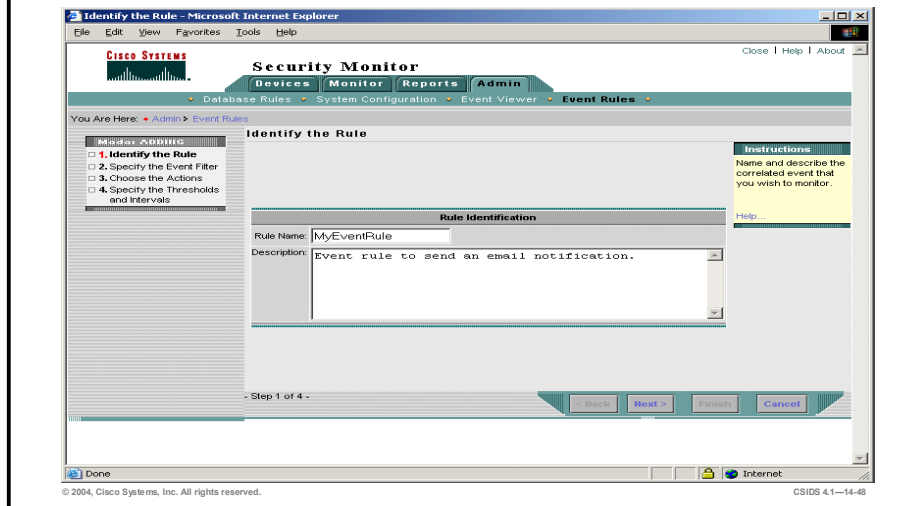
Event rules use IDS events, which can come from a Sensor appliance or module, a PIX Firewall, a Cisco router running Cisco Intrusion Detection System software, or a Cisco IDS host console. Event rules do not use firewall events, which can come from a PIX Firewall or a Cisco IOS device running the firewall feature set. However, firewall events are collected and stored in the database by Security Monitor. 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

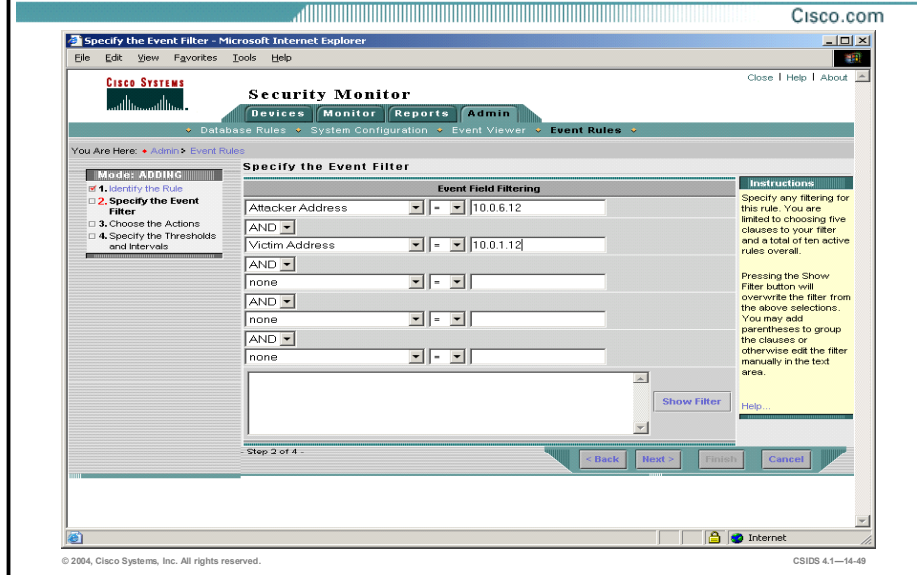
Cisco.com

Choose **Admin > Event Rules > Add**.



- 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.

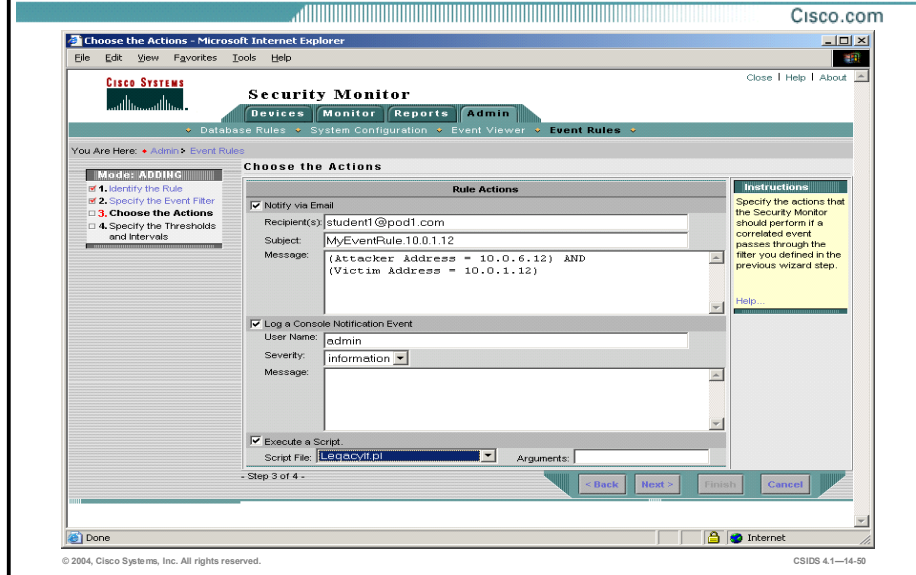
Event Rules—Step 2



Step 4 Use the drop-down menus 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



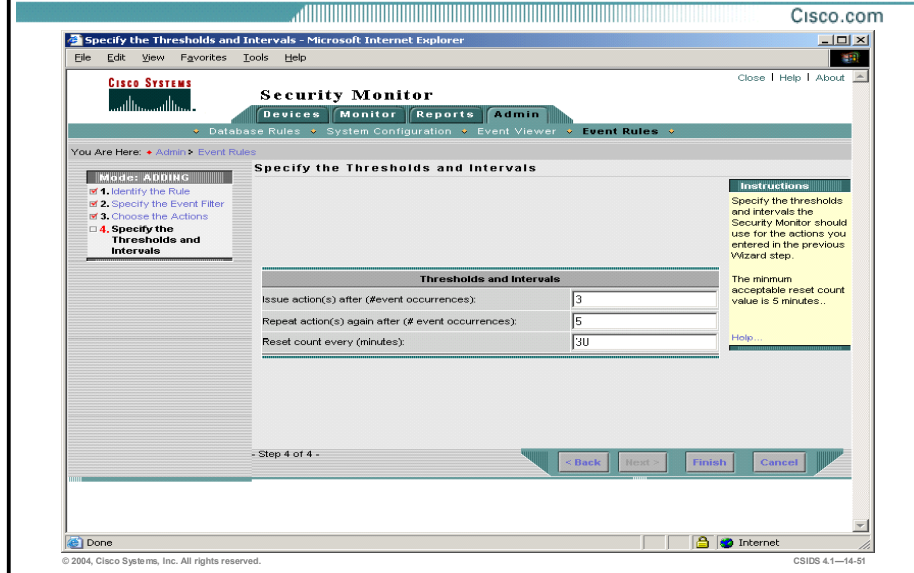
Step 6 Enter values for settings listed in the following table:

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



Step 8 Enter the threshold in the Issue actions after field, the Repeat actions again after field, and the Reset count every field.

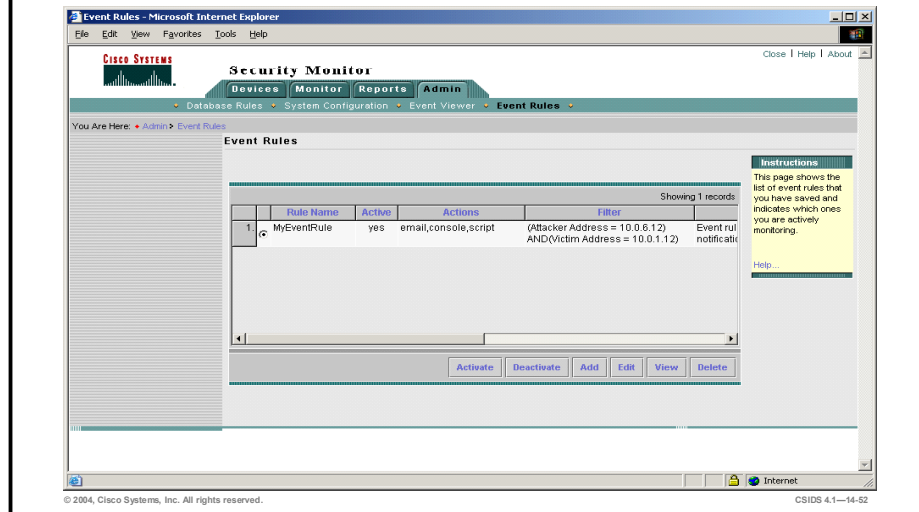
Step 9 Click **Finish**.

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: `\CSCOp\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**.



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.

Cisco Threat Response

This topic explains the capabilities of Cisco Threat Response.

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 by up to 95%**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—14-54

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:

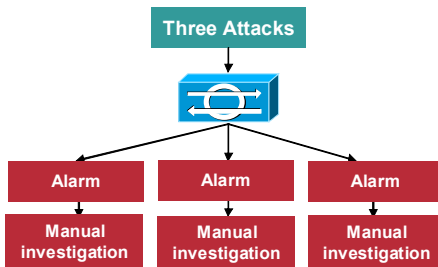
- Examines every alert your Sensor generates
- Eliminates false alarms and escalates real attacks—By inspecting the targeted host to assess what, if any damage, has been perpetrated, Threat Response is able to eliminate false and fruitless alarms. By the same token, it escalates true alarms so that they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

Cisco.com



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 the Security Monitor displays several real attack events.

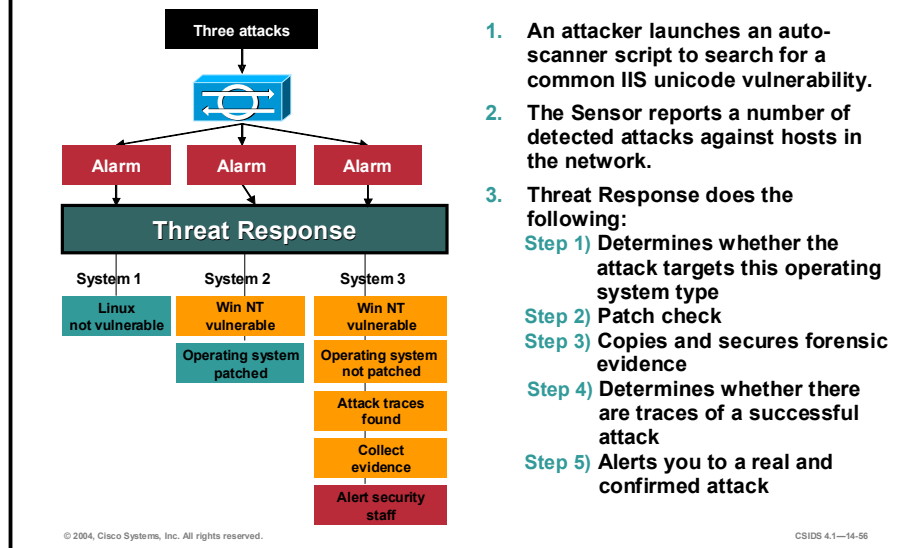
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-55

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

Cisco.com



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 is 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.

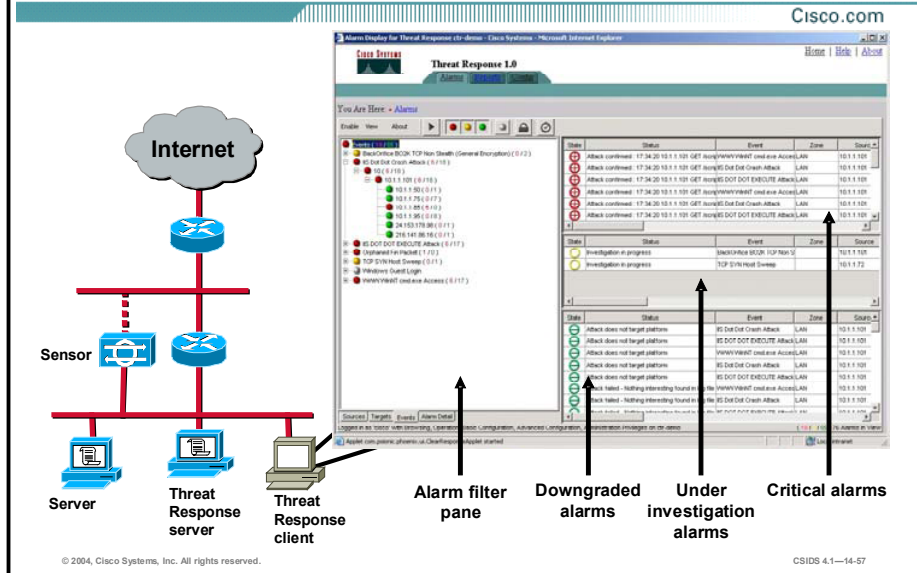
Step 4 Checks for other signs of intrusion. Discovers dropper files and other evidence.

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



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

Summary

This topic summarizes the information you learned in this lesson.

Summary

Cisco.com

- **The Security Monitor is a component of the CiscoWorks 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:**
 - **Sensor appliances**
 - **IDS Services Modules**
 - **IDS Network Modules**
 - **Cisco IOS routers**
 - **PIX Firewalls**
 - **Firewall Services Modules**
 - **CSA MCs**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-58

Summary (Cont.)

Cisco.com

- To efficiently monitor the events from multiple devices on your network, you can configure the Security Monitor event rules.
- Event rules enable you to perform one of the following actions when the Security Monitor receives certain events:
 - Send an e-mail 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.
- Threat Response performs just-in-time analysis of target hosts to assess damage while discriminating between successful and unsuccessful attacks.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—14-60

Cisco Intrusion Detection System Network Module

Overview

This lesson provides information on the Cisco Intrusion Detection System Network Module (NM-CIDS). This lesson includes the following topics:

- Objectives
- NM-IDS overview
- How the NM-CIDS works
- Design considerations
- Installation and configuration tasks
- Maintenance tasks unique to the NM-CIDS
- Summary
- Lab exercise (Optional.)

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

- Describe the Cisco NM-CIDS.
- Explain how the NM-CIDS works.
- List the tasks for configuring the NM-CIDS.
- Describe maintenance tasks for the NM-CIDS.

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—15-3


NM-CIDS Overview

This topic describes the key features, specifications, and benefits of the NM-CIDS.

Key Features

Cisco.com

- **Integrates IDS into several Cisco access router platforms**
- **Provides full-featured intrusion protection**
- **Runs the IDS 4.1 Sensor software**
- **Able to monitor traffic from all router interfaces**
- **Able to inspect GRE and IPSec traffic that has been decrypted at the router**
- **Delivers comprehensive intrusion protection at branch offices, isolating threats from corporate network**



© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—15-5

The NM-CIDS is a fully featured IDS Sensor that provides the ability to inspect all traffic traversing a router. It is factory-loaded with the Cisco Intrusion Detection System (IDS) 4.1 Sensor software and is at feature and function parity with the other implementations of Cisco IDS, such as the Sensor appliance and the Intrusion Detection System Module 2 (IDS-M-2); therefore, it can be managed and monitored with the same applications as the other Cisco IDS Sensor devices.

The NM-CIDS can monitor traffic from all interfaces on the router, including inside and outside interfaces. Through collaboration with IPSec virtual private network (VPN) and Generic Routing Encapsulation (GRE) traffic, it can allow decryption, tunnel termination, and traffic inspection at the first point of entry into the network (an industry first). When GRE or IPSec tunnels terminate at the router, the module is able to monitor the decrypted traffic.

The NM-CIDS fits into a single network module slot on the Cisco 2600XM Series, 2691, 3660, 3725, and 3745 routers. Only one NM-CIDS is supported in a given router, but it is not restricted to a specific network module slot within the router.

By integrating IDS and branch office routing, it reduces the complexity of securing WAN links while offering reduced operating costs. The NM-CIDS also simplifies power management by using the power options on the router.

The NM-CIDS uses a separate processor to maximize performance. This design frees the router CPU from any processor-intensive IDS tasks.

Specifications

Cisco.com



Performance	45 Mbps
Interface	Onboard external 100mb interface for command and control and internal 100mb interface for monitoring
Routers supported	2600XM, 2691, 3660, 3725, 3745
Cisco IOS software	12.2(15)ZJ or later
2691/3700 ROM version	12.2(8r)T2 or later
IDS Sensor software	IDS 4.1

© 2004, Cisco Systems, Inc. All rights reserved.

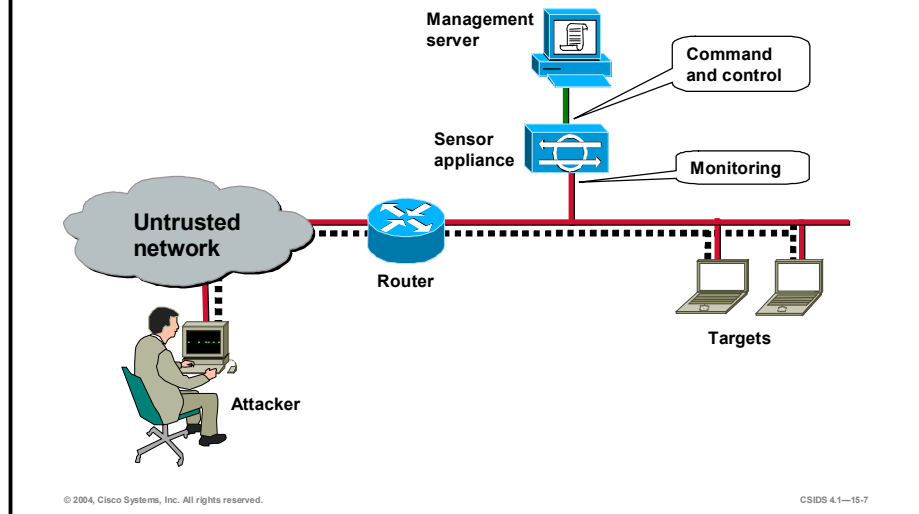
CSIDS 4.1—15-6

The following are some of the technical specifications of the NM-CIDS:

- **Performance**—The NM-CIDS can monitor up to 45 Mbps of traffic, which is suitable for T1/E1 and T3 environments.
- **Interfaces**—The NM-CIDS has the following interfaces:
 - One external 100-Mbps Fast Ethernet port, which is used as the command and control interface
 - One internal 100-Mbps interface, which is connected to the internal router port and is used for monitoring
- **Routers supported**—The NM-CIDS is supported on the Cisco 2600XM Series, 2691, 3660, 3725, and 3745 routers.
- **Cisco IOS software**—The NM-CIDS works with any Cisco IOS firmware or IDS feature license that is in Cisco IOS Software Release 12.2(15)ZJ or later. Refer to the NM-CIDS data sheet for a complete list of the Cisco IOS software images.
- **ROM version**—When using the 2691 and 3700 routers, the ROM version must be 12.2(8r)T2 or later.
- **IDS Sensor software**—The NM-CIDS uses the same Cisco IDS Sensor Version 4.1 software as the other Cisco IDS platforms.

Traditional Cisco IDS Network Architecture

Cisco.com



Before the NM-CIDS, the traditional network architecture for a branch office included two devices, the router and a dedicated Cisco IDS Sensor. This solution typically consists of a Cisco 26xx, 36xx, or 37xx branch office router connected to a Sensor. The Cisco IDS Sensor portfolio for the branch office consists of the Cisco IDS 4210 and 4215 and the 4235 platforms. Each Sensor functions as an external appliance that typically has two Fast Ethernet interfaces, one for packet monitoring and the other for command and control.

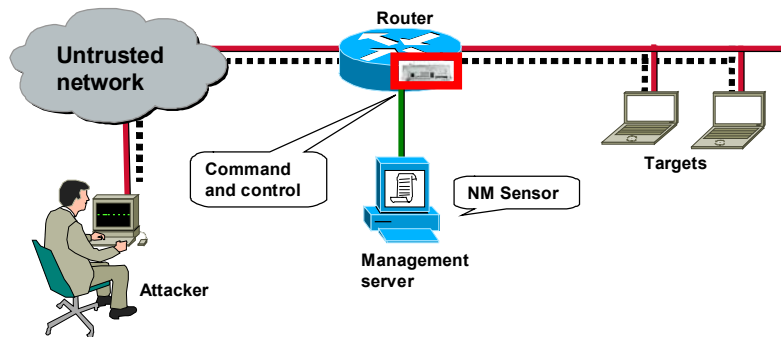
Little to no configuration is required on the branch router, and the branch router's CPU is only affected to the extent that it processes WAN traffic to the correct LAN interface. This process should not tax the router, so the CPU utilization should remain low.

The Cisco IDS Sensors run their own Cisco IDS software. The router's Cisco IOS software is not affected if a signature file needs to be updated. Since the router is not actively participating in the IDS inspection, the level of performance that can be inspected within a network increases dramatically. For example, the IDS 4215 can inspect up to 80 Mbps, and the IDS 4235 can inspect up to 250 Mbps.

There are some disadvantages to using this solution. The Cisco IDS solution is a two-box solution that affects the real estate needs within your branch office and adds complexity to your network management solution, compared to a one-box solution.

Network Architecture with NM-CIDS

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-8

The scenario in the figure is similar to the one on the previous page; however, in this scenario, the network architecture includes the NM-CIDS. The NM-CIDS integrates the functionality of the Cisco IDS Sensor into the branch router. The NM-CIDS is physically installed in a network module slot inside a Cisco 2600XM, 2691, 3660, 3725, or 3745 router. This provides a one-box IDS solution and the ability to monitor all the router's interfaces.

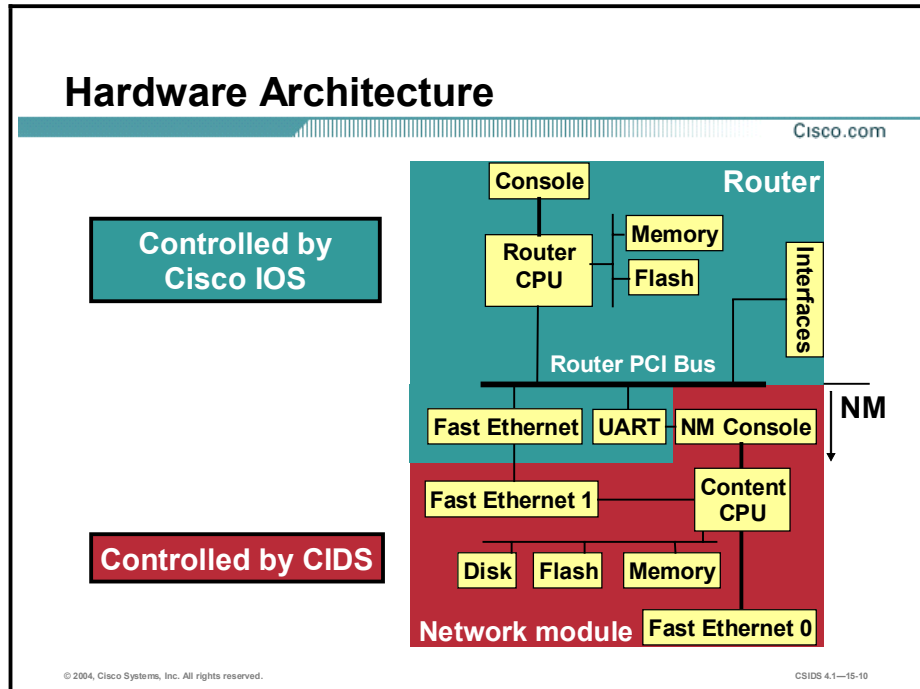
The NM-CIDS is directly connected to the router's backplane via an internal Fast Ethernet interface onboard the NM-CIDS. This internal interface serves as a monitoring port for traffic. Traffic entering the branch office from the WAN interface no longer needs to be ported to the LAN interface as is required for the Sensor appliance solution; rather, the data is copied across the backplane to the internal Fast Ethernet monitoring port of the NM-CIDS.

As with Cisco IOS-IDS, WAN interface traffic can be inspected without having to be routed to a LAN interface. However, the NM-CIDS also has an advantage over the Cisco IOS-IDS solution because it runs the same CIDS 4.1 Sensor software as the Sensor appliance. This feature allows support for a greater number of signatures and ease of signature update.

The disadvantage to this solution is that it impacts the performance of the router. Although the actual packet inspection function is offloaded to the NM-CIDS module, the router must copy packets to the module, which places an additional load on the router's processor.

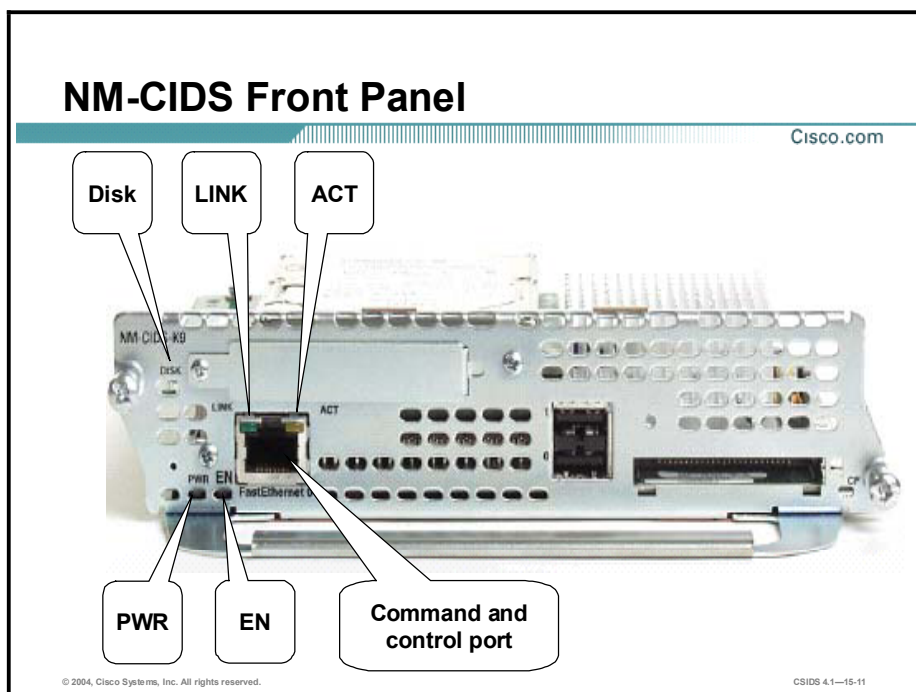
How the NM-CIDS Works

This topic describes the architecture and functionality of the NM-CIDS.



The NM-CIDS provides interface-level packet monitoring capability. You can select one or more router interfaces or subinterfaces for IDS monitoring. The following are the hardware components of the router and NM-CIDS that enable this functionality:

- Internal Fast Ethernet interface—Connects to the internal PCI bus on the router's backplane to provide monitoring capability. This internal Fast Ethernet interface provides a 100-Mbps full-duplex interface between the router and the NM-CIDS. The router sends a copy of each packet to be inspected from its PCI bus to this internal Fast Ethernet interface. The packets are passed through the internal monitoring interface for classification and processing. The router-side interface for the internal Ethernet segment is known as interface `ids-sensor` in the Cisco IOS software. This interface is the only interface associated with the IDS that is visible in the output of the **show interfaces sensing** command. The router-side internal interface is connected to the router PCI backplane.
- External Fast Ethernet interface on the NM-CIDS—Used as the command and control port. This interface can be connected to a switch, to a hub, or directly to a workstation with IDS management software.
- Internal Universal Asynchronous Receiver/Transmitter (UART) interface—Provides a virtual console access to the NM-CIDS from the backplane of the router. The NM-CIDS differs from a standalone IDS appliance in that it does not have an external console port. The internal UART interface is used to provide the console access. Console access to the NM-CIDS is enabled when you issue a **service-module ids-sensor <slot>/0 session** command from the Cisco IOS command line interface (CLI).
- NM-CIDS disk, Flash, and memory—The NM-CIDS has its own disk, Flash, and memory rather than sharing that of the router.



The following features are available on the front panel of the NM-CIDS:

- One Fast Ethernet connection (FE0)
- LED indicators:
 - ACT—Displays activity on the Fast Ethernet connection
 - DISK—Displays activity on the IDS hard-disk drive
 - EN—Indicates that the NM-CIDS has passed self-test and is available to the router
 - LINK—Is lit when the Fast Ethernet connection is available to the NM-CIDS
 - PWR—Indicates that power is available to the NM-CIDS

Traffic Capture for the NM-CIDS

Cisco.com

Traffic capture for the NM-CIDS is characterized by the following:

- Cisco IOS software provides interface-level and subinterface-level packet monitoring capability.
- The forwarding of packets to the NM-CIDS is implemented in the CEF switching path of the Cisco IOS software.
- Some of the Cisco IOS forwarding features and services implemented within CEF can impact NM-CIDS packet analysis.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-13

The forwarding of packets to the NM-CIDS is implemented in the Cisco Express Forwarding (CEF) switching path of Cisco IOS software. CEF is advanced Layer 3 IP switching technology supported in Cisco IOS Software Releases 12.0 and later. CEF mode must be enabled at the router CLI in order for the router to forward packets to the NM-CIDS. Several Cisco IOS forwarding features and services are implemented within CEF architecture. Based on which feature or service is configured, these features are processed in a sequence. The content of packets may be altered after processing certain features, and altered packets can impact the monitoring done by the NM-CIDS.

Design Considerations

This topic discusses Cisco IOS features require special consideration when used with NM-CIDS monitoring.

Cisco IOS Features That Require Special Consideration When Using the NM-CIDS

Cisco.com

The following Cisco IOS software features require special consideration when used with NM-CIDS monitoring:

- ACLs
- Encryption
- NAT
- IP multicast
- UDP flooding
- IP broadcast
- GRE tunnels

© 2004, Cisco Systems, Inc. All rights reserved.

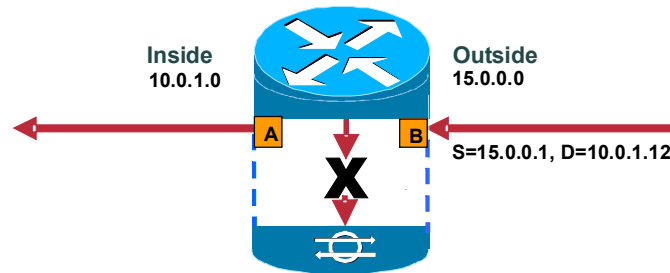
CSIDS 4.1—15-15

As explained in the preceding topic, the contents of a packet may be altered after processing certain Cisco IOS forwarding features such as Network Address Translation (NAT). The following is a list of the features whose processing can impact the operations of the NM-CIDS:

- Access control lists (ACLs)
- Encryption
- NAT
- IP multicast
- UDP flooding
- IP broadcast
- GRE tunnels

NM-CIDS and Input ACLs

Cisco.com



```
router(config)# access-list 101 deny ip 15.0.0.0 0.0.0.255 any
router(config)# interface FastEthernet 0/0
router(config-if)# ip access-group 101 in
```

- Packets that are dropped by inbound ACLs are not forwarded to the NM-CIDS.

© 2004, Cisco Systems, Inc. All rights reserved.

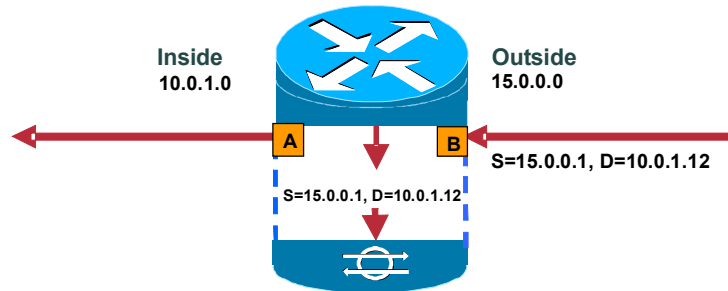
CSIDS 4.1—15-16

The Cisco IOS-IDS implementation checks for certain signatures before an input ACL filters the packet. The purpose is to look for any possible attacks that were destined for the network before they were dropped by the router.

Such scheme is difficult to implement with the NM-CIDS. The router sends a copy of the packet to the NM-CIDS, and it is desirable to send only one copy of the packet. If the packet is forwarded to the NM-CIDS even before it is dropped, the router has to send another copy of the packet after the packet is decrypted (if encryption is enabled) or when the IP address is changed because of NAT. To avoid sending multiple copies of packets to the NM-CIDS, the router does not forward any packet that should be dropped according to an input ACL.

NM-CIDS and Output ACLs

Cisco.com



```
router(config)# access-list 101 deny ip 15.0.0.0 0.0.0.255 any
router(config)# interface FastEthernet 0/1
router(config-if)# ip access-group 101 out
```

When output ACLs are configured in the Cisco IOS, the router:

- Performs output-ACL check after the packet is forwarded to the NM-CIDS.
- Forwards the packet to the NM-CIDS even if the output ACL drops the packet.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-17

The Cisco IOS software performs an input-ACL check on a packet before it processes the packet for NAT or encryption. As explained earlier, the NM-CIDS analyzes the packet after NAT and decryption are processed. Therefore, if the packet is dropped by the inbound ACL, it is never forwarded to the NM-CIDS. However, the Cisco IOS software performs output-ACL check after the packet is forwarded to the NM-CIDS, so the packet is forwarded to the NM-CIDS even if the output ACL drops the packet.

NM-CIDS and Encryption

Cisco.com

Encryption is handled by the router and NM-CIDS as follows:

- **If an IPSec tunnel terminates on the router, intrusion detection is handled as follows:**
 - **The router decrypts incoming packets and then sends them to the NM-CIDS.**
 - **The router encrypts outgoing packets after copying them to the NM-CIDS.**
- **Pass-through IPSec traffic is not interpreted by the NM-CIDS.**
- **The NM-CIDS cannot interpret encrypted packets for Layer 4 and above signatures.**

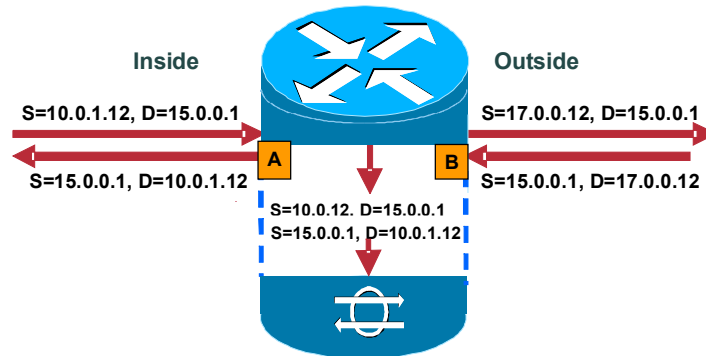
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-18

If an IPSec tunnel is terminated at the router, the router decrypts incoming packets before passing them to the NM-CIDS. It encrypts outgoing packets after copying them to the NM-CIDS. Therefore, the NM-CIDS can fully analyze those packets. However, if encrypted traffic is merely passed through the router, the router does not decrypt it and passes the packets to the NM-CIDS in the encrypted state. The NM-CIDS cannot analyze those encrypted packets.

NM-CIDS and Inside NAT

Cisco.com



- **Only the untranslated inside source address is sent to the NM-CIDS for processing. This facilitates identification of the inside target.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-15-19

Network Address Translation (NAT) is a common router feature that can be configured to change the source or destination address of a packet. The IDS signature engines maintain the TCP session states for all TCP sessions they monitor. The engines need to analyze packets in both directions in order to adequately analyze TCP sessions. The source and destination IP addresses of the bidirectional packets must be consistent. NAT can impact the ability of the Sensor to determine a true source or destination address.

In the figure, interfaces A and B are configured on the router. Interface A is on the inside of the NAT domain, while B is on the outside. The packet entering interface A has a source address of 10.0.1.12 and a destination address of 15.0.0.1. The router processes the packet and sends it to the outbound interface, changing the source address of the outbound packet to 17.0.0.12. The outside domain sees this address as the IP address of the host inside the NAT domain.

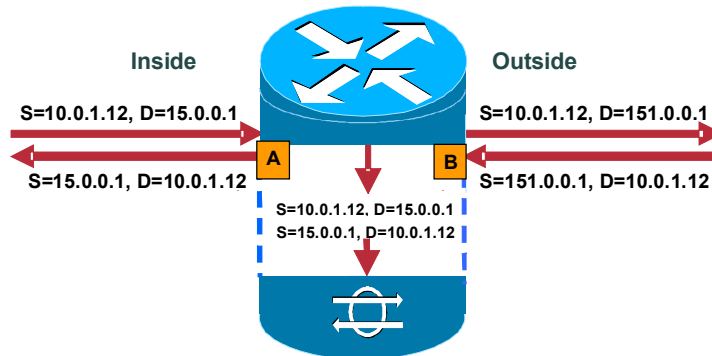
When the return packet arrives on interface B, the source IP address is 15.0.0.1, while the destination IP address is 17.0.0.12. The router translates the destination address to 10.0.1.12, and sends the packet out interface A.

If a 10.0.1.12 address is recorded by the NM-CIDS as the source address for packets moving from interface A to interface B but a 17.0.0.12 address is recorded as the destination in the return packet moving from interface B to interface A, the NM-CIDS is unable to maintain consistent session state. In order for session state to be accurately maintained, either the 10.0.1.12 address or the 17.0.0.12 address must be recorded.

The outside or global IP addresses are often dynamically assigned and shared. If outside IP addresses were sent to the NM-CIDS it would be difficult to identify which of the hosts on the inside network was attacked. Therefore, the router sends only the inside IP addresses to the NM-CIDS. In the scenario in the figure, only the 10.0.1.12 address is sent.

NM-CIDS and Outside NAT

Cisco.com



- A device's real global address (151.0.0.1) is seen on the inside as 15.0.0.1.
- Only the translated address is sent to the NM-CIDS for processing.
- The attacker's real address is not displayed in the alarm, so the source of the attack may not be easily traced.

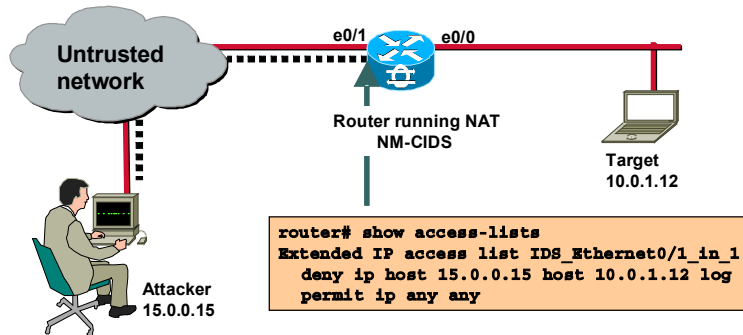
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-20

The case just explained describes inside NAT, inside local to inside global translation. The example in this figure explains the router's behavior in relation to the NM-CIDS when outside NAT, or outside local to outside global translation, is configured. The global address 151.0.0.1 is seen as 15.0.0.1 by the inside network. The inside address 10.0.1.12 is passed untranslated by the router. The NM-CIDS analyzes the packet with the 15.0.0.1 address. When an attack is detected, the alarm contains information about the 15.0.0.1 address, and the attacker's actual address, 151.0.0.1, is not displayed. This means that the attack source may not be easily traced.

NM-CIDS, NAT, and Blocking

Cisco.com



- The NM-CIDS currently supports blocking only on source address.
- Only external interfaces can be used for blocking. This enables NAT and blocking to work together within the same router.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—16-21

IDS Sensors can generate ACLs and apply them to router interfaces after detecting intrusion activity. This capability is called blocking. You can select the interfaces on the router where the ACLs should be applied. If you select multiple interfaces, the same ACL is applied to all of them.

To avoid problems that could result from running NAT on a router containing an NM-CIDS that initiates blocking, the following guidelines have been established for blocking and the NM-CIDS:

- The NM-CIDS currently supports blocking only on the source address.
- Only external interfaces can be used for blocking.

If the NM-CIDS in the figure supported blocking on both the source and destination addresses and allowed you to use any interface for blocking, NAT could render the blocking ACLs ineffective. For example, if the NM-CIDS detected an intrusion on a packet flow between 15.0.0.15 and 10.0.1.12, it would generate an ACL to block all traffic with source address 15.0.0.15 and destination address 10.0.1.12. If this ACL is applied on interface e0/1, it works fine. However, if the following two conditions exist, the packet originating from the 15.0.0.15 attacker has the destination address 17.0.0.12, which renders the ACL ineffective:

- NAT is configured to translate inside address 10.0.1.12 so that it is seen as 17.0.0.12 by the outside network.
- The ACL is applied to interface e0/0.

Special Considerations for Using the NM-CIDS

Cisco.com

- **IP multicast, UDP flooding, and IP broadcast**
 - **The input interface must be configured for IDS monitoring. If only the output interfaces are configured for monitoring, the packet is not forwarded to the NM-CIDS.**
- **GRE**
 - **If the router in which the NM-CIDS is installed receives a GRE-encapsulated packet, the packet is not forwarded to the NM-CIDS.**
 - **If the router in which the NM-CIDS is installed encapsulates the packet into a GRE tunnel, the packet is analyzed by the NM-CIDS before encapsulation.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-22

Other features that can affect NM-CIDS operations include the following:

- **IP multicast, UDP flooding, and IP broadcast**—If the router is configured for IP multicast, UDP flooding, or IP broadcast, a packet received on input interface is forwarded on two or more output interfaces. In this situation, if the input interface is configured for IDS monitoring, the packet is sent to the NM-CIDS. However, if only the output interfaces are configured for monitoring, the packet is not forwarded to the NM-CIDS.
- **GRE tunnels**—The NM-CIDS does not analyze GRE encapsulated packets. If a GRE packet is received and the incoming interface is enabled for IDS monitoring, the packet is not forwarded to the NM-CIDS for monitoring. However, if the router encapsulates a packet in a GRE tunnel and the incoming interface is enabled for IDS monitoring, the packet is sent to the NM-CIDS before encapsulation.

Packets Not Forwarded to NM-CIDS

Cisco.com

The following packets are not inspected by the NM-CIDS:

- **Packets not forwarded to the NM-CIDS**
 - ARP packets
- **Packets dropped by Cisco IOS software**
 - Bad IP version
 - Invalid IP option
 - Bad header length
 - Any header error
 - Total length greater than 1548 bytes or less than 20 bytes
 - IP CRC failure
 - TTL less than 1

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—16-23

There are other cases in which the packet is not inspected by the NM-CIDS. For example, Address Resolution Protocol (ARP) packets are not forwarded to the NM-CIDS. Therefore, ARP-based signatures are missed by the NM-CIDS. In addition, Cisco IOS software examines the IP header of all packets and drops any packet that contains an error, such as an irregularity in a field. Possible irregularities include the following:

- Bad IP version
- Incorrect IP option field
- Bad header length
- Total packet length greater than 8192 bytes or less than 20 bytes
- IP cyclic redundancy check (CRC) failure
- Time to Live (TTL) less than 1

Installation and Configuration Tasks

This topic explains how to install and configure the NM-CIDS.

Configuration Tasks

Cisco.com

Configuration tasks are the same as those for the Sensor appliance with the following exceptions:

- **Initial configuration requires establishing a session from the router console.**
- **The NM-CIDS clock cannot be set directly. One of the following must be used:**
 - **Router's clock**
 - **NTP server**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-25

The configuration tasks for the NM-CIDS are similar to those of the IDS Sensor appliance with the following exceptions:

- The initial configuration requires establishing a session from the router console.
- The NM-CIDS clock cannot be set directly. It must use the router's clock or an Network Time Protocol (NTP) server as a reference clock.

Installation and Configuration Tasks

Cisco.com

Task 1—Install the NM-CIDS.

Task 2—Configure the internal ids-sensor interface.

Task 3—Configure the clock settings.

Task 4—Configure packet monitoring.

Task 5—Log in to the NM-CIDS console.

Task 6—Perform additional IDS configuration.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—16-26

The installation and configuration tasks are as follows:

- Task 1—Install the NM-CIDS.
- Task 2—Configure the internal ids-sensor interface.
- Task 3—Assign the clock settings.
- Task 4—Set up packet monitoring.
- Task 5—Log in to NM-CIDS console.
- Task 6—Perform additional IDS configuration via the **setup** command.

After completing your configuration, you should verify that the NM-CIDS is analyzing traffic and back up the configuration if it is functioning properly.

Task 1—Install the NM-CIDS

Cisco.com

Step 1—Insert the NM-CIDS into a router.

Step 2—Connect the NM-CIDS to the network.

Step 3—Verify the presence of the NM-CIDS.

Step 4—Verify that Cisco IOS-IDS is not running.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-27

Task 1 involves the following steps:

- Step 1** Insert the NM-CIDS into a router.
- Step 2** Connect the NM-CIDS to the network.
- Step 3** Verify that the router recognizes the NM-CIDS.
- Step 4** Verify that Cisco IOS-IDS is not running.

Note Refer to the Cisco Intrusion Detection System Version 4.1 Quick Start Guide for details.

Task 1, Step 1—Insert the NM-CIDS into a Router

Cisco.com

When inserting the NM-CIDS in the router, keep in mind the following important points:

- **The 2600XM series and 2691 routers must be powered down before you install the NM-CIDS.**
- **The 3660, 3725 and 3745 routers allow OIR.**
- **Only one NM-CIDS should be installed in a router.**
- **Running Cisco IOS-IDS on a router in which the NM-CIDS is installed is not recommended.**

© 2004, Cisco Systems, Inc. All rights reserved.

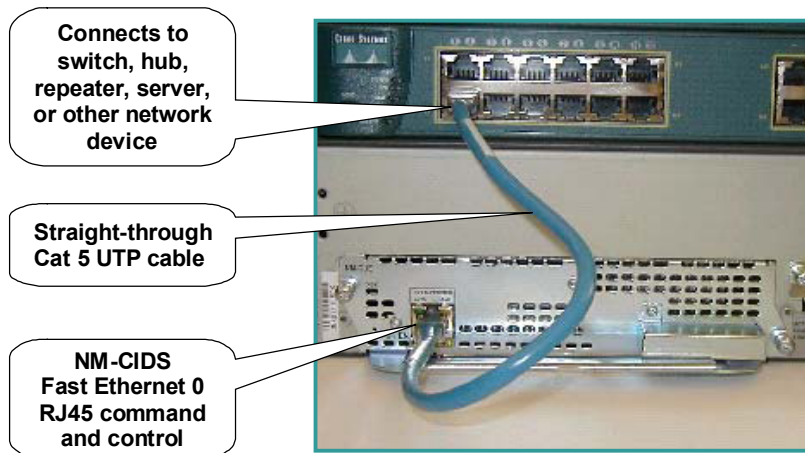
CSIDS 4.1—16-28

When inserting the NM-CIDS in the router, you should adhere to the following guidelines:

- If you are using a 2600XM Series router or a 2691 router, power it down before installing the NM-CIDS. This procedure is not necessary if you use the 3660, 3725, or 3745 routers because they allow online insertion and removal (OIR).
- Do not install more than one NM-CIDS in a router.
- Do not run Cisco IOS-IDS while the NM-CIDS is present. Running both simultaneously adversely impacts the performance of the router.

Task 1, Step 2—Connect the NM-CIDS to the Network

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-29

To connect the NM-CIDS to the network, use a straight-through two-pair Category 5 unshielded twisted-pair (UTP) cable. Connect the RJ-45 port to the NM-CIDS Fast Ethernet 0 port, which is the command and control interface. Connect the other end to a switch, hub, repeater, server, or other network device.

Task 1, Step 3—Verify the Presence of the NM-CIDS

Cisco.com

The following are indications that the router recognizes the NM-CIDS:

- The NM-CIDS PWR and EN LEDs are green.
- The `show running-config` command displays the following line:

```
interface IDS-Sensor1/0
```

- The `show version` command displays the following line:
`1 cisco ids sensor(s), ids monitoring on slot 1`

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-30

Make sure the router recognizes the NM-CIDS by using the **show running-config** command at the router console prompt. If the router recognizes the NM-CIDS, you should see the following line in the command output:

```
interface IDS-sensor1/0
```

You can also use the **show version** command for the same purpose. If the router recognizes the NM-CIDS, the **show version** output contains the following line:

```
1 cisco ids sensor(s),ids monitoring on slot 1
```

If the router does not recognize the presence of the NM-CIDS, verify that you are using the correct Cisco IOS version, 12.2(15)ZJ or later, and that the NM-CIDS is firmly seated in the router.

Task 1, Step 4—Verify that Cisco IOS-IDS Is Not Running

Cisco.com

Running Cisco IOS-IDS in the router that hosts the NM-CIDS causes performance reduction in the router. To verify that Cisco IOS-IDS is not running, use the `show ip interface` command. The output should be blank.

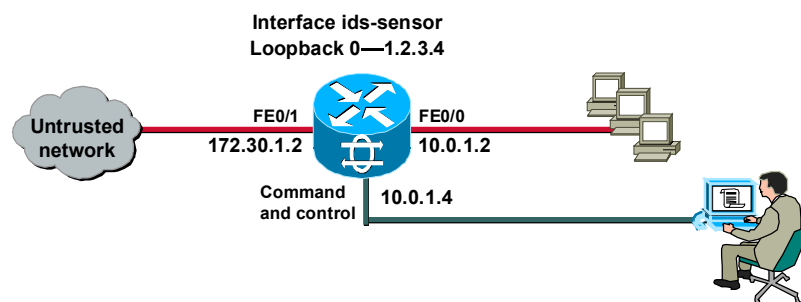
© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-31

Running Cisco IOS-IDS while the NM-CIDS is present is not recommended because doing so significantly reduces router performance. The easiest way to determine whether Cisco IOS-IDS is enabled is to use the **show ip interface** command.

Task 2—Configure the Internal IDS-Sensor Interface

Cisco.com



Step 1—Verify the NM-CIDS slot number.

Step 2—Enable CEF.

Step 3—Configure the interface.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-32

The router side internal Fast Ethernet interface is known as interface `ids-sensor`. It can be seen in the Cisco IOS **show interface** and **show controller** commands. An IP address must be assigned to this interface in order to obtain console access to the NM-CIDS. However, if this IP address is advertised via routing updates, the monitoring interface itself can become vulnerable to attacks. Therefore, it is highly recommended that you assign a loopback address to this interface. To assign a loopback address to this interface, complete the following steps:

Step 1 Verify the NM-CIDS slot number.

Step 2 Enable CEF.

Step 3 Configure the interface.

Task 2, Step 1—Verify the NM-CIDS Slot Number

Cisco.com

router#

```
show interfaces ids-sensor slot-number/port-number
```

- Displays statistics for the ids-sensor interface in your router

```
router#show interfaces ids-sensor 1/0
IDS-Sensor1/0 is up, line protocol is up
Hardware is I82559FE, address is 000d.bc3a.d090 (bia
000d.bc3a.d090)
Interface is unnumbered. Using address of Loopback0
(1.2.3.4)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:17, output 00:00:00, output hang never
.
.
.
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-33

Use the **show interfaces ids-sensor** command to confirm the NM-CIDS slot number in your router. Cisco IOS software gives the NM-CIDS the name `ids-sensor`. In this example, 1 is the slot number and 0 is the port number because there is only one port.

The syntax for the **show interfaces ids-sensor** command is as follows:

```
show interfaces ids-sensor slot-number/port-number
```

Command	Description
<i>slot-number</i>	The number of the router slot in which the NM-CIDS is installed.
<i>port-number</i>	The port number for the NM-CIDS. Zero is the only valid value.

Task 2, Step 1 (Cont.)

Cisco.com

```
router#
```

```
show running-config
```

- Displays the contents of the currently running configuration file

```
router#show running-config
.
.
.
interface FastEthernet0/1
 ip address 172.30.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface IDS-Sensor1/0
 ip unnumbered Loopback0
 hold-queue 60 out
.
.
.
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-34

To display the contents of the currently running configuration file or the configuration for a specific interface, use the **show running-config** command in privileged-EXEC mode. The **show running-config** command without any arguments or keywords displays the entire contents of the running configuration file.

The syntax for the **show running-config** command is as follows:

```
show running-config [interface type number]
```

Command	Description
interface <i>type number</i>	(Optional.) Displays interface-specific configuration information. If you use the interface keyword, you must specify the interface type and the interface number (for example, interface ethernet 0). Use the show run interface ? command to determine the interfaces available on your system.

Task 2, Step 2—Enable CEF

Cisco.com

router(config)#

```
ip cef
```

- Globally enables CEF on the router

```
router (config) #ip cef
```

- Globally enables CEF on the router, enabling the router to forward packets to the NM-CIDS

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-35

Use the **ip cef** command to enable the CEF switching path. This must be done in order for the router to forward packets to the NM-CIDS.

Task 2, Step 3—Configure the Interface

Cisco.com

```
router(config)#
```

```
interface loopback number
```

- Creates a loopback interface and enters interface configuration mode

```
router(config)#interface loopback 0  
router(config-if)#ip address 1.2.3.4  
255.255.255.255
```

- Creates loopback interface 0 and assigns IP address 1.2.3.4/32 to it

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-36

The **session** command used to access to the NM-CIDS console starts a reverse Telnet connection using the IP address of the ids-sensor interface. The ids-sensor interface is an interface between the NM-CIDS and the router. You must assign an IP address to the ids-sensor interface before invoking the **session** command. However, assigning a routable IP address can make the ids-sensor interface itself vulnerable to attacks. To counter that vulnerability, assign a loopback IP address to the ids-sensor interface.

To enable the ids-sensor interface to use a loopback IP address, complete the following substeps:

1. Create a loopback interface by entering configuration mode in the router and issuing the **interface loopback** command. This command creates the interface and enters configuration mode for the interface:

```
router(config)# interface loopback 0
```

2. Within the configuration mode for the loopback interface, assign an IP address to the loopback interface. Choose an IP address that does not overlap with any of the networks assigned to the other interfaces in the router. You will not use this address to actually access the NM-CIDS.

```
router(config-if)# ip address 1.2.3.4 255.255.255.255
```

The syntax for the **loopback interface** command is as follows:

```
interface loopback number
```

Command	Description
number	Identification number for the loopback interface

Note A loopback interface is a virtual interface that is always up.

Task 2, Step 3 (Cont.)

Cisco.com

```
router(config)#
```

```
interface ids-sensor slot-number/port-  
number
```

- Enters configuration mode for the ids-sensor interface

```
router(config-if)#
```

```
ip unnumbered type number
```

- Enables IP processing on an interface without assigning an explicit IP address to the interface

```
router(config)#interface ids-sensor 1/0  
router(config-if)#ip unnumbered loopback 0
```

- Enables the ids-sensor interface to use the IP address of loopback interface 0

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-37

After you create the loopback interface and assign an IP address to it, you must map the loopback interface to the ids-sensor interface.

Step 1 Enter the configuration mode for the ids-sensor interface.

```
router(config)# interface ids-sensor 1/0
```

Step 2 Within the configuration mode for the ids-sensor interface, execute the **ip unnumbered** command. This enables IP processing on the interface without assigning an explicit IP address to it.

```
router(config-if)# ip unnumbered loopback 0
```

Step 3 Activate the interface with the **no shutdown** command.

```
router(config-if)# no shutdown
```

Step 4 Exit configuration mode:

```
router(config-if)# end
```

Step 5 Write the configuration to NVRAM:

```
router# write mem
```

The syntax for the **ip unnumbered** command is as follows:

ip unnumbered type number

Command	Description
type number	Type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface. The interface you specify by the type and number arguments must be enabled. If it is enabled, it is listed as "up" in the show interfaces command output.

After completing the configuration of the ids-sensor interface, execute the **show interfaces ids-sensor** command to view the configuration. The output should be similar to that in the following example:

```
rP#show interfaces ids-sensor 1/0
IDS-Sensor1/0 is up, line protocol is up
  Hardware is I82559FE, address is 000d.bc3a.d090 (bia 000d.bc3a.d090)
  Interface is unnumbered. Using address of Loopback0 (1.2.3.4)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:17, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
  Queueing strategy: fifo
  Output queue: 0/60 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    3042 packets input, 185400 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    63975 packets output, 6750422 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Task 3—Configure the Clock Settings

Cisco.com

When assigning clock settings, keep in mind the following important information:

- **The NM-CIDS clock cannot be set directly.**
- **The NM-CIDS must obtain its time from one of the following:**
 - **The router clock (Cisco IOS mode)**
 - **An NTP server (NTP mode)**
- **In both Cisco IOS and NTP modes, the NM-CIDS module:**
 - **Obtains UTC (GMT) time from the router or NTP server**
 - **Converts to local time using its own time zone and summer time settings**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-38

The NM-CIDS clock cannot be set directly. It must use the router's clock or an NTP server as a reference clock. By default, the NM-CIDS automatically synchronizes its clock with the router time.

If you use the default setting, Greenwich Mean Time (GMT) is synchronized between the router and the NM-CIDS. The time zone and summer time settings are not synchronized between the router and the NM-CIDS. Therefore, be sure to set the time zone and summer time settings on both the router and the NM-CIDS to ensure that the GMT time settings are correct.

It is recommended that you use an NTP time synchronization source. NTP uses an authoritative time source to set the time on your NM-CIDS.

What Determines NM-CIDS Clock Accuracy?

Cisco.com

Cisco IOS clock mode

Accurate IDS local time depends on:

- Router's local time
- Router's time zone offset
- Router's summer time mode and offset
- IDS module's time zone offset
- IDS module's summer time mode and offset

NTP mode

Accurate IDS local time depends on:

- NTP server's clock reference
- IDS NTP configuration
- IDS time zone offset
- IDS summer time mode and offset

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-39

When using Cisco IOS clock mode, accurate NM-CIDS time depends on the following:

- The router's local time
- The router's time zone offset
- The router's summer time mode and offset
- The NM-CIDS's time zone offset
- The NM-CIDS's summer time mode and offset

When using NTP mode, accurate NM-CIDS time depends on the following:

- The NTP server's clock reference, which is configured in the router's Cisco IOS software
- The NM-CIDS's NTP configuration
- The NM-CIDS's time zone offset
- The NM-CIDS's summer time mode and offset

Clock Considerations

Cisco.com

When choosing the NM-CIDS clock mode, keep the following in mind:

- **UTC time sent to the NM-CIDS is calculated by the router from its local time, time zone, and summer time settings.**
- **If the router's time zone settings are incorrect, the UTC time sent to the IDS module is incorrect.**
- **Setting the router clock to UTC is recommended.**
- **IDS alarm time stamps indicate both UTC and local time.**
- **If the router is power-cycled, the clock is reset.**
- **TLS certificates expire based on current time.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-40

When choosing your clock mode, consider the following about Cisco IOS clock mode:

- Universal Coordinated Time (UTC) time sent to the NM-CIDS is calculated by the router from its local time, time zone, and summer time settings. If the router's time zone settings are incorrect, the UTC time sent to the NM-CIDS will also be incorrect.
- If you are using Cisco IOS clock mode, it is recommended that you set the router clock to UTC.
- The NM-CIDS alarm time stamps indicate both UTC and local time.
- The router clock is reset by a power-cycle.
- Transport Layer Security (TLS) certificates expire based on current time. If the router time resets to the default date of March 1993, those certificates will no longer work.

Clock Recommendations

Cisco.com

Clock recommendations from best to worst are as follows:

- **Use NTP mode on the NM-CIDS.**
- **Run an NTP client on the router and use Cisco IOS mode on the NM-CIDS.**
- **Run Cisco IOS mode on the NM-CIDS and set the router's time zone to UTC.**
- **Run Cisco IOS mode on the NM-CIDS and set the router's time zone to the local time zone.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-41

Considering the information just given, it is obvious that Cisco IOS clock mode is not the best choice. The following are clock recommendations, listed in order from the best choice to the worst choice:

- Use NTP mode on the NM-CIDS.
- Run an NTP client on the router and use Cisco IOS clock mode on the NM-CIDS.
- Run Cisco IOS clock mode on the NM-CIDS and set the Cisco IOS time zone to UTC.
- Run Cisco IOS clock mode on the NM-CIDS and set the Cisco IOS time zone to the local time zone.

Setting NTP Clock Mode

Cisco.com

```
router(config)#
```

```
ntp server ip-address [version number]
[key keyid] [source interface] [prefer]
```

- Enables the software clock to be synchronized by an NTP time server

```
router(config)#ntp server 172.26.26.54
router(config)#ntp server 172.26.26.55
prefer
```

- Designates two NTP servers and specifies server 172.26.26.55 as the preferred of the two

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-42

To configure NTP mode, first specify the NTP server's IP address by using the **ntp server** command.

The syntax for the **ntp server** command is as follows:

```
ntp server ip-address [version number] [key keyid] [source interface] [prefer]
```

Command	Description
ip-address	IP address of the time server providing the clock synchronization.
version number	(Optional.) Defines the NTP version number. Valid values are 1-3.
key keyid	(Optional.) Defines the authentication key. This is the authentication key to use when sending packets to this peer.
source interface	(Optional.) The name of the interface from which to pick the IP source address.
prefer	(Optional.) Specifies that the server referenced in this command is preferred over other configured NTP servers.

Setting NTP Clock Mode (Cont.)

Cisco.com

```
router(config)#
```

```
ntp authentication-key number md5 value
```

- Defines an authentication key for NTP

```
router(config)#ntp authentication-key  
12345 md5 NTPKEY
```

- Specifies the NTP authentication key ID and value

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-43

To complete the task of configuring your NM-CIDS to use NTP, define an authentication key for NTP by using the **ntp authentication-key** command. The authentication key consists of a key ID, which is a unique numeric identifier, and a key value, which is the authentication key. When this command is written to NVRAM, the key is encrypted so that it is not displayed when the configuration is viewed.

The syntax for the **ntp authentication-key** command is as follows:

ntp authentication-key number md5 value

Command	Description
number	Key number. Valid values are from 1 to 4294967295.
md5	Authentication key. Message authentication support is provided using the Message Digest 5 (MD5). The key type md5 is currently the only key type supported.
value	Key value. The key value is an arbitrary string of up to eight characters.

Task 4—Configure Packet Monitoring

Cisco.com

```
router(config-if)#
```

```
ids-service-module monitoring
```

- Configures packet monitoring on the interface

```
router (config) #interface FastEthernet0/0
```

```
router (config-if) #ids-service-module monitoring
```

- Specifies that packets sent and received on Fast Ethernet interface 0/0 should be forwarded to the NM-CIDS for inspection

```
router (config) #interface FastEthernet0/0.1
```

```
router (config-if) #ids-service-module monitoring
```

- Specifies that packets sent and received on Fast Ethernet subinterface 0/0.1 should be forwarded to the NM-CIDS for inspection

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-44

To configure packet monitoring, enter configuration mode for the interface you want the NM-CIDS to monitor. Then use the **ids-service-module monitoring** command to specify that all packets sent and received on this interface are sent to the NM-CIDS for inspection. Do the same for each interface and subinterface you want the NM-CIDS to monitor.

Task 5—Log In to the NM-CIDS Console

Cisco.com



- **No physical console port is available on the NM-CIDS.**
- **The Cisco IOS software creates a reverse Telnet to access the NM-CIDS console.**
- **The NM-CIDS console can be accessed via the session command or Telnet.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-45

Unlike the IDS appliances, the NM-CIDS has no console port of its own. Internal UARTs provide console access to the NM-CIDS through the Cisco IOS software. The Cisco IOS software performs a reverse Telnet that enables you to access the CIDS console. The reverse Telnet to the NM-CIDS console can be invoked by the session command or by direct Telnet.

You can establish and disconnect sessions between the router and the NM-CIDS by using one of the following procedures:

- To leave and re-enter an NM-CIDS console session, do the following:
 - From the NM-CIDS console, press **Ctrl-Shift-6** and then press **x** to suspend the session and return to the Cisco IOS console.
 - From the Cisco IOS console, press **Enter** to resume the session and return to the NM-CIDS console.
- To permanently disconnect the session, do the following:
 - At the NM-CIDS prompt, enter **exit**.
 - Press **Ctrl-Shift-6** and then **x**.
 - At the router prompt, enter the command **disconnect**.

Note Failing to close a session properly makes it possible for others to exploit a connection that is still established.

Console Access to the NM-CIDS via the Session Command

Cisco.com

router#

```
service-module ids-sensor slot-number/port-number session
```

- Establishes a session between the router and the NM-CIDS

```
router#service-module ids-sensor 1/0 session  
Trying 1.2.3.4, 2033 ... Open
```

```
sensor login:
```

- Establishes a session between the router and the module in slot 1

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-46

You can use the **service-module ids-sensor session** command to access the NM-CIDS console.

The syntax for the **service-module ids-sensor session** command is as follows:

service-module ids-sensor *slot-number/port-number* session

Command	Description
<i>slot-number</i>	The number of the router slot in which the NM-CIDS is installed.
<i>port-number</i>	The port number for the NM-CIDS. Zero is the only valid value.

Console Access to the NM-CIDS via Telnet

Cisco.com

- You can telnet directly into the NM-CIDS by using an IP address and port number.
- The port number is calculated with the following formula:
 - $2001 + (32 \times \text{slot number})$
- The following are examples of using Telnet for console access:
 - To telnet to the NM-CIDS in slot 1 via router interface 10.0.1.2:
C:\>telnet 10.0.1.2 2033
 - To telnet to the NM-CIDS in slot 2 via router interface 10.0.1.2:
C:\>telnet 10.0.1.2 2065

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-47

The second method to access to the NM-CIDS console is by using direct Telnet. You can open a Telnet session by using the IP address of any interface on the router and a special port number. This actually opens a connection to the console via the internal UART, just like the session command from the router console.

The formula for calculating the port number is $(32 \times \text{slot number}) + 2001$. For example, the port number for slot 1 would be 2033, and the port number for slot 2 would be 2065.

Note For the purpose of this discussion, we assume that the VTY port has been previously configured to support Telnet.

Log In to the NM-CIDS

Cisco.com

```
sensor login: cisco
Password:*****
You are required to change your password immediately
(password aged)
Changing password for cisco
(current) UNIX password:
New password:
Retype new password:
.
.
.
sensor#
```

- You must first log in with the default username **cisco**.
- The password for the **cisco** account is also **cisco**.
- You are forced to change the password for the default **cisco** account at the first login.
- After login, execute the **setup** command to initialize the NM-CIDS.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-48

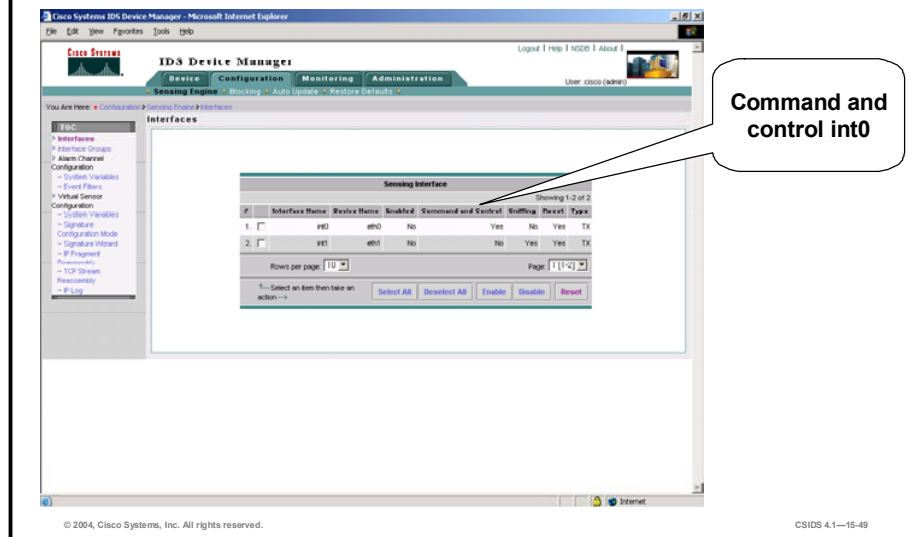
Like the Sensor appliances, the NM-CIDS is configured by default with the following administrator account:

- Username: **cisco**
- Password: **cisco**

You can use this account to initially log in to the NM-CIDS. However, the default **cisco** password is temporary and expires upon initial login. When prompted, you must change the password for this default account to a string that is not a dictionary word and is at least eight alphanumeric characters long. Special characters are not supported. After logging in, you are presented with the privileged-EXEC Sensor prompt. You can then perform the initial NM-CIDS configuration as you would for any other 4.X Sensor by using the **setup** command.

NM-CIDS Interfaces

Cisco.com



When you install a new NM-CIDS, the Cisco IDS 4.1 software detects the available monitoring interfaces during the boot process and adds those interfaces to Interface Group 0 by default. The figure shows IDS Device Manager (IDM) Configuration > Interfaces page as it appears the first time you access it. Notice that the command and control interface is int0 and the sniffing (or monitoring) interface is int1. Enable the monitoring interface to complete the initialization of the NM-CIDS.

Maintenance Tasks Unique to the NM-CIDS

This topic explains maintenance tasks that are unique to the NM-CIDS.

Cisco IOS Command for NM-CIDS Support

Cisco.com

```
router#  
service-module ids-sensor slot-number/port-number  
{reload | reset | session | shutdown | status}
```

- Enables you to do the following from the router console:
 - Reload the NM-CIDS
 - Reset the NM-CIDS
 - Establish a session to the NM-CIDS
 - Shut down the NM-CIDS
 - View the status of the NM-CIDS

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—15-61

The **service-module ids-sensor** command is a Cisco IOS command that supports the NM-CIDS. It enables you to do the following from the router console:

- Reload the NM-CIDS.
- Reset the NM-CIDS.
- Establish a session to the NM-CIDS.
- Shut down the NM-CIDS.
- View the status of the NM-CIDS.

Reload the NM-CIDS Hardware

Cisco.com

```
router#service-module ids-sensor 1/0 reload
```

```
Do you want to proceed with reload? [confirm] y  
Trying to reload Service Module IDS-Sensor1/0
```

- Reloads the NM-CIDS in slot 1 from the router console
- Stops the application, and then reloads the software

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-52

Used with the reload option, the **service-module ids-sensor** command initiates a software reboot. It stops and then reloads the IDS 4.1 software.

Reset the NM-CIDS Hardware

Cisco.com

```
router#service-module ids-sensor 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset? [confirm]
```

- Resets the NM-CIDS in slot 1 from the router console
- Initiates a hardware reboot
- Must be used with caution because it could corrupt the file system on the hard disk

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-53

Used with the **reset** option, the **service-module ids-sensor** command resets the NM-CIDS hardware. Use **reset** only to recover from a failed state. Use it with caution as it may cause you to lose all the data on the hard disk. **Reset** is a hardware reboot, while **reload** is a software reboot.

Shut Down the IDS Applications

Cisco.com

```
router#service-module ids-sensor 1/0 shutdown
Do you want to proceed with shutdown? [confirm] y
Use service module reset command to recover from shutdown

router#
Sep 12 15:24:13.919: %SERVICEMODULE-5-SHUTDOWN2: Service
module IDS-Sensor1/0 shutdown complete
```

- Shuts down the IDS applications

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-54

When used with the **shutdown** option, the **service-module ids-sensor** command gracefully halts the Linux operating system on the NM-CIDS. This option is typically used before removing the NM-CIDS from the router. Removing the NM-CIDS without proper shutdown can corrupt the data on the hard disk.

If you remove the NM-CIDS, either install a replacement NM-CIDS or install a blank panel. If you shut down the NM-CIDS but decide not to remove it, you must use the **reset** command to bring the Linux operating system back up.

Check the Status of the IDS Software

Cisco.com

```
router#service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please
wait..
Cisco Systems Intrusion Detection System Network
Module
Software version: 4.1(1)S47
Model:NM-CIDS
Memory:254676 KB
sensor#
```

- Checks the status of the IDS software

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-55

When used with the **status** option, the **service-module ids-sensor** command displays the status of the NM-CIDS software. If the NM-CIDS is operational, the following line is displayed:

```
Service Module is in Steady state
```

NM-CIDS Removal and Replacement

Cisco.com

- **The Linux operating system on the NM-CIDS must be appropriately shut down before you remove the NM-CIDS from the router.**
- **The 2600XM Series and 2691 routers must be powered down before you remove the NM-CIDS.**
- **The 3660, 3725 and 3745 routers allow OIR.**
- **The 3660, 3725, and 3745 routers support OIR with similar modules only. If you remove an NM-CIDS, install another NM-CIDS in its place.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-56

When removing or replacing the NM-CIDS, keep the following rules in mind:

- Use the **service-module ids-sensor shutdown** command to properly shut down the NM-CIDS before removing it.
- Power down the 2600XM Series and 2691 routers before removing the NM-CIDS. This is not necessary for the 3660, 3725, and 3745 routers.
- If you remove the NM-CIDS from the router and replace it with another NM-CIDS, be sure to insert the new NM-CIDS in the same slot from which you removed the old one.

Recovering the NM-CIDS Software Image

Cisco.com

- **You might need to recover the NM-CIDS software image in the following circumstances:**
 - **Lost password**
 - **Corrupted operating system**
 - **Corrupted hard drive**
- **If you perform an image recovery, all IDS configuration settings are reset to the defaults.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-57

In the following situations, you might need to recover the NM-CIDS software image:

- The password is lost and you are unable to access the NM-CIDS.
- The operating system is corrupt.
- The hard drive is corrupt.

After the recovery procedure, all NM-CIDS configuration settings are reset to the defaults. You must either use a backed-up configuration to restore your custom settings or manually re-enter them.

Recovering the NM-CIDS Software Image (Cont.)

Cisco.com

To recover the NM-CIDS software image, you will need the following:

- **Application image**
- **Helper image**
- **Latest signature and service pack updates**
- **Backup configuration file**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-58

In addition to the latest signature and service pack updates and a backup configuration file, you need the following two images to perform a software recovery:

- **Application image**—The IDS software that is stored on the hard drive.
- **Helper image**—An image used only for installing the application image. It is stored on a network TFTP server and downloaded by the NM-CIDS each time the helper image is booted.

Image Recovery Overview

Cisco.com

1. **Configure the boot loader using the config command.**
2. **Boot the helper image.**
3. **Select either SSH or TFTP as the file transfer method.**
4. **Download and write the application image to disk.**
5. **Boot the application image.**
6. **Configure the IDS application or restore a saved configuration.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-59

Complete the following steps to recover the NM-CIDS software image:

- Step 1** Configure the boot loader using the **config** command. The boot loader's functions are as follows:
- Determining which image to boot
 - Loading the image into memory and booting it
 - Loading the application image from disk
 - Downloading the helper image from a TFTP server
- Step 2** Boot the helper image.
- Step 3** Select either Secure Shell (SSH) or TFTP as the file transfer method.
- Step 4** Download and write the application image to disk.
- Step 5** Boot the application image.
- Step 6** Configure the IDS application or restore a saved configuration.

Step 1—Configure the Boot Loader

Cisco.com

```
ServicesEngine boot-loader> config
```

- Obtain the boot loader prompt by completing the following substeps:
 1. Establish a session into the NM-CIDS.
 2. Suspend the session by pressing **Ctrl-Shift-6** x.
 3. Reset the NM-CIDS.
 4. Resume the suspended session by pressing **Enter**.
 5. At the following prompt, enter *******.
Please enter '*' to change boot configuration:**
- At the **ServicesEngine boot-loader>** prompt, enter **config** to obtain the interactive prompts that enable you to set up the following boot loader network parameters:
 - NM-CIDS's IP address, netmask, and gateway
 - TFTP server's IP address
 - Path to helper image file
 - Internal/external interface
 - Default boot device

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-60

To configure the boot loader, you must first download the helper file from Cisco.com to a TFTP server on your network and copy the helper image to the /tftpboot directory on your TFTP server. Then obtain the boot loader prompt by completing the following substeps:

1. Establish a session into the NM-CIDS.
2. Suspend the session by pressing **Ctrl-Shift-6** and then **x**. This should present the **router#** prompt.
3. Reset the NM-CIDS.
4. Resume the suspended session by pressing **Enter**. After displaying its version, the boot loader displays the following prompt for 15 seconds:
Please enter '*' to change boot configuration:**
5. Enter *******. If you type ******* during the 15-second delay or if there is no default boot device configured, you enter the boot loader CLI.
6. At the boot loader CLI prompt, enter **config** to begin configuring the boot loader network parameters:
ServicesEngine boot-loader>config
7. Set up the boot loader network parameters. You are prompted for each of the following values line by line:
 - IP address

Note The IP address is the address of the external Fast Ethernet port on the NM-CIDS. This must be a real IP address on your network.

- Subnet mask
- TFTP server IP address

- Gateway IP address
- Default helper file
- Ethernet interface
- Default boot device

Step 2—Boot the Helper Image

Cisco.com

```
ServicesEngine boot-loader> boot helper
```

- Boot the helper file by entering the `boot helper` command at the `ServicesEngine boot-loader>` prompt.
- When the TFTP load actually begins, a spinning character is displayed to indicate packets arriving from the TFTP server.
- The following Helper utility is launched:

```
Cisco Systems, Inc.  
Services engine helper utility for NM-CIDS  
Version 1.0(1) [200305011547]  
Main menu  
1 - Download application image and write to HDD  
2 - Download bootloader and write to flash  
3 - Display software version on HDD  
4 - Display total RAM size  
5 - Change file transfer method (currently secure shell)  
r - Exit and reset Services Engine  
h - Exit and shutdown Services Engine  
Selection [12345rh]:
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-61

To boot the helper file, enter `boot helper` at the `ServicesEngine boot-loader>` prompt.

```
ServicesEngine boot-loader> boot helper
```

The boot loader brings up the external interface and locates the TFTP server host. When the TFTP load actually begins, a spinning character is displayed to indicate packets arriving from the TFTP server. When the load completes, a message indicates the helper is valid and the Helper utility is launched:

```
Image signature verified successfully.
```

```
Cisco Systems, Inc.  
Services engine helper utility for NM-CIDS  
Version 1.0(1) [200305011547]  
---  
Main menu  
1 - Download application image and write to HDD  
2 - Download bootloader and write to flash  
3 - Display software version on HDD  
4 - Display total RAM size  
Change file transfer method (currently secure shell)  
r - Exit and reset Services Engine  
h - Exit and shutdown Services Engine  
Selection [1234rh]:
```

Step 3—Select the File Transfer Method

Cisco.com

```
Selection [12345rh]: 5
```

```
Change file transfer method menu  
The current file transfer method is secure  
shell.
```

```
1 - Change to secure shell  
2 - Change to tftp  
r - return to main menu
```

- From the Helper utility, select 5 if you want to change the file transfer method.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-62

Select **5** to choose the file transfer method to be used for downloading the application image. This controls the protocol used for downloading application and boot loader image files only. The boot loader always uses TFTP when downloading the helper image.

You can select Secure Shell or TFTP. Secure Shell is the default.

Step 4—Download and Install the Application Image

Cisco.com

```
Selection [12345rh]: 1
Download recovery image via secure shell and write to HDD
secure shell server user name [cisco]:
server IP address [10.4.4.4]:
full pathname of recovery image []: NM-CIDS-K9-a-4.1-1-S42-1.bin
Ready to begin
Are you sure? [y/N] y
```

- From the Helper utility, select 1 to download and install the application image.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-63

To begin reimaging the hard disk, enter **1** at the Selection [12345rh]: prompt. Then complete the following substeps:

1. Enter values for each of the following as prompted:
 - SSH server username
 - SSH server IP address
 - Full path name of recovery image
2. Enter **y** when asked if you are sure you are ready to begin.
3. Enter **yes** when asked if you are sure you want to continue connecting.
4. Enter the server password.

If the restore is successful, you receive the following message and are then returned to the main menu with the Selection [12345rh] prompt.

```
Disk restore was successful
The operation was successful
```

Step 5—Boot the Application Image

Cisco.com

```
Selection [12345rh]: r
About to exit and reset Services Engine.
Are you sure? [y/N]
```

- From the Helper utility, select **r** to boot the application image.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-64

After downloading and installing the application image, reboot the NM-CIDS by entering **r** at the Selection [1234rh]: prompt. Enter **y** when asked if you are sure you want to exit and reset the Services Engine. After the reboot, you must initialize your NM-CIDS with the **setup** command.

Software Upgrades

Cisco.com

- **The NM-CIDS accepts the same software revision upgrades, service packs, and signature updates as all other Cisco IDS Sensors.**
- **The upgrade process is also the same. You can use the upgrade command in the CLI.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-65

Use the same software revision upgrades, service packs, and signature updates to upgrade the NM-CIDS that you would use for any other Cisco IDS Sensor. The upgrade process is also the same. Use the **upgrade** command in the CLI.

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco.com

- **The NM-CIDS is a fully featured IDS Sensor that runs on Cisco 2600XM, 2691, 3660, 3725, and 3745 routers.**
- **The NM-CIDS can inspect all traffic traversing the router.**
- **The NM-CIDS runs the Cisco IDS 4.1 Sensor software.**
- **The NM-CIDS has one external Fast Ethernet interface that is used as the command and control port.**
- **An internal Fast Ethernet interface on the NM-CIDS connects to the internal PCI bus on the router's backplane. This provides the monitoring or sniffing capability.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-67

Summary (Cont.)

Cisco.com

- **Tasks for enabling the NM-CIDS to analyze network traffic include the following:**
 - **Enabling CEF on the router.**
 - **Creating a loopback interface on the router.**
 - **Assigning an IP address to the router's loopback interface.**
 - **Enabling the router's ids-sensor interface to use the loopback interface's IP address.**
 - **Configuring the NM-CIDS clock settings.**
 - **Configuring packet monitoring.**
- **NM-CIDS software upgrades use the same software revision upgrades, service packs, and signature updates as all other CIDS sensors.**
- **Like other Sensor devices, the NM-CIDS can be upgraded using the upgrade command.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-68

Summary (Cont.)

Cisco.com

- **The service-module ids-sensor command is a Cisco IOS command that supports the NM-CIDS by providing the ability to reload, reset, shut down, establish a session to, and check the status of the NM-CIDS.**
- **Before removing the NM-CIDS from the router, you must do the following:**
 - **Shut down the Linux operating system on the NM-CSIDS.**
 - **Power down the router if it is a 2600XM or 2691 model.**
- **There is a recovery procedure that enables you to recover the NM-CIDS software image in situations such as the following:**
 - **Lost password**
 - **Corrupted operating system**
 - **Corrupted hard drive**
- **All IDS configuration settings are reset to the defaults when you perform the software recovery procedure.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—15-69

Intrusion Detection System Module Configuration

Overview

This lesson covers information on the Catalyst 6500 Intrusion Detection System (IDS) Module 2 (IDSM-2) and how to configure it for intrusion detection.

This lesson includes the following topics:

- Objectives
- Introduction
- Ports and traffic
- Initialization
- Verifying IDSM-2 status
- Summary

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

- Describe the Catalyst IDSM-2 features.
- Distinguish between the functions of the various Catalyst IDSM-2 ports.
- Initialize a Catalyst IDSM-2.
- Verify the Catalyst 6500 switch and Catalyst IDSM-2 configurations.

© 2004, Cisco Systems, Inc. All rights reserved.


CSIDS 4.1 — 16-3

Introduction

This topic introduces the IDSM-2.

IDSM-2

Cisco.com



	IDSM-2
Performance	600 Mbps
Size	1 RU/slot
Processor	Dual 1.13 GHz
Operating system	Linux
Response	IP log, reset, and block

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1 — 16-5

The following are the IDSM-2 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

IDS-2 Key Features

Cisco.com

- **Brings switching and security into a single chassis**
- **Supports an unlimited number of VLANs**
- **No impact on switch performance**
- **Provides an effective platform across all Catalyst 6500 chassis**
- **Uses the same code as the Cisco IDS network appliances**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 —16-6

The following are the IDS-2 key features:

- Provides an in-switch IDS solution supplying access to the data stream via VLAN access control list (VACL) capture, Switch Port Analyzer (SPAN), or Remote SPAN (RSPAN).
- Supports an unlimited number of VLANs.
- Transparent operation via passive, promiscuous operation that inspects copies of packets via VACL capture, SPAN, and RSPAN without exposing the network to performance degradation or downtime if the unit needs maintenance. This is possible because the IDS-2 is not in the switch forwarding path.
- Takes only a single slot in the switch chassis making it an effective platform across all Catalyst 6500 chassis, from the three-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

	IDS	IDS-2
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)

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—16-7

The Cisco IDS-2 is a fabric-enabled, second-generation IDS offering more than five times the performance of the first-generation module. All Cisco Catalyst 6500 Series switches support the Cisco IDS-2.

In addition to increased performance, the IDS-2 features the following enhancements as compared to the IDS:

- 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 Switch Requirements

Cisco.com

The IDSM-2 runs in any Catalyst 6500 Series switch that meets one of the following requirements:

- Catalyst Software Release 7.5(1), 7.6(1), or later with one of the following:
 - Supervisor Engine 1A
 - Supervisor Engine 1A/PFC2
 - Supervisor Engine 1A/MSFC1
 - Supervisor Engine 1A/MSFC2
 - Supervisor Engine 2
 - Supervisor Engine 2/MSFC2
- Cisco IOS Software Release 12.2(14)SY with Supervisor Engine 2 and MSFC2
- Cisco IOS Software Release 12.1(19)E with one of the following:
 - Supervisor Engine 1A with MSFC2
 - Supervisor Engine 2 with MSFC2
- Cisco IOS Software Release 12.2(14)SX1 with Supervisor Engine 720

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 —16-8

The IDSM-2 runs in any Catalyst 6500 Series switch that meets one of the following requirements:

- Catalyst Operating System Software Release 7.5(1), 7.6(1), or later with one of the following:
 - Supervisor Engine 1A
 - Supervisor Engine 1A/Policy Feature Card 2 (PFC2)
 - Supervisor Engine 1A/MSFC1
 - Supervisor Engine 1A/MSFC2
 - Supervisor Engine 2
 - Supervisor Engine 2/MSFC2
- Cisco IOS Software Release 12.2(14)SY with Supervisor Engine 2 and MSFC2
- Cisco IOS Software Release 12.1(19)E with one of the following:
 - Supervisor Engine 1a with MSFC2
 - Supervisor Engine 2 with MSFC2
- Cisco IOS Software Release 12.2(14)SX1 with Supervisor Engine 720

Note If you are using the Catalyst switch in hybrid mode, Cisco IOS Software Release 12.1(13)E or higher is recommended for the MSFC.

IDS-2 and Switch Configuration Tasks

Cisco.com

- **Initialize the IDS-2.**
- **Configure the switch to capture traffic for intrusion detection analysis.**
- **Assign the command and control port to the proper VLAN.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 — 16-9

Complete the following tasks to configure the IDS-2 and the Catalyst 6500 switch:

- Initialize the IDS-2. 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 topic discusses the ports on the IDSM-2 and how traffic is captured for intrusion detection analysis.

IDSM-2 Ports

Cisco.com

The IDSM-2 has the following four logical ports:

- **Port 1—TCP resets**
- **Port 2—Command and control**
- **Port 7 and/or 8—Sensing**

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—16-11

Packets are directed to the monitoring ports of the IDSM-2 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 IDSM-2 can monitor. A copy of transmit (TX), receive (RX), or both TX and RX traffic can be sent from the spanned port to an IDSM-2 monitor port. The IDSM-2 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 RX traffic, all TX traffic, or all RX and TX 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 two per chassis. For TX SPAN sessions, you can have a maximum of four sessions per chassis. For SPAN sessions that copy and send both RX and TX traffic from a port, you can configure a maximum of two SPAN sessions per chassis.

When using SPAN, refer to the following rules:

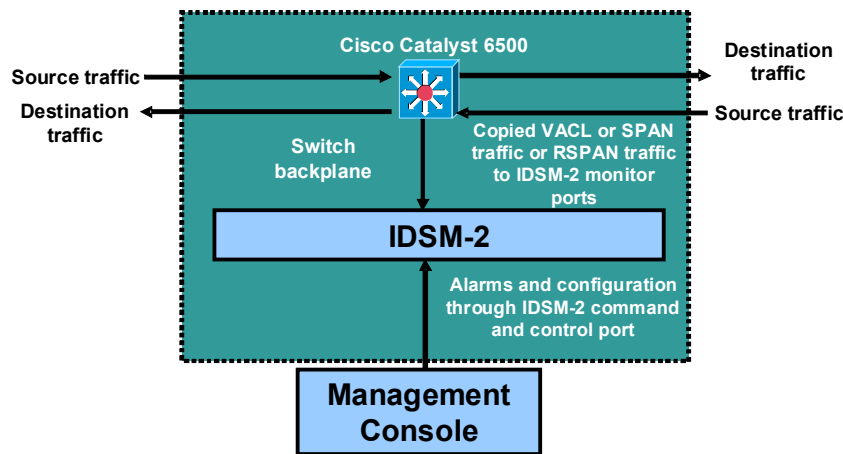
- The total amount of spanned traffic cannot exceed the maximum throughput of the IDSM-2, 600 Mbps.

- The limitation on the number of SPAN sessions limits the number of ports in the chassis that can have their traffic monitored by the IDSM-2.

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 is copied and sent to a configured capture port. The monitor port of the IDSM-2 can be configured as the VACL capture port. Although configuring SPAN is easier, the VACL method of sending traffic to the IDSM-2 may be preferable because it allows a subset of traffic to be copied and sent to the IDSM-2, 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 IDSM-2 has to process.

IDSM-2 Traffic Flow

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 — 16-12

The traffic flow is an important aspect of understanding how the IDSM-2 captures and analyzes network traffic. The Catalyst 6500 switch must first be configured to capture traffic for intrusion detection analysis. If this configuration is not done, the IDSM-2 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 IDSM-2. The IDSM-2 performs intrusion detection analysis and performs the defined actions.

Initialization

This topic covers how to access and initialize the IDSM-2.

IDSM-2 Initialization Tasks

Cisco.com

- **Access the IDSM-2 using the switch session command.**
- **Log in at the IDSM-2 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 IDSM-2.**

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1 —16-14

Because the IDSM-2 runs the same code as the Sensor appliance, the initialization of the IDSM-2 is essentially the same as that of the Sensor appliance. The main difference is the method of accessing the IDSM-2 CLI. To initialize the IDSM-2, complete the following steps:

- Step 1** Initiate a session with the IDSM-2 from the switch CLI.
- Step 2** Log in to the IDSM-2 using the default username **cisco** and the password **cisco**.
- Step 3** Follow the prompts to change the default password.

Note Passwords must be at least eight characters long and must not be words found in the dictionary.

- Step 4** Run the **setup** command and respond to its interactive prompts to complete the initial configuration.
- Step 5** Reset the IDSM-2 to enable and apply the configuration changes.

Although the Sensor appliance can be configured to use either its internal clock or Network Time Protocol (NTP), the IDSM-2 can be configured to use either the switch's time or NTP. The IDSM-2 cannot be configured to use an internal clock. Therefore, there is no option to set the clock time in the IDSM-2's CLI. By default, the IDSM-2 is configured to use the switch's time. The switch converts its local time into the Coordinated Universal Time (UTC) time that is used by the Sensor to time-stamp its events. Because the Sensor's time zone is also configurable, the Sensor uses its time zone and summer time settings to convert the UTC to local time. The Sensor uses both its local time and UTC time settings for time-stamping events,

as well as for other time functions. For this reason, it is important to ensure that the time zone and summer time settings are correct on both the switch and the IDSM-2, and that the clock setting is correct on the switch. The IDSM-2 does not use the switch's time zone and summer time settings because these settings are not reported to the module. The switch sends its UTC time only to the IDSM-2.

Access the IDSM-2—Catalyst Operating System

Cisco.com

```
switch> (enable)
```

```
session mod
```

- Enables you to access an IDSM-2 installed in the Catalyst 6500 switch

```
switch> (enable) session 3
```

- Enables access to the IDSM-2 installed in slot 3 of the Catalyst 6500 switch

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 —16-15

Using the **session** command from the Catalyst 6500 CLI to access the module gives you access to the IDSM-2 CLI. The syntax for the Catalyst operating system **session** command is as follows:

session mod

mod	Number of the module
------------	----------------------

Access the IDSM-2—Cisco IOS Software

Cisco.com

Router#

```
session slot mod {processor processor-id}
```

- Opens a session with an IDSM-2 and enables you to use the IDSM-2-specific CLI

```
Router# session slot 3 processor 1
```

- Enables access to the IDSM-2 installed in slot 3 of the Catalyst 6500 switch

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 —16-16

Using the **session** command from the Catalyst 6500 CLI to access the module gives you access to the IDSM-2 CLI. The syntax for the Cisco 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 IDSM-2 is processor 1.

Verifying IDSM-2 Status

This topic explains how to verify the status of the IDSM-2.

IDSM-2 Status LED

Cisco.com

IDSM-2 status LED colors and their descriptions are as follows:

- **Green**—IDSM-2 is operational.
- **Amber**—IDSM-2 is disabled, running a boot and self-diagnostic sequence, or shut down.
- **Red**—Diagnostics other than an individual port test failed.
- **Off**—IDSM-2 power is off.

© 2004, Cisco Systems, Inc. All rights reserved.CSIDS 4.1 —16-18

Checking the status LED is a quick method to determine the state of the IDSM-2. The status LED is located in the left corner of the IDSM-2. LED status colors are described in the following table:

Status Color	Description
Green	IDSM-2 is operational.
Amber	IDSM-2 is disabled, running a boot and self-diagnostic test, or is shut down.
Red	Diagnostics other than an individual port test failed.
Off	IDSM-2 power is off.

In addition to the LED, the front panel of the IDSM-2 has a shutdown switch. To prevent corruption of the IDSM-2, you must shut it down properly. To shut it down properly, log in to the IDSM-2 from the Catalyst 6500 series console and enter the **shutdown** command. If the IDSM-2 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 IDSM-2 is hot-swappable, but you should not remove it from the switch until the IDSM-2 shuts down completely. Removing the IDSM-2 without going through a shutdown procedure can damage your IDSM-2.

show module Command

Cisco.com

switch>

```
show module [mod]
```

- Displays module status and information

```
switch>show module
Mod Slot Ports Module-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 System WS-SVC-IDS-2 yes ok
5 5 0 Switch Fabric Module 2 WS-X6500-SFM2 no ok
6 6 8 Intrusion Detection System WS-SVC-IDS-2 yes ok
7 7 8 Intrusion Detection System WS-SVC-IDS-2 yes ok
```

- Displays the status of all modules in the switch. Three IDS-2s are installed, one in slot 4, one in slot 6, and one in slot 7. The ok state indicates that the IDS-2s are online.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 — 16-19

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 Cisco IOS **show module** command is as follows:

```
show module [mod-num | all]
```

mod-num	(Optional.) Number of the module
all	(Optional.) Displays the information for all modules

The figure shows the output of the **show module** command. It is normal for the status to display “other” when the IDS-2 is first installed. After the IDS-2 completes the diagnostics routines and comes online, the status displays “ok.” Allow up to 5 minutes for the IDS-2 to come online.

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **The IDSM-2 is a line card for the Cisco Catalyst 6500 Series switches.**
- **The IDSM-2 runs the same code as the Cisco IDS Sensor appliance.**
- **The IDSM-2 is delivered with IDS Software Revision 4.0 or higher.**
- **The IDSM-2 does not affect switch performance because it is not in the forwarding path of the switch.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1 — 16-21

Capturing Network Traffic for Intrusion Detection Systems

Overview

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

This lesson includes the following topics:

- Objectives
- Traffic capture overview
- Configuring SPAN for Catalyst 4500 and 6500 traffic capture
- Configuring RSPAN for Catalyst 4500 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 capture
- Summary

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

Upon completion of this lesson, 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-3

Traffic Capture Overview

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

Overview

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—17-5

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 capture.” 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.)

Cisco.com

- **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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-6

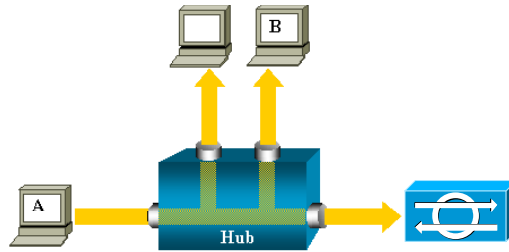
The network devices that are used to capture traffic for IDSs are hubs, network taps, and switches. Methods of capturing traffic include the following:

- 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 lists (VACLs)—Can selectively filter and forward VLAN traffic to the Intrusion Detection System Module (IDSM) in a Catalyst 6500 Series switch.
- The **mls ip ids** command—The **mls ip ids** command is used instead of a VACL when 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 Series switch with an IDSM. VACLs are incompatible with Context-Based Access Control (CBAC); therefore, you cannot apply VACLs on the same VLAN in which you have applied a rule using the **ip inspect** command 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 Cisco Catalyst 6000 IOS documentation for more information regarding CBAC and IDS.

Hub Traffic Flow

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

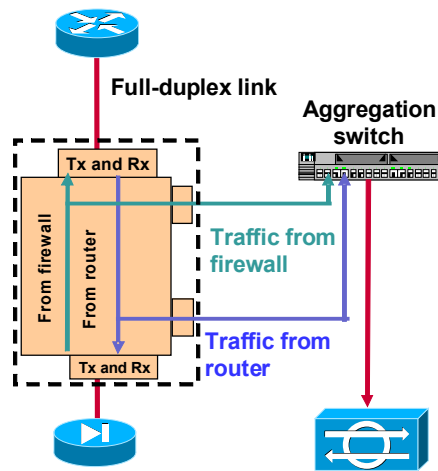
CSIDS 4.1-17.7

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, because all other ports “see” the traffic between host A and B.

Note The sniffer is the network IDS.

Network Tap Traffic Flow

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-8

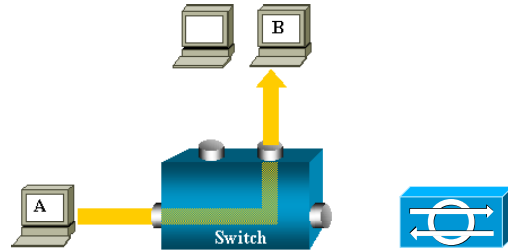
A network tap is a device used to split full-duplex traffic flows into single traffic flows that can be aggregated at a switch device. The network tap has four connectors:

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

In the figure, 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

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

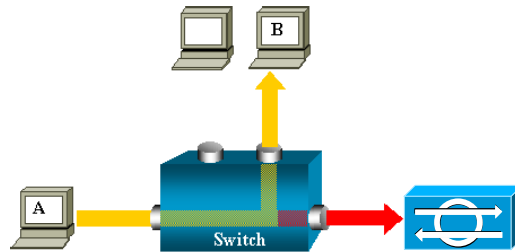
CSIDS 4.1—17-9

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 is not seen by the sniffer.

Note The sniffer is the network IDS.

SPAN Traffic Flow

Cisco.com



© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-10

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 between switches and 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.

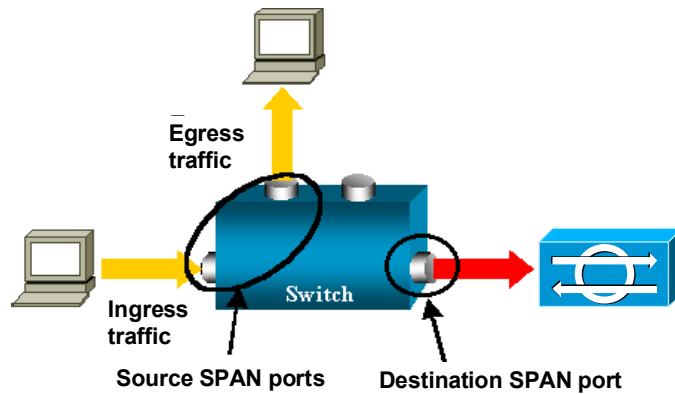
In the diagram, the sniffer is attached to a port that is configured to receive a copy of every single packet that is sent by host A. This port is called a SPAN port.

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



© 2004, Cisco Systems, Inc. All rights reserved.

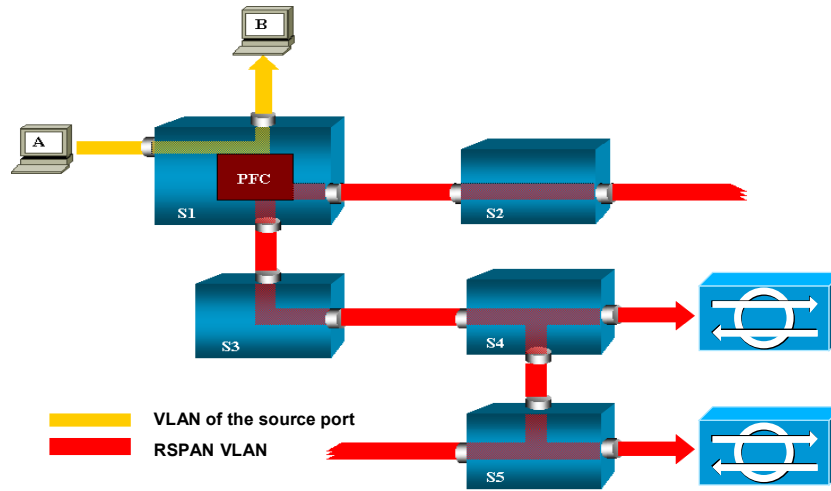
CSIDS 4.1—17-11

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

- Ingress traffic—Traffic that enters the switch.
- Egress traffic—Traffic that 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.
- 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).
- RSPAN—Some source ports are not located on the same switch as the destination port. This is an advanced feature that requires a special VLAN to carry the traffic being monitored by SPAN between switches.
- 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

Cisco.com



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 (shown in the figure on S4 and S5).

Note The sniffers are network IDSs.

TCP Resets and Switches

Cisco.com

- **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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-13

The Cisco IDS TCP reset signature action terminates a TCP session by sending TCP packets with the reset (RST) flag 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 4500 and 6500 Traffic Capture

This topic provides the commands used to configure the SPAN feature on Cisco Catalyst 4500 and 6500 Series switches.

Catalyst Operating System 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

© 2004, Cisco Systems, Inc. All rights reserved. CSIDS 4.1—17-15

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]
```

<i>src_mod</i>	Monitored module (SPAN source).
<i>src_ports...</i>	Monitored ports (SPAN source).
<i>src_vlans...</i>	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 (egress SPAN) and received at the source (ingress SPAN) 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.
<i>dest_mod</i>	(Optional.) Monitoring module (SPAN destination).
<i>dest_port</i>	(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 the **create** keyword. If you specify the keyword **create** and there is no matching destination port, the session is created.

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

Cisco IOS SPAN Configuration— Configuring the Source

Cisco.com

Router(config)#

```
monitor session session_number 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-16

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

<i>session_number</i>	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.

Cisco IOS SPAN Configuration— Configuring the Destination

Cisco.com

Router(config)#

```
monitor session session_number 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-17

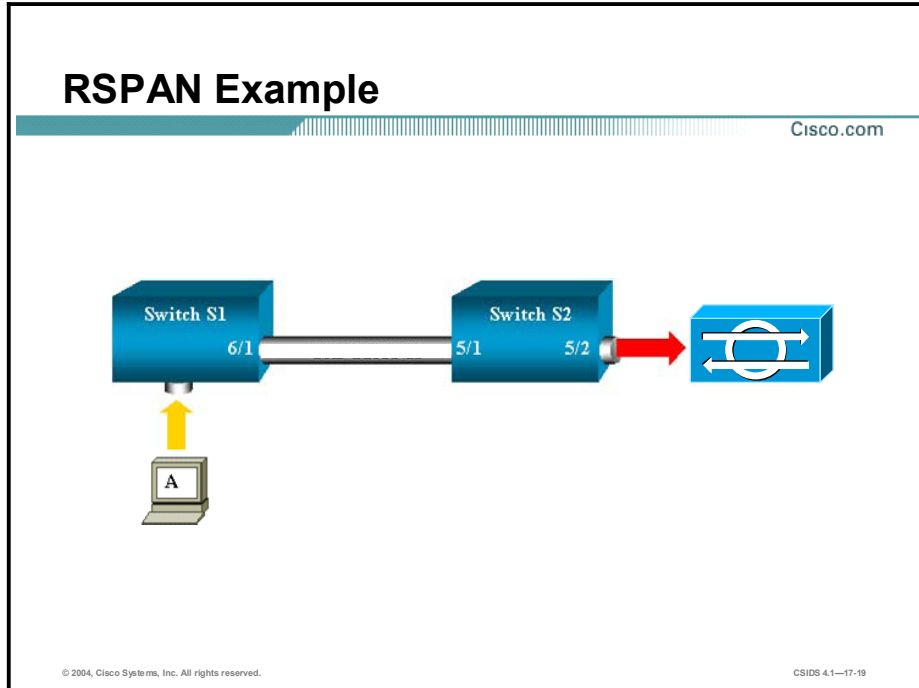
To complete the SPAN configuration, configure the SPAN destination with the **monitor session destination** command. The syntax for the **monitor session destination** command is as follows:

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

<i>session_number</i>	Number of the SPAN session; valid values are from 1 to 66.
destination	SPAN destination interface.
<i>interface type</i>	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.
<i>vlan type</i>	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 4500 and 6500 Traffic Capture

This topic provides the commands used to configure the RSPAN feature on Cisco Catalyst 4500 and 6500 Series switches.



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 4500 does not support RSPAN in Cisco IOS software. The Catalyst 6500 supports RSPAN in both Catalyst operating system software and Cisco IOS software.

CatOS Configuration Tasks

Cisco.com

Complete the following tasks to configure CatOS 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-20

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

Cisco.com

```
switch>(enable)
```

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

- Configures the RSPAN VLAN

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

- Creates RSPAN VLAN 901

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-21

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 IEEE 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
```

<i>vlans</i>	Number identifying the VLAN; valid values are from 1 to 1005 and from 1025 to 4094.
<i>mod/ports</i>	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 topic applies to the Catalyst 6500 Series switches. For command syntax for 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-22

The **set rspan source** command is used to create RSPAN source sessions. For Catalyst 6500 switches, 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.
<i>rspan_vlan</i>	RSPAN VLAN.
all	(Optional.) Keyword to disable all RSPAN source or destination sessions.
disable destination	Keywords to disable RSPAN destination information.
<i>mod/port</i>	(Optional.) RSPAN destination port.
<i>src_mod/src_ports</i>	Monitored ports (RSPAN source).
<i>src_vlans</i>	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.

Note This command syntax applies only to the Catalyst 6500 Series switch. The syntax for the Catalyst 4500 Series switch is slightly different and requires the **reflector** keyword. See the *Catalyst 4500 Series Command Reference* for details.

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 assigned as destination for monitored traffic sent on RSPAN VLAN 901

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-23

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

```
set rspan 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.
<i>mod/port</i>	(Optional.) RSPAN destination port.
all	(Optional.) Keyword to disable all RSPAN source or destination sessions.
<i>rspan_vlan</i>	(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.

Cisco IOS Configuration Tasks

Cisco.com

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

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-24

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-25

Use the **vlan** command to add a VLAN and enter config-VLAN sub-mode. 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*}

<i>vlan-id</i>	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.
<i>vlan-range</i>	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

Cisco.com

Router1(config)#

```
monitor session session_number 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_number 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 (Router 1). Traffic entering S1 on port 6/2 is monitored. VLAN 901 is the destination.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-26

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

Cisco.com

```
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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-27

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 topic discusses the configuration tasks and commands used to configure the Cisco Catalyst 6500 Series switch capture feature.

CatOS Configuration Tasks

Cisco.com

Complete the following tasks to configure the use of CatOS 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-29

The tasks to capture traffic using VLAN access control lists (VACLs) on a Catalyst 6500 Series switch running the Catalyst operating system 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]
```

- 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-30

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 to remove 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]
```

<i>acl_name</i>	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.
<i>src_ip_spec</i>	Source IP address and the source mask.
ip	(Optional.) Keyword or number to match any IP packets.

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

Cisco.com

```
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
```

- Sets the VACL 10_NET to capture traffic destined to or originating from the 10.0.0.0 network.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-31

The WEBONLY 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

Cisco.com

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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-32

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

```
commit security acl acl_name | all
```

<i>acl_name</i>	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
```

<i>acl_name</i>	Unique name that identifies the list to which the entry belongs.
<i>vlan</i>	Number of the VLAN to be mapped to the VACL.

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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-33

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>...]
```

<i>mod/ports</i>	Module and port number
------------------	------------------------

Cisco IOS Configuration Tasks

Cisco.com

Complete the following tasks to capture traffic by using VACLs on a Catalyst 6500 Series switch running Cisco 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-34

The tasks to capture traffic using VACLs on a Catalyst 6500 Series switch running Cisco IOS software 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-35

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 configuration 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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-36

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

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-37

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.
<i>interface-number</i>	Module and port number; refer to the “Usage Guidelines” section for valid values.
port-channel <i>channel-id</i>	Port channel to redirect traffic; refer to the “Usage Guidelines” section for valid values.

Apply VLAN Access Map to VLANs

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-38

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*}

<i>map-name</i>	VLAN access map tag.
<i>vlan-list</i>	VLAN list. Refer to the “Usage Guidelines” section for valid values.
<i>interface</i>	Specifies the WAN interface type. Valid values are pos, atm, or serial.
<i>number</i>	Interface number. The <i>interface-number</i> format can be <i>mod/port</i> or <i>slot/port_adapter/port</i> . 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 Fast Ethernet interface for module 2, port 4, of an IDSM

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-39

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*

<i>type</i>	Type of interface to be configured
<i>number</i>	Module and port number

Enable Capture on the Interface

Cisco.com

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-40

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 Inter-Switch Link (ISL) or IEEE 802.1Q 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 topic explains how to use the **mls ip ids** command to configure the Cisco Catalyst 6500 Series switch capture feature.

CatOS Configuration Tasks

Cisco.com

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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-42

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** command 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 whether they should be captured.

The tasks to capture traffic using the **mls ip ids** command 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 Cisco IOS ACLs

Cisco.com

```
router(config)#
```

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

- Creates a Cisco IOS extended IP ACL

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

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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-43

The Cisco 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
```

<i>acl-name</i>	Name of the ACL.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>protocol</i>	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.
<i>source</i>	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.
<i>source-wildcard</i>	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.

<i>destination</i>	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.
<i>destination-wildcard</i>	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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-44

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 ACL 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 whether 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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-45

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>...]
```

<i>mod/ports</i>	Module and port number
------------------	------------------------

Cisco 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.

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-46

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

- Use the Cisco 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 was presented earlier in this lesson.

Advanced Catalyst 6500 Traffic Capture

This topic explains how to limit the capture of encapsulated (trunked) traffic using the Cisco Catalyst 6500 Series switch capture features for VACLs and the `mls ip ids` command.

Controlling Capture VLAN Traffic

Cisco.com

- **By default, a Sensor appliance receives captured traffic only from the VLAN assigned to the switch port to which the Sensor is connected.**
- **The appliance Sensor port can receive captured traffic from multiple VLANs if the switch port to which the Sensor is connected 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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1-17-48

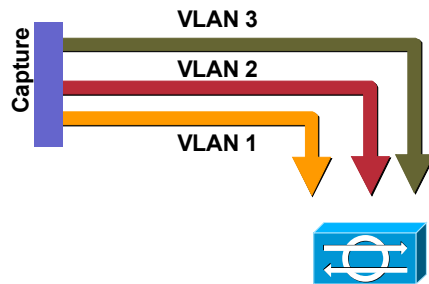
An appliance Sensor by default receives captured traffic only from the VLAN assigned to the switch port to which the Sensor is connected. The appliance Sensor's monitoring port is typically connected to an access port on a switch. The switch port must be configured as a trunk port to enable the appliance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

Cisco.com



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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-49

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.

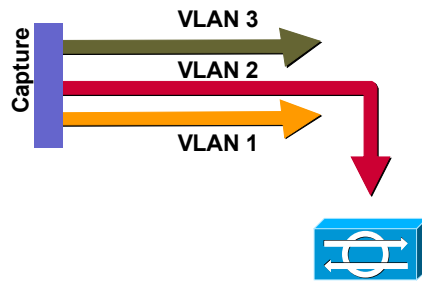
Note The scenario is based on the use of ACLs to capture traffic.

Complete the following steps to configure the switch to capture traffic only 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

Cisco.com



```
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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-50

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.

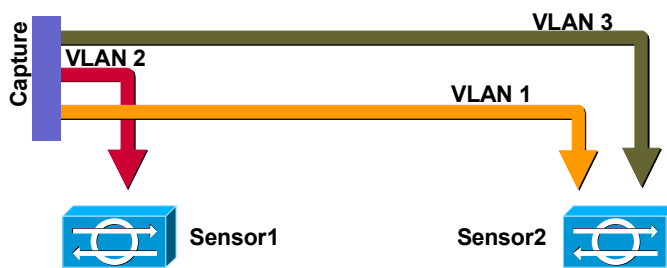
Note The scenario is based on the use of ACLs to capture traffic.

Complete the following steps to configure the switch to capture traffic only 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 1-1005,
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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-51

This scenario illustrates that the switch has been configured to capture traffic only from VLAN 2 to port 6/1 and only from VLANs 1 and 3 to port 7/1. Traffic from other VLANs is ignored.

Notice that Sensor 1's monitoring port is a member of VLAN 2, and the Sensor 2's monitoring port is a member of VLAN 1. VLAN 2 is the native VLAN for Sensor 1's monitoring port, and VLAN 1 is the native VLAN for Sensor 2'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.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-52

Complete the following tasks to configure the switch to control traffic capture and to send traffic to the IDS's monitoring port:

- Configure the destination capture port as a switch trunk port using the **set trunk** command.
- Clear all VLANs from the switch's destination capture port using the **clear trunk** switch command.
- Assign the VLANs of interest to the switch's 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
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-53

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]

<i>mod/port</i>	Number of the module and the port on the module.
<i>vlans</i>	(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]

<i>mod/port</i>	Number of the module and the port on the module.
<i>vlans</i>	(Optional.) VLANs to add to the list of allowed VLANs on the trunk. Valid values range from 1 to 1005 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

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-54

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

Cisco.com

```
switch> (enable)
```

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

- Defines security ACL capture ports

```
switch>(enable) set security acl capture-ports 6/1
```

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-55

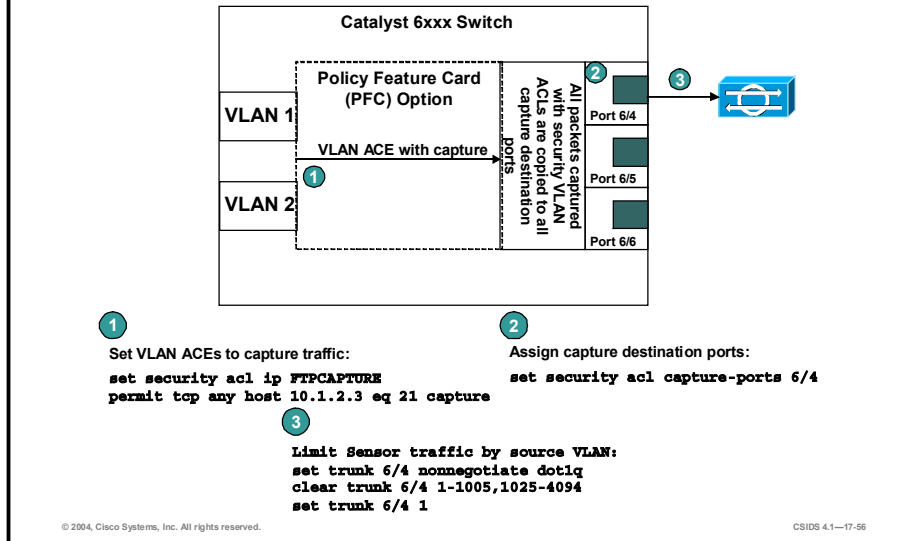
The **set security acl capture-ports** command is used to set the destination ports that receive the captured traffic specified in the **set security acl ip** command. Use the **clear security acl capture-ports** command to remove a port from the capture port list. The syntax for the **set security acl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

```
set security acl capture-ports <mod/ports>[,<mod/ports>...]
```

mod/ports	Module and port number
------------------	------------------------

VACL Packet Capture Example

Cisco.com



The example in the graphic illustrates how to limit the VLAN traffic the sent to the Sensor from a Catalyst 6xxx Series switch. Initially the switch is configured with a VACL to capture FTP traffic that is permitted to host 10.1.2.3 using the following command:

```
set security acl ip FTPCAPTURE permit tcp any host 10.1.2.3 eq 21 capture
```

Then the capture is assigned a destination port of slot 6, port 4, with the following command:

```
set security acl capture-ports 6/4
```

When this command is implemented, the capture port then receives this traffic from all VLANs. In order to limit the VLAN traffic sent to the Sensor, the capture port is configured to receive traffic only from a specific VLAN by using the following commands:

```
set trunk 6/4 nonnegotiate dot1q  
clear trunk 6/4 1-1005 1025-4094  
set trunk 6/4 1
```

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **Network traffic 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 Series switches can capture traffic using a VLAN or Cisco IOS ACLs.**
- **VLAN traffic captured using a Catalyst 6500 Series switch may be controlled using the clear trunk and set trunk commands.**

© 2004, Cisco Systems, Inc. All rights reserved.

CSIDS 4.1—17-58

Lab Guide

Overview

This guide presents the instructions and other information concerning the activities for this course.

Outline

This guide includes these activities:

- Lab Exercise 5: Getting Started with the IDS Command Line Interface
- Lab Exercise 6: Cisco IDS Device Manager and Event Viewer
- Lab Exercise 7: Sensor Configuration
- Lab Exercise 8: Configuring Signatures
- Lab Exercise 9: Configuring Signatures
- Lab Exercise 10: Signature and Sensor Configuration
- Lab Exercise 11: Blocking Configuration
- Lab Exercise 12: Cisco IDS System Maintenance
- Lab Exercise 13: Enterprise Intrusion Detection System Management
- Lab Exercise 14: Enterprise IDS Monitoring and Reporting
- Lab Exercise 15: Initializing the NM-CIDS

Copyright © 2004, Cisco Systems, Inc. All rights reserved.

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 • Cyprus • 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



Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, iQ logo, the iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Lesson 5

Lab Exercise—Getting Started with the IDS Command Line Interface

Complete the following lab exercise to practice what you learned in this chapter.

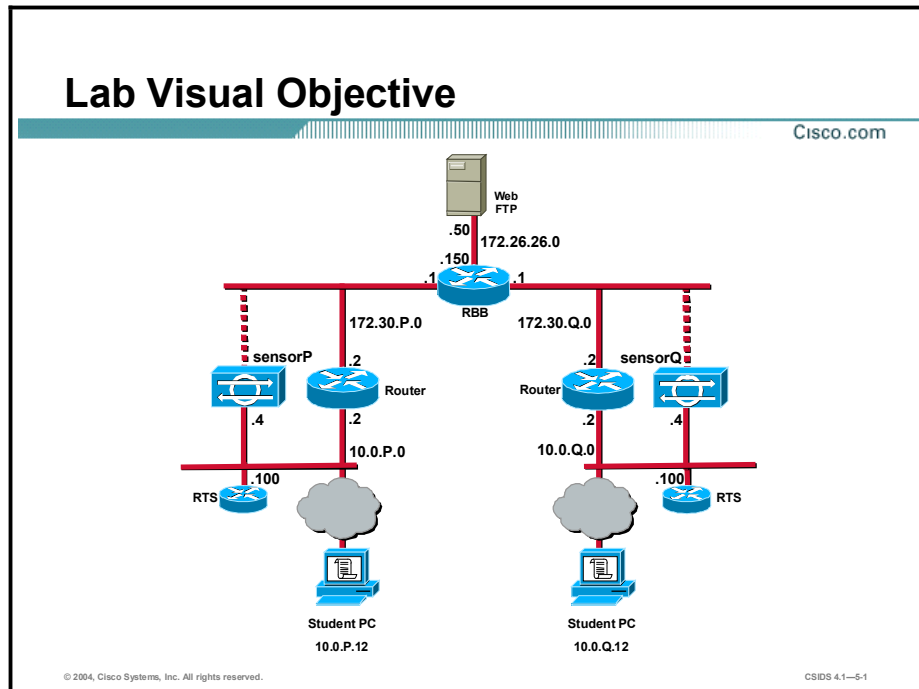
Objective

In this lab exercise, you will complete the following tasks:

- Assign the Sensor's IP network settings.
- Navigate the CLI.
- Add a network to the network access control list.
- Test your initial configuration.
- Create and test user accounts.
- Configure and test account locking.
- 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.



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 pod number.

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.
- 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: iattacku2
```

Step 4 Enter the **setup** command and press the space bar. The System Configuration Dialog is displayed.

```
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:

```
networkParams  
ipAddress 10.1.9.201  
netmask 255.255.255.0  
defaultGateway 10.1.9.1  
hostname sensor  
telnetOption disabled  
accessList ipAddress 10.0.0.0 255.0.0.0  
exit  
timeParams  
summerTimeParams  
active-selection none  
exit  
exit  
service webServer  
general  
ports 443  
exit  
exit
```

Current time: Fri Oct 3 17:02:01 2003

Setup Configuration last modified: Fri Oct 3 19:36:25 2003

- Continue with configuration dialog? [yes]:
- Step 5** Press **Enter** when prompted to continue with the configuration dialog:
Continue with configuration dialog? [yes]: **<Enter>**
- Step 6** Assign a name to the Sensor:
Enter host name [sensor]: **sensorP**
(where P= pod number)
- Step 7** 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 8** Assign a netmask for the IP address:
Enter netmask [255.255.255.0]: **255.255.255.0**
- Step 9** Assign a default gateway:
Enter default gateway [10.1.9.1]: **10.0.P.2**
(where P = pod number)
- Step 10** Press **Enter** to accept the default setting for Telnet services:
Enter telnet-server status [disabled]: **<Enter>**
- Step 11** Press **Enter** to accept the default web server port:
Enter web-server port [443]: **<Enter>**
- Step 12** Enter **yes** when prompted to modify the current ACL. The current ACL entries appear:
Modify current access list? [no] **yes**
Current access list entries:
[1] 10.0.0.0 255.0.0.0
Delete:
- Step 13** Enter **1** to delete the default ACL entry:
Delete: **1**
Delete:
- Step 14** Press **Enter** again:
Delete: **<Enter>**
Permit:
- Step 15** Enter the IP address of your student PC:
Permit: **10.0.P.12**
Permit:
- Step 16** Press **Enter** again:
Permit: **<Enter>**

Step 17 Press **Enter** to answer no when prompted to modify system clock settings:

```
Modify system clock settings?[no]: <Enter>
```

The following configuration was entered.

```
networkParams
ipAddress 10.0.P.4
defaultGateway 10.0.P.2
hostname sensorP
accessList ipAddress 10.0.P.12 netmask 255.255.255.255
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
```

[0] Go to the command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration and exit setup.

Enter your selection[0]:

Step 18 Enter **2** to select “Save this configuration and exit setup.”

```
Enter your selection[0]: 2
```

```
Configuration Saved.
```

```
*17:06:26 UTC Fri Oct 03 2003
```

```
Modify system date and time?[no]:
```

Step 19 Enter **yes** to modify the system date and time:

```
Modify system date and time?[no]: yes
```

Step 20 Enter today’s date in the following format: YYYY-MM-DD

```
Local Date []: <YYYY-MM-DD>
```

Step 21 Use 24-hour time to enter the current time in the following format: hh:mm:ss

```
Local Time []: <hh:mm:ss>
```

```
sensor#
```

Step 22 Reboot the Sensor:

```
sensor# reset
```

Warning: Executing this command will stop all applications and reboot the node.

Continue with reset? :

(where P = pod number)

Step 23 Enter **yes** to continue rebooting the Sensor:

Warning: Executing this command will stop all applications and reboot the node.

Continue with reset? : **yes**

Task 2—Navigate the CLI

Complete the following steps to familiarize yourself with the command line interface. Observe the output of the commands carefully.

Step 1 Log back in to the Sensor using the username **cisco** and the password **iattacku2**.

Step 2 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
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 3 Enter the second level of the CLI, configuration mode:

```
sensorP# configure terminal
```

```
sensorP(config)#
```

(where P = pod number)

Step 4 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)#
(where P = pod number)

```

Step 5 Enter a third-level mode, interface command-control configuration mode:

```

sensorP(config)# interface command-control
sensorP(config-if)#
(where P = pod number)

```

Step 6 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 7 Exit interface command-control configuration mode:

```
sensorP(config-if)# exit
sensorP(config)#
(where P = pod number)
```

Step 8 Enter another third-level mode, interface group configuration mode:

```
sensorP(config)# interface group 0
sensorP(config-ifg)#
(where P = pod number)
```

Step 9 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 10 Exit interface group configuration mode:

```
sensorP(config-ifg)# exit
sensorP(config)#
(where P = pod number)
```

Step 11 Enter another third-level mode, interface sensing configuration mode:

```
sensorP(config)# interface sensing int0
sensorP(config-ifs)#
(where P = pod number)
```

Step 12 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 13 Exit interface sensing configuration mode:

```
sensorP(config-ifs)# exit
sensorP(config)#
(where P = pod number)
```

Step 14 Display the services that can be configured via the CLI:

```
sensorP(config)# service ?
alarm-channel-configuration      Enter configuration mode for the
                                  alarm channel
Authentication
user                             Enter configuration mode for
                                  authentication options
Host
node                             Enter configuration mode for
                                  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 15 Enter another third-level mode, virtual alarm configuration mode:

```
sensorP(config)# service alarm-channel-configuration virtualAlarm
sensorP(config-acc)#
(where P = pod number)
```

Step 16 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 17 Exit virtual alarm configuration mode:

```
sensorP(config-acc)# exit
sensorP(config)#
(where P = pod number)
```

Step 18 Enter another third-level mode, virtual sensor configuration mode:

```
sensorP(config)# service virtual-sensor-configuration virtualSensor
sensorP(config-vsc)#
(where P = pod number)
```

Step 19 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 20 Enter a fourth level mode, micro-engine tuning mode:

```
sensorP(config-vsc)# tune-micro-engines
sensorP(config-vsc-virtualSensor)#
(where P = pod number)
```

Step 21 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.
for               Use SummaryKey to define the address view
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.UDPUDP Floods directed at a single host
FLOOD.NET         Multi-protocol floods directed at a network
segment. Ip Addresses are wildcarded for
inspection.
this
```

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 22 Exit micro-engine tuning mode:

```
sensorP(config-vsc-virtualSensor)# exit
sensorP(config-vsc)#
(where P = pod number)
```

Step 23 Exit virtual sensor configuration mode:

```
sensorP(config-vsc)# exit
sensorP(config)#
(where P = pod number)
```

Task 3—Add a Network to the Network Access Control List

Complete the following steps to add your peer pod's network to the ACL:

Step 1 Enter host configuration mode:

```
sensorP(config)# service host
sensorP(config-Host)#
(where P = pod number)
```

Step 2 Enter network parameters configuration mode:

```
sensorP(config-Host)# networkParams
sensorP(config-Host-net)#
(where P = pod number)
```

Step 3 View the current settings:

```
sensorP(config-Host-net)# show settings
networkParams
  ipAddress: 10.0.P.4
  netmask: 255.255.255.0 <defaulted>
  defaultGateway: 10.0.P.2
  hostname: sensorP
  telnetOption: disabled default: disabled
  accessList (min: 0, max: 512, current: 1)
    ipAddress: 10.0.P.12
    netmask: 255.255.255.255 default:
    255.255.255.255
```

(where P = pod number)

Step 4 Add your peer pod's network to the ACL:

```
sensorP(config-Host-net)# accessList ipAddress 10.0.Q.0 netmask  
255.255.255.0
```

(where P = pod number, Q = peer pod number)

Step 5 View your changes:

```
sensorP(config-Host-net)# show settings  
networkParams  
    ipAddress: 10.0.P.4  
    netmask: 255.255.255.0 <defaulted>  
    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>  
    ipAddress: 10.0.Q.0  
    netmask: 255.255.255.0 default:  
    255.255.255.255
```

(where P = pod number)

Step 6 Exit network parameters configuration mode:

```
sensorP(config-Host-net)# exit  
sensorP(config-Host)#
```

(where P = pod number)

Step 7 Exit configure host mode:

```
sensorP(config-Host)# exit
```

Step 8 Press **Enter** to apply your changes:

```
Apply Changes:? [yes] : <Enter>
```

(where P = pod number)

Task 4—Test Your Initial Configuration

Complete the following steps to test your Sensor's configuration:

- Step 1** Establish an SSH session to your peer pod Sensor at IP address 10.0.Q.4 (where Q = peer pod number).
- Step 2** Log in to the Sensor with the administrator account, **cisco**, and the password **iattacku2**. Access to your peer pod Sensor should be allowed.
- Step 3** Exit the SSH session.
- Step 4** 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.

Task 5—Create and Test User Accounts

Complete the following steps to create user accounts on your Sensor:

Step 1 From configuration mode, create a service account:

```
sensorP(config)# username service password servpass privilege service
(where P = pod number)
```

Step 2 Create a user with administrative privileges:

```
sensorP(config)# username admin password adminpass privilege
administrator
(where P = pod number)
```

Step 3 Create a user with viewer privileges:

```
sensorP(config)# username view password viewpass privilege viewer
(where P = pod number)
```

Step 4 Create a user with operator privileges:

```
sensorP(config)# username oper password operpass privilege operator
(where P = pod number)
```

Step 5 Exit configuration mode:

```
sensorP(config)# exit
sensorP#
(where P = pod number)
```

Step 6 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 7 Exit privileged exec mode:

```
sensorP# exit
sensorP login:
(where P = pod number)
```

Step 8 Log in with the viewer account:

```
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 9 Display the monitoring interface:

```
sensorP# show interfaces sensing
```

```
Sensing int0 is down
```

```
Hardware is eth0, TX
```

```
Reset port
```

```
Sensing int2 is down
```

```
Hardware is eth2, TX
```

```
Reset port
```

```
Sensing int3 is down
```

```
Hardware is eth3, TX
```

```
Reset port
```

```
Sensing int4 is down
```

```
Hardware is eth4, TX
```

```
Reset port
```

```
Sensing int5 is down
```

```
Hardware is eth5, TX
```

```
Reset port
```

```
sensorP#
```

(where P = pod number)

Step 10 Enter configuration mode:

```
sensorP# configure terminal
sensorP(config)#
(where P = pod number)
```

Step 11 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 12 Attempt to add a TLS trusted host to the system:

```
sensorP(config)# tls trusted-host ip-address 10.0.P.12
^
% INVALID INPUT DETECTED AT '^' MARKER
sensorP(config)#
(where P = pod number)
```

Step 13 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 14 Log out of the viewer account:

```
sensorP(config)# exit
sensorP# exit
sensorP login:
(where P = pod number)
```

Step 15 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 16 Enter configuration mode:

```
sensor# configure terminal
```

```
sensorP(config)#
```

(where P = pod number)

Step 17 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 18 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 19 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 20 Log out of the operator account:

```
sensorP(config)# exit
```

```
sensorP# exit
sensorP login:
(where P = pod number)
```

Step 21 Log in with the administrator account, admin:

```
Sensor login: admin
Password: adminpass
***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 22 Enter configuration mode:

```
sensorP# configure terminal
sensorP(config)#
```

Step 23 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 6—Configure and Test Account Locking

Complete the following steps to limit the number of times a user can attempt authentication before the account becomes disabled:

Step 1 Enter service authentication mode:

```
sensorP(config)# service authentication
sensorP(config-Authentication)#
```

(where P = pod number)

Step 2 Enter the general authentication application configuration mode:

```
sensorP(config-Authentication)# general  
sensorP(config-Authentication-gen)#  
(where P = pod number)
```

Step 3 Set the attempt limit to three:

```
sensorP(config-Authentication-gen)# attemptLimit 3  
sensorP(config-Authentication-gen)#  
(where P = pod number)
```

Step 4 Exit the general authentication application configuration mode:

```
sensorP(config-Authentication-gen)# exit  
sensorP(config-Authentication)#  
(where P = pod number)
```

Step 5 Exit service authentication mode:

```
sensorP(config-Authentication)# exit  
Apply Changes:?[yes]:
```

Step 6 Press **Enter** to apply your changes:

```
Apply Changes:?[yes]: <Enter>  
sensorP(config)#  
(where P = pod number)
```

Step 7 Log out of the administrator account:

```
sensorP(config)# exit  
sensorP# exit  
sensorP login:  
(where P = pod number)
```

Step 8 Attempt three times to log into the operator account with an incorrect password:

```
Sensor login: oper  
Password: badpassword  
Login incorrect
```

```
login: oper  
Password: badpassword  
Login incorrect
```

```
login: oper  
Password: badpassword
```

Login incorrect

login:

- Step 9** Attempt to log into the operator account with the correct password, operpass. Authentication should fail:

login: **oper**

Password: **operpass**

Authentication

SensorP login:

(where P = pod number)

- Step 10** Log in with the administrator account, admin:

Sensor login: **admin**

Password: **adminpass**

- Step 11** Display all user accounts. The parentheses indicate that the operator account, (oper), is disabled:

sensorP# **show users all**

CLI ID	User	Privilege
* 973	cisco	administrator
	service	service
	admin	administrator
	view	viewer
	(oper)	operator

(where P = pod number)

- Step 12** Enter configuration mode:

sensorP# **configure terminal**

sensorP(config)#

(where P = pod number)

- Step 13** Re-enable the operator account by changing the account password:

sensorP(config)# **password oper**

Enter new login password : **resetpassword**

Re-enter new login password: **resetpassword**

sensorP(config)#

- Step 14** Log out of the administrator account:

sensorP(config)# **exit**

sensorP# **exit**

sensorP login:

(where P = pod number)

Step 15 Log in with the operator, oper:

```
Sensor login: oper  
Password: resetpassword  
sensorP#  
(where P = pod number)
```

Task 7—Remove a User Account

Complete the following steps to remove a user account:

Step 1 Log out of the operator account:

```
sensorP# exit  
sensorP login:  
(where P = pod number)
```

Step 2 Log in with the administrator, admin:

```
Sensor login: admin  
Password: adminpass  
sensorP#  
(where P = pod number)
```

Step 3 Enter configuration mode:

```
sensorP# configure terminal  
sensorP(config)#  
(where P = pod number)
```

Step 4 Remove the viewer account:

```
sensorP(config)# no username view  
sensorP(config)#  
(where P = pod number)
```

Step 5 Exit configuration mode:

```
sensorP(config)# exit  
sensorP#  
(where P = pod number)
```

Step 6 Verify that the user has been removed:

```
sensorP# show users all  
  
CLI ID      USER          PRIVILEGE  
* 1043      cisco          ADMINISTRATOR  
           service       SERVICE  
           admin         ADMINISTRATOR  
           oper          OPERATOR
```

```
sensorP#  
(where P = pod number)
```

Task 8—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 and observe the ACL entries:

Note You can press **Ctrl-C** to return to the CLI prompt.

```
sensorP# more backup-config  
! -----  
service Authentication  
general  
attemptLimit 3  
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.Q.0 netmask 255.255.255.0  
exit  
optionalAutoupgrade  
active-selection none  
exit  
timeParams  
summerTimeParams  
active-selection none  
exit  
exit
```



```
exit
```

```
.  
. .  
. .
```

(where P = pod number)

Step 3 Enter configuration mode:

```
sensorP# configure terminal
```

```
sensorP(config)#
```

(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 submode:

```
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 submode:

```
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:

```
sensorP(config)# exit
```

```
sensorP#  
(where P = pod number)
```

- Step 11** Display the Sensor's current configuration, but limit it so that only the ACL entries are shown. Notice that the trusted hosts lists contains the host you just added:

```
sensorP# show configuration | include accessList  
accessList ipAddress 10.0.P.12 netmask 255.255.255.255  
accessList ipAddress 10.0.Q.0 netmask 255.255.255.0  
accessList ipAddress 10.0.P.13 netmask 255.255.255.255
```

- Step 12** Overwrite the current configuration with the backup configuration:

```
sensorP# copy /erase backup-config current-config  
(where P = pod number)
```

- Step 13** View the ACLs in 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# show configuration | include accessList  
accessList ipAddress 10.0.P.12 netmask 255.255.255.255  
accessList ipAddress 10.0.Q.0 netmask 255.255.255.0
```

Task 9—Display Events

Complete the following steps to practice troubleshooting the Sensor via the CLI.

- Step 1** Display all events that occurred since 8:00 a.m. today:

Note The following command and command output is an example. The command you enter should contain the current date and produce output that is similar to the example. You can press **Ctrl-C** at any time to return to the CLI prompt.

```
sensorP# show events 8:00 april 1 2004  
evLogTransaction: command=getVersion eventId=1062838476053560057  
successful=true  
  
originator:  
  hostId: sensorP  
  appName: mainApp  
  appInstanceId: 1047  
time: 2004/10/03 19:36:26 2003/10/03 19:36:26 UTC  
requestor:  
  user: cids  
  application:  
    hostId: localhost  
    appName: cidwebserver  
    appInstanceId: 1089
```

evError: eventId=1062838476053560058 severity=warning
originator:
 hostId: sensorP
 appName: sshd
 appInstanceId:
time: 2004/10/03 19:36:28 2003/10/03 19:36:28 UTC
errorMessage: name=errSyslog Starting sshd:

evError: eventId=1062838476053560059 severity=warning
originator:
 hostId: sensorP
 appName: sshd
 appInstanceId:
time: 2004/10/03 19:36:28 2003/10/03 19:36:28 UTC
errorMessage: name=errSyslog succeeded

evError: eventId=1062838476053560060 severity=warning
originator:
 hostId: sensorP
 appName: sshd
 appInstanceId:
time: 2004/10/03 19:36:28 2003/10/03 19:36:28 UTC
errorMessage: name=errSyslog ^[[60G

evAlert: eventId=1062838476053561489 severity=informational
originator:
 hostId: sensorP
 appName: sensorApp
 appInstanceId: 1092
time: 2004/10/06 08:00:26 2003/10/06 08:00:26 UTC
interfaceGroup: 0
vlan: 0
signature: sigId=7102 sigName=Reply-to-Broadcast subSigId=0
version=S37
participants:
 attack:
 attacker: proxy=false
 addr: locality=OUT 172.30.1.2
 victim:

```
addr: locality=OUT 172.30.1.2
alertDetails: Traffic Source: int0 ;
--MORE--
```

Step 2 Display log events that have occurred since 8:00 this morning:

Note The following command and command output is an example. The command you enter should contain the current date and produce output that is similar to the example. You can press **Ctrl-C** at any time to return to the CLI prompt.

```
sensorP# show events log 8:00 april 1 2004
evLogTransaction: command=execAuthenticateUser
eventID=1074345371890293085 successful=true
originator:
  hostId: sensorP
  appName: authentication
  appInstanceId: 1103
  time: 2004/02/16 09:25:15 2004/02/16 09:25:15 UTC
  requestor:
    user: oper
    application:
      hostId: CONSOLE
      appName: -cidcli
      appInstanceId: 1104
```

```
--MORE--
```

(where P = pod number)

Step 3 Delete events from the EventStore:

```
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
sensorP#
```

Step 5 Verify that events have been cleared from the EventStore by again displaying all events that have occurred since 8:00 a.m. this morning:

Note The following command and command output is an example. The command you enter should contain the current date and produce output that is similar to the example. You can press **Ctrl-C** at any time to return to the CLI prompt.

```
sensorP# show events 8:00 april 1 2004
```

(where P = pod number)

Step 6 Enter **Ctrl-C** to return to the CLI prompt.

Task 10—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 EventStore statistics and note the number of status events.

Note Current statistics could vary.

```
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 = 2
```

```
    Shun request events = 0
```

```
Error events, warning = 3
Error events, error = 0
Error events, fatal = 0
Alert events, informational = 49
Alert events, low = 0
Alert events, medium = 0
Alert events, high = 0
```

(where P = pod number)

Step 3 Display the command-control interface view of statistics:

```
sensorP# show interface command-control
command-control is up
  Internet address is 10.0.P.4, subnet mask is 255.255.255.0, telnet
  is
  enabled.
  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:155245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6709 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:13013548 (12.4 Mb)  TX bytes:1726221 (1.6 Mb)
          Interrupt:16 Base address:0xdcc0 Memory:feb20000-feb40000
```

```
sensorP#
```

(where P = pod number)

Step 4 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 = 9908
  Measure of the level of resource utilization = 0
  Total number of packets processed since reset = 9967
  Total number of IP packets processed since reset = 4636
```

```

Total number of packets that were not IP processed since reset =
5331
Total number of TCP packets processed since reset = 0
Total number of UDP packets processed since reset = 360
Total number of ICMP packets processed since reset = 0
Total number of packets that were not TCP, UDP, or ICMP
processed
since reset = 4276
Total number of ARP packets processed since reset = 62
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 = 792102
The rate of packets per second since reset = 1
The rate of bytes per second since reset = 79
The average bytes per packet since reset = 79
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 = 12
TCP nodes keyed on both IP addresses and both ports = 0
UDP nodes keyed on both IP addresses and both ports = 1
IP nodes keyed on both IP addresses = 3
```

The number of each type of node inserted since reset

```
Total nodes inserted = 174
TCP nodes keyed on both IP addresses and both ports = 0
UDP nodes keyed on both IP addresses and both ports = 60
IP nodes keyed on both IP addresses = 78
```

The rate of nodes per second for each time since reset

```
Nodes per second = 0
second TCP nodes keyed on both IP addresses and both ports per
= 0
second UDP nodes keyed on both IP addresses and both ports per
= 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 = 61
Number of alarms excluded by filters = 0
Number of alarms removed by summarizer = 0
Number of alarms sent to the Event Store = 61
```

(where P = pod number)

Task 11—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 EventStore statistics again. Notice the increment in status events:

```
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 = 4
```

```
    Log transaction events = 14
```

```
    Shun request events = 0
```

```
    Error events, warning = 71
```

```
    Error events, error = 0
```

```
    Error events, fatal = 0
```

```
    Alert events, informational = 58
```

```
    Alert events, low = 0
```

```
    Alert events, medium = 0
```

```
    Alert events, high = 0
```

```
sensorP#
```

(where P = pod number)

Lesson 6

Lab Exercise—Cisco IDS Device Manager and Event Viewer

Complete this lab exercise to practice what you learned in this lesson.

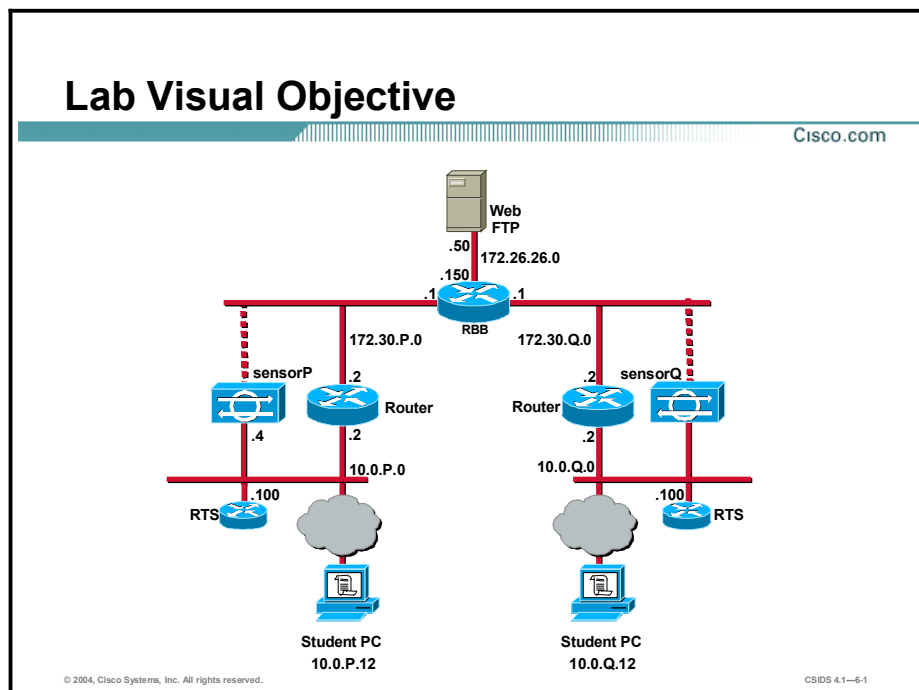
Objective

In this lab exercise you will complete the following tasks:

- Access and navigate the IDS Device Manager (IDM).
- Enable the Sensor's sensing interface.
- Install IEV software on the student PC.
- Add IDS devices to the list of devices monitored by IEV.
- Review the status of your Sensor.
- Monitor Cisco IDS events using the IEV Realtime Dashboard.
- Investigate alerts via IEV default views.
- Create a filter and apply it to a view.
- Test your filter.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



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 panel.
- 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—Enable the Sensor's Sensing Interface

Complete the following steps to enable the Sensor's sensing interface:

- Step 1** Choose **Configuration > Sensing Engine** from the IDM. The Sensing Engine window opens.
- Step 2** Select **Interfaces** from the TOC. The Interfaces page is displayed.
- Step 3** Select the checkbox for **int0** and click **Enable**. The following message is displayed:
Configuration update is in progress. This page will be unavailable for a few minutes.
- Step 4** Click **OK**. The Interfaces page is displayed with the following message:
Configuration update is in progress. This page will be unavailable for a few minutes.
- Step 5** Select **Interfaces** from the TOC. The Interfaces page is refreshed.
- Step 6** Verify that int0 displays **Yes** in the Enabled column.

Task 3—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 from the student PC desktop 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 4—Add the IDS Devices to the List of Devices Monitored by IEV

Complete the following steps to add the IDS devices to the list of devices monitored by 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 substeps:
 - 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 **resetpassword** 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) option 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.

- Click **Yes** to accept the certificate. Your Sensor appears in the Devices folder on the left side of the screen.

Task 5—Review the Status of Your Sensor

Complete the following steps to review the version information and connection status for your Sensor:

- Step 1** Right-click the **sensorP** icon in the Devices folder and click **Device Status**. The Device Status dialog box displays Connection Status, Sensor Version, Web Server Statistic Information, Event Server Statistic Information, and Analysis Engine Statistic Information.
- Step 2** Verify that the device status is **Subscription successfully opened**.
- Step 3** Click **OK** to close the Device Status dialog box.

Task 6—Monitor Cisco IDS Events Using the IEV Realtime Dashboard

Complete the following steps to monitor Cisco IDS events using IEV's Realtime Dashboard:

- 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** Open a web browser and enter the following URL to trigger the WWW IIS Unicode Attack signature on your peer Sensor. Also, have your peer trigger the WWW IIS Unicode Attack on your Sensor:

<http://10.0.Q.12/scripts/..%c0%af../winnt/system32>

(where Q = peer pod number)

- Step 4** Maximize the Realtime Dashboard and observe the events displayed as a result of your peer triggering the WWW IIS Unicode Attack on your Sensor. The Realtime Dashboard displays the most recent events received by the Sensor since the request was opened.
- Step 5** Fill in the table by completing the following substeps:
 - Right-click the **Signature Name** column heading and select **Show All Columns**.
 - Right-click **WWW IIS Unicode attack** and select **Show Context**.
 - Right-click **IIS Unicode attack** and select **NSDB Link**.

Subhead	Value
Signature Name	
Sig ID	
Severity level	
Device name	
Event UTC date and time	
Event local date and time	

Subhead	Value
Source address	
Destination address	
Source port	
Destination port	
Event ID	
Trigger string	
App name	
Receive date	
Receive time	
Subsig ID	
Sig details	
Sig version	
Total attacks	
Source locality	
Dst locality	
Summary count	
Interface group	
Vlan	
Context	

Step 6 Close the Realtime Dashboard.

Task 7—Investigate Alerts Via IEV Default Views

Complete the following steps to investigate alarms via the IEV default Sig Name Group view:

Step 1 Enter the following URL in your browser to trigger the WWW WinNT cmd.exe signature on your peer Sensor. Also, have your peer trigger the WWW WinNT cmd.exe signature on your Sensor.

<http://10.0.Q.12/scripts/./%35c./winnt/system32/cmd.exe?/c+dir>

(where Q = peer pod number)

Step 2 Click the **Refresh** icon in the IEV toolbar.

Step 3 Complete the following substeps to investigate the alert that appears when your peer triggers the WWW WinNT cmd.exe signature on your Sensor:

1. Double-click the **Sensor Name Group** view from the Views folder. The alert is displayed in the Sensor Name Group view in the pane on the right.
2. Double-click the **Sig Name Group** view from the Views folder. The alert is displayed in the Sig Name Group view in the pane on the right.

3. Right-click **WWW WinNT cmd.exe access** in the Signature Name column and select **Expand Whole Details**. The Expanded Details Dialog window opens with the Whole Address panel displayed.
4. Right-click the alarm in the Expanded Details Dialog window and choose **View Alarms**. The Alarm Information Dialog window opens.
5. Right-click a column heading and choose **Show All Columns** to display all the data associated with the alarm.
6. Use the horizontal scroll bar to view the available information. Notice that the Captured Packet column is blank. This is because the signature is not configured for packet capture.
7. Right-click the alarm and choose **Show Context** to view the context data associated with the alarm. The Decode Alarm Context window opens and displays the context data.

Step 4 Close the Decoded Alarm Context window.

Step 5 Close the Alarm Information Dialog window.

Step 6 Close the Expanded Details Dialog window.

Step 7 Right-click the **Sig Name Group** tab and select **Delete All Rows from Database**. The Confirmation window opens.

Step 8 Click **Yes** to confirm the deletion.

Step 9 Right-click the **Sensor Name Group** tab and select **Delete All Rows from Database**. The Confirmation window opens.

Step 10 Click **Yes** to confirm the deletion.

Task 8—Create a Filter and Apply It to a View

Complete the following steps to create a filter that excludes alarms having a severity level of medium, low, or informational:

Step 1 From the IDS Event Viewer main menu, choose **File > New > Filter**. The Filter Properties window opens.

Step 2 Enter **MyFilter** in the Filter Name field.

Step 3 Select the **By Severity** check box under Filter Functions.

Step 4 Select the **Informational**, **Low**, and **Medium** severity level check boxes from the Excluded Alarm Severity Levels panel.

Step 5 Click **OK** to save the filter. The filter is added to the Filters folder and can now be used in a view.

Step 6 Right-click **Sig Name Group** in the Views folder and select **Properties**. The View Wizard window opens.

Step 7 Select the **Use Filter** check box, and select **MyFilter** from the drop-down menu.

Step 8 Click **Finished**. A Warning window opens and displays the following message:

View 'Sig Name Group' already exists, overwrite it?

Step 9 Click **Yes**.

Task 9—Test Your Filter

Complete the following steps to test the filter you created:

- Step 1** Double-click the **Sig Name Group** view in the Views folder list. The Sig Name Group tab is displayed in the pane on the right.
- Step 2** Generate a web alert by entering the following URL in your browser to trigger the WWW WinNT cmd.exe signature on your peer Sensor. Also, have your peer trigger the WWW WinNT cmd.exe signature on your Sensor:

<http://10.0.Q.12/scripts/./%3c./winnt/system32/cmd.exe?/c+dir>

(where Q = peer pod number)

- Step 3** Click **Refresh** in the IEV toolbar. No alerts should appear in the Sig Name Group view.
- Step 4** Double-click **Sensor Name Group** in the Views folder. The alert generated by your peer is displayed in the pane on the right.

Lesson 7

Lab Exercise—Sensor Configuration

Complete the following lab exercise to practice what you learned in this lesson.

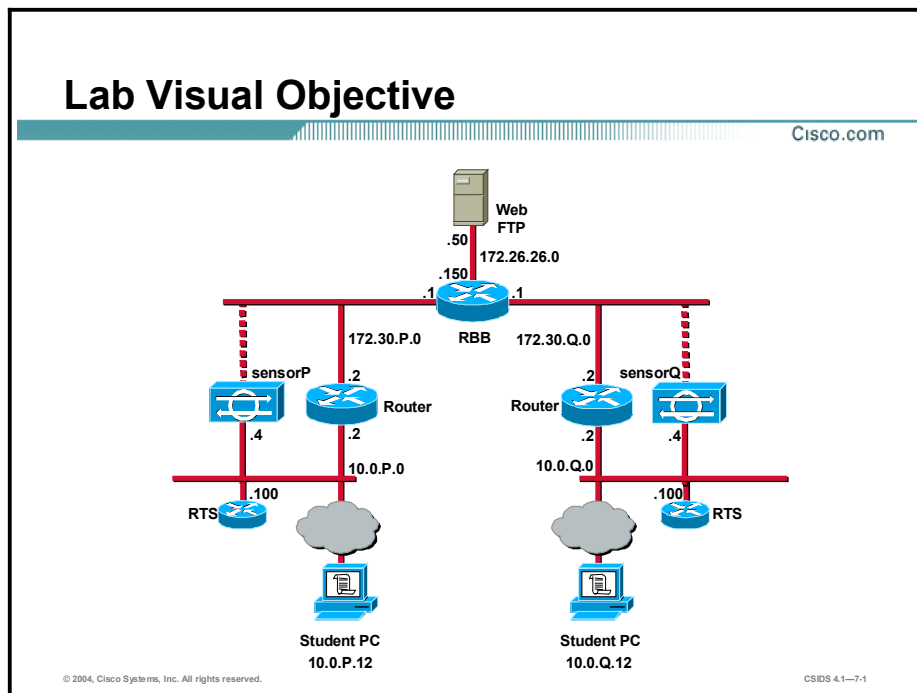
Objective

In this lab exercise you will complete the following tasks:

- Verify the Sensor's network settings.
- Add allowed hosts.
- Add users.
- Configure the events display.
- View Sensor statistics.
- View diagnostics and system information.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



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 pod number. The S in an IP address, name, or command indicates the pod number of a secondary peer pod assigned by the instructor. Make sure to replace it with your secondary peer pod number.
-------------	---

Setup

Before starting this lab exercise, your instructor will pair you with a pod other than your usual peer pod.

Task 1—Verify the Sensor’s Network Settings

Complete the following steps to access the IDM on the Sensor:

- Step 1** If IEV is open, close it.
- Step 2** Launch your web browser and specify the Sensor as the location. To do this, enter the following URL in your web browser:
https://10.0.P.4
(where P = pod number)
- Step 3** Click **Yes** when the Security Alert panel appears asking if you want to proceed.
- Step 4** Log in to the IDM as user **admin**. The admin password is **adminpass**.

Note	If you receive the message “User limit has been reached,” click click here to force login .
-------------	--

- Step 5** Choose **Device > Sensor Setup > Network**. The Network page is displayed.
- Step 6** Verify that **sensorP** appears in the Host Name field.
(where P = pod number)
- Step 7** Verify that your Sensor’s IP address, **10.0.P.4**, appears in the IP Address field.
(where P = pod number)
- Step 8** Verify that **255.255.255.0** appears in the Netmask field.
- Step 9** Verify that the default gateway for the Sensor, **10.0.P.2**, appears in the Default Route field.
(where P = pod number)
- Step 10** Verify that the **Enable TLS/SSL** check box is selected to enable TLS/SSL in the web server.
- Step 11** Verify that **443** appears in the Web Server Port field.

Task 2—Add Allowed Hosts

Complete the following steps to enable your student PC to access the Sensor of a secondary peer pod assigned for this task.

Step 1 Verify that you are unable to establish an SSH connection to the secondary peer pod Sensor by completing the following substeps:

1. Double-click the Tera Term Pro SSH icon on your desktop. The Tera Term: New Connection window opens.
2. Enter the IP address of the secondary peer pod Sensor, **10.0.S.4**, in the Host field.
(where S = secondary peer pod number)
3. Select the SSH radio button.
4. Click **OK**. The SSH Authentication window opens.
5. Enter **admin** in the user name field and **adminpass** in the passphrase field.
6. Click **OK**. The connection should time out.

Step 2 Select **Device > Sensor Setup > Allowed Hosts**. The Allowed Hosts page is displayed.

Step 3 Click **Add**. The Adding panel is displayed.

Step 4 Enter **10.0.S.12** in the IP Address field.

(where S = secondary peer pod number)

Step 5 Enter **255.255.255.255** in the Netmask field.

Step 6 Click **Apply to Sensor** to save and apply your changes. The Allowed Hosts page refreshes with the host information you entered.

Step 7 Verify that you can now establish an SSH connection to your secondary peer pod Sensor by completing the following substeps:

1. Double-click the Tera Term Pro SSH icon on your desktop. The Tera Term: New Connection window opens.
2. Enter the IP address of your secondary peer pod Sensor, **10.0.S.4**, in the Host field.
(where S = secondary peer pod number)
3. Select the **SSH** radio button.
4. Click **OK**. The Security Warning window opens.
5. Click **Continue**. The SSH Authentication window opens.
6. Enter **admin** in the user name field and **adminpass** in the passphrase field.
7. Click **OK**. The login should be successful.

Task 3—Add Users

Complete the following steps to add a user via IDM:

Step 1 Select **Device > Sensor Setup > Users**. The Users page is displayed.

Step 2 Click **Add** to add a user. The Adding panel is displayed.

Step 3 Enter the username **admin2** in the User Name field.

- Step 4** Enter the password **admin2pass** in the Password field.
- Step 5** Enter the password **admin2pass** in the Password Again field.
- Step 6** Choose **Administrator** from the User Role drop-down menu.
- Step 7** Click **Apply to Sensor** to save your changes. The Users page appears displaying the new user you created.
- Step 8** Click the **logout** icon in the upper right-hand corner of the window. The following message appears:

```
You are currently logged out
Click here to login to IDM
```
- Step 9** Click **Click here to log in to IDM**. The login prompt appears.
- Step 10** Log in with the username **admin2** and the password **admin2pass**.

Task 4—Configure the Events Display

Complete the following steps to configure the events display and view events in IDM:

- Step 1** Trigger the WWW IIS Unicode Attack signature on your peer pod Sensor to generate an IDS alert by entering the following URL in your browser:

```
http://10.0.Q.12/scripts/..%c0%af../winnt/system32
```

(where Q = peer pod number)
- Step 2** Select **Monitoring > Events**. The Events page is displayed.
- Step 3** Select the **Show Alerts** and **High** check boxes.
- Step 4** Enter the approximate time at which you started this task as the Start Time.
- Step 5** Enter today's date as the Start Date.
- Step 6** Click **Apply to Sensor**. The Events page refreshes, displaying no events.
- Step 7** Select **Monitoring > Events** again. The Events page is displayed.
- Step 8** Select the **Show Alerts** and **Medium** check boxes.
- Step 9** Enter the approximate time at which you started this task as the Start Time.
- Step 10** Enter today's date as the Start Date.
- Step 11** Click **Apply to Sensor**. The Events page refreshes displaying alerts generated by your peer in Step 1.

Task 5—View Sensor Statistics

Complete the following steps to display statistics for your Sensor:

- Step 1** Select **Monitoring > Statistics**. The Statistics page is displayed.
- Step 2** Scroll to the bottom of the page and observe the Authentication Statistics.
- Step 3** Open another browser window and complete the following substeps to create a login failure:

1. Enter **https://10.0.P.4** in the web browser Address field. The Security Alert window opens. (where P = peer pod number)
2. Click **Yes**. The Enter Network Password window opens.
3. Enter **badpassword** in the username and password fields.
4. Click **OK**.

Step 4 Return to your IDM browser session and select **Monitoring > Statistics**.

Step 5 Scroll to the bottom of the page and observe the Authentication Statistics again. The number of total authentication attempts and failed authentication attempts should have incremented.

Task 6—View Diagnostics and System Information

Complete the following steps to view diagnostics and system information:

Step 1 To view diagnostics, complete the following substeps:

1. Select **Administration > Support > Diagnostics**. The Diagnostics page is displayed.
2. Click **Run Diagnostics**. The following message appears:

Diagnostics are being generated. Please stand by.

3. When the View Diagnostics Result page is displayed, click **View Results** to see the diagnostics report. The System Status Report appears in HTML format in another window.
4. Close the System Status Report.

Step 2 Select **Administration > Support > System Information** to view system information. The System Information page is displayed.

Lesson 9

Lab Exercise—Configuring Signatures

Complete the following lab exercise to practice what you learned in this lesson.

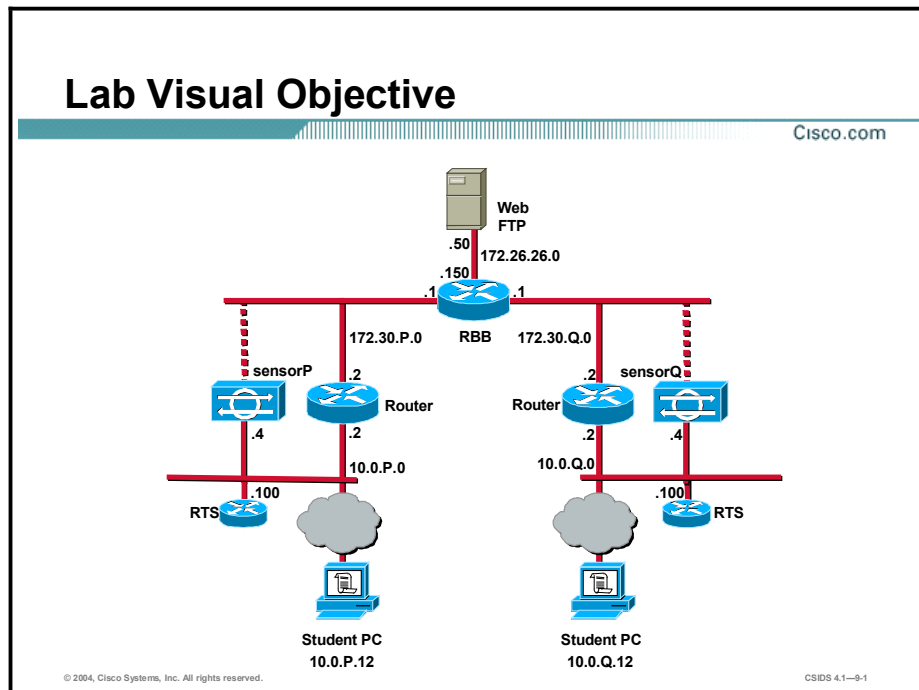
Objective

In this lab exercise you will complete the following tasks:

- Tune a signature via IDM's signature configuration mode.
- Test the tuned signature.
- Modify the tuned signature to trigger an alarm only on a specific IP address.
- Test the modified tuned signature.
- Create a custom signature via IDM's signature wizard.
- Test the custom signature.
- Enable built-in signatures.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



Task 1—Tune a Signature via IDM’s Signature Configuration Mode

This task involves modifying a built-in signature’s behavior. Complete the following steps to tune a signature:

- Step 1** Choose **Configuration > Sensing Engine > Signature Configuration Mode**. The Signature Configuration Mode window opens.
- Step 2** Click **All Signatures**. The All signatures panel is displayed.
- Step 3** Select **4 [1220-2007]** from the Page popup menu. The All signatures page refreshes and displays only the signatures within the 1220–2007 range.
- Step 4** Select the check box to the left of the 2004 signature.
- Step 5** Click **Edit**. The Editing ATOMIC.ICMP - SIGID [2004] SubSig [0] page is displayed.
- Step 6** Select **high** from the AlarmSeverity drop-down menu.
- Step 7** Select **FireAll** from the AlarmThrottle drop-down menu.
- Step 8** Select **True** from the Enabled drop-down menu.
- Step 9** Enter **3** in the MinHits field.
- Step 10** Enter **Three Echo Requests** in the SigComment field.
- Step 11** Click **OK**. The following message is displayed:

```
Signature has been updated. To commit the changes please click the
save changes icon in the Activity bar.
```
- Step 12** Click **OK**. The All signatures panel is refreshed. The ICMP Echo Request signature’s Type column now displays Tuned, and its Severity column now displays high.
- Step 13** Click the save changes icon in the Activity bar.

Task 2—Test the Tuned Signature

Complete the following tasks to verify that the 2004 signature is triggered when your peer pings your Sensor:

- Step 1** Select **Start > Programs > Cisco Systems > Cisco IDS Event Viewer > Cisco IDS Event Viewer** to launch IEV.
- Step 2** Double-click **Sig Name Group** from the Views list.
- Step 3** Right-click the **Sig Name Group** tab, and clear all existing alarms in IEV by selecting the **Delete All Rows from Database** option. The confirmation window appears with the following message:

```
Do you really want to delete all the events from the table?
```
- Step 4** Click **Yes**. The Sig Name Group window is refreshed.
- Step 5** Verify that all existing alarms have been deleted.
- Step 6** Open a Windows command prompt and issue the command **ping 10.0.Q.4**. Also, have your peer ping your Sensor.

(where Q = peer pod number)

- Step 7** Click the **Refresh** button in IEV, and verify that the ping issued by your peer triggered an alert event.
- Step 8** Minimize but do not close the IEV window.

Task 3—Modify the Tuned Signature to Trigger an Alarm Only on a Specific IP Address

For this task, your instructor will assign you a secondary peer. Complete the following steps to configure a signature to trigger an alarm only on your secondary peer pod's IP address:

- Step 1** Configure the 2004 signature to fire only on your secondary peer's address by completing the following substeps:
 1. Choose **Configuration > Sensing Engine > Signature Configuration Mode**. The Signature Configuration Mode window opens.
 2. Click **All Signatures**. The All Signatures page is displayed.
 3. Select **4 [1220-2007]** from the Page popup menu. The All signatures page refreshes and displays only the signatures within the 1220–2007 range.
 4. Select the check box to the left of the 2004 signature.
 5. Click **Edit**. The Editing ATOMIC.ICMP - SIGID [2004] SubSig [0] page is displayed.
 6. Select **True** from the CapturePacket drop-down menu.
 7. Enter **10.0.S.12** in the SrcIpAddr field.

(where S = secondary peer pod number)

8. Enter **255.255.255.255** in the SrcIpMask field.
9. Click **OK**. The following message is displayed:

Signature has been updated. To commit the changes please click the save changes icon in the Activity bar.

10. Click **OK**. The All Signatures page is refreshed.

- Step 2** Click the save changes icon in the Activity bar.

Task 4—Test the Modified Tuned Signature

Complete the following steps to verify that the 2004 signature is triggered only when your secondary peer pings your Sensor:

- Step 1** Maximize the IEV window.
- Step 2** Right-click the **Sig Name Group** tab.
- Step 3** Clear all existing alarms in IEV by selecting the **Delete All Rows from Database** option. The confirmation window appears with the following message:

Do you really want to delete all the events from the table?
- Step 4** Click **Yes**. The Sig Name Group window is refreshed.

- Step 5** Verify that all existing alarms have been deleted by clicking the **Refresh** button.
- Step 6** Open a Windows command prompt and issue the command **ping 10.0.Q.4**. Also, have your peer ping your Sensor.
- (where Q = peer pod number)
- Step 7** Open a Windows command prompt and issue the command **ping 10.0.S.4**. Also, have your secondary peer ping your Sensor.
- (where S = secondary peer pod number)
- Step 8** Click the **Refresh** button in IEV again and verify that only the ping issued by your secondary peer triggered an alert event.

Task 5—Create a Custom Signature via IDM’s Signature Wizard

Complete the following steps to create a custom signature that detects three login failures to an FTP server:

- Step 1** Select **Configuration > Sensing Engine > Signature Wizard**. The Signature Wizard page is displayed.
- Step 2** Click **Start the Wizard**. A list of signature types is displayed.
- Step 3** Click the **TCP Packet Signature** radio button.
- Step 4** Click **Next**. The Signature Identification panel is displayed.
- Step 5** Enter **20001** in the SIGID field.
- Step 6** Verify that **0** appears in the SubSignature ID field.
- Step 7** Enter **FTP Auth Failure** in the Signature Name field.
- Step 8** Click **Next**. The TCP Packet Signature panel is displayed.
- Step 9** Enter **[5][3][0]** in the TCP Packet Regular Expression field. The 530 is an FTP login error message.
- Step 10** Enter **21** in the SrcPort field.
- Step 11** Select the **False** radio button for TCP FIN Flag.
- Step 12** Select the **False** radio button for TCP SYN Flag.
- Step 13** Select the **False** radio button for TCP RST Flag.
- Step 14** Select the **True** radio button for TCP PSH Flag.
- Step 15** Select the **True** radio button for TCP ACK Flag.
- Step 16** Select the **False** radio button for TCP URG Flag.
- Step 17** Click **Next**. The Alert Response Actions panel is displayed.
- Step 18** Select **high** from the Severity of the Alert drop-down menu.
- Step 19** Select **No** from the Swap Address Report Ordering drop-down menu.

- Step 20** Select **True** from the Include Packet in Alert drop-down menu.
- Step 21** Click **Next**. The Default Alert Behavior panel is displayed.
- Step 22** Click **Advanced**. The Alert Frequency panel is displayed.
- Step 23** Select the **Alert Each Time** radio button.
- Step 24** Click **Next**. The Alert Dynamic Response panel is displayed.
- Step 25** Click **Next**. The Alert Summary Key panel is displayed.
- Step 26** Click **Next**. The Ready to Create the New Signature panel is displayed.
- Step 27** Click **Create**. The following message is displayed:

```
You have successfully created the signature. Click Apply Changes on
the main page when you are ready to commit the changes.
```
- Step 28** Click **OK**. The Wizard Completed panel is displayed.
- Step 29** Click **OK**. The Signature Wizard main page is displayed.
- Step 30** Click the save changes icon in the Activity bar.

Task 6—Test the Custom Signature

Complete the following steps to test your custom signature:

- Step 1** Establish an FTP session to your peer student PC. Also, have your peer establish an FTP session to your student PC:

```
c:\>ftp 10.0.Q.12
Connected to 10.0.Q.12.
220 2KQ Microsoft FTP Service (Version 5.0).
User (10.0.Q.12:(none)):
```

(where Q = peer pod number)

- Step 2** Enter an invalid password three times by completing the following substeps:

1. Attempt to log in with the username administrator and an invalid password:

```
User (10.0.Q.12:(none)): administrator
331 Password required for user.
Password: badpassword
530 User administrator cannot log in.
Login failed.
ftp>
```

2. Make another login attempt:

```
ftp> user administrator
331 Password required for user.
Password: badpassword2
530 User administrator cannot log in.
Login failed.
```

```
ftp>
3. Make a third login attempt:

ftp> user administrator
331 Password required for user.
Password: badpassword3
530 User administrator cannot log in.
Login failed.
ftp>

(where Q = peer pod number)
```

Step 3 Click the **Refresh** button in IEV.

Step 4 Double-click **Sensor Name Group** in the Views folder. The Sensor Name Group tab becomes active.

Step 5 Right-click **sensorP** in the Sensor Name column and select **Expand Whole Details**.

(where P = pod number)

Step 6 Look at the alarms in IEV. You should see two different signatures that have fired as a result of your peer's failed login attempts. One of these is the default signature for IDS. The other is the one you created.

Note Use the signatures that fired as a result of your peer's failed login attempts to complete this task.

Step 7 Right-click **FTP Auth Failure** and select **View Alarms**. The Alarm Information Dialog window opens.

Step 8 Note the time at which the alert was triggered.

Step 9 Right-click **FTP Auth Failure** and select **Show Captured Packet**. The Ethereal Network Analyzer window opens. Wait for Ethereal to analyze the packet.

Step 10 When the packet is displayed, locate and verify the following information:

- An ACK packet triggered the alert.
- The packet contained the FTP 530 response information.
- The packet's source was 10.0.P.12.

(where P = pod number)

Step 11 Close the Ethereal Network Analyzer window.

Step 12 Establish an SSH session to your Sensor. Log in as user admin with the password adminpass.

Step 13 Display all events since the alarm was triggered:

```
sensor# show events alert <a few minutes before alarm was triggered>
<today's date>
```

Step 14 Locate the alert triggered by the 6250 built-in signature. Notice that the attacker address is your peer, 10.0.Q.12:

EvAlert: eventId=1069279392849191190 severity=informational

originator:

hostId: sensorP

appName: sensorApp

appInstanceId: 1056

time: 2003/11/20 15:32:52 2003/11/20 15:32:52 UTC

interfaceGroup: 0

vlan: 0

signature: sigId=6250 sigName=Auth Failure FTP subSigId=0
version=S47 Failed F

TP Logins

context:

fromVictim:

```
000000 32 32 30 20 32 6B 31 30 20 4D 69 63 72 6F 73 6F 220 2kP  
Microso  
000010 66 74 20 46 54 50 20 53 65 72 76 69 63 65 20 28 ft FTP  
Service (  
000020 56 65 72 73 69 6F 6E 20 35 2E 30 29 2E 0D 0A 33 Version  
5.0)...3  
000030 33 31 20 50 61 73 73 77 6F 72 64 20 72 65 71 75 31 Password  
requ  
000040 69 72 65 64 20 66 6F 72 20 62 6F 62 62 79 2E 0D ired for  
administrator..  
000050 0A 35 33 30 20 55 73 65 72 20 62 6F 62 62 79 20 .530 User  
administrator  
000060 63 61 6E 6E 6F 74 20 6C 6F 67 20 69 6E 2E 0D 0A cannot log  
in...  
000070 33 33 31 20 50 61 73 73 77 6F 72 64 20 72 65 71 331 Password  
req  
000080 75 69 72 65 64 20 66 6F 72 20 6A 61 6D 65 79 2E uired for  
administrator.  
000090 0D 0A 35 33 30 20 55 73 65 72 20 6A 61 6D 65 79 ..530 User  
administrator  
0000A0 20 63 61 6E 6E 6F 74 20 6C 6F 67 20 69 6E 2E 0D cannot log  
in..  
0000B0 0A 33 33 31 20 50 61 73 73 77 6F 72 64 20 72 65 .331  
Password re  
0000C0 71 75 69 72 65 64 20 66 6F 72 20 6A 61 73 2E 0D quired for  
administrator..  
0000D0 0A .
```

fromAttacker:

```
000000 55 53 45 52 20 62 6F 62 62 79 0D 0A 50 41 53 53 USER  
administrator..PASS  
000010 20 74 6F 6D 0D 0A 55 53 45 52 20 6A 61 6D 65 79  
badpassword..USER administrator  
000020 0D 0A 50 41 53 53 20 6A 61 6D 0D 0A 55 53 45 52 ..PASS  
badpassword2..USER
```

```
000030 20 6A 61 73 0D 0A 50 41 53 53 20 6A 61 73 0D 0A
administrator..PASS badpassword3..
```

```
000040 35 33 30
```

530

```
participants:
  attack:
    attacker: proxy=false
      addr: locality=OUT 10.0.Q.12
      port: 1400
    victim:
      addr: locality=OUT 10.0.P.12
      port: 21
  alertDetails: Traffic Source: int0 ;
```

(where Q = peer pod number)

Step 15 Locate the alert triggered by the 20001 custom signature. Notice that the attacker address is your own student PC IP address, 10.0.P.12. This is because you did not set the FlipAddr parameter in your custom signature:

```
evAlert: eventId=1069279392849191191 severity=high
originator:
  hostId: sensor1
  appName: sensorApp
  appInstanceId: 1056
time: 2003/11/20 15:32:52 2003/11/20 15:32:52 UTC
interfaceGroup: 0
vlan: 0
signature: sigId=20001 sigName=ATOMIC.TCP subSigId=0 version=Unknown
participants:
  attack:
    attacker: proxy=false
      addr: locality=OUT 10.0.P.12
      port: 21
    victim:
      addr: locality=OUT 10.0.Q.12
      port: 1400
  alertDetails: Traffic Source: int0 ;
  triggerPacket:
000000 00 08 21 D7 65 00 00 0D BC CE 98 41 08 00 45 00
..!.e.....A..E.
000010 00 45 4E F6 40 00 7F 06 95 A5 0A 00 01 0C 0A 00
.EN.@.....
000020 02 0C 00 15 05 78 36 C0 10 02 FF F3 B2 7D 50 18
.....x6.....}P.
000030 FF BF 1E 94 00 00 35 33 30 20 55 73 65 72 20 6A .....530
User administrator
```

```
000040 61 73 20 63 61 6E 6E 6F 74 20 6C 6F 67 20 69 6E cannot log
in
000050 2E 0D 0A 64 70 F8 5F ...dp._
```

Task 7—Enable Built-in Signatures

Complete the following steps to enable built-in signatures:

- Step 1** Choose **Configuration > Sensing Engine > Signature Configuration Mode**. The Signature Configuration Mode window opens.
- Step 2** Click **All Signatures**. The All Signatures page is displayed.
- Step 3** Select **18 [3212-3221]** from the Page pop-up menu. The All Signatures page refreshes and displays only the signatures within the 3212–3221 range.
- Step 4** Select the check box to the left of the 3216 signature.
- Step 5** Click **Enable**. The following message is displayed:
Selected signatures have been enabled. To commit the changes please click the save changes icon in the Activity bar.
- Step 6** Click **OK**. The All Signatures page is refreshed. The WWW Directory Traversal ../.. signature's enabled column now displays a solid circle which indicates that it is enabled.
- Step 7** Click the save changes icon in the Activity bar.
- Step 8** Select **43 [5043-5051]** from the Page popup menu. The All Signatures page refreshes and displays only the signatures within the 5043–5051 range.
- Step 9** Select the check box to the left of the 5049 signature.
- Step 10** Click **Enable**. The following message is displayed:
Selected signatures have been enabled. To commit the changes please click the save changes icon in the Activity bar.
- Step 11** Click **OK**. The All Signatures page is refreshed. The WWW IIS showcode.asp access signature's enabled column now displays a solid circle which indicates that it is enabled.
- Step 12** Click the save changes icon in the Activity bar.

Lesson 10

Lab Exercise—Signature and Sensor Configuration

Complete the following lab exercise to practice what you learned in this lesson.

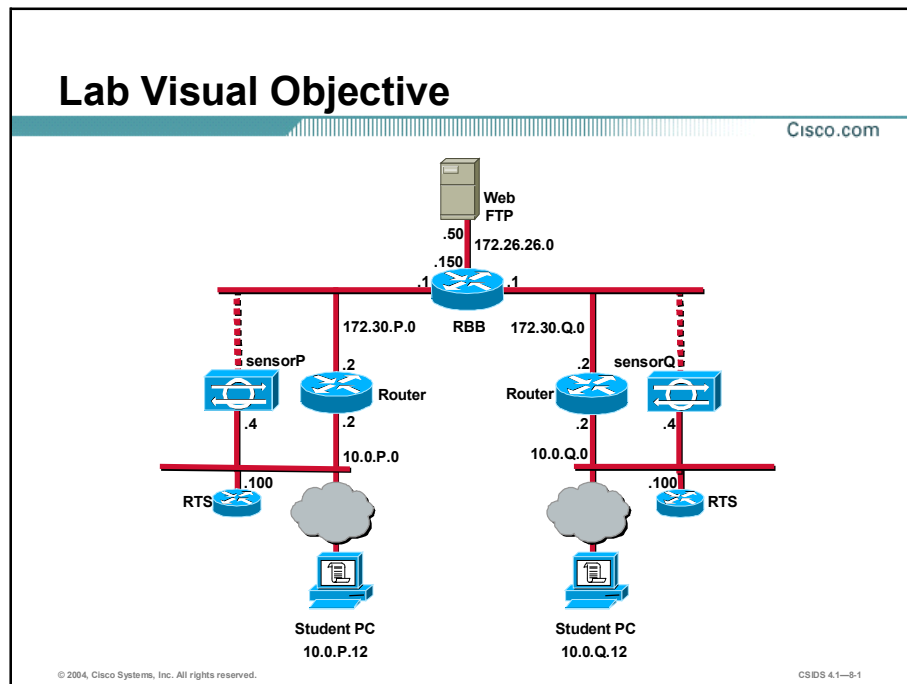
Objective

In this lab exercise you will complete the following tasks:

- Create a custom string match signature.
- Configure Alarm Channel system variables.
- Configure Alarm Channel event filtering.
- Configure IP logging for a specific IP address.
- Download and view IP logs.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



Task 1—Create a Custom String Match Signature

Complete the following steps to create a string match signature:

- Step 1** Log in to IDM as user **admin**. The password for the admin account is **adminpass**.

- Step 2** Choose **Configuration > Sensing Engine > Signature Configuration Mode**. The Signature Configuration Mode page is displayed.
- Step 3** Click **Engines**. The Engines list is displayed.
- Step 4** Click **STRING.TCP**. The STRING.TCP panel is displayed.
- Step 5** Click **Add**. The Adding STRING.TCP panel is displayed.
- Step 6** Enter **20002** in the SIGID field.
- Step 7** Enter **0** in the SubSig field.
- Step 8** Choose **high** from the AlarmSeverity drop-down menu.
- Step 9** Select **FireAll** from the AlarmThrottle drop-down menu.
- Step 10** Verify that **ToService** is selected in the Direction drop-down menu.
- Step 11** Verify that **True** is selected in the Enabled drop-down menu.
- Step 12** Select **Log** and **Reset** from the EventAction menu.

Note Press and hold down the Shift key after selecting Log so that you can select Log and Reset simultaneously.

- Step 13** Enter the string pattern to detect resetP, **[rR][eE][sS][eE][tT]P**, in the RegexString field.
(where P = pod number)
- Step 14** Enter **23** in the ServicePorts field.
- Step 15** Enter **resetPStringTCP** in the SigName field.
(where P = pod number)
- Step 16** Enter **Telnet reset** in the SigStringInfo field.
- Step 17** Click **OK**. The following message is displayed:
Signature has been added. To commit the changes please click the save changes icon in the Activity bar.
- Step 18** Click **OK**. The STRING.TCP list refreshes.
- Step 19** Select **16[5393-20002]** from the Page popup menu. The STRING.TCP list displays your custom string match signature.

Note The Page popup menu could vary depending on the signature version you are using.

- Step 20** Click the save changes icon in the Activity bar to save your configuration.

Task 2—Configure Alarm Channel System Variables

Complete the following steps to configure Alarm Channel system variables:

- Step 1** Select **Configuration > Sensing Engine > Alarm Channel Configuration > System Variables**. The System Variables page appears.
- Step 2** Select the check box to the left of the system variable IN.
- Step 3** Click **Edit**. The Editing panel appears.
- Step 4** Enter **10.0.P.0/24** in the IN field.
(where P = pod number)
- Step 5** Click **OK**. The following message appears:
SystemVariable has been updated. To commit the changes please click the save changes icon in the Activity bar.
- Step 6** Click **OK**.
- Step 7** Click the save changes icon in the Activity bar. The following message is displayed:
Configuration update in progress. This page will be unavailable for a few minutes.
- Step 8** After approximately 5 minutes, click **Alarm Channel Configuration > System Variables** again to see the edited variable in the list. The new value appears in the Value column.

Task 3—Configure Alarm Channel Event Filtering

Complete the following steps to use the IN variable to build an event filter:

- Step 1** Select **Start > Programs > Cisco Systems > Cisco IDS Event Viewer > Cisco IDS Event Viewer** to launch IEV.
- Step 2** Double-click **Source Address Group**. The Source Address Group tab is displayed in the right-hand pane.
- Step 3** Right-click the **Source Address Group** tab and select the **Delete All Rows from Database** option to clear IEV of any existing alerts. The Confirmation window opens.
- Step 4** Click **Yes**.
- Step 5** Open a Windows command prompt and issue the command **ping 10.0.S.12** to trigger an alert. Also, have your secondary peer ping your student PC.
(where S = secondary peer pod number)
- Step 6** Trigger another alert and test your custom string match signature by completing the following substeps:
1. Telnet to IP address 172.26.26.150.
 2. Enter **resetP** at the password prompt.
(where P = pod number)
 3. The Telnet session should close because entering resetP triggers the string match signature.
(where P = pod number)
- Step 7** Click the refresh icon in the IEV toolbar. You should see one alert with a source address of 10.0.S.12 and one with a source address of 10.0.P.12.

(where S = secondary peer pod number and P = pod number)

Step 8 Return to IDM and select **Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters**. The Event Filters page is displayed.

Step 9 Click **Add**. The Adding panel is displayed.

Step 10 Enter **20002** in the Signature ID field.

Step 11 Enter **0** in the SubSignature ID field.

Step 12 Enter **\$IN** in the SrcAddrs field.

Step 13 Click **Apply to Sensor**. The following message is displayed:

`EventFilter has been added. To commit the changes please click the save changes icon in the Activity bar.`

Step 14 Click **OK**. The Event Filters page refreshes, displaying your filter.

Step 15 Click the save changes icon in the Activity bar. The following message is displayed:

`Configuration information is not available at this time. Try again in a few minutes.`

Step 16 Return to IEV, right-click the **Source Address Group** tab, and select the **Delete All Rows from Database** option to clear IEV of any existing alerts. The Confirmation window opens.

Step 17 Click **Yes**.

Step 18 Open a Windows command prompt and issue the command **ping 10.0.S.12** to trigger an alert. Also, have your secondary peer ping your student PC:

(where S = secondary peer pod number)

Step 19 Attempt to trigger another alert by completing the following substeps:

1. Telnet to IP address 172.26.26.150.
2. Enter **resetP** at the password prompt. The Telnet session does not close.
(where P = pod number)

Step 20 Click **Refresh** in the IEV toolbar. You should see one high-severity alert with a source address of 10.0.S.12.

(where S = secondary peer pod number)

Task 4—Configure IP Logging for a Specific IP Address

Complete the following steps to configure the Sensor to log all IP traffic associated with your peer's student PC:

Step 1 Select **Administration > IP Logging**. The IP Logging page is displayed.

Step 2 Click **Add**. The Adding panel is displayed.

Step 3 Enter **10.0.Q.12**, the IP address of your peer's student PC, in the IP Address field.

(where Q = peer pod number)

Step 4 Enter **10** in the Duration field.

Step 5 Click **Apply to Sensor**. The IP Logging Configuration page displays the new log ID.

Task 5—Download and View IP Logs

Complete the following steps to test your IP logging configuration:

Step 1 Establish an SSH session to your Sensor.

Step 2 Clear all events from the EventStore:

```
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 3 When asked whether you want to continue with the clear, answer **yes**:

```
Continue with clear? : yes
```

```
sensor#
```

Step 4 Display all incoming events:

```
sensorP# show events
```

(where P = pod number)

Step 5 Minimize but do not close the SSH window.

Step 6 Generate an IP log by entering the following in your web browser to access your peer's student PC web page. Also, have your peer access your student PC web page:

```
http://10.0.Q.12
```

(where Q = peer pod number)

Step 7 After about 10 minutes, choose **Monitoring > IP Logs** in IDM. The IP Logs page is displayed.

Step 8 Click the hyperlink in the Log ID column. The File Downloaded window opens.

Step 9 Click **Open**. The Open With window opens.

Step 10 Click **Other**. The Open With . . . window opens.

Step 11 Browse to the `ethereal.exe` file on your student PC.

Step 12 Double-click `ethereal.exe`. The Open With window is displayed again with `Ethereal` selected.

Step 13 Click **OK**. The `Ethereal Network Analyzer` window opens and displays the packet data.

Step 14 Maximize the SSH window. Notice that no alerts were triggered by HTTP access to your peer's student PC.

Task 1—Configure Blocking Properties

Complete the following steps to set up global blocking properties for the NAC on the Blocking Properties page:

- Step 1** Login to the IDM with username **admin** and password **adminpass**.
- Step 2** Select **Configuration > Blocking > Blocking Properties**. The Blocking Properties page is displayed.
- Step 3** Verify that the **Enable Blocking** check box is selected.
- Step 4** Enter **10** in the Block Time field.
- Step 5** Click **Apply to Sensor** to save your 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 **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode**. The Signature Groups box is displayed.
- Step 2** Click **All Signatures**. The All Signatures list is displayed.
- Step 3** Select **4[1220-2007]** from the Page popup menu. The All Signatures list refreshes.

Note The Page popup menu could vary depending to the signature version you are using.

- Step 4** Select the check box to the left of the 2004 signature.
- Step 5** Click **Edit**. The Editing ATOMIC.ICMP page is displayed.
- Step 6** Select **shunHost** from the EventAction list.
- Step 7** Click **OK**. The following message is displayed:
Signature has been updated. To commit the changes please click the save changes icon in the Activity bar.
- Step 8** Click **OK**. The All Signatures list is displayed.
- Step 9** Click the save changes icon in the Activity bar.

Task 3—Configure Never-Block Addresses

Complete the following steps to configure addresses that should never be blocked:

- Step 1** Select **Configuration > Blocking > Never Block Addresses**. The Never Block Addresses page is displayed.
- Step 2** Click **Add**. The Adding panel 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 **Apply to Sensor** to save your changes.

Task 4—Configure a Logical Device

Complete the following steps to configure a logical device:

Step 1 Select **Configuration > Blocking > Logical Devices**. The Logical Devices page is displayed.

Step 2 Click **Add**. The Adding panel is displayed.

Step 3 Enter **Router** in the Name field.

Step 4 Enter the router's enable password, **cisco**, in the Enable Password field.

Step 5 Enter the router's SSH password, **cisco**, in the Password field.

Step 6 Enter **cisco** in the Username field.

Step 7 Click **Apply to Sensor** to save your changes.

Task 5—Configure a Blocking Device

Complete the following steps to configure a router as a blocking device:

Step 1 Select **Configuration > Blocking > Blocking Devices**. The Blocking Devices page is displayed.

Step 2 Click **Add**. The Adding panel is displayed.

Step 3 Enter **10.0.P.2** in the IP Address field.

(where P = pod number)

Step 4 Select **Router** from the Apply Logical Device drop-down menu.

Step 5 Verify that **Cisco Router** appears in the Device Type drop-down menu.

Step 6 Select **SSH 3DES** from the Communication field drop-down menu.

Step 7 Click **Apply to Sensor**.

Task 6—Specify the Router's Blocking Interface/Direction

Complete the following steps to specify the router interfaces to which ACLs will be applied:

Step 1 From the IDM main window, choose **Configuration > Blocking > Blocking Devices > Router Blocking Device Interfaces**. The Router Blocking Device Interfaces page is displayed.

Step 2 Click **Add**. The Adding panel is displayed.

Step 3 Verify that **10.0.P.2** is selected from the IP Address drop-down menu.

(where P = pod number)

Step 4 Enter **FastEthernet0/1** in the Blocking Interface field.

Step 5 Select **In** from the Blocking Direction drop-down menu.

Step 6 Click **Apply to Sensor** to save your changes.

Task 7—Add the Blocking Device to the Sensor’s Known Hosts List

Complete the following steps to add the router to the Sensor’s SSH known hosts list:

Step 1 Establish an SSH connection to your Sensor and log in to the CLI with the **admin** account. The password for the admin account is **adminpass**.

Step 2 Enter configure terminal mode:

```
sensor# configure terminal  
sensor(config)#
```

Step 3 Obtain the public key:

```
sensor(config)# ssh host-key 10.0.P.2  
Would you like to add this to the trusted certificate table for this  
host? [yes]:
```

(where P = pod number)

Step 4 Enter **yes** when prompted to confirm adding the public key to the known hosts list:

```
Would you like to add this to the trusted certificate table for this  
host? [yes]: yes
```

Step 5 Exit configuration terminal mode:

```
sensor(config)# exit  
sensor#
```

Step 6 Exit the CLI:

```
sensor# exit
```

Task 8—Test the Blocking Configuration

Complete the following steps to test the blocking configuration:

Step 1 From a Windows command prompt, telnet to your router at IP address 10.0.P.2.

```
C:\>telnet 10.0.P.2
```

(where P = pod number)

Step 2 Enter **cisco** at the Username prompt:

```
Username: cisco
```

Step 3 Enter **cisco** at the password prompt:

```
Password: cisco
```

```
rP>
```

(where P = pod number)

Step 4 Enter privileged mode:

```
rP> en
```

```
Password:
```

Step 5 Enter the password **cisco**:

```
Password: cisco
```

```
rP#
```

(where P = pod number)

Step 6 Execute the **show access-lists** command to verify that there are no access lists that would deny IP packets:

```
rP# show access-lists
```

(where P = pod number)

Step 7 From the student PC, ping your secondary peer pod router's outside interface as assigned by your instructor. Also, have your secondary peer ping your router's outside interface. The pings should be successful.

```
c:\> ping 172.30.S.2
```

(where S = secondary peer pod number)

Step 8 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
      10 permit ip host 10.0.P.4 any
      20 deny ip host 10.0.S.12 any (3 matches)
      30 permit ip any any
```

(where P = pod number and S = secondary peer pod number)

Step 9 From the student PC, attempt to establish a Telnet session to your secondary peer pod router's outside interface. The connection fails if your peer is actively blocking.

```
c:\>telnet 172.30.S.2
```

(where S = secondary peer pod number)

Step 10 Wait approximately ten minutes for the block to expire.

Step 11 Telnet to your secondary peer pod router's outside interface again. The connection should succeed.

Step 12 Return to your Telnet session with your router and execute the **show access-lists** command. Notice that the deny statement has been removed from the ACL:

```
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)

Task 9—Remove the Blocking Configuration

Complete the following steps to remove the blocking configuration:

Caution Wait until the blocking ACL is removed from the router before completing this task. Otherwise, you will need to manually remove the ACL from the router.

- Step 1** Select **Configuration > Blocking > Blocking Properties**. The Blocking Properties page is displayed.
- Step 2** De-select the **Enable Blocking** check box.
- Step 3** Click **Apply to Sensor**.

Lesson 12

Lab Exercise—Cisco IDS System Maintenance

Complete the following lab exercise to practice what you learned in this lesson.

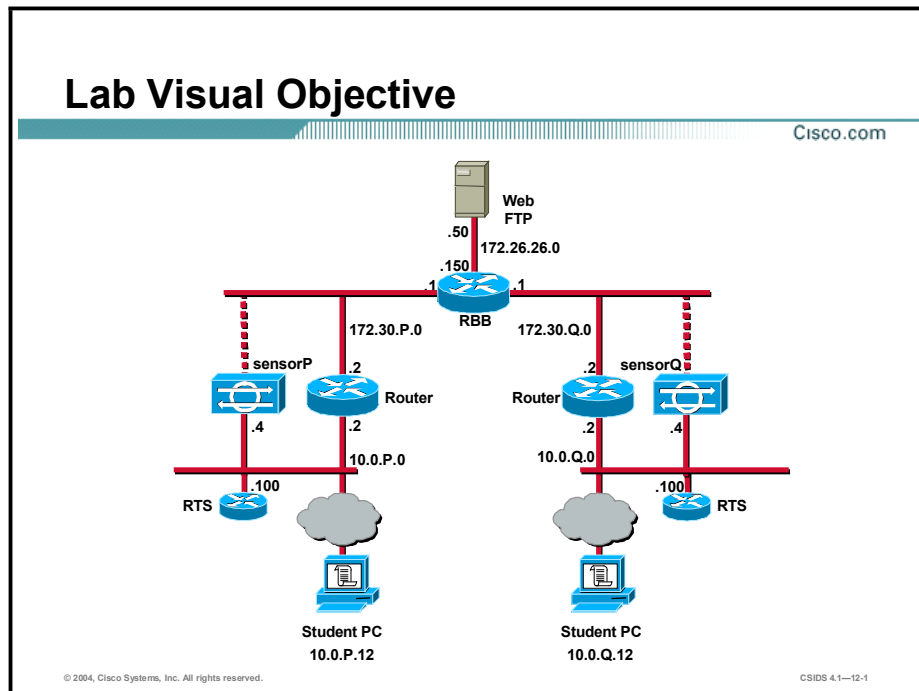
Objectives

In this lab exercise, you will complete the following tasks:

- Install an IDS Sensor signature update.
- Restore the Sensor's default configuration.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Task 1—Install an IDS Sensor Signature Update

Complete the following steps to update the IDS Sensor:

- Step 1** Log in to IDM with the username **admin** and the password **adminpass**.
- Step 2** Check your Sensor's current version by selecting **Administration > Support > System Information** and observing the System Information page.
- Step 3** Apply the signature update by completing the following substeps:
 1. Select **Administration > Update**. The Update page is displayed.
 2. In the URL field, enter the following:

```
ftp://administrator@10.0.P.12/IDS-sig-4.1-3-S64.rpm.pkg
```

(where P = pod number)

3. In the Password field, enter **attack**.
4. Click **Apply to Sensor**. The following message is displayed:

```
An update has been found and is being applied.
```

5. Click **OK**. The Update page is displayed.

- Step 4** Observe the status of the update in the task bar.
- Step 5** When the update is complete, log back in to IDM with the username **admin** and the password **adminpass**.
- Step 6** Check your Sensor's current version by selecting **Administration > Support > System Information** and observing the System Information page. Your Sensor version should now be 4.1(3)S64.
- Step 7** Log out of IDM.

Note The service pack installation may take up to 15 minutes. Please be patient.

Task 2—Restore the Sensor's Default Configuration

Complete the following tasks to restore the default settings to your Sensor.

- Step 1** Establish an SSH session to your Sensor.
- Step 2** Display your Sensor's current configuration:

```
sensorP# show configuration
! -----
service Authentication
general
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.Q.0 netmask 255.255.255.0
accessList ipAddress 10.0.P.12 netmask 255.255.255.255
```

```
exit
optionalAutoUpgrade
active-selection none
```

(where P = pod number)

- Step 3** Minimize, but do not close, your SSH session.
- Step 4** Log back in to IDM as user **admin**. The password for the admin account is **adminpass**.
- Step 5** Select **Configuration > Restore Defaults**. The Restore Defaults page is displayed.
- Step 6** Click **Apply to Sensor** to restore the default configuration.
- Step 7** Wait until the default configuration is restored.
- Step 8** Maximize your SSH session.
- Step 9** Display your Sensor's current configuration. Note that the IP address, netmask, default gateway, and allowed hosts have been reset to their default values.

```
sensorP# show configuration
! -----
service Authentication
general
methods method Local
exit
exit
exit
! -----
service Host
networkParams
ipAddress 10.1.9.201
netmask 255.255.255.0
defaultGateway 10.1.9.1
hostname sensor
telnetOption disabled
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
exit
optionalAutoUpgrade
active-selection none
exit
```

(where P = pod number)

Lesson 13

Lab Exercise—Enterprise Intrusion Detection System Management

Complete the following lab exercise to practice what you learned in this lesson.

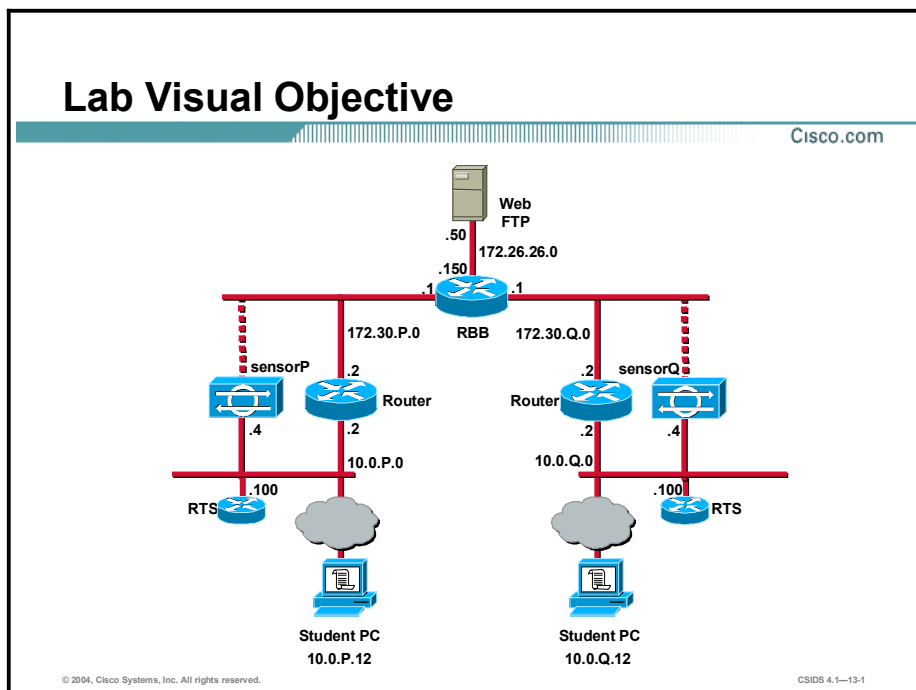
Objective

In this lab exercise you will complete the following tasks:

- Install the IDS MC.
- Launch the IDS MC.
- Update the IDS MC.
- Create a subgroup.
- Add a Sensor to the subgroup.
- Use the IDS MC to configure the Sensor.
- Deploy the IDS device configuration.
- Generate a configuration deployment report.
- Verify the configuration deployment.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.



Students have been assigned to pods in pairs. Each pod has a complete set of equipment to perform the lab exercise. Before beginning this lab exercise, prepare the Sensor as follows:

- Re-initialize the Sensor by using the **setup** command.
- Enable the sensing interface.
- Enable the 5114 signature.

Note The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number.

Task 1—Install the IDS MC

This task involves installing only the Intrusion Detection System (IDS) Management Center (MC) of the Sensors product on 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.
- Step 3** Reboot your student PC, and log back in.

Caution Do not proceed with this task until the IDS Event Viewer has been uninstalled from the student PC.

- Step 4** Go to **Start > Programs > CiscoWorks** to verify that CiscoWorks VPN/Security Management Solution (VMS) Common Services has been installed on the student PC. Notify your instructor if CiscoWorks Common Services is not installed.
- Step 5** Locate and double-click the IDS MC installation file icon as directed by your instructor. The following message is displayed:
Do you really want to install IDS MC & Security Monitor?
- Step 6** Click **Yes**. The Welcome window opens.
- Step 7** Click **Next** to begin the installation. The Software License Agreement panel is displayed.
- Step 8** Click **Yes** to accept the terms of the license agreement. The Setup Type window opens.
- Step 9** Select the **Custom installation** radio button and click **Next** to continue. The Select Components window opens.
- Step 10** Select the **IDS MC only** radio button and click **Next**. The System Requirements panel is displayed.
- Step 11** Click **Next** after verifying that your system meets the minimum disk space and memory requirements. The Summary window opens.
- Step 12** Click **Next** after verifying the selected settings. The Select Database Location window opens.
- Step 13** Click **Next** to accept the default database directory. The Select Database Password window opens.

- Step 14** Enter **cisco** in the Password and Confirm Password fields.
- Step 15** Click **Next**.
- Step 16** When the installation is complete and the Restart window opens, select **Yes, I want to restart my computer now**, and click **Finish**.
- Step 17** Reboot your student PC, and log back in.
- Step 18** Locate the Updates folder on your student PC desktop.
- Step 19** Double-click the IDS MC folder within the Updates folder.
- Step 20** Copy the following files to C:\Program Files\CSCOPx\MDC\etc\ids\updates.
- IDS-K9-min-4.1-1-S47.zip
 - IDS-K9-sp-4.1-2-S58.zip
 - IDS-K9-sp-4.1-3-S61.zip
 - IDS-sig-4.1-3-S64.zip

Task 2—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 by selecting **Start > Programs > CiscoWorks > CiscoWorks**.
- Step 2** Log in by entering the username and password of **admin** and **cisco**, respectively.
- 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 and prompts you to accept a digital certificate.
- Step 7** Click **Yes**. You are now logged in to the IDS MC.

Task 3—Update the IDS MC

Complete the following steps to update the IDS MC to the software version that is running on your Sensor:

Caution You will apply four different updates during this task. Be sure to wait several minutes between updates so that each update has time to complete.

- Step 1** Determine the Sensor software version and signature release level of your IDS MC server by completing the following substeps:
1. Select **Devices > Sensor**. The Sensor page is displayed.
 2. Click **Add**. The Select Sensor Group page is displayed.

3. Select the **Global** group, and then click **Next**. The Enter Sensor Information page is displayed.
4. Enter **10.0.P.4** in the IP Address field.
(where P = pod number)
5. Enter **sensorP** in the Sensor Name field.
(where P = pod number)
6. Enter **cisco** in the User ID field.
7. Enter **iattacku2** in the Password field.
8. Click **Next**. The Sensor Information page is displayed.
9. Click the arrow of the Version drop-down menu to display the Version list.
10. Scroll to the bottom of the list and make note of the latest version of software. This is the Sensor software and signature version that your IDS MC server is currently using.
11. Click **Cancel**.

Step 2 Select **Configuration > Updates > Update Network IDS Signatures**. The Update Network IDS Signatures page is displayed.

Step 3 Select **IDS-K9-min-4.1-1-S47.zip** from the Update File drop-down menu.

Step 4 Click **Apply**. The Update Summary page is displayed.

Step 5 Verify that the following message appears:

Apply the IDS-K9-min-4.1-1-S47.zip update to the Management Center.

Step 6 Click **Finish**. The Update Network IDS Signatures page is displayed.

Step 7 Select **IDS-K9-sp-4.1-2-S58.zip** from the Update File drop-down menu.

Step 8 Click **Apply**. The Update Summary page is displayed. Verify that the following message appears:

Apply the IDS-K9-sp-4.1-2-S58.zip update to the Management Center.

Step 9 Click **Finish**. The Update Network IDS Signatures page is displayed.

Step 10 Select **IDS-K9-sp-4.1-3-S61.zip** from the Update File drop-down menu.

Step 11 Click **Apply**. The Update Summary page is displayed. Verify that the following message appears:

Apply the IDS-K9-sp-4.1-3-S61.zip update to the Management Center.

Step 12 Click **Finish**. The Update Network IDS Signatures page is displayed.

Step 13 Select **IDS-sig-4.1-3-S64.zip** from the Update File drop-down menu.

Step 14 Click **Apply**. The Update Summary page is displayed. Verify that the following message appears:

Apply the IDS-sig-4.1-3-S64.zip update to the Management Center.

Step 15 Click **Finish**. The Update Network IDS Signatures page is displayed.

Task 4—Create a Subgroup

Complete the following steps to create a Sensor subgroup:

- Step 1** Choose **Devices > Sensor Group** from within the IDS MC. The Select Sensor Group page is displayed.
- Step 2** Select **Global** 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** Verify that the **Default (use parent values)** radio button is selected.
- Step 5** Click **OK**. The podP group appears within the Select Sensor Group page.
(where P = pod number)

Task 5—Add a Sensor to the Subgroup

Complete the following steps to import your Sensors to the IDS MC:

- Step 1** Choose **Devices > Sensor** from within the IDS MC. The Sensor page is displayed.
- Step 2** Select **podP** and click **Add**. The Select Sensor Group page is displayed.
(where P = pod number)
- Step 3** Select **podP**.
(where P = pod number)
- Step 4** Click **Next**. The Enter Sensor Information page is displayed.
- Step 5** Enter the Sensor information settings by completing the following substeps:
 1. Enter your Sensor's IP address, **10.0.P.4**, in the IP Address field.
(where P = pod number)
 2. Enter **sensorP** in the Sensor Name field.
(where P = pod number)
 3. Enter **cisco** in the User ID field.
 4. Enter **iattacku2** in the Password field.
- Step 6** Click **Next**. The Sensor Information page is displayed.
- Step 7** Select **4.1(3)S64** from the Version drop-down menu.
- Step 8** Click **Finish**. The Sensor, sensorP, is listed on the Sensor page within the podP subgroup.
(where P = pod number)

Task 6—Use the IDS MC to Configure the Sensor

Complete the following steps to configure a Sensor via the IDS MC.

- Step 1** Configure an allowed host by completing the following substeps:
1. Choose **Configuration > Settings**. The Settings page is displayed.
 2. Use the Object Selector to select **sensorP**. SensorP is displayed in the Object bar. (where P = pod number)
 3. Choose **Allowed Hosts** from the TOC. The Allowed Hosts page is displayed.
 4. Click **Add**. The Enter Allowed Host page is displayed.
 5. Enter **10.0.P.0** in the IP Address field. (where P = pod number)
 6. Enter **255.255.255.0** in the Net Mask field.
 7. Click **OK**. Your pod network is displayed in the Allowed Hosts page.
- Step 2** Enable and set the severity level of a signature:
1. Choose **Signatures** from the TOC. The Signatures page is displayed.
 2. Click **General**. The Signature(s) in Group page is displayed.
 3. Enter **3001** in the field to the left of the Filter button.
 4. Click **Filter**. The 3001 signature is displayed in the Signature(s) in Group page.
 5. Notice that the signature is not enabled and that its severity level is medium.
 6. Select the check box to the left of the 3001 signature.
 7. Click **Edit**. The Edit Signature(s) page is displayed.
 8. Select the **Enable** check box.
 9. Select **High** from the Severity drop-down menu.
 10. Click **OK**. The Signature(s) in Group page is displayed with the new settings for the 3001 signature in the Enabled and Severity columns.

Task 7—Deploy the IDS Device Configuration

Complete the following steps to deploy the configuration to your Sensor:

- Step 1** Choose **Configuration > Pending**. The Pending page is displayed.
- Step 2** Select the check box to the left of the pending configuration.
- Step 3** Click **Save**. The Pending page refreshes.
- Step 4** Choose **Deployment > Generate**. The Generate page is displayed.
- Step 5** Select the **SensorP** check box.
(where P = pod number)
- Step 6** Click **Generate**. The Generate Status window opens, displaying the Sensor name and the date and time the configuration was generated.
- Step 7** Choose **Deployment > Deploy > Submit**. The Submit page is displayed.

- Step 8** Select the **SensorP** check box.
(where P = pod number)
- Step 9** Click **Deploy**. The Select Configurations page is displayed.
- Step 10** Select the check box to the left of the configuration file name.
- Step 11** Click **Next**. The Enter Job Properties page is displayed.
- Step 12** Enter **SensorPDeployment** in the Job Name field and verify that the **Immediate** radio button is selected.
(where P = pod number)
- Step 13** Click **Finish**. The Submit page is displayed.

Task 8—Generate a Configuration Deployment Report

Complete the following steps to generate a configuration deployment report:

- Step 1** Choose **Reports > Generate**. The Select Report page is displayed.
- Step 2** Select the **Audit Log Report** radio button.
- Step 3** Click **Select**. The Report Filtering page is displayed.
- Step 4** Verify that the **Since the dawn of time** radio button is selected in the Date/Time panel.
- Step 5** Choose **Select All** from the Event Severity panel.
- Step 6** Choose **Select All** from the Applications panel.
- Step 7** Choose **Select All** from the Subsystem panel.
- Step 8** Choose **Select All** from the Task Type panel.
- Step 9** Click **Next**. The Schedule Report page is displayed.
- Step 10** Enter **AuditLogReport1** in the Report Title field.
- Step 11** Verify that the **Run Now** radio button is selected.
- Step 12** Click **Finish**. The following message is displayed:
Your report will be listed here when it is ready
- Step 13** Click **OK**. The Choose Completed Report page is displayed.
- Step 14** Click **View** to refresh the page.
- Step 15** Select the check box to the left of the **AuditLogReport1**.
- Step 16** Click **Open in Window**. The report is displayed in a new window.
- Step 17** Verify that the deployment is complete.

Task 9—Verify the Configuration Deployment

Complete the following steps to verify that the configuration deployed correctly and the signature settings you configured via the IDS MC have been accepted by the Sensor:

Step 1 Establish an SSH connection to your Sensor.

Step 2 Log in to the Sensor with the username **cisco** and password **iattacku2**.

Step 3 Enter configuration mode:

```
sensorP# config t  
sensorP(config)#  
(where P = pod number)
```

Step 4 Enter virtual sensor configuration mode:

```
sensorP(config)# service virtual-sensor-configuration virtualSensor  
sensorP(config-vsc)#  
(where P = pod number)
```

Step 5 Enter micro-engine tuning mode:

```
sensorP(config-vsc)# tune-micro-engines  
sensorP(config-vsc-virtualSensor)#  
(where P = pod number)
```

Step 6 Enter configuration mode for the sweep.port.tcp engine:

```
sensorP(config-vsc-virtualSensor)#sweep.port.tcp  
sensorP(config-vsc-virtualSensor-SWE)#  
(where P = pod number)
```

Step 7 Access signature 3001:

```
sensorP(config-vsc-virtualSensor-SWE)# signatures SIGID 3001  
sensorP(config-vsc-virtualSensor-SWE-sig)#  
(where P = pod number)
```

Step 8 View the settings for signature 3001:

```
sensorP(config-vsc-virtualSensor-SWE-sig)# show settings  
  SIGID: 3001 <protected>  
  SubSig: 0 <protected>  
  AlarmDelayTimer: 10 <protected>  
  AlarmInterval:  
  AlarmSeverity: high default: medium  
  AlarmThrottle: FireAll <defaulted>  
  AlarmTraits:  
  CapturePacket: False <defaulted>  
  ChokeThreshold: 200 <defaulted>  
  Enabled: True default: False  
  EventAction: ZERO  
  FlipAddr: True <defaulted>  
  InvertedSweep: True <defaulted>
```

```
Mask: RST|SYN|FIN <protected>
MaxInspectLength:
MaxTTL:
MinHits:
PortRange: 1 <defaulted>
Protocol: TCP <defaulted>
ResetAfterIdle: 20 <defaulted>
SigComment: TCP Port Sweep
SigName: TCP Port Sweep <protected>
SigStringInfo:
SigVersion: 2.1.1 <defaulted>
StorageKey: DOUBLE <defaulted>
SummaryKey: Axxx <defaulted>
SupressReverse: True <defaulted>
TcpFlags: RST <protected>
ThrottleInterval: 30 <defaulted>
Unique: 5 <defaulted>
WantFrag: False <defaulted>
```

(where P = pod number)

Step 9 Exit configuration mode for the 3001 signature:

```
sensorP(config-vsc-virtualSensor-SWE-sig) # exit
sensorP(config-vsc-virtualSensor-SWE) #
```

(where P = pod number)

Step 10 Exit configuration mode for the sweep.port.tcp engine:

```
sensorP(config-vsc-virtualSensor-SWE) # exit
sensorP(config-vsc-virtualSensor) #
```

(where P = pod number)

Step 11 Exit tune-micro-engines mode:

```
sensorP(config-vsc-virtualSensor) # exit
sensorP(config-vsc) #
```

(where P = pod number)

Step 12 Exit virtual-sensor-configuration mode:

```
sensorP(config-vsc) # end
sensorP#
```

(where P = pod number)

Step 13 Exit privileged mode:

```
sensorP# exit
```

(where P = pod number)

Lesson 14

Lab Exercise—Enterprise IDS Monitoring and Reporting

Complete the following lab exercise to practice what you learned in this lesson.

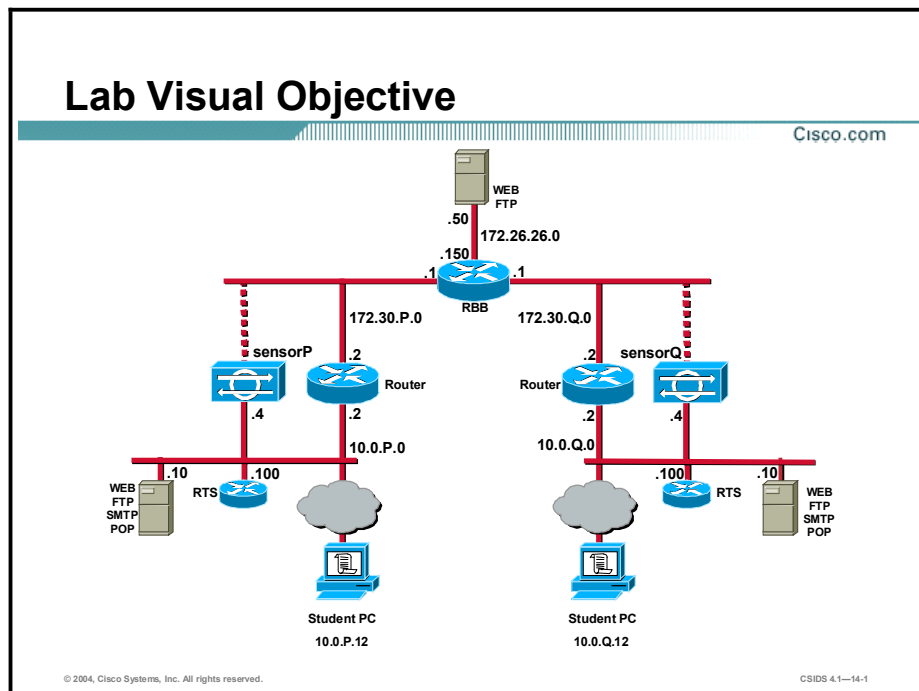
Objective

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.
- Generate an IDS Alarm Source Report.

Visual Objective

The following figure displays the lab topology you will use to complete this lab exercise.



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 following message is displayed:
Do you really want to install IDS MC & Security Monitor?
- Step 5** Click **Yes**. The Welcome panel is displayed.
- Step 6** Click **Next** to begin the installation. The Software License Agreement panel is displayed.
- Step 7** Click **Yes** to accept the terms of the license agreement. The Setup Type window opens.
- Step 8** Select **Custom installation** to install the Security Monitor and click **Next**. The Select Components panel is displayed.
- Step 9** Select the **Security Monitor only** radio button and click **Next**. The System Requirements panel is displayed.
- Step 10** Verify that your system meets the minimum disk space and memory requirements. Click **Next**. The Summary panel is displayed.
- Step 11** Verify the selected components, and click **Next**. The Select CiscoWorks Syslog Port panel is displayed.
- Step 12** Click **Next** to accept the default port. The Configure Communication Properties panel is displayed.
- Step 13** Click **Next**. The Setup Complete panel is displayed after the Security Monitor installation process finishes.
- Step 14** Click **Finish**. The Install Wizard exits.
- Step 15** Restart your student PC.

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** Log back in to your student PC.
- Step 2** Launch your web browser and specify the IP address of the CiscoWorks server as the location:
`http://10.0.P.12:1741`
(where P = pod number)
- Step 3** Log in to CiscoWorks as the default user **admin**. The password is **cisco**.
- Step 4** Click **Connect**. You are now logged in to the CiscoWorks desktop.
- Step 5** Select the **VPN/Security Management Solution** drawer in the left panel.
- Step 6** Select the **Monitoring Center** folder located in the VPN/Security Management Solution drawer.
- Step 7** Select the **Security Monitor** icon to launch the Security Monitor. The Security Alert window opens and prompts you to accept a digital certificate.
- Step 8** Click **Yes**. You are now logged in to the Security Monitor.

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 MC 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 **cisco** 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 an alarm that can be viewed in the Security Monitor Event Viewer. Complete the following steps to view an IDS alarm in the Security Monitor Event Viewer:

- Step 1** Open a web browser and enter the following URL to trigger the WWW IIS Unicode Attack signature on your peer's Sensor. Also, have your peer trigger the WWW IIS Unicode Attack on your Sensor:

```
http://10.0.Q.12/scripts/..%c0%af../winnt/system32
```

(where Q = peer pod number)

- Step 2** Choose **Monitor > Events**. The Events page is displayed.
- Step 3** Accept the default values and click Launch Event Viewer. The Event Viewer is displayed.
- Double-click within the cell beneath the Count column heading. The alarms you generated are displayed.

Task 5—Generate an IDS Alarm Source Report

Complete the following steps to create and view an IDS Alarm Source Report:

- Step 1** Choose **Reports > Generate Report**. The Select Report page is displayed.
- Step 2** Select **IDS Alarm Source Report** from the Available Reports list.
- Step 3** Click **Select**. The Report Filtering page is displayed.
- Step 4** Select **Select All** from the Event Level panel.
- Step 5** Select **Last** from the Time/Date panel and specify 2 days.
- Step 6** Verify that the **Any** radio button is selected in the Event Count panel.
- Step 7** Verify that **Any** is selected from the Source Direction drop-down menu.
- Step 8** Verify that the **Any** radio button is selected from the Source IP Address panel.
- Step 9** Verify that **Any** is selected from the Destination Direction drop-down menu.
- Step 10** Verify that the **Any** radio button is selected from the Destination IP Address panel.
- Step 11** Select **Select All** from the IDS Devices panel.
- Step 12** Verify that the **Any signature** check box is selected in the IDS Signatures panel.
- Step 13** Click **Next**. The Schedule Report page is displayed.
- Step 14** Enter **PodP Alarm Source Report** in the Report Title field.
- (where P = pod number)
- Step 15** Verify that the **Run Now** radio button is selected.

Step 16 Click **Finish** to submit the report. The following message is displayed:

Your report will be listed here when it is ready.

Step 17 Click **OK**. The Choose Completed Report page is displayed.

Step 18 Click **View** to refresh the page. The Choose Completed Report page is refreshed.

Step 19 Select the **PodP Alarm Source Report** and click **View**. The PodP Alarm Source Report is displayed.

(where P = pod number)

Lesson 15

Lab Exercise—(Optional.) Initializing the NM-CIDS

Complete the following lab exercise to practice what you learned in this lesson.

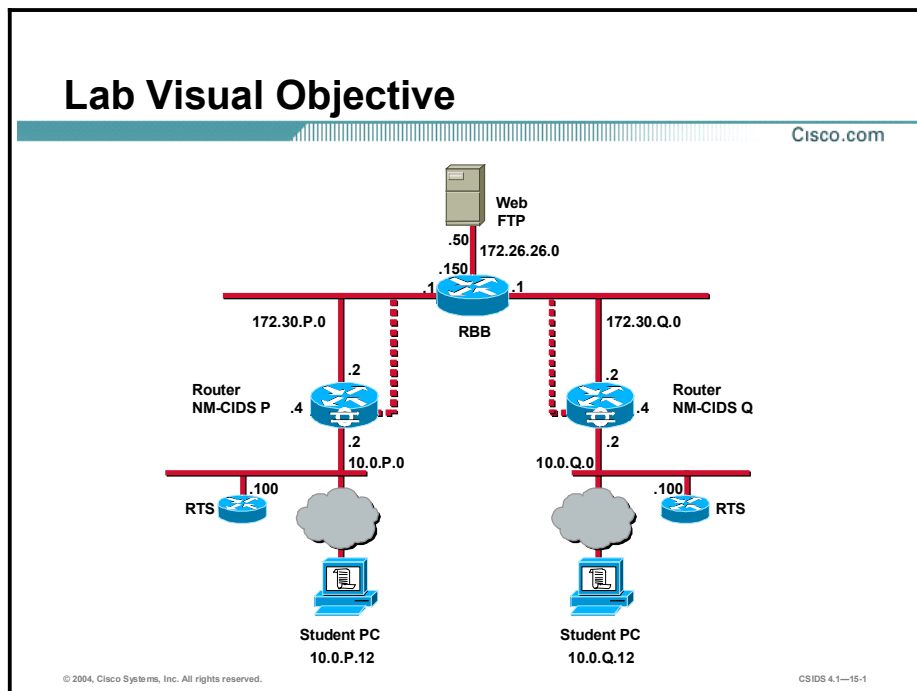
Objectives

In this lab exercise you will complete the following tasks:

- Set up the NM-CIDS interfaces.
- Configure packet capture for the NM-CIDS.
- Initialize the NM-CIDS.
- Verify NM-CIDS functionality.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.



Task 1—Set Up the NM-CIDS Interfaces

Complete the following steps to set up the NM-CIDS interfaces:

Step 1 Confirm the NM-CIDS slot number in your router:

```
rP # show run
Building configuration...
```

```
Current configuration : 1275 bytes
!
version 12.2
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RP
!
logging queue-limit 100
enable secret 5 $1$rV79$UW2YXaBUIMysvRwaLad4u/
!
memory-size iomem 10
ip subnet-zero
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
interface FastEthernet0/0
 ip address 10.0.P.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.30.P.2 255.255.255.0
 duplex auto
 speed auto
!
interface IDS-Sensor1/0
 no ip address
 shutdown
 hold-queue 60 out
!
router eigrp 1
```

```

network 10.0.0.0
network 172.30.0.0
no auto-summary
no eigrp log-neighbor-changes
!
no ip http server
no ip http secure-server
ip classless
ip route 10.0.P.0 255.255.255.0 10.0.P.102
ip route 10.0.Q.0 255.255.255.0 172.30.P.1
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
  password cisco
line 33
  flush-at-activation
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad v120 telnet rlogin udptn ssh
line aux 0
line vty 0 4
  password cisco
  login
!
end

```

(where P = pod number)

Step 2 Verify that Cisco IOS-IDS is not running. There should be no output because the IOS-IDS is not running:

```
rP# show ip interface
```

(where P = pod number)

Step 3 Enter configuration mode:

```
rP# configuration terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
rP(config)#
```

(where P = pod number)

Step 4 Enable the CEF switching path. There should be no output:

```
rP(config)# ip cef
```

(where P = pod number)

Step 5 Create a loopback interface:

```
rP(config)# interface loopback 0
```

```
rP(config-if)#
```

(where P = pod number)

Step 6 Assign an IP address and netmask to the loopback interface:

```
rP(config-if)# ip address 1.2.3.4 255.255.255.255
```

```
rP(config-if)#
```

(where P = pod number)

Step 7 Exit the configuration mode for the loopback interface:

```
rP(config-if)#exit
```

```
rP(config)#
```

(where P = pod number)

Step 8 Enter configuration mode for the module:

```
rP(config)# interface ids-sensor 1/0
```

```
rP(config-if)#
```

(where P = pod number)

Step 9 Assign an unnumbered loopback interface to the ids-sensor interface:

```
rP(config-if)# ip unnumbered loopback 0
```

```
rP(config-if)#
```

(where P = pod number)

Step 10 Activate the port:

```
rP(config-if)# no shutdown
```

```
rP(config-if)#
```

(where P = pod number)

Step 11 Exit configuration mode:

```
rP(config-if)# end
```

```
rP#
```

(where P = pod number)

Step 12 Write the configuration to NVRAM:

```
rP# write mem
Building configuration
[OK]
```

(where P = pod number)

Task 2—Configure Packet Capture for the NM-CIDS

Complete the following steps to set up packet capture on the NM-CIDS:

Step 1 View your interface configuration:

```
rP# show run
Building configuration...

Current configuration : 1375 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RP
!
logging queue-limit 100
enable secret 5 $1$rV79$UW2YXaBUIMysvRwaLad4u/
!
memory-size iomem 10
ip subnet-zero
ip cef
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 1.2.3.4 255.255.255.255
!
interface FastEthernet0/0
```

```
ip address 10.0.P.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 172.30.P.2 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
ip unnumbered Loopback0
hold-queue 60 out
!
router eigrp 1
network 10.0.0.0
network 172.30.0.0
no auto-summary
no eigrp log-neighbor-changes
!
no ip http server
no ip http secure-server
ip classless
ip route 10.0.P.0 255.255.255.0 10.0.P.102
ip route 10.0.P.0 255.255.255.0 172.30.P.1
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
password cisco
line 33
flush-at-activation
no activation-character
no exec
transport preferred none
transport input all
transport output pad v120 telnet rlogin udptn ssh
line aux 0
line vty 0 4
```



```
password cisco
login
!
end
```

(where P = pod number)

Step 2 Enter configuration mode:

```
rP# configure terminal
rP(config)#
```

(where P = pod number)

Step 3 Select the interface:

```
rP(config)# interface FastEthernet0/0
rP(config-if)#
```

(where P = pod number)

Step 4 Configure the interface to copy network traffic to the NM-CIDS:

```
rP(config-if)# ids-service-module monitoring
rP(config-if)#
```

(where P = pod number)

Step 5 Exit interface mode:

```
rP(config-if)# exit
rP(config)#
```

(where P = pod number)

Step 6 Exit configuration mode:

```
rP(config)# exit
rP#
```

(where P = pod number)

Step 7 Check the status of the Cisco IDS software running on the router:

```
rP# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait..
Starting IDS application
```

(where P = pod number)

Task 3—Initialize the NM-CIDS

Complete the following steps to initialize the NM-CIDS:

Step 1 Establish a session with the NM-CIDS:

```
rP# service-module ids-sensor 1/0 session
```

```
Trying 1.2.3.4, 2033 ... Open
```

```
sensor login:
```

(where P = pod number)

Step 2 Log in to the NM-CIDS with the default username **cisco** and the password **cisco**:

```
sensor login: cisco
```

```
Password: cisco
```

```
***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.
```

```
sensor#
```

Step 3 Initialize the NM-CIDS:

```
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:
```

```
networkParams
```

```
ipAddress 10.1.9.201
```

```
netmask 255.255.255.0
```

```
defaultGateway 10.1.9.1
```

```
hostname sensor
```

```
telnetOption disabled
```

```
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
```

```
exit
```

```
timeParams
```

```
summerTimeParams
```

```
active-selection none
```

```
exit
exit
service webServer
general
ports 443
exit
exit
```

Current time: Mon Mar 1 00:44:23 1993

Setup Configuration last modified: Mon Jun 30 21:54:24 2003

Continue with configuration dialog?[yes]:

Step 4 Continue with initial configuration of the NM-CIDS by pressing **Enter**:

Continue with configuration dialog?[yes]: **<Enter>**

Step 5 Enter a host name for the NM-CIDS:

Enter host name[sensor]: **nmsensorP**

(where P = pod number)

Step 6 Enter the IP address for the command and control interface:

Enter IP address[10.1.9.201]: **10.0.P.5**

(where P = pod number)

Step 7 Accept the default netmask:

Enter netmask[255.255.255.0]: **<Enter>**

Step 8 Enter the default gateway for the NM-CIDS:

Enter default gateway[10.1.9.1]: **10.0.P.2**

(where P = pod number)

Step 9 Accept the default Telnet server status:

Enter telnet-server status[disabled]: **<Enter>**

Step 10 Accept the default web server port:

Enter web-server port[443]: **<Enter>**

Step 11 Enter yes to begin modifying the access list:

Modify current access list?[no]: **yes**

Current access list entries:

[1] 10.0.0.0 255.0.0.0

Delete:

Step 12 Remove the default access list entry:

Delete: **1**

Delete:

Step 13 Press **Enter** again to obtain the Permit prompt:

Delete: **<Enter>**

Permit:

Step 14 Configure the access list to allow the student PC to access the NM-CIDS:

Permit: **10.0.P.12**

Permit:

Step 15 Press **Enter** again to exit the access list configuration prompts:

Permit: **<enter>**

Modify system clock settings? [no]:

Step 16 Accept the default clock settings on the NM-CIDS that are to synchronize with the Cisco IOS clock:

Modify system clock settings? [no]: **<Enter>**

Step 17 Review the settings entered:

The following configuration was entered.

```
networkParams
ipAddress 10.0.P.5
defaultGateway 10.0.P.2
hostname nmsensorP
accessList ipAddress 10.0.P.12 netmask 255.255.255.255
exit
timeParams
summerTimeParams
active-selection none
exit
exit
service webServer
general
ports 443
exit
exit
```

[0] Go to the command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration and exit setup.

Enter your selection [2]:

(where P = pod number)

Step 18 Enter **2** to save your configuration:

Enter your selection[2]: 2

Configuration Saved.

*11:00:00 UTC Mon Nov 11 2003

Step 19 Accept the default system date and time:

Modify system date and time?[no]: <Enter>

sensor#

Step 20 Verify that the Sensor time and date are synchronized with the Cisco IOS time and date by completing the following substeps:

1. Check the Sensor's time:

sensor# **show clock**

*15:03:06 UTC Thurs April 1 2004

sensor#

2. Return to the router's privileged-EXEC mode by pressing **Ctrl-Shift-6**, then x.

3. Check the router's time:

rP# **show clock**

15:03:22.977 UTC Thurs April 1 2004

(where P = pod number)

Step 21 Reboot the NM-CIDS:

sensor# **reset**

Step 22 Log in to the NM-CIDS and change the default password:

nmsensorP login: **cisco**

Password: **cisco**

You are required to change your password immediately (password aged)

Changing password for cisco

(current) UNIX password: **cisco**

New password: **!attacku2**

Retype new password: **!attacku2**

Last login: Mon Mar 1 00:43:34 on ttyS0

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.

```
nmsensorP#
```

(where P = pod number)

Step 23 Enable the sensing interface on the NM-CIDS by completing the following substeps:

1. Enter global configuration mode:

```
nmsensorP# config t
```

```
nmsensorP(config)#
```

(where P = pod number)

2. Enter configuration mode for sensing interface int1:

```
nmsensorP(config)# interface sensing int1
```

```
nmsensorP(config-ifs)#
```

(where P = pod number)

3. Enable the interface:

```
nmsensorP(config-ifs)# no shutdown
```

(where P = pod number)

Step 24 Verify that the NM-CIDS is receiving network traffic from the router by completing the following substeps:

1. Display the interface group:

```
nmsensorP# show interface group 0
```

```
Group 0 is up
```

```
  Sensing ports int1
```

```
  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 = 337615447
```

```
  Measure of the level of resource utilization = 0
```

```
  Total number of packets processed since reset = 10049
```

```
  Total number of IP packets processed since reset = 8449
```

```
Total number of packets that were not IP processed since reset = 1600
```

```
  Total number of TCP packets processed since reset = 4722
```

```
  Total number of UDP packets processed since reset = 2411
```

```
  Total number of ICMP packets processed since reset = 1316
```

```
Total number of packets that were not TCP, UDP, or ICMP processed  
since reset = 0
```

```
  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 = 904783

 The rate of packets per second since reset = 0

 The rate of bytes per second since reset = 0

 The average bytes per packet since reset = 90

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 = 1

 TCP streams currently in the closing state = 0

 TCP streams currently in the system = 1

 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 = 3

 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 = 21

 TCP nodes keyed on both IP addresses and both ports = 1

 UDP nodes keyed on both IP addresses and both ports = 2

 IP nodes keyed on both IP addresses = 4

 The number of each type of node inserted since reset

 Total nodes inserted = 768

 TCP nodes keyed on both IP addresses and both ports = 3

 UDP nodes keyed on both IP addresses and both ports = 570

 IP nodes keyed on both IP addresses = 61

 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
```

```
nmsensorP#
```

(where P = pod number)

2. Display the interface group again. Notice that the counters increase. This indicates that the NM-CIDS is receiving network traffic.

```
nmsensorP# show interface group 0
```

```
Group 0 is up
```

```
Sensing ports int1
```

```
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 = 337615447
```

```
Measure of the level of resource utilization = 0
```

```
Total number of packets processed since reset = 11050
```

```
Total number of IP packets processed since reset = 9962
```

```
Total number of packets that were not IP processed since reset = 1800
```

```
Total number of TCP packets processed since reset = 5798
```

```
Total number of UDP packets processed since reset = 3642
```

```
Total number of ICMP packets processed since reset = 1972
```

```
Total number of packets that were not TCP, UDP, or ICMP processed since reset = 0
```

```
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 = 100798
```


The rate of packets per second since reset = 0
 The rate of bytes per second since reset = 0
 The average bytes per packet since reset = 90
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 = 1
 TCP streams currently in the closing state = 0
 TCP streams currently in the system = 1
 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 = 3
 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 = 21
 TCP nodes keyed on both IP addresses and both ports = 1
 UDP nodes keyed on both IP addresses and both ports = 2
 IP nodes keyed on both IP addresses = 4
The number of each type of node inserted since reset
 Total nodes inserted = 768
 TCP nodes keyed on both IP addresses and both ports = 3
 UDP nodes keyed on both IP addresses and both ports = 570
 IP nodes keyed on both IP addresses = 61
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

nmsensorP#

(where P = pod number)

Task 4—Verify NM-CIDS Functionality

Complete the following steps to test the NM-CIDS:

- Step 1** Generate IDS events by entering the following URL in your browser to trigger the WWW WinNT cmd.exe signature on your peer Sensor. Also, have your peer trigger the signature on your Sensor in the same way:

http://10.0.Q.12/scripts/..%35c../winnt/system32/cmd.exe?/c+dir

(where Q = peer pod number)

- Step 2** Return to the Sensor CLI and display alert events that have been triggered by your peer since you began this lab exercise:

Note The time and date you enter in the following command should be today's date and the approximate time you began this lab exercise. The time and date shown in the command below are simply examples.

```
nmsensorP# show events alert 10:00 april 1 2004
evAlert: eventId=315554494769324177 severity=medium
originator:
  hostId: nmsensorP
  appName: sensorApp
  appInstanceId: 820
time: 2003/11/11 14:15:29 2003/11/11 14:15:29 UTC
interfaceGroup: 0
vlan: 0
signature: sigId=5081 sigName=WWW WinNT cmd.exe access subSigId=0
version=S37 /system32/cmd.exe
context:
  fromAttacker:
000000 47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25 GET
/scripts/..%
000010 33 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74
35c../winnt/syst
```

```
000020 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B
em32/cmd.exe?/c+
000030 64 69 72 20 48 54 54 50 2F 31 2E 31 0D          dir
HTTP/1.1.
```

participants:

attack:

attacker: proxy=false

addr: locality=OUT 10.0.Q.12

port: 1878

victim:

addr: locality=OUT 10.0.P.12

port: 80

alertDetails: Traffic Source: int1 ; SlotNum 0 SubSlotNum 0 PortNum
1 SubIntNum 0 IntType 18 VlanId 0 ;

(where P = pod number)

