

Implementing Secure Converged Wide Area Networks

Volume 2

Version 1.0

Student Guide

Editorial, Production, and Graphic Services: 07.21.06

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website 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



© 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

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 2

Cisco Device Hardening **5-1**

Overview	5-1
Module Objectives	5-1

Mitigating Network Attacks **5-3**

Overview	5-3
Objectives	5-3
Cisco Self-Defending Network	5-4
Evolution of Cisco Self-Defending Network	5-5
Types of Network Attacks	5-7
Reconnaissance Attacks and Mitigation	5-9
Packet Sniffers	5-10
Packet Sniffer Mitigation	5-11
Port Scans and Ping Sweeps	5-13
Port Scan and Ping Sweep Mitigation	5-14
Internet Information Queries	5-15
Access Attacks and Mitigation	5-16
Password Attacks	5-17
Password Attack Example	5-18
Password Attack Mitigation	5-19
Trust Exploitation	5-20
Trust Exploitation Attack Mitigation	5-21
Port Redirection	5-22
Man-in-the-Middle Attacks	5-23
DoS Attacks and Mitigation	5-24
Distributed DoS Attacks	5-25
Distributed DoS Example	5-26
DoS and Distributed DoS Attack Mitigation	5-27
IP Spoofing in DoS and DDoS	5-28
IP Spoofing Attack Mitigation	5-30
Worm, Virus, and Trojan Horse Attacks and Mitigation	5-32
Virus and Trojan Horse Attack Mitigation	5-33
The Anatomy of a Worm Attack	5-34
Mitigating Worm Attacks	5-35
Application Layer Attacks and Mitigation	5-36
Netcat	5-37
Netcat Example	5-38
Mitigation of Application Layer Attacks	5-39
Management Protocols and Vulnerabilities	5-40
Configuration Management Recommendations	5-41
Management Protocols	5-42
Management Protocol Best Practices	5-44
Determining Vulnerabilities and Threats	5-45
Blue's Port Scanner and Ethereal	5-47
Microsoft Baseline Security Analyzer	5-48
Summary	5-49

Disabling Unused Cisco Router Network Services and Interfaces **5-51**

Overview	5-51
Objectives	5-51
Vulnerable Router Services and Interfaces	5-52
Vulnerable Router Services	5-53
Router Hardening Considerations	5-56
Locking Down Routers with AutoSecure	5-57
AutoSecure Operation Modes	5-58
AutoSecure Functions	5-59
AutoSecure Failure Scenarios	5-60
AutoSecure Process Overview	5-61

Start and Interface Selection	5-63
Securing Management Plane Services	5-64
Creating Security Banner	5-66
Passwords and AAA	5-67
SSH and Interface-Specific Services	5-68
Forwarding Plane, Verification, and Deployment	5-69
Locking Down Routers with the SDM	5-73
SDM Security Audit Overview	5-74
SDM Security Audit: Main Window	5-75
SDM Security Audit Wizard	5-76
SDM Security Audit Interface Configuration	5-77
SDM Security Audit	5-78
SDM Security Audit: Fix the Security Problems	5-79
SDM Security Audit: Summary	5-80
SDM One-Step Lockdown: Main Window	5-81
SDM One-Step Lockdown Wizard	5-82
Summary	5-84
Securing Cisco Router Installations and Administrative Access	5-85
Overview	5-85
Objectives	5-85
Configuring Router Passwords	5-86
Password Creation Rules	5-87
Initial Configuration Dialog	5-88
Configure the Line-Level Password	5-90
Password Minimum Length Enforcement	5-93
Encrypting Passwords	5-94
Enhanced Username Password Security	5-95
Securing ROMMON	5-97
Setting a Login Failure Rate	5-99
Setting a Login Failure Blocking Period	5-100
Excluding Addresses from Login Blocking	5-102
Setting a Login Delay	5-103
Verifying Login	5-104
Setting Timeouts	5-106
Setting Multiple Privilege Levels	5-107
Configuring Banner Messages	5-110
Configuring Role-Based CLI	5-112
Role-Based CLI Details	5-113
Getting Started with Role-Based CLI	5-114
Configuring CLI Views	5-115
Configuring Superviews	5-117
Role-Based CLI Monitoring	5-118
Role-Based CLI Configuration Example	5-119
Role-Based CLI Verification	5-120
Secure Configuration Files	5-122
Securing Configuration Files	5-124
Cisco IOS Resilient Configuration Feature Verification	5-125
Secure Configuration Files Recovery	5-126
Summary	5-127
Mitigating Threats and Attacks with Access Lists	5-129
Overview	5-129
Objectives	5-129
Cisco ACLs	5-130
Identifying ACLs	5-132
Guidelines for Developing ACLs	5-134
Applying ACLs to Router Interfaces	5-136
Using Traffic Filtering with ACLs	5-137
Filtering Network Traffic to Mitigate Threats	5-139
IP Address Spoofing Mitigation: Outbound	5-140

DoS TCP SYN Attack Mitigation: Blocking External Access	5-141
DoS TCP SYN Attack Mitigation: Using TCP Intercept	5-142
DoS Smurf Attack Mitigation	5-143
Filtering Inbound ICMP Messages	5-144
Filtering Outbound ICMP Messages	5-145
Filtering UDP Traceroute Messages	5-146
Mitigating Distributed DoS with ACLs	5-147
Mitigate Distributed DoS Using Martian Filters	5-149
Distributed DoS Attack Mitigation: TRIN00	5-150
Distributed DoS Attack Mitigation: Stacheldraht	5-151
Distributed DoS Attack Mitigation: Trinity v3	5-152
Distributed DoS Attack Mitigation: SubSeven	5-153
Combining Access Functions	5-154
Caveats	5-158
Summary	5-160
Securing Management and Reporting Features	5-161
Overview	5-161
Objectives	5-161
Secure Management and Reporting Planning Considerations	5-162
Secure Management and Reporting Architecture	5-164
Information Paths	5-166
In-Band Management Considerations	5-167
Secure Management and Reporting Guidelines	5-168
Configuring an SSH Server for Secure Management and Reporting	5-170
Using Syslog Logging for Network Security	5-172
Syslog Systems	5-173
Cisco Log Severity Levels	5-174
Log Message Format	5-175
Configuring Syslog Logging	5-176
Example: Syslog Implementation	5-179
SNMP Version 3	5-180
Community Strings	5-181
SNMP Security Models and Levels	5-182
SNMPv3 Architecture	5-183
SNMPv3 Operational Model	5-184
SNMPv3 Features and Benefits	5-185
Configuring an SNMP Managed Node	5-186
Configuring the SNMP-Server Engine ID	5-187
Configuring the SNMP-Server Group Names	5-189
Configuring the SNMP-Server Users	5-191
Configuring the SNMP-Server Hosts	5-193
SNMPv3 Configuration Example	5-196
Configuring NTP Client	5-197
Configuring NTP Authentication	5-199
Configuring NTP Associations	5-200
Configuring Additional NTP Options	5-202
Configuring NTP Server	5-204
Configuring NTP Server	5-205
NTP Configuration Example	5-207
Summary	5-208
Configuring AAA on Cisco Routers	5-209
Overview	5-209
Objectives	5-209
Introduction to AAA	5-210
Implementing AAA	5-212
Router Access Modes	5-213
AAA Protocols: RADIUS and TACACS+	5-214
RADIUS Authentication and Authorization	5-215
RADIUS Messages	5-216

RADIUS Attributes	5-217
RADIUS Features	5-218
TACACS+ Authentication	5-219
TACACS+ Network Authorization	5-221
TACACS+ Command Authorization	5-223
TACACS+ Attributes and Features	5-224
Configuring the AAA Server	5-226
Configure AAA Login Authentication on Cisco Routers Using CLI	5-228
Character Mode Login Example	5-230
Configure AAA Login Authentication on Cisco Routers Using SDM	5-231
Confirming the AAA Activation	5-232
Defining AAA Servers	5-233
Creating a Login Authentication Policy	5-235
Configuring a Login Authentication Policy	5-236
Creating an EXEC Authorization Policy	5-237
Configuring an EXEC Authorization Policy	5-238
Creating Local User Accounts	5-239
Configuring VTY Line Parameters	5-240
Applying Authentication Policy to VTY Lines	5-241
Applying Authorization Policy to VTY Lines	5-242
Verifying AAA Login Authentication Commands	5-243
Troubleshoot AAA Login Authentication on Cisco Routers	5-244
Troubleshoot AAA Authentication Example	5-245
AAA Authorization Commands	5-246
Authorization Example	5-247
Troubleshooting Authorization	5-248
AAA Accounting Commands	5-251
AAA Accounting Example	5-253
Troubleshooting Accounting	5-255
Summary	5-256
References	5-256
Module Summary	5-257
Module Self-Check	5-258
Module Self-Check Answer Key	5-261

Cisco IOS Threat Defense Features **6-1**

Overview	6-1
Module Objectives	6-1

Introducing the Cisco IOS Firewall **6-3**

Overview	6-3
Objectives	6-3
Layered Defense Strategy	6-4
Layered Defense Features	6-5
Multiple DMZs	6-6
Modern DMZ Design	6-7
Firewall Technologies	6-8
Packet Filtering	6-10
Packet Filtering Example	6-11
Application Layer Gateway	6-12
ALG Firewall Device	6-13
Stateful Packet Filtering	6-14
Stateful Firewall Operation	6-16
Stateful Packet Filter Handling of Different Protocols	6-17
Introducing the Cisco IOS Firewall Feature Set	6-19
Cisco IOS Firewall	6-21
Cisco IOS Firewall Authentication Proxy	6-22
Cisco IOS Firewall IPS	6-23
Cisco IOS Firewall Functions	6-25
Cisco IOS Firewall TCP Handling	6-26

Cisco IOS Firewall UDP Handling	6-27
Cisco IOS Firewall Process	6-28
Supported Protocols	6-30
Alerts and Audit Trails	6-35
Summary	6-36
Implementing Cisco IOS Firewalls	6-37
Overview	6-37
Objectives	6-37
Configuring Cisco IOS Firewall from the CLI	6-38
Set Audit Trails and Alerts	6-40
Inspection Rules for Application Protocols	6-41
Apply an Inspection Rule to an Interface	6-43
Guidelines for Applying Inspection Rules and ACLs to Interfaces	6-44
Example: Two-Interface Firewall	6-45
Example: Three-Interface Firewall	6-46
Verifying Cisco IOS Firewall	6-47
Troubleshooting Cisco IOS Firewall	6-48
Basic and Advanced Firewall Wizards	6-49
Configuring a Basic Firewall	6-50
Basic Firewall Interface Configuration	6-51
Basic Firewall Configuration Summary and Deployment	6-52
Reviewing the Basic Firewall for the Originating Traffic	6-53
Reviewing the Basic Firewall for the Returning Traffic	6-54
Resulting Basic Firewall Inspection Rule Configuration	6-55
Resulting Basic Firewall ACL Configuration	6-56
Resulting Basic Firewall Interface Configuration	6-57
Configuring Interfaces on an Advanced Firewall	6-58
Advanced Firewall Interface Configuration	6-59
Configuring a DMZ on an Advanced Firewall	6-60
Advanced Firewall DMZ Service Configuration: TCP	6-61
Advanced Firewall DMZ Service Configuration: UDP	6-62
Advanced Firewall Security Configuration	6-64
Advanced Firewall Protocols and Applications	6-65
Advanced Firewall Inspection Parameters	6-68
Advanced Firewall Security Policy Selection	6-69
Complete the Configuration	6-70
Resulting Advanced Firewall Inspection Rule Configuration	6-71
Resulting Advanced Firewall ACL Configuration	6-72
Resulting Advanced Firewall Interface Configuration	6-73
Viewing Firewall Activity	6-74
Viewing Firewall Log	6-75
Summary	6-76
References	6-76
Introducing Cisco IOS IPS	6-77
Overview	6-77
Objectives	6-77
Introducing Cisco IOS IDS and IPS	6-78
Intrusion Detection System	6-78
Intrusion Protection System	6-79
Combining IDS and IPS	6-80
Types of IDS and IPS Systems	6-81
Signature-Based IDS and IPS	6-83
Policy-Based IDS and IPS	6-84
Anomaly-Based IDS and IPS	6-85
Honeypot	6-86
Network-Based and Host-Based IPS	6-87
Network-Based Versus Host-Based IPS	6-88
NIPS Features	6-89
NIDS and NIPS Deployment	6-90

IDS and IPS Signatures	6-91
Exploit Signatures	6-93
Signature Examples	6-95
Cisco IOS IPS Signature Definition Files	6-96
Cisco IOS IPS Alarms	6-97
Cisco IOS IPS Alarm Considerations	6-98
Summary	6-99
Configuring Cisco IOS IPS	6-101
Overview	6-101
Objectives	6-101
Configuring Cisco IOS IPS	6-102
Cisco IOS IPS Configuration Steps	6-102
Basic IOS IPS Configuration	6-103
Enhanced Cisco IOS IPS Configuration	6-104
Verifying IOS IPS Configuration	6-105
Cisco IOS IPS SDM Tasks	6-106
Selecting Interfaces and Configuring SDF Locations	6-107
IPS Policies Wizard Overview	6-108
Identifying Interfaces and Flow Direction	6-109
Selecting SDF Location	6-110
Viewing the IPS Policy Summary and Delivering the Configuration to the Router	6-113
Verifying IPS Deployment	6-114
Configuring IPS Policies and Global Settings	6-115
Global Settings	6-116
Viewing SDEE Messages	6-117
Viewing SDEE Status Messages	6-118
Viewing SDEE Alerts	6-119
Tuning Signatures	6-120
Editing a Signature	6-121
Disabling a Signature Group	6-122
Verifying the Tuned Signatures	6-123
Summary	6-124
Module Summary	6-125
Module Self-Check	6-126
Module Self-Check Answer Key	6-128

Cisco Device Hardening

Overview

Cisco IOS software has a full set of security features that you can implement to provide security for the network. This module describes the best practices for securing router administrative access using mechanisms such as password security features, failed login attempt handling, and role-based CLI. You will learn how to mitigate attacks using access lists. The module describes how to design and implement a secure management system including secure protocols such as Secure Shell (SSH), Simple Network Management Protocol version 3 (SNMPv3), and authenticated Network Time Protocol (NTP). The module discusses the most ubiquitous AAA protocols RADIUS and TACACS+, and explains the differences between them.

Module Objectives

Upon completing this module, you will be able to describe and configure Cisco device hardening. This ability includes being able to meet these objectives:

- Explain the strategies used to mitigate network attacks
- Describe the techniques used to harden a Cisco router
- Secure Cisco router installations and administrative access using passwords
- Mitigate threats and attacks to Cisco perimeter routers by configuring and applying ACLs to filter traffic
- Explain the procedures to securely implement management and reporting features of syslog, SSH, SNMPv3, and NTP
- Explain the procedures to configure AAA implementation on a Cisco router using both SDM and CLI

Mitigating Network Attacks

Overview

This lesson describes the types of network attacks and provides some general strategies for reducing vulnerabilities. Understanding what types of attacks are out in the WWW and the damage that they can do is a must for a network administrator. Today's network administrator must also know how to detect vulnerabilities in their network. Today's network administrator must know how to defend and mitigate these network attacks. This lesson will provide the network administrator information on how to use available open source tools to help discover vulnerabilities in their network and common threats that hackers are using today.

Objectives

Upon completing this lesson, you will be able to explain the strategies that are used to mitigate network attacks. This ability includes being able to meet these objectives:

- Describe the Cisco Self-Defending Network strategy
- List the types of attacks that enterprise networks must defend against
- Describe how to mitigate reconnaissance attacks including packet sniffers, port scans, ping sweeps, and Internet information queries
- Describe how to mitigate access attacks including password attacks, trust exploitation, buffer overflow, port redirection, and man-in-the-middle attacks
- Describe how to mitigate DoS attacks including IP spoofing and DDoS
- Describe how to mitigate worm, virus, and Trojan horse attacks
- Describe how to mitigate application layer attacks
- Describe vulnerabilities in configuration management protocols, and recommendations for mitigating these vulnerabilities
- Describe how to use open source tools to discover network vulnerabilities and threats

Cisco Self-Defending Network

This topic describes the Cisco Self-Defending Network strategy.

Cisco Self-Defending Network

- **Cisco strategy to dramatically improve the network ability to identify, prevent, and adapt to threats**
- **There are three categories:**
 - **Secure connectivity:**
 - **VPN solutions including VPN concentrators, VPN-enabled routers, and firewall VPNs**
 - **Threat defense:**
 - **Appliance and Cisco IOS-based firewalls**
 - **Cisco IDSs and IPSs**
 - **Trust and identity:**
 - **NAC, Cisco Secure ACS, and 802.1x technology**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-3

The Cisco Self-Defending Network strategy describes the Cisco vision for security systems, and helps customers more effectively manage and mitigate risks posed to their networked business systems and applications.

Cisco Self-Defending Network is the Cisco response to the increasing challenge of new threats and vulnerabilities that result from constantly evolving technologies and system developments. It provides a comprehensive approach to secure enterprise networks.

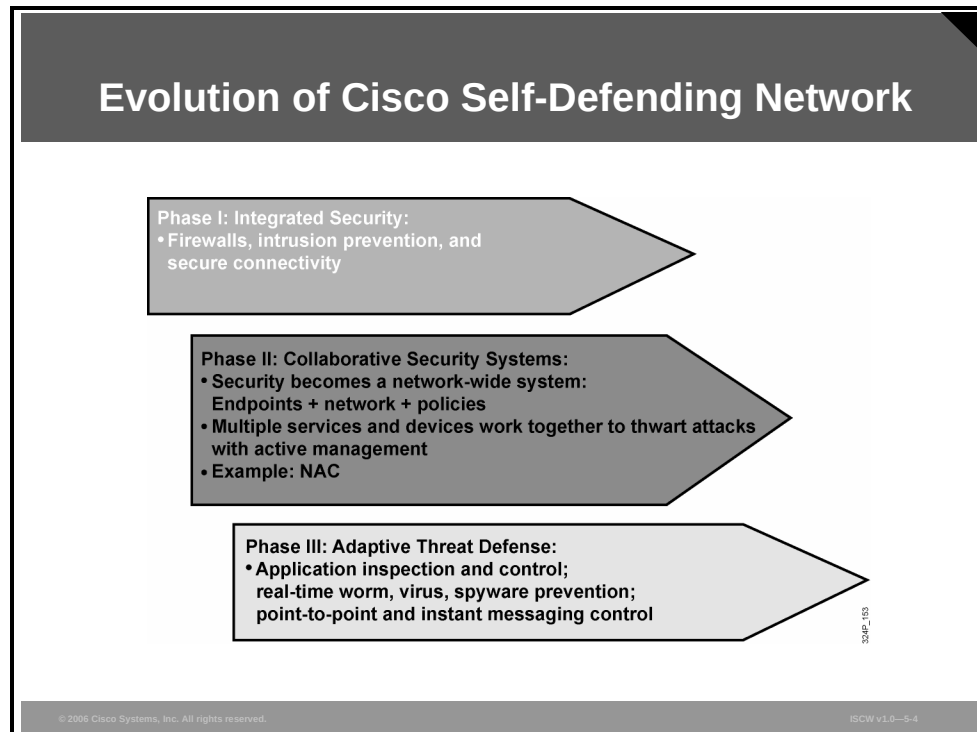
The Cisco Self-Defending Network strategy consists of three systems, or pillars, each with a specific purpose. By using Cisco integrated security solutions, customers can leverage their existing infrastructure to address potential threats to their network. While security risks are inherent in any network, customers can reduce their exposure and minimize these risks by deploying three categories of overlapping and complementary security solutions:

- **Secure connectivity:** Provides secure and scalable network connectivity, incorporating multiple types of traffic.
- **Threat defense:** Prevents and responds to network attacks and threats using network services.
- **Trust and identity:** Allows the network to intelligently protect endpoints using technologies such as authentication, authorization, and accounting (AAA), Cisco Secure Access Control Server (ACS), Network Admission Control (NAC), identity services, and 802.1x.

The Cisco Self-Defending Network is based on a foundation of security integrated throughout the network, with constant innovations in products and technologies and crafted into system-level solutions. Such solutions incorporate all aspects of the network as well as the sophisticated services needed to make it work. In addition, Cisco is working with major industry partners to ensure the completeness of the strategy.

Evolution of Cisco Self-Defending Network

Most customers will not adopt all of the components of the Cisco Self-Defending Network at one time, because it may be difficult to overhaul all of the required subsystems at once without disrupting the integrity of the IT services. Some customers may hesitate to turn over security controls to an automated system until they are confident that the system will operate dependably.



The figure illustrates the evolution of the Cisco Self-Defending Network strategy. While individual security products serve as good incubators for deploying advanced security technologies, they are not by themselves integrated throughout the network fabric. Building network security based solely on single-purpose appliances is no longer practical.

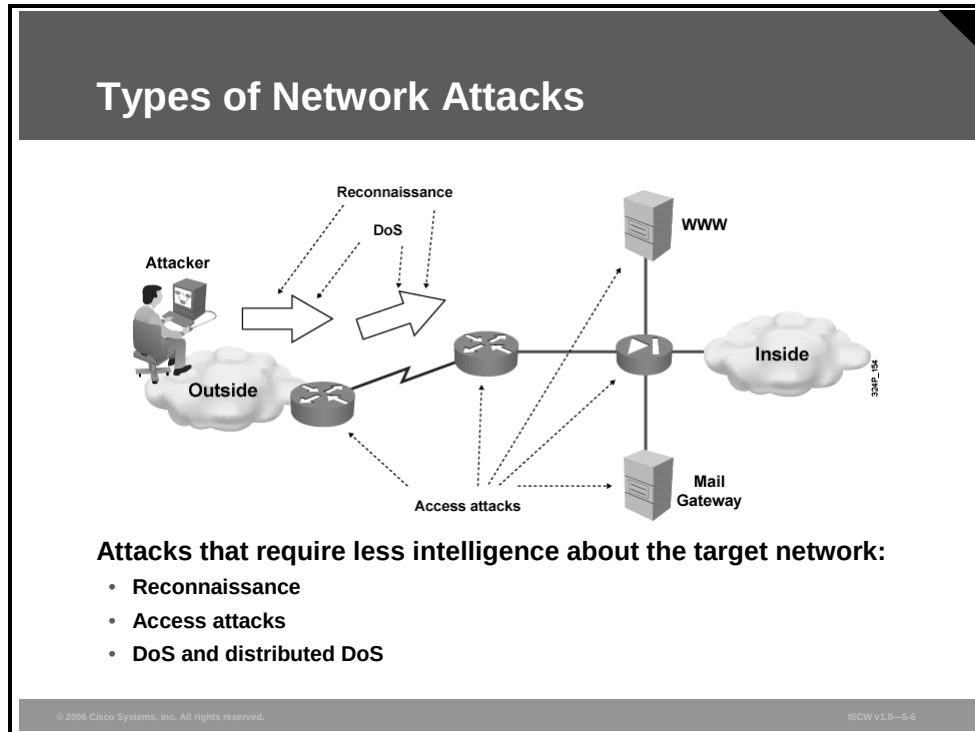
The self-defending network is developed in three phases:

- **Phase 1—Integrated security:** The first phase of the Cisco Self-Defending Network security strategy focuses on the need for integrated security, blending IP and security technologies. This phase aims to distribute security technologies throughout every segment of the network to enable every network element as a point of defense.
- **Phase 2—Collaborative security systems:** The next phase introduces the NAC industry initiative. NAC is a set of technologies and solutions built on an industry initiative led by Cisco. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can restrict the access of noncompliant devices. This initiative is the first industry-wide effort that increases the network ability to identify, prevent, and adapt to security threats. This phase aims to enable the security technologies integrated throughout the network to operate as a coordinated system. Network-wide collaboration among the services and devices throughout the network is used to defeat attacks.

- **Phase 3—Adaptive threat defense:** This phase aims at deploying innovative and threat defense technologies throughout the “integrated security” fabric of the network. The goal is to enable more proactive response to threats with greater operational efficiency by consolidating multiple security services on devices and building a mutual awareness among those services. Mutual awareness combines multiple security technologies on a device in a complementary fashion to deliver stronger security services. As an example, consider that a firewall provides good Layer 3 and Layer 4 access control and inspection, broad enforcement actions, and strong resiliency. Intrusion prevention systems (IPSs) provide strong application intelligence. Combining and integrating these capabilities provides an application intelligent device with broad mitigation capabilities, hardened resiliency, and these services that can be integrated throughout the network fabric:
 - **Application security:** Granular application inspection in firewalls and IPS (including Cisco IOS Firewall and IOS IPS). This service enforces appropriate application use policies (for example, “Do not allow users to use messaging service”). It also provides control of web traffic, including applications that abuse port 80 (messaging service and peer-to-peer), as well as control of web services, such as XML applications.
 - **Anti-X defenses:** Includes broad attack mitigation capabilities, such as malware protection, anti-virus, message security (anti-spam and anti-phishing), anti-distributed denial of service, and anti-worm. While these technologies are interested in and of themselves, anti-X defenses are not just about breadth of mitigation, but about distributing those mitigation points throughout key security enforcement points in the network to stop attacks as far from their intended destination and the core of the network as possible. Stopping an attack before it reaches the network core or host greatly diminishes the damage it can cause and its chances of spreading further.
 - **Network containment and control:** Network intelligence and the virtualization of security technologies provide the ability to layer sophisticated auditing, control, and correlation capabilities to control and protect any networked element. This enables a proactive response to threats by aggregating and correlating security information, as well as protecting network services, such as VoIP, and the device infrastructure, such as from the installation of rogue devices.

Types of Network Attacks

This topic describes the types of attacks that enterprise networks must defend against.



An attack against an enterprise network occurs in several stages. In the initial stages, the attacker may have only limited information about the target. One of the primary attacker objectives is to gather intelligence about the target vulnerabilities. The process of unauthorized collection of information about the network weaknesses is called a reconnaissance attack.

Other attacks that typically do not require in-depth knowledge about the target include access attacks, as well as denial of service (DoS) and distributed DoS attacks.

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.

DoS attacks are one of the most publicized forms of attack, and are also among the most difficult to completely eliminate. They can employ various techniques, such as overwhelming network resources, to render systems unavailable or reduce their functionality.

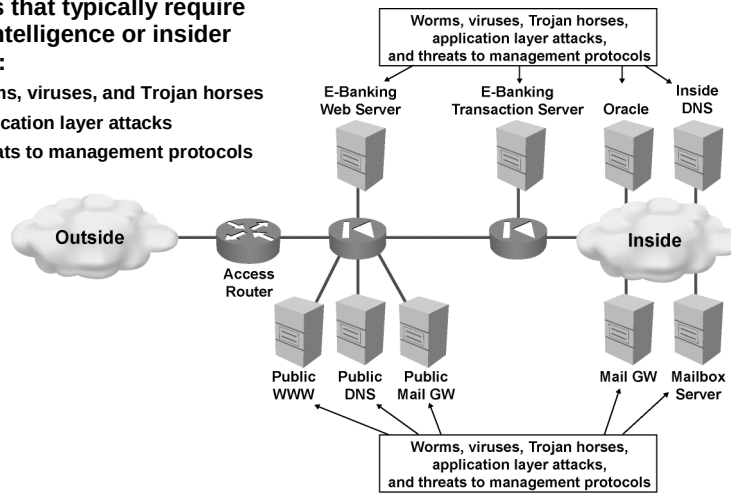
A DoS attack on a server sends extremely large volumes of requests over a network or the Internet. These large volumes of requests cause the attacked server to dramatically slow down, resulting in the attacked server becoming unavailable for legitimate access and use.

Distributed DoS attacks are the “next generation” of DoS attacks on the Internet. Victims of distributed DoS attacks experience packet flooding from many different sources (possibly spoofed IP source addresses) that overwhelm the network connectivity. In the past, the typical DoS attack involved a single attempt to flood a target host with packets. With distributed DoS tools, an attacker can conduct the same attack using thousands of systems.

Types of Network Attacks (Cont.)

Attacks that typically require more intelligence or insider access:

- Worms, viruses, and Trojan horses
- Application layer attacks
- Threats to management protocols



© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--6-7

Once the attacker has gathered information about the target network or even has direct access to the resources as an inside user, a range of other attack types can be launched against the enterprise systems.

Worms, viruses, and Trojan horses are examples of malicious code that can be used to compromise the hosts in the enterprise network. They can either be injected by an inside user or they can be used to exploit a vulnerability in the defense to compromise a protected system.

Application layer attacks are performed on the highest OSI layer in the information flow. The attacker attempts to compromise the protected system by manipulating the application layer data.

Management protocols are needed for system management. Like most other components, management protocols have vulnerabilities that can be exploited by an attacker to gain access to network resources.

Reconnaissance Attacks and Mitigation

This topic describes how to mitigate reconnaissance attacks, including packet sniffers, port scans, ping sweeps, and Internet information queries.

Reconnaissance Attacks and Mitigation

- **Reconnaissance refers to the overall act of learning information about a target network by using readily available information and applications.**
- **Reconnaissance attacks include:**
 - **Packet sniffers**
 - **Port scans**
 - **Ping sweeps**
 - **Internet information queries**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-9

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. Reconnaissance is also known as information gathering, and in most cases, precedes an actual access or DoS attack. First, the malicious intruder typically conducts a ping sweep of the target network to determine which IP addresses are alive. Then, 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 type and version of the application and operating system running on the target host. In many cases, the intruders look for vulnerable services that they can exploit later when there is less likelihood that anyone is looking.

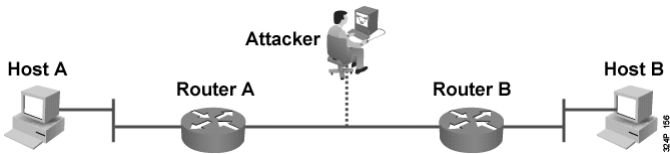
Reconnaissance is somewhat analogous to a thief surveying a neighborhood for vulnerable homes, such as an unoccupied residence, or a house with an easy-to-open door or window to break into. Reconnaissance attacks can consist of the following:

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

Packet Sniffers

This section describes the mitigation of reconnaissance attacks using packet sniffers.

Packet Sniffers



- A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets.
- Packet sniffers:
 - Exploit information passed in plaintext. Protocols that pass information in plaintext are Telnet, FTP, SNMP, POP, and HTTP.
 - Must be on the same collision domain.
 - Used legitimately, or can be designed specifically for attack.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-10

A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN. Packet sniffers can only work in the same collision domain. Promiscuous mode is a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing.

Plaintext is information sent across the network that is not encrypted. Some network applications distribute network packets in plaintext. Because the network packets are not encrypted, they can be processed and understood by any application that can pick them off the network and process them.

A network protocol specifies the protocol operations and packet format. 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. Numerous freeware and shareware packet sniffers are available that do not require the user to understand anything about the underlying protocols.

Note In an Ethernet LAN, promiscuous mode is a mode of operation in which every data frame transmitted can be received and read by a network adapter. Promiscuous mode is the opposite of nonpromiscuous mode.

Packet Sniffer Mitigation

This section describes packet sniffer mitigation.

Packet Sniffer Mitigation

The diagram shows a network topology with Host A connected to Router A, Router A connected to Router B, and Router B connected to Host B. An attacker is positioned between Router A and Router B, attempting to sniff the traffic. A large 'X' is placed over the attacker, indicating that the attack is being mitigated.

The mitigation techniques and tools include:

- Authentication
- Cryptography
- Antisniffer tools
- Switched infrastructure

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-11

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

- Authentication
- Switched infrastructure
- Antisniffer tools
- Cryptography

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. An example of common strong authentication is One Time Password (OTP).

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 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. 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.

Cryptography

Rendering packet sniffers irrelevant is the most effective method for countering packet sniffers. Cryptography is even more effective than preventing or detecting packet sniffers. If a communication channel is cryptographically secure, the only data a packet sniffer detects 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 (SSH) and Secure Sockets Layer (SSL).

Antisniffer Tools

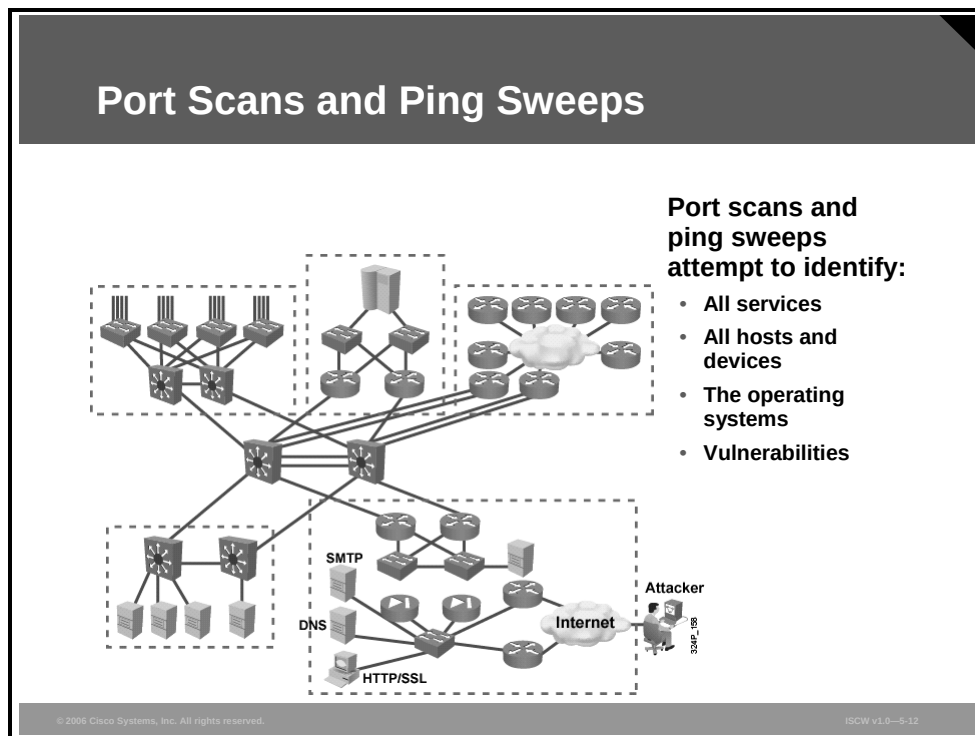
You can use software and hardware designed to detect the use of sniffers on a network. Such software and hardware does not completely eliminate the threat, but like many network security tools, they are part of the overall mitigation system. Antisniffer tools detect changes in the response time of hosts to determine whether the hosts are processing more traffic than their own traffic loads would indicate. One such network security software tool, called AntiSniff, is available from Security Software Technologies.

Switched Infrastructure

This technology, very common today, counters the use of packet sniffers in the network environment. 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.

Port Scans and Ping Sweeps

This section describes the reconnaissance attacks using port scans and ping sweeps.



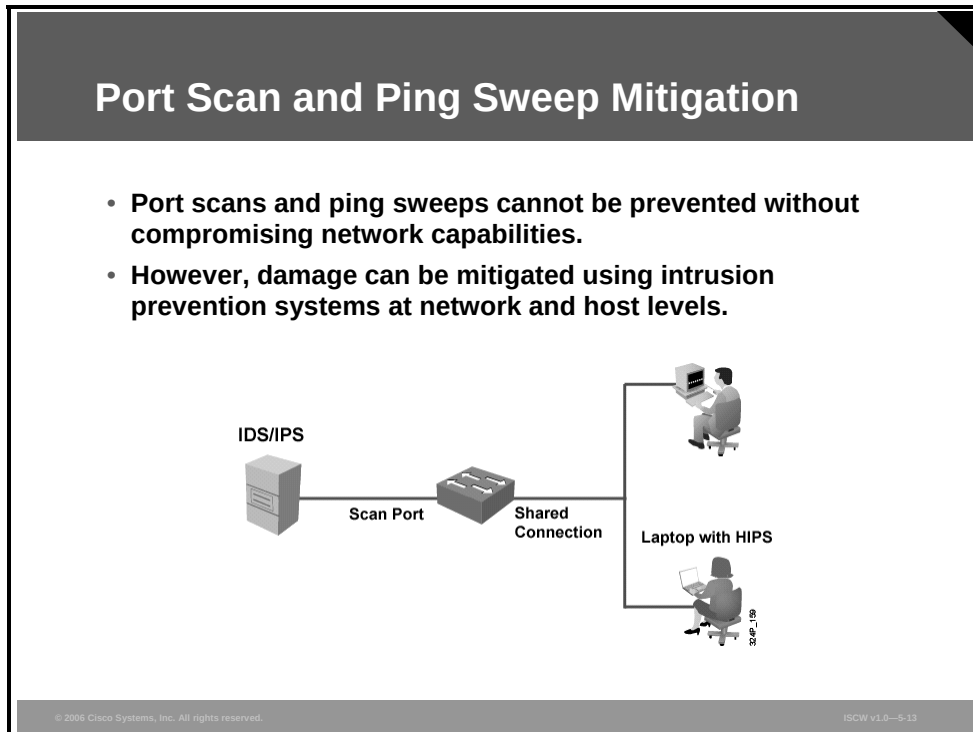
As legitimate tools, port scan and ping sweep applications run a series of tests against hosts and devices to identify vulnerable services. The information is gathered by examining IP addressing and port or banner data from both TCP and User Datagram Protocol (UDP) ports.

In an illegitimate situation, a port scan can be a series of messages sent by someone attempting to break into a computer to learn which computer network services the computer provides. Each service is associated with a “well-known” port number. Port scanning can be an automated scan of a range of TCP or UDP port numbers on a host to detect listening services. Port scanning, a favorite computer hacker approach, provides information to the assailant as to where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

A ping sweep, or Internet Control Message Protocol (ICMP) sweep, is a basic network scanning technique used to determine which range of IP addresses map to live hosts (computers). Whereas a single ping will tell you whether one specified host computer exists on the network, a ping sweep consists of ICMP echo requests sent to multiple hosts. If a given address is live, it will return an ICMP echo reply. Ping sweeps are among the older and slower methods used to scan a network. As an attack tool, a ping sweep sends ICMP (RFC 792) echo requests, or “pings,” to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

Port Scan and Ping Sweep Mitigation

Port scanning and ping sweeping is not a crime and there is no way to stop it when a computer is connected to the Internet. Accessing an Internet server opens a port, which opens a door to the computer. However, there are ways to prevent damage to the system.



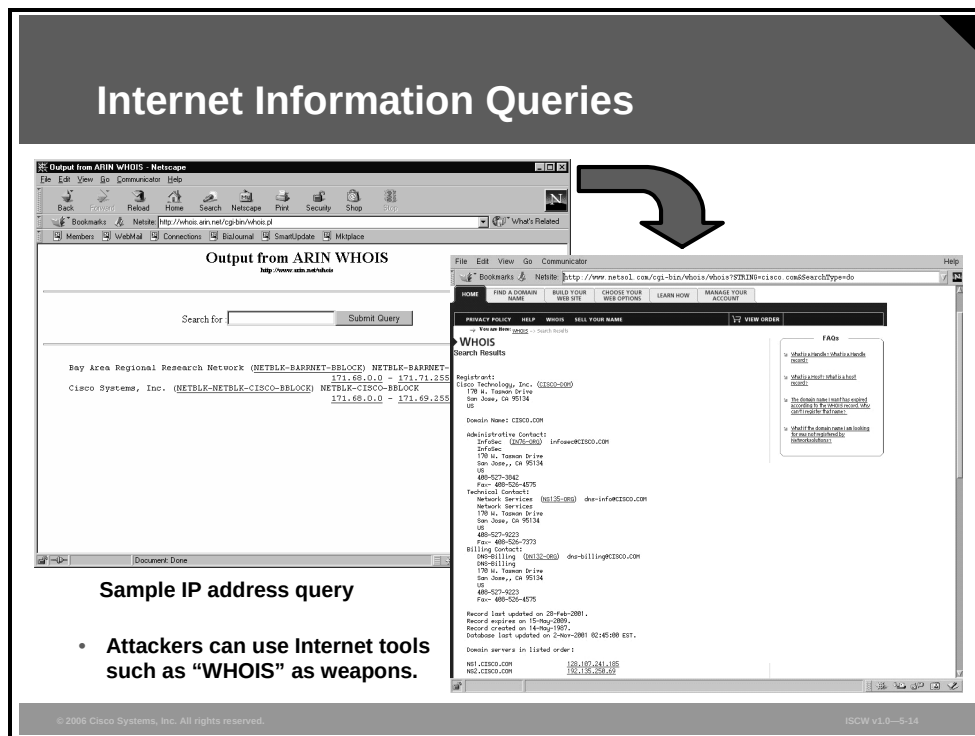
Ping sweeps can be stopped if ICMP echo and echo-reply are turned off on edge routers. However, network diagnostic data is lost. Port scans can easily be run without full ping sweeps; they simply take longer because they need to scan IP addresses that might not be live.

Network-based IPS and host-based IPS (HIPS) can usually notify you when a reconnaissance attack is under way. This warning allows you to better prepare for the coming attack or to notify the Internet service provider (ISP) that is hosting the system launching the reconnaissance probe. ISPs compare incoming traffic to the intrusion detection system (IDS) or the IPS signatures in their database. Signatures are characteristics of particular traffic patterns. A signature, such as “several packets to different destination ports from the same source address within a short period of time,” can be used to detect port scans. Another such signature could be “SYN to a non-listening port.”

A stealth scan is more difficult to detect, and many intrusion detection and prevention systems allow it to go unnoticed. Discovering stealth scans requires kernel-level work.

Internet Information Queries

The figure shows how existing Internet tools can be used for network reconnaissance.



Domain Name System (DNS) queries can reveal information such as who owns a particular domain and what addresses have been assigned to that domain. Ping sweeps of addresses revealed by 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. Hackers can examine the characteristics of the applications that are running on the hosts, which 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 which domain is associated with the addresses.

Access Attacks and Mitigation

This topic describes how to mitigate access attacks, including password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.

Access Attacks

- **Intruders use access attacks on networks or systems for these reasons:**
 - Retrieve data
 - Gain access
 - Escalate their access privileges
- **Access attacks include:**
 - Password attacks
 - Trust exploitation
 - Port redirection
 - Man-in-the-middle attacks
 - Buffer overflow

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-16

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 be performed in different ways. These are the most typical categories of access attacks:

- **Password attacks:** An attacker attempts to guess system passwords. A common example is a dictionary attack.
- **Trust exploitation:** An attacker uses privileges granted to a system in an unauthorized way, possibly leading to compromise of the target.
- **Port redirection:** A compromised system is used as a jump-off point for attacks against other targets. An intrusion tool is installed on the compromised system for session redirection.
- **Man-in-the-middle attacks:** Attackers place themselves in the middle of communications between two legitimate entities, to read or even modify data exchanged between the two parties.
- **Buffer overflow:** A program writes data beyond the allocated end of a buffer in memory. Buffer overflows usually arise as a consequence of a bug and the improper use of languages such as C or C++ that are not “memory-safe.” One consequence of the overflow is that valid data can be overwritten. Buffer overflows are also a commonly exploited computer security risk—program control data often sits in memory areas adjacent to data buffers, and by means of a buffer overflow condition, the computer can be made to execute arbitrary and potentially malicious code.

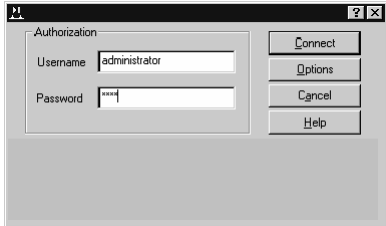
Password Attacks

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.

Password Attacks

Hackers implement password attacks using the following:

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



© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-17

A brute-force attack is often 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, the attacker 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 Example

As with packet sniffer and IP spoofing attacks, a brute-force password attack can provide access to accounts that can be used to modify critical network files and services. An example of a password attack that compromises your network integrity is when an attacker attaches the router password and then uses that information to modify the routing tables for your network. By doing so, the attacker ensures that all network packets are routed to the attacker before they are transmitted to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

Password Attack Example

- L0phtCrack takes the hashes of passwords and generates the plaintext passwords from them.
- Passwords are compromised using one of two methods:
 - Dictionary cracking
 - Brute-force computation

A big security risk is the fact that passwords are stored as plaintext. To overcome this risk, passwords should be encrypted. On most systems, passwords are run through an encryption algorithm to generate a one-way hash. A one-way hash is a string of characters that cannot be reversed into its original text. The hash is not the encrypted password, but rather a result of the algorithm. The strength of the hash lies in the fact that the hash value can only be recreated using the original user and password information, and that it is impossible to retrieve the original information from the hash. This strength makes hashes perfect for encoding passwords for storage. In granting authorization, the hashes are calculated and compared, rather than the plain password.

During the login process, you supply an account and password, and the algorithm generates a one-way hash. This hash is compared to the hash stored on the system. If they are the same, it is assumed that the proper password was supplied.

L0phtCrack is a Windows NT password-auditing tool used to compute Windows NT user passwords from the cryptographic hashes that are stored in the system registry. L0phtCrack computes the password from a variety of sources using a variety of methods. The end result is a state of the art tool for recovering passwords.

Password Attack Mitigation

This section describes the mitigation of password attacks.

Password Attack Mitigation

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 plaintext passwords.
- Use “strong” passwords. (Use “mY8!Rthd8y” rather than “mybirthday”)

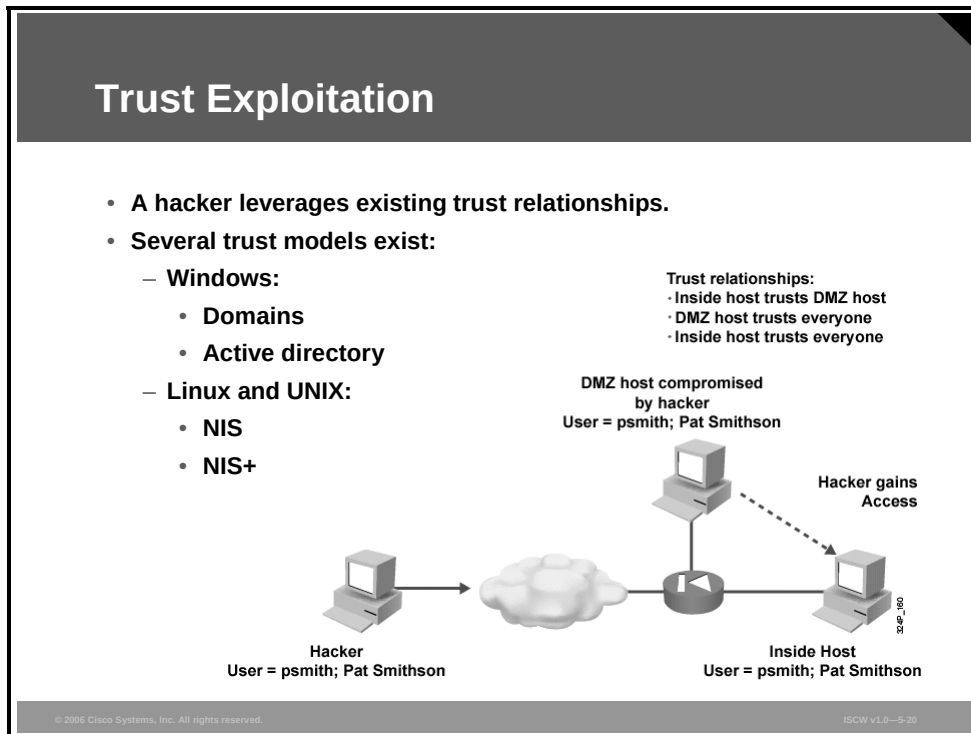
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-19

Password attack mitigation techniques are as follows:

- Do not allow users to have the same password on multiple systems. Most users use the same password for each system they access, and often personal system passwords are also the same.
- Disable accounts after a specific number of unsuccessful logins. This practice helps to prevent continuous password attempts.
- Do not use plaintext passwords. Use of either an OTP or encrypted password is recommended.
- Use “strong” passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters. Many systems now provide strong password support and can restrict a user to the use of strong passwords only.

Trust Exploitation

Although not an attack in itself, trust exploitation refers to an individual taking advantage of a trust relationship within a network.



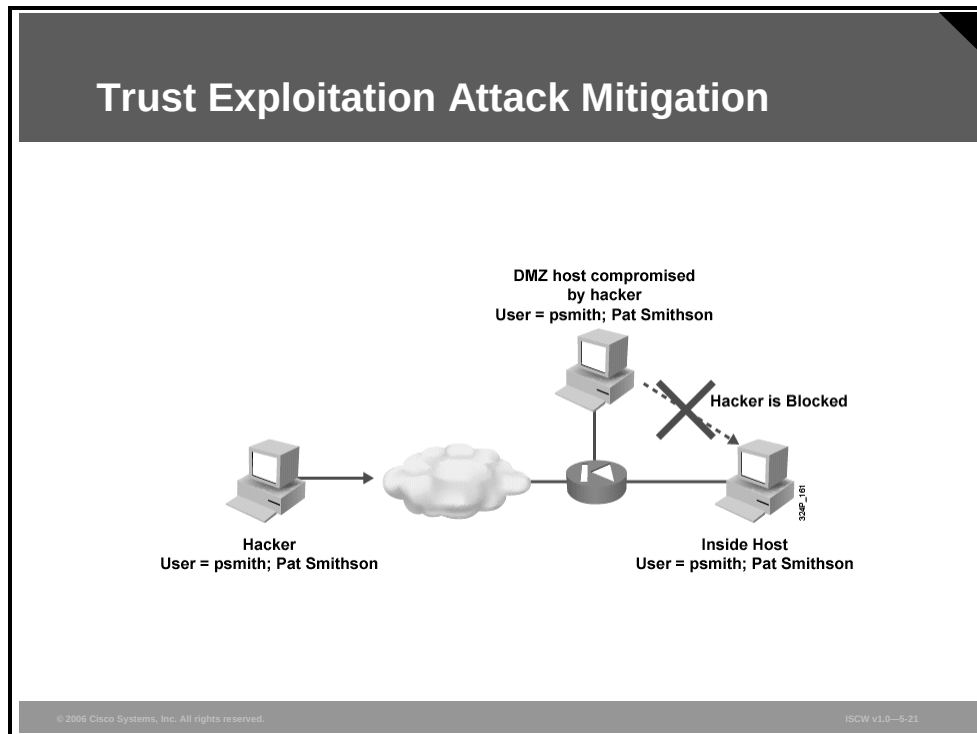
An example of when a trust exploitation can take place is when a perimeter network is connected to a corporate network. These network segments often house DNS, Simple Mail Transfer Protocol (SMTP), and HTTP servers. Because these servers all reside on the same segment, a compromise of one system can lead to the compromise of other systems if those other systems in turn trust systems attached to the same network.

Another example of trust exploitation is a Demilitarized Zone (DMZ) host that has a trust relationship with an inside host connected to the inside firewall interface. The inside host trusts the DMZ host. When the DMZ host is compromised, the attacker can leverage that trust relationship to attack the inside host.

Note	A DMZ is a dedicated part of a network designed to secure communications between the inside and outside network.

Trust Exploitation Attack Mitigation

You can mitigate trust exploitation-based attacks through tight constraints on trust levels within a network.

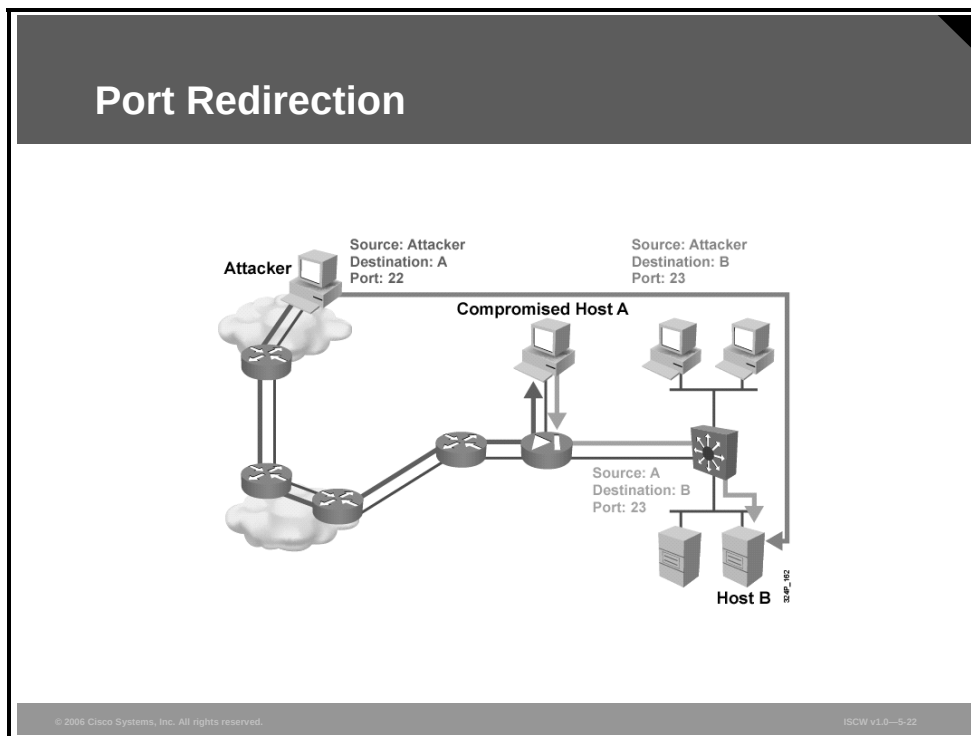


Systems on the inside of a firewall should never absolutely trust systems on the outside of a firewall. Such trust should be limited to specific protocols and, where possible, should be validated by something other than an IP address.

In the example above, the hacker attached to the Internet already exploited some vulnerability of the DMZ host, which is connected to the DMZ interface of the firewall. The hacker controls the entire DMZ host. His next goal is to compromise the inside host that is connected to the inside (trusted) interface of the firewall. To attack the inside host from the DMZ host, the hacker needs to find the protocols that are permitted from the DMZ to the inside interface. Then the attacker would search for vulnerability on the inside host and exploit it. If the firewall is configured to allow only minimum or no connectivity from the DMZ to the inside, this attack can be stopped.

Port Redirection

A port redirection attack is a type of trust exploitation attack that uses a compromised host to pass traffic that would otherwise be dropped through a firewall.



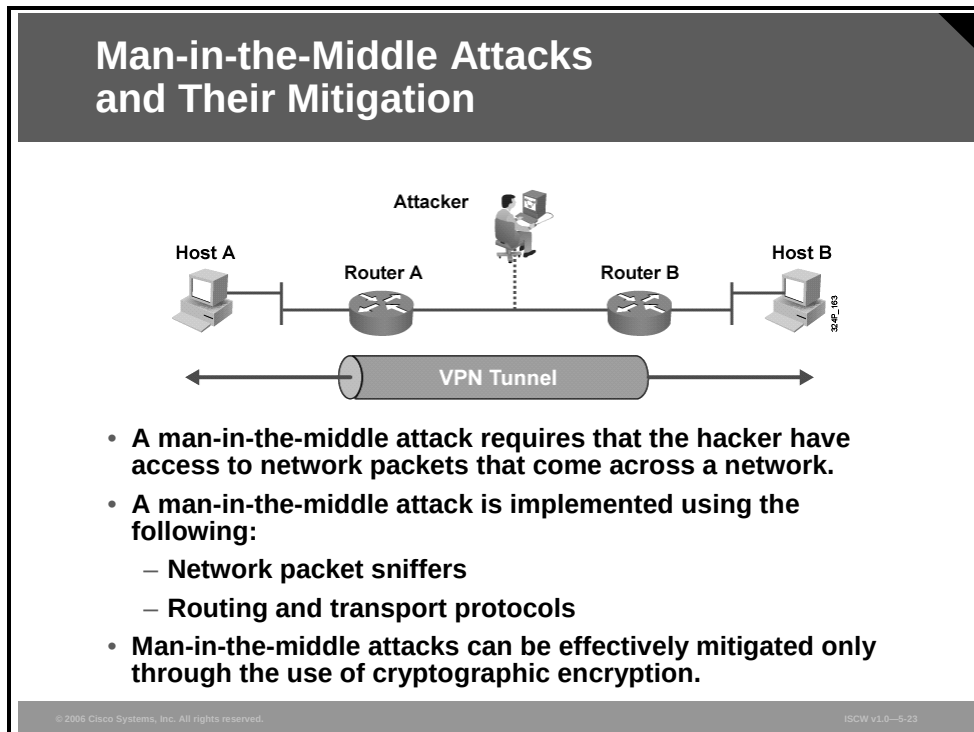
The figure shows a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment (host A), but not the host on the inside (host B). The host on the public services segment can reach the host on both the outside and the inside. If hackers are able to compromise the public services segment host, they can 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 provides that type of access is Netcat.

Port redirection can be mitigated primarily through the use of proper trust models that are network-specific. Assuming a system is under attack, a HIPS can help detect a hacker and prevent installation of such utilities on a host.

Man-in-the-Middle Attacks

Man-in-the-middle attacks have these purposes:

- Theft of information
- Hijacking of an ongoing session to gain access to your internal network resources
- Traffic analysis to obtain information about your network and its users
- DoS
- Corruption of transmitted data
- Introduction of new information into network sessions



An example of a man-in-the-middle attack is when someone working for your ISP gains access to all network packets transferred between your network and any other network. Man-in-the-middle attackers can make sure not to disrupt the traffic and thus set off alarms. Instead, they use their position to stealthily extract information from the network.

Man-in-the-middle attack mitigation is achieved, as shown in the figure, by encrypting traffic in a VPN tunnel. Encryption allows the hacker to see only cipher text.

DoS Attacks and Mitigation

This topic describes how to mitigate DoS attacks, including IP spoofing and distributed DoS.

DoS Attacks and Mitigation

- A DoS attack damages or corrupts your computer system or denies you and others access to your networks, systems, or services.
- Distributed DoS technique performs simultaneous attacks from many distributed sources.
- DoS and Distributed DoS attacks can use IP spoofing.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-25

A DoS attack tries to overload system resources, crashing the applications or processes by executing exploits or a combination of exploits. DoS attacks are the most publicized form of attack, and 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. Nevertheless, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators. DoS attacks can target many various vulnerabilities. A common type of DoS attack is distributed DoS using a spoofed source IP address.

Distributed DoS Attacks

A distributed DoS attack and its simpler version, a DoS attack on a server, send an extremely large number of requests over a network or the Internet. These many requests cause the target server to dramatically slow down. Consequently, the attacked server becomes unavailable for legitimate access and use.

Distributed DoS Attacks

- **DoS and distributed DoS attacks focus on making a service unavailable for normal use.**
- **DoS and distributed DoS attacks have these characteristics:**
 - **Generally not targeted at gaining access to your network or the information on your network**
 - **Require very little effort to execute**
 - **Difficult to eliminate, but their damage can be minimized**

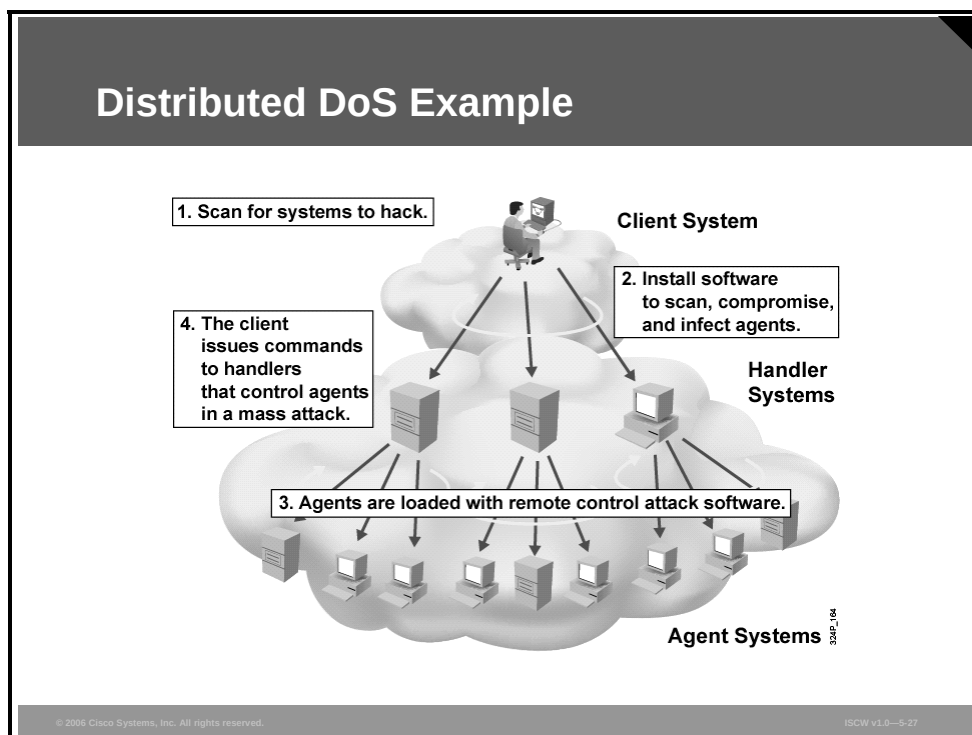
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-25

DoS and distributed 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. This result 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 and distributed DoS attacks are among the most difficult to completely eliminate because of the way they use protocol weaknesses and native or legitimate traffic to attack a network.

For all known DoS and distributed DoS attacks, there are software fixes that you can install to limit the damage caused by the attacks. However, as with viruses, hackers are constantly developing new DoS and distributed DoS attacks.

Distributed DoS Example

Distributed DoS attacks are the next generation of DoS attacks on the Internet. This type of attack is not new. UDP and TCP SYN flooding (sending large numbers of UDP segments or TCP SYN packets to the target system), ICMP echo-request floods, and ICMP directed broadcasts (also known as smurf attacks) are similar to distributed DoS attacks; however, the scope of a distributed DoS attack is different. Victims of distributed DoS attacks experience packet flooding from many different sources, possibly spoofed IP source addresses that bring network connectivity to a halt. In the past, the typical DoS attack involved a single attempt to flood a target host with packets. With distributed DoS tools, an attacker can conduct the same attack using thousands of systems.



In the figure, the hacker uses a terminal to scan for systems to hack. After handler systems are accessed, the hacker installs software on these systems. This software attempts to scan for, compromise, and infect agent systems. When the agent systems are accessed, the hacker then loads remote control attack software to carry out the distributed DoS attack.

DoS and Distributed DoS Attack Mitigation

When attacks involve specific network server applications, such as an HTTP server or an FTP server, the attacker focuses on acquiring and keeping all the available connections supported by that server open. This strategy effectively locks out valid users of the server or service.

DoS and Distributed DoS Attack Mitigation

The threat of DoS attacks can be reduced using:

- **Anti-spoof features on routers and firewalls**
- **Anti-DoS features on routers and firewalls**
- **Traffic rate limiting at the ISP level**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-28

DoS attacks can also be implemented using common Internet protocols, such as TCP and ICMP. For example, “Ping of Death” exploits limitations in the IP protocol. 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 these three methods:

- **Anti-spoof features:** Proper configuration of anti-spoof features on your routers and firewalls can reduce your risk. These features include an appropriate filtering with access lists, unicast reverse path forwarding that looks up the routing table to identify spoofed packets, disabling of source route options, and others.
- **Anti-DoS features:** Proper configuration of anti-DoS features on routers and firewalls can help limit the effectiveness of an attack. These features often involve limits on the amount of half-open TCP connections that a system allows at any given time. This method is also known as SYN-flooding prevention, and can be configured on the router either by limiting the overall number of half-open TCP sessions that can go through the router, by limiting the number of half-open sessions per minute, or limiting the number of half-open sessions destined to a specific server.
- **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 distributed DoS attacks are common.

IP Spoofing in DoS and DDoS

IP spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, hackers must first use a variety of techniques to find an IP address of a trusted host and then modify their packet headers to appear as though packets are coming from that trusted host. Further, the attacker can engage other unsuspecting hosts to also generate traffic that appears as though it too is coming from the trusted host, thus flooding the network.

IP Spoofing in DoS and Distributed DoS

- **IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.**
- **IP spoofing can use either a trusted IP address in the network or a trusted external IP address.**
- **Uses for IP spoofing include:**
 - **Injecting malicious data or commands into an existing data stream**
 - **Diverting all network packets to the hacker who can then reply as a trusted user by changing the routing tables**
- **IP spoofing may only be one step in a larger attack.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0-5-28

Routers determine the best route between distant computers by examining the destination address. The originating address is ignored by routers. However, the destination machine uses the originating address when it responds back to the source. In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. For example, 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 your network trusts and provides specified resource access to. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers so that it appears that the packets are coming from the trusted system. The goal of the attack is to establish a connection that allows the attacker to gain root access to the host and to create a backdoor entry path into the target system.

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 to simply not worry about receiving any response from the applications. For example, if an attacker is attempting to get a system to mail a sensitive file, application responses are unimportant.

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

IP spoofing can also provide access to user accounts and passwords, or it can 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 also possible when simple spoofing attacks are combined with knowledge of messaging protocols.

Distributed DoS attacks are often carried out using a spoofed source IP address.

IP Spoofing Attack Mitigation

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

- Access control configuration
- Encryption
- RFC 3704 filtering
- Additional authentication

IP Spoofing Attack Mitigation

The threat of IP spoofing can be reduced, but not eliminated, using these measures:

- Access control configuration
- Encryption
- RFC 3704 filtering
- Additional authentication requirement that does not use IP address-based authentication; examples are:
 - Cryptographic (recommended)
 - Strong, two-factor, one-time passwords

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-30

Access Control Configuration

The most common method for preventing IP spoofing is to properly configure access control. To reduce the effectiveness of IP spoofing, configure the access control list (ACL) to deny any traffic from the external network that has a source address that should reside on the internal network. 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.

Encryption

Another possible way to prevent IP spoofing is to encrypt all network traffic to avoid source and destination hosts from being compromised.

RFC 3704 Filtering

You can prevent your network users 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 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.

Note	RCF 3704 covers ingress filtering for multihomed networks. It updates RFC 2827.

Note	RFC 2827 defines filters to drop packets coming from source addresses within 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, or 240.0.0.0/4. This source address is a so-called "Martian Address."

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—eliminate 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. However, when cryptographic authentication is not possible, strong two-factor authentication using OTPs can also be effective.

Worm, Virus, and Trojan Horse Attacks and Mitigation

This topic describes how to mitigate worm, virus, and Trojan horse attacks.

Worm, Virus, and Trojan Horse Attacks and Mitigation

The primary vulnerabilities for end-user workstations are:

- **Worms**
- **Viruses**
- **Trojan horse attacks**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-32

Viruses are malicious software programs that are attached to other programs and which execute a particular unwanted function on a user workstation. A virus propagates itself by infecting other programs on the same computer. Viruses can do serious damage, such as erasing files or erasing an entire disk. They can also be a simple annoyance, such as popping up a window that says “Ha, ha, you are infected.” Viruses cannot spread to a new computer without human assistance, for example, opening an infected file on a removable media such as an e-mail attachment, or through file sharing.

A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. It can then infect other hosts from the infected computer. Like a virus, a worm is also a program that propagates itself. Unlike a virus, a worm can spread itself automatically over the network from one computer to the next. Worms are not clever or evil, they just take advantage of automatic file sending and receiving features found on many computers.

Trojan horse is a general term, referring to programs that appear desirable, but actually contain something harmful. For example, a downloaded game could erase files. The contents could also hold a virus or a worm.

A Trojan horse can attack on three levels. A virus known as the “Love Bug” is an example of a Trojan horse because it pretended to be a love letter when it actually carried a harmful program. The Love Bug was a virus because it infected all image files on the attacked disk, turning them into new Trojans. Finally, the Love Bug was a worm because it propagated itself over the Internet by hiding in the Trojan horses that it sent out using addresses in the attacked e-mail address book.

Virus and Trojan Horse Attack Mitigation

Viruses and Trojan horse attacks can be contained through the effective use of antivirus software at the user level and potentially at the network level.

Virus and Trojan Horse Attack Mitigation

Viruses and Trojan horses can be contained by:

- **Effective use of antivirus software**
- **Keeping up-to-date with the latest developments in these methods of attacks**
- **Keeping up-to-date with the latest antivirus software and application versions**
- **Implementing host-based intrusion prevention systems (e.g., CSA)**

© 2006 Cisco Systems, Inc. All rights reserved.

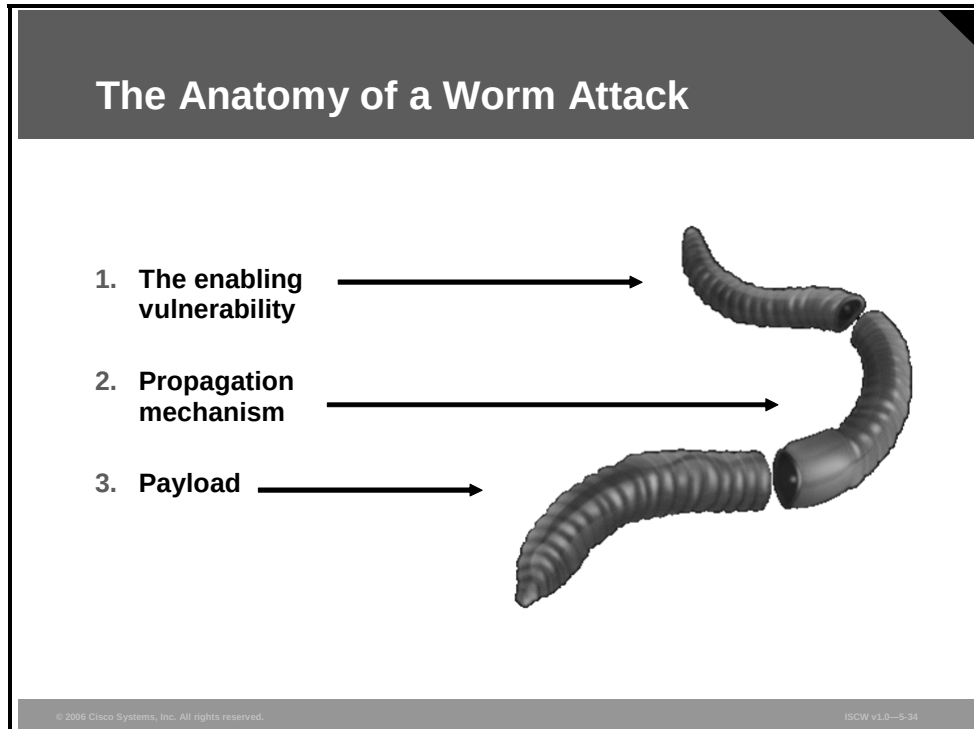
ISCW v1.0--5-33

Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping up-to-date with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus or Trojan horse applications are released, enterprises need to keep up-to-date with the latest antivirus software and application versions and patches. Deploying host-based intrusion prevention systems, such as the Cisco Security Agent (CSA), provides a very effective defense-in-depth method to prevent attacks against the hosts.

The Anatomy of a Worm Attack

The anatomy of a worm attack is as follows:

- **The enabling vulnerability:** A worm installs itself 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 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 vulnerabilities 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 path 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.

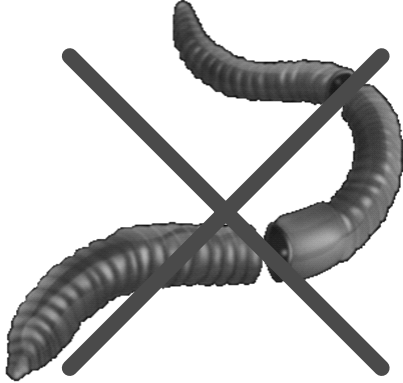
Mitigating Worm Attacks

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.

Mitigating Worm Attacks

Four steps to mitigate worm attacks:

1. **Contain**
2. **Inoculate**
3. **Quarantine**
4. **Treat**



© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-35

The recommended steps for worm attack mitigation are:

- Step 1 Containment:** Contain the spread of the worm inside your network and within your network. Compartmentalize parts of your network that have not been infected.
- Step 2 Inoculation:** Start patching all systems and, if possible, scanning for vulnerable systems.
- Step 3 Quarantine:** Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.
- Step 4 Treatment:** Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.

Typical incident response methodologies can be subdivided into six major categories. These categories are based on the network service provider security 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.

Application Layer Attacks and Mitigation

This topic describes how to mitigate application layer attacks.

Application Layer Attacks

Application layer attacks have these characteristics:

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

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

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-37

Application layer attacks can be implemented using several different methods:

- One of the most common methods of implementing application layer attacks 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 permission of the account running the application. The account 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 may 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 the organization 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 or Bad Password or a combination), exits, and starts the normal login sequence. The user believes that they have incorrectly entered the password, reenters 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 browser.

Netcat

Netcat is a featured networking utility that reads and writes data across network connections using the TCP/IP protocol.

Netcat

```
#nc -h
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [-options] [hostname] [port]
options:
  -g gateway           source-routing hop point[s], up to 8
  -G num              source-routing pointer: 4, 8, 12, ...
  -i secs             delay interval for lines sent, ports scanned
  -l                 listen mode, for inbound connects
  -n                 numeric-only IP addresses, no DNS
  -o file             hex dump of traffic
  -p port             local port number
  -r                 randomize local and remote ports
  -s addr             local source address
  -u                 UDP mode
  -v                 verbose [use twice to be more verbose]
port numbers can be individual or ranges: lo-hi [inclusive]
```

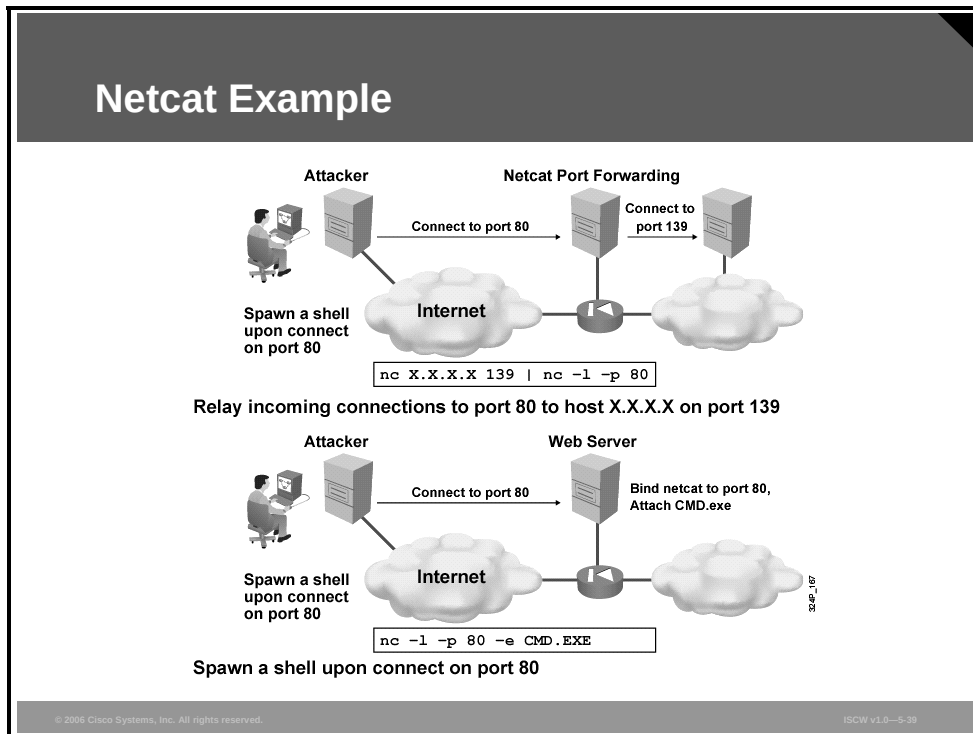
- **Netcat is a tool that reads or writes data on any TCP/UDP connections, relays TCP connections, and can act as a TCP/UDP server**

© 2006 Cisco Systems, Inc. All rights reserved. RSCW v1.0--5.38

Netcat is designed to be a reliable “back-end” tool that can be used directly or can easily be driven by other programs and scripts. At the same time, Netcat is a feature-rich network debugging and exploration tool because it can create almost any kind of connection you would need and it has several interesting built-in capabilities.

Netcat Example

The example illustrates how to use Netcat to redirect a TCP session from port 80 on the host where Netcat is running to port 139 on the machine with the address X.X.X.X.



The first example in the figure shows how a hacker who gained access to a DMZ host uses Netcat on that host to relay traffic. All TCP sessions destined to TCP port 80 on the local system will be redirected to an inside host on TCP port 139. This will allow the hacker to access TCP port 139 of the inside host, although the firewall permits only HTTP traffic to the DMZ host.

The second example shows that Netcat is able to execute a program when the local system accepts a network connection. Any connection accepted by the DMZ system on the local TCP port 80 will spawn a CMD.exe shell. As a result, when a hacker connects to the HTTP server running on that DMZ host, they will receive a command prompt, effectively allowing the attacker to perform any operations within the system.

Mitigation of Application Layer Attacks

You can take various measures to reduce your risks for application layer attacks.

Mitigation of Application Layer Attacks

Measures you can take to reduce your risks include:

- 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 IDS/IPS that can scan for known attacks, monitor and log attacks, and, in some cases, prevent attacks.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-40

These are some of the measures that you can take to reduce your risks:

- 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 IDS, IPS, or both to scan for known attacks, monitor and log attacks, and ultimately prevent attacks. Using these systems is essential to identifying security threats and mitigating some of these threats. In most cases, mitigation can be done automatically.

Management Protocols and Vulnerabilities

This topic describes vulnerabilities in configuration management protocols, and provides recommendations for mitigating these vulnerabilities.

Configuration Management

- Configuration management protocols include SSH, SSL, and Telnet.
- Telnet issues include:
 - The data within a Telnet session is sent as plaintext.
 - The data may include sensitive information.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-42

If the managed device does not support any of the recommended management protocols, such as SSH and SSL, Telnet (not recommended) may have to be used. Recall that Telnet was developed in an era when security was not an issue. The network administrator should recognize that the data within a Telnet session is sent as plaintext 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 or sensitive information, such as the configuration of the device itself, passwords, or other sensitive data.

Configuration Management Recommendations

Regardless of whether SSH, SSL, or Telnet is used for remote access to the managed device, you should configure ACLs to allow only management servers to connect to the device. All attempts from other IP addresses should be denied and logged.

Configuration Management Recommendations

These practices are recommended:

- **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 3704 filtering at the perimeter router should be used to mitigate the chance of an outside attacker spoofing the addresses of the management hosts.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-43

Configuration management is an essential component of the network availability. Therefore, its security is of paramount importance.

You should use secure management protocols when configuring all network devices. Some management protocols, such as SSH and SSL, have been designed with security in mind and can be used in the management solution. Other protocols, such as Telnet and Simple Network Management Protocol version 2 (SNMPv2), must be made secure by protecting the data with IPsec. IPsec provides the encryption and authentication needed to combat an attacker who tries to compromise the data exchange.

You should use access lists to further limit connectivity to the network devices and hosts. The access lists should permit management access, such as SSH or HTTPS, only from the legitimate management hosts.

RFC 3704 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

This section describes the security flaws of some common management protocols.

Management Protocols

These management protocols can be compromised:

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

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-44

SNMP is a network management protocol that you can use 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 version 1 and 2 uses passwords (called community strings) within each message as a simple form of security. Unfortunately, SNMPv1/v2 devices send the community string in plaintext along with the message. Therefore, SNMPv1/v2 messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. SNMPv3 overcomes these shortcomings by providing authentication and encryption to the message exchange.

The syslog protocol is designed to carry messages from a device that is configured for logging to a syslog server that collects the information. The messages are sent as plaintext 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.

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 plaintext, you should recognize that 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. Whenever possible, TFTP traffic should be encrypted within an IPsec tunnel in order to reduce the chance of interception.

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, via satellite or radio, to Coordinated Universal Time (UTC). However, if network administrators do not wish to implement their own master clocks because of cost or other reasons, clock sources are available for synchronization via the Internet.

The current version of NTP is version 4. The latest version defined by an RFC is version 3, which is recommended from a security perspective.

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

Management Protocol Best Practices

This section describes the best practices that should be followed when implementing a secure management solution.

Management Protocol Best Practices	
Management Protocol	Recommendations
SNMP	• Configure SNMP with only read-only community strings. • Set up access control on the device you wish to manage. • Use SNMP version 3.
Syslog	• Encrypt syslog traffic within an IPsec tunnel. • Implement RFC 3704 filtering. • Set up access control on the firewall.
TFTP	• Encrypt TFTP traffic within an IPsec tunnel.
NTP	• 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.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-45

These are recommendations for the correct use of SNMP tools:

- 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. This version provides secure access to devices through a combination of authenticating and encrypting management packets over the network.

When possible, the following management practices are advised:

- Encrypt syslog traffic within an IPsec tunnel.
- Implement RFC 3704 filtering at the perimeter router when allowing syslog access from devices on the outside of a firewall.
- Implement ACLs on the firewall to allow syslog data from only the managed devices themselves to reach the management hosts.
- When possible, encrypt TFTP traffic within an IPsec tunnel in order to reduce the chance of interception.

The following are recommendations to follow when using NTP:

- 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. NTP v3 is currently supported by most vendors, including Cisco. The latest version 4 is not defined by any RFC, and therefore not widely supported.
- Use ACLs that specify which network devices are allowed to synchronize with other network devices.

Determining Vulnerabilities and Threats

This topic describes how to use open source tools to discover network vulnerabilities and threats.

Determining Vulnerabilities and Threats

The following tools are useful when determining general network vulnerabilities:

- **Blue's PortScanner**
- **Ethereal**
- **Microsoft Baseline Security Analyzer**
- **Nmap**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-47

There are several tools and techniques that you can use to find vulnerabilities in your network. Once you identify the vulnerabilities, you can consider and implement mitigation steps as appropriate. Use these tools to determine vulnerabilities:

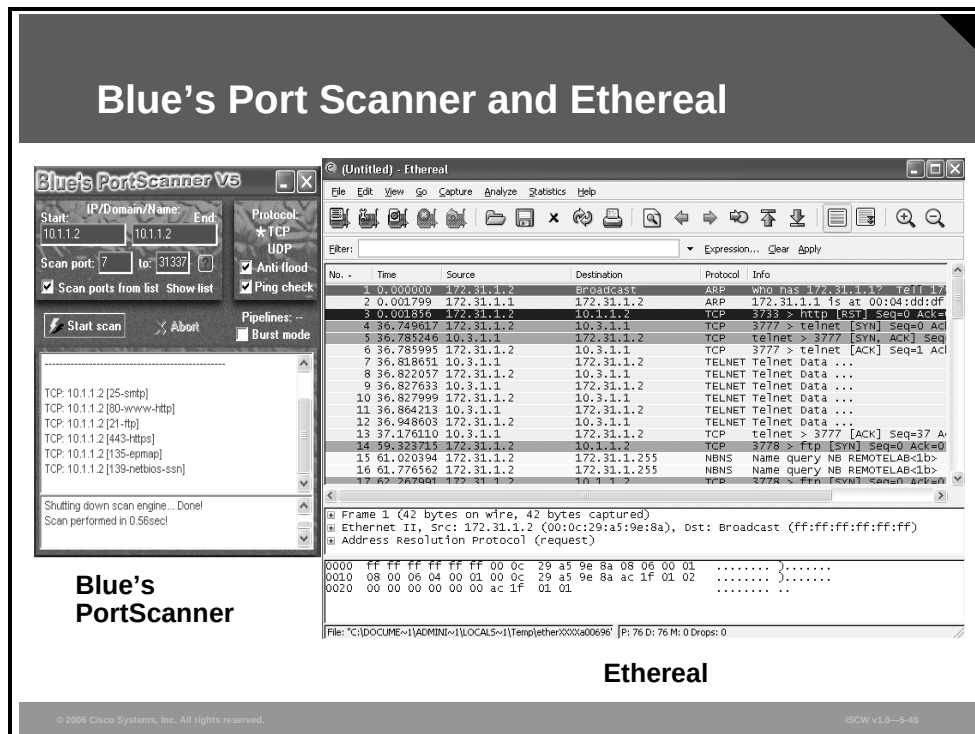
- The Blue's PortScanner scans 300 ports per second on a Windows computer.
- Ethereal is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education. Ethereal has all of the standard features you would expect in a protocol analyzer, and several features not seen in any other product. The Ethereal open source license allows talented experts in the networking community to add enhancements. Ethereal runs on all popular computing platforms, including UNIX, Linux, and Windows.
- Microsoft Baseline Security Analyzer (MBSA) is the free, best practices vulnerability assessment tool for the Microsoft platform. MBSA is a tool designed for the IT professional that helps with the assessment phase of an overall security management strategy. MBSA includes a graphic and command line interface that can perform local or remote scans of Windows systems.

- Nmap is a well-known low-level scanner available to the general public. It is simple to use, and has an array of excellent features which can be used for network mapping and reconnaissance. The basic functionality of nmap allows the user to do the following:
 - Perform classic TCP/UDP port scanning (looking for different services on one host) and sweeping (looking for the same service on multiple systems)
 - Stealth port scans and sweeps, which are hard to detect by the target host or intrusion detection systems
 - Identification of remote operating system (“operating system fingerprinting”) through its TCP idiosyncrasies. This technique analyzes the responses to different stimuli and identifies elements that are characteristic to a specific operating system or platform.

Advanced features of nmap include protocol scanning (Layer 3 port scanning), which can identify Layer 3 protocol support on a host (Generic Routing Encapsulation [GRE] support, Open Shortest Path First [OSPF] support), and so on.

Blue's Port Scanner and Ethereal

The figure on the left illustrates a TCP host scan and a resulting list of open TCP ports produced by Blue's PortScanner. Blue's PortScanner has been used to scan a single host with the address 10.1.1.2. The TCP scan shows that SMTP, HTTP, FTP, HTTPS, EPMAP, and NETBIOS-SSN are open on that host.

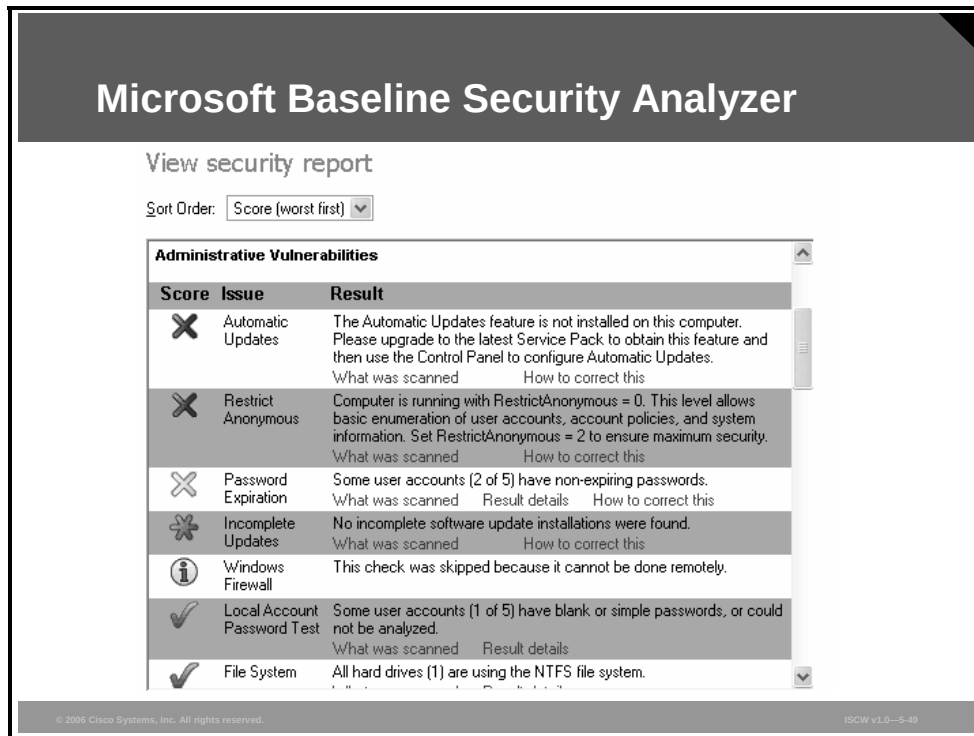


The image on the right shows a packet capture example using Ethereal. Ethereal allows you to specify various options, such as which adapter is used for sniffing and which packet filters to apply to the capture. In the figure, you see a number of packets of different protocols, each of which can be individually investigated in detail.

Caution Limit the scope of the testing so that you do not cause a DoS attack against your network.

Microsoft Baseline Security Analyzer

The figure illustrates the results of a host vulnerability scan using the Microsoft Baseline Security Analyzer.



Microsoft Baseline Security Analyzer is an easy-to-use tool for identifying security vulnerabilities of hosts running Microsoft operating systems. It allows you to scan the local host, on which MBSA itself is running, or any remote systems. The program provides a list of found vulnerabilities that can be sorted using different criteria. The tool provides a description of each detected vulnerability and recommends methods to fix them.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The Cisco Self-Defending Network initiative provides a comprehensive approach to network security.
- Packet sniffer attacks can be mitigated by cryptography, switched infrastructure, and antisniffer tools.
- Port scans and ping sweeps are mitigated by network and host IPS.
- Password attacks can be mitigated by strong password rules, disabling accounts after unsuccessful logins, and never sending passwords in plaintext.
- Trust exploitation and port redirection are defended against by a proper use of trust model.
- Man-in-the-middle attacks can be mitigated through cryptography.
- IP spoofing attacks can be defended against by access control, RFC 3704 filtering, and additional authentication.
- DoS and distributed DoS attacks can be mitigated through antispoof features, anti-DoS features and traffic rate limiting.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-50

Summary (Cont.)

- Worm attacks can be mitigated by containment, inoculation, quarantine, and treatment.
- Viruses and Trojan horse attacks can be defended against using up-to-date antivirus software.
- Application layer attacks can be mitigated by IPS, as well as operating system and application hardening.
- Management protocol attacks can be mitigated by selecting secure protocols and filtering the management traffic.
- The following tools help discover network vulnerabilities:
 - Netcat
 - Blue's PortScanner
 - Ethereal
 - Microsoft Baseline Security Analyzer
 - Nmap

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-51

Disabling Unused Cisco Router Network Services and Interfaces

Overview

This lesson describes the need to change certain Cisco router configuration settings, especially on border (perimeter) routers, to improve security. The lesson describes services that are enabled by default, or that are almost always enabled by users, but that may need to be disabled or reconfigured.

Consideration of these services is particularly important because some of the default settings in Cisco IOS software are there for historical reasons; they made sense when they were chosen, but would probably be different if new defaults were chosen today. Other defaults make sense for most systems, but may create security exposures if they are used in devices that form part of a network perimeter defense. Still other defaults are actually required by standards, but are not always desirable from a security point of view.

This lesson describes ways to secure networks by shutting off unnecessary network services and interfaces.

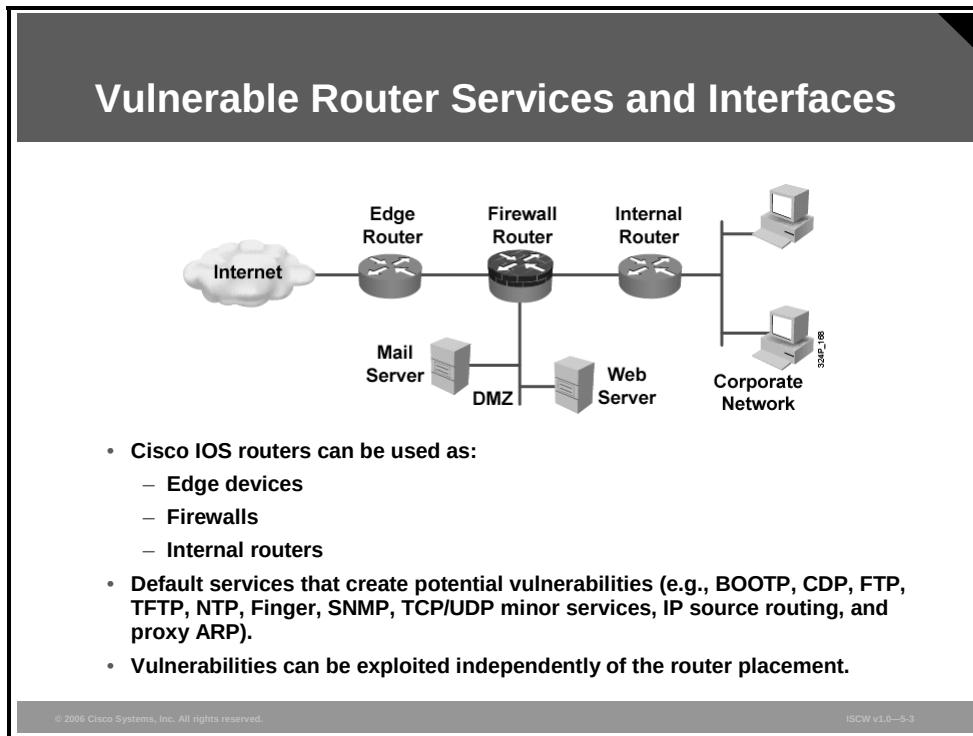
Objectives

Upon completing this lesson, you will be able to describe the techniques used to harden a Cisco device. This ability includes being able to meet these objectives:

- Identify router services and interfaces that are vulnerable to network attack
- Explain how the process of locking down a Cisco router can be automated with the **auto secure** command
- Explain how to configure AutoSecure on a Cisco router
- Compare the process of locking down a Cisco router with the CLI **auto secure** command and the One-Step Lockdown mode of the Security Audit wizard available in SDM

Vulnerable Router Services and Interfaces

This topic describes common vulnerabilities of Cisco IOS routers configured with default settings and provides methods to mitigate these vulnerabilities.



Medium-sized and large networks typically use a firewall appliance behind the perimeter router, which adds security features, and performs user authentication and more advanced packet filtering.

Firewall installations also facilitate the creation of Demilitarized Zones (DMZs) where hosts that are commonly accessed from the Internet are placed.

Cisco IOS software offers an alternative to a firewall appliance by incorporating many firewall features in the perimeter router itself. Although this option does not provide the same performance and security features that a Cisco PIX Security Appliance offers, a router with an integrated firewall feature set can solve most small-to-medium business perimeter security requirements.

Cisco IOS routers run many services that create potential vulnerabilities. To secure an enterprise network, you must disable all unneeded router services and interfaces.

Vulnerable Router Services

Cisco routers support many network services that may not be required in certain enterprise networks.

Vulnerable Router Services

- **Disable unnecessary services and interfaces (BOOTP, CDP, FTP, TFTP, NTP, PAD, and TCP/UDP minor services)**
- **Disable commonly configured management services (SNMP, HTTP, and DNS)**
- **Ensure path integrity (ICMP redirects and IP source routing)**
- **Disable probes and scans (finger, ICMP unreachable, and ICMP mask replies)**
- **Ensure terminal access security (ident and TCP keepalives)**
- **Disable gratuitous and proxy ARP**
- **Disable IP directed broadcast**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.4

The services listed in the figure have been chosen for their vulnerability to malicious exploitation. These are the router services most likely to be used in network attacks. For ease of learning, they have been grouped as follows:

- **Unnecessary services and interfaces:**
 - **Router interfaces:** Limit unauthorized access to the router and the network by disabling unused open router interfaces.
 - **BOOTP server:** This service is enabled by default. This service allows a router to act as a BOOTP server for other routers. This service is rarely required and should be disabled.
 - **Cisco Discovery Protocol (CDP):** This service is enabled by default. CDP is used primarily to obtain protocol addresses of neighboring Cisco devices and discover the platforms of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on most Cisco-manufactured equipment, including routers, bridges, access servers, switches, and IP phones. If not required, this service should be disabled globally or on a per-interface basis.
 - **Configuration auto-loading:** This service is disabled by default. Auto-loading of configuration files from a network server should remain disabled when not in use by the router.
 - **FTP server:** This service is disabled by default. The FTP server enables you to use your router as an FTP server for FTP client requests. Because it allows access to certain files in the router Flash memory, this service should be disabled when it is not required.

- **TFTP server:** This service is disabled by default. The TFTP server enables you to use your router as a TFTP server for TFTP clients. This service should be disabled when it is not in use because it allows access to certain files in the router Flash memory.
- **Network Time Protocol (NTP) service:** This service is disabled by default. When enabled, the router acts as a time server for other network devices. If configured insecurely, NTP can be used to corrupt the router clock and potentially the clock of other devices that learn time from the router. Correct time is essential for setting proper time stamps for IPsec encryption services, log data, and diagnostic and security alerts. If this service is used, restrict which devices have access to NTP. Disable this service when it is not required.
- **Packet assembler and disassembler (PAD) service:** This service is enabled by default. The PAD service allows access to X.25 PAD commands when forwarding X.25 packets. This service should be explicitly disabled when not in use.
- **TCP and User Datagram Protocol (UDP) minor services:** These services are enabled in Cisco IOS software releases prior to Cisco IOS software Release 11.3 and disabled in Cisco IOS software Release 11.3 and later. The minor services are provided by small servers (daemons) running in the router. They are potentially useful for diagnostics, but are rarely used. Disable these services.
- **Maintenance Operation Protocol (MOP) service:** This service is enabled on most Ethernet interfaces. MOP is a Digital Equipment Corporation (DEC) maintenance protocol that should be explicitly disabled when it is not in use.
- Commonly configured management services:
 - **Simple Network Management Protocol (SNMP):** This service is enabled by default. The SNMP service allows the router to respond to remote SNMP queries and configuration requests. If required, restrict which SNMP systems have access to the router SNMP agent and use SNMP version 3 whenever possible because this version offers secure communication not available in earlier versions of SNMP. Disable this service when it is not required.
 - **HTTP configuration and monitoring:** The default setting for this service is Cisco device dependent. This service allows the router to be monitored or have its configuration modified from a web browser via an application such as the Cisco Security Device Manager (SDM). You should disable this service if it is not required. If this service is required, restrict access to the router HTTP service using access control lists (ACLs).
 - **Domain Name System (DNS):** This client service is enabled by default. By default, Cisco routers broadcast name requests to 255.255.255.255. Restrict this service by disabling it when it is not required. If the DNS lookup service is required, make sure that you set the DNS server address explicitly.
- Path integrity mechanisms:
 - **ICMP redirects:** This service is enabled by default. ICMP redirects cause the router to send ICMP redirect messages whenever the router is forced to resend a packet through the same interface on which it was received. This information can be used by attackers to redirect packets to an untrusted device. This service should be disabled when not required.

- **IP source routing:** This service is enabled by default. The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that a datagram will take toward its ultimate destination, and generally the route that any reply will take. These options can be exploited by an attacker to bypass the intended routing path and security of the network. Also, some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending datagrams with source routing options. Disable this service when it is not required.
- Features related to probes and scans:
 - **Finger service:** This service is enabled by default. The finger protocol (port 79) allows users throughout the network to get a list of the users currently using a particular device. The information displayed includes the processes running on the system, the line number, connection name, idle time, and terminal location. This information is provided through the Cisco IOS software **show users EXEC** command. Unauthorized persons can use this information for reconnaissance attacks. Disable this service when it is not required.
 - **ICMP unreachable notifications:** This service is enabled by default. This service notifies senders of invalid destination IP networks or specific IP addresses. This information can be used to map networks and should be explicitly disabled on interfaces to untrusted networks.
 - **ICMP mask reply:** This service is disabled by default. When enabled, this service tells the router to respond to ICMP mask requests by sending ICMP mask reply messages containing the interface IP address mask. This information can be used to map the network, and this service should be explicitly disabled on interfaces to untrusted networks.
- Terminal access security:
 - **IP identification service:** This service is enabled by default. The identification protocol (specified in RFC 1413) reports the identity of a TCP connection initiator to the receiving host. This data can be used by an attacker to gather information about your network, and this service should be explicitly disabled.
 - **TCP keepalives:** This service is disabled by default. TCP keepalives help “clean up” TCP connections where a remote host has rebooted or otherwise stopped processing TCP traffic. Keepalives should be enabled globally to manage TCP connections and prevent certain DoS attacks.
- Gratuitous and proxy Address Resolution Protocol (ARP):
 - **Gratuitous ARP:** This service is enabled by default. Gratuitous ARP is the main mechanism used in ARP poisoning attacks. You should disable gratuitous ARPs on each router interface unless this service is otherwise needed.
 - **Proxy ARP:** This service is enabled by default. This feature configures the router to act as a proxy for Layer 2 address resolution. This service should be disabled unless the router is being used as a LAN bridge.
- **IP directed broadcast:** This service is enabled in Cisco IOS software releases prior to Cisco IOS software Release 12.0 and disabled in Cisco IOS software Release 12.0 or later. IP directed broadcasts are used in the common and popular smurf denial of service (DoS) attack and other related attacks. This service should be disabled when not required.

Router Hardening Considerations

Leaving unused network services running increases the possibility of malicious exploitation of those services. Turning off or restricting access to these services greatly improves network security. While it is not required that you explain why many of these services pose the vulnerabilities they do, you do need to know how and when they need to be disabled.

Router Hardening Considerations

- **Attackers can exploit unused router services and interfaces.**
- **Administrators do not need to know how to exploit the services, but they should know how to disable them.**
- **It is tedious to disable the services individually.**
- **An automated method is needed to speed up the hardening process.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-5

The manual process of disabling the services individually is lengthy and error-prone because you may overlook some services that are not needed and should be disabled. As a result, the manual disabling of services may leave the router vulnerable.

Locking Down Routers with AutoSecure

This topic describes the steps of the automated feature for hardening Cisco IOS routers called AutoSecure.

What is AutoSecure?

AutoSecure helps secure Cisco IOS networks by performing these router functions:

- Disables insecure global services
- Enables security-based global services
- Disables insecure interface services
- Enables appropriate security logging
- Secures router administrative access
- Secures the router management plane
- Secures the router forwarding plane

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-7

The AutoSecure feature is found in Cisco IOS software Release 12.3 and newer.

AutoSecure is a single privileged EXEC program that allows you to quickly and easily eliminate many potential security threats. AutoSecure helps to make you more efficient at securing Cisco routers.

AutoSecure Operation Modes

AutoSecure allows two modes of operation:

- **Interactive mode:** Prompts you to choose the way you want to configure router services and other security-related features
- **Noninteractive mode:** Configures security-related features on your router based on a set of Cisco defaults

AutoSecure Operation Modes

AutoSecure can be deployed using one of the following two modes of operation:

- **Interactive mode:** Prompts the user with options to enable and disable services and other security-related features
- **Noninteractive mode:** Automatically executes the auto secure command using recommended default settings

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5.0

Obviously, interactive mode provides for greater control over the router security-related features than noninteractive mode. However, when you want to quickly secure a router without much human intervention, the noninteractive mode becomes the better choice. You can enable noninteractive portions of the dialogue by selecting the optional **no-interact** keyword.

AutoSecure Functions

AutoSecure allows you to choose which router components to secure. You may want to secure the entire router functionality, or select individual planes or functions. The selectable components are the management plane, forwarding plane, firewall, login, NTP, and Secure Shell (SSH).

AutoSecure Functions

AutoSecure can selectively lock down:

- **Management plane services and functions:**
 - Finger, PAD, UDP & TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP (redirects, mask-replies), directed broadcast, MOP, banner
 - Also provides password security and SSH access
- **Forwarding plane services and functions:**
 - CEF, traffic filtering with ACLs
- **Firewall services and functions:**
 - Cisco IOS Firewall inspection for common protocols
- **Login functions:**
 - Password security
- **NTP protocol**
- **SSH access**
- **TCP Intercept services**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-5

The management plane includes management services, such as finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP (redirects, mask-replies), directed broadcast, MOP, and banner. It also includes the login functions, such as password security and failed login attempt actions, as well as SSH access.

The forwarding plane hardening consists of enabling Cisco Express Forwarding (CEF) and configuring ACLs for traffic filtering.

The firewall component allows you to activate the Cisco IOS Firewall inspection for common protocols and applications.

Login functions include password configuration, and setting options for failed login attempts.

NTP functionality sets up authenticated NTP connectivity.

The SSH feature configures a hostname and a domain-name if not configured already, and enables SSH access to the protected router. TCP Intercept function enables the TCP intercept feature with default settings.

The **full**, **ntp**, **login**, **ssh**, **firewall**, and **tcp-intercept** keywords were added in Cisco IOS software Release 12.3(4)T.

Using the **full** option, the user will be prompted for all interactive questions.

AutoSecure Failure Scenarios

When AutoSecure fails to complete its operation, your running configuration may be harmed.

AutoSecure Failure Scenarios

If AutoSecure fails to complete its operation, your running configuration may be corrupt:

- In 12.3(8)T and later releases
 - Pre-autosecure configuration snapshot is stored in the flash under filename *pre_autosec.cfg*
 - Roll-back reverts the router to its pre-autosecure configuration
 - Command: **configure replace flash:pre_autosec.cfg**
- Prior to 12.3(8)T, you should save the running configuration before running AutoSecure

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-10

You should consider these items to avoid a configuration loss:

- Cisco IOS software Release 12.3(8)T introduces support for rollback of the AutoSecure configuration. Rollback enables a router to revert back to its pre-autosecure configuration state if the AutoSecure configuration fails. Additionally, a pre-autosecure snapshot is saved into the router flash memory as *pre_autosec.cfg* before AutoSecure applies the configuration to the router. The administrator can use this saved snapshot to recover initial router settings.
- To replace the current running configuration with the configuration file that has been saved by AutoSecure, use the **configure replace** command in privileged EXEC mode.
- Prior to Cisco IOS Release 12.3(8)T, rollback of the AutoSecure configuration was unavailable; thus, you should always save the running configuration before configuring AutoSecure.

AutoSecure Process Overview

This topic explains how to configure AutoSecure on a Cisco router.

AutoSecure Process Overview

```
router#  
auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]
```

- Launches AutoSecure
- Main steps with the interactive full option:
 - Identify outside interfaces.
 - Secure the management plane.
 - Create security banner.
 - Configure passwords, AAA, and SSH.
 - Secure the interface settings.
 - Secure the forwarding plane.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-12

AutoSecure is initiated using the **auto secure** command in privileged EXEC mode.

auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]

AutoSecure uses this syntax to provide a level of granularity. To secure all components and functions, select the **full** option. To avoid configuration prompts, select the **no-interact** keyword. To limit the scope of hardening, use any of the remaining options, described in the table below.

auto secure Parameters

Parameter	Description
management	(Optional) Only the management plane will be secured.
forwarding	(Optional) Only the forwarding plane will be secured.
no-interact	(Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords.
full	(Optional) The user will be prompted for all interactive questions. This is the default.
ntp	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command-line interface (CLI).
login	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.

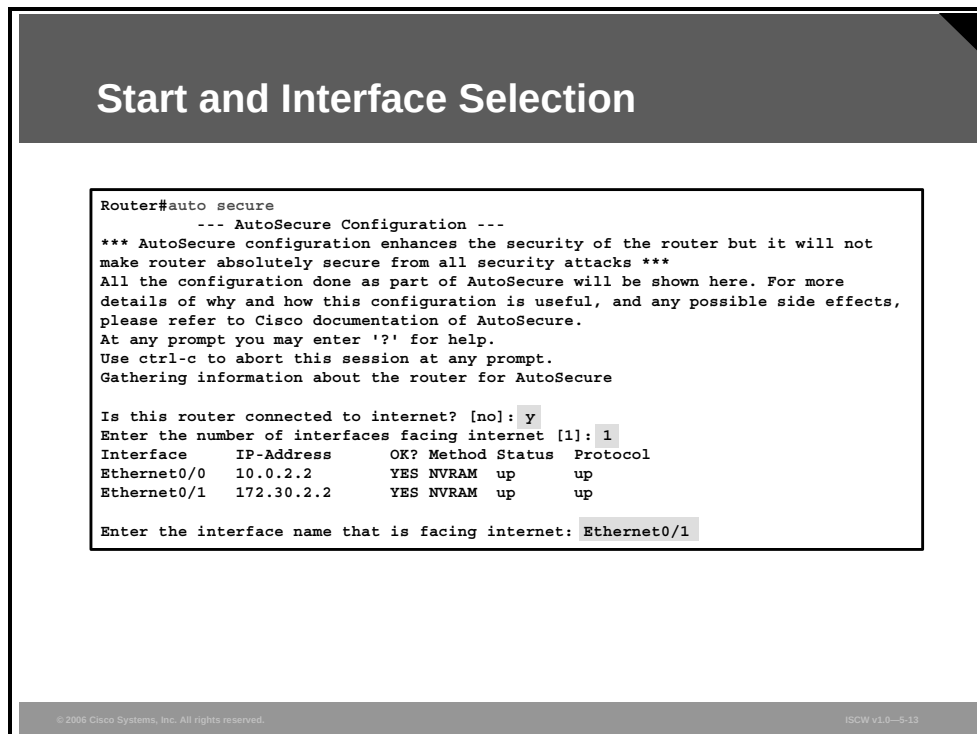
Parameter	Description
ssh	(Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI.
firewall	(Optional) Specifies the configuration of the firewall feature in the AutoSecure CLI.
tcp-intercept	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

AutoSecure configures all functions and services in the following order:

- Identify outside interfaces.
- Secure the management plane.
- Create a security banner.
- Configure passwords, authentication, authorization, and accounting (AAA), and SSH.
- Secure the interface settings.
- Secure the forwarding plane.

Start and Interface Selection

The first questions that AutoSecure asks you are directly related to how the router is connected to the Internet.



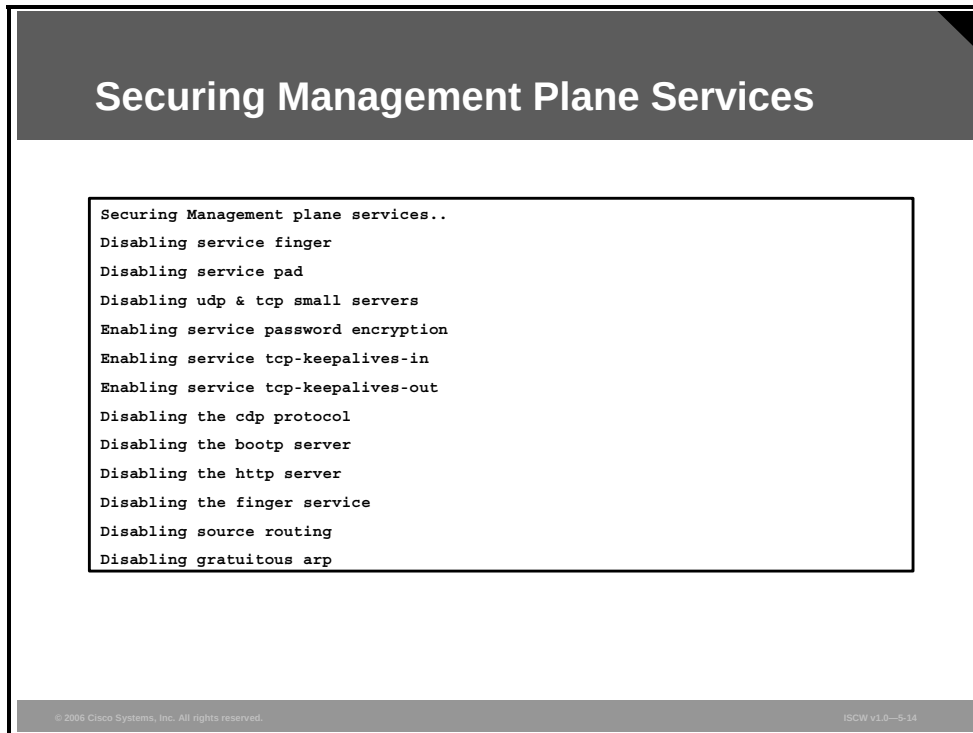
If you do not specify any options, as in the example, AutoSecure starts in the interactive mode and proceeds to secure the full scope of services and functions.

At the beginning, AutoSecure needs to know the following:

- Is the router going to be connected to the Internet?
- How many interfaces are connected to the Internet?
- What are the names of the interfaces connected to the Internet?

Securing Management Plane Services

Next, AutoSecure disables certain router global services.



These are the router global services that AutoSecure disables:

- **Finger:** Disabling this service keeps intruders from seeing who is logged in to the router and from where they are logged in.
- **PAD:** Disabling this service prevents intruders from accessing the X.25 PAD command set on the router.
- **Small servers:** Disabling the UDP and TCP small servers prevents attackers from using those services in DoS attacks.
- **CDP:** Disabling this service prevents attackers from exploiting any CDP security vulnerabilities. CDP is a Layer 2 mechanism used to obtain the data about the neighboring Cisco devices.
- **BOOTP:** Disabling this service prevents attackers from using it to generate DoS attacks.
- **HTTP:** Disabling this service prevents attackers from accessing the HTTP router administrative access interface.
- **Identification:** Disabling this service prevents attackers from querying TCP ports for identification.
- **NTP:** Disabling this service prevents attackers from corrupting router time bases.
- **Source routing:** Disabling this service prevents attackers from using source routing for malicious purposes.
- **Gratuitous ARPs:** Disabling gratuitous ARPs prevents the router from broadcasting the IP address of its interfaces.

Essentially, AutoSecure disables the most common attack vectors by shutting down their associated global router services. The global services listed in this figure have been designated as high-risk attack vectors.

AutoSecure enables the following router global services:

- **Service password encryption:** Automatically encrypts all passwords in the router configuration
- **TCP keepalives in/out:** Allows the router to quickly clean up idle TCP sessions

Creating Security Banner

Next, AutoSecure prompts you to create a banner to be shown every time someone accesses the router.

Creating Security Banner

Here is a sample Security Banner to be shown at every access to device. Modify it to suit your enterprise requirements.

Authorised Access only

This system is the property of So-&-So-Enterprise.

UNAUTHORISED ACCESS TO THIS DEVICE IS PROHIBITED.

You must have explicit permission to access this device. All activities performed on this device are logged and violations of of this policy result in disciplinary action.

Enter the security banner {Put the banner between k and k, where k is any character}:

%This system is the property of Cisco Systems, Inc.

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.%

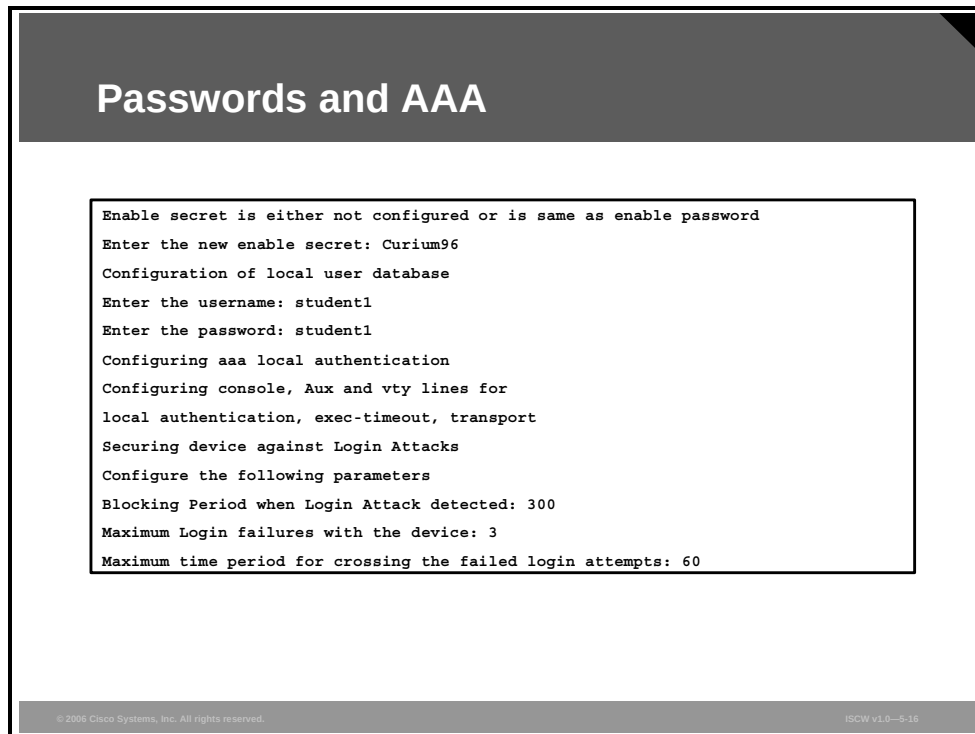
© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-15

This is the same as using the **banner** command in global configuration mode.

Passwords and AAA

Next, AutoSecure proceeds to the configuration of login functionality.



AutoSecure prompts you to configure the following:

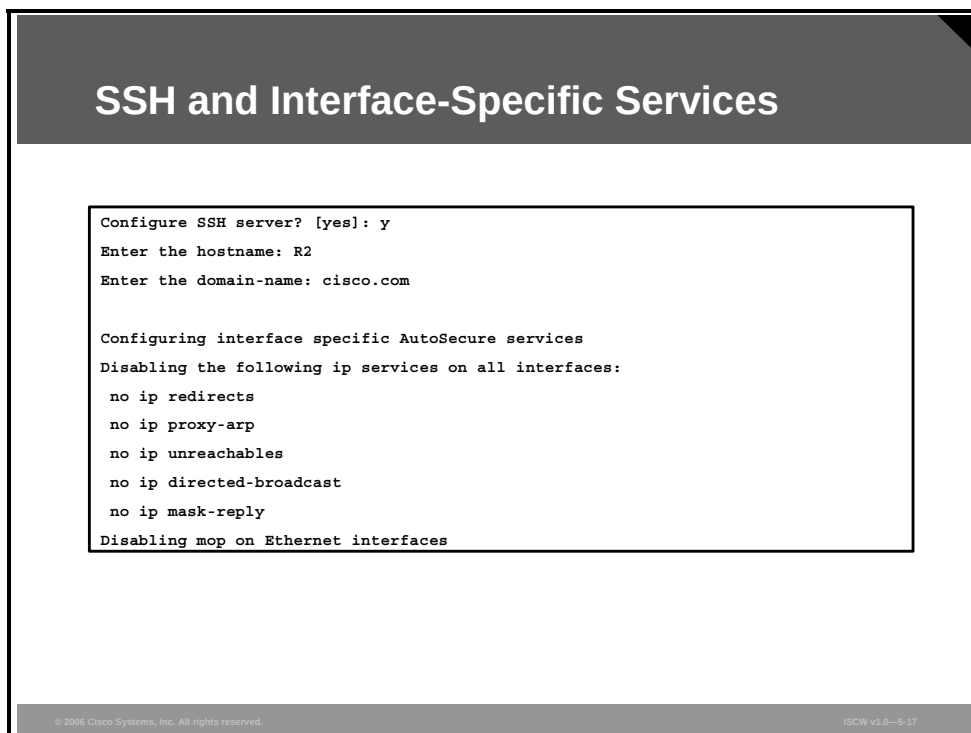
- **Enable secret:** AutoSecure checks to see if the router enable secret password is the same as the enable password or if it is not configured at all. If either is true, you are prompted to enter a new enable secret password.
- **AAA local authentication:** AutoSecure checks to see if AAA local authentication is enabled and if a local user account exists. If neither is true, you are prompted to enter a new username and password. Then, AAA local authentication is enabled. AutoSecure also configures the router console, aux, and VTY lines for local authentication, EXEC timeouts, and transport.

When securing the device against login attacks, you specify the following:

- Duration of time in which login attempts are denied (also known as a quiet period, in seconds).
- Maximum number of failed login attempts that triggers the quiet period.
- Duration of time in which the allowed number of failed login attempts must be made before the blocking period is triggered.

SSH and Interface-Specific Services

Next, AutoSecure proceeds to the SSH functionality and to interface-specific options.



AutoSecure asks whether you want to configure the SSH server. If you answer “yes,” AutoSecure will automatically configure the SSH timeout to 60 seconds and the number of SSH authentication retries to two:

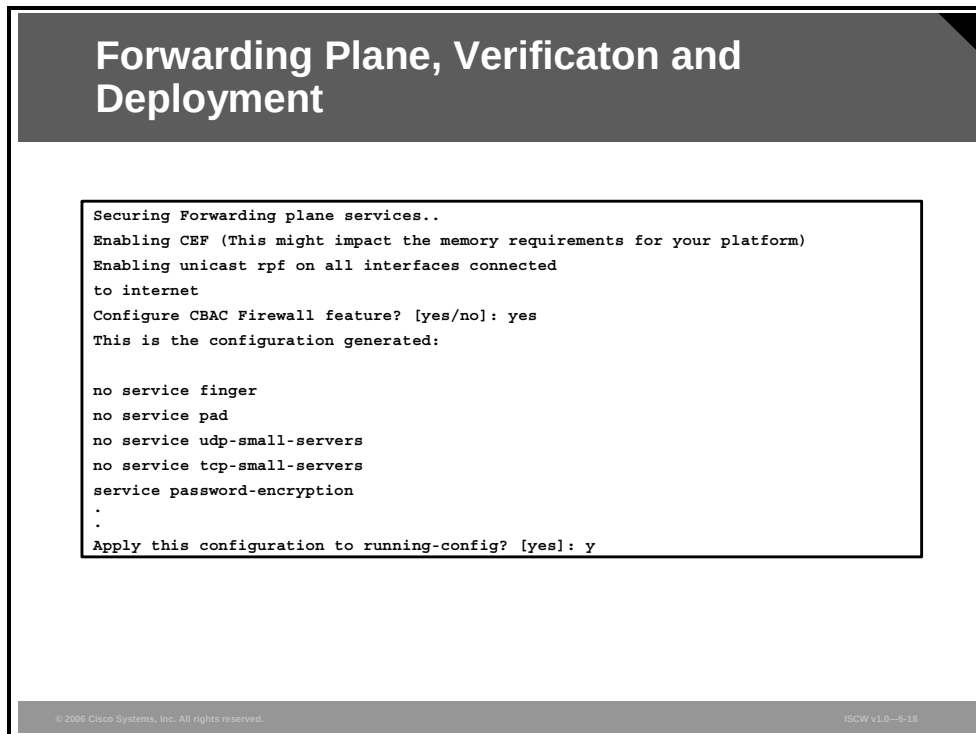
- **Hostname:** If you configured a hostname for this router prior to starting the AutoSecure procedure, you will not be prompted to enter one here. However, if the router is currently using the factory default hostname of **Router**, you will be prompted to enter a unique hostname as shown in the figure. This is important because SSH requires a unique hostname for key generation.
- **Domain name:** AutoSecure prompts you for the domain to which this router belongs. Like the hostname parameter, a domain name is important for SSH key generation.

Then, AutoSecure automatically disables the following services on all router interfaces:

- IP redirects
- IP proxy ARP
- IP unreachable
- IP directed-broadcast
- IP mask replies and disables MOP on Ethernet interfaces

Forwarding Plane, Verification, and Deployment

Next, AutoSecure secures the router forwarding plane.



AutoSecure secures the router forwarding plane by completing the following:

- **Enables Cisco Express Forwarding (CEF):** AutoSecure enables CEF (or distributed CEF) if the router platform supports this type of caching. Routers configured for CEF perform better under SYN flood attacks (directed at hosts, not the routers themselves) than routers configured using a standard cache.
- **Enables Unicast Reverse Path Forwarding (RPF) (only if the router supports this feature):** AutoSecure automatically configures strict Unicast RPF on all interfaces connected to the Internet. This helps drop any source-spoofed packets.

Note	Unicast RPF is an antispoof feature that scans the routing table information to detect and possibly block spoofed IP packets. When an incoming packet arrives on an interface, the router checks the routing entry for the source IP address of the packet. If the route points to the same interface, the packet is accepted. If the packet arrived on a different interface, it may have been spoofed, and is dropped.

- **Configures Context-Based Access Control (CBAC) Firewall feature:** AutoSecure asks if you want to enable generic CBAC inspection rules on all interfaces connected to the Internet. If you answer “yes,” a set of generic inspection rules is assigned to Internet-facing router interfaces.

Finally, AutoSecure displays the changes as they will be applied to the router running configuration. If you now wish to apply these changes, answer “Yes” to the “Apply this configuration to running-config?” question.

The table represents an example of how this portion of the AutoSecure dialogue appears.

AutoSecure Dialogue Example

The Commands that are Applied to the Router	Description
<pre>no service finger no service pad no service udp-small-servers no service tcp-small-servers service password-encryption service tcp-keepalives-in service tcp-keepalives-out no cdp run no ip bootp server no ip http server no ip finger no ip source-route no ip gratuitous-arps no ip identd</pre>	First, AutoSecure disables several router global services that are considered possible attack vectors and enables other global services that help protect the router and the network.
<pre>banner #This system is the property of Cisco Systems, Inc. UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.#</pre>	AutoSecure creates a banner to be displayed upon any access to the router. This banner message contains the text that you provided during the AutoSecure script.
<pre>security authentication failure rate 10 log</pre>	AutoSecure configures an authentication failure rate of ten. This allows a user ten failed login attempts before the router sends an authentication failure event to the logger (router log or syslog server). You are not prompted to specify this rate in the AutoSecure script. This is performed automatically by AutoSecure.
<pre>enable secret 5 \$1\$6NpI\$ClSvtL5Zs63fPpsQT5Dyq/ enable password 7 09674F04100916</pre>	Next , AutoSecure configures the enable secret and enable password that you specified during the AutoSecure script. Enable secret uses an MD-5 hashing mechanism (denoted by the number "5"). Enable password uses a weak encryption method denoted by the number "7".
<pre>aaa new-model aaa authentication login local_auth local line con 0 login authentication local_auth exec-timeout 5 0 transport output telnet line aux 0 login authentication local_auth exec-timeout 10 0 transport output telnet line vty 0 4 login authentication local_auth transport input telnet</pre>	AutoSecure enables local AAA authentication, and configures console line 0, auxiliary line 0, and vty lines 0 through 4 for local authentication, an EXEC session timeout, and outgoing Telnet connections.

The Commands that are Applied to the Router	Description
login block-for 5 attempts 3 within 4	AutoSecure configures login security.
hostname LosAngeles ip domain-name cisco.com crypto key generate rsa general-keys modulus 1024 ip ssh time-out 60 ip ssh authentication-retries 2 line vty 0 4 transport input ssh telnet	AutoSecure the hostname and domain-name. These values are mandatory for the subsequent key generation, which enables SSH access to the router. SSH optional settings are configured. AutoSecure configures VTY lines 0 through 4 to support both SSH and Telnet incoming connections. Note that Telnet was previously configured for the VTY lines. This step simply adds SSH to the list of possible incoming connection types.
service timestamps debug datetime msec localtime show-timezone service timestamps log datetime msec localtime show-timezone logging facility local2 logging trap debugging service sequence-numbers logging console critical logging buffered	AutoSecure configures logging parameters.
interface FastEthernet0/0 no ip redirects no ip proxy-arp no ip unreachableables no ip directed-broadcast no ip mask-reply no mop enabled interface Serial0/0 no ip redirects no ip proxy-arp no ip unreachableables no ip directed-broadcast no ip mask-reply interface FastEthernet0/1 no ip redirects no ip proxy-arp no ip unreachableables no ip directed-broadcast no ip mask-reply no mop enabled	Then, per-interface services are disabled.
ip cef	Next, AutoSecure proceeds with securing the forwarding plane. The first task is to enable Cisco Express Forwarding.
interface Serial0/0 ip access-group autosec_complete_bogon in	AutoSecure applies the configured ACL in the inbound direction to the

The Commands that are Applied to the Router	Description
<pre> exit access-list 100 permit udp any any eq bootpc interface Serial0/0 ip verify unicast source reachable-via rx allow-default 100 </pre>	outside interface and enables unicast RPF on that interface.
<pre> ip inspect audit-trail ip inspect dns-timeout 7 ip inspect tcp idle-time 14400 ip inspect udp idle-time 1800 ip inspect name autosec_inspect cuseeme timeout 3600 ip inspect name autosec_inspect ftp timeout 3600 ip inspect name autosec_inspect http timeout 3600 ip inspect name autosec_inspect rcmd timeout 3600 ip inspect name autosec_inspect realaudio timeout 3600 ip inspect name autosec_inspect smtp timeout 3600 ip inspect name autosec_inspect tftp timeout 30 ip inspect name autosec_inspect udp timeout 15 ip inspect name autosec_inspect tcp timeout 3600 ! end </pre>	Next, CBAC stateful firewall is turned on for common protocols and some CBAC settings configured.
<pre> ip access-list extended autosec_firewall_acl permit udp any any eq bootpc deny ip any any </pre>	AutoSecure configures an ACL that will be applied to the outside interface in outbound direction.
<pre> interface Serial0/0 ip inspect autosec_inspect out ip access-group autosec_firewall_acl in </pre>	The CBAC inspect list is applied to the outside interface in outbound direction. The outbound ACL is applied to the outside interface inbound direction.

Locking Down Routers with the SDM

This topic describes the steps of the automated AutoSecure feature.

Security Device Manager

SDM automated hardening features:

- Security Audit
- One-Step Lockdown

Cisco SDM is an intuitive, web-based device-management tool for Cisco IOS software-based routers. Cisco SDM simplifies router and security configuration through smart wizards, which help you to quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the CLI. Cisco SDM simplifies firewall and Cisco IOS software configuration without requiring expertise about security or Cisco IOS software.

Cisco SDM contains a Security Audit wizard that provides a comprehensive router security audit. Cisco SDM uses security configurations recommended by Cisco Technical Assistance Center (TAC) and International Computer Security Association (ICSA) as its basis for comparisons and default settings. The Security Audit wizard assesses the vulnerability of the existing router and provides quick compliance to best-practice security policies.

SDM can implement almost all of the configurations that AutoSecure offers with the One-Step Lockdown feature.

SDM Security Audit Overview

The Cisco SDM Security Audit feature compares router configurations to a predefined checklist of best practices using ICSA and Cisco TAC recommendations.

SDM Security Audit Overview

- The security audit compares router configuration against recommended settings.
- Examples of the audit include:
 - Shut down unneeded servers.
 - Disable unneeded services.
 - Apply the firewall to the outside interfaces.
 - Disable or harden SNMP.
 - Shut down unused interfaces.
 - Check password strength.
 - Enforce the use of ACLs.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-21

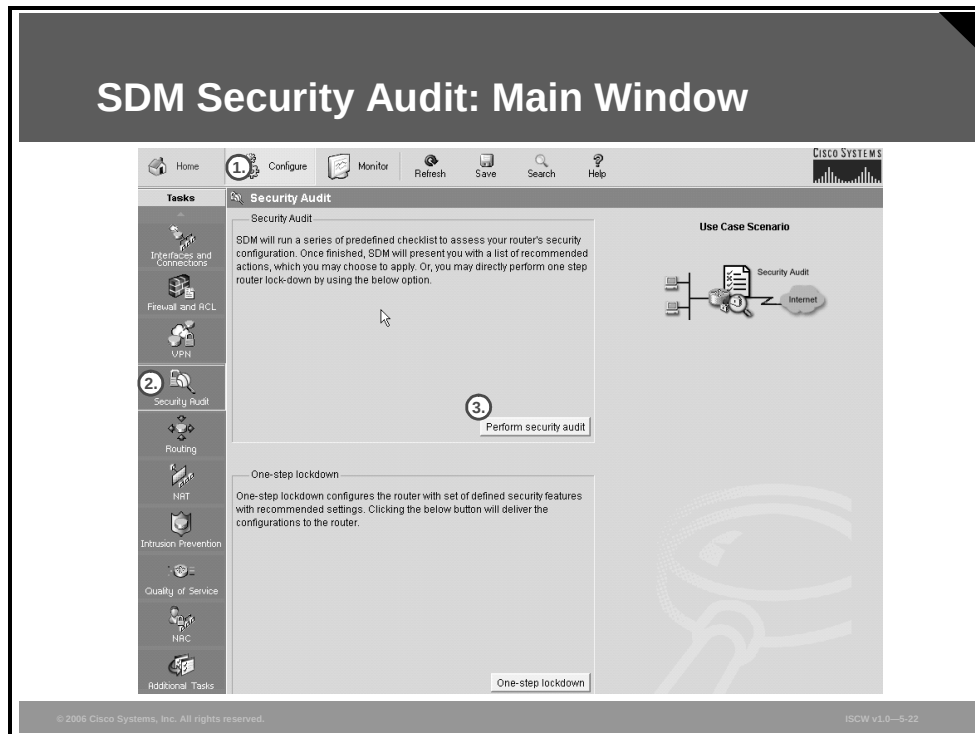
Examples of the audit include, but are not limited to, the following:

- Shuts down unneeded servers on the router (BOOTP, finger, TCP/UDP small servers)
- Shuts down unneeded services on the router (CDP, IP source-route, IP classless)
- Applies a firewall to the outside interfaces
- Disables SNMP, or enables it with hard-to-guess community strings
- Shuts down unused interfaces using the **no ip proxy-arp** command
- Forces passwords for the router console and vty lines
- Forces an enable secret password
- Enforces the use of ACLs

SDM Security Audit: Main Window

The Security Audit wizard contains two modes:

- **Security Audit:** Examines router configuration, then displays the Report Card window, which shows a list of possible security problems. You can choose which vulnerability you would like to lock down.
- **One-Step Lockdown:** Initiates the automatic lockdown using recommended settings.

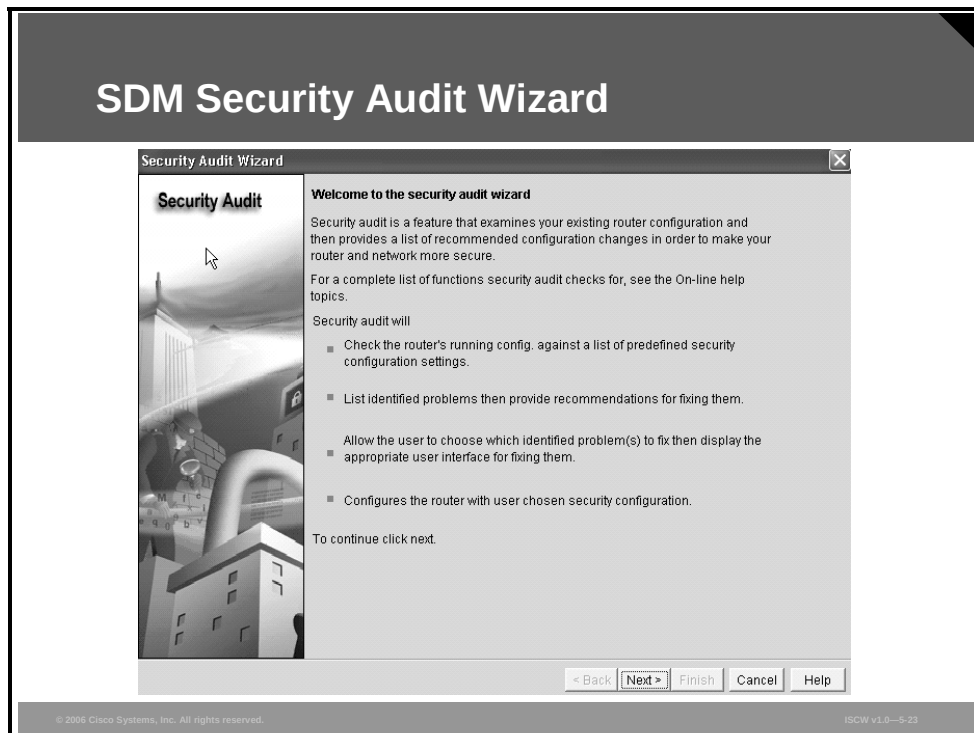


Complete the following steps to perform a security audit:

- Step 1** Click the **Configure** icon in the main toolbar at the top.
- Step 2** Click the **Security Audit** icon in the Tasks toolbar on the left.
- Step 3** You have two wizard buttons available; click the **Perform security audit** button.

SDM Security Audit Wizard

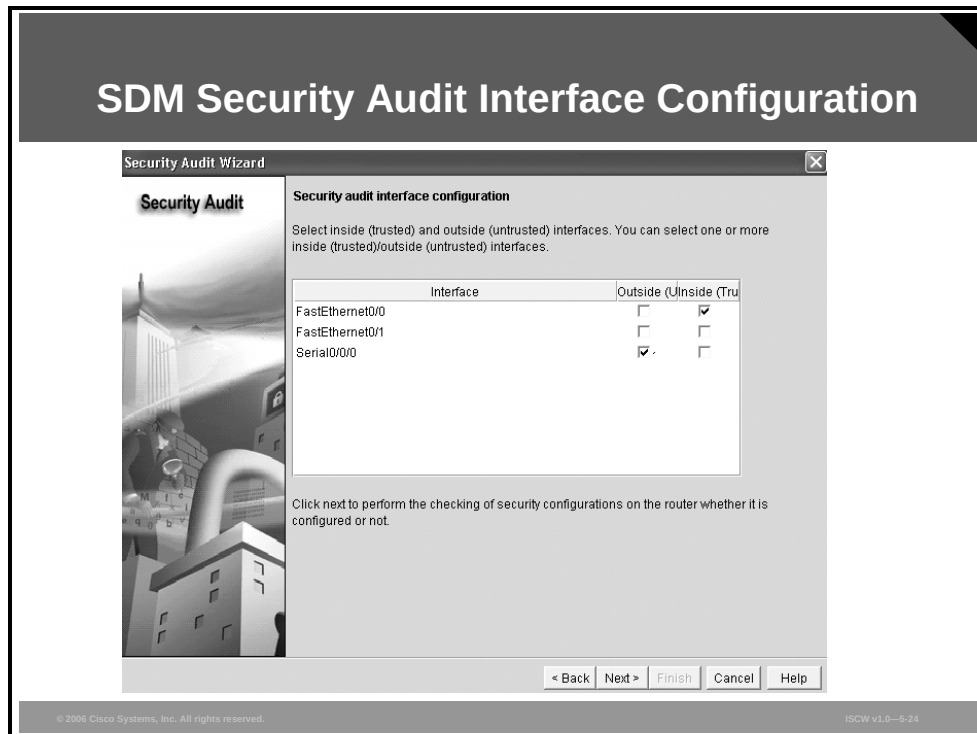
The Security Audit window opens after clicking **Perform security audit**.



A welcome page opens describing the functions performed by the security audit wizard. Click the **Next** button to proceed to the next step.

SDM Security Audit Interface Configuration

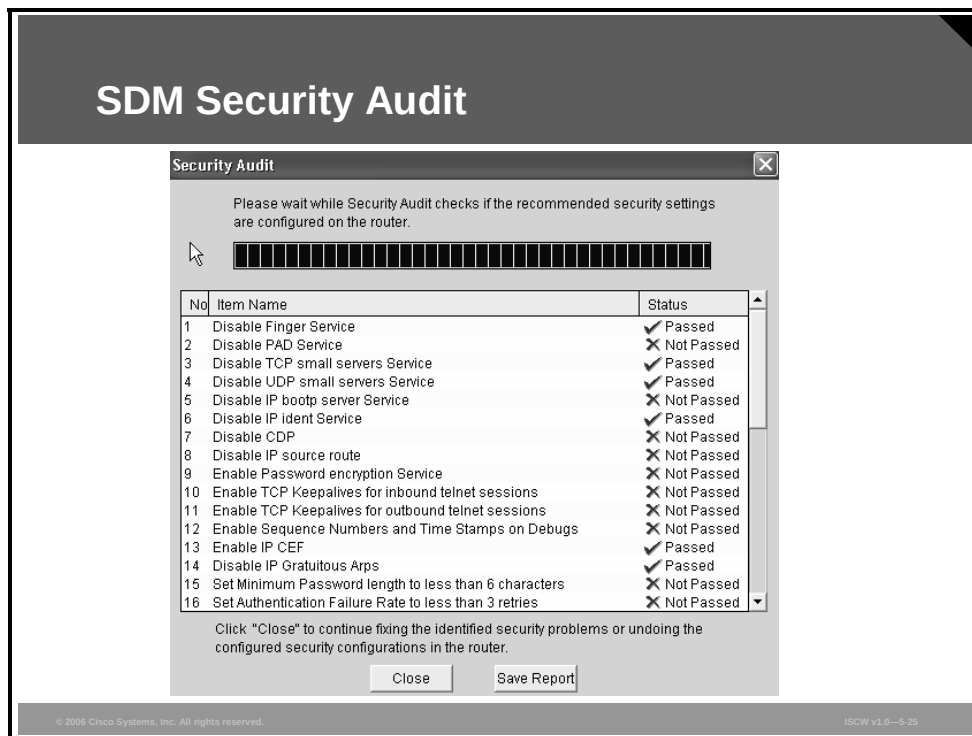
The Security Audit Interface Configuration window opens after clicking **Next**.



In this step, select the inside and outside interfaces. Then, click the **Next** button to proceed to the next step.

SDM Security Audit

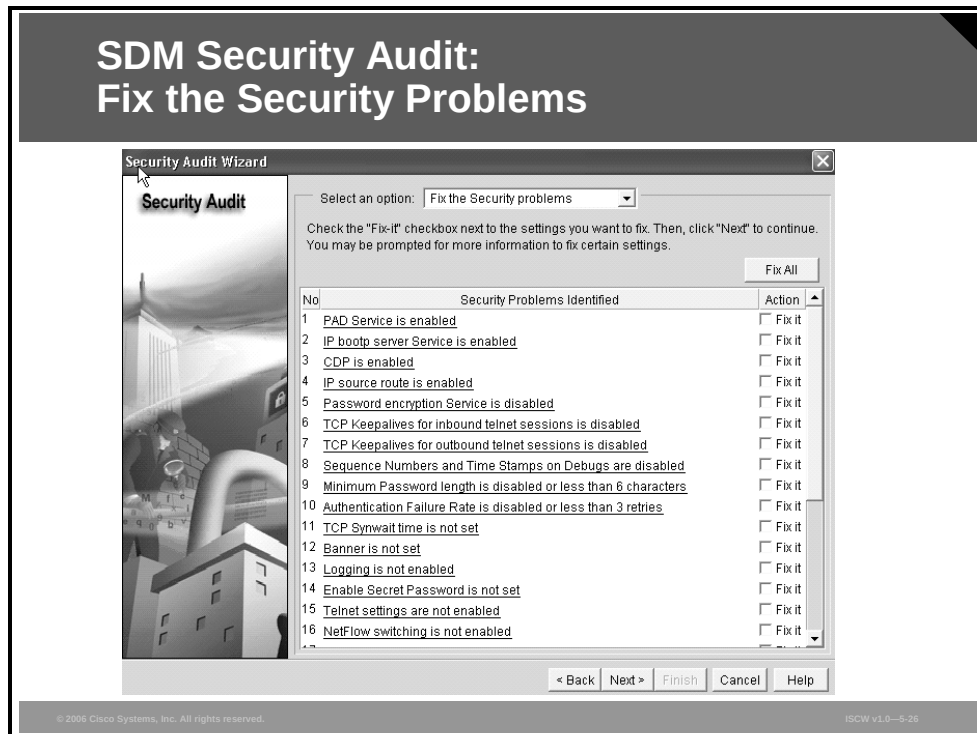
The Security Audit wizard tests your router configuration to determine whether any security vulnerabilities exist and presents the report. Vulnerable items are marked with a red X.



After viewing the report, you have the option of saving it as a file. Click the **Close** button to close the window and proceed to the next step.

SDM Security Audit: Fix the Security Problems

Next, a window appears listing the identified problems.

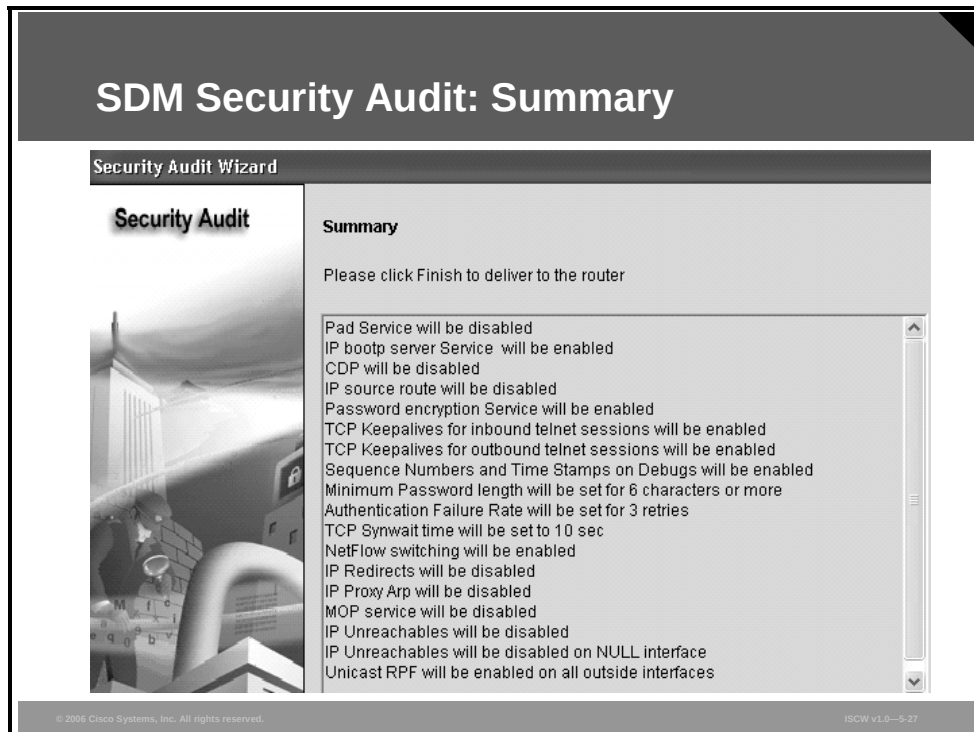


Check the **Fix It** check boxes next to any problems that you want Cisco SDM to fix, and click the **Next** button. Additional windows may appear requiring your input, such as entering a password. Pay special attention to any warning messages that appear. Make sure that you do not “fix” a potential security breach and lock yourself out of the router.

Note For a description of the problem and a list of the Cisco IOS commands that will be added to your configuration, click the problem description hyperlinks. A Help page describing the selected problem will open.

SDM Security Audit: Summary

Next, the SDM Security Audit Summary window appears.

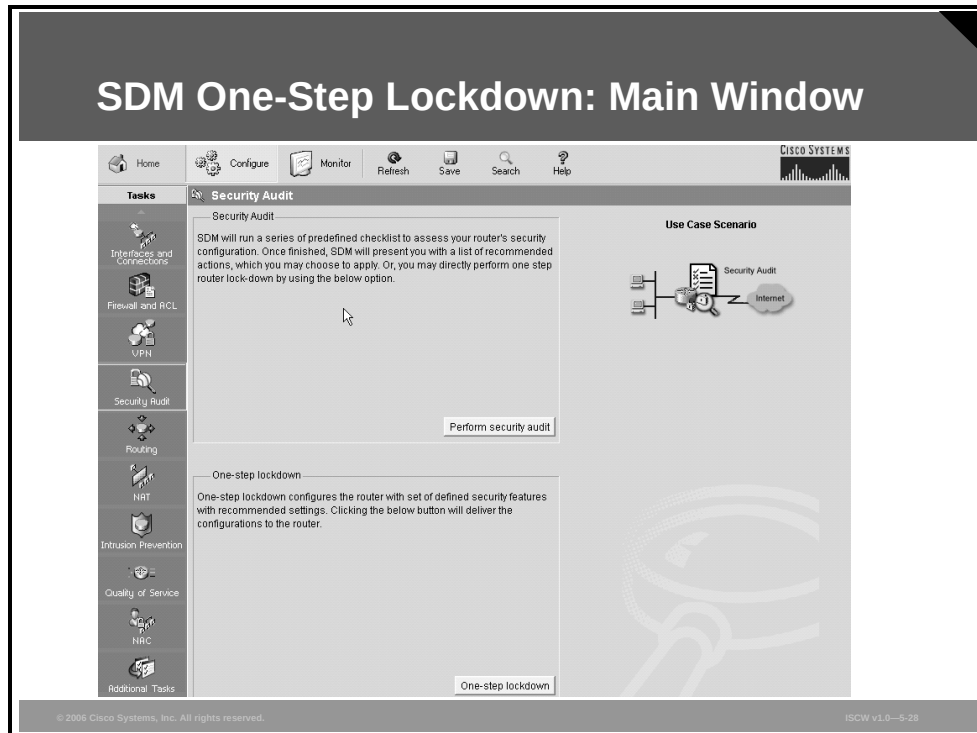


In the example, a number of security features will be enabled on the router.

Review the changes and click **Finish** to send the changes to the router.

SDM One-Step Lockdown: Main Window

Cisco SDM provides an easy one-step router lockdown for many security features. The wizard button is available in the **Security Audit** task under the **Configure** tab.



Click the **One-step lockdown** button to launch the One-Step Lockdown wizard.

SDM One-Step Lockdown Wizard

Cisco SDM provides an easy one-step router lockdown for many security features.



This option tests the router configuration for any potential security problems and automatically makes any necessary configuration changes to correct the problems found.

The conditions tested and, if needed, corrected are as follows:

- Disable Finger Service
- Disable PAD Service
- Disable TCP Small Servers Service
- Disable UDP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route
- Enable Password Encryption Service
- Enable TCP Keepalives for Inbound Telnet Sessions
- Enable TCP Keepalives for Outbound Telnet Sessions
- Enable Sequence Numbers and Time Stamps on Debugs
- Enable IP CEF
- Disable IP Gratuitous ARPs
- Set Minimum Password Length to Less Than Six Characters
- Set Authentication Failure Rate to Less Than Three Retries

- Set TCP SYN Wait Time
- Set Banner
- Enable Logging
- Set Enable Secret Password
- Disable SNMP
- Set Scheduler Interval
- Set Scheduler Allocate
- Set Users
- Enable Telnet Settings
- Enable NetFlow Switching
- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service
- Disable IP Unreachables
- Disable IP Mask Reply
- Disable IP Unreachables on NULL Interface
- Enable Unicast RPF on Outside Interfaces
- Enable Firewall on All of the Outside Interfaces
- Set Access Class on HTTP Server Service
- Set Access Class on VTY Lines
- Enable SSH for Access to the Router

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Unused router services and interfaces should be disabled.
- AutoSecure is a very efficient tool for securing Cisco routers.
- AutoSecure runs in an interactive and noninteractive mode.
- AutoSecure can selectively lock down the management or the forwarding plane, or other router functions such as login, firewall, SSH, NTP, and TCP Intercept.
- AutoSecure provides rollback functionality.
- Cisco SDM includes a Security Audit wizard that allows you to analyze the router configuration and selectively fix the security issues.
- Cisco SDM provides a One-Step Lockdown feature that tests the router configuration for any potential security problems and automatically makes the necessary corrections.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-30

Lesson 3

Securing Cisco Router Installations and Administrative Access

Overview

This lesson describes how to secure Cisco routers by protecting the router administrative interface. The lesson explains password security features, such as enforcing a minimum password length, specifying the login failure rate, and setting timeouts in case of repeated failed login attempts that may accompany a password attack. Privilege levels and command-line interface (CLI) views offer mechanisms to grant different types of administrative access to various users or administrators. Also, this lesson describes banner configuration and the Cisco IOS Configuration Resilience feature, which speeds up router recovery in case of compromise by securing the image and the configuration files against compromise.

Objectives

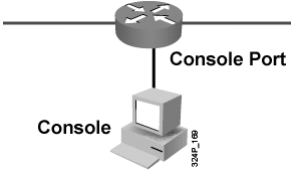
Upon completing this lesson, you will be able to secure Cisco router physical installations and administrative access using passwords. This ability includes being able to meet these objectives:

- Describe how to configure secure administrative access to Cisco routers by configuring passwords
- Describe how to secure administrative access to Cisco routers by setting a login failure rate and using IOS login enhancements
- Describe how to secure administrative access to Cisco routers by setting timeouts
- Describe how to secure administrative access to Cisco routers by setting multiple privilege levels
- Describe how to secure administrative access to Cisco routers by configuring banner messages
- Explain role-based CLI and the commands required to configure basic CLI views
- Explain how to secure Cisco IOS boot image and configuration files

Configuring Router Passwords

This topic describes how to configure secure administrative access to Cisco routers by configuring passwords.

Configuring Router Passwords



- **A console is a terminal connected to a router console port.**
- **The terminal can be a dumb terminal or a PC with terminal emulation software.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5.3

Strong passwords are the primary defense against unauthorized access to your router. The best way to manage passwords is to maintain them on an authentication, authorization, and accounting (AAA) server. Almost every router needs a locally configured password for privileged access, and may also have other password information in its configuration file.

One way to perform initial router configuration tasks is to access the router console port. Consoles are only one of the ways to obtain administrative access to configure and manage routers. Other ways to gain administrative access include:

- Telnet
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- Cisco Security Device Manager (SDM) access using HTTP or HTTPS

Password Creation Rules

This section describes the best practices in password security.

Password Creation Rules

- Passwords can be 1 to 25 characters in length.
- Passwords can include:
 - Alphanumeric characters
 - Uppercase and lowercase characters
 - Symbols and spaces
- Passwords cannot have a number as the first character.
- Password-leading spaces are ignored, but any spaces after the first character are not ignored.
- Change passwords.

© 2006 Cisco Systems, Inc. All rights reserved.

ISOW v1.0—5-4

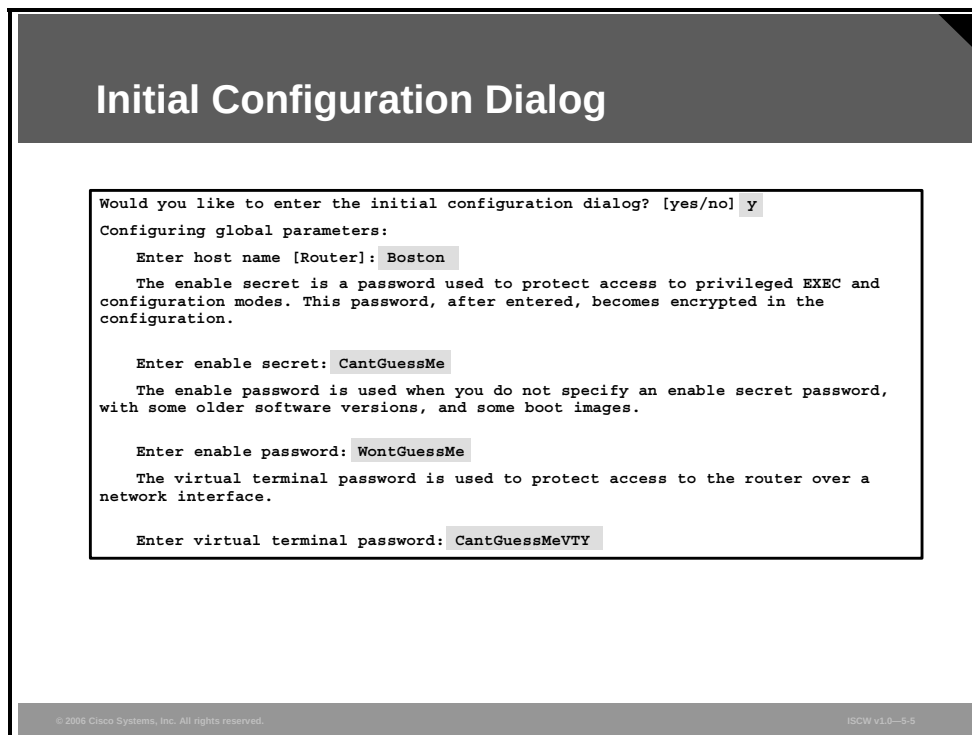
When creating passwords for Cisco routers, always keep these rules in mind:

- The best practice is to have a minimum of ten characters. You can enforce the minimum length using a feature available on Cisco IOS routers, discussed later in this topic. Passwords may include the following:
 - Any alphanumeric character
 - A mix of uppercase and lowercase characters
 - Symbols and spaces
- Passwords should not use dictionary words. Using dictionary words makes the passwords vulnerable to dictionary attacks.
- Password-leading spaces are ignored, but all spaces after the first character are not ignored.
- You should have a policy defining when and how often the passwords should be changed. Changing passwords frequently provides two advantages: It limits the window of opportunity in which a hacker can crack a password, and it limits the window of exposure after a password has been compromised.

You may want to add your own rules to this list, making your passwords even safer.

Initial Configuration Dialog

If you are working on a new router or an existing router that has been reset (possibly using the Cisco password recovery procedure), you are prompted by the Cisco IOS CLI if you want to enter the initial configuration dialog. The figure shows a router configuration sample with this initial prompt.



The first few questions in the initial configuration dialog pertain to these password requirements:

- The router enable secret password
- The router enable password
- The password used to access the router using virtual terminal lines

The enable secret password is used to enter enable mode (sometimes referred to as privileged mode or privileged-EXEC mode). You can set the enable secret password by entering a password during the initial configuration dialog, as shown in the figure, or by using the **enable secret** command in global configuration mode. The enable secret overrides the enable password configured with the **enable password** command. In other words, when enable secret is configured on a router, you cannot access the privileged mode using the password configured with **enable password** command. The **enable secret** command uses a one-way encryption hash based on Message Digest 5 (MD5) and is considered irreversible by most cryptographers. However, even this type of encryption is still vulnerable to brute force or dictionary attacks. If you forget the enable secret password, you have no alternative but to replace it using the Cisco router password recovery procedure.

The **enable password** command is also used to enter enable mode, but is a holdover from older versions of Cisco IOS software. By default, the enable password is not encrypted in the router configuration. Cisco decided to keep the older **enable password** command in later versions of Cisco IOS software even though enable secret password is a safer way to store privileged-EXEC passwords. The older command was kept in case the router is downgraded to a version of Cisco IOS software that did not support enable secret password. The enable password protects the privileged-EXEC mode.

The virtual terminal password is the line-level password entered when connecting to the router using Telnet or SSH. You can set this password during the initial configuration dialog or by using the **password** command in vty line configuration mode. The virtual terminal password is not encrypted.

Configure the Line-Level Password

To secure the router, you should protect the access through the console, auxiliary, and vty lines.

Configure the Line-Level Password

```
router(config)#  
line console 0  
line aux 0  
line vty 0 4
```

- Enters line configuration mode (console, auxiliary, or vty)

```
router(config-line)#  
login
```

- Enables password checking at login

```
router(config-line)#  
password password
```

- Sets the line-level password

```
Boston(config)#line con 0  
Boston(config-line)#login  
Boston(config-line)#password ConUser1
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5-6

Console Port

By default, the Cisco router console ports allow a hard BREAK signal (within 60 seconds of a reboot) to interrupt the normal boot sequence and give the console user complete control of the router. This is used for maintenance purposes, such as when running the Cisco router password recovery procedure. Even though this hard BREAK sequence is, by default, available to someone who has physical access to the router console port, it is still important to set a line-level password for users who might try to gain console access remotely. The hard BREAK sequence may be disabled using the **no service password-recovery** command.

Note If a router is configured with the **no service password-recovery** command, all access to the ROM Monitor (ROMMON) is disabled.

By default, the console port does not require a password for console administrative access. However, you should always configure a console port line-level password. There are two ways to configure a console line password: You can enter the password during the initial configuration dialog, or you can use the **password** command in the console line configuration mode.

VTY Lines

Cisco routers support multiple Telnet sessions (up to five simultaneous sessions, by default—more can be added), each serviced by a logical vty. By default, Cisco routers do not have any line-level passwords configured for these vty.

If you enable password checking, you must also configure a vty password before attempting to access the router using Telnet. If you fail to configure a vty password, and password checking is enabled for vty, you will encounter an error message similar to the following:

```
Telnet 10.0.1.2
Trying 10.0.1.2 .... open

Password required, but none set

[Connection to 10.0.1.2 closed by foreign host]
```

There are two ways to configure a vty password: You can enter the password during the initial configuration dialog, or you can use the **password** command in line vty configuration mode.

The following are a few more things to consider when securing Telnet connections to a Cisco router:

- If you fail to set an enable password for the router, you will not be able to access privileged-EXEC mode using Telnet. Use either the **enable password** or **enable secret password** command to set the enable password for your routers.
- Telnet access should be limited only to specified systems by building a simple access control list (ACL) that does the following:
 - Allows Telnet access from specific hosts only
 - Implicitly or explicitly blocks access from untrusted hosts
 - Ties the ACL to the vty lines using the **access-class** command
 - This example shows ACL 30 restricting Telnet access only from host 10.0.1.1 and implicitly denying access from all other hosts for vty 0 to 4:

```
Boston(config)#access-list 30 permit 10.0.1.1 0.0.0.0
Boston(config)#line vty 0 4
Boston(config-line)#access-class 30 in
```
- You must configure passwords for all of the vty lines on the router. Remember that you can add more vty lines to the router and these lines must be protected as well as the default 0 to 4 lines.

Auxiliary Lines

By default, Cisco router auxiliary ports do not require a password for remote administrative access. Administrators sometimes use auxiliary ports to remotely configure and monitor the router using a dialup modem connection.

Unlike console and vty passwords, the auxiliary password is not configured during the initial configuration dialog and should be configured using the **password** command in auxiliary line configuration mode.

If you wish to turn off the EXEC process for the aux port, use the **no exec** command within the auxiliary line configuration mode.

Setting the auxiliary line-level password is only one of several steps you must complete when configuring a router auxiliary port for remote dial-in access. The table explains commands used when configuring an auxiliary port.

Commands to Configure an Auxiliary Port

Command	Explanation
Boston(config)#line aux 0 Boston(config-line)#modem inout	Permits incoming and outgoing modem calls on this line
Boston(config-line)#speed 9600	Sets the line speed that should be used to communicate with the modem
Boston(config-line)#transport input all	Allows all protocols to use the line
Boston(config-line)#flowcontrol hardware	Enables Ready to Send (RTS) and Clear to Send (CTS) flow control
Boston(config-line)#login	Authenticates incoming connections using the password configured on the line
Boston(config-line)#password NeverGuessMeAux	Configures the password NeverGuessMeAux to authenticate incoming calls on this line

Password Minimum Length Enforcement

Cisco IOS software Release 12.3(1) and later allows you to set the minimum character length for all router passwords using the **security passwords min-length** global configuration command. This command provides enhanced security access to the router by allowing you to specify a minimum password length (0 to 16), which eliminates common passwords that are prevalent on most networks, such as *lab* and *cisco*. This command affects user passwords, enable passwords and secrets, and line passwords created after the command was executed. Existing router passwords remain unaffected.

Password Minimum Length Enforcement

```
router(config)#  
security passwords min-length length
```

- Sets the minimum length of all Cisco IOS passwords

```
Boston(config)#security passwords min-length 10
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.7

It is highly recommended that you set your minimum password length to at least 10 characters.

After this command is enabled, any attempt to create a new password that is less than the specified length fails and results in an error message similar to the following:

```
Password too short - must be at least 10 characters. Password  
configuration failed.
```

Encrypting Passwords

Just like console and vty passwords, auxiliary passwords are not encrypted in the router configuration. This is why it is important to use the **service password-encryption** command.

Encrypting Passwords Using the service password-encryption Command

```
router(config)#  
service password-encryption
```

- Encrypts all passwords in the router configuration file

```
Boston(config)#service password-encryption  
Boston(config)#exit  
Boston#show running-config  
enable password 7 06020026144A061E  
!  
line con 0  
password 7 0956F57A109A  
!  
line vty 0 4  
password 7 034A18F366A0  
!  
line aux 0  
password 7 7A4F5192306A
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6.6

With the exception of the enable secret password, all Cisco router passwords are, by default, stored in plaintext form within the router configuration. View these passwords with the **show running-config** command. Sniffers can also see these passwords if your TFTP server configuration files traverse an unsecured intranet or Internet connection. If an intruder gains access to the TFTP server where the router configuration files are stored, the intruder will be able to obtain these passwords.

A proprietary Cisco algorithm based on a Vigenere cipher (indicated by the number 7 when viewing the configuration) allows the **service password-encryption** command to encrypt all passwords (except the previously encrypted enable secret password) in the router configuration file. This method is not as safe as MD5, which is used with the **enable secret** command, but prevents casual discovery of the router line-level passwords.

Note The encryption algorithm in the **service password-encryption** command is considered relatively weak by most cryptographers and several Internet sites post mechanisms for cracking this cipher. This posting only proves that relying on the encrypted passwords alone is not sufficient security for your Cisco routers. You need to ensure that the communications link between the console and the routers, or between the TFTP or management server and the routers, is a secured connection.

After all of your passwords are configured for the router, you should run the **service password-encryption** command in global configuration mode, as shown in the figure.

When you remove the **service password-encryption** command with the **no** form, this does not decrypt the passwords.

Enhanced Username Password Security

You can choose to use an MD5 hashing mechanism to encrypt username passwords.

Enhanced Username Password Security

```
router(config)#  
username name password {[0] password | 7 hidden-password}
```

- Traditional user configuration with plaintext password

```
router(config)#  
username name secret {[0] password | 5 encrypted-secret}
```

- Uses MD5 hashing for strong password protection
- Better than the type 7 encryption found in service password-encryption command

```
Boston(config)#username rtradmin secret 0 Curium96  
Boston(config)#username rtradmin secret 5 $l$feb0$a104Qd9UZ./Ak007
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.9

Cisco routers can maintain a list of usernames and passwords for performing local login authentication. Traditionally, local users were defined with the **username password** command, which was used to configure users and plaintext passwords. These passwords could then be obfuscated by the password-encryption service, which employed the weak Vigenere cipher that defended against reading the passwords but did not provide adequate protection from hackers.

Option 7 in the **username password** command allowed you to enter the ciphertext of a password, computed by the Vigenere algorithm. This option was used in recovery scenarios in which a previous configuration, using password-encryption service, needed to be reinstalled and only obfuscated passwords were available in the backup configuration.

Enhanced username password security uses the **username secret** command and employs MD5 password hashing. It is a much stronger encryption scheme than the standard type 7 encryption found in the **service password-encryption** command. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Using the **username secret** command in global configuration mode, you can choose to enter a plaintext password for MD5 hashing by the router (option 0), or enter a previously encrypted MD5 secret (option 5).

username name secret {[0] password | 5 encrypted-secret}

username secret Parameters

Parameter	Description
<i>name</i>	The username

Parameter	Description
0	(Optional) Indicates that the following clear text password is to be hashed using MD5
<i>password</i>	The plaintext password to be hashed using MD5
5	Indicates that the following encrypted secret password was hashed using MD5
<i>encrypted-secret</i>	The MD5 encrypted secret password that will be stored as the encrypted user password
Note MD5 encryption is a strong encryption method that is not retrievable; therefore, you cannot use MD5 encryption with protocols that require plaintext passwords, such as Challenge Handshake Authentication Protocol (CHAP).	

Securing ROMMON

By default, Cisco IOS routers allow a break sequence during power up, which forces the router into ROM Monitor (ROMMON) mode. Once the router is in ROMMON mode, anyone can choose to enter a new enable secret password using the well-known Cisco password recovery procedure. This procedure, if performed correctly, leaves the router configuration intact. This scenario presents a potential security breach because anyone who gains physical access to the router console port can enter ROMMON, reset the enable secret password, and discover the router configuration.

Securing ROMMON with the no password-recovery Command

```
router(config)#
```

```
no service password-recovery
```

- **By default, Cisco routers are factory configured with the service password-recovery set.**
- **The no service password-recovery command prevents console from accessing ROMMON.**

```
Boston(config)#no service password-recovery
```

```
WARNING:
```

```
Executing this command will disable password recovery mechanism. Do not  
execute this command without another plan for password recovery.
```

```
Are you sure you want to continue? [yes/no]: yes
```

```
Boston(config)#
```

You can mitigate this potential security breach by using the **no service password-recovery** global configuration command. The **no service password-recovery** command has no arguments or keywords.

Caution If a router is configured with the **no service password-recovery** command, all access to the ROMMON is disabled. If the router flash memory does not contain a valid Cisco IOS image, you will not be able to use the **rommon xmodem** command to load a new flash image. In order to repair the router, you must obtain a new Cisco IOS image on a flash SIMM, or on a PCMCIA card (3600 only). See Cisco.com for more information regarding backup flash images.

Once the **no service password-recovery** command is executed, the router boot sequence will look similar to this:

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
```

```
Copyright (c) 1999 by cisco Systems, Inc.
```

```
C2600 platform with 65536 Kbytes of main memory
```

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
```

```
program load complete, entry point: 0x80008000, size: 0xed9ee4
```

Also, after the **no service password-recovery** command is executed, a **show running configuration** command listing will contain the **no service password-recovery** statement as shown here:

```
!  
version 12.0  
service tcp-keepalives-in  
service timestamps debug datetime localtime show-timezone  
service timestamps log datetime localtime show-timezone  
service password-encryption  
no service password-recovery  
!  
hostname Boston
```

Setting a Login Failure Rate

This topic describes how to secure administrative access to Cisco routers by setting a login failure rate.

Authentication Failure Rate with Login

```
router(config)#  
security authentication failure rate threshold-rate log
```

- Configures the number of allowable unsuccessful login attempts
- By default, router allows 10 login failures before initiating a 15-second delay
- Generates a syslog message when rate is exceeded

```
Boston(config)#security authentication failure rate 10 log
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCM v1.0—5-12

Starting with Cisco IOS software Release 12.3(1), you can configure the number of allowable unsuccessful login attempts by using the **security authentication failure rate** global configuration command.

security authentication failure rate *threshold-rate* **log**

security authentication failure rate Parameters

Parameter	Description
<i>threshold-rate</i>	This is the number of allowable unsuccessful login attempts. The default is 10 (the range is 2 to 1024).
log	The log keyword is required. Results in a generated syslog event.

When the number of failed login attempts reaches the configured rate, two events occur:

- A **TOOMANY_AUTHFAILS** event message is sent by the router to the configured syslog server.
- A 15-second delay timer starts.

After the 15-second delay has passed, the user may continue to attempt to log in to the router.

Setting a Login Failure Blocking Period

With this IOS login enhancement command, available in Cisco IOS software Release 12.3(4)T and later, the IOS router will not accept any additional login connections for a “quiet period” if the configured number of connection attempts fail within a specified time period. Hosts that are permitted by a predefined ACL are excluded from the quiet period. You can specify the predefined ACL that is excluded from the quiet period by using the global configuration mode command **login quiet-mode access-class**.

Setting a Login Failure Blocking Period

```
router(config)#  
login block-for seconds attempts tries within seconds
```

- Blocks access for a quiet period after a configurable number of failed login attempts within a specified period
- Must be entered before any other login command
- Mitigates DoS and break-in attacks

```
Boston(config)#login block-for 100 attempts 2 within 100
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5-10

The first command parameter (seconds) specifies the duration of time, or quiet period, during which login attempts are denied.

The second parameter (attempts) stands for the maximum number of failed login attempts that triggers the quiet period.

The third parameter (within) describes the duration of time, in seconds, during which the allowed number of failed login attempts must be made before the quiet period is triggered.

After the **login block-for** command is enabled, these defaults are enforced:

- A default login delay of one second.
- All login attempts made via Telnet, secure shell (SSH), and HTTP are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is issued.

System Logging Messages for a Quiet Period

After a router switches to and from quiet mode, logging messages are generated. Also, if configured, logging messages are generated upon every successful or failed login request. Logging messages can be generated for successful login requests via the new global configuration command **login on-success**. The **login on-failure** command generates logs for failed login requests.

This logging message is generated after the router switches to quiet-mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for
watching failures is 158 seconds, [user:sfd]
[Source:10.4.2.11] [localport:23] [Reason:Invalid login],
[ACL:22] at 16:17:23 UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF,
because block period timed out at 16:22:23 UTC Wed Feb 26 2003
```

Excluding Addresses from Login Blocking

With the **login quiet-mode access-class** command, introduced in Cisco IOS software Release 12.3(4)T, the IOS router will use the configured ACL to permit login attempts when the router switches to quiet mode. If this command is not configured, all connection attempts will be denied during the quiet period.

Excluding Addresses from Login Blocking

```
router(config)#  
login quiet-mode access-class {acl-name / acl-number}
```

- Specifies an ACL that is applied to the router when it switches to the quiet mode.
- If not configured, all login requests will be denied during the quiet mode.
- Excludes IP addresses from failure counting for login block-for command.

```
Boston(config)#login quiet-mode access-class myacl
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5-14

The ACL also specifies IP addresses that are excluded from login failure counting using the **login block-for** command.

Setting a Login Delay

A Cisco IOS device can accept login connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The **login delay** command introduces a uniform delay between successive login attempts. The delay occurs for all login attempts—failed or successful attempts. Thus, users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Setting a Login Delay

```
router(config)#  
login delay seconds
```

- Configures a delay between successive login attempts.
- Helps mitigate dictionary attacks.
- If not set, a default delay of one second is enforced after the login block-for command is configured.

```
Boston(config)#login delay 30
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-15

The **login delay** command was introduced in Cisco IOS software Release 12.3(4)T. If not enabled, a login delay of one second is automatically enforced after the **login block-for** command is applied to the router configuration.

Verifying Login

You can verify the login functionality by using the **show login** command.

Verifying Login

```
router#  
show login [failures]
```

- Displays login parameters and failures

```
Boston(config)#show login  
  
A default login delay of 1 seconds is applied.  
No Quiet-Mode access list has been configured.  
All successful login is logged and generate SNMP traps.  
All failed login is logged and generate SNMP traps.  
Router enabled to watch for login Attacks.  
If more than 15 login failures occur in 100 seconds or less, logins  
will be disabled for 100 seconds.  
Router presently in Watch-Mode, will remain in Watch-Mode for 95  
seconds.  
Present login failure count 5.
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-16

The sample output from the **show login** command verifies that the **login block-for** command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; five login requests have already failed.

Router#**show login**

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins
will be disabled for 100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95
seconds.
Present login failure count 5.

The sample output from **show login failures** command shows all failed login attempts on the router.

```
Router#show login failures
```

Information about login failure's with the device

Username	Source IPAddr	lPort	Count	TimeStamp
try1	10.1.1.1	23	1	21:52:49 UTC Sun Mar 9 2003
try2	10.1.1.2	23	1	21:52:52 UTC Sun Mar 9 2003

Setting Timeouts

This topic describes how to secure administrative access to Cisco routers by setting timeouts.

Setting Timeouts for Router Lines

```
router(config-line)#  
exec-timeout minutes [seconds]
```

- Default is 10 minutes
- Terminates an unattended connection
- Provides an extra safety factor when an administrator walks away from an active console session

```
Boston(config)#line console 0  
Boston(config-line)#exec-timeout 3 30  
Boston(config)#line aux 0  
Boston(config-line)#exec-timeout 3 30
```

- Terminates an unattended console and auxiliary connection after 3 minutes and 30 seconds

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-18

By default, an administrative interface stays active (and logged on) for ten minutes after the last session activity. After that, the interface times out and logs out of the session. It is recommended that you fine-tune these timers to limit the amount of time to within two or three minutes maximum.

Caution Setting the exec-timeout value to 0 means that there will be no timeout and the session will stay active for an unlimited time. Do not set the value to 0.

You can adjust these timers using the **exec-timeout** command in line configuration mode for each of the line types used.

exec-timeout *minutes* [*seconds*]

exec-timeout Parameters

Parameter	Description
<i>minutes</i>	This integer specifies the number of minutes.
<i>seconds</i>	(Optional) This integer specifies the additional time interval in seconds.

Setting Multiple Privilege Levels

This topic describes how to secure administrative access to Cisco routers by setting multiple privilege levels.

Setting Multiple Privilege Levels

```
router(config)#  
privilege mode {level level command | reset command}
```

- Level 0 is predefined for user-level access privileges.
- Levels 1 to 14 may be customized for user-level privileges.
- Level 15 is predefined for enable mode (enable command).

```
Boston(config)#privilege exec level 2 ping  
Boston(config)#enable secret level 2 Patriot
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-20

Cisco routers enable you to configure various privilege levels for your administrators. Different passwords can be configured to control who has access to the various privilege levels. This is especially helpful in a help desk environment where certain administrators are allowed to configure and monitor every part of the router (level 15) while other administrators may be restricted to only monitoring (customized levels 2 to 14). The 16 levels (0 to 15) are defined in the figure.

Privileges are assigned to levels 2 to 14 using the **privilege** command from global configuration mode.

The example shown in the figure assigns the **ping** command to privilege level 2 and establishes “Patriot” as the secret password users must enter to use level 2 commands. Using the **enable 2** command, you will be prompted for the enable secret password for privilege level 2. The **show privilege** command is used to display the current privilege level.

```
router>enable 2  
Password: Patriot  
  
router#show privilege  
Current privilege level is 2
```

privilege mode {level level command | reset command}

privilege Parameters

Parameter	Description
<i>mode</i>	This command specifies the configuration mode. See the list after this table for options for this argument.
<i>level</i>	This command enables setting a privilege level with a specified command.
<i>level</i>	This is the privilege level associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
<i>command</i>	This sets the command to which the privilege level is associated.
<i>reset</i>	This command resets the privilege level of a command.
<i>command</i>	This is the command for which you want to reset the privilege level.

Use the **privilege ?** option of the command in the global configuration mode to see a complete list of router configuration modes on your router. The table contains some of the router configuration modes that can be configured using the **privilege** command.

Router Configuration Modes

Configuration Mode	Description
accept-dialin	Virtual private dialup network (VPDN) group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address family configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 table
cascustom	Channel associated signaling (CAS) custom configuration mode
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map configuration mode
dhcp	DHCP pool configuration mode
dspfarm	Digital signal processor (DSP) farm configuration mode
exec	EXEC mode
flow-cache	Flow aggregation cache configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay data-link connection identifier (DLCI) configuration mode
ip-vrf	Configure IP VPN routing and forwarding (VRF) parameters
line	Line configuration mode
map-class	Map class configuration mode

Configuration Mode	Description
map-list	Map list configuration mode
null-interface	Null interface configuration mode
preaut	AAA preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode
route-map	Route map configuration mode
router	Router configuration mode
vpdn-group	VPDN group configuration mode
voipdialpeer	Dial peer configuration mode

Configuring Banner Messages

This topic describes how to secure administrative access to Cisco routers by configuring banner messages.

Configuring Banner Messages

```
router(config)#  
banner {exec | incoming | login | motd | slip-ppp}  
  d message d
```

- Specifies what is “proper use” of the system
- Specifies that the system is being monitored
- Specifies that privacy should not be expected when using this system

```
Boston(config)#banner motd %  
WARNING: You are connected to $(hostname) on the Cisco Systems,  
Incorporated network. Unauthorized access and use of this network will  
be vigorously prosecuted. %
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-22

Banner messages should be used to warn would-be intruders that they are not welcome on your network. Banners are important, especially from a legal perspective. Intruders have been known to win court cases because they did not encounter appropriate warning messages when accessing router networks.

Choosing what to place in your banner messages is extremely important and should be reviewed by legal counsel before placing them on your routers. Never use the word *welcome* or any other familiar greeting that may be misconstrued as an invitation to use the network.

Banners are disabled by default and must be explicitly enabled by the administrator. As shown in the figure, use the **banner** command from global configuration mode to specify appropriate messages.

banner {exec | incoming | login | motd | slip-ppp} d message d

banner Parameters

Parameter	Description
exec	This command specifies and enables a message to be displayed when an EXEC process is created on the router (an EXEC banner).
incoming	This command specifies and enables a banner to be displayed when there is an incoming connection to a terminal line from a host on the network.
login	This command specifies and enables a customized banner to be displayed before the username and password login prompts.

Parameter	Description
<code>motd</code>	This command specifies and enables a message-of-the-day (MOTD) banner.
<code>slip-ppp</code>	This command specifies and enables a banner to be displayed when a Serial Line Interface Protocol (SLIP) or PPP connection is made.
<code>d</code>	This represents the delimiting character of your choice (for example, a pound sign [#]). You cannot use the delimiting character in the banner message.
<code>message</code>	This represents message text. You can include tokens in the form <code>\$(token)</code> in the message text. Tokens are replaced with the corresponding configuration variable.

This list contains valid tokens for use within the *message* section of the **banner** command:

- **\$(hostname)**: Displays the hostname for the router
- **\$(domain)**: Displays the domain name for the router
- **\$(line)**: Displays the vty or tty (asynchronous) line number
- **\$(line-desc)**: Displays the description attached to the line

Configuring Role-Based CLI

This topic describes the use of role-based CLI by network administrators.

Role-Based CLI Overview

- **Traditional approach of limiting CLI access based on privilege levels and enable passwords provided too little control:**
 - No access control to specific interfaces
 - Commands placed on a higher privilege level could not be reused for lower-privileged users
- **CLI views provide more granular control.**
- **CLI views include accessible commands and interfaces.**
- **Access to a view is protected with a secret.**
- **Views can be grouped to superviews to create large sets of accessible commands and interfaces.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-24

Although users can control CLI access via both privilege levels and enable mode passwords, these functions do not provide the necessary level of detail needed when working with Cisco IOS routers and switches.

The Role-Based CLI Access feature allows you to define “views,” which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration mode commands. Views restrict user access to Cisco IOS CLI and configuration information; that is, a view can define which commands are accepted and what configuration information is visible. CLI views provide a more detailed access control capability for network administrators, thereby improving the overall security and accountability of Cisco IOS software.

As of Cisco IOS software Release 12.3(11)T, you can also specify an interface or a group of interfaces to a view, thereby allowing access on the basis of specified interfaces.

Access to a view is protected with a password, similarly to the concept used by the privilege levels.

To simplify the view management, views can be grouped to superviews, to create large sets of commands and interfaces. A superview encompasses several individual views, resulting in wider administrative privileges.

Role-Based CLI Details

When a system is in root view, it has all of the access privileges as a user who has level 15 privileges. If you wish to configure any view to the system, the system must be in root view.

Role-Based CLI Details

- Root view is the highest administrative view.
- Creating and modifying a view or superview is possible only from root view.
- The difference between root view and privilege 15 is that only a rootview user can create or modify views and superviews.
- CLI views require AAA new-model:
 - Necessary even with local view authentication
 - View authentication can be offloaded to an AAA server using the new attribute "cli-view-name"
- A maximum of 15 CLI views can exist in addition to the root view.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5.25

The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view. Also, when you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

View authentication can be performed by an external AAA server via the new *cli-view-name* attribute. AAA authentication associates only one view name to a particular user; that is, only one view name can be configured for a user in an authentication server.

Note	AAA provides access to an external user database that is used for authentication, authorization, and accounting tasks. Without the external AAA server, all network devices would need to maintain a local copy of the user database, which may have a severe impact on scalability and functionality of the system.

The maximum number of CLI views and superviews, including one lawful intercept view, that can be configured is 15. (This does not include the root view.)

Getting Started with Role-Based CLI

This section describes the configuration steps related to role-based CLI.

Getting Started with Role-Based CLI

```
router#  
enable [privilege-level] [view [view-name]]
```

- Enter a privilege level or a CLI view.
- Use **enable** command with the **view** parameter to enter the root view.
- Root view requires privilege 15 authentication.
- The **aaa-new** model must be enabled.

```
Boston(config)#aaa new-model  
Boston(config)#exit  
Boston#enable view  
Password:  
Boston#  
%PARSER-6-VIEW_SWITCH: successfully set to view 'root'
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-26

Before you enter or create a view, you must enable AAA via the **aaa new-model** command.

Then use the **enable** command with the **view** parameter to enter the root view. You will be prompted for authentication, if configured. Use the privilege 15 password.

Note If AAA is not enabled, you will get this error:
router#**enable view**
% AAA must be configured

enable [*privilege-level*] [**view** [*view-name*]]

enable Parameters

Parameter	Description
<i>privilege-level</i>	(Optional) Sets the privilege level at which to log in.
<i>view</i>	(Optional) Enters into root view, which enables users to configure CLI views. This keyword is required if you want to configure a CLI view.
<i>view-name</i>	(Optional) Enters or exits a specified CLI view. This keyword can be used to switch from one CLI view to another CLI view.

Configuring CLI Views

After **aaa new-model** has been enabled and you enter the root view, create a view and enter the view configuration mode using the **parser view** command. You need to specify the name of the view to be created or the existing view to be modified.

Configuring CLI Views

```
router(config)#  
parser view view-name  
• Creates a view and enters view configuration mode  
  
router(config-view)#  
password 5 encrypted-password  
commands parser-mode {include | include-exclusive |  
exclude} [all] [interface interface-name | command]  
  
• Sets a password to protect access to the view  
• Adds commands or interfaces to a view  
  
Boston(config)#parser view monitor_view  
Boston(config-view)#password 5 hErMeNe%GiLdE!  
Boston(config-view)#commands exec include show version
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-27

Next, protect access to the CLI view with a secret using the **password** command. The only available encryption algorithm is MD5, represented by the number 5 in the first parameter field. Then provide a password that will be required to enter this view. You must issue this command before you can configure additional attributes for the view.

Finally, add commands or interfaces to a view using the **commands** command.

commands parser-mode {include | include-exclusive | exclude} [all] [interface interface-name | command]

commands Parameters

Parameter	Description
<i>parser-mode</i>	Specifies the mode in which the specified command exists
<i>include</i>	Adds a command or an interface to the view and allows the same command or interface to be added to an additional view
<i>include-exclusive</i>	Adds a command or an interface to the view and excludes the same command or interface from being added to all other views
<i>exclude</i>	Excludes a command or an interface from the view; that is, customers cannot access a command or an interface
<i>all</i>	(Optional) Specifies a “wildcard” that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view

Parameter	Description
<code>interface interface-name</code>	(Optional) Specifies interface that is added to the view
<code>command</code>	(Optional) Specifies command that is added to the view

Configuring Superviews

Role-based CLI facilitates the concept of grouping CLI views into view supersets, called superviews.

Configuring Superviews

```
router(config)#
```

`parser view view-name`

- **Creates a (super)view and enters its configuration**

```
router(config-view)#
```

`password 5 encrypted-password`
`view view-name`

- **Sets a password to protect access to the superview**
- **Adds a CLI view to a superview**

`Boston(config)#parser view monitor audit`
`Boston(config-view)#password 5 AnA6TaSiA$`
`Boston(config-view)#view monitor view`
`Boston(config-view)#view audit view`

© 2006 Cisco Systems, Inc. All rights reserved.ISCW v1.0--5.28

A superview consists of one or more CLI views, which allow users to define which commands are accepted and what configuration information is visible. Superviews allow you to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews have these characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
- If a superview is deleted, all CLI views associated with that superview will *not* also be deleted.

To configure a superview, use the **parser view** command and configure a password for that superview. Then, add a normal CLI view to the superview using the **view** command. Issue this command for each CLI view that is to be added to the superview.

Note Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Role-Based CLI Monitoring

When monitoring role-based CLI, use the command **show parser view** to display information about the view that the user is currently in. The option **all** displays information for all views that are configured on the router.

Note The **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in any CLI view.

Role-Based CLI Monitoring

```
router#  
show parser view [all]
```

- Displays the current view name
- The option **all**:
 - Displays all CLI views configured on the router
 - Is by default available only to root users
 - Can be added to other CLI views

```
router#  
debug parser view
```

- Displays debug messages for all views

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-29

To display debug messages for all views—use the **debug parser view** command in privileged EXEC mode.

Role-Based CLI Configuration Example

In this example, the CLI view **first** is created and configured to include the commands **show version**, **configure terminal**, and all commands starting with **show ip**.

Role-Based CLI Configuration Example

```
Boston(config)#aaa new-model
Boston(config)#exit
Boston#enable view
%PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
Boston#configure terminal
Boston(config)#parser view first
%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Boston(config-view)#secret 5 firstpass
Boston(config-view)#command exec include show version
Boston(config-view)#command exec include configure terminal
Boston(config-view)#command exec include all show ip
Boston(config-view)#exit
```

© 2006 Cisco Systems, Inc. All rights reserved. RSCW v1.0--5.30

Next, this configuration will be verified by entering and viewing the available commands.

Role-Based CLI Verification

When a user enters the CLI view, an indication message is displayed. Apart from the commands **enable** and **exit** that are available in all views, the only two commands visible in the CLI view are **configure** and **show**.

```
Boston>enable view first
Password:
%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Boston#?
Exec commands:
configure      Enter configuration mode
enable         Turn on privileged commands
exit           Exit from the EXEC
show           Show running system information
Boston#show ?
ip             IP information
parser         Display parser information
version        System hardware and software status
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5-31

To further verify the view configuration, the user looks at the available options of the **show** command. The available options include *parser*, which is always available, and the configured keywords *ip* and *version*.

Role-Based CLI Verification (Cont.)

```
Boston#show ip ?
access-lists      List IP access lists
accounting        The active IP accounting database
aliases           IP alias table
arp               IP ARP table
as-path-access-list List AS path access lists
bgp               BGP information
cache             IP fast-switching route cache
casa              Display casa information
cef               Cisco Express Forwarding
community-list    List community-list
dfp               DFP information
dhcp              Show items in the DHCP database drp
--More--
```

Next, the user verifies that all sub-options of the **show ip** command are available in the view.

Secure Configuration Files

This topic describes how to limit the router downtime by implementing the Cisco IOS Resilient Configuration feature.

Secure Configuration Files Introduction

- **Traditional risk that the configuration and the image are erased after a router compromise:**
 - **Availability threat (downtime)**
- **Need to secure the primary bootset (configuration file and the running image)**
- **Also known as the Cisco IOS Resilient Configuration feature**
- **Speeds up the recovery process**
- **Files must be stored locally**
- **Feature can be disabled through a console session**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-34

A great challenge for network operators is to deal with the total downtime experienced after a router has been compromised and its operating software and configuration data erased from its persistent storage. The operator must retrieve an archived copy (if any) of the configuration and a working image to restore the router. Recovery must then be performed for each affected router, adding to the total network downtime.

The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage in NVRAM and flash.

The Cisco IOS Resilient Configuration feature is intended to speed up the recovery process. The feature maintains a secure working copy of the router image and the startup configuration at all times. These secure files cannot be removed by the user. This set of image and router running configuration is referred to as the primary bootset.

The following factors were considered in the design of Cisco IOS Resilient Configuration:

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.

Restrictions for Cisco IOS Resilient Configuration

This feature is available only on platforms that support a Personal Computer Memory Card International Association (PCMCIA) Advanced Technology Attachment (ATA) disk. There must be enough space on the storage device to accommodate at least one Cisco IOS image and a copy of the running configuration.

It may be possible to force removal of secured files using an older version of Cisco IOS software that does not contain file system support for hidden files.

This feature can be disabled only by using a console connection to the router. With the exception of the upgrade scenario, feature activation does not require console access.

Secured files will not appear in the output of a **dir** command issued from an executive shell because secure files are not listed. ROMMON mode does not have any such restriction and can be used to list and boot secured files. The running image and running configuration archives will not be visible in the Cisco IOS **dir** command output. Instead, the **show secure bootset** command must be used to verify archive existence.

Securing Configuration Files

To secure the running image and the startup configuration file, use the commands **secure boot-image** and **secure boot-config** in the configuration mode.

Securing Configuration Files

```
router(config)#
```

`secure boot-image`

- Enables Cisco IOS image resilience

```
router(config)#
```

`secure boot-config`

- Stores a secure copy of the primary bootset in persistent storage

```
router#
```

`show secure bootset`

- Displays the status of configuration resilience and the primary bootset filename

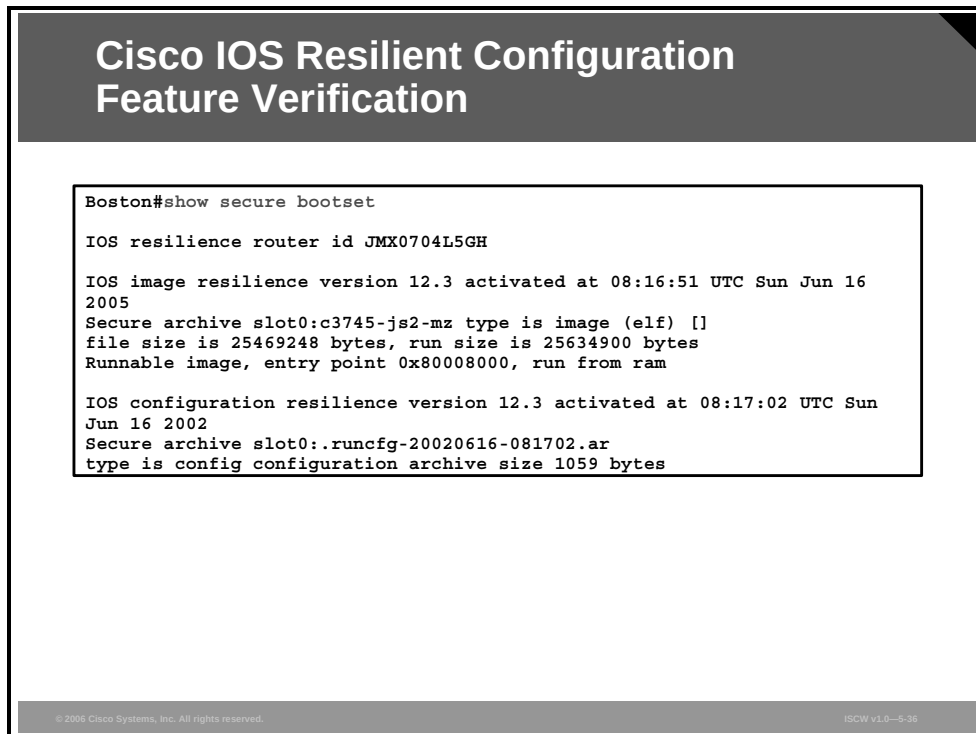
`Boston(config)#secure boot-image`
`Boston(config)#secure boot-config`

© 2006 Cisco Systems, Inc. All rights reserved.ISCW v1.0--5-35

To verify the status of the resilience feature and the primary bootset filename, use the **show secure bootset** command.

Cisco IOS Resilient Configuration Feature Verification

This printout shows a sample output of the **show secure bootset** command.



The printout shows the status of the resilience feature and the primary bootset filename (both the startup configuration and the running image).

Secure Configuration Files Recovery

When a router is compromised, you may have to reload it to start the recovery procedure. This is not always necessary and may depend on the circumstances. You can use the **reload** command in the router privileged mode to restart it and interrupt the boot sequence to enter the ROMMON mode. In the ROMMON, use the **dir** and **boot** commands to view the contents of the file system and select a secure image to boot the router from.

Secure Configuration Files Recovery

```
rommon 1 >
```

```
dir [filesystem:]
```

```
boot [partition-number:] [filename]
```

- Lists the contents of the device with secure bootset
- Boots up the router using the secure bootset image

```
router(config)#
```

```
secure boot-config [restore filename]
```

- Restores the secure configuration to a filename

```
rommon 1 >dir slot0:
```

```
rommon 2 >boot slot0:c3745-js2-mz
```

```
....
```

```
Router(config)#secure boot-config restore slot0:rescue
```

```
Router#copy slot0:rescue running-config
```

© 2006 Cisco Systems, Inc. All rights reserved.ISCW v1.0--5.37

When the router recovery process starts in the ROMMON mode, you can view the contents of the file system with the **dir** command to identify the image that the router should boot from. Then use the **boot** command to load the specified secured image. After the router boots and if the startup configuration was deleted, the router will prompt you for interactive configuration input. You should decline to enter an interactive configuration session in setup mode if you secured the configuration file. Instead, use the **secure boot-config restore** command to recover the secured startup configuration and save it under a specified filename (*slot0:rescue* in the example). Finally, copy the recovered file to the running configuration to resume normal operations.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Strong passwords and protection of all access methods are essential for router security.**
- **Enable secrets should be used in addition or instead of enable passwords for increased password protection.**
- **Password-encryption service encrypts all system passwords with Vigenere cipher to protect against shoulder surfing.**
- **Enhanced username password security provides a strong MD5 password encryption.**
- **Login failure rate and blocking period after login failures mitigate password attacks.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-38

Summary (Cont.)

- **Banner messages should warn against unauthorized access.**
- **Privilege levels facilitate management by multiple administrators.**
- **Role-based CLI provides more manageability than privilege levels.**
- **The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash).**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-38

Mitigating Threats and Attacks with Access Lists

Overview

This lesson describes how to mitigate threats and attacks to Cisco peripheral routers by formatting and applying access control lists (ACLs) to filter traffic. ACLs provide packet filtering at the router level and are used extensively at a firewall to protect internal networks from the outside world. This lesson outlines the types of ACLs that are available and provides guidelines that help create these ACLs.

Objectives

Upon completing this lesson, you will be able to mitigate threats and attacks to Cisco perimeter routers by configuring and applying ACLs to filter traffic. This ability includes being able to meet these objectives:

- Identify the types and formats of IP ACLs that are used by routers to restrict access and filter packets
- Describe how to apply ACLs to router interfaces
- Explain the use of traffic filtering with ACLs to mitigate threats in a network
- Explain how to implement ACLs to mitigate threats
- Explain how to configure router ACLs to help reduce the effects of distributed DoS attacks
- Describe how to combine many ACL functions into two or three larger ACLs
- Explain some of the caveats to be considered when building ACLs

Cisco ACLs

This topic describes the types and formats of IP ACLs that are used by routers to restrict access and filter packets.

Standard and Extended ACLs

Cisco routers support two basic types of IP ACLs:

- **Standard IP ACL: Filters IP packets based on the source address only**

```
access-list 10 permit 192.168.3.0 0.0.0.255
```

- **Extended IP ACL: Filters IP packets based on several attributes, including:**
 - Protocol type (IP, ICMP, UDP, TCP, or protocol number)
 - Source and destination IP addresses
 - Source and destination TCP and UDP ports

```
access-list 101 permit tcp 172.31.9.0 0.0.0.255 any eq 80
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5.3

The Cisco ACL is probably the most commonly used object in Cisco IOS software. The ACLs are not only used for packet filtering (a type of firewall) but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way.

The ACL is a list of statements. Each statement defines a pattern that would be found in an IP packet. As each packet comes through an interface with an associated ACL, the list is scanned from top to bottom, and in the exact order in which it was entered, for a pattern that matches the incoming packet. A permit or deny rule associated with the pattern determines what will happen to that packet.

Cisco routers use ACLs as packet filters to decide which packets can access a router service or which packets can be allowed across an interface. Packets that are allowed across an interface are called permitted packets. Packets that are not allowed across an interface are called denied packets. ACLs contain one or more rules or statements that determine which data is to be permitted or denied across an interface.

ACLs are designed to enforce one or more corporate security policies. For example, a corporate security policy may allow only packets using source addresses from within the trusted network to access the Internet. Once this policy is written, you can develop an ACL that includes certain statements which, when applied to a router interface, can implement this policy.

Cisco router security depends upon well-written ACLs to restrict access to router network services, and to filter packets as they traverse the router.

Cisco routers support three types of IP ACLs: standard, extended, and enhanced IP ACLs. The examples in the figure describe these two types:

- **Standard IP ACLs:** A standard ACL only allows you to permit or deny traffic from specific IP addresses. The destination of the packet and the ports involved do not matter. The first example allows traffic from all addresses in the range 192.168.3.0 to 192.168.3.255.
- **Extended IP ACLs:** An IP extended ACL is a list of statements that are created in global mode. This list can filter IP packets based on several attributes (protocol type, source and IP address, destination IP address, source TCP or User Datagram Protocol [UDP] ports, destination TCP or UDP ports, optional protocol type information for finer granularity of control). The second example configures ACL 101 to permit traffic originating from any address on the 172.31.9.0/24 network to any destination host port 80 (http). More on extended ACLs will be presented later in the lesson.

Identifying ACLs

Either a number or a name can identify Cisco ACLs and the protocols that they filter.

Identifying ACLs

Cisco routers can identify ACLs using two methods:

- **ACL number:** The number of the ACL determines which protocol it is filtering:
 - 1 to 99 and 1300 to 1999: Standard IP ACLs
 - 100 to 199 and 2000 to 2699: Extended IP ACLs
- **ACL name:** You provide the name of the ACL:
 - Names contain alphanumeric characters.
 - Names cannot contain spaces or punctuation and must begin with an alphabetic character.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-4

Using numbered ACLs is effective on smaller networks with more homogeneously defined traffic. Because each ACL type is limited to an assigned range of numbers, it is easy to determine the type of ACL that you are using. There can be up to 99 standard IP ACLs in the range from 1 to 99. The extended IP ACL number range is assigned from 100 to 199, and from 2000 to 2699.

The table lists the number range and the type of associated ACL.

ACL Number and Type

Number Range	Type of Associated ACL
1–99	IP standard ACL
100–199	IP extended ACL
200–299	Protocol type-code ACL
300–399	DECnet ACL
400–499	XNS standard ACL
500–599	XNS extended ACL
600–699	AppleTalk ACL
700–799	48-bit MAC address ACL
800–899	IPX standard ACL
900–999	IPX extended ACL
1000–1099	IPX SAP ACL
1100–1199	Extended 48-bit MAC address ACL

Number Range	Type of Associated ACL
1200–1299	IPX summary address ACL
1300–1999	IP standard ACL (expanded range)
2000–2699	IP extended ACL (expanded range)

You can also identify ACLs with an alphanumeric string (a name) rather than a number. Named ACLs allow you to configure more ACLs in a router than if you were to use numbered ACLs alone.

Note	If you identify your ACL with a name rather than a number, the mode and command syntax are slightly different. Currently, only packet and route filters can use a named ACL.

Guidelines for Developing ACLs

This section recommends methods that should be followed to create effective, easy-to-use, and easy-to-understand ACLs

Guidelines for Developing ACLs

- **Base ACLs on the security policy.**
- **Write ACL out:**
 - Write out what you want this ACL to accomplish.
 - This is the time to think about potential problems.
- **Set up a development system:**
 - This allows you to copy and paste statements easily.
 - It also allows you to develop a library of ACLs.
 - Store the files as ASCII text files.
- **Apply ACL to a router and test:**
 - If at all possible, run your ACLs in a test environment before placing them into production.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6.5

Before you start to develop any ACLs, consider these basic rules:

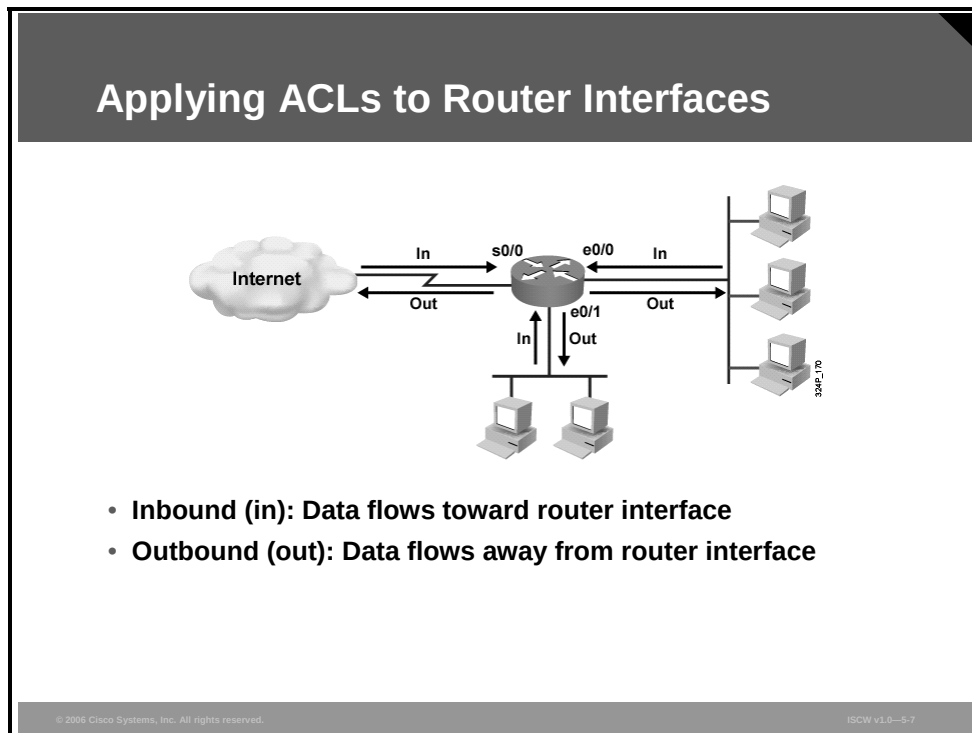
- **Base your ACLs on your security policy:** Unless the ACL is anchored in a comprehensive security policy, you cannot be absolutely certain it will effectively control access in the way access needs to be controlled.
- **Write the ACL out:** Never sit down at a router and start to develop an ACL without first spending some time in design. The best ACL developers suggest that you write out a list of things you want the ACL to accomplish. Starting with something as simple as, “This ACL must block all Simple Network Management Protocol (SNMP) access to the router except for the SNMP host at 10.1.1.15.”
- **Set up a development system:** Whether you use your laptop PC or a dedicated server, you need a place to develop and store your ACLs. Word processors or text editors of any kind are suitable, as long as you can save the files in ASCII text format. Build yourself a library of your most commonly used ACLs and use them as sources for new files. ACLs can be pasted into the router running configuration (requires console or Telnet access), or can be stored in a router configuration file. The system you choose should support TFTP to make it easy to transfer any resulting configuration files to the router.

Note Hackers love to gain access to router configuration development systems or TFTP servers that store ACLs. A hacker can discover a lot about your network from looking at these easily read text files. For this reason, it is imperative that the system where you choose to develop and store your router files be a secure system.

- **Test:** If possible, test your ACLs in a secure environment before placing them into production. Testing is a common-sense approach to any router configuration changes. Most enterprises maintain their own network test beds. While testing may appear to be an unnecessary cost, over time it can save time and money.

Applying ACLs to Router Interfaces

This topic describes how to apply ACLs to router interfaces.

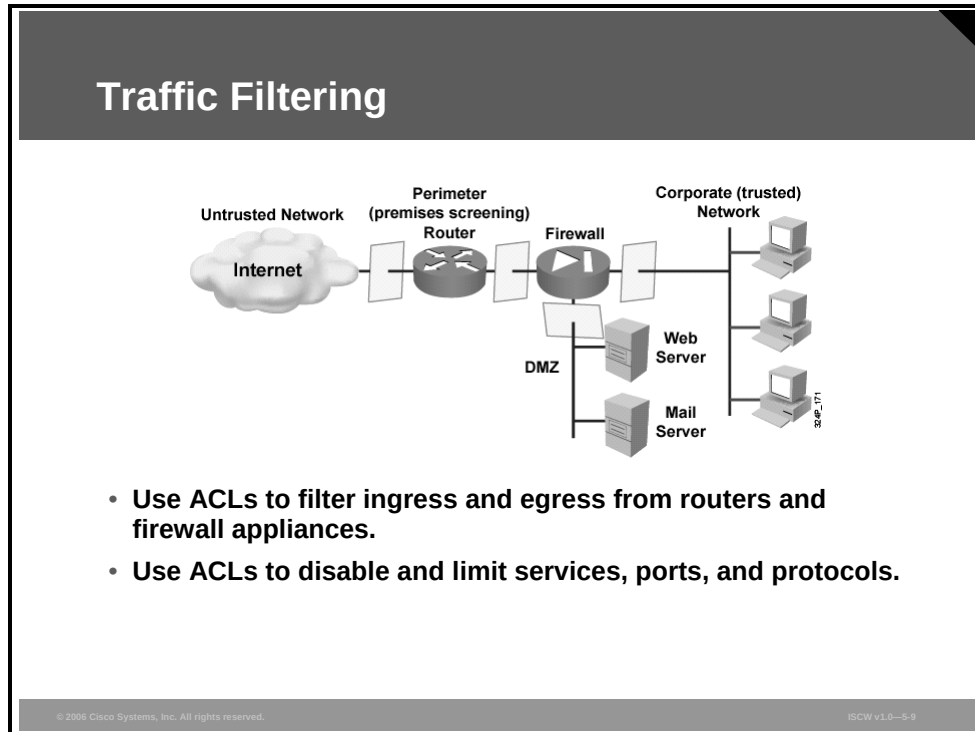


Packet-filtering ACLs must be applied to a router interface to take effect. It is important to note that ACLs are applied to an interface based on the direction of the data flow as shown in the figure. You can apply the ACL to incoming packets (an “in” ACL) or outgoing packets (an “out” ACL), as follows:

- **Inbound (in):** The packet filtering ACL applies to packets received on the router interface.
- **Outbound (out):** The packet filtering ACL applies to packets transmitted out of the router interface. For outbound ACLs, you need to set up the filter only on one outgoing interface rather than on individual incoming interfaces. This improves performance because only the network you are protecting will force a lookup on the ACL.

Using Traffic Filtering with ACLs

This topic explains the use of traffic filtering with ACLs to mitigate threats in a network.



Always apply the following general rules when deciding how to handle router services, ports, and protocols:

- Disable unused services, ports, or protocols. In the case where no one, including the router itself, needs to use an enabled service, port, or protocol, disable that service, port, or protocol.
- Limit access to services, ports, or protocols. In the case where a limited number of users or systems require access to an enabled router service, port, or protocol, limit access to that service, port, or protocol using ACLs.

ACLs are important because they act as traffic filters between the corporate (trusted) network and the Internet (untrusted network). Using ACLs, the router enforces corporate security policies by rejecting protocols and restricting port usage.

The table contains a list of common router services that can be used to gather information about your network, or worse, can be used to attack your network. Unless your network configuration specifically requires one of these services, the services should not be allowed to traverse the router. Use ACLs to block these services inbound to the protected network and outbound to the Internet.

Blocked Services

Service	Port	Transport	Service	Port	Transport
tcpmux	1	TCP and UDP	netbios-ssn	139	TCP and UDP
echo	7	TCP and UDP	xdmcp	177	UDP
discard	9	TCP and UDP	netbios (ds)	445	TCP

Service	Port	Transport	Service	Port	Transport
systat	11	TCP	rexec	512	TCP
daytime	13	TCP and UDP	lpr	515	TCP
netstat	15	TCP	talk	517	UDP
chargen	19	TCP and UDP	ntalk	518	UDP
time	37	TCP and UDP	uucp	540	TCP
whois	43	TCP	Microsoft UPnP SSDP	1900, 5000	TCP and UDP
bootp	67	UDP	nfs	2049	UDP
tftp	69	UDP	X Window System	6000-6063	TCP
subdup	93	TCP	irc	6667	TCP
sunrpc	111	TCP and UDP	NetBus	12345	TCP
loc-srv	135	TCP and UDP	NetBus	12346	TCP
netbios-ns	137	TCP and UDP	Back Orifice	31337	TCP and UDP
netbios-dgm	138	TCP and UDP			

This table contains a listing of common services that reside either on the corporate protected network or on the router itself. These services should be denied to untrusted clients using ACLs.

Denied Services

Service	Port	Transport	Service	Port	Transport
finger	79	TCP	who	513	UDP
snmp	161	TCP and UDP	rsh, rcp, rdist, rdump	514	TCP
snmp trap	162	TCP and UDP	syslog	514	UDP
rlogin	513	TCP	new who	550	TCP and UDP

These are two ways to control access to router services:

- **Disable the service itself:** Once a router service is disabled, no one can use that service. Disabling a service is safer, and more reliable, than attempting to block all access to the service using an ACL.
- **Restrict access to the service using ACLs:** If your situation requires limited access to a service, build and test appropriate ACLs that can be applied to the service.

Filtering Network Traffic to Mitigate Threats

This topic describes how to implement ACLs to mitigate a range of threats.

IP Address Spoofing Mitigation: Inbound

```
R2(config)#access-list 150 deny ip 10.2.1.0 0.0.0.255 any log
R2(config)#access-list 150 deny ip 127.0.0.0 0.255.255.255 any log
R2(config)#access-list 150 deny ip 0.0.0.0 0.255.255.255 any log
R2(config)#access-list 150 deny ip 172.16.0.0 0.15.255.255 any log
R2(config)#access-list 150 deny ip 192.168.0.0 0.0.255.255 any log
R2(config)#access-list 150 deny ip 224.0.0.0 15.255.255.255 any log
R2(config)#access-list 150 deny ip host 255.255.255.255 any log
R2(config)#access-list 150 permit ip any 10.2.1.0 0.0.0.255
R2(config)#interface e0/0
R2(config-if)#ip access-group 150 in
R2(config-if)#exit
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-11

ACLs can be used to mitigate many threats:

- IP address spoofing—Inbound
- IP address spoofing—Outbound
- Denial of service (DoS) TCP SYN attacks—Blocking external attacks
- DoS TCP SYN attacks—Using TCP Intercept
- DoS Smurf attacks
- Filtering Internet Control Message Protocol (ICMP) messages—Inbound
- Filtering ICMP messages—Outbound
- Filtering traceroute

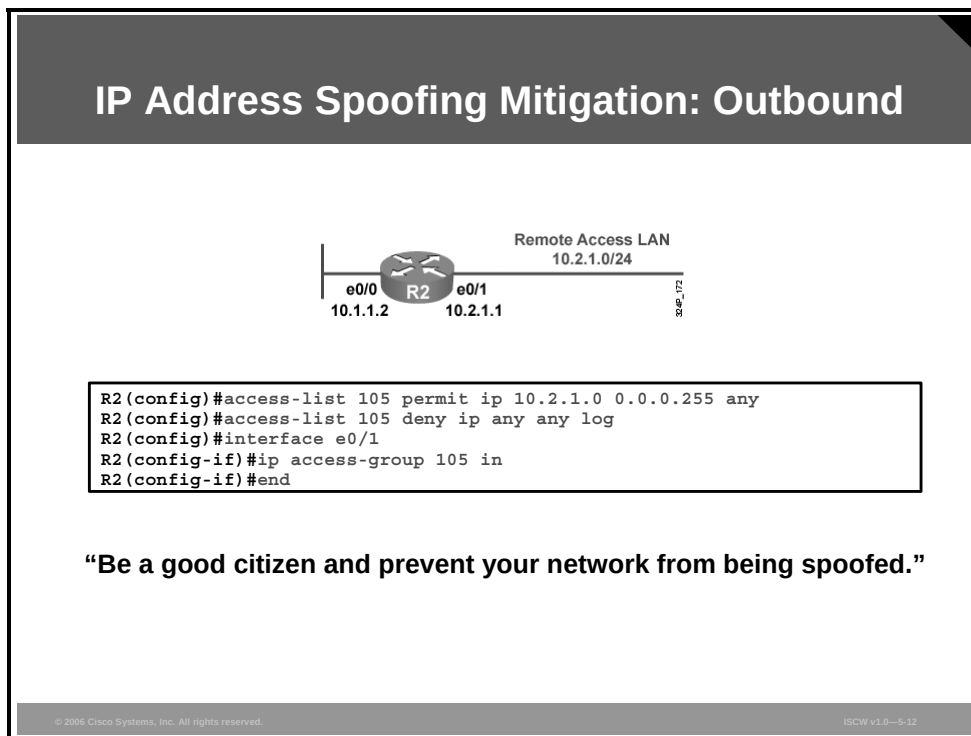
As a rule, do not allow any IP packets containing the source address of any internal hosts or networks, inbound to a private network. The figure shows ACL 150 for router R2. In this example, any packets containing these IP addresses in their source field will be denied:

- Addresses from the internal 10.2.1.0 network
- Any local host addresses (127.0.0.0/8)
- Any reserved private addresses (RFC 1918), in this case with the exception of 10.0.0.0/8, which is used for addressing
- Any addresses in the IP multicast address range (224.0.0.0/4)

This ACL is applied inbound to the external interface (e0/0) of router R2.

IP Address Spoofing Mitigation: Outbound

As a rule, you should not allow any outbound IP packets with a source address other than a valid IP address of the internal network.



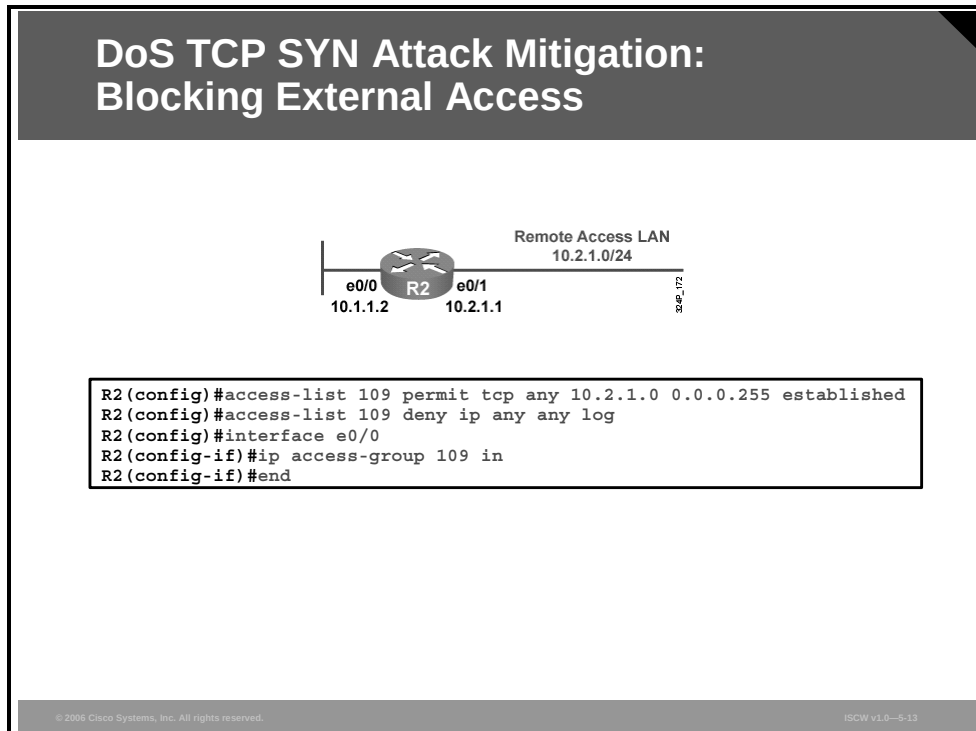
The example in the figure shows ACL 105 for router R2. This ACL permits only those packets that contain source addresses from the 10.2.1.0/24 network and denies all others.

This ACL is applied inbound to the inside interface (e0/1) of router R2.

Note Cisco routers running Cisco IOS software Release 12.0 and later may use IP Unicast Reverse Path Forwarding (RPF) verification as an alternative IP address spoof mitigation mechanism.

DoS TCP SYN Attack Mitigation: Blocking External Access

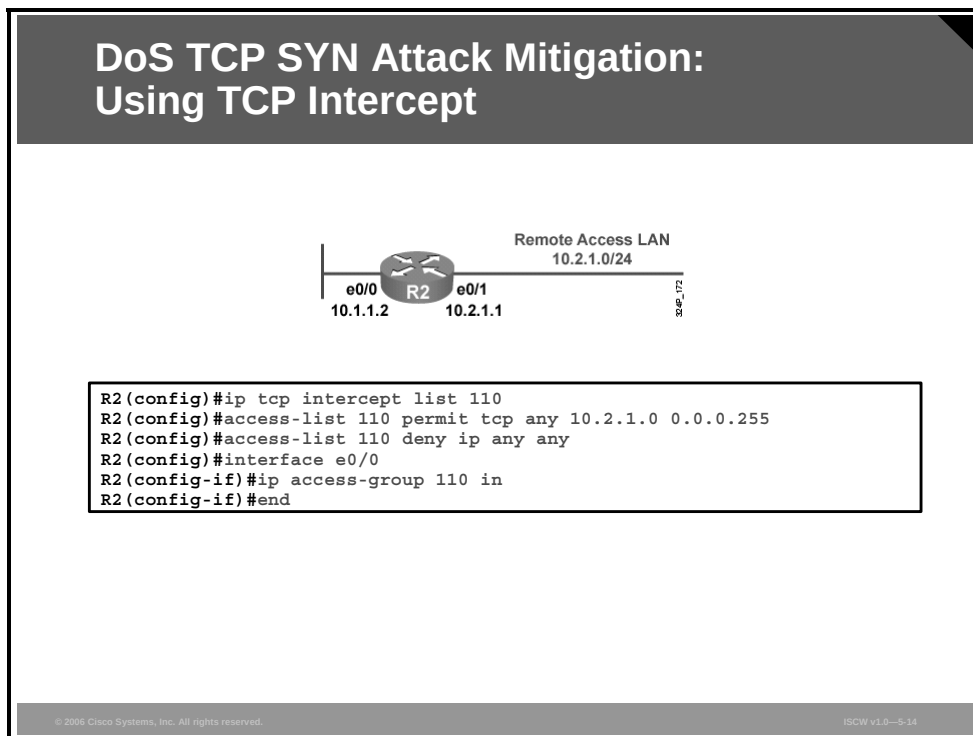
TCP SYN attacks involve sending large numbers of TCP SYN packets from a spoofed source into the internal network, which results in the flooding of the TCP connection queues of the receiving nodes.



The ACL in the figure is designed to prevent inbound packets, with the SYN flag set, from entering the router. However, the ACL does allow TCP responses from the outside network for TCP connections that originated on the inside network (keyword **established**). The **established** option is used for the TCP protocol only. It indicates return traffic from an established connection. A match occurs if the TCP datagram has the ACK control bit set.

DoS TCP SYN Attack Mitigation: Using TCP Intercept

TCP Intercept is a very effective tool for protecting internal network hosts from external TCP SYN attacks.

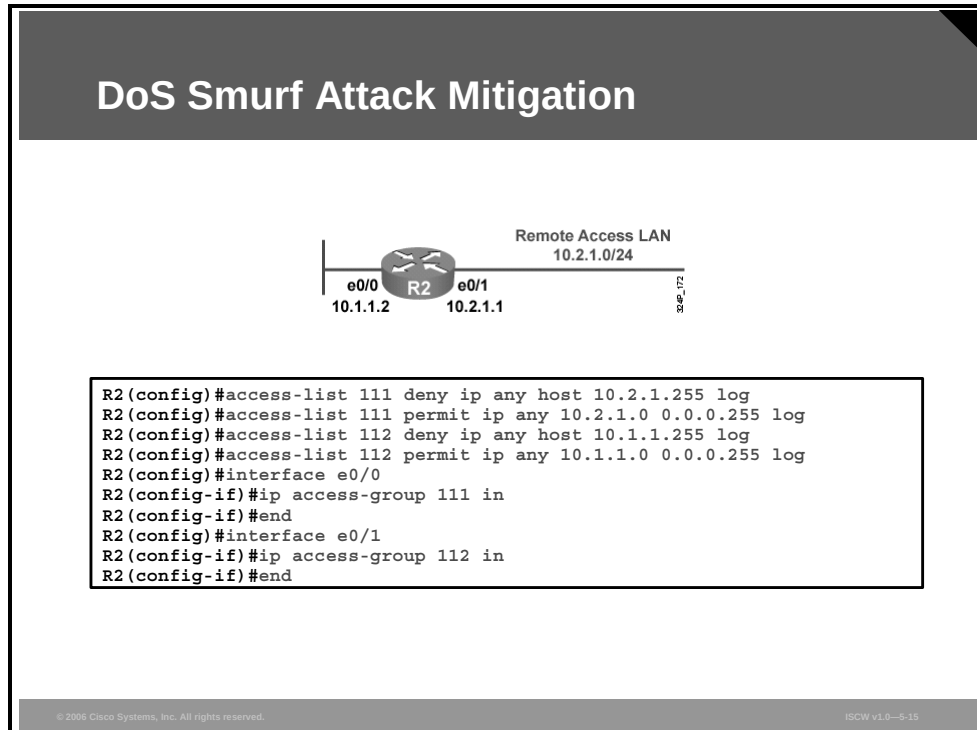


TCP Intercept protects internal hosts from SYN flood attacks by intercepting and validating TCP connection requests before they reach the hosts. Valid connections (those connections established within the configured thresholds) are passed on to the host. Invalid connection attempts are dropped.

Note Because TCP Intercept examines every TCP connection attempt, TCP Intercept can impose a performance burden on your routers. Always test for any performance problems before using TCP Intercept in a production environment.

DoS Smurf Attack Mitigation

Smurf attacks consist of large numbers of ICMP packets sent to a router subnet broadcast address using a spoofed source IP address from that same subnet. Some routers may be configured to forward these broadcasts to other routers in the protected network, and this process causes performance degradation. The ACL shown in the figure is used to prevent this forwarding process and halt the smurf attack.

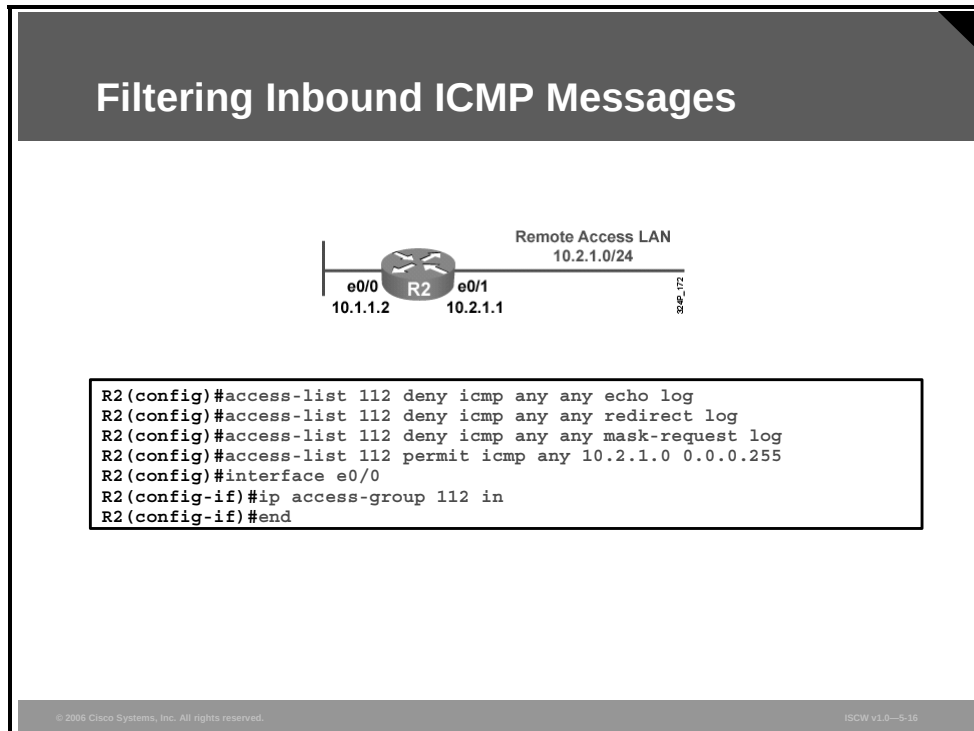


The ACLs in the figure block all IP packets originating from any host destined for the subnet broadcast addresses specified (10.2.1.255 and 10.1.1.255).

Note Cisco IOS software Release 12.0 and later now have the **no ip directed-broadcast** feature enabled by default, which prevents this type of ICMP attack. Therefore, you may not need to build an ACL as shown here.

Filtering Inbound ICMP Messages

There are several types of ICMP message types that can be used against your network. Programs use some of these messages; others are used for network management and so are automatically generated by the router.



ICMP echo packets can be used to discover subnets and hosts on the protected network and can also be used to generate DoS floods. ICMP redirect messages can be used to alter host routing tables. Both ICMP echo and redirect messages should be blocked inbound by the router.

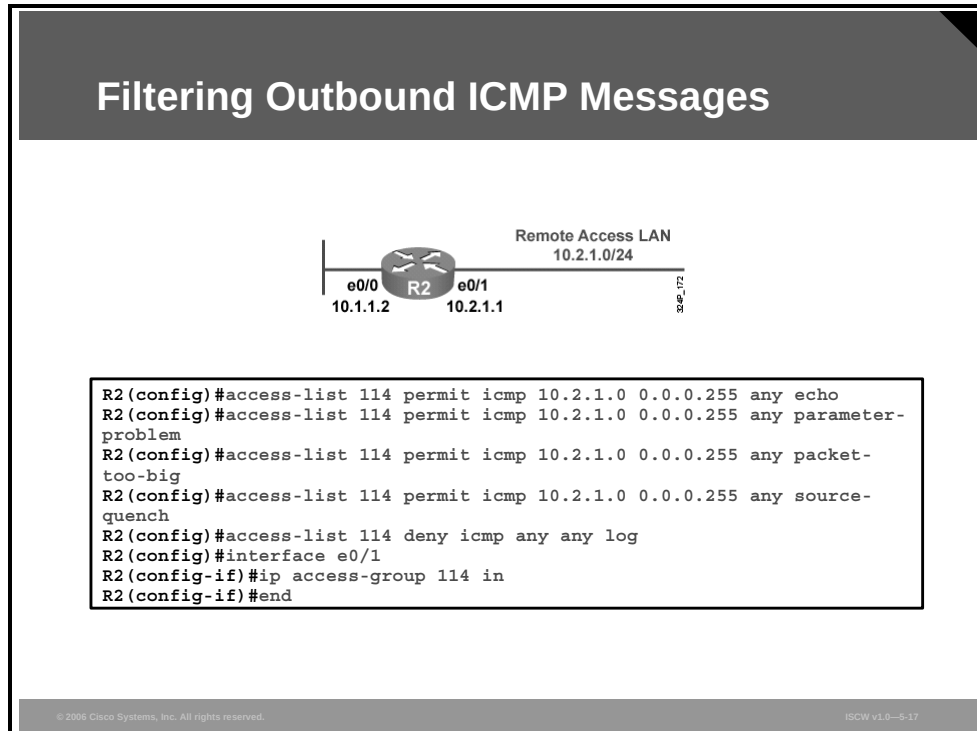
The ACL statement shown in the figure blocks all ICMP echo and redirect messages. As an added safety measure, this ACL also blocks mask-request messages. All other ICMP messages inbound to the 10.2.1.0/24 network are allowed.

Filtering Outbound ICMP Messages

These ICMP messages are required for proper network operation and should be allowed outbound:

- **Echo:** Allows users to ping external hosts
- **Parameter problem:** Informs host of packet header problems
- **Packet too big:** Required for packet maximum transmission unit (MTU) discovery
- **Source quench:** Throttles down traffic when necessary

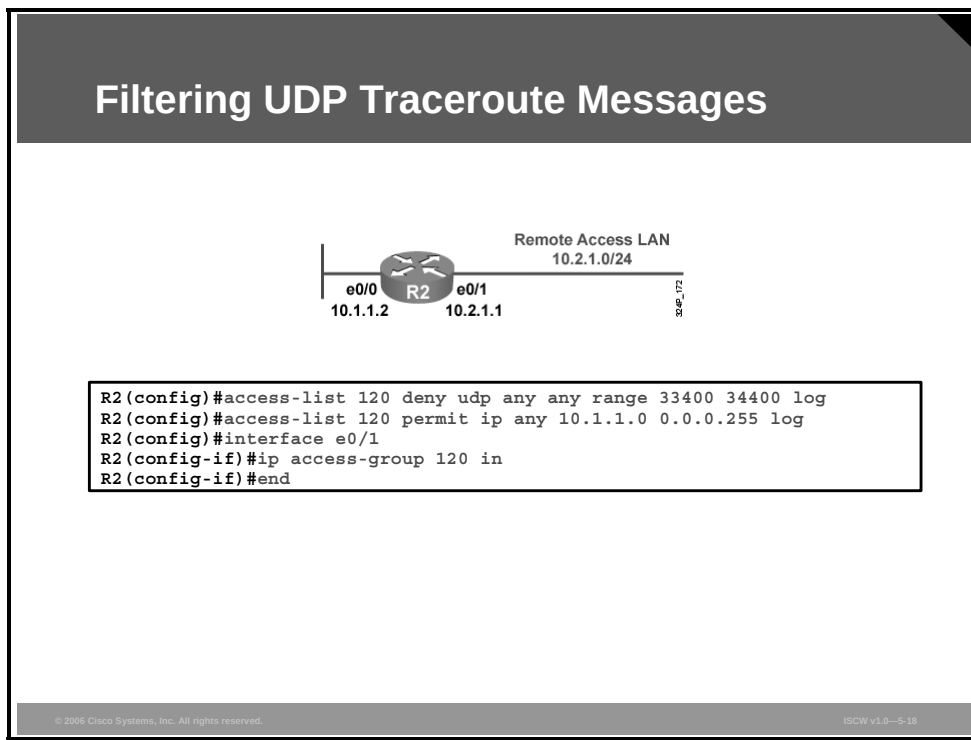
As a general rule, you should block all other ICMP message types outbound.



The ACL shown in the figure permits all of the required ICMP messages inbound to the e0/1 interface while denying all others.

Filtering UDP Traceroute Messages

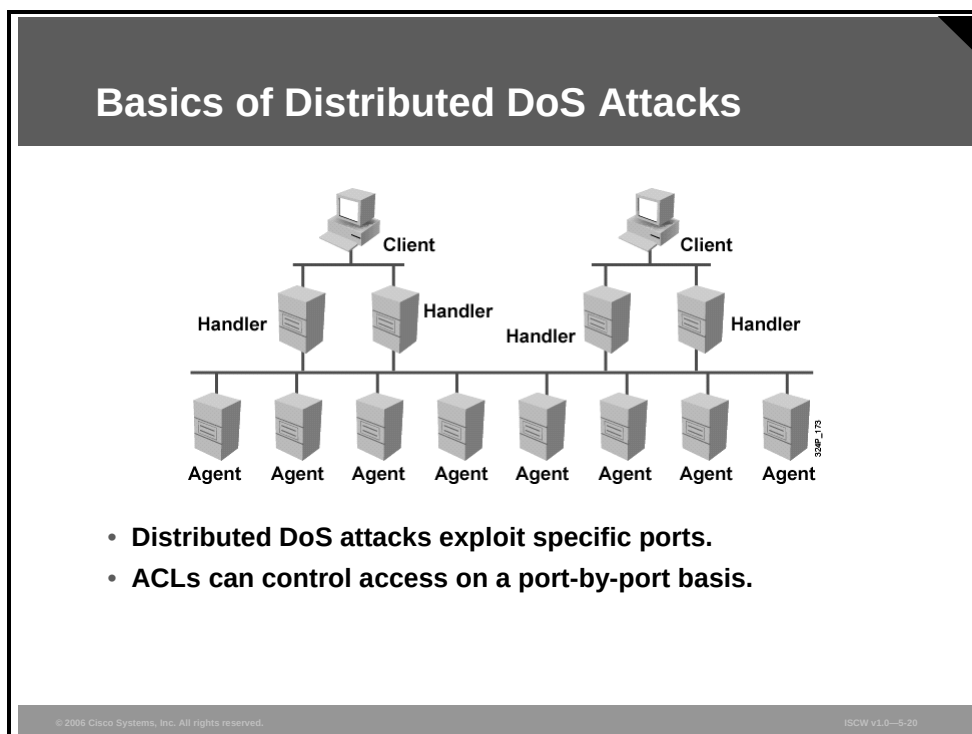
The traceroute feature uses some of the ICMP message types to complete several tasks. Traceroute displays the IP addresses of the routers that a packet encounters along its path (hops) from source to destination. Attackers can use ICMP responses to the UDP traceroute packets to discover subnets and hosts on the protected network.



As a rule, you should block all inbound traceroute UDP messages, as shown in the figure (UDP ports 33400 to 34400).

Mitigating Distributed DoS with ACLs

This topic describes how to configure router ACLs to help reduce the effects of distributed DoS attacks.



The figure shows how a distributed DoS attack occurs:

- Behind a *Client* is a person who launches the attack.
- A *Handler* is a compromised host that is running the attacker program. Each *Handler* is capable of controlling multiple *Agents*.
- An *Agent* is a compromised host that is running the attacker program. Each *Agent* is responsible for generating a stream of packets that is directed toward the intended victim.

Generally, routers cannot prevent all distributed DoS attacks, but they can help reduce the number of occurrences by building ACLs that filter known attack ports. Methods used to block distributed DoS by blocking selected ports include TRIN00, Stacheldraht, Trinity v3, and SubSeven. ACL rules are generally applied to inbound and outbound traffic between the protected network and the Internet.

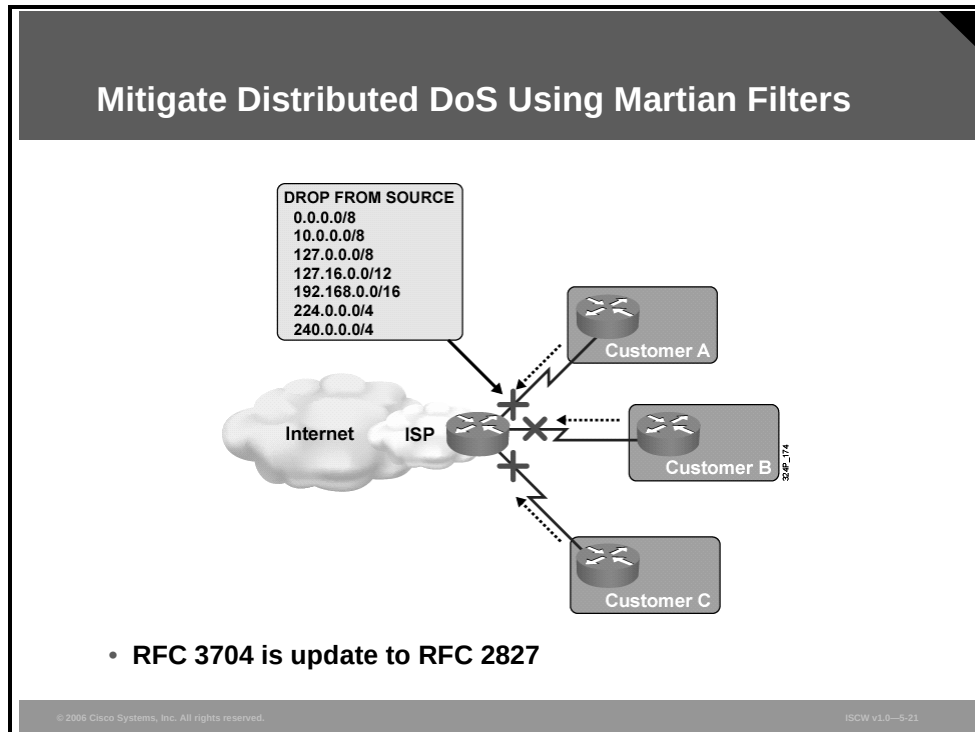
A distributed DoS attack can compromise several hundred to several thousand hosts. The hosts are usually Linux and SUN computers. However, the attack tools can be ported to other platforms as well. The process of compromising a host and installing the tool is automated. A DoS attack proceeds as follows:

- Step 1** The attacker initiates a scan phase in which a large number of hosts (perhaps 100,000 or more) are probed for a known vulnerability.
- Step 2** The attacker compromises the vulnerable hosts to gain access.
- Step 3** The attacker installs the tool on each host.
- Step 4** The attacker uses the compromised hosts for further scanning and compromises.

Because an automated process is used, attackers can compromise and install the tool on a single host in less than five seconds, and several thousand hosts can be compromised in less than one hour.

Mitigate Distributed DoS Using Martian Filters

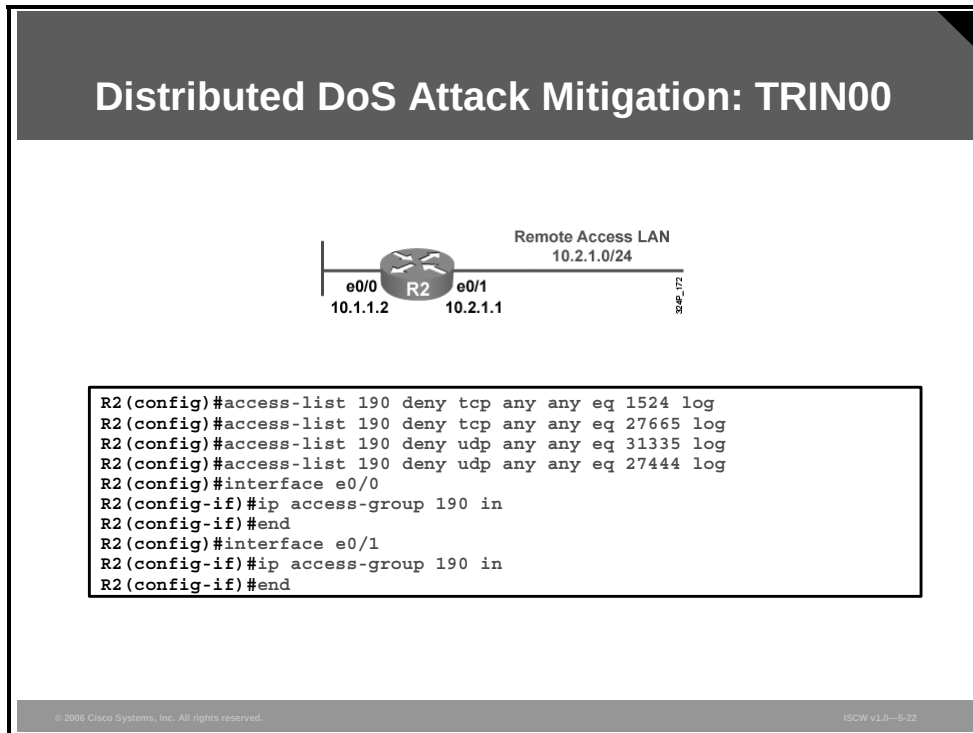
RFC 2827 recommends that ISPs police their customer traffic by dropping traffic entering their networks that is coming from a source address not legitimately in use by the customer network. The filtering includes, but is not limited to, traffic whose source address is a “Martian address”—a reserved address that includes any address within 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, or 240.0.0.0/4. RFC 3704 is the update to RFC 2827.



The reasoning behind the ingress filtering procedure is that distributed DoS attacks frequently spoof source addresses of other systems, placing a random number in the field. In some attacks, this random number is deterministically within the target network, simultaneously attacking one or more machines and causing those machines to attack others with ICMP messages or other traffic. Attacked sites can protect themselves by proper filtering, by verifying that their prefixes are not used in source addresses of packets received from the Internet. In other attacks, the source address is literally a random 32-bit number, resulting in the source of the attack being difficult to trace. If traffic leaving an edge network and entering an ISP can be limited to traffic being legitimately sent, attacks can be somewhat mitigated. Traffic with random or improper source addresses can be suppressed before it does significant damage, and attacks can be readily traced back to at least their source networks.

Distributed DoS Attack Mitigation: TRIN00

TRIN00 is a distributed SYN DoS attack. The attack method is a UDP flood.



The TRIN00 attack sets up communications between clients, handlers, and agents using these ports:

- 1524 tcp
- 27665 tcp
- 27444 udp
- 31335 udp

The mitigation tactic for the TRIN00 attack, as well as for the other DoS attacks considered in this topic, is to block both interfaces in the *in* direction. The goal is to prevent infected outside systems from sending messages to an internal network, and to prevent any infected internal systems from sending messages out of an internal network to the vulnerable ports.

For example, in the figure, the command **access-list 190 deny tcp any any eq 1524 log** translates to “ACL number 190 will deny any TCP traffic going from any network to any network which has the TCP port equivalent of 1524 and this will be logged.”

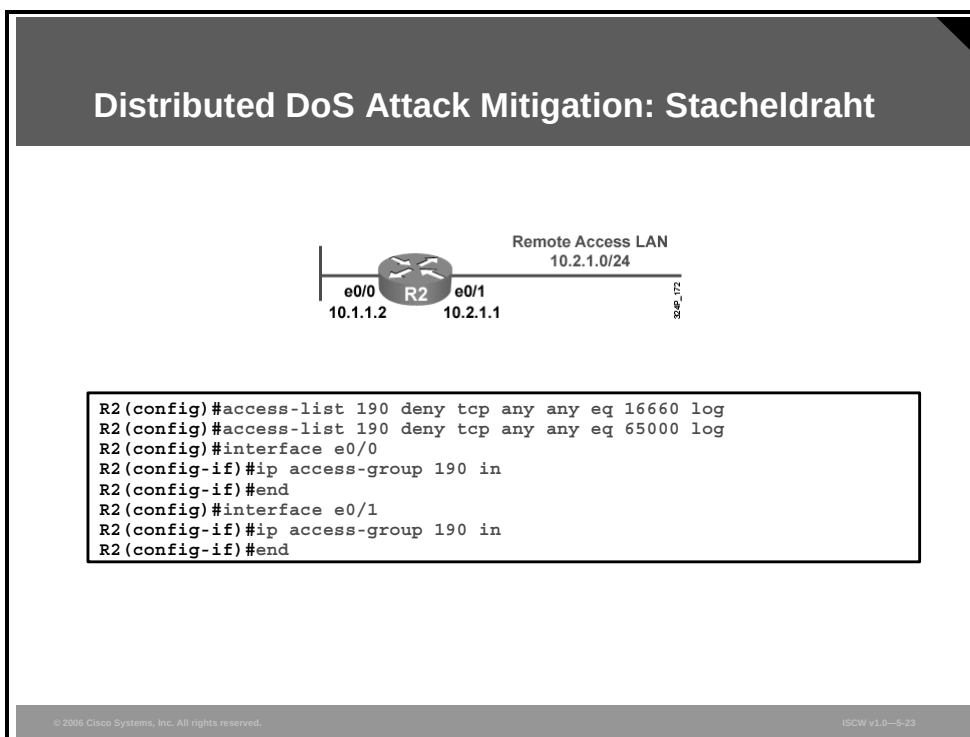
If you want to be specific about the exact incoming and outgoing network, those ports need to be specified. For example, if the IP address of the inside network is 10.0.1.0 and you want to block all traffic going from this inside network to the Internet, the command would be **access-list 190 deny tcp 10.0.1.0 0.0.0.255 any eq 1524 log**.

However, blocking these ports may have an impact on regular network users because it may block some high port numbers that may be used by legitimate network clients. You may wish to wait to block these port numbers until a particular threat presents itself.

Note The permit ACL entry to allow the desired traffic is not shown in this example, for simplicity.

Distributed DoS Attack Mitigation: Stacheldraht

Stacheldraht is a distributed DoS tool that appeared in 1999 and combines features of TRIN00 and Tribe Flood Network (TFN). Stacheldraht also contains some advanced features, such as encrypted attacker-master communication and automated agent updates. The possible attacks are similar to those of TFN; namely, ICMP flood, SYN flood, UDP flood, and smurf attacks.



A Stacheldraht attack sets up communication between clients, handlers, and agents using these ports:

- 16660 tcp
- 65000 tcp

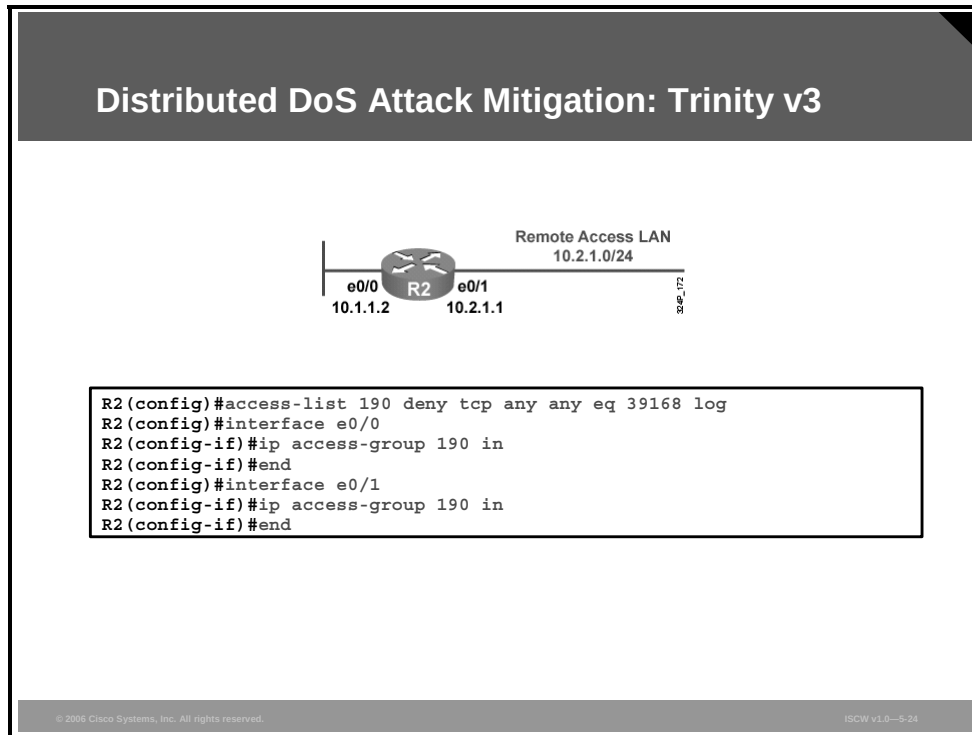
The figure shows an example that mitigates a Stacheldraht distributed DoS attack by blocking traffic on these ports.

Note The ports listed above are the default ports for the Stacheldraht tool. Use these ports for orientation and example only, because the port numbers can easily be changed.

Note The permit ACL entry to allow the desired traffic is not shown in this example, for simplicity.

Distributed DoS Attack Mitigation: Trinity v3

Trinity is capable of launching several types of flooding attacks on a victim site, including UDP, fragment, SYN, restore (RST), acknowledgement (ACK), and other floods. Communication from the handler or intruder to the agent is accomplished via Internet Relay Chat (IRC) or ICQ from AOL. Trinity appears to use primarily TCP port 6667 and also has a backdoor program that listens on TCP port 33270.

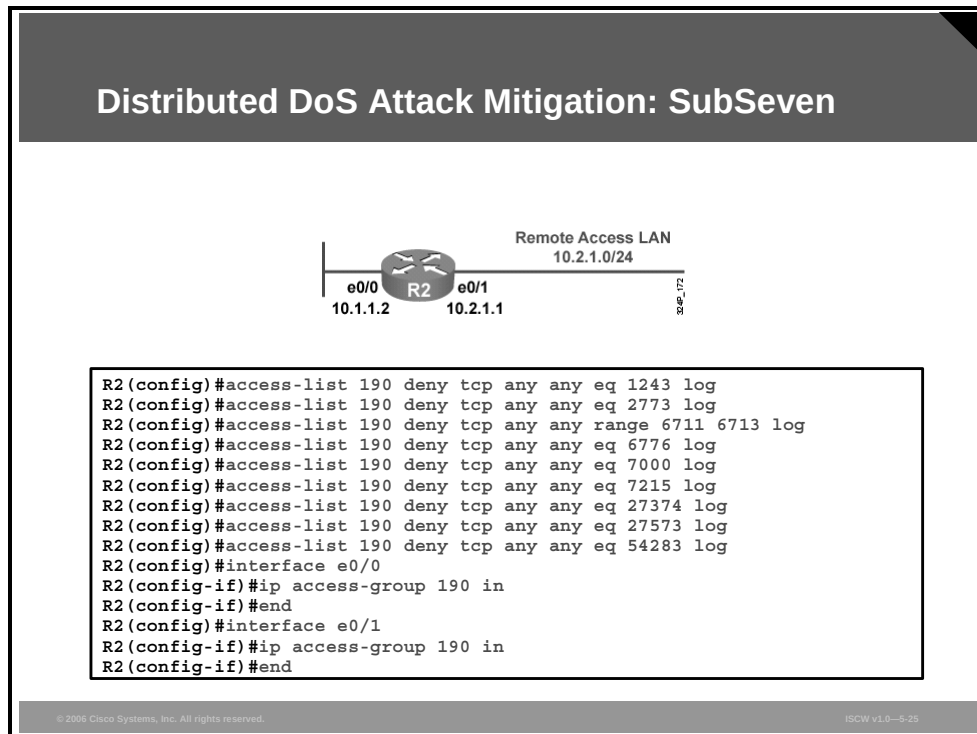


The figure shows an example that mitigates a Trinity v3 distributed DoS attack by blocking traffic on TCP port 33270.

Note The permit ACL entry to allow the desired traffic is not shown in this example, for simplicity.

Distributed DoS Attack Mitigation: SubSeven

Depending on the version, an attacker will try to exploit TCP ports 1243, 2773, 6711, 6712, 6713, 6776, 7000, 7215, 27374, 27573, and 54283.



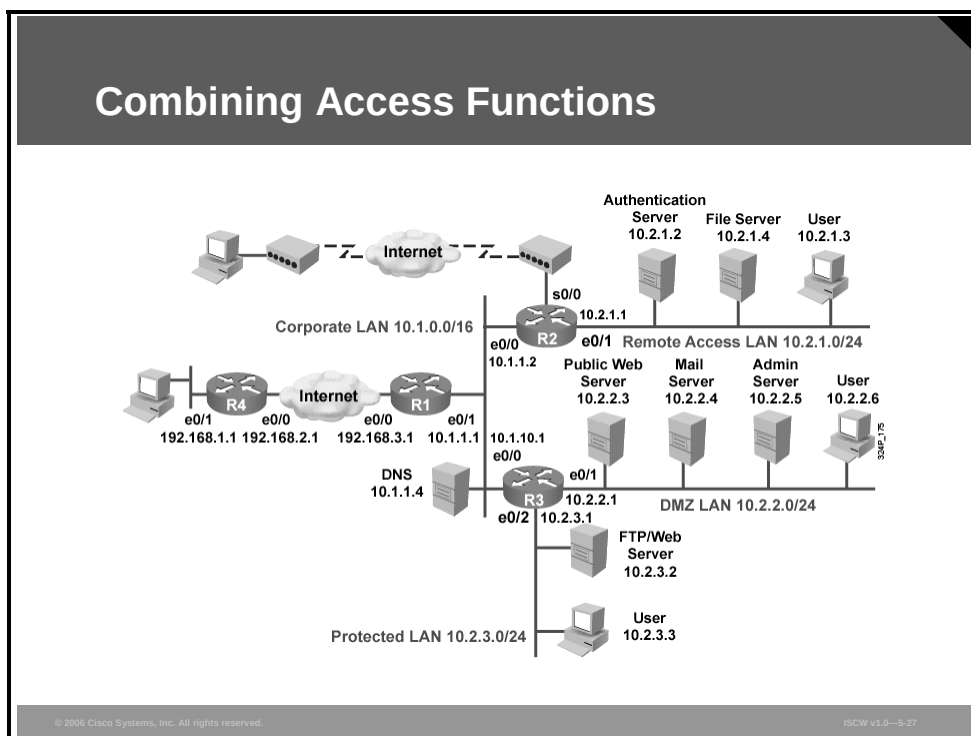
The figure shows an example that mitigates a SubSeven distributed DoS attack by blocking traffic on these ports:

- TCP—Range 6711 to 6712
- TCP—6776
- TCP—6669
- TCP—2222
- TCP—7000

Note The permit ACL entry to allow the desired traffic is not shown in this example, for simplicity.

Combining Access Functions

This topic describes how to combine many ACL functions into two or three larger ACLs.



This is an example of a possible configuration for Router R2 in the reference network. This partial configuration file contains several ACLs that contain most of the ACL features explained in this lesson. View this partial configuration as an example of how to integrate multiple ACL policies into a few main router ACLs.

The partial configuration file in the table shows how to combine many ACL functions into two or three larger ACLs.

Configuration	Description
<pre>hostname R2 ! interface Ethernet0/0 ip address 10.1.1.2 255.255.0.0 ip access-group 126 in ! interface Ethernet0/1 ip address 10.2.1.1 255.255.255.0 ip access-group 128 in ! router rip network 10.0.0.0 !</pre>	ACL 126 is applied to traffic flowing from external networks to the internal network or to the router itself. ACL 128 is applied to traffic flowing from the internal network to external networks or to the router itself.

Configuration	Description
no access-list 126 !	First, delete ACL 126 to make sure that you create a new ACL and do not append the configuration to an existing ACL.
access-list 126 deny ip 10.2.1.0 0.0.0.255 any log !	Prevent any IP packets containing the source address of any internal hosts or networks inbound to the private network.
access-list 126 deny ip 127.0.0.0 0.255.255.255 any log access-list 126 deny ip 0.0.0.0 0.255.255.255 any log access-list 126 deny ip 172.16.0.0 0.15.255.255 any log access-list 126 deny ip 192.168.0.0 0.0.255.255 any log access-list 126 deny ip 224.0.0.0 15.255.255.255 any log !	Prevent any IP packets containing the invalid source address, such as the local loopback, addresses starting with the first octet set to 0, RFC1918 private ranges (with the exception of 10.0.0.0/8, which is used in this network), or multicast addresses.
access-list 126 deny ip any host 10.2.1.255 log access-list 126 deny ip any host 10.2.1.0 log !	Deny packets destined to the network, and broadcast addresses of the remote access LAN.
access-list 126 permit tcp any 10.2.1.0 0.0.0.255 established !	Permit TCP return traffic to the remote access LAN.
access-list 126 deny icmp any any echo log access-list 126 deny icmp any any redirect log access-list 126 deny icmp any any mask-request log access-list 126 permit icmp any 10.2.1.0 0.0.0.255 !	Deny ICMP echo requests, ICMP redirects, and mask requests, and permit all other ICMP traffic to the remote access LAN.
access-list 126 permit udp 10.1.0.0 0.0.255.255 host 255.255.255.255 eq 512 !	Permit Routing Information Protocol (RIP) updates.
access-list 126 deny tcp any any eq 1524 log access-list 126 deny tcp any any eq 27665 log access-list 126 deny tcp any any eq 16660 log access-list 126 deny tcp any any eq 65000 log access-list 126 deny tcp any any eq 39168 log access-list 126 deny tcp any any eq 65000 log !	Block TRIN00, Stacheldraht, and Trinity.

Configuration	Description
access-list 126 permit tcp any eq 20 10.2.1.0 0.0.0.255 gt 1023 !	Permit initial packets from the FTP data sessions so that FTP clients in the remote access LAN can use FTP.
access-list 126 deny udp any any eq 27444 log access-list 126 deny udp any any eq 31335 log !	Block the TRIN00 UDP ports.
access-list 126 deny udp any any range 33400 34400 log !	Deny tracing of the remote access LAN.
access-list 126 permit udp any eq 53 10.2.1.0 0.0.0.255 gt 1023 !	Allow return DNS traffic.
access-list 126 deny tcp any range 0 65535 any range 0 65535 log access-list 126 deny udp any range 0 65535 any range 0 65535 log access-list 126 deny ip any any log !	Deny all remaining traffic and provide detailed logging information.
no access-list 128 !	Delete ACL 128 to make sure that you create a new ACL and do not append the configuration to an existing ACL.
access-list 128 permit icmp 10.2.1.0 0.0.0.255 any echo access-list 128 permit icmp 10.2.1.0 0.0.0.255 any parameter-problem access-list 128 permit icmp 10.2.1.0 0.0.0.255 any packet-too-big access-list 128 permit icmp 10.2.1.0 0.0.0.255 any source-quench !	Permit needed ICMP messages.
access-list 128 deny tcp any any range 1 19 log access-list 128 deny tcp any any eq 43 log access-list 128 deny tcp any any eq 93 log access-list 128 deny tcp any any range 135 139 log access-list 128 deny tcp any any eq 445 log access-list 128 deny tcp any any range 512 518 log access-list 128 deny tcp any any eq 540 log !	Block access to certain outside TCP services.
access-list 128 permit tcp 10.2.1.0 0.0.0.255 gt 1023 any lt 1024 access-list 128 permit udp 10.2.1.0 0.0.0.255 gt 1023 any eq 53 access-list 128 permit udp 10.2.1.0 0.0.0.255 any range 33400 34400 log !	Permit access to all remaining outside TCP services, to DNS (UDP/53), and allow tracing outside destinations.

Configuration	Description
<pre>access-list 128 deny tcp any range 0 65535 any range 0 65535 log access-list 128 deny udp any range 0 65535 any range 0 65535 log access-list 128 deny ip any any log</pre>	Deny all remaining access and provide detailed logging.

Caveats

This topic explains some of the caveats to be considered when building ACLs.

ACL Caveats	
Statement	Caveat
Implicit deny all	You may not see this statement but it does exist.
Standard ACL limitation	You may need to create extended ACLs to implement security policies.
Statement evaluation order	ACL statements are evaluated from top down, so always consider the order of the statements.
Order of ACL statements	Place more specific ACL statements higher in the ACL. Ensure that statements at the top of the ACL do not negate any statements found lower in the list.
Directional filtering	Always double-check the direction (inbound or outbound) of data that your ACL is filtering.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-29

There are several caveats to consider when working with ACLs:

- **Implicit deny all:** All Cisco ACLs end with an implicit deny all statement. Although you may not actually see this statement in your ACLs, it does exist.
- **Standard ACL limitation:** Because standard ACLs are limited to packet filtering on source addresses only, you may need to create extended ACLs to implement your security policies.
- **Statement evaluation order:** ACL statements are evaluated in a sequential, top-down order, starting with the first entry in the list. This means that it is very important to consider the order in which you place statements in your ACLs.
- **Specific statements:** Certain ACL statements are more specific than others and therefore should be placed higher in the ACL. For example; blocking all UDP traffic at the top of the list negates the blocking of SNMP packets lower in the list. Care must be taken that statements at the top of the ACL do not negate any statements found lower in the list.
- **Directional filtering:** Cisco ACLs have a directional filter that determines whether they examine inbound packets (toward the interface) or outbound packets (away from the interface). Always double-check the direction of data that your ACL is filtering.

ACL Caveats (Cont.)

Statement	Caveat
Modifying numbered ACLs	Adding new statements may require a new ACL to be created.
Special packets	If filtering router-generated packets is part of the security policy, they must be acted upon by inbound ACLs on adjacent routers or through other router filter mechanisms using ACLs.
Extended ACL placement	Always consider placing extended ACLs on routers as close as possible to the source being filtered.
Standard ACL placement	Always place standard ACLs as close to the destination as possible.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-30

- **Adding statements:** New statements added to an existing ACL are always appended to the bottom of the ACL. Because of the inherent top-down statement evaluation order of ACLs, these new entries may render the ACL unusable. In these cases, a new ACL must be created (with the correct statement ordering). Delete the old ACL and assign the new ACL to the router interface.
- **Special packets:** Router-generated packets, such as routing table updates, are not subject to outbound ACL statements on the source router. If filtering these types of packets is part of your security policy, then they must be acted upon by inbound ACLs on adjacent routers or through other router filter mechanisms using ACLs.
- **Extended ACL placement:** Extended ACLs that are placed on routers too far from the source being filtered can adversely impact packets flowing to other routers and interfaces. Always consider placing extended ACLs on routers as close as possible to the source being filtered.
- **Standard ACL placement:** Because standard ACLs filter packets based on the source address, placing these ACLs too close to the source can adversely impact packets destined to other destinations. Always place standard ACLs as close to the destination as possible.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Standard, extended, enhanced, named, and numbered ACLs can be created.**
- **Simple rules should be followed when creating ACLs.**
- **ACLs must be applied based on the direction of the data flow.**
- **ACLs can be used to filter traffic to mitigate security threats.**
- **ACLs can be used to mitigate distributed DoS attacks.**
- **Packets with source IP address within 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, or 240.0.0.0/4, should be denied on the ISP edge.**
- **Many ACL functions can be combined into two or three larger ACLs.**
- **Several caveats should be considered when creating ACLs.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-31

Securing Management and Reporting Features

Overview

This lesson describes how to securely implement the management and reporting features of syslog, Secure Shell (SSH) protocol, Simple Network Management Protocol version 3 (SNMPv3), and Network Time Protocol (NTP).

Objectives

Upon completing this lesson, you will be able to explain the procedures to securely implement management and reporting features of syslog, SSH, SNMPv3, and NTP. This ability includes being able to meet these objectives:

- Describe the factors you must consider when planning the secure management and reporting configuration of network devices
- Describe the factors that affect the architecture of secure management and reporting in terms of in-band and OOB information paths
- Describe the steps used to configure an SSH server for secure management and reporting
- Describe how the syslog function plays a key role in network security
- Describe how to configure syslog on Cisco routers using syslog router commands
- Describe the security features of SNMPv3
- Describe how to configure SNMPv3 on a Cisco IOS router or a switch
- Configure an NTP client including authentication in client mode
- Configure a Cisco router as an NTP server

Secure Management and Reporting Planning Considerations

This topic explains the factors you must consider when planning the secure management and reporting configuration of network devices.

Secure Management and Reporting Planning Considerations

- Which are the most important logs?
- How are important messages separated from routine notifications?
- How do you prevent tampering with logs?
- How do you make sure time stamps match?
- What log data is needed in criminal investigations?
- How do you deal with the volume of log messages?
- How do you manage all the devices?
- How can you track changes when attacks or network failures occur?

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-3

Configuring logging for your Cisco routers is a straightforward operation when your network contains only a few Cisco routers. However, logging and reading information from hundreds of devices can prove to be a challenging proposition. Too much information can be as bad as too little, and can raise these important questions:

- Which logs are most important?
- How do you separate important messages from mere notifications?
- How do you ensure that logs are not tampered with in transit?
- How do you ensure that time stamps match each other when multiple devices report the same alarm?
- What information is needed if log data is required for a criminal investigation?
- How do you deal with the volume of messages that can be generated by a large network?

Securing administrative access and device configurations is also a straightforward operation for smaller Cisco router networks. However, managing administrative access and device configurations for a large number of devices can raise these questions:

- How do you securely manage many devices in many locations?
- How can you track and troubleshoot changes on devices when attacks or network failures occur?

Each of these issues is specific to your needs. To identify the priorities of reporting and monitoring, input from management, as well as from the network and security teams, is required. The implemented security policy should also play a large role in answering these questions.

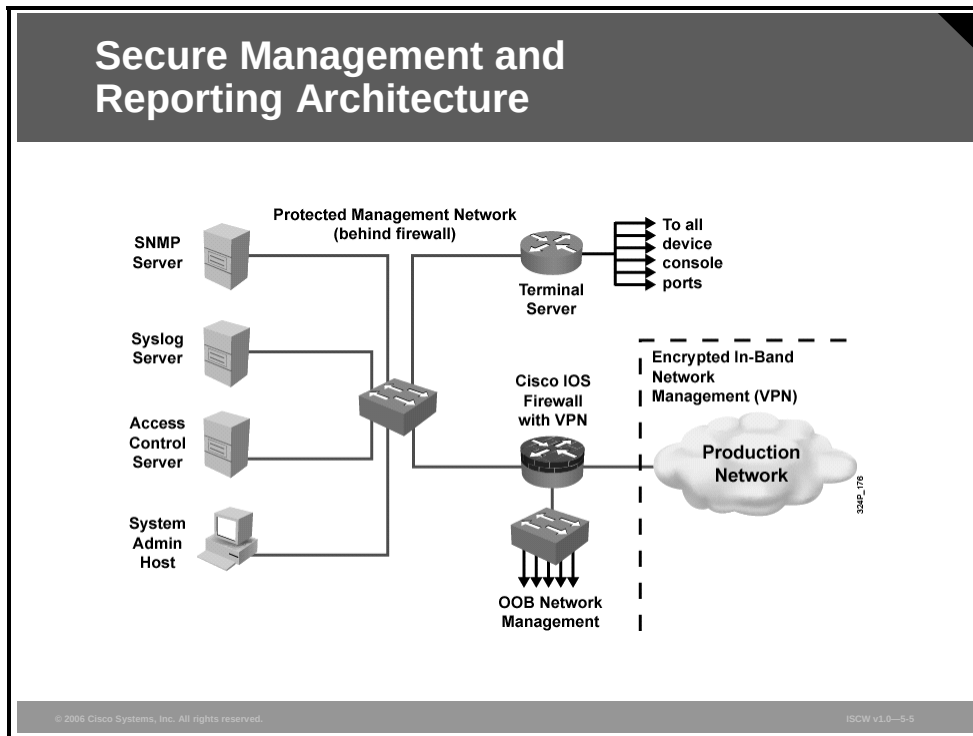
From a reporting standpoint, most networking devices can send syslog data when you are troubleshooting network problems or security threats. You can send this data to your syslog analysis host from any device whose logs you wish to view. This data can be viewed in real time, on demand, or in scheduled reports. Depending on the device involved, you can choose various logging levels to ensure that the correct amount of data is sent to the logging device. You must also flag device log data within the analysis software to permit granular viewing and reporting. For example, during an attack, the log data provided by Layer 2 switches might not be as interesting as the data provided by the intrusion detection system (IDS).

To ensure that log messages are time-synchronized, clocks on hosts and network devices must be synchronized. For devices that support it, NTP provides a way to ensure that accurate time is kept on all devices. When you are dealing with an attack, seconds matter, because it is important to identify the order in which a specified attack occurred.

Configuration change management is another issue related to secure management. When a network is under attack, it is important to know the state of critical network devices and when the last known modifications occurred. Creating a plan for change management should be a part of your comprehensive security policy, but, at a minimum, you should record changes using authentication systems on the devices, and archive configurations via FTP or TFTP.

Secure Management and Reporting Architecture

This topic describes factors that affect the architecture of secure management and reporting in terms of in-band and out-of-band (OOB) information paths.



The figure shows a management module with two network segments separated by a Cisco IOS router that acts as a firewall and a virtual private network (VPN) termination device. The segment outside the firewall connects to all the devices that require management. The segment inside the firewall contains the management hosts themselves and the Cisco IOS routers that act as terminal servers.

Information flow between management hosts and the managed devices can take two paths:

- **In-band:** Information flows across the enterprise production network or the Internet (or both).
- **OOB:** Information flows within a network on which no production traffic resides.

The connection to the production network is only provided for selective Internet access, limited in-band management traffic, and IPsec-protected management traffic from predetermined hosts. In-band management occurs only when a management application itself does not function out-of-band, or when the Cisco device being managed does not physically have enough interfaces to support the normal management connection. It is this latter case that employs IPsec tunnels. The Cisco IOS firewall is configured to allow syslog information into the management segment, as well as Telnet, SSH, and SNMP, if these services are first initiated by the inside network.

Both management subnets operate under an address space that is completely separate from the rest of the production network. This practice ensures that the management network is not advertised by any routing protocols, and it enables the production network devices to block any traffic from the management subnets that appear on the production network links.

Any in-band management or Internet access occurs through a Network Address Translation (NAT) process on the Cisco IOS router that translates the nonroutable management IP addresses to previously determined production IP address ranges.

The management module provides configuration management for nearly all devices in the network using two primary technologies:

- **Cisco IOS routers acting as terminal servers:** The routers provide a reverse Telnet function to the console ports on the Cisco devices throughout the enterprise.
- **Dedicated management network segment:** More extensive management features (such as software changes, content updates, log and alarm aggregation, and SNMP management) are provided through the dedicated management network segment.

Because the management network has administrative access to nearly every area of the network, it can be a very attractive target to hackers. The management module was built with several technologies designed to mitigate those risks.

The first primary threat is a hacker attempting to gain access to the management network itself. This threat can be mitigated only through effective deployment of security features in the remaining enterprise modules.

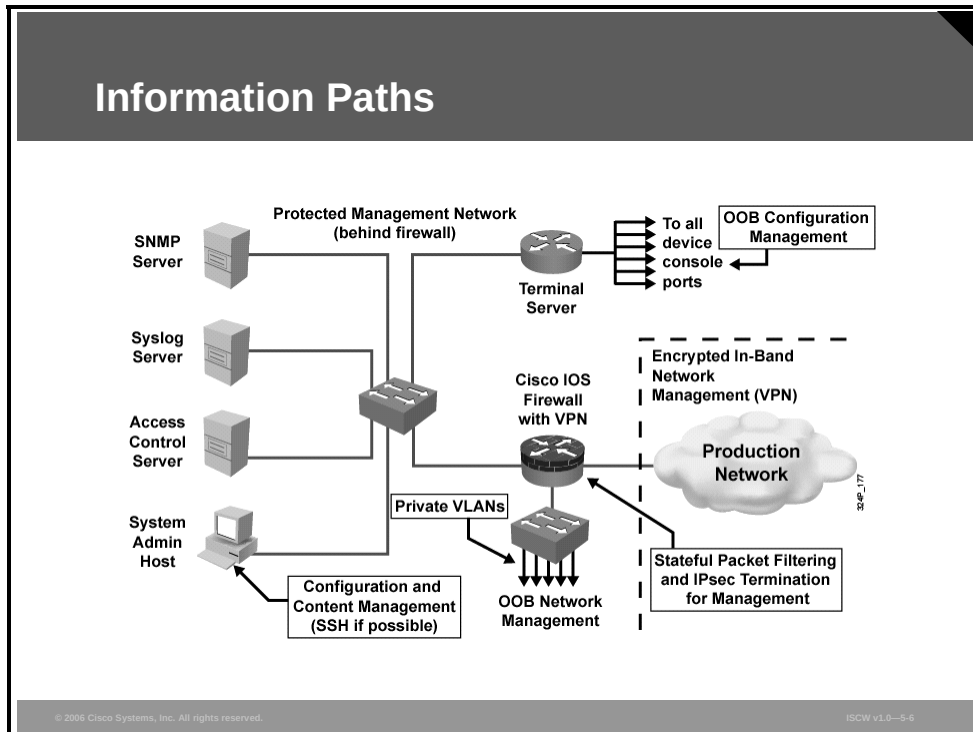
The other threats assume that the primary line of defense has been breached. To mitigate the threat of a compromised device, access control is implemented at the firewall and at every other possible device to prevent exploitation of the management channel. A compromised device cannot even communicate with other hosts on the same subnet because private VLANs (PVLANS) on the management segment switches force all traffic from the managed devices directly to the Cisco IOS firewall, where filtering takes place. Password sniffing reveals only useless information because of the One Time Password (OTP) environment. Use SNMPv3 wherever possible because SMNPv3 supports authentication and encryption.

SNMP management has its own set of security needs. Keeping SNMP traffic on the management segment allows the traffic to traverse an isolated segment when it pulls management information from devices. In Cisco self-defending network topology, SNMP management only pulls information from devices rather than being allowed to push changes. To ensure that management information is pulled, each device is configured with a *read-only* string. You may configure SNMP *read-write* when using an OOB network, but be aware of the increased security risk of a plaintext string allowing modification of device configurations.

Proper aggregation and analysis of syslog information is critical for proper management of a network. From a security perspective, syslog provides important information about security violations and configuration changes. Depending on the device in question, different levels of syslog information might be required. Having full logging with all messages sent might provide too much information for an individual or syslog analysis algorithm to sort. Logging for the sake of logging does not improve security.

Information Paths

Network administrators need to securely manage all devices and hosts in the network. Logging and reporting information flow from devices to management hosts, while content, configurations, and new software flow from the management hosts to the devices.



From an architectural perspective, providing OOB management of network systems is the best first step in any management and reporting strategy. Devices should have a direct local connection to such a network wherever possible; and where this is not possible because of geographic or system-related issues, the device should connect via a private encrypted tunnel over the production network. Such a tunnel should be preconfigured to communicate only across specific ports required for management and reporting. The tunnel should also be locked down so that only appropriate hosts can initiate and terminate the tunnel.

OOB management is not always desirable. Often, the decision depends on the type of management application that you are running, and the protocols that are required. For example, consider a management tool whose goal is determining the reachability of all devices on the production network. If a critical link between two core switches fails, you would want this management console to alert an administrator. If this management application is configured to use an OOB network, it may never determine that the link has failed, because the OOB network makes all devices appear to be attached to a single network. It is preferable to run this kind of management application in-band. In-band management must be configured as securely as possible.

In-Band Management Considerations

This section describes issues to be considered when designing an in-band management solution.

In-Band Management Considerations

- Which management protocols does each device support?
- Does the management channel need to be active at all times?
- Is SNMP necessary?

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5.7

When in-band management of a device is required, you should consider these questions:

- **Which management protocols does the device support?** Devices with IPsec should be managed by simply creating a tunnel from the management network to the device. This setup allows many insecure management protocols to flow over a single encrypted tunnel. When IPsec is not possible because it is not supported on a device, other less-secure options must be chosen. For configuration of the device, SSH or Secure Sockets Layer (SSL) can often be used instead of Telnet to encrypt configuration modifications made to a device. These protocols can sometimes also be used to push and pull data to and from a device instead of insecure protocols, such as FTP and TFTP. Often, however, TFTP is required on Cisco equipment to back up configurations or to update software versions. This fact leads to the second question.
- **Does the management channel need to be active at all times?** If not, temporary holes can be placed in a firewall while the management functions are performed, and then later removed. This process, however, does not scale with a large number of devices, and should be used sparingly, if at all, in enterprise deployments. If the channel needs to be active at all times, such as with SNMP, the third question should be considered.
- **Do you really need this management tool?** Often, SNMP management tools are used on the inside of a network to ease troubleshooting and configuration. However, SNMP should be treated with the utmost care because the underlying protocol has its own set of security vulnerabilities. If SNMP is required, consider providing read-only access to devices via SNMP, and treat the SNMP community string with the same care you might use for a root password on a critical UNIX host. By introducing SNMP into your production network, you introduce a potential vulnerability into your environment. And finally, if you do need the tool, use SNMPv3 authentication and encryption features.

Secure Management and Reporting Guidelines

The figure lists guidelines for in-band and OOB management of the network .

Secure Management and Reporting Guidelines

- **In-band management guidelines:**
 - Apply only to devices needing to be managed or monitored.
 - Use IPsec when possible.
 - Use SSH or SSL instead of Telnet.
 - Decide whether the management channel needs to be open at all times.
 - Keep clocks on hosts and network devices synchronized.
 - Record changes and archive configurations.
- **OOB management guidelines:**
 - Provide highest level of security and mitigate the risk of passing insecure management protocols over the production network.
 - Keep clocks on hosts and network devices synchronized.
 - Record changes and archive configurations.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-8

As a general rule, OOB management is appropriate for large enterprise networks. In smaller networks, in-band management is recommended as a means of achieving a more cost-effective security deployment. In smaller architectures, management traffic flows in-band in all cases, and is made as secure as possible by using tunneling protocols and secure variants to insecure management protocols (for example, SSH is used whenever possible instead of Telnet).

To ensure that log messages are time-synchronized, clocks on hosts and network devices must be synchronized. For devices that support it, NTP provides a way to ensure that accurate time is kept on all devices. When you are dealing with an attack, seconds matter, because it is important to identify the order in which a specified attack occurred. 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. The private network should then be synchronized to Coordinated Universal Time (UTC) via satellite or radio. However, clock sources are available that synchronize via the Internet. Such clocks should be used by network administrators who do not wish to implement their own master clocks because of cost or other reasons.

An attacker could attempt a denial of service (DoS) attack on a network by sending bogus NTP data across the Internet in an attempt to change the clocks on network devices so that digital certificates are 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. NTP version 3 and above supports a cryptographic authentication mechanism between peers. The use of the authentication mechanism, as well as the use of access control lists (ACLs) that specify which network devices are allowed to synchronize with other network devices, is recommended to help mitigate such an attack.

The network administrator should weigh the cost benefits of pulling the clock time from the Internet with the possible risk of allowing unsecured packets through the firewall. Many NTP servers on the Internet do not require any authentication of peers. Therefore, the network administrator must trust that the clock itself is reliable, valid, and secure. NTP uses User Datagram Protocol (UDP) port 123.

Configuring an SSH Server for Secure Management and Reporting

This topic describes the steps used to configure an SSH server for secure management and reporting.

Configuring an SSH Server for Secure Management and Reporting

```
Austin2#configure terminal
Austin2(config)#ip domain-name cisco.com
Austin2(config)#crypto key generate rsa general-keys modulus 1024

Sept 22 13:20:45: %SSH-5-ENABLED: SSH 1.5 has been enabled

Austin2(config)#ip ssh timeout 120
Austin2(config)#ip ssh authentication-retries 4
Austin2(config)#line vty 0 4
Austin2(config-line)#no transport input telnet
Austin2(config-line)#transport input ssh
Austin2(config-line)#end
```

1. Configure the IP domain name
2. Generate the RSA keys
3. Configure the SSH timeout interval
4. Configure the SSH retries
5. Disable vty inbound Telnet sessions
6. Enable vty inbound SSH sessions

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0-5.10

You should use SSH instead of Telnet to manage your Cisco routers whenever possible. SSH version 1 (SSHv1) is supported in Cisco IOS software Release 12.1(1)T and later, while SSH version 2 (SSHv2) is supported in Cisco IOS software Release 12.3(4)T and later. Cisco routers configured for SSH act as SSH servers. You must provide an SSH client, such as PuTTY, OpenSSH, or TeraTerm, for the administrator workstation that you wish to use to configure and manage routers using SSH.

Note Cisco routers with Cisco IOS software Releases 12.1(3)T and later can act as SSH clients as well as SSH servers. This means that you could initiate an SSH client-to-server session from your router to a central SSH server system. SSH employs strong encryption to protect the SSH client-to-server session. Unlike Telnet, where anyone with a sniffer can see exactly what you are sending and receiving from your routers, SSH encrypts the entire session.

Complete these tasks before configuring your routers for SSH server operations:

- Ensure that the target routers are running a Cisco IOS software Release 12.1(1)T image or later with the IPsec feature set. Only Cisco IOS software images containing the IPsec feature set support an SSH server.
- Ensure that the target routers are configured for local authentication, AAA server for username/password authentication, or both.
- Ensure that each of the target routers has a unique hostname.
- Ensure that each of the target routers is using the correct domain name of your network.

Complete these steps to configure your Cisco router to support SSH server:

- Step 1** Configure the IP domain name of your network using the **ip domain-name** command in global configuration mode:
- ```
Austin2 (config) #ip domain-name cisco.com
```
- Step 2** Generate keys to be used with SSH by generating the RSA keys using the **crypto key generate rsa** command in global configuration mode:
- ```
Austin2 (config) #crypto key generate rsa general-keys modulus 1024
```

Note It is recommended that you use a minimum key length of modulus 1024.

- Step 3** Optionally, to display the generated keys, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.
- Step 4** Configure the time that the router waits for the SSH client to respond using the **ip ssh timeout** command in global configuration mode:
- ```
Austin2 (config) #ip ssh timeout 120
```
- Step 5** Configure the SSH retries using the **ip ssh authentication-retries** command in global configuration mode:
- ```
Austin2 (config) #ip ssh authentication-retries 4
```

Caution Be sure to disable Telnet transport input on all of the router vty lines or the router will continue to allow insecure Telnet sessions.

- Step 6** Disable vty inbound Telnet sessions:
- ```
Austin2 (config) #line vty 0 4
Austin2 (config-line) #no transport input telnet
```
- Step 7** Enable vty inbound SSH sessions:
- ```
Austin2 (config-line) #transport input ssh
```

The SSH protocol is automatically enabled once you generate the SSH (RSA) keys, as shown in the figure. Once the keys are created, you may access the router SSH server using your SSH client software.

The procedure for connecting to a Cisco router SSH server varies depending on the SSH client application that you are using. Generally, the SSH client passes your username to the router SSH server. The router SSH server prompts you for the correct password. Once the password has been verified, you can configure and manage the router as if you were a standard vty user.

Using Syslog Logging for Network Security

This topic describes how the syslog function plays a key role in network security.

Implementing Log Messaging for Security

- **Routers should be configured to send log messages to one or more of these:**
 - Console
 - Terminal lines
 - Memory buffer
 - SNMP traps
 - Syslog
- **Syslog logging is a key security policy component.**

© 2006 Cisco Systems, Inc. All rights reserved.

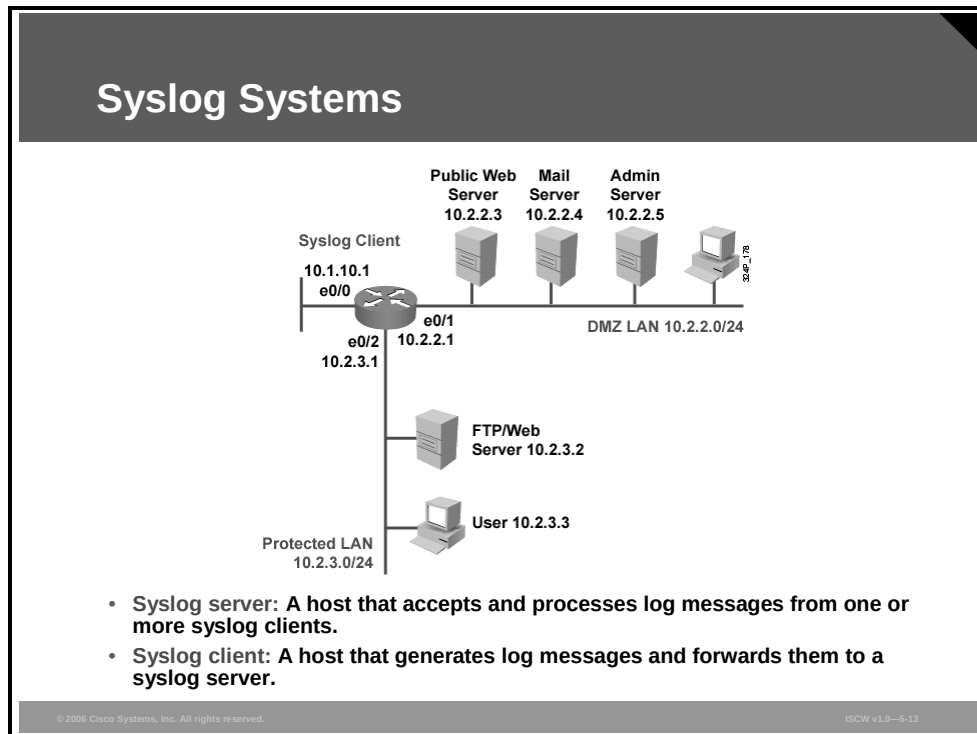
ISCW v1.0--5.12

Implementing a router logging facility is an important part of any network security policy. Cisco routers can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Cisco routers can direct log messages to several different facilities. You should configure the router to send log messages to one or more of the following:

- **Console:** Console logging is used when modifying or testing the router while it is connected to the console. Messages sent to the console are not stored by the router, and are, therefore, not very valuable as security events.
- **Terminal lines:** Enabled EXEC sessions can be configured to receive log messages on any terminal lines. Similar to console logging, this type of logging is not stored by the router and is, therefore, only valuable to the user on that line.
- **Memory buffer:** You may direct a router to store log messages in router memory. Buffered logging is a bit more useful as a security tool, but has the drawback of having events cleared whenever the router is booted.
- **SNMP traps:** Certain router events may be processed by the router SNMP agent, and forwarded as SNMP traps to an external SNMP host. This is a viable security logging facility, but requires the configuration and maintenance of an SNMP system.
- **Syslog:** Cisco routers can be configured to forward log messages to an external syslog service. This service may reside on any number of servers, including Microsoft Windows and UNIX-based systems. Syslog is the most popular message logging facility because it provides long-term log storage capabilities and a central location for all router messages.

Syslog Systems

Syslog is a standard for logging system events.



As shown in the figure, syslog implementations contain two types of systems:

- **Syslog servers:** These systems, also known as log hosts, accept and process log messages from syslog clients.
- **Syslog clients:** Syslog clients are routers or other types of Cisco equipment that generate and forward log messages to syslog servers.

Note Using router logs can become very difficult if your router clocks are not running the proper time. It is recommended that you use an NTP facility to ensure that all of your routers are operating at the correct time.

Cisco Log Severity Levels

Cisco router log messages fall into one of eight levels as shown in the figure.

Cisco Log Severity Levels		
Level	Name	Description
0	Emergencies	Router unusable
1	Alerts	Immediate action required
2	Critical	Condition critical
3	Errors	Error condition
4	Warnings	Warning condition
5	Notifications	Normal but important event
6	Informational	Informational message
7	Debugging	Debug message

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-14

The lower the level number, the higher the severity level, as shown in the table.

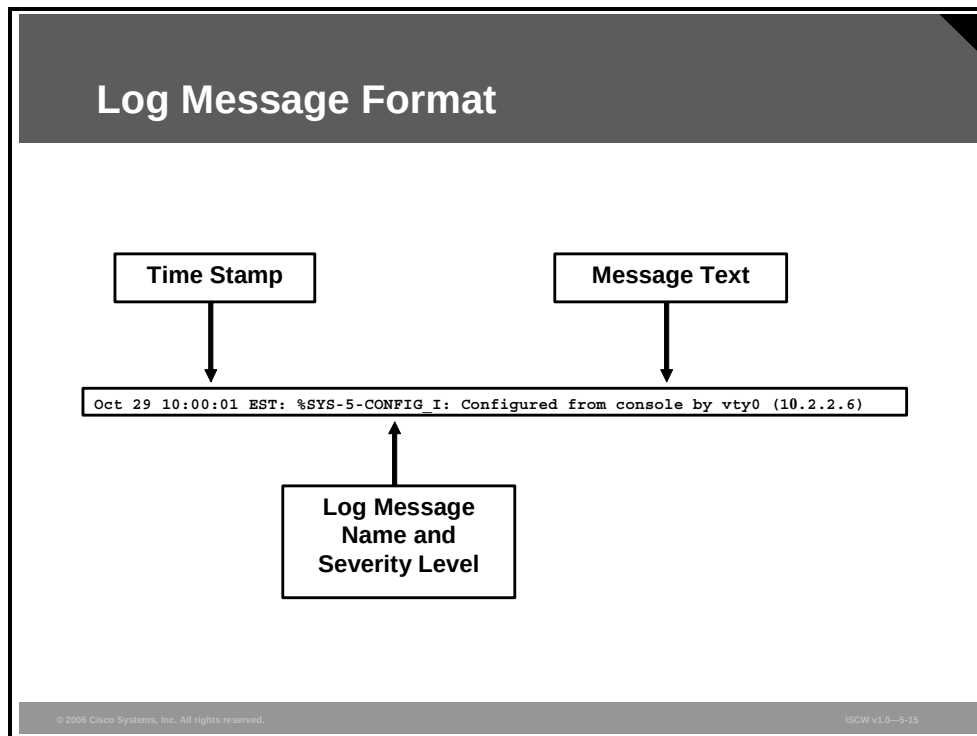
Cisco Log Severity Levels

Syslog Level	Definition	Example
0 LOG_EMERG	A panic condition normally broadcasted to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions, for example, hard device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Conditions that are not error conditions, but should possibly be handled specially	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information normally of use only when debugging a program	Packet type invalid

Note When entering logging levels in commands in Cisco IOS software Release 11.3 and earlier, you must specify the level name. Cisco IOS software Release 12.0 and later support using the level number or the level name, or both the number and the name.

Log Message Format

This section describes the log message format.



Cisco router log messages contain three main parts:

- Time stamp
- Log message name and severity level
- Message text

The figure shows a syslog entry example for a level 5 syslog message indicating that someone has configured the router from the vty 0 port.

Note	The log message name is not the same as a severity level name.

Configuring Syslog Logging

This topic describes how to configure syslog on Cisco routers.

Configuring Syslog

```
Router(config)#  
logging [host-name | ip-address]
```

1. Sets the destination logging host

```
Router(config)#  
logging trap level
```

2. (Optional) Sets the log severity (trap) level

```
Router(config)#  
logging facility facility-type
```

3. (Optional) Sets the syslog facility

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.17

Complete these five steps to implement syslog on your Cisco routers:

- Step 1** **Configure log hosts:** You must configure the router to send log messages to one or more syslog servers (log hosts). There is no maximum number of log hosts supported by Cisco routers, but usually only one or two are needed. Log hosts are identified by their host name or IP address. Use the **logging** command in global configuration mode to set the destination (log) hosts.

logging [host-name | ip-address]

logging Parameters

Parameter	Description
host-name	The name of the host to be used as a syslog server
ip-address	The IP address of the host to be used as a syslog server

- Step 2** **(Optional) Set the log severity (trap) level:** Setting the log severity level limits the error messages sent to syslog servers to only those at the specified level. Default value is severity level 6. Use the **logging trap** command in global configuration mode to set the severity level.

logging trap level

logging trap Parameter

Parameter	Description
<i>level</i>	Limits the logging of messages to the syslog servers to a specified level. You can enter the level number (0 to 7) or level name.

Step 3 (Optional) Set the syslog facility: You must configure the syslog facility in which error messages are sent. The eight commonly used syslog facility names for Cisco routers are local0 through local7. Default value is facility local7. Use the **logging facility** command in global configuration mode to set the syslog facility.

logging facility *facility-type*

logging facility Parameter

Parameter	Description
<i>facility-type</i>	The syslog facility type (local0 to local7)

Configuring Syslog (Cont.)

Router(config)#

`logging source-interface interface-type interface-number`

4. (Optional) Sets the source interface

Router(config)#

`logging on`

5. Enables logging

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5.18

- Step 4 (Optional) Set the source interface:** By default, syslog messages are sent using the IP address of the source interface. You should specify the source IP address of syslog packets, regardless of the interface where the packets actually exit the router. Use the **logging source-interface** command in global configuration mode to set the source interface.

logging source-interface *interface-type interface-number*

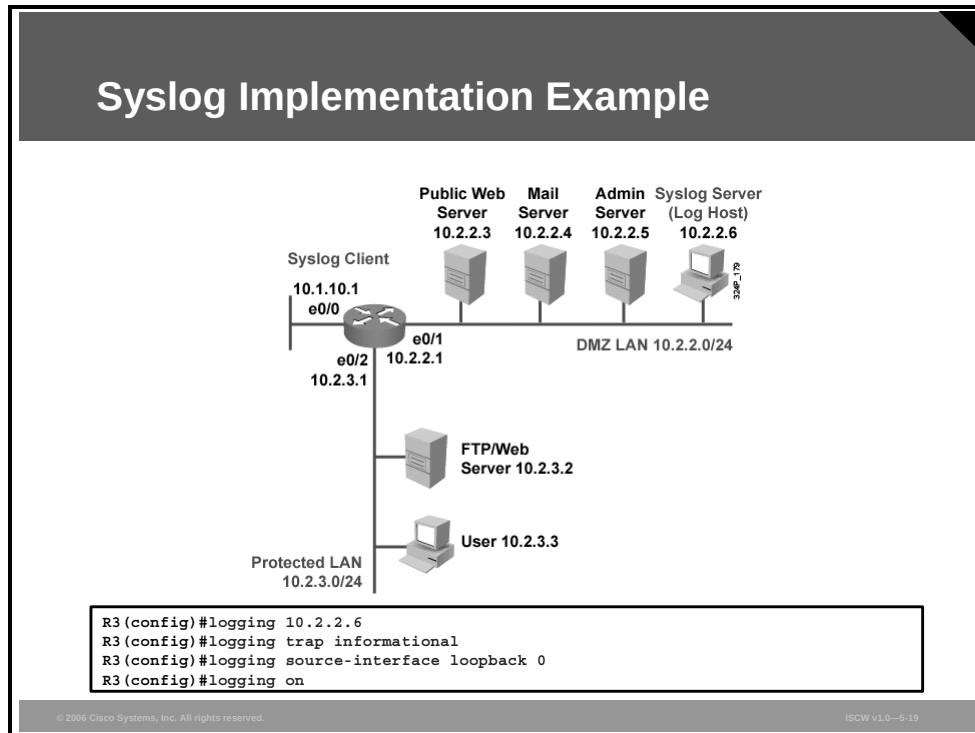
logging source-interface Parameters

Parameter	Description
<i>interface-type</i>	The interface type (for example, Ethernet)
<i>interface-number</i>	The interface number (for example, 0/1)

- Step 5 Enable logging:** Make sure that the router logging process is enabled using the **logging on** command in global configuration mode. The **logging on** command has no arguments or keywords.

Example: Syslog Implementation

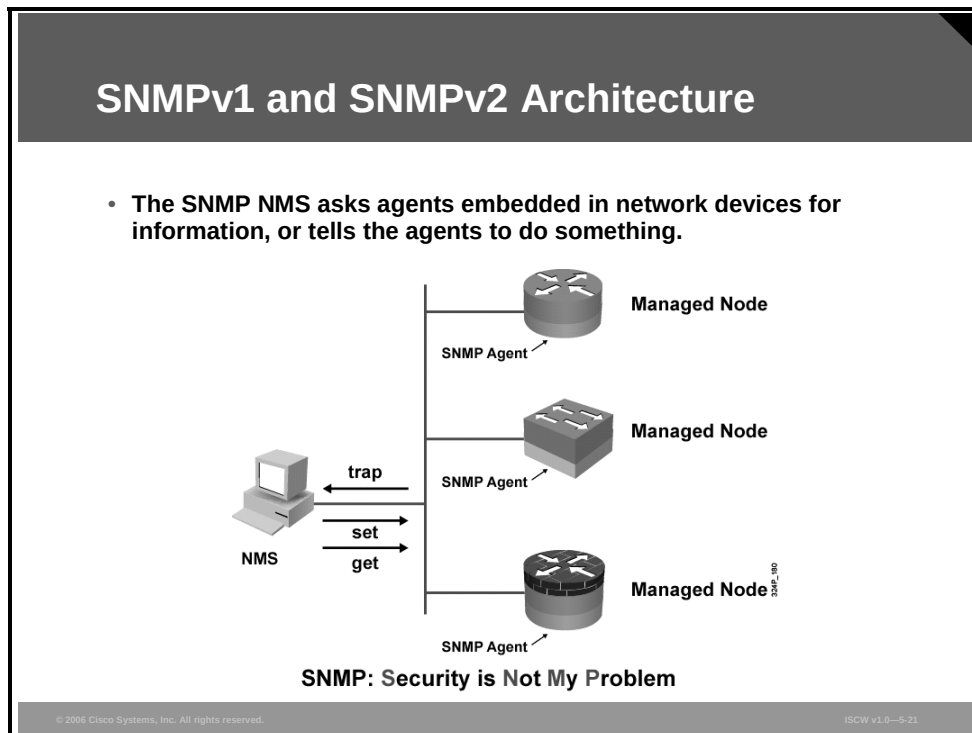
The figure contains an example of configuring syslog for router R3 using the commands previously described.



In this example, the administrator wishes to log all events that occur on the router except the debugging (level 7) information. An example of an informational level (level 6) event is an ACL hit. The router will send the messages from level 6 and all more critical levels (0–5) to the syslog server with the IP address 10.2.2.6.

SNMP Version 3

This topic describes the security features of SNMPv3.



SNMP was developed to manage nodes (servers, workstations, routers, switches, hubs, and security appliances) on an IP network. All versions of SNMP are application layer protocols that facilitate the exchange of management information between network devices. SNMP is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMPv1 and SNMPv2 are based on three concepts:

- **Managers:** In any configuration, at least one manager node runs SNMP management software.
- **Agents:** Network devices that need to be managed, such as bridges, switches, routers, servers, and workstations, are equipped with an agent software module.
- **MIB:** The agent is responsible for providing access to a local MIB of objects that reflects the resources and activity at its node.

The SNMP manager can retrieve (get) information from the agent, or change (set) information in the agent. Sets can change variables (settings and configuration) in the agent device, or initiate actions in devices. A reply to a set indicates the new setting in the device. For example, a set can cause a router to reboot, or to send or receive a configuration file.

Network devices send “traps” to the SNMP manager to indicate that an event or incident has occurred within the network device.

The actions *gets* and *sets* are the vulnerabilities that open SNMP to an attack.

Community Strings

SNMPv1 and SNMPv2 use a community string to access router SNMP agents.

Community Strings

Used to authenticate messages between a management station, and an SNMPv1 or SNMPv2 engine:

- **Read only community strings** can get information, but can not set information in an agent.
- **Read-write community strings** can get and set information in the agent.
- **Having read-write access** is like having the enable password for the device.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-22

SNMP community strings act like passwords. An SNMP community string is a text string used to authenticate messages between a management station and an SNMP engine:

- If the manager sends one of the correct read-only community strings, it can get information, but not set information in an agent.
- If the manager uses one of the correct read-write community strings, it can get or set information in the agent.

In effect, having read-write access is equivalent to having the enable password.

SNMP agents accept commands and requests only from SNMP systems using the correct community string. By default, most SNMP systems use a community string of “public.” If you configure your router SNMP agent to use this commonly known community string, anyone with an SNMP system is able to read the router MIB. Because router MIB variables can point to things like routing tables and other security-critical parts of the router configuration, it is important that you create your own custom SNMP community strings.

SNMP Security Models and Levels

A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

SNMP Security Models and Levels				
Definitions:				
• Security model is a security strategy used by the SNMP agent • Security level is the permitted level of security within a security model				
Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	• Authenticates with a community string match
v2	noAuthNoPriv	Community String	No	• Authenticates with a community string match
v3	noAuthNoPriv	Username	No	• Authenticates with a username
	authNoPriv	MD5 or SHA	No	• Provides HMAC MD5 or SHA algorithms for authentication
	authPriv	MD5 or SHA	DES	• Provides HMAC MD5 or SHA algorithms for authentication • Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-23				

A security model is an authentication strategy that is set up for a user and the group in which the user resides. Currently, Cisco IOS software supports three security models: SNMPv1, SNMPv2, and SNMPv3.

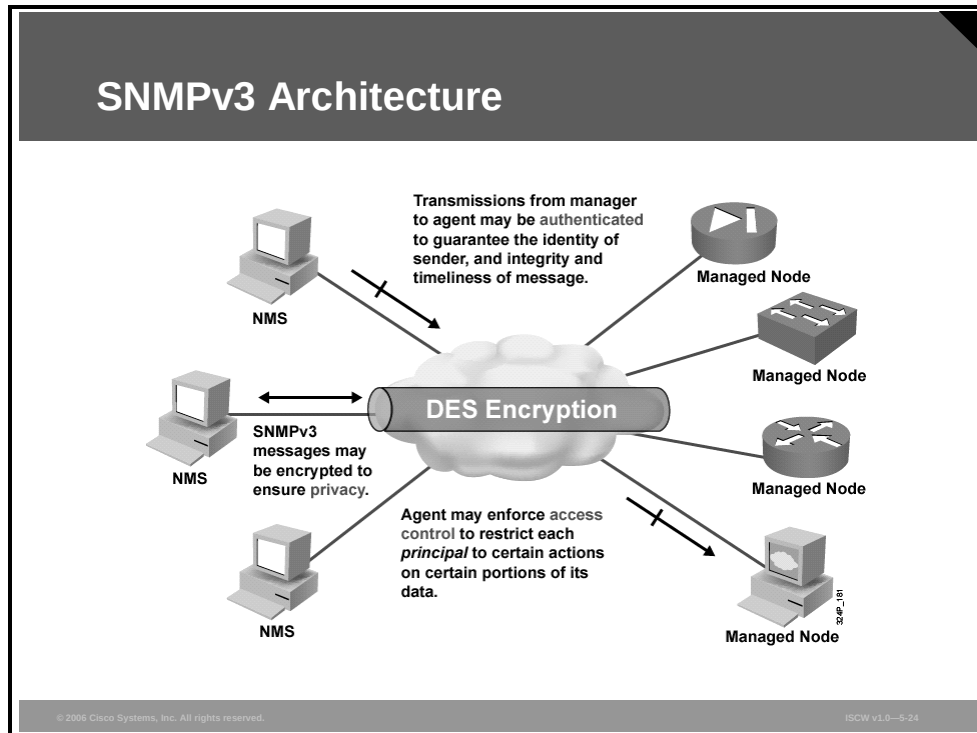
A security level is the permitted level of security within a security model. The security level is a type of security algorithm performed on each SNMP packet. There are three security levels:

- **noAuth:** Authenticates a packet by a string match of the user name or community string.
- **Auth:** Authenticates a packet by using either the Hash-based Message Authentication Codes (HMACs) with Message Digest 5 (MD5) (RFC 2104) or Secure Hash Algorithms (SHAs).
- **Priv:** Authenticates a packet by using either the HMAC MD5 or SHAs, and encrypts the packet using the Cipher Block Chaining-Data Encryption Standard (CBC-DES) (DES-56) algorithm.

SNMPv3 adds security and remote configuration capabilities to the previous versions. SNMPv3 provides three security model and security level options. The table in the figure identifies the combinations of security models and levels.

SNMPv3 Architecture

In its natural evolution, the current version of SNMPv3 addresses the vulnerabilities of earlier versions by including three important services: authentication, privacy, and access control.

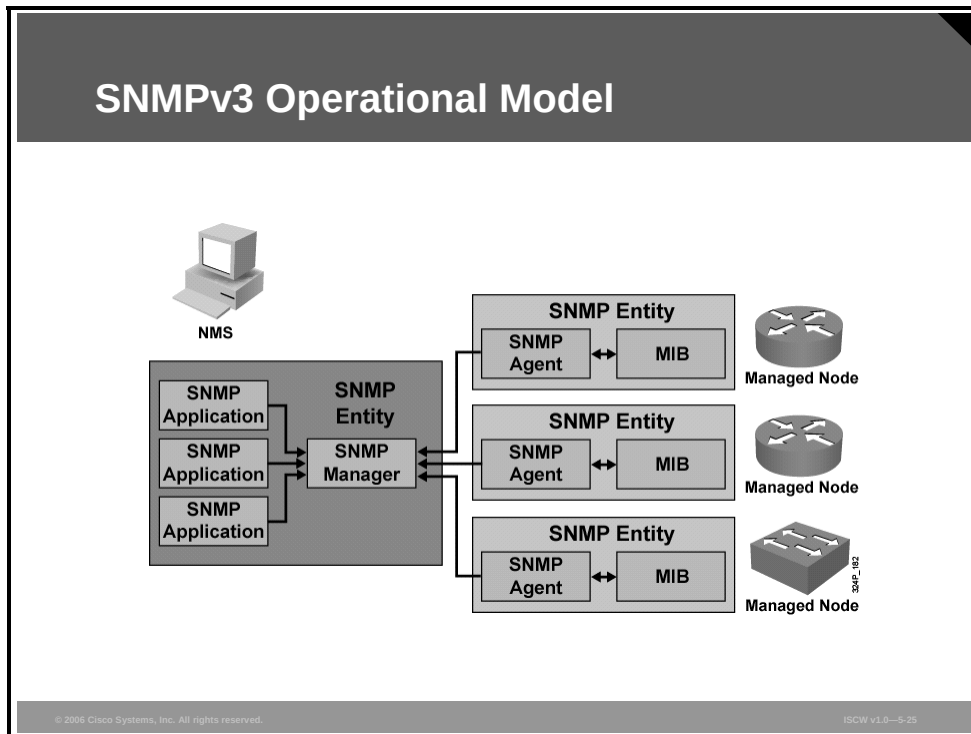


SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- **Message integrity:** Ensuring that a packet has not been tampered with in transit
- **Authentication:** Determining that the message is from a valid source
- **Encryption:** Scrambling the content of a packet to prevent it from being seen by an unauthorized source

SNMPv3 Operational Model

The concepts of separate SNMP agents and SNMP managers do not apply in SNMPv3. These concepts have been combined into single SNMP entities.



Each managed node and the NMS is a single entity. There are two types of entities, each containing different applications:

- **Managed node SNMP entities:** The managed node SNMP entity includes an SNMP agent and an SNMP MIB. The agent implements the SNMP protocol, and allows a managed node to provide information to the NMS and accept instructions from it. The MIB defines the information that can be collected and used to control the managed node. Information exchanged using SNMP takes the form of objects from the MIB.
- **SNMP NMS entities:** The SNMP entity on an NMS includes an SNMP manager and SNMP applications. The manager implements the SNMP protocol, and collects information from managed nodes and sends instructions to them. The SNMP applications are software applications used to manage the network.

SNMPv3 Features and Benefits

The figure summarizes the features and benefits of SNMPv3.

SNMPv3 Features and Benefits	
Features	• Message integrity: Ensures that a packet has not been tampered with in transit. • Authentication: Determines that the message is from a valid source. • Encryption: Scrambles the contents of a packet to prevent it from being seen by an unauthorized source.
Benefits	• Data can be collected securely from SNMP devices without fear of the data being tampered with or corrupted. • Confidential information, such as, SNMP Set command packets that change a router configuration, can be encrypted to prevent its contents from being exposed on the network.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-25

It is strongly recommended that all network management systems use SNMPv3 rather than SNMPv1 or SNMPv2.

Configuring an SNMP Managed Node

This topic explains how to configure SNMPv3 on a Cisco IOS router or a switch.

SNMPv3 Configuration Task List

Cisco IOS SNMPv3 server configuration tasks:

1. **Configuring the SNMP-server engine ID**
2. **Configuring the SNMP-server group names**
3. **Configuring the SNMP-server users**
4. **Configuring the SNMP-server hosts**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-28

Four configuration tasks are used to set up SNMPv3 communications on a Cisco IOS router:

1. Configuring the SNMP-server engine ID to identify the devices for administrative purposes
2. Configuring the SNMP-server group names for grouping SNMP users
3. Configuring the SNMP-server users to define usernames that reside on hosts that connect to the local agent
4. Configuring the SNMP-server hosts to specify the recipient of a notification operation (trap or inform)

Configuring the SNMP-Server Engine ID

To configure a name for either the local or remote SNMP engine on the router, use the **snmp-server engineID** global configuration command.

To remove a specified SNMP engine ID, use the **no** form of this command.

Configuring the SNMP-Server Engine ID

```
Router(config)#  
snmp-server engineID [local engineid-string] | [remote  
ip-address udp-port port-number engineid-string]
```

- Configures names for both the local and remote SNMP engine (or copy of SNMP) on the router

```
PR1(config)#snmp-server engineID local 1234
```

© 2006 Cisco Systems, Inc. All rights reserved.ISCW v1.0—5-23

snmp-server engineID [**local** *engineid-string*] | [**remote** *ip-address* **udp-port** *port-number* *engineid-string*]

snmp-server engineID Parameters

Parameter	Description
local	(Optional) Specifies the local engine ID of the router.
<i>engineid-string</i>	(Optional) The name of the SNMP engine.
remote	(Optional) Specifies the engine ID of a remote SNMP device.
<i>ip-address</i>	(Optional) The IP address of the remote SNMP device.
udp-port	(Optional) Specifies a UDP port of the host to use.
<i>port-number</i>	(Optional) This is the socket number on the remote SNMP device. The default value is 161.

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do not need to specify an engine ID for the device; a default string is generated using a Cisco enterprise number (1.3.6.1.4.1.9) and the MAC address of the first interface on the device.

If you wish to specify your own ID, you do not need to specify the entire 24-character engine ID, if it contains trailing zeros. Specify only a portion of the engine ID up to the point at which only zeros remain in the value. This portion must be 10 hexadecimal characters or more. For example, to configure an engine ID of 1234000000000000000000, you can specify **snmp-server engineID local 1234000000**.

A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. Informs are acknowledged traps. The agent sends an inform to the manager. When the manager receives the inform, it sends a response to the agent. Thus, the agent knows that the inform reached its destination.

Configuring the SNMP-Server Group Names

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** global configuration command. This command is used to group SNMP users residing on hosts that connect to the local SNMP agent.

Configuring the SNMP-Server Group Names

```
Router(config)#  
snmp-server group groupname {v1 | v2c | v3 {auth | noauth |  
priv}} [read readview] [write writeview] [notify  
notifyview] [access access-list]  
• Configures a new SNMP group, or a table that maps SNMP  
users to SNMP views  
PR1(config)#snmp-server group johngroup v3 auth  
PR1(config)#snmp-server group billgroup v3 auth priv
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-30

An SNMP view is a mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

snmp-server group groupname {v1 | v2c | v3 {auth | noauth | priv}} [read readview] [write writeview] [notify notifyview] [access access-list]

snmp-server group Parameters

Parameter	Description
<i>groupname</i>	The name of the group.
v1	The least secure of the possible User Security Models (USMs).
v2c	The second least secure of the possible USMs. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	The most secure of the possible USMs.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet and then scrambles it.
read	(Optional) The option that allows you to specify a read view.

Parameter	Description
<i>readview</i>	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent.
write	(Optional) The option that allows you to specify a write view.
<i>writeview</i>	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.
notify	(Optional) The option that allows you to specify a notify view.
<i>notifyview</i>	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
access	(Optional) The option that enables you to specify an ACL.
<i>access-list</i>	(Optional) A string (not to exceed 64 characters) that is the name of the ACL.

The example in the figure shows how to define a group *johnsgroup* for SNMP v3, using authentication but not privacy (encryption).

The other example shows how to define a group *billgroup* for SNMP v3, using both authentication and privacy.

Configuring the SNMP-Server Users

To add a new user to an SNMP group, use the **snmp-server user** global configuration command.

Configuring the SNMP-Server Users

Router(config)#

```
snmp-server user username groupname [remote ip-address  
[udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 |  
sha} auth-password [priv des56 priv-password]]} [access  
access-list]
```

- Configures a new user to an SNMP group

```
PR1(config)#snmp-server user John johngroup v3 auth md5 john2passwd  
PR1(config)#snmp-server user Bill billgroup v3 auth md5 bill3passwd des56  
password2  
PR1(config)#snmp-server group johngroup v3 auth  
PR1(config)#snmp-server group billgroup v3 auth priv
```

© 2006 Cisco Systems, Inc. All rights reserved.

RSBW v1.0--5.21

To configure a user existing on a remote SNMP device, specify the IP address or port number for the remote SNMP device where the user resides. Also, before you configure remote users for that device, configure the SNMP engine ID, using the command **snmp-server engineID** with the **remote** option. The SNMP engine ID of the remote device is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

snmp-server user username groupname [**remote** ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password [priv des56 priv-password]]} [access access-list]

snmp-server user Parameters

Parameter	Description
username	The name of the user on the host that connects to the agent.
groupname	The name of the group to which the user is associated.
remote	(Optional) Specifies the remote copy of SNMP on the router.
ip-address	(Optional) The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a UDP port of the host to use.
port	(Optional) This is a UDP port number that the host uses. The default value is 162.
v1	The least secure of the possible SNMP versions.

Parameter	Description
v2c	The second least secure of the possible SNMP versions. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	The most secure of the possible SNMP versions.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Initiates an authentication level setting session.
md5	(Optional) The HMAC-MD5-96 authentication level.
sha	(Optional) The HMAC-SHA-96 authentication level.
<i>auth-password</i>	(Optional) A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv	(Optional) Initiates a privacy authentication level setting session.
des56	(Optional) The CBC-DES privacy authentication algorithm.
<i>priv-password</i>	(Optional) A string (not to exceed 64 characters) that enables the host to encrypt the contents of the message that it sends to the agent.
access	(Optional) Enables you to specify an ACL.
<i>access-list</i>	(Optional) A string (not to exceed 64 characters) that is the name of the ACL.

The example in the figure shows how to define a user *John*, belonging to the group *johnsgroup*. Authentication uses the password *john2passwd* and no privacy (no encryption) is applied. Then a user *Bill*, belonging to the group *billgroup*, is defined using the password *bill3passwd* and privacy (encryption) is applied.

Configuring the SNMP-Server Hosts

To specify the recipient of an SNMP notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

Configuring the SNMP-Server Hosts

Router(config)#

```
snmp-server host host-address [traps | informs] [version  
{1 | 2c | 3 [auth | noauth | priv]}] community-string  
[udp-port port] [notification-type]
```

- Configures the recipient of an SNMP trap operation.

```
PR1(config)#snmp-server engineID remote 10.1.1.1 1234  
PR1(config)#snmp-server user bill billgroup remote 10.1.1.1 v3  
PR1(config)#snmp-server group billgroup v3 noauth  
PR1(config)#snmp-server enable traps  
PR1(config)#snmp-server host 10.1.1.1 inform version 3 noauth bill  
PR1(config)#snmp-server manager
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5.32

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received.

An SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). However, informs consume more resources in the agent and in the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To be able to send an “inform,” perform these steps:

- Step 1** Configure a remote engine ID.
- Step 2** Configure a remote user.
- Step 3** Configure a group on a remote device.
- Step 4** Enable traps on the remote device.
- Step 5** Enable the SNMP manager.

snmp-server host host-address [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]

snmp-server host Parameters

Parameter	Description
<i>host-address</i>	The address of the recipient for which the traps are targeted.
traps	(Optional) Specifies that the type of notification being sent should be a trap.
informs	(Optional) Specifies that the type of notification being sent should be an inform.
version	(Optional) Specifies the security model to use.
1	(Optional) The least secure of the possible security models.
2c	(Optional) This is the second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
3	(Optional) The most secure of the possible security models.
auth	(Optional) Specifies authentication of a packet without encrypting it.
noauth	(Optional) Specifies no authentication of a packet.
priv	(Optional) Specifies authentication of a packet and then scrambles it.
<i>community-string</i>	This is a string that is used as the name of the community and it acts as a password by controlling access to the SNMP community. This string can be set using the snmp-server host command, but it is recommended that you set the string using the snmp-server community command before using the snmp-server host command.
udp-port	(Optional) Specifies a UDP port of the host to use.
<i>port</i>	(Optional) This is a UDP port number that the host uses. The default is 162.
<i>notification-type</i>	(Optional) This is the type of trap to be sent to the host. If no type is specified, all traps are sent.

For a full list refer to the *SNMPv3 Configuration Guide*. Some of the types of traps are listed in the table.

Types of Traps

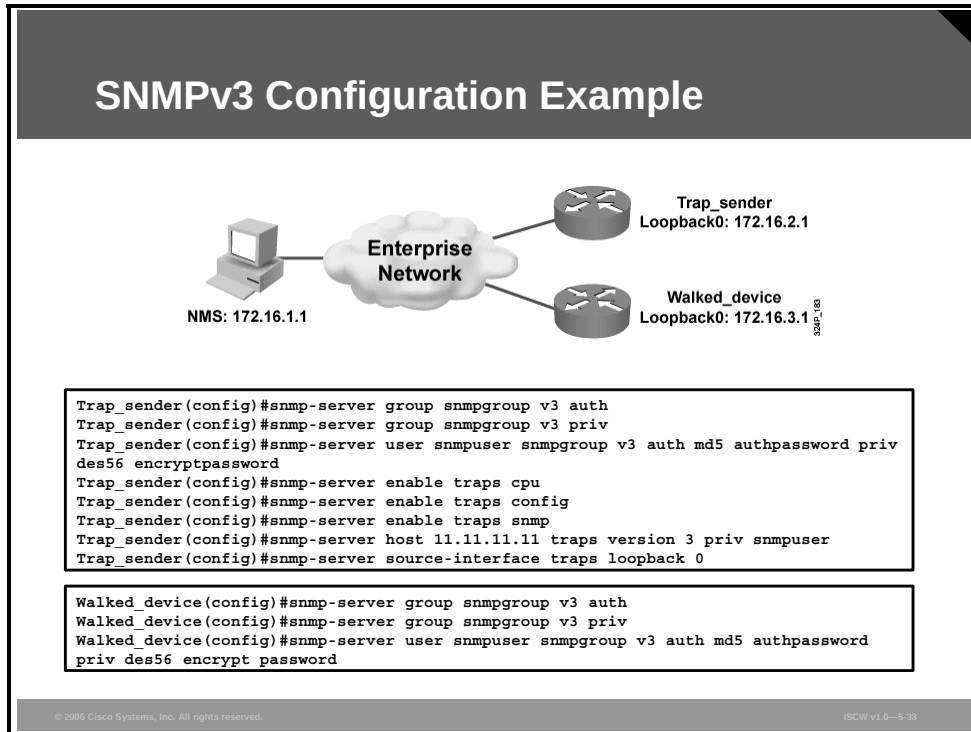
Trap	Description
bgp	Sends Border Gateway Protocol (BGP) state change traps.
config	Sends configuration traps.
hsrp	Sends Hot Standby Router Protocol (HSRP) notifications.
sdhc	Sends Synchronous Data Link Control (SDLC) traps.
snmp	Sends SNMP traps defined in RFC 1157.
syslog	Sends error message traps (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.
tty	Sends Cisco enterprise-specific traps when a TCP connection closes.
x25	Sends X.25 event traps.

The example in the figure shows how to send configuration informs to the 10.1.1.1 remote host.

Note	There are several more snmp-server commands available that are described in the <i>Cisco IOS Master Commands List, Release 12.4</i> at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm .

SNMPv3 Configuration Example

The figure shows how to configure Cisco IOS routers for SNMPv3.



The router Trap_sender is configured to send traps to the NMS host with the IP address 11.11.11.11. The traps are encrypted using the credentials configured for the local user snmpuser belonging to the group snmpgroup. The Trap_sender router sends traps related to CPU, configuration, and SNMP. The trap packets are sourced from the router loopback 0 interface.

The router Walked_device is configured so that the NMS host can read the MIBs on the local device. The NMS server will need to use the username credentials configured on the Walked_device (snmpuser with respective authentication and encryption passwords) to get access to the SNMP information of the router.

Configuring NTP Client

This topic describes the procedure to configure an NTP client, including authentication in client mode.

Understanding NTP

- **NTP is used to synchronize the clocks in the entire network.**
- **System clock is set by the battery system calendar during bootup.**
- **System clock can then be modified manually or via NTP.**
- **NTP runs over UDP port 123; current version is 4.**
- **Only NTP up to version 3 has been documented in RFCs.**
- **Stratum describes how many “NTP hops” away a machine is from authoritative time source.**
- **NTP establishes associations to synchronize time.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-35

NTP is used to synchronize the clocks in the entire network. Many features depend on it, such as accurate time information in syslog messages, certificate-based authentication in VPNs, ACLs with time range configuration, key rollover in routing protocol authentication (Enhanced Interior Gateway Routing Protocol [EIGRP], Routing Information Protocol [RIP]).

Most Cisco routers have two clocks: a battery-powered system calendar in the hardware and a software-based system clock. These two clocks are managed separately.

The heart of the time service is the software-based system clock. This clock runs from the moment the system starts up and keeps track of the current date and time. The system clock can be set from a number of sources and in turn can be used to distribute the current time through various mechanisms to other systems. When a router with a system calendar is initialized or rebooted, the system clock is set based on the time in the internal battery-powered system calendar. The system clock can then be set manually or by using NTP.

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight savings time) so that the time is displayed correctly relative to the local time zone.

The system clock keeps track of whether the time is “authoritative” or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time will be available only for display purposes and will not be redistributed.

The NTP is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which in turn runs over IP.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

The current version is NTP version 4; however, as of 2005, only NTP up to version 3 has been documented in RFCs. Cisco devices support only RFC specifications of NTP.

NTP uses the concept of a “stratum” to describe how many NTP “hops” away a machine is from an authoritative time source. A “stratum 1” time server typically has a radio or atomic clock directly attached, a “stratum 2” time server receives its time via NTP from a “stratum 1” time server, and so on. A machine running NTP will automatically choose as its time source the machine with the lowest stratum number that it is configured to communicate with via NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP is careful to avoid synchronizing to a machine whose time may not be accurate. It avoids doing so in two ways. First, NTP will never synchronize to a machine that is not in turn synchronized itself. Secondly, NTP will compare the time reported by several machines, and will not synchronize to a machine whose time is significantly different than the others, even if its stratum is lower.

The communications between machines running NTP (known as “associations”) are usually statically configured; each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is made possible by exchanging NTP messages between each pair of machines with an association. However, in a LAN environment, you can configure NTP to use IP broadcast messages instead. This alternative reduces configuration complexity, because each machine can simply be configured to send or receive broadcast messages. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

The time kept on a machine is a critical resource, so you should use the security features of NTP to avoid the accidental or malicious setting of incorrect time. Two mechanisms are available: an ACL-based restriction scheme and an encrypted authentication mechanism.

It is recommended that time service for your network be derived from the public NTP servers available in the Internet. If the network is isolated from the Internet, the Cisco implementation of NTP allows a machine to be configured so that it acts as though it is synchronized via NTP, when in fact it has determined the time using other means. Other machines then synchronize to that machine via NTP.

When multiple sources of time (for example, manual configuration) are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

An NTP association can be a peer association (meaning that this system is willing to either synchronize to the other system or to allow the other system to synchronize to it), or it can be a server association (meaning that only this system will synchronize to the other system, and not the other way around).

Configuring NTP Authentication

NTP services are enabled on all interfaces by default. If you want to disable NTP on a specific interface, use the **ntp disable** command in the interface configuration mode. All NTP configuration tasks discussed in this lesson are optional.

Configuring NTP Authentication

```
Router(config)#  
ntp authenticate
```

- Enables the authentication feature

```
Router(config)#  
ntp authentication-key number md5 value
```

- Defines the authentication keys
- Used for both peer and server associations

```
Router(config)#  
ntp trusted-key key-number
```

- Defines the trusted authentication keys
- Required to synchronize to a system (server association)

```
R1(config)#ntp authentication  
R1(config)#ntp authentication-key 1 md5 NeVeRgUeSs  
R1(config)#ntp trusted-key 1
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-35

If you want to authenticate the associations with other systems for security purposes, use the commands that follow. The first command enables the NTP authentication feature. The second command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently the only key type supported is **md5**. Finally, a list of trusted authentication keys is defined. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.

To configure NTP authentication, use the global configuration commands listed in the table.

NTP Authentication Commands

Command	Description
ntp authenticate	Enables the NTP authentication feature. If this command is specified, the system will not synchronize to a system unless its NTP messages carry one of the authentication keys specified in the ntp trusted-key global configuration command.
ntp authentication-key <i>number md5 value</i>	Defines an authentication key. Message authentication support is provided using the MD5 algorithm. The key type md5 is currently the only key type supported. The key value can be any arbitrary string of up to eight characters.
ntp trusted-key <i>key-number</i>	Defines trusted authentication keys.

Configuring NTP Associations

If you want to configure a router as an NTP client, you must either create an association to a server or configure the router to listen to NTP broadcast packets.

Configuring NTP Associations

```
Router(config)#  
ntp server {ip-address | hostname} [version number] [key  
keyid] [source interface] [prefer]
```

- Forms a server association with another system

```
Router(config-if)#  
ntp broadcast client
```

- Receives NTP broadcast packets

```
R1(config)#ntp server 10.1.1.1 key 1  
R1(config)#ntp server 10.2.2.2 key 2 prefer  
R1(config)#interface FastEthernet 0/1  
R1(config-if)#ntp broadcast client
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-37

Although you may configure either a peer or a server association, NTP clients would be typically configured with a server association (meaning that only this system will synchronize to the other system, and not the other way around). If you want to allow the software clock to be synchronized by an NTP time server, use the **ntp server** command in global configuration mode.

ntp server {ip-address | hostname} [version number] [key key-id] [source interface] [prefer]

ntp server Parameters

Parameter	Description
<i>ip-address</i>	IP address of the time server providing the clock synchronization.
<i>hostname</i>	Name of the time server providing the clock synchronization.
version	(Optional) Defines the NTP version number.
<i>number</i>	(Optional) NTP version number (1 to 3). Default is 3.
key	(Optional) Defines the authentication key.
<i>key-id</i>	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Identifies the interface from which to pick the IP source address. Default is to take the interface address.
<i>interface</i>	(Optional) 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.

In addition or instead of creating unicast NTP associations, you can allow the system to listen to broadcast packets on an interface-by-interface basis. To do so, use the **ntp broadcast client** command in interface configuration mode.

Configuring Additional NTP Options

To control access to NTP services, in addition to packet authentication, you can create an NTP access group and apply a basic IP ACL to it.

Configuring Additional NTP Options

```
Router(config)#  
ntp access-group {query-only | serve-only | serve | peer}  
access-list-number
```

- Controls NTP message exchange

```
Router(config)#  
ntp source interface
```

- Modifies the source IP address of NTP packets

```
R1(config)#access-list 1 permit host 10.1.1.1  
R1(config)#ntp access-group peer 1  
R1(config)#ntp source loopback 0
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5/38

To control access to NTP services, use the **ntp access-group** command in global configuration mode.

ntp access-group {query-only | serve-only | serve | peer} access-list-number

The access group options are scanned in the following order, from least restrictive to most restrictive:

1. **peer:** Allows time requests and NTP control queries and allows the system to synchronize itself to a system whose address passes the ACL criteria. This option is used in scenarios in which either the local or the remote system can become the NTP source.
2. **serve:** Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the ACL criteria. This option allows you to filter IP addresses of systems that can become clients of the local system from which NTP control queries will be permitted.
3. **serve-only:** Allows only time requests from a system whose address passes the ACL criteria. This option allows you to filter IP addresses of systems that can become clients of the local system from which NTP control queries will be denied.
4. **query-only:** Allows only NTP control queries from a system whose address passes the ACL criteria.

If the source IP address matches the ACLs for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all systems. If any access groups are specified, only the specified access types will be granted.

When the system sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** command in global configuration mode if you want to configure a specific interface from which the IP source address will be taken.

ntp source *interface*

This interface will be used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** parameter on the **ntp peer** or **ntp server** command.

Configuring NTP Server

This topic describes the procedure for configuring a Cisco router as an NTP server.

Implementing NTP Server

- Cisco IOS routers work as an NTP server by default.
- As soon as a router is synchronized to an authoritative time source, it will allow peers with lower stratum to synchronize to that router:
 - Requires a peer association
- You can make a router an authoritative NTP server, even if the system is not synchronized to an outside time source.
- Two options to establish a peer association:
 - Unicast
 - Broadcast
- Same exchange control methods as with client:
 - Packet authentication
 - Access group filtering

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0-5.40

Cisco IOS routers activate the NTP protocols and work as clients or servers depending on the peer association that is established with another device. An IOS router will offer the time information to any peer with a lower stratum number as soon as it is itself synchronized with its own authoritative source.

You can configure an IOS to become an authoritative time source even when there is no higher-stratum source to retrieve the time from.

When a router is functioning as an NTP server, it may establish associations either by broadcasting the NTP packets or sending the messages to configured peers using unicast packets.

You can control the exchange of NTP information by authenticating the messages or by permitting and denying the connections based on IP addresses.

Configuring NTP Server

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the **ntp peer** command in global configuration mode.

Configuring NTP Server

```
Router(config)#  
ntp peer ip-address [normal-sync] [version number] [key  
keyid] [source interface] [prefer]  
• Forms a peer association with another system  
Router(config)#  
ntp master [stratum]  
• Makes the system an authoritative NTP server  
Router(config-int)#  
ntp broadcast [version number] [destination address] [key keyid]  
• Configures an interface to send NTP broadcast packets  
R2(config)#ntp peer 10.1.1.1 key 1  
R2(config)#ntp master 3  
R2(config)#interface FastEthernet0/0  
R2(config-int)#ntp broadcast
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-41

ntp peer *ip-address* [**normal-sync**] [**version number**] [**key keyid**] [**source interface**] [**prefer**]

ntp peer Parameters

Parameter	Description
<i>ip-address</i>	IP address of the peer providing, or being provided, the clock synchronization
normal-sync	(Optional) Disables the rapid synchronization at startup
version	(Optional) Defines the NTP version number
<i>number</i>	(Optional) NTP version number (1 to 3)
key	(Optional) Defines the authentication key
<i>keyid</i>	(Optional) Authentication key to use when sending packets to this peer
source	(Optional) Names the interface
<i>interface</i>	(Optional) Name of the interface from which to pick the IP source address
prefer	(Optional) Makes this peer the preferred peer that provides synchronization

Use the **ntp master** command in global configuration mode if you want the system to be an authoritative NTP server (a master clock), even if the system is not synchronized to an outside time source or an external NTP source is not available. Stratum is an optional number from 1 to

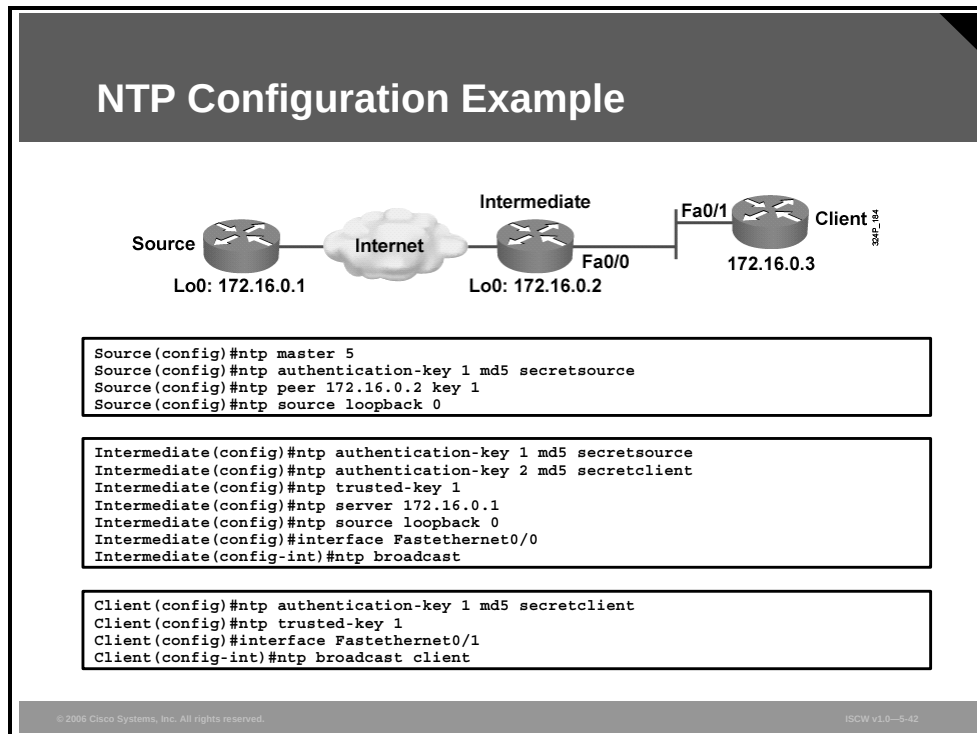
15 that indicates the NTP stratum number that the system will claim. By default, the master clock function is disabled. When enabled, the default stratum is 8.

Caution Use this command with caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the **ntp master** command can cause instability in keeping time if the machines do not agree on the time.

To configure the system to send NTP broadcast packets on a specified interface, use the **ntp broadcast** command in interface configuration mode. The version parameter is an optional number from 1 to 3 indicating the NTP version. Use the **destination** keyword if you want the NTP host to restrict broadcast of NTP frames to the IP address of a designated system. The optional **key** parameter is configured when only the specified key should be included in the transmitted NTP broadcast packets.

NTP Configuration Example

This section presents an NTP configuration example.



This example shows three routers configured for NTP exchange. *Source* is configured as an authoritative NTP server with stratum 5 and has all settings for an authenticated association with *Intermediate*.

Intermediate receives the time information through the configured association with the *Source* and then broadcasts the current time, authenticating it with all available keys via the FastEthernet0/0 interface.

Client accepts the broadcast packets on its FastEthernet0/1 interface and trusts the messages that have been authenticated with the NTP key that has been locally configured as trusted.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Since OOB management provides higher levels of security and performance than in-band, the decision to use an in-band solution must be considered carefully.
- Management communications should use SSH rather than Telnet.
- Implementing a router logging facility is an important part of any network security policy.
- Syslog is implemented on your Cisco router using syslog router commands.
- Network management will be greatly enhanced by implementing the security features of SNMPv3 rather than earlier versions.
- Cisco IOS SNMPv3 server configuration tasks include configuring SNMP-server engine ID, group names, users, and hosts.
- Cisco routers can be configured as NTP servers or clients.
- Packet authentication and filtering should be used to protect NTP exchange.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5-43

Configuring AAA on Cisco Routers

Overview

This lesson describes authentication, authorization and accounting (AAA). It discusses various router access modes, and compares the AAA protocols, TACACS+ and RADIUS. The lesson also describes how to configure, verify, and troubleshoot AAA on a Cisco Systems router through the command-line interface (CLI), and leads you through the process of AAA configuration using the Cisco Security Device Manager (SDM).

Objectives

Upon completing this lesson, you will be able to explain the procedures to configure AAA implementation on a Cisco router using both SDM and CLI. This ability includes being able to meet these objectives:

- Describe the three components of AAA
- Describe the AAA access modes
- Describe the AAA RADIUS and TACACS+ protocols
- Configure AAA login authentication on Cisco routers using CLI
- Configure AAA login authentication on Cisco routers using SDM
- Troubleshoot AAA on a Cisco perimeter router using the **debug aaa** command
- Explain AAA authorization and the commands that are required to configure it on Cisco routers
- Explain AAA accounting and the commands that are required to configure it on Cisco routers

Introduction to AAA

This topic describes the concepts of authentication, authorization, and accounting.

AAA Model

- **Authentication:**
 - Who are you?
 - “I am user *student* and my password *validateme* proves it.”
- **Authorization:**
 - What can you do? What can you access?
 - “User *student* can access host *serverXYZ* using Telnet.”
 - “Assign an IP address and ACL to user *student* connecting through VPN.”
 - “When user *student* starts an EXEC session, assign privilege level 10.”
- **Accounting:**
 - What did you do? How long and how often did you do it?
 - “User *student* accessed host *serverXYZ* using Telnet for 15 minutes.”
 - “User *student* was connected to VPN for 25 minutes.”
 - “EXEC session of user *student* lasted 20 minutes and only show commands were executed.”

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-3

AAA services provide a higher degree of scalability than line-level and privileged-EXEC authentication.

Unauthorized access in campus, dialup, and Internet environments creates the potential for network intruders to gain access to sensitive network equipment and services. The Cisco AAA architecture enables systematic and scalable access security.

Network and administrative access security in the Cisco environment, whether it involves campus, dialup, or Internet access, is based on a modular architecture that has three functional components: authentication, authorization, and accounting:

- **Authentication:** Requires users and administrators to prove that they really are who they say they are. Authentication is established using a username and password, challenge and response, token cards, and other methods: “I am user *student* and my password *validateme* proves it.”
- **Authorization:** After authenticating the user and administrator, authorization services decide which resources the user and administrator are allowed to access and which operations the user and administrator are allowed to perform: “User *student* can access host *serverXYZ* using Telnet.”

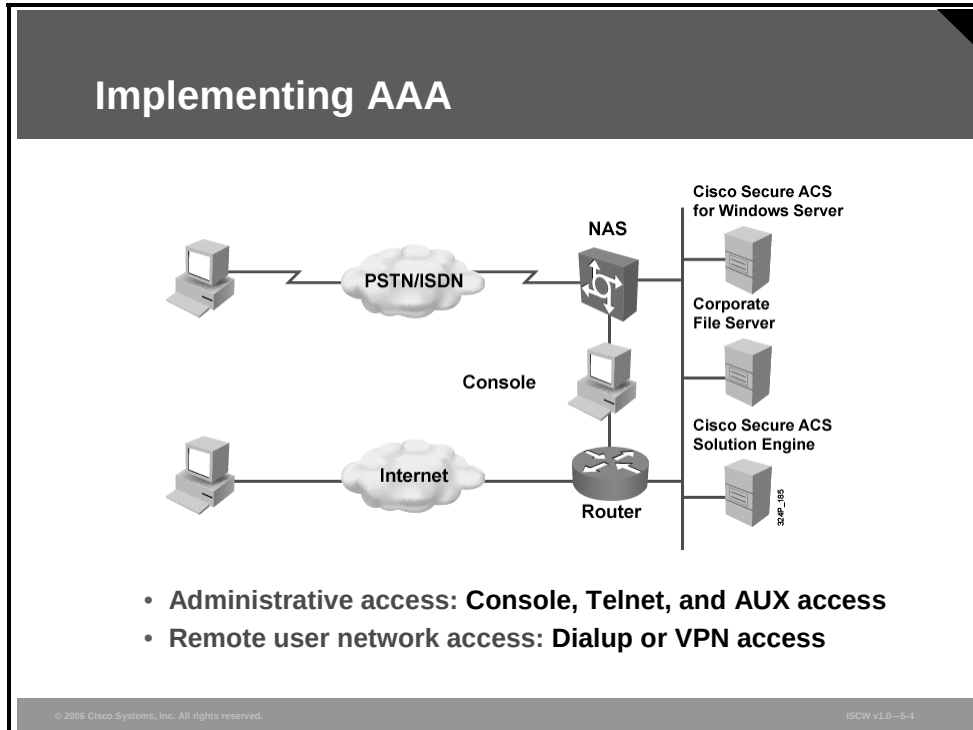
Other typical authorization tasks are:

- Assigning parameters, such as IP addresses and access control lists (ACLs) to connected users
- Assigning privilege levels to users who run EXEC sessions
- Controlling the usage of specific EXEC commands

- **Accounting and auditing:** Accounting records what the user and administrator actually did, what they accessed, and how long they accessed it for accounting and auditing purposes. Accounting keeps track of how network resources are used: “User *student* accessed host *ServerXYZ* using Telnet for 15 minutes.”

Implementing AAA

Cisco networking products support AAA access control using line passwords, a local username/password database, or remote security server databases. A local security database is configured in the router for a small group of network users using the **username xyz password (or secret) strongpassword** command. A remote security database is a separate server running an AAA security protocol, providing AAA services for multiple network devices and large numbers of network users.



Two examples of AAA implementation include authenticating remote users accessing the corporate LAN through dialup or Internet connections, and authenticating administrators accessing the router console port, aux port, and vty ports.

Cisco provides three ways of implementing AAA services for Cisco routers, network access servers (NASs), and switch equipment, as shown in the figure:

- **Self-contained AAA:** AAA services may be self-contained in the router or NAS itself (also known as local authentication).
- **Cisco Secure ACS for Windows Server:** AAA services on the router or NAS contact an external Cisco Secure Access Control Server (ACS) for Windows system for user and administrator authentication.
- **Cisco Secure ACS Solution Engine:** AAA services on the router or NAS contact an external Cisco Secure ACS Solution Engine for user and administrator authentication.

Router Access Modes

This topic describes the AAA router access modes.

Router Access Modes		
Modes	Router Ports	AAA Command Element
Character mode (line mode or interactive login)	tty, vty, aux, con	<i>login, exec, nasi connection, enable, command</i>
Packet mode (interface mode or link protocol session)	async, group-async, BRI, PRI, serial, dialer profiles, dialer rotaries	<i>ppp, network</i>

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-6

Understanding router access modes is a key to understanding AAA commands and how they work to secure your network access server.

With the exception of the **aaa accounting system** command, all of the AAA commands apply to either character mode or packet mode. The mode refers to the format of the packets requesting AAA. If the query is presented as Service-Type = Exec-User, it is presented in character mode. If the request is presented as Service-Type = Framed-User and Framed-Type = PPP, it is presented in packet mode.

Character mode allows a network administrator with a large number of routers in a network to authenticate one time as the user, and then access all routers configured in this method. The figure shows how to decode the meaning of an AAA command by associating the AAA command element with the connection mode to the router.

Primary applications for the Cisco Secure ACS include securing dialup access to a network and securing the management of routers within a network. Both applications have unique AAA requirements.

With the Cisco Secure ACS, you can choose a variety of authentication methods, each providing a set of authorization privileges. These router ports must be secured using the Cisco IOS software and a Cisco Secure ACS server.

AAA Protocols: RADIUS and TACACS+

This topic describes the AAA RADIUS and TACACS+ protocols.

AAA Protocols: RADIUS and TACACS+		
AAA Protocols	TACACS+	RADIUS
Layer 3 Protocol	TCP/IP	UDP/IP
Encryption	Entire body	Password only
Standard	Cisco	Open/IETF

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.0

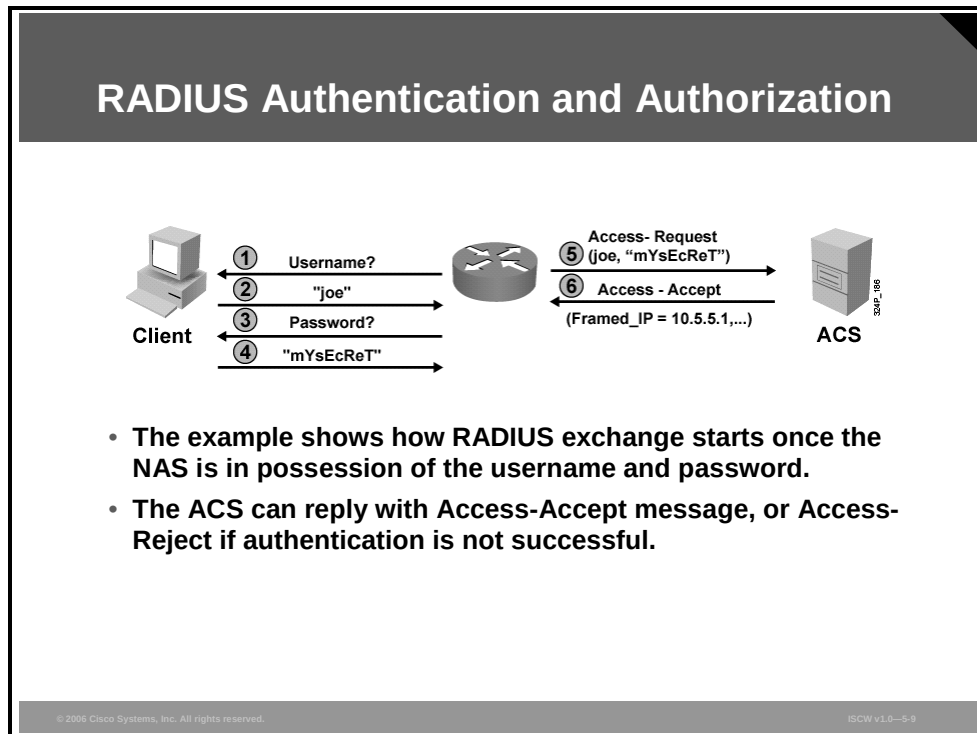
The best-known and best-used types of AAA protocols are TACACS+ and RADIUS. TACACS+ supersedes older versions of TACACS and XTACACS. TACACS+ and RADIUS have different features that make them suitable for different situations.

For example, RADIUS is maintained by a standard that was created by the Internet Engineering Task Force (IETF); TACACS+ is a proprietary Cisco Systems technology that encrypts data. Another key difference is that TACACS+ runs in TCP while RADIUS operates in User Datagram Protocol (UDP).

TACACS+ provides many benefits for configuring Cisco devices to use AAA for management and terminal services. TACACS+ can control the authorization level of users, while RADIUS cannot. Also, because TACACS+ separates authentication and authorization, it is possible to use TACACS+ for authorization and accounting while using a different method for authentication, such as Kerberos.

RADIUS Authentication and Authorization

This topic describes the RADIUS authentication process.



This figure illustrates the authentication process with RADIUS. These steps are involved in the exchange:

- Step 1** The NAS prompts the client for a username.
- Step 2** The client provides a username to the NAS.
- Step 3** NAS prompts for a password.
- Step 4** The client provides the password.
- Step 5** The information about the username and the password is sent to the RADIUS server using an Access-Request datagram, which contains all the necessary attribute-value (AV) pairs.
- Step 6** If the user-information is correct, the server responds with an Access-Accept datagram. The Access-Accept message also contains authorization parameters in the form of AV pairs, such as the IP address to be assigned, and so on. If the user information is invalid, an Access-Reject message is returned and the NAS terminates the connection.

RADIUS Messages

This topic describes the message types involved in a RADIUS authentication exchange.

RADIUS Messages

There are four types of messages:

- **Access-Request**
- **Access-Challenge**, to facilitate challenge-response authentication protocols
- **Access-Accept**
- **Access-Reject**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-10

There are these four RADIUS message types:

- **Access-Request:** Contains AV pairs for the username, password (this is the only information that is encrypted by RADIUS), and additional information such as the NAS port
- **Access-Challenge:** Necessary for challenge-based authentication methods such as Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), and Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- **Access-Accept:** The positive answer if the user information is valid
- **Access-Reject:** Sent as a negative reply if the user information is invalid

RADIUS Attributes

Each message can contain a number of attribute-value (AV) pairs. Some are used for authentication purposes and some are used for authorization purposes.

RADIUS Attributes

- **RADIUS messages contain zero or more AV-pairs, for example:**
 - **User-Name**
 - **User-Password (this is the only encrypted entity in RADIUS)**
 - **CHAP-Password**
 - **Service-Type**
 - **Framed-IP-Address**
- **There are approximately 50 standard-based attributes (RFC 2865).**
- **RADIUS allows proprietary attributes.**
- **Basic attributes are used for authentication purposes.**
- **Most other attributes are used in the authorization process.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--5.11

These are examples of commonly used RADIUS AV pairs:

- User-Name
- User-Password (the only encrypted entity in RADIUS)
- CHAP-Password
- NAS-IP-Address
- NAS-Port
- Service-Type
- Framed-IP-Address

In addition to approximately 50 AV pairs defined in IETF standards, Cisco has added several vendor-specific attributes on the server side. Cisco IOS devices will, by default, always use Cisco AV pairs, but they can be configured to use only IETF attributes for standard compatibility.

Accounting information is sent within special RADIUS accounting messages.

RADIUS Features

You can augment standard attributes with proprietary attributes or with extensions to RFC 2865 (for example, RFC 2868, RFC 2869).

RADIUS Features

- **Standard protocol (RFC 2865)**
- **Standard attributes can be augmented by proprietary attributes:**
 - Vendor-specific attribute 26 allows any TACACS+ attribute to be used over RADIUS
- **Uses UDP on standard port numbers (1812 and 1813; Cisco Secure ACS uses 1645 and 1646 by default)**
- **Includes only two security features:**
 - Encryption of passwords (MD5 encryption)
 - Authentication of packets (MD5 fingerprinting)
- **Authorization only possible as part of authentication**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-12

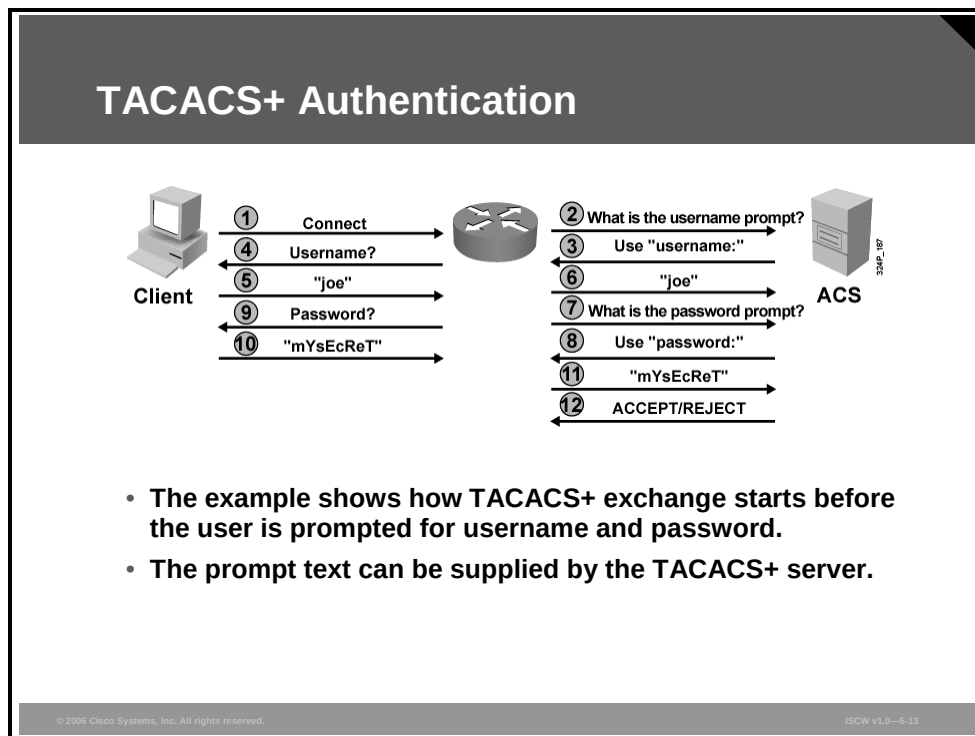
RADIUS (Cisco) is the RADIUS (IETF) support plus IETF attribute 26, the vendor-specific attribute (VSA) for Cisco. It is under this VSA that any authorization request specified in the TACACS+ specification can be sent to an access device through RADIUS.

The most notable limitations of RADIUS include the following:

- Limited security features
- The combination of authentication and authorization in one function

TACACS+ Authentication

The figure shows a typical authentication process using the TACACS+ protocol.



The TACACS+ protocol is much more flexible than the RADIUS communication. It permits the TACACS+ server to use virtually arbitrary dialogs to collect enough information until a user is authenticated.

Note TACACS+ allows an arbitrary conversation to be held between the daemon and the user, until the daemon receives enough information to authenticate the user. This is usually done by prompting for a username and password combination, but may include other items, such as mother's maiden name, all under the control of the TACACS+ daemon.

The figure illustrates the authentication process with TACACS+. These steps are involved in the exchange:

- Step 1** A user requests access.
- Step 2** NAC requests a username prompt from the TACACS+ server.
- Step 3** The TACACS+ server provides a username prompt.
- Step 4** NAC prompts the user.
- Step 5** The user provides a username.
- Step 6** NAC forwards the username to the TACACS+ server.
- Step 7** NAC requests the password prompt from the TACACS+ server.
- Step 8** The TACACS+ server provides a password prompt.
- Step 9** NAC prompts the user for the password.
- Step 10** User submits the password.

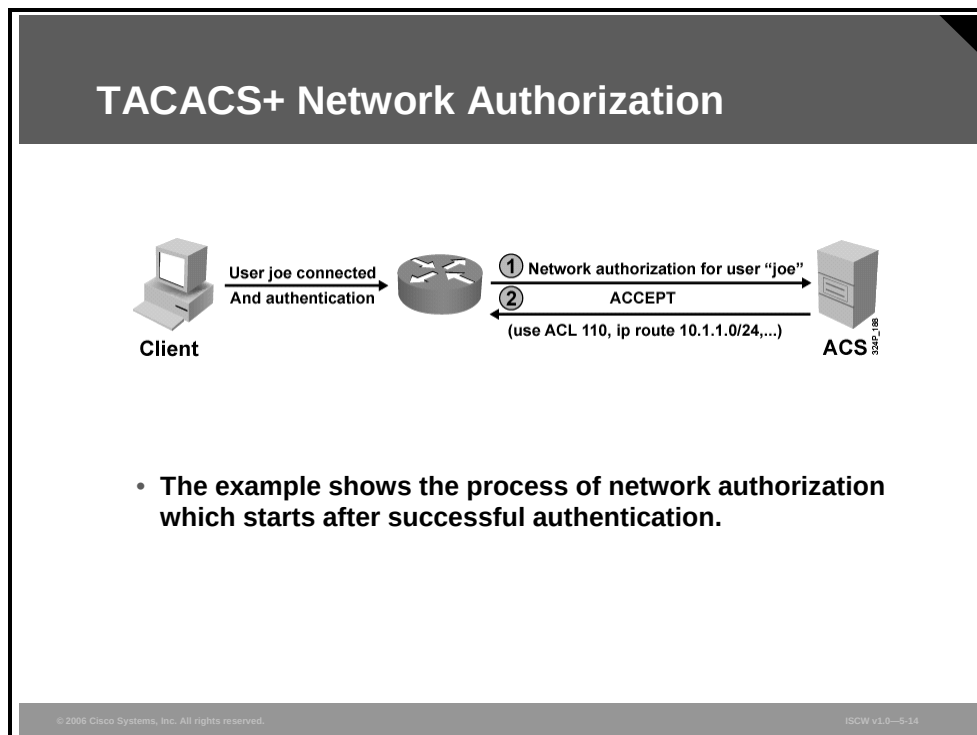
Step 11 NAC forwards the password to the TACACS+ server.

Step 12 The TACACS+ server accepts or rejects the user.

TACACS+ Network Authorization

The NAS eventually receives one of these responses from the TACACS+ daemon:

- **ACCEPT:** The user is authenticated and service may begin. If the NAS is configured to require authorization, authorization will begin at this time.
- **REJECT:** The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence, depending on the TACACS+ daemon.
- **ERROR:** An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the NAS. If an ERROR response is received, the NAS will typically try to use an alternative method to authenticate the user.
- **CONTINUE:** The user is prompted for additional authentication information.



Following authentication, the user is also required to undergo an additional authorization phase, if authorization has been enabled on the NAS. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

If TACACS+ authorization is required, the TACACS+ daemon is again contacted and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response will contain data in the form of attributes that are used to direct the EXEC or NETWORK session for that user. This determines the services that the user can access. Services include the following:

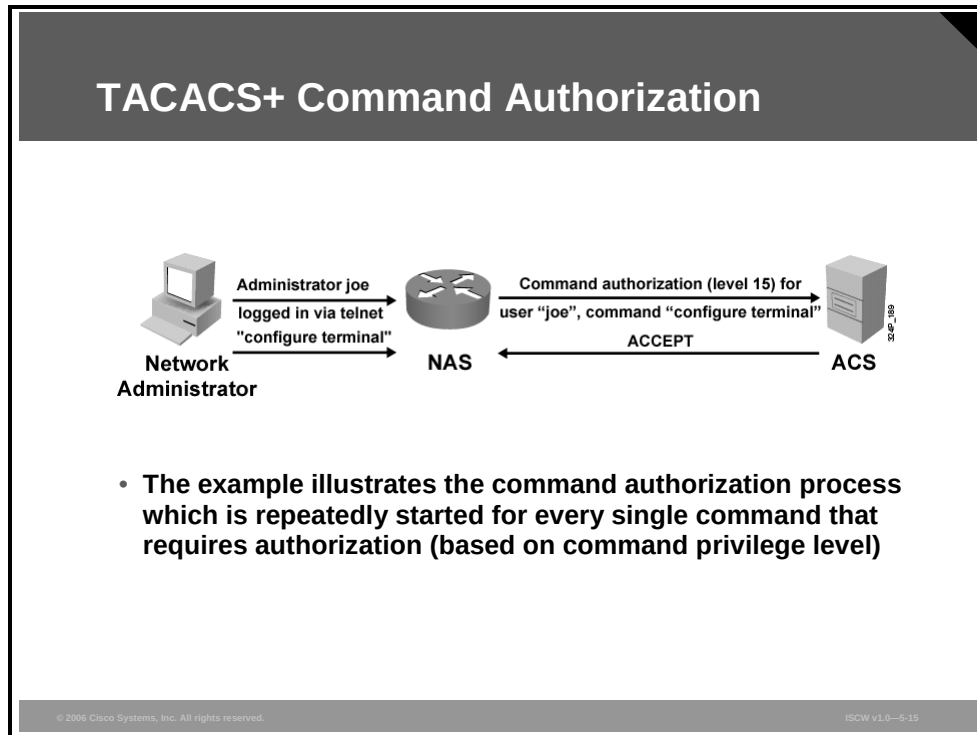
- Telnet, rlogin, PPP, Serial Line Interface Protocol (SLIP), or EXEC services
- Connection parameters, including the host or client IP address, ACL, and user timeouts

The figure illustrates the authorization process with TACACS+, after the user has successfully authenticated. A per-user ACL and static route are uploaded to the NAS. TACACS+ can be used for uploading a variety of other parameters to the NAS. These steps are involved in the exchange:

- Step 1** NAC issues an authorization request for network access to the TACACS+ server.
- Step 2** The TACACS+ server permits or denies access. If the access is permitted, authorization parameters are sent to the NAC to be applied to the user connection.

TACACS+ Command Authorization

Another important aspect of authorization is the access control to services available to a user. Controlling access to configuration commands greatly simplifies the infrastructure security in large enterprise networks. Per-user permissions can easily be configured on the ACS, which simplifies the configuration on network devices.



The example in the figure shows the authorization process when a network administrator issues the **configure terminal** command on a router. The router queries the ACS for permission to execute the command on behalf of user “joe.”

Note	TACACS+ by default establishes a new TCP session for every authorization request, which may lead to delays when users enter commands. Cisco Secure ACS supports persistent TCP sessions to improve performance. Both the Cisco Secure ACS and the router have to be configured for this functionality.

TACACS+ Attributes and Features

This topic describes TACACS+ attributes and features.

TACACS+ Attributes and Features

- TACACS+ messages also contain AV-pairs, such as these:
 - ACL
 - ADDR
 - CMD
 - Interface-Config
 - Priv-Lvl
 - Route
- TACACS+ uses TCP on well-known port number 49.
- TACACS+ establishes a dedicated TCP session for every AAA action.
- Cisco Secure ACS can use one persistent TCP session for all actions.
- Protocol security includes authentication and encryption of all TACACS+ datagrams.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-16

These are some examples of TACACS+ attributes frequently used for authentication and authorization:

- **ACL (EXEC authorization):** Contains an access-class number to be applied to a line.
- **ADDR (SLIP, PPP/IP authorization):** Specifies the IP address of the remote host that should be assigned when using a SLIP or PPP/IP connection.
- **CMD (EXEC):** The AV pair is used for starting an authorization request for an EXEC command.
- **Priv-lvl (EXEC authorization):** Specifies the current privilege level for command authorizations, a number from 0 to 15.
- **Route (PPP/IP, SLIP authorization):** Specifies a route to be applied to an interface.
- **InACL (PPP/IP, SLIP authorization):** Contains an inbound IP ACL for SLIP or PPP/IP connections.
- **OutACL:** Contains an outbound IP ACL for SLIP or PPP/IP.
- **Addr-pool:** Specifies the name of a local address pool from which to get the address of the remote host.
- **Autocmd:** Specifies a command to be automatically executed at EXEC startup.

Many other attributes exist for most network applications, such as dial-in solutions, proxy-authentication on firewalls, or command authorization for Cisco devices.

TACACS+ is the primary protocol for Cisco AAA implementations and is supported on IOS routers, switches, and the Cisco PIX Firewall.

TACACS+, the Cisco proprietary protocol, uses TCP port 49 as a default transport layer. Normally, each AAA transaction uses a dedicated TCP connection. A single session can be established to ensure less server load and better detection of a break in communication. This session persists as long as the server or the network device is operational.

Configuring the AAA Server

This section describes how to configure an IOS router to communicate with an AAA server.

Configuring the AAA Server

TACACS+

```
router(config)# aaa new-model
router(config)# tacacs-server host 192.168.229.76
single-connection
router(config)# tacacs-server key shared1
```

or

```
router(config)# aaa new-model
router(config)# radius-server host 192.168.229.76
router(config)# radius-server key shared1
```

RADIUS

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-17

These are the first steps in configuring the network access server:

- Step 1** Globally enable AAA to allow the use of all AAA elements. This step is a prerequisite for all other AAA commands.
- Step 2** Specify the Cisco Secure ACS that will provide AAA services for the network access server.
- Step 3** Configure the encryption key that will be used to encrypt the data transfer between the network access server and the Cisco Secure ACS.

The table shows commonly used AAA configuration commands and describes their function.

AAA Configuration Commands

Command	Description
aaa new-model	Enables AAA on the router. Prerequisite for all other AAA commands.
tacacs-server host ip-address single-connection	Indicates the address of the Cisco Secure ACS server and specifies use of the TCP single-connection feature of Cisco Secure ACS. This feature improves performance by maintaining a single TCP connection for the life of the session between the network access server and the Cisco Secure ACS server, rather than opening and closing TCP connections for each session (the default).
tacacs-server key key	Establishes the shared secret encryption key between the network access server and the Cisco Secure ACS server.
radius-server host ip-address	Specifies a RADIUS AAA server.

Command	Description
radius-server key <i>key</i>	Specifies an encryption key to be used with the RADIUS AAA server.

Configure AAA Login Authentication on Cisco Routers Using CLI

This topic describes the configuration of AAA login authentication using Cisco IOS CLI.

AAA Authentication Commands

```
Router(config)#  
  
aaa authentication login {default | list_name} group  
{group_name | tacacs+ | radius} [method2 [method3  
[method4]]]
```

- Use this command to configure the authentication process.

```
Router(config)#aaa authentication login default group tacacs+  
local line
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.19

The **authentication login** command in global configuration mode enables the AAA authentication process.

```
aaa authentication login {default | list-name} group {group-name | radius | tacacs+}  
[method2 [method3 [method4]]]
```

aaa authentication login Parameters

Parameter	Description
default	This command creates a default that is automatically applied to <i>all</i> lines and interfaces, specifying the method or sequence of methods for authentication.
<i>list-name</i>	This command creates a list, with a name of your choosing, that is applied explicitly to a line or interface using the method or methods specified. This defined list overrides the default when applied to a specific line or interface.
group <i>group-name</i> group radius group tacacs+	These methods specify the use of an AAA server. The group radius and group tacacs+ methods refer to previously defined RADIUS or TACACS+ servers. The <i>group-name</i> string allows the use of a predefined group of RADIUS or TACACS+ servers for authentication (created with the aaa group server radius or aaa group server tacacs+ command).

Parameter	Description
method2 method3 method4	This command executes authentication methods in the listed order. If an authentication method returns an error, such as a timeout, the Cisco IOS software attempts to execute the next method. If the authentication fails, access is denied. You can configure up to four methods for each operation. The method must be supported by the authentication operation specified. A general list of methods includes: ■ enable: Uses the enable password for authentication ■ group: Uses server-group ■ krb5: Uses Kerberos Version 5 for authentication ■ line: Uses the line password for authentication ■ local: Uses the local username and password database for authentication ■ local-case: Uses case-sensitive local username authentication ■ none: Uses no authentication

Character Mode Login Example

This topic describes the configuration of AAA character mode login authentication using Cisco IOS CLI.

Character Mode Login Example

```
Router#show running-config
...
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login my_list group tacacs+
...
line con 0
line aux 0
line vty 0 4
  login authentication my_list
```

- Because the authentication has not been specified for line con 0 and aux 0, the default option will be used.

© 2006 Cisco Systems, Inc. All rights reserved.

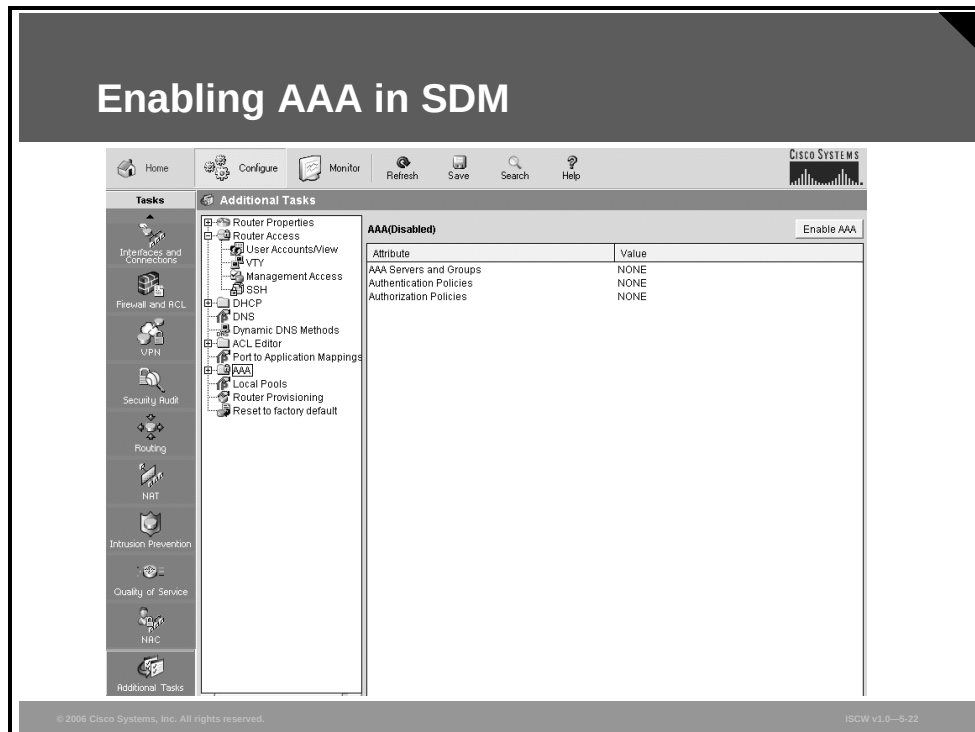
ISCW v1.0--5.20

The table describes how to configure AAA authentication using TACACS+.

Command	Description
aaa authentication login default group tacacs+ local	The default login is TACACS+ server. If no response from the server, then use the local username and password database.
aaa authentication login my_list group tacacs+	Used for character mode username and password challenge. A new list name, <i>my_list</i> , is defined, and the only method is TACACS+.
line con 0	Enters console configuration mode.
login authentication my_list	Configures the console line to use the AAA list name <i>my_list</i> , which has been previously defined to use only TACACS+.
line 1 48 login authentication my_list	Configures lines 1 through 48 to use the AAA list name <i>my_list</i> , which has been previously defined to use only TACACS+.
line vty 0 4	On lines vty 0 through 4, the default list is used, which in this case specifies the aaa authentication login default tacacs+ local command.

Configure AAA Login Authentication on Cisco Routers Using SDM

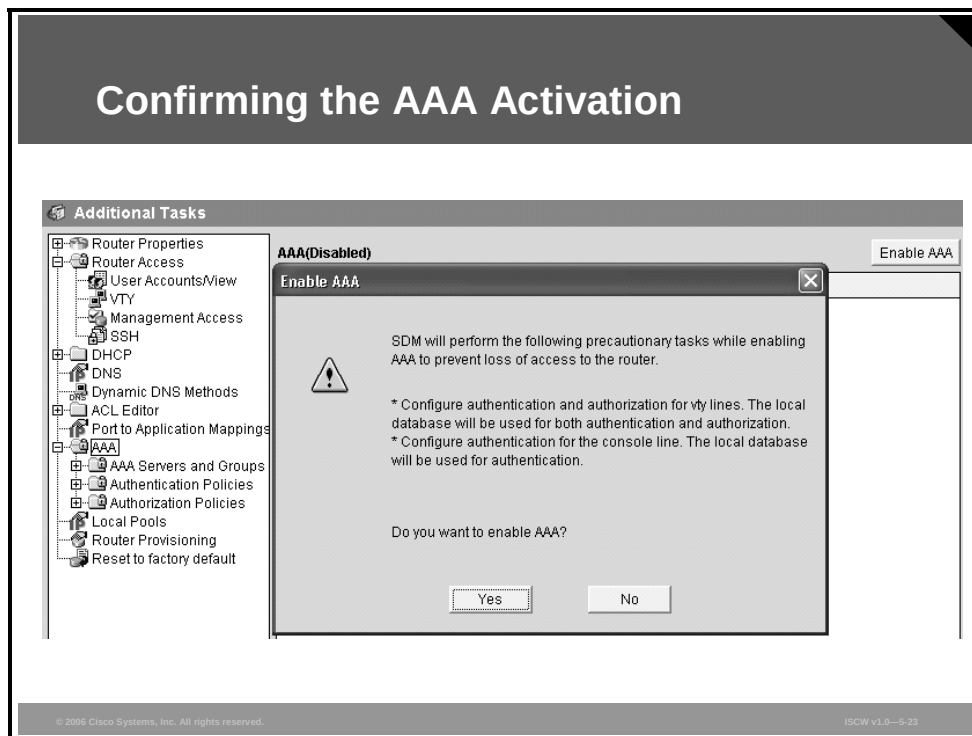
This topic describes the procedure to configure AAA login authentication on Cisco routers using SDM.



The first task when configuring AAA using the Security Device Manager is to enable AAA. This option is available under **Configure > Additional Tasks > AAA**. Locate the **Enable AAA** button in the upper right corner to enable AAA on the router.

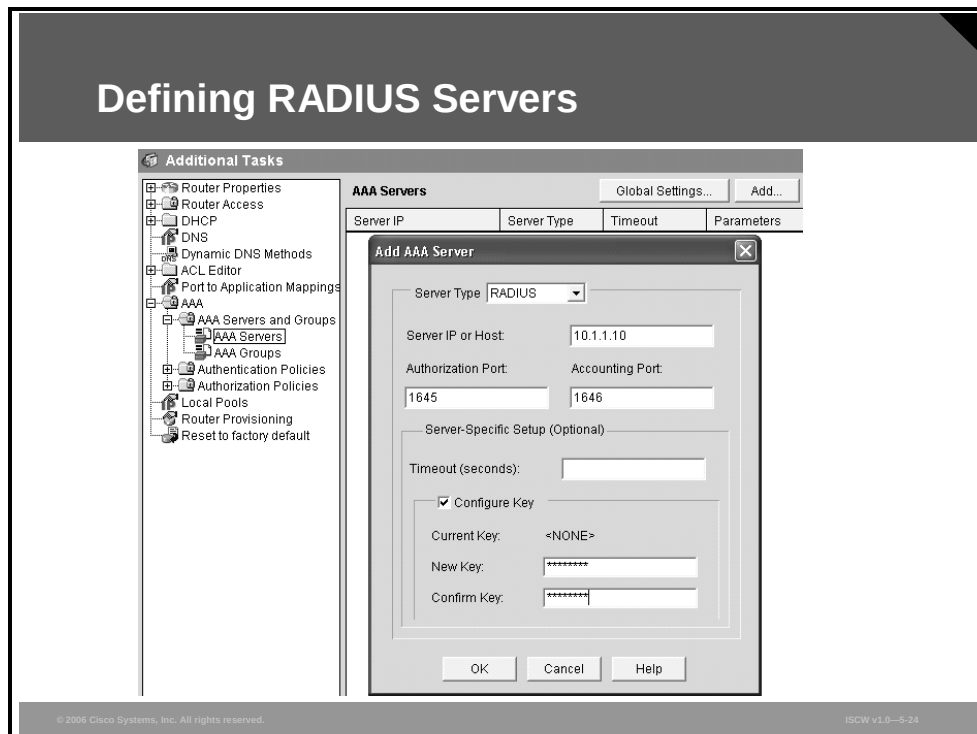
Confirming the AAA Activation

After clicking the button **Enable AAA**, the SDM will perform some precautionary tasks to prevent locking the router or disconnecting the SDM session.



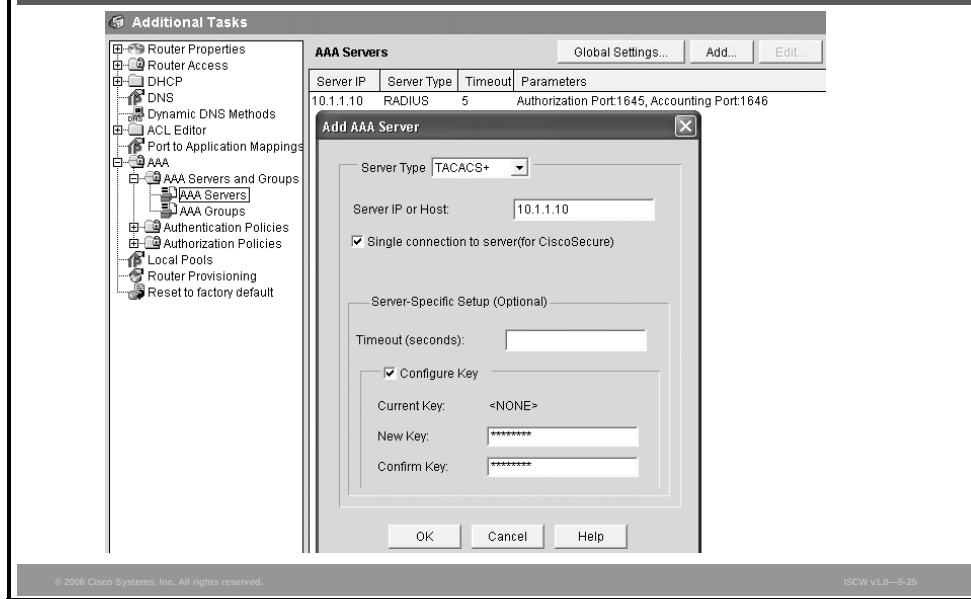
Defining AAA Servers

When AAA is enabled on the router, you can proceed to the task of defining AAA servers. Locate the AAA Servers option under **Configure > Additional Tasks > AAA > AAA Servers and Groups**. Click the **Add** button in the upper right corner to create a new AAA server entry.



The figure illustrates how to define a RADIUS server. After you click the **Add** button in the AAA Servers configuration section, an Add AAA Server window appears. You can choose either RADIUS or TACACS+ from the **Server Type** drop-down box. When you choose RADIUS, you have the option of modifying the UDP ports for authorization and accounting, setting the timeout, and configuring the RADIUS key.

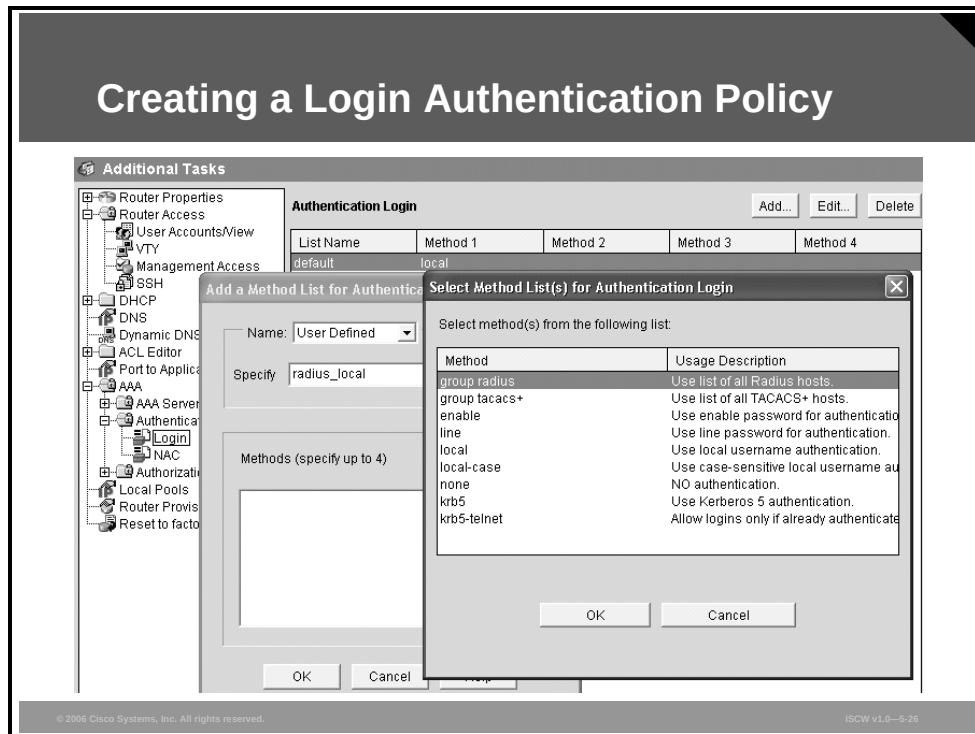
Defining TACACS+ Servers



This example illustrates how to create and configure an entry for a TACACS+ server.

Creating a Login Authentication Policy

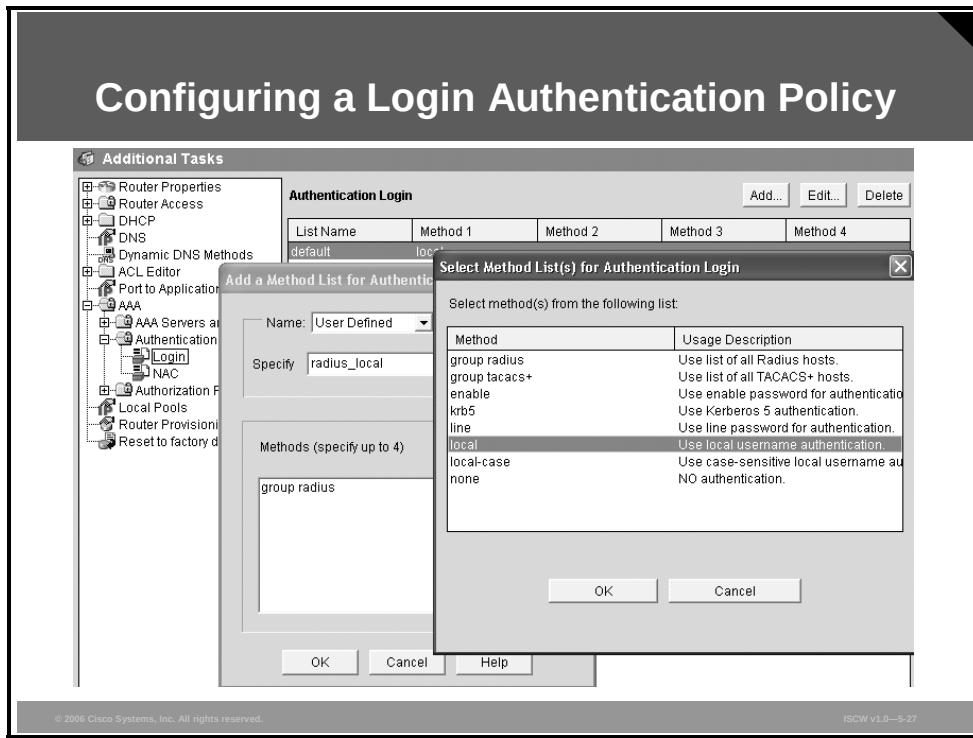
Next, you will have to create or modify an authentication policy.



This option can be found in the menu **Configure > Additional Tasks > AAA > Authentication Policies > Login**. You can either edit an existing policy by highlighting it and selecting the **Edit** button in the upper right corner, or create a new policy by clicking the **Add** button. After AAA is enabled on the router, a default authentication policy (using local authentication) is automatically created by SDM to prevent session lockout. The figure above shows how to create a new policy named *radius_local* that should use **group radius** as the first authentication method.

Configuring a Login Authentication Policy

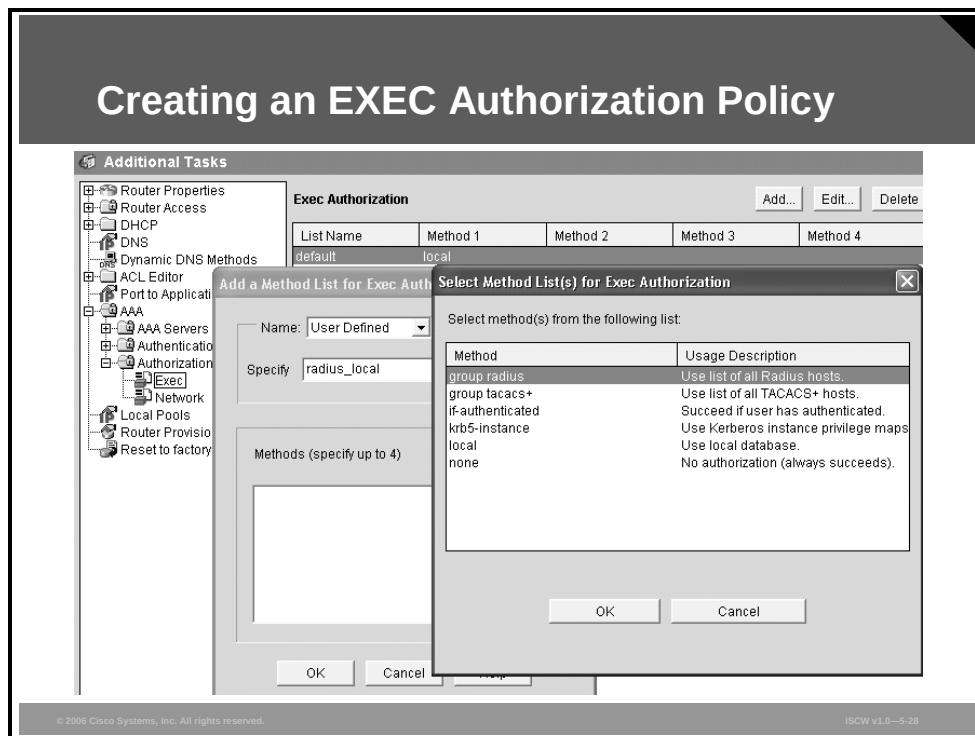
The authentication policy *radius_local* that uses the configured RADIUS server as the only authentication method will not be able to authenticate any users if the RADIUS server fails. Therefore, you may configure one or more backup authentication methods that would be used in the event of RADIUS failure.



In this example, you add the local authentication as a backup authentication method to the policy *radius_local*.

Creating an EXEC Authorization Policy

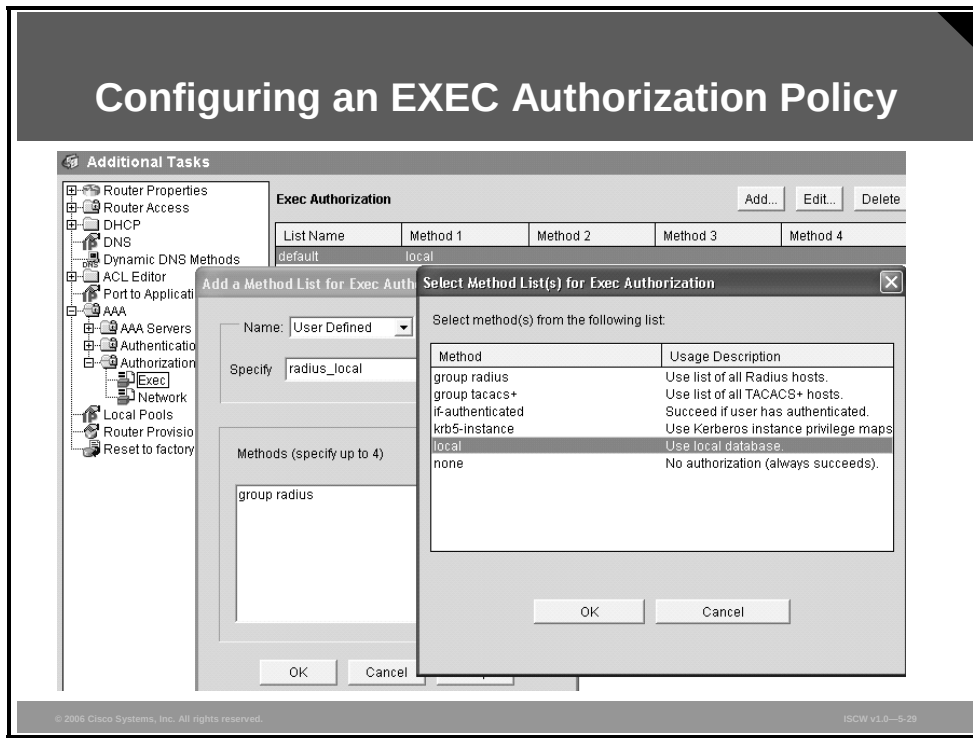
Next, you can create or modify an authorization policy.



This option can be found in the menu **Configure > Additional Tasks > AAA > Authorization Policies > Edit**. You can either edit an existing policy by highlighting it and clicking the **Edit** button in the upper right corner, or create a new policy by clicking the **Add** button. After AAA is enabled on the router, a default authentication policy (using local authentication) is created. The figure shows how to create a new policy, named *radius_local*, that should use **group radius** as the first authentication method. The policy name in this example is identical to the previously configured authentication policy because it should use the same methods. The names of the authentication and authorization policies may be different or the same.

Configuring an EXEC Authorization Policy

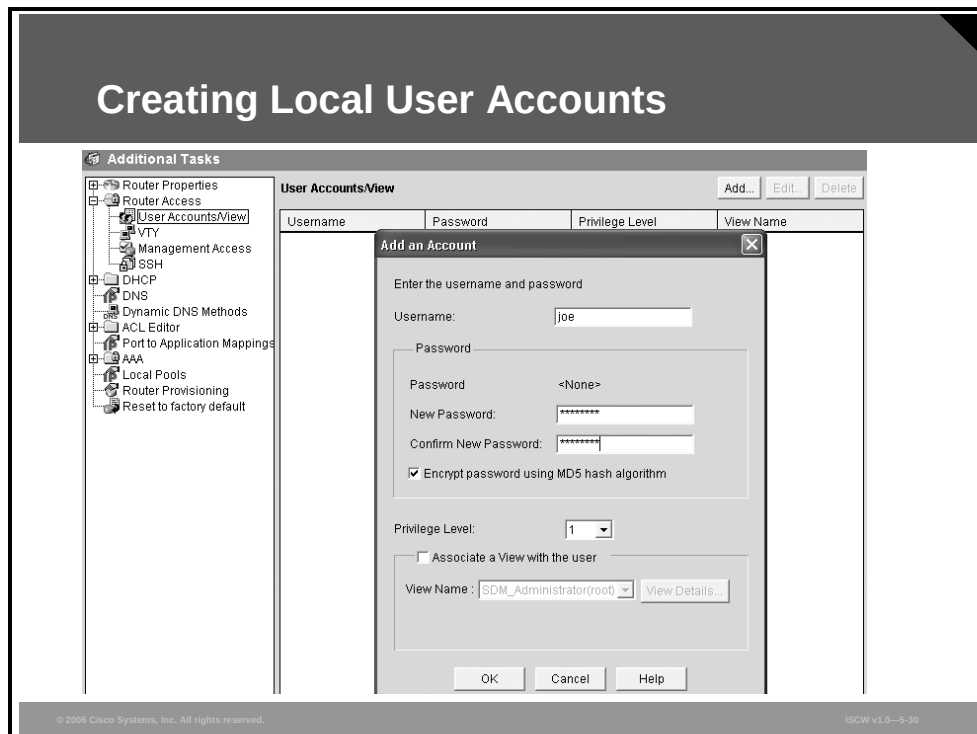
The authorization policy *radius_local* that uses the configured RADIUS server as the only authorization method will not be able to authorize any users if the RADIUS server fails. Therefore, you may configure one or more backup authentication methods that would be used in the event of RADIUS failure.



In this example, you add the local authorization as a backup authorization method to the policy *radius_local*.

Creating Local User Accounts

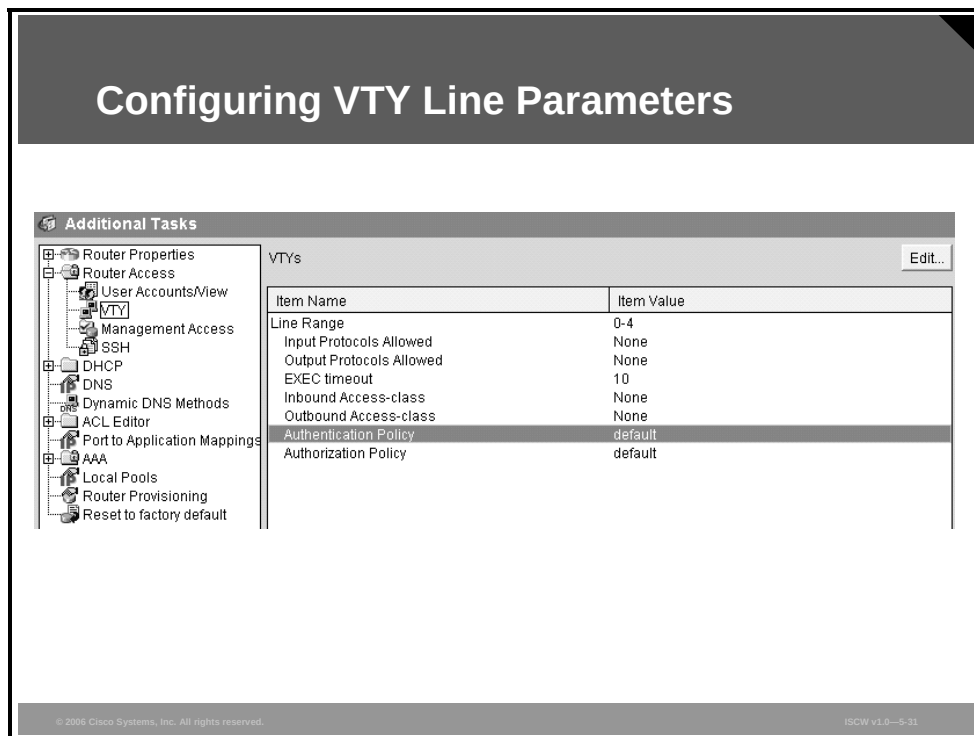
After you decide to use local authentication in the AAA configuration on the router, you will populate the local router database with user accounts. This option is available in the menu **Configure > Additional Tasks > Router Access > User Account/View**. You can add or modify user accounts by clicking the **Add** or **Edit** buttons, respectively.



In this example, a new user *joe* is created using the password encryption scheme.

Configuring VTY Line Parameters

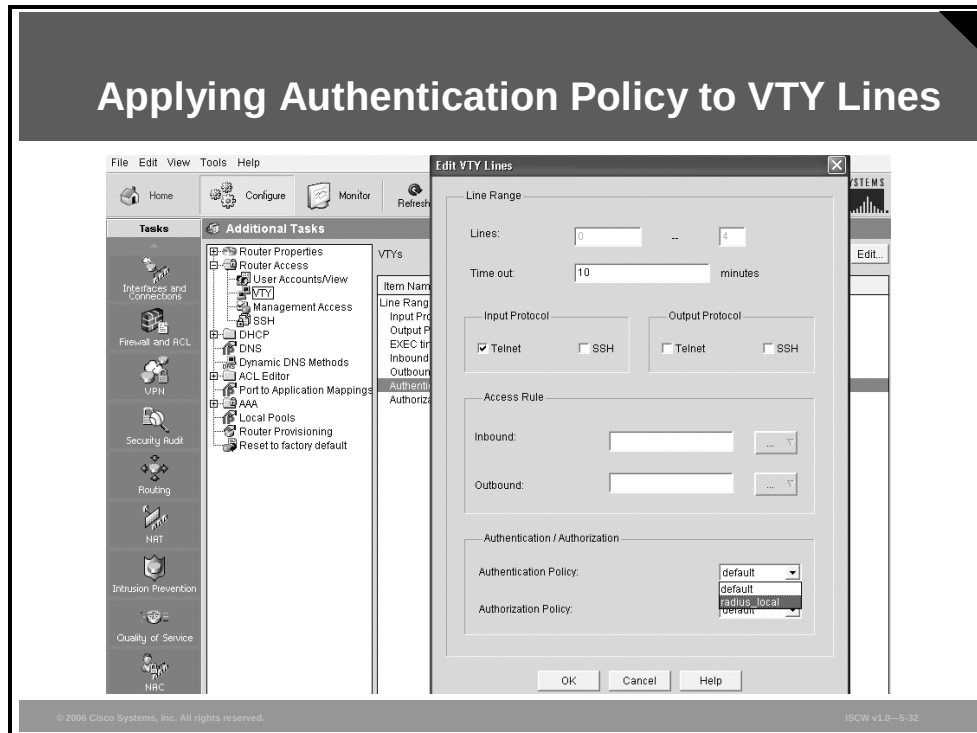
Next, you may want to apply the created authentication policy to router access ports, such as the console port, vty lines, or auxiliary port.



You do not have to apply to the default authentication policy because it is applied by default. If you wish to apply an authentication policy to vty lines, select the menu **Configure > Additional Tasks > Router Access > VTY > Authentication Policy** and click the **Edit** button in the upper right corner.

Applying Authentication Policy to VTY Lines

The Edit VTY Lines window will open and you can choose the desired policy from the Authentication Policy drop-down menu.



In the Edit VTY Lines window, you can select which vty lines to edit, specify the EXEC timeout, select the transport protocols, apply access rules, and select the authentication and authorization policies from the respective drop-down boxes. There is a preconfigured default authentication policy, and the custom policies that have additionally been created. The default authentication policy uses the local method, that is, it uses the local user database, to control access. In this example, the custom authentication policy *radius_local* is being applied to the vty lines.

Applying Authorization Policy to VTY Lines

In the Edit VTY Lines window, you can choose the desired policy from the Authorization Policy drop-down menu.



In the Edit VTY Lines window, you can select the authorization policy. There is a preconfigured default authorization policy, and the custom policies that have additionally been created. The default authorization policy uses the local method, that is, it uses the local user database to control access. In this example, the custom authorization policy *radius_local* is being applied to the vty lines.

Verifying AAA Login Authentication Commands

This configuration lists all commands actually sent to the router as a result of the AAA configuration performed in SDM.

Verifying AAA Login Authentication Commands

```
aaa new-model
!
aaa authentication login default local
aaa authentication login radius_local group radius group radius
aaa authorization exec default local
!
username joe secret 5 $1$SlZh$I083V..6/8WEQYTis2SEW1
!
tacacs-server host 10.1.1.10 single-connection key secrettacacs
radius-server host 10.1.1.10 auth-port 1645 acct-port 1646 key
secretradius
!
line vty 0 4
login authentication radius_local
```

The first, second, and fourth command result from enabling AAA on the router. The remaining commands are used to define an authentication policy, create a local user account, configure the AAA servers, and apply the authentication policy to the vty lines.

Troubleshoot AAA Login Authentication on Cisco Routers

This topic describes troubleshooting methods of the AAA login authentication on Cisco IOS routers.

Troubleshoot AAA Login Authentication on Cisco Routers

```
router#  
debug aaa authentication
```

- Use this command to help troubleshoot AAA authentication problems.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-36

Use the **debug aaa authentication** command on your routers to trace AAA packets and monitor authentication.

The command displays debugging messages on authentication functions.

Troubleshoot AAA Authentication Example

Troubleshoot AAA Authentication Example

```
R2#debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''
ruser='' port='tty1' rem_addr='async/81560' authn_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

© 2006 Cisco Systems, Inc. All rights reserved.

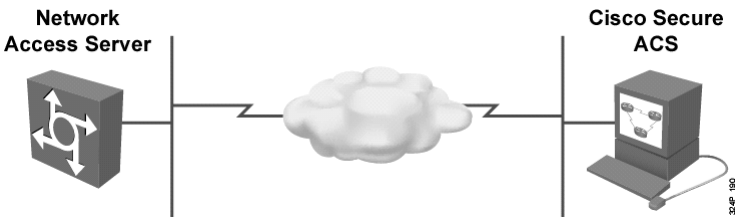
ISCW v1.0-5.37

The **debug aaa authentication** command displays debugging messages on authentication functions. In the example, a user attempts to log in to the router via the tty1 port and tries to access the user mode (privilege level 1) using a plaintext authentication method (Password Authentication Protocol [PAP]). The router identifies the “default” list to be used for authentication. The “default” list has been configured for authentication against the local user database. Subsequent status messages of ‘GETUSER’ and ‘GETPASS’ indicate that the router collects the username and password. A lookup in the local database, denoted as ‘LOCAL’ in the debugging output, verifies that the submitted credentials are correct, and the user is permitted to access the router. This state corresponds to the ‘PASS’ status in the debugging output.

AAA Authorization Commands

This topic describes how to enable AAA authorization.

AAA Authorization Commands



```
router(config)#  
aaa authorization {network | exec | commands level | config-commands  
| reverse-access} {default | list-name} method1 [method2...]
```

Example:

```
router(config)#aaa authorization exec default group radius local none
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-5.39

You can configure the access server to restrict the user to perform certain functions only after successful authentication. Use the **aaa authorization** command in global configuration mode to select the function authorized and the method of authorization.

aaa authorization {**network** | **exec** | **commands level** | **config-commands** | **reverse-access**}
{**default** | *list-name*} *method1* [*method2...*]

aaa authorization Parameters

Parameter	Description
network	All network services, including SLIP, PPP, and AppleTalk Remote Access protocol (ARA protocol)
exec	EXEC process
commands level	All EXEC commands at the specified level (0–15)
config-commands	For configuration mode commands
reverse-access	For reverse Telnet connections
if-authenticated	Allows the user to use the requested function if the user is authenticated
local	Uses the local database for authorization (with the username password or username secret commands)
none	Performs no authorization
group radius	Uses RADIUS for authorization
group tacacs+	Uses TACACS+ for authorization

Authorization Example

This topic provides an authentication and authorization example with character mode access.

Authorization Example

```
R2#show running-config
...
aaa new-model
!
aaa authentication login default local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
...
username admin password 0 cisco123
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-40

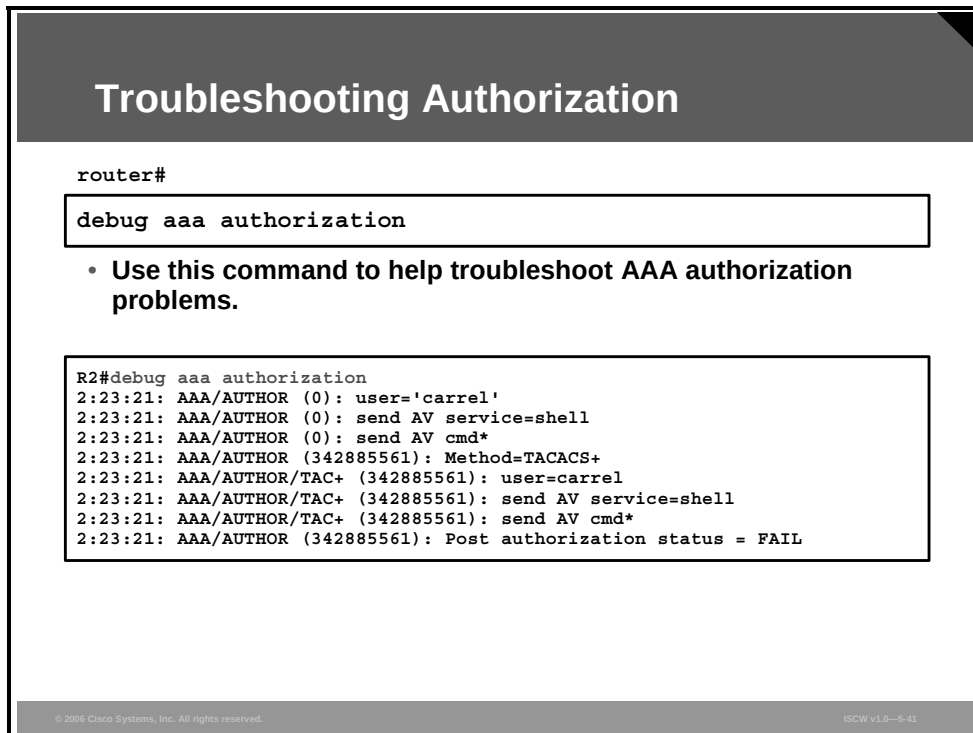
The table shows character mode with authorization commands.

Example of AAA Command Usage

Command	Description
<code>aaa authentication enable default group tacacs+ enable</code>	Determines if the user can access the enabled command level. If authentication via TACACS+ server is unavailable, then use the enable password.
<code>aaa authorization exec default group tacacs+ local</code>	Determines if the user is allowed access to an EXEC shell, and, if so, which shell attributes are permitted or denied. The method is TACACS+. If there is no response from the TACACS+ server, then the method is local, using the local username and password database.
<code>aaa authorization command n default group tacacs+ local</code>	Runs authorization for all commands at the specified privilege level (n). It is possible to have every line entered by a user authorized by TACACS+.

Troubleshooting Authorization

To display information on AAA authorization, use the **debug aaa authorization** command in privileged-EXEC mode. Use the **no debug aaa authorization** form of the command to disable this debug mode.



The figure displays sample output from the **debug aaa authorization** command, which performs an EXEC authorization for user *carrel*. The output is interpreted as follows:

- On the first line, the username *carrel* is authorized.
- On the second and third lines, the AV pairs are authorized.
- The debug output displays a line for each AV pair that is authorized.
- The display indicates the authorization protocol used.
- The final line in the display indicates the status of the authorization process, which, in this case, has failed.

The **aaa authorization** command causes a request packet containing a series of AV pairs to be sent to the TACACS daemon as part of the authorization process. The daemon responds in one of the following three ways:

- Accepts the request as is
- Makes changes to the request
- Refuses the request, thereby refusing authorization

The table describes AV pairs associated with the **debug aaa authorization** command that may appear in the debug output.

AV Pairs Associated with the debug aaa authorization Command

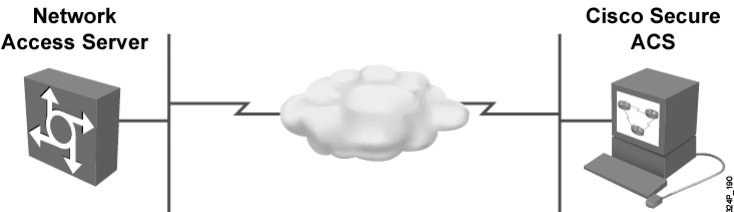
AV Pair	Description
service=arap	Authorization for the ARA protocol is being requested.
service=shell	Authorization for EXEC startup and command authorization is being requested.
service=ppp	Authorization for PPP is being requested.
service=slip	Authorization for SLIP is being requested.
protocol=lcp	Authorization for Link Control Protocol (LCP) is being requested (lower layer of PPP).
protocol=ip	Used with service=slip and service=ppp to indicate which protocol layer is being authorized.
protocol=ipx	Used with service=ppp to indicate which protocol layer is being authorized.
protocol=atalk	Used with service=ppp or service=arap to indicate which protocol layer is being authorized.
protocol=vines	Used with service=ppp for Virtual Integrated Network Service (VINES) over PPP.
protocol=unknown	Used for undefined or unsupported conditions.
cmd=x	Used with service=shell, if cmd=NULL. This is an authorization request to start an EXEC. If cmd is not NULL, this is a command authorization request and will contain the name of the command being authorized (for example, cmd=telnet).
cmd-arg=x	Used with service=shell. When performing command authorization, the name of the command is given by a cmd=x pair for each argument listed (for example, cmd-arg=archie.sura.net).
acl=x	Used with service=shell and service=arap. For ARA, this pair contains an ACL number. For service=shell, this pair contains an access class number (for example, acl=2).
inacl=x	Used with service=ppp and protocol=ip. Contains an IP input ACL for SLIP or PPP/IP (for example, inacl=2).
outacl=x	Used with service=ppp and protocol=ip. Contains an IP output ACL for SLIP or PPP/IP (for example, outacl=4).
addr=x	Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP (for example, addr=172.30.23.11).
routing=x	Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the /routing flag in SLIP and PPP commands. Can either be true or false (for example, routing=true).
timeout=x	Used with service=arap. The number of minutes before an ARA session disconnects (for example, timeout=60).
autocmd=x	Used with service=shell and cmd=NULL. Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet yxz.com).
noescape=x	Used with service=shell and cmd=NULL. Specifies a no escape option to the username configuration command. Can be either true or false (for example, noescape=true).

AV Pair	Description
nohangup=x	Used with service=shell and cmd=NULL. Specifies a no hangup option to the username configuration command. Can be either true or false (for example, nohangup=false).
priv-lvl=x	Used with service=shell and cmd=NULL. Specifies the current privilege level for command authorization as a number from 0 to 15 (for example, priv-lvl=15).
zonelist=x	Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).
addr-pool=x	Used with service=ppp and protocol=ip. Specifies the name of a local pool from which to get the address of the remote host.

AAA Accounting Commands

This topic describes how to use AAA accounting commands.

AAA Accounting Commands



```
router(config)#  
aaa accounting {command level | connection | exec | network |  
system} {default | list-name} {start-stop | stop-only | wait-start}  
group {tacacs+ | radius}
```

Example:

```
R2(config)#aaa accounting exec default start-stop group tacacs+
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-43

Use the **aaa accounting** command in global configuration mode for auditing and billing purposes.

aaa accounting {commands *level* | **connection** | **exec** | **network** | **system**} {**default** | *list-name*} {**start-stop** | **stop-only** | **wait-start**} **group** {**tacacs+** | **radius**}

aaa accounting Parameters

Parameter	Description
commands <i>level</i>	Audits all commands at the specified privilege level (0–15).
connection	Audits all outbound connections, such as Telnet and rlogin.
exec	Audits the EXEC process.
network	Audits all network service requests, such as SLIP, PPP, and ARAP.
system	Audits all system-level events, such as reload.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice has been received by the accounting server.
stop-only	Sends a stop accounting notice at the end of the requested user process.

Parameter	Description
wait-start	As in start-stop , sends both a start and a stop accounting notice to the accounting server. With the wait-start keyword, the requested user service does not begin until the start accounting notice is acknowledged. A stop accounting notice is also sent.
group { tacacs+ radius }	Uses TACACS+ for accounting, or enables RADIUS-style accounting.

AAA Accounting Example

The example shows how to configure a Cisco IOS router for accounting of user EXEC sessions.

AAA Accounting Example

```
R2#show running-config | begin aaa
aaa new-model
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
...
tacacs-server host 10.1.1.3
tacacs-server key SeCrEtKeY
...
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-44

Accounting of user EXEC sessions requires that *aaa new-model* is enabled, and that the authentication and authorization configuration is in place. In the example, TACACS+ is used for authentication, authorization, and accounting purposes.

AAA Accounting Example (Cont.)

The screenshot displays the Cisco Secure ACS web interface. On the left is a navigation menu with options like User Setup, Group Setup, Network Configuration, and Reports and Activity. The main area is titled 'Reports and Activity' and contains a 'Select' dropdown menu. Below this, a list of reports is shown, including 'TACACS+ Accounting'. The 'TACACS+ Accounting' report is selected, displaying a table of active sessions. The table has columns for Date, Time, User-Name, Group-Name, Caller-Id, Acct-Flags, and elapsed time. The data shows several sessions for user 'joe' and 'admin' on 04/13/2006.

Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed time
04/13/2006	18:42:47	joe	Default Group	10.1.1.3	stop	120
04/13/2006	18:40:48	joe	Default Group	10.1.1.3	start	..
04/13/2006	18:39:33	admin	Default Group	10.1.1.3	stop	21
04/13/2006	18:39:12	admin	Default Group	10.1.1.3	start	..
04/13/2006	18:29:35	admin	Default	10.1.1.3	stop	121

The Cisco Secure ACS serves as a central repository for accounting information by completing the access control functionality. Accounting tracks events occurring on the network.

Each session that is established through the Cisco Secure ACS can be fully accounted for and stored on the server. This stored information can be very helpful for management, security audits, capacity planning, and network usage billing. In the example, you use the Cisco Secure ACS to view the accounting information for user EXEC sessions. In ACS, select **Reports and Activity** > **Tacacs+ Accounting**, and if needed - **Refresh**, to view the current accounting information.

Troubleshooting Accounting

To display information on accounting events as they occur, use the **debug aaa accounting** privileged EXEC command, as shown in the figure. Use the **no debug aaa accounting** command to disable debug mode. This figure displays sample output from the **debug aaa accounting** command.

Troubleshooting Accounting

```
router#  
debug aaa accounting
```

- Use this command to help troubleshoot AAA accounting problems.

```
R2#debug aaa accounting  
16:49:21: AAA/ACCT: EXEC acct start, line 10  
16:49:32: AAA/ACCT: Connect start, line 10, glare  
16:49:47: AAA/ACCT: Connection acct stop:  
task_id=70 service=exec port=10 protocol=telnet address=172.31.3.78  
cmd=glare bytes_in=308 bytes_out=76 paks_in=45 paks_out=54  
elapsed_time=14
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-46

The information displayed by the **debug aaa accounting** command is independent of the accounting protocol used to transfer the accounting information to a server. Use the **debug tacacs** and **debug radius** protocol-specific commands to get more detailed information about protocol-level issues.

You can also use the **show accounting** command to step through all active sessions and to print all the accounting records for actively accounted functions. The **show accounting** command enables you to display the active accounting events on the system. This command provides you with a quick look at what is happening, and may also be useful for collecting information in the event of data loss on the accounting server. The **show accounting** command displays additional data on the internal state of the AAA security system, if the **debug aaa accounting** command is active as well.

In the example debugging output, the first two messages inform about the start of an EXEC session through port 10. The third message informs about the termination of that connection and provides additional parameters about the endpoint address, the amount of exchanged data, and session duration.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Authentication, authorization, and accounting are used to effectively control network access.**
- **The router access modes for AAA are character and packet.**
- **The most popular AAA protocols are TACACS+ and RADIUS.**
- **AAA can be configured on the router using CLI or SDM.**
- **SDM simplifies the AAA configuration process.**
- **One of the troubleshooting tools for login authentication is the debug aaa authentication command.**
- **The aaa authorization exec command is used for character mode while aaa authorization network command is used for packet mode access authorization.**
- **The aaa accounting command provides numerous options for accounting purposes.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--5-47

References

For additional information, refer to these resources:

- *Remote Authentication Dial In User Service (RADIUS)* at:
<http://www.ietf.org/rfc/rfc2865.txt>
- *TACACS+ Attribute-Value Pairs* at:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804fe2d8.html

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- **Attacks can target various components of modern networks, such as system integrity, confidentiality, and availability.**
- **Disabled unneeded router services and interfaces make the router less vulnerable to attacks.**
- **Administrative access should be secured using password security features, proper failed login handling, and role-based CLI.**
- **Network devices should be managed using secure protocols, such as SNMPv3, SSH, SSL, and authenticated NTP.**
- **Syslog is the ubiquitous logging protocol.**
- **ACLs filter malicious traffic and mitigate attacks.**
- **AAA operations can be offloaded to a TACACS+ or RADIUS server to increase security and scalability.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—5-1

This module describes various aspects of Cisco device hardening. The most common threats to network devices are described, along with mitigation techniques. The module explains that attackers can compromise unused services, and provides methods to disable them using the command-line interface (CLI) and Security Device Manager (SDM). Administrative access security is introduced, including password security, protection of various access paths, failed login handling, security banner, privilege levels, role-based CLI, and secure configuration files. Furthermore, the module covers traffic filtering using access control lists (ACLs), and explains how to design and implement a secure management system, including secure protocols such as Secure Shell (SSH), Simple Network Management Protocol version 3 (SNMPv3), and authenticated Network Time Protocol (NTP). The module addresses the logging component of a management solution that uses the syslog protocol and various logging levels. The module also describes authentication, authorization, and accounting (AAA), and describes its configuration using both the CLI interface and the SDM. A detailed comparison between the AAA protocols RADIUS and TACACS+ is also provided.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) What is a major difficulty that a hacker would encounter when performing an IP spoofing attack? (Source: Mitigating Network Attacks)
- A) It is difficult to source packets using the IP address of someone else.
 - B) Antispoofing ACLs usually block such attacks.
 - C) Return traffic typically does not go back to the attacker.
 - D) uRPF always blocks such attacks.
- Q2) What is a typical attack against a public web server? (Source: Mitigating Network Attacks)
- A) DoS by TCP SYN flooding
 - B) brute-force attack
 - C) packet sniffer
 - D) exploit of Telnet-based management
- Q3) Which AutoSecure mode should be used for setting up SSH access to a router with an empty configuration: interactive or non-interactive? (Source: Disabling Unused Cisco Router Network Services and Interfaces)
- A) Non-interactive, if default settings are desired.
 - B) Interactive, because the administrator must provide the hostname and domain name.
 - C) Non-interactive, because the RSA keys are generated using the default length.
 - D) Interactive, because it is considered more secure.
- Q4) Can AutoSecure affect connectivity of a lab environment with private addresses? (Source: Disabling Unused Cisco Router Network Services and Interfaces)
- A) No, AutoSecure does not have any caveats.
 - B) Yes, because management plane security requires public addressing.
 - C) Yes, because forwarding plane filtering blocks packets sourced from private address ranges.
- Q5) How can you provide the same degree of protection to line-level passwords and the enable secret password? (Source: Securing Cisco Router Installations and Administrative Access)
- A) By enabling the **service password-encryption**.
 - B) By lowering the protection of the enable secret to the Vigenere cipher.
 - C) You cannot, because the line-level passwords can only be protected using the **service password-encryption** (Vigenere cipher) and the enable secret password cipher uses MD5 encryption.
 - D) By enabling enhanced password security for line-level passwords.

- Q6) What is the Cisco IOS Resilient Configuration feature used for? (Source: Securing Cisco Router Installations and Administrative Access)
- A) to speed up the recovery process once a router is compromised and the IOS image or configuration is erased
 - B) to provide device resilience in a standby router setup
 - C) to prevent anyone from reading the configuration file or the IOS image
 - D) to provide a backup configuration file once the primary is corrupted
- Q7) Why would you use an explicit deny statement to drop all remaining packets at the end of an ACL? (Source: Mitigating Threats and Attacks with Access Lists)
- A) An implicit deny statement at the end of an ACL works only under certain conditions.
 - B) An explicit deny is recommended for strict packet dropping.
 - C) To log the corresponding event.
 - D) Allows longer ACLs to be compiled more effectively.
- Q8) How can you use ACLs to control Telnet and SSH access to a Cisco IOS router? (Source: Mitigating Threats and Attacks with Access Lists)
- A) The only method is to apply the ACLs to the router interfaces in inbound direction.
 - B) By using configuration commands **telnet** and **ssh** that control such access..
 - C) The only method is to use the access-class command in combination with the filtering ACL.
 - D) By using the access-class command in combination with the filtering ACL or applying the filtering ACLs to the router interfaces in inbound direction.
- Q9) Which two of the following can you use to secure a syslog transmission? (Choose two.) (Source: Securing Management and Reporting Features)
- A) ACL deployment
 - B) IPsec protection
 - C) SSL protection
 - D) an out-of-band channel dedicated to management traffic
 - E) nothing, syslog is considered secure for most environments
- Q10) Which IP protocol and port is used by NTP? (Source: Securing Management and Reporting Features)
- A) TCP, port 112
 - B) UDP, port 112
 - C) TCP, port 123
 - D) UDP, port 123
- Q11) What is the difference between TACACS+ and RADIUS? (Source: Configuring AAA on Cisco Routers)
- A) TACACS+ encrypts passwords while RADIUS does not.
 - B) TACACS+ is better for authentication and RADIUS is better for authorization.
 - C) TACACS+ can be used for command authorization while RADIUS cannot.
 - D) TACACS+ has more options than RADIUS.

- Q12) Which three of the following are authorization actions? (Choose three.) (Source: Configuring AAA on Cisco Routers)
- A) assigning a privilege level
 - B) stopping a TCP flooding attack
 - C) denying access to a service
 - D) redirecting the traffic over a better path
 - E) reporting an authorization event
 - F) assigning an IP address
 - G) denying access because of an incorrect username

Module Self-Check Answer Key

Q1)	C
Q2)	A
Q3)	B
Q4)	C
Q5)	C
Q6)	A
Q7)	C
Q8)	D
Q9)	B, D
Q10)	D
Q11)	C
Q12)	A, C, F

Cisco IOS Threat Defense Features

Overview

Cisco IOS Firewall software offers a full set of security features that you can implement to provide security for a network. In this module, you will learn about the Cisco IOS Firewall and Cisco IOS intrusion prevention system (IPS) functionality. The module explains various firewall technologies, such as packet filters, stateful firewalls, and proxy servers, and discusses their filtering capabilities and features. Further, the module describes how to design effective firewall topologies, and how to configure Cisco IOS Firewall functionality on Cisco IOS routers. The module covers the two configuration methods for Cisco IOS Firewall: using the command-line interface (CLI) and the Security Device Manager (SDM). The module also explains the IDS and IPS technologies, describes types of intrusion detection system (IDS) and IPS systems, compares host-based and network-based approaches, describes the placement of IPS systems, lists signature categories, and discusses possible actions that an IOS router can take when an attack is detected. Cisco IOS IPS can, just like the Cisco IOS Firewall, be configured using the CLI and SDM, and both methods are covered. This module explains the IPS configuration wizard included in the SDM, and explains the IPS verification and customization options of the SDM.

Module Objectives

Upon completing this module, you will be able to describe and configure Cisco IOS Firewall features. This ability includes being able to meet these objectives:

- Explain the Cisco IOS Firewall functionality
- Describe the procedure to configure Cisco IOS Firewall features using the CLI and SDM, explain the resulting configurations, and verify firewall operations using SDM and **show** commands
- Explain the features, components, and functionality of Cisco IOS IPS
- Describe the procedure to configure Cisco IOS IPS operations using SDM

Introducing the Cisco IOS Firewall

Overview

This lesson describes the concept of stateful filtering and its implementation on Cisco IOS routers, called Cisco IOS Firewall, formerly known as Content-Based Access Control (CBAC). Cisco IOS Firewall is available on routers running the Cisco IOS Firewall Feature Set (FFS), which includes three main functions: Cisco IOS Firewall, authentication proxy, and the intrusion prevention system (IPS). Authentication proxy and IPS are mentioned briefly, while the lesson focuses on the details of the Cisco IOS Firewall. It describes the handling of TCP and User Datagram Protocol (UDP) and discusses the inspection of the most common application protocols.

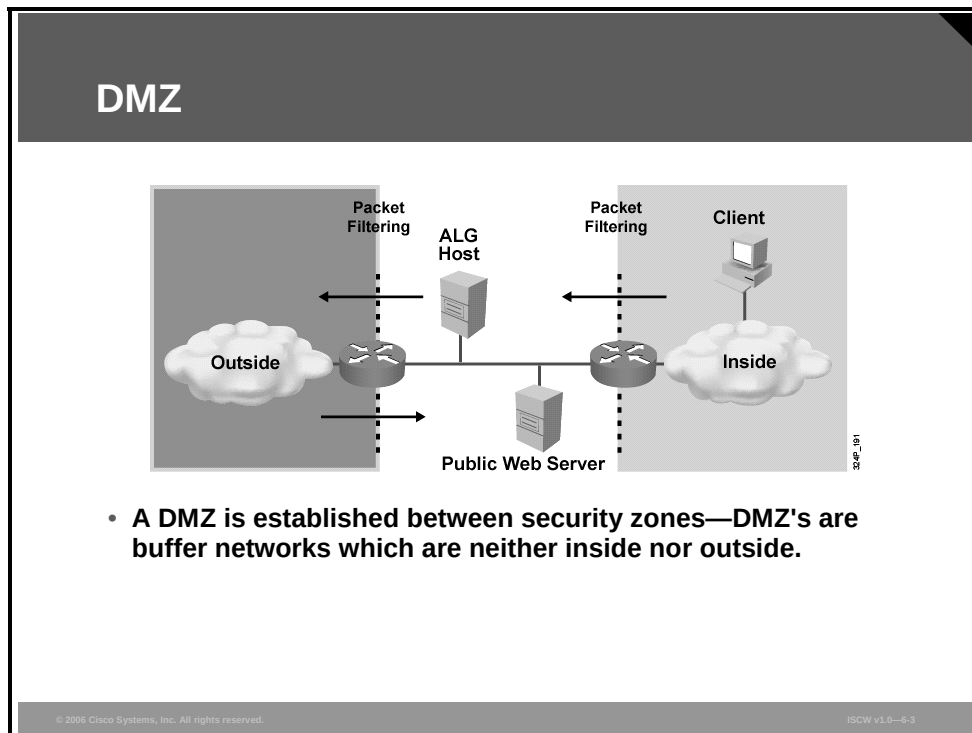
Objectives

Upon completing this lesson, you will be able to explain the Cisco IOS Firewall functionality. This ability includes being able to meet these objectives:

- Explain the basic structure of a layered defense
- Describe the operational strengths and weaknesses of the three firewall technologies
- Explain the basic operation of a stateful firewall
- Describe the features of the Cisco IOS Firewall
- Describe how the Cisco IOS Firewall combines the features of packet inspection and proxy firewalls to provide an optimal security solution
- Explain the Cisco IOS Firewall process

Layered Defense Strategy

This topic describes the basic structure of a layered defense.



Firewalls enforce access control between networks, which can be of different types and levels of trust. A common name for a group of networks reachable over a single firewall network interface is a security zone. A security zone is therefore an administratively separate domain, to or from which a firewall can filter incoming or outgoing traffic. The most notable security zones are *inside* and *outside* networks that are connected to firewalls over *inside* or *outside* interfaces, respectively.

In order to provide a layered approach, the idea of the screened subnet was developed. The idea is based on creation of a buffer network, which is situated between security zones, and actually represents a miniature zone itself. This small network, often called the Demilitarized Zone (DMZ), is neither an inside nor an outside network. It acts as a “no-man’s land,” and access to it is permitted from inside and outside, although typically no traffic can directly cross the DMZ.

Note DMZ is also referred to as a “buffer network” and a “screened subnet.”

Filtering points, set up on DMZ edges to connect it to the inside and outside networks, enforce access control for traffic entering or exiting the DMZ. These filtering points are usually implemented with classic or stateful packet filters.

Another type of a filtering device is a proxy server, also known as an application layer gateway (ALG). An ALG establishes two application sessions—one with the client, and the other with the application server. The ALG acts as server to the client and as client to the server, and provides security by sanitizing the data flow.

Layered Defense Features

This section explains the features of a layered defense approach.

Layered Defense Features

- **Access control is enforced on traffic entering and exiting the buffer network to all security zones by:**
 - Classic routers
 - Dedicated firewalls
- **DMZs are used to host services:**
 - Exposed public services are served on dedicated hosts inside the buffer network.
 - The DMZ may host an application gateway for outbound connectivity.
- **A DMZ contains an attacker in the case of a break-in.**
- **A DMZ is the most useful and common modern architecture.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW V1.0—6-4

The DMZ is an ideal place to host services—public services, exposed servers that untrusted users connect to, or proxy servers such as ALGs—to enable inside users to connect to the outside perimeter.

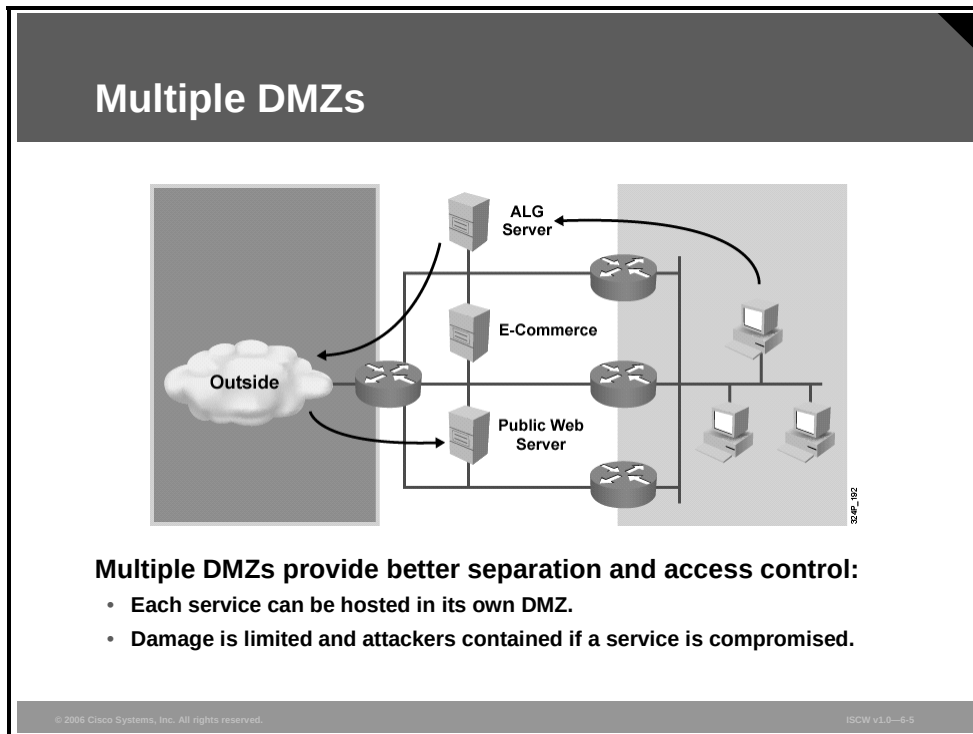
Note Because of its ability to contain an attack and limit damage in the case of a break-in, the DMZ approach is the most popular and commonly used modern architecture.

The multiple layers of security offered by a DMZ are distributed between services and filtering points, as follows:

- The filtering points initially protect the services and, if the services are compromised, limit the ability of an attacker to proceed further into the system. Both entering and exiting traffic is filtered, either by classic routers or dedicated firewalls.
- Public servers placed in the DMZ require proper security measures. The services are hardened, making it difficult for an attacker to compromise them.
- ALGs, also known as proxy servers, located in the DMZ sanitize the data exchange within the application flow. This is especially recommended for outbound connectivity.
- An attacker who manages to break into the DMZ may not be able to launch attacks against the trusted inside network because the filtering points provide additional defense.

Multiple DMZs

The DMZ is a single network, nested between the inside and outside security zones. The concept of multiple DMZs is an alternative.

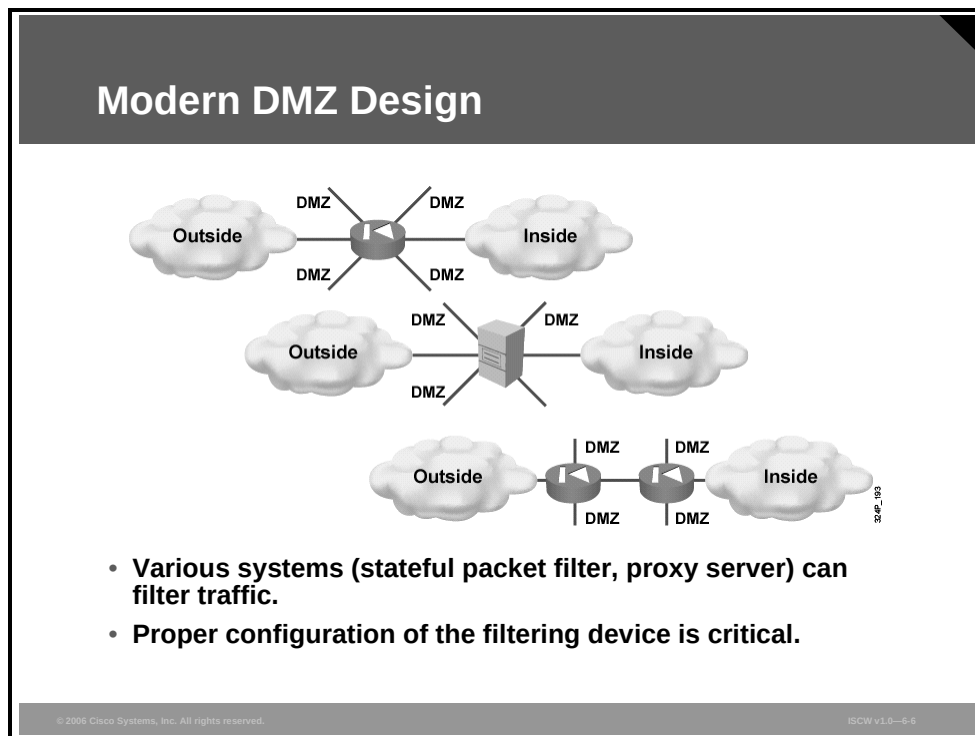


Using a single DMZ zone, there is no access control available between the different hosts inside the DMZ. If a host is broken into, it is likely that other hosts in the same DMZ can be compromised if their operating systems and applications are not properly hardened. For security reasons, modern applications are often multi-tiered, and separating the web server from the application server, as well as the database server, is required in a robust system.

A solution is multiple DMZ networks, in which each DMZ hosts a particular service. The figure illustrates an implementation of a multiple DMZ in which each new DMZ creates a new security zone, with filtering points in each single DMZ controlling traffic entering and exiting. A web server can now be isolated from an application server. A compromise of one server will leave an attacker in an extremely restricted environment, with only a few carefully chosen services available, in accordance with the least privilege philosophy.

Modern DMZ Design

The figure shows simplified versions of the multi-DMZ configuration.



A modern firewall device with multiple “legs or interfaces” creates multiple DMZs, each “leg network” being separated from others via a single filtering device. The single device substitutes “outside” and “inside” routers of a classic DMZ, providing the same level of ingress and egress filtering. Such a setup has the benefit of being simple, manageable, and cost-effective.

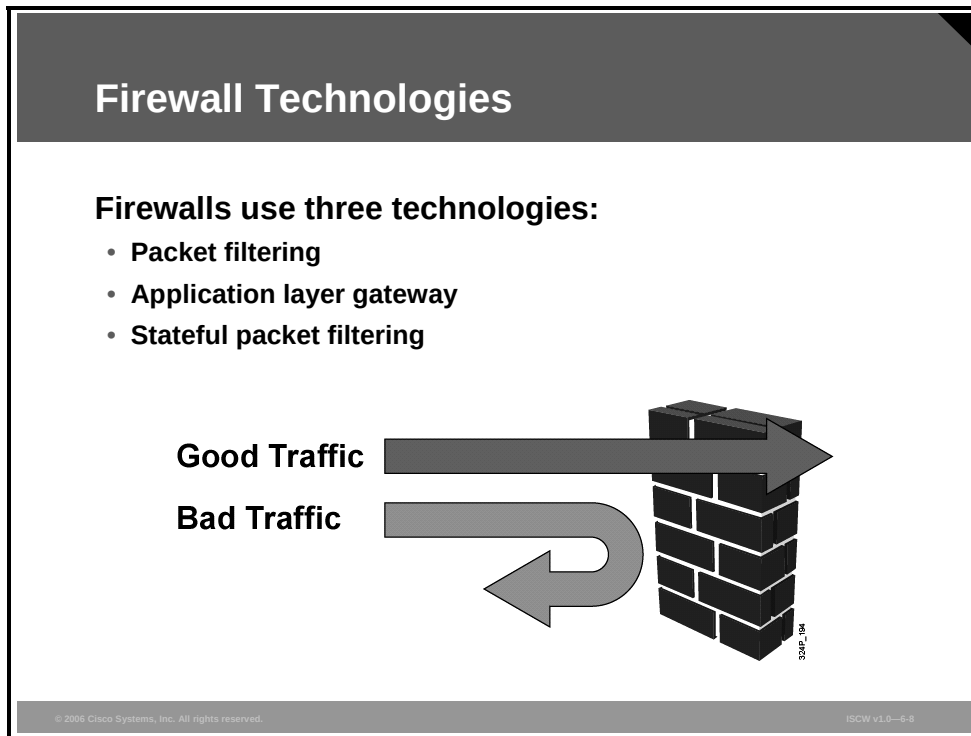
The first topology in the figure illustrates a stateful firewall, also known as stateful packet filter, with six network interfaces attached to it. Two interfaces each connect to the inside and outside networks. The remaining interfaces are for the four DMZs.

The second topology is identical to the first except that an ALG is used as the filtering device instead of a stateful firewall.

The third topology also identifies four DMZs, but two stateful firewalls provide the connectivity structure instead of one. This topology provides better performance, because the filtering tasks are divided between two devices, which provide more security through compartmentalization but increase the overall costs of the solution.

Firewall Technologies

This topic describes the operational strengths and weaknesses of the three firewall technologies: packet filter, stateful firewall, and application gateway.



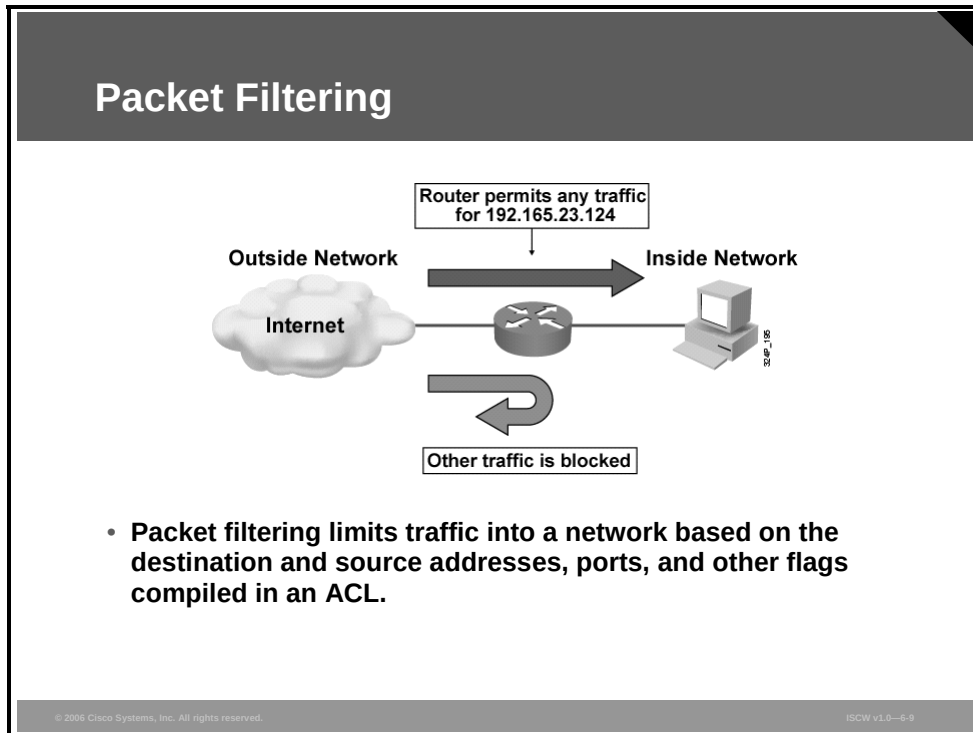
Firewall operations are based on one of the three technologies:

- **Packet filtering:** Packet filtering limits information entering a network based on static packet header information. Packet filtering is usually employed by a Layer 3 device to statically define access control lists (ACLs) that determine which traffic is permitted or denied. Packet filtering can examine protocol header information up to the transport layer to permit or deny certain traffic. Packets that make it through the filters are sent to the requesting system. All other packets are discarded.
- **ALGs work at the application layer.** An ALG is a special piece of software designed to relay application-layer requests and responses between endpoints. An ALG acts as an intermediary between an application client, for which it acts as a virtual server, and a server, for which it acts as a virtual client. The client connects to the proxy server and submits an application layer request. The application layer request includes the true destination and the data request itself. The proxy server analyzes the request and may filter or change its contents, and then opens a session to the destination server. The destination server replies to the proxy server. The proxy server passes the response, which may be filtered and changed, back to the client.
- **Stateful packet filtering:** Stateful packet filtering combines the best of packet filtering and proxy server technologies. Firewalls using stateful packet filtering are also called hybrid firewalls. Stateful packet filtering is the most widely used firewall technology. Stateful packet filtering is an application-aware method of packet filtering that works on the connection, or flow, level. Stateful packet filtering maintains a state table to keep track of all active sessions crossing the firewall. A state table, which is part of the internal structure of the firewall, tracks all sessions and inspects all packets passing through the firewall. If packets have the expected properties, predicted by the state table, they are forwarded. The state table changes dynamically according to the traffic flow.

Note	Each technology has advantages and disadvantages and each one has a “best fit” role to play, depending on the needs of the security policy.

Packet Filtering

A packet filtering firewall selectively routes or drops IP packets based on information in the network (IP) and transport (TCP or UDP) headers. It can be implemented on routers or on dual-homed gateways.



A packet filter uses rules to accept or reject incoming packets based on source and destination IP addresses, source and destination port numbers, and packet type. These rules can also be used to reject any packet from the outside that claims to come from an address inside the network. Recall that each service relies on specific ports. By restricting certain ports, you can restrict those services. For example, blocking port 23 for all user workstations prevents the users from using Telnet, which is an insecure management protocol.

Any device that uses ACLs can do packet filtering. ACLs are probably the most commonly used objects in Cisco IOS router configuration. Not only are they used for packet filtering firewalls, but they can also select specified types of traffic to be analyzed, forwarded, or influenced in some way.

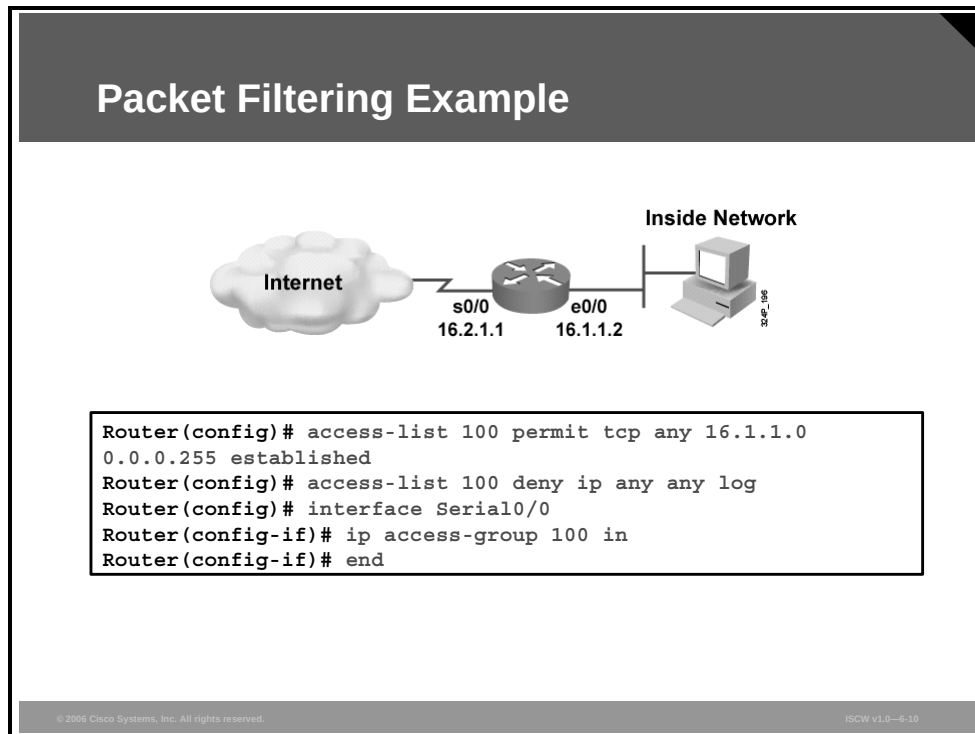
While packet filtering is effective and transparent to users, there are these disadvantages:

- Packet filtering is susceptible to IP spoofing. Arbitrary packets can be sent that fit ACL criteria and pass through the filter.
- Packet filters do not filter fragmented packets well. Because fragmented IP packets carry the TCP header in the first fragment and packet filters filter on TCP header information, all non-first fragments are passed unconditionally. This process is based on the assumption that the filter of the first fragment is accurately enforcing the policy.
- Complex ACLs are difficult to implement and maintain correctly.

Some services cannot be filtered. For example, it is difficult to permit dynamically negotiated sessions without opening up access to a whole range of ports, which in itself might be dangerous.

Packet Filtering Example

The figure shows a simple packet filter example using a Cisco IOS router.

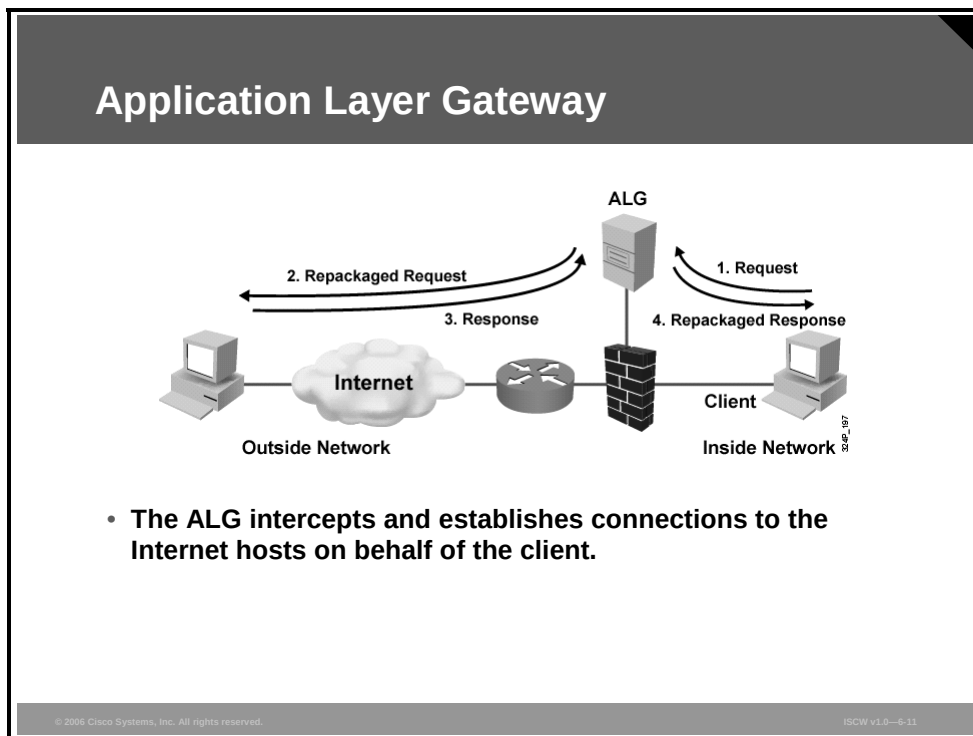


In most network topologies, the Ethernet interface connecting to the internal (inside) network needs to be protected. The serial interface connects to the Internet.

In this example, only one ACL is applied in the inbound direction to the outside interface Serial 0/0. It permits packets from established TCP sessions destined to the inside network 16.1.1.0/24 and drops all other traffic. Packets that belong to established TCP flows are recognized by the ACK flag set to 1 in the TCP header. The sessions have been originated by the hosts in the trusted zone (inside network). There is no ACL blocking the initial flows from the inside network toward the Internet.

Application Layer Gateway

An ALG is a firewall device that examines packets at the application layer of the Open Systems Interconnection (OSI) reference model.



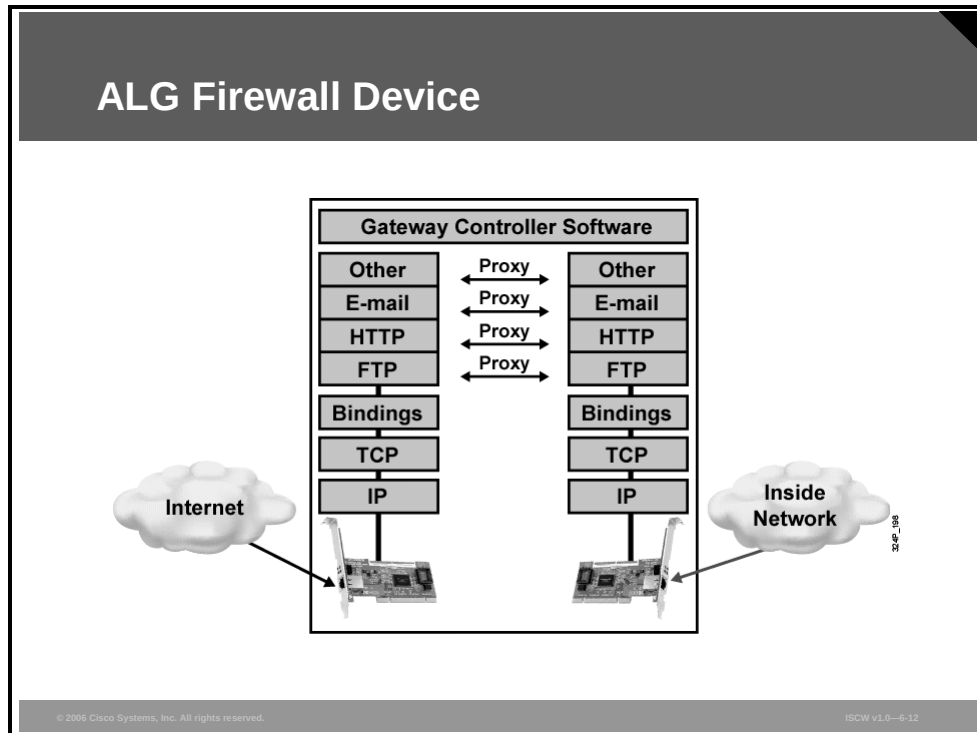
An ALG acts as an intermediary between the users and the protected system. Users gain access to the network by going through a process that establishes sessions, performs user authentication, and enforces authorized policy.

These problems are associated with ALGs:

- ALGs must evaluate a lot of information in many packets and therefore can slow down the network performance.
- ALGs are typically designed to filter a single application. Adding new services would require running multiple ALG programs on one machine or even setting up new ALG hosts.
- ALGs create a single point of failure in the network. If the ALG is compromised, the entire network becomes compromised.

ALG Firewall Device

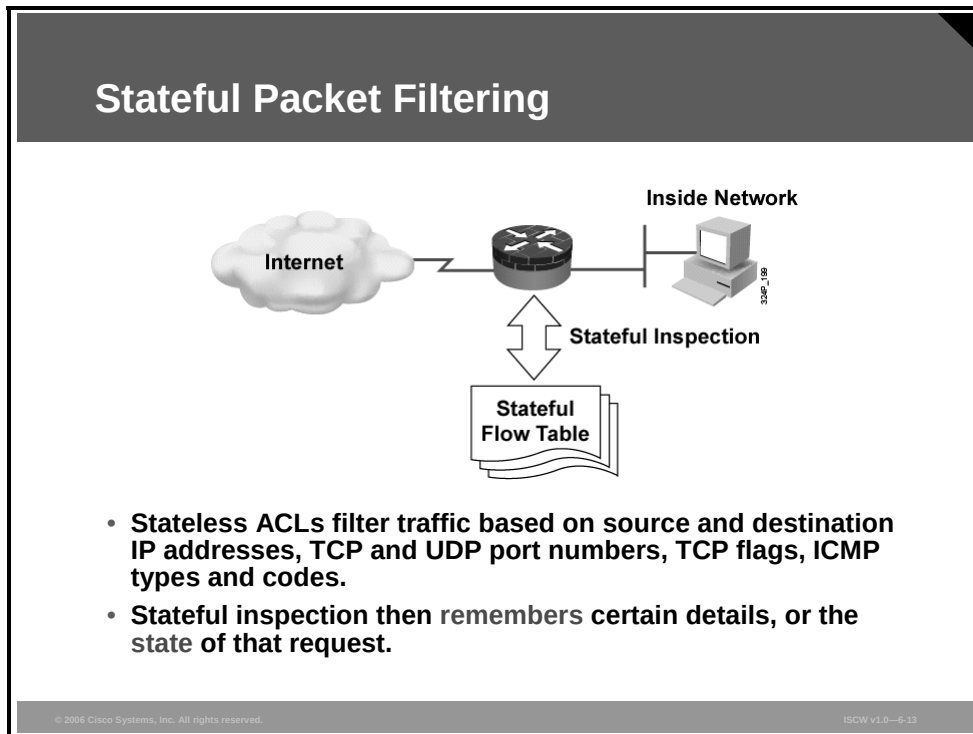
ALG services run at the application level of the network protocol stack for each different type of service (for example FTP or HTTP).



An ALG controls how internal users access the outside world and how Internet users access the internal network. In some cases, the proxy blocks all connections coming from the outside and only allows internal users to access the Internet. The only packets allowed back through the proxy are those that return responses to requests from inside the firewall. In other cases, both inbound and outbound traffic are allowed under strictly controlled conditions. The ALG controls such connectivity by working as a filtering agent for internal or external users.

Stateful Packet Filtering

In the mid-1990s, packet filters and proxy servers were the two technologies used to build firewall systems. As the number of applications that needed to pass through firewalls increased, proxy server vendors could not keep up with the development of new proxy servers. On the other hand, packet filtering also could not support the dynamic nature of the many modern applications. Thus, a new technology was born.



Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection and makes sure the connections are valid. A stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

For example, if the initial packet of a request arrives through the inside interface, the stateful packet filter remembers certain details of that request. This remembering is called “saving the state.” Each time a TCP or UDP connection is established for inbound or outbound connections, the state information is logged in the stateful session table. When the outside system responds to the initial request, the firewall compares the received packets with the saved state to determine if it should be allowed into the network.

Stateful firewalling, also known as stateful packet filtering, is an application-aware method of packet filtering that works on the connection level. A stateful packet filter is application-aware, able to recognize all sessions of a dynamic application. In addition, a stateful packet filter maintains a state table (or connection table), where it keeps track of all the active sessions over the firewall.

Stateful packet filtering is effective for these reasons:

- It works on packets and connections.
- It operates at a higher performance level than packet filtering or using a proxy server.
- It records data for every connection or connectionless transaction in a stateful session flow table. This table serves as a reference point to determine if packets belong to an existing connection or are from an unauthorized source.

Stateful Firewall Operation

This topic describes the operation of a stateful firewall.

Stateful Firewalls

- Also called “Stateful packet filters” and “Application-aware packet filters.”
- Stateful firewalls have two main improvements over packet filters:
 - They maintain a **session table (state table)**, where they track all connections.
 - They recognize **dynamic applications** and know which **additional connections will be initiated between the endpoints**.
- Stateful firewalls inspect every packet, compare it against the state table, and may examine the packet for any special protocol negotiations.
- Stateful firewalls operate mainly at the connection (TCP and UDP) layer.

© 2006 Cisco Systems, Inc. All rights reserved.ISCW v1.0--6-16

The State Table

The state table, or session table, is part of the internal data structure of a stateful packet filter. It tracks all the sessions, and inspects all the packets passing over the stateful packet filter firewall. The packets only pass if they have the expected properties that the state table predicts. The state table dynamically changes and adapts with the traffic flow. If no state exists, a state is created and entered into the state table if the traffic flow meets the rules allowed in the firewall.

Application Awareness

Stateful packet filters are application-aware through additional inspection of passing traffic. By inspecting the session more closely, up to the application layer, a stateful packet filter is able to associate any dynamic channels of the application with the initial session of the application.

The concept of a session in the stateful packet filter world is mainly connected to the TCP and UDP notion of a session. Some stateful packet filter implementations, however, can keep the state of other protocols, such as the Internet Control Message Protocol (ICMP) or Generic Routing Encapsulation (GRE).

Note

Stateful packet filters do not usually change packet headers or payloads in any way. Packets are only compared against the state table and, if permitted, are transmitted in their original form. An SPF may optionally perform Network Address Translation (NAT) or Port Address Translation (PAT). However, address or port translation is distinct from the stateful packet filtering process.

Stateful Packet Filter Handling of Different Protocols

Stateful firewalls provide different filtering granularity for various protocols.

Stateful Firewall Handling of Different Protocols	
TCP Sessions	• Keeping track of a TCP connection is easy (check flow information, check TCP sequence numbers against state table entry)
UDP Connections	• No flags or sequence numbers, hard to robustly track • Only flow information is checked against, timeouts are used to delete state table entries
Other Connectionless Services (GRE, IPsec)	• Usually handled like a stateless packet filter
Dynamic Applications	• Handled automatically by snooping on application negotiation channels

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-16

Stateful Packet Filter Handling of TCP Sessions

When an Stateful Packet Filter permits a TCP session, the session creates an entry in the state table. The Stateful Packet Filter checks every subsequent packet against the state table to verify that each packet is the next expected packet in the session. Stateful firewalls robustly filter TCP sessions. They check the flow information of each packet (network addresses and transport layer ports) to find a matching entry in the state table, and verify that the TCP sequence and acknowledgement numbers are within the expected range. There is a window of allowed values to allow minor reordering of packets, which is legal in IP networks.

Stateful firewalls usually process TCP flags (SYN and ACK), to ensure that a session starts with a proper three-way handshake. The stateful firewalls then remove the state table entry after the session has closed with a connection close, or with a forceful teardown using the restore (RST) flag. Timeouts delete half-open, half-closed, and idle TCP sessions.

Stateful Packet Filter Handling of UDP Connections

The UDP protocol does not contain sufficient information in each packet to robustly verify the integrity of the UDP flow, or its opening or closing. A stateful filter, when permitting a UDP application, creates a state table entry when the first UDP packet is permitted. The state table will contain flow information (network addresses and transport layer ports), and an idle timer. The Stateful Packet Filter permits all packets of the session if they match the flow description, and the state table entry is deleted when the idle timer expires.

Stateful Packet Filter Handling of Other IP Protocols

Stateful firewalls do not usually track other protocols, such as GRE and IPsec, but handle them statelessly, similar to a classic packet filter. If stateful support is provided for other protocols, it is usually similar to that of UDP. When a protocol flow is initially permitted, all packets matching the flow are permitted until an idle timer expires.

Stateful Packet Filter Handling of Dynamic Applications

Dynamic applications, such as FTP, SQLnet, and many protocols used for voice and video signaling and media transfer, open a channel on a well-known port, and then negotiate additional channels through the initial session. Stateful firewalls support these dynamic applications through application inspection features. The Stateful Packet Filter snoops the initial session, and parses the application data to learn about the additional negotiated channels. Then the Stateful Packet Filter usually enforces the policy that if the initial session was permitted, any additional channels of that application should be permitted as well.

Introducing the Cisco IOS Firewall Feature Set

This topic describes the key features of the Cisco IOS Firewall Feature Set.

The Cisco IOS Firewall Feature Set

The Cisco IOS Firewall Feature Set contains three main features:

- Cisco IOS Firewall
- Authentication proxy
- IPS

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-18

The Cisco IOS Firewall Feature Set is a security-specific option for Cisco IOS software available in security IOS images. It integrates robust firewall functionality, authentication proxy, and intrusion prevention for every network perimeter, and enriches existing Cisco IOS security capabilities. It adds more flexibility to existing Cisco IOS security solutions, such as authentication, encryption, and failover, by delivering application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts. When combined with Cisco IOS IPsec software and other Cisco IOS software-based technologies, such as Layer 2 Tunneling Protocol (L2TP) and quality of service (QoS), the Cisco IOS Firewall provides a complete, integrated virtual private network (VPN) solution.

The Cisco IOS Firewall features are designed to prevent unauthorized external individuals from gaining access to your internal network and to block attacks on your network, while at the same time allowing authorized users to access network resources.

Creating a Customized Firewall

To create a firewall customized to the security policy of your organization, you should determine which Cisco IOS Firewall features are appropriate, and configure those features. These are some of the IOS Firewall features to consider:

- Standard and extended ACLs
- TCP intercept
- Cisco IOS Firewall
- Cisco IOS Firewall IPS
- Authentication proxy
- Port-to-application mapping (PAM)

- NAT
- IPsec network security
- Event logging
- User authentication and authorization

Cisco IOS Firewall

The Cisco IOS Firewall, formerly known as CBAC, is the stateful packet filtering engine of a Cisco IOS router. Cisco IOS Firewall allows you to implement firewall intelligence as part of an integrated, single-box solution.

For example, sessions with an extranet partner involving Internet applications, multimedia applications, or Oracle databases no longer need to open a network doorway accessible via weaknesses in the network of a partner. The stateful engine enables tightly secured networks to run the basic application traffic as well as advanced applications, such as multimedia and videoconferencing, securely through a router.

Authentication Proxy

You can create specific security policies for each user with Cisco IOS Firewall dynamic, per-user authentication and authorization.

The authentication proxy feature allows a Cisco IOS router to intercept an HTTP or HTTPS session and prompt the user for authentication. The authentication is typically offloaded to an authentication, authorization, and accounting (AAA) server. In addition to just accepting or denying the connection, the router can download an authorization profile from the AAA server and apply that profile as an ACL to its interface. The profile includes information about the services that are accessible to the connecting user. Consequently all other traffic will be denied.

Intrusion Prevention System

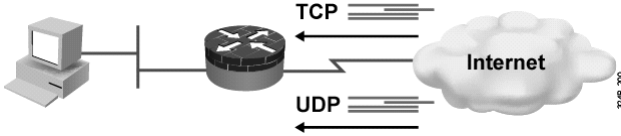
IPSs provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS Firewall IPS technology enhances perimeter firewall protection by taking appropriate actions on packets and flows that violate the security policy, or represent malicious network activity.

Cisco IOS Firewall IPS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. You can now enjoy more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts.

Cisco IOS Firewall

Cisco IOS Firewall is the Stateful Packet Filter engine of Cisco IOS routers.

Cisco IOS Firewall



- **Packets are inspected entering the Cisco IOS firewall if they are not specifically denied by an ACL.**
- **Cisco IOS Firewall permits or denies specified TCP and UDP traffic through a firewall.**
- **A state table is maintained with session information.**
- **ACLs are dynamically created or deleted.**
- **Cisco IOS Firewall protects against DoS attacks.**

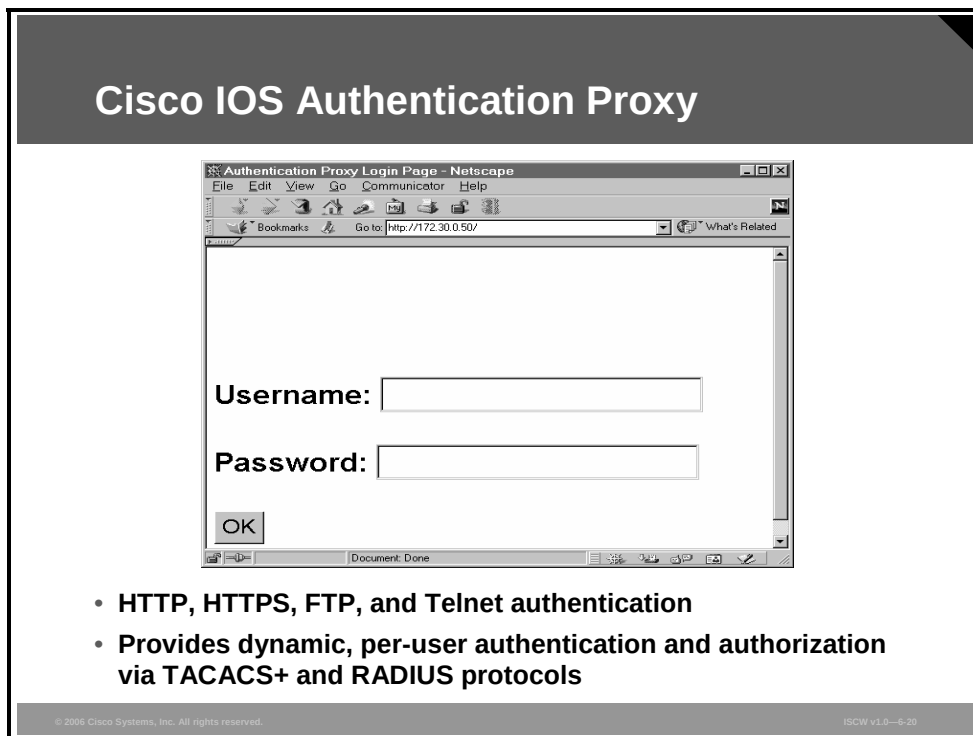
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-19

Cisco IOS Firewall intelligently filters TCP and UDP packets based on application layer protocol session information. It inspects traffic for sessions that originate on any interface of the router and manages state information for TCP and UDP sessions. This state information is used to create temporary openings in the ACLs to allow return traffic and additional data connections for permissible sessions.

Inspecting packets at the application layer and maintaining TCP and UDP session information helps prevent certain types of network attacks, such as SYN flooding. Cisco IOS Firewall inspects packet sequence numbers in TCP connections to see if they are within expected ranges, and drops any suspicious packets. Additionally, Cisco IOS Firewall can detect unusually high rates of new connections and issue alert messages. The firewall inspection can help protect against certain denial of service (DoS) attacks involving fragmented IP packets.

Cisco IOS Firewall Authentication Proxy

The Cisco IOS Firewall authentication proxy feature enables you to apply specific security policies on a per-user basis.



Traditionally, user identity and related authorized access was associated with a user IP address, or a single security policy had to be applied to an entire user group or subnet. Now, users can be identified and authorized on the basis of the per-user policy, and access privileges tailored on an individual basis are possible, as opposed to a general policy applied across multiple users.

With the authentication proxy feature, users can start an HTTP, HTTPS, FTP, or Telnet session that traverses the router, and the router will intercept that session and prompt the user for authentication, as shown in the figure. User-specific access profiles are then automatically retrieved from a Cisco Secure Access Control Server (ACS) or other RADIUS or TACACS+ authentication server and applied to the router interface. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features, such as NAT, IPsec, and VPN client software.

Cisco IOS Firewall IPS

The Cisco IOS Firewall IPS offers intrusion prevention technology for midrange and high-end router platforms with firewall support.

Cisco IOS IPS

- Acts as an inline intrusion prevention sensor—traffic goes through the sensor
- When an attack is detected, the sensor can perform any of these actions:
 - Alarm: Send an alarm to SDM or syslog server.
 - Drop: Drop the packet.
 - Reset: Send TCP resets to terminate the session.
 - Block: Block an attacker IP address or session for a specified time.
- Identifies 700+ common attacks

© 2006 Cisco Systems, Inc. All rights reserved. IOSFW v1.0—6-21

Cisco IOS IPS is especially suited for locations in which a router is deployed and additional security between network segments is required. It can protect intranet and extranet connections where additional security is mandated, and branch-office sites connecting to the corporate office or Internet.

The Cisco IOS Firewall IPS identifies 700 or more prepackaged common attacks using signatures to detect patterns of misuse in network traffic. In addition to the predefined signature database, administrators can define their own custom signatures. The intrusion prevention signatures of the Cisco IOS IPS were chosen from a broad cross-section of intrusion prevention signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

When IOS IPS detects a match against a signature, IOS IPS can be configured to take one or more of the actions listed in the table.

Signature Actions

Action	Description
Alarm	Generates an alert that can be logged to the logging destinations, or via Security Device Event Exchange (SDEE)
Drop	Drops the packet
Reset	Resets the TCP connection by sending TCP RST packets to both the sender and receiver
Block attacker	Blocks all communications from the offending IP address for a specified time

Action	Description
Block connection	Blocks the offending TCP or UDP session for a specified time

Cisco IOS Firewall Functions

This topic describes how Cisco IOS Firewall combines the features of packet inspection and proxy firewalls to provide an optimal security solution.

Cisco IOS ACLs Revisited

- **ACLs provide traffic filtering by these criteria:**
 - **Source and destination IP addresses**
 - **Source and destination ports**
- **ACLs can be used to implement a filtering firewall leading to these security shortcomings:**
 - **Ports opened permanently to allow traffic, creating a security vulnerability**
 - **Do not work with applications that negotiate ports dynamically**
- **Cisco IOS Firewall addresses these shortcomings of ACLs.**

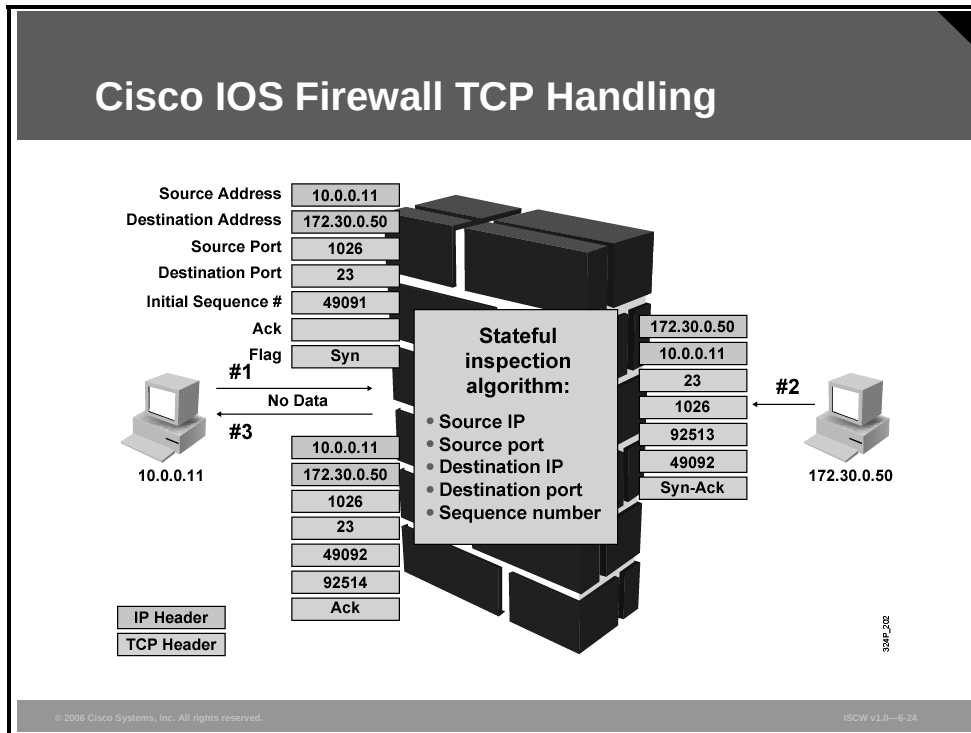
First, some basic ACL concepts need to be reviewed briefly. An ACL provides packet filtering. It has an implied “deny all” at the end of the ACL, and if the ACL is not configured, it permits all connections. Without Cisco IOS Firewall, traffic filtering is limited to ACL implementations that examine packets at the network layer, or at most, the transport layer.

The static nature of classic ACLs has severe security implications for applications that dynamically negotiate additional communication channels. Such dynamic channels must be statically permitted through the ACLs. Attackers can misuse holes created in the ACLs for the dynamic applications in order to inject malicious traffic into the protected network.

These shortcomings are addressed by the stateful packet filtering functionality available in Cisco IOS Firewall.

Cisco IOS Firewall TCP Handling

The figure illustrates TCP filtering on a Cisco IOS Firewall router.



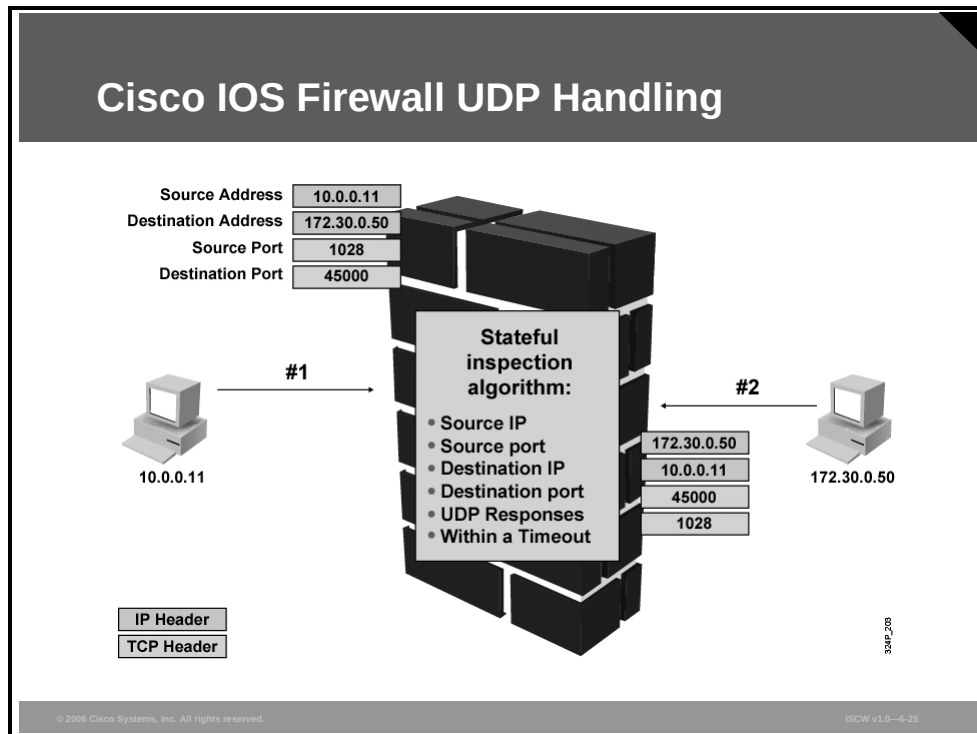
When the first packet from a TCP flow is received by the router (TCP SYN), the inbound ACL on the inside secured interface is checked. If the packet is permitted, a dynamic session entry is created. The session is described by endpoint addresses, port numbers, sequence numbers, and flags. All subsequent packets belonging to this session will be checked against the current state and discarded if invalid.

The figure illustrates the three-way handshake used in TCP. The first packet contains a random sequence number and sets the TCP SYN flag. The second packet contains a random sequence number generated by the responding host, an acknowledgment sequence number which is the received sequence number incremented by one, and the TCP SYN and ACK flags set. The third packet acknowledges the received packet by incrementing its sequence number in the acknowledgment sequence, raising the sequence number by the appropriate number of transmitted octets, and sets the ACK flag. All subsequent segments will increment their sequence numbers by the number of transmitted octets and acknowledge the last received segment by an increment of 1, according to the TCP state machine. After the three-way handshake, all packets will have the ACK flag set, until the session is terminated.

Note Apart from stateful filtering, the router may perform other options, such as address translation (NAT or PAT), or packet authentication (authentication proxy).

Cisco IOS Firewall UDP Handling

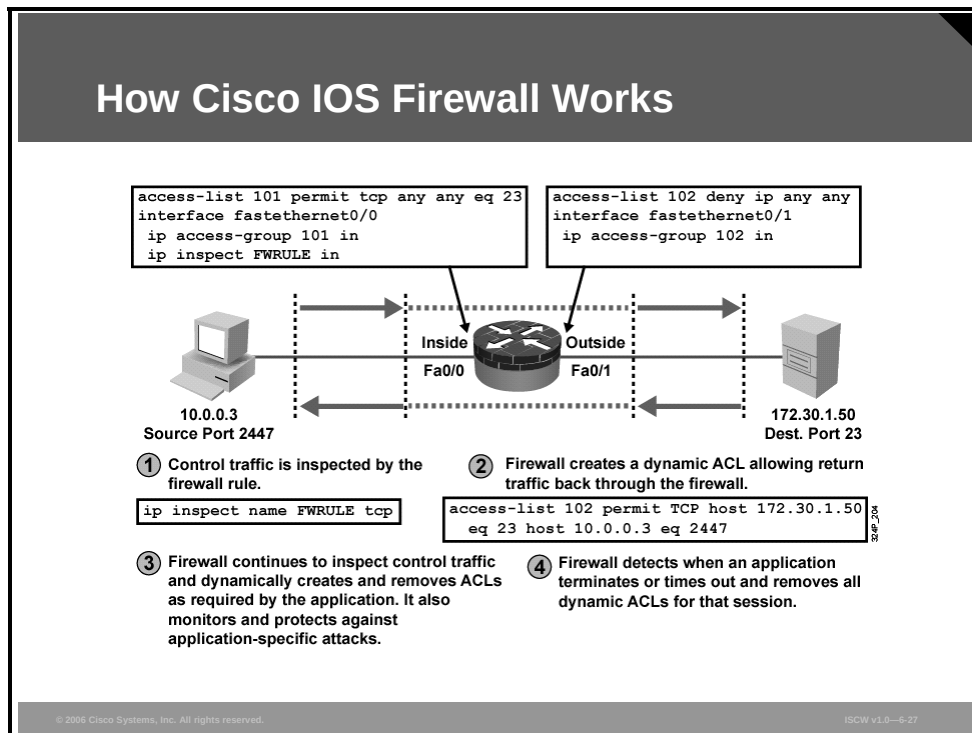
A similar process is invoked when a UDP connection is established through a Cisco IOS Firewall router.



The only difference from the TCP example is that UDP is not stateful, so the router cannot track the sequence numbers and flags. There is no three-way handshake and no teardown process. If the first packet from a UDP flow is permitted through the router, a UDP entry is created in the connection table. The endpoint addresses and port numbers describe the UDP connection entry. When no data is exchanged within the connection for a configurable UDP timeout, the connection description is deleted from the connection table.

Cisco IOS Firewall Process

This topic describes the process of the Cisco IOS Firewall.



With Cisco IOS Firewall, you specify which protocols to inspect, and you specify an interface and interface direction (in or out) where the inspection is applied. The firewall engine inspects only the specified protocol packets if they first pass the inbound ACL applied to the inside interface. If a packet is denied by the ACL, the packet is dropped and not inspected by the firewall.

ACL entries on the inbound ACL applied to the outside interface are dynamically created and deleted. Cisco IOS Firewall dynamically creates and deletes ACL entries at the firewall outside interfaces, according to the information maintained in the state tables. These ACL entries are applied to the outside interface in the inbound direction to examine traffic flowing back into the internal network. These entries create temporary openings in the firewall to permit only traffic that is part of a permissible session initiated from the inside. The temporary ACL entries are never saved to NVRAM.

The figure illustrates the actions when a packet arrives at the Cisco IOS Firewall:

- Step 1** A packet traveling through the inside interface triggers an inspection rule and an entry to be logged in the connection state table.
- Step 2** The IOS firewall opens a dynamic ACL entry allowing the return traffic to be permitted through the outside interface inbound ACL.
- Step 3** The IOS firewall filter engine keeps inspecting the incoming traffic from the outside to permit the proper return traffic and blocks application attacks or misuses.
- Step 4** When the session terminates, the IOS firewall filter engine removes the dynamic information from the connection state table and removes the dynamic ACL entry.

Cisco IOS Firewall inspects and monitors only the control channels of connections; the data channels are not inspected. For example, during FTP sessions, both the control and data channels (which are created when a data file is transferred) are monitored for state changes, but only the control channel is inspected (that is, the firewall engine software parses the FTP commands and responses).

Cisco IOS Firewall inspection recognizes application-specific commands in the control channel and detects and prevents certain application-level attacks. The firewall engine recognizes application-specific commands (such as illegal Simple Mail Transfer Protocol [SMTP] commands) in the control channel, and detects and prevents certain application-level attacks. When the IOS firewall suspects an attack, the IOS firewall can take several actions:

- Generate alert messages
- Protect system resources that could impede performance
- Block packets from suspected attackers

The table lists the timeout and threshold values that Cisco IOS Firewall uses to manage connection state information, helping to determine when to drop connections that do not become fully established or that time out.

Timeout and Threshold Values

Value	Description
Setting timeout values for TCP and UDP sessions	Helps prevent DoS attacks by freeing system resources. Timeouts can be set separately for TCP and UDP.
Setting threshold values for TCP sessions	Helps prevent DoS attacks by controlling the number of half-opened sessions, which limits the amount of system resources applied to half-opened sessions. When a session is dropped, the firewall sends a reset message to the devices at both endpoints (source and destination) of the session. When the system under DoS attack receives a reset command, it releases, or frees, processes and resources related to that incomplete session. Thresholds are configured only for TCP.

Cisco IOS Firewall provides three thresholds against TCP-based DoS attacks:

- The total number of half-opened TCP sessions
- The number of half-opened sessions in a time interval
- The number of half-opened TCP sessions per host

If a threshold for the number of half-opened TCP sessions is exceeded, the firewall engine has two options:

- It can send a reset message to the endpoints of the oldest half-opened session, making resources available to service newly arriving SYN packets.
- It blocks all SYN packets temporarily for the duration configured by the threshold value. When the router blocks a SYN packet, the TCP three-way handshake is never initiated, which prevents the router from using memory and processing resources needed for valid connections.

Supported Protocols

Cisco IOS Firewall supports a wide range of protocols.

Supported Protocols

- TCP (single channel)
- UDP (single channel)
- RPC
- FTP / FTPS
- TFTP
- Telnet / SSH
- UNIX R-commands (such as rlogin, rexec, and rsh)
- SMTP
- HTTP / HTTPS
- ICMP
- SNMP
- Kazaa
- SQL*Net
- RTSP (such as Real Networks)
- Tacacs+ / Radius
- Signalling
 - H.323
 - Skinny
 - SIP
- Other multimedia:
 - Microsoft NetShow
 - StreamWorks
 - VDOLive
- BGP
- And many others

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6-28

You can configure the Cisco IOS Firewall to inspect these types of sessions:

- All TCP sessions, regardless of the application layer protocol (sometimes called single-channel or generic TCP inspection)
- All UDP connections, regardless of the application layer protocol (sometimes called single-channel or generic UDP inspection)

You can also configure Cisco IOS Firewall to specifically inspect certain application layer protocols, which are listed in the table.

Application Layer Protocols

Protocol	Description	Protocol	Description
802-11-iapp	IEEE 802.11 WLANs WG IAPP	ms-sna	Microsoft SNA Server/Base
ace-svr	ACE server/propagation	ms-sql	Microsoft SQL
aol	America Online	ms-sql-m	Microsoft SQL Monitor
appfw	Application firewall	ms-exch-routing	Microsoft Exchange Routing
appleqt	Apple QuickTime	mysql	MySQL
bgp	Border Gateway Protocol (BGP)	n2h2server	N2H2 Filter Service Port
bliff	Bliff mail notification	ncp-tcp	NCP (Novell)
bootpc	Bootstrap Protocol Client	net8-cman	Oracle Net8 Cman/Admin

Protocol	Description	Protocol	Description
bootps	Bootstrap Protocol Server	netbios-dgm	NETBIOS Datagram Service
cddbp	CD Database Protocol	netbios-ns	NETBIOS Name Service
cifs	Common Internet file system (CIFS)	netbios-ssn	NETBIOS Session Service
cisco-fna	Cisco FNATIVE	netshow	Microsoft NetShow Protocol
cisco-net-mgmt	cisco-net-mgmt	netstat	Variant of systat
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs	nfs	Network File System (NFS)
cisco-sys	Cisco SYSMANT	nntp	Network News Transport Protocol (NNTP)
cisco-tdp	Cisco Tag Distribution Protocol (TDP)	ntp	Network Time Protocol (NTP)
cisco-tna	Cisco TNATIVE	oem-agent	OEM Agent (Oracle)
citrix	Citrix IMA/ADMIN/RTMP	oracle	Oracle
citriximaclient	Citrix IMA client	oracle-em-vp	Oracle EM/VP
clp	Cisco Line Protocol	oraclenames	Oracle Names
creativepartnr	Creative Partner	orasrv	Oracle SQL*Net v1/v2
creativeserver	Creative Server	parameter	Specify inspection parameters
cuseeme	CUSEeMe Protocol	pcanywheredata	pcANYWHEREdata
daytime	Daytime (RFC 867)	pcanywherestat	pcANYWHEREstat
dbase	dBASE UNIX	pop3	POP3
dbcontrol_agent	Oracle dbControl Agent po	pop3s	POP3 over TLS/SSL
ddns-v3	Dynamic DNS Version 3	pptp	Point-to-Point Tunneling Protocol (PPTP)
dhcp-failover	Dynamic Host Control Protocol (DHCP) failover	pwdgen	Password Generator Protocol
discard	Discard port	qmtcp	Quick Mail Transfer Protocol
dns	Domain Name System (DNS)	r-winsock	remote-winsock
dnsix	DNSIX Securit Attribute Token Map	radius	RADIUS and accounting
echo	Echo port	rcmd	R commands (r-exec, r-login, r-sh)
entrust-svc-handler	Entrust KM/Administration Service Handler	rdb-dbs-disp	Oracle RDB
entrust-svcs	Entrust sps/aaas/aams	realaudio	Real Audio Protocol

Protocol	Description	Protocol	Description
esmtplib	Extended SMTP	realmedia	RealNetwork's Realmedia Protocol
exec	Remote process execution	realsecure	ISS Real Secure Console Service Port
fcip-port	FCIP	router	Local Routing Process
finger	Finger	rpc	Remote Procedure Call (RPC) Protocol
fragment	IP fragment inspection	rsvd-tcp	RSVD
ftp	File Transfer Protocol (FTP)	rsvp-encap	RSVP ENCAPSULATION-1/2
ftps	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)	rsvp_tunnel	RSVP Tunnel
gdoi	Group Domain of Interpretation (GDOI) Protocol	rtc-pm-port	Oracle RTC-PM port
giop	Oracle GIOP/SSL	rtelnet	Remote Telnet service
gopher	Gopher	rtsp	Real-Time Streaming Protocol (RTSP)
gtpv0	General Packet Radio Service (GPRS) Tunneling Protocol Version 0	send-tcp	SEND
gtpv1	GPRS Tunneling Protocol Version 1	shell	Remote command
h323	H.323 Protocol (Microsoft NetMeeting, Intel Video Phone)	sip	Session Initiation Protocol (SIP)
h323callsigalt	H.323 Call Signal Alternate	sip-tls	SIP-TLS
h323gatestat	H.323 Gatestat	skinny	Skinny Client Control Protocol (SCCP)
hp-alarm-mgr	HP Performance data alarm manager	sms	SMS RCINFO/XFER/CHAT
hp-collector	HP Performance data collector	smtp	Simple Mail Transfer Protocol (SMTP)
hp-managed-node	HP Performance data managed node	snmp	Simple Network Management Protocol (SNMP)
hsrp	Hot Standby Router Protocol (HSRP)	snmptrap	SNMP Trap
http	HTTP	socks	Socks
https	Secure HTTP	sql-net	SQL-NET
ica	ica (Citrix)	sqlnet	SQL Net Protocol
icabrowser	icabrowser (Citrix)	sqlserv	SQL Services
icmp	Internet Control Message Protocol (ICMP)	sqlsrv	SQL Service

Protocol	Description	Protocol	Description
ident	Authentication Service	ssh	SSH Remote Login Protocol
igmpv3lite	Internet Group Management Protocol (IGMP) over UDP for SSM	sshell	SSLshell
imap	IMAP	ssp	State Sync Protocol
imap3	Interactive Mail Access Protocol 3	streamworks	StreamWorks Protocol
imaps	IMAP over TLS/SSL	stun	cisco STUN
ipass	IPASS	sunrpc	SUN Remote Procedure Call
ipsec-msft	Microsoft IP Security (IPSec) NAT-T	syslog	Syslog service
ipx	IPX	syslog-conn	Reliable Syslog service
irc	Internet Relay Chat Protocol	tacacs	Login Host Protocol (TACACS)
irc-serv	IRC-SERV	tacacs-ds	TACACS -Database Service
ircs	IRC over TLS/SSL	tarantella	Tarantella
ircu	IRCU	tcp	Transmission Control Protocol (TCP)
isakmp	ISAKMP	telnet	Telnet
iscsi	iSCSI	telnets	Telnet over TLS/SSL
iscsi-target	iSCSI port	tftp	Trivial File Transfer Protocol (TFTP)
kazaa	KAZAA	time	Time
kerberos	Kerberos	timed	Time server
kermit	kermit	tr-rsrb	Cisco RSRB
l2tp	Layer 2 Tunneling Protocol (L2TP)/Layer 2 Forwarding (L2F)	ttc	Oracle TTC/SSL
ldap	Lightweight Directory Access Protocol (LDAP)	udp	User Datagram Protocol (UDP)
ldap-admin	LDAP admin server port	uucp	UUCPD/UUCP-RLOGIN
ldaps	LDAP over TLS/SSL	vdolive	VDOLive Protocol
login	Remote login	vqp	VQP
lotusmtap	Lotus Mail Tracking Agent Protocol	webster	Network dictionary
lotusnote	Lotus Notes	who	Whois service
microsoft-ds	Microsoft-DS	wins	Microsoft WINS
ms-cluster-net	Microsoft Cluster Net	x11	X Window System
ms-dotnetster	Microsoft .NETster Port	xdmcp	XDM Control Protocol

Refer to the latest Cisco IOS documentation for the latest and full listing of the IOS Firewall applications support.

When a protocol is filtered by the firewall, that protocol traffic is inspected, state information is maintained, and, in general, packets are allowed back through the firewall only if they belong to a permissible session.

Alerts and Audit Trails

Cisco IOS Firewall generates real-time alerts and audit trails based on events tracked by the firewall engine.

Alerts and Audit Trails

- Cisco IOS Firewall generates real-time alerts and audit trails.
- Audit trail features use syslog to track all network transactions.
- With Cisco IOS Firewall inspection rules, you can configure alerts and audit trail information on a per-application protocol basis.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6-29

Enhanced audit trail features use syslog to track all network transactions, recording time stamps, source host, destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting.

Real-time alerts send syslog error messages to central management consoles upon detecting suspicious activity. Using firewall inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the inspection rule covering HTTP inspection.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Layered defense strategy enhances security by providing buffer networks with filtering capabilities.**
- **There are three main firewall technologies: packet filtering, application proxy, and stateful packet filtering.**
- **The Cisco IOS Feature Set contains three main features: Cisco IOS Firewall, authentication proxy, and IPS.**
- **Cisco IOS Firewall intelligently filters TCP and UDP packets based on session and application layer protocol information.**
- **The Cisco IOS authentication proxy is used to apply specific security policies on a per-user basis.**
- **The Cisco IOS IPS identifies attacks using signatures to detect patterns of misuse in network traffic.**

Implementing Cisco IOS Firewalls

Overview

The attacks on the internal network of your enterprise can be mitigated in different ways. One of those ways is to implement a firewall to separate your internal network from the outside network.

Objectives

Upon completing this lesson, you will be able to describe the procedure to configure Cisco IOS Firewall features using the CLI and SDM, explain the resulting configurations, and verify firewall operations using SDM and **show** commands. This ability includes being able to meet these objectives:

- Explain the procedure to configure Cisco IOS Firewall from the Cisco IOS CLI
- Explain when and how to use the Basic and Advanced Firewall Configuration wizards in SDM
- Explain how to configure a basic firewall using SDM
- Explain how to configure the interfaces on an advanced firewall using SDM
- Explain how to configure a DMZ on an advanced firewall
- Explain how to configure inspection rules
- Explain how to complete the Advanced Firewall wizard configuration by viewing the settings in the Summary window
- Explain how to use the SDM logging function to monitor firewall activity

Configuring Cisco IOS Firewall from the CLI

This topic describes the procedure to configure Cisco IOS Firewall from the CLI.

Cisco IOS Firewall Configuration Tasks Using the CLI

1. **Pick an interface: internal or external.**
2. **Configure IP ACLs at the interface.**
3. **Define inspection rules.**
4. **Apply inspection rules and ACLs to interfaces.**
5. **Test and verify.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-6.3

To configure Cisco IOS Firewall through the CLI, you should perform the tasks described in the figure. The first two tasks are discussed below, and the remaining tasks are covered on the next pages.

Pick an Interface: Internal or External

You must decide whether to configure Cisco IOS Firewall on an internal or external router interface.

If you configure the firewall in two directions, you should configure the inspection in one direction first, using the appropriate internal and external interface designations. When you configure the inspection in the other direction, the interface designations will be swapped.

Note Cisco IOS Firewall can be configured in two directions at one or more interfaces. Configure the firewall in two directions when the networks on both sides of the firewall require protection, such as with extranet or intranet configurations, and for protection against denial of service (DoS) attacks.

Configure IP ACLs at the Interface

For Cisco IOS Firewall to work properly, you need to make sure that you have IP ACLs configured appropriately at the inside, outside, and Demilitarized Zone (DMZ) interfaces.

Follow these general rules when evaluating your IP ACLs at the firewall:

- Start with a basic configuration. A basic initial configuration allows all network traffic to flow from protected networks to unprotected networks, while it blocks network traffic from any unprotected networks.

- Permit traffic that should be inspected by the Cisco IOS Firewall. For example, if Telnet will be inspected by the firewall, then Telnet traffic should be permitted on all ACLs that apply to the initial Telnet flow.
- Use extended ACLs to filter traffic entering the router from the unprotected networks. For temporary openings to be created dynamically by Cisco IOS Firewall, the access control list (ACL) for the returning traffic must be an extended ACL.

Note If your firewall only has two connections, one to the internal network and one to the external network, using all inbound ACLs works well because packets are stopped before they get a chance to affect the router itself.

- Deny any inbound traffic (incoming on external interface) from a source address matching an address on the protected network. This is known as antispoofing protection, because it prevents traffic from an unprotected network from assuming the identity of a device on the protected network.
- Deny broadcast messages with a source address of 255.255.255.255. This entry helps to prevent broadcast attacks.
- By default, the last entry in an ACL is an implicit denial of all IP traffic not specifically allowed by other entries in the ACL. Optionally, you can add an entry to the ACL denying IP traffic with any source or destination address, thus making the denial rule explicit. This is especially useful if you want to log information about the denied packets.

For complete information about how to configure IP ACLs, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*.

For complete information about Cisco IOS Firewall configuration, including optional parameters, refer to

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html.

Note You do not necessarily need to configure an extended ACL at both the outbound internal interface and the inbound external interface, but at least one is necessary to restrict traffic flowing through the firewall into the internal protected network.

Set Audit Trails and Alerts

This section explains how to configure notification settings in Cisco IOS Firewall.

Set Audit Trails and Alerts

```
Router(config)#  
ip inspect audit-trail
```

- Enables the delivery of audit trail messages using syslog

```
Router(config)#  
no ip inspect alert-off
```

- Enables real-time alerts

```
Router(config)#logging on  
Router(config)#logging host 10.0.0.3  
Router(config)#ip inspect audit-trail  
Router(config)#no ip inspect alert-off
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-6.4

Turn on audit trail logging and real-time alerts globally to provide a record of network access through the firewall, including illegitimate access attempts, and inbound and outbound services:

- Step 1** Turn on logging to your syslog host using standard logging commands. Set the syslog server IP address with the **logging host** command.
- Step 2** Turn on Cisco IOS Firewall audit trail messages using the **ip inspect audit-trail** command in global configuration mode.
- Step 3** The Cisco IOS Firewall real-time alerts are off by default (the command **ip inspect alert-off** is active by default). To enable real-time alerts, the **no** version of the command is needed—so use **no ip inspect alert-off** command in global configuration mode.

Inspection Rules for Application Protocols

You must define inspection rules to specify which IP traffic (that is, which application layer protocols) will be inspected by Cisco IOS Firewall at an interface.

Define Inspection Rules for Application Protocols

```
Router(config)#
```

```
ip inspect name inspection-name protocol [alert  
{on|off}] [audit-trail {on|off}] [timeout seconds]
```

- Defines the application protocols to inspect.
- Will be applied to an interface:
 - Available protocols are tcp, udp, icmp, smtp, esmtp, cuseeme, ftp, ftps, http, h323, netshow, rcmd, realaudio, rpc, rtsp, sip, skinny, sqlnet, tftp, vdolive, etc.
 - Alert, audit-trail, and timeout are configurable per protocol, and override global settings.

```
Router(config)#ip inspect name FWRULE smtp alert on audit-trail on timeout 300  
Router(config)#ip inspect name FWRULE ftp alert on audit-trail on timeout 300
```

© 2006 Cisco Systems, Inc. All rights reserved.ISFW v1.0-6.5

Normally, you define only one inspection rule. The only exception might occur if you want to enable the firewall engine in two directions at a single firewall interface. In this case you must configure two rules, one for each direction.

An inspection rule should specify each desired application layer protocol that needs to be inspected, as well as generic TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP), if desired.

Note Generic TCP and UDP inspection dynamically permits return traffic of active sessions. ICMP inspection allows ICMP echo reply packets forwarded as a response to previously seen ICMP echo messages.

The inspection rule consists of a series of statements, each listing a protocol and specifying the same inspection rule name. Inspection rules include options for controlling alert and audit trail messages, and for checking IP packet fragmentation.

In the figure, the IP inspection rule shown is named FWRULE. This rule will inspect the extended Simple Mail Transfer Protocol (SMTP) and FTP protocols with alert and audit trail enabled, and an idle timeout of 300 seconds.

Use the **ip inspect name** command in global configuration mode to define a set of inspection rules. Use the **no** form of this command to remove the inspection rule for a protocol, or to remove the entire set of inspection rules.

ip inspect name *inspection-name* protocol [alert {on | off}] [audit-trail {on | off}] [timeout *seconds*]

ip inspect name Parameters

Parameter	Description
<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name.
<i>protocol</i>	The protocol to inspect.
alert {on off}	(Optional) For each inspected protocol, the generation of alert messages can be set to on or off. If no option is selected, alerts are generated based on the setting of the ip inspect alert-off command.
audit-trail {on off}	(Optional) For each inspected protocol, the audit-trail option can be set to on or off. If no option is selected, audit trail messages are generated based on the setting of the ip inspect audit-trail command.
timeout <i>seconds</i>	(Optional) Specify the number of seconds for a different idle timeout to override the global TCP or UDP idle timeouts for the specified protocol. This timeout overrides the global TCP and UDP timeouts, but will not override the global Domain Name Service (DNS) timeout.

Apply an Inspection Rule to an Interface

Next, an inspection rule must be applied to an interface.

Apply an Inspection Rule to an Interface

```
Router(config-if)#  
ip inspect inspection-name {in | out}
```

- Applies the named inspection rule to an interface

```
Router(config)#interface e0/0  
Router(config-if)#ip inspect FWRULE in
```

- Applies the inspection rule to interface e0/0 in inward direction

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-6-6

Use the **ip inspect** interface configuration command to apply a set of inspection rules to an interface in either the inbound or outbound direction.

ip inspect *inspection-name* {**in** | **out**}

ip inspect Parameters

Parameter	Description
<i>inspection-name</i>	Names the set of inspection rules
in	Applies the inspection rules to inbound traffic
out	Applies the inspection rules to outbound traffic

Guidelines for Applying Inspection Rules and ACLs to Interfaces

For the Cisco IOS Firewall to be effective, both inspection rules and ACLs must be strategically applied to all the router interfaces.

Guidelines for Applying Inspection Rules and ACLs to Interfaces

- **On the interface where traffic initiates:**
 - **Apply ACL on the inward direction that permits only wanted traffic.**
 - **Apply rule on the inward direction that inspects wanted traffic.**
- **On all other interfaces, apply ACL on the inward direction that denies all unwanted traffic.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6-7

The general rule of thumb for applying inspection rules and ACLs on the router is as follows:

- On the interface where traffic initiates:
 - Apply the ACL in the inward direction that permits only wanted traffic.
 - Apply the rule in the inward direction that inspects wanted traffic.
- On all other interfaces, apply the ACL in the inward direction that denies all traffic, except traffic that has not been inspected by the firewall, such as Generic Routing Encapsulation (GRE) and ICMP that is not related to echo and echo reply messages.

Example: Two-Interface Firewall

The figure shows a simple, two-interface Cisco IOS Firewall configuration example.

Example: Two-Interface Firewall

```
ip inspect name OUTBOUND tcp
ip inspect name OUTBOUND udp
ip inspect name OUTBOUND icmp
!
interface FastEthernet0/0
 ip access-group OUTSIDEACL in
!
interface FastEthernet0/1
 ip inspect OUTBOUND in
 ip access-group INSIDEACL in
!
ip access-list extended OUTSIDEACL
 permit icmp any any packet-too-big
 deny ip any any log
!
ip access-list extended INSIDEACL
 permit tcp any any
 permit udp any any
 permit icmp any any
```

Inside Fa0/1 Fa0/0 Outside

Permit outbound TCP, UDP, and ICMP flows

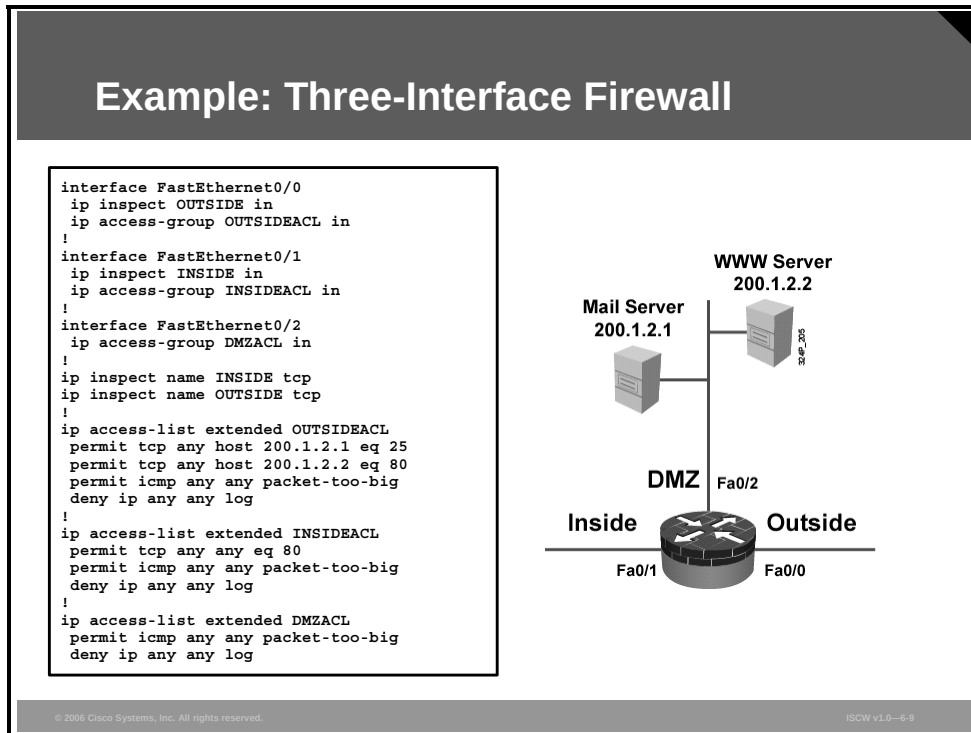
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-6

The simplest, clearest, and easiest-to-verify configuration results when both an ACL and an inspection rule are applied inbound on an interface. Because such configurations are easy to verify, the chance to leave backdoors is minimized.

In this example, the inspection rule OUTBOUND performs generic TCP, UDP, and ICMP traffic. The access list OUTSIDEACL is applied to the outside interface and blocks all incoming traffic except ICMP unreachable “packet-too-big” messages that support maximum transmission unit (MTU) path discovery. The access list INSIDEACL, applied to the inside interface in the inbound direction, permits all TCP, UDP and ICMP traffic initiated from the inside network. The inspection rule OUTBOUND, applied to the inside interface in the inbound direction, inspects the outbound packets and automatically allows the corresponding return traffic.

Example: Three-Interface Firewall

The figure shows a Cisco IOS Firewall configuration example with three interfaces.



In this example, inside users are permitted to browse the Internet. Outbound HTTP sessions are allowed by the ACL INSIDEACL applied to the inside interface in inbound direction. Further, outside clients are allowed to communicate with the SMTP server (200.1.2.1) and HTTP server (200.1.2.2) located in the enterprise DMZ. Inbound SMTP and HTTP are permitted by the ACL OUTSIDEACL applied to the outside interface in inbound direction. Additionally, ICMP unreachable “packet-too-big” messages are accepted on all interfaces to support MTU path discovery. The inspection rules include the generic TCP inspection and are applied to inbound connections on the outside interface and to outbound sessions on the inside interface. The TCP inspection will automatically allow return traffic of the outbound HTTP sessions and allow return traffic of the inbound SMTP and HTTP sessions.

Verifying Cisco IOS Firewall

Cisco IOS CLI offers several commands that verify the configuration and inspected sessions of Cisco IOS Firewall.

Verifying Cisco IOS Firewall

```
Router#  
show ip inspect name inspection-name  
show ip inspect config  
show ip inspect interfaces  
show ip inspect session [detail]  
show ip inspect statistics  
show ip inspect all
```

- Displays inspections, interface configurations, sessions, and statistics

```
Router#show ip inspect session  
Established Sessions  
Session 6155930C (10.0.0.3:35009)=>(172.30.0.50:34233) tcp SIS_OPEN  
Session 6156F0CC (10.0.0.3:35011)=>(172.30.0.50:34234) tcp SIS_OPEN  
Session 6156AF74 (10.0.0.3:35010)=>(172.30.0.50:5002) tcp SIS_OPEN
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-10

Use the **show ip inspect EXEC** command to display information about various components of Cisco IOS Firewall.

In this example, three TCP sessions have been established from host 10.0.0.3 to the host 172.30.0.50 and inspected by the Cisco IOS Firewall. The output of the command includes the respective port numbers involved in the TCP communications.

show ip inspect {**name** *inspection-name* | **config** | **interfaces** | **statistics** | **session** [**detail**] | **all**}

show ip inspect Parameters

Parameter	Description
name <i>inspection-name</i>	Shows the configured inspection rule for the inspection name.
config	Shows the complete inspection configuration.
interfaces	Shows the interface configuration with respect to applied inspection rules and ACLs.
statistics	Shows the inspection statistics such as current session count and max session counts.
session [detail]	Shows existing sessions that are currently being tracked and inspected by Cisco IOS Firewall. The optional detail keyword shows additional details about these sessions.
all	Shows the complete firewall configuration, and all existing sessions that are currently being tracked and inspected.

Troubleshooting Cisco IOS Firewall

Cisco IOS CLI offers several commands that assist in troubleshooting Cisco IOS Firewall.

Troubleshooting Cisco IOS Firewall

```
Router#
debug ip inspect function-trace
debug ip inspect object-creation
debug ip inspect object-deletion
debug ip inspect events
debug ip inspect timers
debug ip inspect detail
```

- General debug commands

```
Router#
debug ip inspect protocol
```

- Protocol-specific debug

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6-11

Use the **debug ip inspect EXEC** command to display messages about firewall events.

debug ip inspect {function-trace | object-creation | object-deletion | events | timers | protocol | detailed}

debug ip inspect Parameters

Parameter	Description
function-trace	Displays messages about software functions called by the firewall.
object-creation	Displays messages about created software objects. Object creation corresponds to the beginning of inspected sessions.
object-deletion	Displays messages about deleted software objects. Object deletion corresponds to the closing of inspected sessions.
events	Displays messages about software events, including information about packet processing.
timers	Displays messages about timer events, such as when an idle timeout is reached.
<i>protocol</i>	Displays messages about inspected protocol events, including details about the packets of the protocol.
detailed	Displays detailed information for all other enabled debugging. Use this form of the command in conjunction with other firewall debugging commands.

Basic and Advanced Firewall Wizards

This topic describes when and how to use the Basic and Advanced Firewall Configuration wizards in SDM.

Basic and Advanced Firewall Wizards

- **SDM offers configuration wizards to simplify Cisco IOS Firewall configuration.**
- **Two configuration wizards exist:**
 - **Basic Firewall Configuration wizard:**
 - Supports two interface types (Inside and Outside)
 - Applies predefined rules
 - **Advanced Firewall Configuration wizard:**
 - Supports more interfaces (Inside, Outside, and DMZ)
 - Applies predefined or custom rules

© 2006 Cisco Systems, Inc. All rights reserved.

ISFW v1.0—6-13

SDM, a configuration and management tool for Cisco IOS routers using a GUI, offers a simple method to set up the Cisco IOS Firewall. Depending on the number of router interfaces, you will select either the Basic Firewall Configuration wizard, which supports only one outside interface and one or more inside interfaces, or the Advanced Firewall Configuration wizard, which, in addition to the inside and outside interfaces, also supports a DMZ interface.

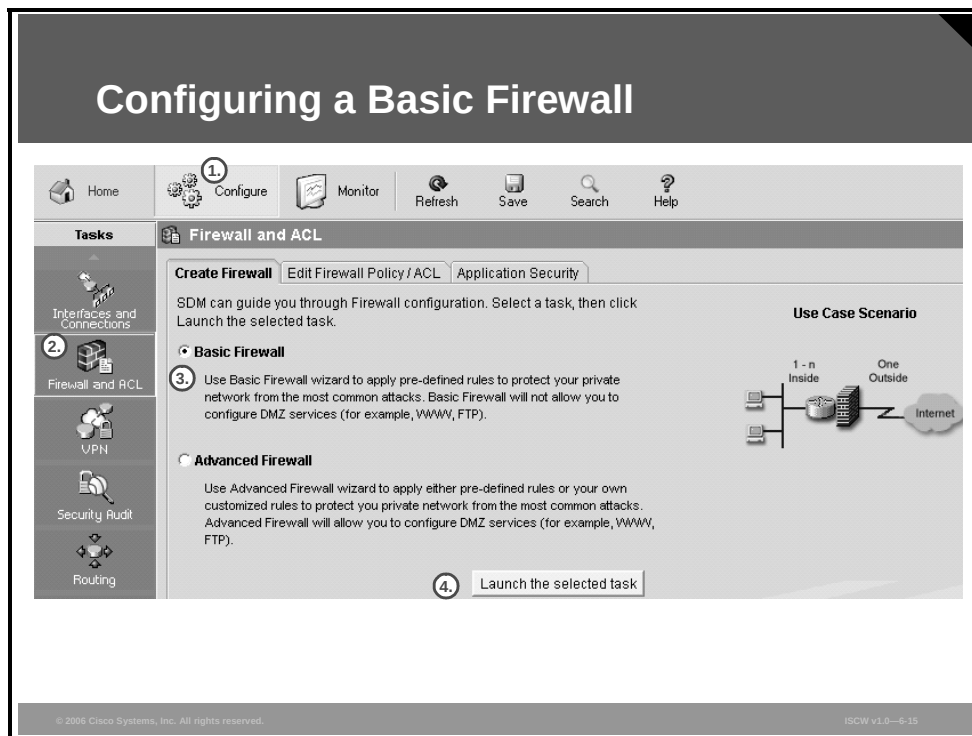
The Basic Firewall Configuration wizard applies default access rules to both inside and outside interfaces, applies default inspection rules to the outside interface, and enables IP unicast reverse-path forwarding on the outside interface.

The Advanced Firewall Configuration wizard applies default or custom access rules, as well as default or custom inspection rules, to inside, outside, and DMZ interfaces. Furthermore, the Advanced Firewall Configuration wizard enables IP unicast reverse-path forwarding on the outside interface.

Note	Unicast reverse path forwarding checks incoming packets for IP source address integrity and compares the source IP address with the routing table. If the packet arrived on one interface and the IP route to the source network points to another interface, it means that the packet traversed a suboptimal path and will be discarded.

Configuring a Basic Firewall

This topic describes how to configure a basic firewall.



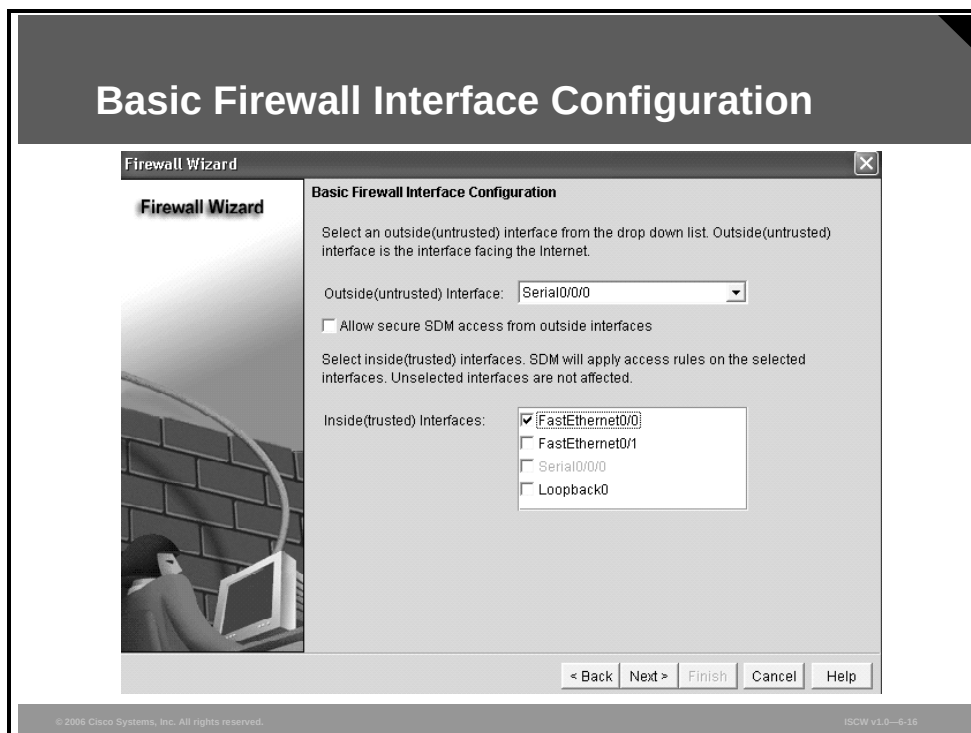
To launch the Basic Firewall Configuration wizard, follow this procedure:

- Step 1** Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.
- Step 2** Click the **Firewall and ACL** icon in the left vertical navigation bar.
- Step 3** Click the **Basic Firewall** radio button on the Create Firewall tab.
- Step 4** Click **Launch the selected task** to proceed to the next window.

A new window opens describing the objective of the Basic Firewall Configuration wizard. Click **Next**.

Basic Firewall Interface Configuration

Next, the Basic Firewall Interface Configuration window appears.



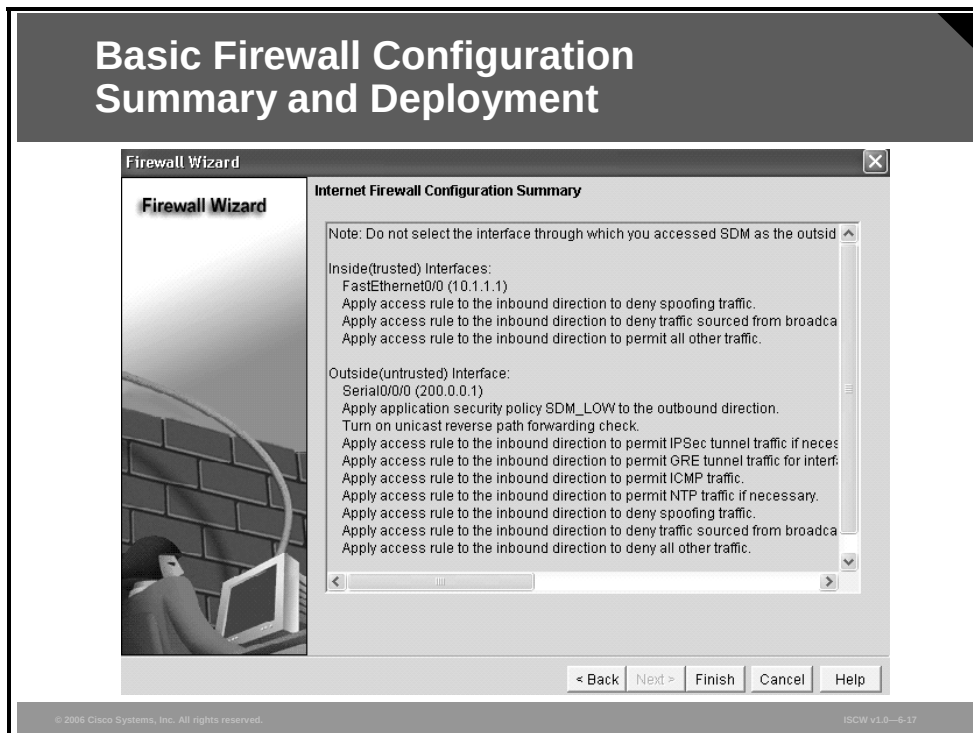
In this window, identify the outside interface by selecting it from the **Outside(untrusted) Interface** drop-down list, and the inside router interfaces by checking their check boxes in the **Inside(trusted) Interfaces** section. You may select several inside interfaces. In the example, the interface FastEthernet0/1 will not be affected because it is not selected.

At this stage, you can check the **Allow secure SDM access from outside interfaces** check box. When selected, HTTPS access to the outside router interfaces will be permitted from the untrusted domain. HTTP access will be denied. In this example, HTTPS access from outside is not desired.

Click **Next** to proceed to the next window. You will receive a warning that you will not be able to launch the SDM via the outside interface—in this case Serial0/0. Make sure that you are not accessing the SDM through the outside interface, and click **OK** to proceed to the next task.

Basic Firewall Configuration Summary and Deployment

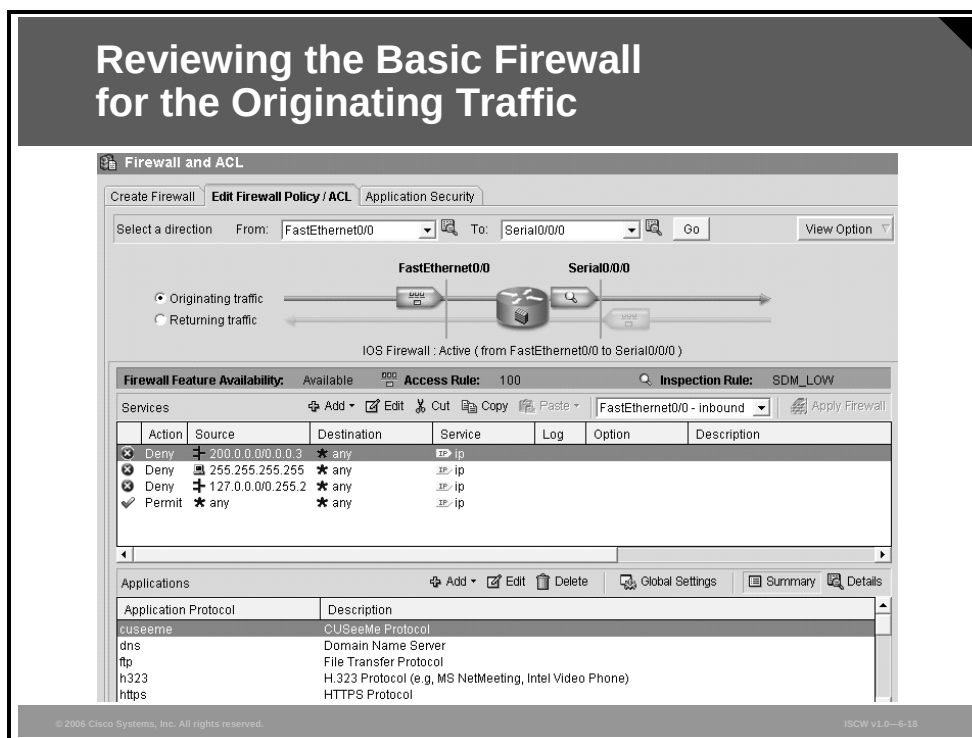
The final step of the wizard is the Internet Firewall Configuration Summary.



After clicking **OK**, you will get a summary of protection rules to be applied to the router. Review this report, and if all of the rules are listed, click **Finish** and then **OK** to send the commands to the device.

Reviewing the Basic Firewall for the Originating Traffic

Next, you can verify and customize the firewall settings. The figure illustrates the policy for outbound traffic.



When the firewall features are configured on the router, the wizard finishes and you are placed in the Edit Firewall Policy / ACL tab of the Firewall and ACL menu. In this window, you can review and modify the configured options. The figure illustrates how to view the ACL entries applied for the originating traffic (ACL 100 in this example); in other words, you examine the ACL that is applied to the inside interface in inbound direction.

ACL 100 will be applied inbound to the inside interface. It prevents spoofing by denying packets sourced from 200.0.0.0/30 network, which is configured on the outside interface. The ACL also blocks packets sourced from the broadcast address and the 127.0.0.0/8 network and permits all other traffic.

The inspection rule name in this example is SDM_LOW

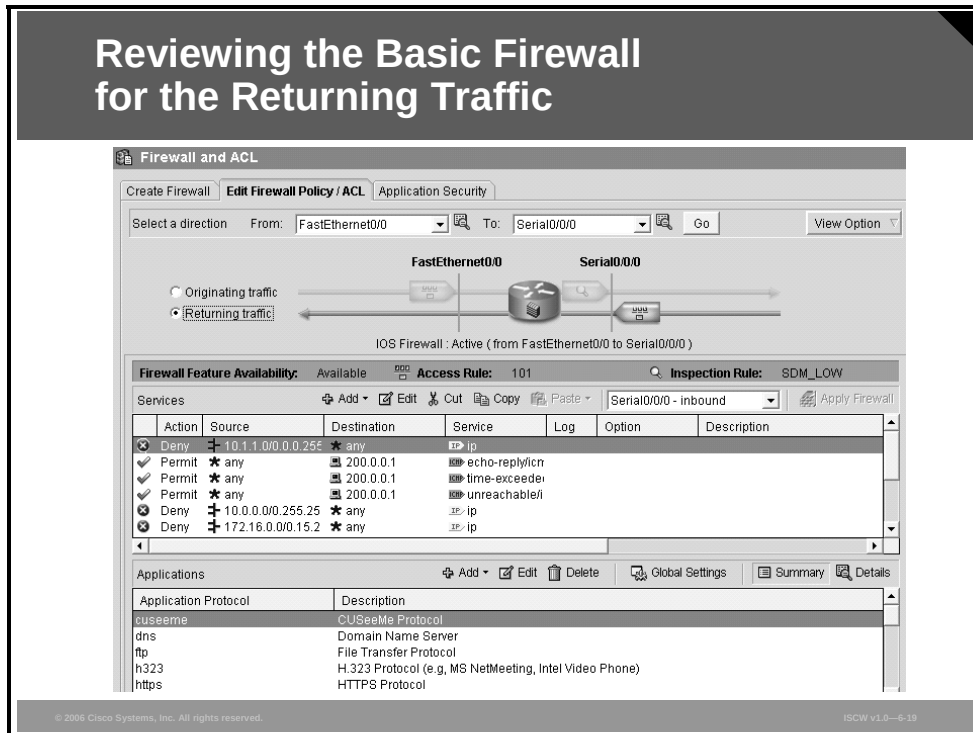
In this example, the firewall is active from the Fa0/0 to S0/0/0 direction, where Fa0/0 is in the inside (trusted) interface and S0/0/0 is the outside (untrusted) interface. You can also verify that the firewall is active by the firewall icon displayed inside the router icon.

If you select the **View Option > Swap From and To** interface, you will see that the firewall is inactive from the S0/0/0 to Fa0/0 direction.

To view the ACL applied for the returning traffic, click the Returning traffic radio button.

Reviewing the Basic Firewall for the Returning Traffic

The figure illustrates the firewall policy for inbound traffic.

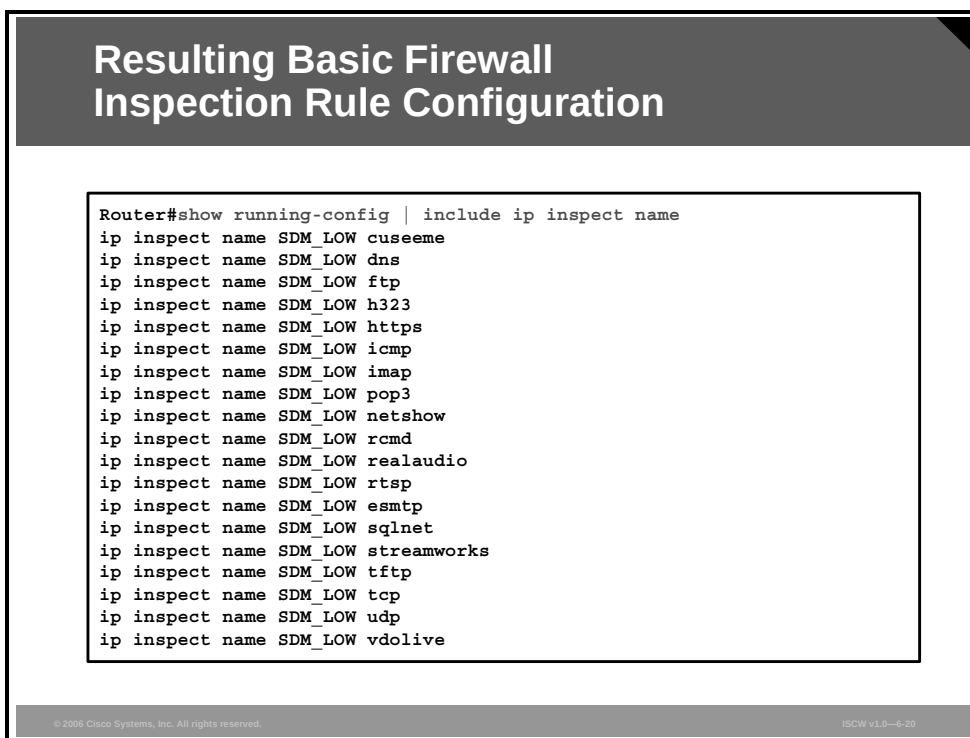


You can review the filter rules for returning traffic in a similar way as the rules for the originating traffic. This window displays all ACL entries that have been applied to the outside interface in inbound direction (ACL 101).

ACL 101 will be applied in inbound direction to the outside interface. The ACL permits ICMP echo-reply, time-exceeded, and unreachable messages destined to the outside router interface (200.0.0.1), and blocks packets sourced from private address ranges, the broadcast, and the 0.0.0.0 address. The final entry denies and logs all other packets.

Resulting Basic Firewall Inspection Rule Configuration

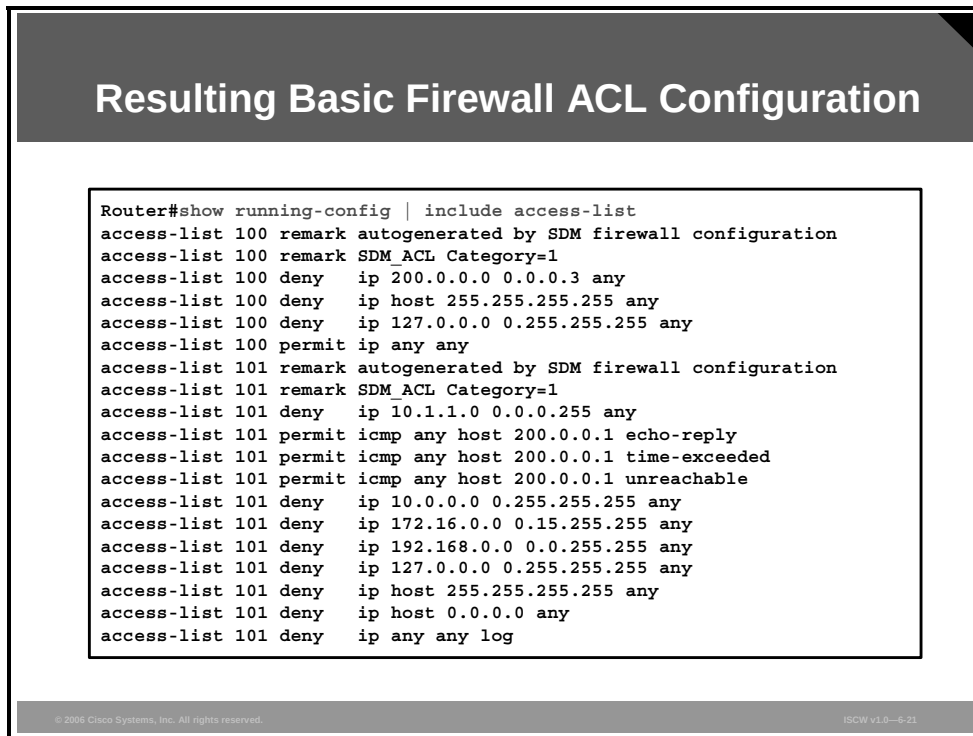
Another verification method is to check the commands that have been applied to the router using the CLI. This configuration has been generated by the SDM in previous pages.



This figure illustrates the inspection rule configuration that is applied to the router. The SDM_LOW predefined rule inspects all protocols commonly used in enterprise networks. This group includes: cuseeme, dns, ftp, h323, https, icmp, imap, pop3, netshow, rcmd, realaudio, rtsp, esmtp, sqlnet, streamworks, tftp, tcp, udp, and vdolive. The tcp, udp, and icmp offer generic inspection, while the remaining protocols require enhanced application awareness.

Resulting Basic Firewall ACL Configuration

This figure includes two ACLs that have been generated by the Basic Firewall Configuration wizard and will be applied to the router interfaces.



The resulting ACLs filter the traffic in this way:

- ACL 100 will be applied inbound to the inside interface. It prevents spoofing by denying packets sourced from 200.0.0.0/30 network, which is configured on the outside interface. The ACL also blocks packets sourced from the broadcast address and the 127.0.0.0/8 network and permits all other traffic.
- ACL 101 will be applied in inbound direction to the outside interface. The ACL permits ICMP echo-reply, time-exceeded, and unreachable messages destined to the outside router interface (200.0.0.1), and blocks packets sourced from private address ranges, the broadcast, and the 0.0.0.0 address. The final entry denies and logs all other packets.

Resulting Basic Firewall Interface Configuration

Finally, the Basic Firewall Configuration wizard applies the configured ACLs and inspection rules to the router interfaces.

Resulting Basic Firewall Interface Configuration

```
Router#show running-config | begin interface
interface FastEthernet0/0
  description $FW_INSIDE$
  ip address 10.1.1.1 255.255.255.0
  ip access-group 100 in
  !
interface Serial0/0/0
  description $FW_OUTSIDE$
  ip address 200.0.0.1 255.255.255.252
  ip access-group 101 in
  ip verify unicast reverse-path
  ip inspect SDM_LOW out
  !
<...rest of output removed...>
```

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-22

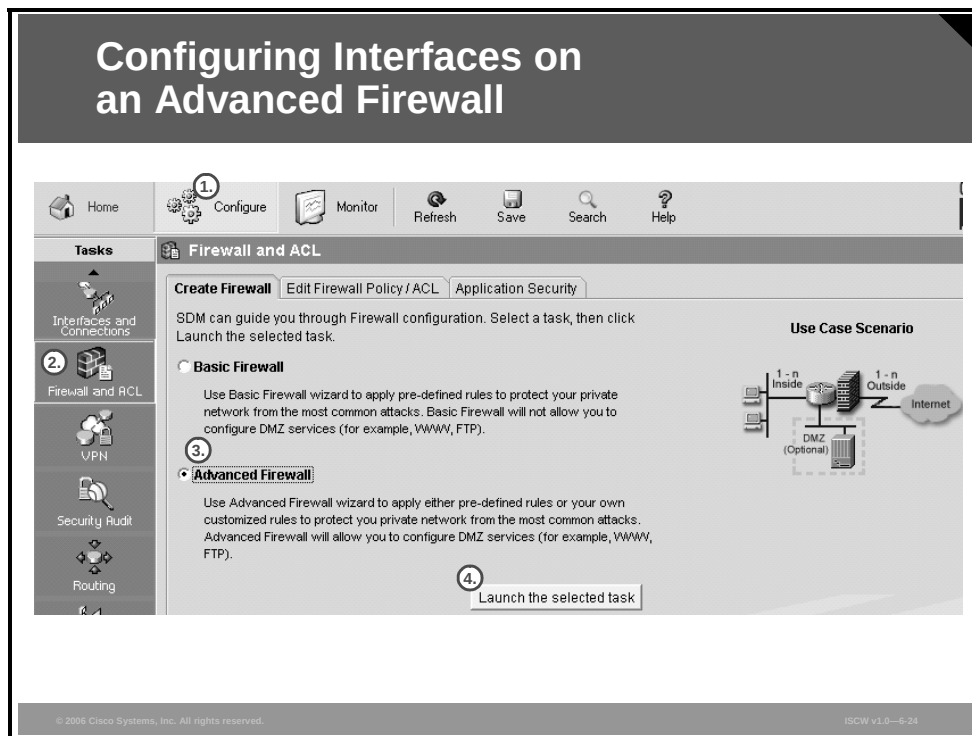
Note SDM applies the inspection rule to the outside interface in outbound direction although it was previously stated that applying inspection rules in inbound direction provides the most clarity. That recommendation is especially valid in environments with many interfaces and multiple flows. The SDM Basic and Advanced Firewall wizards operate in relatively simple environments, so that recommendation is not followed.

In addition to the ACLs and inspection rules applied to the respective interfaces, unicast reverse path forwarding is enabled on the outside interface.

Note In an Internet environment, the functionality of the unicast reverse path forwarding depends on the existence of a default route (0.0.0.0 0.0.0.0). If there is no default route, and a packet comes in from an unmatched IP address, it will be dropped by the unicast reverse path forwarding feature.

Configuring Interfaces on an Advanced Firewall

This topic describes how to configure the interfaces on an advanced firewall.



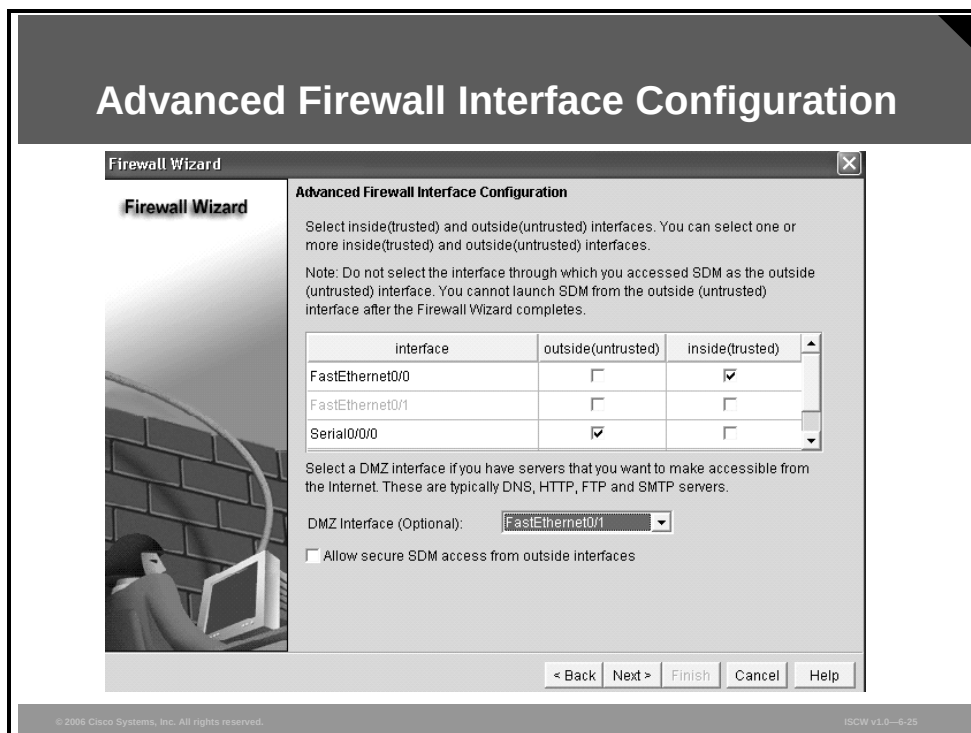
To launch the Advanced Firewall Configuration wizard follow this procedure:

- Step 1** Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.
- Step 2** Click the **Firewall and ACL** icon in the left vertical navigation bar.
- Step 3** Click the **Advanced Firewall** radio button on the Create Firewall tab.
- Step 4** Click **Launch the selected task** to proceed to the next window.

A new window opens describing the objective of the Advanced Firewall Configuration wizard. Click **Next**.

Advanced Firewall Interface Configuration

Next, the Advanced Firewall Interface Configuration window appears.

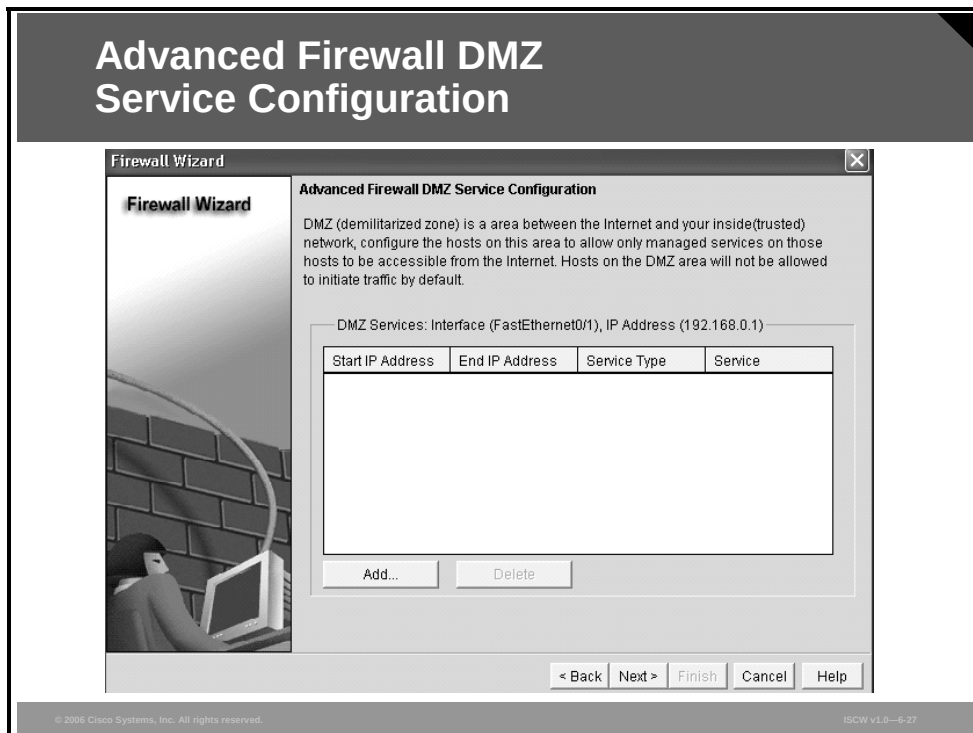


In this window, identify the outside (untrusted) and the inside (trusted) interfaces by checking their check boxes in the appropriate column, and the DMZ interface by choosing it from the **DMZ Interface (Optional)** drop-down list. In addition, you can check the **Allow secure SDM access from outside interfaces** check box. This allows HTTPS connectivity from the untrusted domain. HTTP will be denied from outside.

Click **Next** to proceed to the next window. You will receive a warning that you will not be able to launch the SDM via the outside interface—in this case Serial0/0/0.

Configuring a DMZ on an Advanced Firewall

This topic explains how to configure a DMZ on an advanced firewall.

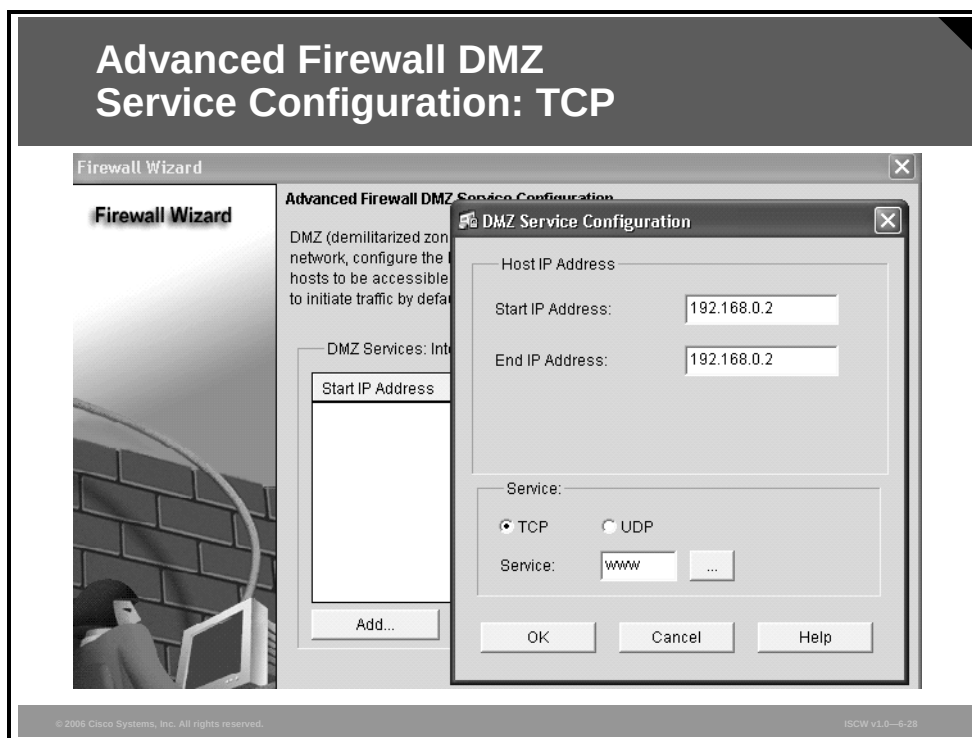


Next, the Advanced Firewall DMZ Service Configuration window appears.

In the window, you can define DMZ services that should be accessible from the outside world. Typically, here you would include information about public web, mail, and FTP, as well as VPN site-to-site and remote access devices. Click the **Add** button to define a DMZ service.

Advanced Firewall DMZ Service Configuration: TCP

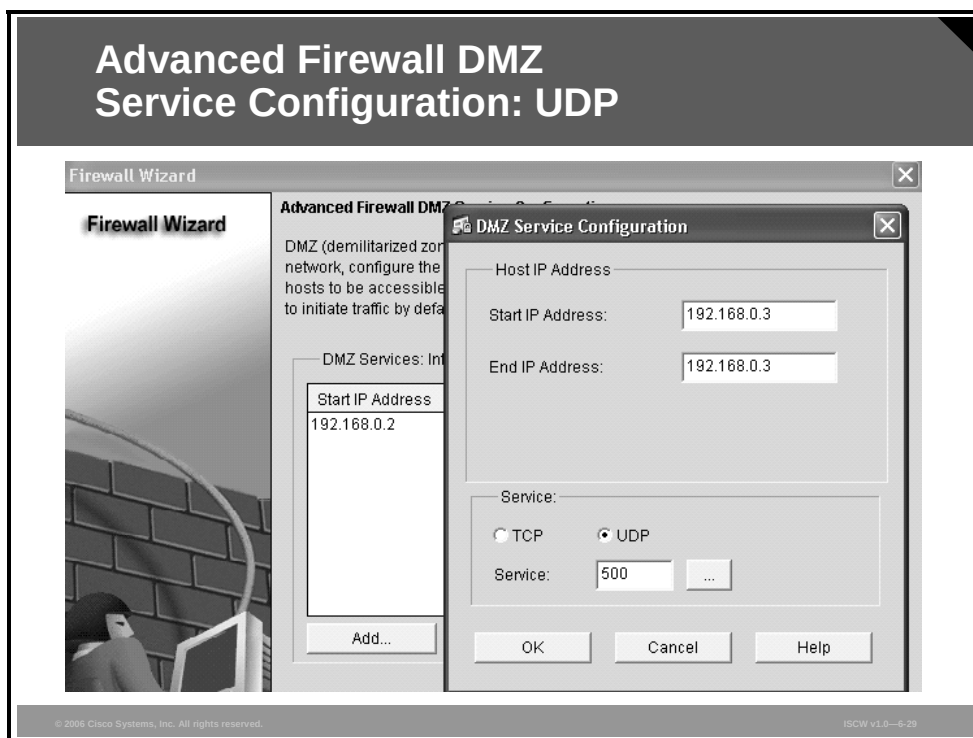
Next, you optionally specify which TCP services are hosted on servers attached to the DMZ interface.



When you click the **Add** button in the Advanced Firewall DMZ Service Configuration page, the DMZ Service Configuration window appears. You must provide the server addresses and select the DMZ services either by clicking the list of well-known services or by manually specifying the port number. In this figure, an access to the web server running on server 192.168.0.2 port TCP/80 (identified as www service) is permitted.

Advanced Firewall DMZ Service Configuration: UDP

Next, you optionally specify which UDP services are hosted on servers attached to the DMZ interface.



In this figure, Internet Security Association and Key Management Protocol (ISAKMP) connectivity (UDP port 500) to the VPN server using the address 192.168.0.3 is permitted.

Note ISAKMP is the VPN protocol that negotiates parameters that will be used to encrypt and authenticate data when the IPsec VPN tunnel is established. The data traversing the tunnel will be encrypted using Encapsulation Security Payload (ESP) protocol within the IPsec. Because ESP is not session-oriented, return ESP traffic cannot be dynamically permitted by the firewall engine. In such a scenario, you would have to explicitly permit inbound ESP traffic in the customization phase.

Advanced Firewall DMZ Service Configuration (Cont.)

Firewall Wizard

Advanced Firewall DMZ Service Configuration

DMZ (demilitarized zone) is a area between the Internet and your inside(trusted) network, configure the hosts on this area to allow only managed services on those hosts to be accessible from the Internet. Hosts on the DMZ area will not be allowed to initiate traffic by default.

DMZ Services: Interface (FastEthernet0/1), IP Address (192.168.0.1)

Start IP Address	End IP Address	Service Type	Service
192.168.0.2	192.168.0.2	tcp	www
192.168.0.3	192.168.0.3	udp	500

Add... Delete

< Back Next > Finish Cancel Help

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-30

After including all TCP and UDP services running on hosts attached to the DMZ interface in the Advanced Firewall DMZ Service Configuration window, click the **Next** button to proceed to the next task.

Advanced Firewall Security Configuration

This topic explains how to configure inspection rules.



After completing the DMZ service configuration, and clicking **Next**, the Advanced Firewall Security Configuration window appears. Here you can define the inspection granularity for services that run in the DMZ.

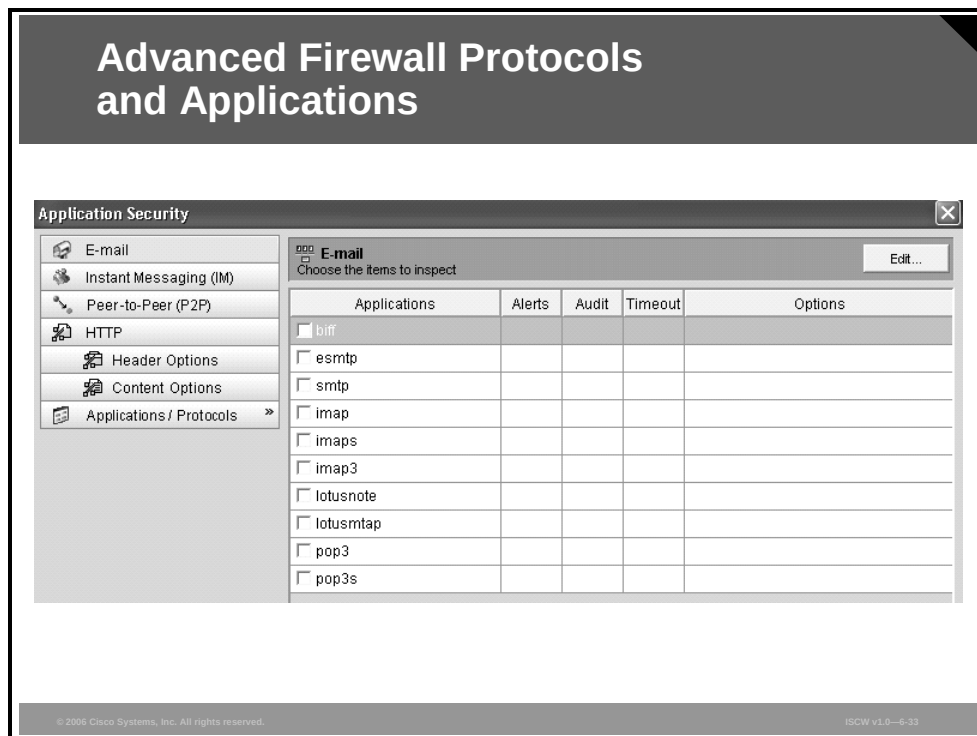
You have the option of choosing the default SDM application security policy by selecting the **Use a default SDM Application Security Policy** and modifying its security level, or using a custom policy.

You may preview the commands that constitute the SDM default policy by clicking the **Preview Commands** button.

If you want to use a custom policy, you must either create a new policy or select an existing one. In this example, no custom policies exist, so you need to create a custom policy by selecting the **Create a new policy** option.

Advanced Firewall Protocols and Applications

When defining a custom application security policy, you can select applications that should be inspected by the firewall.

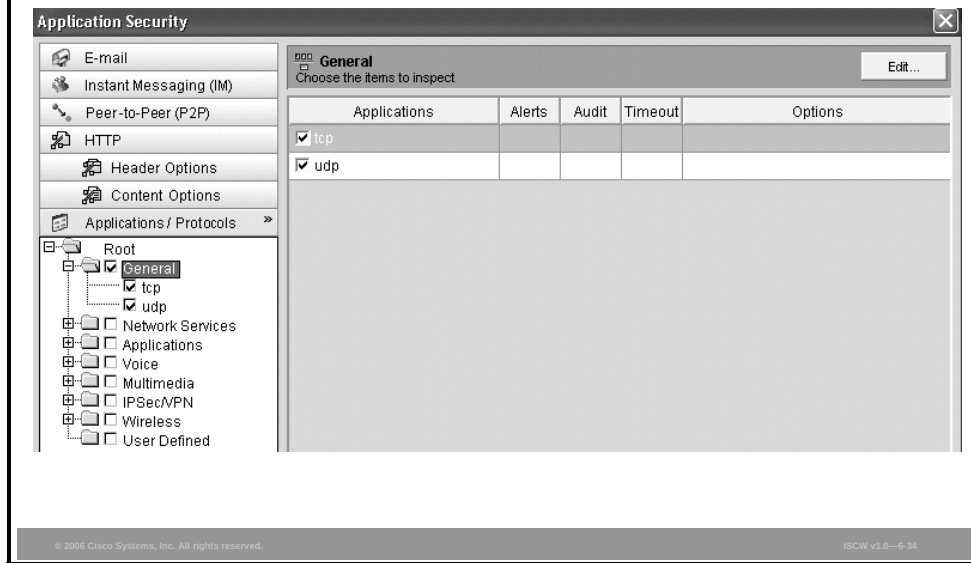


The applications are grouped into categories listed on the left side of the Application Security window:

- E-mail
- Instant Messaging (IM)
- Peer-to-Peer (P2P)
- HTTP
- Applications / Protocols, which includes the subcategories General, Network Services, Applications, Voice, Multimedia, IPsec/VPN, Wireless, and User Defined.

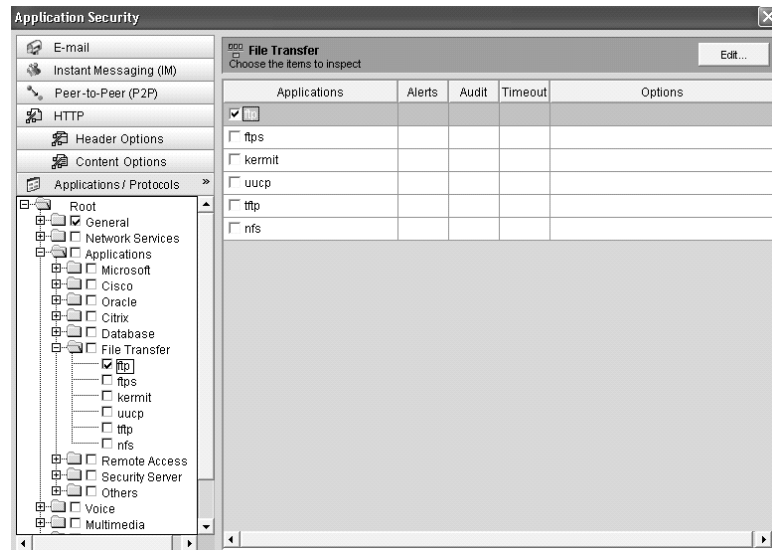
You can browse through the menu, and select the protocols and applications that should be inspected by the firewall.

Advanced Firewall Protocols and Applications (Cont.)



In this example, you enable generic inspection for TCP and UDP protocols only. This inspection will be applied in inbound direction to the inside interface.

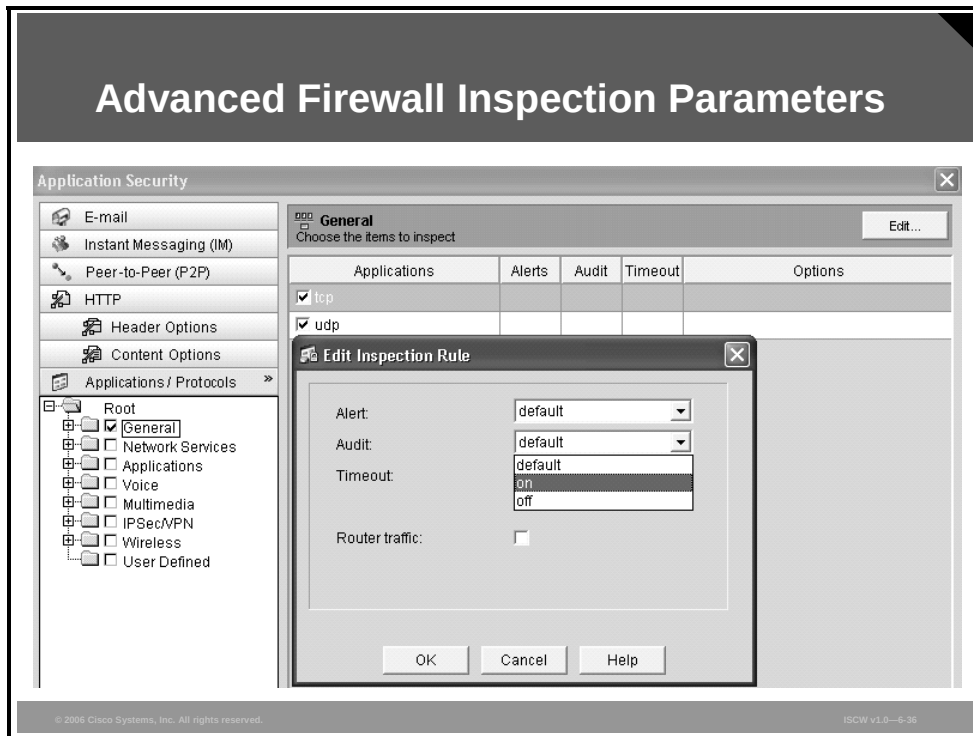
Advanced Firewall Protocols and Applications (Cont.)



In addition to the generic TCP and UDP inspection, you want to activate the inspection for FTP. This inspection will be applied in the inbound direction to the inside interface.

Advanced Firewall Inspection Parameters

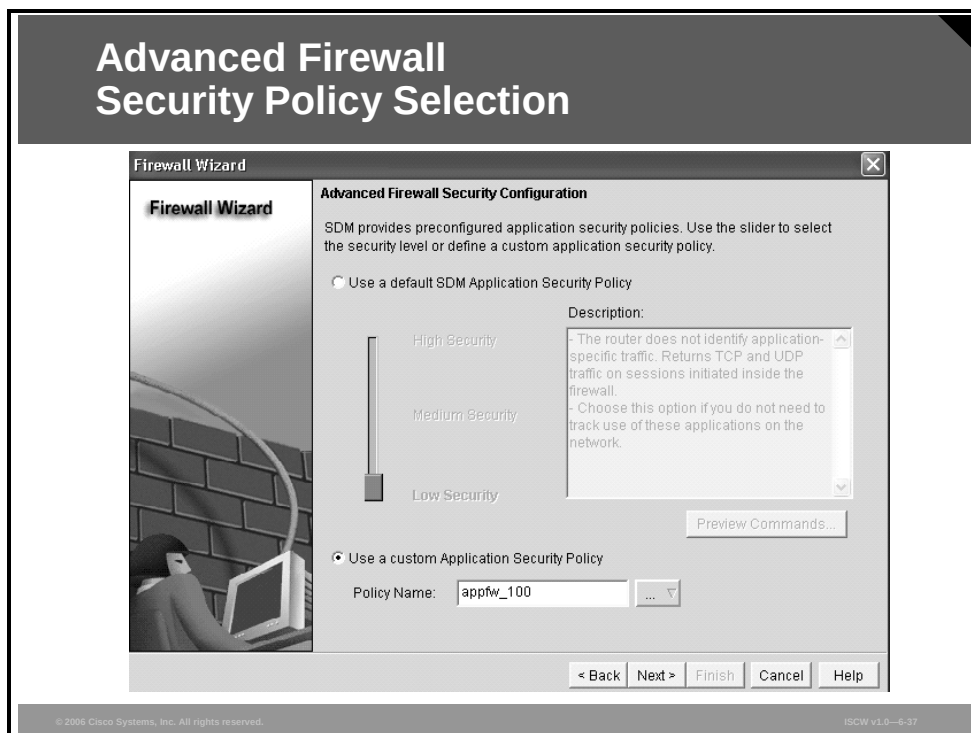
You can modify the inspection parameters by clicking the **Edit** button in the upper-right corner of the window.



The parameters that can be modified are alerts, audit, and timeout, and also whether local router traffic should be inspected. You can set those parameters for each inspected protocol. In this example, you want to keep most parameters unchanged and enable audit trail for TCP inspection. Audit trail is disabled by default. Click **OK** twice to return to the main wizard thread.

Advanced Firewall Security Policy Selection

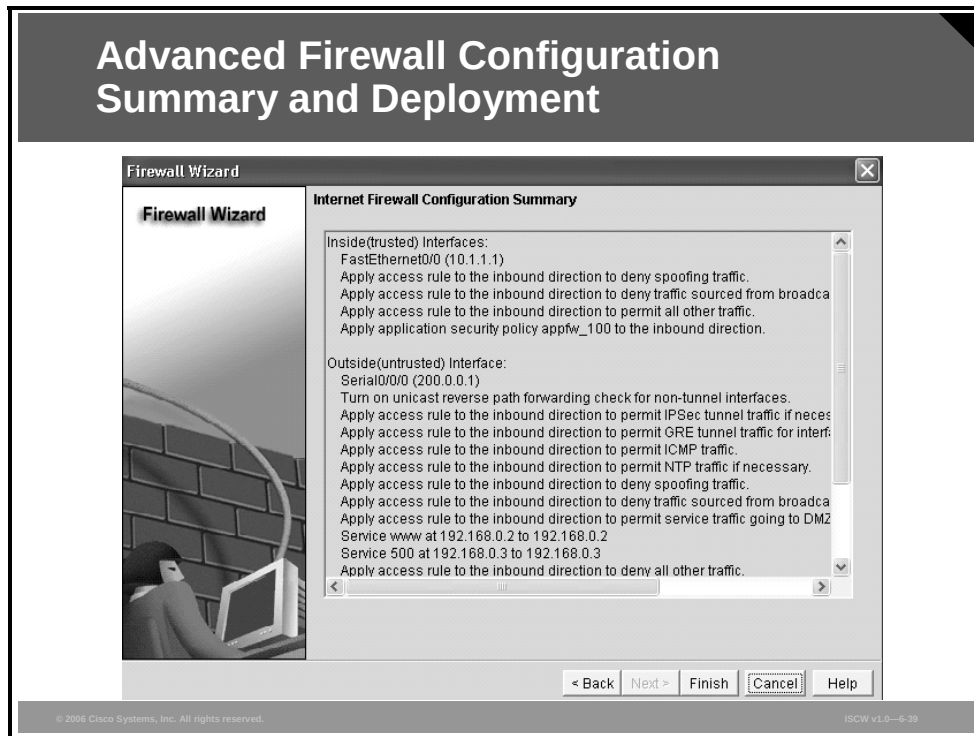
Next, you need to select the security policy to be deployed to the router.



You can verify that your custom policy will be deployed by clicking the **Use a custom Application Security Policy** radio button and choosing the policy from the **Policy Name** drop-down list. If you configured several policies, you would need to select which one to deliver to the router. Click **Next** to proceed.

Complete the Configuration

This topic describes how to complete the Advanced Firewall Configuration wizard by viewing the settings in the Summary window.



After selecting the application security policy in the Advanced Firewall Security Configuration window, and clicking **Next**, the Internet Firewall Configuration Summary window appears. The window lists all firewall rules that will be applied to the router interfaces. Click **Finish** to apply the configuration to the router.

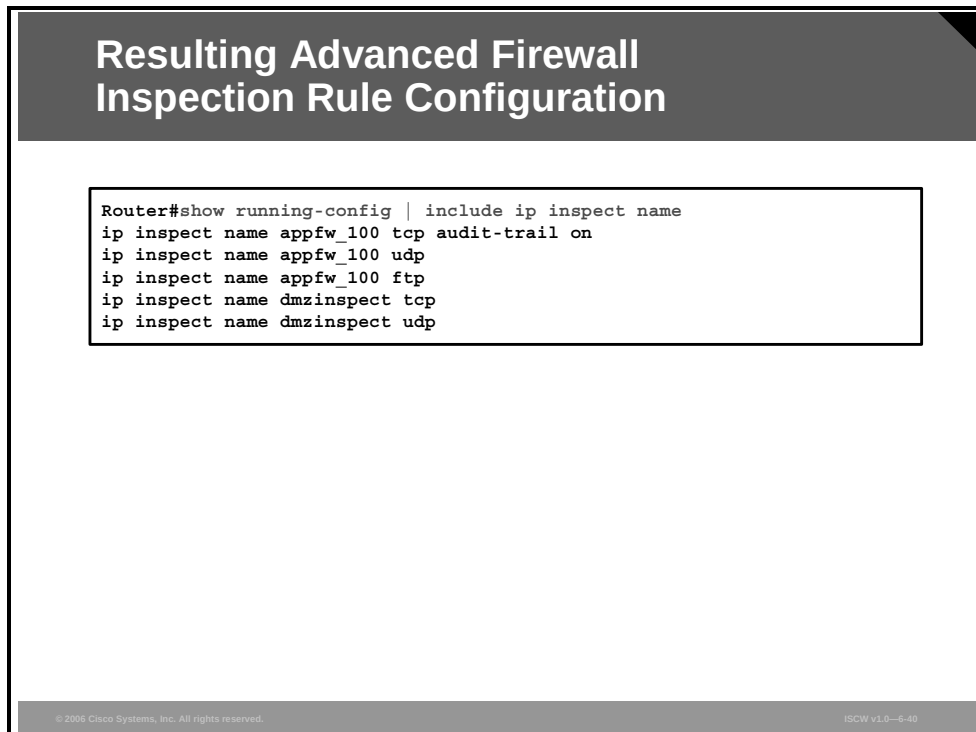
The wizard finishes and you are placed in the Edit Firewall Policy / ACL tab of the Firewall and ACL menu. In this window, you can review and modify the configured options.

Such fine-tuning will be necessary in situations when non-TCP and non-UDP traffic, such as ESP, must be permitted in inbound direction, or when separate inspection rules should be applied to different interfaces.

Note If the SDM detects NAT or IPsec VPN configurations on the router already, it will automatically adjust the ACLs so that NAT or IPsec VPN operations will not be affected.

Resulting Advanced Firewall Inspection Rule Configuration

Finally, you can verify the router configuration using the CLI.



This figure illustrates the inspection rules configuration that is applied to the router. First, you see the custom inspection rule `appfw_100` that you created using the wizard. It will be applied to the inside interface in inbound direction (for inspecting the outbound traffic from the inside to outside). This rule includes generic TCP and UDP, as well as FTP inspection and enabled audit trail for TCP traffic. The rule `dmzinspect` will be applied to the DMZ interface in outbound direction (for inspecting traffic from the outside to the DMZ services) and checks generic TCP and UDP.

Resulting Advanced Firewall ACL Configuration

The following ACLs are sent to the router as a result of the wizard.

Resulting Advanced Firewall ACL Configuration

```
Router#show running-config | include access-list
access-list 100 remark autogenerated by SDM firewall configuration
access-list 100 remark SDM_ACL Category=1
access-list 100 deny ip 200.0.0.0 0.0.0.3 any
access-list 100 deny ip 192.168.0.0 0.0.0.255 any
access-list 100 deny ip host 255.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
access-list 101 remark autogenerated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 deny ip any any log
access-list 102 remark autogenerated by SDM firewall configuration
access-list 102 remark SDM_ACL Category=1
access-list 102 deny ip 192.168.0.0 0.0.0.255 any
access-list 102 deny ip 10.1.1.0 0.0.0.255 any
access-list 102 permit icmp any host 200.0.0.1 echo-reply
access-list 102 permit icmp any host 200.0.0.1 time-exceeded
access-list 102 permit icmp any host 200.0.0.1 unreachable
access-list 102 permit tcp any host 192.168.0.2 eq www
access-list 102 permit udp any host 192.168.0.3 eq isakmp
access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 172.16.0.0 0.15.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
access-list 102 deny ip host 255.255.255.255 any
access-list 102 deny ip host 0.0.0.0 any
access-list 102 deny ip any any log
```

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--6-41

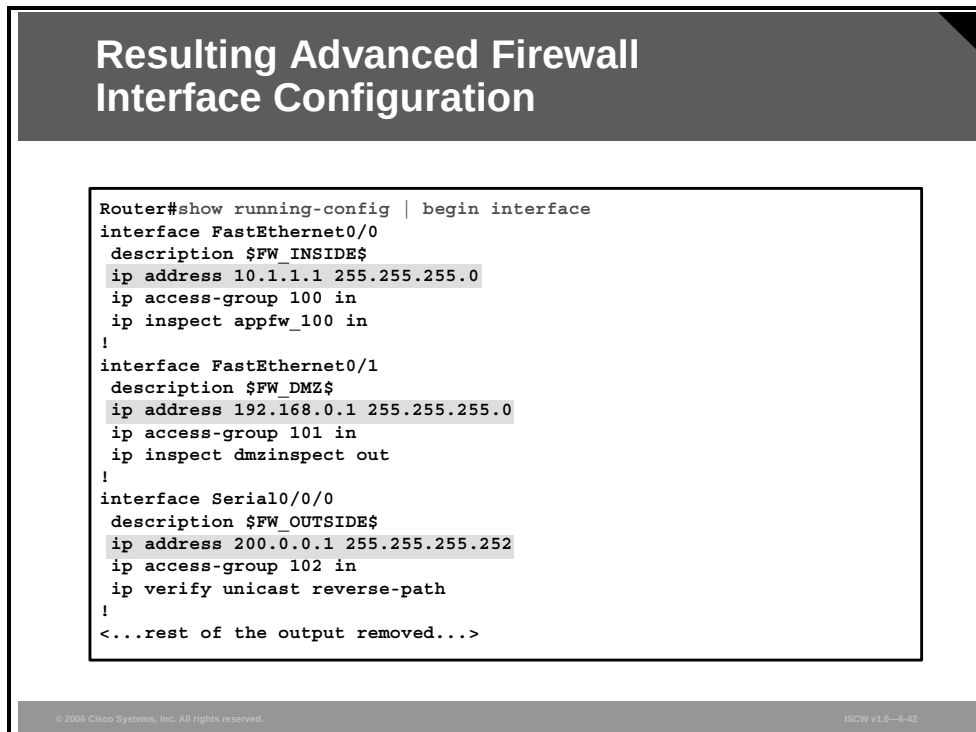
This configuration includes three ACLs that will be applied to the router interfaces:

- ACL 100 will be applied in inbound direction to the inside interface. The ACL prevents spoofing by denying packets sourced from 200.0.0.0/30 and 192.168.0.0/24 networks, which are configured on the outside and DMZ interfaces, respectively. The ACL also blocks packets sourced from the broadcast address and the 127.0.0.0/8 network and permits all other traffic.
- ACL 101 will be applied in inbound direction to the DMZ interface. This ACL blocks and logs all packets.
- ACL 102 will be applied in inbound direction to the outside interface. The ACL prevents spoofing by denying packets sourced from 192.168.0.0/24 and 10.1.1.0/24 networks, which are configured on the DMZ and inside interfaces, respectively. The ACL permits ICMP echo-reply, time-exceeded, and unreachable messages destined to the outside router interface (200.0.0.1). It also permits packets destined to the DMZ servers—HTTP traffic to host 192.168.0.2 and ISAKMP data to host 192.168.0.3. Next, the ACL blocks packets sourced from private address ranges, the broadcast, and the 0.0.0.0 address. The final entry denies and logs all other packets.

Note The Advanced Firewall wizard was used to permit HTTP (TCP/80) to the web server (192.168.0.2) and ISAKMP (UDP/500) to the VPN server (192.168.0.3) residing in the DMZ. The VPN server will communicate with its peers using both ISAKMP and ESP (IP/50). Because ESP is stateless, the Advanced Firewall wizard did not allow ESP-based access to the VPN server. In a real-life scenario, you will have to modify the ACL applied to the outside interface (102) to permit ESP data to the VPN server.

Resulting Advanced Firewall Interface Configuration

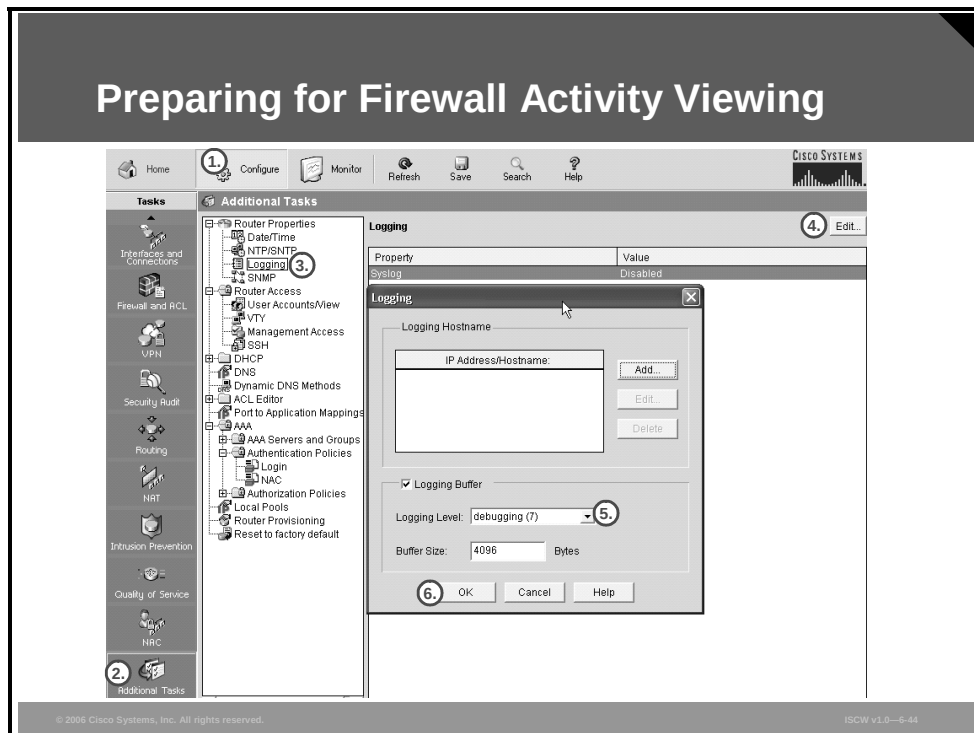
This figure describes the resulting interface configuration options.



Finally, the Advanced Firewall Configuration wizard applies the configured ACLs and inspection rules to the router interfaces. Additionally, unicast reverse path forwarding is enabled on the outside interface.

Viewing Firewall Activity

This topic explains how to use the SDM logging function to monitor firewall activity.



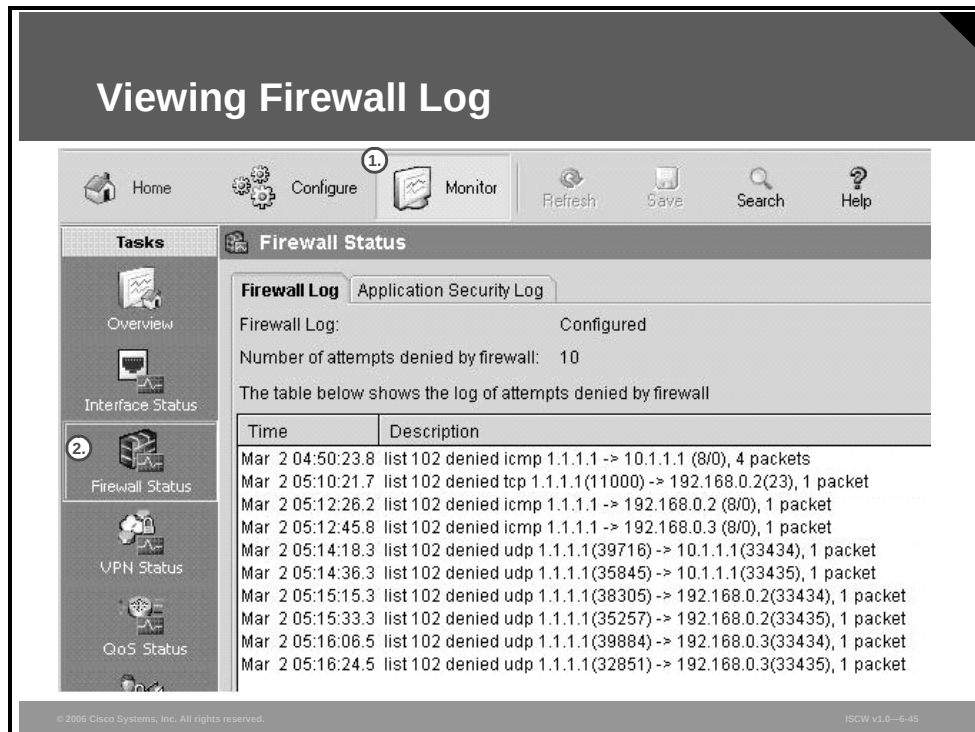
To be able to view the firewall activity, you must enable logging:

- Step 1** Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.
- Step 2** Click the **Additional Tasks** icon in the left vertical navigation bar.
- Step 3** Select the **Router Properties > Logging** item in the middle section of the window.
- Step 4** Click the **Edit** button in the upper-right corner of the window to modify the logging settings.
- Step 5** Select the **debugging (7)** option from the Logging Level drop-down list.
- Step 6** Click **OK**.

Note Logging is not activated by default.

Viewing Firewall Log

This figure illustrates how to view the firewall log.



After activating firewall logging, you can view the firewall log:

Step 1 Click the **Monitor** icon in the top horizontal navigation bar to enter the configuration page.

Step 2 Click the **Firewall Status** icon in the left vertical navigation bar.

In the example, you see a number of packets that have been denied on the outside interface because they did not comply to the firewall policy created by the firewall wizard. A number of packets from an attacker using the address 1.1.1.1 have been dropped. The attacker attempted to send ICMP, TCP (Telnet), and UDP packets to some high ports, probably using a traceroute. The target systems were the two hosts in the DMZ: 192.168.0.2 and 192.168.0.3, and the inside interface address 10.1.1.1.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco IOS Firewall can be configured using the CLI or the SDM.
- Inspection rules must specify which protocols will be inspected by the firewall engine at an interface.
- Inspection rules can help protect hosts against certain DoS attacks involving fragmented IP packets.
- SDM offers configuration wizards to expedite the firewall configuration process.
- Basic Firewall Configuration wizard supports two interfaces and predefines filter rules.
- Advanced Firewall Configuration wizard supports three interfaces and customized filter rules.
- SDM offers monitoring capabilities to view the firewall activity.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6-46

References

For additional information, refer to these resources:

- *Cisco IOS IP Configuration Guide, Release 12.2 (also pertains to 12.3), Configuring IP Services* at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ae127.html
- *Configuring Context-Based Access Control* at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html

Introducing Cisco IOS IPS

Overview

This lesson describes the intrusion detection system (IDS) and intrusion prevention system (IPS) technologies, and discusses the differences between them. The lesson covers various approaches to IPS and IDS, such as signature-based, policy-based, anomaly-based, and honeypot, as well as the operational scope, which can be either network- or host-based. The lesson describes the common signature categories, such as exploit, connection, string, and denial of service (DoS), and explains the IPS components used on Cisco IOS routers: signature definition files (SDFs) and signature microengines (SMEs). Finally, the lesson describes actions that can be taken by an IPS or IDS system when a signature is triggered.

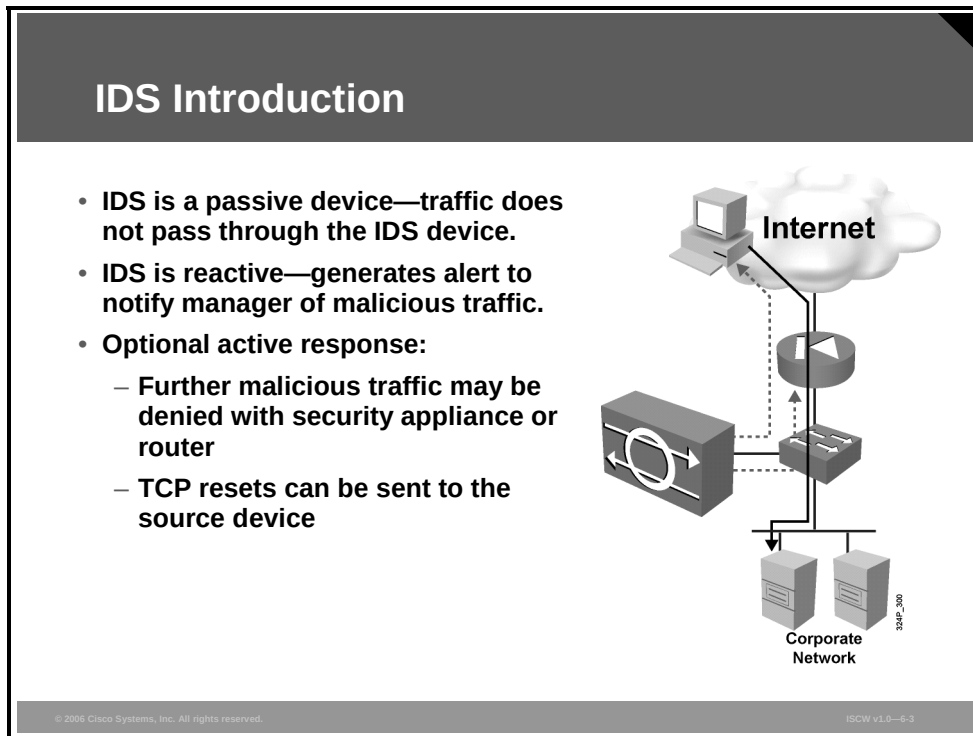
Objectives

Upon completing this lesson, you will be able to explain the features, components, and functionality of Cisco IOS IPS. This ability includes being able to meet these objectives:

- Describe the functions and operations of IDS and IPS systems, and the difference between IDS and IPS
- Describe the types of IDS and IPS systems
- Describe the four types of IDS and IPS signatures
- Describe what happens when a signature is matched

Introducing Cisco IOS IDS and IPS

This topic describes the functions and operations of IDS and IPS systems, and the difference between them.



Intrusion Detection System

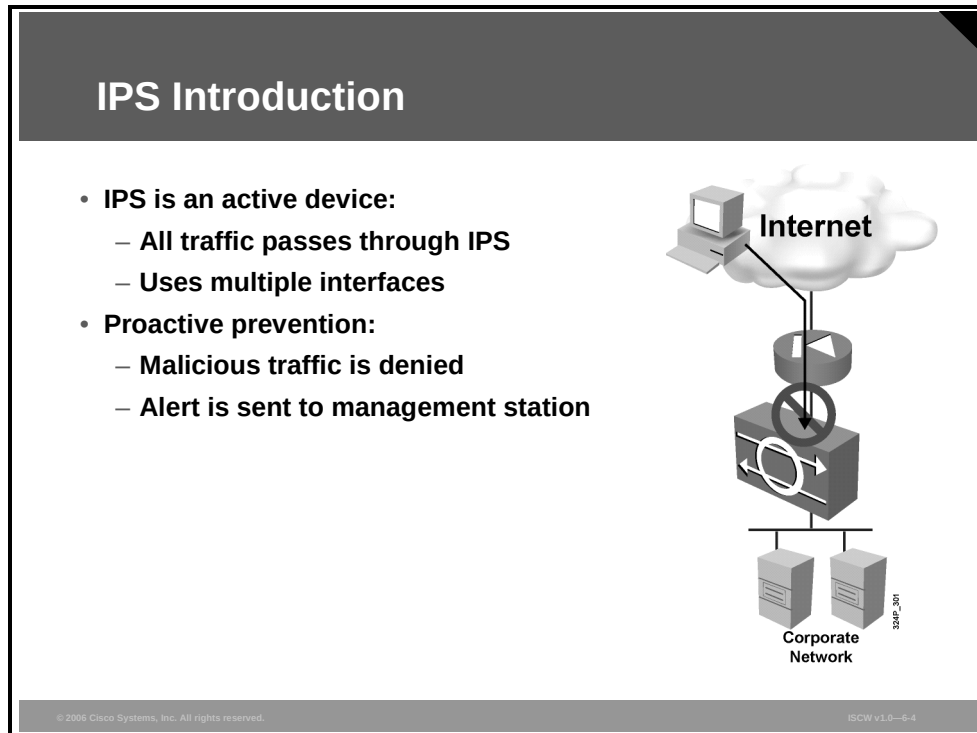
The IDS is a software- or hardware-based solution that passively listens to network traffic. The IDS is not in the traffic path, but listens promiscuously to all traffic on the network. Typically, only one promiscuous interface is required for network monitoring. Additional promiscuous interfaces can be used to monitor multiple networks.

When the IDS detects malicious traffic, it sends an alert to the management station.

The IDS has limited active response capabilities. When configured, the IDS can block further malicious traffic by actively configuring network devices (for example, security appliances or routers) in response to malicious traffic detection. However, the original malicious traffic has already passed through the network to its destination and cannot be blocked. Only subsequent traffic will be blocked. The IDS also has the capability of sending a TCP reset to the end host to terminate any malicious TCP connections.

Intrusion Protection System

IPSs are active devices in the traffic path, listening to network traffic and permitting or denying flows and packets into the network.



All traffic passes through an IPS for inspection. Traffic arrives on one IPS interface and exits on another.

When the IPS detects malicious traffic, it sends an alert to the management station and blocks the malicious traffic immediately. The original and subsequent malicious traffic is blocked as the IPS proactively prevents attacks.

Because network attack mechanisms are becoming more sophisticated, this proactive approach is required to protect against network viruses, worms, malicious applications, and vulnerability exploits.

Combining IDS and IPS

You should view IDS and IPS as complementary technologies that are often deployed in enterprise networks in parallel.

Combining IDS and IPS

- **IPS actively blocks offending traffic:**
 - Should not block legitimate data
 - Only stops “known malicious traffic”
 - Requires focused tuning to avoid connectivity disruption
- **IDS complements IPS:**
 - Verifies that IPS is still operational
 - Alerts about any suspicious data except “known good traffic”
 - Covers the “gray area” of possibly malicious traffic that IPS did not stop

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6-5

The IPS actively blocks offending traffic and can be considered another implementation of a firewall system. The IPS should be tuned to block only known malicious traffic in order to avoid connectivity disruptions. An IDS can verify that the IPS is really blocking offending traffic. In addition, the IDS can be configured to alert about the “gray area” traffic—data that is neither clearly malicious nor clearly legitimate. Such traffic should not be blocked by IPS because legitimate connectivity would be interrupted, but it may give a valuable insight into potential problems or attack techniques, if configured properly.

Types of IDS and IPS Systems

This topic describes the types of IDS and IPS systems.

Types of IDS and IPS Systems		
Criteria	Type	Description
Approach to identify malicious traffic	Signature-based	• Vendor provides a signature database. • Signatures should be customized.
	Policy-based	• Policy definition and description is created.
	Anomaly-based	• 'Normal' and 'abnormal' traffic is defined.
	Honeypot	• Sacrificial host is set up to lure the attacker.
Coverage scope	Network-based	• Network sensors scan traffic destined to many hosts.
	Host-based	• Host agent monitors all operations within an operating system.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-7

IDS and IPS solutions can be grouped into these general classifications:

1. The approach to identify offending traffic
2. The coverage scope

Differences in the approach to identify malicious traffic can be classified as follows:

- Signature-based
- Policy-based
- Anomaly-based
- Honeypot

The two possible coverage scopes are:

- Network-based
- Host-based

Signature-Based Approach

Signature-based pattern matching refers to searching for a fixed sequence of bytes in a single packet, or predefined content. As its name suggests, it is an approach that is fairly rigid but simple to employ. In most cases, the signature pattern is matched only if the suspect packet is associated with a particular service or, more precisely, destined to or from a particular port. This method lessens the amount of inspection done on every packet. However, it tends to make it more difficult for systems to deal with protocols that do not reside on well-defined ports, and, in particular, Trojan horses and their associated traffic, which can usually be moved at will.

Initially, there might be many alerts, but which are no threat for the network. After the system is tuned and adjusted to the specific network parameters, there will be fewer false alerts than with the policy-based approach.

Policy-Based Approach

The policy-based approach uses some type of algorithm on which to base alarm decisions. An example of this type of policy is a policy that would be used to detect a port sweep. This policy looks for the presence of a threshold number of unique ports being scanned on a particular machine. The policy may further restrict itself through the specification of the types of packets that it is interested in (for example, SYN packets). Additionally, there may be a requirement that all the probes must originate from a single source.

Policies of this type require some threshold manipulations to make them conform to the utilization patterns on the network they are monitoring. This type of policy may be used to look for very simple statistical events or complex relationships.

Anomaly-Based Approach

Anomaly-based signatures are typically engineered to look for network traffic that deviates from what is considered “normal.” The main issue regarding this methodology is the definition of “normal.” Some systems have hard-coded definitions of “normal” traffic patterns.

Other systems are designed to learn “normal” traffic behavior, but the challenge with these systems is to eliminate the possibility of improperly classifying abnormal behavior as normal. Consequently, while relatively easy to implement in small environments, the anomaly-based approach can be difficult to deploy in large networks.

Honeypot Approach

Honeypot systems provide a dummy server to attract attacks. The philosophy of the honeypot approach is to distract attacks away from the real network devices. The honeypot offers the possibility of analyzing incoming attacks and malicious traffic patterns in order to be prepared when this type of traffic hits the real network. When implementing honeypots, dedicate servers that can be sacrificed to be compromised, and never trust such systems, because they may have been compromised without you noticing it.

Host-Based IPS

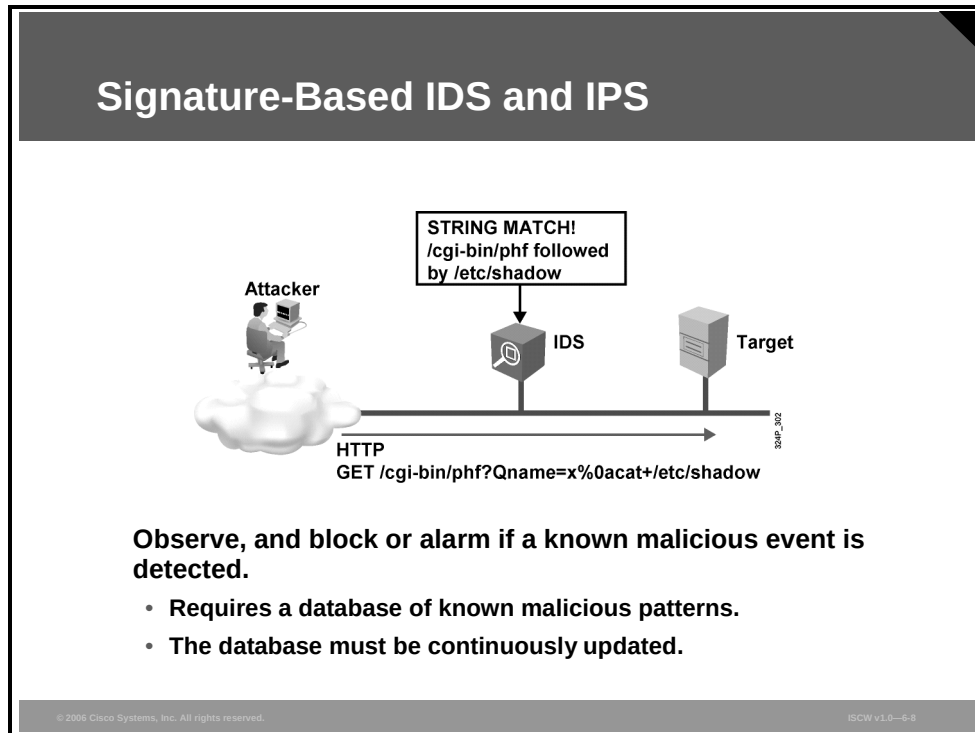
In a host-based system, a host-based intrusion prevention system (HIPS) examines the activity on each individual computer or host. The HIPS has full access to the internals of the end station, and can relate incoming traffic to the activity on the end station to understand the context. In VPN environments, where encrypted traffic flows through the network, the HIPS is the only option to examine traffic in plaintext. However, HIPS is typically written for a specific operating system and does not protect against lower level attacks, such as attacks targeting Layers 1 through 3 of the Open System Interconnection (OSI) model. Another disadvantage is that the attacker, after sufficient reconnaissance, can detect the host existence, and possibly even discover that the host is being protected by HIPS.

Network-Based IPS

In a network-based system, or network intrusion prevention system (NIPS), the individual packets flowing through a network are analyzed. NIPS can detect malicious packets that are overlooked by simplistic filtering rules of a firewall. NIPS is placed inside the network and allows verification of all network traffic, or at least of the critical areas in the network. NIPS can prevent lower-level attacks but cannot investigate encrypted traffic that passes through the sensor. NIPS sees attacks taken out of context, which can limit correlation capabilities and severity judgment.

Signature-Based IDS and IPS

To determine an attack signature, which is usually a well-known pattern of attack, IDS and IPS inspect packet headers or data payloads and match them against a signature database.



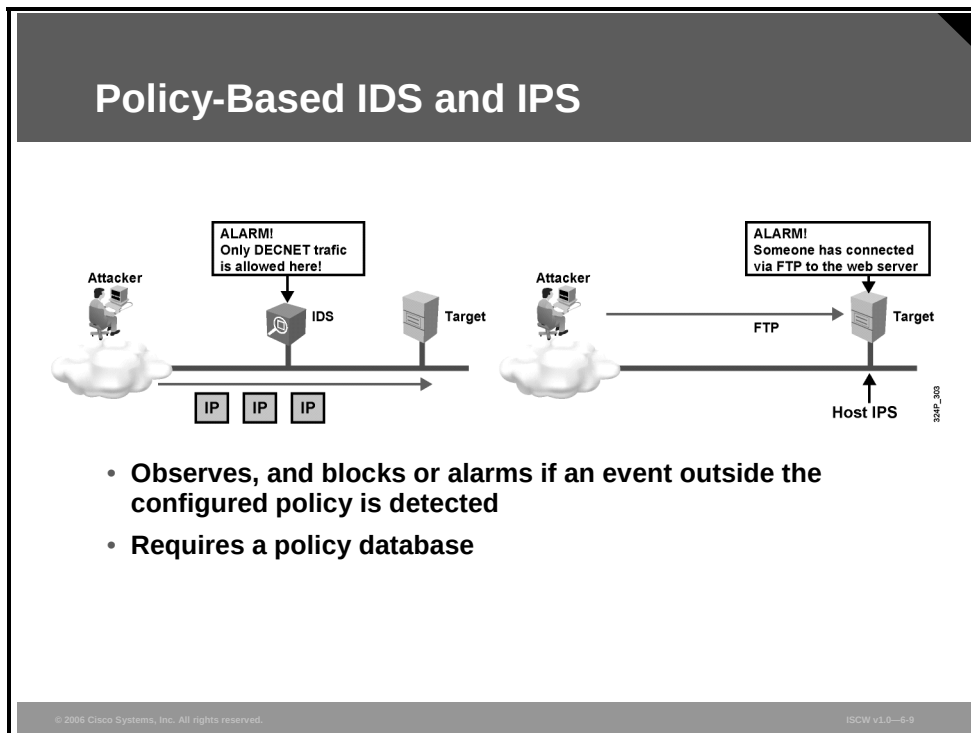
A signature is a sequence or a string of bytes in a certain context. The context may be the position of the sequence in the data flow, a part of a valid command in the application layer protocol, or a combination of options in the IP datagram. The following are some signature examples:

- Attacks against a web server are usually in the form of specially crafted URLs, so the IDS and IPS look for the signature at the start of the data flow, which begins with an HTTP request from the client.
- An attack against a Simple Mail Transfer Protocol (SMTP) server may be in the form of a buffer overflow in the **mail from** command of the SMTP session. IDS and IPS will look for an attack signature in the SMTP session that starts with the **mail from** command, and includes a particular pattern before the end of the line.
- An attack on the mail client may be in the form of a buffer overflow in the Multipurpose Internet Mail Extension (MIME) header of the message itself. IPS or IDS will look for the sequence of bytes that identifies the start of a new MIME part in the message, and a sequence of bytes that compose a buffer overflow following it.

These examples illustrate the fact that a signature-based IDS and IPS only detects attacks that have been entered into a database by the vendor or the administrator. Usually, IDS and IPS will be unable to detect undiscovered or unreported attacks (day zero attacks). Therefore, all signature-based IDSs and IPSs place a certain amount of burden on the administrators, as they must regularly update the signature database. Usually, the manufacturers publish database updates. If not, the administrator must create custom signatures that will cover these attacks.

Policy-Based IDS and IPS

Policy-based IDS and IPS block or alarm if a violation of a configured policy occurs.



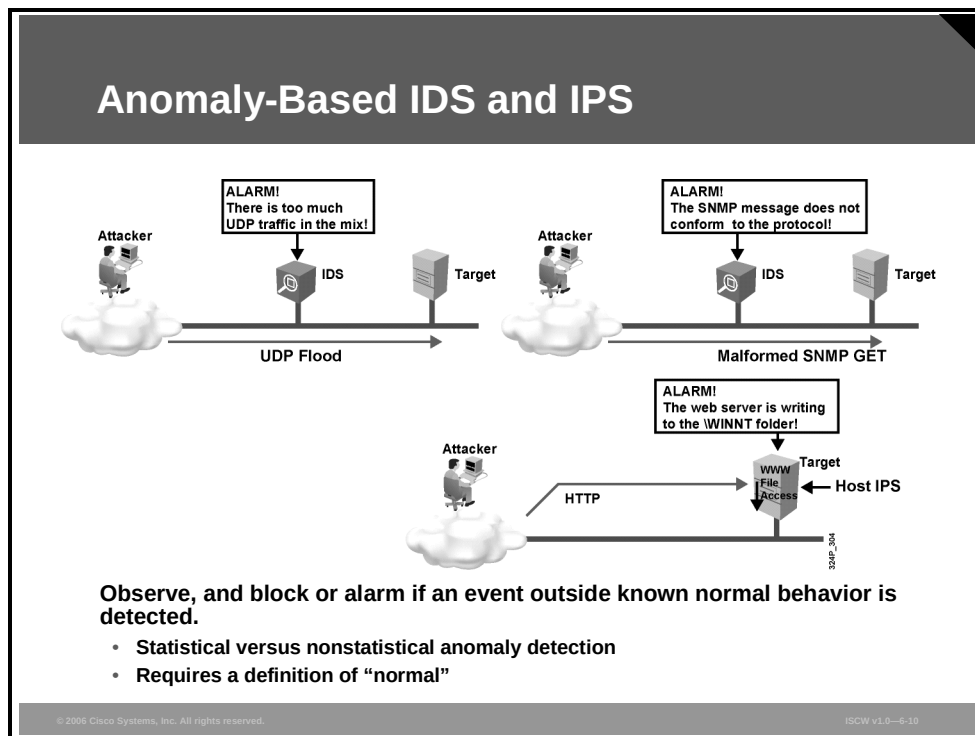
A policy-based system is a popular method of detection, especially if unknown attacks need to be detected.

Policy-based IDS and IPS have to have a clear representation of what the security policy is. For example, you can write a network access policy in terms of permissions—which networks can communicate with which other networks using which protocols.

Some security policies are hard to incorporate into IDS and IPS. For example, if browsing of pornographic, hacking, or “warez” (term referring to illegally copied, pirated software) sites is not allowed, the system must be able to communicate with some type of blacklist database to check if a policy violation has occurred.

Anomaly-Based IDS and IPS

Anomaly-based IDSs and IPSs monitor the network for events and content that represent an anomaly, or a departure from normal behavior.



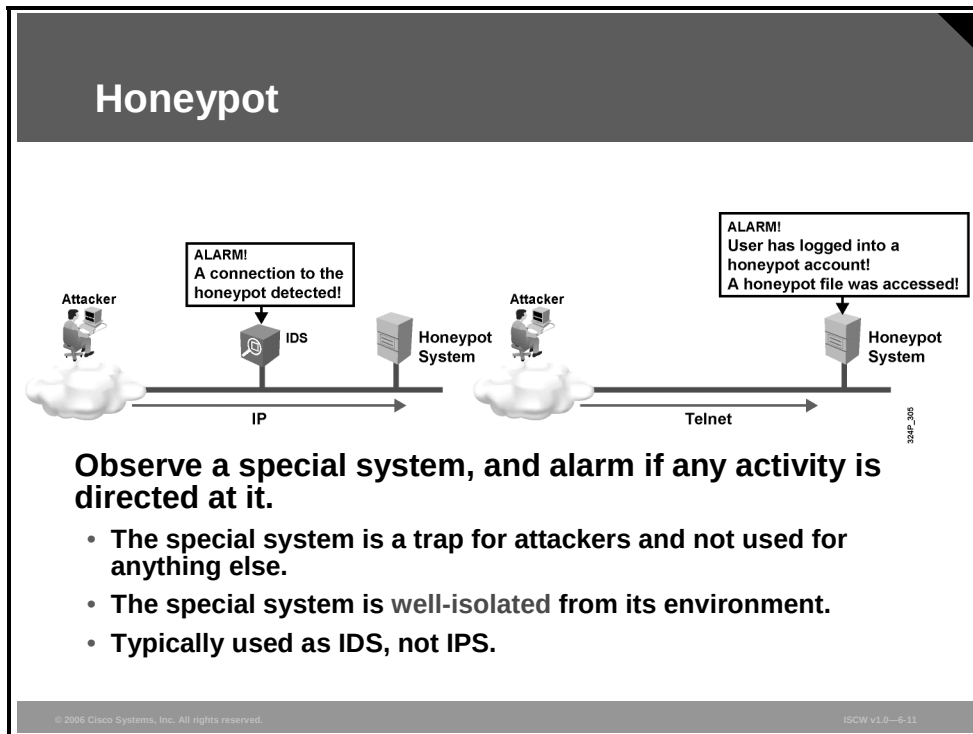
An anomaly may be an unusual increase in a certain type of traffic, an occurrence of some type of traffic not usually present on a monitored network, or a malformed message of a known protocol.

These are the two types of anomaly-based IDSs and IPSs:

- **Statistical anomaly detection:** This type of anomaly-based system approach learns about the profile of the monitored network (traffic patterns) from the network itself over a period of time. After that period, the system can detect if statistical properties of the network traffic deviate enough from the usual pattern, and if they do, the system triggers an alarm.
- **Nonstatistical approach:** This type of anomaly-based system has a predefined definition of a known good behavior, usually coded by the vendor, and triggers when an event outside such a profile occurs. These are examples of events that can be considered malicious by nonstatistical anomaly IPS or IDS systems:
 - A communication between two devices using Internetwork Package Exchange (IPX) in a network where only TCP/IP protocol is used
 - An occurrence of a routing protocol update originating from a user device
 - A broadcast storm or a network sweep
 - An anomalous packet, such as a "Christmas tree" packet in which all TCP flags are set, or a TCP segment in which the source and destination IP addresses are the same, and the TCP source and destination ports are the same.

Honeypot

Honey pots are a special type of IDS used to lure the attacker either to leave the real targets alone or to give the administrator the time to tighten the defense.



There are two basic philosophies for building honeypots, as follows:

- Honeypots can be systems which, to a certain degree, are vulnerable to attackers. Any attacks against a honeypot are made to seem successful to the attacker, giving administrators time to mobilize, log, and track the attacker without ever exposing production systems.
- Honeypots can be very interesting systems or resources—enticing to the attackers—that are well-hardened against attacks. They might *appear* to be more vulnerable, and thus appear more likely to be penetrable, by using, for example, these techniques:
 - Allowing more connectivity (less secured access) to the honeypot system
 - Configuring some applications to report a different (vulnerable) application or version number than the one actually used

In the event that the honeypot actually does contain some weakness that you may or may not be aware of, it is extremely important that the honeypot system or resource is extremely well-isolated from other devices in the network. This isolation protects other legitimate systems on the network if the honeypot system or resource is used as a “jump-off” point for attacks.

Examples

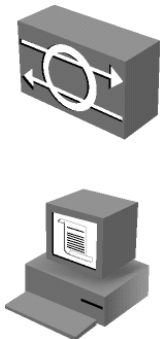
A classic honeypot is a UNIX system, which allows the attacker to log in, for example, using weak passwords or no passwords for certain accounts. When the attacker logs in, the administrator usually sets up a fake environment (a “jail”), in which the administrator can monitor the actions of the attacker.

Some people have built so-called spam honeypots—mail servers, which appear to be open relays, but in fact simply suck spamming e-mail in (attracting spam senders), and route it to the bit bucket.

Network-Based and Host-Based IPS

IPS systems can differ in their operational scope.

Network-Based and Host-Based IPS



- **NIPS:** Sensor appliances are connected to network segments to monitor many hosts.
- **HIPS:** Centrally managed software agents are installed on each host.
 - Cisco Security Agents (CSAs) defend the protected hosts and report to the central management console.
 - HIPS provides individual host detection and protection.
 - HIPS does not require special hardware.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-12

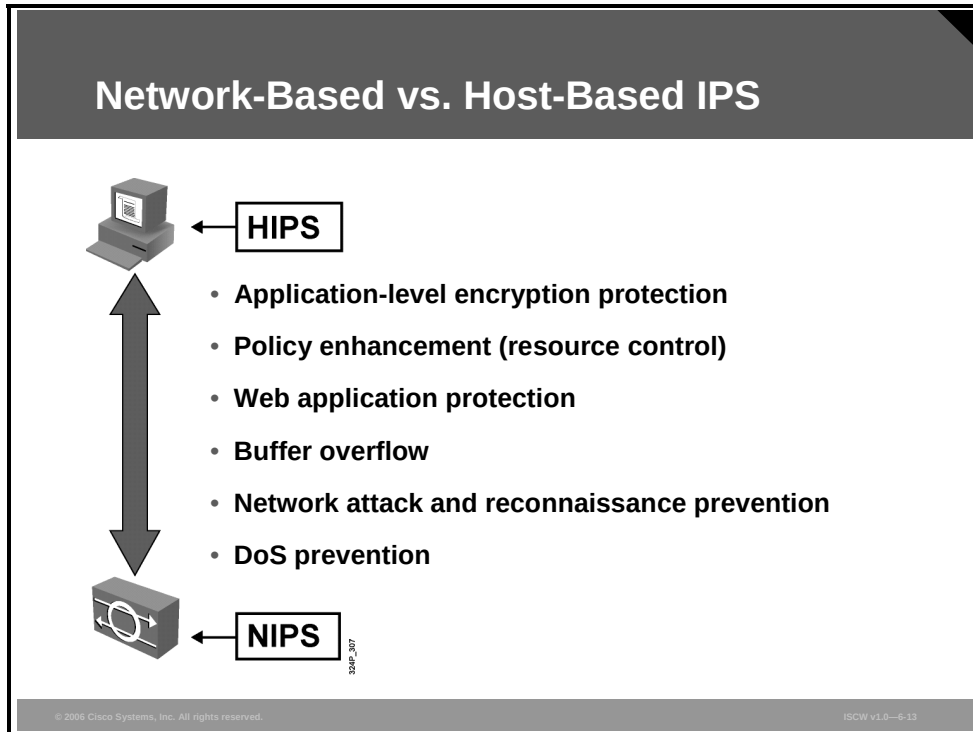
Monitoring intrusive activity can occur at two locations:

- **Network-based IPS (NIPS):** Instead of looking for intrusive activity at the host level, network-based monitoring systems examine packets that are traveling through the network for known signs of malicious activity. Because these systems are watching network traffic, any attack signatures detected may succeed or fail. It is usually difficult or impossible for network-based monitoring systems to assess the success or failure of actual attacks. They only indicate the presence of intrusive activity.
- **Host-based IPS (HIPS):** A host-based monitoring system examines information at the local host or operating system. It can be complex and examine actual system calls, or it can be simple and just examine system log files. Some host-based monitoring systems can halt attacks before they can succeed, whereas others report only on what has already happened. Cisco implementation of HIPS uses software packages called Cisco Security Agents (CSAs) that are deployed on the protected hosts and report their actions to the central management console, called Cisco Security Agent Management Center (CSA MC).

Note	The classification into network-based and host-based systems applies to IDS in the same way as it applies to IPS. For simplicity, the lesson refers to IPS only, because Cisco IPS encompasses a wider functionality than IDS.

Network-Based Versus Host-Based IPS

The figure shows how NIPS and HIPS complement each other.



While NIPS focuses on detecting buffer overflows, attacks on web servers, network reconnaissance, and denial of service (DoS) attacks, HIPS focuses on application and host resource protection.

A significant advantage of HIPS is that it can monitor operating system processes and protect critical system resources, including files that may exist only on a specific host. HIPS combines behavioral analysis and signature filters. HIPS can also combine the best features of antivirus, network firewalls, and application firewalls in one package.

A simple form of HIPS enables system logging and log analysis on the host. However, this approach can be extremely labor-intensive. HIPS requires software such as the CSA to be installed on each host to monitor activity performed on and against the host. The CSA performs the intrusion prevention analysis and protects the host.

NIPS Features

NIPS Features

- **Sensors are network appliances tuned for intrusion detection analysis.**
 - The operating system is “hardened.”
 - The hardware is dedicated to intrusion detection analysis.
- **Sensors are connected to network segments. A single sensor can monitor many hosts.**
- **Growing networks are easily protected.**
 - New hosts and devices can be added without adding sensors.
 - New sensors can be easily added to new networks.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—6-14

NIPS involves the deployment of monitoring devices, or sensors, throughout a network to capture and analyze traffic. Sensors detect malicious and unauthorized activity in real time and can take action when required. Sensors are deployed at designated network points, which enables security managers to monitor network activity while it occurs, regardless of the location of the target of the attack.

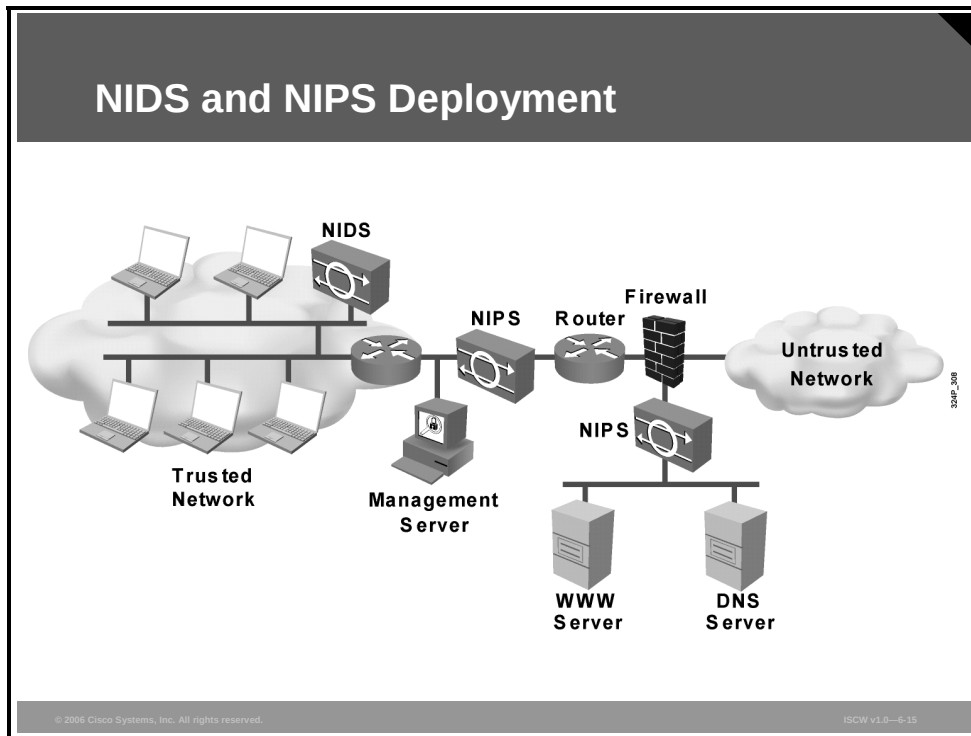
NIPS sensors are tuned for intrusion analysis. The underlying operating system of the platform on which the NIPS software is mounted is stripped of unnecessary network services, and essential services are secured. The hardware includes these components:

- **Network interface card (NIC):** NIPS must be able to connect into any network (Ethernet, FastEthernet, Gigabit Ethernet are common.)
- **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 NIPS to efficiently and accurately detect an attack.

NIPS gives security managers real-time security insight into their networks regardless of network growth. Additional hosts can be added to protected networks without needing additional sensors. When new networks are added, additional sensors are easy to deploy. Additional sensors are only required when their rated traffic capacity is exceeded, when their performance does not meet current needs, or when a revision in security policy or network design requires additional sensors to help enforce security boundaries.

NIDS and NIPS Deployment

For NIPS and network IDS (NIDS), the placement of sensors in the network is of crucial importance.



The figure illustrates a typical NIPS and NIDS deployment. Sensors are deployed at network entry points that protect critical network segments. The network segments have internal and external corporate resources. The sensors report to the Management Server located inside the corporate firewall.

Advantages of Network IPS and IDS

A network-based monitoring system has the benefit of easily seeing attacks that are occurring across the entire network. Seeing the attacks against the entire network gives a clear indication of the extent to which the network is being attacked. Furthermore, because the monitoring system is only examining traffic from the network, it does not have to support every type of operating system that is used on the network.

Disadvantages of Network IPS and IDS

Encryption of the network traffic stream can effectively blind the sensor. Reconstructing fragmented traffic can also be a difficult problem to solve. Possibly the biggest drawback to network-based monitoring is that as networks become increasingly larger (with respect to bandwidth), it becomes more difficult to place the sensor at a single location in the network and successfully capture all the traffic. Eliminating this problem requires the use of more sensors throughout the network. However, multiple sensors increase costs.

IDS and IPS Signatures

This topic describes the four types of IDS and IPS signatures.

Signature Categories

- **Four types of signatures:**
 - **Exploit signatures match specific known attacks.**
 - **Connection signatures match particular protocol traffic.**
 - **String signatures match string sequences in data.**
 - **DoS signatures match DoS attempts.**
- **Signature selection is based on:**
 - **Type of network protocol**
 - **Operating system**
 - **Service**
 - **Attack type**
- **Number of available signatures:**
 - **About 1500 for IPS sensors, 1200 for IOS IPS**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—6-17

A signature detects patterns in network traffic that should generate an alarm or drop packets. The IPS mechanism that matches the signatures against data packets is called a microengine. An IPS system contains several microengines and each microengine handles a set of signatures, typically grouped together by protocol or some other common characteristics.

Generally, there are four categories of signatures:

- **Exploit signatures:** Since exploit signatures typically identify a traffic pattern unique to a specific exploit, each exploit variant may require its own signature. Attackers may be able to bypass detection by slightly modifying the attack payload. Therefore, it is often necessary to produce an exploit signature for each attack tool variant.
- **Connection signatures:** Connection signatures generate an alarm based on the conformity and validity of the network connections and protocols.
- **String signatures:** The string signature engines support regular expression pattern matching and alarm functionality.
- **DoS signatures:** DoS signatures contain behavior descriptions that are considered characteristic of a DoS attack.

When malicious traffic passes through the sensor, one or more sensor microengines are activated to inspect the data. Each microengine controls a set of signatures. The sensor must decide which microengine to activate for scanning of the associated signatures. This selection is based on:

- The network protocol of the traversing traffic
- The type of the operating system a signature is associated with
- The session port
- Type of attack

For IPS sensor platforms, such as the Cisco IPS 4200 Series, there are about 1500 signatures available, while for the IOS IPS, there are about 1200 signatures. Cisco IOS IPS uses SDFs that contain signature descriptions for the most relevant attacks and are updated by Cisco on a regular basis.

Exploit Signatures

Exploit-specific signatures seek to identify network activity or upper-level protocol transactions that are unique to a specific exploit or attack tool.

Exploit Signatures	
OSI Layer	Exploit Signatures
Application layer	• DNS reconnaissance and DoS • Worms, viruses, Trojan horses, adware, malware
Transport layer	• Port sweeps • TCP SYN attack
Network layer	• Fragmentation attacks • IP options • ICMP reconnaissance and DoS

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6.18

The specificity of exploit signatures may provide an analyst with some insight into the methodology of an attacker, and may allow the analyst to identify and mitigate targeted vulnerabilities. Exploit signatures are often relatively easy to produce for simple protocols and attacks, and are often employed in “pattern matching” IDS and IPS products. Examples of exploit signatures are grouped by OSI layer.

These are examples of exploit signatures in the network layer:

- The most common fragmentation attack attempts to exhaust target resources by sending many noninitial fragments and tying up reassembly buffers.
- Target systems may be configured to not accept IP datagrams with certain IP options, such as source routing. Signatures may analyze these datagrams before they are discarded. The configuration for this analysis is based upon the target operating system or the default. This analysis is enabled by default, but may be turned off for performance.
- Distributed DoS attacks are the “next generation” of DoS attacks on the Internet. Examples of such attacks on the network layer include Internet Control Message Protocol (ICMP) echo request floods, and ICMP directed broadcasts (also known as smurf attacks).

These are examples of exploit signatures in the transport layer:

- Port sweeps, in which the attacker sends packets to all well-known TCP and User Datagram Protocol (UDP) ports of a host or network. Port sweeps provide a complete list of all services running on the hosts.
- TCP SYN flooding, aimed at compromising the availability of a server that runs out of resources to serve legitimate sessions.

These are examples of exploit signatures in the application layer:

- When hackers attempt to penetrate a particular network, they often need to learn as much information as possible about the network before launching attacks. Examples include Domain Name System (DNS) queries, which reveal information such as who owns a particular domain and what addresses have been assigned to that domain.
- Malicious code operating at the application layer includes worms, viruses, Trojan horses, adware, and malware.

Signature Examples

This topic describes some examples of signatures implemented in Cisco IOS IPS.

Signature Examples		
ID	Name	Description
1101	Unknown IP Protocol	Triggers when an IP datagram is received with the protocol field set to 134 or greater.
1307	TCP Window Size Variation	This signature will fire when the TCP window varies in a suspect manner.
3002	TCP SYN Port Sweep	Triggers when a series of TCP SYN packets have been sent to a number of different destination ports on a specific host.
3227	WWW HTML Script Bug	Triggers when an attempt is made to view files above the HTML root directory.

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—4-19

The table lists examples of selected signatures with their description explaining the signature operations.

Signature Examples

Signature ID	Signature Name	Signature Description
1101	Unknown IP Protocol	Triggers when an IP datagram is received with the protocol field set to 134 or greater. These protocol types are undefined or reserved, and should not be used. Use of undefined or reserved protocol types may be indicative of establishment of a proprietary communication channel. No known exploits implement this concept. This does not preclude the possibility that exploits do exist outside of the realm of Cisco Systems knowledge domain.
1307	TCP Window Size Variation	Fires when the TCP window varies in a suspect manner.
3002	TCP SYN Port Sweep	Triggers when a series of TCP SYN packets have been sent to a number of different destination ports on a specific host. This is indicative that a reconnaissance sweep of your network may be in progress. This may be the prelude to a more serious attack. For testing purposes, this sweep can be generated using a widely available public domain tool called nmap.
3227	WWW HTML Script Bug	Triggers when an attempt is made to view files above the HTML root directory.

Cisco IOS IPS Signature Definition Files

This section describes how SDFs work.

Cisco IOS IPS SDFs

- A Cisco IOS router acts as an in-line intrusion prevention sensor.
- Signature databases:
 - Built-in (100 signatures embedded in Cisco IOS software)
 - SDF files (can be downloaded from Cisco.com):
 - Static (attack-drop.sdf)
 - Dynamic (128MB.sdf, 256MB.sdf)—based on installed RAM
- Configuration flexibility:
 - Load built-in signature database, SDF file, or even merge signatures to increase coverage
 - Tune or disable individual signatures

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—0-21

The Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, and scanning each packet to match any of the Cisco IOS IPS signatures. When the IPS detects suspicious activity, it responds before network security can be compromised, and logs the event through syslog or Security Device Event Exchange (SDEE) protocol.

Note SDEE is an application level communication protocol that is used to exchange IPS messages between IPS clients and IPS servers. It provides a secure communication path using Secure Socket Layer (SSL) (Secure HTTP [HTTPS]). SDEE replaced the Post Office Protocol (POP) on Cisco IOS routers.

Cisco IOS IPS offers configuration flexibility by providing these two functions:

- The administrator can load the built-in signature database (available in the IOS image itself), load a specific signature database file (sdf), or even merge different databases to extend the protection scope.
- Individual signatures can be disabled or tuned in case of false positives.

IPS signature files are dynamically updated and posted to Cisco.com on a regular basis. Thus, customers can access signatures that help protect their network from the latest known network attacks. Multiple definition sources are available, such as the default, built-in signatures that are shipped with the routers, or the SDF files named 64MB.sdf, 128MB.sdf, and 256MB.sdf. They differ in the number of configured signatures. The administrator should select the appropriate SDF file based on the amount of RAM memory in the router. The SDF files are dynamically updated and accessed from Cisco.com.

Cisco IOS IPS Alarms

This topic describes what happens when a signature is matched.

Cisco IOS IPS Alarms: Configurable Actions

- **Send an alarm to a syslog server or a centralized management interface (syslog or SDEE).**
- **Drop the packet.**
- **Reset the connection.**
- **Block traffic from the source IP address of the attacker for a specified amount of time.**
- **Block traffic on the connection on which the signature was seen for a specified amount of time.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISFW v1.0—6-23

When a signature is matched, the IPS responds in real time, before network security can be compromised, and logs the event through Cisco IOS syslog messages or SDEE. You can configure IPS to choose the appropriate response to various threats. When packets in a session match a signature, IPS can take any of these actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface. This action is typically combined with other preventive actions.
- Drop the packet. This action is effective for all IP protocols and does not affect any legitimate user if the source IP address was spoofed.
- Reset the connection. This action works only for TCP sessions.

Note The sensor sends TCP RST to both communication endpoints and spoofs the source IP address in those TCP RST packets. For example, if A and B were communicating via TCP, the sensor sends RST to A pretending to be B, and to B pretending to be A.

- Block traffic from the source IP address of the attacker for a specified amount of time. This action imposes a penalty on the attacker IP address.
- Block traffic on the connection on which the signature was seen for a specified amount of time. This action imposes a penalty on the attacker session.

Cisco IOS IPS Alarm Considerations

This section describes additional issues that you should consider when implementing signatures.

Cisco IOS IPS Alarm Considerations

- **Alarms can be combined with reactive actions.**
- **SDEE is a communication protocol for IPS message exchange between IPS clients and IPS servers:**
 - **More secure than syslog**
 - **Reports events to the SDM**
- **When blocking an IP address, beware of IP spoofing:**
 - **May block a legitimate user**
 - **Especially recommended where spoofing is unlikely**
- **When blocking a connection:**
 - **IP spoofing less likely**
 - **Allows the attacker to use other attack methods**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--6-24

You can configure a combination of actions when a signature is triggered. Typically, you would combine an alert with some preventive action, such as packet drop.

Cisco IOS IPS can report IPS intrusion alerts either using syslog or SDEE. SDEE is more secure and therefore recommended, because it uses HTTPS to exchange data. Cisco IOS routers use SDEE to report IPS events to the SDM.

Note Although SDM provides secure communications, its monitoring capabilities are limited in that it is not a real-time monitoring tool and it does not offer advanced filtering and correlation features. For a fully functional monitoring solution, deploy other Cisco tools, such as Cisco Security Monitoring, Analysis, and Response system (CS-MARS) or CiscoWorks Monitoring Center for Security, which is a component of the VPN/Security Management Solution.

When implementing an IOS-based IPS, you should consider the following:

- With IP address blocking, you may block a legitimate user whose address was spoofed by an attacker. This method is especially recommended in environments where IP spoofing is unlikely.
- With connection blocking, a potential connectivity disruption in case of address spoofing is less likely, because it is difficult to establish a bidirectional session using a spoofed IP address because return traffic will typically never reach the attacker. The disadvantage of connection blocking is that the hacker can use other protocols or ports to attack the target.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **IDS and IPS are complementary technologies.**
- **IDS is passive and triggers a wider range of alarms.**
- **IPS is reactive and more focused on the environment.**
- **Common types of IDS and IPS are: policy, signature, anomaly, honeypot, network- and host-based.**
- **Signatures are categorized based on their nature and OSI layer.**
- **Cisco IOS IPS in-line sensor uses SDFs to prevent intrusions.**
- **Possible actions when a signature triggers include: alarm, drop packet, reset connection, block IP address, block connection.**

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—6-25

Configuring Cisco IOS IPS

Overview

This lesson describes how to configure a Cisco IOS intrusion prevention system (IPS) using the router command-line interface (CLI) and the Security Device Manager (SDM). SDM offers an IPS Policies wizard that simplifies the configuration process. The lesson explains the steps performed within the wizard, such as interface selection, flow identification, and specification of the signature definition file (SDF). The lesson also describes how to use the SDM to verify configuration deployment, modify IPS policies, customize global settings, view IPS events, and tune signatures.

Objectives

Upon completing this lesson, you will be able to describe the procedure to configure Cisco IOS IPS operations using SDM. This ability includes being able to meet these objectives:

- Configure and verify IOS IPS using the CLI interface
- Describe the Cisco IOS IPS tasks you can complete with SDM
- Select interfaces and configure SDF locations within the SDM IPS Policies wizard
- View the IPS policy summary and deliver the IPS configuration to the router using the SDM IPS Policies wizard
- Configure IPS policies and global settings using the SDM
- View SDEE messages in the SDM
- Tune signatures using the SDM

Configuring Cisco IOS IPS

This topic describes how to configure IPS on Cisco IOS routers.

Cisco IOS IPS Configuration Steps

1. **Configure basic IPS settings:**
 - Specify SDF location
 - Configure failure parameter
 - Create an IPS rule and, optionally, combine it with a filter
 - Apply the IPS rule to interface
2. **Configure enhanced IPS settings:**
 - Merge SDFs
 - Disable, delete, and filter selected signatures
 - Reapply the IPS rule to the interface
3. **Verify the IPS configuration.**

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0-6.3

Cisco IOS IPS Configuration Steps

To set up Cisco IOS IPS, you need to configure basic IPS settings and, optionally, use the enhanced settings.

The basic configuration steps are as follows:

- Specify the SDF from which to load the signatures.
- Configure a failure parameter that defines whether to block or forward traffic if signature microengines (SMEs) are not operational.
- Create an IPS rule and, optionally, combine it with an access control list (ACL) for traffic filtering purposes.
- Apply the IPS rule to an interface.

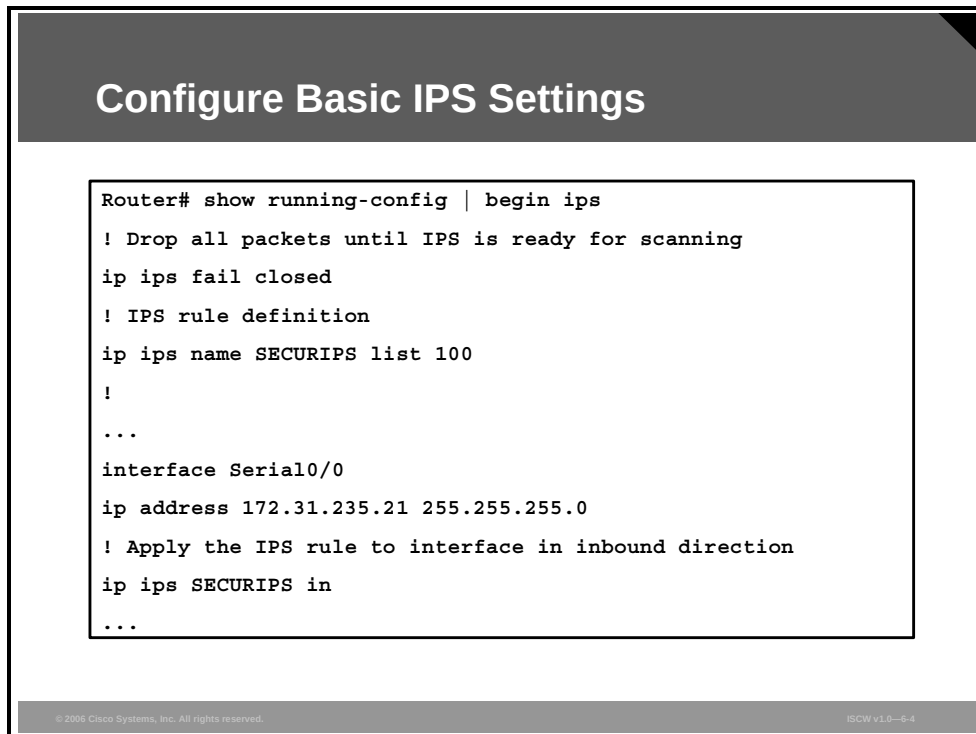
These are the enhanced configuration steps:

- Merge two or more SDFs to increase the signature coverage.
- Delete, disable, or filter individual signatures.
- Reapply the IPS rule to an interface for the changes to take effect.

In the end, you will verify the IPS configuration and operations.

Basic IOS IPS Configuration

The figure shows a simple Cisco IOS IPS configuration.



The default command **ip ips sdf builtin** does not appear in this IPS configuration example because the configuration specifies the default built-in SDF. This file contains 100 signatures, but with sub-signatures, the total number is 132. The keyword **builtin** is the default option of the **ip ips sdf** command.

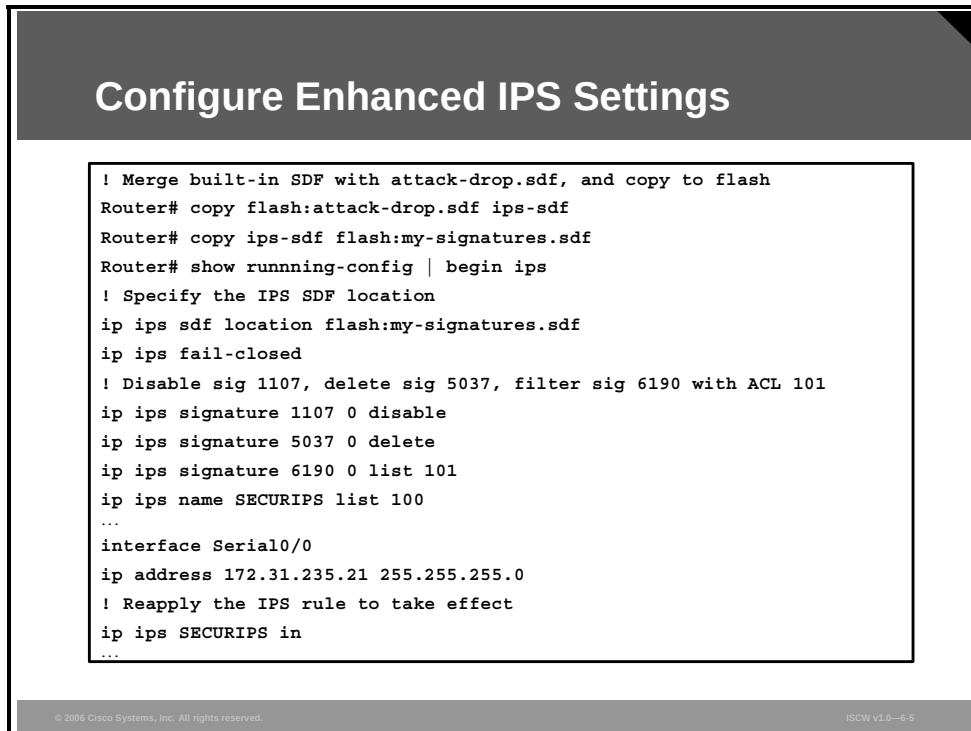
The command **ip ips fail closed** instructs the router to drop all traffic if any of the SMEs that should scan the data are not available. This command has no other parameters. If the SMEs are unavailable and you want to forward the packets without scanning, use the no **ip ips fail closed** command.

The command **ip ips name SECURIPS** is used to create an IPS rule. The IPS rule is combined with an ACL (**list 100**). This optional standard or extended ACL filters the traffic that will be scanned. If the packet is permitted by the ACL, the signature will be scanned and reported; if the packet is denied by the ACL, it will bypass the scanning engine and go directly to its destination.

At the end, the IPS rule is applied to a router interface (**ip ips SECURIPS in**). IPS rules can be applied to an interface in either the inbound or outbound direction. In this example, the rule is applied inbound to the interface, as specified by the parameter **in**. Typically, it is recommended to apply the rules in inbound direction.

Enhanced Cisco IOS IPS Configuration

This enhanced configuration example is a continuation of the basic IOS IPS configuration.



In this enhanced Cisco IOS IPS configuration example, the first command, **copy flash:attack-drop.sdf ips-sdf**, merges the attack-drop.sdf file in flash with the built-in SDF that has been loaded as a result of the basic configuration.

The second command, **copy ips-sdf flash:my-signatures.sdf**, copies the resulting merged SDF to flash so that the signature database becomes usable after a router reload.

The configuration command **ip ips sdf location flash:my-signatures.sdf** specifies a new SDF location pointing to the merged SDF file in the flash.

The command **ip ips signature 1107 0 disable** deactivates the signature with ID 1107 and sub-signature ID 0.

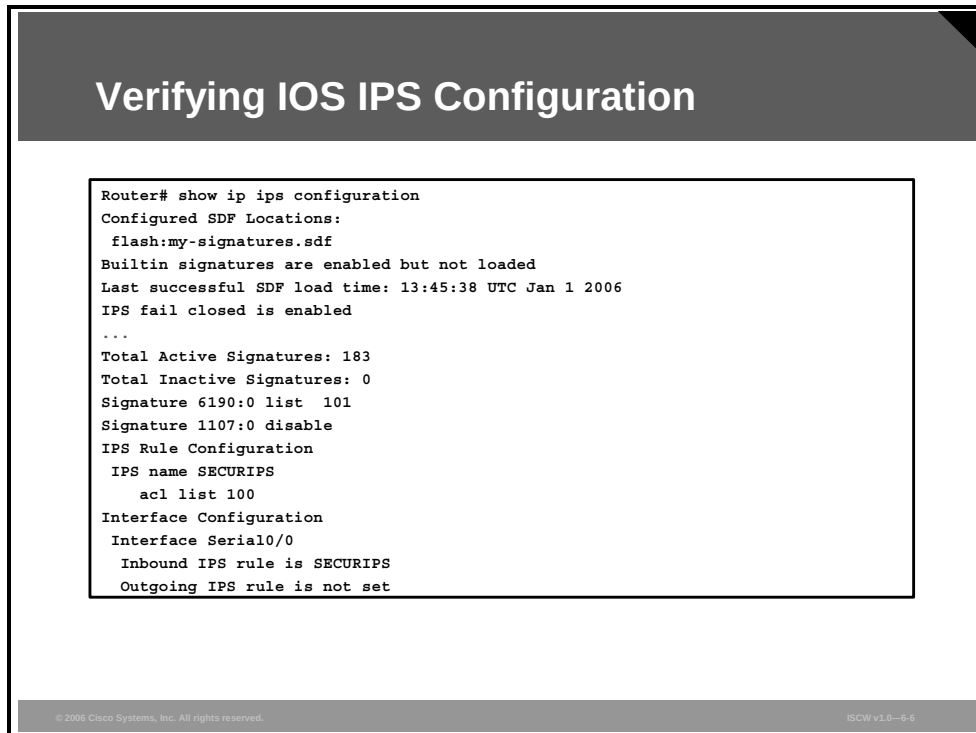
The command **ip ips signature 5037 0 delete** marks the signature with ID 5037 and sub-signature ID 0 for deletion. The signature will be removed when the signatures are reloaded or saved.

The command **ip ips signature 6190 0 list 101** filters the traffic prior to scanning by the signature with ID 6190 and sub-signature ID 0. If the packet is permitted by the ACL, the signature will be scanned; if the packet is denied by the ACL, the signature is deemed disabled.

Finally, the IPS rule needs to be reapplied to the interface for the changes in SDF to take effect. You can do so by unbinding the IPS rule from the interface and assigning the rule to the interface again (using the **no ip ips SECURIPS in** and **ip ips SECURIPS in** commands in interface configuration mode).

Verifying IOS IPS Configuration

You can verify the Cisco IOS IPS configuration and parameters by using the **show ip ips configuration** EXEC command, and the sample resulting output is shown in the figure.



The merged SDF (my-signatures.sdf) is configured as the SDF location. Built-in signatures are reported to not have been loaded. This is correct, although in this example they are included in the merged signature file and effectively loaded from the flash location. The fail-close is activated. The total number of signatures (183) results from merging the built-in signatures (132) with the signatures from attack-drop.sdf (51). The signature 1107:0 is disabled, signature 6190:0 is filtered, and the signature 5037:0 has been deleted and does not appear in this output. The rule SECURIPS is referencing ACL 100 and is applied to Serial0/0 in inbound direction.

Cisco IOS IPS SDM Tasks

This topic describes the Cisco IOS IPS tasks you can complete with SDM.

Cisco IOS IPS SDM Tasks

- **Tasks included in the IPS Policies wizard:**
 - Quick interface selection for rule deployment
 - Identification of the flow direction
 - Dynamic signature update
 - Quick deployment of default signatures
 - Validation of router resources before signature deployment
- **Signature customization available in the SDM IPS Edit menu:**
 - Disable
 - Delete
 - Modify parameters

© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0--6.0

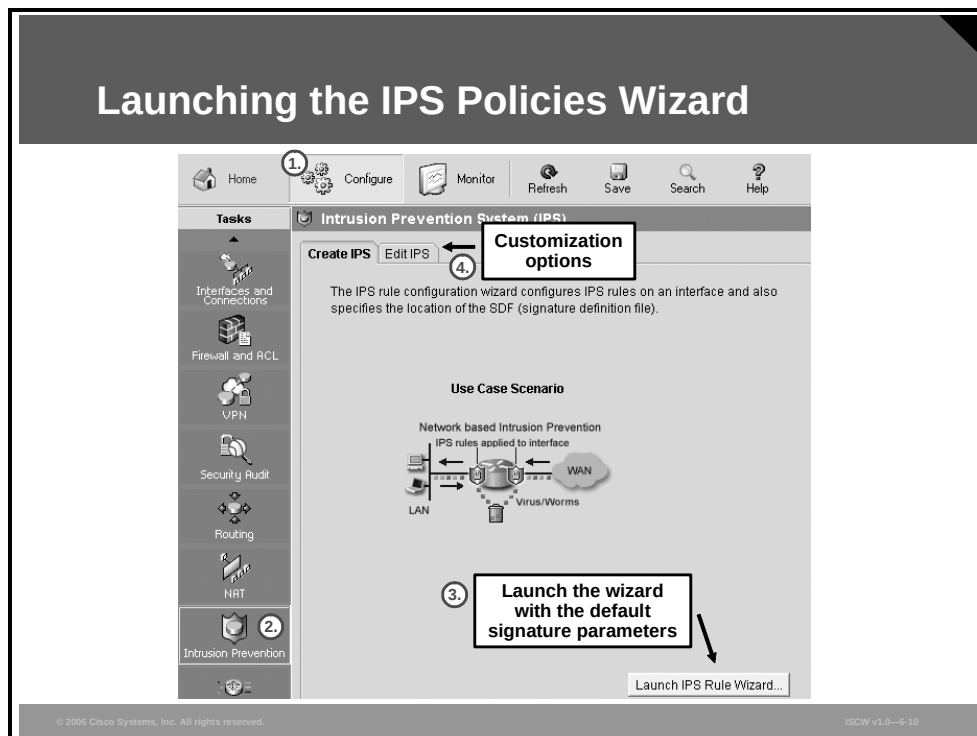
The SDM provides a wide range of configuration capabilities for Cisco IOS IPS. All options are configurable through the IPS Edit menu.

Additionally, SDM offers the IPS Policies wizard, which expedites the deployment of default IPS settings. The wizard provides configuration steps for interface and traffic flow selection, SDF location, and signature deployment. The wizard also verifies the available router resources before the commands are sent to the router. The IPS Policies wizard configures IPS using default signature descriptions, as defined in the SDF files provided by Cisco, or the built-in signatures included in the Cisco IOS.

If you want to customize the signatures after the wizard deploys the default settings, you should use the IPS Edit menu available in SDM. Using the Edit menu, you can modify any signature parameter, as well as disable and delete the signatures.

Selecting Interfaces and Configuring SDF Locations

This topic describes how to launch the IPS Policies wizard available in the SDM.

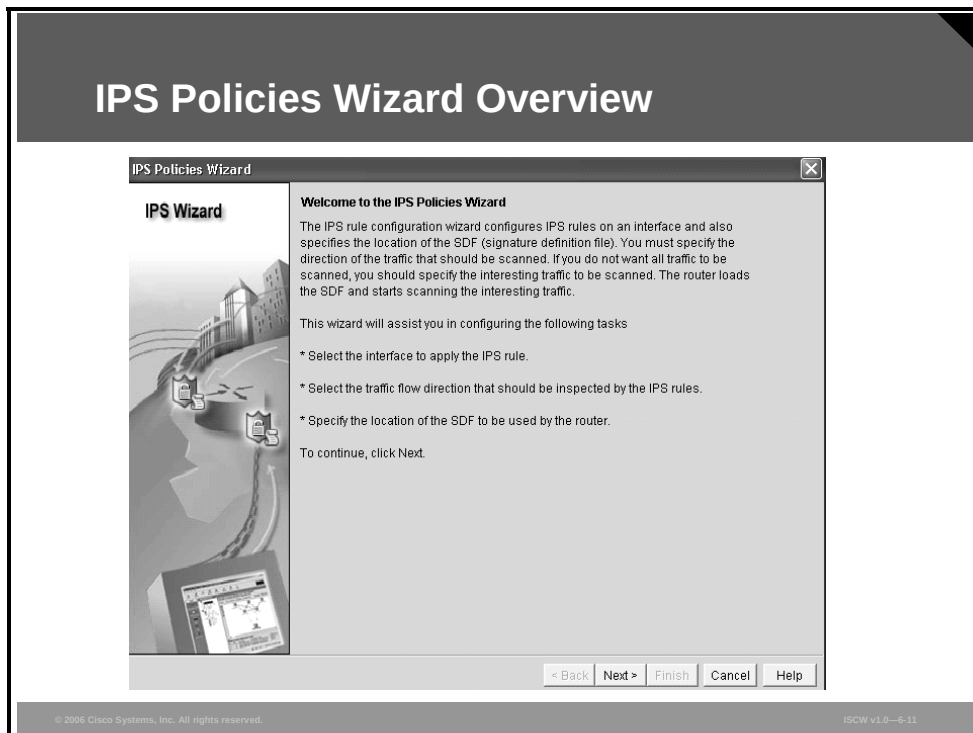


To access the IPS configuration options available in the SDM, follow this procedure:

- Step 1** Click the **Configure** icon in the top horizontal navigation bar to enter the configuration page.
- Step 2** Click the **Intrusion Prevention** icon in the left vertical navigation bar.
- Step 3** To activate IPS functionality using default signature descriptions, click the **Create IPS** tab and click the **Launch IPS Rule Wizard** button.
- Step 4** To configure all IPS features, including the signature customization options, you may optionally select the **Edit IPS** tab.

IPS Policies Wizard Overview

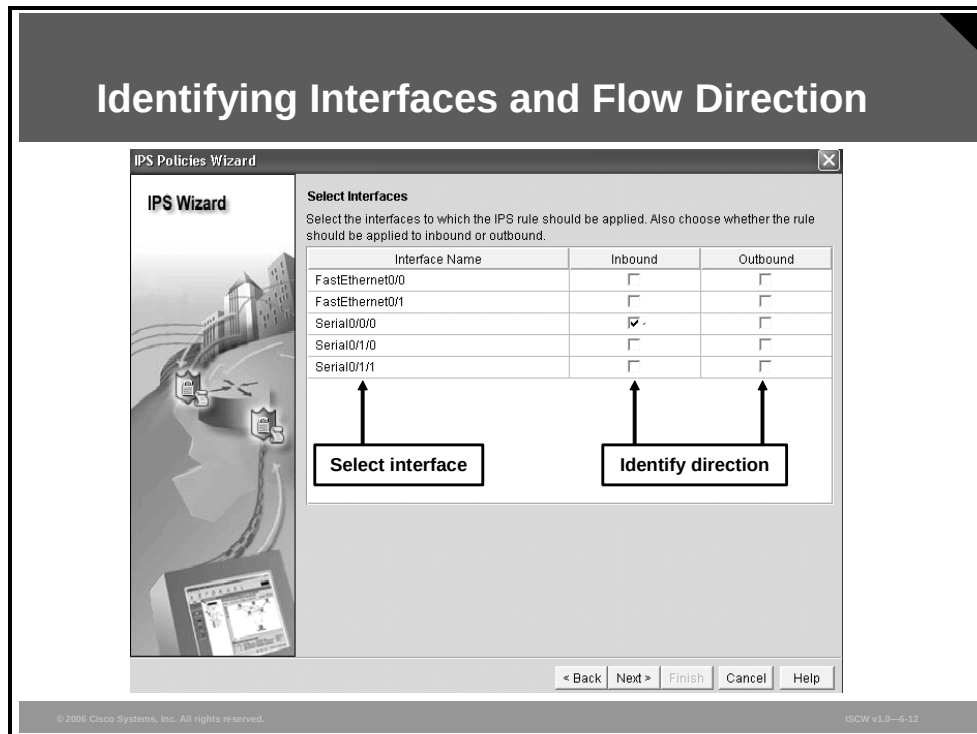
Next, the wizard provides an overview of functions that will be configured on the router.



After clicking the **Launch IPS Rule Wizard** button, a window opens, describing the tasks through which the IPS Policies wizard will guide you. You will select the interfaces to apply the IPS rules to, select traffic flow direction to be inspected by the IPS rules, and specify the SDF location. Click **Next** to proceed to the interface selection.

Identifying Interfaces and Flow Direction

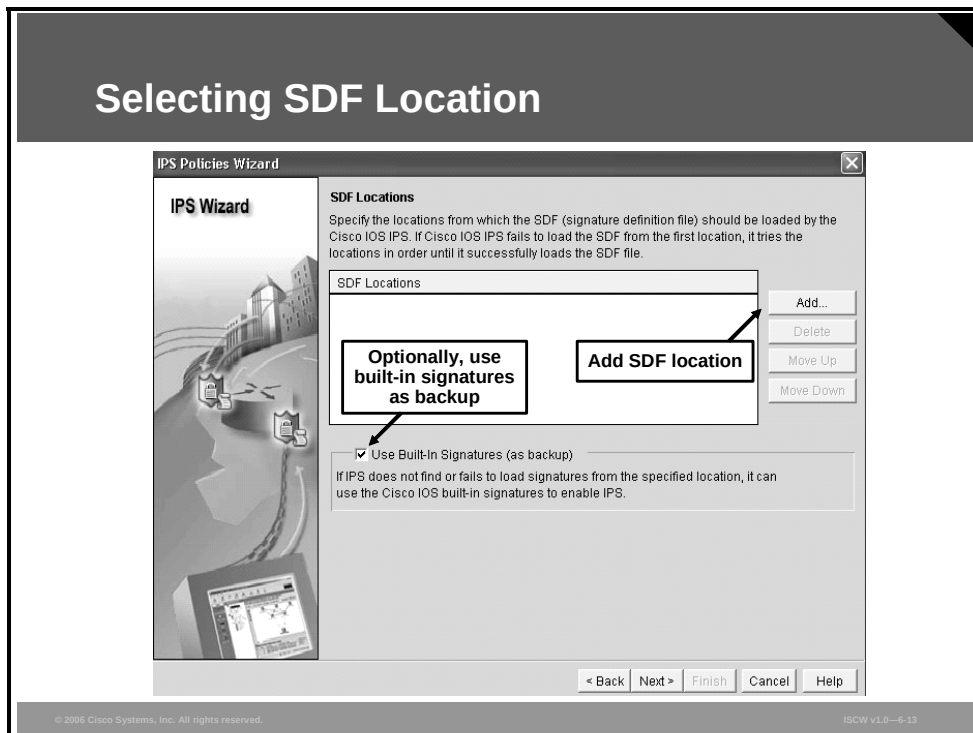
The wizard requires you to provide details about the interfaces and flow directions.



After you have clicked **Next** in the wizard Welcome page, you must specify where the IPS microengines should scan the traffic. The wizard will create an IPS rule that will be applied to an interface. Provide the interface name and the direction in which to assign the IPS rule to. In typical environments, you will apply the rules in inbound direction on interfaces where incoming malicious traffic is likely.

Selecting SDF Location

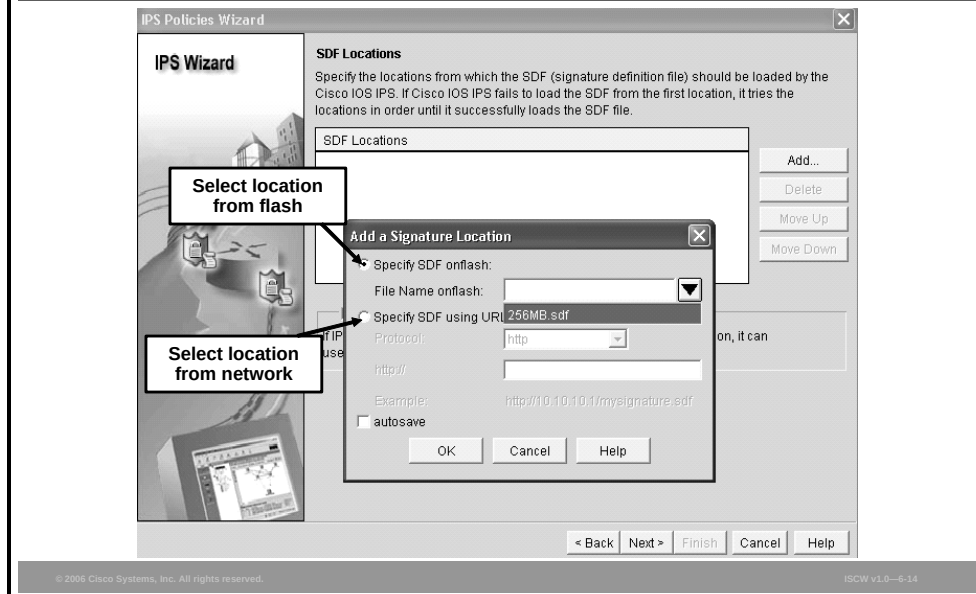
The wizard needs to load the signature database.



Next, you must specify which SDF should be used to load the signatures, and its location. Click the **Add** button to provide the information about the SDF location.

Additionally, there is the **Use Built-in Signatures (as backup)** check box. If checked, the Cisco IOS built-in signature set will be used if the signatures cannot be loaded from the specified location or if no SDF location has been configured.

Selecting SDF Location (Cont.)

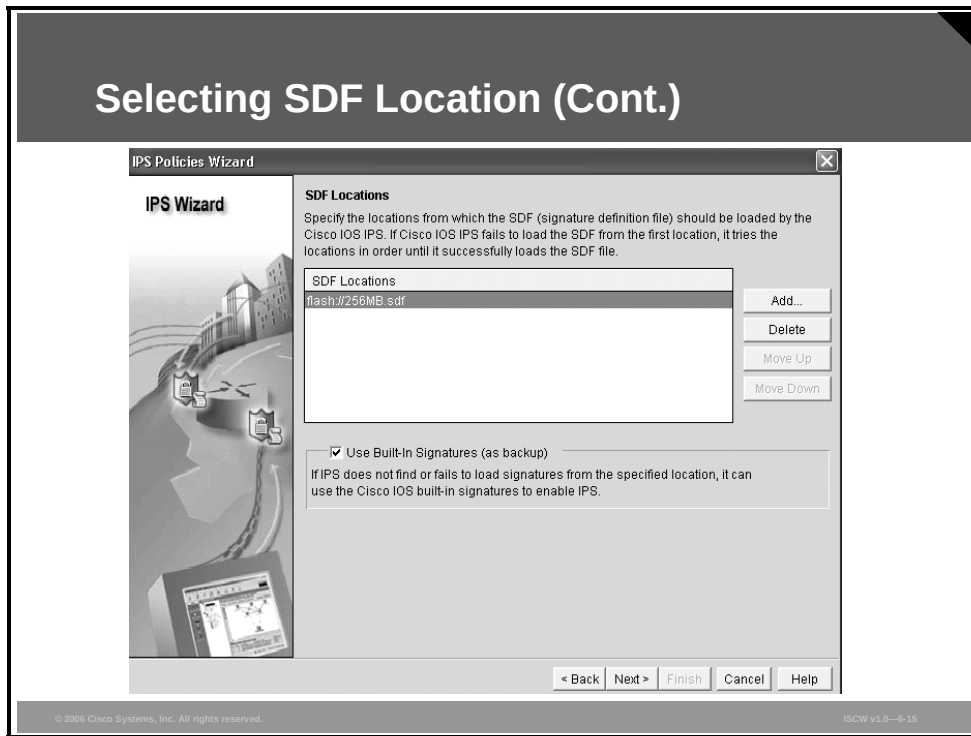


After clicking the **Add** button, you can specify the SDF location in the flash memory or on a network server.

Note Cisco publishes multiple types of SDFs. If you use the Cisco installation program for SDM installation, the most appropriate type of the SDF file is automatically copied to the flash memory based on the amount of the installed RAM.

After you specify the SDF location, click **OK**.

Selecting SDF Location (Cont.)

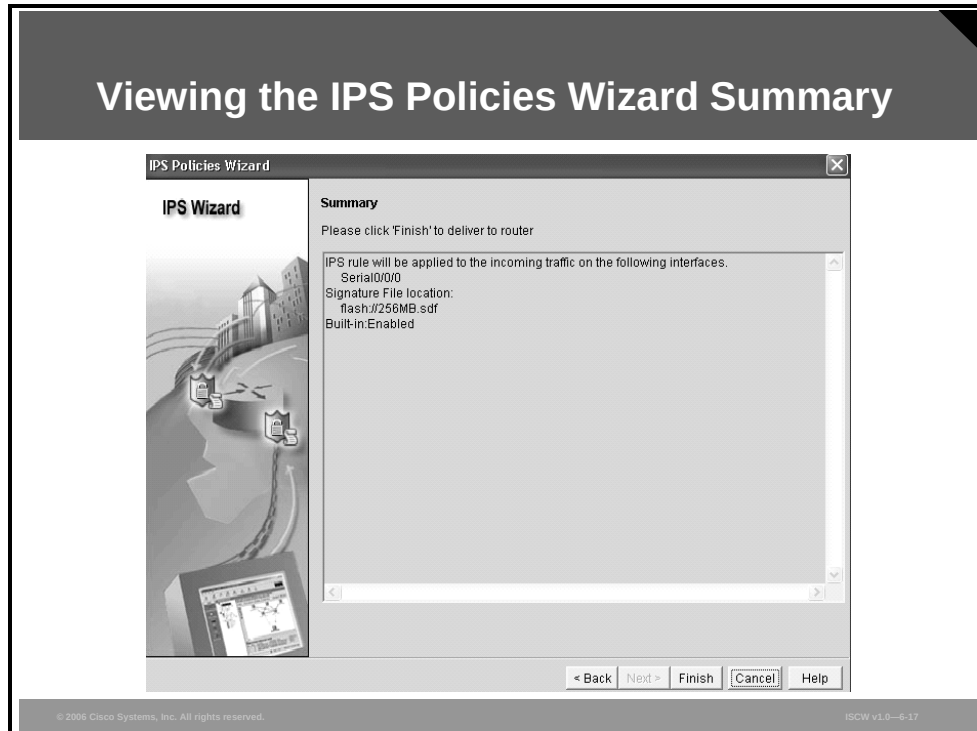


Next, you see a screen showing the currently configured SDF locations. You may configure more than one SDF location by clicking the **Add** button. If you configure more than one SDF location, Cisco IOS will try to load them, starting from the top of the list. If IOS fails to load the SDF from the first location in the list, it will try the subsequent locations one by one until it successfully loads the SDF file.

Click **Next** to proceed to the next task, in which you will view and deploy the IPS configuration.

Viewing the IPS Policy Summary and Delivering the Configuration to the Router

This topic describes how to view the IPS policy summary offered by the SDM and deliver the configuration to the router.

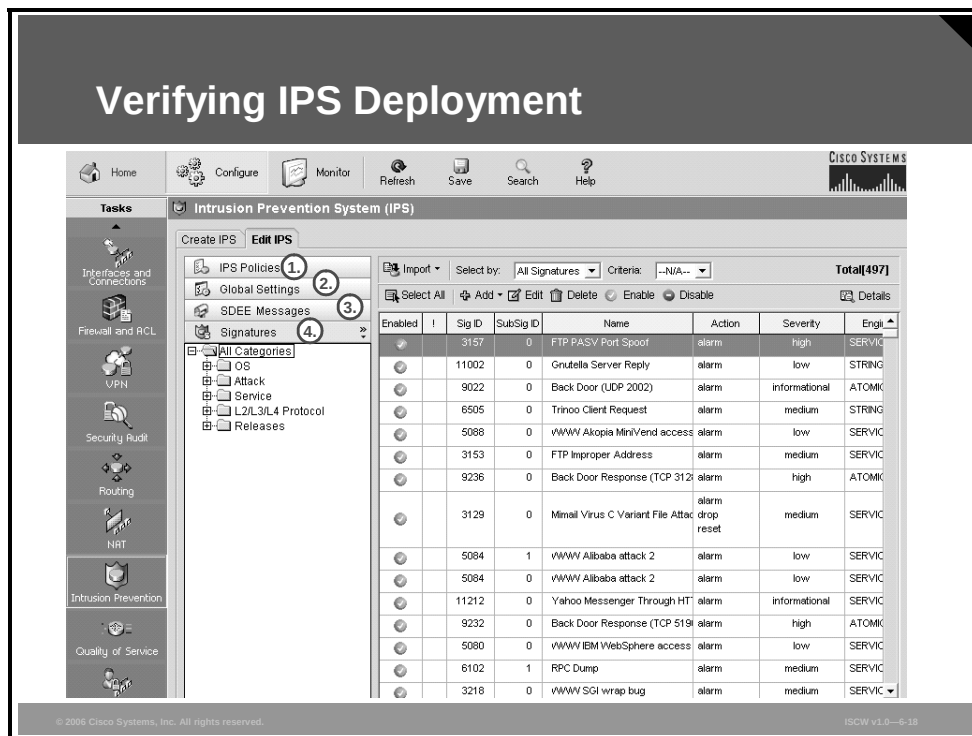


After clicking **Next** in the SDF locations window, the IPS Policies wizard displays a summary of the changes that will be deployed to the router. The wizard includes information about the interfaces and direction in which the IPS rules will be applied, the SDF location, and whether built-in signatures are enabled for backup usage.

Deploy the configuration by clicking the **Finish** button.

Verifying IPS Deployment

After the IPS commands generated by the wizard are sent to the router, you are brought to the Edit IPS tab.



In the menu under the Edit IPS tab, you can verify and modify the configured settings, as well as view and tune the available signatures.

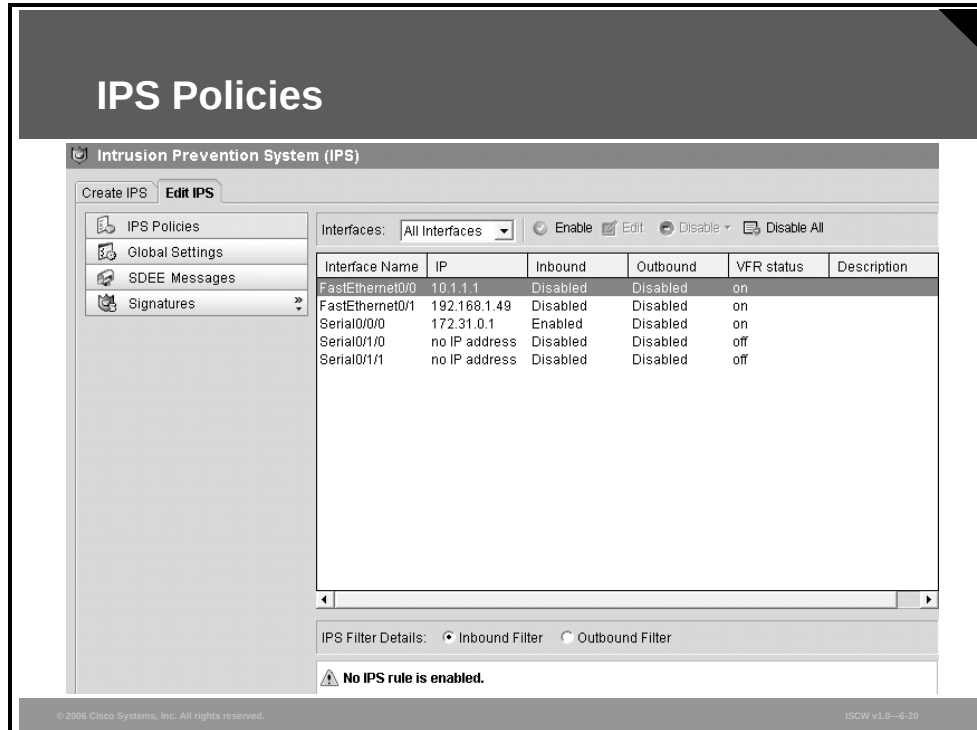
The Edit IPS menu is divided into four sections:

1. IPS policies
2. Global settings
3. Security Device Event Exchange (SDEE) messages
4. Signatures

Configuring IPS Policies and Global Settings

This topic describes how to customize IPS policies and global settings. You need to perform these steps:

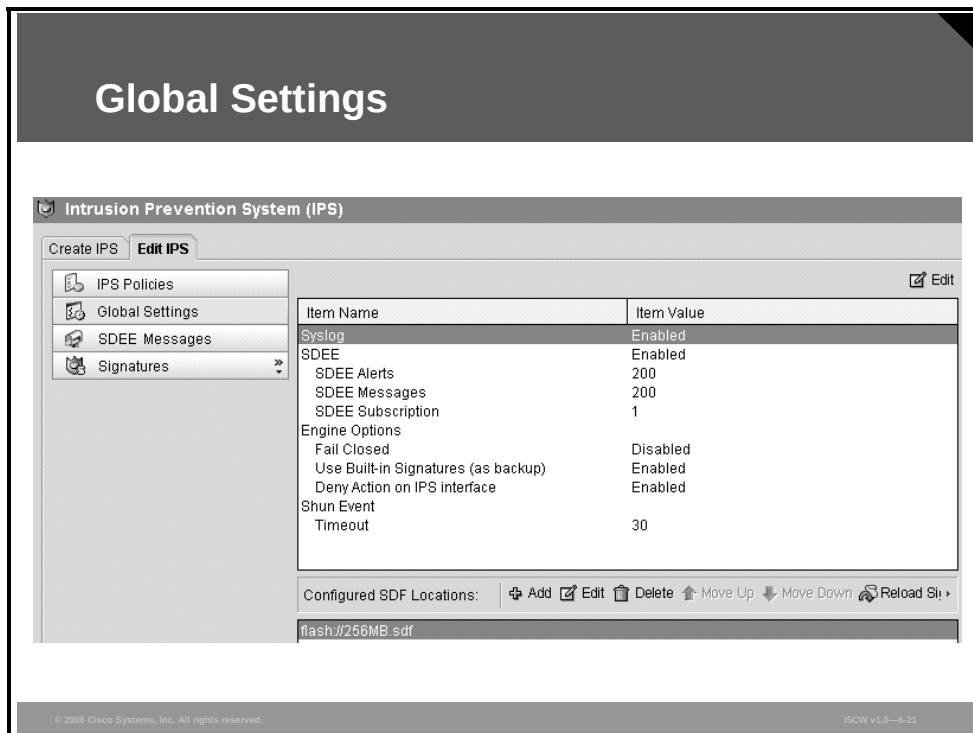
- View and, if needed, modify the IPS policies.
- View and, if needed, change the global settings.



Click **IPS Policies** in the menu part of the Edit IPS tab to verify the assignment of IPS rules to the router interfaces. In the example, the only enabled IPS rule is attached to the Serial0/0/0 interface in the inbound direction. This configuration matches the settings you previously submitted in the IPS Policies wizard. It corresponds to the Identifying Interfaces and Flow Direction step of the IPS Policies wizard, in which the IPS rule was applied inbound to the outside interface (Serial0/0/0).

Global Settings

This section describes how to modify IPS global settings using the SDM.



Click **Global Settings** in the menu of the Edit IPS tab to view and modify the general IPS settings configured on the router. These settings include reporting settings using two protocols: syslog and SDEE.

Note SDEE is an application-level communications protocol that is used to exchange IPS messages between IPS clients and IPS servers. You do not need to configure the address of the SDEE server. SDM uses SDEE to pull the event logs from the router.

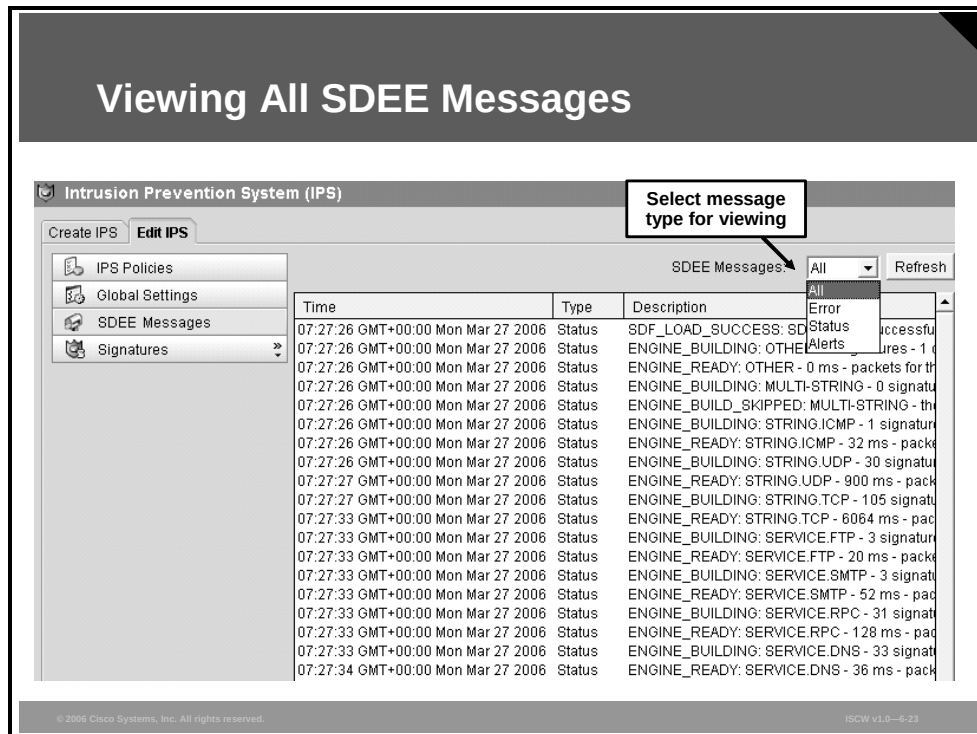
You also see the status of the fail-closed setting. SDM default is fail-closed disabled. If enabled, the router will drop all packets if the IPS engine is unable to scan data. Finally, you can verify if the built-in signatures have been enabled for backup purposes if the configured SDF is unavailable or cannot be loaded.

If you want to modify any of these global settings, click the **Edit** button in the upper-right corner of the window to perform the desired changes. A configuration window will open, in which you can modify any parameters visible in the figure.

Viewing SDEE Messages

This topic describes how to view the SDEE messages. You will perform these steps:

- View all SDEE messages.
- View SDEE status messages.
- View SDEE alerts.



The SDM offers you the option to view the SDEE messages if you click **SDEE Messages** in the middle part of the Edit IPS tab. By default, all message types are displayed in the window. You can limit the number of presented messages by selecting the category from the **SDEE Messages** drop-down list in the upper-right corner.

Note This SDEE Messages view does not work in real time. If you want to display the current messages, you need to click the **Refresh** button in the upper right corner of the window.

Viewing SDEE Status Messages

You can use the SDM to view the SDEE status messages.

Viewing SDEE Status Messages

Intrusion Prevention System (IPS)

Create IPS Edit IPS

SDEE Messages: **Status** Refresh

	Type	Description
Mon Mar 27 2006	Status	SDF_LOAD_SUCCESS: SDF loaded successfully from flash://256MB
Mon Mar 27 2006	Status	ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: OTHER - 0 ms - packets for this engine will be sca
Mon Mar 27 2006	Status	ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines
Mon Mar 27 2006	Status	ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new signa
Mon Mar 27 2006	Status	ENGINE_BUILDING: STRING.ICMP - 1 signatures - 3 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: STRING.ICMP - 32 ms - packets for this engine will
Mon Mar 27 2006	Status	ENGINE_BUILDING: STRING.UDP - 30 signatures - 4 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: STRING.UDP - 900 ms - packets for this engine wi
Mon Mar 27 2006	Status	ENGINE_BUILDING: STRING.TCP - 105 signatures - 5 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: STRING.TCP - 6064 ms - packets for this engine w
Mon Mar 27 2006	Status	ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: SERVICE.FTP - 20 ms - packets for this engine will
Mon Mar 27 2006	Status	ENGINE_BUILDING: SERVICE.SMTP - 3 signatures - 7 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: SERVICE.SMTP - 52 ms - packets for this engine w
Mon Mar 27 2006	Status	ENGINE_BUILDING: SERVICE.RPC - 31 signatures - 8 of 15 engines
Mon Mar 27 2006	Status	ENGINE_READY: SERVICE.RPC - 128 ms - packets for this engine w

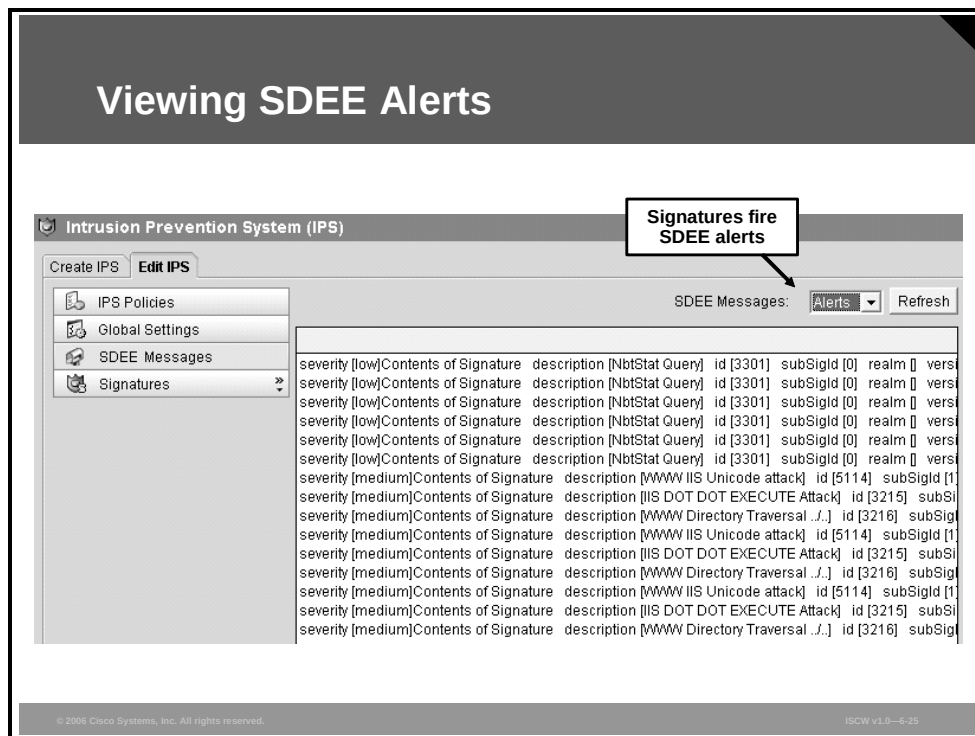
© 2006 Cisco Systems, Inc. All rights reserved. ISCW v1.0—5-24

Select **Status** from the **SDEE Messages** drop-down list to display the status events only.

This view includes reports about the status of all IPS engines. You can see the compilation results for engines that contain some signatures associated with it, along with their status. You can also see which engines have not been built because there were no signatures associated with them. You can identify such engines by looking for the *ENGINE_BUILD_SKIPPED: [engine name] – there are no new signature definitions* message. In this example, that is the case for the MULTI-STRING engine.

Viewing SDEE Alerts

You can use the SDM to view the SDEE alerts.



Select **Alerts** from the **SDEE Messages** drop-down list to view the alerts only.

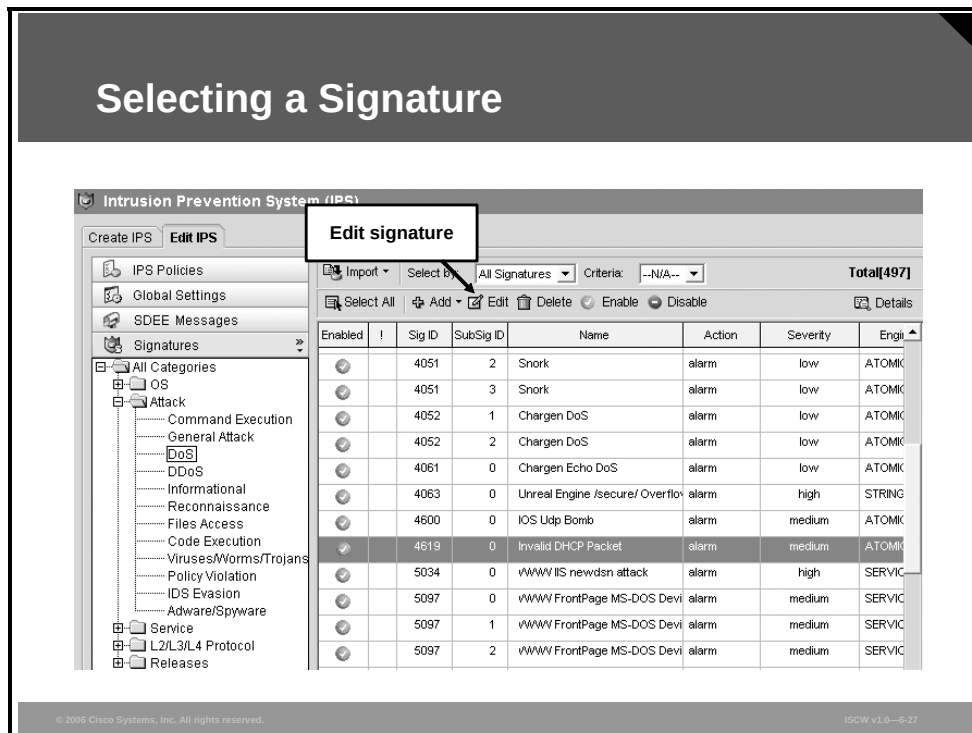
The alerts are fired by the enabled signatures included in the loaded SDF. The messages display all the details of a firing signature, such as the target and attacker IP address, alarm severity, signature ID and sub-ID, signature name, and more.

Note Although you can view all the details about a specific alert, this view is not intended to provide real-time monitoring capabilities. It has no filtering, search, or correlation functions that are necessary for a monitoring solution.

In the example, you can see that a hacker has been attempting to attack the Internet Information Server (IIS) Unicode, IIS Dot Dot Execute, and the WWW Directory Traversal against a protected system. The signatures 3215, 3216, and 5114 fired alarms with medium severity levels. Scrolling the tab would allow you to view the attacker and target IP address and other information.

Tuning Signatures

This topic describes how to tune IPS signatures using the SDM.

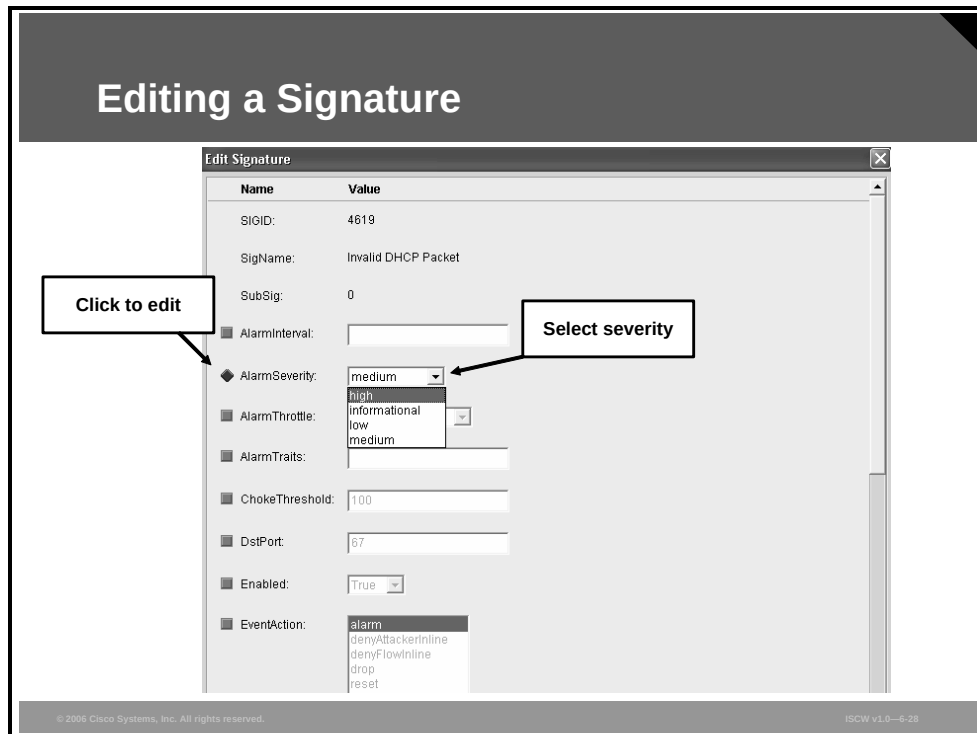


To view the parameters of a specific signature, or tune the signature settings, click **Signatures** in the middle part of the Edit IPS tab, select the appropriate signature category from the list in the middle of the window, and locate the desired signature in the right part of the window. You can also use the search options **Select by** and **Criteria** available at the top of the window to find the signature easily.

In the example, you want to view and modify the settings of the signature named *Invalid DHCP Packet* with number 4619 listed under the *Attack* category. Select the signature and click the **Edit** button to launch a signature edit window.

Editing a Signature

The SDM allows you to modify signature parameters.

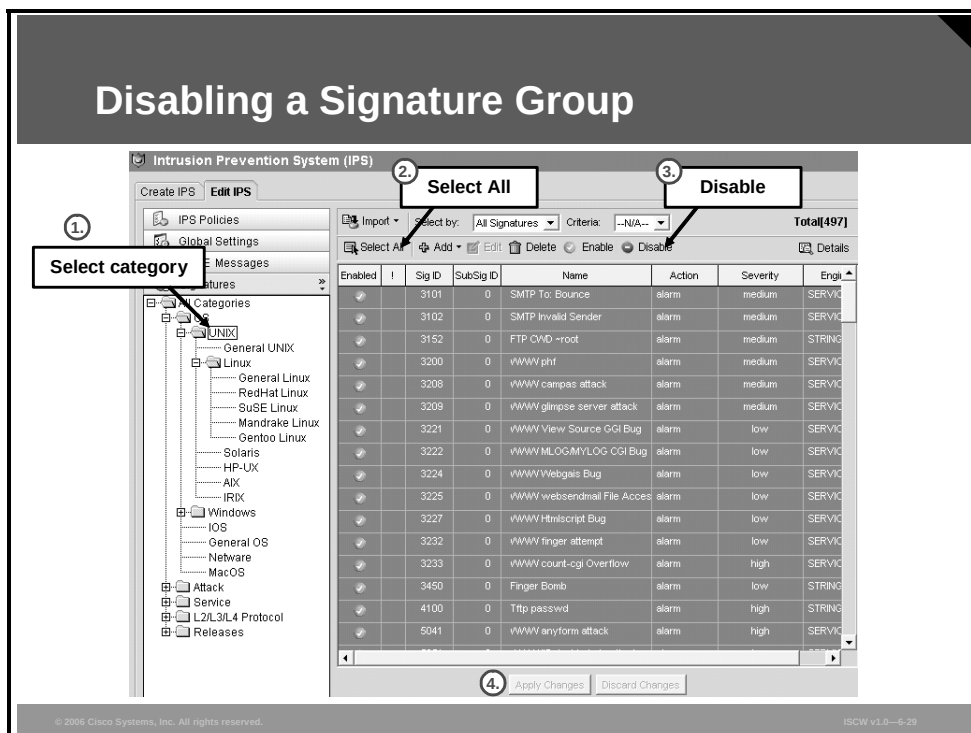


When the Edit Signature window opens, you can view the current signature settings. Select an option that you want to modify by clicking the green square next to the option. The green square turns red and you can select the desired settings from the drop-down list associated with the respective parameter.

In the example, the alarm severity is increased from the default value of *medium* to *high*. Click **OK** to apply the change to the router.

Disabling a Signature Group

SDM allows you to disable individual signatures or entire signature groups.

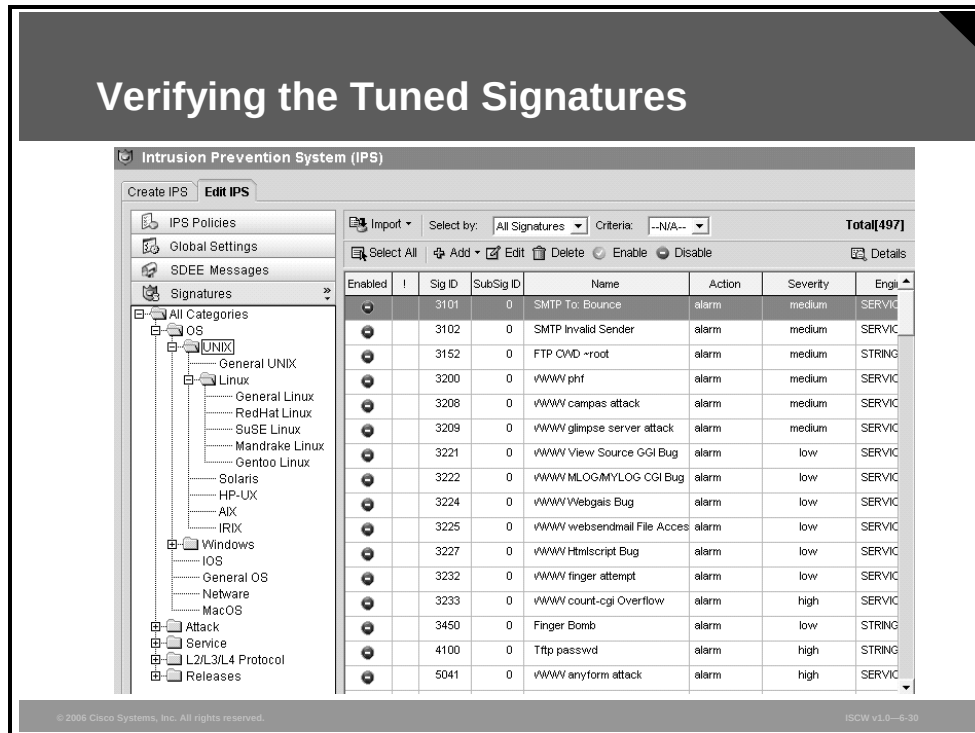


In the example, the IOS router protects a network that contains only Windows hosts. To tune the active signatures better into your environment, you decide to disable all UNIX-related signatures, as follows:

- Step 1** Select the **UNIX** sub-tree under the OS signature category.
- Step 2** Click the **Select All** button to select all signatures in the selected category.
- Step 3** Click the **Disable** button to disable all selected signatures on the IOS router.
- Step 4** Click the **Apply Changes** button to deliver the configuration to the device.

Verifying the Tuned Signatures

After you deliver the configuration to the IOS router, you can verify the current settings by viewing the signatures in the respective category.



In the example, you see that all UNIX-related signatures have in fact been disabled.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- You can configure IPS policy on a router by using the CLI or the SDM.
- CLI does not display the signature parameters.
- IPS CLI allows you to specify SDF locations, merge SDF files, disable signatures, assign rules to interfaces, and limit the detection scope using ACLs.
- SDM offers a wizard that simplifies the IPS configuration.
- IPS Policies wizard deploys default signature definitions from a specified SDF location.
- You can then use the SDM to edit the policy and modify global settings.
- SDM offers a view for SDEE messages containing status, errors, and alerts.
- You can use the SDM to tune the signature parameters.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0--6-31

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- Cisco IOS Firewall combines the stateful firewall engine with application-layer filtering for selected applications.
- Cisco IOS Firewall provides stateful support for TCP, UDP, and ICMP.
- Cisco IOS Firewall can be configured through the CLI, or the SDM, which provides the Basic and Advanced Firewall Configuration wizards for expedited deployment.
- IDS and IPS are considered complementary technologies that differ in reaction to attack, placement in the network, and signature tuning.
- Host and network IPS should be deployed in parallel to maximize the protection strength.
- Cisco IOS IPS can be configured, tuned, and monitored through the CLI or SDM, which offers a wizard for simplified provisioning.

© 2006 Cisco Systems, Inc. All rights reserved.

ISCW v1.0—6-1

This module covers the design and implementation of the Cisco IOS Firewall and Cisco IOS IPS. It describes the most common firewall technologies, such as packet filtering, stateful firewalls, and application-layer filtering. The module describes firewall topologies, showing that a Demilitarized Zone (DMZ)-based approach offers the best defense and scalability options. The concept of stateful firewalls is explained, along with its implementation on Cisco IOS routers, Cisco IOS Firewall. The module describes the two Cisco IOS Firewall configuration methods—command-line interface (CLI) and the Security Device Manager (SDM), including the Basic and Advanced Firewall Configuration wizard. Further, intrusion detection system (IDS) and intrusion prevention system (IPS) are described as complementary technologies that differ in the actions they take when an attack is detected, in the placement in the network, and in the signature coverage scope. It is recommended that both host- and network-based IPS be deployed in parallel, because the two approaches cancel out their individual weaknesses. The module describes the IOS IPS configuration methods with the CLI and the SDM, which provide a wizard for deployment simplicity.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) What is the difference between a packet filter and a stateful firewall in handling static TCP sessions? (Source: Introducing the Cisco IOS Firewall)
- A) None; the **established** keyword ensures that the packet filter permits the return traffic carrying the ACK bit while other data is dropped.
 - B) Stateful firewall is more difficult to configure.
 - C) Stateful firewall checks more than just the ACK flag; it inspects the sequence numbers to ensure the correct state of the TCP session.
 - D) Packet filter is placed differently than a stateful firewall.
- Q2) How does Cisco IOS Firewall handle ICMP traffic? (Source: Introducing the Cisco IOS Firewall)
- A) Exactly as any other stateless protocols; that is, only access lists control the packet flow.
 - B) With ICMP inspection enabled, echo replies to previously seen echo messages are permitted automatically through the router even if denied by the ACL.
 - C) Irrespectively of ICMP inspection configuration, echo replies to previously seen echo messages are permitted automatically through the router even if denied by the ACL.
 - D) Both ICMP unreachable packets and echo replies are permitted through the firewall as a response to previously seen traffic.
- Q3) Which protocol inspection should you activate on a Cisco IOS Firewall router to filter traffic to an ESMTP server? (Source: Implementing Cisco IOS Firewalls)
- A) generic TCP and ESMTP for maximum protection
 - B) generic TCP because it offers more than adequate protection
 - C) generic TCP and SMTP, because ESMTP is not supported
 - D) generic TCP, because ESMTP is not supported
- Q4) How should you tune IDS and IPS signatures that detect a data pattern, which could be a part of an attack or legitimate data? (Source: Introducing Cisco IOS IPS)
- A) both IDS and IPS should ignore such an event
 - B) IDS should send a TCP reset while IPS should alarm
 - C) both IDS and IPS should reset or block the connection
 - D) IDS should alarm while IPS should let the traffic pass, possibly generating an alarm
- Q5) Can an attacker detect the presence of an IPS sensor? (Source: Introducing Cisco IOS IPS)
- A) Yes, a sensor is a Layer 3 device and has MAC and IP addresses on all interfaces.
 - B) Yes, a sensor is Layer 2-transparent but responds to certain probes.
 - C) No, a sensor is Layer 2-transparent, like a switch, except that it inspects traffic prior to forwarding.
 - D) No, a sensor is a security-conscious Layer 3 device and does not respond to probes.

- Q6) Would you recommend the SDM as a monitoring tool for IPS events? (Source: Configuring Cisco IOS IPS)
- A) No, SDM is used only for configuration management and does not receive any events.
 - B) No, although SDM receives and displays SDEE events and alarms, it does not have the required real-time presentation, sorting, and searching capabilities.
 - C) Yes, SDM offers viewing capabilities for SDEE events and alarms.
 - D) Yes, SDM is a sufficient IPS monitoring tool for small environments with limited budget.

Module Self-Check Answer Key

Q1)	C
Q2)	B
Q3)	A
Q4)	D
Q5)	C
Q6)	B