Secur

Securing Cisco IOS Networks

Version 1.1

Student Guide

Text Part Number:

Table of Contents

1

Course Introduction

Overview

This lesson includes the following topics:

- Course objectives
- Course agenda
- Participant responsibilities
- General administration
- Graphic symbols
- Participant introductions
- Cisco Security Career Certifications
- Lab topology overview

Course Objectives

This topic introduces the course and the course objectives.

Course Objectives

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

- **Identify network security threats.**
- **Secure administrative access using Cisco Secure ACS (for MS Windows 2000) and Cisco IOS software AAA features.**
- **Protect Internet access by configuring a Cisco perimeter router.**
- **Configure Cisco IOS Firewall Context-Based Access Control.**

Course Objectives (Cont.)

- **Configure the Cisco IOS Firewall authentication proxy.**
- **Configure the Cisco IOS Firewall IDS.**
- **Use IPSec features in Cisco IOS software to create a secure site-to-site VPN using pre-shared keys and digital certificates.**
- **Use Cisco Easy VPN features to create a secure remote access VPN solution.**
- **Use the Cisco Security Device Manager to manage Cisco access routers.**
- **Use the Cisco Router Management Center to manage Cisco router VPN implementations.**

Course Agenda

Day 1
- Lesson 1—Introduction
- Lesson 2—Security Fundamentals
- Lesson 3—Basic Cisco Router Security
- Lunch
- Lesson 4—Advanced AAA Security for Cisco Router Networks

Day 2
- Lesson 5—Cisco Router Threat Mitigation
- Lunch
- Lesson 6—Cisco IOS Firewall Context-Based Access Control Configuration
- Lesson 7—Cisco IOS Firewall Authentication Proxy

SECUR 1.1—1-5

Course Agenda (Cont.)

Day 3
- Lesson 8—Cisco IOS Intrusion Detection System
- Lunch
- Lesson 9—Building IPSec VPNs Using Cisco Routers

Day 4
- Lesson 10—Building Advanced IPSec VPNs Using Cisco Routers and Certificate Authorities
- Lunch
- Lesson 11—Configuring Cisco IOS Remote Access Using Cisco Easy VPN

Day 5
- Lesson 12—Using Cisco Security Device Manager
- Lesson 13—Using Cisco Router Management Center

SECUR 1.1—1-6

Participant Responsibilities

Student responsibilities

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

SECUR 1.1—1-7

General Administration

Class-related

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

Facilities-related

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

SECUR 1.1—1-8

Graphic Symbols

IOS Router	PIX Firewall	VPN 3000	IDS Sensor	Catalyst 6500 w/ IDS Module	IOS Firewall
Network Access Server	Policy Manager	CA Server	PC	Laptop	Server Web, FTP, etc.
Hub	Modem	Ethernet Link	VPN Tunnel	Network Cloud	
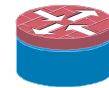
SECUR 1.1—1-9

Participant Introductions

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

SECUR 1.1—1-10

Cisco Security Career Certifications

Cisco.com

Expand Your Professional Options ——
and Advance Your Career
Cisco Certified Security Professional (CCSP) Certification

Professional-level recognition in designing and implementing Cisco security solutions

Expert

CCIE

Professional

CCSP

Associate

CCNA

Network Security

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

www.cisco.com/go/training

SECUR 1.1—1-11

Cisco Security Career Certifications

Cisco.com

Enhance Your Cisco Certifications ——
and Validate Your Areas of Expertise
Cisco Firewall, VPN, and IDS Specialists

Cisco Firewall Specialist

Required Exam	Recommended Training through Cisco Learning Partners
	Pre-requisite: Valid CCNA certification
642-501	Securing Cisco IOS Networks
642-521	Cisco Secure PIX Firewall Advanced

Cisco VPN Specialist

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

Cisco IDS Specialist

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

www.cisco.com/go/training

SECUR 1.1—1-12

Lab Topology Overview

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

Lab Visual Objective

Cisco.com

Web FTP
.50
172.26.26.0
.150
Pods 1-5   .1 .1   **Pods 6-10**
172.30.P.0   RBB   172.30.Q.0
.2   .2
Router   Router
RTS .2   .2 RTS
.100   10.0.P.0   10.0.Q.0 .100
Web   .10   .10 Web
FTP   FTP
Web/FTP   Web/FTP
CSACS   CSACS
Student PC   Student PC
10.0.P.12   10.0.Q.12

SECUR 1.1—1-14
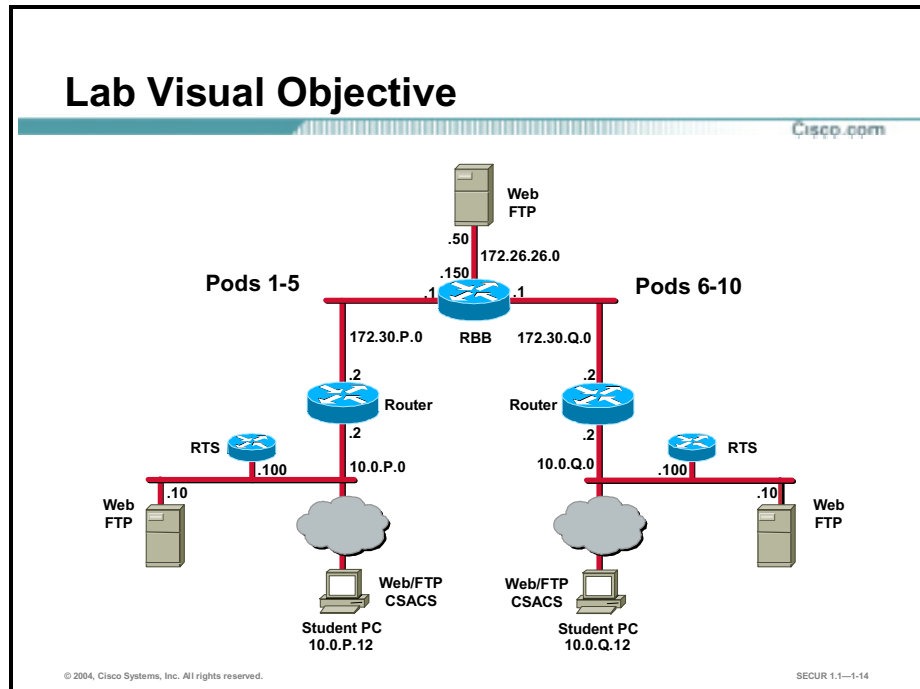
Each pair of students will be assigned a pod. In general, you will be setting up VPNs between your pod (pod P) and your assigned peer pod (pod Q).

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

2

Security Fundamentals

Overview

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

■ Objectives

■ Need for network security

■ Network security policy

■ Primary network threats and attacks

■ Reconnaissance attacks and mitigation

■ Access attacks and mitigation

■ Denial of service attacks and mitigation

■ Worm, virus, and Trojan horse attacks and mitigation

■ Management protocols and functions

■ Summary

Objectives

This topic lists the lesson's objectives.

Objectives

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

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

SECUR 1.1—2-3

Need for Network Security

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

The Closed Network

Closed network

Frame relay X.25 leased line

Remote site

Frame relay X.25 leased line

PSTN

SECUR 1.1—2-5
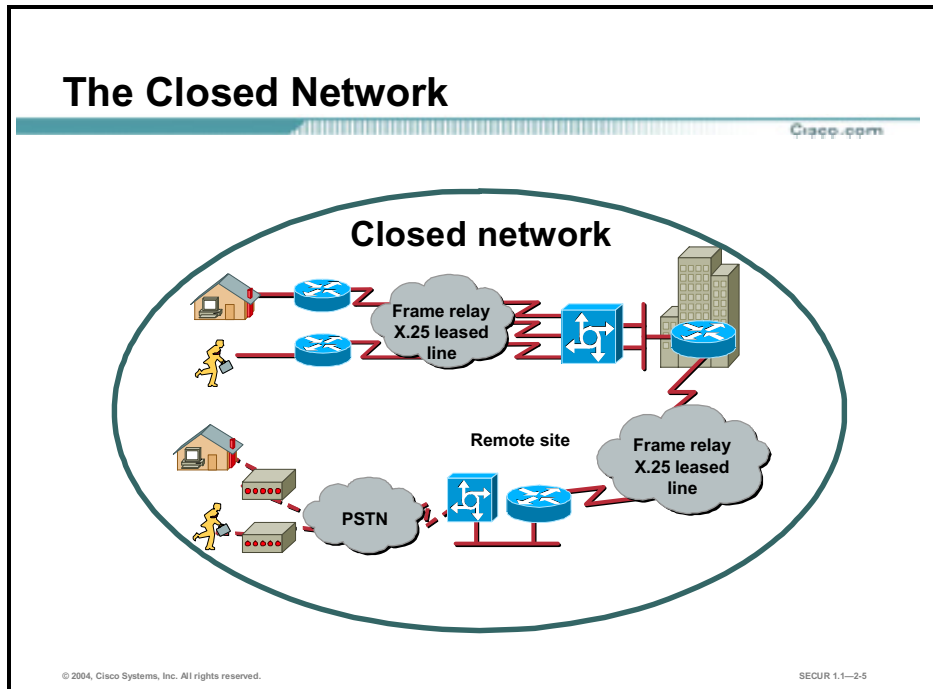
The closed network typically consists of a network designed and implemented in a corporate environment, and it provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because there was no outside connectivity.

The Network Today

Open network

Mobile and remote users

Internet-based intranet (VPN)

Internet-based intranet (VPN)

Internet-based extranet (VPN)

Remote site mobile and remote users

PSTN

Remote site

Partner site
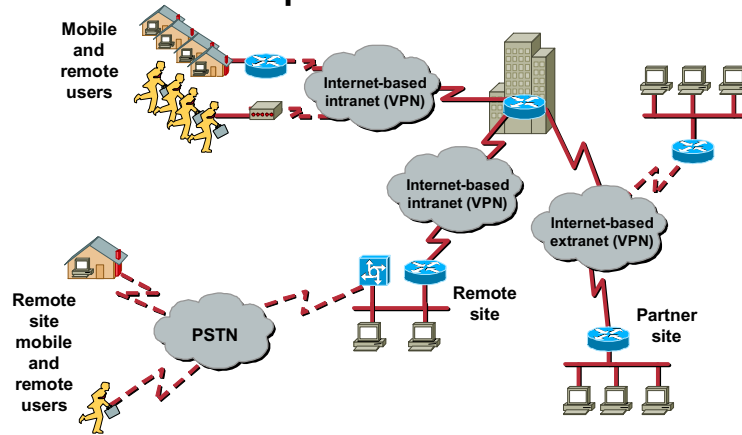
SECUR 1.1—2-6

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

Threat Capabilities—More Dangerous and Easier to Use

Cisco.com

High

Packet forging/ spoofing

Stealth diagnostics

Back doors

Scanners

Sophistication of hacker tools

Sniffers

Exploiting known vulnerabilities

Hijacking sessions

Disabling audits

Self-replicating code

Technical knowledge required

Password cracking

Password guessing

Low   1980   1990   2000
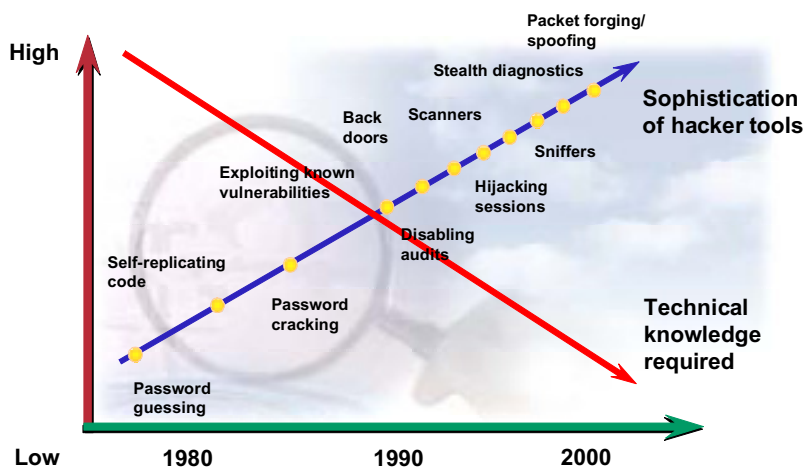
SECUR 1.1—2-7

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

The Role of Security Is Changing

Cisco.com

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

SECUR 1.1—2-8

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

Security is becoming more important because of the following:

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

■ Required for communicating and doing business safely in potentially unsafe environments— Today's business environment requires communication with many public networks and systems, which produces the need for as much security as is possible.

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

The E-Business Challenge

Cisco.com

Internet business value

E-commerce

Supply chain

Customer care

Workforce optimization

E-learning

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

Internet access

Corporate intranet

Internet presence

Expanded access, heightened security risks

SECUR 1.1—2-9

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

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

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

Legal and Governmental Policy Issues

Cisco.com

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

SECUR 1.1—2-10

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

Network Security Is a Continuous Process

Cisco.com

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

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

Secure

Manage and Improve — Corporate Security Policy — Monitor and Respond

Test
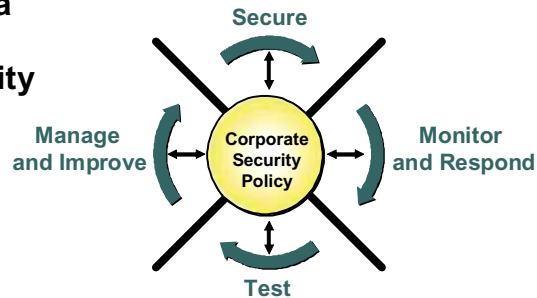
SECUR 1.1—2-11

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

■ Secure—The following are methods used to secure a network:

— Authentication

— Encryption

— Firewalls

— Vulnerability patching

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

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

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

Network Security Policy

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

What Is a Security Policy?

Cisco.com

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

– RFC 2196, Site Security Handbook

SECUR 1.1—2-13

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

Why Create a Security Policy?

- **To create a baseline of your current security posture**
- **To set the framework for security implementation**
- **To define allowed and not-allowed behaviors**
- **To help determine necessary tools and procedures**
- **To communicate consensus and define roles**
- **To define how to handle security incidents**
- **To inform users of their responsibilities**
- **To define assets and the way to use them**
- **To state the ramifications of misuse**

SECUR 1.1—2-14

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

■ Provides a process for auditing existing network security.

■ Provides a general security framework for implementing network security.

■ Defines which behavior is and is not allowed.

■ Helps determine which tools and procedures are needed for the organization.

■ Helps communicate consensus among a group of key decision makers and define responsibilities of users and administrators.

■ Defines a process for handling network security incidents.

■ Enables global security implementation and enforcement. Computer security is now an enterprise-wide issue, and computing sites are expected to conform to the network security policy.

■ Creates a basis for legal action if necessary.

What Should the Security Policy Contain?

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

SECUR 1.1—2-15

The following are some of the key policy components:

- Statement of authority and scope—This topic specifies who sponsors the security policy and what areas the policy covers.

- Acceptable use policy—This topic specifies what the company will and will not allow regarding its information infrastructure.

- Identification and authentication policy—This topic specifies what technologies, equipment, or combination of the two the company will use to ensure that only authorized individuals have access to its data.

- Internet access policy—This topic specifies what the company considers ethical and proper use of its Internet access capabilities.

- Campus access policy—This topic specifies how on-campus users will use the company's data infrastructure.

- Remote access policy—This topic specifies how remote users will access the company's data infrastructure.

- Incident handling procedure—This topic specifies how the company will create an incident response team and the procedures it will use during and after an incident.

Primary Network Threats and Attacks

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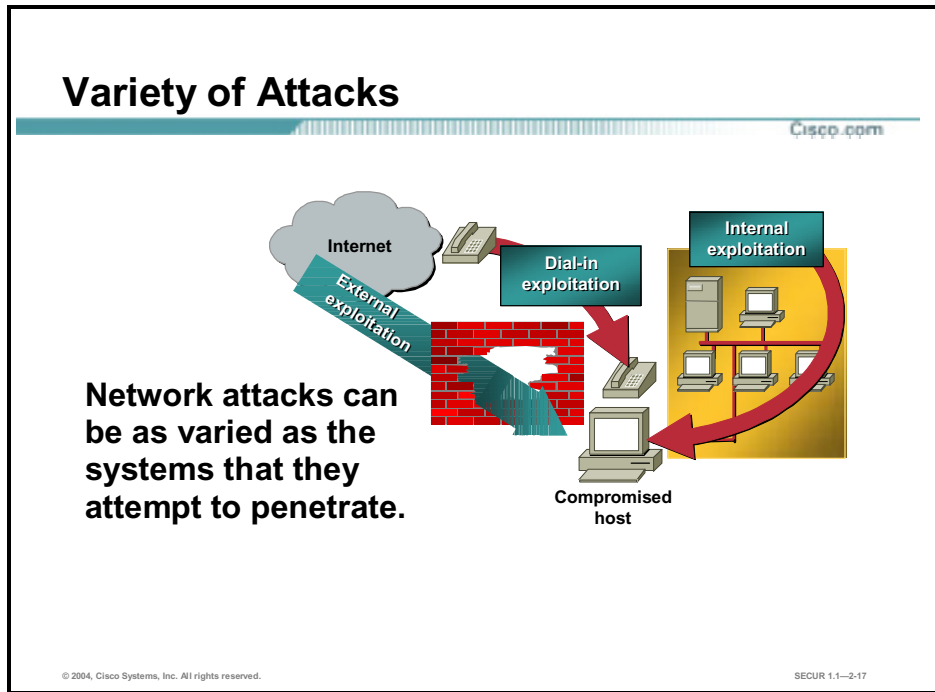
Without proper protection, any part of any network can be susceptible to attacks or unauthorized activity. Routers, switches, and hosts can all be violated by professional hackers, company competitors, or even internal employees. In fact, according to several studies, more than half of all network attacks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

There are four general threats to network security:

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

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

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

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

The Four Primary Attack Categories

Cisco.com

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

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

SECUR 1.1—2-19

There are four types of network attacks:

■ Reconnaissance attacks—An intruder attempts to discover and map systems, services, and vulnerabilities.

■ Access attacks—An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.

■ Denial of service (DoS) attacks—An intruder attacks your network in a way that damages or corrupts your computer system or denies you and others access to your networks, systems, or services.

■ Worms, viruses, and Trojan horses—Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services or access to networks, systems, or services.

Reconnaissance Attacks and Mitigation

This topic describes reconnaissance attacks and their mitigation.

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

Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, a house with an easy-to-open door or window, and so on. In many cases the intruders go as far as "rattling the door handle," not to go in immediately if it is opened, but to discover vulnerable services that they can exploit later when there is less likelihood that anyone is looking.

Reconnaissance attacks can consist of the following:

■ Packet sniffers

■ Port scans

■ Ping sweeps

■ Internet information queries

Packet Sniffers
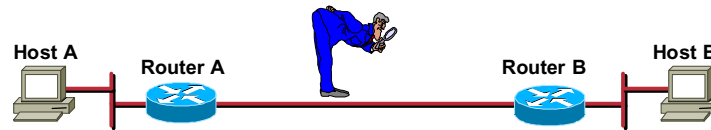
Host A   Router A   Router B   Host B

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

- Packet sniffers exploit information passed in clear text. Protocols that pass information in the clear include the following:
  - Telnet
  - FTP
  - SNMP
  - POP
  - HTTP
- Packet sniffers must be on the same collision domain.
- Packet sniffers can be general purpose or can be designed specifically for attack.

SECUR 1.1—2-22

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

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

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

Packet Sniffer Attack Mitigation

Host A   Router A   Router B   Host B

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

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

SECUR 1.1—2-23

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

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

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

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

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

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

Port Scans and Ping Sweeps
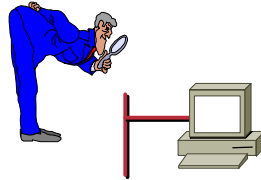
These attacks can attempt to:

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

SECUR 1.1—2-24

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

Copyright © 2004, Cisco Systems, Inc.

Port Scan and Ping Sweep Attack Mitigation

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

SECUR 1.1—2-25

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

Internet Information Queries

Cisco.com

Sample IP address query

Sample domain name query

SECUR 1.1—2-26

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

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

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

Access Attacks and Mitigation

This topic describes specific access attacks and their mitigation.

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

- Password attacks

- Trust exploitation

- Port redirection

- Man-in-the-middle attacks

Password Attacks

Cisco.com

Hackers can implement password attacks using several methods:

- Brute-force attacks
- Trojan horse programs
- IP spoofing
- Packet sniffers
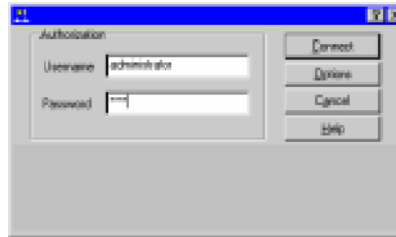
SECUR 1.1—2-29

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

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

Password Attack Example

- **L0phtCrack can take the hashes of passwords and generate the clear-text passwords from them.**
- **Passwords are computed using two methods:**
  – **Dictionary cracking**
  – **Brute-force computation**
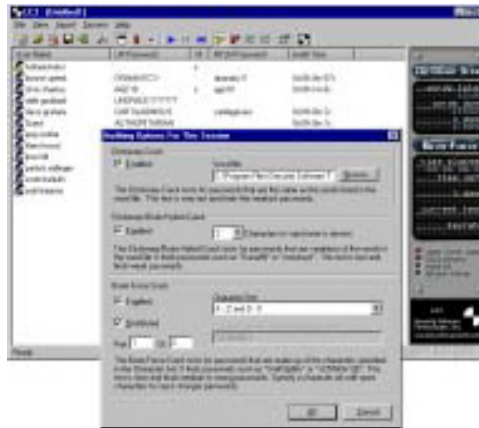
SECUR 1.1—2-30

Just 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 that compromises your network's integrity is an attacker modifying the routing tables for your network. By doing so, the attacker ensures that all network packets are routed to him or her before they are transmitted to their final destination. In such a case, an attacker can monitor all network traffic, effectively becoming a man in the middle.

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

■ Dictionary cracking—The password hashes for all of the words in a dictionary file are computed and compared against all of the password hashes for the users. This method is extremely fast and finds very simple passwords.

■ Brute-force computation—This method uses a particular character set, such as A–Z or A–Z plus 0–9, and computes the hash for every possible password made up of those characters. It will always compute the password if that password is made up of the character set you have selected to test. The downside is that time is required for completion of this type of attack.

The following are password attack mitigation techniques:

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

The following are password attack mitigation techniques:

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

- Disable accounts after a specific number of unsuccessful logins—This practice helps to prevent continuous password attempts.

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

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

Trust Exploitation

Cisco.com

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

SystemA trusts SystemB

SystemB trusts everyone

SystemA trusts everyone

SystemA
User = psmith; Pat Smith

Hacker gains access to SystemA

SystemB – Compromised by hacker
User = psmith; Pat Smith

Hacker
User = psmith; Pat Smithson
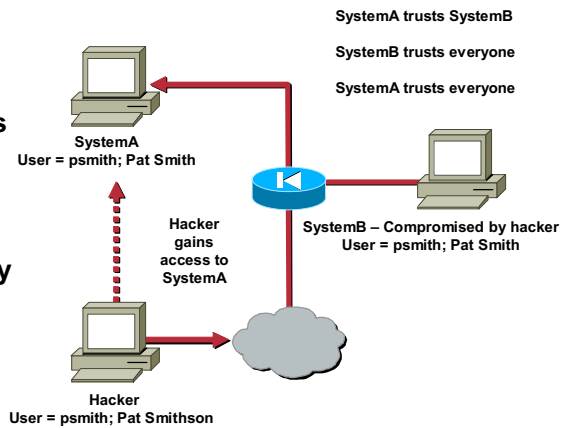
SECUR 1.1—2-32

Although it is not an attack in itself, trust exploitation refers to an individual's taking advantage of a trust relationship within a network. The classic example is a perimeter network connection from a corporation. These network segments often house DNS, Simple Mail Transfer Protocol (SMTP), and HTTP servers. Because they all reside on the same segment, a compromise of one system can lead to the compromise of other systems if those other systems in turn trust systems attached to the same network. Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, the attacker can leverage that trust relationship to attack the inside network.

Trust Exploitation Attack Mitigation

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

SystemA
User = psmith; Pat Smith

SystemB compromised by hacker User = psmith; Pat Smith

Hacker blocked

Hacker User = psmith; Pat Smithson
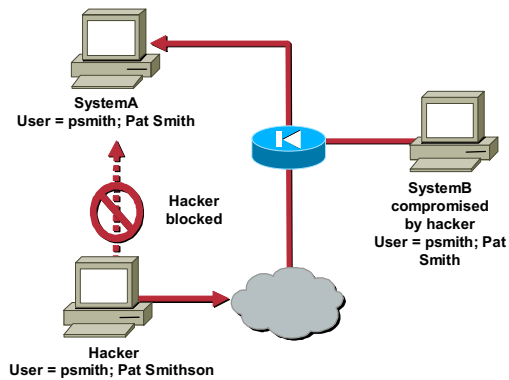
SECUR 1.1—2-33

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

Port Redirection

- Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.
- It is mitigated primarily through the use of proper trust models.
- Antivirus software and host-based IDS can help detect and prevent from a hacker installing port redirection utilities on the host.
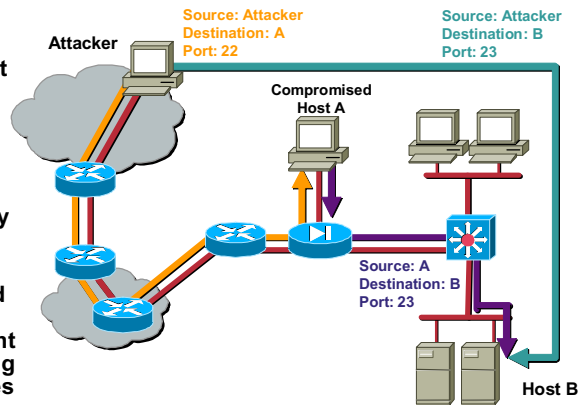
SECUR 1.1—2-34

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

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

Man-in-the-Middle Attacks

Host A   Data in clear text   Host B

Router A   Router B

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

SECUR 1.1—2-35

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

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

Man-in-the-Middle Attack Mitigation

A man-in-the-middle attack can see only cipher text

IPSec tunnel

Host A

Router A   ISP   Router B

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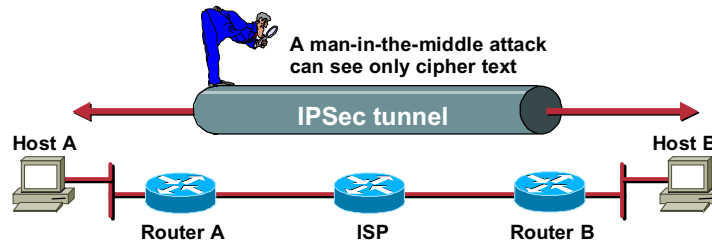
Man-in-the-middle attacks can be effectively mitigated only through the use of cryptography (encryption).

SECUR 1.1—2-36

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

Denial of Service Attacks and Mitigation

This topic describes specific DoS attacks and their mitigation.

Denial of Service Attacks

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

SECUR 1.1—2-38

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

- IP spoofing
- Distributed denial of service (DDoS)

IP Spoofing

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

SECUR 1.1—2-39

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

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

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

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

IP Spoofing Attack Mitigation

Cisco.com

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

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

SECUR 1.1—2-40

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

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

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

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

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

DoS and DDoS Attacks

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

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

SECUR 1.1—2-41

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

DDoS Example

1. Scan for systems to hack.

Client system

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

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

Handler systems

3. Agents are loaded with remote control attack software.

Agent systems

SECUR 1.1—2–42

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

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

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

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

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

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

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

Worm, Virus, and Trojan Horse Attacks and Mitigation

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

Worm, Virus, and Trojan Horse Attacks

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

- **A worm executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.**
- **A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.**
- **A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool.**

SECUR 1.1—2-45

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

- A worm executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.

- A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.

- A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool.

Worm Attacks

1. **The enabling vulnerability**
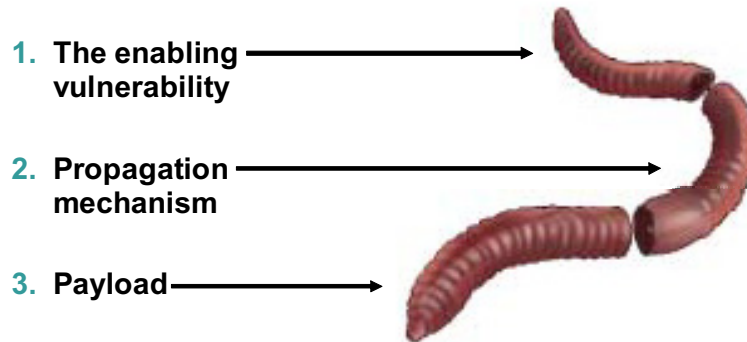
2. **Propagation mechanism**

3. **Payload**

SECUR 1.1—2-46

The anatomy of a worm attack is as follows:

■ The enabling vulnerability—A worm installs itself using an exploit vector on a vulnerable system.

■ Propagation mechanism—After gaining access to devices, a worm replicates and selects new targets.

■ Payload—Once the device is infected with a worm, the attacker has access to the host— often as a privileged user. Attackers could use a local exploit to escalate their privilege level to administrator.

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

Worm Attack Mitigation

- **Containment—Contain the spread of the worm inside your network and within your network. Compartmentize parts of your network that have not been infected.**

- **Inoculation—Start patching all systems and, if possible, scanning for vulnerable systems.**

- **Quarantine—Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.**

- **Treatment—Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.**

　　　　　　　　　　SECUR 1.1—2-47

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

- Containment
- Inoculation
- Quarantine
- Treatment

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

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

Virus and Trojan Horse Attacks

- **Viruses are malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets.**

- **A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool.**

SECUR 1.1—2-48

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

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

Virus and Trojan Horse Attack Mitigation

These kinds of applications can be contained by:

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

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

Application-Layer Attacks

Application-layer attacks have the following characteristics:

- **Exploit well-known weaknesses, such as those in protocols, that are intrinsic to an application or system (for example, sendmail, HTTP, and FTP)**

- **Often use ports that are allowed through a firewall (for example, TCP port 80 used in an attack against a web server behind a firewall)**

- **Can never be completely eliminated, because new vulnerabilities are always being discovered**

7	**Application**
6	**Presentation**
5	**Session**
4	**Transport**
3	**Network**
2	**Data link**
1	**Physical**
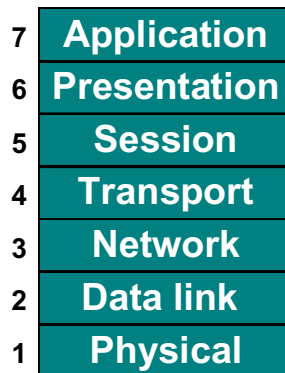
Application-layer attacks can be implemented using several different methods:

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

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

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

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

Application-Layer Attack Mitigation

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

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

SECUR 1.1—2-51

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

- Read operating system and network log files or have them analyzed—It is important to review all logs and take action accordingly.

- Subscribe to mailing lists that publicize vulnerabilities—Most application and operating system vulnerabilities are published on the Web by various sources.

- Keep your operating system and applications current with the latest patches—Always test patches and fixes in a nonproduction environment. This practice prevents downtime and keeps errors from being generated unnecessarily.

- Use IDSs to scan for known attacks, monitor and log attacks, and in some cases, prevent attacks—The use of IDSs can be essential to identifying security threats and mitigating some of those threats. In most cases, it can be done automatically.

Management Protocols and Functions

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

Configuration Management

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

SECUR 1.1—2-53

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

Configuration Management Recommendations

Cisco.com

When possible, the following practices are advised:

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

SECUR 1.1—2-54

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

Management Protocols

The following are management protocols that that can be compromised:

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

SECUR 1.1—2-55

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

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

Trivial File Transfer Protocol (TFTP) is used for transferring configuration or system files across the network. TFTP uses UDP for the data stream between the requesting host and the TFTP server.

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

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

A secure method of providing clocking for the network is for network administrators to implement their own master clocks for private networks synchronized to Coordinated Universal Time (UTC) via satellite or radio. However, clock sources are available for synchronization via

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

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

Management Protocol Recommendations

Cisco.com

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

SECUR 1.1—2-56

The following are SNMP recommendations:

■ Configure SNMP with only read-only community strings.

■ Set up access control on the device you wish to manage via SNMP to allow access by only the appropriate management hosts.

■ Use SNMP Version 3 or above.

When possible, the following practices are advised:

■ Encrypt Syslog traffic within an IPSec tunnel.

■ When allowing Syslog access from devices on the outside of a firewall, you should implement RFC 2827 filtering at the perimeter router.

■ ACLs should also be implemented on the firewall in order to allow Syslog data from only the managed devices themselves to reach the management hosts.

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

The following are NTP recommendations:

■ Implement your own master clock for private network synchronization.

■ Use NTP Version 3 or above because these versions support a cryptographic authentication mechanism between peers.

■ Use ACLs that specify which network devices are allowed to synchronize with other network devices.

Summary

This topic summarizes what you learned in this lesson.

Summary

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

SECUR 1.1—2-58

Summary (Cont.)

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

SECUR 1.1—2-59

3

Basic Cisco Router Security

This lesson presents an introduction to securing Cisco routers using proven methods for securing the physical router device, protecting the router administrative interface, and implementing AAA. In order to practice what you have learned, a hands-on lab exercise has been provided. In this lab exercise you will configure secure access for a router administrative interface.

This lesson includes the following topics:

- Objectives
- Securing Cisco router installations
- Securing Cisco router administrative access
- Introduction to AAA for Cisco routers
- Configuring AAA for Cisco routers
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- **Describe how to secure Cisco router physical installations.**
- **Secure administrative access for Cisco routers.**
- **Describe the components of a basic AAA implementation.**
- **Configure a perimeter router for AAA using a local database.**
- **Test the perimeter router AAA implementation using applicable** debug **commands.**

SECUR 1.1—3-3

Securing Cisco Router Installations

Insecure installation of network routers and switches is an often-overlooked security threat, which, if left unheeded, can have dire results. Software-based security measures alone cannot prevent pre-meditated or even accidental network damage due to poor installations. This topic discusses ways to identify and remedy insecure installations.
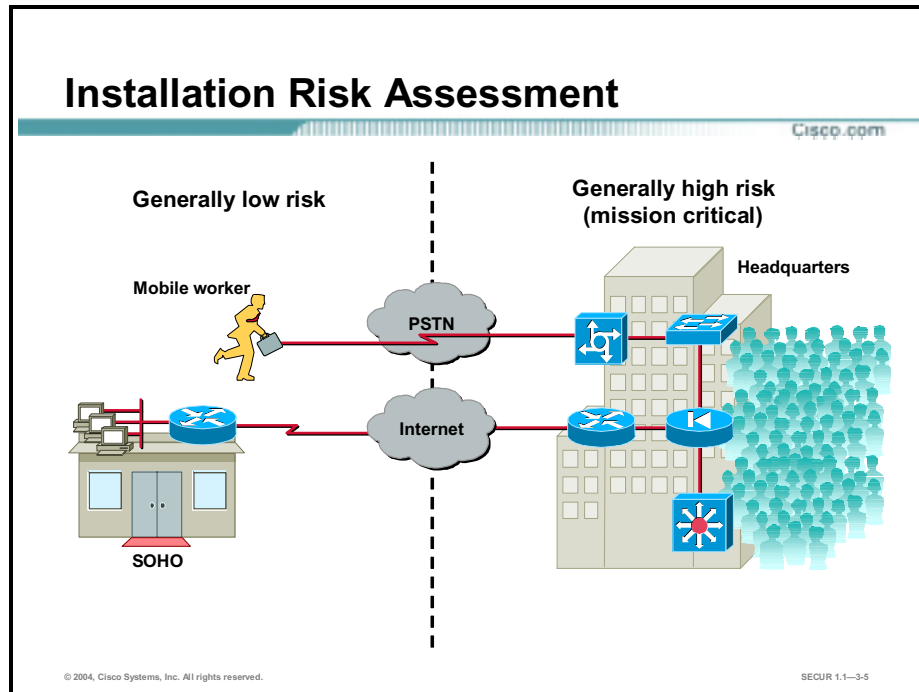
Before discussing how to secure Cisco routing and switching installations, it is important to make a distinction between low-risk and high-risk devices:

■ Low-risk devices—These devices are typically low-end or small office/home office (SOHO) devices, such as the Cisco 800/900/1700 series routers and Cisco switches that are found in environments where access to the physical devices and cabling does not present a high-risk to the corporate network. In these types of installations, it may be physically impossible and even too costly to provide a locked wiring closet for physical device security. In these situations, the IT manager must make a decision on what devices can and cannot be physically secured and at what risk.

■ High-risk (mission-critical) devices—These devices are typically found in larger offices or corporate campuses where tens, hundreds, or even thousands of employees reside, or where the same large numbers of employees remotely access corporate data. These are usually Cisco Internet routers, Catalyst switches, firewalls, and management systems used to route and control large amounts of data, voice, and video traffic. These devices represent a much higher security threat if physically accessed by disgruntled employees or impacted by negative environmental conditions.

This topic concentrates on identifying and physically securing those mission-critical devices while keeping in mind that some physical security resolutions may be easily applied to some low-risk installations as well.

Common Threats to Cisco Router and Switch Physical Installations

- **Hardware threats**
- **Environmental threats**
- **Electrical threats**
- **Maintenance threats**

Insecure installations or "physical access" threats can be generally classified as follows:

- Hardware threats—The threat of physical damage to the router or switch hardware.

- Environmental threats—Threats such as temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).

- Electrical threats—Threats such as voltage spikes, insufficient supply voltage (brown-outs), unconditioned power (noise), and total power loss.

- Maintenance threats—Threats such as poor handling of key electronic components (electrostatic discharge), lack of critical spares, poor cabling, poor labeling, and so on.

Hardware Threat Mitigation

Cisco.com

How do you plan to limit physical damage to the equipment?

• **No unauthorized access (lock it up)**
• **No access via ceiling**
• **No access via raised flooring**
• **No access via ductwork**
• **No window access**
• **Log all entry attempts (electronic log/monitor)**
• **Security cameras (recorded log)**

SECURE INTERNET ACCESS COMPUTER ROOM

AC   UPS BAY

SVRS

LAN

WAN

HELP DESK

Card Reader
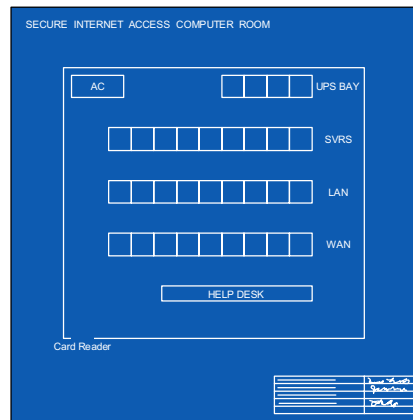
SECUR 1.1—3-7

Mission-critical Cisco routing and switching equipment should be located in wiring closets or computer or telecommunications rooms that meet the following minimum requirements:

■ Authorized personnel must lock the room with limited access only.

■ The room should not be accessible via a dropped ceiling, raised floor, window, ductwork, or point of entry other than the secured access point.

■ If possible, electronic access control should be used with all entry attempts logged by security systems and monitored by security personnel.

■ If possible, security personnel should monitor security cameras with automatic log recording.

Environmental Threat Mitigation

How do you plan to limit environmental damage to the equipment?

- **Temperature control**
- **Humidity control**
- **Positive air flow**
- **Remote environmental alarming and recording and monitoring**

SECUR 1.1—3-8

The following items should be used to limit environmental damage to Cisco router and switching devices:

■ The room must be supplied with dependable systems for temperature and humidity control. Always verify the recommended environmental parameters of the Cisco routing and switching equipment with the supplied product documentation.

■ If possible, the room environmental parameters should be remotely monitored and alarmed.

■ The room must be free from electrostatic and magnetic interferences.

Electrical Threat Mitigation

Cisco.com

How do you plan to limit electrical supply problems?

- **Install UPS systems.**
- **Install generator sets.**
- **Follow a preventative maintenance plan.**
- **Install redundant power supplies.**
- **Perform remote alarming and monitoring.**

SECUR 1.1—3-9

Electrical supply problems can be limited by adhering to the following:

- Install uninterrupted power supply (UPS) systems for mission-critical Cisco routing and switching devices.

- Install backup generator systems for mission-critical supplies.

- Plan for and initiate regular UPS or generator testing and maintenance procedures based on the manufacturer's suggested preventative maintenance schedule.

- Use filtered power.

- Install redundant power supplies on critical devices.

- Monitor and alarm power-related parameters at the supply and device level.

Maintenance-Related Threat Mitigation

Cisco.com

How do you plan to limit maintenance-related threats?

- **Use neat cable runs.**
- **Label critical cables and components.**
- **Use ESD procedures.**
- **Stock critical spares.**
- **Control access to console ports.**

SECUR 1.1—3-10
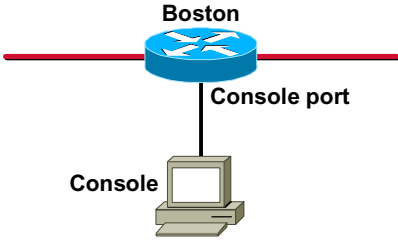
Maintenance-related threats are a broad category that covers many items. The following general rules should be adhered to in order to prevent these types of threats:

■ All equipment cabling should be clearly labeled and secured to equipment racks to prevent accidental damage or disconnection, or incorrect termination.

■ Cable runs, raceways, or both should be used to traverse rack-to-ceiling or rack-to-rack connections.

■ Always follow electrostatic discharge (ESD) procedures when replacing or working inside Cisco router and switch devices.

■ Maintain a stock of critical spares for emergency use.

■ Do not leave a console connected to and logged into any console port. Always log off administrative interfaces when leaving.

■ Always remember that no room is ever totally secure and should not be relied upon to be the sole protector of device access. Once inside a secure room, there is nothing to stop an intruder from connecting a terminal to the console port of a Cisco router or switch.

Securing Cisco Router Administrative Access

This topic describes how to configure secure administrative access to Cisco routers. Configuring secure administrative access is an extremely important security task. If an unauthorized person were to gain administrative access to a router, the person could alter routing parameters, disable routing functions, or discover and gain access to other systems in the network.

Connect to Router Console Port

Boston

Console port

Console

- **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.**

SECUR 1.1—3-12

One way to perform initial router configuration tasks is to access the router console port with a console. A console is a terminal that is connected to a router console port; it can either be a dumb terminal or a PC running terminal emulation software. Consoles are only one way that network administrators obtain administrative access to configure and manage routers. Other ways to gain administrative access include Telnet, HTTP/HTTPS, SSH, Simple Network Management Protocol (SNMP), and the Cisco Security Device Manager (SDM) feature.

The first step in securing Cisco router administrative access is to configure secure system passwords. These passwords are either stored in the router itself (local) or on remote Authentication, Authorization, and Accounting (AAA) servers, such as the Cisco Secure Access Control Server (ACS). This topic contains information on configuring local passwords only. Password authentication using AAA will be discussed later in this course.

Password Creation Rules

The following list of rules should be used when creating passwords for Cisco routers:

- **Passwords must be anywhere from 1 to 25 characters in length and include the following:**
  - **Alphanumeric characters**
  - **Upper-case characters, lower-case characters, or both**
- **Passwords cannot have a number as the first character.**
- **Password-leading spaces are ignored, but any and all spaces after the first character are not ignored.**
- **Change passwords often.**

SECUR 1.1—3-13

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

■ Passwords must be anywhere from 1 to 25 characters in length. It is highly recommended that you always use passwords containing 10 or more characters. Passwords may include the following:

— Any alphanumeric characters

— Uppercase characters, lowercase characters, or both

■ Passwords cannot have a number as the first character.

■ Passwords should not utilize dictionary words.

■ Password-leading spaces are ignored, but all spaces after the first character are not ignored.

■ You should decide when and how often the passwords should be changed.

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

Initial Configuration Dialog

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no] y

Configuring global parameters:

   Enter host name [Router]: Boston

   The enable secret is a password used to protect access to
   privileged EXEC and configuration modes. This password, after
   entered, becomes encrypted in the configuration.
   Enter enable secret: CantGessMe

   The enable password is used when you do not specify an enable
   secret password, with some older software versions, and some boot
   images.
   Enter enable password: WontGessMe

   The virtual terminal password is used to protect access to the
   router over a network interface.
   Enter virtual terminal password: CantGessMeVTY
                  .
                  .
```

SECUR 1.1—3-14

If you are working on a new router (from the factory) or an existing router that has been reset (possibly using the Cisco password recovery procedure), you will be prompted by the Cisco IOS command line interface (CLI) if you want to enter the initial configuration dialog, as shown in the figure.

Within the first few questions of the initial configuration dialog can be found several Cisco router password requirements:

■   What will be this router's enable secret password?

■   What will be this router's enable password?

■   What will be the password used to access the router using virtual terminal (Telnet)?

The enable secret password is used to enter enable mode (sometimes referred to as privileged 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 password is always encrypted inside the router configuration using a Message Digest 5 (MD5) hashing algorithm.

The enable password 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 even though enable secret password is a safer way to store privileged-EXEC passwords. The thinking was that if you downgraded the router to a version of Cisco IOS that did not support enable secret password, you would still have the enable password protecting the privileged-EXEC.

The virtual terminal password is the line-level password entered when connecting to the router using Telnet. You can set this password during the initial configuration dialog (as shown in the figure) or by using the **password** command in vty line configuration mode.

Password Minimum Length Enforcement

router(config)#

```
security passwords min-length length
```
- Sets the minimum length of all Cisco IOS passwords
- Minimum length of ten characters highly recommended

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

Cisco IOS Software Release 12.3(1) and greater allow administrators to set the minimum character length for all router passwords using the **security passwords** global configuration command, as shown in the figure. This command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating 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).

The syntax for the **security passwords** command is as follows:

security passwords min-length *length*

length	Minimum length of a configured password (choose a length from 0–16). A minimum length of 10 characters is recommended.

Note:	It is highly recommended that you set your minimum password length to at least 10 characters. Never use a length of 0.

After this command is enabled, any attempt to create a new password that is less than the specified length will fail. Any attempt to create a smaller password will result in an error message like the one shown here:

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

Configure the Enable Password Using enable secret

router(config)#

```
enable secret password
```

- **Hashes the password in the router configuration file**
- **Uses a strong hashing algorithm based on MD5**

```
Boston(config)# enable secret Curium96
```

```
Boston# show running-config
!
hostname Boston
!
no logging console
enable secret 5 $1$ptCj$vRErS/tehv53JjaqFMzBT/
!
```

SECUR 1.1—3-16

If you did not use the initial configuration dialog to configure your enable secret password, you must use the **enable secret** command in global configuration mode. The **enable secret** command uses a one-way encryption hash based on MD5 (designated by the number 5 in the figure) and is considered irreversible by most cryptographers. That being said, it should be noted that even this type of encryption is still vulnerable to brute force or dictionary attacks.

Use the **enable secret** command in global configuration mode, as shown in the figure.

The syntax for the **enable secret** command is as follows:

enable secret *password*

Note:	If you forget the enable secret password, you have no alternative but to replace it using the Cisco router password recovery procedure.

Configure the Console Port Line-Level Password

router(config)#

```
line console 0
```

- **Enters console line configuration mode**

router(config-line)#

```
login
```

- **Enables password checking at login**

router(config-line)#

```
password password
```

- **Sets the line-level password to password**

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

- **Creates the line-level password "ConUser1"**
- **The password is displayed in clear text**

SECUR 1.1—3-17

By default, the console port does not require a password for console administrative access.

Note:	By default, 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 described later in this lesson.

Always configure a console port line-level password. Complete the following steps to create a new line-level password for the console line from global configuration mode:

Step 1 Enter console 0 line configuration mode:

Boston(config)# **line console 0**

Step 2 Enable password checking on login:

Boston(config-line)# **login**

Step 3 Enter the new console line-level password (in this example "ConUser1"):

Boston(config-line)# **password ConUser1**

If you were to view the router configuration using the **show run** command, you would see the following for the console line configuration:

line con 0

login

password ConUser1

Notice that the password is seen in clear text (unencrypted). Passwords left in clear text pose a serious threat to router security.

Configure a VTY Line-Level Password

router(config)#

```
line vty start-line-number end-line-number
```

- **Enters VTY line configuration mode**
- **Specifies the range of VTY lines to configure**

router(config-line)#

```
login
```

- **Enables password checking at login for VTY (Telnet) sessions**

router(config-line)#

```
password password
```

- **Sets the line-level password to password**

```
Boston(config)# line vty 0 4
Boston(config-line)# login
Boston(config-line)# password CantGessMeVTY
```

Cisco routers support multiple Telnet sessions (up to five simultaneous sessions by default—more can be added) each serviced by a logical VTY line. By default, Cisco routers do not have any line-level passwords configured for these VTY lines. If you enable password checking, you must also configure a VTY line-level password before attempting to access the router using Telnet. If you fail to configure a VTY line-level password, and password checking is enabled for VTY lines, you will encounter an error message similar to the following:

```
Telnet 10.0.1.2
Trying…
Connected to 10.0.1.2.
Escape character is '^]'.
Password required, but none set
Connection closed by remote host.
```

There are two ways to configure a line-level VTY password; the first way is to enter the password during the initial configuration dialog (virtual terminal password), the second way is by using the **password** command in VTY line configuration mode, as shown in the figure. Always configure passwords for all of the VTY ports in this manner.

Note: An enable password must also be configured if Telnet is to gain access to the privileged-EXEC (enable) mode of the router. Use either the **enable *password*** or **enable secret *password*** command to set the enable password for your routers.

In the example shown in the figure, VTY lines 0−4 (logical VTY lines 1−5) are configured simultaneously to look for the password specified. Just like console line-level passwords, VTY passwords are, by default, shown as clear text (unencrypted) in the router configuration.

The following are a few more things to keep in mind 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 to only specified systems by building a simple access control list (ACL) that does the following (ACLs are covered in-depth later in this course):

— Allows Telnet access from specific hosts only (allows certain IP addresses)

— Blocks Telnet access from specific untrusted hosts (disallows certain IP addresses)

— Ties the ACL to the VTY lines using the **access-class** command

— The following is an example showing ACL 30 restricting Telnet access to host 10.0.1.1 and denying access from host 10.0.1.2 for VTY lines 0–4:

```
Boston(config)# access-list 30 permit 10.0.1.1
Boston(config)# access-list 30 deny 10.0.1.2
Boston(config)# line vty 0 4
Boston(config-line)# access-class 30 in
```

■ Make sure that you 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 0–4 lines.

Configure an Auxiliary Line-Level Password

Cisco.com

router(config)#

```
line aux 0
```

- **Enters auxiliary line configuration mode**

router(config-line)#

```
login
```

- **Enables password checking at login for auxiliary line connections**

router(config-line)#

```
password password
```

- **Sets the line-level password to password**

```
Boston(config)# line aux 0
Boston(config-line)# login
Boston(config-line)# password NeverGessMeAux
```

SECUR 1.1—3-19

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

Unlike console and VTY line-level 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, as shown in the figure.

Note:	If you wish to prevent someone from accessing privileged-EXEC from an auxiliary 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 following example shows other important commands used when configuring an auxiliary port.

Step 1   Permit incoming and outgoing modem calls on this line.

```
Boston(config)# line aux 0
Boston(config-line)# modem inout
```

Step 2   Specify the line speed that should be used to communicate with the modem.

```
Boston(config-line)# speed 9600
```

Step 3   Allow all protocols to use the line.

```
Boston(config-line)# transport input all
```

Step 4   Enable RTS/CTS flow control.

```
Boston(config-line)# flowcontrol hardware
```

Step 5   Authenticate incoming connections using the password configured on the line (the password is configured in step 6).

```
Boston(config-line)# login
% Login disabled on line 65, until 'password' is set
```

Step 6   Configure a password to authenticate incoming calls on this line.

```
Boston(config-line)# password NeverGessMeAux
```

For more information on configuring router auxiliary ports, see Cisco.com. Just like console and VTY line-level passwords, auxiliary passwords are not encrypted in the router configuration. This is why it is important to use the **service password-encryption** command, which is covered next.

With the exception of the enable secret password, all Cisco router passwords are by default stored in clear text form within the router configuration. These passwords can be clearly seen by performing a **show running-config** command. Sniffers can also see them if your TFTP server configuration files traverse an unsecured intranet or Internet connection. If an intruder were to gain access to the TFTP server where the router configuration files are stored, the intruder would be able to obtain these passwords.

The **service password-encryption** command encrypts all passwords (except the previously encrypted enable secret password) in the router configuration file using a proprietary Cisco algorithm based on a Vigenere cipher (indicated by the number **7** when viewing the configuration). This method is not as safe as MD5, which is used with the enable secret password command, but it will prevent casual discovery of the router's 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 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. Securing this connection is discussed later in this lesson.

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

The syntax for the **service password-encryption** command is as follows:

service password-encryption

There are no arguments for this command.

Enhanced Username Password Security

router(config)#

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

- **Uses MD5 hashing for better username password security**
- **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
   $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

SECUR 1.1—3-21

Starting with Cisco IOS Software Release 12.0(18)S, system administrators can choose to use an MD5 hashing mechanism to encrypt username passwords. MD5 hashing of passwords is a much better 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.

MD5 hashing of Cisco IOS username passwords is accomplished using the **username secret** command in global configuration mode, as shown in the figure. Administrators can choose to enter a clear text password for MD5 hashing by the router (option **0**), or they can enter a previously encrypted MD5 secret (option **5**).

The syntax for the **username secret** command is as follows:

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

name	The username.
0	(Optional.) Indicates that the following clear text *password* is to be hashed using MD5.
password	Clear text password to be hashed using MD5.
5	Indicates that the following *encrypted-secret* password was hashed using MD5.
encrypted-secret	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; thus, you cannot use MD5 encryption with protocols that require clear text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

Securing ROMMON with *no service password-recovery*

router(config)#

```
no service password-recovery
```

- **By default, Cisco routers are factory configured with** *service password-recovery* **set.**
- **The** no **version 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)#
```

SECUR 1.1—3-22

By default, Cisco IOS routers allow a break sequence during power up, forcing the router into 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 in that anyone who gains physical access to the router console port can enter ROMMON, reset the enable secret password, and discover the router configuration.

This potential security breach can be mitigated using the **no service password-recovery** global configuration command, as shown in the figure.

Note: The **no service password-recovery** command is a hidden Cisco IOS command.

The syntax for the **no service password-recovery** command is as follows:

no service password-recovery

This command has no arguments or keywords.

Caution: If a router is configured with **no service password-recovery**, all access to the ROMMON is disabled. If the router's 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 the following:

```
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** 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
```

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
```

SECUR 1.1—3-23

Starting with Cisco IOS Software Release 12.3(1), system administrators can configure the number of allowable unsuccessful login attempts using the **security authentication failure rate** global configuration command, as shown in the figure.

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.

Once the 15-second delay has passed, the user may continue to attempt to login to the router.

The syntax for the **security authentication failure rate** command is as follows:

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

threshold-rate	Number of allowable unsuccessful login attempts. The default is 10 (range: 2–1024).

Note:	The **log** keyword is required. This command must result in a generated Syslog event.

Setting Timeouts for Router Lines

Cisco.com

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

```
exec-timeout minutes [seconds]
```

- **Default is 10 minutes**
- **Terminates an unattended console 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/auxiliary connection after 3 minutes and 30 seconds**

SECUR 1.1—3-24

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 to three minutes maximum.

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

The syntax for the **exec-timeout** command is as follows:

exec-timeout *minutes* [*seconds*]

minutes	Integer that specifies the number of minutes.
seconds	(Optional.) Additional time interval in seconds.

Setting Multiple Privilege Levels

router(config)#

```
privilege mode {level level command | reset
  command}
```

- Level 1 is predefined for user-level access privileges.
- Levels 2–14 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
```

SECUR 1.1—3-25

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 2–14). The 16 levels (numbered 0–15) are designated as shown in the figure.

Privileges are assigned to levels 2–14 using the **privilege** command from global configuration mode, as shown in the figure.

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

privilege *mode* {**level** *level command* | **reset** *command*}

mode	Specifies the configuration mode. See the list after this table for options for this argument.
level	(Optional.) Enables setting a privilege level with a specified command.
level	(Optional.) The privilege level associated with a command. You can specify up to 16 privilege levels, using numbers 0 through 15.
command	(Optional.) Command to which the privilege level is associated.
reset	(Optional.) Resets the privilege level of a command.
command	(Optional.) The command for which you want to reset the privilege level.

The following list contains all the router configuration modes that can be configured using the **privilege** command:

- *accept-dialin*—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
- *dhcp*—DHCP pool configuration mode
- *dspfarm*—DSP farm configuration mode
- *exec*—Exec mode
- *flow-cache*—Flow aggregation cache configuration mode
- *interface*—Interface configuration mode
- *interface-dlci*—Frame Relay DLCI configuration mode
- *ip-vrf*—Configure IP VRF parameters
- *line*—Line configuration mode
- *map-class*—Map class configuration mode
- *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
- *tdm-conn*—TDM connection configuration mode
- *vc-class*—VC class configuration mode
- *vpdn-group*—VPDN group configuration mode
- *rsvp_policy_local*
- *alps-ascu*—ALPS ASCU configuration mode
- *alps-circuit*—ALPS circuit configuration mode
- *config-rtr-http*—RTR HTTP raw request Configuration
- *crypto-map*—Crypto map config mode
- *crypto-transform*—Crypto transform config modeCrypto transform configuration mode

- *gateway*—Gateway configuration mode
- *ipenacl*—IP named extended access-list configuration mode
- *ipsnacl*—IP named simple access-list configuration mode
- *lane*—ATM LAN Emulation Lecs Configuration Table
- *mpoa-client*—MPOA Client
- *mpoa-server*—MPOA Server
- *rtr*—RTR Entry Configuration
- *sg-radius*—RADIUS server group definition
- *sg-tacacs+*—Terminal Access Controller Access Control System Plus (TACACS+) server group
- *sip-ua*—SIP UA configuration mode
- *subscriber-policy*—Subscriber policy configuration mode
- *tcl*—Tcl mode
- *template*—Template configuration mode
- *translation-rule*—Translation Rule configuration mode
- *voiceclass*—Voice Class configuration mode
- *voiceport*—Voice configuration mode
- *voipdialpeer*—Dial Peer configuration mode

Configuring Banner Messages

router(config)#

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

- **Specify what is "proper use" of the system**
- **Specify that the system is being monitored**
- **Specify that privacy should not be expected when using this system**
- **Do not use the word "welcome"**
- **Have legal department review the content of the message**

```
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. %
```

SECUR 1.1—3-26

Banner messages should be used to warn would-be intruders that they are not welcome on your network. Banners are very 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. The banner command is comprised of five distinct commands:

- **banner exec**—Specifies and enables a message to be displayed when an EXEC process is created on the router (an EXEC banner)

- **banner incoming**—Specifies and enables a banner to be displayed when there is an incoming connection to a terminal line from a host on the network

- **banner login**—Specifies and enables a customized banner to be displayed before the username and password login prompts

- **banner motd**—Specifies and enables a message-of-the-day (MOTD) banner

- **banner slip-ppp**—Specifies and enables a banner to be displayed when a Serial Line Interface Protocol (SLIP) or PPP connection is made

Use the **banner** command from global configuration mode to specify appropriate messages, as shown in the figure.

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

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

`d`	Delimiting character of your choice (for example, a pound sign [#]. You cannot use the delimiting character in the banner message.
`message`	— Message text. You can include tokens in the form $(*token*) in the message text. Tokens will be replaced with the corresponding configuration variable.

The following list contains valid tokens for use within 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

Introduction to AAA for Cisco Routers

This topic introduces you to the concept of authentication, authorization, and accounting (AAA) services for authenticating router administrators and users who wish to access the corporate LAN through dial-in or Internet connections.

AAA services provide higher degrees of scalability than the line-level and privileged-EXEC authentication you have learned so far.

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.

AAA Model—Network Security Architecture

- **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."**
- **Accounting**
  - **What did you do? How long did you do it? How often did you do it?**
  - **"User *student* accessed host *serverXYZ* using Telnet for 15 minutes."**

SECUR 1.1—3-28

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, using a username and password, challenge and response, token cards, and other methods: "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."

■ 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 Cisco AAA

Cisco.com

Remote client (Dialup client)

PSTN/ISDN

NAS

Cisco Secure ACS for Windows Server

Console

Corporate file server

Remote client (VPN Client)

Internet

Router

Cisco Secure ACS Solution Engine
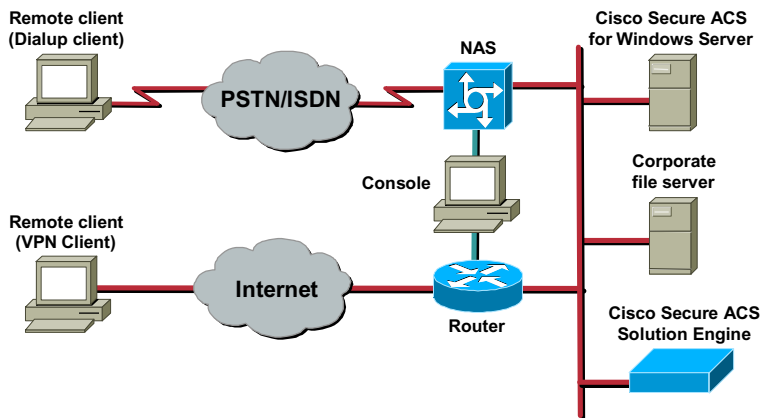
• **Administrative access—console, Telnet, and aux access**
• **Remote user network access—Dialup or VPN access**

SECUR 1.1—3-29

Cisco networking products support AAA access control using line passwords, a local security database, or remote security server databases. A local security database is configured in the router for a small group of network users. A remote security database is a separate server running a AAA security protocol, providing AAA services for multiple network devices and large numbers of network users.

Cisco provides several 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/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 ACS for Windows Server 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.

Implementing Authentication Using Local Services

Cisco.com

Remote client

Perimeter router
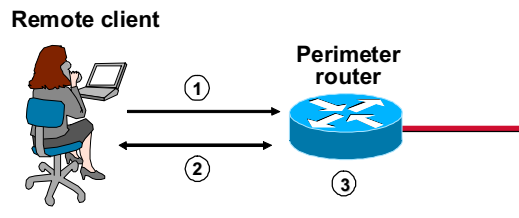
1. The client establishes connection with the router.
2. The router prompts the user for a username and password.
3. The router authenticates the username and password in the local database. The user is authorized to access the network based on information in the local database.

SECUR 1.1—3-30

If you have one or two NASs or routers providing access to your network for a limited number of users, you may store username and password security information locally on the Cisco NASs or routers. This is referred to as local authentication on a local security database. Local authentication characteristics are as follows:

- Used for small networks
- Username and password are stored in the Cisco router
- User authenticates against the local security database in the Cisco router
- Does not require an external database

The system administrator must populate the local security database by specifying username profiles for each user that might log in.

Local authentication typically works as shown in the figure.

Implementing Authentication Using External Servers
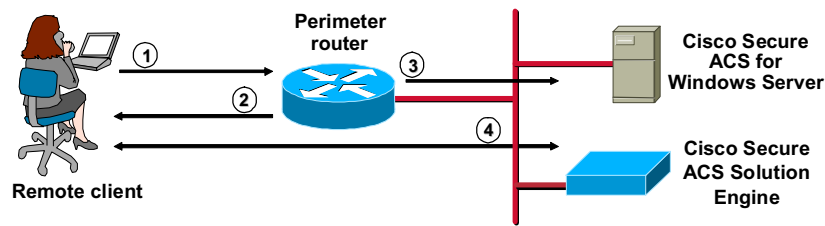
1. The client establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access) or the network based on information found in the Cisco Secure ACS database.

SECUR 1.1—3-31

The problem with local implementations of AAA is that it does not scale well. Most corporate environments have multiple Cisco routers and NASs with multiple router administrators and hundreds or thousands of users vying for access to the corporate LAN. Maintaining local databases for each Cisco router and NAS for this size network is just not feasible.

One or more Cisco Secure ACS systems (server or engine) can manage all of the user and administrative access needs for an entire corporate network using one or more databases.

External AAA systems, such as the Cisco Secure ACS for Windows Server or Cisco Secure ACS Solution Engine, communicate with Cisco routers and NASs using AAA protocols. These protocols are discussed next.

The TACACS+ and RADIUS AAA Protocols

Cisco.com

Security server

Cisco Secure ACS

- Two different protocols are used to communicate between the AAA security servers and authenticating devices.
- Cisco Secure ACS supports both TACACS+ and RADIUS:
  - TACACS+ remains more secure than RADIUS.
  - RADIUS has a robust API and strong accounting.

TACACS+   **RADIUS**

Firewall   **Router**   **Network access server**
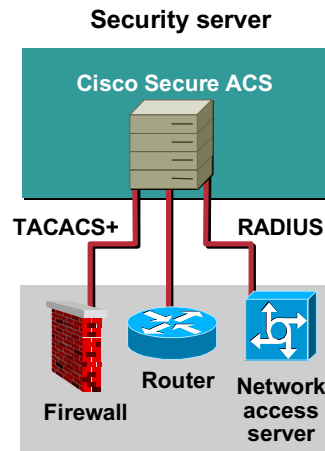
SECUR 1.1—3-32

TACACS+ and Remote Access Dial-In User Service (RADIUS) are the two predominant security server protocols used for AAA with Cisco firewalls, routers, and NAS. Cisco developed the Cisco Secure ACS family of AAA servers to support both TACACS+ and RADIUS.

The Cisco Secure ACS family is a comprehensive and flexible platform for securing access to the network. Cisco Secure ACS secures network access for the following:

- Dialup access via Cisco access servers and routers

- Router and switch console, auxiliary, and vty port administrative and network access

- Cisco PIX Firewall access

- Cisco Virtual Private Network (VPN) 3000 Series Concentrators (RADIUS only)

Cisco Secure ACS works closely with the NAS, router, VPN 3000 Concentrator, and PIX Firewall to implement a comprehensive security policy via the AAA architecture. It also works with industry-leading token cards and servers.

The Cisco Secure ACS for Windows Server is easily managed via standard browsers, enabling simple moves, adds, and changes to usernames, passwords, and network devices. It is implemented on Microsoft Windows 2000 Server platforms.

The Cisco Secure ACS Solution Engine performs many of the same functions as the Cisco Secure ACS for Windows Server products, but in a single rack-unit (RU) mounted, dedicated hardware platform.

You will learn more about using these remote AAA alternatives in a later lesson.

Authentication Methods and Ease of Use

Strong

Token cards or soft tokens using OTPs

S/Key (OTP for terminal login)

Username and password (aging)

Username and password (static)

No username or password

Weak

Low   Ease of use   High
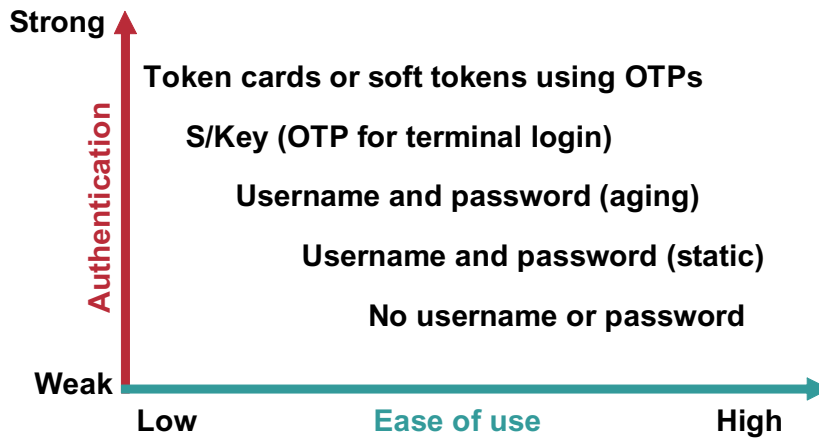
© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—3-33

The most common user authentication method is the use of usernames and passwords. Username and password methods range from weak to strong in authentication security. Simple authentication methods use a database of usernames and passwords, while methods that are more complex use one-time passwords (OTPs). Consider each of the methods listed in the figure from the bottom of the list up:

■ No username or password—Some system administrators and users decide not to use the username and password capabilities of their access devices. This is the least secure option. A network intruder only has to discover the access method to gain access to the networked system.

■ Username and password (static)—Stays the same until changed by the system administrator or user. Susceptible to playback attacks, eavesdropping, theft, and password cracking programs.

■ Username and password (aging)—Expires after a set time (usually 30 to 60 days) and must be reset, usually by the user, before network access is granted. Susceptible to playback attacks, eavesdropping, theft, and password cracking, but to a lesser degree than static username and password pairs.

■ OTPs—A stronger method, providing the most secure username and password authentication. Most OTP systems are based on a "secret pass-phrase," which is used to generate a list of passwords. They are only good for one login and are, therefore, not useful to anyone who manages to eavesdrop and capture it. S/KEY is an OTP method developed and trademarked by Bellcore, typically used for terminal logins. In S/KEY, the secret pass-phrase is used to generate the first password, and each successive password is generated from the previous one by encrypting it. A list of passwords is generated by the S/KEY server software, and is distributed to users.

■ Token cards and soft tokens—Based on something you have (token card) and something you know (token card personal identification number [PIN]). Token cards are typically small electronic devices about the size and complexity of a credit card-sized calculator. There are many token card vendors, and each has its own token card server. The PIN is

placed (manually or automatically generated) into the card, which generates a secure password. A token server receives and validates the password. The password interplay usually consists of a remote client computer, an NAS, and a security server running token security software.

The authentication method should be chosen and implemented based on the guidelines established in the network security policy.

Authentication—Remote PC Username and Password

Cisco.com

Windows dialup networking connection username and password fields

Security server

Network access server

PSTN/ISDN

Windows remote PC

username/password (TCP/IP PPP)

SECUR 1.1—3-34
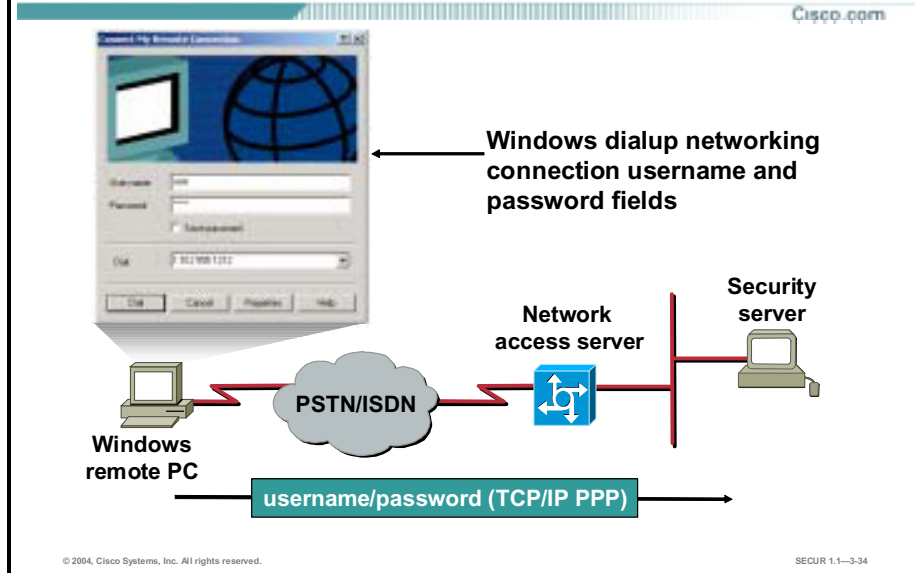
An example of dialup authentication using username and password authentication is shown in the figure. On the client end, the Windows dialup networking connection prompts the user for their username and password, which is sent over communication lines using TCP/IP and PPP to a remote NAS or a security server for authentication. As a matter of policy, do not allow users to select the Save password check box.

Authentication—One-Time Passwords, S/KEY

Cisco.com

- **List of one-time passwords**
- **Generated by S/KEY program hash function**
- **Sent in clear text over network**
- **Server must support S/KEY**

```
308202A8 30820211 A0030201 02020438
0500301B 310B3009 06035504 06130255
1E170D39 39313032 32313730 3634375A
C84DFBC0 4C7BD4B1 F79FC2ED 30A02EA4
```
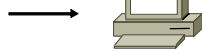
Security server supports S/KEY

S/KEY passwords   **Workstation**   **S/KEY password (clear text)**

SECUR 1.1—3-35

Remote logins can allow passwords to be sent as clear text over networks. An eavesdropper could capture passwords and use them to gain unauthorized access to systems. One way to create passwords that can be safely sent over remote connections is to use a one-way hashing algorithm to create an OTP scheme, which is what S/KEY does.

S/KEY uses either Message Digest 4 (MD4) or MD5 (one-way hashing algorithms developed by Ron Rivest) to create an OTP system. In this system, passwords are sent clear text over the network; however, after a password has been used, it is no longer useful to the eavesdropper. The main advantage of S/KEY is that it protects against eavesdroppers without modification of client software and imposes only marginal inconvenience to the users.

The S/KEY system involves three main pieces: the client, the host, and a password calculator. The client is responsible for providing the login shell to the user. It does not contain any persistent storage for password information. The host is responsible for processing the user's login request. It stores the current OTP as well as the login sequence number in a file. It is also responsible for providing the client with a seed value. The password calculator is a one-way hashing function that creates an irreversible password. The network protocol between the client and the host is completely independent of the scheme. Cisco Secure ACS supports S/KEY authentication.

Authentication—Token Cards and Servers
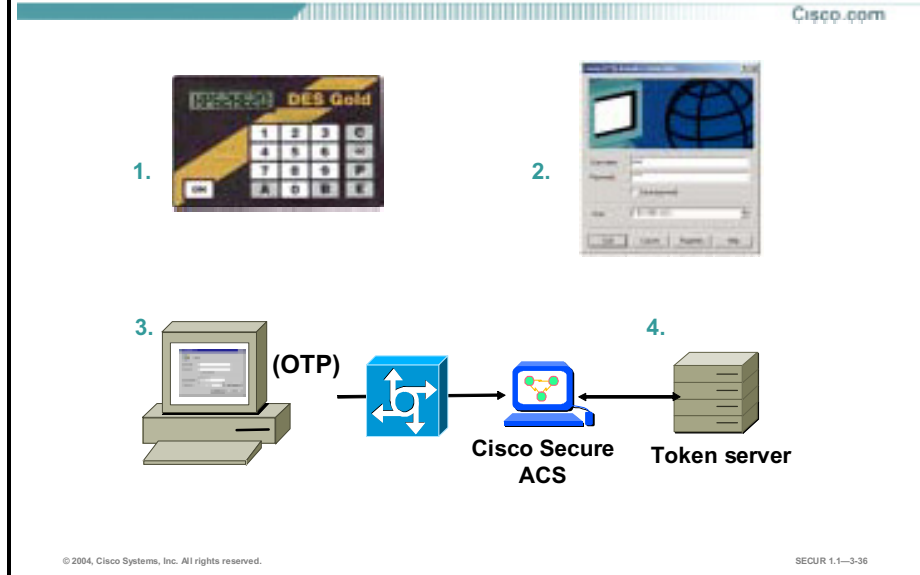
Another OTP authentication method that adds a new layer of security is accomplished with a token card (or smart card) and a token server. Each token card, about the size of a credit card, is programmed to a specific user and each user has a unique PIN that can generate a password keyed strictly to the corresponding card. OTP authentication takes place between the specified token server with a token card database and the user.

Token cards and servers generally work as shown in the figure and the following steps:

Step 1   The user generates an OTP with the token card that uses a security algorithm.

Step 2   The user enters the OTP into the authentication screen generated by the remote client (in this example the Windows Dial-Up Networking screen).

Step 3   The remote client sends the OTP to the token server via the network and an authenticating device, either directly or through the AAA server.

Step 4   The token server uses the same algorithm to verify that the password is correct and authenticates the remote user.

Two token card and server methods are used:

■   Time-based—In this system, the token card contains a cryptographic key and generates a password (or token) using a PIN entered by the user. The password is entered into the remote client, which sends it to the token server. The password is loosely synchronized in time to the token server. The server compares the token received to a token generated internally. If they match, the user is authenticated and allowed access.

■   Challenge-response—In this system, the token card stores a cryptographic key. The token server generates a random string of digits and sends it to the remote client that is trying to access the network. The remote user enters the random string, and the token card computes a cryptographic function using the stored key and random string. The result is sent back to the token server, which has also computed the function. If the results match, the user is authenticated.

Token cards are now implemented in software for installation on the remote client. SofToken, which generates single-use passwords without the associated cost of a hardware token, is one example of software token cards.

AAA Example—Authentication via PPP Link

Cisco.com

TCP/IP and PPP client —PPP— PSTN or ISDN —PPP— Network access server

- **PAP—Password Authentication Protocol**
  - **Clear text, repeated password**
  - **Subject to eavesdropping and replay attacks**
- **CHAP—Challenge Handshake Authentication Protocol**
  - **Secret password, per remote user**
  - **Challenge sent on link (random number)**
  - **Challenge can be repeated periodically to prevent session hijacking**
  - **The CHAP response is an MD5 hash of (challenge + secret) provides authentication**
  - **Robust against sniffing and replay attacks**
- **MS-CHAP—Microsoft CHAP v1 (supported in Cisco IOS > 11.3) and v1 or v2 (supported in Cisco IOS > 12.2)**

SECUR 1.1—3-37

An important component to consider in remote access security is support for authentication accomplished with Password Authentication Protocol (PAP), CHAP, and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). PPP is a standard encapsulation protocol for the transport of different network-layer protocols (including, but not limited to, IP) across serial point-to-point links. PPP enables authentication between remote clients and servers using PAP, CHAP, or MS-CHAP.

■ PAP—Provides a simple method for the remote client to establish its identity using a two-way handshake. The handshake is done only after initial PPP link establishment. After the link establishment phase is complete, a username and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

■ CHAP—Used to periodically verify the identity of the peer using a three-way handshake. The handshake is done upon initial link establishment, and may be repeated anytime after the link has been established.

CHAP provides protection against playback attack by the peer using an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

This authentication method depends upon a "secret" known only to the authenticator and that remote client. The secret is not sent over the link. Although the authentication is only one-way, by negotiating CHAP in both directions the same secret set may easily be used for mutual authentication.

CHAP requires that the secret be available in plaintext form. Irreversibly encrypted password databases commonly available (such as the Windows 2000 SAM hive) cannot be used.

MS-CHAP is the Microsoft version of CHAP. MS-CHAP is an extension of the CHAP described in RFC 1994. MS-CHAP enables PPP authentication between a PC using Microsoft Windows and an NAS. PPP authentication using MS-CHAP can be used with or without AAA security services.

MS-CHAP differs from standard CHAP as follows:

- MS-CHAP is enabled while the remote client and the NAS negotiate PPP parameters after link establishment.

- The MS-CHAP Response packet is in a format designed for compatibility with Microsoft's Windows networking products.

- MS-CHAP enables the network security server (authenticator) to control retry and password-changing mechanisms. MS-CHAP allows the remote client to change the MS-CHAP password.

- MS-CHAP defines a set of reason-for-failure codes returned to the remote client by the NAS.

Cisco routers support MS-CHAP in Cisco IOS Release 11.3 and later releases with the **ppp authentication ms-chap** command.

Cisco NASs and routers are configured to perform authorization using the **aaa authorization** commands.

You can configure Cisco Secure ACS to perform authorization tasks with NAS and routers. The per-user security policy determines how authorization is configured.

You can configure Cisco NASs and routers to capture and display accounting data using the **aaa accounting** commands, including the following: **exec** commands; network services such as SLIP, PPP, and AppleTalk Remote Access Protocol (ARAP); and system-level events not associated with users.

Configuring AAA for Cisco Routers

The remainder of this lesson describes how to configure a Cisco router to perform AAA using a local database for authentication.

Authenticating Router Access
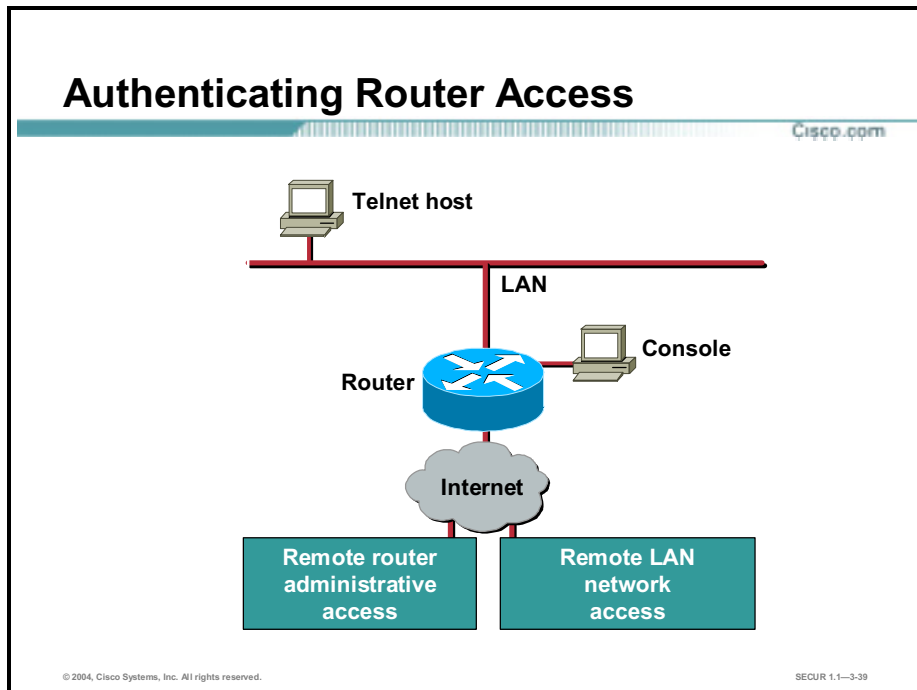
It is important that you secure the interfaces of all your routers, particularly your network access servers and Internet routers.

You must configure the router to secure administrative access and remote LAN network access using AAA commands. The router access modes, port types, and AAA command elements are compared in the table.

Access Type	Modes	Network Access Server Ports	AAA Command Element
Remote administrative access	Character (line/exec mode)	TTY, VTY, AUX, and console	login, exec, NASI connection, ARAP, and enable
Remote network access	Packet (interface mode)	async, group-async BRI and PRI	PPP, network, and ARAP

Router Local Authentication Configuration Process

The following are the general steps to configure a Cisco router for local authentication:

- **Secure access to privileged-EXEC mode.**
- **Enable AAA globally on the perimeter router with the** aaa new-model **command.**
- **Configure AAA authentication lists.**
- **Configure AAA authorization for use after the user has passed authentication.**
- **Configure the AAA accounting options for how you want to write accounting records.**
- **Verify the configuration.**

SECUR 1.1—3-40

The following are the general steps to configure the router for AAA:

Step 1   Secure access to privileged exec and configuration mode on vty, asynchronous, auxiliary, and tty ports.

Step 2   Enable AAA globally on the router.

Step 3   Configure AAA on the router.

Secure Access to Privileged-EXEC and Configuration Mode

router(config)#

```
enable password password
```

```
router(config)# enable password changeme
```

router(config)#

```
service password-encryption
```

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

router(config)#

```
enable secret password
```

```
router(config)# enable secret supersecret
```

This figure contains three methods for securing privileged-EXEC mode for Cisco routers. The methods are arranged with the least secure method at the top of the figure and the most secure method at the bottom of the figure.

Use one of the commands listed in the figure to secure privileged exec mode. It is recommended that you use the **enable secret** command whenever possible because it has a stronger encryption algorithm than the **service password-encryption** command and because **enable password** is written to the configuration file in clear text.

Note:	A lost encrypted password cannot be recovered. The only solution is to execute the proper password recovery routine and set a new enable password. Improperly executing the password recovery routine may damage the configuration file.

Enable AAA Globally Using the *aaa new-model* Command

router(config)#

```
aaa new-model
```

router(config)# aaa new-model

- **Establishes AAA section in configuration file**

router(config)#

```
username username password password
```

router(config)# username Joe106 password 1MugOJava

- **Helps prevent administrative access lockout while configuring AAA**

SECUR 1.1—3-42

The first step to configure an NAS or router to use the AAA process is to establish an AAA topic in the configuration file using the **aaa new-model** command, as shown in the figure.

The **aaa new-model** command forces the router to override every other authentication method previously configured for the router lines. If an administrative Telnet or console session is lost while enabling AAA on a Cisco router, and no local AAA user authentication account and method exists, the administrator will be locked out of the router. Therefore, it is important that you configure a local database account, as shown in the figure.

Caution:	When using the Cisco IOS **aaa new-model** command, always provide for a local login method. This guards against the risk of being locked out of a router should the administrative session fail while you are in the process of enabling AAA.

At a minimum the following commands should be entered in the order shown:

Router(config)# **aaa new-model**

Router(config)# **username *username* password *password***

Router(config)# **aaa authentication login default local**

Specifying the "local" authentication method enables you to re-establish your Telnet or console session and use the locally defined authentication list to access the router. If you fail to do this, and you become locked out of the router, physical access to the router is required (console session), with a minimum of having to perform a password recovery sequence. At worst, the entire configuration saved in NVRAM can be lost.

The **aaa authentication login** command is covered in more detail later in this topic.

aaa authentication Commands

```
router(config)#

aaa authentication arap
aaa authentication banner
aaa authentication enable default
aaa authentication fail-message
aaa authentication login
aaa authentication password-prompt
aaa authentication ppp
aaa authentication username-prompt
```

- **These** aaa authentication **commands are available in Cisco IOS releases 12.2 and above.**
- **Each of these commands has its own syntax and options (methods).**

SECUR 1.1—3-43

This figure contains a complete listing of **aaa authentication** commands for Cisco IOS release 12.2 or greater. It is important that you learn three of these commands and how to implement them in an AAA environment:

■ **aaa authentication login**

■ **aaa authentication ppp**

■ **aaa authentication enable default**

After enabling AAA globally on the access server, you need to define the authentication method lists and apply them to lines and interfaces. These authentication method lists are security profiles that indicate the service, PPP, AppleTalk Remote Access Protocol (ARAP), or NetWare Access Server Interface (NASI) or login and authentication method (local, TACACS+, RADIUS, line, or enable authentication). Up to four authentication methods may be applied to a line or interface. A good security practice is to have either **local** or **enable** as a last resort method to recover from a severed link to the chosen method's server.

Complete the following steps to define an authentication method list using the **aaa authentication** command:

Step 1 Specify the service (PPP, ARAP, or NASI) or login authentication.

Step 2 Identify a list name or **default**. A list name is any alphanumeric string you choose. You assign different authentication methods to different named lists. You can specify only one dial-in protocol per authentication method list. However, you can create multiple authentication method lists with each of these options. You must give each list a different name.

Step 3 Specify the authentication method and how the router should handle requests when one of the methods is not operating (the AAA server is down). You can specify up to four methods for AAA to try before stopping the authentication process.

Step 4 After defining these authentication method lists, apply them to each of the following:

- Lines—tty, vty, console, aux, and async lines or the console port for login and asynchronous lines (in most cases) for ARA

- Interfaces—Interfaces sync, async, and virtual configured for PPP, SLIP, NASI or ARAP

Step 5 Use the **aaa authentication** command in global configuration mode to enable the AAA authentication processes.

aaa authentication login Command

router(config)#

```
aaa authentication login {default | list-name}
  method1 [method2...]
```

```
router(config)# aaa authentication login default enable
```

```
router(config)# aaa authentication login console-in local
```

```
router(config)# aaa authentication login tty-in line
```

SECUR 1.1—3-44

Use the **aaa authentication login** command in global configuration mode, as shown in this figure, to set AAA authentication at login.

The following is the syntax for the **aaa authentication login** command:

aaa authentication login {default | *list-name*} *method1* [*method2. . .*]

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method	Specifies at least one of the following keywords.
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands.

aaa authentication ppp Command

```
router(config)#

aaa authentication ppp {default | list-name}
  method1 [method2...]
```

```
router(config)# aaa authen ppp default local
```

```
router(config)# aaa authen ppp dial-in local none
```

Use the **aaa authentication ppp** command in global configuration mode, as shown in this figure, to specify one or more AAA authentication methods for use on serial interfaces running PPP.

The following is the syntax for the **aaa authentication ppp** command:

aaa authentication ppp {default | *list-name*} *method1* [*method2. . .*]

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method	Specifies at least one of the following keywords.
if-needed	Does not authenticate if user has already been authenticated on a tty line.
krb5	Uses Kerberos 5 for authentication (can only be used for PAP authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands.

Cisco.com

router(config)#

```
aaa authentication enable default method1 [method2...]
```

```
router(config)# aaa authentication enable default group
  tacacs+
```

SECUR 1.1—3-46

Use the **aaa authentication enable default** command in global configuration mode, as shown in this figure, to enable AAA authentication to determine if a user can access the privileged command level.

The following is the syntax for the **aaa authentication enable default** command:

aaa authentication enable default *method1* **[***method2. . .* **]**

method	Specifies at least one of the following keywords.
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands.

Apply Authentication Commands to Lines and Interfaces

Cisco.com

```
router(config)# line console 0
router(config-line)# login authentication console-in
router(config)# int s3/0
router(config-if)# ppp authentication chap dial-in
```

- **Authentication commands can be applied to lines or interfaces.**

SECUR 1.1—3-47

Authentication commands can be applied to router lines and interfaces, as shown in this figure.

The following is a brief explanation of the examples shown in the figure:

- **line console 0**—Enters line console configuration mode

- **login authentication console-in**—Uses the list named *console-in* for login authentication on console port 0

- **int s3/0**—Specifies port 0 of serial interface slot number 3

- **ppp authentication chap dial-in**—Uses the list named *dial-in* for PPP CHAP authentication on interface s3/0

Note:	It is recommended that you always define a default list for AAA to provide "last resort" authentication on all lines and interfaces protected by AAA.

aaa authorization Command

router(config)#

```
aaa authorization {network | exec | commands level |
 reverse-access | configuration} {default | list-name}
 method1 [method2...]
```

```
router(config)# aaa authorization commands 1 alpha local
```

```
router(config)# aaa authorization commands 15 bravo local
```

```
router(config)# aaa authorization network charlie local none
```

```
router(config)# aaa authorization exec delta if-authenticated
```

SECUR 1.1—3-48

Use the **aaa authorization** command in global configuration mode, as shown in this figure, to set parameters that restrict administrative access to the routers or user access to the network.

The following is the syntax for the **aaa authorization** command:

aaa authorization {network | exec | commands *level* | reverse-access | configuration} {default | *list-name*} *method1* [*method2...*]

network	Runs authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARA.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as **autocommand** information.
commands	Runs authorization for all commands at the specified privilege level.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
configuration	Downloads the configuration from the AAA server.
default	Uses the listed authentication methods that follow this argument as the default list of methods for authorization.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
list-name	Character string used to name the list of authorization methods.
method	Specifies at least one of the following keywords.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** commands.
if-authenticated	Allows the user to access the requested function if the user is authenticated.

krb5-instance	Uses the instance defined by the **kerberos instance map** command.
local	Uses the local database for authorization.
none	No authorization is performed.

There is a provision for naming the authorization list after specifying the service just like there is for naming an authentication list. Also the list of methods is not limited to just a single method as the figure and explanations show, but rather may have up to four methods listed for failing over to, just as the **aaa authentication** command could.

Named authorization lists allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

A brief explanation of the examples is shown here:

■ **aaa authorization commands 1 alpha local**—Uses local user name database to authorize the use of all level 1 commands for the Alpha list.

■ **aaa authorization commands 15 bravo local**—Uses the local database to authorize the use of all level 15 commands for the Bravo list.

■ **aaa authorization network charlie local none**—Uses the local database to authorize the use of all network services such as SLIP, PPP, and ARAP for the Charlie list. If the local server is not available, this command performs no authorization, and the user can use all network services.

■ **aaa authorization exec delta if-authenticated**—Lets the user run the exec process if the user is already authenticated.

Troubleshooting AAA Using *debug* Commands

router#

```
debug aaa authentication
```

- **Use this command to help troubleshoot AAA authentication problems.**

router#

```
debug aaa authorization
```

- **Use this command to help troubleshoot AAA authorization problems.**

router#

```
debug aaa accounting
```

- **Use this command to help troubleshoot AAA accounting problems.**

SECUR 1.1—3-49

Use the following **debug** commands on your routers to trace AAA packets and monitor authentication, authorization, or accounting activities:

- **debug aaa authentication**—Displays debugging messages on authentication functions

- **debug aaa authorization**—Displays debugging messages on authorization functions

- **debug aaa accounting**—Displays debugging messages on accounting functions

Troubleshooting AAA Using the *debug aaa authentication* Command

```
router# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''
ruser='' port='tty1' rem_addr='async/81560' authen_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
```

　　　　　　SECUR 1.1—3-50

Use the **debug aaa authentication** privileged exec command, as shown in the figure, to display information on AAA authentication. Use the **no debug aaa authentication** form of the command to disable this debug mode.

This figure contains debug output for a successful AAA authentication using a local database.

Troubleshooting AAA Using the *debug aaa authorization* Command

```
router# debug aaa authorization
2:23:21: AAA/AUTHOR (0): user='carrel'
2:23:21: AAA/AUTHOR (0): send AV service=shell
2:23:21: AAA/AUTHOR (0): send AV cmd*
2:23:21: AAA/AUTHOR (342885561): Method=TACACS+
2:23:21: AAA/AUTHOR/TAC+ (342885561): user=carrel
2:23:21: AAA/AUTHOR/TAC+ (342885561): send AV service=shell
2:23:21: AAA/AUTHOR/TAC+ (342885561): send AV cmd*
2:23:21: AAA/AUTHOR (342885561): Post authorization status =
  FAIL
```

Use the **debug aaa authorization** privileged-EXEC command to display information on AAA authorization. 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 where an exec authorization for user *carrel* is performed:

- On the first line, the username *carrel* is authorized.

- On the second and third lines, the attribute value (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 AV pairs associated with the **debug aaa authorization** command that may appear in the debug output are described as follows:

- 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 LCP is being requested (lower layer of PPP).

- protocol=ip—Used with service=slip and service=slip 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 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 access list 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 access list for SLIP or PPP/IP (for example, inacl=2).

- outacl=x—Used with service=ppp and protocol=ip. Contains an IP output access list 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 noescape option to the username configuration command. Can be either true or false (for example, noescape=true).

- nohangup=x—Used with service=shell and cmd=NULL. Specifies a nohangup 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.

Troubleshooting AAA Using the *debug aaa accounting* Command

```
router# 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
```

SECUR 1.1—3-52

Use the **debug aaa accounting** privileged exec command, as shown in the figure, to display information on accounting events as they occur. Use the **no debug aaa accounting** form of the command to disable this debug mode. This figure displays sample output from the **debug aaa accounting** command.

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. It provides systems administrators 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 **debug aaa accounting** is active as well.

Summary

This topic summarizes this lesson.

Summary

- **It is very important to provide physical installation security for enterprise routers and switches.**
- **It is extremely important that you configure secure administrative access for enterprise routers.**
- **Administrative and remote network access modes can be secured with AAA.**
- **Cisco router AAA configuration should follow an orderly progression.**

SECUR 1.1—3-54

Summary (Cont.)

- **Use the** aaa new-model **command to add AAA services to a Cisco router.**
- **Use** aaa **commands to specify authentication, authorization, and accounting processes and methods.**
- **Use** debug aaa **commands selectively to troubleshoot AAA.**

SECUR 1.1—3-55

Lab Exercise—Configuring Basic Cisco Router Security

In this hands-on exercise you will configure the perimeter router to work with the local database, enable password, and line authentication to provide authentication, authorization, and accounting (AAA) services.

Objectives

In this lab exercise, you will complete the following tasks:

- Complete the lab exercise setup.
- Configure password minimum length.
- Configure the enable secret password.
- Configure the console port line-level password.
- Configure the VTY line-level password.
- Configure the auxiliary port line-level password.
- Encrypt clear text passwords.
- Test administrative access security.
- Configure local database authentication using AAA.
- Verify the perimeter router configuration.
- Test authentication using debug.
- Configure enhanced username password security.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.

Lab Visual Objective

Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1   Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2   Configure your student PC for IP address **10.0.P.12** with a default gateway of **10.0.P.2** (where P = pod number).

Task 2—Configure Password Minimum Length

Complete the following steps to configure a minimum length for all router passwords:

Step 1   Establish a Telnet session to the remote terminal server (RTS) and connect to the console port of your perimeter router. Your instructor will explain how to do this.

Step 2   Enter enable mode using a password of cisco:

```
RP> enable
Password: cisco
RP#
```

Step 3 View the router running configuration using the **show run** command:

```
RP# show run
```

Q1) Can you read the enable password?

A) _____

Step 4 Enter global configuration mode using the **configure terminal** command:

```
RP# config terminal
RP(config)#
```

Step 5 Configure a minimum password length of eight characters using the **security passwords** command:

```
RP(config)# security passwords min-length 8
RP(config)#
```

Task 3—Configure the Enable Secret Password

The perimeter router currently has enable password protection only. This enable password is unencrypted by default. Configure an encrypted password by completing the following steps on the perimeter router (where P = pod number):

Step 1 Attempt to configure an enable secret password of Curium using the **enable secret** command (passwords are case sensitive):

```
RP(config)# enable secret Curium
```

Q2) Does the router accept the new enable secret password? Why or why not?

A) _____

Step 2 Configure an enable secret password of Curium96 using the **enable secret** command (passwords are case-sensitive):

```
RP(config)# enable secret Curium96
RP(config)# end
```

Step 3 Show the running configuration using the **show run** command:

```
RP# show run
```

Q3) Can you read the enable secret password? Why or why not?

A) _____

Note: Find the enable password in the router configuration listing. Notice that the enable password, cisco, is shorter than the minimum length required of new passwords. This is because minimum length only affects passwords created after the **security passwords min-length** command is run. It has no effect on older passwords until you reboot the router. (This is an important item for you to note when you configure your router passwords, and it is the reason why it is a good idea to set the minimum password length first.) The next time you reboot the router, an error message will inform you that the enable password is too short.

Task 4—Configure the Console Port Line-Level Password

By default, Cisco router console ports do not require a password for administrative access. Complete the following steps to configure a console port line-level password (where P = pod number):

Step 1   Enter console 0 line configuration mode using the **line console** command:

```
RP# config t
RP(config)# line console 0
RP(config-line)#
```

Step 2   Enable password checking on login using the **login** command:

```
RP(config-line)# login
% Login disabled on line 0, until 'password' is set
RP(config-line)#
```

Step 3   Enter a new console line-level password of ConUser1 using the **password** command (passwords are case sensitive):

```
RP(config-line)# password ConUser1
RP(config-line)# end
RP#
```

Step 4   Show the running configuration and view the **line con 0** section.

Q4)   Can you read the console line 0 line-level password? Why or why not?

A)   _____

Task 5—Configure the VTY Line-Level Password

By default, Cisco router VTY lines do not have a line-level password for Telnet administrative access. You must configure a VTY line-level password before attempting to access the router using Telnet. If VTY login password checking is enabled, and no password is configured, the router will not allow you to complete the Telnet connection. Complete the following steps to configure a VTY line-level password for your router:

Step 1   Enter VTY line 0–4 configuration mode using the **line vty** command:

```
RP# config t
RP(config)# line vty 0 4
RP(config-line)#
```

Step 2   Enable password checking on login using the **login** command:

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

Step 3 Enter a new console line-level password of VTYUser1 using the password command (passwords are case sensitive):

```
RP(config-line)# password VTYUser1
RP(config-line)# end
RP#
```

Step 4 Show the running configuration and view the **line vty 0 4** section.

Q5)   Can you read the VTY line 0 4 line-level password? Why or why not?

A)   _____

Task 6—Configure the Auxiliary Port Line-Level Password

By default, Cisco router auxiliary ports do not require a line-level password for administrative access. Complete the following steps to configure an auxiliary port line-level password for your router:

Step 1 Enter auxiliary line 0 configuration mode using the **line aux** command:

```
RP# config t
RP(config)# line aux 0
RP(config-line)#
```

Step 2 Enable password checking on login using the **login** command:

```
RP(config-line)# login
% Login disabled on line 65, until 'password' is set.
RP(config-line)#
```

Step 3 Enter a new auxiliary port line-level password of AuxUser1 using the **password** command (passwords are case sensitive):

```
RP(config-line)# password AuxUser1
RP(config-line)# end
RP#
```

Step 4 Show the running configuration and view the **line aux 0** section.

Q6)   Can you read the auxiliary line 0 line-level password? Why or why not?

A)   _____

Task 7—Encrypt Clear Text Passwords

Up to this point, the only hashed password on the router has been the enable secret password. Now that you have entered your line-level passwords for the console, VTY, and auxiliary lines, you should encrypt them as well. Complete the following steps to encrypt the passwords you just configured:

Step 1 Encrypt all clear text passwords using the **service password-encryption** command:

```
RP# config t
RP(config)# service password-encryption
RP(config)# end
```

Step 2 Show the running configuration and view the passwords.

> Q7) Can you read the passwords? Why or why not?
>
> A) _____
>
> Q8) At what level (number) is the enable secret password encrypted?
>
> A) _____
>
> Q9) At what level (number) are the other passwords encrypted?
>
> A) _____
>
> Q10) Which level of encryption is harder to crack and why?
>
> A) _____
>
> Q11) Is the enable (not the enable secret) password used anymore? Why or why not?
>
> A) _____

Step 3 Save your running configuration to the startup-config file using the **copy run start** command:

```
RP# copy run start
Destination filename [startup-config]? <Enter>
Building configuration…
[OK]
RP#
```

Task 8—Test Administrative Access Security

Complete the following to test your enable secret and line-level passwords:

Step 1 Log out of the router console port connection.

Step 2 Access your router console port.

Step 3 Log in using the **ConUser1** console port line-level password.

Step 4 Enter privileged-EXEC mode using the **Curium96** enable secret password.

Step 5 Log out of the router console port connection.

Step 6 Leave the command prompt session window open. Open another command prompt shell on your student PC and establish a Telnet session to the inside interface of your router at IP address **10.0.P.2** (where P = pod number).

Step 7 Log in using the **VTYUser1** VTY line-level password.

Step 8 Attempt to enter privileged-EXEC mode using the **cisco** enable password.

> Q12) Are you able to use the enable password? Why or why not?
>
> A) _____

Step 9 Enter privileged-EXEC mode using the **Curium96** enable secret password.

Step 10   Log out of the router and close this command prompt session window.

Step 11   Return to the Telnet command prompt window and log in to the console port using the
ConUser1 console port line-level password.

Step 12   Enter privileged-EXEC mode using the **Curium96** enable secret password.

Task 9—Configure Local Database Authentication Using AAA

In this section, you configure local database authentication using AAA for the enable, line, and
local methods so you can experience the differences between the methods.

Now that the perimeter router administrative access points are protected (except PPP, of
course), you need to use AAA commands to prepare for migration to a Cisco Secure Access
Control Server (ACS) environment. The goal of this task is to show you that each router access
point can be secured using unique methods.

There are five access points to protect: line, VTY, AUX, console, and PPP.

Complete the following steps to configure unique method login authentication on all access
points:

Step 1   Turn on AAA features using the **aaa new-model** command:

```
RP# config t
RP(config)# aaa new-model
```

Step 2   As an added safety measure, create a local username/password account to use in case you lose
your Telnet connection during AAA configuration:

```
RP(config)# username admin password admindoor
RP(config)#
```

Step 3   Configure login authentication to use the enable password (or enable secret password if it is
configured) from the default list:

```
RP(config)# aaa authentication login default enable
RP(config)# end
```

This protects all login access instantly (except PPP).

Step 4   Log out of the router.

Step 5   Access the router console port. You should be prompted for a password.

Q13)   Which password should you use, ConUser1 or Curium96? Why?

A)   _____

Step 6   Using the local database, configure a specific login authentication method for the console port.
Create a username of **admin** with a password of **admindoor** and a list name of **console-in**
using the following commands (passwords are case sensitive and may contain spaces):

```
RP> enable
Password: Curium96
RP# config t
```

```
RP(config)# username admin password admindoor
RP(config)# aaa authentication login console-in local
RP(config)# line con 0
RP(config-line)# login authentication console-in
RP(config-line)# end
RP#
```

Note:	It is recommended that you never use "admin" as a username because it is too easy to guess.

Step 7 Log out of the router.

Step 8 Test the console port authentication method you just configured.

Step 9 Secure VTY access for the IS department username **isgroup** with a password of **isdoorin1** and a new list name of **is-in** using the following commands:

```
RP> enable
Password: Curium96
RP# config t
RP(config)# username isgroup password isdoorin1
RP(config)# aaa authentication login is-in local
RP(config)# line vty 0 4
RP(config-line)# login authentication is-in
RP(config-line)# end
```

This is the same idea as the console protection, but on the Telnet access via VTY ports.

Step 10 Exit privileged-EXEC mode and log out of the router.

Step 11 Leave the command prompt session window open. Open another command prompt shell on your PC and telnet to the inside interface of your router at IP address **10.0.P.2** (where P = pod number).

Step 12 Test the VTY line authentication method you just configured.

Step 13 Enter enable mode and copy the router running configuration to the startup configuration.

Step 14 Log out of the router and close this command prompt window.

Task 10—Verify the Perimeter Router Configuration

At this point, your perimeter router configuration should look similar to the following subsections. Use the **show run** command to view the configuration.

Note:	This is a partial view of your router configuration containing only the sections modified in this lab exercise. Your encrypted passwords may vary.

```
!
hostname RP
```

```
!
security passwords min-length 8
no logging console
aaa new-model
!
!
aaa authentication login default enable
aaa authentication login console-in local
aaa authentication login is-in local
aaa session-id common
enable secret 5 $1$.1EP$T2wmSWx6VY1Q6y81sESvN/
enable password 7 060506324F41
!
username admin password 7 14161606050A2E242B3A
username isgroup password 7 011A1500540414
!
line con 0
 password 7 072C2E427B1A1C1746
 login authentication console-in
line aux 0
 password 7 052A1317145F4B1B48
line vty 0 4
 password 7 122F312E271809167B
 login authentication is-in
!
end
```

Task 11—Test Authentication Using Debug

In this task, you will use debug to look at the indicators for successful and unsuccessful authentication attempts. Before beginning this section, ensure that all Telnet sessions are disconnected. Leave the console session open.

It is important in debugging to ensure that you have a proper time reference for messages, especially if you are logging multiple devices to a central logging system. Log in to user mode and enter the **show clock** command to check the router clock. If the time and date are incorrect, access enable mode and enter the following command: **clock set HH:MM:SS DD month YYYY** (for example, **clock set 10:00:00 21 March 2002**).

Complete the following steps to look at the indicators for successful and unsuccessful authentication attempts:

Step 1 Enter global configuration mode and use the following command to ensure that you have detailed time stamp information for your debug output:

```
RP(config)# service timestamps debug datetime msec

RP(config)# logging console
```

```
              RP(config)# end
```

Step 2   Turn on debugging for AAA authentication:

```
RP# debug aaa authentication
```

Step 3   Trigger an AAA authentication event by logging out of your console connection and logging in with username **admin** and password **admindoor**.

Step 4   When you have logged in and are presented with the user mode prompt, continue in enable mode. The debug output follows (with notes in <brackets>):

```
Username: admin
```

```
Password: <valid password entered here>
```

```
Mar 21 17:05:00.461: AAA/AUTHEN/LOGIN (00000053): Pick method list
'console-in'
```

```
RP> enable
```

```
Password: <valid enable password entered here>
```

```
Mar 21 17:05:11.656: AAA: parse name=tty0 idb type=-1 tty=-1
```

```
Mar 21 17:05:11.656: AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=0 channel=0
```

```
Mar 21 17:05:11.656: AAA/MEMORY: create_user (0x82B2138C) user='admin'
ruser='NULL' ds0=0 port='tty0' rem_addr='async' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'
```

```
Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): port='tty0'
list='' action=LOGIN service=ENABLE
```

```
Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): console enable -
default to enable password (if any)
```

```
Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): Method=ENABLE
```

```
Mar 21 17:05:11.660: AAA/AUTHEN(3254755694): Status=GETPASS
```

```
Mar 21 17:05:18.671: AAA/AUTHEN/CONT (3254755694): continue_login
(user='(undef)')
```

```
Mar 21 17:05:18.671: AAA/AUTHEN(3254755694): Status=GETPASS
```

```
Mar 21 17:05:18.671: AAA/AUTHEN/CONT (3254755694): Method=ENABLE
```

```
Mar 21 17:05:18.755: AAA/AUTHEN(3254755694): Status=PASS
```

```
Mar 21 17:05:18.755: AAA/MEMORY: free_user (0x82B2138C) user='NULL'
ruser='NULL' port='tty0' rem_addr='async' authen_type=ASCII
service=ENABLE priv=15
```

```
              RP#
```

Step 5   Log out of the router.

Step 6   Log in again, but this time enter an invalid enable password:

```
Username: admin
```

```
Password: <valid password entered here>
```

```
Mar 21 17:07:40.612: AAA/AUTHEN/LOGIN (00000054): Pick method list
'console-in'
```

```
RP> enable
```

```
Password: <invalid enable password entered here>
```

```
Mar 21 17:07:52.103: AAA: parse name=tty0 idb type=-1 tty=-1
```

```
Mar 21 17:07:52.103: AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=0 channel=0

Mar 21 17:07:52.107: AAA/MEMORY: create_user (0x82CE62E0) user='admin'
ruser='NULL' ds0=0 port='tty0' rem_addr='async' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): port='tty0'
list='' action=LOGIN service=ENABLE

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): console enable -
default to enable password (if any)

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): Method=ENABLE

Mar 21 17:07:52.107: AAA/AUTHEN(2358711356): Status=GETPASS

% Access denied

RP>

Mar 21 17:07:55.180: AAA/AUTHEN/CONT (2358711356): continue_login
(user='(undef)')

Mar 21 17:07:55.180: AAA/AUTHEN(2358711356): Status=GETPASS

Mar 21 17:07:55.180: AAA/AUTHEN/CONT (2358711356): Method=ENABLE

Mar 21 17:07:55.260: AAA/AUTHEN(2358711356): password incorrect

Mar 21 17:07:55.260: AAA/AUTHEN(2358711356): Status=FAIL

Mar 21 17:07:55.260: AAA/MEMORY: free_user (0x82CE62E0) user='NULL'
ruser='NULL' port='tty0' rem_addr='async' authen_type=ASCII
service=ENABLE priv=15

RP>
```

Step 7   Turn off logging to the console using the **no logging console** command.

Step 8   Log out of the router.

Task 12—Configure Enhanced Username Password Security

The **service password-encryption** command encrypts user passwords using a weak encryption scheme. A safer way to encrypt your user passwords is to use MD5 hashing. Use MD5 hashing of new user passwords by completing the following steps:

Step 1   Log in to the router and enter global configuration mode.

Step 2   Create a new user account with MD5 hashing for the password:

```
RP(config)# username rtradmin secret 0 Iridium77
```

Step 3   Exit global configuration mode and list the running configuration.

Q14)   Can you read the password for the new user account? Why or why not?

A)   _____

Q15)   Which hashing method is used for the password?

A)   _____

Answers

This section contains the answers to the questions posed earlier:

Q1)   Yes. The enable password is not yet encrypted.

Q2)   No. The password is not at least eight characters in length.

Q3)   No. You cannot read the enable secret password because it is automatically hashed when created.

Q4)   Yes. The password is not yet encrypted.

Q5)   Yes. The password is not yet encrypted.

Q6)   Yes. The password is not yet encrypted.

Q7)   No. The passwords have all been encrypted using the **service password-encryption** command.

Q8)   Level 5.

Q9)   Level 7.

Q10)   Level 5 is harder to crack because it uses a strong MD5 hashing algorithm.

Q11)   No. The enable secret password takes precedence over the enable password.

Q12)   No. The enable secret password takes precedence over the enable password.

Q13)   Curium96 is used because the enable secret password takes precedence over the enable password.

Q14)   No. The password is encrypted.

Q15)   The password is hashed using MD5 (as noted by the number "5" in the configuration).

4

Advanced AAA Security for Cisco Router Networks

Overview

This lesson covers Cisco Secure Access Control Server (ACS) for Windows Server, Cisco Secure ACS for UNIX (Solaris), and Cisco Secure ACS Solution Engine. The Windows Server version has the most coverage in the lesson. The configuration of the Windows Server product is covered as a high-level overview, with the emphasis on the lab exercise. The UNIX and Solution Engine products are not included in the lab. The lesson also covers the security services of Terminal Access Controller Access Control System Plus (TACACS+), Remote Access Dial-In User Service (RADIUS), and Kerberos. Only TACACS+ is included in the lab.

This lesson includes the following topics:

- Objectives

- Introduction to Cisco Secure ACS

- Product overview—Cisco Secure ACS for Windows Server

- Product overview—Cisco Secure ACS for UNIX (Solaris)

- Product overview—Cisco Secure ACS Solution Engine

- Installing Cisco Secure ACS for Windows Server version 3.2

- Administering and troubleshooting Cisco Secure ACS for Windows Server version 3.2

- TACACS+ overview and configuration

- Verifying TACACS+

- RADIUS configuration overview

- Kerberos overview

- Summary

- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- **Describe the features and architecture of Cisco Secure ACS for Windows Server.**
- **Configure Cisco Secure ACS for Windows Server to perform AAA functions.**
- **Describe the features and architecture of Cisco Secure ACS for UNIX.**
- **Describe the features and architecture of the Cisco Secure ACS Solution Engine.**
- **Configure a router to communicate with a AAA server using TACACS+.**

SECUR 1.1—4-3

Introduction to Cisco Secure ACS

This topic presents an introduction to the Cisco Secure ACS offerings and includes the following products:

■ Cisco Secure ACS for Windows Server

■ Cisco Secure ACS for UNIX

■ Cisco Secure ACS Solution Engine
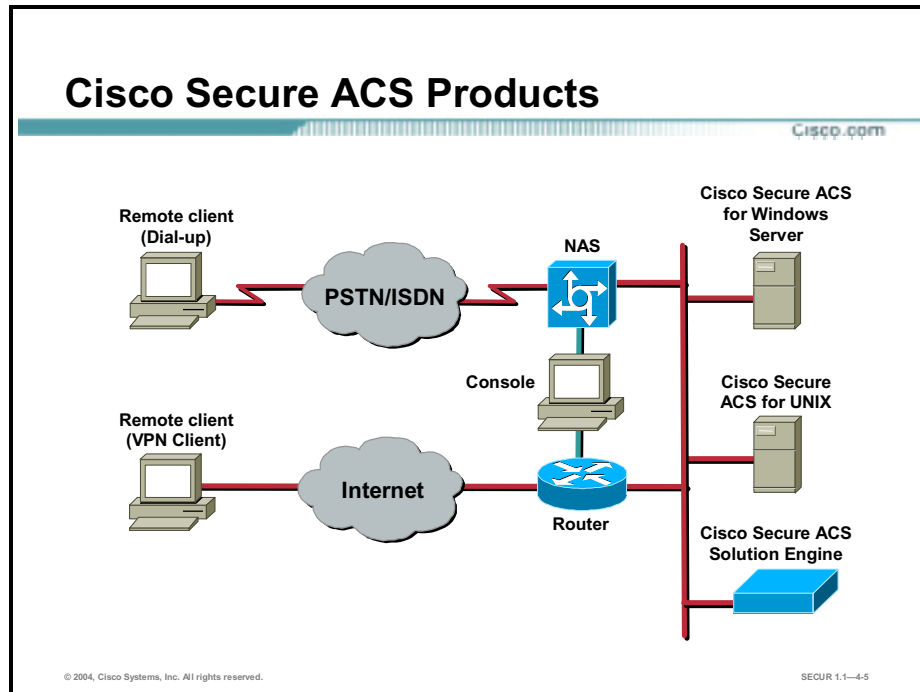
The next three topics discuss each of the Cisco Secure ACS product offerings.

Product Overview—Cisco Secure ACS for Windows Server

Cisco Secure ACS for Windows Server is a network security software application that helps you control access to the campus, dial-in access, and Internet access. Cisco Secure ACS for Windows Server operates as Windows 2000 services and controls authentication, authorization, and accounting (AAA) of users accessing the network.

This topic presents an overview of the product and prepares you to install and configure Cisco Secure ACS for Windows Server.

What Is Cisco Secure ACS for Windows Server?

Cisco.com

- **Provides AAA services to network devices that function as AAA clients, such as routers, NASs, PIX Firewalls, or VPN 3000 Concentrators**
- **Helps centralize access control and accounting, in addition to router and switch access management**
- **Allows network administrators to quickly administer accounts and globally change levels of service offerings for entire groups of users**
- **Although the use of an external user database is optional, Cisco Secure ACS for Windows Server supports many popular user repository implementations**
- **Uses the TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment**
- **Can authenticate against many popular token servers**

SECUR 1.1—4-7

Cisco Secure ACS for Windows Server provides AAA services to network devices that function as AAA clients, such as routers, network access servers, PIX Firewalls, or VPN 3000 Concentrators. An AAA client is any device that provides AAA client functionality and uses one of the AAA protocols supported by Cisco Secure ACS. It also supports third-party devices that can be configured with TACACS+ or RADIUS protocols. Cisco Secure ACS treats all such devices as AAA clients. Cisco Secure ACS uses the TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment.

Cisco Secure ACS helps centralize access control and accounting, in addition to router and switch access management. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users. Although the use of an external user database is optional, support for many popular user repository implementations enables companies to use the working knowledge gained from and the investment already made in building the corporate user repositories.

Cisco Secure ACS for Windows Server version 3.2 is an easy-to-use AAA server that is simple to install and administer. It runs on the popular Microsoft Windows 2000 Server operating

system. The Cisco Secure ACS for Windows Server administration interface is viewed using supported web browsers, making it easy to administer.

Cisco Secure ACS for Windows Server authenticates usernames and passwords against the Windows 2000 user database, the Cisco Secure ACS for Windows Server database, a token server database, or NDS.

Different levels of security can be used with Cisco Secure ACS for different requirements. The basic user-to-network security level is password authentication protocol (PAP). Although it does not represent the highest form of encrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows 2000 database. With this configuration, users need to log in only once. CHAP allows a higher level of security for encrypting passwords when communicating from a client to the network access server (NAS). You can use CHAP with the Cisco Secure ACS user database.

Cisco Secure ACS for Windows Server—General Features
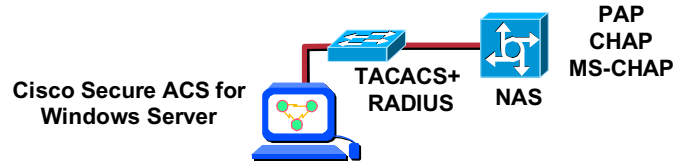
Cisco Secure ACS for Windows Server has the following general features:
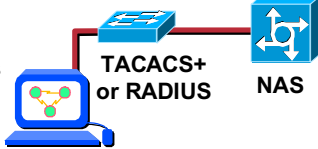
■ Simultaneous TACACS+ and RADIUS support

■ Windows 2000 user database support:

— Leverages and consolidates Windows 2000 username and password management

— Enables single login to network and Windows 2000 domains

— Runs on Windows 2000 standalone, primary domain controller (PDC), and backup domain controller (BDC) server configurations

---

Note: Windows 2000 Advanced Server and Windows 2000 Datacenter Server are not supported operating systems.

■ Other locations of user database:

— External token card servers

— Novell Directory Service (NDS)

— ACS databases

— Others

■ Supports the following, leading authentication protocols:

— ASCII/Password Authentication Protocol (PAP)

— Challenge Handshake Authentication Protocol (CHAP)

— Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

— Light Extensible Authentication Protocol (LEAP)

— Extensible Authentication Protocol-CHAP (EAP-CHAP)

— EAP-Transport Layer Security (EAP-TLS)

— AppleTalk Remote Access Protocol (ARAP)

■ Network access server callback feature supported for increased security

Cisco Secure ACS for Windows Server—AAA Features

Cisco Secure
ACS for Windows
Server

TACACS+
or RADIUS

NAS

• **TACACS+ support for:**
  – **Access lists (named or numbered)**
  – **Controls time-of-day and day-of-week access**
  – **ARA support**
  – **Enable privilege support levels**
• **RADIUS support for:**
  – **IETF RADIUS**
  – **Cisco RADIUS AV-pair**
  – **Proprietary RADIUS extensions**
• **Single TACACS+ or RADIUS database for simultaneous support**

SECUR 1.1—4-9

Cisco Secure ACS for Windows Server supports the following AAA features:

■ TACACS+ support for:

— Access lists, named or numbered

— Time-of-day and day-of-week access restrictions

— AppleTalk Remote Access (ARA)

— Enable privilege support levels

— Authentication to a Lightweight Directory Access Protocol (LDAP) server

— One-time password (OTP) for enable passwords

■ RADIUS versions:

— Internet Engineering Task Force (IETF) RADIUS

— Cisco RADIUS attribute value (AV) pair

— Proprietary RADIUS extensions (Lucent)

■ Single TACACS+/RADIUS database for simultaneous support

Other AAA product features are as follows:

■ Virtual Private Network (VPN) and Virtual Private Dialup Network (VPDN) support available at the origination and termination of VPN (Layer 2 Forwarding, or L2F) tunnels

■ User restrictions based on remote address Calling Line Identification (CLID)

■ Can disable an account on a specific date, or after "n" failed attempts

Cisco Secure ACS for Windows Server—Administration Features

- **Browser interface allows for easy management**
- **Displays logged-in users**
- **Creates separate TACACS+ and RADIUS CSV accounting files**

SECUR 1.1—4-10

Cisco Secure ACS has many user-friendly administration features such as:

- Browser-based GUI allows management from a web browser via LAN, WAN, or dial-up access. Simplifies and distributes configuration for ACS, user profiles, and group profiles:

    — Help and online documentation included for quick problem solving, accessible via web browser (not a Secure Sockets Layer [SSL] browser, it uses CSAdmin)

    — Group administration of users for maximum flexibility and to facilitate enforcement and changes of security policies

    — Remote administration permitted/denied by unique administrative username/password

    — Remote administrator session has timeout value

    — Can view logged-in user list for quick view of who is currently connected

- Creates separate TACACS+ and RADIUS files stored in a comma-separated value (CSV) spreadsheet format for easy import into databases and spreadsheet applications

- Has import utility to rapidly import a large number of users

- Hash indexed flat-file database support for high-speed transaction processing (Cisco Secure ACS user database)

Cisco Secure ACS for Windows Server—Distributed System Features

- **Authentication forwarding**
- **Fallback on failed connection**
- **Remote and centralized accounting**

Cisco Secure ACS for Windows Server

NAS

Cisco Secure ACS for Windows Server

Cisco Secure ACS for Windows Server
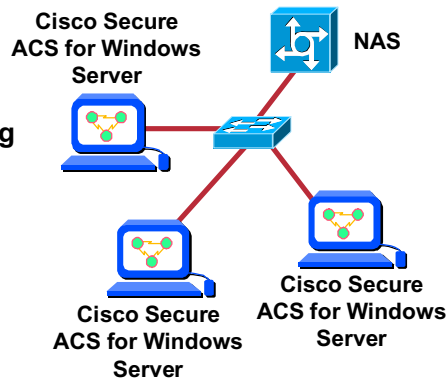
SECUR 1.1—4-11

Cisco Secure ACS can be used in a distributed system. Multiple Cisco Secure ACS servers and AAA servers can be configured to communicate with one another as masters, clients, or peers. It also allows Cisco Secure ACS to recognize network access restrictions of other Cisco Secure ACS servers on the distributed network. Cisco Secure ACS allows you to use powerful features such as:

■ Authentication forwarding—Authentication forwarding allows the Cisco Secure ACS to automatically forward an authentication request from a network access server to another Cisco Secure ACS. After authentication, authorization privileges are applied to the network access server for that user authentication.

■ Fallback on failed connection—You can configure the order in which Cisco Secure ACS checks the remote Cisco Secure ACS servers if the network connection to the primary Cisco Secure ACS server fails. If an authentication request cannot be completed to the first listed server, the next listed server is checked until a Cisco Secure ACS server handles the authentication. If Cisco Secure ACS cannot connect to any of the servers in the list, authentication fails.

■ Remote and centralized accounting—Cisco Secure ACS can be configured to point to a centralized Cisco Secure ACS that is used as the accounting server. The centralized Cisco Secure ACS has all the capabilities that a Cisco Secure ACS server has, with the addition of being a central repository for all accounting logs that are sent.

Cisco Secure ACS for Windows Server—External Database Support

- **Windows 2000 user database**
- **Generic LDAP**
- **NDS**
- **ODBC-compliant relational databases**
- **LEAP proxy RADIUS servers**
- **RSA SecurID token servers**
- **RADIUS-based token servers, including:**
  - **ActivCard token servers**
  - **CRYPTOCard token servers**
  - **VASCO token servers**
  - **PassGo token servers**
  - **SafeWord token servers**
  - **Generic RADIUS token servers**

SECUR 1.1—4-12

You can configure Cisco Secure ACS to forward authentication of users to one or more external user databases. Support for external user databases means that Cisco Secure ACS does not require that you create duplicate user entries in the Cisco Secure user database. Users can be authenticated using the databases shown in this figure. Regardless of which database is used to authenticate users, the Cisco Secure user database, internal to Cisco Secure ACS, authorizes requested network services.

For Cisco Secure ACS to interact with an external user database, Cisco Secure ACS requires an API for a third-party authentication source. The Cisco Secure ACS communicates with the external user database using the API. For Windows 2000 and Generic LDAP, the program interface for the external authentication is local to the Cisco Secure ACS system and is provided by the local operating system. In these cases, no further components are required.

In the case of NDS authentication, the Novell Requestor must be installed on the same Windows Server as Cisco Secure ACS.

In the case of Open Database Connectivity (ODBC) authentication sources, in addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the same Windows Server as Cisco Secure ACS.

To communicate with an RSA Security Inc. token server, you must have installed software components provided by RSA.

For RADIUS-based token servers, such as ActivCard, CRYPTOCard, PassGo, SafeWord, and VASCO, the standard RADIUS interface serves as the third-party API.

Cisco Secure ACS for Windows Server—Database Features

- Database replication
- RDBMS synchronization
- ODBC import

Primary Cisco Secure ACS for Windows Server

NAS

ODBC database
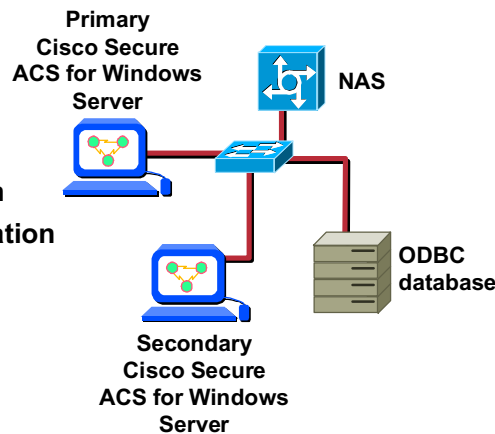
Secondary Cisco Secure ACS for Windows Server

SECUR 1.1—4-13

Database Replication and Remote Database Management System (RDBMS) Synchronization are provided with Cisco Secure ACS for Windows Server. These utilities automate the process of keeping your Cisco Secure ACS database and network configuration current. Cisco Secure ACS for Windows Server supports the import of data from ODBC-compliant databases, such as Microsoft Access and Oracle Corporation databases. Another utility, CSUtil, provides database backup and restore functionality.

Database Replication

Database replication is a powerful feature designed to simplify the construction of a fault-tolerant AAA service environment based on the Cisco Secure ACS for Windows Server. The primary purpose of database replication is to provide the facility to replicate various parts of the configuration and user database on a Cisco Secure ACS primary server to one or more Cisco Secure ACS secondary servers, allowing the administrator to automate the creation of mirror systems. These mirror systems can then be used to provide server load distribution or redundancy by acting as fallback systems to support fault-tolerant operation in case of the failure of the primary system.

Do not confuse database replication with database/system backup. Database replication is not a complete replacement for database backup. You should still have a reliable database backup strategy to ensure data integrity.

RDBMS Synchronization

RDBMS Synchronization is an integration feature designed to simplify integration of Cisco Secure ACS for Windows Server with a third-party RDBMS application. RDBMS Synchronization automates synchronization with another RDBMS data source by providing the following functions:

- Specification of an ODBC data source to use for synchronization data shared by Cisco Secure ACS and the other RDBMS application and to provide control of the Cisco Secure ACS updates to an external application

- Control of the timing of the import/synchronization process including the creation of schedules

- Control of which systems are to be synchronized

The RDBMS Synchronization feature has two components:

- CSDBSync—A dedicated service that performs automated user and group account management services for Cisco Secure ACS.

- An ODBC data store (table)—This table specifies the record format. Each record holds user or group information that corresponds with the data stored for each user in the Cisco Secure ACS database. Additionally, each record contains other fields, including an action code for the record. Any application can write to this table, and CSDBSync reads from it and takes actions on each record it finds in the table (for example, add user, delete user, and so on) as determined by the action code.

OBDC Import Definitions

Cisco Secure ACS supports the import of data from ODBC-compliant databases, such as Microsoft Access or Oracle. Importing is done using a single table to import information into one or more ACS servers.

The CSAccupdate service processes the table and updates local/remote ACS installations according to its configuration.

Cisco Secure ACS for Windows Server Version 3.2—System Requirements

Cisco.com

Go to Cisco.com for the latest specifications for installing Cisco Secure ACS for Windows Server version 3.2.

Before installing Cisco Secure ACS for Windows Server version 3.2, ensure that the host system meets the minimum requirements as specified at Cisco.com. To improve performance, you may choose to increase the RAM, CPU speed, and hard drive speed and capacity of the Cisco Secure ACS for Windows Server system.

Cisco Secure ACS for Windows Server—System Architecture

• **Provides ACS to multiple Cisco authenticating devices**
• **Comprises several modular Windows 2000 services, operating together on one server**

NAS 1
NAS 2
NAS 3

Administration service
Authentication service
Authorization service
TACACS+ service
RADIUS service
Logging service
Sync service
Monitor service
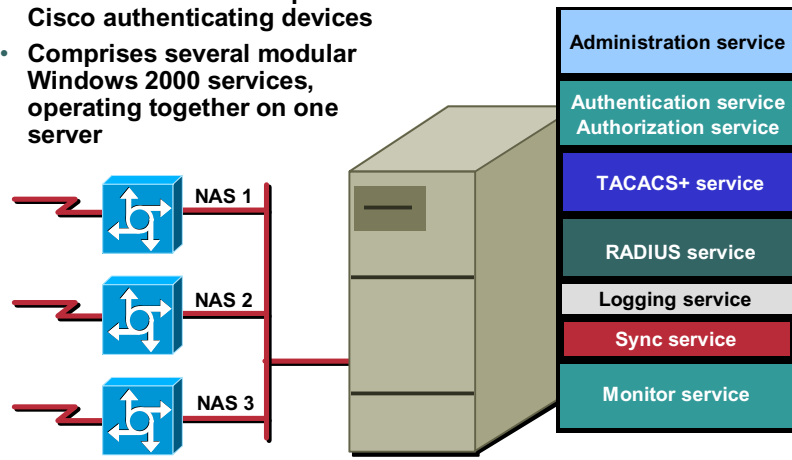
SECUR 1.1—4-15

Cisco Secure ACS for Windows Server provides AAA services for multiple routers. It includes seven service modules. Each module can be started and stopped individually from within the Microsoft Service Control Panel or as a group from within the Cisco Secure ACS for Windows Server browser interface.

- Administration service (CSAdmin)—Cisco Secure ACS for Windows Server is equipped with its own internal web server. After Cisco Secure ACS for Windows Server is installed, you must configure it from its HTML/Java interface, which requires CSAdmin to always be enabled.

- Authentication and authorization service (CSAuth)—The primary responsibility of Cisco Secure ACS for Windows Server is the authentication and authorization of requests from devices to permit or deny access for a specified user. CSAuth is the service responsible for determining if access should be granted and defining the privileges associated with that user. CSAuth is the database manager.

- TACACS and RADIUS service (CSTacacs and CSRadius)—These services communicate between the CSAuth module and the access device requesting the authentication and authorization services. CSTacacs is used to communicate with TACACS+ devices and CSRadius to communicate with RADIUS devices. Both services can run at the same time. When only one security protocol is used, only the respective service needs to be running.

- Logging service (CSLog)—The service used to capture and store logging information. CSLog gathers data from the TACACS+ or RADIUS packet and CSAuth and manipulates the data to be put into the CSV files. The CSV files are created daily starting at midnight.

- Database synchronization service (CSDBSync)—Provides RDBMS synchronization services for Cisco Secure ACS for Windows Server.

- Monitoring service (CSMonitor)—Cisco Secure ACS for Windows Server monitors itself and attempts to correct system problems using the CSMonitor service.

Cisco Secure ACS for Windows Server—ACS User Database
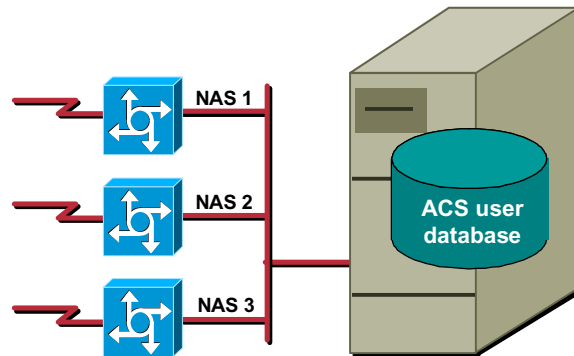
The Cisco Secure ACS user database is crucial for the authorization process. Regardless of whether a user is authenticated by the internal user database or by an external user database, Cisco Secure ACS authorizes network services for users based upon group membership and specific user settings found in the Cisco Secure ACS user database. Thus, all users authenticated by Cisco Secure ACS, even those authenticated by an external user database, have an account in the Cisco Secure ACS user database.

Note:	You can use external user databases only to authenticate users and to determine which group Cisco Secure ACS assigns a user to. The Cisco Secure ACS user database, internal to Cisco Secure ACS for Windows Server, provides all authorization services. With few exceptions, Cisco Secure ACS cannot retrieve authorization data from external user databases. For more information on using external databases, see Cisco.com.

The Cisco Secure ACS user database draws information from several data sources, including a memory-mapped, hash-indexed file, VarsDB.MDB (in Microsoft Jet database format), and the Windows Registry. VarsDB.MDB uses an index and tree structure, so searches can occur logarithmically rather than linearly, thus yielding very fast lookup times. This structure enables the Cisco Secure ACS user database to authenticate users quickly.

Unless you have configured Cisco Secure ACS to authenticate users with an external user database, Cisco Secure ACS uses usernames and passwords in the Cisco Secure ACS user database during authentication.

There are five ways to create user accounts in the Cisco Secure ACS user database. Of these, RDBMS Synchronization and CSUtil.exe support importing user accounts from external sources. The five methods are:

- Cisco Secure ACS HTML interface—The HTML interface provides the ability to create user accounts manually, one user at a time. Regardless of how a user account was created, you can edit a user account by using the HTML interface.

- Unknown User Policy—The Unknown User Policy enables Cisco Secure ACS to add users automatically when a user without an account in the Cisco Secure ACS user database is found in an external user database. The creation of a user account in the Cisco Secure ACS user database occurs only when the user attempts to access the network and is successfully authenticated by an external user database.

- RDBMS Synchronization—RDBMS Synchronization enables you to create large numbers of user accounts and to configure many settings for user accounts. It is recommended that you use this feature whenever you need to import users in bulk; however, setting up RDBMS Synchronization for the first time requires several important decisions and time to implement them.

- CSUtil.exe—The CSUtil.exe command-line utility provides a simple means of creating basic user accounts. Compared to RDBMS Synchronization, its functionality is limited; however, it is simple to prepare for importing basic user accounts and assigning users to groups.

- Database Replication—Database Replication creates user accounts on a secondary Cisco Secure ACS by overwriting all existing user accounts on a secondary Cisco Secure ACS with the user accounts from the primary Cisco Secure ACS. Any user accounts unique to a secondary Cisco Secure ACS are lost in the replication.

How Cisco Secure ACS for Windows Server Works—Using ACS Database Alone
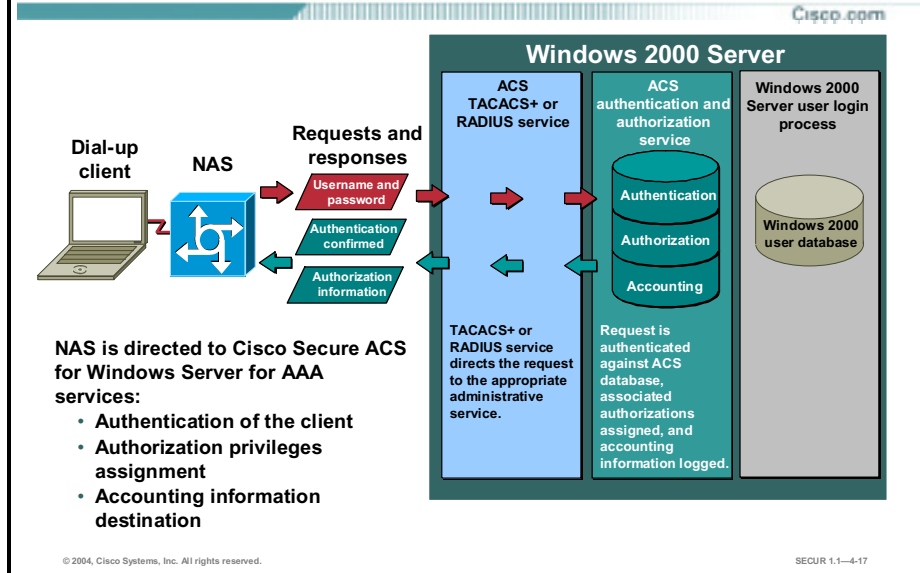
Using either the RADIUS or TACACS+ protocol, the network access server directs all dial-in user access requests to Cisco Secure ACS for Windows Server for authentication and authorization of privileges, which verifies the username and password. Cisco Secure ACS then returns a success or failure response to the network access server, which permits or denies user access. When the user has been authenticated, Cisco Secure ACS sends a set of authorization attributes to the network access server, and the accounting functions take effect.

When the Cisco Secure ACS user database is used alone, the following service and ACS user database interaction occurs:

■ The TACACS+ or RADIUS service directs request to the Cisco Secure ACS authentication and authorization service, where the request is authenticated against the Cisco Secure ACS user database, associated authorizations are assigned, and accounting information is logged to the Cisco Secure ACS logging service.

■ The Windows 2000 user database does not authenticate and grant dial permission as a local user. The user may log in to Windows 2000 once the dial-up AAA process is complete.

How Cisco Secure ACS for Windows Server Works—Using Windows Database
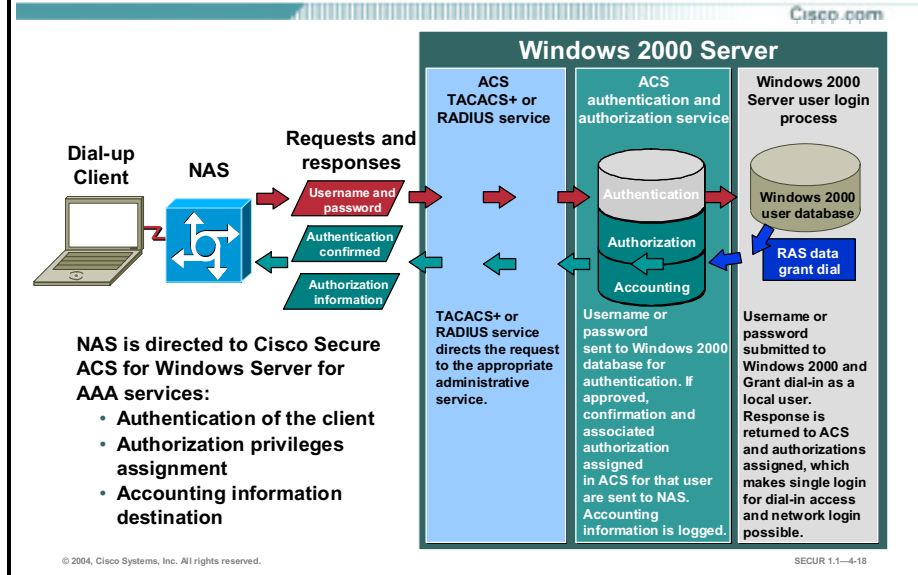
When Cisco Secure ACS for Windows Server uses the Windows 2000 Server user database for AAA, the following service and database interaction occurs:

- TACACS+ or RADIUS service directs request to the Cisco Secure ACS Authentication and Authorization service, where the username and password are sent to the Windows 2000 user database for authentication.

- If approved, Windows 2000 Server grants dial permission as a local user.

- A response is returned to Cisco Secure ACS and authorizations are assigned.

- Confirmation and associated authorizations assigned in Cisco Secure ACS for that user are sent to the network access server. Accounting information is logged.

- Using the Windows 2000 user database makes single login for dial-in and network login possible.

An added benefit of using the Windows 2000 user database is that the username and password used for authentication are the same used for network login. As such, you can require users to enter their username and password once, for the convenience of a simple, single login.

Cisco Secure ACS for Windows Server—External User Databases
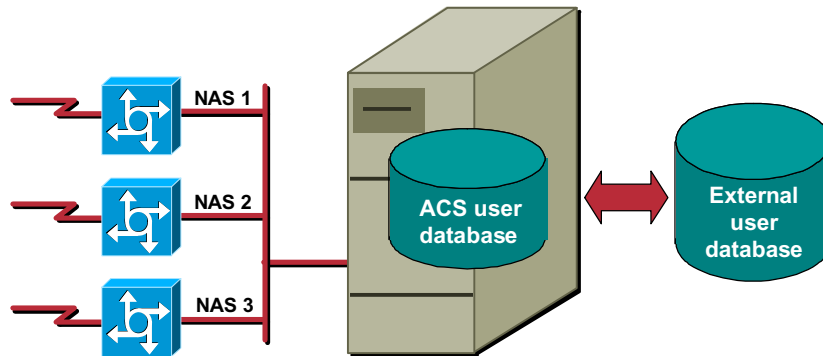
SECUR 1.1—4-19

You can configure Cisco Secure ACS for Windows Server to forward authentication of users to one external user database or more. Support for external user databases means that Cisco Secure ACS for Windows Server does not require that you create duplicate user entries in the Cisco Secure ACS user database. In organizations in which a substantial user database already exists, Cisco Secure ACS can leverage the work already invested in building the database without any additional input.

For Cisco Secure ACS to interact with an external user database, Cisco Secure ACS requires an API for third-party authentication. Cisco Secure ACS communicates with the external user database using the API. For Windows user databases and Generic LDAP, the program interface for the external authentication is local to Cisco Secure ACS. In these cases, no further components are required.

In the case of NDS authentication, Novell Requestor must be installed on the same Windows server as Cisco Secure ACS.

In the case of ODBC authentication sources, in addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the Cisco Secure ACS for Windows Server.

To communicate with an RSA token server, you must have installed software components provided by RSA.

For RADIUS-based token servers, such as ActivCard, CRYPTOCard, PassGo, SafeWord, and VASCO, the standard RADIUS interface serves as the third-party API.

In addition to performing authentication for network access, Cisco Secure ACS can perform authentication for TACACS+ enable privileges using external user databases. For more information regarding the configuration of TACACS+ enable privileges see Cisco.com.

Cisco Secure ACS for Windows Server—Token Card Server Support

Token card server

Cisco Secure ACS

Proprietary protocols

TACACS+ or RADIUS

- LEAP proxy RADIUS servers
- RSA SecurID token servers
- RADIUS-based token servers, including:
  – ActivCard token servers
  – CRYPTOCard token servers
  – VASCO token servers
  – PassGo token servers
  – SafeWord token servers
  – Generic RADIUS token servers

Token card

3178454

SECUR 1.1—4-20
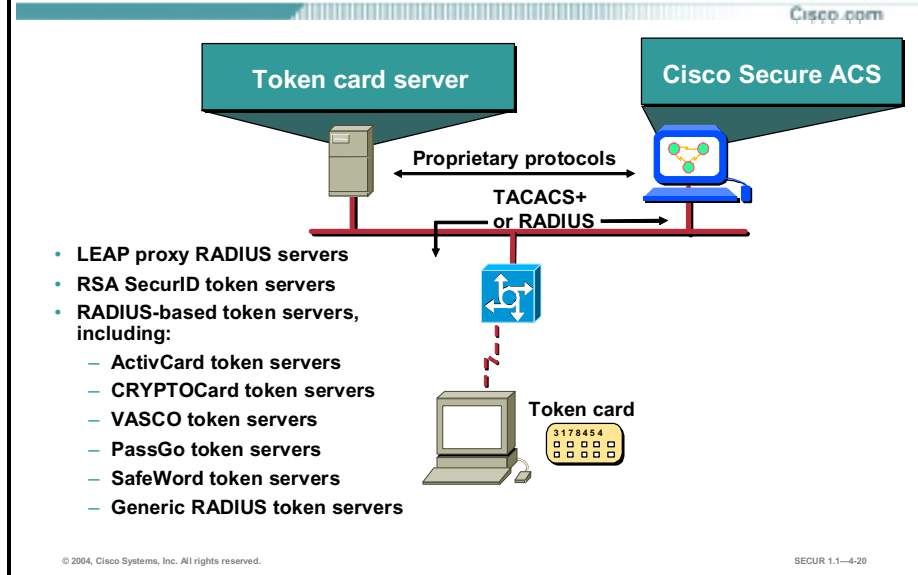
Cisco Secure ACS for Windows Server supports several third-party token servers. For some token servers, Cisco Secure ACS acts as a client to the token server. For others, it uses the token server's RADIUS interface for authentication requests. As with the Windows 2000 database, after the username is located in the Cisco Secure ACS user database, CSAuth can check the selected token server to verify the username and token-card password. The token server then provides a response approving or denying validation. If the response is approval, CSAuth knows that authentication should be granted for the user.

Cisco Secure ACS for Windows Server can support token servers using the RADIUS server built into the token server. Rather than using the vendor's proprietary API, Cisco Secure ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server.

Cisco Secure ACS for Windows Server supports any token server that is a RADIUS server compliant with IETF RFC 2865. So, in addition to the RADIUS-enabled token server vendors explicitly supported, you can use any token server that supports RADIUS-based authentication.

You can create multiple instances of each of these token server types in Cisco Secure ACS for Windows Server.

Cisco Secure ACS for Windows Server—User-Changeable Passwords
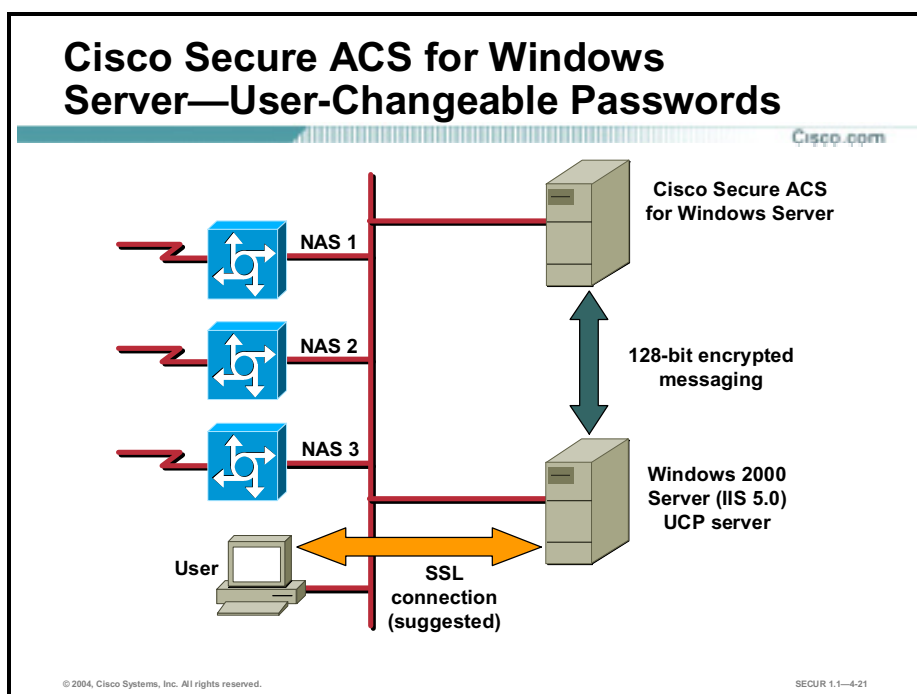
Starting with Cisco Secure ACS for Windows Server version 3.2, system administrators can enable User-Changeable Password (UCP). UCP is an application that enables users to change their Cisco Secure ACS passwords with a web-based utility. To install UCP, you must have a web server that runs Microsoft Internet Information Server (IIS) 5.0 or later.

When users need to change passwords, they can access the UCP server web page using a supported web browser. The UCP web page requires users to log in. The password required is the PAP password for the user account. UCP authenticates the user with Cisco Secure ACS and then allows the user to specify a new password. UCP changes both the PAP and CHAP passwords for the user to the password submitted.

Communication between the UCP server and the Cisco Secure ACS for Windows Server system is protected with 128-bit encryption. To further increase security, it is recommended that you implement SSL to protect communication between user web browsers and the UCP server.

The SSL protocol provides security for remote access data transfer between the UCP web server and the user's web browser. Because users change their Cisco Secure ACS database passwords over a connection between their web browsers and Microsoft IIS, user and password data is vulnerable. The SSL protocol encrypts data transfers, including passwords, between web browsers and Microsoft IIS.

Product Overview—Cisco Secure ACS for UNIX (Solaris)

Cisco Secure ACS for UNIX is used to authenticate users and determine which internal networks and services they may access. By authenticating users against a database of user and group profiles, Cisco Secure ACS for UNIX effectively secures private enterprise and service provider networks from unauthorized access.

Cisco Secure ACS for UNIX incorporates a multiuser, web-based Java configuration and management tool that simplifies server administration and enables multiple system administrators to simultaneously manage security services from multiple locations. The GUI supports Microsoft and Netscape web browsers, providing multi-platform compatibility and offering secure administration via the industry-standard SSL communication mechanism.

Token cards from CRYPTOCard, Secure Computing Corporation, and Security Dynamics Technologies are supported. Token cards are the strongest available method used to authenticate users dialing in and prevent unauthorized users from accessing proprietary information. Cisco Secure ACS for UNIX now supports industry-leading relational database technologies from Sybase Inc. and Oracle. Traditional scalability, redundancy, and nondistributed architecture limitations are removed with the integration of relational database technologies such as Sybase's SQL Anywhere. Storage and management of user and group profile information is greatly simplified.

Cisco Secure ACS for UNIX (Solaris) Features

- **Secures a network for dial-in access and also for managing routers**
- **Uses TACACS+ or RADIUS security protocols**
- **Provides authentication, authorization, and accounting (AAA)**
- **Relational database support—Oracle, Sybase, SQL Anywhere**
- **MaxSessions—Limits the number of logins or B channels per user**
- **Account disable after n failed attempts**
- **Web-based management interface**

SECUR 1.1—4-23

Security is an increasingly important aspect of the growth and proliferation of LANs and WANs. You want to provide easy access to information on your network, but you also want to prevent access by unauthorized personnel. Cisco Secure ACS for UNIX is designed to help ensure the security of your network and track the activity of people who successfully connect to your network. Cisco Secure ACS for UNIX uses the TACACS+ protocol to provide this network security and tracking.

TACACS+ uses AAA to provide network access security and enable you to control access to your network from a central location. Each facet of AAA significantly contributes to the overall security of your network, as follows:

- Authentication determines the identity of users and whether they should be allowed access to the network.

- Authorization determines the level of network services available to authenticated users once they are connected.

- Accounting keeps track of each user's network activity.

- AAA within a client or server architecture (in which transaction responsibilities are divided into two parts: client [front end], and server [back end]) allows you to store all security information in a single, centralized database instead of distributing the information around the network in many different devices.

You can use Cisco Secure ACS for UNIX to make changes to the database that administers security on your network on a few security servers instead of making changes to every NAS in your network.

Using Cisco Secure ACS for UNIX, you can expand your network to accommodate more users and provide more services without overburdening system administrators with security issues. As new users are added, system administrators can make a small number of changes in a few places and still ensure network security.

Cisco Secure ACS for UNIX can be used with the TACACS+ protocol, the RADIUS protocol, or both. Some features are common to both protocols, while other features are protocol-dependent.

The Cisco Secure ACS for UNIX has the following features when used with either the TACACS+ or RADIUS protocol:

- Support for use of common token card servers including CRYPTOCard, Secure Computing (formerly Enigma Logic), and Security Dynamics Inc. (SDI)

- Relational database support

- Encrypted protocol transactions so passwords are never subject to unauthorized monitoring

- Supported on SPARC Solaris version 2.51 or greater

- Support for group membership

- Support for accounting

- Support for S/Key authentication

- Ability to specify the maximum number of sessions per user

- Ability to disable an account after n failed attempts

- Web-based interface for easy administration of network security

Customers can upgrade to any 2.x version of Cisco Secure ACS for UNIX from existing versions, gaining access to the many user-friendly features of the latest version of Cisco Secure ACS for UNIX.

The Cisco Secure ACS for UNIX 2.3 adds the Distributed Systems Manager (DSM), which enables system administrators to:

- Limit the number of concurrent sessions that are available to a specific user, group, or VPDN (DSM enabled)

- Set per user session limits for individual users or groups of users (limited support without DSM enabled)

Cisco Secure ACS for UNIX (Solaris) Minimum System Requirements

Cisco.com

Go to Cisco.com for the latest specifications for installing Cisco Secure ACS for UNIX.

SECUR 1.1—4-24

Before installing Cisco Secure ACS for UNIX 2.3 on a Solaris platform, ensure that the system meets the minimum requirements as specified on Cisco.com.

Product Overview—Cisco Secure ACS Solution Engine

This topic covers the Cisco Secure ACS Solution Engine.

The Cisco Secure ACS Solution Engine is a headless server that performs many of the same functions as the Cisco Secure ACS for Windows Server version 3.2 product. Additional functionality has been added to manage the engine itself using both a serial console port interface and a customized web interface.

Compared to the Cisco Secure ACS for Windows Server product, the Cisco Secure ACS Solution Engine reduces the total cost of ownership by eliminating the need to install and maintain a Microsoft Windows 2000 Server machine.

- **Hewlett-Packard ProLiant DL320 G2 server (Cisco 1111 hardware platform)**
  - **Intel 2.26 GHz Pentium 4 processor (512-KB level 2 ECC cache)**
  - **1-GB RAM**
  - **Two built-in NC7760 PCI Gigabit Ethernet server adapters**
  - **40-GB ATA hard disk drive**
  - **Floppy disk drive**
  - **CD-ROM drive**
  - **Serial port**
- **Uses serial port for console connection**
- **Additional hardware that is not used includes mouse and keyboard controllers, parallel port, and video port**

SECUR 1.1—4-27

The Cisco Secure ACS Solution Engine is built on a Hewlett-Packard ProLiant DL320 G2 server rack-mountable (1U) platform. For security reasons, the following hardware interfaces are not used:

- Mouse port

- Keyboard port

- Parallel port

- Video port

Note:	Even though the video, mouse, and keyboard ports are active, the Cisco Secure ACS Solution Engine does not allow GUI login to the Windows 2000 Server system. Also, the engine utilizes only one of the two installed Ethernet adapters.

The Cisco Secure ACS Solution Engine uses a standard BIOS with serial console port redirection and Flash memory. A small portion of the Flash memory is used to store an engine signature (appliance type). During an engine upgrade, the upgrade process reads this signature to ensure that the correct device is being upgraded.

**Cisco Secure ACS Solution Engine—
Software Platform**

• **Security-hardened operating system**
  - **Uses the Microsoft Windows 2000
    Server kernel (no access to file system)**
  - **Only services necessary for Cisco
    Secure ACS functions are enabled**
  - **Does not use IIS (not installed)**
  - **File and print sharing disabled**
  - **Does not allow installation of arbitrary
    applications**
• **Limited TCP/IP port connections**
• **Serial console and web interface
  administrative access**
• **Backup/restore of ACS data using FTP**
• **Secure recovery procedures**

SECUR 1.1—4-28

The Cisco Secure ACS Solution Engine utilizes a hardened implementation of the Microsoft Windows 2000 Server kernel. This hardened operating system is much more secure than a standard Windows Server machine for the following reasons:

■ Automatic reboot on crash—The operating system is designed to automatically reboot if a system crash occurs. In addition, the following components may be automatically restarted:

— Console port service restart—The console process is designed to automatically restart if it fails.

— Cisco Secure ACS service restart—The Cisco Secure ACS monitors all ACS services and automatically restarts them if they fail.

■ No Windows GUI login—The ability to login to Windows Server has been removed from the engine operating system. This helps prevent unauthorized access to the engine file system and installation of non-Cisco Secure ACS applications. The engine has a single operating system account, used by the console. The username and password for the single operating system account are by default, preset by the factory. During initial engine configuration, the installer is asked to change this default username/password combination.

■ No IIS—Microsoft IIS is not used or installed on the engine. This eliminates any traditional security threats associated with IIS installations.

■ Essential services only—Only those system services essential to the operation of the engine are enabled. Traditional services such as file and print sharing are disabled. Only the following operating system services are active:

— COM+ Event System

— Dynamic Host Configuration Protocol (DHCP) Client (only if engine is using DHCP)

— DNS Client

— Event Log

— IPSec Policy Agent

- — License Logging Service
- — Logical Disk Manager
- — Network Connections
- — Plug and Play
- — Protected Storage
- — Remote Procedure Call (RPC)
- — Removable Storage
- — RunAs Service
- — Security Accounts Manager
- — Server
- — System Event Notification
- — Telnet Service (required by serial console)
- — Windows Management Instrumentation (WMI)
- — Windows Management Instrumentation Driver Extensions

Note: Operating System services are not accessible remotely due to packet filtering.

- Packet filtering blocks traffic on all but necessary IP ports. Only the ports shown in this table are open:

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication and authorization (draft RFC)	1645	
RADIUS accounting (draft RFC)	1646	
RADIUS authentication and authorization (revised RFC)	1812	
RADIUS accounting (revised RFC)	1813	
Proxy DLLs (RSA)	5500-5509	
TACACS+ authentication, authorization, and accounting		49
ACS replication		2000
ACS logging		2001
ACS distributed logging		2003
ACS HTTP administration		2002
ACS HTTPS administration		2002
ACS administration port range		Dynamic range (see note)

Note: The Cisco Secure ACS Solution Engine assigns unique port numbers from this range for each administrative session. The range is defined using the engine Administration control/Access policy web page.

The Cisco Secure ACS Solution Engine runs the same code as the software version of Cisco Secure ACS for Windows Server version 3.2. In most cases Cisco Secure ACS works the same way on the engine as the software version. When it is necessary to operate differently, the version 3.2 software senses that it is operating on an engine by checking the platform type (found in the registry). The following Cisco Secure ACS components operate differently when running on the Cisco Secure ACS Solution Engine:

- Backup/restore—The engine uses an external FTP server instead of the local file system for Cisco Secure ACS data backup and restore.

- Login—The engine allows only administrator access.

The Cisco Secure ACS Solution Engine ships with a recovery CD that can be used in the following instances:

- Lost administrative password—The recovery CD can be used to reset the password to the factory default. For this reason, it is extremely important that you secure the recovery CD.

- Corrupted hard drive—The recovery CD can be used to reimage the engine hard drive, returning it to the factory default configuration. This is, of course, another very important reason to secure the recovery CD.

Warning   The Cisco Secure ACS Solution Engine Recovery CD can be used to reset the engine
administrative password or return the engine hard drive to the default factory image. For
obvious reasons, it is extremely important that you secure all Cisco Secure ACS Solution
Engine Recovery CDs.

The Cisco Secure ACS Solution Engine provides nearly the same features and functions as the Cisco Secure ACS for Windows Server—in a dedicated, security-hardened, application-specific option. The engine version of Cisco Secure ACS differs from the Windows Server version as noted here:

- Authentication as performed by the Cisco Secure ACS Solution Engine differs from authentication as performed by the Cisco Secure ACS Windows Server in the following ways:

    — Solution Engine authentication against a Windows domain requires a Cisco Secure ACS remote agent running on a domain controller or member server. The Cisco Secure ACS remote agent is necessary to establish a Windows member or domain controller trust relationship.

    — Solution Engine authentication against an ODBC source is not supported. LDAP authentication can be used instead.

    — Solution Engine authentication against OTP directories is performed using the generic RADIUS-based OTP interface on the engine. Any OTP vendor that provides an RFC-compliant RADIUS interface can interface with Cisco Secure ACS.

- User database synchronization—User database synchronization with an ODBC source is not supported. Instead, the administrator can configure Cisco Secure ACS to synchronize its user database with a CSV file on a remote FTP server.

- ODBC logging—ODBC logging is not supported. Administrators can use local or remote CSV logging.

- Backup/restore and engine diagnostics—Backup/restore and gathered engine diagnostics are performed through a remote FTP server and configured using the current Cisco Secure ACS HTML GUI.

Installing Cisco Secure ACS for Windows Server Version 3.2

Cisco Secure ACS for Windows Server is easy to install and configure. This topic presents a brief overview of the essential installation steps. The following discussion is based on a PPP dial-up user being authenticated against Cisco Secure ACS for Windows Server using the Windows 2000 user database, via the TACACS+ protocol.

Cisco Secure ACS for Windows Server—Installation Overview

Cisco.com

- Step 1—Preconfigure Windows 2000 Server system.
- Step 2—Verify connection between Windows 2000 Server system and Cisco routers.
- Step 3—Install Cisco Secure ACS for Windows Server on the Windows 2000 Server system.
- Step 4—Initially configure Cisco Secure ACS for Windows Server via web browser.
- Step 5—Configure routers for AAA.
- Step 6—Verify correct installation and operation.

SECUR 1.1—4-30

The Cisco Secure ACS installation can be condensed to the following steps:

Step 1   Preconfigure the Windows 2000 Server system.

Step 2   Verify a basic network connection between the Windows 2000 Server and the router or routers using ping and Telnet.

Step 3   Install Cisco Secure ACS for Windows Server on the Windows 2000 Server system.

Step 4   Initially configure Cisco Secure ACS for Windows Server via the web browser interface.

Step 5   Configure the router or routers for AAA.

Step 6   Verify correct installation and operation.

Preconfigure the Windows 2000 Server System

The first step to follow when installing Cisco Secure ACS for Windows Server is to configure the Windows 2000 Server system by doing the following:

■ Determine Windows 2000 Server type—This decision must be made based on the design of the Windows 2000 Server architecture of your company.

■ Configure Windows 2000 User Manager.

■ Use Windows 2000 Server services to control Cisco Secure ACS.

■ Cisco does not recommend that you install Cisco Secure ACS for Windows Server on PDCs or BDCs.

Note:	If you are upgrading from a previous version of Cisco Secure ACS that is running on Windows NT 4.0, you cannot upgrade the operating system to Windows 2000 Server. This is because the setup program for previous versions of Cisco Secure ACS detected which Windows operating system the computer used and customized Cisco Secure ACS for that operating system. As a result, upgrading the operating system to Windows 2000 Server without also installing the new version of Cisco Secure ACS for Windows Server causes Cisco Secure ACS to fail.

Verify Connections Between Windows 2000 Server System and Other Network Devices

Verify that the NAS or router can ping the Windows 2000 Server system that will host Cisco Secure ACS for Windows Server. This verification will simplify installation and eliminate problems when configuring Cisco Secure ACS for Windows Server and devices that interface with it.

Cisco Secure ACS for Windows Server is easy to install from a CD-ROM. It installs like any other Windows application, using an InstallShield template. Before you begin the installation, ensure you have NAS information such as hostname, IP address, and TACACS+ key.

Install Cisco Secure ACS for Windows Server on the Windows 2000 Server System

Follow the InstallShield instructions as listed below:

■ Select and configure the database.

■ Configure Cisco Secure ACS for Windows Server for NAS or router using the web browser.

■ Configure the NAS or router for Cisco Secure ACS for Windows Server.

Configure Cisco Secure ACS for Windows Server Using the Web Browser

After successfully installing Cisco Secure ACS for Windows Server, a Cisco Secure icon labeled ACS Admin appears on the Windows 2000 Server desktop. You need to continue initially configuring Cisco Secure ACS for Windows Server with the web browser interface as follows:

■ Cisco Secure ACS for Windows Server supports only HTML; a web browser is the only way to configure it. Cisco Secure ACS for Windows Server version 3.2 supports the following English-language version browsers:

— Microsoft Internet Explorer version ≥ 6.0 (with Service Pack 1) for Microsoft Windows

— Netscape version ≥ 7.0 for Microsoft Windows

— Netscape version ≥ 7.0 for Solaris 2.7

Note: Browsers must have Java and JavaScript enabled with HTTP proxy disabled.

■ Selecting the Admin icon launches the browser with the address http://127.0.0.1:2002/.

■ The address http://<ip address>:2002/ and http://<host name>:2002/ also works.

After you have installed Cisco Secure ACS for Windows Server, you configure and manage it through the web-based GUI. The GUI is designed using frames, so you must view it with a supported web browser.

Configure Remaining Devices for AAA

You must configure the NAS, routers, and switches to work with Cisco Secure ACS. Specific configuration of these devices is covered in later lessons.

You may also need to configure a token card server to work with Cisco Secure ACS to perform AAA.

Here are some of the possible configuration combinations where Cisco Secure ACS is used to perform AAA. In each configuration, each of the devices must be configured to work with Cisco Secure ACS:

1. Dial-in access using the Windows 2000 user database with TACACS+

2. Dial-in access using the Cisco Secure ACS user database with TACACS+

3. Dial-in access using a token card server with TACACS+

4. Dial-in access using the Cisco Secure ACS user database with RADIUS (Cisco)

5. Dial-in access for an ARAP client using the Cisco Secure ACS user database with TACACS+

6. Router management using the Cisco Secure ACS user database with TACACS+

7. PIX Firewall authentication/authorization using the Windows 2000 user database with TACACS+

Administering and Troubleshooting Cisco Secure ACS for Windows Server Version 3.2

The next topic covers administering and troubleshooting Cisco Secure ACS for Windows Server.

Cisco Secure ACS for Windows Server—Administration Procedures

- **User setup**
- **Group setup**
- **Shared profile components**
- **Network configuration**
- **System configuration**
- **Interface configuration**
- **Administration control**
- **External user databases**
- **Reports and activity**
- **Online documentation**

　　　　　　　SECUR 1.1—4-32

The Cisco Secure ACS for Windows Server web browser interface makes administration of AAA features easy.

Each of the buttons on the navigational bar represents a particular area or function that you can configure. Depending on your configuration, you may not need to configure all of the areas. Select one of these buttons to begin configuring:

- User Setup—Add, edit, delete user accounts, list users in databases.

- Group Setup—Create, edit, rename groups, list all users in a group.

- Shared Profile Components—Develop and name reusable, shared sets of authorization components which may be applied to one or more users or groups of users and referenced by name within their profiles. Components include network access restrictions (NARs), command authorization sets, and downloadable PIX Firewall access control lists (ACLs).

- Network Configuration—Configure and edit network access server parameters; add and delete network access servers; configure AAA server distribution parameters.

- System Configuration—Start and stop Cisco Secure ACS for Windows Server services, configure logging, control database replication, control RDBMS synchronization.

- Interface Configuration—Configure user defined fields that will be recorded in accounting logs; configure TACACS+ and RADIUS options, control display of options in the user interface.

- Administration Control—Control administration of Cisco Secure ACS from any workstation on the network.

- External User Databases—Configure the unknown user policy; configure authorization privileges for unknown users; configure external database types.

- Reports and Activity—Select **Reports & Activity** in the navigational bar to view the following information. You can import these files into most database and spreadsheet applications. Here is a partial list of the types of reports available to you when accessing Reports & Activity:

    — TACACS+ Accounting Report—Lists when sessions stop and start; records network access server messages with username; provides caller line identification information; records the duration of each session

    — RADIUS Accounting Report—Lists when sessions stop and start; records network access server messages with username; provides caller line identification information; records the duration of each session

    — Failed Attempts Report—Lists authentication and authorization failures with an indication of the cause

    — Logged-In Users—Lists all users currently receiving services for a single network access server or all network access servers with access to Cisco Secure ACS

    — Disabled Accounts—Lists all user accounts that are currently disabled

    — Admin Accounting Reports—Lists configuration commands entered on a TACACS+ (Cisco) network access server

- Online Documentation—Provides more detailed information about the configuration, operation, and concepts of Cisco Secure ACS for Windows Server.

Cisco Secure ACS for Windows Server—Main Window

The previous bulleted list follows the order of the buttons in the navigational bar, as shown in the figure. The order to follow for configuration depends on your preferences and needs. One typical order of configuration is as follows:

Step 1 Administration Control—Configure access for remote administrators.

Step 2 NAS Configuration—Configure and verify connectivity to a network access server.

Step 3 Group Setup—Configure available options and parameters for specific groups. All users must belong to a group.

Step 4 User Setup—Add users to a group that is configured.

Step 5 All other necessary areas.

Cisco Secure ACS for Windows Server—Troubleshooting

Failed Attempts 2002-12-06.csv

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port	NAS-IP-Address
12/06/2002	12:59:46	Author failed	aaauser	Default Group	10.1.2.12		Service denied	service=auth-proxy cmd*	Ethernet0/0	10.0.2.2
12/06/2002	12:58:31	Author failed	aaauser	Default Group	10.1.2.12		Service denied	service=auth-proxy cmd*	Ethernet0/0	10.0.2.2
12/06/2002	12:38:10	Authen failed	andy	u-in	async	CS password invalid			tty0	10.0.2.2

- Use the Failed Attempts Report under Reports and Activity as a starting point.
- Provides a valuable source of troubleshooting information.

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—4-34

Start troubleshooting Cisco Secure ACS-related AAA problems by examining the Failed Attempts Report under Reports and Activity. The report shows several types of failures.

Authentication Failure

Assuming that Cisco Secure ACS and the router are communicating, you can check the following.

If authenticating against the Windows 2000 user database, check these items:

- Are the username and password being entered correctly? (The password is case sensitive.)
- Do the username and password exist in the Windows 2000 user database? (Check in User Manager.)
- Is the dial-in interface on the network access server configured with the **ppp authentication pap** command?
- Is the User must change password at next login check box selected in Windows 2000 Server? (Deselect it if it is.)
- Does the username have the rights to log on locally in the Windows 2000 Server window (Trust Relationship/Domain)?
- Is Cisco Secure ACS configured to authenticate against the Windows 2000 user database?
- Is Cisco Secure ACS configured to reference the grant dial-in permission to user setting (Trust Relationship/Domain)?
- If the username was able to authenticate before and cannot now, is the account disabled on Windows 2000 Server or Cisco Secure ACS?
- Has the password expired on Windows 2000 Server?
- Does the username contain an illegal character?

- Windows 2000 Server will send domain name and username for authentication if using dial-up networking.

Authorization Failure

If the dial-in user is authenticating, but authorization is failing, check the following:

- Are the proper network services checked in the Group Settings area?

- If IP is checked, how is the dial-in user obtaining an IP address?

- Is there an IP pool configured on the NAS?

- Is the name of the IP pool entered in the Group Settings area? (Leave blank if a default IP pool has been configured.)

- If authorizing commands, has the **aaa authorization commands 1 tacacs+** command been entered in to the Cisco IOS software configuration? (The "1" can be substituted for any privilege level from 0–15.)

- Has the Permitted radio button for the command been selected?

- Has the Permitted radio button for the argument been selected?

No Entry In the Failed Attempts Report

If AAA is not working, yet there is no entry in the report, there is an invalid setup between Cisco Secure ACS and the router. Check the following items to troubleshoot this:

- Can the router ping the Cisco Secure ACS for Windows Server system?

- Can the Cisco Secure ACS for Windows Server system ping the router?

- Is the TACACS+ host IP address correctly configured in the router?

- Is the identical TACACS+ host key entered on both the router and Cisco Secure ACS?

- Is TACACS+ accounting configured on the router?

Dial-In Client PC Problems

If the dial-in user is a Windows 95 or Windows 98 PC using dial-up networking, here are some things to check:

- Are connection properties configured to use Require encrypted password under Server Type?

- Is the connection configured to use the correct protocol?

- Is the selected dial-in server type "PPP: Windows 95/98, Windows NT 3.5, Internet?"

- Is the user authorized to use a specific command?

Other Troubleshooting Tips

Other problems may be encountered with remote administration. Check the following:

- Ensure that the web browser is correctly configured: enough cache is allocated and Java is enabled.

- Ensure that Remote Administration is configured to allow remote web browser access (IP address, username/password).

Useful Cisco IOS Commands

The following Cisco IOS debug commands are useful for troubleshooting:

```
debug aaa authentication
debug aaa authorization
debug TACACS+
debug RADIUS
```

TACACS+ Overview and Configuration

Terminal Access Controller Access Control System Plus (TACACS+) is an improved version of TACACS. TACACS+ forwards username and password information to a centralized security server.
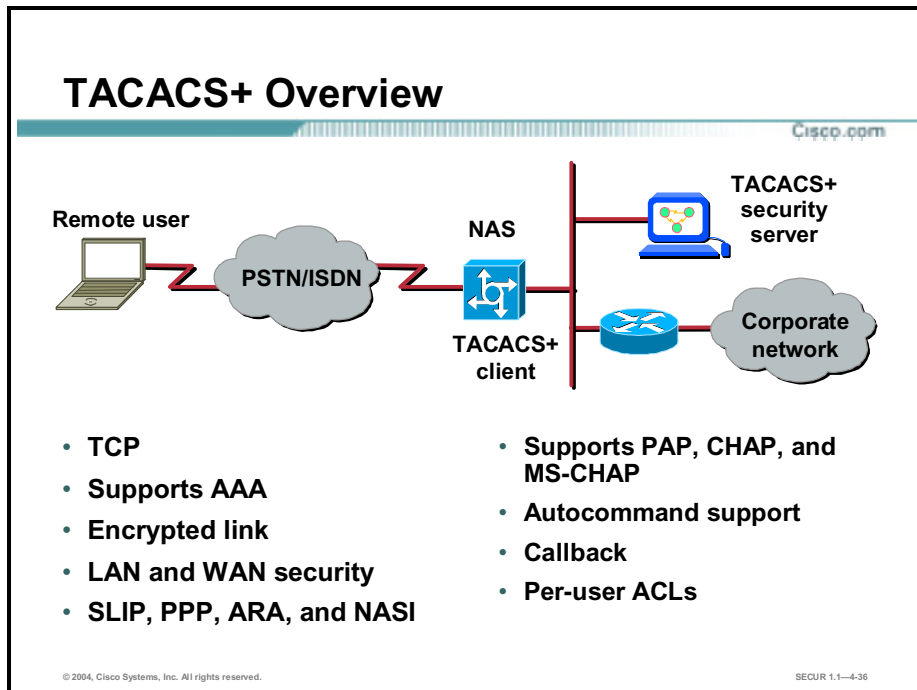
TACACS+ has the following features:

■ TCP packets for reliable data transport—Uses TCP as the communication protocol between the remote client and security server

■ Supports the AAA architecture

■ Link is encrypted—Data payload of IP packets (TCP packets) encrypted for security and stored in encrypted form in the remote security database

■ Supports PAP, CHAP, and MS-CHAP authentication

■ Useful for both LAN and WAN security

■ Serial Line Internet Protocol (SLIP), PPP, and ARA supported for dial-in access security— TN3270 and X.121 addresses used with X.25 also supported

■ Autocommand supported

■ Callback supported

■ Per-user access lists can be assigned in authorization phase

There are three versions of TACACS:

■ TACACS—An industry-standard protocol specification, RFC 1492, that forwards username and password information to a centralized server. The centralized server can be either a TACACS database or a database like the UNIX password file with TACACS protocol support. For example, the UNIX server with TACACS passes requests to the UNIX database and sends the accept or reject message back to the access server.

■ XTACACS—Defines the extensions that Cisco added to the TACACS protocol to support new and advanced features. XTACACS is multiprotocol and can authorize connections with SLIP, enable, PPP (IP or Internetwork Packet Exchange [IPX]), ARA, EXEC, and Telnet. XTACACS supports multiple TACACS servers, and Syslog for sending accounting information to a UNIX host, connects where the user is authenticated into the access server "shell," and can Telnet or initiate slip or PPP or ARA after initial authentication. XTACACS is essentially obsolete concerning Cisco AAA features and products.

■ TACACS+—Enhanced and continually improved version of TACACS that allows a TACACS+ server to provide the services of AAA independently. Each service can be tied into its own database or can use the other services available on that server or on the network. TACACS+ was introduced in Cisco IOS Release 10.3. This protocol is a completely new version of the TACACS protocol referenced by RFC 1492 and developed by Cisco. It is not compatible with XTACACS. TACACS+ has been submitted to the IETF as a draft proposal.

The rich feature set of the TACACS+ client/server security protocol is fully supported in Cisco Secure ACS software.

Globally Enable AAA

Cisco.com

**Cisco Secure
ACS for Windows Server**

10.1.2.4
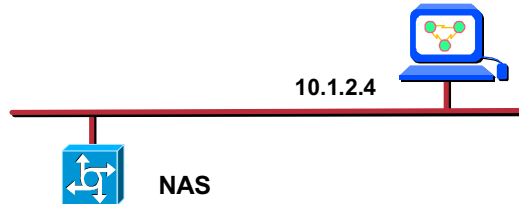
NAS

router(config)#

```
aaa new-model
```

```
router(config)# aaa new-model
```

SECUR 1.1—4-37

The first steps in configuring the router are to enable TACACS+, specify the list of Cisco Secure ACS servers that will provide AAA services for the router, and configure the encryption key that is used to encrypt the data transfer between the router and the Cisco Secure ACS server.

The **aaa new-model** command forces the router to override every other authentication method previously configured for the router lines. If an administrative Telnet or console session is lost while enabling AAA on a Cisco router, and no enable password is specified, the administrator may be locked out of the router.

Warning	When using the Cisco IOS **aaa new-model** command, always provide for an enable password login method. This guards against the risk of being locked out of router should the administrative session fail while you are in the process of enabling AAA, or if the TACACS+ server becomes unavailable.

At a minimum the following commands should be entered in the order shown:

```
Router(config)# aaa new-model
```
```
Router(config)# aaa authentication login default tacacs+ enable
```

Specifying the "enable" authentication method enables you to re-establish your Telnet or console session and use the enable password to access the router once more. If you fail to do this, and you become locked out of the router, physical access to the router is required (console session), with a minimum of having to perform a password recovery sequence. At worst, the entire configuration saved in NVRAM can be lost.

tacacs-server Commands

You can either use the two commands shown here

```
router(config)#
```
```
tacacs-server key keystring
```

```
router(config)# tacacs-server key 2bor!2b@?
```

```
router(config)#
```
```
tacacs-server host ipaddress
```

or

```
router(config)# tacacs-server host 10.1.2.4
```

use this single command (see note in text).

```
router(config)#
```
```
tacacs-server host ipaddress key keystring
```

```
router(config)# tacacs-server host 10.1.2.4 key
    2bor!2b@?
```

To begin global configuration, enter the following commands, using the correct IP address of the Cisco Secure ACS servers and your own encryption key:

```
router(config)# tacacs-server key 2bor!2b@?
router(config)# tacacs-server host 10.1.2.4
router(config)# tacacs-server host 10.1.2.5
```

In this example, the 2bor!2b@? global key is the encryption key that is shared between the router and the two Cisco Secure ACS servers. The encryption key you choose for your environment should be kept secret in order to protect the privacy of passwords that are sent between the Cisco Secure ACS servers and the router during the authentication process.

Note:	The **tacacs-server key** command is used when two or more TACACS+ servers share the same key. If you need to configure multiple TACACS+ servers, each with its own specific key, then you need to use the method shown below.

You can specify multiple Cisco Secure ACS servers, each with its own key, by repeating the **tacacs-server host** command (one for each TACACS+ host and its specific key) as follows:

```
router(config)# tacacs-server host 10.1.2.4 key keyforTACACS1
router(config)# tacacs-server host 10.1.2.5 key keyforTACACS2
```

AAA Configuration Commands

router(config)#

```
aaa authentication {login | enable default | arap | ppp
  | nasi} {default | list-name} method1 [method2
  [method3 [method4]]]
```

router(config)#

```
aaa authorization {network | exec | commands level |
  reverse-access} {default | list-name}
  {if-authenticated | local | none | radius | tacacs+ |
  krb5-instance}
```

router(config)#

```
aaa accounting {system | network | exec | connection |
  commands level}{default | list-name} {start-stop |
  wait-start | stop-only | none} [method1 [method2]]
```

After enabling AAA globally on the access server, define the authentication method lists, apply them to lines and interfaces. These authentication method lists are security profiles that indicate the protocol (ARAP or PPP) or login and authentication method (TACACS+, RADIUS, or local authentication).

To define an authentication method list using the **aaa authentication** command, complete the following steps:

Step 1 Specify the dial-in protocol (ARAP, PPP, or NetWare Access Server Interface [NASI]) or login authentication.

Step 2 Identify a list name or default. A list name is any alphanumeric string you choose. You assign different authentication methods to different named lists. You can specify only one dial-in protocol per authentication method list. However, you can create multiple authentication method lists with each of these options. You must give each list a different name.

Step 3 Specify the authentication method. You can specify up to four multiple methods, such as TACACS+, followed by local in case a TACACS+ server is not available on the network.

After defining these authentication method lists, apply them to one of the following:

■ Lines—tty lines or the console port for login and asynchronous lines (in most cases) for ARA

■ Interfaces—Interfaces (synchronous or asynchronous) configured for PPP

Use the **aaa authentication** command as described in lesson 3, in global configuration mode to enable AAA authentication processes.

NAS AAA Configuration Example for TACACS+

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication ppp default tacacs+
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting exec start-stop tacacs+
aaa accounting network start-stop tacacs+
enable secret 5 $1$x1EE$33AXd2VTVvhbWL0A37tQ3.
enable password 7 15141905172924
!
username admin password 7 094E4F0A1201181D19
!
interface Serial2
 ppp authentication pap
!
tacacs-server host 10.1.1.4
tacacs-server key ciscosecure
!
line con 0
  login authentication no_tacacs
```

SECUR 1.1—4-40

Consider the NAS configuration example in the figure, which has been edited to show only commands important to AAA security:

```
aaa new-model
```

This command enables the AAA access control model. Use the **no** form of this command disables this functionality. You can subsequently restore previously configured AAA commands by reissuing the command.

You could use the **aaa authentication login default tacacs+ enable** command to specify that if your TACACS+ server fails to respond, you can log in to the access server by using your enable password. If you do not have an enable password set on the router, you will not be able to log in to it until you have a functioning TACACS+ Windows 2000 Server process configured with usernames and passwords. The enable password in this case is a last-resort authentication method. You also can specify **none** as the last-resort method, which means that no authentication is required if all other methods failed.

```
aaa authentication login default tacacs+ enable
```

Sets AAA authentication at login using the default list against the TACACS+ server. In this example, the enable password would be used if the TACACS+ server became unavailable.

```
aaa authentication ppp default tacacs+
```

Sets AAA authentication for PPP connections using the default list against the TACACS+ database.

```
aaa authorization exec tacacs+
```

Sets AAA authorization to determine if the user is allowed to run an EXEC shell on the NAS against the TACACS+ database.

```
aaa authorization network tacacs+
```

Sets AAA authorization for all network-related service requests, including SLIP, PPP, PPP network control protocols (NCPs), and ARA protocol against the TACACS+ database. The TACACS+ database and the NAS must be configured to specify the authorized services.

```
aaa accounting exec start-stop tacacs+
```

Sets AAA accounting for EXEC processes on the NAS to record the start and stop time of the session against the TACACS+ database.

```
aaa accounting network start-stop tacacs+
```

Sets AAA accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARA protocol to record the start and stop time of the session against the TACACS+ database.

```
username admin password 7 094E4F0A1201181D19
```

Sets a username and password in the local security database for use with the **aaa authentication local-override** command.

```
interface Serial2
 ppp authentication pap
```

Sets PPP authentication to use PAP. CHAP, or both CHAP, PAP, and MS-CHAP could also be specified. The **ppp authentication if-needed** command causes the NAS to not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.

```
tacacs-server host 10.1.1.4
tacacs-server key ciscosecure
```

The first steps in configuring the router are to:

■ Enable TACACS+.

■ Specify the list of Cisco Secure ACS servers that will provide AAA services for the router.

■ Configure the encryption key that is used to encrypt the data transfer between the router and the Cisco Secure ACS server.

Note: The shared key set with the **tacacs-server key** command specifies the key to be used if a per-host key was not set. It is a better practice to set specific keys per tacacs-server host.

It is possible to configure TACACS+ with no shared key at both the client device (that is, the router) and the security server (that is, Cisco Secure) if one wishes the connection to not be encrypted. This might be useful for a lab or training environment, but is highly discouraged in a production environment.

The **tacacs-server** command is described in the following table:

tacacs-server host (hostname | ip-address)	Specifies the IP address or the host name of the remote TACACS+ server host. This host is typically a UNIX system running TACACS+ software.

tacacs-server key *shared-secret-text-string*	Specifies a shared secret text string used between the access server and the TACACS+ server. The access server and TACACS+ server use this text string to encrypt passwords and exchange responses. The shared key set with the **tacacs-server key** command is a default key to be used if a per-host key was not set. It is a better practice to set specific keys per tacacs-server host. It is possible to configure TACACS+ without a shared key at both the client device (that is, NAS) and the security server (that is, Cisco Secure) if one wishes the connection to not be encrypted. This might be useful for a lab or training environment, but is strongly discouraged in a production environment.

The following command specifies that the AAA authentication list called no_tacacs is to be used on the console:

```
line con 0
 login authentication no_tacacs
```

Verifying TACACS+

This topic explains how to verify AAA TACACS+ operations using Cisco IOS debug commands.

AAA TACACS+ Troubleshooting

router#

```
debug tacacs
```

- **Displays detailed information associated with TACACS+**

router#

```
debug tacacs events
```

- **Displays detailed information from the TACACS+ helper process**

SECUR 1.1—4-42

When TACACS+ is used on a router, you can use the **debug tacacs** command for more detailed debugging information.

Use the following **debug** command on the router to trace TACACS+ packets:

```
debug tacacs
```

Use the following **debug** command to display information from the TACACS+ helper process:

```
debug tacacs events
```

The figure shows part of the **debug aaa authentication** command output for a TACACS login attempt that was successful. The information indicates that TACACS+ is the authentication method used.

Also, note that the AAA/AUTHEN status indicates that the authentication has passed.

There are three possible results of an AAA session:

■ Pass

■ Fail

■ Error

The debug of each result is shown in the following three figures.

debug tacacs Command Example Output—Failure

```
13:53:35: TAC+: Opening TCP/IP connection to 10.1.1.4/49
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 10.1.1.4/49
(AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 10.1.1.4/49
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 10.1.1.4/49
(AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 10.1.1.4/49
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 10.1.1.4/49
(AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 10.1.1.4/49
13:53:38: TAC+ (416942312): received authen response status = FAIL  ◄───────
13:53:40: TAC+: Closing TCP/IP connection to 10.1.1.4/49
```

SECUR 1.1—4-44

The figure shows part of the **debug tacacs** command output for a TACACS login attempt that was unsuccessful as indicated by the status FAIL. The status fields are probably the most useful part of the **debug tacacs** command.

debug tacacs Command Example Output—Pass

```
14:00:09: TAC+: Opening TCP/IP connection to 10.1.1.4/49
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 10.1.1.4/49
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 10.1.1.4/49
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 10.1.1.4/49
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 10.1.1.4/49
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 10.1.1.4/49
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 10.1.1.4/49
14:00:14: TAC+ (383258052): received authen response status = PASS  ←
14:00:14: TAC+: Closing TCP/IP connection to 10.1.1.4/49
```

　　　　SECUR 1.1—4-45

The figure shows part of the **debug tacacs** command output for a TACACS login attempt that was successful, as indicated by the status PASS.

debug tacacs events Command Output

```
router# debug tacacs events
%LINK-3-UPDOWN: Interface Async2, changed state to up
00:03:16: TAC+: Opening TCP/IP to 10.1.1.4/49 timeout=15
00:03:16: TAC+: Opened TCP/IP handle 0x48A87C to 10.1.1.4/49
00:03:16: TAC+: periodic timer started
00:03:16: TAC+: 10.1.1.4 req=3BD868 id=-1242409656 ver=193 handle=0x48A87C (ESTAB)
expire=14 AUTHEN/START/SENDAUTH/CHAP queued
00:03:17: TAC+: 10.1.1.4 ESTAB 3BD868 wrote 46 of 46 bytes
00:03:22: TAC+: 10.1.1.4 CLOSEWAIT read=12 wanted=12 alloc=12 got=12
00:03:22: TAC+: 10.1.1.4 CLOSEWAIT read=61 wanted=61 alloc=61 got=49
00:03:22: TAC+: 10.1.1.4 received 61 byte reply for 3BD868
00:03:22: TAC+: req=3BD868 id=-1242409656 ver=193 handle=0x48A87C (CLOSEWAIT) expire=9
AUTHEN/START/SENDAUTH/CHAP processed
00:03:22: TAC+: periodic timer stopped (queue empty)
00:03:22: TAC+: Closing TCP/IP 0x48A87C connection to 10.1.1.4/49
00:03:22: TAC+: Opening TCP/IP to 10.1.1.4/49 timeout=15
00:03:22: TAC+: Opened TCP/IP handle 0x489F08 to 10.1.1.4/49
00:03:22: TAC+: periodic timer started
00:03:22: TAC+: 10.1.1.4 req=3BD868 id=299214410 ver=192 handle=0x489F08 (ESTAB)
expire=14 AUTHEN/START/SENDPASS/CHAP queued
00:03:23: TAC+: 10.1.1.4 ESTAB 3BD868 wrote 41 of 41 bytes
00:03:23: TAC+: 10.1.1.4 CLOSEWAIT read=12 wanted=12 alloc=12 got=12
00:03:23: TAC+: 10.1.1.4 CLOSEWAIT read=21 wanted=21 alloc=21 got=9
00:03:23: TAC+: 10.1.1.4 received 21 byte reply for 3BD868
00:03:23: TAC+: req=3BD868 id=299214410 ver=192 handle=0x489F08 (CLOSEWAIT) expire=13
AUTHEN/START/SENDPASS/CHAP processed
00:03:23: TAC+: periodic timer stopped (queue empty)
```

SECUR 1.1—4-46

The figure shows sample **debug tacacs events** output.

In this example, the opening and closing of a TCP connection to a TACACS+ server are shown, and also the bytes read and written over the connection and the connection's TCP status.

The TACACS messages are intended to be self-explanatory or for consumption by service personnel only. However, the messages shown are briefly explained in the following text:

■ This message indicates that a TCP open request to host 10.1.1.4 on port 49 will time out in 15 seconds if it gets no response:

```
00:03:16: TAC+: Opening TCP/IP to 10.1.1.4/49 timeout=15
```

■ This message indicates a successful open operation and provides the address of the internal TCP "handle" for this connection:

```
00:03:16: TAC+: Opened TCP/IP handle 0x48A87C to 10.1.1.4/49
```

There is more information provided in the output than there is time or space to address in this course. For more detailed information, refer to the *Debug Command Reference* on the documentation CD-ROMs, on Cisco.com, or in printed form.

You can get more meaningful output from **debug** command output if you first configure the router using the **service timestamps** *type* [**uptime**] **datetime** [**msec**] [**localtime**] [**show-timezone**] command. The following table describes the **service timestamps** command.

type	Type of message to timestamp; debug or log.
uptime (Optional.)	Timestamp with time since the system was rebooted.
datetime	Timestamp with the date and time.
msec (Optional.)	Include milliseconds in the date and timestamp.
localtime (Optional.)	Timestamp relative to the local time zone.
show-timezone (Optional.)	Include the time zone name in the timestamp.

RADIUS Configuration Overview

This topic describes the RADIUS protocol.

RADIUS Background

Cisco.com

RADIUS was developed by Livingston Enterprises, now part of Lucent Technologies. It contains a:

- **Protocol with a frame format that uses UDP**
- **Server**
- **Client**

SECUR 1.1—4-48

RADIUS is an access server authentication, authorization, and accounting protocol developed by Livingston Enterprises, Inc. (now part of Lucent Technologies). It is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises three components:

- Protocol with a frame format that uses UDP/IP

- Server

- Client

The server runs on a central computer typically at the customer site, while the clients reside in the dial-in access servers and can be distributed throughout the network. Cisco incorporated the RADIUS client into Cisco IOS, starting with IOS release 11.1.

Client/Server Model

A router operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. The RADIUS servers can act as proxy clients to other kinds of authentication servers.

Network Security

Transactions between the client and RADIUS server are authenticated using a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecured network could determine a user's password.

Flexible Authentication Mechanisms

The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP, CHAP, or MS-CHAP UNIX login, and other authentication mechanisms.

Configuration

RADIUS configuration is a three-step process:

Step 1   Configure communication between the router and the RADIUS server.

Step 2   Use the AAA global configuration commands to define method lists containing RADIUS to define authentication and authorization methods. Method lists include the following keywords:

Keyword	Description
enable	Uses the enable password for authentication
line	Uses the line password for authentication
local	Uses the local username database for authentication
none	Uses no authentication
radius	Use RADIUS authentication
tacacs+	Uses TACACS+ authentication

You can create AAA accounting for RADIUS connections and with TACACS+.

Step 3   Use line and interface commands to cause the defined method lists to be used.

RADIUS Server Command

You can either use the two commands shown here

router(config)#

```
radius-server key keystring
```

router(config)# radius-server key 2bor!2b@?

router(config)#

```
radius-server host {host-name | ipaddress}
```

router(config)# radius-server host 10.1.2.4

or

you can use this single command to do the same thing.

router(config)#

```
radius-server host ipaddress key keystring
```

router(config)# radius-server host 10.1.2.4 key
    2bor!2b@?

Use the **radius-server** command to configure router to RADIUS server communication.

Note: The **radius-server** global command is analogous to **tacacs-server** global commands.

RADIUS is a fully open protocol, distributed in source code format that can be modified to work with any security system currently available on the market. Cisco supports RADIUS under its AAA security paradigm. RADIUS can be used with other AAA security protocols, such as TACACS+, Kerberos, or local username lookup. Cisco Secure ACS supports RADIUS.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users. RADIUS combines authentication and authorization. The protocol is specified in RFCs 2138 and 2139.

Three major versions or flavors of RADIUS are available today:

■ IETF with approximately 63 attributes—Developed and proposed to IETF by Livingston Enterprises, now a division of Lucent Technologies. The RADIUS protocol is specified in RFC 2138, and RADIUS accounting in RFC 2139.

■ Cisco implementation supporting approximately 58 attributes—Starting in Cisco IOS release 11.2, an increasing number of attributes and functionality are included in each release of Cisco IOS software and Cisco Secure ACS.

■ Lucent supporting over 254 attributes—Lucent is constantly changing and adding vendor-specific attributes such as token caching and password changing. An Application Programming Interface (API) enables rapid development of new extensions, making competing vendors work hard to keep up. Although Livingston Enterprises developed RADIUS originally, it was championed by Ascend.

Vendors have implemented proprietary extensions to RADIUS features. TACACS+ is considered superior because:

■ TACACS+ encrypts the entire TACACS+ packet (RADIUS only encrypts the shared-secret password portion).

■ TACACS+ separates authentication and authorization, making possible distributed security services.

■ RADIUS has limited "name space" for attributes.

TACACS+/RADIUS Comparison

Cisco.com

Dial

TACACS+ client
RADIUS client

Campus

TACACS+ server

RADIUS server
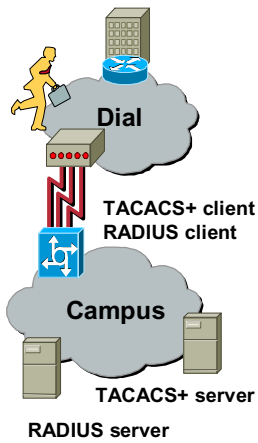
	TACACS+	RADIUS
Functionality	Separates AAA	Combines authentication and authorization
Transport Protocol	TCP	UDP
CHAP	Bidirectional	Unidirectional
Protocol Support	Multiprotocol Support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Accounting	Limited	Extensive

SECUR 1.1—4-50

There are several differences between TACACS+ and RADIUS:

■ Functionality—TACACS+ separates AAA functions according to the AAA architecture, allowing modularity of the security server implementation. RADIUS combines authentication and authorization, separates accounting, thus allowing less flexibility in implementation.

■ Transport protocol—TACACS+ uses TCP. RADIUS uses UDP, which was chosen for simplification of client and server implementation, yet it makes the RADIUS protocol less robust and requires the server to implement reliability measures such as packet retransmission and timeouts instead of the Layer 3 protocol.

■ Challenge/Response—TACACS+ supports bidirectional challenge and response as used in CHAP between two routers. RADIUS supports unidirectional challenge and response from the RADIUS security server to the RADIUS client.

■ Protocol Support—TACACS+ provides more complete dial-in and WAN protocol support.

■ Data Integrity—TACACS+ encrypts the entire packet body of every packet. RADIUS only encrypts the Password Attribute portion of the Access-Request packet, which makes TACACS+ more secure.

■ Customization—The flexibility provided in the TACACS+ protocol allows many things to be customized on a per-user basis (that is, customizable username and password prompts). RADIUS lacks flexibility and therefore many features that are possible with TACACS+ are not possible with RADIUS. (that is, message catalogs).

■ Authorization process—With TACACS+, the server accepts or rejects the authentication request based on the contents of the user profile. The client (router) never knows the contents of the user profile. With RADIUS, all reply attributes in the user profile are sent to the router. The router accepts or rejects the authentication request based on the attributes received.

- Accounting—TACACS+ accounting includes a limited number of information fields. RADIUS accounting can contain more information than TACACS+ accounting records, which is the key strength of RADIUS over TACACS+.

Kerberos Overview

Kerberos is a secret-key network authentication protocol, developed at the Massachusetts Institute of Technology (MIT) that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos, like other secret-key systems, is based on the concept of a trusted third party that performs secure verification of users and services.

In the Kerberos protocol, this trusted third party is called the Key Distribution Center (KDC). It performs the same function as a certification authority (CA), which is the subject of a later lesson.

Kerberos-Authenticated Server-Client System

- **Secret-key authentication protocol**
- **Authenticates users and network services they use**
- **Uses 40- or 56-bit DES for encryption and authentication (weak by today's standards)**
- **Relies on trusted third party for key distribution (Key Distribution Center)**
- **Embodies "single login" concept**
- **Expensive to administer—labor intensive**

SECUR 1.1—4-52

Cisco IOS Software Release 12.0 includes Kerberos 5 support, which allows organizations already deploying Kerberos 5 to use an existing Key Distribution Center (KDC, similar to a Certificate Authority in IPSec) with their routers and NASs. The following network services are Kerberized in Cisco IOS software:

- Telnet—Telnet client (from router to another host) and Telnet server (from another host to router)

- rlogin—Logs a user into a remote UNIX host for an interactive session similar to Telnet

- rsh—Logs a user into a remote UNIX host and allows execution of one UNIX command

- rcp—Logs a user into a remote UNIX host and allows copying of files from the host

---

Note: You can use the **connect** EXEC command with the /telnet or /rlogin keywords to log in to a host that supports Telnet or rlogin. You can use the /encrypt kerberos keyword to establish an encrypted Telnet session from a router to a remote Kerberos host. Alternatively, you can use the **telnet** EXEC command with the /encrypt kerberos keyword to establish an encrypted Telnet session.

Note: You can use the **rlogin** and **rsh** EXEC commands to initiate rlogin and rsh sessions.

Note: You can use the **copy rcp** EXEC or configuration command to enable obtaining configuration or image files from an RCP server.

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco Secure ACS for Windows Server has the following characteristics:

- It runs as a group of services on Windows 2000 Server.
- It authenticates using TACACS+ or RADIUS.
- Cisco NAS, PIX Firewall, VPN 3000, or routers can authenticate against Cisco Secure ACS for Windows Server.
- It can use usernames and passwords in a Windows 2000 Server user database, Cisco Secure ACS user database, token server, or NDS.
- Installation is similar to other Windows applications (InstallShield).
- Management is done via a web browser.
- It supports distributed ACS systems.
- With a remote security server for AAA, the server performs AAA, enabling easier management.
- TACACS+, RADIUS, and Kerberos are the security server protocols supported by Cisco.
- Troubleshooting tools include debug commands for TACACS+.

SECUR 1.1—4-54

Summary (Cont.)

Cisco Secure ACS for UNIX has the following characteristics:

- It provides AAA security for enterprise networks.
- It supports both TACACS+ and RADIUS.
- It uses the Sybase SQL Anywhere database as standard and can interface with Sybase SQL and Oracle databases.
- Customers can upgrade any 2.x version of Cisco Secure ACS for UNIX to the most current release.
- It is easy to install and has a web-based GUI.
- RADIUS databases can be imported into Cisco Secure ACS for UNIX.

SECUR 1.1—4-55

Summary (Cont.)

Cisco Secure ACS Solution Engine has the following characteristics:

- **It provides AAA security for enterprise networks.**
- **It supports both TACACS+ and RADIUS.**
- **It contains a hardened Windows 2000 Server operating system.**
- **It is built on the Hewlett-Packard ProLiant DL320 G2 (Cisco 1111) rack-mounted system.**

SECUR 1.1—4-56

Lab Exercise—Configuring Cisco Secure ACS for Windows Server

In this lab exercise, you will configure a Cisco Secure Access Control Server (Cisco Secure ACS) for Windows Server to provide authentication, authorization, and accounting (AAA) services.

Objectives

In this lab exercise, you will complete the following tasks:

- Complete the lab exercise setup.
- Install Cisco Secure ACS for Windows Server.
- Take a grand tour of Cisco Secure ACS for Windows Server.
- Configure the Cisco Secure ACS for Windows Server database for authentication.
- Configure the router to authenticate to the Cisco Secure ACS for Windows Server database.

Visual Objective

The following figure illustrates the network environment that you will create.

Lab Visual Objective

SECUR 1.1—4-2
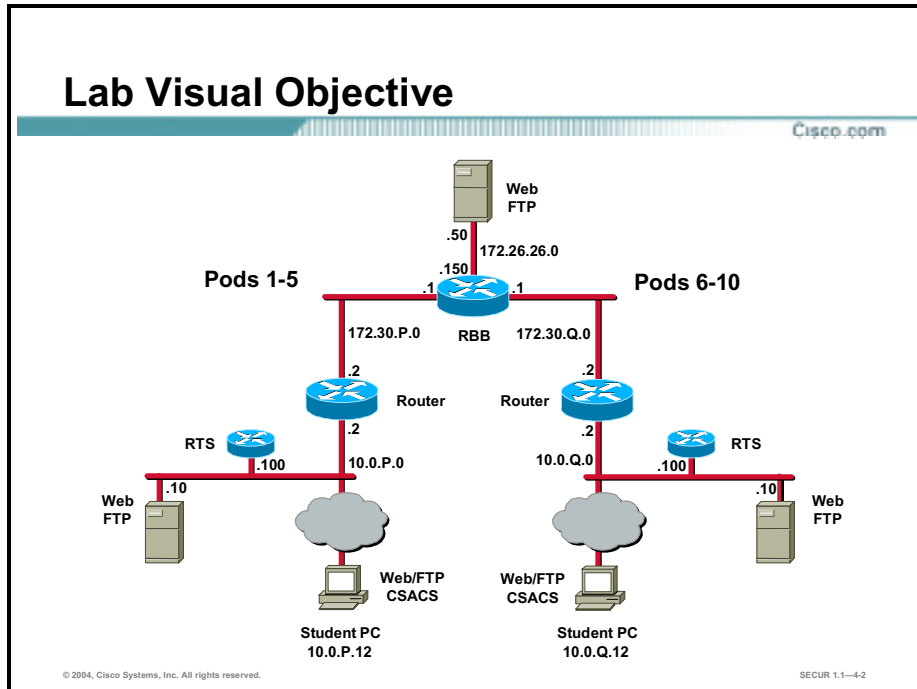
Scenario

You will configure an AAA server to perform AAA services to secure Telnet, EXEC, and VTY access to a Cisco perimeter router. You will configure Cisco Secure ACS to use the Cisco Secure ACS database.

Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1 Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2 Configure your student PC for IP address **10.0.P.12** with a default gateway of **10.0.P.2** (where P = pod number).

Step 3 If you just completed the lab exercise from the previous lesson, disable logging to the router console using the **no logging console** command.

Task 2—Install Cisco Secure ACS for Windows Server

Complete the following steps to install Cisco Secure ACS for Windows Server on your Microsoft Windows 2000 Server student PC. This procedure assumes that Microsoft Windows 2000 Server is operational.

Step 1 Log in to Microsoft Windows 2000 Server using the administrator account. Your instructor will provide you with the correct username and password combination for the administrator account.

Step 2   Open the **CiscoApps** folder on your desktop.

Step 3   Open the **Cisco Secure ACS** folder.

Step 4   Begin the Cisco Secure ACS installation by double-clicking the **setup.exe** file. The Cisco Secure ACS for Windows Server installation wizard starts.

Step 5   Click **Accept** to acknowledge the terms of the Cisco Secure ACS license agreement.

Step 6   Click **Next** in the Welcome window.

Step 7   Select all items listed in the Before You Begin window and click **Next**.

Step 8   Click **Next** to accept the default settings in the Choose Destination Location window.

Step 9   Complete the following sub-steps within the Authentication Database Configuration window:

1. Select the **Also check the Windows User Database** check box.

2. Select the **Yes, refer to "Grant dialin permission to user" setting** check box.

3. Click **Next**.

Step 10   Complete the following sub-steps within the Cisco Secure ACS Network Access Server Details window:

1. Select **TACACS+ (Cisco IOS)** from the Authenticate Users Using scroll box.

2. Enter the name of your router in the Access Server Name box (for example, R1, R2, and so on).

3. Enter the IP Address of your router inside interface (**10.0.P.2**) in the Access Server IP Address box (where P = pod number).

4. Ensure the IP address of your student PC is entered in the Windows Server IP Address field.

5. Enter **ciscosecure** (one word, all lowercase) in the TACACS+ or RADIUS Key field.

6. Click **Next**. Setup will start installing files on your student PC.

Step 11   Select all check boxes within the Advanced Options window and click **Next**. It is important that you select all check boxes as this determines what ACS options you will be able to configure later.

Step 12   Accept the default settings within the Active Service Monitoring window by clicking **Next**.

Step 13   Accept the default settings within the Network Access Server Configuration window by clicking **Next**.

Step 14   Accept the default setting (no password specified) in the Enable Secret Password window by clicking **Next**. You already specified the router enable secret password in the previous lab exercise.

Step 15   Accept the default settings within the Access Server Configuration window by clicking **Next**.

Step 16   Complete the following sub-steps within the NAS Configuration window:

1. Use the scroll bar to view all of the parameters in the command box. These parameters are created during the installation process of the Cisco Secure ACS software.

2. Do NOT use the **Telnet Now?** function at this time. The Telnet Now function allows you to telnet to your router and then copy and paste these parameters into your router, saving time in the router setup process. You will be entering these commands and parameters manually later in this lab exercise.

3. Click **Next**.

Step 17 Accept the default settings within the Cisco Secure ACS Service Initiation window by clicking **Next**.

Step 18 Click **Finish** to close the Setup Complete window.

Step 19 Review the contents of the README.TXT file and close the associated window.

Step 20 Close the Internet Explorer window containing the Cisco Secure ACS main window.

Step 21 Use the Windows Task Manager (**Ctrl**+**Alt**+**Delete**>**Task Manager**) to verify the following services are running on your student PC:

■ CSAdmin

■ CSAuth

■ CSDBSync

■ CSLog

■ CSMon

■ CSRadius

■ CSTacacs

If these services are not running, restart your student PC and repeat this step.

Step 22 Close any open windows.

Task 3—Take a Grand Tour of Cisco Secure ACS for Windows Server

Complete the following steps to become familiar with the Cisco Secure ACS for Windows Server administration interface, and to change some global settings. Ensure you complete each step:

Step 1 Start the ACS configuration manager by double-clicking the **ACS Admin** desktop icon.

Step 2 Select the **Cisco Systems** icon at the top of the left frame.

Q1) What is the full release version and build number?

A) _____

Step 3 Examine the user setup functions by completing the following sub-steps:

1. Select **User Setup** in the left frame.

2. Select the **List All Users** button.

Q2) How many users are configured?

A) _____

Step 4 Examine the group setup functions by completing the following sub-steps:

1. Select **Group Setup** in the left frame.

Q3) What group is shown in the Group: scroll list?

   A) _____

2. Select the **Users in Group** button.

Q4) How many users are in the group?

   A) _____

Step 5 Select **Network Configuration** in the left frame.

Q5) How many routers (AAA client hosts) are configured?

   A) _____

Step 6 Examine the system configuration functions by completing the following sub-steps:

1. Select **System Configuration** in the left frame.

2. Select **Service Control** and answer the following questions:

Q6) What is the status of the Cisco Secure service, level of detail for logging, and frequency of new file generation?

   A) _____

3. Click **Cancel** to return to the select list.

4. Select **Logging** and answer the following question:

Q7) What log targets are enabled?

   A) _____

5. Click **Cancel** to return to the select list.

6. Select **Local Password Management** and answer the following question:

Q8) What is the purpose of the password validation option?

   A) _____

7. Click **Cancel** to return to the select list.

8. Select **Cisco Secure Database Replication** and answer the following question:

Q9) What is the purpose of Database Replication Setup?

   A) _____

9. Click **Cancel** to return to the select list.

10. Select **ACS Backup** and answer the following question:

Q10) Where can the ACS user and group databases be backed up?

   A) _____

11. Click **Cancel** to return to the select list.

12. Select **ACS Restore** and answer the following question:

Q11)   What components can be backed up and restored?

    A)   _____

13. Click **Cancel** to return to the select list.

14. Select **ACS Service Management** and answer the following question:

Q12)   What are the two ways a system administrator can be notified of logged events?

    A)   _____

Step 7   Click **Cancel** to return to the select list.

Step 8   Examine the interface configuration functions by completing the following sub-steps:

1. Select **Interface Configuration** in the left frame.

2. Select **User Data Configuration** and answer the following question:

Q13)   How are user-defined fields useful?

    A)   _____
         _____

3. Click **Cancel** to return to the select list.

4. Select **Advanced Options**.

5. Select all options and answer the following question:

Q14)   What is the purpose of selecting advanced options?

    A)   _____
         _____

6. Select **Submit** and return to the select list.

7. Select **TACACS+ (Cisco IOS)**.

8. In the TACACS+ Services section, select **PPP IP**, **PPP LCP**, **PPP Multilink and Shell (exec)** in both the User and Group columns.

9. In the Advanced Configuration Options section, select all four options.

10. Select **Submit** to return to the select list and answer the following question:

Q15)   Where are the TACACS+ services and advanced configuration objects applied that you configure in this window?

    A)   _____
         _____

Step 9   Select **Administration Control** in the left frame and answer the following questions:

Q16)   What administrator accounts are configured?

A)   _____

Q17)   What is the purpose of administrator control?

A)   _____
_____

Step 10   Examine the external user database functions by completing the following sub-steps:

1.   Select **External User Databases** in the left frame.

2.   Select **Unknown User Policy** and answer the following questions:

Q18)   What two options are available if a user is not found in the Cisco Secure database? Which one is the default?

A)   _____

Q19)   What external databases can be checked for the unknown user?

A)   _____

3.   Click **Cancel** to return to the select list.

4.   Select **Database Group Mappings** and view the help section.

5.   Click **Cancel** to return to the select list.

6.   Select **Database Configuration** and answer the following question:

Q20)   What do you select in the External User Database Configuration section?

A)   _____

Step 11   Click **Cancel** to return to the select list.

Step 12   Examine the reports and activity functions by completing the following sub-steps:

1.   Select **Reports and Activity** in the left frame.

2.   Select **Administration Audit** and answer the following question:

Q21)   What appears in the Administration Audit.csv file?

A)   _____

Step 13   Select **Online Documentation** in the left frame.

Take a moment to browse the new features, software requirements, and troubleshooting sections of the online documentation.

Task 4—Configure the Cisco Secure ACS for Windows Server Database for Authentication

In the previous lab exercise, you tested authentication attempts against the router's local database where access was based on the configurations allowed on the router's various access points. Now, you will move to a centralized authentication and authorization model. To do this, you will change parts of the configuration on the router to reflect a more secure, consolidated security plan using an AAA server, which includes the following policies:

■ Provides the IS group with access to the console and unlimited VTY access for control of the network.

■ Changes AUX port configurations to remove EXEC or login services.

Complete the following steps to add a group and user to the Cisco Secure ACS for Windows Server database:

Step 1 Create a new user group by completing the following sub-steps:

1. Select the **Group Setup** button in the left frame.

2. Select **Group 1** from the drop-down list.

3. Rename the group to is-in by selecting the **Rename Group** button, highlighting the existing name, typing in the new group name, and selecting the **Submit** button.

4. Select **Edit Settings** and set the group settings as follows:

■ In the Password Aging Rules section, select the **Apply age-by-date rules** check box.

■ Configure the apply age-by-date rule for **30** days active, a warning period of **4**, and a grace period of **4**.

■ In the IP Assignment section, select **No IP address assignment**.

■ In the TACACS+ Settings section, select **Shell (exec)**.

■ In the Enable Options section, select **Max Privilege for any AAA Client** and set the level to **level 15**.

■ Leave all other sections at their default values.

5. Click **Submit + Restart**.

Q22) How else can password aging be controlled when authenticating against the Cisco Secure ACS for Windows Server database?

A) _____

Step 2 Set the router host and key value by completing the following sub-steps:

1. Select **Network Configuration** from the left frame.

2. Select the (Not Assigned) **Network Device Group**.

3. Select the router host shown.

4. Verify that the key value is ciscosecure.

5. Click **Submit + Restart**.

Step 3   Add and configure a user to authenticate against the Cisco Secure ACS database by completing the following sub-steps:

1. Click the **User Setup** button in the left-frame.

2. Enter a username of **isadmin**.

3. Click **Add/Edit** and make sure Account Disabled is deselected.

4. Scroll to the User Setup frame and select **CiscoSecure Database** for password authentication.

5. Enter a password of **isuser** for the user isadmin. Ensure that you enter the password twice to confirm it.

6. Scroll to the Group to which the user is assigned section and assign the user to the is-in group.

7. Scroll to the Account Disable section and select **Disable account if…** and select the **Failed attempts exceed:5** check box.

8. Scroll to the Advanced TACACS+ Settings section and select **Use group level setting**. Remember that the group setting is level 15.

9. Scroll to the TACACS+ Enable Password section and select the **Use Separate Password** check box.

10. Enter a password of **ispassword**. Remember to enter it twice to confirm it.

11. Click **Submit** to enable the settings.

12. Click **List All Users** in the User Setup Select frame and verify that the user you just added is present and correctly configured.

Q23)   What is the main difference between the parameters in the user and group setups?

A)   _____
_____

Step 4   Minimize the Cisco Secure ACS window.

Task 5—Configure the Router to Authenticate to the Cisco Secure ACS for Windows Server Database

In this section you will modify existing router AAA methods, add commands to tell the router how to locate a Cisco Secure ACS for Windows Server system, and protect the TTY and AUX ports. Complete the following steps to do this:

Step 1   Log into the router using the AAA administrator account user name of **admin** with a password of **admindoor**.

Step 2   Enter and enable privileged-EXEC mode using the **Curium96** password.

Step 3   Enter configuration terminal mode:

```
RP# config t
```

Step 4 Enter the location of the Cisco Secure ACS IP address and encryption key for TACACS+ as shown (where P = pod number):

```
RP(config)# tacacs-server host 10.0.P.12 key ciscosecure
```

Step 5 Enable AAA accounting for Cisco Secure ACS for Windows Server:

```
RP(config)# aaa accounting connection default start-stop group tacacs+
```

Step 6 Complete the following sub-steps on the router to consolidate the VTY and Console:

1. Enter the following commands exactly as shown:

```
RP(config)# no aaa authentication login console-in local
RP(config)# no aaa authentication login is-in local
RP(config)# aaa authentication login is-in group tacacs+ local
RP(config)# line con 0
RP(config-line)# login authentication is-in
RP(config-line)# exit
```

2. Enter the following command to protect the enable password and privileged mode:

```
RP#(config)# aaa authentication enable default group tacacs+
```

This will force the use of the enable restrictions you placed in the Cisco Secure ACS for Windows Server, and it overrides the enable secret password on the router.

Step 7 Change the AUX access by entering the following commands:

```
RP(config)#  line aux 0
RP(config-line)# no password AuxUser1
RP(config-line)#  no exec
RP(config-line)#  exit
```

Step 8 There is one other item. If something happens and ports or access points are added into the machine, then you have to protect them. You have the default login list already protected with the enable password. You will change this to use tacacs+. Enter the following commands exactly as shown:

```
RP(config)#  no aaa authentication login default enable
RP(config)#  aaa authentication login default group tacacs+ enable
```

Note:	You should always place an **enable** at the end of the **aaa authentication login default group tacacs+ enable** command as shown in this step. This allows you to access privileged-EXEC mode even if the TACACS+ server is down. The router first tries to locate a TACACS+ server, and if it cannot find one, will default to the standard enable password.

Step 9 Open a new command prompt shell and telnet to the inside interface of your router: **10.0.P.2** (where P = pod number).

Step 10 Log in using the **isadmin** username and the **isuser** password. Your router should authenticate with the ACS and allow you to log in. If you cannot log in, recheck your work and try again.

Step 11 Enter privileged-EXEC mode using the **ispassword** password. Your router should authenticate with the ACS and allow you to log in. If you cannot log in, recheck your work and try again.

Step 12 Copy the running configuration to the startup configuration using the **copy run start** command:

```
RP(config)# end
RP# copy run start
```

Step 13 Log out of the Telnet session and close the command prompt window.

Step 14 Log out of Cisco Secure ACS and minimize the window.

Step 15 Return the router to the default lab configuration in preparation for the next lab.

Answers

This topic contains the answers to the questions posed earlier:

Q1) The Cisco Secure ACS home page; version 3.2 or later.

Q2) None at this point.

Q3) The Default Group.

Q4) None; no users are configured at this point.

Q5) One.

Q6) Cisco Secure is currently running; the level is low, new file every day.

Q7) Failed Attempts, RADIUS Accounting, TACACS+ Accounting, TACACS+ Administration.

Q8) Enables control of password length when users change their password.

Q9) Enables control of database replication components, scheduling, and partners.

Q10) A local or networked directory; however the default is …\CiscoSecure…\CSAuth\System Backups.

Q11) User and group database and the Cisco Secure ACS System Configuration.

Q12) Events can be logged to the NT/2000 event log, or an e-mail notification of the event can be sent to the system administrator.

Q13) You can specify unique information that will be displayed for each user, such as location or department and can have the information reflected in the accounting logs if desired.

Q14) You can configure the advanced features that will appear in the user interface. You select only applicable features, reducing the complexity of the Cisco Secure ACS windows displayed.

Q15) TACACS+ Services and Advanced Configuration Objects configured in the TACACS+ (Cisco) window are applied and appear as selectable options in the User and Group setup windows for each user and group.

Q16) No administrator accounts are configured at this time.

Q17) You can add, delete, and control administrator accounts from a web browser. You can control administrator passwords, privileges, system configuration, reports, and activity.

Q18) It depends on the configuration that was created during the installation.

Q19) The Windows NT or Windows 2000 user database, or any configured, supported external database (CRYPTOCard, ODBC, and so on).

Q20) The external user database you want to use for authentication.

Q21) A record of all administration actions.

Q22) By using the age-by-uses rules in the Password Aging Rules window.

Q23) Group setup parameters apply to all users assigned to the group. User setup parameters only apply to that user. User parameters can override group parameters.

5

Cisco Router Threat Mitigation

This lesson describes the risks associated with connecting an enterprise to the Internet and the methods used to reduce those risks.

It includes the following topics:

- Objectives
- Using routers to secure the network
- Disabling unused router services and interfaces
- Introduction to Cisco access lists
- Using access lists to mitigate security threats
- Filtering router service traffic
- Filtering network traffic
- DDoS mitigation
- Sample router configuration
- Implementing Syslog logging
- Designing secure management and reporting for enterprise networks
- Using AutoSecure to secure Cisco routers
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

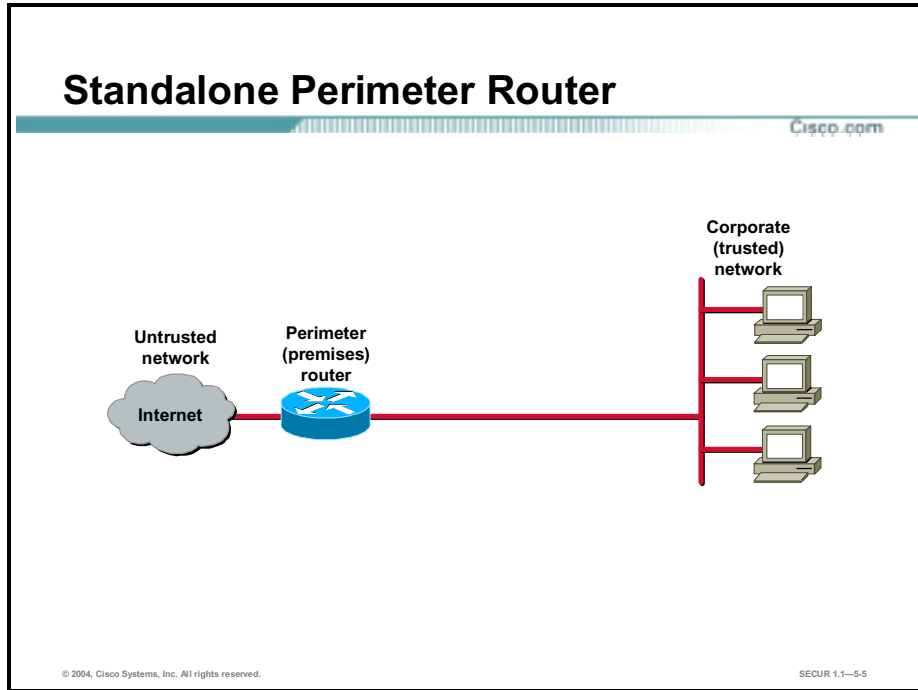**Upon completion of this lesson, you will be able to perform the following tasks:**

- Disable unused router services and interfaces.
- Describe the differences between various types of Cisco access lists.
- Design and build both standard and extended access lists.
- Use access lists to mitigate common router security threats.
- Implement Syslog logging.
- Design secure management and reporting for router networks.
- Use AutoSecure to secure Cisco routers.

SECUR 1.1—5-3

Using Routers to Secure the Network

This topic considers different router topologies and their uses.

Standalone Perimeter Router

SECUR 1.1—5-5

Corporate
(trusted)
network

Perimeter
(premises)
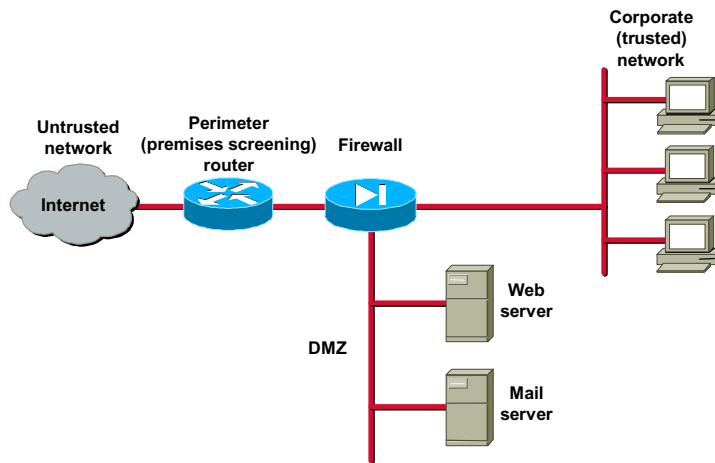router

Untrusted
network

Internet

The most basic routed network consists of a corporate LAN connected to the Internet using a single perimeter router. This router must secure the corporate network (trusted network) from malicious activity originating on the Internet (untrusted network). Installations of this type are typical of small enterprises.

The perimeter router, being the first line of defense for the enterprise, is relied upon to provide Internet access and basic attack prevention.

Perimeter Router and Firewall

Cisco.com

Corporate (trusted) network

Untrusted network

Perimeter (premises screening) router

Firewall

Internet

DMZ

Web server

Mail server

SECUR 1.1—5-6

Medium-sized networks typically employ a firewall appliance behind the perimeter router as shown in the figure. In this scenario, the perimeter router still provides basic packet filtering on packets destined for the corporate network.. The firewall appliance, with its additional security features, can perform user authentication as well as 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.

Note	Routers can also be used to facilitate the creation of basic DMZs. As a system administrator, you need to decide which configuration best fits your security requirements.

Perimeter Router with Integrated Firewall
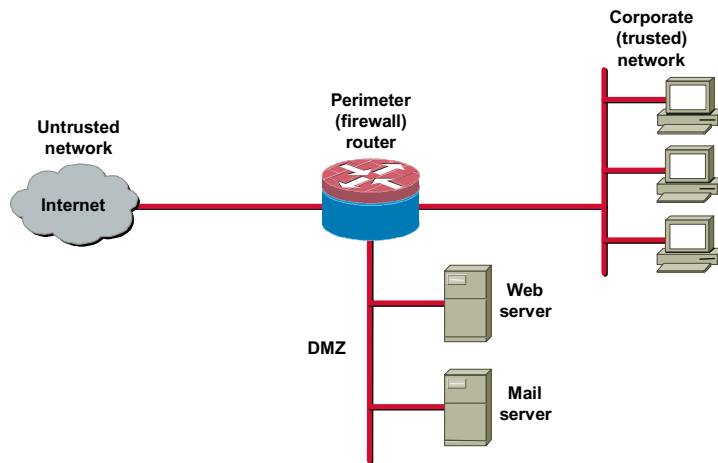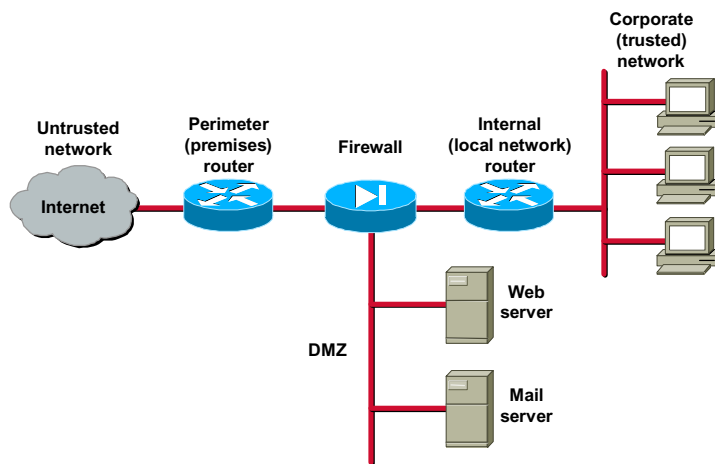
Cisco offers an alternative to the firewall appliance by incorporating many firewall features in the perimeter router itself.

Although this approach does not provide the same performance and security features that a Cisco PIX Firewall appliance offers, a router with an integrated firewall feature set may solve many small-to-medium business perimeter security requirements.

Perimeter Router, Firewall, and Internal Router

Corporate (trusted) network

Untrusted network

Perimeter (premises) router

Firewall

Internal (local network) router

Internet

Web server

DMZ

Mail server

SECUR 1.1—5-8

Finally, many medium-to-large sized enterprises use a combination of internal (local network) routers and perimeter (premises) routers and firewall appliances. Internal routers provide additional security to the network by screening traffic to various parts of the protected corporate network.

Sometimes internal (local network) routers are replaced by high-end Cisco Catalyst switches, which contain their own security features.

Securing Router Services and Interfaces

This topic discusses Cisco router network services and interfaces and how to secure them.

Cisco routers support many network services that may or may not be required in certain enterprise networks. Turning off or restricting access to these services greatly improves network security.

One of the most basic rules of router security is to provide only those services the network requires, and no more. Leaving unused network services enabled increases the possibility of those services being maliciously exploited.

The services listed in the figure have been chosen for their vulnerability to malicious exploitation. These are the router services that are most likely to be used in network attacks.

■ Bootp server—This service is enabled by default. This service allows a router to act as a Bootp server for other enterprise 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 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 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.

■ Domain Name System (DNS)—This client service is enabled by default. By default, Cisco routers broadcast name requests to 255.255.255.255. Disable this service when it is not

required. If the DNS lookup service is required, make sure that you set the DNS server address explicitly.

- Finger—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.

- HTTP server—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 as when using the Cisco Security Device Manager. You should disable this service if it is not required. If this service is required, restrict access to the router's HTTP service using access control lists (ACLs).

- 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 a router's 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 router Flash memory.

- IP directed broadcast—This service is enabled in Cisco IOS Software Releases < 12.0 and disabled in Cisco IOS Software Releases ≥ 12.0. IP directed broadcasts are used in the extremely common and popular smurf denial of service (DoS) attack, and can also be used in related attacks. This service should be disabled when not required.

- Internet Control Message Protocol (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's IP address mask. This information can be used to map the network, and this service should be explicitly disabled on interfaces to untrusted networks.

- 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 them datagrams with source routing options. 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.

- 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.

- 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's 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 used, restrict which devices have access to NTP. Disable this service when it is not required.

- Packet assembler/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.

- Proxy Address Resolution Protocol (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.

- 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.

- 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's 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.

- TCP small servers—This service is enabled in Cisco IOS Software Releases < 11.3 and disabled in Cisco IOS Software Releases ≥ 11.3. The small servers are servers (daemons) running in the router that are sometimes useful for diagnostics, but are rarely used. Disable this service explicitly.

- UDP small servers—This service is enabled in Cisco IOS Software Releases < 11.3 and disabled in Cisco IOS Software Releases ≥ 11.3. The small servers are servers (daemons) running in the router that are sometimes useful for diagnostics, but are rarely used. Disable this service explicitly.

- Maintenance Operation Protocol (MOP) service—This service is enabled on most Ethernet interfaces. MOP is a Digital Equipment Corporation maintenance protocol that should be explicitly disabled when it is not in use.

- 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.

Disable Bootp Server

Cisco.com

Austin1

Austin2

Austin3

Austin4

Austin1, I need a Cisco IOS image.

Bootp request
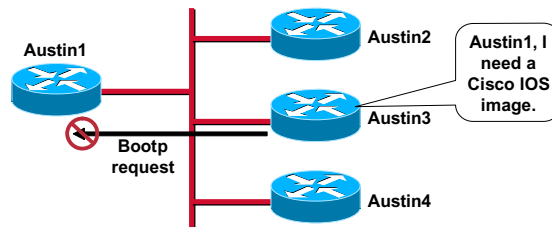
Router(config)#

```
no ip bootp server
```

• **Globally disables the Bootp service for this router**

```
Austin1(config)# no ip bootp server
```

SECUR 1.1—5-11

Bootp is a user datagram protocol (UDP) that can be used by Cisco routers to access copies of Cisco IOS software images on another Cisco router running the Bootp service. In this scenario, one Cisco router acts as a Cisco IOS server that can download Cisco IOS software to other Cisco routers acting as Bootp clients. This service is rarely used, but when it is, it can allow the following to occur:

■ An attacker can use this service to download a copy of a router's Cisco IOS software.

■ An attacker could exploit this service to perform DoS attacks against the router.

This service is enabled by default.

To disable the Bootp service, use the **no ip bootp server** command from global configuration mode as shown in the figure.
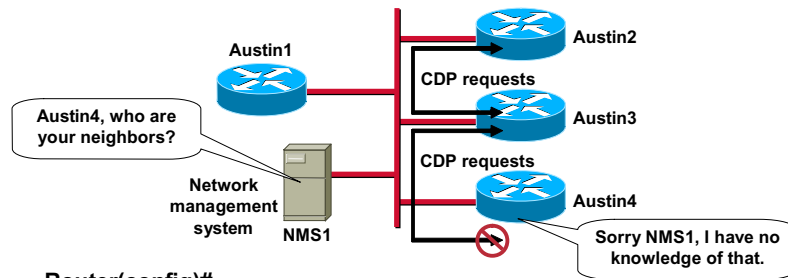
The syntax for the **no ip bootp server** command is as follows:

no ip bootp server

This command has no arguments or keywords.

Disable CDP

Austin1

Austin2

CDP requests

Austin4, who are your neighbors?

Austin3

CDP requests

Network management system

NMS1

Austin4

Sorry NMS1, I have no knowledge of that.

```
Router(config)#
```
```
no cdp run
```
• **Globally disables CDP**

```
Austin4(config)# no cdp run
```

SECUR 1.1—5-12

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. This service is enabled by default.

With CDP enabled, network management applications, such as CiscoWorks Campus Manager, can learn the device type and the IP addresses of neighboring devices. This feature enables applications to use the learned IP addresses to send queries to neighboring devices.

Attackers can use CDP during reconnaissance attacks to learn of a router's neighboring devices, thus discovering the network. For this reason, CDP should be disabled, either globally or on a per-interface basis, when not required.

Disable CDP globally on the router using the **no cdp run** command in global configuration mode as shown in the figure.

The syntax for the **no cdp run** command is as follows:

**no cdp run**

This command has no arguments or keywords.

If you need to use CDP, restrict its use to only those interfaces that require it. Keep the global setting enabled, but use the **no cdp enable** command in interface configuration mode to disable it on a per-interface basis as shown here:

```
Austin4(config)# interface e0/1
Austin4(config-if)# no cdp enable
```

Disable Configuration Auto-Loading (Network Booting)

Cisco.com
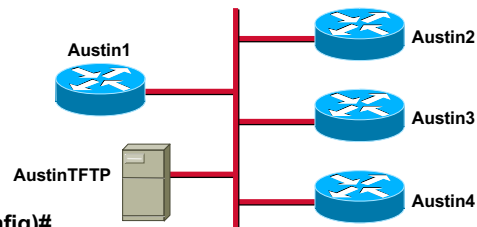
Router(config)#

```
no boot network remote-url
```

```
Austin4(config)# no boot network
  tftp://AustinTFTP/TFTP/Austin4.confg
```

Router(config)#

```
no service config
```

```
Austin4(config)# no service config
```

SECUR 1.1—5-14

Most Cisco routers are configured to load their Cisco IOS image and startup configuration from local Flash memory. However, you may configure your Cisco routers to load their IOS image and startup configuration from a network server instead. Loading router images and configurations across a network can be dangerous and should be considered only for fully trusted networks (as in a stand-alone test network). This setting is disabled by default.

If enabled, it is recommended that you set your routers to obtain their images and configurations from a local (trusted) source using the **boot network** *remote-url* command in global configuration mode. This setting should be disabled when not required.

Explicitly disable configuration auto-loading for a previously configured remote host using the **no boot network** and **no service config** commands in global configuration mode as shown in the figure.

The syntax for the **no boot network** command is as follows:

no boot network *remote-url*

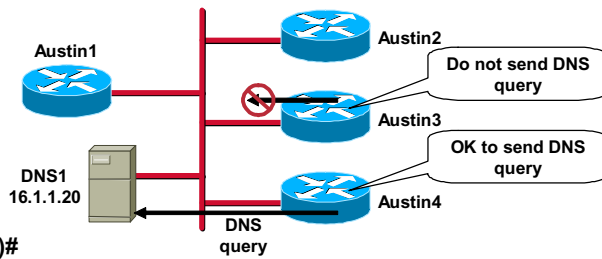| *remote-url*	Location of the configuration file. Use the following syntax:
	■ ftp:[[[//[username[:password]@]location]/directory]/filename]
	■ rcp:[[[//[username@]location]/directory]/filename]
	■ tftp:[[[//location]/directory]/filename]

The syntax for the **no service config** command is as follows:

no service config

This command has no arguments or keywords.

Restricting DNS Service

Router(config)#
```
ip name-server server-address1
  [server-address2…server-address6]
```
```
Austin4(config)# ip name-server 16.1.1.20
```

Router(config)#
```
no ip domain-lookup
```
```
Austin3(config)# no ip domain-lookup
```

SECUR 1.1—5-14

By default, the Cisco router DNS lookup service sends name queries to the 255.255.255.255 broadcast address. Using this broadcast address should be avoided as it may allow an attacker to emulate one of your DNS servers and respond to router queries with erroneous data.

This service is enabled by default. If your routers need to use this service, make sure that you explicitly set the IP address of your DNS servers in the router configuration.

Set the DNS server IP addresses using the **ip name-server** command in global configuration mode as shown in the figure.

The syntax for the **ip name-server** command is as follows:

ip name-server *server-address1* [*server-address2...server-address6*]

server-address1	IP address of name server.
server-address2…server-address6	(Optional.) IP addresses of additional name servers (a maximum of six name servers is allowed).

Note   Always disable the DNS lookup service when it is not in use.

Disable the DNS lookup service using the **no ip domain-lookup** command in global configuration mode as shown in the figure.
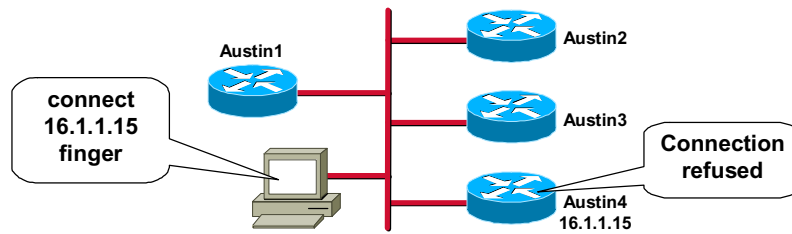
The syntax for this command is as follows:

no ip domain-lookup

This command has no arguments or keywords.

Disable Finger Service

Austin1

Austin2

Austin3

Austin4
16.1.1.15

connect
16.1.1.15
finger

Connection
refused

Router(config)#

```
no ip finger
```

```
Austin4(config)# no ip finger
Austin4(config)# no service finger
Austin4(config)# exit
Austin4# connect 16.1.1.15 finger
Trying 16.1.1.15, 79 ...
% Connection refused by remote host
```

SECUR 1.1—5-15

Cisco routers provide an implementation of the "finger" service that is used to find out which users are logged into a network device. Although this information is not usually sensitive, it can sometimes be useful to an attacker for reconnaissance purposes. This service is enabled by default.

Disable the finger service using the **no ip finger** or **no service finger** commands in global configuration mode as shown in the figure.

Note	The **service finger** command has been replaced by the **ip finger** command (introduced in Cisco IOS Software Release 11.3). However, the **service finger** and **no service finger** commands continue to function to maintain backward compatibility with versions of Cisco IOS software prior to 11.3.

The syntax for the **no ip finger** command is as follows:

no ip finger

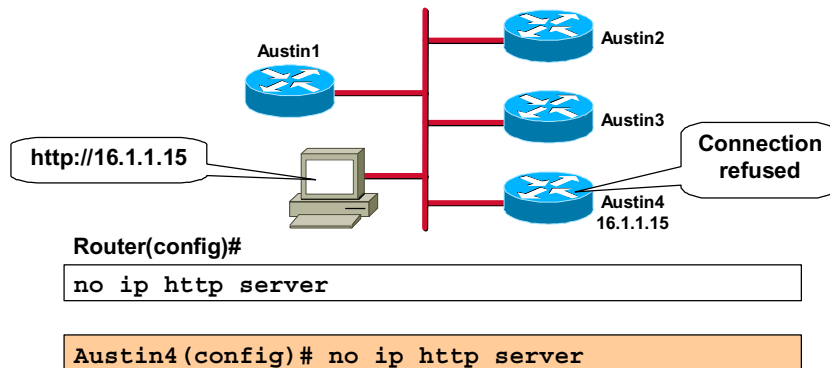This command has no arguments or keywords.

The syntax for the **no service finger** command is as follows:

no service finger

This command has no arguments or keywords.

Disable HTTP Service

Austin1

Austin2

Austin3

http://16.1.1.15

Connection refused

Austin4
16.1.1.15

Router(config)#

```
no ip http server
```

```
Austin4(config)# no ip http server
```

SECUR 1.1—5-16

Most Cisco IOS software releases support remote configuration and monitoring using the World Wide Web's HTTP protocol. In general, HTTP access is equivalent to interactive access to the router. The authentication protocol used for HTTP is equivalent to sending a clear text password across the network. This makes HTTP a relatively risky choice for use across the public Internet. This service is disabled by default.

Note	Several router management tools, such as the Cisco Security Device Manager (SDM), use HTTP to access the router. Do not disable the router HTTP service if SDM, or another HTTP dependent management system, is to be used to manage the router.

If Web-based administration is not required, disable the HTTP service using the **no ip http server** command in global configuration mode as shown in the figure.

The syntax for the **no ip http server** command is as follows:

no ip http server

This command has no arguments or keywords.

If Web-based administration is a requirement for your network, make sure to implement the following:

■ Be sure to configure usernames and passwords as described in the previous lesson. Because the password is sent as clear text, it is recommended that you avoid using the enable password as an HTTP password.

■ Use authentication, authorization, and accounting (AAA) using external AAA servers, whenever possible. As with interactive logins, the best choice for HTTP authentication is a TACACS+ or RADIUS server.

- Use IP access lists to restrict which hosts have Web server access to the routers (presented later in this lesson).

- Use Syslog logging to track who accesses the routers and when (presented later in this lesson).

Note	The latest versions of Cisco IOS crypto images support the use of a secure version of HTTP called HTTPS. If your router IOS image and the Web-based manager both support this feature, use HTTPS for Web-based administration of your routers instead of HTTP.

Disable FTP Server

Austin1
Austin2
Austin3
Austin4
16.1.1.15

ftp 16.1.1.15

Connection refused
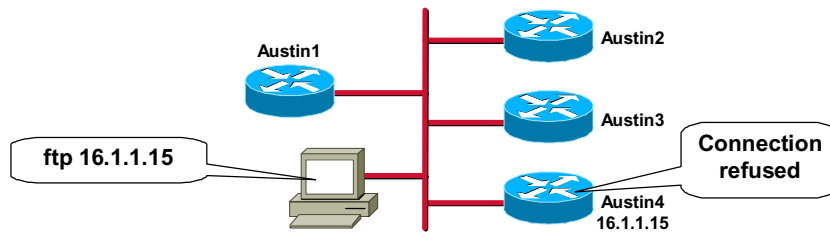
Router(config)#

```
no ftp-server enable
```

```
no ftp-server write-enable
```

```
Austin4(config)# no ftp-server enable
```
```
Austin4(config)# no ftp-server write-enable
```

SECUR 1.1—5-17

The FTP server feature configures a router to act as an FTP server. FTP clients can copy files to and from certain directories on the router. In addition, the router can perform many other standard FTP server functions. This feature first became available in Cisco IOS Software Release 11.3 AA.

FTP access to your routers can be used to gain access to the router file system and therefore can be used to attack the network or the router itself. Unless your routers are being used as FTP servers, you should always disable the FTP server feature.

Starting in Cisco IOS Software Release 12.3, the router FTP service is disabled by default using the **no ftp-server write-enable** command. This can be seen in any Cisco IOS Software Release 12.3 or greater by using the **show running-config** command as shown here (this example shows only a small portion of the **show running-config** command output):

```
Austin4# show running-config
!
!
no ftp-server write-enable
!
```

Routers operating with a Cisco IOS software earlier than release 12.3 should have their FTP servers disabled using the **no ftp-server enable** command, as shown in the figure.

Routers operating with a Cisco IOS Software Release of 12.3 or later, where the FTP server has been manually enabled, should have the FTP server disabled using the **no ftp-server write-enable** command, as shown in the figure.
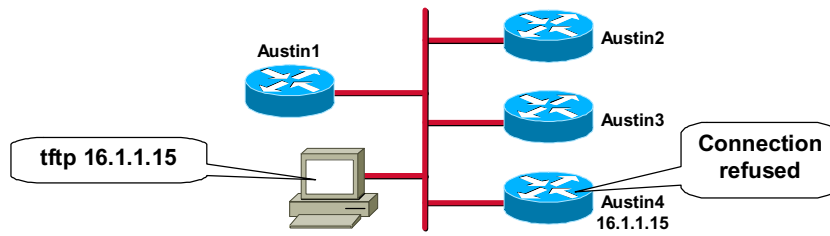
The syntax for the commands is as follows:

no ftp-server enable

no ftp-server write-enable

These commands have no arguments or keywords.

Disable TFTP Server

Austin1

Austin2

Austin3

Connection refused

tftp 16.1.1.15

Austin4
16.1.1.15

Router(config)#

```
no tftp-server flash:
```

```
Austin4(config)# no tftp-server flash:
```

SECUR 1.1—5-18

The TFTP server feature configures a router to act as a TFTP server host. As a TFTP server host, the router responds to TFTP Read Request messages by sending a copy of the system image contained in ROM or one of the system images contained in Flash memory to the requesting host. The TFTP Read Request message must use one of the filenames that are specified in the configuration. This feature is disabled by default.

Flash memory can be used as a TFTP file server for other routers on the network. This feature allows you to boot a remote router with an image that resides in the Flash server memory. Some Cisco devices allow you to specify one of the various Flash memory locations (bootflash:, slot0:, slot1:, slavebootflash:, slaveslot0:, or slaveslot1:) as the TFTP server.

TFTP access to your routers can be used to gain access to the router file system and therefore can be used to attack the network or the router itself. Unless your routers are being used as TFTP servers, you should always disable the TFTP server feature.

Note	Disabling the TFTP server varies across different Cisco router product lines. Always consult the configuration guide for your particular Cisco router model before continuing.

Disable the TFTP server for Flash memory using the **no tftp-server flash:** global configuration command as shown in the figure.

The syntax for the **no tftp-server** command is as follows:

no tftp-server flash: [*partition-number*:]*filename1* [alias *filename2*]

flash:	Specifies TFTP service of a file in Flash memory. Use **flash:** to disable the TFTP server for all files in Flash memory.
partition-number:	(Optional.) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used.

filename1	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.
filename2	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.

Disable IP Directed Broadcast

Cisco.com

Host with falsified source address

Austin1

Austin2

e0/0   e0/1

Target segment

ICMP echo requests to directed broadcast address

Internet

Directed broadcasts dropped
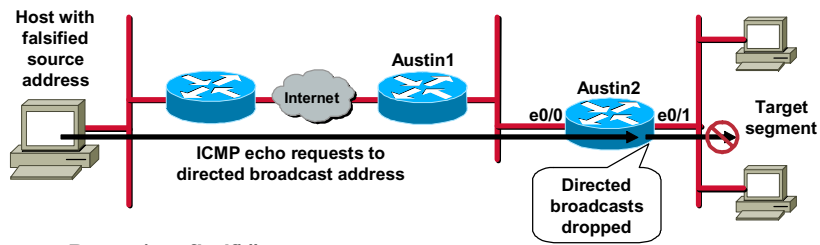
Router(config-if)#

```
no ip directed-broadcast
```

```
Austin2(config)# interface e0/1
Austin2(config-if)# no ip directed-broadcast
```

SECUR 1.1—5-19

IP directed broadcasts are used in the extremely common and popular smurf denial of service attack, and can also be used in related attacks. This service is enabled in Cisco IOS Software Releases < 12.0 and disabled in Cisco IOS Software Releases ≥ 12.0.

An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common.

In a smurf attack, the attacker sends ICMP echo requests from a spoofed source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the spoofed source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely overwhelm the host whose address is being spoofed.

If a Cisco interface is configured with the **no ip directed-broadcast** command, directed broadcasts that would otherwise be converted into link-layer broadcasts at that interface are dropped instead. Note that this means that **no ip directed-broadcast** must be configured on every interface of every router that might be connected to a target subnet; it is not sufficient to configure only perimeter routers. The **no ip directed-broadcast** command is the default in Cisco IOS Software Release 12.0 and later. In earlier releases, the command should be applied to every LAN interface that is not required to forward legitimate directed broadcasts.

Disable IP directed broadcasts using the **no ip directed-broadcast** command in interface configuration mode as shown in the figure.

The syntax for the **no ip directed-broadcast** command is as follows:

no ip directed-broadcast

This command has no arguments or keywords.

Disable ICMP Mask Replies

Austin1

Internet

Austin2

e0/0   e0/1

ICMP mask request to
16.1.1.12

16.1.1.12

No ICMP
mask
replies
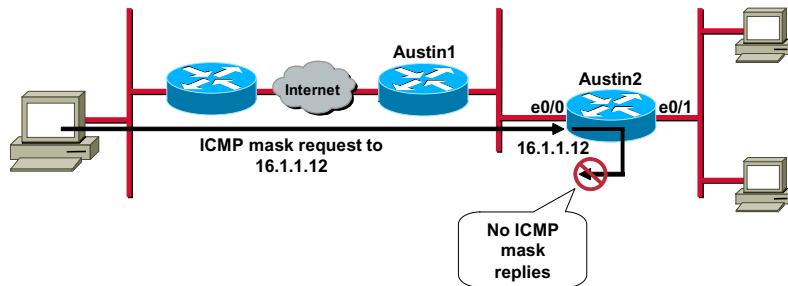
Router(config-if)#

```
no ip mask-reply
```

```
Austin2(config)# interface e0/0
Austin2(config-if)# no ip mask-reply
```

SECUR 1.1—5-21

Mask replies are disabled in Cisco IOS software by default. When mask replies are enabled, the Cisco IOS software responds to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages. These messages can provide an attacker with critical network information in reconnaissance attacks. Automatic replies should be disabled on all router interfaces, especially those pointing to untrusted networks.

Disable IP mask replies using the **no ip mask-reply** command in interface configuration mode as shown in the figure.
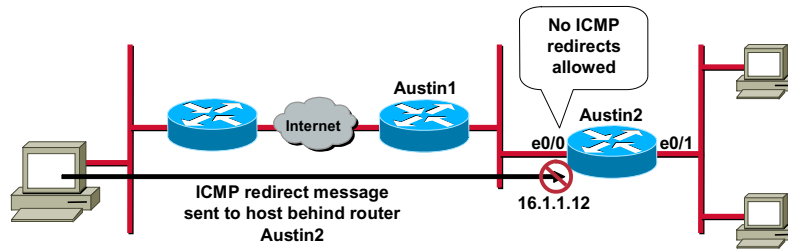
The syntax for the **no ip mask-reply** command is as follows:

no ip mask-reply

This command has no arguments or keywords.

Disable ICMP Redirects

No ICMP redirects allowed

Austin1

Austin2

Internet

e0/0

Austin2

e0/1

ICMP redirect message sent to host behind router Austin2

16.1.1.12

Router(config-if)#

```
no ip redirect
```

```
Austin2(config)# interface e0/0
Austin2(config-if)# no ip redirect
```

SECUR 1.1—5-22

ICMP redirect messages are enabled in Cisco IOS software by default. An ICMP redirect message instructs an end node to use another, more efficient path to a particular destination. In a properly functioning IP network, a router should send redirects only to hosts on its own local subnets, end nodes should never send a redirect, and redirects should never be sent more than one network hop away. However, an attacker may violate these rules.

Disable IP redirects using the **no ip redirect** command in interface configuration mode as shown in the figure.

The syntax for the **no ip redirect** command is as follows:

no ip redirect

This command has no arguments or keywords.

It is a good idea to filter out incoming ICMP redirects at the input interfaces of any router that lies at a border between administrative domains. You should also configure any access list that is applied on the input side of a Cisco router interface to filter out all ICMP redirects. This will cause no operational impact in a correctly configured network.

Note that this filtering prevents a router from ever processing or acting upon any ICMP messages and can also prevent buffer overflow DoS attacks on routers running older Cisco IOS images. It is still possible for attackers to exploit redirect vulnerabilities if their host is directly connected to the same segment as a host that is under attack.

Disable ICMP Unreachable Messages

Router(config-if)#

```
no ip unreachable
```

```
Austin2(config)# interface e0/0
Austin2(config-if)# no ip unreachable
```

SECUR 1.1—5-23

Attackers can use ICMP unreachable messages to map your network. These messages are enabled in Cisco IOS software by default and should be disabled on all interfaces, especially those interfaces connected to untrusted networks.

Disable IP unreachable messages using the **no ip unreachable** command in interface configuration mode as shown in the figure.

The syntax for the **no ip unreachable** command is as follows:

no ip unreachable

This command has no arguments or keywords.

Disable IP Source Routing

```
Router(config)#
no ip source-route
```

```
Austin2(config)# no ip source-route
```

The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that datagram will take toward its ultimate destination, and generally the route that any reply will take on the return trip. These options are sometimes used for performing path analysis and testing, but are rarely utilized during normal traffic patterns. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options. Source routing is enabled in Cisco IOS software by default.

A Cisco router with **no ip source-route** set will never forward an IP packet that carries a source routing option. You should use this command unless you know that your network needs source routing.

Disable IP source routing using the **no ip source-route** command in global configuration mode as shown in the figure.

The syntax for the **no ip source-route** command is as follows:

no ip source-route

This command has no arguments or keywords.

Disable IP Identification

Router(config)#

```
no ip identd
```

```
Austin2(config)# no ip identd
```

SECUR 1.1—5-24

Identification support allows you to query a TCP port for identification. This feature enables RFC 1413, an unsecure protocol for reporting the identity of a client that is initiating a TCP connection and a host responding to the connection.

With identification support, an attacker can connect to a TCP port on a host, issue a simple text string to request information, and get back a simple text-string reply. No attempt is made to protect against unauthorized queries. This service should be explicitly disabled.

Disable RFC 1413 identification using the **no ip identd** global configuration command as shown in the figure.

The syntax for the **no ip identd** command is as follows:

no ip identd

This command has no arguments or keywords.

Disable NTP Service

Router(config)#

```
no ntp
```

```
Austin4(config)# no ntp
```

Router(config-if)#

```
ntp disable
```

```
Austin4(config)# interface e0/0
Austin4(config-if)# ntp disable
```

Corrupting the network time base is one way in which attackers subvert certain security protocols, and for this reason you should disable the Network Time Protocol (NTP) when it is not required. This service is disabled by default.

To disable the NTP service globally, use the **no ntp** command in global configuration mode as shown in the figure.

The syntax for the **no ntp** command is as follows:

no ntp

This command has no arguments or keywords.

If you require NTP for some router interfaces but wish to prohibit its use on specific interfaces, use the **ntp disable** interface configuration command as shown in the figure. Keep in mind that disabling the reception of NTP messages on a router interface does not prevent NTP messages from traversing the router. Use an access list to keep NTP messages from traversing the router interfaces (more on writing access lists later in this lesson).

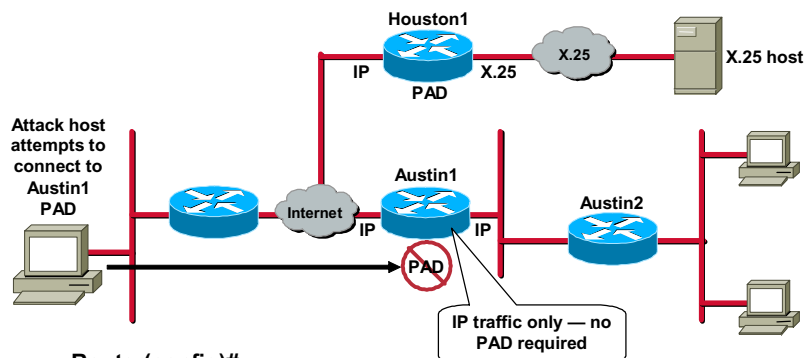The syntax for the **ntp disable** command is as follows:

ntp disable

This command has no arguments or keywords.

If you need to use NTP, it is important that you consider the following:

■ Configure a trusted time source and configure all routers as part of an NTP hierarchy (configure static NTP peer and NTP server addresses).

■ Use NTP authentication.

Disable PAD Service

Houston1

IP   X.25   PAD   X.25   X.25 host

Attack host
attempts to
connect to
Austin1
PAD

Austin1

Internet   IP   IP   Austin2

PAD

IP traffic only — no
PAD required

Router(config)#

```
no service pad
```

```
Austin1(config)# no service pad
```

SECUR 1.1—5-26

The packet assembler/disassembler (PAD) service is, by default, enabled on most Cisco routers. This service is used to enable X.25 connections between the routers and other network devices. One example of where the PAD service is used is when a router must process traffic between a remote IP user and an X.25 host. In this scenario, the remote IP user communicates with the enterprise router PAD service, which then performs any IP-to-X.25 protocol translation and X.25 message forwarding.

Once a connection to the router PAD service is established, an attacker could use the PAD interface to cause disruptions to both route processing and device stability. Therefore, the PAD service should be explicitly disabled when not required for X.25 network operations.

Disable the PAD service using the **no service pad** global configuration command, as shown in the figure.
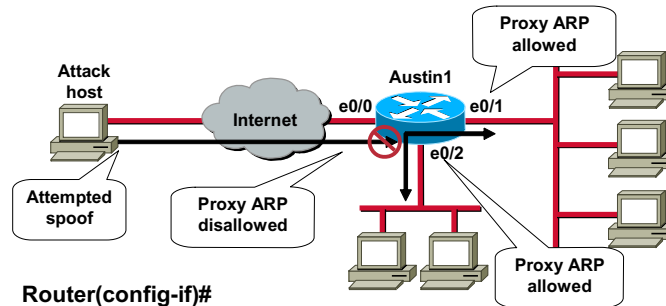
The syntax for the **no service pad** command is as follows:

no service pad

This command has several arguments and keywords but they are not required to disable the PAD service and therefore are not described here.

Disable Proxy ARP

Proxy ARP allowed

Attack host

Austin1

e0/0   e0/1

e0/2

Attempted spoof

Proxy ARP disallowed

Internet

Proxy ARP allowed

Router(config-if)#

```
no ip proxy-arp
```

```
Austin1(config)# interface e0/0
Austin1(config-if)# no ip proxy-arp
```

SECUR 1.1—5-28

When proxy ARP is enabled on a Cisco router, it allows that router to extend the network (at Layer 2) across multiple interfaces (LAN segments). Cisco routers enable proxy ARP on all interfaces by default.

Because proxy ARP allows the traversal of LAN segments, proxy ARP is only safe when used between trusted LAN segments. Attackers can take advantage of the trusting nature of proxy ARP by spoofing a trusted host and then intercepting packets. Because of this inherent security weakness, you should always disable proxy ARP on router interfaces that do not require it, especially those connected to untrusted networks.

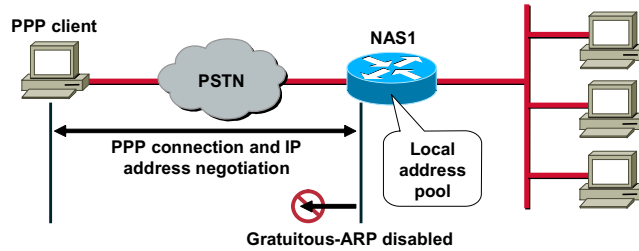Disable proxy ARP using the **no ip proxy-arp** command in interface configuration mode as shown in the figure.

The syntax for the **no ip proxy-arp** command is as follows:

no ip proxy-arp

This command has no arguments or keywords.

Disable Gratuitous ARPs

PPP client

NAS1

PSTN

PPP connection and IP
address negotiation

Local
address
pool

Gratuitous-ARP disabled

Router(config-if)#

```
no ip gratuitous-arps
```

```
NAS1(config)# no ip gratuitous-arps
```

SECUR 1.1—5-29

Most Cisco routers (by default) will send out a gratuitous Address Resolution Protocol (ARP)
message whenever a client connects and negotiates an IP address over a PPP connection.
Gratuitous ARP is the main mechanism used in ARP poisoning attacks. You should disable
gratuitous ARPs unless they are otherwise needed.

Note	Cisco routers generate a gratuitous ARP transmission even when the client receives the address from a local address pool.

Starting with Cisco IOS Software Release 11.3, system administrators can disable gratuitous
ARP transmissions using the **no ip gratuitous-arps** command in global configuration mode, as
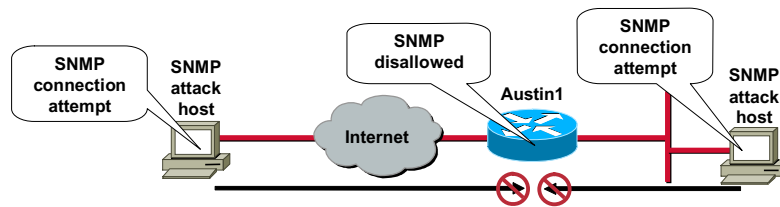shown in the figure.

The syntax for the **no ip gratuitous-arps** command is as follows:

no ip gratuitous-arps

This command has no arguments or keywords.

Disable SNMP

```
Austin1(config)# no snmp-server community public ro
Austin1(config)# no snmp-server community config rw
Austin1(config)# no snmp-server enable traps
Austin1(config)# no snmp-server system-shutdown
Austin1(config)# no snmp-server
```

SECUR 1.1—5-30

The SNMP service allows a router to respond to remote SNMP queries and configuration changes. If you plan on using SNMP, you should restrict which SNMP systems have access to the routers using access lists. When you decide not to use SNMP for a router, you must make sure that you complete several steps to ensure that SNMP is truly unavailable to an attacker. Disabling the SNMP service alone does not fully protect the router. The default for this service depends on the Cisco IOS version.

The following steps should be completed on a Cisco router in order to fully disable SNMP access to that router:

Step 1 Remove any existing SNMP community strings using the **no snmp-server community** command in global configuration mode, as shown in the figure.

The syntax for the **no snmp-server community** command is as follows:

no snmp-server community *string* **[ro | rw]**

string	Community string that you wish to remove.
ro	Specifies that the string to be removed has read-only access.
rw	Specifies that the string to be removed has read-write access.

Step 2 Create an access list that explicitly denies all SNMP messages for this router as shown in the figure (more about writing access lists later in this lesson).

Step 3 Create a new, difficult-to-crack read-only SNMP community string, and make it subject to the new access list you created in step 2 as shown in the figure.

Step 4 Disable all SNMP trap functions using the **no snmp-server enable traps** command in global configuration mode as shown in the figure.

The syntax for the **no snmp-server enable traps** command is as follows:

no snmp-server enable traps [*notification-type*]

notification-type	(Optional.) Type of notification (trap or inform) to disable. If no type is specified (most secure form of the command), all notifications available on the router are disabled.

Step 5 Disable the SNMP system shutdown function using the **no snmp-server system-shutdown** command in global configuration mode as shown in the figure. This prevents an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco SNMP agent on the router.

The syntax for the **no snmp-server system-shutdown** command is as follows:

no snmp-server system-shutdown

This command has no arguments or keywords.

Step 6 Disable the SNMP service using the **no snmp-server** command in global configuration mode as shown in the figure.

The syntax for the **no snmp-server** command is as follows:

no snmp-server

This command has no arguments or keywords.

Disable Small Servers

Router(config)#

```
no service tcp-small-servers
```

Router(config)#

```
no service udp-small-servers
```

```
Austin2(config)# no service tcp-small-servers
Austin2(config)# no service udp-small-servers
```

SECUR 1.1—5-30

By default, Cisco devices up through Cisco IOS Software Release 11.3 offer the "small services": echo, chargen, daytime, and discard. Small services are enabled by default in Cisco IOS Software Release < 11.3 and disabled in Cisco IOS Software Release ≥ 11.3. These services, especially their UDP versions, can be used to launch denial of service and other attacks against the router that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable by the attacker, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the Cisco router UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by using anti-spoofing access lists, the services should almost always be disabled in any router that is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The small services are disabled by default in Cisco IOS Software Release 12.0 and later software. In earlier software, they may be disabled using the commands **no service tcp-small-servers** and **no service udp-small-servers** in global configuration mode as shown in the figure.

The syntax for the **no service tcp-small-servers** command is as follows:

no service tcp-small-servers

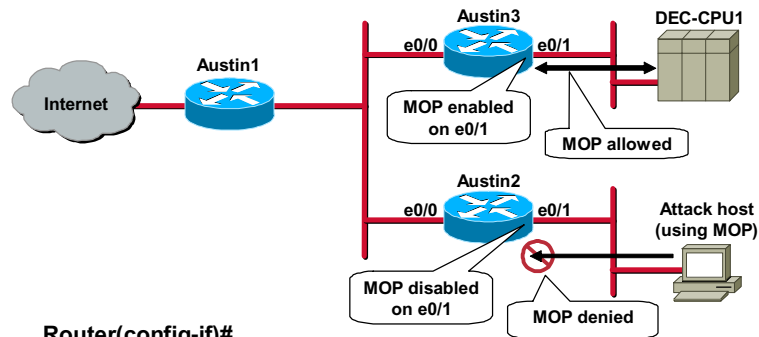This command has no arguments or keywords.

The syntax for the **no service udp-small-servers** command is as follows:

no service udp-small-servers

This command has no arguments or keywords.

Disable MOP Service

Router(config-if)#

```
no mop enabled
```

```
Austin2(config)# interface e0/1
Austin2(config-if)# no mop enabled
```

SECUR 1.1—5-31

The Digital Equipment Corporation Maintenance Operation Protocol (MOP) service is enabled, by default, on many Cisco router interfaces. MOP presents a potential attack vector on the router and therefore should be explicitly disabled at all interfaces that do not require it.
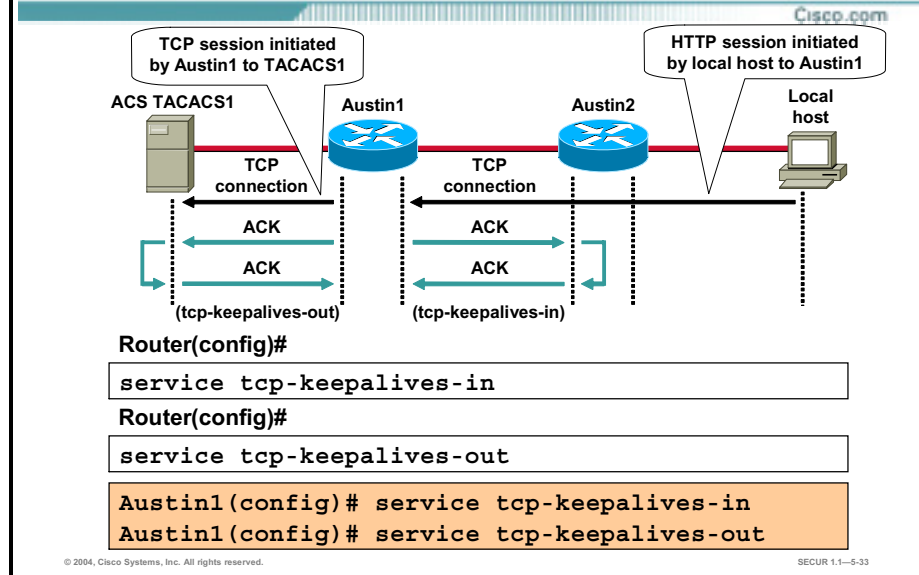
Disable the MOP service using the **no mop enabled** command in interface configuration mode, as shown in the figure.

The syntax for the **no mop enabled** command is as follows:

no mop enabled

This command has no arguments or keywords.

Enable TCP Keepalives

TCP session initiated by Austin1 to TACACS1

HTTP session initiated by local host to Austin1

ACS TACACS1   Austin1   Austin2   Local host

TCP connection   TCP connection

ACK   ACK

ACK   ACK

(tcp-keepalives-out)   (tcp-keepalives-in)

Router(config)#
```
service tcp-keepalives-in
```
Router(config)#
```
service tcp-keepalives-out
```

```
Austin1(config)# service tcp-keepalives-in
Austin1(config)# service tcp-keepalives-out
```

SECUR 1.1—5-33

By default, Cisco routers do not continually test whether a previously connected TCP endpoint is still reachable. If one end of a TCP connection idles out or terminates abnormally (crashes, reloads, and so on), the opposite end of the connection may still believe the session is available. These "orphaned" sessions use up valuable router resources. Attackers have been known to take advantage of this weakness to attack Cisco routers.

To remedy this situation, Cisco routers can be configured to send periodic keepalive messages (one ACK per minute) to ensure that the remote end of a session is still available. If the remote device fails to respond (with another ACK) to the keepalive message within five minutes, the router will clear the connection. This action immediately frees router resources for other more important tasks. Keepalives are important because they help guard against orphaned sessions.

Use the **service tcp-keepalives-in** global configuration command to detect and delete inactive incoming sessions as shown in the figure.

Use the **service tcp-keepalives-out** global configuration command to detect and delete inactive outgoing sessions initiated by the router as shown in the figure.

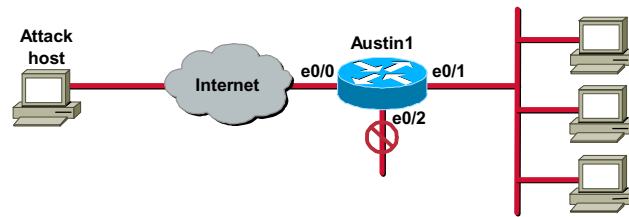The syntax for the **service tcp-keepalives** commands is as follows:

service tcp-keepalives-in

service tcp-keepalives-out

These commands have no arguments or keywords.

Disable Unused Router Interfaces

Router(config-if)#

```
shutdown
```

```
Austin1(config)# interface e0/2
Austin1(config-if)# shutdown
```

SECUR 1.1—5-33

Unused open router interfaces invite unauthorized access to the router and the network. You can limit this type of attack by administratively disabling the unused interfaces on all routers.

Always disable unused router interfaces using the **shutdown** command in interface configuration mode as shown in the figure.

The syntax for the shutdown command is as follows:

shutdown

This command has no keywords or arguments.

Once an interface is shutdown, the router requires administrative privileges to open the interface to new network connections.

Introduction to Cisco Access Lists

This topic provides a review of basic Cisco access list design and implementation.

Cisco routers use access lists as packet filters to decide which packets can access a router service or to allow 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. Access lists contain one or more rules or statements that determine what data is to be permitted and/or denied across an interface.

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

Cisco router security depends strongly on well-written access lists to restrict access to router network services and for filtering packets as they traverse the router.

Either a number or a name can identify Cisco access lists and the protocols they filter.

The table lists access list numbers and their associated types.

Access List Number	Type
1-99	IP standard access list
100-199	IP extended access list
1000-1099	IPX SAP access list
1100-1199	Extended 48-bit MAC address access list

1200-1299	IPX summary address access list
1300-1999	IP standard access list (expanded range)
200-299	Protocol type-code access list
2000-2699	IP extended access list (expanded range)
300-399	DECnet access list
400-499	XNS standard access list
500-599	XNS extended access list
600-699	AppleTalk access list
700-799	48-bit MAC address access list
800-899	IPX standard access list
900-999	IPX extended access list

Starting with Cisco IOS Software Release 11.2, you can identify access lists with an alphanumeric string (a name) rather than a number. Named access lists allow you to configure more access lists in a router than if you were to use numbered access lists alone. If you identify your access list 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 list.

Note	Named access lists will not be recognized by any software release prior to Cisco IOS Software Release 11.2.

Basic Types of IP Access Lists

Cisco.com

Cisco routers support two basic types of IP access lists:

- **Standard—Filter IP packets based on the source address only**
- **Extended—Filter IP packets based on several attributes, including:**
  - **Protocol type**
  - **Source and destination IP addresses**
  - **Source and destination TCP/UDP ports**
  - **ICMP and IGMP message types**

SECUR 1.1—5-36

Cisco routers support two types of IP access lists as shown in the figure:

- Standard IP access lists—This type of IP access list can filter IP packets based on the source address only.

- Extended IP access lists—This type of IP access list can filter IP packets based on several attributes, including the following:

  — Source IP address

  — Destination IP address

  — Source TCP/UDP ports

  — Destination TCP/UDP ports

  — Optional protocol type information for finer granularity of control

Note	Cisco IOS Software Release ≥ 11.1 introduced substantial changes to IP access lists. These extensions are backward compatible; migrating from a release earlier than Release 11.1 to the current image will convert your access lists automatically. However, previous releases are not forward compatible with these changes. Thus, if you save an access list with the current image and then use older software, the resulting access list will not be interpreted correctly. This could cause you severe security problems. Save your old configuration file before booting Release ≥ 11.1 images.

Standard Numbered Access List Format

Router(config)#

```
access-list access-list-number {deny | permit}
  source [source-wildcard]
```

```
Austin2(config)# access-list 2 permit 36.48.0.3
Austin2(config)# access-list 2 deny 36.48.0.0
  0.0.255.255
Austin2(config)# access-list 2 permit 36.0.0.0
  0.255.255.255
```

SECUR 1.1—5-37

Create a standard numbered access list using the **access-list** command, as shown in the figure.

The syntax for the standard numbered **access-list** command is as follows:

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

access-list-number	This number serves a dual purpose: ■ It is the unique identifier of the access list. ■ It specifies that this is a standard IP protocol access list (range 1-99 and 1300-1999).
deny	Drops all packets matching the specified source address.
permit	Allows packets matching the specified source address.
source	Specifies the IP address of a host or group of hosts (if a wildcard mask is also specified) whose packets are to be examined.
source-wildcard	The wildcard mask applied to the source to determine a source group of hosts whose packets are to be examined. Note that when no mask is specified, the default mask becomes **0.0.0.0**.

In the example shown in the figure, the first line of access list 2 permits the single host with IP address 36.48.0.3. The second line denies all other hosts on subnet 36.48.0.0. The last line permits all other hosts on the 36.0.0.0 network.

Note	When building either standard or extended access lists, by default, the end of the access list contains an implicit **deny all** statement. Further, with standard access lists, if you omit the mask from the access list entry, the mask defaults to **0.0.0.0**.

In addition to the keywords specified above, standard numbered IP access lists also support the following keywords:

any	Specifies any host. This is the same as using an IP address and wildcard mask of: **0.0.0.0 255.255.255.255**.
host	Specifies an exact host match. This is the same as specifying a wildcard mask of: **0.0.0.0**.
log	Enables logging of packets that match the deny or permit statements (Cisco IOS Software Release ≥ 11.3).

Starting with Cisco IOS Software Release 11.3(3)T, standard access lists can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the access list will cause an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** command. This capability was previously only available in extended IP access lists.

The first packet that triggers the access list causes an immediate logging message. Subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

Note	The router logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be solely relied upon as a security tool as it may not be an accurate source of the number of matches to an access list.

Standard Named Access List Format

Router(config)#

```
ip access-list standard access-list-name
```

Router(config-std-nacl)#

```
{deny | permit} source [source-wildcard]
```

```
Austin2(config)# ip access-list standard protect
Austin2(config-std-nacl)# deny 36.48.0.0
  0.0.255.255
Austin2(config-std-nacl)# permit 36.0.0.0
  0.255.255.255
Austin2(config-std-nacl)# exit
```

SECUR 1.1—5-39

Note	Named access lists will not be recognized by any software release prior to Cisco IOS Software Release 11.2.

Complete the following steps to create a standard named access list:

Step 1 Enter the **ip access-list standard** command in global configuration mode, as shown in the figure.

The syntax for the **ip access-list standard** command is as follows:

ip access-list standard *access-list-name*

access-list-name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Step 2 Enter the **deny** or **permit** command in standard named access list mode, as shown in the figure.

The syntax for these standard named access list commands is as follows:

{deny | permit} *source* **[***source-wildcard***]**

deny	Drops all packets matching the specified source address.
permit	Allows packets matching the specified source address.
source	Specifies the IP address of a host or group of hosts (if a wildcard mask is also specified) whose packets are to be examined.
source-wildcard	The wildcard mask applied to the source to determine a source group of hosts whose packets are to be examined.

In addition to the keywords specified above, standard named IP access lists also support the following keywords:

any	Specifies any host. This is the same as using an IP address and wildcard mask of: **0.0.0.0 255.255.255.255**.
host	Specifies an exact host match. This is the same as specifying a wildcard mask of: **0.0.0.0**.
log	Enables logging of packets that match the deny or permit statements (Cisco IOS Software Release ≥ 11.3).

Starting with Cisco IOS Software Release 11.3(3)T, standard access lists can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the access list will cause an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** command. This capability was previously only available in extended IP access lists.

The first packet that triggers the access list causes an immediate logging message. Subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

Note	The router logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be solely relied upon as a security tool as it may not be an accurate source of the number of matches to an access list.

Extended Numbered Access List Format
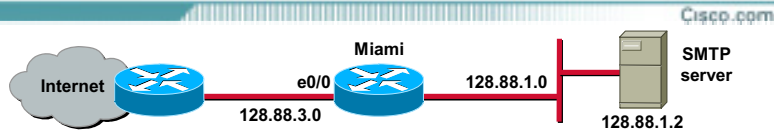
Miami

Internet

e0/0

128.88.3.0

128.88.1.0

SMTP server

128.88.1.2

Router(config)#

```
access-list access-list-number {deny | permit}
  {protocol-number | protocol-keyword}{source
  source-wildcard | any | host} {source-port}
  {destination destination-wildcard | any | host}
  {destination-port} [established][log | log-input]
```

```
Miami(config)# access-list 103 permit tcp any
  128.88.0.0 0.0.255.255 established
Miami(config)# access-list 103 permit tcp any host
  128.88.1.2 eq smtp
```

SECUR 1.1—5-40

Extended access lists allow packet filtering on source and destination addresses, protocol type, source and destination port, as well as several protocol-dependent options.

Create a extended numbered access list using the **access-list** command in global configuration mode as shown in the figure.

The syntax for the **access-list** command is as follows:

access-list *access-list-number* {**deny** | **permit**} {*protocol-number* | *protocol-keyword*}
{*source source-wildcard* | **any** | **host**} {*source-port*} {*destination destination-wildcard* | **any** | **host**} {*destination-port*} [**established**] [**log** | **log-input**]

access-list-number	This number serves a dual purpose: ■ It is the unique identifier of the access list. ■ It specifies that this is a extended IP protocol access list (range 100-199 and 2000-2699).
deny	Drops all packets matching the specified source address.
permit	Allows packets matching the specified source address.
protocol-number	Integer in the range of 0-255 that represents an IP protocol.
protocol-keyword	Name of an IP protocol. Can be one of the following: **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**.
source	IP address of the host or network where the packet originated.
source-wildcard	The wildcard mask applied to the source IP address.
source-port	Specifies the port that the packet originated from. This can be the actual port number (for example; **80**), or the common name (for example; **HTTP**).
destination	IP address of the host or network where the packet is being sent.

destination-wildcard	The wildcard mask applied to the destination IP address.
destination-port	Specifies the port number to which the packet is being sent. This can be the actual port number (for example; **80**), or the common name (for example; **HTTP**).
established	(TCP only.)Verifies if either the RST or ACK bit is set. If either of these bits is set, the packet is part of a previously established connection. This can be used to restrict TCP responses to one direction when sessions are initiated from the opposite direction.
log	Enables logging of packets that match the deny or permit statements.
log-input	Includes the input interface, source MAC address or VC in the logging output.
any	Specifies any host. This is the same as using an IP address and wildcard mask of: **0.0.0.0 255.255.255.255**.
host	Specifies an exact host match. This is the same as specifying a wildcard mask of: **0.0.0.0**.

In the example in the figure, the Miami router interface e0/0 is part of a Class B network with the address 128.88.0.0. The mail server, with the address 128.88.1.2, delivers Internet mail. The **established** keyword within the access list is used only for TCP datagrams to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, indicating that the packet belongs to an existing connection. In this scenario, if the ACK bit is not set and the SYN bit is set, then someone on the Internet has initialized the session and the packet is denied.

Note	When building either standard or extended access lists, by default, the end of the access list contains an implicit **deny all** statement.

Extended Named Access List Format

Router(config)#

```
ip access-list extended access-list-name
```

Router(config-ext-nacl)#

```
{deny | permit} {protocol-number | protocol-
  keyword} {source source-wildcard | any | host}
  {source-port} {destination destination-wildcard
  | any | host} {destination-port}
  [established][log | log-input]
```

```
Miami(config)# ip access-list extended mailblock
Miami(config-ext-nacl)# permit tcp any
  128.88.0.0 0.0.255.255 established
Miami(config-ext-nacl)# permit tcp any host
  128.88.1.2 eq smtp
Miami(config-ext-nacl)# exit
```

SECUR 1.1—5-40

Note	Named access lists will not be recognized by any software release prior to Cisco IOS Software Release 11.2.

Complete the following steps to create a extended named access list:

Step 1 Enter the **ip access-list extended** command in global configuration mode as shown in the figure.

The syntax for the **ip access-list extended** command is as follows:

ip access-list extended *access-list-name*

access-list-name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Step 2 Enter the **deny** or **permit** command in extended named access list mode as shown in the figure.

The syntax for the extended named access list **deny** and **permit** commands is as follows:

{deny | permit} {*protocol-number* | *protocol-keyword***}**
{*source source-wildcard* | **any** | **host} {***source-port***} {***destination destination-wildcard* | **any** | **host} {***destination-port***} [established] [log | log-input]**

deny	Drops all packets matching the specified source address.
permit	Allows packets matching the specified source address to flow through the interface.
protocol-number	Integer in the range of 0-255 that represents an IP protocol.

protocol-keyword	Name of an IP protocol. Can be one of the following: **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**.
source	IP address of the host or network where the packet originated.
source-wildcard	The wildcard mask applied to the source IP address.
source-port	Specifies the port that the packet originated from. This can be the actual port number (for example; **80**), or the common name (for example; **HTTP**).
destination	IP address of the host or network where the packet is being sent.
destination-wildcard	The wildcard mask applied to the destination IP address.
destination-port	Specifies the port number to which the packet is being sent. This can be the actual port number (for example; **80**), or the common name (for example; **HTTP**).
established	(TCP only.)Verifies if either the RST or ACK bit is set. If either of these bits is set, the packet is part of a previously established connection. This can be used to restrict TCP responses to one direction when sessions are initiated from the opposite direction.
log	Enables logging of packets that match the deny or permit statements.
log-input	Includes the input interface, source MAC address or VC in the logging output.
any	Specifies any host. This is the same as using an IP address and wildcard mask of: **0.0.0.0 255.255.255.255**.
host	Specifies an exact host match. This is the same as specifying a wildcard mask of: **0.0.0.0**.

Note   When building either standard or extended access lists, by default, the end of the access list contains an implicit **deny all** statement.

In addition to the keywords specified above, both extended numbered IP access lists and extended named IP access lists also support the following keywords:

icmp-type	Specifies that the access list perform filtering based on the ICMP message type (**0–255**).
icmp-message	Specifies that the access list perform filtering based on the ICMP message symbolic name (for example; **echo-reply**).
precedence *precedence*	Specifies that the access list perform filtering based on the precedence level name or number (0-7).
remark	Used to add remarks (up to 100 characters long) to access lists (Cisco IOS Software Release ≥ 12.0).

Commenting IP Access List Entries

Router(config)#

```
remark message
```

```
Miami(config)# access-list 102 remark Allow
  traffic to file server
Miami(config)# access-list 102 permit ip any
  host 128.88.1.6
```

SECUR 1.1—5-41

To write a helpful comment (remark) for an entry in an IP access list, use the **remark** access-list configuration command in global configuration mode, as shown in the figure.

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

remark *message*

message	The remark to add to the access list (100 character maximum).

Before you start to develop any access lists, consider the following basic rules:

■ Rule 1: Write it out—Never sit down at a router and start to develop an access list without first spending some time in design. The best access list developers suggest that you write out a list of things you want the access list to accomplish. Starting with something as simple as, "This access list must block all SNMP access to the router except for the SNMP host at 16.1.1.15." will do.

■ Rule 2: Set up a development system—Whether this is your laptop PC or a dedicated server, you need a place to develop and store your access lists. Word processors or text editors of any kind will do, as long as you can save the files in ASCII text format. Build yourself a library of your most commonly used access lists and use them as sources for new files. Access lists can be pasted into the router's running configuration (requires console or Telnet access), or can be stored in a router configuration file. The system you chose 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 access lists. 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.

■ Rule 3: Test—If at all possible, test your access lists in a secure environment before placing them into production. This is a common sense approach to any router configuration changes with most enterprises maintaining their own network test beds. Yes, testing costs money, but it can save a lot more time and money in the long run.

Access List Directional Filtering
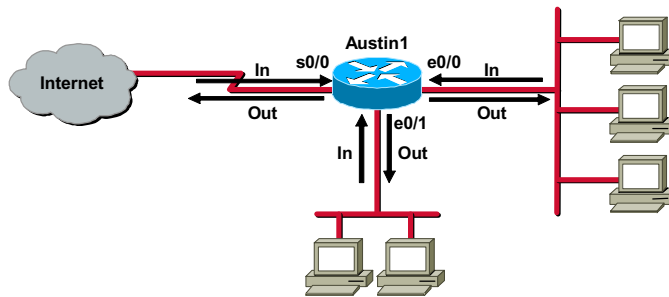
- **Inbound (in)—Data flows toward router interface.**
- **Outbound (out)—Data flows away from router interface.**

SECUR 1.1—5-43

Packet filtering access lists must be applied to a router interface to take effect. It is important to note that access lists are applied to an interface based on the direction of the data flow as shown in the figure.

■ Inbound (in)—The packet filtering access list applies to packets received on the router interface.

■ Outbound (out)—The packet filtering access list applies to packets transmitted out of the router interface.

Applying Access Lists to Interfaces

Router(config)#

```
ip access-group {access-list-number | access-
 list-name} {in | out}
```

```
Tulsa(config)# interface e0/1
Tulsa(config-if)# ip access-group 2 in
Tulsa(config-if)# exit
Tulsa(config)# interface e0/2
Tulsa(config-if)# ip access-group mailblock out
```

SECUR 1.1—5-44

Before applying a packet filtering access list to a router interface, make sure you know which direction it will be filtering.

Apply access lists to router interfaces using the **ip access-group** command in interface configuration mode as shown in the figure.

The syntax for the **ip access-group** command is as follows:

ip access-group {*access-list-number* | *access-list-name*} {**in** | **out**}

access-list-number	Number of the IP standard numbered or IP extended numbered access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
access-list-name	Name of the IP standard named or IP extended named access list as specified by the **ip access-list** command.
in	Filters on inbound (flowing toward router interface) packets.
out	Filters on outbound (flowing away from router interface) packets.

Displaying Access Lists

Router#

```
show access-lists {access-list-number | access-
    list-name}
```

```
Miami# show access-lists
Extended IP access list 102
  permit ip any host 128.88.1.6
Extended IP access list mailblock
  permit tcp any 128.88.0.0 0.0.255.255
    established
Miami#
```

SECUR 1.1—5-45

Display current router access lists using the **show access-lists** command in privileged EXEC mode as shown in the figure.

The syntax for the **show access-lists** command is as follows:

show access-lists {*access-list-number* | *access-list-name***}**

access-list-number	Number of the IP standard numbered or IP extended numbered access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
access-list-name	Name of the IP standard named or IP extended named access list as specified by the **ip access-list** command.

Optionally, you may use the **show ip interface** command to view which ACLs are bound to which router interfaces.

The syntax for the **show ip interface** command is as follows:

show ip interface [*type number***]**

type	(Optional.) Specifies the interface type.
number	(Optional.) Specifies the interface number.

Copyright © 2004, Cisco Systems, Inc.

Enable Turbo ACLs

Cisco.com

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

Router(config)#

```
access-list compiled
```

Router#

```
show access-list compiled
```

```
R2(config)# access-list compiled
R2(config)# exit
R2# show access-list compiled
```

SECUR 1.1—5-46

Cisco IOS Software Releases ≥ 12.0(6)S support the compiling of access lists into turbo ACLs for certain models of Cisco routers. Access lists are normally searched sequentially to find a matching rule, and are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point that searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo ACL feature compiles the access lists into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The benefits of this feature include the following:

■　For ACLs larger than 3 entries, the CPU load required to match the packet to the predetermined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring additional CPU overhead penalties. The larger the ACL, the greater the benefit.

■　The time taken to match the packet is fixed, so that latency of the packets are smaller (significantly in the case of large ACLs) and more importantly, consistent, allowing better network stability and more accurate transit times.

If your router supports turbo ACLs, you should use the **access-list compiled** command in global configuration mode as shown in the figure whenever you develop access lists with more than three statements.

The syntax for the **access-list compiled** command is as follows:

access-list compiled

This command has no keywords or arguments.

To view the status of your turbo access lists, use the **show access-lists compiled** command in privileged EXEC mode as shown in the figure.

The syntax for the **show access-lists compiled** command is as follows:

show access-lists compiled

This command has no keywords or arguments.

So far, this lesson has discussed two basic types of Cisco access lists:

■ Standard

■ Extended

However, these are not the only types of access lists supported by Cisco routers. Enhanced types of access lists have been designed to better secure routers and their networks as shown in the figure.

These enhanced access lists are described as follows:

■ Dynamic—Dynamic access lists (also known as lock and key), create specific, temporary openings in response to user authentication. The syntax for dynamic access lists is very similar to extended access lists. Dynamic access lists are available in Cisco IOS Software Release ≥ 11.1.

   Here is an example of using a dynamic access list:

— A user originates a Telnet session with a router.

— The router authenticates the user with a username and password lookup.

— The router closes the Telnet session and creates a dynamic entry in the access list permitting packets from the authenticated user's source IP address.

— Once the user closes the session, the dynamic entry goes away.

■ Time-based—These access lists are simply numbered or named access lists that are implemented based upon the time of day or the day of the week. They make it easier to implement changes to your routing plans for after hours, weekends, or for other time and day related organizational events. Time-based access lists are available in Cisco IOS Software Releases ≥ 12.0.

■ Reflexive—These access lists create dynamic entries for IP traffic on one interface of the router based upon sessions originating from a different interface of the router. This allows

you to control connections on the untrusted side of a router when a connection is initiated from the trusted side. These access lists are actually modified extended IP named access lists. Reflexive access lists are available in Cisco IOS Software Release ≥ 11.3.

- Context-based access control (CBAC)—Where reflexive access lists can only secure single-channel applications like Telnet, CBAC can secure multichannel operations based on upper-layer information. CBAC examines packets as they enter or leave router interfaces, and determines which application protocols to allow. CBAC access lists are available in Cisco IOS Software Release ≥ 12.0T as part of the Firewall feature set.

For now, it is important that you understand how to use standard and extended access lists. These enhanced types of access lists will be covered in more depth later in this course.

There are several caveats to consider when working with access lists:

- Implicit deny all—All Cisco access lists end with an implicit deny all statement. Although you may not actually see this statement in your access lists, they do exist.

- Standard access list limitation—Because standard access lists are limited to packet filtering on source addresses only, you may need to create extended access lists to implement your security policies.

- Statement evaluation order—Access list statements are evaluated in a sequential (top down) order starting with the first entry in the list. This means that it is very important that you consider the order in which you place statements in your access lists.

- Specific statements—Certain access list statements are more specific than others and therefore should be placed higher in the access list. 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 access list do not negate any statements found lower in the list.

- Directional filtering—Cisco access lists 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 access list is filtering.

- Adding statements—New statements added to an existing access list will always be appended to the bottom of the access list. Because of the inherent top down statement evaluation order of access lists, these new entries may render the access list unusable. In these cases, a new access list will need to be created (with the correct statement ordering), the old access list deleted, and the new access list assigned to the router interface.

- Special packets—Router generated packets such as routing table updates, are not subject to outbound access list 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 access lists on adjacent routers or through other router filter mechanisms using ACLs.

- Extended access list placement—Extended access lists 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 access lists on routers as close as possible to the source being filtered.

- Standard access list placement—Because standard access lists filter packets based on the source address, placing these access lists to close to the source can adversely impact packets destined to other destinations. Always place standard access lists as close to the destination as possible.

Using Access Lists to Mitigate Security Threats

This topic explains how to use access lists to mitigate common perimeter router security threats.
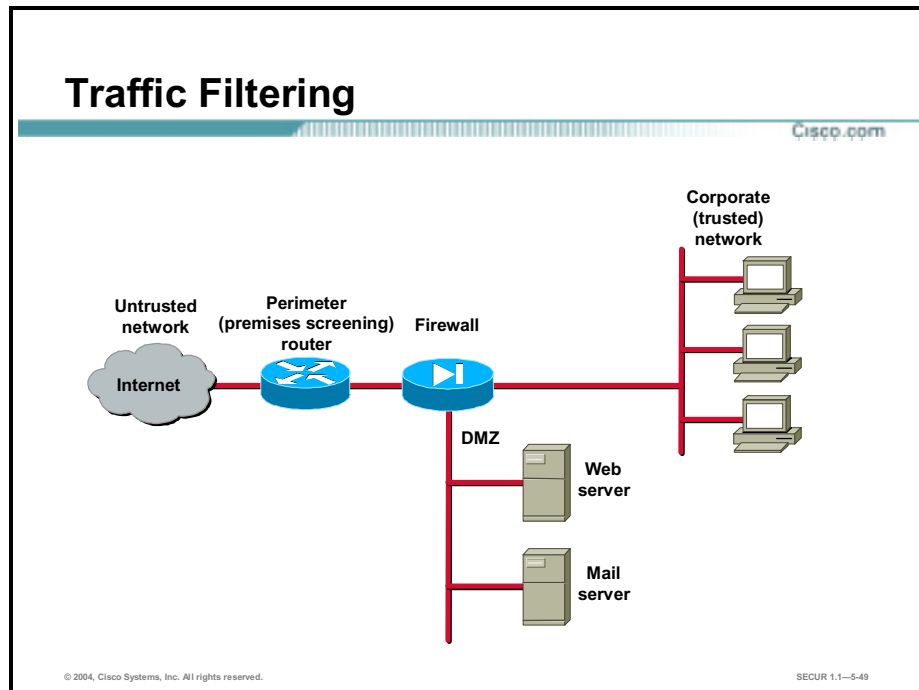
To review, always apply the following general rules when deciding how to handle router services, ports, and protocols:

■ 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 access control lists.

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

The following 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, they should not be allowed to traverse the router. Block these services inbound to the protected network and outbound to the Internet using access lists.

Service	Port	Transport
tcpmux	1	TCP and UDP
echo	7	TCP and UDP
discard	9	TCP and UDP

| systat	11	TCP
daytime	13	TCP and UDP
netstat	15	TCP
chargen	19	TCP and UDP
time	37	TCP and UDP
whois	43	TCP
bootp	67	UDP
tftp	69	UDP
subdup	93	TCP
sunrpc	111	TCP and UDP
loc-srv	135	TCP and UDP
netbios-ns	137	TCP and UDP
netbios-dgm	138	TCP and UDP
netbios-ssn	139	TCP and UDP
xdmcp	177	UDP
netbios (ds)	445	TCP
rexec	512	TCP
lpr	515	TCP
talk	517	UDP
ntalk	518	UDP
uucp	540	TCP
Microsoft UPnP SSDP	1900, 5000	TCP and UDP
nfs	2049	UDP
X Window System	6000-6063	TCP
irc	6667	TCP
NetBus	12345	TCP
NetBus	12346	TCP
Back Orifice	31337	TCP and UDP

The following 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 access lists.

Service	Port	Transport
finger	79	TCP
snmp	161	TCP and UDP
snmp trap	162	TCP and UDP
rlogin	513	TCP

who	513	UDP
rsh, rcp, rdist, rdump	514	TCP
syslog	514	UDP
new who	550	TCP and UDP

There are several 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 access list.

■ Restrict access to the service using access lists—If your situation requires limited access to a service, then build and test appropriate access lists that are applied to the service.

Theoretical Network
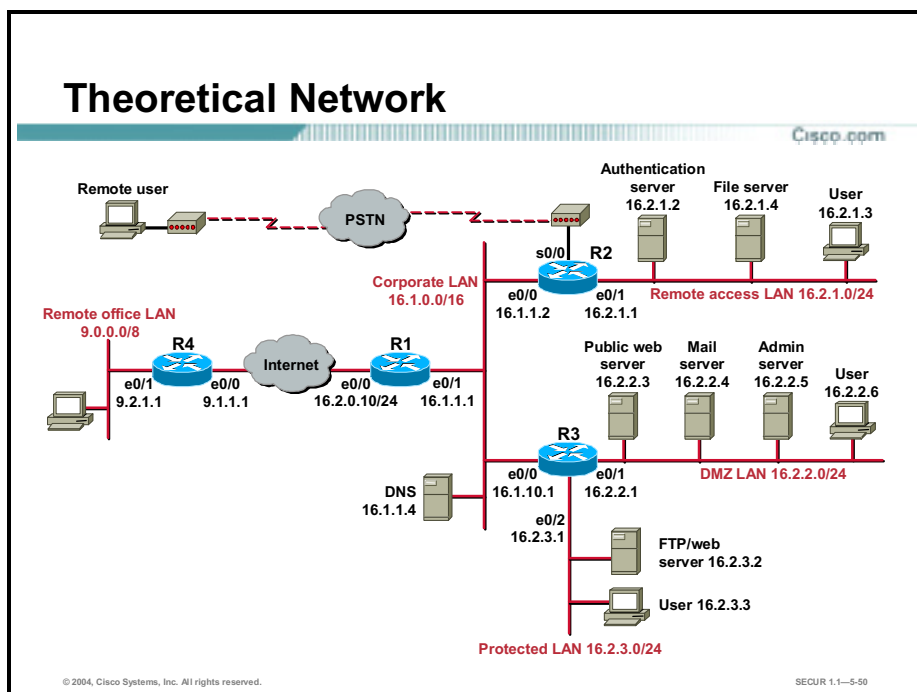
This figure contains a theoretical network that will be referenced throughout the remainder of this lesson.

Note   For the sake of clarity, the access lists contained in the following topics are depicted as individual access lists. Generally, you will not build many small access lists as shown here. Most likely, you would build at least one access list for the outside router interface, one for the inside router interface, and one or more access lists for general router use. Do not attempt to combine the small examples shown here into these larger lists, as the statements will tend to contradict one another. A sample router configuration is shown at the end of this lesson which details how these functions are combined into logical access lists.

Filtering Router Service Traffic

This topic explains how to implement access lists for filtering IP traffic destined for the following router services:
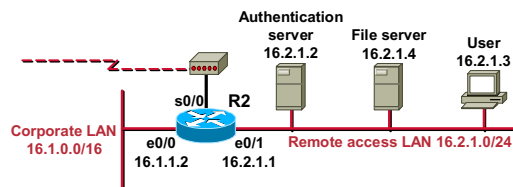
- Telnet

- SNMP

- OSPF

Telnet Service Filtering

```
R2(config)# access-list 90 permit host 16.2.1.3 log
R2(config)# access-list 90 permit host 16.2.1.2 log
R2(config)# access-list 90 deny any log
R2(config)# line vty 0 4
R2(config-line)# access-class 90 in
R2(config-line)# end
```

SECUR 1.1—5-53
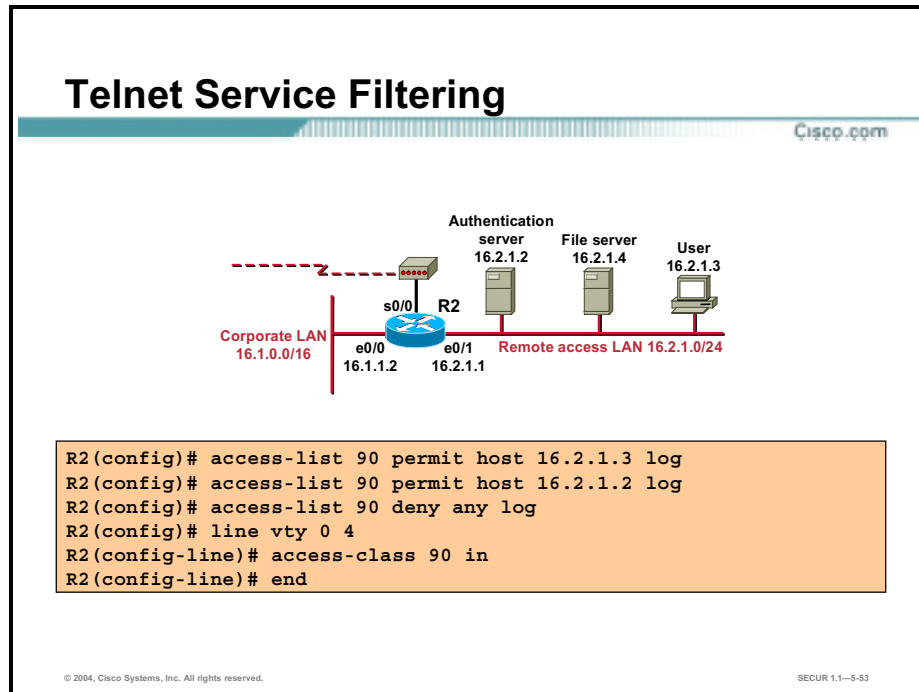
Telnet (vty) is typically used by systems administrators to remotely access the router console for configuration and maintenance. You should restrict which hosts have access to the vty lines of the router by using an access list as shown in the figure.

In this example, IP standard access list 90 allows only hosts 16.2.1.3 and 16.2.1.2 to access router R2 using Telnet (port 23). All other hosts are denied Telnet access to R2. This access list is also designed to log all attempts to access R2 using Telnet, successful and unsuccessful.

SNMP Service Filtering

Cisco.com

Authentication server 16.2.1.2
File server 16.2.1.4
User 16.2.1.3

s0/0 R2

Corporate LAN 16.1.0.0/16
e0/0 16.1.1.2
e0/1 16.2.1.1
Remote access LAN 16.2.1.0/24

```
R2(config)# access-list 80 permit host 16.2.1.3
R2(config)# snmp-server community snmp-host1 ro 80
```
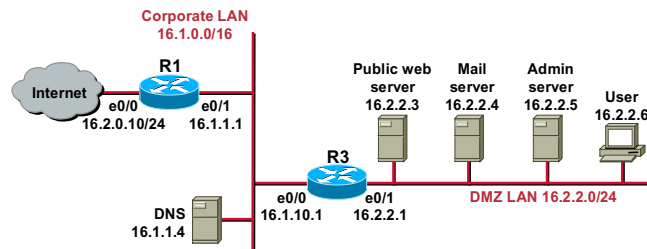
SECUR 1.1—5-53

Because of the inherent lack of authentication in SNMPv1, this version of SNMP should be utilized only on protected, internal networks. You should limit access to a router's SNMP agent using an access list as shown in the figure.

In this example, only the SNMP host with IP address 16.2.1.3 may access router R2's SNMP agent. It further specifies that the SNMP host must use a community string of snmp-host1.

Note	The latest Cisco IOS versions support SNMPv3, which offers more secure SNMP operations. It is recommended that you implement SNMPv3 whenever possible instead of older SNMP versions.

OSPF Route Filtering

Corporate LAN
16.1.0.0/16

R1

Internet

e0/0   e0/1
16.2.0.10/24 16.1.1.1

Public web   Mail   Admin
server   server   server   User
16.2.2.3   16.2.2.4 16.2.2.5   16.2.2.6

R3

e0/0   e0/1
16.1.10.1   16.2.2.1   DMZ LAN 16.2.2.0/24

DNS
16.1.1.4

```
R1(config)# access-list 12 deny 16.2.2.0 0.0.0.255
R1(config)# access-list 12 permit any
R1(config)# router ospf 1
R1(config-router)# distribute-list 12 out
R1(config-router)# end
```

SECUR 1.1—5-55

Cisco routers share routing table update information to provide directions on where to route traffic. Access lists should be used to limit which routes a router will accept (take in) or advertise (send out) to its counterparts.

The example in the figure shows a standard IP access list as it is applied to the OSPF routing protocol, with process-id 1. In this example, router R1 will not advertise out interface e0/0 any routes of the 16.2.2.0 DMZ network.

Filtering Network Traffic

This topic explains how to implement access lists for mitigating the following threats:

- IP address spoofing—Inbound
- IP address spoofing—Outbound
- DoS TCP SYN attacks—Blocking external attacks
- DoS TCP SYN attacks—Using TCP intercept
- DoS Smurf attacks
- Filtering ICMP messages—Inbound
- Filtering ICMP messages—Outbound
- Filtering traceroute

IP Address Spoof Mitigation—Inbound

Cisco.com

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 150 deny ip 16.2.1.0 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 10.0.0.0 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 192.168.0.0 0.0.255.255 any log
R2(config)# access-list 150 deny 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 16.2.1.0 0.0.0.255
R2(config)# interface e0/0
R2(config-if)# ip access-group 150 in
R2(config-if)# exit
```

SECUR 1.1—5-56

As a rule, you should not allow any IP packets inbound to a private network that contain the source address of any internal hosts or networks.

The example in the figure shows access list 150 for router R2. In this example, any packets containing the following IP addresses in their source field will be denied:

- Denies any addresses from the internal 16.2.1.0 network.
- Denies any local host addresses (127.0.0.0/8).
- Denies any reserved private addresses (RFC 1918).
- Denies any addresses in the IP multicast address range (224.0.0.0/4).

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

IP Address Spoof Mitigation— Outbound

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 105 permit ip 16.2.1.0 0.0.0.255 any
R2(config)# access-list 105 deny ip any any log
R2(config)# interface e0/1
R2(config-if)#ip access-group 105 in
R2(config-if)# end
```

SECUR 1.1—5-57

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 access list 105 for router R2. This access list permits only those packets that contain source addresses from the 16.2.1.0/24 network and denies all others.

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

Note	Cisco routers running Cisco IOS Software Release ≥12.0 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

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 109 permit tcp any 16.2.1.0 0.0.0.255
  established
R2(config)# access-list 109 deny ip any any log
R2(config)# interface e0/0
R2(config-if)#ip access-group 109 in
R2(config-if)# end
```

SECUR 1.1—5-58

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

The access list in the figure is designed to prevent inbound packets, with the SYN flag set, from entering the router. However, it does allow TCP responses from the outside network for requests that originated on the inside network.

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 it 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

Cisco.com

R2
e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 111 deny ip any host 16.2.1.255 log
R2(config)# access-list 111 deny ip any host 16.2.1.0 log
R2(config)# interface e0/0
R2(config-if)# ip access-group 111 in
R2(config-if)# end
```

SECUR 1.1—5-60

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

The access list in the figure blocks all IP packets originating from any host destined for the broadcast addresses specified (16.2.1.255 and 16.2.1.0).

Note	Cisco IOS Software Releases ≥ 12.0 now have **no ip directed-broadcast** on by default, preventing this type of ICMP attack. Therefore, you may not need to build an ACL as shown here.

Filtering ICMP Messages—Inbound

R2

e0/0 e0/1 Remote access LAN 16.2.1.0/24
16.1.1.2 16.2.1.1

```
R2(config)# access-list 112 deny icmp any any echo log
R2(config)# access-list 112 deny icmp any any redirect log
R2(config)# access-list 112 deny icmp any any mask-request log
R2(config)# access-list 112 permit icmp any 16.2.1.0 0.0.0.255
R2(config)# interface e0/0
R2(config-if)# ip access-group 112 in
R2(config-if)# end
```

SECUR 1.1—5-61

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 access list shown in the figure blocks all ICMP echo and redirect messages. As an added safety measure, this access list also blocks mask-request messages. All other ICMP messages inbound to the 16.2.1.0/24 network are allowed.

Filtering ICMP Messages—Outbound

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any echo
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any
  parameter-problem
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any
  packet-too-big
R2(config)# access-list 114 permit icmp 16.2.1.0 0.0.0.255 any
  source-quench
R2(config)# access-list 114 deny icmp any any log
R2(config)# interface e0/1
R2(config-if)# ip access-group 114 in
R2(config-if)# end
```

SECUR 1.1—5-62

The following 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 rule, you should block all other ICMP message types outbound.

The access list shown in the figure permits all of the required ICMP messages outbound while denying all others.

Filtering UDP Traceroute Messages

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 120 deny udp any any range 33400 34400 log
R2(config)# interface e0/0
R2(config-if)# ip access-group 120 in
R2(config-if)# end
R2(config)# access-list 121 permit udp 16.2.1.0 0.0.0.255 any range
   33400 34400 log
R2(config)# interface e0/1
R2(config-if)# ip access-group 121 in
R2(config-if)# end
```

SECUR 1.1—5-64

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

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

DDoS Mitigation

This topic explains how to configure your routers to help reduce the effect of distributed denial of service (DDoS) attacks.

Generally, routers cannot prevent all DDoS attacks, but they can help reduce the number of occurrences by building access lists that filter known attack ports.

This topic explains how to block the following DDoS agents:

- Trin00
- Stacheldraht
- Trinity v3
- SubSeven

Note	Blocking these ports may have an impact on regular network users as they 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.

The following access list rules are generally applied to inbound and outbound traffic between the protected network and the Internet.

DDoS Attack Mitigation—Trin00

Cisco.com

R2
e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 190 deny tcp any any eq 27665 log
R2(config)# access-list 190 deny udp any any eq 31335 log
R2(config)# access-list 190 deny udp any any eq 27444 log
```

SECUR 1.1—5-65
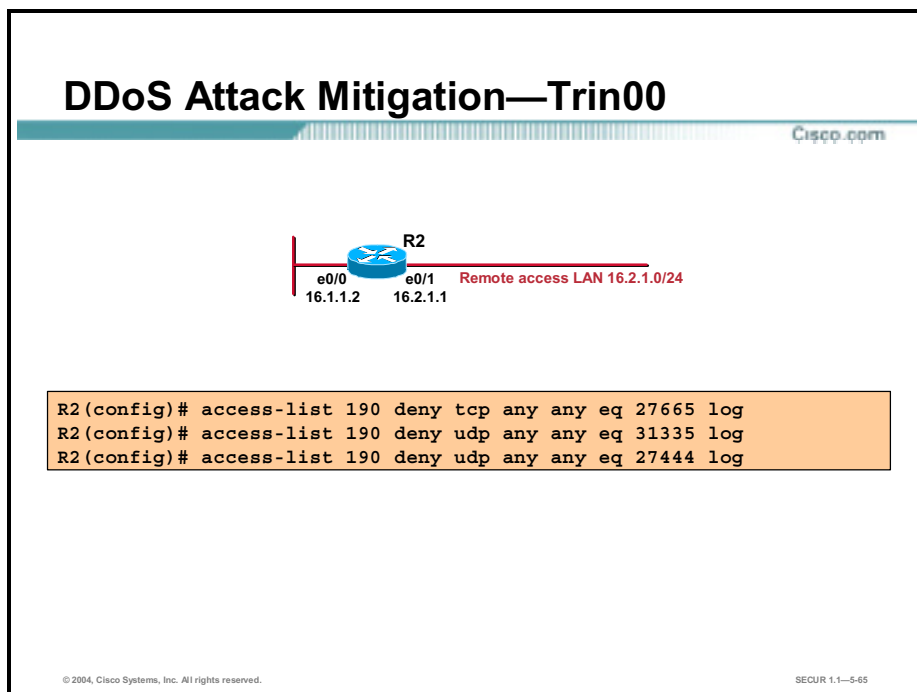
This figure shows an example of blocking the Trin00 DDoS attack by blocking traffic on the following ports:

- TCP—27665
- UDP—31335
- UDP—27444

DDoS Attack Mitigation—Stacheldraht

Cisco.com

R2
e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 190 deny tcp any any eq 16660 log
R2(config)# access-list 190 deny tcp any any eq 65000 log
```

This figure shows an example of blocking the Stacheldraht DDoS attack by blocking traffic on the following ports:

■ TCP—16660

■ TCP—65000

DDoS Attack Mitigation—Trinity v3

R2
e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 190 deny tcp any any eq 33270 log
R2(config)# access-list 190 deny tcp any any eq 39168 log
```

SECUR 1.1—5-67

This figure shows an example of blocking the Trinity v3 DDoS attack by blocking traffic on the following ports:

■ TCP—33270

■ TCP—39168

DDoS Attack Mitigation—SubSeven

R2

e0/0   e0/1   Remote access LAN 16.2.1.0/24
16.1.1.2   16.2.1.1

```
R2(config)# access-list 190 deny tcp any any range 6711 6712 log
R2(config)# access-list 190 deny tcp any any eq 6776 log
R2(config)# access-list 190 deny tcp any any eq 6669 log
R2(config)# access-list 190 deny tcp any any eq 2222 log
R2(config)# access-list 190 deny tcp any any eq 7000 log
```

   SECUR 1.1—5-68

This figure shows an example of blocking the SubSeven DDoS attack by blocking traffic on the following ports:

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

Sample Router Configuration

This topic contains a sample router configuration for our theoretical network router R2. This partial configuration file contains several access lists containing most of the access list features already explained in this lesson. View this partial configuration as an example of how to integrate multiple access list policies into a few main router access lists.

Theoretical Network—Sample Configuration for Router R2
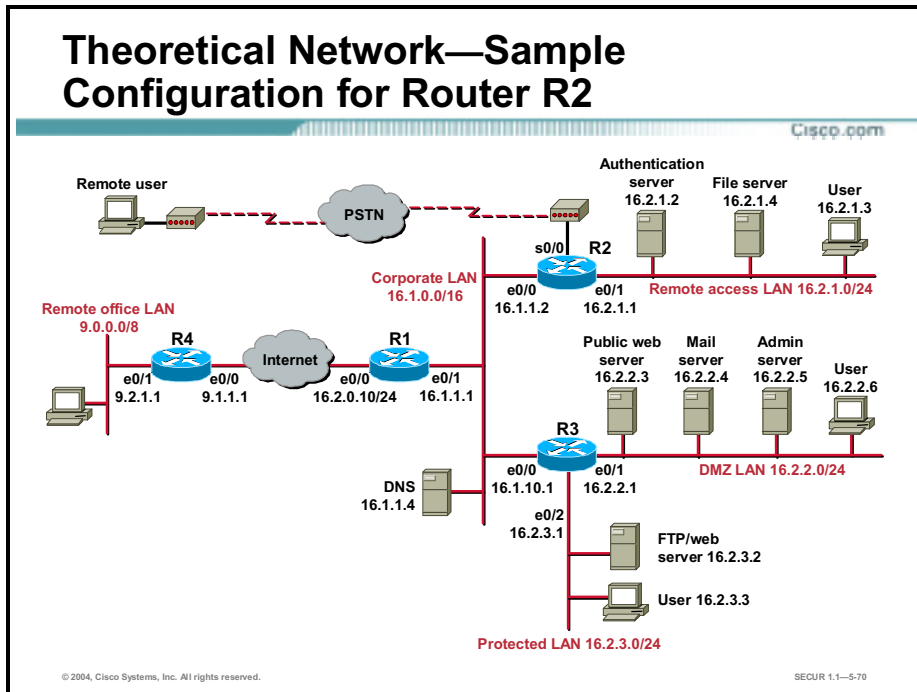
The following partial configuration file shows how to combine many access list functions into two or three larger access lists.

```
!
hostname R2
!
interface Ethernet0/0
  ip address 16.1.1.2 255.255.0.0
  ip access-group 126 in
!
interface Ethernet0/1
  ip address 16.2.1.1 255.255.255.0
  ip access-group 128 in
!
router ospf 44
network 16.1.0.0 0.0.255.255 area 0
network 16.2.1.0 0.0.0.255 area 1
!
! Access list 80 applies to SNMP hosts allowed to access this router
```

```
no access-list 80
access-list 80 permit host 16.2.1.2
access-list 80 permit host 16.2.1.3
!
! Access list 126 applies to traffic flowing from external networks to
the
! internal network or to the router itself
no access-list 126
access-list 126 deny ip 16.2.1.0 0.0.0.255 any log
access-list 126 deny ip host 16.1.1.2 host 16.1.1.2 log
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 10.0.0.0 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
access-list 126 deny ip any host 16.2.1.255 log
access-list 126 deny ip any host 16.2.1.0 log
access-list 126 permit tcp any 16.2.1.0 0.0.0.255 established
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 16.2.1.0 0.0.0.255
access-list 126 permit ospf 16.1.0.0 0.0.255.255 host 16.1.1.2
access-list 126 deny tcp any any range 6000 6063 log
access-list 126 deny tcp any any eq 6667 log
access-list 126 deny tcp any any range 12345 12346 log
access-list 126 deny tcp any any eq 31337 log
access-list 126 permit tcp any eq 20 16.2.1.0 0.0.0.255 gt 1023
access-list 126 deny udp any any eq 2049 log
access-list 126 deny udp any any eq 31337 log
access-list 126 deny udp any any range 33400 34400 log
access-list 126 permit udp any eq 53 16.2.1.0 0.0.0.255 gt 1023
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
!
! Access list 128 applies to traffic flowing from the internal network
to external ! networks or to the router itself
no access-list 128
access-list 128 deny ip host 16.2.1.1 host 16.2.1.1 log
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any echo
```

```
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any parameter-problem
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any packet-too-big
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any source-quench
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
access-list 128 permit tcp 16.2.1.0 0.0.0.255 gt 1023 any lt 1024
access-list 128 permit udp 16.2.1.0 0.0.0.255 gt 1023 any eq 53
access-list 128 permit udp 16.2.1.0 0.0.0.255 any range 33400 34400
log
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
!
! Access list 85 applies to remote access for the specified hosts to
the router
! itself
no access-list 85
access-list 85 permit tcp host 16.2.1.10 host 0.0.0.0 eq 23 log
access-list 85 permit tcp host 16.2.1.11 host 0.0.0.0 eq 23 log
access-list 85 permit tcp host 16.2.1.12 host 0.0.0.0 eq 23 log
access-list 85 deny ip any any log
!
snmp-server community snmp-host1 ro 80
!
```

Implementing Syslog Logging

This topic provides an overview of Syslog logging and how to configure your routers to support this function.

Implementing a router logging facility is an important part of any network security policy. Cisco routers can log information regarding configuration changes, access list 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 connected to the console. Messages sent to the console are not stored by the router, and therefore are not very valuable as security events.

- Terminal lines—Enabled EXEC sessions can be configured to receive log messages on any terminal lines. Like console logging, this type of logging is not stored by the router and therefore is 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 its' 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 Windows and UNIX-based systems. This is the most popular message logging facility because of its' long-term log storage capabilities and because it provides a central location for all router messages.

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

Syslog Systems

Public web server 16.2.2.3   Mail server 16.2.2.4   Admin server 16.2.2.5   Syslog server host 16.2.2.6

Syslog client

R3

e0/0 16.1.10.1   e0/1 16.2.2.1   DMZ LAN 16.2.2.0/24

e0/2 16.2.3.1

Syslog server (log host)

FTP/web server 16.2.3.2

User 16.2.3.3

Protected LAN 16.2.3.0/24
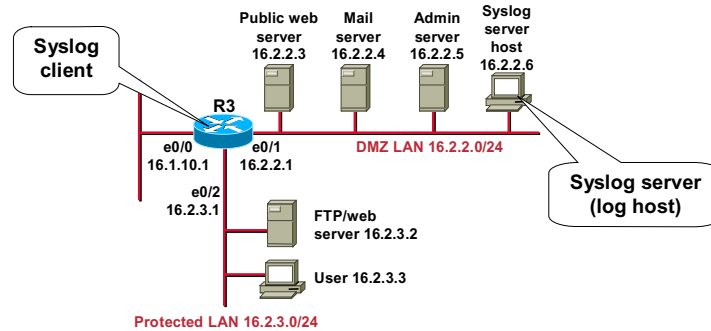
- **Syslog server—A host that accepts and processes log messages from one or more Syslog clients**
- **Syslog client—A host that generates log messages and forwards them to a Syslog server**

SECUR 1.1—5-73

Syslog implementations contain two types of systems, as shown in the figure:

■ Syslog servers—Also known as log hosts, these systems accept and process log messages from Syslog clients

■ Syslog clients—Router or other types of Cisco equipment that generate and forward log messages to Syslog servers

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

SECUR 1.1—5-73

Cisco router log messages fall into one of eight levels as shown in the figure. The lower the level number, the higher the severity level.

Note   When entering logging levels in commands in Cisco IOS Software Releases ≤ 11.3, you must specify the level name. Cisco IOS Software Releases ≥ 12.0 support using both the level number and/or the level name.

Here are some examples of different level messages:

- 0—IOS could not load
- 1—Temperature too high
- 2—Unable to allocate memory
- 3—Invalid memory size
- 4—Crypto operation failed
- 5—Interface changed state, up or down
- 6—Packet denied by access list
- 7—Packet type invalid

Log Message Format

Time message was generated (time stamp)

Log message name and severity level

```
Oct 29 10:00:01 EST: %SYS-5-CONFIG_I: Configured from console by
   vty0 (16.2.2.6)
```

Message text

SECUR 1.1—5-74

Cisco router log messages contain three main parts as shown in the figure.

■ Time stamp

■ Log message name and severity level

■ Message text

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

Syslog Router Commands

Router(config)#

```
logging [host-name | ip-address]
```

Router(config)#

```
logging trap level
```

Router(config)#

```
logging facility facility-type
```

Router(config)#

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

Router(config)#

```
logging on
```

Complete the following steps to implement Syslog on your Cisco routers:

Step 1   Configure log host(s)—You must configure the router to send log messages to one or more Syslog servers (also known as 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 as shown in the figure.

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

logging [*host-name* | *ip-address*]

host-name	Name of the host to be used as a Syslog server.
ip-address	IP address of the host to be used as a Syslog server.

Step 2   (Optional.) Set the log severity (trap) level—This limits the logging of error messages sent to Syslog servers to only those messages at the specified level (default is severity level 6).

Use the **logging trap** command in global configuration mode to set the severity (trap) level as shown in the figure.

The syntax for the **logging trap** command is as follows:

logging trap *level*

level	Limits the logging of messages to the Syslog servers to a specified level. You can enter the level number (0–7) 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 is facility *local7*).

Use the **logging facility** command in global configuration mode to set the Syslog facility as shown in the figure.

The syntax for the **logging facility** command is as follows:

logging facility *facility-type*

facility-type	The Syslog facility type (*local0-local7*).

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 which interface the packets actually exit the router.

Use the **logging source-interface** command in global configuration mode to set the source interface as shown in the figure.

The syntax for the **logging source-interface** command is as follows:

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

interface-type	The interface type (example; **Ethernet**).
interface-number	The interface number (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 as shown in the figure.

The syntax for the **logging on** command is as follows:

logging on

This command has no arguments or keywords.

Implementing Syslog

Public web server 16.2.2.3
Mail server 16.2.2.4
Admin server 16.2.2.5
Syslog server host 16.2.2.6

Syslog client

R3

e0/0 16.1.10.1
e0/1 16.2.2.1

DMZ LAN 16.2.2.0/24

e0/2 16.2.3.1

FTP/web server 16.2.3.2

User 16.2.3.3

Protected LAN 16.2.3.0/24

Syslog server (log host)
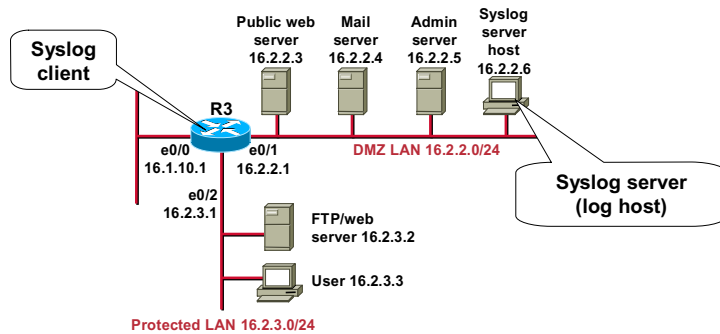
```
R3(config)# logging 16.2.2.6
R3(config)# logging trap informational
R3(config)# logging source-interface loopback 0
R3(config)# logging on
```

SECUR 1.1—5-77

This figure contains an example of configuring Syslog for router R3 using the commands previously specified.

Designing Secure Management and Reporting for Enterprise Networks

This topic provides an overview of the Cisco SAFE Extending the Security Blueprint to Small, Midsize, and Remote-User Networks (SAFE SMR) secure management and reporting design specification.

The principal goal of SAFE is to provide best-practice information on designing and implementing secure networks. The SAFE SMR specification contains design and implementation information specific to the management and reporting portion of your network. The SAFE blueprint refers to the design of the management and reporting systems as the "management module."

Note   This topic discusses only a small portion of the SAFE blueprint. For more detailed information regarding the SAFE blueprint, see Cisco.com (search on "SAFE") or attend the Cisco SAFE Implementation (CSI) course.

Earlier in this lesson, you learned how to configure logging for your Cisco routers. This is a fairly 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 and can raise several 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 your 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?

Earlier in this lesson you also learned about the basics of router management. You learned about securing administrative access and device configurations. Like device logging, this is a fairly straightforward operation for smaller Cisco router networks. However, managing administrative access and device configurations for many more devices can raise a different set of questions:

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

**Secure Management and Reporting—
SAFE Architectural Perspective**

Cisco.com

Protected management network
(behind firewall)

SNMP server

Syslog server

Access control server

System admin host

Terminal server

To all device console ports

Cisco IOS Firewall with VPN

Encrypted in-band network management (VPN)

Production network

OOB network management

SECUR 1.1—5-78
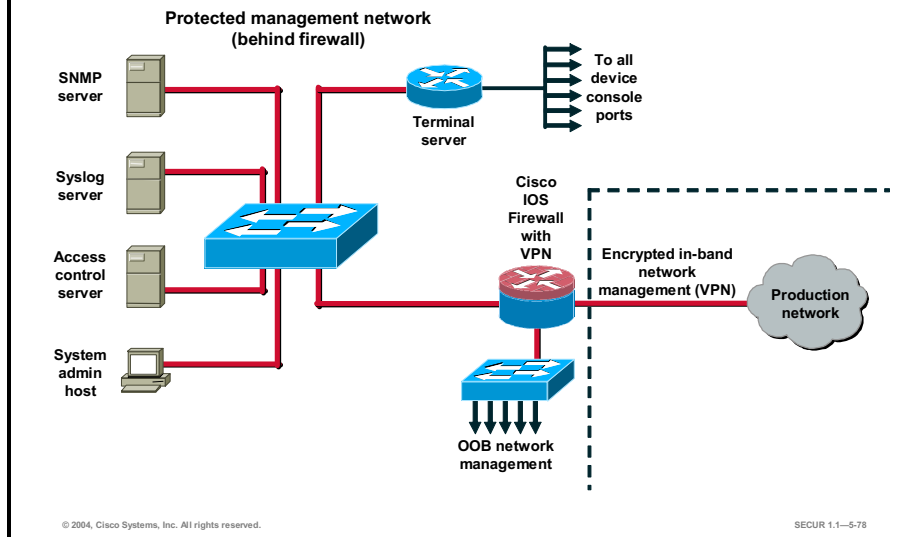
As can be seen in the figure, the SAFE enterprise management module has two network segments that are separated by a Cisco IOS router that acts as a firewall and a virtual private network (VPN) termination device. The segment outside the firewall connects to all the devices that require management. The 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:

■ Out of band (OOB)—Information flows within a network on which no production traffic resides.

■ In band—Information flows across the enterprise production network or the Internet (or both).

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 OOB 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, Secure Shell (SSH), and SNMP if these 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 will not be advertised by any routing protocols. It also enables the production network devices to block any traffic from the management subnets that appears 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 through the use of 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 (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 has been 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 the effective deployment of security features in the remaining modules in the enterprise. All the remaining 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 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.

SNMP management has its own set of security needs. Keeping SNMP traffic on the management segment allows it to traverse an isolated segment when pulling management information from devices. With SAFE, SNMP management pulls information only from devices rather than being allowed to push changes. To ensure this, each device is configured with a "read-only" string.

Proper aggregation and analysis of the Syslog information is critical to the 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. You may configure SNMP "read-write" when using an OOB network, but be aware of the increased security risk of a clear text string allowing modification of device configurations.

Secure Management and Reporting— Information Paths

Cisco.com

Protected management network (behind firewall)

SNMP server

Syslog server

Access control server

System admin host

Terminal server

OOB configuration management

To all device console ports

Cisco IOS Firewall with VPN

Encrypted in-band network management (VPN)

Production network

Private VLANs

Stateful packet filtering and IPSec termination for management

OOB network management

Configuration and content management (SSH if possible)

SECUR 1.1—5-79

The primary goal of SAFE SMR is to facilitate the secure management of all devices and hosts within the enterprise architecture. Logging and reporting information flow from the devices to the management hosts, while content, configurations, and new software flow to the devices from the management hosts.

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 where possible, and where impossible (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 the specific ports required for management and reporting. The tunnel should also be locked down so that only appropriate hosts can initiate and terminate tunnels.

After you have implemented an OOB management network, dealing with logging and reporting becomes more straightforward. Most networking devices can send Syslog data, which can be invaluable when troubleshooting network problems or security threats. Send this data to one or more Syslog analysis hosts on the management network. Depending on the device involved, you can choose various logging levels to ensure that the correct amount of data is sent to the logging devices. To ensure that log message times are comparable to one another, 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 took place.

Note	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 reachability of all the devices on the production network. If a critical link failed between two core switches, 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. With management applications such as these, it is preferred to run the management application in-band. In-band management needs to be configured in as secure a manner as possible. Often in-band and OOB management can be configured from the same management network, provided that there is a firewall between the management hosts and the devices needing management.

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

1. What 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 any configuration modifications made to a device. These protocols can sometimes also be used to push and pull data to a device instead of insecure protocols such as TFTP and FTP. Often, however, TFTP is required on Cisco equipment to back up configurations or to update software versions. This fact leads to the second question.

2. Does this 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 does not scale with large numbers of devices, however, 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.

3. Do you really need this management tool?—Often, SNMP managers 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. Know that by introducing SNMP into your production network, you are introducing a potential vulnerability into your environment.

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 took place. 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—General Guidelines

- **The following are out-of-band management guidelines for the architecture:**
  - **Should provide the highest level of security; should mitigate the risk of passing insecure management protocols over the production network**
  - **Should keep clocks on hosts and network devices in sync**
  - **Should record changes and archive configurations.**
- **The following are in-band management guidelines:**
  - **Decide if the device really needs 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 in sync.**
  - **Record changes and archive configurations.**

SECUR 1.1—5-80

The following are OOB secure management guidelines for the architecture:

- It should provide the highest level of security; it should mitigate the risk of passing insecure management protocols over the production network.

- It should keep clocks on hosts and network devices synchronized.

- It should record changes and archive configurations.

The following are in-band secure management guidelines:

- Decide if the device really needs 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.

Even though OOB management is recommended for devices in SAFE Enterprise, SAFE SMR recommends in-band management, because the goal is cost-effective security deployment.

In the SAFE SMR architecture, management traffic flows in-band in all cases and is made as secure as possible using tunneling protocols and secure variants to insecure management protocols (for example, SSH is used whenever possible instead of Telnet). With management traffic flowing in-band across the production network, it becomes very important to follow more closely the axioms mentioned earlier in the lesson.

To ensure that log messages are time-synchronized to one another, 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.

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. 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 for network administrators who do not wish to implement their own master clocks because of cost or other reasons.

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

NTP version 3 and above supports a cryptographic authentication mechanism between peers. The use of the authentication mechanism, as well as the use of 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 from the Internet with the possible risk of doing so and allowing it through the firewall. Many NTP servers on the Internet do not require any authentication of peers. Therefore, the network administrator must trust that the clock itself is reliable, valid, and secure. NTP uses UDP port 123.

Logging and reading information from many devices can be very challenging. You must consider the following issues:

- Identify which logs are most important.

- Separate important messages from notifications.

- Ensure that logs are not tampered with in transit.

- Ensure that time stamps match each other when multiple devices report the same alarm.

- Identify what information is needed if log data is required for a criminal investigation.

- Identify how to deal with the volume of messages that can be generated when a system is under attack.

Each of these issues is company specific and requires input from management, as well as from the network and security teams, to identify the priorities of reporting and monitoring. 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 that can be invaluable when you are troubleshooting network problems or security threats. You can send this data to your Syslog analysis host from any devices whose logs you wish to view. This data can be viewed in real time or on demand and 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 also need to 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 to one another, 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— Configuring SSH Server

```
Austin2# config t
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 time-out 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
Austin2#
```

SECUR 1.1—5-82

Whenever possible, you should use SSH instead of Telnet to manage your Cisco routers. SSH version 1 is supported in Cisco IOS Software Releases ≥ 12.1(1)T. SSH version 2 is supported in Cisco IOS Software Releases ≥ 12.3(4)T. Cisco routers configured for SSH act as SSH servers. You will need to provide an SSH client such as PuTTY, OpenSSH, or Tera Term for the administrator workstation you wish to use to configure and manage your routers using SSH.

Note	Cisco routers operating at Cisco IOS Software Releases ≥ 12.1(3)T 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. The SAFE SMR design does not typically utilize this functionality because it is more likely that you will be accessing the router from a SSH client system, not the other way around.

SSH employs strong encryption to protect the SSH client-to-SSH server session. Unlike Telnet, where anyone with a sniffer can see exactly what you are sending and receiving to and from your routers, SSH encrypts the entire session.

Complete the following tasks before configuring your routers for SSH server operations:

■ Ensure that the target routers are running a Cisco IOS software image ≥ 12.1(1)T and the IPSec feature set. Only Cisco IOS software images containing the IPSec feature set support SSH server.

■ Ensure that the target routers are configured for either local authentication or AAA for username /password authentication.

■ 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 the following steps to configure your Cisco router to support SSH server:

Step 1 Configure the IP domain name using the **ip domain-name** global configuration command as shown in the figure:

```
Austin2(config)# ip domain-name cisco.com
```

Step 2 Generate the Rivest, Shamir, and Adleman (RSA) keys using the **crypto key generate rsa** global configuration command as shown in the figure:

```
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 Configure the time that the router waits for the SSH client to respond using the **ip ssh time-out** global configuration command as shown in the figure:

```
Austin2(config)# ip ssh time-out 120
```

Step 4 Configure the SSH retries using the **ip ssh authentication-retries** global configuration command as shown in the figure:

```
Austin2(config)# ip ssh authentication-retries 4
```

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

Step 5 Disable VTY inbound Telnet sessions as shown in the figure:

```
Austin2(config)# line vty 0 4
Austin2(config-line)# no transport input telnet
```

Step 6 Enable VTY inbound SSH sessions as shown in the figure:

```
Austin2(config-line)# transport input ssh
Austin2(config-line)# end
Austin2#
```

The SSH protocol is automatically enabled once you generate the SSH 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 will then prompt 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.

Securing SNMP Access

Router PR1

SNMP agent

SNMP management system 10.0.1.1

SNMP management system 10.0.1.2
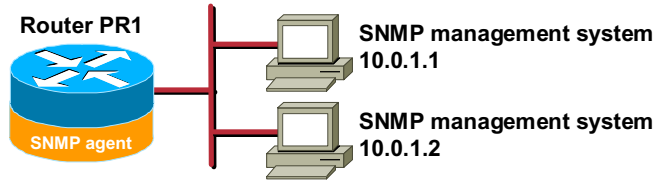
```
router(config)#
snmp-server community string [ro | rw] [number]
```

```
PR1(config)# snmp-server community ReadSNMP ro
```

```
PR1(config)# snmp-server community ReadWriteSNMP rw
```

```
PR1(config)# access-list 10 permit 10.0.1.1
PR1(config)# access-list 10 permit 10.0.1.2
PR1(config)# snmp-server community RWSNMP rw 10
```

SECUR 1.1—5-83

SNMP systems may gain administrative access to Cisco routers by communicating with the router's internal SNMP agent and management information base (MIB).

An SNMP agent is responsible for reading and formatting all SNMP messages between the router and an SNMP network management system (NMS). An SNMP MIB is a tree-like list of objects within the router that point the SNMP agent to various router configuration parameters and statistics. After the SNMP agent on the router is configured, SNMP systems may perform some or all of the following tasks:

■ Read certain configuration parameters and statistics found in the router SNMP agent MIB (read-only mode)

■ Write certain configuration parameters to the router SNMP agent MIB (read-write mode)

■ Receive SNMP traps (router events) from the router SNMP agent

SNMP systems use a community string as a type of password to access router SNMP agents. 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 were to configure your router SNMP agent to use this commonly known community string, anyone with an SNMP system would be able to—at a minimum—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 extremely important that you create your own custom SNMP community strings.

You must consider the following questions when developing SNMP access for Cisco routers:

■ Which community strings will have read-only access?

■ Which community strings will have read-write access?

■ Which SNMP systems will be permitted to access the router SNMP agents (limiting host IP addresses using ACLs)?

Note	The latest Cisco IOS Software Releases contain support for SNMPv3. If you are planning to use SNMP to manage your Cisco routers, it is recommended that you use SNMPv3 because it is a more secure protocol than its predecessors.

To configure a router SNMP community string, use the **snmp-server community** command in global configuration mode, as shown in the figure. You may configure multiple community strings for your Cisco router by repeating this command for each string.

The syntax for the **snmp-server** command is as follows:

snmp-server community *string* **[ro | rw] [***number***]**

string	Community string that acts like a password and permits access to the SNMP protocol.
ro	(Optional.) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional.) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
number	(Optional.) Integer from 1 to 99 that specifies an ACL of IP addresses that are allowed to use the community string to gain access to t he router.

Use the **ro** option to limit a community string to read-only access (only SNMP get-requests and get-next-requests are allowed), as shown in the figure:

```
PR1(config)# snmp-server community readSNMP ro
```

Use the **rw** option to allow read and write access (SNMP get-requests, get-next-requests, and set-requests are allowed) for the designated community string, as shown in the figure:

```
PR1(config)# snmp-server community ReadWriteSNMP rw
```

ACLs can be used for both read-only and read-write modes. Use the **snmp-server** command in association with ACLs to limit which hosts are allowed access to the router SNMP agent, as shown in the figure (this example shows a read-write mode community string):

```
PR1(config)# access-list 10 permit 10.0.1.1
```

```
PR1(config)# access-list 10 permit 10.0.1.2
```

```
PR1(config)# snmp-server community string RWSNMP rw 10
```

SNMP traps and informs are router events that are automatically sent to one or more SNMP systems by a router SNMP agent. Traps are sent to designated SNMP systems regardless of whether the host is there or not. Informs always require an acknowledgment from the designated SNMP system to verify that the message was received. Because traps and informs can contain critical routing and configuration information, it is important that you designate exactly where you want the traps and informs sent.

The following list contains types of router SNMP traps that are enabled (sent) by default (all other types of traps must be specifically enabled to be sent):

■ Interface traps—These traps are sent whenever an interface becomes active or inactive.

■ Reload traps—Theses traps are sent whenever a router reload occurs.

■ Configuration change traps—These traps are sent whenever a change is made to the router configuration.

There are two ways to specifically enable traps and informs to be generated by the router:

■ Enable global traps and informs—Use the **snmp-server enable traps** command to enable all SNMP traps and informs to be sent by the router.

■ Enable host—Use the **snmp-server host** command to specify which traps and informs to send while simultaneously specifying the SNMP system host where the traps and informs are to be sent.

Use the **snmp-server enable traps** command from global configuration mode to enable the sending of all traps and informs by the router. Note that this command only enables traps and informs, it does not specify the SNMP system host to which the traps and informs are to be sent.

The syntax for the **snmp-server enable traps** command is as follows:

snmp-server enable traps [notification-type]

notification-type	(Optional.) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. The notification type can be one of the following keywords:
	■ **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.
	■ **dlsw [circuit | tconn]**—Controls DLSw notifications, as defined in the CISCO-DLSW-MIB (enterprise 1.3.6.1.4.1.9.10.9.1.7). When the **dlsw** keyword is used, you can specify the specific notification types you wish to enable or disable. If no keyword is used, all DLSw notification types are enabled. The option can be one of the following keywords:
	— **circuit**—Enables DLSw circuit traps: (5) ciscoDlswTrapCircuitUp (6) ciscoDlswTrapCircuitDown
	— **tconn**—Enables DLSw peer transport connection traps: (1) ciscoDlswTrapTConnPartnerReject (2) ciscoDlswTrapTConnProtViolation (3) ciscoDlswTrapTConnUp (4) ciscoDlswTrapTConnDown
	■ **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This is from the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) and the notification type is: (1) cpmDS0BusyoutNotification.
	■ **ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as: (2) cpmDS1LoopbackNotification.
	■ **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.
	■ **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is: (1) cHsrpStateChange.
	■ **ipmulticast**—Controls IP multicast notifications.
	■ **modem-health**—Controls modem-health notifications.

- **rsvp**—Controls Resource Reservation Protocol (RSVP) notifications.

- **rtr**—Controls Service Assurance Agent/ Response Time Reporter (RTR) notifications.

- **syslog**—Controls error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.

- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my and the notifications are: enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification.

A more efficient way of enabling traps and informs is to use the **snmp-server host** command because it accomplishes two tasks at once:

- Specifies which SNMP system host is to be sent the traps and informs

- Specifies which traps and informs are to be enabled

You must specify which SNMP systems (host-addr) are to receive SNMP traps by entering the **snmp-server host** command in global configuration mode.

The syntax for the **snmp-server host** command is as follows:

snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]

host-addr	Name or Internet address of the SNMP system host (the targeted recipient).
traps	(Optional.) Sends SNMP traps to this host. This is the default.
informs	(Optional.) Sends SNMP informs to this host.
version	(Optional.) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following must be specified: ■ **1**—SNMPv1. This option is not available with informs. ■ **2c**—SNMPv2C. ■ **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword: — **auth**—(Optional.) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. — **noauth**—(Default.) The noAuthNoPriv security level. This is the default if the **[auth	noauth	priv]** keyword choice is not specified. — **Priv**—(Optional.) Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host command** by itself, it is recommended that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	(Optional.) UDP port of the host to use. The default is 162.
notification-type	(Optional.) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: ■ **bgp**—Sends Border Gateway Protocol (BGP) state change notifications

- **calltracker**—Sends Call Tracker call-start/call-end notifications
- **config**—Sends configuration notifications
- **dspu**—Sends downstream physical unit (DSPU) notifications
- **entity**—Sends Entity MIB modification notifications
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded
- **frame-relay**—Sends Frame Relay notifications
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications
- **isdn**—Sends Integrated Services Digital Network (ISDN) notifications
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications
- **repeater**—Sends standard repeater (hub) notifications
- **rsrb**—Sends remote source-route bridging (RSRB) notifications
- **rsvp**—Sends RSVP notifications
- **rtr**—Sends SA Agent (RTR) notifications
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications
- **sdllc**—Sends SDLC over Logical Link Control (SDLLC) notifications
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications
- **stun**—Sends serial tunnel (STUN) notifications
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command
- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes
- **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command
- **x25**—Sends X.25 event notifications

The following is an example of using the **snmp-server host** command to limit where the router will send SNMP traps:

```
PR1(config)# snmp-server host 10.0.1.1 traps
```

The following is an example of using the **snmp-server host** command to limit where TCP connection close traps will be sent by the router:

```
PR1(config)# snmp-server host 10.0.1.2 traps tty
```

One final SNMP-related command is the **snmp-server trap-source** command. This command specifies which interface on the router (and, hence, the corresponding IP address) will be the source for all SNMP traps and informs generated by the router. The loopback0 interface makes an excellent choice for the source interface because it is always considered to be active.

Use the **snmp-server trap-source** command from the global configuration mode.

The syntax for the **snmp-server trap-source** command is as follows:

snmp-server trap-source *interface*

The following is an example of using the **snmp-server trap-source** command for the loopback 0 interface:

```
PR1(config)# snmp-server trap-source loopback0
```

There are several more **snmp-server** commands available to you that are described in the Cisco IOS Software Command Reference at Cisco.com.

Using AutoSecure to Secure Cisco Routers

This topic explains how to use the Cisco IOS Software Release 12.3 AutoSecure feature to secure Cisco routers.

What Is AutoSecure?

AutoSecure helps secure Cisco IOS networks by performing the following 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 forwarding plane**

SECUR 1.1—5-85

The AutoSecure feature is found in Cisco IOS Software Release 12.3 and subsequent 12.3T releases for Cisco 800, 1700, 2600, 3600, 3700, and 7200 Series routers.

AutoSecure is a single privileged EXEC command that allows you to quickly and easily eliminate many of the potential security threats already covered in this course. AutoSecure helps make you more efficient at securing Cisco routers.

AutoSecure performs the following tasks on the target router:

- Disables certain potentially insecure global services

- Enables certain security-based global services

- Disables certain potentially insecure interface services

- Enables appropriate security-related logging

- Takes steps to secure administrative access to the router

- Takes steps to secure the router forwarding plane

AutoSecure—Modes of Operation

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 AutoSecure command using recommended default settings**

SECUR 1.1—5-86

AutoSecure allows two modes of operation, as shown in the figure:

- Interactive mode—Prompts you to choose the way you want to configure router services and other security-related features

- Noninteractive mode—Configures your router's security-related features based on a set of Cisco defaults

Obviously, interactive mode provides for greater control over the router security-related features than noninteractive mode. However, there may be occasions when you want to quickly secure a router without much human intervention. In these latter cases, the noninteractive mode becomes the better choice.

AutoSecure—Getting Started

Router#

```
auto secure [management | forwarding][no-interact]
```

```
Router# auto secure
        --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the
router but it will not make router absolutely secure from all
security attacks ***

All the configuration done as part of AutoSecure will be shown
here. For more details of why and how this configuration is
useful, and any possible side effects, please refer to Cisco
documentation of AutoSecure.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure
```

AutoSecure is initiated using the **auto secure** command in privileged EXEC mode, as shown in the figure.

The syntax for this command is as follows:

auto secure [management | forwarding] [no-interact]

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.

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Router# auto secure

                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***

All the configuration done as part of AutoSecure will be
shown here. For more details of why and how this configuration
is useful, and any possible side effects, please refer to Cisco
documentation of AutoSecure.
At any prompt you may enter '?' for help.
```

```
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure
```

AutoSecure—Interface Selection

```
Is this router connected to internet? [no]: y
Enter the number of interfaces facing internet [1]: 1
Interface      IP-Address      OK? Method Status  Protocol
Ethernet0/0   10.0.2.2        YES NVRAM  up       up
Ethernet0/1   172.30.2.2      YES NVRAM  up       up


Enter the interface name that is facing internet: Ethernet0/1
```

As shown in the figure, the first questions that AutoSecure asks you are directly related to how the router is connected to the Internet. 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?

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Is this router connected to internet? [no]: y

Enter the number of interfaces facing internet [1]: 1

Interface      IP-Address      OK? Method Status  Protocol

Ethernet0/0   10.0.2.2        YES NVRAM  up       up

Ethernet0/1   172.30.2.2      YES NVRAM  up       up


Enter the interface name that is facing internet: Ethernet0/1
```

Next, AutoSecure disables the following router global services:

■ 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 a recently discovered CDP security threat.

■ 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 exploiting older Cisco IOS software–based routers that do not process source routing properly.

■ 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

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
```

AutoSecure—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.%
```

Next, AutoSecure prompts you to create a banner to be shown every time someone accesses the router. This is the same as using the **banner** command in global configuration mode.

The following is an example of how this portion of the AutoSecure dialogue appears:

```
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.%
```

Note	Remember to place the banner between two delimiting characters of your choice. In this example, percent (%) characters are used as delimiters.

AutoSecure—Configuring Passwords, AAA, SSH Server, and Domain Name

```
Enable secret is either not configured or is same as enable
password
Enter the new enable secret: Curium96


Configuration of local user database
Enter the username: student1
Enter the password: student1
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport


Configure SSH server? [yes]: y
Enter the hostname: R2
Enter the domain-name: cisco.com
```

SECUR 1.1—5-91

Next, 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.

■ SSH server—AutoSecure asks you 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 2.

■ 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.

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Enable secret is either not configured or is same as enable password
Enter the new enable secret: Curium96


Configuration of local user database
Enter the username: student1
```

```
Enter the password: student1
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport

Configure SSH server? [yes]: y
Enter the domain-name: cisco.com
```

```
Configuring interface specific AutoSecure services

Disabling the following ip services on all interfaces:


 no ip redirects

 no ip proxy-arp

 no ip unreachables

 no ip directed-broadcast

 no ip mask-reply
```

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

- IP redirects

- IP proxy ARP

- IP unreachables

- IP directed-broadcast

- IP mask replies

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Configuring interface specific AutoSecure services

Disabling the following ip services on all interfaces:


 no ip redirects

 no ip proxy-arp

 no ip unreachables

 no ip directed-broadcast

 no ip mask-reply
```

AutoSecure—Configuring CEF and Ingress Filtering

```
Securing Forwarding plane services..

Enabling CEF (it might have more memory requirements on some
low end platforms)

Configuring the named acls for Ingress filtering

autosec_iana_reserved_block: This block may subject to

change by iana and for updated list visit

www.iana.org/assignments/ipv4-address-space.

1/8, 2/8, 5/8, 7/8, 23/8, 27/8, 31/8, 36/8, 37/8, 39/8,…

autosec_private_block:

10/8, 172.16/12, 192.168/16

autosec_complete_block: This is union of above two and the
addresses of source multicast, class E addresses and addresses
that are prohibited for use as source.

source multicast (224/4), class E(240/4), 0/8, 169.254/16,

192.0.2/24, 127/8.
```

Next, 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.

■ Builds the following three extended-named ACLs for ingress filtering (antispoofing):

— autosec_iana_reserved_block—Denies all IANA reserved IP address blocks

— autosec_private_block—Denies RFC 1918 private IP address blocks

— autosec_complete_block—Denies multicast, class E, and other IP addresses prohibited for source address (and all addresses blocked by first two ACLs listed here)

Note	Although the AutoSecure user interface refers to the third ACL as "autosec_complete_block", in reality, the router creates it as "autosec_complete_bogon".

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Securing Forwarding plane services..


Enabling CEF (it might have more memory requirements on some low end
platforms)


Configuring the named acls for Ingress filtering


autosec_iana_reserved_block: This block may subject to

change by iana and for updated list visit
```

```
www.iana.org/assignments/ipv4-address-space.
1/8, 2/8, 5/8, 7/8, 23/8, 27/8, 31/8, 36/8, 37/8, 39/8,
41/8, 42/8, 49/8, 50/8, 58/8, 59/8, 60/8, 70/8, 71/8,
72/8, 73/8, 74/8, 75/8, 76/8, 77/8, 78/8, 79/8, 83/8,
84/8, 85/8, 86/8, 87/8, 88/8, 89/8, 90/8, 91/8, 92/8, 93/8,
94/8, 95/8, 96/8, 97/8, 98/8, 99/8, 100/8, 101/8, 102/8,
103/8, 104/8, 105/8, 106/8, 107/8, 108/8, 109/8, 110/8,
111/8, 112/8, 113/8, 114/8, 115/8, 116/8, 117/8, 118/8,
119/8, 120/8, 121/8, 122/8, 123/8, 124/8, 125/8, 126/8,
197/8, 201/8

autosec_private_block:
10/8, 172.16/12, 192.168/16

autosec_complete_block: This is union of above two and
the addresses of source multicast, class E addresses
and addresses that are prohibited for use as source.
source multicast (224/4), class E(240/4), 0/8, 169.254/16,
192.0.2/24, 127/8.
```

Cisco.com

```
Configure Ingress filtering on edge interfaces? [yes]: y


[1] Apply autosec_iana_reserved_block acl on all edge
interfaces
[2] Apply autosec_private_block acl on all edge interfaces
[3] Apply autosec_complete_bogon acl on all edge interfaces
Enter your selection [3]: 1
Enabling unicast rpf on all interfaces connected to internet


Configure CBAC Firewall feature? [yes/no]: y
```

SECUR 1.1—5-94

Next, AutoSecure performs several steps, as shown in the figure:

■ Configures ingress filtering on edge interfaces—AutoSecure asks if you want to apply
   ingress filtering on the router edge (connected to Internet) interfaces. If you answer "yes,"
   AutoSecure prompts you to choose which one of the three previously configured
   antispoofing ACLs to apply.

■ Enables Unicast 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.

■ Configures 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 inspect rules is assigned to Internet-facing router interfaces.

The following is an example of how this portion of the AutoSecure dialogue appears:

```
Configure Ingress filtering on edge interfaces? [yes]: y


[1] Apply autosec_iana_reserved_block acl on all edge interfaces
[2] Apply autosec_private_block acl on all edge interfaces
[3] Apply autosec_complete_bogon acl on all edge interfaces
Enter your selection [3]: 1
Enabling unicast rpf on all interfaces connected to internet


Configure CBAC Firewall feature? [yes/no]: y
```

AutoSecure—Checking Configuration and Applying to Running Configuration

```
This is the configuration generated:


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
.
.
.
Apply this configuration to running-config? [yes]: y
```

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 following is an example of how this portion of the AutoSecure dialogue appears.

| Note | Notes have been inserted into this example to help you understand what AutoSecure is doing at various points. These notes are not part of the router AutoSecure command line interface (CLI) output. |

```
This is the configuration generated:
```

| Note | Here 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. |

```
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
```

```
banner #This system is the property of Cisco Systems, Inc.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.#
```

```
security passwords min-length 6
```

```
security authentication failure rate 10 log
```

```
enable secret 5 $1$D5gC$4X79guFOe4rTOTqJgngZ0.
```

```
username student1 password 7 0832585B0D1C0B0343
```

```
aaa new-model
aaa authentication login local_auth local
```

```
line console 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
```

```
hostname R2
```

```
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
```

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

```
int Ethernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply

int Ethernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
```

```
ip cef
```

```
ip access-list extended autosec_iana_reserved_block
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
```

```
deny ip 7.0.0.0 0.255.255.255 any
deny ip 23.0.0.0 0.255.255.255 any
deny ip 27.0.0.0 0.255.255.255 any
deny ip 31.0.0.0 0.255.255.255 any
deny ip 36.0.0.0 0.255.255.255 any
deny ip 37.0.0.0 0.255.255.255 any
deny ip 39.0.0.0 0.255.255.255 any
deny ip 41.0.0.0 0.255.255.255 any
deny ip 42.0.0.0 0.255.255.255 any
deny ip 49.0.0.0 0.255.255.255 any
deny ip 50.0.0.0 0.255.255.255 any
deny ip 58.0.0.0 0.255.255.255 any
deny ip 59.0.0.0 0.255.255.255 any
deny ip 60.0.0.0 0.255.255.255 any
deny ip 70.0.0.0 0.255.255.255 any
deny ip 71.0.0.0 0.255.255.255 any
deny ip 72.0.0.0 0.255.255.255 any
deny ip 73.0.0.0 0.255.255.255 any
deny ip 74.0.0.0 0.255.255.255 any
deny ip 75.0.0.0 0.255.255.255 any
deny ip 76.0.0.0 0.255.255.255 any
deny ip 77.0.0.0 0.255.255.255 any
deny ip 78.0.0.0 0.255.255.255 any
deny ip 79.0.0.0 0.255.255.255 any
deny ip 83.0.0.0 0.255.255.255 any
deny ip 84.0.0.0 0.255.255.255 any
deny ip 85.0.0.0 0.255.255.255 any
deny ip 86.0.0.0 0.255.255.255 any
deny ip 87.0.0.0 0.255.255.255 any
deny ip 88.0.0.0 0.255.255.255 any
deny ip 89.0.0.0 0.255.255.255 any
deny ip 90.0.0.0 0.255.255.255 any
deny ip 91.0.0.0 0.255.255.255 any
deny ip 92.0.0.0 0.255.255.255 any
deny ip 93.0.0.0 0.255.255.255 any
deny ip 94.0.0.0 0.255.255.255 any
deny ip 95.0.0.0 0.255.255.255 any
deny ip 96.0.0.0 0.255.255.255 any
deny ip 97.0.0.0 0.255.255.255 any
deny ip 98.0.0.0 0.255.255.255 any
deny ip 99.0.0.0 0.255.255.255 any
deny ip 100.0.0.0 0.255.255.255 any
```

```
 deny ip 101.0.0.0 0.255.255.255 any
 deny ip 102.0.0.0 0.255.255.255 any
 deny ip 103.0.0.0 0.255.255.255 any
 deny ip 104.0.0.0 0.255.255.255 any
 deny ip 105.0.0.0 0.255.255.255 any
 deny ip 106.0.0.0 0.255.255.255 any
 deny ip 107.0.0.0 0.255.255.255 any
 deny ip 108.0.0.0 0.255.255.255 any
 deny ip 109.0.0.0 0.255.255.255 any
 deny ip 110.0.0.0 0.255.255.255 any
 deny ip 111.0.0.0 0.255.255.255 any
 deny ip 112.0.0.0 0.255.255.255 any
 deny ip 113.0.0.0 0.255.255.255 any
 deny ip 114.0.0.0 0.255.255.255 any
 deny ip 115.0.0.0 0.255.255.255 any
 deny ip 116.0.0.0 0.255.255.255 any
 deny ip 117.0.0.0 0.255.255.255 any
 deny ip 118.0.0.0 0.255.255.255 any
 deny ip 119.0.0.0 0.255.255.255 any
 deny ip 120.0.0.0 0.255.255.255 any
 deny ip 121.0.0.0 0.255.255.255 any
 deny ip 122.0.0.0 0.255.255.255 any
 deny ip 123.0.0.0 0.255.255.255 any
 deny ip 124.0.0.0 0.255.255.255 any
 deny ip 125.0.0.0 0.255.255.255 any
 deny ip 126.0.0.0 0.255.255.255 any
 deny ip 197.0.0.0 0.255.255.255 any
 deny ip 201.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date. Visit
www.iana.org/assignments/ipv4-add
ress-space for update list
exit
```

Note   Next, AutoSecure configures an extended-named ACL called "autosec_private_block." Once it has been assigned to the inbound direction of an Internet-facing router interface, this ACL will block all RFC 1918 private addresses (currently known to this version of AutoSecure).

```
ip access-list extended autosec_private_block
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 permit ip any any
```

```
exit
```

Note   Next, AutoSecure configures an extended-named ACL called "autosec_complete_bogon" (a union of the previous two ACLs plus some extra address restrictions). Once assigned to the inbound direction of an Internet-facing router interface, this ACL will block all IANA reserved IP addresses, RFC 1918 private addresses, source multicast addresses, and class-E addresses (currently known to this version of AutoSecure). Please note the remark at the end of this ACL regarding updates to the IANA list of reserved addresses. If you wish to block any IANA reserved addresses not included in this list, you will need to update the ACL manually after running the AutoSecure script.

```
ip access-list extended autosec_complete_bogon
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
 deny ip 7.0.0.0 0.255.255.255 any
 deny ip 23.0.0.0 0.255.255.255 any
 deny ip 27.0.0.0 0.255.255.255 any
 deny ip 31.0.0.0 0.255.255.255 any
 deny ip 36.0.0.0 0.255.255.255 any
 deny ip 37.0.0.0 0.255.255.255 any
 deny ip 39.0.0.0 0.255.255.255 any
 deny ip 41.0.0.0 0.255.255.255 any
 deny ip 42.0.0.0 0.255.255.255 any
 deny ip 49.0.0.0 0.255.255.255 any
 deny ip 50.0.0.0 0.255.255.255 any
 deny ip 58.0.0.0 0.255.255.255 any
 deny ip 59.0.0.0 0.255.255.255 any
 deny ip 60.0.0.0 0.255.255.255 any
 deny ip 70.0.0.0 0.255.255.255 any
 deny ip 71.0.0.0 0.255.255.255 any
 deny ip 72.0.0.0 0.255.255.255 any
 deny ip 73.0.0.0 0.255.255.255 any
 deny ip 74.0.0.0 0.255.255.255 any
 deny ip 75.0.0.0 0.255.255.255 any
 deny ip 76.0.0.0 0.255.255.255 any
 deny ip 77.0.0.0 0.255.255.255 any
 deny ip 78.0.0.0 0.255.255.255 any
 deny ip 79.0.0.0 0.255.255.255 any
 deny ip 83.0.0.0 0.255.255.255 any
 deny ip 84.0.0.0 0.255.255.255 any
 deny ip 85.0.0.0 0.255.255.255 any
 deny ip 86.0.0.0 0.255.255.255 any
 deny ip 87.0.0.0 0.255.255.255 any
```

```
deny ip 88.0.0.0 0.255.255.255 any
deny ip 89.0.0.0 0.255.255.255 any
deny ip 90.0.0.0 0.255.255.255 any
deny ip 91.0.0.0 0.255.255.255 any
deny ip 92.0.0.0 0.255.255.255 any
deny ip 93.0.0.0 0.255.255.255 any
deny ip 94.0.0.0 0.255.255.255 any
deny ip 95.0.0.0 0.255.255.255 any
deny ip 96.0.0.0 0.255.255.255 any
deny ip 97.0.0.0 0.255.255.255 any
deny ip 98.0.0.0 0.255.255.255 any
deny ip 99.0.0.0 0.255.255.255 any
deny ip 100.0.0.0 0.255.255.255 any
deny ip 101.0.0.0 0.255.255.255 any
deny ip 102.0.0.0 0.255.255.255 any
deny ip 103.0.0.0 0.255.255.255 any
deny ip 104.0.0.0 0.255.255.255 any
deny ip 105.0.0.0 0.255.255.255 any
deny ip 106.0.0.0 0.255.255.255 any
deny ip 107.0.0.0 0.255.255.255 any
deny ip 108.0.0.0 0.255.255.255 any
deny ip 109.0.0.0 0.255.255.255 any
deny ip 110.0.0.0 0.255.255.255 any
deny ip 111.0.0.0 0.255.255.255 any
deny ip 112.0.0.0 0.255.255.255 any
deny ip 113.0.0.0 0.255.255.255 any
deny ip 114.0.0.0 0.255.255.255 any
deny ip 115.0.0.0 0.255.255.255 any
deny ip 116.0.0.0 0.255.255.255 any
deny ip 117.0.0.0 0.255.255.255 any
deny ip 118.0.0.0 0.255.255.255 any
deny ip 119.0.0.0 0.255.255.255 any
deny ip 120.0.0.0 0.255.255.255 any
deny ip 121.0.0.0 0.255.255.255 any
deny ip 122.0.0.0 0.255.255.255 any
deny ip 123.0.0.0 0.255.255.255 any
deny ip 124.0.0.0 0.255.255.255 any
deny ip 125.0.0.0 0.255.255.255 any
deny ip 126.0.0.0 0.255.255.255 any
deny ip 197.0.0.0 0.255.255.255 any
deny ip 201.0.0.0 0.255.255.255 any
```

```
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any

deny ip 224.0.0.0 15.255.255.255 any
deny ip 240.0.0.0 15.255.255.255 any
deny ip 0.0.0.0 0.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip 192.0.2.0 0.0.0.255 any
deny ip 127.0.0.0 0.255.255.255 any
permit ip any any
remark This acl might not be up to date. Visit
www.iana.org/assignments/ipv4-add
ress-space for update list
exit
```

Note   Next, AutoSecure applies the ACL that you selected via the AutoSecure script to the Internet-facing router interface or interfaces. Here the autosec_iana_reserved_block (option 1) ACL is applied on the inbound side of the Ethernet0/1 interface.

```
interface Ethernet0/1
 ip access-group autosec_iana_reserved_block in
exit
```

Note   Next, AutoSecure creates an extended-numbered ACL (100). This ACL permits UDP Bootstrap Protocol client (bootpc) packets from any source to any destination. This ACL is used by Unicast RPF on Internet-facing router interfaces.

```
ip access-list extended 100
 permit udp any any eq bootpc
```

Note   Next, AutoSecure enables Unicast RPF strict checking mode using ACL 100 on all Internet-facing router interfaces. Because ACL 100 permits bootpc packets, spoofed bootpc packets will be forwarded to the destination address. The forwarded bootpc packets are counted in the interface statistics.

```
interface Ethernet0/1
 ip verify unicast source reachable-via rx 100
```

Note   Next, AutoSecure enables CBAC audit-trail logging to provide a record of network access through the Cisco IOS Firewall, including illegitimate access attempts, and inbound and outbound services.

```
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
```

```
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
```

```
interface Ethernet0/1
 ip inspect autosec_inspect out
!
end
```

```
Apply this configuration to running-config? [yes]: y
```

Note	If you chose to configure SSH server, AutoSecure will now generate the RSA keys using the hostname and domain name you configured during the AutoSecure script. Please note that the factory default router name of **Router** will cause errors during key generation.

```
Applying the config generated to running-config
The name for the keys will be: R2.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys …[OK]
```

Example: Typical Router Configuration Before AutoSecure

The following example shows the router configuration just prior to applying the AutoSecure configuration changes:

```
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
no logging console
enable password cisco
!
memory-size iomem 15
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
interface Ethernet0/0
 ip address 10.0.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.2.2 255.255.255.0
 half-duplex
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
```

```
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
!
!
end
```

Example: Typical Router Configuration After AutoSecure

The following example shows the result of applying this configuration to the running configuration:

```
!
version 12.3
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname R2
!
security authentication failure rate 10 log
security passwords min-length 6
logging buffered 4096 debugging
logging console critical
enable secret 5 $1$O4np$y8yIPRJ07h2.bZzPngIDC.
enable password 7 00071A150754
!
username student1 password 7 095F5A1C1D0019065A
memory-size iomem 15
aaa new-model
```

```
!
!
aaa authentication login local_auth local
aaa session-id common
ip subnet-zero
no ip source-route
no ip gratuitous-arps
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
!
no ip bootp server
ip inspect audit-trail
ip inspect udp idle-time 1800
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
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
ip audit notify log
ip audit po max-events 100
ip ssh time-out 60
ip ssh authentication-retries 2
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
interface Ethernet0/0
 ip address 10.0.2.2 255.255.255.0
 no ip redirects
 no ip unreachables
```

```
 no ip proxy-arp
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.2.2 255.255.255.0
 ip access-group autosec_iana_reserved_block in
 ip verify unicast source reachable-via rx 100
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip inspect autosec_inspect out
 half-duplex
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
!
!
ip access-list extended autosec_complete_bogon
 deny    ip 1.0.0.0 0.255.255.255 any
 deny    ip 2.0.0.0 0.255.255.255 any
 deny    ip 5.0.0.0 0.255.255.255 any
 deny    ip 7.0.0.0 0.255.255.255 any
 deny    ip 23.0.0.0 0.255.255.255 any
 deny    ip 27.0.0.0 0.255.255.255 any
 deny    ip 31.0.0.0 0.255.255.255 any
 deny    ip 36.0.0.0 0.255.255.255 any
 deny    ip 37.0.0.0 0.255.255.255 any
 deny    ip 39.0.0.0 0.255.255.255 any
 deny    ip 41.0.0.0 0.255.255.255 any
 deny    ip 42.0.0.0 0.255.255.255 any
 deny    ip 49.0.0.0 0.255.255.255 any
 deny    ip 50.0.0.0 0.255.255.255 any
 deny    ip 58.0.0.0 0.255.255.255 any
 deny    ip 59.0.0.0 0.255.255.255 any
 deny    ip 60.0.0.0 0.255.255.255 any
 deny    ip 70.0.0.0 0.255.255.255 any
```

```
deny   ip 71.0.0.0 0.255.255.255 any
deny   ip 72.0.0.0 0.255.255.255 any
deny   ip 73.0.0.0 0.255.255.255 any
deny   ip 74.0.0.0 0.255.255.255 any
deny   ip 75.0.0.0 0.255.255.255 any
deny   ip 76.0.0.0 0.255.255.255 any
deny   ip 77.0.0.0 0.255.255.255 any
deny   ip 78.0.0.0 0.255.255.255 any
deny   ip 79.0.0.0 0.255.255.255 any
deny   ip 83.0.0.0 0.255.255.255 any
deny   ip 84.0.0.0 0.255.255.255 any
deny   ip 85.0.0.0 0.255.255.255 any
deny   ip 86.0.0.0 0.255.255.255 any
deny   ip 87.0.0.0 0.255.255.255 any
deny   ip 88.0.0.0 0.255.255.255 any
deny   ip 89.0.0.0 0.255.255.255 any
deny   ip 90.0.0.0 0.255.255.255 any
deny   ip 91.0.0.0 0.255.255.255 any
deny   ip 92.0.0.0 0.255.255.255 any
deny   ip 93.0.0.0 0.255.255.255 any
deny   ip 94.0.0.0 0.255.255.255 any
deny   ip 95.0.0.0 0.255.255.255 any
deny   ip 96.0.0.0 0.255.255.255 any
deny   ip 97.0.0.0 0.255.255.255 any
deny   ip 98.0.0.0 0.255.255.255 any
deny   ip 99.0.0.0 0.255.255.255 any
deny   ip 100.0.0.0 0.255.255.255 any
deny   ip 101.0.0.0 0.255.255.255 any
deny   ip 102.0.0.0 0.255.255.255 any
deny   ip 103.0.0.0 0.255.255.255 any
deny   ip 104.0.0.0 0.255.255.255 any
deny   ip 105.0.0.0 0.255.255.255 any
deny   ip 106.0.0.0 0.255.255.255 any
deny   ip 107.0.0.0 0.255.255.255 any
deny   ip 108.0.0.0 0.255.255.255 any
deny   ip 109.0.0.0 0.255.255.255 any
deny   ip 110.0.0.0 0.255.255.255 any
deny   ip 111.0.0.0 0.255.255.255 any
deny   ip 112.0.0.0 0.255.255.255 any
deny   ip 113.0.0.0 0.255.255.255 any
deny   ip 114.0.0.0 0.255.255.255 any
deny   ip 115.0.0.0 0.255.255.255 any
```

```
deny    ip 116.0.0.0 0.255.255.255 any
deny    ip 117.0.0.0 0.255.255.255 any
deny    ip 118.0.0.0 0.255.255.255 any
deny    ip 119.0.0.0 0.255.255.255 any
deny    ip 120.0.0.0 0.255.255.255 any
deny    ip 121.0.0.0 0.255.255.255 any
deny    ip 122.0.0.0 0.255.255.255 any
deny    ip 123.0.0.0 0.255.255.255 any
deny    ip 124.0.0.0 0.255.255.255 any
deny    ip 125.0.0.0 0.255.255.255 any
deny    ip 126.0.0.0 0.255.255.255 any
deny    ip 197.0.0.0 0.255.255.255 any
deny    ip 201.0.0.0 0.255.255.255 any
deny    ip 10.0.0.0 0.255.255.255 any
deny    ip 172.16.0.0 0.15.255.255 any
deny    ip 192.168.0.0 0.0.255.255 any
deny    ip 224.0.0.0 15.255.255.255 any
deny    ip 240.0.0.0 15.255.255.255 any
deny    ip 0.0.0.0 0.255.255.255 any
deny    ip 169.254.0.0 0.0.255.255 any
deny    ip 192.0.2.0 0.0.0.255 any
deny    ip 127.0.0.0 0.255.255.255 any
permit ip any any
remark This acl might not be up to date. Visit
www.iana.org/assignments/ipv4-ad
dress-space for update list
ip access-list extended autosec_firewall_acl
permit udp any any eq bootpc
deny    ip any any
ip access-list extended autosec_iana_reserved_block
deny    ip 1.0.0.0 0.255.255.255 any
deny    ip 2.0.0.0 0.255.255.255 any
deny    ip 5.0.0.0 0.255.255.255 any
deny    ip 7.0.0.0 0.255.255.255 any
deny    ip 23.0.0.0 0.255.255.255 any
deny    ip 27.0.0.0 0.255.255.255 any
deny    ip 31.0.0.0 0.255.255.255 any
deny    ip 36.0.0.0 0.255.255.255 any
deny    ip 37.0.0.0 0.255.255.255 any
deny    ip 39.0.0.0 0.255.255.255 any
deny    ip 41.0.0.0 0.255.255.255 any
deny    ip 42.0.0.0 0.255.255.255 any
```

```
deny    ip 49.0.0.0 0.255.255.255 any
deny    ip 50.0.0.0 0.255.255.255 any
deny    ip 58.0.0.0 0.255.255.255 any
deny    ip 59.0.0.0 0.255.255.255 any
deny    ip 60.0.0.0 0.255.255.255 any
deny    ip 70.0.0.0 0.255.255.255 any
deny    ip 71.0.0.0 0.255.255.255 any
deny    ip 72.0.0.0 0.255.255.255 any
deny    ip 73.0.0.0 0.255.255.255 any
deny    ip 74.0.0.0 0.255.255.255 any
deny    ip 75.0.0.0 0.255.255.255 any
deny    ip 76.0.0.0 0.255.255.255 any
deny    ip 77.0.0.0 0.255.255.255 any
deny    ip 78.0.0.0 0.255.255.255 any
deny    ip 79.0.0.0 0.255.255.255 any
deny    ip 83.0.0.0 0.255.255.255 any
deny    ip 84.0.0.0 0.255.255.255 any
deny    ip 85.0.0.0 0.255.255.255 any
deny    ip 86.0.0.0 0.255.255.255 any
deny    ip 87.0.0.0 0.255.255.255 any
deny    ip 88.0.0.0 0.255.255.255 any
deny    ip 89.0.0.0 0.255.255.255 any
deny    ip 90.0.0.0 0.255.255.255 any
deny    ip 91.0.0.0 0.255.255.255 any
deny    ip 92.0.0.0 0.255.255.255 any
deny    ip 93.0.0.0 0.255.255.255 any
deny    ip 94.0.0.0 0.255.255.255 any
deny    ip 95.0.0.0 0.255.255.255 any
deny    ip 96.0.0.0 0.255.255.255 any
deny    ip 97.0.0.0 0.255.255.255 any
deny    ip 98.0.0.0 0.255.255.255 any
deny    ip 99.0.0.0 0.255.255.255 any
deny    ip 100.0.0.0 0.255.255.255 any
deny    ip 101.0.0.0 0.255.255.255 any
deny    ip 102.0.0.0 0.255.255.255 any
deny    ip 103.0.0.0 0.255.255.255 any
deny    ip 104.0.0.0 0.255.255.255 any
deny    ip 105.0.0.0 0.255.255.255 any
deny    ip 106.0.0.0 0.255.255.255 any
deny    ip 107.0.0.0 0.255.255.255 any
deny    ip 108.0.0.0 0.255.255.255 any
deny    ip 109.0.0.0 0.255.255.255 any
```

```
 deny    ip 110.0.0.0 0.255.255.255 any
 deny    ip 111.0.0.0 0.255.255.255 any
 deny    ip 112.0.0.0 0.255.255.255 any
 deny    ip 113.0.0.0 0.255.255.255 any
 deny    ip 114.0.0.0 0.255.255.255 any
 deny    ip 115.0.0.0 0.255.255.255 any
 deny    ip 116.0.0.0 0.255.255.255 any
 deny    ip 117.0.0.0 0.255.255.255 any
 deny    ip 118.0.0.0 0.255.255.255 any
 deny    ip 119.0.0.0 0.255.255.255 any
 deny    ip 120.0.0.0 0.255.255.255 any
 deny    ip 121.0.0.0 0.255.255.255 any
 deny    ip 122.0.0.0 0.255.255.255 any
 deny    ip 123.0.0.0 0.255.255.255 any
 deny    ip 124.0.0.0 0.255.255.255 any
 deny    ip 125.0.0.0 0.255.255.255 any
 deny    ip 126.0.0.0 0.255.255.255 any
 deny    ip 197.0.0.0 0.255.255.255 any
 deny    ip 201.0.0.0 0.255.255.255 any
 permit ip any any
 remark This acl might not be up to date. Visit
www.iana.org/assignments/ipv4-ad
dress-space for update list
ip access-list extended autosec_private_block
 deny    ip 10.0.0.0 0.255.255.255 any
 deny    ip 172.16.0.0 0.15.255.255 any
 deny    ip 192.168.0.0 0.0.255.255 any
 permit ip any any
logging trap debugging
logging facility local2
access-list 100 permit udp any any eq bootpc
no cdp run
!
radius-server authorization permit missing Service-Type
!
!
!
!
banner motd ^CThis system is the property of Cisco Systems, Inc.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.^C
!
line con 0
```

```
 exec-timeout 5 0
 login authentication local_auth
 transport output telnet
line aux 0
 login authentication local_auth
 transport output telnet
line vty 0 4
 password 7 14141B180F0B
 login authentication local_auth
 transport input telnet ssh
!
!
!
end
```

Summary

This topic summarizes what you have learned in this lesson.

Summary

- **Unused router services and interfaces should be disabled.**
- **There are several different types of Cisco access lists, and it is important that you know where and when they should be used.**
- **Access lists are used to mitigate many common router and network security threats.**
- **Syslog logging is a very useful tool to have in your security toolkit.**
- **A secure management and reporting environment is a very important part of your network.**
- **AutoSecure is a very efficient tool for securing Cisco routers.**

SECUR 1.1—5-97

Lab Exercise—Cisco Router Threat Mitigation

Complete the following lab exercise to practice what you learned in this lesson.

Objectives

In this lab exercise, you will complete the following tasks:

- Complete the lab exercise setup.
- Configure and apply ACL 103.
- Configure Syslog logging.
- Perform security tests.
- Use AutoSecure to secure the perimeter router.

Visual Objective

The figure displays the configuration you will complete in this lab exercise.
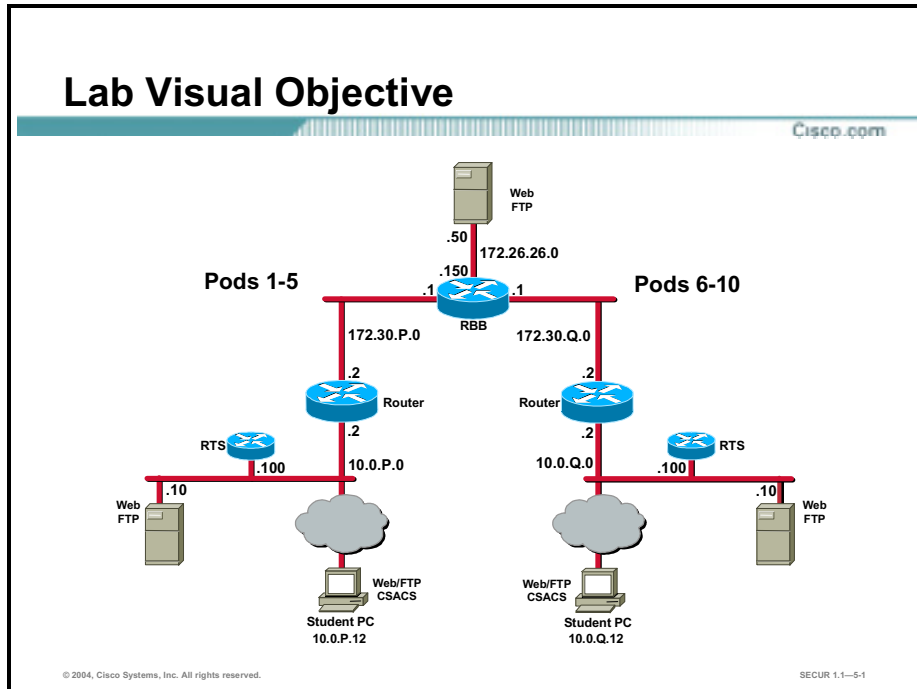
Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1 Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2 Configure your student PC for IP address **10.0.P.12** with a default gateway of **10.0.P.2** (where P = pod number).

Step 3 Make sure that your student PC has an appropriate Syslog server application installed (for example; Kiwi's Syslog Daemon).

Step 4 Reload your perimeter router using the default lab configuration.

Step 5 Make sure that you can ping your peer perimeter router and student PC.

Step 6 Make sure that your router is running the correct date and time.

Step 7 Make sure that your student PC is running the correct date and time.

Step 8 Reference the following table when configuring ACLs for this lab.

Protocol	Protocol type	Port Number
FTP	TCP	20, 21, and random ports greater than 1023
Telnet	TCP	23
DNS	TCP/UDP	53/53

HTTP	TCP	80
SHTTP	TCP	443
NNTP	TCP	119
NTP	UDP	123
SMTP	TCP	25
SNMP	UDP	161
Ping	ICMP	Echo-Request Echo-Reply

Task 2—Configure and Apply ACL 103

Complete the following steps to configure ACL 103 and apply it to router interface e0/1:

Step 1 Create a new text file and save it to your student PC desktop using an appropriate file name.

Step 2 Enter the following lines in the text file to configure ACL 103 to permit routing updates from the backbone router:

```
access-list 103 remark Permit routing updates from backbone router
access-list 103 permit eigrp host 172.30.P.1 host 172.30.P.2
access-list 103 permit eigrp host 172.30.P.1 host 224.0.0.10
access-list 103 permit eigrp host 172.26.26.150 host 172.30.P.2
access-list 103 permit eigrp host 172.26.26.150 host 224.0.0.10
```

(where P = pod number)

Step 3 Enter the following lines in the text file to configure ACL 103 to permit established sessions:

```
access-list 103 remark Permit established sessions
access-list 103 permit tcp any 172.30.P.0 0.0.0.255 established
access-list 103 permit tcp any 10.0.P.0 0.0.0.255 established
```

(where P = pod number)

Step 4 Enter the following lines in the text file to configure ACL 103 to deny reserved loopback addresses:

```
access-list 103 remark Deny reserved loopback addresses
access-list 103 deny ip 127.0.0.0 0.255.255.255 any log
```

Step 5 Enter the following lines in the text file to configure ACL 103 to deny the reserved broadcast address:

```
access-list 103 remark Deny reserved broadcast address
access-list 103 deny ip 255.0.0.0 0.255.255.255 any log
```

Step 6 Enter the following lines in the text file to configure ACL 103 to deny multi-cast addresses:

```
access-list 103 remark Deny multi-cast addresses
access-list 103 deny ip 224.0.0.0 7.255.255.255 any log
```

Step 7 Enter the following lines in the text file to configure ACL 103 to deny RFC 1918 address:

```
access-list 103 remark Deny RFC 1918 address not in use for lab
```

```
access-list 103 deny ip 192.168.0.0 0.0.255.255 any log
```

Step 8   Enter the following lines in the text file to configure ACL 103 to deny untrusted network traffic using trusted network source addresses:

```
access-list 103 remark Deny source address of trusted network
access-list 103 deny ip 10.0.P.0 0.0.0.255 any log
```

(where P = pod number)

Step 9   Enter the following lines in the text file to configure ACL 103 to deny any undefined source addresses:

```
access-list 103 remark Deny undefined source address
access-list 103 deny ip host 0.0.0.0 any log
```

Step 10   Enter the following lines in the text file to configure ACL 103 to deny all SNMP traffic originating from outside the trusted network:

```
access-list 103 remark Deny SNMP access from outside of the trusted
network
access-list 103 deny udp any any eq snmp
```

Step 11   Enter the following lines in the text file to configure ACL 103 to permit specific service traffic:

```
access-list 103 remark Permit specific services
access-list 103 permit tcp any host 10.0.P.10 eq 20
access-list 103 permit tcp any host 10.0.P.10 eq 21
access-list 103 permit tcp any host 10.0.P.10 eq 23
access-list 103 permit tcp any host 10.0.P.10 eq 25
access-list 103 permit tcp any host 10.0.P.10 eq 53
access-list 103 permit udp any host 10.0.P.10 eq 53
access-list 103 permit tcp any host 10.0.P.10 eq 80
access-list 103 permit tcp any host 10.0.P.10 eq 119
access-list 103 permit udp any host 10.0.P.10 eq 123
access-list 103 permit tcp any host 10.0.P.10 eq 443
access-list 103 permit tcp any host 10.0.P.10 gt 1023
```

(where P = pod number)

Step 12   Enter the following lines in the text file to configure ACL 103 to control Ping access from ISP devices:

```
access-list 103 remark Control Ping access from ISP devices
access-list 103 permit icmp host 172.26.26.50 host 172.30.P.2
access-list 103 permit icmp host 172.30.P.1 host 172.30.P.2
access-list 103 permit icmp host 172.30.P.1 10.0.P.0 0.0.0.255
access-list 103 permit icmp host 172.26.26.50 10.0.P.0 0.0.0.255
```

(where P = pod number)

Step 13 Enter the following lines in the text file to configure ACL 103 to explicitly deny all other traffic:

```
access-list 103 deny ip any any log
```

Step 14 Save the text file and double-check your work.

Step 15 Copy the contents of the text file into the running configuration of the router.

Step 16 Use the **show run** command to make sure that ACL 103 is configured properly.

Step 17 Apply ACL 103 to router interface Ethernet0/1 (inbound):

```
RP(config)# interface fast 0/1
RP(config-if)# ip access-group 103 in
RP(config-if)# end
```

Step 18 Save your configuration changes to startup-config.

Task 3—Configure Syslog Logging

Complete the following steps to configure Syslog logging on your perimeter router to send logging messages to the Syslog server on your student PC:

Step 1 Configure the destination Syslog server by entering a destination IP address of **10.0.P.12**.

```
RP(config)# logging 10.0.P.12
```

(where P = pod number)

Step 2 Configure the logging severity (trap) level:

```
RP(config)# logging trap debug
```

(where P = pod number)

Step 3 Configure the logging source interface:

```
RP(config)# logging source-interface fast 0/0
```

(where P = pod number)

Step 4 Exit configuration mode.

Step 5 Save your router configuration changes to startup-config.

Step 6 Start the Syslog daemon on your student PC.

Note: If you do not have a Syslog server application, enable the router console logging using the **logging console** command. Although this does not test the Syslog server settings you just configured, you will still be able to view debug messages generated from ACL 103 deny statements.

Task 4—Perform Security Tests

Work with the opposite pod group to verify the access lists from the opposite perimeter router using Cisco IOS commands. If you cannot complete the following steps, correct any deficiencies and retest:

Step 1   Open a command shell on your student PC and complete the remaining steps using this shell.

Step 2   Ping **172.30.Q.2**. You should see a denied message in the Syslog (where Q = peer pod number).

Step 3   Ping **10.0.Q.2**. You should see a denied message in the Syslog (where Q = peer pod number).

Step 4   Telnet to **172.30.Q.2**. You should see a denied message in the Syslog (where Q = peer pod number).

Step 5   Telnet to **10.0.Q.2**. You should see a denied message in the Syslog (where Q = peer pod number).

Step 6   Ping **172.30.P.2**. You should be able to ping your own router interface (where P = pod number).

Step 7   Ping **10.0.P.2**. You should be able to ping your own router interface (where P = pod number).

Step 8   Telnet to **10.0.P.2**. You should be able to telnet to your own router (where P = pod number).

Step 9   Close the Syslog server window.

Task 5—Use AutoSecure to Secure the Perimeter Router

Complete the following steps to secure the perimeter router using the AutoSecure feature:

Step 1   Reload your perimeter router using the default lab configuration.

Step 2   View the default router configuration to understand what the router settings are before you run AutoSecure.

Step 3   Run AutoSecure in interactive mode.

```
RP# auto secure
```

Note: AutoSecure will prompt you to answer several questions regarding the configuration of the
               perimeter router. Answer these questions as they appear. At the end of the AutoSecure
               script, you will be prompted to apply the changes to the router running configuration.

Step 4   Answer **yes** when prompted to apply the AutoSecure changes to the router running configuration.

Step 5   View the new running configuration of your perimeter router and note the changes.

Step 6   (Optional.) If time permits, return the router to the default lab configuration and rerun AutoSecure. This time, choose to run AutoSecure in noninteractive mode.

```
RP# auto secure no-interact
```

Step 7   (Optional.) Once AutoSecure completes the noninteractive procedure, check to see what changes were made to your perimeter router running configuration.

6

Cisco IOS Firewall Context-Based Access Control Configuration

Overview

This lesson includes the following topics:

- Objectives
- Introduction to the Cisco IOS Firewall
- Context-Based Access Control
- Global timeouts and thresholds
- Port-to-Application Mapping
- Define inspection rules
- Inspection rules and ACLs applied to router interfaces
- Test and verify
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- **Define the Cisco IOS Firewall.**
- **Define CBAC.**
- **Configure CBAC.**

SECUR 1.1—6-3

Introduction to the Cisco IOS Firewall

This topic introduces the features of the Cisco IOS Firewall.

The Cisco IOS Firewall Feature Set

Cisco.com

The Cisco IOS Firewall contains the following three main features:

• **Context-Based Access Control (CBAC)**
• **Authentication Proxy**
• **Intrusion Detection System**

SECUR 1.1—6-5

The Cisco IOS Firewall is a security-specific option for Cisco IOS software. It integrates robust firewall functionality, authentication proxy, and intrusion detection for every network perimeter, and enriches existing Cisco IOS security capabilities. It adds greater depth and flexibility to existing Cisco IOS security solutions, such as authentication, encryption, and failover, by delivering state-of-the-art security features, such as stateful, application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts. When combined with Cisco IOS Internet Protocol Security (IPSec) software and other Cisco IOS software-based technologies, such as Layer 2 Tunneling Protocol (L2TP) tunneling and quality of service (QoS), the Cisco IOS Firewall provides a complete, integrated virtual private network (VPN) solution.

Context-Based Access Control

The Cisco IOS Firewall Context-Based Access Control (CBAC) engine provides secure, per-application access control across network perimeters. CBAC enhances security for TCP and UDP applications that use well-known ports, such as FTP and e-mail traffic, by scrutinizing source and destination addresses. CBAC allows network administrators 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 would no longer need to open a network doorway accessible via weaknesses in a partner's network. CBAC enables tightly secured networks to run today's basic application traffic, as well as advanced applications such as multimedia and videoconferencing, securely through a router.

Authentication Proxy

Network administrators can create specific security policies for each user with Cisco IOS Firewall LAN-based, dynamic, per-user authentication and authorization. Previously, user identity and related authorized access were determined by a user's fixed IP address, or a single security policy had to be applied to an entire user group or subnet. Now, per-user policy can be downloaded dynamically to the router from a Terminal Access Controller Access Control System Plus (TACACS+) or Remote Access Dial-In User Service (RADIUS) authentication server using Cisco IOS software authentication, authorization, and accounting (AAA) services.

Users can log into the network or access the Internet via HTTP, and their specific access profiles will automatically be downloaded. Appropriate dynamic individual access privileges are available as required, protecting the network against more general policies applied across multiple users. Authentication and authorization can be applied to the router interface in either direction to secure inbound or outbound extranet, intranet, and Internet usage.

Intrusion Detection System

Intrusion detection systems (IDS) provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS IDS 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 IDS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators now enjoy more robust protection against attacks on the network, and can automatically respond to threats from internal or external hosts.

Cisco IOS Firewall CBAC

TCP

Internet

UDP
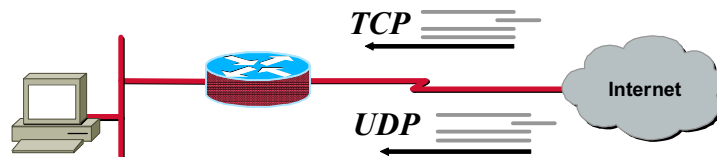
- **Packets are inspected entering the firewall by CBAC if they are not specifically denied by an ACL.**
- **CBAC permits or denies specified TCP and UDP traffic through a firewall.**
- **A state table is maintained with session information.**
- **ACLs are dynamically created or deleted.**
- **CBAC protects against DoS attacks.**

SECUR 1.1—6-6

CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information. It can inspect traffic for sessions that originate on any interface of the router. CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's Access Control Lists (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 provides CBAC with the ability to detect and prevent certain types of network attacks, such as SYN flooding. CBAC also inspects packet sequence numbers in TCP connections to see if they are within expected ranges—CBAC drops any suspicious packets. Additionally, CBAC can detect unusually high rates of new connections and issue alert messages. CBAC inspection can help protect against certain denial of service (DoS) attacks involving fragmented IP packets.

You will learn how to configure and administer the Cisco IOS Firewall CBAC feature in this lesson.

Cisco IOS Firewall Authentication Proxy
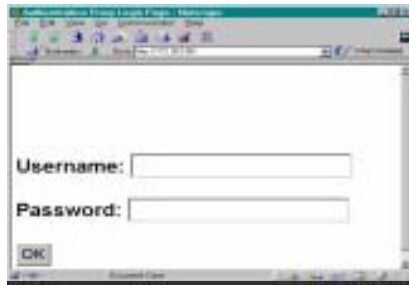
- **HTTP, HTTPS, FTP, and Telnet authentication**
- **Provides dynamic, per-user authentication and authorization via TACACS+ and RADIUS protocols**

The Cisco IOS Firewall authentication proxy feature enables network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's 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 general policy applied across multiple users.

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, HTTPS, FTP, and Telnet and their specific access profiles are automatically retrieved and applied from a Cisco Secure Access Control Server (CSACS), or other RADIUS or TACACS+ authentication server. 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 Network Address Translation (NAT), IPSec encryption, and VPN client software.

Cisco IOS Intrusion Detection System

TCP

Internet

UDP
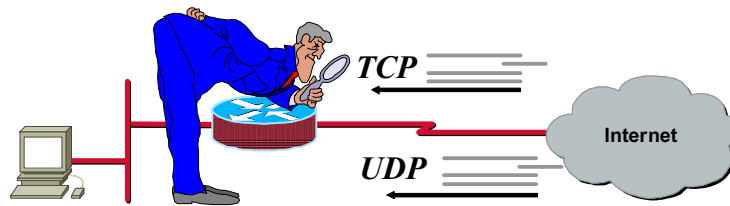
- **Acts as an in-line IOS intrusion detection sensor.**
- **When a packet or packets match a signature, it can perform any of the following configurable actions:**
  - **Alarm—Send an alarm to a CIDS Director or Syslog server.**
  - **Drop—Drop the packet.**
  - **Reset—Send TCP resets to terminate the session.**
- **Identifies 100+ common attacks.**

SECUR 1.1—6-8

The Cisco IOS IDS now offers intrusion detection technology for mid-range and high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations in which a router is being deployed and additional security between network segments is required. It also 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 IDS identifies 100+ common attacks using signatures to detect patterns of misuse in network traffic. The intrusion detection signatures of the Cisco IOS IDS were chosen from a broad cross-section of intrusion detection signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

Context-Based Access Control

This topic describes the limitations of Cisco IOS ACLs and explains how Context-Based Access Control (CBAC) better protects users from attack. It also lists the protocols supported by CBAC and describes the added alert and audit trail features. Finally, the CBAC configuration tasks are listed.

Cisco IOS ACLs

- **Provide traffic filtering by**
    - **Source and destination IP addresses.**
    - **Source and destination ports.**
- **Can be used to implement a filtering firewall**
    - **Ports are opened permanently to allow traffic, creating a security vulnerability.**
    - **Do not work with applications that negotiate ports dynamically.**

SECUR 1.1—6-10

Before delving into CBAC, some basic ACL concepts need to be covered 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 CBAC, traffic filtering is limited to ACL implementations that examine packets at the network layer, or at most, the transport layer.

How CBAC Works

1 Control traffic is inspected by the CBAC rule.

`ip inspect name FWRULE tcp`
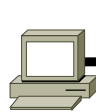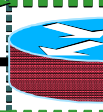
2 CBAC creates a dynamic ACL allowing return traffic back through the firewall.

`access-list 102 permit TCP host 172.30.1.50 eq 23 host 10.0.0.3 eq 2447`

Port 2447

Port 23

3 CBAC continues to inspect control traffic and dynamically creates and removes ACLs as required by the application. It also monitors and protects against application-specific attacks.

4 CBAC detects when an application terminates or times out and removes all dynamic ACLs for that session.

SECUR 1.1—6-11

With CBAC, you specify which protocols you want inspected, and you specify an interface and interface direction (in or out) where the inspection originates. Only specified protocols will be inspected by CBAC. For these protocols, packets flowing through the firewall in any direction are inspected, as long as they flow through the interface where inspection is configured. Packets entering the firewall are inspected by CBAC only if they first pass the inbound ACL at the interface. If a packet is denied by the ACL, the packet is simply dropped and not inspected by CBAC.

CBAC 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 CBAC software parses the FTP commands and responses).

CBAC inspection recognizes application-specific commands in the control channel, and detects and prevents certain application-level attacks. CBAC inspection tracks sequence numbers in all TCP packets, and drops those packets with sequence numbers that are not within expected ranges. CBAC inspection 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 CBAC suspects an attack, the DoS feature can take several actions:

■ Generate alert messages

■ Protect system resources that could impede performance

■ Block packets from suspected attackers

CBAC uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. Setting timeout values for network sessions helps prevent DoS attacks by freeing system resources, dropping sessions after a specified amount of time. Setting threshold values for network 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, CBAC 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.

CBAC provides three thresholds against DoS attacks:

- The total number of half-opened TCP or UDP sessions

- The number of half-opened sessions based on time

- The number of half-opened TCP-only sessions per host

If a threshold is exceeded, CBAC has two options:

- Send a reset message to the endpoints of the oldest half-opened session, making resources available to service newly arriving SYN packets.

- In the case of half-opened TCP-only sessions, CBAC 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.

DoS detection and prevention requires that you create a CBAC inspection rule and apply that rule on an interface. The inspection rule must include the protocols that you want to monitor against DoS attacks. For example, if you have TCP inspection enabled on the inspection rule, then CBAC can track all TCP connections to watch for DoS attacks. If the inspection rule includes FTP protocol inspection but not TCP inspection, CBAC tracks only FTP connections for DoS attacks.

A state table maintains session state information. Whenever a packet is inspected, a state table is updated to include information about the state of the packet's connection. Return traffic will only be permitted back through the firewall if the state table contains information indicating that the packet belongs to a permissible session. Inspection controls the traffic that belongs to a valid session and forwards the traffic it does not know. When return traffic is inspected, the state table information is updated as necessary.

UDP sessions are approximated. With UDP there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, similar source or destination addresses and port numbers), and if the packet was detected soon after another, similar UDP packet. Soon means within the configurable UDP idle timeout period.

ACL entries are dynamically created and deleted. CBAC dynamically creates and deletes ACL entries at the firewall interfaces, according to the information maintained in the state tables. These ACL entries are applied to the interfaces 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. The temporary ACL entries are never saved to nonvolatile RAM (NVRAM.)

Supported Protocols

Cisco.com

- TCP (single channel)
- UDP (single channel)
- RPC
- FTP
- TFTP
- UNIX R-commands (such as rlogin, rexec, and rsh)
- SMTP
- HTTP (Java blocking)
- ICMP

- Java
- SQL*Net
- RTSP (such as RealNetworks)
- H.323 (such as NetMeeting, ProShare, CUSeeMe)
- Other multimedia
  - Microsoft NetShow
  - StreamWorks
  - VDOLive
- SIP

SECUR 1.1—6-12

You can configure CBAC to inspect the following types of sessions:

- All TCP sessions, regardless of the application-layer protocol (sometimes called single-channel or generic TCP inspection)

- All UDP sessions, regardless of the application-layer protocol (sometimes called single-channel or generic UDP inspection)

You can also configure CBAC to specifically inspect certain application-layer protocols. The following application-layer protocols can all be configured for CBAC:

- RPC (Sun RPC, not DCE RPC)

- Microsoft RPC

- FTP

- TFTP

- UNIX R-commands (such as rlogin, rexec, and rsh)

- SMTP

- HTTP (Java blocking)

- ICMP

- SQL*Net

- RTSP (for example: RealNetworks)

- H.323 (for example: NetMeeting, ProShare, CU-SeeMe [only the White Pine version])

- Microsoft NetShow

- StreamWorks

- VDOLive

- SIP

When a protocol is configured for CBAC, 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.

- **CBAC generates real-time alerts and audit trails.**
- **Audit trail features use Syslog to track all network transactions.**
- **With CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis.**

CBAC also generates real-time alerts and audit trails based on events tracked by the firewall. 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 CBAC 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 CBAC rule covering HTTP inspection.

CBAC Configuration

- Set audit trails and alerts.
- Set global timeouts and thresholds.
- Define PAM.
- Define inspection rules.
- Apply inspection rules and ACLs to interfaces.
- Test and verify.

SECUR 1.1—6-14

The following are the tasks used to configure CBAC:

- Set audit trails and alerts.

- Set global timeouts and thresholds.

- Define Port-to-Application Mapping (PAM).

- Define inspection rules.

- Apply inspection rules and ACLs to interfaces.

- Test and verify.

Enable 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 10.0.0.3
Router(config)# ip inspect audit-trail
Router(config)# no ip inspect alert-off
```

Turn on audit trail logging and real-time alerts 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.

Step 2 Turn on CBAC audit trail messages using the **ip inspect audit-trail** command in global configuration mode. To turn off CBAC audit trail messages, use the **no** form of this command.

Step 3 Turn on CBAC real-time alerts using the **no ip inspect alert-off** command in global configuration mode. To turn off CBAC real-time alerts, use the standard form of this command (CBAC real-time alerts are off by default).

The syntax for the **ip inspect audit-trail** commands is as follows:

ip inspect audit-trail

no ip inspect audit-trail

These commands have no arguments or keywords.

The syntax for the **no ip inspect alert-off** command is as follows:

no ip inspect alert-off

This command has no keywords or arguments.

Global Timeouts and Thresholds

This topic discusses how to configure the following global timeouts and thresholds:

- TCP, SYN, and FIN wait times
- TCP, UDP, and Domain Name System (DNS) idle times
- TCP flood DoS protection

TCP, SYN, and FIN Wait Times

Cisco.com

Router(config)#

```
ip inspect tcp synwait-time seconds
```

- **Specifies the time the Cisco IOS Firewall waits for a TCP session to reach the established state**

Router(config)#

```
ip inspect tcp finwait-time seconds
```

- **Specifies the time the Cisco IOS Firewall waits for a FIN exchange to complete before quitting the session**

SECUR 1.1—6-17

CBAC uses timeouts and thresholds to determine how long to manage state information for a session, and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply globally to all sessions.

You can use the default timeout and threshold values, or you can change to values more suitable to your security requirements. You should make any changes to the timeout and threshold values before you continue configuring CBAC.

Use the **ip inspect tcp synwait-time** global configuration command to define how long the software will wait for a TCP session to reach the established state before dropping the session. Use the **no** form of this command to reset the timeout to the default.

The syntax of the **ip inspect tcp synwait-time** command is as follows:

ip inspect tcp synwait-time *seconds*

no ip inspect tcp synwait-time

seconds	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session (the default is 30 seconds).

Use the **ip inspect tcp finwait-time** global configuration command to define how long a TCP session will still be managed after the firewall detects a FIN exchange. Use the **no** form of this command to reset the timeout to default.

The syntax of the **ip inspect tcp finwait-time** command is as follows:

ip inspect tcp finwait-time *seconds*

no ip inspect tcp finwait-time

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN exchange (the default is 5 seconds).

TCP, UDP, and DNS Idle Times

Router(config)#

```
ip inspect tcp idle-time seconds
ip inspect udp idle-time seconds
```

- **Specifies the time allowed for a TCP or UDP session with no activity**

Router(config)#

```
ip inspect dns-timeout seconds
```

- **Specifies the time allowed for a DNS session with no activity**

Use the **ip inspect tcp idle-time** global configuration command to specify the TCP idle timeout (the length of time a TCP session will still be managed after no activity). Use the **no** form of this command to reset the timeout to default.

Use the **ip inspect udp idle-time** global configuration command to specify the UDP idle timeout (the length of time a UDP session will still be managed after no activity). Use the **no** form of this command to reset the timeout to default.

The syntax for the **ip inspect {tcp | udp} idle-time** commands is as follows:

ip inspect {tcp | udp} idle-time *seconds*

no ip inspect {tcp | udp} idle-time

seconds	Specifies the length of time a TDP or a UDP session will still be managed after no activity. For TCP sessions, the default is 3600 seconds (1 hour). For UDP sessions, the default is 30 seconds.

Use the **ip inspect dns-timeout** global configuration command to specify the DNS idle timeout (the length of time a DNS name lookup session will still be managed after no activity). Use the **no** form of this command to reset the timeout to the default.

The syntax for the **ip inspect dns-timeout** command is as follows:

ip inspect dns-timeout *seconds*

no ip inspect dns-timeout

seconds	Specifies the length of time a DNS name lookup session will still be managed after no activity (the default is 5 seconds).

Global Half-Opened Connection Limits

Router(config)#

```
ip inspect max-incomplete high number
```

- **Defines the number of existing half-opened sessions that cause the software to start deleting half-opened sessions (aggressive mode)**

Router(config)#

```
ip inspect max-incomplete low number
```

- **Defines the number of existing half-opened sessions that cause the software to stop deleting half-opened sessions**

SECUR 1.1—6-19

An unusually high number of half-opened sessions (either absolute or measured as the arrival rate) could indicate that a DoS attack is occurring. For TCP, half-opened means that the session has not reached the established state—the TCP three-way handshake has not yet been completed. For UDP, half-opened means that the firewall has detected no return traffic.

CBAC measures both the total number of existing half-opened sessions and the rate of session establishment attempts. Both TCP and UDP half-opened sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-opened sessions rises above a threshold (the **max-incomplete high** *number*), CBAC will go in to aggressive mode and delete half-opened sessions as required to accommodate new connection requests. The software continues to delete half-opened requests as necessary, until the number of existing half-opened sessions drops below another threshold (the **max-incomplete low** *number*).

Use the **ip inspect max-incomplete high** command in global configuration mode to define the number of existing half-opened sessions that will cause the software to start deleting half-opened sessions. Use the **no** form of this command to reset the threshold to default.

The syntax for the **ip inspect max-incomplete high** command is as follows:

ip inspect max-incomplete high *number*

no ip inspect max-incomplete high *number*

high *number*	Specifies the number of existing half-opened sessions that will cause the software to start deleting half-opened sessions (the default is 500 half-opened sessions).

Use the **ip inspect max-incomplete low** command in global configuration mode to define the number of existing half-opened sessions that will cause the software to stop deleting half-opened sessions. Use the **no** form of this command to reset the threshold to default.

The syntax for the **ip inspect max-incomplete low** command is as follows:

ip inspect max-incomplete low *number*

no ip inspect max-incomplete low *number*

low *number*	Specifies the number of existing half-opened sessions that will cause the software to stop deleting half-opened sessions (the default is 400 half-opened sessions).

When the rate of new connection attempts rises above a threshold (the **one-minute high number**), the software will delete half-opened sessions as required to accommodate new connection attempts. The software continues to delete half-opened sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low number**). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. The firewall router reviews the one-minute rate on an ongoing basis, meaning that the router reviews the rate more frequently than one minute and does not keep deleting half-opened sessions for one-minute after a DoS attack has stopped—it will be less time.

Use the **ip inspect one-minute high** command in global configuration mode to define the rate of new un-established sessions that will cause the software to start deleting half-opened sessions. Use the **no** form of this command to reset the threshold to default.

The syntax for the **ip inspect one-minute high** command is as follows:

ip inspect one-minute high *number*

no ip inspect one-minute high

high *number*	Specifies the rate of new un-established TCP sessions that will cause the software to start deleting half-opened sessions (the default is 500 half-opened sessions).

Use the **ip inspect one-minute low** command in global configuration mode to define the rate of new un-established TCP sessions that will cause the software to stop deleting half-opened sessions. Use the **no** form of this command to reset the threshold to the default.

The syntax for the **ip inspect one-minute low** command is as follows:

ip inspect one-minute low *number*

no ip inspect one-minute low

low *number*	Specifies the number of existing half-opened sessions that will cause the software to stop deleting half-opened sessions (the default is 400 half-opened sessions).

Router(config)#

```
ip inspect tcp max-incomplete host number
 block-time minutes
```

- Defines the number of half-opened TCP sessions with the same host destination address that can exist at a time before the Cisco IOS Firewall starts deleting half-open sessions to the host.
- After the number of half-opened connections is exceeded to a given host, the software deletes half-open sessions on that host in the following manner:
  - If block-time is 0, the oldest half-opened session is deleted, per new connection request, to allow new connections.
  - If block-time is greater than 0, all half-opened sessions are deleted, and new connections to the host are not allowed during the specified block time.

SECUR 1.1—6-21

An unusually high number of half-opened sessions with the same destination host address could indicate that a DoS attack is being launched against the host. Whenever the number of half-opened sessions with the same destination host address rises above a threshold (the **max-incomplete host** *number*), the software will delete half-opened sessions according to one of the following methods:

■ If the **block-time** *minutes* timeout is 0 (the default), the software deletes the oldest existing half-opened session for the host for every new connection request to the host. This ensures that the number of half-opened sessions to a given host will never exceed the threshold.

■ If the **block-time** *minutes* timeout is greater than 0, the software deletes all existing half-opened sessions for the host, and then blocks all new connection requests to the host. The software will continue to block all new connection requests until the block time expires.

The software also sends Syslog messages whenever the **max-incomplete host** *number* is exceeded, and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections inspected by CBAC.

Use the **ip inspect tcp max-incomplete host** global configuration command to specify threshold and blocking time values for TCP host-specific DoS detection and prevention. Use the **no** form of this command to reset the threshold and blocking time to the default values.

The syntax for the **ip inspect tcp max-incomplete host** command is as follows:

ip inspect tcp max-incomplete host *number* **block-time** *minutes*

no ip inspect tcp max-incomplete host

host *number*	Specifies how many half-opened TCP sessions with the same host destination address can exist at a time before the software starts deleting half-opened sessions to the host. Use a number from 1 to 250 (the default is 50 half-opened sessions).
block-time *minutes*	Specifies how long the software will continue to delete new connection requests to the host (the default is 0 minutes).

Port-to-Application Mapping

This topic discusses the configuration of port numbers for application protocols.

Port-to-Application Mapping

- **Ability to configure any port number for an application protocol.**
- **CBAC uses PAM to determine the application configured for a port.**

    SECUR 1.1—6-23

Port-to-Application Mapping (PAM) enables you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

Using the port information, PAM establishes a table of default port-to-application mapping information at the firewall. The information in the PAM table enables CBAC supported services to run on nonstandard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

PAM also supports host or subnet-specific port mapping, which enables you to apply PAM to a single host or subnet using standard ACLs. Host- or subnet-specific port mapping is done using standard ACLs.

PAM creates a table, or database, of system-defined mapping entries using the well-known or registered port mapping information set up during the system startup. The system-defined entries comprise all the services supported by CBAC, which requires the system-defined mapping information to function properly.

Note	The system-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

The following are the default system-defined services and applications found in the PAM table.

Application	Port
cuseeme	7648
dns	53
exec	512
ftp	21
http	80
https	443
h323	1720
login	513
mgcp	2427
msrpc	135
netshow	1755
realmedia	7070
rtsp	554
rtsp	8554
shell	514
sip	5060
skinny	2000
smtp	25
sql-net	1521
streamworks	1558
sunrpc	111
telnet	23
tftp	69
vdolive	7000

The following services and applications are not defined by default in the router PAM table, but may be defined by the system administrator:

■ Finger

■ Gopher

■ IMAP

■ Kerberos

■ LDAP

■ Lotusnote

■ MS-SQL

- NFS
- NNTP
- POP2
- POP3
- SAP
- SNMP
- Sybase-SQL
- TACACS

User-Defined Port Mapping

Router(config)#

```
ip port-map appl_name port port_num
```

- **Maps a port number to an application**

Router(config)#

```
access-list permit acl_num ip_addr
ip port-map appl_name port port_num list acl_num
```

- **Maps a port number to an application for a given host**

Router(config)#

```
access-list permit acl_num ip_addr wildcard_mask
ip port-map appl_name port port_num list acl_num
```

- **Maps a port number to an application for a given network**

SECUR 1.1—6-24

Network services or applications that use nonstandard ports require user-defined entries in the PAM table. For example, your network might run HTTP services on the nonstandard port 8000 instead of on the system-defined default port 80. In this case, you can use PAM to map port 8000 with HTTP services. If HTTP services run on other ports, use PAM to create additional port mapping entries. After you define a port mapping entry, you can overwrite that entry at a later time by simply mapping that specific port with a different application.

| **Note** | If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict. |

User-defined port mapping information can also specify a range of ports for an application by establishing a separate entry in the PAM table for each port number in the range.

User-defined entries are saved with the default mapping information when you save the router configuration.

Use the **ip port-map** configuration command to establish PAM. Use the **no** form of this command to delete user-defined PAM entries.

The syntax for the **ip port-map** command is as follows:

ip port-map *appl_name* **port** *port_num* **[list** *acl_num***]**

appl_name	Specifies the name of the application with which to apply the port mapping.
port *port_num*	Identifies a port number in the range 1 to 65535.
list *acl_num*	Identifies the standard ACL number used with PAM for host- or network-specific port mapping.

User-defined entries in the mapping table can include host- or network-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet.

With host-specific port mapping, you can use the same port number for different services on different hosts. This means that you can map port 8000 with HTTP services for one host, while mapping port 8000 with Telnet services for another host.

Host-specific port mapping also enables you to apply PAM to a specific subnet when that subnet runs a service that uses a port number that is different from the port number defined in the default mapping information. For example, hosts on subnet 192.168.0.0 might run HTTP services on nonstandard port 8000, while other traffic through the firewall uses the default port 80 for HTTP services.

Host- or network-specific port mapping enables you to override a system-defined entry in the PAM table. For example, if CBAC finds an entry in the PAM table that maps port 25 (the system-defined port for SMTP) with HTTP for a specific host, CBAC identifies port 25 as HTTP protocol traffic on that host.

Note	If the host-specific port mapping information is the same as existing system- or user-defined default entries, host-specific port changes have no effect.

Use the **list** option for the **ip port-map** command to specify an ACL for a host or subnet that uses PAM.

Display PAM Configuration

Router#

```
show ip port-map
```

• **Shows all port mapping information**

Router#

```
show ip port-map appl_name
```

• **Shows port mapping information for a given application**

Router#

```
show ip port-map port port_num
```

• **Shows port mapping information for a given application on a given port**

```
Router# sh ip port-map ftp
Default mapping: ftp port 21   system defined
Host specific:   ftp port 1000 in list 10 user
```

SECUR 1.1—6-25

Use the **show ip port-map** privileged EXEC command to display the PAM information.

The syntax for the **show ip port-map** command is as follows:

show ip port-map [*appl_name* | port *port_num*]

appl_name	Specifies the application for which to display information.
port *port_num*	Specifies the alternative port number that maps to the application for which to display information.

Define Inspection Rules

This topic discusses how to configure the rules used to define the application protocols for inspection.

Inspection Rules for Application Protocols

Cisco.com

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: tcp, udp, cuseeme, ftp, http, h323, netshow, rcmd, realaudio, rpc, smtp, sqlnet, streamworks, tftp, and vdolive**
  – **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
```

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—6-27

Inspection rules must be defined to specify what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface. Normally, you define only one inspection rule. The only exception might occur if you want to enable CBAC 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, as well as generic TCP or generic UDP, if desired. 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.

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.

The syntax for the **ip inspect name** command is as follows:

ip inspect name *inspection-name protocol* [alert {on | off}] [audit-trail {on | off}] [timeout *seconds*]

no ip inspect name *inspection-name protocol*

no ip inspect name

name *inspection-name*	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name*.
protocol	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, **audit-trail** 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 *seconds*	(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 UPD timeouts, but will not override the global DNS timeout.

Inspection Rules for Java

Router(config)#

```
ip inspect name inspection-name http java-list
  acl-num [alert {on|off}] [audit-trail {on|off}]
  [timeout seconds]
```

- **Controls java blocking with a standard ACL**

```
Router(config)# ip access-list 10 deny 172.26.26.0
  0.0.0.255
Router(config)# ip access-list 10 permit 172.27.27.0
  0.0.0.255
Router(config)# ip inspect name FWRULE http java-list
  10 alert on audit-trail on timeout 300
```

SECUR 1.1—6-28

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as friendly. If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except for sites specifically designated as hostile.

Note	If you do not configure an ACL, but use a "placeholder" ACL in the **ip inspect name inspection-name http** command, all Java applets will be blocked.

Note	CBAC does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are not blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

The syntax for the **ip inspect name** command for Java applet filtering inspection is as follows:

ip inspect name *inspection-name* **http java-list acl-num [alert {on | off}] [audit-trail {on | off}] [timeout** *seconds***]**

no ip inspect name *inspection-name* **http**

name *inspection-name*	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name* as the existing set of rules.
http	Specifies the HTTP protocol used.
java-list *acl-num*	Specifies the ACL (name or number) to use to determine "friendly" sites. This keyword is available only for the HTTP protocol for Java applet blocking. Java blocking only works with standard ACLs.

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, **audit-trail** 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 *seconds*	(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 UPD timeouts, but will not override the global DNS timeout.

Inspection Rules for RPC Applications

Router(config)#

```
ip inspect name inspection-name rpc
  program-number number [wait-time minutes]
  [alert {on|off}] [audit-trail {on|off}]
  [timeout seconds]
```

• **Allows given RPC program numbers—wait-time keeps the connection open for a specified number of minutes**

```
Router(config)# ip inspect name FWRULE rpc
  program-number 100022 wait-time 0 alert off
  audit-trail on
```

Remote Procedure Call (RPC) inspection enables the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you create an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

The syntax of the **ip inspect name** command for RPC applications is as follows:

ip inspect name *inspection-name* **rpc program-number** *number* **[wait-time** *minutes*] **[alert {on | off}] [audit-trail {on | off}] [timeout** *seconds*]

no ip inspect name inspection-name protocol

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same ***inspection-name*** as the existing set of rules.
rpc program_number *number*	Specifies the program number to permit.
wait-time *minutes*	(Optional.) Specifies the number of minutes to keep the connection opened in the firewall, even after the application terminates, allowing subsequent connections from the same source address and to the same destination address and port. The default **wait-time** is zero minutes.
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, **audit-trail** 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 *seconds*	(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 UPD timeouts, but will not override the global DNS timeout.

Router(config)#

```
ip inspect name inspection-name smtp [alert
 {on|off}] [audit-trail {on|off}] [timeout
 seconds]
```

- **Allows only the following legal commands in SMTP applications: DATA, EXPN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY**
- **If disabled, all SMTP commands are allowed through the firewall, and potential mail server vulnerabilities are exposed**

```
Router(config)# ip inspect name FWRULE smtp
```

SECUR 1.1—6-30

SMTP inspection causes SMTP commands to be inspected for illegal commands. Any packets with illegal commands are dropped, and the SMTP session hangs and eventually times out. An illegal command is any command except for the following legal commands: DATA, EXPN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY.

The syntax for the **ip inspect name** command for SMTP application inspection is as follows:

ip inspect name *inspection-name* smtp [alert {on | off}] [audit-trail {on | off}] [timeout *seconds*]

no ip inspect name *inspection-name* smtp

name *inspection-name*	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name* as the existing set of rules.
smtp	Specifies the SMTP protocol for inspection.
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, **audit-trail** 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 *seconds*	(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 DNS timeout.

Inspection Rules for IP Packet Fragmentation

Router(config)#

```
ip inspect name inspection-name fragment max
  number timeout seconds
```

- **Protects hosts from certain DoS attacks involving fragmented IP packets**
  - **max—number of unassembled fragmented IP packets**
  - **timeout—seconds when the unassembled fragmented IP packets begin to be discarded**

```
Router(config)# ip inspect name FWRULE
  fragment max 254 timeout 4
```

SECUR 1.1—6-31

CBAC inspection rules can help protect hosts against certain DoS attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many noninitial IP fragments, or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an interfragment state (structure) for IP traffic. Noninitial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Noninitial fragments received before the corresponding initial fragments are discarded.

Note	Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** (global) command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

The syntax of the **ip inspect name** command for IP packet fragmentation is as follows:

ip inspect name *inspection-name* **fragment max** *number* **timeout** *seconds*

no ip inspect name *inspection-name* **fragment**

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same ***inspection-name*** as the existing set of rules.
fragment	Specifies fragment inspection for the named rule.
max *number*	Specifies the maximum number of unassembled packets for which state information (structures) is allocated by the software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries. Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.
timeout *seconds*	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is one second. If this number is set to a value greater than one second, it will be automatically adjusted by the software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2; when the number of free states is less than 16, the timeout will be set to 1 second.

Inspection Rules for ICMP

Router(config)#

```
ip inspect name inspection-name icmp [alert
 {on|off}] [audit-trail {on|off}] [timeout
 seconds]
```

- **Configures IOS Firewall to use stateful inspection to "trust" ICMP packets that are generated within a private network and to permit the associated ICMP replies**
- **Allows network administrators to troubleshoot the network using "trusted" ICMP packets while blocking other potentially malicious ICMP packets**

```
Router(config)# ip inspect name checkICMP icmp
 alert on audit-trail on timeout 30
```

SECUR 1.1—6-32

While ICMP is a very useful tool for debugging network connectivity issues, it can also be used by intruders to map private networks. Armed with the information provided by ICMP replies, intruders may attempt targeted attacks on critical network resources. For this reason, many network administrators configure their routers and firewalls to block all ICMP packets from entering the private network. The downside to blocking all ICMP packets is that, while it keeps intruders from using ICMP, it also takes away a valuable network troubleshooting tool.

Cisco routers using IOS releases 12.2(11)YU and greater with the IOS Firewall feature set, contain the ability to perform stateful inspection of ICMP packets. This feature enables the router to "trust" ICMP packets generated from inside the private network (and permit their associated replies) while blocking other possibly malicious ICMP packets.

Although Cisco IOS routers can be configured to selectively allow certain ICMP packets through the router, the network administrator must still determine which messages are potentially malicious and which are not.

Stateful inspection of ICMP packets is limited to the most common types of ICMP messages used by network administrators to debug network connectivity issues. ICMP messages that do not provide useful troubleshooting services will not be allowed. The following table identifies the IOS Firewall-supported ICMP packet types.

Note   Stateful inspection of ICMP messages does not work for UDP traceroute, where UDP datagrams are sent instead of ICMP packets. The UDP traceroute is typically the default for UNIX systems. To use ICMP inspection with a UNIX host, use the "I" option with the **traceroute** command. This option will cause the UNIX host to generate ICMP traceroute packets, which will then be inspected by the ICMP stateful inspection function.

The following table lists the ICMP packet types that are supported by CBAC:

ICMP Packet Type	Name	Description
0	Echo Reply	Reply to Echo Request (Type 8)
3	Destination Unreachable	Possible reply to any request (this packet is included because it is a possible response to any ICMP packet request)
8	Echo Request	Ping or traceroute request
11	Time Exceeded	Reply to any request if the time-to-live (TTL) packet is 0
13	Timestamp Request	Request
14	Timestamp Reply	Reply to Timestamp Request (Type 13)

ICMP packet types 0 and 8 are used for pinging where the source sends out an Echo Request packet, and the destination responds with an Echo Reply packet. ICMP packet types 0, 8, and 11 are used for ICMP traceroute where Echo Request packets are sent out starting with a time-to-live (TTL) packet of 1, and the TTL is incremented for each hop. The intermediate hops respond to the Echo Request packet with a Time Exceeded packet; the final destination responds with an Echo Reply packet.

ICMP stateful inspection is explicitly enabled using the **ip inspect name** *inspection-name* **icmp** (global) command as shown in the figure.

The syntax of the **ip inspect name** *inspection-name* **icmp** command for ICMP packet inspection is as follows:

ip inspect name *inspection-name* **icmp [alert {on|off}] [audit-trail {on|off}] [timeout** *seconds***]**

no ip inspect *inspection-name* **icmp**

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name* as the existing set of rules. The inspection-name cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.
icmp	Specifies ICMP inspection for the named rule.
alert {on|off}	(Optional.) For ICMP inspection, the generation of alert messages can be set to **on** or **off**. If no option is selected, alerts are generated on the basis of the setting of the **ip inspect alert-off** command.
audit-trail {on|off}	(Optional.) For ICMP inspection, audit trail can be set **on** or **off**. If no option is selected, audit trail messages are generated on the basis of the setting of the **ip inspect audit-trail** command.
timeout *seconds*	(Optional.) Specifies the number of seconds for an ICMP idle timeout.

The following example shows a portion of a Cisco IOS Firewall router configuration detailing stateful inspection of ICMP packets. Note that it is important to assign the new ICMP inspection rule to a router interface. In this example the inspection rule has been assigned to interface Ethernet0:

```
!
!
ip inspect audit-trail
ip inspect name checkICMP icmp alert on audit-trail on timeout 30
!
interface Ethernet0
 ip address 192.168.10.2 255.255.255.0
 ip inspect checkICMP
!
interface Ethernet1
 ip address 192.168.20.2 255.255.255.0
 ip access-group 101 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.20.3
no ip http server
!
access-list 101 deny ip any any
!
```

The following example is sample output from the **show ip access-list** command. In this example, Dynamic ACLs are created for an ICMP session on which only ping packets were issued from the host:

```
Router# show ip access-list 101
Extended IP access list 101
Permit icmp any host 192.168.133.3 time-exceeded
Permit icmp any host 192.168.133.3 unreachable
Permit icmp any host 192.168.133.3 timestamp-reply
Permit icmp any host 192.168.133.3 echo-reply (4 matches)
```

ICMP inspection sessions are based on the source address of the inside host that originates the ICMP packet. Dynamic ACLs are created for return ICMP packets of the allowed types (echo-reply, time-exceeded, destination unreachable, and timestamp reply) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card address is used because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

Inspection Rules and ACLs Applied to Router Interfaces

This topic discusses the application of inspection rules and ACLs to router interfaces.

Apply an Inspection Rule to an Interface

Cisco.com

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**

SECUR 1.1—6-34

Use the **ip inspect** interface configuration command to apply a set of inspection rules to an interface. Use the **no** form of this command to remove the set of rules from the interface.

The syntax for the **ip inspect** command is as follows:

ip inspect *inspection-name* {**in** | **out** }

no ip inspect inspection-name {in | out}

inspection-name	Names the set of inspection rules.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

General Rules for Applying Inspection Rules and ACLs

Cisco.com

- **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.**
- **All other interfaces**
  - **Apply ACL on the inward direction that denies all unwanted traffic.**

SECUR 1.1—6-35

For the Cisco IOS Firewall to be effective, both inspection rules and ACLs must be strategically applied to all the router's interfaces. The following is the general rule of thumb for applying inspection rules and ACLs on the router:

■ On the interface where traffic initiates

— Apply the ACL on the inward direction that only permits wanted traffic.

— Apply the rule on the inward direction that inspects wanted traffic.

■ On all other interfaces apply the ACL on the inward direction that denies all traffic, except traffic (such as ICMP) not inspected by CBAC.

Example—Two-Interface Firewall

Outbound
- Allow all general TCP and UDP traffic
- Allow all ICMP traffic
- Deny everything else

10.0.0.0

Inside
e0/0

Outside
e0/1

Internet

10.0.0.3

Inbound
- Allow all ICMP and HTTP traffic only to 10.0.0.3
- Deny everything else

SECUR 1.1—6-36
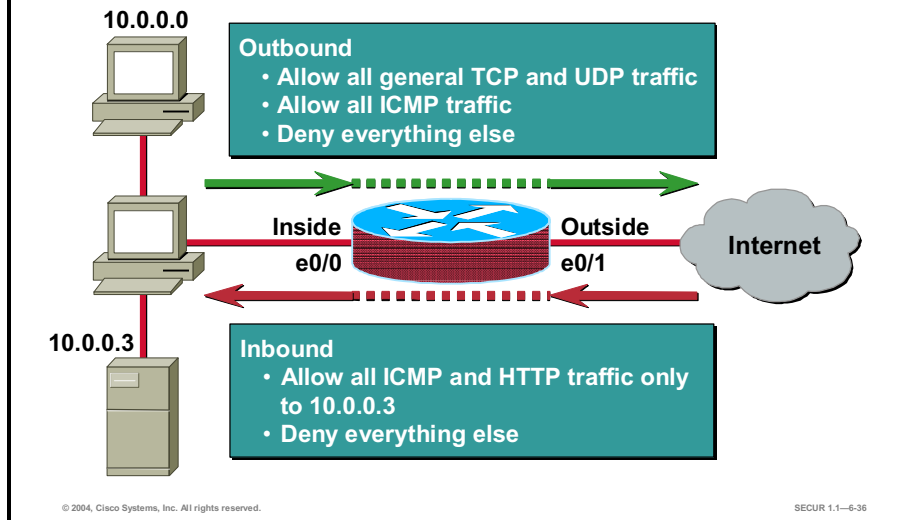
As an example, configure the router to be a firewall between two networks: inside and outside. The following is the security policy to implement: allow all general TCP and UDP traffic initiated on the inside (outbound) from network 10.0.0.0 to access the Internet. ICMP traffic will also be allowed from the same network. Other networks on the inside, which are not defined, must be denied. For traffic initiated on the outside (inbound), allow everyone to access only ICMP and HTTP to host 10.0.0.3. Any other traffic not initiated from the inside must be denied.

Outbound Traffic

Inside   Outside

e0/0   e0/1

```
Router(config)# ip inspect name OUTBOUND tcp
Router(config)# ip inspect name OUTBOUND udp
Router(config)# ip inspect name OUTBOUND icmp
```
• **Configures CBAC to inspect TCP, UDP, and ICMP traffic**

```
Router(config)# access-list 101 permit ip 10.0.0.0
  0.0.0.255 any
Router(config)# access-list 101 deny ip any any
```
• **Permits inside-initiated traffic from the 10.0.0.0 network**

```
Router(config)# interface e0/0
Router(config-if)# ip inspect OUTBOUND in
Router(config-if)# ip access-group 101 in
```
• **Applies an ACL and inspection rule to the inside interface in an inward direction**

Complete the following steps to implement the security policy of the previous example for outbound traffic:

Step 1   Write a rule to inspect TCP and UDP traffic:

Router(config)# **ip inspect name OUTBOUND tcp**

Router(config)# **ip inspect name OUTBOUND udp**

Router(config)# **ip inspect name OUTBOUND icmp**

Step 2   Write an ACL that permits IP traffic from the 10.0.0.0 network to any destination:

Router(config)# **access-list 101 permit ip 10.0.0.0 0.0.0.255 any**

Router(config)# **access-list 101 deny ip any any**

Step 3   Apply the inspection rule and ACL to the inside interface on the inward direction:

Router(config)# **interface e0/0**

Router(config-if)# **ip inspect OUTBOUND in**

Router(config-if)# **ip access-group 101 in**

Inside   **Outside**

e0/0   **e0/1**

```
Router(config)# access-list 102 permit icmp any
  host 10.0.0.3
Router(config)# access-list 102 permit tcp any host
  10.0.0.3 eq www
Router(config)# access-list 102 deny ip any any
```

• **Permits outside-initiated ICMP and HTTP traffic to host 10.0.0.3.**

```
Router(config)# interface e0/1
Router(config-if)# ip access-group 102 in
```

• **Applies an ACL to outside interface in inward direction.**

Complete the following steps to implement the security policy of the previous example for inbound traffic:

Step 1   Write an ACL that permits only ICMP and HTTP traffic from the Internet to the 10.0.0.3 host:

```
Router(config)# access-list 102 permit icmp any host 10.0.0.3
Router(config)# access-list 102 permit tcp any host 10.0.0.3 eq www
Router(config)# access-list 102 deny ip any any
```

Step 2   Apply the inspection rule and ACL to the outside interface in the inward direction:

```
Router(config)# interface e0/1
Router(config-if)# ip access-group 102 in
```

Example—Three-Interface Firewall

Cisco.com

10.0.0.0

Outbound
- Allow all general TCP and UDP traffic
- Allow all ICMP traffic
- Deny everything else

Inside
e0/0

Outside
e0/1

Internet

DMZ e1/0

172.16.0.2

DMZ-bound
- Allow all ICMP and HTTP traffic only to 172.16.0.2
- Deny everything else
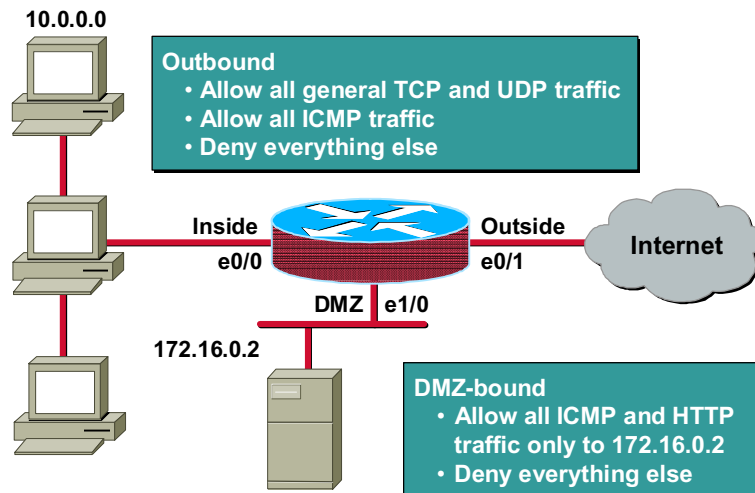
SECUR 1.1—6-39

As an example, configure the router to be a firewall between three networks: inside, outside, and DMZ. The following is the security policy to implement: allow all general TCP and UDP traffic initiated on the inside (outbound) from network 10.0.0.0 to access the Internet and the DMZ host 172.16.0.2. ICMP traffic will also be allowed from the same network to the Internet and the DMZ host. Other networks on the inside, which are not defined, must be denied. For traffic initiated on the outside (inbound) allow everyone to only access ICMP and HTTP to DMZ host 172.16.0.2. Any other traffic not initiated from the inside must be denied.

Outbound Traffic

Inside   Outside

e0/0   e0/1

DMZ e1/0

```
Router(config)# ip inspect name OUTBOUND tcp
Router(config)# ip inspect name OUTBOUND udp
Router(config)# ip inspect name OUTBOUND icmp
```

- **Configures CBAC to inspect TCP, UDP, and ICMP traffic**

```
Router(config)# access-list 101 permit ip 10.0.0.0
  0.0.0.255 any
Router(config)# access-list 101 deny ip any any
```

- **Permits inside-initiated traffic from 10.0.0.0 network**

```
Router(config)# interface e0/0
Router(config-if)# ip inspect OUTBOUND in
Router(config-if)# ip access-group 101 in
```

- **Applies an ACL and inspection rule to the inside interface in an inward direction**

SECUR 1.1—6-40

Complete the following steps to implement the security policy of the previous example for outbound traffic:

Step 1 Write a rule to inspect TCP and UDP traffic:

```
Router(config)# ip inspect name OUTBOUND tcp
Router(config)# ip inspect name OUTBOUND udp
Router(config)# ip inspect name OUTBOUND icmp
```

Step 2 Write an ACL that permits IP traffic from the 10.0.0.0 network to any destination:

```
Router(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255 any
Router(config)# access-list 101 deny ip any any
```

Step 3 Apply the inspection rule and ACL to the inside interface in the inward direction:

```
Router(config)# interface e0/0
Router(config-if)# ip inspect OUTBOUND in
Router(config-if)# ip access-group 101 in
```

Inbound Traffic

Cisco.com

Inside / Outside
e0/0 / e0/1
DMZ | e1/0

```
Router(config)# ip inspect name INBOUND tcp
```
• **Configures CBAC to inspect TCP traffic**

```
Router(config)# access-list 102 permit icmp any host
  172.16.0.2
Router(config)# access-list 102 permit tcp any host
  172.16.0.2 eq www
Router(config)# access-list 102 deny ip any any
```
• **Permits outside-initiated ICMP and HTTP traffic to host 172.16.0.2**

```
Router(config)# interface e0/1
Router(config-if)# ip inspect INBOUND in
Router(config-if)# ip access-group 102 in
```
• **Applies an ACL and inspection rule to the outside interface in an inward direction**

© 2004, Cisco Systems, Inc. All rights reserved. SECUR 1.1—6-41

Complete the following steps to implement the security policy of the previous example for inbound traffic:

Step 1   Write a rule to inspect TCP traffic:

```
Router(config)# ip inspect name INBOUND tcp
```

Step 2   Write an ACL that permits only ICMP and HTTP traffic from the Internet to the 172.16.0.2 host:

```
Router(config)# access-list 102 permit icmp any host 172.16.0.2
Router(config)# access-list 102 permit tcp any host 172.16.0.2 eq www
Router(config)# access-list 102 deny ip any any
```

Step 3   Apply the inspection rule and ACL to the outside interface in the inward direction:

```
Router(config)# interface e0/1
Router(config-if)# ip inspect INBOUND in
Router(config-if)# ip access-group 102 in
```

DMZ-Bound Traffic

Inside   **Outside**

e0/0   e0/1

DMZ | e1/0

```
Router(config)# access-list 103 permit icmp host 172.16.0.2 any
Router(config)# access-list 103 deny ip any any
```

• **Permits only ICMP traffic initiated in the DMZ**

```
Router(config)# access-list 104 permit icmp any host 172.16.0.2
Router(config)# access-list 104 permit tcp any host 172.16.0.2
  eq www
Router(config)# access-list 104 deny ip any any
```

• **Permits only outward ICMP and HTTP traffic to host 172.16.0.2**

```
Router(config)# interface e1/0
Router(config-if)# ip access-group 103 in
Router(config-if)# ip access-group 104 out
```

• **Applies proper access lists to the interface**

   SECUR 1.1—6-42

Complete the following steps to implement the security policy of the previous example for inbound traffic:

Step 1   Write an ACL to permit only ICMP traffic to initiate from the DMZ host:

Router(config)# **access-list 103 permit icmp host 172.16.0.2 any**

Router(config)# **access-list 103 deny ip any any**

Step 2   Write an ACL that permits only ICMP and HTTP traffic from any network to the 172.16.0.2 host:

Router(config)# **access-list 104 permit icmp any host 172.16.0.2**

Router(config)# **access-list 104 permit tcp any host 172.16.0.2 eq www**

Router(config)# **access-list 104 deny ip any any**

Step 3   Apply the ACLs to the DMZ interface:

Router(config)# **interface e1/0**

Router(config-if)# **ip access-group 103 in**

Router(config-if)# **ip access-group 104 out**

Test and Verify

This topic discusses the commands available to help test and verify CBAC.

show Commands

Router#

```
show ip inspect name inspection-name
show ip inspect config
show ip inspect interfaces
show ip inspect session [detail]
show ip inspect all
```

• **Displays CBAC configurations, interface configurations, and sessions**

```
Router# sh 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
```

SECUR 1.1—6-44

The syntax for the **show ip inspect** command is as follows:

show ip inspect name *inspection-name* | **config** | **interfaces** | **session [detail]** | **all**

inspection-name	Shows the configured inspection rule for *inspection-name*.
config	Shows the complete CBAC inspection configuration.
interfaces	Shows interface configuration with respect to applied inspection rules and ACLs.
session [detail]	Shows existing sessions that are currently being tracked and inspected by CBAC. The optional **detail** keyword shows additional details about these sessions.
all	Shows the complete CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

debug Commands

```
Router#

debug ip inspect function-trace
debug ip inspect object-creation
debug ip inspect object-deletion
debug ip inspect events
debug ip inspect timers
```

- **General debug commands**

```
Router(config)#

debug ip inspect protocol
```

- **Protocol-specific debug**

SECUR 1.1—6-45

Use the **debug ip inspect** EXEC command to display messages about CBAC events. The **no** form of this command disables debugging output.

The syntax for the **debug ip inspect** command is as follows:

debug ip inspect {function-trace | object-creation | object-deletion | events | timers |*protocol* | detailed}

no debug ip inspect

function-trace	Displays messages about software functions called by CBAC.
object-creation	Displays messages about software objects being created by CBAC. Object creation corresponds to the beginning of CBAC-inspected sessions.
object-deletion	Displays messages about software objects being deleted by CBAC. Object deletion corresponds to the closing of CBAC-inspected sessions.
events	Displays messages about CBAC software events, including information about CBAC packet processing.
timers	Displays messages about CBAC timer events, such as when a CBAC idle timeout is reached.
protocol	Displays messages about CBAC-inspected protocol events, including details about the protocol's packets.
detailed	Use this form of the command in conjunction with other CBAC debugging commands. This displays detailed information for all other enabled CBAC debugging.

Remove CBAC Configuration

Router(config)#

```
no ip inspect
```

- **Removes entire CBAC configuration**
- **Resets all global timeouts and thresholds to the defaults**
- **Deletes all existing sessions**
- **Removes all associated dynamic ACLs**

Use the **no ip inspect** command to remove the entire CBAC configuration, reset all global timeouts and thresholds to their defaults, delete all existing sessions, and remove all associated dynamic ACLs. This command has no other arguments, keywords, default behavior, or values.

Summary

This topic summarizes what you learned in this lesson.

Lab Exercise—Configure Cisco IOS Firewall CBAC on a Cisco Router

Complete the following lab exercise to practice what you learned in this lesson.

Objectives

In this lab exercise you will configure Context-Based Access Control (CBAC) on a Cisco router with a partner by completing the following tasks:

- Complete the lab exercise setup.

- Configure logging and audit trails.

- Define and apply inspection rules and ACLs.

- Test and verify CBAC.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.

Lab Visual Objective

Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1 Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2 Configure your student PC for IP address 10.0.P.12 with a default gateway of 10.0.P.2 (where P = pod number).

Step 3 Make sure that your student PC has an appropriate Syslog server application installed (for example; Kiwi's Syslog Daemon).

Step 4 Reload your perimeter router using the default lab configuration.

Step 5 Ensure you can ping the peer router and network hosts before beginning.

Step 6 Make sure that your router is running the correct date and time.

Step 7 Make sure that your student PC is running the correct date and time.

Task 2—Configure Logging and Audit Trails

Complete the following steps to configure logging and auditing trails:

Step 1 Log into your perimeter router and access global configuration mode.

Step 2 On your router, enable logging to the console and the Syslog server.

```
RP(config)# logging on
```

```
RP(config)# logging 10.0.P.12
```

(where P = pod number)

Step 3 Enable the audit trail:

```
RP(config)# ip inspect audit-trail
```

Step 4 Save your configuration and return to global configuration mode:

```
RP(config)# end
RP# copy run start
```

Task 3—Define and Apply Inspection Rules and ACLs

Complete the following steps to define and apply inspection rules and Access Control Lists (ACLs):

Step 1 Enter global configuration mode on your perimeter router.

Step 2 On your router, define a CBAC rule to inspect all TCP and FTP traffic.

```
RP(config)# ip inspect name FWRULE tcp timeout 300
RP(config)# ip inspect name FWRULE ftp timeout 300
```

Step 3 Define the ACLs to allow outbound ICMP traffic and CBAC traffic (FTP and WWW). Block all other inside-initiated traffic.

```
RP(config)# access-list 103 permit icmp any any
RP(config)# access-list 103 permit tcp 10.0.P.0 0.0.0.255 any eq ftp
RP(config)# access-list 103 permit tcp 10.0.P.0 0.0.0.255 any eq www
RP(config)# access-list 103 deny ip any any
```

(where P = pod number)

Step 4 Define ACLs to allow inbound ICMP traffic and CBAC traffic (FTP and WWW) to the inside web or FTP server. Block all other outside-initiated traffic.

```
RP(config)# access-list 104 permit eigrp any any
RP(config)# access-list 104 permit icmp any any
RP(config)# access-list 104 deny ip any any
```

(where P = pod number)

Step 5 Apply the inspection rule and ACL to the inside interface:

```
RP(config)# interface fast 0/0
RP(config-if)# ip inspect FWRULE in
RP(config-if)# ip access-group 103 in
```

Step 6 Apply the ACL to the outside interface:

```
RP(config-if)# interface fast 0/1
RP(config-if)# ip access-group 104 in
```

Step 7 Save your configuration and return to global configuration mode:

```
RP(config-if)# end
```

```
RP# copy run start
```

Task 4—Test and Verify CBAC

Complete the following steps to test and verify CBAC:

Step 1   Check your ACLs:

```
RP# show access-lists
```

Step 2   Ping the backbone server from your PC's command prompt:

```
C:\> ping 172.26.26.50
Pinging 172.26.26.50 with 32 bytes of data:

Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
Reply from 172.26.26.50: bytes=32 time=34ms TTL=125
Reply from 172.26.26.50: bytes=32 time=36ms TTL=125
```

Step 3   Use your web browser to connect to the backbone web server. Enter **http://172.26.26.50** in the URL field.

Step 4   From the command prompt on your student PC, connect to the backbone FTP server using anonymous FTP:

```
C:\> ftp 172.26.26.50
...
User (10.0.P.12:(none)): anonymous
...
Password: user@
```

(where P = pod number)

Step 5   Display a directory listing to verify data channel connectivity:

```
ftp> ls
```

Step 6   On your router, use the following **show** command to view the new dynamic ACL entry added by the **ip inspect** statement in Task 3, Step 2:

```
RP# show access-lists
```

Step 7   On your router, use the following **show** commands to verify the CBAC operation:

```
RP# show ip inspect name FWRULE
RP# show ip inspect config
RP# show ip inspect interfaces
RP# show ip inspect sessions
RP# show ip inspect sessions detail
RP# show ip inspect all
```

Step 8   Ping your peer's inside server from your PC's command prompt:

```
C:\> ping 10.0.Q.12
```

```
Pinging 10.0.Q.12 with 32 bytes of data:


Reply from 10.0.Q.12: bytes=32 time=34ms TTL=125
Reply from 10.0.Q.12: bytes=32 time=34ms TTL=125
Reply from 10.0.Q.12: bytes=32 time=34ms TTL=125
Reply from 10.0.Q.12: bytes=32 time=36ms TTL=125
```

(where Q = peer pod number)

Step 9 Use your Web browser to connect to your peer's inside server. Enter **http://10.0.Q.12** in the URL field.

(where Q = peer pod number)

Step 10 Connect to your peer's FTP server using anonymous FTP.

```
C:\> ftp 10.0.Q.12

...
User (10.0.Q.12:(none)): anonymous

...
Password: user@
```

(where Q = peer pod number)

Step 11 On your router, use the following **show** commands to verify the CBAC operation:

```
RP# show ip inspect name FWRULE
RP# show ip inspect config
RP# show ip inspect interfaces
RP# show ip inspect sessions
RP# show ip inspect sessions detail
RP# show ip inspect all
```

7

Cisco IOS Firewall Authentication Proxy

Overview

This lesson includes the following topics:

- Objectives
- Introduction to the Cisco IOS Firewall authentication proxy
- AAA server configuration
- AAA configuration
- Authentication proxy configuration
- Test and verify the configuration
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- Define an authentication proxy.
- Describe how users authenticate to a Cisco IOS Firewall.
- Describe how authentication proxy technology works.
- Name the AAA protocols supported by the Cisco IOS Firewall.
- Configure AAA on a Cisco IOS Firewall.

SECUR 1.1—7-3

Introduction to the Cisco IOS Firewall Authentication Proxy

This topic introduces the features of the Cisco IOS Firewall authentication proxy.

What Is the Authentication Proxy?

- **HTTP, HTTPS, FTP, and Telnet authentication**
- **Provides dynamic, per-user authentication and authorization via TACACS+ and RADIUS protocols**
- **Once authenticated, all types of application traffic can be authorized**
- **Works on any interface type for inbound or outbound traffic**

SECUR 1.1—7-5

The Cisco IOS Firewall authentication proxy feature enables network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access were associated with a user's 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 their per-user policy, and access privileges can be tailored on an individual basis, as opposed to a general policy applied across multiple users.
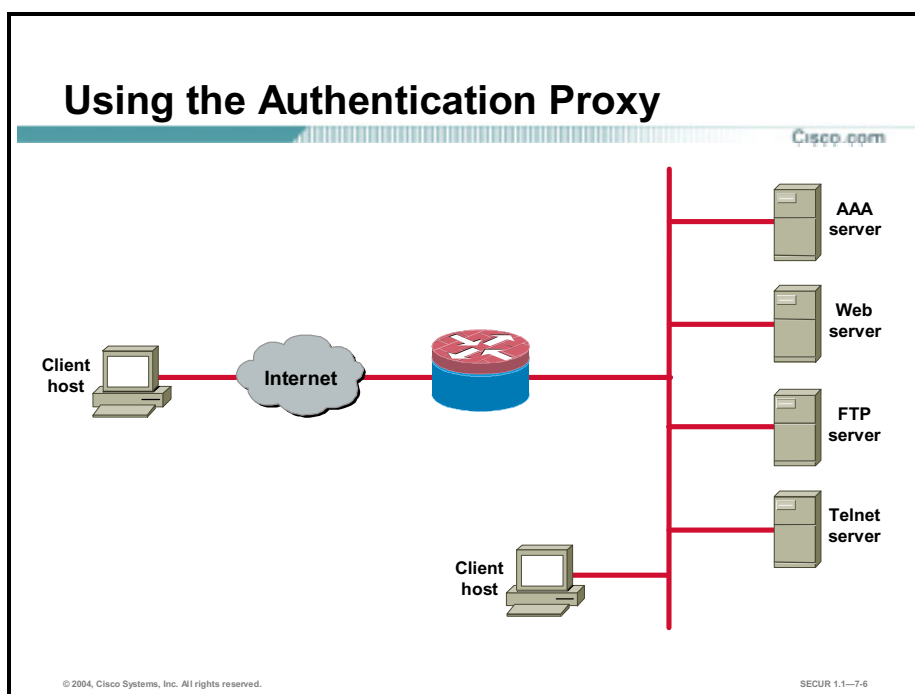
Using the Authentication Proxy

AAA server

Web server

FTP server

Telnet server

Client host

Internet

Client host

SECUR 1.1—7-6

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, HTTPS, FTP, or Telnet, and their specific access profiles are automatically retrieved and applied from a Cisco Secure Access Control Server (ACS) or other Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) authentication server. 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 Network Address Translation (NAT), Context-Based Access Control (CBAC), IPSec encryption, and Cisco Virtual Private Network (VPN) Client.

When a user initiates an HTTP, HTTPS, FTP, or Telnet session through the firewall, it triggers the authentication proxy. The authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the session is allowed and no further intervention is required by the authentication proxy. If no entry exists, the authentication proxy responds to the connection request by prompting the user for a username and password.

Users must successfully authenticate with the authentication server by entering a valid username and password. If the authentication succeeds, the user's authorization profile is retrieved from the authentication, authorization, and accounting (AAA) server. The authentication proxy uses the information in this profile to create dynamic access control entries (ACEs) and add them to the inbound (input) access control list (ACL) of an input interface, and to the outbound (output) ACL of an output interface if an output ACL exists at the interface. By doing this, the firewall allows authenticated users access to the network as permitted by the authorization profile.

If the authentication fails, the authentication proxy reports the failure to the user and prompts the user for a configurable number of retries.

The authentication proxy sets up an inactivity (idle) timer for each user profile. As long as there is activity through the firewall, new traffic initiated from the user's host does not trigger the authentication proxy, and all authorized user traffic is permitted access through the firewall.

If the idle timer expires, the authentication proxy removes the user's profile information and dynamic ACL entries. When this happens, traffic from the client host is blocked. The user must initiate another HTTP, HTTPS, FTP, or Telnet connection to trigger the authentication proxy.

Supported AAA Servers

Cisco.com

TACACS+

- Cisco Secure ACS NT/2000
- Cisco Secure ACS UNIX
- TACACS+ Freeware

RADIUS
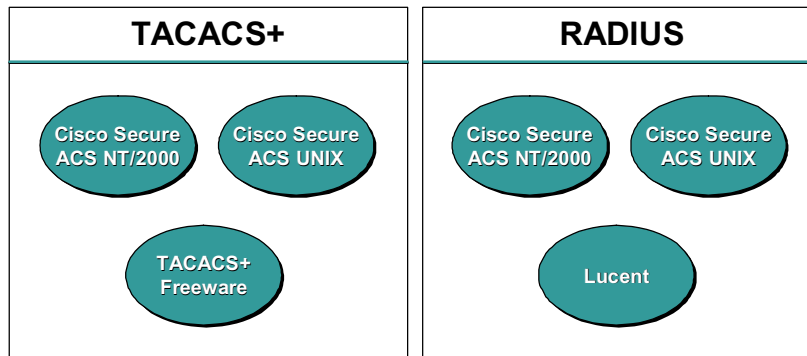
- Cisco Secure ACS NT/2000
- Cisco Secure ACS UNIX
- Lucent

SECUR 1.1—7-7

The Cisco IOS Firewall authentication proxy supports the following AAA protocols and servers:

- TACACS+

    — Cisco Secure ACS for Windows 2000 Server

    — Cisco Secure ACS for UNIX

    — TACACS+ Freeware

- RADIUS

    — Cisco Secure ACS for Windows 2000 Server

    — Cisco Secure ACS for UNIX

    — Lucent

    — Other standard RADIUS servers

Authentication Proxy Configuration

For inbound proxy authentication—Add an ACL to block inward traffic from the outside.

For outbound proxy authentication—Add an ACL to block inward traffic from the inside, except from the AAA server.

Web, FTP, or Telnet server

User

AAA server

Outside   Inside

User

For inbound proxy authentication—Enable the authentication proxy to intercept inward HTTP, HTTPS, FTP, or Telnet traffic from the outside.

For outbound proxy authentication—Enable the authentication proxy to intercept inward HTTP, HTTPS, FTP, or Telnet traffic from the inside.

SECUR 1.1—7-8

Apply the authentication proxy in the inward direction at any interface on the router where you want per-user authentication and authorization. Applying the authentication proxy inward at an interface causes it to intercept a user's initial connection request before that request is subjected to any other processing by the firewall. If the user fails to authenticate with the AAA server, the connection request is dropped.

How you apply the authentication proxy depends on your security policy. For example, you can block all traffic through an interface, and enable the authentication proxy feature to require authentication and authorization for all user-initiated HTTP, HTTPS, FTP, or Telnet connections. Users are authorized for services only after successful authentication with the AAA server. The authentication proxy feature also enables you to use standard ACLs to specify a host or group of hosts whose initial HTTP, HTTPS, FTP, or Telnet traffic triggers the proxy.

AAA Server Configuration

This topic discusses how to configure the AAA server to provide authentication and authorization for the Cisco IOS Firewall authorization proxy. This topic uses the Cisco Secure ACS for Windows Server (using the TACACS+ protocol) as an example of how to configure the AAA server.
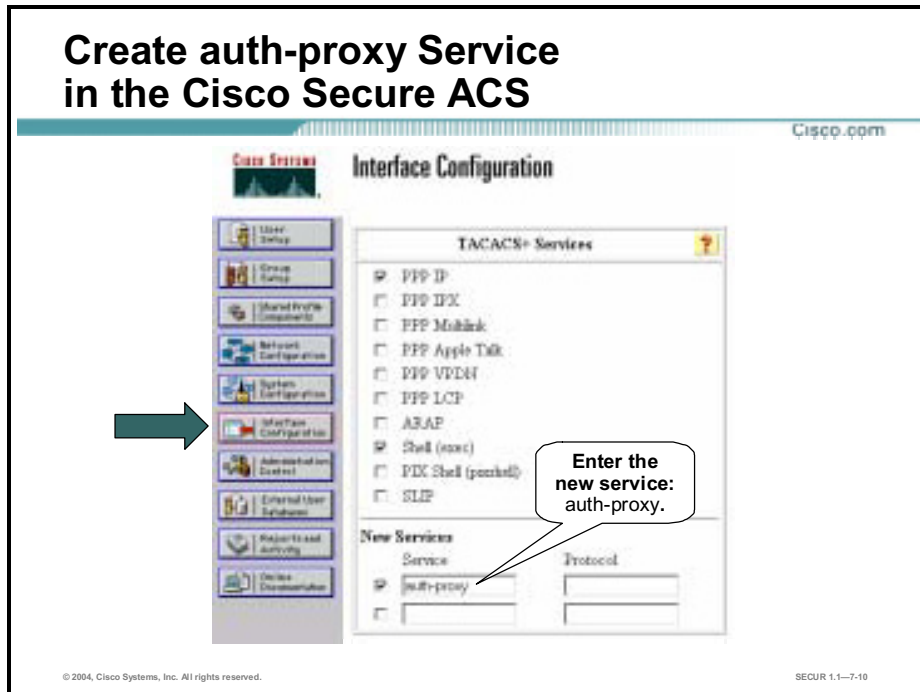
To support the authentication proxy, configure the AAA authorization **auth-proxy** service on the Cisco Secure ACS for Windows Server AAA server. This creates a new section in the Group Setup frame in which user profiles can be created. This does not interfere with other types of services that the AAA server may have. Complete the following steps to add authorization rules for specific services in the Cisco Secure ACS for Windows Server:

Step 1 In the navigation bar, click **Interface Configuration**. The Interface Configuration frame opens.

Step 2 Click **TACACS+ (Cisco IOS)**.

Step 3 Scroll down in the TACACS+ Services frame until you find the New Services group box.

Step 4 Select the check box closest to the service field.

Note	Depending on which options your Cisco Secure ACS is running, there may be one or two check boxes in front of the service fields. The presence of two check boxes indicates support for both user and group settings. Making check box selections simply indicates where the configuration of this feature can be performed; in other words, it can be done at group or user level or at both levels. If there is only one check box, then select it (as shown in the figure).

Step 5 Enter **auth-proxy** in the first empty Service field next to the check box you just selected and click **Submit**. For HTTP or HTTPS authentication, the corresponding Protocol field should be empty. For FTP and Telnet authentication, enter **ip** in the Protocol field.

Step 6 Scroll down to **Advanced Configuration Options** and select the **Advanced TACACS+ Features** check box, if it is not already selected.

Step 7 Click **Submit** when finished.

Create a User Authorization Profile in the Cisco Secure ACS

Cisco.com

Group Setup

Jump To [TACACS+]

Select auth-proxy.

Select Custom attributes.

Enter ACLs to apply after the user authenticates.

☑ auth-proxy

☑ Custom attributes

proxyacl#1=permit tcp any any priv-lvl=15

Enter the privilege level of the user; it must be 15 for all users.

SECUR 1.1—7-11
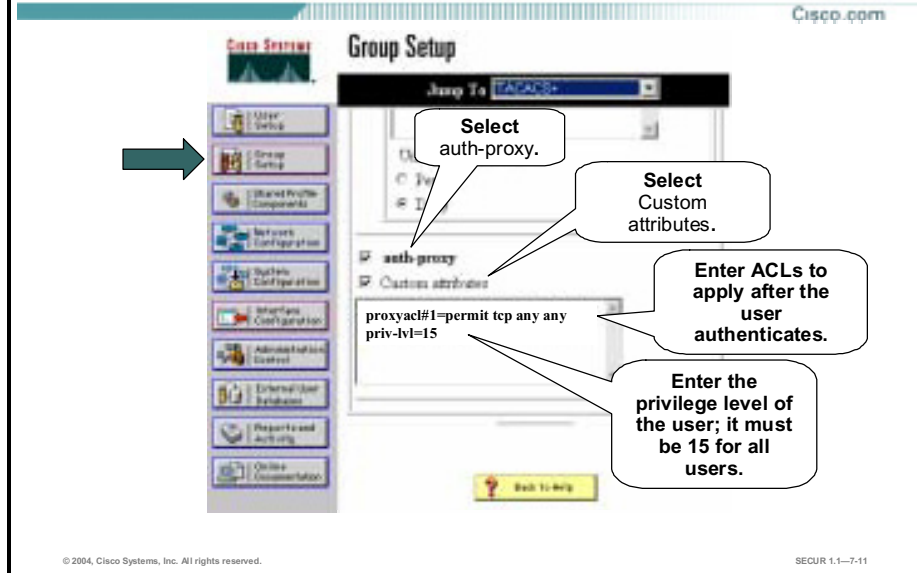
Step 8   In the navigation bar, click **Group Setup**. The Group Setup frame opens.

Step 9   Choose your group from the drop-down list and click **Edit Settings**.

Step 10   Scroll down in the Group Setup frame until you find the newly created auth-proxy service.

Step 11   Select the **auth-proxy** check box.

Step 12   Select the **Custom attributes** check box.

Step 13   Using the **proxyacl#***n* format described on the following page, enter ACLs in the field below the Custom attributes check box. These ACLs will be applied after the user authenticates.

Step 14   Enter the privilege level of the user (must be 15 for all users) using the format from the following page.

Step 15   Click **Submit** + **Restart** when finished.

User Authorization Profiles

```
proxyacl#n=permit protocol any {any | host ip_addr
 | ip_addr wildcard_mask} [eq auth_service]
```

- **Defines the allowable protocols, services, and destination addresses**
- **The source address is always** any **and is replaced in the router with the IP address of host making the request**

```
priv-lvl=15
```

- **Privilege level must be set to 15 for all users**

```
proxyacl#1=permit tcp  any any eq 26
proxyacl#2=permit icmp any host 172.30.0.50
proxyacl#3=permit tcp  any any eq ftp
proxyacl#4=permit tcp  any any eq smtp
proxyacl#5=permit tcp  any any eq telnet
priv-lvl=15
```

SECUR 1.1—7-12

Use the **proxyacl#n** attribute when configuring the ACLs in the profile. The **proxyacl#n** attribute is for both RADIUS and TACACS+ attribute-value pairs. The ACLs in the user profile on the AAA server must have **permit** access commands only. Set the source address to **any** in each of the user profile ACL entries. The source address in the ACLs is replaced with the source IP address of the host making the authentication proxy request when the user profile is downloaded to the firewall.

The syntax of the ACLs used to enter in the Custom attributes field is as follows:

proxyacl#n=permit *protocol* **any {any | host** *ip_addr* **|** *ip_addr wildcard_mask***} [eq** *auth_service***]**

protocol	Keyword indicating the protocol to allow users to access: **tcp**, **udp**, or **icmp**.
any	Indicates any hosts. The first **any** after *protocol* is mandatory. This indicates any source IP address, which is actually replaced with the IP address of the user that requests authorization in the ACL applied in the router.
host *ip_addr*	IP address of a specific host users can access.
ip_addr wildcard mask	IP address and wildcard mask for a network that users can access.
eq *auth_service*	Specific service that users are allowed to access.

Use **priv-lvl=15** to configure the privilege level of the authenticated user. The privilege level must be set to 15 for all users.

AAA Configuration

This topic discusses how to configure the Cisco IOS Firewall to work with an authentication, authorization, and accounting (AAA) server and enable the authentication proxy feature.

Enable AAA

Router(config)#

```
aaa new-model
```

- **Enables the AAA functionality on the router (default = disabled)**

SECUR 1.1—7-14

Use the **aaa new-model** global configuration command to enable the AAA access control system. Use the **no** form of this command to disable the AAA access control model.

Note   After you have enabled AAA, TACACS and extended TACACS commands are no longer available. If you initialize AAA functionality and later decide to use TACACS or extended TACACS, issue the **no** version of this command and then enable the version of TACACS that you want to use.

The syntax of the **aaa new-model** command is as follows:

aaa new-model

no aaa new-model

This command has no arguments.

By default, **aaa new-model** is not enabled.

Specify Authentication Protocols

Router(config)#

```
aaa authentication login default
 method1 [method2]
```

- **Defines the list of authentication methods that will be used**
- **Methods: TACACS+, RADIUS, or both**

```
Router(config)# aaa authentication
 login default group tacacs+
```

SECUR 1.1—7-15

To set AAA authentication, use the **aaa authentication login** global configuration command. Use the **no** form of this command to disable AAA authentication.

The syntax of the **aaa authentication login** command is as follows:

aaa authentication login default *method1* [*method2*]

no aaa authentication login default *method1* [*method2*]

method1, *method2*	The following are the authentication protocols to use: **group tacacs+**, **group radius**, or both.

Specify Authorization Protocols

Router(config)#

```
aaa authorization auth-proxy default method1
  [method2]
```

- **Use the auth-proxy keyword to enable authorization proxy for AAA methods**
- **Methods: TACACS+, RADIUS, or both**

```
Router(config)# aaa authorization auth-proxy
  default group tacacs+
```

To set AAA authorization, use the **aaa authorization auth-proxy** global configuration command. Use the **no** form of this command to disable AAA authorization.

The syntax of the **aaa authorization auth-proxy** command is as follows:

aaa authorization auth-proxy default *method1* [*method2*]

no aaa authorization auth-proxy default *method1* [*method2*]

method1, *method2*	The following are the authorization protocols to use: **group tacacs+**, **group radius**, or both.

Define a TACACS+ Server and Its Key

Router(config)#

```
tacacs-server host ip_addr
```

• **Specifies the TACACS+ server IP address**

Router(config)#

```
tacacs-server key string
```

• **Specifies the TACACS+ server key**

```
Router(config)# tacacs-server host 10.0.0.3
Router(config)# tacacs-server key secretkey
```

To specify the IP address of a TACACS+ server, use the **tacacs-server host** global configuration command. Use the **no** form of this command to delete the specified IP address. You can use multiple **tacacs-server host** commands to specify additional servers. The Cisco IOS Firewall software searches for servers in the order in which you specify them.

The syntax of the **tacacs-server host** command is as follows:

tacacs-server host *ip_addr*

no tacacs-server host *ip_addr*

ip_addr	IP address of the TACACS+ server.

To set the authentication encryption key used for all TACACS+ communications between the Cisco IOS Firewall router and the AAA server, use the **tacacs-server key** global configuration command. Use the **no** form of this command to disable the key.

Note	The key entered must match the key used on the AAA server. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

The syntax of the **tacacs-server key** command is as follows:

tacacs-server key *string*

no tacacs-server key *string*

string	Key used for authentication and encryption.

To specify the IP address of a RADIUS server, use the **radius-server host** global configuration command. Use the **no** form of this command to delete the specified IP address. You can use multiple **radius-server host** commands to specify additional servers. The Cisco IOS Firewall software searches for servers in the order in which you specify them.

The syntax of the **radius-server host** command is as follows:

radius-server host *ip_addr*

no radius-server host *ip_addr*

ip_addr	IP address of the RADIUS server.

To set the authentication encryption key used for all RADIUS communications between the Cisco IOS Firewall router and the AAA server, use the **radius-server key** global configuration command. Use the **no** form of this command to disable the key.

Note	The key entered must match the key used on the AAA server. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

The syntax of the **radius-server key** command is as follows:

radius-server key *string*

no radius-server key *string*

string	Key used for authentication and encryption.

Allow AAA Traffic to the Router

```
Router(config)# access-list 111 permit tcp host
  10.0.0.3 eq tacacs host 10.0.0.1
Router(config)# access-list 111 permit icmp any any
Router(config)# access-list 111 deny ip any any
Router(config)# interface ethernet0/0
Router(config-if)# ip access-group 111 in
```

- **Create an ACL to permit TACACS+ traffic from the AAA server to the firewall**
  - **Source address = AAA server**
  - **Destination address = interface where the AAA server resides**
- **May want to permit ICMP**
- **Deny all other traffic**
- **Apply the ACL to the interface on the side where the AAA server resides**

All traffic requiring authentication and authorization should be denied by the router using extended ACLs. Upon successful authentication, dynamic ACEs will be inserted into the ACLs to permit only the traffic authorized by the user's profile. The authentication proxy customizes each of the ACEs in the user profile by replacing the source IP addresses in the downloaded ACL with the source IP address of the authenticated host.

An extended ACL should be applied to the inbound direction of the interface that is configured for proxy authentication. All other ACLs that restrict traffic in the direction of authenticated traffic flow should be extended ACLs so that proxy authentication can dynamically update the ACEs as necessary to permit authorized traffic to pass.

Note	Proxy authentication does not update ACLs blocking return traffic. If traffic in the opposite direction must be restricted, then use static ACLs to manually permit return traffic for authorized traffic. Preferably, use CBAC to dynamically create ACLs to securely permit return traffic for proxy-authenticated sessions.

If the AAA server resides on the same interface where proxy authentication is configured, then you need to configure and apply an ACL to permit TACACS+ or RADIUS traffic from the AAA server to the firewall.

Use the following guidelines when writing the extended ACL:

- To permit AAA server communication, create an ACE where the source address is the AAA server and destination address is the interface where the AAA server resides.

- You may want to permit some traffic without requiring authentication, such as Internet Control Message Protocol (ICMP) or routing updates.

- Deny all other traffic.

- Apply the extended ACL to the inbound direction of the interface where proxy authentication is configured.

Enable the Router's HTTP or HTTPS Server for AAA

Router(config)#

```
ip http server
```

- **Enables the HTTP server on the router**

Router(config)#

```
ip http authentication aaa
```

- **Sets the HTTP server authentication method to AAA**
- **Proxy uses HTTP server for communication with a client**

Router(config)#

```
ip http secure-server
```

- **Enables the HTTPS server on the router**

```
Router(config)# ip http server
Router(config)# ip http authentication aaa
```

SECUR 1.1—7-20

To use the authentication proxy with HTTP, use the **ip http server** command to enable the HTTP server on the router and the **ip http authentication aaa** command to make the HTTP server use AAA for authentication.

The syntax of the **ip http server** command is as follows:

ip http server

This command has no arguments.

The syntax of the **ip http authentication aaa** command is as follows:

ip http authentication aaa

This command has no arguments.

The HTTPS feature requires a Cisco IOS crypto image. Enabling this feature supports these options:

■ HTTP-initiated sessions normally exchange the username and password in clear text; this exchange is encrypted when using HTTPS.

■ HTTPS-initiated sessions are proxy authenticated.

To use the authentication proxy with HTTPS, use the **ip http secure-server** command to enable the HTTP server on the router and the **ip http authentication aaa** command to make the HTTP server use AAA for authentication.

The syntax of the **ip http secure-server** command is as follows:

ip http secure-server

This command has no arguments or keywords.

Authentication Proxy Configuration

This topic discusses how to configure the authentication proxy settings on a Cisco router.

Set Global Timers

Router(config)#

```
ip auth-proxy {inactivity-timer min |
  absolute-timer min}
```

- **Authentication inactivity timer in minutes (default = 60 minutes)**
- **Absolute activity timer in minutes (default = 0 minutes)**

```
Router(config)# ip auth-proxy inactivity-
  timer 120
```

SECUR 1.1—7-22

To set the authentication proxy inactivity timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity), use the **ip auth-proxy inactivity-timer** global configuration command. To set the default value, use the **no** form of this command. The **inactivity-timer** argument replaces the *auth-cache-time* in previous releases; some versions support both arguments. Use this command to set the global idle timeout value for the authentication proxy. You must set the value of the **inactivity-timer** *min* option to a higher value than the idle timeout of any CBAC protocols. Otherwise, when the authentication proxy removes the user profile along with the associated dynamic user ACLs, there might be some idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

The **absolute-timer** *min* option allows users to configure a window during which the authentication proxy on the enabled interface is active. Once the absolute timer expires, the authentication proxy will be disabled regardless of any activity. The global absolute timeout value can be overridden by the local (per protocol) value, which is enabled via the **ip auth-proxy name** command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

The syntax of the **ip auth-proxy** command is as follows:

ip auth-proxy {inactivity-timer *min* | absolute-timer *min*}

---

inactivity-timer *min*	Specifies the length of time in minutes that an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes.
absolute-timer *min*	Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.

Define and Apply Authentication Proxy Rules

Router(config)#

```
ip auth-proxy name auth-proxy-name {ftp | http
 | telnet} [inactivity-timer min] [absolute-
timer min][list {acl | acl-name}]
```

• **Creates an authorization proxy rule**

Router(config-if)#

```
ip auth-proxy auth-proxy-name
```

• **Applies an authorization proxy rule to an interface**
  – **For outbound authentication, apply to inside interface**
  – **For inbound authentication, apply to outside interface**

```
Router(config)# ip auth-proxy name aprule http
  list 111
Router(config)# interface ethernet0
Router(config-if)# ip auth-proxy aprule
```

SECUR 1.1—7-23

To create an authentication proxy rule, use the **ip auth-proxy name** global configuration command. To remove the authentication proxy rules, use the **no** form of this command.

The syntax of the **ip auth-proxy name** command is as follows:

ip auth-proxy name *auth-proxy-name* **{ftp | http | telnet} [inactivity-timer** *min*] **[absolute-timer** *min*]
[list {acl | acl-name}]

no ip auth-proxy name *auth-proxy-name*

auth-proxy-name	Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
**ftp	http	telnet**	Choose one of the three protocols to trigger the authentication proxy.
inactivity-timer *min*	(Optional.) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 2,147,483,647. The default value is equal to the value set with the ip auth-proxy command. This argument replaces **auth-cache-time** in previous releases; some versions support both arguments.
absolute-timer *min*	(Optional.) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.
list {*acl* **|** *acl-name***}**	(Optional.) Specifies a standard (1-99), extended (1-199), or named IP ACL to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the ACL. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy** interface configuration command. To remove the authentication proxy rules, use the **no** form of this command.

The syntax of the **ip auth-proxy** command is as follows:

ip auth-proxy *auth-proxy-name*

no ip auth-proxy *auth-proxy-name*

auth-proxy-name	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the **authentication proxy name** command.

Note	A proxy authentication rule can consist of multiple statements, each specifying a different authentication type (http, ftp, telnet). This configuration support proxy authentication for multiple applications (HTTP, HTTPS, FTP, and Telnet) at the same time.

Authentication Proxy Rules with ACLs

Router(config)#

```
ip auth-proxy name auth-proxy-name http list
  {acl-num | acl-name}
```

• **Creates an authorization proxy rule with an access list**

```
Router(config)# ip auth-proxy name aprule http
  list 10
Router(config)# access-list 10 permit 10.0.0.0
  0.0.0.255
Router(config)# interface ethernet0
Router(config-if)# ip auth-proxy aprule
```

SECUR 1.1—7-24

You can associate an authentication proxy rule with an ACL, providing control over which hosts use the authentication proxy. To create an authentication proxy rule with ACLs, use the **ip auth-proxy name** global configuration command with the **list *acl*** option. To remove the authentication proxy rules, use the **no** form of this command.

The syntax of the **ip auth-proxy name** with ACLs command is as follows:

ip auth-proxy name *auth-proxy-name* http list {*acl-num* | *acl-name*}

no ip auth-proxy name *auth-proxy-name*

auth-proxy-name	Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
**list *acl-num*	*acl-name***	(Optional) Specifies a standard (1-99), extended (1-199), or named IP access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the ACL. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.

Test and Verify the Configuration

This topic discusses the procedures for testing and verifying the authentication proxy configuration.

show Commands

Cisco.com

Router(config)#

```
show ip auth-proxy cache
show ip auth-proxy configuration
show ip auth-proxy statistics
```

- **Displays statistics, configurations, and cache entries of authentication proxy subsystems**

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—7-26

Use the **show ip auth-proxy** command to display the authentication proxy entries, the running authentication proxy configuration, or the authentication proxy statistics.

The syntax of the **show ip auth-proxy** command is as follows:

show ip auth-proxy {cache | configuration | statistics}

cache	Lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.
configuration	Displays all authentication proxy rules configured on the router.
statistics	Displays all the router statistics related to the authentication proxy.

debug Commands

Router(config)#

```
debug ip auth-proxy ftp
debug ip auth-proxy function-trace
debug ip auth-proxy http
debug ip auth-proxy object-creation
debug ip auth-proxy object-deletion
debug ip auth-proxy tcp
debug ip auth-proxy telnet
debug ip auth-proxy timer
```

• **Helps with troubleshooting**

SECUR 1.1—7-27

The syntax of the **debug ip auth-proxy** command is as follows:

debug ip auth-proxy {ftp | function-trace | http | object-creation | object-deletion | tcp | telnet | timer}

ftp	Displays FTP events related to the authentication proxy.
function-trace	Displays the authentication proxy functions.
http	Displays HTTP events related to the authentication proxy.
object-creation	Displays additional entries to the authentication proxy cache.
object-deletion	Displays deletion of cache entries for the authentication proxy.
tcp	Displays TCP events related to the authentication proxy.
telnet	Displays Telnet-related authentication proxy events.
timer	Displays authentication proxy timer-related events.

Clear the Authentication Proxy Cache

Router(config)#

```
clear ip auth-proxy cache {* | ip_addr}
```

- **Clears authentication proxy entries from the router**

The syntax of the **clear ip auth-proxy cache** command is as follows:

clear ip auth-proxy cache {* | *ip_addr*}

*	Clears all authentication proxy entries, including user profiles and dynamic ACLs.
ip_addr	Clears the authentication proxy entry, including user profiles and dynamic ACLs, for the specified IP address.

Summary

This topic summarizes what you have learned in this lesson.

Summary

- **The Cisco IOS Firewall authentication proxy feature supports the following AAA protocols:**
  – **TACACS+**
  – **RADIUS**
- **Users can be authenticated using HTTP, HTTPS, FTP, and Telnet by a Cisco IOS Firewall.**
- **Authentication proxy technology allows users through a Cisco IOS Firewall after authenticating.**

SECUR 1.1—7-30

Lab Exercise—Configure Authentication Proxy on a Cisco Router

Complete the following lab exercise to practice what you learned in this chapter.

Objectives

In this lab exercise you will complete the following tasks:

- Complete the lab exercise setup.
- Configure the Cisco Secure ACS for Windows 2000.
- Configure AAA.
- Configure an authentication proxy.
- Test and verify an authentication proxy.

Visual Objective

The following figure displays the configuration you will use to complete in this lab exercise.
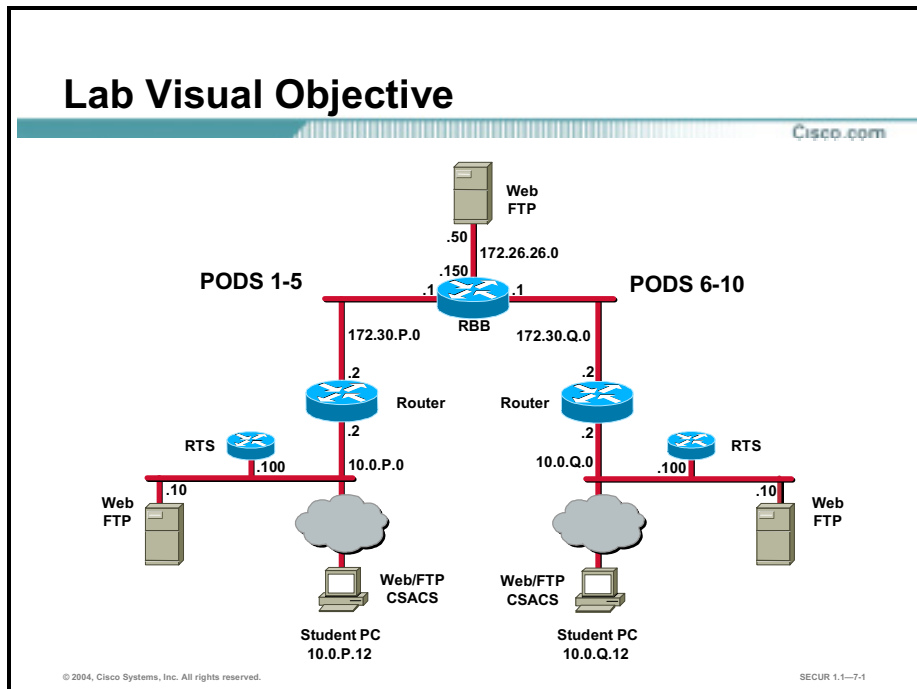
Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1 Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2 Configure your student PC for IP address 10.0.P.12 with a default gateway of 10.0.P.2 (where P = pod number).

Step 3 Reload your perimeter router using the default lab configuration.

Step 4 Ensure you can ping the other routers and network hosts before beginning.

Task 2—Configure the Cisco Secure ACS for Windows 2000

Complete the following steps to configure the Cisco Secure Access Control Server (Cisco Secure ACS) for Windows 2000:

Step 1 On your workstation, open the Cisco Secure ACS from the desktop.

Step 2 **Click Interface Configuration** on the far left column of Cisco Secure ACS. The Interface Configuration window opens.

Step 3 Click **TACACS+ (Cisco IOS)** to configure this option.

Step 4 Scroll down to locate the New Services frame.

Step 5 Select the first field under New Services and enter **auth-proxy** in the Service field.

Step 6 Select the **Service** field group check box. Make sure you select the check box directly to the left of the Service field.

Step 7 Scroll to the Advanced Configuration Options section and select the **Advanced TACACS+ features** option. This parameter will already be selected if you previously completed lab exercise 4.

Step 8 Click the **Submit** button to submit your changes.

Step 9 Click the **Group Setup** button. The Group Setup window opens.

Step 10 Select **Group 2** from the Group drop-down menu.

Step 11 Click **Edit Settings** to view the Group Settings for this group.

Step 12 Scroll down to the TACACS+ Settings section and locate the auth-proxy and Custom attributes check boxes. Select both the **auth-proxy** check box and the **Custom attributes** check box.

Step 13 Enter the following in the Custom attributes box. Please note that long lines of text, like the proxyacl#1 line shown here, can wrap within the custom attributes box and may look like two lines:

```
proxyacl#1=permit tcp any host 172.26.26.50 eq www
proxyacl#2=permit icmp any any
priv-lvl=15
```

Step 14 Click the **Submit** + **Restart** button to submit your changes and restart the Cisco Secure ACS. Wait for the interface to return to the Group Setup main window.

Task 3—Configure AAA

Complete the following steps to configure authentication, authorization, and accounting (AAA):

Step 1 On your router, enter global configuration mode:

```
Router# configure terminal
```

Step 2 Enable AAA:

```
Router(config)# aaa new-model
Router(config)# username cisco password cisco
```

Step 3 Specify the authentication protocol:

```
Router(config)# aaa authentication login default group tacacs+
```

Step 4 Specify the authorization protocol:

```
Router(config)# aaa authorization auth-proxy default group tacacs+
```

Step 5 Define the TACACS+ server and its key:

```
RP(config)# tacacs-server host 10.0.P.12
RP(config)# tacacs-server key ciscosecure
```

(where P = pod number)

Step 6 Define a new access control list (ACL) to allow TACACS+ traffic to the inside interface from your AAA server. Also, allow outbound ICMP traffic and context-based access control (CBAC) traffic (FTP and WWW). Block all other inside-initiated traffic.

```
RP(config)# access-list 101 permit tcp host 10.0.P.12 eq tacacs host
10.0.P.2
RP(config)# access-list 101 permit icmp any any
RP(config)# access-list 101 deny ip any any
```

(where P = pod number, and Q = peer pod number)

Step 7 Apply the new ACL to the e0/0 interface of your perimeter router:

```
RP(config)# interface fast 0/0
RP(config-if)# ip access-group 101 in
RP(config-if)# exit
```

Step 8 Enable the router's HTTP server for AAA:

```
RP(config)# ip http server
RP(config)# ip http authentication aaa
```

Task 4—Configure an Authentication Proxy

Complete the following steps to configure authentication proxy:

Step 1 Define an authentication proxy rule:

```
RP(config)# ip auth-proxy name APRULE http inactivity-timer 5
```

Step 2 Apply the authentication proxy rule to the inside interface:

```
RP(config)# interface fast 0/0
RP(config-if)# ip auth-proxy APRULE
RP(config-if)# end
```

Task 5—Test and Verify an Authentication Proxy

Complete the following steps to test and verify authentication proxy:

Step 1 On your router, use the **show access-list** command to check your access lists. Fill in the blanks below using the output from this command:

```
RP# show access-list
Extended IP access list 101
```

_____

_____

_____

Step 2 Use the **show ip auth-proxy configuration** command to verify the authorization proxy configuration. Fill in the blanks below using the output from this command:

```
RP# show ip auth-proxy configuration
Authentication global cache time is _____ minutes
Authentication Proxy Rule Configuration
```

```
        Auth-proxy name _____

        http list not specified auth-cache-time _____ minutes
```

Step 3 From your workstation command prompt, ping the backbone server:

```
C:\> ping 172.26.26.50

Pinging 172.26.26.50 with 32 bytes of data:


Reply from 172.26.26.50: bytes=32 time=34ms TTL=125

Reply from 172.26.26.50: bytes=32 time=34ms TTL=125

Reply from 172.26.26.50: bytes=32 time=34ms TTL=125

Reply from 172.26.26.50: bytes=32 time=36ms TTL=125
```

Step 4 Return to the Cisco Secure ACS and add a new username of **aaauser** with a password of **aaapass** to Group 2.

| **Note** | Return to lab exercise 4 if you need to review how to add a new user to a group. |

Step 5 Use your web browser to connect to the backbone web server. In the URL field enter the following:

http://172.26.26.50

Step 6 Enter the following when the web browser prompts you for a username and password:

```
Username: aaauser

Password: aaapass
```

Step 7 Use the **show access-list** command to check your ACLs. Fill in the blanks below using the output from this command:

```
RP# show access-list

Extended IP access list 101
```

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Step 8 Use the **show ip auth-proxy statistics** command to verify the authorization proxy statistics. Fill in the blanks below using the output from this command:

```
RP# show ip auth-proxy statistics
```

```
Authentication Proxy Statistics
     proxied client number _____
```

Step 9   Use the **show ip auth-proxy cache** command to verify the authorization proxy configuration. Fill in the blanks below using the output from this command:

```
RP# show ip auth-proxy cache
```

_____

_____

8

Cisco IOS Intrusion Detection System

Overview

This lesson covers information on the Cisco IOS Intrusion Detection System (IDS) package for Cisco routers and how to configure it.

This lesson includes the following topics:

■ Objectives

■ Cisco IOS IDS introduction

■ Initializing the Cisco IOS IDS

■ Configuring, disabling, and excluding signatures

■ Creating and applying audit rules

■ Verifying the configuration

■ Cisco IDS Network Module introduction

■ Summary

■ Lab exercise

Objectives

This topic lists the lesson objectives.

Objectives

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

• **Describe the Cisco IOS IDS package.**

• **Name the two types of signature implementations used by the Cisco IOS IDS.**

• **Name the response options available with the Cisco IOS IDS.**

• **Initialize a Cisco IOS IDS router.**

• **Configure, disable, and exclude signatures.**

• **Create and apply audit rules.**

• **Verify the Cisco IOS IDS configuration.**

• **Add a Cisco IOS IDS router to a Syslog server.**

• **Describe the Cisco IDS Network Module option.**

SECUR 1.1—8-2

Cisco IOS IDS Introduction

This topic introduces the Cisco IOS Intrusion Detection System (IDS) feature for Cisco IOS routers.

Cisco IOS IDS

Director

Syslog server

Cisco IOS router with IDS

E0   S0

Untrusted network

Attack

Send alarm to Director or Syslog server

SECUR 1.1—8-4
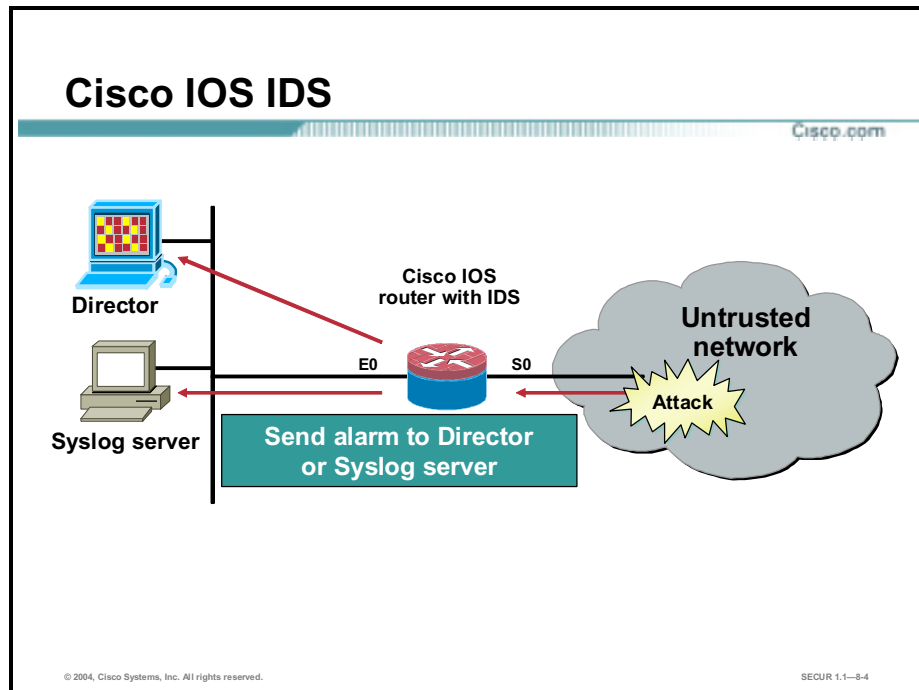
Cisco offers several non-router-based products to monitor your network including the following:

■ Cisco Secure IDS Sensors—The Cisco IDS 4200 Series appliance sensors are purpose-built, high-performance network security "appliances" that protect against unauthorized, malicious activity traversing the network, such as attacks by hackers. Cisco IDS sensors analyze traffic in real-time, enabling users to quickly respond to security breaches.

■ Cisco Secure Intrusion Detector Director—Centrally monitors the activity of multiple Cisco Secure IDS sensors located on local or remote network segments. It is designed to address the increased requirements for security visibility, denial-of-service protection and anti-hacking detection.

The Cisco IOS IDS provides intrusion detection capabilities within a variety of Cisco IOS routers. It acts just like a Cisco Secure IDS Sensor from an intrusion detection point-of-view, and can be added to the Cisco Secure Intrusion Detector Director map as another icon to provide a consistent view of all Sensors throughout a network. The Cisco IOS IDS contains an enhanced reporting mechanism that permits logging to the router's Syslog service in addition to the Director.

The Cisco IOS IDS provides a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. This technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS IDS Network Visibility

Cisco.com

Sales offices

Engineering

Finance

International sales offices

Mainframe

WAN

Campus backbone

VPN

Suppliers

Accounting

Internet

Intranet servers
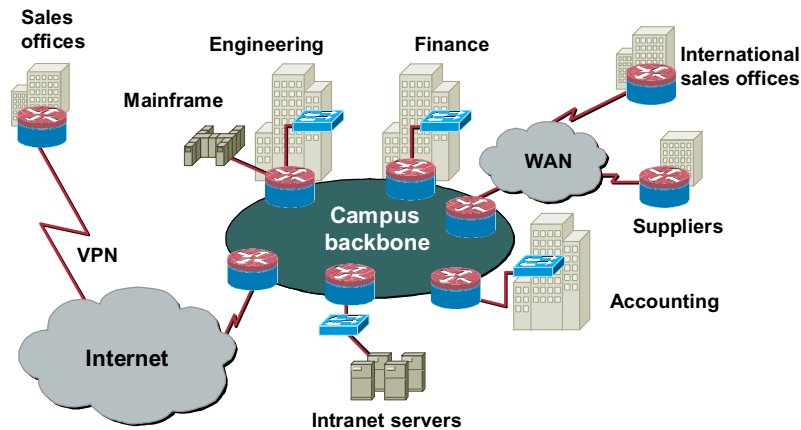
SECUR 1.1—8-5

The Cisco IOS IDS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators now have more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts. IDS signatures can be deployed alongside or independently of other Cisco IOS Firewall features. Existing Cisco IDS customers can deploy the Cisco IOS software-based IDS signatures to complement their current protection. This enables intrusion detection to be deployed to areas that may not be capable of supporting a Sensor.

The Cisco IOS IDS is intended to satisfy the security goals of all Cisco customers, and is particularly appropriate for the following:

■ Enterprise customers who are interested in a cost-effective method of extending their perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters.

■ Small- and medium-sized businesses that are looking for a cost-effective router that has an integrated firewall with intrusion detection capabilities.

■ Service provider customers who want to set up managed services, providing firewall and intrusion detection to their customers, all housed within the necessary function of a router.

Supported Router Platforms

Go to Cisco.com to view the current listing of routers that support Cisco IOS IDS features.

SECUR 1.1—8-6

Always reference the Cisco web site for up-to-date information regarding IOS IDS feature support.

- **Memory use and performance impact**
  - **Limited persistent storage**
  - **CPU intensive**
- **Updated signature coverage**

The following are issues to consider when implementing the IOS IDS:

- Memory usage and performance impact—The performance impact of intrusion detection depends on the number of signatures enabled, the level of traffic on the router, the router platform, and other individual features enabled on the router (for example, encryption and source route bridging). Because this router is being used as a security device, no packet is allowed to bypass the security mechanisms. The IDS process in the router sits directly in the packet path and thus searches each packet for signature matches. In some cases, the entire packet needs to be searched, and state information and even application state and awareness must be maintained by the router.

- Updated signature coverage—The Cisco IOS IDS now identifies more than 100 of the most common attacks using signatures to detect patterns of misuse in network traffic. The intrusion detection signatures were chosen from a broad cross-section of intrusion detection signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans. On the other hand, the dedicated Sensor audits over 1000 signatures, providing the most comprehensive coverage on network attacks.

Signature Implementations

- **Atomic**
  - **Single packet signatures**
  - **Typically does not require memory allocation**
- **Compound**
  - **Multiple packets over extended period of time, possibly to multiple hosts**
  - **Requires memory allocation to maintain session state**

Atomic signatures are those that trigger on a single packet. For auditing atomic signatures, there is no traffic-dependent memory requirement. Compound signatures are those that trigger on multiple packets. For auditing compound signatures, the IOS IDS allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.

Response Options

- **Alarm**
  - **Sends alarms to the Cisco IDS Director, Syslog server, or router console**
  - **Forwards the packet**
- **Reset—Sends packets with a reset flag to both session participants if TCP forwards the packet**
- **Drop—Immediately drops the packet**

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

- Alarm—Sends alarms to the Director, Syslog server, or router console, and then forwards the packet through.
- Reset—Sends packets with a reset flag to both session participants if it is a TCP session. It then forwards the packet through.
- Drop—Immediately drops the packet.

Note	It is recommended that you use the drop and reset actions together to ensure that the attack is terminated.

Configuration Tasks

- **Initialize IOS IDS on the router.**
- **Configure, disable, or exclude signatures.**
- **Create and apply audit rules.**
- **Verify the configuration.**
- **Add the Cisco IOS IDS router to the Director or Syslog server.**

To configure the IOS IDS on a router and to have it report alarms to a Director, complete the following tasks:

■ Initialize the IOS IDS on the router—This includes setting the notification type, the router's PostOffice parameters, the Director's PostOffice parameters, the protected network definition, and the router's maximum queue size for holding alarms.

■ Configure, disable, or exclude signatures—This includes setting the spam attack threshold, disabling signatures globally, and excluding signatures by host or network.

■ Create and apply audit rules—This includes creating an audit rule for information or attack signatures and then applying it to an interface. Another option is to create an audit rule that excludes hosts or networks and then applying it to an interface.

■ Verify the configuration—This includes using available **show**, **clear**, and **debug** commands for the IOS IDS.

■ Add the IOS IDS to the Director's map—The IDS-enabled router appears as another Sensor on the Cisco IDS Home map.

Initializing the Cisco IOS IDS

This topic covers the commands to set the notification type, the router's PostOffice parameters, the Director's PostOffice parameters, the protected network definition, and the router's maximum queue size for holding alarms.

Set Notification Type

Router (config)#

```
ip audit notify {nr-director|log}
```

• **Sets notification type**

```
Router(config)# ip audit notify nr-director
Router(config)# ip audit notify log
```

SECUR 1.1—8-12

Use the **ip audit notify** global configuration command to specify the methods of alarm notification. Use the **no** form of this command to disable event notifications.

The syntax for the **ip audit notify** command is as follows:

ip audit notify {nr-director | log}

no ip audit notify {nr-director | log}

nr-director	Send messages in PostOffice format to the Director or Sensor.
log	Send messages in Syslog format to the router's console or a remote Syslog server.

Set the Protected Network

Router (config)#

```
ip audit protected ip-addr [to ip-addr]
```

- **Specifies addresses on the protected network**
- **Has no impact on intrusion detection functionality, and is used only in log records (IN and OUT direction fields)**

```
Router(config)# ip audit protected 10.0.0.1
  to 10.0.0.254
```

SECUR 1.1—8-13

Use the **ip audit protected** global configuration command to specify whether an IP address is on a protected network. Use the **no** form of this command to remove network addresses from the protected network list. If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

The syntax for the **ip audit protected** command is as follows:

ip audit protected *ip-addr* **[to** *ip-addr***]**

no ip audit protected [*ip-addr***]**

to	Specifies a range of IP addresses.
ip-addr	IP address of a network host.

Set the Notification Queue Size

Router (config)#

```
ip audit po max-events num-of-events
```

- **Sets the maximum number of alarms saved in the router queue**
- **Default is 100 alarms**
- **Caution, router has limited persistent storage; if queue fills, alarms are lost on FIFO basis**
- **Reliability vs. memory trade-off is that each alarm uses 32 KB of memory**

```
Router(config)# ip audit po max-events 300
```

SECUR 1.1—8-14

Use the **ip audit po max-events** global configuration command to specify the maximum number of event notifications that are placed in the router's event queue. Use the **no** version of this command to set the number of recipients to the default setting.

The syntax for the **ip audit po max-events** command is as follows:

ip audit po max-events *num-of-events*

no ip audit po max-events

number-of-events	Integer in the range of 1–65535 that designates the maximum number of events allowable in the event queue. Use with the max-events keyword. The default number of events is 100.

Configuring, Disabling, and Excluding Signatures

This topic covers the commands to set the spam attack threshold, disable signatures globally, and exclude signatures by host or network.

Configure Spam Attack

Router (config)#

```
ip audit smtp spam num-of-recipients
```

- **Specifies the number of mail recipients over which a spam attack is suspected (signature identification 3106)**
- **The default is 250**

```
Router(config)# ip audit smtp spam 350
```

SECUR 1.1—8-16

Use the **ip audit smtp spam** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected. Use the **no** version of this command to set the number of recipients to the default setting.

The syntax for the **ip audit smtp spam** command is as follows:

ip audit smtp spam *num-of-recipients*

no ip audit smtp spam

num-of-recipients	Integer in the range of 1–65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the spam keyword. The default number of recipients is 250.

Disable Signatures Globally

Router (config)#

```
ip audit signature sig-id disable
```

- **Specifies signatures that will not be audited**

```
Router(config)# ip audit signature 1004 disable
Router(config)# ip audit signature 1006 disable
Router(config)# ip audit signature 3102 disable
Router(config)# ip audit signature 3104 disable
```

SECUR 1.1—8-17

Use the **ip audit signature** global configuration command to globally disable a signature. Use the **no** form of this command to re-enable the signature.

The syntax for the **ip audit signature** command is as follows:

ip audit signature *sig-id* **disable**

no ip audit signature *sig-id*

sig-id	Unique integer specifying a signature as defined in the Cisco IDS Network Security Database (NSDB).
disable	Globally disables a signature from being audited by the IOS IDS router. All 59 signatures are enabled.

Exclude Signatures by Host or Network

Cisco.com

Router (config)#

```
ip audit signature sig-id list acl-list
```

• **Assigns an ACL number to the excluded signature**

```
Router(config)# ip audit signature 3100 list 91
Router(config)# ip audit signature 3102 list 91
```

Router (config)#

```
access-list acl-num deny host ip-addr
```

• **Uses deny statements to exclude hosts or networks**
• **Ends with permit any**

```
Router(config)# access-list 91 deny host 10.0.0.33
Router(config)# access-list 91 deny 10.1.1.0 255.255.255.0
Router(config)# access-list 91 permit any
```

Use the **ip audit signature** and the **access-list** global configuration commands to attach a signature to an ACL and stop the signature from triggering when generated from a given host or network. Use the **no** form of this command to remove the signature from the ACL.

The syntax for the **ip audit signature** command is as follows:

ip audit signature *sig-id* **list** *acl-num*

no ip audit signature *sig-id*

sig-id	Unique integer specifying a signature as defined in the NSDB.
list	Specifies an ACL to associate with the signature.
acl-num	Unique integer specifying a configured ACL on the router. Use with the list keyword.

The syntax for the **access-list** command is as follows:

access-list *acl-num* **deny [host]** *ip-addr* **[***wildcard***]**

no access-list *acl-num*

acl-num	Number of an ACL. This is a decimal number from 1 to 99.
deny	Denies signature trigger if the conditions are matched.
hosts	Identifies that the following IP address is that of a host.

ip-addr	IP address of the network or host from which the packet is being sent. There are two alternative ways to specify the source: ■ Use a four-octet, dotted-decimal IP address. ■ Use the keyword any as an abbreviation for an IP address and wildcard of 0.0.0.0 255.255.255.255.
wildcard	Wildcard bits to be applied to the IP address. There are two alternative ways to specify the source wildcard: ■ Use a four-octet, dotted-decimal format. Place ones in the bit positions you want to ignore. ■ Use the keyword any as an abbreviation for an IP address and wildcard of 0.0.0.0 255.255.255.255.

Creating and Applying Audit Rules

This topic covers the commands to create the Cisco IOS IDS audit rules and apply them to an interface.

Packet Auditing Process

- **Step 1—Set the default actions for information and attack signatures.**
- **Step 2—Create an audit rule:**
  - **Signatures to audit—Information, attack**
  - **Actions to take—Alarm, reset, drop**
- **Step 3—Apply the audit rule to an interface:**
  - **Inbound—Audit packets before ACLs discard them**
  - **Outbound—No auditing of the packets discarded by ACLs**
- **Step 4—Packets are audited.**
  - **1—IP**
  - **2—ICMP, TCP, or UDP**
  - **3—Application**
- **Step 5—Upon signature match, execute user-configured actions.**

SECUR 1.1—8-20

The following describes the packet auditing process with the Cisco IOS IDS:

Step 1   Set the default actions for both information and attack signatures.

Step 2   Create an audit rule that specifies the signatures that should be applied to packet traffic and the actions to take when a match is found. An audit rule can apply information and attack signatures to network packets.

Step 3   Apply the audit rule to an interface on the router, specifying a traffic direction (in or out):

- If the audit rule is applied to the inbound direction of the interface, packets passing through the interface are audited before any inbound ACL has a chance to discard them. This enables an administrator to be alerted if an attack or reconnaissance activity is underway even if the router would normally reject the activity.

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

Step 4   Packets going through the interface that match the audit rule are audited by a series of modules, starting with IP; then either Internet Control Message Protocol (ICMP), TCP, or UDP (as appropriate); and finally, the Application level.

Step 5   If a signature match is found in a module, then the user-configured actions occur.

Step 1—Set the Default Actions for Information and Attack Signatures

Router (config)#

```
ip audit info action [alarm] [drop] [reset]
```

• **Sets default actions for information signatures**

```
Router(config)# ip audit info action alarm
```

Router (config-if)#

```
ip audit attack action [alarm] [drop] [reset]
```

• **Sets default actions for attack signatures**

```
Router(config-if)# ip audit attack action alarm
  drop reset
```

SECUR 1.1—8-21

Use the **ip audit info** global configuration command to specify the default actions for info signatures. Use the **no** form of this command to set the default action for info signatures.

Use the **ip audit attack** global configuration command to specify the default actions for attack signatures. Use the **no** form of this command to set the default action for attack signatures.

The syntax for the **ip audit info** command is as follows:

ip audit info action [alarm] [drop] [reset]

no ip audit info

The syntax for the **ip audit info** command is as follows:

ip audit attack action [alarm] [drop] [reset]

no ip audit attack

action	Sets an action for the information signature to take in response to a match. The default action is to alarm.
alarm	Sends an alarm to the console, Director, or to a Syslog server. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.

Steps 2 and 3—Create and Apply an IDS Audit

Router (config)#

```
ip audit name audit-name {info|attack} [action
  [alarm] [drop] [reset]]
```

- **Specifies audit name, signature type, and actions**

```
Router(config)# ip audit name AUDIT1 info action alarm
Router(config)# ip audit name AUDIT1 attack action alarm
  drop reset
```

Router (config-if)#

```
ip audit audit-name {in|out}
```

- **Applies audit to interface**

```
Router(config)# interface e0
Router(config-if)# ip audit AUDIT1 in
```

SECUR 1.1—8-22

Use the **ip audit name** global configuration command to create audit rules for information and attack signature types. Use the **no** form of this command to delete an audit rule.

Use the **ip audit** interface configuration command to apply an audit specification created with the **ip audit name** command to a specific interface and for a specific direction. Use the **no** version of this command to disable auditing of the interface for the specified direction.

The syntax for the **ip audit name** command is as follows:

ip audit name *audit-name* **{info | attack} [action [alarm] [drop] [reset]]**

no ip audit name audit-name {info | attack}

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for information signatures.
attack	Specifies that the audit rule is for attack signatures.
action	Specifies an action or actions to take in response to a match. If an action is not specified, the default action is to alarm.
alarm	Sends an alarm to the console, Director, or to a Syslog server. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.

The syntax for the **ip audit** command is as follows:

ip audit *audit-name* **{in | out}**

no ip audit *audit-name* **{in | out}**

audit-name	Name for an audit specification. No audit specifications are applied to an interface or direction.
in	Apply to inbound traffic.
out	Apply to outbound traffic.

Create an IDS Audit with Excluded Addresses

Cisco.com

Router (config)#

```
ip audit name audit-name {info|attack}
  list acl-num [action [alarm] [drop] [reset]]
```

• **Specifies audit name, signature type, ACL number, and actions**

```
Router(config)# ip audit name AUDIT2 info list 93 action alarm
Router(config)# ip audit name AUDIT2 attack list 93 action alarm
  drop reset
```

```
Router(config)# access-list 93 deny host 10.1.1.16
Router(config)# access-list 93 permit any
```

• **Uses deny statements to exclude hosts or networks**

```
Router(config)# interface e0
Router(config-if)# ip audit AUDIT2 in
```

• **Applies audit to interface**

SECUR 1.1—8-23

The **ip audit name** and **access-list** global configuration commands can be used to create audit rules for information and attack signature types that you want to exclude from triggering when generated by a particular host or network. Use the **no** form of this command to delete an audit rule.

The syntax for the **ip audit name** command is as follows:

ip audit name *audit-name* **{info | attack} [list** *acl-num***] [action [alarm] [drop] [reset]]**

no ip audit name audit-name {info | attack}

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for information signatures.
attack	Specifies that the audit rule is for attack signatures.
list	Specifies an ACL to attach to the audit rule.
acl-num	Unique integer specifying a configured ACL on the router. Use with the list keyword.
action	Specifies an action or actions to take in response to a match. If an action is not specified, the default action is to alarm.
alarm	Sends an alarm to the console, Director, or to a Syslog server. Use with the action keyword.
reset	Resets the TCP session. Use with the action keyword.
drop	Drops the packet. Use with the action keyword.

Verifying the Configuration

This topic covers the commands that allow you to verify that the configuration is correct. These include the **show**, **clear**, and **debug** commands.

show Commands

Cisco.com

```
Router# show ip audit statistics
Router# show ip audit configuration
Router# show ip audit interface
Router# show ip audit debug
```

• **Displays various statistics, configurations, interface configurations, and debug flags**

Use the **show ip audit statistics** command to display the number of packets audited and the number of alarms sent, among other information. The syntax for the **show ip audit statistics** command is as follows:

show ip audit statistics

Use the **show ip audit configuration** command to display additional configuration information, including default values that may not be displayed using the **show run** command. The syntax for the **show ip audit configuration** command is as follows:

show ip audit configuration

An example output of the **show ip audit configuration** command follows:

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

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

Use the **show ip audit interface** command to display the interface configuration. The syntax for the **show ip audit interface** command is as follows:

show ip audit interface

An example output of the **show ip audit interface** command follows:

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

Use the **show ip audit debug** command to display the enabled debug flags. The syntax for the **show ip audit debug** command is as follows:

show ip audit debug

clear Commands

Router#

```
clear ip audit statistics
```

- **Resets IDS statistics**

Router#

```
clear ip audit configuration
```

- **Disables IDS**
- **Removes all IDS configurations**
- **Releases dynamic resources**

Use the **clear ip audit statistics** command to reset statistics on packets analyzed and alarms sent. The syntax for the **clear ip audit statistics** command is as follows:

clear ip audit statistics

Use the **clear ip audit configuration** command to disable the Cisco IOS IDS, remove all intrusion detection configuration entries, and release dynamic resources. The syntax for the **clear ip audit configuration** command is as follows:

clear ip audit configuration

debug Commands

```
Router# debug ip audit timers
Router# debug ip audit object-creation
Router# debug ip audit object-deletion
Router# debug ip audit function trace
Router# debug ip audit detailed
Router# debug ip audit ftp-cmd
Router# debug ip audit ftp-token
Router# debug ip audit icmp
Router# debug ip audit ip
Router# debug ip audit rpc
Router# debug ip audit smtp
Router# debug ip audit tcp
Router# debug ip audit tftp
Router# debug ip audit udp
```

• **Instead of** no, undebug **may be used**

SECUR 1.1—8-27

A plethora of debug commands are available to troubleshoot and test the Cisco IOS IDS configurations. Use the **no** form of the commands to disable debugging a given option. The following is the list of available debug commands:

debug ip audit timers

debug ip audit object-creation

debug ip audit object-deletion

debug ip audit function trace

debug ip audit detailed

debug ip audit ftp-cmd

debug ip audit ftp-token

debug ip audit icmp

debug ip audit ip

debug ip audit rpc

debug ip audit smtp

debug ip audit tcp

debug ip audit tftp

debug ip audit udp

Cisco IDS Network Module Introduction

This topic introduces the Cisco IDS Network Module option.

Note	The Cisco IDS Network Module is a Cisco IDS Sensor on a card. It is not the same thing as the Cisco IOS IDS features that have been discussed so far in this lesson. This topic is included as an introduction to this module only. This introduction will help you to identify this module and differentiate between its functionality and that of the Cisco IOS IDS feature set. For more information on Cisco IDS Sensors and the Cisco IDS Network Module, see the Cisco Secure Intrusion Detection System (CSIDS) course.

Overview of the Cisco IDS Network Module

- **Integrates IDS and branch office routing**
- **Fits into a single network module slot on the Cisco 2600XM, Cisco 3660, and Cisco 3700 Series platforms**
- **Requires Cisco IOS Software Revision 12.2(15)ZJ or greater**

SECUR 1.1—8-29

The Cisco IDS Network Module makes it possible to integrate Cisco IDS Sensor technology and branch office routing into a single Cisco router platform. This integration reduces the complexity of securing WAN links, while reducing operational costs. The integration of the IDS into the branch office router provides many important benefits, including the following:

- Physical space savings—The Cisco IDS Network Module fits into a single network module slot in a Cisco 2600XM Series, Cisco 3660, or Cisco 3700 Series branch office router. For more information regarding specific Cisco router platforms and models that support this option, go to Cisco.com.

- Simple power and cable management—The module takes advantage of the existing DC power and redundant power options of the router.

- Common management interface—The module can be configured and managed from the Cisco IOS command-line interface (CLI). This module supports the same CiscoWorks Management Center for IDS Sensors that the Cisco IDS 4200 Series supports, allowing customers to use one centralized management system for both IDS Sensor appliances and router-based IDS Sensors.

- Network command and control interface—By using the external Fast Ethernet port for command and control, the internal router connection of the Cisco IDS Network Module is free to capture packets to the module for processing by the IDS engine.

- Dedicated IDS engine—The module contains a dedicated CPU, freeing the router CPU from process-intensive IDS tasks.

The Cisco IDS Network Module can monitor from 10 to 45 Mbps of traffic (depending on the router model) and is suitable for T1/E1 and T3 environments. Routers containing the module may also support other Cisco IOS security features such as virtual private network (VPN), firewall, Multiprotocol Label Switching (MPLS), Network Address Translation (NAT), and Web Cache Communication Protocol (WCCP), while supporting all common Cisco IOS functions.

Cisco IDS Network Modules fit into a single network module slot on the Cisco 2600XM, Cisco 3660, and Cisco 3700 Series platforms. The module contains a 20-GB hard disk drive for logging and storing events. The external Ethernet port of the module is used for command and control of the IDS functions, keeping security and network operations administrative interfaces separated.

Cisco routers containing the Cisco IDS Network Module must be operating at a minimum of Cisco IOS Software Release 12.2(15)ZJ or greater.

Detailed information on configuring and administering the Cisco IDS Network Module is beyond the scope of this course. For more information regarding this module, refer to the CSIDS course.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **The Cisco IOS IDS package is a smaller version of the IDS Sensor located within Cisco IOS routers.**
- **The two types of signature implementations used by the Cisco IOS IDS are atomic and compound.**
- **You need to create and apply audit rules to the IDS configuration.**
- **You need to select the attack signatures for IDS monitoring.**
- **You need to verify the Cisco IOS IDS configuration using** debug **commands.**
- **You may add a Cisco IOS IDS router to a Syslog server.**
- **The Cisco IDS Network Module integrates IDS and branch office routing.**

SECUR 1.1—8-31

Lab Exercise—Configure a Cisco Router with IOS IDS

Complete the following lab exercise to practice what you have learned in this chapter.

Objectives

In this lab you will complete the following tasks:

- Complete the lab exercise setup.
- Initialize IDS on the router.
- Disable and exclude signatures.
- Create and apply audit rules.
- Verify the IDS router's configuration.
- Generate a test message.

Visual Objective

The following figure displays the configuration you will complete in the lab exercise.
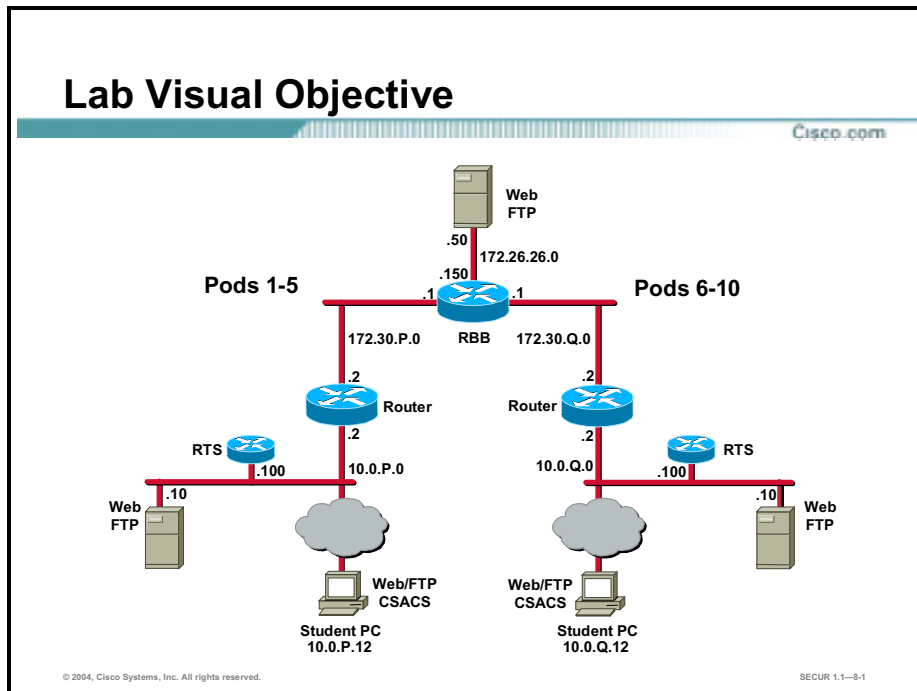
Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1   Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the laptop PC.

Step 2   Configure your student PC for IP address 10.0.P.12 with a default gateway of 10.0.P.2 (where P = pod number).

Step 3   Make sure that your student PC has an appropriate Syslog server application installed (for example; Kiwi's Syslog Daemon).

Step 4   Reload your perimeter router using the default lab configuration.

Step 5   Ensure you can ping the other routers and network hosts before beginning.

Task 2—Initialize IDS on the Router

Complete the following steps to initialize IDS on the router:

Step 1   From your student PC, access the router console.

Step 2   Switch to privileged-EXEC mode:

```
RP> enable
Password: cisco
RP#
```

Step 3 Switch to global configuration mode:

```
RP# conf t
RP(config)#
```

Step 4 Set the router to send Syslog messages to a Syslog server:

```
RP(config)# ip audit notify log
```

Step 5 Configure logging to a Syslog server:

```
RP(config)# logging on
RP(config)# logging host 10.0.P.12
```

(where P = pod number)

Step 6 (Optional.) Designate one network as the protected network:

Note   This step is optional and shows how to configure PostOffice alarms only.

```
RP(config)# ip audit protected 10.0.P.20 to 10.0.P.254
```

(where P = pod number)

Step 7 Save your configuration:

```
RP(config)# exit
RP# write memory
```

Task 3—Disable and Exclude Signatures

Complete the following steps to disable and exclude signatures:

Step 1 Globally disable signature 2004 (ICMP echo request):

```
RP(config)# ip audit signature 2004 disable
```

Step 2 Exclude 10.0.P.12 and 10.0.Q.12 and network address 10.2.P.0 from triggering signatures 2150 (fragmented ICMP traffic) and (half-open SYN attack) 3050:

```
RP(config)# ip audit signature 2150 list 90
RP(config)# ip audit signature 3050 list 90
RP(config)# access-list 90 deny host 10.0.P.12
RP(config)# access-list 90 deny host 10.0.Q.12
RP(config)# access-list 90 deny 10.2.P.0 0.0.0.255
RP(config)# access-list 90 permit any
```

(where P = pod number, and Q = peer pod number)

Task 4—Create and Apply Audit Rules

Complete the following steps to create and apply audit rules:

Step 1 Set the default actions for info and attack signatures:

```
RP(config)# ip audit info action alarm
```

```
RP(config)# ip audit attack action alarm drop reset
```

Step 2   Create audit rules for both info and attack signatures:

```
RP(config)# ip audit name AUDIT.1 info
RP(config)# ip audit name AUDIT.1 attack
```

Step 3   Create an audit rule to globally exclude network 10.2.P.0 from triggering info signatures:

```
RP(config)# ip audit name AUDIT.1 info list 91
RP(config)# access-list 91 deny 10.2.P.0 0.0.0.255
RP(config)# access-list 91 permit any
```

(where P = pod number)

Step 4   Apply the previously created audit rule to the Ethernet0/1 interface using the in direction:

```
RP(config)# interface e0/1
RP(config-if)# ip audit AUDIT.1 in
```

Step 5   Leave interface configuration mode:

```
RP(config-if)# exit
RP(config)#
```

Step 6   Leave terminal configuration mode:

```
RP(config)# exit
RP#
```

Step 7   Save configuration to flash memory:

```
RP# write memory
RP#
```

Task 5—Verify the IDS Router's Configuration

Complete the following steps to verify your configuration on the router is correct:

Step 1   Display your IDS configuration:

```
RP# show ip audit configuration
```

The parameters you just configured along with several default settings are displayed.

Step 2   Display your IDS interface configuration:

```
RP# show ip audit interface
```

The parameters you just configured along with several default settings are displayed.

Task 6—Generate a Test Message

Complete the following steps to test your peer pod's configuration. Have your peer pod do the same to your perimeter router:

Step 1   Start the Syslog server on your Windows 2000 Server.

Step 2   Send multiple fragmented packets to another pod's perimeter router using the following special technique:

```
RP# ping

Protocol [IP] <Enter>

Target IP address: <Enter Ip address of peer perimeter router public
interface>

Repeat count [5]: 20

Datagram size [100]: 2000

Timeout in seconds [2]: <Enter>

Extended commands [n]: <Enter>

Sweep range of sizes [n]: <Enter>
```

Your router will now send multiple fragmented packets to the peer router causing audit rules to
generate events to the Syslog server.

Step 3 Analyze the Syslog messages on the Syslog server.

9

Building IPSec VPNs Using Cisco Routers

Overview

This lesson teaches how to configure Cisco IOS IPSec using pre-shared keys for authentication. After presenting an overview of the process, the lesson shows you each major step of the configuration. It includes the following topics:

- Objectives

- Cisco routers enable secure VPNs

- IPSec overview

- IPSec protocol framework

- How IPSec works

- Configuring IPSec encryption

- Task 1—Prepare for IKE and IPSec

- Task 2—Configure IKE

- Task 3—Configure IPSec

- Step 1—Configure transform set suites

- Step 2—Configure global IPSec Security Association lifetimes

- Step 3—Create crypto ACLs

- Step 4—Create crypto maps

- Step 5—Apply crypto maps to interfaces

- Task 4—Test and verify IPSec

- Overview of configuring IPSec manually

- Overview of configuring IPSec for RSA encrypted nonces

- Summary

- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- **Define two types of Cisco router VPN solutions.**
- **Identify the IPSec standard and other open standards supported by Cisco VPN routers.**
- **Identify the component technologies of IPSec.**
- **Explain how IPSec works.**

SECUR 1.1—9-3

Objectives (cont.)

- **Configure a Cisco router for IKE using pre-shared keys.**
- **Configure a Cisco router for IPSec using pre-shared keys.**
- **Verify the IKE and IPSec configuration.**
- **Explain the issues regarding configuring IPSec manually and using RSA encrypted nonces.**

SECUR 1.1—9-4

Cisco Routers Enable Secure VPNs

Cisco routers support the latest in Virtual Private Network (VPN) technology. A VPN is a service offering secure, reliable connectivity over a shared public network infrastructure such as the Internet.

VPN Definition

VPN—An encrypted connection between private networks over a public network such as the Internet

SECUR 1.1—9-6
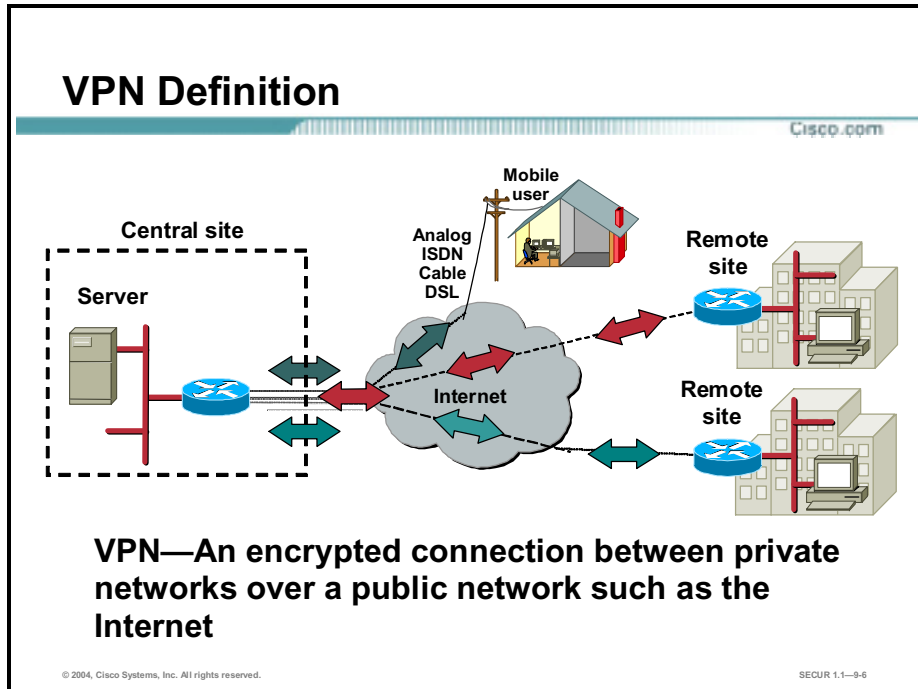
Cisco defines a VPN as an encrypted connection between private networks over a public network such as the Internet. The V and N stand for virtual network. The information from a private network is transported over a public network, an Internet, to form a virtual network. The P stands for private. To remain private, the traffic is encrypted to keep the data confidential. VPN is a private virtual network.

There are two types of router-based VPN networks:

■   Remote access

■   Site-to-site

Remote Access VPNs

Cisco.com

Central site

Remote access client

DSL
cable

POP

Telecommuter

Internet

Router

Mobile

POP

Extranet
Consumer-to-business
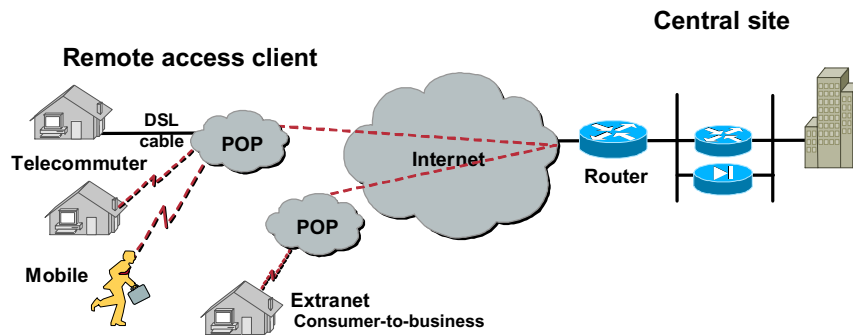
Remote access VPN—Extension/evolution of dial

SECUR 1.1—9-7

Remote access VPNs are targeted to mobile users and home telecommuters. In the past, corporations supported remote users via dial-in networks. This typically necessitated a toll or toll-free call to access the corporation. With the advent of VPNs, a mobile user can make a local call to their ISP to access the corporation via the Internet wherever they may be. It is an evolution of dial networks. Remote access VPN can support the needs of telecommuters, mobile users, extranet consumer-to-business, and so on.

Site-to-Site VPNs

Cisco.com

Remote office
1700/2600 Series

Main office
7000 Series

Regional office
3600/3700 Series

Internet

Small office/
home office
800/900 Series
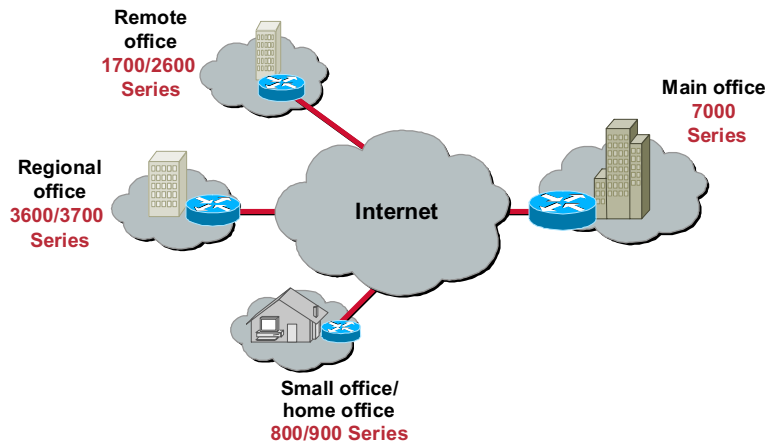
SECUR 1.1—9-8

Site-to-site VPNs provide cost benefits relative to private WANs and also enable new applications like extranets. However, site-to-site VPNs are still an end-to-end network and are subject to the same scalability, reliability, security, multi-protocol, and so on—requirements that exist in the private WAN. In fact, because VPNs are built on a public network infrastructure, they have additional requirements such as heightened security and advanced Quality of Service (QoS) capabilities, and a set of policy management tools to manage these additional features.

Cisco provides a suite of VPN-optimized routers. Cisco IOS software running in Cisco routers combines rich VPN services with industry-leading routing, thus delivering a comprehensive solution. Cisco routing software adds scalability, reliability, multi-protocol, multi-service, management, Service Level Agreement monitoring, and QoS to site-to-site applications. The Cisco VPN software adds strong security via encryption and authentication. VPN hardware acceleration cards are available for certain Cisco routers (see Cisco.com for more details on router models that support hardware encryption cards). Hardware encryption accelerator cards provide high-performance, hardware-assisted encryption and key generation suitable for VPN applications. Hardware encryption accelerators improve overall system performance by offloading encryption and decryption processing, thus freeing main system resources for other tasks, such as route processing, QoS, and other network services. These Cisco VPN-based products provide high performance for site-to-site, intranet, and extranet VPN solutions.

IPSec Overview

This topic presents an overview of the IPSec family of open standards.
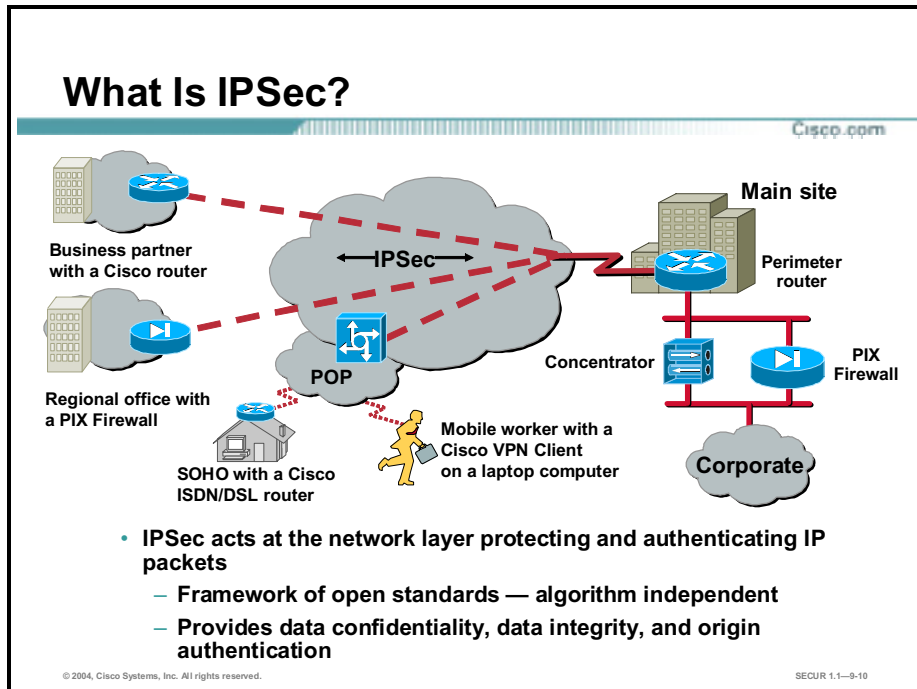
IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (peers), such as PIX Firewalls, Cisco routers, Concentrators, Cisco VPN Clients, and other IPSec-compliant products. IPSec is not bound to any specific encryption or authentication algorithms, keying technology, or security algorithms. IPSec is a framework of open standards. By not binding IPSec to specific algorithms, IPSec allows for newer and better algorithms to be implemented without patching the existing IPSec standards. IPSec provides data confidentiality, data integrity, and origin authentication between participating peers at the IP layer. IPSec is used to secure a path between a pair of gateways, a pair of hosts, or a gateway and host.

IPSec security services provides four critical functions:

- Confidentiality (encryption)—The sender can encrypt the packets before transmitting them across a network. By doing so, no one can eavesdrop on the communication. If intercepted, the communications cannot be read.

- Data integrity—The receiver can verify that the data was transmitted through the Internet without being changed or altered in any way.

- Origin authentication—The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.

- Anti-replay protection—Anti-replay protection verifies that each packet is unique, not duplicated. IPSec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. Packets whose sequence number is before the sliding window is considered late, or a duplicate. Late and duplicate packets are dropped.
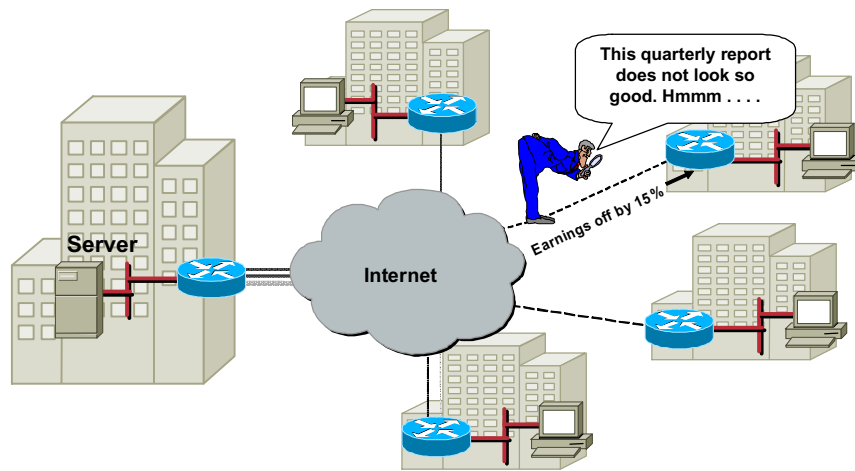
The Internet is a public network. Clear text data transported over the public Internet can be intercepted and read. In order to keep the data private, the data can be encrypted. By digitally scrambling, the data is rendered unreadable.

Types of Encryption

Cisco.com

| Pay to Terry Smith $100.00 |
| One Hundred and xx/100   Dollars |

Encryption algorithm

Hmmm . . . .
I cannot read a thing.

Encryption algorithm

| Pay to Terry Smith $100.00 |
| One Hundred and xx/100   Dollars |

4ehIDx67NMop9eR
U78IOPotVBn45TR

Internet

4ehIDx67NMop9eR
U78IOPotVBn45TR
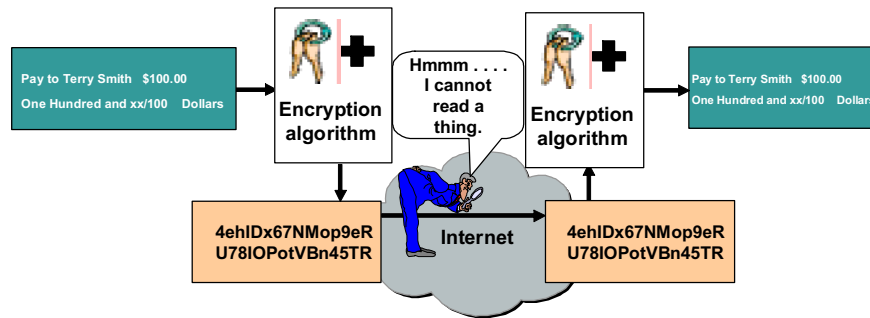
SECUR 1.1—9-13

For encryption to work, both the sender and receiver need to know the rules used to transform the original message into its coded form. Rules are based on an algorithm and a key. An algorithm is a mathematical function, which combines a message, text, digits, or all three with a string of digits called a key. The output is an unreadable cipher string. Decryption is extremely difficult or impossible without the correct key.

In the example in the figure, someone wants to send a financial document across the Internet. At the local end, the document is combined with a key and run through an encryption algorithm. The output is undecipherable cyber text. The cyber text is then sent through the Internet. At the remote end, the message is recombined with a key and sent back through the encryption algorithm. The output is the original financial document.

There are two types of encryption keys: symmetric and asymmetric. With symmetric key encryption, each peer uses the same key to encrypt and decrypt the data. With asymmetric key encryption, the local end uses one key to encrypt, and the remote end uses another key to decrypt the traffic.

DH Key Exchange

Cisco.com

Terry
Public key B
+ Private key A
Shared secret key (BA)

Key = Key

Alex
Public key A
+ Private key B
Shared secret key (AB)

Protocol Messages
Data Traffic
Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

Decrypt

Decrypt

Protocol Messages
Data Traffic
Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

4ehIDx67NMop9eR
U78IOPotVBn45TR

Internet

4ehIDx67NMop9eR
U78IOPotVBn45TR
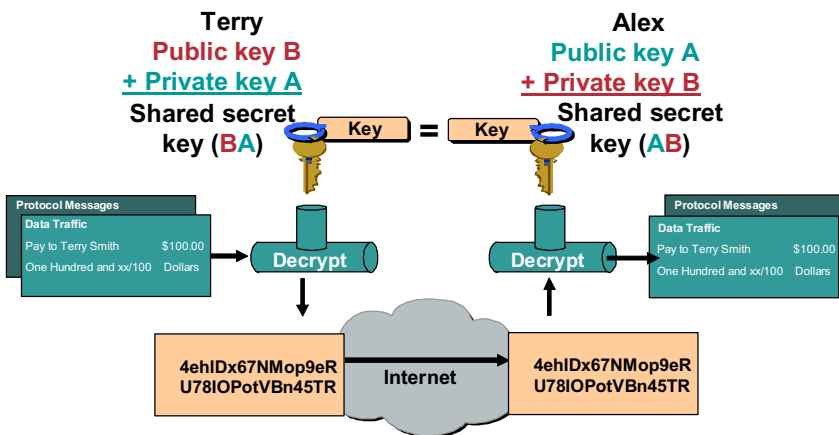
SECUR 1.1—9-14

DES, 3DES, HMAC-Message Digest 5 (MD5), and HMAC-SHA require a symmetric shared secret key to perform encryption and decryption. The question is how do the encrypting and decrypting devices get the shared secret key? The keys can be sent by e-mail, courier, overnight express, or public key exchange. The easiest method is DH public key exchange. The DH key agreement is a public key exchange method that provides a way for two peers to establish a shared secret key, which only they know, although they are communicating over an insecure channel.

Public key cryptosystems rely on a two-key system: a public key, which is exchanged between end-users, and a private key, which is kept secret by the original owners. DH public key algorithm states that if user A and user B exchange public keys and a calculation is performed on their individual private key and one another's public key, the end result of the process is an identical shared key. The shared key is used to derive encryption and authentication keys. DH key exchange is covered in more depth later in this lesson.

There are variations of the DH key exchange algorithm, known as DH group 1 through 7. DH groups 1, 2, and 5 support exponentiation over a prime modulus with a key size of 768,1024, and 1536 respectively. Cisco VPN Clients support DH groups 1,2, and 5. DES and 3DES encryption supports DH groups 1 and 2. AES encryption supports DH groups 2 and 5. The Certicom wireless VPN Client supports group 7. Group 7 supports elliptical curve cryptography that reduces the time needed to generate keys. During tunnel setup, VPN peers negotiate which DH group to use.

Security is not an issue with the DH key exchange. Although someone may know a user's public key, the shared secret cannot be generated because the private key never becomes public.

DH Key Exchange (cont.)

Cisco.com

Peer A   Peer B

1. Generate large integer p.   1. Generate large integer q.
   Send p to Peer B.   Send q to Peer A.
   Receive q.   Receive p.
   Generate g.   Generate g.

2. Generate private key X_A 2. Generate private key X_B

3. Generate public key   3. Generate public key
   $Y_A = g \wedge X_A \bmod p$ $Y_B = g \wedge X_B \bmod p$

4. Send public key Y_A 4. Send public key Y_B

5. Generate shared secret   5. Generate shared secret
   number $ZZ = Y_B \wedge X_A \bmod p$ number $ZZ = Y_A \wedge X_B \bmod p$

6. Generate shared secret key   6. Generate shared secret key
   from ZZ (DES, 3DES, or AES)   from ZZ (DES, 3DES, or AES)

SECUR 1.1—9-15

The Diffie-Hellman (DH) key exchange is a public key exchange method that provides a way
for two IPSec peers to establish a shared secret key that only they know, although they are
communicating over an insecure channel.

With DH, each peer generates a public and private key pair. The private key generated by each
peer is kept secret and never shared. The public key is calculated from the private key by each
peer and is exchanged over the insecure channel. Each peer combines the other's public key
with its own private key, and computes the same shared secret number. The shared secret
number is then converted into a shared secret key. The shared secret key is never exchanged
over the insecure channel.

Complete the following steps to implement the Diffie-Hellman process:

Step 1 The DH process starts with each peer generating a large prime integer, p and q. Each peer sends
the other its prime integer over the insecure channel. For example, Peer A sends p to Peer B.
Each peer then uses the p and q values to generate g, a primitive root of p.

Step 2 Each peer generates a private DH key (peer A: Xa, peer B: Xb).

Step 3 Each peer generates a public DH key. The local private key is combined with the prime number
p and the primitive root g in each peer to generate a public key, Ya for peer A and YA for peer
B. The formula for peer A is Ya =g^Xa mod p. The formula for peer B is Yb =g^Xb mod p.
The exponentiation is computationally expensive. The ^ character denotes exponentiation (g to
the Xa power); mod denotes modulus.

Step 4 The public keys Ya and Yb are exchanged in public.

Step 5 Each peer generates a shared secret number (ZZ) by combining the public key received from
the opposite peer with its own private key. The formula for peer A is ZZ=(YbXa) mod p. The
formula for peer B is ZZ=(YaXb) mod p. The ZZ values are identical in each peer. Anyone
who knows p or g, or the DH public keys, cannot guess or easily calculate the shared secret
value—largely because of the difficulty in factoring large prime numbers.

Step 6 Shared secret number ZZ is used in the derivation of the encryption and authentication symmetrical keys.

RSA Encryption

Cisco.com

Local

Key

Remote's
public key

Encrypt

Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

KJklzeAidJfdlwiej47
Dlltfd578MNSbXoE

Remote

Remote's
private key

Decrypt

Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

SECUR 1.1—9-16
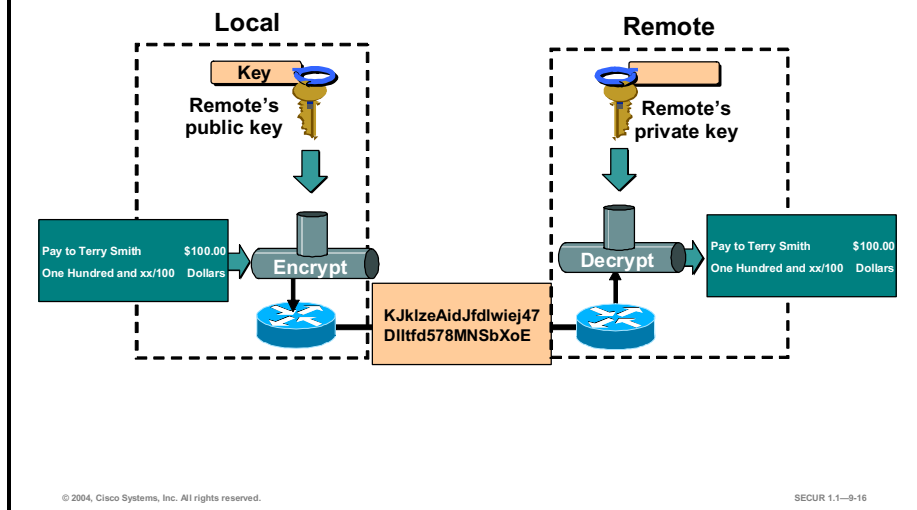
Rivest, Shamir, and Adelman (RSA) encryption uses asymmetric keys for encryption and decryption. Each end, local and remote, generates two encryption keys: a private and public key. They keep their private key and exchange their public key with people they wish to communicate. To send an encrypted message to the remote end, the local end encrypts the message using the remote's public key and the RSA encryption algorithm. The result is an unreadable cyber text. This message is sent through the Internet. At the remote end, the remote end uses its private key and the RSA algorithm to decrypt the cyber text. The result is the original message. The only one who can decrypt the message is the destination that owns the private key.

With RSA encryption, the opposite also holds true. The remote end can encrypt a message using its own private key. The receiver can decrypt the message using the sender's public key. This RSA encryption technique is used for digital signatures.

Encryption Algorithms

Encryption algorithms
- DES
- 3DES
- AES
- RSA

SECUR 1.1—9-17
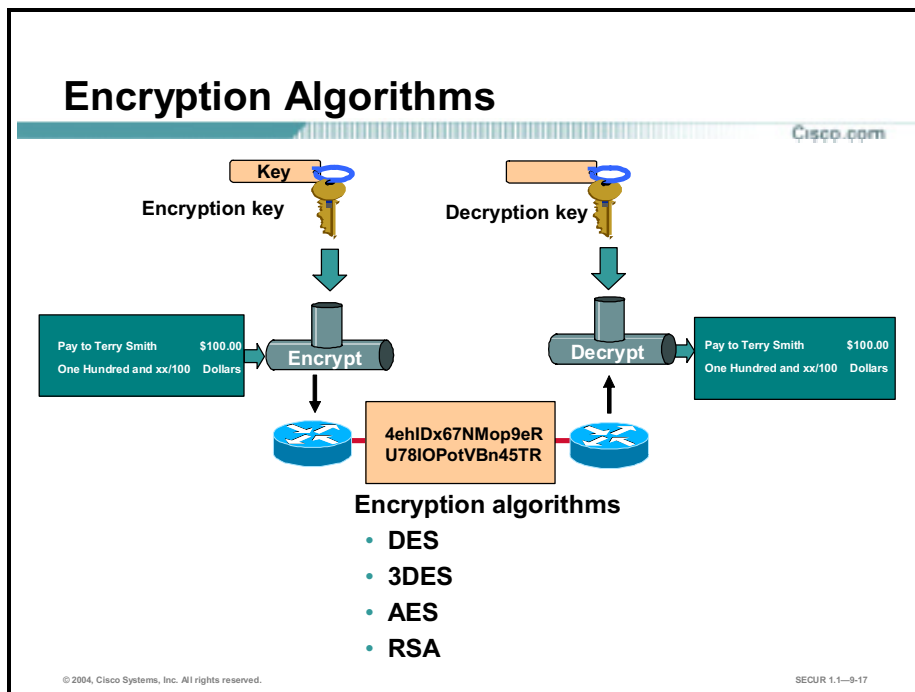
The degree of security depends on the length of the key. If someone tries to hack the key through a brute force attack, guessing every possible combination, the number of possibilities is a function of the length of the key. The time to process all the possibilities is a function of the computing power of the computer. Therefore, the shorter the key, the easier it is to break. A 64-bit key with a relatively sophisticated computer can take approximately 1 year to break. A 128-bit key with the same machine can take roughly 10 to the 19th years to decrypt.

Some of the encryption algorithms are as follows:

■ DES algorithm—DES was developed by IBM. DES uses a 56-bit key, ensuring high performance encryption. DES is a symmetric key cryptosystem.

■ 3DES algorithm—The 3DES algorithm is a variant of the 56-bit DES. 3DES operates similarly to DES, in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES. DES is a symmetric key cryptosystem.

■ Advanced Encryption Standard (AES)—The National Institute of Standards and Technology (NIST) has recently adopted a new Advanced Encryption Standard to replace existing DES encryption in cryptographic devices. AES provides stronger security than DES and computationally more efficient than 3DES. AES offers three different key strengths: 128, 192, and 256-bit keys.

■ RSA—RSA is an asymmetrical key cryptosystem. It uses a key length of 512, 768, 1024, or larger. IPSec does not use RSA for data encryption. Internet Key Exchange (IKE) only uses RSA encryption during the peer authentication phase. There will be more on RSA encryption and peer authentication later in this lesson.

Data Integrity
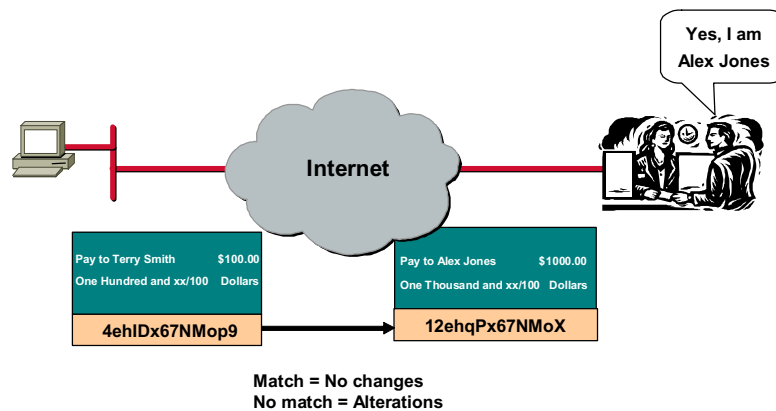
The next VPN-critical function is data integrity. VPN data is transported over the public Internet. Potentially, this data could be intercepted and modified. To guard against this, each message has a hash attached to the message. A hash guarantees the integrity of the original message. If the transmitted hash matches the received hash, the message has not been tampered with. However, if there is no match, the message was altered.

In the example in the figure, someone is trying to send Terry Smith a check for $100. At the remote end, Alex Jones is trying to cash the check for $1000. As the check progressed through the Internet, it was altered. Both the recipient and dollar amounts were changed. In this case, the hashes did not match. The transaction is no longer valid.

HMAC

Cisco.com

Local

Variable-length input message

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars

Shared secret key

Hash function

4ehIDx67NMop9

Remote

Received message

Shared secret key

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars

Hash function

4ehIDx67NMop9

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
4ehIDx67NMop9

Message + hash

① ②

SECUR 1.1—9-19
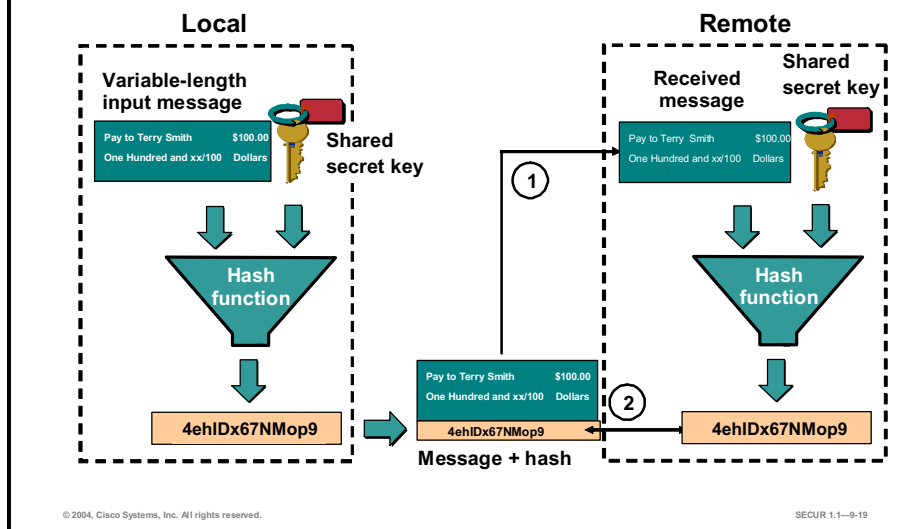
Hashed Message Authentication Codes (HMAC) guarantees the integrity of the message. At the local end, the message and a shared secret key are sent through a hash algorithm, which produces a hash value. Basically, a hash algorithm is a formula used to convert a variable length message into a single string of digits of a fixed length. It is a one-way algorithm. A message can produce a hash, but a hash cannot produce the original message. It is analogous to dropping a plate on the floor. The plate can produce a multitude of pieces, but the pieces cannot be recombined to reproduce the plate in its original form. The message and hash are sent over the network.

At the remote end, there is a two-step process. First, the received message and shared secret key are sent through the hash algorithm, resulting in a re-calculated hash value. Second, the receiver compares the re-calculated hash with the hash that was attached to the message. If the original hash and re-calculated hash match, the integrity of the message is guaranteed. If any of the original message is changed while in transit, the hash values are different.

HMAC Algorithms

Cisco.com

Pay to Terry Smith **$100.00**
One Hundred and xx/100 Dollars

HMAC algorithms
- **HMAC-MD5**
- **HMAC-SHA-1**

Hash function

4ehIDx67NMop9

Pay to Terry Smith **$100.00**
One Hundred and xx/100 Dollars

4ehIDx67NMop9

SECUR 1.1—9-20
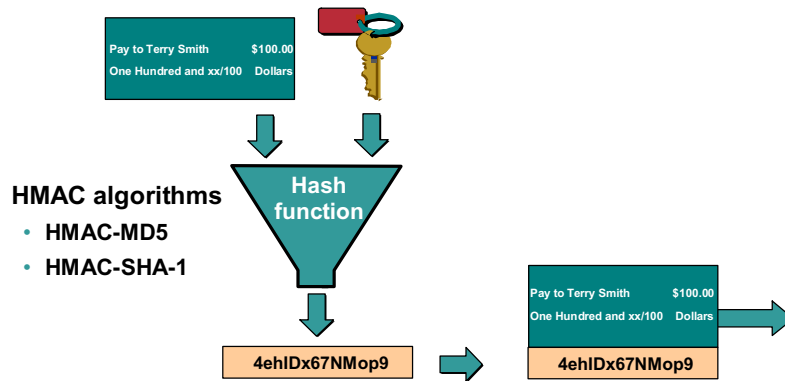
There are two common Hashed Message Authentication Codes (HMAC) algorithms:

■ HMAC-MD5—Uses a 128-bit shared secret key. The variable length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.

■ HMAC-SHA-1—HMAC-SHA-1 uses a 160-bit secret key. The variable length message and the 160-bit shared secret key are combined and run through the HMAC-SHA-1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

HMAC-SHA-1 is considered cryptographically stronger than HMAC-MD5. HMAC-SHA-1 is recommended when the slightly superior security of HMAC-SHA-1 over HMAC-MD5 is important.

Digital Signatures

Local

Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

4ehIDx67NMop9

Private key → **Encryption algorithm**

Hash

Hash algorithm

Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

Internet

Remote

Pay to Terry Smith $100.00
One Hundred and xx/100   Dollars

4ehIDx67NMop9

Hash

Match

Decryption algorithm → **Hash**

Public key

SECUR 1.1—9-21
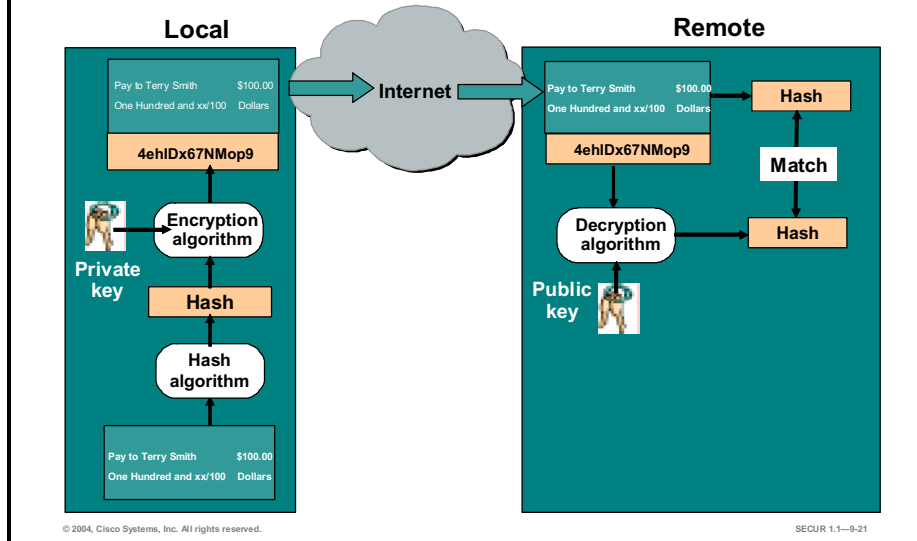
The last critical function is origin authentication. In the middle ages, a seal guaranteed the authenticity of an edict. In modern times, a signed document is notarized with a seal and a signature. In the electronic era, a document is signed using the sender's private encryption key—a digital signature. A signature is authenticated by decrypting the signature with the sender's public key.

In the example in the figure, the local device derives a hash and encrypts it with its private key. The encrypted hash—digital signature—is attached to the message and forwarded to the remote end. At the remote end, the encrypted hash is decrypted using the local end's public key. If the decrypted hash matches the re-computed hash, the signature is genuine. A digital signature ties a message to a sender. The sender is authenticated. It is used during the initial establishment of a VPN tunnel to authenticate both ends to the tunnel.

There are two common digital signature algorithms: RSA and Directory System Agent (DSA). RSA is used commercially and is the most common. DSA is used by U.S. Government agencies and is not as common.

Peer Authentication
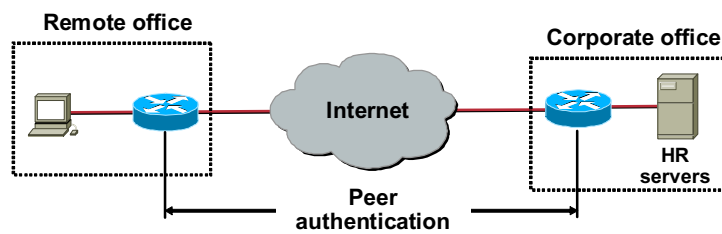
Remote office

Internet

Corporate office

HR servers

Peer authentication

Peer authentication methods:

- **Pre-shared keys**
- **RSA signatures**
- **RSA encrypted nonces**

SECUR 1.1—9-22

When conducting business long distance, it is necessary to know who is at the other end of the phone, e-mail, or fax. The same is true of VPN networking. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. There are three peer authentication methods:

- Pre-shared keys—A secret key value entered into each peer manually used to authenticate the peer.

- RSA signatures—Uses the exchange of digital certificates to authenticate the peers.

- RSA encrypted nonces—Nonces (a random number generated by each peer) are encrypted then exchanged between peers. The two nonces are used during the peer authentication process.

Pre-Shared Keys

Local Peer

Auth. key + ID information

Hash

Authenticating hash (Hash_L)

Internet

Remote Router

Auth. key + ID information

Hash

Computed hash (Hash)

=

Received hash (Hash_L)
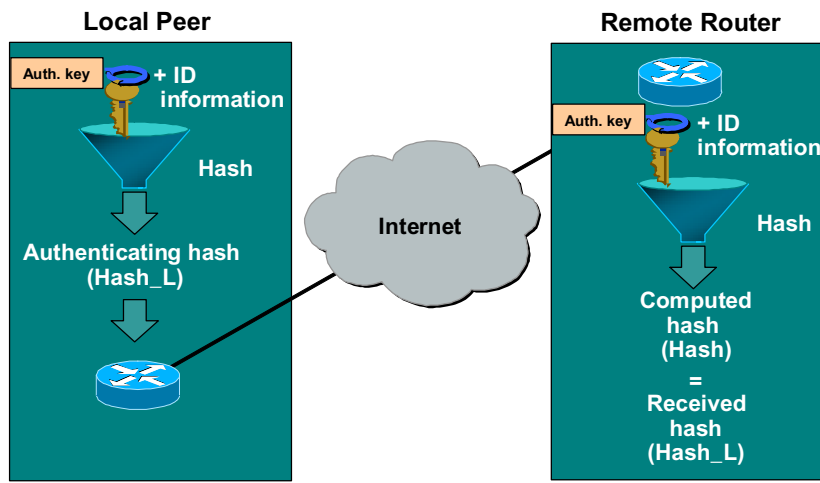
SECUR 1.1—9-23

With pre-shared keys, the same pre-shared key is configured on each IPSec peer. At each end, the pre-shared key is combined with other information to form the authentication key. Starting at the local end, the authentication key and the identity information (device-specific information) are sent through a hash algorithm to form hash_I. The local IKE peer provides one-way authentication by sending hash_I to the remote peer. If the remote peer is able to independently create the same hash, the local peer is authenticated (shown above).

The authentication process continues in the opposite direction. The remote peer combines its identity information with the pre-shared-based authentication key and sends them through a hash algorithm to form hash_R. Hash_R is sent to the local peer. If the local peer is able to independently create the same hash from its stored information and pre-shared-based authentication key, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered secure.Pre-shared keys are easy to configure manually, but do not scale well. Each IPSec peer must be configured with the pre-shared key of every other peer with which it communicates.

RSA Signatures
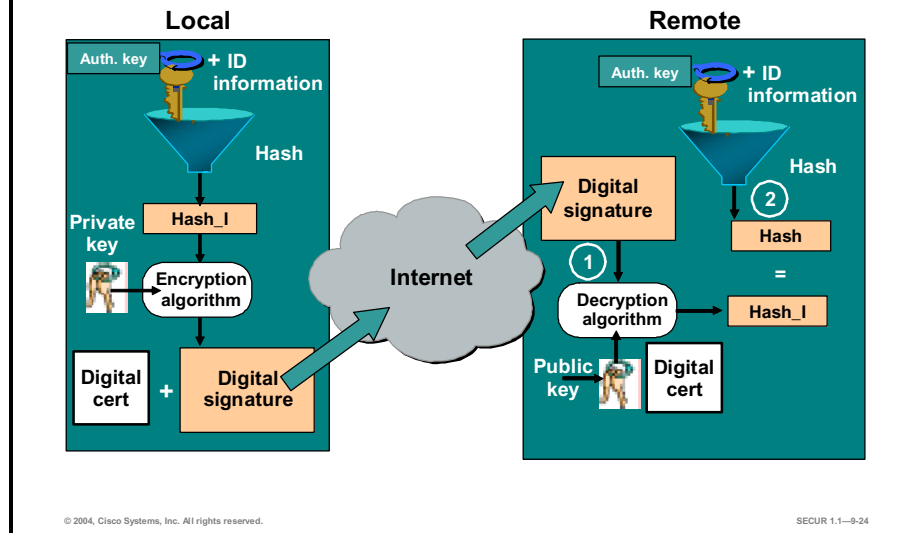
With Rivest, Shamir, and Adelman (RSA) signatures, hash_I and hash_R are not only authenticated, but are also digitally signed. Starting at the local end, the authentication key and identity information (device-specific information) are sent through a hash algorithm to form hash_I. The hash_I is then encrypted using the local peer's private encryption key. The result is a digital signature. The digital signature and a digital certificate are forwarded to the remote peer. (The public encryption key for decrypting the signature is included in the digital certificate exchanged between peers.)

At the remote peer, local peer authentication is a two-step process. First, the remote peer verifies the digital signature by decrypting it using the public encryption key enclosed in the digital certificate. The result is hash_I. Next, the remote peer independently creates hash_I from stored information. If the calculated hash_I equals the decrypted hash_I, the local peer is authenticated (shown in the figure). Digital signatures and certificates are discussed in more detail later in the digital certificate lesson.

After the remote peer authenticates the local peer, the authentication process begins in the opposite direction. The remote peer combines its identity information with the authentication key and sends them through a hash algorithm to form hash_R. Hash_R is encrypted using the remote peer's private encryption key, a digital signature. The digital signature and certificate are sent to the local peer. The local peer performs two tasks: it creates the hash_R from stored information, and it decrypts the digital signature. If the calculated hash_R and the decrypted hash_R match, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered secure.

RSA Encrypted Nonces

Local

Auth. key **+ ID information**

Hash

Authenticating hash (Hash_I)

Internet

Remote

Auth. key **+ ID information**

Hash

Computed hash (Hash_I)

=

Received hash (Hash_I)

SECUR 1.1—9-25
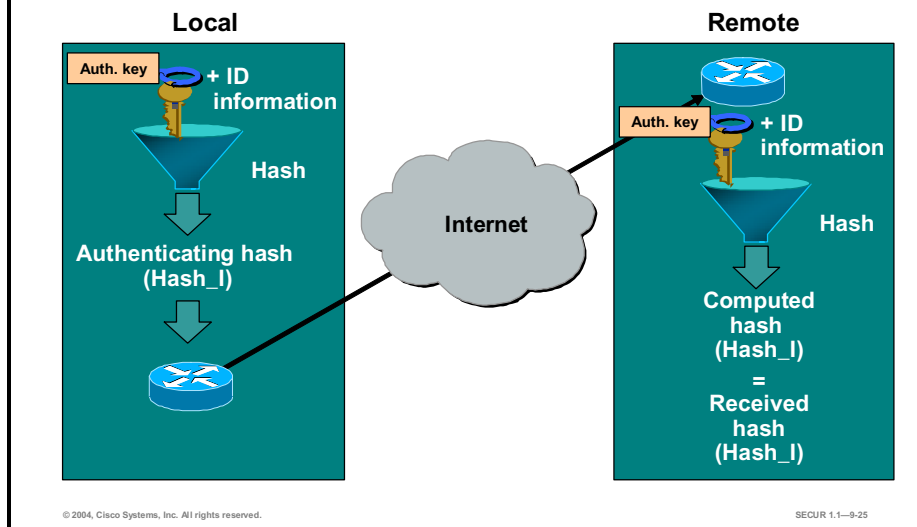
RSA encrypted nonces require that each party generate a nonce—a pseudorandom number. The nonces are then encrypted and exchanged. Upon receipt of the nonce, each end formulates an authentication key made up of the initiator and responder nonces, the DH key, and the initiator and responder cookies. The nonce-based authentication key is combined with device-specific information and run through a hash algorithm. Where the output becomes hash_L. The local IKE peer provides one-way authentication by sending hash_L to the remote peer. If the remote peer is able to independently create the same hash from stored information and its nonce-based authentication key, the local peer is authenticated (shown above).

After the remote end authenticates the local peer, authentication process begins in the opposite direction. The remote peer combines its identity information with the nonce-based authentication key and sends them through a hash algorithm to form hash_R. Hash_R is sent to the local peer. If the local peer is able to independently create the same hash from stored information and the nonce-based key, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered to be secure.

IPSec Protocol Framework

The last topic discussed encryption, authentication, and integrity. This topic explains how encryption, integrity, and authentication are applied to the IPSec protocol suite.

IPSec Security Protocols

Cisco.com

Authentication Header

Router A — All data in clear text — Router B

Authentication Header provides the following:
- Authentication
- Integrity

Encapsulating Security Payload

Router A — Data payload is encrypted — Router B

Encapsulating Security Payload provides the following:
- Encryption
- Authentication
- Integrity

SECUR 1.1—9-27
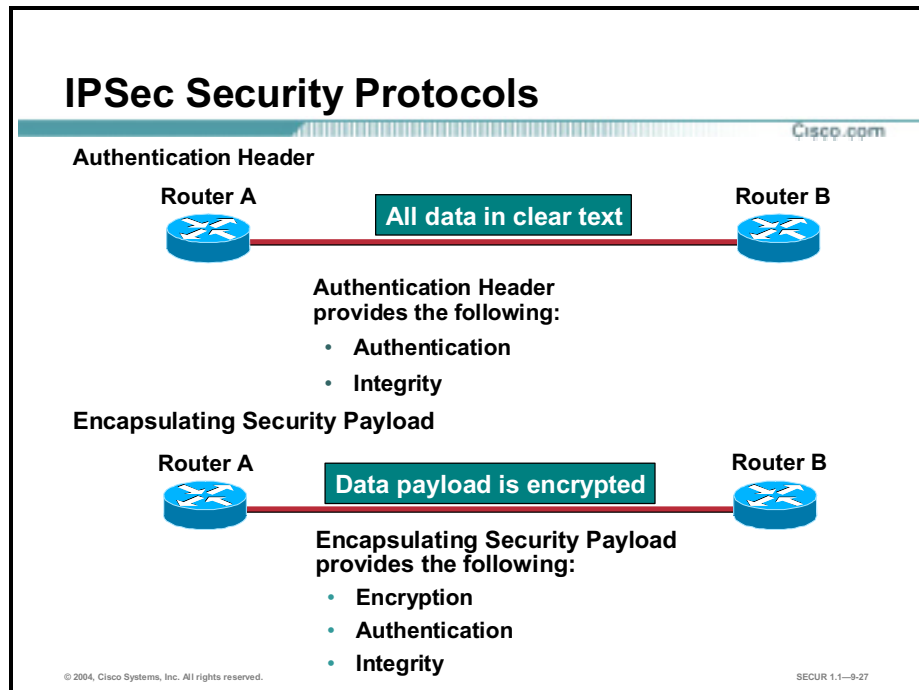
IPSec is a framework of open standards. IPSec spells out the messaging to secure the communications but relies on existing algorithms, such as DES and 3DES, to implement the encryption and authentication. The two main IPSec framework protocols are as follows:

■ Authentication Header (AH)—AH is the appropriate protocol when confidentiality is not required or permitted. It provides data authentication and integrity for IP packets passed between two systems. It is a means of verifying that any message passed from Router A to B has not been modified during transit. It verifies that the origin of the data was either Router A or B. AH does not provide data confidentiality (encryption) of packets. All text is transported in the clear.

■ Encapsulating Security Payload (ESP)—A security protocol may be used to provide confidentiality (encryption) and authentication. ESP provides confidentiality by performing encryption at the IP packet layer. IP packet encryption conceals the data payload and the identities of the ultimate source and destination. ESP provides authentication for the inner IP packet and ESP header. Authentication provides data origin authentication, and data integrity. Although both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.

Authentication Header

Router A

Router B

All data in clear text

- **Ensures data integrity**
- **Provides origin authentication (ensures packets definitely came from peer router)**
- **Uses keyed-hash mechanism**
- **Does not provide confidentiality (no encryption)**
- **Provides anti-replay protection**

SECUR 1.1—9-28

Authentication is achieved by applying a keyed one-way hash function to the packet to create a hash or message digest. The hash is combined with the text and transmitted. Changes in any part of the packet that occur during transit are detected by the receiver when it performs the same one-way hash function on the received packet, and compares the value of the message digest that the sender has supplied. The fact that the one-way hash also involves the use of a symmetric key between the two systems means that authenticity is guaranteed.

AH Authentication and Integrity

IP header + data + key

Router B

Hash

Authentication data
(00ABCDEF)

IP HDR | AH | Data

Internet

IP header + data + key

Hash

IP HDR | AH | Data

Received
hash
(00ABCDEF) =

Recomputed
hash
(00ABCDEF)

Router A

SECUR 1.1—9-29
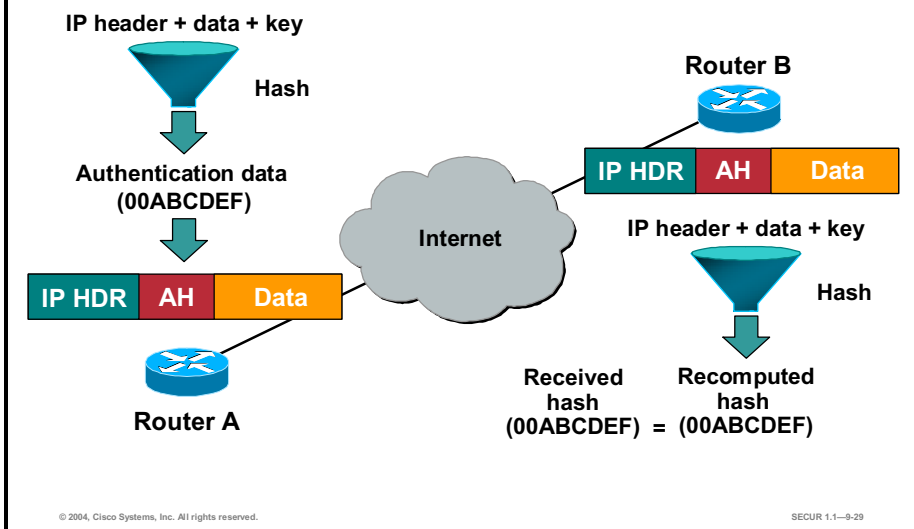
The Authentication Header (AH) function is applied to the entire datagram, except for any mutable IP header fields that change in transit (for example, Time To Live [TTL] fields that are modified by the routers along the transmission path). AH works as follows:

Step 1 The IP header and data payload is hashed.

Step 2 The hash is used to build an AH header, which is appended to the original packet.

Step 3 The new packet is transmitted to the IPSec peer router.

Step 4 The peer router hashes the IP header and data payload.

Step 5 The peer router extracts the transmitted hash from the AH header.

Step 6 The peer router compares the two hashes. The hashes must exactly match. Even if one bit is changed in the transmitted packet, the hash output on the received packet will change and the AH header will not match.

AH supports HMAC-MD5 and HMAC-SHA-1 algorithms.

ESP

Router A — Data payload is encrypted — Router B

- **Data confidentiality (encryption)**
- **Data integrity**
- **Data origin authentication**
- **Anti-replay protection**

SECUR 1.1—9-30

Encapsulating Security Payload (ESP) provides confidentiality by encrypting the payload. It supports a variety of symmetric encryption algorithms. The default algorithm for IPSec is 56-bit DES. Cisco products also support the use of 3DES for stronger encryption.

ESP can be used alone or in combination with AH. ESP with AH also provides integrity, and authentication of the data grams. First, the payload is encrypted. Next, the encrypted payload is sent through a hash algorithm: HMAC-MD5 or HMAC-SHA-1. The hash provides origin authentication and data integrity for the data payload.

Alternatively, ESP may also enforce anti-replay protection by requiring that a receiving host set the replay bit in the header to indicate that the packet has been seen.

ESP Protocol
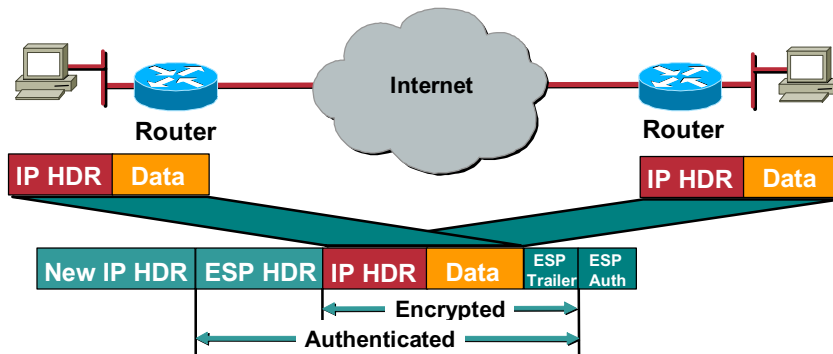
- Provides confidentiality with encryption
- Provides integrity with authentication

Between two security gateways, the original payload is well protected because the entire original IP data gram is encrypted. An Encapsulating Security Payload (ESP) header and trailer are added to the encrypted payload. With ESP authentication, the encrypted IP data gram and the ESP header or trailer are included in the hashing process. Last, a new IP header is appended to the front of the authenticated payload. The new IP address is used to route the packet through the Internet.

When both ESP authentication and encryption are selected, encryption is performed first before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can authenticate inbound packets. By doing this, it can detect the problems and potentially reduce the impact of denial of service (DoS) attacks.

Modes of Use—Tunnel Mode versus Transport Mode

Cisco.com

| IP HDR | Data |

Transport mode

| IP HDR | ESP HDR | Data | ESP Trailer | ESP Auth |

Encrypted
Authenticated

Tunnel mode

| New IP HDR | ESP HDR | IP HDR | Data | ESP Trailer | ESP Auth |
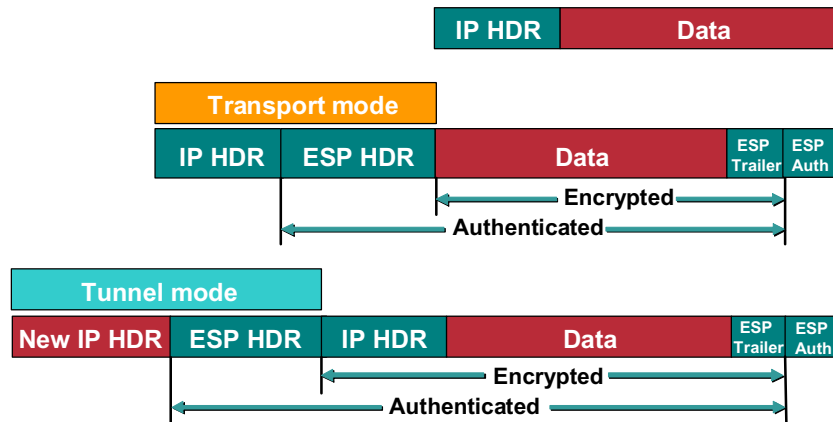
Encrypted
Authenticated

SECUR 1.1—9-32

ESP and AH can be applied to IP packets in two different ways, which are referred to as modes:

■ Transport mode—Transport mode protects the payload of the packet, higher layer protocols, but leaves the original IP address in the clear. The original IP address is used to route the packet through the Internet. ESP transport mode is used between two hosts. Transport mode provides security to the higher layer protocols only.

■ Tunnel mode—ESP tunnel mode is used when either end of the tunnel is a security gateway, a Concentrator, a VPN optimized router, or a PIX Firewall. Tunnel mode is used when the final destination is not a host, but a VPN gateway. The security gateway encrypts and authenticates the original IP packet. Next, a new IP header is appended to the front of the encrypted packet. The outside, new, IP address is used to route the packet through the Internet to the remote end security gateway. Tunnel mode provides security for the whole original IP packet.

Tunnel Mode

Remote office · Internet · Corporate office · HR servers · Tunnel mode

Home office · Internet · Corporate office · HR servers · Tunnel mode
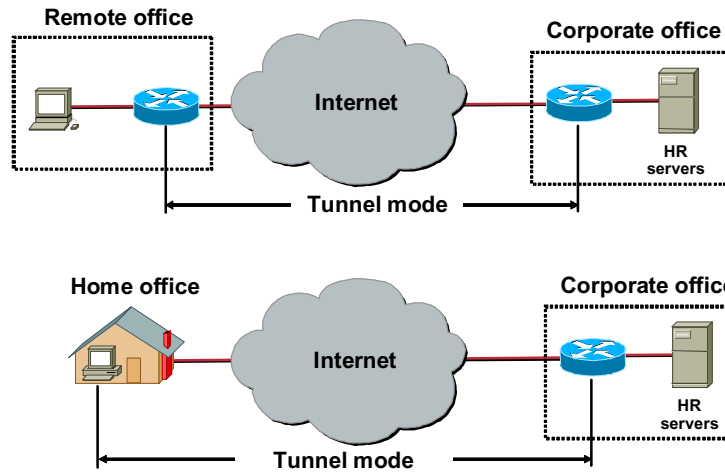
SECUR 1.1—9-33

ESP tunnel mode is used between a host and a security gateway or between two security gateways. For gateway-to-gateway applications, rather than load IPSec on all the computers at the remote and corporate offices, it is easier to have the security gateways perform the IP-in-IP encryption and encapsulation.

In the IPSec remote access application, ESP tunnel mode is used. At a home office, there may be no router to perform the IPSec encapsulation and encryption. In the example in the figure, the IPSec client running on the PC performs the IPSec IP-in-IP encapsulation and encryption. At the corporate office, the router de-encapsulates and decrypts the packet.
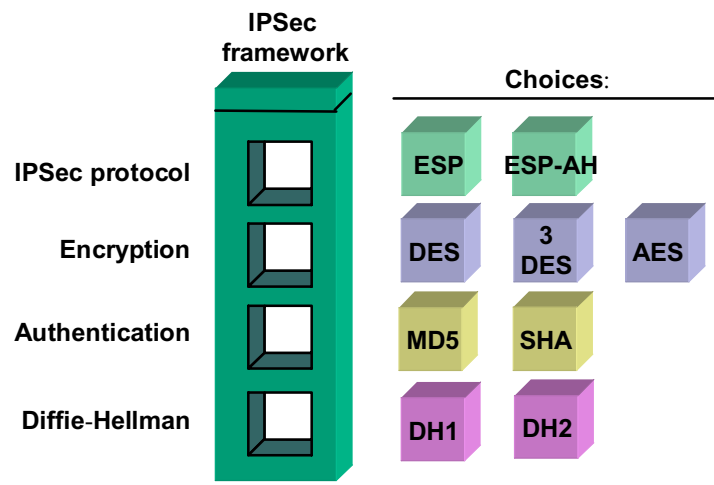
IPSec is a framework of open standards. IPSec spells out the rules for secure communications. IPSec, in turn, relies on existing algorithms to implement the encryption, authentication, and key exchange. Some of the standard algorithms are as follows:

- DES—DES is used to encrypt and decrypt packet data

- 3DES—Effectively doubles encryption strength over 56-bit DES

- AES—AES continues the trend of evolving encryption standards. AES-128 is equal to 3DES, while AES-192 and AES-256 offer superior encryption strength.

- Message Digest 5 (MD5)—Used to authenticate packet data

- Secure Hash Algorithm-1 (SHA)—Authenticates packet data

- DH—A public-key cryptography protocol that allows two parties to establish a shared secret key used by encryption and hash algorithms (for example, DES and MD5) over an insecure communications channel

In the example in the figure, there are four IPSec framework squares to be filled. When configuring security services to be provided by an IPSec gateway, first, an IPSec protocol must be chosen. The choices are ESP or ESP with AH. The second square is an encryption algorithm. Choose the encryption algorithm appropriate for the level of security desired: DES, 3DES, or AES. The third square is Authentication. Choose an authentication algorithm to provide data integrity: MD5 or SHA. The last square is the DH algorithm group. Choose which group to use: DH1 or DH2. IPSec provides framework, and the administrator chooses the algorithms used to implement the security services within that framework.

How IPSec Works

This topic details the individual steps of IPSec.

Five Steps of IPSec
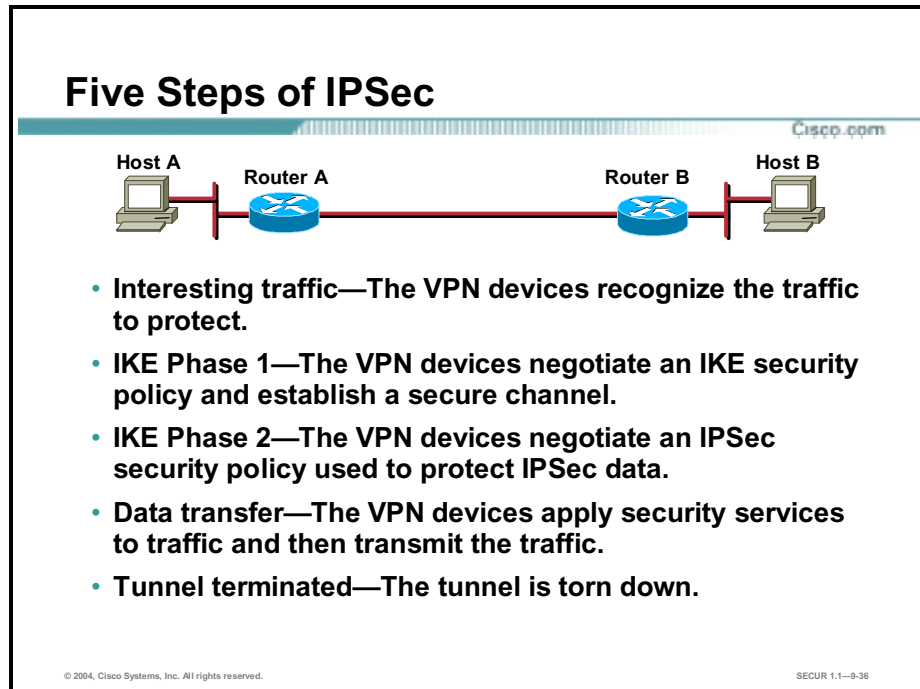
The goal of IPSec is to protect the desired data with the needed security services. IPSec's operation can be broken down into five primary steps:

Step 1 Interesting traffic—Traffic is deemed interesting when the VPN device recognizes that the traffic you want to send needs to be protected.

Step 2 IKE Phase 1—Between peers, a basic set of security services are negotiated and agreed upon. This basic set of security services protects all subsequent communications between the peers. IKE phase 1 sets up a secure communications channel between peers.

Step 3 IKE Phase 2—IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. These security parameters are used to protect data and messages exchanged between endpoints.

Step 4 Data transfer—Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

Step 5 IPSec tunnel termination—IPSec SAs terminate through deletion or by timing out.

Step 1—Interesting Traffic

Host A   Router A   Router B   Host B

10.0.1.3   10.0.2.3

Apply IPSec

Send in clear text
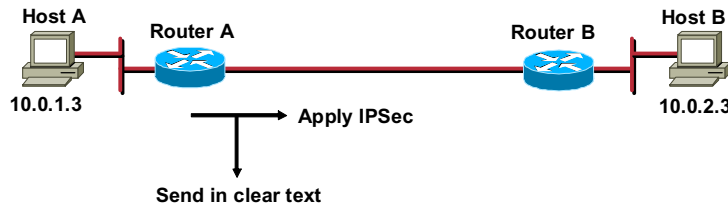
                                  SECUR 1.1—9-37

Determining what traffic needs to be protected is done as part of formulating a security policy for use of a VPN. The policy is used to determine what traffic needs to be protected and what traffic can be sent in the clear. For every inbound and outbound data gram, there are two choices: apply IPSec or bypass IPSec and send the data gram in clear text. For every data gram protected by IPSec, the system administrator must specify the security services applied to the data gram. The security policy database specifies the IPSec protocols, modes, and algorithms applied to the traffic. The services are then applied to traffic destined to each particular IPSec peer. With the VPN Client, you use menu windows to select connections that you want secured by IPSec. When interesting traffic transits the IPSec client, the client initiates the next step in the process: negotiating an IKE Phase 1 exchange.

Step 2—IKE Phase 1

Host A   Router A   Router B   Host B

10.0.1.3

IKE Phase 1:
Main mode exchange

10.0.2.3

Negotiate the policy   → ←   Negotiate the policy

DH exchange   → ←   DH exchange

Verify the peer identity   → ←   Verify the peer identity
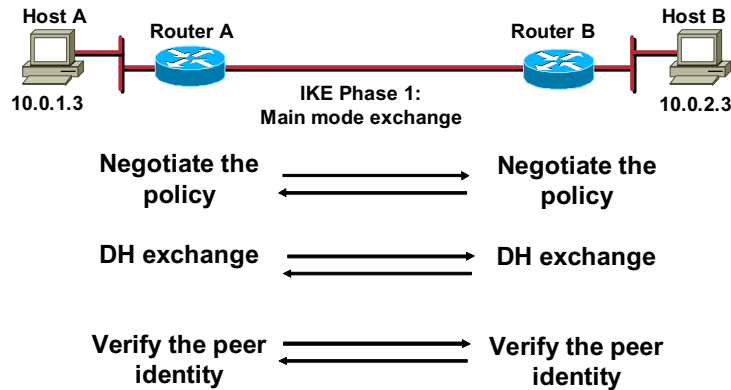
SECUR 1.1—9-38

The basic purpose of Internet Key Exchange (IKE) Phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. IKE Phase 1 occurs in two modes: main mode and aggressive mode.

Main mode has three two-way exchanges between the initiator and receiver:

■ First exchange—The algorithms and hashes used to secure the IKE communications are negotiated and agreed upon between peers.

■ Second exchange—Uses a DH exchange to generate shared secret keys and pass nonces, which are random numbers sent to the other party, signed, and returned to prove their identity. The shared secret key is used to generate all the other encryption and authentication keys.

■ Third exchange—Verifies the other side's identity. It is used to authenticate the remote peer. The main outcome of main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, it is possible to establish a secure communication channel with a hacker who is now stealing all your sensitive material.

In the aggressive mode, fewer exchanges are done and with fewer packets. On the first exchange, almost everything is squeezed in: the IKE policy set negotiation; the DH public key generation; a nonce, which the other party signs; and an identity packet, which can be used to verify their identity via a third party. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange.

IKE Transform Sets

Host A   Router A   Router B   Host B

10.0.1.3   Negotiate IKE Proposals   10.0.2.3

Transform 10
DES
MD5
pre-share
DH1
lifetime

IKE policy sets

Transform 15
DES
MD5
pre-share
DH1
lifetime

Transform 20
3DES
SHA
pre-share
DH1
lifetime
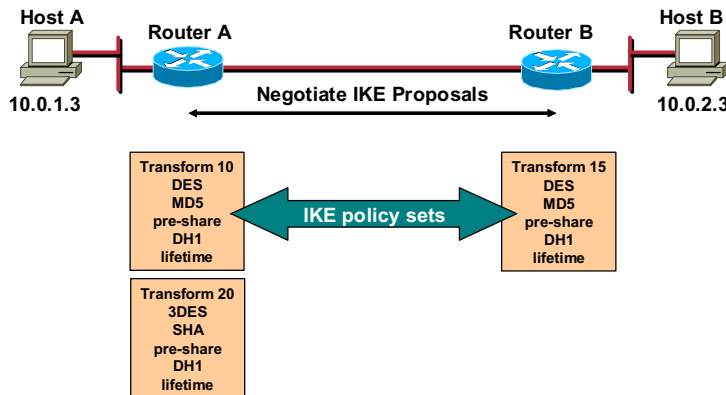
• **Negotiates matching IKE transform sets to protect IKE exchange**

SECUR 1.1—9-39

When trying to make a secure connection between Host A and B through the Internet, Internet Key Exchange (IKE) security proposals are exchanged between Router A and B. The proposals identify the IPSec protocol being negotiated (for example, ESP). Under each proposal, the originator must delineate which algorithms are employed in the proposal (for example, DES with MD5). Rather than negotiate each algorithm individually, the algorithms are grouped into sets, an IKE transform set. A transform set delineates which encryption algorithm, authentication algorithm, mode, and key length are proposed. These IKE proposals and transform sets are exchanged during the IKE main mode first exchange phase. If a transform set match is found between peers, the main mode continues. If no match is found, the tunnel is torn down.

In the example in the figure, Router A sends IKE transform sets 10 and 20 to Router B. Router B compares its set, transform set 15, with those received from Router A. In this instance, there is a match: Router A's transform set 10 matches Router B's transform set 15.

In a point-to-point application, each end may only need a single IKE policy set defined. However, in a hub and spoke environment, the central site may require multiple IKE policy sets to satisfy all the remote peers.

DH Key Exchange

Cisco.com

Terry
Public key B
+ Private key A
Shared secret key (BA)

Key = Key

Alex
Public key A
+ Private key B
Shared secret key (AB)

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars

Encrypt

Decrypt

Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars

4ehIDx67NMop9eR
U78IOPotVBn45TR

Internet

4ehIDx67NMop9eR
U78IOPotVBn45TR
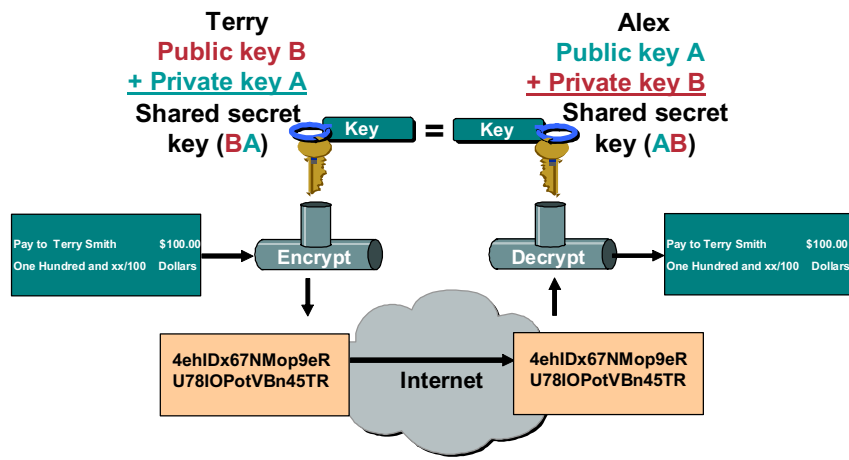
SECUR 1.1—9-40

DH key exchange is a public key exchange method that provides a way for two peers to establish a shared secret key over insecure communications path. With DH, there are several different DH algorithms, or groups defined, DH groups 1–7. A group number defines an algorithm and unique values. For instance, group 1 defines exponentiation over a prime modulus (MODP) algorithm with a 768-bit prime number. Group 2 defines a MODP algorithm with a 1024-bit prime number. During IKE Phase 1, the group is negotiated between peers. Between Cisco VPN devices, either group 1 or 2 is supported.

After the group negotiations are completed, the shared secret key is calculated, SKEYID. The shared secret key, SKEYID, is used in the derivation of three other keys: SKEYID_a, SKEYID_e, and SKEYID_d. Each key has a separate purpose. SKEYID_a is the keying material used during the authentication process. SKEYID_e key is the keying material used in the encryption process. SKEY_d is keying material used to derive keys for non-ISAKMP SAs. All four keys are calculated during IKE Phase 1.

Authenticate Peer Identity
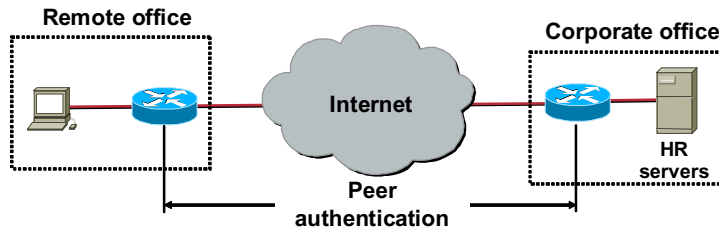
Remote office / Internet / Corporate office

Peer authentication

Peer authentication methods
- **Pre-shared keys**
- **RSA signatures**
- **RSA encrypted nonces**

SECUR 1.1—9-41

When conducting business over the Internet, it is necessary to know who is at the other end of the tunnel. The device on the other end of the VPN tunnel must be authenticated before the communications path is considered secure. The last exchange of IKE Phase 1 is used to authenticate the remote peer.

There are three data origin authentication methods:

■ Pre-shared keys—A secret key value entered into each peer manually used to authenticate the peer.

■ RSA signatures—Uses the exchange of digital certificates to authenticate the peers.

■ RSA encrypted nonces—Nonces (a random number generated by each peer) are encrypted and then exchanged between peers. The two nonces are used during peer authentication process.

Step 3—IKE Phase 2

Host A Router A   Router B Host B

10.0.1.3   Negotiate IPSec   10.0.2.3
                   security parameters

The purpose of Internet Key Exchange (IKE) Phase 2 is to negotiate the IPSec security parameters used to secure the IPSec tunnel. IKE Phase 2 performs the following functions:

■ Negotiates IPSec security parameters, IPSec transform sets

■ Establishes IPSec SAs

■ Periodically renegotiates IPSec SAs to ensure security

■ Optionally performs an additional DH exchange

IKE Phase 2 has one mode, called Quick mode. Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec transform, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode exchanges nonces that are used to generate new shared secret key material and prevent replay attacks from generating bogus SAs.

Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires. Quick mode is used to refresh the keying material used to create the shared secret key based on the keying material derived from the DH exchange in Phase 1.

IPSec Transform Sets

Host A — Router A — Router B — Host B

10.0.1.3

Negotiate transform sets

10.0.2.3

Transform set 30
ESP
3DES
SHA
Tunnel
Lifetime

IPSec transform sets

Transform set 55
ESP
3DES
SHA
Tunnel
Lifetime

Transform set 40
ESP
DES
MD5
Tunnel
Lifetime
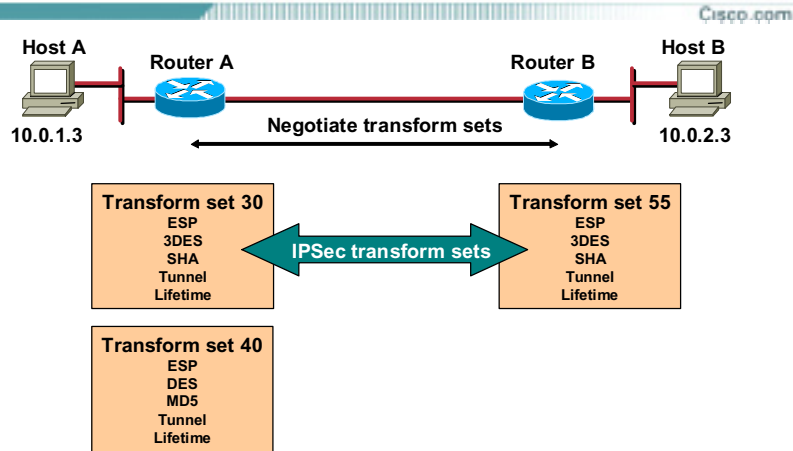
- **A transform set is a combination of algorithms and protocols that enact a security policy for traffic.**

SECUR 1.1—9-43

The ultimate goal of IKE Phase 2 is to establish a secure IPSec session between endpoints. Before that can happen, each pair of endpoints negotiates the level of security required (for example, encryption and authentication algorithms for the session). Rather than negotiate each protocol individually, the protocols are grouped into sets, an IPSec transform set. IPSec transform sets are exchanged between peers during Quick mode. If a match is found between sets, IPSec session-establishment continues. If no match is found, the session is torn down.

In the example in the figure, Router A sends IPSec transform set 30 and 40 to Router B. Router B compares its set, transform set 55, with those received from Router A. In this instance, there is a match. Router A's transform set 30 matches Router B's transform set 55. These encryption and authentication algorithms form an SA.

Security Associations

SA

SA Db
- **Destination IP address**
- **SPI**
- **Protocol (ESP or AH)**

Security policy Db
- **Encryption algorithm**
- **Authentication algorithm**
- **Mode**
- **Key lifetime**

BANK

192.168.2.1
SPI–12
ESP/3DES/SHA
tunnel
28800

Internet

192.168.12.1
SPI–39
ESP/DES/MD5
tunnel
28800
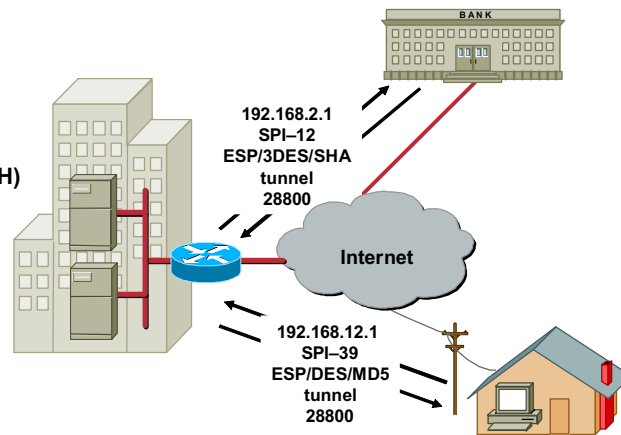
SECUR 1.1—9-44

When the security services are agreed upon between peers, each VPN peer device enters the information in a security policy database (SPD). The information includes the encryption and authentication algorithm, destination IP address, transport mode, key lifetime, and so on. This information is referred to as the SA. An SA is a one-way logical connection that provides security to all traffic traversing the connection. Because most traffic is bi-directional, two SAs are required: one for inbound and one for outbound traffic. The VPN device indexes the SA with a number, a Security Parameter Index (SPI). Rather than send the individual parameters of the SA across the tunnel, the source gateway, or host, inserts the SPI into the ESP header. When the IPSec peer receives the packet, it looks up the destination IP address, IPSec protocol, and SPI in its SA database (SAD), and then processes the packet according to the algorithms listed under the SPD.

The IPSec SA is a compilation of the SAD and SPD. SAD is used to identify the SA destination IP address, IPSec protocol, and SPI number. The SPD defines the security services applied to the SA, encryption and authentication algorithms, and mode and key lifetime. For example, in the corporate-to-bank connection, the security policy provides a very secure tunnel using 3DES, SHA, tunnel mode, and a key lifetime of 28800. The SAD value is 192.168.2.1, ESP, and SPI-12. For the remote user accessing e-mails, a less secure policy is negotiated using DES, MD5, tunnel mode, and a key lifetime of 28800. The SAD values are a destination IP address of 192.169.12.1, ESP, and an SPI-39.

SA Lifetime

Data-based

Time-based

SECUR 1.1—9-45

Like passwords on your company PC, the longer you keep it, the more vulnerable it becomes. The same thing is true of keys and Security Associations (SAs). For good security, the SA and keys should be changed periodically. There are two parameters: lifetime type and duration. The first parameter is lifetime type. How is the lifetime measured? Is it measured by the number of bytes transmitted or the amount of time transpired? The second parameter is the unit of measure: kilobytes of data or seconds of time. Some examples are as follows: lifetime based on 10,000 kilobytes of data transmitted or 28800 seconds of time expired. The keys and SAs remain active until their lifetime expires or until some external event—the client drops the tunnel—causes them to be deleted.

Step 4—IPSec Session

Host A   Router A   Router B   Host B

IPSec session

- **SAs are exchanged between peers.**
- **The negotiated security services are applied to the traffic.**

After IKE Phase 2 is complete and Quick mode has established IPSec SAs, traffic is exchanged between Host A and B via a secure tunnel. Interesting traffic is encrypted and decrypted according to the security services specified in the IPSec SA.

Step 5—Tunnel Termination

Host A   Router A   Router B   Host B
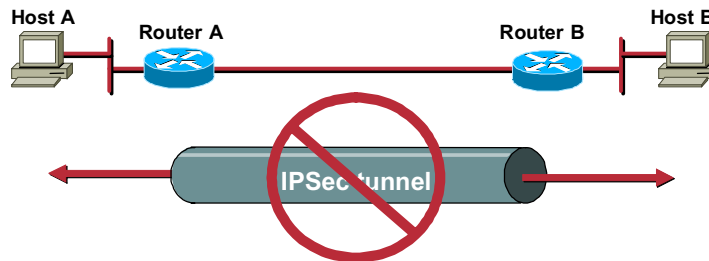
IPSec tunnel

- **A tunnel is terminated by one of the following:**
  - **By an SA lifetime timeout**
  - **If the packet counter is exceeded**
- **IPSec SA is removed**

SECUR 1.1—9-47

IPSec SAs terminate through deletion or by timing out. An SA can time out when a specified number of seconds has elapsed or when a specified number of bytes has passed through the tunnel. When the SAs terminate, the keys are also discarded. When subsequent IPSec SAs are needed for a flow, IKE performs a new Phase 2, and, if necessary, a new Phase 1 negotiation. A successful negotiation results in new SAs and new keys. New SAs are usually established before the existing SAs expire, so that a given flow can continue uninterrupted.

Configuring IPSec Encryption

This topic presents an overview of the major IPSec encryption tasks you will perform in this lesson.

Tasks to Configure IPSec Encryption

Cisco.com

Task 1—Prepare for IKE and IPSec.
Task 2—Configure IKE.
Task 3—Configure IPSec.
Task 4—Test and verify IPSec.

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—9-49

The use of Internet Key Exchange (IKE) pre-shared keys for authentication of IP Security (IPSec) sessions is relatively easy to configure, yet does not scale well for a large number of IPSec clients.

The process for configuring IKE pre-shared keys in Cisco IOS software for Cisco routers consists of four major tasks. Subsequent topics of this lesson discuss each configuration task in more detail. The four major tasks are as follows:

■ Task 1—Prepare for IPSec. This task involves determining the detailed encryption policy: identifying the hosts and networks you wish to protect, determining details about the IPSec peers, determining the IPSec features you need, and ensuring existing ACLs are compatible with IPSec.

■ Task 2—Configure IKE. This task involves enabling IKE, creating the IKE policies, and validating the configuration.

■ Task 3—Configure IPSec. This task includes defining the transform sets, creating crypto ACLs, creating crypto map entries, and applying crypto map sets to interfaces.

■ Task 4—Test and verify IPSec. Use **show**, **debug**, and related commands to test and verify that IPSec encryption works, and to troubleshoot problems.

Task 1—Prepare for IKE and IPSec

Successful implementation of an IPSec network requires advance planning before beginning configuration of individual routers.

Task 1—Prepare for IKE and IPSec

Cisco.com

Step 1—Determine IKE (IKE Phase 1) policy.
Step 2—Determine IPSec (IKE Phase 2) policy.
Step 3—Check the current configuration.
```
show running-configuration
show crypto isakmp policy
show crypto map
```
Step 4—Ensure that the network works without encryption.
```
ping
```
Step 5—Ensure that ACLs are compatible with IPSec.
```
show access-lists
```

SECUR 1.1—9-51

Configuring IPSec encryption can be complicated. You must plan in advance if you desire to configure IPSec encryption correctly the first time and minimize misconfiguration. You should begin this task by defining the IPSec security policy based on the overall company security policy. Some planning steps are as follows:

Step 1   Determine IKE (IKE phase one) policy—Determine the IKE policies between IPSec peers based on the number and location of the peers.

Step 2   Determine IPSec (IKE phase two) policy—Identify IPSec peer details such as IP addresses, IPSec transform sets, and IPSec modes. You then configure crypto maps to gather all IPSec policy details together.

Step 3   Check the current configuration—Use the **show running-configuration**, **show isakmp [policy]**, and **show crypto map** commands, and the many other **show** commands to check the current configuration of the router. This is covered later in this lesson.

Step 4   Ensure the network works without encryption (no excuses!)—Ensure that basic connectivity has been achieved between IPSec peers using the desired IP services before configuring IPSec. You can use the **ping** command to check basic connectivity.

Step 5   Ensure access control lists (ACLs) are compatible with IPSec—Ensure that perimeter routers and the IPSec peer router interfaces permit IPSec traffic. In this step you need to enter the **show access-lists** command.

Step 1—Determine IKE (IKE Phase 1) Policy

Cisco.com

Determine the following policy details:
- ☑ **Key distribution method**
- ☑ **Authentication method**
- ☑ **IPSec peer IP addresses and hostnames**
- ☑ **IKE Phase 1 policies for all peers**
  - – **Encryption algorithm**
  - – **Hash algorithm**
  - – **IKE SA lifetime**
  - **Goal: Minimize misconfiguration.**

SECUR 1.1—9-52

Configuring IKE is complicated. You should determine the IKE policy details to enable the selected authentication method, then configure it. Having a detailed plan lessens the chances of improper configuration. Some planning steps include the following:

■ Determine the key distribution method—Determine the key distribution method based on the numbers and locations of IPSec peers. For a small network, you may wish to manually distribute keys. For larger networks, you may wish to use a CA server to support scalability of IPSec peers. You must then configure the Internet Security Association Key Management Protocol (ISAKMP) to support the selected key distribution method.

■ Determine the authentication method—Choose the authentication method based on the key distribution method. Cisco IOS software supports either pre-shared keys, RSA encrypted nonces, or RSA signatures to authenticate IPSec peers. This lesson focuses on using pre-shared keys.

■ Identify IPSec peer's IP addresses and host names—Determine the details of all of the IPSec peers that will use ISAKMP and pre-shared keys for establishing security associations (SAs). You will use this information to configure IKE.

■ Determine ISAKMP policies for peers—An ISAKMP policy defines a combination or suite of security parameters to be used during the ISAKMP negotiation. Each ISAKMP negotiation begins by each peer agreeing on a common (shared) ISAKMP policy. The ISAKMP policy suites must be determined in advance of configuration. You must then configure IKE to support the policy details you determined. Some ISAKMP policy details include:

— Encryption algorithm

— Hash algorithm

— IKE SA lifetime

The goal of this planning step is to gather the precise data you will need in later steps to minimize misconfiguration.

IKE Phase 1 Policy Parameters

Parameter	Strong	Stronger
Encryption algorithm	DES	3DES or AES
Hash algorithm	MD5	SHA-1
Authentication method	Pre-shared	RSA encryption RSA signature
Key exchange	DH Group 1	DH Group 2
IKE SA lifetime	86,400 seconds	< 86,400 seconds

SECUR 1.1—9-53

An IKE policy defines a combination of security parameters used during the IKE negotiation. A group of policies makes up a protection suite of multiple policies that enable IPSec peers to establish IKE sessions and establish SAs with a minimal configuration. The figure shows an example of possible combinations of IKE parameters into either a strong or stronger policy suite.

Create IKE Policies for a Purpose

IKE negotiations must be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations.

After the two peers agree upon a policy, an SA established at each peer identifies the security parameters of the policy. These SAs apply to all subsequent IKE traffic during the negotiation.

You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

Define IKE Policy Parameters

You can select specific values for each IKE parameter per the IKE standard. You choose one value over another based on the security level you desire and the type of IPSec peer you will connect to.

There are five parameters to define in each IKE policy as outlined in the figure, and in the following table. The figure shows the relative strength of each parameter, and the table shows the default values.

Parameter	Accepted Values	Keyword	Default
Message encryption algorithm	DES 3-DES AES	**des** **3des** **aes**	DES
Message integrity (hash) algorithm	SHA-1 (HMAC variant) MD5 (HMAC variant)	**sha** **md5**	SHA-1
Peer authentication method	Pre-shared keys RSA encrypted nonces RSA signatures	**pre-share** **rsa-encr** **rsa-sig**	RSA signatures
Key exchange parameters (Diffie-Hellman group identifier)	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	**1** **2**	768-bit Diffie-Hellman
ISAKMP-established security association's lifetime	Can specify any number of seconds	**—**	86400 seconds (one day)

You can select specific values for each ISAKMP parameter per the ISAKMP standard. You choose one value over another based on the security level you desire and the type of IPSec peer you will connect to. There are five parameters to define in each IKE policy as presented in the following table. The table shows the relative strength of each parameter.

Parameter	Strong	Stronger
Message encryption algorithm	DES	3DES or AES
Message integrity (hash) algorithm	MD5	SHA-1
Peer authentication method	Pre-share	RSA Encryption RSA Signature
Key exchange parameters (Diffie-Hellman group identifier)	D-H Group 1	D-H Group 2
ISAKMP-established security association's lifetime	86400 seconds	<86400 seconds

IKE Policy Example
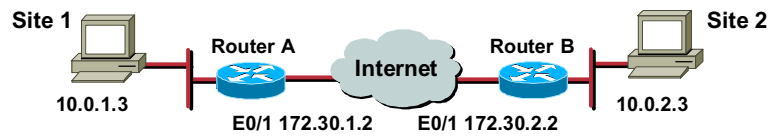
Site 1 — 10.0.1.3 — Router A — E0/1 172.30.1.2 — Internet — Router B — E0/1 172.30.2.2 — 10.0.2.3 — Site 2

Parameter	Site 1	Site 2
Encryption algorithm	DES	DES
Hash algorithm	MD5	MD5
Authentication method	Pre-shared keys	Pre-shared keys
Key exchange	DH Group 1	DH Group 1
IKE SA lifetime	86400 seconds	86400 seconds
Peer IP address	172.30.2.2	172.30.1.2

SECUR 1.1—9-54

You should determine IKE policy details for each peer before configuring IKE. The figure shows a summary of IKE policy details that will be configured in examples and in labs for this lesson. The authentication method of pre-shared keys is covered in this lesson.

Step 2—Determine IPSec (IKE Phase 2) Policy

Cisco.com

Determine the following policy details:

☑ **IPSec algorithms and parameters for optimal security and performance**

☑ **Transforms and, if necessary, transform sets**

☑ **IPSec peer details**

☑ **IP address and applications of hosts to be protected**

☑ **Manual or IKE-initiated SAs**

Goal: Minimize misconfiguration.

SECUR 1.1—9-55

An IPSec policy defines a combination of IPSec parameters used during the IPSec negotiation. Planning for IPSec (IKE phase two) is another important step you should complete before actually configuring IPSec on a Cisco router. Policy details to determine at this stage include:

■ Select IPSec algorithms and parameters for optimal security and performance—Determine what type of IPSec security to use when securing interesting traffic. Some IPSec algorithms require you to make tradeoffs between high performance and stronger security. Some algorithms have import and export restrictions that may delay or prevent implementation of your network.

■ Select transforms and, if necessary, transform sets—Use the IPSec algorithms and parameters previously decided upon to help select IPSec transforms, transform sets, and modes of operation.

■ Identify IPSec peer details—Identify the IP addresses and host names of all IPSec peers to which you will connect.

■ Determine IP address and applications of hosts to be protected—Decide which hosts IP addresses and applications should be protected at the local peer and remote peer.

■ Select manual or IKE-initiated SAs—Choose whether SAs are manually established or are established via IKE.

The goal of this planning step is to gather the precise data you will need in later steps to minimize misconfiguration.

Cisco IOS software supports the following IPSec transforms:

```
RouterA(config)# crypto ipsec transform-set
    transform-set-name ?
ah-md5-hmac    AH-HMAC-MD5 transform
ah-sha-hmac    AH-HMAC-SHA transform
comp-lzs       IP compression using LZS compression algorithm
esp-3des       ESP transform using 3DES(EDE) cipher (168 bits)
esp-aes        ESP transform using AES cipher
esp-des        ESP transform using DES cipher (56 bits)
esp-md5-hmac   ESP transform using HMAC-MD5 auth
esp-null       ESP transform w/o cipher
esp-sha-hmac   ESP transform using HMAC-SHA auth
```

Cisco IOS software supports the following IPSec transforms as shown in the following tables.

Transform	Description
ah-md5-hmac	AH-HMAC-MD5 transform
ah-sha-hmac	AH-HMAC-SHA transform

Note: AH is rarely used because authentication is now available with the esp-sha-hmac and esp-md5-hmac transforms. AH is also not compatible with NAT or PAT.

Transform	Description
esp-des	ESP transform using DES cipher (56 bits).
esp-3des	ESP transform using 3DES(EDE) cipher (168 bits).
esp-aes	ESP transform using AES cipher (128, 192, or 256 bits).
esp-md5-hmac	ESP transform with HMAC-MD5 authentication used with an esp-des or esp-3des transform to provide additional integrity of ESP packet.
esp-sha-hmac	ESP transform with HMAC-SHA authentication used with an esp-des or esp-3des transform to provide additional integrity of ESP packet.
esp-null	ESP transform without a cipher. May be used in combination with esp-md5-hmac or esp-sha-hmac if one wants ESP authentication with no encryption.

Caution: Never use esp-null in a production environment because it does not protect data flows.

Examples of acceptable transforms that can be combined into sets are shown in the table.

Transform Type	Allowed Transform Combinations
AH Transform (Choose up to One)	■ ah-md5-hmac—AH with the MD5 (HMAC variant) authentication algorithm ■ ah-sha-hmac—AH with the SHA (HMAC variant) authentication algorithm
ESP Encryption Transform (Choose up to One)	■ esp-des—ESP with the 56-bit DES encryption algorithm ■ esp-3des—ESP with the 168-bit DES encryption algorithm (3DES or Triple DES) ■ esp-aes—ESP transform using AES cipher (128, 192, or 256 bits) ■ esp-null—Null encryption algorithm
ESP Authentication Transform (Choose up to One)	■ esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm ■ esp-sha-hmac—ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform	comp-lzs—IP compression with the LZS algorithm.

The Cisco IOS command parser prevents you from entering invalid combinations; for example, after you specify an AH transform, it does not allow you to specify another AH transform for the current transform set.

IPSec Policy Example

Site 1 — 10.0.1.3 — Router A — E0/1 172.30.1.2 — Internet — E0/1 172.30.2.2 — Router B — 10.0.2.3 — Site 2
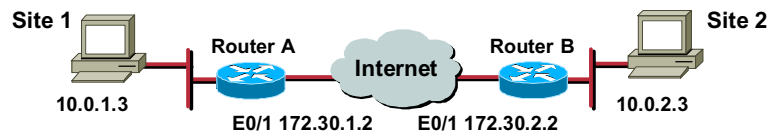
Policy	Site 1	Site 2
Transform set	ESP-DES, tunnel	ESP-DES, tunnel
Peer hostname	RouterB	RouterA
Peer IP address	172.30.2.2	172.30.1.2
Hosts to be encrypted	10.0.1.3	10.0.2.3
Traffic (packet) type to be encrypted	TCP	TCP
SA establishment	Ipsec-isakmp	Ipsec-isakmp

Determining network design details includes defining a more detailed IPSec policy for protecting traffic. You can then use the detailed policy to help select IPSec transform sets and modes of operation. Your IPSec policy should answer the following questions:

■ What protections are required or are acceptable for the protected traffic?

■ Which IPSec transforms or transforms sets should be used?

■ What are the peer IPSec endpoints for the traffic?

■ What traffic should or should not be protected?

■ Which router interfaces are involved in protecting internal nets and external nets?

■ How are SAs set up (manual or IKE negotiated) and often should the SAs be re-negotiated?

The figure shows a summary of IPSec encryption policy details that will be configured in examples in this lesson. Details about IPSec transforms are covered in a later topic in this lesson. The example policy specifies that TCP traffic between the hosts should be encrypted by IPSec using DES.

Identify IPSec Peers

Cisco router

Remote user with
Cisco VPN Client

Cisco router

Cisco
PIX Firewall

Other vendor's
IPSec peers

CA server
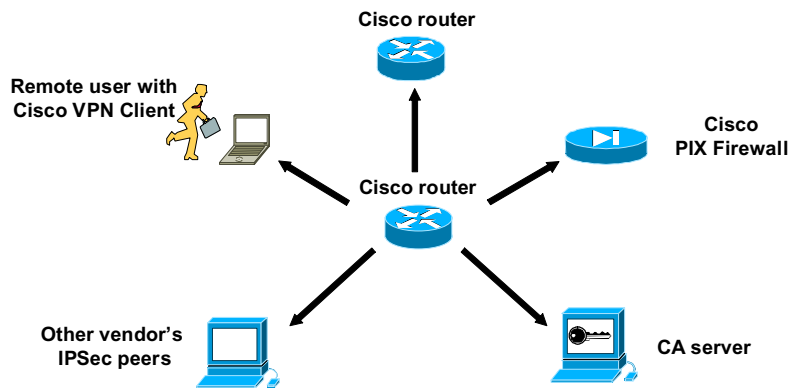
SECUR 1.1—9-58

An important part of determining the IPSec policy is to identify the IPSec peer the Cisco router will communicate with. The peer must support IPSec as specified in the RFCs as supported by Cisco IOS. Many different types of peers are possible. Before configuration identify all the potential peers and their VPN capabilities. Possible peers include, but are not limited to the following:

■ Other Cisco routers

■ The Cisco PIX Firewall

■ The Cisco VPN client

■ CA servers if they are used

■ Other vendor's IPSec products that conform to IPSec RFCs

Step 3—Check Current Configuration

Cisco.com

Site 1 10.0.1.3 — **Router A** 172.30.1.2 — **Internet** — **Router B** 172.30.2.2 — **Site 2** 10.0.2.3
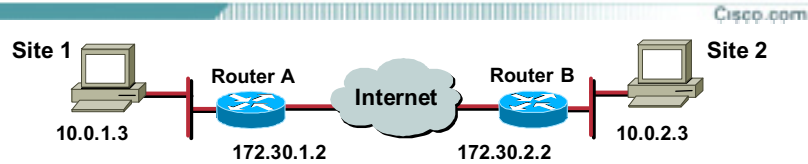
router#

```
show running-config
```

- View router configuration for existing IPSec policies

router#

```
show crypto isakmp policy
```

- View default and any configured IKE Phase 1 policies

```
RouterA# show crypto isakmp policy
Default protection suite
    encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
    hash algorithm:         Secure Hash Standard
    authentication method:  Rivest-Shamir-Adleman Signature
    Diffie-Hellman Group:   #1 (768 bit)
    lifetime:               86400 seconds, no volume limit
```

The current Cisco router configuration should be checked to see if there are any IPSec policies already configured that are useful for, or may interfere with, the IPSec policies you plan to configure. Previously configured IKE and IPSec policies and details can and should be used if possible to save configuration time. However, previously configured IKE and IPSec policies and details can make troubleshooting more difficult if problems arise.

You can see if any IKE policies have previously been configured starting with the **show running-config** command. You can also use the variety of **show** commands specific to IPSec. For example, you can use the **show crypto isakmp policy command,** as shown in the figure, to examine IKE policies. The default protection suite seen here is available for use without modification. You can also use the other available **show** commands covered in other topics of this lesson to view IKE and IPSec configuration.

Step 3—Check Current Configuration (cont.)

Site 1

Router A

Internet

Router B

Site 2

10.0.1.3

172.30.1.2

172.30.2.2

10.0.2.3
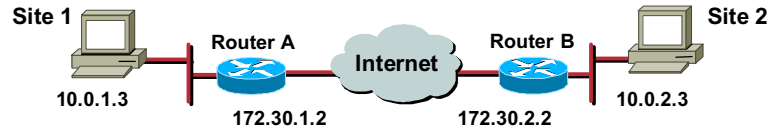
router#

```
show crypto map
```

• **View any configured crypto maps**

```
RouterA# show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
        Peer = 172.30.2.2
        Extended IP access list 102
            access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
        Current peer: 172.30.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
     Transform sets={ mine, }
```

The **show crypto map** command shown in the figure is useful for viewing any previously configured crypto maps (crypto maps are covered in detail later in this lesson). Previously configured maps can and should be used to save configuration time. However, previously configured crypto maps can interfere with the IPSec policy you are trying to configure.

Step 3—Check Current Configuration (cont.)

Cisco.com

Site 1

Router A

Internet

Router B

Site 2

10.0.1.3

172.30.1.2

172.30.2.2

10.0.2.3

```
router#
show crypto ipsec transform-set
```

• **View any configured transform sets**

```
RouterA# show crypto ipsec transform-set mine
Transform set mine: { esp-des   }
   will negotiate = { Tunnel,  },
```

You can also use the **show crypto ipsec transform-set** command to view previously configured transform sets. Previously configured transforms can, and should, be used to save configuration time.

Step 4—Ensure the Network Works

Cisco Router B
172.30.2.2

Remote user with
Cisco Unified
VPN Client

Cisco router

Cisco Router A
172.30.1.2

Cisco
PIX Firewall

Other vendor's
IPSec peers

CA server

```
RouterA# ping 172.30.2.2
```
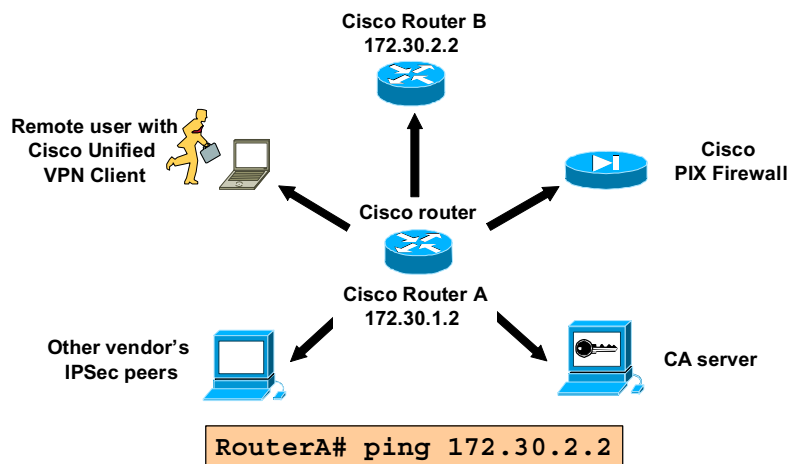
SECUR 1.1—9-62

Basic connectivity between peers must be checked before you begin configuring IPSec.

The router **ping** command can be used to test basic connectivity between IPSec peers. While a successful ICMP echo (ping) will verify basic connectivity between peers, you should ensure the network works with any other protocols or ports you want to encrypt such as Telnet, FTP, or SQL*NET before beginning IPSec configuration.

After IPSec is activated, basic connectivity troubleshooting can be difficult because the security configuration may mask a more fundamental networking problem. Previous security settings could result in no connectivity.

Step 5—Ensure that ACLs Are Compatible with IPSec

Cisco.com

IKE
AH
ESP

Site 1
10.0.1.3
Router A
E0/1 172.30.1.2
Internet
Router B
E0/1 172.30.2.2
Site 2
10.0.2.3
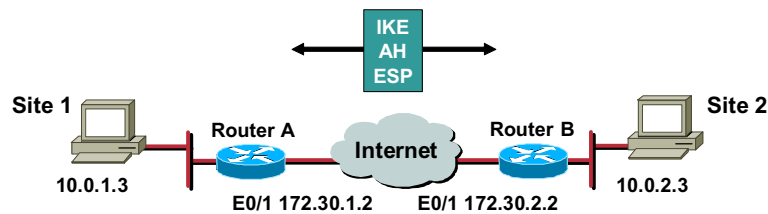
```
RouterA# show access-lists
access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq
  isakmp
```

• **Ensure that protocols 50 and 51 and UDP port 500 traffic is not blocked at interfaces used by IPSec**

SECUR 1.1—9-63

You will need to ensure existing access lists (ACLs) on perimeter routers, the PIX Firewall, or other routers do not block IPSec traffic. Perimeter routers typically implement a restrictive security policy with ACLs, where only specific traffic is permitted and all other traffic is denied. Such a restrictive policy blocks IPSec traffic, so you need to add specific **permit** statements to the ACL to allow IPSec traffic.

Ensure that your ACLs are configured so that ISAKMP, Encapsulating Security Payload (ESP), and Authentication Header (AH) traffic is not blocked at interfaces used by IPSec. ISAKMP uses UDP port 500. ESP is assigned IP protocol number 50, and AH is assigned IP protocol number 51. In some cases, you might need to add a statement to router ACLs to explicitly permit this traffic. You may need to add the ACL statements to the perimeter router by performing the following steps:

Step 1 Examine the current ACL configuration at the perimeter router and determine if it will block IPSec traffic:

RouterA# **show access-lists**

Step 2 Add ACL entries to permit IPSec traffic. To do this copy the existing ACL configuration and paste it into a text editor as follows:

1. Copy the existing ACL configuration and paste it into a text editor.

2. Add the ACL entries to the top of the list in the text editor.

3. Delete the existing ACL with the **no access-list** *access-list number* command.

4. Enter configuration mode and copy and paste the new ACL into the router.

5. Verify the ACL is correct with the **show access-lists** command.

A concatenated example showing ACL entries permitting IPSec traffic for RouterA is as follows:

```
RouterA# show running-config
!
interface Ethernet0/1
 ip address 172.30.1.2 255.255.255.0
 ip access-group 102 in
!
access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
```

Note: The protocol keyword of **esp** equals the ESP protocol (number 50) and the keyword of **ahp** equals the AH protocol (number 51), and the **isakmp** keyword equals UDP port 500.

Task 2—Configure IKE

The next major task in configuring Cisco IOS IPSec is to configure the IKE parameters gathered earlier. This topic presents the steps used to configure IKE policies.

Task 2—Configure IKE

Cisco.com

Step 1—Enable or disable IKE.
`crypto isakmp enable`

Step 2—Create IKE policies.
`crypto isakmp policy`

Step 3—Configure pre-shared keys.
`crypto isakmp key`

Step 4—Verify the IKE configuration.
`show crypto isakmp policy`

SECUR 1.1—9-65

Configuring IKE consists of the following essential steps and commands:

Step 1   Enable or disable IKE with the **crypto isakmp enable** command.

Step 2   Create IKE policies with the **crypto isakmp policy** commands.

Step 3   Configure pre-shared keys with the **crypto isakmp key** and associated commands.

Step 4   Verify the IKE configuration with the **show crypto isakmp policy** command.

Step 1—Enable or Disable IKE

Site 1
10.0.1.3

Router A
172.30.1.2

Internet

Router B
172.30.2.2

Site 2
10.0.2.3
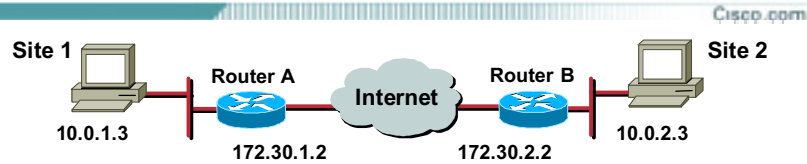
```
router(config)#
```
```
[no] crypto isakmp enable
```

```
RouterA(config)# no crypto isakmp enable
RouterA(config)# crypto isakmp enable
```

- **Globally enables or disables IKE at your router.**
- **IKE is enabled by default.**
- **IKE is enabled globally for all interfaces at the router.**
- **Use the** no **form of the command to disable IKE.**
- **An ACL can be used to block IKE on a particular interface.**

SECUR 1.1—9-66

The first step in configuring IKE is to enable or disable ISAKMP. ISAKMP is globally enabled and disabled with the **crypto isakmp enable** command. ISAKMP is enabled by default. Use the **no** form of the command to disable ISAKMP.

ISAKMP does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router. You may choose to block ISAKMP access on interfaces not used for IPSec to prevent possible denial of service attacks by using an ACL statement that blocks UDP port 500 on the interfaces.

Step 2—Create IKE Policies

Cisco.com

Site 1   Router A   Internet   Router B   Site 2

10.0.1.3   172.30.1.2   172.30.2.2   10.0.2.3
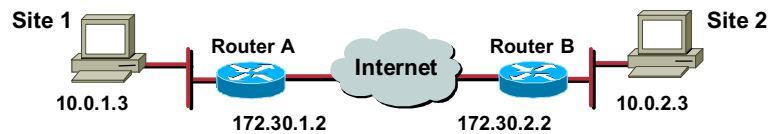
router(config)#

```
crypto isakmp policy priority
```

• **Defines an IKE policy, which is a set of parameters used during IKE negotiation**

• **Invokes the config-isakmp command mode**

```
RouterA(config)# crypto isakmp policy 110
```

The next major step in configuring Cisco IOS ISAKMP support is to define a suite of ISAKMP policies. The goal of defining a suite of IKE policies is to establish ISAKMP peering between two IPSec endpoints. Use the IKE policy details gathered during the planning task.

Use the **crypto isakmp policy** command to define an IKE policy. IKE policies define a set of parameters used during the IKE negotiation. Use the **no** form of this command to delete an IKE policy. The command syntax is as follows:

```
crypto isakmp policy priority
```

Command	Description
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.

This command invokes the ISAKMP policy configuration (config-isakmp) command mode.

Note:	Assign the most secure policy the lowest priority number so that the most secure policy will find a match before any less-secure policies are configured.

Create IKE Policies with the *crypto isakmp* Command

Site 1 `10.0.1.3` — Router A — Internet — Router B — Site 2 `10.0.2.3`

`172.30.2.2`

Policy 110
DES
MD5
Pre-share
86400

Tunnel
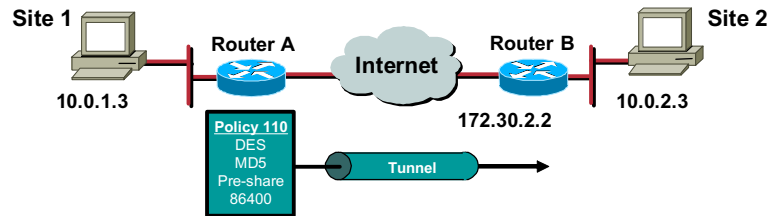
router(config)#

```
crypto isakmp policy priority
```

• **Defines the parameters within the IKE policy 110**

```
RouterA(config)# crypto isakmp policy 110
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# encryption des
RouterA(config-isakmp)# group 1
RouterA(config-isakmp)# hash md5
RouterA(config-isakmp)# lifetime 86400
```

SECUR 1.1—9-68

The **crypto isakmp policy** command invokes the ISAKMP policy configuration command mode (config-isakmp) where you can set ISAKMP parameters. If you do not specify one of these commands for a policy, the default value will be used for that parameter. While in the config-isakmp command mode, the keywords shown in the table are available to specify the parameters in the policy.

Command	Keywords	Accepted Values	Default Value	Description
encryption	des 3des aes	56-bit only 168-bit Choose 128-, 192-, or 256-bit	des	Message encryption algorithm.
hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha	Message integrity (Hash) algorithm.
authen	rsa-sig rsa-encr pre-share	RSA signatures RSA encrypted nonces pre-shared keys	rsa-sig	Peer authentication method.
group	1 2	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1	Key exchange parameters (Diffie-Hellman group identifier).
lifetime	-	Can specify any number of seconds	86,400 seconds (one day)	ISAKMP-established SA's lifetime. You can usually leave this value at the default.

You can configure multiple ISAKMP policies on each peer participating in IPSec. ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPSec.

IKE Policy Negotiation

Site 1   Router A   Internet   Router B   Site 2

10.0.1.3   10.0.2.3

RouterA(config)#
```
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp policy 200
  authentication rsa-sig
  hash sha
crypto isakmp policy 300
  authentication pre-share
  hash md5
```

RouterB(config)#
```
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp policy 200
  authentication rsa-sig
  hash sha
crypto isakmp policy 300
  authentication rsa-sig
  hash md5
```

• **The first two policies in each router can be successfully negotiated, but the last one cannot.**

ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPSec.

When the ISAKMP negotiation begins in IKE phase one main mode, ISAKMP looks for an ISAKMP policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match with its policies. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies in its ISAKMP policy suite. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime from the remote peer's policy is used.) Assign the most secure policy the lowest priority number so that the most secure policy will find a match before any less secure policies configured.

If no acceptable match is found, ISAKMP refuses negotiation and IPSec is not established. If a match is found, ISAKMP completes the main mode negotiation, and IPSec SAs are created during IKE phase two quick mode.

Configure ISAKMP Identity

Site 1 | Router A | Internet | Router B | Site 2
10.0.1.3 | 172.30.1.2 | | 172.30.2.2 | 10.0.2.3
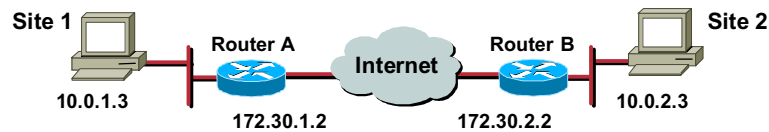
router(config)#

```
crypto isakmp identity {address | hostname}
```

- **Defines whether ISAKMP identity is done by IP address or hostname**
- **Use consistently across ISAKMP peers**

SECUR 1.1—9-70

IPSec peers authenticate each other during ISAKMP negotiations using the pre-shared key and the ISAKMP identity. The identity can either be the router's IP address or host name. Cisco IOS software uses the IP address identity method by default. A command indicating the address mode does not appear in the router configuration.

If you choose to use the host name identity method, you must specify the method with the **crypto isakmp identity** global configuration command. Use the **no** form of this command to reset the ISAKMP identity to the default value (address). The command syntax is as follows:

```
crypto isakmp identity {address | hostname}
```

Command	Description
address	Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during ISAKMP negotiations.
	The keyword is typically used when there is only one interface that will be used by the peer for ISAKMP negotiations, and the IP address is known.
hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, **myhost.domain.com**).
	The keyword should be used if there is more than one interface on the peer that might be used for ISAKMP negotiations, or if the interface's IP address is unknown (such as with dynamically-assigned IP addresses).

If you use the host name identity method, you may need to specify the host name for the remote peer if a DNS server is not available for name resolution. An example of this follows:

```
RouterA(config)# ip host RouterB.domain.com 172.30.2.1
```

Step 3—Configure Pre-Shared Keys
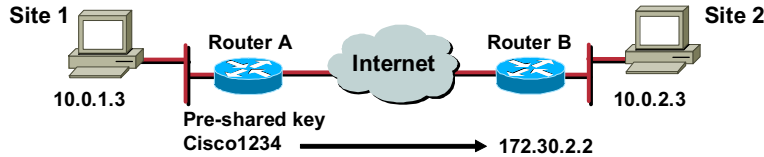
```
router(config)#
```
```
crypto isakmp key keystring address peer-address
```

```
router(config)#
```
```
crypto isakmp key keystring hostname hostname
```

```
RouterA(config)# crypto isakmp key cisco1234
  address 172.30.2.2
```

- **Assigns a keystring and the peer address.**
- **The peer's IP address or host name can be used.**

Configure a pre-shared authentication key with the **crypto isakmp key** global configuration command. You must configure this key whenever you specify pre-shared keys in an ISAKMP policy. Use the **no** form of this command to delete a pre-shared authentication key. The command syntax is as follows:

```
crypto isakmp key keystring address peer-address
```

```
crypto isakmp key keystring hostname peer-hostname
```

Command	Description
keystring	Specify the pre-shared key. Use any combination of alphanumeric characters up to 128 bytes. This pre-shared key must be identical at both peers.
peer-address	Specify the IP address of the remote peer.
hostname	Specify the host name of the remote peer. This is the peer's host name concatenated with its domain name (for example, myhost.domain.com).

Note:	A given pre-shared key is shared between two peers. At a given peer you could specify the same key to share with multiple remote peers; however, a more secure approach is to specify different keys to share between different pairs of peers.

The following configuration example shows ISAKMP and pre-shared keys for routerA and routerB. Note that the keystring of *cisco1234* matches. The address identity method is specified. The ISAKMP policies are compatible. Default values do not have to be configured.

```
RouterA(config)# crypto isakmp key cisco1234 address 172.30.2.1
RouterA(config)# crypto isakmp policy 110
RouterA(config-isakmp)# hash md5
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# exit

RouterB(config)# crypto isakmp key cisco1234 address 172.30.1.1
RouterB(config)# crypto isakmp policy 110
RouterB(config-isakmp)# hash md5
RouterB(config-isakmp)# authentication pre-share
RouterB(config-isakmp)# exit
```

Step 4—Verify the IKE Configuration

Site 1 / Router A / Internet / Router B / Site 2
10.0.1.3 / 10.0.2.3

```
RouterA# show crypto isakmp policy
Protection suite of priority 110
     encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #1 (768 bit)
     lifetime:               86400 seconds, no volume limit
Default protection suite
     encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
     hash algorithm:         Secure Hash Standard
     authentication method:  Rivest-Shamir-Adleman Signature
     Diffie-Hellman group:   #1 (768 bit)
     lifetime:               86400 seconds, no volume limit
```

- **Displays configured and default IKE policies**

SECUR 1.1—9-72

You can use the **show crypto isakmp policy** command to display configured and default policies. The resultant ISAKMP policy for RouterA is as follows and as shown in the figure. RouterB's configuration is identical.

```
RouterA# show crypto isakmp policy

Protection suite of priority 110

      encryption algorithm:    DES - Data Encryption Standard (56 bit
                                keys).

      hash algorithm:          Message Digest 5

      authentication method:   Pre-Shared Key

      Diffie-Hellman group:    #1 (768 bit)

      lifetime:                86400 seconds, no volume limit

Default protection suite

      encryption algorithm:    DES - Data Encryption Standard (56 bit
                                keys).

      hash algorithm:          Secure Hash Standard

      authentication method:   Rivest-Shamir-Adleman Signature

      Diffie-Hellman group:    #1 (768 bit)

      lifetime:                86400 seconds, no volume limit
```

Task 3—Configure IPSec

The next major task in configuring Cisco IOS IPSec is to configure the IPSec parameters previously gathered. This topic presents the steps used to configure IPSec.

Task 3—Configure IPSec

Cisco.com

Step 1—Configure transform set suites.

`crypto ipsec transform-set`

Step 2—Configure global IPSec SA lifetimes.

`crypto ipsec security-association lifetime`

Step 3—Create crypto ACLs.

`access-list`

The general tasks and commands used to configure IPSec encryption on Cisco routers are summarized as follows. Subsequent topics of this lesson discuss each configuration step in detail.

Step 1   Configure transform set suites with the **crypto ipsec transform-set** command.

Step 2   Configure global IPSec security association lifetimes with the **crypto ipsec security-association lifetime** command.

Step 3   Configure crypto ACLs with the **access-list** command.

Task 3—Configure IPSec (cont.)

Cisco.com

Step 4—Create crypto maps.

```
crypto map
```

Step 5—Apply crypto maps to interfaces.

```
interface serial0
crypto map
```

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

SECUR 1.1—9-75

The final steps used to configure IPSec parameters for IKE pre-shared keys are as follows:

Step 1 Configure crypto maps with the **crypto map** command.

Step 2 Apply the crypto maps to the terminating/originating interface with the **interface** and **crypto map** commands.

Step 1—Configure Transform Set Suites

The first major step in configuring Cisco IOS IPSec is to use the IPSec security policy to define a transform set.

A transform set is a combination of individual IPSec transforms designed to enact a specific security policy for traffic. During the ISAKMP IPSec SA negotiation that occurs in IKE phase two quick mode, the peers agree to use a particular transform set for protecting a particular data flow. Transform sets combine the following IPSec factors:

■ Mechanism for payload authentication: AH transform

■ Mechanism for payload encryption: ESP transform

■ IPSec mode (transport versus tunnel)

Transform sets equal a combination of an AH transform, an ESP transform, and the IPSec mode (either tunnel or transport mode). Transform sets are limited to one AH transform and one or two ESP transforms. Define a transform set with the **crypto ipsec transform-set** global configuration command. To delete a transform set, use the **no** form of the command. The command syntax is as follows:

```
crypto ipsec transform-set transform-set-name transform1 [transform2
[transform3]]
```

A description of each follows:

■ *transform-set-name*—Specify the name of the transform set to create (or modify).

■ *transform1*, *transform2*, *transform3*—Specify up to three transforms. These transforms define the IPSec security protocol(s) and algorithm(s).

The command invokes the crypto-transform configuration mode.

You can configure multiple transform sets and then specify one or more of the transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by that crypto map entry's ACL. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both peers' IPSec SAs.

When ISAKMP is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

Edit Transform Sets

Use the following steps if you need to edit a transform set:

Step 1   Delete the transform set from the crypto map.

Step 2   Delete the transform set from global configuration.

Step 3   Reenter the transform set with corrections.

Step 4   Assign the transform set to a crypto map.

Step 5   Clear the SA database.

Step 6   Observe the SA negotiation and ensure it works properly.

Transform Set Negotiation

Cisco.com
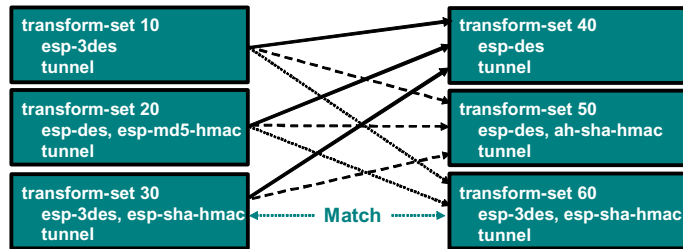
Site 1   Router A   Internet   Router B   Site 2

10.0.1.3   10.0.2.3

transform-set 10
    esp-3des
    tunnel

transform-set 20
    esp-des, esp-md5-hmac
    tunnel

transform-set 30
    esp-3des, esp-sha-hmac
    tunnel

transform-set 40
    esp-des
    tunnel

transform-set 50
    esp-des, ah-sha-hmac
    tunnel

transform-set 60
    esp-3des, esp-sha-hmac
    tunnel

Match

• **Transform sets are negotiated during IKE Phase 2.**

SECUR 1.1—9-78

Transform sets are negotiated during quick mode in IKE phase two using the transform sets you previously configured. You can configure multiple transform sets, then specify one or more of the transform sets in a crypto map entry. Configure the transforms from most to least secure as per your policy. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by that crypto map entry's ACL.

During the negotiation, the peers search for a transform set that is the same at both peers as illustrated in the figure. Each of RouterA's transform sets are compared against each of RouterB's transform sets in succession. RouterA's transform sets 10, 20, and 30 are compared with RouterB's transform set 40. The result is no match. All of RouterA's transform sets are then compared against RouterB's transform. Ultimately, RouterA's transform set 30 matches RouterB's transform set 60. When such a transform set is found, it is selected and is applied to the protected traffic as part of both peer's IPSec SAs. IPSec peers agree on one transform proposal per SA (unidirectional).

The following table describes the various types of allowed transform combinations for IOS versions ≥ 12.2.

Transform types	Allowed combinations
AH transform	Select one of the following: ■ ah-md5-hmac—AH with the MD5 (HMAC variant) authentication algorithm ■ ah-sha-hmac—AH with the SHA (HMAC variant) authentication algorithm
ESP encryption transform	Select one of the following: ■ esp-des—ESP with the 56-bit DES encryption algorithm ■ esp-3des—ESP with the 168-bit DES encryption algorithm (3DES or Triple DES) ■ esp-aes—ESP with either 128, 192, or 256-bit encryption algorithm ■ esp-null—Null encryption algorithm

Transform types	Allowed combinations
ESP authentication transform	Select one of the following: ■ esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm ■ esp-sha-hmac—ESP with the SHA (HMAC variant) authentication algorithm
IP compression transform	comp-lzs—IP compression with the LZS algorithm

Step 2—Configure Global IPSec Security Association Lifetimes

Both global and interface-specific SA lifetimes can be created. This topic covers how to configure global SAs.

***crypto ipsec security-association lifetime* Command**

Site 1 ──── Router A ──── Internet ──── Router B ──── Site 2

10.0.1.3   10.0.2.3

```
router(config)#
crypto ipsec security-association lifetime
    {seconds seconds | kilobytes kilobytes}
```

```
RouterA(config)# crypto ipsec security-association
lifetime 86400
```

- Configures global IPSec SA lifetime values used when negotiating IPSec security associations.
- IPSec SA lifetimes are negotiated during IKE Phase 2.
- You can optionally configure interface specific IPSec SA lifetimes in crypto maps.
- IPSec SA lifetimes in crypto maps override global IPSec SA lifetimes.

SECUR 1.1—9-80

The IPSec security association lifetime determines how long IPSec SAs remain valid before they are renegotiated. Cisco IOS software supports a global lifetime value that applies to all crypto maps. The global lifetime value can be overridden within a crypto map entry. You can change global IPSec security association lifetime values using the **crypto ipsec security-association lifetime** global configuration command. To reset a lifetime to the default value, use the **no** form of the command. The command syntax is as follows:

```
crypto ipsec security-association lifetime {seconds seconds | kilobytes
kilobytes}
```

Command	Description
seconds *seconds*	Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour).
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.

It is recommended that you use the default lifetime values. Individual IPSec SA lifetimes can be configured using crypto maps, which are covered in a later topic in this lesson.

Global Security Association Lifetime Examples

Cisco.com

```
RouterA(config)# crypto ipsec security-association lifetime
kilobytes 1382400
```

```
RouterA(config)# crypto ipsec security-association lifetime
seconds 2700
```

• **When a security association expires, a new one is negotiated without interrupting the data flow.**

SECUR 1.1—9-81

The figure shows an example global SA lifetime. A new SA will be negotiated after 2700 seconds (45 minutes).

Step 3—Create Crypto ACLs

Crypto ACLs are used to define which IP traffic is or is not protected by IPSec. This topic covers how to configure crypto ACLs.

Purpose of Crypto ACLs

Site 1

Router A

Internet

Outbound traffic → Encrypt
→ Bypass (clear text)

Permit ←
Bypass (clear text) ← Inbound traffic

- **Outbound—Indicate the data flow to be protected by IPSec**
- **Inbound—Filter out and discard traffic that should have been protected by IPSec**
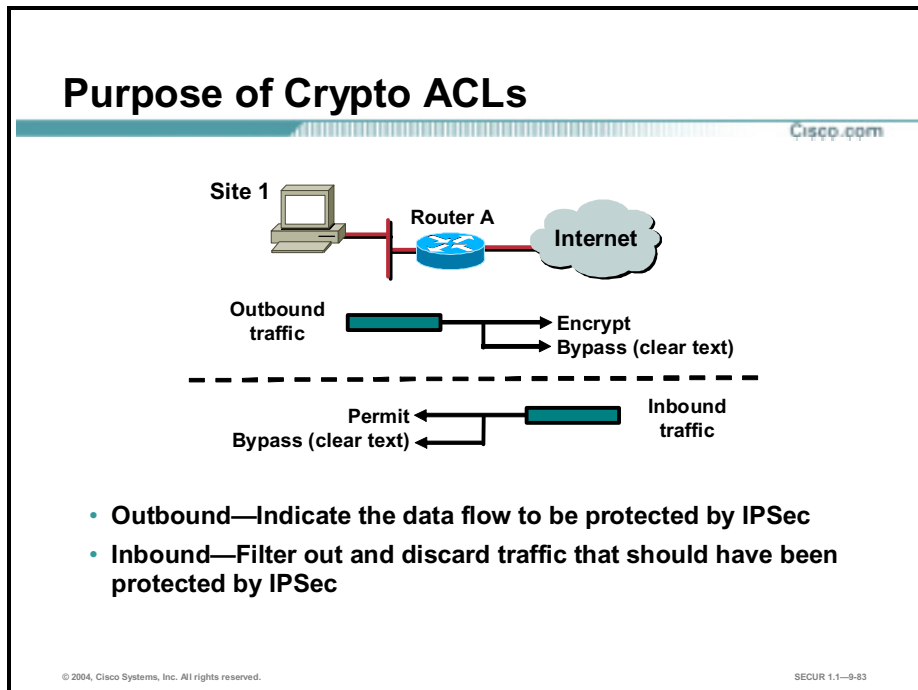
Crypto ACLs perform the following functions:

- Outbound

  — Select outbound traffic to be protected by IPSec.

  — Traffic not selected is sent in clear text.

- Inbound—Process inbound traffic to filter out and discard traffic that should have been protected by IPSec.

Extended IP ACLs for Crypto ACLs

The crypto ACLs identify the traffic flows to be protected. Extended IP ACLs select IP traffic to encrypt by protocol, IP address, network, subnet, and port. Although the ACL syntax is unchanged from extended IP ACLs, the meanings are slightly different for crypto ACLs—*permit* specifies that matching packets must be encrypted; and *deny* specifies that matching packets need not be encrypted. Crypto ACLs behave similar to an extended IP ACL applied to outbound traffic on an interface.

See the command reference for a complete description of this command. The command syntax for the basic form of extended IP access lists is as follows:

```
access-list access-list-number { permit | deny } protocol source source-
wildcard destination destination-wildcard [precedence precedence] [tos tos]
[log]
```

Command	Description
Permit	Causes all IP traffic that matches the specified conditions to be protected by crypto, using the policy described by the corresponding crypto map entry.
Deny	Instructs the router to route traffic in the clear.
source and d*estination*	These are networks, subnets, or hosts.
protocol	Indicates which IP packet type(s) to encrypt.

Note: Although the ACL syntax is unchanged, the meanings are slightly different for crypto ACLs– **permit** specifies that matching packets must be encrypted; **deny** specifies that matching packets need not be encrypted.

Any unprotected inbound traffic that matches a *permit* entry in the crypto ACL for a crypto map entry flagged as IPSec will be dropped, because this traffic was expected to be protected by IPSec.

If you want certain traffic to receive one combination of IPSec protection (authentication only) and other traffic to receive a different combination (both authentication and encryption), create two different crypto ACLs to define the two different types of traffic. These different ACLs are then used in different crypto map entries that specify different IPSec policies.

Warning   It is recommended that you avoid using the **any** keyword to specify source or destination addresses. The **permit any any** statement is strongly discouraged, as this will cause all outbound traffic to be protected (and all protected traffic sent to the peer specified in the corresponding crypto map entry) and will require protection for all inbound traffic. Then, all inbound packets that lack IPSec protection will be silently dropped, including packets for routing protocols, NTP, echo, echo response, and so on.

Try to be as restrictive as possible when defining which packets to protect in a crypto ACL. If you must use the *any* keyword in a permit statement, you must preface that statement with a series of *deny* statements to filter out any traffic (that would otherwise fall within that permit statement) that you do not want to be protected.

In a later step, you will associate a crypto ACL to a crypto map, which in turn is assigned to a specific interface.

Configure Symmetrical Peer Crypto ACLs

Site 1 — 10.0.1.3 — Router A — E0/1 172.30.1.2 — Internet — E0/1 172.30.2.2 — Router B — Site 2 — 10.0.2.3
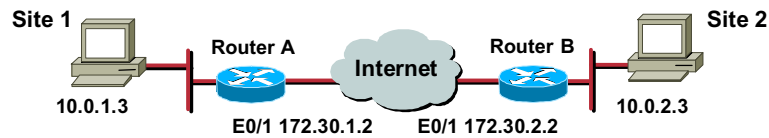
```
RouterA(config)#
access-list 110
permit tcp
    10.0.1.0
    0.0.0.255
    10.0.2.0
    0.0.0.255
```

```
RouterB(config)#
access-list 101
permit tcp
    10.0.2.0
    0.0.0.255
    10.0.1.0
    0.0.0.255
```

• **You must configure mirror-image ACLs.**

SECUR 1.1—9-85

You must configure mirror image crypto ACLs for use by IPSec. Both inbound and outbound traffic is evaluated against the same outbound IPSec ACL. The ACL's criteria is applied in the forward direction to traffic exiting your router, and the reverse direction to traffic entering your router. When a router receives encrypted packets back from an IPSec peer, it uses the same ACL to determine which inbound packets to decrypt by viewing the source and destination addresses in the ACL in reverse order.

The example shown in the figure illustrates why symmetrical ACLs are recommended. For site 1, IPSec protection is applied to traffic between hosts on the 10.0.1.0 network as the data exits RouterA's s0 interface en route to site 2 hosts on the 10.0.2.0 network. For traffic from site 1 hosts on the 10.0.1.0 network to site 2 hosts on the 10.0.2.0 network, the ACL entry on RouterA is evaluated as follows:

■ source = hosts on 10.0.1.0 network

■ dest = hosts on 10.0.2.0 network

For incoming traffic from site 2 hosts on the 10.0.2.0 network to site 1 hosts on the 10.0.1.0 network, that same ACL entry on RouterA is evaluated as follows:

■ source = hosts on 10.0.2.0 network

■ permit = hosts on 10.0.1.0 network

Step 4—Create Crypto Maps

Crypto map entries must be created for IPSec to set up SAs for traffic flows that must be encrypted. This topic looks at the purpose of crypto maps, examines the **crypto map** command, and considers example crypto maps.

Purpose of Crypto Maps

Cisco.com

Crypto maps pull together the various parts configured for IPSec, including:

- **Which traffic should be protected by IPSec**
- **The granularity of the traffic to be protected by a set of SAs**
- **Where IPSec-protected traffic should be sent**
- **The local address to be used for the IPSec traffic**
- **Which IPSec type should be applied to this traffic**
- **Whether SAs are established (manually or via IKE)**
- **Other parameters needed to define an IPSec SA**

SECUR 1.1—9-87

Crypto map entries created for IPSec set up security association parameters, tying together the various parts configured for IPSec, including:

- Which traffic should be protected by IPSec (crypto ACL).

- The granularity of the traffic to be protected by a set of SAs.

- Where IPSec-protected traffic should be sent (who the remote IPSec peer is).

- The local address to be used for the IPSec traffic.

- What IPSec security type should be applied to this traffic (transform sets).

- Whether SAs are established manually or are established via IKE.

- Other parameters that might be necessary to define an IPSec SA.

Crypto Map Parameters

Site 1 — Router A — Internet — Router B — Site 2

10.0.1.3   10.0.2.3

Crypto maps define the following:

• **The ACL to be used.**
• **Remote VPN peers.**
• **Transform set to be used.**
• **Key management method.**
• **SA lifetimes.**

Crypto map → Router interface → Encrypted traffic
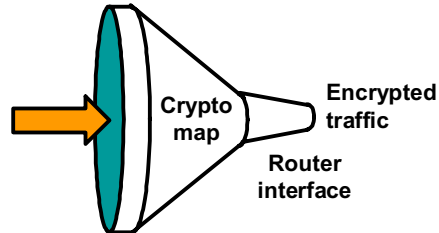
SECUR 1.1—9-88

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of Cisco Encryption Technology (CET), IPSec using IKE, and IPSec with manually configured SA entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

If you create more than one crypto map entry for a given interface, use the sequence number (*seq-num*) of each map entry to rank the map entries: the lower the *seq-num*, the higher the priority. At the interface that has the crypto map set, traffic is evaluated against higher priority map entries first.

You must create multiple crypto map entries for a given interface if any of the following conditions exist:

■ If different data flows are to be handled by separate IPSec peers.

■ If you want to apply different IPSec security to different types of traffic (to the same or separate IPSec peers); for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case, the different types of traffic should have been defined in two separate ACLs, and you must create a separate crypto map entry for each crypto ACL.

■ If you are not using IKE to establish a particular set of security associations, and want to specify multiple ACL entries, you must create separate ACLs (one per permit entry) and specify a separate crypto map entry for each ACL.

Configure IPSec Crypto Maps

Site 1
10.0.1.3

Router A

Internet

Router B

Site 2
10.0.2.3

router(config)#

```
crypto map map-name seq-num ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp
     [dynamic dynamic-map-name]
```

```
RouterA(config)# crypto map mymap 110 ipsec-isakmp
```

• **Use a different sequence number for each peer.**

• **Multiple peers can be specified in a single crypto map for redundancy.**

• **One crypto map per interface.**

SECUR 1.1—9-89

You must use the **crypto map** global configuration command to create or modify a crypto map entry and enter the crypto map configuration mode. Set the crypto map entries referencing dynamic maps to be the lowest priority entries in a crypto map set (that is, have the highest sequence numbers). Use the **no** form of this command to delete a crypto map entry or set. The command syntax is as follows:

```
crypto map map-name seq-num cisco
```

```
crypto map map-name seq-num ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]
```

```
no crypto map map-name [seq-num]
```

A description of each follows:

■ **Cisco**—(Default value.) Indicates that CET will be used instead of IPSec for protecting the traffic specified by this newly specified crypto map entry.

■ *map-name*—The name you assign to the crypto map set.

■ *seq-num*—The number you assign to the crypto map entry.

■ **ipsec-manual**0—Indicates that ISAKMP will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.

■ **ipsec-isakmp**—Indicates that ISAKMP will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.

■ **Dynamic**—(Optional.) Specifies that this crypto map entry references a preexisting static crypto map. If you use this keyword, none of the crypto map configuration commands are available.

■ *dynamic-map-name*—(Optional.) Specifies the name of the dynamic crypto map set that should be used as the policy template.

When you enter the **crypto map** command, you invoke the crypto map configuration mode with the following available commands:

```
router(config-crypto-map)# help
match address [access-list-id | name]
             peer [hostname | ip-address]
             transform-set [set_name(s)]
             security-association [inbound|outbound]
             set
             no
             exit
```

Example Crypto Map Commands

Site 1 — 10.0.1.3
Router A
Internet
Router B — 172.30.2.2
Router C — 172.30.3.2
Site 2 — 10.0.2.3
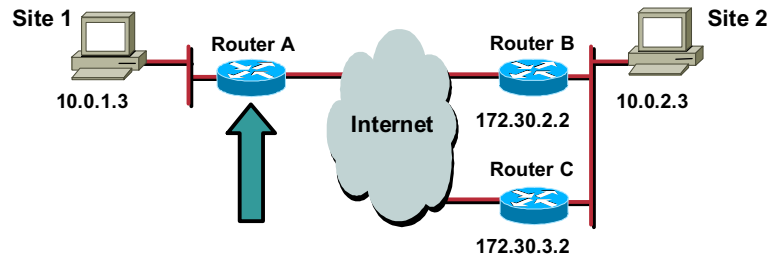
```
RouterA(config)# crypto map mymap 110 ipsec-isakmp
RouterA(config-crypto-map)# match address 110
RouterA(config-crypto-map)# set peer 172.30.2.2
RouterA(config-crypto-map)# set peer 172.30.3.2
RouterA(config-crypto-map)# set pfs group1
RouterA(config-crypto-map)# set transform-set mine
RouterA(config-crypto-map)# set security-association lifetime 86400
```

• **Multiple peers can be specified for redundancy.**

The figure illustrates a crypto map with two peers specified for redundancy. If the first peer cannot be contacted, the second peer is used. There is no limit to the number of redundant peers that can be configured.

The **crypto map** command has a crypto map configuration mode with the commands and syntax shown in the table.

Command	Description
set	Used with the **peer**, **pfs**, **transform-set**, and **security-association** commands.
peer [*hostname* | *ip-address*]	Specifies the allowed IPSec peer by IP address or hostname.
pfs [group1 | group2]	Specifies Diffie-Hellman Group 1 or Group 2.
transform-set [*set_name(s)*]	Specify list of transform sets in priority order. For an **ipsec-manual** crypto map, you can specify only one transform set. For an **ipsec-isakmp** or **dynamic** crypto map entry, you can specify up to six transform sets.
security-association lifetime	Sets security association lifetime parameters in seconds or kilobytes.
match address [*access-list-id* | *name*]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.
no	Used to delete commands entered with the **set** command.
exit	Exits crypto map configuration mode.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface configuration) command.

Note:	ACLs for crypto map entries tagged as ipsec-manual are restricted to a single permit entry and subsequent entries are ignored. The security associations established by that particular crypto map entry are only for a single data flow. To be able to support multiple manually established security associations for different kinds of traffic, define multiple crypto ACLs, and then apply each one to a separate ipsec-manual crypto map entry. Each ACL should include one permit statement defining what traffic to protect.

Step 5—Apply Crypto Maps to Interfaces

The last step in configuring IPSec is to apply the crypto map set to an interface.

Apply the crypto map to the IPSec router's interface connected to the Internet with the **crypto map** command in interface configuration mode. Use the **no** form of the command to remove the crypto map set from the interface. The command syntax is as follows:

```
crypto map map-name
```

Command	Description
map-name	This is the name that identifies the crypto map set, and is the name assigned when the crypto map is created.

IPSec Configuration Examples
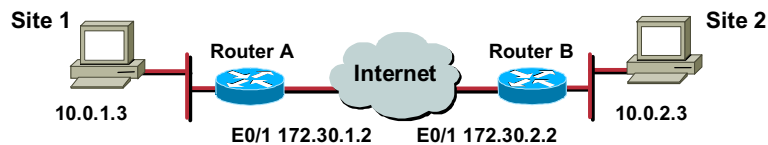
Site 1 — 10.0.1.3 — Router A — E0/1 172.30.1.2 — Internet — Router B — E0/1 172.30.2.2 — Site 2 — 10.0.2.3

```
RouterA# show running config
crypto ipsec transform-set mine esp-des
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.2.2
set transform-set mine
match address 110
!
interface Ethernet 0/1
ip address 172.30.1.2 255.255.255.0
no ip directed-broadcast
crypto map mymap
!
access-list 110 permit tcp 10.0.1.0
0.0.0.255 10.0.2.0 0.0.0.255
```

```
RouterB# show running config
crypto ipsec transform-set mine esp-des
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.1.2
set transform-set mine
match address 101
!
interface Ethernet 0/1
ip address 172.30.2.2 255.255.255.0
no ip directed-broadcast
crypto map mymap
!
access-list 101 permit tcp 10.0.2.0
0.0.0.255 10.0.1.0 0.0.0.255
```

SECUR 1.1—9-93

Consider the configuration example for RouterA and RouterB in the figure and as follows. The examples are concatenated to only show commands related to what has been covered in this lesson to this point.

```
RouterA# show running-config
crypto isakmp policy 100
 hash md5
 authentication pre-share
crypto isakmp key cisco1234 address 172.30.2.1
!
crypto ipsec transform-set mine esp-des
!
 !
 crypto map mymap 110 ipsec-isakmp
 set peer 172.30.2.1
 set transform-set mine
 match address 110
!
interface Ethernet0/1
 ip address 172.30.1.1 255.255.255.0
 ip access-group 101 in
 crypto map mymap
!
access-list 101 permit ahp host 172.30.2.1 host 172.30.1.1
access-list 101 permit esp host 172.30.2.1 host 172.30.1.1
```

```
access-list 101 permit udp host 172.30.2.1 host 172.30.1.1 eq isakmp
access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
access-list 110 deny ip any any
RouterB# show running-config
crypto isakmp policy 100
 hash md5
 authentication pre-share
crypto isakmp key cisco1234 address 172.30.1.1
!
crypto ipsec transform-set mine esp-des
!
 !
 crypto map mymap 100 ipsec-isakmp
 set peer 172.30.1.1
 set transform-set mine
 match address 102
!
interface Ethernet0/1
 ip address 172.30.2.1 255.255.255.0
 ip access-group 101 in
 crypto map mymap
!
access-list 101 permit ahp host 172.30.1.1 host 172.30.2.1
access-list 101 permit esp host 172.30.1.1 host 172.30.2.1
access-list 101 permit udp host 172.30.1.1 host 172.30.2.1 eq isakmp
access-list 102 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny ip any any
```

Task 4—Test and Verify IPSec

Cisco IOS software contains a number of **show**, **clear**, and **debug** commands useful for testing and verifying IPSec and ISAKMP, which are considered in this topic.

You can perform the following actions to test and verify that you have correctly configured the VPN using Cisco IOS:

- Display your configured IKE policies using the **show crypto isakmp policy** command.

- Display your configured transform sets using the **show crypto ipsec transform set** command.

- Display the current state of your IPSec SAs with the **show crypto ipsec sa** command.

Task 4—Test and Verify IPSec (cont.)

- **Display your configured crypto maps.**

  `show crypto map`

- **Enable debug output for IPSec events.**

  `debug crypto ipsec`

- **Enable debug output for ISAKMP events.**

  `debug crypto isakmp`

SECUR 1.1—9-96

You can perform the following actions to test and verify that you have correctly configured VPN using Cisco IOS:

- View your configured crypto maps with the **show crypto map** command.

- Debug IKE and IPSec traffic through the Cisco IOS with the **debug crypto ipsec** and **debug crypto isakmp** commands.

show crypto isakmp policy **Command**

Site 1
Router A
Internet
Router B
Site 2

10.0.1.3
10.0.2.3

router#

```
show crypto isakmp policy
```

```
RouterA# show crypto isakmp policy
Protection suite of priority 110
     encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
     hash algorithm:        Message Digest 5
     authentication method: Rivest-Shamir-Adleman Encryption
     Diffie-Hellman group:  #1 (768 bit)
     lifetime:              86400 seconds, no volume limit
Default protection suite
     encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
     hash algorithm:        Secure Hash Standard
     authentication method: Rivest-Shamir-Adleman Signature
     Diffie-Hellman group:  #1 (768 bit)
     lifetime:              86400 seconds, no volume limit
```

SECUR 1.1—9-97

Use the **show crypto isakmp policy** EXEC command to view the parameters for each ISAKMP policy as shown in the following example for RouterA:

```
RouterA# show crypto isakmp policy

Protection suite of priority 110

        encryption algorithm:   DES - Data Encryption Standard (56 bit
                                keys).

        hash algorithm:         Message Digest 5

        authentication method:  Rivest-Shamir-Adleman Encryption

        Diffie-Hellman group:   #1 (768 bit)

        lifetime:               86400 seconds, no volume limit

Default protection suite

        encryption algorithm:   DES - Data Encryption Standard (56 bit
                                keys).

        hash algorithm:         Secure Hash Standard

        authentication method:  Rivest-Shamir-Adleman Signature

        Diffie-Hellman group:   #1 (768 bit)

        lifetime:               86400 seconds, no volume limit
```

Site 1

Router A

Internet

Router B

Site 2

10.0.1.3

E0/1 172.30.1.2   E0/1 172.30.2.2

10.0.2.3

router#

```
show crypto ipsec transform-set
```

```
RouterA# show crypto ipsec transform-set
    Transform set mine: { esp-des  }
    will negotiate = { Tunnel,  },
```

• **View the currently defined transform sets**

SECUR 1.1—9-98

Use the **show crypto ipsec transform-set** EXEC command to view the configured transform sets. The command has the following syntax:

```
show crypto ipsec transform-set [tag transform-set-name]
```

Command Parameter	Description
tag *transform-set-name*	(Optional.) Shows only the transform sets with the specified transform-set-name.

If no keyword is used, all transform sets configured at the router are displayed.

show crypto ipsec sa Command

Site 1 — Router A — Internet — Router B — Site 2

10.0.1.3   E0/1 172.30.1.2   E0/1 172.30.2.2   10.0.2.3
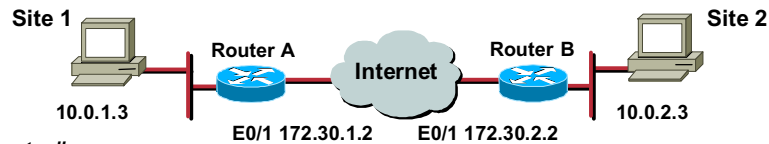
router#
```
show crypto ipsec sa
```

```
RouterA# show crypto ipsec sa
interface: Ethernet0/1
      Crypto map tag: mymap, local addr. 172.30.1.2
      local  ident (addr/mask/prot/port): (172.30.1.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.30.2.2/255.255.255.255/0/0)
   current_peer: 172.30.2.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
     path mtu 1500, media mtu 1500
      current outbound spi: 8AE1C9C
```

SECUR 1.1—9-99

Use the **show crypto ipsec sa** EXEC command to view the settings used by current security associations. If no keyword is used, all security associations are displayed. The command syntax is as follows:

```
show crypto ipsec sa [map map-name | address | identity] [detail]
```

Command	Description
map *map-name*	(Optional.) Shows any existing security associations created for the crypto map.
address	(Optional.) Shows all the existing security associations, sorted by the destination address and then by protocol (AH or ESP).
identity	(Optional.) Shows only the flow information. It does not show the security association information.
detail	(Optional.) Shows detailed error counters. (The default is the high-level send/receive error counters.)

show crypto map Command

Site 1 — 10.0.1.3
Router A — E0/1 172.30.1.2
Internet
Router B — E0/1 172.30.2.2
Site 2 — 10.0.2.3
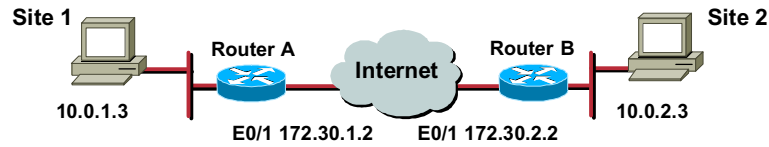
router#

```
show crypto map
```

View the currently configured crypto maps

```
RouterA# show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
        Peer = 172.30.2.2
        Extended IP access list 102
            access-list 102 permit ip host 172.30.1.2 host
        172.30.2.2
        Current peer: 172.30.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ mine, }
```

SECUR 1.1—9-100

Use the **show crypto map** EXEC command to view the crypto map configuration. If no keywords are used, all crypto maps configured at the router will be displayed. The command syntax is as follows:

```
show crypto map [interface interface | tag map-name]
```

Command	Description
interface *interface*	(Optional.) Shows only the crypto map set applied to the specified interface.
tag *map-name*	(Optional.) Shows only the crypto map set with the specified map-name.

debug crypto Commands

router#

```
debug crypto ipsec
```

- **Displays debug messages about all IPSec actions**

router#

```
debug crypto isakmp
```

- **Displays debug messages about all ISAKMP actions**

Use the **debug crypto ipsec** EXEC and the **debug crypto isakmp** commands to display IPSec and ISAKMP events. The **no** form of these commands disables debugging output.

Note:	Because these command generates a significant amount of output for every IP packet processed, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

The following example of ISAKMP and IPSec debugging shows normal IPSec setup messages. Note the inline comments (**!**).

```
RouterA# debug crypto ipsec
Crypto IPSEC debugging is on
RouterA# debug crypto isakmp
Crypto ISAKMP debugging is on
RouterA#
*Feb 29 08:08:06.556 PST: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.30.1.2, dest= 172.30.2.2,
    src_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004
! Interesting traffic from Site1 to Site2 triggers ISAKMP Main Mode.
*Feb 29 08:08:06.556 PST: ISAKMP (4): beginning Main Mode exchange
*Feb 29 08:08:06.828 PST: ISAKMP (4): processing SA payload. message
ID = 0
```

```
*Feb 29 08:08:06.828 PST: ISAKMP (4): Checking ISAKMP transform 1
against priority 100 policy
*Feb 29 08:08:06.828 PST: ISAKMP:      encryption DES-CBC
*Feb 29 08:08:06.828 PST: ISAKMP:      hash MD5
*Feb 29 08:08:06.828 PST: ISAKMP:      default group 1
*Feb 29 08:08:06.832 PST: ISAKMP:      auth pre-share
*Feb 29 08:08:06.832 PST: ISAKMP (4): atts are acceptable. Next
payload is 0
! The IPSec peers have found a matching ISAKMP policy
*Feb 29 08:08:06.964 PST: ISAKMP (4): SA is doing pre-shared key
authentication
! Pre-shared key authentication is identified
*Feb 29 08:08:07.368 PST: ISAKMP (4): processing KE payload. message
ID = 0
*Feb 29 08:08:07.540 PST: ISAKMP (4): processing NONCE payload.
message ID = 0
*Feb 29 08:08:07.540 PST: ISAKMP (4): SKEYID state generated
*Feb 29 08:08:07.540 PST: ISAKMP (4): processing vendor id payload
*Feb 29 08:08:07.544 PST: ISAKMP (4): speaking to another IOS box!
*Feb 29 08:08:07.676 PST: ISAKMP (4): processing ID payload. message
ID = 0
*Feb 29 08:08:07.676 PST: ISAKMP (4): processing HASH payload. message
ID = 0
*Feb 29 08:08:07.680 PST: ISAKMP (4): SA has been authenticated with

172.30.2.2
! Main mode is complete. The peers are authenticated, and secret
! keys are generated. On to Quick Mode!
*Feb 29 08:08:07.680 PST: ISAKMP (4): beginning Quick Mode exchange,
M-ID of -1079597279
*Feb 29 08:08:07.680 PST: IPSEC(key_engine): got a queue event...
*Feb 29 08:08:07.680 PST: IPSEC(spi_response): getting spi 365827691ld
for SA
        from 172.30.2.2     to 172.30.1.2      for prot 3
*Feb 29 08:08:08.424 PST: ISAKMP (4): processing SA payload. message
ID = -1079597279
*Feb 29 08:08:08.424 PST: ISAKMP (4): Checking IPSec proposal 1
*Feb 29 08:08:08.424 PST: ISAKMP: transform 1, ESP_DES
*Feb 29 08:08:08.424 PST: ISAKMP:   attributes in transform:
*Feb 29 08:08:08.424 PST: ISAKMP:      encaps is 1
*Feb 29 08:08:08.424 PST: ISAKMP:      SA life type in seconds
*Feb 29 08:08:08.424 PST: ISAKMP:      SA life duration (basic) of
3600
*Feb 29 08:08:08.428 PST: ISAKMP:      SA life type in kilobytes
*Feb 29 08:08:08.428 PST: ISAKMP:      SA life duration (VPI) of  0x0
0x46 0x50 0x0
*Feb 29 08:08:08.428 PST: ISAKMP:      authenticator is HMAC-MD5
```

```
*Feb 29 08:08:08.428 PST: ISAKMP (4): atts are acceptable.

*Feb 29 08:08:08.428 PST: IPSEC(validate_proposal_request): proposal
part #1,
  (key eng. msg.) dest= 172.30.2.2, src= 172.30.1.2,
    dest_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

*Feb 29 08:08:08.432 PST: ISAKMP (4): processing NONCE payload.
message ID = -10

79597279

*Feb 29 08:08:08.432 PST: ISAKMP (4): processing ID payload. message
ID = -1079597279

*Feb 29 08:08:08.432 PST: ISAKMP (4): processing ID payload. message
ID = -1079597279

! A matching IPSec policy has been negotiated and authenticated.
! Next the SAs are set up.
*Feb 29 08:08:08.436 PST: ISAKMP (4): Creating IPSec SAs

*Feb 29 08:08:08.436 PST:         inbound SA from 172.30.2.2      to
172.30.1.2
     (proxy 10.0.2.0     to 10.0.1.0    )

*Feb 29 08:08:08.436 PST:         has spi 365827691 and conn_id 5 and
flags 4

*Feb 29 08:08:08.436 PST:         lifetime of 3600 seconds

*Feb 29 08:08:08.440 PST:         lifetime of 4608000 kilobytes

*Feb 29 08:08:08.440 PST:         outbound SA from 172.30.1.2      to
172.30.2.2
     (proxy 10.0.1.0     to 10.0.2.0    )

*Feb 29 08:08:08.440 PST:         has spi 470158437 and conn_id 6 and
flags 4

*Feb 29 08:08:08.440 PST:         lifetime of 3600 seconds

*Feb 29 08:08:08.440 PST:         lifetime of 4608000 kilobytes

*Feb 29 08:08:08.440 PST: IPSEC(key_engine): got a queue event...

*Feb 29 08:08:08.440 PST: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.30.1.2, src= 172.30.2.2,
    dest_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x15CE166B(365827691), conn_id= 5, keysize= 0, flags= 0x4

*Feb 29 08:08:08.444 PST: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.30.1.2, dest= 172.30.2.2,
    src_proxy= 10.0.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.0.2.0/255.255.255.0/0/0 (type=4),
```

```
        protocol= ESP, transform= esp-des esp-md5-hmac ,
        lifedur= 3600s and 4608000kb,
        spi= 0x1C060C65(470158437), conn_id= 6, keysize= 0, flags= 0x4
*Feb 29 08:08:08.444 PST: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.30.1.2, sa_prot= 50,
     sa_spi= 0x15CE166B(365827691),
     sa_trans= esp-des esp-md5-hmac , sa_conn_id= 5
*Feb 29 08:08:08.444 PST: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.30.2.2, sa_prot= 50,
     sa_spi= 0x1C060C65(470158437),
     sa_trans= esp-des esp-md5-hmac , sa_conn_id= 6
! IPSec SAs are set up and data can be securely exchanged.
RouterA#
```

Crypto System Error Messages for ISAKMP

```
%CRYPTO-6-IKMP_SA_NOT_AUTH: Cannot accept Quick Mode exchange
from %15i if SA is not authenticated!
```
• **ISAKMP SA with the remote peer was not authenticated.**

```
%CRYPTO-6-IKMP_SA_NOT_OFFERED: Remote peer %15i responded with
attribute [chars] not offered or changed
```
• **ISAKMP peers failed protection suite negotiation for ISAKMP.**

SECUR 1.1—9-102

Cisco IOS software can generate many useful system error messages for ISAKMP. Two of the error messages follow.

■ %CRYPTO-6-IKMP_SA_NOT_AUTH: Cannot accept Quick Mode exchange from %15i if SA is not authenticated!—The ISAKMP security association with the remote peer was not authenticated yet the peer attempted to begin a Quick Mode exchange. This exchange must only be done with an authenticated security association The recommended action is to contact the remote peer's administrator to resolve the improper configuration.

■ %CRYPTO-6-IKMP_SA_NOT_OFFERED: Remote peer %15i responded with attribute [chars] not offered or changed—ISAKMP peers negotiate policy by the initiator offering a list of possible alternate protection suites. The responder responded with an ISAKMP policy that the initiator did not offer. The recommended action is to contact the remote peer's administrator to resolve the improper configuration.

Overview of Configuring IPSec Manually

You can configure your keys manually. This topic provides a brief discussion of how this is done and also details why manual key use is not generally recommended.

Setting Manual Keys with *security-association* Commands

`router(config-crypto-map)#`

```
set security-association inbound|outbound ah spi
hex-key-string
```

```
set security-association inbound|outbound esp spi cipher
hex-key-string [authenticator hex-key-string]
```

- **Specifies inbound or outbound SA.**
- **Sets Security Parameter Index (SPI) for the SA.**
- **Sets manual AH and ESP keys:**
  - **ESP key length is 56 bits with DES, 168 with 3DES.**
  - **AH HMAC key length is 128 bits with MD5, 160 bits with SHA.**
- **SPIs should be reciprocal for IPSec peer.**

SECUR 1.1—9-104

Use the **security-association** command in crypto map configuration mode, to manually specify the IPSec session keys within a crypto map entry. Use

the **no** form of this command to remove IPSec session keys from a crypto map entry. This command is only available for **ipsec-manual** crypto map entries. The command has the following syntax:

```
set security-association {inbound | outbound} ah spi hex-key-string
```

```
set security-association {inbound | outbound} esp spi cipher hex-key-string
[authenticator hex-key-string]
```

Command	Description
inbound	Sets the inbound IPSec session key. (You must set both inbound and outbound keys.)
outbound	Sets the outbound IPSec session key.
ah	Sets the IPSec session key for the AH protocol. Use when the crypto map entry's transform set includes an AH transform.
esp	Sets the IPSec session key for the ESP protocol. Use when the crypto map entry's transform set includes an ESP transform.
spi	Specifies the security parameter index (SPI), a number that is used to uniquely identify an SA. The SPI is an arbitrary number you assign in the range of 256 to 4,294,967,295 (FFFF FFFF).

Command	Description
hex-key-string	Specifies the session key entered in hexadecimal format. It is an arbitrary string of 8, 16, or 20 bytes. The crypto map's transform set includes ■ A DES algorithm, specify at least 8 bytes per key. ■ An MD5 algorithm, specify at least 16 bytes per key. ■ An SHA algorithm, specify 20 bytes per key. Keys longer than the above sizes are simply truncated.
cipher	Indicates that the key string is to be used with the ESP encryption transform.
authenticator	(Optional.) Indicates that the key string is to be used with the ESP authentication transform. This argument is required only when the crypto map entry's transform set includes an ESP authentication transform.

If the crypto map's transform set includes an AH or ESP protocol, you must define IPSec AH or ESP keys for both inbound and outbound traffic. If your transform set includes an ESP authentication protocol, you must define IPSec keys for ESP authentication for inbound and outbound traffic.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI is used to identify the security association used with the crypto map. However, not all peers have the same flexibility in SPI assignment. You should coordinate SPI assignment with your peer's operator, making certain that the same SPI is not used more than once for the same destination address and protocol combination.

SAs established via this command do not expire (unlike SAs established via ISAKMP).

Session keys at one peer must match the session keys at the remote peer. If you change a session key, the SA using the key is deleted and reinitialized.

Configuring IPSec Manually Is Not Recommended

You can configure IPSec SAs manually and not use ISAKMP to set up the SA. It is recommended that you use ISAKMP to set up the SAs because it is very difficult to ensure the SA values match between peers, and D-H is a vastly more secure method to generate secret keys between peers. Other reasons not to configure IPSec manually included the following:

■ Manual keying does not scale well and is often insecure due to difficulty in manually creating secure keying material.

■ Manually established SAs do not expire.

■ ACLs for crypto map entries tagged as *ipsec-manual* are restricted to a single permit entry, and subsequent entries are ignored.

■ The SAs established by a manual crypto map entry are only for a single data flow.

Overview of Configuring IPSec for RSA Encrypted Nonces

This topic provides a brief overview of configuring IPSec for RSA encrypted nonces.

RSA encrypted nonces provide a strong method of authenticating the IPSec peers and the Diffie-Hellman key exchange. RSA encrypted nonces provide repudiation—a quality that prevents a third party from being able to trace your activities over a network. A drawback is that they are somewhat more difficult to configure and, therefore, more difficult to scale to a large number of peers. RSA encrypted nonces require that peers possess each other's public keys but do not use a Certification Authority. Instead, there are two ways for peers to get each other's public keys:

- You manually configure and exchange RSA keys.

- You use RSA signatures previously used during a successful ISAKMP negotiation with a remote peer.

Note: RSA encrypted nonces must initially be exchanged via a secure method.

The IPSec configuration process for RSA encryption is very similar to pre-shared keys with some notable exceptions summarized as follows:

■ Task 1—Prepare for IPSec to determine a detailed security policy for RSA encryption to include how to distribute the RSA public keys.

■ Task 2—Configure RSA keys manually.

■ Task 3—Configure ISAKMP for IPSec to select RSA encryption as the authentication method in an ISAKMP policy.

■ Task 4—Configure IPSec, which is typically done the same as in pre-share.

■ Task 5—Test and verify IPSec and exercise additional commands to view and manage RSA public keys.

Configuring RSA keys can be complex. To illustrate this fact, a simple presentation of the steps and commands used in Task 2 is detailed in the following figures.

Note:	For a complete discussion of all the tasks and steps necessary to configure RSA Encrypted Nonces see the "Configuring IKE Security Protocol" lesson in the Cisco IOS Security Configuration Guide, release 12.1. This topic only provides a brief overview of the commands used for Task 2, as it is unique to RSA Encrypted Nonces.

Configuring RSA keys involves the following six steps:

Step 1 Plan for RSA keys.

Step 2 Configure the router's host name and domain name (if they have not already been configured).

Step 3 Generate the RSA keys.

Task 2—Configure RSA Keys (cont.)

Step 4—Enter peer RSA public keys.

```
crypto key pubkey-chain
crypto key pubkey-chain rsa
addressed-key key address
named-key key name
key-string
```

Step 4 Enter peer RSA public keys—There are several sub-steps necessary to enter the peer's public keys. Attention to detail is important, as any mistakes made entering the keys will cause them not to work.

SECUR 1.1—9-109

Step 5 Verify the key configuration—It is easy for mistakes to be made when copying and pasting the RSA keys. Verifying the keys ensures that they match.

Step 6 Manage RSA keys—Removing old keys is part of the configuration process. Old keys can consume much unnecessary space.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **Cisco supports the following IPSec standards: AH, ESP, DES, 3DES, AES, MD5, SHA, RSA signatures, IKE (also known as ISAKMP), DH, and CAs.**
- **There are five steps to IPSec: interesting traffic, IKE Phase 1, IKE Phase 2, IPSec encrypted traffic, and tunnel termination.**
- **IPSec SAs consist of a destination address, SPI, IPSec transform, mode, and SA lifetime value.**
- **Define the detailed crypto IKE and IPSec security policy before beginning configuration.**
- **Ensure that router ACLs permit IPSec traffic.**

SECUR 1.1—9-111

Summary (cont.)

- **IKE policies define the set of parameters used during IKE negotiation.**
- **Transform sets determine IPSec transform and mode.**
- **Crypto ACLs determine traffic to be encrypted.**
- **Crypto maps pull together all IPSec details and are applied to interfaces.**
- **Use** show **and** debug **commands to test and troubleshoot.**
- **IPSec can also be configured manually or using encrypted nonces.**

SECUR 1.1—9-112

Lab Exercise—Configure Cisco IOS IPSec for Pre-Shared Keys

Complete the following lab exercise to practice what you learned in this lesson.

Objectives

In this lab exercise you will configure a Cisco router to enable IPSec encrypted tunnels to another Cisco router. Work with your lab partner to complete the following tasks:

- Complete the lab exercise setup.

- Prepare to configure VPN support.

- Configure IKE parameters.

- Configure IPSec parameters.

- Verify and test the IPSec configuration.

- (Optional.) Fine-tune the ACL.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.

Lab Visual Objective

Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1 Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2 Configure your student PC for IP address **10.0.P.12** with a default gateway of **10.0.P.2** (where P = pod number).

Step 3 Restore the original course router configuration. Your instructor will explain how to do this.

Step 4 Ensure you can ping your peer's router and network host before beginning.

Task 2—Prepare to Configure VPN Support

Complete the following steps to prepare for the IPSec configuration:

Step 1 Determine the IKE and IPSec policy. In this lab exercise, you will use default values except when you are directed to enter a specific value. The following are the overall policies used in the lab exercise:

- IKE policy is to use pre-shared keys.

- IPSec policy is to use ESP mode with DES encryption.

- IPSec policy is to encrypt all traffic between perimeter routers.

Step 2 Verify that connectivity has been established to the other group's router by entering the following command. Use the command output to answer the following question:

```
RP> enable
password: cisco
RP# ping 172.30.Q.2
```

(where P = pod number, Q = peer pod number)

Q1)   In a production environment, what other steps would you complete at this point?

A)   _____

Task 3—Configure IKE Parameters

Work with the members of the pod group you have been teamed up with to complete this lab exercise. Complete the following steps to configure IKE on your Cisco router:

Note:	While entering commands, notice when the command line prompt changes. Refer to the command line prompt to verify what configuration mode you are in.

Step 1 Ensure that you are in configuration mode:

```
RP# config t
```

Step 2 Enable IKE/ISAKMP on the router:

```
RP(config)# crypto isakmp enable
```

Step 3 Create an IKE policy to use pre-shared keys by completing the following sub-steps:

1. Set the policy priority and enter config-isakmp mode:

```
RP(config)# crypto isakmp policy 110
```

2. Set authentication to use pre-shared keys:

```
RP(config-isakmp)# authentication pre-share
```

3. Set IKE encryption:

```
RP(config-isakmp)# encryption des
```

4. Set the Diffie-Hellman group:

```
RP(config-isakmp)# group 1
```

5. Set the hash algorithm:

```
RP(config-isakmp)# hash md5
```

6. Set the IKE SA lifetime:

```
RP(config-isakmp)# lifetime 86400
```

7. Exit the config-isakmp mode:

```
RP(config-isakmp)# exit
```

8. Set up the pre-shared key and peer address:

```
RP(config)# crypto isakmp key cisco1234 address 172.30.Q.2
```

(where Q = peer pod number)

9. Exit config mode:

```
RP(config)# exit
```

10. Examine the crypto policy suite:

```
RP # show crypto isakmp policy
Protection suite of priority 110
        encryption algorithm:   DES - Data Encryption Standard (56 bit
                                keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit
                                keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Task 4—Configure IPSec Parameters

Complete the following steps to configure IPSec on your Cisco router:

Configure Transform Sets and Security Association Parameters

Step 1 Verify you are in configuration mode:

```
RP# config t
```

Step 2 View the available crypto IPSec command options by entering the following command. Use the command output to answer the following question:

```
RP(config)# crypto ipsec ?
```

Q2)   What options can be set at this level?

A)   _____

Step 3 Check your transform set options by entering the following commands. Use the command output to answer the following question:

```
RP(config)# crypto ipsec transform-set ?
```

Q3)   Is it possible to configure a transform set without naming it first?

A)   _____

Step 4 Define a transform set. Use these parameters to answer the following question:

- Transform name: **mine**
- ESP protocols: **des**
- Mode: **tunnel**

```
RP(config)# crypto ipsec transform-set mine esp-des
```

Q4) Has your command prompt changed? What can you set now? (Hint: Enter **?** to view available options)

A) _____

Step 5 Set the mode to tunnel:

```
RP(cfg-crypto-trans)# mode tunnel
```

Step 6 Exit the configuration mode:

```
RP(cfg-crypto-trans)# ^Z
```

Step 7 Verify your configuration:

```
RP# show crypto ipsec transform-set mine
Transform set mine: { esp-des  }
   will negotiate = { Tunnel,  },
```

Configure Crypto Access Lists

Complete the following steps to configure the crypto access lists. Create an Access Control List (ACL) to select traffic to protect. The ACL should encrypt traffic between perimeter routers. Use the following parameters:

- Traffic permitted: **all**
- Peer address: **peer router external interface**
- ACL number: **102**
- Protocol: **any Internet protocol**

Step 1 Ensure you are in configuration mode:

```
RP(config)# config terminal
```

Step 2 Configure the ACL:

```
RP(config)# access-list 102 permit ip host 172.30.P.2 host 172.30.Q.2
```

(where P = pod number, and Q = peer pod number)

Configure Crypto Maps

Complete the following steps to configure a crypto map. Use the following parameters:

- Name of map: **mymap**
- Number of map: **10**
- Key exchange type: **isakmp**
- Peer: **172.30.Q.2** (where Q = peer pod number)

- Transform set: **mine**
- Match address: **102**

Step 1 Set the name of the map, the map number, and the type of key exchange to be used:

```
RP(config)# crypto map mymap 10 ipsec-isakmp
```

Step 2 Specify the extended ACL to use with this map:

```
RP(config-crypto-map)# match address 102
```

Step 3 Specify the transform set you defined earlier:

```
RP(config-crypto-map)# set transform-set mine
```

Step 4 Assign the virtual private network (VPN) peer using the host name or IP address of the peer and answer the following question:

```
RP(config-crypto-map)# set peer 172.30.Q.2
```

(where Q = peer pod number)

Q5)   What other parameters can be set at this level? (Hint: Enter `set ?`)

A)   _____

Step 5 Exit the crypto map configuration mode:

```
RP(config-crypto-map)# exit
```

Apply the Crypto Map to an Interface

Complete the following steps to assign the crypto map to the appropriate router interface. Use the following parameters:

- Interface to configure: **Ethernet 0/1**
- Crypto map to use: **mymap**

Step 1 Access the interface configuration mode:

```
RP(config)# interface fast 0/1
```

Step 2 Assign the crypto map to the interface:

```
RP(config-if)# crypto map mymap
```

Step 3 Exit configuration crypto mode:

```
RP(config-if)# ^Z
```

Step 4 Save the configuration:

```
RP# copy running-config startup-config
```

Task 5—Verify and Test the IPSec Configuration

Coordinate the test with your peer router's pod group and complete the following steps to verify and test your IPSec configuration:

Step 1 Display your configured IKE policies:

```
RP# show crypto isakmp policy
```

```
Protection suite of priority 110
        encryption algorithm:    DES - Data Encryption Standard (56 bit
                                 keys)
        hash algorithm:          Message Digest 5
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit
                                 keys)
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
```

Step 2   Display your configured transform sets:

```
RP# show crypto ipsec transform-set
Transform set mine: { esp-des  }
   will negotiate = { Tunnel,  },
```

Step 3   Display your configured crypto maps (where P = pod number, and Q = peer pod number):

```
RP# show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
        Peer = 172.30.Q.2
        Extended IP access list 102
            access-list 102 permit ip host 172.30.P.2 host 172.30.Q.2
        Current peer: 172.30.Q.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ mine, }
```

Step 4   Display the current state of your IPSec SAs. IPSec SAs may have been previously established
by routing traffic. The following example shows initialized IPSec SAs before encryption traffic
(where P = pod number and Q = peer pod number):

```
RP# show crypto ipsec sa
interface: Ethernet0/1
    Crypto map tag: mymap, local addr. 172.30.P.2


    local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
    current_peer: 172.30.Q.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
```

```
                        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
                        #send errors 0, #recv errors 0


                         local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2
                         path mtu 1500, media mtu 1500
                         current outbound spi: 0


                         inbound esp sas:
                         inbound ah sas:


                         outbound esp sas:
                         outbound ah sas:
```

Step 5   Clear any existing SAs:

```
RP# clear crypto sa
```

Step 6   Enable debug output for IPSec events:

```
RP# debug crypto ipsec
```

Step 7   Enable debug output for ISAKMP events:

```
RP# debug crypto isakmp
```

Step 8   Turn on console logging so you can see the debug output:

```
RP(config)# logging console
```

Step 9   Initiate a ping to your peer pod's perimeter router. Observe the IKE and IPSec debug output:

```
RP# ping 172.30.Q.2
```

Step 10   Verify IKE and IPSec SAs. Note the number of packets encrypted and decrypted when viewing
the IPSec SAs (where P = pod number, and Q = peer pod number):

```
RP# show crypto isakmp sa
dst               src                state           conn-id   slot
172.30.P.2      172.30.Q.2        QM_IDLE           16       0
RP# show crypto ipsec sa
interface: Ethernet0/1
    Crypto map tag: mymap, local addr. 172.30.P.2


   local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
   current_peer: 172.30.Q.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 0
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 0
    #send errors 4, #recv errors 0
```

```
            local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2
            path mtu 1500, media mtu 1500
            current outbound spi: DB5049D

            inbound esp sas:
             spi: 0x26530A0D(642976269)
               transform: esp-des ,
               in use settings ={Tunnel, }
               slot: 0, conn id: 2, crypto map: mymap
               sa timing: remaining key lifetime (k/sec): (4607999/3542)
               IV size: 8 bytes
               replay detection support: N

            inbound ah sas:

            outbound esp sas:
             spi: 0xDB5049D(229967005)
               transform: esp-des ,
               in use settings ={Tunnel, }
               slot: 0, conn id: 3, crypto map: mymap
               sa timing: remaining key lifetime (k/sec): (4607999/3542)
               IV size: 8 bytes
               replay detection support: N

            outbound ah sas:
```

Step 11 Ensure that encryption is working between routers by generating additional traffic. Then, observe that the packets encrypted and decrypted counter has incremented (where P = pod number, and Q = peer pod number):

```
RP# ping 172.30.Q.2
RP# show crypto ipsec sa
interface: Ethernet0/1
    Crypto map tag: mymap, local addr. 172.30.P.2

   local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
   current_peer: 172.30.2.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 0
    #pkts decaps: 11, #pkts decrypt: 11, #pkts verify 0
```

```
#send errors 4, #recv errors 0

 local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2
 path mtu 1500, media mtu 1500
 current outbound spi: DB5049D

 inbound esp sas:
  spi: 0x26530A0D(642976269)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4607998/3506)
    IV size: 8 bytes
    replay detection support: N

 inbound ah sas:

 outbound esp sas:
  spi: 0xDB5049D(229967005)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3, crypto map: mymap
    sa timing: remaining key lifetime (k/sec): (4607998/3506)
    IV size: 8 bytes
    replay detection support: N

 outbound ah sas:
```

Note: The packet counters have increased from Step 10 due to the encrypted traffic.

Task 6—(Optional.) Fine-Tune the ACL

Fine-tune the crypto ACLs used to determine interesting traffic to encrypt between the internal
Windows 2000 servers. Remember to work with your peer pod group to make the ACLs
symmetrical between the perimeter routers. Ensure that desired traffic is encrypted between
peers.

Step 1   Ensure that you are in configuration mode:

RP# **config terminal**

Step 2   Remove the previously configured ACL:

RP(config)# **no access-list 102**

Step 3   Configure a new ACL for the Windows 2000 servers:

```
              RP(config)# access-list 102 permit ip host 10.0.P.12 host 10.0.Q.12
```

(where P = pod number, and Q = peer pod number)

Step 4 Verify your configuration by connecting to your peer's web server at IP address 10.0.Q.2 (where Q = peer pod number), using the browser on your NT server.

Step 5 Check your router configuration using the **show run** command against the following sample configuration for router R2:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rP
!
enable password cisco
!
memory-size iomem 15
ip subnet-zero
!
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 110
 hash md5
 authentication pre-share
crypto isakmp key cisco1234 address 172.30.Q.2
!
!
crypto ipsec transform-set mine esp-des
!
crypto map mymap 10 ipsec-isakmp
 set peer 172.30.Q.2
 set transform-set mine
 match address 102
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
```

```
!
interface Ethernet0/0
 ip address 10.0.P.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.P.2 255.255.255.0
 half-duplex
 crypto map mymap
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
no ip http server
ip pim bidir-enable
!
!
access-list 102 permit ip host 10.0.P.12 host 10.0.Q.12
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
!
end
```

10

Building Advanced IPSec VPNs Using Cisco Routers and Certificate Authorities

Overview

This lesson introduces configuration of Cisco IOS software IPSec using a Certificate Authority (CA). After presenting an overview of the configuration process, the lesson shows you each major step of the configuration that is unique to CA support. It includes the following topics:

■ Objectives

■ Configure CA support tasks

■ Task 1—Prepare for IKE and IPSec

■ CA support overview

■ Task 2—Configure CA support

■ Task 3—Configure IKE

■ Task 4—Configure IPSec

■ Task 5—Test and verify IPSec

■ Summary

■ Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- **Identify the CA vendor products that support Cisco VPN products.**
- **Configure a Cisco router for CA support.**
- **Configure a Cisco router for IKE using RSA signatures.**
- **Configure a Cisco router for IPSec using RSA signatures.**
- **Verify the IKE and IPSec configuration.**

SECUR 1.1—10-2

Configure CA Support Tasks

This topic presents an overview of the CA support tasks you will perform in this lesson.

Configure CA Support Tasks

- Task 1—Prepare for IKE and IPSec.
- Task 2—Configure CA support.
- Task 3—Configure IKE.
- Task 4—Configure IPSec.
- Task 5—Test and verify IPSec.

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—10-4

The configuration process for Rivest, Shamir, and Adleman (RSA) signatures consists of five major tasks. This lesson discusses the CA configuration tasks and steps in detail. Tasks and steps identical to pre-shared keys are not covered in detail in this lesson. The items covered in this lesson are as follows:

■ Task 1—Prepare for IPSec. Preparing for IPSec involves determining the detailed encryption policy: identifying the hosts and networks you wish to protect, determining IPSec peer details, determining the IPSec features you need, and ensuring that existing access control lists (ACLs) are compatible with IPSec.

■ Task 2—Configure CA support. Involves setting the router's hostname and domain name, generating the keys, declaring a CA, and authenticating and requesting your own certificates.

■ Task 3—Configure Internet Key Exchange (IKE) for IPSec. Configuring IKE involves enabling IKE, creating the IKE policies, and validating the configuration.

■ Task 4—Configure IPSec. IPSec configuration includes defining the transform sets, creating crypto ACLs, creating crypto map entries, and applying crypto map sets to interfaces.

■ Task 5—Test and verify IPSec. Use **show**, **debug**, and related commands to test and verify that IPSec encryption works, and to troubleshoot problems.

Task 1—Prepare for IKE and IPSec

Successful implementation of an IPSec network requires advance planning before beginning configuration of individual routers.

Task 1—Prepare for IPSec

- **Step 1—Plan for CA support.**
- **Step 2—Determine IKE (IKE Phase 1) policy.**
- **Step 3—Determine IPSec (IKE Phase 2) policy.**

Configuring IPSec encryption can be complicated. Having a detailed plan lessens the chances of improper configuration.

You must plan in advance if you desire to configure IPSec encryption correctly the first time and minimize misconfiguration. You should begin this task by defining the IPSec security policy based on the overall company security policy. Some planning steps follow:

Note:	Step 1 and Step 2 are covered in detail in this lesson. The other steps shown in the figure and listed below are presented for review purposes, and are not covered in this lesson.

Step 1 Plan for CA support—Determine the CA server details. This includes variables like the type of CA server to be used, the IP address, and the CA administrator contact information.

Step 2 Determine IKE (IKE Phase 1) policy—Determine the IKE policies between IPSec peers based on the number and location of the peers.

Step 3 Determine IPSec (IKE Phase 2) policy—Identify IPSec peer details such as IP addresses and IPSec modes. You then configure crypto maps to gather all IPSec policy details together.

Cisco.com

- **Step 4—Check the current configuration:**
  ```
  show running-config
  show crypto isakmp policy
  show crypto map
  ```
- **Step 5—Ensure that the network works without encryption:**
  ```
  ping
  ```
- **Step 6—Ensure that ACLs are compatible with IPSec:**
  ```
  show access-lists
  ```

SECUR 1.1—10-7

Step 4   Check the current configuration—Use the **show run**, **show crypto isakmp [policy]**, and **show crypto map** commands, and the many other **show** commands, which are covered later in this lesson.

Step 5   Ensure that the network works without encryption—Ensure that basic connectivity has been achieved between IPSec peers using the desired IP services before configuring IPSec. You can use the **ping** command to check basic connectivity.

Step 6   Ensure that ACLs are compatible with IPSec—Ensure that perimeter routers and the IPSec peer router interfaces permit IPSec traffic. In this step you need to enter the **show access-lists** command.

Step 1—Plan for CA Support

Cisco.com

Planning includes the following steps:
- ☑ Determine the type of CA server used and the requirements of the CA server.
- ☑ Identify the CA server's IP address, hostname, and URL.
- ☑ Identify the CA server's administrator contact information.

Goal: Be ready for CA support configuration.

SECUR 1.1—10-8

Successful implementation of an IPSec network requires advance planning before beginning configuration of individual routers.

Configuring a CA is complicated. Having a detailed plan lessens the chances of improper configuration. Some planning steps include the following:

- Determine the type of CA server to use. CA servers come in a multitude of configurations and capabilities. You must determine which one fits your needs in advance of configuration. Requirements include (but are not limited to) the RSA key type required, certificate revocation list (CRL) capabilities, and support for Registration Authority (RA) mode.

- Identify the CA server's IP address, hostname, and URL. (This information is necessary if you use Lightweight Directory Protocol [LDAP.])

- Identify the CA server administrator contact information. You need to arrange for your certificates to be validated if the process is not automatic.

The goal is to be ready for CA support configuration.

Step 1—Plan for CA Support (Determine CA Server Details)

Cisco.com

Site 1   RouterA   Internet   RouterB   Site 2

10.0.1.0   E0/1 172.30.1.2   E0/1 172.30.2.2   10.0.2.0
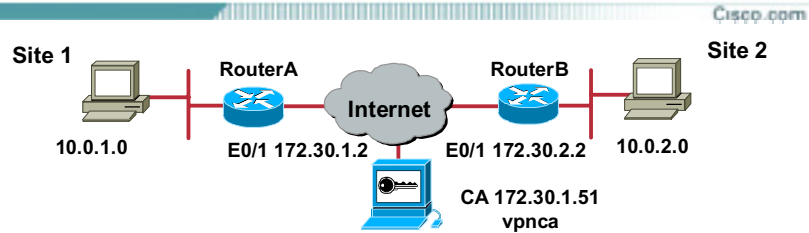
CA 172.30.1.51
vpnca

Parameter	CA Server
Type of CA server	Windows 2000
Hostname	vpnca
IP address	172.30.1.51
URL	vpnca.cisco.com
Administrator contact	1-800-555-1212

The figure illustrates the minimum information needed to configure a CA server on a Cisco router. Depending on the CA server chosen, other variables may also have to be identified and resolved.

Step 2—Determine IKE Phase 1 Policy Details

Cisco.com

Determine the following policy details:
- ☑ Key distribution method
- ☑ Authentication method
- ☑ IPSec peer IP addresses and hostnames
- ☑ IKE Phase 1 policies for all peers
  - – Encryption algorithm
  - – Hash algorithm
  - – IKE SA lifetime

Goal: Minimize misconfiguration

SECUR 1.1—10-10

Configuring IKE is complicated. You should determine the IKE policy details to enable the selected authentication method and then configure it. Having a detailed plan lessens the chances of improper configuration. Some planning steps include the following:

- Determine the key distribution method—Determine the key distribution method based on the numbers and locations of IPSec peers. For small networks, you may wish to manually distribute keys. For larger networks, you may wish to use a CA server to support scalability of IPSec peers. You must then configure Internet Security Association Key Management Protocol (ISAKMP) to support the selected key distribution method.

- Determine the authentication method—Choose the authentication method based on the key distribution method. Cisco IOS software supports either pre-shared keys, RSA encrypted nonces, or RSA signatures to authenticate IPSec peers. This lesson focuses on using RSA signatures.

- Identify IPSec peer's IP addresses and hostnames—Determine the details of all the IPSec peers that will use ISAKMP and RSA signature keys for establishing security associations (SAs). You will use this information to configure IKE.

- Determining ISAKMP policies for peers—An ISAKMP policy defines a combination or "suite" of security parameters to be used during the ISAKMP negotiation. Each ISAKMP negotiation begins by each peer agreeing on a common (shared) ISAKMP policy. The ISAKMP policy suites must be determined in advance of configuration. You must then configure IKE to support the policy details you determined. Some ISAKMP policy details include the following:

  — Encryption algorithm

  — Hash algorithm

  — IKE SA lifetime

The goal of this planning step is to gather the precise data you will need in later steps to minimize misconfiguration.

Step 2—Determine IKE Phase 1 Policy Details (Examine Parameters)

Parameter	Strong	Stronger
Encryption algorithm	DES	3DES or AES
Hash algorithm	MD5	SHA-1
Authentication method	Pre-shared	RSA encryption RSA signature
Key exchange	DH group 1	DH group 2
IKE SA lifetime	86400 seconds	< 86400 seconds

SECUR 1.1—10-11

An IKE policy defines a combination of security parameters used during the IKE negotiation. A group of policies makes up a "protection suite" of multiple policies that enable IPSec peers to establish IKE sessions and establish SAs with a minimal configuration. The figure shows an example of possible combinations of IKE parameters into either a strong or stronger policy suite.

Creating IKE Policies for a Purpose

IKE negotiations must be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation.

You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

Defining IKE Policy Parameters

You can select specific values for each IKE parameter per the IKE standard. You choose one value over another based on the security level you desire and the type of IPSec peer to which you will connect.

There are five parameters to define in each IKE policy as outlined in the figure, and in the following table. The figure shows the relative strength of each parameter, and the table shows the default values.

Parameter	Accepted Values	Keyword	Default
Message encryption algorithm	DES 3DES AES	**des** **3des** **aes**	DES
Message integrity (hash) algorithm	SHA-1 (HMAC variant) MD5 (HMAC variant)	**sha** **md5**	SHA-1
Peer authentication method	Pre-shared keys RSA encrypted nonces RSA signatures	**pre-share** **rsa-encr** **rsa-sig**	RSA signatures
Key exchange parameters (DH group identifier)	768-bit DH or 1024-bit DH	**1** **2**	768-bit DH
ISAKMP-established SA's lifetime	Can specify any number of seconds	—	86,400 seconds (one day)

You can select specific values for each ISAKMP parameter per the ISAKMP standard. You choose one value over another based on the security level you desire and the type of IPSec peer to which you will connect. There are five parameters to define in each IKE policy as presented in the following table. The table shows the relative strength of each parameter. You can select specific values for each ISAKMP parameter per the ISAKMP standard. You choose one value over another based on the security level you desire and the type of IPSec peer to which you will connect.

Parameter	Strong	Stronger
Message encryption algorithm	DES	3DES or AES
Message integrity (hash) algorithm	MD5	SHA-1
Peer authentication method	Pre-share	RSA encryption RSA signature
Key exchange parameters (DH group identifier)	DH Group 1	DH Group 2
ISAKMP-established SA's lifetime	86,400 seconds	<86,400 seconds

Step 2—Determine IKE Phase 1 Policy Details (IKE Policy Example)

Cisco.com
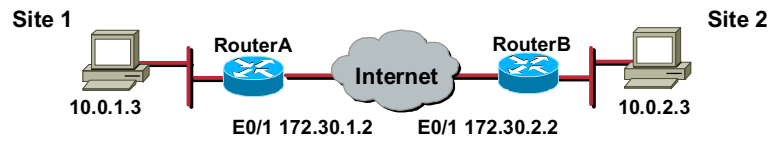
Site 1 — 10.0.1.3 — RouterA — E0/1 172.30.1.2 — Internet — E0/1 172.30.2.2 — RouterB — 10.0.2.3 — **Site 2**

Parameter	Site 1	Site 2
Encryption algorithm	DES	DES
Hash algorithm	MD5	MD5
Authentication method	RSA signatures	RSA signatures
Key exchange	DH group 1	DH group 1
IKE SA lifetime	86400 seconds	86400 seconds
Peer IP address	172.30.2.2	172.30.1.2

SECUR 1.1—10-12

You should determine IKE policy details for each peer before configuring IKE. The figure shows a summary of IKE policy details that will be configured in examples and in the lab exercise for this lesson. The authentication method of RSA signature keys is covered in this lesson.

You will now proceed to Task 2.

CA Support Overview

This topic presents an overview of Cisco IOS software Certificate Authority (CA) support.

Cisco IOS Software CA Support Standards

Cisco IOS software supports the following CA components:

- IKE
- PKCS #7
- PKCS #10
- RSA keys
- X.509v3 certificates
- CA interoperability

Cisco IOS software supports the following open CA standards:

- IKE—A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec SAs.

- Public-Key Cryptography Standard #7 (PKCS #7)—A standard from RSA Data Security, Inc. used to encrypt, sign, and package certificate enrollment messages.

- Public-Key Cryptography Standard #10 (PKCS #10)—A standard syntax from RSA Data Security, Inc. for certificate requests.

- RSA keys—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA keys come in pairs: one public key and one private key.

- X.509v3 certificates—Certificate support that allows the IPSec-protected network to scale by providing the equivalent of a digital identification card to each device. When two devices wish to communicate, they exchange digital certificates to prove their identity (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). These certificates are obtained from a CA. X.509 is part of the X.500 standard.

- CA interoperability—CA interoperability permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented on your network without the use of a CA, using a CA with simple certificate enrollment protocol (SCEP) provides manageability and scalability for IPSec.

SCEP

- **Cisco-sponsored IETF draft**
- **Lightweight protocol to support certificate life-cycle operations on the PIX Firewall**
- **Uses PKCS #7 and PKCS #10**
- **Transaction-oriented request and response protocol**
- **Transport mechanism independent**
- **Requires manual authentication during enrollment**

Simple certificate enrollment protocol (SCEP) is a Cisco, VeriSign, Entrust, Microsoft, Netscape, and Sun Microsystems initiative that provides a standard way of managing the certificate lifecycle.

Note:	The certificate enrollment protocol (CEP) terminology used in some Cisco documentation is the same as the SCEP terminology used here.

This initiative is important for driving open development for certificate handling protocols that can be interoperable with many vendors' devices.

SCEP is described in the IETF draft which can be found at http://www.ietf.org/.

SCEP provides two authentication methods: manual authentication, and authentication based on pre-shared secret. In the manual mode, the end entity submitting the request is required to wait until the CA operator using any reliable out-of-band method can verify its identity. A Message Digest 5 (MD5) "fingerprint" generated on the PKCS# must be compared out-of-band between the server and the end entity. SCEP clients and CAs (or RAs, if appropriate) must display this fingerprint to a user to enable this verification, if manual mode is used.

When using a pre-shared secret scheme, the server should distribute a shared secret to the end entity, which can uniquely associate the enrollment request with the given end entity. The distribution of the secret must be private: only the end entity should know this secret. When creating the enrollment request, the end entity is asked to provide a challenge password.

When using the pre-shared secret scheme, the end entity must enter the redistributed secret as the password. In the manual authentication case, the challenge password is also required because the server may challenge an end entity with the password before any certificate can be revoked. Later on, this challenge password is included as a PKCS #10 attribute, and is sent to the server as encrypted data. The PKCS #7 envelope protects the privacy of the challenge password with Data Encryption Standard (DES) encryption.

There are several CA vendors that interoperate with Cisco IOS software on Cisco routers. See Cisco.com for the latest information regarding supported CA servers for your version of Cisco IOS software.

Several CA vendors support SCEP for enrolling Cisco routers. Cisco is using the Cisco Security Associate Program to test new CA and Public Key Infrastructure (PKI) solutions with the Cisco security family of products. More information on the Security Associate Program can be found at Cisco.com.

The following subtopics present several common CA servers which interoperate with Cisco IOS software:

- Entrust Technologies

- VeriSign OnSite 4.5

- Baltimore Technologies

- Microsoft Windows 2000 Certificate Services 5.0

Entrust Technologies

The Entrust CA server is one of several servers interoperable with Cisco. Entrust uses software that is installed and administered by the user. The Cisco IOS software interoperates with the Entrust/PKI 4.0 CA server. Entrust/PKI delivers the ability to issue digital identifications to any device or application supporting the X.509 certificate standard, meeting the need for security, flexibility, and low cost by supporting all devices and applications from one PKI. Entrust/PKI™ offers the following features:

- Requirements—Entrust runs on the Windows NT 4.0 (required for Cisco interoperability), Solaris 2.6, HP-UX 10.20, and AIX 4.3 operating systems. Entrust requires RSA usage keys on the routers. You must use Cisco IOS Software Release 11.(3)5T and later.

- Standards supported—Entrust supports certificate authority services, and RA capability, SCEP, and PKCS #10.

Refer to the Entrust web site at http://www.entrust.com for more information.

VeriSign OnSite 4.5

The VeriSign OnSite CA server is another CA that operates with Cisco routers. VeriSign administers the CA, providing the certificates as a service.

VeriSign's OnSite 4.5 solution delivers a fully integrated enterprise PKI to control, issue, and manage IPSec certificates for Cisco PIX Firewalls and Cisco routers. VeriSign OnSite is a service administered by VeriSign. VeriSign OnSite offers the following features:

- Requirements—There are no local server requirements. Configure the router for CA mode with a high (>60 second) retry count. You must use Cisco IOS Software Release 12.0(6.0.1)T and later. Cisco IOS Software Release 12.0(5)T is not supported because of a known bug in that release.

- Standards supported—Supports SCEP, x509 certificate format, and PKCS# 7, 10, 11, and 12.

Refer to the VeriSign web site at http://www.verisign.com for more information.

Baltimore Technologies

Baltimore Technologies has implemented support for SCEP in UniCERT (Baltimore's CA server) as well as the PKI Plus toolkit—these make it easy for customers to enable certificate within their environments. The following are the features:

- Requirements—The current release of the UniCERT CA module is available for Windows NT. You must use Cisco IOS Software Release 12.0(5)T and later.

- Standards Supported—The following standards are supported with this CA server: X509 v3, X.9.62, X.9.92, X9.21-2; CRL v2; RFC 2459; PKCS# 1,7,10,11,12; RFC 2510, RFC 2511; SCEP, LDAP v2, LDAP v3, DAP, SQL, TCP/IP, POP3, SMTP, HTTP, OCSP, FIPS 186-1, FIPS 180-1, FIPS 46-3, and FIPS 81 CBC.

Refer to the Baltimore web site at http://www.baltimore.com for more information.

Microsoft Windows 2000 Certificate Services 5.0

Microsoft has integrated SCEP support into the Windows 2000 CA server through the Security Resource Kit for Windows 2000. This support lets customers use SCEP to obtain certificates and certificate revocation information from Microsoft Certificate Services for all of Cisco's virtual private network (VPN) security solutions. The following are the features:

- Requirements—Compatible PC capable of running Windows 2000 Server. You must use Cisco IOS Software Release 12.0(5)T and above.

- Standards Supported—The following standards are supported with this CA server: X.509 version 3, CRL version 2, PKCS family (PKCS #7, #10, and #12), PKIX, SSL version 3, Kerberos v5 RFC 1510, 1964 tokens, SGC, IPSec, PKINIT, PC/SC, and IETF 2459.

The SCEP tool is not installed by the Windows 2000 Resource Kit Setup. You must install the SCEP tool separately. To install it, complete the following steps:

Step 1   Install the SCEP Add-on for Certificate Services on a root (CA). Both enterprise root CAs and stand-alone root CAs are supported.

Step 2   Log on with the appropriate administrative privileges to the server on which the root CA is installed.

Step 3   Run the cepsetup.exe file located on the Windows 2000 Resource Kit CD.

Step 4   In the SCEP Add-on for Certificate Services Setup wizard complete the following substeps:

1. Select whether or not you want to require a challenge phrase for certificate enrollment. You may wish to use a challenge phrase for added security, especially if you configure the CA to automatically grant certificates. You later obtain the challenge phrase immediately before enrolling the IPSec client by accessing the CA's URL, http://URLHostName/certsrv/mscep/mscep.dll, and copying the phrase. The phrase is then entered upon IPSec client enrollment.

2. Enter information about who is enrolling for the RA certificate, which will later allow certificates to be requested from the CA on behalf of the router.

3. (Optional.) Select Advanced Enrollment Options if you want to specify the cryptographic service provider (CSP) and key lengths for the RA signature and encryption keys.

Step 5   The URL, http://URLHostName/certsrv/mscep/mscep.dll, is displayed when the SCEP Setup wizard finishes and confirms a successful installation. URLHostName is the name of the server that hosts the CA's enrollment web pages (also referred to as Certificate Services web pages).

You may need to update the mscep.dll with a later version.

Refer to the Microsoft web site at http://www.microsoft.com for more information.

Enroll a Device with a CA

Configure CA support

Generate keys

Request the CA/RA certificate → Generate the CA/RA certificate

Authenticate the CA/RA ← Download the CA/RA certificate

Certificate request → Generate the identity certificate

Verify the identity certificate ← Download the identity certificate

SECUR 1.1—10-17
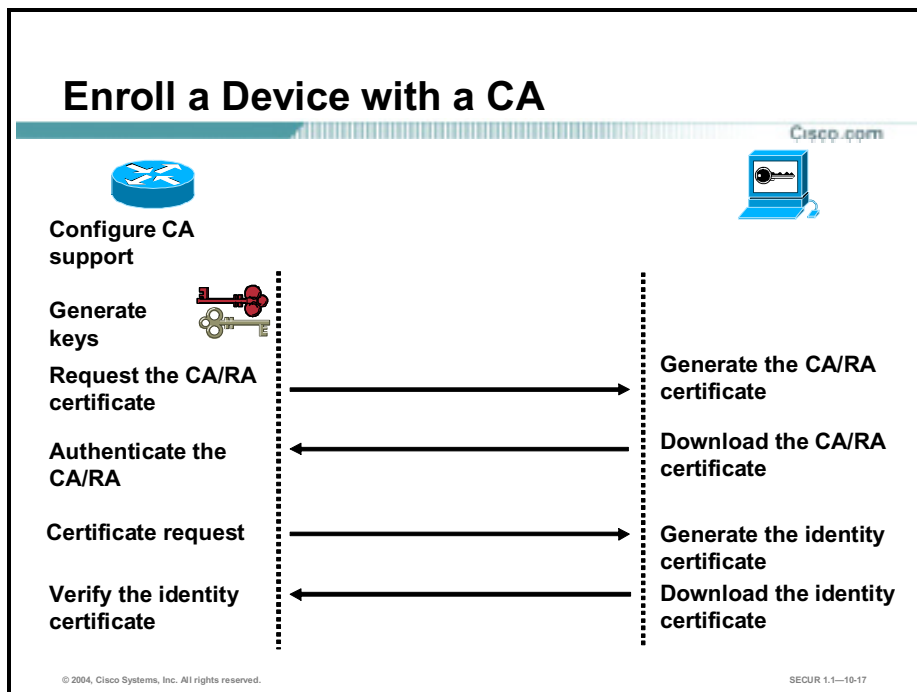
The following is the typical process for enrolling in a CA:

Step 1   Configure the router for CA support.

Step 2   Generate a public and private key-pair on the router.

Step 3   The router authenticates the CA server:

1.   Send the certificate request to the CA/RA.

2.   Generate a CA/RA certificate.

3.   Download a CA/RA certificate to a router.

4.   Authenticate a CA/RA certificate via the CA/RA finger print.

Step 4   The router sends a certificate request to the CA.

Step 5   The CA generates and signs an identity certificate.

Step 6   The CA sends the certificates to the router and posts the certificates in its public repository (directory).

Step 7   The router verifies the identify certificate and posts the certificate.

Most of these steps have been automated by Cisco and the SCEP protocol that is supported by many CA server vendors. Each vender determines how long certificates are valid**.** Contact the relevant vendor to determine how long the certificates will be valid in your particular case.

Task 2—Configure CA Support

This topic presents a detailed explanation of the steps necessary to configure Certificate Authority (CA) support on Cisco routers.

Cisco IOS Software CA Configuration Procedure

- **Step 1—(Optional.) Manage the NVRAM memory usage.**
- **Step 2—Set the router time and date:**
  ```
  clock timezone
  clock set
  ```
- **Step 3—Configure the router hostname and domain name:**
  ```
  hostname name
  ip domain-name name
  ```
- **Step 4—Generate an RSA key pair:**
  ```
  crypto key generate rsa usage keys
  ```
- **Step 5—Declare a CA:**
  ```
  crypto ca trustpoint name
  ```

SECUR 1.1—10-19

Configuring Cisco IOS software CA support is complicated. Having a detailed plan lessens the chances of improper configuration. Some planning steps and their associated commands include the following steps:

Step 1   (Optional.) Manage the non-volatile RAM (NVRAM) memory usage—In some cases, storing certificates and CRLs locally does not present a problem. However, in other cases, memory might become an issue—particularly if your CA supports an RA and a large number of CRLs end up being stored on your router.

Step 2   Set the router's time and date—The router must have an accurate time and date to enroll with a CA server.

Step 3   Configure the router's hostname and domain name—The hostname is used in prompts and default configuration filenames. The domain name is used to define a default domain name that the Cisco IOS software uses to complete unqualified hostnames.

Step 4   Generate an RSA key pair—RSA keys are used to identify the remote virtual private network (VPN) peer. You can generate one general-purpose key or two special-purpose keys.

Step 5   Declare a CA—To declare the CA your router should use, use the **crypto ca trustpoint** global configuration command. Use the **no** form of this command to delete all identity information and certificates associated with the CA.

Step 6 Authenticate the CA—The router needs to authenticate the CA. It does this by obtaining the CA's self-signed certificate that contains the CA's public key.

Step 7 Request your own certificate—Complete this step to obtain your router's identity certificate from the CA.

Step 8 Save the configuration—After configuring the router for CA support, the configuration should be saved.

Step 9 (Optional.) Monitor and maintain CA interoperability—The following substeps are optional, depending on your particular requirements:

1. Request a CRL.

2. Delete your router's RSA keys.

3. Delete both public and private certificates from the configuration.

4. Delete the peer's public keys.

Step 10 Verify the CA support configuration—The commands detailed in this topic allow you to view your and any other configured CA certificates.

Step 1—(Optional.) Manage NVRAM Memory Usage

- **Types of certificates stored on a router**
  - **The router's own identity certificate**
  - **The CA's root certificate**
  - **RA certificates (CA vendor-specific)**
- **The number of CRLs stored on a router**
  - **One, if the CA does not support an RA**
  - **Multiple, if the CA supports an RA**

SECUR 1.1—10-21

In some cases, storing certificates and CRLs locally will not present a problem. However, in other cases, memory might become an issue—particularly if your CA supports an RA and a large number of CRLs end up being stored on your router. These certificates and CRLs can consume a large amount of NVRAM space.

To save NVRAM space, you can specify that certificates and CRLs should not be stored locally, but should be retrieved from the CA when needed. This will save NVRAM space but could have a slight performance impact.

To specify that certificates and CRLs should not be stored locally on your router, but should be retrieved when required, turn on query mode by using the **crypto ca certificate query** command in global configuration mode.

Step 2—Set the Router Time and Date

router(config)#

```
clock timezone zone hours [minutes]
```

• **Sets the router time zone and offset from UTC**

```
RouterA(config)# clock timezone cst -5
```

router#

```
clock set hh:mm:ss day month year
clock set hh:mm:ss month day year
```

• **Sets the router time and date**

```
RouterA# clock set 23:59:59 31 december 2001
```

SECUR 1.1—10-22

Ensure that the router's time zone, time, and date has been accurately set with the **show clock** commands in privileged exec mode. The clock must be accurately set before generating RSA key pairs and enrolling with the CA server because certificates are time-sensitive. On certificates there is a valid from and to date and time. When the certificate is validated by the router, the router determines if its system clock falls within the validity range. If it does, the certificate is valid. If not, the certificate is deemed invalid or expired.

To specify the router's time zone, use the **clock timezone** global configuration command. The command sets the time zone and an offset from Universal Time Code (UTC, displayed by the router).

The syntax for the **clock timezone** command is as follows:

clock timezone *zone hours* [*minutes*]

zone	Name of the time zone to be displayed when standard time is in effect.
hours	Hours offset from UTC.
minutes	(Optional.) Minutes offset from UTC.

The following example sets the time zone to Central Standard Time (CST) in the United States:

```
RouterA(config)# clock timezone cst -6
```

To set the router's time and date, use the **clock set** privileged EXEC command.

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

clock set *hh:mm:ss day month year*

clock set *hh:mm:ss month day year*

hh:mm:ss	Current time in hours (military format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

The following example sets the time to one second before midnight, December 31, 2001:

```
RouterA(config)# clock set 23:59:59 31 december 2001
```

You can also optionally set your router to automatically update the calendar and time from a Network Time Protocol (NTP) server with the **ntp** series of commands.

Note: It is recommended that you use an NTP server to set the router's time on routers that do not have a clock circuit chip.

Step 3—Add a CA Server Entry to the Router Host Table

Site 1   **RouterA**   **Internet**   **RouterB**   **Site 2**

10.0.1.0   172.30.1.2   172.30.2.2   10.0.2.0

CA 172.30.1.51

router(config)#

```
hostname name
```

• **Specifies a unique name for the router**

```
router(config)# hostname RouterA
```

router(config)#

```
ip domain-name name
```

• **Specifies a unique domain name for the router**

```
RouterA(config)# ip domain-name xyz.com
```

SECUR 1.1—10-23

If the router's hostname and domain name have not previously been configured, you will need to configure them for CA support to work correctly.

To specify or modify the hostname for the network server, use the **hostname** global configuration command. The hostname is used in prompts and default configuration filenames. The setup command facility also prompts for a hostname at startup.

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

hostname *name*

name	New hostname for the network server.

To define a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name), use the **ip domain-name** global configuration command. To disable use of the DNS, use the **no** form of this command.

The command syntax for the **ip domain-name** command is as follows:

ip domain-name *name*

name	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Step 3—Add a CA Server Entry to the Router Host Table (Cont.)

Site 1
RouterA
Internet
RouterB
Site 2

10.0.1.0   172.30.1.2   172.30.2.2   10.0.2.0
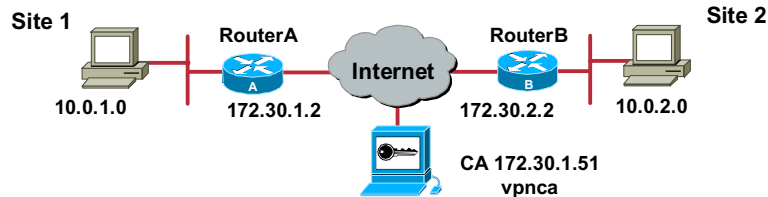
CA 172.30.1.51
vpnca

router(config)#

```
ip host name address1 [address2...address8]
```

- **Defines a static hostname-to-address mapping for the CA server**
- **Step necessary if the domain name is not resolvable**

```
RouterA(config)# ip host vpnca 172.30.1.51
```

SECUR 1.1—10-24

Use the **ip host** global configuration command to define a static hostname-to-address mapping in the host cache. To remove the name-to-address mapping, use the **no** form of this command.

The syntax for the **ip host** command is as follows:

ip host *name address1* **[***address2...address8***]**

name	Name of the host. The first character can be either a letter or a number.
address1	Associated IP address.
address2...address8	(Optional.) Additional associated IP address. You can bind up to eight addresses to a hostname.

Step 4—Generate an RSA Key Pair

Site 1   RouterA   Internet   RouterB   Site 2

10.0.1.0   A   B   10.0.2.0

CA
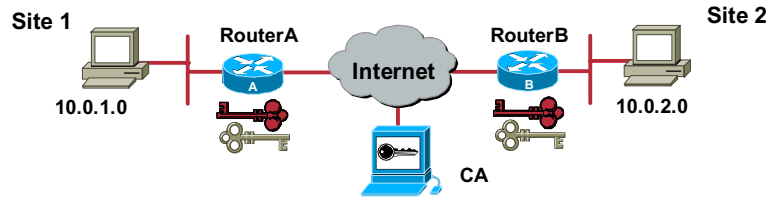
router(config)#

```
crypto key generate rsa usage-keys
```

• **Using the keyword** usage-keys **generates two sets of RSA keys:**
  – **Use one key set for RSA signatures.**
  – **Use one key set for RSA encrypted nonces.**

```
RouterA(config)# crypto key generate rsa usage-keys
```

SECUR 1.1—10-25

Use the **crypto key generate rsa** global configuration command to generate RSA key pairs.

The syntax for the **crypto key generate rsa** command is as follows:

crypto key generate rsa [*usage-keys*]

usage-keys	(Optional.) Specifies that two RSA special-usage key pairs should be generated (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.

By default, RSA key pairs do not exist. If usage-keys is not used in the command, general-purpose keys are generated. RSA keys are generated in pairs: one public RSA key and one private RSA key. If your router already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys.

Note:	Before issuing the command to generate RSA keys, make sure your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name.

The keys generated by the **generate RSA keys** command are saved in the private configuration in NVRAM, which is never displayed to the user or backed up to another device.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you can indicate whether to generate special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys are generated. One pair is used with any IKE policy that specifies RSA signatures as the authentication method, and the other pair is used with any IKE policy that specifies RSA encrypted nonces as the authentication method.

If you plan to have both types of RSA authentication methods in your IKE policies, you might prefer to generate special usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing that key's exposure.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys is generated. This pair is used with IKE policies specifying either RSA signatures or RSA encrypted nonces. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Step 4—Generate RSA Keys (Example Output)

```
RouterA(config)# crypto key generate rsa
The name for the keys will be: router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take a few
minutes.

How many bits in the modulus [512]: 512
Generating RSA keys ...
[OK]
```

```
RouterA# show crypto key mypubkey rsa
% Key pair was generated at: 23:58:59 UTC Dec 31 2000
Key name: RouterA.cisco.com
 Usage: General Purpose Key
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A9443B 62FDACFB
  CCDB8784 19AE1CD8 95B30953 1EDD30D1 380219D6 4636E015 4D7C6F33 4DC1F6E0
  C929A25E 521688A1 295907F4 E98BF920 6A81CE57 28A21116 E3020301 0001
```

SECUR 1.1—10-26

Key generation can be very time-consuming based on the router and length of the key chosen. The figure shows an example of generating a general key pair.

When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus could offer stronger security, but takes longer to generate and takes longer to use. A modulus below 512 is normally not recommended. Cisco recommends using a minimum modulus of 1024. The following table shows examples of how long it takes to generate keys of different modulus lengths:

Router	360 bits	512 bits	1024 bits	2048 bits
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	Longer than 1 hour
Cisco 4700	Less than 1 second	1 second	4 seconds	50 seconds

Step 5—Declare a CA

Site 1   RouterA   Internet   RouterB   Site 2

10.0.1.0   172.30.1.2   172.30.2.2   10.0.2.0

CA 172.30.1.51
vpnca
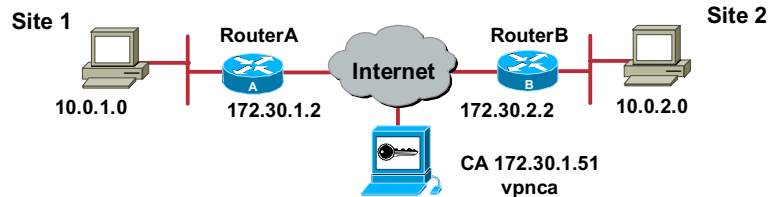
router(config)#

```
crypto ca trustpoint name
```

- **Specifies the desired CA server name**
- **Puts you in the ca-trustpoint configuration mode**

```
RouterA(config)# crypto ca trustpoint vpnca
RouterA(ca-trustpoint)#
```

SECUR 1.1—10-27

Note that in 12.2(8)T, **crypto ca trustpoint** replaces the **crypto ca identity** command from previous Cisco IOS software releases. This is done so the router will try to enroll to the CA server automatically when its certificates expire.

Use the **crypto ca trustpoint** global configuration command to declare what CA your router will use. Use the **no** form of this command to delete all identity information and certificates associated with the CA.

The syntax for the **crypto ca trustpoint** command is as follows:

crypto ca trustpoint *name*

name	Create a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.) The CA might require a particular name, such as its domain name.

Note: The **crypto ca trustpoint** command is only significant locally. It does not have to match the identity defined on any of the VPN peers.

Step 5—Commands Used to Declare a CA

```
RouterA(config)# crypto ca trustpoint vpnca
RouterA(ca-trustpoint)# ?
ca trustpoint configuration commands:
  crl          CRL option
  default      Set a command to its defaults
  enrollment   Enrollment parameters
  exit         Exit from certificate authority identity entry
               mode
  no           Negate a command or set its defaults
  query        Query parameters

RouterA(ca-trustpoint)# enrollment ?
  http-proxy   HTTP proxy server for enrollment
  mode ra      Mode supported by the Certicicate Authority
  retry        Polling parameters
  url          CA server enrollment URL\
```

SECUR 1.1—10-28

Performing the **crypto ca trustpoint** command puts you into the ca-trustpoint configuration mode, where you can specify characteristics for the CA with the following commands:

■ **enrollment url**—Specify the URL of the CA (always required).

■ **enrollment mode ra**—Specify the RA mode (required only if your CA system provides an RA).

■ **query url**—Specify the URL of the LDAP server (required only if your CA supports an RA and the LDAP protocol).

■ **enrollment retry-period**—(Optional.) Specify a period of time the router should wait between sending certificate request retries.

■ **enrollment retry-count**—(Optional.) Specify how many certificate request retries your router will send before giving up.

■ **crl optional**—(Optional.) Specify that your router can still accept other peers' certificates if the CRL is not accessible.

Step 5—Declare a CA (Example)
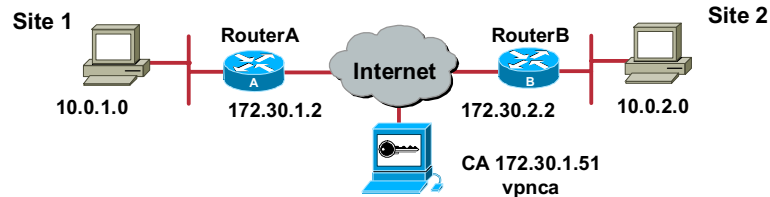
Site 1   RouterA   Internet   RouterB   Site 2

10.0.1.0   172.30.1.2   172.30.2.2   10.0.2.0

CA 172.30.1.51
vpnca

```
RouterA(config)# crypto ca trustpoint vpnca
RouterA(ca-trustpoint)# enrollment url
     http://vpnca/certsrv/mscep/mscep.dll
RouterA(ca-trustpoint)# enrollment mode ra
RouterA(ca-trustpoint)# exit
```

• **Specifies the URL for the CA server**
• **Minimum configuration to declare a CA**

The example shown in the figure declares an Entrust CA and identifies characteristics of the CA. In this example, the name *vpnca* is created for the CA, which is located at http://vpnca. The example also declares a CA using an RA. The CA's scripts are stored in the default location, and the CA uses SCEP instead of LDAP. This is the minimum possible configuration required to declare a CA that uses an RA.

The following example declares a Microsoft Windows 2000 CA. Note that the enrollment URL points to the MSCEP DLL.

```
crypto ca trustpoint labca
 enrollment mode ra
 enrollment url http://vpnca/certsrv/mscep/mscep.dll
 crl optional
```

Step 6—Authenticate the CA

Site 1   RouterA   Internet   RouterB   Site 2

10.0.1.0   10.0.2.0

Get CA/RA Cert ➡   CA 172.30.1.51
⬅ CA/RA Dnld   vpnca

CA/RA Fingerprint   CA/RA Fingerprint
xxxx aaaa zzzz bbbb ⬅➡ xxxx aaaa zzzz bbbb
Compare
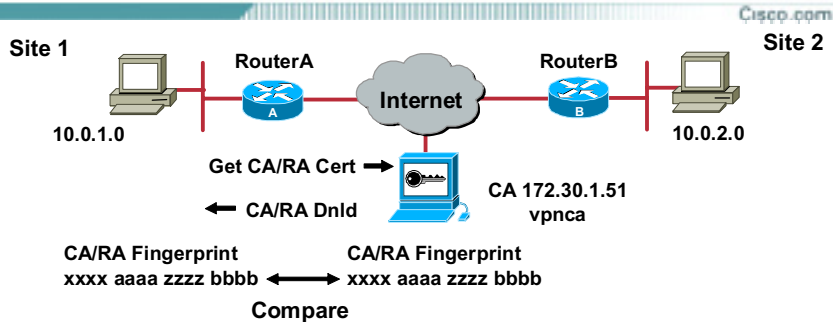
router(config)#

```
crypto ca authenticate name
```

• **Manually authenticates the CA's public key by contacting the CA administrator to compare the CA certificate's fingerprint**

```
RouterA(config)# crypto ca authenticate vpnca
```

SECUR 1.1—10-30

The router needs to authenticate the CA to verify that it is valid. The router does this by obtaining the CA's self-signed certificate that contains the CA's public key. Because the CA's certificate is self-signed (the CA signs its own certificate), the CA's public key should be manually authenticated by contacting the CA administrator to compare the CA certificate's fingerprint when you perform this step. To get the CA's public key, use the **crypto ca authenticate** *name* command in global configuration mode. Use the same name that you used when declaring the CA with the **crypto ca trustpoint** command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, the RA signing and encryption certificates are returned from the CA as well as the CA certificate.

The following example shows a CA authentication:

```
RouterA(config)# crypto ca authenticate labca
Certificate has the following attributes:
Fingerprint: 93700C31 4853EC4A DED81400 43D3C82C
% Do you accept this certificate? [yes/no]: y
```

Step 7—Request Your Own Certificate

Site 1   RouterA   Internet   RouterB   Site 2

10.0.1.0

Enroll request
and password

Identity certificate
download

CA 172.30.1.51
vpnca

10.0.2.0
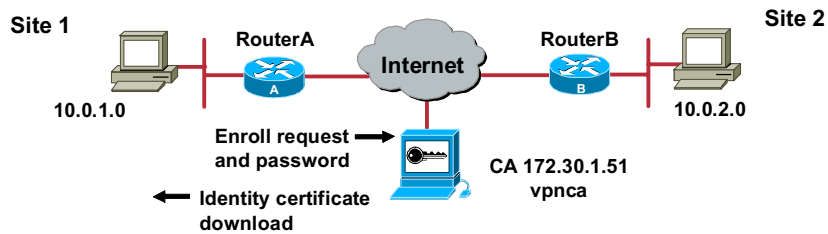
```
router(config)#
```

```
crypto ca enroll name
```

• **Requests a signed identity certificate from the CA/RA**

```
RouterA(config)# crypto ca enroll vpnca
```

SECUR 1.1—10-31

To obtain your router's identity certificate from the CA, use the **crypto ca enroll** global configuration command. Use the **no** form of this command to delete a current enrollment request.

The syntax for the **crypto ca enroll** command is as follows:

crypto ca enroll *name*

name	Specify the name of the CA. Use the same name as when you declared the CA using the **crypto ca trustpoint** command.

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as "enrolling" with the CA.

During the enrollment process, you are prompted for a challenge password, which can be used by the CA administrator to validate your identity**.** Do not forget the password you use. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when the **crypto ca enroll** command is issued.)

Your router needs a signed certificate from the CA for each of your router's RSA key pairs; if you previously generated general-purpose keys, this command obtains the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special-usage keys, this command obtains two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys, you will be unable to complete this command; instead, you are prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The following example shows a CA enrollment:

```
RouterA(config)# crypto ca enroll labca
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons, your password will not be saved in the
configuration.
    Please make a note of it.

Password: <password>
Re-enter password: <password>

% The subject name in the certificate will be: r1.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the
fingerprint.

RouterA(config)#
    Signing Certificate Request Fingerprint:
    0EE481F1 CBB4AF30 5D757610 6A4CF13D
  Encryption Certificate Request Fingerprint:
    710281D4 4DE854C7 AA61D953 CC5BD2B9
```

| Caution: | The **crypto ca enroll** command is not saved in the router configuration. If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificates, you must reissue the command. |

Step 8—Save the Configuration

Cisco.com

Site 1
RouterA
Internet
RouterB
Site 2

10.0.1.0
172.30.1.2
172.30.2.2
10.0.2.0

CA 172.30.1.51
vpnca
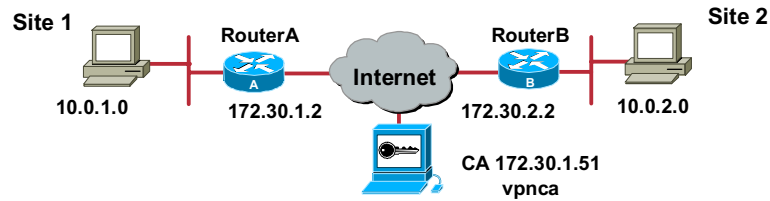
```
RouterA# copy running-config startup-config
```
• **Saves the router's running configuration to NVRAM**

SECUR 1.1—10-32

After configuring the router for CA support, the configuration should be saved using the **copy running-config startup-config** command.

The following steps are optional, depending on your particular requirements:

Step 1   Request a CRL—A CRL is not always required. If the CA server requires a CRL, you need to request one from the CA server. To request immediate download of the latest CRL, use the **crypto ca crl request** *name* command.

The syntax for the **crypto ca crl request** *name* is as follows:

crypto ca crl request *name*

name	Specify the name of the CA. Use the same name as when you declared the CA using the **crypto ca trustpoint** command.

When your router receives a certificate from a peer, it downloads a CRL from either the CA or a CRL distribution point as designated in the peer's certificate. Your router then checks the CRL to make sure the certificate the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.)

With CA systems that support RAs, multiple CRLs exist and the peer's certificate indicates which CRL applies and should be downloaded by your router. If your router does not have the applicable CRL and is unable to obtain one, your router rejects the peer's certificate—unless you include the **crl optional** command in your configuration. If you use the **crl optional** command, your router will still try to obtain a CRL, but if it cannot obtain a CRL it can still accept the peer's certificate.

When your router receives additional certificates from peers, your router continues to attempt to download the appropriate CRL, even if it was previously unsuccessful, and even if the **crl optional** command is enabled. The **crl optional** command only specifies that when the router cannot obtain the CRL, the router is not forced to reject a peer's certificate outright.

Step 2 Delete your router's RSA keys—There might be circumstances where you would want to delete your router's RSA keys. For example, if you believe the RSA keys were compromised in some way and should no longer be used, you should delete the keys. To delete all of your router's RSA keys, use the following command in global configuration mode: **crypto key zeroize rsa**.

Step 3 Delete certificates from the configuration—After you delete a router's RSA keys, you should also delete the certificates from the configuration. Complete the following substeps to do this:

1. Ask the CA administrator to revoke your router's certificates at the CA. You must supply the challenge password you created when you originally obtained the router's certificates with the **crypto ca enroll** command.

2. Manually remove the router's certificates from the router configuration. To delete your router's certificate or RA certificates from your router's configuration, use the following commands in global configuration mode:

- **show crypto ca certificates**—Views the certificates stored on your router. Note the serial number of the certificate you wish to delete.

- **crypto ca certificate chain** *name*—Enters the certificate chain configuration mode.

- **no certificate** *certificate-serial-number*—Deletes the certificate. Use the serial number you noted in the first bullet.

Note: To delete the CA's certificate, you must remove the entire CA trustpoint, which also removes all certificates associated with the CA: your router's certificate, the CA certificate, and any RA certificates. To remove a CA trustpoint, use the following command in global configuration mode: **no crypto ca trustpoint** *name*.

Step 4 Delete the peer's public keys—There might be circumstances where you would want to delete other peer's RSA public keys from your router's configuration. For example, if you no longer trust the integrity of a peer's public key, you should delete the key. To delete the peer's public keys, use the following commands:

- **crypto key pubkey-chain rsa**—Enter the public key chain configuration mode.

- **no named-key** *key-name* **[encryption | signature]** or **no addressed-key** *key-address* **[encryption | signature]**—Delete a remote peer's RSA public key. Specify the peer's fully qualified domain name or the remote peer's IP address. You can optionally delete just the encryption key or the signature key by using the encryption or signature keywords.

Step 10—Verify the CA Support Configuration

Site 1
RouterA
Internet
RouterB
Site 2
10.0.1.0
172.30.1.2
172.30.2.2
10.0.2.0
CA 172.30.1.51
vpnca
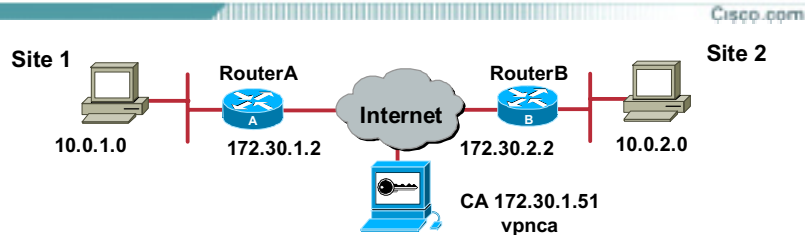
router#

```
show crypto ca certificates
```

• View any configured CA/RA certificates

router#

```
show crypto key mypubkey │ pubkey-chain rsa
```

• View RSA keys for your router and other IPSec peers enrolled with a CA

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—10-34

The following example illustrates the result of the **show crypto ca certificates** command:

```
RouterA# show crypto ca certificates


Certificate
  Subject Name
    Name: myrouter.xyz.com
        IP Address: 172.30.1.2
    Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose


CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto key mypubkey rsa** command. Special usage RSA keys were previously generated for this router using the **crypto key generate rsa** command:

```
% Key pair was generated at: 23:57:50 UTC Dec 31 2000
Key name: myrouter.xyz.com
  Usage: Signature Key
  Key Data:
    005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22
```

```
    04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C
73A05DD2
   BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001
% Key pair was generated at: 23:58:59 UTC Dec 31 2000
Key name: myrouter.xyz.com
  Usage: Encryption Key
  Key Data:
 00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748
429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD
9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

The following is sample output from the **show crypto key pubkey-chain rsa** command:

```
Codes: M - Manually Configured, C - Extracted from certificate
Code        Usage              IP-address          Name
M           Signature          10.0.0.l            myrouter.domain.com
M           Encryption         10.0.0.1            myrouter.domain.com
C           Signature          172.30.1.2          RouterA.domain.com
C           Encryption         172.30.1.2          RouterA.domain.com
C           General            172.30.2.2          RouterB.domain1.com
```

This sample shows manually configured special usage RSA public keys for the peer somerouter. This sample also shows three keys obtained from peers' certificates: special-usage keys for peer RouterA and a general-purpose key for peer RouterB.

Certificate support is used in the previous example; if certificate support was not in use, none of the peers' keys would show *C* in the code column, but would all have to be manually configured.

CA Support Configuration Example

```
RouterA# show running-config
!
hostname RouterA
!
ip domain-name cisco.com
!
crypto ca trustpoint mycaserver
 enrollment mode ra
 enrollment url http://vpnca:80
 query url ldap://vpnca
 crl optional
crypto ca certificate chain entrust
 certificate 37C6EAD6
  30820299 30820202 A0030201 02020437 C6EAD630 0D06092A
  864886F7 0D010105
  (certificates concatenated)
```

The figure displays the running-config of a router properly configured for CA support.

Task 3—Configure IKE

The next major task in configuring Cisco IOS software IPSec is to configure Internet Key Exchange (IKE) parameters gathered earlier. This topic presents the steps used to configure IKE policies.

Task 3—Configure IKE

- **Step 1—Enable or disable IKE:**
  `crypto isakmp enable`
- **Step 2—Create IKE policies:**
  `crypto isakmp policy`
- **Step 3—Set IKE identity:**
  `crypto isakmp identity`
- **Step 4—Test and verify IKE configuration:**
  `show crypto isakmp policy`
  `show crypto isakmp sa`

SECUR 1.1—10-37

| **Note:** | The following steps are identical to configuring pre-shared keys except for Step 2. Refer to the previous lesson for the detailed explanation of each step not covered here. |

Configuring IKE consists of the following essential steps and commands:

Step 1 Enable or disable IKE with the **crypto isakmp enable** command.

Step 2 Create IKE policies with the **crypto isakmp policy** command.

Step 3 Set the IKE identity to address or hostname with the **crypto isakmp identity** command.

Step 4 Test and verify the IKE configuration with the **show crypto isakmp policy** and **show crypto isakmp sa** commands.

Step 2—Create IKE Policies
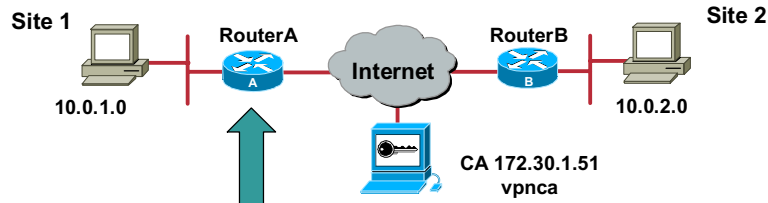
```
RouterA(config)# crypto isakmp policy 110
RouterA(config-isakmp)# authentication rsa-sig
RouterA(config-isakmp)# encryption des
RouterA(config-isakmp)# group 1
RouterA(config-isakmp)# hash md5
RouterA(config-isakmp)# lifetime 86400
```

SECUR 1.1—10-38

The **crypto isakmp policy** command invokes the ISAKMP policy configuration command mode (config-isakmp) where you can set ISAKMP parameters. If you do not specify one of these commands for a policy, the default value is used for that parameter. While in the **config-isakmp** command mode, the following keywords are available to specify the parameters in the policy:

Command	Keywords	Accepted Values	Default Value	Description
encryption	**des** **3des** **aes**	56-bit only 168-bit Choose 128-, 192-, or 256-bit	des	Message encryption algorithm
hash	**sha** **md5**	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha	Message integrity (hash) algorithm
authen	**rsa-sig** **rsa-encr** **pre-share**	RSA signatures RSA encrypt nonces Pre-shared keys	rsa-sig	Peer authentication method
group	**1** **2**	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1	Key exchange parameters (DH group identifier)
lifetime	-	Can specify any number of seconds	86,400 seconds (one day)	ISAKMP-established SA lifetime; usually can be left at the default

You can configure multiple ISAKMP policies on each peer participating in IPSec. ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPSec.

Task 4—Configure IPSec

The next major task in configuring Cisco IOS software IPSec is to configure the IPSec parameters previously gathered. This topic presents the steps used to configure IPSec.

Steps to Complete Task 4—Configure IPSec

- **Step 1—Configure transform set suites:**
  `crypto ipsec transform-set`
- **Step 2—Configure global IPSec SA lifetime:**
  `crypto ipsec security-association lifetime`
- **Step 3—Create crypto ACLs:**
  `access-list`

SECUR 1.1—10-40

Note: The following steps are identical to configuring pre-shared keys.

The general steps and commands used to configure IPSec encryption on Cisco routers are summarized as follows:

Step 1   Configure transform set suites with the **crypto ipsec transform-set** command.

Step 2   Configure global IPSec SA lifetimes with the **crypto ipsec security-association lifetime** command.

Step 3   Configure crypto ACLs with the **access-list** command.

Step 4   Configure crypto maps with the **crypto map** command.

Step 5   Apply the crypto maps to the terminating or originating interface with the **interface** and **crypto map** commands.

Task 5—Test and Verify IPSec

Cisco IOS software contains a number of **show**, **clear**, and **debug** commands useful for testing and verifying IPSec and ISAKMP, which are considered in this topic.

Steps to Complete Task 5—Test and Verify IPSec

- **Step 1—Display your configured IKE policies:**
  `show crypto isakmp policy`
- **Step 2—Display your configured transform sets:**
  `show crypto ipsec transform set`
- **Step 3—Display the current state of your IPSec SAs:**
  `show crypto ipsec sa`

Note:	Although many of the test and verify commands are used the same as when configuring pre-shared keys, there are some commands unique to RSA signatures.

Complete the following steps to test and verify that you have correctly configured a VPN using Cisco IOS software:

Step 1 Display your configured IKE policies using the **show crypto isakmp policy** command.

Step 2 Display your configured transform sets using the **show crypto ipsec transform set** command.

Step 3 Display the current state of your IPSec SAs with the **show crypto ipsec sa** command.

Steps to Complete Task 5—Test and Verify IPSec (Cont.)

- **Step 4—Display your configured crypto maps:**
  `show crypto map`
- **Step 5—Enable debug output for IPSec events:**
  `debug crypto ipsec`
- **Step 6—Enable debug output for ISAKMP events:**
  `debug crypto isakmp`

SECUR 1.1—10-44

Step 4 View your configured crypto maps with the **show crypto map** command.

Step 5 Debug IKE and IPSec traffic through the Cisco IOS software with the **debug crypto ipsec** command.

Step 6 Debug IKE and IPSec traffic through the Cisco IOS software with the **debug crypto isakmp** command.

Caution: Use **debug** commands with caution. In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems. Enabling debugging can disrupt operation of the router when internetworks are experiencing high load conditions.

Before you start a **debug** command, always consider the output that this command will generate and the amount of time this may take.

Before debugging, look at your CPU load using the **show processes cpu** command. Verify that you have ample CPU available before beginning the debugs.

Note: When debugs are running, you do not usually see the router prompt, especially when the debug is intensive. However, in most cases, you can use the **no debug all** or **undebug all** commands to stop the debugs.

Steps to Complete Task 5—Test and Verify IPSec (Cont.)

- **Step 7—Enable debug output for CA events:**
  ```
  debug crypto key-exchange
  debug crypto pki {messages|transactions}
  ```

SECUR 1.1—10-45

Step 7   Debug CA events through the Cisco IOS software with the **debug crypto key-exchange** and **debug crypto pki** commands.

Summary

This topic summarizes the tasks you learned to complete in this lesson.

Summary

- **Define the detailed crypto CA, IKE, and IPSec security policy before beginning configuration.**
- **Ensure that you can contact your CA administrator before beginning configuration.**
- **Configure CA details before configuring IKE.**
- **Manually verify the CA certificate with the CA administrator. Each CA server supported by Cisco IOS software has a slightly different configuration process.**
- **Use the RSA signatures authentication method for IKE when using CA support.**
- **The IPSec configuration process is the same as that used for pre-shared and RSA encrypted nonces authentication.**

SECUR 1.1—10-47

Lab Exercise—Configure Cisco IOS CA Support (RSA Signatures)

Complete the following lab exercise to practice what you learned in this lesson.

Objectives

The objective of this lab exercise is to work with a partner to configure a Cisco router to enable IPSec encrypted tunnels using RSA signatures for authentication to another Cisco router. In this lab exercise you will complete the following tasks:

■ Complete the lab exercise setup.

■ Prepare for IKE and IPSec.

■ Configure CA support.

■ Configure IKE.

■ Configure IPSec.

■ Test and verify IPSec.

■ (Optional.) Fine-tune the ACL.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.
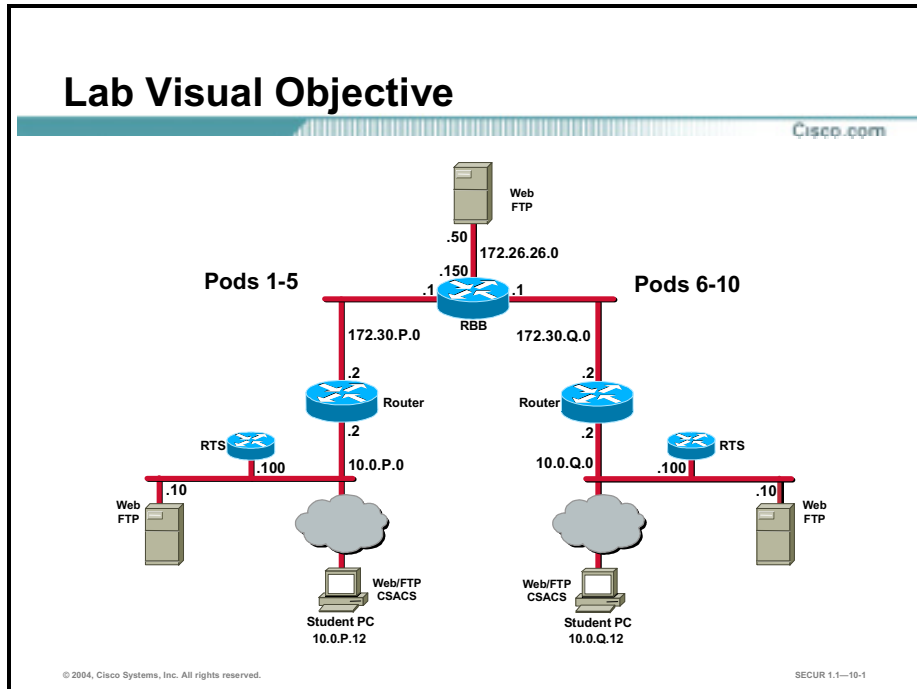
CA and IKE Command and Keyword List

In this lab exercise, you will use the following commands and keywords in the order listed. Refer to this list if you need assistance during the lab exercise.

Command and Keywords	Description
config terminal	Enters configuration mode.
crypto isakmp ?	Displays crypto ISAKMP options.
ping	Verifies communication with destination.
ip domain-name cisco.com	Defines the router's domain name.
ip host	Defines the CA server's static hostname-to-IP address mapping.
crypto key generate rsa usage-keys	Generates RSA usage-keys.
crypto ca trustpoint	Creates a name for the CA.
enrollment mode ra	Chooses the registration authority mode.
enrollment url http://vpnca	Specifies the URL of the CA.
crl optional	Specifies that your router can still accept other peers' certificates if the CRL is not accessible.
crypto ca authenticate labca	Authenticates the CA server. Verifies the fingerprint of the CA server with the CA administrator.
crypto ca enroll labca	Enrolls to the CA server.

Command and Keywords	Description
show crypto ca certificate	Shows the CA certificates.
crypto isakmp enable	Enables Internet Key Exchange (IKE) on the Router.
crypto isakmp policy	Used to create IKE policy.
authentication	Sets IKE authentication method.
encryption	Sets IKE encryption method.
group	Sets Diffie-Hellman group number.
hash	Sets hash algorithm.
lifetime	Sets lifetime in seconds and KB.
exit	Exits current config mode.
crypto isakmp trustpoint address	Sets isakmp trustpoint to address.

Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your lab exercise environment:

Step 1 Ensure that your Windows 2000 server is operating with the correct date and time.

Step 2 Ensure that your router is turned on.

Step 3 Access the router's console port.

Step 4 Reset your router to the default configuration.

Step 5 Ensure that you can ping from your router to the opposite pod group's router.

Step 6 Ensure that you can ping from your Windows 2000 server to the opposite pod group's Windows 2000 server.

Step 7 Build a static route to the 172.27.27.0/24 network (where P = pod number):

```
RP(config)# ip route 172.27.27.0 255.255.255.0 172.30.P.1
```

Task 2—Prepare for IKE and IPSec

Complete the following steps to prepare for IPSec configuration:

Step 1 Determine the Internet Key Exchange (IKE) and IPSec policy. In this lab exercise, you will use default values except when you are directed to enter a specific value:

- The IKE policy is to use RSA Signature keys.

- The IPSec policy is to use Encapsulating Security Payload (ESP) mode with Data Encryption Standard (DES).

- The IPSec policy is to encrypt all traffic between perimeter routers.

Step 2 Set the router's time zone, calendar, and time:

```
RP(config)# clock timezone zone hours [minutes]
RP# clock set hh:mm:ss day month year
```

Step 3 Verify that you have connectivity with the other group's router:

```
RP# ping 172.30.Q.2
```

(where Q = peer pod number)

Step 4 Ensure that you can connect to the Certificate Authority (CA) server from your router:

```
RP# ping 172.26.26.51
```

Step 5 Ensure that you can establish an HTTP session to the CA server. Test this capability from your Windows 2000 server by opening a web browser and entering the location: **http://172.26.26.51/certsrv**.

Step 6 Turn on console logging to view the debug output:

```
RP# config terminal
RP(config)# logging console
```

Task 3—Configure CA Support

Complete the following steps to configure CA support on your Cisco router (work with the CA server administrator to complete this portion of the lab exercise):

Step 1 Define the router's domain name:

```
RP(config)# ip domain-name cisco.com
```

Step 2 Define the CA server's static hostname-to-IP address mapping:

```
RP(config)# ip host vpnca 172.26.26.51
```

Step 3 Generate RSA usage-keys:

```
RP(config)# crypto key generate rsa usage-keys
```

Note: Follow the router prompts to complete the task. Use **512** for the number of bits for the modulus.

Step 4 Complete the following substeps to configure the CA server trustpoint:

1. Create a name for the CA and enter ca-trustpoint mode:

```
RP(config)# crypto ca trustpoint vpnca
```

2. Choose the registration authority mode:

```
RP(ca-trustpoint)# enrollment mode ra
```

3. Specify the URL of the CA:

■   For an Entrust CA:

```
RP(ca-trustpoint)# enrollment url http://vpnca
```

■   For a Microsoft CA:

```
RP(ca-trustpoint)# enrollment url http://vpnca/certsrv/mscep/mscep.dll
```

Note: Check with your instructor to determine the type of CA used in this course.

---

4. Specify that your router can still accept other peers' certificates if the certificate revocation list (CRL) is not accessible:

```
RP(ca-trustpoint)# crl optional
```

5. Exit CA configuration mode:

```
RP(ca-trustpoint)# ^Z
RP# copy running-config startup-config
```

6. Turn on Public Key Infrastructure (PKI) debugging so you can observe debug messages for the CA process:

```
RP# debug crypto pki messages
RP# debug crypto pki transactions
```

7. Authenticate the CA server. Verify the fingerprint of the CA server with the CA administrator:

```
RP# config term
RP(config)# crypto ca authenticate vpnca
Certificate has the following attributes:
Fingerprint: 527D8DCA 4D52A047 C8DA1DAD D5368629
% Do you accept this certificate? [yes/no]: y
```

Note: Because debug is on, several full screen messages flash by, which may require you to press **Enter** to see this question.

---

8. Enroll the CA server using the **crypto ca enroll** command as shown here. Ensure that the CA administrator accepts your enrollment request. Answer the prompts as shown in the example.

Caution: Stop and ensure that the instructor is ready to accept your enrollment request before continuing to the next step.

```
RP(config)# crypto ca enroll vpnca
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the
configuration. Please make a note of it.
Password: cisco
Re-enter password: cisco

% The subject name in the certificate will be: r1.cisco.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [yes/no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
```

```
% The 'show crypto ca certificate' command will also show the
fingerprint.
```

9. Verify the CA certificates:

```
RP(config)# exit

RP# copy running-config startup-config

RP# show crypto ca certificate
```

Task 4—Configure IKE

Work with the members of your peer's pod and complete the following steps to configure IKE on your Cisco router:

Note:	While entering commands, notice when the command line prompt changes because it will help you to notice what configuration mode you are in.

Step 1 Enable IKE/ISAKMP on your router:

```
RP(config)# crypto isakmp enable
```

Step 2 Create an IKE policy to use RSA signatures by completing the following substeps:

1. Set the policy priority:

```
RP(config)# crypto isakmp policy 110
```

2. Set authentication to use RSA signatures:

```
RP(config-isakmp)# authentication rsa-sig
```

3. Set the IKE encryption:

```
RP(config-isakmp)# encryption des
```

4. Set the Diffie-Hellman group:

```
RP(config-isakmp)# group 1
```

5. Set the hash algorithm:

```
RP(config-isakmp)# hash md5
```

6. Set the IKE Security Association (SA) lifetime:

```
RP(config-isakmp)# lifetime 86400
```

7. Exit config-isakmp mode:

```
RP(config-isakmp)# exit
```

Task 5—Configure IPSec

Complete the following steps to configure IPSec on your Cisco router:

Configure Transform Sets and SA Parameters

Complete the following steps to configure transform sets and Security Association (SA) parameters:

Step 1 Ensure that you are in configuration mode:

```
router# config terminal
```

Step 2 View the available crypto IPSec command options:

```
RP(config)# crypto ipsec ?
```

Step 3 Check your transform set options:

```
RP(config)# crypto ipsec transform-set ?
```

Step 4 Define a transform set. Use the following parameters:

- Transform name = **mine**

- ESP protocols = **des**

- Mode = **tunnel**

```
RP(config)# crypto ipsec transform-set mine esp-des
```

Step 5 Set the mode to tunnel:

```
RP(cfg-crypto-trans)# mode tunnel
```

Step 6 Exit configuration mode:

```
RP(cfg-crypto-trans)# ^Z
```

Step 7 Check your configuration:

```
RP# show crypto ipsec transform-set mine
Transform set mine: { esp-des  }
   will negotiate = { Tunnel,  },
```

Configure Crypto ACLs

Complete the following steps to configure the crypto access control lists (ACLs). Create an ACL to select traffic to protect. The ACL should encrypt traffic between perimeter routers. Use the following parameters:

- Traffic permitted = **all**

- Peer address = **Peer router Ethernet interface**

- Access list number = **102**

- Protocol = **IP**

Step 1 Ensure that you are in configuration mode:

```
RP(config)# config terminal
```

Step 2   Configure the access list:

```
RP(config)# access-list 102 permit ip host 172.30.P.2 host 172.30.Q.2
```

(where P = pod number, and Q = peer pod number)

Configure Crypto Maps

Complete the following steps to configure a crypto map. Use the following parameters:

- Name of map = **mymap**
- Number of map = **10**
- Key exchange type = **isakmp**
- Peer = **172.30.Q.2**
- Transform set = **mine**
- Match address = **102**

Step 1   Set the name of the map, the map number, and the type of key exchange to be used (where P = pod number, and Q = peer pod number):

```
RP(config)# crypto map mymap 10 ipsec-isakmp
```

Step 2   Specify the extended access list to use with this map:

```
RP(config-crypto-map)# match address 102
```

Step 3   Specify the transform-set you defined earlier:

```
RP(config-crypto-map)# set transform-set mine
```

Step 4   Assign the virtual private network (VPN) peer using the hostname or IP address of the peer:

```
RP(config-crypto-map)# set peer 172.30.Q.2
```

Step 5   Exit crypto-map configuration mode:

```
RP(config-crypto-map)# exit
```

Apply the Crypto Map to an Interface

Complete the following steps to assign the crypto map to the appropriate router interface. Use the following parameters:

- Interface to configure = **fast 0/1**
- Crypto map to use = **mymap**

Step 1   Access the interface configuration mode:

```
RP(config)# interface fast 0/1
```

Step 2   Assign the crypto map to the interface:

```
RP(config-if)# crypto map mymap
```

Step 3   Exit configuration crypto mode:

```
RP(config-if)# ^Z
```

Task 6—Test and Verify IPSec

Complete the following steps to verify and test your IPSec configuration. Coordinate your test with your peer router's pod group:

Step 1   Display your configured IKE policies:

```
RP# show crypto isakmp policy
Protection suite of priority 110
        encryption algorithm:   DES - Data Encryption Standard (56 bit
                                keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adelman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit
                                keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adelman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Step 2   Display your configured transform sets:

```
RP# show crypto ipsec transform-set
Transform set mine: { esp-des  }
   will negotiate = { Tunnel,  },
```

Step 3   Display your configured crypto maps (where P = pod number, and Q = peer pod number):

```
RP# show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
        Peer = 172.30.Q.2
        Extended IP access list 102
            access-list 102 permit ip host 172.30.P.2 host 172.30.Q.2
        Current peer: 172.30.Q.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ mine, }
```

Step 4   Display the current state of your IPSec SAs. IPSec SAs may have already been established by routing traffic(where P = pod number, and Q = peer pod number):

```
RP# show crypto ipsec sa
interface: Ethernet0/1
    Crypto map tag: mymap, local addr. 172.30.P.2


   local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
```

```
      remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
   current_peer: 172.30.Q.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2
    path mtu 1500, media mtu 1500
    current outbound spi: 8AE1C9C

    inbound esp sas:
     spi: 0x1B781456(460854358)
       transform: esp-des ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 17, crypto map: mymap
       sa timing: remaining key lifetime (k/sec): (4607997/3107)
       IV size: 8 bytes
       replay detection support: N

    inbound ah sas:

    outbound esp sas:
     spi: 0x8AE1C9C(145628316)
       transform: esp-des ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 18, crypto map: mymap
       sa timing: remaining key lifetime (k/sec): (4607997/3107)
       IV size: 8 bytes
       replay detection support: N

    outbound ah sas:
```

Step 5   Clear any existing SAs:

```
RP# clear crypto sa
```

Step 6   Enable debug output for IPSec events:

```
RP# debug crypto ipsec
```

Step 7   Enable debug output for ISAKMP events:

```
RP# debug crypto isakmp
```

Step 8   Initiate a ping to your peer pod's perimeter router. Observe the IKE and IPSec debug output.

```
RP# ping 172.30.Q.2
```

Step 9 Verify IKE and IPSec SAs. Note the number of packets encrypted and decrypted when viewing the IPSec SAs (where P = pod number, and Q = peer pod number).

```
RP# show crypto isakmp sa
dst             src             state           conn-id   slot
172.30.Q.2      172.30.P.2      QM_IDLE             16        0


RP# show crypto ipsec sa
interface: Ethernet0/1
    Crypto map tag: mymap, local addr. 172.30.P.2


   local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
   current_peer: 172.30.Q.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 26, #pkts encrypt: 26, #pkts digest 0
    #pkts decaps: 26, #pkts decrypt: 26, #pkts verify 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2
     path mtu 1500, media mtu 1500
     current outbound spi: 8AE1C9C

     inbound esp sas:
      spi: 0x1B781456(460854358)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 17, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4607996/2963)
        IV size: 8 bytes
        replay detection support: N



     inbound ah sas:

     outbound esp sas:
      spi: 0x8AE1C9C(145628316)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 18, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4607996/2963)
```

```
                IV size: 8 bytes
                replay detection support: N


        outbound ah sas:
```

Step 10 Ensure that encryption is working between the routers by first generating additional traffic, and then by observing that the packets encrypted and decrypted counter has incremented (where P = pod number, and Q = peer pod number):

```
RP# ping 172.30.Q.2
RP# show crypto ipsec sa
interface: Ethernet0/1Ethernet0/1
    Crypto map tag: mymap, local addr. 172.30.P.2


  local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
  current_peer: 172.30.Q.2
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 31, #pkts encrypt: 31, #pkts digest 0
   #pkts decaps: 31, #pkts decrypt: 31, #pkts verify 0
   #send errors 0, #recv errors 0


   local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2
   path mtu 1500, media mtu 1500
   current outbound spi: 8AE1C9C


   inbound esp sas:
    spi: 0x1B781456(460854358)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 17, crypto map: mymap
      sa timing: remaining key lifetime (k/sec): (4607995/2954)
      IV size: 8 bytes
      replay detection support: N


   inbound ah sas:


   outbound esp sas:
    spi: 0x8AE1C9C(145628316)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 18, crypto map: mymap
```

```
                sa timing: remaining key lifetime (k/sec): (4607996/2954)
                IV size: 8 bytes
                replay detection support: N

        outbound ah sas:
```

Note: The packet counters have increased from Step 9 because of the encrypted traffic.

Task 7—(Optional.) Fine-Tune the ACL

Fine-tune the crypto access control lists (ACLs) used to determine interesting traffic to encrypt traffic only between the internal NT servers. Remember to work with your peer pod group to make the ACL symmetrical between the perimeter routers. Ensure that desired traffic is encrypted between peers.

Step 1   Remove the previously configured ACL:

```
RP(config)# no access-list 102
```

Step 2   Configure a new ACL for the Windows 2000 servers:

■   For a remote lab, enter the following:

```
RP(config)# access-list 102 permit ip host 10.1.P.12 host 10.1.Q.12
```

(where P = pod number, and Q = peer pod number)

■   For a local lab, enter the following:

```
RP(config)# access-list 102 permit ip host 10.0.P.12 host 10.0.Q.12
```

(where P = pod number, and Q = peer pod number)

Step 3   Verify your configuration by connecting to the web server at **10.1.Q.12** for a remote lab exercise, or **10.0.Q.12** for a local lab exercise, using the browser on your Windows 2000 server (where P = pod number, and Q = peer pod number).

Step 4   Verify your router configuration using the **show run** command against the following sample configuration for router R2:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rP
!
no logging console
enable password cisco
!
ip subnet-zero
```

```
clock timezone cst -5
no ip domain-lookup
ip domain-name cisco.com
!
!
crypto isakmp policy 110
 hash md5
 authentication rsa-encr
!
!
crypto ipsec transform-set mine esp-des
!
!
crypto key pubkey-chain rsa
 addressed-key 172.30.P.2
  address 172.30.P.2
  key-string
    305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A9443B
62FDACFB
    CCDB8784 19AE1CD8 95B30953 1EDD30D1 380219D6 4636E015 4D7C6F33
4DC1F6E0
   C929A25E 521688A1 295907F4 E98BF920 6A81CE57 28A21116 E3020301 0001
  quit
 !
 crypto map mymap 10 ipsec-isakmp
 set peer 172.30.Q.2
 set transform-set mine
 match address 102
!

 Ethernet0/0
 ip address 10.0.P.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Ethernet0/1
 ip address 172.30.P.2 255.255.255.0
 no ip directed-broadcast
```

```
 crypto map mymap
!
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 network 192.168.1.0
 no auto-summary
!
ip classless
ip http server
!
access-list 102 permit ip host 172.30.P.2 host 172.30.Q.2
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
 transport input all
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
end
```

11

Configuring Cisco IOS Remote Access Using Cisco Easy VPN

Overview

This lesson covers the configuration of Cisco IOS remote access using the Cisco Easy Virtual Private Network (VPN) and the Cisco VPN Client.

It includes the following topics:

■ Objectives

■ Introduction to the Cisco Easy VPN

■ How the Cisco Easy VPN works

■ Configuring the Easy VPN Server

■ Configuring Easy VPN Remote for the Cisco VPN Client 3.x

■ Using the Cisco VPN Client 3.x

■ Configuring Easy VPN Remote for access routers

■ Summary

■ Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

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

- **Describe the Easy VPN Server.**
- **Describe the Easy VPN Remote.**
- **Configure the Easy VPN Server.**
- **Configure the Easy VPN Remote using the Cisco VPN Client 3.x.**

SECUR 1.1—11-3

Introduction to the Cisco Easy VPN

This topic discusses the Cisco Easy VPN and its two components.

Cisco Easy VPN Components

Cisco.com

The Cisco Easy VPN is made up of two components:

- **Easy VPN Server—Enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN 3000 Series Concentrators to act as VPN head-end devices in site-to-site or remote-access VPNs, where the remote office devices are using the Cisco Easy VPN Remote feature**
- **Easy VPN Remote—Enables Cisco IOS routers, Cisco PIX Firewalls, and Cisco VPN 3002 Hardware Clients or Software Clients to act as remote VPN Clients**

SECUR 1.1—11-5

Cisco Easy VPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies virtual private network (VPN) deployment for remote offices and teleworkers. Based on the Cisco Unified Client framework, the Cisco Easy VPN centralizes VPN management across all Cisco VPN devices, greatly reducing the complexity of VPN deployments. The Cisco Easy VPN enables an integration of Easy VPN Remotes—Cisco routers, Cisco PIX Firewalls, and Cisco VPN 3002 Hardware Clients or Software Clients— within a single deployment with a consistent policy and key management method that simplifies remote-side administration.

The Cisco Easy VPN consists of two components: the Cisco Easy VPN Server and the Cisco Easy VPN Remote feature.

The Easy VPN Server

The Easy VPN Server enables Cisco IOS routers, PIX Firewalls, and Cisco VPN 3000 Series Concentrators to act as VPN headend devices in site-to-site or remote-access VPNs, where the remote office devices are using the Easy VPN Remote feature. Using this feature, security policies defined at the headend are pushed to the remote VPN device, ensuring that those connections have up-to-date policies in place before the connection is established.

In addition, an Easy VPN Server-enabled device can terminate IPSec tunnels initiated by mobile remote workers running VPN Client software on PCs. This flexibility makes it possible for mobile and remote workers, such as salespeople on the road or teleworkers, to access their headquarters intranet where critical data and applications exist.

The Easy VPN Remote Feature

The Easy VPN Remote feature enables Cisco IOS routers, PIX Firewalls, and Cisco VPN 3002 Hardware Clients or Software Clients to act as remote VPN Clients. These devices can receive security policies from an Easy VPN Server, minimizing VPN configuration requirements at the remote location. This cost-effective solution is ideal for remote offices with little information technology (IT) support or for large customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices. This feature makes VPN configuration as easy as entering a password, which increases productivity and lowers costs because the need for local IT support is minimized.

Cisco Easy VPN Server Releases

- **Cisco IOS Software Release 12.2(8)T (Easy VPN Phase 1)— Provided support for Cisco VPN Client 3.x software clients and hardware clients, mode configuration version 6 support, XAUTH version 6 support, IKE DPD, split tunneling control, and group-based policy control**
- **Cisco IOS Software Release 12.2(13) (Easy VPN Phase 1.1)— Added support for AES, IPSec NAT transparency, VAM card support, group lock, and idle timeout**
- **Cisco IOS Software Release 12.3(1st)T (Easy VPN Phase 2.0)— Added support for exclude local LAN, firewall "are you there," split tunnel checking for PC clients, and saving of XAUTH password at remote**
- **Cisco IOS Software Release 12.3(2)XA—Added Easy VPN Server support for 83X platforms**

This figure identifies Easy VPN Server phased releases and their required Cisco IOS software releases. It is important to understand which features are offered by the various Easy VPN phases and their respective Cisco IOS software releases.

Cisco Easy VPN Remote Releases

- **12.2(4)YA & 12.2(13)T (Phase 1)—Provided support for client mode, network extension mode, and XAUTH**
- **12.2(8)YJ (Phase 2)—Added support for manual tunnel control, Web interface for uBR900, CRWS support for Cisco 800 Series, multiple inside and outside interface support, and static NAT interoperability**
- **12.2(15)T (Phase 3.0)—Added support for IPSec NAT transparency (UDP), secure ID support for XAUTH, and Cisco 2600/3600 Series support**
- **12.2(13)ZH (Special)—Added support for IPSec NAT transparency (UDP), 831 support, XAUTH save password and username saving option, peer backup (multiple peer support), and SDM**
- **12.3(1)T (Phase 3.1)—Added support for AES, Easy VPN key garbled, and IP compression**
- **12.3(2)T—Added support for type 6 password**
- **12.3(4)T—Added support for save password feature**

SECUR 1.1—11-7

This figure identifies Easy VPN Remote phased releases and their required Cisco IOS software releases. It is important to understand which features are offered by the various Easy VPN phases and their respective Cisco IOS software releases.

Always consult Cisco.com for the latest information regarding Easy VPN features and the supporting Cisco IOS software releases.

Remote Access Using Cisco Easy VPN

SECUR 1.1—11-8

PC with Easy Remote VPN Client 3.x

Cisco 800 Router

Cisco 900 Router

Cisco 1700 Router

Cisco IOS router 12.2(8)T (or later) Easy VPN Server

Cisco PIX 501 Firewall

Cisco VPN 3002 Hardware Client
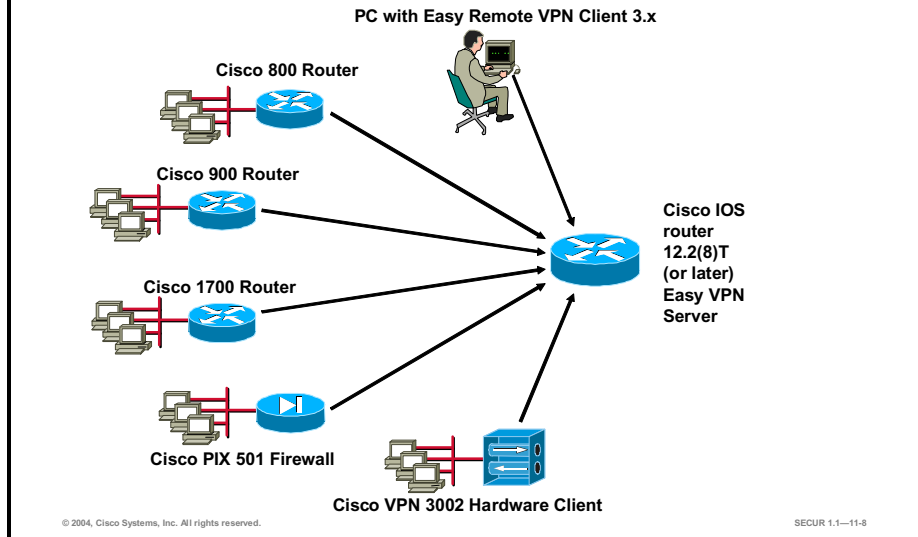
In the example in the figure, the VPN gateway is a Cisco IOS router running the Easy VPN Server feature. Remote Cisco IOS routers and VPN Software Clients connect to the Cisco IOS router Easy VPN Server for access to the corporate intranet.

See Cisco.com for a complete list of Cisco routers that support the Easy VPN.

How the Cisco Easy VPN Works

When an Easy VPN Remote client initiates a connection with an Easy VPN Server gateway, the "conversation" that occurs between the peers generally consists of the following major steps:

- Device authentication via Internet Key Exchange (IKE)

- User authentication using IKE Extended Authentication (XAUTH)

- VPN policy push (using mode configuration)

- IPSec Security Association (SA) creation

Easy VPN Remote Connection Process

Cisco.com

- **Step 1—The VPN Client initiates the IKE Phase 1 process.**
- **Step 2—The VPN Client establishes an IKE SA.**
- **Step 3—The Easy VPN Server accepts the SA proposal.**
- **Step 4—The Easy VPN Server initiates a username/ password challenge.**
- **Step 5—The mode configuration process is initiated.**
- **Step 6—The RRI process is initiated.**
- **Step 7—IKE quick mode completes the connection.**

SECUR 1.1—11-10

The following is a detailed description of the Easy VPN Remote connection process:

Step 1 The VPN Client initiates the IKE Phase 1 process.

Step 2 The VPN Client establishes an IKE SA.

Step 3 The Easy VPN Server accepts the SA proposal.

Step 4 The Easy VPN Server initiates a username/password challenge.

Step 5 The mode configuration process is initiated.

Step 6 The Reverse Route Injection (RRI) process is initiated.

Step 7 IKE quick mode completes the connection.

Step 1—The VPN Client Initiates the IKE Phase 1 Process

Cisco.com

Remote PC with Easy Remote VPN Client 3.x

Cisco IOS router 12.2(8)T Easy VPN Server
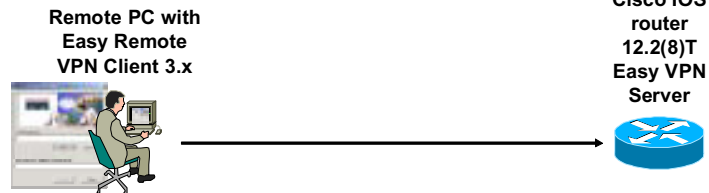
• **Using pre-shared keys? Initiate aggressive mode (AM).**
• **Using digital certificates? Initiate main mode (MM).**

SECUR 1.1—11-11

Because there are two ways to perform authentication, the VPN Client must consider the following when initiating this phase:

■ If a pre-shared key is to be used for authentication, the VPN Client initiates aggressive mode (AM). When pre-shared keys are used, the accompanying group name entered in the configuration GUI (ID_KEY_ID) is used to identify the group profile associated with this VPN Client.

■ If digital certificates are to be used for authentication, the VPN Client initiates main mode (MM). When digital certificates are used, the organizational unit (OU) field of a distinguished name (DN) is used to identify the group profile.

Because the VPN Client may be configured for pre-shared key authentication, which initiates IKE AM, it is recommended that the administrator change the identity of the Cisco IOS VPN device via the **crypto isakmp identity hostname** command. This action does not affect certificate authentication via IKE MM.

Step 2—The VPN Client Establishes an IKE SA

Remote PC with
Easy Remote
VPN Client 3.x

Cisco IOS
router
12.2(8)T
Easy VPN
Server

Proposal 1, proposal 2, proposal 3

• **The VPN Client attempts to establish an SA between peer IP addresses by sending multiple IKE proposals to the Easy VPN Server.**
• **To reduce manual configuration on the VPN Client, these IKE proposals include several combinations of the following:**
  – **Encryption and hash algorithms**
  – **Authentication methods**
  – **Diffie-Hellman group sizes**

SECUR 1.1—11-12

To reduce the amount of manual configuration on the VPN Client, every combination of encryption and hash algorithms, in addition to authentication methods and Diffie-Hellman (DH) group sizes, is proposed.

Step 3—The Easy VPN Server Accepts the SA Proposal

Remote PC with Easy Remote VPN Client 3.x

Cisco IOS router 12.2(8)T Easy VPN Server

Proposal checking finds proposal 1 match

Proposal 1

- **The Easy VPN Server searches for a match:**
  - **The first proposal to match the server's list is accepted (highest-priority match).**
  - **The most secure proposals are always listed at the top of the Easy VPN Server's proposal list (highest priority).**
- **IKE SA is successfully established.**
- **Device authentication ends and user authentication begins.**

SECUR 1.1—11-13

IKE policy is global for the Easy VPN Server and can consist of several proposals. In the case of multiple proposals, the Easy VPN Server will use the first match (so you should always have your most secure policies listed first).

Device authentication ends and user authentication begins at this point.

Step 4—The Easy VPN Server Initiates a Username/Password Challenge

Remote PC with
Easy Remote
VPN Client 3.x

Cisco IOS
router
12.2(8)T
Easy VPN
Server

Username/password challenge

Username/password

AAA
checking

- **If the Easy VPN Server is configured for XAUTH, the VPN Client waits for a username/password challenge:**
  - **The user enters a username/password combination.**
  - **The username/password information is checked against authentication entities using AAA.**
- **All Easy VPN Servers should be configured to enforce user authentication.**

SECUR 1.1—11-14

The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and Terminal Access Controller Access Control System Plus (TACACS+). Token cards may also be used via AAA proxy.

VPN devices that are configured to handle remote VPN Clients should always be configured to enforce user authentication.

Step 5—The Mode Configuration Process Is Initiated

Remote PC with
Easy Remote
VPN Client 3.x

Cisco IOS router
12.2(8)T
Easy VPN
Server

Client Requests Parameters

System Parameters via Mode Config

- **If the Easy VPN Server indicates successful authentication, the VPN Client requests the remaining configuration parameters from the Easy VPN Server:**
  - **Mode configuration starts.**
  - **The remaining system parameters (IP address, DNS, split tunneling information, and so on) are downloaded to the VPN Client.**
- **Remember that the IP address is the only required parameter in a group profile; all other parameters are optional.**

SECUR 1.1—11-15

The remaining system parameters (IP address, Domain Name System [DNS], split tunnel attributes, and so on) are pushed to the VPN Client at this time using mode configuration. The IP address is the only required parameter in a group profile; all other parameters are optional.

Step 6—The RRI Process Is Initiated

Remote PC with Easy Remote VPN Client 3.x

Cisco IOS router 12.2(8)T Easy VPN Server

RRI static route creation

VPN Tunnel

- **After the Easy VPN Server knows the VPN Client's assigned IP address, it must determine how to route packets through the appropriate VPN tunnel:**
  - **RRI creates a static route on the Easy VPN Server for each VPN Client's internal IP address.**
  - **RRI must be enabled on the crypto maps supporting VPN Clients.**
- **RRI need not be enabled on a crypto map applied to a GRE tunnel that is already being used to distribute routing information.**

SECUR 1.1—11-16

RRI ensures that a static route is created on the Easy VPN Server for each VPN Client's internal IP address.

Note	It is recommended that you enable RRI on the crypto map (static or dynamic) for the support of VPN Clients, unless the crypto map is being applied to a Generic Routing Encapsulation (GRE) tunnel that is already being used to distribute routing information.

Step 7—IKE Quick Mode Completes the Connection
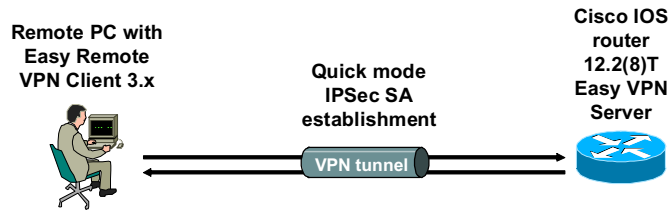
- After the configuration parameters have been successfully received by the VPN Client, IKE quick mode is initiated to negotiate IPSec SA establishment.
- After IPSec SA establishment, the VPN connection is complete.

After IPSec SAs have been created, the connection is complete.

Configuring the Easy VPN Server

This topic examines the general tasks used to configure an Easy VPN Server to support XAUTH for Easy VPN Remote VPN client access.

Easy VPN Server General Configuration Tasks

Cisco.com

The following general tasks are used to configure Easy VPN Server on a Cisco router:

- Task 1—Create IP address pool.
- Task 2—Configure group policy lookup.
- Task 3—Create ISAKMP policy for remote VPN Client access.
- Task 4—Define group policy for mode configuration push.
- Task 5—Create a transform set.
- Task 6—Create a dynamic crypto map with RRI.
- Task 7—Apply mode configuration to the dynamic crypto map.
- Task 8—Apply a dynamic crypto map to router interface.
- Task 9—Enable IKE DPD.
- Task 10—(Optional.) Configure XAUTH.
- Task 11—(Optional.) Enable XAUTH save password feature.

　　　　　　SECUR 1.1—11-19

Complete the following tasks to configure an Easy VPN Server for XAUTH with Easy VPN Remote clients:

- Task 1—Create IP address pool.

- Task 2—Configure group policy lookup.

- Task 3—Create an Internet Security Association Key Management Protocol (ISAKMP) policy for remote VPN client access.

- Task 4—Define a group policy for a mode configuration push.

- Task 5—Create a transform set.

- Task 6—Create a dynamic crypto map with RRI.

- Task 7—Apply a mode configuration to the dynamic crypto map.

- Task 8—Apply a dynamic crypto map to the router interface.

- Task 9—Enable IKE dead peer detection (DPD).

- Task 10—(Optional.) Configure XAUTH. XAUTH is not required when using Easy VPN but it is covered here as part of this example.Task 11—(Optional.) Enable XAUTH save password feature.

Task 1—Create IP Address Pool

Remote client

vpngate1

Pool
remote-pool
10.0.1.100 to
10.0.1.150
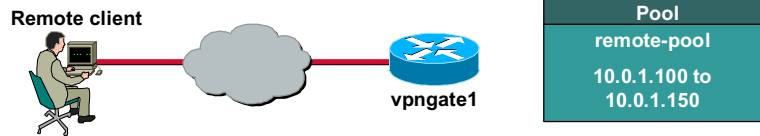
router(config)#

```
ip local pool {default | pool-name
  low-ip-address [high-ip-address]}
```

```
vpngate1(config)# ip local pool remote-pool
  10.0.1.100 10.0.1.150
```

• **Creating a local address pool is optional if you are using an external DHCP server.**

If you are using a local IP address pool, you will also need to configure that pool using the **ip local pool** command. The syntax for this command is as follows:

ip local pool {default | *pool-name low-ip-address* **[***high-ip-address***]}**

Task 2—Configure Group Policy Lookup

Configuring group policy lookup is completed in two steps, as shown in the figure:

Step 1   The first step when preparing your Easy VPN Server router for remote access is to establish an authentication, authorization, and accounting (AAA) section in the configuration file using the **aaa new-model** command in global configuration mode. The syntax for this command is as follows:

aaa new-model

Step 2   Enable group policy lookup using the **aaa authorization network** command. A local and RADIUS server may be used together and will be tried in the order listed.

The syntax for the **aaa authorization network** command is as follows:

aaa authorization network *list-name* **local group** *group-name*

list-name	Character string used to name the list of authorization methods.
method1 [*method2*]…	Specifies an authorization method or multiple authorization methods to be used for authorization.

Task 3—Create ISAKMP Policy for Remote VPN Client Access

Complete this task to configure the ISAKMP policy for all Easy VPN Remote clients attaching to this router. Use the standard ISAKMP configuration commands to accomplish this task. Here is a general example of how to configure the ISAKMP policy starting in global configuration mode:

```
vpngate1(config)# crypto isakmp enable
vpngate1(config)# crypto isakmp policy 1
vpngate1(config-isakmp)# authen pre-share
vpngate1(config-isakmp)# encryption 3des
vpngate1(config-isakmp)# group 2
vpngate1(config-isakmp)# exit
```

Task 4 contains the following steps:

- **Step 1—Add the group profile to be defined.**
- **Step 2—Configure the IKE pre-shared key.**
- **Step 3—Specify the DNS servers.**
- **Step 4—Specify the WINS servers.**
- **Step 5—Specify the DNS domain.**
- **Step 6—Specify the local IP address pool.**

SECUR 1.1—11-23

Complete this task to define a group policy to be pushed during mode configuration. Although users may belong to only one group per connection, they may belong to specific groups with different policy requirements.

Use the following steps beginning in global configuration mode to define the policy attributes that are pushed to the VPN Client via mode configuration:

Step 1   Add the group profile to be defined.

Step 2   Configure the IKE pre-shared key.

Step 3   Specify the DNS servers.

Step 4   Specify the Windows Internet Name Service (WINS) servers.

Step 5   Specify the DNS domain.

Step 6   Specify the local IP address pool.

Task 4-Step 1—Add the Group Profile to Be Defined

Remote client

vpngate1

Group: vpn-remote-access

Key: myvpnkey
DNS: DNS1 & DNS2
WINS: WINS1 & WINS2
Domain: cisco.com
Pool name: remote-pool
Pool: 10.0.1.100 to 10.0.1.150
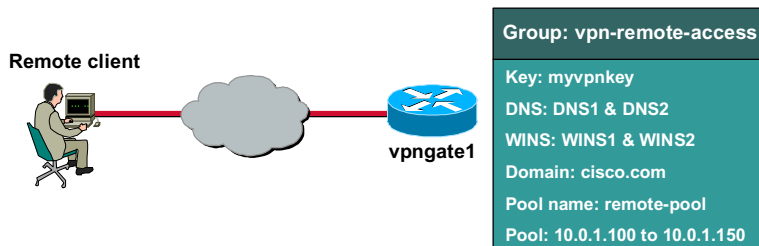
router(config)#

```
crypto isakmp client configuration group
  {group-name | default}
```

```
vpngate1(config)# crypto isakmp client
  configuration group vpn-remote-access
vpngate1(config-isakmp-group)#
```

SECUR 1.1—11-24

Step 1 Use the **crypto isakmp client configuration group** command to specify group policy information that needs to be defined or changed.

The syntax for the **crypto isakmp client configuration group** command is as follows:

crypto isakmp client configuration group {*group-name* | default}

group-name	Group definition that identifies which policy is enforced for users.
default	Policy that is enforced for all users who do not offer a group name that matches a group-name argument. The default keyword can only be configured locally.

Task 4-Step 2—Configure the IKE Pre-Shared Key

Cisco.com

Remote client

vpngate1

Group: vpn-remote-access
Key: myvpnkey
DNS: DNS1 & DNS2
WINS: WINS1 & WINS2
Domain: cisco.com
Pool name: remote-pool
Pool: 10.0.1.100 to 10.0.1.150

router(config-isakmp-group)#
```
key name
```

```
vpngate1(config-isakmp-group)# key myvpnkey
```

SECUR 1.1—11-25

Step 2   Use the **key** command to specify the IKE pre-shared key when defining group policy information for the mode configuration push. You must use this command if the VPN Client identifies itself to the router with a pre-shared key.

Use the **key** command in ISAKMP group configuration mode to specify the IKE pre-shared key for the group policy attribute definition.

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

key *name*

name	IKE pre-shared key that matches the password entered on the VPN Client. This value must match the "password" field defined in the Cisco VPN Client 3.x configuration user interface.

Task 4-Step 3—Specify the DNS Servers

Cisco.com

Remote client

Group: vpn-remote-access
Key: myvpnkey
DNS: DNS1 & DNS2
WINS: WINS1 & WINS2
Domain: cisco.com
Pool name: remote-pool
Pool: 10.0.1.100 to 10.0.1.150

vpngate1

```
router(config-isakmp-group)#
```
```
 dns primary-server secondary-server
```
```
vpngate1(config-isakmp-group)# dns DNS1 DNS2
```
```
vpngate1(config-isakmp-group)# dns
  172.26.26.120 172.26.26.130
```

SECUR 1.1—11-26

Step 3   (Optional.) Specify the primary and secondary DNS servers using the **dns** command in ISAKMP group configuration mode.

Note	You must enable the **crypto isakmp configuration group** command, which specifies group policy information that needs to be defined or changed, before using the **dns** command.

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

dns *primary-server secondary-server*

primary-server	Name or IP address of the primary DNS server.
secondary-server	Name or IP address of the secondary DNS server.

Task 4-Step 4—Specify the WINS Servers

Remote client

vpngate1

Group: vpn-remote-access
Key: myvpnkey
DNS: DNS1 & DNS2
WINS: WINS1 & WINS2
Domain: cisco.com
Pool name: remote-pool
Pool: 10.0.1.100 to 10.0.1.150

router(config-isakmp-group)#

```
wins primary-server secondary-server
```

```
vpngate1(config-isakmp-group)# wins WINS1 WINS2
```

```
vpngate1(config-isakmp-group)# wins
  172.26.26.160 172.26.26.170
```

SECUR 1.1—11-27

Step 4   (Optional.) Specify the primary and secondary WINS servers using the **wins** command in ISAKMP group configuration mode.

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

wins *primary-server secondary-server*

primary-server	Name or IP address of the primary WINS server.
secondary-server	Name or IP address of the secondary WINS server.

Task 4-Step 5—Specify the DNS Domain

Cisco.com

Group: vpn-remote-access

Key: myvpnkey

DNS: DNS1 & DNS2

WINS: WINS1 & WINS2

Domain: cisco.com

Pool name: remote-pool

Pool: 10.0.1.100 to 10.0.1.150

Remote client

vpngate1

```
router(config-isakmp-group)#
```
```
 domain name
```

```
vpngate1(config-isakmp-group)# domain cisco.com
```

SECUR 1.1—11-28

Step 5 (Optional.) Specify the DNS domain to which a group belongs by using the **domain** command in ISAKMP group configuration mode.

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

domain *name*

name	Name of the DNS domain.

Task 4-Step 6—Specify the Local IP Address Pool

Group: vpn-remote-access
Key: myvpnkey
DNS: DNS1 & DNS2
WINS: WINS1 & WINS2
Domain: cisco.com
Pool name: remote-pool
Pool: 10.0.1.100 to 10.0.1.150

Remote client

vpngate1

```
router(config-isakmp-group)#
pool name
```

```
vpngate1(config-isakmp-group)# pool remote-pool
```

SECUR 1.1—11-29

Step 6   Use the **pool** command to refer to an IP local address pool, which defines a range of addresses that will be used to allocate an internal IP address to a VPN Client.

Use the **pool** command in the ISAKMP group configuration mode to define a local pool address.

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

pool *name*

name	Name of the local pool.

Task 5—Create Transform Set
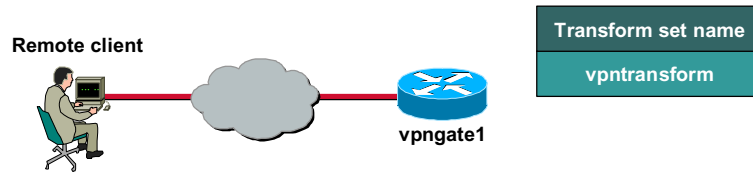
Remote client

vpngate1

Transform set name

vpntransform

router(config)#

```
crypto ipsec transform-set transform-set-name
  transform1 [transform2 [transform3]]
```

```
vpngate1(config)# crypto ipsec transform-set
  vpntransform esp-3des esp-sha-hmac
vpngate1(cfg-crypto-trans)# exit
```

SECUR 1.1—11-30

This task creates a transform set for the Easy VPN Remote clients to use when they attempt to build an IPSec tunnel to this router. Use the standard method for creating a transform set, as shown in this figure.

Here is an example of how to create a transform set for Easy VPN Remote client access.

```
vpngate1(config)# crypto ipsec transform-set vpntransform esp-3des
esp-sha-hmac
```

```
vpngate1(cfg-crypto-trans)# exit
```

Task 6 contains the following steps:
- **Step 1—Create a dynamic crypto map.**
- **Step 2—Assign a transform set.**
- **Step 3—Enable RRI.**

This task creates a dynamic crypto map to be used when building IPSec tunnels to Easy VPN Remote clients. In this example, Reverse Route Injection (RRI) is used to ensure that returning data destined for a particular IPSec tunnel can find that tunnel. RRI ensures that a static route is created on the Easy VPN Server for each client internal IP address.

Complete the following steps to create the dynamic crypto map with RRI:

Step 1   Create a dynamic crypto map.

Step 2   Assign a transform set to the crypto map.

Step 3   Enable RRI.

Task 6-Step 1—Create a Dynamic Crypto Map

Crypto map name/sequence #

dynmap 1

Remote client
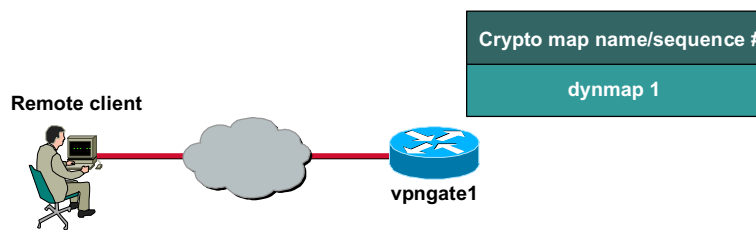
vpngate1

router(config)#

```
crypto dynamic-map dynamic-map-name
  dynamic-seq-num
```

```
vpngate1(config)# crypto dynamic-map dynmap 1

vpngate1(config-crypto-map)#
```

SECUR 1.1—11-32

Step 1 Create a dynamic crypto map entry and enter the crypto map configuration mode using the **crypto dynamic-map** command.

The syntax for the **crypto dynamic-map** command is as follows:

crypto dynamic-map *dynamic-map-name dynamic-seq-num*

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the number of the dynamic crypto map entry.

A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This practice allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all of the remote peer's requirements.

Dynamic crypto maps are not used by the router to initiate new IPSec SAs with remote peers. Dynamic crypto maps are used when a remote peer tries to initiate an IPSec SA with the router. Dynamic crypto maps are also used in evaluating traffic.

Task 6-Step 2—Assign Transform Set to Dynamic Crypto Map
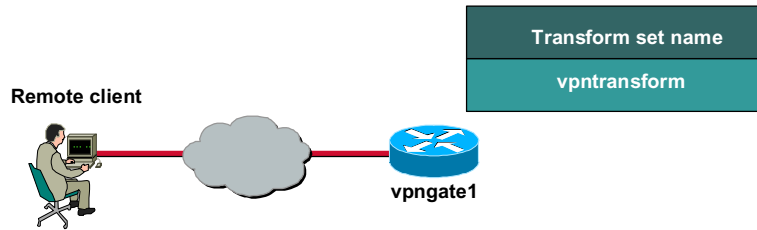
Transform set name

vpntransform

Remote client

vpngate1

router(config-crypto-map)#

```
set transform-set transform-set-name
  [transform-set-name2…transform-set-name6]
```

```
vpngate1(config-crypto-map)# set transform-set
  vpntransform
vpngate1(config-crypto-map)#
```

SECUR 1.1—11-33

Step 2   Specify which transform sets are allowed for the crypto map entry using the **set transform-set** command. When using this command, be sure to list multiple transform sets in order of priority (highest priority first). Note that this is the only configuration statement required in dynamic crypto map entries.

The syntax for the **set transform-set** command is as follows:

set transform-set *transform-set-name* [*transform-set-name2…transform-set-name6*]

transform-set-name	Name of the transform set:
	■ For an IPSec-manual crypto map entry, you can specify only one transform set.
	■ For an IPSec-ISAKMP or dynamic crypto map entry, you can specify up to six transform sets.

Task 6-Step 3—Enable RRI
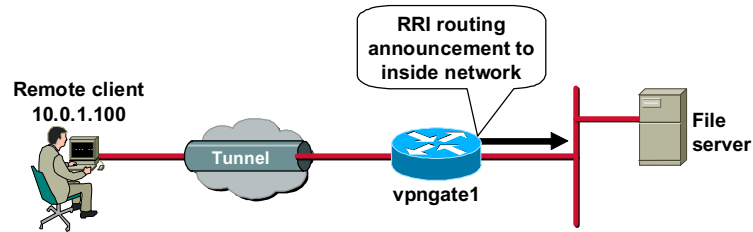
RRI routing announcement to inside network

Remote client 10.0.1.100

Tunnel

vpngate1

File server

```
router(config-crypto-map)#
  reverse route
```

```
vpngate1(config-crypto-map)# reverse route
vpngate1(config-crypto-map)# exit
```

SECUR 1.1—11-34

Step 3   Enable RRI using the **reverse-route** command.

The syntax for the reverse-route command is as follows:

reverse-route

This command has no arguments or keywords.

**Task 7—Apply Mode Configuration
to Dynamic Crypto Map**

Task 7 contains the following steps:

- **Step 1—Configure the router to respond
  to mode configuration requests.**
- **Step 2—Enable IKE querying for a group policy.**
- **Step 3—Apply changes to the dynamic crypto
  map.**

SECUR 1.1—11-35

Apply mode configuration to a dynamic crypto map using the following steps in global configuration mode:

Step 1   Configure the router to respond to mode configuration requests.

Step 2   Enable IKE queries for group policy lookup.

Step 3   Apply changes to the dynamic crypto map.

Task 7-Step 1—Configure Router to Respond to Mode Configuration Requests

Remote client

vpngate1

router(config)#

```
crypto map map-name client configuration
  address {initiate | respond}
```

```
vpngate1(config)# crypto map dynmap client
  configuration address respond
```

SECUR 1.1—11-36

Step 1   Configure the router to initiate or reply to mode configuration requests. Note that VPN Clients require the respond keyword to be used. The initiate keyword was used with older VPN Clients and is no longer used with the 3.x version Cisco VPN Clients.

The syntax for the **crypto map** *map-name* **client configuration** command is as follows:

crypto map *map-name* **client configuration address {initiate | respond}**

map-name	The name that identifies the crypto map.
initiate	A keyword that indicates the router will attempt to set IP addresses for each peer (no longer used with the Cisco VPN Client 3.x and above).
respond	A keyword that indicates the router will accept requests for IP addresses from any requesting peer.

Task 7-Step 2—Enable IKE Querying for Group Policy

Cisco.com
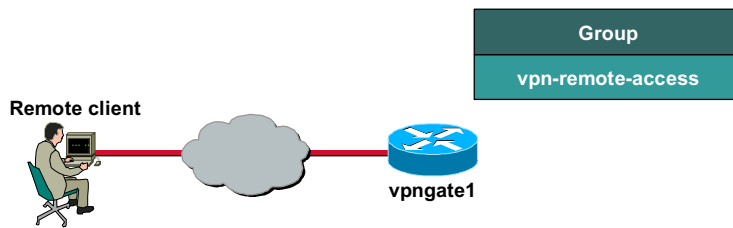
Group

vpn-remote-access

Remote client

vpngate1

router(config)#

```
crypto map map-name isakmp authorization list
   list-name
```

```
vpngate1(config)# crypto map dynmap isakmp
  authorization list vpn-remote-access
```

SECUR 1.1—11-37

Step 2 Enable IKE querying for group policy when requested by the VPN Client. AAA uses the list-name argument to determine which storage is used to find the policy (local or RADIUS) as defined in the **aaa authorization network** command.

The syntax for the **crypto map isakmp authorization list** command is as follows:

crypto map *map-name* **isakmp authorization list** *list-name*

map-name	Name you assign to the crypto map set.
list-name	Character string used to name the list of authorization methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

Task 7-Step 3—Apply Changes to Dynamic Crypto Map

Crypto map name/sequence #

dynmap 1

Remote client
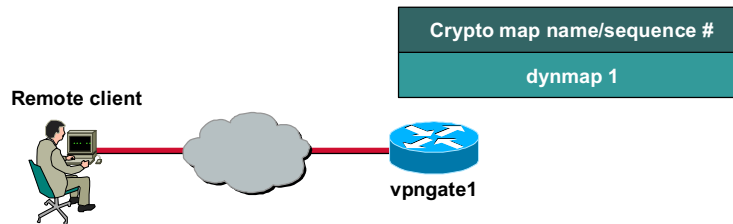
vpngate1

router(config)#

```
crypto map map-name seq-num ipsec-isakmp
  dynamic dynamic-map-name
```

```
vpngate1(config)# crypto map dynmap 1
  ipsec-isakmp dynamic dynmap
```

SECUR 1.1—11-38

Step 3 Apply changes to the dynamic crypto map using the **crypto map** command in global configuration mode.

The syntax for the **crypto map** command is as follows:

crypto map *map-name seq-number* **ipsec isakmp dynamic** *dynamic-map-name*

map-name	The name you assign to the dynamic crypto map.
dynamic-map-name	The name you assign to the dynamic crypto map.
seq-num	Specifies the number of the dynamic crypto map entry.

Task 8—Apply Dynamic Crypto Map to Router Outside Interface

This task is used to apply the new dynamic crypto map to the Easy VPN Server router's outside interface.

Here is an example of how to apply the new dynamic crypto map to the outside interface beginning in global configuration mode:
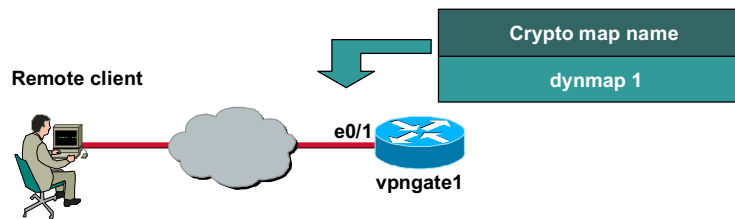
```
vpngate1(config)# interface ethernet0/1
vpngate1(config-if)# crypto map dynmap
vpngate1(config-if)# exit
```

Task 9—Enable IKE DPD

1) DPD send: Are you there?

Remote client

vpngate1

2) DPD reply: Yes, I am here.
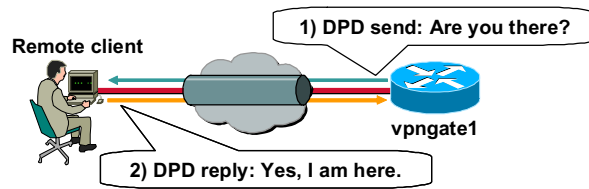
router(config)#

```
crypto isakmp keepalive secs retries
```

```
vpngate1(config)# crypto isakmp keepalive 20 10
```

SECUR 1.1—11-40

Use the **crypto isakmp keepalive** command in global configuration mode to enable a Cisco IOS VPN gateway (instead of the VPN Client) to send IKE DPD messages.

The syntax for the **crypto isakmp keepalive** command is as follows:

crypto isakmp keepalive *secs retries*

secs	Specifies the number of seconds between DPD messages. The range is between 10–3600 seconds.
retries	Specifies the number of seconds between retries if DPD messages fail. The range is between 2–60 seconds.

Task 10—Configure XAUTH

Cisco.com

Task 10 contains the following steps:

- **Step 1—Enable AAA login authentication.**
- **Step 2—Set the XAUTH timeout value.**
- **Step 3—Enable IKE XAUTH for the dynamic crypto map.**

SECUR 1.1—11-41

Complete the following steps to configure XAUTH on your Easy VPN Server router:

Step 1 Enable AAA login authentication.

Step 2 Set XAUTH timeout value.

Step 3 Enable IKE XAUTH for the dynamic crypto map.

Task 10-Step 1—Enable AAA Login Authentication

Cisco.com

Remote client

VPN user group
vpnusers
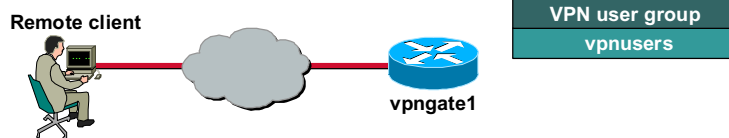
vpngate1

router(config)#

```
aaa authentication login list-name method1
  [method2...]
```

```
vpngate1(config)# aaa authentication login
  vpnusers local
```

SECUR 1.1—11-42

Step 1   Enable AAA login authentication using the **aaa authentication login** command in global configuration mode.

The syntax for the **aaa authentication login** command is as follows:

aaa authentication login *list-name method1* [*method2...*]

list-name	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name defined during AAA configuration.
method	Keyword used to describe the authentication method used.

Task 10-Step 2—Set XAUTH Timeout Value

Remote client

20 seconds

VPN user group

vpnusers
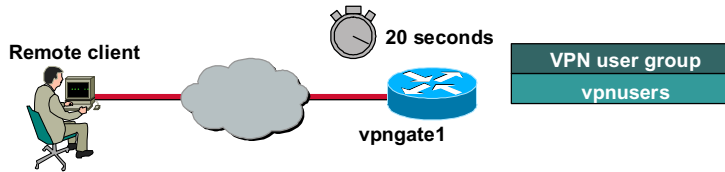
vpngate1

router(config)#

```
crypto isakmp xauth timeout seconds
```

```
vpngate1(config)# crypto isakmp xauth timeout
  20
```

SECUR 1.1—11-43

Step 2   Set the XAUTH timeout value using the **crypto isakmp xauth timeout** command.

The syntax for the **crypto isakmp xauth timeout** command is as follows:

crypto isakmp xauth timeout *seconds*

seconds	The XAUTH timeout value in seconds.

Task 10-Step 3—Enable IKE XAUTH for Dynamic Crypto Map

Crypto map name
dynmap 1
VPN user group
vpnusers

Remote client

vpngate1

router(config)#

```
crypto map map-name client authentication list
  list-name
```

```
vpngate1(config)# crypto map dynmap client
  authentication list vpnusers
```
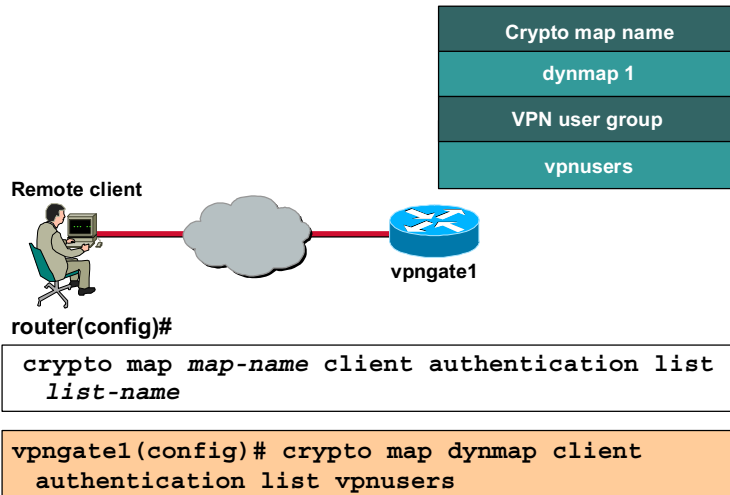
SECUR 1.1—11-44

Step 3 Enable IKE XAUTH for the dynamic crypto map using the **crypto map** command.

The syntax for the **crypto map** command is as follows:

crypto map *map-name* client authentication list *list-name*

map-name	Name you assign to the crypto map set.
list-name	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

Task 11—(Optional.) Enable XAUTH Save Password

Remote client

Group
vpn-remote-access
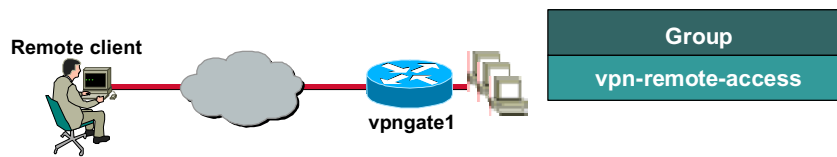
vpngate1

router(config-isakmp-group)#

```
save-password
```

```
vpngate1(config)# crypto isakmp client
 configuration group vpn-remote-access
vpngate1(config-isakmp-group)# save-password
```

• **This step could have been completed in Step 1 of Task 4 following the** crypto isakmp client configuration group **command.**

SECUR 1.1—11-45

Cisco Easy VPN Remote uses one of three available authentication methods:

■ No XAUTH—When no XAUTH is used, there is no authentication for the user when establishing the VPN tunnels. This is the least secure practice when configuring and using Cisco Easy VPN Remote.

■ XAUTH with no password save feature—This is better than no XAUTH, but it requires that users re-enter the password each time they need to establish the VPN tunnel (this may occur several times in one VPN session). Although this is the most secure form of authentication for Cisco Easy VPN Remote, it is also the most bothersome to users.

■ XAUTH with password save feature—Using the password save function, users need only enter their password once when establishing the VPN tunnel. After that, the Cisco Easy VPN Remote automatically re-enters the password when required.

Enabling the XAUTH save password feature is an optional step. When configured, it allows the Easy VPN Remote to save and reuse the last validated username and password for reauthentication. This means that a user no longer needs to re-enter the information manually. This step could have been done earlier, in Step 1 of Task 4, while performing the **crypto isakmp client configuration group** command.

Use the **save-password** command in ISAKMP group configuration mode as shown in the figure.

The syntax for the **save-password** command is as follows:

save-password

This command has no arguments or keywords.

Note   Please note that the save password feature must be configured in both the Cisco Easy VPN Server and the Cisco Easy VPN Remote.

Configuring Easy VPN Remote for the Cisco VPN Client 3.x

This topic contains information regarding the installation and configuration of the Cisco VPN Client release 3.x.

Configuring Easy VPN Remote for the Cisco VPN Client 3.x—General Tasks

Perform the following general tasks when configuring the Cisco VPN Client 3.x:

- Task 1—Install Cisco VPN Client 3.x.
- Task 2—Create a new client connection entry.
- Task 3—Modify client options.
- Task 4—Configure client general properties.
- Task 5—Configure client authentication properties.
- Task 6—Configure client connection properties.

SECUR 1.1—11-47

Complete the following general tasks to configure the Cisco VPN Client 3.x for Easy VPN Remote access:

- Task 1—Install the Cisco VPN Client 3.x on the remote user's PC.

- Task 2—Create a new client connection entry.

- Task 3—Modify the client options.

- Task 4—Configure the client general properties.

- Task 5—Configure the client authentication properties.

- Task 6—Configure the client connection properties.

Task 1—Install Cisco VPN Client 3.x
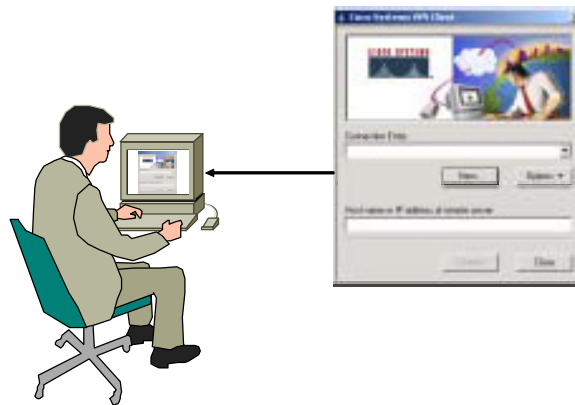
SECUR 1.1—11-48

Installation of the Cisco VPN Client varies slightly based on the type of operating system. Always review the installation instructions that come with the Cisco VPN Client before attempting any installation. Generally, installation of the Cisco VPN Client 3.x involves the following steps (this example is based on installing the Cisco VPN Client on a Windows 2000 PC):

Step 1 Obtain a copy of the Cisco VPN Client application. The application can be downloaded from the Cisco website or can be obtained from a Cisco VPN 3000 Series Concentrator CD-ROM.

Step 2 Locate and run the Cisco VPN Client **setup.exe** executable. If this is the first time the Cisco VPN Client is being installed, a window opens and displays the following message: Do you want the installer to disable the IPSec Policy Agent?

Step 3 Click **Yes** to disable the IPSec policy agent. The Welcome window opens.

Step 4 Read the Welcome window and click **Next**. The License Agreement window opens.

Step 5 Read the license agreement and click **Yes**. The Choose Destination Location window opens.

Step 6 Click **Next**. The Select Program Folder window opens.

Step 7 Accept the defaults by clicking **Next**. The Start Copying Files window opens.

Step 8 The files are copied to the hard disk drive of the PC and the InstallShield Wizard Complete window opens.

Step 9 Select **Yes, I want to restart my computer now** and click **Finish**. The PC restarts.

This completes the installation of the Cisco VPN Client.

Task 2—Create a New Client Connection Entry

The Cisco VPN Client enables users to configure multiple connection entries. Multiple connection entries enable the user to build a list of possible network connection points. For example, a corporate telecommuter may want to connect to the Sales office in Boston for sales data (the first connection entry), and then may want to connect to the Austin factory for inventory data (a second connection entry). Each connection contains a specific entry name and remote server hostname or IP address.

Generally, creating a new connection entry involves the following steps (this example is based on creating new connection entries on a Windows 2000 PC):

Step 1   Choose **Start>Programs>Cisco Systems VPN Client>VPN Dialer**. The Cisco Systems VPN Client window opens.

Step 2   Click **New**. The New Connection Entry wizard opens.

Step 3   Enter a name for the new connection entry in the Name of the New Connection Entry field (for example, Boston Sales).

Step 4   Click **Next**.

Step 5   Enter the public interface IP address or hostname of the remote Easy VPN Server in the remote server field.

Step 6   Click **Next**.

Step 7   Select **Group Access Information** and complete the following substeps. The following entries are always case sensitive:

1.   Enter a group name that matches a group on the Easy VPN Server.

2.   Enter the group password.

3.   Confirm the password.

Step 8 Click **Next**.

Step 9 Click **Finish** and leave the Cisco Systems VPN Client window open.

You have successfully configured the network parameters for the Cisco VPN Client and created a new VPN connection entry.

Task 3—Modify Client Options

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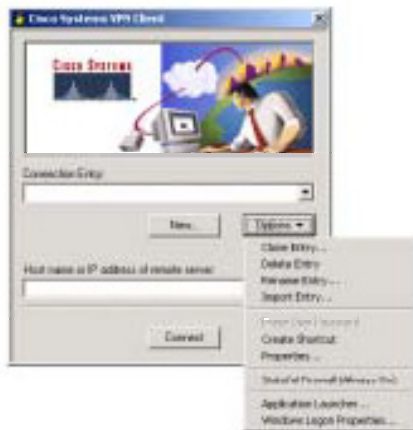
© 2004, Cisco Systems, Inc. All rights reserved.

SECUR 1.1—11-50

Several configuration options are available from the Options menu. This figure shows how to select the Options menu from the splash window.

The Options drop-down menu enables you to configure or change optional parameters. By clicking the **Options** button, the following options become available:

- Clone Entry—Enables you to copy a connection entry with all its properties.

- Delete Entry—Enables you to delete a connection entry.

- Rename Entry—Enables you to rename a connection entry (not case sensitive).

- Import Entry—Provides a preconfigured .pcf file that will load the Cisco VPN Client parameters.

- Erase User Password—Eliminates a saved password. Erase User Password is available only when you have enabled Allow Password Storage under the mode configuration parameters for this group.

- Create Shortcut—Enables you to create a shortcut for your desktop.

- Properties—Enables you to configure or change the properties of the connection.

- Stateful Firewall (Always On)—Blocks all inbound traffic to the Cisco VPN Client that is not related to an outbound session. After the remote user enables the stateful firewall, it is always on.

- Application Launcher—Enables you to launch an application before establishing a connection. This is used in conjunction with Windows Login Properties. Windows Login Properties enables the Cisco VPN Client to make the connection to the Concentrator before the user logs in.

If you want to know which version of the Cisco VPN Client you have installed on your PC, right-click the Cisco VPN Dialer icon in the system tray, to view the Cisco VPN Client version.

Task 4—Configure Client General Properties

Windows 95/98/ME | Windows NT 4/2000/XP

SECUR 1.1—11-51
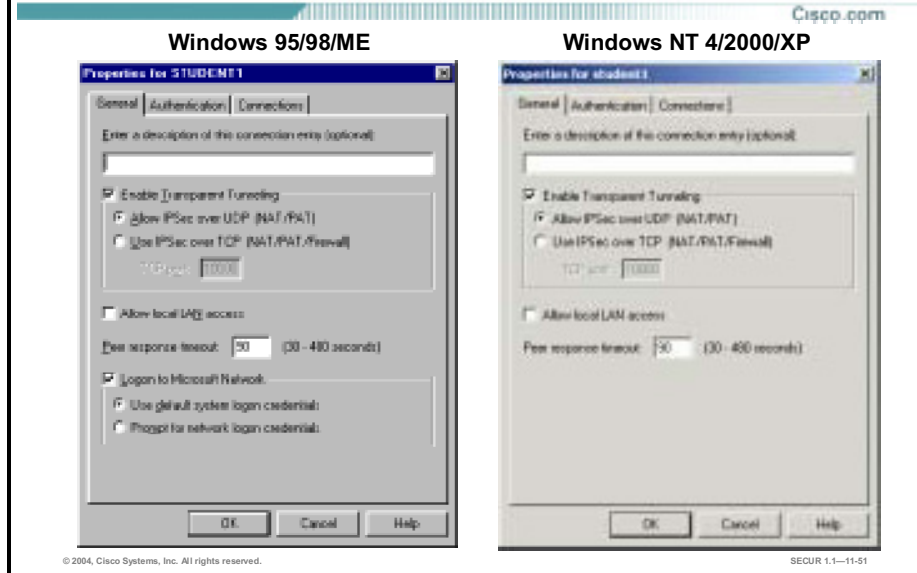
Choose **Properties** from the Options drop-down menu. The following three tabs are found under Properties:

■ General tab—Enables IPSec through Network Address Translation (NAT), displays the status of the local LAN access feature, and selects Microsoft network logon options.

■ Authentication tab—Configures the Cisco VPN Client's group or digital certificate information.

■ Connections tab—Enables backup connections, and links the VPN connection to Dialup Networking phone book entries.

The figure displays the General tab for both the Windows 95, 98, and Millennium Edition (ME) and Windows NT, 2000, and XP operating systems.

There are two versions of General tab, depending on the operating system you are using: the Windows 95, 98, and ME version and the Windows NT 4.0, 2000, and XP version. The Windows 95, 98, and ME version provides options for transparent tunneling, local LAN access, and Microsoft login options. The Windows NT 4.0, 2000, and XP version provides transparent tunneling and local LAN access only.

The functions of the General tab are as follows:

■ Enable Transparent Tunneling check box—Works with Windows 95, 98, NT 4.0, 2000, and XP.

■ Allow IPSec over UDP (NAT/PAT) radio button—Enables you to use the Cisco VPN Client to connect to the Easy VPN Server via UDP through a firewall or router that is running NAT. Both the Cisco VPN Client and Easy VPN Server must be enabled for this feature to work.

■ Use IPSec over TCP (NAT/PAT/Firewall) radio button—Enables you to use the Cisco VPN Client to connect to the Easy VPN Server via TCP through a firewall or router that is

running NAT. Both the Cisco VPN Client and the Easy VPN Server must be enabled for this feature to work.

- Allow local LAN access check box—For security purposes, the user has the ability to disable local LAN access when using an insecure local LAN (for example, in a hotel). This option is not available when using a Cisco IOS software-based Easy VPN Server or PIX Firewall as the VPN gateway.

- Peer response timeout field—The number of seconds to wait before the Cisco VPN Client decides that the peer is no longer active. The Cisco VPN Client continues to send DPD requests until it reaches the peer response timeout value.

- Logon to Microsoft Network check box—Works with Windows 95, 98, and ME only.

- Use default system logon credentials radio button—Uses the logon username and password resident on your PC to log onto the Microsoft network (for example, student4).

- Prompt for network logon credentials radio button—If your logon username and password differ from the enterprise network, the enterprise network prompts you for the username and password.

Task 5—Configure Client Authentication Properties

The Easy VPN Server and the Cisco VPN Client connection can be authenticated with either the group name and password, or digital certificates. The Authentication tab enables you to set your authentication information. You need to choose one method, group or certificates, via the radio buttons.

Within the Group Access information group box in the Authentication tab, enter the group name and password in the appropriate fields. The group name and password must match what is configured for this group within the Easy VPN Server. Entries are case sensitive.

For certificates to be exchanged, the Certificate radio button must be selected. In the Name drop-down menu, any personal certificates loaded on your PC are listed. Choose the certificate to be exchanged with the Easy VPN Server during connection establishment. If no personal certificates are loaded in your PC, the drop-down menu is blank. Use the Validate Certificate button to check the validity of the Cisco VPN Clients' certificate.

Task 6—Configure Client Connection Properties

The Connections tab defines backup networks and connection to the Internet via dialup networking.

An enterprise network may include one or more backup Easy VPN Servers to use if the primary Easy VPN Server gateway is not available. Select the **Enable backup server(s)** check box to enable this feature. Once selected, click **Add** to enter the IP address of the backup Easy VPN Server.

The Cisco VPN Client attempts to connect to the primary Easy VPN Server first. If that Easy VPN Server cannot be reached, the Cisco VPN Client accesses the backup list for the addresses of available backup Easy VPN Server.

Connecting to an enterprise network using a dialup connection is typically a two-step process:

Step 1   Use a dialup connection to your Internet service provider (ISP).

Step 2   Use the Cisco VPN Client to connect to the enterprise network.

Connecting to the Internet via dialup automatically launches the connection before making the VPN connection. It makes connecting to the ISP and Easy VPN Server an easy, one-step process. Select **Connect to the Internet via Dial-Up Networking** to enable the option.

Using the Cisco VPN Client 3.x

This topic contains information regarding the Cisco VPN Client program menus, log viewer, and status displays.
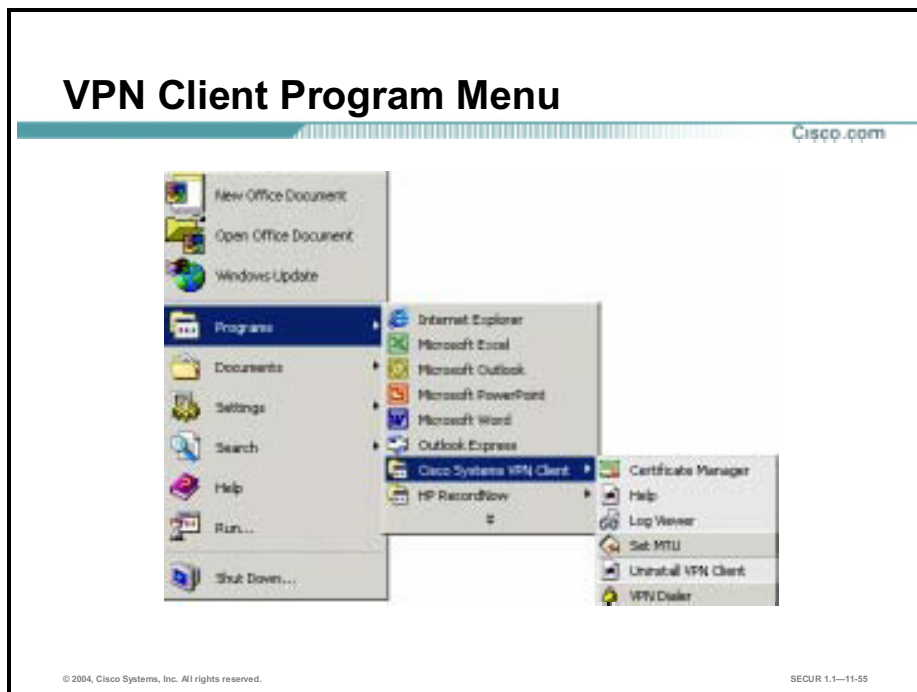
This figure displays the Cisco VPN Client program menu as viewed on a Windows 2000 PC.

After the Cisco VPN Client is installed, access the Cisco VPN Client program menu by choosing **Start>Programs>Cisco Systems VPN Client**. Under the Cisco VPN Client menu, a number of options are available:

- Certificate Manager—Enables you to enroll, import, export, verify, and view certificates.

- Help—Accesses the Cisco VPN Client help text. Help is also available by doing the following:

    — Press **F1** at any window while using the Cisco VPN Client.

    — Click the **Help** button.

    — Click the logo in the title bar.

- Log Viewer—Displays the Cisco VPN Client event log.

- Set MTU—The Cisco VPN Client automatically sets the maximum transmission unit (MTU) size to approximately 1420 bytes. For unique applications, Set MTU can change the MTU size to fit a specific scenario.

- Uninstall VPN Client—Only one Cisco VPN Client can be loaded at a time. When upgrading, the old Cisco VPN Client must be uninstalled before the new Cisco VPN Client is installed. Choose Uninstall VPN Client to remove the old Cisco VPN Client.

- Cisco VPN Dialer—Initiates the Cisco VPN Client connection process by displaying the Cisco VPN Client splash window.

VPN Client Log Viewer

Toolbar

Log display

SECUR 1.1—11-56
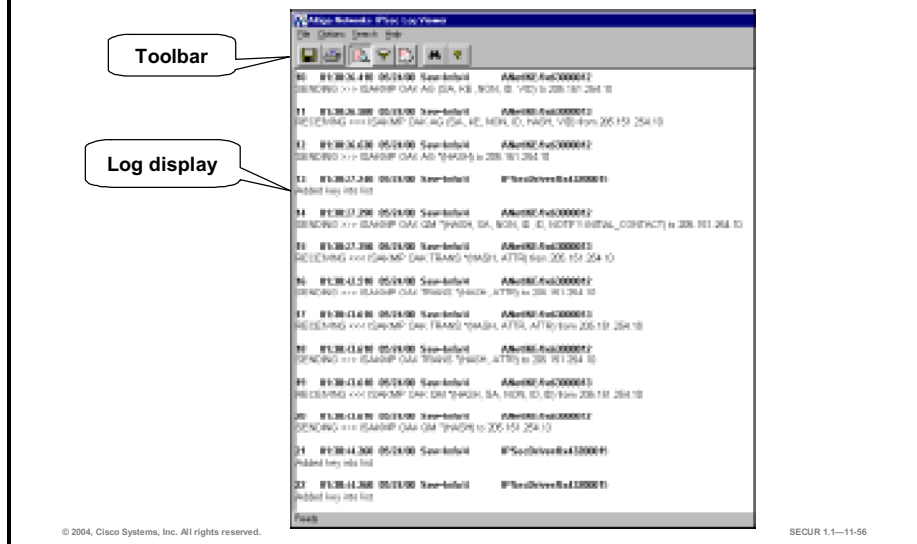
Examining the event log can help a network administrator diagnose problems with an IPSec connection between a Cisco VPN Client and an Easy VPN Server. The Log Viewer application collects event messages from all processes that contribute to the Cisco VPN Client-Easy VPN Server connection.

This figure displays the Log Viewer window with a sample Cisco VPN Client log file. From the toolbar, you can perform the following:

- Save the log file.
- Print the log file.
- Capture event messages to the log.
- Filter the events.
- Clear the event log.
- Search the event log.

Setting MTU Size
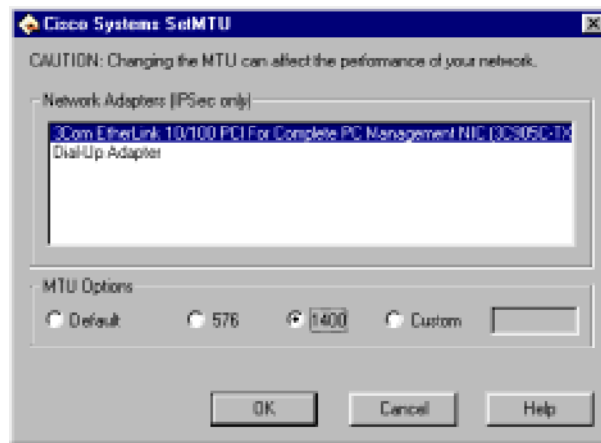
This figure displays the SetMTU window, which is where you set the maximum transmission unit (MTU) size.

The Cisco VPN Client automatically sets the MTU size to approximately 1420 bytes. For unique applications where fragmentation is still an issue, SetMTU can change the MTU size to fit the specific scenario. In the Network Adapters (IPSec only) field, select the network adapter. In the example in the figure, 3Com EtherLink is selected. In the MTU Options group box, set the MTU size by selecting the appropriate radio button. You must reboot for MTU changes to take effect.

VPN Client Connection Status— General Tab
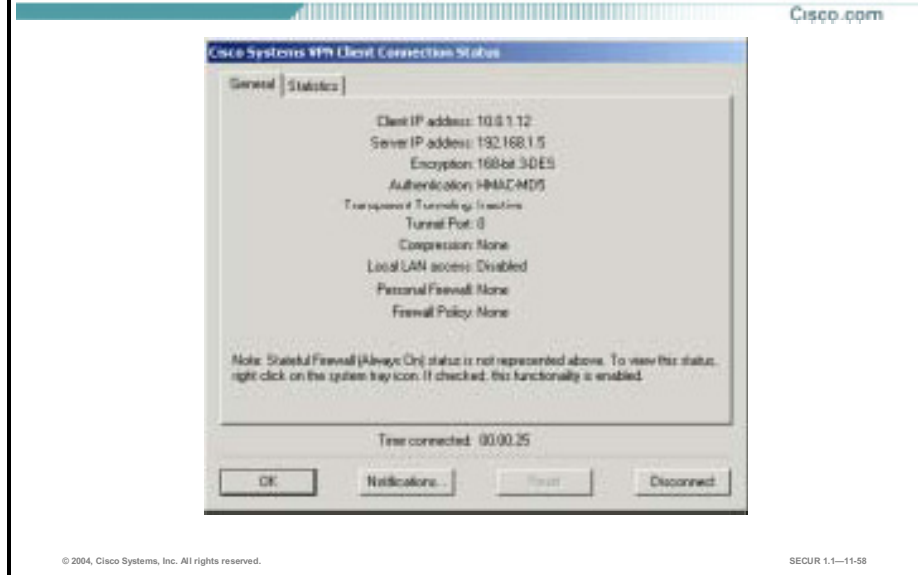
The Cisco Systems VPN Client Connection Status window contains up to three tabs: General, Statistics, and Firewall (Firewall is not shown in the figure as it is not currently supported by IOS 12.2(8)T Cisco Easy VPN). The figure displays the General tab.

The General tab provides IP security information, listing the IPSec parameters that govern this IPSec tunnel. The following information is available within the General tab:

■ Client IP address—The IP address assigned to the Cisco VPN Client for the current session.

■ Server IP address—The IP address of the Easy VPN Server device to which the Cisco VPN Client is connected.

■ Encryption—The data encryption method for traffic through this tunnel.

■ Authentication—The data or packet authentication method used for traffic through this tunnel.

■ Transparent Tunneling—The status of transparent tunnel mode in the Cisco VPN Client (either active or inactive).

■ Tunnel Port—If transparent mode is active; the tunnel port through which packets are passing is displayed. This field also identifies whether the Cisco VPN Client is sending packets through UDP or TCP. If transparent tunneling is inactive, then the value of Tunnel Port is zero.

■ Compression—Displays whether data compression is in effect as well as the type of compression in use. Currently, the type of compression is Lempel-Ziv-Stac (LZS).

■ Local LAN Access—Displays whether this parameter is enabled or disabled.

■ Personal Firewall—Displays the name of the firewall in use on the Cisco VPN Client PC, such as the Cisco Integrated Client, Zone Labs ZoneAlarm, ZoneAlarm Pro, BlackICE Defender, and so on. This feature is not currently supported in IOS 12.2(8)T Cisco Easy VPN.

■ Firewall Policy—Displays the firewall policy in use:

— AYT (Are You There)—Not currently supported in IOS 12.2(8)T Cisco Easy VPN.

— Centralized Protection Policy (CPP) or "policy pushed" as defined on the VPN gateway. Not currently supported in IOS 12.2(8)T Cisco Easy VPN.

Client Connection Status—Statistics Tab

This figure displays the Statistics tab. The Statistics tab in the Connection Status window shows statistics for data packets that the Cisco VPN Client has processed during the current session, or since the statistics were reset. The following information is available in this window:

- Bytes in—The total amount of data received after a secure packet has been successfully decrypted.

- Bytes out—The total amount of encrypted data transmitted through the tunnel.

- Packets decrypted—The total number of data packets received on the port.

- Packets encrypted—The total number of secured data packets transmitted out of the port.

- Packets bypassed—The total number of data packets that the Cisco VPN Client did not process because they did not need to be encrypted. Local Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) packets fall into this category.

- Packets discarded—The total number of data packets that the Cisco VPN Client rejected because they did not come from the secure Easy VPN Server gateway.

- Secured routes—The IP address of the private network with which this Cisco VPN Client has a secure connection.

- Local LAN routes—If present, the Local LAN routes box shows the network addresses of the networks you can access on your local LAN while you are connected to your organization's private network.

Configuring Easy VPN Remote for Access Routers

This topic explains how to configure Cisco access routers for Easy VPN Remote.

Configuration Methods for Easy VPN Remote Access Routers

There are three ways to configure your remote Cisco routers for Cisco Easy VPN Remote:

- Cisco IOS CLI
- Security Device Manager (SDM) with Cisco Access Routers
- Cisco Router Web Setup Tool (CRWS) with Cisco 800 Series Router

SECUR 1.1—11-61

There are three ways to configure your Cisco access routers for Cisco Easy VPN Remote as shown in the figure:

- Cisco IOS command line interface (CLI)

- Security Device Manager (SDM) with Cisco Access Routers beginning with 12.2(13)ZH on many router platforms.

- Cisco Router Web Setup Tool (CRWS) with Cisco 800 Series Routers.

This section describes how to configure Easy VPN Remote using the Cisco IOS CLI method only.

Easy VPN Remote Modes of Operation

Easy VPN Remote contains two modes of operation. You must choose one of these two methods for your remote routers (both modes support split tunneling):

- **Client mode**
  - **Specifies that NAT/PAT be used.**
  - **Client automatically configures the NAT/PAT translation and the ACLs needed to implement the VPN tunnel.**
    - ip nat inside **command applied to all inside interfaces.**
    - ip nat outside **command applied to interface configured for Easy VPN remote.**
- **Network extension mode**
  - **Specifies that the hosts at the client end of the VPN connection use fully routable IP addresses.**
  - **PAT is not used.**

SECUR 1.1—11-62

Beginning with Easy VPN Remote phase II, two modes of Easy VPN Remote access are supported for your Cisco access routers:

- Client mode—This mode specifies that NAT/Port Address Translation (PAT) be configured to allow PCs and hosts on the client side of the VPN connection to form a private network. Their IP addresses must not use any of the destination server's IP addresses. Client mode automatically configures the NAT/PAT translation and access control lists (ACLs) that are needed to implement the VPN connection. These configurations are automatically (but temporarily) created when the VPN connection is initiated. When the tunnel is torn down, the NAT/PAT and ACL configurations are automatically deleted. The NAT/PAT configuration is created with the following assumptions.

  — The **ip nat inside** command is applied to all inside interfaces, including default inside interfaces. The default inside interface is Ethernet0 for the Cisco 800 and uBR900 Series routers. The default inside interface is FastEthernet0 for Cisco 1700 Series routers.

  — The **ip nat outside** command is applied to the interface that is configured for Easy VPN Remote. On the Cisco uBR905 and Cisco uBR925 routers, this is always the cable-modem0 interface. On the Cisco 800 and 1700 Series routers, this is the outside interface configured for Easy VPN Remote. The Cisco 1700 Series routers can have multiple outside interfaces configured.

- Network extension mode—This mode specifies that the hosts at the client end of the VPN connection use fully routable IP addresses that are reachable by the destination network over the tunneled network. Together they form one logical network. Because PAT is not used, the client PCs and hosts have direct access to the PCs and hosts on the destination network.

Both modes of operation optionally support split tunneling.

Easy VPN Remote Client Mode

Cisco.com

10.0.0.3

10.0.0.4

10.0.0.2

Cisco uBR905
router
(Easy VPN
Remote)
12.2(8)YJ

VPN tunnel

192.168.100.X
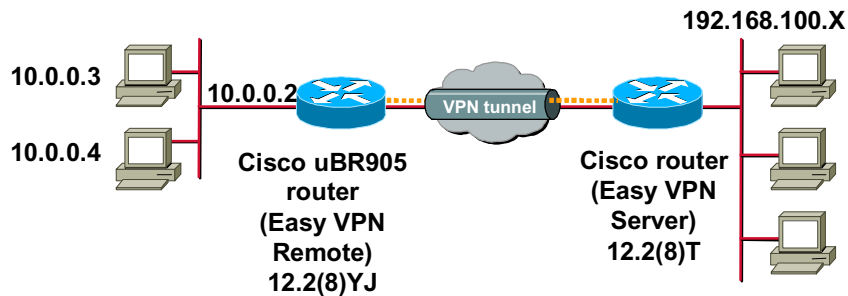
Cisco router
(Easy VPN
Server)
12.2(8)T

SECUR 1.1—11-63

In this figure, the Cisco uBR905 cable access router provides access to two PCs, which have IP addresses in the 10.0.0.0 private network space. These PCs connect to the Ethernet interface on the Cisco uBR905 router, which also has an IP address in that private network space.

The Cisco uBR905 router performs NAT/PAT translation over the IPSec tunnel so that the PCs can access the destination network.

This example could also represent a split tunneling connection, in which the client PCs could access public resources in the global Internet without including the corporate network in the path for the public resources.

Easy VPN Remote Network Extension Mode
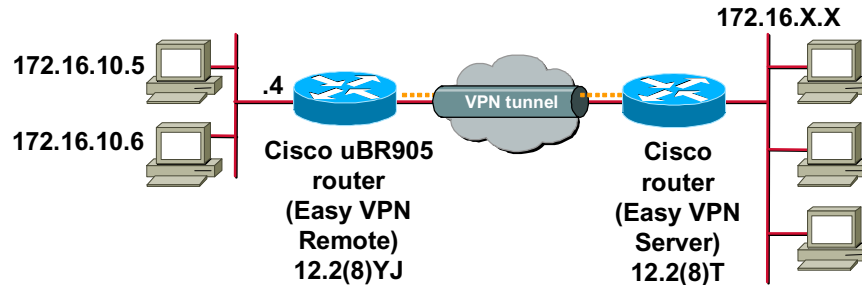
SECUR 1.1—11-64

In this example, the Cisco uBR905 cable access router acts as Cisco Easy VPN Remote client, connecting to an Easy VPN Server router.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network or in separate subnets, as long as the destination routers are configured to properly route those IP addresses over the tunnel. This provides a seamless extension of the remote network.

Easy VPN Remote Phase II Restrictions

- **Subinterfaces are not supported.**
- **Only one destination peer is supported.**
- **Digital certificates are not supported.**
- **Only ISAKMP policy Group 2 is supported when connecting to Easy VPN Servers.**
- **Perfect Forward Secrecy is not supported.**
- **Only certain transform sets are supported.**
- **You must use the correct method to change the IP address on the LAN interface of Cisco 800 Series routers.**

The following list details and restrictions inherent to Easy VPN Remote phase II:

- Establishing Easy VPN Remote phase II tunnels over subinterfaces is not supported.

- The Phase II feature supports the configuration of only one destination peer and tunnel connection. If your application requires multiple IPSec tunnels, you must manually configure the IPSec tunnel and NAT/PAT parameters on both the client and the server.

- Digital certificates are not supported—Authentication is supported using pre-shared keys and XAUTH only.

- Only ISAKMP policy Group 2 is supported on Cisco Easy VPN Remote clients.

- Perfect Forward Secrecy (PFS) is not yet supported by the Easy VPN Remote phase II feature. It is available on the Concentrator.

- Only certain transform sets are supported. To ensure a secure tunnel connection, the Easy VPN Remote phase II feature does not support transform sets that provide encryption without authentication or transform sets that provide authentication without encryption.

- The Ethernet 0 LAN interface on the Cisco 800 Series routers defaults to a primary IP address of 10.10.10.0. You can change this IP address to match the local network's configuration. When the CRWS is used, the new IP address is assigned as the secondary address and the existing IP address is preserved as the primary address for the interface. This allows CRWS to maintain the existing connection between the PC web browser and the 800 Series router. Because of this behavior, the Easy VPN Remote phase II feature assumes that if a secondary IP address exists on the Ethernet 0 interface, the secondary address should be used as the IP address of the inside interface for the NAT/PAT configuration. If no secondary address exists, the primary IP address is used for the inside interface address, as is normally done on other platforms. If this behavior is not desired, use the **ip address** command to change the interface's address, instead of using CRWS.

**Easy VPN Remote Configuration
General Tasks for Access Routers**

Cisco.com

**Complete the following general tasks when
configuring the Cisco Easy VPN client feature on a
Cisco router:**

• **Task 1—Configure the DHCP server pool (required for
client mode).**
• **Task 2—Configure and assign the Cisco Easy VPN client
profile.**
• **Task 3—(Optional.) Configure XAUTH password save.**
• **Task 4—Initiate the VPN tunnel.**
• **Task 5—Verify the Cisco Easy VPN configuration.**

SECUR 1.1—11-66

Configuring Cisco access routers to act as Easy VPN Remote clients consists of the following tasks:

■ Task 1—Configure the DHCP server pool (required for client mode).

■ Task 2—Configure and assign the Cisco Easy VPN client profile.

■ Task 3—(Optional.) Configure XAUTH password save.

■ Task 4—Initiate the VPN tunnel.

■ Task 5—Verify the Cisco Easy VPN configuration.

Task 1—Configure the DHCP Server Pool

router(config)#
```
ip dhcp pool pool-name
```

router(dhcp-config)#
```
network ip-address [ mask | / prefix-length]
```
```
default-router address [ address2 ... address8]
```
```
import all
```
```
lease { days [ hours][ minutes] | infinite}
```
```
exit
```

router(config)#
```
ip dhcp excluded-address lan-ip-address
```

SECUR 1.1—11-67

If you want to use the local router's DHCP server to assign IP addresses to the hosts that are connected to the router's LAN interface, you must create a pool of IP addresses for the router's onboard DHCP server. The DHCP server then assigns an IP address from this pool to each host when it connects to the router.

In a typical VPN connection, the hosts connected to the router's LAN interface are assigned an IP address in a private address space. The router then uses Network Address Translation/Port Address Translation (NAT/PAT) to translate those IP addresses into a single IP address that is transmitted across the VPN tunnel connection.

The steps in task 1 create the DHCP server pool:

Step 1 Create a DHCP server address pool using the **ip dhcp pool** *pool-name* command. This places you in DHCP pool configuration mode.

Step 2 Use the **network** command to specify the IP network and subnet mask of the address pool that will be used by the hosts connected to the router's local Ethernet interface.

Step 3 Use the **default-router** command to specify the IP address of the default router for a DHCP client. You must specify at least one address. You can optionally specify up to eight addresses per command.

Step 4 Use the **import all** command to ensure the router is configured with the proper DHCP parameters from the central DHCP server. This option requires a central DHCP server be configured to provide the DHCP options. This server can be on a different subnet or network.

Step 5 The **lease** command is optional. Use this command if your want to specify the duration of the DHCP lease. Use the **exit** command to leave the DHCP pool configuration mode.

Step 6 Last, use the **ip dhcp excluded-address** command to exclude the specified address from the DHCP server pool. The *lan-ip-address* should be the IP address assigned to the router's LAN interface.

Task 1 Example—DHCP Server Pool
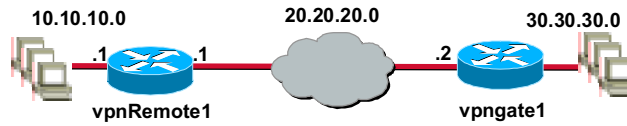
SECUR 1.1—11-68

One example of how to configure a DHCP server pool is shown in the figure.

Task 2—Configure the Cisco Easy VPN Client Profile

router(config)#

```
crypto ipsec client ezvpn name
```

router(config-crypto-ezvpn)#

```
group group-name key group-key
```

```
peer [ ip-address | hostname]
```

```
mode {client | network-extension}
```

```
exit
```

The steps in Task 2 configure the Cisco Easy VPN client profile and to assign the profile to a router interface.

Step 1   Use the **crypto ipsec client ezvpn** *name* command to create a profile. This places you in Cisco Easy VPN Remote configuration mode.

Step 2   Use the **group** *group-name* **key** *group-key* command to specify the IPSec group and IPSec key values to be associated with this profile. The values of *group-name* and *group-key* must match the values assigned in the Easy VPN Server.

Step 3   Use the **peer** command to specify the IP address or hostname for the destination peer. This is typically the IP address of the Easy VPN Server router's outside interface. If you prefer to specify a hostname, you must have a DNS server configured and available in order for this to work.

Step 4   Use the **mode** command to specify the type of VPN connection that should be made (client or network extension.)

Step 5   Enter the **exit** command to leave Easy VPN Remote configuration mode.

Task 2 Example—Configure the Cisco Easy VPN Client Profile

HQ_VPN_Gate1
Group: vpn-remote-access
Peer: 20.20.20.2
Key: myvpnkey
Mode: Client
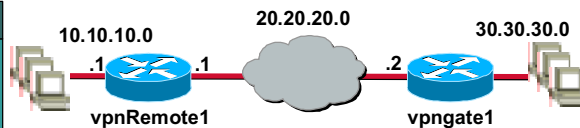
10.10.10.0   20.20.20.0   30.30.30.0

.1   .1   .2

vpnRemote1   vpngate1

```
vpnRemote1(config)# crypto ipsec client ezvpn
  HQ_VPN_Gate1
vpnRemote1(config-crypto-ezvpn)# group vpn-remote-
  access key myvpnkey
vpnRemote1(config-crypto-ezvpn)# peer 20.20.20.2
vpnRemote1(config-crypto-ezvpn)# mode client
vpnRemote1(config-crypto-ezvpn)# exit
vpnRemote1(config)#
```

One example of how to configure an Easy VPN Client profile is shown in the figure.

Task 2 Example—Assign Easy VPN Remote to the Interface

Cisco.com

HQ_VPN_Gate1

10.10.10.0   20.20.20.0   30.30.30.0

.1   .1   .2

vpnRemote1   vpngate1
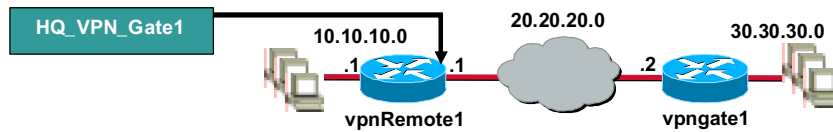
router(config-if)#

```
crypto ipsec client ezvpn name [outside]
```

```
vpnRemote1(config)# interface ethernet1
vpnRemote1(config-if)# crypto ipsec client
  ezvpn HQ_VPN_Gate1
vpnRemote1(config-if)# exit
```

SECUR 1.1—11-71

Use the **crypto ipsec client ezvpn** *name* command to assign the Easy VPN client profile to a router interface.

One example of how to assign the Easy VPN Client profile to a router interface is shown in the figure.

Task 3—(Optional.) Configure XAUTH Save Password Feature

- If the Save Password feature is enabled in Easy VPN Server, you must enable it in the client. Both ends must match, otherwise the tunnel will not come up.
- This task could be done as part of Task 2, when configuring the Cisco Easy VPN client profile.

router(config)#

```
crypto ipsec client ezvpn name
```

router(config-crypto-ezvpn)#

```
username aaa-username password aaa-password
```

```
vpnRemote1(config)# crypto ipsec client ezvpn
  HQ_VPN_Gate1

vpnRemote1(config-crypto-ezvpn)# username vpnusers
  password vpnusers

vpnRemote1(config-crypto-ezvpn)# exit
```

SECUR 1.1—11-72

Task 3 is an optional task. If you are not using XAUTH, then skip this task.

If you have the save password feature enabled in the Cisco Easy VPN Server, you must enable it on the client as well. If both ends of the tunnel do not match, the VPN tunnel will not be established.

This task could be done as part of Task 2, "Configure the Cisco Easy VPN Client Profile," to speed up the entry process.

Enter the **username** command in ezvpn crypto configuration mode for the specific client profile as shown in the figure. This is the AAA username and password used to automatically reauthenticate the user with the XAUTH password save feature enabled in the Cisco Easy VPN Server.

Task 4—(Optional.) Initiate the VPN Tunnel (XAUTH)

```
01:34:42: EZVPN: Pending XAuth Request, Please enter
the following command:

01:34:42: EZVPN: crypto ipsec client ezvpn xauth
```

- **Cisco IOS message: Waiting for valid XAUTH username and password.**

router#

```
crypto ipsec client ezvpn xauth
```

```
vpnRemote1# crypto ipsec client ezvpn xauth
Enter Username and Password: vpnusers
Password: ********
```

- **With XAUTH—When SA expires, username and password must be manually entered.**
- **With XAUTH Password Save enabled—When SA expires, the last valid username and password will be reused automatically.**

Task 4 is also optional. If you are not using XAUTH, then skip this task.

With XAUTH configured, you must initiate the VPN tunnel manually (for at least the first time). The Cisco IOS software message shown on the slide is displayed because the software is waiting for a valid XAUTH username and password. You will see this message whenever you log in to the remote router console port.

Step 1   Enter the **crypto ipsec client ezvpn xauth** command.

Step 2   Enter the username and password as prompted.

Which of two options happens next is determined by the XAUTH configuration:

- With just the XAUTH feature enabled, when the SA expires, you must manually re-enter the username and password. This process is ongoing. You will see the same Cisco IOS message and will have to repeat this manual process to reauthenticate each time.

- With the XAUTH password save enabled, when the SA expires, the last valid username and password will be reused automatically. This option is the more popular of the two.

Task 5—Verify the Cisco Easy VPN Configuration

```
vpnRemote1# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 2

Tunnel name : HQ_VPN_Gate1
Inside interface list: Ethernet0,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 30.30.30.24
Mask: 255.255.255.255
DNS Primary: 30.30.30.10
DNS Secondary: 30.30.30.11
NBMS/WINS Primary: 30.30.30.12
NBMS/WINS Secondary: 30.30.30.13
Default Domain: cisco.com
```

SECUR 1.1—11-74

Task 5 consists of reviewing the Easy VPN configuration using the **show crypto ipsec client ezvpn** command.

Easy VPN Remote Configuration Example

```
version 12.2
hostname vpnRemote1
!
username admin privilege 15 password 7 070E25414707485744
ip subnet-zero
ip domain-name cisco.com
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool client
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
   lease 3
!
crypto ipsec client ezvpn HQ_VPN_Gate1
 connect auto
 group vpn-remote-access key 0 myvpnkey
 mode client
 peer 20.20.20.2
 username vpnusers password 0 vpnusers
```

SECUR 1.1—11-75

This figure and the next detail an example of Easy VPN Remote access router configuration.

Easy VPN Remote Configuration Example (Cont.)

```
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 crypto ipsec client ezvpn HQ_VPN_Gate1 inside
!
interface Ethernet1
 ip address 20.20.20.1 255.255.255.0
 crypto ipsec client ezvpn HQ_VPN_Gate1
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1
ip route 30.30.30.0 255.255.255.0 Ethernet1
ip http server
no ip http secure-server
!
line con 0
 no modem enable
 stopbits 1
line aux 0
line vty 0 4
!
end
```

This figure contains the second half of the example shown in the previous slide of Easy VPN Remote access router configuration.

Summary

This topic summarizes what you have learned in this lesson.

Summary

- **Cisco Easy VPN features greatly enhance deployment of remote access solutions for Cisco IOS software customers.**
- **The Easy VPN Server adds several new commands to Cisco IOS software in release 12.2(8)T.**

SECUR 1.1—11-78

Lab Exercise—Configure Remote Access Using Cisco Easy VPN

Complete the following optional lab exercise to practice what you learned in this lesson.

Objectives

In this lab exercise, you will configure a Cisco Easy VPN Server using a Cisco 2600 Series router. You will also configure the Cisco VPN Client 3.x using a student laptop running Windows 2000 Server. Upon completion of these configuration tasks, you will test connectivity between the Cisco VPN Client and the Easy VPN Server. Work with your lab exercise partner to complete the following tasks:

- Complete the lab exercise setup.

- Prepare a perimeter router for the Easy VPN Server.

- Enable policy lookup via AAA.

- Create an ISAKMP policy for remote client access.

- Define group policy information for a mode configuration push.

- Create a transform set.

- Create a dynamic crypto map.

- Apply mode configuration to the dynamic crypto map.

- Apply a dynamic crypto map to the router interface.

- Enable perimeter router dead peer detection.

- Verify the Easy VPN Server configuration.

- Install the Cisco VPN Client 3.x.

- Create a new connection entry.

- Launch the Cisco VPN Client.

- Test the remote access connection.

- Configure extended authentication.

- Test extended authentication.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.
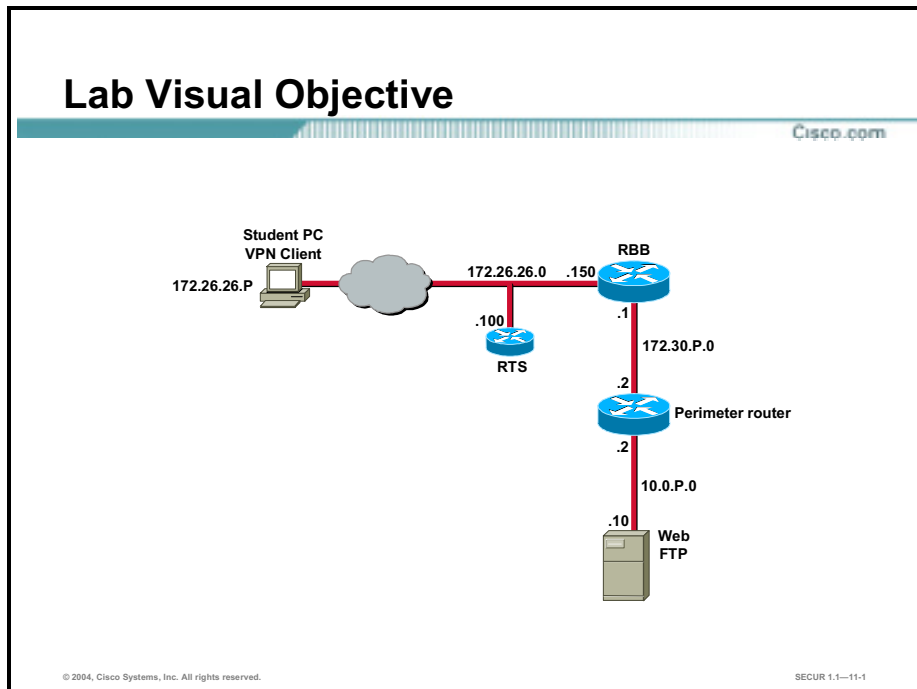
Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1   Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log in to the student PC.

Step 2   Before beginning this lab exercise, it is imperative that you change the static IP address of your student laptop. Configure a student PC IP address of **172.26.26.P** with a default gateway of **172.26.26.150** (where P = pod number).

Step 3   If this lab exercise is being performed on local equipment, directly cabled to the student PC, you must ensure that the student PC NIC cable is attached to SW1 port **1P** (where P = pod number).

Step 4   Restore the original course router configuration. Your instructor will explain how to do this.

Step 5   Ensure that you can ping the other routers and network hosts before beginning.

Task 2—Prepare a Perimeter Router for the Easy VPN Server

Complete the following steps to prepare your perimeter router for use as an Easy VPN Server, beginning in global configuration mode.

Note: This lab exercise assumes that your perimeter router has been returned to the default **rP.confg** (where P = pod number) configuration. Check with your instructor to determine if this needs to be completed before continuing with this lab exercise.

Step 1   Create a local IP address pool named remote-pool with an IP address range of 10.0.P.32 to 10.0.P.64:

```
RP(config)# ip local pool remote-pool 10.0.P.32 10.0.P.64
```

(where P = pod number)

Step 2   Configure a local username of **cisco**, and a password of **cisco** for an account accessing the perimeter router:

```
RP(config)# username cisco password 0 cisco
```

Note: The **aaa new-model** command (performed in Task 3) causes the local username/password on the router to be used in the absence of other AAA statements. It is important to create a known local username/password combination to prevent you from being locked-out of the router.

Task 3—Enable Policy Lookup via AAA

Complete the following commands for your perimeter router beginning in global configuration mode to enable policy lookup via AAA:

Step 1   Enable AAA using the **aaa new-model** command:

Note: Ensure that you have completed Task 2 before entering this command.

```
RP(config)# aaa new-model
```

Step 2   Create a group called vpn-remote-access to be used for local AAA authorization and policy lookup for remote clients:

```
RP(config)# aaa authorization network vpn-remote-access local
```

Task 4—Create an ISAKMP Policy for Remote Client Access

Complete the following commands for your perimeter router beginning in global configuration mode to create a new ISAKMP policy for remote client access:

Step 1   Enable ISAKMP:

```
RP(config)# crypto isakmp enable
```

Step 2   Create ISAKMP policy 1:

```
RP(config)# crypto isakmp policy 1
```

Step 3   Configure ISAKMP policy 1 to use pre-shared keys for authentication:

```
RP(config-isakmp)# authentication pre-share
```

Step 4   Configure ISAKMP policy 1 to use 3-DES encryption:

```
RP(config-isakmp)# encryption 3des
```

Step 5   Configure ISAKMP policy 1 to use Diffie-Hellman group 2:

```
RP(config-isakmp)# group 2
```

Step 6   Return to global configuration mode:

```
RP(config-isakmp)# exit
```

Task 5—Define Group Policy Information for a Mode Configuration Push

Use the following commands, beginning in global configuration mode, to define the policy attributes that are pushed to the VPN Client via mode configuration:

Step 1   Specify which group's policy profile will be defined and enter ISAKMP group configuration mode. If no specific group matches and a default group is defined, users will automatically be given the default group's policy. For this lab exercise, use a group name of vpn-remote-access:

```
RP(config)# crypto isakmp client configuration group vpn-remote-access
```

Step 2   Specify the IKE pre-shared key for group policy attribute definition. Note that this command must be enabled if the VPN Client identifies itself with a pre-shared key. For this lab exercise, use a key name of sw-client-password:

```
RP(config-isakmp-group)# key sw-client-password
```

Step 3   Specify the domain name to be pushed to the client. For this lab exercise use a domain name of **cisco.com**:

```
RP(config-isakmp-group)# domain cisco.com
```

Step 4   Select a local IP address pool. Note that this command must refer to a valid local IP address pool or the VPN Client connection will fail. For this lab exercise, use the remote-pool pool name:

```
RP(config-isakmp-group)# pool remote-pool
```

Step 5   Return to global configuration mode:

```
RP(config-isakmp-group)# exit
```

Task 6—Create a Transform Set

Create a transform set named transform-1 using the following commands:

Step 1   Create transform set 1:

```
RP(config)# crypto ipsec transform-set transform-1 esp-3des esp-sha-
hmac
```

Step 2   Return to global configuration mode:

```
RP(cfg-crypto-trans)# exit
```

Task 7—Create a Dynamic Crypto Map

In this lab exercise, you will use a dynamic crypto map to handle remote access traffic for the perimeter router. Use the following commands to create dynamic crypto map 1:

Step 1   Create dynamic crypto map 1, dynmap, and enter the crypto map configuration mode:

```
RP(config)# crypto dynamic-map dynmap 1
```

Step 2   Assign transform set 1 to dynmap 1:

```
RP(config-crypto-map)# set transform-set transform-1
```

Step 3 Enable RRI for the dynmap crypto map:

```
RP(config-crypto-map)# reverse-route
```

Step 4 Return to global configuration mode:

```
RP(config-crypto-map)# exit
```

Task 8—Apply Mode Configuration to the Dynamic Crypto Map

Mode configuration must be applied to a crypto map to be enforced. Use the following commands in global configuration mode to apply mode configuration to a crypto map:

Step 1 Configure the router to initiate or reply to mode configuration requests. Note that Cisco VPN Clients require the respond keyword to be used. The initiate keyword was used with older Cisco VPN Clients and is no longer used with the 3.x version Cisco VPN Clients:

```
RP(config)# crypto map dynmap client configuration address respond
```

Step 2 Enable IKE querying for group policy when requested by the VPN Client. The list-name argument is used by AAA to determine which storage is used to find the policy (local or RADIUS) as defined in the **aaa authorization network** command.

```
RP(config)# crypto map dynmap isakmp authorization list vpn-remote-
access
```

Step 3 Apply changes to the dynmap dynamic crypto map:

```
RP(config)# crypto map dynmap 1 ipsec-isakmp dynamic dynmap
```

Task 9—Apply a Dynamic Crypto Map to the Router Interface

Use the following commands to apply the new dynamic crypto map to the outside interface of the perimeter router:

Step 1 Enter interface configuration mode:

```
RP(config)# interface fast 0/1
```

Step 2 Assign the dynmap crypto map to the interface:

```
RP(config-if)# crypto map dynmap
```

Step 3 Return to global configuration mode:

```
RP(config-if)# exit
```

Task 10—Enable Perimeter Router Dead Peer Detection

Use the following commands to enable DPD for the perimeter router:

Step 1 Enable keepalives for DPD. The 20 value specifies the number of seconds between DPD messages (range is between 10 and 3600 seconds); the 10 value specifies the number of seconds between retries if DPD messages fail (range is between 2 and 60 seconds):

```
RP(config)# crypto isakmp keepalive 20 10
```

Step 2 Exit global configuration mode:

```
RP(config)# exit
```

Step 3 Save the router configuration:

```
RP# copy run start
```

Task 11—Verify the Easy VPN Server Configuration

Use the following command in exec mode to verify your configurations for this feature:

```
RP# show run
```

Your configuration should look similar to the following:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rP
!
no logging console
!
aaa new-model
!
!
aaa authorization network vpn-remote-access local
aaa session-id common
enable password cisco
!
username cisco password 0 cisco
memory-size iomem 15
ip subnet-zero
!
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 20 10
!
crypto isakmp client configuration group vpn-remote-access
```

```
 key sw-client-password
 domain cisco.com
 pool remote-pool
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap isakmp authorization list vpn-remote-access
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Ethernet0/0
 ip address 10.0.P.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.P.2 255.255.255.0
 half-duplex
 crypto map dynmap
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip local pool remote-pool 10.0.P.32 10.0.P.64
ip classless
ip http server
ip pim bidir-enable
```

```
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
 password cisco
!
!
end
```

Task 12—Install the Cisco VPN Client 3.x

Complete the following steps to install the Cisco VPN Client Release 3.x on your Windows 2000 Server student PC:

Step 1   Open the CiscoApps desktop folder.

Step 2   Open the Cisco VPN Client folder.

Step 3   Locate and run the Cisco VPN Client **setup.exe** executable. If this is the first time the VPN Client is being installed, a window opens and displays the following message: "Do you want the installer to disable the IPSec Policy Agent?"

Step 4   Click **Yes** to disable the IPSec policy agent. The Welcome window opens.

Step 5   Read the Welcome window and click **Next**. The License Agreement window opens.

Step 6   Read the license agreement and click **Yes**. The Choose Destination Location window opens.

Step 7   Click **Next**. The Select Program Folder window opens.

Step 8   Accept the defaults by clicking **Next**. The Start Copying Files window opens.

Step 9   The files are copied to the hard disk drive of the student PC and the InstallShield Wizard Complete window opens.

Step 10 Select **Yes, I want to restart my computer now** and click **Finish**. The student PC restarts.

Task 13—Create a New Connection Entry

Complete the following steps to create a new VPN connection entry:

Step 1   Choose **Start>Programs>Cisco Systems VPN Client>VPN Dialer**. The Cisco Systems VPN Client window opens.

Step 2   Click **New**. The New Connection Entry wizard opens.

Step 3   Enter **VPN Server** in the connection entry field.

Step 4   Click **Next**.

Step 5   Enter a perimeter router outside interface IP address of **172.30.P.2** in the remote server field
(where P = pod number).

Step 6   Click **Next**.

Step 7   Select **Group Access Information** and complete the following substeps. The following entries
are always case sensitive.

    1.   Enter a group name: **vpn-remote-access**. This is the group you created earlier on the
perimeter router.

    2.   Enter the group password: **sw-client-password**. This is the key you created earlier for the
vpn-remote-access group.

    3.   Confirm the password: **sw-client-password**.

Step 8   Click **Next**.

Step 9   Click **Finish** and leave the Cisco Systems VPN Client window open.

Task 14—Launch the Cisco VPN Client

Complete the following steps to launch the Cisco VPN Client on your student PC:

Step 1   Choose **Start>Programs>Cisco Systems VPN Client>VPN Dialer**.

Step 2   Verify that the connection entry is **VPN Server**.

Step 3   Verify that the IP address of remote server is set to your perimeter router public interface IP
address of **172.30.P.2** (where P = pod number).

Step 4   Click **Connect**. The Connection History window opens and several messages flash by quickly;
the window closes and a Cisco VPN Dialer icon appears in the system tray.

Task 15—Test the Remote Access Connection

Now that the VPN tunnel is operating, it is time to test the functionality. Complete the
following steps to test the VPN tunnel and the client connection:

Step 1   Right-click the **Cisco VPN Dialer** icon in the student PC system try and select the **status**
option.

    Q1)   What is the assigned client IP address?

    A)   _____

Step 2   Select the **Statistics** tab and move the window to a corner of your student PC display. You will
need to view the Status window for the next few steps.

Step 3   Open a command prompt shell and ping the inside interface of the perimeter RP:

C:\> **ping 10.0.P.2**

(where P = pod number)

Q2) Was the ping successful?

A) _____

Note: If you see packets going out but no packets returning, check to make sure that you enabled RRI in Task 7. Without RRI enabled, the router does not know which tunnel to return requested data on. Data goes through the tunnel to the router, but no packets return through the tunnel to the client.

Step 4 Close the command prompt shell.

Step 5 Click **OK** to close the status window.

Step 6 Select **Start>Programs>Cisco Systems VPN Client>Log Viewer** to start the Log Viewer application. If this is the first time you have entered Log Viewer, you may see a warning message asking if you really want to start the log capture. If this message appears, click **Yes** to enable capture now.

Step 7 Select the **Options** drop-down menu and select **Filter**.

Step 8 Right-click the **IKE** verbose level and set it to **high**.

Step 9 Right-click the **IPSEC** verbose level and set it to **high**.

Step 10 Click **OK** and leave the Log Viewer window open.

Step 11 Right-click the **Cisco VPN Dialer** icon in the student PC system tray and select the **disconnect** option.

Q3) What happened to the keys?

A) _____

Step 12 Select the Log Viewer options drop-down menu and select the **clear log display** option.

Step 13 Reconnect to the router using the Cisco VPN Dialer and view the results in the Log Viewer.

Step 14 Locate the MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN:, value event and answer the following question:

Q4) What is the domain name?

A) _____

Step 15 Disconnect the Cisco VPN Client and close the Log Viewer.

Task 16—Configure Extended Authentication

Now that you have configured and tested a basic Easy VPN implementation, it is time to add XAUTH. Use the following steps to add XAUTH to the existing Easy VPN Server configuration, starting in global configuration mode.

Step 1 Enable AAA login authentication for the local vpnusers user group:

```
RP(config)# aaa authentication login vpnusers local
```

Step 2   Set the timeout value (0–60 seconds) for the amount of time the remote user has to enter a username and password on the client. Use **20** seconds for the timeout value for this lab exercise:

```
RP(config)# crypto isakmp xauth timeout 20
```

Step 3   Enable IKE XAUTH for the dynmap dynamic crypto map using the vpnusers user group:

```
RP(config)# crypto map dynmap client authentication list vpnusers
```

Step 4   Exit global configuration mode:

```
RP(config)# exit
```

Step 5   Save the router configuration to the startup-config file:

```
RP# copy run start
```

Step 6   Use the following command in exec mode to verify your configurations for this feature:

```
RP# show run
```

Your configuration should look similar to the following. Bolded items are associated with extended authentication:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rP
!
no logging console
!
aaa new-model
!
!
```
`aaa authentication login vpnusers local`
```
aaa authorization network vpn-remote-access local
aaa session-id common
enable password cisco
!
username cisco password 0 cisco
memory-size iomem 15
ip subnet-zero
!
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
```

```
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 20 10
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group vpn-remote-access
 key sw-client-password
 domain cisco.com
 pool remote-pool
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap client authentication list vpnusers
crypto map dynmap isakmp authorization list vpn-remote-access
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Ethernet0/0
 ip address 10.0.P.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.P.2 255.255.255.0
 half-duplex
 crypto map dynmap
!
router eigrp 1
```

```
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip local pool remote-pool 10.0.P.32 10.0.P.64
ip classless
ip http server
ip pim bidir-enable
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
 password cisco
!
!
end
```

Task 17—Test Extended Authentication

Use the following steps to test the XAUTH configuration of the Easy VPN Server:

Step 1   Open the Cisco VPN Dialer application by selecting **Start>Programs>Cisco Systems VPN Client>VPNDialer**.

Step 2   Ensure that the Easy VPN Server connection entry is selected and that the IP address of your Easy VPN Server appears in the remote server field.

Step 3   Click **Connect**. If XAUTH is working correctly, the User Authentication for the Easy VPN Server window should appear.

Step 4   Enter a username of **cisco**.

Step 5   Enter a password of **cisco**.

Step 6   Click **OK**. The Cisco VPN Dialer icon should appear in the system tray of the student PC.

Step 7   Check the status of the VPN connection by right-clicking on the Cisco VPN Dialer icon in the student PC system tray and selecting **status** and the **statistics** tab.

Step 8   With the Status window still open, open a command shell and telnet to the Easy VPN Server. You should see the packets encrypted/decrypted counters increment.

Answers

This section contains answers to questions posed earlier:

Q1)   The address should be one of the addresses in the 10.0.P.32–10.0.P.64 range (where P = pod number). This is the address assigned by the router to the client using the **remote-pool** addresses.

Q2)   The ping should work correctly and you should see the statistics bytes in and bytes out counters incrementing with each ping. You should also see the packets encrypted and packets decrypted counters incrementing.

Q3)   The keys should be deleted as shown in the Log Viewer.

Q4)   The name should be cisco.com. This is the domain name you configured for the **vpn-remote-access** group earlier.

12

Using Security Device Manager

Overview

This lesson introduces and explains the Cisco Security Device Manager (SDM). The following topics are covered in this lesson:

- Objectives
- SDM overview
- SDM software
- Using the startup wizard
- Introducing the SDM user interface
- Using SDM to configure a WAN
- Using SDM to configure a firewall
- Using SDM to configure a VPN
- Using SDM to perform security audits
- Using the factory reset wizard
- Using SDM advanced and monitor modes
- Summary
- Lab exercise

Objectives

This topic lists the lesson's objectives.

Objectives

Cisco.com

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

- **Install the Cisco SDM on a Cisco router.**
- **Use SDM wizards to configure VPN policies on a Cisco router.**
- **Use SDM wizards to configure Cisco IOS Firewall policies on a Cisco router.**

SECUR 1.1—12-3

SDM Overview

This topic introduces the Security Device Manager.

What Is Security Device Manager?

- **Easy-to-use, browser-based device management tool embedded within the Cisco IOS access routers (Cisco 800–3700 Series)**
- **Provides intelligent wizards to enable quicker and easier deployments and does not require knowledge of Cisco IOS CLI or security expertise**
- **Tools for more advanced users**
  - **ACL editor**
  - **VPN crypto map editor**
  - **Cisco IOS CLI preview**

The Security Device Manager (SDM) is a browser-based device management tool for configuring single Cisco IOS routers. The SDM software files reside in the router Flash memory alongside other router operating system files.

The SDM contains several wizards to enable efficient configuration of major router virtual private network (VPN) and Cisco IOS Firewall parameters.

The SDM is designed to help you secure your Cisco routers and their associated networks without having to memorize multiple command line interface (CLI) commands.

SDM Features

- **Security audit—Automate with ICSA- and Cisco TAC-approved security configuration**
- **Intelligent wizards:**
  - **Autodetect misconfigurations and propose fixes**
  - **Strong security defaults and a router security audit**
  - **Cisco TAC- and ICSA-recommended security configurations**
- **Quick deployment—Startup wizard, one-step router lockdown (firewall), and one-step VPN (site-to-site) for quick deployment**
- **Guides untrained users through workflow**

| LAN | WAN | Firewall | VPN | Security Audit |

SDM contains a unique Security Audit wizard that provides a comprehensive Router Security Audit. SDM uses Cisco Technical Assistance Center (TAC) and International Computer Security Association (ICSA) recommended security configurations as its basis for comparisons and default settings.

Other SDM intelligent wizards include the following:

- An autodetect wizard for finding misconfigurations and for proposing fixes.
- Strong security defaults and configuration entry checks.
- Router and interface specific defaults that reduce configuration time.

SDM wizards help provide for faster VPN and firewall deployments. The SDM contains a suggested workflow (located in the lower part of the browser pages) to guide untrained users through router configuration.

A typical process flow proceeds as shown in the figure:

- Configure LAN parameters
- Configure WAN parameters
- Configure firewall parameters
- Configure VPN parameters
- End with a security audit.

SDM Features (Cont.)

- **Advanced users can quickly fine-tune configurations (ACL editor) or diagnose problems (VPN tunnel quality).**
- **Offers WAN interface (T1, serial, and DSL) discovery and wizard-based configuration.**
- **Online help is embedded with SDM.**

Although SDM is designed for users with little to no CLI experience, it is just as useful to advanced users. Advanced CLI users use SDM to quickly fine-tune configurations (using the access control list [ACL] editor) or diagnose problems (using the VPN tunnel quality monitor).

In addition to the configuration wizards already mentioned, SDM can be used to discover and configure existing LAN and WAN interfaces.

SDM contains an intuitive embedded online help system.

Intelligent About Security Configurations

SECUR 1.1—12-8

SDM contains embedded parameter checking intelligence to help you accurately configure router VPN and firewall settings.

Two examples are shown in the figure. If SDM detects a configuration conflict, the SDM software will generate a warning window describing the condition.

You should always read SDM warning messages and consider following the recommendations to repair the original condition. Warnings messages usually allow you to choose either to let SDM fix the configuration conflict automatically or choose to fix the conflict manually yourself.

SDM was designed with the following users in mind:

- Small office/home office (SOHO)—These SDM users usually have a working knowledge of networking and security, but no significant Cisco IOS CLI experience. SOHO/800 users typically use the Cisco Router Web Setup (CRWS) tool for general router configuration tasks, and then use SDM for router security configuration.

- SMB/SMB branch office—Small-to-medium business (SMB) and SMB branch office SDM users typically possess basic technical system administrator level knowledge. These users may have a rudimentary knowledge of networks and security, but no significant Cisco IOS CLI experience.

- Enterprise branch office—Enterprise branch office SDM users are typically network site administrators with a modest knowledge of Cisco CLI and basic security.

- Enterprise headquarters—These SDM users are typically very knowledgeable of CLI and are capable in both networking and security.

All of these users can benefit from SDM features.

SDM Software

This topic provides an overview of SDM software functions.

Supported Cisco Routers and Cisco IOS Software Releases

Cisco.com

- **SDM is supported on a number of Cisco router platforms and Cisco IOS software releases.**
- **Always verify SDM router and Cisco IOS release support at www.cisco.com/go/sdm.**

SECUR 1.1—12-11

SDM is supported on a number of Cisco routers and their associated Cisco IOS software versions.

Always consult the latest information regarding SDM router and Cisco IOS software release support at www.cisco.com/go/sdm.

Obtaining SDM

- **SDM is factory loaded on supported routers manufactured as of June 2003.**
- **Always check www.cisco.com/go/sdm for the latest information regarding SDM support.**
- **SDM cannot be ordered independent of the router.**
- **SDM can be downloaded from Cisco.com for existing routers at http://www.cisco.com/public/sw-center/sw-netmgmt.shtml.**

SECUR 1.1—12-12

SDM comes preinstalled on several Cisco router models manufactured in June 2003 or later that were purchased with the VPN bundle.

SDM is also available as a separate option on all supported routers with Cisco IOS software security features manufactured in June 2003 or later.

If you have a router that does not have SDM installed, and would like to use SDM, you must download it from Cisco.com and install SDM on your router. Ensure that your router contains enough Flash memory to support both your existing Flash file structure and the SDM files.

SDM Files

The sdm-v10.zip file contains the following files:

- **sdm.tar**
- **sdm.shtml**
- **sdmconfig-xxx.cfg file:**
  - **Enables HTTP server**
  - **Enables SSH/Telnet**
  - **Provides a default credential—username/password**
  - **Default configuration file specific to router series:**
    - **For example: sdmconfig-1710-1721.cfg**

SECUR 1.1—12-13

If you choose to install SDM on an existing (SDM supported) Cisco router, you must obtain the sdm-vXX.zip file from Cisco.com and copy it to your router Flash file system.

When you install SDM on an existing router, always use the latest "Downloading and Installing Cisco Security Device Manager (SDM)" documentation.

Follow the procedure for your specific router to download the SDM Files. SDM contains two procedures for accomplishing this depending on the type of Cisco router you have:

- Cisco non-800 Series router procedure

- Cisco 800 Series router procedure

Once you download the SDM files, there are two processes to replace the router configuration in Flash memory:
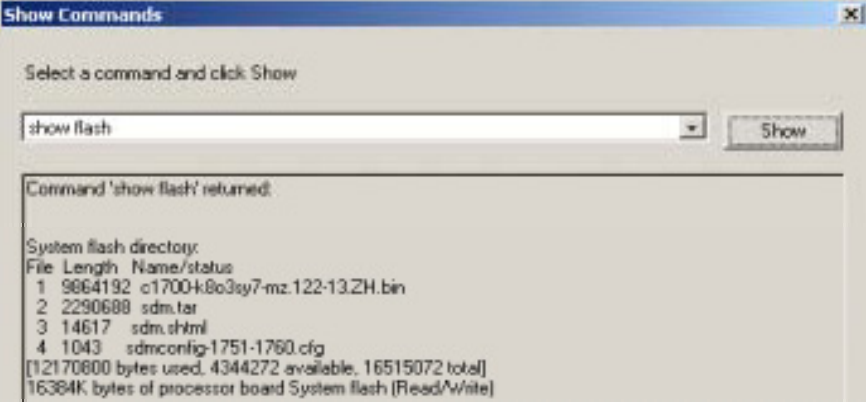
- Use the "Modify Your Existing Configuration File" procedure if you want to retain your existing configuration.

- Use the "Default Configuration File" procedure if the router does not contain a pre-existing configuration and you want to start from a fresh (SDM-provided) default configuration file.

| Note | SDM requires approximately 2.8 MB of free (available) router Flash memory. |

Displaying Router Flash

- **Use the** show flash **CLI command.**
- **Many** show **commands are also available within SDM user interface.**

If you are not sure whether SDM is loaded into Flash or you need to know how much Flash is available, use the **show flash** CLI command.

SDM contains several **show** commands. The **show flash** command is executed as shown in the figure. This SDM command displays the same information as the CLI command but in a GUI window.

In the example in the figure, you can see the Cisco IOS image and other files including the sdm.tar and sdm.shtml required files. Also you can see how much Flash is used and how much is available.

SDM Software Requirements

- **SDM is stored in the router Flash memory.**
- **SDM supports the following browsers:**
  - **Netscape version 4.79 or later.**
  - **Internet Explorer version 5.5 or later.**
  - **Java and JavaScript must be enabled.**
- **SDM is supported on the following Microsoft platforms:**
  - **Windows 98 SE**
  - **Windows NT 4.0 (SP 4)**
  - **Windows 2000**
  - **Windows XP**
  - **Windows ME**

SECUR 1.1—12-16

SDM uses an industry-standard Java client application to minimize the impact of the SDM application on router performance.

You access SDM by executing an HTML file in the router, which then loads the SDM Java file. Always use a supported browser to launch SDM from a PC. SDM currently supports the following browsers:

■   Netscape version $\geq$ 4.79

■   Internet Explorer version $\geq$ 5.5

| **Note** | Java and JavaScript must be enabled on the selected browser. The browsers listed here contain Java plug-ins with Java Virtual Machine (JVM). SDM also supports Java Runtime Engine (JRE) versions $\geq$ 1.3.1. |

The SDM client is compatible with the Microsoft operating systems listed in the figure.

SDM communicates with the router when accessing the SDM application for download to the PC, when reading and writing the router configuration, and when checking router status.

SDM uses different communications methods based on the Cisco IOS software version of the target routers.

■ For Cisco IOS Software Releases ≥ 12.3M and ≥ 12.2(13)ZH, SDM uses either an HTTP transport or a secure HTTP transport method (HTTPS). For earlier Cisco IOS versions, SDM uses remote copy (RCP) as the transport. In both cases SDM relies on Telnet access for communication to the routers.

Note   Because SDM can deny certain types of traffic, and lock down router access, it is very important for you to know how SDM communicates with your router. If you lock the router down too tightly, you may not be able to use SDM to administer the router.

■ For Cisco IOS Software Releases 12.2(11)T, 12.2(13)T and 12.2(15)T, SDM uses Secure Shell (SSH) and Telnet:

— When configuration changes are made in SDM, Cisco IOS commands are transferred to the router flash as a temporary file using RCP.

— The temporary file is copied to the router running configuration and then deleted.

— SDM uses a "squeeze" process to reclaim router flash. You use the squeeze function in two instances:

■ Whenever you are removing an older SDM version and adding a newer one

■ Whenever SDM prompts you to perform a "squeeze"

Using the Startup Wizard

This topic explains how to access the SDM startup wizard.

Router Administration Using SDM

Cisco.com

- **SDM is used for configuring, managing, and monitoring a single Cisco access router.**
- **SDM allows the ability for multiple concurrent users to be logged in.**
- **It is *not* recommended that multiple users use SDM to modify the configuration at the same time.**
- **You can use SDM and/or CLI commands:**
  - **Use CLI commands for features not supported by SDM.**
  - **Use SDM to configure security policies on unsupported interfaces.**

SECUR 1.1—12-19

SDM is a tool for configuring, managing and monitoring a single Cisco access router.

Each Cisco access router is accessible by its own copy of SDM which is located in the routers flash memory.

A common scenario that can be supported by SDM is to have a user monitoring the router while at the same time another user may use SDM to modify the configuration of the router. It is *not* recommended that multiple users use SDM to modify the configuration at the same time. Although SDM will permit this scenario, it does not assure consistent or predictable results.

Users now have the flexibility to configure the router with both SDM and the CLI. Since the SDM user interface does not support all of the Cisco IOS software functionality, for example, quality of service (QoS), you can augment the SDM generated configuration with some CLI commands.

For unsupported interfaces, such as ISDN interfaces, SDM automatically detects if the interfaces support security features, like firewalls, crypto maps, and NAT. If the security features are supported, users can use SDM to configure the security features to the unsupported interfaces. However, the user will still need to configure the unsupported interface parameters directly through CLI.

Accessing SDM for the First Time

Accessing SDM on a factory-fresh router with SDM installed:

1. **Connect PC to the router's lowest LAN Ethernet port using crossover cable.**
2. **Use a static IP address for PC: (10.10.10.2/255.255.255.0)**
3. **Launch supported browser.**
4. **Default URL to access SDM: https://10.10.10.1/flash/sdm.shtml**
5. **SDM default login:**
   - **Username: sdm**
   - **Password: sdm**

Use the following process when you access SDM for the first time. This procedure assumes either an out-of-box router with SDM installed, or a default SDM configuration was loaded into flash.

Step 1 Connect a PC to the router's lowest number LAN Ethernet port using a cross-over cable.

Step 2 Assign a static IP address to the PC. It's recommended to use **10.10.10.2** with a **255.255.255.0** subnet mask.

Step 3 Launch a supported Browser.

Step 4 Use URL **https://10.10.10.1/flash/sdm.shtml**. You will be prompted to log in.

Step 5 Log in using the default user account:

- Username: **sdm**
- Password: **sdm**

The SDM startup wizard opens, requiring you to enter basic network configuration.

Startup Wizard—Welcome Window

• **Automatically displays the default configuration.**

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—12-21

| **Note** | The startup wizard information needs to be entered only once and will only appear when a default configuration is detected. |

Step 6 Click **Next**. The Basic Configuration window opens.

Startup Wizard—Basic Configuration, Change Default Username and Password

Cisco.com

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

SECUR 1.1—12-22
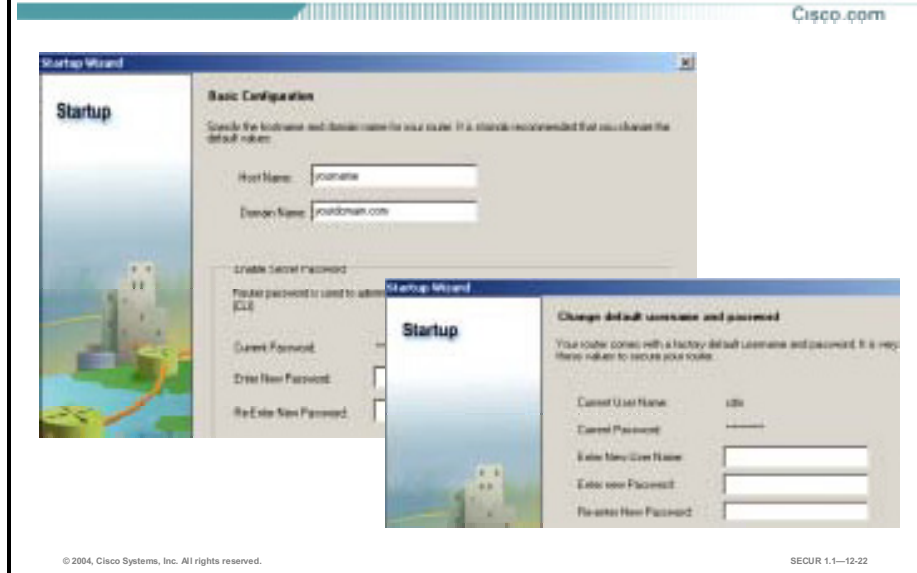
Step 7 (Optional.) Enter the router host name in the **Host Name** field.

Step 8 (Optional.) Enter the router domain name in the **Domain Name** field.

Step 9 Enter a new enable secret password using a minimum length of 6 characters in the **Enter New Password** field.

Step 10 Enter the new password, once more, in the **Re-Enter New Password** field.

Note   SDM will not allow you to proceed until a valid password is entered and re-entered.

Step 11 Click **Next**. The Change default username and password window opens.

Step 12 Enter a new username in the **Enter New User Name** field.

Step 13 Enter a new password in the **Enter New Password** field.

Step 14 Enter the new password, once more, in the **Re-enter New Password** field.

Step 15 Click **Next**. The LAN Interface Configuration window opens.

Startup Wizard—LAN Interface Configuration

Cisco.com

Startup Wizard

Startup

LAN Interface Configuration

Configure the IP address of this interface. It is recommended that you change the default value of the IP Address.

Interface: Ethernet0

IP address: [10.10.10.1]

Subnet Mask: [255.255.255.0]   or Subnet bits: [__]

SECUR 1.1—12-23

Step 16 Enter the IP address of the router interface connected to the LAN network in the **IP address** field.

Step 17 Enter an appropriate subnet mask in the **Subnet Mask** field.

Step 18 Click **Next**. The DHCP Server Configuration window opens.

Startup Wizard—DHCP Server Configuration

Step 19   Check the **Enable DHCP Server on LAN Interface** check box.

Note	For 8xx routers, the checkbox is selected by default.

Step 20   Enter the DHCP pool starting IP address in the **Start IP address** field.

Step 21   Enter the DHCP pool ending IP address in the **End IP address** field.

Note	The address pool must be based on the LAN IP address and subnet mask that you entered in the LAN Interface Configuration window.

Step 22   Click **Next**. The Domain Name Server window opens.

Startup Wizard—DNS Configuration

Cisco.com

Startup Wizard

Startup

Domain Name Server Configuration

It is recommended that you enter the Primary and Secondary Domain Name Server IP addresses. These will be used by SDM for domain name and address resolution. Your network administrator or ISP can provide these to you.

Primary DNS: [   ] (Optional)

Secondary DNS: [   ] (Optional)

SECUR 1.1—12-25

Step 23   Enter a primary DNS server IP address in the **Primary DNS** field.

Step 24   Enter a secondary DNS server IP address in the **Secondary DNS** field.

Step 25   Click **Next**. The Security Configuration window opens.

Startup Wizard—Security Configuration

SDM lets you disable some features that are on by default in Cisco IOS software. When enabled, these features can create security risks or use up valuable memory in the router. SDM also enables basic security features for protecting the router and the surrounding networks.

Generally, you should leave the check boxes in this window selected, unless you know that your requirements are different. Later if you decide to enable a feature listed here, you can use the SDM Advanced mode to re-enable them.

Step 26 Select or deselect the checkboxes according to your security requirements:

■ **Disable SNMP services on your router**—Disables SNMP services on your router.

■ **Disable services that involve security risks**—Disables services that are considered security risks. Examples include the finger service, TCP and UDP small servers, Cisco Discovery Protocol (CDP), and others.

■ **Enable services for enhanced security on the router/network**—Enables TCP SYN wait time, logging, a basic firewall on all outside interfaces, and others.

■ **Enhance security on router access**—Secures vty (Telnet) access, passwords and parameters, banner settings, and others.

■ **Encrypt passwords**—Enables password encryption within the router configuration.

Step 27 Click **Next**. The Wizard Summary window opens.

Startup Wizard—Summary Window

SECUR 1.1—12-27
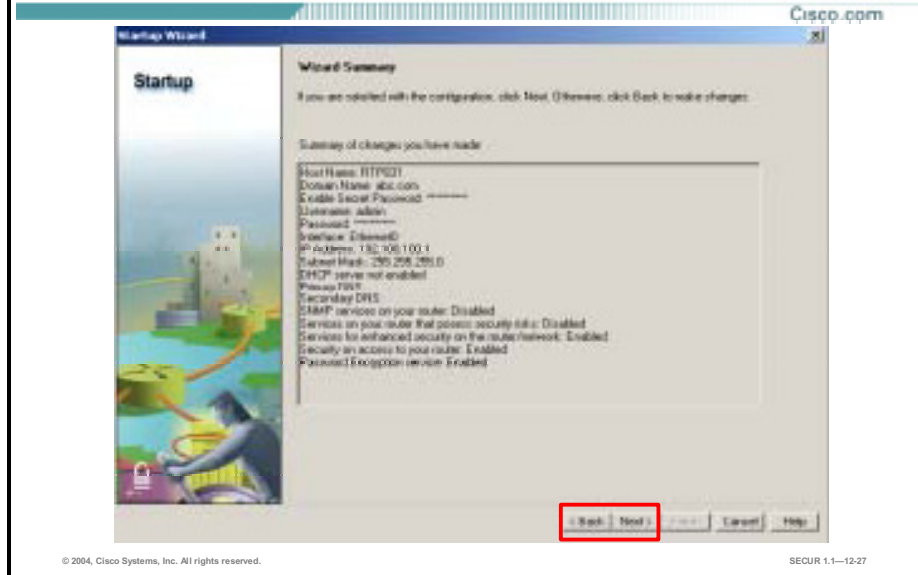
Step 28 Review the contents of the summary window.

Step 29 Click **Next**. The Startup Wizard Completed window opens.

Startup Wizard—Configuration Delivery
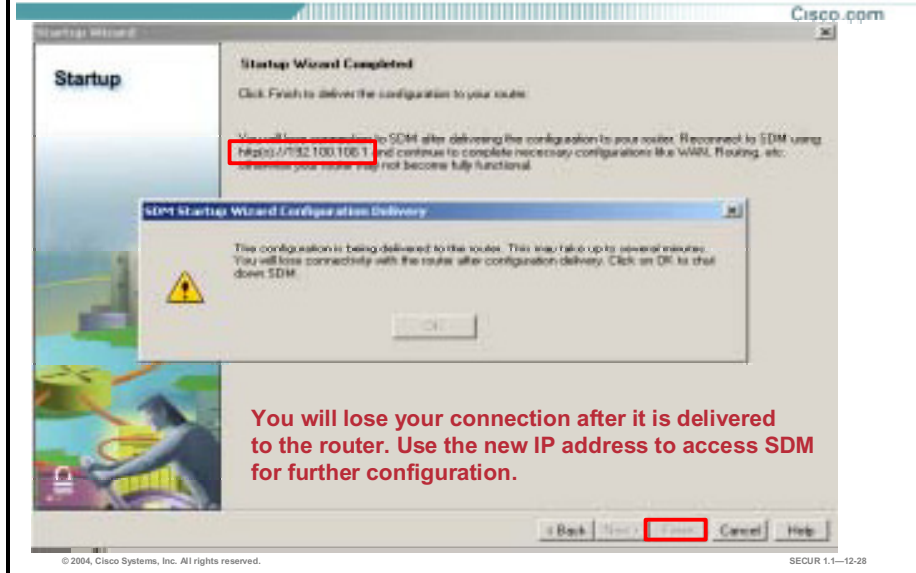
Note	The new IP address that must be used to reconnect to the router and re-launch SDM is displayed.

Step 30 Click **Finish** to deliver the configuration to router flash memory. The SDM Startup Wizard Configuration Delivery message box opens. Once the configuration is delivered the OK button becomes enabled.

Step 31 Click **OK** to shut down SDM and terminate the connection.

- **Already configured router with SDM installed:**
    1. **Use a LAN/WAN connection.**
    2. **Manage the router using either HTTP or HTTPS with https://<router IP address>/flash/sdm.shtml.**
- **Note:**
    - **https:// specifies that SSL be used for a secure connection.**
    - **http:// can be used if SSL is not available.**

To access SDM after the initial startup wizard is completed, use either http: or https:, followed by the router IP address /flash/sdm.shtml, as shown in the figure.

When you enter https it specifies that the Secure Sockets Layer (SSL) protocol be used for a secure connection. If SSL is not available, use http: to access the router.

Once you have your WAN interface configured, you can access SDM through a LAN or WAN interface.

SDM—Startup Troubleshooting

Cisco.com

- **Browser problem?**
  - Enable Java and JavaScript on the browser.
  - Disable popup blockers or unsupported Java plug-ins on PC.
- **Router not allowing access?**
  - Ensure that HTTP server is enabled on router.
  - Ensure PC is not blocked on interface by Firewall ACL.
    - Requires HTTP/HTTPS and SSH/Telnet or SSH/Telnet and RCP access to router
    - Open specific addresses/ports in ACL editor in advanced mode
- **SDM installed?**
  - Access it with https://<router IP address>/flash/sdm.shtml.
  - Enter CLI show flash **command.**

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

SECUR 1.1—12-30

Use the following tips to troubleshoot SDM access problems:

■ First determine if there is a browser problem by checking the following:

— Are Java and JavaScript enabled on the browser? Enable them.

— Are popup windows being blocked? Disable popup blockers on the PC (SDM requires popup windows).

— Are there any unsupported Java plug-ins installed and running? Disable them using the Windows Control Panel.

■ Is the router preventing access?—Remember that certain configuration settings are required for SDM to work. Check the following:

— Did you use one of the default configurations, or did you use an existing router configuration? Sometimes new configurations disable SDM access.

— Is HTTP server enabled on the router? If it is not, enable it and check that other SDM prerequisite parameters are configured as well. Refer to the "Downloading and Installing Cisco SDM" document for the required settings.

— Did SDM access work before, but now its not? Ensure your PC is not being blocked by a new ACL. Remember SDM requires HTTP, SSH, Telnet access and/or RCP access to the router (which could have been inadvertently disabled in a security lockdown).

■ Is SDM installed?

— The quickest way to determine this is to access it using the appropriate HTTP or HTTPS method (https://<router IP address>/flash/sdm.shtml).

— Use the **show flash** command to view the flash file system and make sure the required SDM files are present.

Introducing the SDM User Interface

This topic explains the various elements of the SDM user interface.
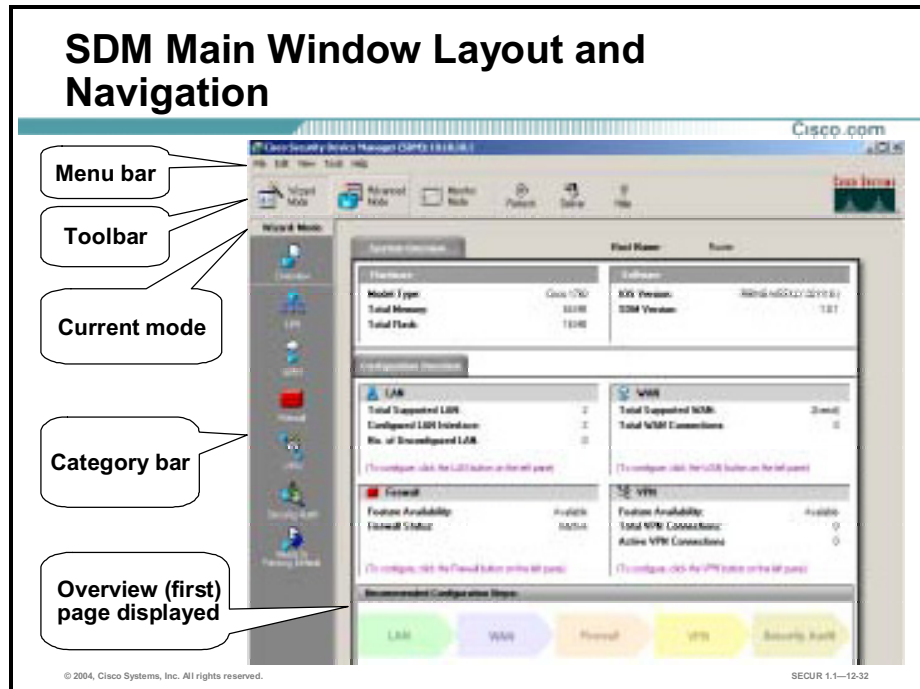
SDM uses an intelligent configuration reader. When SDM is launched, it reads the existing router configuration and presents the features that are available for SDM configuration.

The SDM main window contains the following elements:

- Menu bar—Provides the standard File, Edit, View, Tools, and Help menus.
- Tool bar—Provides access to SDM wizards and operating modes.
- Current mode indicator—Displays the current mode you are in.

Note The menu, tool bar, and current mode are always displayed at the top of each window. The other parts of the screen change based upon the mode and function you are performing.

- Category bar—Displays the options available in the present window. The selection changes to reflect the options available for the current mode.

When you first log into SDM, the Overview window opens. This window displays a summary of the router configuration settings. It displays the router model, total amount of installed memory and flash, Cisco IOS and SDM versions, the hardware installed, and a summary of some security features such as the state of the firewall and the number of active VPN connections.

SDM Menu Bar and Menu Items
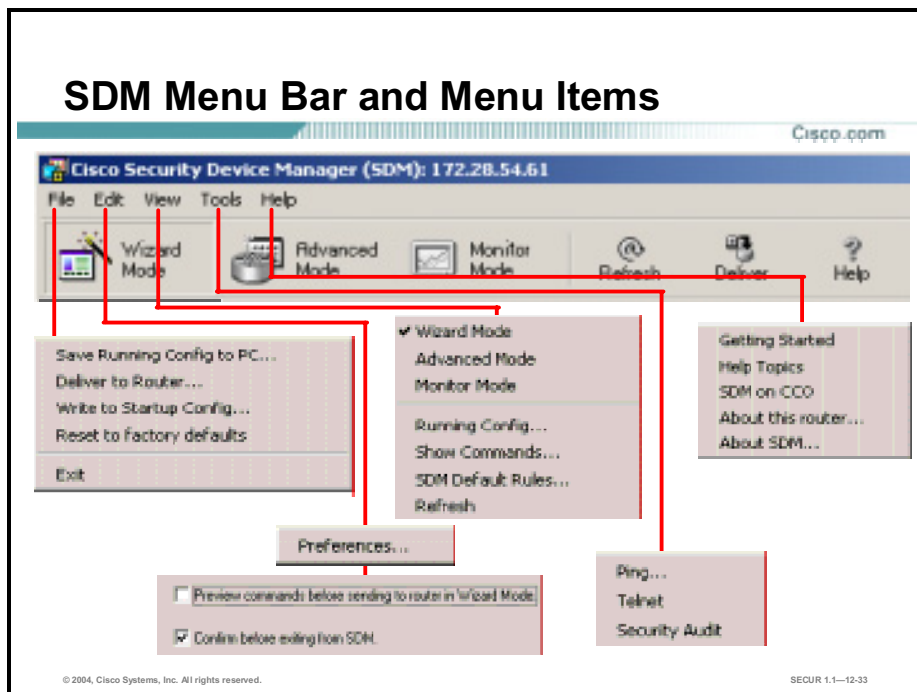
The SDM menu bar contains the following elements:

■ **File**—Contains the common file functions such as save the running configuration to the PC, deliver SDM configuration changes to the router, write running configuration to startup configuration, and reset the router to the SDM factory default configuration.

■ **Edit>Preferences**—Contains the following two options:

— **Preview commands before sending to router in Wizard Mode**—Select this option if you would like SDM to display a list of the configuration commands generated in Wizard Mode before the commands are sent to the router. The default is to not display the commands.

— **Confirm before exiting from SDM**—Select this option if you want SDM to display a dialog box asking for confirmation (are you sure?) when you exit SDM. The default is to display the message.

Note   Each time you log in, SDM remembers these preferences.

■ **View**—Allows you to switch modes, view router running configurations, use common router **show** commands, display SDM default rules, or perform a refresh (removes all undelivered SDM configurations).

■ **Tools**—Allows you to use extended ping, Telnet into the router, or perform a router security audit. SDM 1.0.1 contains an additional tool called Update SDM. This new tool is used to determine whether a newer version of SDM is available for download from Cisco.com, and it can perform an SDM update from the PC or directly from Cisco.com.

■ **Help**—Provides access to common online help methods and the current SDM and router software versions.

SDM Modes

SECUR 1.1—12-34
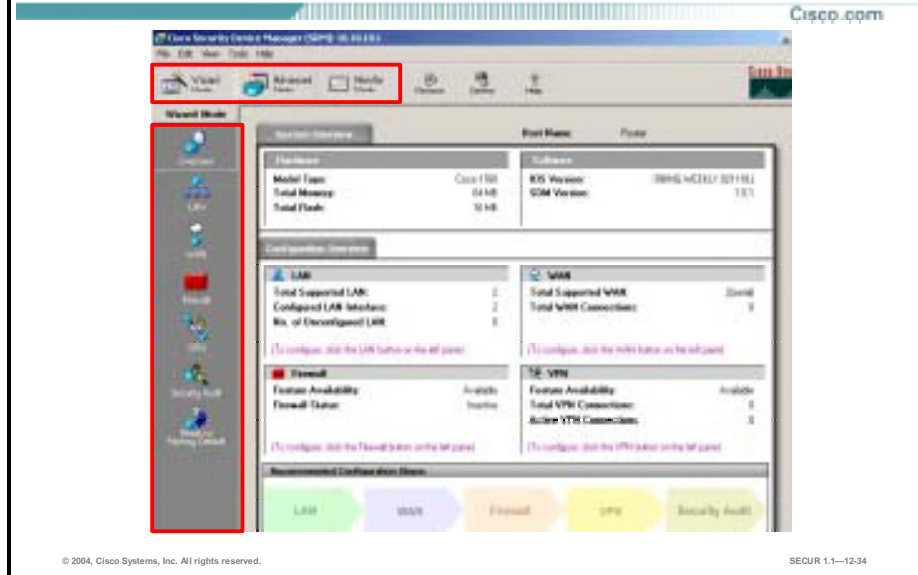
Navigating the SDM user interface is done through the toolbar.

SDM contains the following three modes:

■ Wizard mode—Designed for the novice, this mode can be used to guide you through common SDM tasks.

■ Advanced mode—This mode is designed for more experienced SDM users who prefer to perform tasks in any order. In this mode, you can freely view existing configurations and configure features within and outside of the wizards.

■ Monitor mode—This mode is used to view the following:

— Router status

— Interface status

— Firewall status

— VPN status

— Logging status

Other Toolbar Functions
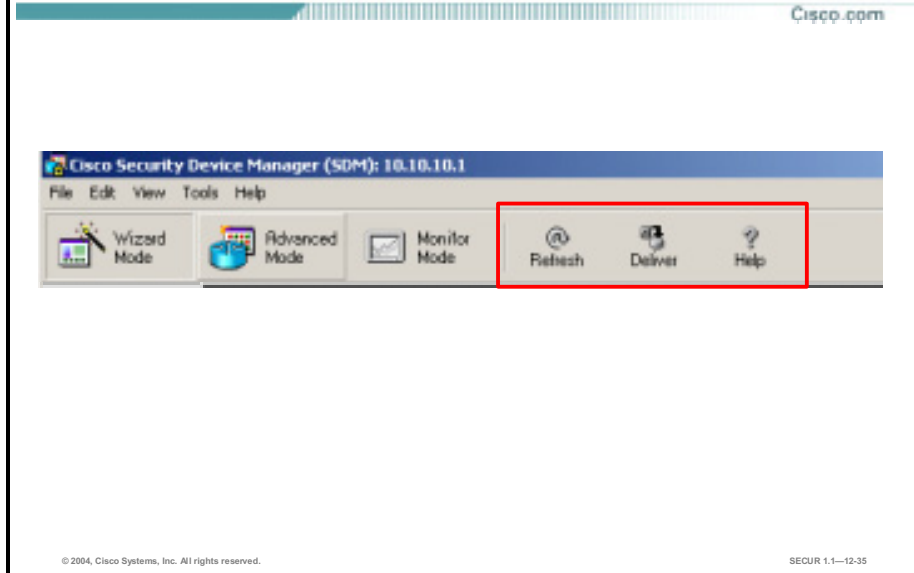
The toolbar also contains three other buttons as shown in the figure:

- **Refresh**—Reloads information from the router and updates the SDM display. This removes all undelivered SDM configurations.

- **Deliver**—Displays the Deliver to Router dialog box, which lets you send the configuration commands you have generated with SDM to the router. Your router is not configured until you complete this step. This is the last step that is done automatically when you use a Wizard.

Note　　When in the Advanced mode, you must manually deliver the configuration.

- **Help**—Displays the online help.

Using the Deliver Function

SECUR 1.1—12-36
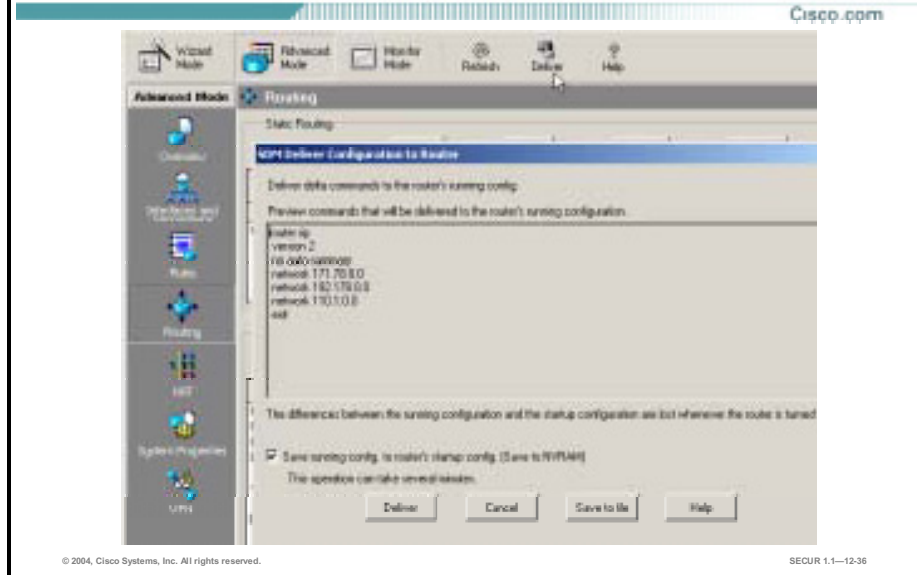
The Deliver function displays the commands to be delivered to the router.

You may choose to save the router configuration as a file on your PC. When you click **Save to file**, SDM creates an **sdm-cli-*timestamp*.txt** file to a specified directory on your PC HDD.

SDM Wizard Options
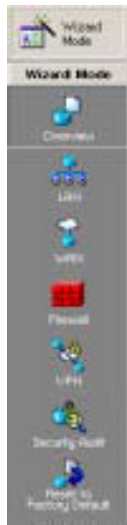
- **Overview—View the Cisco IOS version, the hardware installed, and configuration summary for the router.**
- **LAN Configuration—Configure LAN interfaces and DHCP.**
- **WAN Configuration—Configure PPP, Frame Relay, and HDLC WAN interfaces.**
- **Firewall—Access two types of firewall wizards:**
  - **Simple inside/outside.**
  - **More complex inside/outside/DMZ with multiple interfaces.**
- **VPN—Access three types of VPN wizards:**
  - **Secure site-to-site VPN**
  - **Easy VPN**
  - **GRE tunnel with IPSec VPN**
- **Security Audit—Performs a router security audit and provides easy instructions on how to lock down the router.**
- **Reset—Restores router to factory default settings.**

SECUR 1.1—12-37

SDM contains several wizard options as shown in the figure:

- LAN wizard—Used to configure the LAN interfaces and DHCP.

- WAN wizard—Used to configure PPP, Frame Relay, High-Level Data Link Control (HDLC) WAN interfaces. Check www.cisco.com/go/sdm for the latest information regarding wizards and the interfaces they support.

- Firewall wizards—Contains two options:

  — A simple inside/outside firewall wizard.

  — A more complex inside/outside/DMZ with multiple interfaces wizard.

- VPN wizards—Contains three options:

  — A secure site-to-site VPN wizard.

  — An Easy VPN wizard.

  — A GRE tunnel with IPSec wizard.

- Security Audit wizards—Contains two options:

  — The router security audit wizard.

  — An easy one-step router security lock down wizard.

- Reset wizard—Resets the router configuration back to the SDM factory default configuration settings.

Note   At the end of each wizard procedure, all changes are automatically delivered to the router using SDM-generated CLI commands. You may choose whether or not to preview the commands to be sent. The default is to not preview the commands.

Using SDM to Configure a WAN

This topic explains how to configure a WAN using SDM.

WAN Wizard—Create a New WAN Connection

SECUR 1.1—12-39

Step 1 Click the **WAN** wizard mode button. The WAN—Create a new WAN connection window opens. This window allows you to create new WAN connections and to view existing WAN connections.

Step 2 Select a WAN connection type radio button from the list. The types shown in this list are based on the physical interfaces installed on the router and awaiting configuration. A use case scenario diagram for the selected interface type appears to the right.
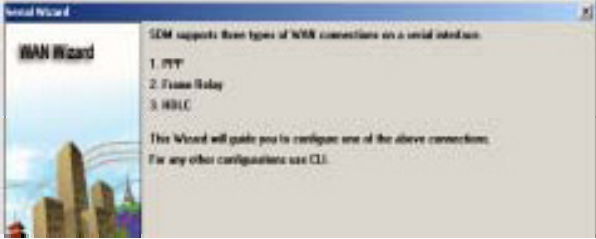
Note If your router has interfaces not supported by SDM, such as an ISDN interface, or a supported interface that has an unsupported configuration that was created using CLI, the interface will not appear in this window. If you need to configure another type of connection, you can do that by using the CLI.

Step 3 Click **Create a new connection**. In our example, we have chosen to configure a serial frame relay WAN. The Serial Wizard window opens.
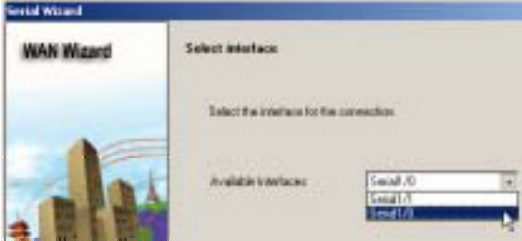
The SDM Serial wizard first reviews the different types of WAN connections supported by SDM.

Step 1   Click **Next**. The Select Interface window opens.

Step 2   Select the interface that you want to use for this connection from the Available Interfaces list box. This list contains the available unconfigured interfaces.

Step 3   Click **Next**. The Configure Encapsulation window opens.

WAN Wizard—Configure Encapsulation and IP Address

- **Select the encapsulation.**

- **Enter IP address.**
- **Enter subnet mask or select /X.**

Step 4 Select the appropriate Encapsulation type radio button.

Step 5 Click **Next**. The Enter the IP Address for the connection window opens.

Step 6 Select the **Static IP Address** radio button.

Step 7 Enter a static IP address in the IP Address field.

Step 8 Enter a subnet mask in the Subnet Mask field (or click the subnet up/down arrows and let SDM enter the correct subnet).

Step 9 Click **Next**. The Configure LMI and DLCI window opens.

WAN Wizard—Configure LMI and DLCI

- **Select the LMI type.**
- **Enter the DLCI.**
- **Select the Use IETF Frame Relay Encapsulation check box for non-Cisco routers.**

SECUR 1.1—12-42

Step 10 Select the LMI Type radio button (or select the autosense function radio button) from the LMI type list.

Step 11 Enter the DLCI for this interface in the DLCI field.

Step 12 If the remote end of the WAN terminates on a non-Cisco router, select the **Use IETF FR Encapsulation** check box.

Step 13 Click **Next**. The Advanced Options window opens.

WAN Wizard—Advanced Options
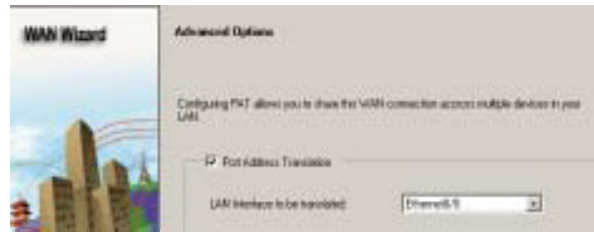
- **Select the Port Address Translation check box and the LAN interface to be translated.**

SECUR 1.1—12-43

Step 14 (Optional.) Select the PAT radio button.

Step 15 (Optional.) Select the LAN interface to be translated from the list box.

Step 16 Click **Next**. The Summary window opens.

WAN Wizard—Summary

SECUR 1.1—12-44
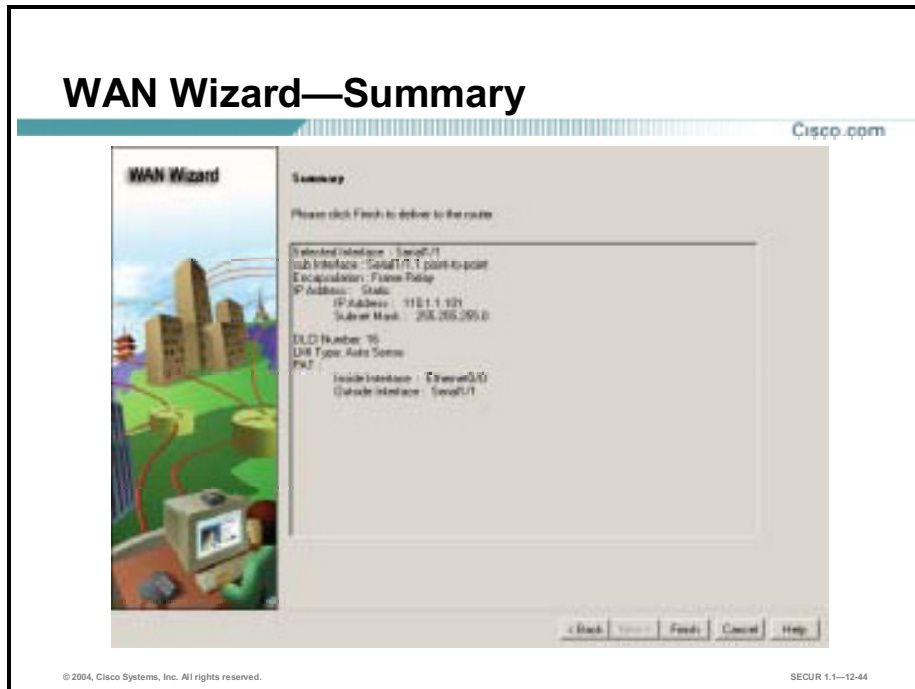
Step 17   Examine the summary. Go back and make any changes if required.

Step 18   Click **Finish**. The SDM Commands Delivery Status message box opens. Once the delivery is completed, the OK button becomes active.

WAN Wizard—Deliver Configuration Changes to Router Flash

SECUR 1.1—12-45
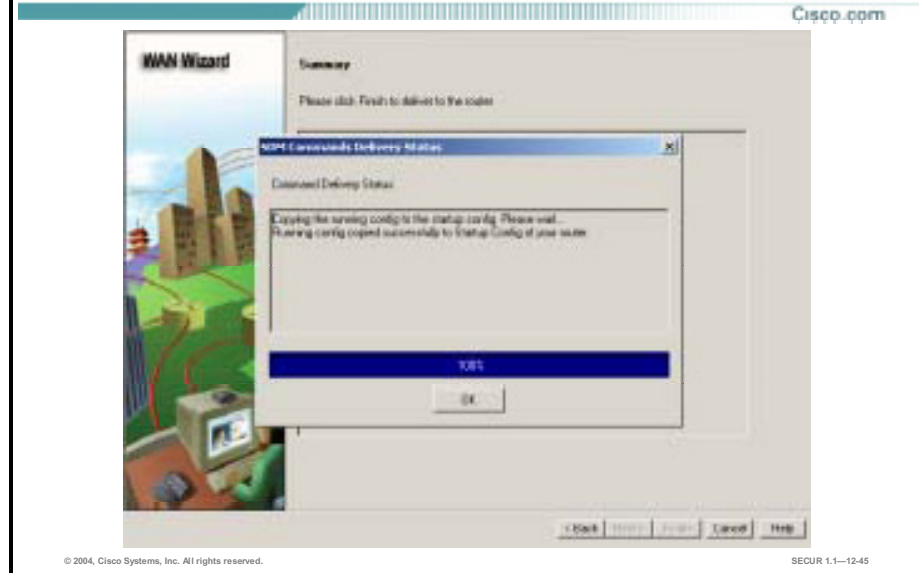
Step 19 Verify that the configuration was successfully copied to router and click **OK**. The WAN wizard main window opens.

WAN Wizard—Edit Existing WAN Connection
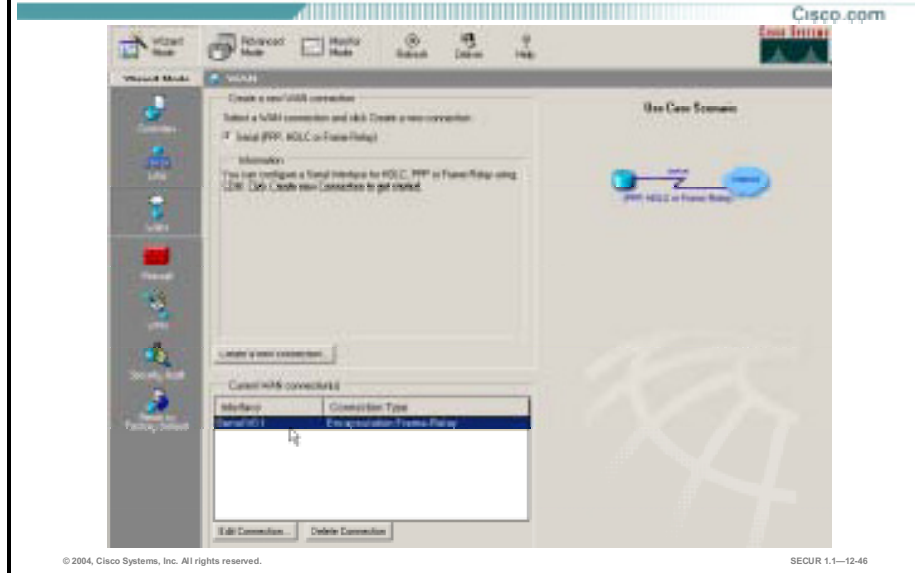
The new WAN connection appears in the Current WAN connection(s) list.

At this point, you could select the connection and edit or delete it.

Advanced Mode—Interface Status

SDM automatically enables the new WAN interface by issuing the **no shutdown** CLI command.

Select **Advanced Mode>Interfaces and Connections** to verify the interface status. This window displays all of the router connections and their states (up=green, down=red). You can also use this window to take a router connection down/up or up/down.

Using SDM to Configure a Firewall

This topic explains how to use SDM to configure the Cisco IOS Firewall feature on SDM supported routers.
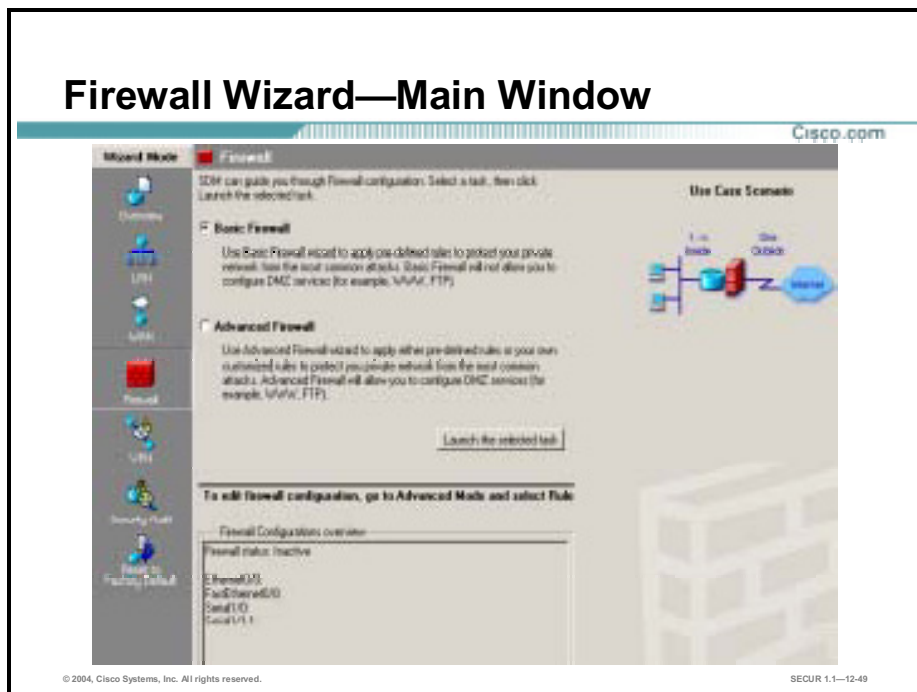
Step 1   Click **Firewall** from the Wizard Mode category bar. The firewall wizard main window opens.

Step 2   Select the type of firewall that you want to create:

■   **Basic Firewall**—Select this radio button if you want SDM to create a firewall using SDM default rules. This one-step firewall wizard configures only one outside interface and one or more inside interfaces. It does not support configuring a DMZ or custom inspection rules. The use case scenario diagram represents a typical network configuration for this type of firewall. This is a basic Firewall used in telecommuter or SOHO scenarios.

■   **Advanced Firewall**—Select this radio button if you want SDM to lead you through the configuration of a firewall with a DMZ interface. This wizard allows you to configure the router to connect to the Internet and configure hosts off a DMZ interface to be accessible to outside users. This wizard also lets you specify an inspection rule for the firewall.

Step 3   Click **Launch the selected task**. The Welcome to the One-step Firewall Configuration Wizard window opens.

Firewall Wizard—Basic Firewall Interface Configuration

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

SECUR 1.1—12-50
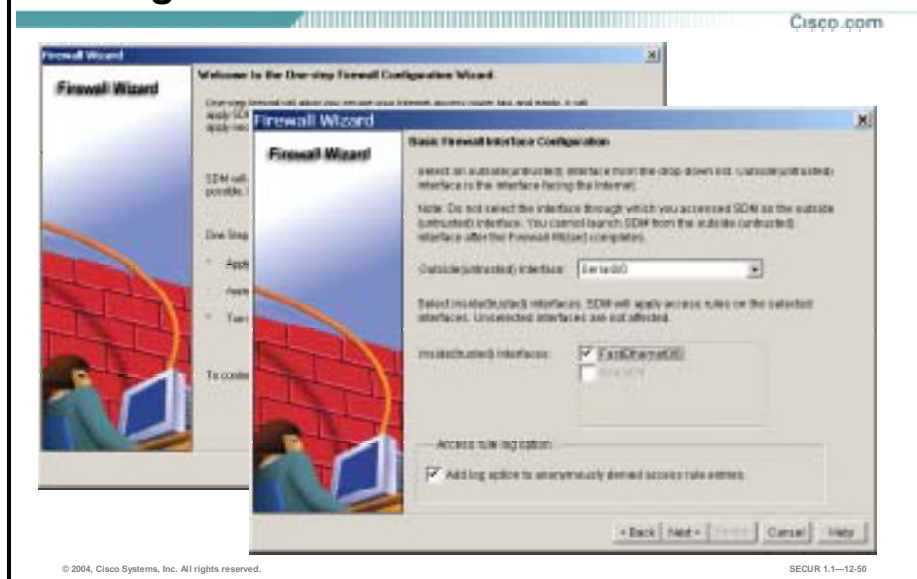
Step 4   Click **Next**. The Basic Firewall Interface Configuration window opens.

Step 5   Specify the following:

- The outside (untrusted) interface is connected to the Internet or to your organizations WAN.

- The inside (trusted) interfaces connect to the LAN. You can select multiple interfaces.

Note	When making firewall settings, keep in mind which interface you are using to access SDM through. If you select the interface that you accessed SDM as the outside (untrusted) interface, it will cause you to lose your connection to SDM because it is now protected by a firewall. This means you will not be able to launch SDM from the outside interface after the Firewall Wizard completes. There is a warning window that reminds you of this possibility. If you should inadvertently lock yourself out, you will need to access the router using the console and modify the firewall access lists before you can log into SDM again.

Step 6   Check the **Add log option to anonymously denied access rule entries** radio button if you want to log all failed network access attempts caused by unauthorized users or protocols that are specified in the firewall access rules.

Step 7   Click **Next**. The One-step Firewall Configuration Summary window opens.

Firewall Wizard—One-Step Firewall Configuration Summary
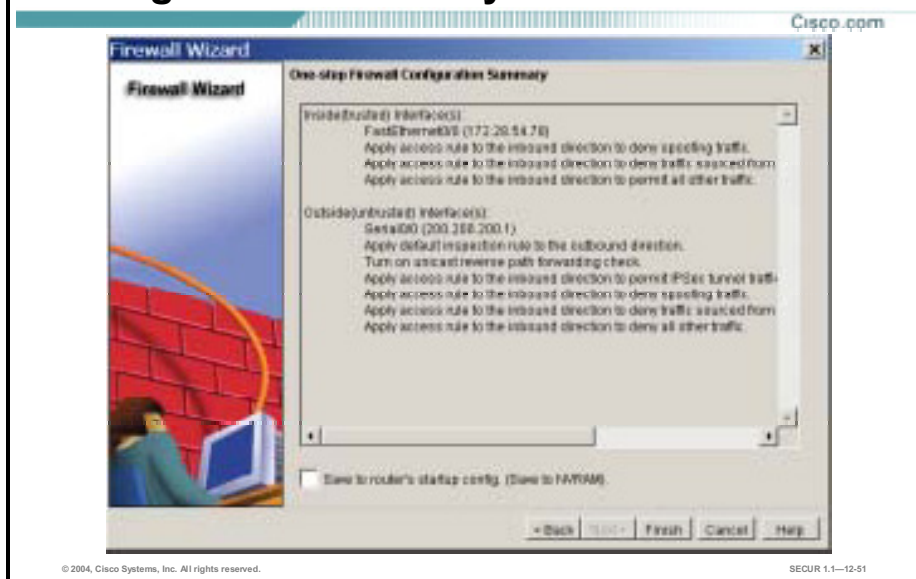
This window summarizes the firewall information. You can review the information by using use the **Back** button to return to screens in the wizard to make changes.

SDM lists the router's interfaces that you designated as the interfaces in this wizard session, along with their IP addresses. SDM describes in English versus CLI syntax the access and inspection rules that will be associated with these interfaces if these changes are applied.

Step 8 Read your firewall wizard summary screen to determine the types of settings are what you want.

Note	At the bottom of the window, you may also select to save the configuration to the router's startup configuration.

Step 9 Click **Finish**. The SDM Commands Delivery Status message box opens.

Firewall Wizard—SDM Commands Delivery Status

SECUR 1.1—12-52
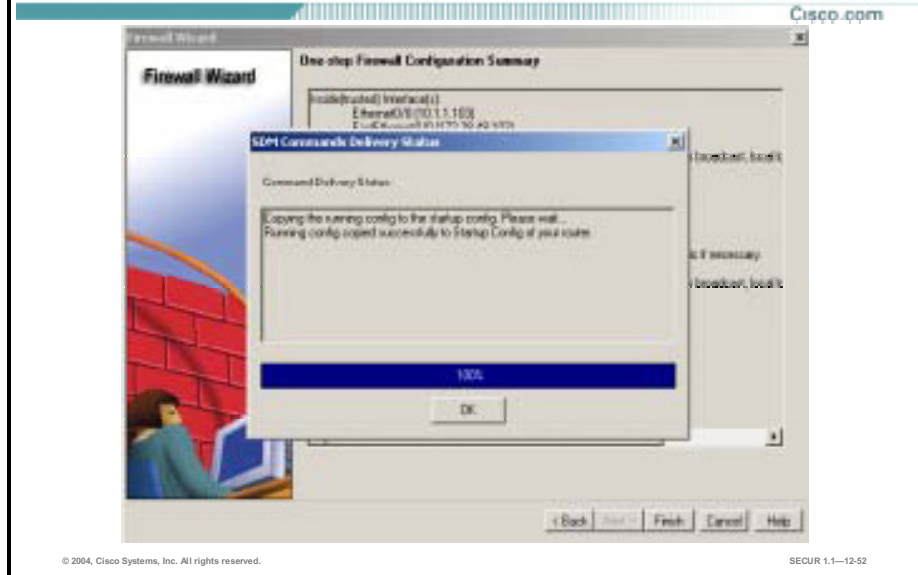
If you checked the Preview option in the Preferences menu, clicking Finish will display the commands you are sending to the router's configuration in flash.

Step 10   Click **OK**.

Advanced Firewall Wizard—Interface Configuration
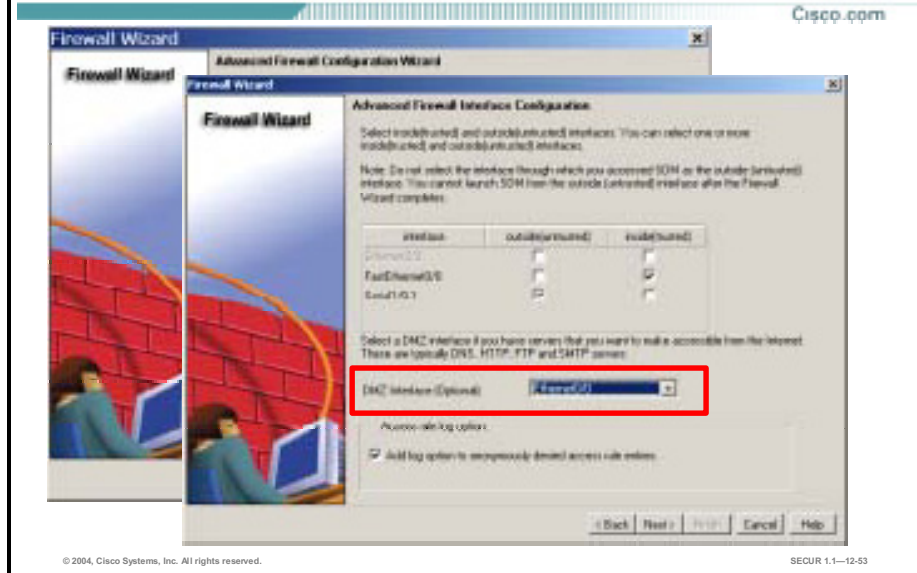
To create an advanced firewall, select a DMZ interface as shown in the figure.

Step 1 Select the router interface that connects to the DMZ network.

Step 2 Click **Next**. The Advanced Firewall DMZ Service Configuration window opens.

Advanced Firewall Wizard—DMZ Service Configuration

SECUR 1.1—12-54
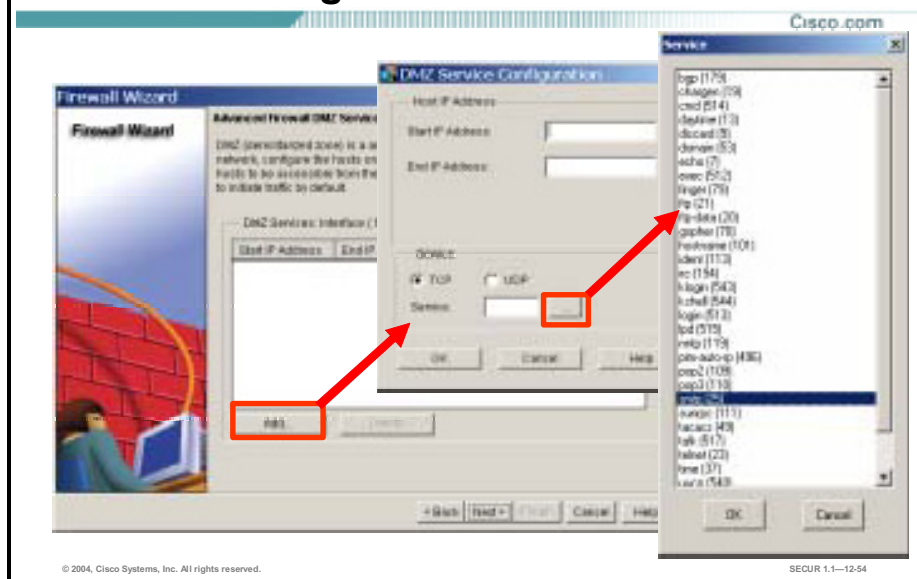
Step 3   Click **Add**. The DMZ Service Configuration window opens.

Step 4   Configure the DMZ network hosts by specifying the address range with start and end IP addresses.

Note   To specify an individual host, just enter a start IP address with no end IP address.

Step 5   Select either the TCP or UDP radio button, if you want to allow traffic for one of those services.

Step 6   Click the **Service …** button. The Service window opens.

Step 7   Select a service from the list and click **OK**.

Step 8   Repeat steps 6 and 7 to add additional services to the DMZ service list.

Step 9   When finished adding services, click **Next**. The Internet Firewall Inspection Rule Configuration window opens.

Advanced Firewall Wizard—Configure Inspection Rules

© 2004, Cisco Systems, Inc. All rights reserved. SECUR 1.1—12-55
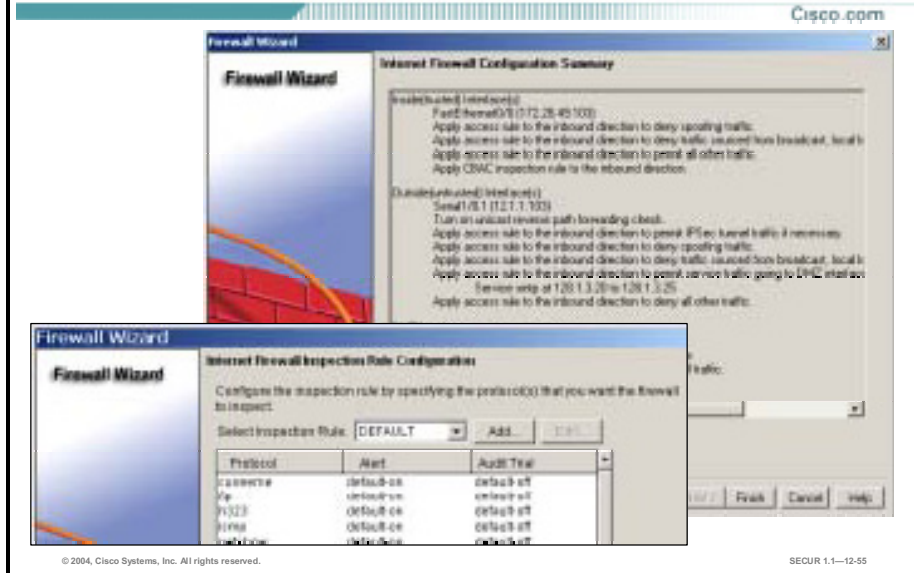
Step 10   Use the default SDM inspection rule or click **Add** and build a new inspection rule.

Step 11   Click **Next**. The Internet Firewall Configuration Summary window opens.

Note	The firewall wizard takes into consideration any pre-existing VPNs configured for the router. The firewall wizard will not create a rule that will block valid VPN users.

Step 12   Click **Finish**. The configuration changes are sent to the router.

The inspection rule is applied to the inside interface in the inbound direction and the DMZ interface in the outbound direction.

Using SDM to Configure a VPN

This topic explains how to use SDM to configure VPNs on supported routers.
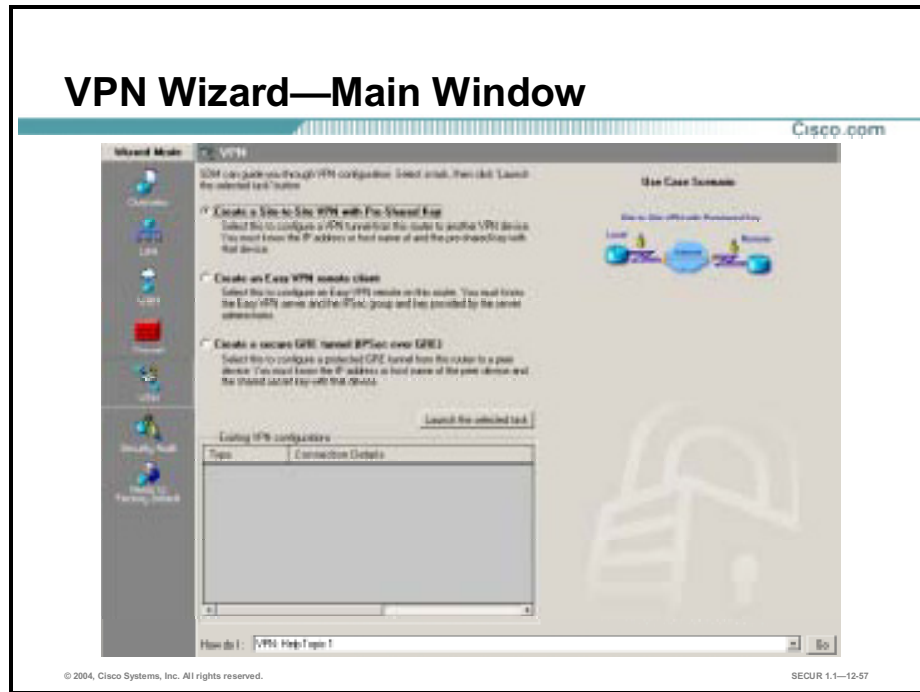
You can let SDM guide you through a simple VPN configuration by using the VPN wizard.

Step 1   Click **VPN** in the Wizard Mode category bar. The VPN wizard main window opens.

Step 2   Select one of the three VPN wizard radio buttons:

- **Create a Site-to-Site VPN with Pre-Shared Key**—Creates a router-to-router VPN using pre-shared keys.

- **Create an Easy VPN remote client**—Configures the router's VPN client for connection to a VPN server (Easy VPN Remote phase II support only).

- **Create a Secure GRE tunnel (IPSec over GRE)**—Configures a protected GRE tunnel between this router and a peer system.

Step 3   Click **Launch**. In this example, we have chosen to create a site-to-site VPN with pre-shared keys. The Site-to-Site VPN with Pre-Shared Key window opens.

VPN Wizard—Site-to-Site with Pre-Shared Key
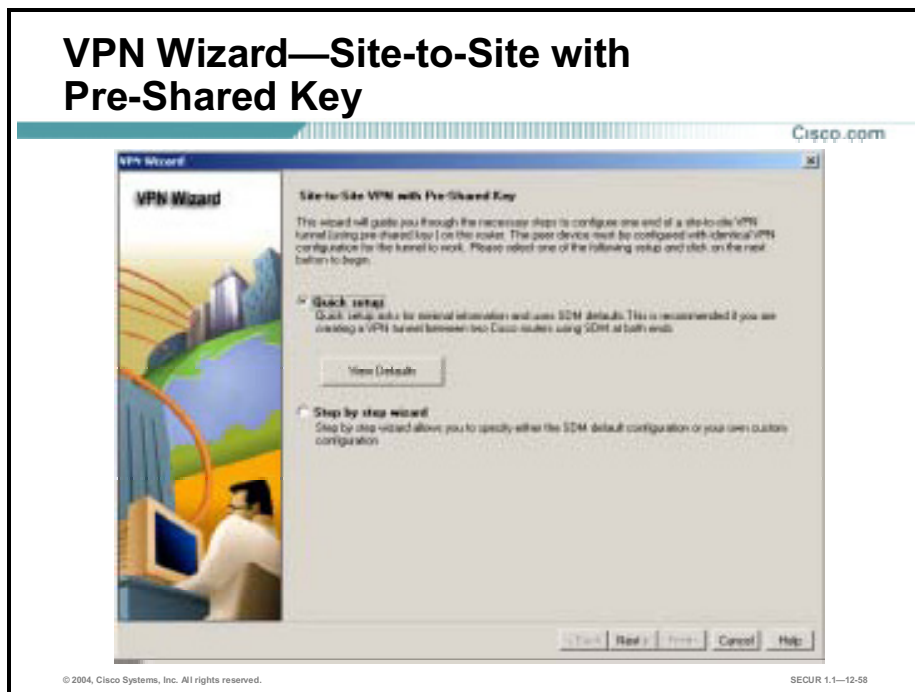
Step 4   Select one of the two wizard option radio buttons:

- **Quick setup**—Uses SDM generated defaults:
    — Default IKE policy for authentication.
    — Default transform set to control the encryption of data.
    — Default IPSec rule to encrypt all traffic between the router and the remote device.
    — Click **View Defaults** to view the default settings.
- **Step by step wizard**—Allows you to create custom policies.

Note   Quick setup is best used when both the local and remote routers are Cisco routers using SDM.

Step 5   Click **Next**. The VPN Connection Information window opens.

VPN Wizard—VPN Connection Configuration

SECUR 1.1—12-59

Step 6 Select the router interface used for the VPN connection from the list box.

Step 7 Enter the remote VPN router IP address or host name in the **Peer Identity** field.

Step 8 Enter a pre-shared key in the **Pre-Shared Key** field. Both sides must agree on the Pre-shared key that is used to authenticate each other.

Note The key can be up to 128 characters with any combination of letters and numbers, but question marks (?) and spaces are not allowed. The key is displayed in asterisks to protect its secrecy.

Step 9 Re-enter the pre-shared key in the **Reenter Key** field.

Step 10 Select the source (inside) interface in the Protect all IP traffic from interface list box.

Step 11 Select one of the two destination radio buttons:

- **Specific subnet**—Select this radio button to specify a remote subnet as the destination to enter the VPN tunnel.

    — Enter the IP address in the **IP Address** field.

    — Enter a network mask in the **Network Mask** field, or select a pre-defined mask using the list box.

- **All destinations**—Permits all destinations to enter the VPN tunnel.

Note SDM creates an access list that permits IP traffic between the source and destination as specified in this record.

Step 12 Click **Next**. The Summary of the configuration window opens.

VPN Wizard—Summary of the Configuration

Cisco.com

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

SECUR 1.1—12-60
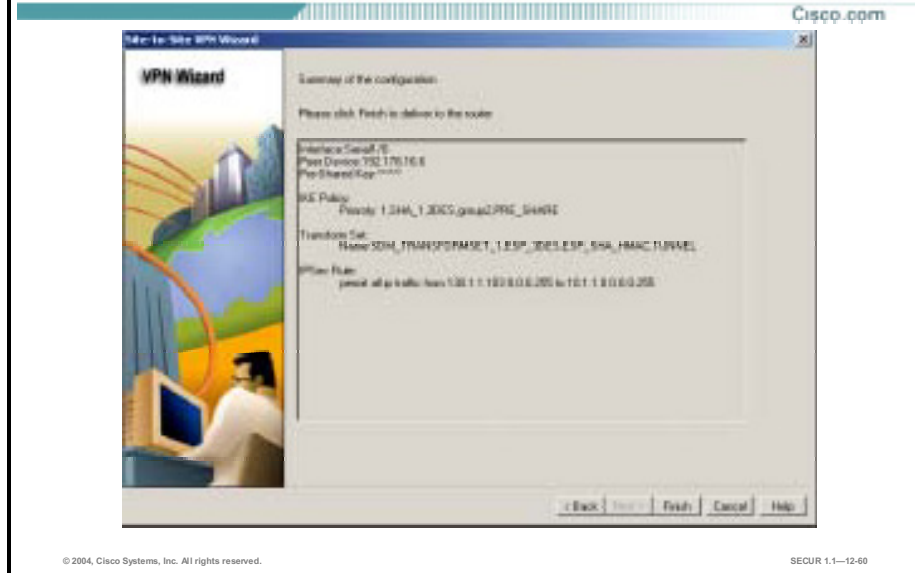
Step 13 Click **Finish** to deliver the configuration to the router. The SDM Commands Delivery Status window opens.

VPN Wizard—Configuration Completion

SECUR 1.1—12-61
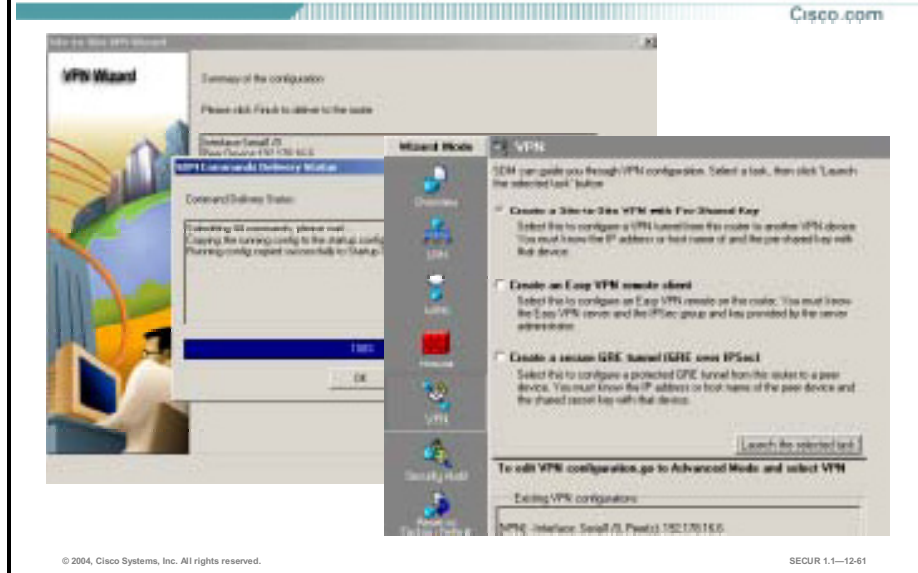
Step 14 Click **OK** when the OK button goes active. The VPN wizard main window updates and lists the new VPN configuration in the Existing VPN configurations field.

Advanced Mode—Viewing or Changing VPN Settings

SECUR 1.1—12-62

Use the SDM Advanced Mode to view, add, or edit VPN rules, policies, and global settings.

You can also view the status of you interface by clicking **Interfaces and Connections**. If you highlight your VPN interface, it will provide a summary of the entire configuration including the IPSec policy number, assigned access list, and inspection rules.

Using SDM to Perform Security Audits

This topic explains how to use SDM to perform router security audits.

Security Audit—Overview

Cisco.com

- **Compares router configuration against a predefined checklist of best practices (ICSA, TAC approved).**
- **Examples of the audit include (but are not limited to) the following:**
  - **Shut down unneeded servers on the router (BOOTP, finger, tcp/udp small-servers).**
  - **Shut down unneeded services on the router (CDP, ip source-route, ip classless.**
  - **Apply firewall to outside interfaces.**
  - **Disable SNMP or enable with hard-to-guess community strings.**
  - **Shut down unused interfaces, no ip proxy-arp.**
  - **Force passwords for console and vty lines.**
  - **Force an enable secret password.**
  - **Enforce the use of access lists.**

SECUR 1.1—12-64

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

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 Simple Network Management Protocol (SNMP) or enables it with hard-to-guess community strings
- Shuts down unused interfaces using **no ip proxy-arp**
- Forces passwords for the router console and vty lines
- Forces an enable secret password
- Enforces the use of ACLs

Security Audit—Main Window
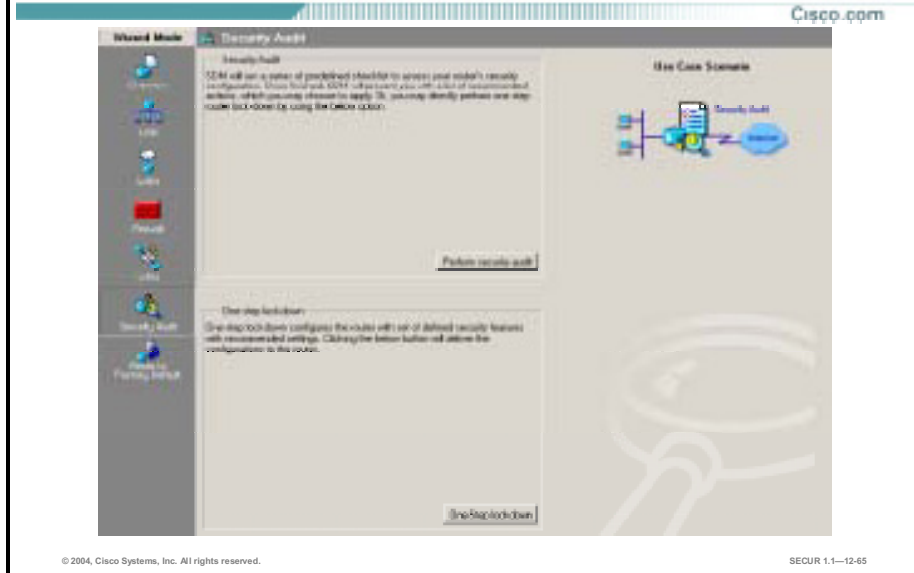
Security Audit contains two modes:

- Security Audit—Examines router configuration, then displays the Report Card screen, which shows a list of possible security problems. You can pick and choose which vulnerability you would like to lock down.

- One-step lockdown—Initiates the automatic lockdown using recommended settings.

Step 1   Click **Security Audit** from the Wizard Mode category bar.

Step 2   Select one of the two available security audit wizard radio buttons. In the example shown in the slide, the **Perform security audit** radio button is selected. The Inside and Outside Interfaces dialog box opens.

Step 3   Select the inside and outside interfaces from the list.

Step 4   Click **Next**. The Security Audit window opens.

Security Audit—Wizard

SECUR 1.1—12-66
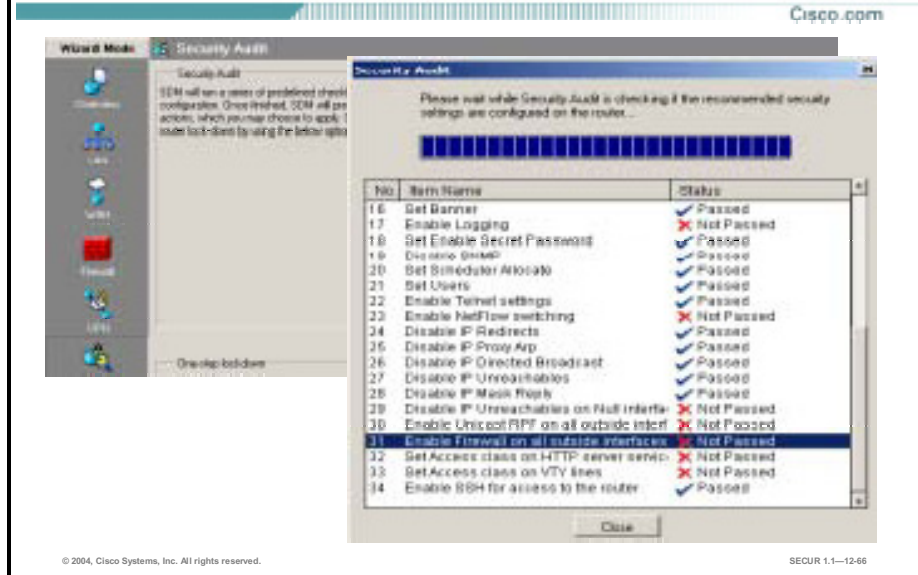
The Security Audit wizard tests your router configuration to determine if any security vulnerabilities exist. Vulnerable items are marked in red.

Step 5   Click **Close**. The Security Audit Report Card window opens.

Security Audit—Fix Security Problems

Cisco.com

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—12-67
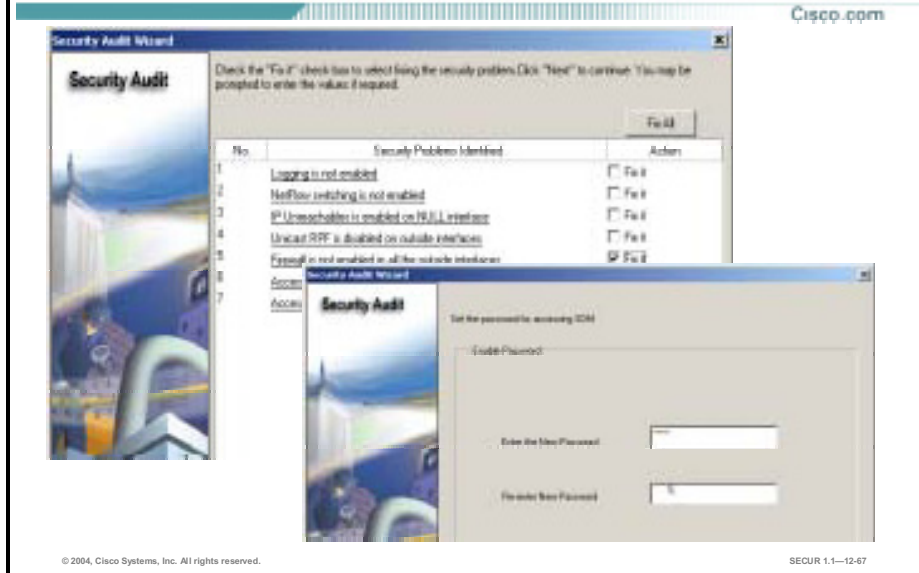
Step 6 Select the **Fix it** check boxes next to any problems that you want SDM to fix.

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.

Step 7 Click **Next**. Additional screens may appear requiring your input such as enter a password.

Note	You can also click **Fix All** to automatically secure all vulnerabilities found with a "best practice" solution.

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 too. The Security Audit Summary window opens.

Security Audit—Summary
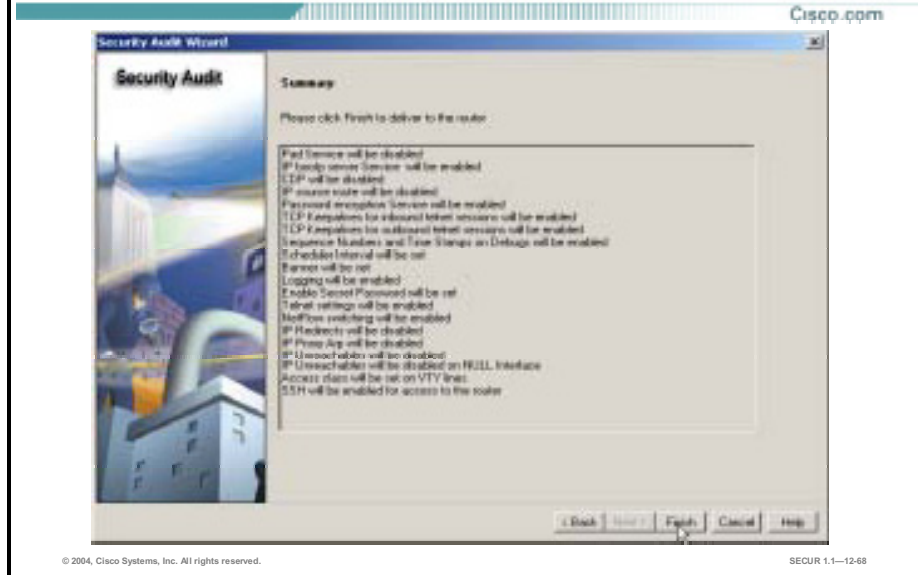
SECUR 1.1—12-68

Step 8 Review the changes that will be delivered to the router.

Step 9 Click **Finish**. The changes are sent to the router.

Security Audit—One-Step Lockdown Wizard

This wizard 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 any problems found.

Refer to the SDM online help for a list of security features and a description of them.

| Note | You can use the **Advanced Mode-System Properties** function to undo specific settings. |

Using the Factory Reset Wizard

This topic explains how to use the SDM router factory reset wizard.
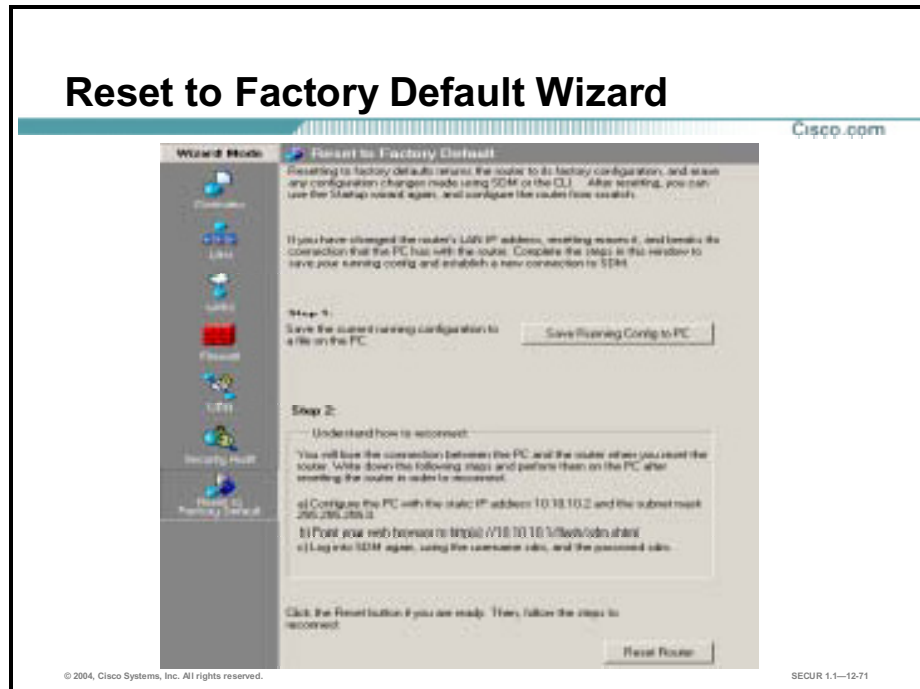
You can reset your Cisco router to factory defaults using the SDM Reset to Factory Default wizard.

Access the wizard by selecting **Reset to Factory Default** from the Wizard Mode category bar. The Reset to Factory Default window opens.

This wizard contains two steps:

■ Save Running Config to PC—This function copies the router running configuration to the SDM host PC. SDM verifies that step is completed before allowing you to continue with the reset (or erase) procedure.

■ Reset Router—Performs the actual reset procedure.

Step 1 Click **Save Running Config to PC**. SDM prompts you to select a directory on your local PC where it will store the configuration file.

Note Before you proceed with step 2, understand how to reconnect to your router following the reset procedure. The wizard window explains the process for reconnecting to your router. Make sure you read and understand this procedure before continuing with step 2.

Step 2 Click **Reset Router**. You will lose your connection to SDM. Wait a couple of minutes while the router resets and then reloads with the default settings.

Now you may reconnect SDM to the router using the router's lowest LAN interface.

Using SDM Advanced and Monitor Modes

This topic explains how to use the SDM advanced and monitor modes.

SDM advanced mode is designed for more experienced users who prefer to jump to desired configuration functions, rather than using the wizards.

Advanced Mode—Interfaces and Connections

SECUR 1.1—12-74

The upper portion of the screen shows logical and physical interfaces present in the router. It also shows the current status of the interfaces. You can toggle the interface states, by administratively disabling and re-enabling them.

The lower portion of the screen shows details about the selected interface (NAT, ACL, crypto associations, and so on).

Advanced Mode—Rules

The Rules window is where you define how the router should behave when it encounters a particular kind of traffic. SDM provides default rules that are used in the wizards. You can create custom rules which can also be used in the wizards or in advanced mode configurations.

The different types of rules include the following:

■ Access Rules—Specify the traffic that can enter and leave the network. These rules include both standard and extended ACLs.

■ NAT Rules—Determine how private IP addresses are translated into valid Internet IP addresses.

■ IPSec Rules—Determine which traffic will be encrypted on secure connections.

■ Unsupported Rules—Rules which were not created using SDM and so, are not supported by SDM. These rules are read only, and cannot be modified using SDM. You must use CLI to edit these rules directly.

■ Externally-Defined Rules—Rules which were not created using SDM, but are supported by SDM. These rules cannot be assigned to a router interface using SDM. You must use CLI to assign these rules to router interfaces.

■ SDM Default Rules—These rules are predefined in the SDM software and can be applied in both Wizard Mode and Advanced Mode.

■ Inspection rules—These are CBAC firewall inspection rules.

Use the online help to learn how to use SDM to configure these rules. It is assumed that you have a basic understanding of these common rules before altering them in the advanced mode.

Advanced Mode—Routing

SECUR 1.1—12-76

Use the Routing window to configure static routes and dynamic routing (including RIP, OSPF, and EIGRP routes). Check www.cisco.com/go/sdm for the latest information regarding supported protocols.

Advanced Mode—NAT

The Network Address Translation Rules window lets you view NAT rules, and lets you designate interfaces as inside or outside, view address pools, and set translation timeouts.

The NAT main page shows a list of all the translation rules. You can create, modify, and delete NAT rules using this page. Rules that not supported by SDM are marked as read-only with a special icon to as shown in the figure. These rules were created using CLI.

Click **Designate NAT Interfaces** to designate the inside and outside interfaces which you want to use for NAT translations.

Advanced Mode—System Properties

SECUR 1.1—12-78
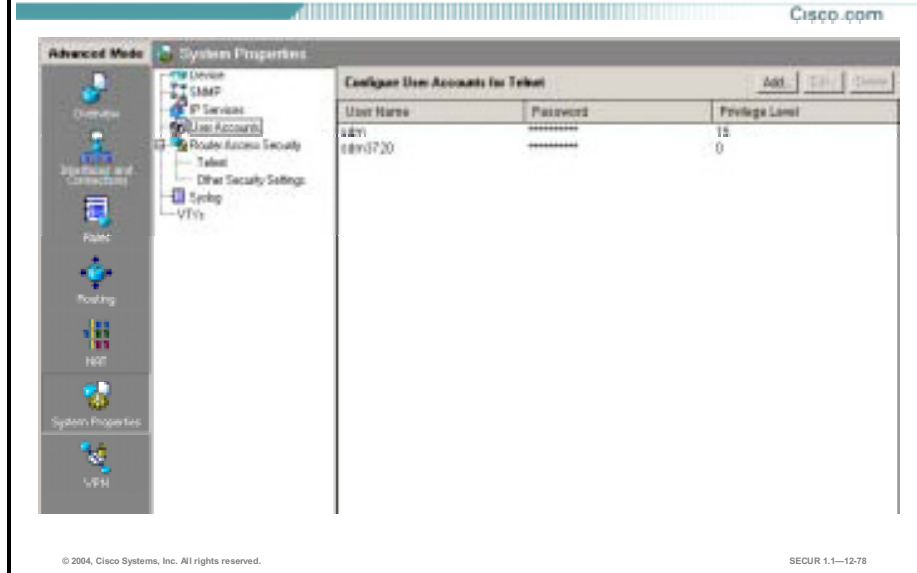
System properties let you define the overall attributes of the router.

Here you assign the router name, domain name, password, SNMP status, Domain Name System (DNS) server address, user accounts, router log attributes, VTY settings, SSH settings, and other router access security settings.

SDM 1.0.1 adds the ability to configure the router's date and time. You can use SDM to directly change the router's date and time, or you can use SDM to synchronize the router's date and time settings with those of the PC.

SDM .0.1 also adds a management access utility that allows you to create management policies. These policies can specify the networks or hosts from which SDM can run and can specify the protocols that can be used to run SDM and manage the router in other ways. For example, you can specify that a specific host may connect to the router via the FastEthernet 0/0 interface and be allowed to use SDM using secure protocols only (SSH, HTTPS, and RCP).

Advanced Mode—VPN

Example—Editing an IKE Policy:

1. **Expand the VPN tab (+).**
2. **Select the** IKE Policies **tab.**
3. **Select the policy from the list.**
4. **Click** Edit **in the upper right corner.**
5. **The Edit window opens, allowing you to make modifications.**

SECUR 1.1—12-79

The VPN window is used to configure IPSec policies, Internet Key Exchange (IKE) policies, and assign global settings such as IKE keepalives and IPSec Security Association (SA) lifetime settings.

The figure shows an example of how to edit an IKE Policy:

Step 1 First expand the VPN tab (press the + key).

Step 2 Select the **IKE Policies** tab.

Step 3 Select the policy you want to edit from the list.

Step 4 Click the **Edit** button. The Edit IKE Policy window opens.

Step 5 Make modifications to the policy.

Step 6 Click **OK**.

Note   Whenever you make a change in Advanced mode, the configuration changes are not made to the router until you click the **Deliver** button. Only after the delivery function is complete will the configuration changes reside in the router running configuration.

Monitor Mode
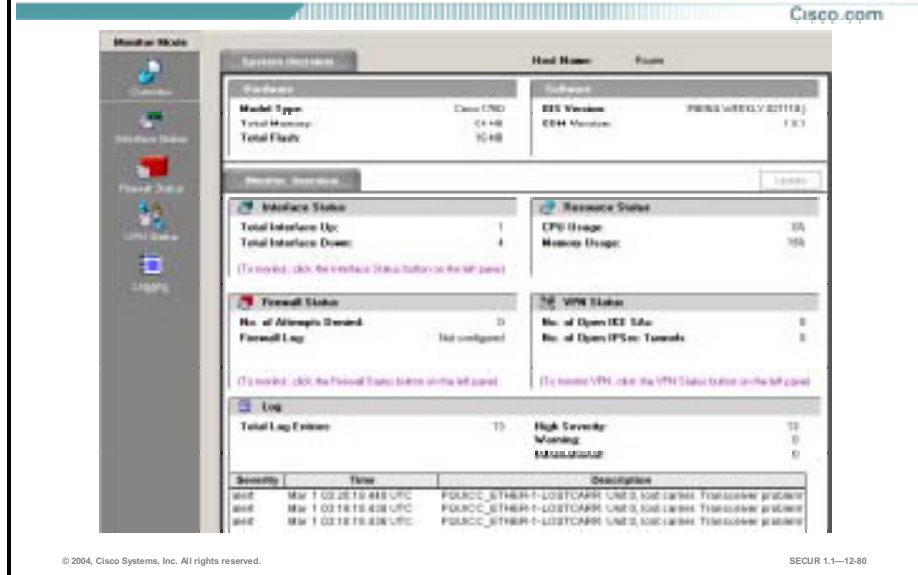
Monitor mode lets you view information about your router, the router interfaces, the firewall, and any active VPN connections. You can also view any messages in the router event log.

The monitor function includes the following elements:

■ Overview—Displays the router status including a list of the error log entries.

■ Interface Status—Used to select the interface to monitor and the conditions (for example, packets and errors, in or out) to view.

■ Firewall Status—Displays a log showing the number of entry attempts that were denied by the firewall.

■ VPN Status—Displays statistics about active VPN connections on the router.

■ Logging—Displays an event log categorized by severity level.

Summary

This topic summarizes what you have learned in this lesson.

Summary

- **The Cisco SDM is a useful tool for configuring Cisco access routers.**
- **SDM contains several easy-to-use wizards for efficient configuration of Cisco access routers.**
- **SDM allows you to customize Cisco access router configurations using advanced features.**

SECUR 1.1—12-82

Lab Exercise—Using Security Device Manager

In this lab exercise you will use SDM to configure your perimeter router.

Objectives

In this lab exercise, you will complete the following tasks:

- Complete the lab exercise setup.
- Copy the SDM files to router Flash memory.
- Configure the router to support SDM.
- Launch SDM.
- Configure a basic firewall.
- Create a site-to-site VPN using pre-shared keys.
- Reset a router interface.
- Add a rule to an ACL.
- Create a banner.
- Create a new IKE policy.
- Perform a security audit.
- Perform an automatic lockdown.

Visual Objective

The following figure displays the configuration you will complete in this lab exercise.

Lab Visual Objective

Task 1—Complete the Lab Exercise Setup

Complete the following steps to setup your training pod equipment:

Step 1 Ensure that your student PC is powered on and Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log into the student PC.

Step 2 Configure your student PC for IP address **10.0.P.12** with a default gateway of **10.0.P.2** (where P = pod number).

Step 3 Reload your perimeter router using the default lab configuration.

Step 4 Ensure you can ping the perimeter router from your student PC.

Step 5 Ensure that your perimeter router can ping the super server host at 172.26.26.50. The super server host will be used as the TFTP server for this lab exercise.

Task 2—Copy the SDM Files to Router Flash Memory

Complete the following steps to copy the SDM files from the TFTP server to your perimeter router flash memory (where P = pod number):

Step 1 Telnet to the remote terminal server (RTS) and connect to the console port of your perimeter router. Your instructor will explain how to do this.

Step 2 Enter enable mode using a password of **cisco**:

```
RP> enable
Password: cisco
```

```
RP#
```

Step 3 Check the contents of flash memory:

```
RP# show flash
```

Note	Make sure that there are no *sdm.tar* or *sdm.shtml* files in flash memory. If these files exist, delete them using the **delete** *filename* command, and then permanently remove them using the **squeeze flash** command.

Step 4 Copy the sdm.tar file to the router flash using TFTP:

Caution	When prompted, do NOT erase the flash memory.

```
RP# copy tftp://172.26.26.50/sdm.tar flash:
RP#
```

Step 5 Copy the sdm.shtml file to the router flash using TFTP:

Caution	When prompted, do *not* erase the Flash memory.

```
RP# copy tftp://172.26.26.50/sdm.shtml flash:
RP#
```

Task 3—Configure the Router to Support SDM

Complete the following steps to configure your perimeter router to support SDM (where P = pod number):

Step 1 Enter global configuration mode using the **configure terminal** command:

```
RP# conf t
RP(config)#
```

Step 2 Enable the Cisco Web browser user interface using the **ip http server** command:

```
RP(config)# ip http server
RP(config)#
```

Step 3 Enable the Cisco Web secure browser user interface using the **ip http secure-server** command:

```
RP(config)# ip http secure-server
RP(config)#
```

Step 4 Enable local authentication for Cisco Web browser user interface connections using the **ip http authentication local** command:

```
RP(config)# ip http authentication local
RP(config)#
```

Step 5 Create a local privilege level 15 user account for SDM Cisco Web browser user interface login authentication:

```
RP(config)# username sdm privilege 15 password 0 sdm
RP(config)#
```

Step 6   Enter VTY line configuration mode using the line vty command:

```
RP(config)# line vty 0 4
RP(config-line)#
```

Step 7   Configure the VTY privilege level for level 15 using the privilege level command:

```
RP(config-line)# privilege level 15
RP(config-line)#
```

Step 8   Configure VTY login for local authentication using the login local command:

```
RP(config-line)# login local
RP(config-line)#
```

Step 9   Configure VTY to allow both Telnet and SSH connections using the transport input command:

```
RP(config-line)# transport input telnet ssh
RP(config-line)# end
```

Step 10 Copy the router running configuration to the startup configuration.

```
RP# copy run start
RP#
```

Task 4—Launch SDM

SDM is stored in the router's Flash memory. It is launched by executing an HTML file, which then loads a signed SDM Java file. Complete the following steps to launch SDM:

Step 1   Launch Internet Explorer on your student PC.

Step 2   Enter the following URL in the browser address field (where P = pod number):

https://10.0.P.2/flash/sdm.shtml

Note	If a security alert window appears, click **Yes** to continue.

Step 3   Enter the correct user name and password in the Enter Network Password window:

```
User Name: sdm
Password: sdm
```

Step 4   Click **Yes** at the Security Warning window. The SDM window appears and the SDM loads the current configuration from the router.

Task 5—Configure a Basic Firewall

Complete the following steps to configure a basic firewall on your perimeter router:

Step 1   Access the SDM Wizard mode.

Step 2   Select **Firewall** from the category bar.

Step 3 Select **Basic Firewall**.

Step 4 Click **Launch the selected task**.

Step 5 For the outside (untrusted) interface, select your **172.30.P.2** Ethernet interface (where P = pod number).

Step 6 For the inside (trusted) interface, select the **FE0/0** interface.

Step 7 Allow all denied firewall attempts to be logged.

Step 8 Verify your firewall configuration is correct (notice the access rules that will be applied to your firewall).

Step 9 Once you configuration summary is correct, click **Finish** to deliver the configuration to the router).

Once complete the new firewall appears on the Firewall wizard page under the Firewall Configurations overview box. Note the ACL rules that will be applied to the interfaces that make up your firewall.

Task 6—Configure a Site-to-Site VPN Using Pre-Shared Keys

Complete the following steps to configure a site-to-site VPN using pre-shared keys:

Step 1 Select **VPN** from the category bar.

Step 2 Select the appropriate VPN site-to-site option.

Step 3 Click **Launch the selected task**.

Note	At this point, you can choose one of two options. You may choose to use the Quick Setup mode or the Step by Step Wizard. For this lab exercise, you will use the Quick Setup mode.

Step 4 Click **View Defaults** to see how the quick setup will configure the VPN.

Step 5 Select **Quick Setup**.

Step 6 Select the outside **172.30.P.2** interface for the VPN connection (where P = pod number).

Step 7 Select a Peer Identity of **172.30.Q.2** (where Q = peer pod number).

Step 8 Enter a pre-shared key of **secretkey** to be used for authentication.

Step 9 Select the **10.0.P.2** interface to protect the source traffic (where P = pod number).

Step 10 Make the appropriate selection to protect all destination traffic.

Step 11 Verify the configuration summary. Note which IKE policy and Transform set will be deployed. If you made any mistakes, go back and fix them before proceeding.

Step 12 Click **Finish** to apply this change to the router configuration.

Step 13 If a SDM Warning window appears with a NAT conversion warning, click **Yes** so the VPN will work correctly.

Once complete the new VPN connection appears in the VPN wizard page.

Task 7—Reset a Router Interface

Complete the following steps to reset a router interface:

Step 1   Access the SDM Advanced Mode.

Step 2   Select **Interfaces and Connections** from the category bar.

Step 3   Select your **172.30.P.2** interface (where P = pod number). The interface should be in the up state.

Step 4   Click **Disable**. Note how the change state goes from up to down.

Step 5   Click **Enable**. The interface should come back up.

Task 8—Add a Rule to an ACL

Complete the following steps to add a rule to an existing ACL:

Step 1   Select **Access Rules** from the category bar.

Step 2   Select rule **101** from the list.

Step 3   Click **Edit**.

Step 4   Create a new permit statement using the following parameters:

- Permit
- Source: Any IP address
- Destination: 172.30.P.2
  (where P = pod number)
- Protocol: tcp
- Destination port: smtp

Step 5   The new statement appears at the bottom of the ACL. Move the new permit statement before the first deny statement in the ACL.

Task 9—Create a Banner

Complete the following steps to create a banner to discourage unauthorized access:

Step 1   Select **System Properties** from the category bar.

Step 2   Select **Banner**.

Step 3   Click **Edit**.

Step 4   Enter a banner to discourage unauthorized access.

Task 10—Create a New IKE Policy

Complete the following steps to add a new IKE policy for AES encryption:

Step 1   Select **VPN** from the category bar.

Step 2   Select **IKE**>**IKE Policies** from the VPN menu tree.

Step 3   Click **Add**.

Step 4   Add priority 2 with encryption **AES_256** using D-H **group 2**.

Task 11—Perform a Security Audit

Complete the following steps to perform a router security audit:

Step 1   Access the SDM Wizard Mode.

Step 2   Select **Security Audit** from the category bar.

Step 3   Take time to read the audit pages.

Step 4   Select all the interfaces you wish to audit. A report card opens.

Step 5   Close the report card window. Any items that did not pass the audit are marked as such in the list.

Step 6   Select the items you wish SDM to fix (do not fix them all).

Step 7   Allow SDM to fix a few of the items (do not fix them all).

Task 12—Perform an Automatic Lockdown

Complete the following steps to automatically lock down all security problems found on the router (as long as you left a few after running the security audit).

Step 1   Select **Security Audit** from the category bar.

Step 2   Click **One-Step Lockdown**.

Step 3   Return to the security audit to make sure all the vulnerabilities were automatically fixed.

Note   Some problems found during a security audit may require a manual entry to be locked down.

13

Using Router MC

Overview

This lesson describes how to configure Cisco router VPNs and Cisco IOS Firewalls using Management Center for VPN Routers (Router MC) 1.2.1. It includes the following topics:

- Objectives

- Router MC overview

- Installing Router MC

- Getting started

- Task 1—Creating an activity

- Task 2—Creating device groups

- Task 3—Importing devices

- Task 4—Defining VPN settings

- Task 5—Defining VPN policies

- Task 6—Approving activities

- Task 7—Creating and deploying jobs

- Configuring general Cisco IOS Firewall settings

- Building access rules

- Using building blocks

- Using upload

- Summary

- Lab exercise

Objectives

This topic lists the lesson objectives.

Objectives

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

- Define key features and concepts of the Router MC.
- Install the Router MC.
- Import and manage router policies.
- Configure Cisco IOS VPN policies.
- Deploy Cisco IOS VPN policies.
- Configure Cisco IOS Firewall policies.
- Deploy Cisco IOS Firewall policies.

SECUR 1.1—13-3

Router MC Overview

This topic provides an overview of Router MC 1.2.1.
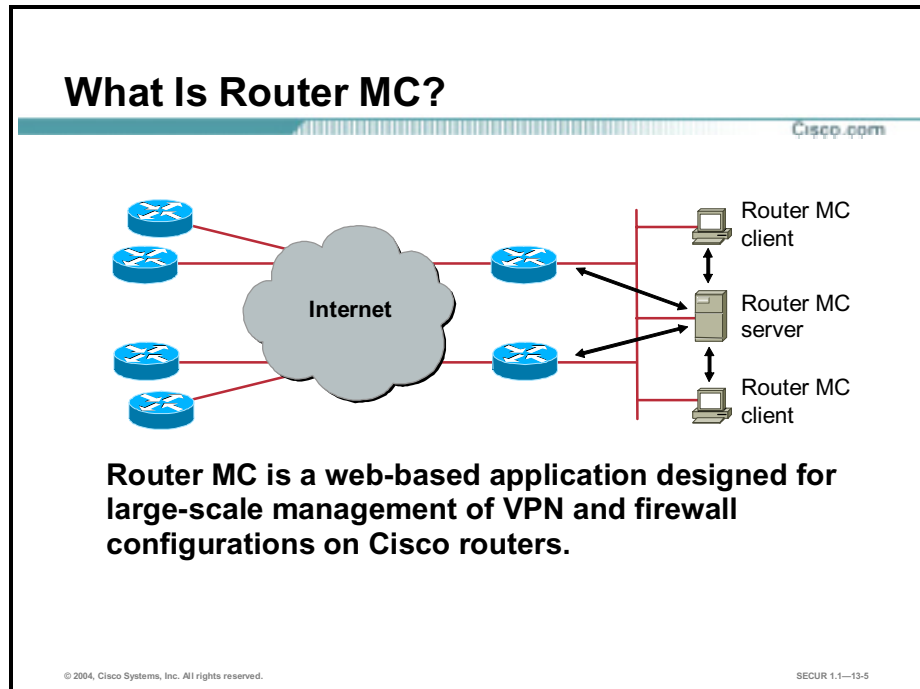
Router MC is a web-based application designed for large-scale management of virtual private network (VPN) and firewall configurations on Cisco routers. Router MC 1.2.1 provides the following features:

- Enables the setup and maintenance of VPN connections among multiple Cisco VPN routers, in a hub-and-spoke topology.

- Enables the provisioning of the critical connectivity, security, and performance parameters of a site-to-site VPN, quickly and easily.

- Allows for efficient migration from leased line connections to Internet or intranet-based VPN connections.

- Allows for the overlay of a VPN over a Frame Relay network for added security.

- Enables the configuration of Cisco IOS routers to function as firewalls.

Router MC is scalable to a large number of routers. Its hierarchical router grouping and policy inheritance features enable the configuration of multiple like routers simultaneously, instead of having to configure each router individually. Router MC enables deployment of VPN or firewall configurations to groups of routers or individual routers. It translates the configurations into command line interface (CLI) commands and either deploys them directly to the routers in the network, or to a configuration file for each router. It also uses reusable policy components that can be referenced across multiple connections.

Router MC Components

Cisco.com

CiscoWorks 2000 Management Server

| CSA MC | Firewall MC | IDS MC | Router MC |

Common Services

Web-based applications for configuring and managing multiple devices such as PIX Firewalls, routers, IDS Sensors, HIDS, and so on

Common set of management services that are shared by multiple network management application

SECUR 1.1—13-6
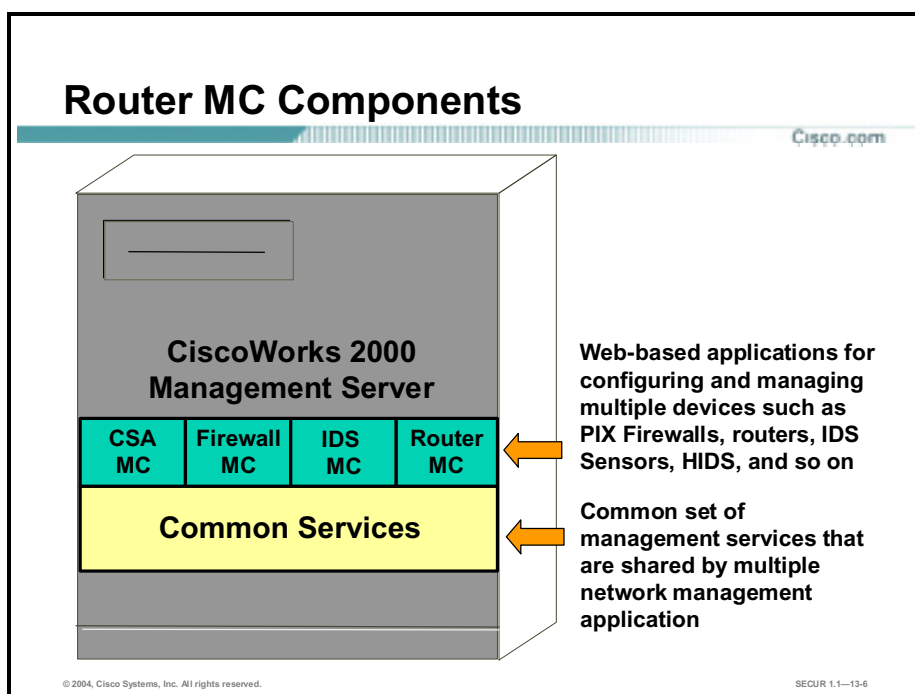
Router MC is integrated with CiscoWorks Common Services, which supplies core server-side components required by Router MC, such as Apache Web server, Secure Sockets Layer (SSL) libraries, Secure Shell (SSH) libraries, embedded SQL database, Tomcat servlet engine, the CiscoWorks desktop, and others.

Before installing Router MC 1.2.1, you must ensure that CiscoWorks Common Services 2.2 is installed and operational. CiscoWorks Common Services provides centralized management of certain functions for all the CiscoWorks VPN/Security Management Solution (VMS) products you have installed. These functions include:

- Backup and restore of data
- Integration with Access Control Server (ACS) or Common Management Framework (CMF) for user authentication and permissions
- Licensing
- Starting/stopping the database
- Logging of administration tasks

Note These functions are not performed from within the Router MC user interface, but are accessed using the CiscoWorks user interface.

Once you have installed CiscoWorks Common Services 2.2, you may install the Router MC 1.2.1 VMS module (or any of the other VMS modules as shown in the figure).

Router MC Communications
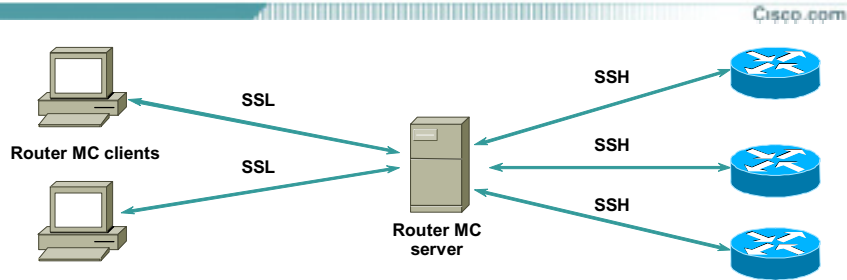
Router MC uses both SSL and SSH:
- SSL—Router MC client to Router MC server
- SSH—Router MC server to managed routers

SECUR 1.1—13-7

Router MC communications are handled by both SSL and SSH, as shown in the figure. This ensures that the information passed between the Router MC components is secure.

■ SSL—Processes all communications between the Router MC server and the Router MC clients.

■ SSH—Processes all communications between the Router MC server and the managed Cisco routers.

Note	You must configure SSH on your Cisco routers before attempting to manage them using the Router MC.

Supported Tunneling Technologies

Cisco.com

Router MC supports the following tunneling technologies:

• **IPSec**
• **IPSec with GRE**
• **IPSec with GRE over a Frame Relay network**
• **IPSec with GRE and DMVPN**

SECUR 1.1—13-8

Router MC supports the following tunneling technologies:

■ IPSec—IPSec is a framework of open standards that provides data confidentiality, data integrity, and data origin authentication between peers that are connected over unprotected networks such as the Internet.

■ IPSec with Generic Routing Encapsulation (GRE)—GRE is a tunneling protocol that can encapsulate a variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to routers at remote points over an IP internetwork.

■ IPSec with GRE over a frame relay network—This option provides all the advantages of using IPSec with GRE and the ability to create secure VPN tunnels over a frame relay network. Router MC supports a frame relay topology in which the hub acts only as a VPN endpoint, while each spoke acts as both a VPN endpoint and a frame relay endpoint. This means that there must be a router in the hub subnet before the VPN endpoint at the hub that acts as the second frame relay endpoint.

■ IPSec with GRE and DMVPN—Dynamic Multipoint VPN (DMVPN) combines GRE tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP). It allows for the management of devices with dynamically assigned IP addresses. It also enables direct spoke-to-spoke communication, without the need to go through the hub.
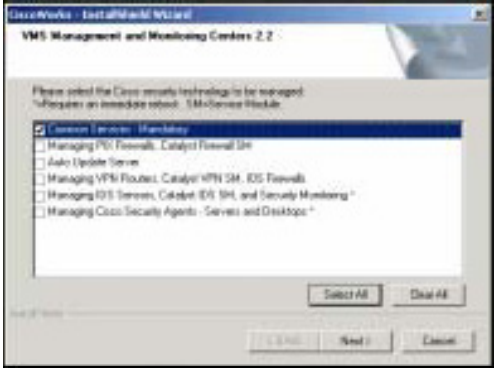
Installing Router MC

This topic explains how to install Router MC server and how to configure your Cisco routers to communicate with the Router MC server.

Installation of Router MC is a two step process as shown here:

Step 1   Install VMS Common Services 2.2 on the Windows 2000 Server system.

Step 2   Install Router MC 1.2.1.

Configure Routers for SSH

Router MC clients

SSL

SSL

Router MC server

SSH

SSH

SSH
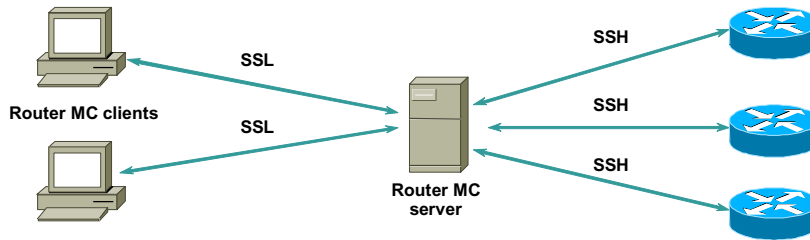
```
Router(config)# hostname Austin
Austin(config)# ip domain-name cisco.com
Austin(config)# crypto key generate rsa usage-keys
  modulus 1024
Austin(config)# ip ssh time-out 60
Austin(config)# ip ssh authentication 2
```

SECUR 1.1—13-11

Complete the following mandatory steps to configure your routers to support SSH:

Step 1   Configure a unique router hostname.

Step 2   Configure a domain name.

Step 3   Generate RSA usage keys.

Note   Ensure that your RSA keys use a modulus size of $\geq$ 1024.

Getting Started

This topic explains how to start using Router MC. It covers how to log in to CiscoWorks and which roles are responsible for delegation of tasks. When you are logged in to CiscoWorks, you can create accounts based upon the authorization roles that CiscoWorks uses and then launch the Router MC. Additionally, the Router MC interface is described to help familiarize you with the product.
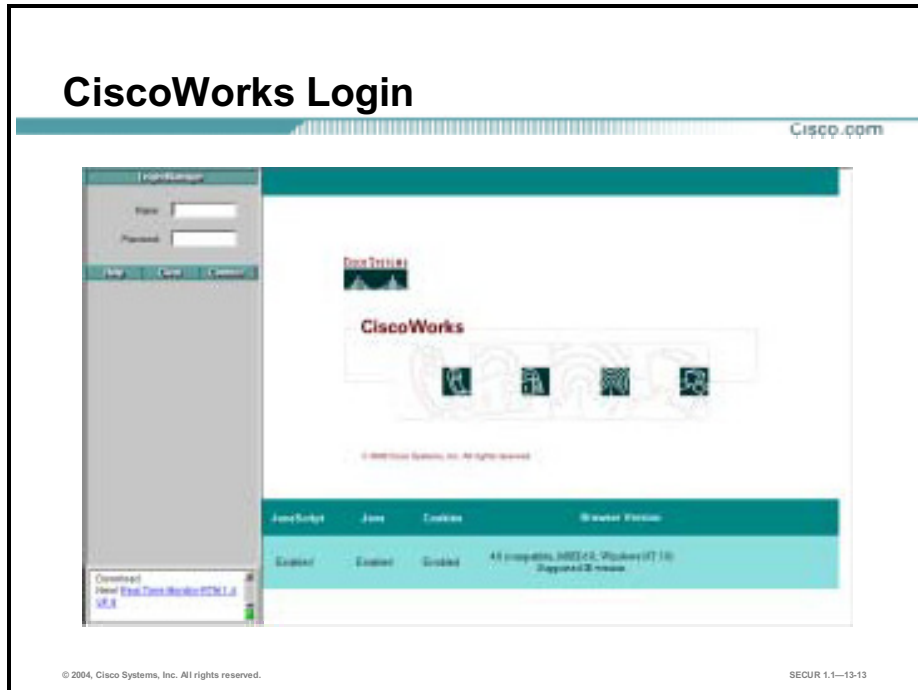
Complete the following steps to log in to CiscoWorks:

Step 1 Open a browser and point the browser to the IP address of the CiscoWorks server with a port number of 1741. If the CiscoWorks server is local, type the following address in the browser:

```
http://127.0.0.1:1741 <enter>
```

Step 2 If this is the first time that you are using CiscoWorks, enter the username **admin** and the password **admin**.

Launching Router MC
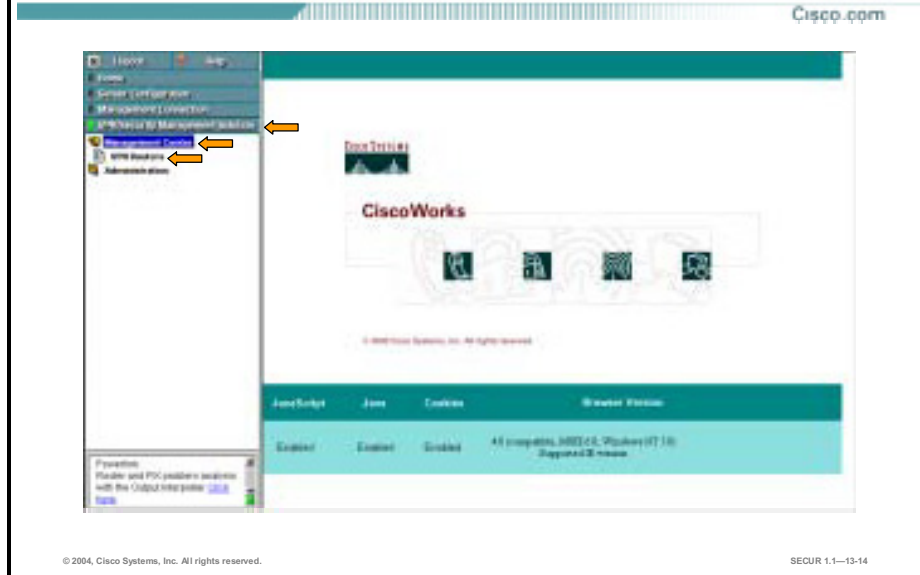
Complete the following steps to access the Router MC:

Step 1   Click VPN/Security Management Solution.

Step 2   Click **Management Center**.

Step 3   Click **VPN Routers**. The Router MC main window opens.

Router MC Main Window

SECUR 1.1—13-15
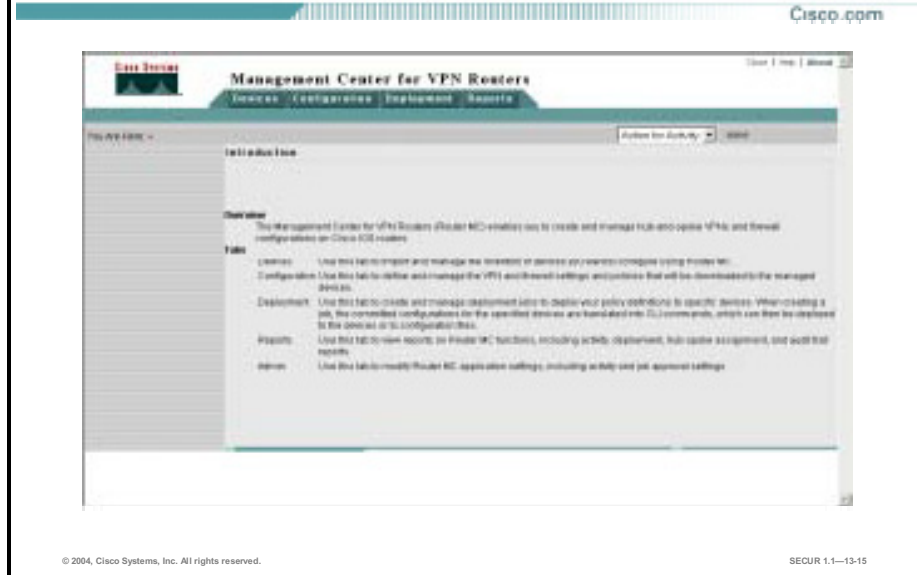
The Router MC main window is the first window you encounter when you enter the Router MC. The Router MC user interface contains four tabs as shown in the figure:

■ Devices—Use this tab to import and manage the inventory of routers you want to configure using Router MC.

■ Configuration—Use this tab to define and manage the VPN and firewall settings and policies that will be downloaded to the managed routers.

■ Deployment—Use this tab to create and manage deployment jobs to deploy your policy definitions to specific routers. When creating a job, the committed configurations for the specified routers are translated into CLI commands, which can then be deployed to the routers or to configuration file.

■ Reports—Use this tab to view reports on Router MC functions, including activity, deployment, hub-spoke assignment, and audit trail reports.

■ Admin—Use this tab to modify Router MC application settings, including activity and job approval settings.

Router MC Interface
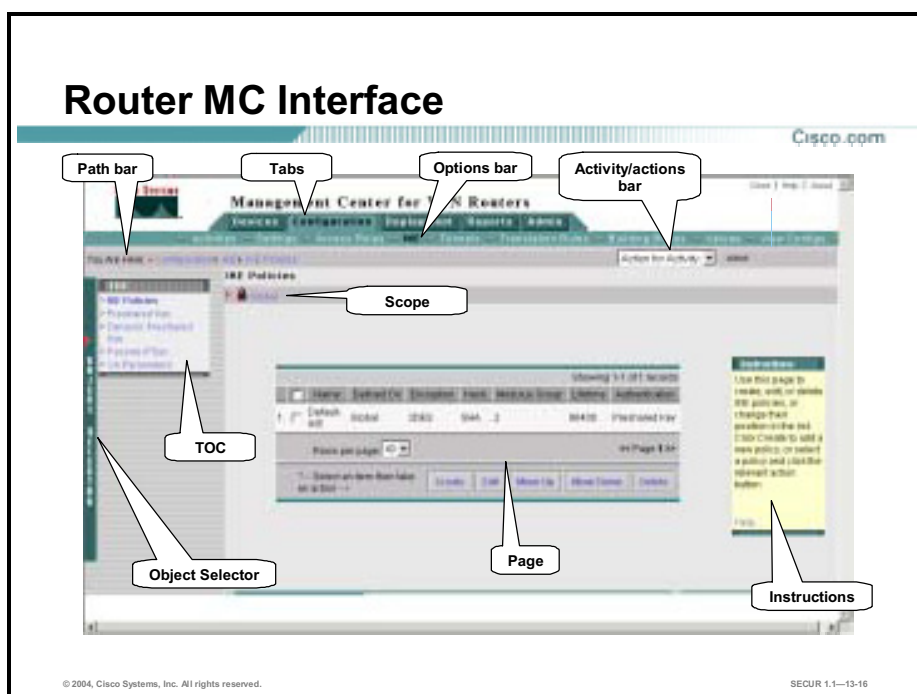
The Router MC user interface contains several key areas as shown in the figure:

- Path bar—Provides a context for the displayed page. Shows tab, option, and then current page.

- TOC—Table of contents. Displays available suboptions, if available.

- Options bar—Displays the options available for the tab.

- Tabs—Provides access to product functionality, by clicking a tab you are able to access its options.

- Activity and actions bar—Displays activity and action icons that change, depending upon what state the activity is in. Viewed from Devices and Configure tabs only. Options are:

    — Create—Creates a new activity.

    — Open—Opens a new or existing activity. A popup window opens from which you make your selection.

    — Close—Closes the activity shown by the activity bar.

    — Lock current object—Reserves selected objects for your activity so that they cannot be selected for any other activity.

    — Submit—Submits an activity for approval.

    — Approve—Commits the activity's configurations to the database.

    — Reject—Prevents the activity's configurations from being applied to the database.

    — Delete—Discards the activity shown by the activity bar.

    — View Details—Displays the details of the current changes.

- Instructions—Provides a brief overview of how to use the page.

- Page—Displays the area in which you perform application tasks.

- Scope—Displays the object selected in the Object Selector.

- Object Selector—Enables you to select groups and/or devices.

Devices Tab

SECUR 1.1—13-17
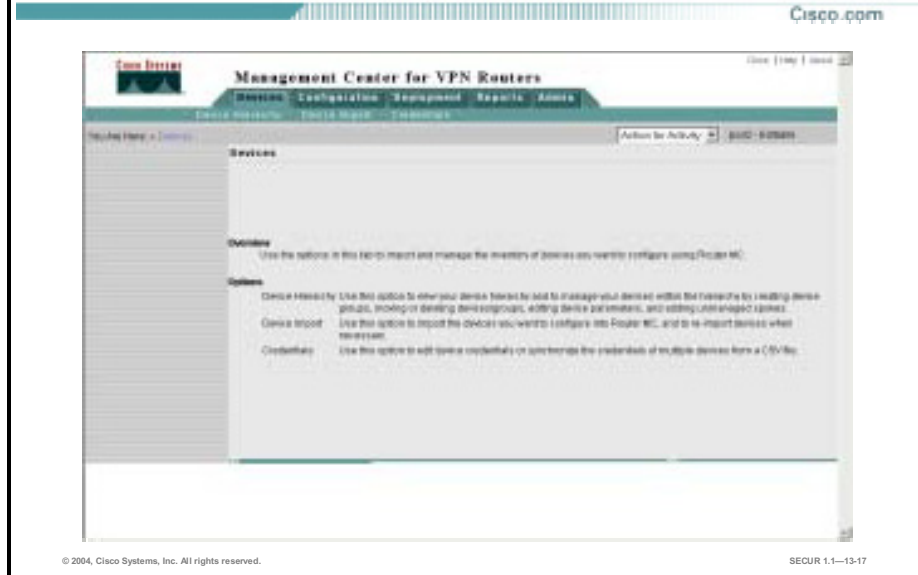
The Devices tab is used to import and manage the inventory of routers you want to configure using the Router MC.

- Device hierarchy—Use this option to view your device hierarchy and to manage your routers within the hierarchy by creating device groups, moving or deleting devices/groups, editing router parameters, and adding unmanaged spokes.

- Device import—Use this option to import the routers you want to configure into Router MC, and to re-import routers when necessary.

- Credentials—Use this option to edit router credentials or synchronize the credentials of multiple routers from a comma-separated value (CSV) file.

Note   Device credentials include the username, password, and enable password.

Configuration Tab

SECUR 1.1—13-18

Use the options in the Configuration tab to configure VPN and firewall settings and policies for deployment to your routers. You can configure settings and policies globally for all routers, for groups of routers, or for individual routers. Select your configuration context using the Object Selector along the left-hand side of the page.

- Activities—Use this option to create and manage activities. All router management and configuration tasks must be done within the context of an activity. Changes made in an activity are only committed to the database and visible to other users when the activity is approved. The name and status of an open activity is displayed at the top right of the context area, next to the action for Activity list box, which can also be used to manage activities.

- Settings—Use this option to define VPN and firewall settings for groups or individual routers. VPN settings include failover and routing and fragmentation settings, and interfaces on the hubs and spokes to be used for VPN connections. Firewall settings include Context-Based Access Control (CBAC) settings and access control list (ACL) ranges.

- Access Rules—Use this option to create access rules that define whether specific traffic flows on an interface should be permitted, denied, or inspected.

- IKE—Use this option to create and manage Internet Key Exchange (IKE) policies, configure pre-shared keys, and define Certificate Authority (CA) enrollment parameters.

- Tunnels—Use this option to create and manage tunnel policies that define what data to protect and how, and dynamic crypto policies for hubs.

- Translation Rules—Use this option to define address pools and traffic filters for Network Address Translation (NAT).

- Building Blocks—Use this option to create network groups, service groups, and transform sets, which are reusable named components that can be referenced by multiple policies.

- Upload—Use this option to transfer existing configurations on a source router to the currently selected object.

- View Configs—Use this option to view the proposed CLI commands that will be generated for a selected router based on the configuration changes made in the current activity.

Deployment Tab

SECUR 1.1—13-19

Deployment of VPN and firewall configurations is always done within the context of a deployment job. When you create a job, you specify the routers or router groups to which you want to deploy configurations. Router MC translates the committed policy configurations for each router into CLI commands. These CLI commands can be previewed and deployed either directly to the routers in the network or to output files in a specified directory.

The deployment tab offers you the following options:

- Jobs—Use this option to create and manage jobs. The name and status of an open job is displayed at the top right of the context area, next to the Action for Job list box, which can also be used to manage jobs.

- View Configs—Use this option to view the CLI commands generated for a specific router in the open job.

- Status—Displays the status of the routers targeted for deployment in the open job.

Reports Tab
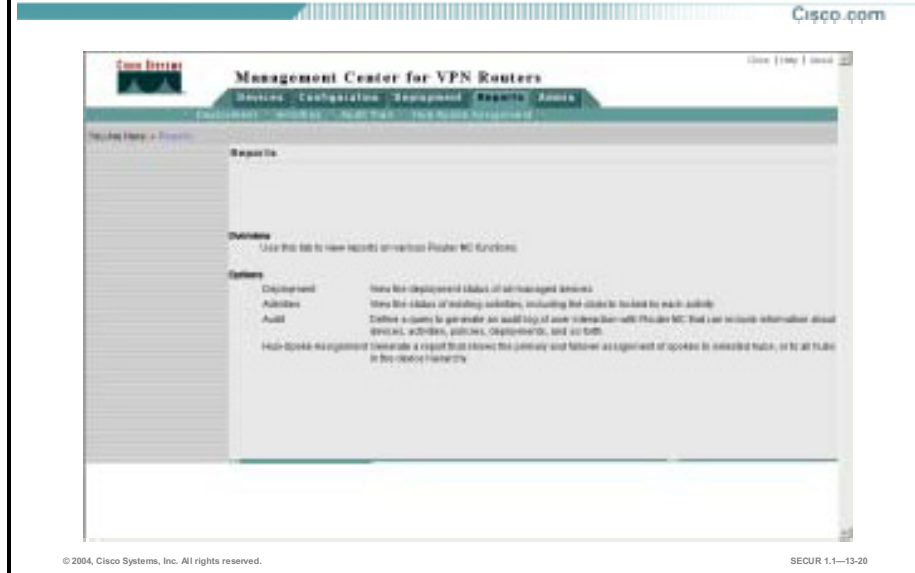
The Reports tab is used to view reports on various Router MC functions. This tab presents you with the following options:

- Deployment—Use this option to view the deployment status of all managed routers.

- Activities—Use this option to view the status of existing activities, including the objects locked by each activity.

Note The Router MC uses a locking model, in which the objects for which policies are being defined and all their descendants in the object hierarchy are locked to other users until the activity is approved or deleted. This is important in large networks where several people have the authority to configure routers. It prevents a potential situation where two or more people are making configuration changes to the same objects at the same time.

- Audit—Use this option to define a query to generate an audit log of user interaction with the Router MC that can include information about routers, activities, policies, deployments, and so forth.

- Hub-Spoke Assignment—Use this option to generate a report that shows the primary and failover assignment of spokes to selected hubs, or to all hubs in the device hierarchy.

Admin Tab

SECUR 1.1—13-21
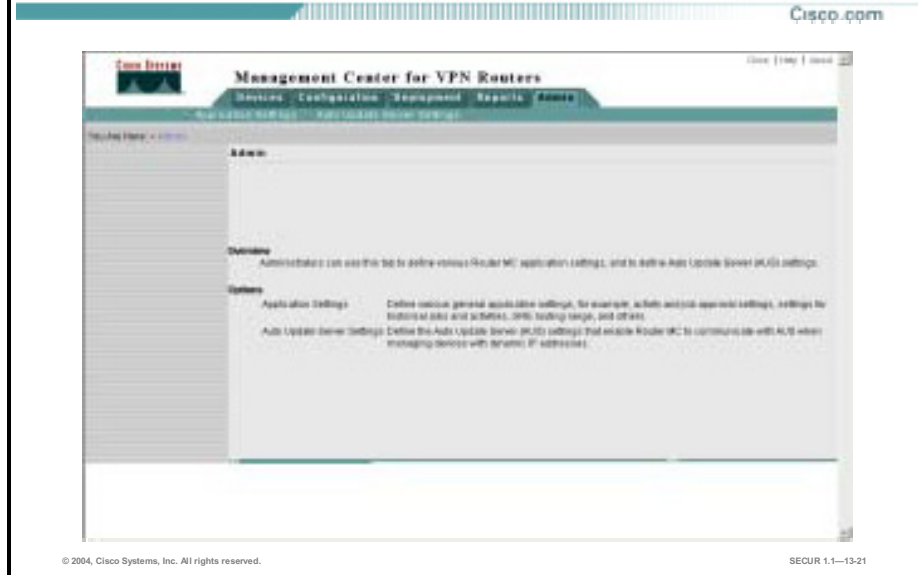
Administrators use the Admin tab to define various Router MC application settings, and to define Auto Update Server (AUS) settings.

This tab presents you with the following options:

- Application Settings—Use this option to define various general application settings, for example, activity and job approval settings, settings for historical jobs and activities, GRE routing range, and others.
- Auto Update Server Settings—Use this option to define the AUS settings that enable the Router MC to communicate with AUS when managing routers with dynamic IP addresses.

Most Router MC tasks are completed in the following basic order:

- **Task 1—Create an activity.**
- **Task 2—Create device groups.**
- **Task 3—Import devices.**
- **Task 4—Define VPN and/or firewall settings.**
- **Task 5—Define VPN policies and/or firewall ACLs.**
- **Task 6—Approve the activity.**
- **Task 7—Create and deploy a job.**

The Router MC has an inherent basic user work flow as shown in the figure. Most Router MC tasks are ordered as follows:

■ Task 1—Create an activity. All router management and VPN configuration must be done within the context of an activity. When you create an activity, you prepare a proposal to create or change VPN or firewall configurations on specific routers. This proposal must be approved before configurations can be deployed to the routers.

■ Task 2—Create device groups. Organize your routers in a hierarchy. When you create device groups, you divide your router inventory strategically to facilitate management and deployment. All routers within a device group can share common policies, which can be deployed to a set of routers at the same time, rather than individually. Device groups help you to keep a clear picture of the relationships between the routers in your network.

■ Task 3—Import devices. When you import devices, you bring their router information into the device inventory, allowing you to manage the routers using Router MC. You can import router information by having Router MC query the routers directly or by importing router information that is contained in a file.

■ Task 4—Define VPN and/or firewall settings. There are two ways to complete this task:

— If you are configuring a VPN, you must specify the inside interfaces and internal networks on the hub and spoke, and the VPN interface on the spokes and the hubs to which the spokes are assigned. You can also choose the method to be used for resiliency, either IKE keepalive or GRE. Additional VPN settings not covered in the basic user workflow include more advanced configurations for GRE, and packet fragmentation.

— If you are configuring firewall policies to be deployed to your routers, you must define the parameters required for implementing CBAC and for defining access rules, such as fragmentation, timeouts, half-open connections, logging, and ACL ranges.

- Task 5—Define VPN policies and/or firewall ACLs. There are two ways to complete this task:

  — For VPN policy configuration, you must define an IKE policy and a tunnel policy. The IKE policy defines a combination of security parameters to be used during IKE negotiation and authentication of peers. A tunnel policy defines the VPN connection from a spoke to its assigned hub. Tunnel policies that you define on the spoke are then implemented on the hub. You can select the authentication and encryption algorithms that will be used to secure the traffic.

  — To define your network security policy for firewall policy configuration, you must use ACLs. ACLs provide traffic filtering by enabling the implementation of ACLs and CBAC inspection rules on the routers' interfaces.

- Task 6—Approve the activity. Upon completing your VPN or firewall configurations, the activity must be approved before the configurations are committed to the database, and can be deployed.

- Task 7—Create and deploy a job. When you create a job, you specify the devices or device groups to which you want to deploy the configurations, and you choose whether to deploy directly to your routers or to files. CLI commands are generated according to your configurations and you can view them before deployment.

Task 1—Creating an Activity

This topic explains how to create an activity using the Router MC.

An activity is a temporary context within which you make VPN configuration changes to specific objects (global, device groups or devices). The activity must be approved before its configuration changes are committed to the Router MC database, at which point they are ready for deployment to the relevant devices or files.

Before you make any configuration changes, you must create a new activity or open an existing activity. An activity can be opened by only one person at a time but can be worked on by several people in sequence. This means that before the activity is approved, another user can open it and make further configuration changes to the selected objects. The objects being configured within the activity, and all their descendants in the hierarchy, are locked until the activity is approved or deleted. No other activity can have the same objects or any of their descendents selected for configuration. This ensures that there is no overlap between users, which might result in configuration discrepancies.
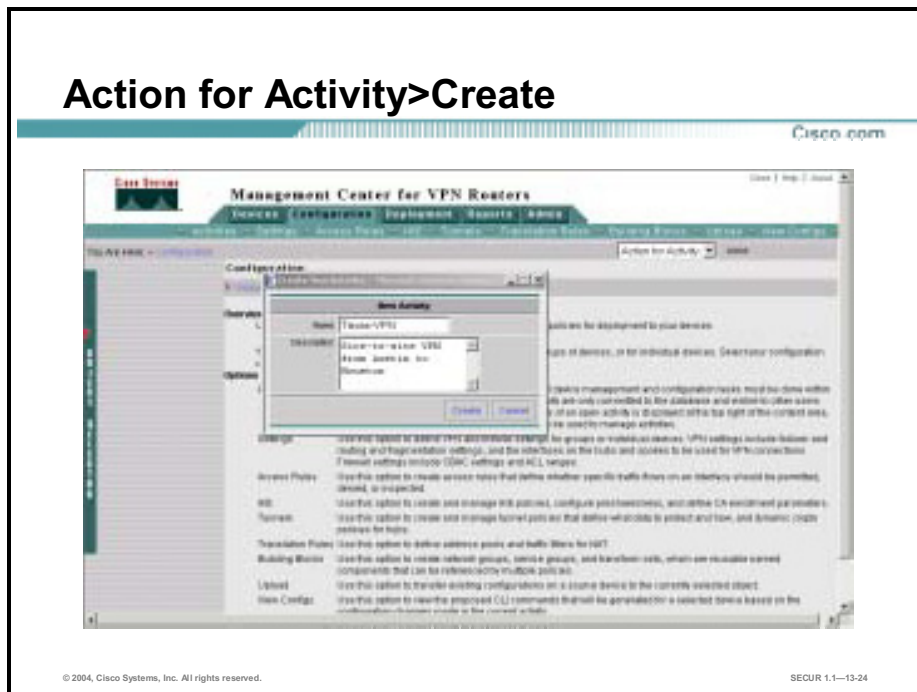
Before importing any routers or making any configuration changes, you must create an activity. Complete the following steps to create a new activity.

Step 1 Select the Configuration tab and select **Create** from the Action for Activity list box. The Create New Activity dialog box opens.

Step 2 Enter a unique name for this activity in the Name field.

Step 3 (Optional.) Enter a description for this activity in the Description field.

Step 4 Click **Create**. The new activity is created and the name appears next to the Action for Activity list box.

Updated Configuration Tab

SECUR 1.1—13-25

In this figure you can see the updated Configuration tab with the name of the activity listed next to the Action for Activity list box.

Notice that the new activity is marked as editable. When an activity is in this editable state, configuration changes can be made to the objects selected for the activity. An activity remains editable until it is approved (or submitted for approval) or deleted. An activity can be opened and closed and edited any number of times while it is in the editable state. The objects being configured in the activity are locked, meaning they cannot be configured within the context of another activity. The configuration changes can only be seen in the context of the current activity.

At this point, you could choose one of several configuration options as shown here:

■ Activities

■ Settings

■ Access Rules

■ IKE

■ Tunnels

■ Translation Rules

■ Building Blocks

■ Upload

■ View Configurations

Because this example involves building a VPN, you can ignore these options for now and move to task 2 and the Devices tab to create a new device group.

Task 2—Creating Device Groups

This topic explains how to create device groups using the Router MC.

Router MC provides a default two-level device hierarchy in which all routers are contained within a global group. Router MC allows you to create additional levels in the hierarchy by grouping your devices within the global group. Using device groups facilitates efficient management of a large number of devices by enabling you to define VPN or firewall policies on multiple devices simultaneously, rather than having to configure each device individually. Policy inheritance in the device hierarchy is implemented in a top-down fashion. The global group is the highest-level object.

- Policies defined on the global level are inherited by all devices in the device inventory.

- Policies defined on a device group are inherited by all the groups and devices contained within that group, and override the global configurations (if any) for those devices.

- Policies defined on an individual device apply to that device only, and override any policies inherited from higher level objects in the hierarchy.
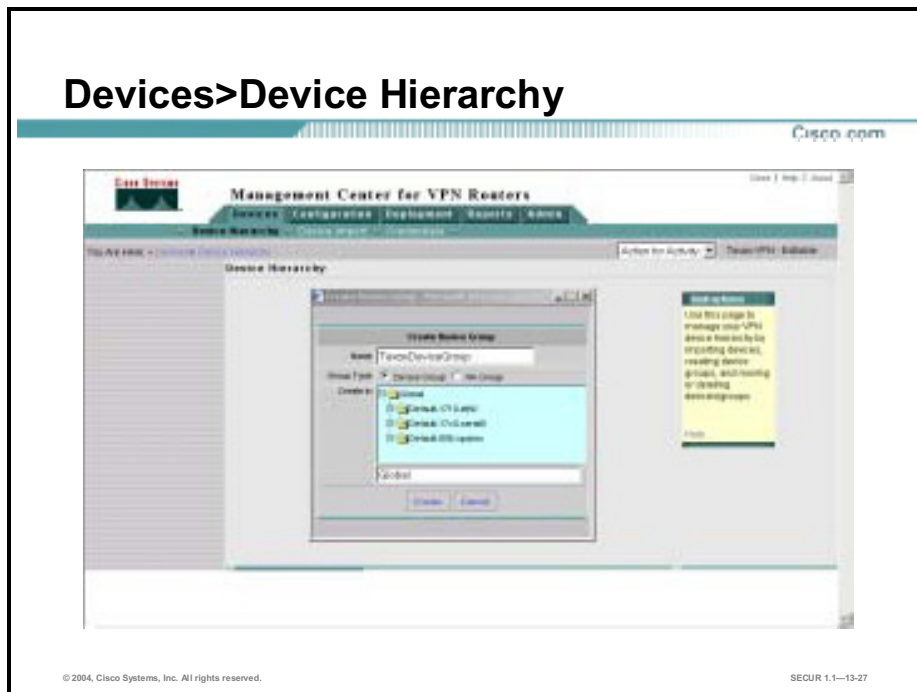
Grouping routers provides an easy and scalable mechanism for assigning common policies simultaneously to a set of routers, rather than doing so individually and in sequence. Device groups allow you to divide your network by any strategy you choose, including geographic locale, organizational function, corporate priority, or schedule of deployment.

Note	It is best to group your routers according to the policies that should apply to them. The primary benefits of grouping relate to managing policies across multiple similar routers simultaneously. A group that contains a combination of hubs and spokes will disperse its policies to those routers in ways that apply appropriately to them.

Complete the following steps to create a new device group:

Step 1   Select the **Devices** tab.

Step 2   Select **Device Hierarchy**. The Device Hierarchy page opens.

Step 3   Enter a unique name for your device group in the Name field.

Step 4   Select the type of group you want to create, either a standard device group or a High Availability (HA) group. In this example, a standard device group type is selected.

Note	An HA group consists of two or more hub routers that use Hot Standby Routing Protocol (HSRP) and Reverse Route Injection (RRI) to provide transparent, automatic router failover.

Step 5   Go to the Create in area and select the parent object in which the device group will be created. In our example, we chose to create the new device group as a child of the Global tree by clicking the **Global** folder or text.

Note	The Router MC contains three predefined device groups called Default-1710-eth0, Default-17x0-serial0, Default-806-spokes. These predefined device groups are based on the Cisco router models used most frequently in VPN environments and on those configurations most commonly used for those VPNs. Each configuration contains a specific IKE policy and two transform sets. Additionally, the inside interfaces and VPN interfaces are also predefined.

Step 6   Click **Create**. The Device Hierarchy page refreshes. The new device group appears within the Global folder along with the three predefined device groups.

View Device Hierarchy

SECUR 1.1—13-28

In a hub-and-spoke VPN topology, multiple remote routers (spokes) communicate securely with a central router (hub). A separate, secured tunnel extends between the centralized hub and each of the individual spokes.

Here you can see the new device group under the Global folder. You have several options available to you from within the **Devices>Device Hierarchy** page as shown in the figure.

■ Edit—Select a device folder (to select all devices in the group) or individual routers and click **Edit** to perform the following sub-tasks:

— Rename the device group (only when the device group is selected).

— Change router roles (hub or spoke).

— Change router Cisco IOS versions (list starts with Software Release 12.2)

■ Move—Click **Move** to move devices or groups from one position to another within the device hierarchy.

■ Delete—Select one or more routers or groups in the tree and click **Delete** to remove them from your hierarchy. If you delete a group, you will also delete all of its routers, subgroups, and associated policies unless you first move them elsewhere.

■ Add Unmanaged Spoke—Click this button to add an unmanaged spoke to your inventory. Unmanaged spokes are VPN routers in your inventory that are unavailable for direct Router MC configuration. Router MC uses the policy settings of an unmanaged spoke only to configure—by inference—its associated hub. You must use the CLI to configure unmanaged spokes.

■ Create Group—Click this button to add a new device group.

The Device Hierarchy page contains a small tab called All. This tab displays the entire device hierarchy found in the Router MC database.

Task 3—Importing Devices

This topic explains how to import device identity information using the Router MC.

Device import brings into Router MC a range of identifying information for the router, such as its domain name, its interfaces and sub interfaces, and the IP addresses of its interfaces and sub interfaces. Router MC imports devices either by querying the physical devices for information, or by reading device information from a file or multiple files in a specified directory on the server. Devices can be imported individually or in groups.

Note	The device import function is not the same as the configuration upload function. Configuration upload gathers information about the actual configuration of the router including policies such as transform sets, pre-shared keys, dynamic pre-shared keys, CA policies, routing policies, and IKE policies. You will learn more about the configuration upload function later in this lesson.
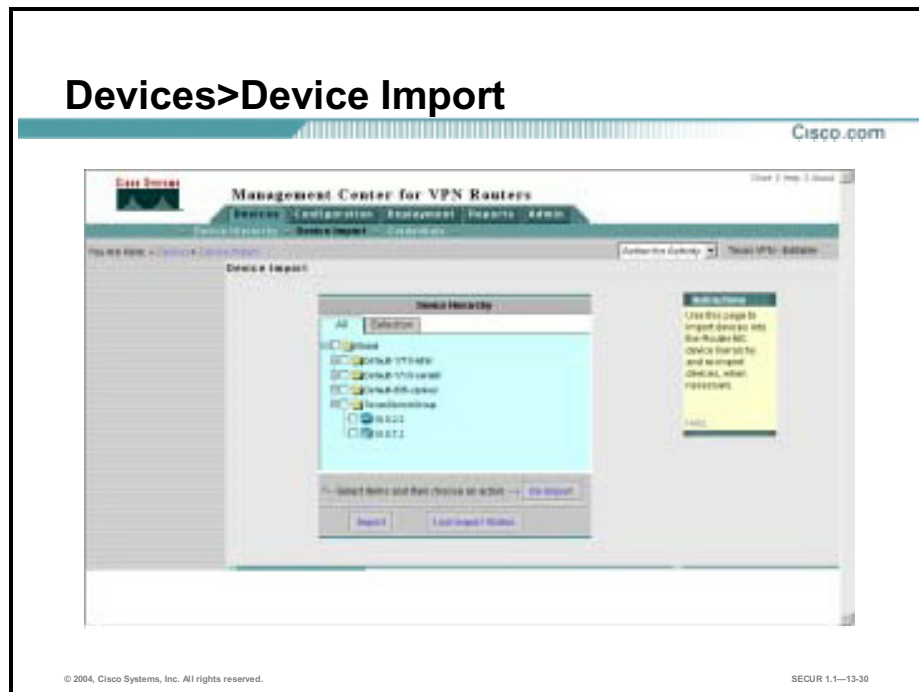
The Router MC device import feature allows you to update the Router MC device inventory database with information from the following sources:

■ Pre-existing router configuration files

■ Physical router configuration files

■ CSV files

You have several options available to you from within the **Devices>Device Import** page as shown in the figure.

- Import—Click this button to access the import wizard to import routers into Router MC.

- Last Import Status—Click this button to display the import status of the routers in the most recent import operation.

- Re-import—Click this button to reimport the selected router or device group. This is useful if router information has changed and you want to bring the new router information into the Router MC database.

The Device Import page contains two small tabs as shown in the figure:

- All—Displays the entire device hierarchy.

- Selection—Displays only the routers you selected for import.

Choose Import Method

SECUR 1.1—13-31
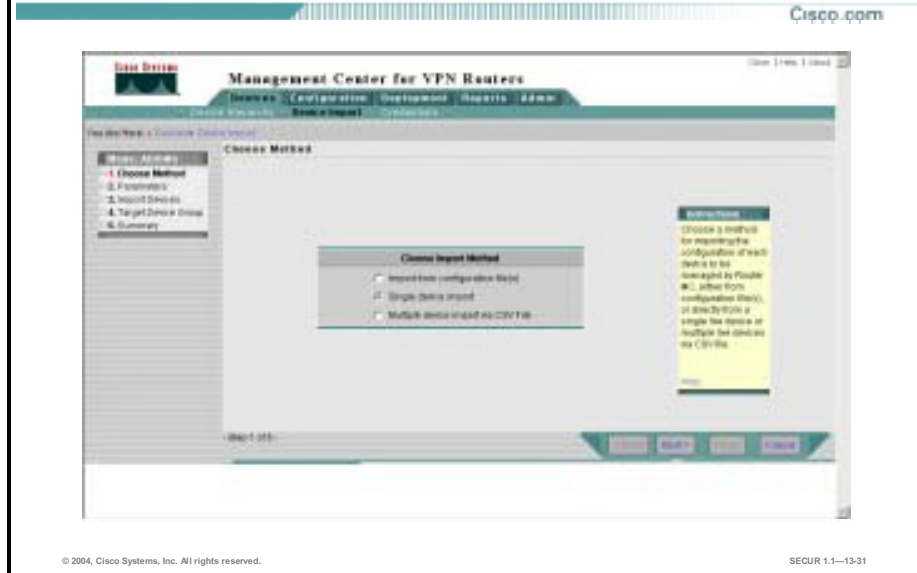
Complete the following steps to import device configurations into the Router MC database:

Step 1 Select **Devices>Device Import**. The Device Import page opens.

Step 2 Click **Import**. The Choose Method page opens.

Step 3 Select the appropriate import method radio button from the following list:

■ Import from configuration file(s)—(Default) Select this radio button to import router configuration information from either a pre-existing directory or single router configuration file. By default, configuration files must be named *primary-device-name*.**cfg**. The Router MC administrator may change the required suffix for the configuration files in the Admin tab.

■ Single device import—Select this radio button to import the configuration of a single router using an SSH session. For routers using dynamic IP addressing, the IP address is retrieved from AUS.

■ Multiple device import via CSV File—Select this radio button to import configurations from multiple routers using SSH and a CSV reference file. To use this import option, you must first create a CSV reference file containing the IP addresses, and administrative passwords of the routers you wish to import configurations from. See the Router MC online help function for more information on how to create the CSV file for multiple device import.

Step 4 Click **Next**. The Parameters page opens.

Note	In our example, we chose to use the single device import option which means we now need to inform the Router MC exactly which router to communicate with using SSH. If we had chosen to import from a configuration file, we would have been prompted for the location of the file. If we had chosen to import multiple devices using a CSV file, we would have been prompted for the location of the CSV file.

Configure Import Parameters
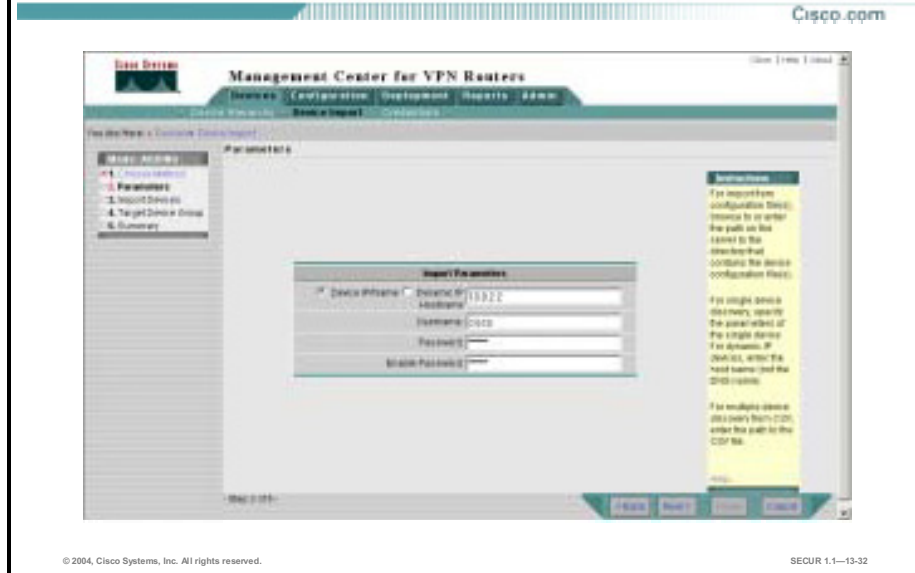
Step 5   Select one of the following two radio buttons:

■ Device IP/Name—Select this radio button if you are importing a configuration from a router with a fixed IP address (preferably the IP address of the external router interface). Then, enter the fixed IP address in the adjacent field.

■ Dynamic IP Hostname—Select this radio button if you are importing a configuration from a spoke router with a dynamic IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server. Then, enter the hostname of the router you wish to import the configuration from (not the Domain Name System [DNS] server) in the adjacent field.

Step 6   Enter the login name for an administrative account on the router in the Username field.

Step 7   Enter the password associated with the above login name (administrative account) in the Password field.

Step 8   Enter the enable password for the router in the Enable Password field.

Step 9   Click **Next**. The Import Devices page opens. Now we need to select the router role.

Select Device Role
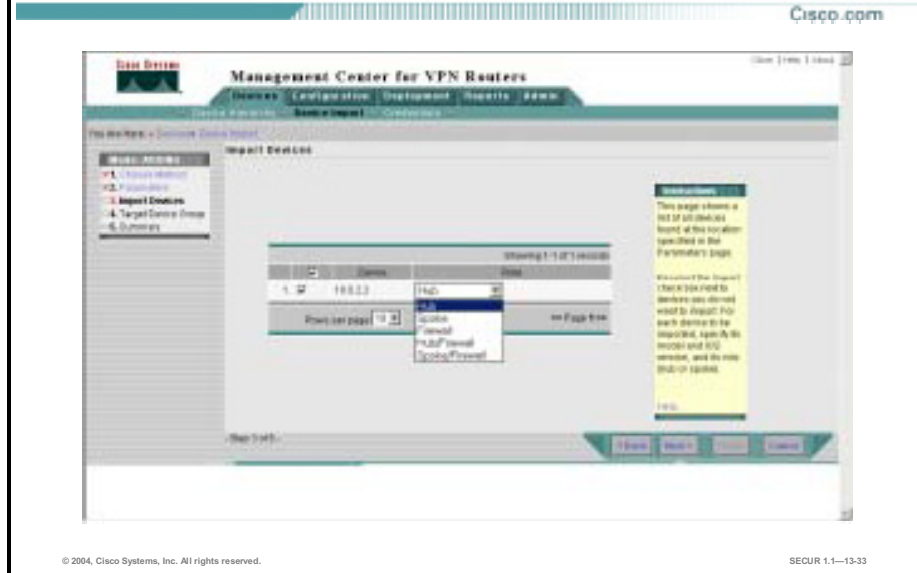
Step 10 Select the router role from the Role list box. Your choices include the following:

■ Hub—Select this role if the router serves as a primary or secondary hub in a VPN. On deployment, only hub-specific VPN configurations are deployed to this router.

■ Spoke—Select this role if the router serves as a spoke in a VPN. On deployment, only spoke-specific VPN configurations are deployed to this router.

■ Firewall—Select this role if the router serves as firewall router only and does not participate in a VPN. On deployment, only firewall configurations will be deployed to this router.

■ Hub/Firewall—Select this role if the router serves as hub in a VPN and will also provide firewall functionality. On deployment, both hub-related VPN configurations and firewall configurations will be deployed to this router.

■ Spoke/Firewall—Select this role if the router serves as a spoke in a VPN and will also provide firewall functionality. On deployment, both spoke-related VPN configurations and firewall configurations will be deployed to this router.

Note   In our example we chose to import the router as a hub.

Step 11 Click **Next**. The Target Device Group page opens.

Select Target Device Group

Cisco.com

© 2004, Cisco Systems, Inc. All rights reserved. SECUR 1.1—13-34
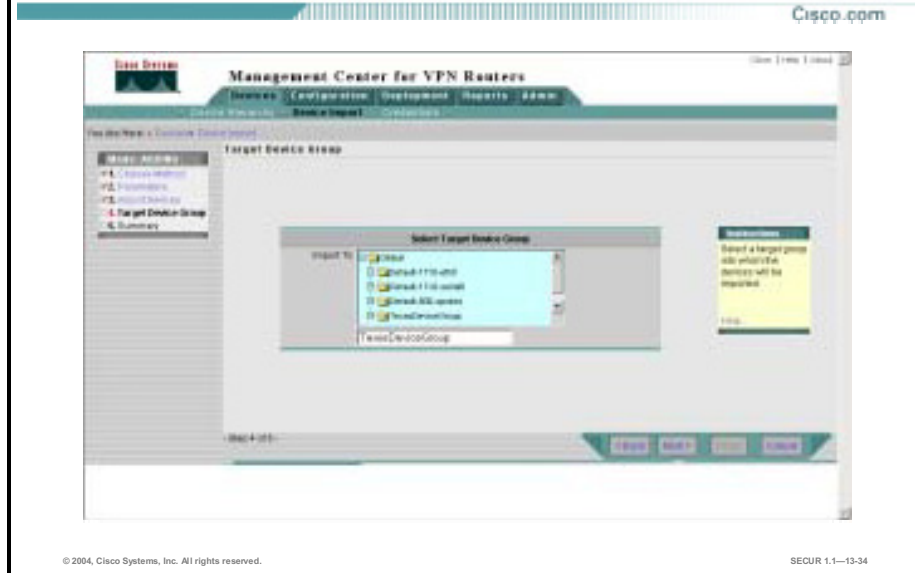
Step 12 Go to the Import To: area and select the device group you wish the imported router to become a member of.

| **Note** | This example shows the router imported to the TexasDeviceGroup created earlier. |

Step 13 Click **Next**. The Device Import Summary page opens.

Review Device Import Summary and Finish

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

SECUR 1.1—13-35
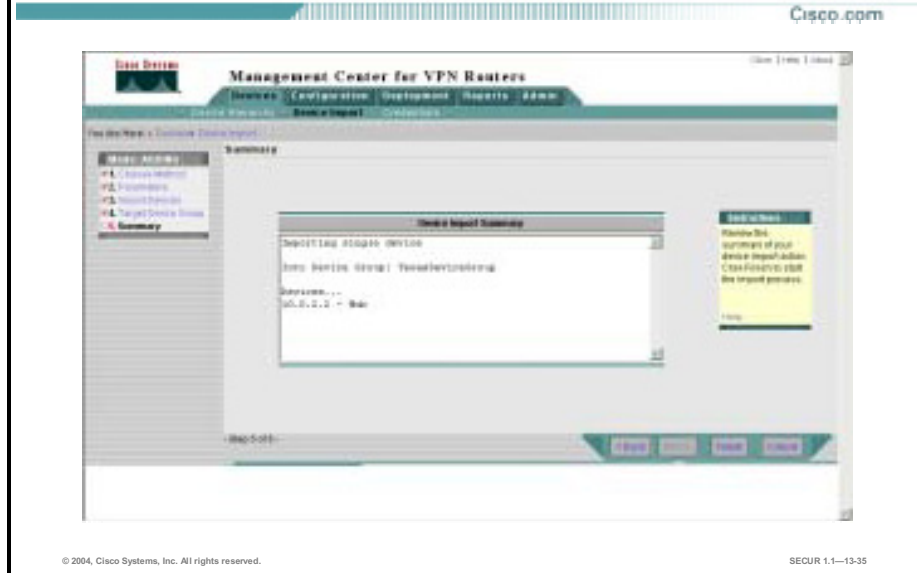
Step 14   Review the information in the Device Import Summary page. This page identifies each router selected for import, by listing its name, role, and parent device group. For routers imported from a pre-existing configuration file, it also lists the router model and Cisco IOS version.

Step 15   Click **Finish** to start the import process. The Last Import Status dialog box opens.

Review Import Status

Management Center for VPN Routers
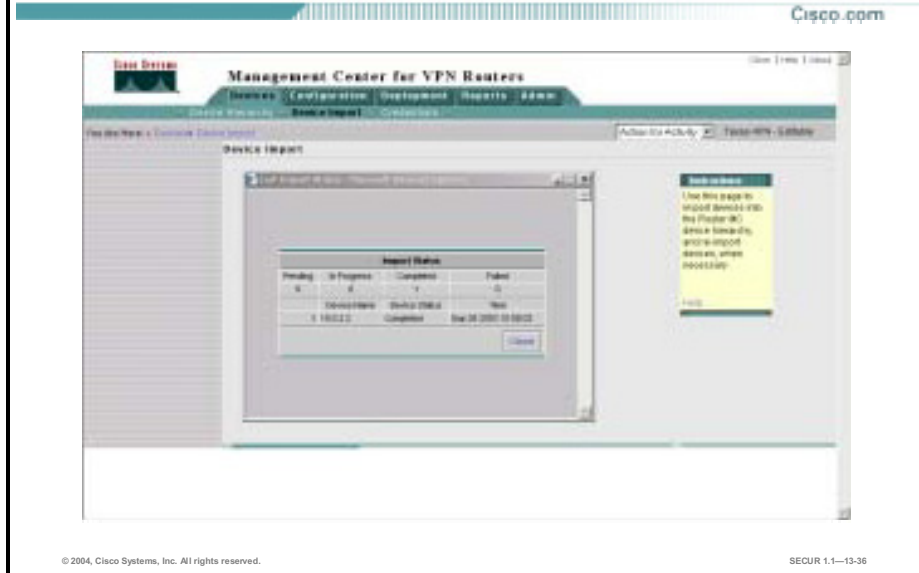
Device Import

Step 16 View the Last Import Status dialog box. The device status updates as the import process proceeds. There are four possible indicators for the import status:

■ Pending—Displayed while awaiting the import procedure to begin.

■ In Progress—Displayed during the import procedure.

■ Completed—Displayed following a successful import procedure.

■ Failed—Displayed whenever an error occurs during the import procedure. Failures also contain an error field which provides basic error information.

Step 17 Click **Close**. You are returned to the Device Import Device Hierarchy page.

View Device Hierarchy
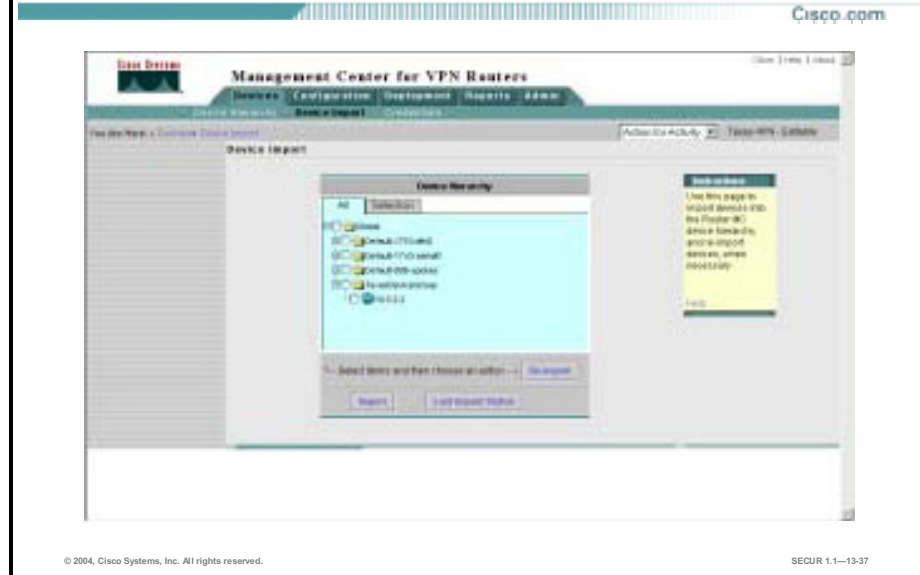
Step 18   View the updated Device Hierarchy page. Note that the newly imported router appears in the All tab.

This completes the procedure for importing routers into the Router MC database. Now we move onto task 4 where we will define the VPN settings.

Task 4—Defining VPN Settings

This topic explains how to define basic VPN settings using the Router MC.

VPN settings provide a framework for network behavior and VPN policy implementation. VPN settings include selection of failover method and routing protocol, packet fragmentation settings, specification of internal networks and inside interfaces for hubs and spokes, and hub assignment for spokes.
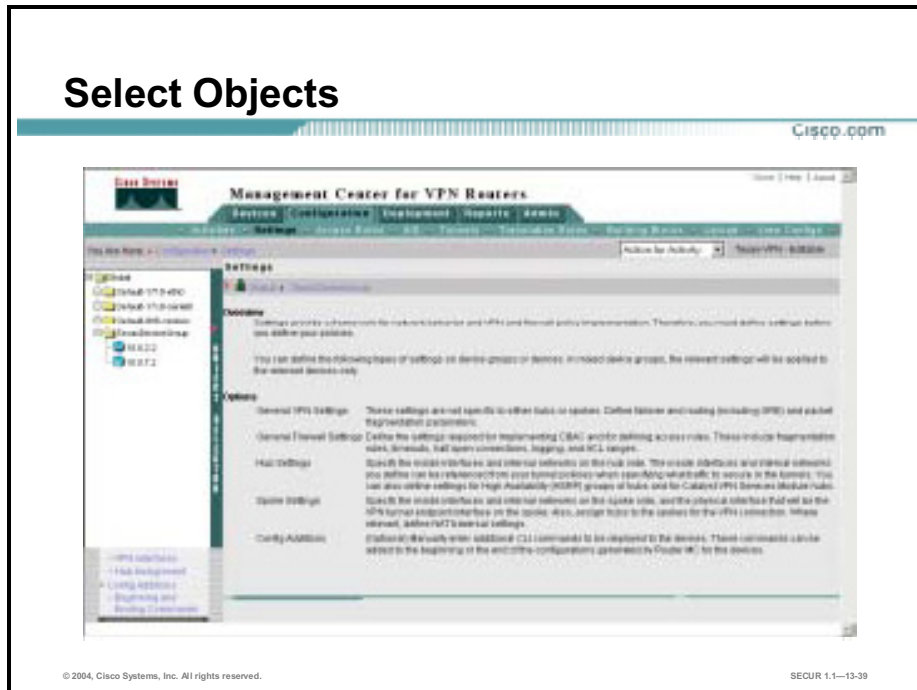
When you create the tunnel policy for the VPN, you secure the traffic flow between the inside interfaces on the hubs and the inside interfaces on the spokes.

Complete the following steps to configure basic VPN settings:

Step 1   Select **Configuration>Settings**. The Settings page opens.

Step 2   Expand the Object Selector, then select the folder for the device group you wish to configure.

Note   The example uses the TexasDeviceGroup device group folder configured earlier.

Step 3   Select **Hub>Inside Interfaces** from the TOC. The Hub Inside Interfaces page opens.

Hub Inside Interfaces

SECUR 1.1—13-40

Step 4   Click **Show Interfaces**. The Show Interfaces dialog box opens.

Note	Clicking **Show Interfaces** displays all the interfaces for the router type in the device group. Alternatively, you may select a Slot, Port, and Sub interface then use the **>>** button to add that interface to the list. Use the **<<** button to remove an interface from the list.

Select Hub Inside Interfaces

Cisco.com

© 2004, Cisco Systems, Inc. All rights reserved. SECUR 1.1—13-41

Step 5 Select the check box for the inside interface of the hub router.

Step 6 Click **Select**. The Show Interfaces dialog box closes, and the name of the selected interface appears in the selection confirmation area.

Show Hub Inside Interfaces

SECUR 1.1—13-42

Step 7 Click **Apply**. Upon deployment, each hub in the device group will be configured with the selected interface as the inside interface. Now you need to define the inside interfaces for the spokes.

Select Spoke Inside Interfaces
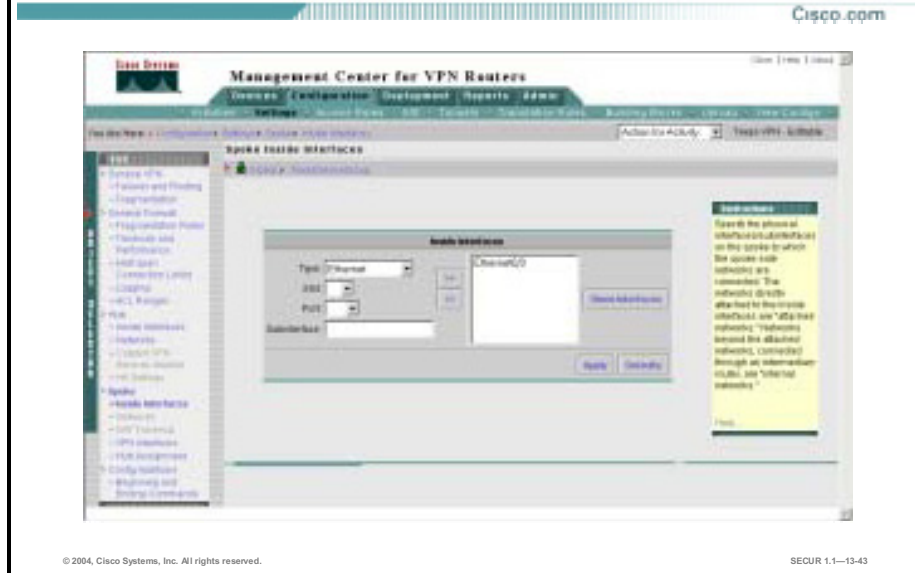
Step 8   Select **Spoke>Inside Interfaces** from the TOC. The Spoke Inside Interfaces page opens.

Step 9   Click **Show Interfaces**. The Show Interfaces dialog box opens.

Step 10   Select the check box for the inside interface of the spoke routers.

Step 11   Click **Select**. The Show Interfaces dialog box closes, and the name of the selected interface appears in the selection confirmation area. Now you need to select the spoke VPN interfaces.

Select Spoke VPN Interfaces

Cisco.com

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

SECUR 1.1—13-44
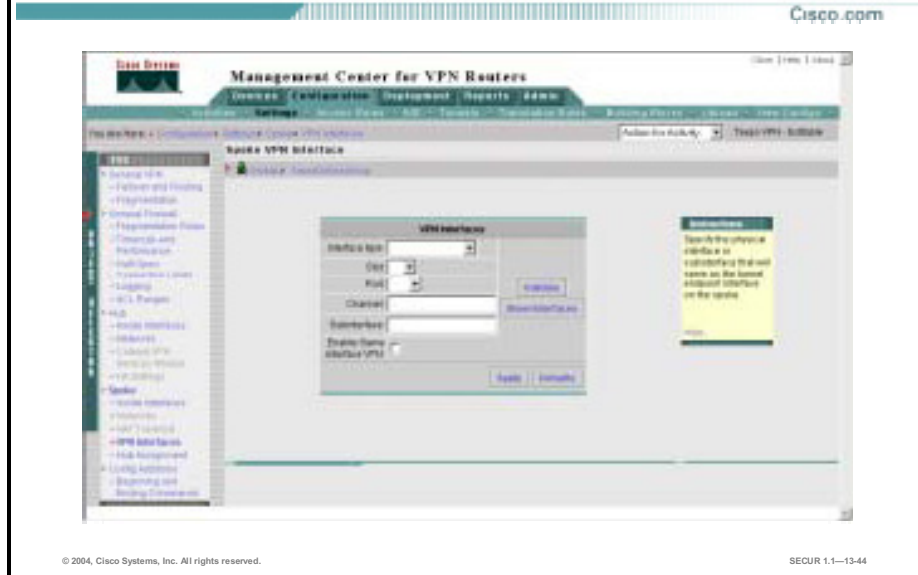
Step 12   Select **Spoke>VPN Interfaces** from the TOC. The Spoke VPN Interface page opens.

Step 13   Click **Show Interfaces**. The Show Interfaces page appears.

Show Available Spoke VPN Interfaces

Cisco.com

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—13-45
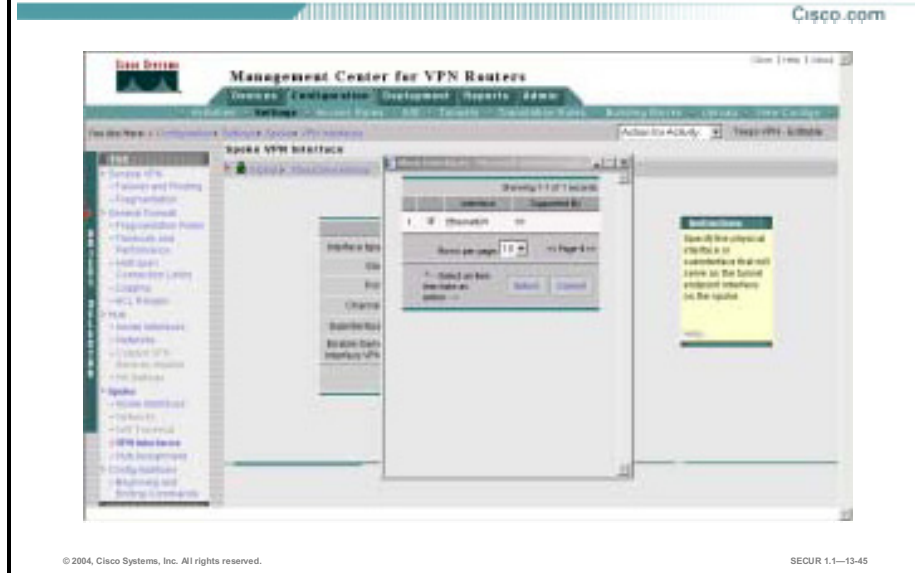
Step 14   Select the radio button for the spoke VPN interface.

Step 15   Click **Select**. The Spoke VPN Interface page updates.

Show Selected Spoke VPN Interfaces

Step 16 Click **Apply**. The Spoke VPN Interface page updates.

Validate Spoke VPN Interfaces

SECUR 1.1—13-47
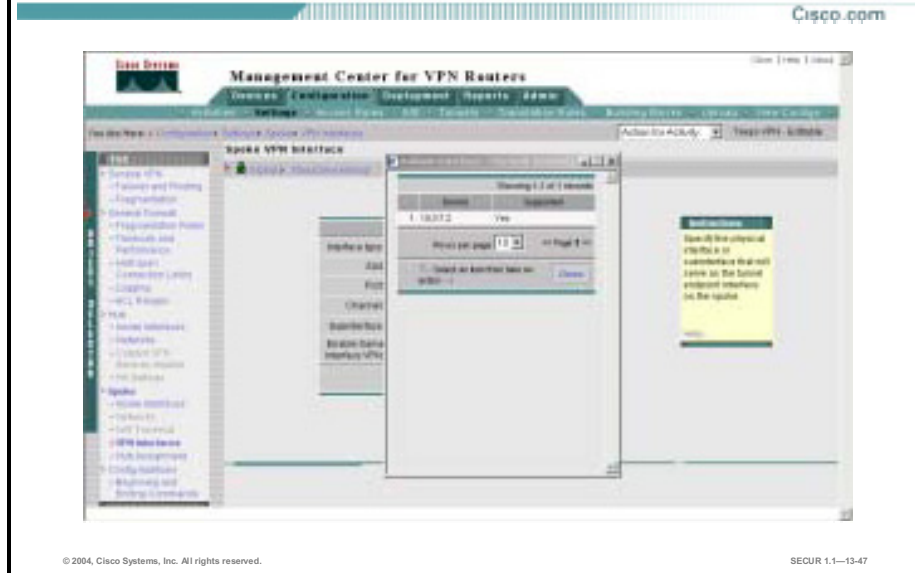
Step 17 Optionally, you may want to validate which routers have the selected interface by completing the following:

- Click **Validate**. The Validate Interface page appears.

- Check to see if the VPN interface you selected earlier is available on all the spoke routers.

- Click **Close**.

Now you need to assign a hub for the spokes.

Step 18 Select **Spoke>Hub Assignment**. The Hub Assignment page appears.

Spoke Hub Assignment

SECUR 1.1—13-48

Step 19   Select the primary hub from the Primary Hub list box.

Step 20   Select the primary interface from the Primary Interface list box.

Step 21   Select the failover hub from the Failover Hub list box.

Step 22   Select the failover interface from the Failover Interface list box.

Step 23   Click **Apply**. The Hub Assignment page updates.

This completes task 4. Now you need to configure the VPN policies in task 5.

Task 5—Defining VPN Policies

This topic explains how to define VPN policies using the Router MC.

Configuration>IKE
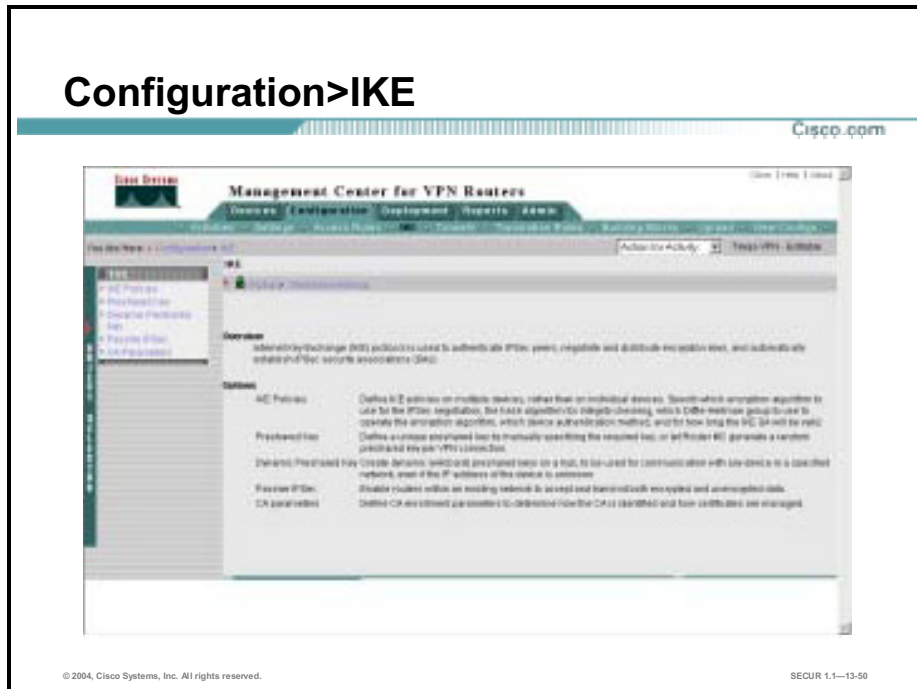
IKE policies define the combination of security parameters to be used during IKE negotiation between two IPSec peers, including the encryption and authentication algorithms, the Diffie-Hellman (DH) group identifier and the lifetime of the Security Association (SA).

Complete the following steps to configure an IKE policy:

Step 1 Select **Configuration>IKE**. The IKE page opens.

Step 2 If you need to, expand the Object Selector and select the device group for which you want to configure an IKE policy.

Note	Router MC remembers the last device group you worked with and presents that device group as you move through other tabs and menus.

View Existing IKE Policies

SECUR 1.1—13-51

Step 3   Select **IKE Policies** from the TOC. The IKE Policies page opens. You have several options available to you from within this page as follows:

- Create—Click this button to create a new IKE policy.

- Edit—Click this button to edit an existing IKE policy.

- Move Up—Click this button to move an IKE policy up one row in the list (increasing the priority of the IKE policy).

- Move Down—Click this button to move an IKE policy down one row in the list (decreasing the priority of the IKE policy).

- Delete—Click this button to delete the selected IKE policy.

Step 4   Click **Create**. The Name and Comment page appears.

Configure Name and Comment
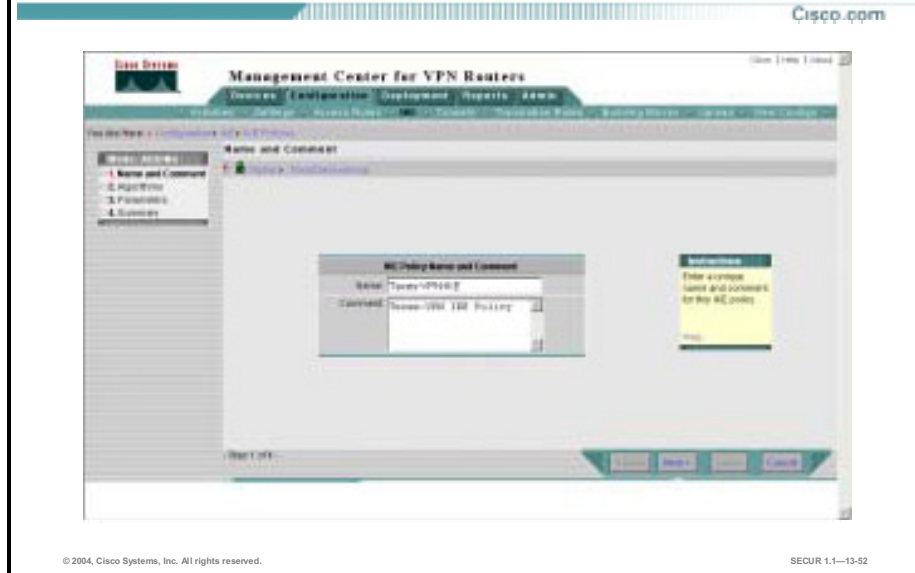
Step 5 Enter an appropriate name for the new IKE policy in the Name field.

Step 6 (Optional.) Enter an optional comment describing the new IKE policy in the Comment field.

Step 7 Click **Next**. The Algorithms page opens.

Select Encryption Algorithm

Step 8   Select an appropriate encryption algorithm from the Encryption Algorithm list box.

Select Hash Algorithm

Step 9 Select an appropriate hash algorithm from the Hash Algorithm list box.

Select Modulus Group

SECUR 1.1—13-55

Step 10 Select an appropriate modulus group from the Modulus Group list box.

Step 11 Click **Next**. The Parameters page opens.

Select Lifetime and Authentication Type
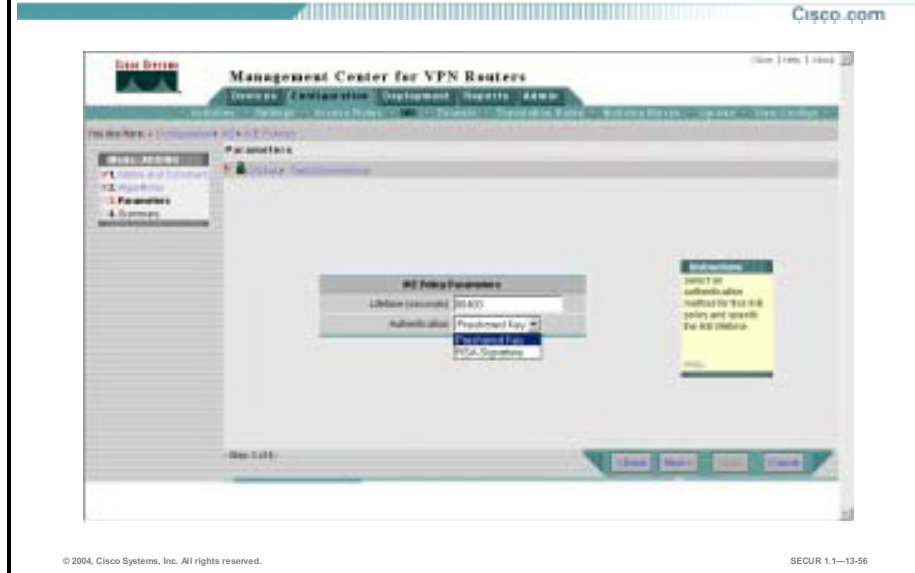
Step 12   Enter an appropriate lifetime (in seconds) in the Lifetime field.

Step 13   Select an appropriate authentication method in the Authentication field.

| Note | In this example, Preshared Key is chosen. |

Step 14   Click **Next**. The IKE Policy Summary page opens.

View IKE Policy Summary

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

SECUR 1.1—13-57
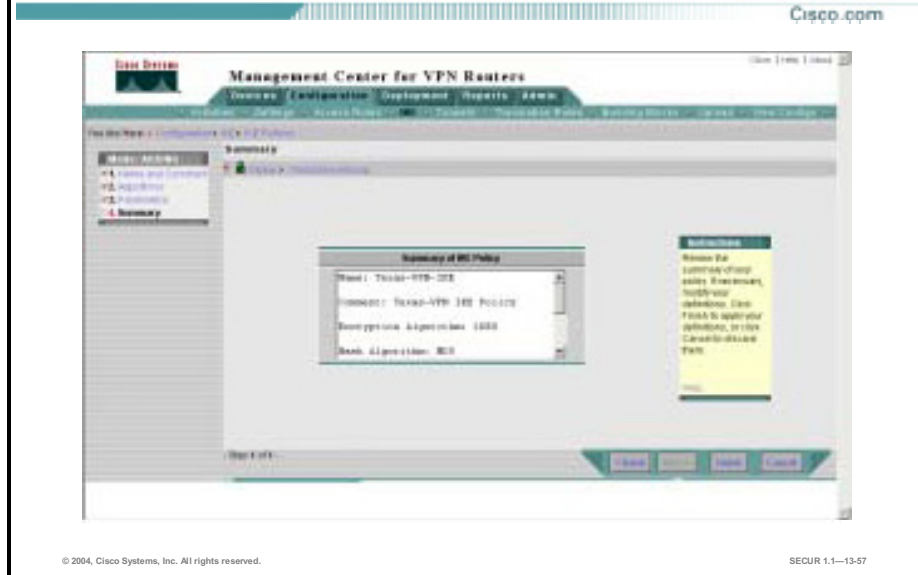
Step 15 Review the IKE policy summary.

Step 16 Click **Finish**. The IKE policies list is updated.

View New IKE Policy

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

SECUR 1.1—13-58
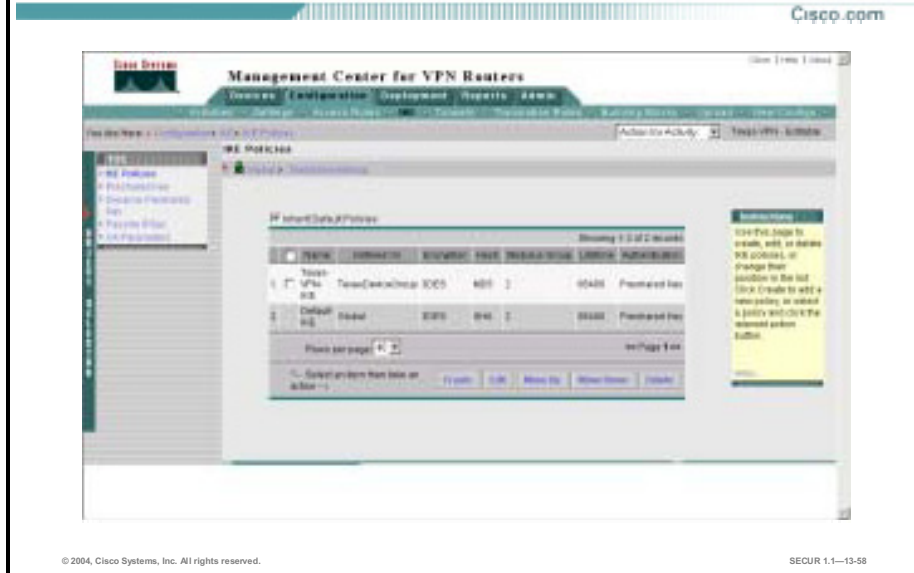
Step 17 View the updated IKE policies list for the selected device group.

Step 18 (Optional.) If appropriate, select the check box next to an IKE policy and use the Move Up and Move Down buttons to either increase or decrease the selected IKE policy's priority.

Step 19 Select **Configuration>Tunnels**. The Tunnels page opens.

Configuration>Tunnels

Cisco.com

SECUR 1.1—13-59
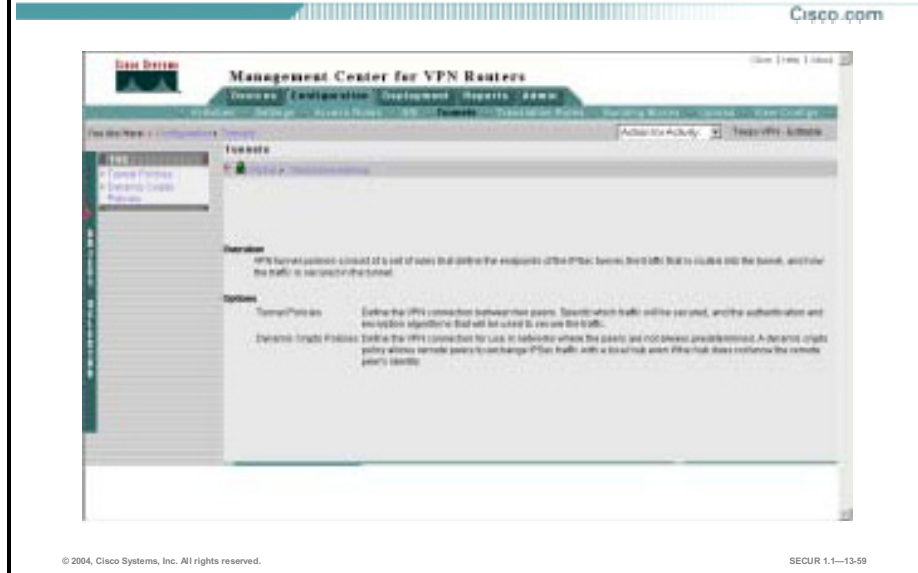
Tunnel policies define what data will be securely transmitted via the tunnel (crypto ACL) and which authentication and encryption algorithms will be applied to the data to ensure its authenticity, integrity and confidentiality (transform set).

Note	In the Router MC, tunnel policies are defined on spokes. The Router MC generates the relevant CLI commands for the spoke and also automatically adds matching policies on the spoke's corresponding hub so that the VPN connection between the peers can be established. If you always deploy to both peers of the VPN connection together, Router MC will ensure compatible policy configuration.

Step 20 Choose an appropriate tunneling option from the TOC:

- Tunnel Policies—Select this option if you wish to define a VPN connection between two predetermined peers.

- Dynamic Crypto Policies—Select this option if you wish to define a VPN for environments where the peers are not always predetermined.

Note	In this example, Tunnel Policies is chosen. The Tunnel Policies page opens.

View Tunnel Policies
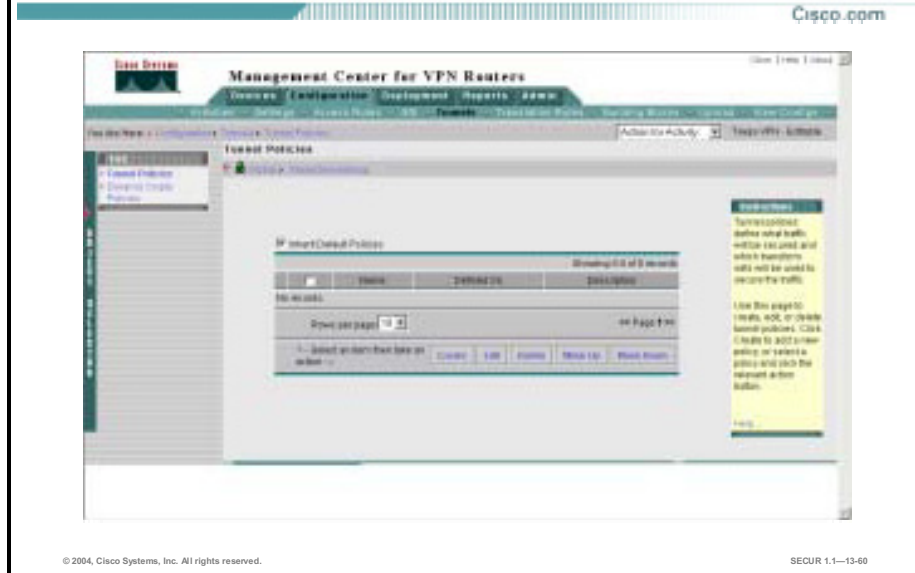
Step 21 Click **Create**. The Name and Comment page opens.

Add Name and Comment

SECUR 1.1—13-61
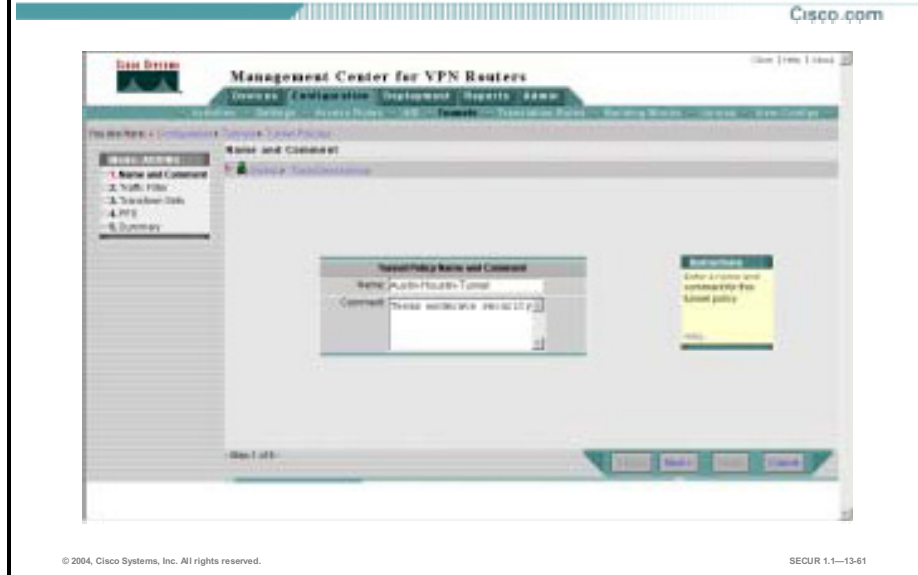
Step 22   Enter an appropriate name in the Name field.

Step 23   (Optional.) Enter an appropriate comment in the Comment field.

Step 24   Click **Next**. The Traffic Filter page opens.

View Traffic Filters

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

SECUR 1.1—13-62
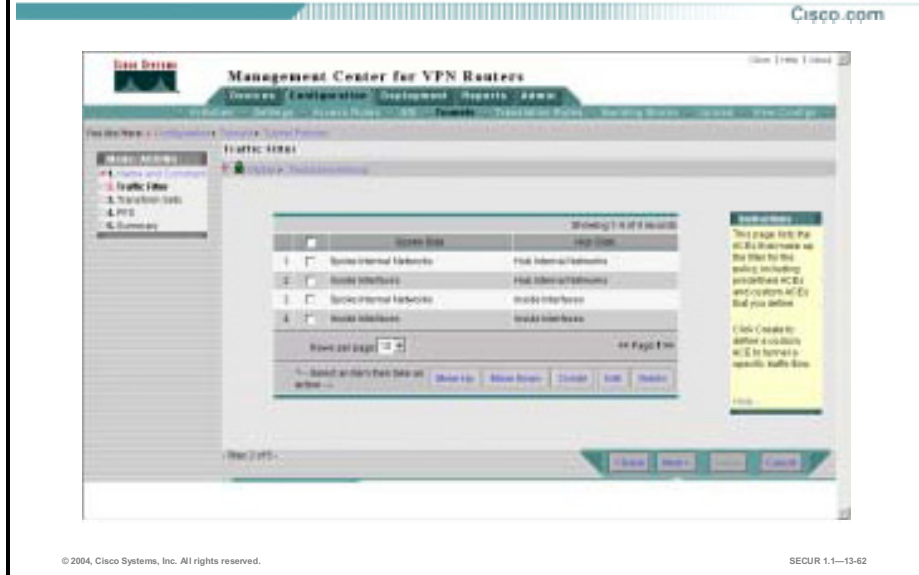
Step 25 View the predefined access control entries (ACEs).

An ACL is an ordered list of rules, known as ACEs, that describe how an entire subnet or specific network host interacts with another to permit or deny a specific service, protocol, or both. By default, the Router MC allows automatic generation of supplementary ACEs for your jobs.

Each ACE describes network traffic based on source IP address, destination IP address, protocol, and possibly ports. Each ACE has an action to permit or deny. When a packet arrives at a router, the ACEs in the ACL are scanned for the first one that matches the packet. When the router finds a matching ACE, it executes the associated permit or deny action. If no ACE match is found, the packet is denied. At deployment, Router MC compares the settings on your selected routers to all four of the predefined ACEs. Router MC applies the ACEs shown in the figure under circumstances where they match the configuration of your routers.

Note	The recommended best practice is to leave all of the predefined ACEs in the list. If there are any conflicts with your selected routers, you will be notified at deployment.

You could, at this point, click **Create** and specify a new ACE, or click **Edit** to edit an existing ACE. You could also choose to move an ACE up or down in the list to change its priority.

Note	This example leaves all of the predefined ACEs. This will secure all internal traffic on the selected hub and spokes.

Step 26 Click **Next**. The Transform Sets page opens.

View Transform Sets

SECUR 1.1—13-63

Step 27   Click **Create**. The Name and Comment page opens.

Name Transform Set

Cisco.com

Management Center for VPN Routers

SECUR 1.1—13-64
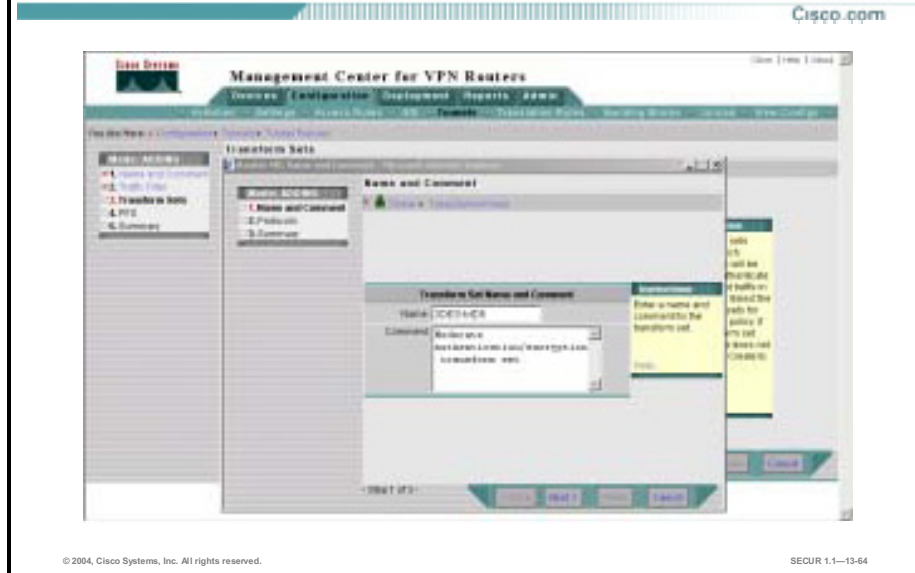
Step 28   Enter an appropriate name in the Name field.

Step 29   (Optional.) Enter an appropriate comment in the Comment field.

Step 30   Click **Next**. The Protocols page opens.

Select Transform Set Protocols

SECUR 1.1—13-65
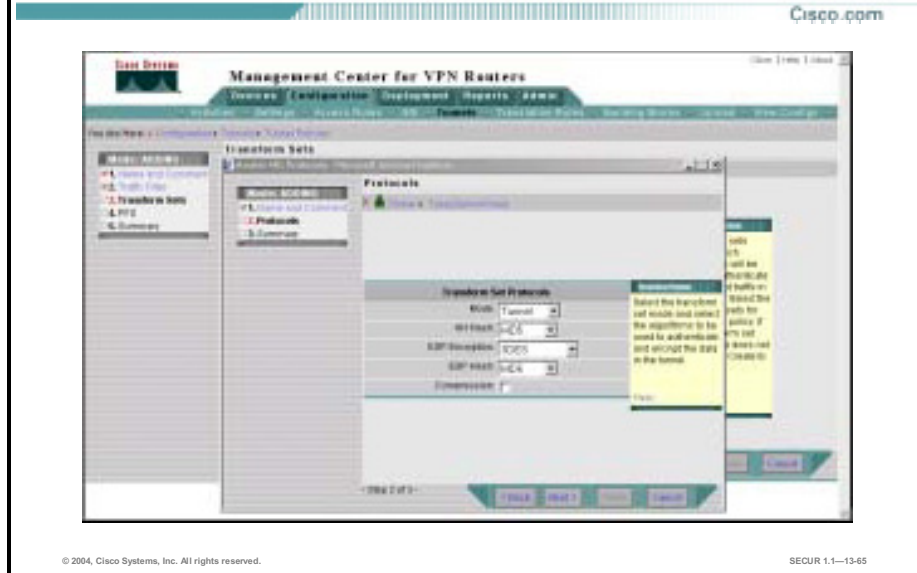
Step 31   Select the appropriate IPSec mode of operation from the Mode list box. Your choices are as follows:

- Transport

- Tunnel

Step 32   Select an appropriate AH hash method from the AH Hash list box. Your choices are as follows:

- MD5

- SHA

Note   If you do not want to use AH authentication, do not make a selection in this field.

Step 33   Select an appropriate Encapsulating Security Payload (ESP) encryption method from the ESP Encryption list box. Your choices are as follows:

- DES

- 3DES

- ESP-AES

- ESP-AES 128

- ESP-AES 192

- ESP-AES 256

Step 34   Select an appropriate ESP hash method from the ESP Hash list box. Your choices are as follows:

- MD5

- SHA

Step 35 If you want the data in the IPSec tunnel to be compressed using the Lempel-Ziv-STAC (LZS) algorithm, select the **Compression** check box.

Step 36 Click **Next**. The Summary page opens.

View Transform Set Summary

SECUR 1.1—13-66
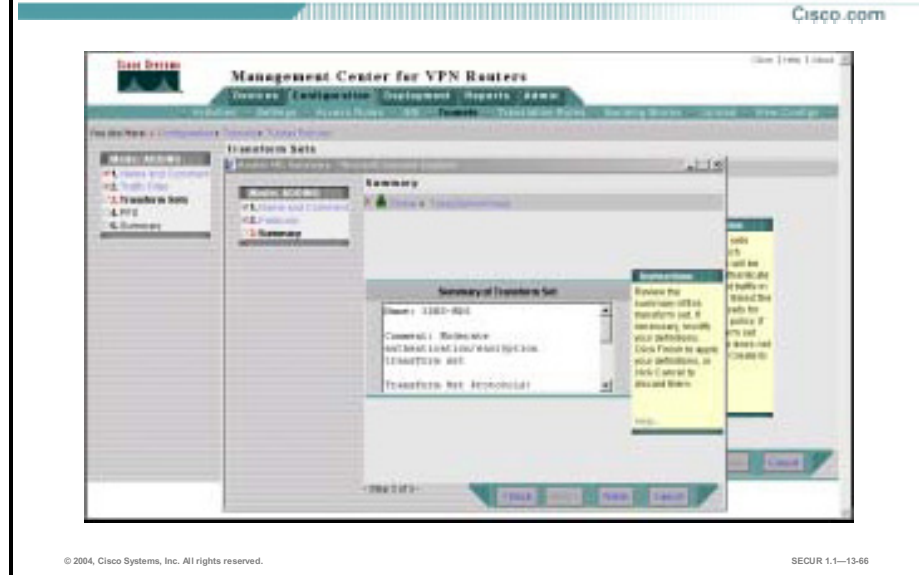
Step 37   Verify that the new transform set parameters are correct. If they are not correct, click **<Back** and correct the mistake.

Step 38   Click **Finish**. The new transform set policy is created. Now you need to assign the new policy to a transform set.

Assign New Policy to Transform Set 1

Cisco.com

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

SECUR 1.1—13-67
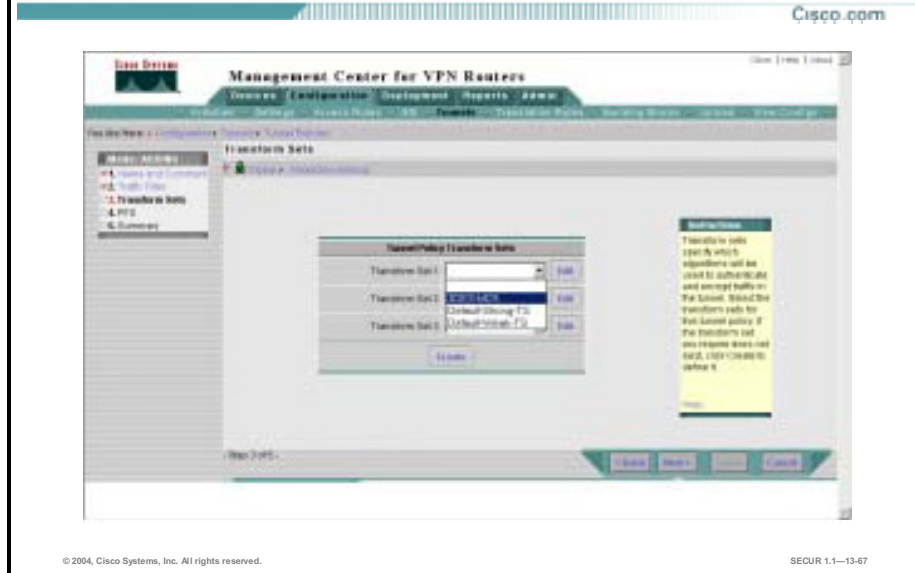
Step 39 Select the new transform set policy from the Transform Set 1 list box. Router MC provides you with two predefined transform sets:

- Default-Strong-TS—Offers high security using the following parameters:
    — Mode—Tunnel
    — AH hash—None
    — Encryption algorithm—3DES
    — Hash algorithm—SHA
    — Compression—None
- Default-Weak-TS—Offers lower security using the following parameters:
    — Mode—Tunnel
    — AH hash—None
    — Encryption algorithm—DES
    — Hash algorithm—SHA
    — Compression—None

Note   You can select up to three transform sets per tunnel policy. If you are defining the policy on a spoke or group of spokes, it is usually not necessary to select more than one transform set. This is because the spoke's assigned hub would typically be a higher performance router capable of supporting any transform set that the spoke supports. However, if you are defining the policy on a hub for a dynamic crypto environment, you should select more than one transform set to ensure that there will be a transform set match between the hub and the unknown spoke.

Step 40 Click **Next**. The Perfect Forward Secrecy (PFS) page opens.

Select Perfect Forward Secrecy

SECUR 1.1—13-68
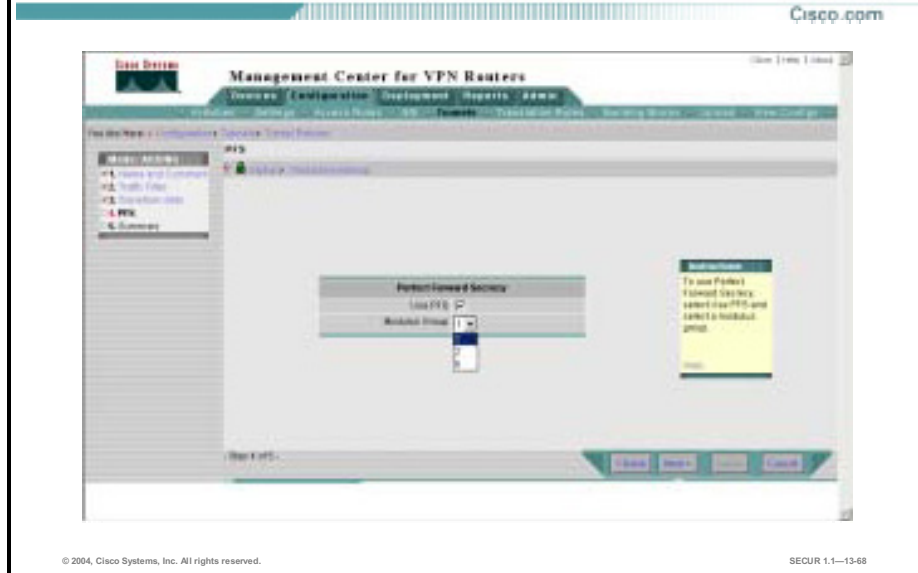
Step 41 If you wish to use PFS, select the **PFS** check box and select an appropriate DH group from the Modulus Group list box.

Perfect Forward Secrecy (PFS) generates a new key by carrying out a DH exchange every time a new quick-mode SA requires a new key to be generated. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. This option increases the level of security but at the cost of increased processor overhead. You should use PFS only if the sensitivity of the data mandates it.

You need to select the strength of the DH exchange by selecting one of the following from the Modulus Group list box:

■ Group 1—768 bits

■ Croup 2—1024 bits

■ Group 5—2048 bits

Note	DH Group 2 is recommended because Group 5 is not supported on some smaller Cisco routers, such as the Cisco 800, 2500, or 1700 Series.

Step 42 Click **Next**. The Summary page opens.

Review Tunnel Policy Summary
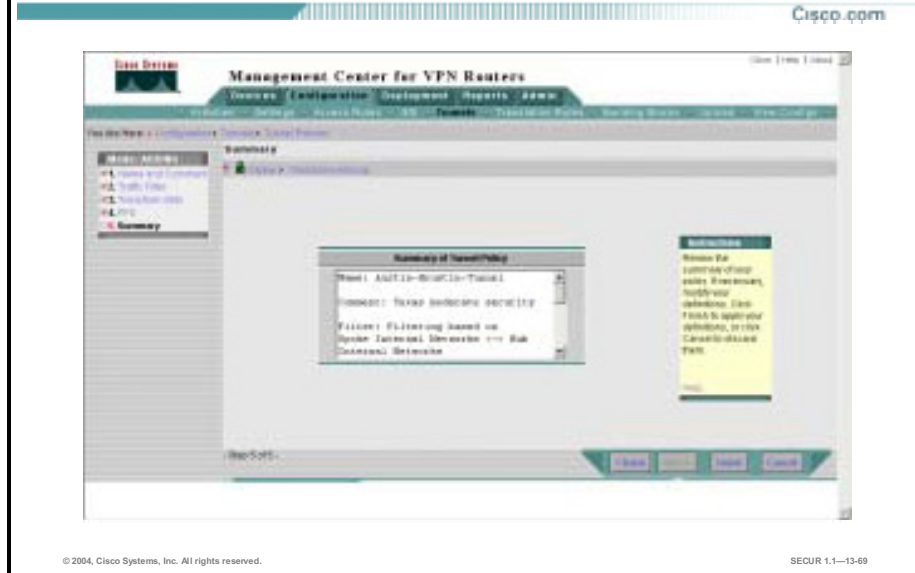
Step 43 Verify the tunnel policy information in the Summary of Tunnel Policy page.

Step 44 Click **Finish**. The tunnel policy is created and the main Tunnel Policies page opens.

Show Tunnel Policies

SECUR 1.1—13-70
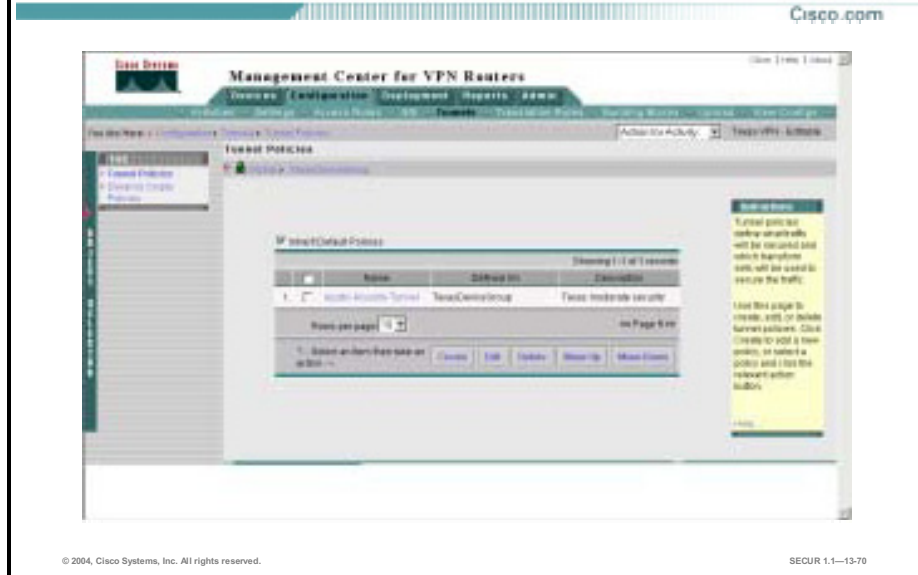
Upon deployment, the tunnel policy will be applied to the selected device group (in this example, the TexasDeviceGroup).

Next, you need to approve your activity.

Task 6—Approving Activities

This topic explains how to approve activities using the Router MC.
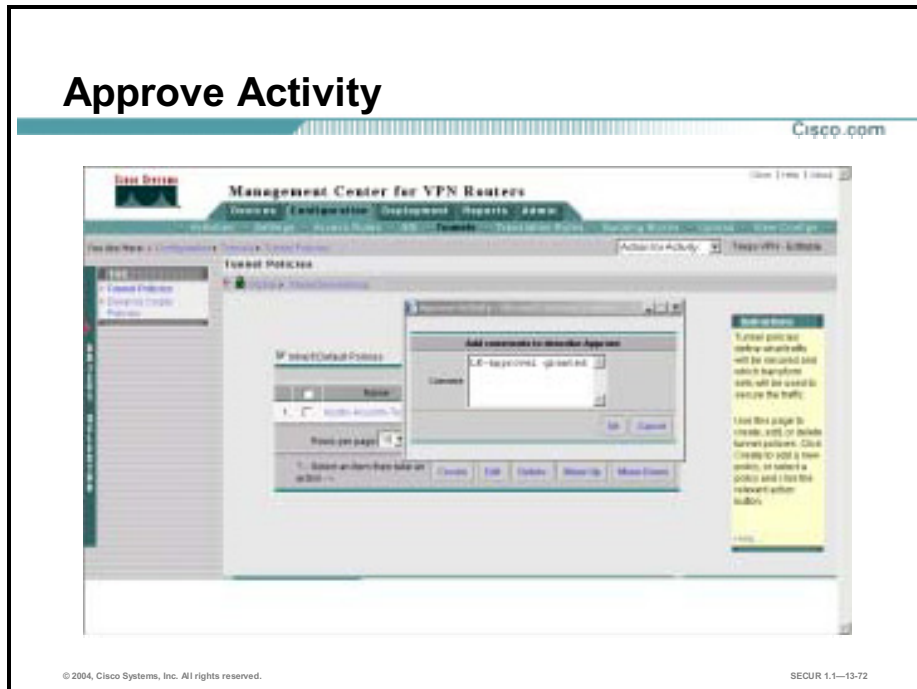
An activity must be approved before its configurations are committed and can be deployed.

Note	By default, Router MC allows any user who creates an activity to approve that activity. Later we will explain how to use the Admin tab to require submission of activities for approval by a user with appropriate permissions.

Complete the following steps to approve your new activity:

Step 1 Select **Approve** from the Actions for Activity list box. The Approve Activity dialog box opens.

Step 2 (Optional.) Enter a description for your activity approval.

Note	It is recommended that you develop a system by which approval comments are entered. At a minimum, users should enter their initials for later tracking purposes.

Step 3 Click **OK**. The activity is approved, and your configurations are committed to the Router MC database. The Activities page is updated to indicate that the activity was approved.

View Updated Activity

SECUR 1.1—13-73

You are now ready to create a job to deploy your committed configurations to a device group.

Task 7—Creating and Deploying Jobs

This topic explains how to create and deploy jobs using the Router MC.

A job is a deployment task in which you specify the routers to which VPN and firewall configurations should be deployed. Router MC generates the CLI commands for the routers specified in the job, based on the policies you defined. These commands can be previewed before deployment takes place. Within the context of the job, you can specify whether to deploy the commands directly to the routers in the network or to a file.
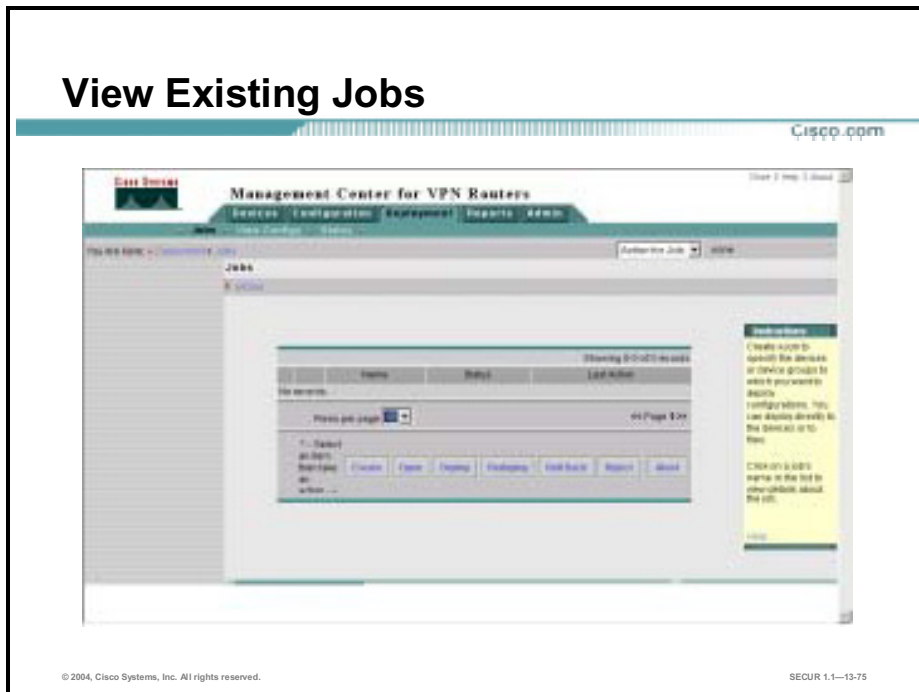
Complete the following steps to create and deploy a Router MC job:

Step 1 Select **Deployment>Jobs**. The Jobs page opens.

Step 2 Click **Create**. The Name and Description page opens.

Enter Job Name and Description

Cisco.com

© 2004, Cisco Systems, Inc. All rights reserved. SECUR 1.1—13-76
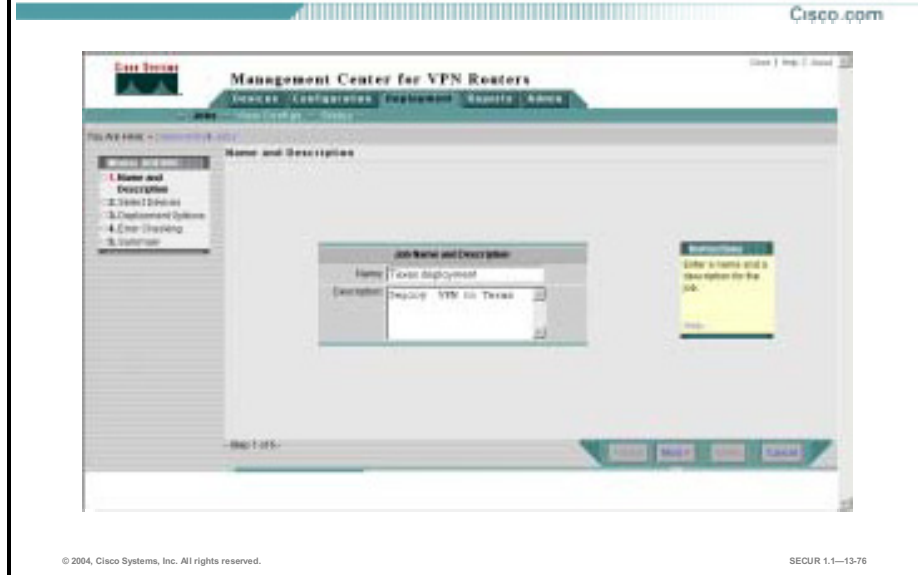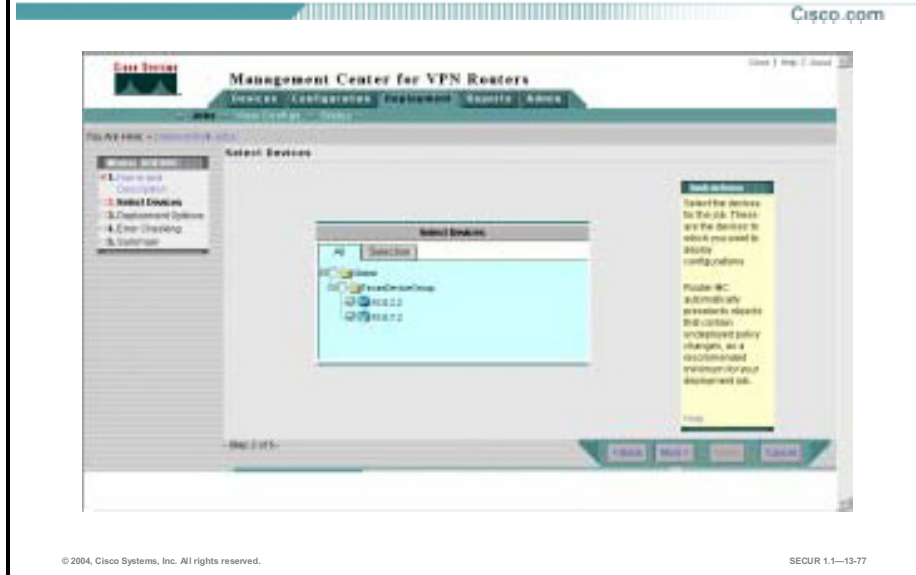
Step 3 Enter a unique name for the job in the Name field.

Step 4 (Optional.) Enter an appropriate description of the job in the Description field.

**Step 5** Click **Next**. The Select Devices page opens.

Select Devices

SECUR 1.1—13-77

Note	Since Router MC automatically selects routers on which policy changes have been made but have not yet been deployed, in most cases, you won't need to make any device selections.

Step 6 If not already selected by the Router MC, select the device group or individual routers from the All tab.

Step 7 Click **Next**. If Router MC has added routers to the job, a dialog box opens listing the names of the added routers and the reason they were added.

Step 8 Click **Close**. The Deployment Options page opens.

Select Deployment Options
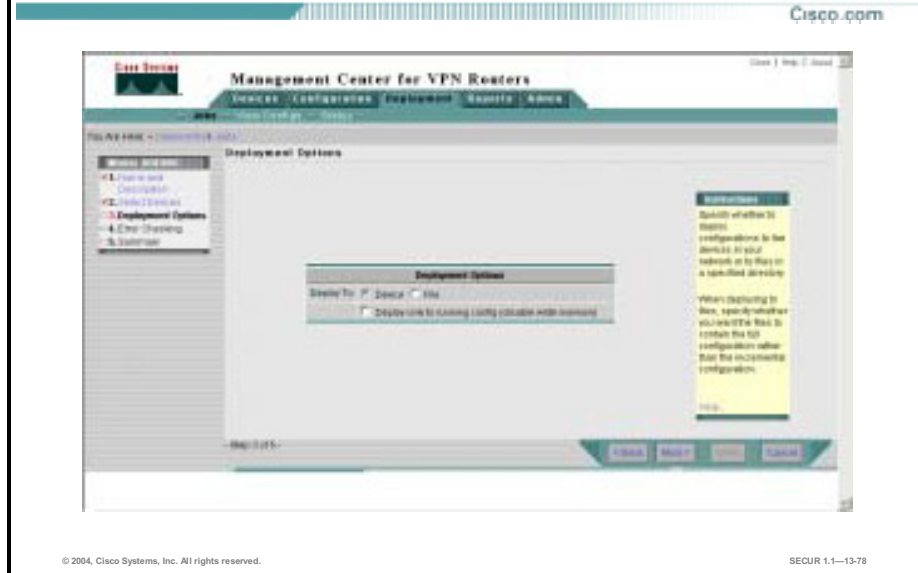
Step 9 Select an appropriate deployment method from the following list:

- Deploy To: **Device**—Select this radio button if you want Router MC to deploy the configurations directly to the selected routers by sending CLI commands over a SSH connection.

- Deploy To: **File**—Select this radio button if you want Router MC to deploy the configurations to an output file for each router in the job and place the files in the directory of your choice.

Note	If you deploy configurations to a file, you must transfer the configurations from the file to your routers at a later stage. Deploying configurations to a file is useful when the routers are not yet in place in the physical network (also known as greenfield deployment), or if you wish to delay deployment.

Step 10 If you want to deploy the configurations to your router running configuration only, select the **Deploy only to running config (disable write memory)** check box.

Step 11 Click **Next**. The Error Checking page opens.

Resolve Any Errors

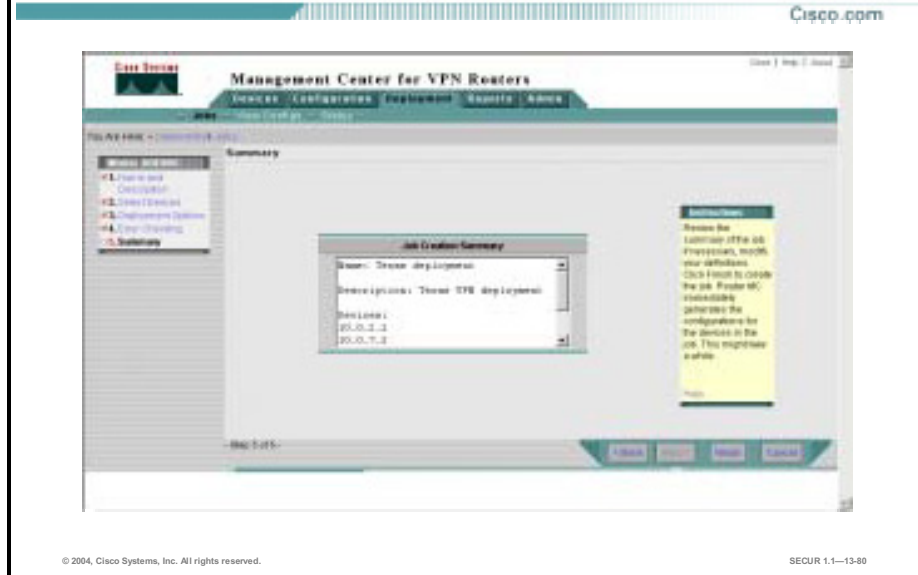© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—13-79

| **Note** | Errors prevent deployment, while warnings do not prevent deployment. If any errors are issued, you must go back and resolve them before deployment may proceed. |

Step 12 Click **Next**. The Summary page opens.

Review Job Creation Summary

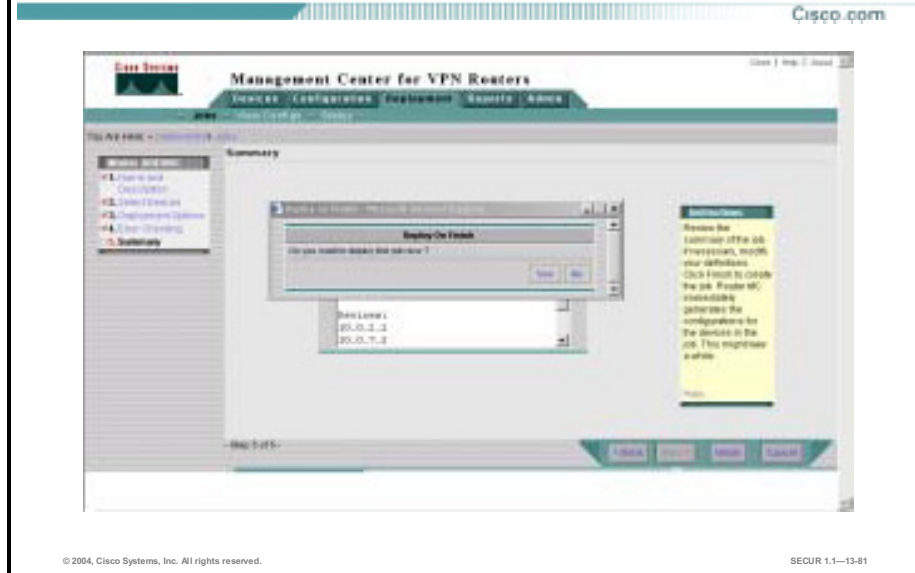© 2004, Cisco Systems, Inc. All rights reserved.

SECUR 1.1—13-80

Step 13 Review the job creation summary.

Step 14 Click **Finish**. A dialog box opens asking if you want to deploy the job immediately.

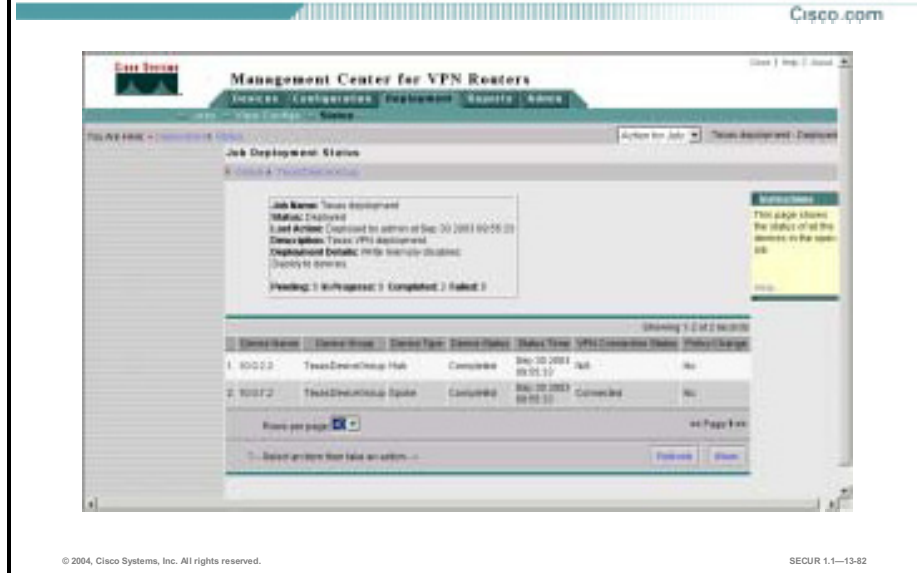## Select Deploy on Finish

Cisco.com

Management Center for VPN Routers

© 2004, Cisco Systems, Inc. All rights reserved.   SECUR 1.1—13-81

Step 15 Click **Yes** to deploy the job now. The Job Deployment Status page opens.

Review Job Deployment Status

SECUR 1.1—13-82

In this page, you can view the deployment status of your job, and of each router in the job relative to the job status.

Jobs proceed through the following states:

■ Generating—Status displayed while CLI commands are being generated.

■ Deployed—Status displayed after the job has been deployed.

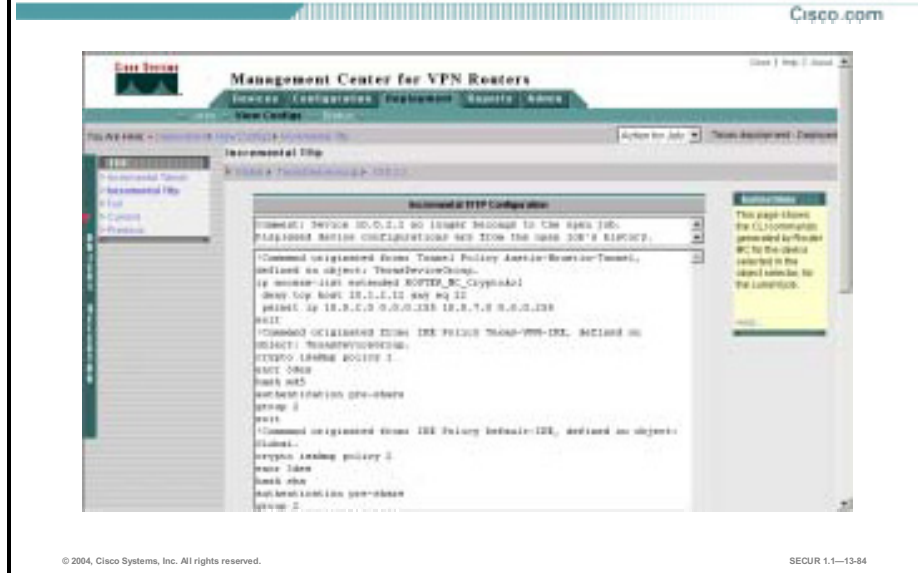Devices proceed through the following states:

■ Pending—Status displayed just before deployment starts.

■ Deploying—Status displayed during deployment.

■ Completed—Status displayed after the configuration of the router has been deployed.

Step 16 Click **Refresh** to obtain an updated view of job and router states.

Step 17 Select **Deployment>View Configs**. The Current page opens.

View Current Configuration

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

SECUR 1.1—13-83

Step 18 Scroll through the Current Configuration window to see the configuration deployed to the router device group.

Step 19 Select **Incremental Tftp** from the TOC. The Incremental Tftp page opens.

View Incremental TFTP Configuration

SECUR 1.1—13-84

Step 20 Scroll through the Incremental TFTP Configuration page to view the CLI commands generated by Router MC.

You have several options available to you for viewing configurations as follows:

- Incremental Telnet—Displays the CLI commands generated by Router MC for the router, in the current activity or job, in Telnet format. This includes the **do** and **undo** commands required to implement the policies defined for the router in the Router MC.

- Incremental Tftp—Displays the CLI commands generated by Router MC for the router, in the current activity or job, in TFTP format. This includes the **do** and **undo** commands required to implement the policies defined for the router in the Router MC.

- Full—Displays the proposed complete configuration on the router after deployment, including the incremental configuration and the previous configuration of the router.

- Current—Displays the current configuration on the router. If deployment has not yet taken place, the current configuration reflects the configuration on the router at the time it was imported. If configurations were previously deployed to the router, the current configuration reflects the full configuration of the router after the last deployment, including the commands that were on the router previously and the commands that Router MC generated for the router to implement the policy definitions.

- Previous—Displays the configuration on the router prior to the last successful deployment. If you perform a "rollback" on the job, this will be the configuration that will be restored on the router. If the router has not previously been included in a deployed job, no previous configuration will be available.

Configuring General Cisco IOS Firewall Settings

This topic explains how to configure general Cisco IOS Firewall settings using Router MC.

General Firewall Settings

Cisco.com

**General firewall settings include the following:**

- **Fragmentation rules**
- **Timeouts and performance settings**
- **Half-open connection limits**
- **Logging settings**
- **ACL ranges**

SECUR 1.1—13-86

Router MC lets you configure your router to function as a firewall by using CBAC and access rules. General firewall settings include the parameters that are required for implementing CBAC and defining ACL ranges for access rules as shown in the figure:

- Fragmentation rules

- Timeouts and performance

- Half-open connection limits

- Logging settings

- ACL ranges

General Firewall>Fragmentation Rules
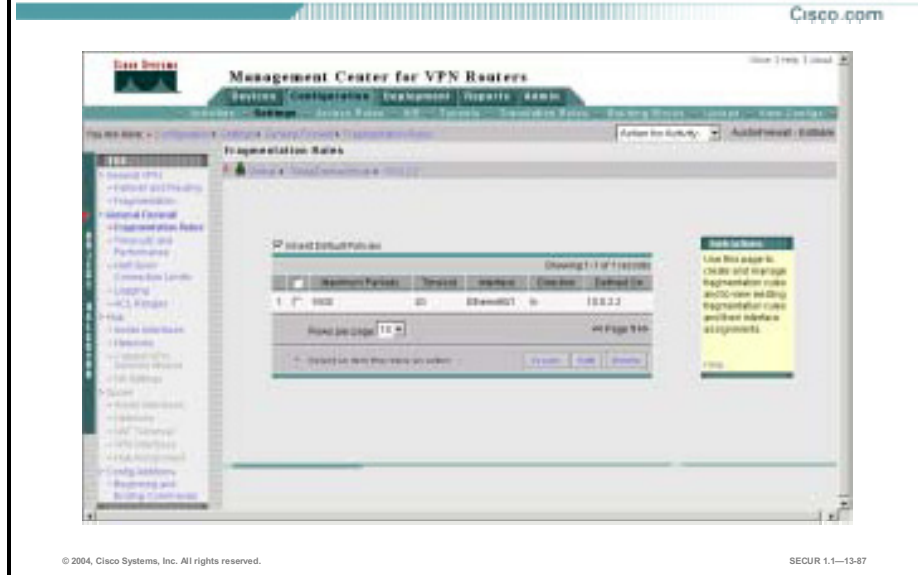
Fragmentation rules protect hosts from denial of service (DoS) attacks that involve fragmented IP packets. Fragmentation rules contain the following elements:

- Maximum packets—Enter the maximum number of packets that will be inspected in the fragmentation rule (Range: 50–10,000 packets).

- Timeout—Enter the maximum time (in seconds) that a connection for a given protocol in the fragmentation rule can remain active without any traffic passing through the router (Range: 1–1,000 seconds).

- Interface—Select the router interface that you wish to assign the fragmentation rule to.

- Direction—Select the direction on the router interface (In or Out) where the fragmentation rule is to be applied.

General Firewall>Timeouts and Performance
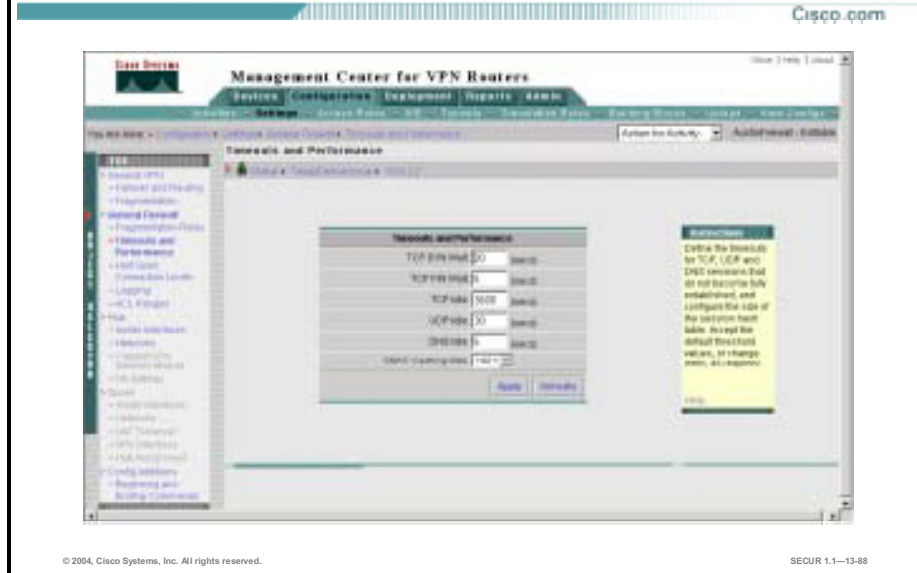
CBAC uses timeout and threshold values to manage session state information, to determine when to drop sessions that do not become fully established. These timeouts apply to all sessions that are inspected.

The Timeouts and Performance record contains the following elements:

- TCP SYN Wait—Enter the length of time (in seconds) the firewall will wait for a TCP session to reach the established state before dropping that session (Cisco IOS default: 30 seconds).

- TCP FIN Wait—Enter the length of time (in seconds) a TCP session will continue to be managed after the firewall detects the exchange has ended (Cisco IOS default: 5 seconds).

- TCP Idle—Enter the length of time (in seconds) a TCP session will continue to be managed after no activity is detected (Cisco IOS default: 3,600 seconds).

- UDP Idle—Enter the length of time (in seconds) a UDP session will continue to be managed after no activity is detected (Cisco IOS default: 5 seconds).

- DNS Idle—Enter the length of time (in seconds) a DNS name lookup session will continue to be managed after no activity is detected (Cisco IOS default: 5 seconds).

- CBAC Caching Size—Select a number that specifies the size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192 (Cisco IOS default: 1024).

General Firewall>Half-Open Connection Limits
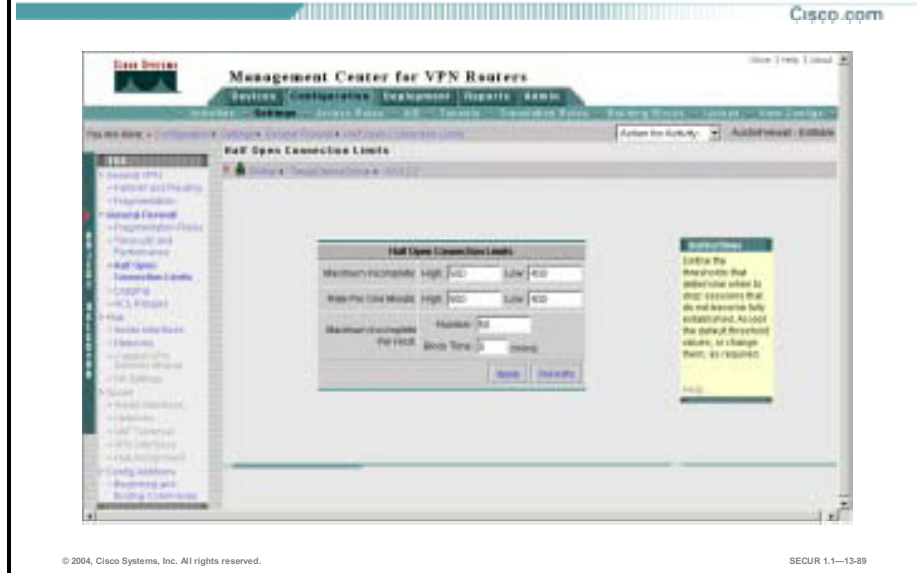
Half-open connections occur when a network attacker floods a server with a barrage of requests for connection and does not complete the connection. The resulting volume of half-open connections can overwhelm the server, causing it to deny service to valid requests.

The Half-Open Connection Limits record contains the following elements:

■ Maximum Incomplete: High—Enter the number of existing half open sessions that will cause the firewall to start deleting half open sessions, to accommodate new connection requests (Cisco IOS default: 500).

■ Maximum Incomplete: Low—Enter the number of existing half open sessions that will cause the firewall to stop deleting half open sessions (Cisco IOS default: 400).

■ Rate Per One Minute: High—Enter the rate of new session connection attempts (detected in the last one-minute sample period) that will cause the firewall to start deleting half open sessions, to accommodate new session attempts (Cisco IOS default: 500).

■ Rate Per One Minute: Low—Enter the rate of new session connection attempts (detected in the last one-minute sample period) that will cause the firewall to stop deleting half open session (Cisco IOS default: 400).

■ Maximum Incomplete Per Host: Number—Enter the number of existing half open sessions with the same destination host address, that will cause the firewall to start dropping half open sessions to that destination host address (Cisco IOS default: 50).

■ Maximum Incomplete Per Host: Block Time—Enter the length of time (in minutes) for the firewall to block a host that tried to open more than the specified number of connections per minute (Cisco IOS default: 0 minutes).

General Firewall>Logging

Cisco.com

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

SECUR 1.1—13-90
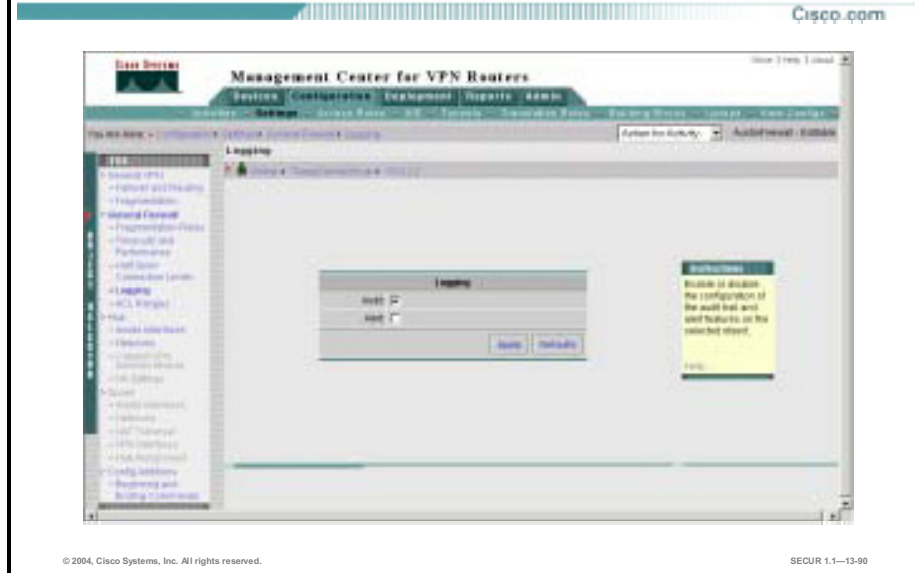
The Logging record allows you to enable or disable the configuration of the audit trail and alert features on the selected routers. By default, the Alert option is selected in Cisco IOS software.

Note	Deselecting the audit or alert options will disable these actions in the inspection rules and fragmentation rules policies upon deployment, for new policies only. Access rules that previously enabled these logging features will not be changed automatically.

■ Audit—Select this check box if you want inspection rules to configure audit trails to be generated on the selected routers (Cisco IOS default: enabled).

■ Alert—Select this check box if you want inspection rules to configure alert messages on the selected routers.

General Firewall>ACL Ranges

SECUR 1.1—13-91
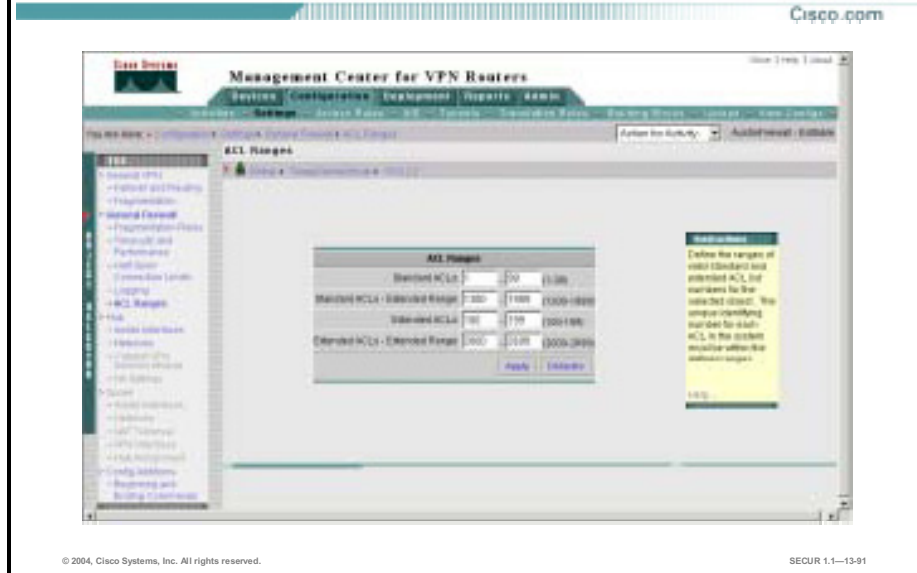
Both standard and extended type ACLs may be used when configuring CBAC on an outbound ACL (at an external interface), or inbound ACL (at an internal interface). Only extended ACLs can be used to deny CBAC return traffic from entering the network through the firewall. This means, when CBAC creates temporary openings in an ACL, the ACL must be an extended type ACL.

Each ACL on a router has a unique name or number that is used to identify it. Although names are usually used to identify ACLs, specific cases require ACLs to be identified by numbers, such as, when using Java-blocking in an HTTP inspection rule. When a number is used to identify an ACL, the number must be within the specific range of numbers that is valid for the protocol.

| **Note**	When uploading ACLs from a router, the uploaded ACLs might be numbered. The values of the ACL ranges will distinguish between Router MC ACLs and non-Router MC ACLs.

In the ACL Ranges record, you define the ranges of standard and extended ACL numbers. Since only 99 numbers are available for each type of ACL, Router MC provides an extended range of numbers for each of the standard and extended ACL types.

Building Access Rules

This topic explains how to build access rules using Router MC.

Router MC uses access rules to define your network security policy. When you configure firewall policies that will be deployed to devices, access rules provide traffic filtering by enabling the implementation of ACLs and CBAC inspection rules on the devices' interfaces.
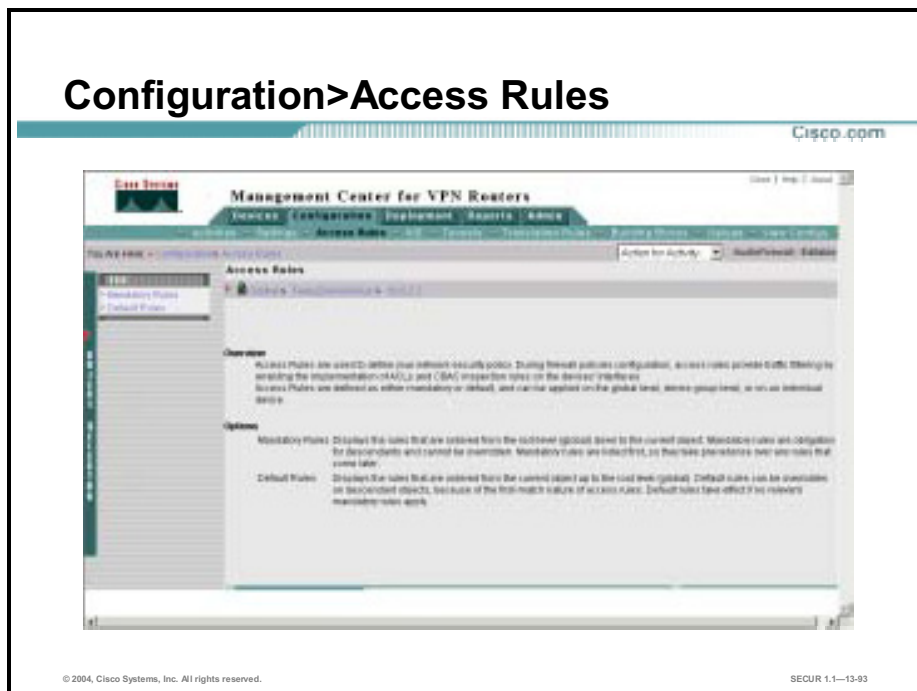
In Router MC, access rules are defined as either mandatory or default, and can be applied on the global level, device group level, or on an individual router.

■ Mandatory—Mandatory rules are obligatory for descendant objects and cannot be overridden. Mandatory rules are listed first, so they take precedence over any rules that come later.

■ Default—Default rules can be overridden on descendant objects, because of the first-match nature of access rules. Default rules take effect if no relevant mandatory rules apply.

Access Rule Elements

SECUR 1.1—13-94

Access rules are used to build ACLs and CBAC inspection rules for your router interfaces. Access rules contain the following elements:

- Source Address
- Destination Address
- Service (protocol)
- Action (permit, deny, inspect)
- Assigned Interface
- Enable (true or false)

Using Building Blocks

This topic explains how to use building blocks with Router MC.

Configuration>Building Blocks
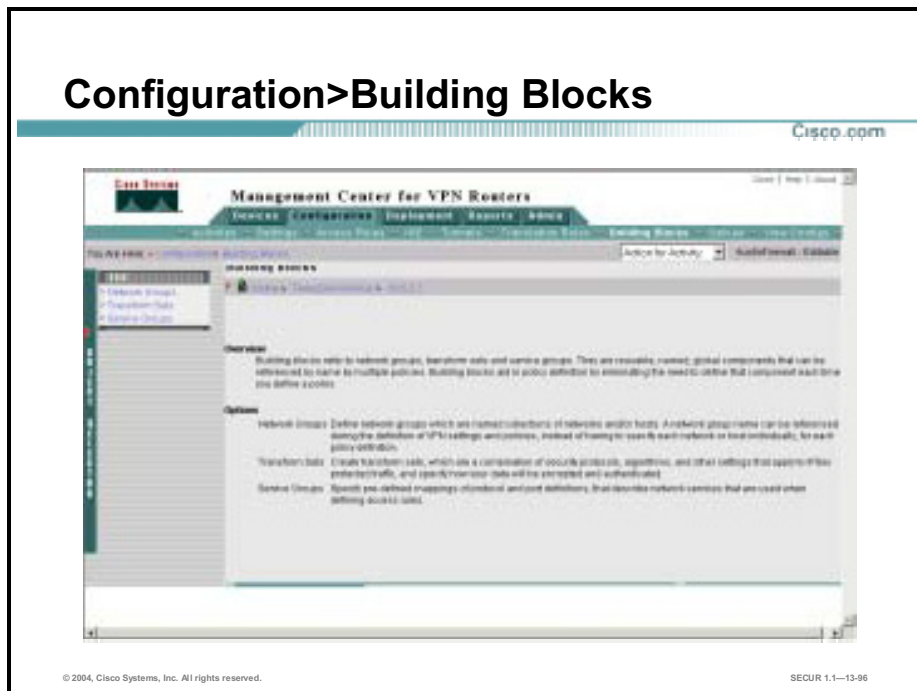
Building blocks are reusable, named, global components that can be referenced by multiple policies. When referenced, a building block is incorporated as an integral component of the policy. If you change the definition of a building block, this change is reflected in all policies that reference that building block.

Building blocks aid in policy definition by eliminating the need to define that component each time you define a policy. For example, although transform sets are integral to tunnel policies, you can define several transform sets independent of your tunnel policy definitions. These transform sets are always available for selection when you create tunnel policies (on the object on which you defined them and its descendants). The following building blocks can be defined:

- Transform sets—A combination of security protocols, algorithms and other settings that specify exactly how the data in the IPSec tunnel will be encrypted and authenticated. During the IPSec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

- Network groups—Named collections of networks and/or hosts. A network group name can be referenced during the definition of policies, instead of having to specify each network or host individually for each policy definition.

- Service groups—Named collections of protocol and port definition mappings that describe specific network services. Service groups can be referenced during the definition of access rules.
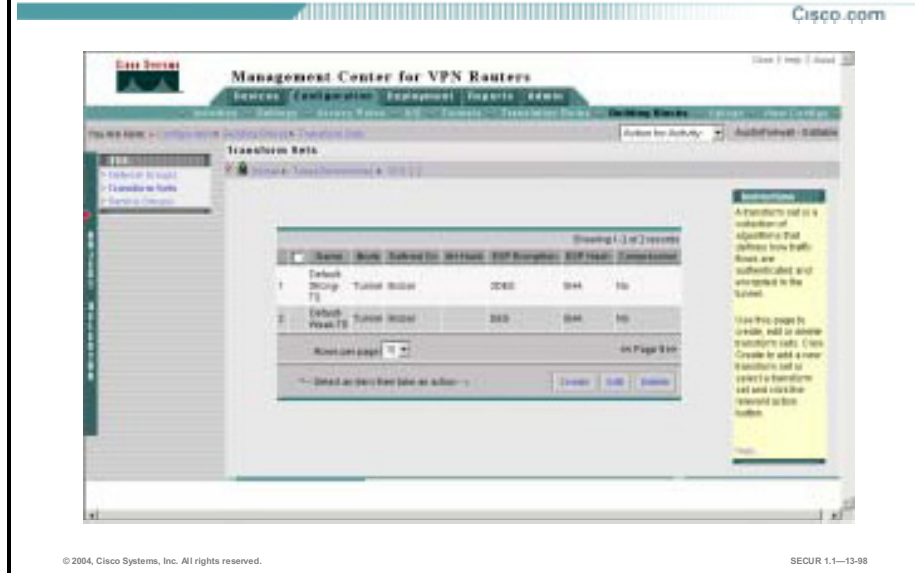
Network Groups

Network groups contain the following elements:

- Name—Enter a name for the new network group.
- Defined On—Enter a network for the new network group.

Transform Sets

Transform sets contain the following elements:

- Name—Enter a name for the new transform set.

- Mode—Select the mode for the new transform set.

- Defined On—Select the object group or object that the new transform set applies to.

- AH Hash—Select AH Hash if AH is being utilized for the new transform set.

- ESP Encryption—Select the ESP encryption method for the new transform set.

- ESP Hash—Select the ESP hash method for the new transform set.

- Compression—Select if compression is used for the new transform set.

View Service Groups
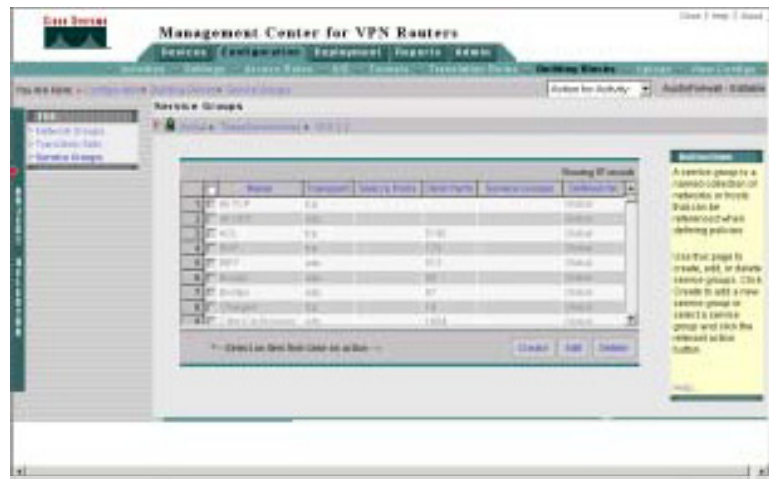
SECUR 1.1—13-99

Router MC 1.2.1 contains 97 predefined service groups.

Create New Service Group
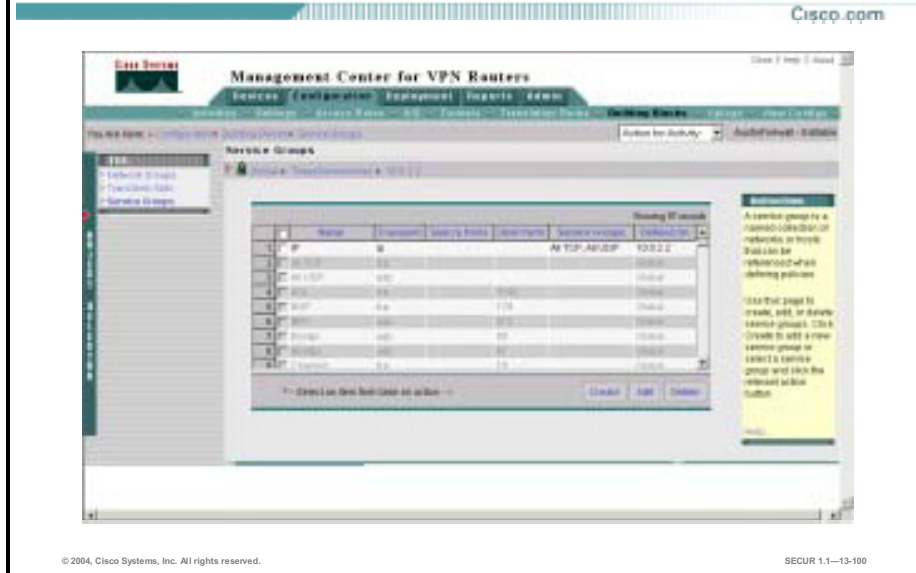
Service groups contain the following elements:

- Name—Enter a name for the new service group.

- Transport—Select the transport protocol for the new service group.

- Source Ports—Select the source ports for the new service group.

- Destination Ports—Select the destination ports for the new service group.

- Service Groups—Select the services to be part of the new service group.

- Defined On—Select the object to which the new service group is to be defined on.

Using Upload

This topic explains how to upload router configurations using the Router MC.
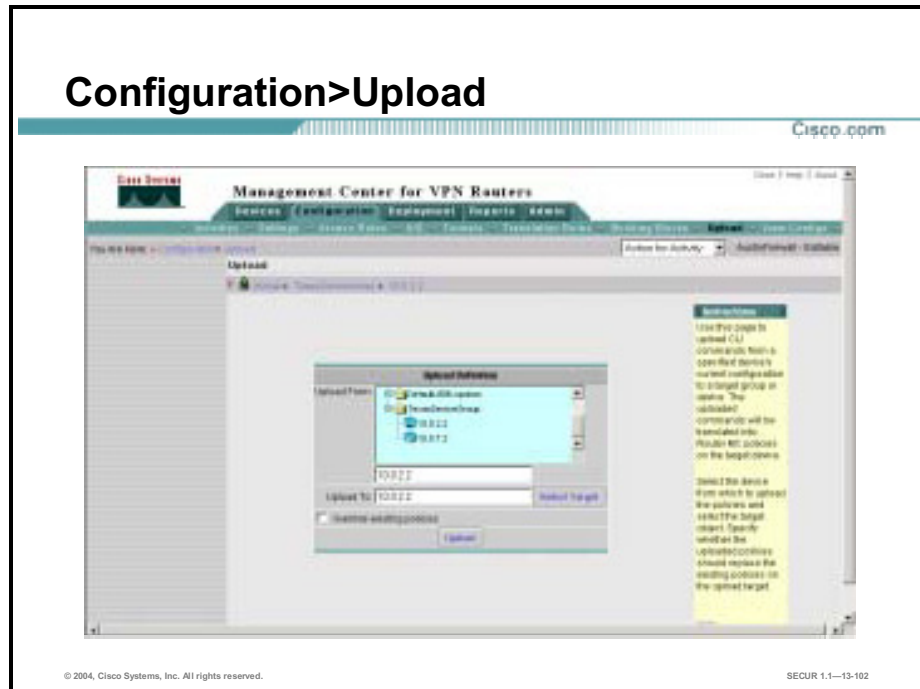
Upload refers to the process of transferring policies that exist on a router into Router MC. This means that you do not have to redefine all your VPN or firewall configurations when you start using Router MC, or when you want to copy policies from one device to other devices. Router MC only supports the upload of policies that are not peer-specific. These include transform sets, pre-shared keys, dynamic pre-shared keys, CA policies, routing policies, and IKE policies.

Note   Before you can upload policies from a physical router, you must first import the device.

Complete the following steps to upload policies from your router into the Router MC database:

Step 1   Select the router to upload from using the Upload From field.

Step 2   Select the target to upload to from the Upload Target dialog box.

Step 3   Select the **Override existing policies** checkbox if you wish to override any existing policies in the Router MC database for this router.

Step 4   Click **Upload**. The Upload Summary page opens.

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco.com

- **Router MC is a useful tool for configuring Cisco IOS router VPN policies.**
- **Router MC is a useful tool for configuring Cisco IOS Firewall policies.**

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

SECUR 1.1—13-104

Lab Exercise—Using Router MC

Complete the following lab exercise to practice what you learned in this lesson.

Objectives

The objective of this lab exercise is to work with a partner to configure Cisco routers that will enable a site-to-site VPN using the Router MC. In this lab exercise you will complete the following tasks:

- Complete the lab exercise setup.

- Enable the pod router to accept SSH connections.

- Install Router MC.

- Launch Router MC.

- Create an activity and a device group.

- Create a device inventory.

- Define VPN settings.

- Define an IKE policy.

- Define a tunnel policy.

- Deploy the configurations to the VPN routers.

- Test the configuration of the VPN routers.

Visual Objectives

The following figure displays the configuration you will complete in this lab exercise.
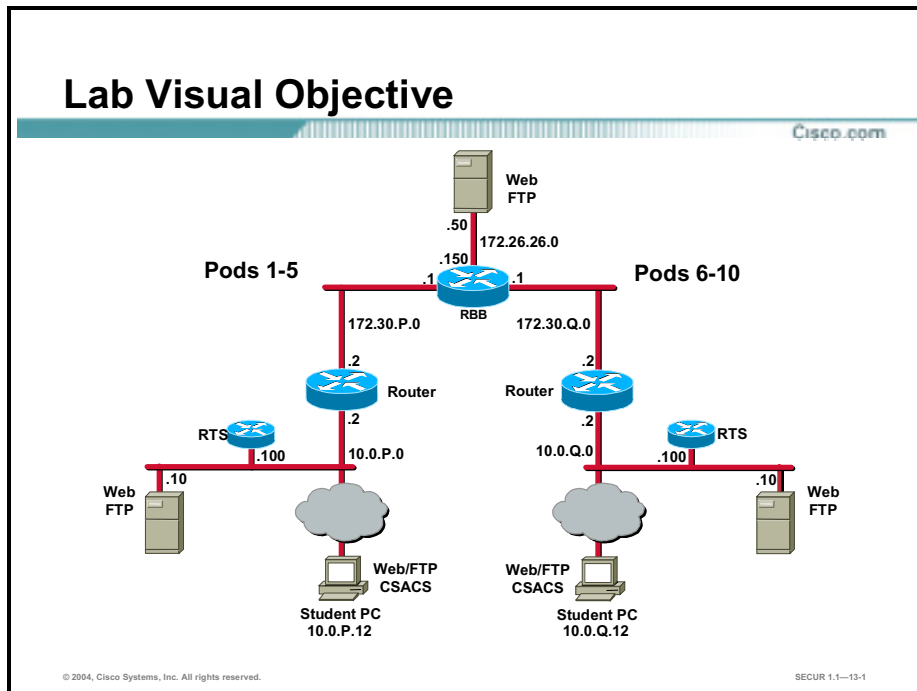
Note	The P in an IP address, name, or command indicates your pod number. Make sure to replace it with your pod number. The Q in an IP address, name, or command indicates the pod number of a peer pod assigned by the instructor. Make sure to replace it with your peer's pod number.

Task 1—Complete the Lab Exercise Setup

Complete the following steps to set up your lab exercise equipment:

Step 1 Ensure your router is turned on.

Step 2 Access the router's console port.

Step 3 (Optional.) Save your router's configuration from the previous lab exercise to a text file.

Step 4 Reset your router to the default configuration.

Step 5 Ensure you can ping from your router to the opposite pod group's router.

Step 6 Ensure that the CiscoWorks2000 (CiscoWorks) VMS Common Services have been installed on the student PC. Notify your instructor if the VMS common services are not installed.

Task 2—Enable the Pod Router to Accept SSH Connections

In this task, you will connect to your local router to turn on SSH. This allows Router MC to communicate with the router. Complete the following steps to configure your pod router to accept SSH connections:

Step 1 Telnet to the RTS and connect to the console port of your router.

Step 2 Enter configuration mode.

Step 3 Create a static route to the backbone router of the peer pod:

```
RP(config)# ip route 0.0.0.0 0.0.0.0 172.30.Q.1
```

(where P = pod number, and Q = peer pod number)

Step 4 Enable the router to use a secure AAA login:

```
RP(config)# aaa new-model
```

Step 5 Enter a local name and password to be used in the absence of other AAA statements:

```
RP(config)# username cisco password cisco
```

Step 6 Configure the pod router to use a domain name:

```
RP(config)# ip domain-name cisco.com
```

Step 7 Configure the pod router to generate a RSA key:

```
RP(config)# crypto key generate rsa usage-keys modulus 1024
The name for the keys will be: RP.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys …[OK]
% Generating 1024 bit RSA keys …[OK]
```

Step 8 Change the SSH timeout to 60 seconds and allow only two authentication retries:

```
RP(config)# ip ssh time-out 60
RP(config)# ip ssh authentication 2
RP(config)# end
```

Step 9 Write the configuration to memory.

Task 3—Install Router MC

Complete the following steps to install Router MC:

Step 1 Log in as the local administrator on the student PC.

Step 2 Verify the CiscoWorks VMS Common services are installed on the student PC.

Step 3 Locate and execute the Router MC installation files as directed to by your instructor. The InstallShield Wizard starts extracting files and the Router MC Installation window opens.

Step 4 Click **Next** to begin the installation. A Router MC window opens, prompting you to enter a password to the Router MC database.

Step 5 Enter a password of **cisco** in the Password field.

Step 6 Re-enter the password of **cisco** in the Confirm password field.

Step 7 Click **Next**. The Start Copying Files window opens.

Step 8 Confirm that the settings displayed are correct and click Next. The Setup Status window opens with a status bar that progresses with the installation of the Router MC.

Step 9 After the installation completes, the InstallShield Wizard Complete message box opens.

Step 10 Click **Yes, I want to restart my computer now** and then click **Finish**. The student PC will restart after you click Finish.

Task 4—Launch Router MC

Complete the following steps to log in to the CiscoWorks server and launch Router MC:

Step 1 Access the CiscoWorks server from your web browser by entering the following in the URL field:

http://127.0.0.1:1741

Be patient when connecting to the CiscoWorks server. The server requires additional software to be installed. The software is installed during the initial access. Subsequent attempts should not require the user to install additional software.

Note Select **Grant Always** when prompted to accept the Sun certificate to avoid future messages.

Step 2 Log in by entering the default username and password of **admin** and **admin**.

Note It is recommended to change the default admin account password.

Step 3 Click **Connect**. You are now logged in to the CiscoWorks desktop.

Step 4 Select the **VPN/Security Management Solution** drawer located in the left panel.

Step 5 Select the **Management Center** folder located in the VPN/Security Management Solution drawer.

Step 6 Select **VPN Routers** from the Management Center folder. The Security Alert page opens prompting you to accept a digital certificate.

Step 7 Click **Yes**. You are now logged in to the Router MC.

Step 8 Minimize the CiscoWorks browser page before proceeding to the next task.

Task 5—Create an Activity and a Device Group

Complete the following steps to create an activity and a device group:

Step 1 Select the **Configuration** tab. The Configuration page opens.

Step 2 Select **Create** from the Action for Activity list box. The Create New Activity dialog box opens.

Step 3 Enter **podP** in the name field and click **Create**. The new activity is created with the podP name listed next to the Action for Activity drop-down menu.
(where P = pod number)

Step 4 Select the **Devices** tab. The Devices page opens.

Step 5 Click **Device Hierarchy**. The Device Hierarchy page opens.

Step 6 Click **Create Group**. The Create Device Group page opens.

Step 7   Enter **podP** in the Name field.
(where P = pod number)

Step 8   Select the **Global** folder to create the group in.

Step 9   Click **Create**. The Device Hierarchy page refreshes.

Step 10   Click **Create Group**. The Create Device Group page opens.

Step 11   Enter **podP-hubs** in the Name field.
(where P = pod number)

Step 12   Select the **podP** folder to create the group in.
(where P = pod number)

Step 13   Click **Create**. The Create Device Group page closes, and the Device Hierarchy page is refreshed with the new group.

Step 14   Click **Create Group**. The Create Device Group page opens.

Step 15   Enter **podP-spokes** in the Name field.
(where P = pod number)

Step 16   Select the **podP** folder to create the group in (where P = pod number).

Step 17   Click **Create**. The Device Hierarchy page is refreshed with the new group.

Task 6—Create a Device Inventory

In this task, you will import your pod router as a hub. Then, you will import your peer's pod router as a spoke. Complete the following steps to create a device inventory:

Step 1   Select the **Devices** tab. The Devices page opens.

Step 2   Select **Device Import**. The Device Import page opens.

Step 3   Click **Import**. The Choose Method page opens.

Step 4   Select the **Single device import** radio button and click **Next**. The Import Parameters page opens.

Step 5   Complete the following substeps to configure the parameters:

1. Select the **Device IP/Name** radio button.

2. Enter **10.0.P.2** in the Device IP/Name field.
(where P = pod number)

3. Enter **cisco** in the Username field.

4. Enter **cisco** in the Password field.

5. Enter **cisco** in the Enable Password field.

Step 6   Click **Next**. The Import Devices page opens.

Step 7   Select **Hub/Firewall** from the Role list box and click **Next**. The Select Target Device Group page opens.

Step 8 Select **podP-hubs** from Import To: field in the Select Target Device Group area, and click **Next** (where P = pod number). The Device Import Summary page opens.

Step 9 Verify that the information displayed is correct and click **Finish**. The Last Import Status page opens.

Note	The Import Status page refreshes roughly every 10 seconds, providing an update on the import status.

Step 10 Click **Close** to close the Last Import Status page.

Step 11 Select **Import** from the Device Import window. The Choose Import Method page opens.

Step 12 Select the **Single device import** radio button and click **Next**. The Import Parameters page opens.

Step 13 Complete the following substeps to configure the parameters:

1. Select the **Device IP/Name** radio button.

2. Enter **172.30.Q.2** in the Device IP/Name field.
   (where Q = peer pod number)

3. Enter **cisco** in the Username field.

4. Enter **cisco** in the Password field.

5. Enter **cisco** in the Enable Password field.

Step 14 Click **Next**. The Import Devices page opens.

Step 15 Select **Spoke** from the Role list box and click **Next**. The Select Target Device Group page opens.

Step 16 Select **podP-spokes** from the Select Target Device Group Import To: field and click **Next** (where P = pod number). The Device Import Summary page opens.

Step 17 Verify that the information displayed is correct and click **Finish**. The Last Import Status page opens.

Note	The Import Status page refreshes roughly every 5 seconds, providing an update on the import status.

Step 18 Click **Close** to close the Last Import Status page.

Task 7—Define VPN Settings

You will complete this task by configuring the hub inside interface settings, spoke inside interface settings, and VPN interface settings. Complete the following steps to define VPN settings:

Step 1 Complete the following substeps to configure the hub router's inside interface settings:

1. Choose **Configuration>Settings**. The Settings page opens.

2. Select the red triangle at left border of page to access the Object Selector.

3. Select **podP-hubs** using the Object Selector.
   (where P = pod number)

4. Select **Hub>Inside Interfaces** from the TOC. The Hub Inside Interfaces page opens.

5. Click **Show Interfaces**. The Show Interfaces dialog box opens.

6. Select the **Fast Ethernet0/0** check box and click **Select**. The Show Interfaces page closes and the Hub Inside Interfaces page refreshes with Fast Ethernet0/0 listed.

7. Click **Apply**. The Hub Inside Interfaces page is refreshed to indicate that the Router MC received the changes.

Step 2 Complete the following substeps to configure the spoke router's inside interface settings:

1. Select **podP-spokes** using the Object Selector.
   (where P = pod number)

2. Select **Spoke>Inside Interfaces** from the TOC. The Spoke Inside Interfaces page opens.

3. Click **Show Interfaces**. The Show Interfaces dialog box opens.

4. Select the **Fast Ethernet0/0** check box and click **Select**. The Show Interfaces page closes and the Spoke Inside Interfaces page refreshes with Fast Ethernet0/0 listed.

5. Click **Apply**. The Spoke Inside Interfaces page is refreshed to indicate that the Router MC received the changes.

Step 3 Complete the following substeps to configure the spoke router's VPN interface settings:

1. Select **Spoke>VPN Interfaces** from the TOC. The Spoke VPN Interfaces page opens.

2. Click **Show Interfaces**. The Show Interfaces page opens.

3. Select the **Fast Ethernet0/1** radio button and click **Select**. The Show Interfaces page closes and the Spoke VPN Interfaces page refreshes with Fast Ethernet0/1 listed.

4. Click **Validate** to list the number of devices that support that interface. The Validate Interface page opens.

5. Verify that the Supported column displays Yes and click **Close**. The Validate Interface page closes and the Spoke VPN Interfaces page opens.

6. Click **Apply**. The Spoke VPN Interface page is refreshed, indicating that the Router MC received the changes.

Step 4 Complete the following substeps to configure the spoke router's hub assignment:

1. Select **Spoke>Hub Assignment**. The Hub Assignment page opens.

2. Select the hub router (**10.0.P.2)** from the Primary Hub list box (where P = pod number).

3. Select a VPN interface of **Fast Ethernet0/1** from the Primary Interface list box. Do not select either a failover hub or a failover interface at this time.

4. Click **Apply**. The Hub Assignment page is refreshed to indicate the Router MC received the changes.

Task 8—Define an IKE Policy

In this task, you will learn how to define an IKE policy using moderate security for authentication and encryption for the podP group (where P = pod number). In this task, you will use a dynamic pre-shared key as the authentication method.

Step 1   Select **podP** using the Object Selector (where P = pod number).

Step 2   Select **IKE**. The IKE page opens.

Step 3   Select **IKE Policies** from the TOC. The IKE Policies page opens.

Step 4   Click **Create**. The Name and Comment page opens.

Step 5   Enter **podP-IKE-Policy** in the Name field and click **Next**. The Algorithms page opens (where P = pod number).

Step 6   Complete the following substeps to configure the IKE algorithms:

1. Select **3DES** from the Encryption Algorithm list box.

2. Select **MD5** from the Hash Algorithm list box.

3. Select **2** from the Modulus Group list box.

Step 7   Click **Next**. The Parameters page opens.

Step 8   Enter **86400** in the Lifetime (seconds) field and select **Preshared Key** from the Authentication list box.

Step 9   Click **Next**. The Summary of IKE Policy page opens.

Step 10   Verify that the information displayed in the Summary of IKE Policy page is correct and click **Finish**. The IKE Policies page opens, listing the podP-IKE-Policy as a higher priority than the default IKE policy (where P = pod number).

Task 9—Define a Tunnel Policy

In this task, you will create a transform set and apply it to a tunnel while you are defining the tunnel settings. You will apply security using a transform set with moderate authentication, encryption, and compression settings. Complete the following steps to define a tunnel policy for your routers:

Step 1   Select **Configuration>Tunnels**. The Tunnels page opens.

Step 2   Select **Tunnel Policies** from the TOC. The Tunnel Policies page opens.

Step 3   Click **Create**. The Name and Comment page opens.

Step 4   Enter **podP-Tunnel-Policy** in the Name field (where P = pod number).

Step 5   Click **Next**. The Traffic Filter page opens. View the predefined ACEs.

Step 6   Click **Next**. The Transform Sets page opens.

Step 7   Click **Create**. The Name and Comment page opens.

Step 8   Enter **podP-TS** in the Name field (where P = pod number).

Step 9   Click **Next**. The Protocols page opens.

Step 10 Select **Tunnel** from the Mode list box.

| **Note** | Do not select anything from the **AH-Hash** list box. |

Step 11 Select **3DES** from the ESP Encryption list box.

Step 12 Select **MD5** from the ESP Hash list box.

| **Note** | Do not select the **Compression** check box. |

Step 13 Click **Next**. The Summary page opens.

Step 14 Click **Finish**. The new transform set is created and the Transform Sets page opens.

Step 15 Select the new **podP-TS** transform set from the Transform Set 1 list box.

Step 16 Click **Next**. The PFS page opens.

| **Note** | Do not select anything in the PFS page. |

Step 17 Click **Next**. The Summary page opens.

Step 18 Click **Finish**. The tunnel policy is created and the main Tunnel Policies page refreshes.

Task 10—Deploy the Configurations to the VPN Routers

Complete the following steps to deploy the configurations to the VPN routers:

| **Caution** | Only one pod should proceed with the rest of this lab exercise. Work with your peer pod to determine who will actually deploy the configurations. Do not attempt to deploy the configurations to the same routers at the same time. |

Step 1 Select **Approve** from the Action for Activity list box. The Approve Activity dialog box opens.

Step 2 Enter your initials and an appropriate comment in the Comment field.

Step 3 Click **OK**. The activity is approved.

Step 4 Choose **Deployment>Jobs**. The Jobs page opens.

Step 5 Click **Create**. The Name and Description page opens.

Step 6 Enter **podP Job** in the Name field (where P = pod number).

Step 7 Click **Next**. The Select Devices page opens. Your routers should already be selected. If not, select them now.

Step 8 Click **Next**. The Deployment Options page opens.

Step 9 Select the **Device** radio button in the Deploy To list box.

Step 10 Select the **Deploy only to running config** check box.

Step 11   Click **Next**. The Error Checking page opens to let you know it might take awhile for the configuration to be checked prior to deployment. Then, the Error Checking page opens with any warnings or error messages.

Note	You will receive some warnings. These warnings let you know that several of the predefined network groups are not necessary when deploying to the routers. Ignore this warning, as it does not affect the configuration deployment. If you receive an error message, it will be necessary to examine the error message and correct the problem before continuing.

Step 12   Click **Next**. The Summary page opens.

Step 13   Verify that the information displayed is correct and click **Finish**. The Deploy On Finish message box opens.

Step 14   Click **Yes** to deploy the job now. The Job Deployment Status page opens.

Step 15   Click **Refresh** to obtain an updated view of the job and router states.

Step 16   Select **Deployment>View Configs**. The Current page opens.

Step 17   Scroll through the Current Configuration window to view the configuration deployed to the device group.

Step 18   Click **Refresh** to view the job's deployment status. When the VPN Connection Status reads Connected, you will know that your VPN is set up and working.

Note	You may also telnet into the podP router and use the **sh crypto ipsec sa** command to view the packet counts, (where P = pod number). If the packet counts increase with a ping to the remote student workstation, 10.0.Q.12, then you will know if the connection is working, (where Q = peer pod number).

Task 11—Test the Configuration of the VPN Routers

Now that you have configured the VPN parameters, you need to test them by building a VPN tunnel between the hub and spoke routers.

Step 1   Ping from the hub router to the spoke router.

Step 2   View the VPN statistics on the router using the **show crypto isakmp sa** and **show crypto ipsec sa** commands.