

SNRS

Securing Networks with Cisco Routers and Switches

Volumes 1 & 2

Version 1.0

Student Guide

CLS Production Services: 06.28.05

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

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

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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

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

Table of Contents

Volume 1

<i>Course Introduction</i>	1
Overview	1
Learner Skills and Knowledge	2
Course Goal and Objectives	3
Course Flow	4
Additional References	5
Cisco Glossary of Terms	5
<i>Cisco Secure Access Control Server for Windows Server</i>	1-1
Overview	1-1
Module Objectives	1-1
<i>Deploying Cisco Secure Access Control Server for Windows Server</i>	1-3
Overview	1-3
Objectives	1-3
Cisco Secure ACS for Windows Server Product Overview	1-4
Product Overview: Cisco Secure ACS for Windows Server	1-4
Authentication and User Databases	1-7
AAA Protocols—TACACS+ and RADIUS	1-9
Comparing TACACS+ and RADIUS	1-11
Passwords	1-13
Administration	1-14
Key Features in Cisco Secure ACS 3.3	1-16
AAA Servers in Distributed Systems	1-18
System Requirements	1-20
Keeping Databases Current	1-22
Database Replication	1-22
RDBMS Synchronization	1-24
ODBC Import Definitions	1-25
Cisco Secure ACS for Windows Server Architecture	1-26
How Cisco Secure ACS Authenticates Users	1-28
Cisco Secure ACS User Database	1-28
User-Changeable Passwords	1-34
Summary	1-35
<i>Configuring RADIUS and TACACS+ with Cisco Secure ACS for Windows Server</i>	1-37
Overview	1-37
Objectives	1-37
Installing Cisco Secure ACS	1-38
Gathering Answers for the Installation Questions	1-38
Preconfigure the Windows 2000 Server System	1-40
Verify Connections Between Windows 2000 Server System and Other Network Devices	1-41
Install Cisco Secure ACS for Windows Server on the Windows 2000 Server System	1-41
Configure Cisco Secure ACS for Windows Server Using the Web Browser	1-41
Configure Remaining Devices for AAA	1-42
Creating a Cisco Secure ACS Installation	1-42
Administering Cisco Secure ACS for Windows Server	1-47
Navigation Buttons	1-47
Troubleshooting	1-49
Authentication Failure	1-49
Authorization Failure	1-50
No Entry in the Failed Attempts Report	1-50
Dial-In Client PC Problems	1-50
Other Troubleshooting Tips	1-51
Useful Cisco IOS Commands	1-51
TACACS+	1-52
TACACS+ Overview	1-52

Enabling TACACS+	1-53
Verifying TACACS+	1-60
RADIUS	1-65
Client-Server Model	1-65
Network Security	1-65
Configuring RADIUS	1-66
Summary	1-68
Module Summary	1-69
Cisco IOS Security Features	2-1
Overview	2-1
Module Objectives	2-1
Introducing Cisco IOS Firewall Context-Based Access Control	2-3
Overview	2-3
Objectives	2-3
Cisco IOS Firewall Feature Set	2-4
Creating a Customized Firewall	2-5
Context-Based Access Control	2-6
Authentication Proxy	2-6
Intrusion Prevention System	2-6
Context-Based Access Control	2-7
Authentication Proxy	2-8
Intrusion Prevention System	2-9
Cisco IOS ACLs	2-10
CBAC Process	2-11
Summary	2-15
Configuring Cisco IOS Firewall Context-Based Access Control	2-17
Overview	2-17
Objectives	2-17
CBAC Configuration Tasks	2-18
Picking an Interface: Internal or External	2-19
Configuring IP Access Lists at the Interface	2-19
Basic Configuration	2-20
External Interface	2-21
Internal Interface	2-21
Audit Trail Logging	2-22
Global Timeouts and Thresholds	2-23
Port-to-Application Mapping	2-31
Define Inspection Rules	2-37
Apply Inspection Rules and ACLs to Interfaces	2-49
Test and Verify	2-58
Summary	2-61
Configuring Cisco IOS Firewall Authentication Proxy	2-63
Overview	2-63
Objectives	2-63
Cisco IOS Firewall Authentication Proxy	2-64
AAA Server Configuration	2-69
AAA Configuration	2-73
Authentication Proxy Configuration	2-80
Test and Verify	2-84
Summary	2-87
Configuring Cisco IOS Firewall Intrusion Prevention System	2-89
Overview	2-89
Objectives	2-89
Cisco IOS Firewall Intrusion Prevention System	2-90
Features and Benefits	2-92
Origin of Cisco IOS Firewall IPS	2-93
Signature Micro-Engines	2-93

Signatures	2-93
The Signature Definition File	2-94
Attack-drop.sdf	2-94
Cisco IOS Firewall IPS Configuration Tasks	2-100
Installing the Cisco IOS Firewall IPS	2-101
Configure Logging via Syslog or SDEE	2-104
SDEE Overview	2-105
Benefits	2-105
Storing SDEE Events in the Buffer	2-106
Upgrading to the Latest Cisco IOS Firewall IPS Signature Definition File	2-108
Verifying the Configuration	2-110
Summary	2-114
Module Summary	2-115
<u>Layer 2 Security</u>	3-1
Overview	3-1
Module Objectives	3-1
<u>Mitigating Layer 2 Attacks</u>	3-3
Overview	3-3
Objectives	3-3
Types of Attacks	3-4
CAM Table Overflow Attack	3-5
MAC Flooding	3-6
Mitigating the CAM Table Overflow Attack	3-7
Port Security	3-8
MAC Spoofing—Man-in-the-Middle Attacks	3-11
Mitigating MAC Spoofing Attacks	3-12
Using DHCP Snooping	3-13
Address Resolution Protocol Spoofing	3-13
Solution	3-13
DHCP Starvation Attacks	3-17
Mitigating DHCP Starvation Attacks	3-18
Summary	3-19
<u>Configuring Cisco Identity-Based Networking Services</u>	3-21
Overview	3-21
Objectives	3-21
IBNS Overview	3-22
Features and Benefits	3-22
IEEE 802.1x	3-25
802.1x and EAP	3-29
802.1x Components	3-30
802.1x Technology	3-30
802.1x Applications with Cisco IOS Software	3-31
802.1x in Cisco IOS Increases Network Security and Reliability	3-31
Device Roles	3-32
How 802.1x Works	3-33
Authentication Initiation and Message Exchange	3-33
Ports in Authorized and Unauthorized States	3-34
Selecting the Correct EAP	3-36
Cisco LEAP	3-39
EAP-TLS	3-40
PEAP	3-41
EAP Type Configuration	3-41
Cisco Secure ACS	3-42
AAA in a Cisco Catalyst Switch (802.1x and EAPOL) Environment	3-42
Network Topology	3-44
Network Access Policy	3-46
Cisco Secure ACS RADIUS Profile Configuration	3-46
Summary	3-48

Configuring 802.1x Port-Based Authentication **3-51**

Overview	3-51
Objectives	3-51
802.1x Port-Based Authentication Configuration Tasks	3-52
Configuring 802.1x Authentication	3-52
Default 802.1x Configuration	3-54
802.1x Configuration Guidelines	3-55
Enabling 802.1x Authentication	3-56
Configuring the Switch-to-RADIUS Server Communication	3-59
Enabling Periodic Reauthentication	3-61
Manually Reauthenticating a Client Connected to a Port	3-63
Enabling Multiple Hosts	3-64
Resetting the 802.1x Configuration to the Default Values	3-66
Displaying 802.1x Statistics and Status	3-67
Summary	3-69

Identifying Layer 2 Security Best Practices **3-71**

Overview	3-71
Objectives	3-71
Factors Affecting Layer 2 Mitigation Techniques	3-72
Single Security Zone, One User Group, One Physical Switch	3-74
Vulnerabilities	3-74
Mitigation	3-75
Single Security Zone, One User Group, Multiple Physical Switches	3-76
Vulnerabilities	3-76
Mitigation	3-77
Single Security Zone, Multiple User Groups, Single Physical Switch	3-78
Vulnerabilities	3-78
Mitigation	3-78
Single Security Zone, Multiple User Groups, Multiple Physical Switches	3-79
Vulnerabilities	3-79
Mitigation	3-80
Multiple Security Zones, One User Group, Single Physical Switch	3-81
Vulnerabilities	3-81
Mitigation	3-82
Multiple Security Zones, One User Group, Multiple Physical Switches	3-83
Vulnerabilities	3-83
Mitigation	3-84
Multiple Security Zones, Multiple User Groups, Single Physical Switch	3-85
Vulnerabilities	3-85
Mitigation	3-86
Multiple Security Zones, Multiple User Groups, Multiple Physical Switches	3-87
Vulnerabilities	3-87
Mitigation	3-88
Best Practices	3-89
Summary	3-92
Module Summary	3-93

Cisco IOS-Based VPNs Using Cisco Pre-Shared Keys **4-1**

Overview	4-1
Module Objectives	4-1

Preparing a Network for IPSec Configuration with Pre-Shared Keys **4-3**

Overview	4-3
Objectives	4-3
Configuring IPSec Encryption with Pre-Shared Keys	4-4
Planning the IKE and IPSec Policy	4-5
Step 1—Determine ISAKMP (IKE Phase 1) Policy	4-6
Create IKE Policies for a Purpose	4-8
Define IKE Policy Parameters	4-9

Step 2—Determine IPsec (IKE Phase 2) Policy	4-11
Step 3—Check the Current Configuration	4-16
Step 4—Ensure That the Network Works Without Encryption	4-19
Step 5—Ensure That ACLs Are Compatible with IPsec	4-20
Summary	4-22
Configuring Internet Key Exchange with Pre-Shared Keys	4-23
Overview	4-23
Objectives	4-23
Configuring the IKE Policy	4-24
Step 1—Enable or Disable ISAKMP	4-25
Step 2—Create IKE Policies	4-27
Why Do You Need to Create These Policies?	4-27
Parameters Defined in a Policy	4-28
Setting ISAKMP Identity	4-31
Step 3—Configure Pre-Shared Keys	4-32
Step 4—Verify the ISAKMP Configuration	4-34
Summary	4-35
Configuring IPsec	4-37
Overview	4-37
Objectives	4-37
Configuring IPsec	4-38
Step 1—Configure Transform Sets	4-40
Edit Transform Sets	4-42
Step 2—Configure Global IPsec SA Lifetimes	4-44
How These Lifetimes Work	4-45
Step 3—Create Crypto ACLs	4-47
Defining Mirror-Image Crypto ACLs at Each IPsec Peer	4-50
Step 4—Create Crypto Maps	4-52
Step 5—Apply Crypto Maps to Interfaces	4-58
IPsec Configuration Example	4-60
Summary	4-62
Testing and Verifying IPsec Configuration	4-63
Overview	4-63
Objectives	4-63
Testing and Verifying IPsec	4-64
Display Your Configured ISAKMP Policies	4-66
Display Your Configured Transform Sets	4-67
Display the Current State of Your IPsec SAs	4-68
Display Your Configured Crypto Maps	4-69
Enable Debug Output for IPsec Events	4-70
Enable Debug Output for ISAKMP Events	4-73
Summary	4-76
Module Summary	4-77

Volume 2

<i>Cisco IOS-Based VPNs Using Certificate Authorities</i>	5-1
Overview	5-1
Module Objectives	5-1
Preparing a Network for IPsec Configuration Using Certificate Authorities	5-3
Overview	5-3
Objectives	5-4
Overview of CA Support	5-5
Restrictions	5-6
Prerequisites	5-6
Overview of CAs	5-7
Simple Certificate Enrollment Protocol Overview	5-9

Entrust Technologies	5-12
VeriSign OnSite	5-12
Microsoft Windows 2000 Certificate Services	5-13
Configuring IPsec Encryption with Digital Certificates	5-15
Planning the ISAKMP and IPsec Policy	5-16
Step 1—Plan for CA Support	5-18
Step 2—Determine ISAKMP (IKE Phase 1) Policy	5-20
Creating ISAKMP Policies for a Purpose	5-22
Defining ISAKMP Policy Parameters	5-23
Step 3—Determine IPsec (IKE Phase 2) Policy	5-25
Step 4—Check the Current Configuration	5-30
Step 5—Ensure That the Network Works Without Encryption	5-32
Step 6—Ensure That ACLs Are Compatible with IPsec	5-33
Summary	5-35
Configuring Certificate Authority on Cisco Routers	5-37
Overview	5-37
Objectives	5-37
Configuring Certificate Authorities	5-38
Step 1—Manage the NVRAM Use	5-40
Step 2—Set the Router Time and Date	5-42
Step 3—Add a CA Server Entry to the Router Host Table	5-44
Step 4—Generate an RSA Key Pair	5-46
Special-Usage Keys	5-47
General-Purpose Keys	5-48
Step 5—Declare a CA	5-49
Step 6—Authenticate the CA	5-52
Step 7—Request Your Own Certificate	5-53
Step 8—Save the Configuration	5-55
Step 9—Monitor and Maintain CA Interoperability	5-56
Requesting a CRL	5-57
Deleting RSA Keys from Your Router	5-58
Deleting Certificates from the Configuration	5-58
Deleting the Public Keys from a Peer	5-59
Step 10—Verify the CA Support Configuration	5-60
Summary	5-63
Configuring ISAKMP and IPsec on Cisco Routers	5-65
Overview	5-65
Objectives	5-65
Step 1—Enable or Disable ISAKMP	5-66
Step 2—Create ISAKMP Policies	5-68
Step 3—Set the ISAKMP Identity Address or Host Name	5-71
Step 4—Test and Verify the ISAKMP Configuration	5-73
Step 5—Configure Transform Set Suites	5-74
Edit Transform Sets	5-76
Step 6—Configure Global IPsec SA Lifetimes	5-77
Step 7—Configure Crypto ACLs	5-79
Defining Mirror-Image Crypto ACLs at Each IPsec Peer	5-82
Step 8—Configure Crypto Maps	5-84
Step 9—Apply Crypto Map to Interface	5-87
Summary	5-91
Testing and Verifying an IPsec CA Configuration	5-93
Overview	5-93
Objectives	5-93
Step 1—Display Configured ISAKMP Policies	5-94
Step 2—Display Configured Transform Sets	5-95
Step 3—Display the Current State of IPsec SAs	5-96
Step 4—View Configured Crypto Maps	5-97
Step 5—Debug IPsec Traffic	5-98

Step 6—Debug ISAKMP Traffic	5-101
Step 7—Debug CA Events with Cisco IOS Software	5-103
The debug crypto pki messages Command	5-103
Summary	5-105
Module Summary	5-106
<i>Cisco IOS Remote Access Using Cisco Easy VPN</i>	6-1
Overview	6-1
Module Objectives	6-1
Introducing Cisco Easy VPN	6-3
Overview	6-3
Objectives	6-3
Introduction to Cisco Easy VPN	6-4
Cisco Easy VPN Server	6-5
Cisco Easy VPN Remote	6-5
Restrictions for Cisco Easy VPN Remote	6-9
How Cisco Easy VPN Works	6-11
Step 1—Authentication Begins	6-12
Step 2—An IKE SA Is Established	6-13
Step 3—Cisco Easy VPN Server Authenticates the Device	6-14
Step 4—Username and Password Challenge Is Processed	6-15
Step 5—Mode Configuration	6-16
Step 6—The RRI Process Is Initiated	6-17
Step 7—Connection Is Completed with IPsec Quick Mode	6-18
Summary	6-19
Configuring the Easy VPN Server	6-21
Overview	6-21
Objectives	6-21
Cisco Easy VPN Server Configuration Tasks	6-22
Task 1—Create IP Address Pool	6-23
Task 2—Configure Group Policy Lookup	6-24
Task 3—Create ISAKMP Policy for Remote VPN Client Access	6-25
Task 4—Define Group Policy for Mode Configuration Push	6-26
Task 5—Create a Transform Set	6-33
Task 6—Create a Dynamic Crypto Map with RRI	6-34
Task 7—Apply Mode Configuration to the Crypto Map	6-38
Task 8—Apply the Crypto Map to the Router Interface	6-42
Task 9—Enable ISAKMP DPD	6-43
Task 10—Configure or Disable Extended Authentication	6-44
Task 11—Enable Xauth Save Password Feature	6-48
Task 12—Verify	6-50
Summary	6-51
Configuring Easy VPN Remote for the Cisco VPN Client 4.x	6-53
Overview	6-53
Objectives	6-53
Cisco VPN Client 4.x Configuration Tasks	6-54
Task 1—Install Cisco VPN Client	6-55
Verifying System Requirements	6-56
Gathering the Information That You Need	6-57
Installing the VPN Client Through InstallShield	6-57
Installing the VPN Client through Microsoft Windows Installer	6-58
Task 2—Create New Client Connection Entries	6-60
Creating a New Connection Entry	6-61
Task 3—Configure Client Authentication Properties	6-62
Group Authentication	6-62
Mutual Group Authentication	6-63
Certificate Authentication	6-63
Task 4—Configure Transparent Tunneling	6-64

Enabling Transparent Tunneling	6-64
Allowing Local LAN Access	6-65
Task 5—Enable and Add Backup Servers	6-67
Task 6—Configure Connection to the Internet Through Dial-Up Networking	6-68
Summary	6-69
Configuring Cisco Easy VPN Remote for Access Routers	6-71
Overview	6-71
Objectives	6-71
Easy VPN Remote Modes of Operation	6-72
Cisco Easy VPN Remote Features	6-76
Configuration Tasks for Cisco Easy VPN Remote for Access Routers	6-78
Task 1—Configure the DHCP Server Pool	6-79
Task 2—Configure and Assign the Cisco Easy VPN Client Profile	6-81
Task 3—Configure Xauth Password Save	6-83
Task 4—Initiate the VPN Tunnel	6-84
Task 5—Verify the Cisco Easy VPN Configuration	6-85
Summary	6-87
Module Summary	6-88
Cisco Router and Security Device Manager	7-1
Overview	7-1
Module Objective	7-1
Using Cisco Router and Security Device Manager	7-3
Overview	7-3
Objectives	7-3
Cisco SDM Overview	7-4
Router Configuration	7-12
Monitoring and Troubleshooting	7-13
Cisco SDM Software	7-15
Task 1: Download the Cisco SDM Files and a Cisco IOS Image to a TFTP Server	7-19
Task 2: Configure Your Router to Support Cisco SDM	7-20
Task 3: Copy the Cisco SDM Files to the Router	7-21
Task 4: Start Cisco SDM	7-23
Using the Startup Wizard	7-25
Cisco SDM User Interface	7-37
The More Link	7-38
Configuration Overview	7-38
Cisco SDM Wizards	7-41
Using Cisco SDM to Configure a WAN	7-43
Using Cisco SDM to Configure a Firewall	7-49
Using Cisco SDM to Configure a VPN	7-55
Using Cisco SDM to Perform Security Audits	7-59
Using the Reset to Factory Default Wizard	7-66
Using Cisco SDM Monitor Mode	7-67
Monitor Interface or Stop Monitoring Button	7-68
Test Connection Button	7-68
Interface List	7-68
Select Chart Types to Monitor Group	7-69
Interface Status Area	7-69
Firewall Statistics	7-70
Monitoring Firewall with a Non-Administrator View User Account	7-71
IPSec Tunnels Tab	7-72
DMVPN Tunnels Tab	7-73
Easy VPN Server Tab	7-74
IKE SAs Tab	7-75
Summary	7-77
Module Summary	7-78

Course Introduction

Overview

Securing Networks with Cisco Routers and Switches (SNRS) 1.0 is a five-day, leader-led, lab-intensive course that is delivered by Cisco Learning Partners (CLPs). It is aimed at providing network specialists with the knowledge and skills needed to secure Cisco IOS router and switch networks. Successful graduates will be able to secure the network environment using existing Cisco IOS security features, configure the three primary components of the Cisco IOS Firewall feature set (Context-based Access Control [CBAC], intrusion prevention, and authentication proxy), implement secure tunnels using IPSec technology, and implement basic access switch security. This task-oriented course teaches the knowledge and skills needed to secure Cisco IOS router networks using features and commands in Cisco IOS software and using router configuration applications.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should complete in order to benefit fully from this course.

Learner Skills and Knowledge

Cisco.com

- **Certification as a Cisco CCNA® or the equivalent knowledge (optional)**
- **Basic knowledge of the Windows operating system**
- **Familiarity with networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications)**
- **Interconnecting Cisco Network Devices (ICND)**
- **Securing Cisco Network Devices (SND)**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—3

Course Goal and Objectives

This topic describes the course goal and objectives.

Course Goal

Cisco.com

“To secure a network using existing Cisco IOS features, including the Cisco IOS Firewall feature set (Context-based Access Control [CBAC], intrusion prevention, and authentication proxy), implement secure tunnels using IPSec technology, and implement basic switch security. In addition, you will be able to configure routers, firewalls, and VPNs and complete a security audit using functions embedded in Cisco SDM.”

Securing Networks with Cisco Routers and Switches

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4

Upon completing this course, you will be able to meet these objectives:

- Install, configure, operate, and troubleshoot Cisco Secure ACS for Windows Server
- Install, configure, operate, and troubleshoot Cisco IOS Firewall, Cisco IOS Firewall authentication proxy, and Cisco IOS Firewall IPS on a Cisco router
- Install, configure, operate, and troubleshoot Layer 2 security features
- Plan, configure, operate, and troubleshoot IPSec VPNs using Cisco routers and pre-shared keys
- Plan, configure, operate, and troubleshoot IPSec VPNs using Cisco routers and certificate authorities
- Plan, configure, operate, and troubleshoot IPSec VPNs using Cisco Easy VPN
- Use the wizards and tools embedded in the Cisco SDM to complete a wide range of configuration tasks

Course Flow

This topic presents the suggested flow of the course materials.

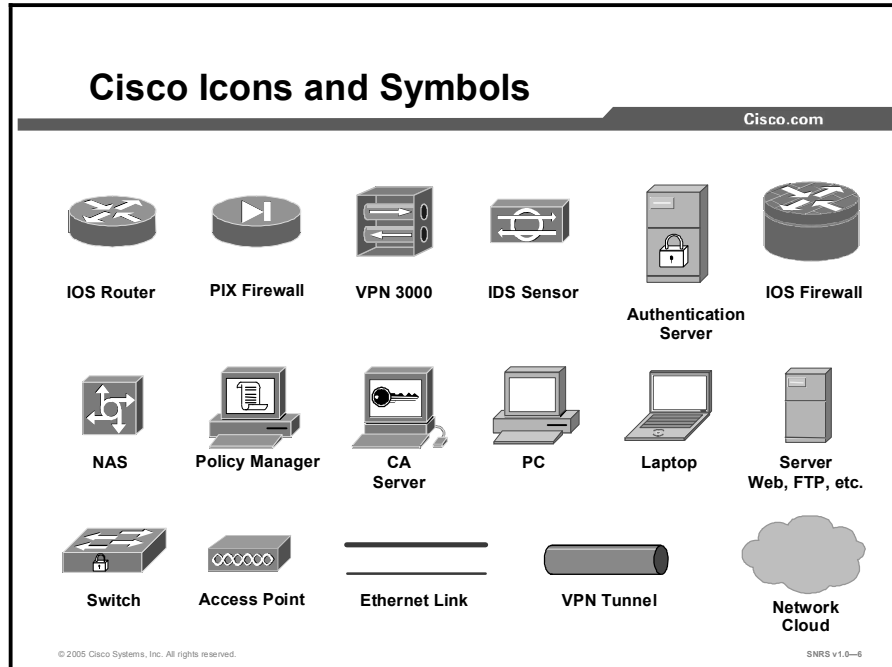
		Course Flow				
		Cisco.com				
		Day 1	Day 2	Day 3	Day 4	Day 5
A M	Course Introduction	Cisco Secure Access Control Server for Windows Server	Configuring Cisco IOS Security Features	Layer 2 Security	Building Cisco IOS-Based VPNs Using Certificate Authorities	Cisco IOS Remote Access Using Cisco Easy VPN Cisco Router and Security Device Manager
		Lunch				
P M	Cisco Secure Access Control Server for Windows Server	Configuring Cisco IOS Security Features	Building Cisco IOS-Based VPNs Using Pre-Shared Keys	Cisco IOS Remote Access Using Cisco Easy VPN	Cisco Router and Security Device Manager	

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols used in this course, as well as information on where to find additional technical references.



Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.

Module 1

Cisco Secure Access Control Server for Windows Server

Overview

Cisco Secure Access Control Server (ACS) network security software helps you authenticate users by controlling access to an authentication, authorization, and accounting (AAA) client—any one of many network devices that can be configured to defer authentication and authorization of network users to an AAA server. Cisco Secure ACS operates as a set of Windows services that control the authentication, authorization, and accounting of users accessing networks. This module describes features, functions, and architectures of Cisco Secure ACS and how to configure TACACS+ and RADIUS on Cisco routers and switches to work with Cisco Secure ACS.

Module Objectives

Upon completing this module, you will be able to install, configure, operate, and troubleshoot Cisco Secure ACS for Windows Server. This ability includes being able to meet these objectives:

- Describe the function, features, and architecture of the three components of Cisco Secure ACS for Windows Server
- Configure TACACS+ and RADIUS with the Cisco Secure ACS for Windows Server

Lesson 1

Deploying Cisco Secure Access Control Server for Windows Server

Overview

With the ever-increasing number of methods of accessing networks today, security breaches and uncontrolled user access are a primary concern. Cisco Secure Access Control Server (ACS) for Windows Server provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security-management applications. This lesson covers Cisco Secure ACS for Windows Server. Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control the following:

- Who can log into the network
- The privileges that each user has in the network
- Recorded security audit or account billing information
- Access and command controls that are enabled for the administrator of each configuration

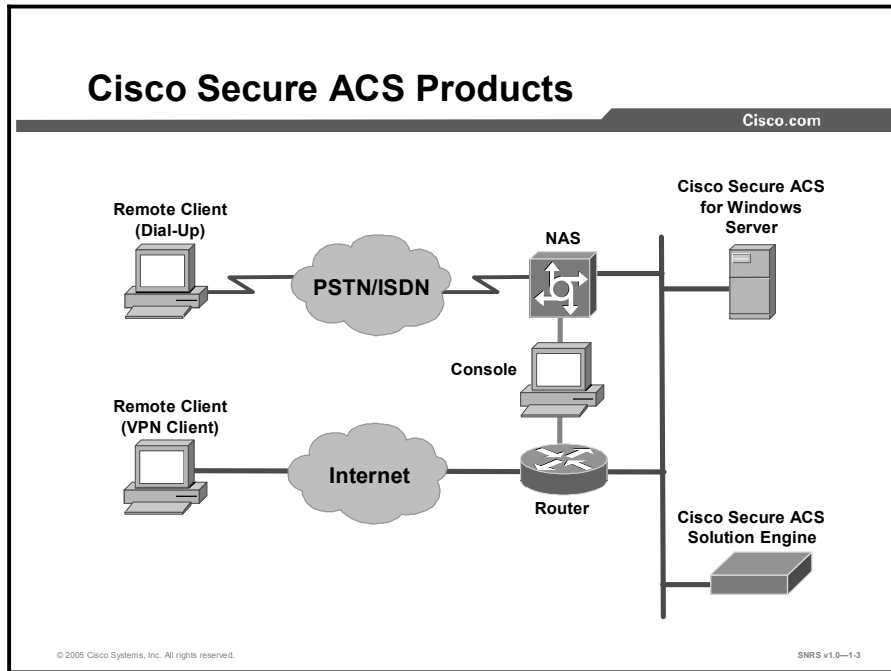
Objectives

Upon completing this lesson, you will be able to describe the functions, features, and architecture of the three components of Cisco Secure ACS for Windows Server, including Cisco Secure ACS for Windows Server, Cisco Secure ACS for UNIX, and Cisco Secure ACS Solution Engine. This ability includes being able to meet these objectives:

- Describe the functions, features, and architecture of Cisco Secure ACS for Windows Server
- Describe how the database utilities keep the Cisco Secure ACS database and network configuration current
- Describe what each of the seven service modules does to provide AAA services for multiple routers
- Describe the service and database interactions that occur when using Cisco Secure ACS
- Describe how Cisco Secure ACS for Windows Server allows users to change passwords

Cisco Secure ACS for Windows Server Product Overview

This topic presents an introduction to Cisco Secure ACS for Windows Server and prepares you to install and configure Cisco Secure ACS for Windows Server. The figure shows two versions of Cisco Secure ACS in a typical network.



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, Cisco PIX Firewalls, or Cisco VPN 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.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—1-4

Cisco Secure ACS for Windows Server provides AAA services to network devices that function as AAA clients, such as routers, network access servers, Cisco PIX Firewalls, or Cisco Virtual Private Network (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. Cisco Secure ACS also supports third-party devices that can be configured with TACACS+ or RADIUS protocols. It 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.

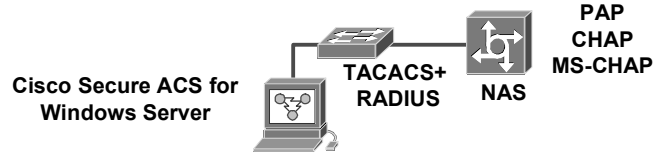
Cisco Secure ACS helps centralize access control and accounting, in addition to router and switch access management. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users. Although the use of an external 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 3.3 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 Novell Directory Service (NDS).

Cisco Secure ACS for Windows Server: General Features

Cisco.com



- **Uses TACACS+ or RADIUS between Cisco Secure ACS and NAS**
- **Allows authentication against Windows 2000 user database, Cisco Secure ACS user database, token server, or other external databases**
- **Supports PAP, CHAP, and MS-CHAP authentication on the NAS**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.5

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. Challenge Handshake Authentication Protocol (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.

Identity networking and the ability to provision the network to user- or device-specific services are now possible with Cisco Secure ACS. Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS server or TACACS+ server. Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user productivity gains. Cisco Secure ACS reduces the administrative and management burden involved in scaling user and network administrative access to your network. By using a central database for all user accounts, Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network. As an accounting service, Cisco Secure ACS reduces IT operating costs by providing detailed reporting and monitoring capabilities of network user behavior and by keeping a record of every access connection and device configuration change across the entire network. Cisco Secure ACS supports a wide array of access connection types, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and virtual private networks (VPNs).

Cisco Secure ACS supports Cisco AAA clients such as the Cisco 2509, 2511, 3620, and 3640, Cisco AS5200, AS5300, and AS5800, the Cisco PIX Firewall, Cisco Aironet Access Point wireless networking devices, Cisco VPN 3000 Concentrators, and Cisco VPN 5000 Concentrators. It also supports third-party devices that can be configured with the TACACS+ or the RADIUS protocol. 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.

Authentication and User Databases

Cisco.com

- **Windows NT/2000 User Database**
- **Generic LDAP**
- **NDS**
- **ODBC-compliant relational databases**
- **CRYPTOcard token server**
- **SafeWord token server**
- **AXENT token server**
- **RSA SecurID token server**
- **ActivCard token server**
- **Vasco token server**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1-8

Authentication and User Databases

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More modern and secure methods use technologies such as CHAP and one-time passwords (OTPs). Cisco Secure ACS supports a wide variety of these authentication methods.

There is a fundamental implicit relationship between authentication and authorization. The more authorization privileges granted to a user, the stronger the authentication should be. Cisco Secure ACS supports this fundamental relationship by providing various methods of authentication.

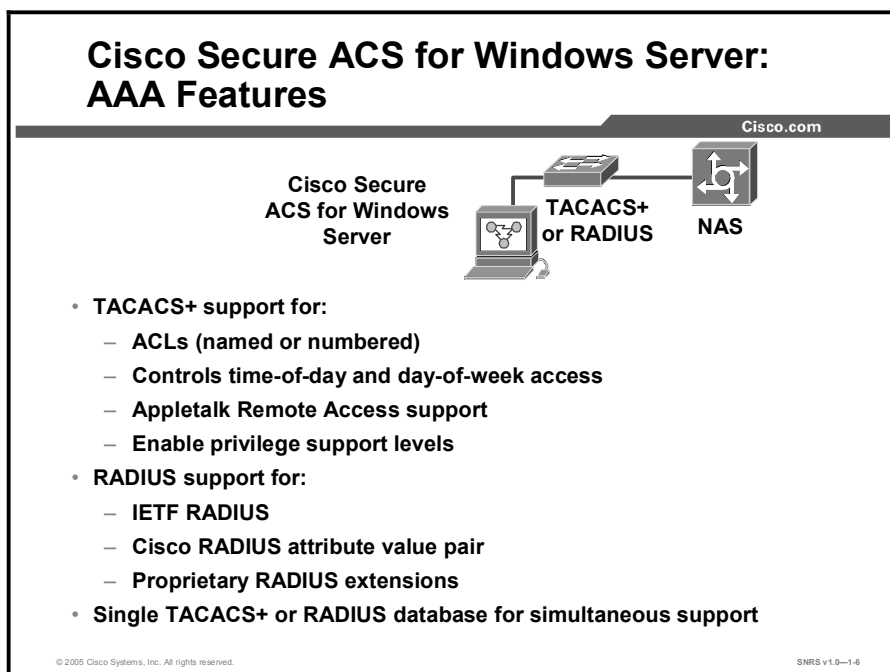
Network administrators who offer increased levels of security services, and corporations that want to lessen the chance of intruder access resulting from password capturing, can use an OTP. Cisco Secure ACS supports several types of OTP solutions, including PAP for PPP remote-node login. Token cards are considered one of the strongest OTP authentication mechanisms.

Cisco Secure ACS supports a variety of user databases. In addition to the Cisco Secure ACS user database, Cisco Secure ACS supports several external user databases, including these:

- Windows NT or 2000 user database
- Generic Lightweight Directory Access Protocol (LDAP)
- NDS
- Open Database Connectivity (ODBC)-compliant relational databases
- CRYPTOcard token server
- SafeWord token server
- AXENT token server

- RSA SecurID token server
- ActivCard token server
- VASCO token server

Cisco Secure ACS for Windows Server: AAA Features



- **TACACS+ support for:**
 - ACLs (named or numbered)
 - Controls time-of-day and day-of-week access
 - Appletalk Remote Access support
 - Enable privilege support levels
- **RADIUS support for:**
 - IETF RADIUS
 - Cisco RADIUS attribute value pair
 - Proprietary RADIUS extensions
- **Single TACACS+ or RADIUS database for simultaneous support**

AAA Protocols—TACACS+ and RADIUS

Cisco Secure ACS can use both the TACACS+ and RADIUS AAA protocols.

TACACS+

Cisco Secure ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77.

RADIUS

Cisco Secure ACS conforms to the RADIUS protocol as defined in the draft of April 1997 and in the following RFCs:

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- RFC 2865
- RFC 2866
- RFC 2867
- RFC 2868

The ports used for authentication and accounting have changed in RADIUS RFC documents. To support both the older and newer RFCs, Cisco Secure ACS accepts authentication requests on port 1645 and port 1812. For accounting, Cisco Secure ACS accepts accounting packets on port 1646 and 1813.

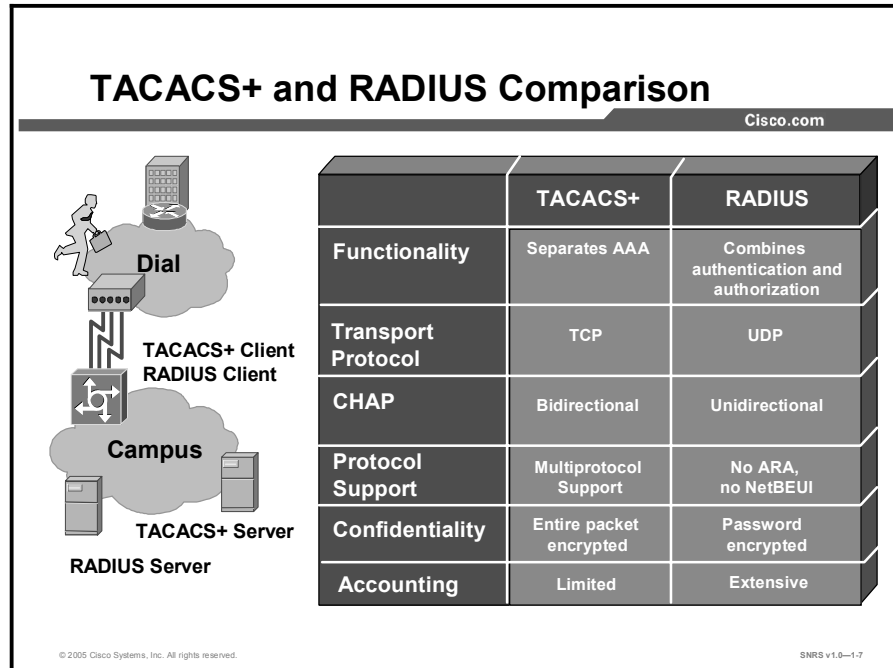
In addition to support for standard Internet Engineering Task Force (IETF) RADIUS attributes, Cisco Secure ACS includes support for RADIUS vendor-specific attributes (VSAs). Cisco has predefined the following RADIUS VSAs in Cisco Secure ACS:

- Cisco IOS/PIX
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend
- Juniper
- Microsoft
- Nortel

Cisco Secure ACS also supports up to 10 RADIUS VSAs that you define. After you define a new RADIUS VSA, you can use it as you would one of the RADIUS VSAs that come predefined in Cisco Secure ACS. In the Network Configuration section of the Cisco Secure ACS HTML interface, you can configure an AAA client to use a user-defined RADIUS VSA as its AAA protocol. In Interface Configuration, you can enable user-level and group-level attributes for user-defined RADIUS VSAs. In User Setup and Group Setup, you can configure the values for enabled attributes of a user-defined RADIUS VSA.

Comparing TACACS+ and RADIUS

This topic compares TACACS+ and RADIUS.



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, but 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; however, 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 and 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 encrypts only 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 (such as customizable username and password prompts). RADIUS lacks this flexibility, and therefore many features that are possible with TACACS+ are not possible with RADIUS (such as 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+.

Passwords

Cisco.com

Cisco Secure ACS supports many common password protocols:

- ASCII/PAP
- CHAP
- MS-CHAP
- LEAP
- EAP-CHAP
- EAP-TLS
- ARAP

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—1-9

Passwords

Cisco Secure ACS supports many common password protocols:

- ASCII/PAP
- CHAP
- Microsoft CHAP (MS-CHAP)
- Light Extensible Authentication Protocol (LEAP)
- Extensible Authentication Protocol-CHAP (EAP-CHAP)
- Extensible Authentication Protocol Transport Layer Security (EAP-TLS)
- AppleTalk Remote Access (ARA) protocol

Passwords can be processed using these password authentication protocols based on the version and type of security control protocol used (for example, RADIUS or TACACS+) and the configuration of the AAA client and end-user client.

In the case of token servers, Cisco Secure ACS acts as a client to the token server, either using its proprietary application programming interface (API) or its RADIUS interface, depending on the token server.

Different levels of security can be used concurrently with Cisco Secure ACS for different requirements. The basic user-to-network security level is PAP. Although it represents the unencrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows NT or 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 an end-user client to the AAA client. You can use CHAP with the Cisco Secure ACS user database. ARA protocol support is included to support Apple clients.

Cisco Secure ACS for Windows Server: Administration Features

Cisco.com

- **Browser interface allows for easy management**
- **Allows remote administration**
- **Ability to define different privileges per administrator**
- **Ability to log administrator activities**
- **Ability to view a list of logged-in users**
- **CSMonitor service, providing monitoring, notification, logging, and limited automated failure response**
- **Ability to import of large numbers of users with the CSUtil.exe command line**
- **Synchronization of the Cisco Secure user database with a relational database management system (RDBMS)**
- **Replication of Cisco Secure user database components to other Cisco Secure ACS servers**
- **Ability to restore Cisco Secure ACS configuration, user accounts, and group profiles from a backup file**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—1-10

Administration

To configure, maintain, and protect its AAA functionality, Cisco Secure ACS provides a flexible administration scheme. You can perform nearly all administration of Cisco Secure ACS through its HTML interface.

You can access the HTML interface from computers other than the Cisco Secure ACS server. This feature enables remote administration of Cisco Secure ACS.

The HTTP port allocation feature allows you to configure the range of TCP ports used by Cisco Secure ACS for remote administrative HTTP sessions (that is, administrative sessions conducted by a browser running on a computer other than the Cisco Secure ACS server). Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network by a port open for administrative sessions.

It is not recommended that you administer Cisco Secure ACS through a firewall. Doing so requires that you configure the firewall to permit HTTP traffic over the range of HTTP administrative session ports that Cisco Secure ACS uses. Although narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of Cisco Secure ACS from outside a firewall. A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port that a remote web browser must access to initiate an administrative session.

Note A broad HTTP port range could create a security risk. To prevent accidental discovery of an active administrative port by unauthorized users, keep the HTTP port range as narrow as possible. Cisco Secure ACS tracks the IP address associated with each remote administrative session. An unauthorized user would have to impersonate, or spoof, the IP address of the legitimate remote host to make use of the active administrative session HTTP port.

In addition to the administration-related features discussed in this topic, the following features are provided by Cisco Secure ACS:

- Ability to define different privileges per administrator
- Ability to log administrator activities
- Ability to view a list of logged-in users
- CSMonitor service, providing monitoring, notification, logging, and limited automated failure response
- Ability to import of large numbers of users with the CSUtil.exe command-line
- Synchronization of the Cisco Secure ACS user database with a relational database management system (RDBMS)
- Replication of Cisco Secure ACS user database components to other Cisco Secure ACS servers
- Scheduled and on-demand Cisco Secure ACS system
- Ability to restore Cisco Secure ACS configuration, user accounts, and group profiles from a backup file

Key Features in Cisco Secure ACS Version 3.3

Cisco.com

- Cisco NAC support
- EAP-Flexible Authentication via Secure Tunneling (FAST) support for wireless authentication
- Downloadable IP ACLs
- Certification revocation list (CRL) comparison
- Machine access restrictions (MAR)
- Network access filtering (NAF)
- Cisco Security Agent integration on Cisco Secure ACS Solution Engine
- Replication enhancements

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1-11

Key Features in Cisco Secure ACS 3.3

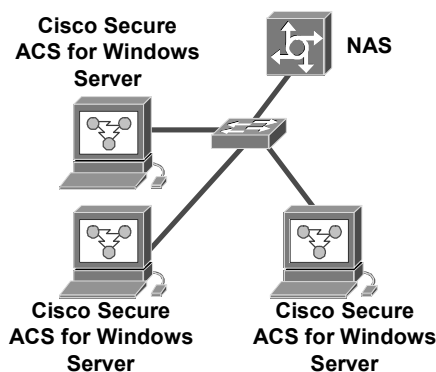
- **Cisco network admission control (NAC) support:** Cisco Secure ACS 3.3 acts as a policy decision point in NAC deployments. Using policies that you configure, it evaluates the credentials sent to it by Cisco Trust Agent, determines the state of the host, and sends the AAA client access control lists (ACLs) that are appropriate to the host state. Evaluation of the host credentials can enforce many specific policies, such as operating system patch level and antivirus .dat file version. Cisco Secure ACS records the results of policy evaluation for use with your monitoring system. Policies can be evaluated locally by Cisco Secure ACS or can be the result returned from an external policy server to which Cisco Secure ACS forwards credentials. For example, credentials specific to an antivirus vendor can be forwarded to the vendor antivirus policy server.
- **EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) support for wireless authentication:** EAP-FAST is a new, publicly accessible IEEE 802.1x EAP type developed by Cisco to support customers who cannot enforce a strong password policy and who wish to deploy an 802.1x EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco EAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks. Cisco Secure ACS 3.3 adds support for EAP-FAST supplicants available today on Cisco compatible client devices and Cisco Aironet 802.11a/b/g wireless LAN (WLAN) client adapters.
- **Downloadable IP ACLs:** Cisco Secure ACS 3.3 extends per-user ACL support to any Layer 3 network device that supports this feature. These devices include Cisco PIX Firewalls, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that can be applied per user or per group. This feature complements NAC support by enabling the enforcement of the correct ACL policy. When used in conjunction with network access filters (NAFs), downloadable ACLs can be applied differently per AAA client, enabling you to tailor ACLs uniquely per user, per access device.

- **Certificate revocation list (CRL) comparison:** Cisco Secure ACS 3.3 adds support for certificate revocation using the X.509 CRL profile. A CRL is a time-stamped list identifying revoked certificates that is signed by a certificate authority (CA) or CRL issuer and made freely available in a public repository. Cisco Secure ACS 3.3 periodically retrieves the CRLs from provisioned CRL Distribution Points, using LDAP or HTTP, and stores them for use during EAP-TLS authentication. If the certificate presented by the user during an EAP-TLS authentication is present in the retrieved CRL, Cisco Secure ACS fails the authentication and denies access to the user. This capability is extremely important in accommodating organizational changes and ensures protection of valuable company assets in case of fraudulent network use.
- **Machine access restrictions (MARs):** Cisco Secure ACS 3.3 includes MARs as an enhancement of Windows machine authentication. When Windows machine authentication is enabled, you can use MARs to control authorization of EAP-TLS and Microsoft Protected Extensible Authentication Protocol (MS-PEAP) users who authenticate with a Windows external user database. Users who access the network with a computer that has not passed machine authentication within a configurable length of time are given the authorizations of a user group that you specify and that you can configure to limit authorization as needed. Alternatively, you can deny network access altogether.
- **Network access filtering:** Cisco Secure ACS 3.3 includes NAFs as a new type of Shared Profile Component. Network access filtering provides a flexible way of applying network access restrictions and downloadable ACLs on AAA client names, network device groups, or the IP addresses of AAA clients. NAFs applied by IP addresses can use IP address ranges and wildcards. This feature introduces granular application of network access restrictions and downloadable ACLs, both of which previously supported only the use of the same access restrictions or ACLs to all devices. NAFs allow flexible network device restriction policies to be defined, a requirement common in large environments.
- **Cisco Security Agent integration on Cisco Secure ACS Solution Engine:** Cisco Secure ACS 3.3 Solution Engine now ships with a preinstalled, standalone Cisco Security Agent. This integration into the base appliance image helps protect Cisco Secure ACS Solution Engine from Day Zero attacks. By using the new behavior-based technology available with Cisco Security Agent, the Cisco Secure ACS Solution Engine can be protected against the constantly changing threats of viruses and worms.
- **Replication enhancements:** Cisco Secure ACS 3.3 now allows you to replicate the user and group databases separately. Replicating changes to user accounts no longer automatically requires replicating groups. Likewise, replicating groups no longer requires replicating users. This increase in replication component granularity reduces the amount of data sent between Cisco Secure ACS systems during a replication event. Furthermore, a configurable replication timeout option has been added to provision for slow network connectivity between Cisco Secure ACS replication partners.

Cisco Secure ACS for Windows Server— Distributed System Features

Cisco.com

- **Fallback on failed connection**
- **Remote and centralized logging**
- **Proxy**
- **Cisco Secure database replication**



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—1-12

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. This capacity also allows Cisco Secure ACS to recognize network access restrictions of other Cisco Secure ACS servers on the distributed network.

AAA Servers in Distributed Systems

“AAA server” is a generic term for an access server, and the two terms are often used interchangeably. AAA servers are used to determine who can access the network and what services are authorized for each user. The AAA server stores a profile containing authentication and authorization information for each user. Authentication information validates user identity, and authorization information determines which network services a user is permitted to use. A single AAA server can provide concurrent AAA services to many dialup access servers, routers, and firewalls. Each network device can be configured to communicate with an AAA server. This makes it possible to centrally control dialup access and to secure network devices from unauthorized access.

These types of access control have unique authentication and authorization requirements. With Cisco Secure ACS, system administrators can use a variety of authentication methods with different degrees of authorization privileges.

Completing the AAA functionality, Cisco Secure ACS serves as a central repository for accounting information. Each user session granted by Cisco Secure ACS can be fully accounted for, and its accounting information can be stored in the server. This accounting information can be used for billing, capacity planning, and security audits.

Note If the fields mentioned in this section do not appear in the Cisco Secure ACS HTML interface, enable them by clicking **Interface Configuration**, clicking **Advanced Options**, and then checking the **Distributed System Settings** check box.

Default Distributed System Settings

You use both the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters configured within these tables create the foundation to enable multiple Cisco Secure ACS systems to be configured to work with one another. Each table contains a Cisco Secure ACS entry for itself. In the AAA Servers table, the only AAA server initially listed is itself; the Proxy Distribution Table lists an initial entry of (Default), which displays how the local Cisco Secure ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. This process enables these devices to become available in the HTML interface so that they can be configured for other distributed features such as proxy, Cisco Secure ACS user database replication, remote logging, and relational database management system (RDBMS) synchronization.

Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use Cisco Secure ACS for authentication in a network that uses more than one AAA server. Using proxy, Cisco Secure ACS automatically forwards an authentication request from an AAA client to another AAA server. After the request has been successfully authenticated, the authorization privileges that have been configured for the user on the remote AAA server are passed back to the original Cisco Secure ACS, where the AAA client applies the user profile information for that session.

Fallback on Failed Connection

You can configure the order in which Cisco Secure ACS checks remote AAA servers when a failure of the network connection to the primary AAA server has occurred. If an authentication request cannot be sent to the first listed server, because of a network failure, for example, the next listed server is checked. This process continues, in order, down the list until an AAA server handles the authentication request. (Failed connections are detected by failure of the nominated server to respond within a specified time period. That is, the request is timed out.) If Cisco Secure ACS cannot connect to any server in the list, authentication fails.

Remote and Centralized Logging

The Remote Logging feature enables you to centralize accounting logs generated by multiple Cisco Secure ACS systems. You can configure each Cisco Secure ACS to point to one Cisco Secure ACS that is to be used as a central logging server. The central logging Cisco Secure ACS still performs AAA functions, but it also is the repository for accounting logs it receives.

Cisco Secure Database Replication

Database replication creates mirror systems of a Cisco Secure ACS by duplicating parts of the primary Cisco Secure ACS setup to one or more secondary Cisco Secure ACS systems. You can configure your AAA clients to use these secondary Cisco Secure ACS systems if the primary Cisco Secure ACS fails or is unreachable. With a secondary Cisco Secure ACS whose Cisco Secure database is a replica of the Cisco Secure database on the primary Cisco Secure ACS, if the primary Cisco Secure ACS goes out of service, incoming requests are authenticated without network downtime, provided that your AAA clients are configured to fail over to the secondary Cisco Secure ACS.

System Requirements

Cisco.com

Hardware requirements

- Pentium III processor, 550 MHz or faster.
- 256 MB of RAM.
- At least 250 MB of free disk space. If you are running your database on the same computer, more disk space is required.
- Minimum graphics resolution of 256 colors at 800 x 600 lines.

Operating system requirements

- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server, with the following conditions:
 - With Service Pack 4 installed
 - Without Microsoft Clustering Service installed
 - Without other features specific to Windows 2000 Advanced Server enabled
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—1-13

System Requirements

The computer running Cisco Secure ACS must meet the minimum hardware and software requirements detailed in the following sections.

Hardware Requirements

The computer running Cisco Secure ACS must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster.
- 256 MB of RAM.
- At least 250 MB of free disk space. If you are running your database on the same computer, more disk space is required.
- Minimum graphics resolution of 256 colors at 800 x 600 lines.

Operating System Requirements

Cisco Secure ACS for Windows Server 3.3 supports the Windows operating systems listed here. Both the operating system and the service pack must be English-language versions.

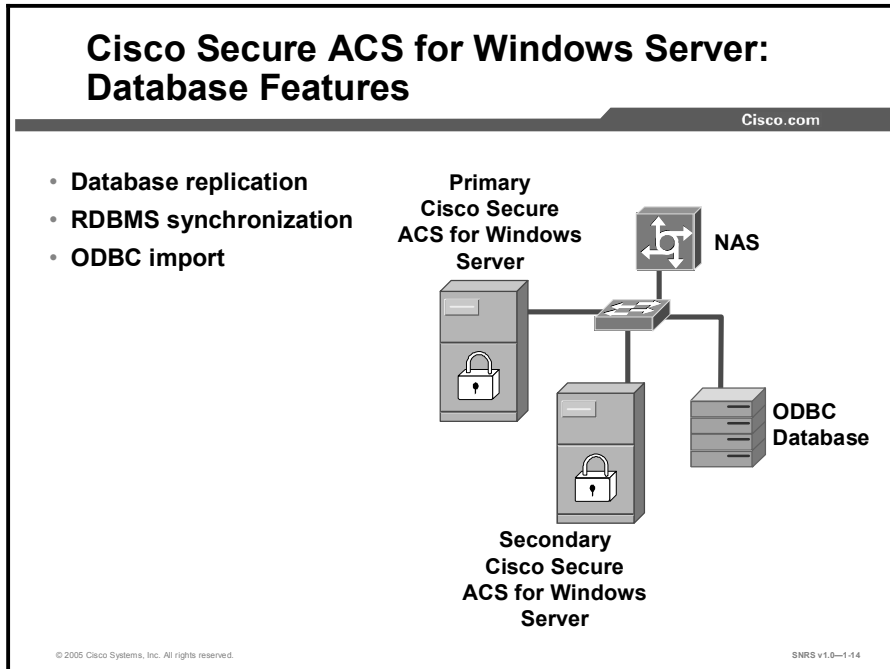
- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server, with the following conditions:
 - With Service Pack 4 installed
 - Without Microsoft Clustering Service installed
 - Without other features specific to Windows 2000 Advanced Server enabled

Note The multiprocessor feature of Windows 2000 Advanced Server has not been tested and is not supported. Windows 2000 Datacenter Server is not a supported operating system.

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition

Keeping Databases Current

This topic describes how the database utilities keep the Cisco Secure ACS database and network configuration current.



Database replication and 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 databases. Another utility, CSUtil, provides database backup and restore functionality.

Database Replication

Database replication allows you to do the following:

- Select the parts of the primary Cisco Secure ACS configuration to be replicated
- Control the timing of the replication process, including creating schedules
- Export selected configuration items from the primary Cisco Secure ACS
- Securely transport selected configuration data from the primary Cisco Secure ACS to one or more secondary Cisco Secure ACS systems
- Update the secondary Cisco Secure ACS systems to create matching configurations

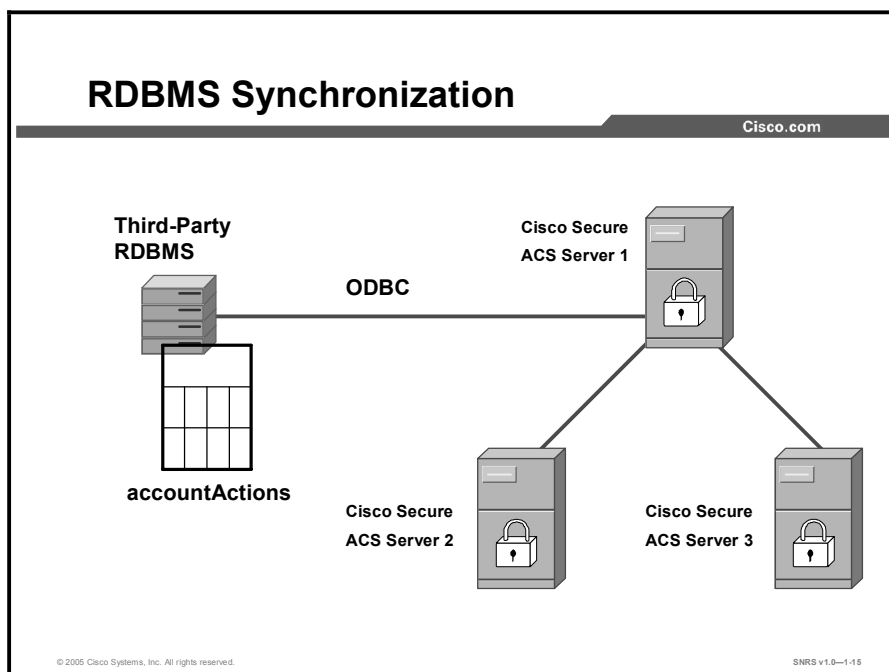
With regard to database replication, make the following distinctions about Cisco Secure ACS systems:

- **Primary Cisco Secure ACS:** A Cisco Secure ACS that sends replicated Cisco Secure database components to other Cisco Secure ACS systems.
- **Secondary Cisco Secure ACS:** A Cisco Secure ACS that receives replicated Cisco Secure database components from a primary Cisco Secure ACS. In the HTML interface, these are identified as replication partners.

A Cisco Secure ACS can be both a primary Cisco Secure ACS and a secondary Cisco Secure ACS, provided that it is not configured to be a secondary Cisco Secure ACS to a Cisco Secure ACS for which it performs as a primary Cisco Secure ACS.

Note Bidirectional replication, wherein a Cisco Secure ACS both sends database components to and receives database components from the same remote Cisco Secure ACS, is not supported. Replication fails if a Cisco Secure ACS is configured to replicate to and from the same Cisco Secure ACS.

Note All Cisco Secure ACS systems involved in replication must run the same release of the Cisco Secure ACS software. For example, if the primary Cisco Secure ACS is running Cisco Secure ACS 3.2, all secondary Cisco Secure ACS systems should be running Cisco Secure ACS 3.2. Because patch releases can introduce significant changes to the Cisco Secure database, it is strongly recommended that Cisco Secure ACS systems involved in replication use the same patch level, too.



RDBMS Synchronization

The RDBMS Synchronization feature enables you to update the Cisco Secure ACS user database with information from an ODBC-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, Cisco Secure ACS reads the file or database via the ODBC connection. You can also regard RDBMS Synchronization as an API—much of what you can configure for a user, group, or device through the Cisco Secure ACS HTML interface, you can alternatively maintain through this feature. RDBMS Synchronization supports addition, modification, and deletion for all data items that it can access.

You can configure synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the Cisco Secure ACS user database on demand.

Synchronization performed by a single Cisco Secure ACS can update the internal databases of other Cisco Secure ACS systems, so that you need configure RDBMS Synchronization on only one Cisco Secure ACS. Cisco Secure ACS systems listen on TCP port 2000 for synchronization data. RDBMS Synchronization communication between Cisco Secure ACS systems is encrypted using a 128-bit encrypted, proprietary algorithm.

RDBMS Synchronization Components

The RDBMS Synchronization feature comprises two components:

- **CSDBSync:** A dedicated Windows service that performs automated user and group account management services for Cisco Secure ACS
- **accountActions table:** The data object that holds information used by CSDBSync to update the Cisco Secure ACS user database

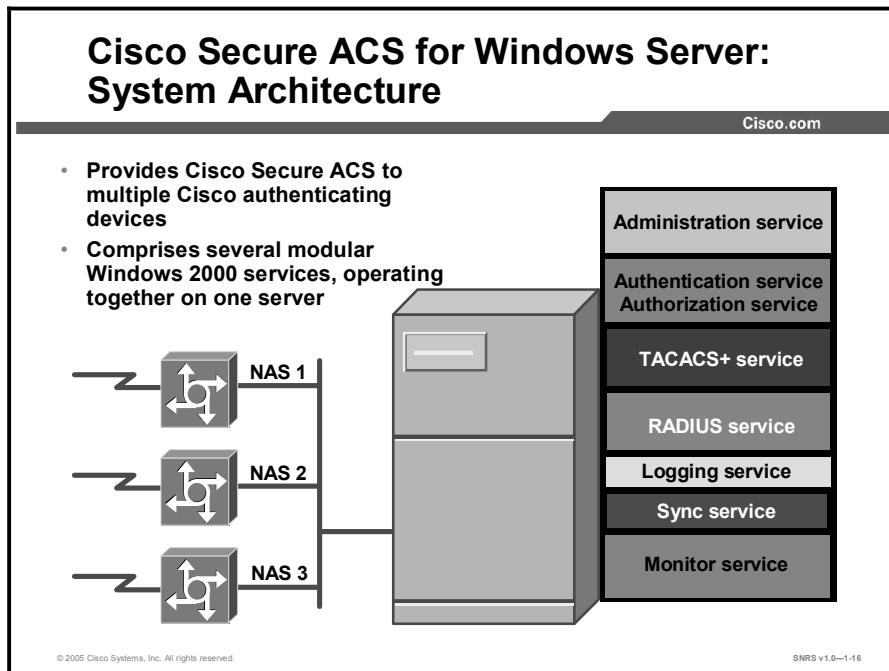
ODBC Import Definitions

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 Cisco Secure ACS servers.

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

Cisco Secure ACS for Windows Server Architecture

This topic describes what each of the seven service modules does to provide AAA services for multiple routers.



Cisco Secure ACS operates as a set of Microsoft Windows services and controls the authentication, authorization, and accounting of users accessing networks.

When you install Cisco Secure ACS, the installation adds several Windows services. The services provide the core of Cisco Secure ACS functionality. The Cisco Secure ACS services on the computer running Cisco Secure ACS include the following:

- **CSAdmin:** Provides the HTML interface for administration of Cisco Secure ACS
- **CSAuth:** Provides authentication services
- **CSDBSync:** Provides synchronization of the Cisco Secure ACS user database with an external RDBMS application
- **CSLog:** Provides logging services, both for accounting and system activity
- **CSMon:** Provides monitoring, recording, and notification of Cisco Secure ACS performance, and includes automatic response to some scenarios
- **CSTacacs:** Provides communication between TACACS+ AAA clients and the CSAuth service
- **CSRadius:** Provides communication between RADIUS AAA clients and the CSAuth service

Cisco Secure ACS Windows Services

Cisco.com

- **CSAdmin**—Provides the HTML interface for administration of Cisco Secure ACS
- **CSAuth**—Provides authentication services
- **CSDBSync**—Provides synchronization of the Cisco Secure user database with an external RDBMS application
- **CSLog**—Provides logging services, both for accounting and system activity
- **CSMon**—Provides monitoring, recording, and notification of Cisco Secure ACS performance, and includes automatic response to some scenarios
- **CSTacacs**—Provides communication between TACACS+ AAA clients and the CSAuth service
- **CSRADIUS**—Provides communication between RADIUS AAA clients and the CSAuth service

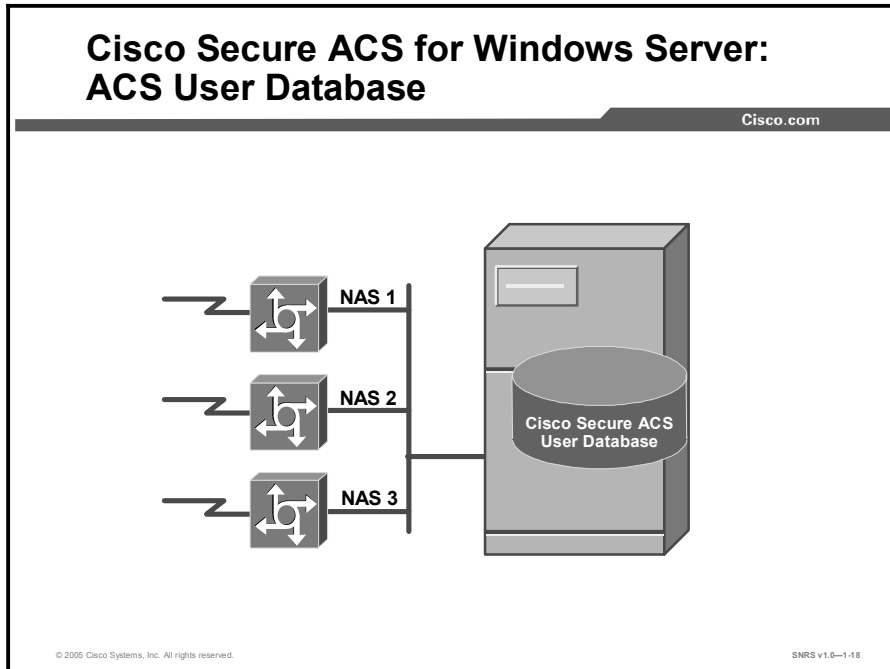
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—1.17

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 HTML interface.

How Cisco Secure ACS Authenticates Users

This topic describes the service and database interactions that occur when using Cisco Secure ACS.



Cisco Secure 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.

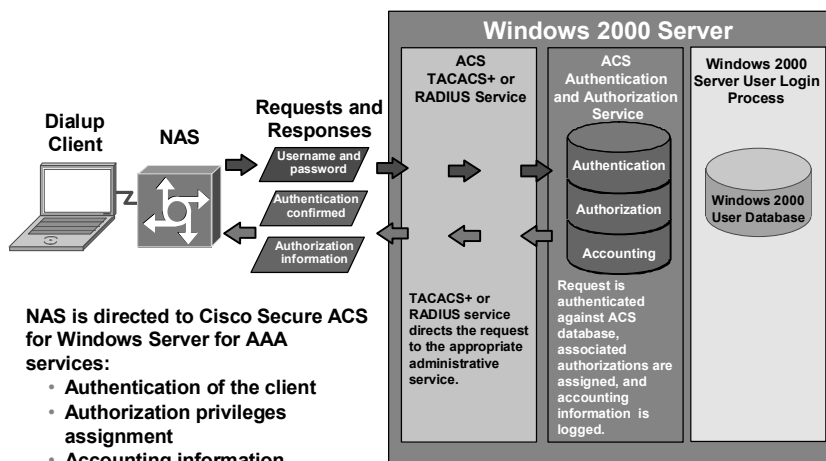
Unless you have configured Cisco Secure ACS to authenticate users with an external user database, Cisco Secure ACS uses usernames and passwords in the Cisco Secure ACS user database during authentication.

There are five ways to create user accounts in Cisco Secure ACS for Windows 2000 Servers. Of these, RDBMS Synchronization and CSUtil.exe support importing user accounts from external sources.

- **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. We recommend using 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 Cisco Secure ACS Database Alone

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1-19

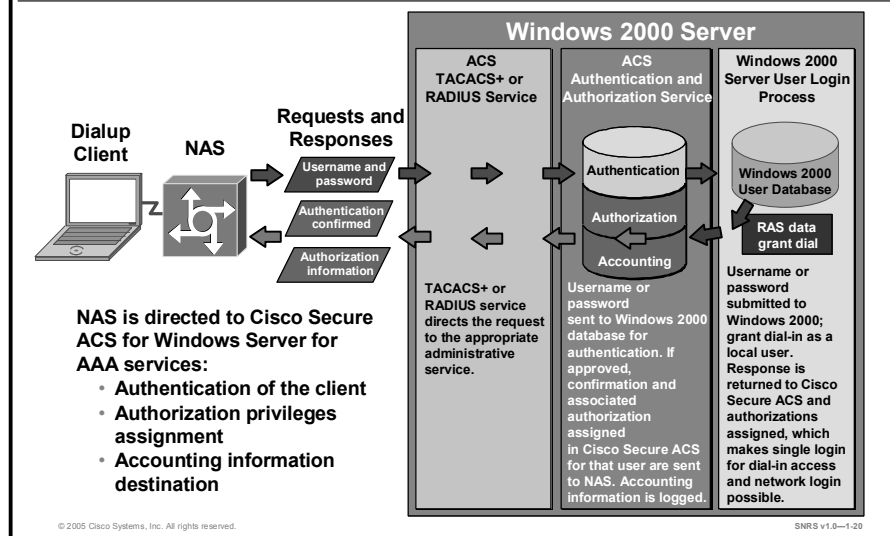
Using either the RADIUS or TACACS+ protocol, the network access server directs all dial-in user access requests to Cisco Secure ACS for Windows Server, which verifies the username and password, for authentication and authorization of privileges. Cisco Secure ACS then returns a success or failure response 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 NAS, 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 the 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-in permission as a local user. The user may log in to Windows 2000 after the dialup AAA process is complete.

How Cisco Secure ACS for Windows Server Works: Using Windows Database

Cisco.com



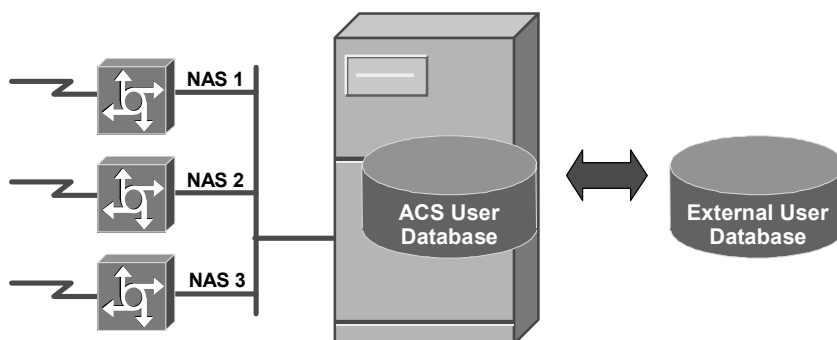
When Cisco Secure ACS for Windows Server uses the Windows 2000 Server user database for AAA, the following service and database interaction occurs:

- The TACACS+ or RADIUS service directs the 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-in 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 NAS. Accounting information is logged.
- Using the Windows 2000 user database makes a single login for dial-in and network access 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. You can require users to enter their username and password once only, for the convenience of a simple, single login.

Cisco Secure ACS for Windows Server: External User Databases

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1-21

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.

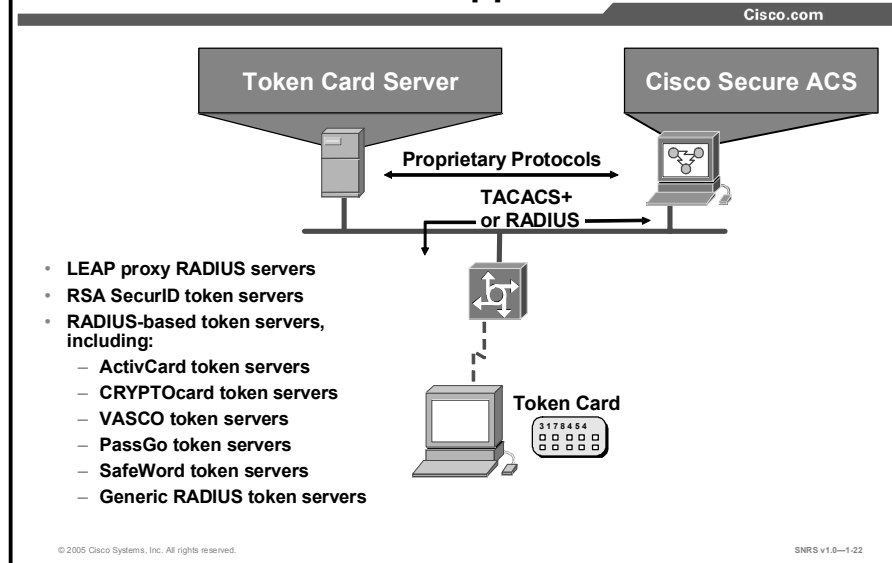
In the case of ODBC authentication sources, in addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the Cisco Secure ACS for Windows Server.

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

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



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 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.

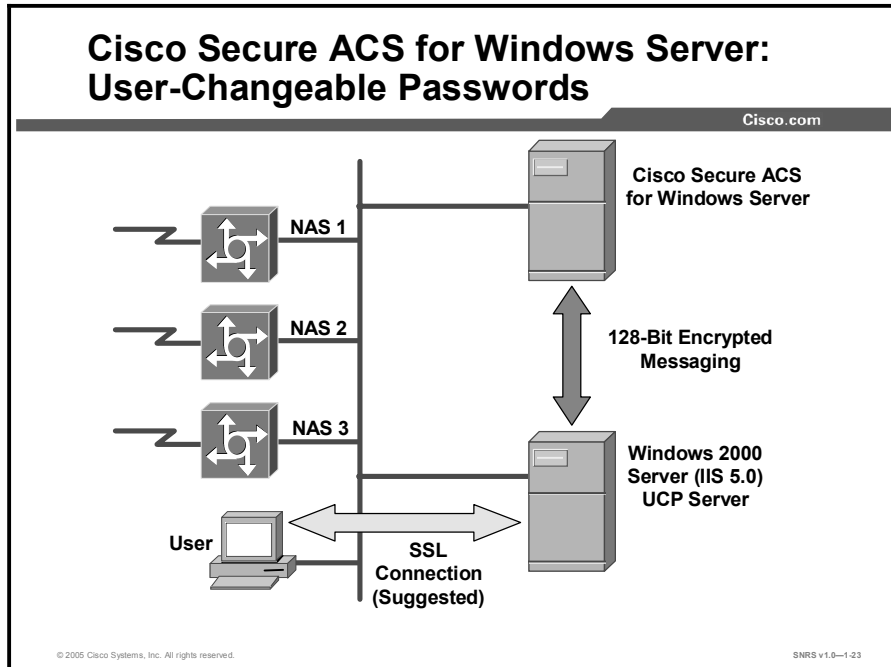
Cisco Secure ACS for Windows Server can support token servers using the RADIUS server built into the token server. Rather than using the vendor-proprietary API, Cisco Secure ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server.

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.

User-Changeable Passwords

This topic describes how Cisco Secure ACS for Windows Server allows users to change passwords.



Starting with Cisco Secure ACS for Windows Server 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 Secure Socket Layer (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 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.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

Cisco Secure ACS for Windows Server has the following characteristics:

- It runs as a group of services on Windows 200x Server.
- It authenticates using TACACS+ or RADIUS.
- Cisco NAS, PIX Firewall, VPN concentrators, 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, LDAP, token server, or NDS.
- Installation is similar to other Windows applications (InstallShield).
- Management is done via a web browser.
- It supports distributed Cisco Secure 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.

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-1-24

Lesson 2

Configuring RADIUS and TACACS+ with Cisco Secure ACS for Windows Server

Overview

This lesson covers the configuration process required when configuring TACACS+ and RADIUS on a router to work with a Cisco Secure Access Control Server (ACS) for Windows Server.

Objectives

Upon completing this lesson, you will be able to configure TACACS+ and RADIUS with Cisco Secure ACS for Windows Server. This ability includes being able to meet these objectives:

- Describe each of the six steps in installing Cisco Secure ACS for Windows Server
- Describe the function of each of the buttons on the navigational bar on the Cisco Secure ACS web interface
- Recommend the actions needed to resolve failure types
- Describe TACACS+
- Explain the commands to enable AAA using TACACS+ on an access router
- Explain the Cisco IOS debug commands used in troubleshooting TACACS+
- Describe RADIUS
- Explain the commands to enable AAA using RADIUS on an access router
- Recommend TACACS+ or RADIUS

Installing Cisco Secure ACS

This topic describes the process for installing Cisco Secure ACS.

Gathering Answers for the Installation Questions

Cisco.com

- **Determine whether the computer that you will install Cisco Secure ACS on is a domain controller or a member server.**
- **Determine which AAA protocol and vendor-specific attribute you want to implement.**
- **Record the name of the AAA client.**
- **Record the IP address of the AAA client.**
- **Record the IP address of the computer that you want to install Cisco Secure ACS on.**
- **Record the TACACS+ or RADIUS key (shared secret).**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-1.4

The first thing you need is information used in the installation process.

Gathering Answers for the Installation Questions

During new installations, or upgrades and reinstallations that do not preserve the existing configuration, the installation requires specific information about the computer you want to install Cisco Secure ACS on and an authentication, authorization, and accounting (AAA) client on your network. To facilitate the installation, collect the applicable information before beginning the installation.

Note If you are upgrading or reinstalling Cisco Secure ACS and intend to keep the existing configuration and database, you do not need to perform the procedure described in this topic.

To collect information that is required during the installation of Cisco Secure ACS, follow these steps:

- Step 1** Determine whether the computer that you will install Cisco Secure ACS on is a domain controller or a member server. If you want Cisco Secure ACS to authenticate users with a Windows domain user database, be aware that after you install Cisco Secure ACS you must perform the additional Windows configuration.

- Step 2** For the first AAA client that you want to configure to use AAA services provided by Cisco Secure ACS, determine which AAA protocol and vendor-specific attribute you want to implement:
- TACACS+ (Cisco IOS software)
 - RADIUS (Cisco Aironet)
 - RADIUS (Cisco Building Broadband Service Manager [BBSM])
 - RADIUS (Cisco IOS software/PIX Firewall)
 - RADIUS (Cisco VPN 3000 Series Concentrator)
 - RADIUS (Cisco VPN 5000 Series Concentrator)
 - RADIUS (Internet Engineering Task Force [IETF])
 - RADIUS (Ascend)
 - RADIUS (Juniper)
 - RADIUS (Nortel)
 - RADIUS (iPass)
- Step 3** Record the name of the AAA client.
- Step 4** Record the IP address of the AAA client.
- Step 5** Record the IP address of the computer on which you want to install Cisco Secure ACS.
- Step 6** Record the TACACS+ or RADIUS key (shared secret).

Cisco Secure ACS for Windows Server: Installation Overview

Cisco.com

- **Task 1: Preconfigure Windows 2000 Server system.**
- **Task 2: Verify connection between Windows 2000 Server system and Cisco routers.**
- **Task 3: Install Cisco Secure ACS for Windows Server on the Windows 2000 Server system.**
- **Task 4: Initially configure Cisco Secure ACS for Windows Server via web browser.**
- **Task 5: Configure routers for AAA.**
- **Task 6: Verify correct installation and operation.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.5

The Cisco Secure ACS installation can be condensed to the following tasks:

- Preconfigure the Windows 2000 Server system.
- Verify a basic network connection between the Windows 2000 Server and the router or routers using ping and Telnet.
- Install Cisco Secure ACS for Windows Server on the Windows 2000 Server system.
- Initially configure Cisco Secure ACS for Windows Server via the web browser interface.
- Configure the router or routers for AAA.
- 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 the 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.
- It is not recommended that you install Cisco Secure ACS for Windows Server on primary domain controllers (PDCs) or backup domain controllers (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 network access server (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 host name, IP address, and TACACS+ key.

Install Cisco Secure ACS for Windows Server on the Windows 2000 Server System

Follow these InstallShield instructions:

- 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 3.3 supports the following English-language version browsers:
 - Microsoft Internet Explorer Version 6.0 or later (with Service Pack 1) for Microsoft Windows
 - Netscape Version 7.0 or later for Microsoft Windows
 - Netscape Version 7.0 or later for Solaris 2.7

Note Browsers must have Java and JavaScript enabled with HTTP proxy disabled.

- Click the Admin icon to launch the browser with the address `http://127.0.0.1:2002/`.
- The addresses `http://<ip address>:2002/` and `http://<host name>:2002/` also work.

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 AppleTalk Remote Access (ARA) protocol 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 and authorization using the Windows 2000 user database with TACACS+

Creating a Cisco Secure ACS Installation

Use this procedure to install Cisco Secure ACS for the first time.

- Step 1** Using a local administrator account, log in to the computer you want to install Cisco Secure ACS on.
- Step 2** Insert the Cisco Secure ACS CD into a CD-ROM drive on the computer.
- Step 3** Do one of the following:
 - If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
 - If the Cisco Secure ACS for Windows Server dialog box does not appear, run `setup.exe`, located in the root directory of the Cisco Secure ACS CD.
- Step 4** Read the software license agreement. If you accept the software license agreement, click **Accept**.
- Step 5** After you have read the information in the Welcome dialog box, click **Next**.
- Step 6** If you have completed all items listed in the Before You Begin dialog box, check the corresponding check box for each item, and then click **Next**.

Step 7 If you want to change the installation location, follow these steps:

1. Click **Browse**.
2. Change the installation location. You can either type the new location in the Path box or use the Drives and Directories menus to select a new drive and directory. The installation location must be on a drive local to the computer.

Note Do not specify a path that contains a percent character (%). If you do so, installation may appear to continue properly but will fail before it completes.

3. Click **OK**.

Step 8 Click **Next**.

The Authentication Database Configuration dialog box lists options for authenticating users. You can authenticate with the Cisco Secure ACS user database only or with a Windows user database also.

Note After you have installed Cisco Secure ACS, you can configure authentication support for all external user database types in addition to Windows user databases.

Step 9 If you want to authenticate users with the Cisco Secure user database only, choose the **Check the CiscoSecure ACS database only** option.

Step 10 If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the Cisco Secure ACS user database, follow these steps:

1. Choose the **Also check the Windows User Database** option.

The Yes, Refer to “Grant Dialin Permission to User” Setting check box becomes available.

Note The Yes, Refer to “Grant Dialin Permission to User” Setting check box applies to all forms of access controlled by Cisco Secure ACS, not just dial-in access. For example, a user accessing your network through a VPN tunnel is not dialing into an NAS; however, if the Yes, Refer to “Grant Dialin Permission to User” setting check box is selected, Cisco Secure ACS applies the Windows user dial-in permissions to determine whether to grant the user access to your network.

2. If you want to allow access by users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, check the **Yes, Refer to “Grant Dialin Permission to User” Setting** check box.

Step 11 Click **Next**.

The CiscoSecure ACS Network Access Server Details dialog box appears. The information you provide in this dialog box has two uses:

- The setup program creates the AAA client definition in the Network Configuration section of Cisco Secure ACS.
- If you specify TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX) in the Authenticate Users Using list, the setup program uses this information in Step 19, in which you can configure a Cisco IOS network device to use this Cisco Secure ACS for AAA services.

Note You are not limited to defining an NAS in this dialog box. You can define any network device that can act as an AAA client.

Step 12 Complete the following items in the CiscoSecure ACS Network Access Server Details dialog box:

- **Authenticate Users Using:** Choose the AAA protocol used by the AAA client that you are defining. If you specify TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX), in Step 19 you can configure the network device specified in this dialog box.
- **Access Server Name:** Enter the name of the AAA client that will use Cisco Secure ACS for AAA services.
- **Access Server IP Address:** Enter the IP address of the AAA client that will use Cisco Secure ACS for AAA services.
- **Windows Server IP Address:** Enter the IP address of the computer that you are installing Cisco Secure ACS on.
- **TACACS+ or RADIUS Key:** Enter the shared secret of the AAA client and Cisco Secure ACS. To ensure proper function and communication between the AAA client and Cisco Secure ACS, the key must be identical to the AAA client key. Shared secrets are case-sensitive.

Step 13 Click **Next**.

The setup program installs Cisco Secure ACS and updates the Windows registry.

The Advanced Options dialog box lists several features of Cisco Secure ACS that are not enabled by default. For more information about these features, see the *User Guide for Cisco Secure ACS for Windows Server, Version 3.3*.

Note The listed features appear in the Cisco Secure ACS HTML interface only if you enable them. After installation, you can enable or disable them on the Advanced Options page in the Interface Configuration section.

Step 14 For each feature that you want to enable, check the corresponding check box.

Step 15 Click **Next**.

The Active Service Monitoring dialog box appears.

Note After installation, you can configure active service monitoring features on the Active Service Management page in the System Configuration section.

Step 16 If you want Cisco Secure ACS to monitor user authentication services, check the **Enable Log-in Monitoring** check box. From the Script to execute menu, choose the option you want applied in the event of authentication service failure:

- **No Remedial Action:** Cisco Secure ACS does not run a script.
- **Reboot:** Cisco Secure ACS runs a script that reboots the computer that runs Cisco Secure ACS.
- **Restart All:** Cisco Secure ACS restarts all Cisco Secure ACS services.
- **Restart RADIUS/TACACS+:** Cisco Secure ACS restarts only the RADIUS and TACACS+ services.

Step 17 If you want Cisco Secure ACS to send an e-mail message when service monitoring detects an event, check the **Mail Notification** check box.

Step 18 Click **Next**.

If, in Step 12, you specified TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX) as the AAA protocol for your first AAA client, the Network Access Server Configuration dialog box appears.

If, in Step 12, you specified an AAA protocol other than TACACS+ (Cisco IOS) or RADIUS (Cisco IOS/PIX), the CiscoSecure ACS Service Initiation dialog box appears.

Step 19 If the Network Access Server Configuration dialog box appears and you want to configure AAA functionality on a Cisco IOS network device, follow these steps:

1. Check the **Yes, I Want to Configure Cisco IOS Software Now** check box and click **Next**.

The Enable Secret Password dialog box appears.

2. In the Enable Secret Password box, type an enable secret password for the Cisco IOS network device.

Note You must type the shared secret exactly as it is configured on the Cisco IOS device, including whether the characters are uppercase or lowercase.

3. Click **Next**.

The Access Server Configuration dialog box displays information about configuring a Cisco IOS network device.

4. After reading the text in the Access Server Configuration dialog box, click **Next**.

The NAS Configuration dialog box displays the minimum Cisco IOS configuration needed for the network device that you specified in Step 12. The minimum configuration includes information that you have provided during installation, including the IP address of the computer you are installing Cisco Secure ACS on, the TACACS+ or RADIUS key, and the enable secret password.

5. If you want to print the minimum Cisco IOS configuration, click **Print**.
6. To Telnet to the network device that you specified in Step 12, click **Telnet Now**.
7. After you finish with the options in the NAS Configuration dialog box, click **Next**.

Step 20 For each option that you want, check the corresponding check box. The actions associated with the options occur after the setup program finishes.

- **Yes, I Want to Start the CiscoSecure ACS Service Now:** Starts the Windows services that compose Cisco Secure ACS. If you do not check this option, the Cisco Secure ACS HTML interface is not available unless you reboot the computer or start the CSAdmin service.
- **Yes, I Want Setup to Launch the CiscoSecure ACS Administrator from My Browser Following Installation:** Opens the Cisco Secure ACS HTML interface in the default web browser for the current Windows user account.
- **Yes, I Want to View the Readme File:** Opens the README.TXT file in Windows Notepad.

Step 21 Click **Next**.

Step 22 Click **Finish**.

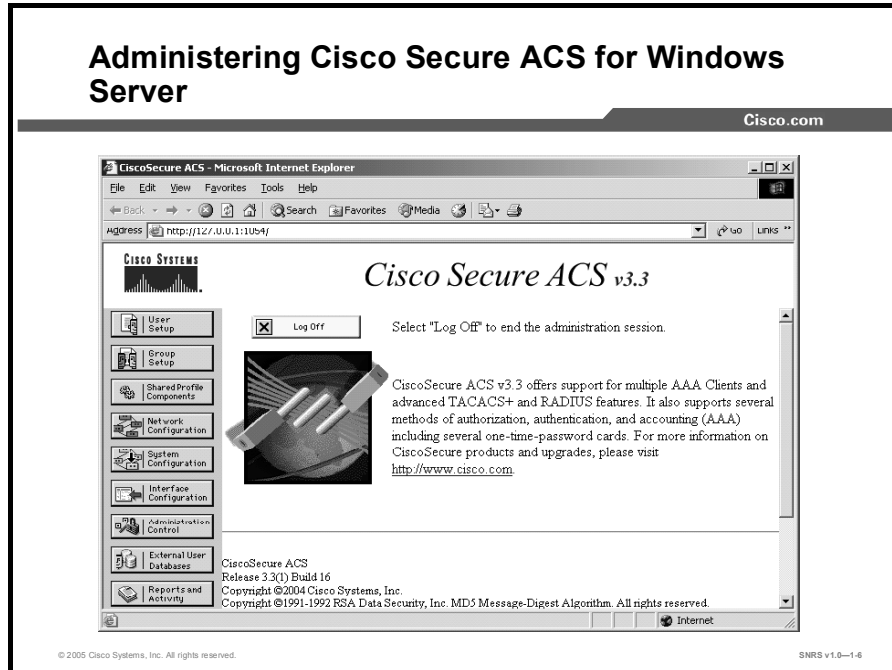
On the computer running Cisco Secure ACS, you can access the Cisco Secure ACS HTML interface using the **ACS Admin** desktop icon, or you can use the following URL in a supported web browser:

<http://127.0.0.1:2002>

Step 23 If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration.

Administering Cisco Secure ACS for Windows Server

This topic describes basic Cisco Secure ACS for Windows Server administration.



The Cisco Secure ACS for Windows Server web browser interface makes administration of AAA features easy.

Navigation Buttons

Each of the buttons on the menu 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. Click one of these buttons to begin configuring:

- **User Setup:** Add, edit, or delete user accounts, and list users in databases.
- **Group Setup:** Create, edit, or rename groups, and list all users in a group.
- **Shared Profile Components:** Develop and name reusable, shared sets of authorization components that 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 AAA clients and server parameters; add and delete network access clients and servers; and configure AAA server distribution parameters.
- **System Configuration:** Start and stop Cisco Secure ACS for Windows Server services, configure logging, control database replication, and control RDBMS synchronization.

- **Interface Configuration:** Configure user-defined fields that will be recorded in accounting logs; configure TACACS+ and RADIUS options; and 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; and configure external database types.
- **Reports and Activity:** Click **Reports and Activity** in the menu 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 and Activity:
 - **TACACS+ Accounting Report:** Lists when sessions stop and start; records NAS messages with username; provides caller line identification information; records the duration of each session
 - **RADIUS Accounting Report:** Lists when sessions stop and start; records NAS 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 NAS or all NASs 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) NAS
- **Online Documentation:** Get more detailed information about the configuration, operation, and concepts of Cisco Secure ACS for Windows Server.

Troubleshooting

This topic describes troubleshooting techniques for Cisco Secure ACS.

Cisco Secure ACS for Windows Server: Troubleshooting

Cisco.com

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	aauser	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	aauser	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	is-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.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.6--1.7

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 NAS configured with the **ppp authentication pap** command?
- Is the User Must Change Password at Next Login check box checked in Windows 2000 Server? (Uncheck it if it is.)
- Does the user 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 user 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 the 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 it 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 clicked?
- Has the Permitted radio button for the argument been clicked?

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 condition:

- 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 dialup 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 and username and password).

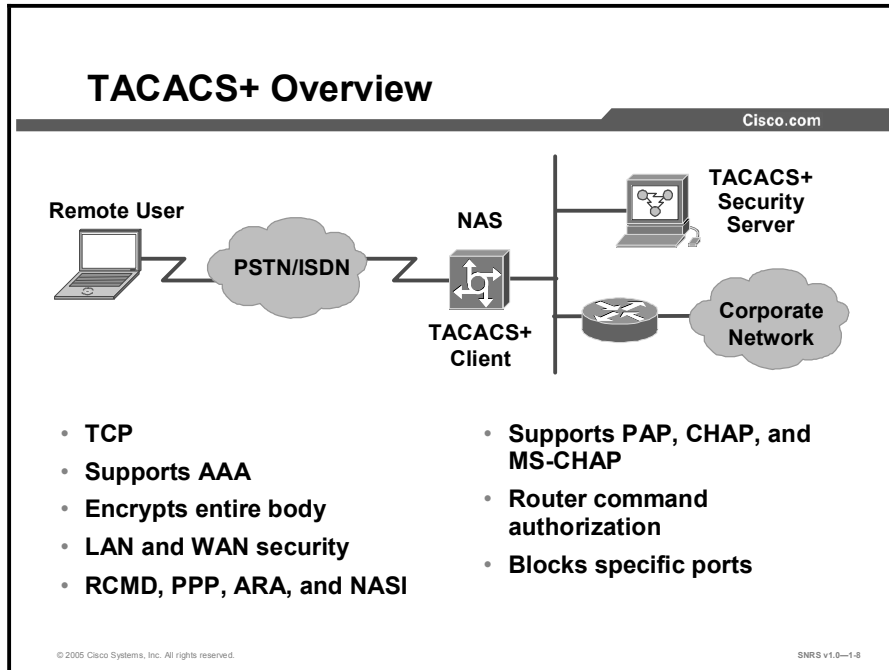
Useful Cisco IOS Commands

The following Cisco IOS **debug** commands are useful for troubleshooting:

```
debug aaa authentication
debug aaa authorization
debug TACACS+
debug RADIUS
```

TACACS+

This topic gives an overview of TACACS+.



TACACS+ Overview

Key TACACS+ features include these:

- TACACS+ separates AAA into three distinct functions (authentication, authorization, and accounting).
- TACACS+ supports router command authorization integration with advanced authentication mechanisms, such as Data Encryption Standard (DES) and One-Time Password (OTP) key.
- TACACS+ supports 16 different privilege levels (0–15).
- TACACS+ permits the control of services, such as PPP, shell, standard login, enable, ARA protocol, Novell Asynchronous Services Interface (NASi), remote command (RCMD), and firewall proxy.
- TACACS+ permits the blocking of services to a specific port, such as a TTY or VTY interface on a router.

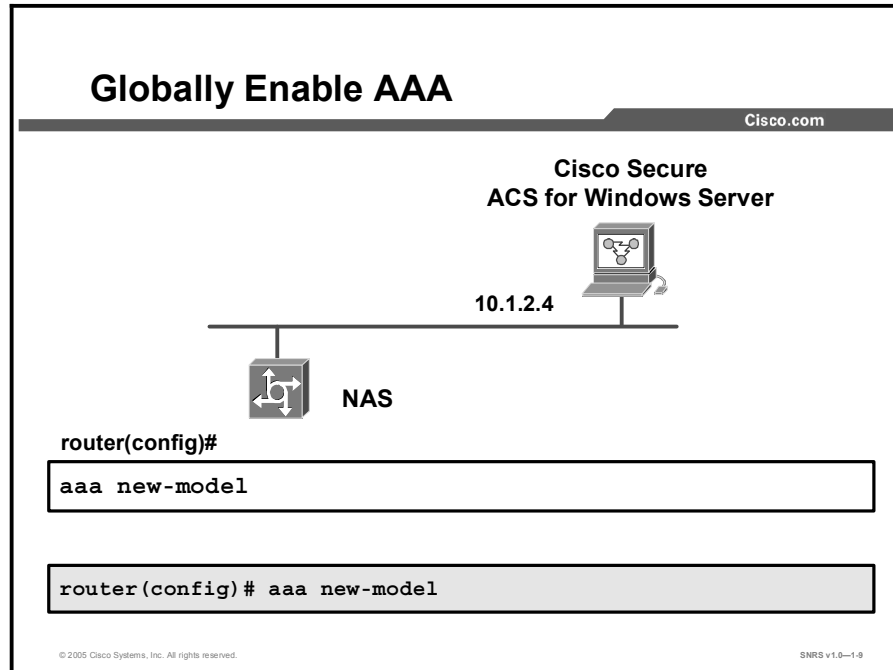
The most common services supported by TACACS+ are PPP for IP and router EXEC shell access using console or VTY ports. EXEC shell allows users to connect to router shells and choose services such as PPP, Telnet, or TN3270 or manage the router itself.

When configured correctly, the AAA server validates AAA and responds to requests from routers and access servers with a pass or fail signal.

The AAA server acts as a proxy server by using TACACS+ to authenticate, authorize, and account for access to Cisco routers and NASs.

Enabling TACACS+

This topic describes how to enable TACACS+ on a router.



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.

Caution 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 group 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

Cisco.com

You can either use the two commands shown here to share the key with all servers or

use this command for a single server (see note in text)

```
router(config)#
```

```
tacacs-server key keystring
```

```
router(config)# tacacs-server key 2bor!2b@?
```

```
router(config)#
```

```
tacacs-server host ipaddress
```

```
router(config)# tacacs-server host 10.1.2.4
```

```
router(config)#
```

```
tacacs-server host ipaddress key keystring
```

```
router(config)# tacacs-server host 10.1.2.4 key 2bor!2b@?
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.10

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 that you choose for your environment should be kept secret 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 next.

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

Cisco.com

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]]
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.11

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 (ARA protocol 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 (ARA protocol, PPP, or NASI) or login authentication.
- Step 2** Identify a list name or default. A list name is any alphanumeric string that 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 protocol.
- Interfaces: Interfaces (synchronous or asynchronous) configured for PPP.
- Use the **aaa authentication** command in global configuration mode to enable AAA authentication processes.

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
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in
<i>method</i>	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 <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ commands

NAS AAA Configuration Example for TACACS+

Cisco.com

```
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication ppp default group 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$33AXd2VTVvvhbWLOA37tQ3.
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.12

Consider the NAS configuration example in the figure, which has been edited to show only commands important to AAA security:

```
■ router(config)# aaa new-model
```

This command enables the AAA access control model. Using 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:

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

This command 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:

```
■ router(config)# aaa authentication ppp default tacacs+
```

This command sets AAA authentication for PPP connections using the default list against the TACACS+ database:

```
■ router(config)# aaa authorization exec tacacs+
```

This command sets AAA authorization to determine if the user is allowed to run an EXEC shell on the NAS against the TACACS+ database:

```
■ router(config)# aaa authorization network tacacs+
```

This command sets AAA authorization for all network-related service requests, including Serial Line Interface Protocol (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:

```
■ router(config)# aaa accounting exec start-stop tacacs+
```

This command sets AAA accounting for EXEC processes on the NAS to record the start and stop time of the session against the TACACS+ database:

```
■ router(config)# aaa accounting network start-stop tacacs+
```

This command 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:

```
■ router(config)# username admin password 7 094E4F0A1201181D19
```

This command sets a username and password in the local security database for use with the **aaa authentication local-override** command:

```
■ router(config)# interface Serial2
```

```
■ router(config-if)# ppp authentication pap
```

This command sets PPP authentication to use Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or CHAP, PAP, and Microsoft CHAP (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:

```
■ router(config)# tacacs-server host 10.1.1.4
```

```
■ router(config)# tacacs-server key ciscosecure
```

The first steps in configuring the router are these:

- 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.

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 ACS) if you wish the connection not to be encrypted. This configuration might be useful for a lab or training environment, but is strongly discouraged in a production environment.

The **tacacs-server** command is described in the table.

tacacs-server host { <i>hostname</i> <i>ip-address</i> }	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 <i>shared-secret-text-string</i>	<p>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.</p> <p>It is possible to configure TACACS+ without a shared key at both the client device (that is, the NAS) and the security server (that is, Cisco Secure ACS) if you wish the connection not to be encrypted. This configuration might be useful for a lab or training environment, but is strongly discouraged in a production environment.</p>

The following commands specify that the AAA authentication list called `no_tacacs` is to be used on the console:


```
router(config)# line con 0
router(config-if)# login authentication no_tacacs
```

Verifying TACACS+

This topic describes the process of TACACS+ verification.

AAA TACACS+ Troubleshooting

Cisco.com



router#

`debug tacacs`

- **Displays detailed information associated with TACACS+**

router#

`debug tacacs events`

- **Displays detailed information from the TACACS+ helper process**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-1-13

When TACACS+ is used on a router, you can use the **debug tacacs** command for more detailed debugging information.

Use the **debug tacacs** command on the router to trace TACACS+ packets.

Use the **debug tacacs events** command to display information from the TACACS+ helper process.

debug aaa authentication Command TACACS+ Example Output

Cisco.com

```
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen
      response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.14

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

Cisco.com

```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1-15

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

Cisco.com

```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1-16

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

Cisco.com

```
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)
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-1.17

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 TCP status of the connection.

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:

- **00:03:16: TAC+: Opening TCP/IP to 10.1.1.4/49 timeout=15:** 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+: Opened TCP/IP handle 0x48A87C to 10.1.1.4/49:** This message indicates a successful open operation and provides the address of the internal TCP “handle” for this connection.

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 the **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.

<i>type</i>	Type of message to time-stamp—debug or log
uptime	(Optional) Time-stamp with time since the system was rebooted
datetime	Time-stamp with the date and time
msec	(Optional) Include milliseconds in the date and time stamp
localtime	(Optional) Time-stamp relative to the local time zone
show-timezone	(Optional) Include the time zone name in the time stamp

RADIUS

This topic describes RADIUS.

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

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-1.18

RADIUS is an access server AAA protocol developed by Livingston Enterprises (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 software, starting with Cisco IOS Software 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 password.

Configuring RADIUS

This topic describes RADIUS configuration.

RADIUS Server Command

Cisco.com

You can either use the two commands shown here to share the key with all servers

or

you can use this command for a single server.

```
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
```

```
router(config)#
radius-server host ipaddress key keystring
```

```
router(config)# radius-server host 10.1.2.4 key
2bor!2b@?
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-1-19

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 keywords shown in the table.

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	Uses RADIUS authentication
tacacs+	Uses TACACS+ authentication

You can create AAA accounting for RADIUS connections and with TACACS+.

Use line and interface commands to cause the defined method lists to be used.

Use the **radius-server** command to configure the router to RADIUS server communication.

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 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 is specified in RFC 2139.
- **Cisco implementation, supporting approximately 58 attributes:** Starting in Cisco IOS Software Release 11.2, an increasing number of attributes and functionality have been included in each release of Cisco IOS software and Cisco Secure ACS.
- **Lucent, supporting more than 254 attributes:** Lucent is constantly changing and adding vendor-specific attributes (VSAs) such as token caching and password changing. An application programming interface (API) enables rapid development of new extensions. Although Livingston Enterprises developed RADIUS originally, it was championed by Ascend.

Vendors have implemented proprietary extensions to RADIUS features. TACACS+ is considered superior because of the following:

- TACACS+ encrypts the entire TACACS+ packet. (RADIUS encrypts only the shared-secret password portion.)
- TACACS+ separates authentication and authorization, making possible distributed security services.
- RADIUS has limited name space for attributes.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Installation requires specific information about the computer that you want to install Cisco Secure ACS on and a AAA client on your network.**
- **If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform the additional Windows configuration.**
- **Initial configuration is done via a web interface.**
- **You should check connectivity between Cisco Secure ACS server and AAA clients.**
- **Troubleshooting tools include debug commands for TACACS+.**
- **The failed Attempts report is used in troubleshooting access problems.**
- **TACACS+ and RADIUS are supported by Cisco Secure ACS.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-1-20

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **Cisco Secure ACS for Windows Server is a feature-rich application used to work with a wide variety of AAA clients and databases. Authentication is done using TACACS+ or RADIUS configured on various network devices such as NASs, Cisco PIX Firewall, Cisco VPN Concentrator, routers, and now switches for Layer 2 security.**
- **A web interface is required for initial configuration and makes administration user-friendly. Tools include reports for troubleshooting access problems and debug commands for troubleshooting TACACS+ and RADIUS.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0--1-1

This module covered Cisco Secure ACS for Windows Server and described how to configure it to provide AAA services for a typical network. The module first introduced Cisco Secure ACS for Windows Server, describing the features, functions, architecture, and supported protocols and databases. It then detailed these objects as well as the services installed as part of Cisco Secure ACS and listed key features of the latest release, Cisco Secure ACS 3.3. The module then covered the installation and configuration of a new installation of Cisco Secure ACS for Windows Server. Administration and troubleshooting of Cisco Secure ACS was then covered, after which AAA configuration on the router was covered. This included configuration for TACACS+ and RADIUS. Troubleshooting and debugging AAA was reviewed last.

Module 2

Cisco IOS Security Features

Overview

Cisco IOS software has a full set of security features that the user can implement to provide security for the network. In this module, you will learn how to install, configure, operate, and troubleshoot Cisco IOS Firewall Context-Based Access Control (CBAC), Cisco IOS Firewall authentication proxy and Cisco IOS Firewall Intrusion Prevention System (IPS) on a Cisco router attached to a lab network.

Module Objectives

Upon completing this module, you will be able to install, configure, operate, and troubleshoot Cisco IOS Firewall CBAC, Cisco IOS Firewall authentication proxy, and Cisco IOS Firewall IPS on a Cisco router. This ability includes being able to meet these objectives:

- Describe the purpose, application, and operation of the main features of the Cisco IOS Firewall, including CBAC, authentication proxy, and IPS
- Configure the main features of the Cisco IOS Firewall, including CBAC, on a Cisco router
- Configure Cisco IOS Firewall authentication proxy on a Cisco router
- Configure Cisco IOS IPS on a Cisco router

Lesson 1

Introducing Cisco IOS Firewall Context-Based Access Control

Overview

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and the Context-based Access Control (CBAC) feature. When you configure the Cisco IOS Firewall on your Cisco router, you turn your router into an effective, robust firewall. To create a firewall customized to fit the security policy of your organization, you should determine which Cisco IOS Firewall features are appropriate and configure those features. At a minimum, you should configure basic traffic filtering to provide a basic firewall. This lesson covers the Cisco IOS Firewall feature set and introduces CBAC.

Objectives

Upon completing this lesson, you will be able to describe the purpose, application, and operation of the main features of the Cisco IOS Firewall, including CBAC, authentication proxy, and IPS. This ability includes being able to meet these objectives:

- Describe the role of the each component of the Cisco IOS Firewall feature set
- Explain how Cisco IOS Firewall CBAC inspects traffic
- Describe Cisco IOS Firewall authentication proxy
- Describe Cisco IOS Firewall IPS
- Describe how Cisco IOS ACLs provide traffic filtering
- Explain how CBAC protects networks from attack

Cisco IOS Firewall Feature Set

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 Prevention System**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2.3

The Cisco IOS Firewall is a security-specific option for Cisco IOS software. It integrates robust firewall functionality, authentication proxy, and intrusion prevention 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 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.

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and the Context-based Access Control (CBAC) feature. When you configure the Cisco IOS Firewall on your Cisco router, you turn your router into an effective, robust firewall.

The Cisco IOS Firewall features are designed to prevent unauthorized external individuals from gaining access to your internal network and to block attacks on your network, while at the same time allowing authorized users to access network resources.

You can use the Cisco IOS Firewall features to configure your Cisco IOS router as one of the following:

- An Internet firewall or part of an Internet firewall
- A firewall between groups in your internal network
- A firewall providing secure connections to or from branch offices
- A firewall between your company network and the networks of your company's partners

The Cisco IOS Firewall features provide the following benefits:

- Protection of internal networks from intrusion
- Monitoring of traffic through network perimeters
- Enabling of network commerce through the World Wide Web

Creating a Customized Firewall

To create a firewall customized to fit the security policy of your organization, you should determine which Cisco IOS Firewall features are appropriate, and configure those features. At a minimum, you must configure basic traffic filtering to provide a basic firewall. You can configure your Cisco networking device to function as a firewall by using the following Cisco IOS Firewall features:

- Standard access control lists (ACLs) and static extended ACLs
- Lock-and-Key (dynamic ACLs)
- Reflexive ACLs
- TCP intercept
- CBAC
- Cisco IOS Firewall Intrusion Prevention System (IPS)
- Authentication proxy
- Port-to-application mapping (PAM)
- Security server support
- Network Address Translation (NAT)
- IPsec network security
- Neighbor router authentication
- Event logging
- User authentication and authorization

Context-Based Access Control

The Cisco IOS Firewall 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 the network of a partner. CBAC enables tightly secured networks to run the basic application traffic of today, 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 fixed IP address for a user, 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 TACACS+ or RADIUS authentication server using Cisco IOS software authentication, authorization, and accounting (AAA) services.

Users can log in to 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.

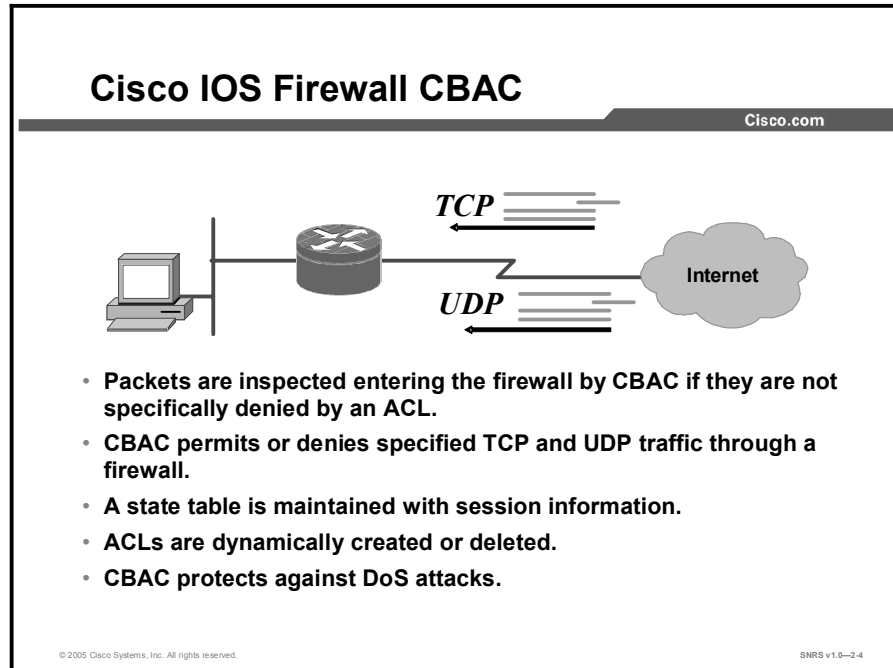
Intrusion Prevention System

Intrusion prevention systems (IPSs) provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS Firewall IPS technology enhances perimeter firewall protection by taking appropriate actions on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS Firewall IPS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators now enjoy more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts.

Context-Based Access Control

This topic describes CBAC.



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 ACLs to allow return traffic and additional data connections for permissible sessions.

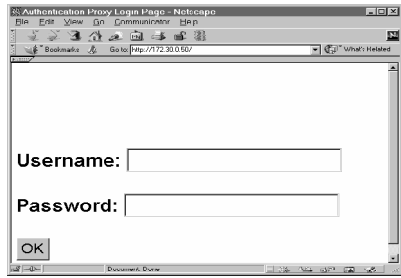
Inspecting packets at the application layer and maintaining TCP and UDP session information provides CBAC with the ability to detect and prevent certain types of network attacks, such as SYN flooding. CBAC also inspects packet sequence numbers in TCP connections to see if they are within expected ranges—CBAC 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.

Authentication Proxy

This topic describes Cisco IOS Firewall authentication proxy.

Cisco IOS Firewall Authentication Proxy

Cisco.com



The screenshot shows a Netscape browser window titled "Authentication Proxy Login Page - Netscape". The address bar contains "Go to [http://7172.30.0.160/". The main content area displays a login form with two input fields: "Username:" and "Password:". Below the fields is an "OK" button. The browser's status bar at the bottom shows "Document: Done".

- **HTTP, HTTPS, FTP, and Telnet authentication**
- **Provides dynamic, per-user authentication and authorization via TACACS+ and RADIUS protocols**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.6

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 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 (ACS) or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

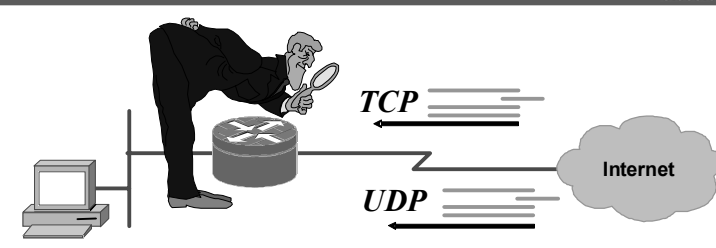
The authentication proxy is compatible with other Cisco IOS security features, such as NAT, IPSec encryption, and VPN client software.

Intrusion Prevention System

This topic describes intrusion protection.

Cisco IOS Firewall Intrusion Prevention System

Cisco.com



The diagram shows a person in a suit leaning over a Cisco IOS router, inspecting traffic. To the left is a PC. To the right is a cloud labeled 'Internet'. Arrows labeled 'TCP' and 'UDP' indicate traffic flow between the router and the Internet.

- Acts as an inline Cisco IOS intrusion prevention sensor.
- When a packet or packets match a signature, it can perform any of the following configurable actions:
 - Alarm: Send an alarm to a Security Device Manager or syslog server.
 - Drop: Drop the packet.
 - Reset: Send TCP resets to terminate the session.
- Identifies 700+ common attacks.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0--2.4

The Cisco IOS Firewall IPS now offers intrusion prevention technology for midrange 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 Firewall IPS identifies 700 or more common attacks using signatures to detect patterns of misuse in network traffic. The intrusion prevention signatures of the Cisco IOS Firewall IPS were chosen from a broad cross-section of intrusion prevention signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

Cisco IOS ACLs

This topic describes the limitations of Cisco IOS ACLs and explains how 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

Cisco.com

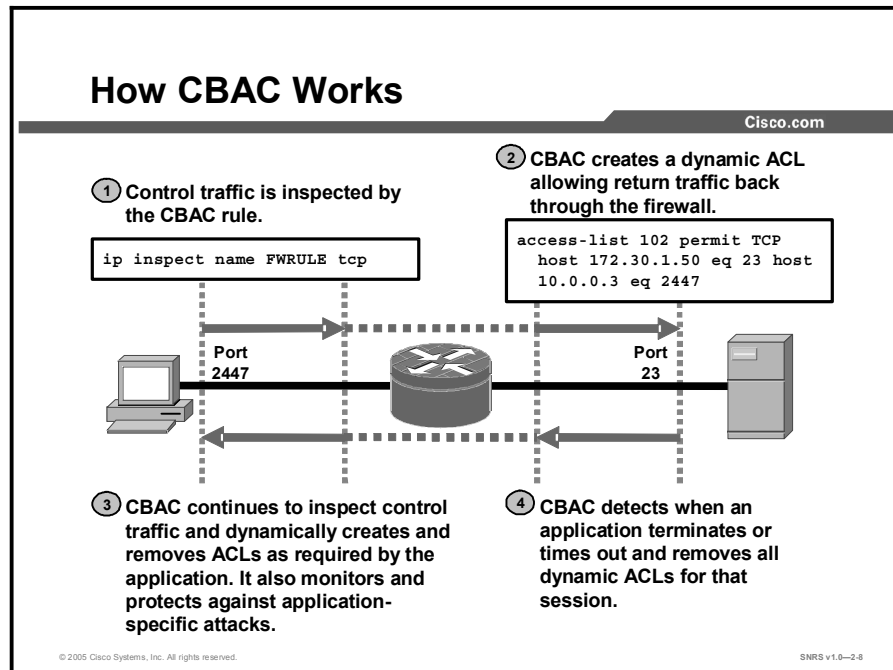
- **Provide traffic filtering by**
 - **Source and destination IP addresses**
 - **Source and destination ports**
- **Can be used to implement a filtering firewall**
 - **Ports opened permanently to allow traffic, creating a security vulnerability**
 - **Do not work with applications that negotiate ports dynamically**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2.7

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.

CBAC Process

This topic describes the CBAC process.



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 are 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:

- It can 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 connection. Return traffic will be permitted back through the firewall only 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 Real Networks)**
- **H.323 (such as NetMeeting, ProShare, CUseeMe)**
- **Other multimedia**
 - **Microsoft NetShow**
 - **StreamWorks**
 - **VDOLive**
- **SIP**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.0

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:

- Remote-procedure call (RPC) (Sun RPC, not Distributed Computing Environment [DCE] RPC)
- Microsoft RPC
- FTP
- TFTP
- UNIX R-commands (such as rlogin, rexec, and rsh)
- SMTP
- HTTP (Java blocking)
- Internet Control Message Protocol (ICMP)
- SQL*Net
- Real-Time Streaming Protocol (RTSP) (for example: RealNetworks)
- H.323 (for example: NetMeeting, ProShare, CUseeMe [only the White Pine version])
- Microsoft NetShow
- StreamWorks
- VDOLive
- Session Initiation Protocol (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.

Alerts and Audit Trails

Cisco.com

- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—2-10

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.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The Cisco IOS Firewall contains three main features: Context-based Access Control, authentication proxy, Intrusion Prevention System.**
- **CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information.**
- **You can also configure CBAC to specifically inspect certain application-layer protocols.**
- **The Cisco IOS Firewall authentication proxy feature enables network administrators to apply specific security policies on a per-user basis.**
- **The Cisco IOS Firewall IPS identifies 700 or more common attacks using signatures to detect patterns of misuse in network traffic.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.11

Summary (Cont.)

Cisco.com

- **With CBAC, you specify which protocols you want inspected, and you specify an interface and interface direction (in or out) where the inspection originates.**
- **Enhanced audit trail features use syslog to track all network transactions.**
- **Real-time alerts send syslog error messages to central management consoles upon detecting suspicious activity.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.12

Lesson 2

Configuring Cisco IOS Firewall Context-Based Access Control

Overview

This lesson covers the tasks required to configure Cisco IOS Firewall Context-based Access Control (CBAC) on a perimeter router. You will learn basic access control list (ACL) configuration as well as configuration of inside and outside interfaces. Audit trail logging, alerts, and global timeouts and thresholds are covered to allow you to maintain and monitor CBAC.

Objectives

Upon completing this lesson, you will be able to configure CBAC. This ability includes being able to meet these objectives:

- List the tasks required to configure CBAC
- List the steps required to turn on audit trail logging and real-time alerts
- Configure global timeouts and thresholds
- Configure port numbers for application protocols (optional)
- Configure the rules used to define the application protocols
- Apply inspection rules and ACLs to router interfaces
- Verify CBAC configurations

CBAC Configuration Tasks

This topic lists the tasks required to configure CBAC.

CBAC Configuration

Cisco.com

- **Pick an interface: internal or external.**
- **Configure IP ACLs at the interface.**
- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2.3

The following are the tasks used to configure CBAC:

- Pick an interface: internal or external
- Configure IP ACLs at the interface
- 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

Picking an Interface: Internal or External

You must decide whether to configure CBAC on an internal or external interface of your firewall.

“Internal” refers to the side where sessions must originate for their traffic to be permitted through the firewall. “External” refers to the side where sessions cannot originate (sessions originating from the external side will be blocked).

If you will be configuring CBAC in two directions, you should configure CBAC in one direction first, using the appropriate “internal” and “external” interface designations. When you configure CBAC in the other direction, the interface designations will be swapped. (CBAC can be configured in two directions at one or more interfaces. Configure CBAC in two directions when the networks on both sides of the firewall require protection, such as with extranet or intranet configurations, and for protection against denial of service [DoS] attacks.)

Configuring IP Access Lists at the Interface

For CBAC to work properly, you need to make sure that you have IP ACLs configured appropriately at the interface.

Follow these three general rules when evaluating your IP ACLs at the firewall:

- Start with a basic configuration.

If you try to configure ACLs without a good understanding of how ACLs work, you might inadvertently introduce security risks to the firewall and to the protected network. You should be sure you understand what ACLs do before you configure your firewall.

A basic initial configuration allows all network traffic to flow from the protected networks to the unprotected networks, while blocking network traffic from any unprotected networks.

- Permit CBAC traffic to leave the network through the firewall.

All ACLs that evaluate traffic leaving the protected network should permit traffic that will be inspected by CBAC. For example, if Telnet will be inspected by CBAC, then Telnet traffic should be permitted on all ACLs that apply to traffic leaving the network.

- Use extended ACLs to deny CBAC return traffic entering the network through the firewall.

For temporary openings to be created in an ACL, the list must be an extended ACL. So wherever you have ACLs that will be applied to returning traffic, you must use extended ACLs. The ACLs should deny CBAC return traffic because CBAC will open up temporary holes in the ACLs. (You normally want traffic to be blocked when it enters your network.)

Note If your firewall only has two connections, one to the internal network and one to the external network, using all inbound ACLs works well because packets are stopped before they get a chance to affect the router itself.

Basic Configuration

The first time that you configure the Cisco IOS Firewall, it is helpful to start with a basic ACL configuration that makes the operation of the firewall easy to understand without compromising security. The basic configuration allows all network traffic from the protected networks to have access to the unprotected networks, while blocking all network traffic (with some exceptions) from the unprotected networks to the protected networks.

Any firewall configuration depends on your site security policy. If the basic configuration does not meet your initial site security requirements, configure the firewall to meet your policy. If you are unfamiliar with that policy or need help with the configuration, contact your network administration group for assistance.

Use the following guidelines for configuring the initial firewall ACLs:

- Do not configure an ACL for traffic from the protected networks to the unprotected networks, meaning that all traffic from the protected networks can flow through the interface.

This configuration helps to simplify firewall management by reducing the number of ACLs applied at the interfaces. Of course it assumes a high level of trust for the users on the protected networks, and it assumes there are no malicious users on the protected networks who might launch attacks from the inside. You can fine-tune network access for users on the protected networks as you gain experience with ACL configuration and the operation of the firewall.

- Configure an ACL that includes entries permitting certain ICMP traffic from unprotected networks.

While an ACL that denies all IP traffic not part of a connection inspected by CBAC seems most secure, it is not practical for normal operation of the router. The router expects to see ICMP traffic from other routers in the network. Additionally, ICMP traffic is not inspected by CBAC, meaning that specific entries are needed in the ACL to permit return traffic for ICMP commands. For example, a user on a protected network uses the **ping** command to get the status of a host on an unprotected network; without entries in the ACL that permit echo-reply messages, the user on the protected network gets no response to the **ping** command.

- Add an ACL entry denying any network traffic from a source address matching an address on the protected network.

This is known as antispoofing protection because it prevents traffic from an unprotected network from assuming the identity of a device on the protected network.

- Add an entry denying broadcast messages with a source address of 255.255.255.255.

This entry helps to prevent broadcast attacks.

- By default, the last entry in an extended ACL is an implicit denial of all IP traffic not specifically allowed by other entries in the ACL.

Although it is the default setting, this final deny statement is not shown by default in an ACL. Optionally, you can add an entry to the ACL denying IP traffic with any source or destination address with no undesired effects.

External Interface

Here are some guidelines for your ACLs when you configure CBAC on an external interface:

- If you have an outbound IP ACL at the external interface, the ACL can be a standard or extended ACL. This outbound ACL should permit traffic that you want to be inspected by CBAC. If traffic is not permitted, it will not be inspected by CBAC but will simply be dropped.
- The inbound IP ACL at the external interface must be an extended ACL. This inbound ACL should deny traffic that you want to be inspected by CBAC. (CBAC will create temporary openings in this inbound ACL as appropriate to permit only return traffic that is part of a valid, existing session.)
- For complete information about how to configure IP ACLs, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*.

Internal Interface

Here are some tips for your ACLs when you configure CBAC on an internal interface:

- If you have an inbound IP ACL at the internal interface or an outbound IP ACL at one or more external interfaces, these ACLs can be either a standard or extended ACL. These ACLs should permit traffic that you want to be inspected by CBAC. If traffic is not permitted, it will not be inspected by CBAC, but will simply be dropped.
- The outbound IP ACL at the internal interface and the inbound IP ACL at the external interface must be extended ACLs. These outbound ACLs should deny traffic that you want to be inspected by CBAC. (CBAC will create temporary openings in these outbound ACLs as appropriate to permit only return traffic that is part of a valid, existing session.) You do not necessarily need to configure an extended ACL at both the outbound internal interface and the inbound external interface, but at least one is necessary to restrict traffic flowing through the firewall into the internal protected network.
- For complete information about how to configure IP ACLs, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*.

Audit Trail Logging

This topic lists the steps required to turn on audit trail logging and real-time alerts.

Enable Audit Trails and Alerts

Cisco.com

```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2.4

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 that 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 that the Cisco IOS Firewall waits for a FIN exchange to complete before quitting the session

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.5

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
```

<i>seconds</i>	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 continue to 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
```

<i>seconds</i>	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

Cisco.com

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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0--2.6

Use the **ip inspect tcp idle-time** global configuration command to specify the TCP idle timeout (the length of time that a TCP session will continue to be managed when there is no activity). Use the **no** form of this command to reset the timeout to the default.

Use the **ip inspect udp idle-time** global configuration command to specify the UDP idle timeout (the length of time that a UDP session will continue to be managed when there is no activity). Use the **no** form of this command to reset the timeout to the 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
```

<i>seconds</i>	Specifies the length of time that a TCP or a UDP session will continue to be managed when there is 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
```

<i>seconds</i>	Specifies the length of time that a DNS name lookup session will continue to be managed when there is no activity (the default is 5 seconds).
----------------	---

Global Half-Opened Connection Limits

Cisco.com

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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.7

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 (set by the **max-incomplete high *number*** command), CBAC will go into 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 (set by the **max-incomplete low *number*** command).

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 the 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
```

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 the 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
```

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).
-------------------	---

Global Half-Opened Connection Limits (Cont.)

Cisco.com

Router(config)#

```
ip inspect one-minute high number
```

- Defines the number of new half-opened sessions per minute at which they start being deleted

Router(config)#

```
ip inspect one-minute low number
```

- Defines the number of new half-opened sessions per minute at which they stop being deleted

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0--2-8

When the rate of new connection attempts rises above a threshold (set by the **one-minute high number** command), 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 (set by the **one-minute low number** command). The rate thresholds are measured as the number of new session connection attempts detected in the most recent 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 once a minute and that it 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 unestablished sessions that will cause the software to start 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 high** command is as follows:

```
ip inspect one-minute high number
```

```
no ip inspect one-minute high
```

high <i>number</i>	Specifies the rate of new unestablished 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 unestablished 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 <i>number</i>	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).
--------------------------	---

Half-Opened Connection Limits by Host

Cisco.com

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 to a given host is exceeded, the software deletes half-opened 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.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0--2.0

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 (set by the **max-incomplete host number** command), the software will delete half-opened sessions according to one of the following methods:

- If the timeout set by the **block-time minutes** command 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 process ensures that the number of half-opened sessions to a given host will never exceed the threshold.
- If the timeout set by the **block-time minutes** command 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 value specified by the **max-incomplete host number** command 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 <i>number</i>	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 <i>minutes</i>	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 describes the configuration of port numbers for application protocols.

Port-to-Application Mapping

Cisco.com

- **Ability to configure any port number for an application protocol.**
- **CBAC uses PAM to determine the application configured for a port.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2.10

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 table shows 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
- Internet Message Access Protocol (IMAP)
- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- Lotusnote
- Microsoft SQL (MS-SQL)
- Network File System (NFS)
- Network News Transfer Protocol (NNTP)
- Post Office Protocol Version 2 (POP2)
- POP3
- Service Advertisement Protocol (SAP)
- Simple Network Management Protocol (SNMP)
- Sybase-SQL
- TACACS+

User-Defined Port Mapping

Cisco.com

Router(config)#

```
ip port-map appl_name port port_num
```

- Maps a port number to an application

Router(config)#

```
access-list acl_num permit 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 acl_num permit 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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2-11

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]
```

<i>appl_name</i>	Specifies the name of the application with which to apply the port mapping
port <i>port_num</i>	Identifies a port number in the range 1 to 65535
list <i>acl_num</i>	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

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2-12

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]
```

<i>appl_name</i>	Specifies the application for which to display information
port <i>port_num</i>	Specifies the alternative port number that maps to the application for which to display information

Define Inspection Rules

This topic describes how to configure the rules used to define the application protocols.

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, ftp, and vdolive
 - alert, audit-trail, and timeout 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
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.13

Inspection rules must be defined to specify which 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 <i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name.
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, the audit-trail option can be set to on or off. If no option is selected, audit trail messages are generated based on the setting of the ip inspect audit trail command.
timeout <i>seconds</i>	(Optional) Specify the number of seconds for a different idle timeout to override the global TCP or UDP idle timeouts for the specified protocol. This timeout overrides the global TCP and UDP timeouts but will not override the global DNS timeout.

Inspection Rules for Java

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.14

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 is 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 <i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.
http	Specifies the HTTP protocol used.
java-list <i>acl-num</i>	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 works only 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, the audit-trail option can be set to on or off. If no option is selected, audit trail messages are generated based on the setting of the ip inspect audit-trail command.
timeout <i>seconds</i>	(Optional) Specifies 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 RPC Applications

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.15

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
```

<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.
rpc program_number <i>number</i>	Specifies the program number to permit.
wait-time <i>minutes</i>	(Optional) Specifies the number of minutes to keep the connection open 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 0 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, the audit-trail option can be set to on or off. If no option is selected, audit trail messages are generated based on the setting of the ip inspect audit-trail command.
timeout <i>seconds</i>	(Optional) Specifies 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 SMTP Applications

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.16

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 <i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name 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, the audit-trail option can be set to on or off. If no option is selected, audit trail messages are generated based on the setting of the ip inspect audit-trail command.
timeout <i>seconds</i>	(Optional) Specifies 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

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0–2-17

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 fragment state resources of the firewall, 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
```

<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.
fragment	Specifies fragment inspection for the named rule.
max <i>number</i>	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 <i>seconds</i>	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 1 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

Cisco.com

Router(config)#

```
ip inspect name inspection-name icmp [alert  
{on|off}] [audit-trail {on|off}] [timeout  
seconds]
```

- Configures Cisco 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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2-18

Although 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 Cisco IOS Software Releases 12.2(11)YU and later with the Cisco 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 are not allowed. The following table identifies the Cisco 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 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 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
```

<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name 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 <i>seconds</i>	(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 in
!
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 a wildcard address in the ACL. The wildcard 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.

Apply Inspection Rules and ACLs to Interfaces

This topic describes how to apply 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

```
Router(config)# interface e0/0
Router(config-if)# ip inspect FWRULE in
```

- Applies the inspection rule to interface e0/0 in inward direction

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.19

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 }
```

<i>inspection-name</i>	Names the set of inspection rules.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

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**

© 2005 Cisco Systems, Inc. All rights reserved.

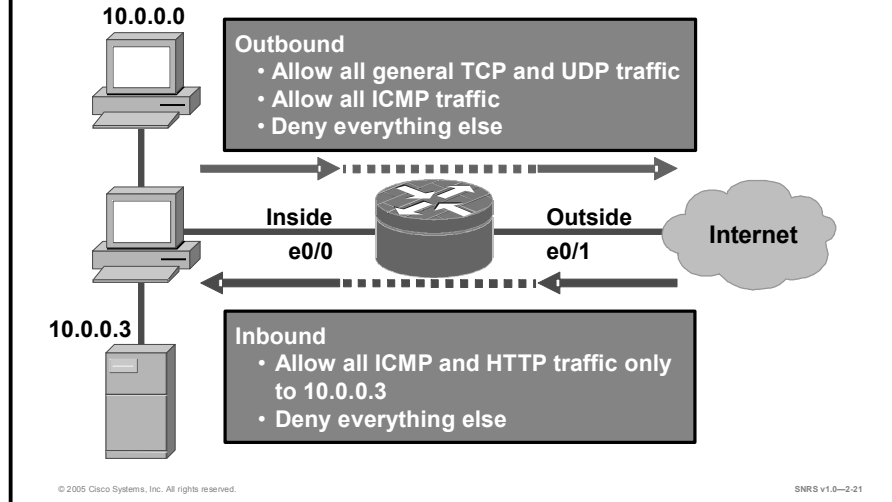
SNRS v1.0—2-20

For the Cisco IOS Firewall to be effective, both inspection rules and ACLs must be strategically applied to all the router interfaces. The following is the general rule of thumb for applying inspection rules and ACLs on the router:

- On the interface where traffic initiates, do the following:
 - Apply the ACL on the inward direction that permits only 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

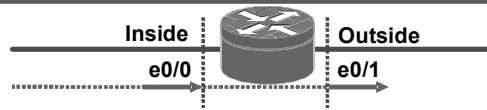
Cisco.com



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. Traffic from 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

Cisco.com



```
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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.22

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:

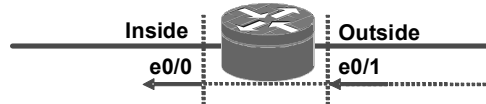
```
Router(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255
any
Router(config)# access-list 101 deny ip any any
```

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
```

Inbound Traffic

Cisco.com



```
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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.23

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:

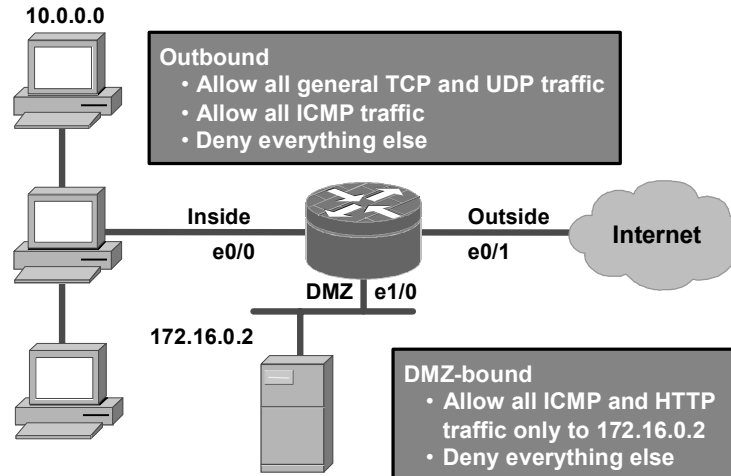
```
Router(config)# access-list 102 permit icmp any host 10.0.0.3
Router(config)# access-list 102 permit tcp any host 10.0.0.3
  eq www
Router(config)# access-list 102 deny ip any any
```

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



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2-24

As an example, configure the router to be a firewall among three networks: inside, outside, and Demilitarized Zone (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 is also allowed from the same network to the Internet and the DMZ host. Traffic from 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 DMZ host 172.16.0.2. Any other traffic not initiated from the inside must be denied.

Outbound Traffic

Cisco.com



```
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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.25

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:

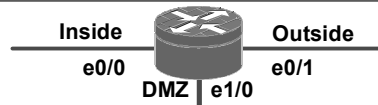
```
Router(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255
any
Router(config)# access-list 101 deny ip any any
```

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



```
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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2-26

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

Cisco.com



```
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 ACLs to the interface

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.27

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

Cisco.com

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
    
```

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0-2-28

The syntax for the **show ip inspect** command is as follows:

```
show ip inspect name inspection-name | config | interfaces | session
[detail] | all
```

<i>inspection-name</i>	Shows the configured inspection rule for the inspection name.
config	Shows the complete CBAC inspection configuration.
interfaces	Shows the 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

Cisco.com

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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.29

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.
<i>protocol</i>	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. It displays detailed information for all other enabled CBAC debugging.

Remove CBAC Configuration

Cisco.com

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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-30

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 the key points discussed in this lesson.

Summary

Cisco.com

- Turn on audit trail logging and real-time alerts to provide a record of network access through the firewall.
- 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.
- An unusually high number of half-opened sessions (either absolute or measured as the arrival rate) could indicate that a DoS attack is occurring.
- 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.
- PAM enables you to customize TCP or UDP port numbers for network services or applications.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.31

Summary (Cont.)

Cisco.com

- Network services or applications that use nonstandard ports require user-defined entries in the PAM table.
- Inspection rules must be defined to specify what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface.
- An inspection rule should specify each desired application-layer protocol, as well as generic TCP or generic UDP, if desired.
- Java inspection enables Java applet filtering at the firewall.
- RPC inspection enables the specification of various program numbers.
- SMTP inspection causes SMTP commands to be inspected for illegal commands.
- CBAC inspection rules can help protect hosts against certain DoS attacks involving fragmented IP packets.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.32

Lesson 3

Configuring Cisco IOS Firewall Authentication Proxy

Overview

This lesson describes the Cisco IOS Firewall authentication proxy feature. Authentication proxy provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks. You will learn how to configure a Cisco router to authenticate using authentication proxy.

Objectives

Upon completing this lesson, you will be able to configure Cisco IOS Firewall authentication proxy on a Cisco router. This ability includes being able to meet these objectives:

- Describe how system administrators can use Cisco IOS Firewall authentication proxy to allow specific security policies on a per-user basis for TACACS+ and RADIUS servers
- Describe how to provide authentication and authorization for the Cisco IOS Firewall authentication proxy using Cisco Secure ACS for Windows Server
- Describe the steps to be followed to configure the Cisco IOS Firewall to work with an AAA server
- Describe the steps to be followed to configure the authentication proxy settings on a Cisco router
- Describe how to use **show**, **debug**, and **clear** commands to test and verify CBAC configurations

Cisco IOS Firewall Authentication Proxy

This topic describes the features of the Cisco IOS Firewall authentication proxy.

What Is the Authentication Proxy?

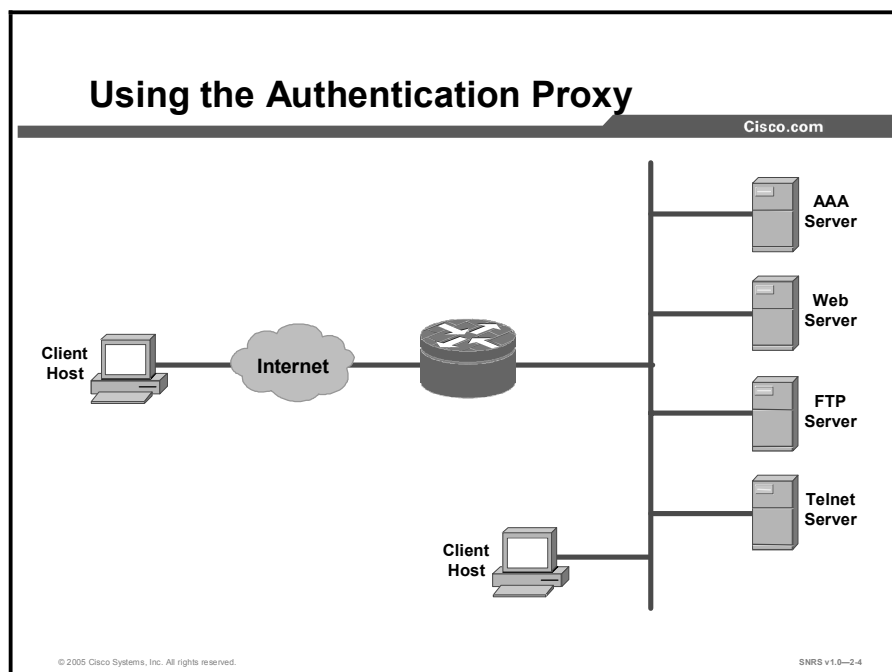
Cisco.com

- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.3

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 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.



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 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), 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 whether 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 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.

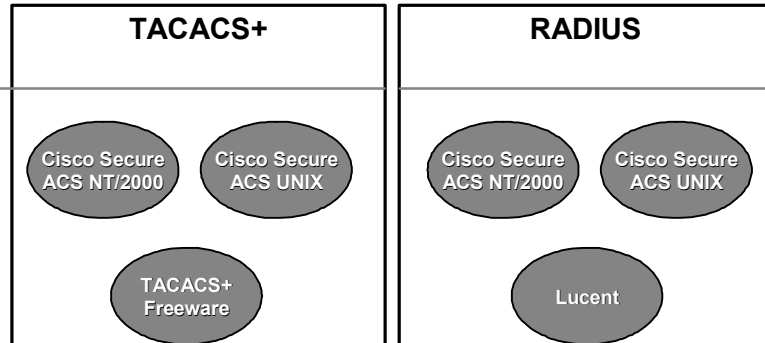
If the authentication fails, the authentication proxy reports the failure to the user and prompts the user for a configurable number of retries.

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 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 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



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.6

The Cisco IOS Firewall authentication proxy supports the following AAA protocols and servers:

■ TACACS+

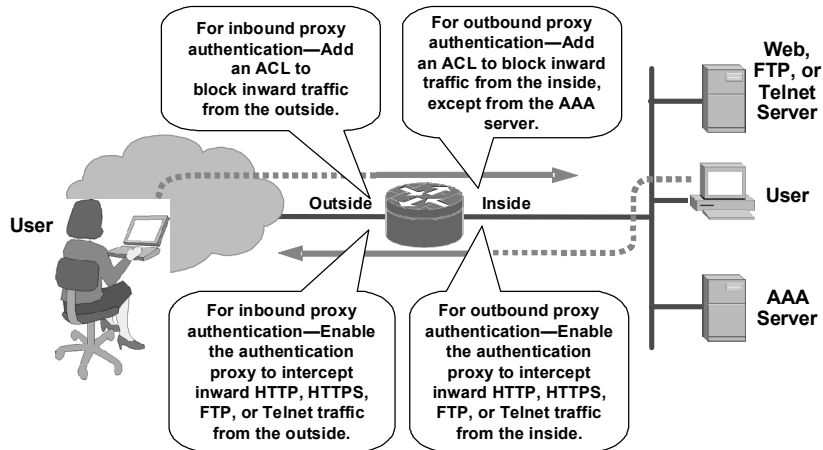
- Cisco Secure ACS for Windows 2000 Server
- Cisco Secure ACS for UNIX
- TACACS+ freeware

■ RADIUS

- Cisco Secure ACS for Windows 2000 Server
- Cisco Secure ACS for UNIX
- Lucent
- Other standard RADIUS servers

Authentication Proxy Configuration

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

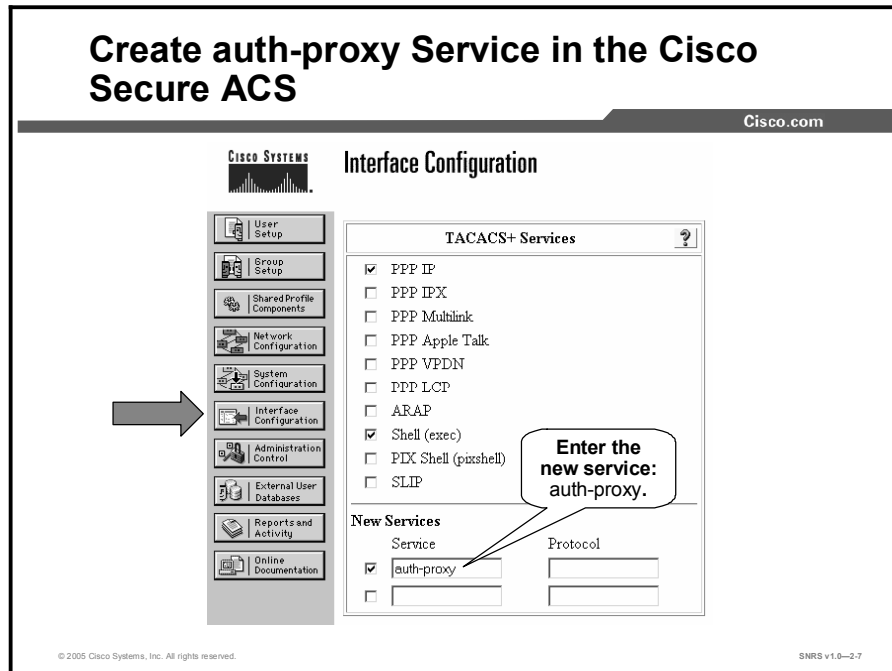
SNRS v1.0-2.6

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 the initial connection request from a user 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 authentication 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.



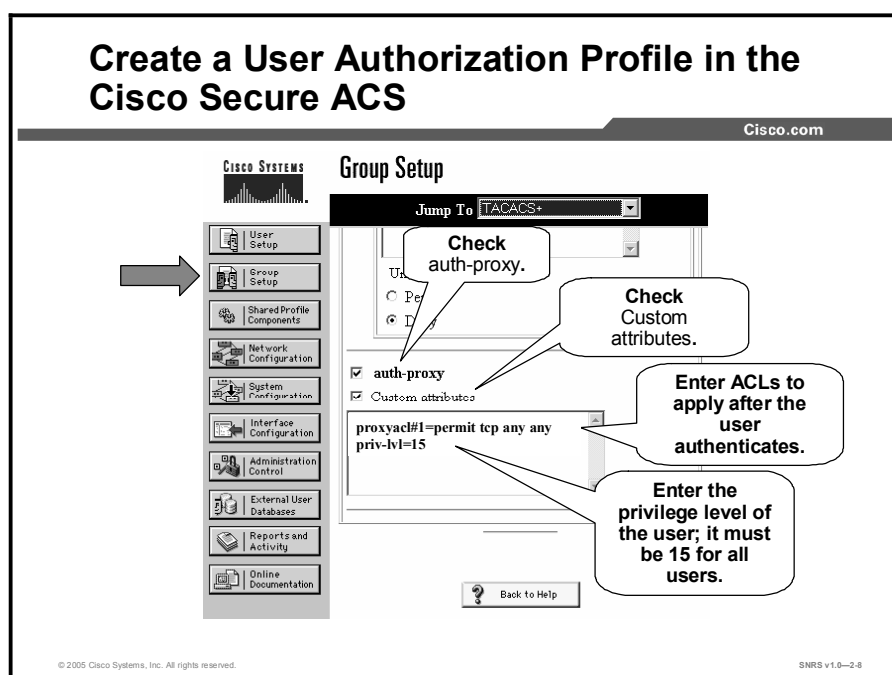
To support the authentication proxy, configure the AAA authorization auth-proxy service on the Cisco Secure ACS for Windows Server AAA server. This action creates a new section in the Group Setup window in which user profiles can be created. It does not interfere with other types of services that the 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 menu bar, click **Interface Configuration**. The Interface Configuration window opens.
- Step 2** Click **TACACS+ (Cisco IOS)**.
- Step 3** Scroll down in the TACACS+ Services window until you find the New Services group box.
- Step 4** Check 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 check it (as shown in the figure).

- Step 5** Enter **auth-proxy** in the first empty Service field next to the check box that you just checked 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 check the **Advanced TACACS+ Features** check box, if it is not already checked.
- Step 7** Click **Submit** when finished.

Create a User Authorization Profile in the Cisco Secure ACS



- Step 8** In the navigation bar, click **Group Setup**. The Group Setup window opens.
- Step 9** Choose your group from the drop-down menu and click **Edit Settings**.
- Step 10** Scroll down in the Group Setup window until you find the newly created auth-proxy service.
- Step 11** Check the **auth-proxy** check box.
- Step 12** Check 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 shown on the following page.
- Step 15** Click **Submit + Restart** when finished.

User Authorization Profiles

Cisco.com

```
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 443 (HTTPS)  
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.9

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 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]
```

<i>protocol</i>	Keyword indicating the protocol to allow users to access: <i>tcp</i> , <i>udp</i> , or <i>icmp</i> .
any	Indicates any hosts. The first any after the 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.
<i>ip_addr wildcard mask</i>	IP address and wildcard mask for a network that users can access.
eq auth_service	Specific service that users are allowed to access.

Use the **priv-lvl=15** command 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 AAA server and enable the authentication proxy feature.

Enable AAA

Cisco.com


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

- Enables the AAA functionality on the router (default = disabled)

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2.10

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

Cisco.com

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+
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-11

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

Cisco.com

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+
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.12

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

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2-13

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
```

<i>ip_addr</i>	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
```

<i>string</i>	Key used for authentication and encryption
---------------	--

Define a RADIUS Server and Its Key

Cisco.com

Router(config)#

```
radius-server host ip_addr
```

- Specifies the RADIUS server IP address

Router(config)#

```
radius-server key string
```

- Specifies the RADIUS server key

```
Router(config)# radius-server host 10.0.0.3
Router(config)# radius-server key secretkey
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.14

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
```

<i>ip_addr</i>	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
```

<i>string</i>	Key used for authentication and encryption
---------------	--

Allow AAA Traffic to the Router

Cisco.com

```
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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0–2-15

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 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 the 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 HTTP or HTTPS Server for AAA

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.16

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

Cisco.com


```
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
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2-17

To set the authentication proxy inactivity timeout value (the length of time that 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** command in earlier software 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 stop responding. 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 <i>min</i>	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 35,791. The default value is 60 minutes.
absolute-timer <i>min</i>	Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 35,791 minutes (45 and a half days). The default value is 0 minutes.

Define and Apply Authentication Proxy Rules

Cisco.com

```
Router(config)#
ip auth-proxy name auth-proxy-name {ftp | http
| telnet} [inactivity-time 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
Router(config)# interface ethernet0
Router(config-if)# ip auth-proxy aprule
```

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0-2.18

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 the auth-cache-time command in earlier 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 supports proxy authentication for multiple applications (HTTP, HTTPS, FTP, and Telnet) at the same time.

Authentication Proxy Rules with ACLs

Cisco.com

Router(config)#

```
ip auth-proxy name auth-proxy-name http list
{acl-num | acl-name}
```

- Creates an authorization proxy rule with an ACL

```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.19

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
```

<i>auth-proxy-name</i>	Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
list <i>acl-num acl-name</i>	(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.

Test and Verify

This topic discusses the procedures for testing and verifying the authentication proxy configuration.

show Commands

Cisco.com

Router#

```
show ip auth-proxy cache
show ip auth-proxy configuration
show ip auth-proxy statistics
show ip auth-proxy watch list
```

- **Displays statistics, configurations, and cache entries of authentication proxy subsystems**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-2-20

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

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-2.21

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

Cisco.com

Router#

```
clear ip auth-proxy cache { * | ip_addr }
```

- Clears authentication proxy entries from the router

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-22

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
<i>ip_addr</i>	Clears the authentication proxy entry, including user profiles and dynamic ACLs, for the specified IP address

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- The Cisco IOS Firewall authentication proxy feature enables network administrators to apply specific security policies on a per-user basis.
- With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, HTTPS, FTP, or Telnet.
- The authentication proxy is compatible with other Cisco IOS security features such as NAT, CBAC, IPSec, and Cisco VPN Client.
- The Cisco IOS Firewall authentication proxy supports TACACS+ and RADIUS AAA protocols.
- To support the authentication proxy, configure the AAA authorization auth-proxy service on the Cisco Secure ACS for Windows Server AAA server.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.23

Summary (Cont.)

Cisco.com

- Use the `aaa new-model global configuration` command to enable the AAA access control system.
- To set AAA authentication, use the `aaa authentication login global configuration` command.
- To set AAA authorization, use the `aaa authorization auth-proxy global configuration` command.
- To specify the IP address of a TACACS+ server, use the `tacacs-server host global configuration` command.
- To specify the IP address of a RADIUS server, use the `radius-server host global configuration` command.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-2.24

Summary (Cont.)

Cisco.com

- **All traffic requiring authentication and authorization should be denied by the router using extended ACLs.**
- **To create an authentication proxy rule, use the ip auth-proxy name global configuration command.**
- **To apply an authentication proxy rule at a firewall interface, use the ip auth-proxy interface configuration command.**
- **Use the show ip auth-proxy command to display the authentication proxy entries, the running authentication proxy configuration, or the authentication proxy statistics.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-25

Lesson 4

Configuring Cisco IOS Firewall Intrusion Prevention System

Overview

This lesson covers the Cisco IOS Firewall Intrusion Prevention System (IPS). Intrusion prevention systems provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS Firewall IPS technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity. You will learn how to configure a Cisco router for intrusion prevention, including enabling IPS, working with signatures, and monitoring with syslog or Security Device Event Exchange (SDEE).

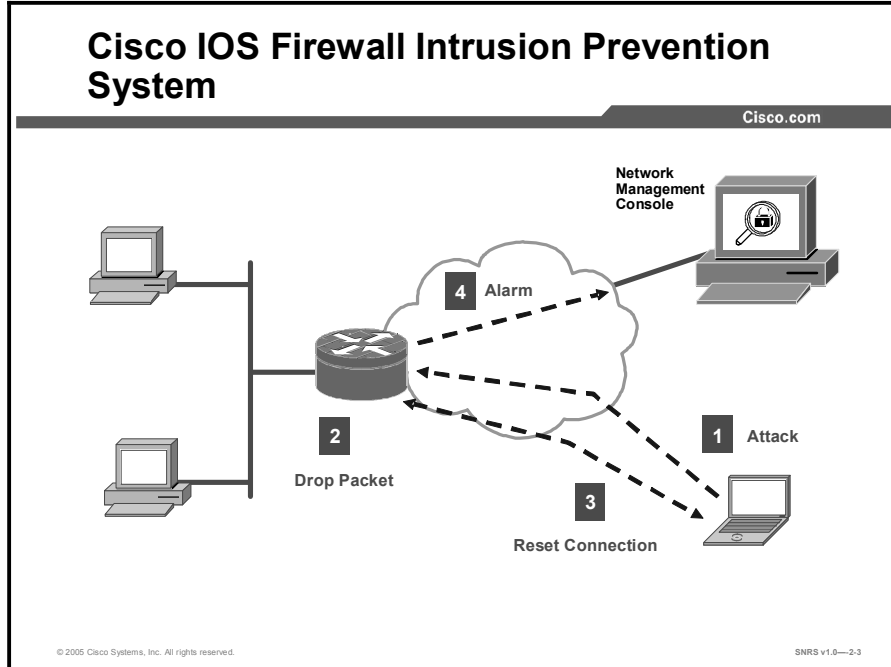
Objectives

Upon completing this lesson, you will be able to configure Cisco IOS Firewall IPS on a Cisco router. This ability includes being able to meet these objectives:

- Describe the features, functions, limitations, and applications of Cisco IOS Firewall IPS
- List the tasks involved in configuring Cisco IOS Firewall IPS on a router
- Describe the steps to be followed to install Cisco IOS Firewall IPS
- Describe the steps to be followed to configure logging and alerts
- Describe the steps to be followed to upgrade to the latest SDF
- Describe how to use **show**, **debug**, and **clear** commands to test and verify Cisco IOS Firewall IPS configurations

Cisco IOS Firewall Intrusion Prevention System

This topic introduces the Cisco IOS Firewall IPS feature for Cisco IOS routers.



Cisco IOS Firewall IPS, with inline intrusion capabilities, is the first in the industry to provide an inline, deep-packet-inspection-based IPS solution that helps enable Cisco routers to effectively mitigate a wide range of network attacks without compromising traffic-forwarding performance. Armed with the intelligence to accurately identify, classify, and stop malicious or damaging traffic in real time, Cisco IOS Firewall IPS is a core component of the Cisco Self-Defending Network, enabling the network to protect itself. This technology uses Cisco IPS Sensor software and signatures. Because Cisco IOS Firewall IPS is inline, it can drop traffic, send an alarm, or reset a connection, enabling the router to respond immediately to security threats.

Cisco IOS Firewall IPS capabilities include the ability to dynamically load and enable selected IPS signatures in real time, support for more than 740 signatures supported by Cisco IPS Sensor platforms, and the ability for a user to modify an existing signature or create a new signature to address newly discovered threats.

The Cisco IOS Firewall IPS acts as an inline intrusion prevention sensor, watching packets and sessions as they flow through the router, scanning each packet to match any of the Cisco IOS Firewall IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS Firewall IPS to choose the appropriate response to various threats.

When packets in a session match a signature, the Cisco IOS Firewall IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS Firewall IPS to support network security policies. However, each of these features can be enabled independently and on different router interfaces.

Features

Cisco.com

- **Uses the underlying routing infrastructure**
- **Ubiquitous protection of network assets**
- **Inline deep packet inspection**
- **IPS signature support**
- **Customized signature support**
- **Parallel signature scanning**
- **Named and numbered extended ACL support**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.4

Features and Benefits

- **Uses the underlying routing infrastructure**
 - This feature provides an additional layer of security with investment protection.
- **Ubiquitous protection of network assets**
 - Cisco IOS Firewall IPS is supported on a broad range of Cisco routers, enabling the user to protect network users and assets deep into the network architecture. The router is a security enforcer.
- **Inline deep packet inspection**
 - Cisco IOS Firewall IPS enables users to stop known network attacks. By alerting the router to an event, Cisco IOS Firewall IPS will intercept intrusion attempts to traverse the router. Cisco IOS Firewall IPS utilizes deep packet inspection to get into the payload of a packet and uncover the known malicious activity.
- **IPS signature support**
 - Cisco IOS Firewall IPS can now be enabled with any of the 700 or more IPS signatures supported by the Cisco IPS Sensors to mitigate known network attacks. As attacks are identified in the Internet, these signatures are updated and posted to Cisco.com so that they can be downloaded to the Cisco router.
- **Customized signature support**
 - Cisco IOS Firewall IPS can now customize existing signatures while also creating new ones. This Day One capability mitigates attacks that try to capitalize on slight deviations of known or newly discovered attacks.
- **Parallel signature scanning**
 - Cisco IOS Firewall IPS uses the Parallel Signature Scanning Engine to scan for multiple patterns within a Signature Micro-Engine (SME) at any given time. IPS signatures are no longer scanned on a serial basis.

- Named and numbered extended ACL support
 - In releases earlier than Cisco IOS Software Release 12.3(8)T, only standard, numbered ACLs were supported. Cisco IOS Firewall IPS now supports both named and numbered extended ACLs by using either the **ip ips ips-name list acl** command or the **ip ips signature signature-id list acl-list** command.

Origin of Cisco IOS Firewall IPS

Cisco IOS Firewall IPS restructures the existing Cisco IOS software-based intrusion detection system (IDS). The primary difference between Cisco IOS software-based IDS and the new, enhanced Cisco IOS Firewall IPS is that an intrusion detection system monitors traffic and sends an alert when suspicious patterns are detected, while an intrusion prevention system can drop traffic, send an alarm, or reset the connection, enabling the router to mitigate and protect against threats in real time. Cisco IOS Firewall IPS inherited the built-in 132 signatures from Cisco IOS software-based IDS technology; with the introduction of inline IPS capability, new signatures can be added by downloading a signature definition file (SDF) to the router flash memory, or users can specify the location of the SDF in the Cisco IOS Firewall IPS configuration on the router.

Signature Micro-Engines

Cisco IOS Firewall IPS uses SMEs to load the SDF and scan signatures.

Each engine categorizes a group of signatures, and each signature detects patterns of misuse in network traffic. For example, all HTTP signatures are grouped under the HTTP engine. Currently, Cisco IOS Firewall IPS supports more than 740 signatures. These signatures are part of the common set of signatures that Cisco IPS Sensors support, helping to ensure that all Cisco products use a common resource and are available for download from Cisco.com.

Signatures contained within the SDF are handled by a variety of SMEs. The SDF typically contains signature definitions for multiple engines. The SME typically corresponds to the protocol in which the signature occurs and looks for malicious activity in that protocol.

A packet is processed by several SMEs. Each SME scans for various conditions that can lead to a signature pattern match. When an SME scans the packets, it extracts certain values, searching for patterns within the packet via the regular expression engine.

Signatures

A signature detects patterns of misuse in network traffic. As of Cisco IOS Software Release 12.3(8)T, Cisco IOS Firewall IPS has 132 built-in signatures available in the Cisco IOS software image. The built-in signatures are hard-coded into the Cisco IOS software image for backward compatibility. Each signature can be set to send an alarm, drop the connection, or reset the connection. Each action is enabled on a per-signature basis. Each signature has an action assigned by default, based on the severity of the signature. “Alarm” sends a notification about the attack via syslog, post office, or SDEE protocol. “TCP reset” is effective for TCP-based connections and sends a reset to both the source and destination addresses. For example, in case of a half-open SYN attack, Cisco IOS Firewall IPS can reset the TCP connections. “Drop” discards the packet without sending a reset. By default, the 132 built-in signatures are set to alarm only.

Additionally, Cisco IOS Firewall IPS has the ability to download IPS signatures without the need for a Cisco IOS software image update. Typically, new signatures are released every two weeks, with emergency signature updates posted as needed. The signatures are posted to Cisco.com at: <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>.

The Nimda virus, for example, can be detected by loading and enabling the following signatures:

- **Signature ID:** 5081:0 WWW WinNT cmd.exe access
- **Signature ID:** 5114:2 WWW IIS Unicode attack
- **Signature ID:** 5326:0 root.exe access

The Signature Definition File

The SDF is integral to Cisco IOS Firewall IPS. The SDF is an Extensible Markup Language (XML) file with a definition of each signature along with relevant configurable actions. Cisco IOS Firewall IPS reads in the SDF, parses the XML, and populates its internal tables with the information necessary to detect each signature. The SDF contains the signature definition and configuration. Actions such as alarm, drop, or reset can be selected for individual signatures within the SDF. The SDF can be modified so that the router will detect only specific signatures; as a result, it can contain all or a subset of the signatures supported in Cisco IOS Firewall IPS. The user specifies the location of the SDF. The SDF can reside on the local flash file system (recommended) or on a remote server. Remote servers can be accessed via TFTP, FTP, Secure Copy Protocol (SCP), or Remote Copy Protocol (RCP).

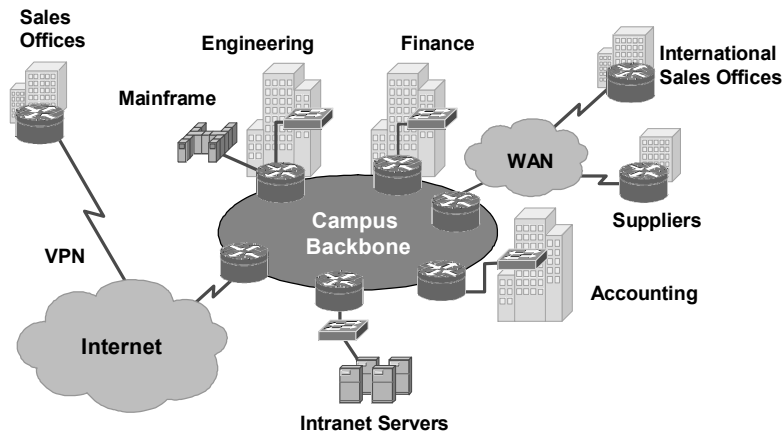
An SDF contains definitions for each signature it contains. The signatures are preset with actions to mitigate the attack by dropping the packet and resetting the connection, if applicable. After signatures are loaded and compiled onto a router running Cisco IOS Firewall IPS, IPS can begin detecting the new signatures immediately.

Attack-drop.sdf

The attack-drop.sdf file is available in flash on all Cisco access routers that are shipped with Cisco IOS Software Release 12.3(8)T or later. The attack-drop.sdf file can then be loaded directly from flash into the Cisco IOS Firewall IPS system. If flash is erased, the attack-drop.sdf file may also be erased. Thus, if you are copying a Cisco IOS image to flash and are prompted to erase the contents of flash before copying the new image, you might risk erasing the attack-drop.sdf file. If this occurs, the router will refer to the built-in signatures within the Cisco IOS image. The attack-drop.sdf file can also be downloaded onto your router from Cisco.com.

Cisco IOS Firewall IPS Network Visibility

Cisco.com



The Cisco IOS Firewall IPS 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. IPS signatures can be deployed alongside or independently of other Cisco IOS Firewall features. Existing Cisco IOS Firewall IPS customers can deploy the Cisco IOS software-based IPS signatures to complement their current protection. This enables intrusion prevention to be deployed to areas that may not be capable of supporting a Sensor.

The Cisco IOS Firewall IPS is intended to satisfy the security goals of all Cisco customers, and is particularly appropriate for these customers:

- 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 prevention capabilities
- Service provider customers who want to set up managed services, providing firewall and intrusion prevention to their customers, all housed within the necessary function of a router

Supported Router Platforms

Cisco.com

Go to Cisco.com to view the current listing of routers that support Cisco IOS Firewall IPS features.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.6

Always refer to the Cisco web site for up-to-date information regarding Cisco IOS Firewall IPS feature support.

Issues to Consider

Cisco.com

- **Memory use and performance impact**
 - Limited persistent storage
 - CPU-intensive
- **Updated signature coverage**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.7

The following are issues to consider when implementing Cisco IOS Firewall IPS:

- **Memory usage and performance impact:** The performance impact of intrusion prevention 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 IPS 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 Firewall IPS now identifies more than 700 of the most common attacks, using signatures to detect patterns of misuse in network traffic. These intrusion prevention signatures were chosen from a broad cross-section of intrusion prevention signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

Signature Implementations

Cisco.com

In Cisco IOS Firewall IPS, signatures are categorized into four types

- **Info**
 - Detects information-gathering activity
 - Port sweeps, etc.
- **Attack**
 - Detects attacks attempted into the protected network
 - DoS, etc.
- **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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.8

In Cisco IOS Firewall IPS, signatures are categorized into four types:

- Info atomic
- Info compound
- Attack atomic
- Attack compound

An info signature detects information-gathering activity, such as a port sweep.

An attack signature detects attacks attempted into the protected network, such as denial-of-service (DoS) attempts or the execution of illegal commands during an FTP session.

Info and attack signatures can be either atomic or compound signatures. Atomic signatures can detect patterns as simple as an attempt to access a specific port on a specific host. Compound signatures can detect complex patterns, such as a sequence of operations distributed across multiple hosts over an arbitrary period of time.

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 Cisco IOS Firewall IPS 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

Cisco.com

- **Alarm**
 - Sends alarms to the Cisco VMS, syslog server, or buffer
 - Forwards the packet
- **Reset:** Sends packets with a reset flag to both session participants if TCP forwards the packet
- **Drop:** Immediately drops the packet

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.9

The Cisco IOS Firewall IPS acts as an inline sensor, watching packets as they traverse the router interfaces and acting upon them in a definable fashion. When a packet matches a signature, or a number of packets in a session match a signature, the Cisco IOS Firewall IPS may perform the following configurable actions:

- **Alarm:** Sends alarms to a Cisco Virtual Private Network/Security Management Solution (VMS) Server, syslog server, or router buffer, 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.

Cisco IOS Firewall IPS Configuration Tasks

This topic describes tasks for configuring Cisco IOS Firewall IPS.

Configuration Tasks

Cisco.com

- **Install Cisco IOS Firewall IPS on the router.**
 - **Specify location of Signature Definition File (SDF)**
 - **Create an IPS rule**
 - **Attach a policy to a signature (optional)**
 - **Apply IPS rule at an interface**
- **Configure logging via syslog or SDEE.**
- **Verify the configuration.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—2-10

To configure the Cisco IOS Firewall IPS on a router and to have it report alarms to a syslog server or Cisco Router and Security Device Manager (SDM), install Cisco IOS Firewall IPS on the router.

To install Cisco IOS Firewall IPS, complete the following steps:

- Step 1** Specify the location of the SDF.
- Step 2** Create an IPS rule.
- Step 3** Attach a policy to a signature (optional).
- Step 4** Apply the IPS rule at an interface.
- Step 5** Configure logging via syslog or SDEE.
- Step 6** Verify the configuration. This includes using available **show**, **clear**, and **debug** commands for the Cisco IOS Firewall IPS.

Installing the Cisco IOS Firewall IPS

This topic describes the procedure to install the Cisco IOS Firewall IPS.

Specify Location of SDF

Cisco.com

Router (config)#

```
ip ips sdf location url
```

- **(Optional) Specifies the location in which the router will load the SDF attack-drop.sdf.**
- **If this command is not issued, the router will load the default, built-in signatures.**

```
Router(config)# ip ips sdf location  
disk2:attack-drop.sdf
```

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—2-11

Use the procedure given in this topic to install the latest Cisco IOS Firewall IPS signatures on a router for the first time.

This procedure allows you to load either the default, built-in signatures or the attack-drop.sdf file—but not both. If you want to merge the two signature files, you must load the default, built-in signatures as described in this topic. Then, you can merge the default signatures with the attack-drop.sdf file.

Create IPS Rule

Cisco.com

```
Router (config)#
```

```
ip ips name ips-name [list acl]
```

- **Creates an IPS rule**

```
Router(config)# ip ips name MYIPS
```

- **Creates an IPS rule named MYIPS that will be applied to an interface**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-12

Create a named IPS rule that you will apply to interface later.

Attach a Policy to a Given Signature (Optional)

Cisco.com

```
Router (config)#
```

```
ip ips signature signature-id [:sub-signature-id]  
{delete | disable | list acl-list}
```

- **Attaches a policy to a given signature**

```
Router(config)# ip ips signature 1000 disable
```

- **Disables signature 1000 in the SDF**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-13

Attach the policy to a given signature if you choose to.

Change to interface configuration mode at the interface on which you want to implement Cisco IOS Firewall IPS:

```
router(config)# interface FA0/1
```


Apply an IPS Rule at an Interface

Cisco.com

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

```
ip ips ips-name {in | out}
```

- Applies an IPS rule at an interface

```
Router(config-if)# ip ips MYIPS in
```

© 2005 Cisco Systems, Inc. All rights reserved.

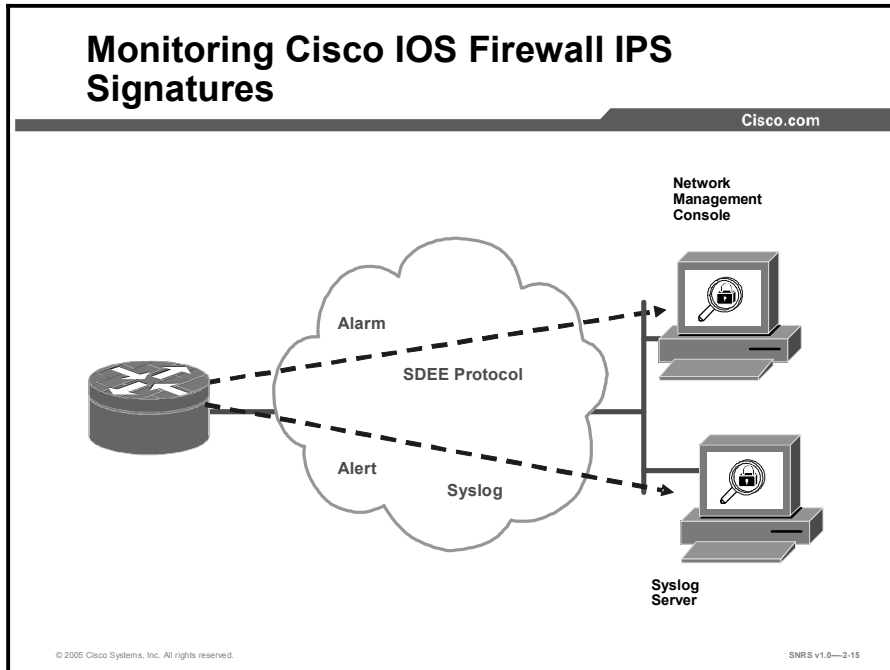
SNRS v1.0—2.14

The command shown in the figure applies an IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.

Note Whenever signatures are replaced or merged, the router prompt is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built. Depending on your platform and how many signatures are being loaded, building the engine can take up to several seconds. It is recommended that you enable logging messages to monitor the engine building status.

Configure Logging via Syslog or SDEE

This topic describes how to configure logging.



As of Cisco IOS Software Release 12.3(11)T, Cisco IOS Firewall IPS provides two methods to report IPS intrusion alerts—Cisco IOS logging (syslog) and Security Device Event Exchange (SDEE). Use the procedure described in this topic to enable SDEE to report IPS intrusion alerts.

Note Effective as of Cisco IOS Software Release 12.3(11)T, the Post Office Protocol (POP) is no longer supported.

Cisco IOS software now supports the SDEE protocol. SDEE is a new standard that specifies the format of messages and protocols used to communicate events generated by security devices. SDEE is flexible, so that all vendors can support address compatibility. This allows mixed IPS vendor environments to have one network management alert interface. TruSecure (International Computer Security Association [ICSA] Labs) is currently proposing SDEE as the unified industry protocol format for communicating with network management applications. SDEE uses a pull mechanism: Requests come from the network management application, and the IPS appliance or IPS router responds. SDEE utilizes HTTP and XML to provide a standardized interface. The Cisco IOS Firewall IPS router will still send IPS alerts via syslog.

SDEE and Syslog

Cisco.com

- Cisco IOS software now supports the Security Device Event Exchange (SDEE) protocol.
- SDEE uses a pull mechanism: Requests come from the network management application, and the IDS or IPS router responds.
- SDEE will become the standard format for all vendors to communicate events to a network management application.
- The use of HTTP over SSL or HTTPS ensures that data is secured as it traverses the network.
- The Cisco IOS Firewall IPS router will still send IPS alerts via syslog.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2-16

SDEE Overview

SDEE is an application-level communication protocol that is used to exchange IPS messages between IPS clients and IPS servers.

SDEE is always running, but it does not receive and process events from IPS unless SDEE notification is enabled. If it is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

Benefits

- Vendor interoperability
 - SDEE will become the standard format for all vendors to communicate events to a network management application. This lowers the cost of supporting proprietary vendor formats and potentially multiple network management platforms.
- Secured transport
 - The use of HTTP over Secure Socket Layer (SSL) or HTTPS ensures that data is secured as it traverses the network.

Storing SDEE Events in the Buffer

When SDEE notification is enabled (via the **ip ips notify sdee** command), 200 events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer starts overwriting the earliest stored events. (If overwritten events have not yet been reported, you receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer are lost.
- If a new, larger buffer is requested, all existing events are saved.

Set Notification Type

Cisco.com

Router (config)#

```
ip ips notify [log | sdee]
```

- Sets notification type

```
Router(config)# ip ips notify sdee
```

```
Router(config)# ip ips notify log
```

Router (config)#

```
ip sdee events num_of_events
```

- Sets the maximum number of SDEE events that can be stored in the event buffer

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.17

To use SDEE, the HTTP server must be enabled (via the **ip http server** command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the requests.

Note The **ip ips notify** command replaces the **ip audit notify** command. If the **ip audit notify** command is part of an existing configuration, the IPS will interpret it as the **ip ips notify** command.

To specify the method of event notification, use the **ip ips notify** command in global configuration mode. To disable event notification, use the **no** form of this command.

```
ip ips notify [log | sdee]
```

```
no ip ips notify [log | sdee]
```

log	(Optional) Send messages in syslog format. Note that if an option is not specified, alert messages are sent in syslog format.
sdee	(Optional) Send messages in SDEE format.

The default number of events is 100.

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Upgrading to the Latest Cisco IOS Firewall IPS Signature Definition File

This topic describes how to upgrade to latest SDF.

Upgrade to Latest SDF

Cisco.com

```
Router (config)#  
ip ips name ips-name
```

- **Creates an IPS rule**

```
Router (config)#  
no ip ips sdf builtin
```

- **Instructs the router not to load the built-in signatures**

```
Router (config)#  
ip ips fail closed
```

- **Instructs the router to drop all packets until the signature engine is built and ready to scan traffic**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—2-18

An important part of IPS is keeping up with the latest attack signatures. Use the information in this topic to replace the existing signatures in your router with the latest IPS signature file, `attack-drop.sdf`.

The latest SDF file can be found at <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>.

Note The latest IPS image will read and convert all commands that begin with the words “ip audit” to “ip ips.” For example, the **ip audit name** command will become the **ip ips name** command.

Although IPS will accept the **audit** keyword, it will generate the **ips** keyword when you show the configuration. Also, if you issue the help character (?), the command-line interface (CLI) will display the **ips** keyword instead of the **audit** keyword, and the Tab key used for command completion will not recognize the **audit** keyword.

Upgrade to Latest SDF (Cont.)

Cisco.com

Router (config-if)#

```
ip ips ips-name {in | out} [list acl]
```

- **Applies an IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.**

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 ips configuration

- **Verifies that Cisco IOS IPS is properly configured**

Router#

show ip ips signatures [detailed]

- **Verifies signature configuration, such as signatures that have been disabled**

Router#

show ip ips interface

- **Displays the interface configuration**

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0—2-20

To display IPS information such as configured sessions and signatures, use the **show ip ips** command in privileged EXEC mode.

The syntax for the **show ip ips** command is as follows:

```
show ip ips { [all] [configuration] [interfaces] [name name]
              [statistics [reset]] [sessions [details]] [signatures
              [details]] }
```

all	Displays all available IPS information.
configuration	Displays additional configuration information, including default values that may not be displayed using the show running-config command.
interfaces	Displays the interface configuration.
name name	Displays information only for the specified IPS rule.
statistics [reset]	Displays information such as the number of packets audited and the number of alarms sent. The optional reset keyword resets sample output to reflect the latest statistics.
sessions [details]	Displays IPS session-related information. The optional details keyword shows detailed session information.
signatures [details]	Displays signature information, such as which signatures are disabled and marked for deletion. The optional details keyword shows detailed signature information.

Use the **show ip ips 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 ips configuration** command is as follows:

```
show ip ips 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
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)
```

```
Audit Rule Configuration
```

```
Audit name AUDIT.1
    info actions alarm
```

Use the **show ip ips interface** command to display the interface configuration. The syntax for the **show ip ips interface** command is as follows:

```
show ip ips interface
```

An example output of the **show ip ips interface** command follows:

```
Interface Configuration
Interface Ethernet0
    Inbound IPS audit rule is AUDIT.1
        info actions alarm
    Outgoing IPS audit rule is not set
Interface Ethernet1
    Inbound IPS audit rule is AUDIT.1
        info actions alarm
    Outgoing IPS audit rule is AUDIT.1
        info actions alarm
```

clear Commands

Cisco.com

Router#

```
clear ip ips configuration
```

- **Removes all intrusion prevention configuration entries and releases dynamic resources**

Router#

```
clear ip ips statistics
```

- **Resets statistics on packets analyzed and alarms sent**

Router#

```
clear ip sdee {events | subscriptions}
```

- **Clears SDEE events or subscriptions**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.21

To disable Cisco IOS Firewall IPS, remove all intrusion prevention configuration entries, and release dynamic resources, use the **clear ip ips configuration** command in EXEC mode. The syntax for the **clear ip ips configuration** command is as follows:

```
clear ip ips configuration
```

Use the **clear ip ips statistics** command to reset statistics on packets analyzed and alarms sent. The syntax for the **clear ip ips statistics** command is as follows:

```
clear ip ips statistics
```

To clear SDEE events or subscriptions, use the **clear ip sdee** command in EXEC configuration mode. The syntax for the **clear ip sdee** command is as follows:

```
clear ip sdee {events | subscriptions}
```

events	Clears SDEE events from the event buffer
subscriptions	Clears SDEE subscriptions

debug Commands

Cisco.com

```
Router# debug ip ips timers
Router# debug ip ips object-creation
Router# debug ip ips object-deletion
Router# debug ip ips function trace
Router# debug ip ips detailed
Router# debug ip ips ftp-cmd
Router# debug ip ips ftp-token
Router# debug ip ips icmp
Router# debug ip ips ip
Router# debug ip ips rpc
Router# debug ip ips smtp
Router# debug ip ips tcp
Router# debug ip ips tftp
Router# debug ip ips udp
```

- **Instead of no, undebug command may be used.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—2.22

A plethora of debug commands are available to troubleshoot and test the Cisco IOS Firewall IPS configurations. Use the **no** form of the commands to disable debugging of a given option. The following is the list of available debug commands:

- **debug ip ips timers**
- **debug ip ips object-creation**
- **debug ip ips object-deletion**
- **debug ip ips function trace**
- **debug ip ips detailed**
- **debug ip ips ftp-cmd**
- **debug ip ips ftp-token**
- **debug ip ips icmp**
- **debug ip ips ip**
- **debug ip ips rpc**
- **debug ip ips smtp**
- **debug ip ips tcp**
- **debug ip ips tftp**
- **debug ip ips udp**

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The Cisco IOS Firewall IPS acts as an inline intrusion prevention sensor.**
- **When packets in a session match a signature, the Cisco IOS Firewall IPS can take any of the following actions: send an alarm, drop the packet, or reset the connection.**
- **The new Cisco IOS Firewall IPS capability enables the user to load and enable any of the 700 or more IPS signatures that are supported by the Cisco IDS Sensor.**
- **As of Cisco IOS Software Release 12.3(11)T, Cisco IOS Firewall IPS provides two methods to report IPS intrusion alerts—Cisco IOS logging (syslog) and SDEE.**
- **SDEE is a new standard that specifies the format of messages and protocol used to communicate events generated by security devices.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0—2-23

Summary (Cont.)

Cisco.com

- **An SDF file contains definitions for each signature it contains.**
- **In Cisco IOS Firewall IPS, signatures are categorized into four types: Info Atomic, Info Compound, Attack Atomic, and Attack Compound.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0—2-24

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **The Cisco IOS Firewall features include CBAC, authentication proxy, and IPS.**
- **CBAC uses dynamically created ACLs to control access to the network. It provides protection from DOS, RPC, Java, SMTP, and many other types of attacks based application-layer protocol session information.**
- **The Cisco IOS Firewall authentication proxy feature enables network administrators to apply specific security policies on a per-user basis as users log on to the network or Internet using HTTP, FTP, Telnet, and HTTPS. This feature uses the auth-proxy service provided by ACS along with ACLs used to define traffic requiring authentication and authorization.**
- **The Cisco IOS Firewall IPS acts as an inline intrusion detection sensor sending alarms, dropping packets, or resetting the connection in response to events triggered by the IPS. More than 700 signatures are available with the latest release. Syslog or SDEE are used to monitor and send alerts.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0--2.1

This module covered the Cisco IOS security features and their configuration. Cisco IOS software has an extensive feature set tailored to the security issues facing networks today. This feature set includes CBAC, authentication proxy, and IPS. CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information as well as certain application-layer protocols. The Cisco IOS Firewall authentication proxy feature enables network administrators to apply specific security policies on a per-user basis. The Cisco IOS Firewall IPS identifies 700 or more common attacks using signatures to detect patterns of misuse in network traffic.

Module 3

Layer 2 Security

Overview

Layer 2 security is now available as a tool to use against the attacks faced by the networks of today. In this module, you will identify types of Layer 2 attacks, examine and configure Cisco Identity-Based Networking Services (IBNS), examine 802.1x port-based authentication, and troubleshoot Layer 2 security features.

Module Objectives

Upon completing this module, you will be able to install, configure, operate, and troubleshoot Layer 2 security features on a lab network using Cisco IOS and Catalyst operating system commands. This ability includes being able to meet these objectives:

- Identify mitigation techniques against network Layer 2 attacks
- Configure Cisco IBNS to enhance Layer 2 security
- Configure IEEE 802.1x port-based authentication
- Recommend appropriate mitigation techniques for Layer 2 attacks

Lesson 1

Mitigating Layer 2 Attacks

Overview

Like routers, both Layer 2 and Layer 3 switches have their own sets of network security requirements. Unlike routers, however, there is not much public information available that discusses the network security risks in switches and what can be done to mitigate those risks. This lesson covers Layer 2 attacks and how to use Cisco IOS software and Cisco Catalyst operating system software features to mitigate such threats to the network. You will be introduced to several types of Layer 2 attacks and will learn strategies to mitigate these attacks.

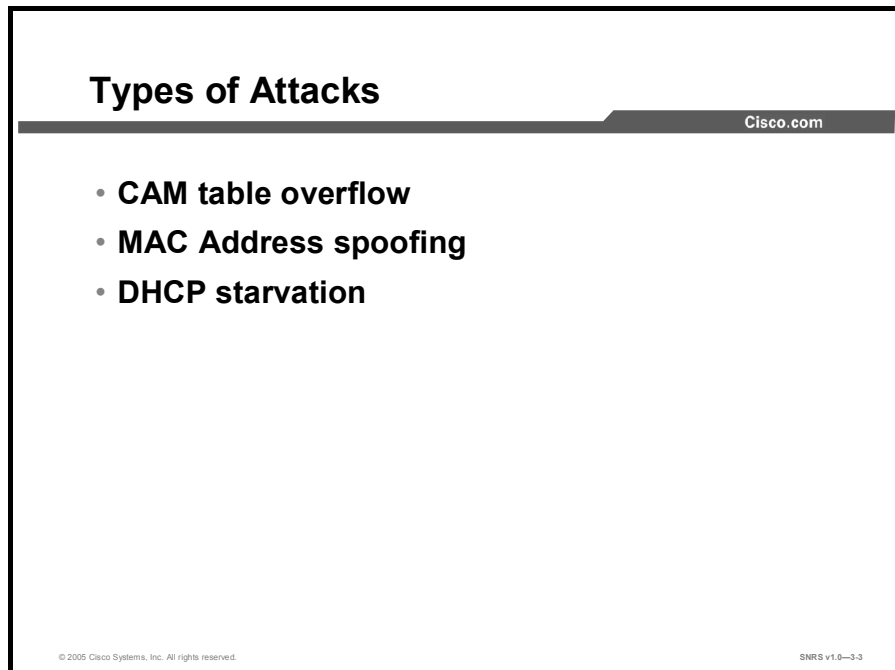
Objectives

Upon completing this lesson, you will be able to mitigate network Layer 2 attacks including CAM table overflow, MAC address spoofing, and DHCP starvation using Cisco IOS and Catalyst operating system features. This ability includes being able to meet these objectives:

- List the types of Layer 2 network attacks that can be mitigated using Cisco IOS and Catalyst operating system commands
- Describe how CAM table overflow is used in a network attack
- Explain how to prevent CAM table overflow
- Describe MAC spoofing attacks
- Explain how to prevent MAC spoofing
- Explain how to use DHCP snooping
- Describe how an attacker can broadcast DHCP requests
- Describe how to mitigate DHCP starvation attacks

Types of Attacks

This topic describes types of Layer 2 attacks.



The screenshot shows a presentation slide with the following content:

- **CAM table overflow**
- **MAC Address spoofing**
- **DHCP starvation**

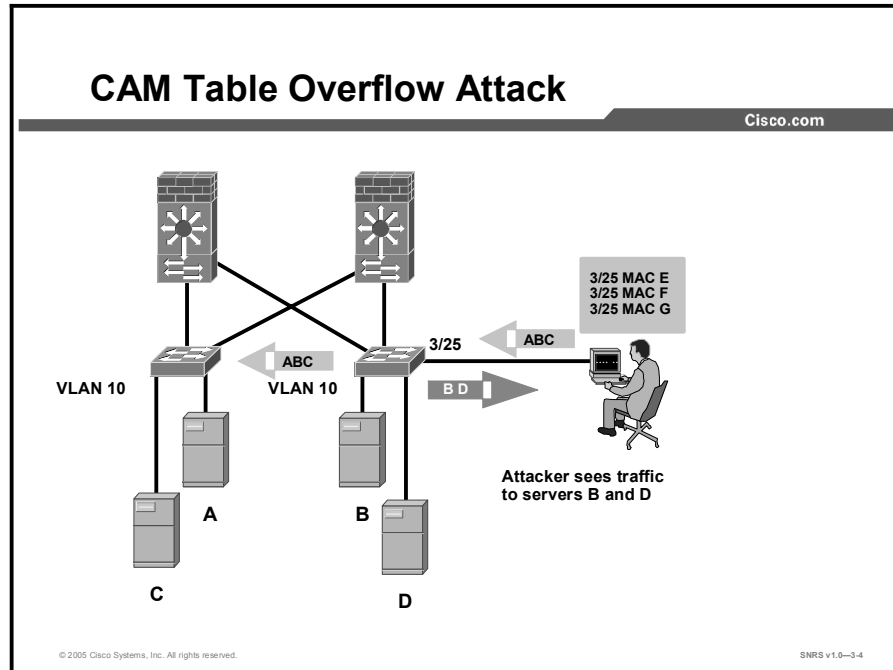
At the bottom of the slide, there is a copyright notice: © 2005 Cisco Systems, Inc. All rights reserved. and a reference code: SNRS v1.0-3.3.

Like routers, both Layer 2 and Layer 3 switches have their own sets of network security requirements. But not as much public information is available about the network security risks in switches and what can be done to mitigate those risks. Switches are susceptible to many of the same Layer 3 attacks as routers. Most of the network-security techniques detailed in the section of the SAFE Enterprise white paper titled “Routers Are Targets” also apply to switches. However, switches, and Layer 2 of the Open Systems Interconnection (OSI) reference model in general, are subject to network attacks in unique ways. These include the following:

- Content-Addressable Memory (CAM) table overflow
- MAC Address spoofing
- Dynamic Host Configuration Protocol (DHCP) starvation

CAM Table Overflow Attack

This topic describes the CAM table overflow attack.



In the figure, the machine of the attacker resides on VLAN 10. The attacker floods MAC addresses to port 3/25 on the switch. When the CAM table threshold is reached, the switch operates as a hub and simply floods traffic out all ports. This flooding also occurs on adjacent switches configured with VLAN 10; however, flooding is limited to the source VLAN and does not affect other VLANs.

MAC Flooding

MAC flooding is the attempt to exploit the fixed hardware limitations of the switch CAM table. The Cisco Catalyst switch CAM table stores the source MAC address and the associated port of each device connected to the switch. The CAM table on the Cisco Catalyst 6000 Series can contain 128,000 entries. These 128,000 entries are organized as eight pages that can store approximately 16,000 entries. A 17-bit hash algorithm is used to place each entry in the CAM table. If the hash results in the same value, each entry is stored on separate pages. Once these eight locations are full, the traffic is flooded out all ports on the same VLAN on which the source traffic is being received.

CAM tables are limited in size. If enough entries are entered into the CAM table before other entries have expired, the CAM table fills up to the point that no new entries can be accepted. Typically, a network intruder floods the switch with a large number of invalid-source MAC addresses until the CAM table fills up. When that occurs, the switch floods all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. The switch, in essence, acts like a hub. If the intruder does not maintain the flood of invalid-source MAC addresses, the older MAC address entries eventually time out of the CAM table, and the switch begins to act like a switch again. A CAM table overflow floods traffic only within the local VLAN, so the intruder will see only traffic within the local VLAN to which he or she is connected.

In May of 1999 the tool macof was released. It was written in approximately 100 lines of Perl code and was later ported to C code and incorporated into the dsniff package. This tool floods a switch with packets containing randomly generated source and destination MAC and IP addresses. When the switch CAM table fills up with these addresses, the switch begins to forward all frames it receives to every port. The previous figure illustrates a CAM table overflow attack. In this figure, the attacker is sending out multiple packets with various source MAC addresses. Over a short period, the CAM table in the switch fills up until it cannot accept new entries. As long as macof is left running, the CAM table on the switch will remain full. When this happens, the switch begins to broadcast all packets that it receives out of every port, so that packets sent from server B to server D are also broadcast out of port 3/25 on the switch the attacker is attached to.

Mitigating the CAM Table Overflow Attack

This topic describes steps to mitigate the CAM table overflow attack.

Mitigating the CAM Table Overflow Attack

Cisco.com

```
switch(config-if) #  
switchport port-security
```

- **Enables port security on interface**

```
switch(config-if) #  
switchport port-security [mac_addr]
```

- **Enables port security and set specific MAC address (H.H.H)**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0--3-5

The CAM table overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port.

Specifying MAC addresses on switch ports is far too unmanageable a solution for a production environment. Limiting the number of MAC addresses on a switch port is manageable. A more administratively scalable solution would be the implementation of dynamic port security at the switch. To implement dynamic port security, specify a maximum number of MAC addresses that will be learned, as shown in the second example in the next topic.

Mitigating the CAM Table Overflow Attack (Cont.)

Cisco.com

```
switch(config-if)#  
switchport port-security maximum (1-132)
```

- Sets maximum number of MAC addresses

```
switch(config-if)#  
switchport port-security violation shutdown [protect |  
restrict | shutdown]
```

- Sets action on violation

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3.6

Port Security

Port security allows you to specify MAC addresses for each port or to permit a limited number of MAC addresses. When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port either shuts down permanently (the default mode), shuts down for the time you have specified, or drops incoming packets from the insecure host. The behavior of the port depends on how you configure it to respond to a security violator.

It is recommended that you configure the port security feature to issue a shutdown instead of dropping packets from insecure hosts through the restrict option. The restrict option may fail under the load of an attack, and then the port is disabled anyway.

To restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port, complete these steps:

- Step 1** Enter interface configuration mode, and enter the physical interface to configure.

```
Router(config)# interface interface_id
```

- Step 2** Set the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.

```
Router(config-if)# switchport mode access
```

- Step 3** Enable port security on the interface.

```
Router(config-if)# switchport port-security
```

- Step 4** (Optional) Set the maximum number of secure MAC addresses for the interface. The range is 1 to 128; the default is 128.

```
Router(config-if)# switchport port-security maximum value
```

Step 5 (Optional) Set the violation mode and the action to be taken when a security violation is detected.

```
Router(config-if)# switchport port-security violation {protect  
| restrict | shutdown}
```

Step 6 (Optional) Enter a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.

```
Router(config-if)# switchport port-security mac-address  
mac_address
```

Step 7 Return to privileged EXEC mode.

```
Router(config-if)# end
```

There are two ways to check your configuration:

■ Router# **show port-security interface** *interface_id*

Note This command displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.

■ Router# **show port-security address**

Note This command displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.

The following is an example of the **show port-security** command when you do not enter an interface:

```
sw-class#sh port-security
```

```
Secure Port   MaxSecureAddr   CurrentAddr   SecurityViolation   Security Action  
                (Count)         (Count)         (Count)
```

```
-----  
Fa0/12                1             0             0             Shutdown  
-----
```

```
Total Addresses in System (excluding one mac per port) : 0
```

```
Max Addresses limit in System (excluding one mac per port) : 1024
```

This example displays output from the **show port-security** command for a specified interface:

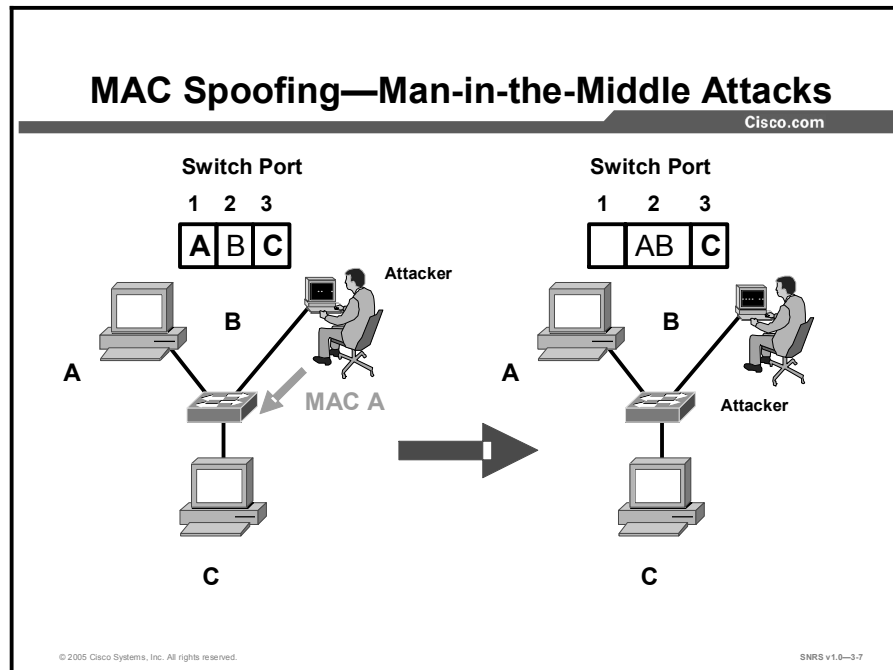
```
sw-class#sh port-security interface fa0/12
Port Security           : Enabled
Port Status            : Secure-down
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address    : 0000.0000.0000
Security Violation Count : 0
```

This example displays output from the **show port-security address** privileged EXEC command:

```
sw-class#sh port-security address
          Secure Mac Address Table
-----
Vlan      Mac Address      Type                Ports    Remaining Age
          (mins)
-----
1         0000.ffff.aaaa    SecureConfigured    Fa0/12   -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```


MAC Spoofing—Man-in-the-Middle Attacks

This topic describes MAC spoofing, one type of man-in-the-middle attack.



MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. By sending a single frame with the source Ethernet address of the other host, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic, it will not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.

The diagram shows how MAC spoofing works. In the beginning, the switch learns that host A is on port 1, host B is on port 2, and host C is on port 3. Host B sends out a packet identifying itself as the host B IP address, but with the host A MAC address or another packet with the same IP address and MAC address combination. This traffic causes the switch to move the location of host A in its CAM table from port 1 to port 2. Traffic from host C destined for host A is now visible to host B.

Mitigating MAC Spoofing Attacks

This topic describes how to mitigate MAC spoofing attacks.

Mitigating MAC Spoofing Attacks—Cisco IOS Software

Cisco.com

```
switch(config-if)#  
port security max-mac-count {1-132}
```

- **Enables port security and sets maximum MAC address**

```
switch(config-if)#  
port security action {shutdown|trap}
```

- **Specifies action to take when violation occurs**

```
switch(config-if)#  
arp timeout seconds
```

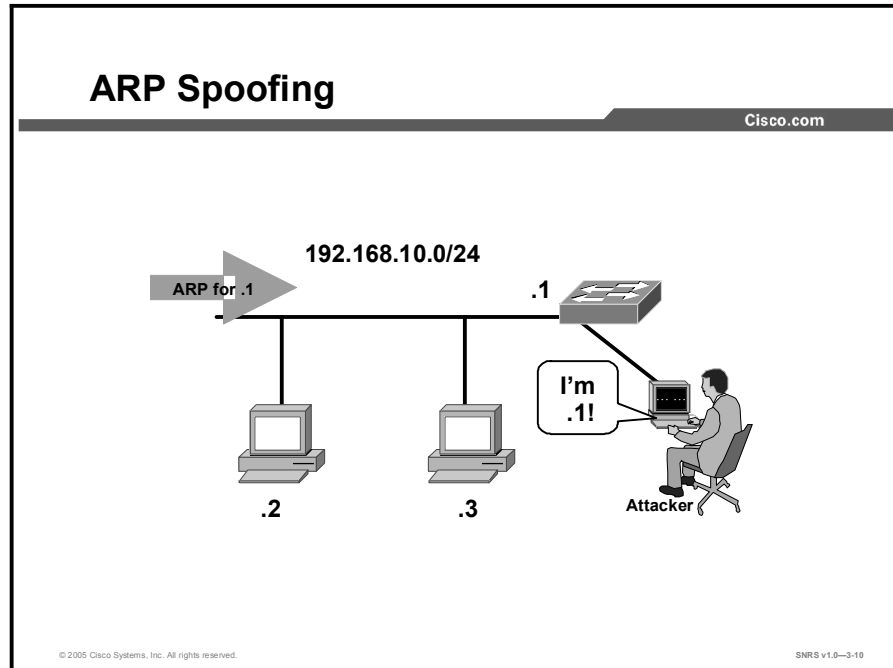
- **Specifies ARP timeout**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-3.9

Use the **port security** commands to mitigate MAC spoofing attacks. The **port security** command provides the ability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate Address Resolution Protocol (ARP) spoofing attacks by setting the length of time that an entry will stay in the ARP cache. However, hold-down timers by themselves are insufficient. Modification of the ARP cache expiration time on all end systems would be required, as well as static ARP entries. Even in a small network, this approach does not scale well. One solution would be to use private VLANs to help mitigate these network attacks.

Using DHCP Snooping

This topic describes ARP spoofing and the use of DHCP Snooping.



Address Resolution Protocol Spoofing

ARP is used to map IP addressing to MAC addresses in a LAN segment where hosts of the same subnet reside. Normally, a host sends out a broadcast ARP request to find the MAC address of another host with a particular IP address, and an ARP response comes from the host whose address matches the request. The requesting host then caches this ARP response. Within the ARP protocol, another provision is made for hosts to perform unsolicited ARP replies. The unsolicited ARP replies are called gratuitous ARP (GARP). GARP can be exploited maliciously by an attacker to spoof the identity of an IP address on a LAN segment. Typically, this technique is used to spoof the identity between two hosts or all traffic to and from a default gateway in a man-in-the-middle attack.

By crafting an ARP reply, a network attacker can make his or her system appear to be the destination host sought by the sender. The ARP reply causes the sender to store the MAC address of the network attacker system in the ARP cache. This MAC address is also stored by the switch in its CAM table. In this way, the network attacker has inserted the MAC address of his or her system into both the switch CAM table and the ARP cache of the sender. This allows the network attacker to intercept frames destined for the host that he or she is spoofing.

Solution

A solution that can be used to mitigate various ARP-based network exploits is the use of DHCP snooping along with Dynamic ARP Inspection (DAI). These Cisco Catalyst switch features validate ARP packets in a network and permit the interception, logging, and discarding of ARP packets with invalid MAC address to IP address bindings.

Mitigating ARP Spoofing with DHCP Snooping and DAI

Cisco.com

```
switch(config)#
```

```
ip dhcp snooping
```

- **Enables DHCP snooping**

```
switch(config)#
```

```
ip dhcp snooping vlan vlan_id {,vlan_id}
```

- **Enables DHCP snooping for specific VLANs**

```
switch(config-if)#
```

```
ip dhcp snooping trust
```

- **Configures an interface as trusted for DHCP snooping purposes**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3-11

DHCP snooping provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table. DHCP snooping considers DHCP messages originating from any user-facing port that is not a DHCP server port or an uplink to a DHCP server as untrusted. From a DHCP snooping perspective, these untrusted user-facing ports should not send DHCP server type responses such as DHCP OFFER, DHCP ACK, or DHCP NAK. Untrusted DHCP messages are messages received from outside the network or firewall. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. The DHCP snooping binding table can contain both dynamic as well as static MAC address-to-IP address bindings.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

DHCP Snooping Configuration Guidelines

These are the configuration guidelines for DHCP snooping:

- You must globally enable DHCP snooping on the switch.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- Before configuring the DHCP information option on your switch, make sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude or configure DHCP options for devices.

Mitigating ARP Spoofing with DHCP Snooping and DAI (Cont.)

Cisco.com

```
switch(config-if)#
```

```
ip dhcp snooping limit rate rate
```

- **Sets rate limit for DHCP snooping**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3-12

DAI determines the validity of an ARP packet based on the valid MAC address-to-IP address bindings stored in a DHCP snooping database. Additionally, DAI can validate ARP packets based on user-configurable access control lists (ACLs). This allows for the inspection of ARP packets for hosts using statically configured IP addresses. DAI allows for the use of per-port and VLAN access control lists (VACLs) to limit ARP packets for specific IP addresses to specific MAC addresses.

The following are the steps to mitigate ARP spoofing using DAI:

- Step 1** Enable DHCP snooping globally.

```
switch(config)#ip dhcp snooping
```

- Step 2** Enable DHCP snooping on a VLAN or range of VLANs. You can specify a single VLAN identified by VLAN ID number or specify start and end VLAN IDs to identify a range of VLANs. The range is 1 to 4094.

```
switch(config)#ip dhcp snooping vlan vlan_id {,vlan_id}
```

- Step 3** Enter interface configuration mode, and specify the interface to be configured.

```
switch(config)#interface interface-id
```

- Step 4** (Optional) Configure the interface as trusted or untrusted. You can use the **no** form of the command to configure an interface to receive messages from an untrusted client. The default is untrusted.

```
switch(config-if)#ip dhcp snooping trust
```

- Step 5** (Optional) Configure the number of DHCP packets per second than an interface can receive. The range is 1 to 4,294,967,294. The default is to have no rate limit configured.

```
switch(config-if)#ip dhcp snooping limit rate rate
```

Note An untrusted rate limit of not more than 100 packets per second is recommended. Normally, the rate limit applies to untrusted interfaces. If you configure rate limiting for trusted interfaces, you will need to adjust the rate limit to a higher value because trusted interfaces might aggregate DHCP traffic in the switch.

Step 6 Display the switch DHCP snooping configuration.

```
sw-class#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
201
Insertion of option 82 is enabled
Interface                Trusted      Rate limit (pps)
-----                -
FastEthernet0/12         yes         unlimited
```

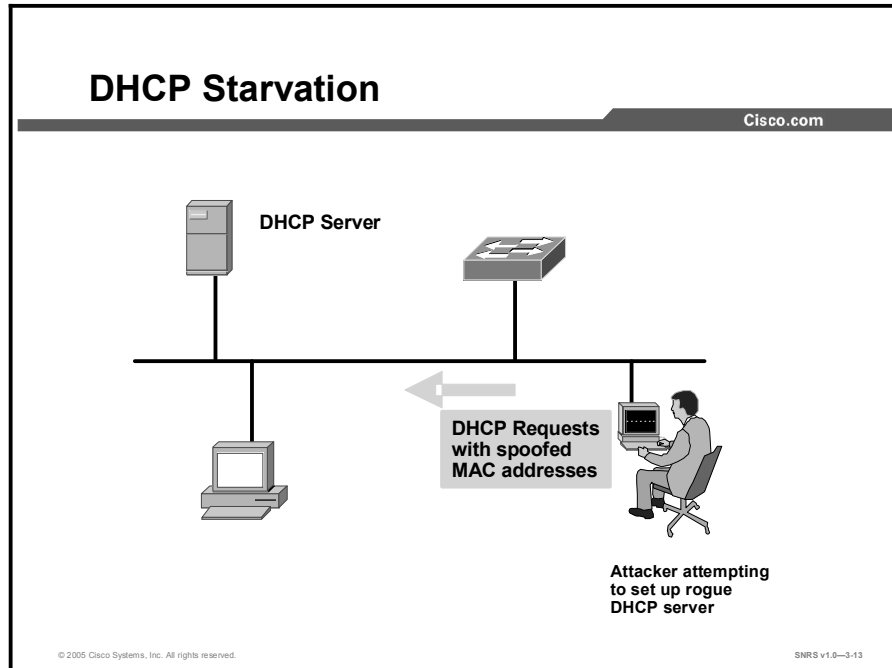
The DHCP snooping binding table for each switch has binding entries that correspond to untrusted ports. The table does not have information about hosts interconnected with a trusted port because each interconnected switch has its own DHCP snooping binding table.

This example shows how to display the DHCP snooping binding entries for a switch.

```
Switch# show ip dhcp snooping binding
MacAddress                IpAddress        Lease(sec)  Type           VLAN  Interface
-----                -
00:30:94:C2:EF:35        41.0.0.51        286         dynamic        41    FastEthernet0/3
00:D0:B7:1B:35:DE        41.0.0.52        237         dynamic        41    FastEthernet0/3
00:00:00:00:00:01        40.0.0.46        286         dynamic        40    FastEthernet0/9
00:00:00:00:00:03        42.0.0.33        286         dynamic        42    FastEthernet0/9
00:00:00:00:00:02        41.0.0.53        286         dynamic        41    FastEthernet0/9
```

DHCP Starvation Attacks

This topic describes DHCP starvation attacks.



A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is easily achieved with attack tools such as gobble. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack, just as a SYN flood is a starvation attack. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network. Exhausting all of the DHCP addresses is not required to introduce a rogue DHCP server, though. As stated in RFC 2131: “The client collects DHCPOFFER messages over a period of time, selects one DHCPOFFER message from the (possibly many) incoming DHCPOFFER messages (for example, the first DHCPOFFER message or the DHCPOFFER message from the previously used server) and extracts the server address from the ‘server identifier’ option in the DHCPOFFER message. The time over which the client collects messages and the mechanism used to select one DHCPOFFER are implementation dependent.”

By placing a rogue DHCP server on the network, a network attacker can provide clients with addresses and other network information. Because DHCP responses typically include default gateway and Domain Name System (DNS) server information, the network attacker can supply his or her own system as the default gateway and DNS server, resulting in a man-in-the-middle attack.

Mitigating DHCP Starvation Attacks

This topic describes the commands used to mitigate DHCP starvation attacks.

Commands to Mitigate DHCP Starvation Attacks

Cisco.com

```
switch(config)#  
ip dhcp snooping
```

- **Enables DHCP snooping**

```
switch(config)#  
ip dhcp snooping vlan vlan_id {,vlan_id}
```

- **Enables DHCP snooping for specific VLANs**

```
switch(config-if)#  
ip dhcp snooping trust
```

- **Sets interface to trusted state**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-3-14

The techniques that mitigate CAM table flooding also mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. As implementation of RFC 3118, “Authentication for DHCP Messages,” increases, DHCP starvation attacks will become more difficult.

Additional features in the Cisco Catalyst family of switches, such as the DHCP snooping command, can be used to help guard against a DHCP starvation attack. DHCP snooping is a security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table. The binding table contains information such as the MAC address, IP address, lease time, binding type, VLAN number, and the interface information corresponding to the local untrusted interfaces of a switch. Untrusted messages are those received from outside the network or firewall, and untrusted switch interfaces are those that are configured to receive such messages from outside the network or firewall.

The following shows commands to mitigate DHCP starvation attacks using DHCP snooping:

```
switch(config)#ip dhcp snooping  
switch(config)#ip dhcp snooping vlan vlan_id {,vlan_id}  
switch(config-if)#ip dhcp snooping trust  
switch(config-if)#ip dhcp snooping limit rate rate
```


Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Types of Layer 2 attacks include these:**
 - CAM table overflow
 - VLAN hopping
 - STP manipulation
 - MAC address spoofing
 - ARP spoofing
 - PVLAN
 - DHCP starvation
- **MAC flooding is the attempt to exploit the fixed hardware limitations of the switch CAM table.**
- **MAC spoofing attacks involve the use of a known MAC address of another host.**
- **Gratuitous ARP can be exploited maliciously by an attacker to spoof the identity of an IP address on a LAN segment.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-16

Summary (Cont.)

Cisco.com

- **A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses.**
- **Port security is a feature used to mitigate some Layer 2 attacks.**
- **Another solution that can be used to mitigate various ARP-based network exploits is the use of DHCP snooping along with DAI.**
- **DHCP snooping provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table.**
- **DAI determines the validity of an ARP packet based on the valid MAC address-to-IP address bindings stored in a DHCP snooping database.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-17

Lesson 2

Configuring Cisco Identity-Based Networking Services

Overview

Cisco Identity-Based Networking Services (IBNS) is an integrated solution combining several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco IBNS enables greater security while simultaneously offering cost-effective management of changes throughout the organization. This lesson introduces Cisco IBNS. You will be introduced to 802.1x and Extensible Authentication Protocol (EAP) as they relate to IBNS. You will then learn to configure the Cisco Secure Access Control Server (ACS) server to authenticate using EAP-Message Digest 5 (EAP-MD5) and RADIUS.

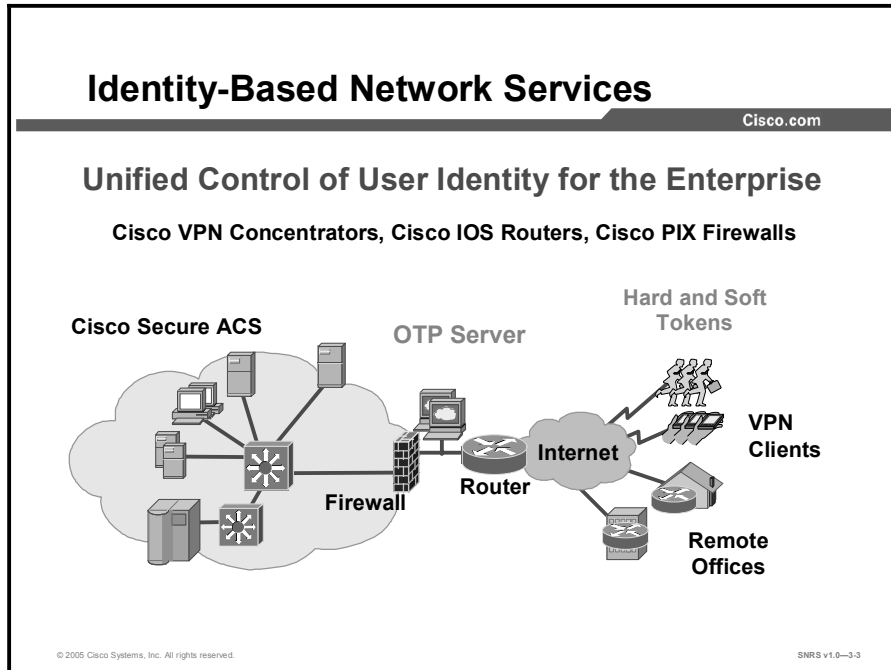
Objectives

Upon completing this lesson, you will be able to configure Cisco IBNS to enhance Layer 2 security. This ability includes being able to meet these objectives:

- Explain how Cisco IBNS improves the security of physical and logical access of LANs
- Describe how 802.1x provides port-based identity network access control
- Define the role of each 802.1x component
- Describe how 802.1x uses EAP
- Select the appropriate EAP type to meet a given set of network requirements
- Describe how Cisco Secure ACS provides RADIUS-based AAA

IBNS Overview

This topic describes Cisco IBNS.



By offering a secure IBNS framework for enterprises to manage user mobility and reduce the overhead costs associated with granting and managing access to network resources, Cisco provides enterprises with the ability to increase user productivity and reduce operating costs.

Features and Benefits

The Cisco IBNS solution provides the following benefits:

- **Intelligent adaptability for offering greater flexibility and mobility to stratified users:** Creating user or group profiles with policies that define trust relationships between users and network resources allows organizations to easily authenticate, authorize, and account for all users of wired or wireless networks. This architecture-secure flexibility is a primary enabler for the networked virtual organization (NVO).
- **A combination of authentication, access control, and user policies to secure network connectivity and resources:** Because policies are associated with users and not physical ports, users obtain more mobility and freedom, and IT administration is simplified. Greater scalability and ease of management is achieved through policy enforcement and dynamic provisioning.
- **User productivity gains and reduced operating costs:** Providing security and greater flexibility for wired or wireless network access provides enterprises with the ability to have cross-functional or new project teams form more quickly, enables secure access for trusted partners and vendors, and facilitates secure conference-room connectivity. Enabling flexibility with secure network access through centralized policy-based administration decreases the time, complexity, and effort associated with port security techniques at the MAC level.

Identity-Based Networking Services

Cisco.com

Features and benefits:

- **Intelligent adaptability for offering greater flexibility and mobility to stratified users**
- **A combination of authentication, access control, and user policies to secure network connectivity and resources**
- **User productivity gains and reduced operating costs**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—3-4

IBNS and 802.1x are supported on all Cisco Catalyst switches, including Cisco Catalyst 6500, 4500, 3550, and 2950 switches, Cisco ACS, and Cisco Aironet Access Points.

Cisco IBNS is a solution for increasing the security of physical and logical access to an enterprise network that is built on the IEEE 802.1x standard.

Cisco IBNS allows the network administrator to implement true identity-based network access control and policy enforcement at the user and port levels. It provides user and device identification using secure and reliable strong authentication technologies. This solution associates identified entities with policies. The policies are created and administered by management and provide increased granularity of control.

Prior to the development of 802.1x-based port security, Cisco offered and still offers capabilities such as port security and the Cisco User Registration Tool (URT). The port security feature still has applicability in certain environments. Port security enables network access management on a per-port basis and is manually configured on the switch. The Cisco URT provides dynamic VLAN segmentation of the LAN based on user- or device-based authentication. The Cisco URT uses the VLAN Membership Policy Server (VMPS) function on Cisco switches that currently use the proprietary VMPS Query Protocol (VQP). Cisco IBNS is a standards-based implementation of port security that is centrally managed by a RADIUS server (Cisco Secure ACS). Additionally, Cisco IBNS offers greater flexibility and mobility to users by combining access control and user profiles to secure network connectivity, services, and applications. This allows enterprises to increase user productivity and reduce operating costs.

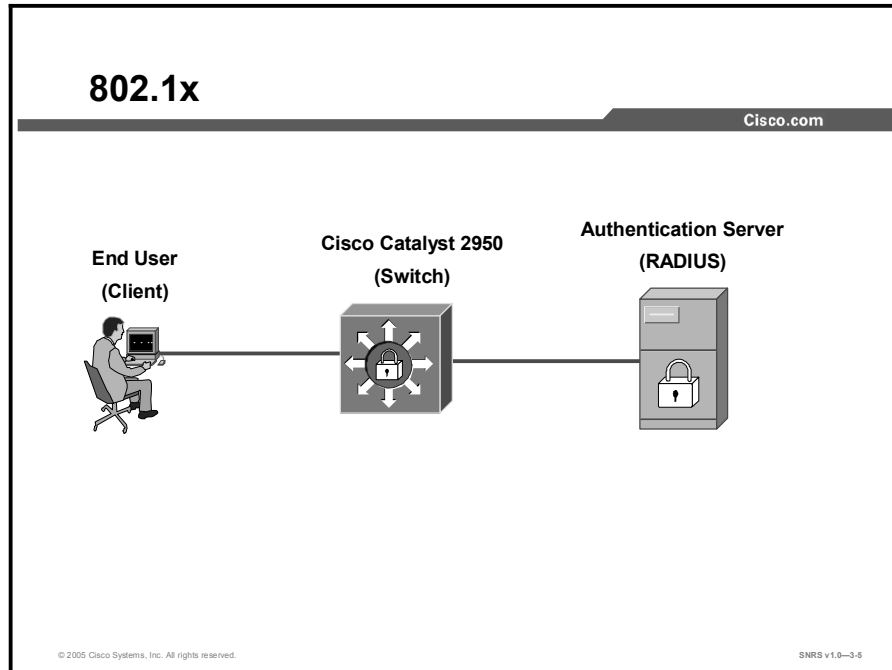
The Cisco IBNS solution will adapt to meet the changing requirements of the standards and of customers. This phase is an early one in a multiphase implementation.

Cisco Catalyst switches support Microsoft Windows XP, Linux, and HP UNIX, with additional 802.1x client support anticipated in the future. Cisco Aironet products support all current versions of Microsoft Windows, Windows CE, Mac OS, Linux, and MS-DOS.

The Cisco IBNS solution is based on standard RADIUS and 802.1x implementations. It interoperates with all Internet Engineering Task Force (IETF) authentication servers that comply with these two standards. Cisco has enhanced Cisco Secure ACS to provide a tight integration across all Cisco switches.

IEEE 802.1x

This topic describes the IEEE 802.1x standard.



IEEE 802.1x is a standardized framework defined by the IEEE, designed to provide port-based network access. The 802.1x standard authenticates network clients using information unique to the client and with credentials known only to the client. This service is called *port-level authentication* because, for security reasons, it is offered to a single endpoint for a given physical port. The 802.1x framework defines three roles in the authentication process:

- The endpoint that is seeking network access is known as the *supplicant*. The supplicant may be an end-user device or a standalone device, such as an IP phone.
- The device to which the supplicant directly connects and through which the supplicant obtains network access permission is known as the *authenticator*.
- The authenticator acts as a gateway to the *authentication server*, which is responsible for actually authenticating the supplicant.

The authentication process, which consists of exchanges of EAP messages, occurs between the supplicant and the authentication server. The authenticator acts as a transparent relay for this exchange and as a point of enforcement for any policy configuration instructions the authentication server may send back as a result of the authentication process.

The IEEE 802.1x specification defines a new link layer protocol, 802.1x, which is used for communications between the supplicant and the authenticator. Communications between the supplicant and authentication server also leverage the RADIUS protocol carried over standard UDP.

IEEE 802.1x is a well-defined standard with industry-wide acceptance. Supplicant, authenticator, and authentication server implementations are available from many vendors, including Cisco Systems.

802.1x Benefits

Cisco.com

Feature	Benefit
802.1x authenticator support	Enables interaction between the supplicant component on workstations and application of appropriate policy.
MAC address authentication	Adds support for devices such as IP phones that do not at present include 802.1x supplicant support.
Default authorization policy	Permits access for unauthenticated devices to basic network service.
Multiple DHCP pools	Authenticated users can be assigned IP addresses from a different IP range than unauthenticated users, allowing network traffic policy application by address range.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3.6

The table shows the benefits of 802.1x.

802.1x Benefits

Feature	Benefit
802.1x authenticator support	Enables interaction between the supplicant component on workstations and the application of appropriate policy.
MAC address authentication	Adds support for devices such as IP phones that at present do not include 802.1x supplicant support.
Default authorization policy	Permits access for unauthenticated devices to basic network service. In a home-network environment, a default access policy could be defined to allow Internet access for a spouse or children.
Multiple DHCP pools	Authenticated users can be assigned IP addresses from a different IP range than unauthenticated users, allowing network traffic policy application by address range.

Supported Topologies

Cisco.com

The 802.1X port-based authentication is supported in two topologies:

- **Point-to-point**
- **Wireless LAN**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—3.7

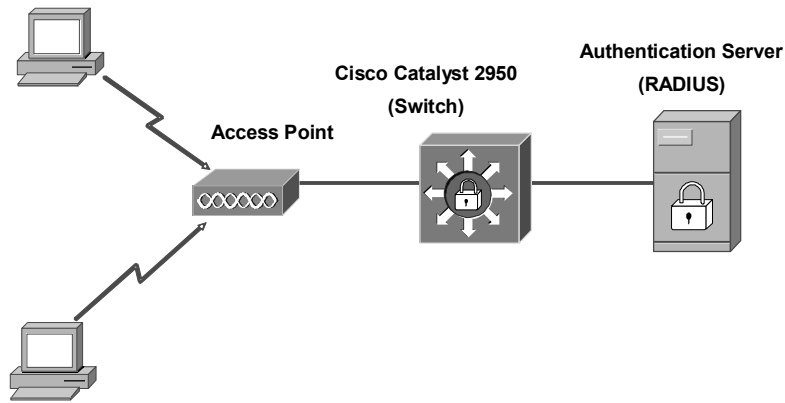
The 802.1x port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration, only one client can be connected to the 802.1x-enabled switch port. The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

802.1x Wireless LAN Example

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3.8

The figure shows 802.1x-port based authentication in a wireless LAN. The 802.1x port is configured as a multiple-host port that becomes authorized as soon as one client is authenticated. When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAP over LAN [EAPOL] logoff message is received), the switch denies access to the network to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and the wireless access point acts as a client to the switch.

802.1x and EAP

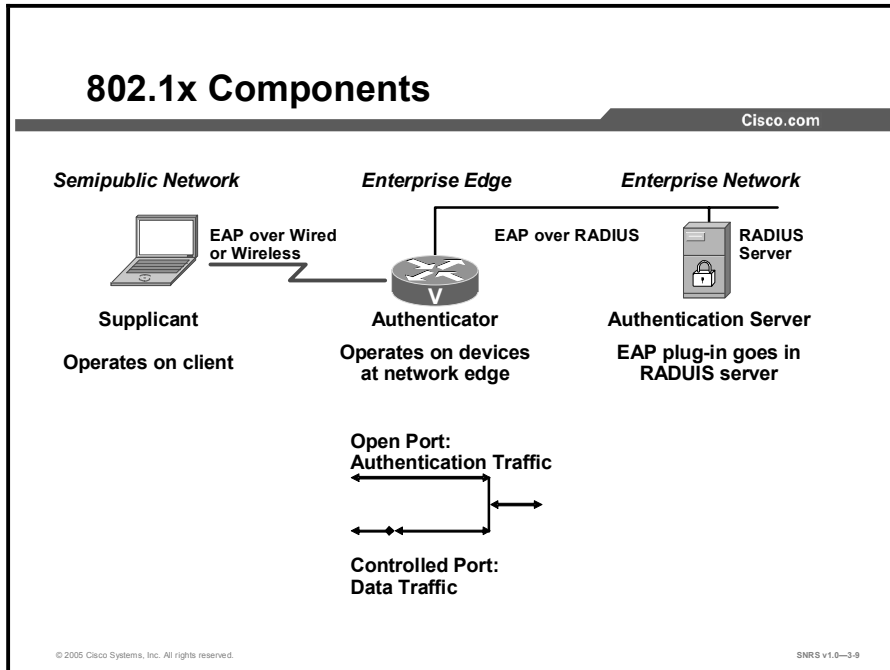
An alternative wireless LAN (WLAN) security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11 Task Group I end-to-end framework using 802.1x and EAP to provide this enhanced functionality. Cisco has incorporated 802.1x and EAP into its WLAN security solution—the Cisco Wireless Security Suite. The three main elements of an 802.1x and EAP approach are as follows:

- Mutual authentication between client and authentication (RADIUS) server
- Encryption keys dynamically derived after authentication
- Centralized policy control, where session timeout triggers reauthentication and new encryption key generation

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform mutual authentication, with the client verifying the RADIUS server credentials, and vice versa. An EAP supplicant is used on the client machine to obtain the user credentials (user ID and password, user ID and one-time password [OTP], or digital certificate). Upon successful client and server mutual authentication, the RADIUS server and client then derive a client-specific Wired Equivalent Privacy (WEP) key to be used by the client for the current logon session. User passwords and session keys are never transmitted in the clear over the wireless link.

802.1x Components

This topic describes the components of 802.1x.



The 802.1x specification is an IEEE standard for media-level access control, offering the ability to permit or deny network connectivity, control VLAN access, and apply traffic policy, based on user or machine identity.

802.1x Technology

Most applications are deployed to authenticate users, such as desktop users in a corporation or teleworkers at their home offices. In these situations, access control is required in order to prevent others, such as other residents of the home, from gaining access to controlled corporate resources. Two components are used to implement 802.1x functionality: the authenticator and the supplicant. The authenticator is a network component that checks credentials and applies the access policy, usually implemented on a router, switch, or wireless access point. The supplicant is a software component on the user workstation that answers the challenge from the authenticator. Supplicant functionality may also be implemented on network devices to authenticate to upstream devices; alternatively, mutual authentication functionality may be employed when network devices must restrict access policy to each other. Cisco IOS software does not currently support mutual authentication.

In the simplest scenario, no traffic is allowed to flow from a client device to the network until the client authenticates. The 802.1x frames are the only traffic between the client (supplicant) and the access-control device (authenticator). A user trying to access network resources must provide access credentials via software on the client workstation. Microsoft Windows XP includes 802.1x supplicant support, while an add-on component for Microsoft Windows 2000 is available as a Microsoft Hotfix.

When users provides their credentials, the information is transmitted to the authenticator by some variant of EAP. The user information is encrypted in the EAP transfer, so that the credentials cannot be easily compromised. The authenticator transmits the credentials to the authentication, authorization, and accounting (AAA) server, which verifies the user credentials against its database. If the AAA server is configured to return network access policy, it returns the policy associated with the user or the corresponding group. The authenticator applies the network policy to the user connection, allowing traffic to flow according to the policy. The policy may include traffic engineering values, VLAN information for user connection, and IP address information.

The authenticator can be configured with default access policies to offer restricted connectivity for client devices that do not have supplicant support. This allows unauthenticated users to have limited network access, but they will be required to provide credentials in some other fashion if access to restricted resources is needed. Default policy provision for IP phones, for instance, may be required, because IP phones do not yet include supplicant capability.

802.1x Applications with Cisco IOS Software

Cisco IOS software support for 802.1x functionality can be leveraged to improve security on telecommuter connections, where remote workers have single or multiple computers in the home and the user needs to prevent a spouse or children from gaining access to the corporate network. Through the application of default user policy, the spouse and children can have access to the public Internet but not the business network.

Extranet virtual private networking offers another application for 802.1x access control, in which users at the facilities of business partners are not allowed to access corporate resources until their controlled credentials are provided, ensuring that unauthorized users cannot access the network and that traffic from network attacks does not cross into the network of the partner.

The 802.1x technology can be leveraged inside the enterprise to ensure that only permitted users are allowed access to network connectivity resources. This capability could be integrated with other workstation software components to ensure that user computers have all required software updates (such as operating system service packs or antivirus software signature files), thus preventing restricted network access for users who represent a security risk.

802.1x in Cisco IOS Increases Network Security and Reliability

By leveraging the access-control features of 802.1x functionality, networks can be secured at the network access level against unauthorized intrusion. This moves the users closer to control of access to network bandwidth and resources closer to users, reducing the likelihood of unintentional network damage through the introduction of harmful agents. The 802.1x functionality also makes unauthorized access to protected resources more difficult through the requirement of valid access credentials. By deploying 802.1x, administrators effectively eliminate the possibility of enterprising users deploying unsecured wireless access points, resolving one of the biggest issues of easy-to-deploy wireless network equipment.

Several components of 802.1x support in Cisco IOS software offer capability for increased security on access router platforms.

Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles as shown in the previous figure.

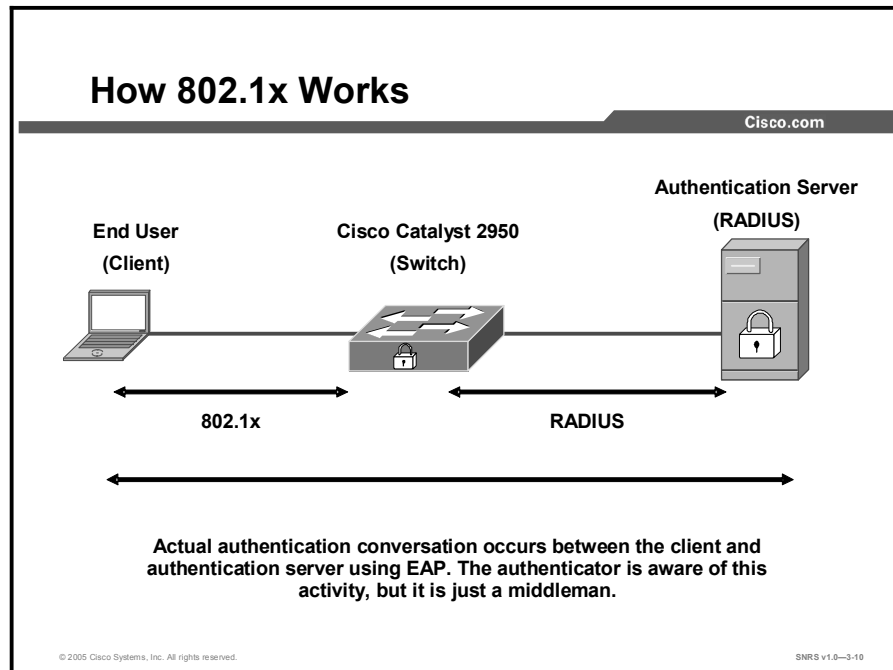
- **Client:** The device (workstation) that requests access to the LAN and switch services and responds to the requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the supplicant in the IEEE 802.1x specification.)
- **Authentication server:** Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch of whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the RADIUS security system with EAP extensions is the only supported authentication server; it is available in Cisco Secure ACS 3.0 or later. RADIUS operates in a client-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Switch (edge switch or wireless access point):** Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

The devices that can act as intermediaries include the Cisco Catalyst 3550 multilayer switch, Catalyst 2950 switch, or a wireless access point. These devices must be running software that supports the RADIUS client and 802.1x.

How 802.1x Works

This topic describes the operation of 802.1x.



The 802.1x technology works on a complex series of challenges and responses. This topic covers the authentication initiation, message exchanges, and port states.

Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the identity of the client.

Note If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

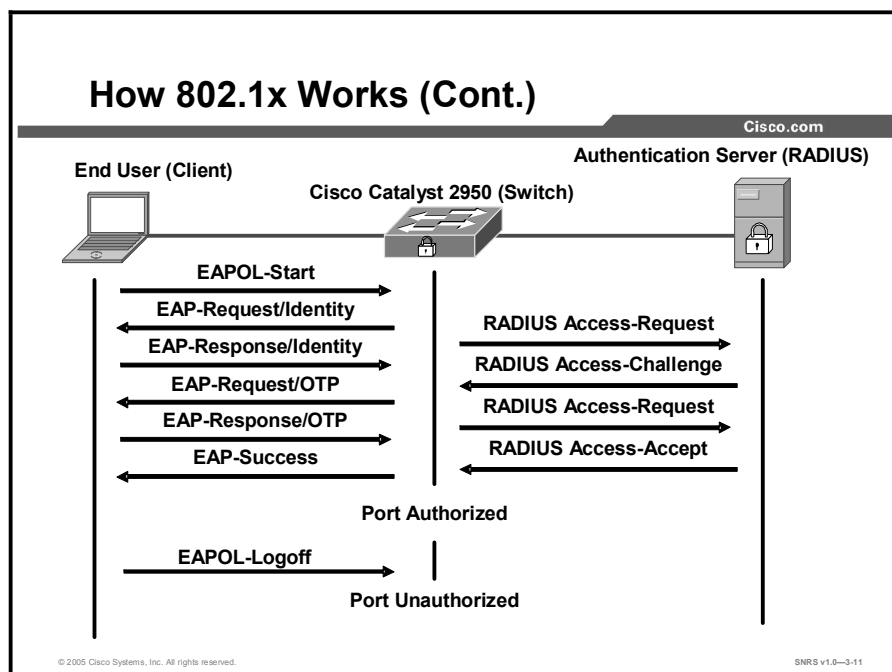
The specific exchange of EAP frames depends on the authentication method being used. The diagram shows a message exchange initiated by the client using the one-time password (OTP) authentication method with a RADIUS server.

Ports in Authorized and Unauthorized States

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1x packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the switch requests the identity of the client. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running 802.1x, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.



You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized:** Disables 802.1x and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
- **force-unauthorized:** Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
- **auto:** Enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Selecting the Correct EAP

This topic describes EAP types.

Selecting the Correct EAP

Cisco.com

- **EAP—Extensible Authentication Protocol**
- **Extension of PPP to provide additional authentication features**
- **A flexible protocol used to carry arbitrary authentication information**
- **Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)**
- **Specified in RFC 2284**
- **Support multiple authentication types :**
 - **EAP-MD5: Plain password hash (CHAP over EAP)**
 - **EAP-TLS (based on X.509 certificates)**
 - **LEAP (EAP-Cisco Wireless)**
 - **PEAP (Protected EAP)**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0–3-12

The Extensible Authentication Protocol (EAP), based on IETF 802.1x, is an end-to-end framework that allows the creation of authentication types without changing AAA client configurations.

EAP has the following characteristics:

- An extension of PPP to provide additional authentication features
- A flexible protocol used to carry arbitrary authentication information
- Typically rides on top of another protocol, such as 802.1x or RADIUS
- Specified in RFC 2284
- Supports multiple authentication types such as these:
 - EAP-MD5: Plain password hash (Challenge Handshake Authentication Protocol [CHAP] over EAP)
 - EAP-Transport Layer Security (EAP-TLS; based on X.509 certificates)
 - Lightweight EAP (LEAP, or EAP-Cisco Wireless)
 - Protected EAP (PEAP)

EAP Selection

Cisco.com

Cisco Secure ACS supports the following varieties of EAP:

- EAP-MD5
- EAP-TLS
- LEAP
- PEAP
- EAP-FAST

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3-13

Cisco Secure ACS supports the following varieties of EAP:

- **EAP-MD5:** An EAP protocol that does not support mutual authentication
- **EAP-TLS:** EAP incorporating Transport Layer Security
- **LEAP:** An EAP protocol used by Cisco Aironet wireless equipment that supports mutual authentication
- **PEAP:** Protected EAP, which is implemented with EAP-Generic Token Card (GTC) and EAP-Microsoft CHAP Version 2 (EAP-MS-CHAP v2) protocols
- **EAP-FAST:** EAP-Flexible Authentication via Secured Tunnel (EAP-FAST), a faster means of encrypting EAP authentication; supports EAP-GTC authentication

The table compares EAP types.

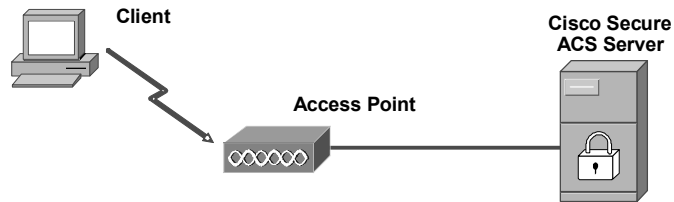
	LEAP	Microsoft PEAP	Cisco PEAP	EAP-TLS
Static password support	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OTP Support	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Microsoft Windows password change	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Requires server certificate	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Requires client certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lightweight Directory Access Protocol/Novell Directory Service (LDAP/NDS) database support	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LDAP only
Multi-operating system support	<input checked="" type="checkbox"/>	Microsoft operating systems	<input type="checkbox"/>	<input type="checkbox"/>
Single sign-on for Windows	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

The architecture of Cisco Secure ACS is extensible with regard to EAP; additional varieties of EAP will be supported as those protocols mature.

Cisco LEAP

Cisco.com

Lightweight Extensible Authentication Protocol



- Derives per-user, per-session key
- Enhancement to IEEE 802.11b Wired Equivalent Privacy (WEP) encryption
- Mutual Authentication—both user and access points need to be authenticated

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3.14

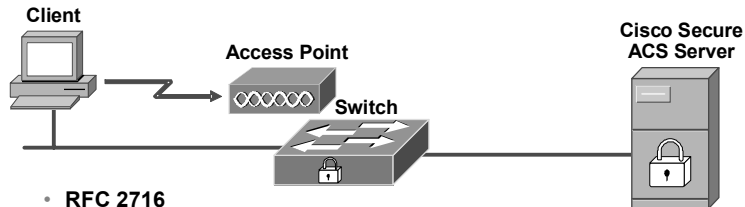
Cisco LEAP

Cisco LEAP is the widely deployed EAP type in use today in WLANs. With LEAP, mutual authentication relies on a shared secret, the user logon password, which is known by the client and the network. The RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server. When this process is complete, an EAP Success message is sent to the client, and both the client and the RADIUS server derive the dynamic WEP key.

EAP-TLS

Cisco.com

Extensible Authentication Protocol- Transport Layer Security



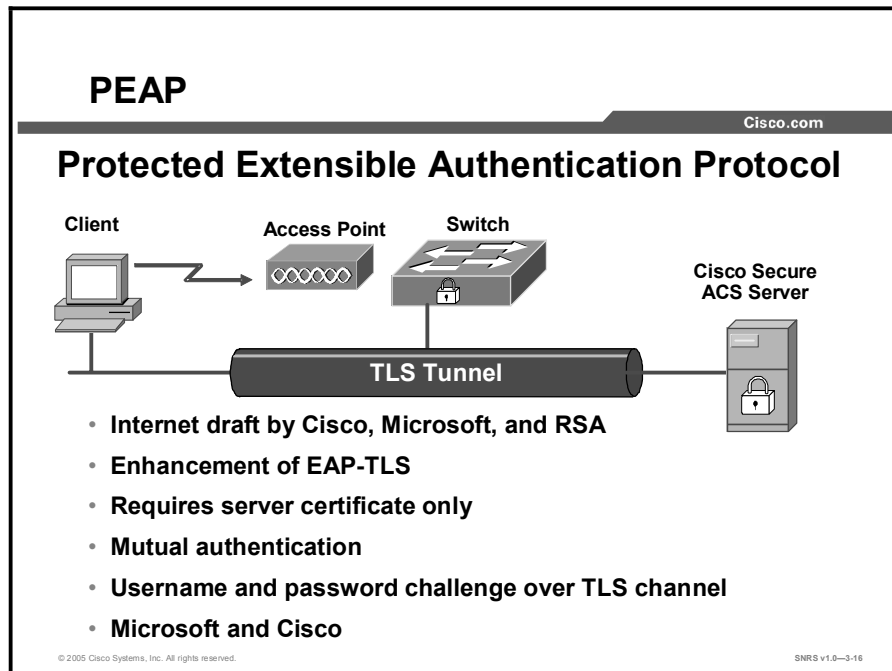
- RFC 2716
- Used for TLS handshake authentication (RFC 2246)
- Requires PKI (X.509) certificates rather than username and password
- Mutual authentication
- Requires client and server certificates
- Certificate management complex and costly

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—3-15

EAP-TLS

EAP-TLS is an IETF standard (RFC 2716) that is based on the TLS protocol (RFC 2246). EAP-TLS uses digital certificates for both user and server authentication and supports the three key elements of 802.1x and EAP mentioned previously. The RADIUS server sends its certificate to the client in phase 1 of the authentication sequence (server-side TLS). The client validates the RADIUS server certificate by verifying the issuer of the certificate—a certificate authority server entity—and the contents of the digital certificate. When this process is complete, the client sends its certificate to the RADIUS server in phase 2 of the authentication sequence (client-side TLS). The RADIUS server validates the client certificate by verifying the issuer of the certificate (certificate authority server entity) and the contents of the digital certificate. When this process is complete, an EAP Success message is sent to the client, and both the client and the RADIUS server derive the dynamic WEP key.



PEAP

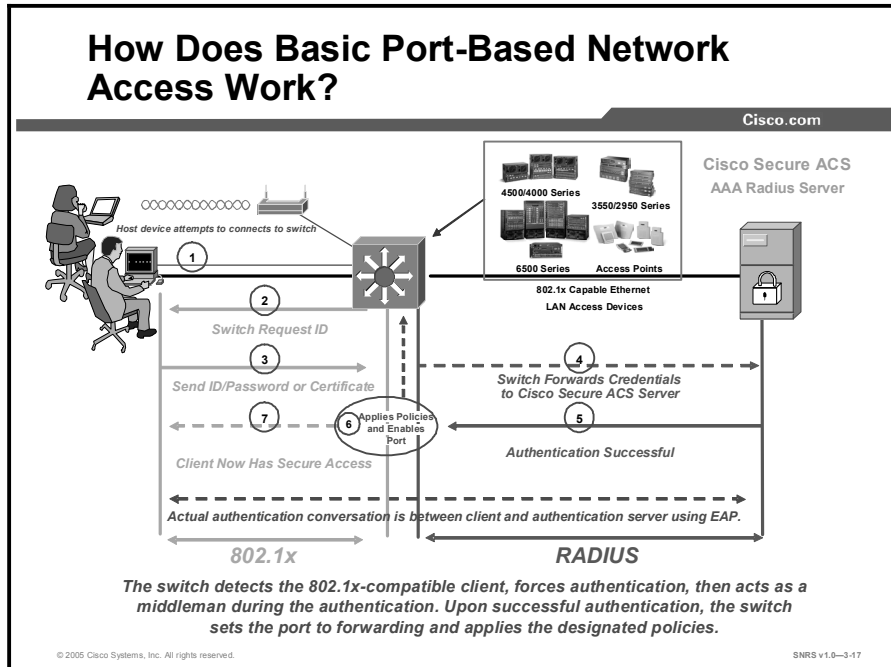
PEAP is an IETF draft RFC authored by Cisco Systems, Microsoft, and RSA Security. PEAP uses a digital certificate for server authentication. For user authentication, PEAP supports various EAP-encapsulated methods within a protected TLS tunnel. Phase 1 of the authentication sequence is the same as that for EAP-TLS (server-side TLS). At the end of phase 1, an encrypted TLS tunnel is created between the user and the RADIUS server for transporting EAP authentication messages. In phase 2, the RADIUS server authenticates the client through the encrypted TLS tunnel via another EAP type. As an example, a user can be authenticated using an OTP using the EAP-GTC subtype (as defined by the PEAP draft). In this case, the RADIUS server will relay the OTP credentials (user ID and OTP) to an OTP server to validate the user login. When this process is complete, an EAP Success message is sent to the client, and both the client and the RADIUS server derive the dynamic WEP key. For more information on PEAP, refer to the IETF Web site for the latest draft.

EAP Type Configuration

The important policy decision regarding authentication in a Cisco Catalyst switch environment is which EAP authentication type to deploy. The two choices are EAP-MD5 and EAP-TLS. This choice is likely to be influenced by which database is in use as well as by security implications. It is also worth noting that, unlike non-EAP RADIUS devices, where EAP is employed to carry the password protocol traffic over RADIUS, the AAA client device cannot function as policy enforcement point. Enforcement has to be provided by the Cisco Secure ACS because the AAA client device functions as a router of EAP traffic between the end-user client and the Cisco Secure ACS; the dialogue is essentially opaque to it. For a description of how to configure which EAP type to be enforced by the Cisco Secure ACS, see “Guidelines for Deploying EAP with Cisco Secure ACS for Windows NT/2000 Servers” at <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>.

Cisco Secure ACS

This topic describes how Cisco Secure ACS provides RADIUS-based AAA capabilities inside the LAN.



AAA in a Cisco Catalyst Switch (802.1x and EAPOL) Environment

Historically, Ethernet-based networks, whether simple broadcast or switched, offered few capabilities for the authentication of devices, or users, to the network. When originally developed, the protocols underpinning TCP/IP over Ethernet—Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP), for example—simply did not address user authentication, authorization, or accounting. The key challenge at the time was connectivity. Advanced security concerns were issues for the future. It is still true today that in the vast majority of organizations, any person who can physically attach a computer to the LAN will automatically be granted TCP/IP connectivity to the network without further checks concerning whether such connectivity is appropriate. With the security focus of most organizations having been on the external risks posed by connection to the Internet, relatively uncontrolled IP access has been available on the LAN. With the wider deployment of networks and the accompanying vulnerabilities, most organizations are becoming concerned about this reliance on crude physical security to limit access to their “sensitive” networks, which now includes all them.

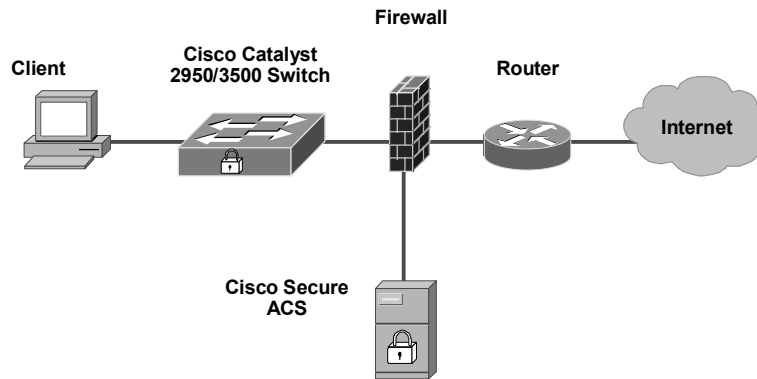
The addition of RADIUS support to Cisco Catalyst switches means that the user-based access control schemes—long available to control user access to the “point-to-point” links on remote-access routers—are now available on the “broadcast” links of Cisco Catalyst switches. This represents a fundamental breakthrough in the access-control schemes that can now be achieved on broadcast or switch-based Ethernet networks. An obvious example of configuration data that an organization might want delivered by RADIUS is the virtual LAN identification for each user.

EAP, as defined by IETF RFC 2284 and the IEEE 802.1x standards, represents the technology framework that makes it possible to deploy RADIUS into Ethernet network environments. It also facilitates the adoption of AAA schemes with the security advantages that using such AAA servers confer. The 802.1x standard, also known as EAPOL, concerns that part of the wider EAP standard that relates to broadcast media networks. Upon connection, EAPOL provides a “communications channel” between an end user on a client LAN device to the AAA server through the LAN switch. Conceptually, the functionality is very similar to that provided by PPP servers on point-to-point links. With the addition of AAA support for user access control, all Ethernet LAN connections can be authenticated against the individual user requesting it; only if valid credentials are supplied will network connectivity be provided. In addition, the RADIUS protocol provides for delivery of fine-grained control of the network connectivity to be supplied by switch to the user. Finally, RADIUS provides for the collection of user usage statistics of network resources.

By supporting complex challenge-response dialogues, EAP facilitates the user-based authentication demands of both conventional one-way hashed password authentication schemes such as CHAP and also of more advanced authentication schemes such as TLS, or digital certificates. Moreover, because EAP is extensible, additional password protocol schemes such as MS-CHAP or Kerberos will almost certainly become supported over time as demand for them grows. The flexible capabilities provided by EAP thus allow deploying organizations to start with less secure but simpler to implement authentication protocols and advance to more competent but demanding protocols as requirements dictate. For a more complete explanation of EAP and a discussion of the capabilities and security attributes of the different password protocol schemes supported, see “Guidelines for Deploying EAP with Cisco Secure ACS for Windows NT/2000 Servers” at <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>.

Cisco Secure ACS Deployment in a Small LAN

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

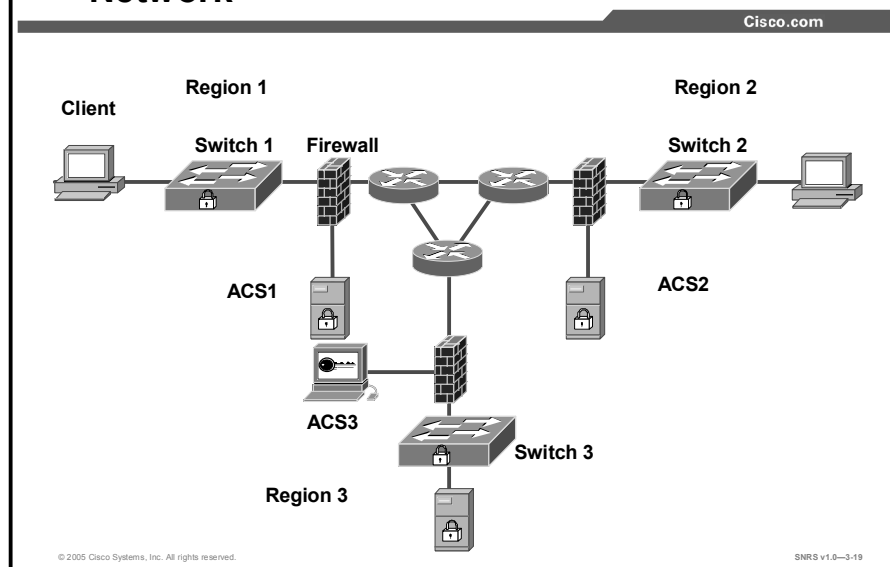
SNRS v1.0-3-18

Network Topology

How an enterprise network is configured is probably the most important factor in deciding how and where to deploy Cisco Secure ACS. With the complexity and wide geographic dispersion of enterprise networks today, the decision of how to deploy Cisco Secure ACS may vary widely depending on the network topology into which it is being deployed.

In the small LAN environment, a single Cisco Secure ACS would usually be located close to the switch. In this environment, the user database is usually small because few switches would require access to the Cisco Secure ACS for AAA, so the workload will be modest and require only a single Cisco Secure ACS. Even so, it would be wise to deploy a second server for redundancy, and it should be set up as a replication partner to the primary server because losing the Cisco Secure ACS would prevent users from gaining access to the network. As shown in the figure, an Internet connection via firewall and router is included because these are likely to be features of such a network; but they are not strictly related to the Cisco Catalyst AAA setup or required as part of it. It is also worth noting that it is prudent security policy to limit access to the system hosting the Cisco Secure ACS to as small a number of users and devices as necessary. In the figure, this is achieved by connecting the Cisco Secure ACS host through to a private LAN segment on the firewall; access to this segment would be limited to the Cisco Catalyst switch client and user machines that require HTTP access to the Cisco Secure ACS for administrative purposes. Normal LAN users should not be able to “see” the Cisco Secure ACS at all.

Cisco Secure ACS Deployment in a Global Network



In a larger network that is geographically dispersed, speed, redundancy, and reliability are important in determining whether to use a centralized Cisco Secure ACS service or a number of geographically dispersed Cisco Secure ACS units. As with many applications, AAA clients rely upon timely and deterministic responses to their queries. Network speed can be important in deciding how Cisco Secure ACS should be deployed, because delays in authentication introduced by the network can result in timeouts at the client side or the switch.

A useful approach in large extended networks, such as for a globally dispersed corporation, is to have at least one Cisco Secure ACS deployed in each major geographical region. Depending upon the quality of the WAN links, these may act as backup partners to servers in other regions to protect against failure of the Cisco Secure ACS in any particular region. In this figure, Switch 1 is configured with Cisco Secure ACS 1 as its primary AAA server but with Cisco Secure ACS 2 of Region 2 as its secondary. Switch 2 is configured with Cisco Secure ACS 2 as its primary but with Cisco Secure ACS 3 as its secondary. Likewise, Switch 3 uses Cisco Secure ACS 3 as its primary but Cisco Secure ACS 1 as its secondary. In this way, AAA WAN traffic is minimized by using a local Cisco Secure ACS as the primary AAA server, and the number of Cisco Secure ACS units required is also minimized by using the primary Cisco Secure ACS from another region as the secondary when necessary.

The model may be extended further down to the campus or even individual site level if reliable high-speed connections between locations are not incorporated or if the requirements of the individual sites are such that remotely sited servers may not provide adequate performance. The issues are similar to those relating to providing adequate performance for web users by means of caching: The greater the performance required, the closer to the user the cache needs to be located, particularly if the intermediate links are slow. It is worth noting, however, that RADIUS—being based on UDP and consisting of small challenge and response packets—imposes relatively low bandwidth demands and will not stress a WAN link that has a small amount of usable capacity, even in busy environments. Conversely, attention may be needed where virtual private network (VPN) connections between sites using the Internet are employed to provide the link. Although VPN connections save time and money, they do not always provide the deterministic response times and reliability that a dedicated Frame Relay or T1 link

would. If reliable authentication performance is critical to maintaining business functionality—most certainly the case where corporate users are accessing the LAN—the loss of the WAN connection between the switch and the remote Cisco Secure ACS could be catastrophic.

The same issue can be applied to an external database used by the Cisco Secure ACS. The database should be deployed near enough to the Cisco Secure ACS installation to ensure reliable and timely access. For more information, see “Guidelines for Placing ACS in the Network” at <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>

Network Access Policy

Network access policy is a broad concept. In general, it defines how users can connect to the network and what services they will be provided with when they are connected to it.

Cisco Secure ACS-based access policy enforcement provides control by using central authentication and authorization of network users. The Cisco Secure ACS database maintains all user IDs, passwords, and privileges (which are held in the form of a RADIUS access profile). Upon receipt of a RADIUS Access-Request packet from the switch on behalf of a particular user, the Cisco Secure ACS first determines which authentication method will be used for that request and then processes it. As noted above, with EAP, the authentication may actually be quite a complex process requiring multiple iterations through a challenge-response dialogue.

Cisco Secure ACS RADIUS Profile Configuration

After a user successfully completes the EAP authentication process of whatever type, the Cisco Secure ACS responds to the switch with a RADIUS Authentication-Accept packet granting that user access to the network. This packet is a fairly standard RADIUS Authentication-Accept packet and can carry a variety of the usual RADIUS attributes that may be communicated and that will be understood by the Cisco Catalyst switch. Taken as a whole, the attributes that compose the Access-Accept packet constitute an access profile. Once received by the switch, the attributes are then processed in compliance with the RADIUS protocol and whatever logic is implemented above the level of the protocol. The access profile generally contains user-specific authorization information, such as access control lists (ACLs) to be applied or the VLAN ID to be assigned. For a more complete description of the RADIUS profile and what each attribute means, see the “Cisco Secure ACS 3.0 for Windows 2000/NT Servers User Guide.” For a more complete description of which RADIUS attributes may be configured for consumption by a particular Cisco Catalyst switch, consult the documentation for that device at <http://www.cisco.com/en/US/products/>

Configuration of the RADIUS profile is performed on the Cisco Secure ACS under the Group Setup section or the User Setup section. For attributes to show up in the Group and User sections, they first have to be configured as required in the Interface Configuration section. The attributes required are as follows:

- [064] Tunnel-Type
- [081] Tunnel-Private-Group-ID

These attributes can be found under the IETF RADIUS Settings section of Interface Control. Checking these boxes causes the appropriate fields to appear on the Group and User pages.

For reasons of administrative scalability, RADIUS profiles are usually configured at the group level rather than one for each user. To configure a VLAN ID to be assigned to all users belonging to a specific group accessing the network through a Cisco Catalyst 4000, 5000, or 6000 Series switch, navigate to that group's page within Cisco Secure ACS and locate the IETF RADIUS settings section. If the steps in the Interface Configuration section have been followed, then attributes Tunnel-Type [# 64] and Tunnel-Private-Group-ID [# 81] will appear there for configuration.

To configure these, check the check box on the left of both attributes. For the Tunnel-Type attribute ensure the first Tag list is set to **1** and the corresponding value is set to **VLAN**. Make sure that the second Tag list is set to **0**. For the Tunnel-Private-Group-ID, again make sure that the first Tag list value is set to **1**, and then set the corresponding value field to the appropriate number for the VLAN to be assigned. Again, make sure that the second Tag list is set to **0**. In normal usage, RADIUS supports multiple tunnel attribute support tags. When assigning VLAN IDs to a Cisco Catalyst switch, it will ignore anything with a tag other than 1. In other words, only a single VLAN ID may be supplied in each RADIUS response packet to a Cisco Catalyst switch.

Note Because RADIUS VLAN ID assignment is not supported by Cisco Catalyst 2950 and 3550 switches, assignment of it by the Cisco Secure ACS using RADIUS should not be attempted. Support for VLAN ID to Cisco Catalyst 6000 switches by RADIUS requires Cisco Catalyst Operating System Software Version 7.2; so provision of the RADIUS VLAN ID attributes to switches running Cisco Catalyst operating systems at v7.1 or earlier should likewise not be attempted.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Cisco IBNS combines several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources.
- Benefits include the following:
 - Intelligent adaptability
 - A combination of authentication, access control, and user policies
 - User productivity gains and reduced operating costs
- The Cisco IBNS solution is based on standard RADIUS and 802.1x implementations.
- 802.1x is a standardized framework defined by the IEEE, designed to provide port-based network access.
- The EAP, based on IETF 802.1x, is an end-to-end framework that allows the creation of authentication types without changing AAA client configurations.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-20

Summary (Cont.)

Cisco.com

- 802.1x roles are supplicant, authenticator, and authentication server.
- The authentication process consists of exchanges of EAP messages.
- 802.1x supported in two topologies: point-to-point and wireless LAN.
- The switch port state determines whether or not the client is granted access to the network.
- You control the port authorization state by using the dot1x port-control interface configuration command.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-21

Summary (Cont.)

Cisco.com

- EAP supports multiple authentication types, such as these:
 - EAP-MD5: plain password hash (CHAP over EAP)
 - EAP-TLS (based on X.509 certificates)
 - LEAP (EAP-Cisco Wireless)
 - PEAP
- The two choices for authentication in a Cisco Catalyst switch environment are EAP-MD5 and EAP-TLS.
- In a larger network that is geographically dispersed, speed, redundancy, and reliability will be important in determining whether to use a centralized Cisco Secure ACS service or a number of geographically dispersed Cisco Secure ACS units.
- EAP is specified in RFC 2284.
- The 802.1x service is called port-level authentication.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—3-22

Lesson 3

Configuring 802.1x Port-Based Authentication

Overview

This lesson describes how to configure IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. As LANs extend to hotels, airports, and corporate lobbies, insecure environments could be created. The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN. You will review the process for and configure 802.1x port-based authentication on a Cisco Catalyst 2950T switch.

Objectives

Upon completing this lesson, you will be able to configure a Cisco Catalyst switch for 802.1x authentication. This ability includes being able to meet these objectives:

- List the tasks involved in configuring 802.1x port-based authentication on a Cisco Catalyst switch.
- Enable 802.1x authentication
- Configure the RADIUS server parameters on the switch
- Enable periodic reauthentication of the client
- Reauthenticate the client connected to a specific port at any time
- Configure the switch to allow multiple hosts (clients)
- Reset the 802.1x configuration to the default values
- Display 802.1x statistics for all interfaces and a specific interface and display the administrative and operational status of the switch using the appropriate form of the **show dot1x** privileged EXEC command

802.1x Port-Based Authentication Configuration Tasks

This topic describes tasks for 802.1x port-based authentication.

802.1x Port-Based Authentication Configuration

Cisco.com

- **Enable 802.1x authentication (required)**
- **Configure the switch-to-RADIUS-server communication (required)**
- **Enable periodic reauthentication (optional)**
- **Manually reauthenticate a client connected to a port (optional)**
- **Reset the 802.1x configuration to the default values (optional)**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3.4

Configuring 802.1x Authentication

The following lists the tasks involved in configuring 802.1x port-based authentication on your switch:

- 802.1x configuration guidelines
- Enable 802.1x authentication (required)
- Configure the switch-to-RADIUS-server communication (required)
- Enable periodic reauthentication (optional)
- Manually reauthenticating a client connected to a port (optional)
- Changing the quiet period (optional)
- Changing the switch-to-client retransmission time (optional)
- Setting the switch-to-client frame-retransmission number (optional)
- Enabling multiple hosts (optional)
- Resetting the 802.1x configuration to the default values (optional)

802.1x Port-Based Authentication Configuration (Cont.)

Cisco.com

- **Change the quiet period (optional)**
- **Change the switch-to-client retransmission time (optional)**
- **Set the switch-to-client frame-retransmission number (optional)**
- **Enable multiple hosts (optional)**
- **Reset the 802.1x configuration to the default values (optional)**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—3-6

Default 802.1x Configuration

The table describes the default 802.1x configuration on a switch.

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled.
RADIUS server	
<ul style="list-style-type: none"> ■ IP address ■ UDP authentication port ■ Key 	<ul style="list-style-type: none"> ■ None specified. ■ 1812. ■ None specified.
Per-interface 802.1x enable state	Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.
Periodic reauthentication	Disabled.
Number of seconds between reauthentication attempts	3600 seconds.
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	30 seconds (number of seconds that the switch should wait for a response to an Extensible Authentication Protocol [EAP]-request/identity frame from the client before resending the request).
Maximum retransmission number	Two times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).
Multiple host support	Disabled.
Client timeout period	30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before resending the request to the client).
Authentication server timeout period	30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before resending the response to the server). This setting is not configurable.

802.1x Configuration Guidelines

These are the 802.1x authentication configuration guidelines:

- When 802.1x is enabled, ports are authenticated before any other Layer 2 features are enabled.
- The 802.1x protocol is supported on Layer 2 static-access ports, but it is not supported on these port types:
 - **Trunk port:** If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.
 - **Dynamic ports:** A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x on a dynamic port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, the port mode is not changed.
 - **Dynamic-access ports:** If you try to enable 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
 - **EtherChannel port:** Before enabling 802.1x on the port, you must first remove it from the EtherChannel. If you try to enable 802.1x on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1x is not enabled. If you enable 802.1x on a not-yet-active port of an EtherChannel, the port does not join the EtherChannel.
 - **Secure port:** You cannot configure a secure port as an 802.1x port. If you try to enable 802.1x on a secure port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to a secure port, an error message appears, and the security settings are not changed.
 - **Switched Port Analyzer (SPAN) destination port:** You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. You can enable 802.1x on a SPAN source port.
 - **Long-Reach Ethernet (LRE) switch interface with Cisco 585 LRE Customer Premises Equipment (CPE):** The 802.1x protocol is not supported on an LRE switch interface that has a Cisco 585 LRE CPE connected to it.

Enabling 802.1x Authentication

This topic describes the tasks required to enable 802.1x authentication on the switch.

Enabling 802.1x Authentication

Cisco.com

Switch#

`configure terminal`

- **Enter global configuration mode**

Switch(config)#

`aaa new-model`

- **Enables AAA**

Switch(config)#

`aaa authentication dot1x default group radius`

- **Creates an 802.1x authentication method list**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3.6

To enable 802.1x port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication. This procedure is required:

- Step 1** Enter global configuration mode.
configure terminal

- Step 2** Enable AAA.
aaa new-model

- Step 3** Create an 802.1x authentication method list.
aaa authentication dot1x {default} method1 [method2...]

To create a default list that is used when a named list is not specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

Enter at least one of these keywords:

- **group radius:** Use the list of all RADIUS servers for authentication.
- **none:** Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Enabling 802.1x Authentication (Cont.)

Cisco.com

```
Switch(config)#
```

```
interface fastethernet0/12
```

- Enter interface configuration mode

```
Switch(config-if)#
```

```
dot1x port-control auto
```

- Enables 802.1x authentication on the interface

```
Switch(config-if)#
```

```
end
```

- Returns to privileged EXEC mode

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-37

Step 4 Enter interface configuration mode, and specify the interface connected to the client that is to be enabled for 802.1x authentication.

```
interface interface-id
```

Step 5 Enable 802.1x authentication on the interface.

```
dot1x port-control auto
```

You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized:** Disables 802.1x and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
- **force-unauthorized:** Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

- **auto**: Enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAP over LAN (EAPOL) frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.

Step 6 Return to privileged EXEC mode.

end

Step 7 Verify your entries.

show dot1x

To disable AAA, use the **no aaa new-model** global configuration command. To disable 802.1x AAA authentication, use the **no aaa authentication dot1x {default | list-name} method1 [method2...]** global configuration command. To disable 802.1x authentication, use the **dot1x port-control force-authorized** or the **no dot1x port-control** interface configuration command.

This example shows how to enable AAA and 802.1x on Fast Ethernet port 0/12:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# interface fastethernet0/12
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```


Configuring the Switch-to-RADIUS Server Communication

This topic describes the configuration of switch-to-RADIUS server communications.

Configuring Switch-to-RADIUS Communication

Cisco.com

```
Switch(config)#  
radius-server host 172.120.39.46 auth-port 1812 key rad123
```

- **Configures the RADIUS server parameters on the switch**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0--3-8

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the failover backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required:

Step 1 Enter global configuration mode.

configure terminal

Step 2 Configure the RADIUS server parameters on the switch.

radius-server host {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*

For *hostname* | *ip-address*, specify the host name or IP address of the remote RADIUS server.

For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1812.

For **key string**, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.

Note Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.

If you want to use multiple RADIUS servers, re-enter this command.

Step 3 Return to privileged EXEC mode.
end

Step 4 Verify your entries.
show running-config

To delete the specified RADIUS server, use the **no radius-server host** *{hostname | ip-address}* global configuration command.

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to rad123, matching the key on the RADIUS server:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 key  
rad123
```

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, refer to the RADIUS server documentation.

Enabling Periodic Reauthentication

This topic describes how to enable periodic reauthentication.

Enabling Periodic Reauthentication

Cisco.com

Switch#

`configure terminal`

- **Enter global configuration mode**

Switch(config)#

`dot1x re-authentication`

- **Enables periodic reauthentication of the client, which is disabled by default**

Switch(config)#

`dot1x timeout re-authperiod seconds`

- **Sets the number of seconds between reauthentication attempts**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3.9

You can enable periodic 802.1x client reauthentication and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication attempts is 3600.

Automatic 802.1x client reauthentication is a global setting and cannot be set for clients connected to individual ports.

Beginning in privileged EXEC mode, follow these steps to enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts:

- Step 1** Enter global configuration mode.
- configure terminal**
- Step 2** Enable periodic reauthentication of the client, which is disabled by default.
- dot1x re-authentication**
- Step 3** Set the number of seconds between reauthentication attempts.
- dot1x timeout re-authperiod** seconds
- The range is 1 to 4294967295; the default is 3600 seconds.
- This command affects the behavior of the switch only if periodic reauthentication is enabled.
- Step 4** Return to privileged EXEC mode.
- end**

Step 5 Verify your entries.

show dot1x

To disable periodic reauthentication, use the **no dot1x re-authentication** global configuration command. To return to the default number of seconds between reauthentication attempts, use the **no dot1x timeout re-authperiod** global configuration command.

This example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000:

```
Switch(config)# dot1x re-authentication
```

```
Switch(config)# dot1x timeout re-authperiod 4000
```

Manually Reauthenticating a Client Connected to a Port

This topic describes how to manually reauthenticate a client connected to a port.

Manually Reauthenticating a Client Connected to a Port

Cisco.com

```
Switch(config)#  
dot1x re-authenticate interface fastethernet0/12
```

- **Starts reauthentication of the client**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-10

You can manually reauthenticate the client connected to a specific port at any time by entering the **dot1x re-authenticate interface *interface-id*** privileged EXEC command.

This example shows how to manually reauthenticate the client connected to Fast Ethernet port 0/1:

```
Switch(config)# dot1x re-authenticate interface fastethernet0/12
```

- Starts reauthentication on FastEthernet0/12

Enabling Multiple Hosts

This topic describes the steps required to enable multiple hosts on a single port.

Enabling Multiple Hosts

Cisco.com

Switch#

`configure terminal`

- **Enter global configuration mode**

Switch(config)#

`interface fastethernet0/12`

- **Enter interface configuration mode and specifies the interface to which multiple hosts are indirectly attached**

Switch(config-if)#

`dot1x multiple-hosts`

- **Allows multiple hosts (clients) on an 802.1x-authorized port**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-11

You can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**.

- Step 1** Enter global configuration mode.
configure terminal

- Step 2** Enter interface configuration mode, and specify the interface to which multiple hosts are indirectly attached.
interface *interface-id*

- Step 3** Allow multiple hosts (clients) on an 802.1x-authorized port. Make sure that the **dot1x port-control** interface configuration command set is set to **auto** for the specified interface.
dot1x multiple-hosts

- Step 4** Return to privileged EXEC mode.
end

Step 5 Verify your entries.

show dot1x interface *interface-id*

To disable multiple hosts on the port, use the **no dot1x multiple-hosts** interface configuration command.

This example shows how to enable 802.1x on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Switch(config)# interface fastethernet0/1  
Switch(config-if)# dot1x port-control auto  
Switch(config-if)# dot1x multiple-hosts
```

Resetting the 802.1x Configuration to the Default Values

This topic describes steps required to reset the 802.1x to the default values.

Resetting the 802.1x Configuration to the Default Values

Cisco.com

Switch#

`configure terminal`

- **Enter global configuration mode**

Switch(config)#

`dot1x default`

- **Resets the configurable 802.1x parameters to the default values**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0—3-12

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x configuration to the default values:

- Step 1** Enter global configuration mode.
configure terminal
- Step 2** Reset the configurable 802.1x parameters to the default values.
dot1x default
- Step 3** Return to privileged EXEC mode.
end
- Step 4** Verify your entries.
show dot1x

Displaying 802.1x Statistics and Status

This topic describes how to review 802.1x status and statistics.

Displaying 802.1x Statistics

Cisco.com

Switch#

```
show dot1x statistics
```

- **Displays 802.1x statistics**

Switch#

```
show dot1x statistics interface interface-id
```

- **Displays 802.1x statistics for s specific interface**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-3-13

To display 802.1x statistics for all interfaces, use the **show dot1x statistics** privileged EXEC command. To display 802.1x statistics for a specific interface, use the **show dot1x statistics interface *interface-id*** privileged EXEC command.

Displaying 802.1x Status

Cisco.com

Switch#

```
show dot1x
```

- Displays 802.1x administrative and operational status

Switch#

```
show dot1x interface interface-id
```

- Displays 802.1x administrative and operational status for a specific interface

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3-14

To display the 802.1x administrative and operational status for the switch, use the **show dot1x** privileged EXEC command. To display the 802.1x administrative and operational status for a specific interface, use the **show dot1x interface *interface-id*** privileged EXEC command.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- When 802.1x is enabled, ports are authenticated before any other Layer 2 features are enabled.
- The 802.1x standard is not supported on certain port types such as trunks.
- To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list.
- A method list describes the sequence and authentication methods to be queried to authenticate a user.
- If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.
- You can create a default list that is used when a named list is not specified.
- RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-15

Summary (Cont.)

Cisco.com

- The RADIUS host entries are tried in the order that they were configured.
- The key is a text string that must match the encryption key used on the RADIUS server.
- You also need to configure some settings on the RADIUS server.
- If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication attempts is 3600.
- You can manually reauthenticate the client connected to a specific port at any time.
- You can attach multiple hosts to a single 802.1x-enabled port.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-16

Lesson 4

Identifying Layer 2 Security Best Practices

Overview

This lesson covers informational material on best practices for Layer 2 security. You will be exposed to multiple physical network scenarios and be given vulnerabilities and mitigation techniques for each.

Objectives

Upon completing this lesson, you will be able to, for topologies using single and multiple switches, recommend an appropriate approach to threat mitigation. This ability includes being able to meet these objectives:

- List the three factors affecting mitigation strategy techniques applicable to a range of situations
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of a single security zone, one user group, and one physical switch
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of a single security zone, one user group, and multiple physical switches
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of a single security zone, multiple user groups, and a single physical switch
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of a single security zone, multiple user groups, and multiple physical switches
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of multiple security zones, one user group, and a single physical switch
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of multiple security zones, one user group, and multiple physical switches
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of multiple security zones, multiple user groups, and a single physical switch
- Recommend an appropriate mitigation technique against the vulnerabilities of a topology consisting of multiple security zones, multiple user groups, and multiple physical switches

Factors Affecting Layer 2 Mitigation Techniques

This topic describes the factors affecting Layer 2 mitigation techniques.

Factors Affecting Layer 2 Mitigation Techniques

Cisco.com

- **The number of security zones in the network design**
- **The number of user groups in the network design**
- **The number of switch devices in the design**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-3.4

Much of the information covered in this lesson is applicable to many situations. The following cases are meant to highlight implementation of some of the Layer 2 mitigation techniques in specific situations. The various cases considered depend on three factors:

- The number of security zones in the network design
- The number of user groups in the network design
- The number of switch devices in the design.

These scenarios can be broken down into eight total cases, as shown in the next figure.

Typical Cases

Cisco.com

Case Number	Security Zones	Number of User Groups	Number of Switch Devices
1	Single	Single	Single
2	Single	Single	Multiple
3	Single	Multiple	Single
4	Single	Multiple	Multiple
5	Multiple	Single	Single
6	Multiple	Single	Multiple
7	Multiple	Multiple	Single
8	Multiple	Multiple	Multiple

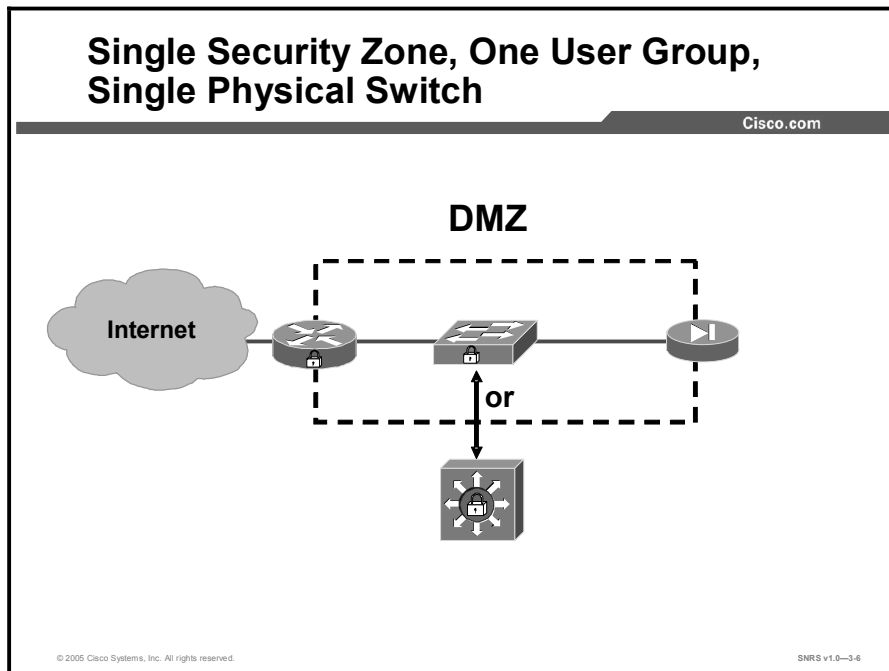
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—3-6

The table in the figure can be read as follows: Case 1 involves a network design where there is a single security zone of trust, used by a single user group, that includes only one physical switch. Case 8 involves a network design where there are multiple security zones of trust, with multiple user groups, and multiple physical switches in the design. An example of case 1 could be a small business network using a broadband connection behind a DSL router or firewall. An example of case 8 could be a large application service provider data center. These cases are discussed in further detail in this lesson.

Single Security Zone, One User Group, One Physical Switch

This topic describes a scenario with a single security zone, one user group, and one physical switch.



This design provides for a single physical switch existing within a zone of trust. Traffic from only one user group traverses the switch. An example of such a design would be a switch within a network Demilitarized Zone (DMZ) created between an edge router and a corporate firewall, as shown in the figure. In this design, all systems within the security zone are on the same VLAN.

Vulnerabilities

This primary Layer 2 vulnerabilities of this design include the following:

- MAC spoofing
- CAM table overflow

Mitigation

Use the mitigation techniques described in the “CAM Table Overflow Attack” and “MAC Spoofing” topics to secure the Layer 2 environment in this design. Port security may well be administratively appropriate in this case because of the limited size of the design. The Layer 2 switches are a part of the security perimeter between the zones of trust and should be managed as securely as possible, including the use of Secure Shell (SSH) protocol for command line management, Simple Network Management Protocol Version 3 (SNMP v3) for remote management, configuration audits and regular penetration testing of each VLAN using tools capable of exploiting Layer 2 vulnerabilities such as dsniff. An equally effective and less administratively burdensome approach would be to use dynamic port security through the application of Dynamic Host Configuration Protocol (DHCP) snooping and Dynamic Address Resolution Protocol Inspection (DAI).

Commands to mitigate MAC spoofing (Cisco Catalyst operating system) are as follows:

```
set port security mod/port enable [mac_addr]
set port security mod/port [mac_addr]
set port security mod/port violation {shutdown | restrict}
```

Commands to mitigate MAC spoofing (Cisco IOS software) are as follows:

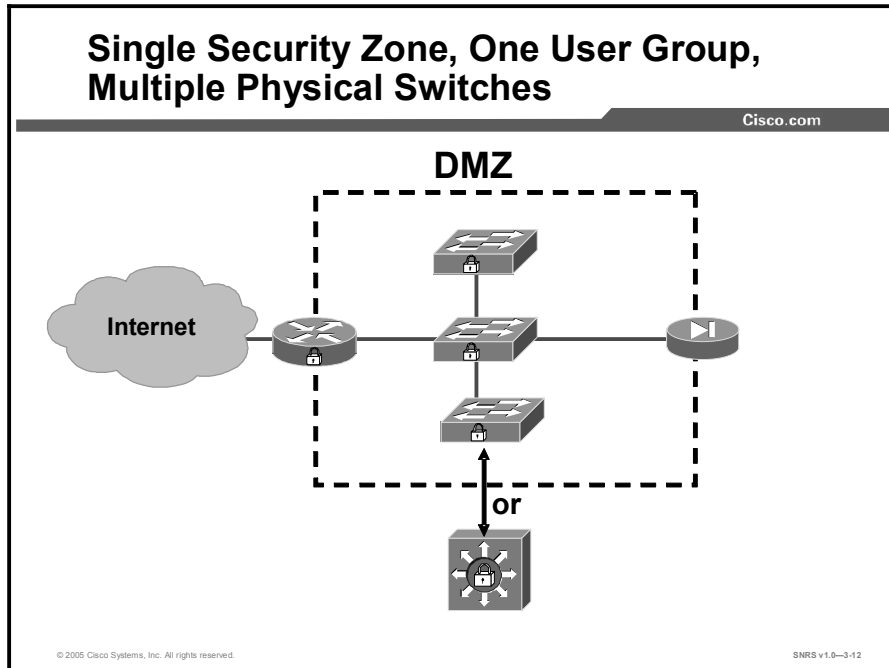
```
switchport port-security maximum value
switchport port-security violation {protect | restrict | shutdown}
arp timeout seconds
```

Commands configuring DHCP snooping (Cisco IOS software) are as follows:

```
ip dhcp snooping
ip dhcp snooping vlan vlan_id {,vlan_id}
ip dhcp snooping trust
ip dhcp snooping limit rate rate
```

Single Security Zone, One User Group, Multiple Physical Switches

This topic describes a single security zone, one user group, and multiple physical switches.



This design provides for multiple physical switches existing within a single zone of trust. Traffic for only one user group traverses the switch and can be represented by a very large DMZ, as shown in the figure, or a DMZ with multiple VLANs, all existing within a single security zone of trust. This could also be represented as a Layer 3 switch within the DMZ to provide inter-VLAN routing.

Vulnerabilities

This design's primary Layer 2 vulnerabilities include the following:

- MAC spoofing
- CAM table overflow
- VLAN hopping
- Spanning tree attacks (for multiple switches)

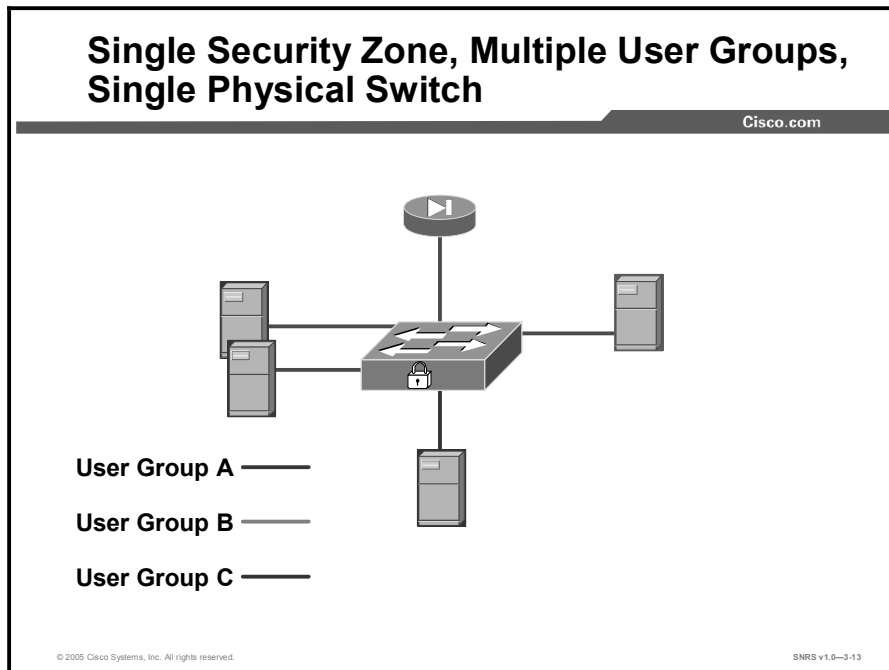
Mitigation

If the security zone is small enough, use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. Bridge protocol data unit (BPDU) guard and root guard can be used to mitigate attacks against Spanning Tree Protocol (STP).

The Layer 2 switches are a part of the security perimeter between zones of trust and should be managed as securely as possible, including the use of SSH for command line management, SNMP v3 for remote management, configuration audits, and regular penetration testing of each VLAN using tools capable of exploiting Layer 2 vulnerabilities such as dsniff.

Single Security Zone, Multiple User Groups, Single Physical Switch

This topic describes a single security zone, multiple user groups, and a single physical switch.



In this design, VLANs are used to logically separate the traffic of multiple user groups within a single physical network. A typical example of such a design would be an application service provider data center or different departments within a single corporate enterprise that require data segregation.

Vulnerabilities

The primary Layer 2 vulnerabilities of this design include the following:

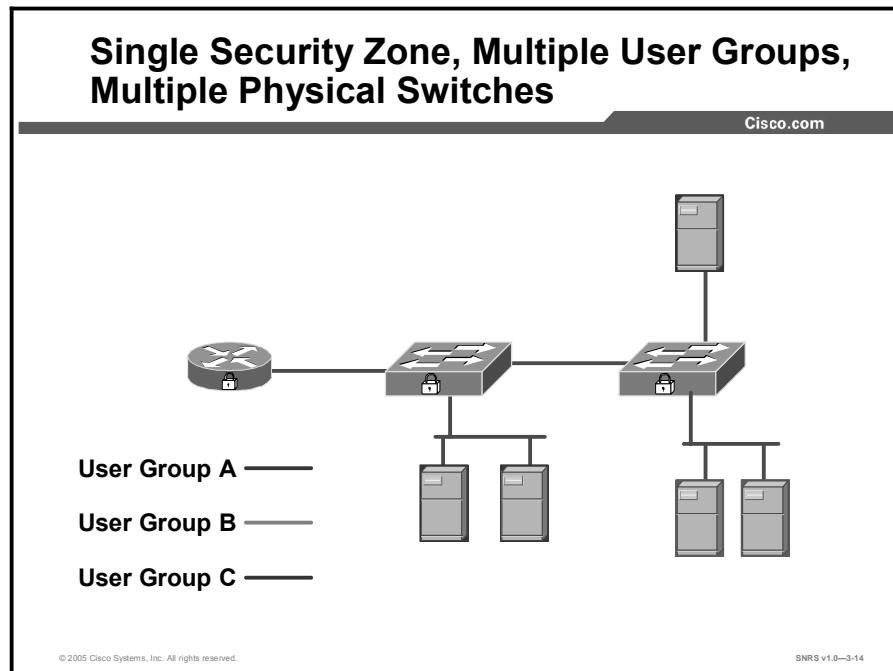
- MAC spoofing
- CAM table overflow
- VLAN hopping

Mitigation

If the security zone is small enough, use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this lesson. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Single Security Zone, Multiple User Groups, Multiple Physical Switches

This topic describes a single security zone, multiple user groups, and multiple physical switches.



This scenario represents a slightly more complex case than the case in the previous topic. This design, shown in the diagram, represents one where high availability is a factor as well as the need to trunk information between the switch devices. In addition, the direction of travel for the network traffic as determined through STP requires additional considerations when you are determining some of the more specific mitigation techniques. VLANs are used to provide traffic segmentation between the various user groups.

Vulnerabilities

The primary Layer 2 vulnerabilities of this design include the following:

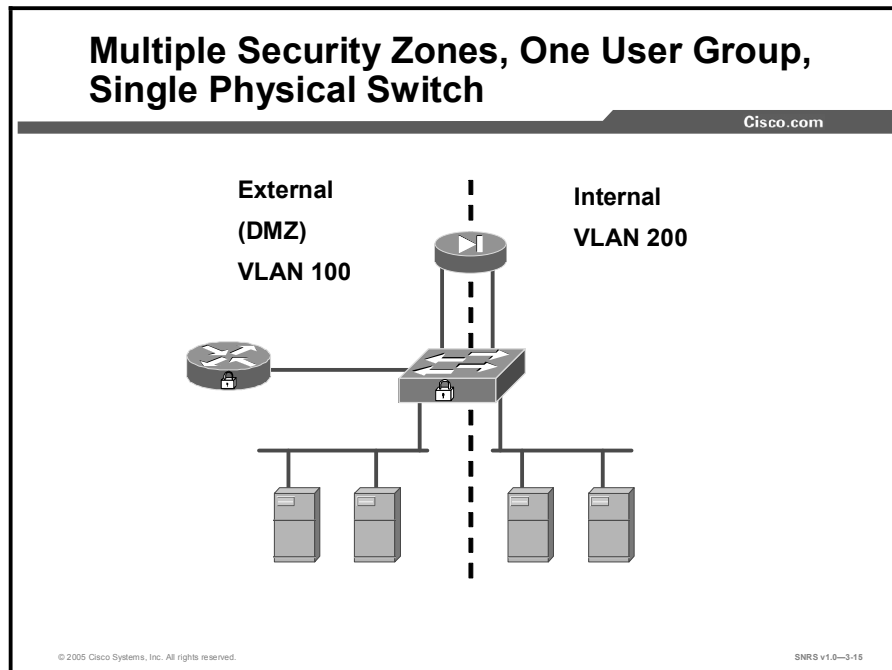
- MAC spoofing
- CAM table overflow
- VLAN hopping
- STP attacks

Mitigation

If the security zone is small enough, use port security to help mitigate the CAM table overflow vulnerability and MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this lesson. If necessary, deploy 802.1x authentication to prevent unauthorized access to the security zone from an attacker who may physically connect to a switch in the design. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Multiple Security Zones, One User Group, Single Physical Switch

This topic describes multiple security zones, one user group, and a single physical switch.



This design provides for a single physical switch existing two security zones of trust. Traffic from only one user group traverses the switch. An example of such a design would be a switch which is configured for “double duty” on a firewall DMZ or internal interfaces. VLANs separate traffic on a single physical LAN into multiple logical LANs through the use of VLAN tags. The use of VLANs can be considered as a possible way of segmenting multiple interfaces of a firewall on a single switch as shown in the figure. In this example, the external network, the DMZ, and the internal network utilize the same switch for Layer 2 connectivity. The external network traffic is tagged as VLAN 100, while the internal network traffic is tagged as VLAN 200. Although it is technically feasible to make this design secure, there are significant ramifications should the switch be compromised.

Vulnerabilities

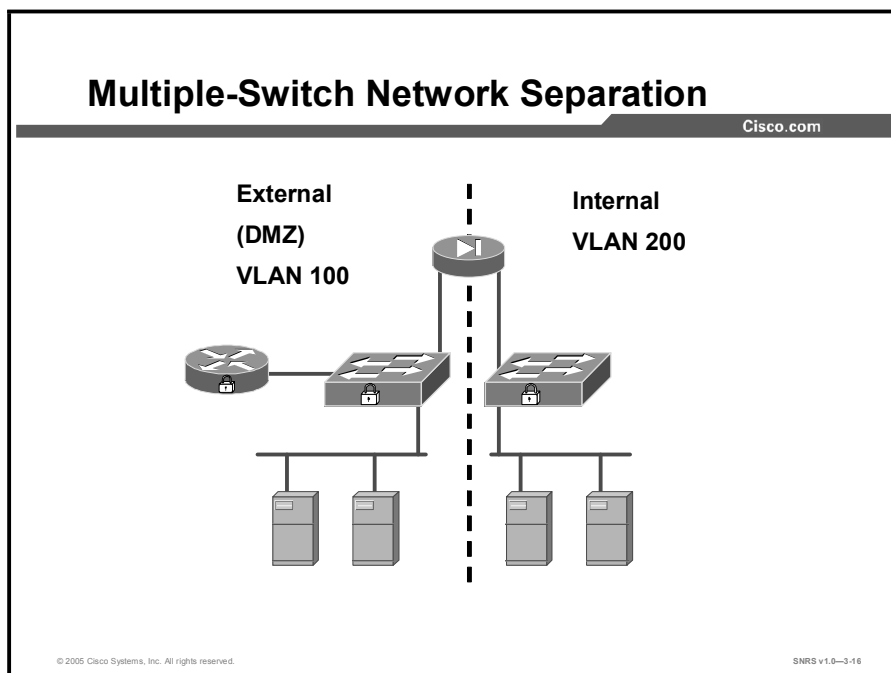
The primary Layer 2 vulnerabilities of this design include the following:

- MAC spoofing (within VLANs)
- CAM table overflow (per-VLAN traffic flooding)
- VLAN hopping

Mitigation

If the security zones are small enough, use port security to help mitigate the CAM table overflow vulnerability as well as the MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this lesson. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

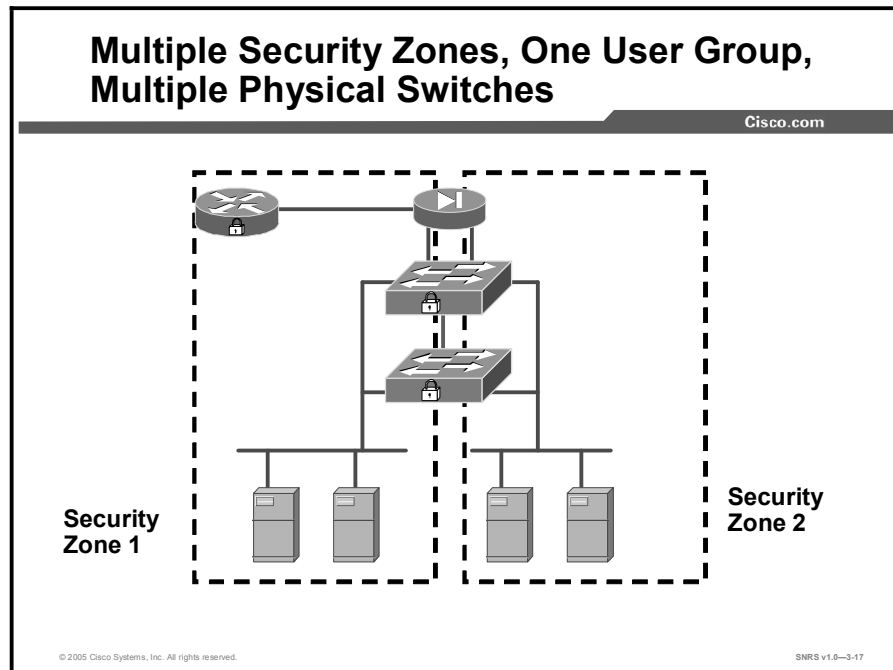
In this design another mitigation approach would be to split the Layer 2 functionality of the switch to two separate physical switches. If this is done, then the mitigation techniques described in case 1 would apply to both distinct security zones.



If private VLANs (PVLANS) are employed in any of the VLANs, consideration must be given to the possibility of PVLAN attacks. If the VLANs utilize DHCP for address assignment, then DHCP starvation by an attacker needs to be considered.

Multiple Security Zones, One User Group, Multiple Physical Switches

This topic describes multiple security zones, one user group, and multiple physical switches.



This design represents a large data center within a single enterprise. However, the need to segregate traffic and data for various groups or departments within the enterprise is reflected by the separation of the data center into security zones. This can be accomplished securely through the use of VLANs within the data center; however, there are considerations that must be evaluated regarding some of the potential vulnerabilities. The two switches have a trunk between them, represented by the solid green line, carrying all of the VLAN traffic between the switches.

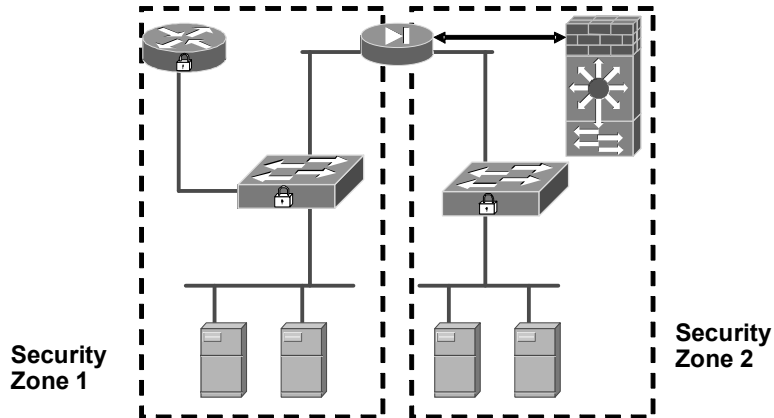
Vulnerabilities

The primary Layer 2 vulnerabilities of this design include the following:

- MAC spoofing (within VLANs)
- CAM table overflow (per-VLAN traffic flooding)
- VLAN hopping
- STP attacks

Alternative Design for Multiple Security Zones, One User Group, Multiple Switches

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

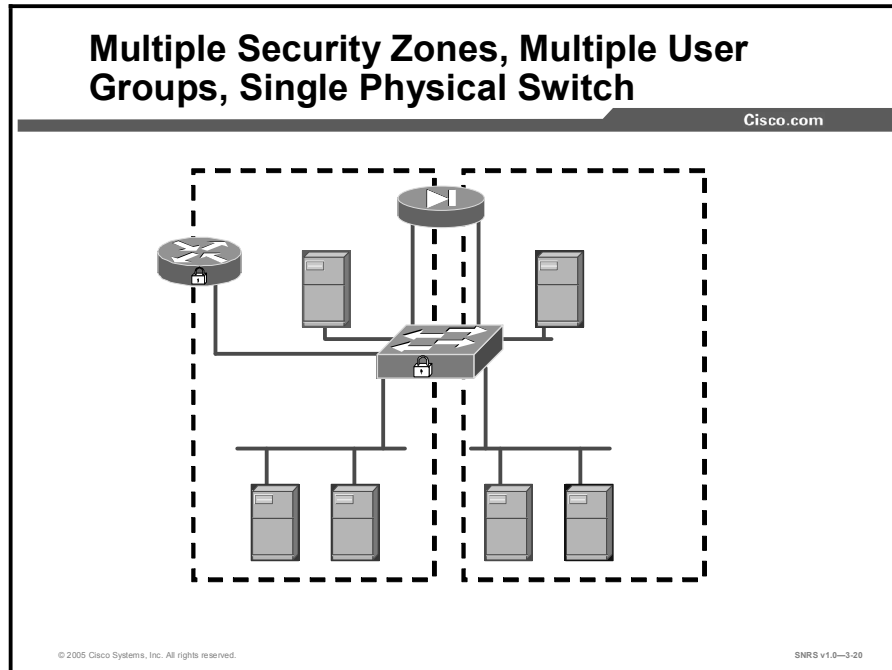
SNRS v1.0-3-19

Mitigation

If the security zones are small enough, use port security to help mitigate CAM table overflow vulnerabilities and MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this lesson. If necessary, deploy 802.1x authentication to prevent unauthorized access to each of the security zones by an attacker who may physically connect to a switch in the design. Another possible mitigation method would be to add a firewall within the design or add a Layer 3 switch with an integrated firewall, as shown in the figure. The firewall enforces additional Layer 3 traffic segregation. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Multiple Security Zones, Multiple User Groups, Single Physical Switch

This topic describes multiple security zones, multiple user groups, and a single physical switch.



This design is very similar to the previous scenario in having multiple user groups within the data center, each requiring their own level of security for their systems. However in this case, all of the user groups connect to a single central switch. VLANs can be used to provide traffic segregation between the security zones.

Vulnerabilities

The primary Layer 2 vulnerabilities of this design include the following:

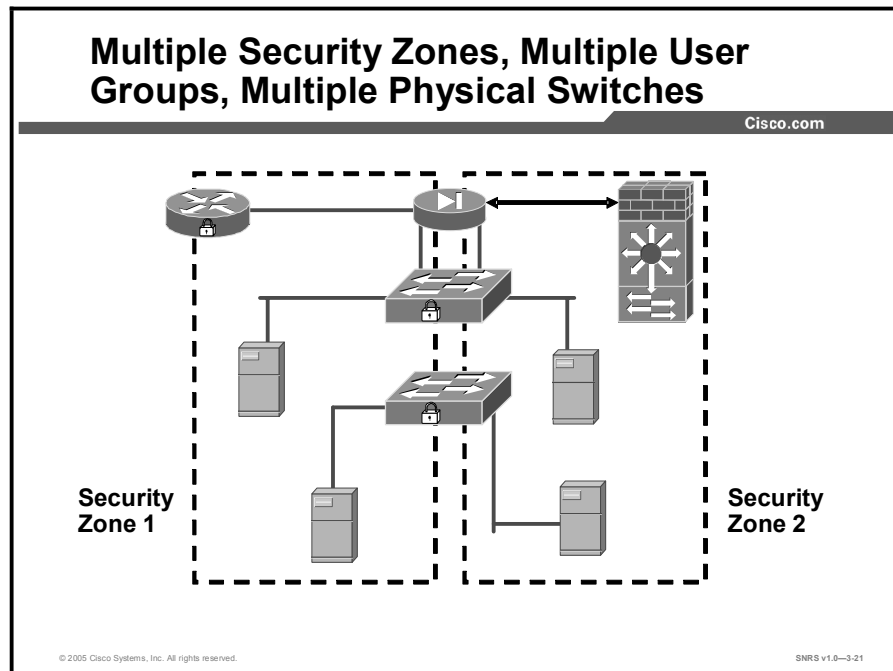
- MAC spoofing (within VLANs)
- CAM table overflow (per-VLAN traffic flooding)
- VLAN hopping
- PVLAN attacks (on a per-VLAN basis)

Mitigation

If the security zones are small enough, use port security to help mitigate CAM table overflow vulnerabilities and MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this lesson. If necessary, deploy 802.1x authentication to prevent unauthorized access to each of the security zones by an attacker who may physically connect to a switch in the design. Another possible mitigation method would be to add a firewall within the data center design and integrate it into the central switch, similar to the technique employed in the previous design. The firewall enforces additional Layer 3 traffic segregation between the various user groups. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Multiple Security Zones, Multiple User Groups, Multiple Physical Switches

This topic describes multiple security zones, multiple user groups, and multiple physical switches.



This design represents the most complex of the series. It is very similar to the previous scenario in having multiple user groups within the data center, each requiring their own level of security for their systems. Instead of all the user groups connecting to a single central switch, there are multiple switches (both Layer 2 and Layer 3) throughout the design. VLANs can be used to provide traffic segregation between the security zones; however, the need to provide high security in some of the zones may require additional measures.

Vulnerabilities

- MAC spoofing (within VLANs)
- CAM table overflow (per-VLAN traffic flooding)
- VLAN hopping
- STP attacks
- VLAN Trunking Protocol (VTP) attacks

If private VLANs are implemented within each VLAN, this design may also be vulnerable to the PVLAN proxy attack described earlier. Additionally, if one of the VLANs is large and DHCP is used for address management, then this design may be vulnerable to the DHCP starvation attacks described earlier.

Mitigation

If the security zones are small enough, use port security to help mitigate CAM table overflow vulnerabilities and MAC spoofing vulnerability. Additionally, mitigation of VLAN hopping can be accomplished by following the VLAN best practices outlined within this lesson. If necessary, deploy 802.1x authentication to prevent unauthorized access to each of the security zones by an attacker who may physically connect to a switch in the design. Another possible mitigation method would be to add a firewall within the data center design and integrate it into one or more of the switches, similar to the technique employed in the case 6 design. The firewall enforces additional Layer 3 traffic segregation between the various user groups. As with the previous cases, the switches must be managed as securely as possible and tested on a regular basis.

Best Practices

This topic recommends Layer 2 best practices.

Best Practices

Cisco.com

- **Manage switches as securely as possible. Use SSH if possible, or an out-of-band management system. Avoid the use of clear text management protocols such as Telnet or SNMP Version 1.**
- **Use IP permit lists to restrict access to management ports.**
- **Selectively use SNMPv3 and treat community strings like root passwords.**
- **When SNMPv3 is used as a management protocol, restrict management access to the VLAN so that entities on untrusted networks cannot access management interfaces or protocols. Consider using DHCP snooping and IP source guard to mitigate DHCP starvation attacks.**
- **Always use a dedicated VLAN ID for all trunk ports.**
- **Avoid using VLAN 1.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-3.22

Although security attacks on networks are not new events, attacks that use Layer 2 to bypass VLAN restrictions are quickly gaining in sophistication and popularity. To mitigate the effects of these attacks as much as possible, the following precautions are recommended:

- Manage switches as securely as possible. Use SSH, if possible, or an out-of-band management system. Avoid the use of clear text management protocols such as Telnet or SNMP v1.
- Use IP permit lists to restrict access to management ports.
- Selectively use SNMP v3 and treat community strings like root passwords.
- When SNMP v3 is used as a management protocol, restrict management access to the VLAN so that entities on untrusted networks cannot access management interfaces or protocols. Consider using DHCP snooping and IP source guard to mitigate DHCP starvation attacks.
- Always use a dedicated VLAN ID for all trunk ports.
- Avoid using VLAN 1.

Best Practices (Cont.)

Cisco.com

- **Set all user ports to nontrunking mode.**
- **Deploy port security where possible for user ports.**
- **Have a plan for the ARP security issues in your network.**
- **Use VACLs to prevent rogue DHCP servers by limiting replies to DHCP clients to valid DHCP servers on the network. A more flexible approach would be to use DHCP snooping to block unauthorized DHCP servers from responding to DHCP-Request packets.**
- **Enable STP attack mitigation (BPDU guard, root guard).**
- **Use PVLANS where appropriate to further divide Layer 2 networks.**
- **Use Cisco Discovery Protocol only where appropriate.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3-23

- Set all user ports to nontrunking mode.
- Deploy port security where possible for user ports. When feasible, configure each port to associate a limited number of MAC addresses (approximately two to three). This practice will mitigate MAC flooding and other network attacks. Alternatively, deploy dynamic port security using DHCP snooping along with DAI.
- Have a plan for the Address Resolution Protocol (ARP) security issues in your network. Consider using DHCP snooping along with DAI and IP source guard to protect against MAC spoofing and IP spoofing on the network.
- Use VLAN access control lists (VACLs) to prevent rogue DHCP servers by limiting replies to DHCP clients to valid DHCP servers on the network. A more flexible approach would be to use DHCP snooping to block unauthorized DHCP servers from responding to DHCP Request packets.
- Enable STP attack mitigation (BPDU guard, root guard).
- Use PVLANS where appropriate to further divide Layer 2 networks.
- Use Cisco Discovery Protocol only where appropriate.

Best Practices (Cont.)

Cisco.com

- **Disable all unused ports and put them in an unused VLAN.**
- **Use Cisco IOS Software ACLs on IP-forwarding devices to protect Layer 2 proxy on private VLANs.**
- **Eliminate native VLANs from 802.1Q trunks.**
- **Use VTP passwords to authenticate VTP advertisements.**
- **Consider using Layer 2 port authentication such as 802.1x to authenticate clients attempting connectivity to a network.**
- **Procedures for change control and configuration analysis must be in place to ensure that changes result in a secure configuration.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-3.24

- Disable all unused ports and put them in an unused VLAN. This setup prevents network intruders from plugging into unused ports and communicating with the rest of the network.
- Use Cisco IOS software access control lists (ACLs) on IP-forwarding devices to protect Layer 2 proxy on PVLANS.
- Eliminate native VLANs from 802.1Q trunks.
- Use VTP passwords to authenticate VTP advertisements.
- Consider using Layer 2 port authentication such as 802.1x to authenticate clients attempting connectivity to a network.
- Procedures for change control and configuration analysis must be in place to ensure that changes result in a secure configuration. This practice is especially valuable in cases where several organizational groups may control the same switch, and it is even more valuable in network security deployments, where even greater care must be taken.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Three facts affect mitigation strategy techniques: the number of security zones, the number of user groups, and the number of switch devices.**
- **Layer 2 switches should be managed as securely as possible.**
- **Use SSH for command-line management.**
- **Use SNMPv3 for remote management.**
- **Use configuration audits and regular penetration testing.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-25

Summary (Cont.)

Cisco.com

- **Vulnerabilities include these:**
 - **MAC spoofing**
 - **CAM table overflow**
 - **VLAN hopping**
 - **STP attacks**
 - **PVLAN attacks**
 - **VTP attacks**
- **Mitigation techniques include these:**
 - **Port security**
 - **DHCP snooping**
 - **ARP inspection**
 - **802.1x authentication**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-3-26

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **Layer 2 Attacks include MAC spoofing, CAM overflow, ARP spoofing, and DHCP starvation. Port security, DHCP snooping, and ARP inspection are used to mitigate these types of attacks.**
- **Cisco IBNS combines several Cisco products to offer authentication, access control, and user policies to enhance network security. It is based on 802.1x and RADIUS implementations.**
- **When 802.1x is enabled, ports are authenticated before any other Layer 2 features are enabled. A RADIUS server is used to authenticate users. RADIUS keys must match on client and server.**
- **The three factors that affect mitigation strategy techniques are the number of security zones, the number of user groups, and the number of switch devices. Recommendations include secure switch management using SSH, SNMPv3, regular audits, and penetration testing.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0--3-1

This module covered Layer 2 security in some depth. Layer 2 security can be implemented to enhance the total security of a network. Layer 2 attacks were introduced, as well as mitigation techniques for these attacks. Cisco IBNS was introduced as one part of the solution to Layer 2 security. IBNS relies on 802.1x and RADIUS implementations. Configuration of 802.1x was covered, and some examples were given. Finally, Layer 2 Security best practices were covered, with several scenarios given to describe most network types and configurations.

Module 4

Cisco IOS-Based VPNs Using Cisco Pre-Shared Keys

Overview

Virtual private networks (VPNs) can be configured for various types of authentication. One such method is pre-shared keys. In this case, each client shares a common key. This module guides the learner through the process of configuring VPNs using pre-shared keys.

Module Objectives

Upon completing this module, you will be able to plan, configure, operate, and troubleshoot IPsec VPNs using Cisco routers and pre-shared keys. This ability includes being able to meet these objectives:

- Prepare the network for implementation of the required IPsec policy using pre-shared keys
- Configure the IKE policy using pre-shared keys
- Configure the IPsec policy using pre-shared keys
- Verify that the configuration is correct

Lesson 1

Preparing a Network for IPSec Configuration with Pre-Shared Keys

Overview

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. Configuration of a network to work with IPSec allows you to secure the network using IPSec standards supported by Cisco Systems. This lesson covers the preparation of a network to work with IPSec and pre-shared keys.

Objectives

Upon completing this lesson, you will be able to prepare the network for implementation of the required IPSec policy using pre-shared keys. This ability includes being able to meet these objectives:

- Define each of the four tasks in configuring IPSec encryption using IKE pre-shared keys
- Describe each of the planning steps used in defining IPSec security policy using pre-shared keys
- Determine the IKE policies between IPSec peers based on the number and location of the peers
- Determine an IPSec policy detailing IPSec algorithms and parameters
- Determine whether there are any IPSec policies already configured
- Verify connectivity between peers
- Ensure that ACLs on perimeter routers, the Cisco PIX Firewall, or other routers do not block IPSec traffic

Configuring IPsec Encryption with Pre-Shared Keys

This topic describes the configuration of IPsec using pre-shared keys.

Configuring IPsec Encryption

Cisco.com

Task 1: Prepare for ISAKMP and IPsec.

Task 2: Configure ISAKMP.

Task 3: Configure IPsec.

Task 4: Test and verify IPsec.

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4.4

The use of Internet Key Exchange (IKE) pre-shared keys for authentication of 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 lessons 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 that you wish to protect, determining details about the IPsec peers, determining the IPsec features you need, and ensuring that 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.

Planning the IKE and IPSec Policy

This topic describes steps used in preparation for using IKE and IPSec.

Task 1: Prepare for ISAKMP and IPSec

Cisco.com

Step 1: Determine ISAKMP (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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.0

Configuring IPSec encryption can be complicated if no planning is involved. 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 Internet Security Association and Key Management Protocol (ISAKMP, or IKE Phase 1) policy:** Determine the IKE policies between IPSec peers based on the number and location of the peers.
- Step 2 Determine IPSec (IKE Phase 2) 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 many other **show** commands, to check the current configuration of the router. This process is covered later in this lesson.
- Step 4 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 5 Ensure that 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 ISAKMP (IKE Phase 1) Policy

This topic describes the ISAKMP parameters and their configuration.

Step 1: Determine ISAKMP (IKE Phase 1) Policy

Cisco.com

Determine the following policy details:

- **Key distribution method**
- **Authentication method**
- **IPSec peer IP addresses and host names**
- **IKE Phase 1 policies for all peers**
 - **Encryption algorithm**
 - **Hash algorithm**
 - **IKE SA lifetime**

Goal: Minimize misconfiguration

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.6

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 certificate authority (CA) server to support scalability of IPSec peers. You must then configure 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 the IP addresses and host names of IPSec peers:** 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 that you determined. Some ISAKMP policy details include these:
 - Encryption algorithm
 - Hash algorithm
 - IKE SA lifetime

The goal of this planning step is to gather the precise data that you will need in later steps to minimize misconfiguration.

IKE Phase 1 Policy Parameters

Cisco.com

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 DH group 5
IKE SA lifetime	86,400 seconds	< 86,400 seconds

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.7

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 the policy of a remote peer.

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 that you desire and the type of IPSec peer that you will connect to.

There are five parameters to define in each IKE policy, as outlined in the figure and in this table. The figure shows the relative strength of each parameter, and the table shows the default values.

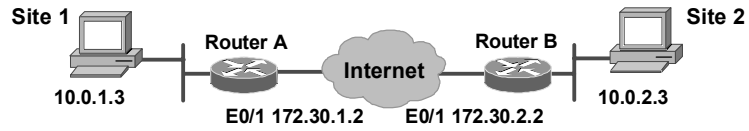
Parameter	Accepted Values	Keyword	Default
Message encryption algorithm	Data Encryption Standard (DES) Triple-DES (3DES) Advanced Encryption Standard (AES) 128, 192, 256 bits	des 3des aes	DES
Message integrity (hash) algorithm	Secure Hash Algorithm-1 (SHA-1; Hash-Based Method Authentication Code [HMAC] variant) Message Digest 5 (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 [DH] group identifier)	768-bit Diffie-Hellman 1024-bit Diffie-Hellman 1536-bit Diffie-Hellman	1 2 5	768-bit Diffie-Hellman
ISAKMP-established SA lifetime	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 that you desire and the type of IPSec peer that you will connect to. There are five parameters to define in each IKE policy, as presented in this 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 (DH group identifier)	DH group 1	DH group 2
ISAKMP-established SA lifetime	86,400 seconds	<86,400 seconds

ISAKMP Policy Example

Cisco.com



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	86,400 seconds	86,400 seconds
Peer IP address	172.30.2.2	172.30.1.2

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.8

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

This topic describes the definition of IPSec policies.

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

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.9

An IPSec policy defines a combination of IPSec parameters used during the IPSec negotiation. Planning for IPSec (IKE Phase 2) is another important step that you should complete before actually configuring IPSec on a Cisco router. Policy details to determine at this stage include these:

- **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 host 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 that you will need in later steps to minimize misconfiguration.

IPSec Transforms Supported in Cisco IOS Software

Cisco.com

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-seal       ESP transform using SEAL cipher (160 bits)
esp-sha-hmac   ESP transform using HMAC-SHA auth
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.10

Cisco IOS software supports the IPSec transforms shown in the following tables.

Transform	Description
ah-md5-hmac	Authentication Header (AH)-HMAC-MD5 transform
ah-sha-hmac	AH-HMAC-SHA transform

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 Network Address Translation (NAT) or Port Address Translation (PAT).

Transform	Description
esp-des	Encapsulating Security Payload (ESP) transform using DES cipher (56 bits)
esp-3des	ESP transform using 3DES-Encrypt-Decrypt-Encrypt (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.

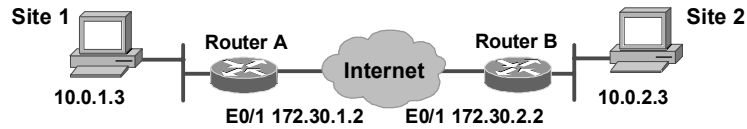
Examples of acceptable transforms that can be combined into sets are shown in the table.

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 Lempel-Ziv-STAC (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

Cisco.com



Policy	Site 1	Site 2
Transform set	ESP-DES, tunnel	ESP-DES, tunnel
Peer host name	Router B	Router A
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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4-11

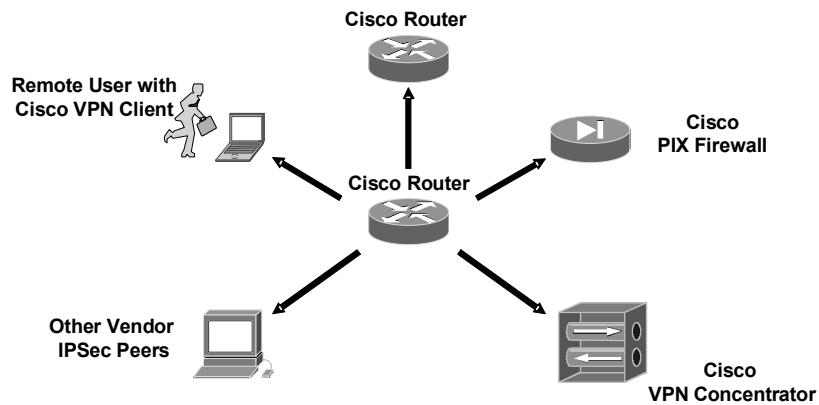
Determining network design details includes defining a more detailed IPSec policy for protecting traffic. You can then use the detailed policy to help select IPSec transform sets and modes of operation. Your IPSec policy should answer the following questions:

- What protections are required or are acceptable for the protected traffic?
- Which IPSec transforms or transform 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 how often should the SAs be renegotiated?

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.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—4-12

An important part of determining the IPSec policy is to identify the IPSec peer that the Cisco router will communicate with. The peer must support IPSec as specified in the RFCs as supported by Cisco IOS software. Many different types of peers are possible. Before configuration, identify all the potential peers and their virtual private network (VPN) capabilities. Possible peers include, but are not limited to the following:

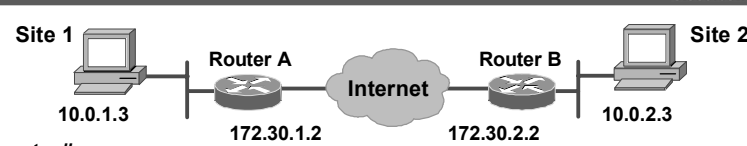
- Other Cisco routers
- The Cisco PIX Firewall
- The Cisco VPN Client
- The Cisco VPN Concentrator
- Other vendor IPSec products that conform to IPSec RFCs

Step 3—Check the Current Configuration

This topic describes how to validate your IPSec configuration.

Step 3: Check Current Configuration

Cisco.com



```
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
```

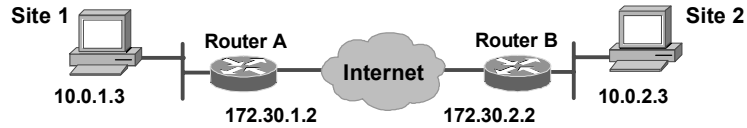
© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-13

You should check the current Cisco router configuration to see if there are any IPSec policies already configured that are useful for, or may interfere with, the IPSec policies that 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 whether any IKE policies have previously been configured by 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.)

Cisco.com



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, }
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4-14

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 that you are trying to configure.

Step 3: Check Current Configuration (Cont.)

Cisco.com



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, },
```

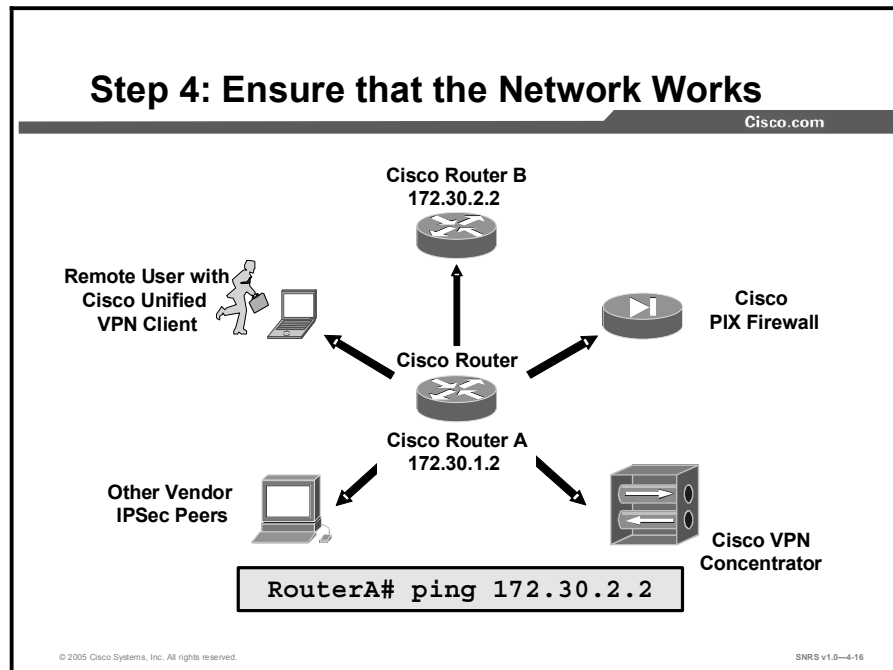
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4-15

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 That the Network Works Without Encryption

This topic describes how to check for network connectivity before applying encryption.



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. Although a successful Internet Control Message Protocol (ICMP) echo (ping) will verify basic connectivity between peers, you should ensure that the network works with any other protocols or ports that 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

This topic covers commands used to check ACLs for IPsec compatibility.

Step 5: Ensure that ACLs Are Compatible with IPsec

Cisco.com

```
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**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-17

You will need to ensure that existing ACLs on perimeter routers, the Cisco 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, ESP, and 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 completing the following steps:

- Step 1** Examine the current ACL configuration at the perimeter router and determine whether 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 that 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 **esp** equals the ESP protocol (number 50), the keyword **ahp** equals the AH protocol (number 51), and the keyword **isakmp** equals UDP port 500.

---

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Tasks for configuring IPSec include the following:**
  - Determine IKE Phase 1 and 2 policy
  - Checking the current configuration
  - Ensuring that the network works without encryption
  - Ensure that ACLs are compatible with IPSec
- **IKE Phase 1 parameters include the following:**
  - Encryption algorithm
  - Hash algorithm
  - Authentication method
  - Key distribution method
  - IKE SA lifetime

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-18

## Summary (Cont.)

Cisco.com

- **Encryption algorithms include DES, 3DES, and AES.**
- **Hash algorithms include SHA and MD5.**
- **Peer authentication methods include pre-shared key, RSA encrypted nonces, and RSA signatures.**
- **Key exchange methods are 768-bit Diffie-Hellman or 1024-bit Diffie-Hellman.**
- **SA lifetimes are expressed in seconds.**
- **Transforms supported include ah-md5-hmac, ah-sha-hmac, esp-des, esp-3des, esp-aes, esp-md5-hmac, esp-sha-hmac, and esp-null.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-19

## Lesson 2

---

# Configuring Internet Key Exchange with Pre-Shared Keys

---

## Overview

Internet Key Exchange (IKE) automatically negotiates IPsec security associations (SAs) and enables IPsec secure communications without costly manual preconfiguration. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations. This lesson covers configuring IPsec using IKE and the configuration of IKE with pre-shared keys.

## Objectives

Upon completing this lesson, you will be able to configure the IKE policy using pre-shared keys. This ability includes being able to meet these objectives:

- Describe each of the steps used in configuring the IKE policy using pre-shared keys
- Enable or disable ISAKMP
- Create ISAKMP policies
- Configure pre-shared keys
- Verify the ISAKMP configuration

# Configuring the IKE Policy

This topic describes the steps involved in configuring IKE policies.

## Configure ISAKMP

Cisco.com

**Step 1: Enable or disable ISAKMP.**  
`crypto isakmp enable`

**Step 2: Create ISAKMP policies.**  
`crypto isakmp policy`

**Step 3: Configure pre-shared keys.**  
`crypto isakmp key`

**Step 4: Verify the ISAKMP configuration.**  
`show crypto isakmp policy`

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.3

Configuring IKE policies involves the following:

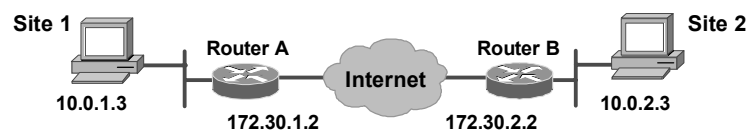
- Enabling or disabling ISAKMP globally
- Creating ISAKMP policies
- Configuring pre-shared keys
- Verifying ISAKMP configuration

# Step 1—Enable or Disable ISAKMP

This topic describes how to enable or disable ISAKMP.

## Step 1: Enable or Disable ISAKMP

Cisco.com



```
router(config)#
[no] crypto isakmp enable
```

```
RouterA(config)# no crypto isakmp enable
RouterA(config)# crypto isakmp enable
```

- Globally enables or disables ISAKMP at your router.
- ISAKMP is enabled by default.
- ISAKMP is enabled globally for all interfaces at the router.
- Use the **no** form of the command to disable ISAKMP.
- An ACL can be used to block ISAKMP on a particular interface.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.4

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but it is enabled globally for all interfaces at the router.

If you do not want IKE to be used with your IPSec implementation, you can disable it at all IPSec peers.

If you disable IKE, you will have to make these concessions at the peers:

- You must manually specify all the IPSec SAs in the crypto maps at all peers.
- The IPSec SAs of the peers will never time out for a given IPSec session.
- During IPSec sessions between the peers, the encryption keys will never change.
- Antireplay services will not be available between the peers.
- Certificate authority (CA) support cannot be used.

To disable or enable IKE, use one of the commands shown in the table in global configuration mode.

| Command                                        | Purpose      |
|------------------------------------------------|--------------|
| Router(config)# <b>no crypto isakmp enable</b> | Disables IKE |
| Router(config)# <b>crypto isakmp enable</b>    | Enables IKE  |

---

**Note** Internet Security Association and Key Management Protocol (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 (DoS) attacks by using an access control list (ACL) statement that blocks UDP port 500 on the interfaces.

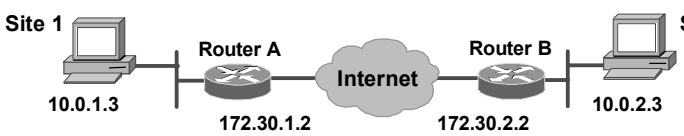
---

## Step 2—Create IKE Policies

This topic describes the process of creating IKE policies.

### Step 2: Create ISAKMP Policies

Cisco.com



```
graph LR
 S1[Site 1
10.0.1.3] --- RA[Router A
172.30.1.2]
 RA --- I((Internet))
 I --- RB[Router B
172.30.2.2]
 RB --- S2[Site 2
10.0.2.3]
```

```
router(config)#
crypto isakmp policy priority
```

- Defines an ISAKMP policy, which is a set of parameters used during IKE negotiation
- Invokes the config-isakmp command mode

```
RouterA(config)# crypto isakmp policy 110
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-5

You must create IKE policies at each peer. An IKE policy defines a combination of security parameters to be used during the IKE negotiation.

### Why Do You Need to Create These Policies?

IKE negotiations must be protected, so each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated.

After the two peers agree upon a policy, the security parameters of the policy are identified by a security association established at each peer, and these security associations 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 the policy of a remote peer.

## Parameters Defined in a Policy

There are five parameters to define in each IKE policy, as shown in the table.

| Parameter                            | Accepted Values                                                                                                                   | Keyword                                                       | Default Value                     |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------|
| Encryption algorithm                 | 56-bit Data Encryption Standard-Cipher Block Chaining (DES-CBC)<br><br>168-bit DES                                                | <b>des</b><br><br><b>3des</b>                                 | 56-bit DES-CBC<br><br>168-bit DES |
| Hash algorithm                       | Secure Hash Algorithm-1 (SHA-1; Hash-Based Method Authentication Code [HMAC] variant)<br><br>Message Digest 5 (MD5; HMAC variant) | <b>sha</b><br><br><b>md5</b>                                  | SHA-1                             |
| Authentication method                | RSA signatures<br><br>RSA encrypted nonces<br><br>Pre-shared keys                                                                 | <b>rsa-sig</b><br><br><b>rsa-encr</b><br><br><b>pre-share</b> | RSA signatures                    |
| Diffie-Hellman (DH) group identifier | 768-bit DH<br><br>1024-bit DH<br><br>1536-bit DH                                                                                  | <b>1</b><br><br><b>2</b><br><br><b>5</b>                      | 768-bit DH                        |
| Lifetime of the SA                   | Any number of seconds                                                                                                             |                                                               | 86,400 seconds (one day)          |

These parameters apply to the IKE negotiations when the IKE SA is established.

You can create multiple IKE policies, each with a different combination of parameter values. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).

You can configure multiple policies on each peer—but at least one of these policies must contain exactly the same encryption, hash, authentication, and DH parameter values as one of the policies on the remote peer.

If you do not configure any policies, your router will use the default policy, which is always set to the lowest priority and which contains the default value of each parameter.



## Create ISAKMP Policies with the `crypto isakmp` Command

Cisco.com

**Policy 110**  
DES  
MD5  
Pre-Share  
86400

```
router(config)#
crypto isakmp policy priority
```

- Defines the parameters within the ISAKMP 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
```

© 2005 Cisco Systems, Inc. All rights reserved. SHRS v1.0-4.6

To configure a policy, use the commands shown in the table, beginning in global configuration mode.

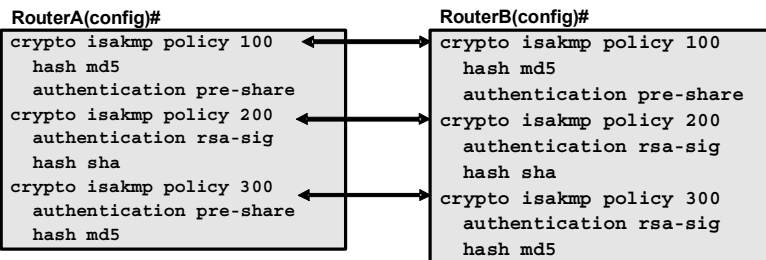
|               | Command                                                                             | Purpose                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <code>crypto isakmp policy priority</code>                          | Identifies the policy to create. (Each policy is uniquely identified by the priority number that you assign.)<br><br>(This command puts you into the config-isakmp command mode.) |
| <b>Step 2</b> | Router(config-isakmp)# <code>encryption {des   3des}</code>                         | Specifies the encryption algorithm.                                                                                                                                               |
| <b>Step 3</b> | Router(config-isakmp)# <code>hash {sha   md5}</code>                                | Specifies the hash algorithm.                                                                                                                                                     |
| <b>Step 4</b> | Router(config-isakmp)# <code>authentication {rsa-sig   rsa-encr   pre-share}</code> | Specifies the authentication method.                                                                                                                                              |
| <b>Step 5</b> | Router(config-isakmp)# <code>group {1   2   5}</code>                               | Specifies the DH group identifier.                                                                                                                                                |
| <b>Step 6</b> | Router(config-isakmp)# <code>lifetime seconds</code>                                | Specifies the lifetime of the SA.                                                                                                                                                 |
| <b>Step 7</b> | Router(config-isakmp)# <code>exit</code>                                            | Exits the config-isakmp command mode.                                                                                                                                             |
| <b>Step 8</b> | Router(config)# <code>exit</code>                                                   | Exits the global configuration mode.                                                                                                                                              |
| <b>Step 9</b> | Router# <code>show crypto isakmp policy</code>                                      | (Optional) Displays all existing IKE policies.<br><br>(Use this command in EXEC mode.)                                                                                            |

If you do not specify a value for a parameter, the default value is assigned.

**Note** The default policy and the default values for configured policies do not show up in the configuration when you issue a **show running** command. Instead, to see the default policy and any default values within configured policies, use the **show crypto isakmp policy** command.

## ISAKMP Policy Negotiation

Cisco.com



- The first two policies in each router can be successfully negotiated, but the last one cannot.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.7

ISAKMP peers negotiate acceptable ISAKMP policies before agreeing upon the SA to be used for IPSec.

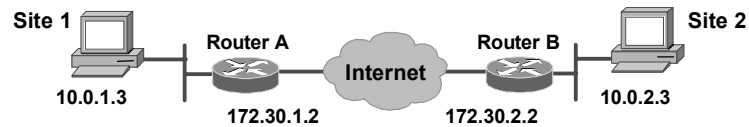
When the ISAKMP negotiation begins in IKE Phase 1 main mode, ISAKMP looks for an ISAKMP policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match with its policies. The remote peer looks for a match by comparing its own highest-priority policy against the policies received from its other peer 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 DH parameter values, and when the remote peer 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 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 2 quick mode.

## Configure ISAKMP Identity

Cisco.com



router(config)#

```
crypto isakmp identity {address | hostname}
```

- Defines whether ISAKMP identity is done by IP address or host name
- Use consistently across ISAKMP peers

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—4-0

## Setting ISAKMP Identity

You should set the ISAKMP identity for each peer that uses pre-shared keys in an IKE policy.

When two peers use IKE to establish IPsec SAs, each peer sends its identity to the remote peer. Each peer sends either its host name or its IP address, depending on how you have set the ISAKMP identity of the router.

By default, the ISAKMP identity of a peer is the IP address of the peer. If appropriate, you could change the identity to be the peer host name instead. As a general rule, set the identities of all peers the same way—either all peers should use their IP addresses or all peers should use their host names. If some peers use their host names and some peers use their IP addresses to identify themselves to each other, IKE negotiations could fail if the identity of a remote peer is not recognized and a Domain Name System (DNS) lookup is unable to resolve the identity.

To set the ISAKMP identity of a peer, use the commands shown in the table in global configuration mode.

|               | Command                                                                | Purpose                                                                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>crypto isakmp identity {address   hostname}</b>     | At the local peer: Specifies the peer ISAKMP identity by IP address or by host name.                                                                                                                                                                                           |
| <b>Step 2</b> | Router(config)# <b>ip host hostname address1 [address2...address8]</b> | At all remote peers: If the local peer ISAKMP identity was specified using a host name, maps the host name of the peer to its IP address or addresses at all the remote peers. (This step might be unnecessary if the host name or address is already mapped in a DNS server.) |

Remember to repeat these tasks at each peer that uses pre-shared keys in an IKE policy.

## Step 3—Configure Pre-Shared Keys

This topic describes how to configure IKE to work with pre-shared keys.

### Step 3: Configure Pre-Shared Keys

Cisco.com

```
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 IP address or host name can be used.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.9

To configure pre-shared keys, complete these steps at each peer that uses pre-shared keys in an IKE policy:

- Step 1** Set the ISAKMP identity of each peer. The identity of each peer should be set to either its host name or its IP address. By default, a peer identity is set to its IP address.
- Step 2** Specify the pre-shared keys at each peer. Note that 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.

To specify pre-shared keys at a peer, use the commands shown in the table in global configuration mode.

|               | Command                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                       |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>crypto isakmp key</b> <i>keystring</i><br><b>address</b> <i>peer-address</i><br><br>or<br>Router(config)# <b>crypto isakmp key</b> <i>keystring</i><br><b>hostname</b> <i>peer-hostname</i> | At the local peer: Specifies the pre-shared key to be used with a particular remote peer.<br><br>If the remote peer specified its ISAKMP identity with an address, use the <b>address</b> keyword in this step; otherwise use the <b>hostname</b> keyword in this step.                                                       |
| <b>Step 2</b> | Router(config)# <b>crypto isakmp key</b> <i>keystring</i><br><b>address</b> <i>peer-address</i><br><br>or<br>Router(config)# <b>crypto isakmp key</b> <i>keystring</i><br><b>hostname</b> <i>peer-hostname</i> | At the remote peer: Specifies the pre-shared key to be used with the local peer. This is the same key that you just specified at the local peer.<br><br>If the local peer specified its ISAKMP identity with an address, use the <b>address</b> keyword in this step; otherwise use the <b>hostname</b> keyword in this step. |
| <b>Step 3</b> | Repeat Steps 1 and 2 for each remote peer.                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                               |

The following example configures ISAKMP and pre-shared keys for two routers (Routers A and B). Note that the key string “cisco1234” matches. The address identity method is specified. The ISAKMP policies are compatible. Default values do not have to be configured.

**Router A**

```
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
```

**Router B**

```
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 ISAKMP Configuration

This topic describes how to verify your IKE configurations.

## Step 4: Verify the ISAKMP Configuration

Cisco.com

```
graph LR
 S1[Site 1
10.0.1.3] --- RA[Router A]
 RA --- I((Internet))
 I --- RB[Router B]
 RB --- S2[Site 2
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 ISAKMP policies**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4-10

You can use the **show crypto isakmp policy** command to display configured and default policies. The resulting ISAKMP policy for Router A, as shown in the figure, is as follows (the Router B 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
```

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **ISAKMP policy configuration includes the following:**
  - Enabling or disabling ISAKMP
  - Creating ISAKMP policies
  - Configuring pre-shared keys
  - Verifying the ISAKMP configuration
- **ISAKMP is enabled by default.**
- **You must create ISAKMP policies at each peer.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-11

## Summary (Cont.)

Cisco.com

- **The policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated.**
- **Each peer sends either its host name or its IP address.**
- **Pre-shared keys must match at both hosts.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-12





## Lesson 3

---

# Configuring IPsec

---

## Overview

This lesson describes how to configure IPsec, which is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco Systems routers. This lesson allows you to configure IPsec on a Cisco router. It covers the configuration of IPsec policies to be used with pre-shared keys and how to configure IPsec security settings.

## Objectives

Upon completing this lesson, you will be able to configure IPsec using pre-shared keys. This ability includes being able to meet these objectives:

- Describe each of the steps used in configuring the IPsec policy using pre-shared keys
- Configure transform set suites
- Configure global IPsec SA lifetimes
- Create crypto ACLs
- Create crypto maps
- Apply crypto maps to interfaces

# Configuring IPSec

This topic describes the process of configuring IPSEC for use with pre-shared keys.

## Configure IPSec

Cisco.com

**Step 1: Configure transform sets.**

```
crypto ipsec transform-set
```

**Step 2: Configure global IPSec SA lifetimes.**

```
crypto ipsec security-association
lifetime
```

**Step 3: Create crypto ACLs.**

```
access-list
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.3

The general tasks and commands used to configure IPSec encryption on Cisco routers are summarized as described in these steps. 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 (SA) lifetimes with the **crypto ipsec security-association lifetime** command.
- Step 3**    Configure crypto access control lists (ACLs) with the **access-list** command.

## Configure IPSec (Cont.)

Cisco.com

### Step 4: Create crypto maps.

```
crypto map
```

### Step 5: Apply crypto maps to interfaces.

```
interface serial0
crypto map
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.4

- 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.

# Step 1—Configure Transform Sets

This topic describes the first major step in configuring Cisco IOS IPsec, which is to use the IPsec security policy to define a transform set.

## Configure Transform Sets

Cisco.com

```
router(config)#
crypto ipsec transform-set transform-set-name
transform1 [transform2 [transform3]]
router (cfg-crypto-trans) #
```

```
RouterA(config)# crypto ipsec transform-set MINE
esp-des esp-md5-hmac
```

- A transform set is a combination of IPsec transforms that enact a security policy for traffic.
- Sets are limited to up to one AH and up to two ESP transforms.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.6

A transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPsec SA negotiation to protect the data flows specified by the ACL of that crypto map entry.

During IPsec SA negotiations with Internet Key Exchange (IKE), 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 to be applied to the protected traffic as part of the IPsec SAs of both peers.

With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.

If you change a transform set definition, the change is applied only to crypto map entries that reference the transform set. The change will not be applied to existing SAs, but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

To define a transform set, use the commands shown in the table, starting in global configuration mode.

|               | Command                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>crypto ipsec transform-set transform-set-name transform1</b><br>[transform2 [transform3]] | Defines a transform set.<br><br>There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the <b>crypto ipsec transform-set</b> command.<br><br>This command puts you into the crypto transform configuration mode. |
| <b>Step 2</b> | Router(cfg-crypto-tran)# <b>mode [tunnel   transport]</b>                                                    | (Optional) Changes the mode associated with the transform set. The transport mode setting is applicable only to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. The default mode is tunnel.                                              |
| <b>Step 3</b> | Router(cfg-crypto-tran)# <b>exit</b>                                                                         | Exits the crypto transform configuration mode.                                                                                                                                                                                                                                                             |

The table shows the allowed transform combinations.

| Transform Type                                                                   | Transform                                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Header (AH) transform<br>(Choose up to one.)                      | ah-md5-hmac<br>ah-sha-hmac                                                                   | AH with the Message Digest 5 (MD5; Hash-Based Method Authentication Code [HMAC] variant) authentication algorithm<br><br>AH with the Secure Hash Algorithm (SHA; HMAC variant) authentication algorithm                                                                                                                                                                                                        |
| Encapsulating Security Payload (ESP) encryption transform<br>(Choose up to one.) | esp-des<br>esp-3des<br><br>esp-null<br>esp-aes<br><br>esp-aes 192<br>esp-aes 256<br>esp-seal | ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm<br>ESP with the 168-bit DES encryption algorithm<br>Triple-DES (3DES)<br>Null encryption algorithm<br>ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm<br>ESP with the 192-bit AES encryption algorithm<br>ESP with the 256-bit AES encryption algorithm<br>ESP with the 160-bit SEAL encryption algorithm |
| ESP authentication transform<br>(Choose up to one.)                              | esp-md5-hmac<br>esp-sha-hmac                                                                 | ESP with the MD5 (HMAC variant) authentication algorithm<br><br>ESP with the SHA (HMAC variant) authentication algorithm                                                                                                                                                                                                                                                                                       |
| IP compression transform<br>(Choose up to one.)                                  | comp-lzs                                                                                     | IP compression with the Lempel-Ziv-STAC (LZS) algorithm                                                                                                                                                                                                                                                                                                                                                        |

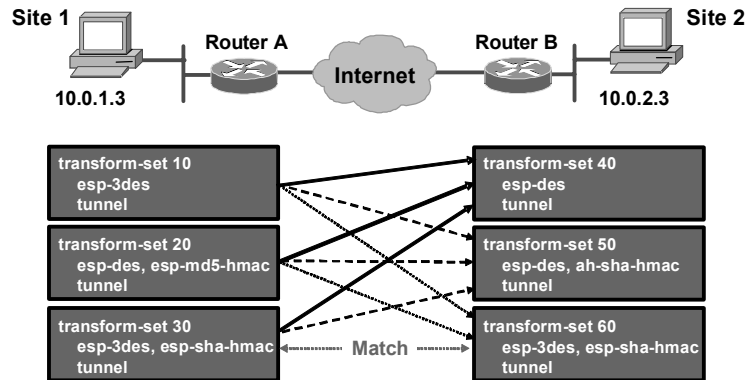
## Edit Transform Sets

Complete 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 the global configuration.
- Step 3** Re-enter 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 that it works properly.

## Transform Set Negotiation

Cisco.com



- Transform sets are negotiated during IKE Phase 2.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.6

Transform sets are negotiated during quick mode in IKE Phase 2 using the transform sets that you previously configured. You can configure multiple transform sets, and 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 the ACL of that crypto map entry.

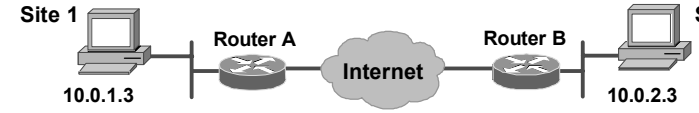
During the negotiation, the peers search for a transform set that is the same at both peers, as illustrated in the figure. Each of the Router A transform sets is compared against each of the Router B transform sets in succession. Router A transform sets 10, 20, and 30 are compared with Router B transform set 40. The result is no match. All of the Router A transform sets are then compared against the Router B transform sets. Ultimately, Router A transform set 30 matches Router B transform set 60. When such a transform set is found, it is selected and is applied to the protected traffic as part of the IPSec SAs of both peers. IPSec peers agree on one transform proposal per SA (unidirectional).

## Step 2—Configure Global IPsec SA Lifetimes

This topic describes how to configure global SA lifetimes.

### crypto ipsec security-association lifetime Command

Cisco.com



```
graph LR
 S1[Site 1
10.0.1.3] --- RA[Router A]
 RA --- I((Internet))
 I --- RB[Router B]
 RB --- S2[Site 2
10.0.2.3]
```

```
router(config)#
crypto ipsec security-association lifetime
 {seconds seconds | kilobytes kilobytes}

RouterA(config)# crypto ipsec security-association
lifetime seconds 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.

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4.7

You can change the global lifetime values that are used when negotiating new IPsec SAs. (These global lifetime values can be overridden for a particular crypto map entry).

These lifetimes only apply to SAs established via IKE. Manually established SAs do not expire.

There are two lifetimes: a timed lifetime and a traffic-volume lifetime. An SA expires after the first of these lifetimes is reached. The default lifetimes are 3600 seconds (one hour) and 4,608,000 kilobytes (10 Mbps for one hour per second for one hour).

If you change a global lifetime, the new lifetime value will not be applied to existing SAs, but will be used in the negotiation of subsequently established SAs. If you wish to use the new values immediately, you can clear all or part of the SA database. Refer to the **clear crypto sa** command for more details.

IPsec SAs use one or more shared secret keys. These keys and their SAs time out together.



The command syntax is as follows:

```
crypto ipsec security-association lifetime seconds seconds
```

- Changes the global timed lifetime for IPsec SAs. This command causes the SA to time out after the specified number of seconds have passed.

or

```
crypto ipsec security-association lifetime kilobytes kilobytes
```

- Changes the global traffic-volume lifetime for IPsec SAs. This command causes the SA to time out after the specified amount of traffic (in kilobytes) has passed through the IPsec “tunnel” using the SA.

## How These Lifetimes Work

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new SAs, it will specify its global lifetime values in the request to the peer; it will use this value as the lifetime of the new SAs. When the router receives a negotiation request from the peer, it will use the smaller of either the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new SAs.

The SA (and corresponding keys) will expire according to whichever comes sooner, either after the number of seconds configured has passed (specified by the **seconds** keyword) or after the amount of traffic in kilobytes configured has passed (specified by the **kilobytes** keyword). Security associations that are established manually (via a crypto map entry marked using the **ipsec-manual** option) have an infinite lifetime.

A new SA is negotiated *before* the lifetime threshold of the existing SA is reached, to ensure that a new SA is ready for use when the old one expires. The new SA is negotiated either 30 seconds before the timed lifetime expires or when the volume of traffic through the tunnel reaches 256 kilobytes less than the **traffic-volume** lifetime (whichever comes first).

If no traffic has passed through the tunnel during the entire life of the SA, a new SA is not negotiated when the lifetime expires. Instead, a new SA will be negotiated only when IPsec sees another packet that should be protected.

## 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.**

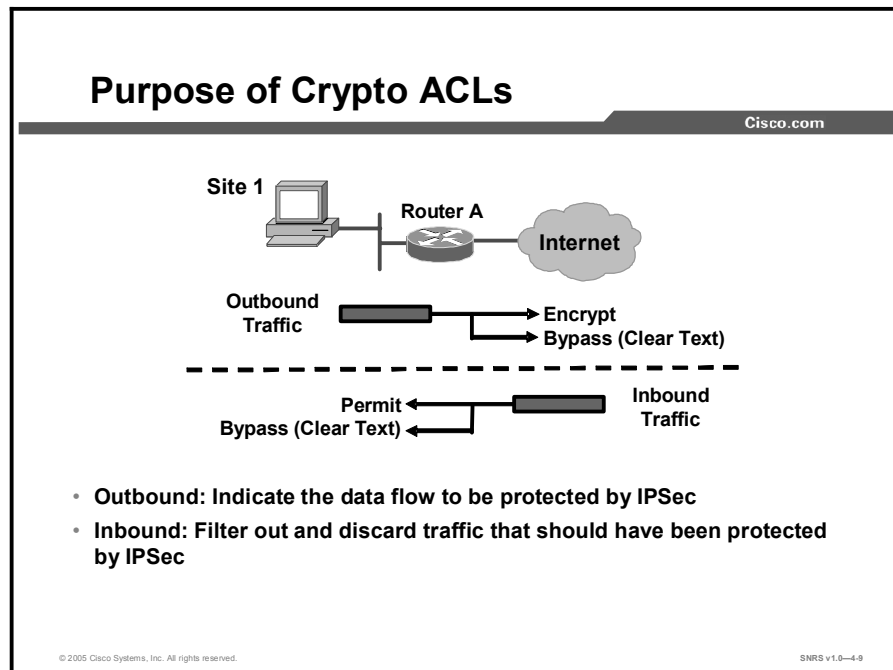
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.3

The figure shows an example of a 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 describes how to configure crypto ACLs.



Crypto ACLs are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. (These ACLs are not the same as regular ACLs, which determine which traffic to forward or block at an interface.) For example, ACLs can be created to protect all IP traffic between subnet A and subnet Y or Telnet traffic between host A and host B.

The ACLs themselves are not specific to IPSec. It is the crypto map entry referencing the specific ACL that defines whether IPSec processing is applied to the traffic matching a **permit** statement in the ACL.

Crypto ACLs associated with IPSec crypto map entries have four primary functions:

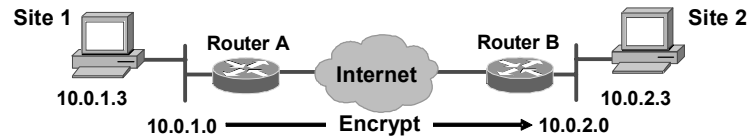
- Select outbound traffic to be protected by IPSec (permit equals protect).
- Indicate the data flow to be protected by the new SAs (specified by a single **permit** entry) when initiating negotiations for IPSec SAs.
- Process inbound traffic to filter out and discard traffic that should have been protected by IPSec.
- Determine whether or not to accept requests for IPSec SAs on behalf of the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is done only for **ipsec-isakmp** crypto map entries.) To be accepted, if the peer initiates the IPSec negotiation, it must specify a data flow that is permitted by a crypto ACL associated with an **ipsec-isakmp** crypto map entry.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to 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.

Later, you will associate the crypto ACLs to particular interfaces when you configure and apply crypto map sets to the interfaces.

## Extended IP ACLs for Crypto ACLs

Cisco.com



router(config)#

```
access-list access-list-number [dynamic dynamic-name
 [timeout minutes]] {deny | permit} protocol source
 source-wildcard destination destination-wildcard
 [precedence precedence] [tos tos] [log]
```

```
RouterA(config)# access-list 110 permit tcp 10.0.1.0
 0.0.0.255 10.0.2.0 0.0.0.255
```

- Define which IP traffic will be protected by crypto
- Permit = encrypt, deny = do not encrypt

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—4-10

To create crypto ACLs, use the following command in global configuration mode:

```
Router(config)# access-list access-list-number {deny | permit}
 protocol source-wildcard destination destination-
 wildcard [log]
```

- Specifies conditions to determine which IP packets will be protected.

**Note** It is recommended that you configure “mirror image” crypto ACLs for use by IPsec and that you avoid using the **any** keyword.

or

```
Router(config)# ip access-list extended name
```

- Follow with **permit** and **deny** statements as appropriate.

| Command                       | Description                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>permit</b>                 | Causes all IP traffic that matches the specified conditions to be encrypted using the policy described by the corresponding crypto map entry |
| <b>deny</b>                   | Instructs the router to route traffic in the clear                                                                                           |
| <i>source and destination</i> | Networks, subnets, or hosts                                                                                                                  |
| <i>protocol</i>               | Indicates which IP packet type or types 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.

---

**Caution** It is recommended that you avoid using the **any** keyword to specify source or destination addresses. The **permit any any** statement is strongly discouraged, because 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, Network Time Protocol (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.

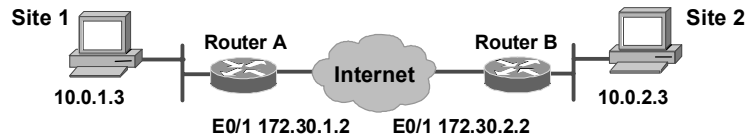
In a later step, you will associate a crypto ACL to a crypto map, which in turn is assigned to a specific interface.

## Defining Mirror-Image Crypto ACLs at Each IPsec Peer

It is recommended that for every crypto ACL specified for a static crypto map entry that you define at the local peer, you define a mirror-image crypto ACL at the remote peer. This practice ensures that traffic that has IPsec protection applied locally can be processed correctly at the remote peer. (The crypto map entries themselves must also support common transforms and must refer to the other system as a peer.)

## Configure Symmetrical Peer Crypto ACLs

Cisco.com



```
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.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4.11

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 criteria of the ACL are 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 the Router A 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 Router A 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 Router A 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
- 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

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—4-12

Crypto map entries created for IPsec set up SA parameters, tying together the various parts configured for IPsec, including these:

- Which traffic should be protected by IPsec (per a crypto ACL)
- 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 entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. Later, you will apply these crypto map sets to interfaces; then, all IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a SA is negotiated with the remote peer according to the parameters included in the crypto map entry. Otherwise, if the crypto map entry specifies the use of manual SAs, a SA should have already been established via configuration. (If a dynamic crypto map entry sees outbound traffic that should be protected and no SA exists, the packet is dropped.)



The policy described in the crypto map entries is used during the negotiation of SAs. If the local router initiates the negotiation, it will use the policy specified in the static crypto map entries to create the offer to be sent to the specified IPSec peer. If the IPSec peer initiates the negotiation, the local router will check the policy from the static crypto map entries, as well as any referenced dynamic crypto map entries to decide whether to accept or reject the request (offer) from the peer.

For IPSec to succeed between two IPSec peers, the crypto map entries of both peers must contain compatible configuration statements.

When two peers try to establish a SA, they must each have at least one crypto map entry that is compatible with one of the crypto map entries of the other peer. For two crypto map entries to be compatible, they must at least meet the following criteria:

- The crypto map entries must contain compatible crypto ACLs (for example, mirror-image ACLs). In the case where the responding peer is using dynamic crypto maps, the entries in the local crypto ACL must be permitted by the peer crypto ACL.
- The crypto map entries must each identify the other peer (unless the responding peer is using dynamic crypto maps).
- The crypto map entries must have at least one transform set in common.

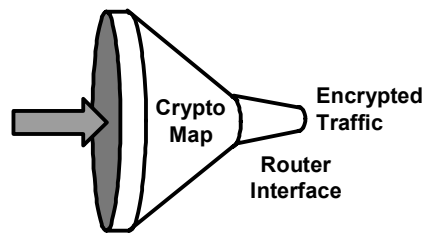
## Crypto Map Parameters

Cisco.com



### Crypto maps define the following:

- The ACL to be used
- Remote VPN peers
- Transform set to be used
- Key management method
- SA lifetimes



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4-13

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 sequence number, 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 SAs, 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

Cisco.com



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.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4-14

You must use the **crypto map** global configuration command to create or modify a crypto map entry and enter 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, having 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 ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]
```

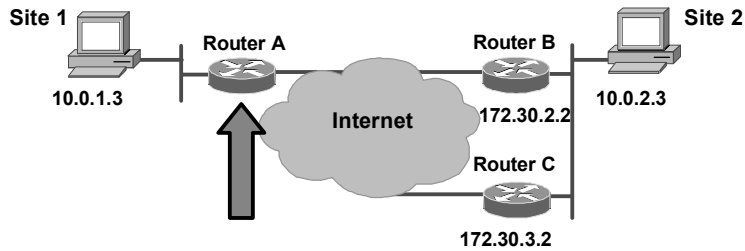
```
no crypto map map-name [seq-num]
```

A description of each is as follows:

- **map-name**: The name that you assign to the crypto map set.
- **seq-num**: The number that you assign to the crypto map entry.
- **ipsec-manual**: Indicates that Internet Security Association and Key Management Protocol (ISAKMP) will not be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry.
- **ipsec-isakmp**: Indicates that ISAKMP will be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry.
- **dynamic**: (Optional) Specifies that this crypto map entry references a pre-existing 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.

## Example Crypto Map Commands

Cisco.com



```
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
seconds 86400
```

- Multiple peers can be specified for redundancy.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-4-15

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                                                                                                                                                                                                              |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>set</b>                                   | Used with the <b>peer</b> , <b>pfs</b> , <b>transform-set</b> , and <b>security-association</b> commands.                                                                                                                |
| <b>peer</b> [hostname   ip-address]          | Specifies the allowed IPsec peer by IP address or host name.                                                                                                                                                             |
| <b>pfs</b> [group1   group2   group5]        | Specifies DH group 1, group 2, or group 5.                                                                                                                                                                               |
| <b>transform-set</b> [set_name(s)]           | Specifies a 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. |
| <b>security-association lifetime</b>         | Sets SA lifetime parameters in seconds or kilobytes.                                                                                                                                                                     |
| <b>match address</b> [access-list-id   name] | Identifies the extended ACL by its name or number. The value should match the <i>access-list-number</i> or <i>name</i> argument of a previously defined IP-extended ACL being matched.                                   |
| <b>no</b>                                    | Deletes commands entered with the <b>set</b> command.                                                                                                                                                                    |
| <b>exit</b>                                  | 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 SAs established by that particular crypto map entry are only for a single data flow. To be able to support multiple manually established SAs 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

This topic describes how to apply the crypto map set to an interface. This is the last step in configuring IPsec.

### Applying Crypto Maps to Interfaces

Cisco.com

```

router(config-if)#
crypto map map-name
RouterA(config)# interface ethernet0/1
RouterA(config-if)# crypto map MYMAP

```

- Applies the crypto map to outgoing interface
- Activates the IPsec policy

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0-4-16

You need to apply a crypto map set to each interface through which IPsec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface traffic against the crypto map set and to use the specified policy during connection or SA negotiation on behalf of traffic to be encrypted.

To apply a crypto map set to an interface, use the command shown in the table in interface configuration mode.

| Command                                              | Purpose                                  |
|------------------------------------------------------|------------------------------------------|
| Router(config-if)# <b>crypto map</b> <i>map-name</i> | Applies a crypto map set to an interface |

For redundancy, you could apply the same crypto map set to more than one interface. The default behavior is as follows:

- Each interface has its own piece of the SA database.
- The IP address of the local interface is used as the local address for IPsec traffic originating from or destined to that interface.

If you apply the same crypto map set to multiple interfaces for redundancy purposes, you need to specify an identifying interface. This action has the following effects:

- The per-interface portion of the IPsec SA database is established one time and shared for traffic through all the interfaces that share the same crypto map.
- The IP address of the identifying interface is used as the local address for IPsec traffic originating from or destined to the interfaces sharing the same crypto map set.

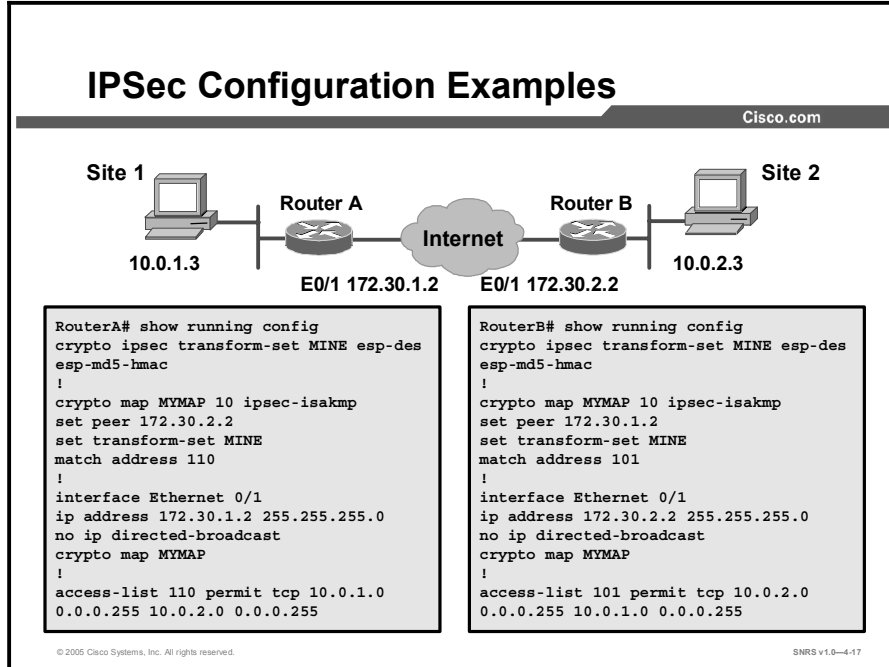
One suggestion is to use a loopback interface as the identifying interface.

To specify redundant interfaces and name an identifying interface, use the command shown in the table in global configuration mode.

| Command                                                                                    | Purpose                                                                                  |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Router(config)# <b>crypto map</b> <i>map-name</i> <b>local-address</b> <i>interface-id</i> | Permits redundant interfaces to share the same crypto map, using the same local identity |

# IPSec Configuration Example

This topic gives an example of an IPSec configuration.



Consider the configuration example for Router A and Router B in the figure and the examples that follow. The examples are concatenated to show only 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 esp-md5-hmac
!
!
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 esp-md5-hmac
!

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

```

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Configuring IPSec includes configuration of the following:**
  - Transform sets
  - Global IPSec SA lifetimes
  - Crypto ACLs
  - Crypto maps
  - Applying maps to interfaces
- **A transform set represents a certain combination of security protocols and algorithms.**
- **There are two lifetimes:**
  - A timed lifetime
  - A traffic-volume lifetime

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-18

## Summary (Cont.)

Cisco.com

- **Crypto ACLs are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto.**
- **For every crypto ACL specified for a static crypto map entry that you define at the local peer, you define a mirror image ACL at the remote peer.**
- **Crypto map entries created for IPSec set up SA parameters, tying together the various parts configured for IPSec.**
- **You need to apply a crypto map set to each interface through which IPSec traffic will flow.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-19

## Lesson 4

---

# Testing and Verifying IPsec Configuration

---

## Overview

The final task is to test and verify your IPsec configuration. This lesson covers the process for verifying proper configuration of Cisco IOS-based virtual private networks (VPNs) using pre-shared keys, including displays of Internet Security Association and Key Management Protocol (ISAKMP) configurations, transform sets, and crypto maps. Debug commands are covered for testing and troubleshooting of IPsec and ISAKMP events.

## Objectives

Upon completing this lesson, you will be able to verify that the configuration is correctly configured. This ability includes being able to meet these objectives:

- Describe each of the steps used to test and verify an IPsec configuration
- Display your configured IKE policies
- Display your configured transform sets
- Display the current state of your IPsec SAs
- View your configured crypto maps
- Debug IPsec traffic
- Debug ISAKMP traffic

# Testing and Verifying IPsec

Cisco IOS software contains several **show**, **clear**, and **debug** commands to assist in testing and verification of IPsec. This topic describes commands used to test and verify IPsec configurations.

## Test and Verify IPsec

Cisco.com

- **Display your configured ISAKMP policies.**  
`show crypto isakmp policy`
- **Display your configured transform sets.**  
`show crypto ipsec transform-set`
- **Display the current state of your IPsec SAs.**  
`show crypto ipsec sa`

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4.4

You can perform the following actions to test and verify that you have correctly configured the VPN using Cisco IOS software:

- Display your configured ISAKMP 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

## Test and Verify IPsec (Cont.)

Cisco.com

- **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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—4-6

You can perform the following actions to test and verify that you have correctly configured VPN using Cisco IOS software:

- View your configured crypto maps with the **show crypto map** command
- Debug ISAKMP and IPsec traffic through the Cisco IOS software with the **debug crypto ipsec** and **debug crypto isakmp** commands

# Display Your Configured ISAKMP Policies

This topic describes how to display your ISAKMP policies.

## show crypto isakmp policy Command

Cisco.com

```
graph LR
 S1[Site 1
10.0.1.3] --- RA[Router A]
 RA --- I((Internet))
 I --- RB[Router B]
 RB --- S2[Site 2
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
```

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4.6

Use the **show crypto isakmp policy EXEC** command to view the parameters for each ISAKMP policy, as shown in the following example for Router A:

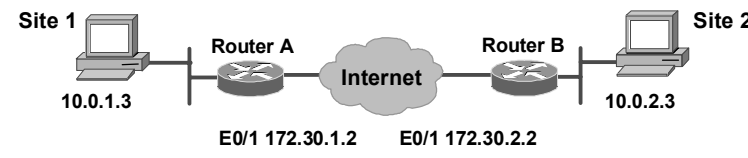
```
RouterA# show crypto isakmp policy
Protection suite of priority 110
 encryption algorithm: DES - Data Encryption Standard
 (56 bit keys).
 hash algorithm: Message Digest 5
 authentication method: Rivest-Shamir-Adleman
 Encryption
 Diffie-Hellman group: #1 (768 bit)
 lifetime: 86400 seconds, no volume 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
```

# Display Your Configured Transform Sets

This topic describes how to display your transform set configurations.

## show crypto ipsec transform-set Command

Cisco.com



```
graph LR
 S1[Site 1
10.0.1.3] --- RA[Router A
E0/1 172.30.1.2]
 RA --- I((Internet))
 I --- RB[Router B
E0/1 172.30.2.2]
 RB --- S2[Site 2
10.0.2.3]
```

```
router#
show crypto ipsec transform-set

RouterA# show crypto ipsec transform-set
Transform set MINE: { esp-des esp-md5-hmac }
will negotiate = { Tunnel, },
```

- View the currently defined transform sets

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.6-4.7

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 [transform-set-name]
```

| Command Parameter         | Description                                                                    |
|---------------------------|--------------------------------------------------------------------------------|
| <i>transform-set-name</i> | (Optional) Shows only the transform sets with the specified transform-set-name |

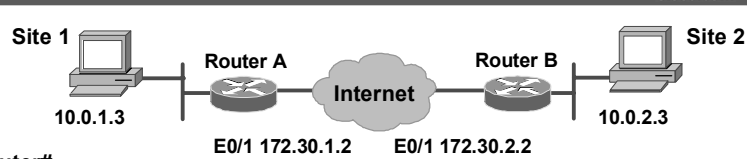
If no keyword is used, all transform sets configured at the router are displayed.

# Display the Current State of Your IPsec SAs

This topic describes how to display the state of IPsec security associations (SAs).

## show crypto ipsec sa Command

Cisco.com



```

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

```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.8

Use the **show crypto ipsec sa EXEC** command to view the settings used by current SAs. If no keyword is used, all SAs are displayed. The command syntax is as follows:

**show crypto ipsec sa** [*map map-name* | **address** | **identity** | **detail**]

| Command                    | Description                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>map</b> <i>map-name</i> | (Optional) Shows any existing SAs created for the crypto map.                                                                                                       |
| <b>address</b>             | (Optional) Shows all the existing SAs, sorted by the destination address and then by protocol (Authentication Header [AH] or Encapsulating Security Payload [ESP]). |
| <b>identity</b>            | (Optional) Shows only the flow information. It does not show the SA information.                                                                                    |
| <b>detail</b>              | (Optional) Shows detailed error counters. (The default is the high-level send-receive error counters.)                                                              |

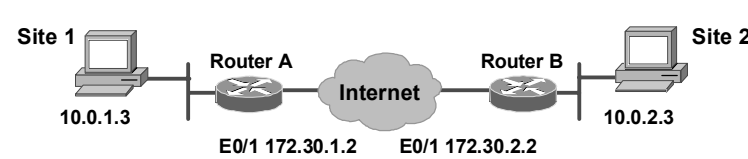


# Display Your Configured Crypto Maps

This topic describes how to display your crypto maps.

## show crypto map Command

Cisco.com



```

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, }

```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.9

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                                                                 |
|----------------------------|-----------------------------------------------------------------------------|
| <b>interface interface</b> | (Optional) Shows only the crypto map set applied to the specified interface |
| <b>tag map-name</b>        | (Optional) Shows only the crypto map set with the specified map name        |

# Enable Debug Output for IPSec Events

This topic describes the use of **debug** commands.

## debug crypto Commands

Cisco.com

```
router#
debug crypto ipsec
```

- Displays debug messages about all IPSec actions

```
router#
debug crypto isakmp
```

- Displays debug messages about all ISAKMP actions

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4-10

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 commands generates a significant amount of output for every IP packet processed, use them only when traffic on the IP network is low, so that other activity on the system is not adversely affected.

---

The following is sample output from the **debug crypto ipsec** command. In this example, SAs have been successfully established.

```
Router# debug crypto ipsec
```

IPSec requests SAs between 172.21.114.123 and 172.21.114.67, on behalf of the **permit ip host 172.21.114.123 host 172.21.114.67** command. It prefers to use the transform set esp-des with esp-md5-hmac, but it will also consider ah-sha-hmac.

```
00:24:30: IPSEC(sa_request): ,
 (key eng. msg.)
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123, dest= 172.21.114.67,
 src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 120s and 4608000kb,
```

```
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
00:24:30: IPSEC(sa_request): ,
(key eng. msg.)
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123, dest= 172.21.114.67,
src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1).,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 120s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0.
```

Internet Key Exchange (IKE) asks for service provider interfaces (SPIs) from IPsec. For inbound SAs, IPsec controls its own SPI space.

```
00:24:34: IPSEC(key_engine): got a queue event...
00:24:34: IPSEC(spi_response): getting spi 302974012ld for SA
 from 172.21.114.67 to 172.21.114.123 for prot 3
00:24:34: IPSEC(spi_response): getting spi 525075940ld for SA
 from 172.21.114.67 to 172.21.114.123 for prot 2
```

IKE asks IPsec if it accepts the SA proposal. In this case, it will be the one sent by the local IPsec in the first place.

```
00:24:34: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.21.114.67,
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123,
dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

After the proposal is accepted, IKE finishes the negotiations, generates the keying material, and then notifies IPsec of the new SAs (one SA for each direction).

```
00:24:35: IPSEC(key_engine): got a queue event...
```

The following output pertains to the inbound SA. The `conn_id` value references an entry in the crypto engine connection table.

```
00:24:35: IPSEC(initialize_sa): ,
 (key eng. msg.) dest= 172.21.114.123,
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.67,
 dest_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 src_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 120s and 4608000 kb,
 spi= 0x120F043C(302974012), conn_id= 29, keysize= 0, flags= 0x4
```

The following output pertains to the outbound SA:

```
00:24:35: IPSEC(initialize_sa): ,
 (key eng. msg.)
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123, dest= 172.21.114.67,
 src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 120s and 4608000kb,
 spi= 0x38914A4(59315364), conn_id= 30, keysize= 0, flags= 0x4
```

IPSec now installs the SA information into its SA database.

```
00:24:35: IPSEC(create_sa): sa created,
 (sa) sa_dest= 172.21.114.123, sa_prot= 50,
 sa_spi= 0x120F043C(302974012),
 sa_trans= esp-des esp-md5-hmac , sa_conn_id= 29
00:24:35: IPSEC(create_sa): sa created,
 (sa) sa_dest= 172.21.114.67, sa_prot= 50,
 sa_spi= 0x38914A4(59315364),
 sa_trans= esp-des esp-md5-hmac , sa_conn_id= 30
```

# Enable Debug Output for ISAKMP Events

This topic describes how to debug ISAKMP events.

## Crypto System Error Messages for ISAKMP

Cisco.com

```
%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.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-4.11

To display messages about IKE events, use the **debug crypto isakmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug crypto isakmp
```

```
no debug crypto isakmp
```

The following is sample output from the **debug crypto isakmp** command for an IKE peer that initiates an IKE negotiation.

First, IKE negotiates its own SA, checking for a matching IKE policy.

```
Router# debug crypto isakmp
20:26:58: ISAKMP (8): beginning Main Mode exchange
20:26:58: ISAKMP (8): processing SA payload. message ID = 0
20:26:58: ISAKMP (8): Checking ISAKMP transform 1 against priority 10
policy
20:26:58: ISAKMP: encryption DES-CBC
20:26:58: ISAKMP: hash MD5
20:26:58: ISAKMP: default group 1
20:26:58: ISAKMP: auth pre-share
20:26:58: ISAKMP (8): atts are acceptable. Next payload is 0
```

IKE has found a matching policy. Next, the IKE SA is used by each peer to authenticate the other peer.

```
20:26:58: ISAKMP (8): SA is doing pre-shared key authentication
20:26:59: ISAKMP (8): processing KE payload. message ID = 0
20:26:59: ISAKMP (8): processing NONCE payload. message ID = 0
20:26:59: ISAKMP (8): SKEYID state generated
20:26:59: ISAKMP (8): processing ID payload. message ID = 0
20:26:59: ISAKMP (8): processing HASH payload. message ID = 0
20:26:59: ISAKMP (8): SA has been authenticated
```

Next, IKE negotiates to set up the IPSec SA by searching for a matching transform set.

```
20:26:59: ISAKMP (8): beginning Quick Mode exchange, M-ID of 767162845
20:26:59: ISAKMP (8): processing SA payload. message ID = 767162845
20:26:59: ISAKMP (8): Checking IPSec proposal 1
20:26:59: ISAKMP: transform 1, ESP_DES
20:26:59: ISAKMP: attributes in transform:
20:26:59: ISAKMP: encaps is 1
20:26:59: ISAKMP: SA life type in seconds
20:26:59: ISAKMP: SA life duration (basic) of 600
20:26:59: ISAKMP: SA life type in kilobytes
20:26:59: ISAKMP: SA life duration (VPI) of
 0x0 0x46 0x50 0x0
20:26:59: ISAKMP: authenticator is HMAC-MD5
20:26:59: ISAKMP (8): atts are acceptable.
```

A matching IPSec transform set has been found at the two peers. Now the IPSec SA can be created (one SA is created for each direction).

```
20:26:59: ISAKMP (8): processing NONCE payload. message ID = 767162845
20:26:59: ISAKMP (8): processing ID payload. message ID = 767162845
20:26:59: ISAKMP (8): processing ID payload. message ID = 767162845
20:26:59: ISAKMP (8): Creating IPSec SAs
20:26:59: inbound SA from 155.0.0.2 to 155.0.0.1 (proxy
155.0.0.2 to 155.0.0.1)
20:26:59: has spi 454886490 and conn_id 9 and flags 4
20:26:59: lifetime of 600 seconds
20:26:59: lifetime of 4608000 kilobytes
20:26:59: outbound SA from 155.0.0.1 to 155.0.0.2
(proxy 155.0.0.1 to 155.0.0.2)
20:26:59: has spi 75506225 and conn_id 10 and flags 4
20:26:59: lifetime of 600 seconds
20:26:59: lifetime of 4608000 kilobytes
```

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 SA 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 SA. The recommended action is to contact the remote peer 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 administrator to resolve the improper configuration.

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Several show, clear , and debug commands are available to test and verify IPsec configurations:**
  - **The show crypto isakmp policy command Displays IKE policies.**
  - **The show crypto ipsec transform set command Displays transform sets.**
  - **The show crypto ipsec sa command Displays the state of SAs.**
  - **The show crypto map command Displays crypto maps.**
- **Debug commands are available to view IPsec and ISAKMP policy negotiation between two devices.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4-12



# Module Summary

This topic summarizes the key points discussed in this module.

## Module Summary

Cisco.com

- **Pre-shared key configuration requires IPsec and ISAKMP configuration.**
- **IKE policy configuration includes the following:**
  - **Enabling or disabling IKE**
  - **Creating IKE policies**
  - **Configuring pre-shared keys**
  - **Verifying the IKE configuration**
- **Configuring IPsec includes configuration of the following:**
  - **Transform sets**
  - **Global IPsec SA lifetimes**
  - **Crypto ACLs**
  - **Crypto maps**
  - **Applying maps to interfaces**
- **Several show, clear, and debug commands are available to test and verify IPsec configurations.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-4-1

This module covered the configuration of pre-shared keys for setting up a secure tunnel between networks. An overview of ISAKMP and IPsec functions introduced the concepts involved. Information on IKE parameters and configuration was followed by IPsec configuration. Hash algorithms, transform sets, and SAs were among the topics covered. Several **show** and **debug** commands for testing and troubleshooting were introduced.



## Module 5

---

# Cisco IOS-Based VPNs Using Certificate Authorities

---

## Overview

Although pre-shared keys work well in small networks, this technique does not scale well. An alternative is using digital certificates. This module covers the use of digital certificates, where all clients authenticate to a certificate authority (CA), also known as a certificate server, instead of using manual configuration of each individual device. This module addresses the issues involved in configuring the router to work with digital certificates.

## Module Objectives

Upon completing this module, you will be able to plan, configure, operate, and troubleshoot IPsec VPNs using Cisco routers and CAs. This ability includes being able to meet these objectives:

- Prepare the network for implementation of the required IPsec policy using digital certificates
- Configure CA support
- Configure Cisco IOS software IKE and IPsec policies with digital certificates
- Verify that the configuration is correct



## Lesson 1

---

# Preparing a Network for IPSec Configuration Using Certificate Authorities

---

## Overview

This lesson describes how to prepare your network for certificate authority (CA) interoperability, which is provided in support of the IPSec protocol. 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 in your network without the use of a CA, using a CA provides manageability and scalability for IPSec. This lesson introduces configuration of Cisco IOS software IPSec using a CA. After presenting an overview of CA and Cisco IOS support features, the lesson describes how to start the process of configuring your router to support CA. Following lessons describe completing the configuration process.

## Objectives

Upon completing this lesson, you will be able to prepare the network for implementation of the required IPSec policy using digital certificates. This ability includes being able to meet these objectives:

- Describe how Cisco IOS software supports open CA standards
- Describe how SCEP manages the certificate lifecycle
- Define each of the five tasks in configuring IPSec encryption using digital certificates
- Describe each of the planning steps used in defining IPSec security policy using digital certificates
- Determine the CA server details
- Determine the ISAKMP policies between IPSec peers
- Identify IPSec peer details
- Determine whether there are any IPSec policies already configured
- Verify connectivity between peers
- Ensure that existing ACLs on perimeter routers do not block IPSec traffic

# Overview of CA Support

This topic describes an overview of Cisco IOS CA support.

## Cisco IOS Software CA Support Standards

Cisco.com

**Cisco IOS software supports the following CA components:**

- IKE
- ISAKMP
- IPSec
- PKCS #7
- PKCS #10
- RSA keys
- X.509 v3 certificates
- SCEP
- CA interoperability

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0--5.4

Cisco IOS software supports the following standards with this feature:

- **Internet Key Exchange (IKE):** A hybrid protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. Although 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 security associations (SAs).
- **ISAKMP:** The Internet Security Association and Key Management Protocol.
- **IPSec:** IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
- **Public-Key Cryptography Standard #7 (PKCS #7):** A standard from RSA Security, used to encrypt and sign certificate enrollment messages.
- **Public-Key Cryptography Standard #10 (PKCS #10):** A standard syntax from RSA Security for certificate requests.
- **Rivest-Shamir-Adleman (RSA) keys:** RSA is the public key cryptographic system developed by Rivest, Shamir, and 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 ID 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 of the ITU.
- **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.

## Restrictions

The following restrictions apply when configuring your CA:

- This feature should be configured only when you also configure both IPSec and ISAKMP in your network.
- The Cisco IOS software *does not* support CA server public keys greater than 2048 bits.

## Prerequisites

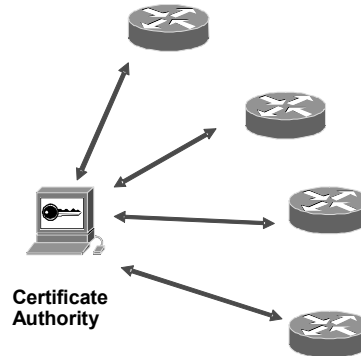
You need to have a CA available to your network before configuring this interoperability feature. The CA must support the Cisco Systems public key infrastructure (PKI) protocol, SCEP (formerly called certificate enrollment protocol [CEP]).



## Implementing IPsec with CAs

Cisco.com

**To add a new IPsec router to the network, you need only configure that new router to request a certificate from the CA, instead of making multiple key configurations with all the other existing IPsec routers.**



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5-6

## Overview of CAs

CAs are responsible for managing certificate requests and issuing certificates to participating IPsec network devices. These services provide centralized key management for the participating devices.

CAs simplify the administration of IPsec network devices. You can use a CA with a network containing multiple IPsec-compliant devices such as routers.

Digital signatures, enabled by public key cryptography, provide a means of digitally authenticating devices and individual users. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. In simple terms, a signature is formed when data is encrypted with the private key of a user. The receiver verifies the signature by decrypting the message with the public key of the sender. The fact that the message could be decrypted using the sender public key indicates that the holder of the private key, the sender, must have created the message. This process relies on the receiver having a copy of the sender public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates provide the link. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the public key of the entity. The certificate is itself signed by a CA, a third party that is explicitly trusted by the receiver to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the public key of the CA. Normally this process is handled out-of-band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default. IKE, an essential component of IPsec, can use digital signatures to scalably authenticate peer devices before setting up SAs.

Without digital signatures, you must manually exchange either public keys or secrets between each pair of devices that use IPSec to protect communications between them. Without certificates, every new device added to the network requires a configuration change on every other device with which it communicates securely. With digital certificates, each device is enrolled with a CA. When two devices wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new device is added to the network, one simply enrolls that device with a CA, and none of the other devices needs modification. When the new device attempts an IPSec connection, certificates are automatically exchanged, and the device can be authenticated.

# Simple Certificate Enrollment Protocol Overview

This topic describes Simple Certificate Enrollment Protocol (SCEP).

## SCEP

Cisco.com

- **Cisco-sponsored IETF draft**
- **Lightweight protocol to support certificate life-cycle operations on the Cisco PIX Firewall**
- **Uses PKCS #7 and PKCS #10**
- **Transaction-oriented request-and-response protocol**
- **Transport mechanism independent**
- **Requires manual authentication during enrollment**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6.6

SCEP is a Cisco Systems, VeriSign, Entrust, Microsoft, Netscape, and Sun Microsystems initiative that provides a standard way of managing the certificate lifecycle.

---

**Note**      The 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.

A white paper describing SCEP in detail can be found at:  
[http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm).

SCEP provides two authentication methods: manual authentication and authentication based on a 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#10 client and CA must be compared out-of-band between the server and the end entity. SCEP clients and CAs (or registration authorities [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.

## CA Servers Interoperable with Cisco Routers

Cisco.com

- **Entrust Technologies**
- **VeriSign OnSite**
- **Microsoft Windows 2000 Certificate Services**

**See Cisco.com for the latest listing of supported CA servers.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—5.7

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 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 that interoperate with Cisco IOS software:

- Entrust Technologies
- VeriSign OnSite 4.5
- Microsoft Windows 2000 Certificate Services 5.0

## Entrust Technologies

The Entrust CA server is one of several servers interoperable with Cisco products. Entrust uses software that is installed and administered by the user. 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 Microsoft Windows NT 4.0 (required for Cisco interoperability), Sun Solaris 2.6, Hewlett-Packard HP-UX 10.20, and IBM AIX 4.3 operating systems. Entrust requires RSA usage keys on the routers. You must use Cisco IOS Software Release 11.(3)5T or later.
- **Standards supported:** Entrust supports CA services, RA capability, SCEP, and PKCS #10.

Refer to the Entrust website at <http://www.entrust.com> for more information.

## VeriSign OnSite

The VeriSign OnSite CA server is another CA that operates with Cisco routers. VeriSign administers the CA, providing the certificates as a service.

The VeriSign OnSite 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 (more than 60 second) retry count. You must use Cisco IOS Software Release 12.0(6.0.1)T or later. Cisco IOS Software Release 12.0(5)T is not supported because of a known issue in that release.
- **Standards supported:** OnSite supports SCEP, the X.509 certificate format, and PKCS# 7, 10, 11, and 12.

Refer to the VeriSign website at <http://www.verisign.com> for more information.

## Microsoft Windows 2000 Certificate Services

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 the Cisco virtual private network (VPN) security solutions. These are the features:

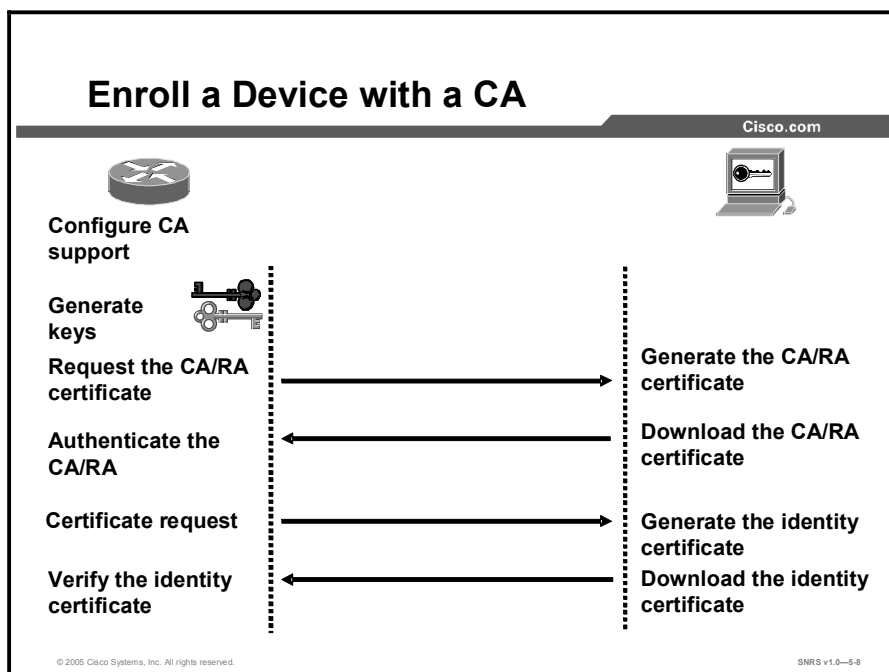
- **Requirements:** Compatible PC capable of running Windows 2000 Server. You must use Cisco IOS Software Release 12.0(5)T and above.
- **Standards supported:** The following standards are supported with this CA server: X.509 Version 3, CRL Version 2, PKCS #7, #10, and #12), PKIX, SSL Version 3, Kerberos Version 5 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:
  - 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 URL, <http://URLHostName/certsrv/mscep/mscep.dll>, and copying the phrase. The phrase is then entered upon IPSec client enrollment.
  - 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.
  - (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 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.



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 or RA.
  2. Generate a CA or RA certificate.
  3. Download a CA or RA certificate to a router.
  4. Authenticate a CA or RA certificate via the CA or RA fingerprint.
- 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 vendor determines how long certificates are valid. Contact the relevant vendor to determine how long the certificates will be valid in your particular case.



# Configuring IPsec Encryption with Digital Certificates

This topic presents an overview of the tasks required to configure CA support on your router.

## Configure CA Support Tasks

Cisco.com

- **Prepare for ISAKMP and IPsec.**
- **Configure CA support.**
- **Configure ISAKMP.**
- **Configure IPsec.**
- **Test and verify IPsec.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5-9

The configuration process for RSA signatures consists of five major tasks.

- **Task 1:** Prepare for ISAKMP and IPsec. Preparing for ISAKMP and IPsec involves determining the detailed encryption policy: identifying the hosts and networks that you wish to protect, determining IPsec peer details, determining the IPsec features that you need, and ensuring that existing access control lists (ACLs) are compatible with IPsec.
- **Task 2:** Configure CA support. This task involves setting the router host name and domain name, generating the keys, declaring a CA, and authenticating and requesting your own certificates.
- **Task 3:** Configure ISAKMP for IPsec. Configuring ISAKMP involves enabling ISAKMP, creating the ISAKMP 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.

The rest of this lesson covers the first task, preparing your router to support IPsec using CAs.

# Planning the ISAKMP and IPsec Policy

Successful implementation of an IPsec network requires advance planning before beginning configuration of individual routers. This topic describes the planning of IKE and IPsec policies.

## Prepare for ISAKMP and IPsec

Cisco.com

- **Step 1: Plan for CA support.**
- **Step 2: Determine ISAKMP (IKE Phase 1) policy.**
- **Step 3: Determine IPsec (IKE Phase 2) policy.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5-10

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:

- Step 1**    Plan for CA support: Determine the CA server details. This includes variables such as the type of CA server to be used, the IP address, and the CA administrator contact information.
  
- Step 2**    Determine ISAKMP (IKE Phase 1) policy: Determine the ISAKMP 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.

## Prepare for ISAKMP and IPsec (Cont.)

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`

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5.11

- Step 4** Check the current configuration: Use the **show run**, **show crypto isakmp policy**, and **show crypto map** commands, and 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

This topic describes the planning steps for CA support.

## 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 IP address, host name, and URL.**
- **Identify the CA server administrator contact information.**

**Goal: Be ready for CA support configuration.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0–5-12

Successful implementation of an IPSec network requires advance planning before beginning configuration of individual routers.

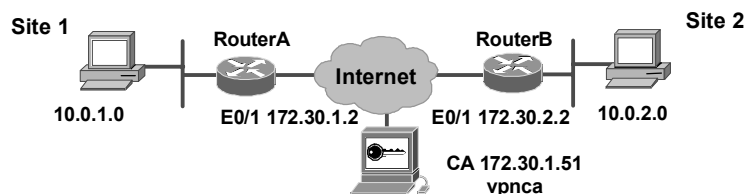
Configuring a CA is complicated. Having a detailed plan lessens the chances of improper configuration. Some planning steps include the following:

- 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 RA mode.
- Identify the CA server IP address, host name, and URL. (This information is necessary if you use Lightweight Directory Access 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



| Parameter             | CA Server       |
|-----------------------|-----------------|
| Type of CA server     | Windows 2000    |
| Host name             | vpnca           |
| IP address            | 172.30.1.51     |
| URL                   | vpnca.cisco.com |
| Administrator contact | 1-800-555-1212  |

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—5-13

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 ISAKMP (IKE Phase 1) Policy

This topic describes the ISAKMP configuration process.

## Step 2: Determine ISAKMP Policy Details

Cisco.com

**Determine the following policy details:**

- **Key distribution method**
- **Authentication method**
- **IPSec peer IP addresses and host names**
- **ISAKMP Phase 1 policies for all peers**
  - **Encryption algorithm**
  - **Hash algorithm**
  - **ISAKMP SA lifetime**

**Goal: Minimize misconfiguration.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0–5-14

Configuring ISAKMP is complicated. You should determine the ISAKMP 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 ISAKMP policy 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 the IP addresses and host names of the IPSec peers:** Determine the details of all the IPSec peers that will use ISAKMP and RSA signature keys for establishing SAs. You will use this information to configure ISAKMP.
- **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 ISAKMP to support the policy details you determined. Some ISAKMP policy details include the following:
  - Encryption algorithm
  - Hash algorithm

— ISAKMP 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 ISAKMP Policy Details (Examine Parameters)

Cisco.com

| Parameter             | Strong         | Stronger                        |
|-----------------------|----------------|---------------------------------|
| Encryption algorithm  | DES            | 3DES or AES                     |
| Hash algorithm        | MD5            | SHA-1                           |
| Authentication method | Pre-shared     | RSA encryption<br>RSA signature |
| Key exchange          | DH group 1     | DH group 2                      |
| IKE SA lifetime       | 86,400 seconds | < 86,400 seconds                |

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—5-15

An ISAKMP policy defines a combination of security parameters used during the ISAKMP negotiation. A group of policies makes up a “protection suite” of multiple policies that enable IPSec peers to establish ISAKMP sessions and establish SAs with a minimal configuration. The figure shows an example of possible combinations of ISAKMP parameters into either a strong or stronger policy suite.

### Creating ISAKMP Policies for a Purpose

ISAKMP negotiations must be protected, so each ISAKMP negotiation begins by each peer agreeing on a common (shared) ISAKMP policy. This policy states which security parameters are used to protect subsequent ISAKMP 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 ISAKMP traffic during the negotiation.

You can create multiple, prioritized policies at each peer to ensure that at least one policy will match the policy of a remote peer .



## Defining ISAKMP Policy Parameters

You can select specific values for each ISAKMP parameter per the IKE standard. You choose one value over another based on the security level that you desire and the type of IPSec peer to which you will connect.

There are five parameters to define in each ISAKMP policy, as outlined in the figure and in this 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                                   | Data Encryption Standard (DES)<br>Triple-Data Encryption Standard (3DES)<br>Advanced Encryption Standard (AES) 128, 192, 256 bits | <b>des</b><br><b>3des</b><br><b>aes</b>               | DES                      |
| Message integrity (hash) algorithm                             | Secure Hash Algorithm-1 (SHA-1; Hash-Based Method Authentication Code [HMAC] variant)<br>MD5 (HMAC variant)                       | <b>sha</b><br><b>md5</b>                              | SHA-1                    |
| Peer authentication method                                     | Pre-shared keys<br>RSA encrypted nonces<br>RSA signatures                                                                         | <b>pre-share</b><br><b>rsa-encr</b><br><b>rsa-sig</b> | RSA signatures           |
| Key exchange parameters (Diffie-Hellman [DH] group identifier) | 768-bit DH<br>1024-bit DH<br>1536-bit DH                                                                                          | <b>1</b><br><b>2</b><br><b>5</b>                      | 768-bit DH               |
| ISAKMP-established SA 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 that you desire and the type of IPSec peer to which you will connect. There are five parameters to define in each ISAKMP policy, as presented in the 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<br>RSA signature |
| Key exchange parameters (DH group identifier) | DH group 1     | DH group 2<br>DH group 5        |
| ISAKMP-established SA lifetime                | 86,400 seconds | <86,400 seconds                 |

## Step 2: Determine ISAKMP Policy Details (Example)

Cisco.com



| 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       | 86,400 seconds | 86,400 seconds |
| Peer IP address       | 172.30.2.2     | 172.30.1.2     |

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—5-16

You should determine ISAKMP policy details for each peer before configuring ISAKMP. The figure shows a summary of ISAKMP 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.

## Step 3—Determine IPSec (IKE Phase 2) Policy

This topic describes the configuration of IPSec policies.

### Step 3: 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.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0–5-17

An IPSec policy defines a combination of IPSec parameters used during the IPSec negotiation. Planning for IPSec (IKE Phase 2) is another important step that you should complete before actually configuring IPSec on a Cisco router. Policy details to determine at this stage include these:

- **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 host 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 that you will need in later steps to minimize misconfiguration.

## IPSec Transforms Supported in Cisco IOS Software

Cisco.com

### 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-seal ESP transform using SEAL cipher (160 bits)
esp-sha-hmac ESP transform using HMAC-SHA auth
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5-18

Cisco IOS software supports the IPSec transforms as shown in the tables.

| Transform   | Description                                   |
|-------------|-----------------------------------------------|
| ah-md5-hmac | Authentication Header (AH)-HMAC-MD5 transform |
| ah-sha-hmac | AH-HMAC-SHA transform                         |

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 Network Address Translation (NAT) or Port Address Translation (PAT).

| Transform    | Description                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| esp-des      | ESP transform using DES cipher (56 bits).                                                                                                          |
| esp-3des     | ESP transform using 3DES-Encrypt-Decrypt-Encrypt (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 the 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 the ESP packet.           |
| esp-null     | ESP transform without a cipher. It may be used in combination with esp-md5-hmac or esp-sha-hmac if you want ESP authentication with no encryption. |

**Caution** Never use esp-null in a production environment because it does not protect data flows.

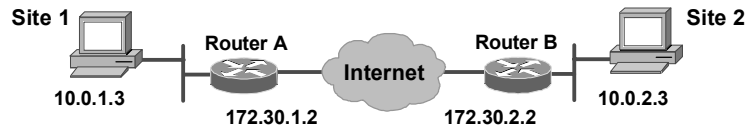
Examples of acceptable transforms that can be combined into sets are shown in the table.

| Transform Type                                      | Allowed Transform Combinations                                                                                                                                                                                                                |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AH transform<br>(Choose up to one.)                 | ah-md5-hmac: AH with the MD5 (HMAC variant) authentication algorithm<br><br>ah-sha-hmac: AH with the SHA (HMAC variant) authentication algorithm                                                                                              |
| ESP encryption transform<br>(Choose up to one.)     | esp-des: ESP with the 56-bit DES encryption algorithm<br><br>esp-3des: ESP with the 168-bit DES encryption algorithm (3DES)<br><br>esp-aes: ESP transform using AES cipher (128, 192, or 256 bits)<br><br>esp-null: Null encryption algorithm |
| ESP authentication transform<br>(Choose up to one.) | esp-md5-hmac: ESP with the MD5 (HMAC variant) authentication algorithm<br><br>esp-sha-hmac: ESP with the SHA (HMAC variant) authentication algorithm                                                                                          |
| IP compression transform                            | comp-lzs: IP compression with the Lempel-Ziv-STAC (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

Cisco.com



| Policy                                | Site 1          | Site 2          |
|---------------------------------------|-----------------|-----------------|
| Transform set                         | ESP-DES, tunnel | ESP-DES, tunnel |
| Peer host name                        | 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    |

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5-19

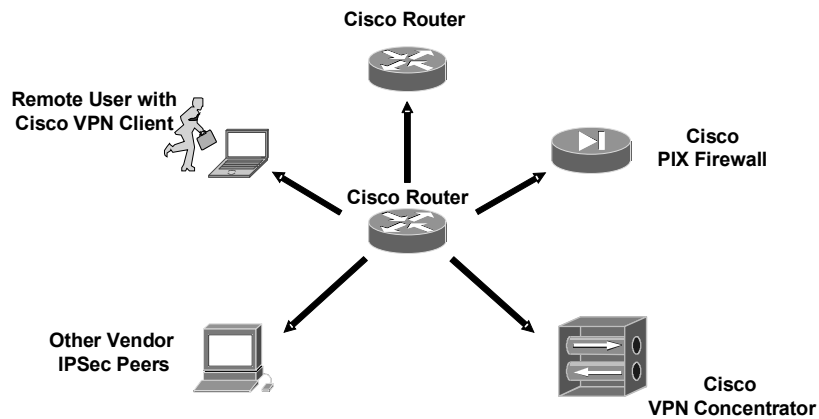
Determining network design details includes defining a more detailed IPSec policy for protecting traffic. You can then use the detailed policy to help select IPSec transform sets and modes of operation. Your IPSec policy should answer the following questions:

- What protections are required or are acceptable for the protected traffic?
- Which IPSec transforms or transform 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 how often should the SAs be renegotiated?

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.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—5-20

An important part of determining the IPsec policy is to identify the IPsec peer that the Cisco router will communicate with. The peer must support IPsec as specified in the RFCs as supported by Cisco IOS software. 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:

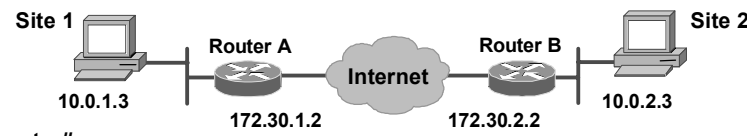
- Other Cisco routers
- Cisco PIX Firewalls
- Cisco VPN Clients
- Cisco VPN Concentrators
- Other vendor IPsec products that conform to IPsec RFCs

## Step 4—Check the Current Configuration

This topic describes how to check the current configuration to see if policies are already configured that may be useful or that may interfere with planned IPSec policies.

### Step 4: Check Current Configuration

Cisco.com



```
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
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-521

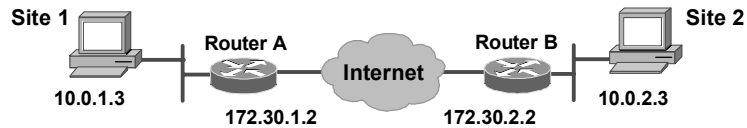
The current Cisco router configuration should be checked to see if there are any IPSec policies already configured that are useful for, or that may interfere with, the IPSec policies that you plan to configure. Previously configured IKE and IPSec policies and details can and should be used, if possible, to save configuration time. However, previously configured IKE and IPSec policies and details can make troubleshooting more difficult if problems arise.

You can see whether any IKE policies have previously been configured by issuing 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 4: Check Current Configuration (Cont.)

Cisco.com



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, }
```

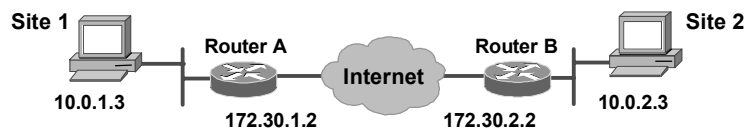
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5.22

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 that you are trying to configure.

## Step 4: Check Current Configuration (Cont.)

Cisco.com



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, },
```

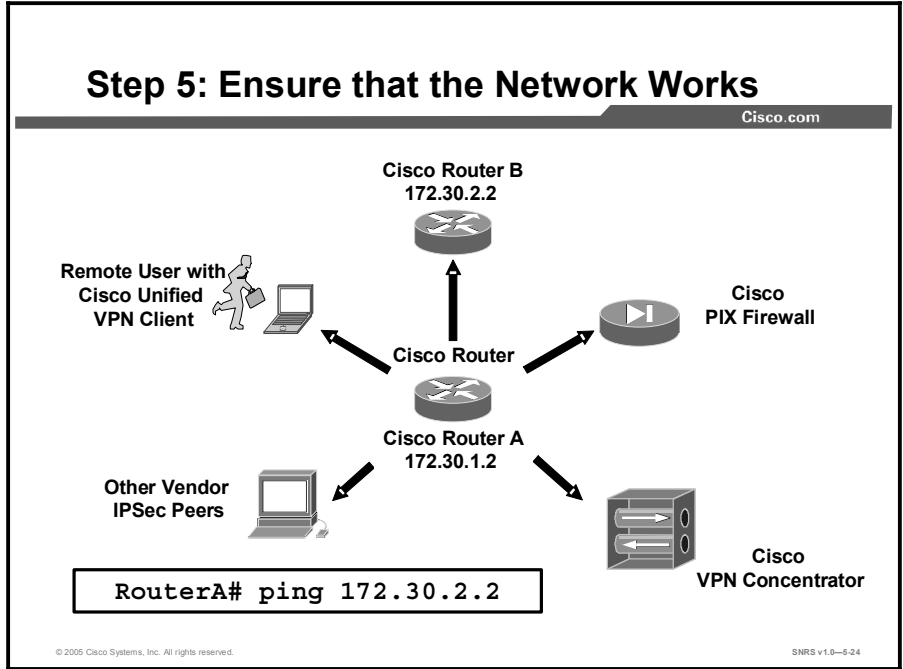
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5.23

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 5—Ensure That the Network Works Without Encryption

This topic describes how to check for network connectivity before applying encryption.



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. Although a successful Internet Control Message Protocol (ICMP) echo (ping) will verify basic connectivity between peers, you should ensure that the network works with any other protocols or ports that 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 6—Ensure That ACLs Are Compatible with IPsec

This topic covers commands used to check ACLs for IPsec compatibility.

### Step 6: Ensure that ACLs Are Compatible with IPsec

Cisco.com

```
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

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-25

You will need to ensure that existing ACLs on perimeter routers, the Cisco 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, ESP, and 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 that 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
```

The protocol keyword **esp** equals the ESP protocol (number 50), the keyword **ahp** equals the AH protocol (number 51), and the keyword **isakmp** equals UDP port 500.

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Standards supported by Cisco include: IKE, ISAKMP, IPSec, PKCS #7 and #10, RSA keys, X.509 v3 certificates, and CA interoperability.**
- **Cisco IOS software does not support CA server public keys greater than 2048 bits.**
- **CAs are responsible for managing certificate requests and issuing certificates to participating IPSec network devices.**
- **SCEP is a Cisco, VeriSign, Entrust, Microsoft, Netscape, and Sun Microsystems initiative that provides a standard way of managing the certificate lifecycle.**
- **Tasks include planning for CA support, determining IKE Phase 1 and 2 policies, checking for current IPSec configurations, ensuring that the network has connectivity before IPSec implementation, and making sure that ACLs are compatible with IPSec.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.26

## Summary (Cont.)

Cisco.com

- **CA preparation includes gathering the type of CA server, the IP address of the server, the host name, the URL, and administrator contact information.**
- **IKE policies include the encryption algorithm, hash algorithm, authentication method, Diffie-Hellman key exchange, and SA lifetime.**
- **IPSec policies include transform sets, peer details, and traffic to be protected.**
- **Use show commands to check current configurations and ACLs.**
- **Use the ping command to check connectivity prior to implementation of IPSec.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.27



## Lesson 2

---

# Configuring Certificate Authority on Cisco Routers

---

## Overview

The previous lesson covered the steps necessary in preparing a network to work with certificate authorities (CAs). This lesson guides the learner through the process of configuring a Cisco router to support CAs. Included are topics on managing NVRAM, router date and time settings, and commands to configure Rivest, Shamir, and Adleman (RSA) keys and CAs.

## Objectives

Upon completing this lesson, you will be able to configure CA support on Cisco routers. This ability includes being able to meet these objectives:

- Describe each of the steps used in configuring CA
- Specify that certificates and CRLs are to be retrieved from the CA only when needed
- Set the router time and date
- Add a CA server entry to the router host table
- Generate an RSA key pair
- Declare a CA on the router
- Authenticate the CA to verify that it is valid
- Obtain the identity certificate for your router from the CA
- Save the CA support configuration
- Complete the optional steps required to monitor and maintain interoperability
- Verify the CA support configuration

# Configuring Certificate Authorities

This topic describes the steps necessary to configure CA interoperability on a Cisco router.

## Cisco IOS Software CA Configuration Procedure

Cisco.com

- **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 host name 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 pki trustpoint name`

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5.4

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:

- Step 1** (Optional) Manage the NVRAM memory usage. In some cases, storing certificates and certificate revocation lists (CRLs) locally does not present a problem. However, in other cases, memory might become an issue—particularly if your CA supports a registration authority (RA) and a large number of CRLs end up being stored on your router.
- Step 2** Set the router time and date. The router must have an accurate time and date to enroll with a CA server.
- Step 3** Configure the router host name and domain name. The host name 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 host names.
- 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 that your router should use, use the **crypto pki trustpoint** global configuration command. Use the **no** form of this command to delete all identity information and certificates associated with the CA.



## Cisco IOS Software CA Configuration Procedure (Cont.)

Cisco.com

- **Step 6: Authenticate the CA:**  
`crypto pki authenticate name`
- **Step 7: Request your own certificate:**  
`crypto pki enroll name`
- **Step 8: Save the configuration:**  
`copy running-config startup-config`
- **Step 9: (Optional) Monitor and maintain CA interoperability:**  
`crypto pki trustpoint name`
- **Step 10: Verify the CA support configuration:**  
`show crypto pki certificates`  
`show crypto key mypubkey | pubkey-chain`

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—5-6

- Step 6** Authenticate the CA. The router needs to authenticate the CA. It does this by obtaining the CA self-signed certificate that contains the CA public key.
- Step 7** Request your own certificate. Complete this step to obtain the identity certificate for your router from the CA.
- Step 8** Save the configuration. After you have configured 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 the RSA keys of your router.
  3. Delete both public and private certificates from the configuration.
  4. Delete the public keys of the peer.
- Step 10** Verify the CA support configuration. The commands detailed in this topic allow you to view your CA certificates and any other configured CA certificates.

# Step 1—Manage the NVRAM Use

This topic describes the optional tasks of managing NVRAM.

## Step 1: (Optional) Manage NVRAM Memory Usage

Cisco.com

- **Types of certificates stored on a router**
  - The router's own identity certificate
  - The CA's root certificate
  - Root certificates obtained from CA servers
  - Two 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

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5.6

Certificates and CRLs are used by your router when a CA is used. Normally, certain certificates and all CRLs are stored locally in the router NVRAM, and each certificate and CRL uses a moderate amount of memory.

The following certificates are normally stored at your router:

- The certificate of your router.
- The certificate of the CA.
- Root certificates obtained from CA servers. (All root certificates are saved in RAM after the router has been initialized.)
- Two RA certificates (only if the CA supports an RA).

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 practice 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.

| Command                                            | Purpose                                                                          |
|----------------------------------------------------|----------------------------------------------------------------------------------|
| Router(config)# <b>crypto ca certificate query</b> | Turns on query mode, which causes certificates and CRLs not to be stored locally |

---

**Note** Query mode may affect availability if the CA is down.

---

If you do not turn on query mode now, you can turn it on later even if certificates and CRLs have already been stored on your router. In this case, when you turn on query mode, the stored certificates and CRLs will be deleted from the router after you save your configuration. (If you copy your configuration to a TFTP site prior to turning on query mode, you will save any stored certificates and CRLs at the TFTP site.)

If you turn on query mode now, you can turn off query mode later if you wish. If you turn off query mode later, you could also perform the **copy system:running-config nvram:startup-config** command at that time to save all current certificates and CRLs to NVRAM. Otherwise they could be lost during a reboot and would need to be retrieved the next time they were needed by your router.

## Step 2—Set the Router Time and Date

The router must have a valid date and time configuration. This topic describes the steps involved with these settings.

### Step 2: Set the Router Time and Date

Cisco.com

**router(config)#**

`clock timezone zone hours [minutes]`

- Sets the router time zone and offset from UTC

`RouterA(config)# clock timezone cst -6`

**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 17 February 2005`

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5.7

Ensure that the time zone, time, and date for the router have 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 time zone, use the **clock timezone** global configuration command. The command sets the time zone and an offset from Coordinated Universal Time (UTC, displayed by the router).

The syntax for the **clock timezone** command is as follows:

```
clock timezone zone hours [minutes]
```

|                |                                                                        |
|----------------|------------------------------------------------------------------------|
| <i>zone</i>    | Name of the time zone to be displayed when standard time is in effect. |
| <i>hours</i>   | Hours offset from UTC.                                                 |
| <i>minutes</i> | (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 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
```

---

|                 |                                                                |
|-----------------|----------------------------------------------------------------|
| <i>hh:mm:ss</i> | Current time in hours (military format), minutes, and seconds. |
| <i>day</i>      | Current day (by date) in the month.                            |
| <i>month</i>    | Current month (by name).                                       |
| <i>year</i>     | 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 17 February 2005
```

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 time on routers that do not have a clock circuit chip.

---

# Step 3—Add a CA Server Entry to the Router Host Table

This topic describes how to give the router a host and domain name and how to add a CA server entry to the router host table.

## Step 3: Add a CA Server Entry to the Router Host Table

```

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

```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-8

You must configure the host name and IP domain name of the router if this has not already been done. This process is required because the router assigns a fully qualified domain name (FQDN) to the keys and certificates used by IPsec, and the FQDN is based on the host name and IP domain name that you assign to the router. For example, a certificate named *router20.example.com* is based on a router host name of *router20* and a router IP domain name of *example.com*.

To specify or modify the host name for the network server, use the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. The setup command facility also prompts for a host name at startup.

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

**hostname** *name*

|             |                                      |
|-------------|--------------------------------------|
| <i>name</i> | New hostname for the network server. |
|-------------|--------------------------------------|

To define a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name), use the **ip domain-name** global configuration command. To disable use of the Domain Name System (DNS), use the **no** form of this command.

The command syntax for the **ip domain-name** command is as follows:

**ip domain-name** *name*

|             |                                                                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i> | Default domain name used to complete unqualified host names. 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.)

Cisco.com

```

router(config)#
ip host name address1 [address2...addressN]
 • Defines a static host name-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

```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.9

Use the **ip host** global configuration command to define a static host name-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...addressN]*

|                            |                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------|
| <i>name</i>                | Name of the host. The first character can be either a letter or a number.                    |
| <i>address1</i>            | Associated IP address.                                                                       |
| <i>address2...addressN</i> | (Optional) Additional associated IP address. You can bind multiple addresses to a host name. |

# Step 4—Generate an RSA Key Pair

This topic describes how to generate your own RSA key pairs.

## Step 4: Generate an RSA Key Pair

Cisco.com

```
router(config)#
crypto key generate rsa [general-keys / 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
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-10

RSA key pairs are used to sign and encrypt Internet Key Exchange (IKE) key management messages and are required before you can obtain a certificate for your router.

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.

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 [general-keys | usage-keys]
```

|                   |                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>usage-keys</i> | (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 the **usage-keys** keyword 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 that your router has a host name 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 host name and IP domain name.

---



The keys generated by the **crypto key generate rsa** command are saved in the private configuration in NVRAM, which is never displayed to the user or backed up to another device.

## 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 the exposure of that key.)

## 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 be used more frequently than a special-usage key pair.

### Step 4: Generate RSA Keys (Example Output)

Cisco.com

```

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
```

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0--5-11

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. It is recommended that you use a minimum modulus of 1024. The 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 Series  | 11 seconds         | 20 seconds | 4 minutes, 38 seconds | Longer than 1 hour |
| Cisco 4700 routers | Less than 1 second | 1 second   | 4 seconds             | 50 seconds         |

## Step 5—Declare a CA

This topic describes the process of declaring a CA.

### Step 5: Declare a CA

Cisco.com

```
router(config)#
crypto pki trustpoint name
```

- Specifies the desired CA server name
- Puts you in the ca-trustpoint configuration mode

```
RouterA(config)# crypto pki trustpoint vpnca
RouterA(ca-trustpoint)#
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-12

Note that in Cisco IOS Software Release 12.3(7)T, the **crypto pki trustpoint** command replaces the **crypto ca trustpoint** command from earlier Cisco IOS software releases. You can still enter the **crypto ca trustpoint** command, but the command will be written in the configuration as “**crypto pki trustpoint**.”

Use the **crypto pki trustpoint** global configuration command to declare which CA your router will use. The **crypto pki trustpoint** command will allow the router to re-enroll to the CA server automatically when its certificates expire. Use the **no** form of this command to delete all identity information and certificates associated with the CA.

The syntax for the **crypto pki trustpoint** command is as follows:

```
crypto pki 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 that you previously created.) The CA might require a particular name, such as its domain name.

**Note** The **crypto pki trustpoint** command is significant locally only. It does not have to match the identity defined on any of the VPN peers.

## Step 5: Commands Used to Declare a CA

Cisco.com

```
RouterA(config)# crypto pki 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 Mode supported by the Certificate Authority
 retry Polling parameters
 url CA server enrollment URL
```

© 2005 Cisco Systems, Inc. All rights reserved.

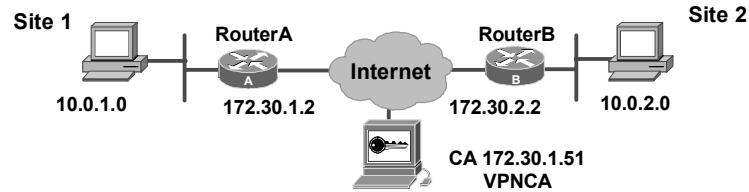
SNRS v1.0-5-13

Performing the **crypto pki 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:** Specify the RA mode (required only if your CA system provides an RA)
- **query url:** Specify the URL of the Lightweight Directory Access Protocol (LDAP) server (required only if your CA supports an RA and the LDAP protocol)
- **enrollment retry-period:** (Optional) Specify a period of time that the router should wait between sending certificate request retries
- **enrollment retry-count:** (Optional) Specify how many certificate request retries that your router will send before giving up
- **crl optional:** (Optional) Specify that your router can still accept the certificates of other peers if the CRL is not accessible

## Step 5: Declare a CA (Example)

Cisco.com



```
RouterA(config)# crypto pki trustpoint VPNCA
RouterA(ca-trustpoint)# enrollment url
http://vpnca/certsrv/mscep/mscep.dll
RouterA(ca-trustpoint)# enrollment mode ra
RouterA(ca-trustpoint)# crl optional
```

- Specifies the URL for the CA server
- Minimum configuration to declare a CA

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5.14

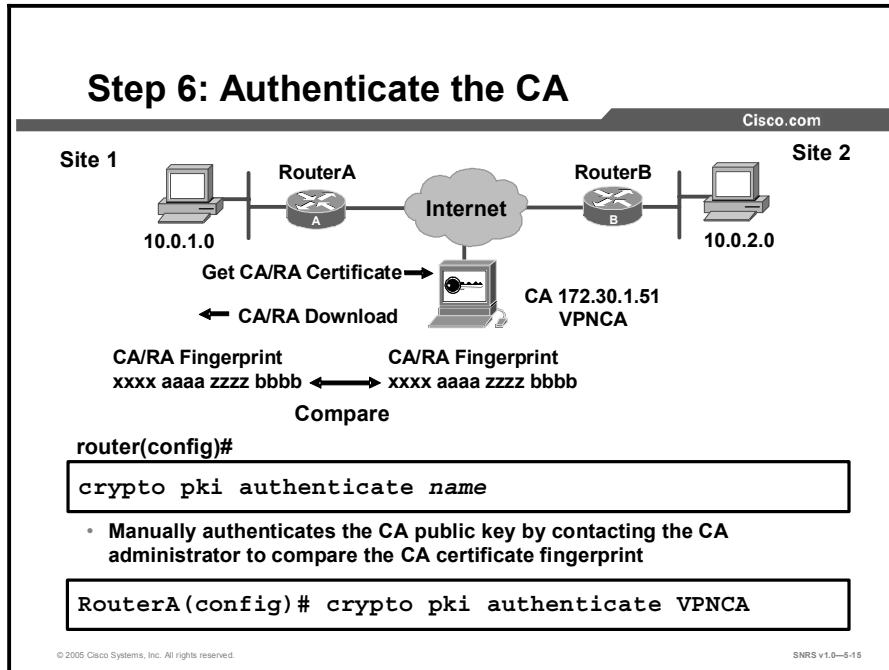
The example shown in the figure declares an Entrust CA and identifies characteristics of the CA. In this example, the name *vpnca* is created for the CA, which is located at <http://vpnca>. The example also declares a CA using an RA. The CA scripts are stored in the default location, and the CA uses Simple Certificate Enrollment Protocol (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 Microsoft SCEP (MSCEP) dynamic link library (DLL):

```
crypto pki trustpoint VPNCA
enrollment url http://vpnca/certsrv/mscep/mscep.dll
enrollment mode ra
crl optional
```

# Step 6—Authenticate the CA

This topic describes the commands for authenticating the CA.



The router needs to authenticate the CA to verify that it is valid. The router does this by obtaining the CA self-signed certificate that contains the public key of the CA. Because the CA certificate is self-signed (the CA signs its own certificate), the CA public key should be manually authenticated by contacting the CA administrator to compare the fingerprint of the CA certificate when you perform this step. To get the public key of the CA, use the **crypto pki authenticate name** command in global configuration mode. Use the same name that you used when declaring the CA with the **crypto pki trustpoint** command.

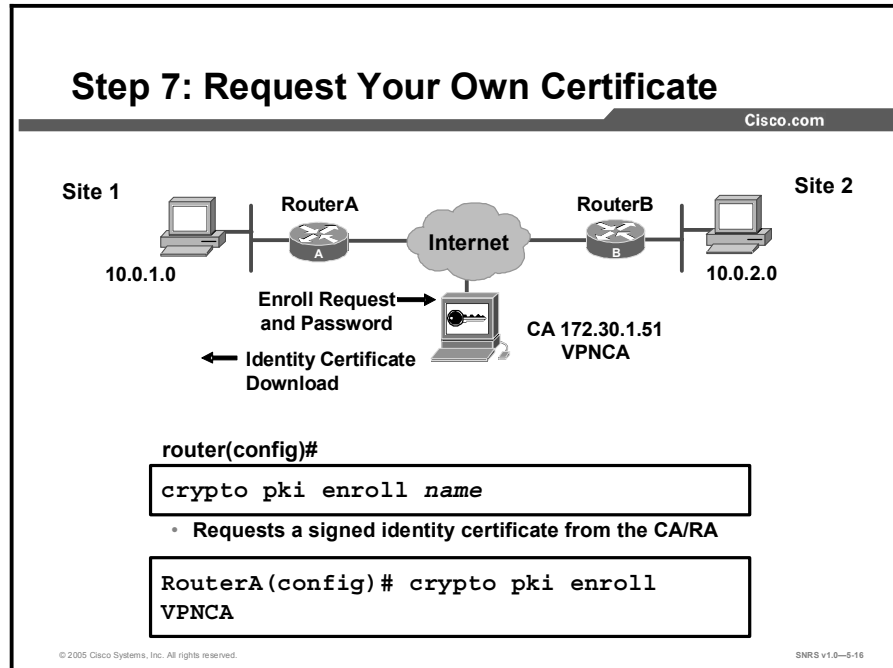
If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto pki authenticate** command, the RA signing and encryption certificates are returned from the CA as well as the CA certificate.

The following example shows a CA authentication:

```
RouterA(config)# crypto pki authenticate VPNCA
Certificate has the following attributes:
Fingerprint: 93700C31 4853EC4A DED81400 43D3C82C
% Do you accept this certificate? [yes/no]: y
```

## Step 7—Request Your Own Certificate

This topic describes the process for requesting your own certificate.



You must obtain a signed certificate from the CA for each of the RSA key pairs of your router. If you generated general-purpose RSA keys, your router has only one RSA key pair and needs only one certificate. If you previously generated special-usage RSA keys, your router has two RSA key pairs and needs two certificates.

To request signed certificates from the CA, use the following command in global configuration mode:

```
Router(config)# crypto pki enroll name
```

| Command                                                  | Purpose                                                                                                                                                                                                                                    |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Router(config)# <b>crypto pki enroll name</b></pre> | Requests certificates for all of your RSA key pairs. This command causes your router to request as many certificates as there are RSA key pairs, so you need perform this command only once, even if you have special-usage RSA key pairs. |

**Note** This command requires you to create a challenge password that is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

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 pki enroll** command is issued.)

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 pki 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: <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 pki enroll** command is not saved in the router configuration. If your router reboots after you issue the **crypto pki enroll** command but before you receive the certificates, you must reissue the command.

---



## Step 8—Save the Configuration

This topic describes how to save your configuration.

### Step 8: Save the Configuration

Cisco.com

Site 1: 10.0.1.0  
Router A: 172.30.1.2  
Internet  
Router B: 172.30.2.2  
Site 2: 10.0.2.0  
CA 172.30.1.51  
VPNCA

```
RouterA# copy running-config startup-config
```

- Saves the router running configuration to NVRAM

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5-17

Use the **copy system:running-config nvram:startup-config** command to save your configuration. This command includes saving RSA keys to private NVRAM. RSA keys are *not* saved with your configuration when you use a **copy system:running-config rep:** or **copy system:running-config tftp:** command.

## Step 9—Monitor and Maintain CA Interoperability

This topic covers monitoring and maintenance of CA support.

### Step 9: Monitor and Maintain CA Interoperability

Cisco.com

**The following steps are optional, depending on your particular requirements:**

- **Request a CRL.**
- **Delete RSA keys from your router.**
- **Delete certificates from the configuration.**
- **Delete the public keys from the peer.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—5-18

The following tasks are optional, depending on your particular requirements:

- Requesting a CRL
- Querying a CRL
- Deleting RSA keys from your router
- Deleting the public keys from a peer
- Deleting certificates from the configuration
- Viewing keys and certificates

## Requesting a CRL

You can request a certificate revocation list (CRL) only if your CA does not support a registration authority (RA). The following description and task applies only when the CA does not support an RA.

When your router receives a certificate from a peer, your router downloads a CRL from the CA. Your router then checks the CRL to make sure that the certificate that 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 certificate of the peer 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 certificate of the peer—unless you include the **cr1 optional** command in your configuration. If you use the **cr1 optional** command, your router will still try to obtain a CRL, but if it cannot obtain a CRL it can still accept the certificate of the peer.

A CRL can be reused with subsequent certificates until the CRL expires if query mode is off. If your router receives a peer certificate after the applicable CRL has expired, the router will download the new CRL.

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 **cr1 optional** command is enabled. The **cr1 optional** command only specifies that when the router cannot obtain the CRL, the router is not forced to reject a peer certificate outright.

If your router has a CRL that has not yet expired, but you suspect that the contents of the CRL are out of date, you can request that the latest CRL be downloaded immediately to replace the old CRL.

To request immediate download of the latest CRL, use the command shown in the table in global configuration mode.

| Command                                                      | Purpose                                                                                                                           |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Router(config)# <b>crypto pki cr1 request</b><br><i>name</i> | Requests an updated CRL.<br><br>This command replaces the currently stored CRL at your router with the newest version of the CRL. |

## Deleting RSA Keys from Your Router

Under certain circumstances you may want to delete the RSA keys from your router. 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 RSA keys from your router, use the command shown in the table in global configuration mode.

| Command                                       | Purpose                            |
|-----------------------------------------------|------------------------------------|
| Router(config)# <b>crypto key zeroize rsa</b> | Deletes the RSA keys from a router |

After you delete the RSA keys from a router, you should also complete these two additional tasks:

- Ask the CA administrator to revoke the certificates for your router at the CA; you must supply the challenge password that you created when you originally obtained the router certificates with the **crypto pki enroll** command.
- Manually remove the router certificates from the router configuration.

## Deleting Certificates from the Configuration

If the need arises, you can delete certificates that are saved at your router. Your router saves its own certificates, the certificate of the CA, and any RA certificates (unless you put the router into query mode).

To delete your router certificates or RA certificates from the router configuration, use the commands shown in the table in global configuration mode.

|               | Command                                                                  | Command                                                                                                                       |
|---------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router# <b>show crypto pki certificates</b>                              | Displays the certificates stored on your router; note (or copy) the serial number of the certificate that you wish to delete. |
| <b>Step 2</b> | Router(config)# <b>crypto pki certificate chain name</b>                 | Enters certificate chain configuration mode.                                                                                  |
| <b>Step 3</b> | Router(config-cert-cha)# <b>no certificate certificate-serial-number</b> | Deletes the certificate.                                                                                                      |

## Deleting the Public Keys from a Peer

Under certain circumstances you may want to delete the RSA public keys of other peers from your router configuration. For example, if you no longer trust the integrity of the public key of a peer, you should delete the key.

To delete the RSA public key from a peer, use the commands shown in the table, beginning in global configuration mode.

|               | Command                                                                                                                                                                       | Command                                                                                                  |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>crypto key pubkey-chain rsa</b>                                                                                                                            | Enters public key configuration mode.                                                                    |
| <b>Step 2</b> | Router(config-pubkey-c)# <b>no named-key key-name [encryption   signature]</b><br>or<br>Router(config-pubkey-c)# <b>no addressed-key key-address [encryption   signature]</b> | Deletes a remote peer RSA public key. Specify the FQDN of the peer or the IP address of the remote peer. |
| <b>Step 3</b> | Router(config-pubkey-c)# <b>exit</b>                                                                                                                                          | Returns to global configuration mode.                                                                    |

To delete the CA certificate, you must remove the entire CA trustpoint, which also removes all certificates associated with the CA—the certificate of your router, the CA certificate, and any RA certificates. To remove a CA trustpoint, use the command shown in the table in global configuration mode.

| Command                                              | Command                                                                    |
|------------------------------------------------------|----------------------------------------------------------------------------|
| Router(config)# <b>no crypto pki trustpoint name</b> | Deletes all trustpoint information and certificates associated with the CA |

# Step 10—Verify the CA Support Configuration

This topic describes how to verify your configuration of CA support.

## Step 10: Verify the CA Support Configuration

Cisco.com

```

router#
show crypto pki certificates

```

- View any configured CA or RA certificates

```

router#
show crypto key {mypubkey | pubkey-chain}
rsa

```

- View RSA keys for your router and other IPsec peers enrolled with a CA

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-19

To view keys and certificates, use the commands shown in the table in EXEC mode.

|               | Command                                                                               | Command                                                                                                                                                                                      |
|---------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router# <b>show crypto key mypubkey rsa</b>                                           | Displays RSA public keys of your router.                                                                                                                                                     |
| <b>Step 2</b> | Router# <b>show crypto key pubkey-chain rsa</b>                                       | Displays a list of all the RSA public keys stored on your router. These include the public keys of peers that have sent your router their certificates during peer authentication for IPsec. |
| <b>Step 3</b> | Router# <b>show crypto key pubkey-chain rsa [name key-name   address key-address]</b> | Displays details of a particular RSA public key stored on your router.                                                                                                                       |
| <b>Step 4</b> | Router# <b>show crypto pki certificates</b>                                           | Displays information about your certificate, the CA certificate, and any RA certificates.                                                                                                    |
| <b>Step 5</b> | Router# <b>show crypto ca roots</b>                                                   | Displays the CA roots configured in the router.                                                                                                                                              |

**Note** The **show crypto ca roots** command can be implemented only when multiple CAs are configured in the router.

The following example illustrates the result of the **show crypto ca certificates** command:

```
RouterA# show crypto pki certificates VPNCA
```

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  | 10.0.0.1   | 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 certificates of peers: 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 keys of the peers would show *C* in the code column but would all have to be manually configured.

## CA Support Configuration Example

Cisco.com

```
RouterA# show running-config
!
hostname RouterA
!
ip domain-name cisco.com
!
crypto pki trustpoint VPNCA
 enrollment mode ra
 enrollment url http://vpnca:80
 query url ldap://vpnca
 crl optional
crypto pki certificate chain entrust
certificate 37C6EAD6
 30820299 30820202 A0030201 02020437 C6EAD630 0D06092A
 864886F7 0D010105
(Certificates concatenated)
```

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5.20

The figure displays the running configuration of a router properly configured for CA support.



# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Configuration steps include these:**
  - Router preparation
    - Date and time
    - NVRAM
    - Host name
    - Domain
  - Generating RSA keys
  - Declaring and authenticating certificate authorities
  - Requesting your own certificate
  - Verifying, monitoring, and saving the CA configuration.
- **Certificates normally stored on router include the router certificate, CA certificate, root certificates, RA certificates.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.21

## Summary (Cont.)

Cisco.com

- **The router assigns an FQDN to the keys and certificates used by IPsec.**
- **RSA key pairs are used to sign and encrypt IKE key management messages and are required before you can obtain a certificate for your router.**
- **There are two RSA key types used general-purpose keys and special-usage keys.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.22



## Lesson 3

---

# Configuring ISAKMP and IPsec on Cisco Routers

---

## Overview

The next step in enabling certificate authority (CA) support is to configure Internet Security Association and Key Management Protocol (ISAKMP) and IPsec parameters gathered earlier in the process. This lesson guides you through the process of configuring ISAKMP and IPsec to support CAs.

## Objectives

Upon completing this lesson, you will be able to configure Cisco IOS software ISAKMP and IPsec policies with digital certificates. This ability includes being able to meet these objectives:

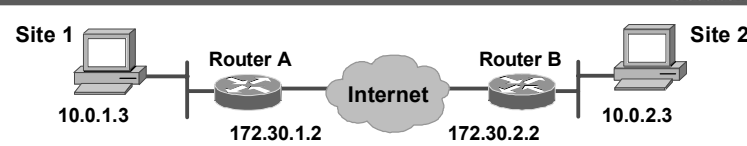
- Enable (or disable) ISAKMP
- Create ISAKMP policies
- Set the ISAKMP identity to address or host name
- Test and verify the ISAKMP configuration
- Configure transform set suites
- Configure global IPsec SA lifetimes
- Configure crypto ACLs
- Configure crypto maps
- Apply the crypto maps to the terminating or originating interface

# Step 1—Enable or Disable ISAKMP

This topic describes how to enable or disable ISAKMP.

## Step 1: Enable or Disable ISAKMP

Cisco.com



```
router(config)#
[no] crypto isakmp enable
```

```
RouterA(config)# no crypto isakmp enable
RouterA(config)# crypto isakmp enable
```

- Globally enables or disables ISAKMP at your router.
- ISAKMP is enabled by default.
- ISAKMP is enabled globally for all interfaces at the router.
- Use the **no** form of the command to disable ISAKMP.
- An ACL can be used to block ISAKMP on a particular interface.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.4

ISAKMP is enabled by default. ISAKMP does not have to be enabled for individual interfaces, but it is enabled globally for all interfaces at the router.

If you do not want ISAKMP to be used with your IPsec implementation, you can disable it at all IPsec peers.

If you disable ISAKMP, you will have to make these concessions at the peers:

- You must manually specify all the IPsec security associations (SAs) in the crypto maps at all peers.
- The IPsec SAs of the peers will never time out for a given IPsec session.
- During IPsec sessions between the peers, the encryption keys will never change.
- Antireplay services will not be available between the peers.
- Certificate authority (CA) support cannot be used.

To disable or enable ISAKMP, use one of the commands shown in the table in global configuration mode.

| Command                                        | Purpose         |
|------------------------------------------------|-----------------|
| Router(config)# <b>no crypto isakmp enable</b> | Disables ISAKMP |
| Router(config)# <b>crypto isakmp enable</b>    | Enables 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 (DoS) attacks by using an access control list (ACL) statement that blocks UDP port 500 on the interfaces.

## Step 2—Create ISAKMP Policies

This topic describes the process of creating ISAKMP policies.

### Step 2: Create ISAKMP Policies

Cisco.com



```
router(config)#
crypto isakmp policy priority
```

- Defines an ISAKMP policy, which is a set of parameters used during ISAKMP negotiation
- Invokes the config-isakmp command mode

```
RouterA(config)# crypto isakmp policy 110
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.6

You must create ISAKMP policies at each peer. An ISAKMP policy defines a combination of security parameters to be used during the ISAKMP negotiation.

There are five parameters to define in each ISAKMP policy, as shown in the table.

| Parameter                            | Accepted Values                                                                                                                  | Keyword                                               | Default Value          |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|------------------------|
| Encryption algorithm                 | Data Encryption Standard (DES) 56-bit<br>Triple-DES (3DES) 168-bit<br>Advanced Encryption Standard (AES) 128, 192, 256 bits      | <b>des</b><br><b>3des</b><br><b>aes</b>               | des                    |
| Hash algorithm                       | Secure Hash Algorithm-1 (SHA-1 ; Hash-Based Message Authentication Code [HMAC] variant)<br>Message Digest 5 (MD5 ; HMAC variant) | <b>sha</b><br><b>md5</b>                              | sha                    |
| Authentication method                | RSA signatures<br>RSA encrypted nonces<br>Pre-shared keys                                                                        | <b>rsa-sig</b><br><b>rsa-encr</b><br><b>pre-share</b> | rsa-sig                |
| Diffie-Hellman (DH) group identifier | 768-bit DH<br>1024-bit DH<br>1536-bit DH                                                                                         | <b>1</b><br><b>2</b><br><b>5</b>                      | 1                      |
| Lifetime of the SA                   | Number of seconds                                                                                                                |                                                       | 86,400 seconds (1 day) |

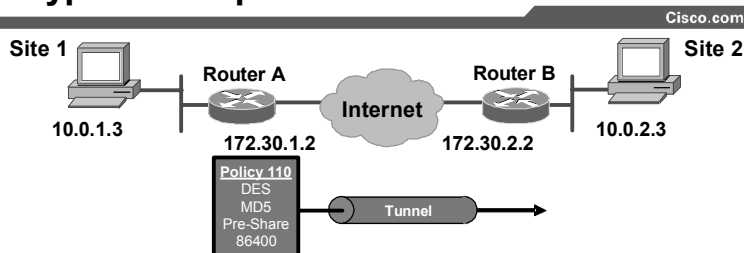
These parameters apply to the ISAKMP negotiations when the ISAKMP SA is established.

You can create multiple ISAKMP policies, each with a different combination of parameter values. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).

You can configure multiple policies on each peer—but at least one of these policies must contain exactly the same encryption, hash, authentication, and DH parameter values as one of the policies on the remote peer.

If you do not configure any policies, your router will use the default policy, which is always set to the lowest priority and which contains the default value of each parameter.

## Create ISAKMP Policies with the `crypto isakmp` Command



`router(config)#`

```
crypto isakmp policy priority
```

- Defines the parameters within the ISAKMP 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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5.6

To configure a policy, use the commands shown in the table, beginning in global configuration mode.

|               | Command                                                                             | Purpose                                                                                                                                                                                     |
|---------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>Router(config)# crypto isakmp policy priority</code>                          | Identifies the policy to create. (Each policy is uniquely identified by the priority number that you assign.)<br><br>(This command puts you into ISAKMP policy configuration command mode.) |
| <b>Step 2</b> | <code>Router(config-isakmp)# encryption {des   3des   aes}</code>                   | Specifies the encryption algorithm.                                                                                                                                                         |
| <b>Step 3</b> | <code>Router(config-isakmp)# hash {sha   md5}</code>                                | Specifies the hash algorithm.                                                                                                                                                               |
| <b>Step 4</b> | <code>Router(config-isakmp)# authentication {rsa-sig   rsa-encr   pre-share}</code> | Specifies the authentication method.                                                                                                                                                        |
| <b>Step 5</b> | <code>Router(config-isakmp)# group {1   2   5}</code>                               | Specifies the DH group identifier.                                                                                                                                                          |
| <b>Step 6</b> | <code>Router(config-isakmp)# lifetime seconds</code>                                | Specifies the lifetime of the SA.                                                                                                                                                           |
| <b>Step 7</b> | <code>Router(config-isakmp)# end</code>                                             | Exits ISAKMP policy configuration command mode.                                                                                                                                             |
| <b>Step 8</b> | <code>Router# show crypto isakmp policy</code>                                      | (Optional) Displays all existing ISAKMP policies.                                                                                                                                           |

If you do not specify a value for a parameter, the default value is assigned.

**Note** The default policy and the default values for configured policies do not show up in the configuration when you issue a **show running** command. Instead, to see the default policy and any default values within configured policies, use the **show crypto isakmp policy** command.




## Step 3—Set the ISAKMP Identity Address or Host Name

This topic describes how to set the ISAKMP identity by address or host name.

### Configure ISAKMP Identity

Cisco.com



```
router(config)#
crypto isakmp identity {address | hostname}
```

- Defines whether ISAKMP identity is done by IP address or host name
- Use consistently across ISAKMP peers

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.7

You should set the ISAKMP identity for each peer that uses pre-shared keys in an ISAKMP policy.

When two peers use ISAKMP to establish IPSec SAs, each peer sends its identity to the remote peer. Each peer sends either its host name or its IP address, depending on how you have set the ISAKMP identity of the router.

By default, the ISAKMP identity for each peer is the IP address of the peer. If appropriate, you could change the identity to be the peer host name instead. As a general rule, set the identities of all peers the same way—either all peers should use their IP addresses or all peers should use their host names. If some peers use their host names and some peers use their IP addresses to identify themselves to each other, ISAKMP negotiations could fail if the identity of a remote peer is not recognized and a Domain Name System (DNS) lookup is unable to resolve the identity.

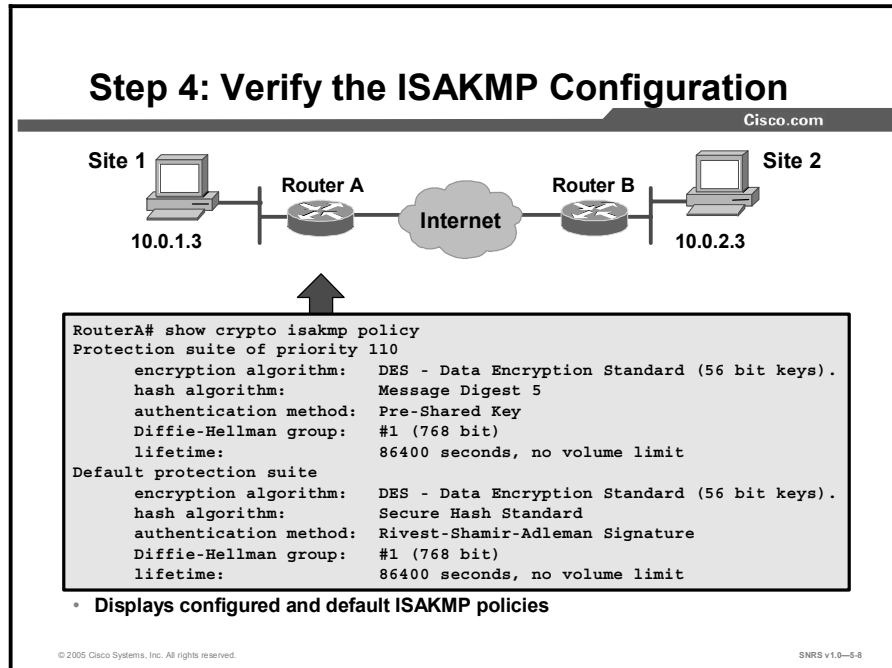
To set the ISAKMP identity of a peer, use the commands shown in the table in global configuration mode.

|               | <b>Command</b>                                                                         | <b>Purpose</b>                                                                                                                                                                                                                                                                 |
|---------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>crypto isakmp identity</b> { <b>address</b>   <b>hostname</b> }     | At the local peer: Specifies the ISAKMP identity of the peer by IP address or by host name.                                                                                                                                                                                    |
| <b>Step 2</b> | Router(config)# <b>ip host hostname</b> <i>address1</i> [ <i>address2...addressN</i> ] | At all remote peers: If the local peer ISAKMP identity was specified using a host name, maps the host name of the peer to its IP address or addresses at all the remote peers. (This step might be unnecessary if the host name or address is already mapped in a DNS server.) |

Remember to repeat these tasks at each peer.

## Step 4—Test and Verify the ISAKMP Configuration

This topic describes how to verify your ISAKMP configurations.



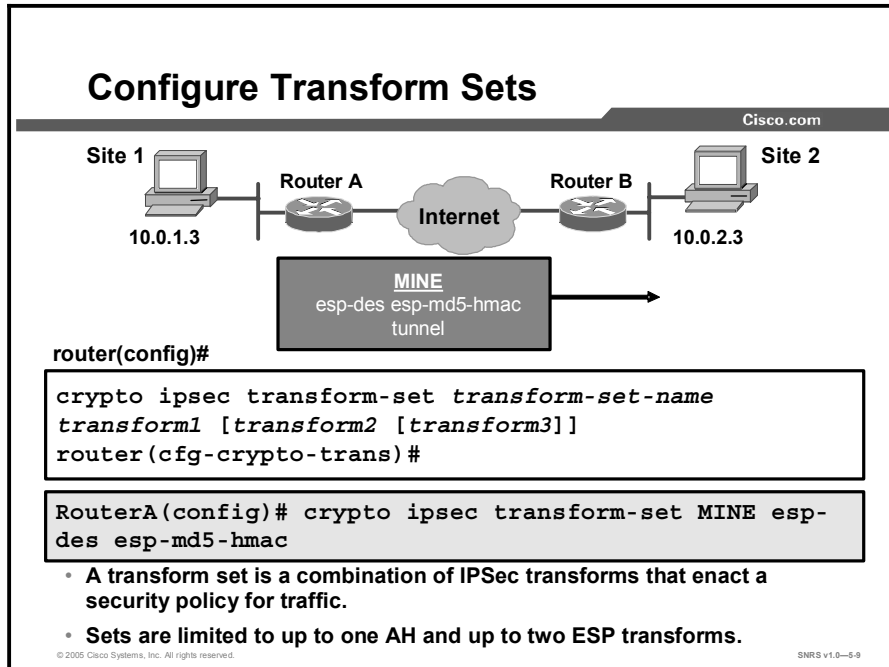
You can use the **show crypto isakmp policy** command to display configured and default policies. The resultant ISAKMP policy for RouterA is as follows and as shown in the figure. The RouterB configuration is identical.

```
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
```

## Step 5—Configure Transform Set Suites

This topic describes the first major step in configuring Cisco IOS software IPsec, which is to use the IPsec security policy to define a transform set.



A transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can specify multiple transform sets and then specify one or more of these 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 the ACL of that crypto map entry.

During IPsec SA negotiations with Internet Key Exchange (IKE), 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 will be applied to the protected traffic as part of the IPsec SAs of both peers.

With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.

If you change a transform set definition, the change is applied only to crypto map entries that reference the transform set. The change is applied to existing SAs, but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

To define a transform set, use the commands shown in the table starting in global configuration mode.

|               | Command                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                |
|---------------|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>crypto ipsec transform-set</b><br><i>transform-set-name transform1 [transform2<br/>[transform3]]</i> | Defines a transform set.<br><br>There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the <b>crypto ipsec transform-set</b> command.<br><br>This command puts you into crypto transform configuration mode. |
| <b>Step 2</b> | Router(cfg-crypto-tran)# <b>mode [tunnel   transport]</b>                                                               | (Optional) Changes the mode associated with the transform set. The transport mode setting is applicable only to traffic whose source and destination addresses are the IPsec peer addresses; it is ignored for all other traffic. The default mode is tunnel.                                          |
| <b>Step 3</b> | Router(cfg-crypto-tran)# <b>exit</b>                                                                                    | Exits crypto transform configuration mode.                                                                                                                                                                                                                                                             |

The table shows the allowed transform combinations.

| Transform Type                                                                   | Transform                                  | Description                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Header (AH) transform<br>(Choose up to one.)                      | ah-md5-hmac<br>ah-sha-hmac                 | AH with the MD5 (HMAC variant) authentication algorithm<br><br>AH with the SHA (HMAC variant) authentication algorithm                                                                                            |
| Encapsulating Security Payload (ESP) encryption transform<br>(Choose up to one.) | esp-des<br>esp-3des<br>esp-null<br>esp-aes | ESP with the 56-bit DES encryption algorithm<br><br>ESP with the 168-bit DES encryption algorithm (3DES)<br><br>Null encryption algorithm<br><br>ESP encryption with 128-, 192-, or 256-bit encryption algorithm. |
| ESP authentication transform<br>(Choose up to one.)                              | esp-md5-hmac<br>esp-sha-hmac               | ESP with the MD5 (HMAC variant) authentication algorithm<br><br>ESP with the SHA (HMAC variant) authentication algorithm                                                                                          |
| IP compression transform                                                         | comp-lzs                                   | IP compression with the Lempel-Ziv-STAC (LZS) algorithm.                                                                                                                                                          |

## Edit Transform Sets

Complete 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 the global configuration.
- Step 3** Re-enter 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 that it works properly.

Transform sets are negotiated during quick mode in IKE Phase 2 using the transform sets that 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 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 the Router A transform sets is compared against each of the Router B transform sets in succession. Router A transform sets 10, 20, and 30 are compared with Router B transform set 40. The result is no match. All of the Router A transform sets are then compared against the Router B transform sets. Ultimately, Router A transform set 30 matches Router B transform set 60. When such a transform set is found, it is selected and is applied to the protected traffic as part of the IPSec SAs of both peers. IPSec peers agree on one transform proposal per SA (unidirectional).

## Step 6—Configure Global IPsec SA Lifetimes

This topic describes how to configure global SA lifetimes.

### crypto ipsec security-association lifetime Command

Cisco.com



```
router(config)#
crypto ipsec security-association lifetime
 {seconds seconds | kilobytes kilobytes}
```

```
RouterA(config)# crypto ipsec security-association
lifetime seconds 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.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.10

You can change the global lifetime values that are used when negotiating new IPsec SAs. (These global lifetime values can be overridden for a particular crypto map entry).

These lifetimes only apply to SAs established via IKE. Manually established SAs do not expire.

There are two lifetimes: a timed lifetime and a traffic-volume lifetime. An SA expires after the first of these lifetimes is reached. The default lifetimes are 3600 seconds (one hour) and 4,608,000 kilobytes (10 Mbps for one hour per second for one hour).

If you change a global lifetime, the new lifetime value will not be applied to currently existing SAs, but will be used in the negotiation of subsequently established SAs. If you wish to use the new values immediately, you can clear all or part of the SA database. Refer to the **clear crypto sa** command for more details.

IPsec SAs use one or more shared secret keys. These keys and their SAs time out together.

The command syntax is as follows:

```
crypto ipsec security-association lifetime seconds seconds
```

- Changes the global timed lifetime for IPsec SAs. This command causes the SA to time out after the specified number of seconds have passed.

or

```
crypto ipsec security-association lifetime kilobytes kilobytes
```

- Changes the global traffic-volume lifetime for IPsec SAs. This command causes the SA to time out after the specified amount of traffic (in kilobytes) has passed through the IPsec “tunnel” using the SA.

## 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 an SA expires, a new one is negotiated without interrupting the data flow.**

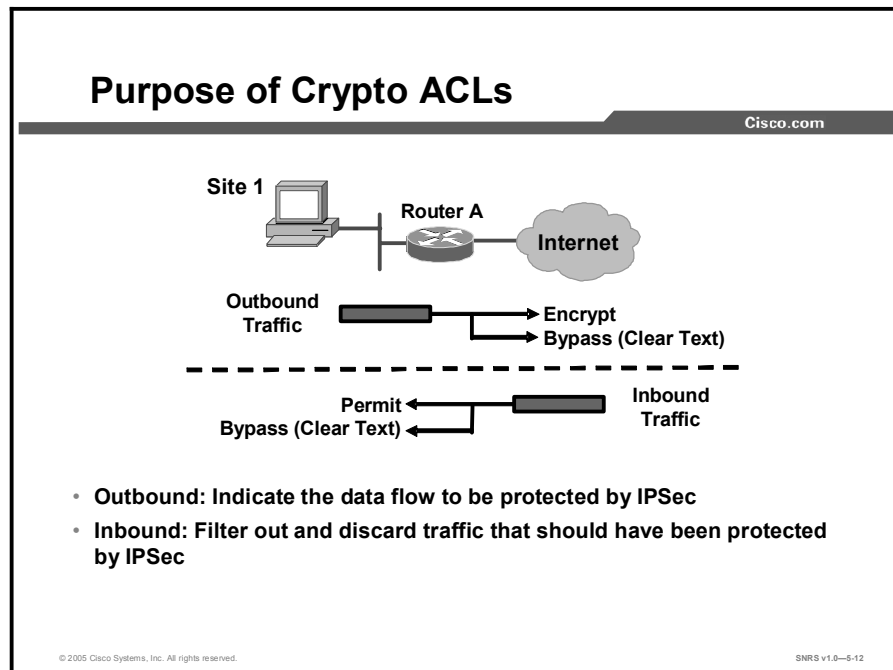
© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5-11

The figure shows an example of a global SA lifetime. A new SA will be negotiated after 2700 seconds (45 minutes).



## Step 7—Configure Crypto ACLs

Crypto ACLs are used to define which IP traffic is or is not protected by IPSec. This topic describes how to configure crypto ACLs.



Crypto ACLs are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. (These ACLs are not the same as regular ACLs, which determine which traffic to forward or block at an interface.) For example, ACLs can be created to protect all IP traffic between subnet A and subnet Y or Telnet traffic between host A and host B.

The ACLs themselves are not specific to IPSec. It is the crypto map entry referencing the specific ACL that defines whether IPSec processing is applied to the traffic matching a **permit** statement in the ACL.

Crypto ACLs associated with IPSec crypto map entries have four primary functions:

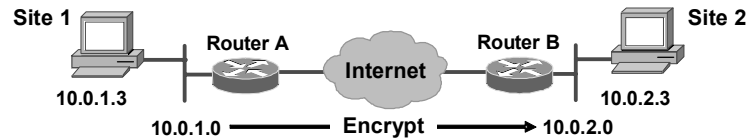
- Select outbound traffic to be protected by IPSec (permit equals protect).
- Indicate the data flow to be protected by the new SAs (specified by a single **permit** entry) when initiating negotiations for IPSec SAs.
- Process inbound traffic to filter out and discard traffic that should have been protected by IPSec.
- Determine whether or not to accept requests for IPSec SAs on behalf of the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is done only for **ipsec-isakmp** crypto map entries.) To be accepted, if the peer initiates the IPSec negotiation, it must specify a data flow that is permitted by a crypto ACL associated with an **ipsec-isakmp** crypto map entry.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to 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.

Later, you will associate the crypto ACLs to particular interfaces when you configure and apply crypto map sets to the interfaces.

## Extended IP ACLs for Crypto ACLs

Cisco.com



router(config)#

```
access-list access-list-number [dynamic dynamic-name
 [timeout minutes]] {deny | permit} protocol source
 source-wildcard destination destination-wildcard
 [precedence precedence] [tos tos] [log]
```

```
RouterA(config)# access-list 110 permit tcp 10.0.1.0
 0.0.0.255 10.0.2.0 0.0.0.255
```

- Define which IP traffic will be protected by encryption
- Permit = encrypt, deny = do not encrypt

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5-13

To create crypto ACLs, use the following command in global configuration mode:

```
Router(config)# access-list access-list-number {deny | permit}
 protocol source source-wildcard destination destination-wildcard
 [log]
```

- Specifies conditions to determine which IP packets will be protected.

**Note** It is recommended that you configure mirror-image crypto ACLs for use by IPSec and that you avoid using the **any** keyword.

or

```
Router(config)# ip access-list extended name
```

- Follow with **permit** and **deny** statements as appropriate.

| Command                              | Description                                                                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>permit</b>                        | Causes all IP traffic that matches the specified conditions to be protected by encryption, using the policy described by the corresponding crypto map entry |
| <b>deny</b>                          | Instructs the router to route traffic in the clear                                                                                                          |
| <i>source</i> and <i>destination</i> | Networks, subnets, or hosts                                                                                                                                 |
| <i>protocol</i>                      | Indicates which IP packet type or types 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.

---

**Caution** It is recommended that you avoid using the **any** keyword to specify source or destination addresses. The **permit any any** statement is strongly discouraged, because 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, Network Time Protocol (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.

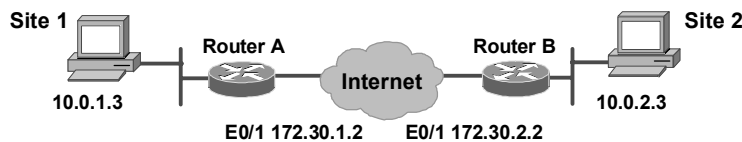
In a later step, you will associate a crypto ACL to a crypto map, which in turn is assigned to a specific interface.

## Defining Mirror-Image Crypto ACLs at Each IPsec Peer

It is recommended that for every crypto ACL specified for a static crypto map entry that you define at the local peer, you define a mirror-image crypto ACL at the remote peer. This practice ensures that traffic that has IPsec protection applied locally can be processed correctly at the remote peer. (The crypto map entries themselves must also support common transforms and must refer to the other system as a peer.)

## Configure Symmetrical Peer Crypto ACLs

Cisco.com



```
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.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-5.14

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 criteria of the ACL 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 the Router A 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 Router A 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 Router A is evaluated as follows:

- source = hosts on 10.0.2.0 network
- permit = hosts on 10.0.1.0 network

## Step 8—Configure Crypto Maps

This topic describes how to configure crypto maps.

### Configure IPsec Crypto Maps

Cisco.com

```
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.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-15

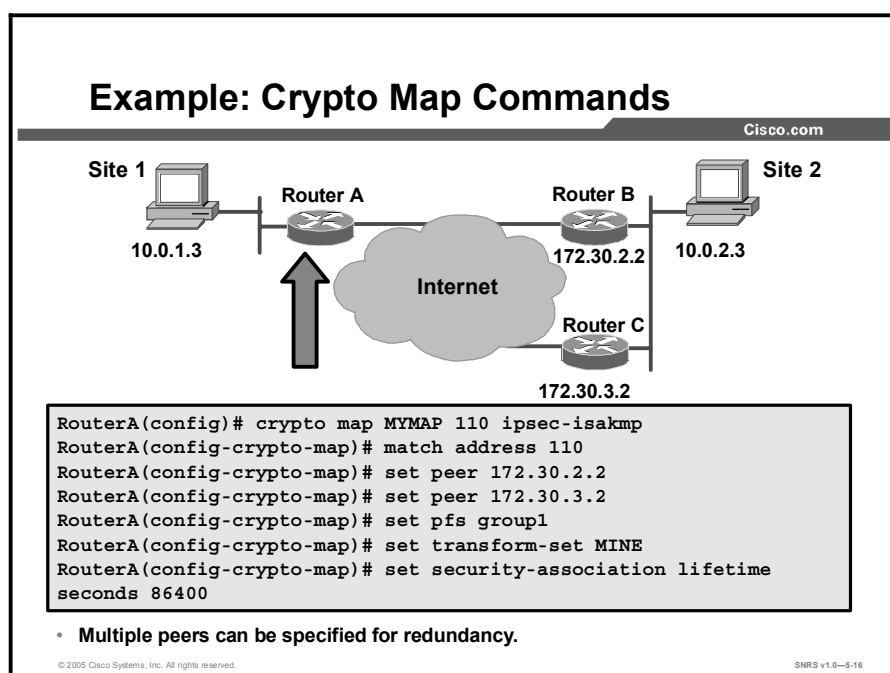
You must use the **crypto map** global configuration command to create or modify a crypto map entry and enter crypto map configuration mode. Set the crypto map entries referencing dynamic maps to be the lowest-priority entries in a crypto map set (that is, having the highest sequence numbers). Use the **no** form of this command to delete a crypto map entry or set. The command syntax is as follows:

```
Router(config)# crypto map map-name seq-num ipsec-manual
Router(config)# crypto map map-name seq-num ipsec-isakmp [dynamic
dynamic-map-name]
Router(config)# no crypto map map-name [seq-num]
```

A description of each is as follows:

- **map-name:** The name that you assign to the crypto map set.
- **seq-num:** The number that you assign to the crypto map entry.
- **ipsec-manual:** Indicates that ISAKMP will not be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry.
- **ipsec-isakmp:** Indicates that ISAKMP will be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry.
- **Dynamic:** (Optional) Specifies that this crypto map entry references a pre-existing 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.

## Example: Crypto Map Commands



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                                                                                                                                                                                                            |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>set</b>                                                   | Used with the <b>peer</b> , <b>pfs</b> , <b>transform-set</b> , and <b>security-association</b> commands.                                                                                                              |
| <b>peer</b> [ <i>hostname</i>   <i>ip-address</i> ]          | Specifies the allowed IPsec peer by IP address or host name.                                                                                                                                                           |
| <b>pfs</b> [ <i>group1</i>   <i>group2</i>   <i>group5</i> ] | Specifies DH group 1, group 2, or group 5.                                                                                                                                                                             |
| <b>transform-set</b> [ <i>set_name(s)</i> ]                  | Specifies 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. |
| <b>security-association lifetime</b>                         | Sets SA lifetime parameters in seconds or kilobytes.                                                                                                                                                                   |
| <b>match address</b> [ <i>access-list-id</i>   <i>name</i> ] | Identifies the extended ACL by its name or number. The value should match the <i>access-list-number</i> or <i>name</i> argument of a previously defined IP-extended ACL being matched.                                 |
| <b>no</b>                                                    | Deletes commands entered with the <b>set</b> command.                                                                                                                                                                  |
| <b>exit</b>                                                  | 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 SAs established by that particular crypto map entry are only for a single data flow. To be able to support multiple manually established SAs 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 9—Apply Crypto Map to Interface

This topic describes how to apply crypto map to an interface. This is the last step in configuring IPSec.

### Applying Crypto Map to Interface

Cisco.com

```

router(config-if)#
crypto map map-name
RouterA (config) # interface ethernet0/1
RouterA (config-if) # crypto map MYMAP

```

- Applies the crypto map to outgoing interface
- Activates the IPSec policy

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-17

You need to apply a crypto map set to each interface through which IPSec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface traffic against the crypto map set and to use the specified policy during connection or SA negotiation on behalf of traffic to be protected by encryption.

To apply a crypto map set to an interface, use the command shown in the table in interface configuration mode.

| Command                                              | Purpose                                  |
|------------------------------------------------------|------------------------------------------|
| Router(config-if)# <b>crypto map</b> <i>map-name</i> | Applies a crypto map set to an interface |

For redundancy, you could apply the same crypto map set to more than one interface. The default behavior is as follows:

- Each interface has its own piece of the SA database.
- The IP address of the local interface is used as the local address for IPSec traffic originating from or destined to that interface.

If you apply the same crypto map set to multiple interfaces for redundancy purposes, you need to specify an identifying interface. This action has the following effects:

- The per-interface portion of the IPSec SA database is established one time and shared for traffic through all the interfaces that share the same crypto map.
- The IP address of the identifying interface is used as the local address for IPSec traffic originating from or destined to those interfaces sharing the same crypto map set.

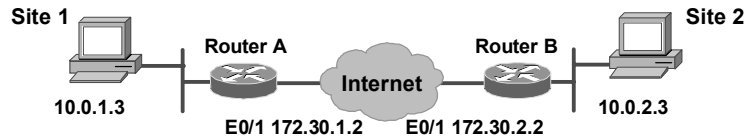
One suggestion is to use a loopback interface as the identifying interface.

To specify redundant interfaces and name an identifying interface, use the command shown in the table in global configuration mode.

| Command                                                                                       | Purpose                                                                                  |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Router(config)# <b>crypto map</b> <i>map-name</i><br><b>local-address</b> <i>interface-id</i> | Permits redundant interfaces to share the same crypto map, using the same local identity |

## IPSec Configuration Examples

Cisco.com



```
RouterA# show running config
crypto ipsec transform-set MINE esp-des
esp-md5-hmac
!
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
esp-md5-hmac
!
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-18

Consider the configuration example for Router A and Router B in the figure and the examples that follow. The examples are concatenated to show only 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 esp-md5-hmac
!
!
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 esp-md5-hmac
!
!
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
```

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **ISAKMP Policy configuration includes the following:**
  - Enabling or disabling ISAKMP
  - Creating IKE policies
  - Configuring pre-shared keys
  - Verifying the ISAKMP configuration
- **ISAKMP is enabled by default.**
- **You must create ISAKMP policies at each peer.**
- **The policy states which security parameters will be used to protect subsequent ISAKMP negotiations and mandates how the peers are authenticated.**
- **Each peer sends either its host name or its IP address.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.19

## Summary (Cont.)

Cisco.com

- **Configuring IPsec includes configuration of the following:**
  - Transform sets
  - Global IPsec SA lifetimes
  - Crypto ACLs
  - Crypto maps
  - Applying maps to interfaces
- **A transform set represents a certain combination of security protocols and algorithms.**
- **Crypto ACLs are used to define which IP traffic will be protected by crypto and which traffic will not be protected by encryption.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.20

## Summary (Cont.)

Cisco.com

- **For every crypto ACL specified for a static crypto map entry that you define at the local peer, you define a mirror-image crypto ACL at the remote peer.**
- **Crypto map entries created for IPsec set up SA parameters, tying together the various parts configured for IPsec.**
- **You need to apply a crypto map set to each interface through which IPsec traffic will flow.**

## Lesson 4

---

# Testing and Verifying an IPSec CA Configuration

---

## Overview

Testing and verification is crucial to the successful implementation of virtual private networks (VPNs). This lesson describes using Cisco IOS commands to verify and troubleshoot your VPN configurations. You will use commands to display Internet Security Association and Key Management Protocol (ISAKMP) and IPSec policies as well as crypto maps and the status of current security associations (SAs). You will then be able to view actual ISAKMP and IPSec negotiations and communications between the certificate authority (CA) and the router.

## Objectives

Upon completing this lesson, you will be able to verify the configuration is correctly configured. This ability includes being able to meet these objectives:

- Display configured ISAKMP policies
- Display configured transform sets
- Display the current state of the IPSec SAs
- View configured crypto maps
- Debug IPSec traffic using Cisco IOS software
- Debug ISAKMP traffic using Cisco IOS software
- Debug CA events with Cisco IOS software

# Step 1—Display Configured ISAKMP Policies

This topic describes how to display your ISAKMP policies.

## show crypto isakmp policy Command

Cisco.com

```
graph LR
 S1[Site 1
10.0.1.3] --- RA[Router A]
 RA --- I((Internet))
 I --- RB[Router B]
 RB --- S2[Site 2
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
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.4

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
```

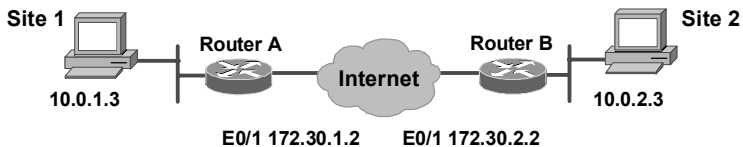


## Step 2—Display Configured Transform Sets

This topic describes how to display your transform set configurations.

### show crypto ipsec transform-set Command

Cisco.com



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 esp-md5-hmac }
will negotiate = { Tunnel, },
```

- View the currently defined transform sets

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.5

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 [transform-set-name]
```

| Command Parameter         | Description                                                                    |
|---------------------------|--------------------------------------------------------------------------------|
| <i>transform-set-name</i> | (Optional) Shows only the transform sets with the specified transform set name |

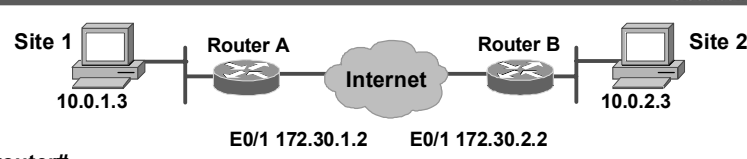
If no keyword is used, all transform sets configured at the router are displayed.

# Step 3—Display the Current State of IPsec SAs

This topic describes how to display the state of IPsec SAs.

## show crypto ipsec sa Command

Cisco.com



```

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

```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.6

Use the **show crypto ipsec sa EXEC** command to view the settings used by current SAs. If no keyword is used, all SAs are displayed. The command syntax is as follows:

**show crypto ipsec sa** [*map map-name* | **address** | **identity** | **detail**]

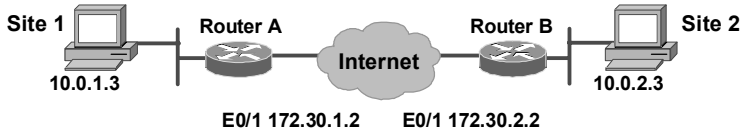
| Command                    | Description                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>map</b> <i>map-name</i> | (Optional) Shows any existing SAs created for the crypto map.                                                                                                        |
| <b>address</b>             | (Optional) Shows all the existing SAs, sorted by the destination address and then by protocol (Authentication Header [AH] or Encapsulating Security Protocol [ESP]). |
| <b>identity</b>            | (Optional) Shows only the flow information. It does not show the SA information.                                                                                     |
| <b>detail</b>              | (Optional) Shows detailed error counters. (The default is the high-level send-receive error counters.)                                                               |

## Step 4—View Configured Crypto Maps

This topic describes how to display your crypto maps.

### show crypto map Command

Cisco.com



```

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, }

```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.6-6-7

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                                                                 |
|-----------------------------------|-----------------------------------------------------------------------------|
| <b>interface</b> <i>interface</i> | (Optional) Shows only the crypto map set applied to the specified interface |
| <b>tag</b> <i>map-name</i>        | (Optional) Shows only the crypto map set with the specified map name        |

## Step 5—Debug IPsec Traffic

This topic describes the command used to debug IPsec.

### debug crypto ipsec Command

Cisco.com

```
router#
debug crypto ipsec
```

- Displays debug messages about all IPsec actions

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-5.8

To display IPsec events, use the **debug crypto ipsec** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug crypto ipsec
```

```
no debug crypto ipsec
```

The following is sample output from the **debug crypto ipsec** command. In this example, SAs have been successfully established.

```
Router# debug crypto ipsec
```

IPsec requests SAs between 172.21.114.123 and 172.21.114.67, on behalf of the **permit ip host 172.21.114.123 host 172.21.114.67** command. It prefers to use the transform set esp-des w/esp-md5-hmac, but it will also consider ah-sha-hmac.

```
00:24:30: IPSEC(sa_request): ,
 (key eng. msg.)
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123, dest= 172.21.114.67,
 src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 120s and 4608000kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
00:24:30: IPSEC(sa_request): ,
```

```
(key eng. msg.)
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123, dest= 172.21.114.67,
 src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1).,
 protocol= AH, transform= ah-sha-hmac ,
 lifedur= 120s and 4608000kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0.
```

Internet Key Exchange (IKE) asks for service provider interfaces (SPIs) from IPsec. For inbound SAs, IPsec controls its own SPI space.

```
00:24:34: IPSEC(key_engine): got a queue event...
00:24:34: IPSEC(spi_response): getting spi 3029740121d for SA
 from 172.21.114.67 to 172.21.114.123 for prot 3
00:24:34: IPSEC(spi_response): getting spi 5250759401d for SA
 from 172.21.114.67 to 172.21.114.123 for prot 2
```

IKE asks IPsec if it accepts the SA proposal. In this case, it will be the one sent by the local IPsec in the first place.

```
00:24:34: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) dest= 172.21.114.67,
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123,
 dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

After the proposal is accepted, IKE finishes the negotiations, generates the keying material, and then notifies IPsec of the new SAs (one SA for each direction).

```
00:24:35: IPSEC(key_engine): got a queue event...
```

The following output pertains to the inbound SA. The conn\_id value references an entry in the crypto engine connection table.

```
00:24:35: IPSEC(initialize_sas): ,
 (key eng. msg.) dest= 172.21.114.123,
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.67,
 dest_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 src_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 120s and 4608000 kb,
 spi= 0x120F043C(302974012), conn_id= 29, keysize= 0, flags= 0x4
```

The following output pertains to the outbound SA.

```
00:24:35: IPSEC(initialize_sas): ,
 (key eng. msg.)
src=http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/12
3tcr/123dbr/ 172.21.114.123, dest= 172.21.114.67,
 src_proxy= 172.21.114.123/255.255.255.255/0/0 (type=1),
 dest_proxy= 172.21.114.67/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-md5-hmac ,
 lifedur= 120s and 4608000kb,
 spi= 0x38914A4(59315364), conn_id= 30, keysize= 0, flags= 0x4
```

IPSec now installs the SA information in its SA database.

```
00:24:35: IPSEC(create_sa): sa created,
 (sa) sa_dest= 172.21.114.123, sa_prot= 50,
 sa_spi= 0x120F043C(302974012),
 sa_trans= esp-des esp-md5-hmac , sa_conn_id= 29
00:24:35: IPSEC(create_sa): sa created,
 (sa) sa_dest= 172.21.114.67, sa_prot= 50,
 sa_spi= 0x38914A4(59315364),
 sa_trans= esp-des esp-md5-hmac , sa_conn_id= 30
```

## Step 6—Debug ISAKMP Traffic

This topic describes how to debug ISAKMP events.

### debug crypto isakmp Command

Cisco.com

```
router#
debug crypto isakmp
```

- Displays debug messages about all ISAKMP actions

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.9

To display messages about ISAKMP events, use the **debug crypto isakmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
router# debug crypto isakmp
router# no debug crypto isakmp
```

The following is sample output from the **debug crypto isakmp** command for an ISAKMP peer that initiates an ISAKMP negotiation.

First, ISAKMP negotiates its own SA, checking for a matching ISAKMP policy.

```
Router# debug crypto isakmp
20:26:58: ISAKMP (8): beginning Main Mode exchange
20:26:58: ISAKMP (8): processing SA payload. message ID = 0
20:26:58: ISAKMP (8): Checking ISAKMP transform 1 against priority 10
policy
20:26:58: ISAKMP: encryption DES-CBC
20:26:58: ISAKMP: hash SHA
20:26:58: ISAKMP: default group 1
20:26:58: ISAKMP: auth pre-share
20:26:58: ISAKMP (8): atts are acceptable. Next payload is 0
```

ISAKMP has found a matching policy. Next, the ISAKMP SA is used by each peer to authenticate the other peer.

```
20:26:58: ISAKMP (8): SA is doing pre-shared key authentication
20:26:59: ISAKMP (8): processing KE payload. message ID = 0
20:26:59: ISAKMP (8): processing NONCE payload. message ID = 0
20:26:59: ISAKMP (8): SKEYID state generated
20:26:59: ISAKMP (8): processing ID payload. message ID = 0
20:26:59: ISAKMP (8): processing HASH payload. message ID = 0
20:26:59: ISAKMP (8): SA has been authenticated
```

Next, ISAKMP negotiates to set up the IPsec SA by searching for a matching transform set.

```
20:26:59: ISAKMP (8): beginning Quick Mode exchange, M-ID of 767162845
20:26:59: ISAKMP (8): processing SA payload. message ID = 767162845
20:26:59: ISAKMP (8): Checking IPsec proposal 1
20:26:59: ISAKMP: transform 1, ESP_DES
20:26:59: ISAKMP: attributes in transform:
20:26:59: ISAKMP: encaps is 1
20:26:59: ISAKMP: SA life type in seconds
20:26:59: ISAKMP: SA life duration (basic) of 600
20:26:59: ISAKMP: SA life type in kilobytes
20:26:59: ISAKMP: SA life duration (VPI) of
 0x0 0x46 0x50 0x0
20:26:59: ISAKMP: authenticator is HMAC-MD5
20:26:59: ISAKMP (8): atts are acceptable.
```

A matching IPsec transform set has been found at the two peers. Now the IPsec SA can be created (one SA is created for each direction).

```
20:26:59: ISAKMP (8): processing NONCE payload. message ID = 767162845
20:26:59: ISAKMP (8): processing ID payload. message ID = 767162845
20:26:59: ISAKMP (8): processing ID payload. message ID = 767162845
20:26:59: ISAKMP (8): Creating IPsec SAs
20:26:59: inbound SA from 155.0.0.2 to 155.0.0.1 (proxy
155.0.0.2 to 155.0.0.1)
20:26:59: has spi 454886490 and conn_id 9 and flags 4
20:26:59: lifetime of 600 seconds
20:26:59: lifetime of 4608000 kilobytes
20:26:59: outbound SA from 155.0.0.1 to 155.0.0.2
(proxy 155.0.0.1
to 155.0.0.2)
20:26:59: has spi 75506225 and conn_id 10 and flags 4
20:26:59: lifetime of 600 seconds
20:26:59: lifetime of 4608000 kilobytes
```



# Step 7—Debug CA Events with Cisco IOS Software

This topic describes how to view CA events using debug commands.

## debug CA Commands

Cisco.com

```
router#
debug crypto pki messages
```

- **Displays messages about the actual data being sent and received during public key infrastructure (PKI) transactions**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5.10

## The debug crypto pki messages Command

To display debugging messages for the details of the interaction (message dump) between the CA and the router, use the **debug crypto pki messages** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
Router# debug crypto pki messages
```

```
Router# no debug crypto pki messages
```

The **debug crypto pki messages** command displays messages about the actual data being sent and received during public key infrastructure (PKI) transactions. This command is internal for use by Cisco support personnel.

The following is sample output from the **debug crypto pki messages** command.

```
Router# debug crypto pki messages
```

```
Fingerprint: 2CFC6265 77BA6496 3AEFCB50 29BC2BF2
00:48:23:Write out pkcs#10 content:274
00:48:23:30 82 01 0E 30 81 B9 02 01 00 30 22 31 20 30 1E 06 09 2A 86
00:48:23:48 86 F7 0D 01 09 02 16 11 70 6B 69 2D 33 36 61 2E 63 69 73
00:48:23:63 6F 2E 63 6F 6D 30 5C 30 0D 06 09 2A 86 48 86 F7 0D 01 01
00:48:23:01 05 00 03 4B 00 30 48 02 41 00 DD 2C C6 35 A5 3F 0F 97 6C
```

```

00:48:23:11 E2 81 95 01 6A 80 34 25 10 C4 5F 3D 8B 33 1C 19 50 FD 91
00:48:23:6C 2D 65 4C B6 A6 B0 02 1C B2 84 C1 C8 AC A4 28 6E EF 9D 3B
00:48:23:30 98 CB 36 A2 47 4E 7E 6F C9 3E B8 26 BE 15 02 03 01 00 01
00:48:23:A0 32 30 10 06 09 2A 86 48 86 F7 0D 01 09 07 31 03 13 01 63
00:48:23:30 1E 06 09 2A 86 48 86 F7 0D 01 09 0E 31 11 14 0F 30 0D 30
00:48:23:0B 06 03 55 1D 0F 04 04 03 02 05 A0 30 0D 06 09 2A 86 48 86
00:48:23:F7 0D 01 01 04 05 00 03 41 00 2C FD 88 2C 8A 13 B6 81 88 EA
00:48:23:5C FD AE 52 8F 2C 13 95 9E 9D 8B A4 C9 48 32 84 BF 05 03 49
00:48:23:63 27 A3 AC 6D 74 EB 69 E3 06 E9 E4 9F 0A A8 FB 20 F0 02 03
00:48:23:BE 90 57 02 F2 75 8E 0F 16 60 10 6F BE 2B
00:48:23:Enveloped Data ...

00:48:23:30 80 06 09 2A 86 48 86 F7 0D 01 07 03 A0 80 30 80 02 01 00
00:48:23:31 80 30 82 01 0F 02 01 00 30 78 30 6A 31 0B 30 09 06 03 55
00:48:23:04 06 13 02 55 53 31 0B 30 09 06 03 55 04 08 13 02 43 41 31
00:48:23:13 30 11 06 03 55 04 07 13 0A 53 61 6E 74 61 20 43 72 75 7A
00:48:23:31 15 30 13 06 03 55 04 0A 13 0C 43 69 73 63 6F 20 53 79 73
00:48:23:74 65 6D 31 0E 30 0C 06 03 55 04 0B 13 05 49 50 49 53 55 31
00:48:23:Signed Data 1382 bytes
00:48:23:30 80 06 09 2A 86 48 86 F7 0D 01 07 02 A0 80 30 80 02 01 01
00:48:23:31 0E 30 0C 06 08 2A 86 48 86 F7 0D 02 05 05 00 30 80 06 09
00:48:23:2A 86 48 86 F7 0D 01 07 01 A0 80 24 80 04 82 02 75 30 80 06
00:48:23:02 55 53 31 0B 30 09 06 03 55 04 08 13 02 43 41 31 13 30 11
00:48:23:33 34 5A 17 0D 31 30 31 31 31 35 31 38 35 34 33 34 5A 30 22
00:48:23:31 20 30 1E 06 09 2A 86 48 86 F7 0D 01 09 02 16 11 70 6B 69
00:48:23:2D 33 36 61 2E 63 69 73 63 6F 2E 63 6F 6D 30 5C 30 0D 06 09
00:48:23:2A 86 48 86 F7 0D 01 01 01 05 00 03 4B 00 30 48 02 41 00 DD
00:48:23:2C C6 35 A5 3F 0F 97 6C 11 E2 81 95 01 6A 80 34 25 10 C4 5F
00:48:23:3D 8B 33 1C 19 50 FD 91 6C 2D 65 4C B6 A6 B0 02 1C B2 84 C1
00:48:23:86 F7 0D 01 01 01 05 00 04 40 C6 24 36 D6 D5 A6 92 80 5D E5
00:48:23:15 F7 3E 15 6D 71 E1 D0 13 2B 14 64 1B 0C 0F 96 BF F9 2E 05
00:48:23:EF C2 D6 CB 91 39 19 F8 44 68 0E C5 B5 84 18 8B 2D A4 B1 CD
00:48:23:3F EC C6 04 A5 D9 7C B1 56 47 3F 5B D4 93 00 00 00 00 00
00:48:23:00 00
00:48:24:Received pki message:1778 types

```

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Several show, clear , and debug commands are available to test and verify IPsec configurations.**
- **The show crypto isakmp policy command displays ISAKMP policies.**
- **The show crypto ipsec transform set command displays transform sets.**
- **The show crypto ipsec sa command display the state of SAS.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-11

## Summary (Cont.)

Cisco.com

- **The show crypto map command displays crypto maps.**
- **The debug crypto ipsec command displays debug messages about IPsec.**
- **The debug crypto isakmp command displays debug messages about ISAKMP.**
- **The debug crypto pki messages command displays during PKI transactions.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-12

# Module Summary

This topic summarizes the key points discussed in this module.

## Module Summary

Cisco.com

- **There are several steps involved in preparing for CA support.**
- **Configuration steps involve the following:**
  - Router preparation
  - RSA keys
  - CA servers and authentication
- **Configuring ISAKMP and IPsec**
- **Several show and debug commands are available for verification and troubleshooting.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-5-1

This module covered the preparation and configuration of the network for using CAs. The CA server role was discussed, and configuring the router to work with a CA was introduced. IKE and IPsec policies were configured, including RSA keys and a description of how to generate them. Several **show** and **debug** commands that are used to test and verify the configurations were introduced.

## Module 6

---

# Cisco IOS Remote Access Using Cisco Easy VPN

---

## Overview

Establishing a virtual private network (VPN) connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of both routers. The Cisco Easy VPN Remote feature eliminates much of this work by implementing the Cisco VPN Client client-server protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN Server. After the Cisco Easy VPN Server has been configured, a VPN connection can be created with minimal configuration on a Cisco Easy VPN Remote Client. This module describes the implementation of Cisco Easy VPN Remote, including server and client operations.

## Module Objectives

Upon completing this module, you will be able to plan, configure, operate, and troubleshoot IPsec VPNs using Cisco Easy VPN. This ability includes being able to meet these objectives:

- Describe how Cisco Easy VPN provides Cisco IOS remote access
- Configure a Cisco Easy VPN Server
- Configure the Cisco VPN Client 4.x
- Explain how to configure a Cisco access router for Cisco Easy VPN Remote from the Cisco IOS CLI



## Lesson 1

---

# Introducing Cisco Easy VPN

---

## Overview

This lesson provides an introduction to configuring and monitoring the Cisco Easy Virtual Private Network (VPN) Remote feature to create IPsec VPN tunnels between a supported router and an Easy VPN Server (Cisco IOS router, Cisco VPN 3000 Concentrator, or Cisco PIX Firewall) that supports this form of IPsec encryption and decryption.

## Objectives

Upon completing this lesson, you will be able to describe how Cisco Easy VPN provides Cisco IOS remote access. This ability includes being able to meet these objectives:

- Describe the role of each component of Cisco Easy VPN
- Describe the activities that occur in each of the seven steps in the Cisco Easy VPN Remote connection process
- Describe how to configure the Cisco Easy VPN Client to authenticate
- Describe how Cisco Easy VPN Client establishes an SA between peer IP addresses
- Describe how Cisco Easy VPN Server accepts the SA proposal and completes device authentication
- Describe how Cisco Easy VPN Server initiates an AAA username and password challenge
- Describe how parameters are downloaded to complete the mode configuration process
- Describe how Cisco Easy VPN completes the RRI process
- Describe how the VPN connection is completed

# Introduction to Cisco Easy VPN

This topic describes the Cisco Easy VPN and its two components.

## Cisco Easy VPN Components

Cisco.com

**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 headend 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 3000 Hardware Clients or Software Clients to act as remote VPN Clients**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.4

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN Server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 Concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client protocol.

After the Cisco Easy VPN Server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN Remote, such as a Cisco 800 Series router or a Cisco 1700 Series router. When the Easy VPN Remote initiates the VPN tunnel connection, the Cisco Easy VPN Server pushes the IPsec policies to the Easy VPN Remote and creates the corresponding VPN tunnel connection.



The Cisco Easy VPN Remote feature provides for automatic management of the following details:

- Negotiating tunnel parameters, such as addresses, algorithms, and lifetime
- Establishing tunnels according to the parameters that were set
- Automatically creating the Network Address Translation (NAT) or Port Address Translation (PAT) and associated access control lists (ACLs) that are needed, if any
- Authenticating users—that is, ensuring that users are who they say they are—by usernames, group names, and passwords
- Managing security keys for encryption and decryption
- Authenticating, encrypting, and decrypting data through the tunnel

Cisco Easy VPN consists of two components: Cisco Easy VPN Server and Cisco Easy VPN Remote.

## Cisco Easy VPN Server

Cisco Easy VPN Server enables Cisco IOS routers, Cisco 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 telecommuters, to access their headquarters intranet, where critical data and applications exist.

## Cisco Easy VPN Remote

Cisco 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. 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.com

- **Cisco IOS Software Release 12.2(8)T (Easy VPN Phase 1):** Provided support for Cisco VPN Client 4.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
- **Cisco IOS Software Release 12.3(2)T:** New attributes added to the server group, and the following commands, which correspond to the added attributes, added: access-restrict, firewall are-u-there, group-lock, include-local-lan, and save-password
- **Cisco IOS Software Release 12.3(4)T:** RADIUS support for user profiles, user-based policy control, session monitoring for VPN group access, backup-gateway list, and PFS added

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.5

This figure identifies Cisco 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 IOS Software Release 12.2(8)T (Easy VPN Phase 1):** Provided support for Cisco VPN Client 4.x software clients and hardware clients, mode configuration version 6 support, Extended Authentication (Xauth) Version 6 support, Internet Key Exchange (IKE) dead peer detection (DPD), split tunneling control, and group-based policy control
- **Cisco IOS Software Release 12.2(13) (Easy VPN Phase 1.1):** Added support for Advanced Encryption Standard (AES), IPSec NAT transparency, VPN Acceleration Module (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 Cisco 83x platforms
- **Cisco IOS Software Release 12.3(2)T:** New attributes added to the server group; the following commands, which correspond to the added attributes, added: **access-restrict**, **firewall are-u-there**, **group-lock**, **include-local-lan**, and **save-password**
- **Cisco IOS Software Release 12.3(4)T:** RADIUS support for user profiles, user-based policy control, session monitoring for VPN group access, backup-gateway list, and Perfect Forward Secrecy (PFS) added

## Cisco Easy VPN Remote Releases

Cisco.com

- **12.2(4)YA & 12.2(13T) (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

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.6

This figure identifies Cisco 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.

- **12.2(4)YA and 12.2(13T) (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, Cisco Router Web Setup (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 and 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 Cisco Router and Security Device Manager (SDM)
- **12.3(1)T (Phase 3.1):** Added support for AES, Easy VPN key garbled, and IP compression

## Cisco Easy VPN Remote Releases (Cont.)

Cisco.com

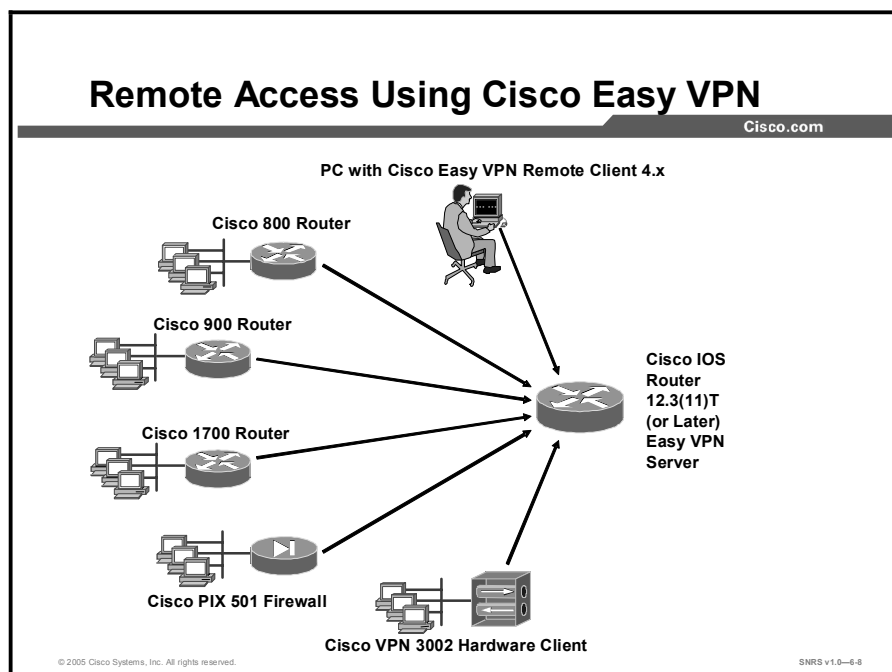
- **12.3(2)T:** Added support for type 6 password
- **12.3(4)T:** Added support for Save Password and Multiple Peer Backup
- **12.3(7)T:** IPSec DPD Periodic Message Option feature added
- **12.3(7)XR:** Introduced DPD with Stateless Failover (Object Tracking with Easy VPN)—Backup Server List Local Configuration and Backup Server List Auto Configuration, Management Enhancements, Load Balancing, VLAN Support, Multiple Subnet Support, Traffic-Triggered Activation, PFS via Policy Push, 802.1x Authentication, Certificate (PKI) Support, Easy VPN Remote and Server on the Same Interface, and Easy VPN Remote and Site to Site on the Same Interface
- **12.3(7)XR2:** The features in Cisco IOS Software Release 12.3(7)XR introduced on Cisco 800 series routers
- **12.3(11)T:** Except for the Dial Backup and Traffic-Triggered Activation features, all features introduced in Cisco IOS Software Releases 12.3(7)XR and 12.3(7)XR2 integrated into Cisco IOS Release 12.3(11)T

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.7

Always consult Cisco.com for the latest information regarding Cisco Easy VPN features and the supporting Cisco IOS software releases.

- **12.3(2)T:** Added support for type 6 password
- **12.3(4)T:** Added support for save password and multiple peer backup
- **12.3(7)T:** IPSec DPD Periodic Message Option feature added
- **12.3(7)XR:** Introduced DPD with Stateless Failover (Object Tracking with Easy VPN)—Backup Server List Local Configuration and Backup Server List Auto Configuration, Management Enhancements, Load Balancing, VLAN Support, Multiple Subnet Support, Traffic-Triggered Activation, PFS via Policy Push, 802.1x Authentication, Certificate (PKI) Support, Easy VPN Remote and Server on the Same Interface, and Easy VPN Remote and Site to Site on the Same Interface
- **12.3(7)XR2:** Features in Cisco IOS Release 12.3(7)XR introduced on Cisco 800 Series routers
- **12.3(11)T:** Except for the Dial Backup and Traffic-Triggered Activation features, all features introduced in Cisco IOS Releases 12.3(7)XR and 12.3(7)XR2 integrated into Cisco IOS Release 12.3(11)T



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.

## Restrictions for Cisco Easy VPN Remote

### Required Easy VPN Servers

The Cisco Easy VPN Remote feature requires that the destination peer be a Cisco IOS Easy VPN Server or VPN concentrator that supports the Cisco Easy VPN Server feature. At the time of publication, this includes the following platforms when running the indicated software releases:

- **Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers:** Cisco IOS Software Release 12.2(8)T or later release. Cisco 800 Series routers are not supported in Cisco IOS Software Release 12.3(7)XR, but they are supported in Cisco IOS Software Release 12.3(7)XR2.
- **Cisco 1700 Series:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 2600 Series:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 3620:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 3640:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 3660:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 7100 Series VPN routers:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 7200 Series routers:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco 7500 Series routers:** Cisco IOS Software Release 12.2(8)T or later release.
- **Cisco PIX 500 Series:** Cisco IOS Software Release 6.2 or later release.
- **Cisco VPN 3000 Series:** Cisco IOS Software Release 3.11 or later release.

## Only ISAKMP Policy Group 2 Supported on Easy VPN Servers

The Cisco Unity protocol supports only Internet Security Association and Key Management Protocol (ISAKMP) policies that use Diffie-Hellman (DH) group 2 (1024-bit DH) IKE negotiation, so the Cisco Easy VPN Server being used with the Cisco Easy VPN Remote feature must be configured for a group 2 ISAKMP policy. The Easy VPN Server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN client.

## Transform Sets Supported

To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (esp-des and esp-3des) or transform sets that provide authentication without encryption (esp-null esp-sha-hmac and esp-null esp-md5-hmac).

---

**Note**        The Cisco Unity Client protocol does not support Authentication Header (AH) authentication, but Encapsulating Security Protocol (ESP) is supported.

---

## Dial Backup for Easy VPN Remotes

Line-status-based backup is not supported in this feature.

## NAT Interoperability Support

NAT interoperability is not supported in client mode with split tunneling.

# How Cisco Easy VPN Works

This topic describes the operations of Cisco Easy VPN.

## Cisco 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 ISAKMP 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: IPsec quick mode completes the connection.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6.9

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:

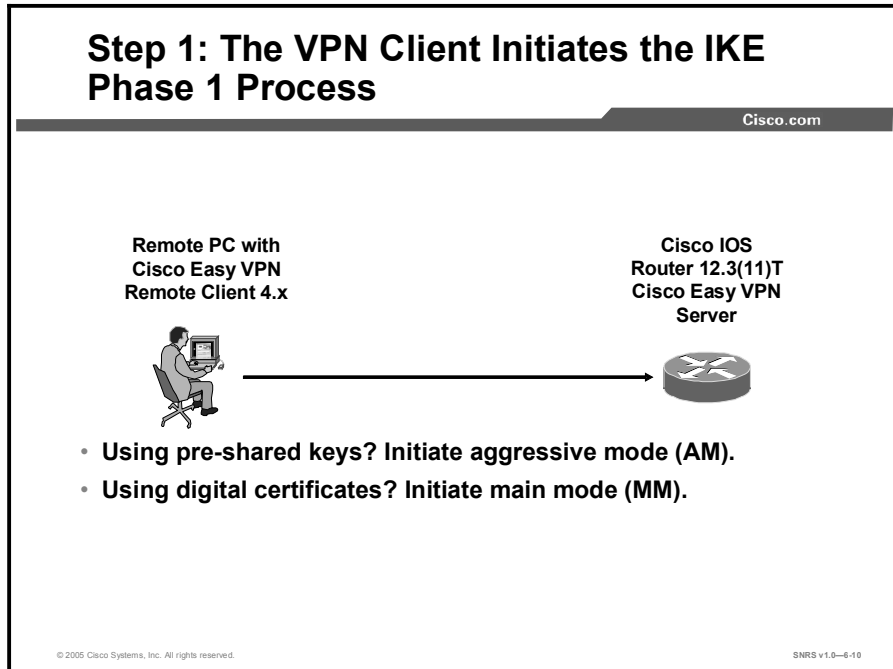
- Device authentication via ISAKMP
- User authentication using IKE Xauth
- VPN policy push (using mode configuration)
- IPsec security association (SA) creation

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 ISAKMP SA.
- Step 3** The Easy VPN Server accepts the SA proposal.
- Step 4** The Easy VPN Server initiates a username and password challenge.
- Step 5** The mode configuration process is initiated.
- Step 6** The Reverse Route Injection (RRI) process is initiated.
- Step 7** IPsec quick mode completes the connection.

# Step 1—Authentication Begins

This topic describes the beginning of the Cisco Easy VPN process, which begins with IKE Phase 1.



Because there are two ways to perform authentication, the VPN Client must consider the following when initiating this phase:

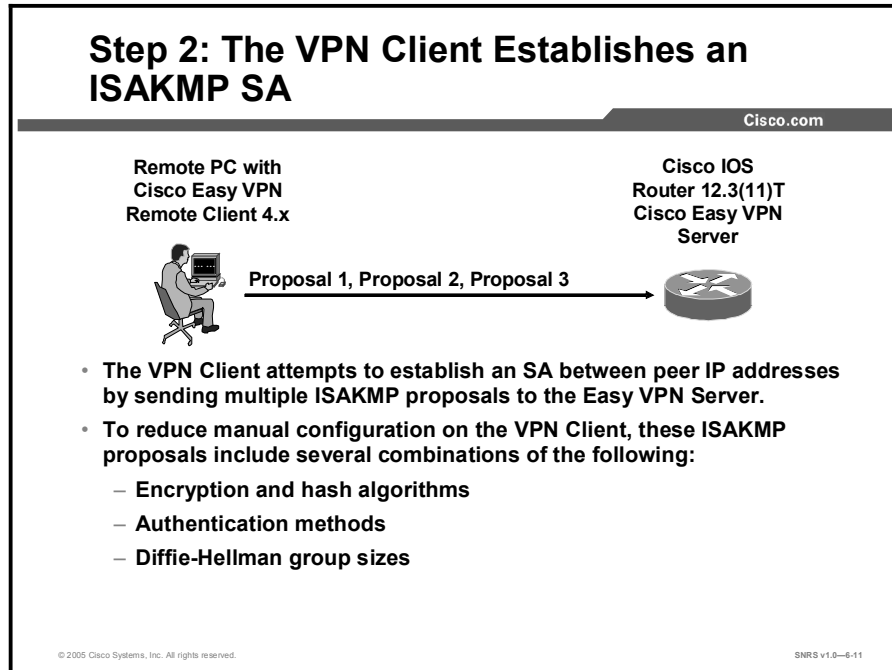
- If a pre-shared key is to be used for authentication, the VPN Client initiates aggressive mode (AM). When pre-shared keys are used, the accompanying group name entered in the configuration GUI (ID\_KEY\_ID) is used to identify the group profile associated with this VPN Client.
- If digital certificates 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—An IKE SA Is Established

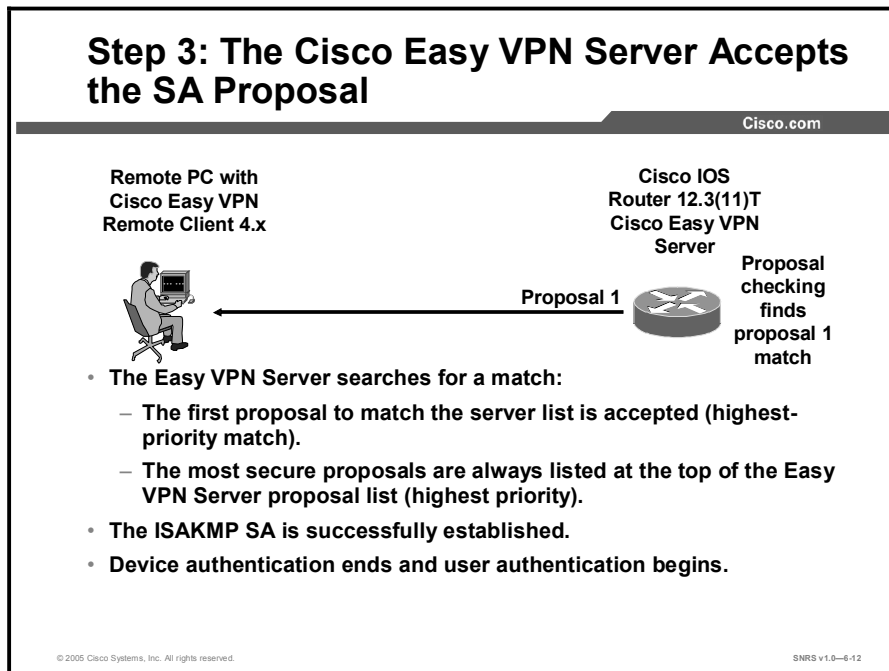
This topic describes the establishing of a security association (SA).



To reduce the amount of manual configuration on the VPN Client, every combination of encryption and hash algorithms, in addition to authentication methods and DH group sizes, is proposed.

## Step 3—Cisco Easy VPN Server Authenticates the Device

This topic describes how the Cisco Easy VPN server authenticates the device first before authenticating the user.

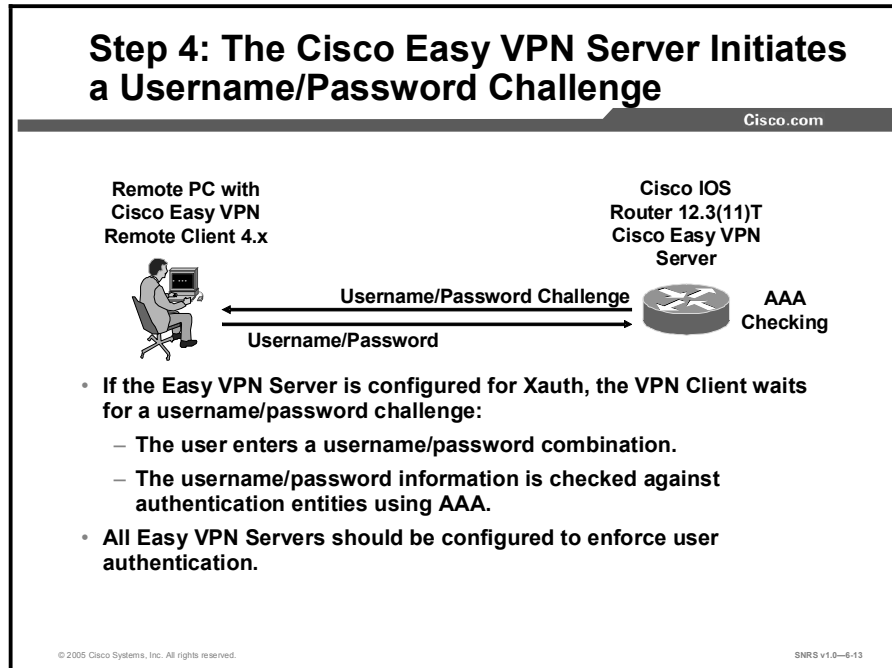


ISAKMP policy is global for the Easy VPN Server and can consist of several proposals. In the case of multiple proposals, the Easy VPN Server will use the first match (so you should always have your most secure policies listed first).

Device authentication ends and user authentication begins at this point.

## Step 4—Username and Password Challenge Is Processed

This topic describes the process of username and password challenge.

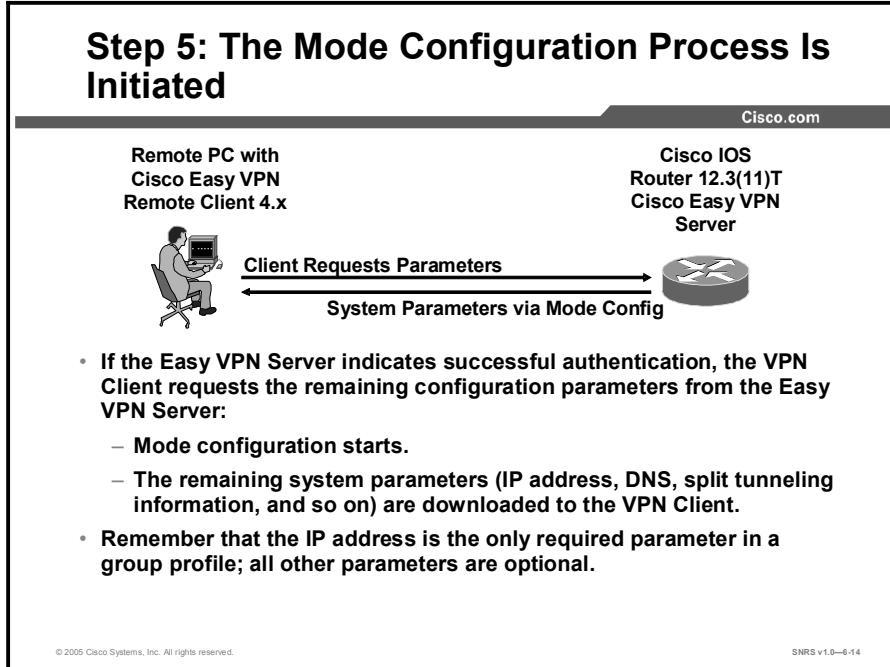


The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy.

VPN devices that are configured to handle remote VPN Clients should always be configured to enforce user authentication.

# Step 5—Mode Configuration

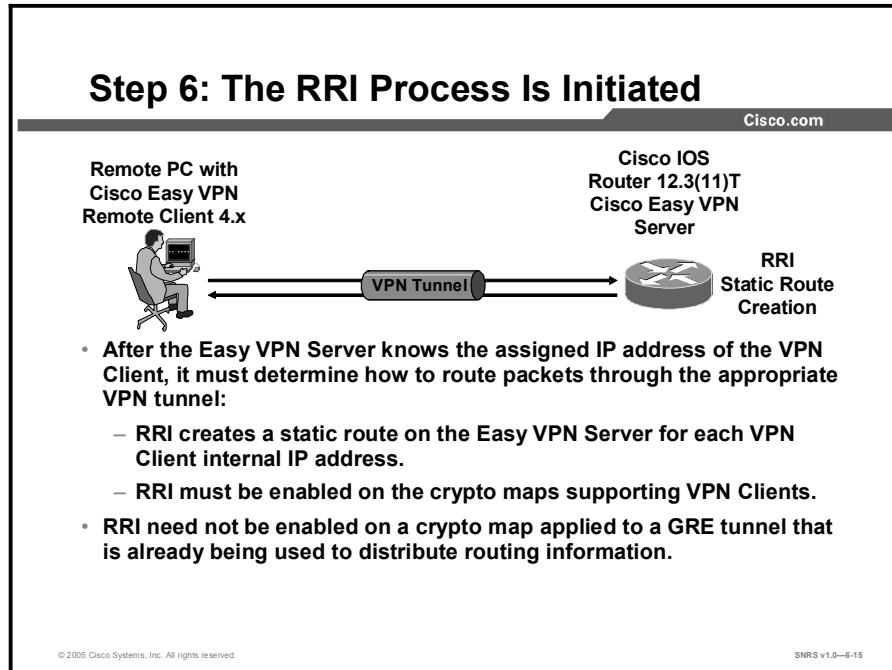
This topic describes mode configuration.



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

This topic describes the Reverse Route Injection (RRI) process.



RRI ensures that a static route is created on the Cisco Easy VPN Server for the internal IP address of each VPN Client.

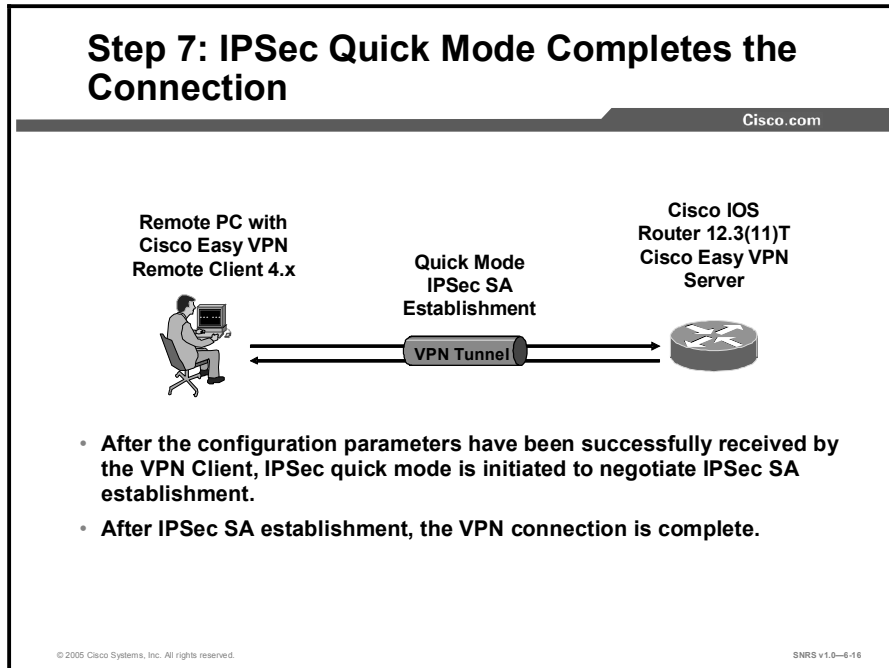
---

**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—Connection Is Completed with IPSec Quick Mode

This topic describes the completion of the VPN connection.



After IPSec SAs have been created, the connection is complete.

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Cisco Easy VPN consists of two components Easy VPN Server and Easy VPN Remote.**
- **Seven steps are involved:**
  - **Step 1: The VPN Client initiates the IKE Phase 1 process.**
  - **Step 2: The VPN Client establishes an ISAKMP 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: IPsec quick mode completes the connection.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6-17





## Lesson 2

---

# Configuring the Easy VPN Server

---

## Overview

This lesson continues the configuration of Cisco Easy Virtual Private Network (VPN). The lesson guides you through the tasks used to configure an Easy VPN Server as it is used to support Extended Authentication (Xauth) for Easy VPN Remote VPN Client access.

## Objectives

Upon completing this lesson, you will be able to configure a Cisco Easy VPN Server. This ability includes being able to meet these objectives:

- List the steps required to configure Cisco Easy VPN Server
- Create an IP address pool
- Configure group policy lookup
- Configure the ISAKMP policy for all Cisco Easy VPN Remote clients attaching to the router
- Define a group policy for mode configuration push
- Create a transform set for the Cisco Easy VPN Remote clients
- Create the dynamic crypto map with RRI
- Apply mode configuration in global configuration mode to a dynamic crypto map
- Apply a crypto map to the Cisco Easy VPN Server router outside interface
- Enable a Cisco IOS VPN gateway (instead of the VPN Client) to send ISAKMP DPD messages
- Configure Xauth on the Cisco Easy VPN Server router
- Enable the Xauth save password feature
- Verify the configuration

# Cisco Easy VPN Server Configuration Tasks

This topic examines the general tasks used to configure an Easy VPN Server to support Xauth for Easy VPN Remote VPN Client access.

## Cisco 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 an IP address pool.**
- **Task 2: Configure group policy lookup.**
- **Task 3: Create an ISAKMP policy for remote VPN Client access.**
- **Task 4: Define a 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 the crypto map to the router interface.**
- **Task 9: Enable IKE DPD.**
- **Task 10: Configure Xauth.**
- **Task 11: (Optional) Enable the Xauth Save Password feature.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.4

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 and 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 the crypto map to the router interface.
- **Task 9:** Enable ISAKMP dead peer detection (DPD).
- **Task 10:** Configure Xauth. Xauth is not required when using Cisco Easy VPN but it is covered here as part of this example. This option can be disabled.
- **Task 11:** (Optional) Enable the Xauth save password feature.


# Task 1—Create IP Address Pool

This topic describes how to create an IP address pool to use as addresses for connecting VPN Clients.

## Task 1: Create IP Address Pool

Cisco.com

Remote Client



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.

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6.0

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:

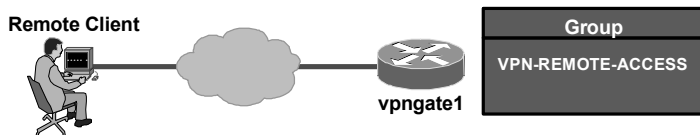
```
ip local pool {default | pool-name low-ip-address [high-ip-address]}
```

# Task 2—Configure Group Policy Lookup

This topic describes how to configure group policy lookup.

## Task 2: Configure Group Policy Lookup

Cisco.com



```

router(config)#
aaa new-model

router(config)#
aaa authorization network list-name local
[method1 [method2...]]

vpngate1(config)# aaa new-model
vpngate1(config)# aaa authorization network
VPN-REMOTE-ACCESS local

```

• **Creates a user group for local AAA policy lookup**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.6

Configuring group policy lookup is completed in two steps, as shown in the figure:

**Step 1** The first step when preparing your Cisco 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 RADIUS server and the router local database may be used together and are tried in the order listed.

The syntax for the **aaa authorization network** command is as follows:

```
aaa authorization network list-name [method1 method2 ...]
```

| Command Parameter           | Description                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------|
| <i>list-name</i>            | Character string used to name the list of authorization methods                                  |
| <i>method1 [method2]...</i> | Specifies an authorization method or multiple authorization methods to be used for authorization |


# Task 3—Create ISAKMP Policy for Remote VPN Client Access

This topic describes the commands use to create your ISAKMP policies.

## Task 3: Create ISAKMP Policy for Remote VPN Client Access

Cisco.com

Remote Client



Policy 1

Authentication: Pre-shared keys  
Encryption: 3-DES  
Diffie-Hellman: Group 2  
Other settings: Default

```
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
```

- Use standard ISAKMP configuration commands.

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6.7

Complete this task to configure the ISAKMP policy for all Cisco 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—Define Group Policy for Mode Configuration Push

This topic describes the steps involved in defining the policy attributes that are pushed to the client via mode configuration.

### Task 4: Define Group Policy for Mode Configuration Push

Cisco.com

**Task 4 contains the following steps:**

- **Step 1: Add the group profile to be defined.**
- **Step 2: Configure the ISAKMP 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.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6-8

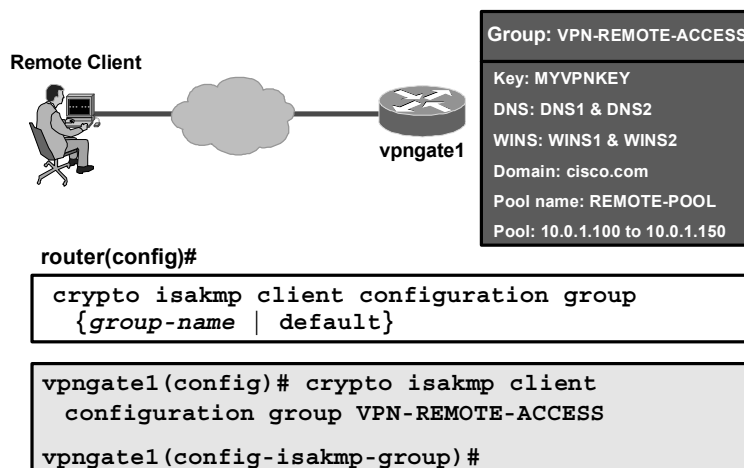
Complete this task to define a group policy to be pushed during mode configuration. Although users may belong to only one group per connection, they may belong to specific groups with different policy requirements.

Complete 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 ISAKMP pre-shared key.
- Step 3**     Specify the Domain Name System (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

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.0

The **crypto isakmp client configuration group** command specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode.

**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}
```

| Command Parameter | Description                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>group-name</i> | Group definition that identifies which policy is enforced for users.                                                                                               |
| <b>default</b>    | Policy that is enforced for all users who do not offer a group name that matches a <i>group-name</i> argument. The default keyword can only be configured locally. |

## Task 4-Step 2: Configure the IKE Pre-Shared Key

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
```

```
router(config-isakmp-group)#
```

```
key name
```

```
vpngate1(config-isakmp-group) # key MYVPNKEY
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-10

- Step 2** Use the **key** command to specify the ISAKMP 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.

**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 **key** command.

Use the **key** command in ISAKMP group configuration mode to specify the ISAKMP pre-shared key for the group policy attribute definition.

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

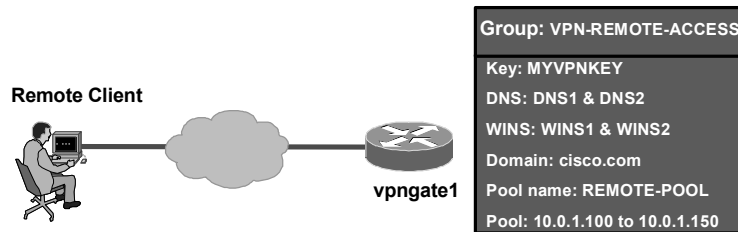
**key** *name*

| Command Parameter | Description                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>       | ISAKMP 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 4.x configuration user interface. |



## Task 4-Step 3: Specify the DNS Servers

Cisco.com



```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-11

**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
```

| Command Parameter       | Description                                    |
|-------------------------|------------------------------------------------|
| <i>primary-server</i>   | Name or IP address of the primary DNS server   |
| <i>secondary-server</i> | Name or IP address of the secondary DNS server |

## Task 4-Step 4: Specify the WINS 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

```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-12

**Step 4** (Optional) Specify the primary and secondary WINS servers using the **wins** 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 **wins** command.

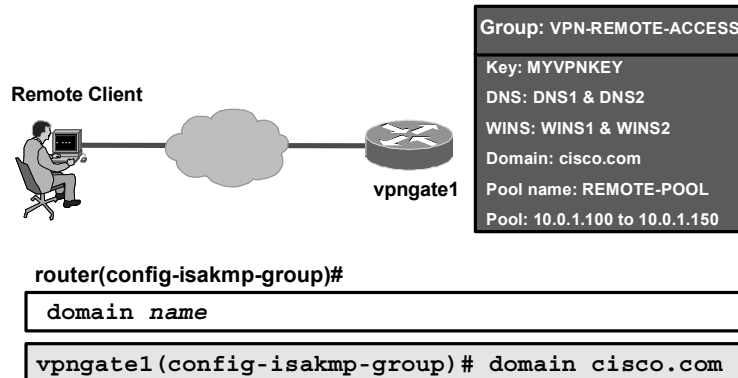
The syntax for the **wins** command is as follows:

```
wins primary-server secondary-server
```

| Command Parameter       | Description                                     |
|-------------------------|-------------------------------------------------|
| <i>primary-server</i>   | Name or IP address of the primary WINS server   |
| <i>secondary-server</i> | Name or IP address of the secondary WINS server |

## Task 4-Step 5: Specify the DNS Domain

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-13

**Step 5** (Optional) Specify the DNS domain to which a group belongs by using the **domain** 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 **domain** command.

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

**domain** *name*

| Command Parameter | Description            |
|-------------------|------------------------|
| <i>name</i>       | Name of the DNS domain |

## Task 4-Step 6: Specify the Local IP Address Pool

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
```

```
router(config-isakmp-group)#
```

```
pool name
```

```
vpngate1(config-isakmp-group)# pool REMOTE-POOL
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-14

**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.

**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 **pool** command.

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
```

| Command Parameter | Description            |
|-------------------|------------------------|
| <i>name</i>       | Name of the local pool |


## Task 5—Create a Transform Set

This topic describes how to create a transform set to be exchanged with clients.

### Task 5: Create Transform Set

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-15

This task creates a transform set for the Cisco 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 Cisco Easy VPN Remote client access:

```
vpngate1(config)# crypto ipsec transform-set VPNTRANSFORM esp-3des
esp-sha-hmac
vpngate1(cfg-crypto-trans)# exit
```

## Task 6—Create a Dynamic Crypto Map with RRI

This topic describes how to enable Reverse Route Injection (RRI) for the client.

### Task 6: Create Dynamic Crypto Map with RRI

Cisco.com

**Task 6 contains the following steps:**

- **Step 1: Create a dynamic crypto map.**
- **Step 2: Assign a transform set.**
- **Step 3: Enable RRI.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—6-16

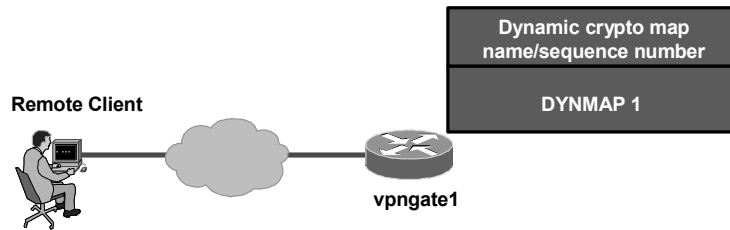
This task creates a dynamic crypto map to be used when building IPsec tunnels to Cisco Easy VPN Remote clients. In this example, RRI is used to ensure that returning data destined for a particular IPsec tunnel can find that tunnel. RRI ensures that a static route is created on the Easy VPN Server for 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

Cisco.com



router(config)#

```
crypto dynamic-map dynamic-map-name
dynamic-seq-num
```

```
vpngate1(config)# crypto dynamic-map DYNMAP 1
vpngate1(config-crypto-map) #
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-17

**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
```

| Command Parameter       | Description                                          |
|-------------------------|------------------------------------------------------|
| <i>dynamic-map-name</i> | Specifies the name of the dynamic crypto map set     |
| <i>dynamic-seq-num</i>  | Specifies the number of the dynamic crypto map entry |

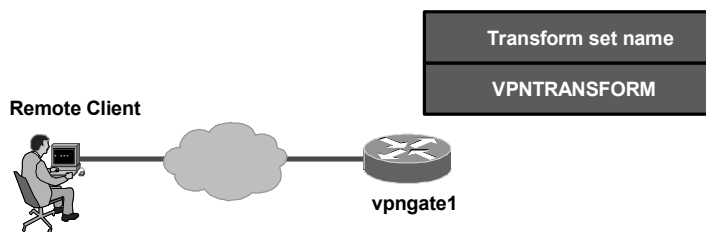
A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPsec negotiation) to match the requirements of a remote peer. This practice allows remote 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 requirements of the remote peer.

Dynamic crypto maps have these characteristics:

- They are not used by the router to initiate new IPsec SAs with remote peers.
- They are used when a remote peer tries to initiate an IPsec SA with the router.
- They are used in evaluating traffic.

## Task 6-Step 2: Assign Transform Set to Dynamic Crypto Map

Cisco.com



router(config-crypto-map)#

```
set transform-set transform-set-name
[transform-set-name2...transform-set-name6]
```

```
vpngate1(config-crypto-map)# set transform-set
VPNTRANSFORM
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-18

- 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:

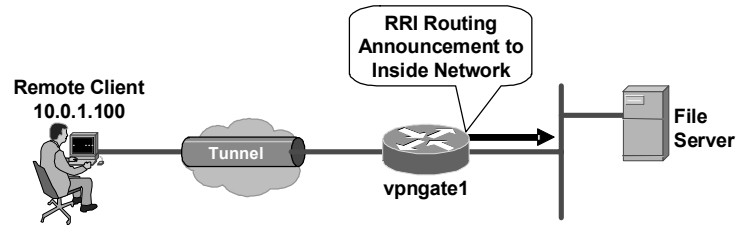
```
set transform-set transform-set-name [transform-set-name2...transform-
set-name6]
```

| Command Parameter         | Description                                                                                                                                                                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>transform-set-name</i> | Name of the transform set: <ul style="list-style-type: none"> <li>For an IPSec manual crypto map entry, you can specify only one transform set.</li> <li>For an IPSec ISAKMP or dynamic crypto map entry, you can specify up to six transform sets.</li> </ul> |



## Task 6-Step 3: Enable RRI

Cisco.com



```
router(config-crypto-map)#
```

```
reverse-route
```

```
vpngate1(config-crypto-map) # reverse-route
```

```
vpngate1(config-crypto-map) # exit
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-19

**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 the Crypto Map

This topic describes how apply mode configuration to the dynamic crypto map.

## Task 7: Apply Mode Configuration to Crypto Map

Cisco.com

### 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 the dynamic crypto map to the crypto map.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—6-20

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 the dynamic crypto map to the crypto map.

## Task 7-Step 1: Configure Router to Respond to Mode Configuration Requests

Cisco.com



router(config)#

```
crypto map map-name client configuration
address {initiate | respond}
```

```
vpngate1(config)# crypto map CLIENTMAP client
configuration address respond
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.21

- 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.

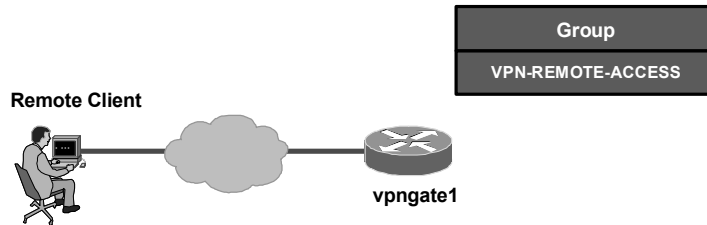
The syntax for the **crypto map map-name client configuration** command is as follows:

```
crypto map map-name client configuration address {initiate | respond}
```

| Command Parameter | Description                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>map-name</i>   | The name that identifies the crypto map                                                                                                          |
| <b>initiate</b>   | A keyword that indicates that the router will attempt to set IP addresses for each peer (no longer used with the Cisco VPN Client 3.x and later) |
| <b>respond</b>    | A keyword that indicates that the router will accept requests for IP addresses from any requesting peer                                          |

## Task 7-Step 2: Enable IKE Querying for Group Policy

Cisco.com



router(config)#

```
crypto map map-name isakmp authorization list
list-name
```

```
vpngate1(config)# crypto map CLIENTMAP isakmp
authorization list VPN-REMOTE-ACCESS
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-22

- Step 2** Enable IKE querying for group policy when requested by the VPN Client. AAA uses the *list-name* argument to determine which method list is used to find the policy (local or RADIUS) as defined in the **aaa authorization network** command.

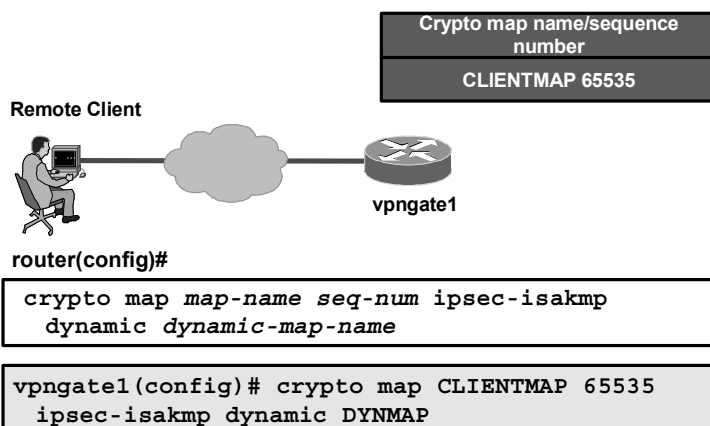
The syntax for the **crypto map isakmp authorization list** command is as follows:

```
crypto map map-name isakmp authorization list list-name
```

| Command Parameter | Description                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>map-name</i>   | Name that you assign to the crypto map set.                                                                                                                             |
| <i>list-name</i>  | 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 Dynamic Crypto Map to the Crypto Map

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.23

**Step 3** Apply the dynamic crypto map to the 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
```

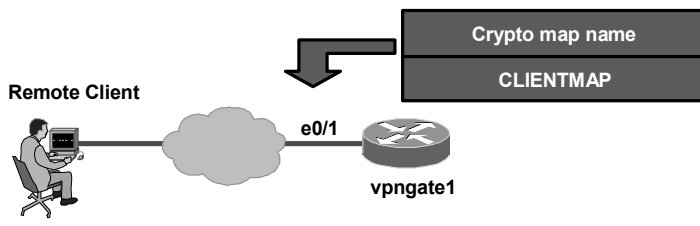
| Command Parameter       | Description                                          |
|-------------------------|------------------------------------------------------|
| <i>map-name</i>         | The name that you assign to the dynamic crypto map   |
| <i>dynamic-map-name</i> | The name that you assign to the dynamic crypto map   |
| <i>seq-num</i>          | Specifies the number of the dynamic crypto map entry |

## Task 8—Apply the Crypto Map to the Router Interface

This topic describes the command used to apply the crypto map to a router interface.

### Task 8: Apply the Crypto Map to Router Outside Interface

Cisco.com



```
vpngate1(config)# interface ethernet0/1
vpngate1(config-if)# crypto map CLIENTMAP
vpngate1(config-if)# exit
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0—6-24

This task applies the crypto map to the Easy VPN Server router outside interface.

Here is an example of how to apply the crypto map to the outside interface beginning in global configuration mode:

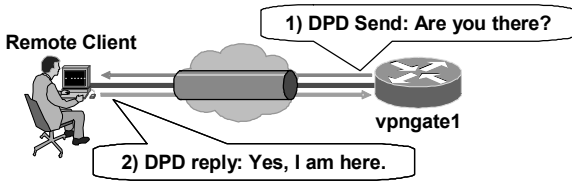
```
vpngate1(config)# interface ethernet0/1
vpngate1(config-if)# crypto map CLIENTMAP
vpngate1(config-if)# exit
```

# Task 9—Enable ISAKMP DPD

This topic describes how to enable dead peer detection (DPD).

## Task 9: Enable ISAKMP DPD

Cisco.com



```
router(config)#
crypto isakmp keepalive secs retries

vpngate1(config)# crypto isakmp keepalive 20 10
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-25

Use the **crypto isakmp keepalive** command in global configuration mode to enable a Cisco IOS VPN gateway (instead of the VPN Client) to send ISAKMP DPD messages.

The syntax for the **crypto isakmp keepalive** command is as follows:

```
crypto isakmp keepalive secs retries
```

| Command Parameter | Description                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------|
| <i>secs</i>       | Specifies the number of seconds between DPD messages. The range is between 10 and 3600 seconds.              |
| <i>retries</i>    | Specifies the number of seconds between retries if DPD messages fail. The range is between 2 and 60 seconds. |

# Task 10—Configure or Disable Extended Authentication

This topic describes how to configure Extended Authentication (Xauth).

## 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 ISAKMP Xauth for the dynamic crypto map.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0—6-26

Complete the following steps to configure Xauth on your Cisco Easy VPN Server router:

- Step 1**    Enable AAA login authentication.
- Step 2**    Set the Xauth timeout value.
- Step 3**    Enable ISAKMP Xauth for the dynamic crypto map.



## Task 10-Step 1: Enable AAA Login Authentication

Cisco.com

Remote Client



vpngate1

VPN user group  
VPNUSERS

router(config)#

```
aaa authentication login list-name method1
[method2...]
```

```
vpngate1(config)# aaa authentication login
VPNUSERS local
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.27

**Step 1** Enable AAA login authentication using the **aaa authentication login** command in global configuration mode.

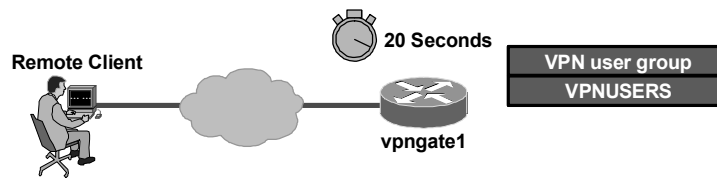
The syntax for the **aaa authentication login** command is as follows:

```
aaa authentication login list-name method1 [method2...]
```

| Command Parameter | Description                                                                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>list-name</i>  | 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. |
| <i>method</i>     | Keyword used to describe the authentication method used.                                                                                                                 |

## Task 10-Step 2: Set Xauth Timeout Value

Cisco.com



router(config)#

```
crypto isakmp xauth timeout seconds
```

```
vpngate1(config)# crypto isakmp xauth timeout 20
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-28

**Step 2** Set the Xauth timeout value using the **crypto isakmp xauth timeout** command.

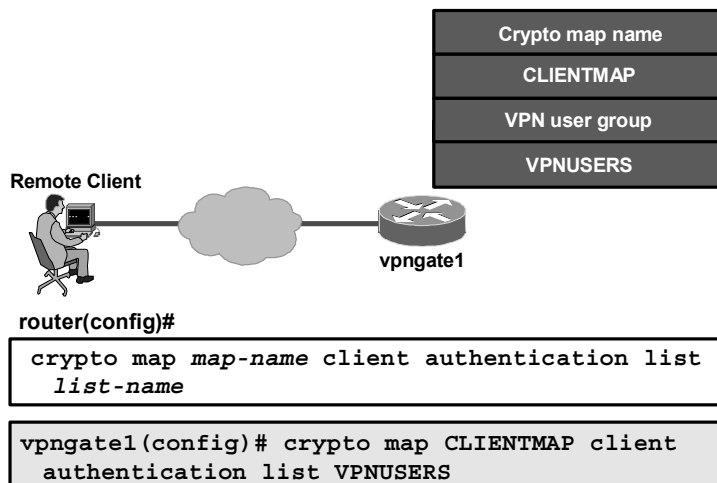
The syntax for the **crypto isakmp xauth timeout** command is as follows:

```
crypto isakmp xauth timeout seconds
```

| Command Parameter | Description                        |
|-------------------|------------------------------------|
| <i>seconds</i>    | The Xauth timeout value in seconds |

## Task 10-Step 3: Enable ISAKMP Xauth for Crypto Map

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-29

**Step 3** Enable ISAKMP 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
```

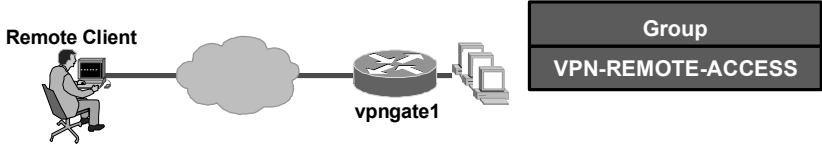
| Command Parameter | Description                                                                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>map-name</i>   | Name that you assign to the crypto map set.                                                                                                                              |
| <i>list-name</i>  | 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—Enable Xauth Save Password Feature

This topic describes how to configure the optional Xauth password save feature.

## Task 11: (Optional) Enable Xauth Save Password

Cisco.com



```
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.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-30

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 (which 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 passwords 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**      The save password feature must be configured in both the Cisco Easy VPN Server and the Cisco Easy VPN Remote.

---

# Task 12—Verify

This topic describes how to verify your configuration.

## Task 12: Verify

Cisco.com

```
router#
show crypto map [interface interface | tag
map-name]
```

```
Router# show crypto map interface ethernet 0
```

- **Displays crypto map configuration**

```
router#
show run
```

```
Router# show run
```

- **Displays running configuration**

© 2005 Cisco Systems, Inc. All rights reserved.
SNRS v1.0-6-31

To verify your configurations for this feature, complete the following steps.

- Step 1** Issue the **enable** command.
- Step 2** Issue the **show crypto map [interface interface | tag map-name]** command.
- Step 3** Issue the **show run** command.

|               | Command                                                                                                                        | Purpose                                                         |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br>Example:<br>Router> <b>enable</b>                                                                             | Enables privileged EXEC mode<br>Enter your password if prompted |
| <b>Step 2</b> | <b>show crypto map [interface interface   tag map-name]</b><br>Example:<br>Router# <b>show crypto map interface ethernet 0</b> | Displays the crypto map configuration                           |
| <b>Step 3</b> | <b>show run</b>                                                                                                                | Displays the running configuration                              |

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **If you are using a local IP address pool, you need to configure that pool for use with Easy VPN.**
- **AAA is enabled for policy lookup.**
- **ISAKMP policies are configured for VPN clients.**
- **The steps for defining group policy include configuring the following:**
  - Policy profile of the group that will be defined
  - Pre-shared key
  - DNS servers
  - WINS servers
  - DNS domain
  - Local IP address pool

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-32

## Summary (Cont.)

Cisco.com

- **Transform sets are configured for exchange with VPN clients.**
- **Enabling RRI for the client includes the following:**
  - Creating a dynamic crypto map
  - Assigning transform set to the crypto map
  - Enabling RRI
- **Applying mode configuration to the dynamic crypto map includes the following:**
  - Configuring the router to respond to mode configuration requests
  - Enabling ISAKMP queries for group policy lookup
  - Applying changes to the dynamic crypto map
- **Examining Extended Authentication (Xauth).**
- **The final step is to verify Easy VPN configurations.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-33





## Lesson 3

---

# Configuring Easy VPN Remote for the Cisco VPN Client 4.x

---

## Overview

The Cisco Virtual Private Network (VPN) Client for Windows (referred to in this lesson as the VPN Client) is software that runs on a Microsoft Windows-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN Server on an enterprise network or with a service provider, creates a secure connection over the Internet. This lesson guides you through the process of setting up the Cisco VPN Client on a laptop to create a secure connection, called a tunnel, between your computer and a private network.

## Objectives

Upon completing this lesson, you will be able to configure the Cisco VPN Client 4.x for Easy VPN Remote access. This ability includes being able to meet these objectives:

- List the steps required to configure Cisco Easy VPN Remote for the Cisco VPN Client 4.x
- Install the Cisco VPN Client 4.x on a Windows 2000 PC
- Create new connection entries
- Select appropriate client options for the drop-down menu
- Select the appropriate client authentication method from the menu radio buttons
- Configure dialup or VPN Client connection properties
- Confirm client settings, and connection status

# Cisco VPN Client 4.x Configuration Tasks

This topic contains information about the installation and configuration of the Cisco VPN Client 4.x.

## Configuring Easy VPN Remote for the Cisco VPN Client 4.x: General Tasks

Cisco.com

- **Task 1: Install Cisco VPN Client 4.x.**
- **Task 2: Create a new client connection entry.**
- **Task 3: Choose an authentication method.**
- **Task 4: Configure transparent tunneling.**
- **Task 5: Enable and add backup servers.**
- **Task 6: Configure connection to the Internet through Dial-Up Networking.**

© 2005 Cisco Systems, Inc. All rights reserved.

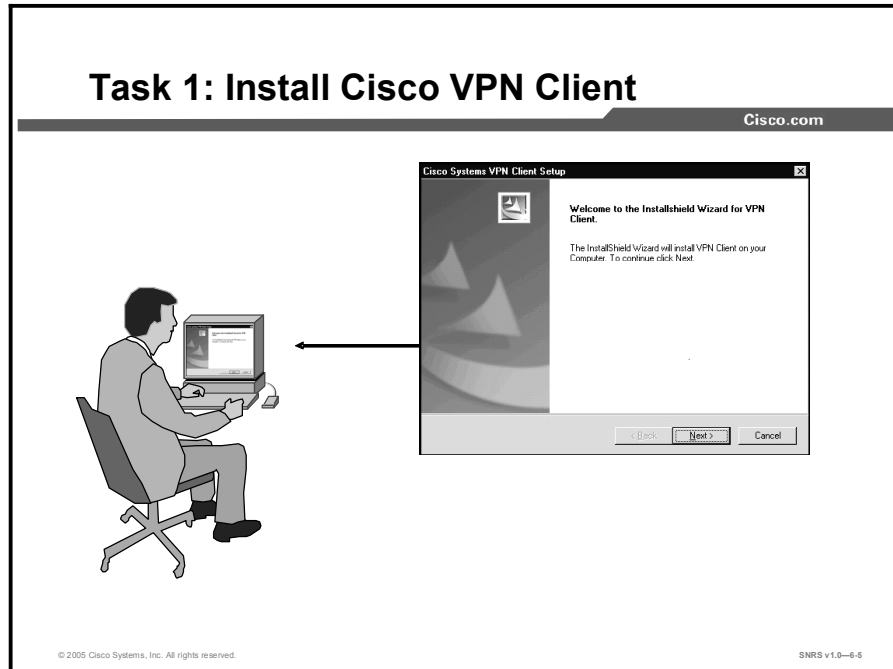
SNRS v1.0-6.4

Complete the following general tasks to configure the Cisco VPN Client for Easy VPN Remote access:

- **Task 1:** Install the Cisco VPN Client on the remote user PC.
- **Task 2:** Create a new client connection entry.
- **Task 3:** Choose an authentication method.
- **Task 4:** Configure transparent tunneling.
- **Task 5:** Enable and add backup servers.
- **Task 6:** Configure connection to the Internet through dialup networking.

# Task 1—Install Cisco VPN Client

This topic describes how to install a Cisco VPN Client on a computer to set up a secure connection to a private network using the Internet.



You can install the VPN Client on your system through either of two applications: InstallShield and Microsoft Windows Installer (MSI). Both applications use installation wizards to walk you through the installation. Installing the VPN Client through InstallShield includes an Uninstall icon in the program group; MSI does not. In the latter case, to manually remove VPN Client applications, you can use the Microsoft Add/Remove Programs utility.

This topic explains how to install the VPN Client on your PC and includes the following:

- Verifying system requirements
- Gathering the information that you need
- Installing the VPN Client through InstallShield
- Installing the VPN Client through MSI

## Verifying System Requirements

Verify that your computer meets these requirements:

- A single, Pentium-class processor.
- One of the following operating systems:
  - Microsoft Windows 98 or Windows 98 (second edition)
  - Windows ME
  - Windows NT 4.0 (with Service Pack 6 or later)
  - Windows 2000
  - Windows XP
- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 50 MB hard disk space.
- RAM:
  - 32 MB for Windows 98
  - 64 MB for Windows NT and Windows ME
  - 64 MB for Windows 2000 (128 MB recommended)
  - 128 MB for Windows XP (256 MB recommended)
- To install the VPN Client:
  - CD-ROM drive
  - 3.5 inch high-density diskette drive
  - Administrator privileges if installing on Windows NT or Windows 2000
- To use the VPN Client:
  - Direct network connection (cable or DSL modem and network adapter or interface card)
  - Internal or external modem
- To connect using a digital certificate for authentication:
  - A digital certificate signed by one of the following certificate authorities (CAs) installed on your PC:
    - Entrust Technologies ([www.entrust.com](http://www.entrust.com))
    - Microsoft Certificate Services—Windows 2000
    - Netscape (Security)
    - VeriSign ([www.verisign.com](http://www.verisign.com))
  - Or a digital certificate stored on a smart card; the VPN Client supports smart cards via the Microsoft Cryptography application programming interface (CAPI)

## Gathering the Information That You Need

To configure and use the VPN Client, you might need the information listed in this section.

Ask for this information from the system administrator of the private network that you want to access. Your system administrator might have preconfigured much of this data; if so, he or she will tell you which items you need.

- Host name or IP address of the secure gateway to which you are connecting
- Your IPsec group name (for pre-shared keys)
- Your IPsec group password (for pre-shared keys)
- If authenticating with a digital certificate, the name of the certificate
- If authenticating through the internal server of the secure gateway, your username and password
- If authenticating through a RADIUS server, your username and password
- If authenticating through a Windows NT domain server, your username and password
- If authenticating through a token vendor, your username and PIN
- If authenticating through a smart card, your smart card, reader, personal identification number (PIN) or passcode, and the name of the certificate stored on the smart card
- If you should configure backup server connections, the host names or IP addresses of the backup servers

## Installing the VPN Client Through InstallShield

To install the VPN Client on your system using InstallShield, follow these steps. It is suggested that you accept the defaults unless your system administrator has instructed otherwise.

- Step 1** Exit all Windows programs, and disable any antivirus software.
- Step 2** Insert the Cisco Systems CD-ROM in the CD-ROM drive of your system.
- Step 3** Choose **Start > Run**. The Run dialog box appears.
- Step 4** Enter **E:\VPN Client\CD-ROM\InstallShield\setup.exe**, where E: is the CD-ROM drive of your system.
- Step 5** Click **OK**.

---

**Note** Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

---

- Step 6** If the InstallShield Wizard identifies an existing version of either the Cisco VPN 3000 Client or the Cisco 5000 VPN Client, it displays a dialog box that asks if you want to uninstall the existing client program. To continue, click **Yes**.

The VPN Client launches the appropriate uninstall wizard: the Cisco VPN Client uninstall wizard to uninstall a previous version of the Cisco VPN 3000 Client or the Cisco 5000 VPN Client. Follow the instructions on the uninstall wizard dialog boxes to automatically uninstall the program and reboot.

After your system reboots, the Cisco Systems VPN Client Setup wizard resumes.

**Step 7** Follow the instructions on the screens and enter a destination folder for the VPN Client files (or click **Next** to enter the default location C:\Program Files\Cisco Systems\VPN Client).

**Step 8** You must restart your computer before you can configure and use the VPN Client.

## Installing the VPN Client through Microsoft Windows Installer

Microsoft Windows Installer (MSI) is available for Windows NT, Windows 2000, and Windows XP.

---

**Note** If you are using MSI, you must have Windows NT-based products such as Windows NT 4.0 (with SP6), Windows 2000, or Windows XP. Installing with MSI also requires administrator privileges.

Windows Installer 2.0 must be installed on a Windows NT or Windows 2000 PC before configuring the PC for a restricted user with elevated privileges (CSCea37900).

---

To install the VPN Client using MSI, complete the following steps:

**Step 1** Exit all Windows programs, and disable any antivirus software.

**Step 2** Insert the Cisco Systems CD-ROM in the CD-ROM drive of your system.

**Step 3** Choose **Start > Run**. The Run dialog box appears.

**Step 4** Enter **E:\VPN Client\CD-ROM\Msi\vpclient\_en.exe**, where E: is the CD-ROM drive of your system.

**Step 5** Click **OK**.

---

**Note** Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

---

The program displays the Cisco Systems logo and the Microsoft Installer Setup window. Click **Next** to start the installation and then follow the instructions on the dialog boxes.

MSI installs the VPN Client in the default location C:\Program Files\Cisco Systems\VPN Client. If you want a different destination folder for the VPN Client files, enter the alternative location when prompted to do so.

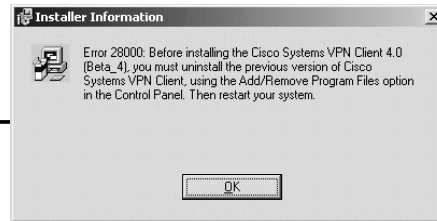
When the installation has completed, the installer displays a confirmation dialog box.

**Step 6** Click **Finish**. MSI prompts you to restart your system.

**Step 7** Click **Yes** to restart your system.

## Task 1: Install Cisco VPN Client (Cont.)

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

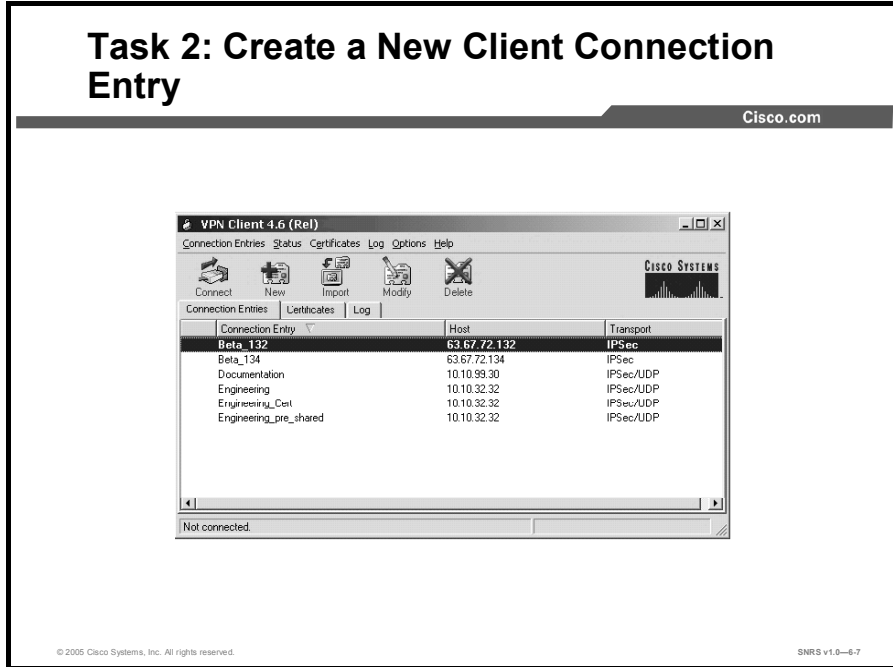
SNRS v1.0-6.6

If you have not removed a previously installed VPN Client, when you execute the **vpnclient\_en.exe** command or **vpnclient\_en.msi** command, an error message displays. You must uninstall the previously installed VPN Client before proceeding with the new installation.

To remove a VPN Client installed with MSI, use the Windows Add/Remove Programs control panel. To remove a VPN Client installed with InstallShield, choose **Start > Programs > Cisco Systems VPN Client > Uninstall Client**.

# Task 2—Create New Client Connection Entries

This topic describes how to create a new client connection entry.



To use the VPN Client, you must create at least one connection entry, which identifies the following information:

- The VPN device (the remote server) to access.
- Pre-shared keys—the IPSec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPSec algorithms that your VPN Client uses.
- Certificates—the name of the certificate that you are using for authentication.
- Optional parameters that govern VPN Client operation and connection to the remote network.

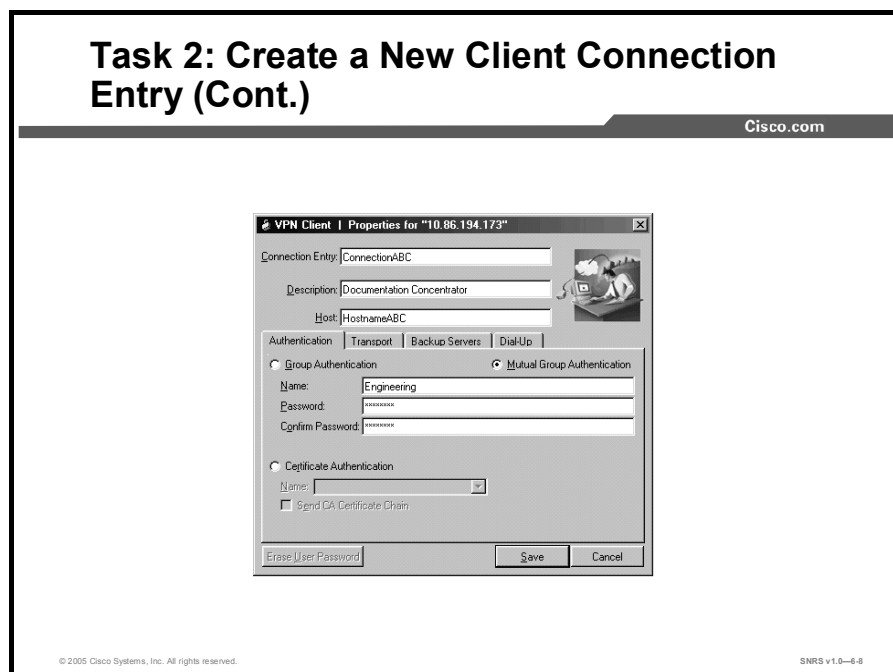
You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously) or if you belong to more than one VPN remote access group.



## Creating a New Connection Entry

Use the following procedure to create a new connection entry.

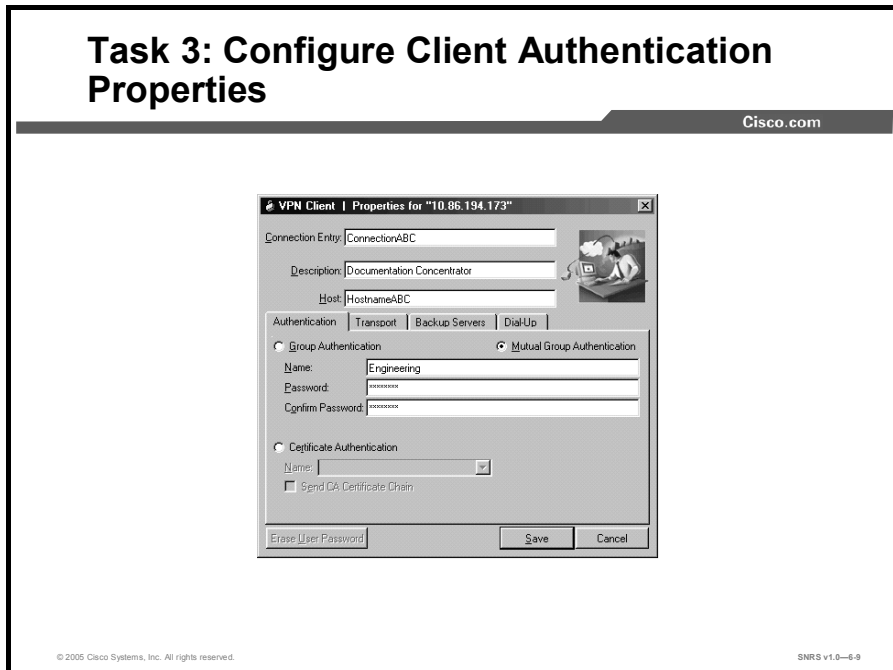
- Step 1** Start the VPN Client by choosing **Start > Programs > Cisco Systems VPN Client > VPN Client**.
- Step 2** The VPN Client application starts and displays the advanced mode main window. If you are not already there, choose the **Options** menu in simple mode and choose **Advanced Mode** or press **Ctrl-M**.
- Step 3** Choose **New** from the toolbar or the Connection Entries menu. The VPN Client displays a form.



- Step 4** Enter a unique name for this new connection. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case-sensitive.
- Step 5** Enter a description of this connection. This field is optional, but it helps further identify this connection; for example, Connection to Engineering remote server.
- Step 6** Enter the host name or IP address of the remote VPN device that you want to access.

# Task 3—Configure Client Authentication Properties

This topic describes how to configure properties used during the client authentication process.



Under the Authentication tab, enter the information for the method that you want to use. You can connect as part of a group (configured on a VPN device) or by supplying an identity digital certificate.

## Group Authentication

The network administrator usually configures group authentication for you. If this is not the case, complete the following procedure:

- Step 1** Click the **Group Authentication** radio button.
- Step 2** In the Name field, enter the name of the IPsec group to which you belong. This entry is case-sensitive.
- Step 3** In the Password field, enter the password (which is also case-sensitive) for your IPsec group. The field displays only asterisks.
- Step 4** Verify your password by entering it again in the Confirm Password field.

## Mutual Group Authentication

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-10

## Mutual Group Authentication

To use mutual group authentication, you need a root certificate that is compatible with the central-site VPN installed on your system. Your network administrator can load a root certificate on your system during installation. When you select mutual group authentication, the VPN Client software verifies whether you have a root certificate installed. If not, it prompts you to install one. Before you continue, you must import a root certificate.

When you have installed a root certificate (if required), follow the steps for group authentication.

## Certificate Authentication

For certificate authentication, perform the following procedure, which varies according the type of certificate you are using:

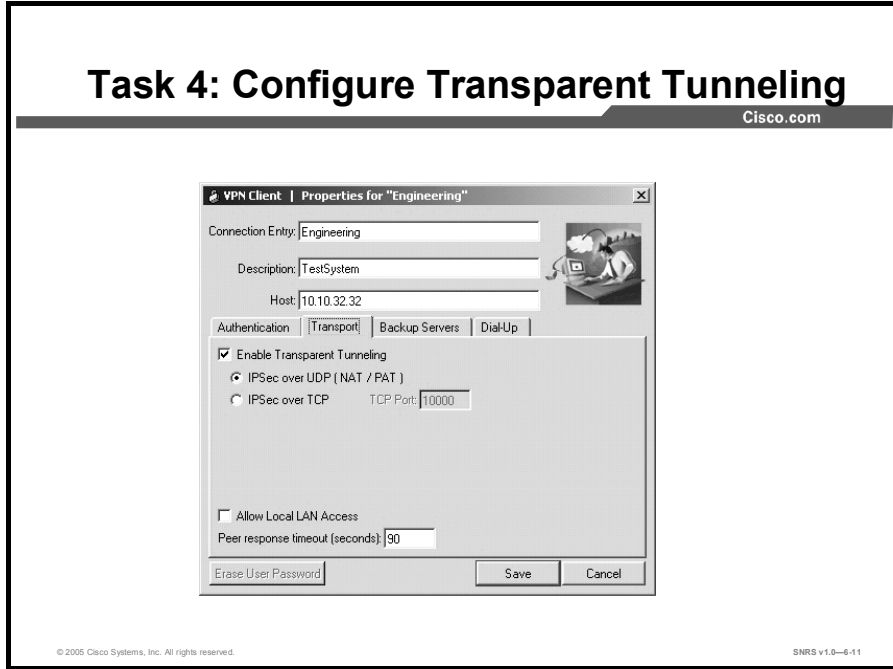
**Step 1** Click the **Certificate Authentication** radio button.

**Step 2** Choose the name of the certificate you are using from the menu.

If the field reads "No Certificates Installed" and is shaded, then you must enroll for a certificate before you can use this feature.

# Task 4—Configure Transparent Tunneling

This topic describes how to enable transparent tunneling.



Next, configure transparent tunneling by completing the fields on the Transport tab.

## Enabling Transparent Tunneling

Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT). Transparent tunneling encapsulates Protocol 50 (Encapsulating Security Payload, or ESP) traffic within UDP packets and can allow for both Internet Security Association and Key Management Protocol (ISAKMP; UDP 500) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.

The VPN Client also sends keepalives frequently, ensuring that the mappings on the devices are kept active.

Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with the vendor of your device to verify whether this limitation exists. Some vendors support Protocol 50 PAT (IPSec passthrough), which might let you operate without enabling transparent tunneling.

To use transparent tunneling, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the Cisco VPN 3000 Concentrator Manager, Configuration | User Management | Groups | Add | IPsec tab (or refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration* or Help in the VPN 3000 Concentrator Manager browser).

This parameter is enabled by default. To disable this parameter, uncheck the check box. It is recommended that you always keep this parameter checked.

Then choose a mode of transparent tunneling, over UDP or over TCP. The mode that you use must match that used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, then in general, TCP mode is preferable. UDP does not operate with stateful firewalls, so in this case, you should use TCP.

### Using IPsec over UDP (NAT/PAT)

To enable IPsec over UDP (NAT or PAT), click the **IPsec over UDP (NAT/PAT)** radio button. With UDP, the port number is negotiated. UDP is the default mode.

### Using IPsec over TCP (NAT/PAT/Firewall)

To enable IPsec over TCP, click the **IPsec over TCP** radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

## Allowing Local LAN Access

In a multiple-network interface card (NIC) configuration, local LAN access pertains only to network traffic on the interface on which the tunnel was established. The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, or other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your client system goes through the IPsec connection to the secure gateway.

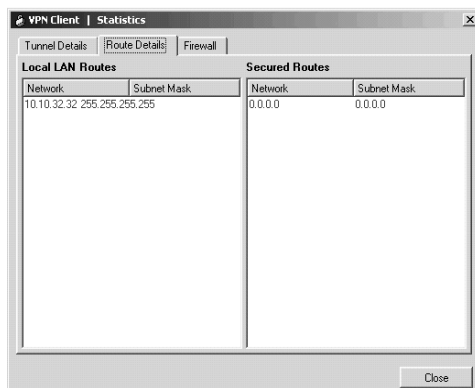
To enable this feature, check the **Allow Local LAN Access** check box; to disable it, uncheck the check box. If the local LAN that you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the client side that you can access. You can access up to 10 networks when this feature is enabled. When the Allow Local LAN Access feature is enabled and you are connected to a central site, all traffic from your system goes through the IPsec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the routes table.

## Routes Table

Cisco.com



The screenshot shows a window titled "VPN Client | Statistics" with three tabs: "Tunnel Details", "Route Details", and "Firewall". The "Route Details" tab is active, displaying a table with two columns: "Local LAN Routes" and "Secured Routes". Each column has sub-columns for "Network" and "Subnet Mask".

| Local LAN Routes |                 | Secured Routes |             |
|------------------|-----------------|----------------|-------------|
| Network          | Subnet Mask     | Network        | Subnet Mask |
| 10.10.32.32      | 255.255.255.255 | 0.0.0.0        | 0.0.0.0     |

A "Close" button is located at the bottom right of the dialog box.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-12

To display the routes table, complete the following steps:

**Step 1** Choose the Status menu, and choose **Statistics**.

**Step 2** Choose **Route Details** from the Statistics dialog box.

The routes table shows local LAN routes, which do not traverse the IPsec tunnel, and secured routes, which do traverse the IPsec tunnel to a central-site device. The routes in the local LAN routes column are for locally available resources.

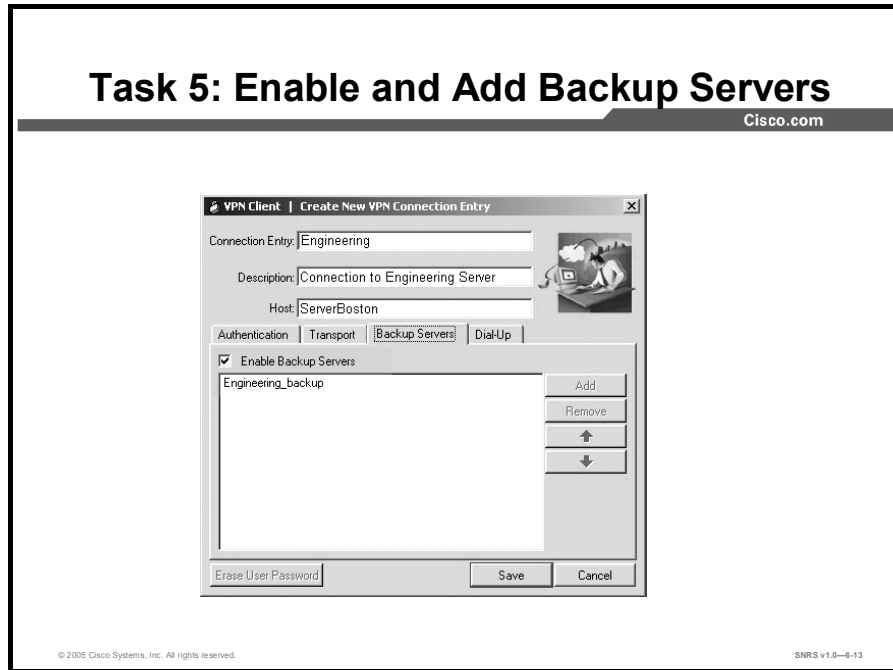
---

**Note** This feature works on only one NIC, the same NIC as the tunnel.

---

## Task 5—Enable and Add Backup Servers

This topic describes how to enable and add backup servers.

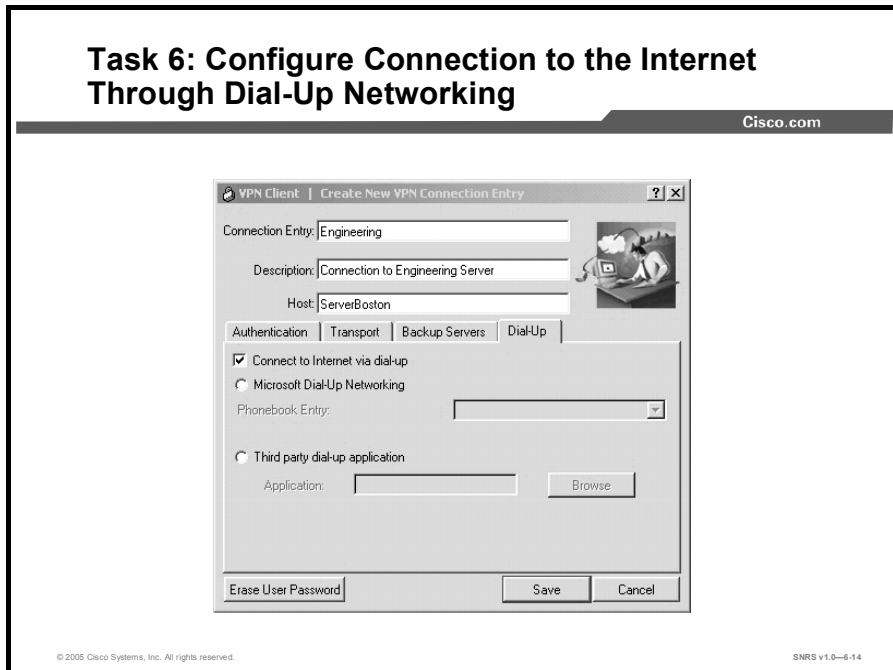


The private network may include one or more backup VPN servers to use if the primary server is not available. Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the VPN Concentrator, or you can manually enter this information.

To enable backup servers from the VPN Client, complete the following steps:

- Step 1** Click the **Backup Servers** tab.
- Step 2** Check the **Enable Backup Servers** check box. This box is not checked by default.
- Step 3** Click **Add** to enter the backup server address.
- Step 4** Enter the host name or IP address of the backup server, using a maximum of 255 characters.
- Step 5** To add more backup devices, repeat Steps 2, 3, and 4.

## Task 6—Configure Connection to the Internet Through Dial-Up Networking



To connect to a private network using a dialup connection, complete the following steps:

- Step 1** Use a dialup connection to your Internet service provider (ISP) to connect to the Internet.
- Step 2** Use the VPN Client to connect to the private network through the Internet.

To enable and configure this feature, check the **Connect to the Internet via Dial-Up** check box. This box is not checked by default.

You can connect to the Internet using the VPN Client application in either of the following ways:

- Microsoft Dial-Up Networking (DUN)
- Third-party dialup program



# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- You can install the VPN Client on your system through either of two different applications: InstallShield and MSI.
- Connection entries include the following:
  - The VPN device (the remote server) to access
  - Pre-shared keys
  - Certificates
  - Optional parameters
- Authentication methods include the following:
  - Group authentication
  - Mutual group authentication
  - Certificate authentication

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-16

## Summary (Cont.)

Cisco.com

- Transparent tunneling allows secure transmission through a router serving as a firewall, which may also be performing network address translation NAT or PAT.
- Access to local LAN resources can be made available.
- The private network may include one or more backup VPN servers to use if the primary server is not available.
- You can connect to the Internet using the VPN Client application in either of the following ways:
  - Microsoft DUN
  - A third-party dialup program, usually from your ISP

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-16



## Lesson 4

---

# Configuring Cisco Easy VPN Remote for Access Routers

---

## Overview

This lesson provides information on configuring and monitoring the Cisco Easy VPN Remote feature to create IPsec virtual private network (VPN) tunnels between a supported router and an Easy VPN server (Cisco IOS router, Cisco VPN 3000 Concentrator, or Cisco PIX Firewall) that supports this form of IPsec encryption and decryption. The lesson covers the three modes of operation and guides you through the process of client mode configuration.

## Objectives

Upon completing this lesson, you will be able to explain how to configure a Cisco access router for Cisco Easy VPN Remote from the Cisco IOS CLI. This ability includes being able to meet these objectives:

- Select the appropriate Cisco Easy VPN Remote mode of operation
- List the steps required to configure Cisco Easy VPN Remote for access routers
- Configure the DHCP server pool
- Configure and assign the Cisco Easy VPN client profile
- Configure Xauth password save
- Initiate the VPN tunnel
- Verify the Cisco Easy VPN configuration

# Easy VPN Remote Modes of Operation

This topic describes the three modes of Cisco Easy VPN available for configuration on your router.

## Configuration Methods for Cisco Easy VPN Remote Access Routers

Cisco.com

```
graph LR; VPN_Remote[VPN Remote] --- Cloud((20.20.20.0)); Cloud --- vpngate1[vpngate1];
```

**There are three ways to configure your remote Cisco routers for Cisco Easy VPN Remote:**

- Cisco IOS CLI
- Cisco Router and Security Device Manager (SDM) with Cisco access routers
- Cisco Router Web Setup (CRWS) tool with Cisco 800 Series Router

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6.4

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)
- Cisco Router and Security Device Manager (SDM) with Cisco access routers, beginning with Cisco IOS Software Release 12.2(13)ZH on many router platforms
- Cisco Router Web Setup Tool (CRWS) with Cisco 800 Series Routers

This topic describes how to configure Easy VPN Remote using the Cisco IOS CLI method only.

## Cisco Easy VPN Remote Modes of Operation

Cisco.com

- **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 not used
- **Network extension plus mode**
  - Additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface
  - IPSec SAs for this IP address automatically created by Easy VPN Remote
  - IP address typically used for troubleshooting (using ping, Telnet, and SSH)

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6.6

The Cisco Easy VPN Remote feature supports three modes of operation: client, network extension, and network extension plus.

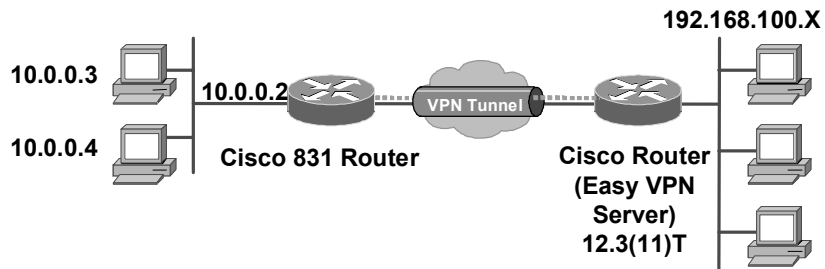
- **Client mode:** This mode specifies that Network Address Translation (NAT) or Port Address Translation (PAT) be configured to allow PCs and hosts on the client side of the VPN connection to form a private network. Their IP addresses must not use any of the destination server IP addresses. Client mode 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.

- **Network extension plus mode:** This mode is identical to network extension mode, with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPSec security associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell [SSH] protocol).

All modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an Internet service provider (ISP) or other service, eliminating the corporate network from the path for web access.

## Cisco Easy VPN Remote Client Mode

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

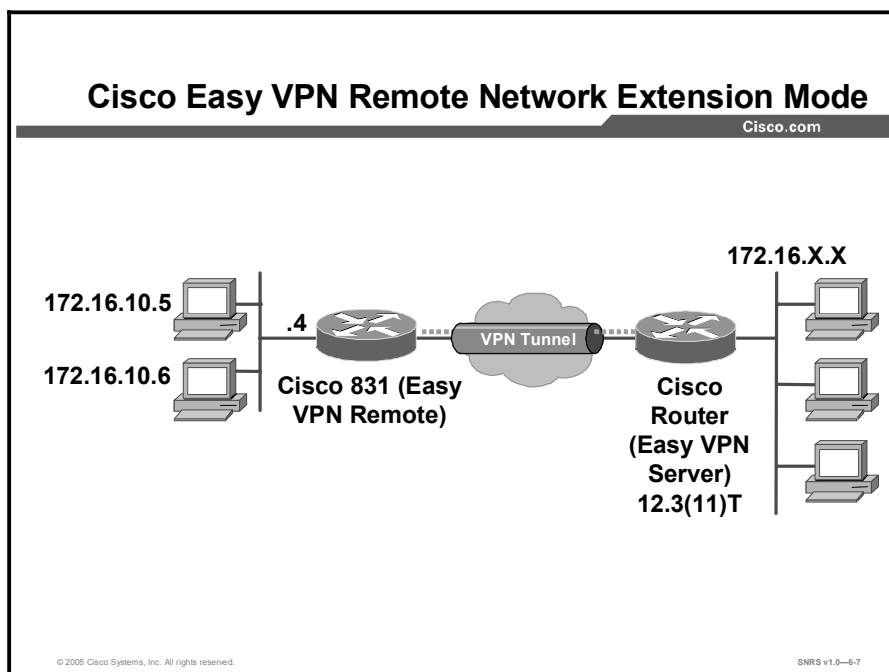
SNRS v1.0-6.6

The figure illustrates the client mode of operation. In this example, the Cisco 831 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 831 router, which also has an IP address in the 10.0.0.0 private network space. The Cisco 831 router performs NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.

---

**Note** The diagram could also represent a split tunneling connection, in which the client PCs can access public resources in the global Internet without including the corporate network in the path for the public resources.

---



This figure illustrates the network extension mode of operation. In this example, the Cisco 831 router acts as a Cisco Easy VPN Remote device, connecting to a router used as a Cisco Easy VPN server.

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, assuming that the destination routers are configured to properly route those IP addresses over the tunnel.

In this example, the PCs and hosts attached to the two routers have IP addresses that are in the same address space as the destination enterprise network. The PCs connect to the Ethernet interface of the Cisco 831 router, which also has an IP address in the enterprise address space. This scenario provides a seamless extension of the remote network.

## Cisco Easy VPN Remote Features

Cisco Easy VPN Remote is a collection of features that improves the capabilities of the Cisco Easy VPN Remote feature introduced in Cisco IOS Software Release 12.2(4)YA. Cisco Easy VPN Remote includes the following:

- **Default inside interface:** Cisco Easy VPN supports the automatic configuration of the default Easy VPN inside interface for Cisco 800 series routers.
- **Multiple inside interfaces:** It configures up to eight inside interfaces on the Cisco Easy VPN Remote.
- **Multiple outside interfaces:** It configures up to four outside tunnels for outside interfaces.
- **VLAN support:** It allows VLANs to be configured as valid Easy VPN inside interfaces.
- **Multiple subnet support:** It allows multiple subnets from the Easy VPN inside interface to be included in the Easy VPN tunnel.



- **NAT interoperability support:** It automatically restores the NAT configuration when the IPsec VPN tunnel is disconnected.
- **Local address support:** Cisco Easy VPN Remote is enhanced to support an additional **local-address** attribute that specifies which interface is used to determine the IP address used to source the Easy VPN tunnel traffic.
- **Peer host name:** When a peer is defined as a host name, the host name is stored and the Domain Name System (DNS) lookup is done at the time of tunnel connection.
- **Proxy DNS server support:** It configures the router in a Cisco Easy VPN Remote configuration to act as a proxy DNS server for LAN-connected users.
- **Cisco IOS Firewall support:** It supports Cisco IOS Firewall configurations on all platforms.
- **Cisco Easy VPN Remote and Server on the same interface:** The Easy VPN Remote and Easy VPN Server are supported on the same interface, which makes it possible to establish a tunnel to another Easy VPN Server and terminate the Easy VPN software client on the same interface simultaneously.
- **Cisco Easy VPN Remote and site to site on the same interface:** Easy VPN Remote and site to site (crypto map) are supported on the same interface, which makes it possible to establish a tunnel to another Easy VPN Server and have another site to site on the same interface simultaneously.
- **Cisco Easy VPN Remote web managers:** Users can manage Cisco Easy VPN Remote on the Cisco uBR905 and Cisco uBR925 cable access routers using a built-in web interface.
- **Dead Peer Detection (DPD) Periodic Message Option:** This feature allows you to configure your router to query the status of its Internet Key Exchange (IKE) peer at regular intervals.
- **Load balancing:** If a remote device is loaded and unable to accept more traffic, the Cisco VPN 3000 Concentrator will send a notify message that contains an IP address that represents the new IKE server to which the remote should connect.
- **Management enhancements:** It allows for remote management of the VPN remote device.
- **Perfect Forward Secrecy (PFS) support:** The PFS configuration mode attribute is sent by the server if requested by the VPN remote device.
- **Dial backup:** It allows you to configure a dial backup tunnel connection on your remote device.

# Configuration Tasks for Cisco Easy VPN Remote for Access Routers

This topic covers the configuration tasks involved in the configuration of Cisco Easy VPN Remote.

## Cisco Easy VPN Remote Configuration General Tasks for Access Routers

Cisco.com

- **Task 1: (Optional) Configure the DHCP server pool.**
- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-8

Configuring Cisco access routers to act as Easy VPN Remote clients consists of the following tasks:

- **Task 1:** (Optional) Configure the Dynamic Host Configuration Protocol (DHCP) server pool.
- **Task 2:** Configure and assign the Cisco Easy VPN client profile.
- **Task 3:** (Optional) Configure Extended Authentication (Xauth) password save.
- **Task 4:** Initiate the VPN tunnel.
- **Task 5:** Verify the Cisco Easy VPN configuration.

# Task 1—Configure the DHCP Server Pool

This topic describes how to configure a local DHCP pool for use in Cisco Easy VPN.

## Task 1: Configure the DHCP Server Pool

Cisco.com

```
router(config)#
ip dhcp pool pool-name

router(dhcp-config)#
network ip-address [mask /prefix-length]
default-router address [address2 ... addressN]
import all
lease {days [hours] [minutes] / infinite}
exit

router(config)#
ip dhcp excluded-address lan-ip-address
```

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6.9

If you want to use the local router DHCP server to assign IP addresses to the hosts that are connected to the LAN interface of the router, you must create a pool of IP addresses for the router 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 LAN interface are assigned an IP address in a private address space. The router then uses NAT or PAT to translate those IP addresses into a single IP address that is transmitted across the VPN tunnel connection.

The following are the steps to 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 local Ethernet interface of the router.
- 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 that the router is configured with the proper DHCP parameters from the central DHCP server. This option requires that 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 you 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* value should be the IP address assigned to the router LAN interface.

### Task 1 Example: DHCP Server Pool

Cisco.com

```
vpnRemotel(config)# ip dhcp pool CLIENT
vpnRemotel(dhcp-config)# network 10.10.10.0
255.255.255.0
vpnRemotel(dhcp-config)# default-router 10.10.10.1
vpnRemotel(dhcp-config)# import all
vpnRemotel(dhcp-config)# lease 3
vpnRemotel(dhcp-config)# exit
vpnRemotel(config)# ip dhcp excluded-address 10.10.10.1
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-10

One example of how to configure a DHCP server pool is shown in the figure.

## Task 2—Configure and Assign the Cisco Easy VPN Client Profile

This topic describes how to configure and assign the Cisco Easy VPN client profile.

### Task 2: Configure the Cisco Easy VPN Client Profile

Cisco.com

```
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 | network-plus}
exit
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-11

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 host name for the destination peer. This is typically the IP address of the Easy VPN Server router outside interface. If you prefer to specify a host name, you must have a DNS server configured and available.
- 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

Cisco.com

```
VPNGATE1
Group: VPN-REMOTE-ACCESS
Peer: 20.20.20.2
Key: MYVPNKEY
Mode: Client
```



```
vpnRemotel(config)# crypto ipsec client ezvpn VPNGATE1
vpnRemotel(config-crypto-ezvpn)# group VPNREMOTE1 key
MYVPNKEY
vpnRemotel(config-crypto-ezvpn)# peer 20.20.20.2
vpnRemotel(config-crypto-ezvpn)# mode client
vpnRemotel(config-crypto-ezvpn)# exit
vpnRemotel(config)#
```

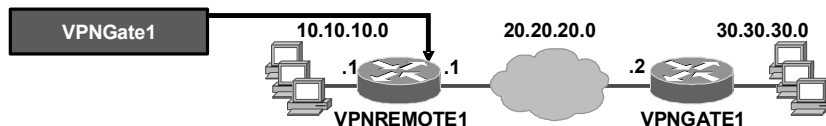
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-12

One example of how to configure an Easy VPN client profile is shown in the figure.

## Task 2 Example: Assign Cisco Easy VPN Remote to the Interface

Cisco.com



```
router(config-if)#
crypto ipsec client ezvpn name [inside | outside]

vpnRemotel(config)# interface ethernet1
vpnRemotel(config-if)# crypto ipsec client ezvpn
VPNGATE1
vpnRemotel(config-if)# exit
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-13

Use the **crypto ipsec client ezvpn name** command in interface configuration mode 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—Configure Xauth Password Save

This topic describes how to configure Extended Authentication (Xauth).

### Task 3: (Optional) Configure Xauth Save Password Feature

Cisco.com

```
router(config)#
crypto ipsec client ezvpn name

router(config-crypto-ezvpn)#
username aaa-username password aaa-password

vpnRemote1(config)# crypto ipsec client ezvpn
VPNGATE1

vpnRemote1(config-crypto-ezvpn)# username VPNUSER
password VPNPASS

vpnRemote1(config-crypto-ezvpn)# exit
```

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-14

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, configuring the Cisco Easy VPN client profile, to speed up the entry process.

Enter the **username** command in Easy VPN Remote configuration mode for the specific client profile, as shown in the figure. This is the authentication, authorization, and accounting (AAA) username and password used to automatically reauthenticate the user with the Xauth password save feature enabled in Cisco Easy VPN Server.

## Task 4—Initiate the VPN Tunnel

This topic describes how to manually initiate the VPN tunnel.

### Task 4: (Optional) Initiate the VPN Tunnel (Xauth)

Cisco.com

```
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
```

```
vpnRemotel# 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.

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-15

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 (at least for the first time). The Cisco IOS software message shown in the figure 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. To initial the VPN tunnel, complete the following steps:

**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 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

This topic describes how to verify the Cisco Easy VPN configuration on the router.

## Task 5: Verify the Cisco Easy VPN Configuration

Cisco.com

```
vpnRemotel# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 2

Tunnel name : VPNGATE1
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
```

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6-16

Task 5 consists of reviewing the Easy VPN configuration using the **show crypto ipsec client ezvpn** command.

## Cisco Easy VPN Remote Configuration Example

Cisco.com

```
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 VPNGATE1
connect auto
group VPNREMOTE1 key 0 MYVPNKEY
mode client
peer 20.20.20.2
username VPNUSER password 0 VPNPASS
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-17

This figure and the next detail an example of Cisco Easy VPN Remote access router configuration.

## Cisco Easy VPN Remote Configuration Example (Cont.)

Cisco.com

```
interface Ethernet0
ip address 10.10.10.1 255.255.255.0
crypto ipsec client ezvpn VPNGATE1 inside
!
interface Ethernet1
ip address 20.20.20.1 255.255.255.0
crypto ipsec client ezvpn VPNGATE1
!
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-6-18

This figure contains the second half of the example begun in the previous figure of Cisco Easy VPN Remote access router configuration.

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **There are three ways to configure Cisco access routers for Cisco Easy VPN Remote: the CLI, SDM, and CRWS.**
- **Cisco Easy VPN Remote supports three modes of operation: client, network extension, and network extension plus.**
- **Xauth is optional.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-6-19

# Module Summary

This topic summarizes the key points discussed in this module.

## Module Summary

Cisco.com

- **Cisco Easy VPN consists of two components: Easy VPN Server and Easy VPN Remote.**
- **Easy VPN Server configuration tasks include DHCP, group policy lookup, mode configuration, RRI, ISAKMP DPD, and ISAKMP and IPSec configuration.**
- **The VPN Client allows for the easy creation of a secure tunnel to a private network for a remote user.**
- **Cisco Easy VPN remote supports three modes of operation: client, network extension, and network extension plus.**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-6-1

This module covered using Cisco Easy VPN in creating VPN tunnels. The Cisco Easy VPN components were explained, including the use of a router as an Easy VPN Server. Cisco VPN Client Version 4.x was described, and the you were guided through the process of setting up a remote client session with the router.

## Module 7

---

# Cisco Router and Security Device Manager

---

## Overview

Cisco Router and Security Device Manager (SDM) is an intuitive, web-based device management tool for Cisco IOS software-based routers. Cisco SDM simplifies router and security configuration through smart wizards, which help customers quickly and easily deploy, configure, and monitor a Cisco Systems router without requiring knowledge of the command-line interface (CLI). This module introduces Cisco SDM and describes the configuration of some of the security features possible through the use of the SDM user-friendly interface and wizards.

## Module Objective

Upon completing this module, you will be able to use the wizards and tools embedded in the Cisco SDM to complete a wide range of configuration tasks. This ability includes being able to meet this objective:

- Configure a Cisco IOS Firewall and Cisco IOS VPN using Cisco SDM wizards



## Lesson 1

---

# Using Cisco Router and Security Device Manager

---

## Overview

Cisco Router and Security Device Manager (SDM) is an easy-to-use, Java-based device-management tool, designed for configuring LAN, WAN, and security features on a router. This lesson guides you through the process of securing a network using Cisco SDM. An overall view of Cisco SDM is given before moving on to describing how to configure the router to protect a network using the wizards contained in the Cisco SDM interface and then describes monitoring. The wizards presented in this lesson include the LAN, WAN, Firewall, VPN, Security Audit, and Startup wizards.

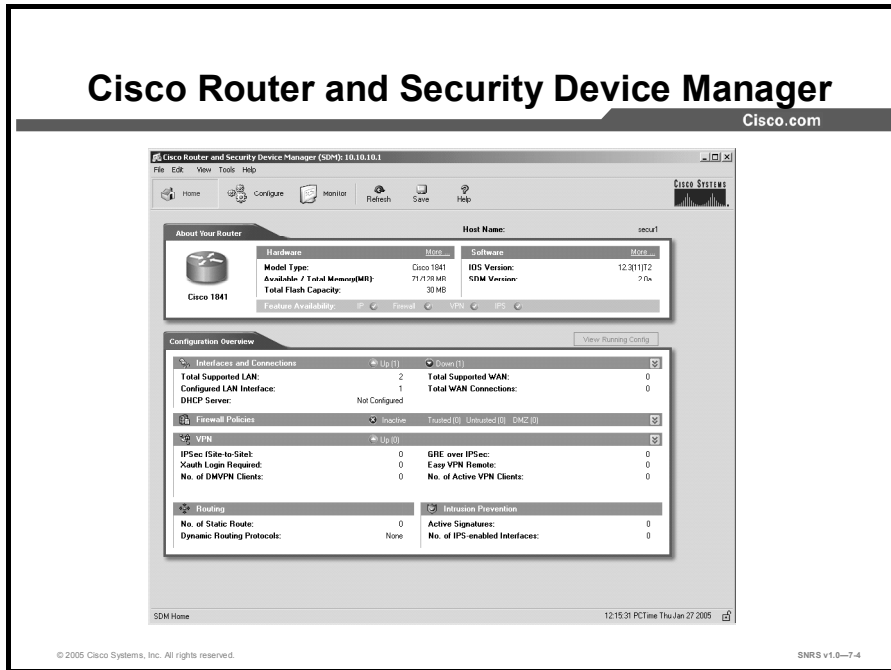
## Objectives

Upon completing this lesson, you will be able to configure a Cisco IOS Firewall and Cisco IOS VPN using Cisco SDM. This ability includes being able to meet these objectives:

- Describe the features of Cisco SDM
- Explain how to install Cisco SDM on a router
- Explain how to set up Cisco SDM for ongoing use
- Explain how to use the elements of the Cisco SDM interface
- Explain what each of the five Cisco SDM wizards is used for
- Describe the tasks required to configure a WAN with Cisco SDM
- Describe the tasks required to configure the Cisco IOS Firewall feature on a Cisco SDM-supported router
- Describe the tasks required to configure a VPN on a Cisco SDM-supported router
- Describe the tasks required to perform security audits on a Cisco SDM-supported router
- Explain the role of the Reset to Factory Default wizard
- Explain the tasks that can be completed using the Cisco SDM configuration and monitor mode windows

# Cisco SDM Overview

This topic gives an overview of Cisco Router and Security Device Manager (SDM).



Cisco SDM is an intuitive, web-based device-management tool for Cisco IOS software-based routers. Cisco SDM simplifies router and security configuration through smart wizards, which help you quickly and easily deploy, configure, and monitor a Cisco Systems router without requiring knowledge of the command-line interface (CLI). Cisco SDM is supported on Cisco 830 Series, Cisco 1700 Series, Cisco 1800 Series, Cisco 2600XM, Cisco 2800 Series, Cisco 3600 Series, Cisco 3700 Series, and Cisco 3800 Series routers and on selected Cisco 7200 Series and Cisco 7301 routers.



## What Is Cisco SDM?

Cisco.com

- **Embedded web-based management tool**
- **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**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-5

Cisco SDM allows you to easily configure routing, switching, security, and quality of service (QoS) services on Cisco routers while helping to enable proactive management through performance monitoring. Whether you are deploying a new router or installing the Cisco SDM on an existing router, you can now remotely configure and monitor these routers without using the Cisco IOS software CLI. The Cisco SDM GUI aids nonexpert users of Cisco IOS software in day-to-day operations, provides easy-to-use smart wizards, automates router security management, and assists you through comprehensive online help and tutorials.

Cisco SDM smart wizards guide you step by step through router and security configuration workflow by systematically configuring the LAN and WAN interfaces, firewall, intrusion prevention system (IPS), and IPSec virtual private networks (VPNs). Cisco SDM smart wizards can intelligently detect incorrect configurations and propose fixes, such as allowing Dynamic Host Configuration Protocol (DHCP) traffic through a firewall if the WAN interface is DHCP-addressed. Online help embedded within the Cisco SDM contains appropriate background information, in addition to step-by-step procedures to help you enter correct data in the Cisco SDM. Networking and security terms and definitions that you might encounter are included in an online glossary.

For network professionals familiar with Cisco IOS software and its security features, Cisco SDM offers advanced configuration tools to allow you to quickly configure and fine-tune router security features, allowing you to review the commands generated by Cisco SDM before delivering the configuration changes to the router.

Cisco SDM helps you configure and monitor routers from remote locations using Secure Socket Layer (SSL) and Secure Shell Protocol Version 2 (SSHv2) connections. This technology helps enable a secure connection over the Internet between the user browser and the router. When deployed at a branch office, a Cisco SDM-enabled router can be configured and monitored from corporate headquarters, reducing the need for experienced network administrators at the branch office.

## Cisco SDM Features

Cisco.com

- **Router security audit: Automate with ICSA- and Cisco TAC-approved security configuration**
- **Smart wizards for most-frequent router and security configuration tasks**
  - Averts misconfigurations with integrated routing and security
  - Secures the existing network infrastructure easily and cost-effectively
  - Cisco TAC- and ICSA-recommended security configurations
- **Startup wizard, one-step router lockdown, policy-based firewall and ACL management (firewall policy), one-step VPN (site-to-site), and inline IPS (Intrusion Prevention System)**
- **Guides untrained users through workflow**



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-7.6

Cisco SDM contains a Security Audit wizard that provides a comprehensive router security audit. Cisco SDM uses the Cisco Technical Assistance Center (TAC)- and International Computer Security Association (ICSA)-recommended security configurations as its basis for comparisons and default settings.

Other Cisco 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

Cisco SDM wizards help provide for faster VPN and firewall deployments. Cisco SDM contains a suggested workflow (located in the lower part of the browser windows) to guide untrained users through router configuration.

A typical process flow proceeds as shown in the figure:

- Step 1** Configure LAN parameters.
- Step 2** Configure WAN parameters.
- Step 3** Configure firewall parameters.
- Step 4** Configure VPN parameters.
- Step 5** End with a security audit.

## Cisco SDM Features (Cont.)

Cisco.com

- **Advanced users 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 embedded with Cisco SDM**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7.7

Although Cisco SDM is designed for users with little to no CLI experience, it is just as useful to advanced users. Advanced CLI users can use Cisco 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, Cisco SDM can be used to discover and configure existing LAN and WAN interfaces.

Cisco SDM contains an embedded online help system.

The table shows features and benefits.

| Feature                                   | Benefit                                                                                                                                                                                                                                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Embedded web-based management tool        | <ul style="list-style-type: none"><li>■ Turns the router into a complete security and remote-access solution with its own management tool</li><li>■ Does not require a dedicated management station</li><li>■ Allows remote management from any supported desktop or laptop</li></ul> |
| SSL- and SSHv2-based secure remote access | <ul style="list-style-type: none"><li>■ Provides for secure management across the WAN</li></ul>                                                                                                                                                                                       |
| At-a-glance router status views           | <ul style="list-style-type: none"><li>■ Offers quick graphical summary of router hardware, software, and primary router services such as VPN, firewall, QoS, and so on</li></ul>                                                                                                      |
| Router security audit                     | <ul style="list-style-type: none"><li>■ Assesses the vulnerability of the existing router</li><li>■ Provides quick compliance to best-practice (Cisco TAC, ICSA recommendations) security policies for routers</li></ul>                                                              |
| One-step router lockdown                  | <ul style="list-style-type: none"><li>■ Simplifies firewall and Cisco IOS software configuration without requiring expertise about security or Cisco IOS software</li></ul>                                                                                                           |

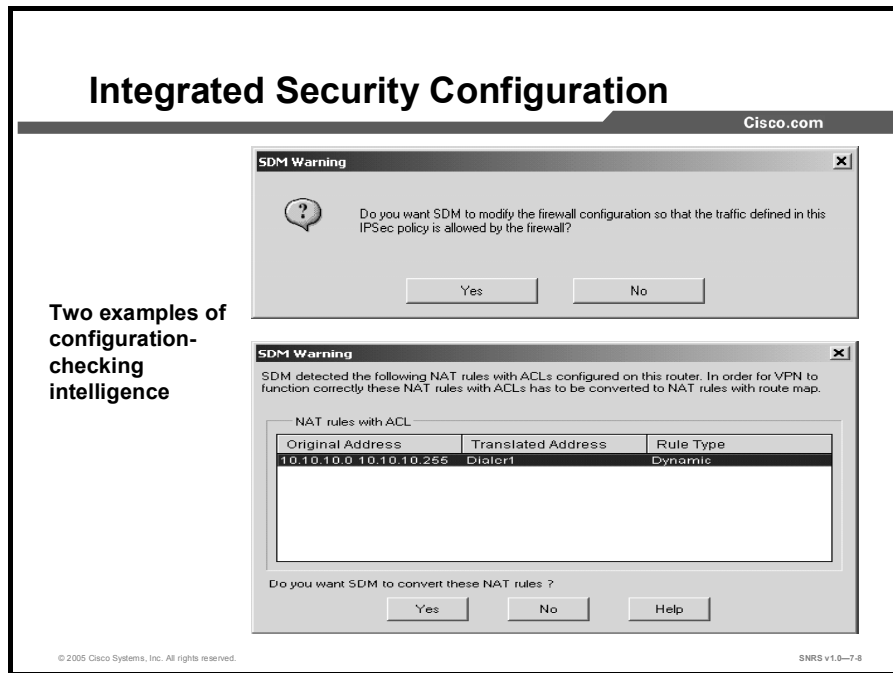
| Feature                                                                 | Benefit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Smart wizards for most frequent router and security configuration tasks | <ul style="list-style-type: none"> <li>■ Generates Cisco TAC-approved configurations</li> <li>■ Averts misconfigurations with integrated routing and security knowledge</li> <li>■ Reduces network administrators training needs for new Cisco IOS software security features</li> <li>■ Secures the existing network infrastructure easily and cost-effectively</li> </ul>                                                                                                               |
| Policy-based firewall and ACL management (firewall policy)              | <ul style="list-style-type: none"> <li>■ Allows security administrators to easily and quickly manage ACLs and packet inspection rules through a graphical and intuitive policy table</li> </ul>                                                                                                                                                                                                                                                                                           |
| Intrusion prevention                                                    | <ul style="list-style-type: none"> <li>■ Allows easy and quick provisioning of high-fidelity attack signatures on any router interface for inbound and outbound traffic</li> <li>■ Allows dynamic update of new IPS signatures without impacting basic router operations</li> <li>■ Allows graphical customization of IPS signatures for immediate response to new worm or virus variants</li> </ul>                                                                                      |
| Role-based access                                                       | <ul style="list-style-type: none"> <li>■ Offers logical separation of router between different router administrators and users</li> <li>■ Provides for secure access to Cisco SDM user interface and Telnet interface specific to the profile of each administrator</li> <li>■ Offers factory-default profiles: <ul style="list-style-type: none"> <li>— Administrator</li> <li>— Firewall administrator</li> <li>— Easy VPN Client user</li> <li>— Read-only user</li> </ul> </li> </ul> |
| WAN and VPN troubleshooting                                             | <ul style="list-style-type: none"> <li>■ Reduces mean time to repair (MTTR) by taking advantage of the integration of routing, LAN, WAN, and security features on the router for detailed troubleshooting</li> </ul>                                                                                                                                                                                                                                                                      |
| Startup wizard                                                          | <ul style="list-style-type: none"> <li>■ Reduces Cisco router deployment time for LAN, WAN, connectivity, and basic router security setup</li> </ul>                                                                                                                                                                                                                                                                                                                                      |
| Real-time monitoring and logging                                        | <ul style="list-style-type: none"> <li>■ Allows administrators to proactively manage router resources and security before they affect mission-critical applications on the network</li> </ul>                                                                                                                                                                                                                                                                                             |
| Preview Cisco IOS software CLI commands                                 | <ul style="list-style-type: none"> <li>■ Helps build Cisco IOS software expertise</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                              |
| Integrated online help and tutorials                                    | <ul style="list-style-type: none"> <li>■ Reduces the need for IT staff members to keep up with security technology updates and complex security configurations</li> </ul>                                                                                                                                                                                                                                                                                                                 |

The table shows features that are new in Cisco SDM.

### Features New in Cisco SDM 2.0

| Feature                                                                                                                                                                                                                    | Benefit                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Easy VPN Server</b></p> <p>Wizard-based configuration and real-time monitoring of remote-access VPN users</p> <p>Integration with on-router or remote authentication, authorization, and accounting (AAA) server</p> | <ul style="list-style-type: none"> <li>■ Offers wizard-based configuration and real-time monitoring of remote-access VPN users</li> <li>■ Provides integration with on-router or remote AAA server</li> </ul>                                                                                                               |
| <p><b>Intrusion prevention</b></p> <p>Dynamic signature update</p> <p>Quick deployment of default signatures</p> <p>Ability to customize signatures</p> <p>Validation of router resources before signature deployment</p>  | <ul style="list-style-type: none"> <li>■ Offers network-based protection against worms, viruses, and operating-system or protocol exploits</li> <li>■ Customizes signatures for Day-Zero protection against new variants of worms and viruses</li> </ul>                                                                    |
| <p><b>Role-based access</b></p> <p>Factory-default profiles:</p> <ul style="list-style-type: none"> <li>■ Administrator</li> <li>■ Read-only</li> <li>■ Firewall</li> <li>■ Easy VPN Remote</li> </ul>                     | <ul style="list-style-type: none"> <li>■ Offers secure, logical separation of router between network operations, security operations, and end users</li> <li>■ Multiservice switching platforms (MSSPs) can offer a graphical, read-only view of the customer premises equipment (CPE) services to end customers</li> </ul> |
| <p><b>WAN and VPN troubleshooting</b></p> <p>Layer 2 and above troubleshooting integrated with TAC knowledge base of recovery actions</p>                                                                                  | <ul style="list-style-type: none"> <li>■ Takes advantage of integration of routing, LAN, WAN, and security features on the router for detailed troubleshooting of IPSec VPNs or WAN links</li> </ul>                                                                                                                        |
| <p><b>QoS policy</b></p> <p>Three predefined categories:</p> <ul style="list-style-type: none"> <li>■ Real time</li> <li>■ Business critical</li> <li>■ Best effort</li> </ul>                                             | <ul style="list-style-type: none"> <li>■ Easily and effectively optimizes WAN and VPN bandwidth and application performance for different business needs (voice and video, enterprise applications, web, and so on)</li> </ul>                                                                                              |
| <p><b>Network-Based Application Recognition (NBAR)</b></p> <p>Application traffic performance monitoring</p>                                                                                                               | <ul style="list-style-type: none"> <li>■ Provides real-time validation of application usage of WAN and VPN bandwidth against predefined service policies</li> </ul>                                                                                                                                                         |
| <p><b>SSHv2</b></p> <p>Automatically use SSHv2 for all encrypted communication between Cisco SDM and router</p>                                                                                                            | <ul style="list-style-type: none"> <li>■ Provides for secure management between PC and Cisco router</li> </ul>                                                                                                                                                                                                              |

| Feature                                                                                                                                                                                  | Benefit                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Digital certificates</b></p>                                                                                                                                                       | <ul style="list-style-type: none"> <li>■ Offers highly scalable and more secure solution than pre-shared keys</li> <li>■ Now easy to use and deploy with the combination of Cisco SDM, Cisco IOS Certificate Authority (CA) Server, and Cisco Easy Secure Device Deployment (EzSDD)</li> </ul> |
| <p><b>Real-time network and router resource monitoring</b></p> <p>Graphical charts for LAN and WAN traffic and bandwidth usage</p>                                                       | <ul style="list-style-type: none"> <li>■ Offers faster and easier analysis of router resource and network resource usage</li> </ul>                                                                                                                                                            |
| <p><b>Task-based Cisco SDM user interface</b></p> <p>Newly designed home page</p> <p>Single starting point for primary security tasks</p> <p>Better navigation between related tasks</p> | <ul style="list-style-type: none"> <li>■ Provides for faster and easier configuration of security configurations—IPSec VPNs, firewall, ACLs, IPS, and so on</li> <li>■ Quick snapshot of router services configuration</li> </ul>                                                              |



When you are deploying a new router, Cisco SDM can be used to configure a Cisco IOS Firewall quickly using best practices recommended by the ICASA and Cisco TAC. Cisco SDM users can configure the strongest VPN defaults and automatically perform security audits. In addition, Cisco SDM users can perform one-step router lockdown for firewalls and one-step VPN for quick deployment of secure site-to-site connections. A recommended list of IPS signatures bundled with Cisco SDM allows quick deployment of worm, virus, and protocol exploit mitigation.

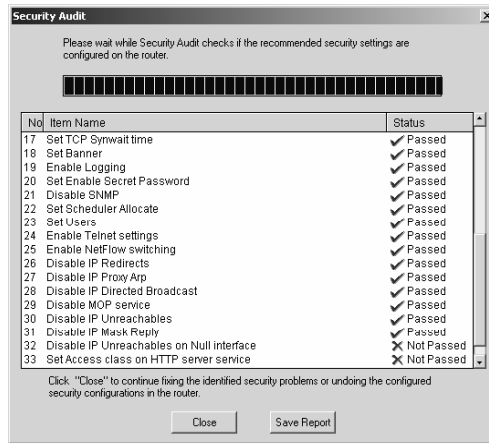
Cisco SDM contains embedded parameter-checking intelligence to help you accurately configure router VPN and firewall settings.

Two examples are shown in the figure. If Cisco SDM detects a configuration conflict, the SDM software will generate a warning window describing the condition.

You should always read Cisco SDM warning messages and consider following the recommendations to repair the original condition. Warnings messages usually allow you to choose either to let Cisco SDM fix the configuration conflict automatically or to fix the conflict manually yourself.

## Integrated Security Configuration

Cisco.com



| No | Item Name                                 | Status       |
|----|-------------------------------------------|--------------|
| 17 | Set TCP Synwait time                      | ✓ Passed     |
| 18 | Set Banner                                | ✓ Passed     |
| 19 | Enable Logging                            | ✓ Passed     |
| 20 | Set Enable Secret Password                | ✓ Passed     |
| 21 | Disable SNMP                              | ✓ Passed     |
| 22 | Set Scheduler Allocate                    | ✓ Passed     |
| 23 | Set Users                                 | ✓ Passed     |
| 24 | Enable Telnet settings                    | ✓ Passed     |
| 25 | Enable NetFlow switching                  | ✓ Passed     |
| 26 | Disable IP Redirects                      | ✓ Passed     |
| 27 | Disable IP Proxy Arp                      | ✓ Passed     |
| 28 | Disable IP Directed Broadcast             | ✓ Passed     |
| 29 | Disable MOP service                       | ✓ Passed     |
| 30 | Disable IP Unreachables                   | ✓ Passed     |
| 31 | Disable IP Mask Reply                     | ✓ Passed     |
| 32 | Disable IP Unreachables on Null interface | ✗ Not Passed |
| 33 | Set Access class on HTTP server service   | ✗ Not Passed |

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-7.9

When installed on an existing router, Cisco SDM allows users to perform one-step security audits to evaluate the strengths and weaknesses of their router configurations against common security vulnerabilities. Administrators can fine-tune their existing router security configurations to better suit their business needs. Cisco SDM also can be used for day-to-day operations such as monitoring, fault management, and troubleshooting.

## Router Configuration

In addition to security configuration, Cisco SDM helps users quickly and easily perform router services configuration, such as LAN and WAN interface configuration, routing, DHCP server, QoS policy, and so on.

Using the LAN configuration wizard, users can assign IP addresses and subnet masks to Ethernet interfaces and can enable or disable the DHCP server. Using the WAN configuration wizard, users can configure xDSL, T1/E1, Ethernet, and ISDN interfaces for WAN and Internet access. Additionally, for serial connections, users can implement Frame Relay, PPP, and High-Level Data Link Control (HDLC) encapsulation. Cisco SDM also allows configuration of static routing and common dynamic routing protocols such as Open Shortest Path First (OSPF), Routing Information Protocol (RIP) Version 2, and Enhanced Interior Gateway Routing Protocol (EIGRP).

QoS policies can now easily be applied to any WAN or VPN tunnel interface using Cisco SDM. The QoS Policy wizard automates the Cisco architecture guidelines for QoS policies to effectively prioritize the traffic between real-time applications (voice or video), business-critical applications (Structured Query Language [SQL], Oracle, Citrix, routing protocols, and so on) and the rest of the network traffic (web and e-mail, for example). Network-Based Application Recognition (NBAR)-based monitoring in the Cisco SDM allows users to visually inspect the application layer traffic in real time and confirms the impact of QoS policies on different classes of application traffic.



## Monitoring and Troubleshooting

In monitor mode, Cisco SDM provides a quick, graphical status of key router resources and performance measurements such as the interface status (up or down), CPU, and memory usage. Cisco SDM takes advantage of integrated routing and security features on routers to provide in-depth diagnostics and troubleshooting of WAN and VPN connections. For example, while troubleshooting a failed VPN connection, the Cisco SDM verifies the router configurations and connectivity from the WAN interface layer to the IPsec crypto map layer. While testing configuration and remote peer connectivity at each layer, Cisco SDM provides pass or fail status, possible reasons of failure, and Cisco TAC-recommended actions for recovery.

Cisco SDM monitor mode also allows users to view the number of network access attempts that were denied by the Cisco IOS Firewall, and it provides easy access to the firewall log. Users also can monitor detailed VPN status, such as the number of packets encrypted or decrypted by IPsec tunnels, and Cisco Easy VPN Client session details.

## Cisco SDM User Profiles

Cisco.com

- **Small office-home office**
  - Working knowledge of networking and security. No significant Cisco IOS CLI experience
  - SOHO Cisco 800 router user typically expected to use Cisco Router Web Setup, then use SDM for security configuration
  - SMB/SMB branch office:
    - Nonexpert, technical system administrator
    - Rudimentary knowledge of networks and security; no significant Cisco IOS CLI experience
- **Enterprise branch office:**
  - Network or site administrator
  - Modest knowledge of Cisco CLI and basic security
- **Enterprise headquarters: Cisco-knowledgeable, CLI-capable; expert in either networking or security**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-10

Cisco SDM was designed with the following users in mind:

- **Small office-home office (SOHO):** These Cisco SDM users usually have a working knowledge of networking and security, but no significant Cisco IOS CLI experience. SOHO Cisco 800 Series router users typically use the Cisco Router Web Setup (CRWS) tool for general router configuration tasks, and then use Cisco SDM for router security configuration.
- **Small-to-medium business (SMB) and SMB branch office:** SMB and SMB branch office Cisco 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 Cisco SDM users are typically network site administrators with a modest knowledge of Cisco CLI and basic security.
- **Enterprise headquarters:** These Cisco SDM users are typically very knowledgeable about the CLI and are capable in both networking and security.

All of these users can benefit from Cisco SDM features.

# Cisco SDM Software

This topic provides an overview of the software functions and processes.

## Supported Cisco Routers and Cisco IOS Software Releases

Cisco.com

- **Cisco SDM is supported on a number of Cisco router platforms and Cisco IOS software releases.**
- **Always verify Cisco SDM router and Cisco IOS release support at [www.cisco.com/go/sdm](http://www.cisco.com/go/sdm).**

© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-7-11

Cisco SDM is supported on a number of Cisco routers and the associated Cisco IOS software versions.

Always consult the latest information regarding Cisco SDM router and Cisco IOS software release support at [www.cisco.com/go/sdm](http://www.cisco.com/go/sdm).

## Obtaining Cisco SDM

Cisco.com

- **Cisco SDM is factory loaded on supported routers manufactured as of June 2003.**
- **Always check [www.cisco.com/go/sdm](http://www.cisco.com/go/sdm) for the latest information regarding SDM support.**
- **Cisco SDM cannot be ordered independent of the router.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-7-12

Cisco SDM comes preinstalled on several Cisco router models manufactured in June 2003 or later that were purchased with the VPN bundle.

Cisco 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 Cisco SDM installed, and you would like to use SDM, you must download it from [Cisco.com](http://Cisco.com) and install it on your router. Ensure that your router contains enough flash memory to support both your existing flash file structure and the Cisco SDM files.

## Cisco SDM Files

Cisco.com

The **sdm-v10.zip** file contains the following files:

- **sdm.tar**
- **home.html**
- **home.shtml**
- **home.tar**
- **ips.tar**
- **attack-drop.sdf**
- **sdmconfig-xxxx.cfg** file:
  - **Enables HTTP server**
  - **Enables SSH/Telnet**
  - **Provides a default credential—username and password**
  - **Default configuration file specific to router series:**
    - **For example: sdmconfig-18xx.cfg**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-13

If you choose to install Cisco SDM on an existing (SDM-supported) Cisco router, you must obtain the **SDM-Vnn.zip** file from Cisco.com and copy it to your router flash file system.

## Installing Cisco SDM

Cisco.com

- **Task 1: Download the Cisco SDM files and a Cisco IOS image to a TFTP server.**
- **Task 2: Configure your router to support Cisco SDM.**
- **Task 3: Copy the Cisco SDM Files to the Router.**
- **Task 4: Start Cisco SDM.**
- **Requires a minimum 5.3 MB extra (available) router flash memory.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-14

---

**Note** For information on how to determine whether or not Cisco SDM is installed on your router, refer to the FAQ document, available at <http://www.cisco.com/go/sdm>. In the left panel, click **Product Literature**, and then click **Q&A**.

---

The sections that follow contain instructions for installing Cisco SDM on your router and using it to configure Cisco IOS features.

## Task 1: Download the Cisco SDM Files and a Cisco IOS Image to a TFTP Server

This section contains instructions for downloading both Cisco SDM and an upgraded version of Cisco IOS software from the Cisco.com website. If you do not need to upgrade your Cisco IOS software, follow only the instructions for downloading Cisco SDM.

---

**Note** Cisco SDM files are contained in a .zip file that is available on Cisco.com. To open this type of file and extract the SDM files, you must have the WinZip utility installed on your PC. You can obtain WinZip by following the link <http://www.winzip.com>.

---

**Step 1** On your PC, open a web browser.

Enter the following URL in your web browser:

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

Log in using your Cisco.com user identification and password, and follow the instructions on the SDM Software page to download the Cisco SDM .zip file (SDM-Vnn.zip).

---

**Note** It is recommended that you also download and read the Cisco SDM release notes for the version of Cisco SDM that you have. That document is also available at the following URL: <http://www.cisco.com/go/sdm>.

---

**Step 2** Double-click the SDM-Vnn.zip file and extract the files to the root directory of a TFTP server. The TFTP server can be a PC with a TFTP server utility. If you need assistance extracting the files to the directory that you want to place them in, refer to the WinZip online help.

**Step 3** If you do not need to upgrade your Cisco IOS version, you are now ready to download the Cisco SDM files to your router. Skip to the appropriate section below:

- Copying SDM Files to Cisco 830, 1700, 1800, 2600, 2800, 3600, 3700, or 3800 Series Routers

If you need to upgrade your Cisco IOS version, enter the following URL into your web browser to access the Cisco IOS Software Center:

<http://www.cisco.com/public/sw-center/sw-ios.shtml>

If you need help determining which Cisco IOS image supports the IOS features that you want, use the Feature Navigator tool. This tool is available at the following link:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

Click **Search by Feature** to select the features that you need and find the Cisco IOS image that has those features. Feature Navigator provides a web-based form that you use to assemble the list of features that you want. Once you have listed the features, you specify the platform. Feature Navigator returns a list of image names for that platform that support the features that you specified. You can click on the name of the Cisco IOS image that you want to go to the download page for that image.

- Step 4** Download the Cisco IOS image to your PC and then transfer it to a TFTP server. If the TFTP server is on your PC, save the file to the TFTP server root directory.

Cisco SDM and the upgraded Cisco IOS image are now downloaded to the TFTP server.

## Task 2: Configure Your Router to Support Cisco SDM

You can install and run Cisco SDM on a router that is already in use without disrupting network traffic, but you must ensure that a few configuration settings are present in the router configuration file.

Access the CLI using Telnet or the console connection to modify the existing configuration before installing Cisco SDM on your router.

- Step 1** Enable the HTTP and HTTPS servers on your router by entering the following global configuration mode commands:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

If the router supports HTTPS, the HTTPS server will be enabled. If not, the HTTP server will be enabled. HTTPS is supported in all images that support the crypto and IPSec feature set, starting from Cisco IOS Software Release 12.2(5)T.

- Step 2** Create a user account defined with privilege level 15 (enable privileges). Enter the following global configuration mode command:

```
Router(config)#username username privilege 15 password 0 password
```

You will use this username and password to log on to Cisco SDM.

- Step 3** Configure SSH and Telnet for local login and privilege level 15. Use the following commands:

```
Router#line vty 0 4
Router(line)# privilege level 15
Router(line)# login local
Router(line)# transport input telnet ssh
Router(line)#exit
```

If your router supports 16 vty lines, you can add the following lines to the configuration file:

```
Router(config)#line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet ssh
Router(config-line)#exit
```



**Step 4** Optionally enable local logging to support the log monitoring function. Enter the following global configuration mode command:

```
Router (config) #logging buffered 51200 warning
```

**Step 5** Leave configuration mode by entering the **end** command at the router prompt:

```
Router (config) #end
```

## Task 3: Copy the Cisco SDM Files to the Router

See the appropriate section below to copy the Cisco SDM files to your router.

- Copying SDM Files to Cisco 830, 1700, 1800, 2600, 2800, 3600, 3700, or 3800 Series Routers

To download the Cisco SDM files to a Cisco 1700, 2600, 3600, or 3700 Series router, follow the instructions in this section. If your router already has Cisco SDM Version 1.0.1 or later installed and running, you can use the Cisco SDM automatic update feature to copy the contents of the `SDM-Vnn.zip` file to the router.

---

**Note** Cisco SDM requires approximately 5.4 MB of free flash memory. If your flash memory has multiple partitions, you must copy the SDM files to partition number 1. You can use the **show flash: summary** command to determine whether partition 1 has sufficient memory.

---

**Step 1** Access the router CLI using a Telnet connection or the console port.

**Step 2** Copy the Cisco SDM files on the TFTP server to the router flash memory, using the **copy tftp** CLI command. In this procedure, the first **copy tftp** command is followed by an explanation of the router prompts and responses that you may see.

**Step 3** Enter the **copy tftp** command to copy `sdm.tar` to flash memory and respond to the router prompts, as shown in the next steps:

```
Router# copy tftp://<tftp server IP address>/sdm.tar flash:
```

**Step 4** Confirm the destination filename by pressing **Return**. Do not change the name.

```
Destination filename [sdm.tar]?
```

If a copy of this file already exists in flash, Cisco IOS software displays the message shown next. If this file does not already exist in flash, you will not see this message.

```
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
```

**Step 5** Confirm the overwrite by pressing **Return**.

When the copy begins, the router displays a message similar to the following:

```
Accessing tftp://171.69.17.19//tftp-root/sdm.tar...
```

**Step 6** When prompted to erase flash, enter **n** so that you do NOT erase flash.

```
Erase flash: before copying? [confirm]n
```

The router displays a message similar to the following:

```
Loading //tftp-root/sdm.tar from 171.69.17.19 (via
FastEthernet0): !!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

If insufficient space is available, the router displays the next message:

```
%Error copying flash:sdm.tar (No space left on device)
```

**Step 7** Copy the files `home.tar`, and `home.html` to flash using the following commands:

```
Router# copy tftp://<tftp server IP address>/home.tar flash:
Router# copy tftp://<tftp server IP address>/home.html flash:
```

**Step 8** The router prompts you to confirm the destination filename as shown earlier, and asks if you want to erase flash memory. Enter **n** so that you do NOT erase flash.

```
Erase flash: before copying? [confirm]n
```

There is no need to copy the file `home.shtml` to the router.

**Step 9** If you intend to use Cisco SDM Intrusion Prevention System (IPS), use the **copy tftp** command to copy the files `ips.tar`, and `attack-drop.sdf` to flash memory.

```
Router# copy tftp://<tftp server IP address>/ips.tar flash:
Router# copy tftp://<tftp server IP address>/attack-drop.sdf
flash:
```

As in earlier steps, do not change the destination filename, and do not erase flash.

**Step 10** (Optional) If you want to use the Cisco SDM Reset to Factory Default feature, you need to copy the default Cisco SDM configuration file for your router from the TFTP server to router flash memory.

---

**Caution** If used, the Reset to Factory Default feature overwrites the router configuration with the Cisco SDM factory default values.

---

The configuration files in the `SDM-Vnn.zip` file are `sdmconfig-83x.cfg`, `sdmconfig-1701.cfg`, `sdmconfig-1710-1721.cfg`, `sdmconfig-1711-1712.cfg`, `sdmconfig-1751-1760.cfg`, `sdmconfig-26xx.cfg`, and `sdmconfig-36xx-37xx.cfg`.

**Step 11** Enter the following command:

```
Router# copy tftp://<tftp server IP address>/sdmconfig-
modelnum.cfg flash:
```

**Step 12** Confirm the destination filename, and when prompted do NOT erase flash memory.

```
Erase flash: before copying? [confirm] n
```

The router displays a message similar to the following:

```
Loading //tftp-root/sdmconfig-modelnum.cfg from 171.69.17.19
(via FastEthernet0): !!!!!
!!
```

Cisco SDM is now installed on your router.

## Task 4: Start Cisco SDM

Cisco SDM is stored in the router flash memory. It is invoked by executing an HTML file in the router archive, which then loads the signed SDM Java file. To launch Cisco SDM, complete the following steps:

**Step 1** From your browser, enter the following URL:

**https://<router IP address>**

The https:// designation specifies that SSL protocol be used for a secure connection.

The http:// designation can be used if SSL is not available.

The Cisco IOS home page will appear in the browser window. Click **Cisco Router and Security Device Manager** in the left pane. The username and password challenge will appear in a separate dialog box.

**Step 2** If you used your existing router configuration file, enter the username and password for the privileged (privilege level 15) account on your router.

The Cisco SDM Java applet will begin loading to your PC.

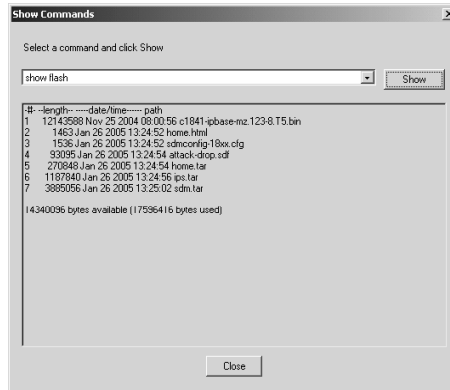
**Step 3** Cisco SDM is a signed Java applet. This may cause your browser to display a security warning. Accept the certificate.

**Step 4** Cisco SDM displays the Launch page.

**Step 5** When the Launch window has loaded, Cisco SDM displays the SDM home page. The home page gives you a snapshot of the router configuration and the features that the Cisco IOS image supports. Cisco SDM starts in Wizard mode, in which you can perform configuration tasks using a sequence of windows that break the configuration task into manageable steps.

## Displaying Router Flash

Cisco.com



- Many show commands are also available within the Cisco SDM user interface.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0--7-15

Cisco 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 memory is used and how much is available.

---

**Note** If you are not sure whether Cisco SDM is loaded into flash memory or you need to know how much flash is available, use the **show flash** CLI command.

---

# Using the Startup Wizard

This topic describes the use of the Startup wizard in the initial configuration of your router.

## Router Administration Using Cisco SDM

Cisco.com

- **Cisco SDM is used for configuring, managing, and monitoring a single Cisco access router.**
- **Cisco SDM allows the ability for multiple concurrent users to be logged in.**
- **It is *not* recommended that multiple users use Cisco SDM to modify the configuration at the same time.**
- **You can use Cisco SDM or CLI commands or both:**
  - **Use CLI commands for features not supported by SDM.**
  - **Use Cisco SDM to configure security policies on unsupported interfaces.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-7-18

Cisco 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 Cisco SDM, which is located in the router flash memory.

A common scenario that can be supported by Cisco SDM is to have a user monitoring the router, while at the same time another user may use Cisco SDM to modify the configuration of the router. It is *not* recommended that multiple users use Cisco SDM to modify the configuration at the same time. Although Cisco SDM will permit this scenario, it does not assure consistent or predictable results.

You now have the flexibility to configure the router with both Cisco SDM and the CLI. Since the Cisco SDM user interface does not support all of the Cisco IOS software functionality, for example, QoS, you can augment the Cisco SDM-generated configuration with some CLI commands.

For unsupported interfaces, such as ISDN interfaces, Cisco SDM automatically detects whether the interfaces support security features, such as firewalls, crypto maps, and Network Address Translation (NAT). If the security features are supported, you can use SDM to configure the security features to the unsupported interfaces. However, you will still need to configure the unsupported interface parameters directly through the CLI.

## Accessing Cisco SDM for the First Time

Cisco.com

### Accessing Cisco SDM on a factory-fresh router with SDM installed:

1. Connect PC to the lowest LAN Ethernet port of the router, using crossover cable.
2. Use a static IP address for the PC: (10.10.10.2/255.255.255.0).
3. Launch a supported browser.
4. The default URL to access Cisco SDM is <https://10.10.10.1>.
5. The Cisco SDM default login is:
  - Username: **sdm**
  - Password: **sdm**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-19

Complete the following steps when you access Cisco SDM for the first time. This procedure assumes that you are either using an out-of-box router with Cisco SDM installed or that a default SDM configuration was loaded into flash memory.

- Step 1** Connect a PC to the lowest-number LAN Ethernet port of the router, using a crossover cable.
- Step 2** Assign a static IP address to the PC. It's recommended that you use 10.10.10.2 with a 255.255.255.0 subnet mask.
- Step 3** Launch a supported browser.
- Step 4** Enter the URL **<https://10.10.10.1>**. You will be prompted to log in.
- Step 5** Log in using the default user account:
- Username: **sdm**
- Password: **sdm**

The Cisco SDM Startup wizard opens, requiring you to enter basic network configuration information.

## Startup Wizard: Welcome Window

Cisco.com



- **Automatically displays the default configuration**

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-20

---

**Note** The Startup wizard information needs to be entered only once and will appear only 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

The screenshot displays the Cisco Startup Wizard interface. The main window is titled "Startup Wizard" and has a "Cisco.com" logo in the top right corner. The interface is divided into two main sections. The left section, titled "Startup", contains a "Basic Configuration" panel. This panel includes a "Host Name" field with the placeholder "yourname" and a "Domain Name" field with the placeholder "yourdomain.com". Below these fields is a section for "Enable Secret Password", which includes a checkbox and a note: "Router password is used to administrate the router (CLI)". The right section, titled "Change default username and password", includes a note: "Your router comes with a factory default username and password. It is very important to change these values to secure your router." This section contains four input fields: "Current User Name" (with the value "sdm"), "Current Password" (with a masked value "\*\*\*\*\*"), "Enter New User Name" (with an empty field), "Enter new Password" (with an empty field), and "Re-enter New Password" (with an empty field). At the bottom of the window, there is a copyright notice: "© 2005 Cisco Systems, Inc. All rights reserved." and a version number: "SNRS v1.0-7-21".

- 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 six characters in the **Enter New Password** field.
- Step 10** Enter the new password, once more, in the **Re-Enter New Password** field.

---

**Note** Cisco 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

The screenshot shows a window titled "Startup Wizard" with a sub-window titled "LAN Interface Configuration". The sub-window contains the following text and fields:

Configure the IP address of this interface. It is recommended that you change the default value of the IP Address

Interface: Ethernet0

IP address:

Subnet Mask:  or Subnet bits:

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7.22

- 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

Cisco.com

Startup Wizard

**Startup**

**DHCP Server Configuration**

You can configure your router to be a DHCP server and provide IP addresses to the other hosts on your Local Area Network:

Enable DHCP Server on LAN Interface

Typical DHCP Start and End IP addresses based on the LAN IP address 192.100.100.1 you entered in previous screen:

Typical Start IP address: 192.100.100.1

Typical End IP address: 192.100.100.254

Start IP address:

End IP address:

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-23

**Step 19** Check the **Enable DHCP Server on LAN Interface** check box.

---

**Note** For Cisco 800 Series routers, the check box is checked 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

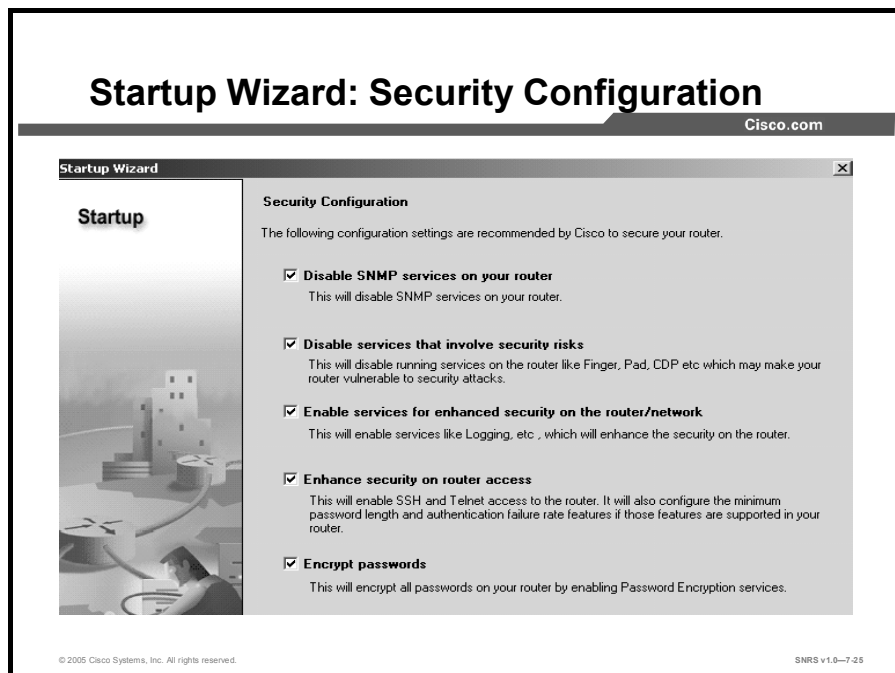
Cisco.com

The screenshot shows a window titled "Startup Wizard" with a sub-window titled "Domain Name Server Configuration". On the left, there is a sidebar with "Startup" selected. The main area contains the following text: "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." Below this text are two input fields: "Primary DNS:" followed by a text box and "(Optional)", and "Secondary DNS:" followed by a text box and "(Optional)".

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7.24

- Step 23** Enter a primary Domain Name System (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.



Cisco SDM lets you disable some features that are enabled by default in Cisco IOS software. When enabled, these features can create security risks or use memory in the router. Cisco SDM also enables basic security features for protecting the router and the surrounding networks.

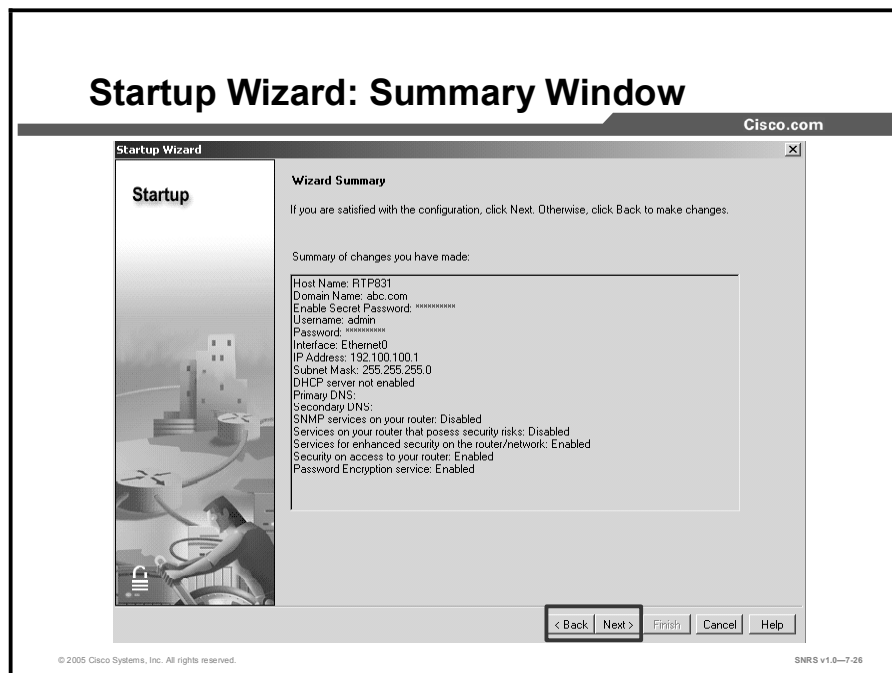
Generally, you should leave the check boxes in this window checked, unless you know that your requirements are different. Later, if you decide to enable a feature listed here, you can use the Cisco SDM advanced mode to re-enable it.

**Step 26** Check or uncheck the check boxes according to your security requirements:

- **Disable SNMP services on your router:** Disables Simple Network Management Protocol (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, 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.

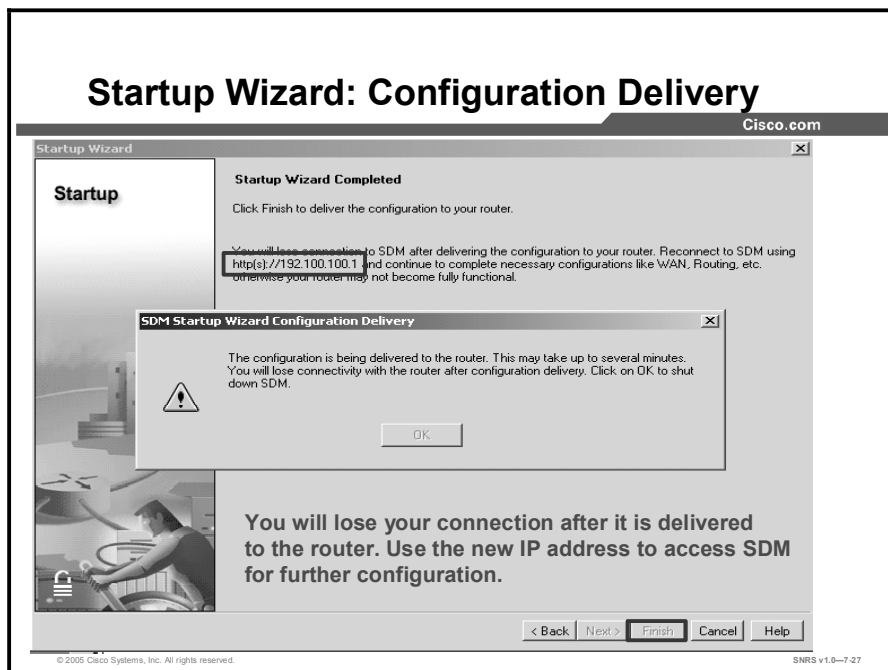
## Startup Wizard: Summary Window



**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 relaunch Cisco SDM is displayed.

---

**Step 30** Click **Finish** to deliver the configuration to router flash memory. The SDM Startup Wizard Configuration Delivery message appears. After the configuration is delivered, the OK button becomes enabled.

**Step 31** Click **OK** to shut down Cisco SDM and terminate the connection.

## Accessing Cisco SDM: Ongoing

Cisco.com

- **Already configured router with Cisco SDM installed:**
  1. Use a LAN/WAN connection.
  2. Manage the router using either HTTP or HTTPS with `https://<router IP address>/`.
- **Note:**
  - `https://` specifies that SSL be used for a secure connection.
  - `http://` can be used if SSL is not available.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-28

To access Cisco SDM after the Startup wizard is completed, use either HTTP or HTTPS and use the router IP address, as shown in the figure.

When you use HTTPS, it specifies that the SSL protocol be used for a secure connection. If SSL is not available, use HTTP to access the router.

After you configure your WAN interface, you can access Cisco SDM through a LAN or WAN interface.

## Cisco 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 that the PC is not blocked on the interface by a 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
- **Cisco SDM installed?**
  - Access it with `https://<router IP address>/flash/sdm.shtml`.
  - Enter the CLI `show flash` command.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-23

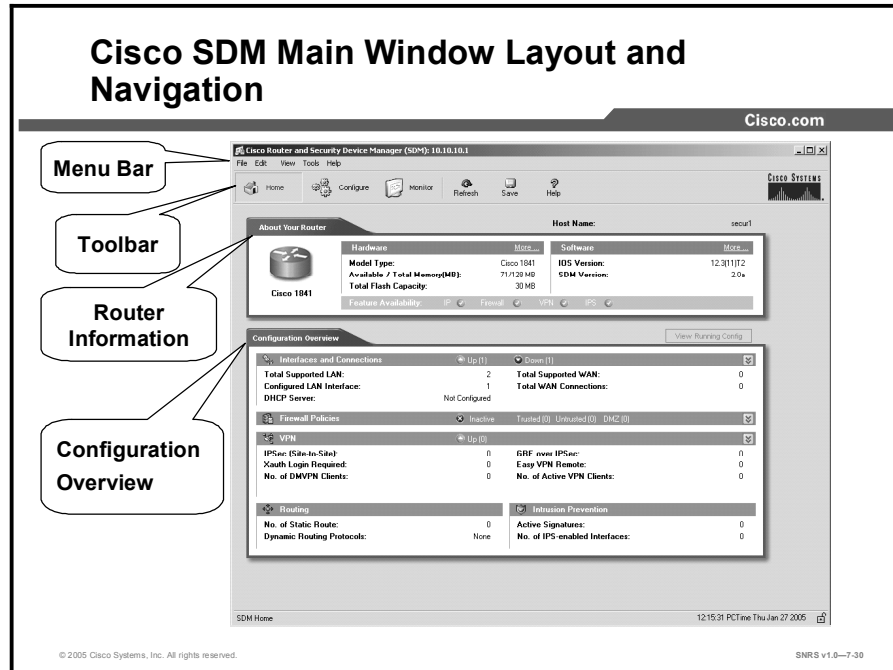
Use the following tips to troubleshoot Cisco SDM access problems:

- First determine whether 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 (Cisco 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 Cisco 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 Cisco SDM access.
  - Is HTTP server enabled on the router? If it is not, enable it and check that other Cisco 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 is not working? Ensure that your PC is not being blocked by a new ACL. Remember that Cisco SDM requires HTTP, SSH, and Telnet access or Remote Copy Protocol (RCP) access to the router (which could have been inadvertently disabled in a security lockdown).
- Is Cisco SDM installed?
  - The quickest way to determine whether Cisco SDM is installed 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 that the required Cisco SDM files are present.



# Cisco SDM User Interface

This topic describes the various elements of the Cisco SDM user interface.



The home page supplies basic information about the router hardware, software, and configuration. This page contains the following sections:

- **Host Name:** This is the configured name of the router.
- **About Your Router:** This area shows basic information about your router hardware and software, and contains the fields shown in the table.

| Hardware               |                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Model Type             | Shows the router model number.                                                                                                                                     |
| Available/Total Memory | Available RAM and total RAM.                                                                                                                                       |
| Total Flash Capacity   | Flash plus webflash (if applicable).                                                                                                                               |
| Software               |                                                                                                                                                                    |
| IOS Version            | The version of Cisco IOS software that is currently running on the router.                                                                                         |
| Cisco SDM Version      | The version of Cisco SDM software that is currently running on the router.                                                                                         |
| Feature Availability   | The features available in the Cisco IOS image that the router is using are designated by a check. The features that SDM checks for are IP, Firewall, VPN, and IPS. |

## The More Link

The More link displays a popup window providing additional hardware and software details.

- **Hardware Details:** In addition to the information presented in the About Your Router window, this tab displays information about the following:
  - Where the router boots from—flash memory or the configuration file
  - Whether the router has accelerators, such as VPN accelerators
  - A diagram of the hardware configuration
- **Software Details:** In addition to the information presented in the About Your Router section, this tab displays information about the feature sets included in the Cisco IOS image.

## Configuration Overview

This section of the home page summarizes the configuration settings that have been made. If you want to view the running configuration, click **View Running Config**.

## Interfaces and Connections

This area shows the following information:

- **Up:** The number of connections that are up.
- **Down:** The number of connections that are down.
- **Double arrow:** Click to display or hide details.
- **Total Supported LAN:** Shows the total number of LAN interfaces that are present in the router.
- **Total Supported WAN:** The number of Cisco SDM-supported WAN interfaces that are present on the router.
- **Configured LAN Interface:** The number of supported LAN interfaces currently configured on the router.
- **Total WAN Connections:** The total number of Cisco SDM-supported WAN connections that are present on the router.
- **DHCP Server:** Configured and not configured.
- **DHCP Pool (Detail View):** If one pool is configured, this area shows the starting and ending address of the DHCP pool. If multiple pools are configured, it shows a list of configured pool names.
- **Number of DHCP Clients (Detail View):** Current number of clients leasing addresses.
- **Interface:** Name of the configured interface.
  - **Type:** Interface type
  - **IP Mask:** IP address and subnet mask
  - **Description:** Description of the interface

## Firewall Policies

This area shows the following information:

- **Active:** A firewall is in place.
- **Inactive:** No firewall is in place.
- **Trusted:** The number of trusted (inside) interfaces.
- **Untrusted:** The number of untrusted (outside) interfaces.
- **DMZ:** The number of Demilitarized Zone (DMZ) interfaces.
- **Double arrow:** Click to display or hide details.
- **Interface:** The name of the interface to which a firewall has been applied.
- **Firewall icon:** Whether the interface is designated as an inside or an outside interface.
- **NAT:** The name or number of the NAT rule applied to this interface.
- **Inspection Rule:** The names or numbers of the inbound and outbound inspection rules.
- **Access Rule:** The names or numbers of the inbound and outbound access rules.

## VPN

This area shows the following information:

- **Up:** The number of active VPN connections.
- **Double arrow:** Click to display or hide details.
- **IPSec (Site-to-Site):** The number of configured site-to-site VPN connections.
- **GRE over IPSec:** The number of configured generic routing encapsulation (GRE) over IPSec connections.
- **Xauth Login Required:** The number of Cisco Easy VPN connections awaiting an Extended Authentication (Xauth) login.

---

**Note** Some VPN servers or concentrators authenticate clients using Xauth. This shows the number of VPN tunnels awaiting an Xauth login. If any Easy VPN tunnel awaits Xauth login, a separate message panel is shown with a Login button. Click **Login** to enter the credentials for the tunnel.

---

---

**Note** If Xauth has been configured for a tunnel, it will not begin to function until the login and password have been supplied. There is no timeout after which it will stop waiting; it will wait indefinitely for this information.

---

- **Easy VPN Remote:** The number of configured Easy VPN Remote connections.
- **No. of DMVPN Clients:** If the router is configured as a Dynamic Multipoint VPN (DMVPN) hub, the number of DMVPN clients.
- **No. of Easy VPN Clients:** If this router is functioning as an Easy VPN Server, the number of Easy VPN clients with active connections.

- **Interface:** The name of an interface with a configured VPN connection.
- **IPSec Policy:** The name of the IPSec policy associated with the VPN connection.

## Routing

This area shows the following information:

- **No. of Static Routes:** The number of static routes configured on the router.
- **Dynamic Routing Protocols:** Lists any dynamic routing protocols that are configured on the router.

## Intrusion Prevention

This area shows the following information:

- **Active Signatures:** The number of active signatures that the router is using. These may be built in, or they may be loaded from a remote location.
- **No. of IPS-Enabled Interfaces:** The number of router interfaces on which IPS has been enabled.

# Cisco SDM Wizards

This topic describes some of the Cisco SDM wizards.

**Cisco SDM Wizard Options** Cisco.com

- **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
  - Advanced inside/outside/DMZ with multiple interfaces
- **VPN:** Access three types of VPN wizards:
  - Secure site-to-site VPN
  - Cisco Easy VPN
  - GRE tunnel with IPSec VPN
- **Security Audit:** Perform a router security audit, with a button for router lockdown.
- **IPS:** Intrusion Prevention System
- **QOS:** Quality of Service

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-7-31

Cisco 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, HDLC WAN interfaces. Check [www.cisco.com/go/sdm](http://www.cisco.com/go/sdm) for the latest information about 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 lockdown wizard
- **Reset to Factory Default wizard:** Resets the router configuration to the Cisco SDM factory default configuration settings.

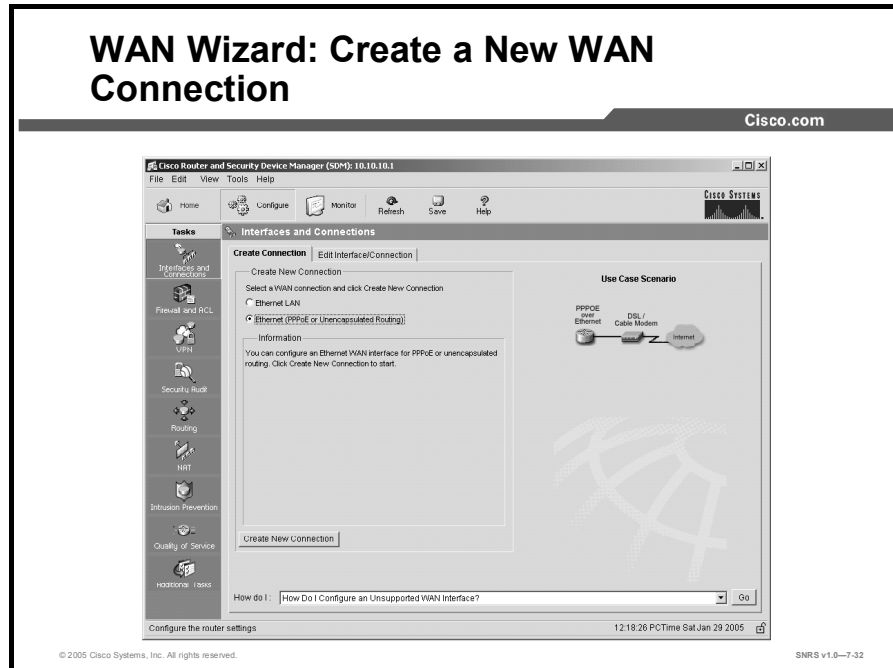
---

**Note** At the end of each wizard procedure, all changes are automatically delivered to the router using Cisco SDM-generated CLI commands. You can choose whether or not to preview the commands to be sent. The default is to not preview the commands.

---

# Using Cisco SDM to Configure a WAN

This topic describes how to configure a WAN interface.



Complete the following steps to create a new WAN connection:

- Step 1** Click the **Interfaces and Connections** wizard button in the Tasks menu. 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** Click a WAN connection type radio button to choose a connection type 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.

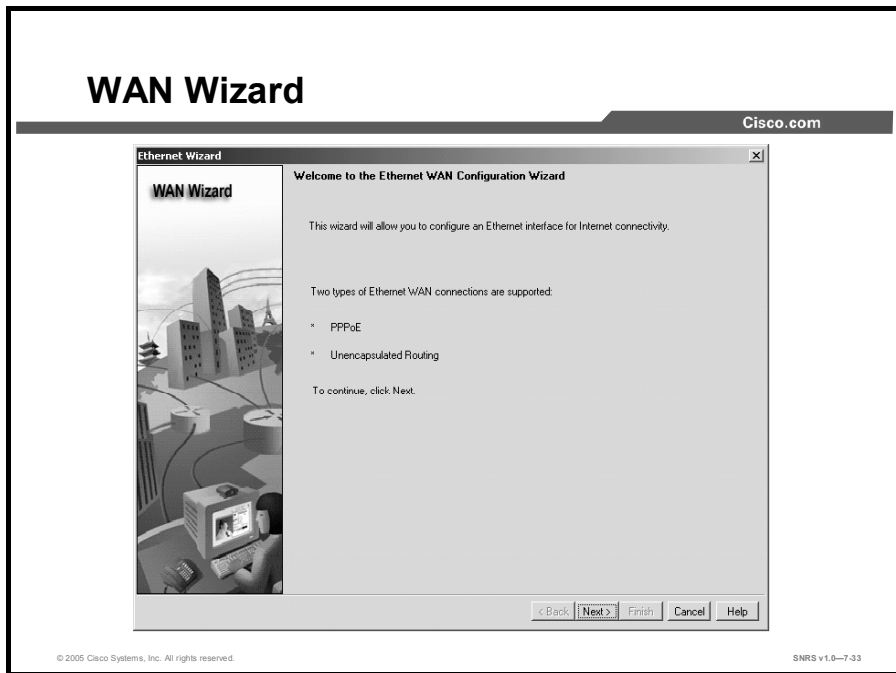
---

**Note** If your router has interfaces not supported by Cisco SDM, such as an ISDN interface, or a supported interface that has an unsupported configuration that was created using the 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.

---

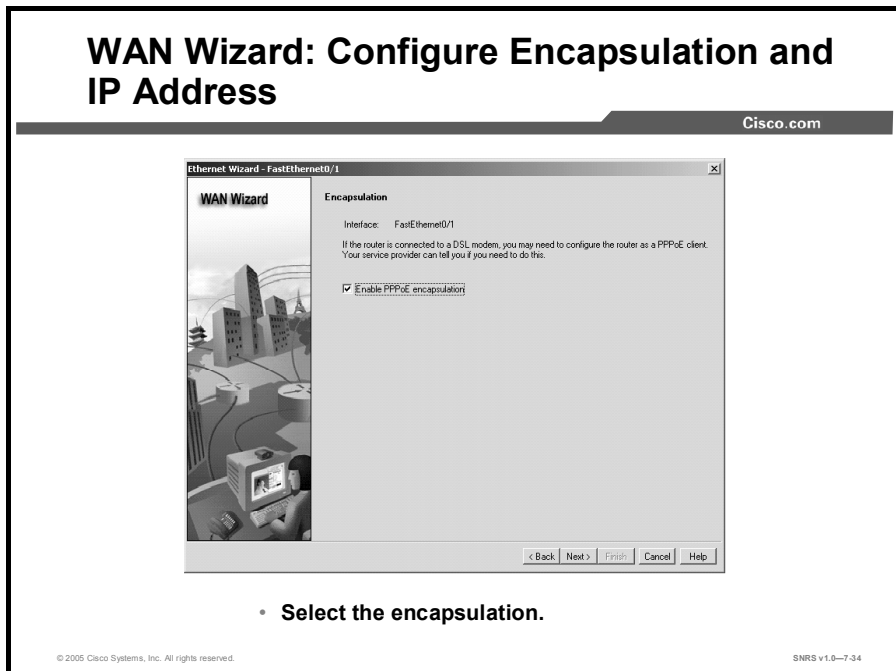
- Step 3** Click **Create a New Connection**.

## WAN Wizard



The WAN Wizard window appears.

**Step 4** Click **Next**.



**Step 5** Check the appropriate encapsulation type check box.

**Step 6** Click **Next**. The IP Address window opens.



## WAN Wizard: IP Address Configuration

Cisco.com

- **IP address**
- **Choose DHCP client**
- **IP unnumbered**
- **Easy IP**

The screenshot shows a dialog box titled "Ethernet Wizard - FastEthernet0/1" with a "WAN Wizard" sub-header. The main heading is "IP Address" with the instruction "Enter the IP Address for this connection". There are four radio button options: "Static IP Address", "Dynamic (DHCP Client)", "IP Unnumbered to", and "Easy IP (IP Negotiated)". The "Dynamic (DHCP Client)" option is selected. The "IP Unnumbered to" option has a dropdown menu showing "FastEthernet0/0". At the bottom, there are buttons for "< Back", "Next >", "Finish", "Cancel", and "Help".

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-35

- Step 7** Click the **Static IP Address** radio button.
- Step 8** Enter a static IP address in the IP Address field.
- Step 9** Enter a subnet mask in the Subnet Mask field (or click the subnet up and down arrows and let Cisco SDM enter the correct subnet).
- Step 10** Click **Next**. The Authentication window opens.

## WAN Wizard: Authentication

Cisco.com

**Authentication**

Select the authentication type, and enter your username and password, provided by your service provider.

Note: If your service provider has given you a username and password, and you are unsure of the authentication type for this connection, select both CHAP and PAP.

Authentication Type:  CHAP  PAP

Username:

Password:

Confirm Password:

< Back Next > Finish Cancel Help

- **Select authentication type.**
- **Enter username and password.**

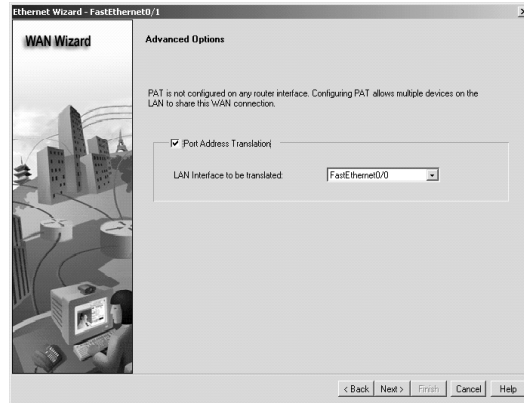
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-36

- Step 11** Choose the appropriate authentication type.
- Step 12** Enter your username and password.
- Step 13** Click **Next**. The Advanced Options window opens.

## WAN Wizard: Advanced Options

Cisco.com



- Check the **Port Address Translation** check box and the **LAN interface to be translated**.

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7.37

- Step 14** (Optional) Check the **Port Address Translation** check box.
- Step 15** (Optional) Choose the LAN interface to be translated from the list.
- Step 16** Click **Next**. The Summary window opens.

## WAN Wizard: Summary

Cisco.com

The screenshot shows the 'WAN Wizard - FastEthernet0/1' window. On the left is a 'WAN Wizard' graphic with a cityscape and a computer. The main area is titled 'Summary' and contains the following configuration details:

Please click Finish to deliver to the router:

Selected Interface : FastEthernet0/1  
Dialer : Dialer0  
PPPoE Encapsulation : Enabled  
IP Address : Dynamic (DHCP Client)

AUTHENTICATION: CHAP and PAP  
Username : cisco  
Password : \*\*\*\*\*

PAT :  
Inside Interface : FastEthernet0/0  
Outside Interface : Dialer0

Test the connectivity after configuring

Navigation buttons: < Back, Next >, Finish, Cancel, Help

© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-38

**Step 17** Examine the summary. Go back and make any changes required.

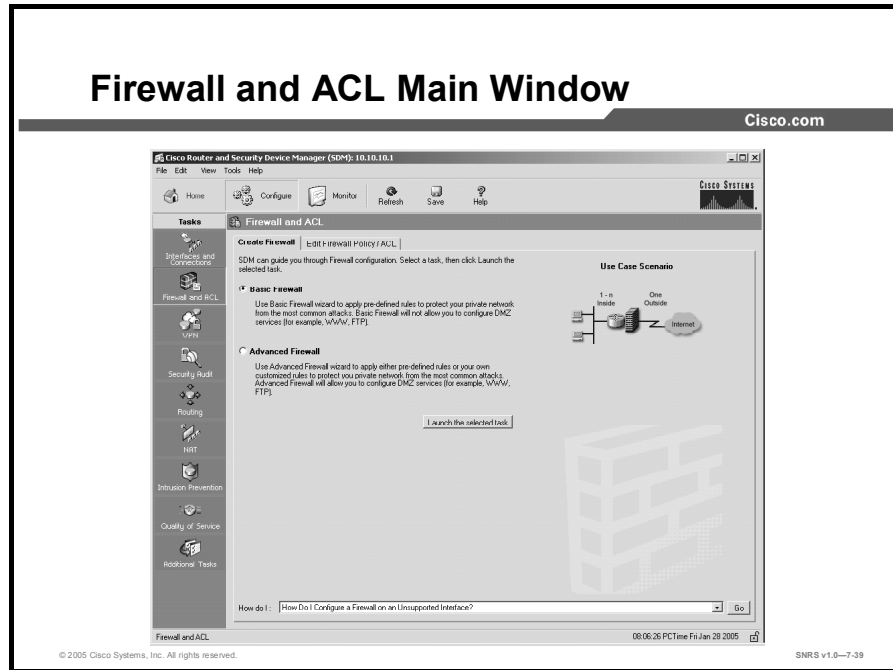
**Step 18** Click **Finish**. The SDM Commands Delivery Status message dialog opens. Once the delivery is completed, the OK button becomes active.

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.

# Using Cisco SDM to Configure a Firewall

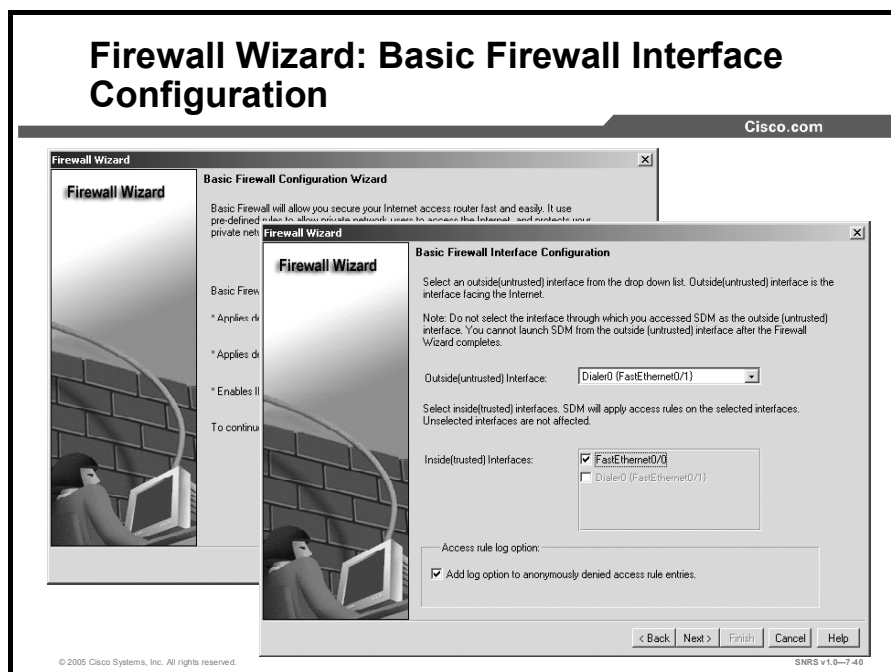
This topic describes how to use Cisco SDM to configure a firewall.



Complete the following steps to configure a firewall:

- Step 1** Click the **Firewall and ACL** button in the Tasks menu. The Firewall wizard main window opens.
- Step 2** Click the radio button for the type of firewall that you want to create:
  - **Basic Firewall:** Click this radio button if you want Cisco 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:** Click this radio button if you want Cisco 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



**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 the WAN of your organization.
- The inside (trusted) interfaces connect to the LAN. You can select multiple interfaces.

---

**Note** When you are choosing firewall settings, keep in mind which interface you are using to access Cisco SDM. If you select the interface through which you accessed SDM as the outside (untrusted) interface, you will lose your connection to SDM because it is now protected by a firewall. This means that you will not be able to launch Cisco 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 ACLs before you can log in to Cisco SDM again.

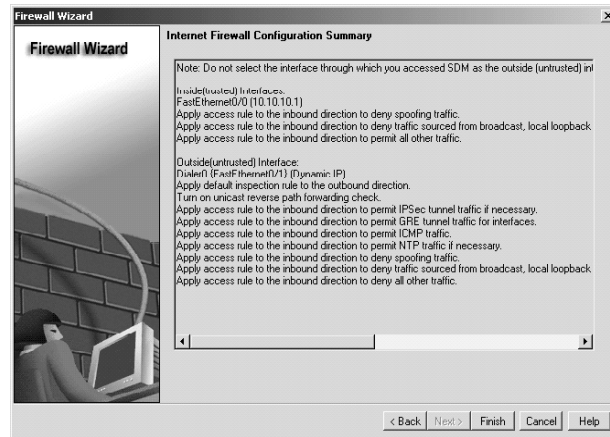
---

**Step 6** Click 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 Internet Firewall Configuration Summary window opens.

## Firewall Wizard: One-Step Firewall Configuration Summary

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

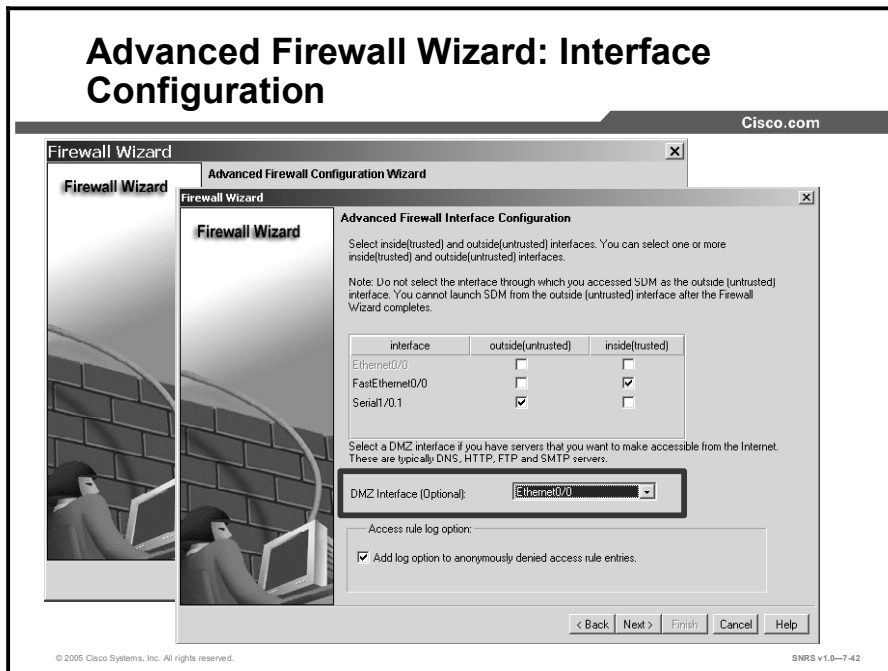
SNRS v1.0-7.41

This window summarizes the firewall information. You can review the information by using the **Back** button to return to windows in the wizard to make changes.

Cisco SDM lists the router interfaces that you designated as the interfaces in this wizard session, along with their IP addresses. Cisco SDM describes in English, rather than in 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 whether the settings are as you want them.
- Step 9** Click **Finish**.

## Advanced Firewall Wizard: Interface Configuration

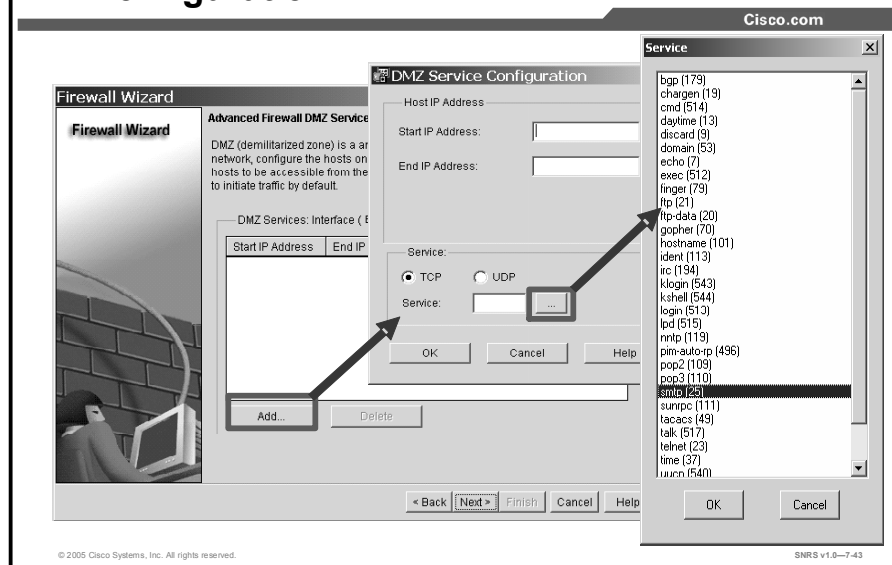


To create an advanced firewall, choose a DMZ interface as shown in the figure.

- Step 1** Choose 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



**Step 3** Click **Add**. The DMZ Service Configuration window opens.

**Step 4** Configure the DMZ network hosts by specifying the address range in the **Start IP Address** and **End IP Address** fields.

---

**Note** To specify an individual host, enter a starting IP address with no ending IP address.

---

**Step 5** Click either the **TCP** or **UDP** radio button, if you want to allow traffic for one of those services.

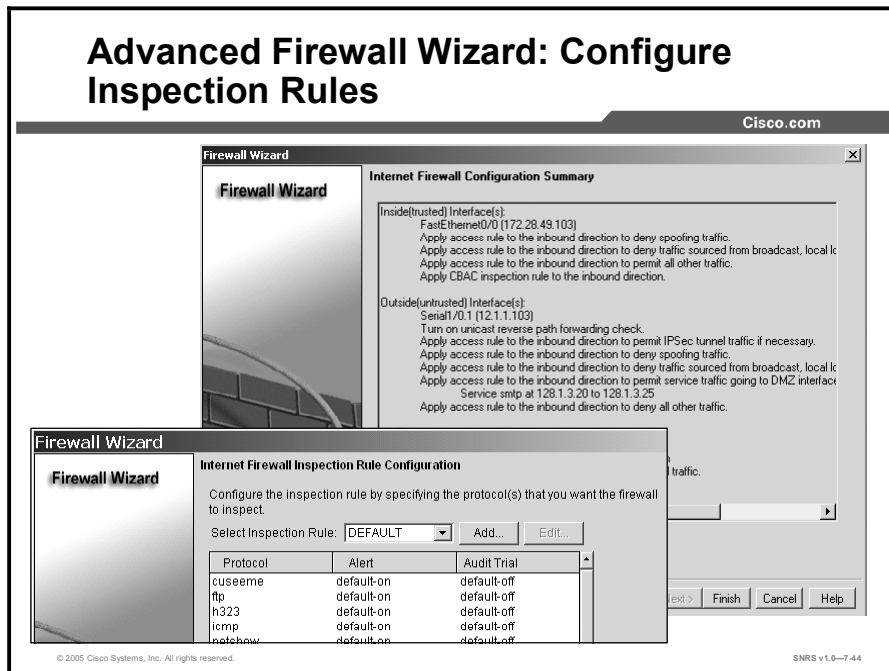
**Step 6** Click the ... button that follows the Service field. The Service window opens.

**Step 7** Choose 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 you are finished adding services, click **Next**. The Internet Firewall Inspection Rule Configuration window opens.

## Advanced Firewall Wizard: Configure Inspection Rules



**Step 10** Use the default Cisco SDM inspection rule or click **Add** to build a new inspection rule.

**Step 11** Click **Next**. The Internet Firewall Configuration Summary window opens.

---

**Note** The Firewall wizard takes into consideration any preexisting VPNs configured for the router. The Firewall wizard will not create a rule that will block valid VPN users.

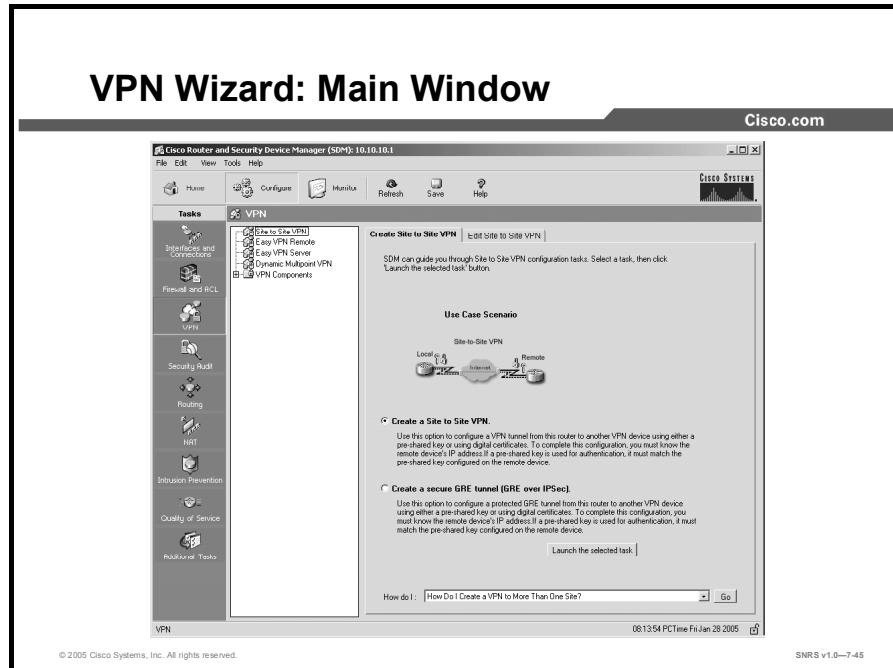
---

**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 Cisco SDM to Configure a VPN

This topic describes how to use Cisco SDM to create VPNs on supported routers.

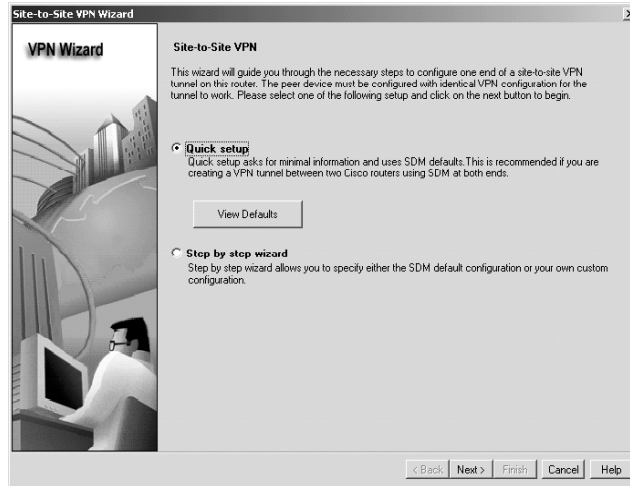


You can let Cisco SDM guide you through a simple VPN configuration by using the VPN wizard:

- Step 1** Click the **VPN** button in the Tasks menu. The VPN main window opens.
- Step 2** Click one of the two VPN wizard radio buttons:
  - **Create a Site-to-Site VPN:** Creates a router-to-router VPN using pre-shared keys
  - **Create a Secure GRE Tunnel (IPSec over GRE):** Configures a protected GRE tunnel between this router and a peer system
- Step 3** Click **Launch the Selected Task** button. This example uses digital certificates. The Site-to-Site VPN window opens.

# VPN Wizard

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7-46

- Step 4** Click one of the two wizard option radio buttons:
- **Quick Setup:** Uses Cisco SDM-generated defaults:
    - Default Internet Key Exchange (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 deviceClick **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 Cisco SDM.

---

- Step 5** Click **Next**. The VPN Connection Information window opens.

## VPN Wizard: VPN Connection Configuration

Cisco.com

Site-to-Site VPN Wizard

VPN Wizard

**VPN Connection Information**  
Select the interface for this VPN connection: Dialer0 (FastEthernet0/0) Details...

**Peer Identity**  
Select the type of peer(s) used for this VPN connection: Peer with static IP address  
Enter the IP Address of the remote peer: 10.10.10.2

**Authentication**  
Authentication ensures that each end of the VPN connection uses the same secret key.  
 Pre-Shared Keys Pre-Shared Key: Re-enter Key:  
 Digital Certificates

**Traffic to encrypt**  
The traffic between the source and the destination specified here will be protected by the transforms (encryption algorithms) defined in the default transform set.

**Source**  
Select a source interface where traffic to be encrypted originates:  
FastEthernet0/0 Details...

**Destination**  
Enter the IP Address and subnet mask of the destination where encrypted traffic terminates:  
IP Address: 10.10.10.0  
Subnet Mask: 255.255.255.0 or 24

< Back Next > Finish Cancel Help

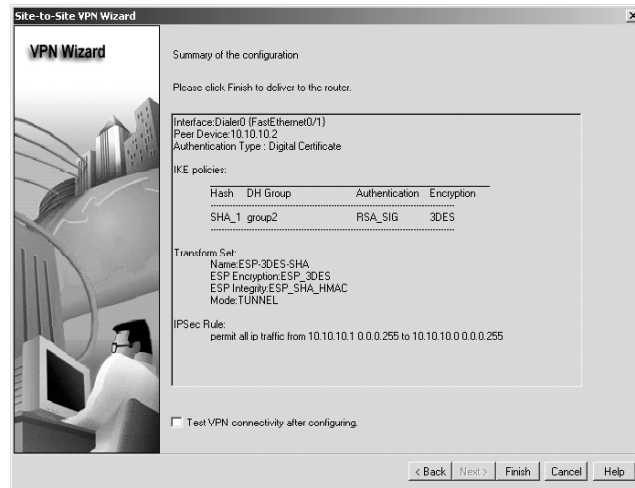
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7.47

- Step 6** Choose the router interface used for the VPN connection from the list.
- Step 7** Enter the remote VPN router IP address or host name in the Peer Identity area.
- Step 8** In the Authentication area, check the **Digital Certificates** radio button.
- Step 9** Choose the source (inside) interface in the Source list.
- Step 10** Input destination address and subnet mask.
- Step 11** Click **Next**. The Summary of the Configuration window opens.

## VPN Wizard: Summary of the Configuration

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-748

**Step 12** Click **Finish** to deliver the configuration to the router. The SDM Commands Delivery Status window opens.

**Step 13** Click **OK**.

# Using Cisco SDM to Perform Security Audits

This topic describes how to use Cisco SDM to perform security audits on your router.

## Security Audit: Overview

Cisco.com

- The security audit 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 the firewall to the outside interfaces.
  - Disable SNMP or enable it 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 ACLs.

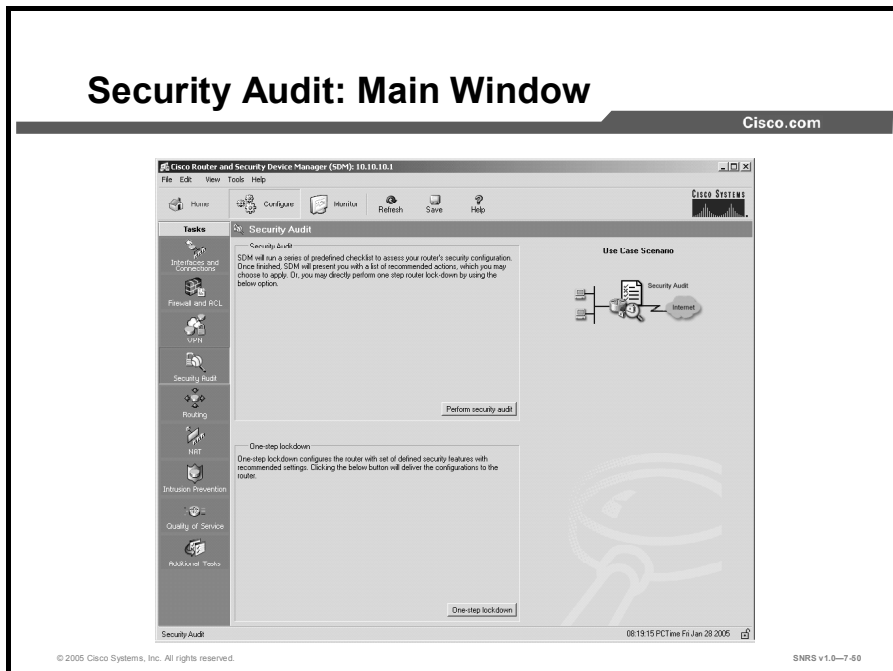
© 2005 Cisco Systems, Inc. All rights reserved.SNRS v1.0-7.49

The Cisco 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 (Cisco Discovery Protocol, ip source-route, ip classless)
- Applies a firewall to the outside interfaces
- Disables SNMP or enables it with hard-to-guess community strings
- Shuts down unused interfaces using the **no ip proxy-arp** command
- Forces passwords for the router console and vty lines
- Forces an enable secret password
- Enforces the use of ACLs

## Security Audit: Main Window



The Security Audit wizard contains two modes:

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

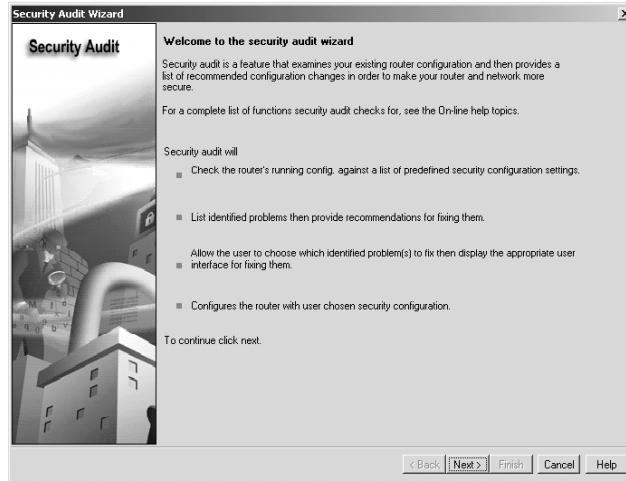
Complete the following steps to perform a security audit:

- Step 1** Click **Security Audit** in the Tasks menu.
- Step 2** Click one of the two available Security Audit wizard buttons. In the example used here, the Perform Security Audit radio button is used. The Inside and Outside Interfaces dialog box opens.
- Step 3** Select the inside and outside interfaces from the list.
- Step 4** Click **Next**. The Welcome to the Security Audit Wizard window opens.



## Security Audit Wizard

Cisco.com



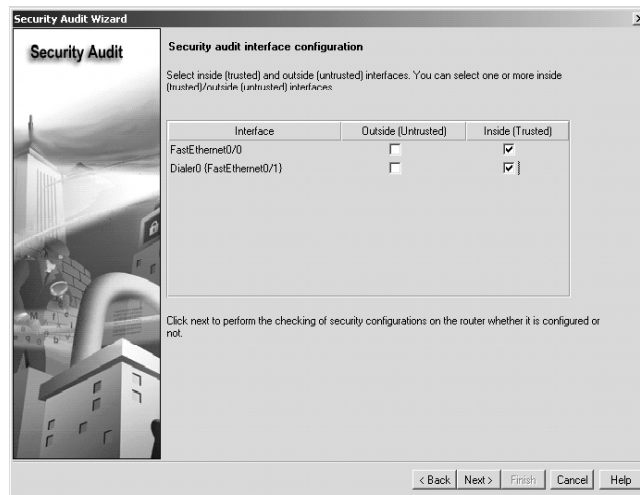
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-7.51

**Step 5** Click **Next**. The Security Audit Interface Configuration window opens.

## Security Audit Interface Configuration

Cisco.com



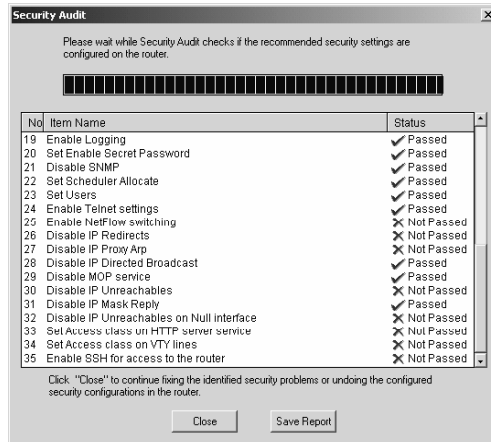
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-7.52

**Step 6** Click **Next**. The Security Audit window appears.

# Security Audit

Cisco.com



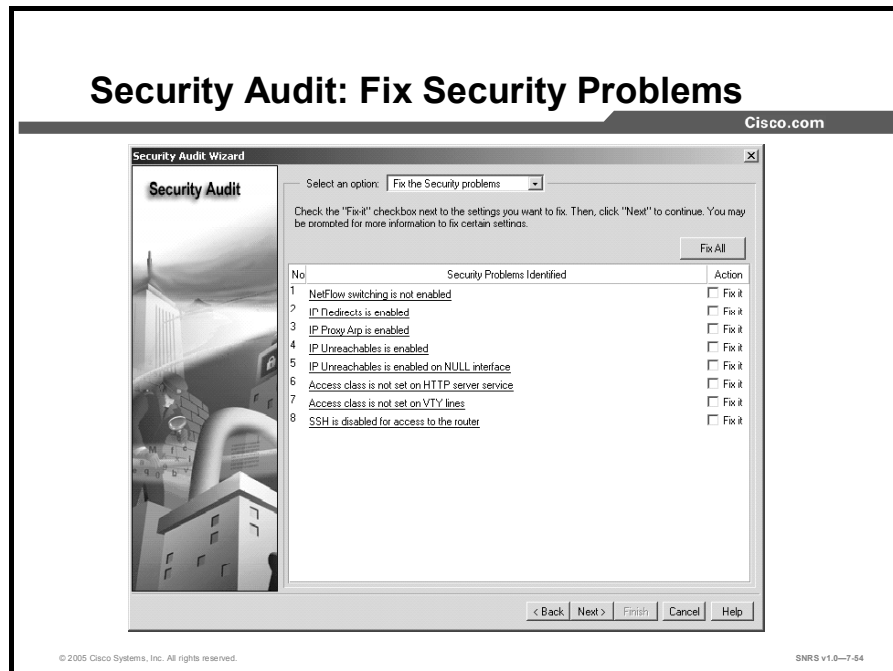
© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0-7-63

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

**Step 7** Click **Close**. The Security Audit Report Card window opens.

## Security Audit: Fix Security Problems



**Step 8** Check the **Fix It** check boxes next to any problems that you want Cisco 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.

---

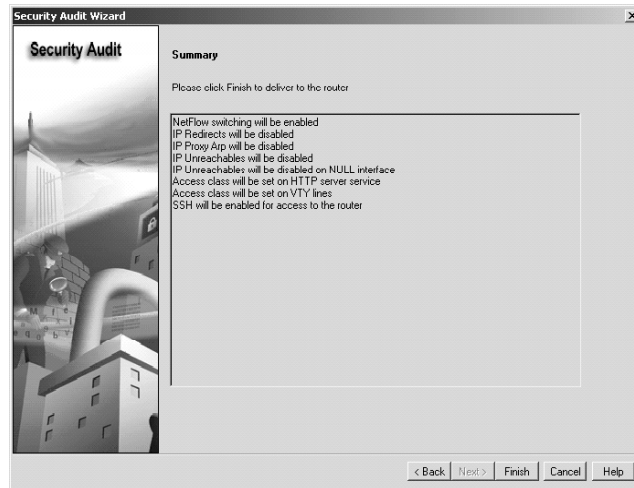
**Step 9** Click **Next**. Additional windows may appear requiring your input, such as entering a password.

Pay special attention to any warning messages that appear. Make sure that you do not “fix” a potential security breach and lock yourself out of the router, too.

The Security Audit Summary window opens.

## Security Audit: Summary

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

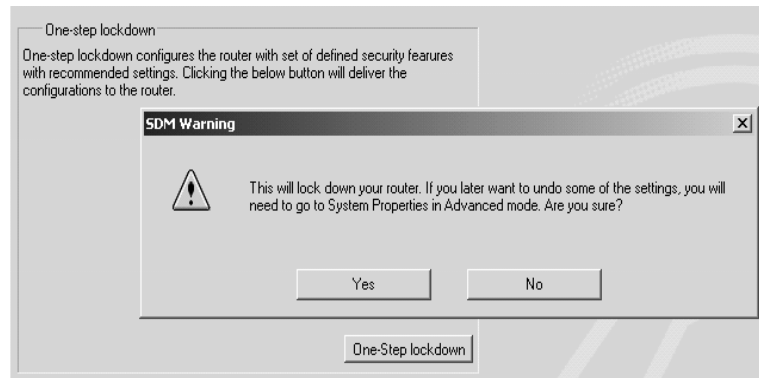
SNRS v1.0—7-55

**Step 10** Review the changes that will be delivered to the router.

**Step 11** Click **Finish**. The changes are sent to the router.

## Security Audit: One-Step Lockdown Wizard

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

SNRS v1.0—7.56

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 the problems found.

Refer to the Cisco SDM online Help for a list of security features and a description of them.

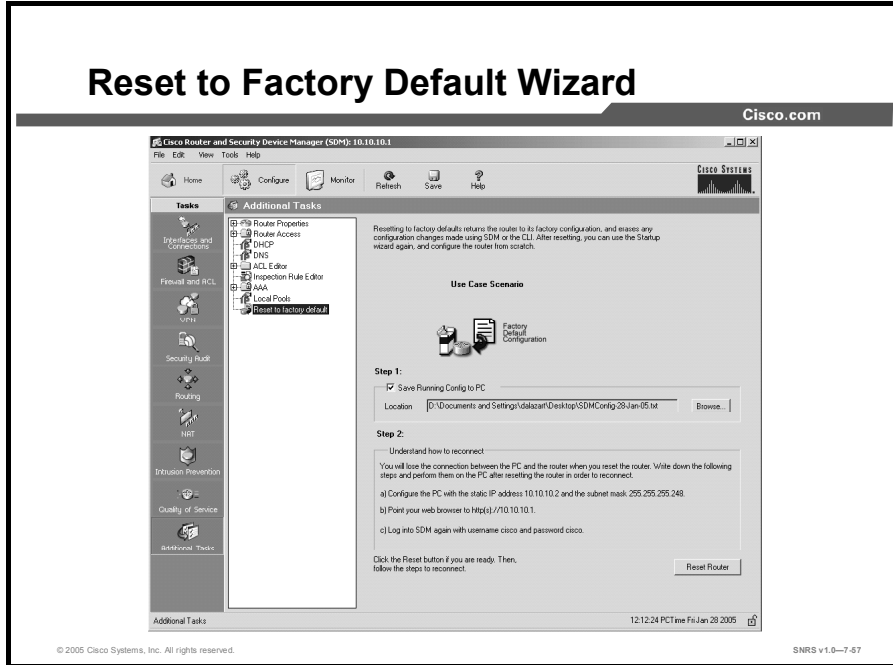
---

**Note** You can use the Advanced Mode-System Properties function to undo specific settings.

---

# Using the Reset to Factory Default Wizard

This topic describes how to perform a reset to factory defaults.



You can reset your Cisco router to factory defaults using the Cisco SDM Reset to Factory Default wizard:

**Step 1** Access the wizard by clicking the **Additional Tasks** button in the Tasks menu, then choosing **Reset to Factory Default** from the menu that appears. 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 Cisco SDM host PC. Cisco SDM verifies that this step has been completed before allowing you to continue with the reset (or erase) procedure.
- **Reset Router:** Performs the actual reset procedure.

**Step 2** In the Step 1 area of the window, check the **Save Running Config to PC** check box. Cisco SDM prompts you to choose a directory on your local PC where it will store the configuration file.

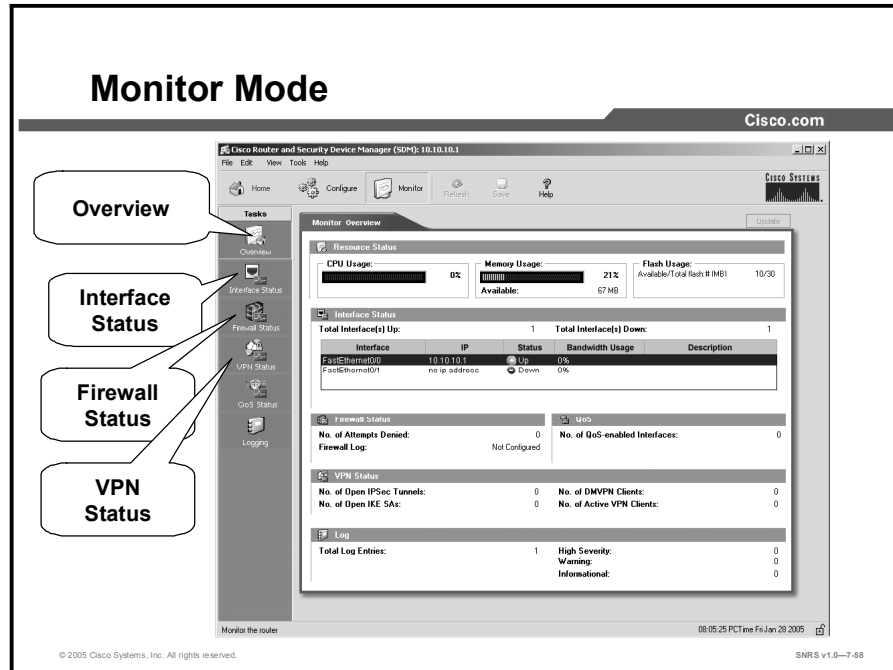
**Note** Before you proceed to the Step 2 area of the window, understand how to reconnect to your router following the reset procedure. The wizard window explains the process for reconnecting to your router. Make sure that you read and understand this procedure before continuing.

**Step 3** Click the **Reset Router** button. You will lose your connection to Cisco 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 lowest-number LAN interface of the router.

# Using Cisco SDM Monitor Mode

This topic describes the elements of the Cisco SDM monitor view.

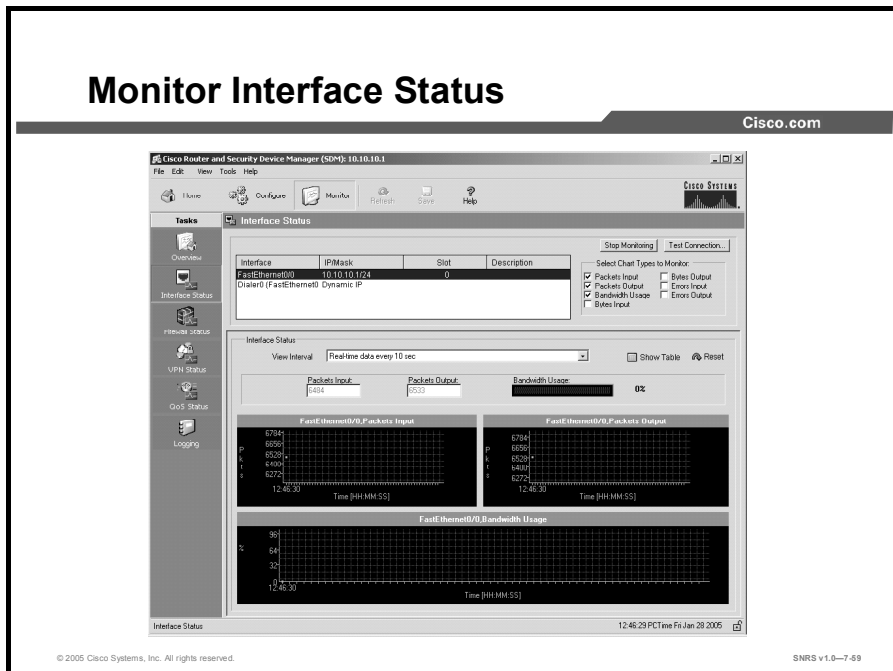


Monitor view lets you view information about your router, the router interfaces, the firewall, and any active VPN connections. You can also view any messages in the router event log.

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 to view (for example, packets and errors, in or out)
- **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
- **QoS Status:** Display statistics on QoS configured on the router
- **Logging:** Displays an event log categorized by severity level

## Monitor Interface Status



The Interface Status window displays the current status of the various interfaces on the router and the numbers of packets, bytes, or data errors that have traveled through the selected interface. Statistics shown in this window are cumulative since the last time the router was rebooted, the counters were reset, or the selected interface were reset.

### Monitor Interface or Stop Monitoring Button

Click this button to start or stop monitoring the selected interface.

### Test Connection Button

Click this button to test the selected connection. A dialog box appears that enables you to specify a remote host to ping through this connection. The dialog then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps that you need to take to correct the problem.

### Interface List

Select the interface for which you want to display statistics from this list. The list contains the name, IP address and subnet mask, the slot and port where it is located, and any Cisco SDM or user description entered.



## Select Chart Types to Monitor Group

These check boxes are the data items for which Cisco SDM can show statistics on the selected interface. These data items are as follows:

- **Packet Input:** The number of packets received on the interface
- **Packet Output:** The number of packets sent by the interface
- **Bytes Input:** The number of bytes received on the interface
- **Bytes Output:** The number of bytes sent by the interface
- **Input Errors:** The number of errors occurring while receiving data on the interface
- **Output Errors:** The number of errors occurring while sending data from the interface

To view statistics for any of these items, complete these steps:

- Step 1** Choose the item or items that you want to view by checking the associated check boxes.
- Step 2** Click the **Monitor Interface** button to see statistics for all selected data items.

## Interface Status Area

### View Interval Field

This drop-down menu allows you to choose both the amount of data shown for each item and the frequency with which the data is updated. It offers the following options:

- Display real-time data; poll every 10 seconds. This option will continue polling the router for a maximum of two hours, resulting in approximately 120 data points.
- Display last 10 minutes of data; poll every 10 seconds.
- Display last 60 minutes of data; poll every 1 minute.
- Display last 12 hours of data; poll every 12 minutes.

### Show Table or Hide Table Button

Click this button to show or hide the performance charts.

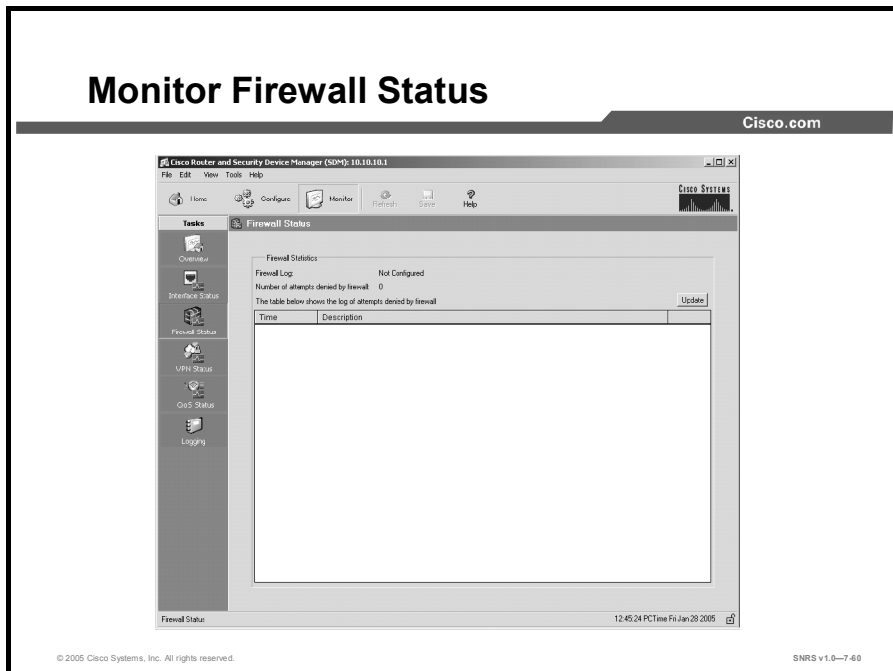
### Reset Button

Click this button to reset the interface statistic counts to zero.

### Chart Area

This area shows the charts and simple numerical values for the data specified.

## Monitor Firewall Status



This Firewall Status page displays statistics about the firewall configured on the router. The statistics and log entries shown in this window are determined by log messages generated by the firewall. In order for the firewall to generate log entries, you must configure individual access rules to generate log messages when they are invoked.

## Firewall Statistics

### Firewall Log

This area shows whether or not the router is configured to maintain a log of connection attempts allowed and denied by the firewall.

### Number of Attempts Denied by Firewall

This area shows the number of connection attempts rejected by the firewall.

### Attempts Denied by Firewall Table

The table in this area shows a list of connection attempts denied by the firewall. This table includes the following columns:

- **Time:** Shows the time that each denied connection attempt occurred.
- **Number of Attempts:** Shows the total number of connection attempts denied that have the same origination and destination and were blocked by the same ACL
- **Attempt From:** Shows the interface name or IP address from which each denied connection attempt originated
- **ACL Name:** Shows the ACL number or name that caused each connection attempt to be denied
- **Attempt To:** Shows the interface name or IP address of the destination of each denied connection attempt

### **Disable Button**

Disables the filter that is currently active on the Attempts Denied by Firewall table. Clicking this button will make all firewall log entries visible in that table.

### **Configured Filter Status**

Displays the parameters of the filter currently in use on the Attempts Denied by Firewall table. Only entries in the firewall log that match the protocol, source address, destination address, and ACL displayed in this field are shown in the table.

### **Update Button**

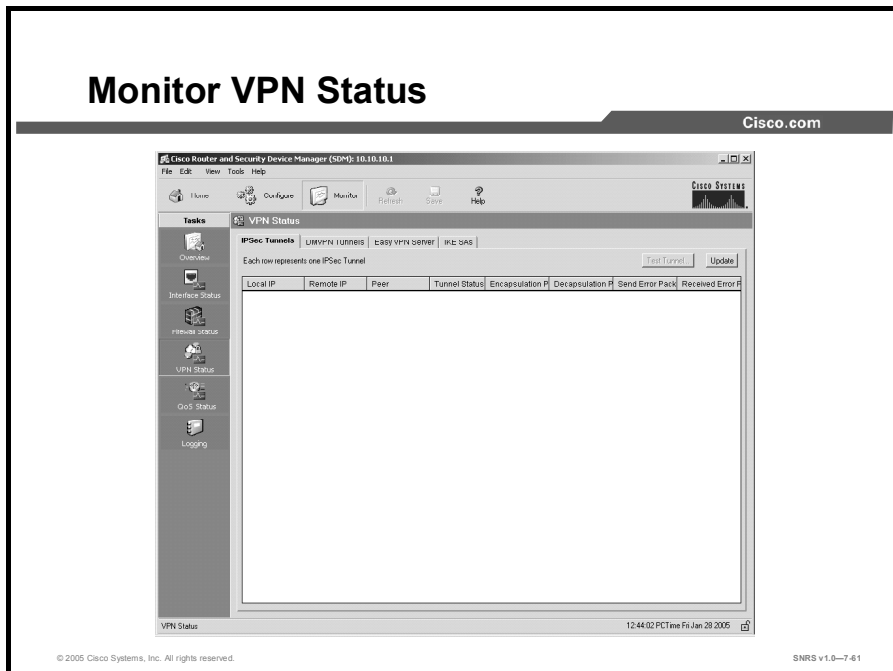
Click this button to poll the router and update the information shown on the screen with current information.

## **Monitoring Firewall with a Non-Administrator View User Account**

Firewall monitoring requires that logging buffered be enabled on the router. If logging buffered is not enabled, log in to Cisco SDM using an administrator view account or using a non-view-based privilege level 15 user account and configure logging.

To configure logging in Cisco SDM, choose **Additional Tasks > Router Properties > Logging**.

## Monitor VPN Status



This window displays statistics about the VPN connections that are active on the router.

Click a tab to view the type of VPN for which you want to see statistics.

- IPSec Tunnels
- DMVPN Tunnels
- Easy VPN Server
- IKE SAs

### Test Tunnel Button

Click to test a selected VPN tunnel. The results of the test will be shown in another window.

### IPSec Tunnels Tab

This group displays statistics about each IPSec VPN that is configured on the router. Each row in the table represents one IPSec VPN. The columns in the table and the information they display are as follows:

- **Interface:** The WAN interface on the router on which the IPSec tunnel is active
- **Local IP:** The IP address of the local IPSec interface
- **Remote IP:** The IP address of the remote IPSec interface
- **Peer:** The IP address of the remote peer
- **Peer Description:** The name of the remote router acting as the IPSec peer
- **Tunnel Status:** The current status of the IPSec tunnel. Possible values are:
  - Up—The tunnel is active.
  - Down—The tunnel is inactive due to an error or hardware failure.

## Update Button

Click this button to refresh the IPSec Tunnel table and display the most current data from the router.

## Clear Button

Select a row in the table and click **Clear** to clear the IPSec tunnel connection.

## DMVPN Tunnels Tab

This group displays the following statistics about Dynamic Multipoint VPN (DMVPN) tunnels. Each row reflects one VPN tunnel.

- **Remote Subnet:** The network address of the subnet to which the tunnel connects.
- **Remote Tunnel Address:** The IP address of the remote tunnel. This is the private IP address given to the tunnel by the remote device.
- **IP Address of the Public Interface of the Remote Router:** The IP address of the public (outside) interface of the remote router.
- **NHRP Cache Expiration:** The time and date when the tunnel registration expires and the VPN tunnel will be shut down.
- **Encapsulation Packets:** The number of packets encapsulated over the IPSec VPN connection.
- **Decapsulation Packets:** The number of packets decapsulated over the IPSec VPN connection.
- **Send Error Packets:** The number of errors that have occurred while sending packets.
- **Receive Error Packets:** The number of errors that have occurred while receiving packets.
- **Encrypted Packets:** The number of packets encrypted over the connection.
- **Decrypted Packets:** The number of packets decrypted over the connection.

## Reset Tunnel Button

This button resets statistics counters for the tunnel listed, setting the number of packets encapsulated and decapsulated, number of send and receive errors, and number of packets encrypted and decrypted to zero.

## Easy VPN Server Tab

This group displays the following information about each Cisco Easy VPN Server group:

- Total number of server clients (in upper right corner)
- Group name
- Number of client connections

### Group Details Button

Clicking **Group Details** shows the following information about the selected group:

- Group name
- Key
- Pool name
- DNS servers
- Windows Internet Name Service (WINS) servers
- Domain name
- ACL
- Backup servers
- Firewall are you there (AYT)
- Include local LAN
- Group lock
- Save password
- Maximum connections allowed for this group
- Maximum logins allowed for this user

### Client Connections in This Group

This area shows the following information about the selected group:

- Public IP address
- Assigned IP address
- Encrypted packets
- Decrypted packets
- Dropped outbound packets
- Dropped inbound packets
- Status

## IKE SAs Tab

This group displays the following statistics about each active IKE security association (SA) configured on the router:

- **Source IP:** The IP address of the peer originating the IKE SA.
- **Destination IP:** The IP address of the remote IKE peer.
- **State:** Describes the current state of IKE negotiations. The following states are possible:
  - **MM\_NO\_STATE:** The Internet Security Association and Key Management Protocol (ISAKMP) SA has been created, but nothing else has happened yet.
  - **MM\_SA\_SETUP:** The peers have agreed on parameters for the ISAKMP SA.
  - **MM\_KEY\_EXCH:** The peers have exchanged Diffie-Hellman (DH) public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
  - **MM\_KEY\_AUTH:** The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM\_IDLE and a quick mode exchange begins.
  - **AG\_NO\_STATE:** The ISAKMP SA has been created but nothing else has happened yet.
  - **AG\_INIT\_EXCH:** The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
  - **AG\_AUTH:** The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM\_IDLE and a quick mode exchange begins.
  - **QM\_IDLE:** The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges.

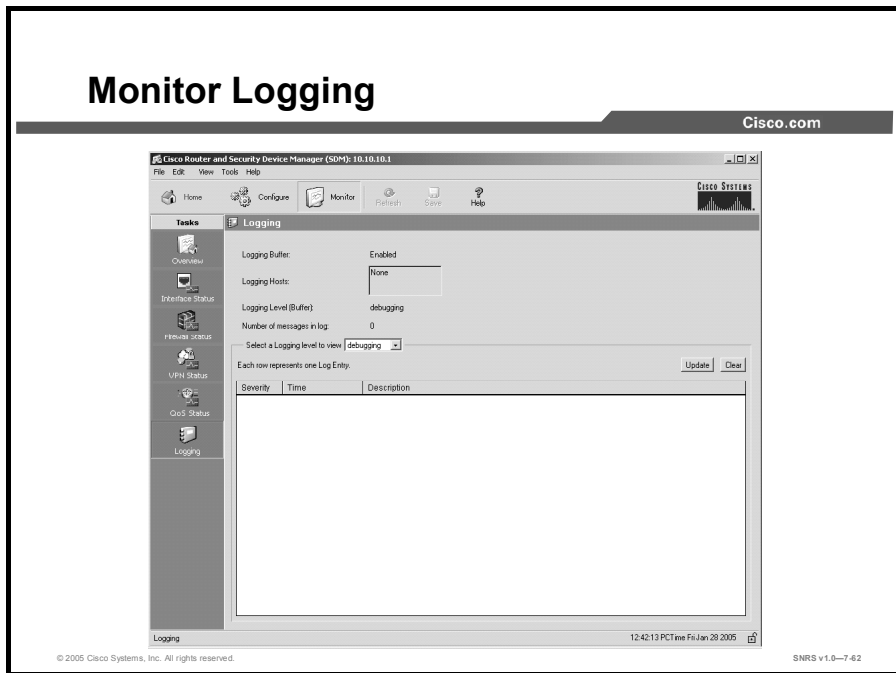
### Update Button

Click this button to refresh the IKE SA table and display the most current data from the router.

### Clear Button

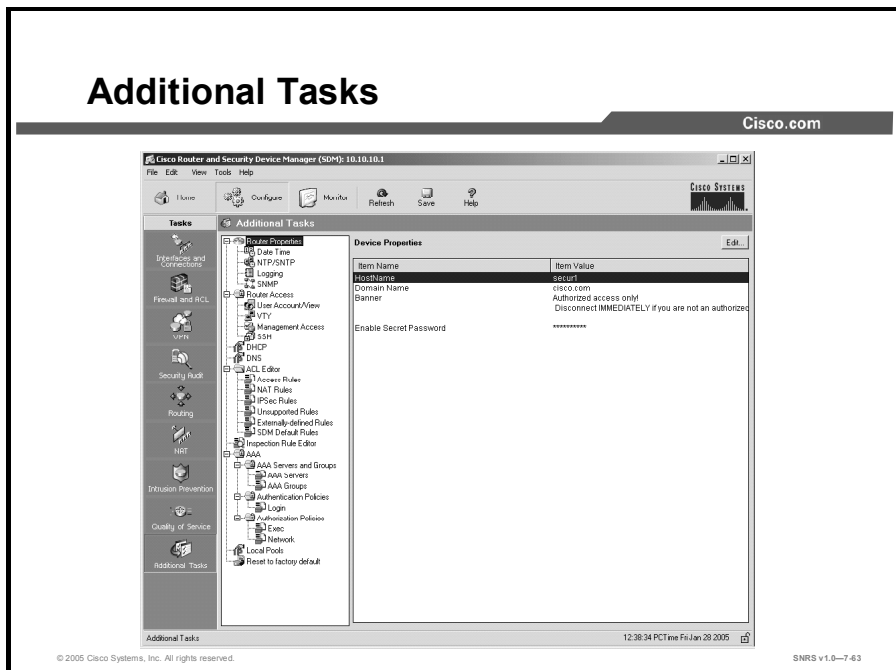
Select a row in the table and click **Clear** to clear the IKE SA connection.

## Monitor Logging



This window is used to view logs from the router.

## Additional Tasks



Some of the tools that appeared in the advanced mode view of Cisco SDM Version 1.1 now are called “additional tasks.” The additional tasks are shown in this figure.



# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Cisco SDM is a useful tool for configuring Cisco access routers.**
- **Cisco SDM contains several easy-to-use wizards for efficient configuration of Cisco access routers.**
- **Cisco SDM allows you to customize Cisco access router configurations using advanced features.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-7-64

# Module Summary

This topic summarizes the key points discussed in this module.

## Module Summary

Cisco.com

- **Cisco SDM allows you to customize Cisco access router configurations using advanced features and wizards.**

© 2005 Cisco Systems, Inc. All rights reserved. SNRS v1.0-7.1

This module covered Cisco SDM. An overview of its features and functions was followed by a more detailed exploration of some of its advanced wizards and features. You were guided through the process of configuring a WAN interface, firewall features, a VPN configuration, and a router security audit. The module ended with an introduction to the monitor view of the Cisco SDM interface.

**SNRS**

---

# Securing Networks with Cisco Routers and Switches

---

Version 1.0

**Lab Guide**

CLS Production Services: 06.28.05

**Copyright © 2005, Cisco Systems, Inc. All rights reserved.**

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

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

# Lab Guide

---

## Overview

This guide presents the instructions and other information concerning the activities for this course.

## Outline

This guide includes these activities:

- Lab 1-1: Configuring Cisco Secure ACS for Windows Server
- Lab 2-1: Configuring Cisco IOS Firewall CBAC on a Cisco Router
- Lab 2-2: Configuring Cisco IOS Firewall Authentication Proxy on a Cisco Router
- Lab 2-3: Configuring a Cisco Router with Cisco IOS Firewall IPS
- Lab 3-1: Mitigating Layer 2 Attacks
- Lab 3-2: Configuring EAP on Cisco Secure ACS for Windows Server
- Lab 3-3: Configuring 802.1x Port-Based Authentication
- Lab 4-1: Preparing the Network for IPSec Configuration with Pre-Shared Keys
- Lab 4-2: Configuring ISAKMP Using Pre-Shared Keys
- Lab 4-3: Configuring IPSec Using Pre-Shared Keys
- Lab 4-4: Testing and Verifying an IPSec Pre-Shared Key Configuration
- Lab 5-1: Preparing the Network for IPSec Configuration Using Digital Certificates
- Lab 5-2: Configuring Certificate Authority on Cisco Routers
- Lab 5-3: Configuring ISAKMP and IPSec on Cisco Routers
- Lab 5-4: Testing and Verifying the IPSec CA Configuration
- Lab 6-1: Configuring Remote Access Using Cisco Easy VPN
- Lab 6-2: Configuring Cisco Easy VPN Remote for the Cisco VPN Client 4.x
- Lab 6-3: Configuring a Cisco Access Router with Cisco Easy VPN
- Lab 7-1: Configuring a Perimeter Router with Cisco SDM

# Lab 1-1: Configuring Cisco Secure ACS for Windows Server

Complete this lab activity to practice what you learned in the related module.

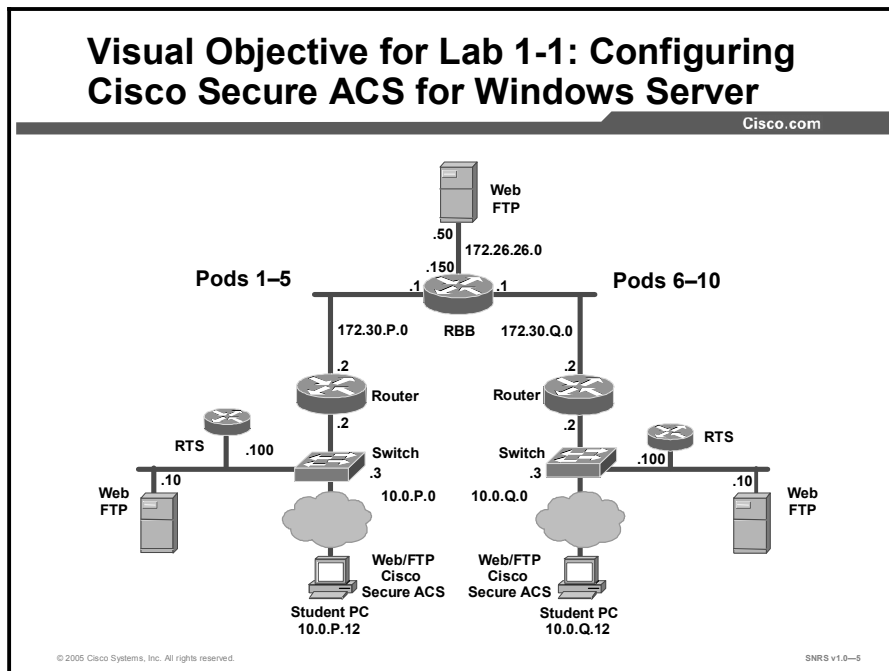
## Activity Objective

In this activity, you will configure a Cisco Secure ACS for Windows Server to provide AAA services. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- Install 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 figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### PC Commands

| Command                  | Description                  |
|--------------------------|------------------------------|
| <code>iconic /all</code> | Displays PC IP configuration |

### Router Commands

| Command                                                                                                                                                                                      | Description                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>aaa accounting {auth-proxy   system   network   exec   connection   commands level} {default   list-name} [vrf vrf-name] {start-stop   stop-only   none} [broadcast] group name</code> | To enable AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the <b>aaa accounting</b> command in global configuration mode. To disable AAA accounting, use the <b>no</b> form of this command.                 |
| <code>aaa authentication enable default method1 [method2...]</code>                                                                                                                          | To enable AAA authentication to determine whether a user can access the privileged command level, use the <b>aaa authentication enable default</b> command in global configuration mode. To disable this authorization method, use the <b>no</b> form of this command. |
| <code>aaa authentication login {default   list-name} method1 [method2...]</code>                                                                                                             | To set AAA authentication at login, use the <b>aaa authentication login</b> command in global configuration mode. To disable AAA authentication, use the <b>no</b> form of this command.                                                                               |
| <code>aaa new-model</code>                                                                                                                                                                   | To enable the AAA access control model, issue the <b>aaa new-model</b> command in global configuration mode. To disable the AAA access control model, use the <b>no</b> form of this command.                                                                          |
| <code>configure terminal</code>                                                                                                                                                              | To enter global configuration mode, use the <b>configure terminal</b> command in privileged EXEC mode.                                                                                                                                                                 |
| <code>copy run start</code>                                                                                                                                                                  | To copy any file from a source to a destination, use the <b>copy</b> command in EXEC mode.                                                                                                                                                                             |
| <code>line [aux   console   tty   vty] line-number [ending-line-number]</code>                                                                                                               | To identify a specific line for configuration and enter line configuration collection mode, use the <b>line</b> command in global configuration mode.                                                                                                                  |
| <code>logging console</code>                                                                                                                                                                 | To send syslog messages to all available TTY lines and limit messages based on severity, use the <b>logging console</b> command in global configuration mode. To disable logging to the console terminal, use the <b>no</b> form of this command.                      |
| <code>login [local   tacacs]</code>                                                                                                                                                          | To enable password checking at login, use the <b>login</b> command in line configuration mode. To disable password checking and allow connections without a password, use the <b>no</b> form of this command.                                                          |
| <code>login authentication {default   list-name}</code>                                                                                                                                      | To enable AAA authentication for logins, use the <b>login authentication</b> command in line configuration mode. To return to the default specified by the <b>aaa authentication login</b> command, use the <b>no</b> form of this command.                            |
| <code>password</code>                                                                                                                                                                        | To specify a password on a line, use the <b>password</b> command in line configuration mode. To remove the                                                                                                                                                             |

| Command                                                                                                                                                                              | Description                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                      | password, use the <b>no</b> form of this command.                                                                                                                                                                                                                 |
| <b>tacacs-server host</b> <i>host-name</i> [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ] [ <b>single-connection</b> ] [ <b>Nat</b> ] | To specify a TACACS+ host, use the <b>tacacs-server host</b> command in global configuration mode. To delete the specified name or address, use the <b>no</b> form of this command.                                                                               |
| <b>tacacs-server key</b>                                                                                                                                                             | To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the <b>tacacs-server key</b> command in global configuration mode. To disable the key, use the <b>no</b> form of this command. |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will set up your PC.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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** 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** Disable logging to the router console using the **no logging console** command.
- Step 4** Enter **iconic /all** command to display the IP information of the PC.

### Activity Verification

You have completed this task when you attain these results:

- Your display shows the proper IP address.

Q1) What is your MAC address?

---



## Task 2: Install Cisco Secure ACS for Windows Server

You will 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.

### Activity Procedure

Complete these steps:

- 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 substeps within the Authentication Database Configuration window:
  - 1. Check the **Also Check the Windows User Database** check box.
  - 2. Check the **Yes, Refer to “Grant Dialing Permission to User” Setting** check box.
  - 3. Click **Next**.
- Step 10** Check all check boxes within the Advanced Options window and click **Next**. It is important that you check all check boxes because this step determines which Cisco Secure ACS options you will be able to configure later.
- Step 11** Accept the default settings within the Active Service Monitoring window by clicking **Next**.
- Step 12** Accept the default settings within the Cisco Secure ACS Service Initiation window by clicking **Next**.  
  
Setup then starts the Cisco Secure ACS service.
- Step 13** Click **Finish**.

A web browser will start and display the Cisco Secure ACS 3.3 home page.

- Q2) What is the release and build number?

- Step 14** Click the **Interface Configuration** tab.
- Step 15** Check the following check boxes:
- **Network Device Groups**
  - **Group-Level Password Aging**
- Step 16** Click the **Network Configuration** tab.
- Step 17** Click **(Not Assigned)** in the Network Device Groups window.
- Step 18** Click **Add Entry** in the AAA Clients section. Complete the following substeps within the Cisco Secure ACS AAA Client Setup window:
1. Choose **TACACS+ (Cisco IOS)** from the Authenticate Users Using pane.
- Q3) What other options are available?
- 
2. Enter the name of your router in the AAA Client Hostname field (for example, R1, R2, and so on).
  3. Enter the IP address of your router inside interface **(10.0.P.2)** in the AAA Client IP Address field (where P = pod number).
- Step 19** Enter **ciscosecure** (one word, all lowercase) in the TACACS+ or RADIUS Key field.
- Step 20** Finish adding your router as the AAA client by clicking **Submit**.
- Step 21** Click the **Network Configuration** tab.
- Step 22** Click **Add Entry** in the AAA Servers section. Complete the following substeps within the Cisco Secure ACS AAA Client Setup window:
1. Enter the name of your PC, **studentX**, in the AAA Server Name field (where P = pod number).
  2. Enter the IP Address of your PC **(10.0.P.12)** in the AAA Server IP Address field (where P = pod number).
  3. Enter **ciscosecure** (one word, all lowercase) in the Key field.
  4. Choose the proper AAA server type.
  5. Choose the **inbound/outbound** traffic type.
- Step 23** Finish adding your router as the AAA client and your PC as the AAA server by clicking **Submit + Restart**.
- Step 24** Close the Internet Explorer window containing the Cisco Secure ACS main window.
- Step 25** Close any open windows.

## Activity Verification

You have completed this task when you attain these results:

Use the Windows Task Manager (press **Ctrl-Alt-Delete** > **Task Manager**) to verify that the following services are running on your student PC:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRADIUS
- CSTacacs

## Task 3: Configure the Cisco Secure ACS for Windows Server Database for Authentication

You will create a group and user for AAA authentication.

### Activity Procedure

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 substeps:
1. Click the **Group Setup** button at the left.
  2. Choose **Group 1** from the drop-down menu.
  3. Rename the group **is-in** by clicking the **Rename Group** button, highlighting the existing name, entering the new group name, and clicking the **Submit** button.
  4. Choose **Edit Settings** and set the group settings as follows:
    - In the Password Aging Rules section, check 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, choose **No IP address assignment**.
    - In the TACACS+ Settings section, choose **Shell (exec)**.
    - In the Enable Options section, choose **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**.

**Step 2** Add and configure a user to authenticate against the Cisco Secure ACS database by completing the following substeps:

1. Click the **User Setup** button at the left.
2. Enter a username of **isadmin**.
3. Click **Add/Edit** and make sure that Account Disabled is deselected.
4. Scroll to the User Setup area and choose **CiscoSecure Database** for password authentication.

Q4) What other options are available?

- 
5. Enter a password of **isuser** for the user isadmin. Ensure that you enter the password a second time 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. Choose **Disable account if...** and check the **Failed Attempts Exceed: 5** check box.
  8. Scroll to the Advanced TACACS+ Settings section and choose **Use Group Level Setting**. Remember that the group setting is level 15.
  9. Scroll to the TACACS+ Enable Password section and check the **Use Separate Password** check box.
  10. Enter a password of **ispassword**. Remember to enter it a second time to confirm it.
  11. Click **Submit** to enable the settings.
  12. Click **List All Users** in the User Setup Select area and verify that the user you just added is present and correctly configured.

### Activity Verification

You have completed this task when you attain these results:

- Check user settings.

## Task 4: Configure the Router to Authenticate to the Cisco Secure ACS for Windows Server Database

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.

### Activity Procedure

Complete the following steps:

**Step 1** Log in to the router using the AAA administrator account user name of **admin** with a password of **admindoor**.

**Step 2** Enter configuration terminal mode:

```
router# config t
```

**Step 3** Enter the location of the Cisco Secure ACS IP address and encryption key for TACACS+, as shown (where P = pod number):

```
router(config)# tacacs-server host 10.0.P.12
router(config)# tacacs-server key ciscosecure
```

**Step 4** Enable AAA:

```
router(config)# aaa new-model
```

Q5) What is the command used to enable AAA?

---

**Step 5** Enable AAA accounting for Cisco Secure ACS for Windows Server:

```
router(config)# aaa accounting connection default start-stop group tacacs+
```

**Step 6** Complete the following substeps on the router to consolidate the VTY and console:

1. Enter the following commands exactly as shown:

```
router(config)# no aaa authentication login console-in local
router(config)# no aaa authentication login is-in local
router(config)# aaa authentication login is-in group tacacs+ local
router(config)# line con 0
router(config-line)# login authentication is-in
router(config-line)# exit
```

Q6) What is the name of the TACACS+ group that will be used for authentication?

---

2. Enter the following command to protect the enable password and privileged mode:

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

This command forces the use of the enable restrictions that you placed in the Cisco Secure ACS for Windows Server, and it overrides the enable secret password on the router.

- Q7) What is the default authentication method for this router?
- 

- Step 7** If 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. Change this to use TACACS+. Enter the following commands exactly as shown:

```
router(config)# no aaa authentication login default enable
router(config)# aaa authentication login default group tacacs+ enable
```

- Note** You should always place an **enable** command 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, it defaults to the standard enable password.
- 

- Q8) Where does the router authenticate if the AAA server is not reachable?
- 

## Activity Verification

Perform the following steps to verify authentication configuration is correct:

- Step 1** Open a new command prompt shell and establish a Telnet session to the inside interface of your router: **10.0.P.2** (where P = pod number).
- Step 2** Log in using the **isadmin** username and the **isuser** password. Your router should authenticate with the Cisco Secure ACS and allow you to log in. If you cannot log in, recheck your work and try again.
- Step 3** Enter privileged EXEC mode using the **ispassword** password. Your router should authenticate with the Cisco Secure ACS and allow you to log in. If you cannot log in, recheck your work and try again.
- Step 4** Copy the running configuration to the startup configuration using the **copy run start** command:

```
router(config)# end
router# copy run start
```
- Step 5** Log out of the Telnet session and close the command prompt window.
- Step 6** Log out of Cisco Secure ACS and minimize the window.
- Step 7** Return the router to the default lab configuration in preparation for the next lab.

## Lab 1-1 Answer Key: Configuring Cisco Secure ACS for Windows Server

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What is your MAC address?

---

Q2) What is the release and build number?

---

Q3) What other options are available?

---

Q4) What other options are available?

---

Q5) What is the command to enable AAA?

---

Q6) What is the name of the TACACS+ group that will be used for authentication?

---

Q7) What is the default authentication method for this router?

---

Q8) Where does the router authenticate if the AAA server is not reachable?

---

# Lab 2-1: Configuring Cisco IOS Firewall CBAC on a Cisco Router

Complete this lab activity to practice what you learned in the related module.

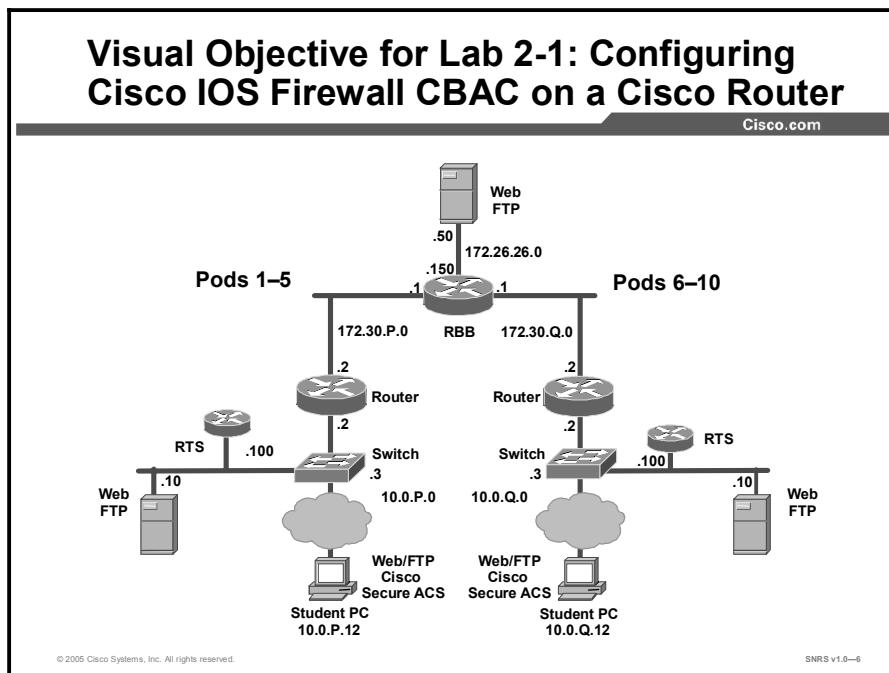
## Activity Objective

In this activity, you will configure Cisco IOS Firewall CBAC on a Cisco router. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- Configure logging and auditing trails
- Define inspection rules and ACLs
- Apply inspection rules and ACLs
- Test and verify CBAC

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.



## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny   permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log   log-input] [time-range time-range-name] [fragments]</code> | To define an extended IP ACL, use the extended version of the <b>access-list</b> command in global configuration mode. To remove the ACLs, use the <b>no</b> form of this command.                                                                                                                                                                      |
| <code>ip access-group {access-list-number   access-list-name}{in   out}</code>                                                                                                                                                                                     | To control access to an interface, use the <b>ip access-group</b> command in interface configuration mode. To remove the specified access group, use the <b>no</b> form of this command.                                                                                                                                                                |
| <code>ip inspect inspection-name {in   out}</code>                                                                                                                                                                                                                 | To apply a set of inspection rules to an interface, use the <b>ip inspect</b> command in interface configuration mode. To remove the set of rules from the interface, use the <b>no</b> form of this command.                                                                                                                                           |
| <code>ip inspect audit trail</code>                                                                                                                                                                                                                                | To turn on CBAC audit trail messages, which will be displayed on the console after each CBAC session closes, use the <b>ip inspect audit trail</b> command in global configuration mode. To turn off CBAC audit trail message, use the <b>no</b> form of this command.                                                                                  |
| <code>ip inspect name inspection-name protocol [alert {on   off}] [audit-trail {on   off}] [timeout seconds]</code>                                                                                                                                                | To define a set of inspection rules, use the <b>ip inspects name</b> command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the <b>no</b> form of this command.                                                                                                        |
| <code>line [aux   console   tty   vty] line-number [ending-line-number]</code>                                                                                                                                                                                     | To identify a specific line for configuration and enter line configuration collection mode, use the <b>line</b> command in global configuration mode.                                                                                                                                                                                                   |
| <code>logging console</code>                                                                                                                                                                                                                                       | To send syslog messages to all available TTY lines and limit messages based on severity, use the <b>logging console</b> command in global configuration mode. To disable logging to the console terminal, use the <b>no</b> form of this command.                                                                                                       |
| <code>logging console [severity-level]</code>                                                                                                                                                                                                                      | To enable logging of system messages, use the <b>logging on</b> command in global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the <b>no</b> form of this command. |
| <code>ping [protocol] [tag] {host-name   system-address}</code>                                                                                                                                                                                                    | To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the <b>ping</b> command in EXEC mode.                                                                                                                                             |
| <code>show access-lists [access-list-number   access-list-name]</code>                                                                                                                                                                                             | To display the contents of current ACLs, use the <b>show access-lists</b> command in privileged EXEC mode.                                                                                                                                                                                                                                              |
| <code>show ip inspect {name inspection-name   config  </code>                                                                                                                                                                                                      | To display CBAC configuration and session information, use                                                                                                                                                                                                                                                                                              |

| Command                                               | Description                                                       |
|-------------------------------------------------------|-------------------------------------------------------------------|
| <code>interfaces   session<br/>[detail]   all}</code> | the <code>show ip inspect</code> command in privileged EXEC mode. |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will complete the lab exercise setup.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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** 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, the Kiwi Syslog Daemon).
- Step 4** Reload your perimeter router using the default lab configuration.
- Step 5** Ensure that 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.

### Activity Verification

You have completed this task when you attain these results:

- You can ping the router and have checked that the date and time are correct.

## Task 2: Configure Logging and Audit Trails

You will configure logging and auditing trails.

### Activity Procedure

Complete these steps:

**Step 1** Log in to your perimeter router and access global configuration mode.

**Step 2** On your router, enable logging to the console and the syslog server:

```
router(config)# logging on
router(config)# logging 10.0.P.12
(where P = pod number)
```

**Step 3** Enable the audit trail:

```
router(config)# ip inspect audit-trail
```

**Step 4** Save your configuration and return to global configuration mode:

```
router(config)# end
router# copy run start
```

### Activity Verification

You have completed this task when you attain these results:

■ Issue a **sh ip inspect config** command. The output should be similar to this:

```
R2#sh ip inspect config
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
```

Q1) What is the status of the session audit trail?

---

## Task 3: Define Inspection Rules and ACLs

You will define inspection rules and ACLs.

### Activity Procedure

Complete these steps:

**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:

```
router(config)# ip inspect name FWRULE tcp timeout 300
router(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.

```
router(config)# access-list 103 permit icmp any any
router(config)# access-list 103 permit tcp 10.0.P.0 0.0.0.255
any eq ftp
router(config)# access-list 103 permit tcp 10.0.P.0 0.0.0.255
any eq www
router(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.

```
router(config)# access-list 104 permit eigrp any any
router(config)# access-list 104 permit icmp any any
router(config)# access-list 104 deny ip any any
```

Q2) What does the last statement in this ACL mean?

---

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh access-list** command. The output should be similar to this:

```
R2#sh access-lists
Extended IP access list 103
 10 permit icmp any any
 20 permit tcp 10.0.2.0 0.0.0.255 any eq ft
 30 permit tcp 10.0.2.0 0.0.0.255 any eq www
 40 deny ip any any
Extended IP access list 104
 10 permit eigrp any any
 20 permit icmp any any
 30 deny ip any any
```

## Task 4: Apply Inspection Rules and ACLs

This task describes how to apply inspection rules and ACLs.

### Activity Procedure

Complete these steps:

**Step 1** Apply the inspection rule and ACL to the inside interface:

```
router(config)# interface fast 0/0
router(config-if)# ip inspect FWRULE in
router(config-if)# ip access-group 103 in
```

**Step 2** Apply the ACL to the outside interface:

```
router(config-if)# interface fast 0/1
router(config-if)# ip access-group 104 in
```

**Step 3** Save your configuration and return to global configuration mode:

```
router(config-if)# end
router# copy run start
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show ip inspect interfaces** command. The output should be similar to this:

```
R2#sh ip inspect interfaces
Interface Configuration
Interface FastEthernet0/0
 Inbound inspection rule is FWRULE
 tcp alert is on audit-trail is on timeout 300
 ftp alert is on audit-trail is on timeout 300
 Outgoing inspection rule is not set
 Inbound access list is 103
 Outgoing access list is not set
```

Q3) What is the direction of the inspection rule?

---

## Task 5: Test and Verify CBAC

This task describes how to test and verify CBAC.

### Activity Procedure

Complete these steps:

**Step 1** Check your ACLs:

```
router# show access-lists
```

**Step 2** Ping the backbone server from the command prompt of your student PC:

```
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** commands to verify the CBAC operation:

```
router# show ip inspect name FWRULE
router# show ip inspect config
router# show ip inspect interfaces
router# show ip inspect sessions
router# show ip inspect sessions detail
router# show ip inspect all
```

**Step 7** Ping the inside server of your peer from your PC 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 8** Use your web browser to connect to your peer inside server. Enter **http://10.0.Q.12** in the URL field.

(where Q = peer pod number)

**Step 9** Connect to the peer 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)
```

## Activity Verification

You have completed this task when you attain these results:

- On your router, use the following **show** commands to verify the CBAC operation:

```
router# show ip inspect name FWRULE
router# show ip inspect config
router# show ip inspect interfaces
router# show ip inspect sessions
router# show ip inspect sessions detail
router# show ip inspect all
```

## Lab 2-1 Answer Key: Configuring Cisco IOS Firewall CBAC on a Cisco Router

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What is the status of the session audit trail?

---

Q2) What does the last statement in this ACL mean?

---

Q3) What is the direction of the inspection rule?

---



# Lab 2-2: Configuring Cisco IOS Firewall Authentication Proxy on a Cisco Router

Complete this lab activity to practice what you learned in the related module.

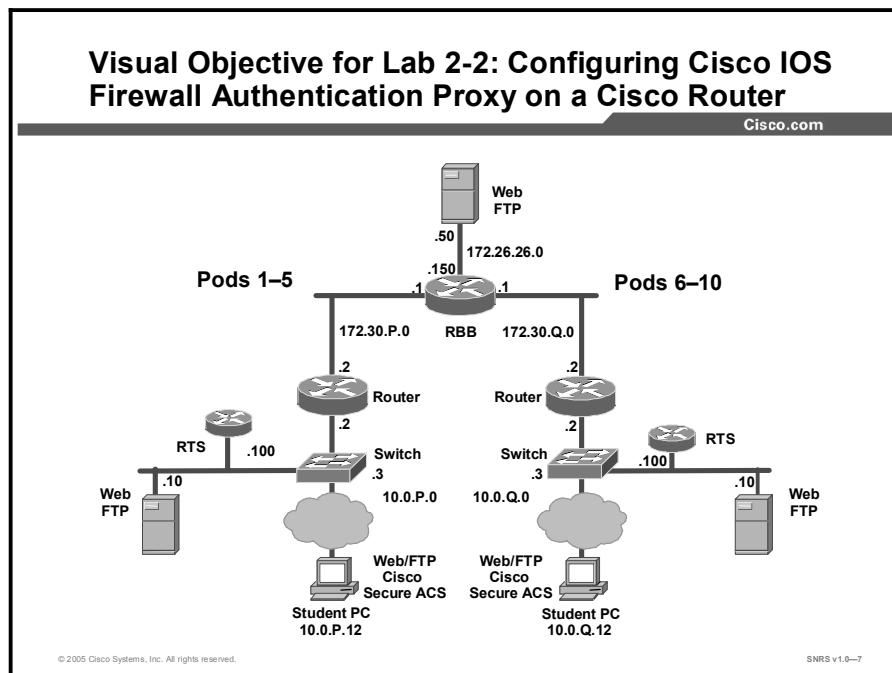
## Activity Objective

In this activity, you will configure authentication proxy on a Cisco Router. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- Configure Cisco Secure ACS
- Configure AAA
- Configure an authentication proxy
- Test and verify the configuration

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>aaa authentication enable default method1 [method2...]</code>                                                                                                                                                                                                | To enable AAA authentication to determine whether a user can access the privileged command level, use the <b>aaa authentication enable default</b> command in global configuration mode. To disable this authorization method, use the <b>no</b> form of this command.                                                                |
| <code>aaa authentication login {default   list-name} method1 [method2...]</code>                                                                                                                                                                                   | To set AAA authentication at login, use the <b>aaa authentication login</b> command in global configuration mode. To disable AAA authentication, use the <b>no</b> form of this command.                                                                                                                                              |
| <code>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} method1 [method2...]</code>                                                                                                                       | To set parameters that restrict user access to a network, use the <b>aaa authorization</b> command in global configuration mode. To disable authorization for a function, use the <b>no</b> form of this command.                                                                                                                     |
| <code>aaa new-model</code>                                                                                                                                                                                                                                         | To enable the AAA access control model, issue the <b>aaa new-model</b> command in global configuration mode. To disable the AAA access control model, use the <b>no</b> form of this command.                                                                                                                                         |
| <code>access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny   permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log   log-input] [time-range time-range-name] [fragments]</code> | To define an extended IP ACL, use the extended version of the <b>access-list</b> command in global configuration mode. To remove the ACLs, use the <b>no</b> form of this command.                                                                                                                                                    |
| <code>ip access-group {access-list-number   access-list-name}{in   out}</code>                                                                                                                                                                                     | To control access to an interface, use the <b>ip access-group</b> command in interface configuration mode. To remove the specified access group, use the <b>no</b> form of this command.                                                                                                                                              |
| <code>ip auth-proxy {inactivity-timer min   absolute-timer min}</code>                                                                                                                                                                                             | To set the authentication proxy idle timeout value (the length of time that an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity), use the <b>ip auth-proxy</b> command in global configuration mode. To set the default value, use the <b>no</b> form of this command. |
| <code>ip auth-proxy auth-proxy-name</code>                                                                                                                                                                                                                         | To apply an authentication proxy rule at a firewall interface, use the <b>ip auth-proxy</b> command in interface configuration mode. To remove the authentication proxy rules, use the <b>no</b> form of this command.                                                                                                                |
| <code>ip http authentication {aaa   enable   local   tacacs}</code>                                                                                                                                                                                                | To specify a particular authentication method for HTTP server users, use the <b>ip http authentication</b> command in global configuration mode. To disable a configured authentication method, use the <b>no</b> form of this command.                                                                                               |
| <code>ip http server</code>                                                                                                                                                                                                                                        | To enable the HTTP server on your system, including the Cisco web browser user interface, use the <b>ip http server</b> command in global configuration mode. To disable the                                                                                                                                                          |

| Command                                                                                                           | Description                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                   | HTTP server, use the <b>no</b> form of this command.                                                                                                                                                                                                              |
| <code>ping [protocol] [tag] {host-name   system-address}</code>                                                   | To diagnose basic network connectivity on AppleTalk, ATM, CLNS, DECnet, IP, Novell IPX, or SRB networks, use the <b>ping</b> command in EXEC mode.                                                                                                                |
| <code>show access-lists [access-list-number   access-list-name]</code>                                            | To display the contents of current ACLs, use the <b>show access-lists</b> command in privileged EXEC mode.                                                                                                                                                        |
| <code>show ip auth-proxy {cache   configuration}</code>                                                           | To display the authentication proxy entries or the running authentication proxy configuration, use the <b>show ip auth-proxy</b> command in privileged EXEC mode.                                                                                                 |
| <code>tacacs-server host host-name [port integer] [timeout integer] [key string] [single-connection] [nat]</code> | To specify a TACACS+ host, use the <b>tacacs-server host</b> command in global configuration mode. To delete the specified name or address, use the <b>no</b> form of this command.                                                                               |
| <code>tacacs-server key key</code>                                                                                | To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the <b>tacacs-server key</b> command in global configuration mode. To disable the key, use the <b>no</b> form of this command. |
| <code>username name {nopassword   password password   password encryption-type encrypted-password}</code>         | To establish a username-based authentication system, use the <b>username</b> command in global configuration mode.                                                                                                                                                |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will complete the lab exercise setup.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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** 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 that you can ping the other routers and network hosts before beginning.

### Activity Verification

You have completed this task when you attain these results:

- You can successfully ping the other hosts.

## Task 2: Configure Cisco Secure ACS

Configure the Cisco Secure ACS for Windows 2000 for authentication proxy.

### Activity Procedure

Complete these steps:

- Step 1** On your student PC, open Cisco Secure ACS from the desktop.
- Step 2** Click **Interface Configuration** on the left column of Cisco Secure ACS. The Interface Configuration window opens.

Q1) What are the options in this window?

---

- Step 3** Click **TACACS+ (Cisco IOS)** to configure this option.
- Step 4** Scroll down to locate the **New Services** area.
- Step 5** Choose the first field under New Services and enter **auth-proxy** in the Service field.
- Step 6** Check the **Service** field group check box. Make sure that you check the check box directly to the left of the Service field.
- Step 7** Scroll to the Advanced Configuration Options area and verify that the **Advanced TACACS+ features** option is selected.
- Step 8** Click the **Submit** button to submit your changes.
- Step 9** Click the **Group Setup** button. The Group Setup window opens.
- Step 10** Choose **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 area and locate the Auth-Proxy and Custom Attributes check boxes. Check both the **Auth-Proxy** check box and the **Custom Attributes** check box.
- Step 13** Enter the following in the Custom Attributes box (note that long lines of text, such as 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
```

Q2) What do these commands do?

---

- Step 14** Return to the User Setup and add a new username of **aauser** with a password of **aaapass** to Group 2.
- Step 15** 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.

## Activity Verification

You have completed this task when you attain these results:

- Review the settings that you just configured in Cisco Secure ACS.

## Task 3: Configure AAA

You will configure AAA on the router.

### Activity Procedure

Complete these steps:

- Step 1** On your router, enter global configuration mode:

```
Router# configure terminal
```

- Step 2** Create a user account in the local database:

```
Router(config)# username cisco password cisco
```

- Q3) Where is this user created?
- 

- Step 3** Enable AAA:

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

- Step 4** Define the TACACS+ server and its key:

```
router(config)# tacacs-server host 10.0.P.12
router(config)# tacacs-server key ciscosecure
(where P = pod number)
```

- Q4) What is the address of the Cisco Secure ACS server?
- 

- Step 5** Specify the authentication protocol for logins:

```
Router(config)# aaa authentication login default group tacacs+ local
```

- Q5) Why do you include the local method as the last statement?
- 

- Step 6** Specify the authorization protocol for authentication proxy:

```
Router(config)# aaa authorization auth-proxy default group tacacs+ local
```

- Step 7** Define a new ACL to allow TACACS+ traffic to the inside interface from your AAA server. Also allow outbound ICMP traffic and CBAC traffic (FTP and WWW). Block all other inside-initiated traffic.

```
router(config)# access-list 101 permit tcp host 10.0.P.12 eq tacacs host 10.0.P.2
```

```
router(config)# access-list 101 permit icmp any any
```

```
router(config)# access-list 101 deny ip any any
```

(where P = pod number)

- Q6) What is the function of this ACL?
- 

- Step 8** Apply the new ACL to the Fa0/0 interface of your perimeter router:

```
router(config)# interface Fa0/0
```

```
router(config-if)# ip access-group 101 in
```

```
router(config-if)# exit
```

- Step 9** Enable the router HTTP server for AAA:

```
router(config)# ip http server
```

```
router(config)# ip http authentication aaa
```

## Activity Verification

You have completed this task when you attain these results:

- Issue a **sh access-lists** and a **sh ip http server status** command. The output should be similar to this:

```
R2#sh access-lists
```

```
Extended IP access list 101
```

```
10 permit tcp host 10.0.2.12 eq tacacs host 10.0.2.2
```

```
20 permit tcp any any eq telnet
```

```
30 permit icmp any any
```

```
40 permit tcp any any eq www
```

```
50 permit tcp any any eq ftp
```

```
60 deny ip any any
```

Q7) Issue a **sh ip http server status** command, then list the results for the following:

HTTP server status:

\_\_\_\_\_

HTTP server authentication method:

\_\_\_\_\_

Maximum number of concurrent server connections allowed:

\_\_\_\_\_

Server idle timeout:

\_\_\_\_\_

Server life timeout:

## Task 4: Configure Authentication Proxy

You will configure an authentication proxy.

### Activity Procedure

Complete these steps:

**Step 1** Define an authentication proxy rule:

```
router(config)# ip auth-proxy name APRULE http inactivity-time
5
```

**Step 2** Apply the authentication proxy rule to the inside interface:

```
router(config)# interface fast 0/0
router(config-if)# ip auth-proxy APRULE
router(config-if)# end
```

### Activity Verification

You have completed this task when you attain these results:

■ Issue a **sh ip auth-proxy configuration** command. The output should be similar to this:

```
R2#sh ip auth-proxy configuration
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
Auth-proxy name APRULE
http list not specified inactivity-timer 5 minutes
```

## Task 5: Test and Verify the Configuration

You will test and verify an authentication proxy.

### Activity Procedure

Complete these steps:

- Step 1** On your router, use the **show access-list** command to check your ACLs. Fill in the blanks here using the output from this command:

```
router# show access-list
Extended IP access list 101
```

---

---

---

- Step 2** Use the **show ip auth-proxy** configuration command to verify the authentication proxy configuration. Fill in the blanks here using the output from this command:

```
router# show ip auth-proxy configuration
Authentication global cache time is _____ minutes
Authentication global absolute time is _____ minutes
Authentication Proxy Watch-list is _____
```

```
Authentication Proxy Rule Configuration
Auth-proxy name _____
http list not specified inactivity-timer _____ 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** Use your web browser to connect to the backbone web server. In the URL field, enter the following:

```
http://172.26.26.50
```

- Step 5** Enter the following when the web browser prompts you for a username and password:

```
Username: aauser
Password: aaapass
```





## Lab 2-2 Answer Key: Configuring Cisco IOS Firewall Authentication Proxy on a Cisco Router

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What are the options in this window?

---

---

---

---

---

Q2) What are the options in this window?

---

---

---

---

---

Q3) Where is this user created?

---

Q4) Where is this user created?

---

Q5) Why do we include the local method as the last statement?

---

Q6) What is the function of this ACL?

---

---

Q7) Issue a **sh ip http server status** command, then fill in the blanks for the following results:

HTTP server status:

---

HTTP server authentication method:

Maximum number of concurrent server connections allowed:

---

Server idle timeout:

---

Server life timeout:

---

# Lab 2-3: Configuring a Cisco Router with Cisco IOS Firewall IPS

Complete this lab activity to practice what you learned in the related module.

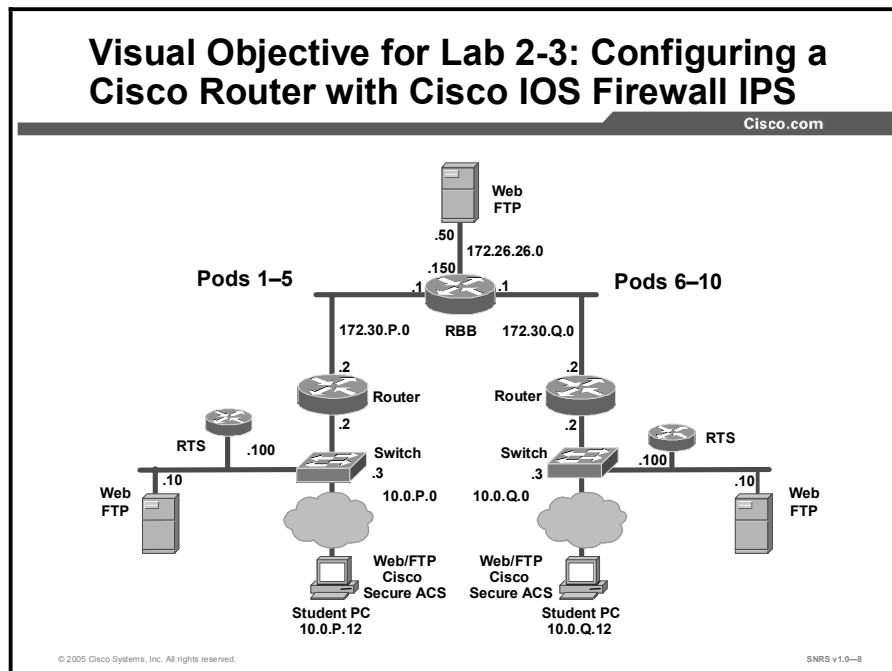
## Activity Objective

In this activity, you will configure a Cisco router with Cisco IOS Firewall IPS. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- Initialize IPS
- Load signatures
- Merge the attack-drop.sdf file with the default, built-in signatures
- Verify the configuration
- Generate a test message

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                      | Description                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip ips ips-name {in   out} [list acl]</code>                                                                                           | To apply an IPS rule to an interface, use the <b>ip ips</b> command in interface configuration mode. To remove an IPS rule from an interface direction, use the <b>no</b> form of this command. <ul style="list-style-type: none"><li>■ <b>list acl</b>—Packets that are permitted via a specified ACL will be scanned by IPS.</li></ul> |
| <code>ip ips fail closed</code>                                                                                                              | To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the <b>ip ips fail closed</b> command in global configuration mode. To return to the default functionality, use the <b>no</b> form of this command.                                                                        |
| <code>ip ips name ips-name</code>                                                                                                            | To specify an IPS rule, use the <b>ip ips name</b> command in global configuration mode. To delete an IPS rule, use the <b>no</b> form of this command.                                                                                                                                                                                  |
| <code>ip ips sdf location url</code>                                                                                                         | To specify the location in which the router will load the SDF, use the <b>ip ips sdf location</b> command in global configuration mode. To remove an SDF location from the configuration, use the <b>no</b> form of this command.                                                                                                        |
| <code>show ip ips { [all] [configuration] [interfaces] [name name] [statistics [reset]] [sessions [details]] [signatures [details]] }</code> | To display IPS information such as configured sessions and signatures, use the <b>show ip ips</b> command in privileged EXEC mode.                                                                                                                                                                                                       |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will complete the lab exercise setup.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log in to 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 Syslog Daemon).
- Step 4** Reload your perimeter router using the default lab configuration.
- Step 5** Ensure that you can ping the other routers and network hosts before beginning.

## Activity Verification

You have completed this task when you attain these results:

- You can ping the other hosts.

## Task 2: Initialize IPS

You will initialize IPS on the router. This task allows you to load the default, built-in signatures. If you want to merge the two signature files, you must load the default, built-in signatures as described in this task. Then, you can merge the default signatures with the attack-drop.sdf file.

### Activity Procedure

Complete these steps:

**Step 1** From your student PC, access the router console.

**Step 2** Switch to privileged EXEC mode:

```
router> enable
Password: cisco
```

**Step 3** Switch to global configuration mode:

```
router# conf t
router(config)#
```

**Step 4** (Optional) Specify the location in which the router will load the SDF named attack-drop.sdf.

```
Router(config)# ip ips sdf builtin
```

Q1) Issue a **sh ip ips configuration** command and record these results:

```
Configured SDF Locations:
```

```

Builtin signatures are _____
Last successful SDF load time: _____
IDS fail closed is _____
Fastpath ips is _____
Quick run mode is enabled
Event notification through syslog is _____
Event notification through Net Director is _____
Event notification through SDEE is _____
Total Active Signatures: ____
Total Inactive Signatures: ____
PostOffice:HostID:0 OrgID:0 Msg dropped:0
 :Curr Event Buf Size:0 Configured:100
Post Office is _____ - ____ connections are active
```

**Step 5** Create an IPS rule:

```
Router(config)# ip ips name SECURIPS
```

**Step 6** Configure an interface type and enter interface configuration mode:

```
Router(config)# interface Fa0/1
```

- Step 7** Apply an IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.
- ```
Router(config-if)# ip ips SECURIPS in
```
- Step 8** Exit to global configuration mode:
- ```
Router(config-if)# exit
```
- Step 9** Configure the logging host:
- ```
R2(config)#logging 10.0.2.12
```
- Step 10** Configure the trap level:
- ```
R2(config)#logging trap
```
- Step 11** Turn on logging:
- ```
R2(config)#logging on
```
- Step 12** Exit to privileged mode:
- ```
R2(config)#^Z
```
- Step 13** Display the configuration of the IPS:
- ```
Router# show ip ips configuration
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **show ips configuration** command and record the following results:

R2#sh ip ips configuration

```
Configured SDF Locations: _____
Builtin signatures are _____ and _____
Last successful SDF load time: _____
IDS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is _____
Event notification through Net Director is disabled
Event notification through SDEE is disabled
Total Active Signatures: _____
Total Inactive Signatures: 0
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
      :Curr Event Buf Size:0 Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
  IPS name _____
Interface Configuration
  Interface FastEthernet0/1
    Inbound IPS rule is SECURIPS
    Outgoing IPS rule is not set
```

Task 3: Load Signatures

In this task, you will replace the existing signatures in your router with the latest IPS signature file, attack-drop.sdf.

Activity Procedure

Complete these steps:

Step 1 Create an IPS rule:

```
Router(config)# ip ips name SECURIPS
```

Step 2 Specify the location where the router will load the SDF. If this command is not issued, the router will load the default SDF.

```
Router(config)# ip ips sdf location flash:attack-drop.sdf
```

Q2) Record the following results:

```
R2#sh ip ips configuration
```

```
Configured SDF locations: _____
```

```
Built-in signatures are: _____
```

Step 3 (Optional) Instruct the router to drop all packets until the signature engine is built and ready to scan traffic. If this command is issued, one of the following scenarios will occur:

- If IPS fails to load the SDF, all packets will be dropped—unless the user specifies an ACL for packets to send to IPS.
- If IPS successfully loads the SDF but fails to build a signature engine, all packets that are destined for that engine will be dropped.

If this command is not issued, all packets will be passed without scanning if the signature engine fails to build.

```
Router(config)# ip ips fail closed
```

Step 4 Configure an interface type and enter interface configuration mode:

```
Router(config)# interface Fa0/1
```

Step 5 Remove the IPS rule at the interface:

```
Router(config-if)# no ip ips SECURIPS in
```

Step 6 Apply an IPS rule at the interface. This command automatically loads the signatures and builds the signature engines.

```
Router(config-if)# ip ips SECURIPS in
```

Note Whenever signatures are replaced or merged, the router prompt is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.

Step 7 Exit configuration mode:

```
Router(config-if)# ^z
```

Q3) Record the following results after issuing a **sh ip ips config** command:

Configured SDF locations: _____

IDS fail closed is: _____

Total active signatures: _____

Step 8 Verify signature configuration, such as signatures that have been disabled:

```
Router# show ip ips signatures
```

Activity Verification

You have completed this task when you attain these results:

- Signatures are displayed after the command in Step 8. The output should be similar to this:

```
R2#sh ip ips signatures
```

```
Signatures were last loaded from flash:attack-drop.sdf
```

```
SDF release version attack-drop.sdf v2
```

```
*=Marked for Deletion Action=(A)larm, (D)rop, (R)eset Trait=AlarmTraits
```

```
MH=MinHits AI=AlarmInterval CT=ChokeThreshold
```

```
TI=ThrottleInterval AT=AlarmThrottle FA=FlipAddr
```

```
WF=WantFrag Ver=Signature Version
```

```
Signature Micro-Engine: SERVICE.SMTP (1 sigs)
```

SigID:SubID	On	Action	Sev	Trait	MH	AI	CT	TI	AT	FA	WF	Ver
3129:0	Y	ADR	MED	0	0	0	0	15	FA	N		S59

```
Signature Micro-Engine: SERVICE.RPC (29 sigs)
```

SigID:SubID	On	Action	Sev	Trait	MH	AI	CT	TI	AT	FA	WF	Ver
6100:0	Y	AD	HIGH	0	0	0	100	30	FA	N		1.0
6100:1	Y	ADR	HIGH	0	0	0	100	30	FA	N		1.0
6101:0	Y	AD	HIGH	0	0	0	100	30	FA	N		1.0
6101:1	Y	ADR	HIGH	0	0	0	100	30	FA	N		1.0
6104:0	Y	AD	HIGH	0	0	0	100	30	FA	N		2.2
6104:1	Y	ADR	HIGH	0	0	0	100	30	FA	N		2.2

Task 4: Merge the attack-drop.sdf File with the Default, Built-in Signatures

You may want to merge the built-in signatures with the attack-drop.sdf file if you find that the built-in signatures are not providing your network with adequate protection from security threats. Use this task to add the SDF and to change default parameters for a specific signature within the SDF or signature engine.

Activity Procedure

Complete these steps:

Step 1 Reload built-in signatures:

```
Router(config)# no ip ips sdf location flash:attack-drop.sdf
Router(config)# int Fa0/1
Router(config-if)# no ip ips SECURIPS in
Router(config-if)# ip ips SECURIPS in
```

Step 2 Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures:

```
Router# copy flash:attack-drop.sdf ips-sdf
```

Loads the SDF in the router. The SDF will merge with the signatures that are already loaded in the router, unless the **/erase** keyword is issued.

Step 3 Save newly merged signatures in a new file:

```
Router# copy ips-sdf flash:my-signatures.sdf
```

Step 4 Configure the router to use new file:

```
Router(config)# ip ips sdf location flash:my-signatures.sdf
```

Step 5 Reinitialize the IPS by removing the IPS rule set and reapplying the rule set:

```
Router(config-if)# interface fa 0/1
Router(config-if)# no ip ips SECURIPS in
```

Step 6 Reapply the rule set to interface:

```
router(config-if)# ip ips SECURIPS in
```

Step 7 Leave interface configuration mode:

```
router(config-if)# exit
```

Step 8 Leave terminal configuration mode:

```
router(config)# exit
```

Q4) Record the following results after issuing a **sh ip ips config** command:

```
Configured SDF Locations:
-----
Builtin signatures _____
Last successful SDF load time: 03:55:17 UTC Mar 2 2002
IDS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Total Active Signatures: _____
Signature 1107:0 disable
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh ip ips config** command and confirm that the output is similar to this:

```
R2#sh ip ips conf
Configured SDF Locations:
  flash:my-signatures.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 03:55:17 UTC Mar 2 2002
IDS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through Net Director is disabled
Event notification through SDEE is disabled
Total Active Signatures: 183
Total Inactive Signatures: 0
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
      :Curr Event Buf Size:0 Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
  IPS name SECURIPS
Interface Configuration
  Interface FastEthernet0/1
    Inbound IPS rule is SECURIPS
    Outgoing IPS rule is not set
```

Task 5: Verify the Configuration

You will verify the IPS router configuration.

Activity Procedure

Complete these steps:

Step 1 Display your IPS configuration:

```
router# show ip ips configuration
```

The parameters that you just configured along with several default settings are displayed.

Step 2 Display your IPS interface configuration:

```
router# show ip ips interface
```

The parameters that you just configured along with several default settings are displayed.

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh ip ips conf** command. The output should be similar to the following:

```
R2#sh ip ips conf
Configured SDF Locations:
  flash:my-signatures.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 03:55:17 UTC Mar 2 2002
IDS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through Net Director is disabled
Event notification through SDEE is disabled
Total Active Signatures: 183
Total Inactive Signatures: 0
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
      :Curr Event Buf Size:0 Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
  IPS name SECURIPS
Interface Configuration
  Interface FastEthernet0/1
```

```
Inbound IPS rule is SECURIPS
Outgoing IPS rule is not set
R2#sh ip ips interfaces
Interface Configuration
Interface FastEthernet0/1
Inbound IPS rule is SECURIPS
Outgoing IPS rule is not set
```

Task 6: Generate a Test Message

You will generate a test message.

Activity Procedure

Complete these steps:

- Step 1** Start the syslog server on your Windows 2000 Server.
- Step 2** Send multiple fragmented packets to the perimeter router of another pod using the following special technique:

```
router# ping
Protocol [IP] <Enter>
Target IP address: 172.30.Q.2<Enter>
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.

Activity Verification

You have completed this task when you attain these results:

- Check syslog server log file.

Lab 2-3 Answer Key: Configuring a Cisco Router with Cisco IOS Firewall IPS

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) Issue a **sh ip ips configuration** command and record these results:

```
Configured SDF Locations:
_____
Builtin signatures are _____
Last successful SDF load time: _____
IDS fail closed is _____
Fastpath ips is _____
Quick run mode is enabled
Event notification through syslog is _____
Event notification through Net Director is _____
Event notification through SDEE is _____
Total Active Signatures: ____
Total Inactive Signatures: ____
PostOffice:HostID:0 OrgID:0 Msg dropped:0
                :Curr Event Buf Size:0 Configured:100
Post Office is _____ - ____ connections are active
```

Q2) Record the following results:

R2#sh ip ips configuration

```
Configured SDF Locations: _____
Builtin signatures are _____ and _____
Last successful SDF load time: _____
IDS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is _____
Event notification through Net Director is disabled
Event notification through SDEE is disabled
Total Active Signatures: _____
Total Inactive Signatures: 0
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
                :Curr Event Buf Size:0 Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
  IPS name _____
Interface Configuration
  Interface FastEthernet0/1
    Inbound IPS rule is SECURIPS
    Outgoing IPS rule is not set
```

Q3) Record the following results:

R2#**sh ip ips configuration**

Configured SDF locations: _____

Built-in signatures are: _____

Q4) Record the following results after issuing a **sh ip ips config** command:

Configured SDF locations: _____

IDS fail closed is: _____

Total active signatures: _____

Q5) Record the following results after issuing a **sh ip ips config** command:

Configured SDF Locations:

Builtin signatures _____

Last successful SDF load time: 03:55:17 UTC Mar 2 2002

IDS fail closed is enabled

Fastpath ips is enabled

Quick run mode is enabled

Event notification through syslog is enabled

Total Active Signatures: _____

Signature 1107:0 disable

Lab 3-1: Mitigating Layer 2 Attacks

Complete this lab activity to practice what you learned in the related module.

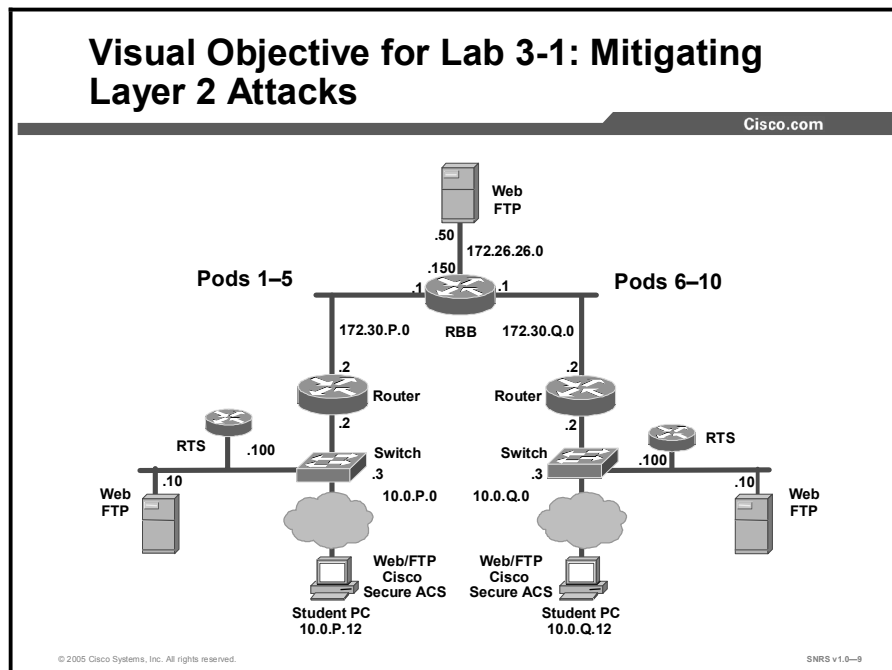
Activity Objective

In this activity, you will configure network switches and routers to mitigate Layer 2 attacks. After completing this activity, you will be able to meet these objectives:

- Mitigate a CAM table overflow attack
- Mitigate a MAC spoofing attack
- Mitigate a DHCP starvation attack

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity

Command List

The table describes the commands used in this activity.

Router Commands

Command	Description
<code>arp timeout seconds</code>	To configure how long an entry remains in the ARP cache, use the arp timeout command in interface configuration mode. To restore the default value, use the no form of this command.
<code>show port-security [address] [interface interface-id]</code>	To display the port security settings for an interface or for the switch, use the show port-security command.
<code>switchport port-security</code>	Enables port security on the interface.
<code>switchport port-security mac-address mac-addr</code>	To set the maximum number of secure MAC addresses on an interface, use the switchport-port-security mac-address command. Use the no form of this command to remove a MAC address from the list of secure MAC addresses.
<code>switchport port-security maximum max-addr</code>	Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 128; the default is 128.
<code>switchport port-security violation {shutdown restrict protect}</code>	Set the security violation mode for the interface.
<code>ip dhcp snooping</code>	Enables DHCP snooping globally.
<code>ip dhcp snooping vlan vlan_id {,vlan_id}</code>	Enable DHCP snooping on a VLAN or range of VLANs.
<code>ip dhcp snooping trust</code>	Configure the interface as trusted or untrusted. The default is untrusted.
<code>ip dhcp snooping limit rate rate</code>	Configure the number of DHCP packets per second than an interface can receive. The range is 1 to 4,294,967,294. The default is no rate limit configured.

Job Aids

There are no job aids for this activity.

Task 1: Mitigate a CAM Table Overflow Attack

You will mitigate a CAM table overflow attack with the appropriate Cisco IOS commands.

Activity Procedure

Complete these steps:

Step 1 Set the port mode to access:

```
sw-class(config-if)# switchport mode access
```

Step 2 Enable port security on the selected interface:

```
sw-class(config-if)# switchport port-security
```

Step 3 Configure the maximum number of MAC addresses (the default is one):

```
sw-class(config-if)# switchport port-security maximum 1
```

Step 4 Configure the action to take on violation (the default is to shut down):

```
sw-class(config-if)# switchport port-security violation shutdown
```

Step 5 Configure the MAC address for the port:

```
sw-class(config-if)# switchport port-security mac-address 0000.ffff.1111
```

Step 6 Plug a laptop into Fa0/12 and try to ping the gateway:

```
C:\WINNT\system32>ping 10.0.2.2
```

Activity Verification

You have completed this task when you attain these results:

- Issue the following commands and fill in the blanks:

Q1) `sw-class#sh port-security int fa0/12`

```
Port Security           : _____
Port Status             : _____
Violation Mode          : _____
Maximum MAC Addresses   : ___
Total MAC Addresses     : ___
Configured MAC Addresses : ___
Last Source Address     : 0050.daeb.43d4
Security Violation Count : ___
```

Q2) `sw-class#sh port-security address`

Secure Mac Address Table

```
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----
1       0000.ffff.1111   _____<answer>_____ Fa0/12    -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Task 2: Mitigate a MAC Spoofing Attack

You will mitigate a MAC spoofing attack with appropriate Cisco Catalyst operating system and Cisco IOS commands.

Activity Procedure

Complete these steps:

Step 1 Configure the maximum number of MAC addresses:

```
rl-class-sw(config-if)# switchport port-security maximum 1
```

Step 2 Configure the action to take on violation:

```
rl-class-sw(config-if)# switchport port-security violation  
shutdown
```

Step 3 Specify the ARP timeout:

```
rl-class-sw(config-if)# arp timeout seconds
```

Activity Verification

You have completed this task when you attain these results:

- You plug in another PC into the port without the correct MAC address, and the port is shut down. The output from the following commands should be similar to this:

```
sw-class#sh port-security  
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action  
              (Count)          (Count)      (Count)  
-----  
Fa0/12        1             1             1                 Shutdown  
-----  
Total Addresses in System (excluding one mac per port) : 0  
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
sw-class#sh port-security int fa0/12  
Port Security : Enabled  
Port Status : Secure-shutdown  
Violation Mode : Shutdown  
Aging Time : 0 mins  
Aging Type : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses : 1  
Total MAC Addresses : 1  
Configured MAC Addresses : 1  
Sticky MAC Addresses : 0  
Last Source Address : 0050.daeb.43d4
```

Security Violation Count : 1

sw-class#sh int statu

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	10/100BaseTX	notconnect	1	auto	auto	
Fa0/2	10/100BaseTX	connected	302	a-full	a-100	
Fa0/3	10/100BaseTX	notconnect	1	auto	auto	
Fa0/4	10/100BaseTX	notconnect	1	auto	auto	
Fa0/5	10/100BaseTX	notconnect	1	auto	auto	
Fa0/6	10/100BaseTX	notconnect	1	auto	auto	
Fa0/7	10/100BaseTX	notconnect	307	auto	auto	
Fa0/8	10/100BaseTX	notconnect	1	auto	auto	
Fa0/9	10/100BaseTX	notconnect	1	auto	auto	
Fa0/10	10/100BaseTX	notconnect	1	auto	auto	
Fa0/11	10/100BaseTX	notconnect	1	auto	auto	
Fa0/12	10/100BaseTX	err-disabled	1	auto	auto	
Fa0/13	10/100BaseTX	notconnect	1	auto	auto	

Q3) What state will the port be in after a violation?

Task 3: Mitigate a DHCP Starvation Attack

You will mitigate a DHCP starvation attack with appropriate Cisco Catalyst operating system and Cisco IOS commands.

Activity Procedure

Complete these steps:

Step 1 Enable DHCP snooping globally:

```
switch(config)#ip dhcp snooping
```

Step 2 Enable DHCP snooping on a VLAN or range of VLANs. You can specify a single VLAN identified by a VLAN ID number or give starting and ending VLAN IDs to specify a range of VLANs. The range is 1 to 4094.

```
switch(config)#ip dhcp snooping vlan vlan_id {,vlan_id
```

Step 3 Switch to interface configuration mode:

```
switch(config)# interface Fa0/12
```

Step 4 Configure the interface as trusted. You can use the **no** keyword to configure an interface to receive messages from an untrusted client. The default is untrusted.

```
switch(config-if)#ip dhcp snooping trust
```

Step 5 Configure the number of DHCP packets per second that an interface can receive. The range is 1 to 4,294,967,294. The default is no rate limit configured.

```
switch(config-if)#ip dhcp snooping limit rate rate
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh ip dhcp snooping** command. Your output should be similar to the following:

```
sw-class#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
201
Insertion of option 82 is enabled
Interface                Trusted      Rate limit (pps)
-----                -
FastEthernet0/12         yes         unlimited
```

Lab 3-1 Answer Key: Mitigating Layer 2 Attacks

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) `sw-class#sh port-security int fa0/12`

```
Port Security           : _____
Port Status             : _____
Violation Mode          : _____
Maximum MAC Addresses   : ____
Total MAC Addresses     : ____
Configured MAC Addresses : ____
Last Source Address     : 0050.daeb.43d4
Security Violation Count : ____
```

Q2) `sw-class#sh port-security address`

Secure Mac Address Table

```
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----
1       0000.ffff.1111    _____         Fa0/12   -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Q3) What state will the port be in after a violation?

Job Aids

There are no job aids for this activity.

Task 1: Install a Server Certificate

You must have a server certificate for your Cisco Secure ACS before you begin installation. With Cisco Secure ACS, certificate files must be in base 64-encoded X.509. (If you do not already have a server certificate in storage, you can use the following procedure or any other means, to obtain a certificate for installation. You can use Cisco Secure ACS to generate a self-signed digital certificate to be used for PEAP authentication or for HTTPS support of Cisco Secure ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.)

Activity Procedure

Complete these steps:

- Step 1** To generate a self-signed certificate, begin by creating a directory on your student PC for use with the certificate:
- ```
c: >md c:\acs_server_cert
```
- Step 2** In the Cisco Secure ACS navigation bar, click **System Configuration**.
- Step 3** Click **ACS Certificate Setup**.
- Step 4** Click **Generate Self-Signed Certificate**.
- Step 5** Enter **cn=securacs** in the Certificate Subject field.
- Step 6** Enter **c:\acs\_server\_cert\acs\_server\_cert.cer** in the Certificate File field.
- Step 7** Enter **c:\acs\_server\_cert\acs\_server\_cert.pvk** in the Private Key File field.
- Step 8** Enter **secur** for the private key password.
- Step 9** In the Retype Private Key Password field, re-enter the private key password.
- Step 10** In the Key Length field, choose the default key length (the default is 2048).
- Step 11** In the Digest to Sign With field, choose the **Sha-1** hash digest to be used to encrypt the key.
- Step 12** To install the self-signed certificate when you submit the page, choose the **Install Generated Certificate** option.

---

**Note** When you use the Install Generated Certificate option, you must restart Cisco Secure ACS services after submitting this form to adopt the new settings.

---

---

**Note** If you do not choose the Install Generated Certificate option, the certificate file and private key file are generated and saved when you click Submit in the next step, but they are not installed in local machine storage.

---

**Step 13** Click **Submit**.

The specified certificate and private key files are generated and stored, as specified. The certificate becomes operational only after you restart Cisco Secure ACS services.

### Activity Verification

- In the System Configuration tab, click ACS Certificate Setup, then click on Install Certificate. You should see your new certificate installed.

## Task 2: Configure EAP Settings

You will configure EAP settings on the Cisco Secure ACS. Use this procedure to select and configure how Cisco Secure ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that you allow and to specify whether you allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

### Activity Procedure

Complete these steps:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Global Authentication Setup**.
- Step 3** Make sure that the **EAP-MD5** check box is checked.
- Step 4** Click **Submit**.

---

**Note** If you want to save the settings that you have made but implement them later, click **Submit**. You can restart Cisco Secure ACS services at any time by using the Service Control page in the System Configuration section.

---

### Activity Verification

You have completed this task when you attain these results:

- Check the EAP settings in the Global Authentication window.



## Task 3: Specify the Access Device

You will specify and configure the switch as an AAA client.

### Activity Procedure

Complete these steps:

- Step 1** Click the **Network Configuration** tab.
- Step 2** Click **Not Assigned** under Device Groups.
- Step 3** Click **Add Entry** in the AAA Client window.
- Step 4** Enter the following:
  1. The switch address
  2. A key of **ciscosecure**
  3. Authenticate using RADIUS (IETF)
- Step 5** Click **Submit**.

### Activity Verification

You have completed this task when you attain these results:

- The host name appears in the AAA Clients window.

## Task 4: Restart the Service

You can restart Cisco Secure ACS services at any time by using the Service Control page in the System Configuration area.

### Activity Procedure

Complete these steps:

- Step 1** Click **System Configuration**.
- Step 2** Click **Service Control**.
- Step 3** Click **Restart**.

### Activity Verification

You have completed this task when you attain these results:

- “Is Currently Running” appears in the System Configuration > Service Control window.

## **Lab 3-2 Answer Key: Configuring EAP on Cisco Secure ACS for Windows Server**

There is no Answer Key for this activity.

# Lab 3-3: Configuring 802.1x Port-Based Authentication

Complete this lab activity to practice what you learned in the related module.

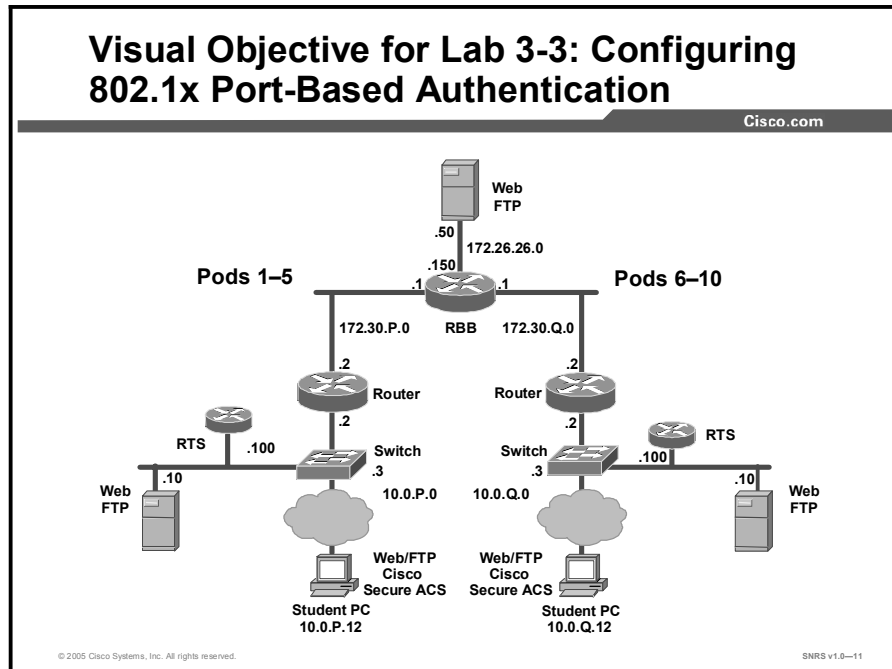
## Activity Objective

In this activity, you will configure 802.1x port-based authentication on a Cisco Catalyst 2950 switch. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- Enable 802.1x authentication
- Configure the switch-to-RADIUS server communication
- Enable periodic reauthentication
- Manually reauthenticate a client connected to a port
- Change the quiet period
- Change the switch-to-client retransmission time
- Set the switch-to-client frame-retransmission number
- Enable multiple hosts
- Reset the 802.1x configuration to the default values
- Display 802.1x statistics and status

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Switch Commands

| Command                                                                                                                                                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>aaa authentication dot1x {default   listname} method1 [method2...]</code>                                                                                                                                      | To specify one or more AAA methods for use on interfaces running IEEE 802.1x, use the <b>aaa authentication dot1x</b> command in global configuration mode. To disable authentication, use the <b>no</b> form of this command                                                                                                                                                                                      |
| <code>aaa new-model</code>                                                                                                                                                                                           | To enable the AAA access control model, issue the <b>aaa new-model</b> command in global configuration mode. To disable the AAA access control model, use the <b>no</b> form of this command.                                                                                                                                                                                                                      |
| <code>dot1x default</code>                                                                                                                                                                                           | To reset the global 802.1x parameters to their default values, use the <b>dot1x default</b> command in global configuration mode.                                                                                                                                                                                                                                                                                  |
| <code>dot1x max-req number-of-retries</code>                                                                                                                                                                         | To set the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the <b>dot1x max-req</b> command in interface configuration or global configuration mode. To disable the number of times that were set, use the <b>no</b> form of this command. |
| <code>dot1x multiple-hosts</code>                                                                                                                                                                                    | To allow multiple hosts (clients) on an 802.1x-authorized port that has the <b>dot1x port-control</b> interface configuration command set to <b>auto</b> , use the <b>dot1x multiple-hosts</b> command in interface configuration mode. To return to the default setting, use the <b>no</b> form of this command.                                                                                                  |
| <code>dot1x port-control {auto   force-authorized   force-unauthorized}</code>                                                                                                                                       | To set an 802.1x port control value, use the <b>dot1x port-control</b> command in interface configuration mode. To disable the port-control value, use the <b>no</b> form of this command.                                                                                                                                                                                                                         |
| <code>dot1x re-authenticate interface-type interface-number</code>                                                                                                                                                   | To enable periodic reauthentication of the client PCs on the 802.1x interface, use the <b>dot1x reauthentication</b> command in interface configuration mode. To disable periodic reauthentication, use the <b>no</b> form of this command.                                                                                                                                                                        |
| <code>dot1x timeout {auth-period seconds   held-period seconds   quiet-period seconds   ratelimit-period seconds   reauth-period seconds   server-timeout seconds   start-period seconds   tx-period seconds}</code> | To set retry timeouts, use the <b>dot1x timeout</b> command in interface configuration mode. To remove the retry timeouts, use the <b>no</b> form of this command.                                                                                                                                                                                                                                                 |
| <code>radius-server host {hostname   ip-address} [auth-port port-number] [acct-port port-number]</code>                                                                                                              | To specify a RADIUS server host, use the <b>radius-server host</b> command in global configuration mode. To delete the specified RADIUS host, use the <b>no</b> form of this command.                                                                                                                                                                                                                              |

| Command                                                                                                     | Description                                                                                         |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <code>[timeout seconds]<br/>[retransmit retries] [key<br/>string] [alias{hostname  <br/>ip-address}]</code> |                                                                                                     |
| <code>show dot1x [interface<br/>interface-name [details]]</code>                                            | To show details for an identity profile, use the <b>show dot1x</b> command in privileged EXEC mode. |
| <code>show dot1x [interface<br/>interface-name [details]]</code>                                            | To show details for an identity profile, use the <b>show dot1x</b> command in privileged EXEC mode. |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will set up the lab.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that Windows 2000 Server is operational. Your instructor will provide you with the correct username and password to log in to 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 Syslog Daemon).
- Step 4** Reload your perimeter router using the default lab configuration.
- Step 5** Ensure that you can ping the other routers and network hosts before beginning.
- Step 6** On the PC, under the Authentication tab of Local Area Network Connection Properties, check the following:
  - The Enable Network Access Control Using IEEE 802.1x check box is checked.
  - The EAP type is MD5-Challenge.

### Activity Verification

You have completed this task when you attain these results:

- You can ping the other hosts.

## Task 2: Enable 802.1x Authentication

You will enable 802.1x authentication.

### Activity Procedure

Complete these steps:

**Step 1** Enable AAA:

```
switch(config)# aaa new-model
```

**Step 2** Create an 802.1x authentication method list:

```
switch(config)# aaa authentication dot1x default group radius local
```

To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

Enter at least one of these keywords:

- **group radius**: Use the list of all RADIUS servers for authentication.
- **none**: Use no authentication. The client is automatically authenticated without the switch using the information supplied by the client.

**Step 3** Configure AAA accounting:

```
switch(config)# aaa accounting network default start-stop group radius
switch(config)# aaa accounting connection default start-stop group radius
```

**Step 4** Issue the **dot1x system-auth-control** command:

```
switch(config)#dot1x system-auth-control
```

**Step 5** Enter interface configuration mode, and specify the interface to be enabled for 802.1x authentication:

```
switch(config)# interface fa0/12
```

**Step 6** Enable 802.1x authentication on the interface:

```
switch(config-if)# dot1x port-control auto
```

**Step 7** Return to privileged EXEC mode:

```
switch(config-if)# end
```

**Step 8** Verify your entries.

Check the Status column in the 802.1x Port Summary section of the display. An Enabled status means that the port-control value is set either to auto or to force-unauthorized.

```
switch# show dot1x
```

Q1) What command enables system authorization?

---

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x** command. The output should be similar to the following:

```
sw-class#sh dot1x
Sysauthcontrol = Enabled
Dot1x Protocol Version = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

## Task 3: Configure the Switch-to-RADIUS Server Communication

You will configure the switch-to-RADIUS server communication.

### Activity Procedure

Complete these steps:

- Step 1** Configure the RADIUS server parameters on the switch:

```
switch(config)# radius-server host 10.0.P.12 auth-port port-number key
string
```

---

**Note** For **auth-port *port-number***, specify the UDP destination port for authentication requests. The default is 1812.

---

- Step 2** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 3** Verify your entries:

```
switch# show running-config
```

### Activity Verification

You have completed this task when you attain these results:

- You should see the following lines:

```
!
radius-server host 10.0.2.12 auth-port 1812 acct-port 1813 key
ciscosecure
radius-server retransmit 3
!
```

## Task 4: Enable Periodic Reauthentication

You will enable periodic reauthentication.

### Activity Procedure

Complete these steps:

**Step 1** Change to interface configuration mode:

```
sw-class(config)#int fa0/12
```

**Step 2** Enable periodic reauthentication of the client, which is disabled by default:

```
switch(config-if)# dot1x re-authentication
```

**Step 4** Set the number of seconds between reauthentication attempts (the default is 3600 seconds):

```
switch(config-if)# dot1x timeout re-authperiod 4000
```

**Step 1** Return to privileged EXEC mode:

```
switch(config)# end
```

**Step 2** Verify your entries:

```
switch# show dot1x
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x all** command. The output should be similar to the following:

```
sw-class#sh dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```

Supplicant MAC <Not Applicable>
 AuthSM State = CONNECTING
 BendSM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 2
HostMode = Single
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod = 4000 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 0
```



## Task 5: Manually Reauthenticate a Client Connected to a Port

You will manually reauthenticate a client connected to a port.

### Activity Procedure

Complete this step:

- Step 1** Manually reauthenticate the client connected to a port:

```
Switch# dot1x re-authenticate interface interface
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x all** command. The output should be similar to this:

```
sw-class#sh dot1x all
Dot1x Info for interface FastEthernet0/12

Supplicant MAC <Not Applicable>
 AuthSM State = CONNECTING
 BendsM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 2
HostMode = Single
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod = 4000 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 0
```

## Task 6: Change the Quiet Period

You will change the quiet period.

### Activity Procedure

Complete this step:

- Step 1** Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

The range is 0 to 65,535 seconds; the default is 60.

```
switch(config-if)# dot1x timeout quiet-period 90
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x all** command. The output should be similar to this:

```
sw-class#sh dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```

Supplicant MAC <Not Applicable>
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 2
HostMode = Single
Port Control = Auto
QuietPeriod = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod = 4000 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
Guest-Vlan = 0
```

## Task 7: Change the Switch-to-Client Retransmission Time

You will change the switch-to-client retransmission time.

### Activity Procedure

Complete this step:

- Step 1** Set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.

The range is 1 to 65,535 seconds; the default is 30.

```
switch(config-if)# dot1x timeout tx-period 45
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x all** command. The output should be similar to this:

```
sw-class#sh dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```

Supplicant MAC <Not Applicable>
 AuthSM State = CONNECTING
 BendSM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 3
HostMode = Multi
Port Control = Auto
QuietPeriod = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod = 4000 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 45 Seconds
Guest-Vlan = 0
```

## Task 8: Set the Switch-to-Client Frame-Retransmission Number

You will set the switch-to-client frame-retransmission number.

### Activity Procedure

Complete this step:

- Step 1** Set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.

```
switch(config-if)# dot1x max-req 3
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x all** command. The output should be similar to this:

```
sw-class#sh dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```

Supplicant MAC <Not Applicable>
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 3
HostMode = Multi
Port Control = Auto
QuietPeriod = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod = 4000 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 45 Seconds
Guest-Vlan = 0
```

## Task 9: Enable Multiple Hosts

You will enable multiple hosts.

### Activity Procedure

Complete these steps:

- Step 1** Enter interface configuration mode, and specify the interface to which multiple hosts are indirectly attached:

```
switch(config)# interface interface-id
```

- Step 2** Issue the following command to allow multiple hosts (clients) on an 802.1x-authorized port:

```
switch(config-if)# dot1x host-mode multi-host
```

Make sure that the **dot1x port-control** interface configuration command set is set to Auto for the specified interface.

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh dot1x all** command. The output should be similar to this:

```
sw-class#sh dot1x all
```

```
Dot1x Info for interface FastEthernet0/12
```

```

Supplicant MAC <Not Applicable>
 AuthSM State = CONNECTING
 BendSM State = IDLE
PortStatus = UNAUTHORIZED
MaxReq = 3
HostMode = Multi
Port Control = Auto
QuietPeriod = 90 Seconds
Re-authentication = Enabled
ReAuthPeriod = 4000 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 45 Seconds
Guest-Vlan = 0
```

## Task 10: Reset the 802.1x Configuration to the Default Values

You will reset the 802.1x configuration to the default values.

### Activity Procedure

Complete this step:

**Step 1** Reset the configurable 802.1x parameters to the default values:

```
switch# dot1x default
```

### Activity Verification

You have completed this task when you attain these results:

- You see the following lines:

```
switch(config-if)#dot1x default
Setting the Default Configuration for Dot1x on this interface
and
switch#sh dot1x all
```

```
No Dot1x Configuration exists
```

## Task 11: Display 802.1x Statistics and Status

You will display 802.1x statistics and status.

### Activity Procedure

Complete this step:

**Step 1** Display 802.1x statistics for a specific interface:

```
switch# show dot1x statistics interface Fa0/12
```

### Activity Verification

You have completed this task when you attain these results:

- Issue the **show dot1x statistics interface Fa0/12** command. The output should be similar to this:

```
sw-class#sh dot1x statistics interface fa0/12
PortStatistics Parameters for Dot1x

TxReqId = 7 TxReq = 0 TxTotal = 7
RxStart = 0 RxLogoff = 0 RxRespId = 0 RxResp = 0
RxInvalid = 0 RxLenErr = 0 RxTotal= 0
RxVersion = 0 LastRxSrcMac 0000.0000.0000
```

## Lab 3-3 Answer Key: Configuring 802.1x Port-Based Authentication

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What command enables system authorization?

---





## Task 1: Complete the Lab Exercise Setup

You will complete the lab exercise setup by ensuring connectivity with other routers in the lab.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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** 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 that you can ping your peer router and network host before beginning.

### Activity Verification

You have completed this task when you attain these results:

- Your pings are successful.

## Task 2: Prepare for ISAKMP and IPsec

Prepare for configuring IPsec by determining ISAKMP and IPsec policy and verifying connectivity with the peer pod router.

### Activity Procedure

Complete these steps:

**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:

- The ISAKMP policy is to use pre-shared keys.
- The IPsec policy is to use ESP mode with DES encryption.
- The IPsec policy is to encrypt all traffic between perimeter routers.

**Step 2** Verify that connectivity has been established to the router of the other group by entering the following command:

```
router> enable
password: cisco
router# ping 172.30.Q.2
```

(where Q = peer pod number)

### Activity Verification

You have completed this task when you attain these results:

- Your output should resemble the following:

```
R2#ping 172.30.7.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.30.7.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

## **Lab 4-1 Answer Key: Preparing the Network for IPSec Configuration with Pre-Shared Keys**

There is no Answer Key for this activity.

# Lab 4-2: Configuring ISAKMP Using Pre-Shared Keys

Complete this lab activity to practice what you learned in the related module.

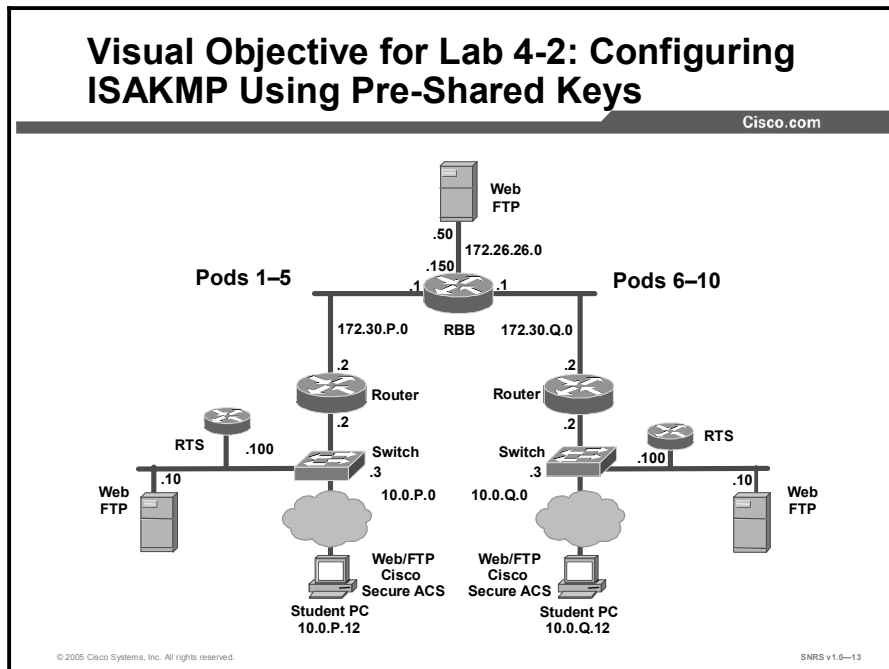
## Activity Objective

In this activity, you will configure ISAKMP on your network for IPsec using pre-shared keys. After completing this activity, you will be able to meet these objectives:

- Enable ISAKMP on the router

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                          | Description                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>authentication {rsa-sig   rsa-encr   pre-share}</code>                     | To specify the authentication method within an IKE policy, use the <b>authentication</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.                                                                                                             |
| <code>crypto isakmp enable</code>                                                | To globally enable IKE at your peer router, use the <b>crypto isakmp enable</b> command in global configuration mode.                                                                                                                                                                                                        |
| <code>crypto isakmp key key-string address peer-address [mask] [no-xauth]</code> | To configure a pre-shared authentication key, use the <b>crypto isakmp key</b> command in global configuration mode.                                                                                                                                                                                                         |
| <code>crypto isakmp policy priority</code>                                       | To define an IKE policy, use the <b>crypto isakmp policy</b> command in global configuration mode. IKE policies define a set of parameters to be used during the IKE negotiation.                                                                                                                                            |
| <code>encryption {des   3des   aes   aes 192   aes 256}</code>                   | To specify the encryption algorithm within an IKE policy, use the <b>encryption</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the <b>no</b> form of this command.                  |
| <code>group {1   2}</code>                                                       | To specify the Diffie-Hellman group identifier within an IKE policy, use the <b>group</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the <b>no</b> form of this command. |
| <code>hash {sha   md5}</code>                                                    | To specify the hash algorithm within an IKE policy, use the <b>hash</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default SHA-1 hash algorithm, use the <b>no</b> form of this command.                     |
| <code>lifetime seconds</code>                                                    | To specify the lifetime of an IKE SA, use the <b>lifetime</b> command in ISAKMP policy configuration mode. To reset the SA lifetime to the default value, use the <b>no</b> form of this command.                                                                                                                            |
| <code>show crypto isakmp policy</code>                                           | To display the parameters for each IKE policy, use the <b>show crypto isakmp policy</b> command in EXEC mode.                                                                                                                                                                                                                |

## Job Aids

There are no job aids for this activity.

## Task 1: Enable ISAKMP

You will enable IKE/ISAKMP on the router. Work with the members of your peer pod to complete this lab exercise.

### Activity Procedure

Complete these steps:

**Step 1** Ensure that you are in configuration mode:

```
router# config t
```

**Step 2** Enable ISAKMP on the router:

```
router(config)# crypto isakmp enable
```

**Step 3** Create an IKE policy to use pre-shared keys by completing the following substeps:

1. Set the policy priority and enter ISAKMP policy configuration mode:

```
router(config)# crypto isakmp policy 110
```

2. Set authentication to use pre-shared keys:

```
router(config-isakmp)# authentication pre-share
```

Q1) What are the options for authentication?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Step 4** Set IKE encryption:

```
router(config-isakmp)# encryption des
```

Q2) What are the options for encryption?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Step 5** Set the Diffie-Hellman group:

```
router(config-isakmp)# group 1
```

Q3) What are the options for the Diffie-Hellman group?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Step 6** Set the hash algorithm:

```
router(config-isakmp)# hash md5
```

Q4) What are the options for hashes?

\_\_\_\_\_  
\_\_\_\_\_

**Step 7** Set the ISAKMP SA lifetime:

```
router(config-isakmp)# lifetime 86400
```

**Step 8** Exit the ISAKMP policy configuration mode:

```
router(config-isakmp)# exit
```

**Step 9** Set up the pre-shared key and peer address:

```
router(config)# crypto isakmp key cisco1234 address 172.30.Q.2
```

(where Q = peer pod number)

**Step 10** Exit configuration mode:

```
router(config)# exit
```

**Step 11** Examine the crypto policy suite:

```
R2#sh crypto isakmp policy
```

```
Global IKE 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
```

## Activity Verification

You have completed this task when you attain these results:

- Your output is similar to the example in Step 11.

## Lab 4-2 Answer Key: Configuring ISAKMP Using Pre-Shared Keys

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What are the options for authentication?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Q2) What are the options for encryption?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Q3) What are the options DH group?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Q4) What are the options for hashes?

\_\_\_\_\_  
\_\_\_\_\_





## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny   permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log   log-input] [time-range time-range-name] [fragments]</code> | To define an extended IP ACL, use the extended version of the <b>access-list</b> command in global configuration mode. To remove the ACLs, use the <b>no</b> form of this command.                                                                                                                                                                                                         |
| <code>crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]</code>                                                                                                                                                       | To define a transform set—an acceptable combination of security protocols and algorithms—use the <b>crypto ipsec transform-set</b> command in global configuration mode. To delete a transform set, use the <b>no</b> form of this command.                                                                                                                                                |
| <code>crypto map map-name [redundancy standby-name]</code>                                                                                                                                                                                                         | To apply a previously defined crypto map set to an interface, use the <b>crypto map</b> command in interface configuration mode. To remove the crypto map set from the interface, use the <b>no</b> form of this command.                                                                                                                                                                  |
| <code>crypto map map-name seq-num [ipsec-manual]</code>                                                                                                                                                                                                            | To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the <b>crypto map</b> command in global configuration mode. To delete a crypto map entry, profile, or set, use the <b>no</b> form of this command. |
| <code>match address [access-list-id   name]</code>                                                                                                                                                                                                                 | To specify an extended ACL for a crypto map entry, use the <b>match address</b> command in crypto map configuration mode. To remove the extended ACL from a crypto map entry, use the <b>no</b> form of this command.                                                                                                                                                                      |
| <code>mode [tunnel   transport]</code>                                                                                                                                                                                                                             | To change the mode for a transform set, use the <b>mode</b> command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the <b>no</b> form of this command.                                                                                                                                                                                 |
| <code>set peer {host-name   ip-address}</code>                                                                                                                                                                                                                     | To specify an IPSec peer in a crypto map entry, use the <b>set peer</b> command in crypto map configuration mode. To remove an IPSec peer from a crypto map entry, use the <b>no</b> form of this command.                                                                                                                                                                                 |
| <code>set transform-set transform-set-name [transform-set-name2...transform-set-name6]</code>                                                                                                                                                                      | To specify which transform sets can be used with the crypto map entry, use the <b>set transform-set</b> command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the <b>no</b> form of this command.                                                                                                                                            |
| <code>show crypto ipsec transform-set [tag transform-set-name]</code>                                                                                                                                                                                              | To display the configured transform sets, use the <b>show crypto ipsec transform-set</b> command in EXEC mode.                                                                                                                                                                                                                                                                             |
| <code>show crypto map [interface interface   tag map-name]</code>                                                                                                                                                                                                  | To display the crypto map configuration, use the <b>show crypto map</b> command in EXEC mode.                                                                                                                                                                                                                                                                                              |

## Job Aids

There are no job aids for this activity.

## Task 1: Configure a Transform Set

You will configure a transform set.

### Activity Procedure

Complete these steps:

**Step 1** Verify that you are in configuration mode:

```
router# config t
```

**Step 2** View the available crypto IPsec command options by entering the following command:

```
router(config)# crypto ipsec ?
```

Q1) What are the options for crypto IPsec?

---

---

---

---

---

---

---

---

**Step 3** Check your transform set options by entering the following command:

```
router(config)# crypto ipsec transform-set ?
```

**Step 4** Define a transform set that includes the following:

- Transform name: **MINE**
- ESP protocols: **des**
- Mode: **tunnel**

```
router(config)# crypto ipsec transform-set MINE esp-des
```

Q2) What are the other options?

---

---

---

---

---

---

---

---

---

---

**Step 5** Set the mode to tunnel:

```
router(cfg-crypto-trans)# mode tunnel
```

Q3) What is the other mode?

---

**Step 6** Exit the configuration mode:

```
router(cfg-crypto-trans)# ^Z
```

**Step 7** Verify your configuration:

```
router# show crypto ipsec transform-set MINE
```

### Activity Verification

You have completed this task when you attain these results:

- Your output should be similar to the following:

```
router# show crypto ipsec transform-set MINE
Transform set MINE: { esp-des }
will negotiate = { Tunnel, },
```

## Task 2: Configure a Crypto ACL

You will 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 external interface**
- ACL number: **102**
- Protocol: **any Internet protocol**

### Activity Procedure

Complete these steps:

**Step 1** Ensure that you are in configuration mode:

```
router(config)# config terminal
```

**Step 2** Configure the ACL:

```
router(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)

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh access-list** command. The output should be similar to this:

```
R2#sh access-lists
Extended IP access list 102
 10 permit ip host 172.30.2.2 host 172.30.7.2
```

## Task 3: Configure a Crypto Map

In this task, you will 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**

### Activity Procedure

Complete these steps:

**Step 1** Set the name of the map, the map number, and the type of key exchange to be used:

```
router(config)# crypto map MYMAP 10 ipsec-isakmp
```

Q4) What is the other option?

---

**Step 2** Specify the extended ACL to use with this map:

```
router(config-crypto-map)# match address 102
```

Q5) What does the 102 refer to?

---

**Step 3** Specify the transform set that you defined earlier:

```
router(config-crypto-map)# set transform-set MINE
```

**Step 4** Assign the VPN peer using the host name or IP address of the peer:

```
router(config-crypto-map)# set peer 172.30.Q.2
```

(where Q = peer pod number)

**Step 5** Exit the crypto map configuration mode:

```
router(config-crypto-map)# exit
```

## Activity Verification

You have completed this task when you attain these results:

- Issue the **sh crypto map** command. The output should be similar to this:

```
R2#sh crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
 Peer = 172.30.7.2
 Extended IP access list 102
 access-list 102 permit ip host 172.30.2.2 host 172.30.7.2
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
 MINE,
 }
 Interfaces using crypto map MYMAP:
```

## Task 4: Apply the Crypto Map to an Interface

You will apply the crypto map to an interface. Use the following parameters:

- Interface to configure: **Ethernet 0/1**
- Crypto map to use: **MYMAP**

## Activity Procedure

Complete these steps:

- Step 1** Access interface configuration mode:  
router(config)# **interface fast 0/1**
- Step 2** Assign the crypto map to the interface:  
router(config-if)# **crypto map MYMAP**
- Step 3** Exit interface configuration mode:  
router(config-if)# **^Z**
- Step 4** Save the configuration:  
router# **copy running-config startup-config**

## Activity Verification

You have completed this task when you attain these results:

- Issue the **show crypto map interface fa0/1** command. The output should be similar to this:

```
R2#sh crypto map interface fa0/1
Crypto Map "MYMAP" 10 ipsec-isakmp
 Peer = 172.30.7.2
 Extended IP access list 102
 access-list 102 permit ip host 172.30.2.2 host 172.30.7.2
 Current peer: 172.30.7.2
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
 MINE,
 }
 Interfaces using crypto map MYMAP:
 FastEthernet0/1
```

## Lab 4-3 Answer Key: Configuring IPSec Using Pre-Shared Keys

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What are the options for crypto IPSec?

---

---

---

---

---

---

---

---

---

---

Q2) What are the other options?

---

---

---

---

---

---

---

---

---

---

---

Q3) What is the other mode?

---

Q4) What is the other option?

---

Q5) What does the 102 refer to?

---



# Lab 4-4: Testing and Verifying an IPSec Pre-Shared Key Configuration

Complete this lab activity to practice what you learned in the related module.

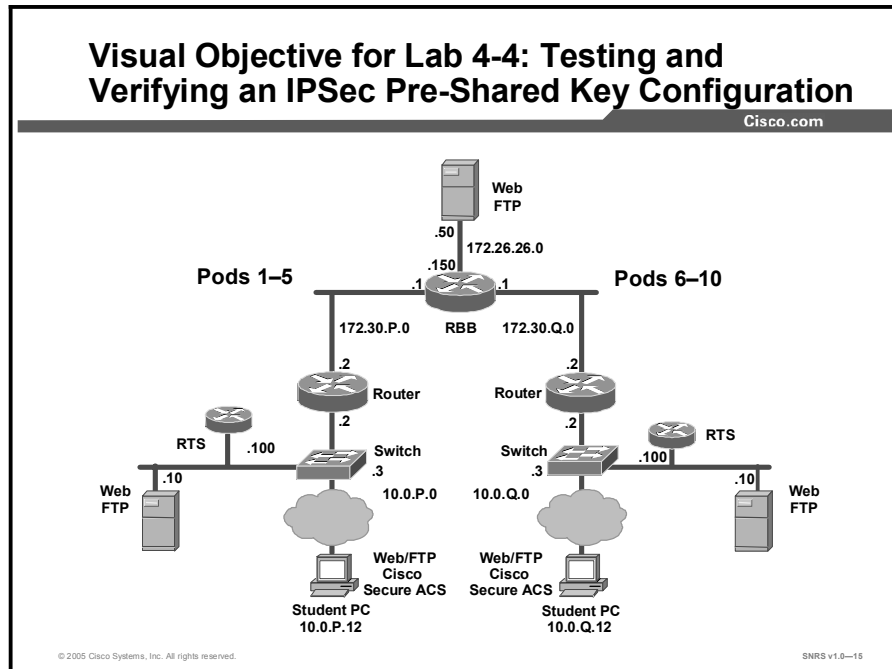
## Activity Objective

In this activity, you will verify the IPSec configuration. After completing this activity, you will be able to meet these objectives:

- Display ISAKMP policies
- Display transform sets
- Display crypto maps
- Display the current state of IPSec SAs
- Clear any existing SAs
- Enable debug output for IPSec events
- Enable debug output for ISAKMP events
- Observe debug output with console logging
- Observe the ISAKMP and IPSec debug output
- Verify ISAKMP and IPSec SAs
- Ensure that encryption is working between routers

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                                                                                                  | Description                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clear crypto isakmp</code><br>[ <i>connection-id</i> ]                                                                                                                                                             | To clear active IKE connections, use the <b>clear crypto isakmp</b> command in EXEC mode.                                                                                                                                                         |
| <code>clear crypto sa</code>                                                                                                                                                                                             | To delete IPsec SAs, use the <b>clear crypto sa</b> command in EXEC mode.                                                                                                                                                                         |
| <code>debug crypto ipsec</code>                                                                                                                                                                                          | To display IPsec events, use the <b>debug crypto ipsec</b> command in privileged EXEC mode. To disable debugging output, use the <b>no</b> form of this command.                                                                                  |
| <code>debug crypto isakmp aaa</code>                                                                                                                                                                                     | To display messages about IKE events, use the <b>debug crypto isakmp</b> command in privileged EXEC mode. To disable debugging output, use the <b>no</b> form of this command.                                                                    |
| <code>logging console</code> [ <i>severity-level</i> ]                                                                                                                                                                   | To send syslog messages to all available TTY lines and limit messages based on severity, use the <b>logging console</b> command in global configuration mode. To disable logging to the console terminal, use the <b>no</b> form of this command. |
| <code>ping</code> [ <i>protocol</i> ] [ <i>tag</i> ]<br>{ <i>host-name</i>   <i>system-address</i> }                                                                                                                     | To diagnose basic network connectivity on AppleTalk, ATM, CLNS, DECnet, IP, Novell IPX, or SRB networks, use the <b>ping</b> command in EXEC mode.                                                                                                |
| <code>show crypto ipsec sa</code> [ <i>map map-name</i>   <i>address</i>   <i>identity</i>   <i>interface interface</i> / <i>peer</i> [ <i>vrf fvrf-name</i> ] <i>address</i>   <i>vrf ivrf-name</i> ] [ <i>detail</i> ] | To display the settings used by current SAs, use the <b>show crypto ipsec sa</b> command in EXEC mode.                                                                                                                                            |
| <code>show crypto ipsec transform-set</code> [ <i>tag transform-set-name</i> ]                                                                                                                                           | To display the configured transform sets, use the <b>show crypto ipsec transform-set</b> command in EXEC mode.                                                                                                                                    |
| <code>show crypto isakmp sa</code>                                                                                                                                                                                       | To display all current IKE SAs at a peer, use the <b>show crypto isakmp sa</b> command in EXEC mode.                                                                                                                                              |
| <code>show crypto map</code> [ <i>interface interface</i>   <i>tag map-name</i> ]                                                                                                                                        | To display the crypto map configuration, use the <b>show crypto map</b> command in EXEC mode.                                                                                                                                                     |
| <code>show logging</code> [ <i>slot slot-number</i>   <i>summary</i> ]                                                                                                                                                   | To display the state of syslog and the contents of the standard system logging message buffer, use the <b>show logging</b> command in privileged EXEC mode.                                                                                       |

## Job Aids

There are no job aids for this activity.

## Task 1: Display ISAKMP Policies

You will display your configured ISAKMP policies.

### Activity Procedure

Complete this step:

**Step 1** Display your configured ISAKMP policies:

```
R2#show crypto isakmp policy
Global IKE 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
```

### Activity Verification

You have completed this task when you attain these results:

- Your output is similar to the output in Step 1.

## Task 2: Display Transform Sets

You will display your configured transform sets.

### Activity Procedure

Complete this step:

**Step 1** Display your configured transform sets:

```
router# show crypto ipsec transform-set
Transform set MINE: { esp-des }
will negotiate = { Tunnel, },
```

### Activity Verification

You have completed this task when you attain these results:

- Your results should be similar to the output in Step 1.

## Task 3: Display Crypto Maps

You will display your configured crypto maps.

### Activity Procedure

Complete this step:

**Step 1** Display your configured crypto maps:

```
R2#sh crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
 Peer = 172.30.7.2
 Extended IP access list 102
 access-list 102 permit ip host 172.30.2.2 host
 172.30.7.2
 Current peer: 172.30.7.2
 Security association lifetime: 4608000 kilobytes/3600
 seconds
 PFS (Y/N): N
 Transform sets={
 MINE,
 }
 Interfaces using crypto map MYMAP:
 FastEthernet0/1
```

### Activity Verification

You have completed this task when you attain these results:

- Your **show crypto map** output is similar to the output in Step 1.

## Task 4: Display the Current State of IPSec SAs

You will display the current state of your IPSec SAs.

### Activity Procedure

Complete this step:

- Step 1** 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:

```
R2#sh crypto ipsec sa

interface: FastEthernet0/1
 Crypto map tag: MYMAP, local addr 172.30.2.2
 protected vrf: (none)
 local ident (addr/mask/prot/port):
(172.30.2.2/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port):
(172.30.7.2/255.255.255.255/0/0)
 current_peer 172.30.7.2 port 500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

 local crypto endpt.: 172.30.2.2, remote crypto endpt.:
172.30.7.2
 path mtu 1500, ip mtu 1500
 current outbound spi: 0x0(0)

 inbound esp sas:

 inbound ah sas:

 inbound pcp sas:

 outbound esp sas:

 outbound ah sas:
```

```
outbound pcp sas:
```

### Activity Verification

You have completed this task when you attain these results:

- Your **show crypto ipsec sa** command output is similar to the example in Step 1.

## Task 5: Clear Existing SAs

You will clear any existing SAs.

### Activity Procedure

Complete this step:

- Step 1** Clear any existing SAs:

```
router# clear crypto sa
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show crypto ipsec sa** and **show crypto isakmp sa** command. Verify that the packet counts are now zero (0).

## Task 6: Enable Debug Output for IPsec Events

You will enable debug output for IPsec events.

### Activity Procedure

Complete this step:

- Step 1** Enable debug output for IPsec events:

```
router# debug crypto ipsec
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show debug** command to show any debugging applied.

## Task 7: Enable Debug Output for ISAKMP Events

You will enable debug output for ISAKMP events.

### Activity Procedure

Complete this step:

- Step 1** Enable debug output for ISAKMP events:

```
router# debug crypto isakmp
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show debug** command to show any debugging applied.

## Task 8: Observe Debug Output with Console Logging

You will observe debug output with console logging.

### Activity Procedure

Complete this step:

- Step 1** Turn on console logging so that you can see the debug output:

```
router(config)# logging console
```

### Activity Verification

You have completed this task when you attain these results:

- Perform a **show logging** command and observe that console logging is enabled.

## Task 9: Observe the ISAKMP and IPSec Debug Output

You will observe the ISAKMP and IPSec debug output by pinging your peer pod perimeter router.

### Activity Procedure

Complete this step:

- Step 1** Initiate a ping to the perimeter router of your peer pod. Observe the ISAKMP and IPSec debug output:

```
router# ping 172.30.Q.2
(where Q = peer pod number)
```

### Activity Verification

You have completed this task when you attain these results:

- Your ping is successful.

## Task 10: Verify ISAKMP and IPsec SAs

You will verify ISAKMP and IPsec SAs.

### Activity Procedure

Complete these steps:

**Step 1** Verify ISAKMP SAs:

```
R2#sh crypto isakmp sa
dst src state conn-id slot
status
172.30.7.2 172.30.2.2 QM_IDLE 1 0
ACTIVE
```

**Step 2** Verify IPsec SAs. Note the number of packets encrypted and decrypted when viewing the IPsec SAs:

```
R2#sh crypto ipsec sa

interface: FastEthernet0/1
 Crypto map tag: MYMAP, local addr 172.30.2.2

 protected vrf: (none)
 local ident (addr/mask/prot/port):
(172.30.2.2/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port):
(172.30.7.2/255.255.255.255/0/0)
 current_peer 172.30.7.2 port 500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0

 local crypto endpt.: 172.30.2.2, remote crypto endpt.:
172.30.7.2
 path mtu 1500, ip mtu 1500
 current outbound spi: 0x5FAA1A55(1604983381)

 inbound esp sas:
 spi: 0x2831CBC6(674352070)
 transform: esp-des ,
 in use settings = {Tunnel, }
```



```

conn id: 2001, flow_id: 1, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec):
(4511705/3537)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x5FAA1A55(1604983381)
transform: esp-des ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: 2, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec):
(4511705/3524)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

### Activity Verification

You have completed this task when you attain these results:

- Note the SPIs in the output. The output of your **show** commands should be similar to the examples in Steps 1 and 2.

## Task 11: Ensure That Encryption Is Working Between Routers

You will generate additional traffic to ensure that encryption is working between the routers.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that encryption is working between routers by first generating additional traffic:

```

router# ping 172.30.Q.2
(where Q = peer pod number)

```

**Step 2** Observe that the packets encrypted and decrypted counter has incremented:

```
router# 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:
```

### Activity Verification

You have completed this task when you attain these results:

- You note the increase in packet counts.

## **Lab 4-4 Answer Key: Testing and Verifying an IPSec Pre-Shared Key Configuration**

There is no Answer Key for this activity.



## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                      | Description                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clock set hh:mm:ss day month year</code>                                                                                               | To manually set the system software clock, use one of the formats of the <b>clock set</b> command in privileged EXEC mode.                                                                                  |
| <code>clock timezone zone hours-offset [minutes-offset]</code>                                                                               | To set the time zone for display purposes, use the <b>clock timezone</b> command in global configuration mode. To set the time to Coordinated Universal Time (UTC), use the <b>no</b> form of this command. |
| <code>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [dhcp] [distance] [name] [permanent] [tag tag]</code> | To establish static routes, use the <b>ip route</b> command in global configuration mode. To remove static routes, use the <b>no</b> form of this command.                                                  |
| <code>ping [protocol] [tag] {host-name   system-address}</code>                                                                              | To diagnose basic network connectivity on AppleTalk, ATM, CLNS, DECnet, IP, Novell IPX, or SRB networks, use the <b>ping</b> command in EXEC mode.                                                          |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will complete the lab exercise setup by setting the correct time and date on the server, resetting router defaults, ensuring connectivity with other routers in the lab, and building a static route.

### Activity Procedure

Complete these steps:

- 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 console port.
- Step 4** Reset your router to the default configuration.
- Step 5** Ensure that you can ping from your router to the router of your peer pod.
- Step 6** Ensure that you can ping from your Windows 2000 Server to the peer pod Windows 2000 Server.
- Step 7** Build a static route to the 172.26.26.0/24 network:

```
router(config)# ip route 172.26.26.0 255.255.255.0 172.30.P.1
(where P = pod number)
```

## Activity Verification

You have completed this task when you attain these results:

- You can ping the 172.26.26.51 address (CA server).

## Task 2: Prepare for Configuring IPSec

You will prepare for configuring IPSec by determining the ISAKMP and IPSec policy; verifying the time zone, calendar, and time on the router; verifying connectivity with the other routers and the CA server; establishing an HTTP session to the CA server; and turning on console logging to view the debug outputs.

### Activity Procedure

Complete these steps:

**Step 1** Determine the ISAKMP and IPSec policy. In this lab exercise, you will use default values except when you are directed to enter a specific value:

- The ISAKMP policy is to use RSA signature keys.
- The IPSec policy is to use ESP mode with DES.
- The IPSec policy is to encrypt all traffic between perimeter routers.

**Step 2** Set the router time zone:

```
router(config)# clock timezone zone hours [minutes]
```

**Step 3** Set the router calendar and time:

```
router# clock set hh:mm:ss day month year
```

**Step 4** Verify that you have connectivity with the peer pod router:

```
router# ping 172.30.Q.2
```

(where Q = peer pod number)

**Step 5** Ensure that you can connect to the CA server from your router:

```
router# ping 172.26.26.51
```

**Step 6** 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 7** Turn on console logging to view the debug output:

```
router# config terminal
```

```
router(config)# logging console
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh clock** command. The output should be similar to this:

```
R2#sh clock
```

```
18:14:24.007 CST Mon Mar 7 2005
```

## **Lab 5-1 Answer Key: Preparing the Network for IPSec Configuration Using Digital Certificates**

There is no Answer Key for this activity.

# Lab 5-2: Configuring Certificate Authority on Cisco Routers

Complete this lab activity to practice what you learned in the related module.

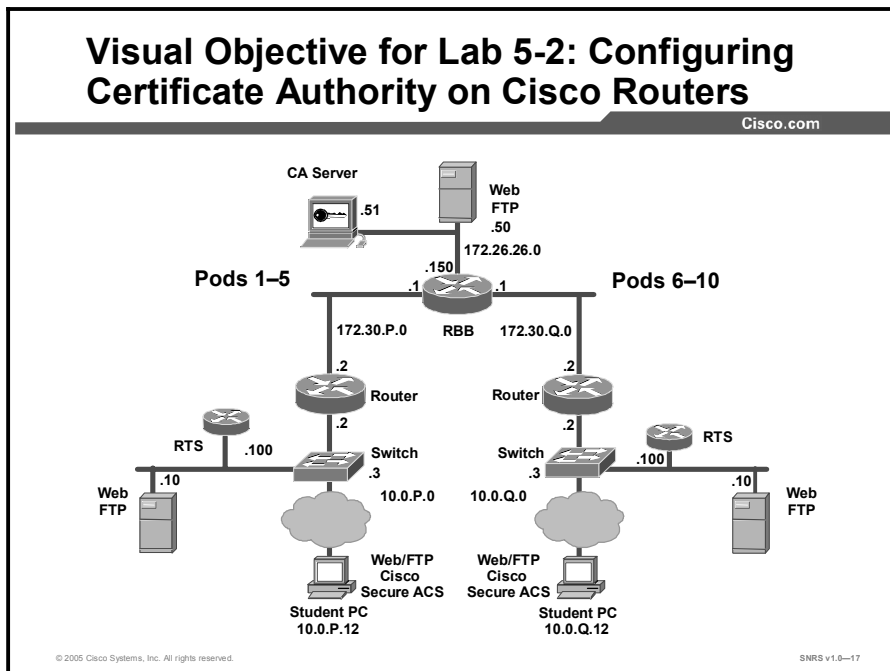
## Activity Objective

In this activity, you will configure CA support on a Cisco router. After completing this activity, you will be able to meet these objectives:

- Define the router domain name
- Define host name-to-IP address mapping
- Generate RSA usage keys
- Configure the CA server trustpoint

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.



## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                 | Description                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>crl optional</code>                                                                                                               | To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the <b>crl optional</b> command in CA identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the <b>no</b> form of this command. |
| <code>crypto ca authenticate<br/>name</code>                                                                                            | To authenticate the CA (by getting the certificate of the CA), use the <b>crypto ca authenticate</b> command in global configuration mode.                                                                                                                                                                                             |
| <code>crypto ca enroll name</code>                                                                                                      | To obtain the certificate or certificates of your router from the CA, use the <b>crypto ca enroll</b> command in global configuration mode. To delete a current enrollment request, use the <b>no</b> form of this command.                                                                                                            |
| <code>crypto ca trustpoint name</code>                                                                                                  | To declare the CA that your router should use, use the <b>crypto ca trustpoint</b> command in global configuration mode. To delete all identity information and certificates associated with the CA, use the <b>no</b> form of this command.                                                                                           |
| <code>crypto key generate rsa<br/>{general-keys   usage-<br/>keys} [label key-label]<br/>[exportable]<br/>[modulus modulus-size]</code> | To generate RSA key pairs, use the <b>crypto key generate rsa</b> command in global configuration mode.                                                                                                                                                                                                                                |
| <code>debug crypto pki messages</code>                                                                                                  | To display debugging messages for the details of the interaction (message dump) between the CA and the router, use the <b>debug crypto pki messages</b> command in privileged EXEC mode. To disable debugging output, use the <b>no</b> form of this command.                                                                          |
| <code>enrollment [mode] [retry<br/>period minutes] [retry<br/>count number] url url<br/>[pem]</code>                                    | To specify the enrollment parameters of a CA, use the <b>enrollment</b> command in CA trustpoint configuration mode. To remove any of the configured parameters, use the <b>no</b> form of this command.                                                                                                                               |
| <code>ip host {name   tmodem-<br/>telephone-number} [tcp-<br/>port-number] {address1<br/>[address2...address8]}</code>                  | To define a static host name-to-address mapping in the host cache, use the <b>ip host</b> command in global configuration mode. To remove the host name-to-address mapping, use the <b>no</b> form of this command.                                                                                                                    |
| <code>show crypto ca<br/>certificates</code>                                                                                            | To display information about your certificate, the CA certificate, and any RA certificates, use the <b>show crypto ca certificates</b> command in EXEC mode.                                                                                                                                                                           |

## Job Aids

There are no job aids for this activity.

## Task 1: Define the Router Domain Name

You will define the router domain name.

### Activity Procedure

Complete this step:

**Step 1** Define the router domain name:

```
router(config)# ip domain-name cisco.com
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show run** command.

## Task 2: Define Host Name-to-IP Address Mapping

You will define the CA server static host name-to-IP address mapping.

### Activity Procedure

Complete these steps:

**Step 1** Define the CA server static host name-to-IP address mapping:

```
router(config)# ip host VPNCA 172.26.26.51
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **sh run** command. The output should contain the following:

```
!
ip domain name cisco.com
ip host VPNCA 172.26.26.51
!
```

## Task 3: Generate RSA Usage Keys

You will generate RSA usage keys.

### Activity Procedure

Complete these steps:

**Step 1** Generate RSA usage keys:

```
router(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.

---

## Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto key mypubkey rsa** command. The output should be similar to this:

```
R2#sh crypto key mypubkey rsa
% Key pair was generated at: 08:27:16 CST Mar 8 2005
Key name: R2.cisco.com
Usage: Signature Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D589C9 E077B874
 4E659CA9 8AFB7BCB 1AFB5534 6AFF4207 0B575271 543AC147 C34383AC F68FA0B0
 65153A9F 56725C8E D0BD5AA4 BB38A91D 3F10EC8D 8209FCB3 71020301 0001
% Key pair was generated at: 08:27:18 CST Mar 8 2005
Key name: R2.cisco.com
Usage: Encryption Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B732F0 6AE5F0A5
 0DAA23D7 86595EE0 A2ECD9B9 EEF0079E 8878DEC7 6F12F304 0F1D0FA8 E3313317
 ECD5521C F82962F5 41903C39 BC26A362 C03D8221 CEE2A7A6 A1020301 0001
% Key pair was generated at: 08:27:27 CST Mar 8 2005
Key name: R2.cisco.com.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AFBE5F 651AE624
 F220E6BD 473A6643 9D24644E 5034F6EF D9B1DB4F E96DCB48 727997ED 46DFC45E
 2FAE67C0 78A82788 D4A27D12 A96E472B D178A7A9 9A23E3E8 60275C72 56603867
 0DF75F9E A682F959 14AA0E1E EB4D49BA 41A2D002 33CA2A1C AD020301 0001
```

## Task 4: Configure the CA Server Trustpoint

You will configure the CA server trustpoint.

### Activity Procedure

Complete these steps:

**Step 1** Complete the following substeps to configure the CA server trustpoint:

1. Create a name for the CA and enter CA trustpoint mode:

```
router(config)# crypto ca trustpoint vpnca
```

2. Choose the RA mode:

```
router(ca-trustpoint)# enrollment mode ra
```

3. Specify the URL of the CA:

- For an Entrust CA:

```
router(ca-trustpoint)# enrollment url http://vpnca
```

- For a Microsoft CA:

```
router(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.

---

**Step 2** Exit CA configuration mode:

```
router(ca-trustpoint)# ^z
router# copy running-config startup-config
```

**Step 3** Complete the following substeps to turn on PKI debugging so that you can observe debug messages for the CA process:

```
router# debug crypto pki messages
router# debug crypto pki transactions
```

**Step 4** Authenticate the CA server. Verify the fingerprint of the CA server with the CA administrator:

```
router# config term
router(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.

---

**Step 5** 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.

---

**Note** Stop and ensure that the instructor is ready to accept your enrollment request before continuing to the next step.

---

```
router(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 fully-qualified domain name in the certificate will be:
R2.cisco.com
% The subject name in the certificate will be: R2.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.
```

**Step 6** Verify the CA certificates:

```
router(config)# exit
router# copy running-config startup-config
router# show crypto ca certificate
```

## Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto ca certificates** command. The output should be similar to this:

```
R2#sh crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number: 02
 Certificate Usage: Signature
 Issuer:
 cn=securcs
 Subject:
```

Name: R2.cisco.com  
hostname=R2.cisco.com  
Validity Date:  
start date: 08:49:41 CST Mar 8 2005  
end date: 08:49:41 CST Mar 8 2006  
Associated Trustpoints: vpnca

CA Certificate

Status: Available  
Certificate Serial Number: 01  
Certificate Usage: Signature  
Issuer:  
cn=securcs  
Subject:  
cn=securcs  
Validity Date:  
start date: 08:38:30 CST Mar 8 2005  
end date: 08:38:30 CST Mar 7 2008  
Associated Trustpoints: vpnca

Certificate

Subject:  
Name: R2.cisco.com  
Status: Pending  
Key Usage: Encryption  
Certificate Request Fingerprint MD5: 697A69E3 0034C566 254CBE9E  
3183E37A  
Certificate Request Fingerprint SHA1: 708FB45A 82CD944E 795C138C  
832988BF 93B

C43B2

Associated Trustpoint: vpnca

## **Lab 5-2 Answer Key: Configuring Certificate Authority on Cisco Routers**

There is no Answer Key for this activity.

# Lab 5-3: Configuring ISAKMP and IPsec on Cisco Routers

Complete this lab activity to practice what you learned in the related module.

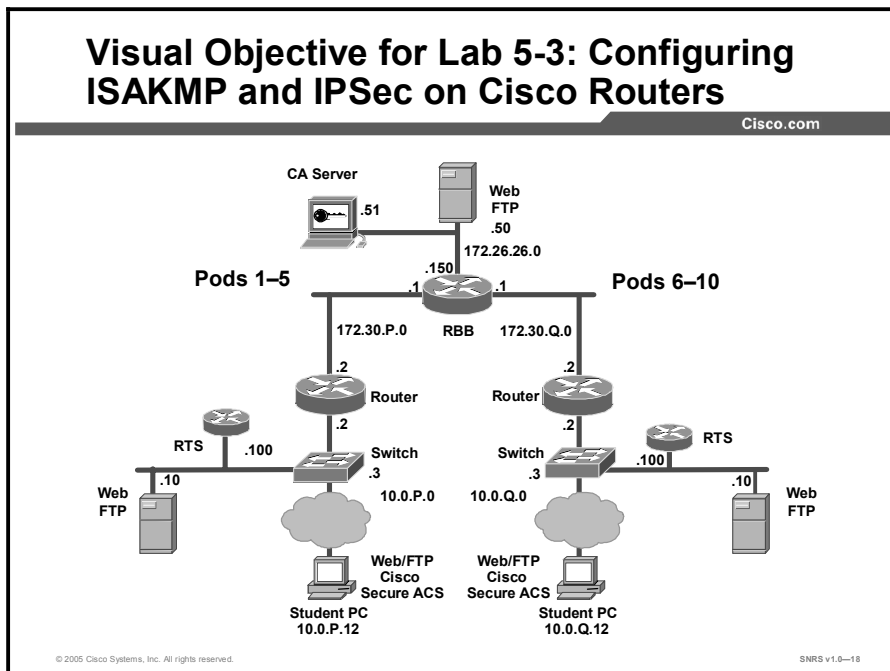
## Activity Objective

In this activity, you will configure ISAKMP and IPsec on Cisco routers. After completing this activity, you will be able to meet these objectives:

- Enable ISAKMP on a Cisco router
- Create an ISAKMP policy to use RSA signatures
- Configure a transform set
- Configure a crypto ACL
- Configure a crypto map
- Apply the crypto map to an interface

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.



## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                  | Description                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>authentication {rsa-sig  <br/>rsa-encr   pre-share}</code>                                                         | To specify the authentication method within an IKE policy, use the <b>authentication</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the <b>no</b> form of this command.            |
| <code>crypto ipsec transform-set<br/>transform-set-name<br/>transform1 [transform2]<br/>[transform3] [transform4]</code> | To define a transform set—an acceptable combination of security protocols and algorithms—use the <b>crypto ipsec transform-set</b> command in global configuration mode. To delete a transform set, use the <b>no</b> form of this command.                                                                                  |
| <code>crypto isakmp enable</code>                                                                                        | To globally enable IKE at your peer router, use the <b>crypto isakmp enable</b> command in global configuration mode. To disable IKE at the peer, use the <b>no</b> form of this command.                                                                                                                                    |
| <code>crypto isakmp policy<br/>priority</code>                                                                           | To define an IKE policy, use the <b>crypto isakmp policy</b> command in global configuration mode. IKE policies define a set of parameters to be used during the IKE negotiation. To delete an IKE policy, use the <b>no</b> form of this command.                                                                           |
| <code>encryption {des   3des  <br/>aes   aes 192   aes 256}</code>                                                       | To specify the encryption algorithm within an IKE policy, use the <b>encryption</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the <b>no</b> form of this command.                  |
| <code>group {1   2}</code>                                                                                               | To specify the Diffie-Hellman group identifier within an IKE policy, use the <b>group</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the <b>no</b> form of this command. |
| <code>hash {sha   md5}</code>                                                                                            | To specify the hash algorithm within an IKE policy, use the <b>hash</b> command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default SHA-1 hash algorithm, use the <b>no</b> form of this command.                     |
| <code>lifetime seconds</code>                                                                                            | To specify the lifetime of an IKE SA, use the <b>lifetime</b> command in ISAKMP policy configuration mode. To reset the SA lifetime to the default value, use the <b>no</b> form of this command.                                                                                                                            |
| <code>show crypto ipsec<br/>transform-set [tag<br/>transform-set-name]</code>                                            | To display the configured transform sets, use the <b>show crypto ipsec transform-set</b> command in EXEC mode.                                                                                                                                                                                                               |
| <code>show crypto isakmp policy</code>                                                                                   | To display the parameters for each IKE policy, use the <b>show crypto isakmp policy</b> command in EXEC mode.                                                                                                                                                                                                                |

## Job Aids

There are no job aids for this activity.

## Task 1: Enable ISAKMP

You will enable IKE/ISAKMP on a Cisco router. Work with the members of your peer pod.

### Activity Procedure

Complete these steps:

**Step 1** Verify that ISAKMP is enabled:

```
router# show crypto isakmp policy
```

---

**Note** If you see the message "ISAKMP is turned off," then complete Step 2.

---

**Step 2** Enable IKE/ISAKMP on your router:

```
router(config)# crypto isakmp enable
router(config)# exit
```

### Activity Verification

You have completed this task when you attain these results:

■ Issue a **show crypto isakmp policy**. The output should be similar to this:

```
R2#sh crypto isakmp policy
Global IKE 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
```

## Task 2: Create an ISAKMP Policy to Use RSA Signatures

You will create an IKE policy to use RSA signatures.

### Activity Procedure

Complete these steps:

- Step 1** Set the policy priority:
- ```
router(config)# crypto isakmp policy 110
```
- Step 2** Set authentication to use RSA signatures:
- ```
router(config-isakmp)# authentication rsa-sig
```
- Step 3** Set the IKE encryption:
- ```
router(config-isakmp)# encryption des
```
- Step 4** Set the Diffie-Hellman group:
- ```
router(config-isakmp)# group 1
```
- Step 5** Set the hash algorithm:
- ```
router(config-isakmp)# hash md5
```
- Step 6** Set the IKE SA lifetime:
- ```
router(config-isakmp)# lifetime 86400
```
- Step 7** Exit ISAKMP policy configuration mode:
- ```
router(config-isakmp)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **show crypto isakmp policy** command. The output should be similar to this:

```
R2#sh crypto isakmp policy
Global IKE 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 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-Adleman Signature
  Diffie-Hellman group:  #1 (768 bit)
  lifetime:              86400 seconds, no volume limit
```

Task 3: Configure a Transform Set

You will configure a transform set and SA parameters.

Activity Procedure

Complete these steps:

Step 1 Ensure that you are in configuration mode:

```
router# config terminal
```

Step 2 View the available crypto IPsec command options:

```
router(config)# crypto ipsec ?
```

Step 3 Check your transform set options:

```
router(config)# crypto ipsec transform-set ?
```

Step 4 Define a transform set. Use the following parameters:

- Transform name = **MINE**
- ESP protocols = **des**
- Mode = **tunnel**

```
router(config)# crypto ipsec transform-set MINE esp-des
```

Step 5 Set the mode to tunnel:

```
router(cfg-crypto-trans)# mode tunnel
```

Step 6 Exit configuration mode:

```
router(cfg-crypto-trans)# ^Z
```

Activity Verification

You have completed this task when you attain these results:

■ Issue a **sh crypto ipsec transform-set**. The output should be similar to this:

```
R2#show crypto ipsec transform-set MINE  
Transform set MINE: { esp-des }  
will negotiate = { Tunnel, },
```

Task 4: Configure a Crypto ACL

You will configure a crypto ACL. 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**
- ACL number = **102**
- Protocol = **IP**

Activity Procedure

Complete these steps:

Step 1 Ensure that you are in configuration mode:

```
router(config)# config terminal
```

Step 2 Configure the ACL:

```
router(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)

Activity Verification

You have completed this task when you attain these results:

■ Issue a **sh access-list** command. The output should be similar to this:

```
R2#sh access-lists  
Extended IP access list 102  
10 permit ip host 172.30.2.2 host 172.30.7.2
```

Task 5: Configure a Crypto Map

You will 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**

Activity Procedure

Complete these steps:

Step 1 Set the name of the map, the map number, and the type of key exchange to be used:

```
router(config)# crypto map MYMAP 10 ipsec-isakmp
```

Step 2 Specify the extended ACL to use with this map:

```
router(config-crypto-map)# match address 102
```

Step 3 Specify the transform-set that you defined earlier:

```
router(config-crypto-map)# set transform-set MINE
```

Step 4 Assign the VPN peer using the host name or IP address of the peer:

```
router(config-crypto-map)# set peer 172.30.Q.2
```

(where Q = peer pod number)

Step 5 Exit crypto map configuration mode:

```
router(config-crypto-map)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto map** command. Check the configuration to make sure that it matches this example:

```
R2#sh crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
  Peer = 172.30.7.2
  Extended IP access list 102
    access-list 102 permit ip host 172.30.2.2 host 172.30.7.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    MINE,
  }
  Interfaces using crypto map MYMAP:
```

Task 6: Apply the Crypto Map to an Interface

You will apply the crypto map to an interface. Use the following parameters:

- Interface to configure = **fast 0/1**
- Crypto map to use = **MYMAP**

Activity Procedure

Complete these steps:

Step 1 Access interface configuration mode:

```
router(config)# interface fast 0/1
```

Step 2 Assign the crypto map to the interface:

```
router(config-if)# crypto map MYMAP
```

Step 3 Exit interface configuration mode:

```
router(config-if)# ^Z
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto map** command. The output should be similar to this:

```
R2#sh crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
  Peer = 172.30.7.2
  Extended IP access list 102
    access-list 102 permit ip host 172.30.2.2 host 172.30.7.2
  Current peer: 172.30.7.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    MINE,
  }
  Interfaces using crypto map MYMAP:
    FastEthernet0/1
```

Lab 5-3 Answer Key: Configuring ISAKMP and IPsec on Cisco Routers

There is no Answer Key for this activity.

Lab 5-4: Testing and Verifying the IPsec CA Configuration

Complete this lab activity to practice what you learned in the related module.

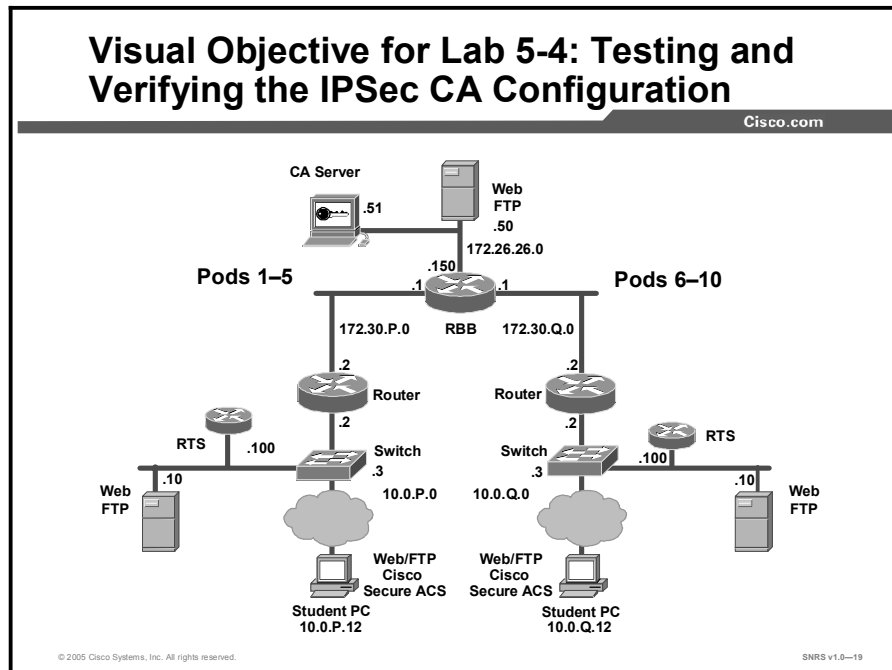
Activity Objective

In this activity, you will verify the IPsec configuration. After completing this activity, you will be able to meet these objectives:

- Display ISAKMP policies
- Display transform sets
- Display crypto maps
- Display the current state of IPsec SAs
- Clear any existing SAs
- Enable debug output for IPsec events
- Enable debug output for ISAKMP events
- Observe the ISAKMP and IPsec debug outputs
- Verify ISAKMP and IPsec SAs
- Ensure that encryption is working

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity .

Command List

The table describes the commands used in this activity.

Router Commands

Command	Description
<code>clear crypto sa</code>	To delete IPsec SAs, use the clear crypto sa command in EXEC mode.
<code>debug crypto ipsec</code>	To display IPsec events, use the debug crypto ipsec command in privileged EXEC mode. To disable debugging output, use the no form of this command.
<code>debug crypto isakmp aaa</code>	To display messages about IKE events, use the debug crypto isakmp command in privileged EXEC mode. To disable debugging output, use the no form of this command.
<code>show crypto ipsec sa [map map-name address identity interface interface / peer [vrf fvrf-name] address vrf ivrf-name] [detail]</code>	To display the settings used by current SAs, use the show crypto ipsec sa command in EXEC mode.
<code>show crypto ipsec transform-set [tag transform-set-name]</code>	To display the configured transform sets, use the show crypto ipsec transform-set command in EXEC mode.
<code>show crypto isakmp policy</code>	To display the parameters for each IKE policy, use the show crypto isakmp policy command in EXEC mode.
<code>show crypto isakmp sa</code>	To display all current IKE SAs at a peer, use the show crypto isakmp sa command in EXEC mode.
<code>show crypto map [interface interface tag map-name]</code>	To display the crypto map configuration, use the show crypto map command in EXEC mode.

Job Aids

There are no job aids for this activity.

Task 1: Display ISAKMP Policies

You will display configured ISAKMP policies.

Activity Procedure

Complete this step:

Step 1 Display your configured ISAKMP policies:

```
router# 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
```

Activity Verification

You have completed this task when you attain these results:

- The output should look similar to the output in Step 1. Compare the output with that of your peer pod.

Task 2: Display Transform Sets

You will display configured transform sets.

Activity Procedure

Complete this step:

Step 1 Display your configured transform sets:

```
router# show crypto ipsec transform-set
Transform set MINE: { esp-des  }
will negotiate = { Tunnel, },
```

Activity Verification

You have completed this task when you attain these results:

- The output should look similar to the output in Step 1. Compare the output with that of your peer pod.

Task 3: Display Crypto Maps

You will display configured crypto maps.

Activity Procedure

Complete this step:

- Step 1** Display your configured crypto maps (where P = pod number, and Q = peer pod number):

```
router# 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, }.
```

Activity Verification

You have completed this task when you attain these results:

- The output should look similar to the output in Step 1. Compare the output with that of your peer pod.

Task 4: Display the Current State of IPSec SAs

You will display the current state of IPSec SAs.

Activity Procedure

Complete this step:

- Step 1** Display the current state of your IPSec SAs (where P = pod number, and Q = peer pod number). IPSec SAs may have already been established by routing traffic.

```
router# 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:

```

Activity Verification

You have completed this task when you attain these results:

- The output should look similar to the output in Step 1. Compare the output with that of your peer pod.

Task 5: Clear Any Existing SAs

You will clear any existing SAs.

Activity Procedure

Complete this step:

- Step 1** Clear any existing SAs:

```
router# clear crypto sa
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto ipsec sa** command to determine whether your SAs have been cleared.

Task 6: Enable Debug Output for IPsec Events

You will enable debug output for IPsec events.

Activity Procedure

Complete this step:

Step 1 Enable debug output for IPsec events:

```
router# debug crypto ipsec
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh debug** command to see what debugging is enabled.

Task 7: Enable Debug Output for ISAKMP Events

You will enable debug output for ISAKMP events.

Activity Procedure

Complete this step:

Step 1 Enable debug output for ISAKMP events:

```
router# debug crypto isakmp
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh debug** command to see what debugging is enabled.

Task 8: Observe the ISAKMP and IPsec Debug Outputs

You will observe the ISAKMP and IPsec debug outputs by pinging the peer pod perimeter router.

Activity Procedure

Complete this step:

Step 1 Initiate a ping to the perimeter router of your peer pod. Observe the ISAKMP and IPsec debug output.

```
router# ping 172.30.Q.2
```

Activity Verification

You have completed this task when you attain these results:

- Your ping should be successful and you should see some debug output.

Task 9: Verify ISAKMP and IPsec SAs

You will verify ISAKMP and IPsec SAs.

Activity Procedure

Complete these steps:

Step 1 Verify ISAKMP SAs (where P = pod number, and Q = peer pod number):

```
router# show crypto isakmp sa
dst                src                state              conn-id  slot
172.30.Q.2        172.30.P.2        QM_IDLE           16      0
```

Step 2 Verify IPsec SAs (where P = pod number, and Q = peer pod number). Note the number of packets encrypted and decrypted when viewing the IPsec SAs.

```
router# 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:
```

Activity Verification

You have completed this task when you attain these results:

- Your output should be similar to the output in Steps 1 and 2.

Task 10: Ensure That Encryption Is Working

You will observe that the packets encrypted and decrypted counter has incremented by generating additional traffic.

Activity Procedure

Complete these steps:

- Step 1** Ensure that encryption is working between the routers by first generating additional traffic (where Q = peer pod number):

```
router# ping 172.30.Q.2
```

- Step 2** Then observe that the packets encrypted and decrypted counter has incremented (where P = pod number, and Q = peer pod number):

```
router# 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 Task 9 because of the encrypted traffic.

Activity Verification

You have completed this task when you attain these results:

- Your output should be similar to the output in Steps 1 and 2.

Lab 5-4 Answer Key: Testing and Verifying the IPsec CA Configuration

There is no Answer Key for this activity.

Lab 6-1: Configuring Remote Access Using Cisco Easy VPN

Complete this lab activity to practice what you learned in the related module.

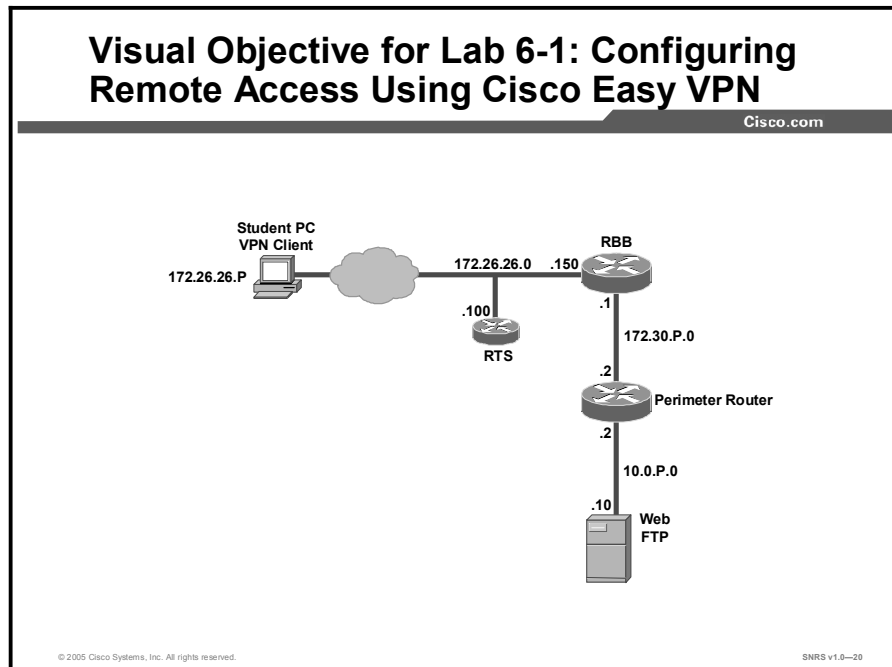
Activity Objective

In this activity, you will configure a Cisco Easy VPN Server using a Cisco 2600 Series router. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- Prepare a perimeter router for Cisco Easy VPN Server
- Enable policy lookup via AAA
- Create an ISAKMP policy for remote client access
- Define the group policy information for a mode configuration push
- Create a transform set
- Create a dynamic crypto map
- Apply mode configuration to the crypto map
- Apply the crypto map to the router interface
- Enable perimeter router dead peer detection

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

Command List

The table describes the commands used in this activity.

Router Commands

Command	Description
<code>aaa authorization {network exec commands level reverse-access configuration} {default list-name} method1 [method2...]</code>	To set parameters that restrict user access to a network, use the aaa authorization command in global configuration mode. To disable authorization for a function, use the no form of this command.
<code>aaa new-model</code>	To enable the AAA access control model, issue the aaa new-model command in global configuration mode. To disable the AAA access control model, use the no form of this command.
<code>authentication {rsa-sig rsa-encr pre-share}</code>	To specify the authentication method within an IKE policy, use the authentication command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the no form of this command.
<code>crypto dynamic-map dynamic-map-name dynamic-seq-num</code>	To create a dynamic crypto map entry and enter the crypto map configuration command mode, use the crypto dynamic-map command in global configuration mode. To delete a dynamic crypto map set or entry, use the no form of this command.
<code>crypto isakmp client configuration group {group-name default}</code>	To specify which group's policy profile will be defined, use the crypto isakmp client configuration group command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the no form of this command.
<code>crypto isakmp enable</code>	To globally enable IKE at your peer router, use the crypto isakmp enable command in global configuration mode.
<code>crypto isakmp keepalive secs [retries]</code>	To allow the gateway to send DPD messages to the peer, use the crypto isakmp keepalive command in global configuration mode. To disable keepalives, use the no form of this command.
<code>crypto isakmp key key-string address peer-address [mask] [no-xauth]</code>	To configure a pre-shared authentication key, use the crypto isakmp key command in global configuration mode.
<code>crypto isakmp policy priority</code>	To define an IKE policy, use the crypto isakmp policy command in global configuration mode. IKE policies define a set of parameters to be used during the IKE negotiation.
<code>domain name</code>	To specify the DNS domain to which a group belongs, use the domain command in ISAKMP group configuration mode. To remove this command from your configuration, use the no form of this command.

Command	Description
<code>encryption {des 3des aes aes 192 aes 256}</code>	To specify the encryption algorithm within an IKE policy, use the encryption command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the no form of this command.
<code>group {1 2}</code>	To specify the Diffie-Hellman group identifier within an IKE policy, use the group command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the no form of this command.
<code>hash {sha md5}</code>	To specify the hash algorithm within an IKE policy, use the hash command in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default SHA-1 hash algorithm, use the no form of this command.
<code>ip local pool {default poolname} [low-ip-address [high-ip-address]] [group group-name] [cache-size size]</code>	To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, use the ip local pool command in global configuration mode. To remove a range of addresses from a pool (the longer of the no forms of this command), or to delete an address pool (the shorter of the no forms of this command), use one of the no forms of this command.
<code>key name</code>	To specify the IKE pre-shared key for group policy attribute definition, use the key command in ISAKMP group configuration mode. To remove a pre-shared key, use the no form of this command.
<code>lifetime seconds</code>	To specify the lifetime of an IKE SA, use the lifetime command in ISAKMP policy configuration mode. To reset the SA lifetime to the default value, use the no form of this command.
<code>pool name</code>	To define a local pool address, use the pool command in ISAKMP group configuration mode. To remove a local pool from your configuration, use the no form of this command.
<code>reverse-route [remote-peer [ip-address]]</code>	To create source proxy information for a crypto map entry, use the reverse-route command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the no form of this command.
<code>set transform-set transform-set-name [transform-set-name2...transform-set-name6]</code>	To specify which transform sets can be used with the crypto map entry, use the set transform-set command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the no form of this command.
<code>show crypto isakmp policy</code>	To display the parameters for each IKE policy, use the show crypto isakmp policy command in EXEC mode.
<code>username name {nopassword password password password encryption-type encrypted-password}</code>	To establish a username-based authentication system, use the username command in global configuration mode.

Job Aids

There are no job aids for this activity.

Task 1: Complete the Lab Exercise Setup

You will set up the training pod equipment.

Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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) and that port is on **VLAN 1**.
- 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.

Activity Verification

You have completed this task when you attain these results:

- You are able to ping the other hosts.

Task 2: Prepare a Perimeter Router for Cisco Easy VPN Server

You will prepare the perimeter router for use as a Cisco Easy VPN Server.

Activity Procedure

Complete these steps:

Note This lab exercise assumes that your perimeter router has been returned to the default rP.config (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**:

```
router(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:

```
router(config)# username cisco password 0 cisco
```

Note The **aaa new-model** command (used in Task 3) causes the local username and password on the router to be used in the absence of other AAA statements. It is important to create a known local username and password combination to prevent you from being locked out of the router.

Activity Verification

You have completed this task when you attain these results:

- Check the configuration file.

Task 3: Enable Policy Lookup via AAA

You will enable policy lookup via AAA. Complete this procedure for your perimeter router beginning in global configuration mode to enable policy lookup via AAA.

Activity Procedure

Complete these steps:

- Step 1** Enable AAA using the **aaa new-model** command:

Note Ensure that you have completed Task 2 before entering this command.

```
router(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:

```
router(config)# aaa authorization network VPN-REMOTE-ACCESS
local
```

Activity Verification

You have completed this task when you attain these results:

- Check the configuration file.

Task 4: Create an ISAKMP Policy for Remote Client Access

You will create a new ISAKMP policy for remote client access on the perimeter router.

Activity Procedure

Complete these steps:

- Step 1** Enable ISAKMP:
- ```
router(config)# crypto isakmp enable
```
- Step 2** Create ISAKMP policy 1:
- ```
router(config)# crypto isakmp policy 1
```
- Step 3** Configure ISAKMP policy 1 to use pre-shared keys for authentication:
- ```
router(config-isakmp)# authentication pre-share
```
- Step 4** Configure ISAKMP policy 1 to use 3-DES encryption:
- ```
router(config-isakmp)# encryption 3des
```
- Step 5** Configure ISAKMP policy 1 to use Diffie-Hellman group 2:
- ```
router(config-isakmp)# group 2
```
- Step 6** Return to global configuration mode:
- ```
router(config-isakmp)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto isakmp policy** command. The output should be similar to this:

```
R2#sh crypto isakmp policy
Global IKE policy
Protection suite of priority 1
  encryption algorithm:  Three key triple DES
  hash algorithm:        Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group:  #2 (1024 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 5: Define Group Policy Information for a Mode Configuration Push

You will define the policy attributes that are pushed to the VPN client via mode configuration.

Activity Procedure

Complete these steps:

- Step 1** Specify which group's policy profile will be defined and enter ISAKMP group configuration mode. If no specific group matches and if 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:

```
router(config)# crypto isakmp client configuration group VPN-REMOTE-ACCESS
```

- Step 2** Specify the ISAKMP 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:

```
router(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**:

```
router(config-isakmp-group)# domain cisco.com
```

- Step 4** Choose 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:

```
router(config-isakmp-group)# pool REMOTE-POOL
```

- Step 5** Return to global configuration mode:

```
router(config-isakmp-group)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Check the configuration file.

Task 6: Create a Transform Set

You will create a transform set named VPNTRANSFORM

Activity Procedure

Complete these steps:

- Step 1** Create a transform set:

```
router(config)# crypto ipsec transform-set VPNTRANSFORM esp-3des esp-sha-hmac
```

- Step 2** Return to global configuration mode:

```
router(cfg-crypto-trans)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto ipsec transform-set** command. The output should be similar to this:

```
R2#sh crypto ipsec transform-set
Transform set VPNTRANSFORM: { esp-3des esp-sha-hmac  }
will negotiate = { Tunnel,  },
```

Task 7: Create a Dynamic Crypto Map

You will create dynamic crypto map to handle remote access traffic for the perimeter router.

Activity Procedure

Complete these steps:

- Step 1** Create dynamic crypto map, DYNMAP, and enter the crypto map configuration mode:

```
router(config)# crypto dynamic-map DYNMAP 1
```

- Step 2** Assign a transform set to DYNMAP:

```
router(config-crypto-map)# set transform-set VPNTRANSFORM
```

- Step 3** Enable RRI for the DYNMAP crypto map:

```
router(config-crypto-map)# reverse-route
```

- Step 4** Return to global configuration mode:

```
router(config-crypto-map)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto dynamic-map** command. The output should be similar to this:

```
R2#sh crypto dynamic-map
Crypto Map Template"DYNMAP" 1
  No matching address list set.
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    VPNTRANSFORM,
  }
```

Task 8: Apply Mode Configuration to the Crypto Map

You will apply mode configuration to a crypto map. Mode configuration must be applied to a crypto map to be enforced. Use the commands shown in the step list in global configuration mode to apply mode configuration to a crypto map.

Activity Procedure

Complete these steps:

- 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 3.x version Cisco VPN Clients.

```
router(config)# crypto map CLIENTMAP client configuration
address respond
```

- Step 2** Enable ISAKMP 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.

```
router(config)# crypto map CLIENTMAP isakmp authorization list
VPN-REMOTE-ACCESS
```

- Step 3** Apply the dynamic crypto map to the crypto map:

```
router(config)# crypto map CLIENTMAP 65535 ipsec-isakmp
dynamic DYNMAP
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto map** command. The output should be similar to this:

```
R2#sh crypto map
Crypto Map "CLIENTMAP" 65535 ipsec-isakmp
    Dynamic map template tag: DYNMAP
    Interfaces using crypto map CLIENTMAP:
```

Task 9: Apply the Crypto Map to the Router Interface

You will apply the crypto map to the outside interface of the perimeter router.

Activity Procedure

Complete these steps:

- Step 1** Enter interface configuration mode:

```
router(config)# interface fast 0/1
```

- Step 2** Assign the CLIENTMAP crypto map to the interface:

```
router(config-if)# crypto map CLIENTMAP
```

- Step 3** Return to global configuration mode:

```
router(config-if)# exit
```

Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto map** command. The output should be similar to this:

```
R2#sh crypto map
Crypto Map "CLIENTMAP" 65535 ipsec-isakmp
      Dynamic map template tag: DYNMAP
      Interfaces using crypto map CLIENTMAP:
          FastEthernet0/1
```

Task 10: Enable Perimeter Router Dead Peer Detection

You will enable DPD for the perimeter router.

Activity Procedure

Complete these steps:

- 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):

```
router(config)# crypto isakmp keepalive 20 10
```

- Step 2** Exit global configuration mode:

```
router(config)# exit
```

- Step 3** Save the router configuration:

```
router# copy run start
```

Activity Verification

You have completed this task when you attain these results:

- Issue the **show run** command. Your configuration should look similar to the following:

```
router#show run
Current configuration : 1826 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot system flash c2600-advsecurityk9-mz.123-11.T2.bin
boot-end-marker
```

```

!
logging buffered 51200 warnings
no logging console
enable secret 5 $1$BQUd$B/vVMntN0Yp7V7Ra9crBY/
!
username cisco password 0 cisco
memory-size iomem 10
clock timezone CST -6
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
aaa authorization network VPN-REMOTE-ACCESS local
aaa session-id common
ip subnet-zero
ip cef
!
ip ips po max-events 100
no ftp-server write-enable
!
!
!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 VPNTRANSFORM esp-3des esp-sha-hmac
!
crypto dynamic-map DYNMAP 1
  set transform-set VPNTRANSFORM
  reverse-route
!
crypto map CLIENTMAP isakmp authorization list VPN-REMOTE-ACCESS
crypto map CLIENTMAP client configuration address respond
crypto map CLIENTMAP 65535 ipsec-isakmp dynamic DYNMAP
!

```

```
interface FastEthernet0/0
  ip address 10.0.2.2 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 172.30.2.2 255.255.255.0
  duplex auto
  speed auto
  crypto map CLIENTMAP
!
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 10.0.2.32 10.0.2.64
ip classless
ip route 10.0.2.0 255.255.255.0 10.0.2.102
ip route 10.0.7.0 255.255.255.0 172.30.7.1
!
no ip http server
no ip http secure-server
!
!
!
control-plane
!
!
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
  transport input telnet ssh
!
!
end
```

Lab 6-1 Answer Key: Configuring Remote Access Using Cisco Easy VPN

There is no Answer Key for this activity.

Lab 6-2: Configuring Cisco Easy VPN Remote for the Cisco VPN Client 4.x

Complete this lab activity to practice what you learned in the related module.

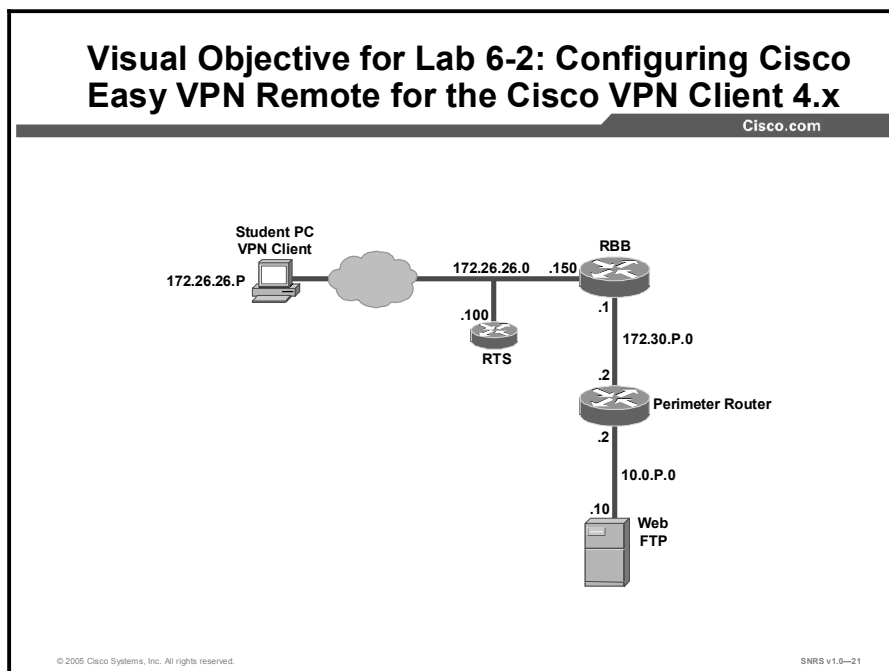
Activity Objective

In this activity, you will configure Cisco Easy VPN Remote for the Cisco VPN Client 4.x. After completing this activity, you will be able to meet these objectives:

- Install the Cisco VPN Client
- Create a new connection entry
- Launch the Cisco VPN Client
- Test the remote access connection
- (Optional) Configure Extended Authentication
- (Optional) Test Extended Authentication

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

Command List

The table describes the commands used in this activity.

Router Commands

Command	Description
<code>aaa authorization {network exec commands level reverse-access configuration} {default list-name} method1 [method2...]</code>	To set parameters that restrict user access to a network, use the aaa authorization command in global configuration mode. To disable authorization for a function, use the no form of this command.
<code>aaa new-model</code>	To enable the AAA access control model, issue the aaa new-model command in global configuration mode. To disable the AAA access control model, use the no form of this command.
<code>crypto isakmp xauth timeout sec</code>	Specifies the amount of time, in seconds, that the user has to enter the appropriate username and password to authenticate the session.

Job Aids

There are no job aids for this activity.

Task 1: Install the Cisco VPN Client

You will install the Cisco VPN Client on the Windows 2000 Server student PC.

Activity Procedure

Complete these steps:

- 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** Choose **Yes, I want to restart my computer now** and click **Finish**. The student PC restarts.

Activity Verification

You have completed this task when you attain these results:

- The VPN Client appears on the program menu.

Task 2: Create a New Connection Entry

You will create a new VPN connection entry.

Activity Procedure

Complete these steps:

- Step 1** Choose **Start > Programs > Cisco Systems VPN Client > VPN Client**. The Cisco Systems VPN Client window opens.
- Step 2** Click the **New** icon. The Create New VPN Connection Entry window opens.
- Step 3** Enter **VPN Server** in the connection entry field.
- Step 4** Enter a perimeter router outside interface IP address of **172.30.P.2** in the host field (where P = pod number).
- Step 5** Choose **Group Authentication** and complete the following fields (the entries are always case-sensitive):
1. Enter a group name: **VPN-REMOTE-ACCESS**. This is the group that you created earlier on the perimeter router.
 2. Enter the group password: **SW-CLIENT-PASSWORD**. This is the key that you created earlier for the VPN-REMOTE-ACCESS group.
 3. Confirm the password: **SW-CLIENT-PASSWORD**.
- Step 6** Click **Save**.

Activity Verification

You have completed this task when you attain these results:

- Verify that the connection entry is VPN Server.
- 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).

Task 3: Launch the Cisco VPN Client

You will launch the Cisco VPN Client on the student PC.

Activity Procedure

Complete this step:

Step 1 Choose **Start > Programs > Cisco Systems VPN Client > VPN Client**.

Activity Verification

You have completed this task when you attain these results:

- The VPN client is launched.

Task 4: Test the Remote Access Connection

You will test the VPN tunnel and the client connection.

Activity Procedure

Complete these steps:

- Step 1** 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.
- Step 2** Right-click the **Cisco VPN Client** icon in the student PC system tray and choose the **Statistics** option.
- Step 3** Open a command prompt shell and ping the inside interface of the perimeter router:
- ```
C:\> ping 10.0.P.2
```
- (where P = pod number)
- Step 4** Close the command prompt shell.
- Step 5** Click **OK** to close the statistics window.
- Step 6** Choose **Start > Programs > Cisco Systems VPN Client > VPN Client**. To start logging, click the **Log** drop-down menu and choose **Enable**. Click the **Log** tab, then click the **Log Window** icon.
- Step 7** Within the log window, click the **Log Settings** button at the bottom.
- Step 8** In the drop-down menu, set the IKE level to **High**.
- Step 9** In the drop-down menu, set the IPSec level to **High**.
- Step 10** Click **OK** to close the Log Settings window.
- Step 11** Right-click the **Cisco VPN Client** icon in the student PC system tray and choose the **Disconnect** option.
- Step 12** Click the **Clear** button at the bottom of the log window.
- Step 13** Reconnect to the router using the Cisco VPN Client 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:

Q1) What is the domain name?

---

**Step 15** Disconnect the Cisco VPN Client and close the Log Viewer.

## Activity Verification

There is no activity verification for this task.

## Task 5: (Optional) Configure Extended Authentication

You will add Xauth to the existing Cisco Easy VPN Server configuration, starting in global configuration mode.

### Activity Procedure

Complete these steps:

**Step 1** Enable AAA login authentication for the local VPNUSERS user group:

```
router(config)# aaa authentication login VPNUSERS local
```

**Step 2** Set the timeout value (0–60 seconds) for the amount of time that the remote user has to enter a username and password on the client. Use **20** seconds for the timeout value for this lab exercise:

```
router(config)# crypto isakmp xauth timeout 20
```

**Step 3** Enable IKE Xauth for the **CLIENTMAP** dynamic crypto map using the VPNUSERS user group:

```
router(config)# crypto map CLIENTMAP client authentication list VPNUSERS
```

**Step 4** Exit global configuration mode:

```
router(config)# exit
```

**Step 5** Save the router configuration to the startup configuration file:

```
router# copy run start
```

**Step 6** Use the following command in EXEC mode to verify your configurations for this feature:

```
router# show run
```

Your configuration should look similar to the following. Bold 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 VPNTRANSFORM esp-3des esp-sha-hmac
!
crypto dynamic-map DYNMAP 1
 set transform-set VPNTRANSFORM

```

```

reverse-route
!
!
crypto map CLIENTMAP client authentication list VPNUSERS
crypto map CLIENTMAP isakmp authorization list VPN-REMOTE-
ACCESS
crypto map CLIENTMAP client configuration address respond
crypto map CLIENTMAP 65535 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
```

### Activity Verification

You have completed this task when you attain these results:

- Your output is similar to the output in Step 6.

## Task 6: (Optional) Test Extended Authentication

You will test the Xauth configuration of the Cisco Easy VPN Server.

### Activity Procedure

Complete these steps:

- Step 1** Open the Cisco VPN Dialer application by choosing **Start > Programs > Cisco Systems VPN Client > VPN Client**.
- Step 2** Ensure that the 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 Client icon should appear in the system tray of the student PC.
- Step 7** Check the status of the VPN connection by right-clicking the Cisco VPN Client icon in the student PC system tray and choosing **Status** and the **Statistics** tab.
- Step 8** With the Status window still open, open a command shell and establish a Telnet session to the Easy VPN Server. You should see the packets encrypted and decrypted counters increment.

### Activity Verification

You have completed this task when you attain these results:

- You can connect using the Cisco VPN Client.

## Lab 6-2 Answer Key: Configuring Cisco Easy VPN Remote for the Cisco VPN Client 4.x

When you complete this activity, your answers will be similar to the following, with differences that are specific to your device or workgroup.

Q1) What is the domain name?

---



# Lab 6-3: Configuring a Cisco Access Router with Cisco Easy VPN

Complete this lab activity to practice what you learned in the related module.

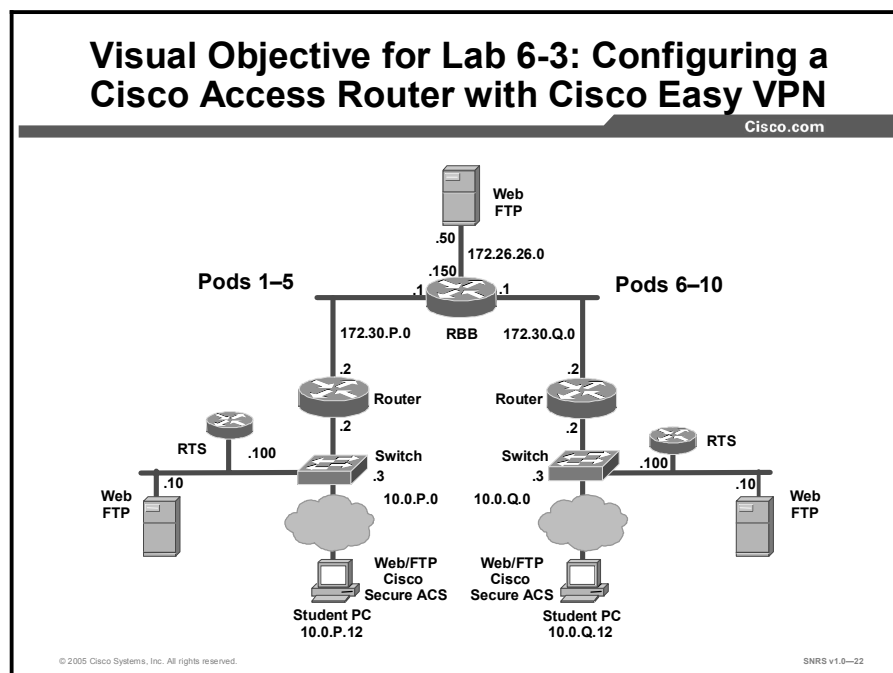
## Activity Objective

In this activity, you will configure a Cisco access router with Cisco Easy VPN. After completing this activity, you will be able to meet these objectives:

- Complete the lab exercise setup
- (Optional) Configure the DHCP server pool
- Configure and assign the Cisco Easy VPN client profile
- (Optional) Configure Xauth password save
- Initiate the VPN tunnel

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip dhcp pool name</code>                                   | Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode (identified by the config-dhcp# prompt).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>network network-number [mask   /prefix-length]</code>      | Specifies the subnet network number and mask of the DHCP address pool. The prefix length specifies the number of bits that constitute the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>default-router address [address2 ... address8]</code>      | Specifies the IP address of the default router for a DHCP client. One IP address is required, although you can specify up to eight addresses in one command line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>ip dhcp excluded-address low-address [high-address]</code> | Specifies the IP addresses that the DHCP server should not assign to DHCP clients.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>crypto ipsec client ezvpn name</code>                      | Creates a Cisco Easy VPN Remote configuration and then enters the Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>group group-name key group-key</code>                      | Specifies the group name and key value for the VPN connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>peer {ipaddress   hostname}</code>                         | Sets the peer IP address or host name for the VPN connection. A host name can be specified only when the router has a DNS server available for host name resolution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>mode {client   network-extension}</code>                   | Specifies the mode of operation of the VPN of the router:<br><br><b>client</b> —(Default) Automatically configures the router for Cisco Easy VPN Client mode operation, which uses NAT or PAT address translations. When the Cisco Easy VPN Remote configuration is assigned to an interface, the router automatically creates the NAT or PAT and ACL configuration needed for the VPN connection.<br><br><b>network-extension</b> —Specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the address space of the enterprise network. |
| <code>crypto ipsec client ezvpn xauth name</code>                | Respond to a pending VPN authorization request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>show crypto ipsec client ezvpn</code>                      | Display the Cisco Easy VPN Remote configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will set up the training pod equipment.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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** Restore the original course router configuration. Your instructor will explain how to do this.
- Step 3** Ensure that you can ping your peer router before beginning.

### Activity Verification

You have completed this task when you attain these results:

- You can ping your peer outside interface (where Q = peer pod number). Your output should look similar to the following:

```
R7# ping 172.30.Q.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.30.2.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

## Task 2: (Optional) Configure the DHCP Server Pool

You will create a DHCP server address pool.

### Activity Procedure

Complete these steps:

- Step 1** Create a DHCP server address pool:

```
router(config)# ip dhcp pool LOCALPOOL
```
- Step 2** Use the **network** command to specify the IP network and subnet mask of the address pool:

```
router(dhcp-config)# network 10.0.P.0 255.255.255.0
```
- Step 3** Use the **default-router** command to specify the IP address of the default router for a DHCP client:

```
router(dhcp-config)# default-router 10.0.2.2
```
- Step 4** Use the **ip dhcp excluded-address** command to exclude the specified address from the DHCP server pool:

```
router(config)# ip dhcp excluded-address 10.0.2.2
```

## Activity Verification

You have completed this task when you attain these results:

- Issue a **sh ip dhcp pool** command. The output should be similar to this:

```
R7#sh ip dhcp pool

Pool LOCALPOOL :
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Pending event : none
 1 subnet is currently in the pool :
 Current index IP address range Leased
 addresses
 10.0.2.1 10.0.2.1 - 10.0.2.254 0
```

## Task 3: Configure and Assign the Cisco Easy VPN Client Profile

You will configure and assign a Cisco Easy VPN client profile on the router.

### Activity Procedure

Complete these steps:

- Step 1** Use the **crypto ipsec client ezvpn name** command to create a profile:  

```
router(config)# crypto ipsec client ezvpn VPNGATE1
```
- 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:  

```
router(config-crypto-ezvpn)# group VPNREMOTE1 key SW-CLIENT-PASSWORD
```
- Step 3** Use the **peer** command to specify the IP address or host name for the destination peer:  

```
router(config-crypto-ezvpn)# peer 172.30.Q.2
```
- Step 4** Use the **mode** command to specify the type of VPN connection that should be made (client or network extension):  

```
router(config-crypto-ezvpn)# mode client
```
- Step 5** Enter the **exit** command to leave Cisco Easy VPN Remote configuration mode:  

```
router(config-crypto-ezvpn)# exit
```
- Step 6** Access interface configuration mode:  

```
router(config)# int Fa0/1
```

- Step 7** Assign the client profile to an interface:
- ```
router(config-if)# crypto ipsec client ezvpn VPNGATE1
```
- Step 8** Enter the **exit** command:
- ```
router(config-if)# exit
```
- Step 9** Change to Interface configuration mode. To configure the inside interface.
- ```
router(config)# int Fa0/0
```
- Step 10** Assign an Inside Interface.
- ```
crypto ipsec client ezvpn VPNGATE1 inside
```
- Step 11** Return to privileged mode.
- Step 12** `router(config-if)# end`

## Activity Verification

You have completed this task when you attain these results:

- Issue a **sh crypto ipsec client ezvpn** and a **sh crypto session** command. The output should be similar to this:

```
R7#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : VPNGATE1
Inside interface list: FastEthernet0/0,
Outside interface: FastEthernet0/1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.2.39
Mask: 255.255.255.255
Default Domain: cisco.com

R7#sh crypto session
Crypto session current status
Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.30.2.2/500
 IKE SA: local 172.30.7.2/500 remote 172.30.2.2/500 Active
 IPSEC FLOW: permit ip host 10.0.2.39 0.0.0.0/0.0.0.0
 Active SAs: 2, origin: crypto map

R7#sh crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication
```

```
Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.30.2.2/500 fvrf: (none) ivrf: (none)
 Phase1_id: 172.30.2.2
 Desc: (none)
IKE SA: local 172.30.7.2/500 remote 172.30.2.2/500 Active
 Capabilities:C connid:9 lifetime:23:48:10
IPSEC FLOW: permit ip host 10.0.2.33 0.0.0.0/0.0.0.0
 Active SAs: 2, origin: crypto map
 Inbound: #pkts dec'ed 5 drop 0 life (KB/Sec) 4557188/2920
 Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4557187/2920
```

## **Lab 6-3 Answer Key: Configuring a Cisco Access Router with Cisco Easy VPN**

There is no Answer Key for this activity.





## Required Resources

These are the resources and equipment required to complete this activity:

- There are no resources required to complete this activity.

## Command List

The table describes the commands used in this activity.

### Router Commands

| Command                                                                                                                                | Description                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip http authentication</code><br>{aaa   enable   local   tacacs}                                                                 | To specify a particular authentication method for HTTP server users, use the <b>ip http authentication</b> command in global configuration mode. To disable a configured authentication method, use the <b>no</b> form of this command. |
| <code>ip http secure-server</code>                                                                                                     | To enable the secure HTTP web server, use the <b>ip http secure-server</b> command in global configuration mode. To disable the secure HTTP server, use the <b>no</b> form of this command.                                             |
| <code>ip http server</code>                                                                                                            | To enable the HTTP server on your system, including the Cisco web browser user interface, use the <b>ip http server</b> command in global configuration mode. To disable the HTTP server, use the <b>no</b> form of this command.       |
| <code>line</code> [aux   console   tty   vty] <i>line-number</i><br>[ending-line-number]                                               | To identify a specific line for configuration and enter line configuration mode, use the <b>line</b> command in global configuration mode.                                                                                              |
| <code>login</code> [local   tacacs]                                                                                                    | To enable password checking at login, use the <b>login</b> command in line configuration mode. To disable password checking and allow connections without a password, use the <b>no</b> form of this command.                           |
| <code>privilege level</code> <i>level</i>                                                                                              | To set the default privilege level for a line, use the <b>privilege level</b> command in line configuration mode. To restore the default user privilege level to the line, use the <b>no</b> form of this command.                      |
| <code>transport input</code> {all   lat   mop   nasi   none   pad   rlogin   telnet   v120}                                            | To define which protocols to use to connect to a specific line of the router, use the <b>transport input</b> command in line configuration mode. To change or remove the protocol, use the <b>no</b> form of this command.              |
| <code>username</code> <i>name</i> {nopassword   password <i>password</i>   password <i>encryption-type</i> <i>encrypted-password</i> } | To establish a username-based authentication system, use the <b>username</b> command in global configuration mode.                                                                                                                      |

## Job Aids

There are no job aids for this activity.

## Task 1: Complete the Lab Exercise Setup

You will complete the lab exercise setup.

### Activity Procedure

Complete these steps:

- Step 1** Ensure that your student PC is powered on and that 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** 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 that you can ping the perimeter router from your student PC.
- Step 5** Ensure that your perimeter router (10.0.P.2, where P = pod number) can ping your PC. Your PC will be used as the TFTP server for this lab exercise.

### Activity Verification

You have completed this task when you attain these results:

- You can ping your perimeter router (10.0.P.2).

## Task 2: Copy Cisco SDM Files to Router Flash Memory

You will copy the Cisco SDM files to router flash memory.

### Activity Procedure

Complete these steps:

- 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**:

```
router> enable
Password: cisco
```

- Step 3** Check the contents of flash memory:

```
router# 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.

---

```
router# copy tftp://10.0.P.12/sdm.tar flash:
```

**Step 5** Copy the sdm.shtml file to the router flash using TFTP.

---

**Caution** When prompted, do *not* erase the flash memory.

---

```
router# copy tftp://10.0.P.12/home.html flash:
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show flash** command. You should see the appropriate files in flash.

## Task 3: Configure the Router to Support Cisco SDM

You will configure the router to support Cisco SDM.

### Activity Procedure

Complete these steps:

**Step 1** Enter global configuration mode using the **configure terminal** command:

```
router# conf t
```

**Step 2** Enable the Cisco web browser user interface using the **ip http server** command:

```
router(config)# ip http server
```

**Step 3** Enable the Cisco web secure browser user interface using the **ip http secure-server** command:

```
router(config)# ip http secure-server
```

**Step 4** Enable local authentication for Cisco web browser user interface connections using the **ip http authentication local** command:

```
router(config)# ip http authentication local
```

**Step 5** Create a local privilege level 15 user account for Cisco SDM Cisco web browser user interface login authentication:

```
router(config)# username sdm privilege 15 password 0 sdm
```

---

**Note** Enter the command exactly as shown for this lab exercise only. Do not use a username/password combination of sdm/sdm on your production routers. Always use unique username/password combinations in production environments.

---

**Step 6** Enter VTY line configuration mode using the **line vty** command:

```
router(config)# line vty 0 4
router(config-line)#
```

**Step 7** Configure the VTY privilege level for level 15 using the **privilege level** command:

```
router(config-line)# privilege level 15
```

**Step 8** Configure VTY login for local authentication using the **login local** command:

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

**Step 9** Configure VTY to allow both Telnet and SSH connections using the **transport input** command:

```
router(config-line)# transport input telnet ssh
router(config-line)# end
```

**Step 10** Copy the router running configuration to the startup configuration:

```
router# copy run start
```

### Activity Verification

You have completed this task when you attain these results:

- Issue a **show run** command. Check your configuration.

## Task 4: Launch Cisco SDM

You will launch Cisco SDM. Cisco SDM is stored in the router flash memory. It is launched by executing an HTML file, which then loads a signed Cisco SDM Java file.

### Activity Procedure

Complete these steps:

**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
```

---

**Note** If a security alert window appears, click **Yes** to continue.

---

**Step 3** Enter the correct username and password in the Enter Network Password window:

```
User Name: sdm
```

```
Password: sdm
```

**Step 4** Click **Yes** in the Security Warning window. The Cisco SDM window appears, and Cisco SDM loads the current configuration from the router.

### Activity Verification

You have completed this task when you attain these results:

- Your login is successful.

## Task 5: Configure a Basic Firewall

You will configure a basic firewall on the perimeter router.

### Activity Procedure

Complete these steps:

- Step 1** Access the Cisco SDM wizard mode.
- Step 2** Choose **Firewall** from the category bar.
- Step 3** Choose **Basic Firewall**.
- Step 4** Click **Launch the selected task**.
- Step 5** For the outside (untrusted) interface, choose your **172.30.P.2** Ethernet interface (where P = pod number).
- Step 6** For the inside (trusted) interface, choose the **FE0/0** interface.
- Step 7** Allow all denied firewall attempts to be logged.
- Step 8** Verify that your firewall configuration is correct (notice the access rules that will be applied to your firewall).
- Step 9** When your configuration summary is correct, click **Finish** to deliver the configuration to the router.

When the process is complete, the new firewall appears in the Firewall Wizard window under the Firewall Configurations Overview area. Note the ACL rules that will be applied to the interfaces that make up your firewall.

### Activity Verification

You have completed this task when you attain these results:

- View the firewall statistics in **Monitor Mode > Firewall Status**.

## Task 6: Create a Site-to-Site VPN Using Pre-Shared Keys

You will create a site-to-site VPN using pre-shared keys.

### Activity Procedure

Complete these steps:

- Step 1** Choose **VPN** from the category bar.
- Step 2** Choose 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 can 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** Choose **Quick Setup**.
- Step 6** Choose the outside **172.30.P.2** interface for the VPN connection (where P = pod number).
- Step 7** Choose 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** Choose 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 ISAKMP 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 Cisco SDM Warning window appears with a NAT conversion warning, click **Yes** so that the VPN will work correctly.

When the process is complete, the new VPN connection appears in the VPN Wizard window.

### Activity Verification

You have completed this task when you attain these results:

- View the VPN statistics in **Monitor Mode > VPN Status**.

## Task 7: Reset the Router Interface

You will reset the router interface.

### Activity Procedure

Complete these steps:

- Step 1** Access the Cisco SDM monitor mode.
- Step 2** Choose **Interfaces and Connections** from the category bar.
- Step 3** Choose 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.

### Activity Verification

You have completed this task when you attain these results:

- View the interface statistics in **Monitor Mode > Interface Status**.

## Task 8: Add a Rule to an ACL

You will add a rule to the existing ACL.

### Activity Procedure

Complete these steps:

- Step 1** Choose **Access Rules** from the category bar.
- Step 2** Choose 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.

### Activity Verification

You have completed this task when you attain these results:

- View the ACL settings in **Configure Mode > Additional Tasks > ACL Editor**.

## Task 9: Create a New ISAKMP Policy

You will create a new ISAKMP policy for AES encryption.

### Activity Procedure

Complete these steps:

- Step 1** Choose **VPN** from the category bar.
- Step 2** Choose **IKE > IKE Policies** from the VPN menu.
- Step 3** Click **Add**.
- Step 4** Add priority **2** with encryption **AES\_256** using D-H **group 2**.

### Activity Verification

You have completed this task when you attain these results:

- Check your configuration in the window.

## Task 10: Perform a Security Audit

You will perform a security audit on the router.

### Activity Procedure

Complete these steps:

- Step 1** Access the Cisco SDM wizard mode.
- Step 2** Choose **Security Audit** from the category bar.
- Step 3** Take time to read the audit pages.
- Step 4** Select all the interfaces that 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 that you wish Cisco SDM to fix (do not fix them all).
- Step 7** Allow Cisco SDM to fix a few of the items (do not fix them all).

### Activity Verification

You have completed this task when you attain these results:

- Return to the security audit to make sure that all the vulnerabilities you selected were automatically fixed.

## Task 11: Perform an Automatic Lockdown

You will perform an automatic lockdown.

### Activity Procedure

Complete these steps:

- Step 1** Choose **Security Audit** from the category bar.
- Step 2** Click **One-Step Lockdown**.

---

**Note** Some problems found during a security audit may require a manual entry to be locked down.

---

### Activity Verification

You have completed this task when you attain these results:

- Return to the security audit to make sure that all the vulnerabilities were automatically fixed.



## **Lab 7-1 Answer Key: Configuring a Perimeter Router with Cisco SDM**

There is no Answer Key for this activity.

