Cisco Systems

Cisco IOS VPN Configuration Guide

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

Text Part Number: OL-8336-01

INDEX

Preface

This preface describes the purpose, objectives, audience, organization, and conventions of the *Cisco IOS VPN Configuration Guide* and includes the following sections:

Note In this Guide, the term 'Cisco 7200 series router' implies that an Integrated Service Adaptor (ISA) or a VAM (VAM, VAM2, or VAM2+) is installed in the Cisco 7200 series router.

Purpose

This software configuration guide explains the basic considerations and tasks necessary to configure IP-based, multiservice site-to-site, and remote access Virtual Private Networks (VPNs) on your Cisco 7200 series router. VPNs integrate security and quality of service (QoS) through network technologies such as Generic Routing Encapsulation (GRE) and IP Security Protocol (IPSec) tunneling, and high-speed encryption to ensure private transactions over public data networks. This guide does not cover every available feature; it is not intended to be a comprehensive VPN configuration guide. Instead, this guide simply explains the basic tasks necessary to configure site-to-site and remote access VPNs on your Cisco 7200 series router.

Note For detailed information on configuring client-initiated and network access server (NAS)-initiated access VPNs using the L2F tunneling protocol, refer to the *Access VPN Solutions Using Tunneling Technology* publication. If you are a registered Cisco user, you can access the *Access VPNs and IP Security Protocol Tunneling Technology* publication.

The intranet, extranet, and remote access business scenarios introduced in this guide include specific tasks and configuration examples. The examples are the recommended methods for configuring the specified tasks. Although they are typically the easiest or the most straightforward method, they are not the only methods of configuring the tasks. If you know of another configuration method not presented in this guide, you can use it.

The network design considerations discussed in this guide are comprised of known factors that hinder or optimize network performance. The considerations are not solid rules, but rather suggestions and discussions that might be helpful in designing your VPN.

Note Use this guide after you install, power up, and initially configure your Cisco 7200 series router for network connectivity. Refer to the *Installation and Configuration Guide* at http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html for instructions on how to install, power up, and initially configure your Cisco 7200 series router.

Audience

This software configuration guide is intended primarily for the following audiences:

- System administrators who are responsible for installing and configuring internetworking equipment, who are familiar with the fundamentals of Cisco 7200 series router-based internetworking, and who are familiar with Cisco IOS software and Cisco products
- System administrators who are familiar with the fundamentals of Cisco 7200 series router-based internetworking and who are responsible for installing and configuring internetworking equipment, but who might not be familiar with the specifics of Cisco products or the routing protocols supported by Cisco products
- Customers with technical networking background and experience

Organization

The major sections of this guide follow:

Chapter	Title	Description
1	Using Cisco IOS Software	Provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI).
2	Network Design Considerations	Provides an overview of the assumptions this guide makes, items you should consider to optimize performance on your Cisco 7200 series router, and a discussion of headend failover.

Chapter	Title	Description
3	Site-to-Site and Extranet VPN Business Scenarios	Explains the basic tasks for configuring a site-to-site or extranet VPN on a Cisco 7200 series router using GRE or IPSec as the tunneling protocol.
4	Remote Access VPN Business Scenarios	Explains the basic tasks for configuring a remote access VPN on a Cisco 7200 series router and discusses client software, considerations, and configurations.
5	VPN Network Management Tools	Provides an overview of Cisco network management software, and IPSec with MIB.

Related Documentation

Your Cisco 7200 series router and the Cisco IOS software running on it contain extensive features and functionality, which are documented in the following resources:

- For Cisco 7200 series router hardware installation and initial software configuration information, refer to the following publications located at http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html:
  - The *Quick Start Guide* for your Cisco 7200 series router
  - The *Installation and Configuration Guide* for your Cisco 7200 series router
- For international agency compliance, safety, and statutory information for Cisco 7200 series router, refer to the *Regulatory Compliance and Safety Information* publication for your Cisco 7200 series router at http://www.cisco.com/en/US/products/hw/routers/ps341/products_regulatory_approvals_and_compliance09186a00800a94d7.html.
- For information on installing and replacing field-replaceable units (FRUs), refer to the Installing field-replaceable units publication for your Cisco 7200 series router at http://www.cisco.com/en/US/products/hw/routers/ps341/prod_installation_guides_list.html.
- For information on installing and replacing the integrated service module (ISM), refer to the integrated service adapter and integrated service module installation and configuration publication for your Cisco 7200 series router at http://www.cisco.com/en/US/products/hw/switches/ps708/prod_module_install_config_guide09186a0080145522.html.
- For information on installing and replacing your VPN Acceleration Module (VAM), refer to the VAM installation and configuration publication for your Cisco 7200 series router at http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_and_configuration_guides_list.html.
- For information on the port adapter installed in the Cisco 7200 series router, refer to the individual installation and configuration guides for each port adapter at http://www.cisco.com/en/US/products/hw/modules/ps2033/tsd_products_support_series_home.html.
- For configuration information and support, refer to the modular configuration and modular command reference publications at http://www.cisco.com/en/US/products/hw/modules/tsd_products_support_category_home.html.

Note Select Translated documentation is available at http://www.cisco.com/ by selecting the topic 'Select a Location / Language' at the top of the page.

- To determine the minimum Cisco IOS software requirements for your Cisco 7200 series router, Cisco maintains the Software Advisor tool on Cisco.com. This tool does not verify whether modules within a system are compatible, but it does provide the minimum IOS requirements for individual hardware modules or components. Registered Cisco Direct users can access the Software Advisor at: http://tools.cisco.com/Support/Fusion/FusionHome.do.
- For detailed information on hardware, software configuration, troubleshooting, and other topics related to IP security and VPN, refer to http://www.cisco.com/en/US/products/hw/vpndevc/tsd_products_support_category_home.html.
- For information on interfaces and Cisco IOS network design, implementation, configuration, verification, troubleshooting, operation, and maintenance, refer to http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html.
- If you're a registered Cisco Direct Customer, you can access the tools index at http://www.cisco.com/en/US/products/prod_tools_index.html.
- For information on network management applications, refer to the "Network Management Considerations" section on page 2-16 of Chapter 2, "Network Design Considerations" and the network management product documentation on Cisco.com and the Product Documentation DVD.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Using Cisco IOS Software

This chapter provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI) and includes the following sections:

For an overview of Cisco IOS software configuration, refer to the *Configuration Fundamentals Configuration Guide*. See "Related Documentation" section on page xi for additional information.

Conventions

Command descriptions use the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{*x* | *y* | *z*}	Alternative keywords are grouped in braces and separated by vertical bars.
[*x* | **y** | *z*]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.

Convention	Description
——→	`This pointer highlights an important line of text in an example.`
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Getting Help

Entering a question mark (**?**) at the system prompt displays a list of commands available for each command mode. You can also get a list of any commands associated keywords and arguments with the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Obtain a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Obtain a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry **<Tab>**	Complete a partial command name.
?	List all commands available for a particular command mode.
command **?**	List command-associated keywords. (Space between command and question mark.)
command keyword **?**	List keyword-associated arguments. (Space between the keyword and question mark.)

Note Press **Ctrl-P** or the up arrow key to recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. Press **Ctrl-N** or the down arrow key to return to more recent commands in the history buffer after recalling commands with **Ctrl-P**

or the up arrow key. Repeat the key sequence to recall successively more recent commands.

The arrow keys function only on ANSI-compatible terminals such as VT100s.

Finding Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list of keywords available along with a brief description of the keywords. For example, if you were in global configuration mode and wanted to see all the keywords for the **arap** command, you would type **arap ?**.

Table 1-1 shows how to use the question mark (**?**) to find the command options for the following two commands:

- **controller t1 1**
- **cas-group 1 timeslots 1-24 type e&m-fgb dtmf**

Table 1-1 How to Find Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands.
	You have entered privileged EXEC mode when the prompt changes to Router#.

`Router# configure terminal`
`Enter configuration commands, one per line.`
`End with CNTL/Z.`
`Router(config)#`
	Enter global configuration mode.
	You have entered global configuration mode when the prompt changes to Router(config)#.

`Router(config)# controller t1 ?`
`  <0-3>  Controller unit number`
`Router(config)# controller t1 1`
`Router(config-controller)#`
	Enter controller configuration mode by specifying the T1 controller that you want to configure using the **controller t1** global configuration command.
	Enter a **?** to display what you must enter next on the command line. In this example, you must enter a controller unit number from 0 to 3.
	You have entered controller configuration mode when the prompt changes to Router(config-controller)#.

Table 1-1 How to Find Command Options (continued)

Command	Comment

`Router(config-controller)# ?`
`Controller configuration commands:`
`  cablelengthSpecify the cable length for a DS1 link`
`  cas-groupConfigure the specified timeslots for CAS (Channel Associate Signals)`
`  channel-groupSpecify the timeslots to channel-group mapping for an interface`
`  clockSpecify the clock source for a DS1 link`
`  defaultSet a command to its defaults`
`  descriptionController specific description`
`  ds0ds0 commands`
`  exitExit from controller configuration mode`
`  fdlSpecify the FDL standard for a DS1 data link`
`  framingSpecify the type of Framing on a DS1 link`
`  helpDescription of the interactive help system`
`  linecodeSpecify the line encoding method for a DS1 link`
`  loopbackPut the entire T1 line into loopback`
`  noNegate a command or set its defaults`
`  pri-groupConfigure the specified timeslots for PRI`
`  shutdownShut down a DS1 link (send Blue Alarm)`
`Router(config-controller)#`
	Enter a **?** to display a list of all the controller configuration commands available for the T1 controller.

`Router(config-controller)# cas-group ?`
`  <0-23>Channel number`
`Router(config-controller)# cas-group`
	Enter the command that you want to configure for the controller. In this example, the **cas-group** command is used.
	Enter a **?** to display what you must enter next on the command line. In this example, you must enter a channel number from 0 to 23.
	When the system redisplays the command, it indicates that you must enter more keywords to complete the command.

`Router(config-controller)# cas-group 1 ?`
`  timeslots List of timeslots in the cas-group`
`Router(config-controller)# cas-group 1`
	After you enter the channel number, enter a **?** to display what you must enter next on the command line. In this example, you must enter the **timeslots** keyword.
	When the system redisplays the command, it indicates that you must enter more keywords to complete the command.

`Router(config-controller)# cas-group 1 timeslots ?`
`  <1-24> List of timeslots which comprise the cas-group`
`Router(config-controller)# cas-group 1 timeslots`
	After you enter the **timeslots** keyword, enter a **?** to display what you must enter next on the command line. In this example, you must enter a list of timeslots from 1 to 24.
	You can specify timeslot ranges (for example, 1–24), individual timeslots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1–3, 8, 17–24). The 16th time slot is not specified in the command line, because it is reserved for transmitting the channel signaling.
	When the system redisplays the command, it indicates that you must enter more keywords to complete the command.

Table 1-1 How to Find Command Options (continued)

Command	Comment

Router(config-controller)# **cas-group 1 timeslots 1-24 ?**
  service Specify the type of service
  type Specify the type of signaling
Router(config-controller)# cas-group 1 timeslots 1-24
	After you enter the timeslot ranges, enter a **?** to display what you must enter next on the command line. In this example, you must enter the **service** or **type** keyword.
	When the system redisplays the command, it indicates that you must enter more keywords to complete the command.

Router(config-controller)# **cas-group 1 timeslots 1-24 type ?**
  e&m-fgb E & M Type II FGB
  e&m-fgd E & M Type IIFGD
  e&m-immediate-start E & M Immediate Start
  fxs-ground-start FXS Ground Start
  fxs-loop-start FXS Loop Start
  sas-ground-start SAS Ground Start
  sas-loop-start SAS Loop Start
Router(config-controller)# cas-group 1 timeslots 1-24 type
	In this example, the **type** keyword is entered. After you enter the **type** keyword, enter a **?** to display what you must enter next on the command line. In this example, you must enter one of the signaling types.
	When the system redisplays the command, it indicates that you must enter more keywords to complete the command.

Router(config-controller)# **cas-group 1 timeslots 1-24 type e&m-fgb ?**
  dtmf DTMF tone signaling
  mf MF tone signaling
  service Specify the type of service
  <cr>
Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb
	In this example, the **e&m-fgb** keyword is entered. After you enter the **e&m-fgb** keyword, enter a **?** to display what you must enter next on the command line. In this example, you can enter the **dtmf**, **mf**, or **service** keyword to indicate the type of channel-associated signaling available for the **e&m-fgb** signaling type.
	When the system redisplays the command, it indicates that you can enter more keywords or press <cr> to complete the command.

Router(config-controller)# **cas-group 1 timeslots 1-24 type e&m-fgb dtmf ?**
  dnis DNIS addr info provisioned
  service Specify the type of service
  <cr>
Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb dtmf
	In this example, the **dtmf** keyword is entered. After you enter the **dtmf** keyword, enter a **?** to display what you must enter next on the command line. In this example, you can enter the **dnis** or **service** keyword to indicate the options available for **dtmf** tone signaling.
	When the system redisplays the command, it indicates that you can enter more keywords or press <cr> to complete the command.

Router(config-controller)# **cas-group 1 timeslots 1-24 type e&m-fgb dtmf** Router(config-controller)#	In this example, enter a <cr> to complete the command.

Understanding Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you at any given time depend on your current mode. By entering a question mark (**?**) at the system prompt, you can obtain a list of commands available for each command mode.

When you start a session on the router, you begin in user mode, often called EXEC mode. Only a limited subset of the commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode (also called enable mode). Normally, you must enter a password to enter privileged EXEC mode. From privileged mode, you can enter any EXEC command or enter global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current status of something, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the router.

Using configuration modes, you can make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots. To get to the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

ROM monitor mode is a separate mode used when the router cannot boot properly. If your router or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter ROM monitor mode.

Summary of Main Command Modes

Table 1-2 summarizes the main command modes of the Cisco IOS software.

Table 1-2 Summary of Main Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To exit back to user EXEC mode, use the **disable** command. To enter global configuration mode, use the **configure terminal** privileged EXEC command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To exit to privileged EXEC mode, use the **exit** or **end** command or press **Ctrl-Z**. To enter interface configuration mode, enter an **interface** configuration command.
Interface configuration	From global configuration mode, enter by specifying an interface with an **interface** command.	`Router(config-if)#`	To exit to global configuration mode, use the **exit** command. To exit to privileged EXEC mode, use the **exit** command or press **Ctrl-Z**. To enter subinterface configuration mode, specify a subinterface with the **interface** command.

Table 1-2 Summary of Main Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Subinterface configuration	From interface configuration mode, specify a subinterface with an **interface** command.	`Router(config-subif)#`	To exit to global configuration mode, use the **exit** command. To enter privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the Break key during the first 60 seconds while the system is booting.	`>`	To exit to user EXEC mode, type **continue**.

For more information about command modes, refer to the "Using the Command Line Interface" chapter of the *Configuration Fundamentals Configuration Guide*.

Using the no and default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a function. Use the command without the keyword **no** to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no ip routing** commands, and specify **ip routing** to reenable it. The Cisco IOS software command references provide the complete syntax for the configuration commands and describe what the **no** form of commands does.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values. The Cisco IOS software command references describe what the **default** form of a command does if it is not the same as the **no** form.

Saving Configuration Changes

Enter the **copy system:running-config nvram:startup-config** command to save your configuration changes to your startup configuration so that they will not be lost if there is a system reload or power outage. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this step saves the configuration to nonvolatile random-access memory (NVRAM). On Class A Flash memory file systems, such as Cisco 7100 series routers, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Network Design Considerations

This chapter provides an overview of the business scenarios covered in this guide, items you should consider when configuring a Virtual Private Network (VPN) on your Cisco 7200 series router, and the assumptions this guide makes.

This chapter includes the following sections:

Note In this Guide, the term 'Cisco 7200 series router' implies that an Integrated Service Adaptor (ISA) or a VAM (VAM, VAM2, or VAM2+) is installed in the Cisco 7200 series router.

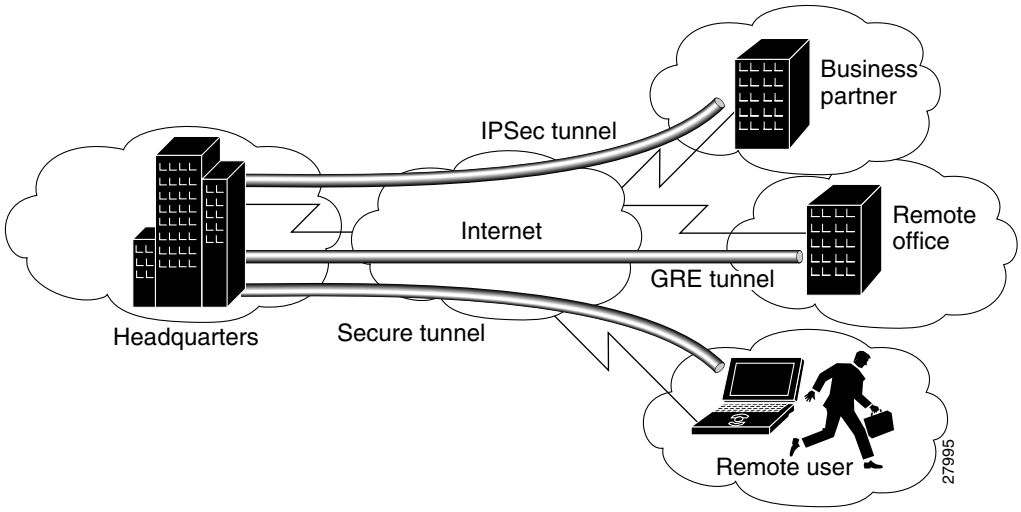
Overview of Business Scenarios

The site-to-site and extranet scenarios explained in this guide provide a remote office and a business partner access to a corporate headquarters network through Generic Routing Encapsulation (GRE) or IP Security Protocol (IPSec) tunnels. The remote access scenario provides a remote user access to a corporate headquarters network through secure IPSec, Point-to-Point Tunneling Protocol (PPTP), or Layer 2 Tunnel Protocol (L2TP) tunnels. (See Figure 2-1.)

Note For detailed information on configuring network access server (NAS)-initiated access VPNs using the Layer 2 Forwarding (L2F) tunneling protocol, refer to the *Access VPN Solutions Using Tunneling Technology* publication.

In each scenario, a tunnel is constructed, encryption is applied on the tunnel, and different traffic types (for example, IP, User Datagram Protocol [UDP], and Transmission Control Protocol [TCP]) are either permitted or denied access to the tunnel. This controls the level of access the remote office and business partner have to the corporate intranet and secures the data exchanged between the sites.

Figure 2-1 Business Scenarios



The site-to-site VPN business scenario explained in Chapter 3, "Site-to-Site and Extranet VPN Business Scenarios" links the corporate headquarters to a remote office using connections across the Internet. Users in the remote office are able to access resources as if they were part of the private corporate intranet.

The extranet VPN business scenario explained in Chapter 3, "Site-to-Site and Extranet VPN Business Scenarios" builds on the VPN scenario by linking the same corporate headquarters to a business partner using connections across the Internet; however, the business partner is given limited access to the headquarters network—the business partner can access only the headquarters public server.

The remote access VPN business scenario, explained in Chapter 4, "Remote Access VPN Business Scenarios" provides a remote user access to the corporate headquarters network through a secure IPSec, PPTP, or L2TP tunnel that is initiated by the remote user running VPN client software on a PC. In this scenario, the user can access the corporate network remotely.

Note This guide does not explain how to configure your router for use with the Cisco Secure VPN Client. For detailed information on client-initiated VPNs using Cisco Secure VPN Client software, refer to the *Cisco Secure VPN Client Solutions Guide* publication. If you are a registered Cisco user, you can access the *Access VPNs and IP Security Protocol Tunneling Technology* publication.

Assumptions

This guide assumes the following:

- You are configuring a service provider transparent VPN, whereby the tunnel endpoints are outside of the service provider network (on the headquarters and remote site routers).

- You are configuring your VPN based on IP, a routing mechanism, cryptography, and tunneling technologies, such as IPSec and GRE.

Note The scenarios in this guide do not explain how to configure certification authority (CA) interoperability on your Cisco 7200 series router. For detailed configuration information on CA interoperability, refer to the "Configuring Certification Authority Interoperability" chapter in the *Cisco IOS Security Configuration Guide*.

- You have identified the Cisco IOS firewall features that you plan to configure on your Cisco 7200 series router features. When considering IOS firewall features, you may find it useful to review the "Network Traffic Considerations" section on page 2-5. The business scenarios in this guide explain how to configure extended access lists, which are sequential collections of permit and deny conditions that apply to an IP address.

Note For advanced firewall configuration information, refer to the "Traffic Filtering and Firewalls" section of the *Cisco IOS Security Configuration Guide.*

Cisco SAFE Blueprint

Cisco's secure blueprint for enterprise networks (SAFE) primary goal is to provide best practice information to interested parties on designing and implementing secure networks. SAFE serves as a guide to network designers considering the security requirements of their network. SAFE takes a defense-in-depth approach to network security design. This type of design focuses on the expected threats and their methods of mitigation. This strategy results in a layered approach to security, where the failure of one security system is not likely to lead to the compromise of network resources. SAFE is based on Cisco products and those of its partners.

Cisco encourages the audience of this configuration guide to reference the SAFE Blueprint.

Refer to the white paper, *SAFE VPN: IPSec Virtual Private Networks in Depth,* for information relevant to network design considerations. While this configuration guide incorporates several key components of the white paper, Cisco recommends referencing it for an expanded discussion in a context relevant to your specific network, such as small, medium, or large network designs, and remote access and VPN modules.

In addition to network topology, network design considerations, and configuration examples, the white paper discusses the following topics:

- Overall design best practices
- High availability (failover)
- Scalability
- Performance
- Identity (authentication methods)
- Secure Management
- NAT (Network Address Translation)
- Security
- Quality of Service
- Routing

- Extranet Considerations

Hybrid Network Environments

While Cisco IOS devices are interoperable with non-IOS devices, such as the PIX Firewall, the Cisco VPN 5000, and the Cisco VPN 3000, this configuration guide focuses on IOS headend VPN configurations. For information on configuring a hybrid VPN, refer to the configuration guide for your particular device.

Mixed Device Deployments

In considering a VPN design, it is critical to ascertain interoperability information about all devices. Networking standards exist, but each manufacturer may or may not utilize the standard in the same way.

For example, although IPSec is a documented standard, the Request for Comments (RFCs) that document it has left room for interpretation. In addition, Internet drafts such as IKE mode-configuration and vendor-proprietary features increase the likelihood of interoperability challenges. For instance, no standard mechanism for IPSec exists to determine tunnel up or down state, and remote peer reachability. For these reasons, check with vendors of both products for Cisco product interoperability information and their participation in interoperability bake-offs. Typically, a few minor changes to configurations, and sometimes code, are necessary to facilitate interoperability in a reliable fashion. Realize, though, that these changes may affect the security stance of the device, and consider the implications of these changes.

Also, in order to ensure interoperability between products from a single vendor, use the same code base across all platforms. Doing so decreases the likelihood of any interoperability issues with products made by the same vendor as changes occur and interoperability with other vendors increases.

Issues in addition to interoperability arise in environments where different device types are deployed to build a VPN. These issues usually arise because of interaction between the VPN and other features that complement its operation. For instance, consider the authentication, authorization, and accounting (AAA) protocol used to manage remote users and administrators. The granularity of support for this protocol, for example Terminal Access Controller Access Control System Plus (TACACS+), or Remote Access Dial-In User Service (RADIUS), may differ among the device types. This difference can complicate matters if your user database does not support one of these mechanisms across all the device types deployed. The mechanisms used for IPSec high-availability and CA support differs for some routers, firewalls, concentrators, and remote-access clients.

Also consider the additional resources required to train administrators on how to configure, manage, monitor, and troubleshoot multiple device types.

Integrated versus Overlay Design

An integrated network design is one in which the WAN, VPN, and IOS firewall functions are run on the same device, for example, on a remote site Cisco 7200 series router. Integrated network designs are common in remote offices because of their simplicity and manageability.

An overlay design is one in which any single function, or all functions, are separated, as in headend designs. Firewall functionality is usually separate, the WAN and VPN functions are often integrated (meaning that the functions run on the same device), and VPN functionality is frequently separate from the WAN and firewall functions.

The primary advantage of an overlay design in the headend configuration is that the separation of tasks optimizes network performance. Each device may be dedicated to one or two tasks, rather than all three, in a heavy traffic environment. For example, ACLs (Access Control Lists) require a fair amount of CPU utilization. Therefore, performing ACL tasks on a device other than the Cisco 7200 series router allows the Cisco 7200 series router more power to support network traffic.

Network Traffic Considerations

Cisco IOS is feature-rich software. However, if improperly used, these features can degrade the flow of VPN traffic. This section provides a discussion of when and how to use several Cisco IOS options to maximize VPN performance, and includes the following topics:

- Dynamic versus Static Crypto Maps
- Digital Certificates versus Pre-shared Keys
- Generic Routing Encapsulation Inside IPSec
- Network Address Translation
- Quality of Service
- Network Intrusion Detection System

Dynamic versus Static Crypto Maps

Cisco recommends using static crypto maps on headend devices whenever possible. Remember that a tunnel being established from a dynamic crypto map can only be originated from the remote end. If devices must be remotely managed, static maps should be used, as the headend cannot establish a tunnel when using dynamic crypto maps.

In network environments in which the remote IP addresses are unknown (such as remote users using dial-up, cable, or DSL), however, dynamic maps must be used. Additionally, dynamic maps can be used for configuration simplicity. They simplify configuration because a crypto map statement is not required for each IP address range. Digital certificates are also highly recommended with the use of dynamic crypto maps. Dynamic cryptographic maps accept only incoming IKE requests. Because dynamic maps cannot initiate IKE requests, it is not always guaranteed that a tunnel exists between the remote device and the headend site.

This problem can be mitigated by configuring a protocol like Network Time Protocol (NTP) on remote peers to ensure that the tunnel has been established. When a protocol such as NTP or SNMP generates traffic to the headend, it forces IPSec tunnel establishment from the remote end, since the time server is at the headend. Forcing tunnel establishment from the remote end allows the use of dynamic crypto maps, while ensuring that an IPSec tunnel exists. If you use static crypto maps, you are assured that an IPSec tunnel exists, and do not need to configure establishment from the remote end.

Another consideration is that dynamic crypto maps decrease VPN security, as they accept IKE requests from any IP address.

Static cryptographic map configurations include the static IP addresses of the remote peers, and are therefore more secure. The lack of ambiguity associated with static maps also allows a faster traffic flow.

Digital Certificates versus Pre-shared Keys

Digital certificates (DCs) simplify authentication, and increases VPN performance. You need only enroll each peer with the CA, rather than manually configuring each peer to exchange keys. Cisco recommends using digital certificates especially in site-to-site networks of more than 50 peers. Digital certificates offer the added security and network management benefit of nonrepudiation, meaning that a peer can verify that communication actually took place.

In addition to easing the flow of network traffic, digital certificates offer inherent benefits over pre-shared keys. Compromised pre-shared keys are susceptible to man-in-the-middle attacks. With the key, a hacker can connect to any device in your network allowed by the remote-site access policy. Digital certificates scale better than unique pre-shared keys because they allow any device to authenticate to any other device. Digital certificates are not tied to IP addresses, but to unique, signed information on the device that is validated by the enterprise CA. If a hacker compromises or steals a device with a digital certificate, the administrator will revoke the digital certificate and notify all other devices by publishing a new certificate revocation list (CRL). The CRL contains a CA-signed list of revoked certificates. When a device receives a request for tunnel establishment and uses a digital certificate for proof of identity, the device checks the peer certificate against the CRL.

Wildcard pre-shared keys should not be used for site-to-site device authentication. When using wildcard pre-shared keys, every device in the network uses the same key. If a single device in your network is compromised and the wildcard pre-shared key has been determined, all the devices are then compromised.

Devices generating digital certificates or validating received certificates during tunnel authentication and establishment must know the correct time of day (preferably Coordinated Universal Time [UTC]). Time also determines when the CRL expires so that a new one can be retrieved.

Although checking CRLs can be configured as optional, it should always be enabled on remote and headend devices when digital certificates are deployed. This is the only revocation scheme for digital certificates compared to pre-shared keys that are simply removed from the uncompromised devices.

Digital certificates also provide more key entropy (more bits for seeding functions), public/private key pair aging, and nonrepudiation. Digital certificates do, however, require additional administrative resources to deploy and manage, given their feature complexity. Using a third-party-managed CA rather than an enterprise managed CA might facilitate deploying an extranet VPN.

If you specify digital certificates as the authentication method in a policy, the CA must be properly configured to issue certificates. You must also configure the peers to obtain certificates from the CA. Configure this certificate support as described in the "Configuring Certification Authority Interoperability" chapter of the *Cisco IOS Security Configuration Guide.*

Generic Routing Encapsulation Inside IPSec

Generic routing encapsulation (GRE) is best suited for site-to-site VPNs because it supports routing updates, multiprotocol, and multicast traffic. Packets are first encapsulated by GRE, and then encapsulated by IPSec. GRE also allows for a single set of IPSec security associations (SAs) to tunnel traffic from one site to another. Typically, IPSec requires a unique set of IPSec SAs to provide tunneling capability for each local network to each remote network. GRE encapsulates all traffic, regardless of its source and destination, and does not encrypt packets. Use GRE when you need support for tunneling packets other than IP unicast type.

Cisco recommends using GRE tunnels with IPSec in tunnel mode to improve the flow of network traffic. IPSec in tunnel mode can be used as a tunneling protocol itself for unicast traffic, but not for multicast traffic. Multicast IPSec traffic requires a GRE tunnel, and that IPSec be used in either transport or tunnel mode. Cisco recommends using IPSec in tunnel mode for the best network traffic performance.

Changing these values increases the level of security; at the same time, however, it increases the processor overhead. The default behavior for SA rekeying is to base the new key in part on the old key to save processing resources. Perfect forward secrecy (PFS) generates a new key based on new seed material by carrying out a Diffie-Hellman (DH) exponentiation every time a new quick-mode (QM) SA needs new key generation. Again, this option increases the level of security but at the same time increases processor overhead. Cisco does not recommend changing the SA lifetimes or enabling PFS unless the sensitivity of the data mandates it. If you choose to change these values, make sure you include this variable when determining the network design. The strength of the Diffie-Hellman exponentiation is configurable; Groups 1 (768 bits), 2 (1024 bits), and 5 (1536 bits) are supported. Group 2 is recommended.

IPSec Considerations

IPSec provides numerous security features. The following have configurable values for the administrator to define their behavior: data encryption, device authentication and credential, data integrity, address hiding, and SA key aging. The IPSec standard requires the use of either data integrity or data encryption; using both is optional. Cisco highly recommends using both encryption and integrity. Cisco recommends the use of Triple DES (3DES), rather than DES, as it provides stronger encryption. Data integrity comes in two types: 128-bit strength Message Digest 5 (MD5)-HMAC or 160-bit strength secure hash algorithm (SHA)-HMAC. Because the bit strength of SHA is greater, it is considered more secure. Cisco recommends the use of SHA because the increased security outweighs the slight processor increase in overhead (in fact, SHA is sometimes faster than MD5 in certain hardware implementations).

Both IPSec phases offer the ability to change the lifetime of the SA. You might consider changing the lifetime from the default when the sensitivity of the tunneled data mandates replacing the encryption keys and reauthenticating each device on a more aggressive basis. Keep in mind that the shorter the SA lifetime, the greater the impact on network traffic (see the "IKE Key Lifetimes" section on page 2-13). The use of strong encryption algorithms in non-US countries is sometimes regulated by local import and usage laws. These strong encryption algorithms cannot be exported to some countries or some customers. For more information about the exportation of encryption algorithms, please see your sales representative.

- Keep in mind the following when configuring IPSec:
  - IPSec works with the following serial encapsulations: High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), and Frame Relay. IPSec also works with the GRE and IPinIP Layer 3, L2F, and L2TP tunneling protocols; however, multipoint tunnels are not supported.
  - IPSec and Internet Key Exchange (IKE) must be configured on the router and a crypto map must be assigned to all interfaces that require encryption services of your Cisco 7200 series router.
  - When using tunnel mode, IPSec can be applied to unicast IP datagrams only. Because the IPSec Working Group has not yet addressed the issue of group key distribution, IPSec does not currently work with multicasts or broadcast IP datagrams. When using IPSec with GRE or L2TP, this restriction does not apply.

If you use NAT, you should configure static NAT as redundant so that IPSec works properly. Preferably, NAT should occur before the router performs IPSec encapsulation; in other words, IPSec should be working with global addresses. The following section discusses NAT in further detail.

Network Address Translation

Network Address Translation (NAT) can occur before or after IPSec. It is important to realize when NAT will occur, since in some cases NAT might interfere with IPSec by blocking tunnel establishment or traffic flow through the tunnel. It is a best practice to avoid the application of NAT to VPN traffic unless it is necessary to provide access, as NAT can have an adverse effect on network traffic flow.

NAT After IPSec

You might consider applying NAT after IPSec encryption for address hiding. However, this provides no benefit because the actual IP addresses of the devices utilizing the tunnel for transport are hidden through encryption. Only the public IP addresses of the IPSec peers are visible, and address hiding of these addresses provides no real additional security. NAT application after IPSec encapsulation occurs in cases where IP address conservation is taking place. This is, in fact, commonplace in hotels, cable and digital subscriber line (DSL) residential deployments, and enterprise networks. In these cases, depending on the type of NAT used, its application might interfere with the IPSec tunnel establishment. When IPSec uses Authentication-Header (AH) mode for packet integrity, if one-to-one address translation occurs it will invalidate the signature checksum. Because the signature checksum is partially derived based on the AH packet IP header contents, when the IP header changes, the signature checksum is invalidated. In this case, the packet will appear to have been modified in transit and is promptly discarded when received by the remote peer. However, when IPSec uses ESP, the devices will be able to successfully send packets over the VPN, even when one-to-one address translation occurs after encapsulation. This scenario is possible because ESP does not use the IP header contents to validate the integrity of the packets. In cases where many-to-one address translation occurs (as in port address translation), the IP address and source IKE port, normally User Datagram Protocol (UDP) port 500, will change. Some VPN devices do not support IKE requests sourced on ports other than UDP 500, and some devices performing many-to-one NAT do not handle ESP or AH correctly. Remember that ESP and AH are higher-layer protocols on top of IP that do not use ports.

NAT Before IPSec

When two sites are connected through an IPSec tunnel, if any of the network address ranges at each site overlap, the tunnel will not establish. This occurs because it is not possible for the VPN termination devices to determine the site to which to forward the packets. Utilizing NAT before IPSec overcomes this restriction by translating one set of the overlapping networks into a unique network address range that will not interfere with the IPSec tunnel establishment. This is the only scenario where the application of NAT is recommended. Be aware, however, that some protocols embed IP addresses in packet data segments. In general, when address translation occurs, make sure that a protocol-aware device carries out the address translation, not only in the IP header but also in the data segment of the packet. If the packet was not correctly address translated before it entered the tunnel due to embedded IP addresses, when the packet exits the tunnel the remote application will not receive the correct IP address embedded in the data segment. In this case, it is likely that the application will fail to function properly. Many remote-access VPN clients today support the ability to use a virtual address assigned by the headend terminating VPN device. Devices at the remote site may connect to the remote access client using this virtual address. This is actually carried out by one-to-one address translating all packets traversing the tunnel. If the VPN client does not address translate packets correctly or a new application arrives that is not yet supported, the application might not function.

Use address ranges at your sites and remote access VPN client virtual address pools that do not overlap with the addresses of other devices you will connect via IPSec. If this is not possible, use NAT only in this scenario to allow for connectivity. Do not address hide the public peer addresses of the VPN devices because it provides no real security value-add and may cause connectivity problems.

Quality of Service

The goal of quality of service (QoS) is to provide more efficient and predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network. QoS prioritizes voice, data, and web traffic to ensure that mission-critical applications get the service they require. Benefits to be derived from QoS include the following:

- Control over resources—You have control over which resources (bandwidth, equipment, wide-area facilities, and so on) are being used. As an example, you can limit the bandwidth consumed over a backbone link by FTP transfers or give priority to an important database access.
- More efficient use of network resources—Using Cisco's network analysis management and accounting tools, you will know what your network is being used for and that you are servicing the most important traffic to your business.
- Tailored services—The control and visibility provided by QoS enables Internet service providers to offer carefully tailored grades of service to their customers.
- Coexistence of mission-critical applications—Cisco's QoS technologies make certain that your WAN is used efficiently by mission- critical applications that are most important to your business; that bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available; and that other applications using the link get their fair service without interfering with mission-critical traffic.
- Foundation for a fully integrated network in the future—Implementing Cisco QoS technologies in your network now is a good first step toward the fully integrated multimedia network needed in the near future. For example, you can implement weighted fair queuing today and get its immediate benefit of increasing service predictability and IP Precedence signaling for traffic differentiation. You reap additional benefits in the future, because weighted fair queuing is Resource Reservation Protocol (RSVP) enabled, thereby allowing you to take advantage of dynamically signaled QoS from the inevitable coming wave of RSVP-enabled applications.

See the "Related Documentation" section on page xi for information on finding additional information on Cisco IOS QoS benefits, features, and application examples.

Network Intrusion Detection System

A Network Intrusion Detection Systems (NIDS) is a technology that can be used to reduce the risk associated with extending the security perimeter. NIDS carries out two primary functions in VPN designs.

First, NIDS can be used after encryption to validate that only encrypted traffic is sent and received by VPN devices. By tuning a NIDS to alarm on any non-VPN packet, you can validate that only encrypted packets are flowing over the network. This guards against any misconfiguration of the VPN devices that could inadvertently allow unencrypted traffic through the device.

Second, NIDS can be used to analyze traffic coming from, or destined to, the VPN device. Here NIDS will detect attacks coming through the VPN from remote sites or remote users. Since we know the traffic origin, and the chances it is spoofed are low, any attack can be met with a strong response from the NIDS. This can include shunning, or TCP resets, as appropriate. NIDS is critical in most VPN environments as most VPN security policies dictate that L3 and L4 access over a VPN should be fairly ubiquitous. This increases the reliance on NIDS to catch and stop most of the attacks from remote sites.

While the benefits of NIDS are compelling, NIDS significantly decreases network throughput, because it inspects every single packet. In a headend environment, consider using alternatives to NIDS. For example, in an overlay network environment (see the "Integrated versus Overlay Design" section on page 2-4), the decrease in performance associated with NIDS can be mitigated by designating a device other than the Cisco 7200 series router, such as the Cisco Intrusion Detection System (CIDS), to perform NIDS functions.

Split Tunneling

Split tunneling occurs when a remote VPN user or site is allowed to access a public network (the Internet) at the same time that they access the private VPN network without placing the public network traffic inside the tunnel first. If split tunneling were disabled, the remote VPN user or site would need to pass all traffic through the VPN headend where it could be decrypted and inspected before being sent out to the public network. Therefore, enabling split tunneling can increase the traffic throughput of your VPN, but poses a security risk if the remote user does not have a personal firewall. Despite the benefit of sending less traffic through the Cisco 7200 series router, Cisco does not recommend enabling split tunneling unless the remote user has sufficient firewall protection.

Network Resiliency

Network resiliency, or redundancy, enables remote sites to locate another tunneling peer if the primary headend peer is unreachable, or if there is a permanent loss of IP connectivity between peers. Consider network resiliency in both the network configuration and in the decision to use GRE tunnels, IPSec tunnels, or tunnels which utilize IPSec inside GRE. Resiliency can be achieved by properly utilizing and configuring GRE tunnels, IKE keepalives, and Hot Standby Routing Protocol (HSRP) with Reverse Route Injection (RRI).

This section contains the following topics:

Headend Failover

Headend failover ensures that network traffic will be routed through a backup Cisco 7200 series router if the primary Cisco 7200 series router should fail. GRE and IKE keepalives are the two primary means of attaining headend failover in Cisco IOS VPNs.

GRE

For VPN resilience, the remote site should be configured with two GRE tunnels, one to the primary headend Cisco 7200 series router, and the other to the backup headend Cisco 7200 series router. If the GRE tunnels are secured with IPSec, each tunnel has its own IKE SA and a pair of IPSec SAs. Since GRE can carry multicast and broadcast traffic, it is possible and very desirable to configure a routing protocol for these virtual links. Once a routing protocol is configured, the failover mechanism comes

automatically. The hello/keepalive packets, such as IKE keepalives, sent by the routing protocol over the GRE tunnels provide a mechanism to detect the loss of connectivity. In other words, if the primary GRE tunnel is lost, the remote site will detect this event by the loss of the routing protocol hello packets.

Once virtual-link loss is detected, the routing protocol will choose the next best route; the backup GRE tunnel will be chosen. Hence, the second part of VPN resilience is obtained by the automatic behavior of the routing protocol. Since the backup GRE tunnel is already up and secured, the failover time is determined by the hello packet mechanism and the convergence time of the routing protocol.

Aside from providing a failover mechanism, GRE tunnels provide the ability to encrypt multicast and broadcast packets and non-IP protocols with IPSec. They also provide enhanced performance and scalability for site-to-site VPN services. Since GRE tunnels are unique interfaces, they can each be assigned their own crypto maps. When the headend router needs to send a packet on the VPN, it first makes a routing decision to send it out an interface and then does a search of the SPI table to find the corresponding SA. With GRE tunnels, the router must make a routing decision across a multitude of GRE interfaces. Once the GRE tunnel is chosen, there are only a few SAs to choose from.

GRE tunnels can encapsulate clear text traffic, which enables the passage of routing updates to peer routers. Passage of routing updates provides reachability information between peers. It also enables detection of a secondary peer in the case of a loss of reachability for the primary peer. IPSec can be applied to the GRE tunnel packet to provide encryption for transport security.

IKE Keepalives

IKE keepalives, or hello packets, are a component of IPSec that tracks reachability of peers by sending hello packets between peers. In the case of loss of reachability to a peer, a tunnel is established with a predefined backup or secondary peer.

During the typical life of the IKE Security Association (SA), as defined by the RFCs, packets are only exchanged over this SA when an IPSec quick mode (QM) negotiation is required at the expiration of the IPSec SAs. For a Cisco IOS device, the default lifetime of an IKE SA is 24 hours and that of an IPSec SA is one hour. There is no standards-based mechanism for either type of SA to detect the loss of a peer, except when the QM negotiation fails. These facts imply that for IOS defaults, an IPSec termination point could be forwarding data into a black hole for as long as one hour before the protocol detects a loss of connectivity.

By implementing a keepalive feature over the IKE SA in Cisco IOS software, Cisco has provided network designers with a simple and non-intrusive mechanism for detecting loss of connectivity between two IPSec peers. The keepalive packets are sent every 10 seconds by default. Once three packets are missed, an IPSec termination point concludes that it has lost connectivity with its peer.

To reestablish connectivity, the IPSec termination point must have at least two IPSec peer addresses in its crypto map statement. The IPSec termination point will send out a main mode (MM) request to initiate the MM and quick mode (QM) negotiations with the second peer in its list. This type of functionality is available in all IOS devices that support the IPSec feature set.

IKE keepalives are suggested for use with devices that do not support GRE.

RRI with HSRP

In environments where redundant VPN devices using IKE keepalives for resiliency are present, be sure to track which device has the active IPSec connection with a remote peer to ensure tunnels are not duplicated across devices. Duplication of tunnels results in a mismatch of IPSec policy and the dropping of traffic. RRI and HSRP are two IOS features which, when used together, increase the resiliency of networks using IKE keepalives.

VPN Reverse Route Injection (RRI) is a new IOS feature that resolves the duplicate tunnel problem by injecting a static route for advertisement on the network. It is based on which device currently holds the IPSec session for a specific peer. Advertising this route ensures return IPSec traffic associated with the specific session will be routed through the device that has the active IPSec session.

The primary benefits of RRI are that it enables the routing of IPSec traffic to a specific VPN headend device in environments with multiple (redundant) VPN headend devices, and ensures predictable failover time of remote sessions between headend devices when using IKE keepalives.

HSRP complements the new RRI feature in attaining network resiliency. Using HSRP, a set of routers work in concert to present the illusion of a single virtual router with a virtual IP address that is linked to real IP addresses. The hosts on the network recognize the virtual router and IP address as the only router and IP address. The set of routers that comprises the virtual router is known as an HSRP group, or a standby group. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the active router. Another router is elected as the standby router. In the event that the active router fails, the standby router assumes the packet forwarding duties of the active router. Although an arbitrary number of routers may run HSRP, only the active router forwards the packets sent to the virtual router.

To minimize network traffic, only the active and the standby routers send periodic HSRP messages once the protocol has completed the election process. If the active router fails, the standby router takes over as the active router. If the standby router fails or becomes the active router, another router is elected as the standby router. RRI then informs peers of the active router, ensuring that peers use the active tunnel that HSRP has established.

While HSRP and RRI can be used in conjunction with each other for maximum network resiliency, they can also be used separately.

VPN Performance Optimization Considerations

Several key considerations can maximize the performance of your VPN. For a further discussion of each subject, you can read the referenced documentation.

This section contains the following topics:

Generic Switching Paths

Choose the best switching path available (from fastest to slowest): CEF, optimum, or fast. Enabling CEF will lead to the best performance. If you configure multiple switching paths such as fast-switching and CEF on the same interface, the router will try all of them from best to worst (starting from CEF and ending with process-switching). Choosing one switching path will increase network performance by eliminating the CPU overhead associated with trying all of them.

Fragmentation

Avoid fragmentation at all costs. Packet reassembly is resource intensive from a CPU and memory allocation perspective, and decreases network performance. Allowing fragmented packets into your network also creates security concerns. Fragmented IPSec packets require reassembly before the packets can undergo integrity validation and decryption.

Fragmentation can typically be avoided, as it usually occurs when an encapsulated packet, sent over a tunnel, is too large to fit on the smallest link on the tunnel path. As long as filtering does not block the Internet Control Message Protocol (ICMP) messages, path maximum transmission unit discovery (PMTUD) will determine the maximum MTU that a host can use to send a packet through the tunnel without causing fragmentation.

To allow PMTUD in your network, do not filter ICMP message Type 3, Code 4. If ICMP filtering occurs and is out of your administrative control, you will have to either manually set the MTU lower on the VPN termination device and allow PMTUD locally, or clear the Don't Fragment (DF) bit and force fragmentation. In this scenario, packets generated by hosts that do not support PMTUD, and have not set the DF bit in the IP header, will undergo fragmentation before IPSec encapsulation. Packets generated by hosts that do support PMTUD will use it locally to match the statically configured MTU on the tunnel. If you manually set the MTU on the tunnel, you must set it low enough to allow packets to pass through the smallest link on the path. Otherwise, the packets that are too large to fit will be dropped, and if ICMP filtering is in place, no feedback will be provided.

Remember that multiple layers of encapsulation will add layers of overhead to the packet. For example, GRE and ESP tunneling protocols are used together frequently. In this scenario, GRE adds 24 bytes of overhead to the packet before it undergoes encapsulation again by ESP. ESP, when using 3DES and SHA, then adds 56 bytes of additional overhead. Use of ESP and GRE to support PMTUD reduces the likelihood of fragmentation.

Depending on the VPN termination device, the manner in which you should set the MTU on the tunnel varies. Options include changing the MTU through the tunnel interface (routers), the TCP maximum segment size (firewalls), policy routing (routers), clear/set/copy DF bit (routers), OS application level (VPN clients), and physical/logical interfaces (any VPN device).

IKE Key Lifetimes

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New SAs are negotiated before current SAs expire.

To save setup time for IPSec, and thereby optimize VPN performance, configure a longer IKE SA lifetime. However, the shorter the lifetime, the more secure the IKE negotiation is likely to be.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is shorter than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior:

If the two peer’s policies’ lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter, and the shorter lifetime will be used.

IKE Keepalives

IKE keepalive settings can aid in optimizing VPN performance. By Cisco IOS default, keepalives are sent in 10 second intervals. A longer interval between keepalives reduces CPU usage, thereby increasing network performance. There is, however, a trade-off. The longer the interval, the longer it will take to detect a loss of connectivity. This risk can be mitigated by implementing RRI and/or HSRP. Refer to the "Network Resiliency" section on page 2-10, for a discussion of RRI and HSRP failover mechanisms.

Practical VPN Suggestions

The following are additional considerations you might implement when configuring a VPN on your Cisco 7200 series router:

- Syslog—Set up a syslog host, such as a CiscoWorks Essentials Workstation, and configure all the routers in the network to use the syslog host. By logging all syslog messages from the routers, you can determine when significant events, like configuration changes, occurred.
- Telnet and console access—In client-initiated or NAS-initiated access VPN environments, implement TACACS+ or Remote Access Dial-In User Service (RADIUS) security for Telnet and console access to the router. Doing so logs all access to the router. The addition of access lists to only allow Telnet access from particular source IP addressees helps to secure the router.
- Access lists—Use access list numbers and names consistently to help manage and troubleshoot configurations.
- Template configurations—Use a configuration template when deploying many routers that require consistent configurations.
- Tunneling—Observe the following when configuring tunneling:
  - To avoid anomalies that occur on physical interfaces, configure each tunnel source and destination on a loopback interface. A loopback interface is a virtual interface that is always up and allows routing protocols to stay up even if the physical interface is down.
  - Process switching and fast switching of the GRE, IPSec, L2F, and L2TP tunneling protocols, and Cisco Express Forwarding (CEF) of the IPSec tunneling protocol is supported on Cisco 7200 series router in Cisco IOS Release 12.0(4)XE or a later 12.1E software release, or Cisco IOS Release 12.0(6)T or a later 12.0 T software release.
  - Be careful not to violate access control lists. You can configure a tunnel with a source and destination that are not restricted by firewall routers.
  - Routing protocols that make their decisions based solely on hop count will often prefer a tunnel over a multipoint real link. A tunnel might appear to be a one-hop, point-to-point link and have the lowest-cost path, but may actually cost more.
- Firewall—Observe the following when configuring Cisco IOS firewall features (when configuring your Cisco 7200 series router as a firewall):
  - When setting passwords for privileged access to the firewall, use the **enable secret** command rather than the **enable password** command, which does not have as strong an encryption algorithm.
  - Configure a password on the console port. In authentication, authorization, and accounting (AAA) environments, use the same authentication for the console as for elsewhere. In a non-AAA environment, at a minimum, configure the **login** and **password** *password* commands.

- Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a *break* on the console port might render total control of the firewall, even with access control configured, to a hacker.
- Apply access lists and password protection to all virtual terminal ports. Use access lists to limit who can Telnet into your router.
- Do not enable any local service (such as Simple Network Management Protocol [SNMP] or Network Time Protocol [NTP]) that you do not plan to use. Cisco Discovery Protocol (CDP) and NTP are on by default, and you should turn these off if you do not need them.

  To turn off CDP, enter the **no cdp run** global configuration command. To turn off NTP, enter the **ntp disable** interface configuration command on each interface not using NTP.

  If you must run NTP, configure NTP only on required interfaces, and configure NTP to listen only to certain peers.

  Any enabled service could present a potential security risk. A determined, hostile party might be able to find creative ways to misuse the enabled services to access the firewall or the network.

  For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring access lists to deny packets for the services at specific interfaces.
- Protect against spoofing: protect the networks on both sides of the firewall from being spoofed from the other side. You could protect against spoofing by configuring input access lists at all interfaces to pass only traffic from expected source addresses and to deny all other traffic.

  You should also disable source routing. For IP, enter the **no ip source-route** global configuration command. If you disable source routing at *all* routers, it helps prevent spoofing.

  You should also disable minor services. For IP, enter the **no service tcp-small-servers** and **no service udp-small-servers** global configuration commands.
- Prevent the firewall from being used as a relay by configuring access lists on any asynchronous Telnet ports.
- Normally, you should disable directed broadcasts for all applicable protocols on your firewall and on all your other routers. For IP, use the **no ip directed-broadcast** command. Rarely, some IP networks do require directed broadcasts; if this is the case, do not disable directed broadcasts.

  Directed broadcasts can be misused to multiply the power of denial-of-service attacks, because every denial-of-service packet sent is broadcast to every host on a subnet. Furthermore, some hosts have other intrinsic security risks present when handling broadcasts.
- Configure the **no proxy-arp** command to prevent internal addresses from being revealed. (This is important to do if you do not already have NAT configured to prevent internal addresses from being revealed).
- Whenever possible, keep the firewall in a secured (locked) room.

To access the documentation for the applications discussed in this section on Cisco.com, refer to the following URL:

http://www.cisco.com/en/US/products/sw/netmgtsw/index.html

Network Management Considerations

This section contains the following topics:

Tunnel Endpoint Discovery

Tunnel Endpoint Discovery (TED) enhances the IPSec feature. Defining a dynamic crypto map allows you to be able to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

TED allows IPSec to scale to large networks by reducing multiple encryptions, reducing the setup time, and allowing for simple configurations on participating peer routers. Each node has a simple configuration that defines the local network that the router protects and the required IPSec transforms.

TED mechanisms best function in partially or fully meshed networks, which require spoke-to-spoke connectivity on an infrequent basis.

IPSec MIB and Third Party Applications

The IPSec Management Information Base (MIB) feature allows users to configure and monitor their IPSec MIB tunnel tables and their trap notifications using Simple Network Management Protocol (SNMP). Utilizing a MIB can increase the performance of your network. It automates the gathering and organization of network management data, which would otherwise add significant CPU overhead to the Cisco 7200 series router.

This feature allows users to specify the desired size of a tunnel history table or a tunnel failure table. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also allows a router to send IPSec trap notifications, which are MIB related, to a random or specified host. A trap notification may be sent when a particular event, such as an error, occurs.

The primary benefit of IPSec MIB is that trap notifications can be sent only once and are discarded as soon as they are sent, thereby reducing traffic and creating lower overhead on your network. Third party MIB applications are available to monitor and control the management information base. One such example is HP Openview, which is a component of several Cisco network management products.

CHAPTER 3

Site-to-Site and Extranet VPN Business Scenarios

This chapter explains the basic tasks for configuring IP-based, site-to-site and extranet Virtual Private Networks (VPNs) on a Cisco 7200 series router using generic routing encapsulation (GRE) and IPSec tunneling protocols. Basic security, Network Address Translation (NAT), Encryption, Cisco IOS weighted fair queuing (WFQ), and extended access lists for basic traffic filtering are configured.

Note In this Guide, the term 'Cisco 7200 series router' implies that an Integrated Service Adaptor (ISA) or a VAM (VAM, VAM2, or VAM2+) is installed in the Cisco 7200 series router.

This chapter describes basic features and configurations used in a site-to-site VPN scenario. Some Cisco IOS security software features not described in this document can be used to increase performance and scalability of your VPN. For up-to-date Cisco IOS security software features documentation, refer to the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications for your Cisco IOS Release. For information on how to access the publications, see "Related Documentation" section on page xi.

This chapter includes the following sections:

Note Throughout this chapter, there are numerous configuration examples and sample configuration outputs that include unusable IP addresses. Be sure to use your own IP addresses when configuring your Cisco 7200 series router.

Scenario Descriptions

This section includes the following topics:

Site-to-Site Scenario

Figure 3-1 shows a headquarters network providing a remote office access to the corporate intranet. In this scenario, the headquarters and remote office are connected through a secure GRE tunnel that is established over an IP infrastructure (the Internet). Employees in the remote office are able to access internal, private web pages and perform various IP-based network tasks.

Note Although the site-to-site VPN scenario in this chapter is configured with GRE tunneling, a site-to-site VPN can also be configured with IPSec only tunneling.

Figure 3-1 Site-to-Site VPN Business Scenario

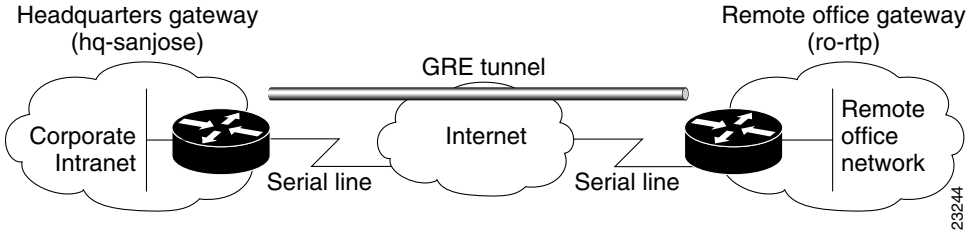
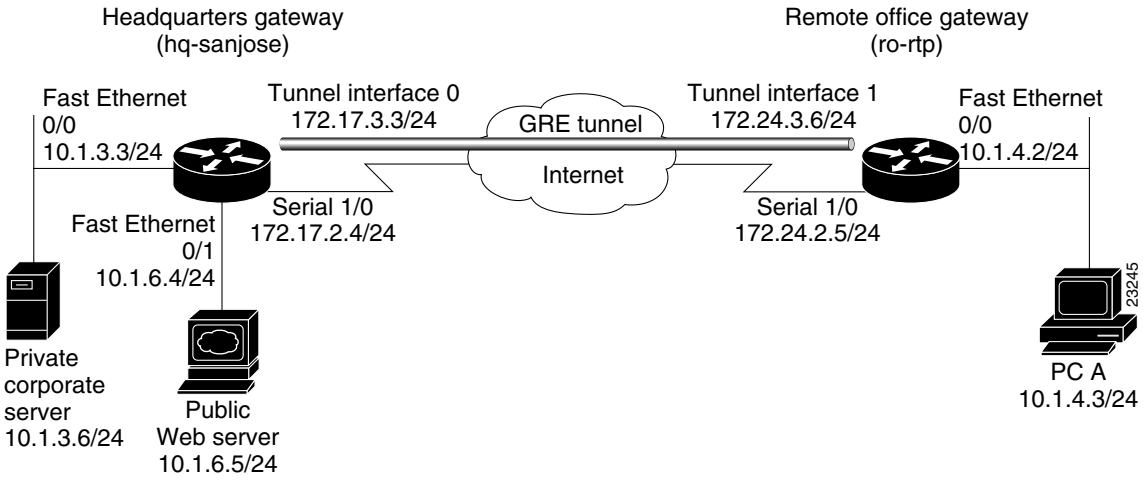


Figure 3-2 shows the physical elements of the scenario. The Internet provides the core interconnecting fabric between the headquarters and remote office routers. Both the headquarters and remote office are using a Cisco IOS VPN gateway (a Cisco 7200 series with an Integrated Service Adaptor (ISA) or VAM (VAM, VAM2, or VAM2+), a Cisco 2600 series router, or a Cisco 3600 series router).

Note VPN Acceleration Module (VAM) information for your Cisco 7200 series router can be found at http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_and_configuration_guides_list.html.

The GRE tunnel is configured on the first serial interface in chassis slot 1 (serial 1/0) of the headquarters and remote office routers. Fast Ethernet interface 0/0 of the headquarters router is connected to a corporate server and Fast Ethernet interface 0/1 is connected to a web server. Fast Ethernet interface 0/0 of the remote office router is connected to a PC client.

Figure 3-2 Site-to-Site VPN Scenario Physical Elements



The configuration steps in the following sections are for the headquarters router, unless noted otherwise. Comprehensive configuration examples for both the headquarters and remote office routers are provided in the "Comprehensive Configuration Examples" section on page 3-39.

Table 3-1 lists the physical elements of the site-to-site scenario.

Table 3-1 Physical Elements

Headquarters Network			Remote Office Network		
Site Hardware	**WAN IP Address**	**Ethernet IP Address**	**Site Hardware**	**WAN IP Address**	**Ethernet IP Address**
hq-sanjose	Serial interface 1/0: 172.17.2.4 255.255.255.0 Tunnel interface 0: 172.17.3.3 255.255.255.0	Fast Ethernet Interface 0/0: 10.1.3.3 255.255.255.0 Fast Ethernet Interface 0/1: 10.1.6.4 255.255.255.0	ro-rtp	Serial interface 1/0: 172.24.2.5 255.255.255.0 Tunnel interface 1: 172.24.3.6 255.255.255.0	Fast Ethernet Interface 0/0: 10.1.4.2 255.255.255.0
Corporate server	—	10.1.3.6	PC A	—	10.1.4.3
Web server	—	10.1.6.5			

Extranet Scenario

The extranet scenario introduced in Figure 3-3 builds on the site-to-site scenario by providing a business partner access to the same headquarters network. In the extranet scenario, the headquarters and business partner are connected through a secure IPSec tunnel and the business partner is given access only to the headquarters public server to perform various IP-based network tasks, such as placing and managing product orders.

Figure 3-3 Extranet VPN Business Scenario

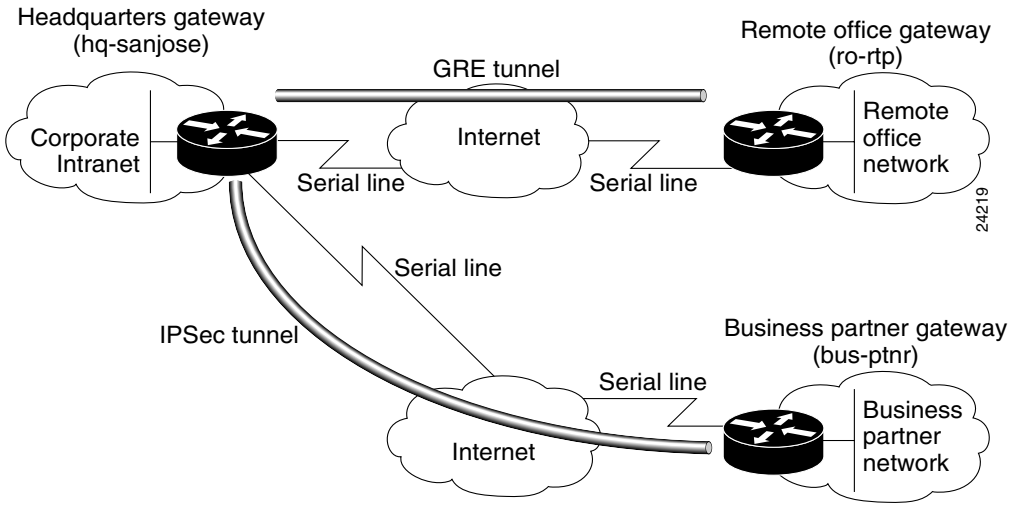
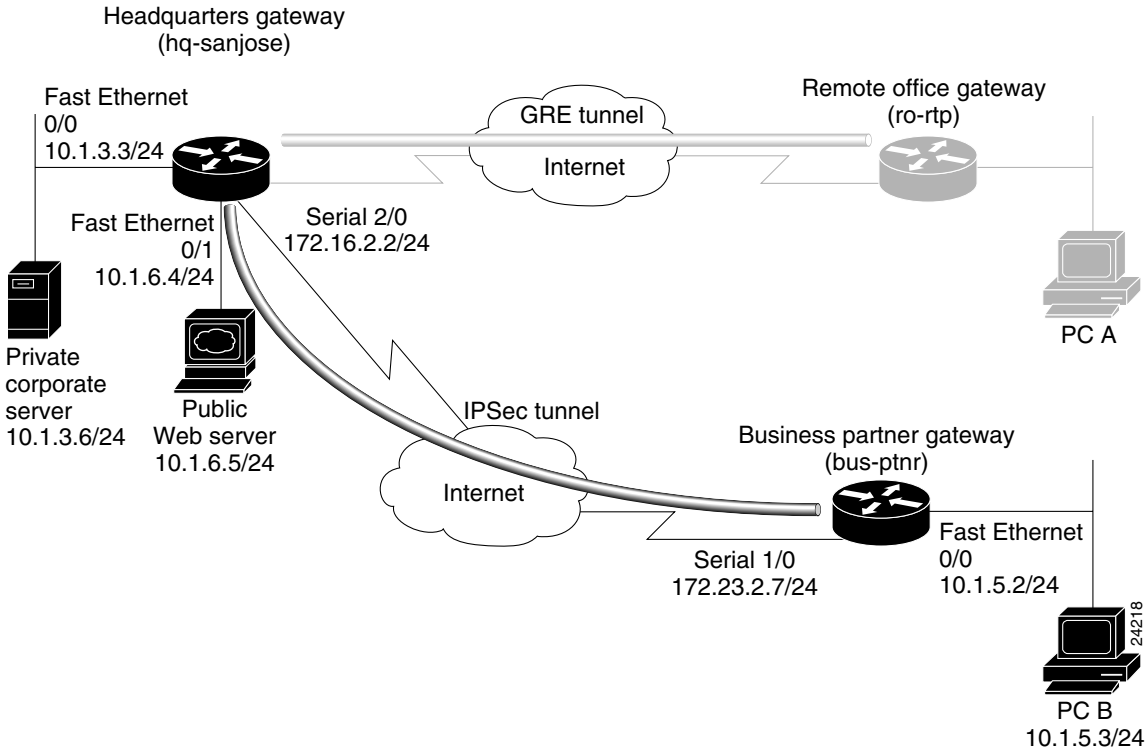


Figure 3-4 shows the physical elements of the scenario. As in the site-to-site business scenario, the Internet provides the core interconnecting fabric between the headquarters and business partner routers. Like the headquarters office, the business partner is also using a Cisco IOS VPN gateway (a Cisco 7200 series with an Integrated Service Adaptor (ISA) or VAM (VAM, VAM2, or VAM2+), a Cisco 2600 series router, or a Cisco 3600 series router).

Note VPN Acceleration Module (VAM) information for your Cisco 7200 series router can be found at http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_and_configuration_guides_list.html.

The IPSec tunnel between the two sites is configured on the second serial interface in chassis slot 2 (serial 2/0) of the headquarters router and the first serial interface in chassis slot 1 (serial 1/0) of the business partner router. Fast Ethernet interface 0/0 of the headquarters router is still connected to a private corporate server and Fast Ethernet interface 0/1 is connected to a public server. Fast Ethernet interface 0/0 of the business partner router is connected to a PC client.

Figure 3-4 Extranet VPN Scenario Physical Elements



The configuration steps in the following sections are for the headquarters router, unless noted otherwise. Comprehensive configuration examples for both the headquarters and business partner routers are provided in the "Comprehensive Configuration Examples" section on page 3-39.

Table 3-2 lists the extranet scenario's physical elements.

Table 3-2 Physical Elements

Headquarters Network			Business Partner Network		
Site Hardware	**WAN IP Address**	**Ethernet IP Address**	**Site Hardware**	**WAN IP Address**	**Ethernet IP Address**
hq-sanjose	Serial interface 2/0: 172.16.2.2 255.255.255.0	Fast Ethernet Interface 0/0: 10.1.3.3 255.255.255.0 Fast Ethernet Interface 0/1: 10.1.6.4 255.255.255.0	bus-ptnr	Serial interface 1/0: 172.23.2.7 255.255.255.0	Fast Ethernet Interface 0/0: 10.1.5.2 255.255.255.0
Corporate server	—	10.1.3.6	PC B	—	10.1.5.3
Web server	—	10.1.6.5[1]			

1. The inside local IP address of the headquarters network public server (10.1.6.5) is translated to inside global IP address 10.2.2.2 in the "Step 2—Configuring Network Address Translation" section on page 3-10.

Step 1—Configuring the Tunnel

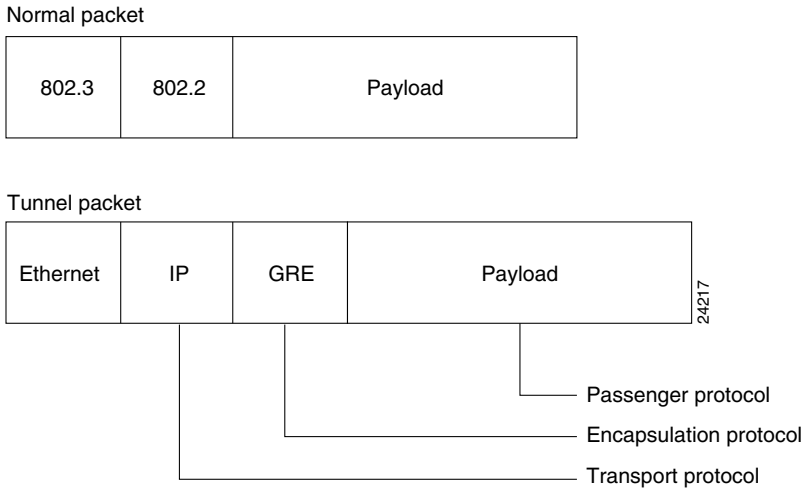
Tunneling provides a way to encapsulate packets inside of a transport protocol. Tunneling is implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface is not tied to specific "passenger" or "transport" protocols, but rather, it is an architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. Because tunnels are point-to-point links, you must configure a separate tunnel for each link.

Tunneling has the following three primary components:

- Passenger protocol, which is the protocol you are encapsulating (AppleTalk, Banyan VINES, Connectionless Network Service [CLNS], DECnet, IP, or Internetwork Packet Exchange [IPX]).
- Carrier protocol, such as the generic routing encapsulation (GRE) protocol or IPSec protocol.
- Transport protocol, such as IP, which is the protocol used to carry the encapsulated protocol.

Figure 3-5 illustrates IP tunneling terminology and concepts.

Figure 3-5 IP Tunneling Terminology and Concepts



This section contains the following topics:

- Configuring a GRE Tunnel
- Configuring an IPSec Tunnel

Configuring a GRE Tunnel

GRE is capable of handling the transportation of multiprotocol and IP multicast traffic between two sites, which only have IP unicast connectivity. The importance of using tunnels in a VPN environment is based on the fact that IPSec encryption only works on IP unicast frames. Tunneling allows for the encryption and the transportation of multiprotocol traffic across the VPN since the tunneled packets appear to the IP network as an IP unicast frame between the tunnel endpoints. If all connectivity must go through the home Cisco 7200 series router , tunnels also enable the use of private network addressing across a service provider's backbone without the need for running the Network Address Translation (NAT) feature.

Network redundancy (resiliency) is an important consideration in the decision to use GRE tunnels, IPSec tunnels, or tunnels which utilize IPSec over GRE. GRE can be used in conjunction with IPSec to pass routing updates between sites on an IPSec VPN. GRE encapsulates the clear text packet, then IPSec (in transport or tunnel mode) encrypts the packet.This packet flow of IPSec over GRE enables routing updates, which are generally multicast, to be passed over an encrypted link. IPSec alone can not achieve this, because it does not support multicast.

Using redundant GRE tunnels protected by IPSec from a remote router to redundant headquarter routers, routing protocols can be employed to delineate the "primary" and "secondary" headquarter routers. Upon loss of connectivity to the primary router, routing protocols will discover the failure and route to the secondary Cisco 7200 series router, thereby providing network redundancy.

It is important to note that more than one router must be employed at HQ to provide resiliency. For VPN resilience, the remote site should be configured with two GRE tunnels, one to the primary HQ VPN router, and the other to the backup HQ VPN router.

This section contains basic steps to configure a GRE tunnel and includes the following tasks:

- Configuring the Tunnel Interface, Source, and Destination
- Verifying the Tunnel Interface, Source, and Destination

Configuring the Tunnel Interface, Source, and Destination

To configure a GRE tunnel between the headquarters and remote office routers, you must configure a tunnel interface, source, and destination on the headquarters and remote office routers. To do this, complete the following steps starting in global configuration mode.

Note The following procedure assumes the tunnel interface, source, and destination on the remote office router are configured with the values listed in Table 3-1.

	Command	Purpose
Step 1	`hq-sanjose(config)# interface tunnel 0` `hq-sanjose(config-if)# ip address 172.17.3.3 255.255.255.0`	Specify a tunnel interface number, enter interface configuration mode, and configure an IP address and subnet mask on the tunnel interface. This example configures IP address and subnet mask 172.17.3.3 255.255.255.0 for tunnel interface 0 on the headquarters router.
Step 2	`hq-sanjose(config-if)# tunnel source 172.17.2.4 255.255.255.0`	Specify the tunnel interface source address and subnet mask. This example uses the IP address and subnet mask of T3 serial interface 1/0 of the headquarters router.
Step 3	`hq-sanjose(config-if)# tunnel destination 172.24.2.5 255.255.255.0`	Specify the tunnel interface destination address. This example uses the IP address and subnet mask of T3 serial interface 1/0 of the remote office router.
Step 4	`hq-sanjose(config-if)# tunnel mode gre ip`	Configure GRE as the tunnel mode. GRE is the default tunnel encapsulation mode, so this command is considered optional.

Step 5	`hq-sanjose(config)# interface tunnel 0`
	`hq-sanjose(config-if)# no shutdown`
	`%LINK-3-UPDOWN: Interface Tunnel0, changed state to up`
		Bring up the tunnel interface.[1]

Step 6	`hq-sanjose(config-if)# exit` `hq-sanjose(config)# ip route 10.1.4.0 255.255.255.0 tunnel 0`	Exit back to global configuration mode and configure traffic from the remote office network through the tunnel. This example configures traffic from the remote office Fast Ethernet network (10.1.4.0 255.255.255.0) through GRE tunnel 0.

1. This command changes the state of the tunnel interface from administratively down to up.

Note When configuring GRE, you must have only Cisco routers or access servers at both ends of the tunnel connection.

Verifying the Tunnel Interface, Source, and Destination

To verify the configuration:

- Enter the **show interfaces tunnel 0** EXEC command to view the tunnel interface status, configured IP addresses, and encapsulation type. Both the interface and the interface line protocol should be "up."

```
ski03_7206#show interfaces tunnel 1
Tunnel1 is up, line protocol is up
Hardware is Tunnel
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 1101:1::1, destination 1501:1::1
Tunnel protocol/transport IPSEC/IPV6
Tunnel TTL 255
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPSec (profile "tunpro")
Last input 00:08:23, output 00:04:28, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 3
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
39 packets input, 22734 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
57 packets output, 30130 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

- Try pinging the tunnel interface of the remote office router (this example uses the IP address of tunnel interface 1 [172.24.3.6]):

```
hq-sanjose(config)# ping 172.24.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.3.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

Tip If you have trouble, make sure you are using the correct IP address and that you enabled the tunnel interface with the **no shutdown** command.

Configuring an IPSec Tunnel

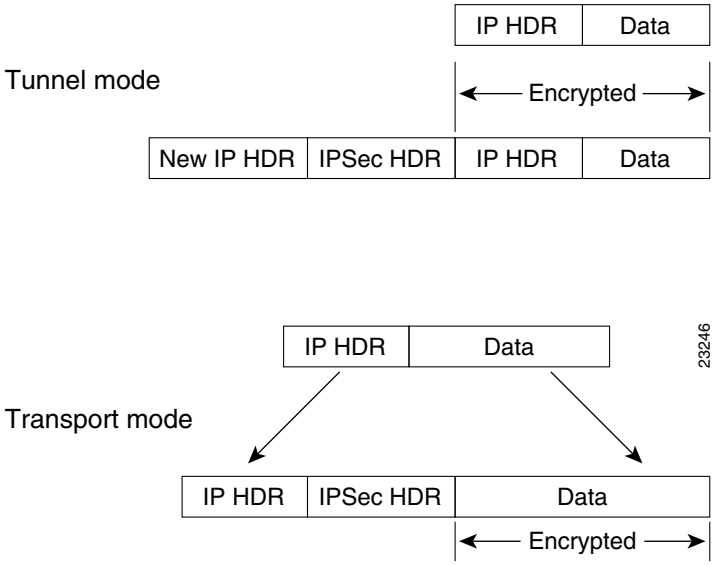
IPSec can be configured in tunnel mode or transport mode. IPSec tunnel mode can be used as an alternative to a GRE tunnel, or in conjunction with a GRE tunnel. In IPSec tunnel mode, the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPSec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. Tunnel

mode protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the packets passing through the tunnel, even if they are the same as the tunnel endpoints.

Note IPSec tunnel mode configuration instructions are described in detail in the "Configuring IPSec and IPSec Tunnel Mode" section on page 3-22.

In IPSec transport mode, only the IP payload is encrypted, and the original IP headers are left intact. (See Figure 3-6.) This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. With this capability, you can enable special processing in the intermediate network based on the information in the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, by passing the IP header in the clear, transport mode allows an attacker to perform some traffic analysis. (See the "Defining Transform Sets and Configuring IPSec Tunnel Mode" section on page 3-23 for an IPSec transport mode configuration example.)

Figure 3-6 IPSec in Tunnel and Transport Modes



Step 2—Configuring Network Address Translation

Note NAT is used if you have conflicting private address spaces in the extranet scenario. If you have no conflicting private address spaces, proceed to the "Step 3—Configuring Encryption and IPSec" section on page 3-14.

Network Address Translation (NAT) enables private IP internetworks with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. NAT is configured on the router at the border of a stub domain (referred to as the *inside network*) and a public network such as the Internet (referred to as the *outside network*). NAT translates the internal

local addresses to globally unique IP addresses before sending packets to the outside network. NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into classless interdomain routing (CIDR) blocks.

This section only explains how to configure *static translation* to translate internal local IP addresses into globally unique IP addresses before sending packets to an outside network, and includes the following tasks:

- Configuring Static Inside Source Address Translation
- Verifying Static Inside Source Address Translation

Static translation establishes a one-to-one mapping between your internal local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

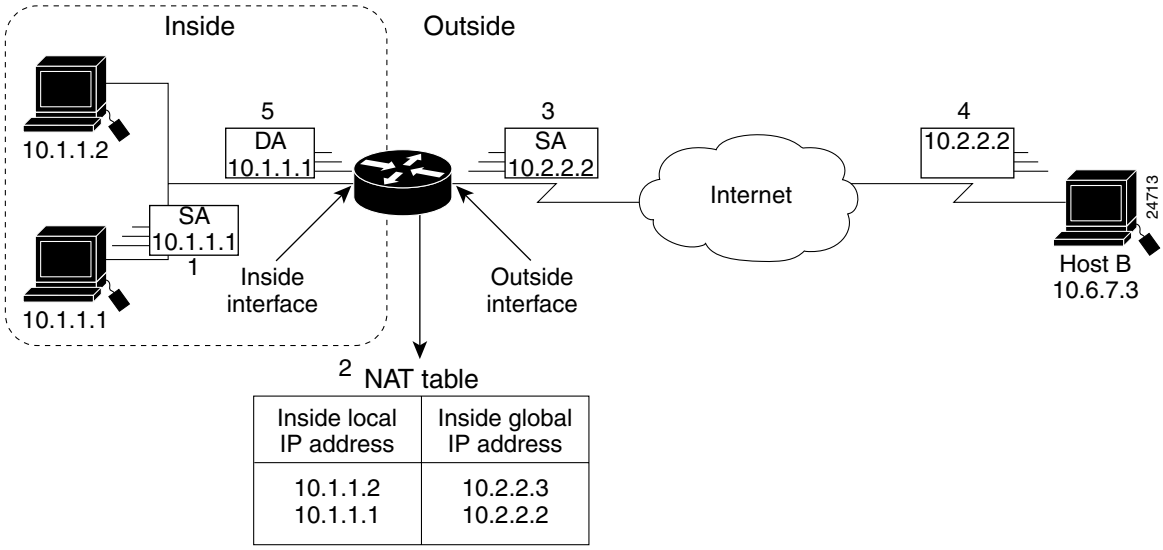
Note For detailed, additional configuration information on NAT—for example, instructions on how to configure *dynamic translation*—refer to the "Configuring IP Addressing" chapter in the N*etwork Protocols Configuration Guide, Part 1*. NAT is also described in RFC 1631.

NAT uses the following definitions:

- **Inside local address**—The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.
- **Inside global address**—A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.
- **Outside local address**—The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from address space routable on the inside.
- **Outside global address**—The IP address assigned to a host on the outside network by the host owner. The address was allocated from a globally routable address or network space.

Figure 3-7 illustrates a router that is translating a source address inside a network to a source address outside the network.

Figure 3-7 NAT Inside Source Translation



The following process describes inside source address translation, as shown in Figure 3-7:

1. The user at Host 10.1.1.1 opens a connection to Host B.
2. The first packet that the router receives from Host 10.1.1.1 causes the router to check its NAT table.

   If a static translation entry was configured, the router goes to Step 3.

   If no translation entry exists, the router determines that source address (SA) 10.1.1.1 must be translated dynamically, selects a legal, global address from the dynamic address pool, and creates a translation entry. This type of entry is called a *simple entry*.
3. The router replaces the inside local source address of Host 10.1.1.1 with the translation entry global address, and forwards the packet.
4. Host B receives the packet and responds to Host 10.1.1.1 by using the inside global IP destination address (DA) 10.2.2.2.
5. When the router receives the packet with the inside global IP address, it performs a NAT table lookup by using the inside global address as a key. It then translates the address to the inside local address of Host 10.1.1.1 and forwards the packet to Host 10.1.1.1.
6. Host 10.1.1.1 receives the packet and continues the conversation. The router performs Steps 2 through 5 for each packet.

This section contains the following topics:

- Configuring Static Inside Source Address Translation
- Verifying Static Inside Source Address Translation

Configuring Static Inside Source Address Translation

To configure static inside source address translation, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# ip nat inside source static 10.1.6.5 10.2.2.2`	Establish static translation between an inside local address and an inside global address. This example translates inside local address 10.1.6.5 (the server) to inside global address 10.2.2.2.
Step 2	`hq-sanjose(config)# interface fastethernet 0/1`	Specify the inside interface. This example specifies Fast Ethernet interface 0/1 on the headquarters router.
Step 3	`hq-sanjose(config-if)# ip nat inside`	Mark the interface as connected to the inside.
Step 4	`hq-sanjose(config-if)# interface serial 2/0`	Specify the outside interface. This example specifies serial interface 2/0 on the headquarters router.
Step 5	`hq-sanjose(config-if)# ip nat outside`	Mark the interface as connected to the outside.
Step 6	`hq-sanjose(config-if)# exit` `hq-sanjose(config)#`	Exit back to global configuration mode.

The previous steps are the minimum you must configure for static inside source address translation. You could configure multiple inside and outside interfaces.

Verifying Static Inside Source Address Translation

To verify the configuration:

- Enter the **show ip nat translations verbose** EXEC command to see the global and local address translations and to confirm static translation is configured.

```
hq-sanjose# show ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside
global
--- 10.2.2.2           10.1.6.5            ---                ---
    create 00:10:28, use 00:10:28, flags:
static
```

- Enter the **show running-config** EXEC command to see the inside and outside interfaces, global and local address translations, and to confirm static translation is configured (display text has been omitted from the following sample output for clarity).

```
hq-sanjose# show running-config

interface FastEthernet0/1
 ip address 10.1.6.5 255.255.255.0
 no ip directed-broadcast
 ip nat inside

interface serial2/0
 ip address 172.16.2.2 255.255.255.0
 ip nat outside

ip nat inside source static 10.1.6.5 10.2.2.2
```

Step 3—Configuring Encryption and IPSec

IPSec is a framework of open standards, developed by the Internet Engineering Task Force (IETF), 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 Cisco 7200 series routers, or between a security Cisco 7200 series router and a host.

IKE is a hybrid security protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, establishes IPSec keys, and provides IKE keepalives. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, ease of configuration for the IPSec standard, and keepalives, which are integral in achieving network resilience when configured with GRE.

Certification authority (CA) interoperability is provided by the ISM in support of the IPSec standard. It 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.

The CA must be properly configured to issue certificates. You must also configure the peers to obtain certificates from the CA. Configure this certificate support as described in the "Configuring Certification Authority Interoperability" chapter of the *Cisco IOS Security Configuration Guide* (see "Related Documentation" section on page xi for additional information on how to access these documents.

To provide encryption and IPSec tunneling services on a Cisco 7200 series router, you must complete the following tasks:

- Configuring IKE Policies
- Verifying IKE Policies
- Configuring IPSec and IPSec Tunnel Mode
- Configuring Crypto Maps

Note You can configure a static crypto map, create a dynamic crypto map, or add a dynamic crypto map into a static crypto map. Refer to the "Configuring Crypto Maps" section on page 3-24.

Optionally, you can configure CA interoperability. This guide does not explain how to configure CA interoperability on your Cisco 7200 series router. Refer to the "IP Security and Encryption" part of the *Security Configuration Guide* and the *Cisco IOS Security Command Reference* publication for detailed information on configuring CA interoperabilty. See "Related Documentation" section on page xi for additional information on how to access these publications.

Note This section only contains basic configuration information for enabling encryption and IPSec tunneling services. Refer to the "IP Security and Encryption" part of the Cisco IOS *Security Configuration Guide* and the *Security Command Reference* publications for detailed configuration information on IPSec, IKE, and CA. See "Related Documentation" section on page xi for information on how to access these publications.

Refer to the *Integrated Service Adapter and Integrated Service Module Installation and Configuration* publication for detailed configuration information on the ISM.

This section contains the following topics:

Configuring IKE Policies

Internet Key Exchange (IKE) is enabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces in the router. You must create IKE policies at each peer. An IKE policy defines a combination of security parameters to be used during the IKE negotiation.

You can create multiple IKE policies, each with a different combination of parameter values. If you do not configure any IKE policies, the router uses the default policy, which is always set to the lowest priority, and which contains each parameter default value.

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 Diffie-Hellman parameter values as one of the policies on the remote peer. If you do not specify a value for a parameter, the default value is assigned.

IKE keepalives (or "hello packets") are required to detect a loss of connectivity, providing network resiliency. If your HQ employs more than two routers and utilizes IPSec, you can specify the length of keepalive packets or use the default time period of 10 seconds. To specify the interval length at which keepalive packets are to be sent, use the **`cry isakmp keepalive`** command, as exemplified in Step 2 of the "Creating IKE Policies" section on page 3-16.

Note The default policy and the default values for configured policies do not show up in the configuration when you issue a **show running-config** EXEC command. Instead, to see the default policy and any default values within configured policies, use the **show crypto isakmp policy** EXEC command.

This section contains basic steps to configure IKE policies and includes the following tasks:

Creating IKE Policies

To create an IKE policy, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto isakmp policy 1`	Enter config-isakmp command mode and identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) This example configures policy 1.
Step 2	`hq-sanjose(config)# cry isakmp keepalive 12 2`	Optional step: Specify the time interval of IKE keepalive packets (default is 10 seconds), and the retry interval when the keepalive packet failed. This example configures the keepalive interval for 12 seconds and the retry interval for 2 seconds.
Step 3	`hq-sanjose(config-isakmp)# encryption des`	Specify the encryption algorithm—56-bit Data Encryption Standard (DES [**des**]) or 168-bit Triple DES (**3des**). This example configures the DES algorithm, which is the default.
Step 4	`hq-sanjose(config-isakmp)# hash sha`	Specify the hash algorithm—Message Digest 5 (MD5 [**md5**]) or Secure Hash Algorithm (SHA [**sha**]). This example configures SHA, which is the default.
Step 5	`hq-sanjose(config-isakmp)# authentication pre-share`	Specify the authentication method—pre-shared keys (**pre-share**), RSA[1] encrypted nonces (**rsa-encr**), or RSA signatures (**rsa-slg**). This example configures pre-shared keys. The default is RSA signatures.
Step 6	`hq-sanjose(config-isakmp)# group 1`	Specify the Diffie-Hellman group identifier—768-bit Diffie-Hellman (**1**) or 1024-bit Diffie-Hellman (**2**). This example configures 768-bit Diffie-Hellman, which is the default.
Step 7	`hq-sanjose(config-isakmp)# lifetime 86400`	Specify the security association's lifetime—in seconds. This example configures 86400 seconds (one day).
Step 8	`hq-sanjose(config-isakmp)# exit` `hq-sanjose(config)#`	Exit back to global configuration mode.

1. RSA = Rivest, Shamir, and Adelman.

Additional Configuration Required for IKE Policies

Depending on which authentication method you specify in your IKE policies, you need to complete an additional companion configuration before IKE and IPSec can successfully use the IKE policies.

Each authentication method requires an additional companion configuration as follows:

- RSA signatures method:

  If you specify RSA signatures as the authentication method in a policy, you must configure the peers to obtain certificates from a certification authority (CA). (And, of course, the CA must be properly configured to issue the certificates.) Configure this certificate support as described in the "Configuring Certification Authority Interoperability" chapter of the *Cisco IOS Security Configuration Guide.*

The certificates are used by each peer to securely exchange public keys. (RSA signatures require that each peer has the remote peer's public signature key.) When both peers have valid certificates, they will automatically exchange public keys with each other as part of any IKE negotiation in which RSA signatures are used.

- RSA encrypted nonces method:

  If you specify RSA encrypted nonces as the authentication method in a policy, you need to ensure that each peer has the other peers' public keys.

  Unlike RSA signatures, the RSA encrypted nonces method does not use certificates to exchange public keys. Instead, you ensure that each peer has the others' public keys by doing the following:

  – Manually configure RSA keys as described in the "Configuring Internet Key Exchange Security Protocol" chapter of the *Cisco IOS Security Configuration Guide.*

  – Ensure that an IKE exchange using RSA signatures has already occurred between the peers. (The peers' public keys are exchanged during the RSA-signatures-based IKE negotiations.)

    To make this happen, specify two policies: a higher-priority policy with RSA encrypted nonces, and a lower-priority policy with RSA signatures. When IKE negotiations occur, RSA signatures will be used the first time because the peers do not yet have each others' public keys. Then, future IKE negotiations will be able to use RSA-encrypted nonces because the public keys will have been exchanged.

    Of course, this alternative requires that you have CA support configured.

- Pre-shared keys authentication method:

  If you specify pre-shared keys as the authentication method in a policy, you must configure these pre-shared keys as described in the "Configuring Pre-shared Keys" section on page 3-17."

- Digital certificate authentication method:

  If you specify digital certificates as the authentication method in a policy, the CA must be properly configured to issue certificates. You must also configure the peers to obtain certificates from the CA. Configure this certificate support as described in the "Configuring Certification Authority Interoperability" chapter of the *Cisco IOS Security Configuration Guide.*

  Digital certificates simplify authentication. You need only enroll each peer with the CA, rather than manually configuring each peer to exchange keys. Cisco recommends using digital certificates in a network of more than 50 peers.

If RSA encryption is configured and signature mode is negotiated, the peer will request both signature and encryption keys. Basically, the router will request as many keys as the configuration will support. If RSA encryption is not configured, it will just request a signature key.

Configuring Pre-shared Keys

To configure pre-shared keys, perform these steps at each peer that uses pre-shared keys in an IKE policy:

Step 1 Set each peer ISAKMP identity. Each peer identity should be set to either its host name or by its IP address. By default, a peer identity is set to its IP address.

Step 2 Specify the 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.

Note The following procedure is based on the "Site-to-Site Scenario" section on page 3-2. However, the same configuration commands can be used in an extranet scenario.

To specify pre-shared keys at a peer, complete the following steps in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto isakmp identity address`	**At the local peer**: Specify the ISAKMP identity (**address** or **hostname**) the headquarters router will use when communicating with the remote office router during IKE negotiations. This example specifies the **address** keyword, which uses IP address 172.17.2.4 (serial interface 1/0 of the headquarters router) as the identity for the headquarters router.
Step 2	`hq-sanjose(config)# crypto isakmp key test12345 address 172.24.2.5`	**At the local peer**: Specify the shared key the headquarters router will use with the remote office router. This example configures the shared key test12345 to be used with the remote peer 172.24.2.5 (serial interface 1/0 on the remote office router).
Step 3	`ro-rtp(config)# crypto isakmp identity address`	**At the remote peer**: Specify the ISAKMP identity (**address** or **hostname**) the remote office router will use when communicating with the headquarters router during IKE negotiations. Again, this example specifies the **address** keyword, which uses IP address 172.24.2.5 (serial interface 1/0 of the remote office router) as the identity for the remote office router.
Step 4	`ro-rtp(config)# crypto isakmp key test12345 address 172.17.2.4`	**At the remote peer**: Specify the shared key to be used with the local peer. This is the same key you just specified at the local peer. This example configures the shared key test12345 to be used with the local peer 172.17.2.4 (serial interface 1/0 on the headquarters router).

Note Set an ISAKMP identity whenever you specify pre-shared keys. The **address** keyword is typically used when there is only one interface (and therefore only one IP address) that will be used by the peer for IKE negotiations, and the IP address is known. Use the **hostname** keyword if there is more than one interface on the peer that might be used for IKE negotiations, or if the interface IP address is unknown (such as with dynamically-assigned IP addresses).

Configuring the Cisco 7200 Series Router for Digital Certificate Interoperability

To configure your Cisco 7200 series router to use digital certificates as the authentication method, use the following steps, beginning in global configuration mode. This configuration assumes the use of the IOS default ISAKMP policy, which uses DES, SHA, RSA signatures, Diffie-Hellman group 1, and a lifetime of 86,400 seconds. Cisco recommends using 3DES. Refer to the "Creating IKE Policies" section on page 3-16 for an ISAKMP configuration example which specifies 3DES as the encryption method.

Note This example only configures the head-end Cisco 7200 series router. Additionally, each peer must be enrolled with a CA. This configuration example does not configure the CA. CA configuration instructions should be obtained from your CA vendor.

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto ca identity name`	Declares a CA. The name should be the domain name of the CA. This command puts you into the ca-identity configuration mode.
Step 2	`hq-sanjose(config)# enrollment url url`	Specifies the URL of the CA. (The URL should include any nonstandard cgi-bin script location.)
Step 3	`hq-sanjose(config)# enrollment mode ra`	(Optional) Specifies RA mode if your CA system provides a registration authority (RA). The Cisco IOS software automatically determines the mode—RA or non-RA; therefore, if RA mode is used, this subcommand is written to NVRAM during "write memory."
Step 4	`hq-sanjose(ca-identity)# query url url`	Specifies the location of the LDAP server if your CA system provides an RA and supports the LDAP protocol.
Step 5	`hq-sanjose(ca-identity)# enrollment retry period minutes`	(Optional) Specifies that other peer certificates can still be accepted by your router even if the appropriate CRL is not accessible to your router.
Step 6	`hq-sanjose(ca-identity)# enrollment retry count number`	(Optional) Specifies how many times the router will continue to send unsuccessful certificate requests before giving up. By default, the router will never give up trying.
Step 7	`hq-sanjose(ca-identity)# crl optional`	(Optional) Specifies that other peers certificates can still be accepted by your router even if the appropriate CRL is not accessible to your router.
Step 8	`hq-sanjose(ca-identity)# exit`	Exits ca-identity configuration mode.

Verifying IKE Policies

To verify the configuration:

- Enter the **show crypto isakmp policy** EXEC command to see the default policy and any default values within configured policies.

```
hq-sanjose# show crypto isakmp policy
Protection suite priority 1
    encryption algorithm:DES - Data Encryption Standard (56 bit keys)
    hash algorithm:Secure Hash Standard
```

```
    authentication method:Pre-Shared Key
    Diffie-Hellman group:#1 (768 bit)
    lifetime:86400 seconds, no volume limit
```

Note Although the above output shows "no volume limit" for the lifetime, you can currently only configure a time lifetime (such as 86400 seconds); volume limit lifetimes are not configurable.

Tip If you have trouble, use the **show version** command to ensure your Cisco 7200 series router is running a Cisco IOS software image that supports crypto.

```
ski03_7206#show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JK9O3S-M), Version 12.3(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 28-Jul-03 15:45 by dchih
Image text-base: 0x60008954, data-base: 0x6219E000
ROM: System Bootstrap, Version 12.1(20000710:044039) [nlaw-121E_npeb 117], DEVELOPMENT
SOFTWARE
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.1(8a)E, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
m5-7206 uptime is 0 minutes
System returned to ROM by reload at 22:20:24 UTC Wed Aug 13 2003
System image file is "tftp://17.8.16.70/images/c7200-jk9o3s-mz.123-3"
Last reload reason: Reload command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 7206VXR (NPE400) processor (revision A) with 229376K/32768K bytes of memory.
Processor board ID 21281666
R7000 CPU at 350Mhz, Implementation 39, Rev 3.2, 256KB L2, 4096KB L3 Cache
6 slot VXR midplane, Version 2.1
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
PCI bus mb0_mb1 has 640 bandwidth points
PCI bus mb2 has 270 bandwidth points
WARNING: PCI bus mb0_mb1 Exceeds 600 bandwidth points
4 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ATM network interface(s)
1 Integrated service adapter(s)
125K bytes of non-volatile configuration memory.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
```

Configuring a Different Shared Key

Because pre-shared keys were specified as the authentication method for policy 1 in the "Configuring IKE Policies" section on page 3-15, (the policy that will also be used on the business partner router) complete the following steps at the headquarters router as well as the business partner router:

Step 1 Set each peer Internet Security Association & Key Management Protocol (ISAKMP) identity. Each peer identity should be set to either its host name or by its IP address. By default, a peer identity is set to its IP address. In this scenario, you only need to complete this task at the *business partner* router.

Step 2 Specify the 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.

Note The following procedure is based on the "Extranet Scenario" section on page 3-4.

To configure a different pre-shared key for use between the headquarters router and the business partner router, complete the following steps in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto isakmp key test67890 address 172.23.2.7`	**At the local peer**: Specify the shared key the headquarters router will use with the business partner router. This example configures the shared key test67890 to be used with the remote peer 172.23.2.7 (serial interface 1/0 on the business partner router).
Step 2	`bus-ptnr(config)# crypto isakmp identity address`	**At the remote peer**: Specify the ISAKMP identity (**address** or **hostname**) the business partner router will use when communicating with the headquarters router during IKE negotiations. (This task was already completed on the headquarters router when policy 1 was configured in the "Configuring IKE Policies" section on page 3-15.) This example specifies the **address** keyword, which uses IP address 172.23.2.7 (serial interface 1/0 of the business partner router) as the identity for the business partner router.
Step 3	`bus-ptnr(config)# crypto isakmp key test67890 address 172.17.2.4`	**At the remote peer**: Specify the shared key to be used with the local peer. This is the same key you just specified at the local peer. This example configures the shared key test67890 to be used with the local peer 172.16.2.2 (serial interface 2/0 on the headquarters router).

Note Set an ISAKMP identity whenever you specify pre-shared keys. The **address** keyword is typically used when there is only one interface (and therefore only one IP address) that will be used by the peer for IKE negotiations, and the IP address is known. Use the **hostname** keyword if there is more than one interface on the peer that might be used for IKE negotiations, or if the interface IP address is unknown (such as with dynamically-assigned IP addresses).

Configuring IPSec and IPSec Tunnel Mode

After you have configured a different shared key, configure IPSec at each participating IPSec peer. This section contains basic steps to configure IPSec and includes the following tasks:

- Creating Crypto Access Lists
- Verifying Crypto Access Lists
- Defining Transform Sets and Configuring IPSec Tunnel Mode
- Verifying Transform Sets and IPSec Tunnel Mode

Note IKE uses User Datagram Protocol (UDP) port 500. The IPSec encapsulating security payload (ESP) and authentication header (AH) protocols use IP protocol numbers 50 and 51. Ensure that your access lists are configured so that IP protocol 50, 51, and UDP port 500 traffic is not blocked at interfaces used by IPSec. In some cases, you might need to add a statement to your access lists to explicitly permit this traffic. Crypto access lists use the same format as standard access lists. However, the **permit** command instructs the router to encrypt data, and the **deny** command instructs the router to allow unencrypted data.

Creating Crypto Access Lists

Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. (These access lists are *not* the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, you can create access lists to protect all IP traffic between the headquarters router and business partner router.

The access lists themselves are not specific to IPSec. It is the crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a **permit** in the access list.

To create a crypto access list, enter the following command in global configuration mode:

Command	Purpose
`hq-sanjose(config)# access-list 111 permit ip host 10.2.2.2 host 10.1.5.3`	Specify conditions to determine which IP packets are protected.[1] (Enable or disable crypto for traffic that matches these conditions.) This example configures access list 111 to encrypt all IP traffic between the headquarters server (translated inside global IP address 10.2.2.2) and PC B (IP address 10.1.5.3) in the business partner office. We recommend that you configure “mirror image” crypto access lists for use by IPSec and that you avoid using the **any** keyword.

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

Verifying Crypto Access Lists

To verify the configuration:

- Enter the **show access-lists 111** EXEC command to see the access list attributes.

```
hq-sanjose# show access-lists 111
Extended IP access list 111
    permit ip host 10.2.2.2 host 10.1.5.3
```

Tip If you have trouble, make sure you are specifying the correct access list number.

Defining Transform Sets and Configuring IPSec Tunnel Mode

You must define transform sets regardless of the tunneling protocol you use. To define a transform set and configure IPSec tunnel mode, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto ipsec transform-set proposal4 ah-sha-hmac esp-des`	Define a transform set and enter crypto-transform configuration mode. This example combines AH[1] transform ah-sha-hmac, ESP[2] encryption transform esp-des, and ESP authentication transform esp-sha-hmac in the transform set proposal4. There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command. You can also use the **crypto ipsec transform-set?** command, in global configuration mode, to view the available transform arguments.
Step 2	`hq-sanjose(cfg-crypto-trans)# mode tunnel`	Change the mode associated with the transform set. The mode setting is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.) This example configures tunnel mode for the transport set proposal4, which creates an IPSec tunnel between the IPSec peer addresses.
Step 3	`hq-sanjose(cfg-crypto-trans)# exit` `hq-sanjose(config)#`	Exit back to global configuration mode.

1. AH = authentication header. This header, when added to an IP datagram, ensures the integrity and authenticity of the data, including the invariant fields in the outer IP header. It does not provide confidentiality protection. AH uses a keyed-hash function rather than digital signatures.
2. ESP = encapsulating security payload. This header, when added to an IP datagram, protects the confidentiality, integrity, and authenticity of the data. If ESP is used to validate data integrity, it does not include the invariant fields in the IP header.

Note AH and ESP can be used independently or together, although for most applications just one of them is sufficient. For both of these protocols, IPSec does not define the specific security algorithms to use, but rather, provides an open framework for implementing industry-standard algorithms.

Verifying Transform Sets and IPSec Tunnel Mode

To verify the configuration:

- Enter the **show crypto ipsec transform-set** EXEC command to see the type of transform set configured on the router.

```
hq-sanjose# show crypto ipsec transform-set
Transform set proposal4: { ah-sha-hmac  }
   will negotiate = { Tunnel,  },
   { esp-des esp-sha-hmac  }
   will negotiate = { Tunnel,  },

  -Display text omitted-
```

Configuring Crypto Maps

Remote devices need to be managed through a VPN from the central site when operating on a centralized IT model. VPN devices support numerous configuration options to determine the tunnel endpoint and, depending on the method chosen, these options may impact the manageability of the network. Refer to the "Dynamic versus Static Crypto Maps" section on page 2-5 for a discussion of when to use static or dynamic crypto maps.

To be the most effective in managing remote devices, you must use static cryptographic maps at the site where your management applications are located. Dynamic cryptographic maps can be used at the headend for ease of configuration. Dynamic maps, however, accept only incoming IKE requests, and because dynamic maps cannot initiate an IKE request, it is not always guaranteed that a tunnel exists between the remote device and the headend site. Static cryptographic map configuration includes the static IP addresses of the remote peers. Thus, remote sites must use static IP addresses to support remote management.

For IPSec to succeed between two IPSec peers, both peer crypto map entries must contain compatible configuration statements.

When two peers try to establish a security association (SA), they must each have at least one crypto map entry that is compatible with one of the other peer crypto map entries. For two crypto map entries to be compatible, they must meet the following minimum criteria:

- The crypto map entries must contain compatible crypto access lists (for example, mirror image access lists). In the case where the responding peer is using dynamic crypto maps, the entries in the local crypto access list must be "permitted" by the peer crypto access list.
- 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.

When IKE is used to establish SAs, the IPSec peers can negotiate the settings they will use for the new SAs. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

After you have completed configuring IPSec at each participating IPSec peer, configure crypto map entries and apply the crypto maps to interfaces.

The task of configuring IPSec at each peer can be eased by utilizing dynamic crypto maps. By configuring the head-end Cisco 7200 series router with a dynamic map, and the peers with a static map, the peer will be permitted to establish an IPSec security association even though the router does not have a crypto map entry specifically configured to meet all of the remote peer requirements.

This section contains basic steps to configure crypto maps and includes the following tasks:

Creating Crypto Map Entries

To create crypto map entries that will use IKE to establish the SAs, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto map s4second local-address serial 2/0`	Create the crypto map and specify a local address (physical interface) to be used for the IPSec traffic. This example creates crypto map s4second and specifies serial interface 2/0 of the headquarters router as the local address. This step is only required if you have previously used the **loopback** command or if you are using GRE tunnels.
Step 2	`hq-sanjose(config)# crypto map s4second 2 ipsec-isakmp`	Enter crypto map configuration mode, specify a sequence number for the crypto map you created in Step 1, and configure the crypto map to use IKE to establish SAs. This example configures sequence number 2 and IKE for crypto map s4second.
Step 3	`hq-sanjose(config-crypto-map)# match address 111`	Specify an extended access list. This access list determines which traffic is protected by IPSec and which traffic is not be protected by IPSec. This example configures access list 111, which was created in the "Creating Crypto Access Lists" section on page 3-22.
Step 4	`hq-sanjose(config-crypto-map)# set peer 172.23.2.7`	Specify a remote IPSec peer (by host name or IP address). This is the peer to which IPSec protected traffic can be forwarded. This example specifies serial interface 1/0 (172.23.2.7) on the business partner router.
Step 5	`hq-sanjose(config-crypto-map)# set transform-set proposal4`	Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first). This example specifies transform set proposal4, which was configured in the "Defining Transform Sets and Configuring IPSec Tunnel Mode" section on page 3-23.
Step 6	`hq-sanjose(config-crypto-map)# exit` `hq-sanjose(config)#`	Exit back to global configuration mode.

To create dynamic crypto map entries that will use IKE to establish the SAs, complete the following steps, starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# crypto dynamic-map` *`dynamic-map-name dynamic-seq-num`*	Creates a dynamic crypto map entry.

	Command	Purpose
Step 2	`hq-sanjose(config)# **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]`	Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first). This is the only configuration statement required in dynamic crypto map entries.
Step 3	`hq-sanjose(config-crypto-map)# **match address** *access-list-id*`	(Optional) Accesses list number or name of an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry. **Note** Although access-lists are optional for dynamic crypto maps, they are highly recommended. If the access list is configured, the data flow identity proposed by the IPSec peer must fall within a permit statement for this crypto access list. If the access list is not configured, the router will accept any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets. This is similar to static crypto maps because they also require that an access list be specified. Care must be taken if the any keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.
Step 4	`hq-sanjose(config-crypto-map)# **set peer** {*hostname* | *ip-address*}`	(Optional) Specifies a remote IPSec peer. Repeat for multiple remote peers. This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.

Step 5	`hq-sanjose(config-crypto-map)# **set security-association lifetime seconds** *seconds*`
	and/or
	`**set security-association lifetime kilobytes** *kilobytes*`
		(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPSec security association lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry.

Step 6	`hq-sanjose(config-crypto-map)# **exit**` `hq-sanjose(config)#`	Exit back to global configuration mode.

Verifying Crypto Map Entries

To verify the configuration:

- Enter the **show crypto map** EXEC command to see the crypto map entries configured on the router.

  In the following example, peer 172.23.2.7 is the IP address of the remote IPSec peer. “Extended IP access list 111” lists the access list associated with the crypto map. “Current peer” indicates the current IPSec peer. “Security-association lifetime” indicates the lifetime of the SA.

  “PFS N” indicates that IPSec will not negotiate perfect forward secrecy when establishing new SAs for this crypto map. “Transform sets” indicates the name of the transform set that can be used with the crypto map.

```
hq-sanjose# show crypto map
Crypto Map: "s4second" idb: Serial2/0 local address: 172.16.2.2
Crypto Map "s4second" 2 ipsec-isakmp
        Peer = 172.23.2.7
        Extended IP access list 111
            access-list 111 permit ip
                source: addr = 10.2.2.2/255.255.255.0
                dest:   addr = 10.1.5.3/255.255.255.0S
        Current peer: 172.23.2.7
        Security-association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={proposal4,}

  -Display text omitted-
```

Tip If you have trouble, make sure you are using the correct IP addresses.

Applying Crypto Maps to Interfaces

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 crypto.

To apply a crypto map set to an interface, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# interface serial 2/0`	Specify a physical interface on which to apply the crypto map and enter interface configuration mode. This example specifies serial interface 2/0 on the headquarters router.
Step 2	`hq-sanjose(config-if)# crypto map s4second`	Apply the crypto map set to the physical interface. This example configures crypto map s4second, which was created in the "Creating Crypto Map Entries" section on page 3-25.
Step 3	`hq-sanjose(config-if)# exit` `hq-sanjose(config)#`	Exit back to global configuration mode.
Step 4	`hq-sanjose# clear crypto sa`	In privileged EXEC mode, clear the existing IPSec SAs so that any changes are used immediately. (Manually established SAs are reestablished immediately.) **Note** Using the **clear crypto sa** command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database.

Verifying Crypto Map Interface Associations

To verify the configuration:

- Enter the **show crypto map interface serial 2/0** EXEC command to see the crypto maps applied to a specific interface.

```
hq-sanjose# show crypto map interface serial 2/0
Crypto Map "s4second" 2 ipsec-isakmp
        Peer = 172.23.2.7
        Extended IP access list 111
            access-list 111 permit ip host 10.2.2.2 host 10.1.5.3
        Current peer:172.23.2.7
        Security association lifetime:4608000 kilobytes/1000 seconds
        PFS (Y/N):N
        Transform sets={ proposal4, }
```

Step 4—Configuring Quality of Service

Cisco IOS quality of service (QoS) refers to the ability of a network to provide better service to selected network traffic over various underlying technologies including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. In particular, QoS features provide better and more predictable network service by:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

You configure QoS features throughout a network to provide for end-to-end QoS delivery. The following three components are necessary to deliver QoS across a heterogeneous network:

- QoS within a single network element, which includes queuing, scheduling, and traffic shaping features.
- QoS signaling techniques for coordinating QoS from end-to-end between network elements.
- QoS policing and management functions to control and administer end-to-end traffic across a network.

Not all QoS techniques are appropriate for all network routers. Because edge routers and backbone routers in a network do not necessarily perform the same operations, the QoS tasks they perform might differ as well.

In general, edge routers perform the following QoS functions:

- Packet classification and prioritization
- Admission control, such as queuing and policing
- Bandwidth management

In general, backbone routers perform the following QoS functions:

- Congestion management
- Congestion avoidance

Cisco IOS QoS service models, features, and sample configurations are explained in detail in the *Quality of Service Solutions Configuration Guide* and the *Quality of Service Solutions Command Reference*. Refer to these two publications as you plan and implement a QoS strategy for your VPN, because there are various QoS service models and features that you can implement on your VPN. See "Related Documentation" section on page xi for information on how to access these publications.

This section contains basic steps to configure QoS weighted fair queuing (WFQ), which applies priority (or weights) to identified traffic on the GRE tunnel you configured in the "Step 1—Configuring the Tunnel" section on page 3-6. This section also contains basic steps to configure Network-Based Application Recognition (NBAR), which is a classification engine that recognizes a wide variety of applications, including web-based and other protocols that utilize dynamic TCP/UDP port assignments.

This section includes the following topics:

Configuring Network-Based Application Recognition

Network-Based Application Recognition (NBAR) adds intelligent network classification to network infrastructures. NBAR is a classification engine that recognizes a wide variety of applications, including web-based and other protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features.

Your interface to NBAR is through the modular QoS command-line interface (MQC). MQC provides a model for QoS configuration under IOS. MQC provides a clean separation between the specification of a classification policy and the specification of other policies that act based on the results of the applied classification.

Configuring a QoS policy typically requires the configuration of traffic classes, the configuration of policies that will be applied to those traffic classes, and the attaching of policies to interfaces using the commands in the sections that follow.

The following tasks are required to configure NBAR:

- Configuring a Class Map
- Verifying a Class Map Configuration
- Configuring a Policy Map
- Attaching a Policy Map to an Interface
- Verifying a Policy Map Configuration

Note You must enable Cisco Express Forwarding (CEF) before you configure NBAR. For more information on CEF, refer to the Cisco IOS Release 12.0 configuration guide titled *Cisco IOS Switching Services Configuration Guide*.

Configuring a Class Map

Use the **class-map** configuration command to define a traffic class and the match criteria that will be used to identify traffic as belonging to that class. Match statements can include criteria such as protocol, ACL, IP precedence value, or interface identifier. The match criteria is defined with one or more of the match statements entered within the class-map configuration mode listed in the table below:

	Command	Purpose
Step 1	`Router(config)# class-map match-all | match-any class-name`	Specifies the user-defined name of the class map. The **match-all** option specifies that all match criteria in the class map must be matched. The **match-any** option specifies that one or more match criteria must match.[1]
Step 2	`Router(config-cmap)# match protocol protocol-name`	Specifies a protocol supported by NBAR as a matching criteria.
Step 3	`Router(config-cmap)# match class-map class-name`	Specifies a class map as a matching criteria (nested class maps).

1. When neither **match-all** nor **match-any** is specified, the default is **match-all**. Use the **no class-map** command to disable the class map. Use the **no match-all** and **no match-any** commands to disable these commands within the class map. Use the **match not** command to configure a match that evaluates to true if the packet does not match the specified protocol.

Verifying a Class Map Configuration

Enter the **show class-map** command to display all class map information. You can also enter the **show class-map** *class-name* command to display the class map information of a user-specified class map.

Configuring a Policy Map

Use the **policy-map configuration** command to specify the QoS policies to apply to traffic classes defined by a class map. QoS policies that can be applied to traffic classification are listed in the table below.

	Command	Purpose
Step 1	`Router(config)# policy-map` *policy-name*	User specified policy map name.
Step 2	`Router(config-pmap)# class` *class-name*	Specifies the name of a previously defined class map.
Step 3	`Router(config-pmap-c)# bandwidth` *kbps*	Specifies a minimum bandwidth guarantee to a traffic class.
Step 4	`Router(config-pmap-c)# police` *bps* `conform transmit exceed drop`	Specifies a maximum bandwidth usage by a traffic class.
Step 5	`Router(config-pmap-c)# set ip precedence {0-7}`	Specifies the IP precedence of packets within a traffic class.
Step 6	`outer(config-pmap-c)# set qos-group {0-99}`	Specifies a QoS-group value to associate with the packet.
Step 7	`Router(config-pmap-c)# random-detect`	Enables weighted random early detection (WRED) drop policy for a traffic class which has a bandwidth guarantee.
Step 8	`Router(config-pmap-c)# queue-limit` *packets*	Specifies maximum number of packets queued for a traffic class (in the absence of random-detect).

Use the **no policy-map** command to deconfigure the policy map. Use the **no bandwidth**, **no police**, **no set,** and **no random-detect** commands to disable these commands within the policy map.

Attaching a Policy Map to an Interface

Use the **service-policy** interface configuration command to attach a policy map to an interface and to specify the direction in which the policy should be applied (on either packets coming into the interface or packets leaving the interface).

	Command	Purpose
Step 1	`Router(config-if)# service-policy output` *policy-map-name*	Specifies the name of the policy map to be attached to the output direction of the interface.
Step 2	`Router(config-if)# service-policy input` *policy-map-name*	Specifies the name of the policy map to be attached to the input direction of the interface.

Use the **no service-policy** [*input* | *output*] *policy-map-name* command to detach a policy map from an interface.

Verifying a Policy Map Configuration

Use the **show policy-map** [**interface** [*interface-spec* [*input* | *output* [**class** *class-name*]]]] command to display the configuration of a policy map and its associated class maps. Forms of this command are listed in the following table:

Command	Purpose
Router# **show policy-map**	Displays all configured policy maps.
Router# **show policy-map** *policy-map-name*	Displays the user-specified policy map.
Router# **show policy-map interface**	Displays statistics and configurations of all input and output policies, which are attached to an interface.
Router# **show policy-map** *interface-spec*	Displays configuration and statistics of the input and output policies attached to a particular interface.
Router# **show policy-map** *interface-spec[input]*	Displays configuration and statistics of the input policy attached to an interface.
Router# **show policy-map** *interface-spec[output]*	Displays configuration statistics of the output policy attached to an interface.
Router# **show policy-map interface-spec***[input|output]* **class** *class-name*	Displays the configuration and statistics for the class name configured in the policy.

Configuring Weighted Fair Queuing

Weighted Fair Queuing (WFQ) provides traffic priority management that automatically sorts among individual traffic streams without requiring that you first define access lists. WFQ can also manage duplex data streams such as those between pairs of applications, and simplex data streams such as voice or video. There are two categories of WFQ sessions: high bandwidth and low bandwidth. Low-bandwidth traffic has effective priority over high-bandwidth traffic, and high-bandwidth traffic shares the transmission service proportionally according to assigned weights.

When WFQ is enabled for an interface, new messages for high-bandwidth traffic streams are discarded after the configured or default congestive messages threshold has been met. However, low-bandwidth conversations, which include control message conversations, continue to enqueue data. As a result, the fair queue may occasionally contain more messages than its configured threshold number specifies.

With standard WFQ, packets are classified by flow. Packets with the same source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, or destination TCP or UDP port belong to the same flow. WFQ allocates an equal share of the bandwidth to each flow. Flow-based WFQ is also called fair queuing because all flows are equally weighted.

To configure fair queuing on an interface, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	hq-sanjose(config)# **interface serial 1/0**	Specify an interface and enter interface configuration mode. This example specifies serial interface 1/0 on the headquarters router.
Step 2	hq-sanjose(config-if)# **fair-queue**	Configure fair queuing on the interface.
Step 3	hq-sanjose(config-if)# **exit** hq-sanjose(config)#	Exit back to global configuration mode.

Verifying Weighted Fair Queuing

To verify the configuration:

- Enter the **show interfaces serial 1/0 fair-queue** EXEC command to see information on the interface that is configured for WFQ.

```
hq-sanjose# show interfaces serial 1/0 fair-queue
Serial1/0 queue size 0
     packets output 35, drops 0
WFQ: global queue limit 401, local queue limit 200
```

- Enter the **show interfaces serial 1/0** EXEC command to verify the queuing for the interface is WFQ.

```
hq-sanjose# show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is M2T-T3 pa

  -Display text omitted-

  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)

  -Display text omitted-
```

Configuring Class-Based Weighted Fair Queuing

Class-based weighted fair queueing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and traffic belonging to a class is directed to that class queue.

Once a class has been defined according to its match criteria, you can assign it characteristics. To characterize a class, you assign it bandwidth, weight, and maximum packet limit. The bandwidth assigned to a class is the minimum bandwidth delivered to the class during congestion.

To characterize a class, you also specify the queue limit for that class, which is the maximum number of packets allowed to accumulate in the class queue. Packets belonging to a class are subject to the bandwidth and queue limits that characterize the class.

After a queue has reached its configured queue limit, enqueuing of additional packets to the class causes tail drop or packet drop to take effect, depending on how class policy is configured.

Tail drop is used for CBWFQ classes unless you explicitly configure policy for a class to use weighted random early detection (WRED) to drop packets as a means of avoiding congestion. Note that if you use WRED packet drop instead of tail drop for one or more classes comprising a policy map, you must ensure that WRED is not configured for the interface to which you attach that service policy.

Note Although CBWFQ supports the use of WRED, this guide does not include WRED configuration procedures. For more information on using WRED with CBWFQ, refer to the Cisco IOS Release 12.2 Configuration Guide Master Index.

If a default class is configured, all unclassified traffic is treated as belonging to the default class. If no default class is configured, then by default the traffic that does not match any of the configured classes is flow classified and given best-effort treatment. Once a packet is classified, all of the standard mechanisms that can be used to differentiate service among the classes apply.

Flow classification is standard WFQ treatment. That is, packets with the same source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, or destination TCP or UDP port are classified as belonging to the same flow. WFQ allocates an equal share of bandwidth to each flow. Flow-based WFQ is also called fair queueing because all flows are equally weighted.

For CBWFQ, which extends the standard WFQ, the weight specified for the class becomes the weight of each packet that meets the match criteria of the class. Packets that arrive at the output interface are classified according to the match criteria filters you define, then each one is assigned the appropriate weight.

The weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it; in this sense the weight for a class is user-configurable.

After a packet's weight is assigned, the packet is enqueued in the appropriate class queue. CBWFQ uses the weights assigned to the queued packets to ensure that the class queue is serviced fairly.

The following tasks are required to configure CBWFQ:

- Defining a Class Map
- Configuring Class Policy in the Policy Map (Tail Drop)
- Attaching the Service Policy and Enabling CBWFQ

Note Attaching a service policy to an interface disables WFQ on that interface if WFQ is configured for the interface. For this reason, you should ensure that WFQ is not enabled on such an interface. For additional information on WFQ, see the "Configuring Weighted Fair Queueing" chapter of the *Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide*.

Defining a Class Map

To create a class map containing match criteria against which a packet is checked to determine if it belongs to a class, and to effectively create the class whose policy can be specified in one or more policy maps, use the first command in global configuration mode to specify the class-map name. Then use one of the following commands in class-map configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# class-map class-map-name`	Specifies the name of the class map to be created.
Step 2	`hq-sanjose(config-cmap)# match access-group access-group`	Specifies the name of the numbered ACL against whose contents packets are checked to determine if they belong to the class.
Step 3	`hq-sanjose(config-cmap)# match input-interface interface-name`	Specifies the name of the output interface used as a match criterion against which packets are checked to determine if they belong to the class.
Step 4	`hq-sanjose(config-cmap)# match protocol protocol`	Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class.

Configuring Class Policy in the Policy Map (Tail Drop)

To configure a policy map and create class policies (including a default class) comprising the service policy, use the first global configuration command to specify the policy-map name. Then use the following policy-map configuration commands to configure policy for a standard class and the default class. For each class that you define, you can use one or more of the following policy-map configuration commands to configure class policy. For example, you might specify bandwidth for one class and both bandwidth and queue limit for another class.

The policy-map default class is the class to which traffic is directed if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map. To configure policy for more than one class in the same policy map, repeat Steps 2 through 4. Note that because this set of commands uses queue-limit, the policy map uses tail drop for both class policies, not WRED packet drop.

To attach a service policy to an interface and enable CBWFQ on the interface, you must create a policy map. You can configure class policies for as many classes as are defined on the router up to the maximum of 64.

	Command	Purpose
Step 1	`hq-sanjose(config)# policy-map policy-map`	Specifies the name of the policy map to be created or modified.
Step 2	`hq-sanjose(config-pmap)# class class-name`	Specifies the name of a class to be created and included in the service policy.
Step 3	`hq-sanjose(config-pmap-c)# bandwidth bandwidth-kbps`	Specifies the amount of bandwidth in kilobits per second (kbps) to be assigned to the class.
Step 4	`hq-sanjose(config-pmap-c)# queue-limit number-of-packets`	Specifies the maximum number of packets that can be enqueued for the class.
Step 5	`hq-sanjose(config-pmap)# class class-default default-class-name`	Specifies the default class in order to configure its policy.
Step 6	`hq-sanjose(config-pmap-c)# bandwidth bandwidth-kbps`	Specifies the amount of bandwidth in kilobits per second to be assigned to the default class.
Step 7	`hq-sanjose(config-pmap-c)# queue-limit number-of-packets`	Specifies the maximum number of packets that can be enqueued for the specified default class.

Attaching the Service Policy and Enabling CBWFQ

To attach a service policy to the output interface and enable CBWFQ on the interface, use the interface configuration command in the following table:

Command	Purpose
`hq-sanjose(config-if)# service-policy output policy-map`	Enables CBWFQ and attaches the specified service policy map to the output interface.

Note When CBWFQ is enabled, all classes configured as part of the service policy map are installed in the fair queueing system.

Verifying Class-Based Weighted Fair Queuing

To display the contents of a specific policy map, a specific class from a specific policy map, or all policy maps configured on an interface, use one of the following global configuration commands:

Command	Purpose
`hq-sanjose# show policy policy-map`	Displays the configuration of all classes comprising the specified policy map.
`hq-sanjose# show policy policy-map class` *class-name*	Displays the configuration of the specified class of the specified policy map.
`hq-sanjose# show policy interface` *interface-name*	Displays the configuration of all classes configured for all policy maps on the specified interface.

Step 5—Configuring Cisco IOS Firewall Features

Cisco IOS software provides an extensive set of security features with which you can configure a simple or elaborate firewall, according to your particular requirements. When you configure Cisco IOS firewall features on your Cisco router, you turn your router into an effective, robust firewall.

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.

Note The Cisco Secure PIX Firewall can be used as an alternative to Cisco IOS firewall features. For detailed information on the Cisco Secure PIX Firewall, refer to the Cisco Secure PIX Firewall documentation.

Note Although Cisco 7200 series routers support intrusion detection features, intrusion detection configuration procedures are not explained in this guide. For detailed information on intrusion detection, refer to the *Intrusion Detection Planning Guide*.

You can use Cisco IOS firewall features to configure your Cisco IOS router as:

- 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 your company partners networks

Cisco IOS firewall features provide the following benefits:

- Protects internal networks from intrusion
- Monitors traffic through network perimeters
- Enables network commerce using the World Wide Web

At a minimum, you must configure basic traffic filtering to provide a basic firewall. You can configure your Cisco 7200 series router to function as a firewall by using the following Cisco IOS security features:

- Static access lists and static or dynamic extended access lists
- Lock-and-key (dynamic extended access lists)

- Reflective access lists
- TCP intercept
- Context-based access control
- Security server support
- Network address translation
- Cisco Encryption Technology
- IPSec network security
- Neighbor router authentication
- Event logging
- User authentication and authorization

Note Refer to the "Traffic Filtering and Firewalls" part of the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* for advanced firewall configuration information. For information on how to access these documents, see "Related Documentation" section on page xi.

This section explains how to configure an extended access list, which is a sequential collection of permit and deny conditions that apply to an IP address.

This section includes the following topics:

Note The extended access list configuration explained in this section is different from the crypto access list configuration explained in the "Creating Crypto Access Lists" section on page 3-22. Crypto access lists are used to define which IP traffic is or is not protected by crypto, while an extended access list is used to determine which IP traffic to forward or block at an interface.

The simplest connectivity to the Internet is to use a single device to provide the connectivity and firewall function to the Internet. With everything being in a single device, it is easy to address translation and termination of the VPN tunnels. Complexity arises when you need to add extra Cisco 7200 series routers to the network. This normally leads people into building a network where the corporate network touches the Internet through a network called the DMZ, or demilitarized zone.

Creating Extended Access Lists Using Access List Numbers

To create an extended access list that denies and permits certain types of traffic, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# access-list 102 deny tcp any any`	Define access list 102 and configure the access list to deny all TCP traffic.

	Command	Purpose
Step 2	`hq-sanjose(config)# access-list 102 deny udp any any`	Configure access list 102 to deny all UDP traffic.
Step 3	`hq-sanjose(config)# access-list 102 permit ip any any`	Configure access list 102 to permit all IP traffic.

Verifying Extended Access Lists

To verify the configuration:

Enter the **show access-lists 102** EXEC command to display the contents of the access list.

```
hq-sanjose# show access-list 102
Extended IP access list 102
    deny   tcp any any
    deny   udp any any
    permit ip any any
```

Applying Access Lists to Interfaces

After you create an access list, you can apply it to one or more interfaces. Access lists can be applied on *either* outbound or inbound interfaces.

To apply an access list inbound and outbound on an interface, complete the following steps starting in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# interface serial 1/0`	Specify serial interface 1/0 on the headquarters router and enter interface configuration mode.
Step 2	`hq-sanjose(config-if)# ip access-group 102 in`	Configure access list 102 inbound on serial interface 1/0 on the headquarters router.
Step 3	`hq-sanjose(config-if)# ip access-group 102 out`	Configure access list 102 outbound on serial interface 1/0 on the headquarters router.
Step 4	`hq-sanjose(config-if)# exit` `hq-sanjose(config)#`	Exit back to global configuration mode.

For inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an “icmp host unreachable” message.

For outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the destination address of the packet against the access list. If the access list permits the address, the software transmits the packet. If the access list rejects the address, the software discards the packet and returns an “ICMP Host Unreachable” message.

When you apply an access list that has not yet been defined to an interface, the software acts as if the access list has not been applied to the interface and will accept all packets. Be aware of this behavior if you use undefined access lists as a means of security in your network.

Verifying Extended Access Lists Are Applied Correctly

To verify the configuration:

- Enter the **show ip interface serial 1/0** EXEC command to confirm the access list is applied correctly (inbound and outbound) on the interface.

```
hq-sanjose# show ip interface serial 1/0
Serial1/0 is up, line protocol is up
  Internet address is 172.17.2.4
  Broadcast address is 255.255.255.255
  Address determined by setup command
  Peer address is 172.24.2.5
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 102
  Inbound  access list is 102

  -Display text omitted-
```

Tip If you have trouble, ensure that you specified the correct interface when you applied the access list.

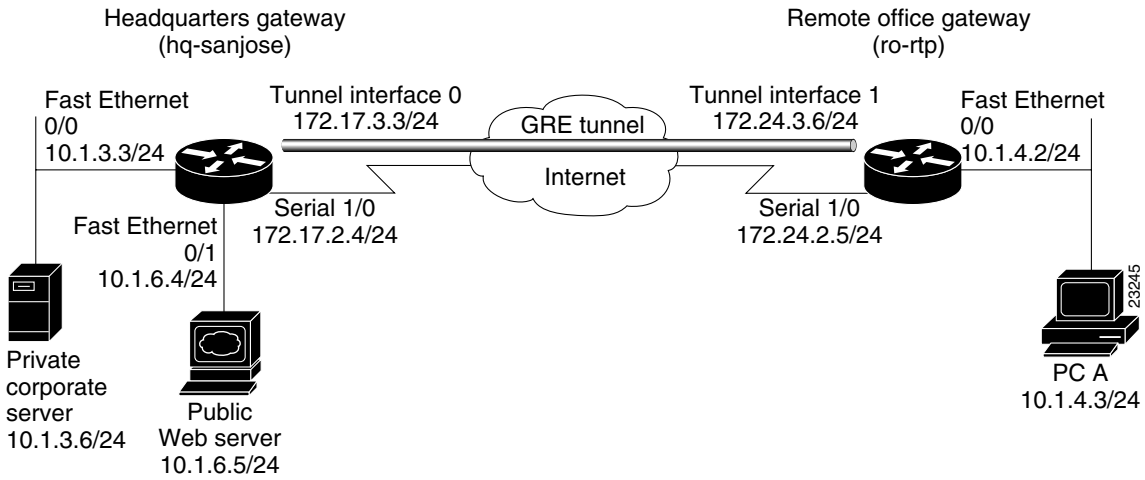
Comprehensive Configuration Examples

Following are comprehensive sample configurations for the site-to-site and extranet scenarios.

Site-to-Site Scenario

The following sample configuration is based on the physical elements shown in Figure 3-8:

Figure 3-8 Site-to-Site VPN Scenario Physical Elements



Headquarters Router Configuration

```
hq-sanjose# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname hq-sanjose
!
boot system flash bootflash:
boot bootldr bootflash:c7200-jk9o3s-mz.123-3
boot config slot0:hq-sanjose-cfg-small
no logging buffered
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 84600
crypto isakmp key test12345 address 172.24.2.5
!
crypto ipsec transform-set proposal1 ah-sha-hmac esp-des esp-sha-hmac
mode transport
!
 !
 crypto map s1first local-address Serial1/0
 crypto map s1first 1 ipsec-isakmp
 set peer 172.24.2.5
 set transform-set proposal1
 match address 101
!
interface Tunnel0
 bandwidth 180
 ip address 172.17.3.3 255.255.255.0
 no ip directed-broadcast
 tunnel source 172.17.2.4
 tunnel destination 172.24.2.5
 crypto map s1first
!
interface FastEthernet0/0
 ip address 10.1.3.3 255.255.255.0
 no ip directed-broadcast
 no keepalive
 full-duplex
 no cdp enable
!
interface FastEthernet0/1
 ip address 10.1.6.4 255.255.255.0
 no ip directed-broadcast
 no keepalive
 full-duplex
 no cdp enable
!
interface Serial1/0
 ip address 172.17.2.4 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
 fair-queue 64 256 0
 framing c-bit
```

```
 cablelength 10
 dsu bandwidth 44210
 clock source internal
 no cdp enable
 crypto map s1first
!
ip route 10.1.4.0 255.255.255.0 Tunnel0
!
access-list 101 permit gre host 172.17.2.4 host 172.24.2.5
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Remote Office Router Configuration

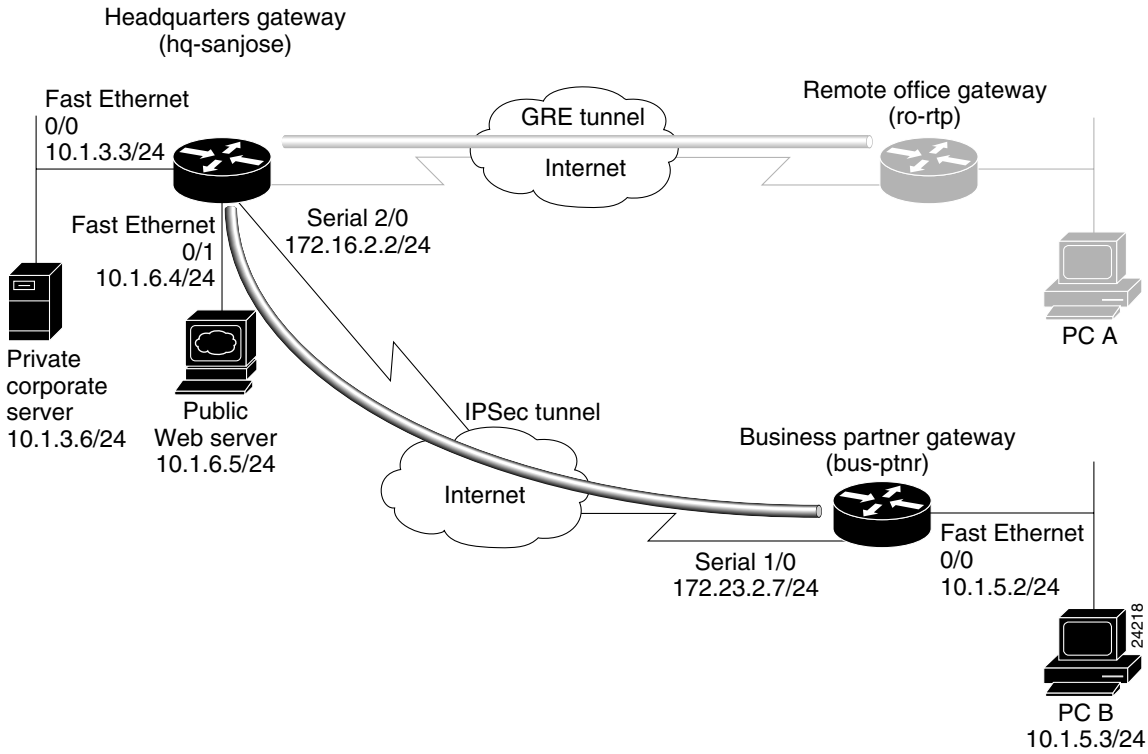
```
ro-rtp# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ro-rtp
!
boot system flash bootflash:
boot bootldr bootflash:c7200-jk9o3s-mz.123-3
boot config slot0:ro-rtp-cfg-small
no logging buffered
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 84600
crypto isakmp key test12345 address 172.17.2.4
!
crypto ipsec transform-set proposal1 ah-sha-hmac esp-des esp-sha-hmac
mode transport
!
 !
 crypto map s1first local-address Serial1/0
 crypto map s1first 1 ipsec-isakmp
 set peer 172.17.2.4
 set transform-set proposal1
 match address 101
!
interface Tunnel1
 bandwidth 180
 ip address 172.24.3.6 255.255.255.0
 no ip directed-broadcast
 tunnel source 172.24.2.5
 tunnel destination 172.17.2.4
 crypto map s1first
!
interface FastEthernet0/0
 ip address 10.1.4.2 255.255.255.0
```

```
 no ip directed-broadcast
 no keepalive
 full-duplex
 no cdp enable
!
interface Serial1/0
 ip address 172.24.2.5 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
 fair-queue 64 256 0
 framing c-bit
 cablelength 10
 dsu bandwidth 44210
 clock source internal
 no cdp enable
 crypto map s1first
!
ip route 10.1.3.0 255.255.255.0 Tunnel1
ip route 10.1.6.0 255.255.255.0 Tunnel1
!
access-list 101 permit gre host 172.24.2.5 host 172.17.2.4
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Extranet Scenario

The following sample configuration is based on the physical elements shown in Figure 3-9:

Figure 3-9 Extranet VPN Scenario Physical Elements



Headquarters Router Configuration

```
hq-sanjose# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname hq-sanjose
!
boot system flash bootflash:
boot bootldr bootflash:c7200-jk9o3s-mz.123-3
boot config slot0:hq-sanjose-cfg-small
no logging buffered
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 84600
crypto isakmp key test12345 address 172.24.2.5
```

```
crypto isakmp key test67890 address 172.23.2.7
!
crypto ipsec transform-set proposal1 ah-sha-hmac esp-des esp-sha-hmac
mode transport
!
crypto ipsec transform-set proposal4 ah-sha-hmac esp-des esp-sha-hmac
!
 !
 crypto map s1first local-address Serial1/0
 crypto map s1first 1 ipsec-isakmp
 set peer 172.24.2.5
 set transform-set proposal1
 match address 101
 !
 crypto map s4second local-address Serial2/0
 crypto map s4second 2 ipsec-isakmp
 set peer 172.23.2.7
 set transform-set proposal4
 match address 111
!
interface Tunnel0
 bandwidth 180
 ip address 172.17.3.3 255.255.255.0
 no ip directed-broadcast
 tunnel source 172.17.2.4
 tunnel destination 172.24.2.5
 crypto map s1first
!
interface FastEthernet0/0
 ip address 10.1.3.3 255.255.255.0
 no ip directed-broadcast
 no keepalive
 full-duplex
 no cdp enable
!
interface FastEthernet0/1
 ip address 10.1.6.4 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 no keepalive
 full-duplex
 no cdp enable
!
interface Serial1/0
 ip address 172.17.2.4 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
 fair-queue 64 256 0
 framing c-bit
 cablelength 10
 dsu bandwidth 44210
 clock source internal
 no cdp enable
 crypto map s1first
!
interface Serial2/0
 ip address 172.16.2.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
no ip mroute-cache
 no keepalive
 fair-queue 64 256 0
 framing c-bit
```

```
 cablelength 10
 dsu bandwidth 44210
 clock source internal
 no cdp enable
 crypto map s4second
!
router bgp 10
 network 10.2.2.2 mask 255.255.255.0
 network 172.16.2.0 mask 255.255.255.0
!
ip route 10.1.4.0 255.255.255.0 Tunnel0
!
ip nat inside source static 10.1.6.5 10.2.2.2
!
access-list 101 permit gre host 172.17.2.4 host 172.24.2.5
access-list 111 permit ip host 10.2.2.2 host 10.1.5.3
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Business Partner Router Configuration

```
bus-ptnr# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname bus-ptnr
!
boot system flash bootflash:
boot bootldr bootflash:c7200-jk9o3s-mz.123-3
boot config slot0:bus-ptnr-cfg-small
no logging buffered
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 84600
crypto isakmp key test67890 address 172.16.2.2
!
crypto ipsec transform-set proposal4 ah-sha-hmac esp-des esp-sha-hmac
!
 !
 crypto map s4second local-address Serial1/0
 crypto map s4second 2 ipsec-isakmp
 set peer 172.16.2.2
 set transform-set proposal4
 match address 111
!
interface FastEthernet0/0
 ip address 10.1.5.2 255.255.255.0
 no ip directed-broadcast
 no keepalive
```

```
 full-duplex
 no cdp enable
!
interface Serial1/0
 ip address 172.23.2.7 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
 fair-queue 64 256 0
 framing c-bit
 cablelength 10
 dsu bandwidth 44210
 clock source internal
 no cdp enable
 crypto map s4second
!
router bgp 10
 network 10.1.5.0 mask 255.255.255.0
 network 172.16.2.0 mask 255.255.255.0
!
access-list 111 permit ip host 10.1.5.3 host 10.2.2.2
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Remote Access VPN Business Scenarios

This chapter explains the basic tasks for configuring an IP-based, remote access Virtual Private Network (VPN) on a Cisco 7200 series router. In the remote access VPN business scenario, a remote user running VPN client software on a PC establishes a connection to the headquarters Cisco 7200 series router.

The configurations in this chapter utilize a Cisco 7200 series router. If you have a Cisco 2600 series router or a Cisco 3600 series router, your configurations will differ slightly, most notably in the port slot numbering. Please refer to your model configuration guide for detailed configuration information. Please refer to the "Obtaining Documentation" section on page xii for instructions about locating product documentation.

Note In this Guide, the term 'Cisco 7200 series router' implies that an Integrated Service Adaptor (ISA) or a VAM (VAM, VAM2, or VAM2+) is installed in the Cisco 7200 series router.

This chapter describes basic features and configurations used in a remote access VPN scenario. Some Cisco IOS security software features not described in this document can be used to increase performance and scalability of your VPN. For up-to-date Cisco IOS security software features documentation, refer to the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* for your Cisco IOS Release. To access these documents, see "Related Documentation" section on page xi.

This chapter includes the following sections:

Note Throughout this chapter, there are numerous configuration examples and sample configuration outputs that include unusable IP addresses. Be sure to use your own IP addresses when configuring your Cisco 7200 series router.

Scenario Description

Figure 4-1 shows a headquarters network providing a remote user access to the corporate intranet. In this scenario, the headquarters and remote user are connected through a secure tunnel that is established over an IP infrastructure (the Internet). The remote user is able to access internal, private web pages and perform various IP-based network tasks.

Figure 4-1 Remote Access VPN Business Scenario

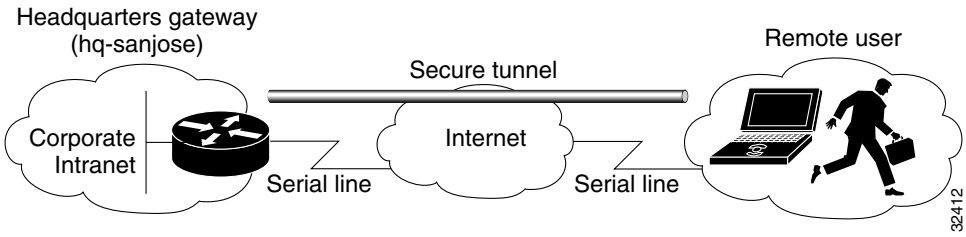
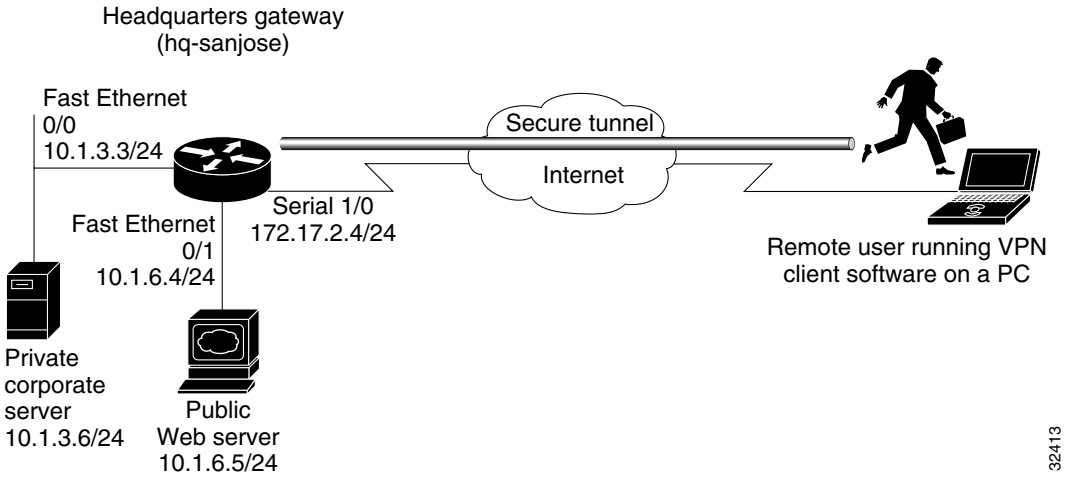


Figure 4-2 shows the physical elements of the scenario. The Internet provides the core interconnecting fabric between the headquarters and remote user. The headquarters is using a Cisco IOS VPN gateway (Cisco 7200 series with an Integrated Service Adaptor (ISA) or VAM, a Cisco 2600 seriesrouter or a 3600 series router), and the remote user is running VPN client software on a PC.

The tunnel is configured on the first serial interface in chassis slot 1 (serial 1/0) of the headquarters and remote office routers. Fast Ethernet interface 0/0 of the headquarters router is connected to a corporate server and Fast Ethernet interface 0/1 is connected to a web server.

Figure 4-2 Remote Access VPN Scenario Physical Elements



The configuration steps in the following sections are for the headquarters router. Comprehensive configuration examples for the headquarters router are provided in the "Comprehensive Configuration Examples" section on page 4-11. Table 4-1 lists the physical elements of the scenario.

Table 4-1 Physical Elements

Headquarters Network			Remote User		
Site Hardware	**WAN IP Address**	**Ethernet IP Address**	**Site Hardware**	**WAN IP Address**	**Ethernet IP Address**
hq-sanjose	Serial interface 1/0: 172.17.2.4 255.255.255.0	Fast Ethernet Interface 0/0: 10.1.3.3 255.255.255.0 Fast Ethernet Interface 0/1: 10.1.6.4 255.255.255.0	PC running VPN client software	Dynamically assigned	—
Corporate server	—	10.1.3.6	—	—	—
Web server	—	10.1.6.5			

Configuring a Cisco IOS VPN Gateway for Use with Cisco Secure VPN Client Software

Using Cisco Secure VPN Client software, a remote user can access the corporate headquarters network through a secure IPSec tunnel. Although Cisco IOS VPN gateways support Cisco Secure VPN Client software, this guide does not explain how to configure your gateway for use with it. For detailed information on configuring client-initiated VPNs using Cisco Secure VPN Client software, refer to the *Cisco Secure VPN Client Solutions Guide* publication.

Configuring a Cisco IOS VPN Gateway for Use with Microsoft Dial-Up Networking

Using Microsoft Dial-Up Networking (DUN), available with Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT 4.0, and Microsoft Windows 2000, a remote user can use Point-to-Point Tunneling Protocol (PPTP) with Microsoft Point-to-Point Encryption (MPPE) to access the corporate headquarters network through a secure tunnel.

Employing PPTP/MPPE, users can use any Internet service provider (ISP) account and any Internet-routable IP address to access the edge of the enterprise network. At the edge, the IP packet is detunneled and the IP address space of the enterprise is used for traversing the internal network. MPPE provides an encryption service that protects the datastream as it traverses the Internet. MPPE is available in two strengths: 40-bit encryption, which is widely available throughout the world, and 128-bit encryption, which may be subject to certain export controls when used outside the United States.

Note PPTP/MPPE is built into Windows DUN1.2 and above. However, 128-bit encryption and stateless (historyless) MPPE is only supported in Windows DUN1.3 or later versions. PPTP/MPPE only supports Cisco Express Forwarding (CEF) and process switching. Regular fast switching is not supported.

Alternatively, a remote user with client software bundled into Microsoft Windows 2000 can use Layer 2 Tunneling Protocol (L2TP) with IPSec to access the corporate headquarters network through a secure tunnel.

Because L2TP is a standard protocol, enterprises can enjoy a wide range of service offerings available from multiple vendors. L2TP implementation is a solution that provides a flexible, scalable remote network access environment without compromising corporate security or endangering mission-critical applications.

Note L2TP is only supported in Microsoft Windows 2000.

This section includes the following topics:

- Configuring PPTP/MPPE
- Verifying PPTP/MPPE
- Configuring L2TP/IPSec

Configuring PPTP/MPPE

PPTP is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multiprotocol, virtual private networking over public networks, such as the Internet.

MPPE is an encryption technology developed by Microsoft to encrypt point-to-point links. These PPP connections can be over a dialup line or over a VPN tunnel. MPPE works as a subfeature of Microsoft Point-to-Point Compression (MPPC).

MPPE uses the RC4 algorithm with either 40- or 128-bit keys. All keys are derived from the cleartext authentication password of the user. RC4 is stream cipher; therefore, the sizes of the encrypted and decrypted frames are the same size as the original frame. The Cisco implementation of MPPE is fully interoperable with that of Microsoft and uses all available options, including historyless mode. Historyless mode can increase throughput in high-loss environments such as VPNs.

Note The VAM, available on Cisco 7200 series routers, does not support MPPE.

Note Windows clients must use Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication for MPPE to work. If you are performing mutual authentication with MS-CHAP and MPPE, both sides of the tunnel must use the same password.

This section contains basic steps to configure PPTP/MPPE and includes the following tasks:

- Configuring a Virtual Template for Dial-In Sessions
- Configuring PPTP
- Configuring MPPE

Configuring a Virtual Template for Dial-In Sessions

Using virtual templates, you can populate virtual-access interfaces with predefined customized configurations. To configure your Cisco IOS VPN gateway to create virtual-access interfaces from a virtual template for incoming PPTP calls, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# interface virtual-template number`	Creates the virtual template that is used to clone virtual-access interfaces.
Step 2	`hq-sanjose(config-if)# ip unnumbered interface-type number`	Specifies the IP address of the interface the virtual-access interfaces uses.
Step 3	`hq-sanjose(config-if)# ppp authentication ms-chap`	Enables MS-CHAP authentication using the local username database. All windows clients using MPPE need to use MS-CHAP.
Step 4	`hq-sanjose(config-if)# ip local pool default first-ip-address last-ip-address`	Configures the default local pool of IP addresses that will be used by clients.
Step 5	`hq-sanjose(config-if)# peer default ip address pool {default|name}`	Returns an IP address from the default pool to the client.
Step 6	`hq-sanjose(config-if)# ip mroute-cache`	Disables fast switching of IP multicast.
Step 7	`hq-sanjose(config-if)# ppp encrypt mppe {auto | 40 | 128} [passive | required] [stateful]`	(Optional) Enables MPPE encryption on the virtual template[1] if you are using an ISA with Cisco 7200 series router, see the "Configuring MPPE" section on page 4-6. **Note** The VAM, available on Cisco 7200 series routers, does not support MPPE.

1. Stateful MPPE encryption changes the key every 255 packets. Stateless (historyless) MPPE encryption generates a new key for every packet. Stateless MPPE is only supported in recent versions of Dial-Up Networking (DUN1.3).

Configuring PPTP

To configure a Cisco 7200 series router to accept tunneled PPP connections from a client, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# vpdn-enable`	Enables virtual private dialup networking on the router.
Step 2	`hq-sanjose(config)# vpdn-group 1`	Creates VPDN group 1.
Step 3	`hq-sanjose(config-vpdn)# accept dialin`	Enables the tunnel server to accept dial-in requests.
Step 4	`hq-sanjose(config-vpdn-acc-in)# protocol pptp`	Specifies that the tunneling protocol will be PPTP.
Step 5	`hq-sanjose(config-vpdn-acc-in)# virtual-template template-number`	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 6	`hq-sanjose(config-vpdn-acc-in)# exit` `hq-sanjose(config-vpdn)# local name localname`	(Optional) Specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

Configuring MPPE

Note The VPN Acceleration Module (VAM) card does not support MPPE.

To configure MPPE on your Cisco 7200 series router (with an ISA), use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# controller isa slot/port`	Enter controller configuration mode on the ISM card.
Step 2	`hq-sanjose(config-controller)# encryption mppe`	Enables MPPE encryption.

Verifying PPTP/MPPE

After you complete a connection, enter the **show vpdn tunnel** command or the **show vpdn session** command to verify your PPTP and MPPE configuration.The following example contains typical output:

```
hq-sanjose# show vpdn tunnel | show vpdn session
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name      State    Remote Address  Port  Sessions
22    22    172.16.230.29  estabd    172.16.230.29   1374  1
```

Configuring L2TP/IPSec

L2TP is an extension of the Point-to-Point (PPP) Protocol and is often a fundamental building block for VPNs. L2TP merges the best features of two other tunneling protocols: Layer 2 Forwarding (L2F) from Cisco Systems and PPTP from Microsoft. L2TP is an Internet Engineering Task Force (IETF) emerging standard.

Note For information on IPSec, see the "Step 3—Configuring Encryption and IPSec" section on page 3-13.

This section contains basic steps to configure L2TP/IPSec and includes the following tasks:

- Configuring a Virtual Template for Dial-In Sessions
- Configuring L2TP
- Configuring Encryption and IPSec

Configuring a Virtual Template for Dial-In Sessions

To configure your Cisco 7200 series router to create virtual-access interfaces from a virtual template for incoming L2TP calls, refer to the "Configuring a Virtual Template for Dial-In Sessions" section on page 4-5.

Note When configuring a virtual template for use with L2TP/IPSec, do not enable MPPE.

Configuring L2TP

To configure a Cisco 7200 series router to accept tunneled L2TP connections from a client, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# vpdn-enable`	Enables virtual private dialup networking on the router.
Step 2	`hq-sanjose(config)# vpdn-group 1`	Creates VPDN group 1.
Step 3	`hq-sanjose(config-vpdn)# accept dialin`	Enables the tunnel server to accept dial-in requests.
Step 4	`hq-sanjose(config-vpdn-acc-in)# protocol l2tp`	Specifies that the tunneling protocol will be L2TP.
Step 5	`hq-sanjose(config-vpdn-acc-in)# virtual-template` *template-number*	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 6	`hq-sanjose(config-vpdn-acc-in)# exit` `hq-sanjose(config-vpdn)# local name` *localname*	(Optional) Specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

Verifying L2TP

Enter the **show vpdn tunnel** command to verify your LT2P configuration.

```
hq-sanjose# show vpdn tunnel
L2TP Tunnel and Session Information (Total tunnels=5 sessions=5)

LocID RemID Remote Name   State  Remote Address  Port  Sessions
  10   8      7206b        est     10.0.0.1      1701      1

LocID RemID TunID Intf    Username    State  Last Chg Fastswitch
   4    6    10   Vi1      las          est   01:44:39   enabled
```

Configuring Encryption and IPSec

For detailed information on configuring encryption and IPSec, refer to the following sections of this guide:

- Configuring IKE Policies, page 3-14
- Verifying IKE Policies, page 3-19
- Creating Crypto Access Lists, page 3-21
- Verifying Crypto Access Lists, page 3-21
- Defining Transform Sets and Configuring IPSec Tunnel Mode, page 3-22
- Verifying Transform Sets and IPSec Tunnel Mode, page 3-23

Note When using IPSec with L2TP, do not configure IPSec tunnel mode.

- Creating Crypto Map Entries, page 3-24
- Verifying Crypto Map Entries, page 3-26
- Applying Crypto Maps to Interfaces, page 3-26

- Verifying Crypto Map Interface Associations, page 3-27

Note Although the configuration instructions in the listed sections refer to the "Extranet Scenario" section on page 3-4, the same configuration instructions apply to the remote access scenario described in the "Scenario Description" section on page 4-2.

Configuring Cisco IOS Firewall Authentication Proxy

Using the Cisco IOS firewall authentication proxy feature, network administrators can apply specific security policies on a per-user basis. Users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, in contrast with general policy applied across multiple users.

With the authentication proxy feature, users can log into the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from an authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and VPN client software.

This section contains basic steps to configure the Cisco IOS Firewall Authentication Proxy and includes the following tasks:

- Configuring Authentication, Authorization, and Accounting
- Configuring the HTTP Server
- Configuring the Authentication Proxy
- Verifying the Authentication Proxy

Configuring Authentication, Authorization, and Accounting

You must configure the authentication proxy for Authentication, Authorization, and Accounting (AAA) services. Use the following commands in global configuration mode to enable authorization and to define the authorization methods:

	Command	Purpose
Step 1	`hq-sanjose(config)# aaa new-model`	Enables the AAA functionality on the router.
Step 2	`hq-sanjose(config)# aaa authentication login default` *TACACS+ RADIUS*	Defines the list of authentication methods at login.
Step 3	`hq-sanjose(config)# aaa authorization auth-proxy default` [*method1* [*method2...*]]	Enables authentication proxy for AAA methods.
Step 4	`hq-sanjose(config)# tacacs-server host` *hostname*	Specifies an AAA server. For RADIUS servers, use the **radius server host** command.
Step 5	`hq-sanjose(config)# tacacs-server key` *sting*	Sets the authentication and encryption key for communications between the router and the AAA server. For RADIUS servers use the **radiusserverkey** command.

	Command	Purpose
Step 6	`hq-sanjose(config)# access-list` *access-list-number* **permit** *tcp* **host** *source* **eq** *tacacs* **host** *destination*	Creates an ACL entry to allow the AAA server return traffic to the firewall. The source address is the IP address of the AAA server, and the destination address is the IP address of the router interface where the AAA server resides.

In addition to configuring AAA on the firewall router, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service "auth-proxy" on the AAA server as outlined here:

- Define a separate section of authorization for **auth-proxy** to specify the downloadable user profiles. This does not interfere with other types of service, such as EXEC. The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
service = auth-proxy
{
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 60.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
```

- The only supported attribute in the AAA server user configuration is **proxyacl#***n.* Use the **proxyacl#***n* attribute when configuring the access lists in the profile. The attribute **proxyacl#***n* is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.
- The access lists in the user profile on the AAA server must have **permit** only access commands.
- Set the source address to **any** in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are CiscoSecure ACS 2.1.x for Window NT (where x is a number 0 to 12) and CiscoSecure ACS 2.3 for Windows NT, CiscoSecure ACS 2.2.4 for UNIX and CiscoSecure ACS 2.3 for UNIX, TACACS+ server (vF4.02.alpha), Ascend RADIUS server - radius-980618 (required avpair patch), and Livingston RADIUS server (v1.16).

Configuring the HTTP Server

To use the authentication proxy, you must also enable the HTTP server on the firewall and set the HTTP server authentication method to use AAA. Enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# ip http server`	Enables the HTTP server on the router. The authentication proxy uses the HTTP server to communicate with the client for user authentication.

	Command	Purpose
Step 2	`hq-sanjose(config)# ip http authentication aaa`	Sets the HTTP server authentication method to AAA.
Step 3	`hq-sanjose(config)# ip http access-class access-list-number`	Specifies the access list for the HTTP server.

Configuring the Authentication Proxy

To configure the authentication proxy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# ip auth-proxy auth-cache-time min`	Sets the global authentication proxy idle timeout value in minutes. If the timeout expires, user authentication entries are removed, along with any associated dynamic access lists. The default value is 60 minutes.
Step 2	`hq-sanjose(config)# ip auth-proxy auth-proxy-banner`	(Optional) Displays the name of the firewall router on the authentication proxy login page. The banner is disabled by default.
Step 3	`hq-sanjose(config)# ip auth-proxy name auth-proxy-name http [auth-cache-time min] [list std-access-list]`	Creates authentication proxy rules. The rules define how you apply authentication proxy. This command associates connection initiating HTTP protocol traffic with an authentication proxy name. You can associate the named rule with an access control list, providing control over which hosts use the authentication proxy feature. If no standard access list is defined, the named authentication proxy rule intercepts HTTP traffic from all hosts whose connection initiating packets are received at the configured interface. (Optional) The **auth-cache-time** option overrides the global authentication proxy cache timer. This option provides more control over timeout values for a specific authentication proxy rule. If no value is specified, the proxy rule assumes the value set with the **ip auth-proxy auth-cache-time** command. (Optional) The **list** option allows you to apply a standard access list to a named authentication proxy rule. HTTP connections initiated from hosts in the access list are intercepted by the authentication proxy.
Step 4	`hq-sanjose(config)# interface type`	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 5	`hq-sanjose(config-if)# ip auth-proxy auth-proxy-name`	In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

Verifying the Authentication Proxy

To check the current authentication proxy configuration, use the **show ip auth-proxy configuration** command in privileged EXEC mode. In the following example, the global authentication proxy idle timeout value is set to 60 minutes, the named authentication proxy rule is "pxy," and the idle timeout value for this named rule is 1 minute. The display shows that no host list is specified, meaning that all connections initiating HTTP traffic at the interface are subject to the authentication proxy rule:

```
router# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 1 minutes
```

To verify that the authentication proxy is successfully configured on the router, ask a user to initiate an HTTP connection through the router. The user must have authentication and authorization configured at the AAA server. If the user authentication is successful, the firewall completes the HTTP connection for the user. If the authentication is unsuccessful, check the access list and the AAA server configurations.

Display the user authentication entries using the **show ip auth-proxy cache** command in privileged EXEC mode. The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.

```
router# show ip auth-proxy cache
Authentication Proxy Cache
Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

Wait for one minute, which is the timeout value for this named rule, and ask the user to try the connection again. After one minute, the user connection is denied because the authentication proxy has removed the user authentication entry and any associated dynamic ACLs. The user is presented with a new authentication login page and must log in again to gain access through the firewall.

Comprehensive Configuration Examples

This section contains PPTP/MPPE, and L2TP/IPSec comprehensive sample configurations for the headquarters Cisco 7200 series router.

PPTP/MPPE Configuration

```
hq-sanjose# show running-config

Current configuration
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mp12
!
no logging console guaranteed
enable password lab
!
username tester41 password 0 lab41
!
```

```
ip subnet-zero
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
! Default PPTP VPDN group
accept-dialin
  protocol pptp
  virtual-template 1
local name cisco_pns
!
memory check-interval 1
!
controller ISA 5/0
encryption mppe
!
process-max-time 200
!
interface FastEthernet0/0
ip address 10.1.3.3 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.1.6.4 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
!
interface Serial1/0
no ip address
no ip directed-broadcast
shutdown
framing c-bit
cablelength 10
dsu bandwidth 44210
!
interface Serial1/1
no ip address
no ip directed-broadcast
shutdown
framing c-bit
cablelength 10
dsu bandwidth 44210
!
interface FastEthernet4/0
no ip address
no ip directed-broadcast
shutdown
duplex half
!
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
ip mroute-cache
no keepalive
ppp encrypt mppe 40
ppp authentication ms-chap
!
ip classless
ip route 172.29.1.129 255.255.255.255 1.1.1.1
ip route 172.29.63.9 255.255.255.255 1.1.1.1
```

```
no ip http server
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
aaa new-model
aaa authentication login default tacacs+ radius
!Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default tacacs+ radius
!Define the AAA servers used by the router
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
!
! Enable the HTTP server on the router:
ip http server
! Set the HTTP server authentication method to AAA:
ip http authentication aaa
!Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
!
!set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
!Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
!
! Apply the authentication proxy rule at an interface.
interface e0
    ip address 10.1.1.210 255.255.255.0
    ip auth-proxy HQ_users
!
end
```

L2TP/IPSec Configuration

```
hq-sanjose# show running-config

Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname LNS
 !
 enable password ww
 !
 username LNS password 0 tunnelpass
 username test@cisco.com password 0 cisco
 ip subnet-zero
 !
 vpdn enable
 !
 vpdn-group 1
```

```
 accept dialin l2tp virtual-template 1 remote LAC
 local name LNS
!
crypto isakmp policy 1
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key cisco address 172.1.1.1
!
crypto ipsec transform-set testtrans esp-des
!
 !
 crypto map l2tpmap 10 ipsec-isakmp
 set peer 172.1.1.1
 set transform-set testtrans
 match address 101
!
interface Ethernet 0/0
 ip address 10.1.3.3 255.255.255.0
 no ip directed-broadcast
 no keepalive
!
interface Ethernet 0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 no ip route-cache
 peer default ip address pool mypool
 ppp authentication chap
!
interface Serial 1/0
 ip address 172.17.2.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no fair-queue
 clockrate 1300000
 crypto map l2tpmap
!
interface Serial 0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip local pool mypool 172.16.3.1 172.20.10.10
no ip classless
!
access-list 101 permit udp host 172.17.2.4 eq 1701 host 172.1.1.1 eq 1701
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
aaa new-model
aaa authentication login default tacacs+ radius
!Set up the aaa new model to use the authentication proxy.
```

```
aaa authorization auth-proxy default tacacs+ radius
!Define the AAA servers used by the router
tcacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
!
! Enable the HTTP server on the router:
ip http server
! Set the HTTP server authentication method to AAA:
ip http authentication aaa
!Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
!
!set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
!Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
!
! Apply the authentication proxy rule at an interface.
interface e0
   ip address 10.1.1.210 255.255.255.0
   ip auth-proxy HQ_users
!
end
```

VPN Network Management Tools

This chapter discusses select Cisco VPN network management software. Each section discusses the particular environments in which the network management tool is applicable.

This chapter includes the following sections:

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) should be used for multi-device, multi-platform VPN, firewall, and IDS (Intrusion Detection System) configuration.

CSPM is a multi-device policy-based management tool for Cisco security products, including PIX Firewalls, the Cisco IOS firewall feature set, Cisco 7200 series router, and Intrusion Detection System (IDS) Sensors. CSPM allows these security devices to be configured and managed with an easy-to-use graphical user interface (GUI). CSPM simplifies the configuration of complex VPN and security devices by creating each device configuration file after the security policies have been defined. CSPM also distributes each device configuration in a secure fashion with IPSec. CSPM allows security devices to be configured from a central location. CSPM also provides other management services including monitoring, notification, and reporting.

CSPM increases the scalability of VPN and security networks by centralizing the management of all devices within a network. CSPM facilitates the deployment of remote VPN devices and firewalls including colocated DSL and Cable Modem users. IPSec templates are included in CSPM for both meshed and hub-and-spoke networks. CSPM adds value in any security networking environment by simplifying small security networks, multi-site enterprise deployments and large service provider environments by centralizing and abstracting the management of security networks.

See the *Cisco Secure Policy Manager* for more information

Cisco VPN/Security Management Solution

The Cisco VPN/Security Management Solution should be used to implement comprehensive, multi-device VPN configuration and monitoring, firewall configuration, and infrastructure management.

The Cisco VPN/Security Management Solution provides key functionality to assist customers who are deploying Cisco 7200 series routers and who require monitoring of remote access and site-to-site VPNs, based upon IPSec, L2TP, and PPTP. The solution also provides key features for deployment and management of perimeter security using the Cisco PIX Firewall.

Note The term 'Cisco 7200 series router' in this Guide implies that an Integrated Service Adaptor (ISA) or a VAM (VAM, VAM2, or VAM2+) is installed in the Cisco 7200 series router.

The following modules are included in the Cisco VPN/Security Management Solution. Together, these modules provide essential VPN and security management capabilities:

- Cisco Secure Policy Manager Lite (CSPM-Lite)— Provides policies for defining VPN policies on Cisco 7200 series routers and PIX Firewalls. CSPM also defines security policies on Cisco PIX Firewalls, and reporting and notifying of intrusions when Cisco Intrusion Detection Sensors technology is deployed.
- Cisco VPN Monitor is a web-based management tool that allows network administrators to collect, store, and report information on L2TP, PPTP remote access, and IPSec-based site-to-site VPNs configured on the Cisco 7200 series routers, Cisco 3600 series routers, Cisco 2600 series routers, Cisco 1700 series routers, Cisco 800 series routers, and Cisco VPN 3000 Concentrator Series. Multiple devices can be viewed from an easy-to-use dashboard configured on a web browser. After the dashboard is configured, Cisco VPN Monitor continuously collects data from the devices it manages over a rolling seven-day window. Operational status, performance, and security information can be viewed at a glance, providing status information on IPsec VPN implementations.

Note The Cisco VPN Monitor does not support PIX Firewalls. For information on monitoring PIX Firewalls, see the PIX Firewall System Management documentation.

- Resource Manager Essentials (RME)—Provides the operational management features required by enterprises. RME features include software distribution, change audit and authorization, device inventory and credentials management and Syslog analysis for problem solving and notification of VPN and security operational problems.
- CiscoWorks2000 Inventory Services (CD Two) — Cisco VPN/Security Management Solution provides an installation option for customers who want to install only the inventory administration tools of RME. Inventory Services tracks the network devices, and reports hardware and software characteristics, and provides device credentials management.
- CiscoView—Provides administrators with browser access to real-time device status, and operational and configuration functions. CiscoView is the most widely used Cisco graphical device management application and is now web-based.
- CiscoWorks2000 Management Server (CD-One)— Provides the common database, web, and desktop services used to integrate with other Cisco and third- party tools.

See the following websites for further information:

- Update for CiscoWorks VPN/Security Management Solution 2.1
- CiscoWorks VPN/Security Management Solution

- CiscoWorks VPN/Security Management Solution FAQ

IPSec MIB and Third Party Monitoring Applications

The IPSec MIB feature allows users to configure and monitor their IPSec MIB tunnel tables and their trap notifications using Simple Network Management Protocol (SNMP). IPSec MIB can increase the performance of your Cisco VPN, as trap notifications can be sent only once and are discarded as soon as they are sent. This reduces traffic and creates lower overhead on your network. This feature allows users to specify the desired size of a tunnel history table or a tunnel failure table. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also allows a router to send IPSec trap notifications, which are MIB related, to a random or specified host. A trap notification may be sent when a particular event, such as an error, occurs.

Note The traps are not supported in the current version of the MIB. They only pertain to the Cisco IOS-specific IPSec MIB.

The IPSec MIB feature is used in conjunction with an SNMP agent, which is based on Version 1 of the SNMP protocol. The SNMP agent implements the IPSec MIB subsystem, which implements the MIBs referred to in the "Supported Standards, MIBs, and RFCs" section of this feature module. By allowing the user to adjust tunnel tables and enable IPSec trap notifications, the IPSec MIB feature provides enhancements to the SNMP agent process.

See IPSec—SNMP Support for more information on IPSec MIB.

Cisco VPN Device Manager

This section provides an overview of Cisco VPN Device Manager (VDM). VDM is a wizard-based GUI application that allows simplified VPN configuration of the device on which it resides.

This section includes the following topics:

- VDM Overview
- Installing and Running VDM
- Using VDM to Configure VPNs
- Using VDM to Monitor VPNs
- Using VDM to Troubleshoot Connectivity
- Related Documents

VDM Overview

VDM enables network administrators to manage and configure site-to-site VPNs on a single IOS VPN device from a web browser, and view the effects of their changes in real time. VDM implements a wizard-based GUI to simplify the process of configuring site-to-site VPNs using the IPSec protocol.

VDM software is installed directly on Cisco VPN devices. It is designed for use and compatibility with other device manager products.

Note VDM supports site-to-site VPNs but not remote-client access VPNs.

Figure 5-1 shows the **VDM Home Page** page under the System menu. This is the first window to appear after you launch VDM and is the starting point for all other VDM activities.

The following other options are also available from the System menu:

- IOS Config—displays device Cisco IOS configuration information
- Log—displays messages about VDM activity

Figure 5-1 VDM Home Page

Number	Description
1	Application menu bar
2	Application-specific primary menu bar
3	Application-specific secondary menu bar
4	Application status bar
between 3 and 4	Application content area

Using a browser, you can log into a Cisco device and use VDM to efficiently configure VPNs on it. You can set particular tunneling, encryption, and other VPN options, which can then be applied to the interfaces facing peer devices. Use VDM to conveniently troubleshoot specific problems and perform configuration updates and changes.

Cisco IOS Commands

You must configure some Cisco IOS CLI commands before VDM becomes fully operational. Details about these commands can be found in the Cisco IOS feature document *VPN Device Manager*.

Benefits

This section contains information about the following benefits of using VDM:

- Configuration Wizards
- Single Device Configuration
- Monitoring Functions
- Convenient Navigation
- No Client Installation

Configuration Wizards

Browser-based VDM wizards help you perform ordinarily complex setup operations including:

- Step-by-step instructional panes for simplified VPN configuration, such as peer-to-peer setup.
- Tunneling and encryption support using transform sets, key lifetimes, IKE policies, security association (SA) lifetime, authentication policies, error reports, and performance monitoring.

Single Device Configuration

VDM configures only the device from which it is launched. It does not read or write configuration information to or from other devices.

Monitoring Functions

Monitored data in graphs and charts contains basic device information, a VPN report card, top-ten lists, and detailed views of user-specified tunnels that monitor duration, errors, and throughput.

Convenient Navigation

The following navigation methods ensure that you can conveniently identify your current location within each wizard:

- Cascading highlighted menu tabs at the top of the GUI.
- A step-by-step tasks list in each wizard's left frame contains a highlighted bar which moves down the list as you progress through that wizard.

No Client Installation

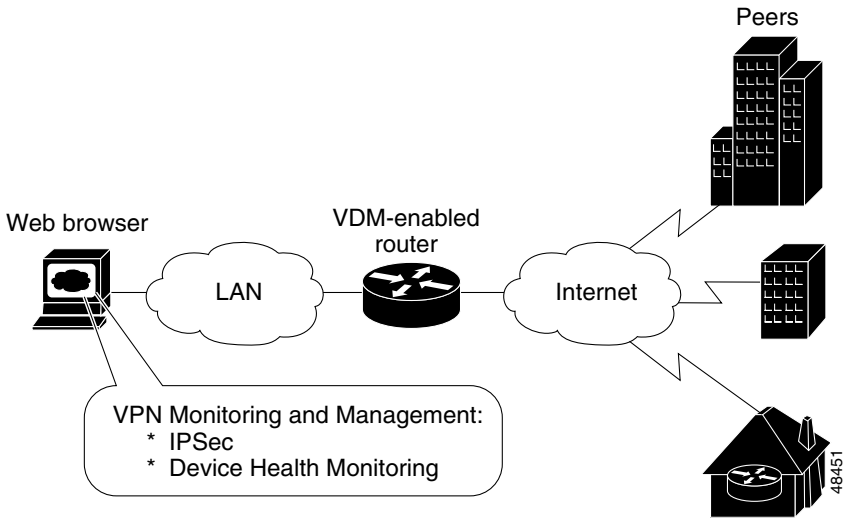
VDM is distributed in the following two components:

- Crypto-enabled Cisco IOS image containing the necessary VPN subsystems.

- File to be installed on the Cisco IOS Flash memory file system.

Figure 5-2 shows the type of VPN that VDM can configure:

Figure 5-2 Simplified VDM Deployment



Installing and Running VDM

You can install the VDM client on your Cisco device in the following ways:

- Order the device with VDM installed (if the device is ordered new).
- Install a Cisco IOS version that VDM supports and upload the VDM client to the device Flash memory.

VDM supports crypto-enabled IOS images. See *VPN Device Manager - Release and Installation Notes* for further information on obtaining the correct Cisco IOS image.

To simplify its use, VDM starts as a GUI into a web-browser home page that is run from the managed device (VPN device on which VDM is installed) at connection time. VDM is a Java application that uses continuous XML data exchange to update the appropriate part of the VDM GUI.

The VDM GUI contains step-by-step configuration wizards for common VPN setups, interfaces, and policies and protocols, including:

- IPSec tunnels
- Pre-shared keys and Internet Key Exchange (IKE) policies

Note VDM does not work with RSA-encrypted nonces. (Nonces are random numbers or keys that are generated once and not reused.)

Using VDM to Configure VPNs

VDM configuration wizards make it easier to perform ordinarily complex setup operations and configure VPN connections.

Table 5-1 describes the following VDM browser-based configuration wizards:

Table 5-1 VDM Configuration Wizard Descriptions

Wizard	Description
Certificates	Starts the Certificates wizard, which allows you to enroll the device with a certificate authority and use digital certificates for authenticating peers.
Connections	Starts the Connections wizard, which creates VPN protected connections for selected traffic between selected local and remote hosts and subnets.
IKE	Starts the IKE wizard, which allows you to create IKE policies that determine how IKE establishes SAs with peers.
Peer Keys	Starts the Peer Keys wizard, which assigns and edits pre-shared keys, used to authenticate peers.
Transforms	Starts the Transforms wizard, which creates transform sets to authenticate, encrypt, and compress VPN traffic.
VLANs	Starts the VLANs wizard, which allows you to create access and interface VLANs on the device.

These configuration wizards contain:

- Simple step-by-step instructions for configuring simple VPNs.
- Tunneling and encryption support using transforms sets, key lifetimes, IKE policies, SA lifetime, authentication policies, error reports, and performance monitoring.

The wizard navigation buttons within the VDM Configure menu allow for flexible multi-directional navigation. The wizard configuration action buttons within the same menu allow you to create or modify your VPN settings conveniently.

Figure 5-3 shows the **Connections** page for the VDM Connections wizard. This wizard allows you to add, edit, or remove VPN connections. The **Select a Connection** list displays existing connections.

The **Connection Description** list provides the following details about the selected connection:

- IP addresses of peers
- Local and remote hosts and subnets
- Protocols
- Transforms
- The interface VLAN that acts as the inside interface to a IPSec VPN Acceleration Serviced Module (only on devices that contain this module)
- Interface(s) to which the connection is applied

Figure 5-3 VDM Connections Wizard Overview Page

Figure 5-4 shows the **Certificates** page for the VDM Certificates wizard. This wizard allows you to enroll a certificate identity with the Certificate Authority (CA) by using the Certificate Enrollment wizard, as well as add, edit, and remove existing certificate identities.

The **Select a Certificate Identity** list displays existing certificate identities. The **Certificate Identity Description** list provides the following details about the selected certificate identity, such as:

- Enrolled URL
- Proxy host and port
- Retry specifics

Figure 5-4 VDM Certificates Wizard Overview Page

Figure 5-5 shows the **IKE Overview** page for the VDM IKE wizard. This wizard allows you to add, edit, or remove IKE policies.

The **Select a Policy** list displays existing user-configured policies, as well as one global and one default IKE policy. The **Policy Description** list provides the following details about the policy selected:

- Encryption and hash algorithms
- Authentication method
- SA specifics

Figure 5-5 VDM IKE Wizard Overview Page

Using VDM to Monitor VPNs

VDM monitors general system statistics and VPN-specific information such as tunnel throughput and errors. You can configure VPNs in parallel, while monitoring is automatically updated based upon a selected polling interval. The graphing capability allows you to compare such parameters as traffic volume, tunnel counts, and system utilization.

Figure 5-6 shows the **VDM Charts** page with the CPU Utilization chart selected. You can generate many charts from this page based on your charting object and charting object attribute selections.

The left list displays all objects with attributes that can be charted, such as CPU, IKE, IPSec, and a variety of interfaces. The right list displays all object attributes associated with a selected object.

You must first select an object attribute to generate a chart. For example, under the IPSec object, you have a choice of the following three different object attributes:

- Tunnels
- Total throughput
- Total crypto throughput

Available object attributes vary according to the selected object. For example, chartable object attributes for the Interface object include the following:

- In and out packets
- Dropped packets
- Octets
- Errors

You can customize charts to display both historical and real-time data from periods as short as 10 minutes to as much as 5 days.

Figure 5-6 VDM Charts Page with CPU Utilization Chart

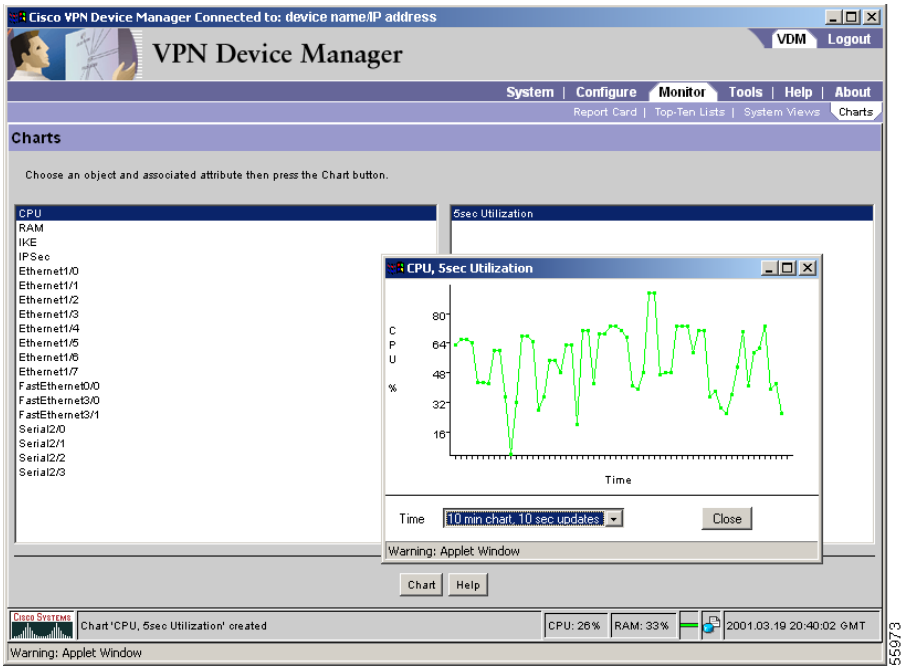


Figure 5-7 shows the **VDM Report Card** page, which displays information about the following activity on the device:

- Total throughput
- Crypto throughput and failures
- IKE and IPSec Tunnels
- Replayed Packets

Figure 5-7 VDM Report Card Page

Figure 5-8 shows the **VDM Top-Ten Lists** page, which displays details about IKE and IPSec tunnels by duration, errors, and traffic volume. You can select any of these reports from the drop-down list.

A top-ten list is a list of 10 tunnels on the device that rank highest when measured by particular criteria. For example, you can view a list of the 10 IKE tunnels on the device that have the highest traffic volume.

Each top-ten list displays information about the following:

- Monitored tunnels
- Tunnel source devices
- Peers
- Transmitted packets and bytes
- SA details

Figure 5-8 VDM Top-Ten Lists Page

Using VDM to Troubleshoot Connectivity

VDM allows you to test device connectivity using two different methods—traceroute or ping. Figure 5-9 shows the **VDM Test Connectivity** page executing the ping command. These options function the same way as executing these commands from the CLI.

Figure 5-9 VDM Test Connectivity Page

Related Documents

Further information on VDM can be found in the following related documents:

- *VPN Device Manager* Cisco IOS feature document
- *Installation and Release Notes for VPN Device Manager*
- *VPN Device Manager Online Help*

For additional information, see the Cisco VPN Device Manager (VDM).

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W