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

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.

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

$\mathcal{Q}$

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