



About This Guide

This guide explains how to configure many fundamental VPN features in the Adaptive Security Appliance (ASA) software. In most cases, it provides instructions for both CLI and the device manager. The description of each feature includes at least one example that illustrates configuration steps with a basic or simple scenario. In general, the instructions show the same values in both CLI and ASDM, although there are a few exceptions.

Audience

This guide is for system engineers (SEs) and network administrators who set up and configure ASAs for virtual private networking. These SEs and customers are familiar with virtual private networking from the perspective of a VPN 3000 Concentrator and need guidance on performing familiar tasks in the ASA software environment.

This document should help you come up to speed quickly on the new system. You should be familiar with networking equipment, basic networking concepts, virtual private networking, and the VPN 3000 Concentrator Manager.

Organization

This guide is organized as follows:

| Chapter | Title | Description |
|-----------|--|--|
| Chapter 1 | Feature Differences | Maps the features in the VPN 3000 Concentrator Features to those in the ASA. |
| Chapter 2 | Introducing the ASA System | Highlights major features of the ASA that are different from the VPN 3000 Concentrator. |
| Chapter 3 | Getting Started | Introduces the Startup wizard and the VPN wizard in the ASDM and lists the information you should have before using the wizards. Compares the Getting Started program in the VPN 3000 Concentrator with these wizards. |

| Chapter | Title | Description |
|------------|--|--|
| Chapter 4 | Building Basic IPSec VPN Tunnels | Shows how to configure VPN LAN-to-LAN and remote-access tunnels using CLI commands and using Adaptive Security Device Manager (ASDM). Also shows how to enroll for digital certificates. |
| Chapter 5 | Performing Selected User Management Tasks | Shows how to configure split tunneling, client firewalls, and how to authenticate using RADIUS. |
| Chapter 6 | Configuring Traffic Management | Shows how to configure load balancing and quality of service features. |
| Appendix A | Mapping Topics from VPN 3000 Series Concentrators to ASDM | Maps configuration and management topics of the VPN 3000 Concentrator Manager and ASDM. |
| Appendix B | Mapping Debug/Event Levels from VPN 3000 Series Concentrators to the ASA | Maps the logging security levels in the VPN 3000 Concentrator Manager to the ASA. |

Related Documentation

This guide is a companion to the following user guides:

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Release Notes for Cisco Secure Desktop*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

Conventions

This document uses the following conventions:

| Convention | Description |
|-----------------------------|---|
| boldface font | User actions and commands are in boldface . |
| <i>italic font</i> | Arguments for which you supply values are in <i>italics</i> . |
| 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 in the command-line interface (for example, vpnclient stat). |

Notes use the following conventions:

**Note**

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

Cautions use the following conventions:

**Caution**

Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

| Type of Data | Format |
|---------------------------------|--|
| IP Addresses | IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position. |
| Subnet Masks and Wildcard Masks | Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position. |
| MAC Addresses | MAC addresses use 6-byte hexadecimal notation (for example, 0001.03cf.0238). |
| Hostnames | Hostnames use legitimate network hostname or end-system name notation (for example, VPN01). Spaces are not allowed. A hostname must uniquely identify a specific system on a network. |
| Text Strings | Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters. |
| Port Numbers | Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number. |

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/univercd/home/home.htm>

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *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>

- *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>

- 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>

