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**.
italic font	Arguments for which you supply values are in *italics*.
`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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.