About This Guide

This preface introduce the *Cisco Security Appliance Command Line Configuration Guide*, and includes the following sections:

Document Objectives

The purpose of this guide is to help you configure the security appliance using the command-line interface. This guide does not cover every feature, but describes only the most common configuration scenarios.

You can also configure and monitor the security appliance by using ASDM, a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online Help for less common scenarios. For more information, see:

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

This guide applies to the Cisco PIX 500 series security appliances (PIX 515E, PIX 525, and PIX 535) and the Cisco ASA 5500 series security appliances (ASA 5510, ASA 5520, and ASA 5540). Throughout this guide, the term “security appliance” applies generically to all supported models, unless specified otherwise. The PIX 501, PIX 506E, and PIX 520 security appliances are not supported in software Version 7.0.

Audience

This guide is for network managers who perform any of the following tasks:

- Manage network security
- Install and configure firewalls/security appliances
- Configure VPNs
- Configure intrusion detection software

Related Documentation

For more information, refer to the following documentation:

- *Cisco PIX Security Appliance Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco PIX 515E Quick Start Guide*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco Security Appliance Logging Configuration and System Log Messages*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*

Document Organization

This guide includes the chapters and appendixes described in Table 1.

Table 1 Document Organization

Chapter/Appendix	Definition
Part 1: Getting Started and General Information	
Chapter 1, “Introduction to the Security Appliance”	Provides a high-level overview of the security appliance.
Chapter 2, “Getting Started”	Describes how to access the command-line interface, configure the firewall mode, and work with the configuration.
Chapter 3, “Enabling Multiple Context Mode”	Describes how to use security contexts and enable multiple context mode.
Chapter 4, “Configuring Ethernet Settings and Subinterfaces”	Describes how to configure Ethernet settings for physical interfaces and add subinterfaces.
Chapter 5, “Adding and Managing Security Contexts”	Describes how to configure multiple security contexts on the security appliance.
Chapter 6, “Configuring Interface Parameters”	Describes how to configure each interface and subinterface for a name, security, level, and IP address.
Chapter 7, “Configuring Basic Settings”	Describes how to configure basic settings that are typically required for a functioning configuration.
Chapter 8, “Configuring IP Routing and DHCP Services”	Describes how to configure IP routing and DHCP.
Chapter 9, “Configuring IPv6”	Describes how to enable and configure IPv6.
Chapter 10, “Configuring AAA Servers and the Local Database”	Describes how to configure AAA servers and the local database.

Table 1 Document Organization (continued)

Chapter/Appendix	Definition
Chapter 11, "Configuring Failover"	Describes the failover feature, which lets you configure two security appliances so that one will take over operation if the other one fails.
Part 2: Configuring the Firewall	
Chapter 12, "Firewall Mode Overview"	Describes in detail the two operation modes of the security appliance, routed and transparent mode, and how data is handled differently with each mode.
Chapter 13, "Identifying Traffic with Access Lists"	Describes how to identify traffic with access lists.
Chapter 14, "Applying NAT"	Describes how address translation is performed.
Chapter 15, "Permitting or Denying Network Access"	Describes how to control network access through the security appliance using access lists.
Chapter 16, "Applying AAA for Network Access"	Describes how to enable AAA for network access.
Chapter 17, "Applying Filtering Services"	Describes ways to filter web traffic to reduce security risks or prevent inappropriate use.
Chapter 18, "Using Modular Policy Framework"	Describes how to use the Modular Policy Framework to create security policies for TCP, general connection settings, inspection, and QoS.
Chapter 19, "Managing the AIP SSM and CSC SSM"	Describes how to configure the security appliance to send traffic to an AIP SSM or a CSC SSM, how to check the status of an SSM, and how to update the software image on an intelligent SSM.
Chapter 20, "Preventing Network Attacks"	Describes how to configure protection features to intercept and respond to network attacks.
Chapter 21, "Applying QoS Policies"	Describes how to configure the network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP routed networks.
Chapter 22, "Configuring Application Layer Protocol Inspection"	Describes how to use and configure application inspection.
Chapter 23, "Configuring ARP Inspection and Bridging Parameters"	Describes how to enable ARP inspection and how to customize bridging operations.
Part 3: Configuring VPN	
Chapter 24, "Configuring IPsec and ISAKMP"	Describes how to configure ISAKMP and IPSec tunneling to build and manage VPN "tunnels," or secure connections between remote users and a private corporate network.
Chapter 25, "Setting General IPSec VPN Parameters"	Describes miscellaneous VPN configuration procedures.
Chapter 26, "Configuring Tunnel Groups, Group Policies, and Users"	Describes how to configure VPN tunnel groups, group policies, and users.
Chapter 27, "Configuring IP Addresses for VPNs"	Describes how to configure IP addresses in your private network addressing scheme, which let the client function as a tunnel endpoint.
Chapter 28, "Configuring Remote Access IPSec VPNs"	Describes how to configure a remote access VPN connection.

Table 1 Document Organization (continued)

Chapter/Appendix	Definition
Chapter 29, "Configuring LAN-to-LAN IPsec VPNs"	Describes how to build a LAN-to-LAN VPN connection.
Chapter 30, "Configuring WebVPN"	Describes how to establish a secure, remote-access VPN tunnel to a security appliance using a web browser.
Chapter 31, "Configuring SSL VPN Client"	Describes how to install and configure the SSL VPN Client.
Chapter 32, "Configuring Certificates"	Describes how to configure a digital certificates, which contains information that identifies a user or device. Such information can include a name, serial number, company, department, or IP address. A digital certificate also contains a copy of the public key for the user or device.
Part 4: System Administration	
Chapter 33, "Managing System Access"	Describes how to access the security appliance for system management through Telnet, SSH, and HTTPS.
Chapter 34, "Managing Software, Licenses, and Configurations"	Describes how to enter license keys and download software and configurations files.
Chapter 35, "Monitoring the Security Appliance"	Describes how to monitor the security appliance.
Chapter 36, "Troubleshooting the Security Appliance"	Describes how to troubleshoot the security appliance.
Part 4: Reference	
Appendix A, "Feature Licenses and Specifications"	Describes the feature licenses and specifications.
Appendix B, "Sample Configurations"	Describes a number of common ways to implement the security appliance.
Appendix C, "Using the Command-Line Interface"	Describes how to use the CLI to configure the the security appliance.
Appendix D, "Addresses, Protocols, and Ports"	Provides a quick reference for IP addresses, protocols, and applications.
Appendix E, "Configuring an External Server for Authorization and Authentication"	Provides information about configuring LDAP and RADIUS authorization servers.

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.

-
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **`boldface screen`** font.
- Variables for which you must supply a value are shown in *`italic screen`* font.

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

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.