



## About This Guide

---

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface includes the following sections:

- [Document Objectives, page xxxvii](#)
- [Audience, page xxxvii](#)
- [Related Documentation, page xxxviii](#)
- [Document Organization, page xxxviii](#)
- [Document Conventions, page xli](#)
- [Obtaining Documentation and Submitting a Service Request, page xli](#)

## Document Objectives

The purpose of this guide is to help you configure the adaptive 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 adaptive 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.

This guide applies only to the Cisco ASA 5580 adaptive security appliance.

## Audience

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

- Manage network security
- Configure firewalls
- Configure VPNs

## Related Documentation

For more information, refer to the following documentation:

- *Navigating the Cisco ASA 5500 Series Documentation*
- *Cisco ASA 5580 Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5580 Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco ASA 5580 Adaptive Security Appliance Command Reference*
- *Cisco ASA 5580 Adaptive Security Appliance System Log Messages Guide*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*
- *Open Source Software Licenses for Cisco ASA 5580 Adaptive Security Appliance*

## Document Organization

This guide includes the chapters and appendixes described in [Table 1](#).

**Table 1** Document Organization

Chapter/Appendix	Definition
<b>Part 1: Getting Started and General Information</b>	
Chapter 1, “Introduction to the Security Appliance”	Provides a high-level overview of the adaptive 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, Redundant Interfaces, 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 adaptive 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”	Describes how to configure IP routing.
Chapter 9, “Configuring DHCP, DDNS, and WCCP Services”	Describes how to configure the DHCP server and DHCP relay.
Chapter 10, “Configuring Multicast Routing”	Describes how to configure multicast routing.
Chapter 11, “Configuring IPv6”	Describes how to enable and configure IPv6.

**Table 1** Document Organization (continued)

Chapter/Appendix	Definition
Chapter 12, “Configuring AAA Servers and the Local Database”	Describes how to configure AAA servers and the local database.
Chapter 13, “Configuring Failover”	Describes the failover feature, which lets you configure two adaptive security appliances so that one will take over operation if the other one fails.
Chapter 14, “Identifying Traffic with Access Lists”	Describes how to identify traffic with access lists.
Chapter 15, “Using Modular Policy Framework”	Describes how to use the Modular Policy Framework to create security policies for TCP, general connection settings, inspection, and QoS.
<b>Part 2: Configuring the Firewall</b>	
Chapter 16, “Firewall Mode Overview”	Describes in detail the two operation modes of the adaptive security appliance, routed and transparent mode, and how data is handled differently with each mode.
Chapter 17, “Configuring NAT”	Describes how address translation is performed.
Chapter 18, “Permitting or Denying Network Access”	Describes how to control network access through the adaptive security appliance using access lists.
Chapter 19, “Applying AAA for Network Access”	Describes how to enable AAA for network access.
Chapter 20, “Applying Filtering Services”	Describes ways to filter web traffic to reduce security risks or prevent inappropriate use.
Chapter 21, “Preventing Network Attacks”	Describes how to configure protection features to intercept and respond to network attacks.
Chapter 22, “Configuring QoS”	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 23, “Configuring Application Layer Protocol Inspection”	Describes how to use and configure application inspection.
Chapter 24, “Configuring ARP Inspection and Bridging Parameters in Transparent Mode”	Describes how to enable ARP inspection and how to customize bridging operations.
<b>Part 3: Configuring VPN</b>	
Chapter 25, “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 26, “Configuring L2TP over IPsec”	Describes how to configure IPsec over L2TP on the adaptive security appliance.
Chapter 27, “Setting General IPsec VPN Parameters”	Describes miscellaneous VPN configuration procedures.
Chapter 28, “Configuring Connection Profiles, Group Policies, and Users”	Describes how to configure VPN tunnel groups, group policies, and users.
Chapter 29, “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.

**Table 1** Document Organization (continued)

Chapter/Appendix	Definition
Chapter 30, “Configuring Remote Access IPsec VPNs”	Describes how to configure a remote access VPN connection.
Chapter 31, “Configuring Network Admission Control”	Describes how to configure Network Admission Control (NAC).
Chapter 32, “Configuring the PPPoE Client”	Describes how to configure the PPPoE client provided with the adaptive security appliance.
Chapter 33, “Configuring LAN-to-LAN IPsec VPNs”	Describes how to build a LAN-to-LAN VPN connection.
Chapter 34, “Configuring Clientless SSL VPN”	Describes how to establish a secure, remote-access VPN tunnel to a adaptive security appliance using a web browser.
Chapter 35, “Configuring AnyConnect VPN Client Connections”	Describes how to install and configure the SSL VPN Client.
Chapter 36, “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.
<b>Part 4: System Administration</b>	
Chapter 37, “Managing System Access”	Describes how to access the adaptive security appliance for system management through Telnet, SSH, and HTTPS.
Chapter 38, “Managing Software, Licenses, and Configurations”	Describes how to enter license keys and download software and configurations files.
Chapter 39, “Monitoring the Adaptive Security Appliance”	Describes how to monitor the adaptive security appliance.
Chapter 40, “Troubleshooting the Security Appliance”	Describes how to troubleshoot the adaptive security appliance.
<b>Part 4: Reference</b>	
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 adaptive security appliance.
Appendix C, “Using the Command-Line Interface”	Describes how to use the CLI to configure the the adaptive 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.
Appendix F, “Configuring the Security Appliance for Use with MARS”	Describes how to configure the adaptive security appliance and add it to MARS as a reporting device.

**Table 1** Document Organization (continued)

Chapter/Appendix	Definition
“Glossary”	Provides a handy reference for commonly-used terms and acronyms.
“Index”	Provides an index for the guide.

## 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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

