



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:

- [Audience, page 1](#)
- [Objectives, page 1](#)
- [Organization, page 1](#)
- [Document Conventions, page 4](#)
- [Related Documentation, page 4](#)
- [Obtaining Documentation and Submitting a Service Request, page 4](#)

Audience

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

- Managing network security
- Installing and configuring firewalls
- Managing default and static routes, and TCP and UDP services

Objectives

This document contains instructions and procedures for configuring the Firewall Services Module (FWSM) 4.0, a single-width services module supported on the Catalyst 6500 switch and the Cisco 7600 router, using ASDM. FWSM protects your network from unauthorized use. This guide does not cover every feature, but describes only the most common configuration scenarios.

Organization

This document contains the following chapters:

Chapter	Title	Description
1	Introduction to the Firewall Services Module	Provides a high-level overview of the FWSM.
2	Welcome to ASDM	Provides a high-level overview of ASDM and how it interacts with FWSM.
3	Defining Preferences and Using Configuration, Diagnostic, and File Management Tools	Describes the preferences and tools available for configuration, problem diagnosis, and file management for ASDM.
4	Configuring the Switch for Use with the FWSM	Describes how to configure the switch for use with the FWSM.
5	Before You Start	Describes how to get started in ASDM with the FWSM.
6	Using the Startup Wizard	Guides you through the initial configuration of the FWSM, and helps you define settings for the FWSM.
7	Configuring Device Settings and Management	Describes how to configure device settings for the FWSM.
8	Configuring Interfaces	Describes how to configure the interface name, security level, and IP address. It also describes how to configure bridge groups for transparent firewall mode interfaces.
9	Configuring Security Contexts	Describes how to configure security context within the FWSM. Each security context has its own security policy, interfaces, and administrators to configure.
10	Configuring Dynamic And Static Routing	Describes how to configure dynamic and static IP routing.
11	Configuring Multicast Routing	Describes how to enable and configure multicast routing on the FWSM.
12	Configuring DHCP and DNS Services	Describes how to configure DHCP servers or DHCP relay services to DHCP clients attached to FWSM interfaces.
13	Configuring Failover	Describes the failover feature, which lets you configure two FWSMs so that one will take over operation if the other one fails.
14	Configuring AAA Servers and the Local Database	Describes how to configure AAA servers and the local database.
15	Configuring Management Access	Describes how to access the FWSM for system management through Telnet, SSH, HTTPS, and VPN.
16	Configuring Logging	Describes how to enable and configure logging to specify how log information is handled.

Chapter	Title	Description
17	Certificates	Describes certificates that provide digital identification for authentication which allows for multiple identities, roots and certificate hierarchies in the FWSM.
18	Firewall Mode Overview	Describes how to set the firewall mode in the FWSM as well as how the firewall works in each firewall mode.
19	Adding Global Objects	Describes how to add, modify and define security objects from the Objects pane in FWSM. This provides a single location where you can configure, view, and modify the reusable components that you need to implement your policies on the FWSM.
20	Configuring Access Rules and EtherType Rules	Describes how to configure access rules and EtherType rules.
21	Configuring NAT	Describes how address translation is performed.
22	Configuring Service Policy Rules	Describes how to enable service policy rules that provides you with a consistent and flexible way to configure FWSM features.
23	Configuring Application Layer Protocol Inspection	Describes how to use and configure application inspection.
24	Applying AAA for Network Access	Describes how to enable AAA for network access.
25	Configuring Filter Rules	Describes ways to filter web traffic as it passes through the FWSM to reduce security risks or prevent inappropriate use.
26	Configuring Advanced Firewall Protection	Describes how to prevent network attacks by configuring advanced firewall protection features such as connection settings, and TCP state bypass.
27	Configuring ARP Inspection and Bridging Parameters	Describes how to enable ARP inspection and how to customize bridging operations.
28	Monitoring Logging	Describes how to monitor logging features.
29	Monitoring Failover	Describes failover monitoring in ASDM for the FWSM.
30	Monitoring Interfaces	Describes how to monitor interface statistics as well as interface-related features.
31	Monitoring Routing	Describes how to monitor OSPF LSAs, OSPF and EIGRP neighbors, and the routing table.
32	Monitoring Properties	Describes how to monitor properties in the FWSM, such as AAA servers, DNS cache, and system resources.
A	Specifications	Describes the FWSM specifications.
	Index	Provides an index for this guide.

Document Conventions

The FWSM command syntax descriptions use the following 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.
- Examples might include output from different platforms; for example, you might not recognize an interface type in an example because it is not available on your platform. Differences should be minor.



Note

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

Related Documentation

For more information, see the following documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Installation Note*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Release Notes*

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.