



## 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 2](#)
- [Document Conventions, page 3](#)
- [Related Documentation, page 4](#)
- [Obtaining Documentation, page 4](#)
- [Documentation Feedback, page 5](#)
- [Cisco Product Security Overview, page 5](#)
- [Product Alerts and Field Notices, page 6](#)
- [Obtaining Technical Assistance, page 7](#)
- [Obtaining Additional Publications and Information, page 8](#)

## 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) 3.2, a single-width services module supported on the Catalyst 6500 switch and the Cisco 7600 router, using the command-line interface. FWSM protects your network from unauthorized use. This guide does not cover every feature, but describes only the most common configuration scenarios.

You can also configure and monitor the FWSM 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/univercd/cc/td/doc/product/netsec/secgmt/asdm/index.htm>.

## Organization

This document contains the following chapters:

Chapter	Title	Description
1	<a href="#">Introduction to the Firewall Services Module</a>	Provides a high-level overview of the FWSM.
2	<a href="#">Configuring the Switch for the Firewall Services Module</a>	Describes how to configure the switch for use with the FWSM.
3	<a href="#">Connecting to the Firewall Services Module and Managing the Configuration</a>	Describes how to access the command-line interface and work with the configuration.
4	<a href="#">Configuring Security Contexts</a>	Describes how to use security contexts and enable multiple context mode.
5	<a href="#">Configuring the Firewall Mode</a>	Describes in detail the two operation modes of the FWSM, routed and transparent mode, and how data is handled differently with each mode.
6	<a href="#">Configuring Interface Parameters</a>	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.
7	<a href="#">Configuring Basic Settings</a>	Describes how to configure basic settings that are typically required for a functioning configuration.
8	<a href="#">Configuring IP Routing and DHCP Services</a>	Describes how to configure IP routing and DHCP.
9	<a href="#">Configuring IPv6</a>	Describes how to enable and configure IPv6.
10	<a href="#">Identifying Traffic with Access Lists</a>	Describes how to identify traffic with access lists.
11	<a href="#">Permitting or Denying Network Access</a>	Describes how to control network access through the FWSM using access lists.
12	<a href="#">Configuring NAT</a>	Describes how address translation is performed.
13	<a href="#">Configuring Failover</a>	Describes the failover feature, which lets you configure two FWSMs so that one will take over operation if the other one fails.
14	<a href="#">Configuring AAA Servers and the Local Database</a>	Describes how to configure AAA servers and the local database.
15	<a href="#">Applying AAA for Network Access</a>	Describes how to enable AAA for network access.
16	<a href="#">Applying Filtering Services</a>	Describes ways to filter web traffic to reduce security risks or prevent inappropriate use.

Chapter	Title	Description
17	<a href="#">Configuring ARP Inspection and Bridging Parameters</a>	Describes how to enable ARP inspection and how to customize bridging operations.
18	<a href="#">Using Modular Policy Framework</a>	Describes how to use the Modular Policy Framework to create security policies for TCP, general connection settings, and inspection.
19	<a href="#">Configuring Advanced Connection Features</a>	Describes how to configure connection features.
20	<a href="#">Applying Application Layer Protocol Inspection</a>	Describes how to use and configure application inspection.
21	<a href="#">Configuring Management Access</a>	Describes how to access the FWSM for system management through Telnet, SSH, HTTPS, and VPN.
22	<a href="#">Managing Software, Licenses, and Configurations</a>	Describes how to enter license keys and download software and configurations files.
23	<a href="#">Monitoring the Firewall Services Module</a>	Describes how to monitor the FWSM.
24	<a href="#">Troubleshooting the Firewall Services Module</a>	Describes how to troubleshoot the FWSM.
A	<a href="#">Specifications</a>	Describes the FWSM specifications.
B	<a href="#">Sample Configurations</a>	Describes a number of common ways to implement the FWSM.
C	<a href="#">Using the Command-Line Interface</a>	Describes how to use the CLI to configure the FWSM.
D	<a href="#">Mapping MIBs to CLI Commands</a>	Lists MIB objects and the equivalent CLI commands.
E	<a href="#">Addresses, Protocols, and Ports</a>	Provides a quick reference for IP addresses, protocols, and applications.
	<a href="#">Glossary</a>	Provides a glossary for terms used in this guide.
	<a href="#">Index</a>	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.

---

For information on modes, prompts, and syntax, see [Appendix C “Using the Command-Line Interface.”](#)

## 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

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

### Cisco.com

You can access the most current Cisco documentation at this URL:

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

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](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — [security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — [psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



### Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

---

## Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Support Website

The Cisco 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 at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco 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

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.



### Tip

#### Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

## 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 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 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)**—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:  
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- 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>
- *Internet Protocol Journal* is a quarterly journal published by Cisco 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>
- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>
- 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>

