# Cisco PDM Release Notes for Firewall Services Module Version 4.0

**June 2004**

## Contents

This document includes the following sections:



## Introduction

Cisco PDM Version 4.0 for FWSM Release 2.2 is a web-based application used to configure and monitor the Firewall Services Module (FWSM) on a Catalyst 6500 switch or Cisco 7600 router. PDM Version 4.0 requires FWSM Release 2.2(1) and supports all of the configuration features in this release. For more information see FWSM Technical Documentation and the FWSM FAQ (Frequently Asked Questions) sections on Cisco.com.

**Note** PDM Version 4.0 is a single image that supports only FWSM Release 2.2. It does not support FWSM Release 1.1 or the PIX OS.


**Corporate Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# PDM Software Overview

PDM Version 4.0 supports FWSM Release 2.2 on a Catalyst 6500 switch or Cisco 7600 router.

PDM Version 4.0 is a single image, which supports only FWSM Release 2.2, and is designed to provide secure administration of the firewall. PDM is implemented as a signed Java applet, which downloads to your PC or workstation when you point your browser at the firewall without requiring a plug-in or other software to be installed beforehand. PDM manages FWSM Release 2.2 when it runs in single or multiple context modes.

PDM provides a graphical user interface to the firewall to administer it without requiring knowledge of the command-line interface (CLI). Additionally, PDM maintains compatibility with the firewall CLI and includes a tool for using the standard CLI commands within the PDM application. PDM lets you graph many aspects of the firewall, as well as print or export graphs of traffic through the firewall and system activity.

To help you use PDM, online Help is provided throughout the application as well as a Help table of contents, index, and glossary.

# Switch/Router System Requirements

The switch and router models that support the FWSM are:

- Catalyst 6500 series switches, with the following required components:
  - Supervisor engine with Cisco IOS software (known as supervisor IOS) or Catalyst operating system (OS).
  - Multilayer Switch Feature Card (MSFC 2) with Cisco IOS software.
- Cisco 7600 series routers, with the following required components:
  - Supervisor engine with Cisco IOS software.
  - MSFC 2 with Cisco IOS software.

For more information, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide Version 2.2* for supported supervisor engine and software versions and the supported Cisco IOS software.

**Note** The FWSM does not support a direct connection to a switch WAN port, because WAN ports do not use static virtual local area networks (VLANs). However, the WAN port can connect to the MSFC, which can also connect to the FWSM.

For more information on switch or router requirements for FWSM, go to the following website: http://www.cisco.com/en/US/partner/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

The following sections list the system requirements for PDM Version 4.0 software.

# FWSM Requirements

The FWSM must run software Release 2.2 and meet all browser requirements below to run PDM Version 4.0.

A firewall must meet the following requirements to successfully install and run PDM:

- **Minimum Software Versions—**Verify that your firewall meets the requirements listed in the *Release Notes for the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Software Release*. You must have Version 2.2 installed on FWSM before using PDM Version 4.0. For more information, refer to the *Cisco PDM Installation and Configuration Guide for Firewall Services Module.*
- **Upgrading Software —**When you install a new version of PDM, close all browser sessions before launching PDM. For information on upgrading your FWSM, see the following websites:

  http://www.cisco.com/cisco/pub/software/portal/select.html

  http://www.cisco.com/en/US/partner/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

**Caution** If you are using PIXMC, use PDM for monitoring only. All changes made using PDM will be overwritten the next time PIXMC synchronizes with the firewall.

# Browser Requirements

The following are required to access one or more firewalls through PDM:

- **Java Virtual Machine (JVM)** For best performance when running Windows, use Internet Explorer 6.0 with or without the Java Plug- in. If Java is not enabled in the browser, PDM guides you on how to enable it. To check which version you have, launch PDM. When the PDM information window appears, note the Java version number. When using the Java Plug-in, there is a significant improvement in PDM load time if you access the firewall using the hostname (not IP address). See "Configuration Recommendations".
- **HTTP 1.1** Settings for Internet Options>Advanced>HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections. Note, this applies only to Internet Explorer.
- **SSL Encryption Settings** All available encryption options are enabled for SSL in the browser preferences.

# Maximum Configuration File Size

For optimum performance, we recommend a configuration file of no more than 500 KB when using PDM.

FWSM Firewall configuration files over 500 KB may interfere with the performance of PDM on your workstation in the following situations:

- While executing commands such as **write term** and **show run**
- Failover (the configuration synchronization time)
- During a PDM Refresh Operation or loading PDM for the first time

# PC/Workstation Requirements

PDM has different requirements depending on the platform from which it is accessed. PDM is not supported for use on computers equipped with the Macintosh OS, or other versions of the Windows operating systems.

## Configuration Recommendations

We recommend the following browser and JVM combinations for these operating systems:

***Table 1 Recommended Browser and JVM combinations***

| Operating System | Browser | JVM |
|---|---|---|
| Microsoft Windows 2000 (Service Pack 3), or Microsoft Windows XP | Internet Explorer 6.0 | Native (built-in) JVM (VM 3809 or higher) |
| Microsoft Windows 2000 (Service Pack 3), or Microsoft Windows XP | Internet Explorer 6.0 | Java Plug-in 1.4.1 or 1.4.2 |
| Microsoft Windows 2000 (Service Pack 3), or Microsoft Windows XP | Netscape 7.1 | Java Plug-in 1.4.1 or 1.4.2 |
| Sun SPARC Solaris 2.8 or 2.9 | Netscape 7.0 | Java Plug-in 1.4.1 or 1.4.2 |
| Red Hat Linux 9.0 or Red Hat Enterprise Linux WS, Version 3 running GNOME or KDE | Netscape 7.1 | Java Plug-in 1.4.1 or 1.4.2 |

## Supported Platforms

Table 2 lists the supported and recommended platforms for PDM Version 4.0.

**Note** The Japanese version of Windows (JOS) is supported in the PDM Version 4.0 release.

*Table 2 Supported and Recommended Platforms for PDM Version 4.0*

| | Operating System | Browser | Hardware |
|---|---|---|---|
| Windows | Windows 2000 (Service Pack 3) or Windows XP operating systems.<br>PDM is not supported on Windows 3.1, 95, 98, ME or Windows NT 4. | Internet Explorer 6.0 with native JVM (VM 3809 or higher)<br>Internet Explorer 6.0 with Java Plug-in 1.4.1 or 1.4.2<br>Netscape 7.1 with Java Plug-in 1.4.1 or 1.4.2 | Any Pentium III or Pentium-compatible processor running at 450 MHz or higher.<br>At least 256 MB of random-access memory (RAM). We recommend 192 MB or more.<br>A 1024 x 768 pixel display and at least High Color (16-bit) |
| SUN Solaris | Sun Solaris 2.8, 2.9, or later running CDE window manager. | Netscape 7.0 with Java Plug-in 1.4.1 or 1.4.2 | SPARC microprocessor.<br>At least 256 MB of random-access memory (RAM).<br>A 1024 x 768 pixel display and at least 256 colors. High Color (16-bit) recommended.<br>At least 256 MB of random-access memory (RAM).<br>A 1024 x 768 pixel display and at least 256 colors. High Color (16-bit) recommended. |
| Linux | Red Hat Linux 9.0 or Red Hat Enterprise Linux WS, Version 3 running GNOME or KDE | Supported browser: Netscape 7.1 with Java Plug-in 1.4.1 or 1.4.2 | At least 128 MB of random-access memory (RAM). 256 MB recommended.<br>A 1024 x 768 pixel display with at least 256 colors. High Color (16-bit) recommended. |

**Note**

- PDM and Linux:
  - When using Netscape on Linux and running the XFree86 Mach64 server, Netscape might hang when running PDM, particularly if you resize the PDM window. A workaround is to change the monitor display to 256 colors.
  - When using Netscape on some Linux platforms, if you select an item under the Properties tab or the Monitoring tab, the entire PDM window shifts a few pixels to the left and up. This movement happens when you select a panel with a text box or a combo box in it.

# New and Changed Information

## Security Contexts

The FWSM supports multiple instances of virtual firewalls, called security contexts. PDM users log on to a context, which appears as a single firewall. PDM admin users log on to the admin context and then change into the System execution space to create contexts and perform global system tasks.

## Resource Management

By default, each security contexts has unlimited access to the resources of the FWSM. Using resource management, you can limit the use of firewall resources per context, including concurrent connections, connections per second, syslogs per second, max number of Telnet/SSH sessions per context, and other settings.

## Transparent Firewall

The firewall service is transparently enabled on the ingress and egress of router VLAN-based Layer 2 interfaces. The FWSM acts like a bump in the wire, and is not a router hop. The FWSM connects the same network on its inside and outside ports, but each port must be on a different VLAN. The initial limit is two interfaces per transparent firewall context.

## Policy NAT

The policy NAT feature provides the ability to translate a host to multiple identities based on access rules. This allows the same local IP address to be translated to different global addresses based on the destination network and translation rules.

## Outbound Destination Interface ACL (Access Control List)

PDM uses the Access Rules panel to generate CLI ACLs that are normally applied to inbound (source interface) traffic. This extension allows ACLs to also be applied to outbound (destination interface) traffic.

## Same Security Level

This extension allows multiple interfaces to have the same security level to better manage large numbers of virtual firewalls and VLAN interfaces.

## Increased VLAN Support

The FWSM supports a maximum of 256 interfaces per context or in single context mode. In multiple context mode, the FWSM has an overall limit of 1000 VLAN interfaces across all contexts. You can share interfaces between contexts if your network requires it.

## ACL Commit

This feature sets the FWSM CLI to a blocked condition until recompilation of ACLs is complete, to assure accurate reporting back to the PDM application.

## Monitoring

New DHCP monitoring functions are present.

## Stateful ICMP Inspection & NAT for ICMP Error Messages

ICMP and NAT enhancements are present for the virtual firewall.

## SNMP

Ability to change UDP port on which traps are sent to the server, ability to specify traps to be sent by feature, and Cisco firewall MIB support.

## Failover

Active/Standby system failover mode on a per-blade basis exists.You can configure the FWSM to monitor essential interfaces.

## Connections

Control of maximum connections for interfaces is present.

## VLAN

802.1Q VLAN support provides added flexibility in managing and provisioning the firewall. This feature enables the decoupling of IP interfaces from physical interfaces and supplies appropriate handling for IEEE 802.1Q tags.

## OSPF (Single Firewall Mode Only)

Route propagation and greatly reduced route convergence times are two of the many benefits of OSPF. Intra-area, inter-area, and external routes are supported. The distribution of static routes to OSPF processes and route redistribution between OSPF processes are also included.

## DHCP Relay (Routed Firewall Only)

Acting as a DHCP relay agent, the firewall can assist in dynamic configuration of IP hosts on any of its interfaces. It receives requests from hosts on a given interface and forwards them to a user-configured DHCP server on another interface.

## Comments in ACLs

This feature lets you include comments in access lists to make the ACL easier to understand and scan.

## Syslog by ACL

This feature lets you configure a specific ACL entry with a logging option. When such an option is configured, statistics for each flow that match the permit or deny conditions of the ACL entry are logged.

## Specify Interface as Address in ACLs

If you are running the DHCP client on the firewall outside interface you will no longer have to adjust access lists every time the outside DHCP address gets changed by the ISP.

## Java Plug-in 1.4

PDM Version 4.0 adds support for Java plug-in versions 1.4.1 and 1.4.2. You can download Java plug-ins from http://java.sun.com.

## New Fixup Features

MGCP, ICMP Error, Sun RPC and NIS+, and Disable SIP UDP. If SIP UDP fixup is disabled, the firewall does not inspect any packets transmitted over SIP UDP port 5060, or translate the IP addresses or ports embedded in the payload of the packets. Disabling SIP UDP fixup also prevents valid non-SIP packets from being dropped by the firewall if they originate from or are destined to the SIP UDP port 5060.

## Change Level for Syslog Messages

This feature lets you change the default logging level for a specific ACL entry with a logging option. When such an option is configured, statistics for each flow that matches the permit or deny conditions of the ACL entry are logged.

## AAA Proxy Limit

You can limit the number of concurrent proxy connections allowed.

## HTTPS/FTP Using Websense

This feature extends the existing Websense-based URL filtering to HTTPS and FTP.

## DHCP Server on Any Interface

You can configure any interface as a DHCP server.

## Management Feature Access

You can perform FWSM management functions, such as running PDM on an internal interface with a fixed IP address over an IPSec VPN tunnel.

## Banner

The Banner panel lets you configure a message of the day, login, and session banners.

## Improved Printing

Printing has been improved so that access lists can be printed and viewed more easily.

## RME Syslog Compatibility

This feature provides the ability to log messages in Cisco EMBLEM format to a syslog server. This feature allows the RME (Resource Manager Essentials) syslog analyzer to parse FWSM messages sent to a syslog host.

## PDM Home Page

The PDM home page lets you view, at a glance, important information about your firewall such as the status of your interfaces, the version you are running, licensing information, and performance.

## Batch Mode When Sending CLIs

PDM is faster in the method it uses to send a series of CLI commands to the firewall. It allows all CLIs to be sent and configured, even if you end up losing the connection because of the changes you make.

## AAA Fallback

By default, a AAA server failure would prevent you from authenticating and/or authorizing. This feature lets you optionally choose to use the LOCAL database on the FWSM for authentication and/or authorization in the event of a AAA server failure.

## Certificates

You can configure a certificate server in the Certificates panel. You must still execute commands on the CLI to get the certificate.

# PDM Enhancements

## New Look-and-Feel

PDM Version 4.0 has a new look-and-feel including a home page, status bar, and flat buttons. The home page displays the device information, interface status, system resources, and traffic status.

## Sharing of Access Control Lists

PDM now supports sharing of ACLs. This means if an access list is used in more than one place, such as one that is used by more than interface, PDM will support this configuration. Previously, it would limit you to the Monitoring tab.

When you attempt to change an access list that is being shared in the Access Rules table or other features that use access lists, it will prompt you to make a copy of the access list so that a change will not affect other parts of your configuration.

## Rule Flow Diagram

In the Access Rules tab, Access Rules, Add/Edit Rule dialog, there is a new Rule Flow Diagram that indicates how the rule is applied. This appears in the Add/Edit Rule dialog for AAA Rules and Filter Rules as well.

## Save All Running Configurations to Flash

As an administrator, you can click File > **Save All Running Configurations to Flash**. This saves the running configuration of each context to flash memory.

## Startup Wizard

This adds a Startup Wizard that covers the basic configuration. It can be used to set up a new context and to allow direct access to this context using PDM. Click Wizard > **Startup Wizard** to run this wizard. In addition, you can configure HTTPS, SSH, and Telnet access to the FWSM. In transparent firewall mode, you can configure the management IP.

## Command-Line Interface Enhancements

This feature can be accessed by clicking Tools > **Command Line Interface**. It remembers the last issued CLIs. You can access common **show** commands from the drop-down list.

## Improved Startup Time

PDM Version 4.0 loads faster because it caches the PDM applet. The first time you run PDM, it will cache the PDM image on your local hard drive. The next time you run PDM, it checks to see if the version matches. If so, it runs PDM from your cache as opposed to downloading the PDM image again. Otherwise, it downloads PDM from the FWSM. The cache is independent of the browser cache and the plug-in cache, so clearing these caches will not affect PDM. You can clear the PDM cache in PDM by

clicking File > **Clear PDM Cache**. Clearing the PDM cache will only clear the cache for that browser and JVM. For example, when using both Internet Explorer and Netscape 7.1, if you clear the cache in Internet Explorer, it will not clear the cache used by Netscape 7.1.

### Improved Performance and Scalability

PDM Version 4.0 applies changes much quicker than the previous release because it no longer rereads the configuration after every change. If another session made a change to the configuration, click the Refresh button to retrieve the latest configuration in your PDM session.

In addition, PDM supports up to a 500 KB configuration. This is simply a recommended limit and is not enforced in the software. Exceeding 500 KB may cause noticeable performance degradation in PDM.

### Support for New Platforms

Support for Red Hat Enterprise Linux WS, version 3 and Red Hat Linux 9 was added. Support for Windows, Japanese OS (JOS) was added. PDM will still display in English but will run on JOS.

# Important Notes

This section describes important notes for PDM software Version 4.0.

## Fixups

Both fixup SIP over TCP and fixup SIP over UDP are supported in FWSM Release 1.1, but fixup SIP over UDP cannot be disabled in FWSM Release 1.1 or PDM Version 2.1. Fixup SIP over UDP can only be disabled in FWSM Release 2.2, PDM Version 4.0.

## CLI Command Support

PDM Version 4.0 adds support to the firewall CLI command syntax. Refer to PDM online Help for more information on the supported CLI commands.

### Fully Supported CLI Commands

PDM parses these commands when uploading or creating the FWSM configuration and grants you full access to all PDM user-interface tabs.

Exceptions are noted in the table and occur when PDM cannot parse certain combinations of command statements. Commands that PDM cannot parse stay in the configuration, their values cannot be changed with PDM, and they appear in the list of unparseable commands.

Table 3 lists the CLI commands that PDM fully supports. PDM parses these commands in the FWSM configuration and allows PDM to operate successfully.

*Table 3 CLI Commands That PDM Parses and Fully Supports in Configuration*

| FWSM Commands |
|---|
| **aaa** command, **include** option |
| **aaa** command, **match acl_name** option |
| **aaa-server** |
| **access-list** and **access-group** |
| **access-list** compiled |
| **access-list ethertype** |
| **arp** |
| **arp inspection** |
| **auth-prompt** |
| **class** (in System mode) |
| **context** (in System mode) |
| **dhcpd** |
| **domain-name** |
| **enable password** |
| **failover** |
| **failover lan** and **show failover lan detail** |
| **failover monitor-interface** |
| **failover polltime** |
| **failover polltime holdtime** |
| **filter** |
| **fixup protocol** |
| **fragment** |
| **global** |
| **hostname** |
| **http** |
| **icmp** |
| **igmp** |
| **interface** |
| **ip address** |
| **ip audit** |
| **ip local pool** |
| **ip verify reverse-path** |
| **isakmp identity** [address \| hostname] |
| **logging** |

*Table 3 CLI Commands That PDM Parses and Fully Supports in Configuration (Continued)*

| FWSM Commands |
|---|
| **mroute** |
| **multicast** |
| **name** |
| **nameif** |
| **nat** |
| **nat** [(*if_name*)] **0 access-list** *acl_name* |
| **ntp** |
| **object-group** (network, service) |
| **passwd** |
| **pdm** |
| **pdm** group |
| **pdm** history |
| **pdm** location |
| **pdm** logging |
| **privilege** |
| **remote-management** |
| **rip** |
| **route** |
| **router** |
| **rpc-server** |
| **same-security-traffic** |
| **service resetinbound** |
| **snmp-server** |
| **ssh** |
| **static** (used for inbound PAT) |
| **sysopt** |
| **telnet** |
| **tftp-server** |
| **timeout** |
| **url-block** |
| **url-cache** |
| **url-server** |
| **user-name** |

## CLI Commands not Fully Supported in FWSM

Table 4 lists commands that cannot be changed. PDM parses these commands in the firewall configuration and handles them transparently.

*Table 4 CLI Commands not Fully Supported That Cannot be Changed with PDM*

| FWSM Commands |
|---|
| **floodguard** |
| **mtu** |
| **name-server** |
| **object-group (protocol, icmp-type)** |
| **object-group (network) nested not supported** |
| **pager** |
| **sysopt ipsec pl-compatible** |
| **sysopt nodnsalias inbound** |
| **sysopt nodnsalias outbound** |
| **sysopt route dnat** |
| **sysopt security fraggaurd** |
| **sysopt uauth allow-http-cache** |
| **terminal** |
| **virtual** |
| **ca** |

## CLI Commands Ignored By PDM in FWSM

These CLI commands are displayed in the list of unparseable commands in PDM. However, PDM does not change or remove these commands from your configuration, and the presence of these commands does not limit your access to the user-interface tabs in PDM.

The following commands are otherwise ignored by PDM except that they are displayed in the list of unparseable commands:

- Access lists not applied to any interface and not applied to the **aaa** command statement—A group of **access-list** command statements without an accompanying **access-group** command statement or **aaa match** *acl* command statement.

  For example:

  ```
  access-list eng permit ip any server1 255.255.255.255
  access-list eng permit ip any server2 255.255.255.255
  access-list eng permit ip any server3 255.255.255.255
  access-list eng deny ip any any
  ```

- Permit return connections on ports other than those used for the originating connection based on an **established** connection.
- For a **prefix-list** not bound to an OSPF area—Must be linked to an OSPF area using **area filter-list prefix** command.

**Note** The following commands are not supported or changed by PDM: **sysopt ipsec pl-compatible**, **sysopt nodnsalias inbound**, and **sysopt nodnsalias outbound**.

PDM does not support discontinuous netmasks.

## Unsupported Command Combinations

The following command combinations allow only monitoring and not configuration facilities:

- **aaa** command with the **match** option appearing in the configuration with other **aaa** commands that contain the **include** or **exclude** options. For example, the following commands would not be parsed by PDM.

```
access-list 101 permit tcp any any
aaa authentication include http inside 1.1.1.1 255.255.255.255 0.0.0.0 0.0.0.0 portal
aaa accounting match 101 inside portal
```

  You can fix this by changing **aaa** commands exclusively to either the **match acl** style or to the **include/exclude** style.

- **User Lacks Privilege.** User lacks privilege to run the following basic commands:

  **write**

  **show pdm**

  **show version**

  **show curpriv**

## Multiple PDM Sessions

PDM allows multiple PCs or workstations to each have one browser session open with the same firewall. A single firewall unit can support up to concurrent 5 PDM sessions. However, only one session per browser per PC or workstation is supported for a particular firewall. Refer to PDM online Help for more information on multiple PDM sessions.

# Caveats

The following sections describe the caveats for PDM software Version 4.0.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Cisco Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note** Please use Bug Navigator II on CCO to view additional caveat information. Bug Navigator II may be accessed at the following website:

https://tools.cisco.com/Support/BugToolKit/action.do

# Open Caveats - Version 4.0

The caveats in Table 5 are yet to be resolved in this version.

***Table 5 Open Caveats***

| | Software Version | |
|---|---|---|
| | 4.0 | |
| ID Number | Corrected | Caveat Title |
| CSCdx44905 | No | No match access list uses subnet wider than IP local pool |
| CSCeb02365 | No | No pdm not parse ACL IP any when no pdm loc, no nat, no apply outside |
| CSCeb05272 | No | No discontinuous netmask causes PDM t be stuck in a loop |
| CSCec58183 | No | Monitoring/config has incorrect help page |
| CSCed71185 | No | Cannot dismiss a dialog that appears over a status dialog |
| CSCee70606 | No | cmd auth+plugin: sending more than 120 pdm location cmds hangs PDM |
| CSCee77936 | No | PDM should check for duplicate IPs |
| CSCee79057 | No | ICMP type object grouping is not supported through PDM |
| CSCee81372 | No | Error popup for a non-IP protocol configured for static policy NAT |
| CSCee81774 | No | Transparent firewall, standby IP cannot be removed |
| CSCee82823 | No | Management IP seems to carry over to other contexts |

# Resolved Caveats - Version 4.0

The caveats in Table 6 are resolved in this version.

***Table 6 Resolved Caveats***

| | Software Version | |
|---|---|---|
| | 4.0 | |
| ID Number | Corrected | Caveat Title |
| CSCea64537 | Yes | AAA-if aaa is cleared, but not acls, the new rule uses the same acl name |
| CSCea93702 | Yes | Remove and recreate two same ospf proc (one empty) only one recreated |
| CSCdy64411 | Yes | The interface table cannot be sorted according to the columns |
| CSCed50799 | Yes | ACL containing udp/www is not recognized by PDM |

# 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.

This document is to be used in conjunction with the appropriate documentation for your Cisco FWSM system.



*Cisco PDM Release Notes for Firewall Services Module Version 4.0*