



Specifications

This appendix lists the specifications of the FWSM and includes the following sections:

- [Switch Hardware and Software Compatibility, page A-1](#)
- [Licensed Features, page A-2](#)
- [Physical Attributes, page A-2](#)
- [Feature Limits, page A-3](#)
- [Managed System Resources, page A-4](#)
- [Fixed System Resources, page A-5](#)
- [Rule Limits, page A-5](#)

Switch Hardware and Software Compatibility

The switch models that support the FWSM include the following platforms:

- Catalyst 6500 series switches, with the following required components:
 - Supervisor engine with Cisco IOS software (known as supervisor IOS) *or* Catalyst operating system (OS). See [Table A-1](#) for supported supervisor engine and software releases.
 - MSFC 2 with Cisco IOS software. See [Table A-1](#) for supported Cisco IOS releases.
- Cisco 7600 series routers, with the following required components:
 - Supervisor engine with Cisco IOS software. See [Table A-1](#) for supported supervisor engine and software releases.
 - MSFC 2 with Cisco IOS software. See [Table A-1](#) for supported Cisco IOS releases.



Note

The FWSM does not support a direct connection to a switch WAN port because WAN ports do not use static VLANs. However, the WAN port can connect to the MSFC, which can connect to the FWSM.

Table A-1 shows the supervisor engine version and software.

Table A-1 Support for FWSM 3.1

	Supervisor Engines ¹
Cisco IOS	
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	2, 720, 32
Cisco IOS Software Modularity	
12.2(18)SXF4	720, 32
Catalyst OS²	
8.5(3) and higher	2, 720, 32

1. The FWSM does not support the supervisor 1 or 1A.
2. When you use Catalyst OS on the supervisor, you can use any of the supported Cisco IOS releases above on the MSFC. (When you use Cisco IOS software on the supervisor, you use the same release on the MSFC.)

Licensed Features

The FWSM supports the following licensed features:

- Multiple security contexts. The FWSM supports two contexts plus one admin context for a total of three security contexts without a license. For more than three contexts, obtain one of the following licenses:
 - 20
 - 50
 - 100
 - 250
- GTP/GPRS support.

Physical Attributes

Table A-2 lists the physical attributes of the FWSM.

Table A-2 Physical Attributes

Specification	Description
Bandwidth	CEF256 line card with a 6-Gbps path to the Switch Fabric Module (if present) or the 32-Gbps shared bus.
Memory	<ul style="list-style-type: none"> • 1-GB RAM. • 128-MB Flash memory.
Modules per switch	<p>Maximum four modules per switch.</p> <p>If you are using failover, you can still only have four modules per switch even if two of them are in standby mode.</p>

Feature Limits

Table A-3 lists the feature limits for the FWSM.

Table A-3 Feature Limits

Specification	Context Mode	
	Single	Multiple
AAA servers (RADIUS and TACACS+)	16	4 per context
Failover interface monitoring	250	250 divided between all contexts
Filtering servers (Websense Enterprise and Sentian by N2H2)	16	4 per context
Fragmented packets	<ul style="list-style-type: none"> If the FWSM receives a fragment set that is originally 8782 Bytes or smaller, then it reassembles the set and transmits it back on the wire, but the fragment size may be different than what was received. If the FWSM receives a fragment set that is originally 8783 Bytes or larger, then: <ul style="list-style-type: none"> If the frame is the first packet in a connection (as in the case of ICMP) then the FWSM reassembles the first 8782 Bytes and pass those on, but the remaining fragments are dropped. If the frame is <i>not</i> the first packet in a connection, then the FWSM reassembles the first 8782 bytes and passes those on, and the remaining fragments are also passed on, but without the reassembly check. 	
Jumbo Ethernet packets	8500 Bytes	8500 Bytes
Security contexts	N/A	250 security contexts (depending on your software license).
Syslog servers	16	4 per context Maximum of 16 divided between all contexts
VLAN interfaces		
Routed Mode	256	100 per context The FWSM has an overall limit of 1000 VLAN interfaces divided between all contexts. You can share outside interfaces between contexts, and in some circumstances, you can share inside interfaces.
Transparent Mode	8 pairs	8 pairs per context

Managed System Resources

Table A-4 lists the managed system resources of the FWSM. You can manage these resources per context using the resource manager. See the “Configuring Resource Management” section on page 4-11.

Table A-4 Managed System Resources

Specification	Context Mode	
	Single	Multiple
MAC addresses (transparent firewall mode only)	64 K	64 K divided between all contexts
Hosts allowed to connect through the FWSM, concurrent	256 K	256 K divided between all contexts
Inspection engine connections, rate	10,000 per second	10,000 per second divided between all contexts
IPSec management connections, concurrent	5	5 per context Maximum of 10 divided between all contexts
ASDM management sessions, concurrent ¹	5	Up to 5 per context Maximum of 80 divided between all contexts
NAT translations (xlates), concurrent	256 K	256 K divided between all contexts
SSH management connections, concurrent ²	5	5 per context Maximum of 100 divided between all contexts
System messages, rate	30,000 per second for messages sent to the FWSM terminal or buffer 25,000 per second for messages sent to a syslog server	30,000 per second divided between all contexts for messages sent to the FWSM terminal or buffer 25,000 per second divided between all contexts for messages sent to a syslog server
TCP or UDP connections ^{3 4} between any two hosts, including connections between one host and multiple other hosts, concurrent and rate	999,900 ⁵ 100,000 per second	999,900 divided between all contexts ⁵ 100,000 per second divided between all contexts
Telnet management connections, concurrent ²	5	5 per context Maximum of 100 connections divided between all contexts.

- ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 80 ASDM sessions represents a limit of 160 HTTPS connections.
- The admin context can use up to 15 Telnet and SSH connections.
- Embryonic connections are included in the total number of connections. If you configure an embryonic connection limit, then embryonic connections above the limit are not counted.

4. The FWSM might take up to 500 ms to remove a connection that is marked for deletion. Because any traffic on the connection is dropped during this period, you cannot initiate a new connection to the same destination using the same source and destination ports until the connection is deleted. Although most TCP applications do not reuse the same ports in back-to-back connections, RSH might reuse the same ports. If you use RSH or any other application that reuses the same ports in back-to-back connections, the FWSM might drop packets.
5. Because PAT requires a separate translation for each connection, the effective limit of connections using PAT is the translation limit (256 K), not the higher connection limit. To use the connection limit, you need to use NAT, which allows multiple connections using the same translation session.

Fixed System Resources

Table A-5 lists the fixed system resources of the FWSM.

Table A-5 Fixed System Resources

Specification	Context Mode	
	Single	Multiple
AAA connections, rate	80 per second	80 per second divided between all contexts
Downloaded ACEs for network access authorization	5000	5000 divided between all contexts
ACL logging flows, concurrent	32 K	32 K divided between all contexts
Alias statements	512	512 divided between all contexts
ARP table entries, concurrent	64 K	64 K divided between all contexts
DNS inspections, rate	5000 per second	5000 per second divided between all contexts
Global statements	4 K	4 K divided between all contexts
Inspection statements	32	32 per context
NAT statements	2 K	2 K divided between all contexts
Packet reassembly, concurrent	30,000	30,000 fragments divided between all contexts
Route table entries, concurrent	32 K	32 K divided between all contexts
Shun statements	5 K	5 K divided between all contexts
Static NAT statements	2 K	2 K divided between all contexts
TFTP sessions, concurrent ¹	999,100	999,100 divided between all contexts
User authentication sessions, concurrent	50 K	50 K divided between all contexts
User authorization sessions, concurrent	150 K Maximum 15 sessions per user.	150 K divided between all contexts Maximum 15 sessions per user.

1. In FWSM Version 1.1, the number of TFTP sessions was limited to 1024 sessions.

Rule Limits

The FWSM supports a fixed number of rules for the entire system. Table A-6 lists the maximum number of each rule type.

Table A-6 Rule Limits

Specification	Context Mode	
	Single	Multiple (Maximum per Partition) with 12 pools
AAA Rules	6451	992
ACEs	72,806	11,200
Established Rules	460	70
Filter Rules	2764	425
ICMP, Telnet, SSH, and HTTP Rules	1843	283
Policy NAT ACEs	1843	283
Inspect Rules	4147	1417