



Specifications

This chapter lists the specifications of the Firewall Services Module (FWSM) and includes the following sections:

- [Physical Attributes, page A-1](#)
- [Feature Limits, page A-2](#)
- [Managed System Resources, page A-3](#)
- [Fixed System Resources, page A-4](#)
- [Rule Limits, page A-5](#)

Physical Attributes

[Table A-1](#) lists the physical attributes of the FWSM.

Table A-1 *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	Maximum four modules per switch. If you are using failover, you can still only have four modules per switch even if two of them are in standby mode.

Feature Limits

Table A-2 lists the feature limits for the FWSM.

Table A-2 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
Jumbo Ethernet packets	8500 Bytes	8500 Bytes
Security contexts	N/A	100 security contexts (depending on your software license).
Syslog servers	16	4 per context
VLAN interfaces		
Routed Mode	256	256 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	2	2 per context

Managed System Resources

Table A-3 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 5-10.

Table A-3 Managed System Resources

Specification	Context Mode	
	Single	Multiple
MAC addresses (transparent firewall mode only)	64,000	64,000 divided between all contexts
Hosts allowed to connect through the FWSM, concurrent	256,000	256,000 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
PDM management sessions, concurrent ¹	5	Up to 5 per context Maximum of 32 divided between all contexts
NAT translations, concurrent	256,000	256,000 divided between all contexts
SSH ² management connections, concurrent	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 ³ or UDP ⁴ connections ⁵ between any two hosts, including connections between one host and multiple other hosts, concurrent and rate ⁶	999,900 100,000 per second	999,900 divided between all contexts 100,000 per second divided between all contexts
Telnet management connections, concurrent	5	5 per context Maximum of 100 connections divided between all contexts.

1. PDM 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 32 PDM sessions represents a limit of 64 HTTPS connections.
2. Secure Shell
3. Transmission Control Protocol
4. User Datagram Protocol

5. 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.
6. Because Port Address Translation (PAT) requires a separate translation for each connection, the effective limit of connections using PAT is the translation limit (256,000), 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-4 lists the fixed system resources of the FWSM.

Table A-4 Fixed System Resources

Specification	Context Mode	
	Single	Multiple
AAA ¹ connections, rate	80 per second	80 per second divided between all contexts
ACL logging flows, concurrent	32,000	32,000 divided between all contexts
Alias statements	1000	1000 divided between all contexts
ARP ² table entries, concurrent	64,000	64,00 divided between all contexts
DNS inspections, rate	5000 per second	5000 per second divided between all contexts
Global statements	1051	1051 divided between all contexts
Inspection engine (fixup) statements	32	32 per context ³
NAT statements	2000	2000 divided between all contexts
Packet reassembly, concurrent	30,000	30,000 fragments divided between all contexts
Route table entries, concurrent	32,000	32,000 divided between all contexts
Shun statements	5000	5000 divided between all contexts
SIP connections, concurrent	5000	5000 divided between all contexts
Static NAT statements	2000	2000 divided between all contexts
TFTP sessions, concurrent ⁴	999,100	999,100 divided between all contexts
User authentication sessions, concurrent	50,000	50,000 divided between all contexts
User authorization sessions, concurrent	150,000 Maximum 15 sessions per user.	150,000 divided between all contexts Maximum 15 sessions per user.

1. authentication, authorization, and accounting
2. Address Resolution Protocol
3. This limit includes the following inspection engines that are enabled by default, making the total number of configurable inspection engines 27: TFTP, Sun RPC over UDP, NetBIOS NameServer, XDMCP, and CUSeeMe. The OraServ and RealAudio inspection engines, which are also enabled by default, do not affect this limit.
4. In FWSM Version 1.1, the number of TFTP sessions was limited to 1024 sessions.

Rule Limits

The FWSM supports approximately 80K rules for the entire system in single mode, and 142K rules for multiple mode.

In multiple context mode, each context supports at most 12,130 rules, but the actual number of rules supported in a context might be less, depending on how many contexts you have. A context belongs to one of 12 pools that offers a maximum of 12,130 rules. The FWSM assigns contexts to the pools in the order they are loaded at startup. For example, if you have 12 contexts, each context is assigned to its own pool, and can use 12,130 rules. If you add one more context, then context number 1 and the new context number 13 are both assigned to pool 1, and can use 12,130 rules divided between them; the other 11 contexts continue to use 12,130 rules each. If you delete contexts, the pool membership does not shift, so you might have some unequal distribution until you reboot, at which time the contexts are evenly distributed.


Note

Rules are used up on a first come, first served basis, so one context might use more rules than another context.

Table A-5 lists the maximum number of each rule type.

Table A-5 Rule Limits

Specification	Context Mode	
	Single	Multiple (Maximum per Pool)
AAA Rules	3942	606 ¹
ACEs ²	63,078	9704
Downloaded ACEs for network access authorization	3000	3000
Established Rules	788	121
Filter Rules	3942	606
ICMP ³ , Telnet, SSH, and HTTP ⁴ Rules	2365	363
Policy NAT ACEs	3942	606

1. For example, if you have 96 contexts evenly distributed among the 12 pools, so there are 8 contexts per pool, each context can use 75 filter rules, if evenly divided.
2. access control entries
3. Internet Control Message Protocol
4. HyperText Transfer Protocol

