



APPENDIX **A**

Specifications

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

- [ASDM Client PC Operating System and Browser Requirements, page A-1](#)
- [Switch Hardware and Software Compatibility, page A-2](#)
- [Licensed Features, page A-3](#)
- [Physical Attributes, page A-4](#)
- [Feature Limits, page A-4](#)
- [Managed System Resources, page A-5](#)
- [Fixed System Resources, page A-6](#)
- [Rule Limits, page A-7](#)

ASDM Client PC Operating System and Browser Requirements

[Table 1](#) lists the supported and recommended PC operating systems and browsers for ASDM Version 5.1.

Table 1 *Operating System and Browser Requirements*

Operating System	Version	Browser	Other Requirements
Microsoft Windows ¹	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4)	Internet Explorer 6.0 or 7.0 with Sun Java SE ² Plug-in 5.0 (1.5.0), or 6.0 Firefox 1.5 or 2.0 with Java SE Plug-in 5.0 (1.5.0), or 6.0	SSL Encryption Settings —All available encryption options are enabled for SSL in the browser preferences.
Note	Cisco supports both the English and Japanese versions of Windows.	Note	HTTP 1.1 —Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.

Table 1 Operating System and Browser Requirements (continued)

Operating System	Version	Browser	Other Requirements
Apple MacIntosh	Apple MacIntosh OS X	Firefox 1.5 or 2.0 or Safari 2.0 with Java SE Plug-in 5.0 (1.5.0), or 6.0	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or 2.0 with Java SE Plug-in 5.0 (1.5.0), or 6.0	

- ASDM is not supported on Windows 3.1, Windows 95, Windows 98, Windows ME, or Windows NT4.
- Obtain Sun Java from java.sun.com.

Switch Hardware and Software Compatibility

You can install the FWSM in the Catalyst 6500 series switches or the Cisco 7600 series routers. The configuration of both series is identical, and the series are referred to generically in this guide as the “switch.” The switch includes a switch (the supervisor engine) as well as a router (the MSFC 2).

The switch supports Cisco IOS software on both the switch supervisor engine and the integrated MSFC router.



Note

The Catalyst operating system software is not supported.

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.

The FWSM runs its own operating system.

This section includes the following topics:

- [Catalyst 6500 Series Requirements, page A-2](#)
- [Cisco 7600 Series Requirements, page A-3](#)

Catalyst 6500 Series Requirements

[Table A-2](#) shows the supervisor engine version and software.

Table A-2 Support for FWSM 4.0 on the Catalyst 6500

Cisco IOS Software Release	Supervisor Engines ¹	FWSM Features:		
		PISA Integration	Route Health Injection	Virtual Switching System
12.2(18)SXF and higher	720, 32	No	No	No
12.2(18)SXF2 and higher	2, 720, 32	No	No	No

Table A-2 Support for FWSM 4.0 on the Catalyst 6500 (continued)

	Supervisor Engines ¹	FWSM Features:		
		PISA Integration	Route Health Injection	Virtual Switching System
12.2(33)SXI	720-10GE	No	Yes	Yes
12.2(33)SXI	720	No	Yes	No
12.2(33)SXI	32	No	Yes	No
12.2(18)ZYA	32-PISA	Yes	No	No
Cisco IOS Software Modularity Release				
12.2(18)SXF4	720, 32	No	No	No

1. The FWSM does not support the supervisor 1 or 1A.

Cisco 7600 Series Requirements

Table A-3 shows the supervisor engine version and software.

Table A-3 Support for FWSM 4.0 on the Cisco 7600

	Supervisor Engines ¹	FWSM Features:		
		PISA Integration	Route Health Injection	Virtual Switching System
Cisco IOS Software Release				
12.2(33)SRA	720, 32	No	No	No
12.2(33)SRC	720-1GE	No	No	No
12.2(33)SRD	720-1GE	No	No	No

1. The FWSM does not support the supervisor 1 or 1A.

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.
- BGP stub support.

Physical Attributes

Table 1-4 lists the physical attributes of the FWSM.

Table 1-4 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 1-5 lists the feature limits for the FWSM.

Table 1-5 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	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 1-6 lists the managed system resources of the FWSM. You can manage these resources per context using the resource manager. See the “Configuring Resource Classes” section on page 9-17.

Table 1-6 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 log 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 1-7 lists the fixed system resources of the FWSM.

Table 1-7 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	3,500	3,500 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	5,000 per second	5,000 per second divided between all contexts
Global statements	4,204	4,204 divided between all contexts
Inspection statements	32	32 per context
NAT statements	2,048	2,048 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	2,048	2,048 divided between all contexts
TFTP sessions, concurrent ¹	999,100	999,100 divided between all contexts
URL filtering requests	200 per second causes 50% CPU usage	200 per second causes 50% CPU usage 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. This section describes the default maximum rules per feature, how to allocate rules between features, and how rules are divided between multiple contexts, and includes the following topics:

- [Default Rule Allocation, page A-7](#)
- [Rules in Multiple Context Mode, page A-7](#)
- [Reallocating Rules Between Features, page A-8](#)

Default Rule Allocation

Table 1-8 lists the default number of rules for each feature type.



Note

Some access lists use more memory than others. Depending on the type of access list, the actual limit the system can support will be less than the maximum. See the [“Maximum Number of ACEs”](#) section on page 12-5 for more information about ACEs and memory usage.

Table 1-8 **Default Rule Allocation**

Specification	Context Mode	
	Single	Multiple (Maximum per Partition) with 12 ¹ pools
AAA Rules	8744	1345
ACEs	100,567	14,801
established commands ²	624	96
Filter Rules	3747	576
ICMP, Telnet, SSH, and HTTP Rules	2498	384
Policy NAT ACEs ³	2498	384
Inspect Rules	5621	1537
Total Rules	124,923	19,219

1. Use the **show resource rule** command to view the default values for partitions other than 12.
2. Each **established** command creates a control and data rule, so this value is doubled in the Total Rules value.
3. This limit is lower than in release 2.3.

Rules in Multiple Context Mode

In multiple context mode with the default of 12 memory partitions, each context supports the maximum number of rules listed in Table 1-8; the actual number of rules supported in a context might be more or less, depending on how many contexts you have and how many partitions you configure. See the [“About Memory Partitions”](#) section on page 9-10 for information about memory distribution among contexts.

If you reduce the number of partitions, the maximum number of rules is recalculated and might not match the total system number available for 12 partitions. To view the maximum number of rules for each partition, go to System > Configuration > Device Management > Resource Allocation > Global Rules. At the top of the pane, ASDM states the total number of rules allowed.

Reallocating Rules Between Features

You can reallocate rules from one feature to another feature.

Guidelines



Caution

Failure to follow these guidelines might result in dropped access list configuration as well as other anomalies, including ACL tree corruption.

- The target partition and rule allocation settings must be carefully calculated, planned, and preferably tested in a non-production environment prior to making the change to ensure that all existing contexts and rules can be accommodated.
- When failover is used, both FWSMs need to be reloaded at the same time after making partition changes. Reloading both FWSMs causes an outage with no possibility for a zero-downtime reload. At no time should two FWSMs with a mismatched number of partitions or rule limits synchronize over failover.

Detailed Steps

To reallocate rules, perform the following steps.



Note

In multiple context mode, you can also set the rule allocation per partition, which overrides the global setting in this section. See the [“Reallocating Rules Between Features for a Specific Memory Partition” section on page 9-15](#).

Step 1

To view the number of rules currently being used so you can plan your reallocation, enter one of the following commands at the Command Line Interface tool.

- In single mode, or within a context:


```
show np 3 acl count 0
```
- In multiple context mode system execution space, enter the following command:


```
show np 3 acl count partition_number
```

For example, the following is sample output from the **show np 3 acl count** command, and shows the number of inspections (Fixup Rule) close to the maximum of 9216. You might choose to reallocate some access list rules (ACL Rule) to inspections.

```
show np 3 acl count
```

```
Result of the command: "show np 3 acl count"
```

```
----- CLS Rule Current Counts -----
CLS Filter Rule Count      :          0
CLS Fixup Rule Count      :        9001
```

```

CLS Est Ctl Rule Count      :          4
CLS AAA Rule Count         :          15
CLS Est Data Rule Count    :          4
CLS Console Rule Count     :          16
CLS Policy NAT Rule Count  :           0
CLS ACL Rule Count        :        30500
CLS ACL Uncommitted Add   :           0
CLS ACL Uncommitted Del   :           0
...

```



Note The **established** command creates two types of rules, control and data. Both of these types are shown in the display, but you allocate both rules by setting the number of **established** commands; you do not set each rule separately.

- Step 2** To reallocate rules between features, go to one of the following panes, depending on your security context mode:
- Single mode—Configuration > Device Management > Dynamic Resource Allocation.
 - Multiple mode—System > Configuration > Device Management > Resource Allocation > Global Rules.
- At the top of the pane, ASDM states the total number of rules allowed.
- Step 3** For each rule type, enter a new number or choose **default** or **max** from the drop-down list. The default and max options show the number of rules representing the default and maximum settings. In multiple context mode, those numbers depend on the number of partitions you set. In multiple context mode, this pane sets the rule allocation *per partition*.
- Step 4** Click **Apply**. These settings take effect immediately when you Apply; you do not need to reload the FWSM.
-

