



# APPENDIX **A**

## 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-3](#)
- [Feature Limits, page A-3](#)
- [Managed System Resources, page A-4](#)
- [Fixed System Resources, page A-5](#)
- [Rule Limits, page A-6](#)

## 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 software releases.
- Cisco 7600 series routers, with the following required components:
  - Supervisor engine with Cisco IOS software. See [Table A-2](#) for supported supervisor engine and software releases.
  - MSFC 2 with Cisco IOS software. See [Table A-2](#) for supported Cisco IOS software 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.

---

This section includes the following topics:

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

## Catalyst 6500 Series Requirements

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

**Table A-1 Support for FWSM 3.2 on the Catalyst 6500**

	Supervisor Engines <sup>1</sup>
<b>Cisco IOS</b>	
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	22, 720, 32
<b>Cisco IOS Software Modularity</b>	
12.2(18)SXF4	720, 32
<b>Catalyst OS<sup>2</sup></b>	
8.5(3) and higher	22, 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.)

## Cisco 7600 Series Requirements

Table A-2 shows the supervisor engine version and software.

**Table A-2 Support for FWSM 3.2 on the Cisco 7600**

	Supervisor Engines <sup>1</sup>
<b>Cisco IOS</b>	
12.2(33)SRA	720, 32
12.2(33)SRB	720, 32
12.2(33)SRC	720, 32, 720-1GE
12.2(33)SRD	720, 32, 720-1GE

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 A-3 lists the physical attributes of the FWSM.

**Table A-3 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"> <li>• 1-GB RAM.</li> <li>• 128-MB Flash memory.</li> </ul>
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-4 lists the feature limits for the FWSM.

**Table A-4 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"> <li>• 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.</li> <li>• If the FWSM receives a fragment set that is originally 8783 Bytes or larger, then: <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> </ul> </li> </ul>	

**Table A-4** Feature Limits (continued)

Specification	Context Mode	
	Single	Multiple
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-5 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-5** 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 <sup>1</sup>	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 <sup>2</sup>	5	5 per context Maximum of 100 divided between all contexts

**Table A-5** *Managed System Resources (continued)*

Specification	Context Mode	
	Single	Multiple
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 <sup>3 4</sup> between any two hosts, including connections between one host and multiple other hosts, concurrent and rate	999,900 <sup>5</sup> 100,000 per second	999,900 divided between all contexts <sup>5</sup> 100,000 per second divided between all contexts
Telnet management connections, concurrent <sup>2</sup>	5	5 per context Maximum of 100 connections divided between all contexts.

1. 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.
2. The admin context can use up to 15 Telnet and SSH connections.
3. 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-6 lists the fixed system resources of the FWSM.

**Table A-6** *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

**Table A-6 Fixed System Resources (continued)**

Specification	Context Mode	
	Single	Multiple
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 <sup>1</sup>	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-6](#)
- [Rules in Multiple Context Mode, page A-7](#)
- [Reallocating Rules Between Features, page A-8](#)

## Default Rule Allocation

Table A-7 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 10-6](#) for more information about ACEs and memory usage.

**Table A-7** Default Rule Allocation

Specification	Context Mode	
	Single	Multiple (Maximum per Partition) with 12 <sup>1</sup> pools
AAA Rules	6451	992
ACEs	74,188	10,633
<b>established</b> commands <sup>2</sup>	460	70
Filter Rules	2764	425
ICMP, Telnet, SSH, and HTTP Rules	1843	283
Policy NAT ACEs <sup>3</sup>	1843	283
Inspect Rules	4147	1417
<b>Total Rules</b>	<b>92,156</b>	<b>14,173</b>

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 A-7](#); 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 [“Configuring Memory Partitions”](#) section on page 4-17 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 partitions, enter the following command in the system execution space:

```
hostname(config)# show resource rule
```

For example, the following display shows the maximum rules as 14173 per partition with 12 partitions (this is an example only, and might differ from the actual number of rules for your system):

```
hostname(config)# show resource rule
```

```

          Default  Configured  Absolute
    CLS Rule  Limit    Limit      Max
-----+-----+-----+-----
    Policy NAT    283      283       833
    ACL          10633    10633    10633
    Filter        425      425       850
    Fixup         1417    1417    2834
    Est Ctl        70       70        70
    Est Data       70       70        70
    AAA           992      992     1984
    Console       283      283       566
-----+-----+-----+-----
    Total         14173    14173

```

```

Partition Limit - Configured Limit = Available to allocate
    14173      -      14173      =          0

```

## Reallocating Rules Between Features

You can reallocate rules from one feature to another feature. To reallocate rules, perform the following steps.

- Step 1** To view the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature, enter the following command:

```
hostname(config)# show resource rule
```

For multiple context mode, enter this command in the system execution space. It shows the number of rules per partition. See the “[Rules in Multiple Context Mode](#)” section on page A-7 for more information about partitions.

For example, the following display shows the maximum rules as 92156 in single mode (this is an example only, and might differ from the actual number of rules for your system):

```
hostname(config)# show resource rule
```

CLS Rule	Default Limit	Configured Limit	Absolute Max
Policy NAT	1843	1843	10000
ACL	74188	74188	74188
Filter	2764	2764	5528
Fixup	4147	4147	10000
Est Ctl	460	460	460
Est Data	460	460	460
AAA	6451	6451	10000
Console	1843	1843	3686
<b>Total</b>	<b>92156</b>	<b>92156</b>	

```

Partition Limit - Configured Limit = Available to allocate
    92156      -      92156      =           0

```

- Step 2** To view the number of rules currently being used so you can plan your reallocation, enter one of the following commands.

- In single mode or within a context, enter the following command:

```
hostname(config)# show np 3 acl count 0
```

- In multiple context mode system execution space, enter the following command:

```
hostname(config)# show np 3 acl count partition_number
```

For example, the following display 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.

```
hostname(config)# show np 3 acl count 0
```

```

----- 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 3** To reallocate rules between features, enter the following command (in multiple context mode, enter it in the system execution space). If you increase the value for one feature, then you must decrease the value by the same amount for one or more features so the total number of rules does not exceed the system limit. See [Step 1](#) to use the **show resource rule** command for the total number of rules allowed.

```
hostname(config)# resource rule nat {max_policy_nat_rules | current | default | max}
acl {max_ace_rules | current | default | max}
filter {max_filter_rules | current | default | max}
fixup {max_inspect_rules | current | default | max}
est {max_established_rules | current | default | max}
aaa {max_aaa_rules | current | default | max}
console {max_console_rules | current | default | max}
```

In multiple context mode, this command sets the rule allocation *per partition*. You must enter all arguments in this command. This command takes effect immediately.

The **nat** *max\_nat\_rules* arguments set the maximum number of policy NAT ACEs, between 0 and 10000.

The **acl** *max\_nat\_rules* arguments set the maximum number of ACEs, between 0 and the system limit. The system limit depends on single or multiple context mode, and how many memory partitions you configured. For single mode, the value is 74188. For multiple mode, see [Step 1](#) to use the **show resource rule** command.

The **filter** *max\_nat\_rules* arguments set the maximum number of filter rules, between 0 and 6000.

The **fixup** *max\_nat\_rules* arguments set the maximum number of inspect rules, between 0 and 10000.

The **est** *max\_nat\_rules* arguments set the maximum number of **established** commands, between 0 and 716. The established command creates two types of rules, control and data. Both of these types are shown in the **show np 3 acl count** and **show resource rules** display, but you set both rules using the **est** keyword, which correlates with the number of **established** commands. Be sure to double the value you enter here when comparing the total number of configured rules with the total number of rules shown in the **show** commands.

The **aaa** *max\_nat\_rules* arguments set the maximum number of AAA rules, between 0 and 10000.

The **console** *max\_nat\_rules* arguments set the maximum number of ICMP, Telnet, SSH, and HTTP rules, between 0 and 4000.

The **current** keyword keeps the current value set.

The **default** keyword sets the maximum rules to the default.

The **max** keyword sets the rules to the maximum allowed for the feature. Be sure to set other features lower to accommodate this value.

For example, to reallocate 1000 rules from the single-mode default 74,188 ACEs to inspections (default 4147), enter the following command:

```
hostname(config)# resource rule nat default acl 73188 filter default fixup 5157 est
default aaa default console default
```

In multiple context mode with 12 partitions, to reallocate 100 ACEs (default 10,633) to inspections (default 1417) as well as all but one established rule (default 70) to filter (default 425), enter the following command:

```
hostname(config)# resource rule nat default acl 10533 filter 494 fixup 1517 est 1 aaa  
default console default
```