Q & A

CISCO FIREWALL SERVICES MODULE FAQ

Q. Can a FlexWAN interface terminate on the FWSM?

A. Not at this time. FlexWAN interfaces and routed ports use hidden VLANs which can't be passed directly to a firewall vlan-group. The WAN traffic must terminate on the MSFC and then pass to the FWSM using another VLAN.

Q. Can we pass traffic between two interfaces at the same security level?

A. Yes in FWSM2.2, No in FWSM1.1. A command has been provided to allow traffic to pass between interfaces at the same security level (`same-security-level permit inter interface`). In addition to invoking this command, the policy must be configured to allow the traffic to pass.

Q. Can we configure more than one interface at security level 100 (inside)?

A. Yes in FWSM2.2, No in FWSM1.1.

FWSM2.2 eliminates the special status given to interfaces with names "inside" and "outside". Beginning with the 2.2 release, the user can assign any name to an interface and configure any security level between 0 to 100 for that interface.

Q. The FWSM has a label that states, "Do not remove card while status light is green or disk corruption may occur." What does this mean?

A. The firewall module should be removed only after disabling power using one of the following methods. (There is no preference for a particular method.)

Use the switch's command-line interface (CLI) and issue one of the following commands.

- CatOS—`set module power down mod`
- Cisco IOS® Software—`no power enable module slot`
- Press the shutdown button on the blade.
- Physically power down the chassis.
- When the status light in longer green, you may remove the module safely.

Q. I used the show module command, and my FWSM has a status of faulty/other. What should I do?

A. Refer to the following checklist to troubleshoot an FWSM with a status of faulty/other.

- Ensure that you are running a supported version of code on your switch. Ensure that the FWSM can co-exist with the other blades located in the same chassis. Refer to the Catalyst 6500 Release Notes and/or Software Advisor (registered customers only) for further information.
- If you are running CatOS/Hybrid code on your switch, reset the configuration for the slot occupied by the FWSM module. To do this, use the following commands.
- Type set module power down mod to power down the FWSM.
- Type to clear the switch's configuration associated with that slot and to power up the module.

For additional information, refer to the following documentation.

- Hardware Failure Checklist for Catalyst 4000, 5000, and 6000 Series Switches Running CatOS
- Troubleshooting Hardware and Common Issues on Catalyst 6000 Series Switches Running Integrated Cisco IOS (Native Mode)

If you are still experiencing problems, please contact Cisco Technical Support for further troubleshooting.

Q. Where can I find FWSM documentation?

A. Release Notes for the FWSM can be found at
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Q. What is the minimum version of code that I need to run to support my FWSM, Intrusion Detection System Module 2 (IDSM2), and VPN Service Module (VPNSM)?

A. The appropriate version of code depends on the type of Supervisor Module in your 6500 or 7600 chassis, as well as the type of software you are running (CatOS [Hybrid] or Cisco IOS [Native]). Please refer to the table below for specific code versions for your module and Multilayer Switch Feature Card (MSFC). In addition, please refer to the release notes for updates to this table.

	Sup1 (with MSFC)		Sup2 (with MSFC)		Sup720	
Module	**Cisco IOS**	**CatOS**	**Cisco IOS**	**CatOS**	**Cisco IOS**	**CatOS**
FWSM	Not Supported	Not Supported	12.1(13)E	7.5(1)	12.2(14)SX1	8.2(1)
IDSM2	Not Supported	7.6(1)	12.1(19)E	7.6(1)	12.2(14)SX1	8.2(1)
VPNSM	Not Supported	Not Supported	12.2(14)SY	Not Supported	12.2(17a)SX10	Not Supported [1]

Note: For information about the differences between CatOS (Hybrid) and Cisco IOS (Native), refer to Comparison of the Cisco Catalyst and Cisco IOS Operating Systems for the Cisco Catalyst 6500 Series Switch.

Q. Can I run the FWSM, Intrusion Detection System Module 2 (IDSM2), and VPN Service Module (VPNSM) in the same chassis?

A. Yes, you can run these modules in the same chassis if the switch is running integrated Cisco IOS software with a minimum version of Cisco IOS Software Release 12.2(14)SY (Sup2) or 12.2(17a)SX10 (Sup720). Currently, there is no CatOS version that can support these service modules in the same 6500 or 7600 chassis.

Q. What are my configuration and management options for the FWSM?

A. Configuration and management options include the following.

[1] There are plans to introduce support.

Option	Version	Description
Management Center for Firewalls	Versions 1.3.0 and 1.3.1	This is a web-based interface for configuring and managing multiple FWSM. **Note:** Support for service groups within object grouping is limited. Service groups are successfully parsed, but flatten immediately. This affects commands with icmp-type, protocol, and service keywords . This limitation applies to versions 1.3 and earlier. V1.3.1 provides support for AAA fallback and online upgrade features introduced in FWSM2.2.
Monitoring Center for Security	Versions 1.2 and later[1]	This is a web-based interface for monitoring Cisco security devices. The software centralizes syslog management from multiple Cisco security devices with flexible reporting and alerting options.
Monitoring Center for Performance	Versions 2.0 and later*	This is a web-based interface for monitoring and troubleshooting the health and performance of services that contribute to network security. Simple Network Management Protocol (SNMP) is the underlying protocol used.
PDM	Version 4.0	This is a web-based interface for configuring, managing, and monitoring a FWSM. PIX Device Manager (PDM) must be installed locally on the FWSM.
Telnet	N/A	Telnet provides remote command-line interface (CLI) access to a firewall. **Note:** To allow Telnet access to the lowest security interface (commonly known as the outside interface), you need to Configure IPSec for Management.
Secure Shell (SSH)	N/A	SSH provides secure remote CLI access to a firewall.
SNMP	N/A	SNMP provides a method of monitoring the FWSM. **Note:** SNMP is read-only on the FWSM.
Syslog	N/A	Syslog provides a method of monitoring the FWSM.

Q. What is an SVI? Can I configure multiple SVIs?

A. SVI stands for Switched Virtual Interface. It represents a logical Layer 3 interface on a switch. For CatOS versions earlier than 7.6(1) and Cisco IOS Software Releases earlier than 12.2(14)SY, only one SVI is allowed as part of the firewall VLANs. In other words, only one Layer 3 interface can be configured between the FWSM and Multilayer Switch Feature Card (MSFC). Attempting to configure multiple SVIs produces a command-line interface (CLI) error message.

For CatOS versions 7.6(1) and later and Cisco IOS Software Releases 12.2(14)SY and later, the FWSM supports multiple SVIs. By default, only one SVI is supported. To enable support for multiple SVIs on your switch, use one of the following commands.

For CatOS, type

`set firewall multiple-vlan-interfaces enable.` For Cisco IOS, type `firewall multiple-vlan-interfaces` .

If you are configuring your switch for the FWSM VLANs and receive an error message indicating that you have more than one SVI, look at your switch and/or MSFC configuration to ensure that only one Layer 3 interface (or VLAN interface) exists as part of the firewall VLANs.

Note: Cisco recommends using only one SVI; this will allow you to avoid a complicated configuration involving policy routing.

[1] This software is part of the CiscoWorks VPN/Security Management Solution (VMS) bundle. This software provides an integrated approach to managing Cisco security devices via a browser-based interface for Enterprise networks.

Q. Why am I unable to ping my FWSM on a directly connected interface?

A. By default, each interface denies Internet Control Message Protocol (ICMP). Use the `icmp` command to allow this traffic to the interface. This behavior differs from that of the PIX.

Note: When ICMP to the interface is denied by the icmp command, you will still see the correct MAC address in the Address Resolution Protocol (ARP) table. If you do not see the MAC address, please see the next question.

Q. I am unable to ping my FWSM on a directly connected interface, and I do not see an Address Resolution Protocol (ARP) entry for the interface. I am running CatOS (or hybrid) software on my switch. What should I do?

A. Configuring the interfaces within the FWSM configuration (with the `nameif` command) or on the Multilayer Switch Feature Card (MSFC) [with the `interface vlan` command] before they are configured on the switch (on the Supervisor Module in CatOS) may make the interfaces appear as if they are not responding at all, with no ARP entry or Internet Control Message Protocol (ICMP) response.

If you configured an interface on the FWSM or MSFC that belongs to the firewall VLANs before you configured the switch, remove the FWSM or MSFC entry, reload the module, then re-add the entry.

Q. Why am I unable to ping or pass any traffic through the FWSM?

A. Unlike the PIX, which allowed traffic from inside to outside, The FWSM has an implicit deny rule on all interfaces. For traffic to pass through the FWSM from a higher security interface (the inside interface) to a lower security interface (outside interface), Network Address Translation (NAT) must be configured using the `nat 0`, `nat/global`, or `static` command.

You must also use the `access-list` command to implement access lists that permit traffic to flow through the FWSM. By default, access lists deny all traffic on all interfaces (deny ip any any). This behavior differs from the PIX's default configuration, which allows traffic from higher to lower security and denies traffic from lower to higher security. To get the FWSM to behave like the PIX, configure an access list with permit ip any and apply it to the high-security interface(s).

Q. I can ping the FWSM interface that is directly connected to my network, but I am unable to ping other interfaces. Is this normal?

A. Yes. This is an built-in security mechanism that also exists on the PIX Firewall.

PERFORMANCE

Q. Does virtualization in FWSM2.2 cause any performance hit over FWSM1.1?

A. Yes, although generally not significantly so. FWSM2.2 performance will be within 90% of the performance of FWSM1.1. Some parameters are lower due to allocations established per context. See limitations section.

Q. Can the administrator prevent an individual context from consuming all of the available blade resources?

A. Yes. FWSM2.2 provides a resource manager function that allows an individual context to be limited to either a percentage of blade resources, or a finite amount. Users can be placed in classes of equivalent limitation, or left in a default class, which allows total resource access on a first come first served basis.

FAILOVER

Q. Can I configure failover between two FWSMs running different versions of code?

A. No with FWSM1.1, and a qualified yes with FWSM2.2. FWSM1.1 Failover requires that both FWSMs run the same version of code. A mechanism within the failover feature verifies the peer version and prevents failover if the versions of code are different. For this reason, you must upgrade both FWSMs at the same time. To allow flexibility in upgrading live networks, FWSM2.2 has a feature called 'online upgrade' that allows failover between FWSM running different point releases of code (e.g. 2.2 to 2.3). Failover is still not allowed between major releases e.g. 2.x to 3.x)

Q. Can I configure failover between two FWSMs in different chassis?

A. Yes. But the FWSMs must be connected by Layer 2 on all interfaces. In other words, all interfaces must be capable of exchanging Layer 2 broadcast packets [Address Resolution Protocol (ARP), and so forth] with each other. Failover protocol packets cannot be routed at Layer 3.

Q. I have set up failover between two FWSMs, but they are not syncing. What could be the problem?

A. Ensure that your configuration meets the following requirements for successful failover.

Both FWSMs must run the same version of code (FWSM1.1(x).

Both FWSMs must have the same number of VLANs.

A Layer 2 connection must exist between all VLANs on the FWSMs. If the FWSMs exist in different chassis with a trunk configured between them, verify that all VLANs exist and are allowed on the trunk. For more information on how to configure and troubleshoot trunks, refer to the following documents.

Sample Configuration: 802.1q Trunking Between Catalyst Switches Running CatOS and Integrated Cisco IOS (Native Mode)

Configuring ISL Trunking on Catalyst 5000 and 6000 Family Switches

VIRTUALIZATION

Q. How many VLAN interfaces does the FWSM2.2 support in virtual (multiple) mode?

A. FWSM version 2.2 supports up to 1000 VLANs per blade in routed multiple mode and 250 VLANs per security context in routed multiple mode until the 1000VLAN limitation is reached per blade, or 4000 VLANs per chassis. Multiple Transparent mode supports two VLAN interfaces per context and they can not be shared with other contexts on the blade.

Q. Can contexts share VLAN interfaces?

A. Yes, in routed mode in some cases. Sharing is not possible in transparent mode in FWSM2.2 but may be allowed in future releases.

Q. Can I allow users to manage their individual contexts?

A. Yes. Users can use PDM4.0 or CLI to manage their context. If a user logs into a context, he/she is not allowed to switch to a different context. The FWSM administrator can change to any context if they log in to the admin context first.

Q. Do I need a license to run multiple contexts?

A. Maybe. You are allowed to configure two contexts and an admin context without a license. Additional contexts will require a license. A tiered licensing structure is provided with 20, 50, and 100 context licenses available. The maximum number of contexts is equal to the license tier plus 1 admin context.

Q. Does my standby failover FWSM require a license?

A. Yes. The standby FWSM requires the same license as the active unit and the context numbers must match. This differs from the PIX, which has a different license for the Active and standby units (UR/R).

Q. Can I re-use my license key if I replace a FWSM?

A. No. The license key is associated with the FWSM hardware serial number, and can not be transferred. A new key will need to be generated.

Q. Does the license have to be renewed every year?

A. No. The license is good indefinitely. There is no expiration date.

Q. Do I need to reboot the blade if I upgrade licenses?

A. No. A reboot is not required.

TRANSPARENCY

Q. Can I configure contexts for both routed and transparent mode on the same FWSM?

A. Not in FWSM2.2. The ability to mix transparent and routed contexts on the same blade is planned for a future release.

LIMITATIONS

Q. How many VLANs does the FWSM support?

A. FWSM version 1.1 supports 100 VLANs and FWSM version 2.2 supports up to 1000 VLANs per blade in routed multiple mode and 250 VLANs per security context in routed multiple mode. Transparent mode supports two interfaces per context (they can not be shared with other contexts).

Q. How many ACLs will the FWSM support?

A. FWSM1.1 supports about 80,000 rules. FWSM2.2 supports about 63,000 rules for the entire blade. In FWSM we store the following types of rules as ACLs in the same tree:

```
access-lists (ACEs)
filter
AAA
ICMP/ssh/telnet/http
established
Policy-based NAT/static
```

All these together comprise the 80K limit in 1.1 (and 2.2 as well). FWSM 1.1 does not restrict the number of individual rule types, so you could potentially configure 80K AAA commands and the user will not be able to get anything else in there. FWSM 2.2 limits the number of individual rules types that a user can configure. The following limits are applied for FWSM 2.2:

Single Mode:

3942 = Filter MAX

788 = Established Rule MAX

3942 = AAA Rule MAX

2365 = Console (icmp/telnet/ssh/http) Rule MAX

3942 = Policy-based NAT Rule MAX

63078 = ACL Rule MAX

Multi Mode (per context):

606 = Filter MAX

121 = Established Rule MAX: 121

606 = AAA Rule MAX: 606

363 = Console (icmp/telnet/ssh/http) Rule MAX: 363

606 = Policy-based NAT Rule MAX: 606

9704 = ACL Rule MAX: 9704

These numbers are derived using the following distribution:

Note: X = 80,000 for single mode and 12130 per context in multi-mode

Total Rules (best case) X.

5% of X = Filter MAX

1% of X = Established Rule MAX

5% of X = AAA Rule MAX

3% of X = Console (icmp/telnet/ssh/http) Rule MAX

5% of X = Policy-based NAT Rule MAX

80% of X = ACL Rule MAX

3000 = Dynamic ACL

Q. Where can I find information on the error messages I am seeing on my FWSM?

A. The Error Message Decoder (registered customers only) provides details on many FWSM error messages. Product documentation on system messages also contains useful information. If you require further assistance, please contact Cisco Technical Support.

Q. Where can I find information on existing bugs for my FWSM?

A. Details on existing bugs can be found in the Bug Toolkit (registered customers only).

Q. Does the FWSM support the access-list compiled command?

A. The FWSM automatically compiles access lists into hardware after 1.0 seconds of inactivity at the command-line interface (CLI), there is no need for turbo access lists. FWSM version 2.2 offers the additional functionality of being able to nominate when the access lists are compiled through use of a manual commit option.

Q. Does the FWSM support the IOS Open Shortest Path First (OSPF) auto-cost reference-bandwidth command?

A. No. The FWSM is not aware of the physical ports connected to it. OSPF cost must be configured manually per interface using the `ospf cost` command.

Q. Can I run Open Shortest Path First (OSPF) protocol in a topology where two different interfaces of the FWSM connect to the same network?

A. Yes. This functionality is supported in versions 2.2 and later. Note that OSPF and RIP are not supported when operating in multiple mode.

Q. What routing protocols are supported by the FWSM?

A. Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) are the supported routing protocols on FWSM1.1 and FWSM2.2 running in single mode. For more information, search for "firewall" in Catalyst 6500 Series Release Notes and Catalyst 6500 Series Module Installation and Configuration Documentation.

Q. Is Multicast (Internet Group Management Protocol [IGMP] v2 and Stub Multicast Routing) supported on the FWSM?

A. No.

Q. Does the FWSM support third party URL and FTP Filtering?

A. Yes. Websense is supported in versions 1.1 and later, with additional support for N2H2 added in version 2.2.

Q. Why are fragmented packets dropped by the FWSM?

A. In FWSM1.1 fragmented packets can not traverse the FWSM by default. You can use the fragment command to configure this feature. This behavior differs from that of the PIX Firewall. In FWSM2.2 fragmented packets can traverse the FWSM, as the default setting is now the same as the PIX (200)

Common protocols that use fragmented packets are Open Shortest Path First (OSPF) and Network File System (NFS).

Q. Can I terminate VPN connections on my FWSM?

A. VPN functionality is not supported on the FWSM except for management connections terminating on the FWSM. Termination of VPN connections for traffic flowing through the FWSM should be performed on the switch and/or VPN Services Module. The 3DES license is provided for management purposes only, such as connecting to the management interface on the FWSM through a low-security interface via Telnet, Secure Shell (SSH), and Secure HTTP (HTTPS).

Q. Is authentication, authorization, and accounting (AAA) for RADIUS or TACACS+ supported on the FWSM?

A. Yes. AAA is supported for both FWSM management and traffic passing through the FWSM. Please refer to the Firewall Services Module documentation for additional details.

The FWSM offers similar functionality to that of the PIX Firewall, with the exceptions of downloadable access lists which are not available on FWSM1.1, but are available on FWSM2.2, and VPNs. With this in mind, you can use the following PIX Firewall documents as guides for FWSM configuration.

- How To Perform Authentication and Enabling on the Cisco Secure PIX Firewall (5.2 Through 6.2)
- Performing Authentication, Authorization, and Accounting of Users Through PIX Versions 5.2 and Later

Q. How do I perform a password recovery for the FWSM?

A. Refer to the following documents for information on password recovery.

- For version 1.1(1), refer to FWSM Configuration Note 1.1(1) on Changing and Recovering Passwords
- For versions 1.1(2) and 1.1(3), refer to FWSM Configuration Note 1.1(2) on Changing and Recovering Passwords

NETPRO DISCUSSION FORUMS—FEATURED CONVERSATIONS FOR SECURITY

Security: Intrusion Detection [Systems]
IDSM-2 service pack upgrades—Apr 20, 2004
connection problem—Apr 20, 2004
Cisco Security Agent—Apr 20, 2004
IDS 4235 sensing interface shutting down alone !—Apr 19, 2004
Configuring TCP SYN HOST SWEEPS(SIGID 3030)—Apr 19, 2004
Security: AAA
Bordermanager Radius and PIX 515e, Apr 20, 2004
User not authenticated sometimes with ACS for Unix—Apr 20, 2004
Differentiating between AAA servers—Apr 20, 2004
Tacacs+/secondary authentication method problem—Apr 19, 2004
how to modify AR snmp.comf file in Solaris 2.8—Apr 19, 2004
Security: General
ACS 3.2 and PEAP—Can NOT get certificate installed!—Apr 20, 2004
NAT problem—Apr 19, 2004
Firewall MC upgrade—Apr 19, 2004
PIX 506E restarting by itself—Apr 18, 2004
Lock and key acl—Apr 16, 2004
Security: Firewalling
VPN and NAT —Apr 20, 2004
port redirection—Apr 20, 2004
internet trouble—Apr 20, 2004
PIX 501 configuration help needed—Apr 20, 2004
Load Balance from two ISPs into single PIX Firewall—Apr 20, 2004

RELATED INFORMATION

Firewall Services Module Documentation

Technical Support—Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe