

# Firewall Services Module FAQ

Document ID: 46385

---

## Questions

### Introduction

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?

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

Where can I find FWSM documentation?

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

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

What are my configuration and management options for the FWSM?

What is an SVI? Can I configure multiple SVIs?

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

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?

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

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

Can I configure failover between two FWSMs that run different versions of code?

Can I configure failover between two FWSMs in different chassis?

Does FWSM support SNMPv3?

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

Where can I find information on the error messages that I see on my FWSM?

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

How many VLANs does the FWSM support?

Does the FWSM support the access-list compiled command?

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

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

What routing protocols are supported by the FWSM?

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

Does the FWSM support URL Filtering?

Why are fragmented packets dropped by the FWSM?

Can I terminate VPN connections on my FWSM?

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

How do I perform a password recovery for the FWSM?

Does FWSM support jumbo frames?

I have a license for an FWSM that runs in multiple context mode. Can I obtain a license for a spare FWSM in the event of a hardware failure?

How do I place additional VLANs behind the FWSM?

How many VLANs can I place behind the FWSM using the Single Context, Routed

mode?

What are the differences between the PIX Firewall and the Firewall Services Module?

I could not issue multiple access-group commands on the FWSM per interface. FWSM seems to only take one access group per interface. Why?

Is PVLAN supported on FWSM?

Is access list line number supported in FWSM?

Can you limit the number of connections a user can have on the FWSM?

Are there any limitations in the implementation of multicast in FWSM?

Is directed broadcast allowed through FWSM?

Can the HTTP Inspection engine detect non-HTTP traffic or non-standard traffic in an HTTP session?

Does FWSM support multiple shared interfaces?

Are the normalization features in ASA and FWSM compatible?

Do we need to enable/disable TCP normalizer?

What is the maximum number of mfib entries that a FWSM can support?

What information is stored in the xlate entries in FWSM?

What do the values and statistics in `show perfmon` on FWSM imply?

Will there be a performance hit on the FWSM with the `no monitor session servicemodule` command?

Can you increase memory in order to store more Access Control Lists (ACLs)?

How can I capture packets in FWSM?

Which version of ASDM does FWSM support?

Why does the capture command when applied to the FWSM stops and does not capture traffic as soon as another capture command is applied on the interface?

Can I configure failover for three or more units of FWSM, which are spread over different switch chassis?

NetPro Discussion Forums – Featured Conversations

Related Information

---

## Introduction

This document contains frequently asked questions (FAQs) about the Catalyst 6500 Series Firewall Services Module (FWSM).

**Note:** Refer to the Cisco Technical Tips Conventions for more information on document conventions.

### 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 you disable power using one of these methods. (There is no preference for a particular method.)

- ◆ Use the command-line interface (CLI) of the switch and issue one of these 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.

You can remove the module safely when the status light is longer green.

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

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

- ◆ Ensure that you run 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 more information.
- ◆ If you run CatOS/Hybrid code on your switch, reset the configuration for the slot occupied by the FWSM module. Use these commands in order to do this.

1. Type **set module power down mod** to power down the FWSM.
2. Type **clear config mod** to clear the configuration of the switch associated with that slot and to power up the module.

Refer to this documentation for more information.

- ◆ 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 continue to experience problems, contact Cisco Technical Support for further troubleshooting.

## Q. Where can I find FWSM documentation?

A. Release Notes for the FWSM can be found under the Catalyst 6500 Series Release Notes. (Search the page for "firewall.") Configuration documentation can be found under the Catalyst 6500 Series Module Installation and Configuration Documentation. (Search the page for "firewall.")

## Q. What is the minimum version of code that I need to run in order 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 run (CatOS [Hybrid] or Cisco IOS [Native]). See this table for specific code versions for your module and Multilayer Switch Feature Card (MSFC).

| Module | Sup1 (with MSFC) |               | Sup2 (with MSFC) |               | Sup720        |                 |
|--------|------------------|---------------|------------------|---------------|---------------|-----------------|
|        | Cisco IOS        | CatOS         | Cisco IOS        | CatOS         | Cisco IOS     | CatOS           |
| FWSM   | 12.1(13)E        | 7.5(1)        | 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 * |

\* There are plans to introduce support.

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

**Q. Can I run the FWSM, Intrusion Detection System Module 2 (IDS M2), and VPN Service Module (VPNSM) in the same chassis?**

**A.** Yes, you can run these modules in the same chassis if the switch runs 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 these.

| Option                            | Version                   | Description   |
|-----------------------------------|---------------------------|---|
| Management Center for Firewalls   | Versions 1.1.1 and later* | This is a web-based interface for configuring and managing multiple firewalls.<br><br><b>Note:</b> Support for service groups within object grouping is limited. Service groups are successfully parsed, but flatten immediately. This affects commands with <b>icmp-type, protocol, and service</b> keywords. This limitation applies to versions 1.3 and earlier. |
| Monitoring Center for Security    | Versions 1.2 and later*   | 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 2.1 | This is a web-based interface for configuring, managing, and monitoring a single firewall. PIX Device Manager (PDM) must be installed locally on the PIX Firewall.  |
| Telnet             | N/A         | Telnet provides remote command-line interface (CLI) access to a firewall.<br><br><b>Note:</b> In order 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.<br><br><b>Note:</b> SNMP is read-only on the FWSM.   |
| Syslog             | N/A         | Syslog provides a method of monitoring the FWSM.  |

\* 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. 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). An attempt 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. Use one of these commands to enable support for multiple SVIs on your switch.

- ◆ For CatOS, type **set firewall multiple-vlan-interfaces enable** .

For Cisco IOS, type **firewall multiple-vlan-interfaces** .

If you configure your switch for the FWSM VLANs and receive an error message which indicates 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:** Only use one SVI. This allows you to avoid a complicated configuration that involves policy routing.

### **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 still see the correct MAC address in the Address Resolution Protocol (ARP) table. If you do not see the MAC address, 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.** Network Address Translation (NAT) must be configured using the **nat 0** , **nat/global** , or **static** command for traffic to pass through the FWSM from a higher security interface (the inside interface) to a lower security interface (outside interface).

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 default configuration of the PIX, which allows traffic from higher to lower security and denies traffic from lower to higher security.

Configure an access list with **permit ip any any** and apply it to the high-security interface(s) to get the FWSM to behave like the PIX.

### **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 a built-in security mechanism that also exists on the PIX Firewall.

### **Q. Can I configure failover between two FWSMs that run different versions of code?**

A. No. 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.

## **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 able to exchange Layer 2 broadcast packets [Address Resolution Protocol (ARP), and so forth] with each other. Failover protocol packets cannot be routed at Layer 3.

## **Q. Does FWSM support SNMPv3?**

A. No.

## **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 these requirements for successful failover.

- ◆ Both FWSMs must run the same version of code.
- ◆ 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.

## **Q. Where can I find information on the error messages that I see 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, 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. How many VLANs does the FWSM support?**

A. FWSM version 1.1 supports 100 VLANs and FWSM version 2.1 supports 250 VLANs.

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

A. Since the FWSM automatically compiles access lists into hardware after 10 seconds of inactivity at the CLI, there is no need for turbo access lists. FWSM version 2.1 offers the additional functionality of being able to nominate when the access lists are compiled.

## **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 for each interface with 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 2.1 and later.

**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. Search for "firewall" in Catalyst 6500 Series Release Notes and Catalyst 6500 Series Module Installation and Configuration Documentation for more information.

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

A. Yes. This functionality is supported in FWSM versions 2.1 and later. If you run version 1.1, you can use generic routing encapsulation (GRE) tunnelling as a workaround.

**Q. Does the FWSM support URL Filtering?**

A. Yes. Websense is supported in versions 1.1 and later, with additional support for N2H2 added in version 2.1.

**Q. Why are fragmented packets dropped by the FWSM?**

A. By default, fragmented packets cannot traverse the FWSM. You can use the **fragment** command to configure this feature. This behavior differs from that of the PIX Firewall. 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. Termination of VPN connections is the responsibility of the switch and/or VPN Services Module. The 3DES license is provided for management purposes only, such as connecting to 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. AAA is supported for both FWSM management and traffic passing through the FWSM. 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 and VPNs. With this in mind, you can use these 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 these 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

## Q. Does FWSM support jumbo frames?

A. Yes, FWSM can support jumbo frames.

## Q. I have a license for an FWSM that runs in multiple context mode. Can I obtain a license for a spare FWSM in the event of a hardware failure?

A. You can obtain a license for the spare FWSM. However, you need to place an order for the spare FWSM license as you would a regular license. In the event of a hardware failure, contact Cisco Technical Support to verify the failure and to obtain a license for the spare FWSM. Refer to Cisco Firewall Module Software Release 2.2(1) for licensing information.

## Q. How do I place additional VLANs behind the FWSM?

A. Use the **nameif** command if you want to add vlan 200 to the configuration. The security level should be between 0 and 100. The complete command syntax is **nameif vlan200 <interface name> <security level>**.

## Q. How many VLANs can I place behind the FWSM using the Single Context, Routed mode?

A. You can place 1000 VLANs behind the FWSM using the Single Context, Routed mode.

## Q. What are the differences between the PIX Firewall and the Firewall Services Module?

A. The PIX and FWSM are based on similar code. However, there are two fundamental differences. The PIX (offers support) provides VPN and IDS functionality. The FWSM does not provide VPN and IDS functionality because these features are offered in other line cards. Refer to the Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module Data Sheet for more information on the Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module. Refer to the Catalyst 6500 IPsec VPN Services Module Product Data Sheet for more information on the Catalyst 6500 IPsec VPN Services Module.

Refer to this documentation for minor differences between the PIX and FWSM:

- ◆ PIX Technical Documentation
- ◆ PIX Release Notes
- ◆ PIX Command References
- ◆ FWSM Technical Documentation

- ◆ FWSM Release Notes
- ◆ FWSM Command References

**Q. I could not issue multiple access-group commands on the FWSM per interface. FWSM seems to only take one access group per interface. Why?**

A. When you issue these commands in FWSM, only the last **access-group** command appears:

```
access-group allow_icmp in interface outside
access-group allow_caltech in interface outside
```

This is because FWSM allows only one access-list per interface per direction.

**Q. Is PVLAN supported on FWSM?**

A. Support of PVLAN begins in software version 3.1. If you run a software version earlier than 3.1, the only possible workaround is to connect the promiscuous port of the PVLAN using the crossover cable to a regular access port, and then make the VLAN of that access port firewalled.

**Q. Is access list line number supported in FWSM?**

A. This feature is supported only in software version 3.1 and later.

**Q. Can you limit the number of connections a user can have on the FWSM?**

A. Yes, you can limit the connections with the help of Modular Policy Framework. Complete these steps in order to limit the number of connections:

1. Create a class map in order to match the traffic.
2. Place the class map to a policy map and use connection limiting in the policy map.
3. Apply the policy map using service policy.

Refer to Configuring Connection Limits and Timeouts for more information and detailed steps.

**Q. Are there any limitations in the implementation of multicast in FWSM?**

A. Yes. FWSM does not support 232.x.x.x subnet as a group name, as it has been already reserved for Security Services Module (SSM).

**Q. Is directed broadcast allowed through FWSM?**

A. No. Unlike a router, the FWSM does not allow directed broadcast through its interfaces. A more similar workaround is to use the built-in dhcp-relay feature to forward broadcasts from one interface to another.

## Q. Can the HTTP Inspection engine detect non-HTTP traffic or non-standard traffic in an HTTP session?

A. Yes. The Application Firewall with Advanced HTTP Inspection can detect and control these traffic. Refer to Application Inspection Engine Overview for more information.

## Q. Does FWSM support multiple shared interfaces?

A. FWSM does not support multiple shared interfaces, but instead you can have one VLAN across multiple contexts. Refer to Sharing Resources and Interfaces Between Contexts for more information.

## Q. Are the normalization features in ASA and FWSM compatible?

A. In FWSM, TCP Normalization only applies to traffic that hits the TCP complex. Normal data plane (fast path) traffic is not affected. This differs from the ASA in that all ASA traffic is subjected to the normalizer.

On the FWSM, if the normalizer is disabled the module falls back to 2.3 behavior. But, if you disable the **control-point tcp-normalizer**, this prevents strict TCP checks, such as the detection of out-of-sequence segments and monitoring TCP options, on the TCP packets received on the Control Plane for Layer 7 inspection in the FWSM, and are not performed. Thus, it is advisable not to disable it. FWSM does not allow tuning in default tcp-map parameters.

## Q. Do we need to enable/disable TCP normalizer?

A. Due to the inability to pass some connection specific information from NPs to control plane, the TCP normalizer possibly does not function properly all the time in the FWSM. Additionally, unique tcp-maps associated with connections cannot be identified. Thus, the FWSM relies on the default tcp-map which possibly do not work correctly for all connections. Because of these limitations, there is a need to enable/disable TCP normalizer in the control plane for traffic going through the firewall. FWSM does not allow tuning in default tcp-map parameters.

## Q. What is the maximum number of mfib entries that a FWSM can support?

A. The maximum number of entries is 5000 entries.

## Q. What information is stored in the xlate entries in FWSM?

A. Xlate entries store this information:

1. **Source Interface** This is the interface that the packet is received, for example, `outside`.
2. **Source IP Address** This is the source IP address of the packet.
3. **Translated IP Address** In the case of no NAT statements, translated IP address and the source IP address are the same.
4. **Destination Interface** The interface that the packet leaves based on the routing table lookup of the destination IP address of the packet.

## Q. What do the values and statistics in `show perfmon` on FWSM imply?

A. Use the `show perfmon` command in order to capture information about the performance of the FWSM.

```
FWSM#show perfmon
FWSM#show console-output
Context: my_context
PERFMON STATS:      Current      Average
Xlates              0/s          0/s
Connections         0/s          0/s
TCP Conns           0/s          0/s
UDP Conns           0/s          0/s
URL Access          0/s          0/s
URL Server Req     0/s          0/s
WebSns Req         0/s          0/s
TCP Fixup           0/s          0/s
TCP Intercept      0/s          0/s
HTTP Fixup         0/s          0/s
FTP Fixup          0/s          0/s
AAA Authen         0/s          0/s
AAA Author         0/s          0/s
AAA Account        0/s          0/s
```

The column `Current` shows the statistics in the current interval, where as the last column `Average` shows the cumulative average since the last time statistics was cleared. It is shown as `/s` because it is the rate, rather than an absolute value.

The statistics shown in command output are updated at an interval of 120 seconds by default. The interval can be changed with the `perfmon interval` command.

```
FWSM#perfmon interval 20
```

It means that the rate of the statistics reported in the `Current` column are calculated every 20 seconds. In addition, whenever you enter the `show perfmon` command, the rates are calculated with the statistics at that point of time.

The FWSM does not include a serial console port, but some messages are only displayed on a console port, which includes output from the `show perfmon` and `perfmon` commands. Use the `show output-console` command in order to view the console buffer, which includes the `show perfmon` command output.

## Q. Will there be a performance hit on the FWSM with the `no monitor session servicemodule` command?

A. The span session is required on the FWSM because of a hardware limitation of an ASIC for traffic replication. FWSM needs an ASIC for packet replication and the span session passes the packets to switch for that using the span session. Traffic affected by this command is Distributed EtherChannel, Multicast and GRE. It is recommended to have the span session configured and not to remove it.

If for some reason you need to remove it, make sure that you do not have replicated nature traffic, for example, Distributed EtherChannel, that can be affected by the Field Notice: FN – 61935 – Catalyst 6500 Series and 7600 Series Service Module Incompatibility With Distributed EtherChannel and Packet Re-Circulation.

## Q. Can you increase memory in order to store more Access Control Lists (ACLs)?

A. Memory allocated for ACLs in FWSM is limited. Refer to Specifications – Rule Limits for more information on FWSM resource allocation.

When the memory allocated for ACLs in a context is exceeded, you get an error message similar to this:

```
ERROR: Unable to add, access-list config limit reached
```

Some access lists use more memory than others. It depends on the type of access list, and the actual limit the system can support is less than the maximum. The mapping between the rules and the memory allocation is not a one-to-one mapping. It actually depends on the rule and how it gets programmed in hardware.

You have two options for the optimization of the ACE memory usage:

- ◆ Summarize and simplify your ACE entries this can be done if you complete these recommended practices:
  1. Use contiguous hosts addresses whenever possible. Aggregate host statements in ACEs/object-groups into networks.
  2. Use any instead of networks, and networks instead of hosts when possible.
  3. Try to simplify object-groups. This can potentially save hundreds of ACEs when the ACLs are expanded. An example is to group together individual port statements into a range.
- ◆ Re-partition the memory allocated for ACE on each partition. This requires the reboot of the FWSM module.

The FWSM basically partitions the memory allocated for ACE into 12 partitions, and allocates corresponding memory for each. This is done automatically. From version 2.3(2) and later, you can use the resource manager to re-allocate the memory, which depends on the number of contexts you have.

Issue the **show context count** command in order to check how many contexts you have. You can then verify this with the configuration. Then find the number of partitions that use the **show resource acl-partition** command. If you have more partitions than your defined context, then you can match the number of partitions to the number of context with the **resource acl-partition number-of-partitions** command.

You need to save the configuration and reboot the FWSM after this. The previous command gives you more memory for the ACE, whether this is enough or not again depends on the ACE that you add to the context.



**Caution:** One drawback of the previous remapping is that if you want to add another context, then you have to reallocate the memory mapping again. This causes less memory available to each context and can break current ACE definitions. The memory on the FWSM allocated to is a finite amount and it carves it out accordingly on a predetermined manner or through manual resource allocation as mentioned previously.

## Q. How can I capture packets in FWSM?

A. Packets can be captured in FWSM. The use of CLI as Packet Capture is not supported in ASDM and the **capture** command is not supported in ASDM. Refer to Ignored and View-Only Commands for more information. Refer to Capturing Packets for more information on the configuration of the Packet Capturing in FWSM. Refer to ASA/PIX/FWSM: Packet Capturing using CLI and ASDM Configuration Example for more information on a packet capture configuration example.

## Q. Which version of ASDM does FWSM support?

A. Refer to FWSM and ASDM Release Compatibility for more information about FWSM and ASDM release compatibility.

## Q. Why does the capture command when applied to the FWSM stops and does not capture traffic as soon as another capture command is applied on the interface?

A. When you configure capture 'z' on the same interface where capture 'x' is already applied, then capture 'z' supercedes capture 'x'. The active capture is the last one attached to the particular interface.

The only exception is when the access-list on the capture 'x' overlaps with the access-list of the capture 'z'. If that is the case, then both captures continue to capture the traffic where the access-lists overlap.

## Q. Can I configure failover for three or more units of FWSM, which are spread over different switch chassis?

A. No. Failover setup is supported only for a pair of FWSM, for example, 2 units. These two units can be in a same switch or two separate switches. If you install the secondary FWSM in the same switch as the primary FWSM, you protect against module-level failure. In order to protect against module-level failure and as well as switch-level failure, you can install the secondary FWSM in a separate switch. FWSM does not coordinate failover directly with the switch, but it works harmoniously with the switch failover operation. Refer to Intra- and Inter-Chassis Module Placement for more information.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

|  |
|--|
| NetPro Discussion Forums – Featured Conversations for Security |
| Security: Intrusion Detection [Systems]                        |
| Security: AAA  |
| Security: General  |
| Security: Firewalling  |

## Related Information

- [FWSM Basic Configuration Example](#)
  - [Firewall Services Module Documentation](#)
  - [Firewall Services Module Product Support Page](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 26, 2008

Document ID: 46385

---