FWSM Basic Configuration Example

Document ID: 98591

Contents

Introduction

This document describes how to configure the basic configuration of the Firewall Services Module (FWSM) installed either in the Cisco 6500 Series Switches or Cisco 7600 Series Routers. This includes the configuration of the IP address, default routing, static and dynamic NATing, Access Control Lists (ACLs) statements in order to allow the desired traffic or block the unwanted traffic, application servers like Websense for the inspection of the internet traffic from the inside network, and the Webserver for the Internet users.

Note: In a FWSM High Availability (HA) scenario, the failover can only successfully sync when the license keys are exactly the same between the modules. Therefore, the failover cannot work between the FWSMs with different licenses.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Firewall Services Module that runs software version 3.1 and later

- Catalyst 6500 series switches, with the required components as shown:

    a. Supervisor engine with Cisco IOS® software, which is known as supervisor Cisco IOS, or Catalyst operating system (OS). See Table for supported supervisor engine and software releases.
    b. Multilayer Switch Feature Card (MSFC) 2 with Cisco IOS software. See Table for supported Cisco IOS software releases.

	Supervisor Engines[1]
Cisco IOS Software Release	
Cisco IOS Software Release 12.2(18)SXF and later	720, 32
Cisco IOS Software Release 12.2(18)SXF2 and later	2, 720, 32
Cisco IOS Software Modularity	
Cisco IOS Software Release 12.2(18)SXF4	720, 32
Catalyst OS[2]	
8.5(3) and later	2, 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 these supported Cisco IOS software releases on the MSFC. When you use Cisco IOS software on the supervisor, you use the same release on the MSFC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used for the Cisco 7600 series routers, with the required components as shown:

- Supervisor engine with Cisco IOS software. See Table for supported supervisor engine and Cisco IOS software releases.
- MSFC 2 with Cisco IOS software. See Table for supported Cisco IOS software releases.

Conventions

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

Background Information

The FWSM is a high−performance, space−saving, stateful firewall module that installs in the Catalyst 6500 series switches and the Cisco 7600 series routers.

Firewalls protect inside networks from unauthorized access by users on an outside network. The firewall can also protect inside networks from each other, for example, when you keep a human resources network separate from a user network. If you have network resources that need to be available to an outside user, such

as a web or FTP server, you can place these resources on a separate network behind the firewall, called a demilitarized zone (DMZ). The firewall allows limited access to the DMZ, but because the DMZ includes only the public servers, an attack there affects only the servers and does not affect the other inside networks. You can also control when inside users access outside networks, for example, access to the Internet, if you allow only certain addresses out, require authentication or authorization, or coordinate with an external URL filtering server.

The FWSM includes many advanced features, such as multiple security contexts that are similar to virtualized firewalls, transparent (Layer 2) firewall or routed (Layer 3) firewall operation, hundreds of interfaces, and many more features.

During the discussion of networks connected to a firewall, the outside network is in front of the firewall, the inside network is protected and behind the firewall, and a DMZ, while behind the firewall, allows limited access to outside users. Because the FWSM lets you configure many interfaces with varied security policies, which includes many inside interfaces, many DMZs, and even many outside interfaces if desired, these terms are used in a general sense only.

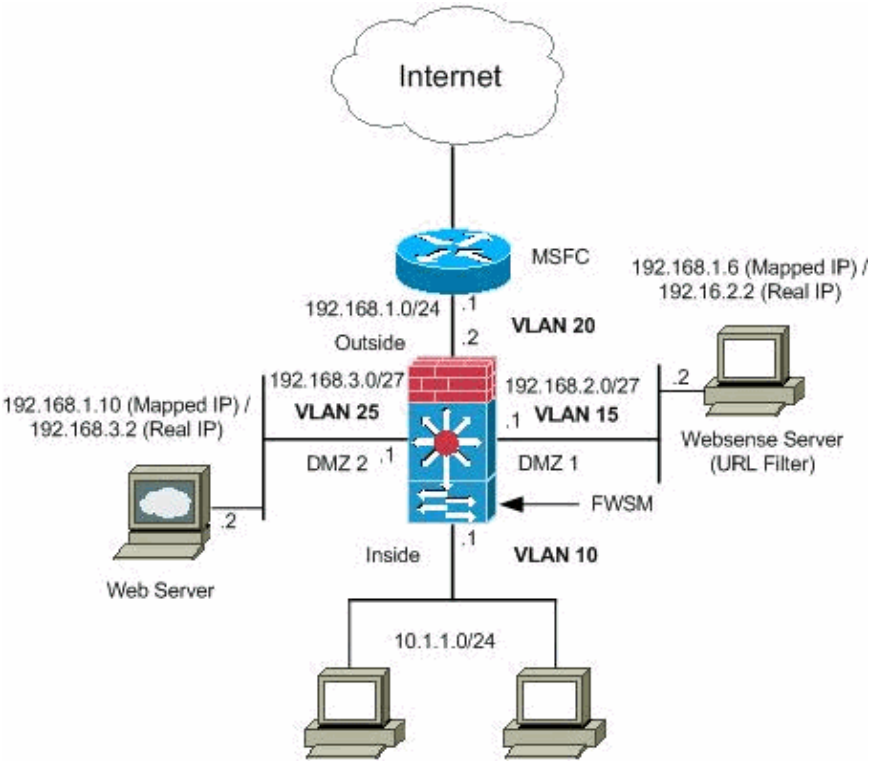
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses, which have been used in a lab environment.

Configurations

This document uses these configurations:

- Catalyst 6500 Series Switch Configuration
- FWSM Configuration

Catalyst 6500 Series Switch Configuration

1. 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 document as the **switch**.

   Note: You need to configure the switch appropriately before you configure FWSM.
2. **Assign VLANs to the Firewall Services Module** This section describes how to assign VLANs to the FWSM. The FWSM does not include any external physical interfaces. Instead, it uses VLAN interfaces. Assigning VLANs to the FWSM is similar to how you assign a VLAN to a switch port; the FWSM includes an internal interface to the Switch Fabric Module, if present, or the shared bus.

   Note: Refer to the Configuring VLANs section of the Catalyst 6500 Switches Software Configuration Guide for more information on how to create VLANs and assign it to switch ports.

   a. **VLAN Guidelines:**

      a. You can use private VLANs with the FWSM. Assign the primary VLAN to the FWSM; the FWSM automatically handles secondary VLAN traffic.
      b. You cannot use reserved VLANs.
      c. You cannot use VLAN 1.
      d. If you use FWSM failover within the same switch chassis, do not assign the VLAN(s) you reserved for failover and stateful communications to a switch port. But, if you use failover between chassis, you must include the VLANs in the trunk port between the chassis.
      e. If you do not add the VLANs to the switch before you assign them to the FWSM, the VLANs are stored in the supervisor engine database and are sent to the FWSM as soon as they are added to the switch.
      f. Assign VLANs to the FWSM before you assign them to the MSFC.

         VLANs that do not satisfy this condition are discarded from the range of VLANs that you attempt to assign on the FWSM.

   b. **Assign VLANs to the FWSM in Cisco IOS Software:**

      In Cisco IOS software, create up to 16 firewall VLAN groups, and then assign the groups to the FWSM. For example, you can assign all the VLANs to one group, or you can create an inside group and an outside group, or you can create a group for each customer. Each group can contain unlimited VLANs.

      You cannot assign the same VLAN to multiple firewall groups; however, you can assign multiple firewall groups to an FWSM and you can assign a single firewall group to multiple FWSMs. VLANs that you want to assign to multiple FWSMs, for example, can reside in a separate group from VLANs that are unique to each FWSM.

      a. Complete the steps in order to assign VLANs to the FWSM:

```
Router(config)#firewall vlan-group firewall_group vlan_range
```

The `vlan_range` can be one or more VLANs, for example, 2 to 1000 and from 1025 to 4094, identified as either a single number (n) like 5, 10, 15 or a range (n−x) like 5−10, 10−20.

Note: Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020−1100 range can already be in use.

Example:

```
firewall vlan-group 1 10,15,20,25
```

b. Complete the steps in order to assign the firewall groups to the FWSM.

```
Router(config)#firewall module module_number vlan-group firewall_group
```

The `firewall_group` is one or more group numbers as either a single number (n) like 5 or a range like 5−10.

Example:

```
firewall module 1 vlan-group 1
```

c. **Assign VLANs to the FWSM in Catalyst Operating System Software** In Catalyst OS software, you assign a list of VLANs to the FWSM. You can assign the same VLAN to multiple FWSMs if desired. The list can contain unlimited VLANs.

Complete the steps in order to assign VLANs to the FWSM.

```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```

The `vlan_list` can be one or more VLANs, for example, 2 to 1000 and from 1025 to 4094, identified as either a single number (n) like 5, 10, 15 or a range (n−x) like 5−10, 10−20.

3. **Add Switched Virtual Interfaces to the MSFC** A VLAN defined on the MSFC is called a switched virtual interface. If you assign the VLAN used for the SVI to the FWSM, then the MSFC routes between the FWSM and other Layer 3 VLANs.

   For security reasons, by default, only one SVI can exist between the MSFC and the FWSM. For example, if you misconfigure the system with multiple SVIs, you can accidentally allow traffic to pass around the FWSM if you assign both the inside and outside VLANs to the MSFC.

   Complete the steps in order to configure the SVI

```
Router(config)#interface vlan vlan_number
Router(config-if)#ip address address mask
```

Example:

```
interface vlan 20
ip address 192.168.1.1 255.255.255.0
```

Catalyst 6500 Series Switch Configuration

```
!--- Output Suppressed

firewall vlan-group 1 10,15,20,25
firewall module 1 vlan-group 1

interface vlan 20
```

```
ip address 192.168.1.1 255.255.255.0

!--- Output Suppressed
```

Note: Session in to the FWSM from the switch with the command appropriate for your switch operating system:

- Cisco IOS Software:

```
Router#session slot <number> processor 1
```

- Catalyst OS Software:

```
Console> (enable) session module_number
```

(Optional) Sharing VLANs with other Service modules If the switch has other service modules, for example, Application Control Engine (ACE), it is possible that you have to share some VLANs with these service modules. Refer to Service Module Design with ACE and FWSM for more information on how to optimize FWSM configuration when you work with such other modules.

FWSM Configuration

1. **Configure Interfaces for FWSM** Before you can allow traffic through the FWSM, you need to configure an interface name and an IP address. You should also change the security level from the default, which is 0. If you name an interface `inside`, and you do not set the security level explicitly, then the FWSM sets the security level to 100.

   Note: Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100, while the outside network connected to the Internet can be level 0. Other networks, such as DMZs, can be in between.

   You can add any VLAN ID to the configuration, but only VLANs, for example, 10, 15, 20 and 25, that are assigned to the FWSM by the switch can pass traffic. Use the **show vlan** command in order to view all VLANs assigned to the FWSM.

```
interface vlan 20
    nameif outside
    security-level 0
    ip address 192.168.1.2 255.255.255.0
interface vlan 10
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
interface vlan 15
    nameif dmz1
    security-level 60
    ip address 192.168.2.1 255.255.255.224
interface vlan 25
    nameif dmz2
    security-level 50
    ip address 192.168.3.1 255.255.255.224
```

   Tip: In the **nameif** <*name*> command, the *name* is a text string up to 48 characters and is not case−sensitive. You can change the name if you reenter this command with a new value. Do not enter the no form, because that command causes all commands that refer to that name to be deleted.
2. **Configure the Default route:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

A default route identifies the gateway IP address (192.168.1.1) to which FWSM sends all IP packets for which it does not have a learned or static route. A default route is simply a static route with 0.0.0.0/0 as the destination IP address. Routes that identify a specific destination take precedence over the default route.

3. **Dynamic NAT** translates a group of real addresses (10.1.1.0/24) to a pool of mapped addresses (192.168.1.20−192.168.1.50) that are routable on the destination network. The mapped pool can include fewer addresses than the real group. When a host you want to translate accesses the destination network, the FWSM assigns it an IP address from the mapped pool. The translation is added only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out.

```
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20−192.168.1.50 netmask 255.255.255.0
access−list Internet extended deny ip any 192.168.2.0 255.255.255.0
access−list Internet extended permit ip any any
access−group Internet in interface inside
```

You need to create an ACL in order to deny the traffic from the inside network 10.1.1.0/24 to go into DMZ1 network (192.168.2.0) and allow the other kinds of the traffic to the Internet through the application of the ACL *Internet* to the inside interface as inward direction for incoming traffic.

4. **Static NAT** creates a fixed translation of real address(es) to mapped address(es).With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host, if there is an access list that allows it.

   The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host, if there is an access list that allows it, while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.

```
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255
access−list outside extended permit tcp any host 192.168.1.10 eq http
access−list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanyw
access−list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanyw
access−list inbound extended permit udp any host 216.70.55.69 range 8766 30000
access−group outside in interface outside
```

   These are the two static NAT statements shown. The first one is meant to translate the real IP 192.168.2.2 on the inside interface to the mapped IP 192.168.1.6 on the outside subnet provided that the ACL allows the traffic from the source 192.168.1.30 to the mapped IP 192.168.1.6 in order to access the Websense server in the DMZ1 network. Similarly, the second static NAT statement meant to translate the real IP 192.168.3.2 on the inside interface to the mapped IP 192.168.1.10 on the outside subnet provided that the ACL allow the traffic from the Internet to the mapped IP 192.168.1.10 in order to access the Webserver in the DMZ2 network and have the udp port number in the range of 8766 to 30000.

5. The **url−server** command designates the server that runs the Websense URL filtering application. The limit is 16 URL servers in single context mode and four URL servers in multi mode, but you can use only one application, either N2H2 or Websense, at a time. Additionally, if you change your configuration on the security appliance, this does not update the configuration on the application server. This must be done separately, in accordance to the vendor instructions.

   The **url−server** command must be configured before you issue the **filter** command for HTTPS and

FTP. If all URL servers are removed from the server list, then all filter commands related to URL filtering are also removed.

Once you designate the server, enable the URL filtering service with the **filter url** command.

```
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1
```

The **filter url** command allows the prevention of access of outbound users from World Wide Web URLS that you designate with the Websense filtering application.

```
filter url http 10.1.1.0 255.255.255.0 0 0
```

FWSM Configuration

```
!--- Output Suppressed

interface vlan 20
    nameif outside
    security-level 0
    ip address 192.168.1.2 255.255.255.0
interface vlan 10
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
interface vlan 15
    nameif dmz1
    security-level 60
    ip address 192.168.2.1 255.255.255.224
interface vlan 25
    nameif dmz2
    security-level 50
    ip address 192.168.3.1 255.255.255.224
passwd fl0wer
enable password treeh0u$e
route outside 0 0 192.168.1.1 1
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections
url-cache dst 128
filter url http 10.1.1.0 255.255.255.0 0 0

!--- When inside users access an HTTP server, FWSM consults with a
!--- Websense server in order to determine if the traffic is allowed.

nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0

!--- Dynamic NAT for inside users that access the Internet

static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255

!--- A host on the subnet 192.168.1.0/24 requires access to the Websense
!--- server for management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.


static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255

!--- A host on the Internet requires access to the Webserver, so the Webserver
!--- uses a static translation for its private address.


access-list Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any
```

```
access-group Internet in interface inside

!--- Allows all inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1



access-list outside extended permit tcp any host 192.168.1.10 eq http

!--- Allows the traffic from the internet with the destination IP address
!--- 192.168.1.10 and destination port 80


access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-status


!--- Allows the management host 192.168.1.30 to use
!--- pcAnywhere on the Websense server


access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000


!--- Allows udp port number in the range of 8766 to 30000.


access-group outside in interface outside


access-list WEBSENSE extended permit tcp host 192.168.2.2 any eq http
access-group WEBSENSE in interface dmz1

!--- The Websense server needs to access the Websense
!--- updater server on the outside.
!--- Output Suppressed
```

Verify

Use this section in order to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

1. View the module information in accordance to your operating system in order to verify that the switch acknowledges the FWSM and has brought it online:

   - Cisco IOS Software:

     ```
     Router#show module
     Mod Ports Card Type                              Model              Serial No
     --- ----- -------------------------------------- ------------------ ----------
       1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD044409
       2   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD034756
       3    2  Intrusion Detection System             WS-X6381-IDS       SAD04250K
       4    6  Firewall Module                        WS-SVC-FWM-1       SAD062302
     ```

   - Catalyst OS Software:

     ```
     Console>show module [mod-num]
     The following is sample output from the show module command:
     ```

```
Console> show module
Mod Slot Ports Module-Type                Model               Sub Status
--- ---- ----- ------------------------ ------------------- --- ------
1   1    2     1000BaseX Supervisor     WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module          WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet       WS-X6408-GBIC       no  ok
```

Note: The **show module** command shows six ports for the FWSM. These are internal ports that are grouped together as an EtherChannel.

2.
```
Router#show firewall vlan-group
Group vlans
----- ------
   1 10,15,20
   51 70-85
   52 100
```

3.
```
Router#show firewall module
Module Vlan-groups
  5    1,51
  8    1,52
```

4. Enter the command for your operating system in order to view the current boot partition:

   - Cisco IOS Software:

     ```
     Router#show boot device [mod_num]
     ```

     Example:

     ```
     Router#show boot device
     [mod:1 ]:
     [mod:2 ]:
     [mod:3 ]:
     [mod:4 ]: cf:4
     [mod:5 ]: cf:4
     [mod:6 ]:
     [mod:7 ]: cf:4
     [mod:8 ]:
     [mod:9 ]:
     ```

   - Catalyst OS Software:

     ```
     Console> (enable) show boot device mod_num
     ```

     Example:

     ```
     Console> (enable) show boot device 6
     Device BOOT variable = cf:5
     ```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

1. **Setting the Default Boot Partition** By default, the FWSM boots from the **cf:4** application partition. But, you can choose to boot from the **cf:5** application partition or into the **cf:1** maintenance partition. In order to change the default boot partition, enter the command for your operating system:

   - Cisco IOS Software:

     ```
     Router(config)#boot device module mod_num cf:n
     ```

     Where n is 1 (maintenance), 4 (application), or 5 (application).

♦ Catalyst OS Software:

```
Console> (enable) set boot device cf:n mod_num
```

Where n is 1 (maintenance), 4 (application), or 5 (application).

2. **Resetting the FWSM in Cisco IOS Software** In order to reset the FWSM, enter the command as shown:

```
Router#hw-module module mod_num reset [cf:n] [mem-test-full]
```

The **cf:n** argument is the partition, either 1 (maintenance), 4 (application), or 5 (application). If you do not specify the partition, the default partition is used, which is typically **cf:4**.

The **mem−test−full** option runs a full memory test, which takes approximately six minutes.

Example:

```
Router#hw-mod module 9 reset
Proceed with reload of module? [confirm] y
% reset issued for module 9
Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

For **Catalyst OS** Software:

```
Console> (enable) reset mod_num [cf:n]
```

Where **cf:n** is the partition, either 1 (maintenance), 4 (application), or 5 (application). If you do not specify the partition, the default partition is used, which is typically **cf:4**.

Note: NTP cannot be configured on FWSM, because it takes its settings from the Switch.

Problem: Unable to pass the VLAN traffic from FWSM to the IPS Sensor 4270

You are unable to pass the traffic from FWSM to the IPS Sensors.

Solution

In order to force traffic through the IPS, the trick is to create an auxiliary VLAN in order to effectively break one of your current VLANs into two and then bridge them together. Check this example with VLAN 401 and 501 in order to clarify:

- If you want to scan traffic on main **VLAN 401**, create another vlan **VLAN 501** (auxillary VLAN). Then disable the VLAN interface 401, which the hosts in 401 currently use as their default gateway.
- Next enable VLAN 501 interface with the *same* address that you previously disabled on the VLAN 401 interface.
- Place one of the IPS interfaces in VLAN 401 and the other in VLAN 501.

All you have to do is to move the default gateway for VLAN 401 onto VLAN 501. You need to do the similar changes for VLANs if present. Note that VLANs are essentially like LAN segments. You can have a default gateway on a different piece of wire than the hosts that use it.

Out−Of−Order packets issue in FWSM

How can I solve the out−of−order packets issue in FWSM?

Solution

Issue the **sysopt np completion−unit** comand in global configuration mode in order to resolve the Out−Of−Order packet issue in FWSM. This command was introduced in FWSM Version 3.2(5) and ensures that packets are forwarded out in the same order they were received.

Problem: Unable to pass asymmetrically routed packets through the firewall

You are unable to pass asymmetrically routed packets through the firewall.

Solution

Issue the **set connection advanced−options tcp−state−bypass** command in class configuration mode in order to pass asymmetrically routed packets through the firewall. This command was introduced in FWSM Version 3.2(1).

Netflow support in FWSM

Does FWSM support Netflow?

Solution

Netflow is not supported in FWSM.

Related Information

- **Cisco Catalyst 6500 Series Firewall Services Module Support Page**
- **Cisco Catalyst 6500 Series Switches Support Page**
- **Cisco 7600 Series Router Support Page**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2009 − 2010 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Sep 05, 2007 Document ID: 98591