Ejemplo de Configuración Básica de un FWSM (Módulo de Servicios Firewall)

Contenido

Introducción

Este documento describe cómo realizar la configuración básica del Firewall Services Module (FWSM) instalado en switches Cisco de la serie 6500 o Cisco 7600 Series Routers. Esto incluye la configuración de la dirección IP, del ruteo predeterminado, del proceso de Traducción de Direcciones de Red (NAT) estática y dinámica, de las sentencias de las Listas de Control de Acceso (ACL) para permitir el tráfico deseado o bloquear el tráfico no deseado, de los servidores de aplicaciones como Websense para la inspección del tráfico de Internet desde la red interna y del Webserver para los usuarios de Internet.

Nota: En un escenario de alta disponibilidad (HA) del FWSM, la conmutación por falla solo puede sincronizarse correctamente cuando las claves de licencia son exactamente iguales entre los módulos. Por lo tanto, la conmutación por falla no puede funcionar entre los FWSM que tienen distintas licencias.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FWSM que ejecuta la versión de software 3.1 o posteriores.
- Switches Catalyst de la serie 6500 con los componentes necesarios que se muestran a continuación:

    a. Motor supervisor con software Cisco IOS®, conocido como supervisor Cisco IOS, o sistema operativo (OS) Catalyst. Consulte la Tabla para conocer las versiones compatibles de software y del motor supervisor.

    b. Multilayer Switch Feature Card (MSFC) 2 con el software Cisco IOS. Consulte la Tabla para conocer las versiones compatibles del software Cisco IOS.

	Supervisor Engines[1]
Versión de software del IOS de Cisco	
Versión 12.2(18)SXF y posterior del software Cisco IOS	720, 32
Versión12.2(18)SXF2 y posterior del software Cisco IOS	2, 720, 32
Modularidad de Cisco IOS Software	
Versión 12.2(18)SXF4 del software Cisco IOS	720, 32
Catalyst OS[2]	
8.5(3) y posterior	2, 720, 32

[1] El FWSM no admite el supervisor 1 o 1A.

[2]Cuando utiliza el Catalyst OS en el supervisor, puede recurrir a cualquiera de estas versiones compatibles del software Cisco IOS en la MSFC. Cuando utiliza el software Cisco IOS en el supervisor, debe utilizar la misma versión en la MSFC.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también puede utilizarse para Cisco 7600 Series Routers, con los componentes necesarios como se muestran a continuación:

- Motor supervisor con el software Cisco IOS. Consulte la Tabla para conocer las versiones compatibles del software Cisco IOS y del motor supervisor.
- MSFC 2 con el software Cisco IOS. Consulte la Tabla para conocer las versiones compatibles del software Cisco IOS.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El FWSM es un módulo de alto rendimiento que ahorra espacio y proporciona servicios de stateful-firewall (firewall de estado completo). Se instala en los switches Catalyst de la serie 6500 y Cisco 7600 Series Routers.

Los firewalls protegen las redes internas del acceso no autorizado por parte de usuarios de una red externa. El firewall también puede proteger las redes internas mutuamente, por ejemplo, si tiene una red de recursos humanos separada de una red de usuario. Si tiene recursos de red que deben estar disponibles para un usuario externo, tal como un servidor web o FTP, puede colocar estos recursos en otra red detrás del firewall, denominada zona perimetral (DMZ). El firewall permite acceso limitado a la DMZ, pero dado que la DMZ incluye solo los servidores públicos, un ataque allí afectaría solamente a los servidores y no a las demás redes internas. También se puede controlar cuándo los usuarios internos acceden a redes externas, por ejemplo, a Internet, si solo permite salir a ciertas direcciones, solicita autenticación o autorización, o coordina con un servidor de filtrado de direcciones URL externo.

El FWSM incluye varias características avanzadas, tales como contextos de seguridad múltiples que son similares a firewalls virtualizados, operación de firewall transparente (capa 2) o ruteado (capa 3), cientos de interfaces y muchas características más.

En la discusión de las redes conectadas a un firewall, la red externa está delante del firewall, la red interna está protegida y detrás del firewall, y una DMZ, si bien está detrás del firewall, permite acceso limitado a usuarios externos. Debido a que el FWSM permite configurar varias interfaces con diversas políticas de seguridad, incluidas varias interfaces internas, varias DMZ e incluso varias interfaces externas si se desea, estos términos se utilizan solo con un sentido general.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración del switch Catalyst de la serie 6500
- Configuración de FWSM

Configuración del switch Catalyst de la serie 6500

1. Puede instalar el FWSM en switches Catalyst de la serie 6500 o en Cisco 7600 Series Routers. La configuración de ambas series es idéntica y, en este documento, se hace referencia genéricamente a las series como el switch.

   Nota: Debe configurar correctamente el switch antes de configurar el FWSM.

2. Asignación de VLAN al Firewall Services Module: en esta sección, se describe cómo asignar VLAN al FWSM. El FWSM no incluye interfaces físicas externas. En su lugar, utiliza las interfaces de las VLAN. La asignación de VLAN al FWSM es similar a cómo se asigna una VLAN a un puerto de switch; el FWSM incluye una interfaz interna al módulo de estructura de switch, si está presente, o al bus compartido.

   Nota: Consulte la sección Configuración de VLAN de la Guía de Configuración del software de los switches Catalyst 6500 para obtener más información sobre cómo crear una VLAN y asignarla a los puertos de switch.

   a. Lineamientos de VLAN:

      a. Puede utilizar VLAN privadas con el FWSM. Asignar la VLAN principal al FWSM; el FWSM procesa automáticamente el tráfico de la VLAN secundaria.

      b. No puede utilizar VLAN reservadas.

c. No puede utilizar VLAN 1.

d. Si utiliza conmutación por falla del FWSM dentro del mismo chasis del switch, no asigne las VLAN que reservó para conmutación por falla y comunicaciones con estado a un puerto de switch. Sin embargo, si utiliza conmutación por falla entre chasis, debe incluir las VLAN en el puerto del enlace troncal entre ellos.

e. Si no agrega las VLAN al switch antes de asignarlas al FWSM, éstas se almacenan en la base de datos del motor supervisor y se envían al FWSM cuando se agregan al switch.

f. Asigne las VLAN al FWSM antes de asignarlas a la MSFC.

   Las VLAN que no cumplen con esta condición se descartan del rango de VLAN que intenta asignar al FWSM.

b. Asignación de VLAN al FWSM en el software Cisco IOS:

En el software Cisco IOS, cree hasta 16 grupos de VLAN de firewall y asigne los grupos al FWSM. Por ejemplo, puede asignar todas las VLAN a un grupo, puede crear un grupo interno y un grupo externo, o puede crear un grupo para cada cliente. Cada grupo puede contener una cantidad ilimitada de VLAN.

No puede asignar la misma VLAN a varios grupos de firewall; sin embargo, puede asignar varios grupos de firewall a un FWSM y puede asignar un solo grupo de firewall a varios FWSM. Las VLAN que desea asignar a varios FWSM, por ejemplo, pueden residir en un grupo distinto de las VLAN que son exclusivas de cada FWSM.

a. Complete los pasos para asignar las VLAN al FWSM.

<#root>

```
Router(config)#
```

firewall vlan-group firewall_group vlan_range

El `vlan_range` puede ser una o más VLAN, por ejemplo, de 2 a 1000 y de 1025 a 4094, identificadas con un solo número (n) como 5, 10, 15 o un rango (n-x) como 5-10, 10-20.

Nota: Los puertos enrutados y los puertos WAN utilizan las VLAN internas, de modo que es posible que las VLAN del rango 1020-1100 ya estén en uso.

Ejemplo:

<#root>

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

b. Complete los pasos para asignar los grupos de firewall al FWSM.

<#root>

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

El `firewall_group` es uno o más números de grupos con un solo número (n) como 5 o un rango como 5-10.

Ejemplo:

<#root>

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

c. Asignación de VLAN al FWSM en el software Catalyst Operating System: en el software Catalyst OS, debe asignar una lista de VLAN al FWSM. Puede asignar la misma VLAN a varios FWSM si lo desea. La lista puede contener una cantidad ilimitada de VLAN.

Complete los pasos para asignar las VLAN al FWSM.

<#root>

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

La `vlan_list` puede ser una o más VLAN, por ejemplo, de 2 a 1000 y de 1025 a 4094, identificadas con un solo número (n) como 5, 10, 15 o un rango (n-x) como 5-10, 10-20.

3. Incorporación de Interfaces Virtuales Conmutadas a la MSFC: una VLAN definida en la MSFC se denomina interfaz virtual conmutada (SVI). Si asigna la VLAN utilizada para la SVI al FWSM, la MSFC se enruta entre el FWSM y otras VLAN de capa 3.

Por razones de seguridad, de forma predeterminada, solo puede existir una SVI entre la MSFC y el FWSM. Por ejemplo, si configura erróneamente el sistema con varias SVI, puede permitir accidentalmente que el tráfico rodee el FWSM si asigna las VLAN internas y externas a la MSFC.

Complete los pasos para configurar la SVI.

<#root>

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

Ejemplo:

<#root>

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

Configuración del switch Catalyst de la serie 6500

`!--- 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`

Nota: Inicie sesión en el FWSM desde el switch con el comando correspondiente al sistema operativo de su switch:

- Software Cisco IOS:

<#root>

```
Router#
session slot
```

```
processor 1
```

- Software Catalyst OS:

  <#root>

  ```
  Console> (enable)
  ```

  session module_number

(Opcional) Uso compartido de VLAN con otros módulos de servicio: si el switch tiene otros módulos de servicio, por ejemplo, Application Control Engine (ACE), es posible que deba compartir algunas VLAN con estos módulos de servicio. Consulte Diseño de módulo de servicio con ACE y FWSM para obtener más información sobre cómo optimizar la configuración de FWSM cuando trabaja con estos otros módulos.

Configuración de FWSM

1. Configuración de interfaces para FWSM: para permitir que el tráfico pase por el FWSM, primero debe configurar un nombre de interfaz y una dirección IP. También debe cambiar el nivel de seguridad predeterminado, que es 0. Si asigna un nombre a una interfaz `inside`, y no establece el nivel de seguridad explícitamente, el FWSM establece el nivel de seguridad en 100.

   Nota: Cada interfaz debe tener un nivel de seguridad de 0 (más bajo) a 100 (más alto). Por ejemplo, debe asignar la red más segura, como la red host interna, al nivel 100, mientras que la red externa conectada a Internet puede ser del nivel 0. Otras redes, como las DMZ, pueden estar en el medio.

   Puede agregar cualquier ID de VLAN a la configuración, pero el tráfico solo puede pasar por las VLAN que el switch asigna al FWSM, por ejemplo, 10, 15, 20 y 25. Utilice el comando show vlan para ver todas las VLAN asignadas al FWSM.

   <#root>

   ```
   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
```

Consejo: En el comando nameif<name> , el name es una cadena de texto de hasta 48 caracteres y no distingue entre mayúsculas y minúsculas. Puede cambiar el nombre si vuelve a ingresar este comando con un valor nuevo. No ingrese la opción no, ya que ese comando hace que se eliminen todos los comandos que se refieren a ese nombre.

2. Configuración de la Ruta predeterminada:

<#root>

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Una ruta predeterminada identifica la dirección IP de la gateway (192.168.1.1) a la que el FWSM envía todos los paquetes IP de los cuales no tiene una ruta estática o aprendida. Una ruta predeterminada es simplemente una ruta estática con 0.0.0.0/0 como dirección IP de destino. Las rutas que identifican un destino específico tienen prioridad sobre la ruta predeterminada.

3. El NAT dinámico traduce un grupo de direcciones reales (10.1.1.0/24) a un grupo de direcciones mapeadas (192.168.1.20-192.168.1.50) que son enrutables en la red de destino. El grupo mapeado puede incluir menos direcciones que el grupo real. Cuando un host que usted desea traducir accede a la red de destino, el FWSM le asigna una dirección IP del grupo mapeado. La traducción se agrega solo cuando el host real inicia la conexión. La traducción existe solo mientras dura la conexión, y un usuario determinado no conserva la misma dirección IP después de que se agota el tiempo de espera de la traducción.

<#root>

```
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
```

Debe crear una ACL para impedir que el tráfico de la red interna 10.1.1.0/24 pase a la red DMZ1 (192.168.2.0) y permitir los otros tipos de tráfico a Internet a través de la aplicación de la ACL Internet a la interfaz interna en dirección entrante para el tráfico entrante.

4. El NAT estático crea una traducción fija de una dirección real a una dirección mapeada. Con

el NAT dinámico y la Traducción de Direcciones de Puertos (PAT), cada host utiliza una dirección o un puerto diferente para cada traducción subsecuente. Debido a que la dirección mapeada es la misma para cada conexión consecutiva con el NAT estático, y existe una regla de traducción que persiste, el NAT estático permite que los hosts de la red de destino inicien el tráfico hacia un host traducido, si hay una lista de acceso que lo permita.

La principal diferencia entre el NAT dinámico y un rango de direcciones para NAT estático es que el NAT estático permite a un host remoto iniciar una conexión con un host traducido, siempre que exista una lista de acceso que lo permita, mientras que el NAT dinámico no lo permite. También necesita un número equivalente de direcciones mapeadas como direcciones reales con NAT estático.


```
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 pcanywhere-data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-status
access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000
access-group outside in interface outside
```

Estas son las dos sentencias de NAT estático que se muestran. La primera se utiliza para traducir la IP real 192.168.2.2 de la interfaz interna a la IP mapeada 192.168.1.6 de la subred externa, siempre que la ACL permita el tráfico de la IP de origen 192.168.1.30 a la IP mapeada 192.168.1.6 para acceder al servidor Websense en la red DMZ1. Del mismo modo, la segunda sentencia de NAT estático se utiliza para traducir la IP real 192.168.3.2 de la interfaz interna a la IP mapeada 192.168.1.10 de la subred externa, siempre que la ACL permita el tráfico de Internet a la IP mapeada 192.168.1.10 para acceder al Webserver en la red DMZ2 y tener el número de puerto udp en el rango de 8766 a 30000.

5. El comando url-server designa el servidor que ejecuta la aplicación de filtrado de URL Websense. El límite es de 16 servidores URL en el modo de contexto único y de 4 servidores URL en el modo múltiple, pero solo puede utilizar una aplicación a la vez, ya sea N2H2 o Websense. Además, si cambia la configuración en el dispositivo de seguridad, no se actualizará la configuración en el servidor de aplicaciones. Esto debe hacerse por separado, según las instrucciones del proveedor.

   El comando url-server debe configurarse antes de ejecutar el comando filter para HTTPS y FTP. Si se eliminan todos los servidores URL de la lista de servidores, también se eliminan todos los comandos de filtrado relacionados con el filtrado de URL.

   Una vez que designó el servidor, habilite el servicio de filtrado de URL con el comando filter url.

```
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5
```

El comando filter url permite impedir el acceso de usuarios de salida de las direcciones URL de la World Wide Web que usted designe con la aplicación de filtrado Websense.

<#root>

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

Configuración d

```
!--- 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 5
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 de

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 tha


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 trans
```

```
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



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 destina


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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

1. Vea la información del módulo de acuerdo con su sistema operativo para verificar que el switch reconoce el FWSM y lo ha puesto en línea:

    - Software Cisco IOS:

      <#root>

      Router#

      show module

      Mod Ports Card Type   Model   Serial No.

```
--- ----- ------------------------------------ ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
  2   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
  3    2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5


 4    6  Firewall Module                        WS-SVC-FWM-1       SAD062302U4
```

- Software Catalyst OS:

<#root>

```
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
```

Nota: El comando show module muestra seis puertos para el FWSM. Estos son puertos internos que están agrupados como un EtherChannel.

2.

<#root>

```
Router#

show firewall vlan-group

Group vlans
----- ------
   1 10,15,20
   51 70-85
   52 100
```

3.

<#root>

```
Router#

show firewall module

Module Vlan-groups
  5    1,51
  8    1,52
```

4. Ingrese el comando de su sistema operativo para ver la partición de arranque actual:

- Software Cisco IOS:

  <#root>

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

  Ejemplo:

  <#root>

  ```
  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 ]:
  ```

- Software Catalyst OS:

  <#root>

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

  Ejemplo:

  <#root>

  ```
  Console> (enable)
  show boot device 6

  Device BOOT variable = cf:5
  ```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

1. Configuración de la Partición de arranque predeterminada: de forma predeterminada, el FWSM arranca desde la partición de aplicación cf:4. No obstante, puede optar por arrancarlo desde la partición de aplicación cf:5 o en la partición de mantenimiento cf:1. Para cambiar la partición de arranque predeterminada, ingrese el comando de su sistema operativo:

    - Software Cisco IOS:

      <#root>

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

      Donde n es 1 (mantenimiento), 4 (aplicación) o 5 (aplicación).

    - Software Catalyst OS:

      <#root>

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

      Donde n es 1 (mantenimiento), 4 (aplicación) o 5 (aplicación).

2. Reinicio del FWSM en el software Cisco IOS: para reiniciar el FWSM, ingrese el comando como se muestra a continuación:

   <#root>

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

   El argumento cf:n es la partición, ya sea 1 (mantenimiento), 4 (aplicación) o 5 (aplicación). Si no especifica la partición, se utiliza la partición predeterminada, que generalmente es cf:4.

   La opción mem-test-full ejecuta una prueba de memoria completa, que dura aproximadamente seis minutos.

Ejemplo:

<#root>

```
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 ...
```

Para el software Catalyst OS:

<#root>

```
Console> (enable)
```

reset mod_num [cf:n]

Donde cf:n es la partición, ya sea 1 (mantenimiento), 4 (aplicación) o 5 (aplicación). Si no especifica la partición, se utiliza la partición predeterminada, que generalmente es cf:4.

Nota: En FWSM, no se puede configurar el Network Time Protocol (NTP), ya que toma su configuración del switch.

Problema: No se puede pasar el tráfico de VLAN de FWSM al sensor IPS 4270

No puede pasar el tráfico de FWSM a los sensores IPS.

Solución

Para forzar el tráfico a través del IPS, el truco consiste en crear una VLAN auxiliar para dividir efectivamente una de sus VLAN actuales en dos y luego unirlas. Verifique este ejemplo con VLAN 401 y 501 para aclarar:

- Si desea analizar el tráfico en la VLAN 401 principal, cree otra VLAN, la VLAN 501 (VLAN auxiliar). Luego, deshabilite la interfaz VLAN 401, que los hosts en 401 utilizan actualmente como gateway predeterminado.
- A continuación, habilite la interfaz VLAN 501 con la misma dirección que deshabilitó anteriormente en la interfaz VLAN 401.
- Coloque una de las interfaces IPS en la VLAN 401 y la otra en la VLAN 501.

Todo lo que tiene que hacer es mover el gateway predeterminado para la VLAN 401 a la VLAN

501. Necesita hacer los cambios similares para las VLAN si están presentes. Tenga en cuenta que las VLAN son esencialmente segmentos de LAN. Puede tener un gateway predeterminado en un cable diferente de los hosts que lo utilizan.

Problema de paquetes fuera de orden en FWSM

¿Cómo puedo resolver el problema de paquetes fuera de orden en FWSM?

Solución

Emita el comando sysopt np completion-unit en el modo de configuración global para resolver el problema de paquetes fuera de orden en FWSM. Este comando se introdujo en la versión 3.2(5) de FWSM y garantiza que los paquetes se reenvíen en el mismo orden en que se recibieron.

Problema: No se pueden pasar paquetes enrutados asimétricamente a través del firewall

No puede pasar paquetes enrutados asimétricamente a través del firewall.

Solución

Emita el comando set connection advanced-options tcp-state-bypass en el modo de configuración de clase para pasar paquetes enrutados asimétricamente a través del firewall. Este comando se introdujo en la versión 3.2 (1) de FWSM.

Compatibilidad de Netflow en FWSM

¿FWSM admite Netflow?

Solución

Netflow no se admite en FWSM.

Información Relacionada

- Página de soporte de Cisco Catalyst 6500 Series Firewall Services Module
- Página de soporte de switches Cisco Catalyst de la serie 6500
- Página de soporte de Cisco 7600 Series Router
- Intercepción de FWSM TCP y cookies SYN explicadas
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).