Ejemplo de Configuración Básica de FWSM

Contenido

Introducción

Este documento describe cómo configurar la configuración básica del Firewall Services Module (FWSM) instalado en los Cisco 6500 Series Switches o en los Cisco 7600 Series Routers. Esto incluye la configuración de la dirección IP, el routing predeterminado, las declaraciones NATing estáticas y dinámicas, las listas de control de acceso (ACL) para permitir el tráfico deseado o bloquear el tráfico no deseado, los servidores de aplicaciones como Websense para la inspección del tráfico de Internet desde la red interna y el servidor web para los usuarios de Internet.

Nota: En un escenario de alta disponibilidad (HA) de FWSM, la conmutación por fallo sólo puede sincronizarse correctamente cuando las claves de licencia son exactamente las mismas entre los módulos. Por lo tanto, el failover no puede funcionar entre los FWSM con licencias diferentes.

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.

- Firewall Services Module que ejecuta la versión de software 3.1 y posteriores
- Catalyst 6500 Series Switches, con los componentes necesarios como se muestra:Supervisor Engine con el software Cisco IOS®, conocido como Supervisor Cisco IOS o sistema operativo Catalyst (OS). Consulte la Tabla para ver las versiones de Supervisor Engine y Software soportadas.Tarjeta de función de switch multicapa (MSFC) 2 con el software Cisco IOS. Consulte Tabla para ver las versiones de software de Cisco IOS soportadas.

[1] El FWSM no soporta al supervisor 1 o 1A.

[2] Cuando utiliza Catalyst OS en el supervisor, puede utilizar cualquiera de estas versiones de Cisco IOS Software soportadas en la MSFC. Cuando utiliza Cisco IOS Software en el supervisor, utiliza la misma versión en la 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.

Productos Relacionados

Esta configuración también se puede utilizar para los Cisco 7600 Series Routers, con los componentes requeridos como se muestra:

- Supervisor Engine con Cisco IOS Software. Consulte la Tabla para ver las versiones de Supervisor Engine y Cisco IOS Software soportadas.
- MSFC 2 con Cisco IOS Software. Consulte la Tabla para ver las versiones de Cisco IOS Software soportadas.

Convenciones

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

Antecedentes

El FWSM es un módulo de firewall de alto rendimiento, que ahorra espacio y con estado que se instala en los switches Catalyst serie 6500 y en los routers Cisco serie 7600.

Los firewalls protegen las redes internas del acceso no autorizado de los usuarios en una red externa. El firewall también puede proteger las redes internas entre sí, por ejemplo, cuando mantiene una red de recursos humanos separada de una red de usuario. Si tiene recursos de red que necesitan estar disponibles para un usuario externo, como un servidor web o FTP, puede colocar estos recursos en una red independiente detrás del firewall, denominada zona desmilitarizada (DMZ). El firewall permite un acceso limitado a la DMZ, pero como la DMZ sólo

incluye los servidores públicos, un ataque afecta solamente a los servidores y no afecta a las otras redes internas. También puede controlar cuando los usuarios internos acceden a redes externas, por ejemplo, el acceso a Internet, si sólo permite el acceso a determinadas direcciones, requiere autenticación o autorización, o se coordina con un servidor de filtrado de URL externo.

El FWSM incluye muchas funciones avanzadas, como varios contextos de seguridad similares a los firewalls virtualizados, firewall transparente (capa 2) o funcionamiento de firewall enrutado (capa 3), cientos de interfaces y muchas otras funciones.

Durante el debate sobre las redes conectadas a un firewall, la red externa se encuentra frente al firewall, la red interna está protegida y detrás del firewall, y una DMZ, mientras se encuentra detrás del firewall, permite un acceso limitado a los usuarios externos. Debido a que el FWSM le permite configurar muchas interfaces con diversas políticas de seguridad, que incluyen muchas interfaces internas, muchas DMZ e incluso muchas interfaces externas si lo desea, estos términos se utilizan en un sentido general solamente.

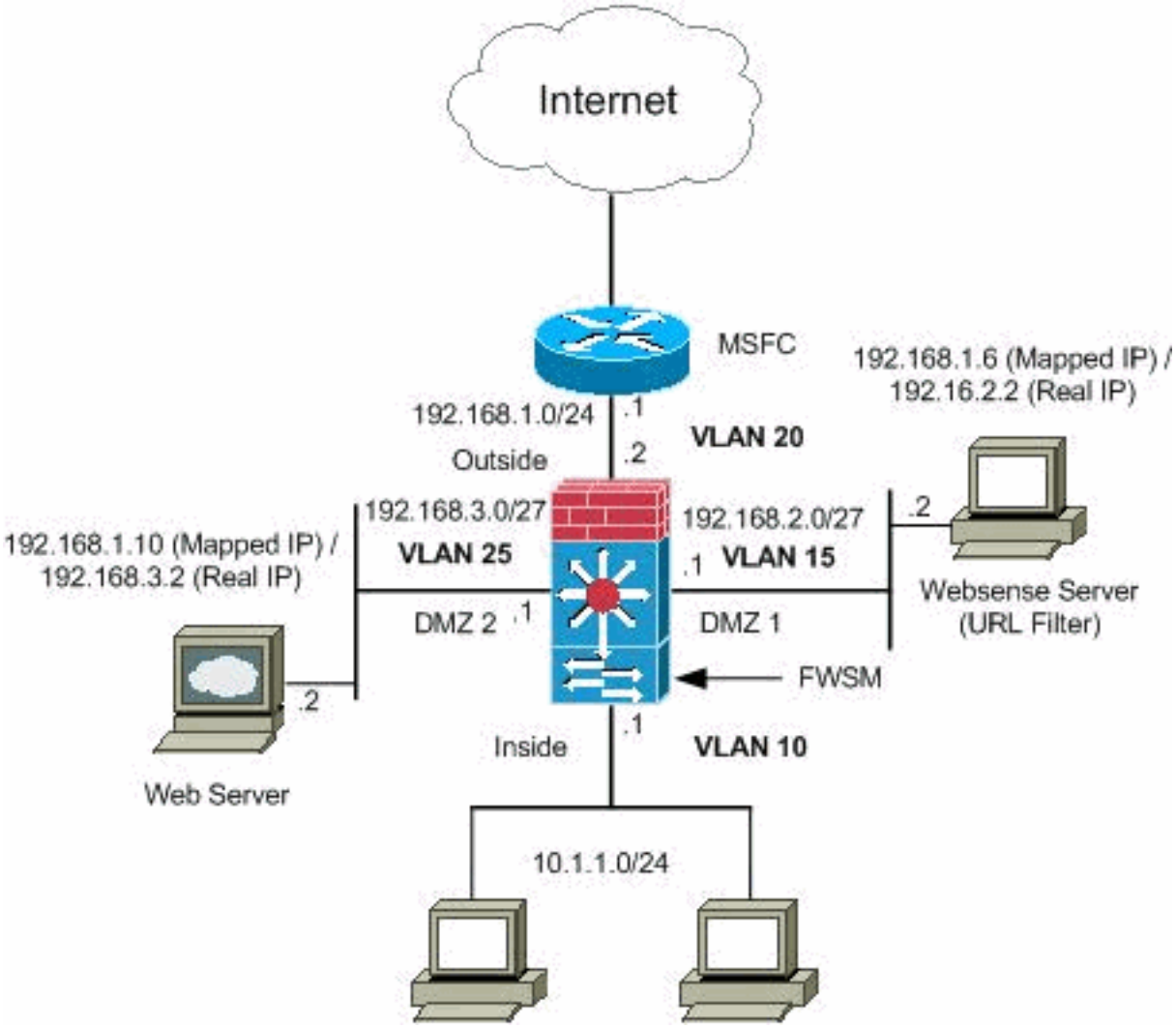
Configurar

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 utilizados 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 serie 6500
- Configuración de FWSM

Configuración del switch Catalyst serie 6500

1. Puede instalar el FWSM en los Catalyst 6500 Series Switches o en los Cisco 7600 Series Routers. La configuración de ambas series es idéntica y en este documento se hace referencia genérica a las series como el **switch**.**Nota:** Debe configurar el switch adecuadamente antes de configurar FWSM.
2. **Asignar VLAN al Módulo de servicios de firewall**: esta sección describe cómo asignar VLAN al FWSM. El FWSM no incluye ninguna interfaz física externa. En su lugar, utiliza interfaces VLAN. La asignación de VLAN al FWSM es similar a la asignación de una VLAN a un puerto de switch; el FWSM incluye una interfaz interna al módulo de entramado de switches, si está presente, o al bus compartido.**Nota:** Refiérase a la sección Configuración de VLAN de la

Guía de Configuración de Software de Catalyst 6500 Switches para obtener más información sobre cómo crear VLAN y asignarlas a los puertos del switch.**Pautas de VLAN:**Puede utilizar VLAN privadas con el FWSM. Asigne la VLAN principal al FWSM; el FWSM administra automáticamente el tráfico VLAN secundario.No puede utilizar VLAN reservadas.No puede utilizar VLAN 1.Si utiliza la conmutación por fallas de FWSM dentro del mismo chasis del switch, no asigne las VLAN que reservó para la conmutación por fallas y las comunicaciones con estado a un puerto del switch. Pero, si utiliza la conmutación por fallas entre chasis, debe incluir las VLAN en el puerto trunk entre el chasis.Si no agrega las VLAN al switch antes de asignarlas al FWSM, las VLAN se almacenan en la base de datos del Supervisor Engine y se envían al FWSM tan pronto como se agregan al switch.Asigne VLAN al FWSM antes de asignarlas a la MSFC.Las VLAN que no satisfacen esta condición se descartan del rango de VLAN que intenta asignar en el FWSM.**Asignación de VLAN al FWSM en Cisco IOS Software:**En Cisco IOS Software, cree hasta 16 grupos de VLAN de firewall y luego asigne los grupos al FWSM. Por ejemplo, puede asignar todas las VLAN a un grupo, o puede crear un grupo interno y un grupo externo, o puede crear un grupo para cada cliente. Cada grupo puede contener VLAN ilimitadas.No puede asignar la misma VLAN a varios grupos de firewall; sin embargo, puede asignar varios grupos de firewall a un FWSM y asignar un único grupo de firewall a varios FWSM. Las VLAN que desea asignar a varios FWSM, por ejemplo, pueden residir en un grupo separado de las VLAN que son únicas para cada FWSM.Complete los pasos para asignar las VLAN al FWSM:

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

`vlan_range` puede ser una o más VLAN, por ejemplo, de 2 a 1000 y de 1025 a 4094, identificadas como un único número (n) como 5, 10, 15 o un rango (n-x) como 5-10, 10-20.**Nota:** Los puertos enrutados y los puertos WAN consumen VLAN internas, por lo que es posible que las VLAN del rango 1020-1100 ya puedan estar en uso.**Ejemplo:**

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

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

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

El `firewall_group` es uno o varios números de grupo como un único número (n) como 5 o un rango como 5-10.**Ejemplo:**

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

Asigne VLAN al FWSM en Catalyst Operating System Software: en el software Catalyst OS, asigne una lista de VLAN al FWSM. Si lo desea, puede asignar la misma VLAN a varios FWSM. La lista puede contener VLAN ilimitadas.Complete los pasos para asignar las VLAN al FWSM.

```
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 como un único número (n) como 5, 10, 15 o un rango (n-x) como 5-10, 10-20.

3. **Agregar interfaces virtuales conmutadas a la MSFC**: una VLAN definida en la MSFC se denomina interfaz virtual conmutada. Si asigna la VLAN utilizada para la SVI al FWSM, entonces la MSFC rutea entre el FWSM y otras VLAN de Capa 3.Por razones de seguridad, de forma predeterminada, sólo puede existir una SVI entre la MSFC y el FWSM. Por

ejemplo, si configura mal el sistema con varias SVI, puede permitir accidentalmente que el tráfico pase alrededor del FWSM si asigna las VLAN internas y externas a la MSFC.Complete los pasos para configurar el SVI

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

Ejemplo:

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

Configuración del switch Catalyst 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: Sesión en el FWSM desde el switch con el comando apropiado para su sistema operativo del switch:

- Software Cisco IOS:
  ```
  Router#session slot
  ```

- Software Catalyst OS:
  ```
  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 tenga que compartir algunas VLAN con estos módulos de servicio. Refiérase a Diseño de Módulo de Servicio con ACE y FWSM para obtener más información sobre cómo optimizar la configuración de FWSM cuando trabaja con tales módulos.

Configuración de FWSM

1. **Configurar interfaces para FWSM**: antes de permitir el tráfico a través del FWSM, debe configurar un nombre de interfaz y una dirección IP. También debe cambiar el nivel de seguridad del valor predeterminado, que es 0. Si nombra una interfaz `interna` 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 entre 0 (el más bajo) y 100 (el 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 el nivel 0. Otras redes, como las DMZ, pueden encontrarse en el medio intermedio.Puede agregar cualquier ID de VLAN a la configuración, pero sólo las VLAN, por ejemplo, 10, 15, 20 y 25, que están asignadas al FWSM por el switch pueden pasar tráfico. Utilice el comando **show vlan** para ver todas las VLAN asignadas al 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
```

Sugerencia: En el comando **nameif *<name>*** , el *nombre* **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 nuevo valor. No ingrese el comando no, porque ese comando hace que se eliminen todos los comandos que hacen referencia a ese nombre.

2. **Configure la ruta predeterminada:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Una ruta predeterminada identifica la dirección IP del gateway (192.168.1.1) a la que FWSM envía todos los paquetes IP para los que no tiene una ruta aprendida o estática. 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. **La NAT dinámica** traduce un grupo de direcciones reales (10.1.1.0/24) a un conjunto de direcciones asignadas (192.168.1.20-192.168.1.50) que son enrutables en la red de destino. El conjunto asignado puede incluir menos direcciones que el grupo real. Cuando un host que desea traducir accede a la red de destino, el FWSM le asigna una dirección IP del conjunto asignado. La traducción se agrega solamente cuando el host real inicia la conexión. La traducción sólo está en vigor durante la duración de la conexión y un usuario determinado no conserva la misma dirección IP después de que se agote el tiempo de traducción.

```
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 denegar el tráfico de la red interna 10.1.1.0/24 para ir a la red DMZ1 (192.168.2.0) y permitir los otros tipos de tráfico a Internet a través de la aplicación de la *Internet* ACL a la interfaz interna como dirección entrante para el tráfico entrante.

4. **La NAT estática** crea una traducción fija de direcciones reales a direcciones asignadas.Con NAT dinámica y PAT, cada host utiliza una dirección o puerto diferente para cada traducción posterior. Debido a que la dirección asignada es la misma para cada conexión consecutiva con NAT estática y existe una regla de traducción persistente, la NAT estática permite que los hosts en la red de destino inicien el tráfico a un host traducido, si hay una lista de acceso que lo permita.La diferencia principal entre NAT dinámica y un rango de direcciones para

NAT estática es que NAT estática permite que un host remoto inicie una conexión con un host traducido, si hay una lista de acceso que lo permite, mientras que NAT dinámica no. También necesita un número igual de direcciones asignadas como direcciones reales con NAT estática.

```
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 NAT estáticas mostradas. La primera pretende traducir la IP real 192.168.2.2 en la interfaz interna a la IP 192.168.1.6 asignada en la subred externa siempre que la ACL permita el tráfico desde el origen 192.168.1.30 a la IP 192.168.1.6 asignada en orden para acceder al servidor de Websense en la red DMZ1. De manera similar, la segunda sentencia NAT estática pretendía traducir la IP real 192.168.3.2 en la interfaz interna a la IP 192.168.1.10 asignada en la subred externa siempre que la ACL permita el tráfico de Internet a la IP asignada 192.168.1.10 para acceder al servidor web en la Z2 y tenga 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 de Websense. El límite es de 16 servidores URL en modo de contexto único y cuatro servidores URL en modo múltiple, pero sólo puede utilizar una aplicación, ya sea N2H2 o Websense, a la vez. Además, si cambia la configuración en el dispositivo de seguridad, esto no actualiza la configuración en el servidor de aplicaciones. Esto debe hacerse por separado, de conformidad con las instrucciones del proveedor.El comando **url-server** debe configurarse antes de ejecutar el comando **filter** para HTTPS y FTP. Si todos los servidores URL se quitan de la lista de servidores, también se quitarán todos los comandos de filtrado relacionados con el filtrado de URL.Una vez designado 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 la prevención del acceso de usuarios salientes de URL de World Wide Web que designe con la aplicación de filtrado de Websense.

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

Configuración de FWSM
!--- 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 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
```

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. Consulte 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:

```
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:

```
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 se agrupan como 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. Ingrese el comando para su sistema operativo para ver la partición de inicio actual:Software Cisco IOS:
```
Router#show boot device [mod_num]
```

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

Ejemplo:
```
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 inicio predeterminada**: de forma predeterminada, el FWSM se inicia desde la partición de aplicación **cf:4**. Sin embargo, puede optar por arrancar desde la partición de aplicación **cf:5** o en la partición de mantenimiento **cf:1**. Para cambiar la partición de inicio predeterminada, ingrese el comando para su sistema operativo:Software

Cisco IOS:

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

Si n es 1 (mantenimiento), 4 (solicitud) o 5 (solicitud).Software Catalyst OS:

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

Si n es 1 (mantenimiento), 4 (solicitud) o 5 (solicitud).

2. **Restablecimiento del FWSM en el Cisco IOS Software**: para reiniciar el FWSM, ingrese el comando como se muestra:

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

El argumento **cf:n** es la partición 1 (mantenimiento), 4 (aplicación) o 5 (aplicación). Si no especifica la partición, se utiliza la partición predeterminada, que normalmente es **cf:4**.La opción **mem-test-full** ejecuta una prueba de memoria completa, que toma aproximadamente seis minutos.**Ejemplo:**

```
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**:

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

Cuando **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 normalmente es **cf:4**.

Nota: NTP no se puede configurar en FWSM porque toma sus parámetros del switch.

Problema: No se puede pasar el tráfico 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 es crear una VLAN auxiliar para romper 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 501** de VLAN (VLAN automática). A continuación, inhabilite la interfaz VLAN 401, que los hosts en 401 utilizan actualmente como su gateway predeterminado.
- A continuación, habilite la interfaz VLAN 501 con la *misma* dirección que desactivó 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 VLAN 401 a VLAN 501. Debe hacer los cambios similares para las VLAN si están presentes. Tenga en cuenta que las VLAN son esencialmente como segmentos LAN. Puede tener un gateway predeterminado en un pedazo de cable diferente que los hosts que lo utilizan.

Envío de paquetes fuera de servicio en FWSM

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

Solución

Ejecute el comando sysopt np complete-unit en el modo de configuración global para resolver el problema del paquete Out-Of-Order en FWSM. Este comando se introdujo en la versión 3.2(5) de FWSM y asegura 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

Ejecute 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 con Netflow en FWSM

¿FWSM admite Netflow?

Solución

Netflow no es compatible con FWSM.

Información Relacionada

- Página de soporte del módulo de servicios de firewall Cisco Catalyst serie 6500
- Página de soporte de switches Catalyst de Cisco serie 6500
- Página de Soporte del Cisco 7600 Series Router
- Explicación de la intercepción TCP de FWSM y las cookies SYN
- Soporte Técnico y Documentación - Cisco Systems