Ejemplo de la configuración básica FWSM

Contenido

Introducción

Este documento describe cómo configurar la configuración básica del Módulo de servicios del Firewall (FWSM) instaló en los Cisco 6500 Series Switch o los Cisco 7600 Series Router. Esto incluye la configuración de la dirección IP, del ruteo predeterminado, de las declaraciones estáticas y dinámicas del NATing, del Listas de control de acceso (ACL) para permitir el tráfico deseado o bloquear el tráfico no deseado, de los servidores de aplicaciones como el Websense para el examen del tráfico de Internet de la red interna, y del web server para los usuarios de Internet.

Nota: En un escenario de gran disponibilidad FWSM (HA), la Conmutación por falla puede sincronizar solamente con éxito cuando las llaves de la licencia son exactamente lo mismo entre los módulos. Por lo tanto, la Conmutación por falla no puede trabajar entre los FWSM con diversas licencias.

prerrequisitos

Requisitos

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.

- Módulo de servicios del Firewall que funciona con la versión de software 3.1 y posterior
- Catalyst 6500 Series Switch, con los componentes requeridos como se muestra:Supervisor Engine con el software del ® del Cisco IOS, que se conoce como Cisco IOS del supervisor, o el Catalyst Operating System (OS). Vea la tabla para el motor y las versiones de software del supervisor admitido.(MSFC) 2 de la Multilayer Switch Feature Card con el Cisco IOS Software. Vea la tabla para las versiones de Cisco IOS Software soportadas.

1 El FWSM no soporta el Supervisor 1 o el 1A.

2When que usted utiliza el Catalyst OS en el supervisor, usted puede utilizar ninguno de estos versiones de Cisco IOS Software soportadas en el MSFC. Cuando usted utiliza el Cisco IOS Software en el supervisor, usted utiliza la misma versión en el 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

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

- Supervisor Engine con el Cisco IOS Software. Vea la tabla para el motor y las versiones de Cisco IOS Software del supervisor admitido.
- MSFC2 con el Cisco IOS Software. Vea la tabla para 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 de alto rendimiento, ahorro de espacio, el módulo del escudo de protección con estado que instala en los Catalyst 6500 Series Switch y los Cisco 7600 Series Router.

Los Firewall protegen las redes internas contra el acceso no autorizado de los usuarios en una red externa. El Firewall puede también proteger las redes internas contra uno a, por ejemplo, cuando usted guarda una red de los Recursos Humanos a parte de una red de usuario. Si usted

tiene los recursos de red que necesitan estar disponibles para un usuario externo, tal como una red o un servidor FTP, usted puede poner estos recursos en una red separada detrás del Firewall, llamado una zona desmilitarizada (DMZ). El Firewall permite el acceso limitado al DMZ, pero porque el DMZ incluye solamente los servidores públicos, un ataque allí afecta solamente a los servidores y no afecta a las otras redes internas. Usted puede también controlar cuando las redes externas interiores del acceso de usuarios, por ejemplo, el acceso a Internet, si usted permite solamente ciertos direccionamientos hacia fuera, requiere la autenticación o la autorización, o coordina con un servidor externo del Filtrado de URL.

El FWSM incluye muchas funciones avanzadas, tales como contextos de seguridad múltiples que sean similares a los Firewall virtualizados, transparentes (Firewall de la capa 2) o ruteado (operación del Firewall de la capa 3), los centenares de interfaces, y muchas más características.

Durante la discusión de las redes conectadas con un Firewall, la red externa está delante del Firewall, la red interna se protege y detrás del Firewall, y un DMZ, mientras que detrás del Firewall, permite el acceso limitado a los usuarios externos. Porque el FWSM le deja configurar muchas interfaces con las políticas de seguridad variadas, que incluye muchas interfaces interiores, muchos DMZ, e incluso muchas interfaces exteriores si está deseado, 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 la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados 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 los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración del Catalyst 6500 Series Switch
- Configuración de FWSM

Configuración del Catalyst 6500 Series Switch

1. Usted puede instalar el FWSM en los Catalyst 6500 Series Switch o los Cisco 7600 Series Router. La configuración de la serie es idéntica y las series se refieren genéricamente en este documento como el **Switch**.**Nota:** Usted necesita configurar el Switch apropiadamente antes de que usted configure el FWSM.
2. **Asigne los VLA N al Módulo de servicios del Firewall** — Esta sección describe cómo asignar

los VLA N al FWSM. El FWSM no incluye ninguna interfaces físicas externa. En lugar, utiliza las interfaces VLAN. La asignación de los VLA N al FWSM es similar a cómo usted asigna un VLA N a un puerto del switch; el FWSM incluye una interfaz interna al módulo switch fabric, si presente, o el bus compartido.**Nota:** Refiera a la sección de los VLA N que configura de la guía de configuración de software de los Catalyst 6500 Switch para más información sobre cómo crear los VLA N y asignarlos a los puertos del switch.**Guías de consulta del VLA N:**Usted puede utilizar los VLAN privados con el FWSM. Asigne el VLAN principal al FWSM; el FWSM maneja automáticamente el tráfico del VLAN secundario.Usted no puede utilizar los VLA N reservados.Usted no puede utilizar el VLAN1.Si usted utiliza la Conmutación por falla FWSM dentro del mismo chasis del switch, no asigne los VLA N que usted reservó para la Conmutación por falla y las comunicaciones stateful a un puerto del switch. Pero, si usted utiliza la Conmutación por falla entre el chasis, usted debe incluir los VLA N en el puerto troncal entre el chasis.Si usted no agrega los VLA N al Switch antes de que usted los asigne al FWSM, los VLA N se salvan en la base de datos del Supervisor Engine y se envían al FWSM tan pronto como se agreguen al Switch.Asigne los VLA N al FWSM antes de que usted los asigne al MSFC.Los VLA N que no satisfacen esta condición se desechan del rango de los VLA N que usted intenta asignar en el FWSM.**Asigne los VLA N al FWSM en Cisco IOS Software:**En Cisco IOS Software, cree a hasta 16 grupos VLAN del Firewall, y después asigne a los grupos al FWSM. Por ejemplo, usted puede asignar todos los VLA N a un grupo, o usted puede crear un grupo interno y a un grupo exterior, o usted puede crear a un grupo para cada cliente. Cada grupo puede contener los VLA N ilimitados.Usted no puede asignar el mismo VLA N a los grupos del firewall múltiple; sin embargo, usted puede asignar a los grupos del firewall múltiple a un FWSM y usted puede asignar a un solo grupo del Firewall a los FWSM múltiples. Los VLA N que usted quiere asignar a los FWSM múltiples, por ejemplo, pueden residir en un grupo separado de los VLA N que son únicos a cada FWSM.Complete los pasos para asignar los VLA N al FWSM:`Router(config)#` **`firewall vlan-group firewall_group vlan_range`** `El vlan_range` puede ser uno o más VLA N, por ejemplo, 2 a 1000 y a partir de 1025 a 4094, identificado como un solo número (n) como 5, 10, 15 o rango (n-x) como 5-10, 10-20.**Nota:** Los puertos ruteados y los puertos de WAN consumen los VLA N internos, así que es posible que los VLA N en el rango 1020-1100 pueden ya ser funcionando.**Ejemplo:**
`firewall vlan-group 1 10,15,20,25` Complete los pasos para asignar a los grupos del Firewall al FWSM.`Router(config)#` **`firewall module module_number vlan-group firewall_group`** `El firewall_group` es uno o más números de grupo como un solo número (n) como 5 o rango como 5-10.**Ejemplo:**
`firewall module 1 vlan-group 1` **Asigne los VLA N al FWSM adentro software del sistema operativo Catalyst** — en software OS Catalyst, usted asigna una lista de VLA N al FWSM. Usted puede asignar el mismo VLA N a los FWSM múltiples si está deseado. La lista puede contener los VLA N ilimitados.Complete los pasos para asignar los VLA N al FWSM.`Console> (enable)` **`set vlan vlan_list firewall-vlan mod_num`** `El vlan_list` puede ser uno o más VLA N, por ejemplo, 2 a 1000 y a partir de 1025 a 4094, identificado como un solo número (n) como 5, 10, 15 o rango (n-x) como 5-10, 10-20.

3. **Agregue las interfaces virtuales conmutadas al MSFC** — UN VLA N definido en el MSFC se llama un Switched Virtual Interface. Si usted asigna el VLA N usado para el SVI al FWSM, después las rutas MSFC entre el FWSM y otro acodan 3 VLA N.Por razones de seguridad, por abandono, solamente un SVI puede existir entre el MSFC y el FWSM. Por ejemplo, si usted configura mal el sistema con los SVI múltiples, usted puede permitir accidentalmente que el tráfico pase alrededor del FWSM si usted asigna ambos los VLA N interiores y

exteriores al 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 Catalyst 6500 Series Switch

`!--- 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 adentro al FWSM del Switch con el comando apropiado para su sistema operativo del Switch:

- Software Cisco IOS:`Router#` **`session slot <number> processor 1`**
- Software OS Catalyst:`Console> (enable)` **`session module_number`**

(Opcional) compartiendo los VLA N con los módulos de otro servicio — si el Switch tiene módulos de otro servicio, por ejemplo, motor del control de la aplicación (ACE), es posible que usted tiene que compartir algunos VLA N con estos módulos de servicio. Refiera al diseño del módulo de servicio con ACE y al FWSM para más información sobre cómo optimizar la configuración de FWSM cuando usted trabaja con tales otros módulos.

Configuración de FWSM

1. **Interfaces de la configuración para el FWSM** — Antes de que usted pueda permitir el tráfico con el FWSM, usted necesita configurar un nombre de la interfaz y una dirección IP. Usted debe también cambiar el nivel de seguridad del valor por defecto, que es 0. Si usted nombra una interfaz `dentro`, y usted no fija el nivel de seguridad explícitamente, después el FWSM fija el nivel de seguridad a 100.**Nota:** Cada interfaz debe tener un nivel de seguridad de 0 (más bajo) a 100 (más alto). Por ejemplo, usted debe asignar su red más segura, tal como la red del host interior, al nivel 100, mientras que la red externa conectada con Internet puede ser el nivel 0. Otras redes, tales como DMZ, pueden estar mientras tanto.Usted puede agregar cualquier VLAN ID a la configuración, pero solamente los VLA N, por ejemplo, 10, 15, 20 y 25, que son asignados al FWSM por el Switch pueden pasar el tráfico. Utilice el **comando show vlan** para ver todos los VLA N asignados 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`
   Consejo: En el comando del **<*name*> *del* nameif**, el *nombre* es una cadena de texto hasta 48 caracteres y no es con diferenciación entre mayúsculas y minúsculas. Usted puede cambiar el nombre si usted entra este comando de nuevo con un nuevo valor. No ingrese la ninguna forma, porque ese comando causa los comandos all que se refieren que nombre que se borrará.
2. **Configure la ruta predeterminado:**
   `route outside 0.0.0.0 0.0.0.0 192.168.1.1` Una ruta predeterminado identifica el Gateway IP Address (192.168.1.1) a las cuales el FWSM envía todos los paquetes del IP para los cuales no tenga un docto o una Static ruta. Una ruta predeterminado es simplemente una Static ruta con 0.0.0.0/0 como el IP Address de destino. Las rutas que identifican un destino específico toman la precedencia sobre la ruta predeterminado.
3. **El NAT dinámico** traduce a un grupo de las direcciones reales (10.1.1.0/24) a un pool de los

direccionamientos asociados (192.168.1.20-192.168.1.50) que son routable en la red de destino. El pool asociado puede incluir menos direccionamientos que el grupo real. Cuando un host que usted quiere traducir accede la red de destino, el FWSM le asigna una dirección IP del pool asociado. Se agrega la traducción solamente cuando el host real inicia la conexión. La traducción existe solamente para la duración de la conexión, y un usuario dado no guarda la misma dirección IP después de los tiempos de la traducción hacia fuera.
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 Usted necesita crear un ACL para negar el tráfico de la red interna 10.1.1.0/24 para entrar la red DMZ1 (192.168.2.0) y para permitir las otras clases del tráfico a Internet con la aplicación de *Internet* ACL a la interfaz interior como hacia adentro dirección para el tráfico entrante.

4. El NAT estático crea una traducción fija de dirección real al direccionamiento asociado. Con el NAT dinámico y la PALMADITA, cada host utiliza un diverso direccionamiento o puerto para cada traducción subsiguiente. Porque el direccionamiento asociado es lo mismo para cada conexión consecutiva con el NAT estático, y existe una regla de traducción persistente, el NAT estático permite que los host en la red de destino inicien el tráfico a un host traducido, si hay una lista de acceso que lo permite.La diferencia principal entre el NAT dinámico y un rango de direcciones para el NAT estático es que el NAT estático permite que un host remoto inicie una conexión a un host traducido, si hay una lista de acceso que lo permite, mientras que no lo hace el NAT dinámico. Usted también necesita un mismo número de direccionamientos asociados como direcciones reales con el 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 Éstas son las dos declaraciones NAT estáticas mostradas. Primer se significa para traducir el IP real 192.168.2.2 en la interfaz interior al IP asociado 192.168.1.6 en la subred exterior a condición de que el ACL permite que el tráfico de la fuente 192.168.1.30 al IP asociado 192.168.1.6 para acceder al servidor Websense en la red DMZ1. Semejantemente, la segunda declaración NAT estática significó traducir el IP real 192.168.3.2 en la interfaz interior al IP asociado 192.168.1.10 en la subred exterior a condición de que el ACL permite que el tráfico de Internet al IP asociado 192.168.1.10 para acceder el web server en la red DMZ2 y tener el número del puerto UDP en el rango de 8766 a 30000.
5. El comando del URL-servidor señala el servidor que ejecuta la aplicación del Filtrado de URL del Websense. El límite es 16 servidores URL en el solo modo del contexto y cuatro servidores URL en el modo múltiple, pero usted puede utilizar solamente una aplicación, N2H2 o Websense, en un momento. Además, si usted cambia su configuración en el dispositivo de seguridad, esto no pone al día la configuración en el servidor de aplicaciones. Esto se debe hacer por separado, del acuerdo a las instrucciones del vendedor.El comando del URL-servidor debe ser configurado antes de que usted publique el comando del filtro para el HTTPS y el FTP. Si todos los servidores URL se quitan de la lista de servidores, después todos los comandos del filtro relacionados con el Filtrado de URL también se quitan.Una vez que usted señala el servidor, habilite el servicio del Filtrado de URL con el comando url del filtro.
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5 El comando url del filtro permite la prevención del acceso de los usuarios de salida del World Wide Web URLS que usted señala con el Websense que filtra la aplicación.

```
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. Vea la información del módulo del acuerdo a su sistema operativo para verificar que el

Switch reconoce el FWSM y lo ha traído 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 OS Catalyst:`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. Éstos son los puertos internos que se agrupan juntos 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 división 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 OS Catalyst:`Console> (enable)` **`show boot device mod_num`** **Ejemplo:**`Console> (enable)` **`show boot device 6`** `Device BOOT variable = cf:5`

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

1. **Fijando la división de inicio predeterminada** — Por abandono, el FWSM inicia de la partición de aplicación **cf:4**. Pero, usted puede elegir iniciar de la partición de aplicación **cf:5** o en la división del mantenimiento **cf:1**. Para cambiar la división de inicio predeterminada, ingrese el comando para su sistema operativo:Software Cisco IOS:`Router(config)#` **`boot device module mod_num cf:n`** Donde está 1 (mantenimiento), 4 (aplicación), o 5 n (aplicación).Software OS Catalyst:`Console> (enable)` **`set boot device cf:n mod_num`** Donde está 1 (mantenimiento), 4 (aplicación), o 5 n (aplicación).
2. **Reajustando el FWSM en Cisco IOS Software** — Para reajustar el FWSM, ingrese el comando como se muestra:`Router#` **`hw-module module mod_num reset [cf:n] [mem-test-full]`** **Los cf:** el argumento **n** es la división, 1 (mantenimiento), 4 (aplicación), o 5 (aplicación). Si usted no especifica la división, se utiliza la partición predeterminada, que es típicamente **cf:4**.La opción mem-prueba-**FULL** funciona con una prueba de toda la memoria, que tarda 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 OS Catalyst**:`Console> (enable)` **`reset mod_num [cf:n]`** Donde **cf: n** es la división, 1 (mantenimiento), 4 (aplicación), o 5 (aplicación). Si usted no especifica la división, se utiliza la partición predeterminada, que es típicamente **cf:4**.

Nota: El NTP no se puede configurar en el FWSM, porque toma sus configuraciones del Switch.

Problema: Incapaz de pasar el tráfico VLAN del FWSM al sensor 4270 IPS

Usted no puede pasar el tráfico del FWSM a los sensores IPS.

Solución

Para forzar el tráfico con el IPS, el truco es crear un VLAN auxiliar para romper con eficacia uno de sus VLA N actuales en dos y después interligarlos juntos. Marque este ejemplo con el VLA N 401 y 501 para aclarar:

- Si usted quiere analizar el tráfico en el **VLA N** principal **401**, cree otro **VLA N** vlan **501** (VLA N auxillary). Entonces inhabilite la interfaz VLAN 401, que los host en 401 utilizan actualmente como su default gateway.
- Interfaz siguiente del VLA N 501 del permiso con el *mismo* direccionamiento que usted inhabilitó previamente en la interfaz del VLA N 401.
- Ponga una de las interfaces IPS en el VLA N 401 y la otra en el VLA N 501.

Todo lo que usted tiene que hacer es mover el default gateway para el VLA N 401 sobre el VLA N 501. Usted necesita hacer los cambios similares para los VLA N si presente. Observe que los VLA N son esencialmente como los segmentos LAN. Usted puede tener un default gateway en un diverso pedazo de alambre que los host que lo utilizan.

Los paquetes defectuosos publican en el FWSM

¿Cómo puedo solucionar los paquetes defectuosos publico en el FWSM?

Solución

Publique el comando de la realización-unidad NP del sysopt en el modo de configuración global para resolver el problema del paquete defectuoso en el FWSM. Este comando fue introducido en el FWSM versión 3.2(5) y se asegura de que los paquetes están remitidos hacia fuera en la misma orden que fueron recibidos.

Problema: Incapaz de pasar asimétrico los paquetes ruteados con el Firewall

Usted no puede pasar asimétrico los paquetes ruteados con el Firewall.

Solución

Publique el comando de TCP-estado-puente de las avanzado-opciones de la conexión del conjunto en el modo de configuración de clase para pasar asimétrico los paquetes ruteados con el Firewall. Este comando fue introducido en el FWSM versión 3.2(1).

Soporte del Netflow en el FWSM

¿El FWSM soporta el Netflow?

Solución

El Netflow no se soporta en el FWSM.

Información Relacionada

- Página de soporte del Módulo de servicios de firewall Cisco Catalyst de la serie 6500
- Página de soporte de los Cisco Catalyst 6500 Series Switch

- Página de soporte del Cisco 7600 Series Router
- Intercepción de tráfico de TCP FWSM y Cookie SYN explicados
- Soporte Técnico y Documentación - Cisco Systems