El Firewall mantiene Module(FWSM) FAQ

Contenido

Introducción

Este documento contiene preguntas frecuentes (FAQ) sobre el módulo Catalyst 6500 Series Firewall Services (FWSM).

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

Características admitidas

Q. ¿Cuál es la versión mínima del código que necesito para funcionar con para el soporte mi FWSM, módulo intrusion detection system 2 (IDSM2), y módulo de servicio VPN (VPNSM)?

A. La versión del código apropiada depende del tipo de módulo de Supervisor en sus 6500 o 7600 chasis, así como del tipo de software que usted funciona con (CatOS [Hybrid] o Cisco IOS [Native]). Vea esta tabla para las versiones del código específicas para su módulo y el (MSFC) de la Multilayer Switch Feature Card.

	Sup1 (con el MSFC)		Sup2 (con el MSFC)		Sup720	
Módulo	IOS de Cisco	CatOS	IOS de Cisco	CatOS	IOS de Cisco	CatOS
FWSM	12.1(13)E	7.5(1)	12.1(13)E	7.5(1)	12.2(14)SX1	8.2(1)
IDSM2	No soportados	7.6(1)	12.1(19)E	7.6(1)	12.2(14)SX1	8.2(1)
VPNSM	No soport	No soport	12.2(14)SY	No soport	12.2(17a)SX10	No soport

	ados	ados		ados		ado *

* Hay planes para introducir el soporte.

Nota: Refiera a la comparación del Cisco Catalyst y de los sistemas operativos del Cisco IOS para el Cisco Catalyst 6500 Series Switch para la información sobre las diferencias entre CatOS (híbrido) y el Cisco IOS (nativo).

Q. ¿Puedo funcionar con el FWSM, el módulo intrusion detection system 2 (IDSM2), y el módulo de servicio VPN (VPNSM) en el mismo chasis?

A. Sí, usted puede funcionar con estos módulos en el mismo chasis si el Switch funciona con el Cisco IOS Software integrado con una versión mínima del Cisco IOS Software Release 12.2(14)SY (Sup2) o de 12.2(17a)SX10 (Sup720). Actualmente, no hay versión CatOS que puede soportar estos módulos de servicio en los mismos 6500 o 7600 chasis.

Q. ¿Cuáles son mi configuración y opciones de administración para el FWSM?

A. La configuración y las opciones de administración incluyen éstos.

Opción	Versión	Descripción
Centro de administración para los Firewall	Versiones 1.1.1 y later*	Esto es un interfaz basada en la Web para configurar y manejar los Firewall múltiples. **Nota:** El soporte para los grupos de servicios dentro de agrupar del objeto es limitado. Analizan, pero aplanan a los grupos de servicios con éxito inmediatamente. Esto afecta a los comandos con el ICMP-**tipo**, el **protocolo**, y las palabras claves del **servicio**. Esta limitación se aplica a las versiones 1.3 y anterior.
Monitorear el centro para la Seguridad	Versiones 1.2 y later*	Esto es un interfaz basada en la Web para monitorear los dispositivos de seguridad de Cisco. El software centraliza la Administración de Syslog de los dispositivos de seguridad múltiples de Cisco con la información flexible y las opciones el alertar.
Monitorear el centro para el funcionamiento	Versiones 2.0 y later*	Éste es un interfaz basada en la Web para monitorear y resolver problemas la salud y funcionamiento de los servicios que contribuyen a la seguridad de la red. El Simple Network Management Protocol (SNMP) es el protocolo subyacente usado.
PDM	Versión	Esto es un interfaz basada en la Web para configurar, manejar, y monitorear

	2.1	un solo Firewall. El PIX Device Manager (PDM) se debe instalar localmente en el firewall PIX.
Telnet	N/A	Telnet proporciona el acceso remoto del comando line interface(cli) a un Firewall. **Nota:** Para permitir el acceso de Telnet a la interfaz de seguridad más baja (conocida comúnmente como la interfaz exterior), usted necesita configurar el IPSec para la Administración.
Secure Shell (SSH)	N/A	SSH proporciona asegura el acceso del telecontrol CLI a un Firewall.
SNMP	N/A	El SNMP proporciona un método de monitorear el FWSM. **Nota:** El SNMP es solo lectura en el FWSM.
Syslog	N/A	El Syslog proporciona un método de monitorear el FWSM.

* Este software es parte de Este software proporciona un acercamiento integrado a manejar los dispositivos de seguridad de Cisco vía una interfaz basada en buscador para las redes para empresas.

Q. ¿Cuál es un SVI? ¿Puedo configurar los SVI múltiples?

A. Switched Virtual Interface de la significa SVI. Representa una interfaz lógica de la capa 3 en un Switch. Para las versiones CatOS anterior de 7.6(1) y las versiones de Cisco IOS Software anterior que 12.2(14)SY, solamente un SVI se permite como parte de los VLA N del Firewall. Es decir solamente una interfaz de la capa 3 se puede configurar entre el FWSM y el (MSFC) de la Multilayer Switch Feature Card. Una tentativa de configurar los SVI múltiples presenta un mensaje de error del comando line interface(cli).

Para las versiones CatOS 7.6(1) y posterior y Cisco IOS Software Release 12.2(14)SY y Posterior, FWSM admite múltiples los SVI. Por abandono, se soporta solamente un SVI. Utilice uno de estos comandos de habilitar el soporte para los SVI múltiples en su Switch.

- Para CatOS,Para el Cisco IOS, múltiple-VLAN-interfaces del Firewall del tipo.

Si usted configura su Switch para los VLA N FWSM y recibe un mensaje de error que indique que usted tiene más de un SVI, la mirada en su Switch y/o configuración de MSFC para asegurarse de que solamente una interfaz de la capa 3 (o la interfaz VLAN) existe como parte de los VLA N del Firewall.

Nota: Utilice solamente un SVI. Esto permite que usted evite una configuración complicada que implique el Policy Routing.

Q. ¿El FWSM soporta el SNMPv3?

A. No.

Q. ¿Cuántos VLA N el FWSM soporta?

A. El FWSM versión 1.1 soporta 100 VLA N y el 2.1 del FWSM versión soporta 250 VLA N.

Q. ¿El FWSM apoya el comando access-list compiled?

A. Puesto que el FWSM compila automáticamente las Listas de acceso en el hardware después de 10 segundos de inactividad en el CLI, no hay necesidad de las Listas de acceso de turbo. El 2.1 del FWSM versión ofrece las funciones adicionales de poder nombrar cuando se compilan las Listas de acceso.

Q. Hace el soporte FWSM el comando? del referencia-ancho de banda del auto-coste del Open Shortest Path First (OSPF) IOS

A. No. El FWSM no es consciente de los puertos físicos conectados con él. El costo de OSPF se debe configurar manualmente para cada interfaz con el comando ospf cost.

Q. ¿Puedo funcionar con el protocolo del Open Shortest Path First (OSPF) en una topología donde dos diversas interfaces del FWSM conectan con la misma red?

A. Sí. Estas funciones se soportan en el 2.1 de las versiones y posterior.

Q. ¿Qué Routing Protocol son soportados por el FWSM?

A. El Open Shortest Path First (OSPF) y el Routing Information Protocol (RIP) son los Routing Protocol soportados. Para más información sobre el FWSM, refiera a la documentación disponible en la página del Módulo de servicios de firewall Cisco Catalyst de la serie 6500.

Q. ¿El Multicast (del Internet Group Management Protocol v2 y Stub Multicast Routing [IGMP]) se soporta en el FWSM?

A. Sí. Estas funciones se soportan en el 2.1 de los FWSM versión y posterior. Si usted funciona con la versión 1.1, usted puede utilizar el Generic Routing Encapsulation (GRE) que hace un túnel como solución alternativa.

Q. ¿El FWSM soporta el Filtrado de URL?

A. Sí. El Websense se soporta en las versiones 1.1 y posterior, con el soporte adicional para el N2H2 agregado en la versión 2.1.

Q. ¿Por qué los paquetes fragmentados son caídos por el FWSM?

A. Por abandono, los paquetes fragmentados no pueden atravesar el FWSM. Usted puede utilizar el comando fragment de configurar esta característica. Este comportamiento diferencia del del firewall PIX. Los protocolos comunes que utilizan los paquetes fragmentados son Open Shortest Path First (OSPF) y Network File System (NFS).

Q. ¿Puedo terminar las conexiones VPN en mi FWSM?

A. La funcionalidad VPN no se soporta en el FWSM. La finalización de las conexiones VPN es la responsabilidad del Switch y/o del módulo de servicios VPN. La licencia 3DES se proporciona para los fines de administración solamente, por ejemplo la conexión con una interfaz de la bajo-Seguridad vía Telnet, el Secure Shell (SSH), y HTTP seguro (HTTPS).

Q. ¿El Authentication, Authorization, and Accounting (AAA) para el RADIUS o el TACACS+ se soporta en el FWSM?

A. El AAA se soporta para la administración de FWSM y el tráfico que pasan con el FWSM. Refiera a la documentación del Módulo de servicios del Firewall para los detalles adicionales.

El FWSM ofrece las funciones similares a la del firewall PIX, con las excepciones de las Listas de acceso transferibles y de los VPN. Con esto en la mente, usted puede utilizar estos documentos del firewall PIX como guías para la configuración de FWSM.

- Cómo realizar la autenticación y la activación en Cisco Secure PIX Firewall (de 5.2 a 6.2)
- Realización de autenticación, autorización y contabilidad de usuarios por medio de las versiones 5.2 y posteriores de PIX.

Q. ¿Cómo realizo una recuperación de contraseña para el FWSM?

A. Refiera a estos documentos para la información sobre la recuperación de contraseña.

- Para la versión 1.1(1), refiera a la nota de la configuración de FWSM 1.1(1) sobre el cambio y la recuperación de las contraseñas.
- Para las versiones 1.1(2) y 1.1(3), refiere a la nota de la configuración de FWSM 1.1(2) sobre el cambio y la recuperación de las contraseñas.

Q. ¿El FWSM soporta las Tramas gigantes?

A. Sí, el FWSM puede soportar las Tramas gigantes.

Q. ¿Cómo el FWSM responde cuando recibe un paquete con su dirección de origen como loop - direccionamiento posterior?

A. Trata el paquete como inválido y cae el paquete. Por abandono, el FWSM cae los paquetes con una dirección de origen no válida tal como un loop - direccionamiento, dirección de broadcast y dirección de host posteriores del destino. Un mensaje del registro tal y como se muestra en de este ejemplo se genera.

```
%FWSM-2-106016: Deny IP spoof from (IP_address) to
 IP_address on interface interface_name.
```

Q. ¿El PVLAN se soporta en el FWSM?

A. El soporte del PVLAN comienza en la versión de software 3.1. Si usted funciona con una versión de software anterior de 3.1, la única solución alternativa posible es conectar el puerto promiscuo del PVLAN usando el cable de par cruzado con un puerto de acceso regular, y después hace el VLA N de ese puerto de acceso firewalled.

Q. ¿El número de línea de la lista de acceso se soporta en el FWSM?

A. Esta característica se soporta solamente en la versión de software 3.1 y posterior.

Q. ¿Puede usted limitar el número de conexiones que un usuario puede tener en el FWSM?

A. Sí, usted puede limitar las conexiones con la ayuda del Marco de políticas modular. Complete estos pasos para limitar el número de conexiones:

1. Cree una correspondencia de la clase para hacer juego el tráfico.
2. Coloque la correspondencia de la clase a una correspondencia de políticas y utilice la conexión que limita en la correspondencia de políticas.
3. Aplique la correspondencia de políticas usando la política de servicio.

Refiera a configurar los límites y los descansos de la conexión para más información y pasos detallados.

Q. ¿Hay limitaciones en la implementación del Multicast en el FWSM?

A. Sí. El FWSM no soporta la subred 232.x.x.x como nombre del grupo, pues se ha reservado ya para el módulo de Servicios de seguridad (SS).

Q. ¿El broadcast dirigido se permite con el FWSM?

A. No. A diferencia de un router, el FWSM no permite el broadcast dirigido a través de sus interfaces. Una solución alternativa más similar es utilizar la función de Relay DHCP incorporada para remitir los broadcasts a partir de una interfaz a otra.

Q. ¿Puede el motor del examen HTTP detectar el tráfico NON-HTTP o el tráfico no estándar en HTTP session?

A. Sí. El Firewall de la aplicación con el examen avanzado HTTP puede detectar y controlar éstos trafique. Refiera a la descripción del motor de la Inspección de la aplicación para más información.

Q. ¿Son las características de la normalización en el ASA y el FWSM compatibles?

A. En el FWSM, la normalización TCP se aplica solamente para traficar que golpea el complejo TCP. El tráfico plano de los datos normales (trayecto rápido) no es afectado. Esto diferencia del ASA en que todo el tráfico ASA está sujetado al normalizador.

En el FWSM, si el normalizador se inhabilita las caídas del módulo de nuevo al comportamiento 2.3. Pero, si usted inhabilita el TCP-**normalizador del punto de control**, esto previene los controles estrictos TCP, tales como la detección de segmentos del out-of-sequence y de opciones TCP de la supervisión, en los paquetes TCP recibidos en el avión del control para el examen de la capa 7 en el FWSM, y no se realiza. Así, es recomendable no inhabilitarlo. El FWSM no permite el ajustar en los parámetros predeterminados del TCP-mapa.

Q. ¿Necesitamos habilitar/normalizador de la neutralización TCP?

A. Debido a la incapacidad para pasar una cierta conexión la información específica de los NP para controlar el avión, el normalizador TCP no funciona posiblemente correctamente todo el tiempo en el FWSM. Además, las TCP-correspondencias únicas asociadas a las conexiones no pueden ser identificadas. Así, el FWSM confía en el TCP-mapa predeterminado que no trabajan posiblemente correctamente para todas las conexiones. Debido a estas limitaciones, hay una necesidad de habilitar/normalizador de la neutralización TCP en el avión del control para el tráfico que pasa con el Firewall. El FWSM no permite el ajustar en los parámetros predeterminados del TCP-mapa.

Q. ¿Cuál es el número máximo de entradas del mfib que un FWSM pueda soportar?

A. El número máximo de entradas es 5000 entradas.

Q. ¿Cómo puedo capturar los paquetes en el FWSM?

A. Los paquetes se pueden capturar en el FWSM. El uso del CLI como captura de paquetes no se soporta en el ASDM y no soportan al **comando capture** en el ASDM. Refiérase los comandos ignorada y de la vista-Solamente para más información. Refiera a capturar los paquetes para más información sobre la configuración del paquete que captura en el FWSM. Refiera a ASA/PIX/FWSM: Paquete que captura usando el CLI y el ejemplo de la Configuración de ASDM para más información sobre un ejemplo de configuración de la captura de paquetes.

Q. ¿Qué versión del ASDM EL FWSM soporta?

A. Refiera compatibilidad a la versión FWSM y del ASDM para más información sobre compatibilidad de la versión FWSM y del ASDM.

Autorización

Q. Tengo una licencia para un FWSM que se ejecute en el modo de contexto múltiple. ¿Puedo obtener una licencia para un FWSM de repuesto en caso de falla de hardware?

A. Usted puede obtener una licencia para el FWSM de repuesto. Sin embargo, usted necesita poner una pedido para la licencia de repuesto FWSM mientras que usted una licencia común. En caso de falla de hardware, de Soporte técnico de Cisco del contacto de verificar el error y de obtener una licencia para el FWSM de repuesto. Refiera a la versión de software del módulo del escudo de protección Cisco 2.2(1) para la información de autorización.

Q. ¿El FWSM soporta las interfaces compartidas múltiplo?

A. El FWSM no soporta las interfaces compartidas múltiplo, sino que por el contrario usted puede tener un VLA N a través de los contextos múltiples. Refiera a compartir los recursos y las interfaces entre los contextos para más información.

Problemas del VLA N

Q. ¿Cómo coloco los VLA N adicionales detrás del FWSM?

A. Utilice el **comando nameif** si usted quiere agregar 200 vlan a la configuración. El nivel de seguridad debe estar entre 0 y 100. El sintaxis del comando complete es el **nameif vlan200 <interface name> <security level>**.

Q. ¿Cuántos VLA N puedo colocar detrás del FWSM usando el solo contexto, modo ruteado?

A. Usted puede colocar 1000 VLA N detrás del FWSM usando el solo contexto, modo ruteado.

Problemas del ping

Q. ¿Por qué no puedo hacer ping mi FWSM en directamente una interfaz conectada?

A. Por abandono, cada interfaz niega el Internet Control Message Protocol (ICMP). Utilice el **comando icmp** de permitir este tráfico a la interfaz. Este comportamiento diferencia del del PIX.

Nota: Cuando el ICMP a la interfaz es negado por el **comando icmp**, usted todavía ve la dirección MAC correcta en la tabla del Address Resolution Protocol (ARP). Si usted no ve la dirección MAC, vea la pregunta siguiente.

Q. No puedo hacer ping mi FWSM en directamente una interfaz conectada, y no veo una entrada del Address Resolution Protocol (ARP) para la interfaz. Estoy funcionando con el software de CatOS (o híbrido) en mi Switch. ¿Qué debo hacer?

A. Configurar las interfaces dentro de la configuración de FWSM (con el comando nameif) o en el [with the interface vlan command] del (MSFC) de la Multilayer Switch Feature Card antes de que se configuren en el Switch (en el módulo de Supervisor en CatOS) puede hacer que las interfaces aparecen como si no estén respondiendo en absoluto, sin la respuesta de la entrada ARP o del Internet Control Message Protocol (ICMP).

Si usted configuró una interfaz en el FWSM o el MSFC que pertenece a los VLA N del Firewall antes de que usted configurara el Switch, quite el FWSM o la entrada MSFC, recargue el módulo, después re-agregue la entrada.

Q. ¿Por qué no puedo hacer ping o pasar tráfico con el FWSM?

A. El Network Address Translation (NAT) se debe configurar usando el 0 nacional, nacional/global, o el comando static para que el tráfico pase con el FWSM de una interfaz de mayor seguridad (la interfaz interior) a una interfaz de menor seguridad (interfaz exterior).

Usted debe también utilizar el comando access-list de implementar las Listas de acceso que permiten que el tráfico atraviese el FWSM. Por abandono, las Listas de acceso niegan todo el tráfico en todas las interfaces (**deny ip any any**). Este comportamiento diferencia de la configuración predeterminada del PIX, que permite que el tráfico de más arriba baje la Seguridad y niega el tráfico de más bajo a la mayor seguridad. Configure una lista de acceso con el **IP del permiso cualquier** y apliqúela a las interfaces de alta seguridad para conseguir el FWSM para

comportarse como el PIX.

Q. Puedo hacer ping la interfaz FWSM que está conectada directamente con mi red, pero no puedo hacer ping otras interfaces. ¿Es esto normal?

A. Sí. Éste es un mecanismo de seguridad incorporado que también existe en el firewall PIX.

Problemas de la Conmutación por falla

Q. ¿Puedo configurar la Conmutación por falla entre dos FWSM que funcionen con diversas versiones del código?

A. No La Conmutación por falla requiere que ambos FWSM funcionen con la misma versión del código. Un mecanismo dentro de la característica de la Conmutación por falla verifica la versión del par y previene la Conmutación por falla si las versiones del código son diferentes. Por este motivo, usted debe actualizar ambos FWSM al mismo tiempo.

Q. ¿Puedo configurar la Conmutación por falla entre dos FWSM en diversos chasis?

A. Sí. Pero los FWSM se deben conectar por la capa 2 en todas las interfaces. Es decir todas las interfaces deben poder intercambiar el [Address Resolution Protocol (ARP), and so forth] de los paquetes de broadcast de la capa 2 por uno a. Los paquetes del protocolo de fallas no se pueden rutear en la capa 3.

Q. He configurado la Conmutación por falla entre dos FWSM, pero no están sincronizando. ¿Cuál podría ser el problema?

A. Asegúrese de que su configuración cumpla estos requisitos para la recuperación tras falla exitosa.

- Ambos FWSM deben funcionar con la misma versión del código.
- Ambos FWSM deben tener el mismo número de VLA N.
- Una conexión de la capa 2 debe existir entre todos los VLA N en los FWSM. Si los FWSM existen en diverso chasis con un trunk configurado entre él, verifique que todos los VLA N existan y estén permitidos en el trunk.

Q. ¿Puedo configurar la Conmutación por falla para tres o más unidades de FWSM, que son diversos chasis del switch extendidos por?

A. **No** La configuración de la Conmutación por falla se soporta solamente para un par de FWSM, por ejemplo, 2 unidades. Estas dos unidades pueden estar en un mismo Switch o dos switches diferentes. Si usted instala el FWSM secundario en el mismo Switch que el FWSM primario, usted protege contra el error del módulo-nivel. Para proteger contra el error del módulo-nivel y así como el error del Switch-nivel, usted puede instalar el FWSM secundario en un switch diferente. El FWSM no coordina la Conmutación por falla directamente con el Switch, sino que trabaja armonioso con la operación de la Conmutación por falla del Switch. Refiera a la colocación intra y del Inter-chasis del módulo para más información.

Miscelánea

Q. El FWSM tiene una escritura de la etiqueta que estado, “no quita el indicador luminoso LED amarillo de la placa muestra gravedad menor mientras que el indicador luminoso de estado es verde o la corrupción del disco puede ocurrir.” ¿Qué significa?

A. El módulo del Firewall debe ser quitado solamente después que usted inhabilita el poder usando uno de estos métodos. (No hay preferencia por un método determinado.)

- Utilice el comando line interface(cli) del Switch y publique uno de estos comandos.CatOS - **set module power down** *Mod*Cisco IOS ® Software - *ningún* **permiso del poder**
- Presione el botón del **apagar** en la cuchilla.
- Accione físicamente abajo el chasis.

Usted puede quitar el módulo de manera segura cuando el indicador luminoso de estado no es verde.

Q. Utilicé el comando show module, y mi FWSM tiene un estatus de `defectuoso/de otro`. ¿Qué debo hacer?

A. Refiera a esta lista de verificación para resolver problemas un FWSM con un estatus de `defectuoso/de otro`.

- Asegúrese de que usted funcione con una versión admitida del código en su Switch.
- Asegúrese de que el FWSM pueda coexistir con las otras cuchillas situadas en el mismo chasis. Refiera a los Release Note y/o al Software Advisor (clientes registrados solamente) del Catalyst 6500 para más información.
- Si usted funciona con CatOS/el código híbrido en su Switch, reajuste la configuración para el slot ocupado por el módulo FWSM. Utilice estos comandos para hacer esto.Teclee **set module power down la** *Mod* para accionar abajo el FWSM.Teclee la **Mod clara de los config** para borrar la configuración del Switch asociado a ese slot y para accionar para arriba el módulo.

Refiera a esta documentación para más información.

- Lista de fallas de hardware para switches serie Catalyst 4000, 5000 y 6000 que ejecutan CatOS
- Resolviendo problemas el hardware y los problemas frecuentes en los Catalyst 6000 Series Switch que funcionan con el Cisco IOS integrado (modo nativo)

Si usted continúa experimentando los problemas, entre en contacto el Soporte técnico de Cisco para el troubleshooting adicional.

Q. ¿Dónde puedo encontrar la documentación FWSM?

A. Los Release Note para el FWSM se pueden encontrar conforme a los Release Note de las Catalyst 6500 Series. Para más información, refiera a la documentación disponible en la página del Módulo de servicios de firewall Cisco Catalyst de la serie 6500.

Q. ¿Dónde puedo encontrar la información sobre los mensajes de error que veo en mi FWSM?

A. El decodificador de mensajes de error (clientes registrados solamente) proporciona los detalles en muchos mensajes de error FWSM. La Documentación del Producto en los mensajes del sistema también contiene la información útil. Si usted requiere la asistencia adicional, entre en contacto el Soporte técnico de Cisco.

Q. ¿Dónde puedo encontrar la información sobre los bug existentes para mi FWSM?

A. Los detalles en los bug existentes se pueden encontrar en el Bug Toolkit (clientes registrados solamente).

Q. ¿Cuáles son las diferencias entre el firewall PIX y el Módulo de servicios del Firewall?

A. El PIX y el FWSM se basan en el código similar. Sin embargo, hay dos diferencias fundamentales. El PIX (soporte de las ofertas) proporciona las funciones VPN y IDS. El FWSM no proporciona las funciones VPN y IDS porque estas características se ofrecen en el otro linecards. Refiera a la hoja de datos del Módulo de servicios del sistema de la detección de intrusos de las Catalyst 6500 Series (IDSM-2) para más información sobre el Módulo de servicios del sistema de la detección de intrusos de las Catalyst 6500 Series (IDSM-2). Refiera a la hoja de datos del producto del Módulo de servicios del IPSec VPN del Catalyst 6500 para más información sobre el Módulo de servicios del IPSec VPN del Catalyst 6500.

Refiera a esta documentación para las diferencias menores entre el PIX y el FWSM:

- Documentación técnica PIX
- Release Note PIX
- Referencias de Comando PIX
- Documentación técnica FWSM
- Release Note FWSM
- Referencias de comandos FWSM

Q. No podría publicar los comandos de los grupos de acceso múltiples en el FWSM por la interfaz. El FWSM parece tomar solamente a un grupo de acceso por la interfaz. ¿por qué?

A. Cuando usted publica estos comandos en el FWSM, sólo aparece el **comando access-group** más reciente:

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

Esto es porque el FWSM permite solamente una lista de acceso por la interfaz por la dirección.

Q. ¿Qué información se salva en las entradas del xlate en el FWSM?

A. Las entradas del xlate salvan esta información:

1. **Interfaz de origen** — Ésta es la interfaz que el paquete está recibido, por ejemplo, `afuera`.
2. **Dirección IP de origen** — Ésta es la dirección IP de origen del paquete.
3. **Dirección IP traducida** — En el caso de ningunas sentencias NAT, la dirección IP traducida y la dirección IP de origen son lo mismo.
4. **Interfaz de destino** — La interfaz que las hojas del paquete basaron en la búsqueda en la tabla de ruteo del IP Address de destino del paquete.

Q. ¿Qué los valores y las estadísticas en el `perfmon de la demostración` en el FWSM implican?

A. Utilice el **comando show perfmon** para capturar la información sobre el funcionamiento del FWSM.

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

`La corriente de la` columna muestra las estadísticas en el Intervalo actual, donde mientras que la `media` más reciente de la columna muestra la media acumulativa puesto que las estadísticas de la última vez fueron borradas. Se muestra como `/s` porque es la tarifa, bastante que un valor absoluto.

Las estadísticas mostradas en la salida de comando son actualizadas en un intervalo de 120 segundos por abandono. El intervalo se puede cambiar con el comando del **intervalo del perfmon**.

```
FWSM#perfmon interval 20
```

Significa que el índice de las estadísticas señaladas en la columna `actual` está calculado cada 20 segundos. Además, siempre que usted ingrese el **comando show perfmon**, las tarifas se calculan con las estadísticas en esa punta del tiempo.

El FWSM no incluye un puerto de consola en serie, pero algunos mensajes se visualizan solamente en un puerto de la consola, que incluye la salida del **perfmon de la demostración** y de los comandos del **perfmon**. Utilice el comando de la salida-**consola de la demostración** para ver el búfer de la consola, que incluye la salida del **comando show perfmon**.

Q. Habrá un salto de rendimiento en el FWSM con el `ningún` comando? del `servicemodule de la sesión de monitoreo`

`A.` Requieren a la sesión SPAN en el FWSM debido a una limitación del hardware de ASIC para la replicación del tráfico. El FWSM necesita ASIC para la replicación del paquete y la sesión SPAN pasa los paquetes para conmutar para eso usando la sesión SPAN. El tráfico afectado por este comando es EtherChannel, Multicast y GRE distribuidos. Se recomienda para tener la sesión SPAN configurada y para no quitarla.

Si por alguna razón usted necesita quitarlo, aseegurese que usted no ha replicado el tráfico de la naturaleza, por ejemplo, el EtherChannel distribuido, que se puede afectar por el Field Notice: FN - 61935 - incompatibilidad del módulo de servicio de las Catalyst 6500 Series y de las 7600 Series con la recirculación distribuida del EtherChannel y del paquete.

Q. ¿Puede usted aumentar la memoria para salvar más Listas de control de acceso (ACL)?

A. La memoria afectada un aparato para los ACL en el FWSM es limitada. Refiera a las especificaciones - Gobierne los límites para más información sobre la asignación del recurso FWSM.

Cuando la memoria afectada un aparato para los ACL en un contexto se excede, usted puede recibir ninguno de estos mensajes de error:

- `ERROR: Incapaz de agregar, límite de los config de la lista de acceso alcanzado`
- `ERROR: Incapaz de agregar las reglas de la directiva`
- `Incapaz de agregar un agujero a la regla de la directiva`

Algunas Listas de acceso utilizan más memoria que otras. Depende del tipo de lista de acceso, y el límite real que el sistema puede soportar es menos que el máximo. La asignación entre las reglas y la asignación de memoria no es un mapeo uno a uno. Depende realmente de la regla y cómo consigue programada en hardware.

Usted tiene dos opciones para la optimización del uso de la memoria de ACE:

- Resuma y simplifique sus entradas de ACE — esto puede ser hecha si usted completa estas prácticas recomendadas:Utilice los direccionamientos contiguos de los host siempre que sea posible. Agregue las declaraciones del host en los ACE/los grupos de objetos en las redes.Utilice `ningunos` en vez de las redes, y las redes en vez de los host cuando es posible.Intente simplificar los grupos de objetos. Esto puede potencialmente ahorrar centenares de ACEs cuando se amplían las ACLs. Un ejemplo es agrupar juntas las declaraciones del puerto individual en un rango.
- Reparto la memoria afectada un aparato para ACE en cada división. Esto requiere la reinicialización del módulo FWSM.El FWSM divide básicamente la memoria afectada un aparato para ACE en 12 divisiones, y afecta un aparato la memoria correspondiente para cada uno. Esto se hace automáticamente. De la versión 2.3(2) y posterior, usted puede utilizar al administrador de recursos para reasignar la memoria, que depende del número de contextos que usted tiene.Publique el **comando count del contexto de la demostración** para marcar cuántos contextos usted tiene. Usted puede entonces verificar esto con la configuración. Entonces encuentre el número de divisiones que utilicen el comando de la ACL-**división del recurso de la demostración**. Si usted tiene más divisiones que su contexto definido, después usted puede hacer juego el número de divisiones al número de contexto con el comando de las número-de-*divisiones de la ACL*-**división del recurso**.Usted necesita salvar la configuración y reiniciar el FWSM después de esto. El comando anterior le da más memoria para ACE, si éste es bastante o depende no otra vez de ACE que usted agrega al contexto.**Precaución:** Una desventaja del remapping anterior es que si usted quiere agregar otro contexto, después usted tiene que reasignar la asignación de memoria otra vez. Esto causa menos memoria disponible a cada contexto y puede romper las definiciones actuales de ACE. La memoria en el FWSM afectado un aparato a es una cantidad finita y la talla por consiguiente en una manera predeterminada o con la asignación del recurso manual según lo mencionado previamente.

De la versión 4.0 hacia adelante, el FWSM ha introducido una característica llamada la “optimización del ACL” que utiliza eficientemente a los recursos de memoria para las entradas ACL del múltiplo que salva. Esto se ocupa de un algoritmo incorporado que agregue automáticamente las entradas ACL donde sea posible sin la falta de la eficacia de cualquier una entrada ACL. Este algoritmo se une a juntas las subredes contiguas mencionadas en diversas entradas ACL en una sola declaración, y detecta las coincidencias en los rangos de puertos. Esta característica se habilita usando un comando y, después de que se realice la optimización, las

miradas completas de la configuración ACL diferentemente de la configuración ACL (original) anterior. Esta configuración ACL ordenada se podría conservar después de la verificación y la optimización se podría inhabilitar para salvar el overloading (sobrecarga) de cómputo CPU. Para más información sobre esta característica, refiera a la sección de la optimización del grupo de la lista de acceso que describe las funciones de la optimización del ACL junto con sus detalles de la configuración.

La versión 4.0 también introdujo otra característica llamada “capacidad de la lista de acceso de Increasaed”. Con esta característica, los usuarios ahora tienen la capacidad de salvar 130,000 entradas ACL en el modo del solo-contexto y 150,000 entradas en el modo del multicontext. Para más información sobre esta característica, refiera a la sección “de la capacidad creciente de la lista de acceso” en el boletín de la versión de software 4.0 del Módulo de servicios del escudo de protección Cisco.

Q. ¿Por qué hace el comando capture cuando está aplicado a las paradas FWSM y no captura el tráfico tan pronto como apliquen a otro comando capture en la interfaz?

A. Cuando usted configura la captura “z” en la misma interfaz donde la captura “x” de los supercedes de la captura “z” de la captura está ya aplicado “x”, después. La captura activa es la más reciente asociada a la interfaz particular.

La única excepción es cuando la lista de acceso en la captura “x” solapa con la lista de acceso de la captura “z”. Si ése es el caso, después ambas capturas continúan capturando el tráfico donde las listas de acceso solapan.

Q. ¿Cómo puedo resolver el error del `tiempo de espera de la trama del maderero NP-PCcmplx` en el FWSM?

A. Recargue el módulo FWSM para resolver este error.

Q. ¿Cómo puedo configurar el FWSM para utilizar la Intercepción de tráfico de TCP para defender contra los tipos determinados de inundaciones SYN?

A. Usted puede configurar el FWSM para utilizar la Intercepción de tráfico de TCP para defender contra los tipos determinados de inundaciones SYN. Refiera a la Intercepción de tráfico de TCP FWSM y a los Cookie SYN explicados para más información.

Q. ¿Habría problemas de rendimiento para procesar los paquetes del IPv6?

A. Sí. Usted puede ver los problemas de rendimiento al enviar el tráfico del IPv6, como el paquete necesita ser procesado por el CPU. Debido a las diferencias en la manipulación del tráfico del IPv4 y del tráfico del IPv6 por el CPU, el proceso del paquete del IPv6 causará ciertos problemas de rendimiento con el FWSM.

Q. ¿Cómo puedo evitar que el FWSM conteste a un servidor distante con su propia dirección MAC?

A. Usted necesita inhabilitar la característica del proxy ARP en la interfaz especificada con este comando:

"sysopt noproxyarp <interface>"
Para más información sobre la característica del proxy ARP, refiera al guía de referencia de comandos FWSM.

Q. ¿Cómo puedo prevenir las llamadas con el FWSM de la caída?

A. Para resolver este problema, el examen de la neutralización para el H323 y el H225:

```
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
```

Q. ¿Cómo puedo resolver los problemas de la traducción de NAT en el FWSM?

A. Para resolver este problema, utilice el comando de xlate-**puente**. Por abandono, el FWSM crea a las sesiones de NAT para todas las conexiones incluso si usted no utiliza el NAT. Usted puede inhabilitar a las sesiones de NAT para el tráfico sin traducir, que se llama puente del xlate, para evitar el límite máximo de la sesión de NAT. El comando de xlate-**puente** se puede configurar como se muestra:

```
hostname(config)#xlate-bypass
```

Refiera a configurar puente del xlate para más información sobre cómo a la configuración de xlate-puente.

Información Relacionada

- Ejemplo de la configuración básica FWSM
- Documentación del Módulo de servicios del Firewall
- Página de soprte del producto del Módulo de servicios del Firewall
- Soporte Técnico y Documentación - Cisco Systems