Ejemplo transparente de la configuración de escudo de protección del módulo firewall service

Contenido

Introducción

Tradicionalmente, un firewall es un salto ruteado y actúa como gateway predeterminado para los hosts que se conectan a una de sus subredes filtradas. Un Firewall transparente, por otra parte, es un Firewall de la capa 2 que los actos como un *Bump In The Wire* o un *Firewall Stealth* y no se consideran como salto del router a los dispositivos conectados. El módulo firewall service (FWSM) conecta la misma red en sus interfaces interior y exterior. Porque el Firewall no es un salto ruteado, usted puede introducir fácilmente un Firewall transparente en una red existente. La redirección IP es innecesaria.

Se facilita el mantenimiento porque no hay modelos complicados de la encaminamiento a resolver problemas y ninguna configuración del NAT.

Aunque el modo transparente actúa como Bridge, acode 3 que el tráfico (tal como tráfico IP) no puede pasar con el FWSM a menos que usted lo permita explícitamente con una lista de acceso ampliada. El único tráfico permitido con el Firewall transparente sin una lista de acceso es tráfico ARP. El tráfico ARP se puede controlar por la inspección ARP.

En el modo ruteado, algunos tipos de tráfico no pueden pasar con el FWSM incluso si usted lo permite en una lista de acceso. Alternativamente, el Firewall transparente puede permitir cualquier tráfico a través con una lista de acceso ampliada (para el tráfico IP) o una lista de acceso del Ethertype (para el tráfico no IP).

Por ejemplo, usted puede establecer las adyacencias del Routing Protocol con un Firewall transparente. Usted puede permitir el tráfico VPN (IPSec), OSPF, del RIP, del EIGRP, o BGP basado a través en una lista de acceso ampliada. Asimismo, los protocolos tales como HSRP o el VRRP pueden pasar con el FWSM.

El tráfico no IP (por ejemplo, APPLETALK, IPX, BPDU, y MPLS) se puede configurar para ir a través con una lista de acceso del Ethertype.

Para las características que no se soportan directamente en el Firewall transparente, usted puede permitir que el tráfico pase a través de modo que el Routers en sentido ascendente y descendente pueda soportar las funciones. Por ejemplo, con una lista de acceso ampliada, usted puede permitir el tráfico del DHCP (en vez de la función de Relay DHCP sin apoyo) o el tráfico Multicast, tal como eso creada por el IP/TV.

Cuando el FWSM se ejecuta en el modo transparente, la interfaz de salida de un paquete es determinada por las operaciones de búsqueda del MAC address en vez de las operaciones de búsqueda de la ruta. Las sentencias de Route pueden todavía ser configuradas, pero se aplican solamente al tráfico FWSM-originado. Por ejemplo, si su servidor de Syslog está situado en una red remota, usted debe utilizar una Static ruta, así que el FWSM puede alcanzar esa subred.

Una excepción a esta regla es cuando usted utiliza los exámenes de la Voz y el punto final es por lo menos un salto lejos del FWSM. Por ejemplo, si usted utiliza el Firewall transparente entre CCM y un gateway de H.323, y hay un router entre el Firewall transparente y el gateway de H.323, después usted necesita agregar una Static ruta en el FWSM para el gateway de H.323 para la realización de la llamada satisfactoria.

Nota: El modo transparente FWSM no pasa los paquetes CDP o ninguna paquetes que no tienen un Ethertype mayor o igual un 0x600 válidos. Por ejemplo, usted no puede pasar los paquetes IS-IS. Una excepción se hace para los BPDU, se soportan que.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el FWSM con la versión 3.x.

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.

Convenciones

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

Firewall transparente

Grupos de Bridge

Si usted no quiere los gastos indirectos de los contextos de seguridad, o quiera maximizar su uso de los contextos de seguridad, usted puede configurar hasta ocho pares de interfaces, llamados los Grupos de Bridge. Cada Grupo de Bridge conecta con una red separada. El tráfico del Grupo de Bridge se aísla de otros Grupos de Bridge. El tráfico no se rutea a otro Grupo de Bridge dentro del FWSM, y el tráfico debe salir el FWSM antes de que sea ruteado por un router externo de nuevo a otro Grupo de Bridge en el FWSM. Aunque las funciones de Bridging sean separadas para cada Grupo de Bridge, muchas otras funciones se comparten entre todos los Grupos de Bridge. Por ejemplo, todos los Grupos de Bridge comparten un servidor o una configuración de servidor AAA del registro del sistema. Para la separación completa de la política de seguridad, utilice los contextos de seguridad con un Grupo de Bridge en cada contexto.

Porque el Firewall no es un salto ruteado, usted puede introducir fácilmente un Firewall transparente en una red existente. La redirección IP es innecesaria. Se facilita el mantenimiento porque no hay modelos complicados de la encaminamiento a resolver problemas y ninguna configuración del NAT.

Nota: Cada Grupo de Bridge requiere un IP Address de administración. El FWSM utiliza esta dirección IP como la dirección de origen para los paquetes que originan del Grupo de Bridge. El IP Address de administración debe estar en la misma subred como la red conectada.

Pautas

Siga estas guías de consulta cuando usted planea su firewall network transparente:

- Un IP Address de administración se requiere para cada Grupo de Bridge.A diferencia del modo ruteado, que requiere una dirección IP para cada interfaz, un Firewall transparente tiene una dirección IP asignada al Grupo de Bridge entero. El FWSM utiliza esta dirección IP como la dirección de origen para los paquetes que originan en el FWSM, tal como mensajes del sistema o comunicaciones AAA.El IP Address de administración debe estar en la misma subred como la red conectada. Usted no puede fijar la subred a una subred del host (255.255.255.255). El FWSM no soporta el tráfico en las redes secundarias; solamente el tráfico en la misma red que el IP Address de administración se soporta. Refiera a asignar una dirección IP a un Grupo de Bridge para más información sobre las subredes del IP de administración.
- Cada Grupo de Bridge utiliza una interfaz interior y una interfaz exterior solamente.
- Cada uno directamente red conectada debe estar en la misma subred.

- No especifique el IP Address de administración del Grupo de Bridge como el default gateway para los dispositivos conectados. Los dispositivos necesitan especificar al router en el otro lado del FWSM como el default gateway.
- La ruta predeterminado para el Firewall transparente, que se requiere para proporcionar un trayecto de retorno para el tráfico de administración, se aplica solamente al tráfico de administración a partir de una red del Grupo de Bridge. Esto es porque la ruta predeterminado especifica una interfaz en el Grupo de Bridge así como el IP Address del router en la red del Grupo de Bridge, y usted puede definir solamente una ruta predeterminado. Si usted tiene tráfico de administración de más de una red del Grupo de Bridge, usted necesita especificar una Static ruta que identifique la red de la cual usted cuenta con el tráfico de administración.
- Para el modo de contexto múltiple, cada contexto debe utilizar diversas interfaces. Usted no puede compartir una interfaz a través de los contextos.
- Para el modo de contexto múltiple, cada contexto utiliza típicamente diversas subredes. Usted puede utilizar las subredes que solapan, pero su topología de red requiere el router y la configuración del NAT hacerla posible de un punto de vista de la encaminamiento.Usted debe utilizar una lista de acceso ampliada para permitir el tráfico de la capa 3, tal como tráfico IP, con el FWSM. Usted puede también utilizar opcionalmente una lista de acceso del Ethertype para permitir el tráfico no IP a través.

Direcciones MAC permitidas

Estos direccionamientos del MAC de destino se permiten con el Firewall transparente. Cualquier dirección MAC no en esta lista se cae.

- VERDAD la dirección MAC del destino del broadcast igual al FFFF.FFFF.FFFF
- Multicast MAC Address del IPv4 de 0100.5E00.0000 a 0100.5EFE.FFFF
- Direcciones MAC del Multicast IPv6 a partir del 3333.0000.0000 a 3333.FFFF.FFFF
- Dirección Multicast BPDU igual a 0100.0CCC.CCCD
- Multicast MAC Address del APPLETALK a partir de la 0900.0700.0000 a 0900.07FF.FFFF

Características no admitidas

Estas características no se soportan en el modo transparente:

- NAT /PATEl NAT se realiza en el router ascendente.**Nota:** El NAT/PAT se soporta en el Firewall transparente para las versiones del FWSM versión 3.2 y posterior.
- Dynamic Routing Protocol (tales como RIP, EIGRP, OSPF)Usted puede agregar las Static rutas para el tráfico que origina en el FWSM. Usted puede también permitir los Dynamic Routing Protocol con el FWSM con una lista de acceso ampliada.
- IPv6 para la dirección IP del Grupo de Bridge.Sin embargo, usted puede pasar el Ethertype del IPv6 usando una lista de acceso del Ethertype.
- Relé DHCPEl Firewall transparente puede actuar como servidor DHCP, pero no soporta los comandos del relé DHCP. El relé DHCP no se requiere porque usted puede permitir que el tráfico del DHCP pase a través con una lista de acceso ampliada.
- Calidad del servicio (QoS)
- Multicast (multidifusión)Usted puede permitir el tráfico Multicast con el FWSM si usted lo permite en una lista de acceso ampliada. Refiera al paso a través de la sección del tráfico

para más información.
- Terminación VPN para el tráfico directoEl Firewall transparente soporta los túneles del VPN de sitio a sitio para las Conexiones de Administración solamente. No termina las conexiones VPN para el tráfico con el FWSM. Usted puede pasar el tráfico VPN con el FWSM con una lista de acceso ampliada, pero no termina las conexiones de la NON-Administración.
- LoopGuard en el SwitchNo habilite LoopGuard global en el Switch si el FWSM está en el modo transparente. LoopGuard se aplica automáticamente al EtherChannel interno entre el Switch y el FWSM, así que después de una Conmutación por falla y de un failback, LoopGuard hace la unidad secundaria ser desconectado porque el EtherChannel entra estado err-disable.

Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

El diagrama de la red muestra a firewall network transparente típico donde están los dispositivos externos en la misma subred como los dispositivos internos. El router interno y los host aparecen ser conectados directamente con el router externo.

Configuraciones

Usted puede fijar cada contexto para ejecutarse en el modo firewall ruteado (el valor por defecto) o el modo firewall transparente.

Cuando usted cambia los modos, el FWSM borra la configuración porque muchos comandos no se soportan para los modos Both. Si usted tiene ya una configuración poblada, esté seguro de sostener su configuración antes de que usted cambie el modo. Usted puede utilizar este respaldo para la referencia al crear su nueva configuración.

Si usted descarga una configuración de texto al FWSM que cambia el modo con el comando transparent del Firewall, esté seguro de poner el comando en la cima de la configuración. El FWSM cambia el modo tan pronto como lea el comando y después continúe leyendo la configuración que usted descargó. Si el comando es más adelante en la configuración, el FWSM borra todas las líneas precedentes en la configuración.

Para fijar el modo a transparente, ingrese este comando en cada contexto:

```
hostname(config)#firewall transparent
```

Para fijar el modo a ruteado, ingrese este comando en cada contexto:

```
hostname(config)#no firewall transparent
```

Los datos se mueven a través del Firewall transparente en diversos escenarios

Accesos del usuario interiores el servidor de correo electrónico exterior

El usuario en los accesos de red interna que el servidor de correo electrónico puso en Internet (afuera). El FWSM recibe el paquete y agrega el MAC Address de origen a la tabla de la dirección MAC, si procede. Porque es una nueva sesión, verifica que el paquete esté permitido de acuerdo con los términos de la política de seguridad (Listas de acceso, filtros, o AAA).

Nota: Para el modo de contexto múltiple, el FWSM primero clasifica el paquete de acuerdo con una interfaz única.

El FWSM registra que una sesión está establecida. Si la dirección MAC del destino está en su tabla, el FWSM adelante la interfaz exterior de los del paquete. La dirección MAC del destino es la del router ascendente, 192.168.1.2. Si la dirección MAC del destino no está en la tabla FWSM, el FWSM intenta descubrir la dirección MAC cuando envía un pedido ARP y un ping. Se cae el primer paquete.

El servidor de correo electrónico responde a la petición. Porque la sesión se establece ya, el paquete desvía las muchas operaciones de búsqueda asociadas a una nueva conexión. El FWSM adelante el paquete al usuario interior.

Un usuario interior visita a un servidor de correo electrónico con el NAT

Si usted habilita el NAT en el router de Internet, el flujo del paquete a través del router de Internet se cambia levemente.

El usuario en los accesos de red interna que el servidor de correo electrónico puso en Internet (afuera). El FWSM recibe el paquete y agrega el MAC Address de origen a la tabla de la dirección MAC, si procede. Porque es una nueva sesión, verifica que el paquete esté permitido de acuerdo con los términos de la política de seguridad (Listas de acceso, filtros, o AAA).

Nota: Para el modo de contexto múltiple, el FWSM primero clasifica el paquete de acuerdo con una interfaz única.

El router de Internet traduce a la dirección real del host A (192.168.1.5) al direccionamiento asociado del router de Internet (172.16.1.1). Porque el direccionamiento asociado no está en la misma red que la interfaz exterior, aseegurese que el router ascendente tiene una Static ruta a la red asociada esas puntas al FWSM.

El FWSM registra que una sesión está establecida y adelante el paquete de la interfaz exterior. Si la dirección MAC del destino está en su tabla, el FWSM adelante la interfaz exterior de los del paquete. La dirección MAC del destino es la del router ascendente, 172.16.1.1. Si la dirección MAC del destino no está en la tabla FWSM, el FWSM intenta descubrir la dirección MAC cuando envía un pedido ARP y un ping. Se cae el primer paquete.

El servidor de correo electrónico responde a la petición. Porque la sesión se establece ya, el paquete desvía las muchas operaciones de búsqueda asociadas a una nueva conexión. El FWSM realiza el NAT cuando traduce el direccionamiento asociado a la dirección real, 192.168.1.5.

Un usuario interior visita a un servidor Web interior

Si el host A intenta acceder al servidor Web interior (10.1.1.1), el host A (192.168.1.5) envía el paquete de pedidos al router de Internet (puesto que es un default gateway) con el FWSM del

interior al exterior. Entonces el paquete se reorienta al servidor Web (10.1.1.1) a través del FWSM (afuera ante el interior) y del router interno.

Nota: El paquete de pedidos vuelve al servidor Web solamente si el FWSM tiene una lista de acceso para permitir el tráfico del exterior al interior.

Para resolver este problema, cambie el default gateway para el host A (10.1.1.1) para ser el router interno (192.168.1.3) en vez del router de Internet (192.168.1.2). Esto evita cualquier tráfico innecesario enviado al gateway exterior y reorienta los acontecimientos en el router externo (router de Internet). También resuelve de la manera reversa, es decir, cuando el servidor Web o ninguno recibe el presente (de 10.1.1.0/24) en el interior de los intentos del router interno para acceder el host A (192.168.1.5).

Un usuario externo visita a un servidor Web en la red interna

Estos pasos describen cómo los datos se mueven con el FWSM:

1. Un usuario en la red externa pide una página web del servidor Web interior. El FWSM recibe el paquete y agrega el MAC Address de origen a la tabla de la dirección MAC, si procede. Porque es una nueva sesión, verifica que el paquete esté permitido de acuerdo con los términos de la política de seguridad (Listas de acceso, filtros, o AAA).**Nota:** Para el modo de contexto múltiple, el FWSM primero clasifica el paquete de acuerdo con una interfaz única.
2. El FWSM registra que una sesión está establecida solamente si el usuario externo tiene el acceso válido al servidor Web interno. La lista de acceso se debe configurar para permitir que el usuario externo consiga el acceso para el servidor Web.
3. Si la dirección MAC del destino está en su tabla, el FWSM adelante la interfaz interior de los del paquete. La dirección MAC del destino es la del router en sentido descendente, 192.168.1.3.
4. Si la dirección MAC del destino no está en la tabla FWSM, el FWSM intenta descubrir la dirección MAC cuando envía un pedido ARP y un ping. Se cae el primer paquete.
5. El servidor Web responde a la petición. Porque la sesión se establece ya, el paquete desvía las muchas operaciones de búsqueda asociadas a una nueva conexión. El FWSM adelante el paquete al usuario externo.

Un usuario externo intenta acceder un host interior

Un usuario en la red externa intenta alcanzar un host interior. El FWSM recibe el paquete y agrega el MAC Address de origen a la tabla de la dirección MAC, si procede. Porque es una nueva sesión, verifica si el paquete esté permitido de acuerdo con los términos de la política de seguridad (Listas de acceso, filtros, o AAA).

Nota: Para el modo de contexto múltiple, el FWSM primero clasifica el paquete de acuerdo con una interfaz única.

Se niega el paquete, y el FWSM cae el paquete porque el usuario externo no tiene el acceso al host interior. Si el usuario externo intenta atacar la red interna, el FWSM emplea muchas Tecnologías para determinar si un paquete es válido para ya una sesión establecida.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

```
cisco(config)#show firewall Firewall mode: Transparent
```

Troubleshooting

Pase con el tráfico

En el Firewall transparente, pasar el tráfico Multicast del alto a bajo y a bajo a las altas listas de acceso se requieren. En los Firewall normales del alto al punto bajo no se requiere.

Nota: La dirección Multicast (224.0.0.9) puede nunca ser dirección de origen para el tráfico de retorno, así que él no será permitida volverse adentro, por eso necesitamos los ACL de adentro a hacia fuera y hacia fuera a adentro.

Por ejemplo, para pasar con el tráfico del RIP, la lista de acceso transparente del Firewall sería similar a este ejemplo:

RIP

ACL exterior (de hacia fuera a adentro):

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

ACL interior (por dentro al exterior):

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

EIGRP a ejecutarse:

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
 access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

Para OSPF (Abrir la ruta más corta en primer lugar)

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
 access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside sourec ) host ( inside source )
access-group outside in interafce outside
```

VLA N MSFC contra el VLA N FWSM

En el modo transparente, no es necesario tener los mismos VLA N en la interfaz MSFC y el FWSM, puesto que es un tipo de bridging.

Información Relacionada

- Cisco PIX Firewall Software
- Solicitudes de Comentarios (RFC)
- Avisos de campos de productos de seguridad (incluido PIX)
- Referencias de Comandos de Cisco Secure PIX Firewall
- PIX/ASA: Ejemplo transparente de la configuración de escudo de protección
- Soporte Técnico y Documentación - Cisco Systems