FWSM: Fallas debido del tráfico del Troubleshooting para perjudicar Xlates

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Síntomas
Topología lógica
Configuración pertinente
Conductas observadas
Activadores
Soluciones
Configuraciones de ruteo incorrectas de la resolución
Intra-interfaz del permiso del trafico de seguridad igual de la neutralización
Caiga los paquetes que llegan en una interfaz incorrecta (los ACL o el uRPF)
Habilite xlate-puente
Resumen
Información Relacionada

Introducción

Debido al diseño del procesamiento de paquetes del Firewall Services Module (FWSM), las xlates construidas por paquetes ruteados incorrectamente pueden causar errores de tráfico para las conexiones a través del firewall. Para seleccionar una interfaz de egreso para un paquete de entrada, las en primer lugar controles FWSM para ver si el IP de destino del paquete de entrada hace juego cualquier IP/Network global existente en una traducción de NAT (xlate) para esa interfaz en su tabla del xlate. Si se encuentra una coincidencia, la interfaz de egreso simplemente se elige basada en la interfaz local en la entrada del xlate y el Firewall no consulta la tabla de ruteo para tomar la decisión de la interfaz de egreso.

El comportamiento predeterminado del FWSM es construir una entrada del xlate para el IP de la fuente de cualquier paquete permitido que se reciba en una de sus interfaces. Si un paquete se rutea a través de la red incorrectamente (para cualquier número de razones) y llega entrante en la interfaz incorrecta del FWSM, un xlate se construye para reflejar esto. Cuando ocurre esto, las entradas en la tabla del xlate pueden reemplazar las entradas en la tabla de ruteo y causar los errores del tráfico para los destinos afectados.

Este documento describe los síntomas y los activadores para este problema, cómo diagnosticarlo, y proporciona las soluciones para evitar que ocurra.

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de los FWSM.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Síntomas

Topología lógica

Configuración pertinente

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.100.50 255.255.255.0
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.1.50 255.255.255.0
!
interface Vlan20
 nameif dmz
 security-level 50
 ip address 10.20.1.50 255.255.255.0
!
same-security-traffic permit intra-interface
access-list outside_in extended permit tcp any host 10.30.1.1 eq www
access-list inside_in extended permit ip any any
access-group inside_in in interface inside
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.254
route dmz 10.30.1.0 255.255.255.0 10.20.1.254
```

Conductas observadas

Conexiones del PC del cliente en 172.16.1.10 al servidor Web en el fall de 10.30.1.1.

Una captura de paquetes en la **interfaz exterior** muestra un TCP SYN PC del cliente de la llegada la interfaz FWSM.

```
FWSM# show capture outside
3 packets seen, 3 packets captured
```

```
   1: 13:58:09.280752960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   2: 13:58:12.280755950 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   3: 13:58:18.280761960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
3 packets shown
```

Una captura de paquetes en la interfaz del **dmz** no muestra ese paquete que sale del Firewall.

```
FWSM# show capture dmz
0 packet seen, 0 packet captured
0 packet shown
```

No se construye ninguna entrada en la tabla de conexiones FWSM y los Syslog no muestran relacionado con la información al cliente o a los dirección IP del servidor.

Activadores

En un nivel fundamental, este problema es causado por una entrada en la tabla del xlate FWSM que fue construida por incorrectamente un paquete ruteado. Debido a la manera que se diseña el proceso del paquete FWSM, el Firewall marca la tabla del xlate antes de que marque la tabla de ruteo para determinar la interfaz de egreso. Como consecuencia, si un paquete hace juego un xlate existente la interfaz de egreso será seleccionada sobre la base de esa entrada, incluso si la entrada está en conflicto con qué se enumera en la tabla de ruteo. Es decir la tabla del xlate toma la precedencia sobre la tabla de ruteo.

Para diagnosticar este problema, marque la salida del **comando debug del xlate de la demostración**:

```
FWSM# show xlate debug
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
3 in use, 3 most used
NAT from inside:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:00 timeout 3:00:00 connections
0
NAT from inside:10.30.1.1 to inside:10.30.1.1 flags Ii idle 0:00:07 timeout 3:00:00 connections
0

NAT from dmz:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:10 timeout 3:00:00 connections 0
```

Nota: La palabra clave del debug en el xlate de la demostración es crucial. Sin ella, las entradas del xlate no incluirán los nombres de la interfaz que la entrada está asociada a.

La tabla del xlate muestra que hay 3 xlates construidos para el servidor Web. El primer xlate se construye entre la **interfaz interior** y la **interfaz exterior**. El segundo xlate se construye como xlate hairpinned o u-dado vuelta en la **interfaz interior**. El tercer xlate se construye entre el **dmz** y la **interfaz exterior**. El indicador I indica que esto es un xlate de la identidad y el IP no se está traduciendo realmente.

La primera interfaz enumerada en la entrada es “la interfaz real” o “local” donde el IP se supone para existir realmente. La segunda interfaz enumerada es la interfaz asociada” o “global” “donde se está traduciendo el IP. Ningunos de estos xlates mostrados están correctos. Esto es porque el servidor Web (10.30.1.1) existe realmente detrás de la interfaz del **dmz**. El tercer xlate está correcto para este diseño de red.

La falla de conexión ocurre debido al primer xlate enumerado en la tabla. Cuando el cliente paquete TCP Syn llega en la interfaz exterior destinada a 10.30.1.1, el FWSM marca la tabla del

xlate y hace juego la primera entrada. Esta entrada indica que el paquete salida en la **interfaz interior**, que es incorrecta, y el paquete blackholed.

Por abandono, el FWSM construirá automáticamente un xlate de la identidad para cualquier tráfico que no haga juego una regla explícitamente configurada NAT. Debido a esto, incluso si un paquete llega erróneamente en una interfaz incorrecta, un xlate será construido. Específicamente para este caso, los paquetes originados de 10.30.1.1 llegaron entrante en la **interfaz interior** en vez de la llegada en la interfaz del **dmz** como se espera.

El primer xlate (**interior > afuera**) fue construido cuando el servidor Web intentó hacer ping una dirección IP inexistente (10.199.199.1). El pedido de eco dejado el servidor Web destinado a su default gateway (el router DMZ). El router DMZ remitió el paquete hacia el router interno, por su Static ruta:

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Porque no existe la red 10.199.199.0/24 realmente dondequiera, el router interno sigue simplemente su ruta predeterminado y envía el paquete a la **interfaz interior** FWSM:

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

Asimismo, el FWSM también no tiene una ruta para la red de destino. Por lo tanto, selecciona la interfaz exterior como la interfaz de egreso y construye un xlate de la identidad por dentro de **> exterior**:

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.100.254, outside
```

El segundo xlate (**interior > dentro**) fue construido cuando el servidor Web intentado para acceder al servidor DNS mientras que la interfaz de 10.40.1.254 del router interno estaba temporalmente abajo de debido a un flap del link. La petición DNS dejada el servidor Web destinado a su default gateway (el router DMZ). El router DMZ remitió el paquete hacia el router interno, por su Static ruta:

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Sin embargo, la interfaz del router interno conectada con la red 10.40.1.0/24 estaba temporalmente abajo y su Routeconectad para esta red faltaba directamente. Por lo tanto, la única ruta que correspondía con en la tabla de ruteo era la ruta predeterminado detrás hacia el FWSM:

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

El paquete fue ruteado a la **interfaz interior** FWSM. La tabla de ruteo FWSM indicó que la red de destino de 10.40.1.0/24 existió detrás de la misma **interfaz interior**:

```
S    10.40.1.0 255.255.255.0 [1/0] via 10.10.1.254, inside
```

Porque habilitan al **comando intra-interface del permiso del trafico de seguridad igual**, el FWSM permitirá que el xlate u-dado vuelta sea construido.

Para resumir, el primer xlate fue accionado por:

- Una ruta amplia 10.0.0.0/8 configurada en el router DMZ
- **Un IP del permiso cualquier cualquier ACL** configurado en la interfaz interior FWSM

El segundo xlate fue accionado por:

- Una interfaz inestable en el router interno
- **intra-interfaz del permiso del trafico de seguridad igual** configurada en el FWSM

Soluciones

Hay muchas diversas Soluciones posibles a este problema. Sobre todo, borrar el xlate de la tabla debe permitir que el tráfico comience a trabajar otra vez hasta que se reconstruya el xlate. Esto se puede hacer con el **comando clear xlate**. Por ejemplo:

```
FWSM# clear xlate interface inside local 10.30.1.1 global 10.30.1.1
```

Nota: Cualquier conexión que esté utilizando los xlate borrados también será derribada.

Una vez que eso es completo, el foco debe estar en evitar que los xlates vuelvan. A menudo las épocas, la mayoría de la forma más utilizada de hacer esto es reparar la configuración de ruteo en el entorno para evitar que el tráfico llegue en la interfaz incorrecta FWSM. El FWSM también ofrece un puñado de opciones de configuración de abordar estos problemas.

Configuraciones de ruteo incorrectas de la resolución

Esta solución toma las hojas de operación (planning) cuidadosas y una comprensión profunda del entorno de red. En el primer ejemplo anterior, la ruta 10.0.0.0/8 en el router DMZ es técnico incorrecta puesto que la red entera de /8 no existe más allá de su interfaz de 10.50.1.253. En lugar, algunas opciones que existen son:

- Elimine 10.50.1.0/24 la red todos junto y rutee simplemente todo el tráfico con el FWSM. Esto también proporciona una mejores segmentación y Seguridad entre el interior y las redes DMZ.
- Configure una Static ruta en el DMZ para solamente 10.40.1.0/24 y quite la ruta 10.0.0.0/8.
- Utilice un Dynamic Routing Protocol entre el Routers interior y DMZ para hacer publicidad correctamente solamente de las redes que existen realmente.

Hay a menudo muchas posibilidades de ajustar la configuración de ruteo, pero el objetivo final es asegurarse de que el tráfico de un host dado puede llegar solamente en una sola interfaz FWSM.

Intra-interfaz del permiso del trafico de seguridad igual de la neutralización

El comando intra-interface del permiso del trafico de seguridad igual permite el FWSM al giro de 180 grados o al tráfico de la horquilla en una interfaz. Esto significa que un paquete puede ingresar el Firewall en la misma interfaz que sale encendido. Estas funciones se inhabilitan por abandono y tienen muy poco uso en la mayoría de los diseños FWSM. Porque el FWSM utiliza las interfaces VLAN, trafique que las estancias dentro del mismo VLA N se deben nunca procesar por el FWSM.

En el segundo ejemplo anterior, el **comando intra-interface del permiso del trafico de seguridad igual** permitió un paquete a ingresa y deja la **interfaz interior**. Inhabilitar la intra-**interfaz del permiso del trafico de seguridad igual** prevendría este comportamiento y caería el paquete antes de que un xlate fuera construido nunca:

```
FWSM(config)# no same-security-traffic permit intra-interface
```

Caiga los paquetes que llegan en una interfaz incorrecta (los ACL o el uRPF)

En ambos ejemplos anteriores, los xlates fueron construidos cuando un paquete del servidor Web llegó incorrectamente en la **interfaz interior**. Para prevenir el problema todo junto, el FWSM se puede configurar para caer los paquetes que llegan en la interfaz incorrecta.

El FWSM requiere que todo el tráfico sea permitido por un ACL antes de que pueda pasar. Por lo tanto, estas funciones pueden ser alcanzadas solamente permitiendo el tráfico de las redes de origen apropiadas en cada interfaz. En los ejemplos anteriores, la **interfaz interior** permite todo el tráfico IP:

```
access-list inside_in extended permit ip any any
```

En lugar, esto se debe cambiar para permitir solamente el tráfico de las 10.10.1.0/24 y 10.40.1.0/24 subredes:

```
access-list inside_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list inside_in extended permit ip 10.40.1.0 255.255.255.0 any
```

En algunos entornos, esto no es una opción factible debido al tamaño y/o a la escala de las diversas redes que pasan con el FWSM. Sin embargo, estas funciones se pueden alcanzar más simplemente usando una característica llamada Unicast Reverse Path Forwarding (uRPF).

Cuando se habilita la característica del uRPF, el FWSM comparará la dirección IP de origen del primer paquete de cada conexión contra su tabla de ruteo. Si la ruta se encuentra que no hace juego para arriba con la interfaz que llegó el paquete encendido, ese paquete será caído debido a una falla de RPF.

En el ejemplo anterior, el FWSM tiene una Static ruta que utilice la interfaz del **dmz** para alcanzar la red 10.30.1.0/24. Por lo tanto, si el uRPF se habilita en la **interfaz interior**, los paquetes originados del servidor Web (10.30.1.1) que llega incorrectamente en la **interfaz interior** serán caídos.

Para habilitar el uRPF, aplique el **IP verifican el** comando del **trayecto inverso a** cada interfaz en la pregunta. Por ejemplo:

```
FWSM(config)# ip verify reverse-path interface inside
```

Xlate-puente del permiso

En ambos ejemplos anteriores, los xlates se crean con los indicadores Ii. Estos indicadores indican que el xlate es una traducción de la identidad (i) que originó en una interfaz de la gran seguridad (i). Por abandono, el FWSM construirá estos xlates para cualquier tráfico que no haga juego una regla explícita NAT/PAT. Para inhabilitar este comportamiento, el comando de xlate-**puente** se puede habilitar en FWSM 3.2(1) y posterior:

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

Esta característica prevendrá el FWSM de los xlates de la identidad del edificio en el primer lugar. Así, el tráfico en los ejemplos anteriores no sería reorientado a una interfaz incorrecta debido a una entrada de tabla del xlate. Sin embargo, el tráfico todavía pasará con el FWSM sin traducir.

Resumen

Para determinar la interfaz de egreso para un paquete, el FWSM consultará siempre su tabla del xlate antes de mirar su tabla de ruteo. Si ese paquete hace juego un xlate existente, la interfaz de egreso se selecciona sobre la base de la interfaz asociada de los xlate. Esto sucede sin importar cualquier contradicción que se pudiera encontrar en la tabla de ruteo. De esta manera, la tabla del xlate toma la precedencia sobre la tabla de ruteo.

Porque el FWSM construirá siempre una entrada del xlate para todas las nuevas conexiones por

abandono, éste puede causar los errores del tráfico en caso de que los paquetes ruteados hagan incorrectamente el FWSM construir un xlate. Según lo delineado arriba, hay muchos escenarios posibles donde éste puede ocurrir pero todo se relaciona de nuevo a un paquete que es recibido en una interfaz incorrecta. Este documento cubrió estos posibles problemas:

- Un config amplio de la encaminamiento envía los paquetes en una dirección incorrecta
- El FWSM se configura para permitir el tráfico de las redes de origen incorrectas
- El FWSM se configura al tráfico hairpin/u-turn

Para restablecer rápidamente la Conectividad para las conexiones que fallan debido a un xlate incorrecto, borre la entrada con el **comando clear xlate**. Este documento también cubrió las soluciones múltiples para evitar que estos xlates vuelvan en el futuro, incluyendo:

- Configuraciones de ruteo incorrectas de la resolución usando rutas más específicas
- Intra-interfaz del permiso del trafico de seguridad igual de la neutralización
- Paquetes del descenso que llegan en una interfaz incorrecta usando los ACL o el uRPF
- Xlate-puente del permiso

Información Relacionada

- Referencia de comandos: el IP verifica el trayecto inverso
- Referencia de comandos: xlate-puente
- Soporte Técnico y Documentación - Cisco Systems