El tráfico UDP con el ASA falla después de que se vuelva el link del ISP primario Online en una configuración dual ISP

Contenido

Introducción

Si un dispositivo de seguridad adaptante (ASA) tiene dos interfaces de egreso por la subred de destino y la ruta preferida a un destino se quita de la tabla de ruteo por algún tiempo, las conexiones del User Datagram Protocol (UDP) pueden fallar cuando la ruta preferida consigue reagregada a la tabla de ruteo. Las conexiones TCP se pudieron también afectar por el problema, pero puesto que el TCP detecta la pérdida del paquete, estas conexiones son derribadas automáticamente por los puntos finales, y reconstruido usando las más rutas óptimo después de las rutas cambie.

Este problema puede también ser considerado si se utiliza un Routing Protocol y un cambio de la topología acciona un cambio en la tabla de ruteo en el ASA.

Antes de comenzar

Requisitos

Para encontrar este problema, la tabla de ruteo ASA debe cambiar. Esto es común con los links duales ISP en una moda redundante o cuando el ASA está aprendiendo las rutas vía un IGP (OSPF, EIGRP, RIP).

Este problema ocurre cuando se vuelve el link del ISP primario en línea o el IGP dicho ve un reconvergence debido a cuál se substituye una menos ruta preferida que era utilizada por el ASA por la bajo-métrico-ruta preferida. Usted entonces vería las conexiones duraderas, tales como registros del SORBO UDP, GRE, etc, fallando una vez que el primario o la ruta preferida está reinstalado en la tabla de ruteo ASA.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cualquier dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA
- Versiones de ASA 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) y posterior

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Problema

Si una entrada de la tabla de ruteo se quita de la tabla de ruteo ASA y no hay rutas fuera de una interfaz para alcanzar un destino, las conexiones construidas con el Firewall con ese destino no nativo serán borradas por el ASA. Esto ocurre para poder construir las conexiones otra vez usando una diversa interfaz con las entradas de ruteo para el presente del destino.

Sin embargo, si rutas más específicas se agregan de nuevo a la tabla, las conexiones no serán puestas al día para utilizar las nuevas, más específicas rutas, y continuarán utilizando la interfaz menos-óptima.

Por ejemplo, considere que el Firewall tiene dos interfaces que hagan frente a Internet - “exterior” y “respaldo” - y estas dos rutas existen en la configuración ASA:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Si el exterior y las Interfaces de respaldo están “encima de”, después las conexiones construyeron saliente con el Firewall utilizarán la interfaz exterior, pues tiene el métrico preferida de 1. Si se apaga la interfaz exterior (o la función de supervisión SLA que está siguiendo la ruta encuentra una pérdida de conectividad al IP seguido), las conexiones usando la interfaz exterior serían rasgadas abajo y reconstruidas usando la Interfaz de respaldo, pues la Interfaz de respaldo es la única interfaz con una ruta al destino.

El problema ocurre cuando la interfaz exterior se trae la salvaguardia o la ruta seguida se convierte en la ruta favorecida otra vez. La tabla de ruteo se pone al día para preferir la ruta original, pero las conexiones existentes continúan existiendo en el ASA y atravesando la Interfaz de respaldo y no se borran y se reconstruyen en la interfaz exterior con el métrico más-preferida. Esto es porque la ruta predeterminado de reserva todavía existe en la tabla de ruteo interfaz-específica ASA. La conexión continúa utilizando la interfaz con la menos ruta preferida hasta que se borre la conexión; en el caso del UDP, esto pudo ser indefinido.

Esta situación puede causar los problemas con las conexiones duraderas, tales como registros externos del SORBO u otras conexiones UDP.

Solución

Para abordar este problema específico, una nueva función fue agregada al ASA que hará las conexiones ser derribado y ser reconstruido en una nueva interfaz si una más ruta preferida al destino se agrega a la tabla de ruteo. Para activar la característica (se inhabilita por abandono),

fije un descanso no-cero al comando del **descanso flotar-CONN**. Este descanso (especificado en el HH: MILÍMETRO: El SS) especifica el tiempo que el ASA espera antes de que derribe la conexión una más ruta preferida se agrega una vez de nuevo a la tabla de ruteo:

Éste es un ejemplo CLI de habilitar la característica. Con este CLI, si un paquete se recibe en una conexión existente para la cual haya un diferente ahora, más ruta preferida al destino, la conexión será derribada 1 minuto más adelante (y reconstruido usando el nuevo, más ruta preferida):

```
ASA# config terminal ASA(config)# timeout floating-conn 0:01:00 ASA(config)# end ASA# show run
timeout timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:01:00
absolute timeout tcp-proxy-reassembly 0:01:00 timeout xlate 0:01:00 timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00 ASA#
```

Esta característica se agrega a la plataforma ASA en las versiones 8.2(5), 8.3(2)12, 8.4(1)1, y 8.5(1), incluyendo versiones posteriores del software ASA.

Si usted funciona con una versión del código ASA que no implementa esta característica, un workaround al problema sería vaciar manualmente las conexiones UDP que continúan tomando la menos ruta preferida a pesar de una mejor ruta que es hecha disponible vía un ***<IP>* claro del host local** o el ***<IP>* *claro*-CONN**.

Las listas de referencia de comandos esta nueva función bajo sección del descanso.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems