El tráfico UDP a través de ASA falla después de que el link ISP primario vuelva a estar en línea en una configuración ISP dual

Contenido

Introducción

Si un dispositivo de seguridad adaptable (ASA) tiene dos interfaces de salida por subred de destino y la ruta preferida a un destino se elimina de la tabla de routing durante algún tiempo, las conexiones de protocolo de datagramas de usuario (UDP) pueden fallar cuando se vuelve a agregar la ruta preferida a la tabla de routing. Las conexiones TCP también pueden verse afectadas por el problema, pero dado que TCP detecta la pérdida de paquetes, estas conexiones se desactivan automáticamente por los terminales y se vuelven a generar usando las rutas más óptimas después de que cambien las rutas.

Este problema también se puede ver si se utiliza un protocolo de ruteo y un cambio de topología provoca un cambio en la tabla de ruteo en el ASA.

Antes de comenzar

Requirements

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

Este problema ocurre cuando el link ISP primario vuelve a estar en línea o dicho IGP ve una reconvergencia debido a la cual una ruta menos preferida que estaba siendo utilizada por el ASA se reemplaza por la ruta más baja. A continuación, verá conexiones de larga duración, como registros de SIP UDP, GRE, etc., que fallan una vez que la ruta principal o preferida se reinstala en la tabla de ruteo de ASA.

Componentes Utilizados

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

- Cualquier dispositivo de seguridad adaptable Cisco ASA serie 5500
- ASA versiones 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) y posteriores

Convenciones

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

Problema

Si se elimina una entrada de la tabla de ruteo de la tabla de ruteo del ASA y no hay rutas fuera de una interfaz para alcanzar un destino, las conexiones construidas a través del firewall con ese destino externo serán eliminadas por el ASA. Esto ocurre para que las conexiones se puedan construir de nuevo usando una interfaz diferente con entradas de ruteo para el destino presente.

Sin embargo, si se agregan rutas más específicas de nuevo a la tabla, las conexiones no se actualizarán para utilizar las rutas nuevas y más específicas, y continuarán usando la interfaz menos óptima.

Por ejemplo, tenga en cuenta que el firewall tiene dos interfaces que se enfrentan a Internet - "exterior" y "copia de seguridad" - y estas dos rutas existen en la configuración del 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 las interfaces externa y de respaldo están "funcionando", las conexiones generadas de salida a través del firewall utilizarán la interfaz externa, ya que tiene la métrica preferida de 1. Si se apaga la interfaz externa (o la función de supervisión de SLA que realiza el seguimiento de la ruta encuentra una pérdida de conectividad con la IP de seguimiento), las conexiones que utilizan la interfaz externa se desactivarán y se reconstruirán usando la interfaz de respaldo, ya que la interfaz de respaldo es la única interfaz con una ruta hacia el destino.

El problema ocurre cuando la interfaz externa se vuelve a activar o la ruta rastreada se convierte en la ruta favorita de nuevo. La tabla de ruteo se actualiza para preferir la ruta original, pero las conexiones existentes continúan existiendo en el ASA y atravesando la interfaz de respaldo y NO se eliminan y se vuelven a crear en la interfaz exterior con la métrica más preferida. Esto se debe a que la ruta predeterminada de respaldo aún existe en la tabla de ruteo específica de la interfaz de ASA. La conexión continúa utilizando la interfaz con la ruta menos preferida hasta que se elimina la conexión; en el caso de UDP, esto podría ser indefinido.

Esta situación puede causar problemas con conexiones de larga duración, como registros SIP externos u otras conexiones UDP.

Solución

Para abordar este problema específico, se agregó una nueva función al ASA que hará que las conexiones sean desmontadas y reconstruidas en una nueva interfaz si se agrega una ruta más

preferida al destino a la tabla de ruteo. Para activar la función (está desactivada de forma predeterminada), establezca un tiempo de espera distinto de cero en el comando **timeout flotante-conn**. Este tiempo de espera (especificado en HH:MM:SS) especifica el tiempo que el ASA espera antes de que cierre la conexión una vez que se agrega una ruta preferida de nuevo a la tabla de ruteo:

Este es un ejemplo CLI de habilitación de la función. Con esta CLI, si se recibe un paquete en una conexión existente para la que ahora hay una ruta diferente y preferida al destino, la conexión se desactivará 1 minuto después (y se reconstruirá usando la nueva 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 función se agrega a la plataforma ASA en las versiones 8.2(5), 8.3(2)12, 8.4(1)1 y 8.5(1), incluidas las versiones posteriores del software ASA.

Si ejecuta una versión del código ASA que no implementa esta función, una solución alternativa al problema sería vaciar manualmente las conexiones UDP que siguen tomando la ruta menos preferida a pesar de que se está poniendo a disposición una mejor ruta a través de un **clear local-host** *<IP>* o **clear-conn** *<IP>* .

La referencia de comandos enumera esta nueva función en la sección timeout.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems