El ASA tiene CPU elevada uso debido a un loop del tráfico cuando desconexión de los clientes VPN

Contenido

Introducción

Este documento describe un problema frecuente que ocurra cuando la desconexión de los clientes VPN de un dispositivo de seguridad adaptante de Cisco (ASA) ese se ejecuta como headend del VPN de acceso remoto. Este documento también describe la situación donde un loop del tráfico ocurre cuando desconexión de los usuarios de VPN de un Firewall ASA. Este documento no cubre cómo configurar o configurar el Acceso Remoto al VPN, sólo la situación específica que se presenta de ciertas configuraciones de ruteo comunes.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del VPN de acceso remoto en el ASA
- Conceptos de ruteo de la capa básica 3

Componentes Utilizados

La información en este documento se basa en un modelo 5520 ASA que funcione con la versión del código ASA 9.1(1).

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.

Productos Relacionados

Este documento se puede utilizar con estas versiones de software y hardware:

- Cualquier modelo ASA
- Cualquier versión del código ASA

Antecedentes

Cuando un usuario conecta con el ASA como concentrador del VPN de acceso remoto, el ASA instala una ruta basada en el host en la tabla de ruteo ASA que rutea el tráfico a esa interfaz exterior de los del cliente VPN (hacia Internet). Cuando las desconexiones de ese usuario, la ruta se quitan de la tabla, y los paquetes en la red interna (destinada a ese usuario de VPN disconnected) pudo ser colocado entre el ASA y un dispositivo de ruteo interno.

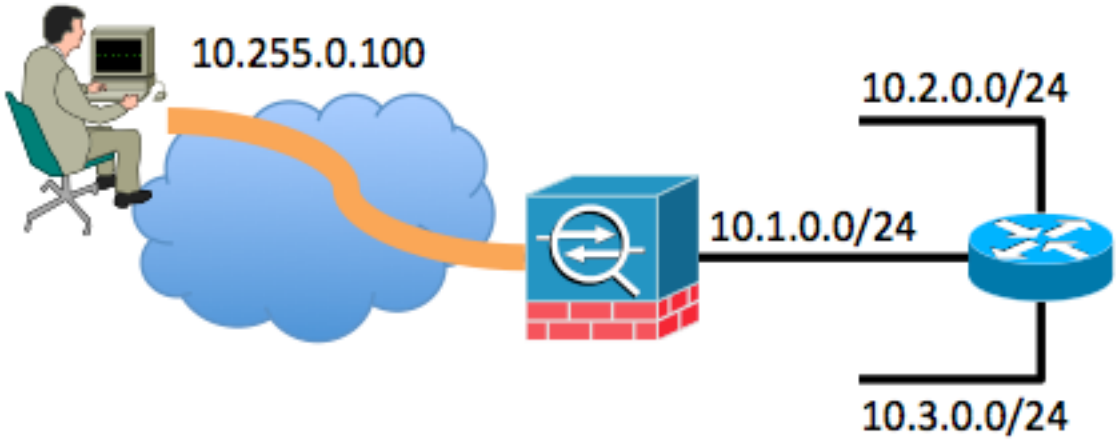
Otro problema es que los paquetes de broadcast dirigidos (de la red) (generados por el retiro de los clientes VPN) se pudieron remitir por el ASA como trama de unidifusión hacia la red interna. Esto pudo remitirlo de nuevo al ASA, que hace el paquete ser colocado hasta que expire el Time to Live (TTL).

Este documento explica estos problemas y muestra qué técnicas de configuración se pueden utilizar para prevenir el problema.

Problema: Paquetes destinados para un loop disconnected del cliente VPN dentro de la red interna

Cuando todavía las desconexiones de un usuario del VPN de acceso remoto de un Firewall ASA, los paquetes presentes en la red interna (destinada para esos usuarios disconnected) y IP asignada el direccionamiento VPN pudieron colocarse dentro de la red interna. Estos Packet Loop pudieron hacer el USO de la CPU en el ASA aumentar hasta las paradas de loop o debido al valor IP TTL en encabezado del paquete IP decrementing a 0, o el usuario vuelve a conectar y la dirección IP se reasigna a un cliente VPN.

Para entender este escenario mejor, considere esta topología:



En este ejemplo, han asignado el cliente de acceso remoto la dirección IP de 10.255.0.100. El ASA en este ejemplo está conectado con el mismo segmento de la red interna junto con un router. El router tiene dos capas adicionales 3 segmentos de red conectados con ella. La interfaz pertinente (encaminamiento) y las configuraciones VPN del ASA y del router se muestran en los ejemplos.

Los resaltados de la configuración ASA se muestran en este ejemplo:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

Los resaltados de la configuración del router se muestran en este ejemplo:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

La tabla de ruteo del router conectado con el interior del ASA tiene simplemente una ruta predeterminado señalada a la interfaz interior ASA de 10.1.0.1.

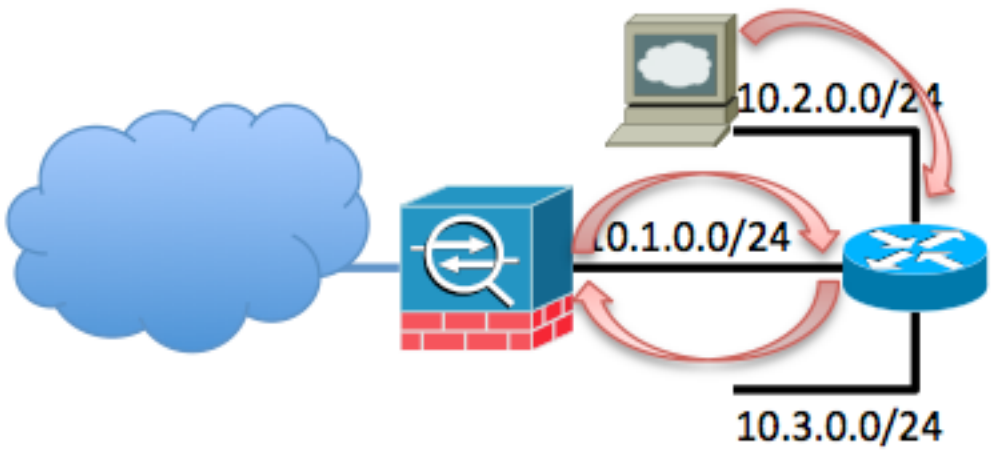
Mientras que el usuario está conectado vía el VPN con el ASA, la tabla de ruteo ASA muestra como sigue:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

El problema ocurre cuando las desconexiones del usuario del VPN de acceso remoto del VPN. En este momento, la ruta basada en el host se quita de la tabla de ruteo ASA. Si un host dentro de la red intenta enviar el tráfico al cliente VPN, ese tráfico es ruteado a la interfaz interior ASA por el router. Esta serie de pasos ocurre:

1. El paquete destinado a 10.255.0.100 llega en la interfaz interior del ASA.
2. Se realizan los controles estándar ACL.
3. La tabla de ruteo ASA se marca para determinar la interfaz de egreso para este tráfico.
4. El destino del paquete hace juego la ruta amplia 10.0.0.0/8 que las puntas retiran de la interfaz interior hacia el router.
5. El ASA verifica si se permite el tráfico de la conexión mediante pines - busca para la intra-**interfaz del permiso de la mismo-Seguridad** y encuentra que está permitido.
6. Una conexión se construye a y desde la interfaz interior y el paquete se devuelve al router como salto siguiente.
7. El router recibe un paquete destinado a 10.255.0.100 en la interfaz que hace frente al ASA. El router marca su tabla de ruteo para un salto siguiente conveniente. El router encuentra que el salto siguiente sería la interfaz interior ASA, y el paquete se envía al ASA.
8. regrese al paso 1

Un ejemplo se muestra aquí:



Este loop ocurre hasta TTL de los decrementos de este paquete a 0. Observe que el Firewall ASA no decrement el valor de TTL por abandono cuando procesa un paquete. El router decrements TTL mientras que rutea el paquete. Esto previene el acontecimiento de este loop indefinidamente, pero este loop aumenta la carga de tráfico en el ASA y hace el USO de la CPU clavar.

Problema: Los paquetes de broadcast dirigidos (de la red) generados por los clientes VPN se colocan en una red interna

Este problema es similar al primer problema. Si un cliente VPN genera un paquete del broadcast dirigido a su IP asignada subred (10.255.0.255 en el ejemplo anterior), después ese paquete se pudo remitir como trama de unidifusión por el ASA al router interno. El router interno pudo entonces remitirlo de nuevo al ASA, que hace el paquete colocar hasta que expire TTL.

Esta serie de eventos ocurre:

1. La máquina de cliente VPN genera un paquete destinado al direccionamiento 10.255.0.255 del broadcast de red, y el paquete llega el ASA.
2. El ASA trata este paquete como trama de unidifusión (debido a la tabla de ruteo) y adelante la al router interno.

3. El router interno, que también trata el paquete como trama de unidifusión, decrements TTL del paquete y adelante del él de nuevo al ASA.

4. Las repeticiones del proceso hasta TTL del paquete se reducen a 0.

Soluciones al problema

Hay varias soluciones potenciales a este problema. Dependiendo de la topología de red y de la situación específica, una solución pudo ser más fácil de implementar que otra.

Static ruta de la solución 1 para la interfaz del null0 (Versión de ASA 9.2.1 y posterior)

Cuando usted envía el tráfico a una interfaz del **null0**, causa los paquetes destinados a la red específicada que se caerá. Esta característica es útil cuando usted configura al agujero negro remotamente accionado (RTBH) para el Border Gateway Protocol (BGP). En esta situación, si usted configura una ruta al null0 para la subred del cliente de acceso remoto, fuerza el ASA para caer el tráfico destinado a los host en esa subred si una ruta más específica (proporcionada por el Reverse Route Injection) no está presente.

```
route Null0 10.255.0.0 255.255.255.0
```

Solución 2 - Utilice a una diversa agrupación IP para los clientes VPN

Esta solución es asignar a los usuarios de VPN remotos una dirección IP que no solape con ninguna subred de la red interna. Esto prevendría el ASA de los paquetes de la expedición destinados a esa subred VPN de nuevo al router interno si el usuario de VPN no fue conectado.

Solución 3 - Haga la tabla de ruteo ASA más específica para las rutas interno

Esta solución es asegurarse que la tabla de ruteo del ASA no tiene ninguna rutas muy amplia que solapen con la agrupación IP VPN. Para este ejemplo de red específico, quite la ruta 10.0.0.0/8 del ASA y configure Static rutas más específicas para las subredes que residen apagado de la interfaz interior. El dependiente sobre el número de subredes y de la topología de red, esto pudo ser un gran número de Static rutas y puede ser que no sea posible.

Solución 4 - Agregue una ruta más específica para la subred VPN se retiran de la interfaz exterior

Esta solución es más complicada que las otras que se describen en este documento. Cisco recomienda que usted intenta utilizar las otras soluciones primero debido a la situación que se describe en la nota más adelante en esta sección. Esta solución es prevenir el ASA de los paquetes del IP de la expedición originados de la subred IP VPN de nuevo al router interno; usted puede hacer esto si usted agrega una ruta más específica para la interfaz exterior de los de la subred VPN. Puesto que esta subred IP es reservada para los usuarios de VPN exteriores, los paquetes con una dirección IP de origen de esta subred IP VPN deben nunca llegar entrante en la interfaz interior ASA. La manera más fácil de alcanzar esto es agregar una ruta para la interfaz exterior de los de la agrupación IP del VPN de acceso remoto con un IP Address de Next Hop del router del ISP por aguas arriba.

En este ejemplo de la topología de red, esa ruta parecería esto:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Además de esta ruta, agregue el **IP verifican el trayecto inverso dentro del** comando para hacer el ASA caer cualquier paquete recibió entrante en la interfaz interior originada de la subred IP VPN debido a la más ruta preferida que existe en la interfaz exterior:

```
ip verify reverse-path inside
```

Después de que estos comandos implemeted, la tabla de ruteo ASA parece similar a esto cuando el usuario está conectado:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Cuando el cliente VPN está conectado, la ruta basada en el host a esa dirección IP VPN está presente en la tabla y se prefiere. Cuando las desconexiones del cliente VPN, trafican originado de ese dirección IP del cliente que llegue en la interfaz interior se marca contra la tabla de ruteo y caída debido al **IP verifican el trayecto inverso dentro del** comando.

Si el cliente VPN genera un broadcast de red dirigido a la subred IP VPN, después ese paquete

se remite al router interno y remitido por el router de nuevo al ASA, donde está caído debido al **IP verifique el trayecto inverso dentro del** comando.

> Nota: Después de que se implemente esta solución, si el **comando intra-interface del permiso de la mismo-Seguridad** está presente en la configuración y las políticas de acceso la permiten, trafique originado de un usuario de VPN destinado a un IP Address en la agrupación IP VPN para un usuario que no esté conectado pudo ser ruteado se retire de la interfaz exterior en el texto claro. Esto es una situación poco común y se puede atenuar con el uso de los VPN-filtros dentro de la política del VPN. Esta situación ocurre solamente si el **comando intra-interface del permiso de la mismo-Seguridad** está presente en la configuración del ASA.
>
> Asimismo, si los host internos generan el tráfico destinados a una dirección IP en el pool VPN y esa dirección IP no se asigna a un usuario de VPN remoto, ese tráfico pudo salida el exterior del ASA en el texto claro.