ASA tiene un uso elevado de la CPU debido a un loop de tráfico cuando los clientes VPN se desconectan

Contenido

Introducción

Este documento describe un problema común que ocurre cuando los clientes VPN se desconectan de un Cisco Adaptive Security Appliance (ASA) que se ejecuta como cabecera VPN de acceso remoto. Este documento también describe la situación en la que ocurre un loop de tráfico cuando los usuarios de VPN se desconectan de un firewall ASA. Este documento no trata sobre cómo configurar o configurar el acceso remoto a la VPN, solamente la situación específica que surge de ciertas configuraciones de ruteo comunes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN de acceso remoto en ASA
- Conceptos básicos de routing de capa 3

Componentes Utilizados

La información de este documento se basa en un modelo ASA 5520 que ejecuta código ASA versión 9.1(1).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

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

- Cualquier modelo ASA
- Cualquier versión de código ASA

Antecedentes

Cuando un usuario se conecta al ASA como concentrador VPN de acceso remoto, el ASA instala una ruta basada en host en la tabla de ruteo ASA que enruta el tráfico a ese cliente VPN fuera de la interfaz exterior (hacia Internet). Cuando ese usuario se desconecta, la ruta se elimina de la tabla y los paquetes en la red interna (destinados a ese usuario VPN desconectado) pueden tener un loop entre el ASA y un dispositivo de ruteo interno.

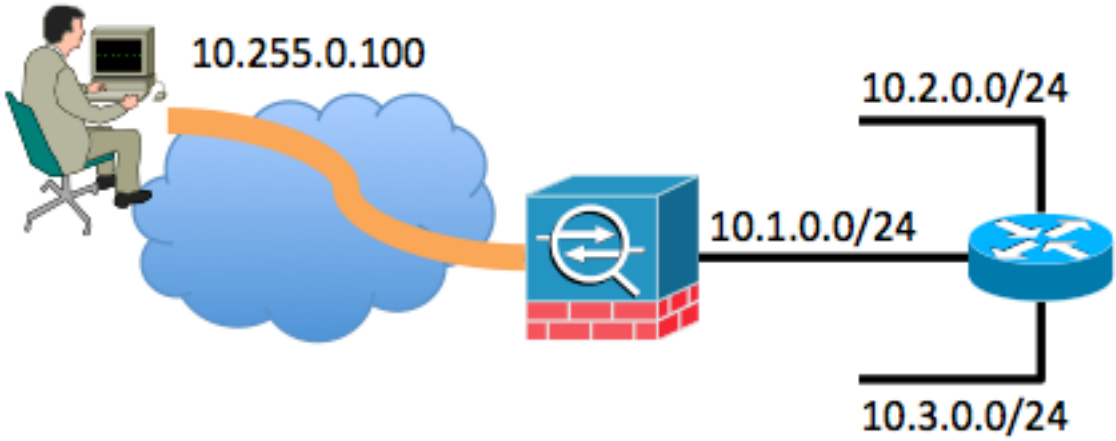
Otro problema es que los paquetes de difusión dirigidos (red) (generados por la eliminación de los clientes VPN) pueden ser reenviados por el ASA como una trama de unidifusión hacia la red interna. Esto podría reenviarlo de vuelta al ASA, lo que hace que el paquete se lance en bucle hasta que caduque el Tiempo de vida (TTL).

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

Problema: Paquetes Destinados a un Loop de Cliente VPN Desconectado dentro de la Red Interna

Cuando un usuario de VPN de acceso remoto se desconecta de un firewall ASA, los paquetes que todavía están presentes en la red interna (destinados a esos usuarios desconectados) y la dirección IP VPN asignada pueden volverse en loop dentro de la red interna. Estos loops de paquetes pueden hacer que el uso de la CPU en el ASA aumente hasta que el loop se detenga debido al valor TTL de IP en el encabezado del paquete IP que disminuye a 0, o el usuario se reconecta y la dirección IP se vuelve a asignar a un cliente VPN.

Para entender mejor este escenario, considere esta topología:



En este ejemplo, se ha asignado al cliente de acceso remoto la dirección IP 10.255.0.100. El ASA en este ejemplo está conectado al mismo segmento de red interno junto con un router. El router tiene dos segmentos de red de capa 3 adicionales conectados a él. En los ejemplos se muestran las configuraciones pertinentes de la interfaz (routing) y VPN del ASA y el router.

Los aspectos destacados de la configuración de 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
```

En este ejemplo se muestran los aspectos destacados de la configuración del router:

```
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 al interior del ASA simplemente tiene una ruta predeterminada apuntando a la interfaz interna del ASA de 10.1.0.1.

Mientras el usuario está conectado a través de VPN al ASA, la tabla de ruteo de ASA muestra lo

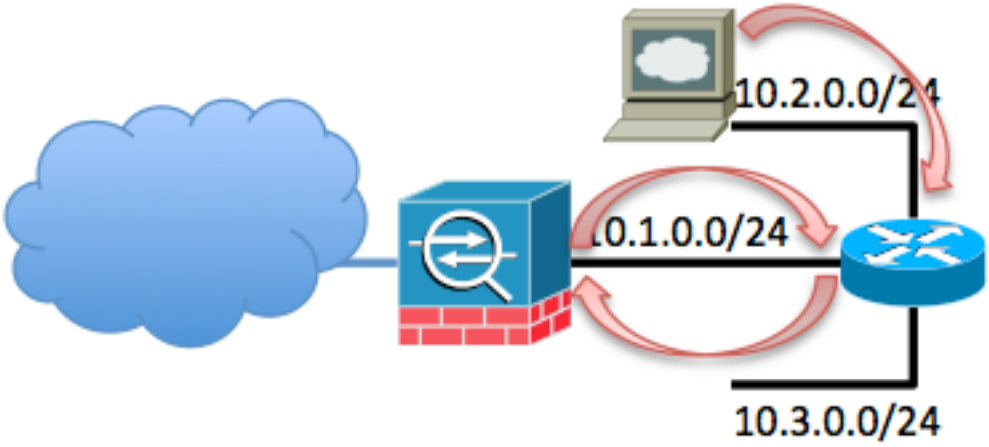
siguiente:

```
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 el usuario VPN de acceso remoto se desconecta de la VPN. En este punto, la ruta basada en host se elimina de la tabla de ruteo de ASA. Si un host dentro de la red intenta enviar tráfico al cliente VPN, ese tráfico es ruteado a la interfaz interna ASA por el router. Esta serie de pasos ocurre:

1. El paquete destinado a 10.255.0.100 llega a la interfaz interna del ASA.
2. Se realizan verificaciones de ACL estándar.
3. La tabla de ruteo ASA se verifica para determinar la interfaz de egreso para este tráfico.
4. El destino del paquete coincide con la ruta amplia 10.0.0.0/8 que apunta de la interfaz interna hacia el router.
5. El ASA verifica si se permite el tráfico de pines de pelo - busca el **permiso de seguridad para la interfaz** y encuentra que está permitido.
6. Una conexión se construye hacia y desde la interfaz interna y el paquete se envía de vuelta al router como salto siguiente.
7. El router recibe un paquete destinado a 10.255.0.100 en la interfaz que enfrenta el ASA. El router verifica su tabla de ruteo en busca de un salto siguiente adecuado. El router descubre que el salto siguiente sería la interfaz interna del ASA y que el paquete se envía al ASA.
8. regrese al paso 1

Un ejemplo se muestra aquí:



Este loop ocurre hasta que el TTL de este paquete disminuye a 0. Tenga en cuenta que el firewall ASA **no** disminuye el valor TTL de forma predeterminada cuando procesa un paquete. El router disminuye el TTL a medida que enruta el paquete. Esto evita la ocurrencia de este loop indefinidamente, pero este loop aumenta la carga de tráfico en el ASA y hace que el uso de la CPU se dispare.

Problema: Los paquetes de difusión dirigidos (de red) generados por los clientes de VPN tienen un loop en una red interna

Este problema es similar al primer problema. Si un cliente VPN genera un paquete de broadcast dirigido a su subred IP asignada (10.255.0.255 en el ejemplo anterior), el ASA podría reenviar ese paquete como una trama de unidifusión al router interno. El router interno luego podría reenviarlo nuevamente al ASA, lo que hace que el paquete se lance hasta que caduque el TTL.

Esta serie de eventos ocurren:

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

3. El router interno, que también trata al paquete como una trama de unidifusión, disminuye el TTL del paquete y lo reenvía de vuelta al ASA.

4. El proceso se repite hasta que el TTL del paquete se reduce a 0.

Soluciones al problema

Hay varias soluciones posibles para este problema. Según la topología de red y la situación específica, una solución podría ser más fácil de implementar que otra.

Solución 1- Ruta estática para interfaz Null0 (ASA versión 9.2.1 y posteriores)

Cuando envía tráfico a una interfaz **Null0**, hace que se descarten los paquetes destinados a la red especificada. Esta función es útil cuando configura el agujero negro desencadenado de forma

remota (RTBH) para el protocolo de gateway fronterizo (BGP). En esta situación, si configura una ruta a Null0 para la subred del cliente de acceso remoto, obliga al ASA a descartar el tráfico destinado a los hosts en esa subred si no hay una ruta más específica (proporcionada por Injection de ruta inversa).

```
route Null0 10.255.0.0 255.255.255.0
```

Solución 2: Uso de un Conjunto de IP Diferente para Clientes VPN

Esta solución es asignar a los usuarios VPN remotos una dirección IP que no se superpone con ninguna subred de red interna. Esto evitaría que el ASA reenvíe los paquetes destinados a esa subred VPN de vuelta al router interno si el usuario VPN no estaba conectado.

Solución 3: haga que la tabla de routing de ASA sea más específica para las rutas internas

Esta solución es para garantizar que la tabla de ruteo del ASA no tenga rutas muy amplias que se superpongan con el conjunto IP de VPN. Para este ejemplo de red específico, quite la ruta 10.0.0.0/8 del ASA y configure rutas estáticas más específicas para las subredes que residen fuera de la interfaz interna. En función del número de subredes y de la topología de la red, podría ser un gran número de rutas estáticas y podría no ser posible.

Solución 4: Adición de una Ruta Más Específica para la Subred VPN de Atrás desde la Interfaz Externa

Esta solución es más complicada que las otras que se describen en este documento. Cisco recomienda que intente utilizar las otras soluciones primero debido a la situación que se describe en la Nota más adelante en esta sección. Esta solución es para evitar que el ASA reenvíe los paquetes IP originados en la subred IP VPN de vuelta al router interno; puede hacer esto si agrega una ruta más específica para la subred VPN fuera de la interfaz externa. Dado que esta subred IP está reservada para usuarios VPN externos, los paquetes con una dirección IP de origen de esta subred IP VPN nunca deben llegar entrantes en la interfaz interna de ASA. La manera más fácil de lograr esto es agregar una ruta para el grupo IP VPN de acceso remoto fuera de la interfaz externa con una dirección IP de siguiente salto del router ISP ascendente.

En este ejemplo de topología de red, esa ruta tendría el siguiente aspecto:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Además de esta ruta, agregue el comando **ip verify reverse-path inside** para hacer que el ASA descarte cualquier paquete recibido de entrada en la interfaz interna originada en la subred IP de VPN debido a la ruta más preferida que existe en la interfaz exterior:

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

Después de implementar estos comandos, la tabla de ruteo de ASA tiene un aspecto similar al siguiente 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 host a esa dirección IP VPN está presente en la tabla y es preferible. Cuando el cliente VPN se desconecta, el tráfico originado en esa dirección IP del cliente que llega a la interfaz interna se verifica con la tabla de ruteo y se descarta debido al comando **ip verify reverse-path inside**.

Si el cliente VPN genera una transmisión de red dirigida a la subred IP VPN, entonces ese paquete se reenvía al router interno y el router lo reenvía de vuelta al ASA, donde se descarta debido al comando **ip verify reverse-path inside**.

> **Nota:** Después de implementar esta solución, si el comando **same-security permit intra-interface** está presente en la configuración y las políticas de acceso lo permiten, el tráfico originado en un usuario VPN destinado a una dirección IP en el conjunto IP VPN para un usuario que no está conectado podría ser ruteado de vuelta fuera de la interfaz externa en texto sin formato. Esta es una situación poco frecuente y se puede mitigar con el uso de vpn-filtros dentro de la política VPN. Esta situación sólo ocurre si el comando **same-security permit intra-interface** está presente en la configuración del ASA.
>
> De la misma manera, si los hosts internos generan tráfico destinado a una dirección IP en el conjunto VPN y esa dirección IP no está asignada a un usuario VPN remoto, ese tráfico podría salir del exterior del ASA en texto sin cifrar.