Configuración de Hairpinning del Tráfico entre Dos Túneles de Sitio a Sitio

Contenido

Introducción

Este documento describe cómo reenviar el tráfico VPN entre dos túneles VPN en una sola interfaz.

Prerequisites

Requirements

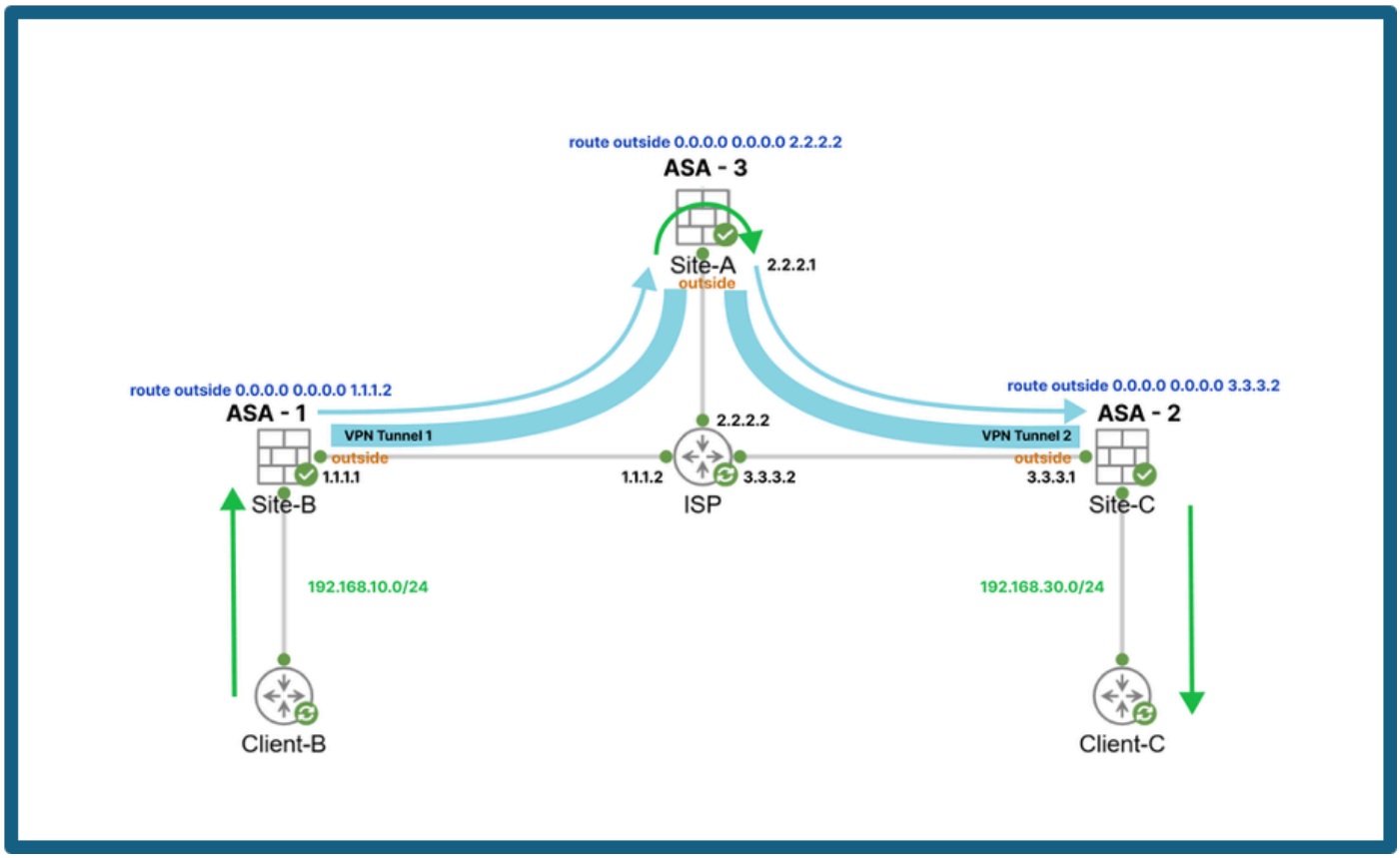
Cisco recomienda conocer estos temas:
· Comprensión básica de la VPN de sitio a sitio basada en políticas
· Experiencia con la línea de comandos de ASA

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.
· Adaptive Security Appliance (ASA) versión 9.20
· IKEv1

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología



Topología

Antecedentes

Esta configuración muestra cómo redirigir el tráfico de un túnel de sitio a sitio a otro en el mismo dispositivo. Para ilustrar esta configuración, hemos utilizado tres ASA que representan el sitio A, el sitio B y el sitio C.

Configuración

Esta sección describe la configuración necesaria para permitir el tráfico de ASA-1 (Sitio B) a ASA-2 (Sitio C) a través de ASA-3 (Sitio A).

Tenemos dos túneles VPN configurados:

- Túnel VPN 1: Túnel VPN entre el Sitio B y el Sitio A
- Túnel VPN 2: Túnel VPN entre el sitio C y el sitio A

Para obtener orientación detallada sobre cómo crear un túnel VPN basado en políticas en ASA, consulte la sección Configuración de ASA en la documentación de Cisco: Configuración de un túnel IPSec IKEv1 de sitio a sitio entre ASA y el router Cisco IOS XE

Configuración de ASA (Sitio B)

Tenemos que permitir el tráfico de la red del sitio B a la red del sitio C en la lista de acceso criptográfica del túnel VPN 1 en la interfaz externa de ASA 1.
En este escenario, es de 192.168.10.0/24 a 192.168.30.0/24

Lista de acceso criptográfica:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Excepción Nat:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

Mapa criptográfico para el túnel VPN 1:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Configuración criptográfica de ASA (Sitio C)

Permitir el tráfico de la red del Sitio C a la red del Sitio B en la lista de acceso criptográfica del Túnel VPN 2 en la interfaz externa de ASA 2.
En este escenario, es de 192.168.30.0/24 a 192.168.10.0/24

Lista de acceso criptográfica:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Excepción Nat:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

Mapa criptográfico para el túnel VPN 2:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Configuración criptográfica de ASA (Sitio A)

Permitir el tráfico de la red del Sitio-C a la red del Sitio-B en la lista de acceso criptográfico del Túnel VPN 1 y el tráfico de la red del Sitio-B a la red del Sitio-C en la lista de acceso criptográfico del Túnel VPN 2 en la interfaz exterior de ASA en el Sitio-A que está en dirección inversa a lo que configuramos en _ ASA.

En esta situación, va de 192.168.30.0/24 a 192.168.10.0/24 para el túnel VPN 1 y de 192.168.10.0/24 a 192.168.30.0/24 para el túnel VPN 2

Lista de acceso criptográfica:

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Configuración de mapa criptográfico para el túnel VPN 1 y 2:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Además de esto, ya que necesitamos rutear el tráfico desde afuera hacia afuera que es la misma interfaz con el mismo nivel de seguridad, necesitamos configurar el comando:

```
same-security-traffic permit intra-interface
```

Flujo de tráfico del sitio B al sitio C

Consideremos que el tráfico se inicia desde el sitio B al sitio C, es decir, desde 192.168.10.0/24 a 192.168.30.0/24.

Sitio B (origen)

1. El tráfico iniciado desde 192.168.10.0/24 network (Sitio-B) y destinado a 192.168.30.0/24 network (Sitio-C) se enruta a la interfaz externa de ASA-1 en función de la tabla de enrutamiento configurada.

2. Una vez que el tráfico llega a ASA-1, coincide con la lista de acceso criptográfica 110 configurada en ASA-1. Esto activa el cifrado del tráfico mediante el túnel VPN 1, que envía los

datos de forma segura hacia el sitio A.

Sitio-A (intermedio)

1. El tráfico cifrado de 192.168.10.0/24 to 192.168.30.0/24 arrives en la interfaz externa del ASA en el Sitio A.
2. En el Sitio A, el tráfico es descifrado por el Túnel VPN 1 para restaurar la carga útil original.
3. A continuación, el tráfico descifrado se vuelve a cifrar mediante el túnel VPN 2 en la interfaz externa de ASA en el sitio A.

Sitio-C (destino)

1. El tráfico cifrado de 192.168.10.0/24 to 192.168.30.0/24 reaches la interfaz externa de ASA-2 en el sitio C.
2. ASA-2 descifra el tráfico mediante el túnel VPN 2 y reenvía los paquetes al lado LAN del sitio C, entregándolos al destino deseado dentro de 192.168.30.0/24 network.

Flujo de tráfico inverso del sitio C al sitio B

El flujo de tráfico inverso, que se origina en el sitio C (192.168.30.0/24) and con destino al sitio B (192.168.10.0/24), da lugar al mismo proceso pero en la dirección inversa:
1. En el sitio C, el tráfico se cifra mediante el túnel VPN 2 antes de enviarse al sitio A.
2. En el sitio A, el tráfico se descifra mediante el túnel VPN 2 y, a continuación, se vuelve a cifrar mediante el túnel VPN 1 antes de reenviarse al sitio B.
3. En el Sitio B, el tráfico es descifrado por el Túnel VPN 1 y entregado al 192.168.10.0/24 network.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).