Hairpinning van verkeer tussen twee tunnels van locatie naar locatie configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u VPN-verkeer tussen twee VPN-tunnels op één interface kunt doorsturen.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:
· Basiskennis van op beleid gebaseerde site-to-site VPN
· Ervaring met ASA-opdrachtregel

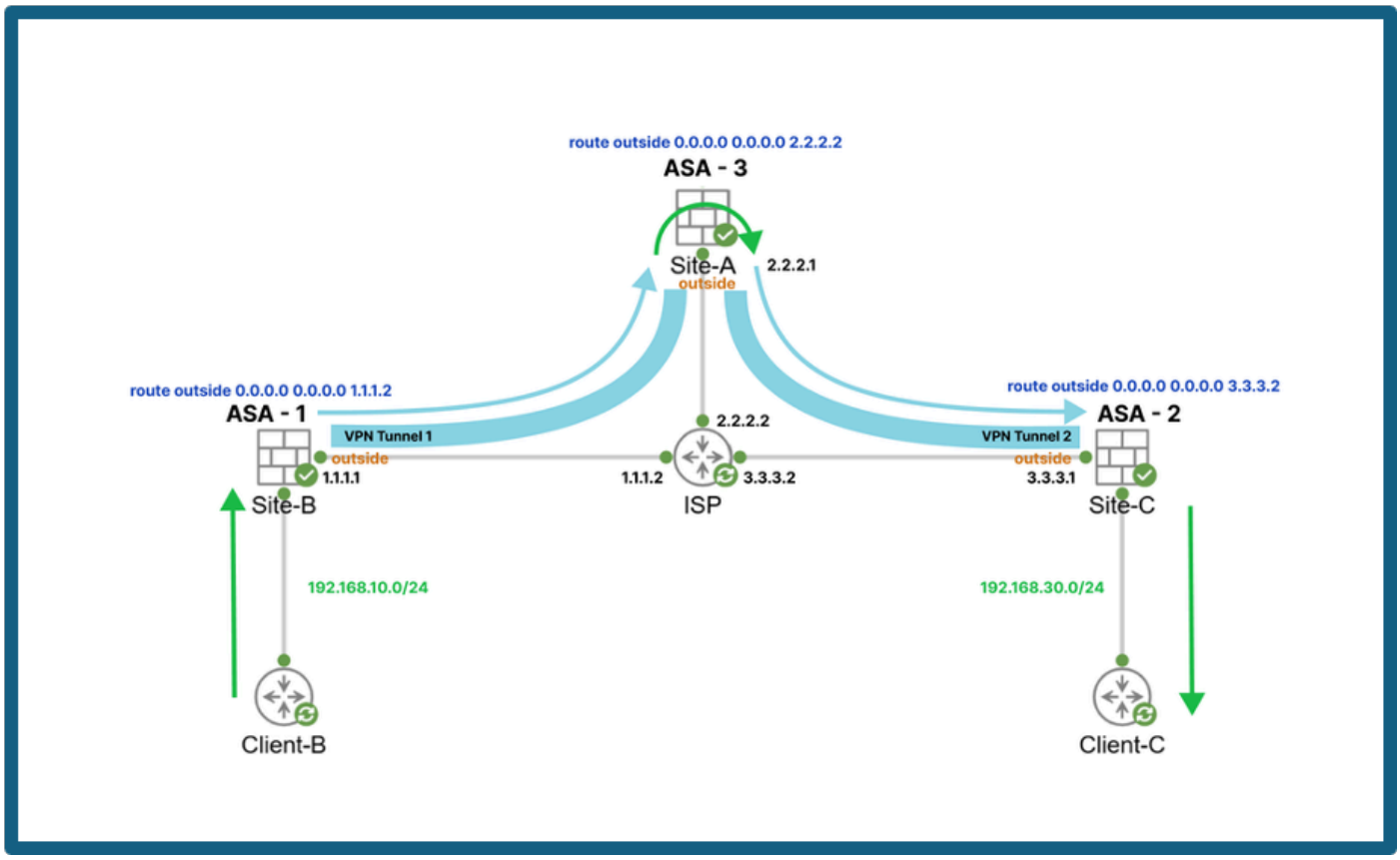
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
· Adaptive Security Appliance (ASA) versie 9.20
· IKEv1

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



Topologie

Achtergrondinformatie

Deze configuratie laat zien hoe u verkeer van de ene site-to-site tunnel naar de andere kunt omleiden op hetzelfde apparaat. Om deze opzet te illustreren, hebben we drie ASA's gebruikt die Site A, Site B en Site C vertegenwoordigen.

Configuratie

In dit gedeelte wordt de configuratie beschreven die nodig is om verkeer van ASA-1 (Site B) naar ASA-2 (Site C) via ASA-3 (Site A) mogelijk te maken.

We hebben twee VPN-tunnels geconfigureerd:

- VPN Tunnel 1: VPN-tunnel tussen Site-B en Site-A
- VPN Tunnel 2: VPN-tunnel tussen Site-C en Site-A

Voor gedetailleerde richtlijnen over het maken van een op beleid gebaseerde VPN-tunnel op ASA, raadpleegt u de sectie ASA-configuratie in de Cisco-documentatie: Configureer een IPSec IKEv1-tunnel tussen ASA en Cisco IOS XE Router

Configuratie ASA (Site B)

We moeten het verkeer van Site-B-netwerk naar Site-C-netwerk toestaan in de crypto-toegangslijst van VPN Tunnel 1 op de externe interface van ASA 1.
In dit scenario is het van 192.168.10.0/24 tot 192.168.30.0/24

Crypto-toegangslijst:

```
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
```

Nat uitzondering:

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

Crypto-kaart voor VPN Tunnel 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
```

Cryptoconfiguratie ASA (Site C)

Sta het verkeer toe van Site-C-netwerk naar Site-B-netwerk in de crypto-toegangslijst van VPN Tunnel 2 op de externe interface van ASA 2.
In dit scenario is het van 192.168.30.0/24 tot 192.168.10.0/24

Crypto-toegangslijst:

```
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
```

Nat uitzondering:

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

Crypto-kaart voor VPN Tunnel 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
```

Cryptoconfiguratie ASA (Site A)

Sta het verkeer toe van Site-C-netwerk naar Site-B-netwerk in de crypto-toegangslijst van VPN Tunnel 1 en het verkeer van Site-B-netwerk naar Site-C-netwerk in de crypto-toegangslijst van VPN Tunnel 2 op de externe interface van ASA op Site-A, die in omgekeerde richting is naar wat we hebben geconfigureerd op _ ASA's.

In dit scenario gaat het van 192.168.30.0/24 naar 192.168.10.0/24 voor VPN tunnel 1 en van 192.168.10.0/24 naar 192.168.30.0/24 voor VPN tunnel 2

Crypto-toegangslijst:

```
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
```

Crypto-kaartconfiguratie voor VPN Tunnel 1 en 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
```

Naast dit als we nodig hebben om het verkeer van buiten naar buiten die dezelfde interface met hetzelfde beveiligingsniveau routeren, moeten we de opdracht configureren:

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

Verkeersstroom van Site-B naar Site-C

Laten we eens kijken naar het verkeer dat wordt geïnitieerd van Site-B naar Site-c, dat is van 192.168.10.0/24 tot 192.168.30.0/24.

Site-B (bron)

1. Verkeer dat wordt gestart vanaf het 192.168.10.0/24-netwerk (Site-B) en bestemd is voor het 192.168.30.0/24-netwerk (Site-C) wordt naar de externe interface van ASA-1 geleid op basis van de geconfigureerde routeringstabel.

2. Zodra het verkeer ASA-1 bereikt, komt het overeen met de crypto-toegangslijst 110 geconfigureerd op ASA-1. Dit leidt tot versleuteling van het verkeer met behulp van VPN Tunnel 1,

die de gegevens veilig naar Site-A stuurt.

Site-A (Intermediair)

1. Het versleutelde verkeer van 192.168.10.0/24 naar 192.168.30.0/24 komt aan op de buiteninterface van de ASA op Site-A.
2. Op Site-A wordt het verkeer door VPN Tunnel 1 gedecodeerd om de oorspronkelijke lading te herstellen.
3. Het gedecodeerde verkeer wordt vervolgens opnieuw gecodeerd met behulp van VPN Tunnel 2 aan de buitenzijde van de ASA op Site-A.

Site-C (Bestemming)

1. Het gecodeerde verkeer van 192.168.10.0/24 naar 192.168.30.0/24 bereikt de buiteninterface van ASA-2 op Site-C.
2. ASA-2 decodeert het verkeer met behulp van VPN Tunnel 2 en stuurt de pakketten door naar de LAN-kant van Site-C en levert ze naar de beoogde bestemming binnen het 192.168.30.0/24-netwerk.

Omgekeerde verkeersstroom van site-C naar site-B

De omgekeerde verkeersstroom, afkomstig van Site-C (192.168.30.0/24) en bestemd voor Site-B (192.168.10.0/24), resulteert in hetzelfde proces, maar in de omgekeerde richting:
1. Op Site-C wordt het verkeer gecodeerd door VPN Tunnel 2 voordat het naar Site-A wordt verzonden.
2. Op Site-A wordt het verkeer ontsleuteld door VPN Tunnel 2 en vervolgens opnieuw gecodeerd met VPN Tunnel 1 voordat het wordt doorgestuurd naar Site-B.
3. Op Site-B wordt het verkeer ontsleuteld door VPN Tunnel 1 en geleverd aan het 192.168.10.0/24-netwerk.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.