Beheer van SFR-module via VPN-tunnels zonder LAN-switch

Inhoud

Inleiding

Serviceproviders bieden beheerde WAN-service in hun portefeuille aan. Cisco ASA Firepower platform biedt Unified Threat Management-functie voor gedifferentieerde services. Een ASA Firepower apparaat heeft verschillende interfaces voor het beheer verbonden met een LAN apparaat. Bij het aansluiten van een beheerinterface met een LAN-apparaat wordt echter een afhankelijkheid van een LAN-apparaat gecreëerd.

Dit document biedt een oplossing waarmee u een Cisco ASA Firepower (SFR) module kunt beheren zonder verbinding te maken met een LAN-apparaat of met een tweede interface van het serviceprovider-randapparaat.

Voorwaarden

Gebruikte componenten

- ASA 5500-X Series platform met FirePOWER-services (SFR).
- Management-interface die wordt gedeeld door de ASA-module en de Firepower-module.

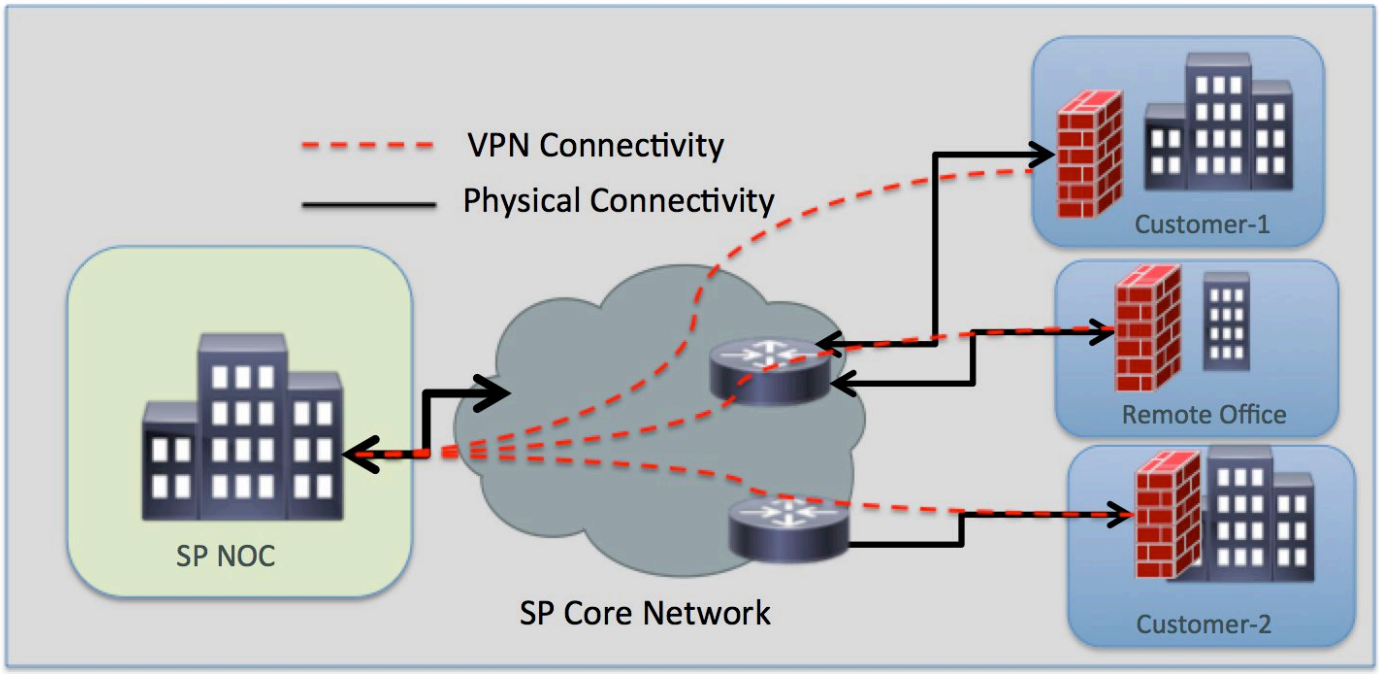
Architectuur

Vereisten

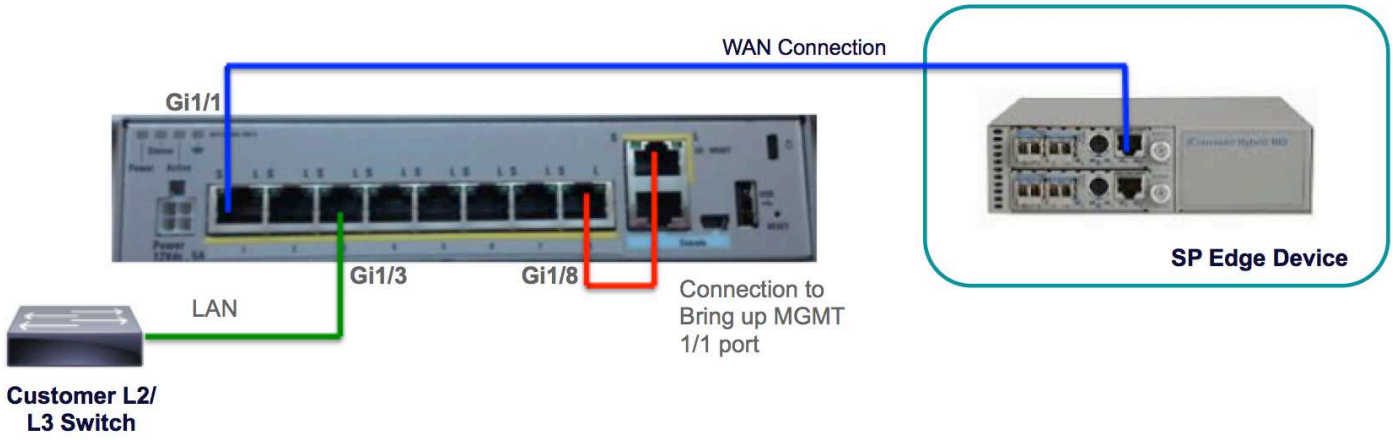
- Enkelvoudige specifieke internettoegangsingang van het randapparaat van de serviceproviders naar ASA Firepower.

- Toegang tot de beheerinterface is nodig om de interfacestatus te wijzigen.
- De beheersinterface van de ASA moet blijven bestaan om de Firepower module te beheren.
- De beheerconnectiviteit zou niet verloren moeten gaan als de klant LAN apparaat ontkoppelt.
- Management-architectuur dient actieve/back-up WAN-failover te ondersteunen.

Overzicht van topologie



Laag ontwerp



Oplossing

De volgende configuraties staan u toe om de SFR-module via VPN extern te beheren, zonder enige LAN-connectiviteit als vereist.

Kabelbekabeling

- Sluit de Management-interface 1/1 aan op de Gigabit Ethernet1/8-interface met een Ethernet-kabel.

Opmerking: De ASA Firepower module moet de Management 1/x (1/0 of 1/1) interface gebruiken om beheerverkeer te verzenden en ontvangen. Aangezien de Management 1/x-interface niet in het gegevensvliegtuig is, moet u de beheerinterface fysiek naar een ander LAN-apparaat kabelten om verkeer via het ASA-venster te kunnen doorgeven.

Als deel van de één-box oplossing, zult u de interface van het Beheer 1/1 aan de interface van Gigabit Ethernet1/8 verbinden met behulp van een Ethernet kabel.

IP-adres

- **Gigabit Ethernet 1/8-interface**: 192.168.10.1/24
- **SFR-beheerinterface**: 192.168.10.2/24
- **SFR-gateway**: 192.168.10.1
- **Management 1/1-interface**: De beheerinterface heeft geen IP-adres ingesteld. De opdracht beheertoegang moet worden geconfigureerd voor MGMT-doel.

Het lokale en afstandsverkeer bevindt zich op de volgende subnetten:

- Het lokale verkeer is op beheersgebied 192.168.10.0/24.
- Afstandsverkeer is op 192.168.11.0/24.

VPN en NAT

- Bepaal het VPN-beleid.
- NAT-opdracht moet met voorvoegsel voor routeraadpleging worden geconfigureerd om de egpersinterface te bepalen met behulp van een routeraadpleging in plaats van de interface te gebruiken die in de NAT-opdracht is gespecificeerd.

Configuratievoorbeeld

```
!
management-access MGMT
!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.106.223.1 255.255.255.0
!

interface GigabitEthernet1/8
 nameif MGMT
 security-level 90
 ip address 192.168.10.1 255.255.255.252
!

interface Management1/1
 management-only
 no nameif
 no security-level
 no ip address
!

object network obj_any
 subnet 0.0.0.0 0.0.0.0
```

```
object-group network LOCAL-LAN
 network-object 192.168.10.0 255.255.255.0
object-group network REMOTE-LAN
 network-object 192.168.11.0 255.255.255.0
access-list INTREST-TRAFFIC extended permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0
access-list TEST extended permit tcp any any eq www
access-list TEST extended permit tcp any any eq https
```

nat (MGMT,outside) source static LOCAL-LAN LOCAL-LAN destination static REMOTE-LAN REMOTE-LAN route-lookup

```
object network obj_any
 nat (any,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 10.106.223.2 1

crypto ipsec ikev1 transform-set TRANS-SET esp-3des esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CMAP 10 match address INTREST-TRAFFIC
crypto map CMAP 10 set peer 10.106.223.2
crypto map CMAP 10 set ikev1 transform-set TRANS-SET
crypto map CMAP interface outside

crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
!
tunnel-group 10.106.223.1 type ipsec-l2l
tunnel-group 10.106.223.1 ipsec-attributes
 ikev1 pre-shared-key *****
!

class-map TEST
 match access-list TEST

policy-map global_policy
 class TEST
 sfr fail-close
!
```