Management des SFR-Moduls über VPN-Tunnel ohne LAN-Switch

Inhalt

Einführung

Service Provider bieten Managed WAN-Services in ihrem Portfolio an. Die Cisco ASA FirePOWER-Plattform bietet Funktionen für das einheitliche Management von Bedrohungen, um differenzierte Services bereitzustellen. Ein ASA-FirePOWER-Gerät verfügt über separate Schnittstellen für die Verwaltungsanbindung an ein LAN-Gerät. Wenn Sie jedoch eine Verwaltungsschnittstelle mit einem LAN-Gerät verbinden, besteht eine Abhängigkeit von einem LAN-Gerät.

Dieses Dokument enthält eine Lösung, mit der Sie ein Cisco ASA FirePOWER (SFR)-Modul verwalten können, ohne eine Verbindung zu einem LAN-Gerät herzustellen oder eine zweite Schnittstelle vom Edge-Gerät des Service Providers zu verwenden.

Voraussetzungen

Verwendete Komponenten

- Plattform der Serie ASA 5500-X mit FirePOWER-Services (SFR)
- Verwaltungsschnittstelle, die von ASA und dem FirePOWER-Modul gemeinsam genutzt wird.

Architektur

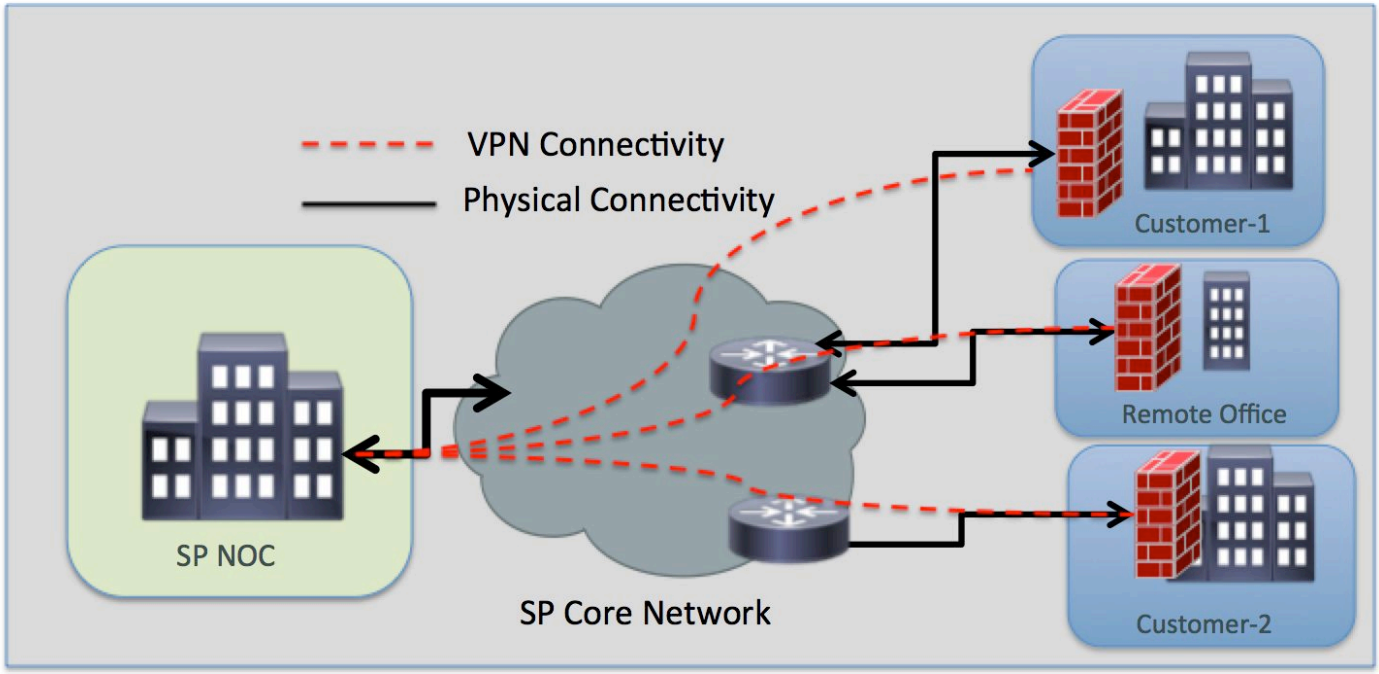
Anforderungen

- Dedizierter Internetzugang, Übergabe vom Edge-Gerät des Service Providers an die ASA

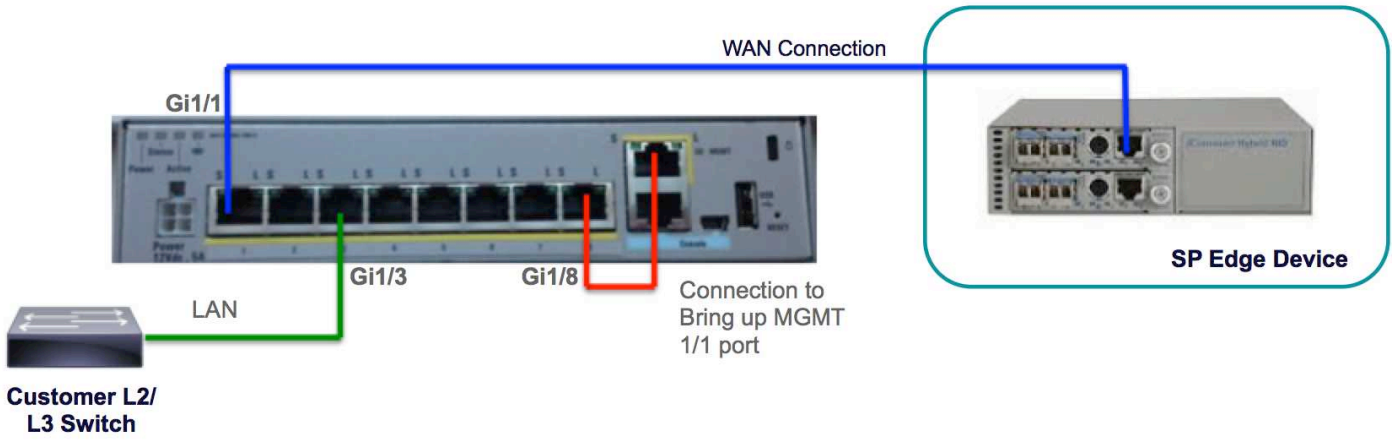
FirePOWER.

- Der Zugriff auf die Verwaltungsschnittstelle ist erforderlich, um den Schnittstellenstatus auf "up" (aktiv) zu ändern.
- Die Management-Schnittstelle der ASA sollte erhalten bleiben, um das FirePOWER-Modul zu verwalten.
- Die Management-Konnektivität sollte nicht verloren gehen, wenn der Kunde das LAN-Gerät trennt.
- Die Verwaltungsarchitektur sollte Active/Backup-WAN-Failover unterstützen.

Topologieübersicht



Low-Level-Design



Lösung

Mit den folgenden Konfigurationen können Sie das SFR-Modul über VPN remote verwalten, ohne dass eine LAN-Verbindung erforderlich ist.

Verkabelung

- Verbinden Sie die Management-Schnittstelle 1/1 mithilfe eines Ethernet-Kabels mit der GigabitEthernet1/8-Schnittstelle.

  Hinweis: Das ASA FirePOWER-Modul muss die Management 1/x (1/0 oder 1/1)-Schnittstelle verwenden, um Management-Datenverkehr zu senden und zu empfangen. Da sich die Management 1/x-Schnittstelle nicht auf der Datenebene befindet, müssen Sie die Verwaltungsschnittstelle physisch mit einem anderen LAN-Gerät verkabeln, um den Datenverkehr über die ASA-Ebene zu leiten.

  Als Teil der One-Box-Lösung verbinden Sie die Management-Schnittstelle 1/1 mithilfe eines Ethernet-Kabels mit der GigabitEthernet1/8-Schnittstelle.

IP-Adresse

- **GigabitEthernet 1/8-Schnittstelle**: 192.168.10.1/24
- **SFR-Management-Schnittstelle**: 192.168.10.2/24
- **SFR-Gateway**: 192.168.10.1
- **Management 1/1-Schnittstelle**: Für die Verwaltungsschnittstelle ist keine IP-Adresse konfiguriert. Der Management-Access-Befehl muss für Verwaltungszwecke (MGMT) konfiguriert werden.

Der lokale und der Remote-Datenverkehr erfolgt in den folgenden Subnetzen:

- Der lokale Datenverkehr befindet sich im Management-Subnetz 192.168.10.0/24.
- Der Remote-Datenverkehr läuft im Subnetz 192.168.11.0/24.

VPN und NAT

- Definieren Sie die VPN-Richtlinien.
- Der NAT-Befehl sollte mit dem Präfix für die Route-Lookup konfiguriert werden, um die Ausgangsschnittstelle mithilfe einer Route-Lookup zu ermitteln, anstatt die im NAT-Befehl angegebene Schnittstelle zu verwenden.

Konfigurationsbeispiel

```
!
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
!
```