LAN 스위치가 없는 VPN 터널을 통한 SFR 모듈 관리

목차

소개

통신 사업자는 포트폴리오에 매니지드 WAN 서비스를 제공합니다.Cisco ASA Firepower 플랫폼은 차별화된 서비스를 제공하기 위한 통합 위협 관리 기능 집합을 제공합니다.ASA Firepower 디바이스에는 관리 인터페이스를 LAN 디바이스에 연결하기 위한 별도의 인터페이스가 있지만, 관리 인터페이스를 LAN 디바이스와 연결하면 LAN 디바이스에 대한 종속성이 생성됩니다.

이 문서에서는 LAN 디바이스에 연결하지 않고 또는 서비스 공급자 에지 디바이스의 두 번째 인터페이스를 사용하지 않고 Cisco ASA Firepower(SFR) 모듈을 관리할 수 있는 솔루션을 제공합니다.

사전 요구 사항

사용되는 구성 요소

- ASA 5500-X Series 플랫폼과 Firepower(SFR) 서비스
- ASA와 Firepower 모듈 간에 공유되는 관리 인터페이스.

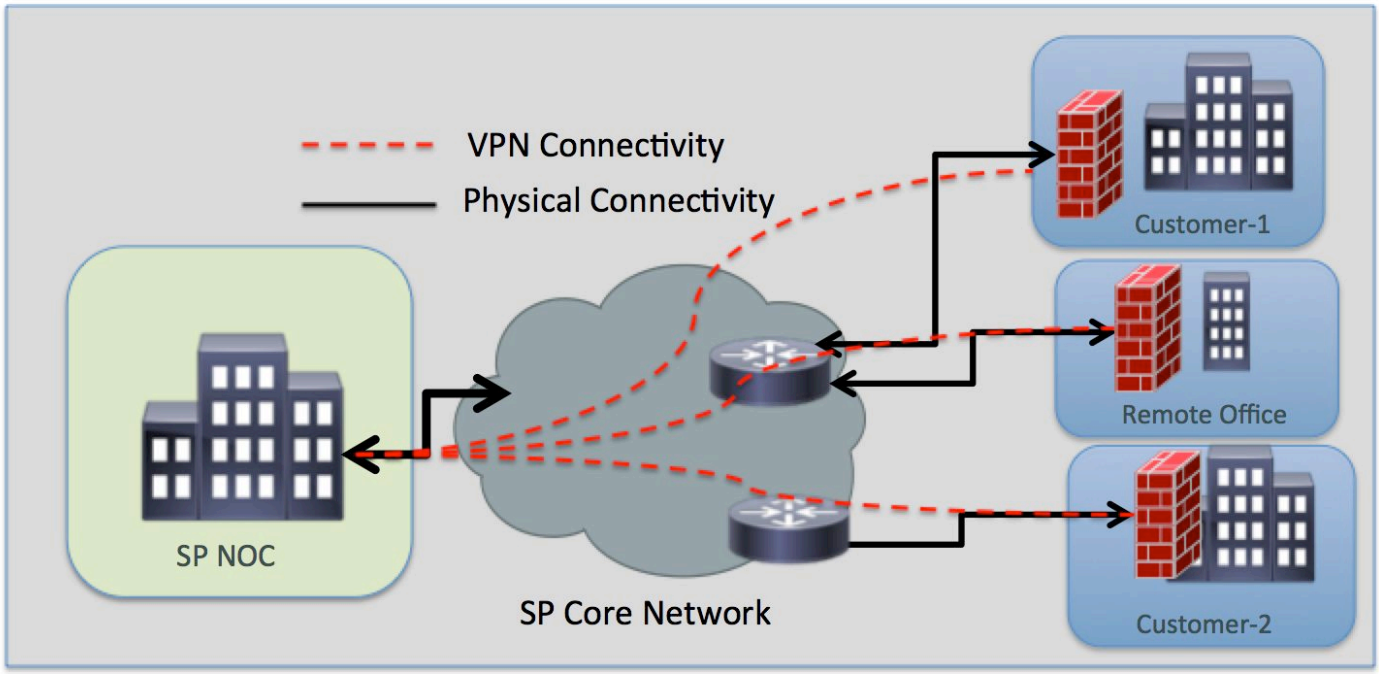
아키텍처

요구 사항

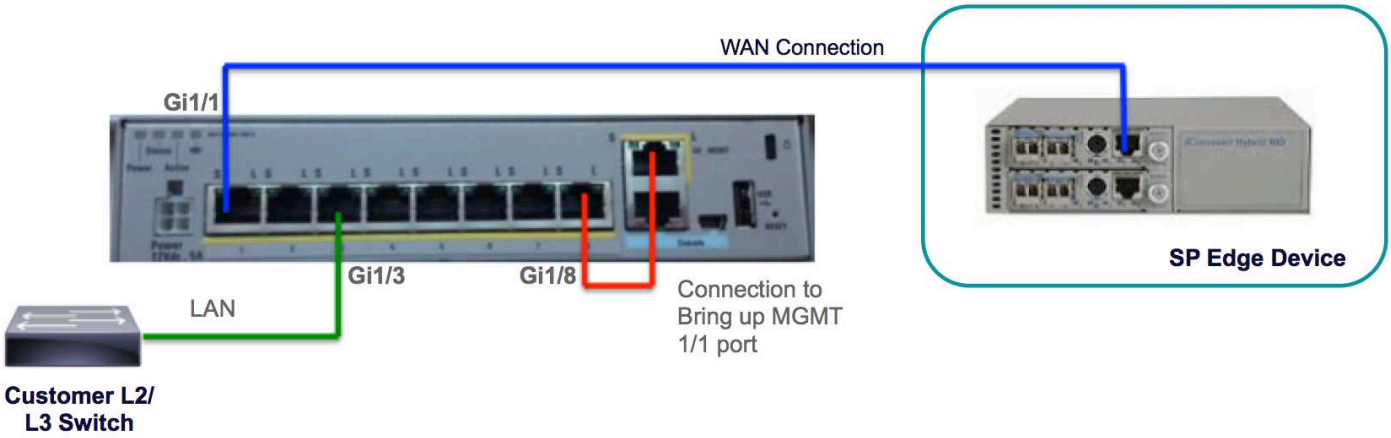
- 서비스 공급자 에지 디바이스에서 ASA Firepower로의 단일 전용 인터넷 액세스 전달
- 인터페이스 상태를 up으로 변경하려면 관리 인터페이스에 대한 액세스가 필요합니다.
- Firepower 모듈을 관리하려면 ASA의 관리 인터페이스가 계속 작동해야 합니다.
- 고객이 LAN 장치의 연결을 끊으면 관리 연결이 끊어지지 않습니다.

- 관리 아키텍처는 액티브/백업 WAN 장애 조치를 지원해야 합니다.

토폴로지 개요



낮은 수준의 설계



솔루션

다음 컨피그레이션을 통해 VPN을 통해 SFR 모듈을 원격으로 관리할 수 있습니다. LAN 연결은 사전 요구 사항으로 하지 않습니다.

케이블 연결

- 이더넷 케이블을 사용하여 관리 인터페이스 1/1을 GigabitEthernet1/8 인터페이스에 연결합니다.

  참고:ASA Firepower 모듈은 관리 트래픽을 보내고 받으려면 Management 1/x(1/0 또는 1/1) 인터페이스를 사용해야 합니다.Management 1/x 인터페이스는 데이터 플레인에 없으므로 ASA를 통해 트래픽을 제어 플레인으로 전달하려면 관리 인터페이스를 다른 LAN 디바이스에

물리적으로 연결해야 합니다.

원박스 솔루션의 일부로서 이더넷 케이블을 사용하여 관리 인터페이스 1/1을 GigabitEthernet1/8 인터페이스에 연결합니다.

IP 주소

- **GigabitEthernet 1/8 인터페이스**:192.168.10.1/24
- **SFR 관리 인터페이스**:192.168.10.2/24
- **SFR 게이트웨이**:192.168.10.1
- **Management 1/1 인터페이스**:관리 인터페이스에 구성된 IP 주소가 없습니다.management-access 명령은 관리(MGMT)용으로 구성해야 합니다.

로컬 및 원격 트래픽은 다음 서브넷에 있습니다.

- 로컬 트래픽은 관리 서브넷 192.168.10.0/24에 있습니다.
- 원격 트래픽은 192.168.11.0/24 서브넷에 있습니다.

VPN 및 NAT

- VPN 정책을 정의합니다.
- NAT 명령은 NAT 명령에 지정된 인터페이스를 사용하는 대신 경로 조회를 사용하여 이그레스 인터페이스를 확인하기 위해 route-lookup 접두사로 구성해야 합니다.

컨피그레이션 예시

```
!
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
!
```