不含LAN交換器的VPN通道上的SFR模組管理

目錄

簡介

服務提供商在其產品組合中提供託管廣域網服務。Cisco ASA Firepower平台提供統一威脅管理功能集，以提供差異化服務。ASA Firepower裝置具有用於管理連線到LAN裝置的獨立介面，但是，將管理介面連線到LAN裝置會對LAN裝置產生依賴性。

本文檔提供的解決方案允許您在不連線LAN裝置或使用服務提供商邊緣裝置的第二個介面的情況下管理Cisco ASA Firepower(SFR)模組。

必要條件

採用元件

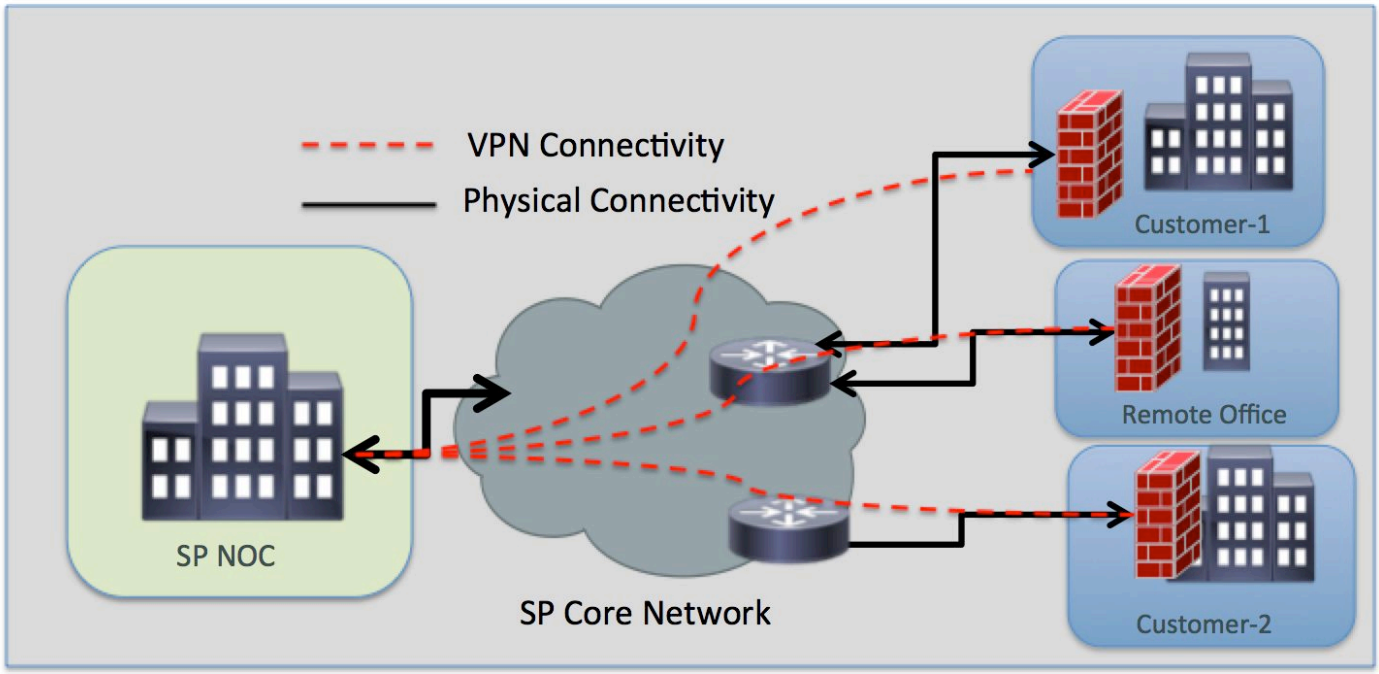
- 具備Firepower(SFR)服務的ASA 5500-X系列平台。
- ASA和Firepower模組之間共用的管理介面。

架構

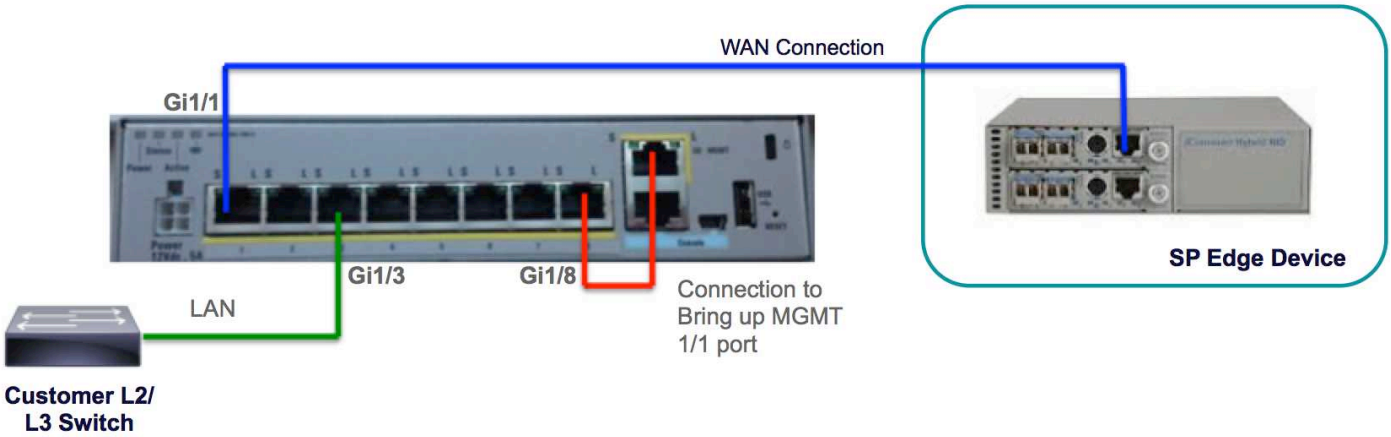
需求

- 從服務提供商邊緣裝置到ASA Firepower的單個專用網際網路接入切換。
- 必須將介面狀態更改為up，才能訪問管理介面。
- ASA的管理介面應保持正常狀態以管理Firepower模組。
- 如果客戶斷開LAN裝置，則不應丟失管理連線。
- 管理架構應支援主用/備用廣域網故障切換。

拓撲概述



低級設計



解決方案

下列配置將允許您通過VPN遠端管理SFR模組，無需任何區域網連線。

佈線

- 使用乙太網電纜將管理介面1/1連線到GigabitEthernet1/8介面。

  附註：ASA Firepower模組必須使用管理1/x（1/0或1/1）介面來傳送和接收管理流量。由於管理1/x介面不在資料平面上，您需要將管理介面用電纜連線到另一台LAN裝置，以便將流量通過ASA通過控制平面。

  作為一盒式解決方案的一部分，您將使用乙太網電纜將管理介面1/1連線到GigabitEthernet1/8介面。

IP 位址

- **GigabitEthernet 1/8介面**:192.168.10.1/24
- **SFR管理介面**:192.168.10.2/24
- **SFR網關**:192.168.10.1
- **Management 1/1介面**:管理介面未配置任何IP地址。management-access命令應配置為管理(MGMT)用途。

本地和遠端流量將位於以下子網中：

- 本地流量位於管理子網192.168.10.0/24上。
- 遠端流量位於192.168.11.0/24子網上。

VPN和NAT

- 定義VPN策略。
- 應使用route-lookup字首來配置NAT命令，以便使用路由查詢而不是使用NAT命令中指定的介面來確定出口介面。

組態範例

```
!
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
!
```