无局域网交换的VPN隧道SFR模块管理

目录

[简介](#)
[先决条件](#)
[使用的组件](#)
[架构](#)
[要求](#)
[拓扑概述](#)
[低级设计](#)
[解决方案](#)
[布线](#)
[IP Address](#)
[VPN和NAT](#)
[配置示例](#)
[相关的思科支持社区讨论](#)

简介

服务提供商在其产品组合中提供托管广域网服务。Cisco ASA Firepower平台提供统一的威胁管理功能集，以提供差异化服务。ASA Firepower设备具有用于管理连接到LAN设备的独立接口，但是，将管理接口连接到LAN设备会对LAN设备产生依赖。

本文档提供的解决方案允许您管理Cisco ASA Firepower(SFR)模块，而无需连接到LAN设备或使用服务提供商边缘设备的第二个接口。

先决条件

使用的组件

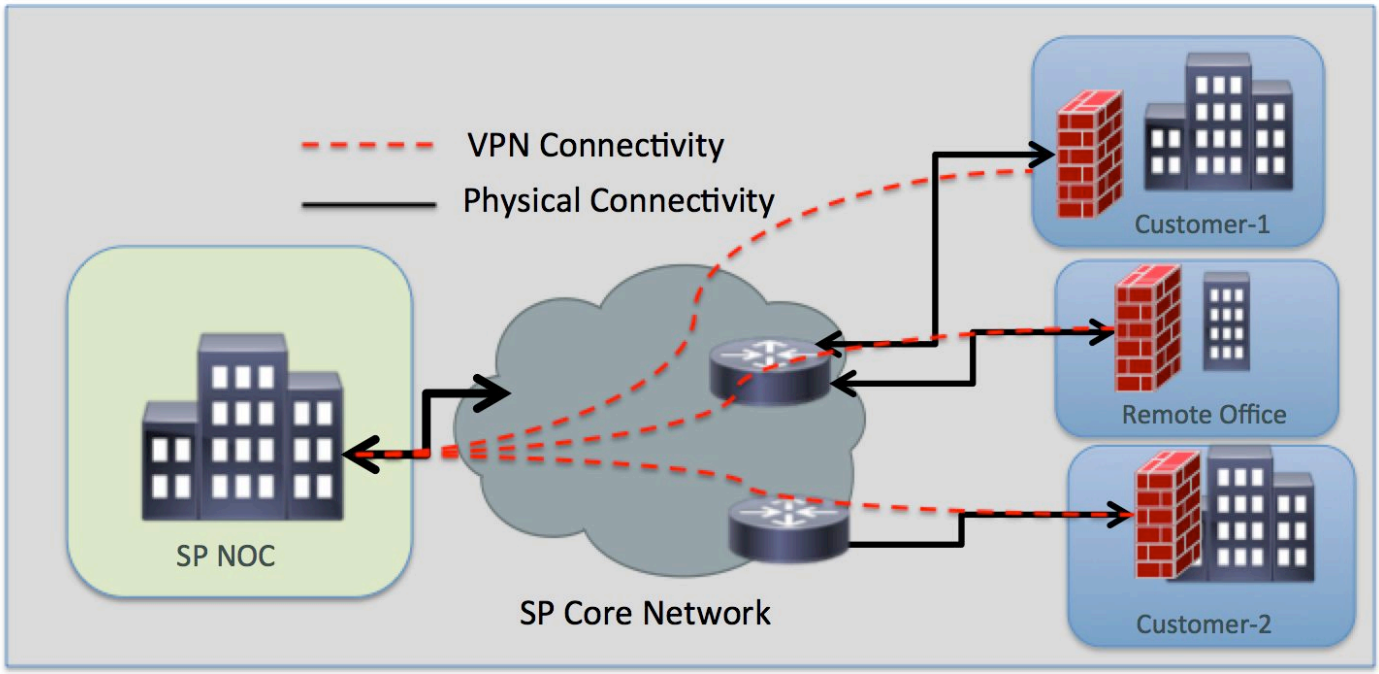
- 具备Firepower(SFR)服务的ASA 5500-X系列平台。
- 在ASA和Firepower模块之间共享的管理接口。

架构

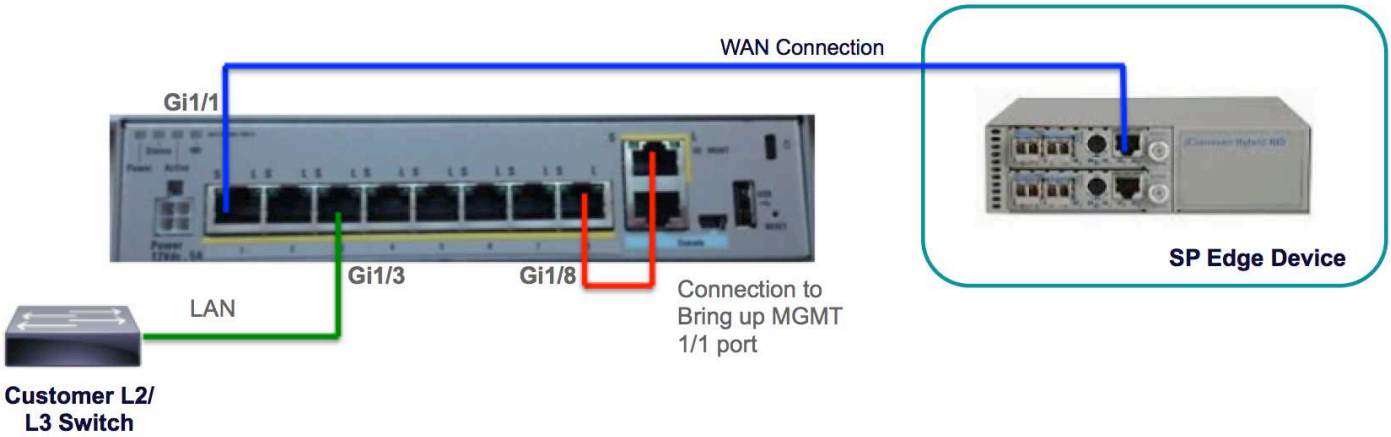
要求

- 从服务提供商边缘设备向ASA Firepower的单个专用互联网接入切换。
- 要将接口状态更改为up，必须访问管理接口。
- ASA的管理接口应保持正常，以便管理Firepower模块。
- 如果客户断开LAN设备，管理连接不应丢失。
- 管理架构应支持主用/备用广域网故障切换。

拓扑概述



低级设计



解决方案

以下配置将允许您通过VPN远程管理SFR模块，而无需预先设置任何LAN连接。

布线

- 使用以太网电缆将管理接口1/1连接到GigabitEthernet1/8接口。

  注意：ASA Firepower模块必须使用管理1/x（1/0或1/1）接口发送和接收管理流量。由于管理1/x接口不在数据平面上，因此您需要将管理接口物理连接到另一台LAN设备，以便通过控制平面将流量通过ASA。

  作为一盒式解决方案的一部分，您将使用以太网电缆将管理接口1/1连接到GigabitEthernet1/8接口。

IP Address

- **千兆以太网1/8接口**:192.168.10.1/24
- **SFR管理接口**:192.168.10.2/24
- **SFR网关**:192.168.10.1
- **管理1/1接口**:管理接口未配置任何IP地址。应为管理(MGMT)目的配置management-access命令。

本地和远程流量将位于以下子网中：

- 本地流量位于管理子网192.168.10.0/24上。
- 远程流量位于192.168.11.0/24子网上。

VPN和NAT

- 定义VPN策略。
- NAT命令应配置有route-lookup前缀，以使用路由查找确定出口接口，而不是使用NAT命令中指定的接口。

配置示例

```
!
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
!
```