SFR模块的管理在VPN通道的没有LAN交换机

目录

简介

在他们的投资组合的服务提供商提供管理的WAN服务。思科ASA Firepower平台提供设置的统一的威胁管理功能提供差异化服务。ASA Firepower设备安排管理的独立接口连接到LAN设备，然而，连接一个管理接口用LAN设备创建在LAN设备的一从属关系。

本文提供允许您管理思科ASA Firepower的一解决方案(SFR)模块，无需连接到LAN设备或使用从服务运营商边缘设备的第二个接口。

先决条件

使用的组件

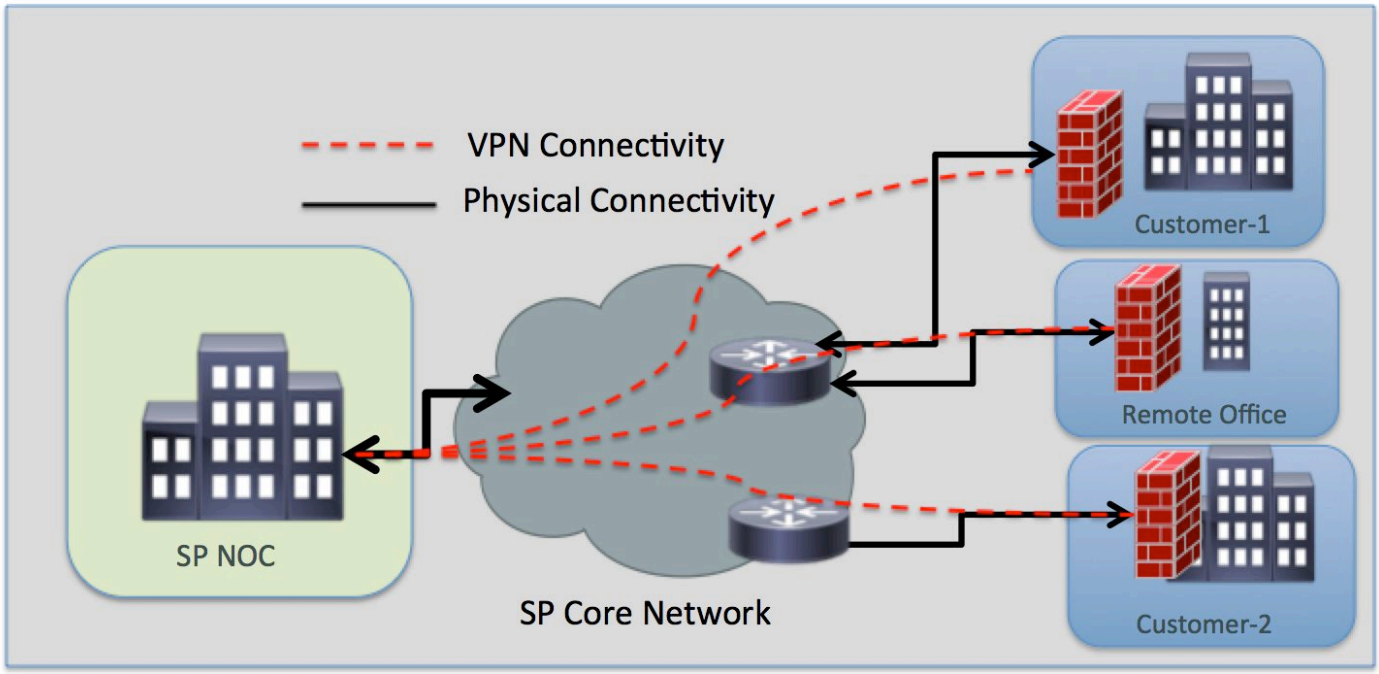
- 有Firepower (SFR)服务的ASA 5500-X系列平台。
- 共享在ASA和Firepower模块之间的管理接口。

体系结构

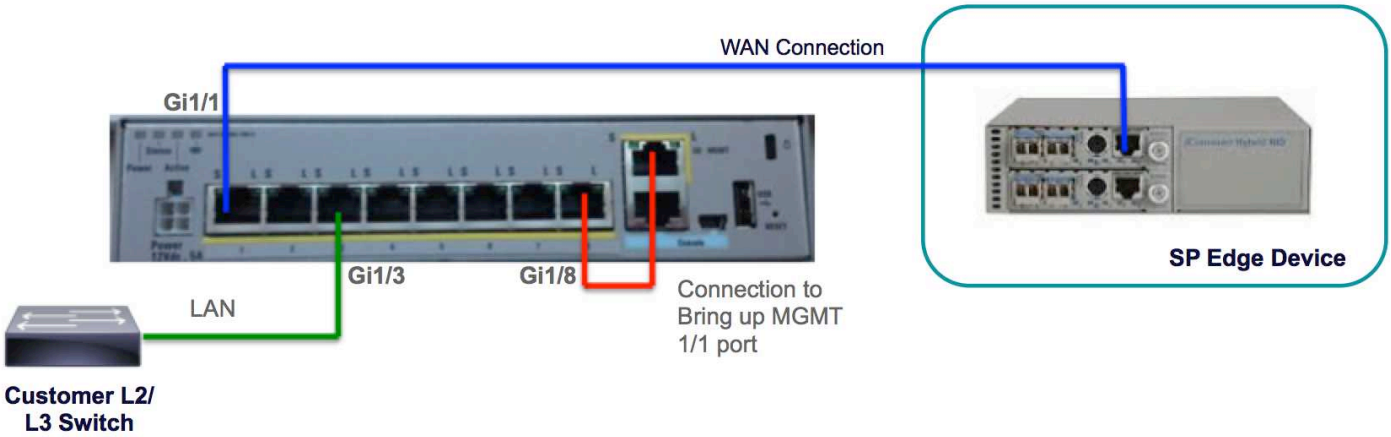
要求

- 单个专用互联网访问移交从服务运营商边缘设备到ASA Firepower。
- 对管理接口的访问是必要为了更改接口状态到。
- ASA的管理接口应该坚持为了管理Firepower模块。
- 管理连接，如果客户断开LAN设备，不应该丢失。
- 管理体系结构应该支持激活/备份广域网故障切换。

拓扑概述



低级设计



解决方案

以下配置将允许您远程管理在VPN的SFR模块，不用任何LAN连通性作为前提。

缚住

- 使用以太网电缆，连接管理接口1/1对GigabitEthernet1/8接口。

  Note:ASA Firepower模块必须使用管理1/x (1/0或1/1)接口发送和收到管理数据流。因为管理1/x接口不在数据层面，您需要物理的缚住管理接口到另一个LAN设备为了通过流量在控制层面的ASA。

  使用以太网电缆，作为一揽子解决方案的部分，您将连接管理接口1/1对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**：管理接口没有配置的任何IP地址。should命令为管理(MGMT)目的配置。

本地和远程流量在以下子网：

- 本地流量在管理子网192.168.10.0/24。
- 远程流量在192.168.11.0/24子网。

VPN和NAT

- 定义VPN策略。
- nat命令应该配置与路由前缀确定出口接口使用路由查找而不是使用指定的接口在nat命令。

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
!
```