Administración del Módulo SFR sobre el Túnel VPN sin Switch LAN

Contenido

Introducción

Los proveedores de servicios ofrecen servicios WAN gestionados en su cartera. La plataforma Cisco ASA Firepower proporciona un conjunto de funciones de gestión unificada de amenazas para proporcionar servicios diferenciados. Un dispositivo ASA Firepower tiene interfaces separadas para la conexión de administración a un dispositivo LAN; sin embargo, la conexión de una interfaz de administración con un dispositivo LAN crea una dependencia de un dispositivo LAN.

Este documento proporciona una solución que le permite administrar un módulo Cisco ASA Firepower (SFR) sin conectarse a un dispositivo LAN ni utilizar una segunda interfaz del dispositivo de extremo del proveedor de servicios.

Prerequisites

Componentes Utilizados

- Plataforma ASA serie 5500-X con servicios FirePOWER (SFR).
- Interfaz de administración compartida entre el módulo ASA y Firepower.

Arquitectura

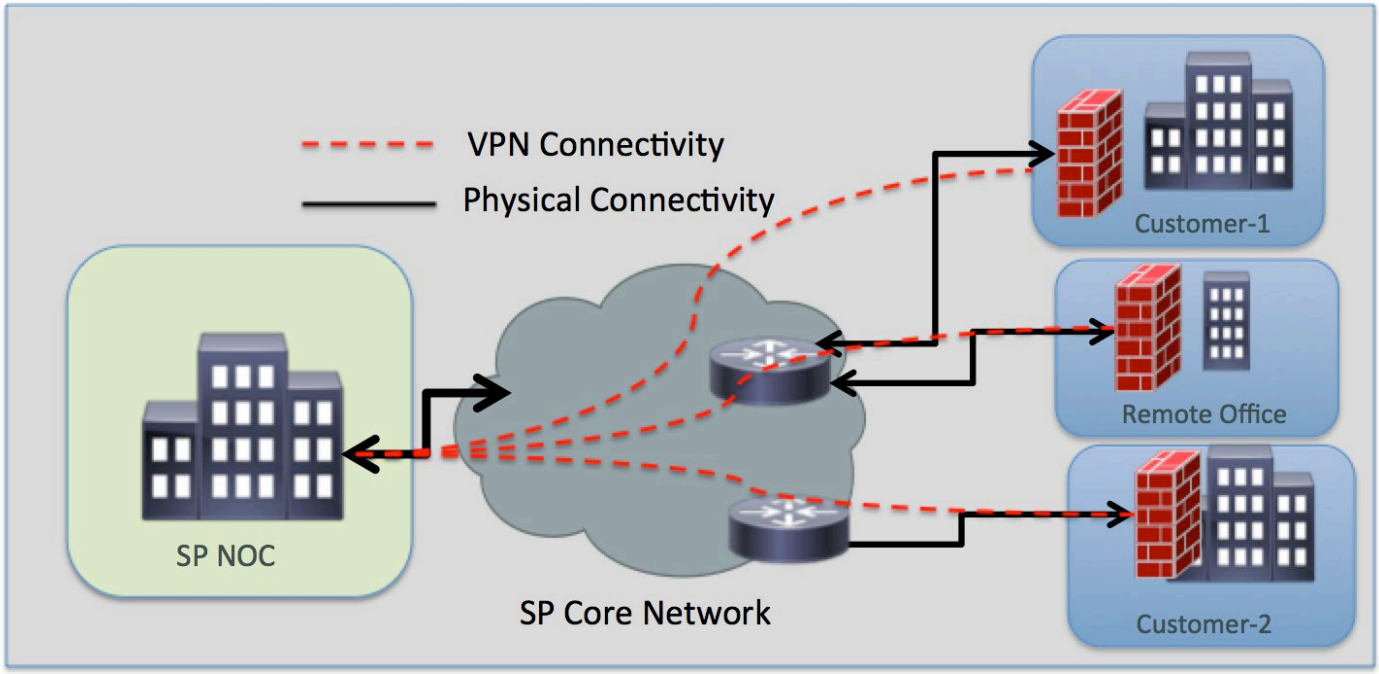
Requirements

- Entrega única de acceso a Internet dedicado desde el dispositivo de extremo del proveedor

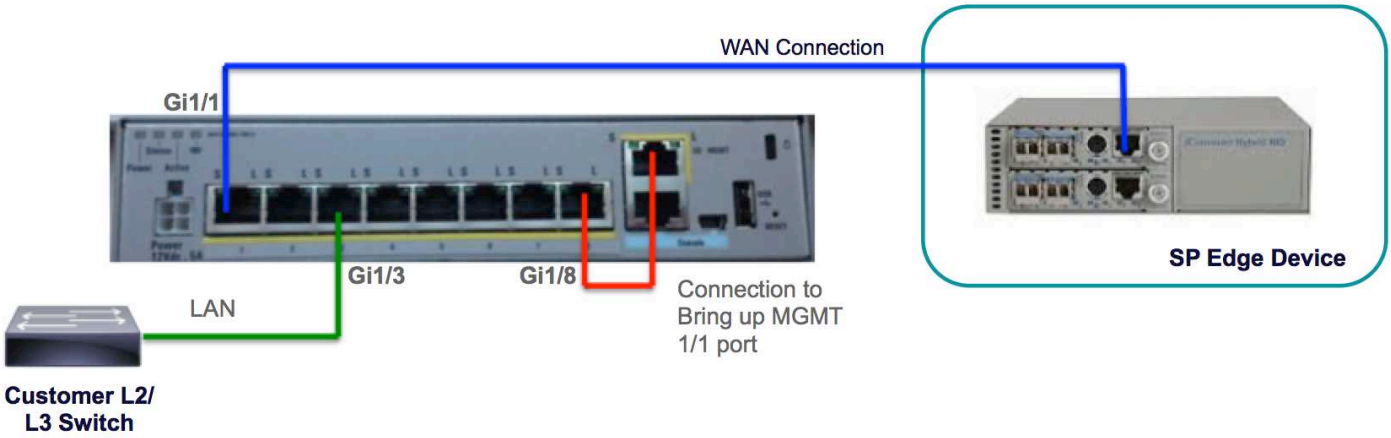
de servicios a ASA Firepower.

- El acceso a la interfaz de administración es necesario para cambiar el estado de la interfaz a activo.
- La interfaz de administración del ASA debe permanecer activa para administrar el módulo Firepower.
- La conectividad de administración no debe perderse si el cliente desconecta el dispositivo LAN.
- La arquitectura de administración debe admitir la conmutación por fallas de WAN activa/de respaldo.

Descripción general de la topología



Diseño de bajo nivel



Solución

Las siguientes configuraciones le permitirán administrar el módulo SFR a través de VPN de forma remota, sin ninguna conectividad LAN como requisito previo.

Cableado

- Conecte la interfaz de administración 1/1 a la interfaz GigabitEthernet1/8 mediante un cable Ethernet.

  Nota: El módulo ASA Firepower debe utilizar la interfaz Management 1/x (1/0 o 1/1) para enviar y recibir tráfico de administración. Dado que la interfaz de administración 1/x no está en el plano de datos, debe cablear físicamente la interfaz de administración a otro dispositivo LAN para pasar el tráfico a través del ASA sobre el plano de control.

  Como parte de la solución de un paquete, conectará la interfaz de administración 1/1 a la interfaz GigabitEthernet1/8 mediante un cable Ethernet.

IP Address

- **Interfaz GigabitEthernet 1/8**: 192.168.10.1/24
- **Interfaz de administración SFR**: 192.168.10.2/24
- **Puerta de enlace SFR**: 192.168.10.1
- **Interfaz de administración 1/1**: La interfaz de administración no tiene ninguna dirección IP configurada. El comando management-access debe configurarse para fines de administración (MGMT).

El tráfico local y remoto estará en las siguientes subredes:

- El tráfico local está en la subred de administración 192.168.10.0/24.
- El tráfico remoto está en la subred 192.168.11.0/24.

VPN y NAT

- Defina las políticas de VPN.
- El comando NAT se debe configurar con el prefijo route-lookup para determinar la interfaz de salida usando una búsqueda de ruta en lugar de utilizar la interfaz especificada en el comando NAT.

Ejemplo de configuración

```
!
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
!
```