Administración del módulo SFR sobre el túnel VPN sin el switch LAN

Contenido

Introducción

Los proveedores de servicio ofrecen el servicio PÁLIDO manejado en su cartera. La plataforma de la potencia de fuego de Cisco ASA proporciona el conjunto unificado de la función de administración de la amenaza para proporcionar los Servicios diferenciados. Un dispositivo de la potencia de fuego ASA hace que las interfaces diferentes para la Administración conecten con un dispositivo LAN, sin embargo, la conexión de una interfaz de administración con un dispositivo LAN crea una dependencia en un dispositivo LAN.

Este documento proporciona una solución que permita que usted maneje un módulo de la potencia de fuego de Cisco ASA (SFR) sin la conexión con un dispositivo LAN o usar una segunda interfaz del dispositivo de borde del proveedor de servicio.

Prerrequisitos

Componentes Utilizados

- Plataforma de las 5500-X Series ASA con los servicios de la potencia de fuego (SFR).
- Interfaz de administración que se comparte entre el ASA y el módulo de la potencia de fuego.

Arquitectura

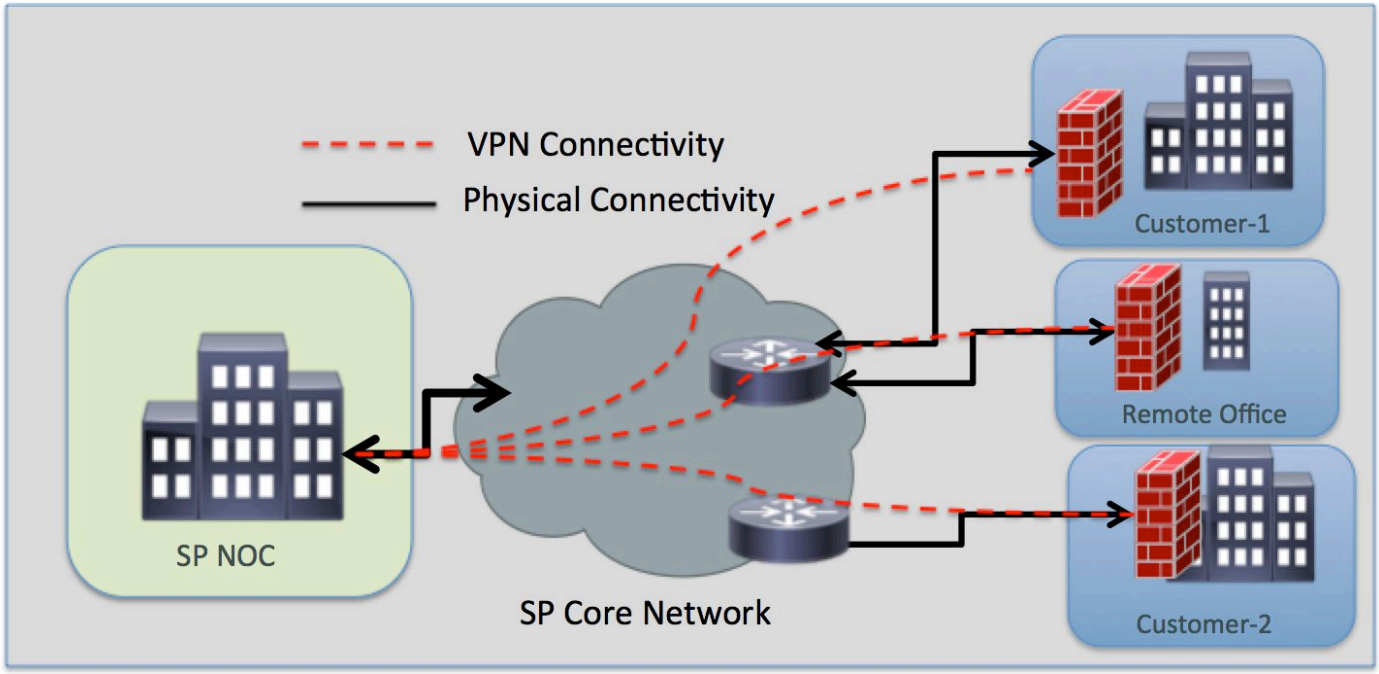
Requisitos

- Escoja las manos dedicadas del acceso a internet del dispositivo de borde del proveedor de

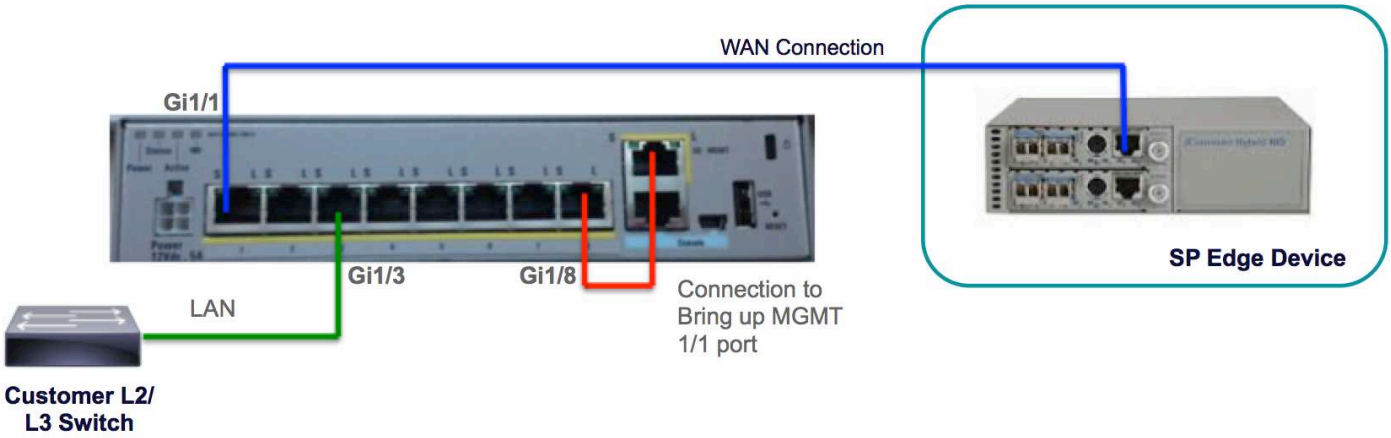
servicio a la potencia de fuego ASA.

- El acceso a la interfaz de administración es necesario para cambiar el estado de la interfaz a para arriba.
- La interfaz de administración del ASA debe permanecer para arriba para manejar el módulo de la potencia de fuego.
- La Conectividad de la Administración no debe ser perdida si el cliente desconecta el dispositivo LAN.
- La arquitectura de administración debe soportar la Conmutación por falla PÁLIDA activa/de reserva.

Descripción de la topología



Diseño de bajo nivel



Solución

Las configuraciones siguientes permitirán que usted maneje el módulo SFR sobre el VPN remotamente, sin ninguna conectividad LAN como requisito previó.

Cableado

- Conecte la interfaz de administración 1/1 con la interfaz GigabitEthernet1/8 usando un cable Ethernet.

  Nota: El módulo de la potencia de fuego ASA debe utilizar la interfaz de la Administración 1/x (1/0 o 1/1) para enviar y para recibir el tráfico de administración. Puesto que la interfaz de la Administración 1/x no está en el avión de los datos, usted necesita telegrafiar físicamente la interfaz de administración a otro dispositivo LAN para pasar el tráfico con el ASA sobre el avión del control.

  Como parte de la solución del uno-cuadro, usted conectará la interfaz de administración 1/1 con la interfaz GigabitEthernet1/8 usando un cable Ethernet.

DIRECCIÓN IP

- **Gigabitethernet 1/8 interfaz**: `192.168.10.1/24`
- **Interfaz de administración SFR**: `192.168.10.2/24`
- **Gateway SFR**: `192.168.10.1`
- **Interfaz de la Administración 1/1**: La interfaz de administración no tiene ninguna dirección IP configurada. El comando del `Acceso de administración` se debe configurar para el propósito de la Administración (MGMT).

El tráfico local y remoto estará en las subredes siguientes:

- 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 del VPN.
- El comando nat debe ser configurado con el prefijo de las ruta-`operaciones de búsqueda` para determinar la interfaz de egreso usando las operaciones de búsqueda de la ruta en vez de usar 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
!
```