Gerenciamento do módulo SFR sobre o túnel VPN sem switch LAN

Índice

[Introdução](#)
[Pré-requisitos](#)
[Componentes Utilizados](#)
[Arquitetura](#)
[Requisitos](#)
[Vista geral da topologia](#)
[Projeto de baixo nível](#)
[Solução](#)
[Cabeamento](#)
[IP Address](#)
[VPN e NAT](#)
[Exemplo de configuração](#)
[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Os provedores de serviços oferecem o serviço MACILENTO controlado em seu portfólio. A plataforma de Cisco ASA FirePOWER fornece o grupo unificado dos recursos de gerenciamento da ameaça para proporcionar Serviços diferenciados. Um dispositivo ASA FirePOWER manda interfaces separadas para o Gerenciamento conectar a um dispositivo de LAN, contudo, conectar uma interface de gerenciamento com um dispositivo de LAN cria uma dependência em um dispositivo de LAN.

Este documento fornece uma solução que permita que você controle um módulo de Cisco ASA FirePOWER (SFR) sem conectar a um dispositivo de LAN ou usar uma segunda relação do dispositivo de ponta do provedor de serviços.

Pré-requisitos

Componentes Utilizados

- Plataforma do 5500-X Series ASA com serviços de FirePOWER (SFR).
- Interface de gerenciamento que é compartilhada entre o ASA e o módulo de FirePOWER.

Arquitetura

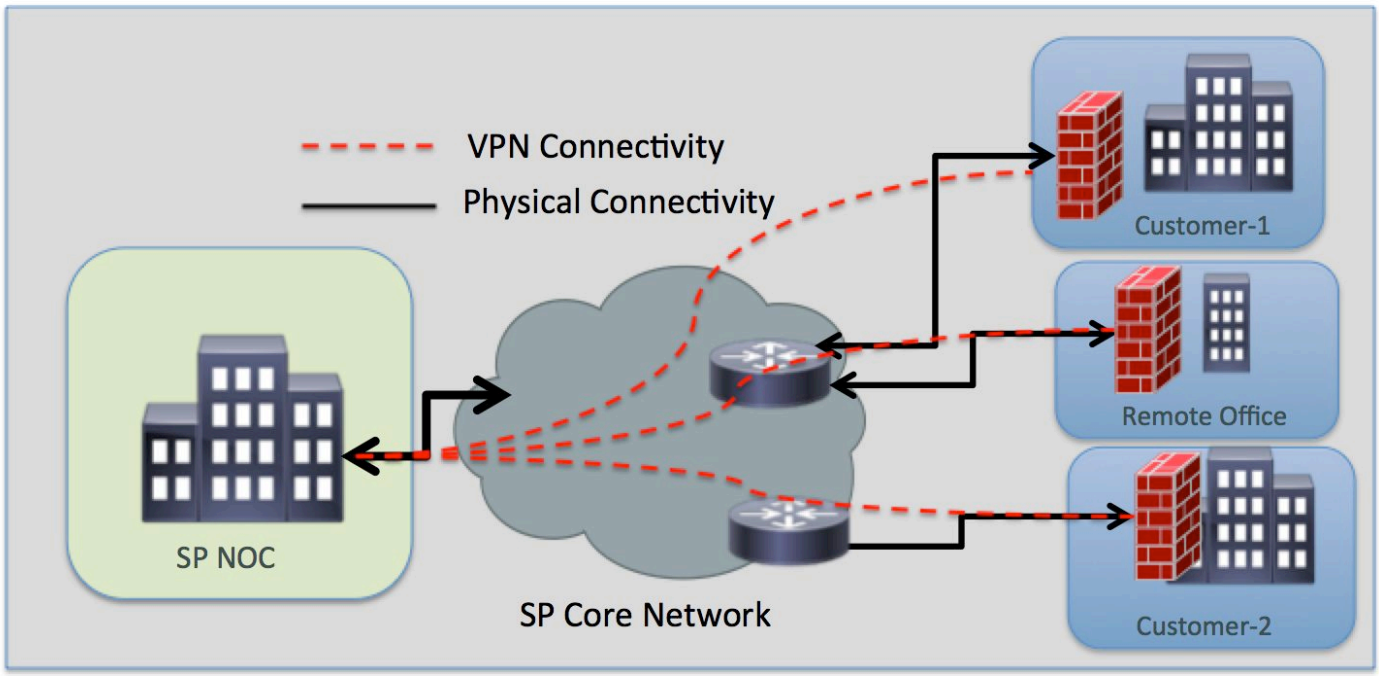
Requisitos

- Escolha entrega dedicada do acesso à internet do dispositivo de ponta do provedor de

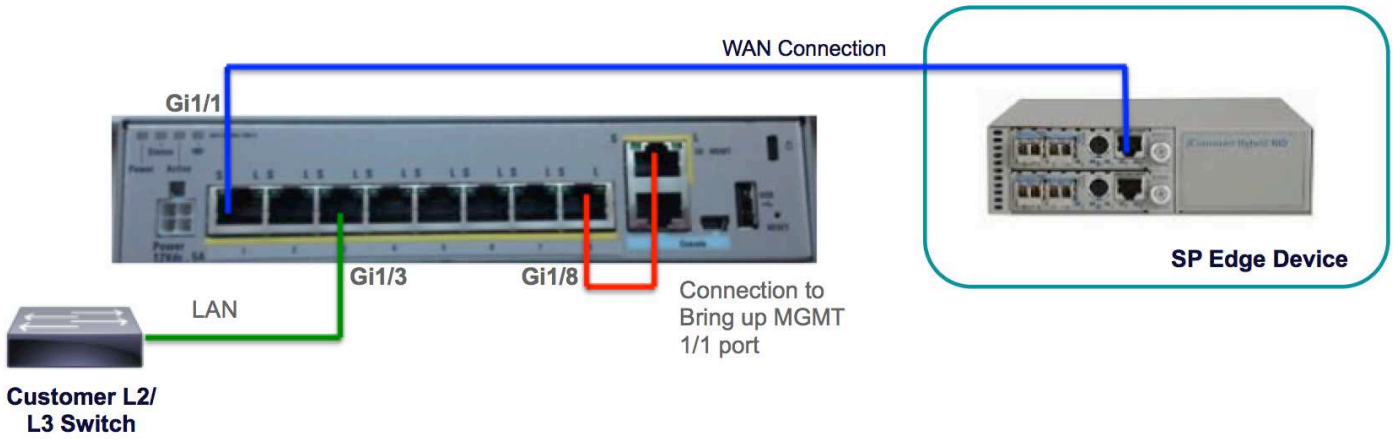
serviços a ASA FirePOWER.

- O acesso à interface de gerenciamento é necessário a fim mudar o estado da relação a acima.
- A interface de gerenciamento do ASA deve ficar acima a fim controlar o módulo de FirePOWER.
- A Conectividade do Gerenciamento não deve ser perdida se o cliente desliga o dispositivo de LAN.
- A arquitetura de gerenciamento deve apoiar Failover MACILENTO ativo/alternativo.

Vista geral da topologia



Projeto de baixo nível



Solução

As seguintes configurações permitirão que você controle o módulo SFR sobre o VPN remotamente, sem nenhuma conectividade de LAN como a condição prévia.

Cabeamento

- Conecte a interface de gerenciamento 1/1 à relação GigabitEthernet1/8 usando um cabo do Ethernet.

  Note: O módulo ASA FirePOWER deve usar a relação do Gerenciamento 1/x (1/0 ou 1/1) para enviar e receber o tráfego de gerenciamento. Desde que a relação do Gerenciamento 1/x não está no plano dos dados, você precisa de cabografar fisicamente a interface de gerenciamento a um outro dispositivo de LAN a fim passar o tráfego com o ASA sobre o plano do controle.

  Como parte da solução da um-caixa, você conectará a interface de gerenciamento 1/1 à relação GigabitEthernet1/8 usando um cabo do Ethernet.

IP Address

- **Gigabitethernet 1/8 de relação**: `192.168.10.1/24`
- **Interface de gerenciamento SFR**: `192.168.10.2/24`
- **Gateway SFR**: `192.168.10.1`
- **Relação do Gerenciamento 1/1**: A interface de gerenciamento não tem nenhum endereço IP de Um ou Mais Servidores Cisco ICM NT configurado. O comando do `acesso de gerenciamento` deve ser configurado para a finalidade do Gerenciamento (MGMT).

O tráfego local e remoto estará nas seguintes sub-redes:

- O tráfego local está na sub-rede de gerenciamento 192.168.10.0/24.
- O tráfego remoto está na sub-rede 192.168.11.0/24.

VPN e NAT

- Defina as políticas de VPN.
- O comando nat deve ser configurado com prefixo da rota-`consulta` para determinar a interface de saída usando uma consulta da rota em vez de usar a relação especificada no comando nat.

Exemplo de configuração

```
!
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
!
```