Gerenciamento do módulo SFR sobre túnel VPN sem switch LAN

Contents

Introduction

Os provedores de serviços oferecem serviço WAN gerenciado em seu portfólio. A plataforma Cisco ASA Firepower oferece um conjunto unificado de recursos de gerenciamento de ameaças para fornecer serviços diferenciados. Um dispositivo ASA Firepower tem interfaces separadas para a conexão de gerenciamento a um dispositivo de LAN, no entanto, conectar uma interface de gerenciamento a um dispositivo de LAN cria uma dependência em um dispositivo de LAN.

Este documento fornece uma solução que permite gerenciar um módulo Cisco ASA Firepower (SFR) sem se conectar a um dispositivo de LAN ou usar uma segunda interface do dispositivo de borda do provedor de serviços.

Prerequisites

Componentes Utilizados

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

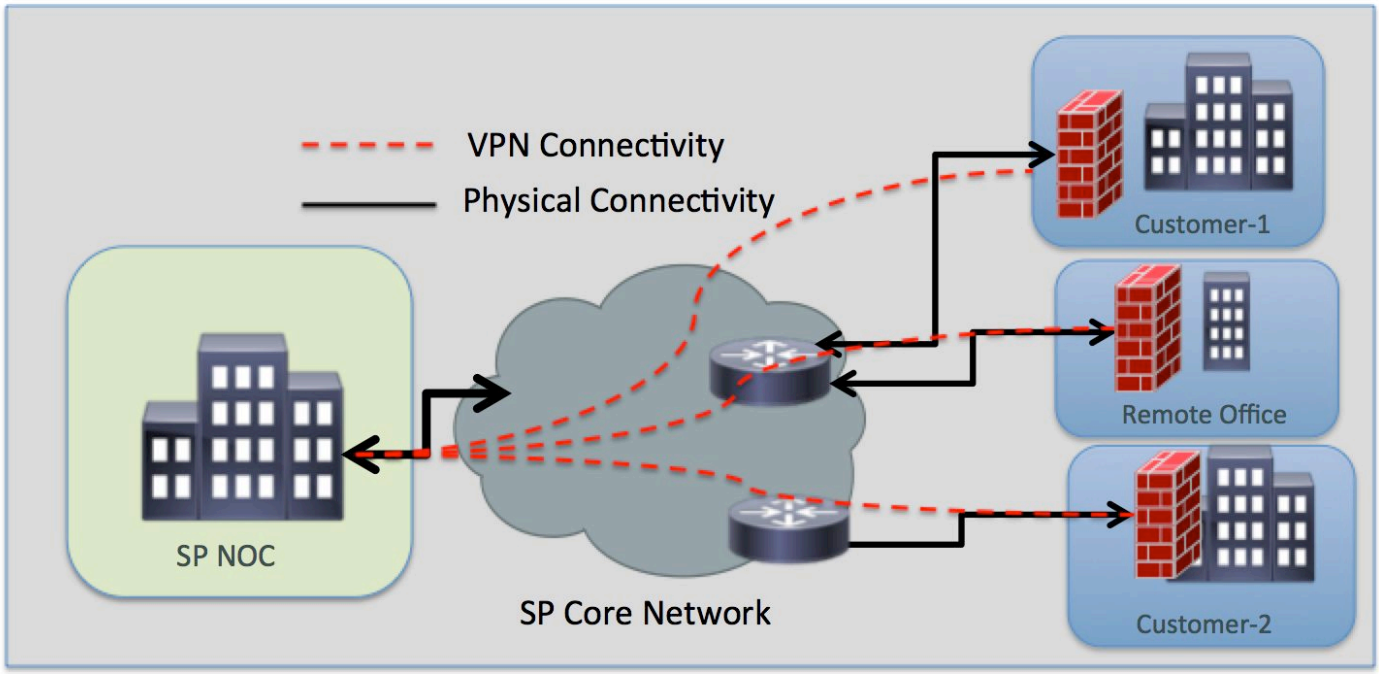
Arquitetura

Requirements

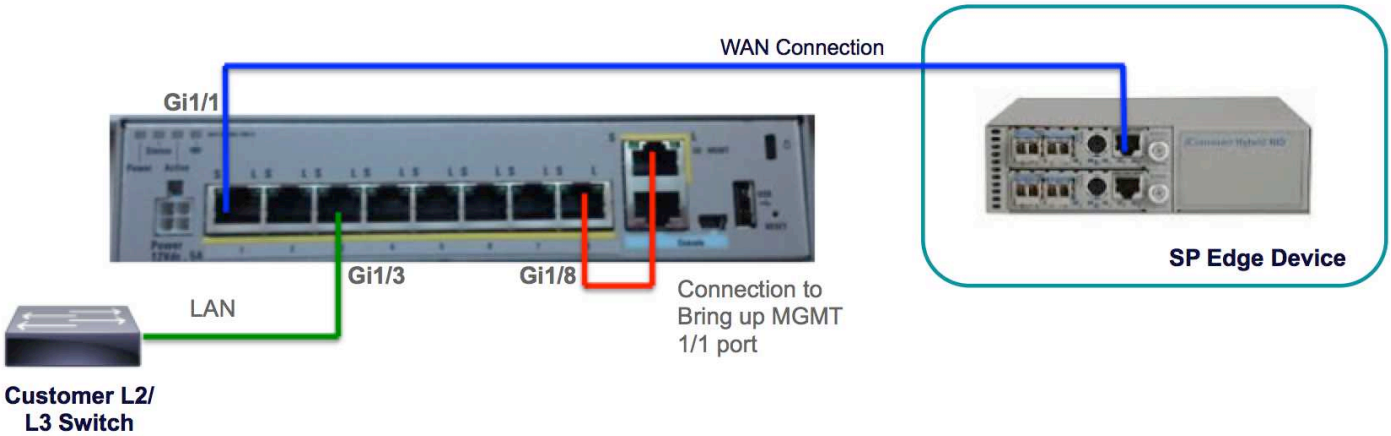
- Transferência de acesso à Internet dedicada única do dispositivo de borda do provedor de serviços para o ASA Firepower.

- O acesso à interface de gerenciamento é necessário para alterar o estado da interface para ativo.
- A interface de gerenciamento do ASA deve permanecer ativa para gerenciar o módulo Firepower.
- A conectividade de gerenciamento não deve ser perdida se o cliente desconectar o dispositivo da LAN.
- A arquitetura de gerenciamento deve suportar failover de WAN ativo/backup.

Visão geral da topologia



Projeto Básico



Solução

As configurações a seguir permitirão que você gerencie o módulo SFR sobre VPN remotamente, sem qualquer conectividade de LAN como pré-requisito.

Cabeamento

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

  Note: O módulo ASA Firepower deve usar a interface Management 1/x (1/0 ou 1/1) para enviar e receber tráfego de gerenciamento. Como a interface Management 1/x não está no plano de dados, você precisa cabear fisicamente a interface de gerenciamento para outro dispositivo de LAN para passar o tráfego pelo ASA pelo plano de controle.

  Como parte da solução de um pacote, você conectará a interface de gerenciamento 1/1 à interface GigabitEthernet1/8 usando um cabo ethernet.

IP Address

- **Interface GigabitEthernet 1/8**: 192.168.10.1/24
- **Interface de gerenciamento SFR**: 192.168.10.2/24
- **Gateway SFR**: 192.168.10.1
- **Interface de gerenciamento 1/1**: A interface de gerenciamento não tem nenhum endereço IP configurado. O comando management-access deve ser configurado para fins de 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 o prefixo route-lookup para determinar a interface de saída usando uma pesquisa de rota em vez de usar a interface 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
!
```