Gestion du module SFR sur tunnel VPN sans commutateur LAN

Contenu

Introduction

Les fournisseurs de services proposent des services WAN gérés dans leur portefeuille. La plate-forme Cisco ASA Firepower fournit un ensemble de fonctionnalités de gestion unifiée des menaces pour fournir des services différenciés. Un périphérique ASA Firepower dispose d'interfaces de gestion distinctes pour la connexion à un périphérique LAN. Toutefois, la connexion d'une interface de gestion à un périphérique LAN crée une dépendance sur un périphérique LAN.

Ce document fournit une solution qui vous permet de gérer un module Cisco ASA Firepower (SFR) sans vous connecter à un périphérique LAN ou en utilisant une deuxième interface à partir du périphérique de périphérie du fournisseur de services.

Conditions préalables

Components Used

- Plate-forme ASA 5500-X avec services Firepower (SFR).
- Interface de gestion partagée entre l'ASA et le module Firepower.

Architecture

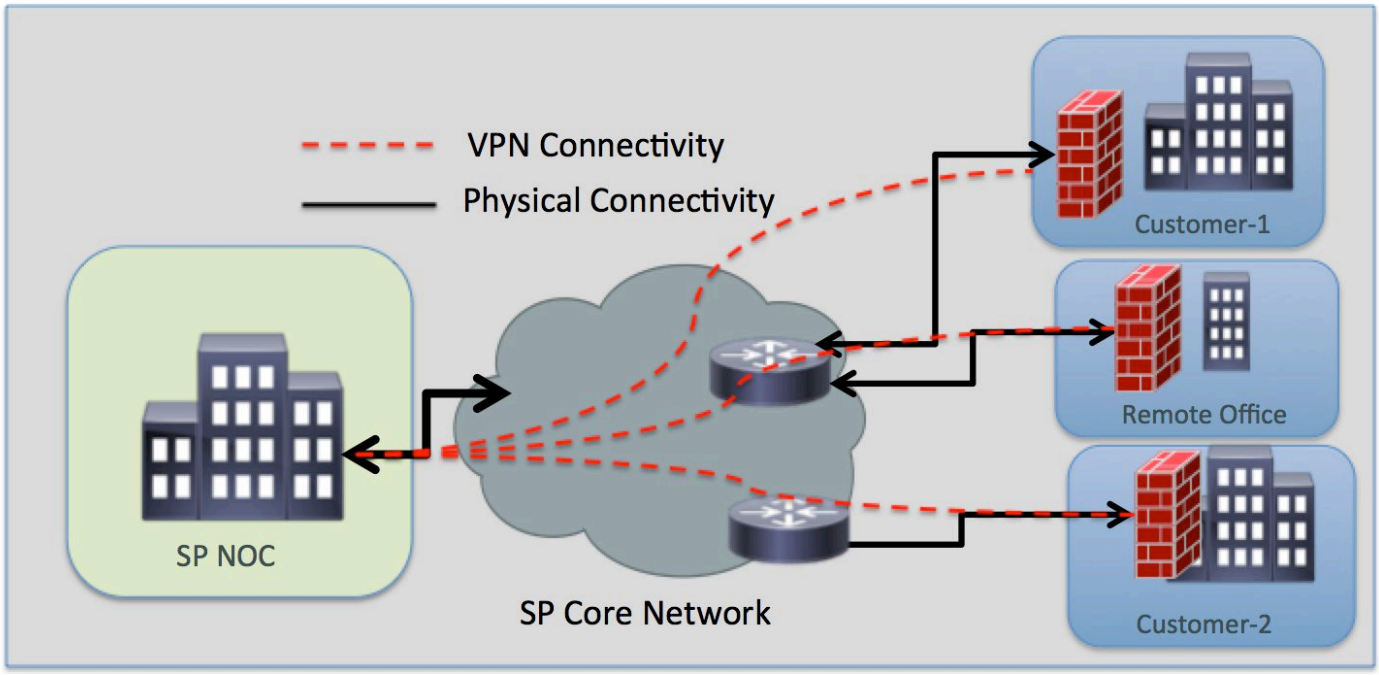
Conditions requises

- Transfert d'accès Internet dédié unique du périphérique de périphérie du fournisseur de

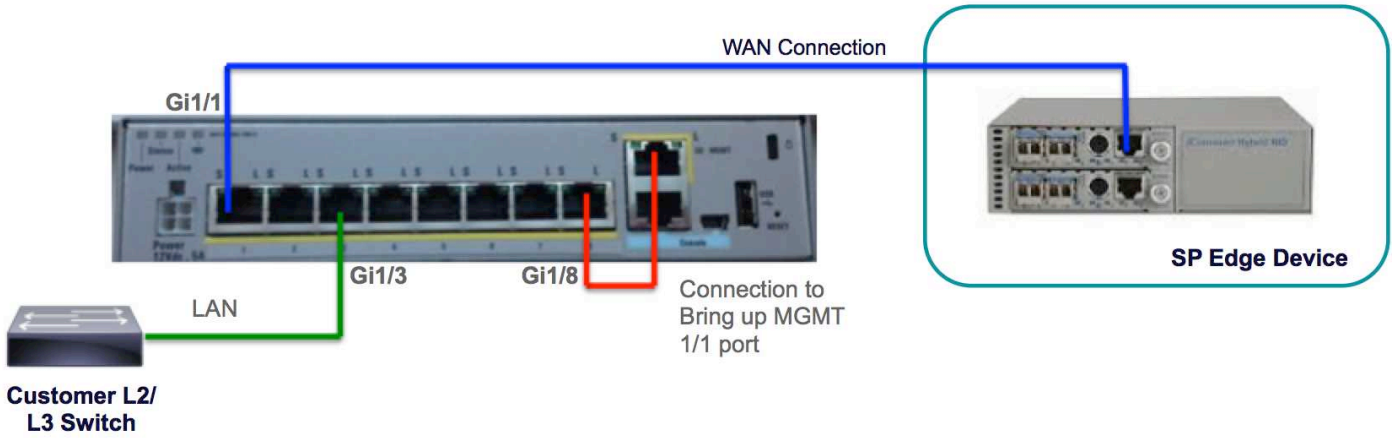
services à ASA Firepower.

- L'accès à l'interface de gestion est nécessaire pour que l'état de l'interface soit activé.
- L'interface de gestion de l'ASA doit rester active afin de gérer le module Firepower.
- La connectivité de gestion ne doit pas être perdue si le client déconnecte un périphérique LAN.
- L'architecture de gestion doit prendre en charge le basculement WAN actif/de sauvegarde.

Présentation de la topologie



Conception de bas niveau



Solution

Les configurations suivantes vous permettront de gérer le module SFR sur VPN à distance, sans aucune connectivité LAN préalable.

Câblage

- Connectez l'interface de gestion 1/1 à l'interface GigabitEthernet1/8 à l'aide d'un câble Ethernet.

  Note: Le module ASA Firepower doit utiliser l'interface Management 1/x (1/0 ou 1/1) pour envoyer et recevoir du trafic de gestion. Comme l'interface Management 1/x ne se trouve pas sur le plan de données, vous devez connecter physiquement l'interface de gestion à un autre périphérique LAN afin de transmettre le trafic via l'ASA sur le plan de contrôle.

  Dans le cadre de la solution prête à l'emploi, vous connecterez l'interface de gestion 1/1 à l'interface GigabitEthernet1/8 à l'aide d'un câble Ethernet.

Adresse IP

- **Interface GigabitEthernet 1/8** : 192.168.10.1/24
- **Interface de gestion SFR** : 192.168.10.2/24
- **Passerelle SFR** : 192.168.10.1
- **Interface Management 1/1** : Aucune adresse IP n'est configurée sur l'interface de gestion. La commande management-access doit être configurée à des fins de gestion (MGMT).

Le trafic local et distant se trouve sur les sous-réseaux suivants :

- Le trafic local se trouve sur le sous-réseau de gestion 192.168.10.0/24.
- Le trafic distant se trouve sur le sous-réseau 192.168.11.0/24.

VPN et NAT

- Définissez les stratégies VPN.
- La commande NAT doit être configurée avec le préfixe route-lookup pour déterminer l'interface de sortie à l'aide d'une recherche de route au lieu d'utiliser l'interface spécifiée dans la commande NAT.

Exemple de configuration

```
!
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
!
```