

Gestion de module SFR au-dessus de tunnel VPN sans commutateur de RÉSEAU LOCAL

Contenu

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Architecture](#)

[Conditions requises](#)

[Aperçu de topologie](#)

[Conception inférieure](#)

[Solution](#)

[Câblage](#)

[Adresse IP](#)

[VPN et NAT](#)

[Exemple de configuration](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Service WAN géré par offre de fournisseurs de services dans leur dossier. La plate-forme de puissance de feu de Cisco ASA fournit le positionnement unifié de fonctionnalité de gestion de menace pour fournir la Différenciation de services. Un périphérique de puissance de feu ASA fait se connecter les interfaces distinctes pour la Gestion à un périphérique de RÉSEAU LOCAL, cependant, connecter une interface de gestion avec un périphérique de RÉSEAU LOCAL crée une dépendance sur un périphérique de RÉSEAU LOCAL.

Ce document fournit une solution qui te permet pour gérer un module de la puissance de feu de Cisco ASA (SFR) sans se connecter à un périphérique de RÉSEAU LOCAL ou utiliser une deuxième interface du périphérique de périphérie de fournisseur de services.

Conditions préalables

[Composants utilisés](#)

- Plate-forme de gamme 5500-X ASA avec des services de la puissance de feu (SFR).
- Interface de gestion qui est partagée entre l'ASA et le module de puissance de feu.

Architecture

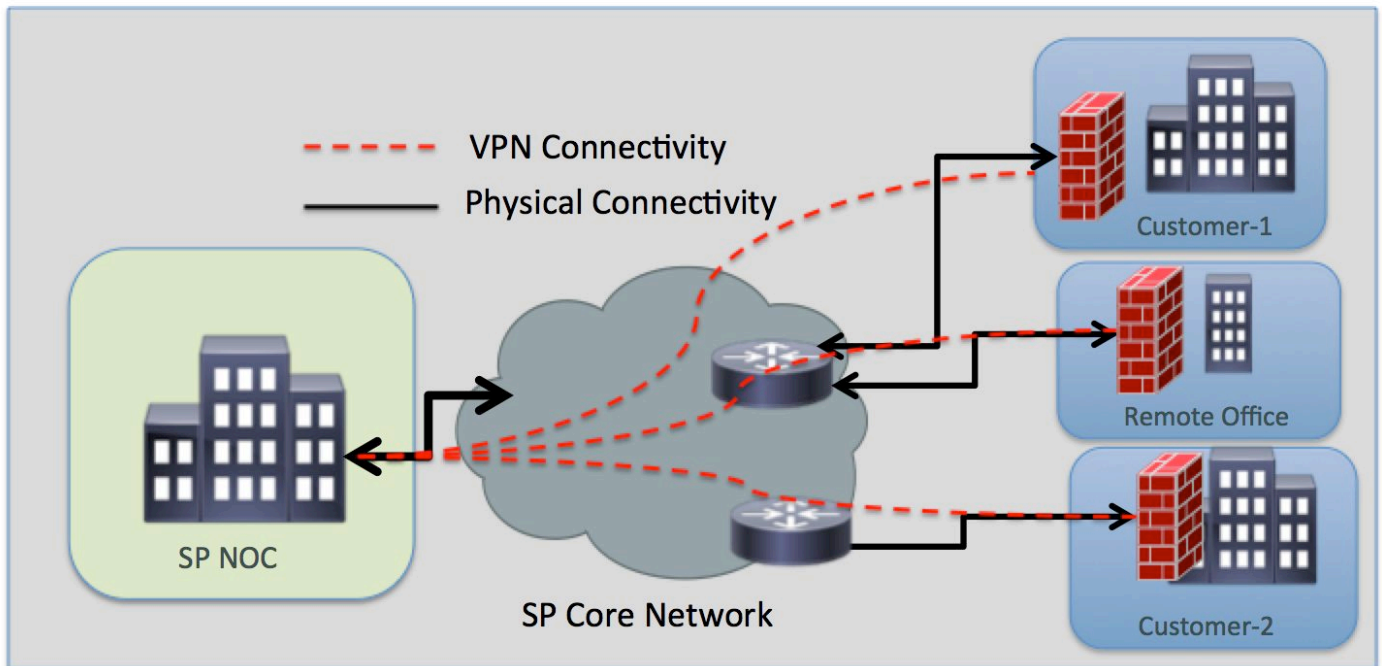
Conditions requises

- Choisissez le transfert dédié d'accès d'Internet du périphérique de périphérie de fournisseur

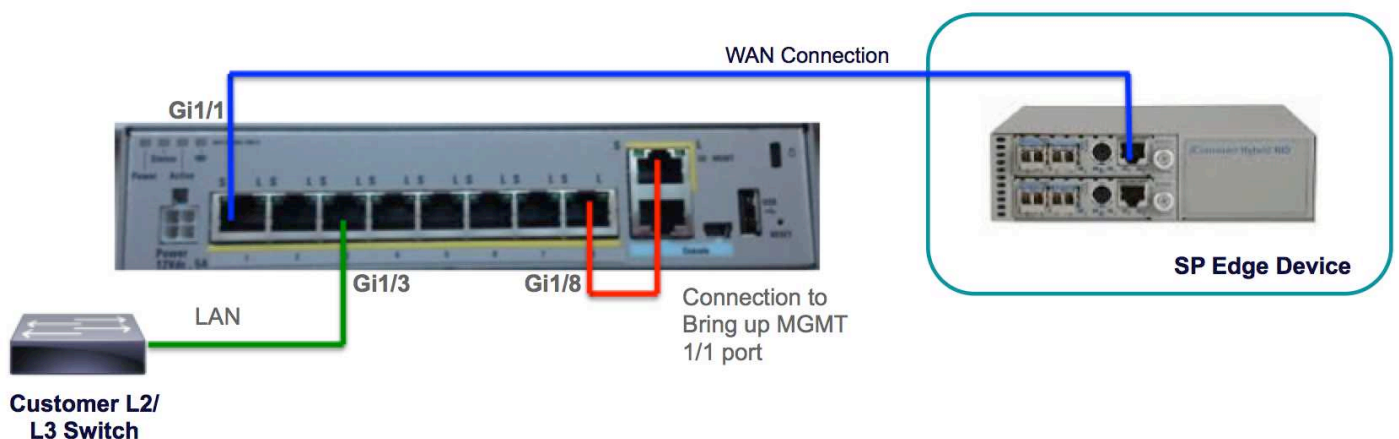
de services à la puissance de feu ASA.

- Access à l'interface de gestion est nécessaire afin de changer l'état d'interface à.
- L'interface de gestion de l'ASA devrait rester afin de gérer le module de puissance de feu.
- La Connectivité de Gestion ne devrait pas être perdue si le client déconnecte le périphérique de RÉSEAU LOCAL.
- L'architecture de Gestion devrait prendre en charge Basculement BLÈME actif/de sauvegarde.

Aperçu de topologie



Conception inférieure



Solution

Les configurations suivantes te permettront pour gérer le module SFR au-dessus du VPN à distance, sans n'importe quelle Connectivité de RÉSEAU LOCAL comme condition préalable.

Câblage

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

Remarque: Le module de puissance de feu ASA doit employer l'interface de la Gestion 1/x (1/0 ou 1/1) pour envoyer et recevoir le trafic d'administration. Puisque l'interface de la Gestion 1/x n'est pas sur le plan de données, vous devez câbler physiquement l'interface de gestion à un autre périphérique de RÉSEAU LOCAL afin de passer le trafic par l'ASA au-dessus de l'avion de contrôle.

Comme partie de la solution d'un-case, vous connecterez l'interface de gestion 1/1 à l'interface GigabitEthernet1/8 utilisant un câble d'Ethernets.

Adresse IP

- **GigabitEthernets 1/8 interface** : 192.168.10.1/24
- **Interface de gestion SFR** : 192.168.10.2/24
- **Passerelle SFR** : 192.168.10.1
- **Interface de la Gestion 1/1** : L'interface de gestion n'a aucune adresse IP configurée. La commande de Gestion-Access devrait être configurée pour le but de Gestion (GESTION).

Les gens du pays et le trafic distant seront sur les sous-réseaux suivants :

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

VPN et NAT

- Définissez les règles VPN.
- La commande NAT devrait être configurée avec le préfixe de recherche de route pour déterminer l'interface de sortie utilisant 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  
!
```