

# LAN スイッチのない VPN トンネルでの SFR モジュールの管理

## 目次

[はじめに](#)

[前提条件](#)

[使用するコンポーネント](#)

[アーキテクチャ](#)

[要件](#)

[トポロジの概要](#)

[低レベル設計](#)

[解決策](#)

[ケーブル接続](#)

[IP アドレス](#)

[VPN および NAT](#)

[設定例](#)

[Cisco サポート コミュニティ - 特集対話](#)

## 概要

サービスプロバイダーはポートフォリオの管理された WAN サービスを提供します。Cisco ASA Firepower プラットフォームは差別化サービスを提供するために統一された脅威 管理機能セットを提供します。ASA Firepower デバイスは管理のための個々のインターフェイスを LAN デバイスに接続されてもらいますが、LAN デバイスが付いているマネージメントインターフェイスを接続することは LAN デバイスの依存関係を作成します。

この資料はソリューションを提供したものです LAN デバイスに接続するか、またはサービスプロバイダーエッジ デバイスからの第 2 インターフェイスを使用しないで Cisco ASA Firepower (SFR) モジュールを管理することを可能にする。

## 前提条件

### 使用するコンポーネント

- Firepower (SFR) サービスの ASA 5500-X シリーズ プラットフォーム。
- ASA と Firepower モジュールの間で共有されるマネージメントインターフェイス。

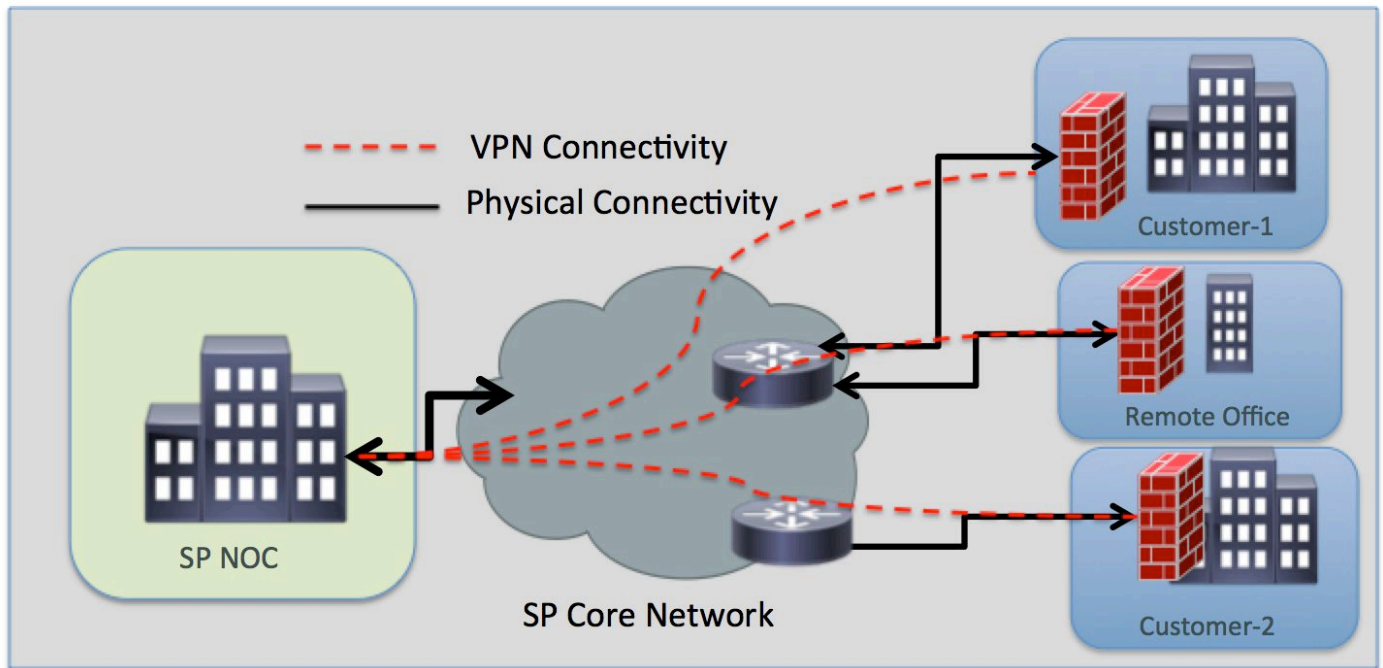
## アーキテクチャ

### 要件

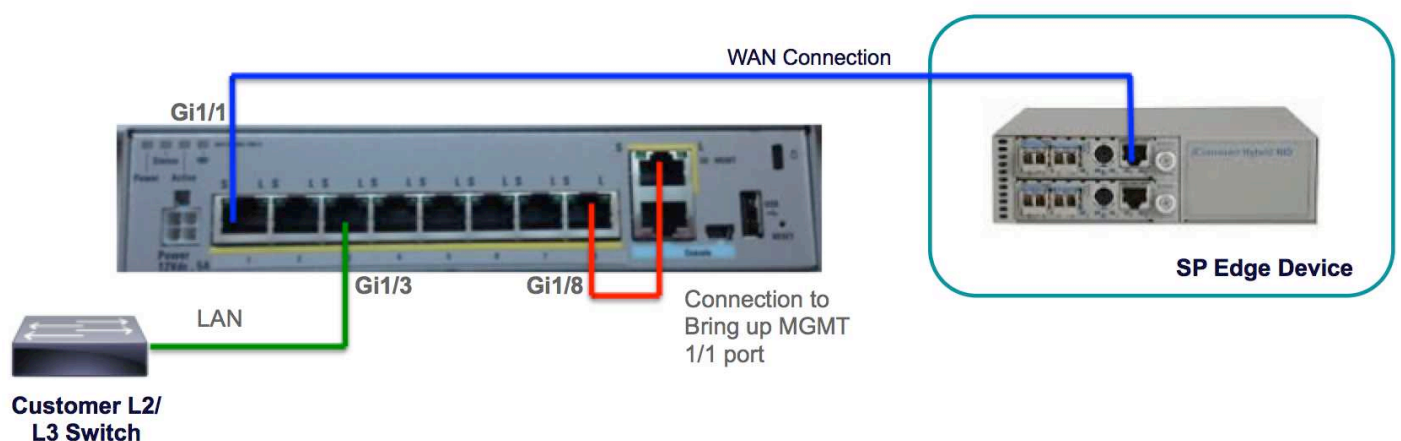
- サービスプロバイダーエッジ デバイスからの ASA Firepower への単一専用のインターネット アクセス ハンドオフ。

- マネージメントインターフェイスへのアクセスはにインターフェイス状態を変更して必要です。
- ASA のマネージメントインターフェイスは Firepower モジュールを管理するためにアップ状態に留まるはずでずです。
- 管理接続は顧客が LAN デバイスを切る場合失うべきではありません。
- 管理アーキテクチャはアクティブな/バックアップ WAN フェールオーバーをサポートする必要があります。

## トポロジの概要



## 低レベル設計



## 解決策

次の設定は前提条件として LAN 接続なしで VPN 上の SFR モジュールを、リモートで管理することを可能にします。

## 配線

- イーサネットケーブルを使用して GigabitEthernet1/8 インターフェイスにマネージメントインターフェイス 1/1 を接続して下さい。

注: ASA Firepower モジュールはマネジメントトラフィックを送信し、受信するのに管理 1/x ( 1/0 か 1/1 ) インターフェイスを使用する必要があります。管理 1/x インターフェイスがデータ平面にないので、物理的にコントロールプレーンを ASA を通してトラフィックを通過させるために別の LAN デバイスにマネージメントインターフェイスをケーブル接続する必要があります。

ワンボックス ソリューションの一部として、イーサネットケーブルを使用して GigabitEthernet1/8 インターフェイスにマネージメントインターフェイス 1/1 を接続します。

## IP アドレス

- GigabitEthernet 1/8 のインターフェイス: 192.168.10.1/24
- SFR マネージメントインターフェイス: 192.168.10.2/24
- SFR ゲートウェイ: 192.168.10.1
- 管理 1/1 インターフェイス: マネージメントインターフェイスに設定される IP アドレスがありません。コマンドは管理 ( MGMT ) 目的で設定する必要があります。

ローカルおよびリモートトラフィックは次のサブネットにあります:

- ローカルトラフィックは管理サブネット 192.168.10.0/24 にあります。
- リモートトラフィックは 192.168.11.0/24 サブネットにあります。

## VPN および NAT

- VPN ポリシーを定義して下さい。
- Nat コマンドはルート プレフィックスで規定される Nat コマンドでインターフェイスを使用するかわりにルート ルックアップを使用して出力 インターフェイスを判別するために設定する必要があります。

## 設定例

```
!  
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
!
```