LAN スイッチのない VPN トンネルでの SFR モジュールの管理

内容

概要

サービス プロバイダーは、そのポートフォリオで管理型 WAN サービスを提供します。Cisco ASA Firepowerプラットフォームは、差別化されたサービスを提供するための統合脅威管理機能セットを提供します。ASA Firepowerデバイスには、管理用にLANデバイスに接続するための別のインターフェイスがありますが、管理インターフェイスをLANデバイスに接続すると、LANデバイスに依存することになります。

このドキュメントでは、LANデバイスに接続したり、サービスプロバイダーのエッジデバイスから2番目のインターフェイスを使用したりせずに、Cisco ASA Firepower(SFR)モジュールを管理できるソリューションについて説明します。

前提条件

使用するコンポーネント

- ASA 5500-Xシリーズプラットフォームと Firepower(SFR)サービス
- ASAとFirepowerモジュール間で共有される管理インターフェイス。

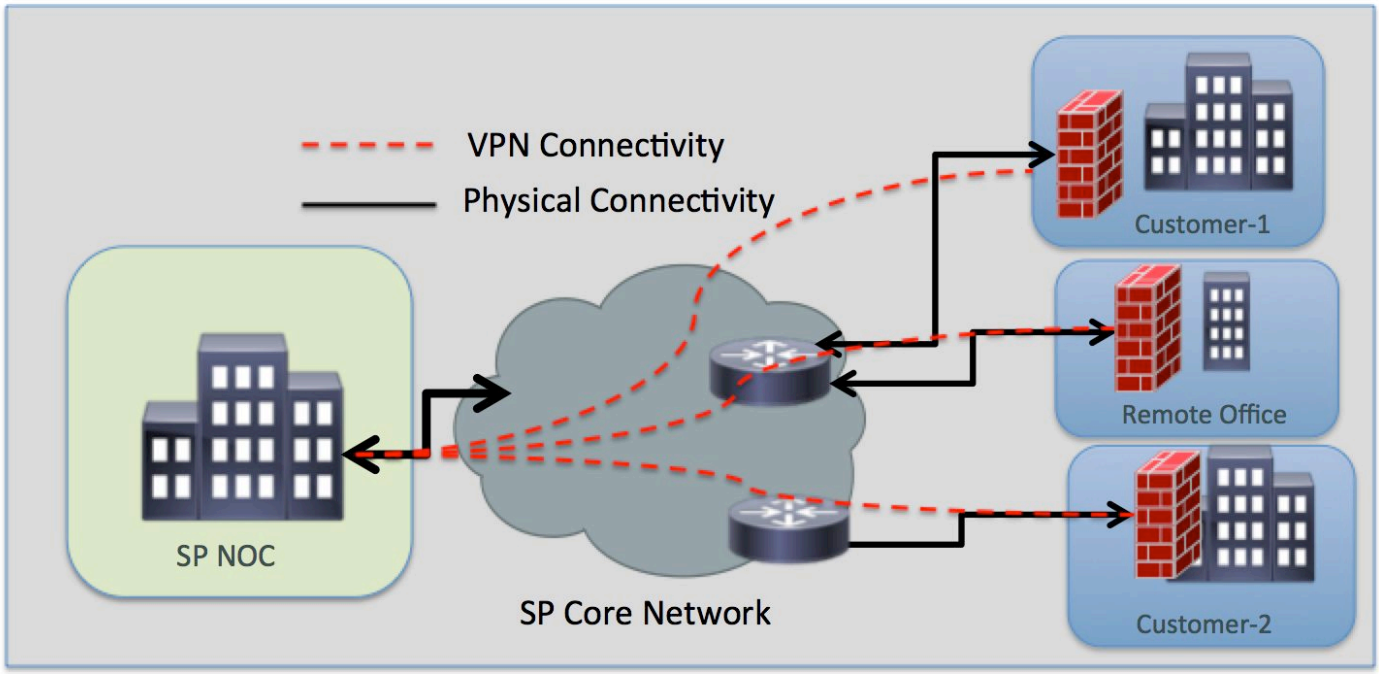
アーキテクチャ

要件

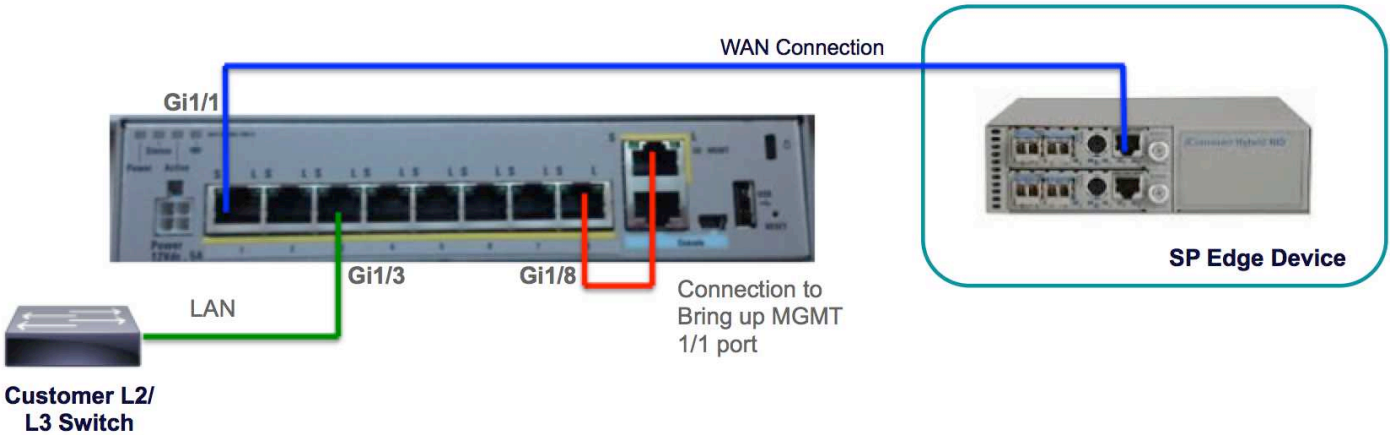
- サービスプロバイダーのエッジデバイスからASA Firepowerへの単一の専用インターネットアクセスハンドオフ。

- インターフェイスの状態をupに変更するには、管理インターフェイスへのアクセスが必要です。
- Firepowerモジュールを管理するには、ASAの管理インターフェイスがアップしたままである必要があります。
- お客様がLANデバイスを切断した場合は、管理接続を失わないでください。
- 管理アーキテクチャは、アクティブ/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



詳細設計



解決方法

次の設定では、LAN接続を必要とせずに、VPN経由でSFRモジュールをリモートで管理できます。

ケーブル接続

- イーサネットケーブルを使用して、管理インターフェイス1/1をGigabitEthernet1/8インターフェイスに接続します。

  注：ASA Firepowerモジュールは、管理トラフィックを送受信するために管理1/x（1/0または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インターフェイスはデータプレーン上にないため、コントロールプレーン上でASAをトラフィックが通過するように、管理インターフェイスを別のLANデバイスに物理的に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管理インターフェイス1/1をGigabitEthernet1/8インターフェイスに接続します。

iSCSIポータルの

- **GigabitEthernet 1/8インターフェイス**:192.168.10.1/24
- **SFR管理インターフェイス**: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**:管理インターフェイスにIPアドレスが設定されていません。management-accessコマンドは、管理(MGMT)の目的で設定する必要があります。

ローカルトラフィックとリモートトラフィックは、次のサブネットに存在します。

- 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ポリシーを定義します。
- NATコマンドは、NATコマンドで指定されたインターフェイスを使用する代わりに、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決定するために、route-lookup prefixで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
!
```