Менеджмент модуля SFR по VPN-туннелю без коммутатора локальной сети (LAN)

Содержание

Введение

Поставщики услуг предлагают управляемую услугу глобальной сети (WAN) в своем портфеле. Платформа Огневой мощи Cisco ASA предоставляет объединенный набор функций управления угрозами для обеспечения дифференцированных сервисов. Устройство Огневой мощи ASA имеет отдельные интерфейсы для подключения управления к устройству LAN (локальной сети), однако, подключение интерфейса управления с устройством LAN (локальной сети) создает зависимость от устройства LAN (локальной сети).

Этот документ предоставляет решение, которое позволяет вам управлять Огневой мощью Cisco ASA (SFR) модуль, не соединяясь с устройством LAN (локальной сети) или с помощью второго интерфейса от устройства поставщика услуг EDGE.

Предварительные условия

Используемые компоненты

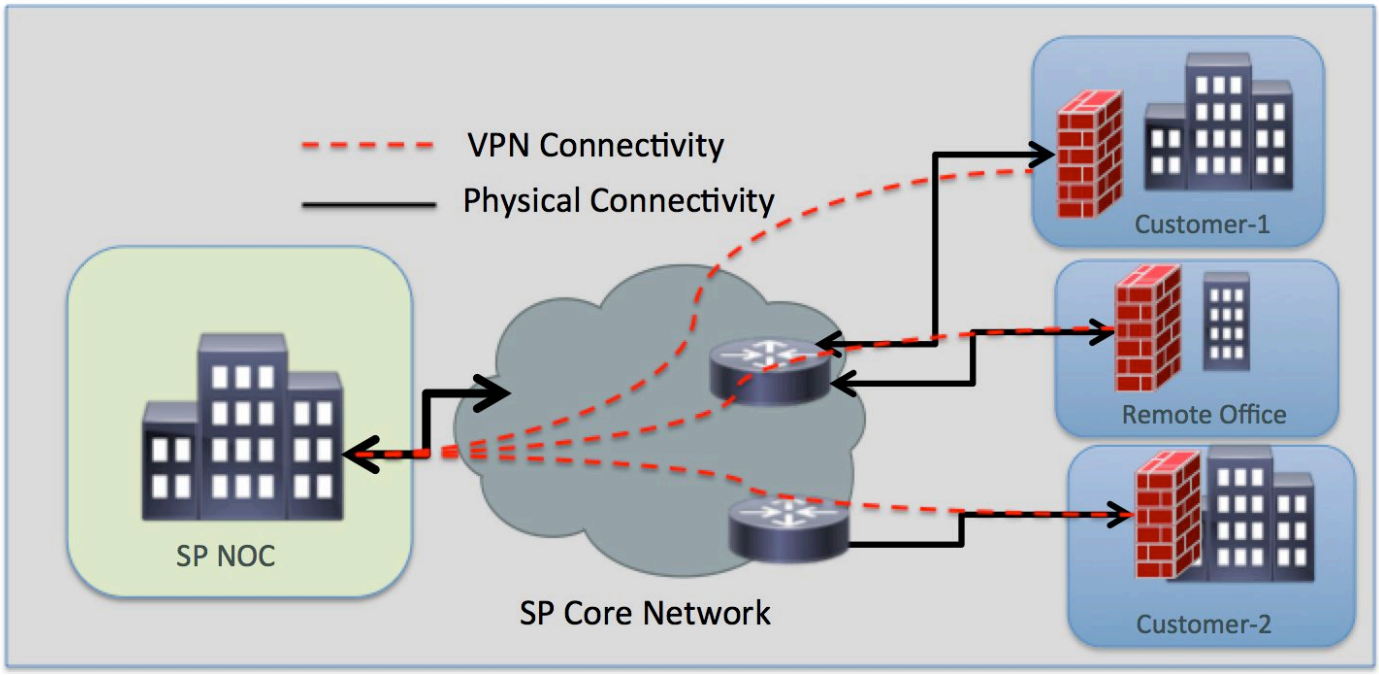
- ASA платформа серии 5500-X с Огневой мощью (SFR) сервисы.
- Интерфейс управления, который разделен между модулем Огневой мощи и ASA.

Архитектура

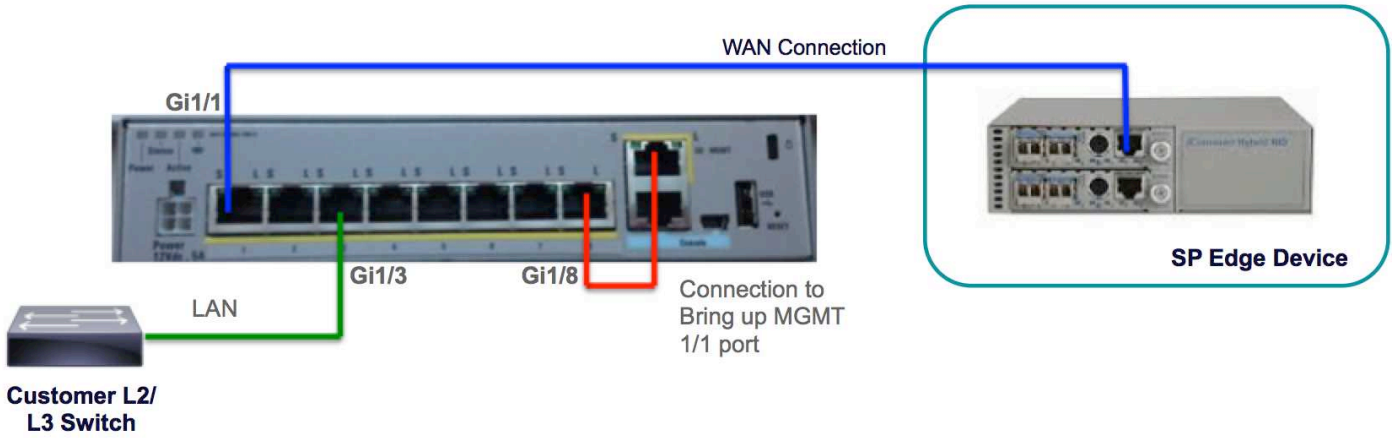
Требования

- Одиночный специализированный доступ в Интернет handoff от устройства Поставщика услуг EDGE до Огневой мощи ASA.
- Доступ к интерфейсу управления необходим для изменения интерфейсного состояния на.
- Интерфейс управления ASA должен не лечь спать для управления модулем Огневой мощи.
- Если клиент разъединяет устройство LAN (локальной сети), подключение менеджмента не должно быть потеряно.
- Архитектура управления должна поддержать Активное/Резервное аварийное переключение глобальной сети (WAN).

Обзор топологии



Низкоуровневый дизайн



Решение

Следующие конфигурации позволят вам управлять модулем SFR по VPN удаленно без

любого подключения по локальной сети как предпосылка.

Кабельное подключение

- Подключите Интерфейс управления 1/1 с интерфейсом GigabitEthernet1/8 использование кабеля Ethernet.

  Примечание: Модуль Огневой мощи ASA должен использовать менеджмент 1/x (1/0 или 1/1) интерфейс, чтобы передать и получить трафик управления. Так как менеджмент 1/x интерфейс не находится на плоскости данных, необходимо физически телеграфировать интерфейс управления к другому устройству LAN (локальной сети) для передачи трафика через ASA по уровню управления.

  Как часть одного готового решения, вы подключите Интерфейс управления 1/1 с интерфейсом GigabitEthernet1/8 использование кабеля Ethernet.

IP-адрес

- **Интерфейс GigabitEthernet 1/8**: `192.168.10.1/24`
- **Интерфейс управления SFR**: `192.168.10.2/24`
- **SFR шлюз**: `192.168.10.1`
- **Менеджмент 1/1 Интерфейс**: Интерфейс управления не имеет никакого IP-адреса настроенным. `Команда management-access` должна быть настроена для управления (MGMT) цель.

Локальный и удаленный трафик будет на следующих подсетях:

- Локальный трафик находится на подсети управления 192.168.10.0/24.
- Удаленный трафик находится на 192.168.11.0/24 подсети.

VPN и NAT

- Определите политику VPN.
- Команда NAT должна быть настроена с префиксом `поиска маршрута` для определения исходящего интерфейса с помощью поиска маршрута вместо того, чтобы использовать интерфейс, заданный в команде NAT.

Пример конфигурации

```
!
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
!
```