# Gestione del modulo SFR su tunnel VPN senza switch LAN

## Sommario



## Introduzione

I provider di servizi offrono servizi WAN gestiti nel loro portafoglio. La piattaforma Cisco ASA Firepower fornisce una serie di funzionalità unificate di gestione delle minacce per fornire servizi differenziati. Un dispositivo ASA Firepower ha interfacce separate per la gestione, da connettere a un dispositivo LAN. Tuttavia, la connessione di un'interfaccia di gestione con un dispositivo LAN crea una dipendenza su un dispositivo LAN.

Questo documento offre una soluzione per gestire un modulo Cisco ASA Firepower (SFR) senza connetterlo a un dispositivo LAN o utilizzare una seconda interfaccia del dispositivo periferico del provider di servizi.

## Prerequisiti

### Componenti usati

- Piattaforma ASA serie 5500-X con servizi Firepower (SFR).
- L'interfaccia di gestione è condivisa tra l'ASA e il modulo Firepower.

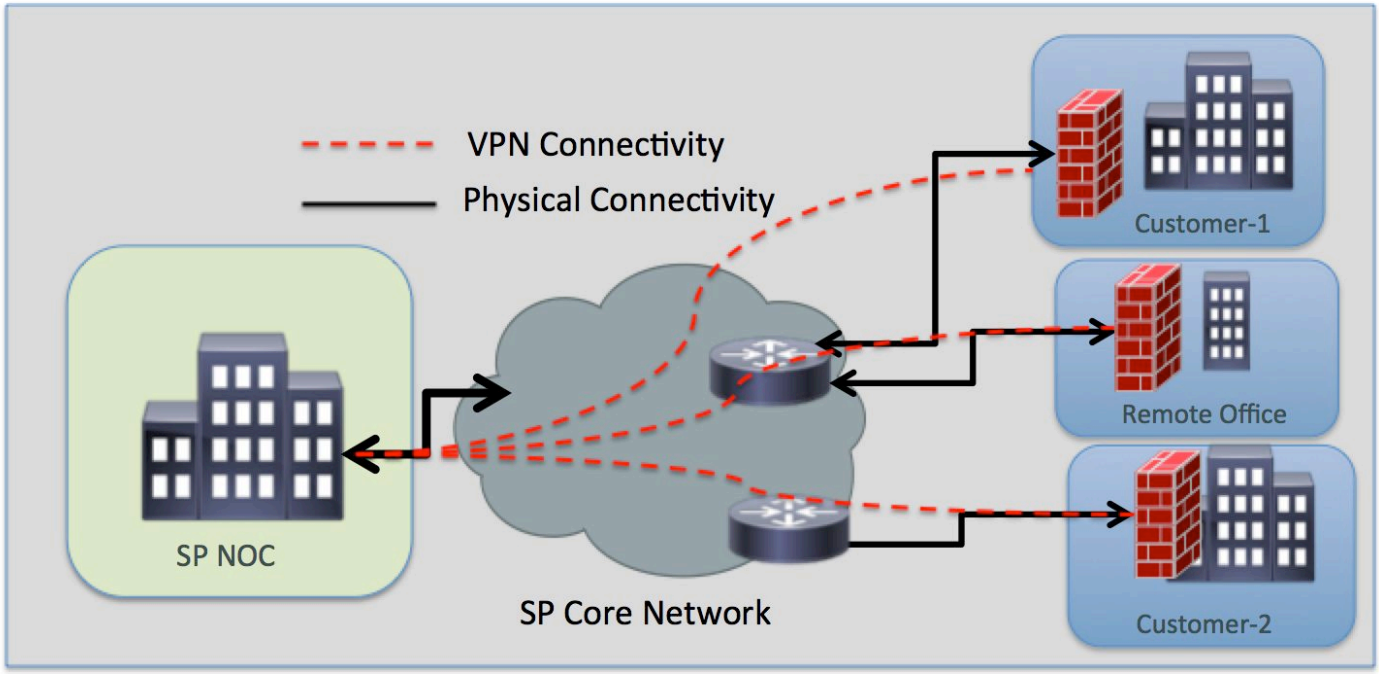
## Architettura

### Requisiti

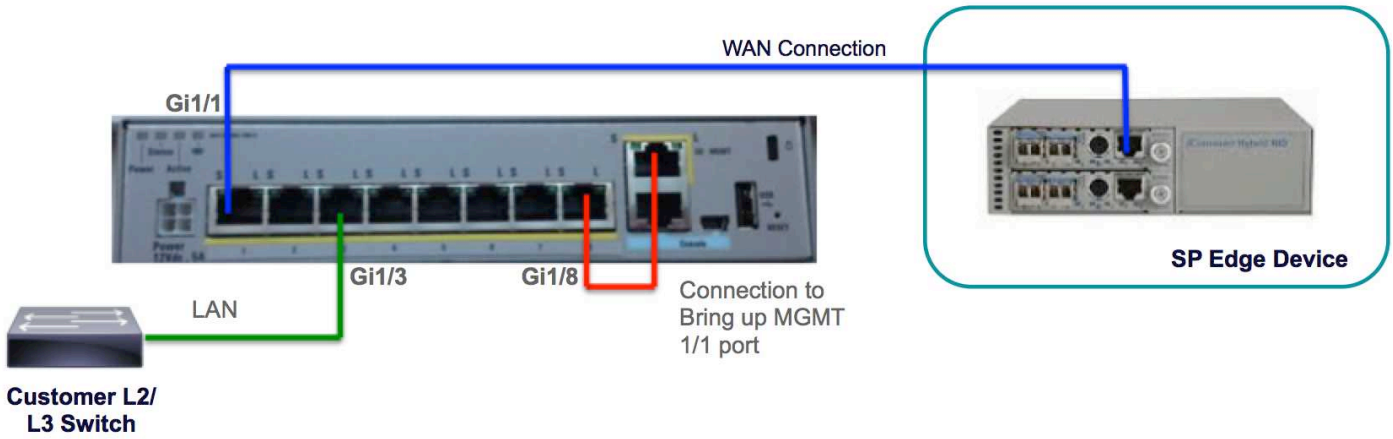
- Handoff di accesso a Internet dedicato singolo dal dispositivo periferico del provider di servizi ad ASA Firepower.

- Per impostare lo stato dell'interfaccia su attivo, è necessario accedere all'interfaccia di gestione.
- L'interfaccia di gestione dell'ASA deve rimanere attiva per gestire il modulo Firepower.
- La connettività di gestione non deve andare persa se il cliente disconnette un dispositivo LAN.
- L'architettura di gestione deve supportare il failover WAN Active/Backup.

### Panoramica della topologia




### Design di basso livello




## Soluzione

Le seguenti configurazioni consentono di gestire il modulo SFR su VPN in remoto, senza alcuna connettività LAN come prerequisito.

### Cablaggio

- Collegare l'interfaccia di gestione 1/1 all'interfaccia Gigabit Ethernet 1/8 tramite un cavo

Ethernet.

**Nota:** Il modulo ASA Firepower deve usare l'interfaccia di gestione 1/x (1/0 o 1/1) per inviare e ricevere il traffico di gestione. Poiché l'interfaccia di gestione 1/x non si trova sul piano dati, è necessario collegare fisicamente l'interfaccia di gestione a un altro dispositivo LAN per consentire il passaggio del traffico attraverso l'ASA sul piano di controllo.

Come parte di una soluzione completa, è possibile collegare l'interfaccia di gestione 1/1 all'interfaccia Gigabit Ethernet 1/8 tramite un cavo Ethernet.

## Indirizzo IP

- **Interfaccia Gigabit Ethernet 1/8**: 192.168.10.1/24
- **Interfaccia di gestione SFR**: 192.168.10.2/24
- **SFR Gateway**: 192.168.10.1
- **Interfaccia di gestione 1/1**: Nessun indirizzo IP configurato per l'interfaccia di gestione. Il comando management-access deve essere configurato per la gestione (MGMT).

Il traffico locale e remoto si troverà nelle seguenti subnet:

- Il traffico locale si trova nella subnet di gestione 192.168.10.0/24.
- Il traffico remoto si trova nella subnet 192.168.11.0/24.

## VPN e NAT

- Definire i criteri VPN.
- Il comando NAT deve essere configurato con il prefisso route-lookup per determinare l'interfaccia di uscita tramite una route lookup anziché utilizzare l'interfaccia specificata nel comando NAT.

## Esempio di configurazione

```
!
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
!
```