Contents

Introduction

Service providers offer managed WAN service in their portfolio. Cisco ASA Firepower platform provides unified threat management feature set to provide differentiated services. An ASA Firepower device has seperate interfaces for management connect to a LAN device, however, connecting a management interface with a LAN device creates a dependency on a LAN device.

This document provides a solution that allows you to manage a Cisco ASA Firepower (SFR) module without connecting to a LAN device or using a second interface from the service provider edge device.

Prerequisites

Components Used

- ASA 5500-X series platform with Firepower (SFR) services.
- Management interface which is shared between the ASA and Firepower module.

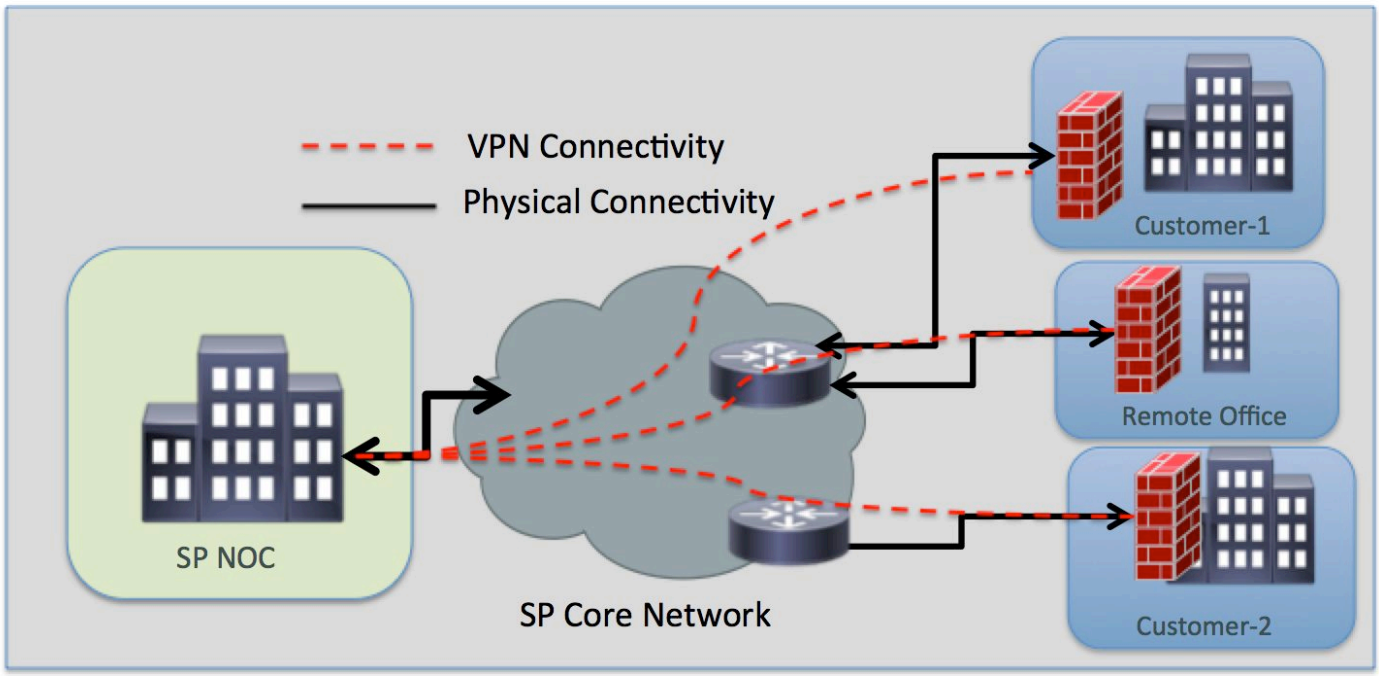
Architecture

Requirements

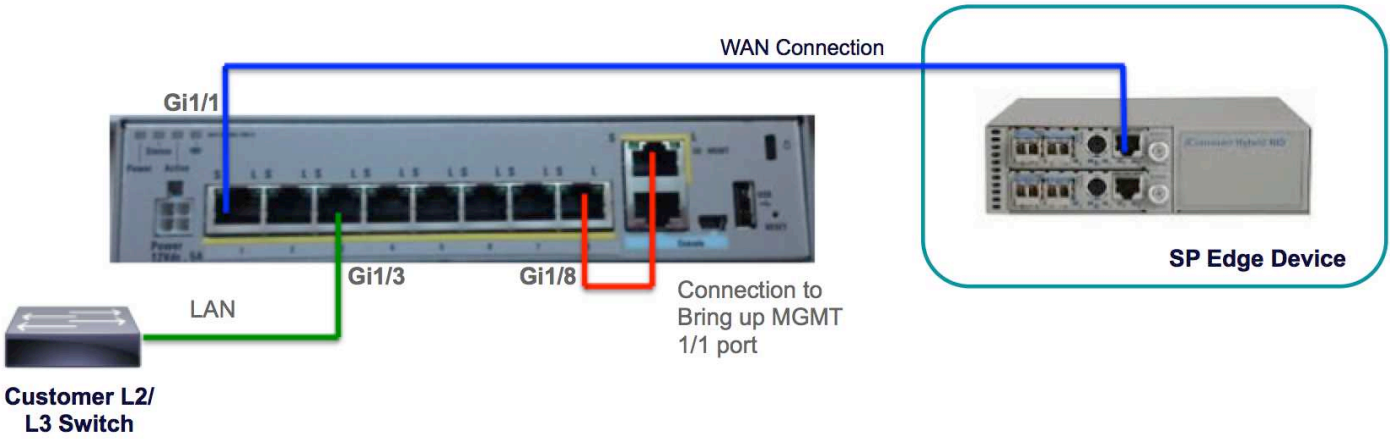
- Single dedicated internet access handoff from Service Provider edge device to ASA Firepower.
- Access to the management interface is necessary in order to change the interface state to up.
- The management interface of the ASA should stay up in order to manage the Firepower module.
- Management connectivity should not be lost if customer disconnects LAN device.

- Management architecture should support Active/Backup WAN failover.

Topology Overview



Low-Level Design



Solution

The following configurations will allow you to manage the SFR module over VPN remotely, without any LAN connectivity as pre-requisite.

Cabling

- Connect the Management interface 1/1 to the GigabitEthernet1/8 interface using an ethernet cable.

  Note: The ASA Firepower module must use the Management 1/x (1/0 or 1/1) interface to send and receive management traffic. Since the Management 1/x interface is not on the data plane, you need to physically cable the management interface to another LAN device in

order to pass traffic through the ASA over the control plane.

As a part of the one-box solution, you will connect the Management interface 1/1 to the GigabitEthernet1/8 interface using an ethernet cable.

IP Address

- **GigabitEthernet 1/8 Interface**: `192.168.10.1/24`
- **SFR Management Interface**: `192.168.10.2/24`
- **SFR Gateway**: `192.168.10.1`
- **Management 1/1 Interface**: Management interface does not have any IP address configured. The `management-access` command should be configured for management (MGMT) purpose.

The local and remote traffic will be on the following subnets:

- Local traffic is on the management subnet 192.168.10.0/24.
- Remote traffic is on 192.168.11.0/24 subnet.

VPN and NAT

- Define the VPN policies.
- NAT command should be configured with `route-lookup` prefix to determine the egress interface using a route lookup instead of using the interface specified in the NAT command.

Configuration Example

```
!
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
!
```