Configure Failover for IPSec Site-to-Site Tunnels with Backup ISP Links on FTD Managed by FMC

Contents

Introduction

This document describes how to configure crypto map based failover for ISP link with the IP SLA track feature on the FTD managed by FMC.

Contributed by Amanda Nava, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of a Virtual Private Network (VPN)
- Experience with FTD
- Experience with FMC

- Experience with Adaptive Security Appliance (ASA) command line

Components Used

The information in this document is based on these software versions:

- FMC version 6.6.0
- FTD version 6.6.0
- ASA Version 9.14.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

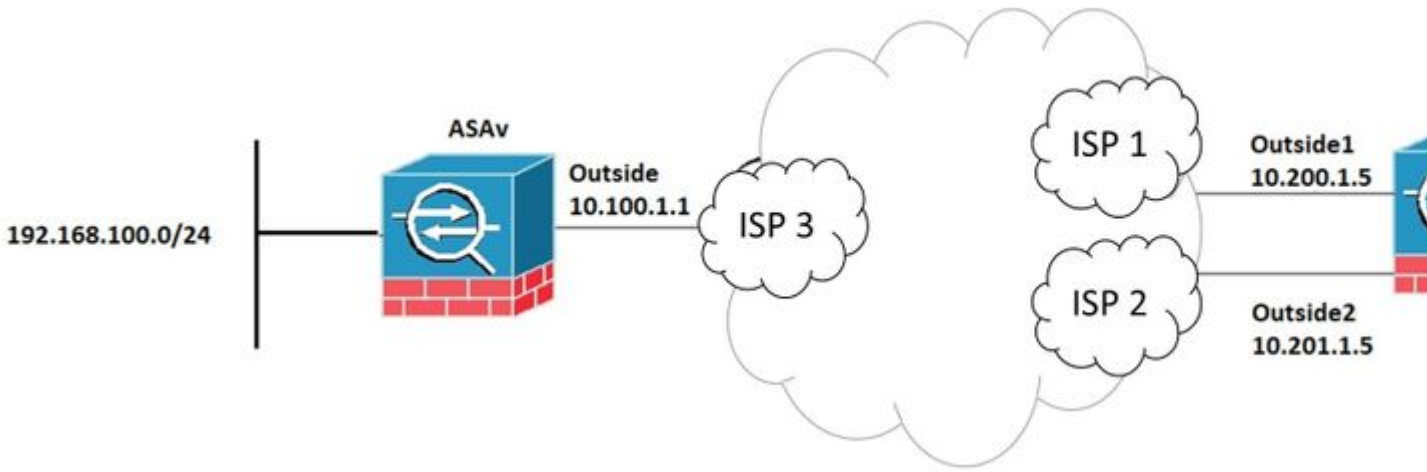
This document describes how to configure crypto map based failover for backup Internet Service Provider (ISP) link with the Internet Protocol Service Level Agreement (IP SLA) track feature on the Firepower Threat Defense (FTD) managed by Firepower Management Center (FMC). It also explains how to configure Network Address Translation (NAT) exemption for the VPN traffic when there are two ISPs and it requires a seamless failover.

In this scenario, the VPN is established from the FTD towards the ASA as the VPN peer with only one ISP interface. The FTD uses one ISP link at that time to establish the VPN. When the Primary ISP link goes down, the FTD takes over with the secondary ISP link through the SLA Monitor and the VPN is established.

Configure

Network Diagram

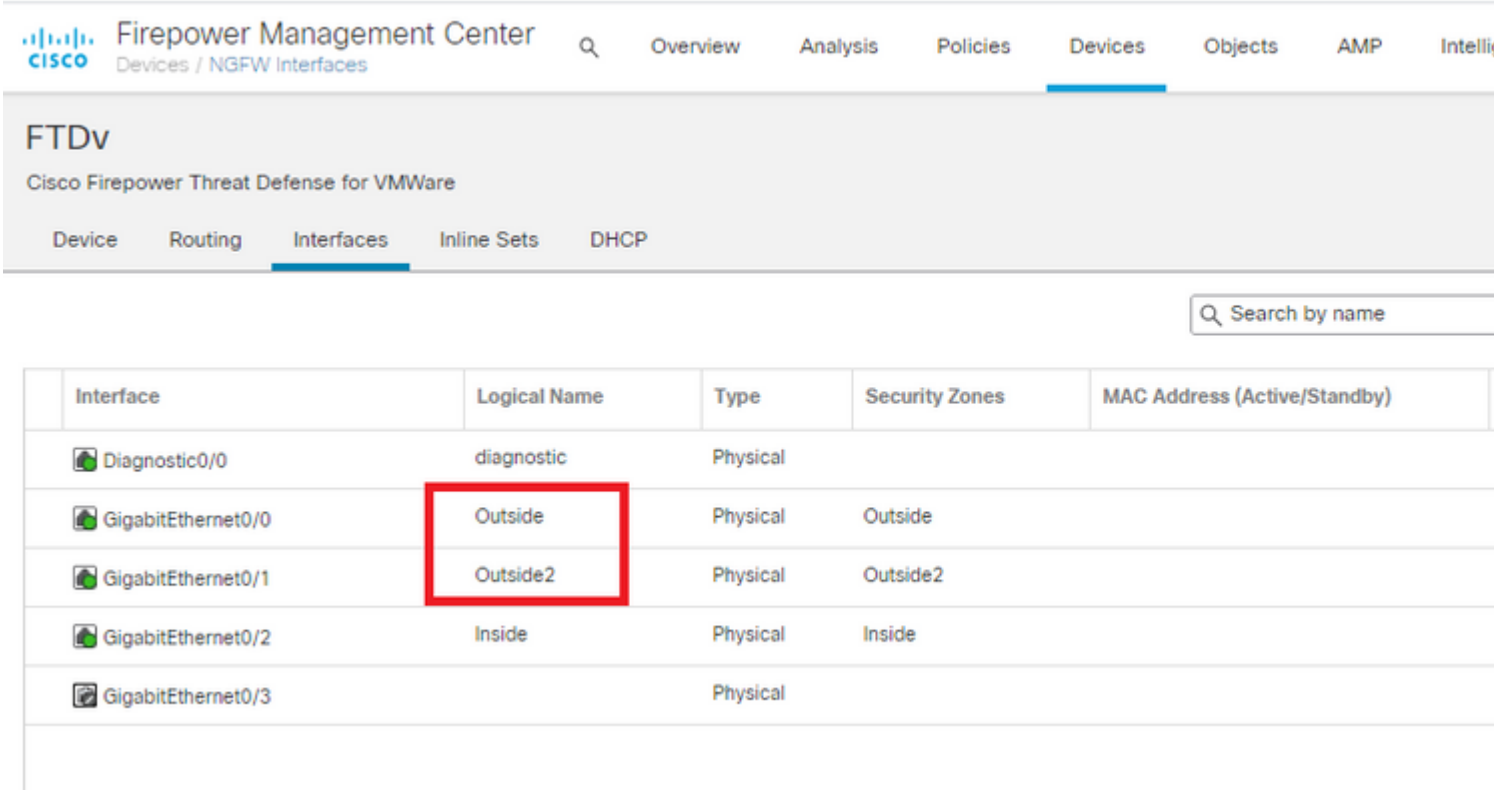
This is the topology used for the example throughout this document:



Configure the FTD

Step 1. Define the Primary and Secondary ISP Interfaces

1. Navigate to **Devices > Device Management > Interfaces** as shown in the image.

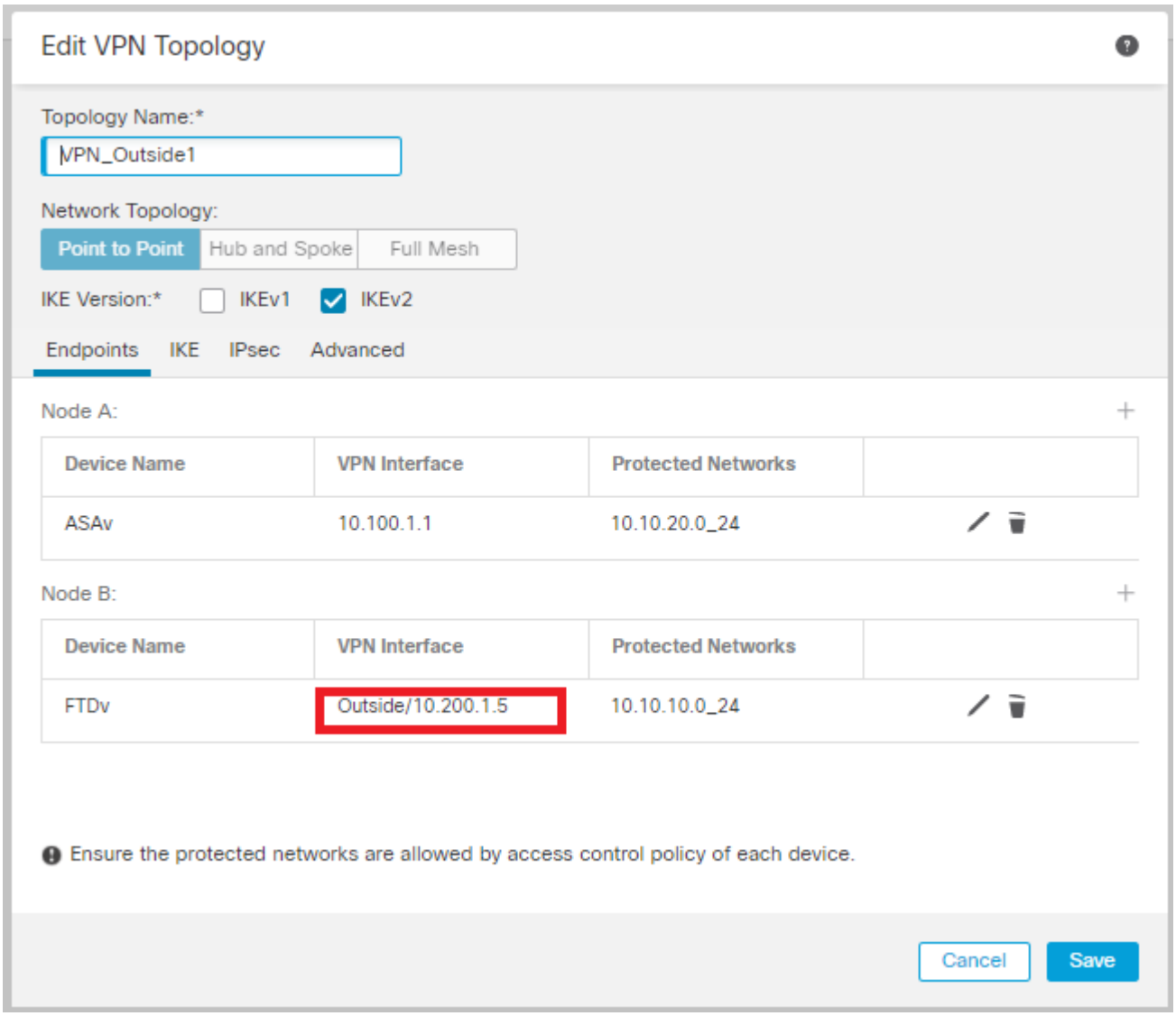


Step 2. Define the VPN Topology for the Primary ISP Interface

1. Navigate to **Devices > VPN > Site To Site.** Under **Add VPN,** click **Firepower Threat Defense Device**, and create the VPN and select the Outside interface.

> **Note:** This document does not describe how to configure an S2S VPN from scratch. For more reference of S2S VPN configuration on FTD go to https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html

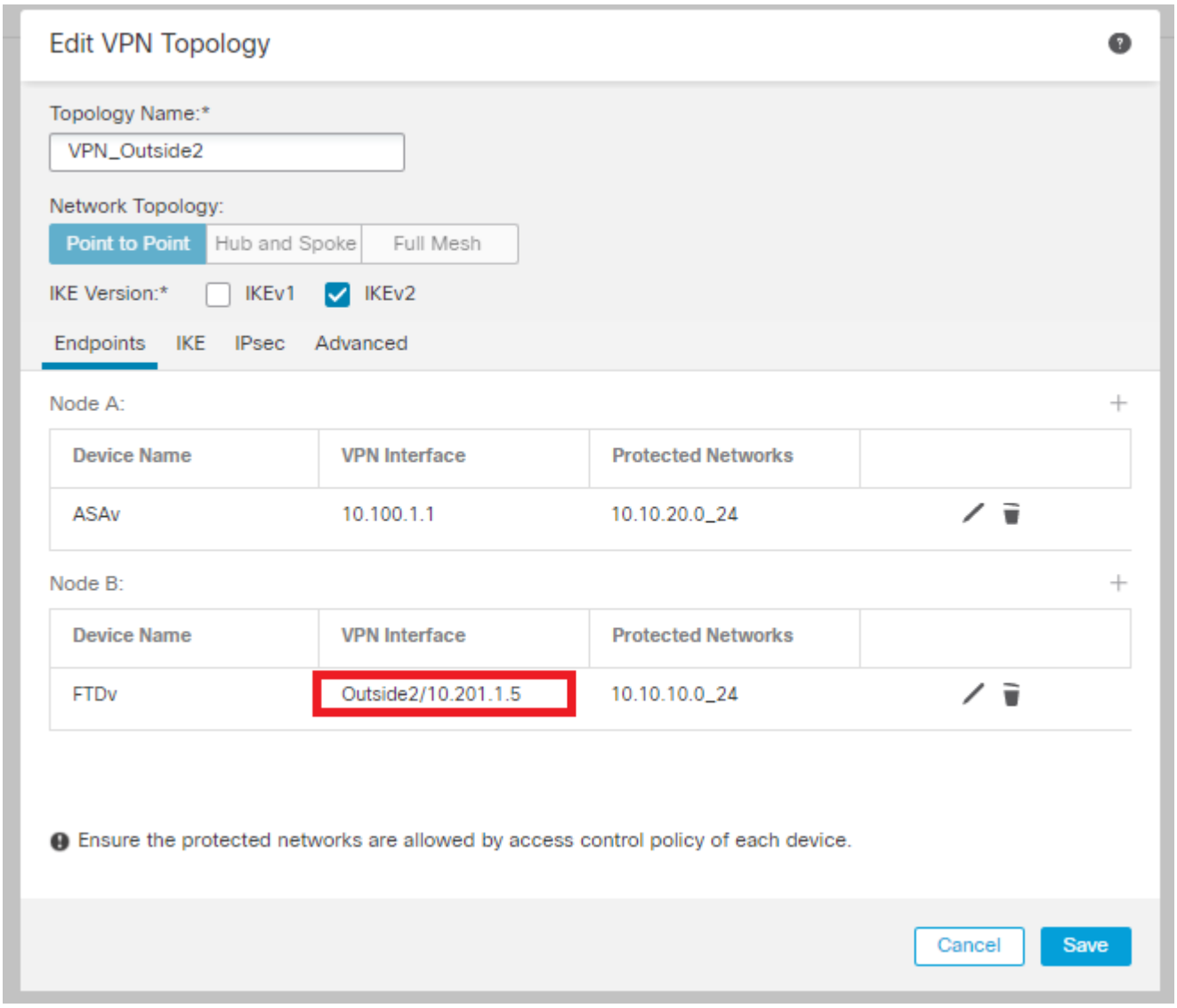
---



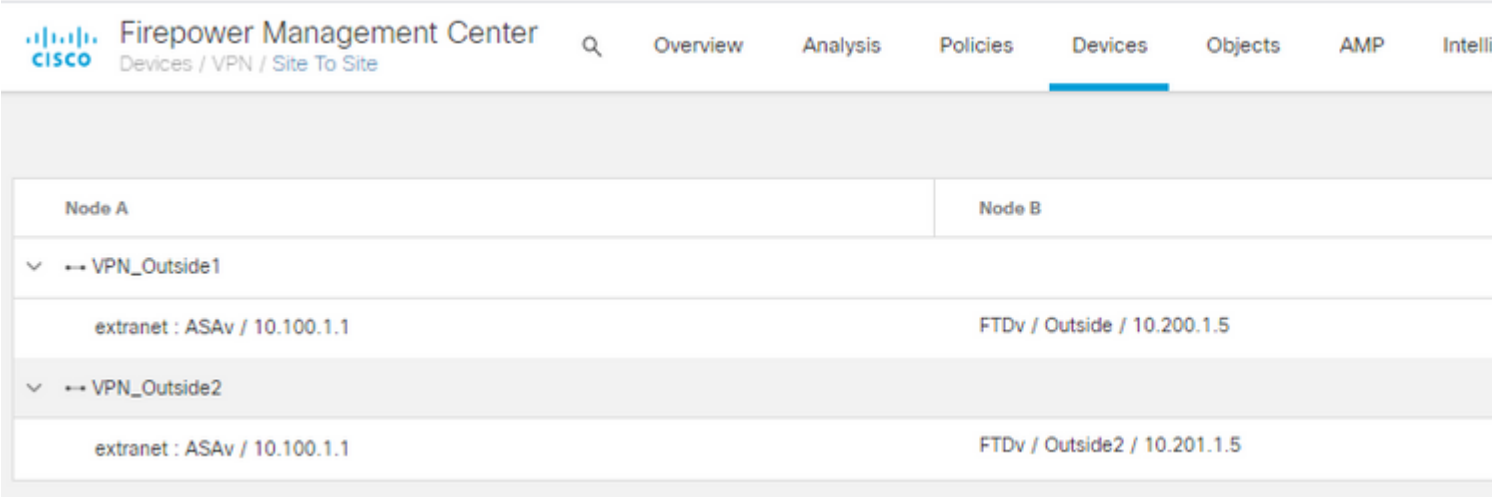
Step 3. Define the VPN Topology for the Secondary ISP Interface

1. Navigate to **Devices > VPN > Site To Site.** Under **Add VPN,** click **Firepower Threat Defense Device**, and create the VPN and select the Outside2 interface.

Note: The VPN configuration that uses the Outside2 interface must be exactly the same as the Outside VPN topology except for the VPN interface.

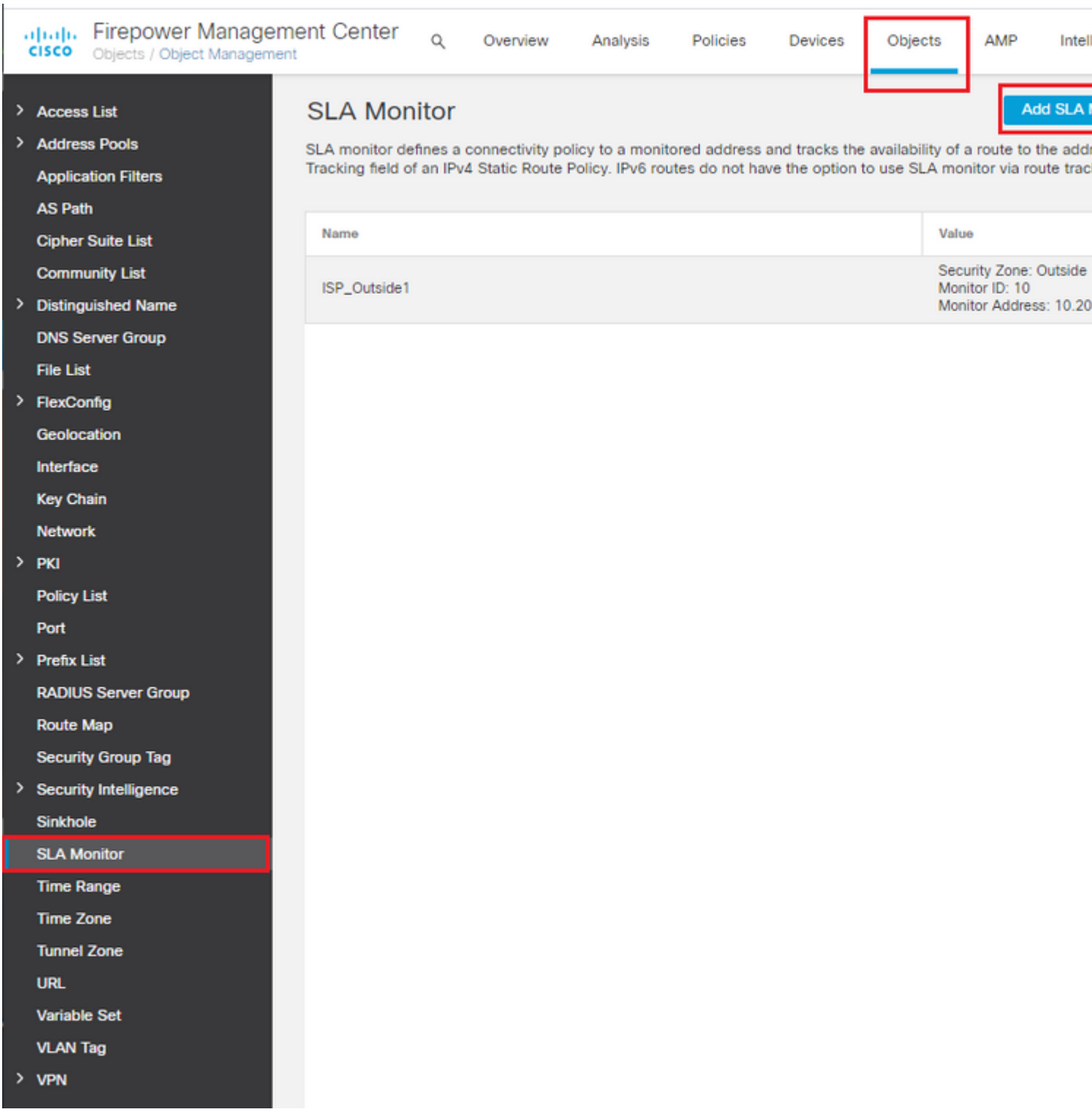


VPN topologies must be configured as shown in the image.

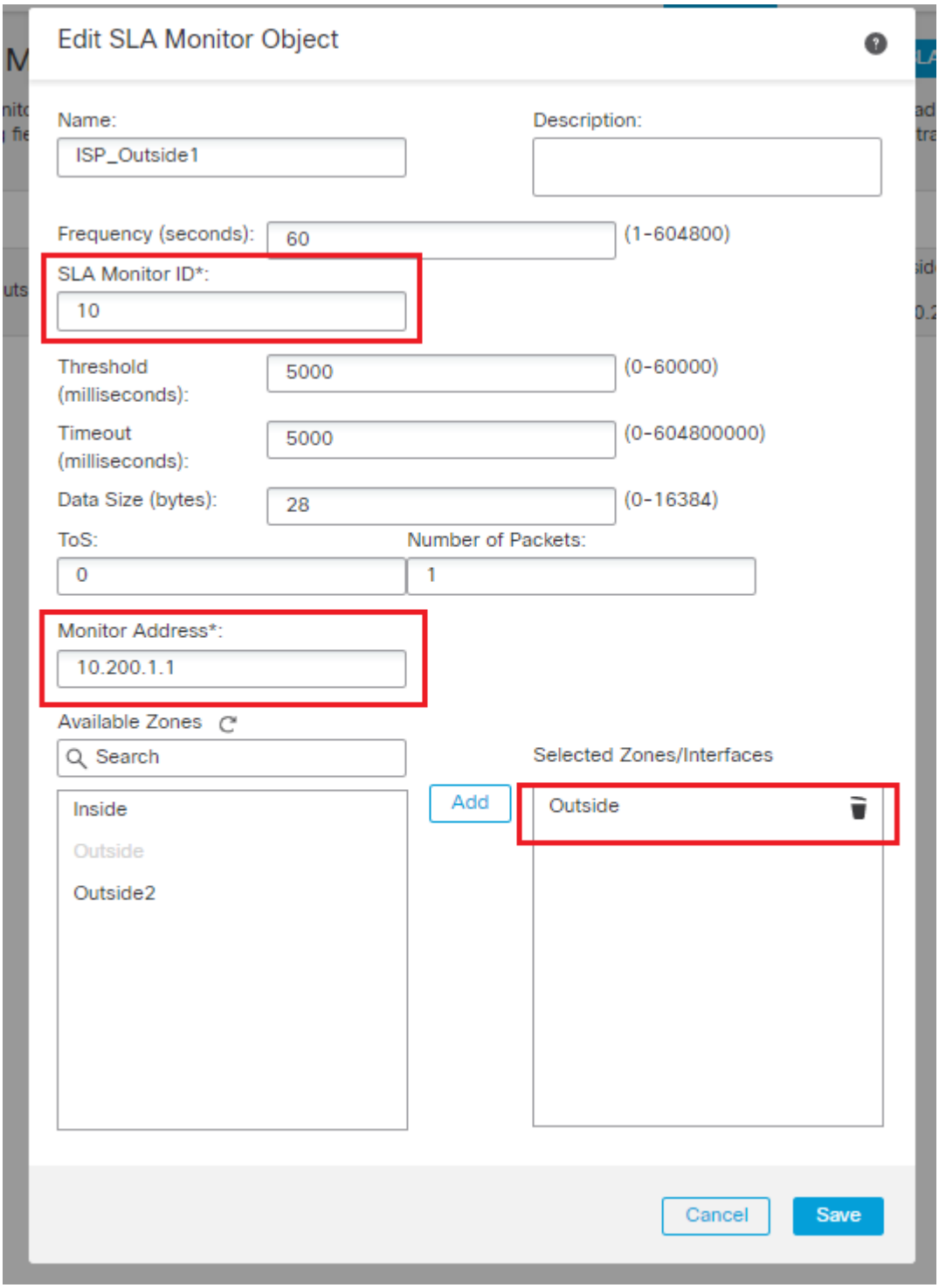


Step 4. Configure the SLA Monitor

1. Navigate to **Objects > SLA Monitor > Add SLA Monitor.** Under **Add VPN,** click **Firepower Threat Defense Device**, and configure the SLA Monitor as shown in the image.

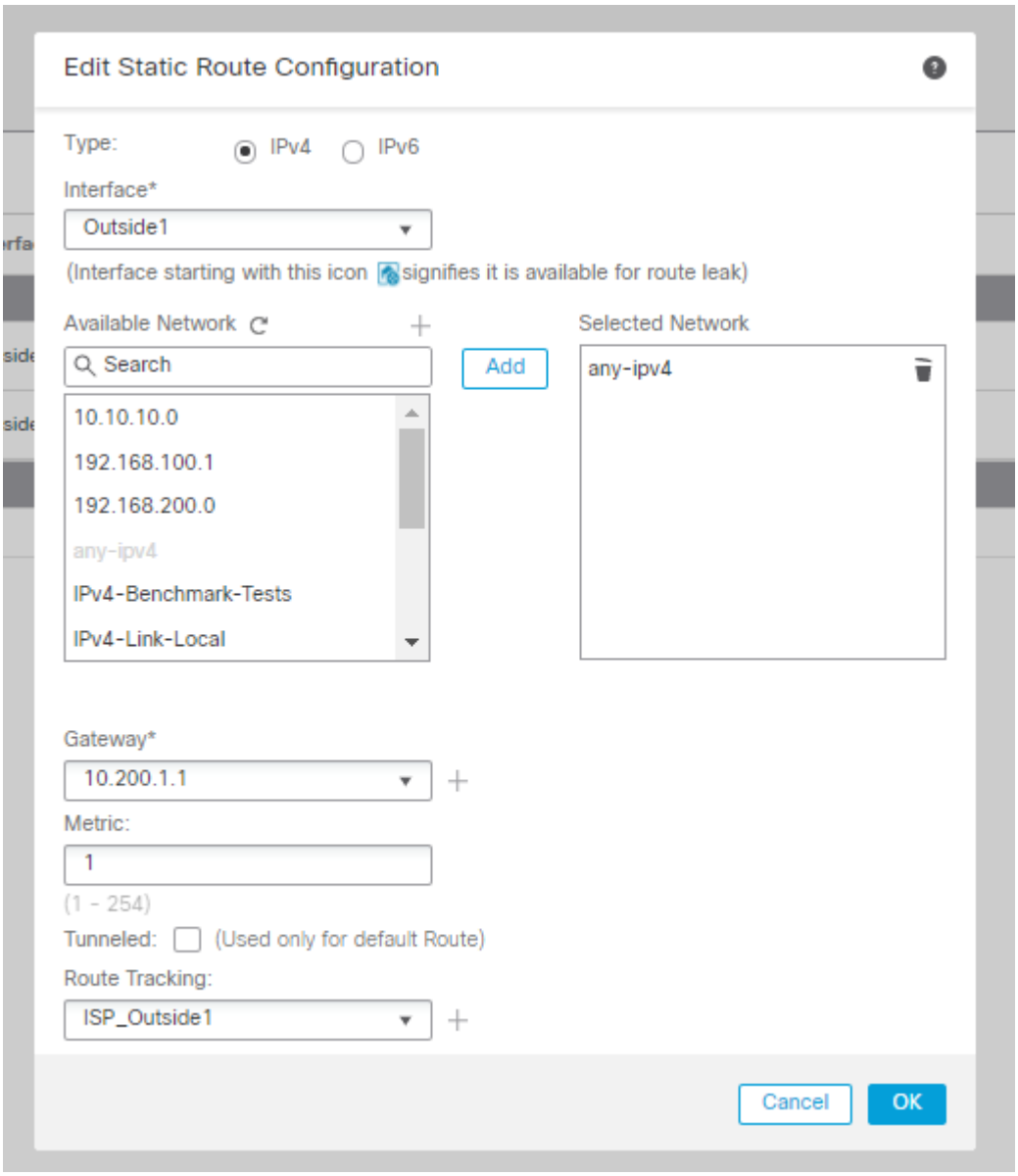


2. For the **SLA Monitor ID*** field use the Outside next-hop IP address.

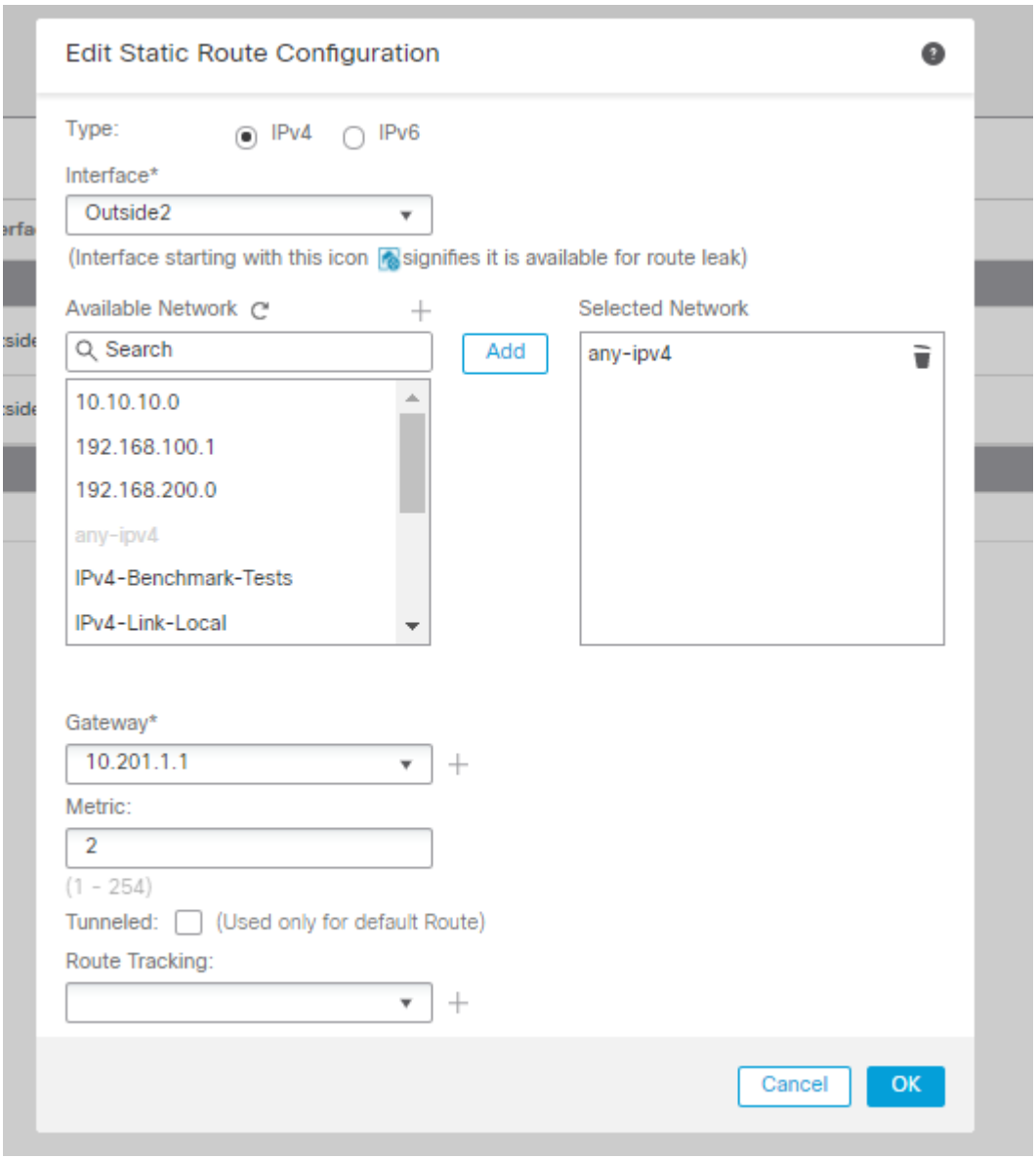


Step 5. Configure the Static routes with the SLA Monitor

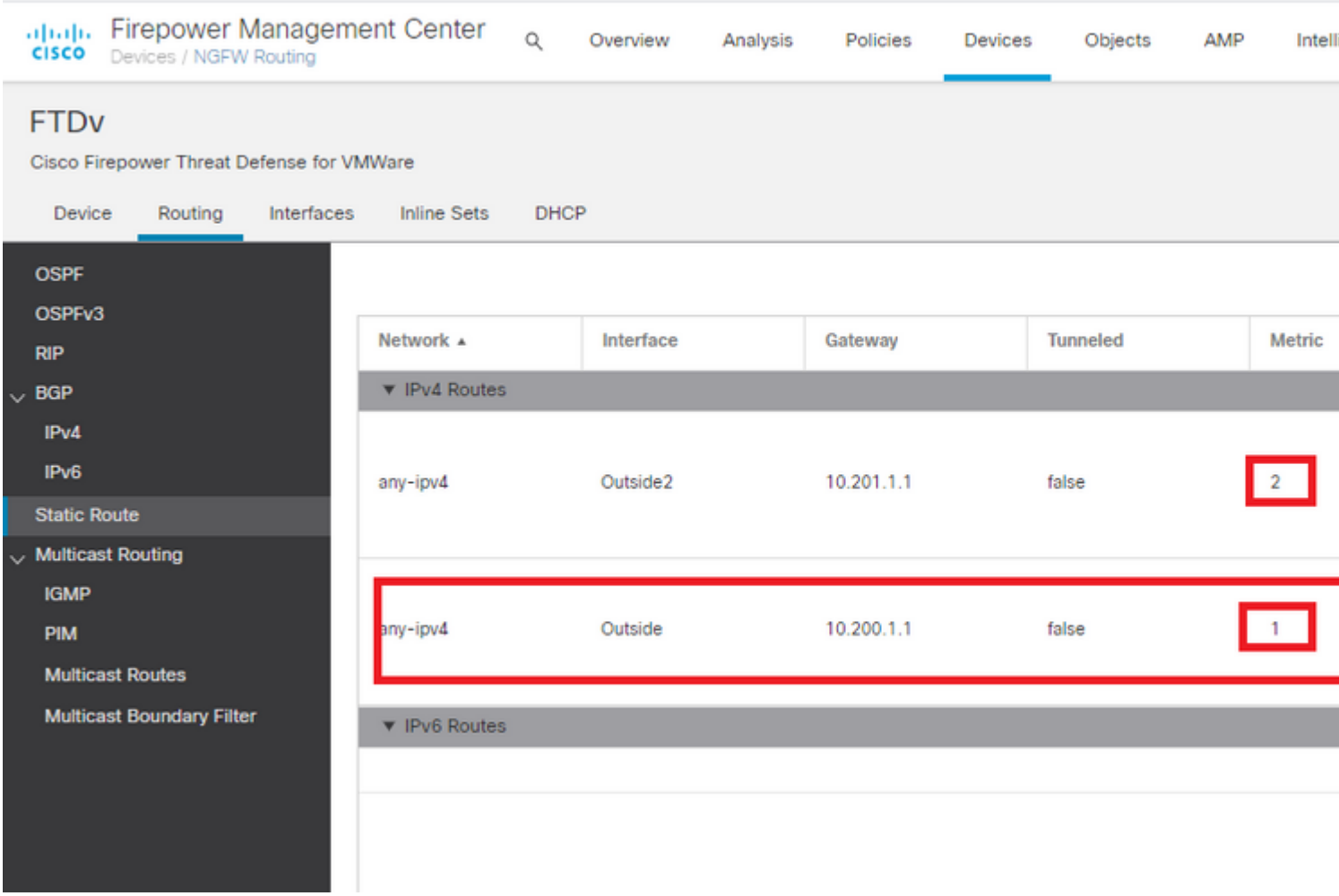
1. Navigate to **Devices > Routing > Static Route.** Select **Add Route,** and configure the default route for the Outside (primary) interface with the SLA Monitor information (Created on step 4) on the **Route tracking** field.



2. Configure the default route for the Outside2 (secondary) interface. The Metric value must be higher than the primary default route. No **Route tracking** field is needed in this section.

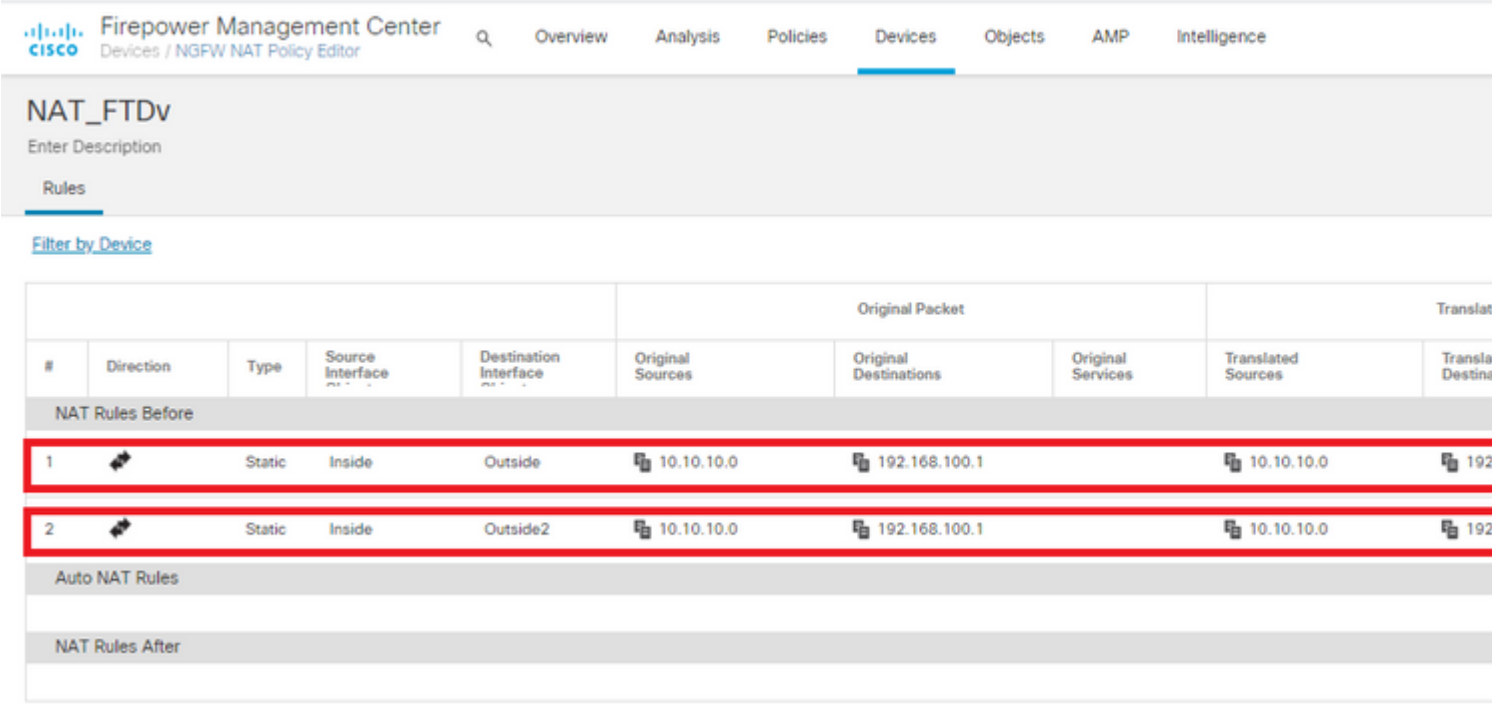


Routes must be configured as shown in the image.



Step 6. Configure the NAT Exemption

1. Navigate to **Devices > NAT > NAT Policy** and select the Policy that targets the FTD device**.** Select **Add Rule** and configure a NAT exemption per ISP interface (Outside and Outside2). NAT rules must be the same except for the Destination interface.



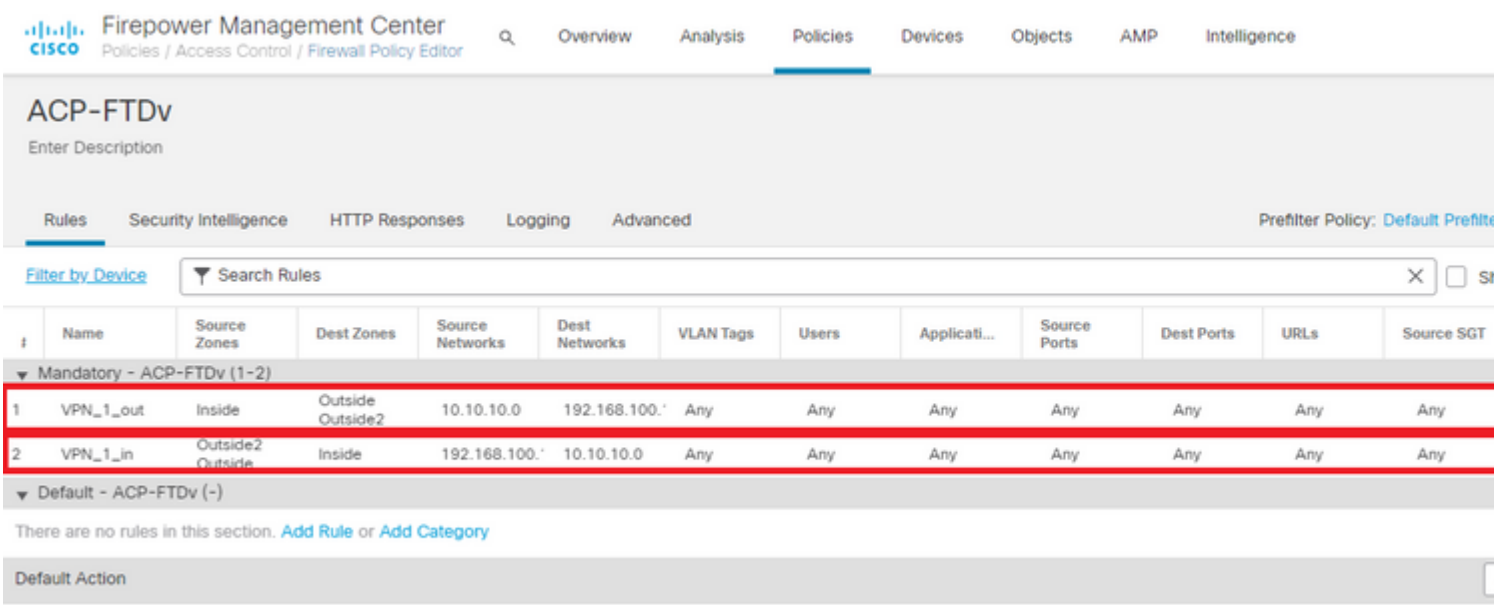
Note: For this scenario, both NAT rules require **Route-lookup** to be enabled. Otherwise, the traffic would hit the first rule and would not keep to the failover routes. If route lookup is not enabled, traffic would always be sent with the use of the (first NAT rule) Outside interface. With **Route-lookup** enabled, traffic always keeps to the Routing table that is controlled through the SLA Monitor.

Step 7. Configure the Access Control Policy for Interesting Traffic

1. Navigate to **Policies > Access Control > Select the Access Control Policy.** In order to add a Rule, click **Add Rule**, as shown in the image here.

Configure one rule from Inside to Outside zones (Outside1 and Outside2) which allows the interested traffic from 10.10.10.0/24 to 192.168.100/24.

Configure another rule from Outside zones (Outside1 and Outside 2) to Inside which allows the interesting traffic from 192.168.100/24 to 10.10.10.0/24.



Configure the ASA

> **Note:** For this specific scenario, a backup peer is configured on the IKEv2 crypto map, this feature requires the ASA to be on 9.14.1 or later versions. If your ASA is running an older version use IKEv1 as a workaround. For more reference go to Cisco bug ID CSCud22276.

---

1. Enable IKEv2 on the outside interface of the ASA:

```
Crypto ikev2 enable Outside
```

2. Create the IKEv2 Policy that defines the same parameters configured on the FTD:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

3. Create a group-policy to allow the ikev2 protocol:

```
group-policy IKEV2 internal
group-policy IKEV2 attributes
 vpn-tunnel-protocol ikev2
```

4. Create a tunnel group for each Outside FTD IP address (Outside1 and Outside2). Reference the group-policy and specify the pre-shared-key:

```
tunnel-group 10.200.1.5 type ipsec-l2l
tunnel-group 10.200.1.5 general-attributes
 default-group-policy IKEV2
tunnel-group 10.200.1.5 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123

tunnel-group 10.201.1.5 type ipsec-l2l
tunnel-group 10.201.1.5 general-attributes
 default-group-policy IKEV2
tunnel-group 10.201.1.5 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123
```

5. Create an access-list that defines the traffic to be encrypted: (FTD-Subnet 10.10.10.0/24) (ASA-Subnet 192.168.100.0/24):

```
Object network FTD-Subnet
 Subnet 10.10.10.0 255.255.255.0
Object network ASA-Subnet
 Subnet 192.168.100.0 255.255.255.0
access-list VPN_1 extended permit ip 192.168.100.0 255.255.255.0 10.10.10.0 255.255.255.0
```

6. Create an ikev2 ipsec-proposal to reference the algorithms specified on the FTD:

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

7. Create a crypto map entry that ties together the configuration and add the Outside1 and Outside2 FTD IP addresses:

```
crypto map CSM_Outside_map 1 match address VPN_1
crypto map CSM_Outside_map 1 set peer 10.200.1.5 10.201.1.5
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map 1 set reverse-route
crypto map CSM_Outside_map interface Outside
```

8. Create a NAT exemption statement that prevents the VPN traffic from being NATTED by the firewall:

```
Nat (inside,Outside) 1 source static ASA-Subnet ASA-Subnet destination static FTD-Subnet FTD-Subnet
```

Verify

Use this section to confirm that your configuration works properly.

FTD

In the command line, use the **show crypto ikev2 sa** command to verify the VPN status.

Note: VPN is established with Outside1's IP address (10.200.1.5) as local.

```
firepower# sh crypto  ikev2 sa

IKEv2 SAs:

Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                Remote
373101057 10.200.1.5/500                                       10.100.1.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/37 sec
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
          remote selector 192.168.100.0/0 - 192.168.100.255/65535
          ESP spi in/out: 0x829ed58d/0x2051ccc9
```

Route

The default route shows the Outside1's next-hop IP address.

```
firepower# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.200.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.200.1.1, Outside1
C        10.10.10.0 255.255.255.0 is directly connected, Inside
L        10.10.10.5 255.255.255.255 is directly connected, Inside
```

```
C        10.200.1.0 255.255.255.0 is directly connected, Outside1
L        10.200.1.5 255.255.255.255 is directly connected, Outside1
C        10.201.1.0 255.255.255.0 is directly connected, Outside2
L        10.201.1.5 255.255.255.255 is directly connected, Outside2
```

Track

As seen in the show track 1 output, "Reachability is Up".

```
firepower#   sh track 1
Track 1
  Response Time Reporter 10 reachability
  Reachability is Up                        <-----
  36 changes, last change 00:00:04
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

NAT

It is needed to confirm the interesting traffic hits the NAT exemption rule with the Outside1 interface.

Use the "packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail" command to verify the NAT rule applied for the interesting traffic.

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det

---------------OMITTED OUTPUT -----------------
Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
NAT divert to egress interface Outside1(vrfid:0)
Untranslate 192.168.100.1/0 to 192.168.100.1/0

---------------OMITTED OUTPUT -----------------

Phase: 7
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
Static translate 10.10.10.1/0 to 10.10.10.1/0
 Forward Flow based lookup yields rule:
 in  id=0x2b3e09576290, priority=6, domain=nat, deny=false
        hits=19, user_data=0x2b3e0c341370, cs_id=0x0, flags=0x0, protocol=0
```

```
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3596, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c8d0250, priority=70, domain=encrypt, deny=false
        hits=5, user_data=0x16794, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any(vrfid:65535), output_ifc=Outside1

Phase: 13
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e095d49a0, priority=6, domain=nat-reverse, deny=false
        hits=1, user_data=0x2b3e0c3544f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0c8ad890, priority=70, domain=ipsec-tunnel-flow, deny=false
        hits=5, user_data=0x192ec, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
        src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Outside1(vrfid:0), output_ifc=any

Phase: 15
Type: NAT
Subtype: per-session
Result: ALLOW
```

```
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3598, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------

Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

Perform Failover

For this example, the failover is performed by a shutdown on the Outside1's Next hop used on the IP SLA monitor configuration.

```
firepower# sh sla monitor configuration 10
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 10
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.200.1.1
Interface: Outside1
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

Route

The default route now uses the Outside2's next-hop IP address and Reachability is Down.

```
firepower# sh route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.201.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 10.201.1.1, Outside2
C        10.10.10.0 255.255.255.0 is directly connected, Inside
L        10.10.10.5 255.255.255.255 is directly connected, Inside
C        10.200.1.0 255.255.255.0 is directly connected, Outside1
L        10.200.1.5 255.255.255.255 is directly connected, Outside1
C        10.201.1.0 255.255.255.0 is directly connected, Outside2
L        10.201.1.5 255.255.255.255 is directly connected, Outside2
```

Track

As seen in the **show track 1** output, "Reachability is Down" at this point.

```
firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Down <----
37 changes, last change 00:17:02
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

NAT

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det
---------------OMITTED OUTPUT -----------------

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
Static translate 10.10.10.1/0 to 10.10.10.1/0
 Forward Flow based lookup yields rule:
 in  id=0x2b3e0c67d470, priority=6, domain=nat, deny=false
        hits=44, user_data=0x2b3e0c3170e0, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

---------------OMITTED OUTPUT -----------------
```

```
Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c67bdb0, priority=70, domain=encrypt, deny=false
        hits=1, user_data=0x1d4cfb24, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any(vrfid:65535), output_ifc=Outside2

Phase: 10
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c6d5bb0, priority=6, domain=nat-reverse, deny=false
        hits=1, user_data=0x2b3e0b81bc00, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

Phase: 11
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0c8a14f0, priority=70, domain=ipsec-tunnel-flow, deny=false
        hits=1, user_data=0x1d4d073c, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
        src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Outside2(vrfid:0), output_ifc=any

Phase: 12
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3669, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------

Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside2(vrfid:0)
output-status: up
output-line-status: up
```

Action: allow