Configure Dual ISP Failover for FTD Managed by FMC

Contents

Introduction

This document describes how to configure DUAL ISP Failover with PBR and IP SLAs on an FTD that is managed by FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Policy Based Routing (PBR)
- Internet protocol service level agreement (IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Components Used

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

- FMCv 7.3.0
- FTDv 7.3.0

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

Static Route Tracking Feature Overview

Static Route Tracking feature allows the FTD to use a connection to a secondary ISP in the event that the primary leased line becomes unavailable. In order to achieve this redundancy, the FTD associates a static route with a monitoring target that you define. The SSLA operation monitors the target with periodic ICMP echo requests.

If an echo reply is not received, then the object is considered down, and the associated route is removed from the routing table. A previously configured backup route is used in place of the route that is removed. While the backup route is in use, the SLA monitor operation continues its attempts to reach the monitoring target.

Once the target is available again, the first route is replaced in the routing table, and the backup route is removed.

You can now configure multiple next-hops and policy-based routing forwarding actions at the same time. When traffic matches the criteria for the route, the system attempts to forward traffic to the IP addresses in the order you specify, until it succeeds.

The feature is available on FTD devices running version 7.1 and later managed by an FMC version 7.3 and later.

Configure

Network Diagram

This image provides an example of a network diagram.

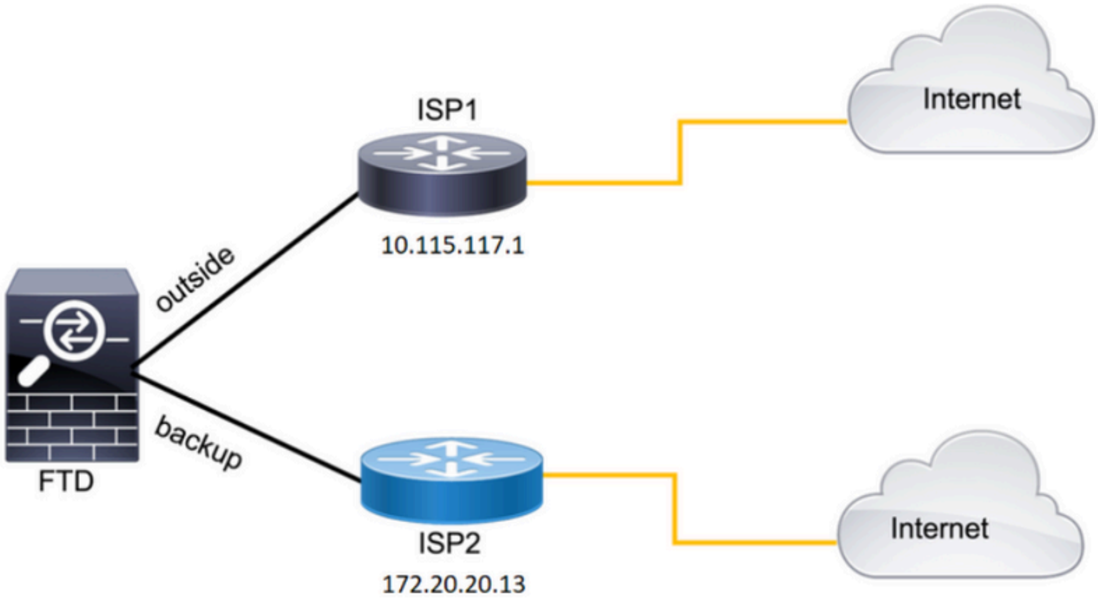


Image 1. Diagram example.

ISP1 = 10.115.117.1

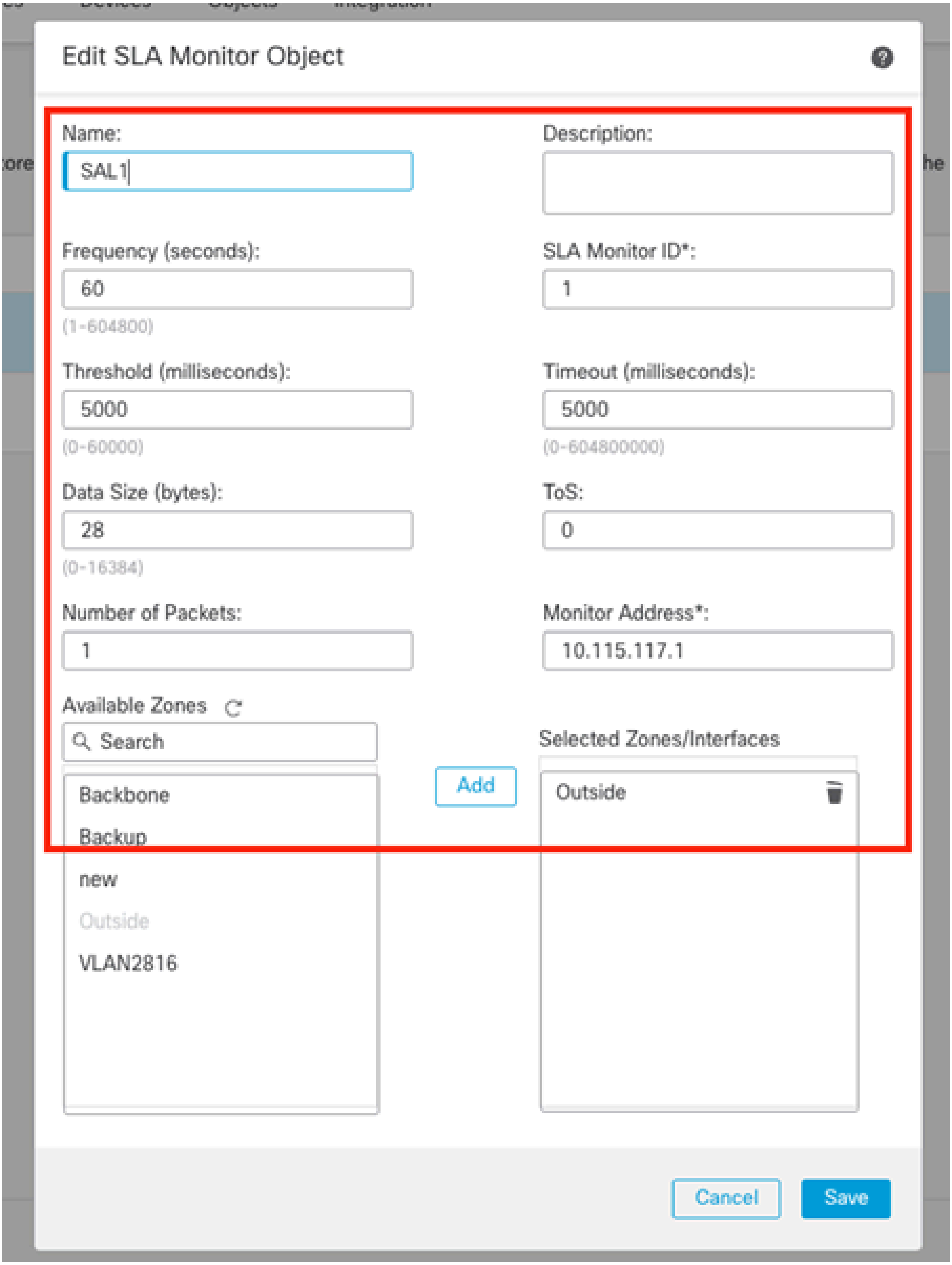
ISP2 = 172.20.20.13

Configurations

Step 1. Configure the SLA Monitor objects.

On the FMC, navigate to Object > Object Management > SLA Monitor > Add SLA Monitor and add an SLA Monitor object for the ISP IP addresses.

SLA monitor for the primary default gateway (ISP1).



Edit SLA Monitor Object

Name: SAL1

Description:

Frequency (seconds): 60

(1-604800)

SLA Monitor ID*: 1

Threshold (milliseconds): 5000

(0-60000)

Timeout (milliseconds): 5000

(0-604800000)

Data Size (bytes): 28

(0-16384)

ToS: 0

Number of Packets: 1

Monitor Address*: 10.115.117.1

Available Zones

Search

Backbone

Backup

new

Outside

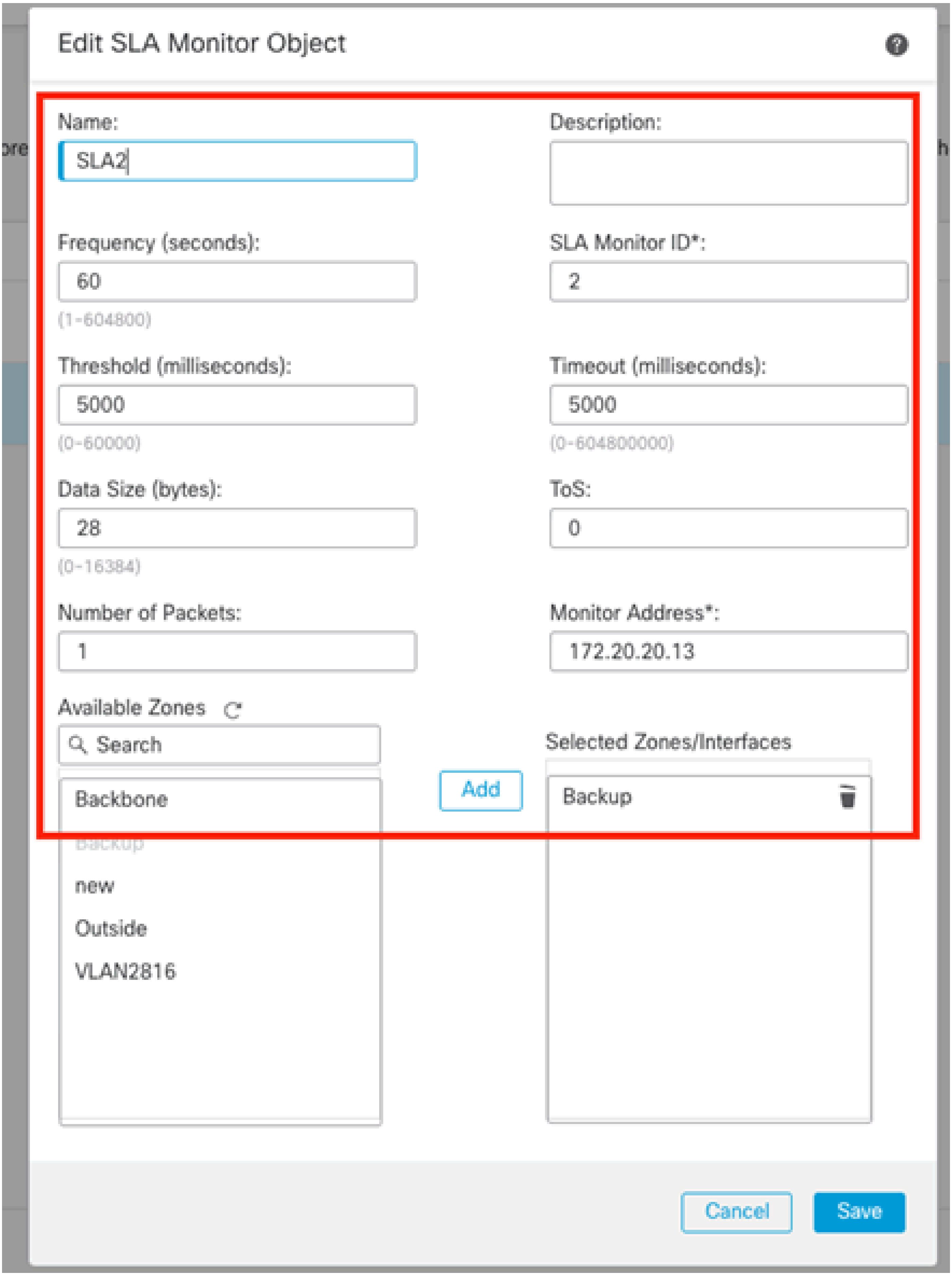
VLAN2816

Selected Zones/Interfaces

Outside

Image 2. SLA1 monitor configuration window.

SLA monitor for the secondary default gateway (ISP2).



Edit SLA Monitor Object

Name: SLA2

Description:

Frequency (seconds): 60 (1-604800)

SLA Monitor ID*: 2

Threshold (milliseconds): 5000 (0-60000)

Timeout (milliseconds): 5000 (0-604800000)

Data Size (bytes): 28 (0-16384)

ToS: 0

Number of Packets: 1

Monitor Address*: 172.20.20.13

Available Zones

Backbone

Backup

new

Outside

VLAN2816

Selected Zones/Interfaces

Backup

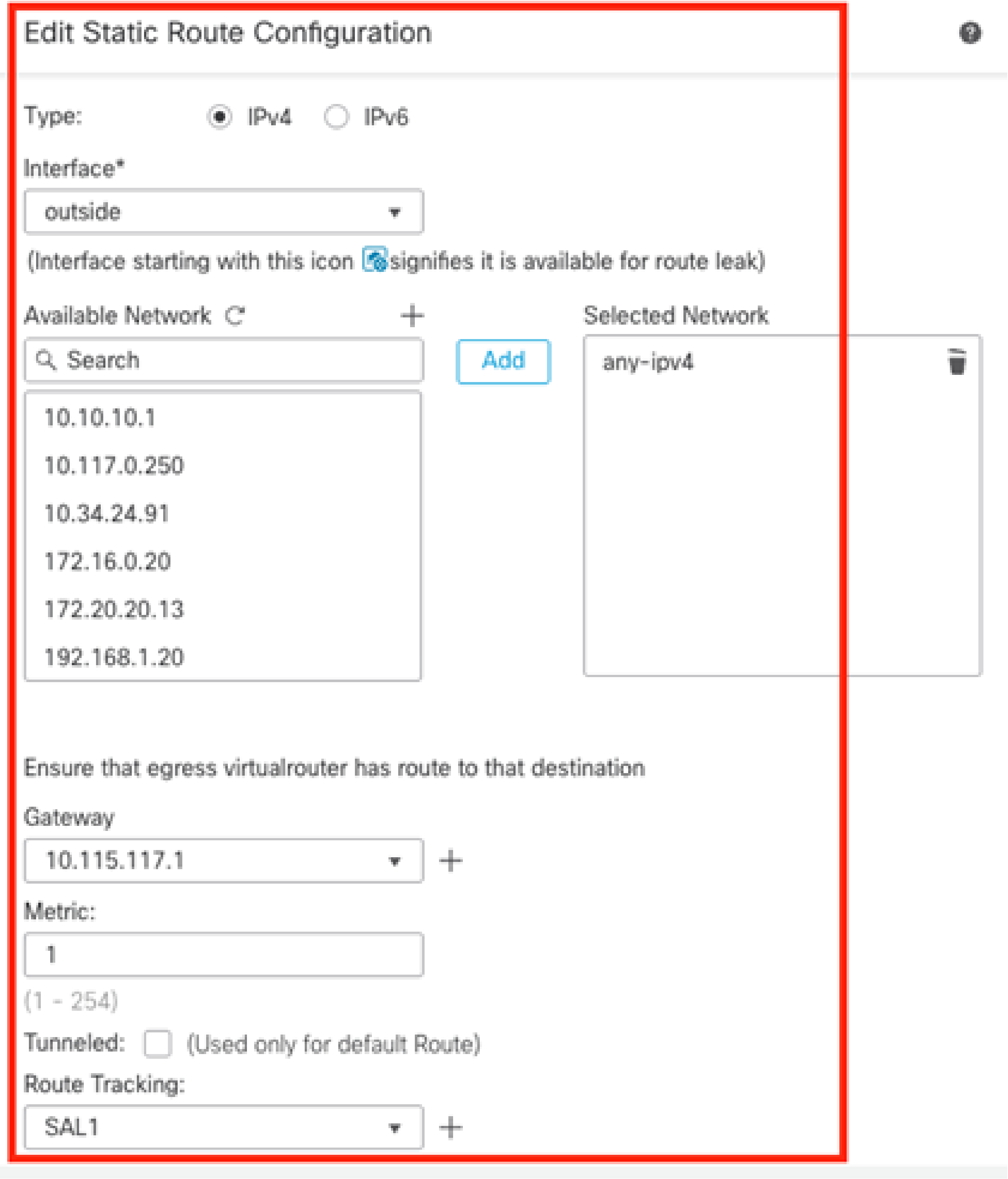
Image 3. SLA2 monitor configuration window.

Step 2. Configure the Static Routes with Route Track.

On the FMC, navigate to Device > Device Management > Edit the desired FTD > Routing > Static Routes, and add the statics routes with the correct SLA monitor.

The SLA monitor must be the one which monitors the default gateway.

Static route for the primary default gateway:



Edit Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside

(Interface starting with this icon signifies it is available for route leak)

Available Network: 10.10.10.1, 10.117.0.250, 10.34.24.91, 172.16.0.20, 172.20.20.13, 192.168.1.20

Selected Network: any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway: 10.115.117.1

Metric: 1

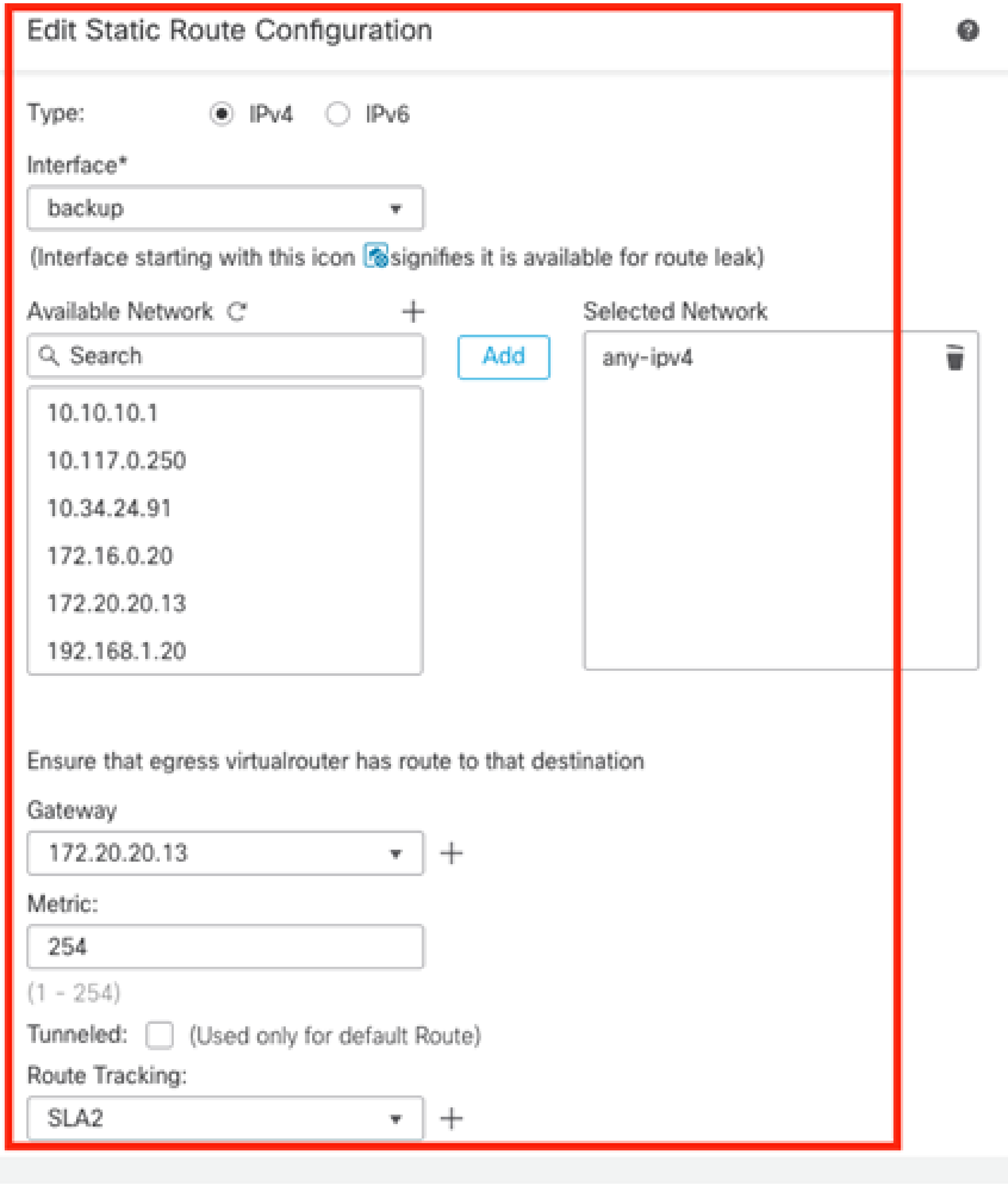
(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking: SAL1

Image 4. Static route configuration window for the Outside interface.

Static route for the secondary default gateway.



Edit Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*

backup

(Interface starting with this icon signifies it is available for route leak)

Available Network

Search

10.10.10.1
10.117.0.250
10.34.24.91
172.16.0.20
172.20.20.13
192.168.1.20

Add

Selected Network

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway

172.20.20.13

Metric:

254

(1 - 254)

Tunneled: □ (Used only for default Route)

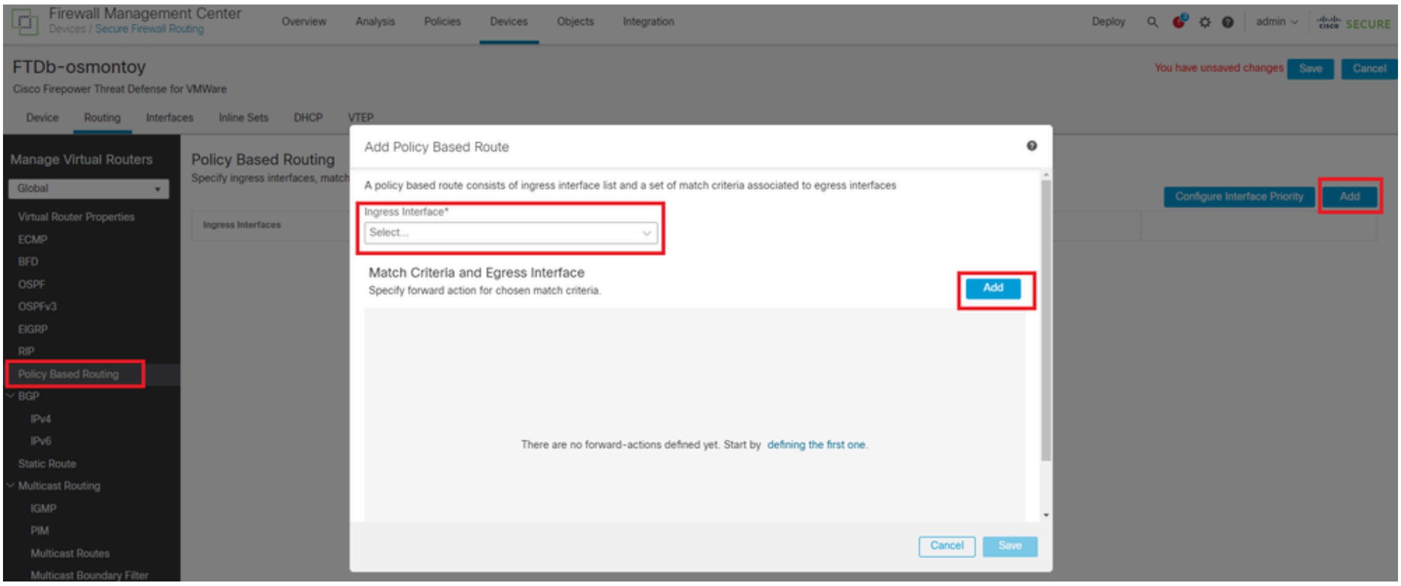
Route Tracking:

SLA2

Image 5. Static route configuration window for the Backup interface.

Step 3. Configure the Policy Base Routes.

Navigate to Device > Device Management > Edit the desired FTD > Routing > Policy Based Routing, add the PBR, and choose the ingress interface.



Add Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*: Select...

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

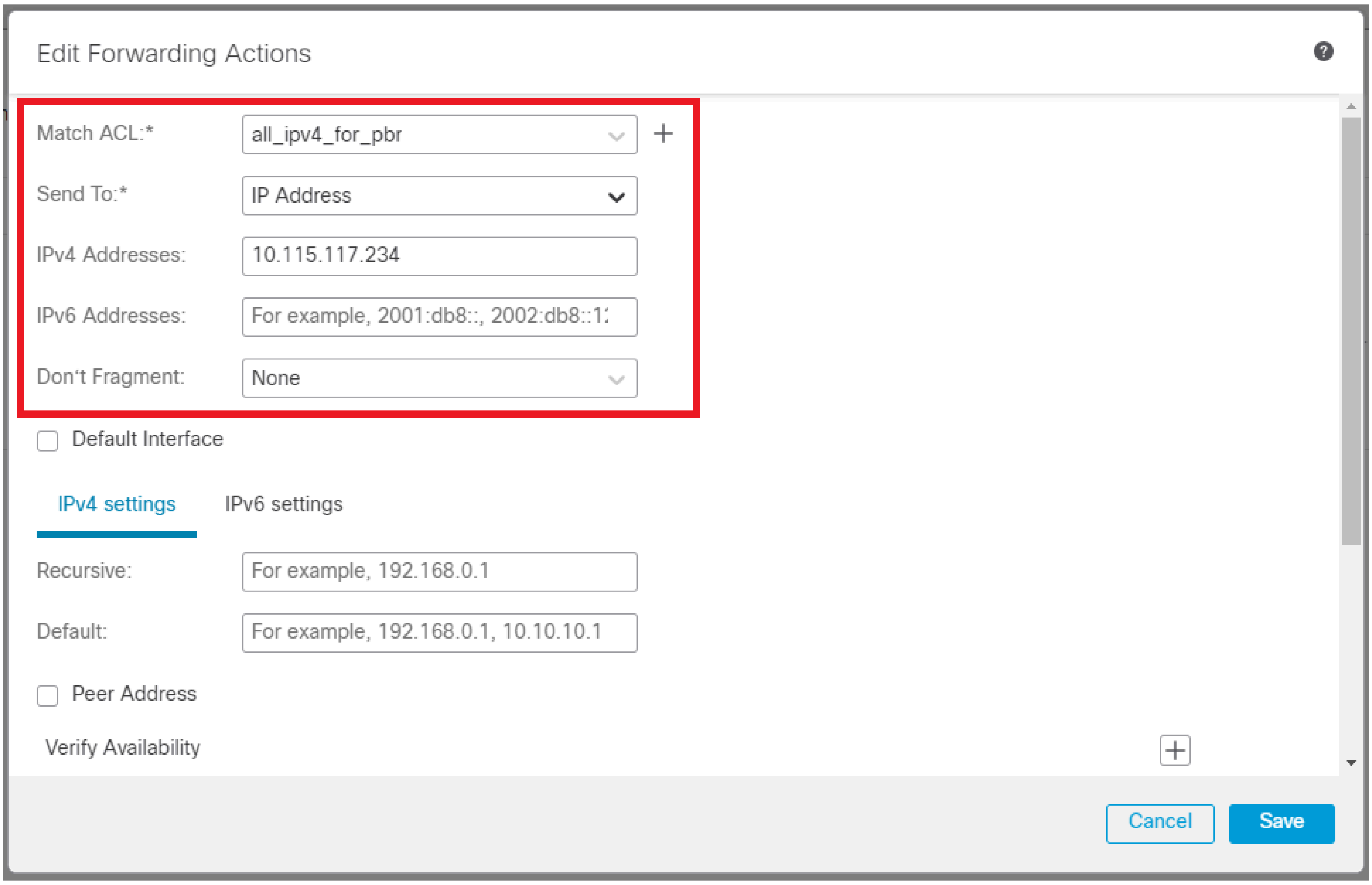
Add

There are no forward-actions defined yet. Start by defining the first one.

Image 6. PBR configuration window.

Configure the forwarding actions.

- Choose or add a new access control list that you want to match.
- ChooseIP Address from the Send to option.
- In this example, 10.115.117.234 is the FTD outside IP address.



Edit Forwarding Actions

Match ACL:* all_ipv4_for_pbr

Send To:* IP Address

IPv4 Addresses: 10.115.117.234

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: None

□ Default Interface

Recursive: For example, 192.168.0.1

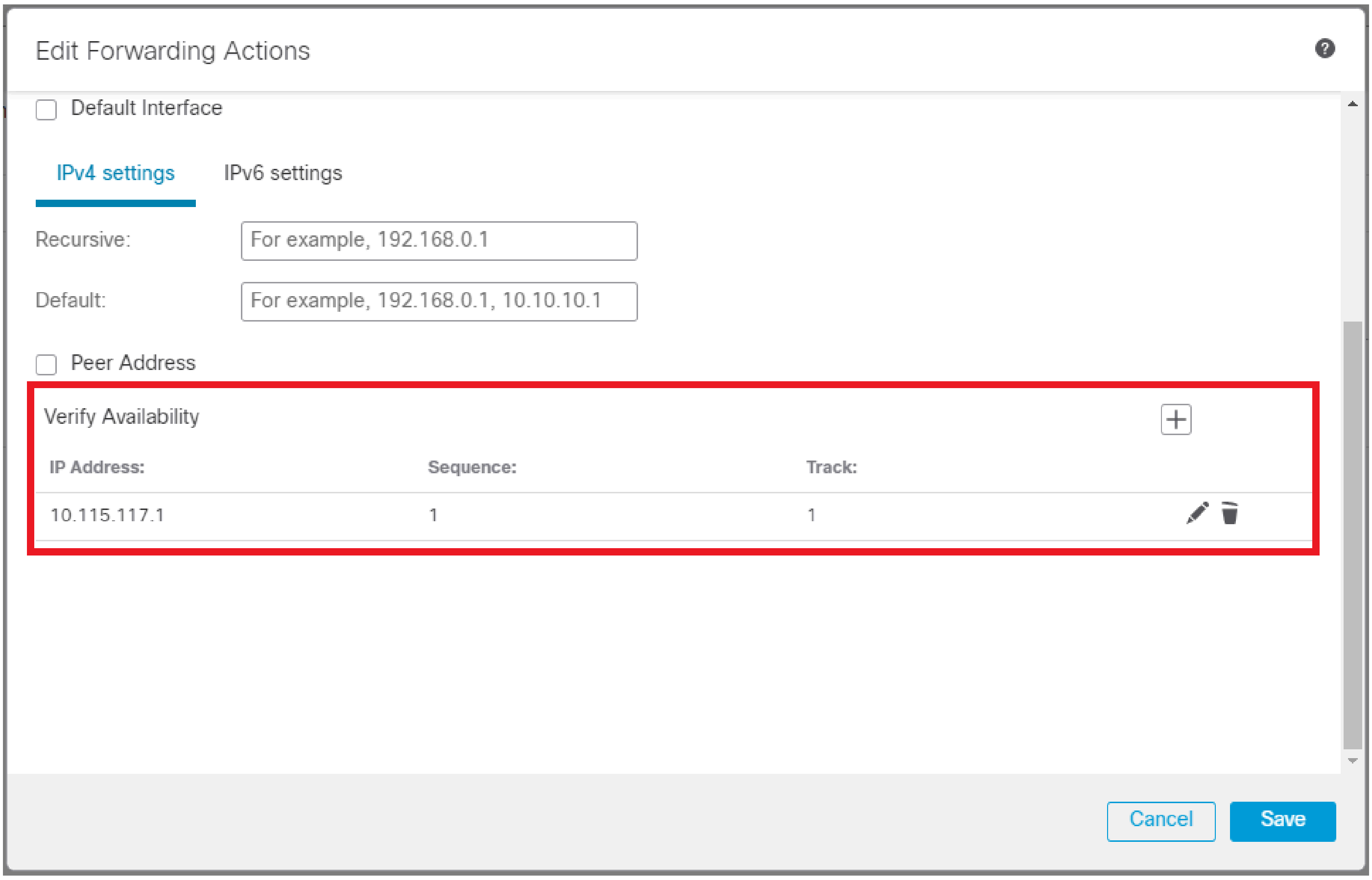
Default: For example, 192.168.0.1, 10.10.10.1

□ Peer Address

Verify Availability

Image 7. Forwarding Actions configuration window.

Scroll down and add the **Verify Availability** values for ISP1.



Edit Forwarding Actions

□ Default Interface

IPv4 settings | IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

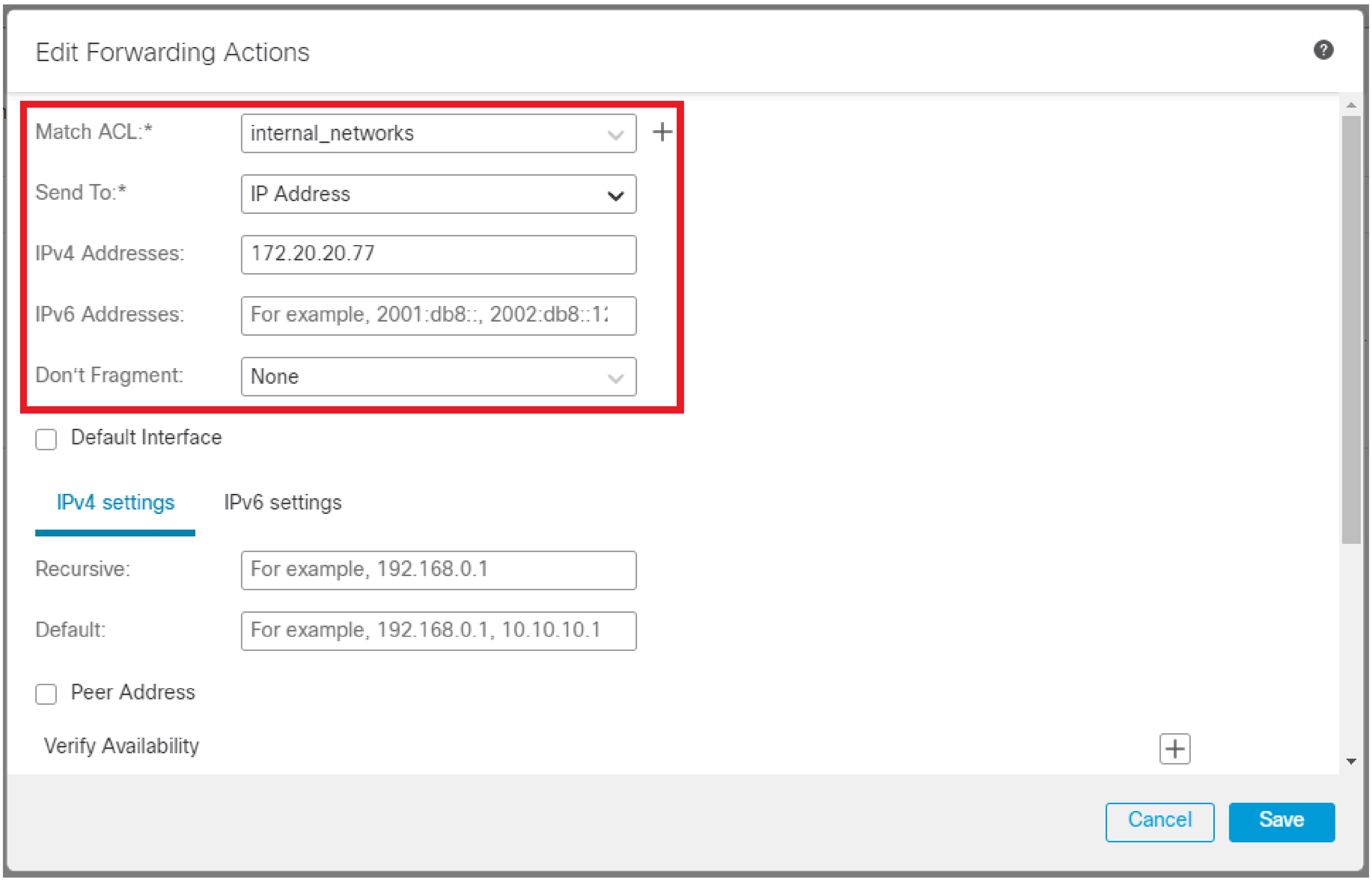
□ Peer Address

Verify Availability

IP Address:	Sequence:	Track:
10.115.117.1	1	1

Image 8. Forwarding Actions configuration window.

Repeat the same process for the backup interface. However, ensure to use a different access control list object.



Edit Forwarding Actions

Match ACL:* internal_networks

Send To:* IP Address

IPv4 Addresses: 172.20.20.77

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: None

□ Default Interface

IPv4 settings | IPv6 settings

Recursive: For example, 192.168.0.1

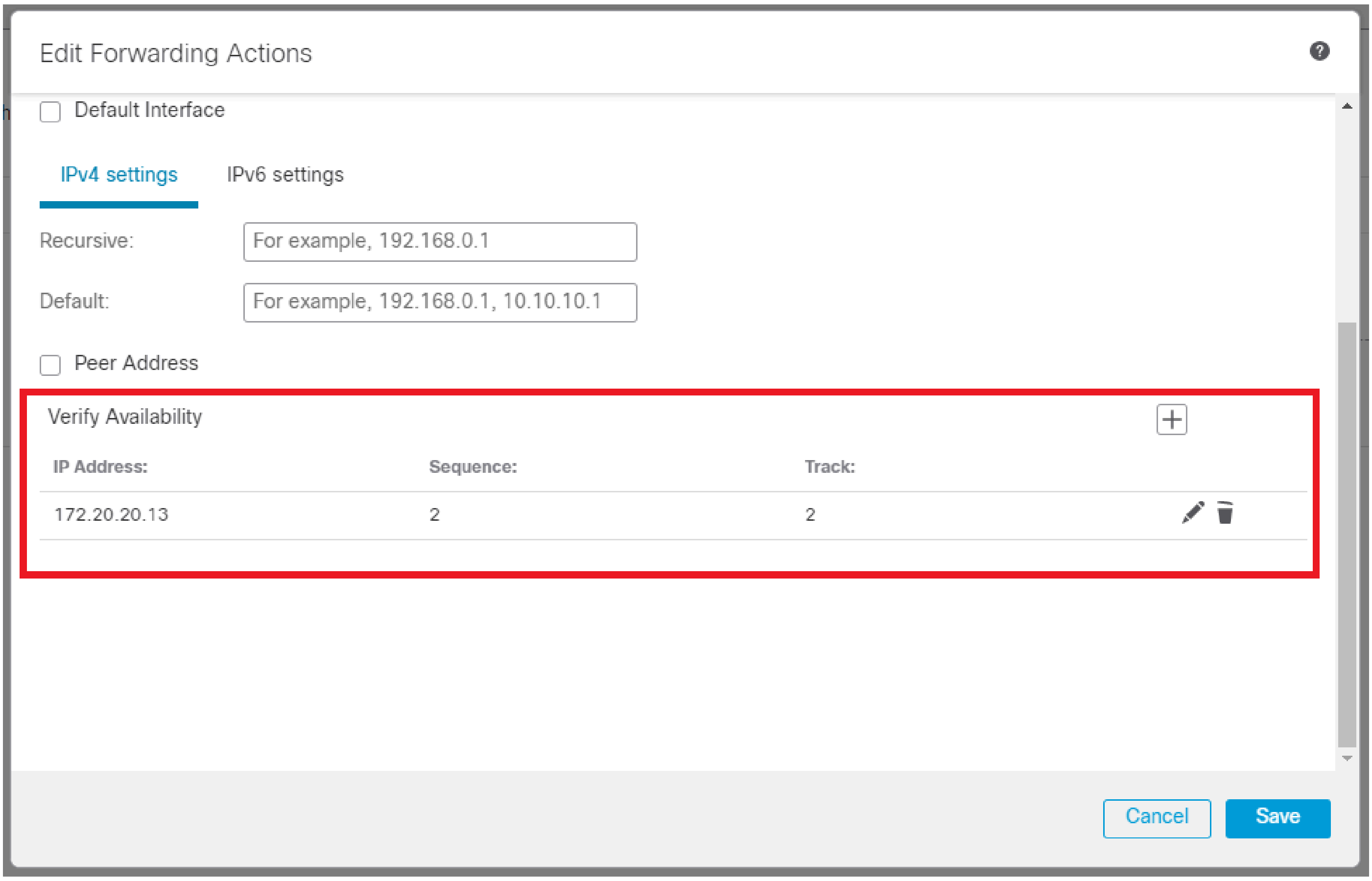
Default: For example, 192.168.0.1, 10.10.10.1

□ Peer Address

Verify Availability

Image 9. Forwarding Actions configuration window

Repeat the same process for theVerify Availabilityconfiguration but now for ISP2.



□ Default Interface

IPv4 settings | IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

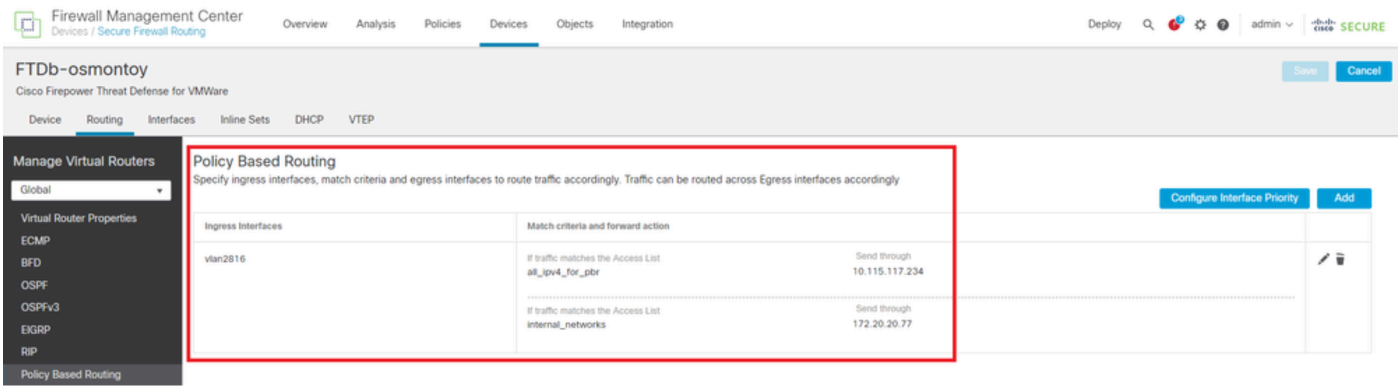
□ Peer Address

Verify Availability

IP Address:	Sequence:	Track:
172.20.20.13	2	2

Image 10.Verify Availability configuraiton.

Validate your configuration.



FTDb-osmontoy

Cisco Firepower Threat Defense for VMWare

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

Ingress Interfaces	Match criteria and forward action	
vlan2816	If traffic matches the Access List all_ipv4_for_pbr	Send through 10.115.117.234
	If traffic matches the Access List internal_networks	Send through 172.20.20.77

Image 11. PBR configuration.

Verify

Access the FTD through Secure Shell (SSH) and use the command system support disagnotsic-cli and run these commands:

- show route-map: This command displays the route-map configuration.

<#root>

```
firepower#

show route-map



route-map FMC_GENERATED_PBR_1679065711925

, permit, sequence 5
Match clauses:
ip address (access-lists): internal_networks

Set clauses:
ip next-hop verify-availability 10.115.117.1 1

track 1 [up]


ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr

Set clauses:
ip next-hop verify-availability 172.20.20.13 2

track 2 [up]


ip next-hop 172.20.20.77
firepower#
```

- show running-config sla monitor: This command displays the SLA configuration.

<#root>

```
firepower#

show running-config sla monitor


sla monitor 1


type echo protocol ipIcmpEcho 10.115.117.1 interface outside
sla monitor schedule 1 life forever start-time now

sla monitor 2


type echo protocol ipIcmpEcho 172.20.20.13 interface backup
sla monitor schedule 2 life forever start-time now
firepower#
```

- show sla monitor configuration: This command displays the SLA configuration values.

<#root>

```
firepower#

show sla monitor configuration


SA Agent, Infrastructure Engine-II
Entry number:

1


Owner:
Tag:
Type of operation to perform: echo

Target address: 10.115.117.1


Interface: outside
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:

Entry number:

2


Owner:
Tag:
Type of operation to perform: echo

Target address: 172.20.20.13


Interface: backup
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:
```

- show sla monitor operational-state: This command displays the operational state of the SLA operation.

<#root>

```
firepower#

show sla monitor operational-state



Entry number: 1


Modification time: 15:48:04.332 UTC Fri Mar 17 2023
Number of Octets Used by this Entry: 2056
Number of operations attempted: 74
Number of operations skipped: 0
Current seconds left in Life: Forever

Operational state of entry: Active


Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 17:01:04.334 UTC Fri Mar 17 2023
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1


Entry number: 2


Modification time: 15:48:04.335 UTC Fri Mar 17 2023
Number of Octets Used by this Entry: 2056
Number of operations attempted: 74
Number of operations skipped: 0
Current seconds left in Life: Forever

Operational state of entry: Active


Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 17:01:04.337 UTC Fri Mar 17 2023
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

- show track: This command displays the information about objects tracked by the SLA Track process.

<#root>

```
firepower#

show track
```

```
Track 1

Response Time Reporter 1 reachability

Reachability is Up

4 changes, last change 00:53:42
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 2 reachability

Reachability is Up

2 changes, last change 01:13:41
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0
```

- show running-config route: This command displays the current route configuration.

<#root>

```
firepower#

show running-config route

route

outside

 0.0.0.0 0.0.0.0 10.115.117.1 1

track 1

route

backup

 0.0.0.0 0.0.0.0 172.20.20.13 254

track 2

route vlan2816 10.42.0.37 255.255.255.255 10.43.0.1 254
firepower#
```

- show route: This command displays the routing table for the data interfaces.

<#root>

```
firepower#

 show 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, BI - BGP InterVRF
Gateway of last resort is 10.115.117.1 to network 0.0.0.0


S* 0.0.0.0 0.0.0.0 [1/0] via 10.115.117.1, outside


S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.255 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
C 172.20.20.0 255.255.255.0 is directly connected, backup
L 172.20.20.77 255.255.255.255 is directly connected, backup
```

When the primary link fails:

- show route-map: This command displays the route-map configuration when a link fails.

<#root>

```
firepower#

show route-map FMC_GENERATED_PBR_1679065711925



route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 5
Match clauses:
ip address (access-lists): internal_networks

Set clauses:
ip next-hop verify-availability 10.115.117.1 1

track 1 [down]
```

```
ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr

Set clauses:
ip next-hop verify-availability 172.20.20.13 2

track 2 [up]


ip next-hop 172.20.20.77
firepower#
```

- show route: This command displays the new routing table per interface.

<#root>

```
firepower#

 show 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, BI - BGP InterVRF
Gateway of last resort is 10.115.117.1 to network 0.0.0.0


S* 0.0.0.0 0.0.0.0 [1/0] via 172.20.20.13, backup


S 10.0.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.255 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
C 172.20.20.0 255.255.255.0 is directly connected, backup
L 172.20.20.77 255.255.255.255 is directly connected, backup
```

Related Information

- Cisco Secure Firewall Management Center Administration Guide, 7.3
- Technical Support & Documentation - Cisco Systems