Configure ECMP with IP SLA on FTD Managed by FMC

Contents

Introduction

This document describes how to configure ECMP along with IP SLA on a FTD that is managed by FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ECMP configuration on Cisco Secure Firewall Threat Defense (FTD)
- IP SLA configuration on Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)

Components Used

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

- Cisco FTD version 7.4.1

- Cisco FMC version 7.4.1

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 Equal-Cost Multi-Path (ECMP) along with Internet Protocol Service Level Agreement (IP SLA) on a Cisco FTD that is managed by Cisco FMC. ECMP allows you to group interfaces together on FTD and load balance traffic across multiple interfaces. IP SLA is a mechanism that monitors end to end connectivity through the exchange of regular packets. Along with ECMP, IP SLA can be implemented in order to ensure availability of the next hop. In this example, ECMP is utilized to distribute packets equally over two Internet Service Provider (ISP) circuits. At the same time, an IP SLA keeps track of connectivity, ensuring a seamless transition to any available circuits in the event of a failure.

Specific requirements for this document include:

- Access to the devices with a user account with administrator privileges
- Cisco Secure Firewall Threat Defense version 7.1 or higher

- Cisco Secure Firewall Management Center version 7.1 or higher

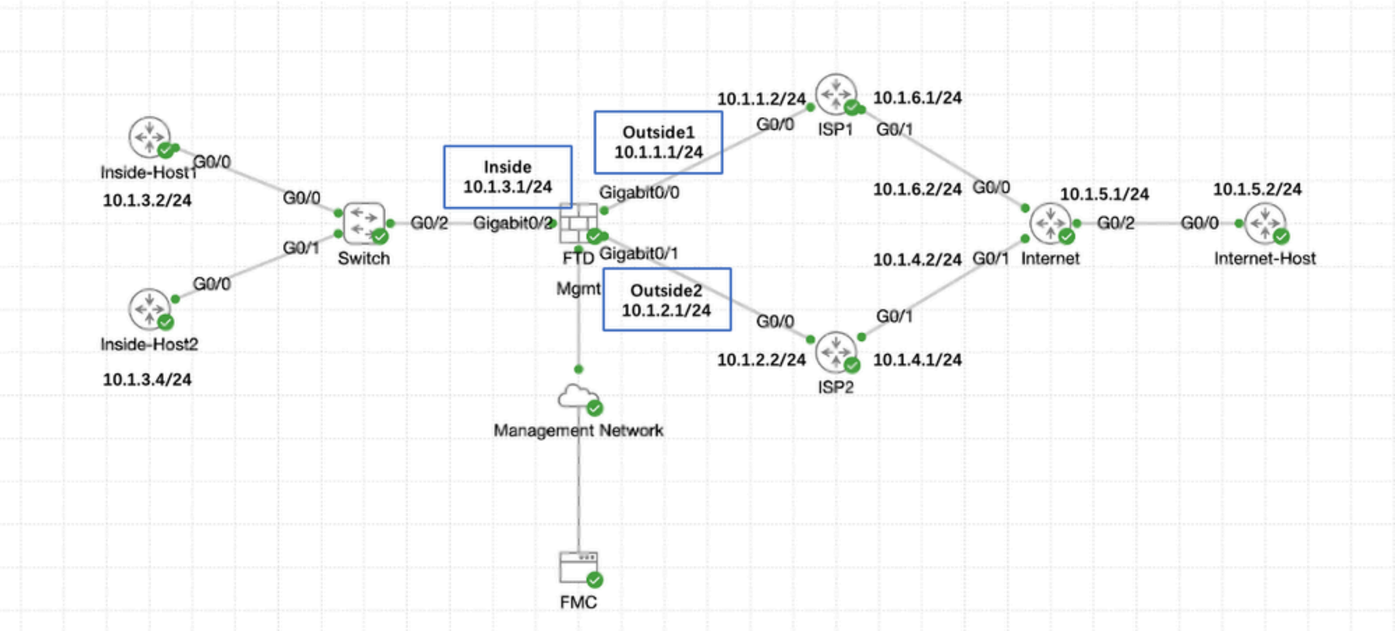
Configure

Network Diagram

In this example, Cisco FTD has two outside interfaces: **outside1** and **outside2** . Each one connects to an ISP gateway, outside1 and outside2 belongs to same ECMP zone named outside.

The traffic from internal network is routed through FTD and get load balanced to the internet through the two ISP.

At the same time, FTD uses IP SLAs in order to monitor connectivity to each ISP Gateway. In case of failure on any of the ISP circuit, FTD failovers to the the other ISP gateway to maintain business continuity.

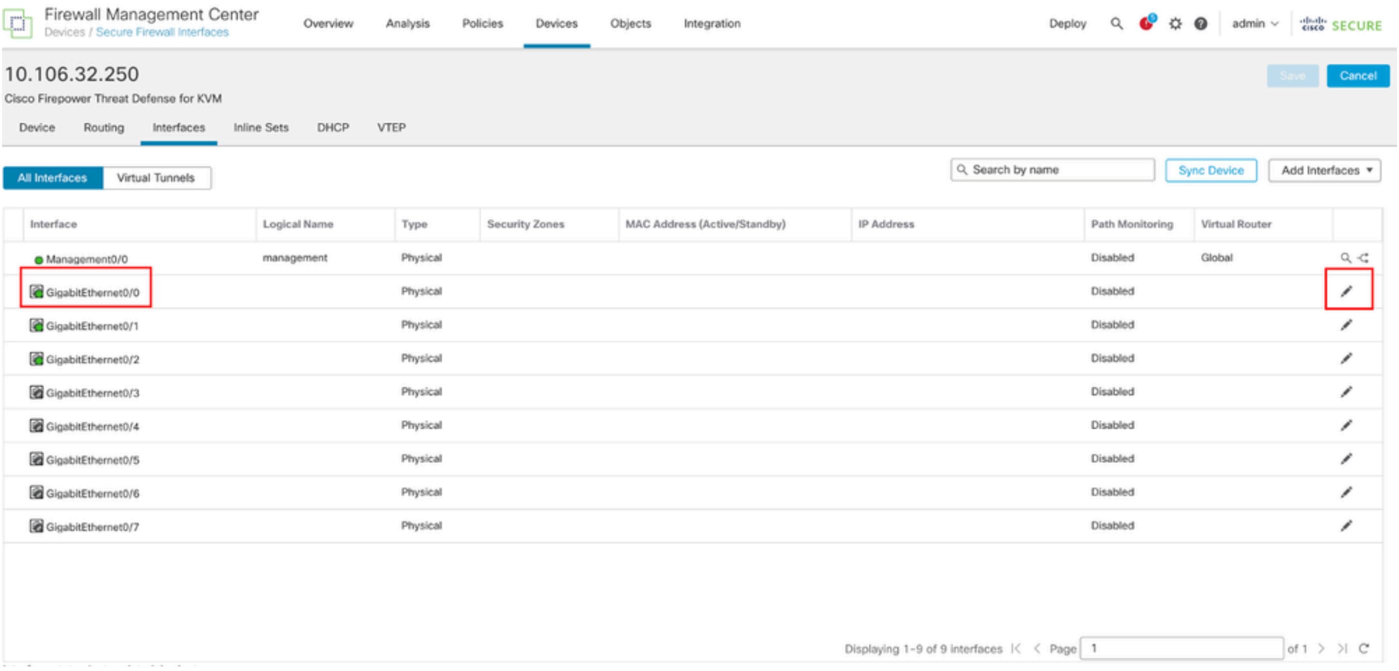


Network Diagram

Configurations

Step 0. Pre-configure Interfaces/Network Objects

Log into the FMC web GUI, Select **Devices**>**Device Management** and click **Edit** button for your threat defense device. The **Interfaces** page is selected by default. Click **Edit** button for the interface you want to edit, in this example **GigabitEthernet0/0**.



10.106.32.250

Cisco Firepower Threat Defense for KVM

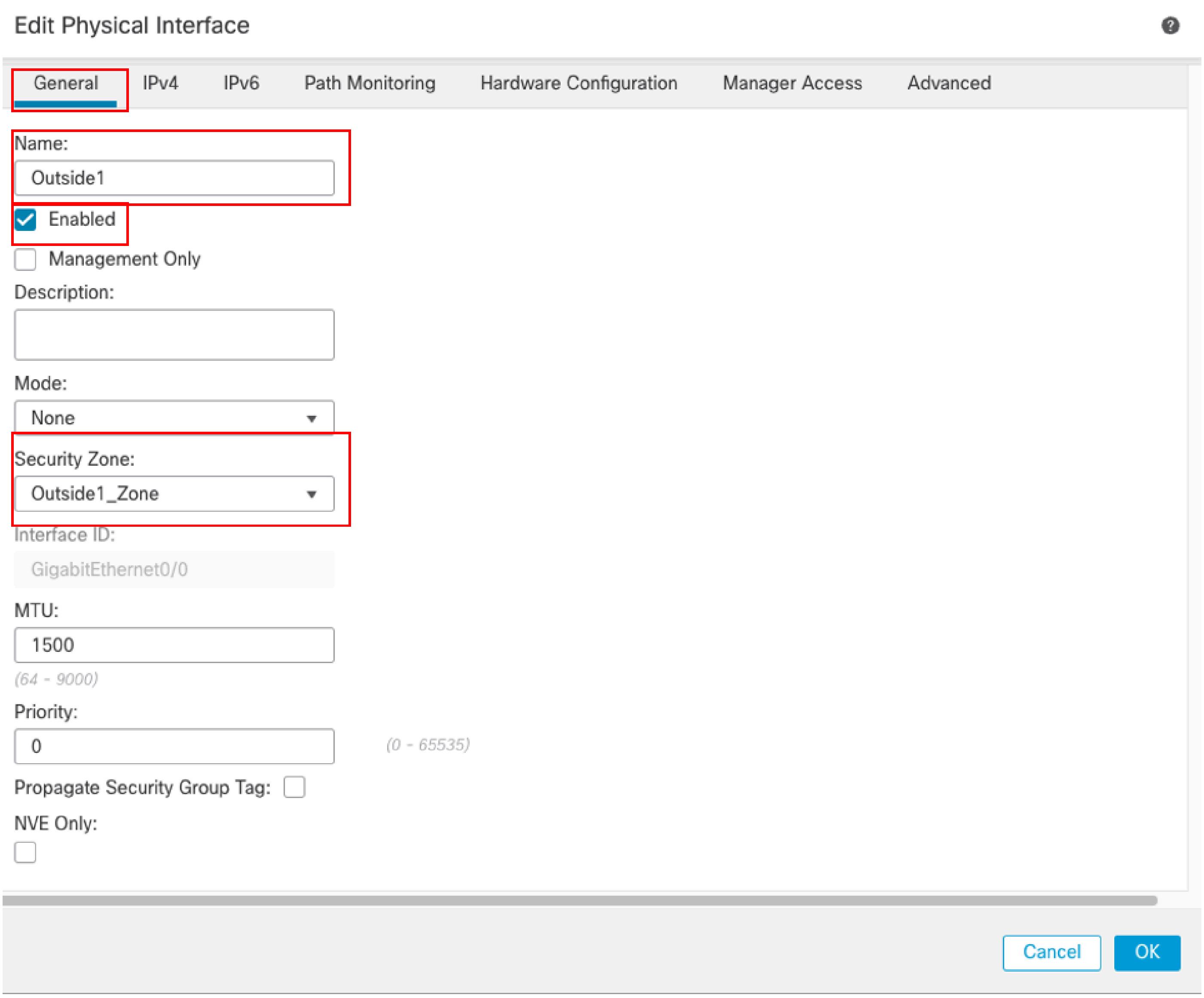
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	
GigabitEthernet0/4		Physical				Disabled	
GigabitEthernet0/5		Physical				Disabled	
GigabitEthernet0/6		Physical				Disabled	
GigabitEthernet0/7		Physical				Disabled	

Displaying 1-9 of 9 interfaces Page 1 of 1

Edit Interface Gi0/0

In the **Edit Physical Interface** window, under **General** tab:

1. Set the **Name**, in this case **Outside1**.
2. Enable the interface by checking the **Enabled** check box.
3. In the **Security Zone** drop-down list, select an existing Security Zone or create a new one, in this example **Outside1_Zone**.



Name: Outside1

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: Outside1_Zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

Priority: 0 (0 - 65535)

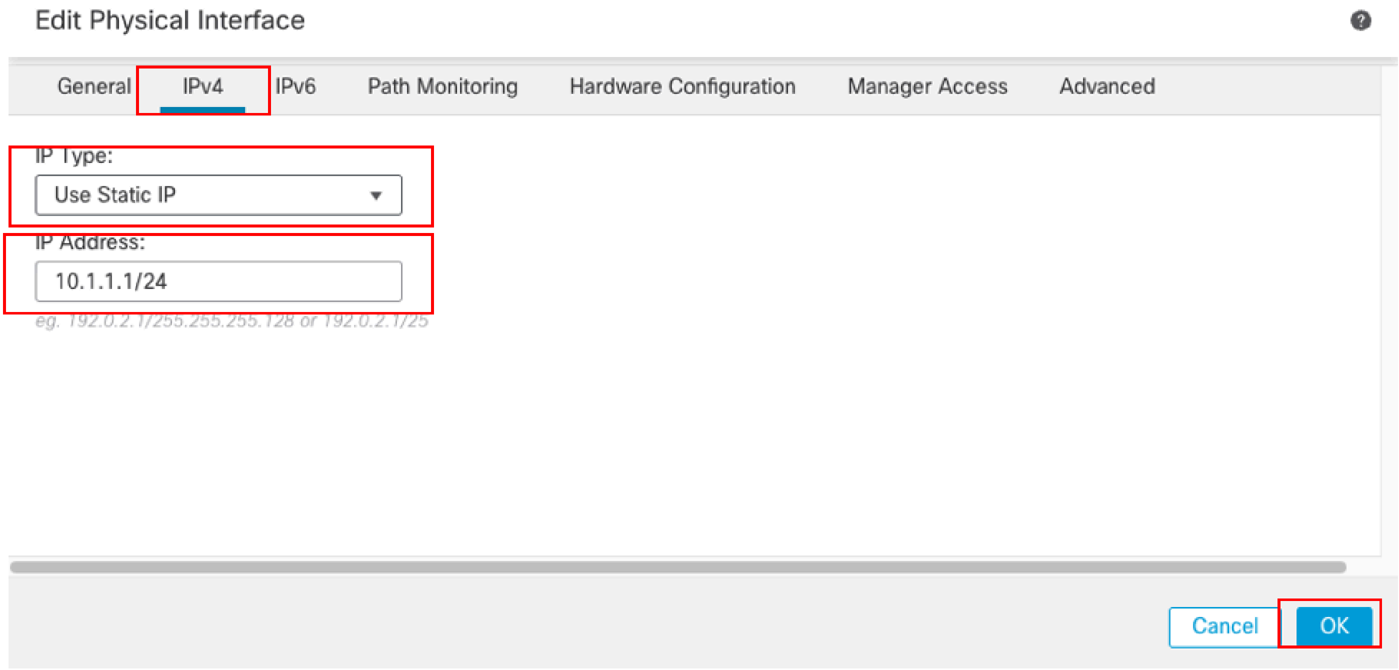
Propagate Security Group Tag: □

NVE Only: □

Interface Gi0/0 General

Under the **IPv4** tab:

1. Choose one of the options from the **IP Type** drop-down list, in this example **Use Static IP**.
2. Set the **IP Address**, in this example **10.1.1.1/24**.
3. Click **OK**.



Edit Physical Interface

IP Type: Use Static IP

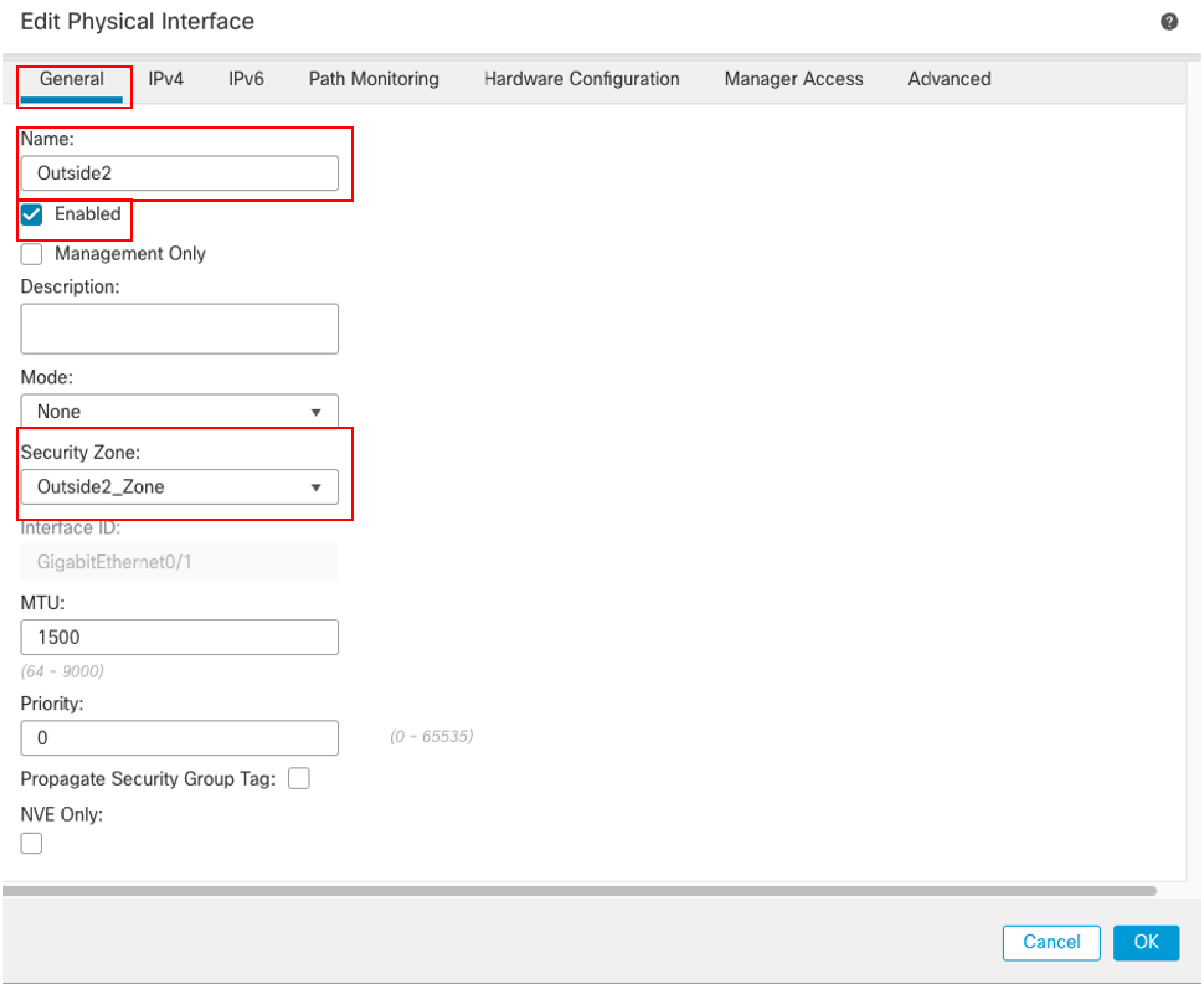
IP Address: 10.1.1.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Interface Gi0/0 IPv4

Repeat similar step to configure interface **GigabitEthernet0/1**, In the **Edit Physical Interface** window, under **General** tab:

1. Set the **Name**, in this case **Outside2**.
2. Enable the interface by checking the **Enabled** check box.
3. In the **Security Zone** drop-down list, select an existing Security Zone or create a new one, in this example **Outside2_Zone**.



Edit Physical Interface

Name: Outside2

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: Outside2_Zone

Interface ID: GigabitEthernet0/1

MTU: 1500

(64 - 9000)

Priority: 0 (0 - 65535)

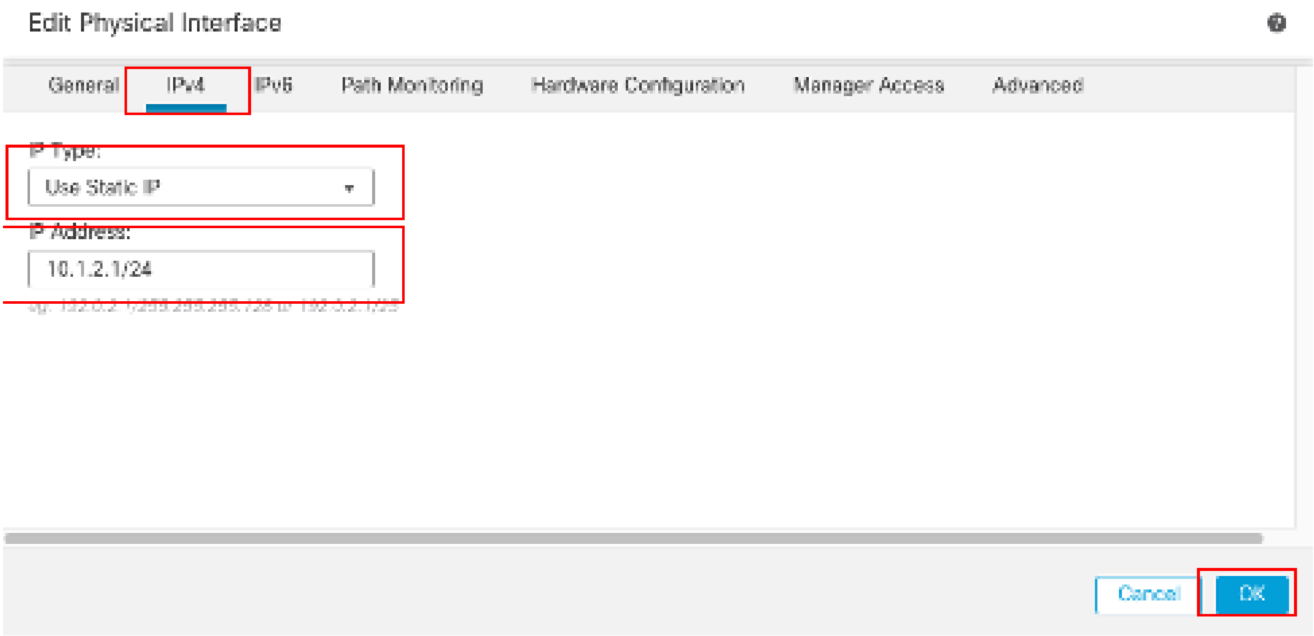
Propagate Security Group Tag: □

NVE Only: □

Interface Gi0/1 General

Under the **IPv4** tab:

1. Choose one of the options from the **IP Type** drop-down list, in this example **Use Static IP**.
2. Set the **IP Address**, in this example **10.1.2.1/24**.
3. Click **OK**.



IP Type: Use Static IP

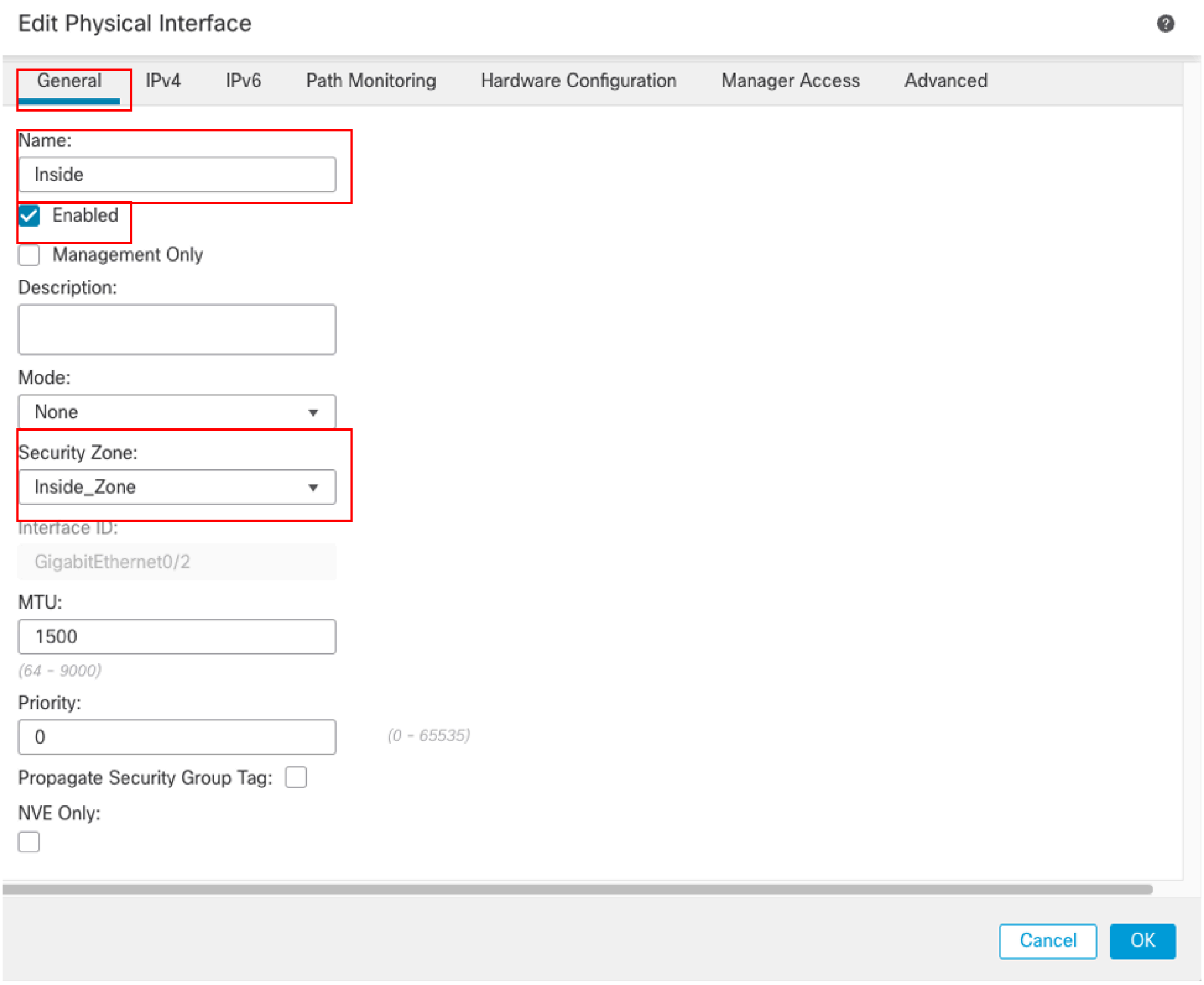
IP Address: 10.1.2.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Interface Gi0/1 IPv4

Repeat similar step to configure interface **GigabitEthernet0/2**, In the **Edit Physical Interface** window, under **General** tab:

1. Set the **Name**, in this case **Inside**.
2. Enable the interface by checking the **Enabled** check box.
3. In the **Security Zone** drop-down list, select an existing Security Zone or create a new one, in this example **Inside_Zone**.



Name: Inside

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: Inside_Zone

Interface ID: GigabitEthernet0/2

MTU: 1500 (64 - 9000)

Priority: 0 (0 - 65535)

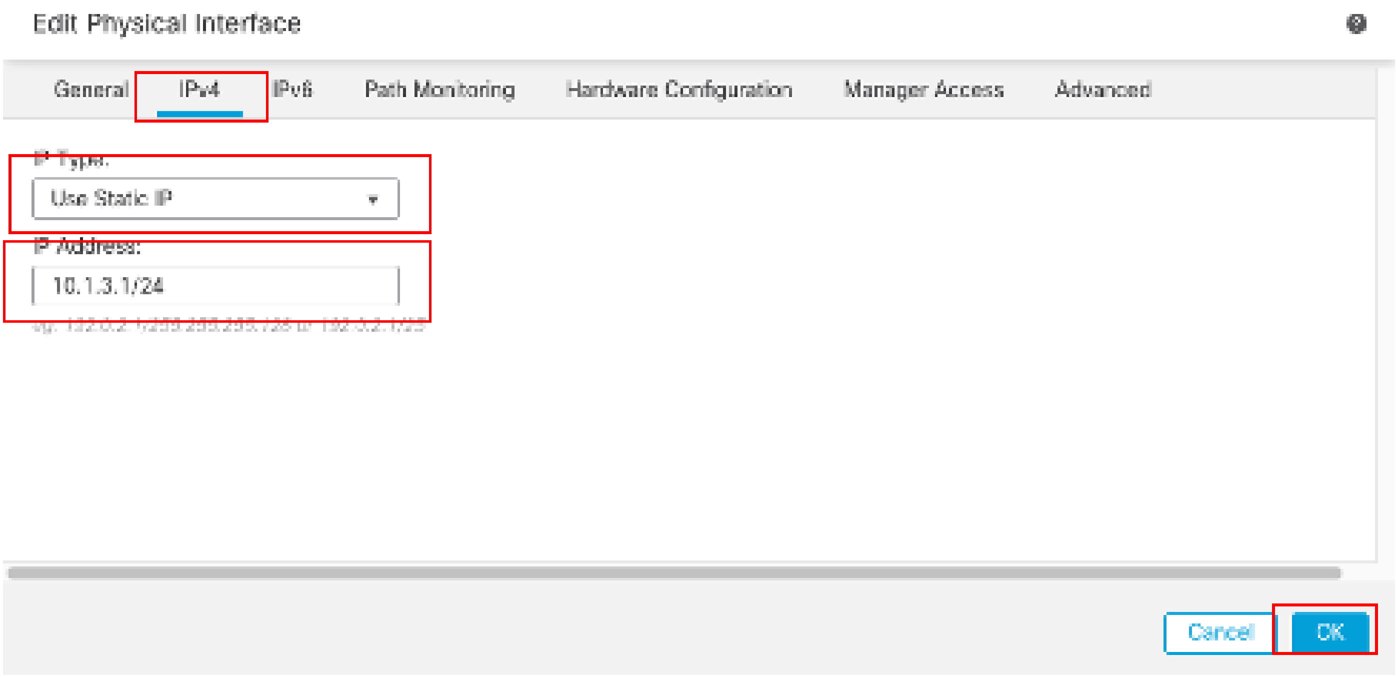
Propagate Security Group Tag: □

NVE Only: □

Interface Gi0/2 General

Under the **IPv4** tab:

1. Choose one of the options from the **IP Type** drop-down list, in this example **Use Static IP**.
2. Set the **IP Address**, in this example **10.1.3.1/24**.
3. Click **OK**.



IP Type:
Use Static IP

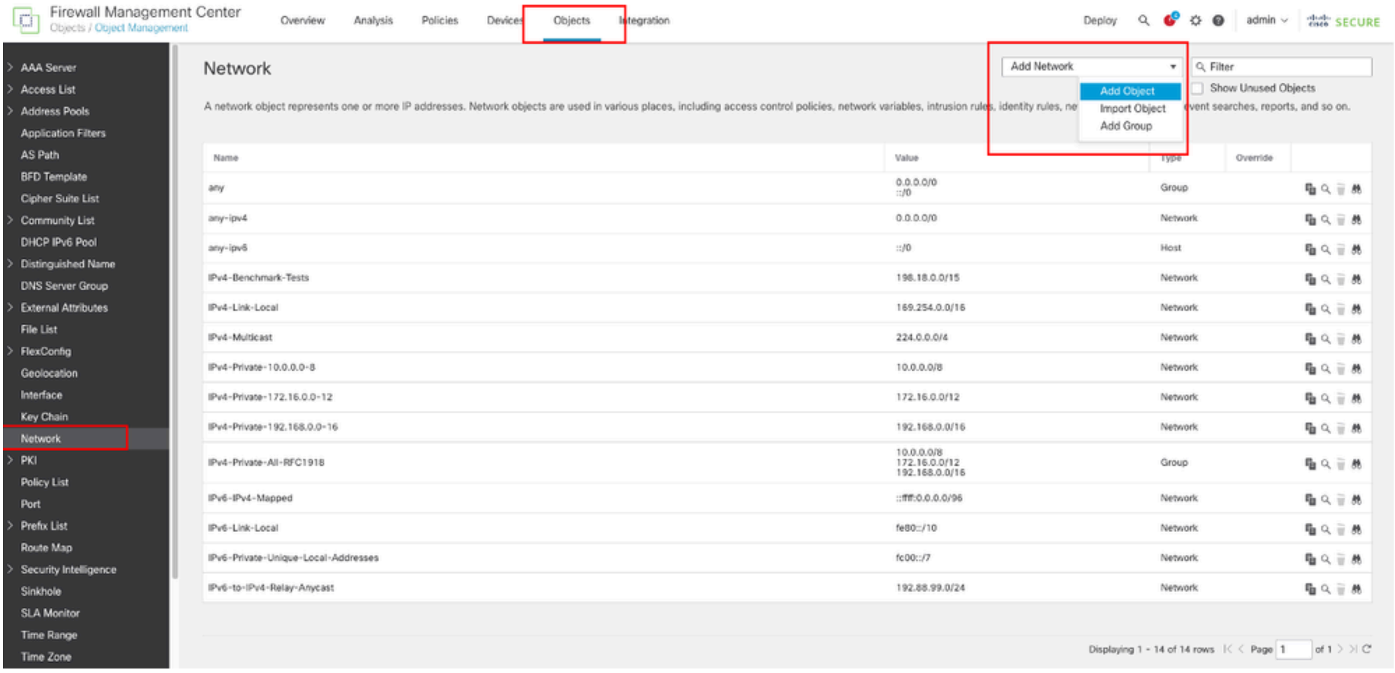
IP Address:
10.1.3.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Interface Gi0/2 IPv4

Click **Save** and **Deploy** the configuration.

Navigate to **Objects** > **Object Management**, Choose **Network** from the list of object types, Choose **Add Object** from the **Add Network** drop-down menu to create a object for first ISP gateway.



Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, ne event searches, reports, and so on.

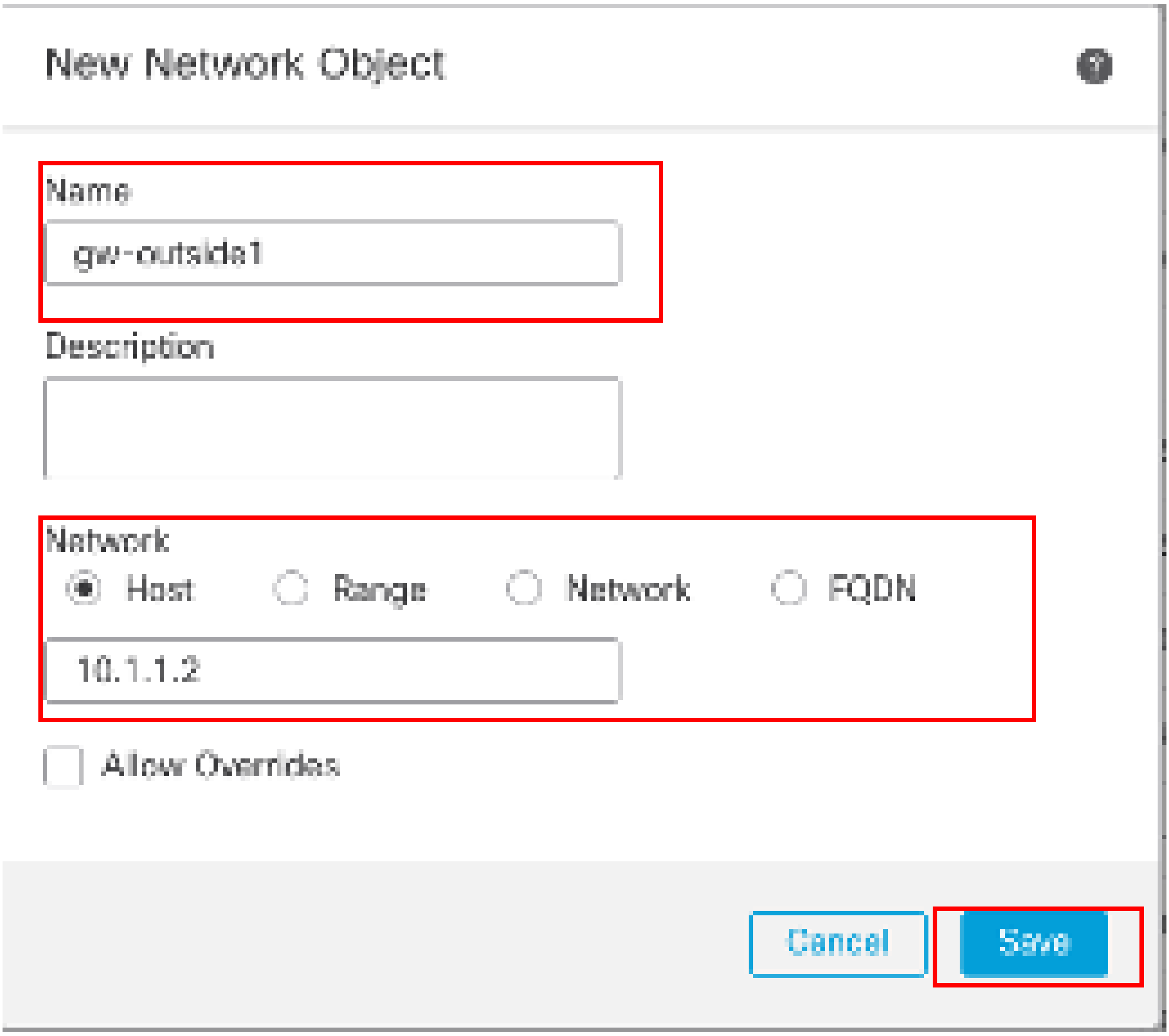
Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	::/0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96	Network	
IPv6-Link-Local	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24	Network	

Displaying 1 - 14 of 14 rows Page 1 of 1

Network Object

In the **New Network Object** window:

1. Set the **Name**, in this example **gw-outside1**.
2. In the **Network** field, select the required option and enter an appropriate value, in this example **Host** and **10.1.1.2**.
3. Click **Save**.



New Network Object

Name

gw-outside1

Description

Network

● Host ○ Range ○ Network ○ FQDN

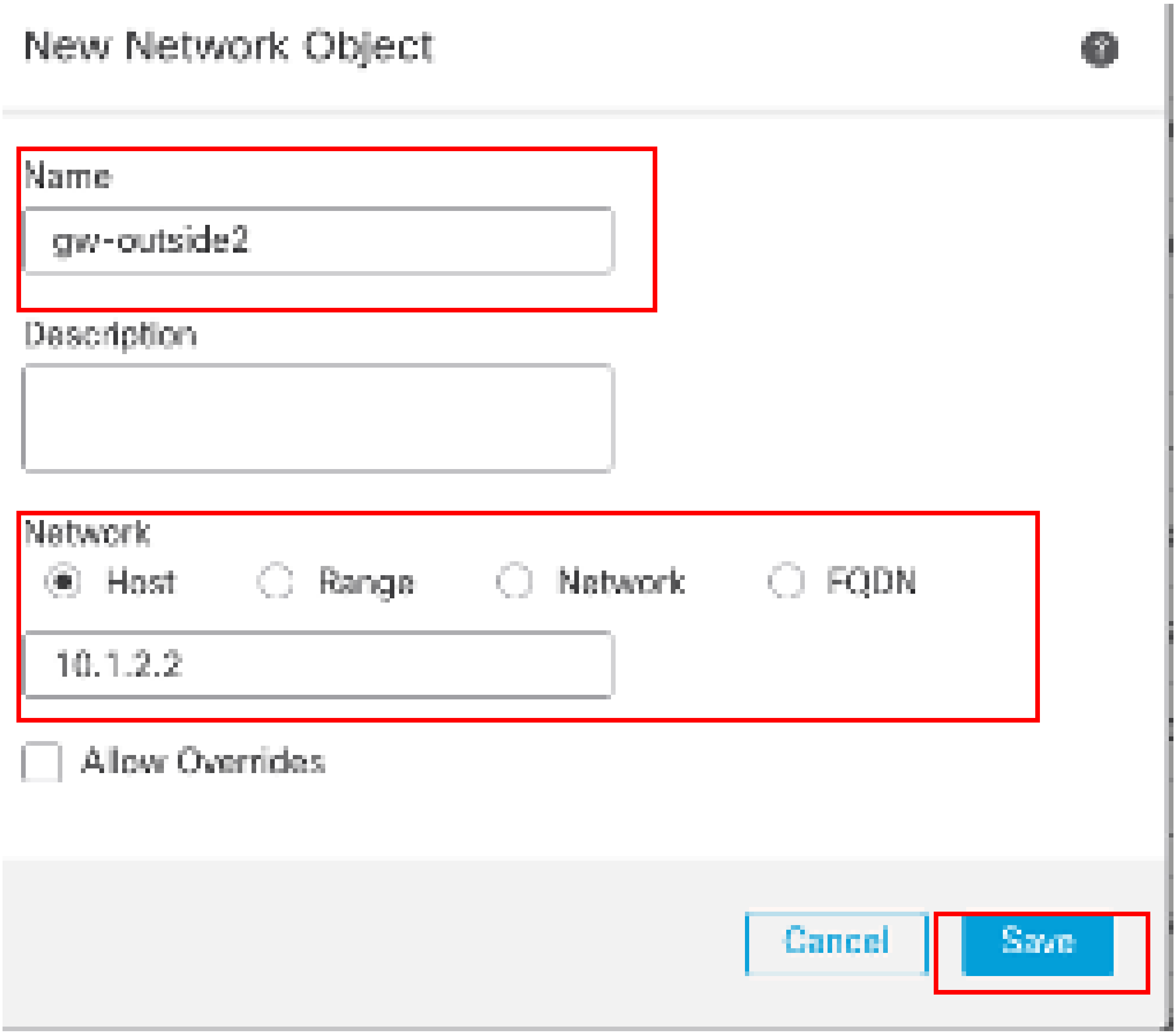
10.1.1.2

□ Allow Overrides

Object Gw-outside1

Repeat similar steps to create another object for second ISP gateway. In the **New Network Object** window:

1. Set the **Name**, in this example **gw-outside2**.
2. In the **Network** field, select the required option and enter an appropriate value, in this example **Host** and **10.1.2.2**.
3. Click **Save**.



New Network Object

Name

gw-outside2

Description

Network

● Host ○ Range ○ Network ○ FQDN

10.1.2.2

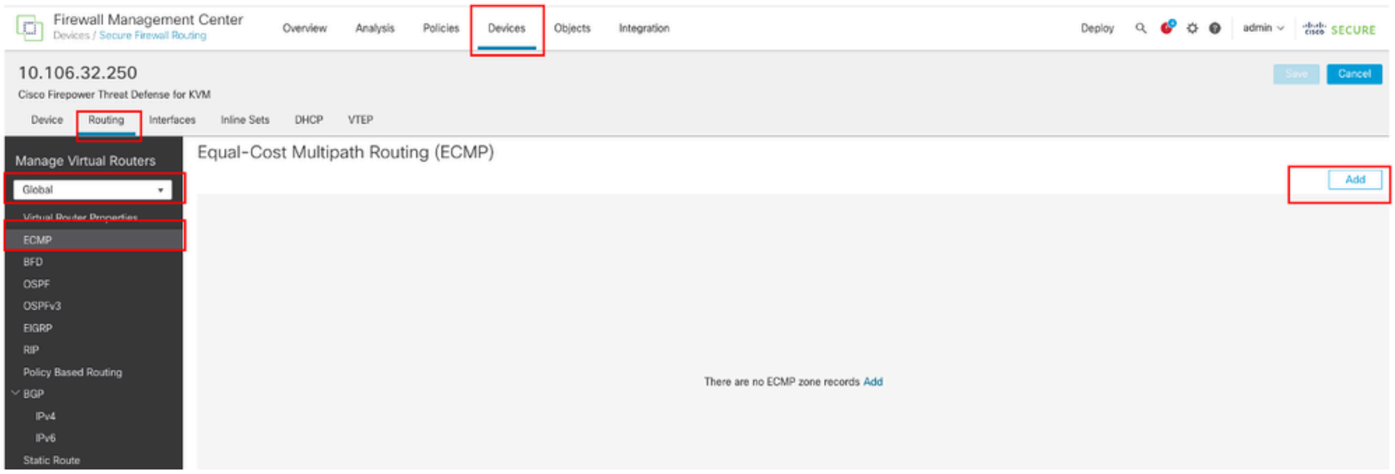
□ Allow Overrides

Object Gw-outside2

Step 1. Configure ECMP Zone

Navigate to **Devices** > **Device Management** and edit the threat defense device, click **Routing**. From the **virtual router** drop-down, select the virtual router in which you want to create the ECMP zone. You can create ECMP zones in global virtual router and user-defined virtual routers. In this example, choose **Global**.

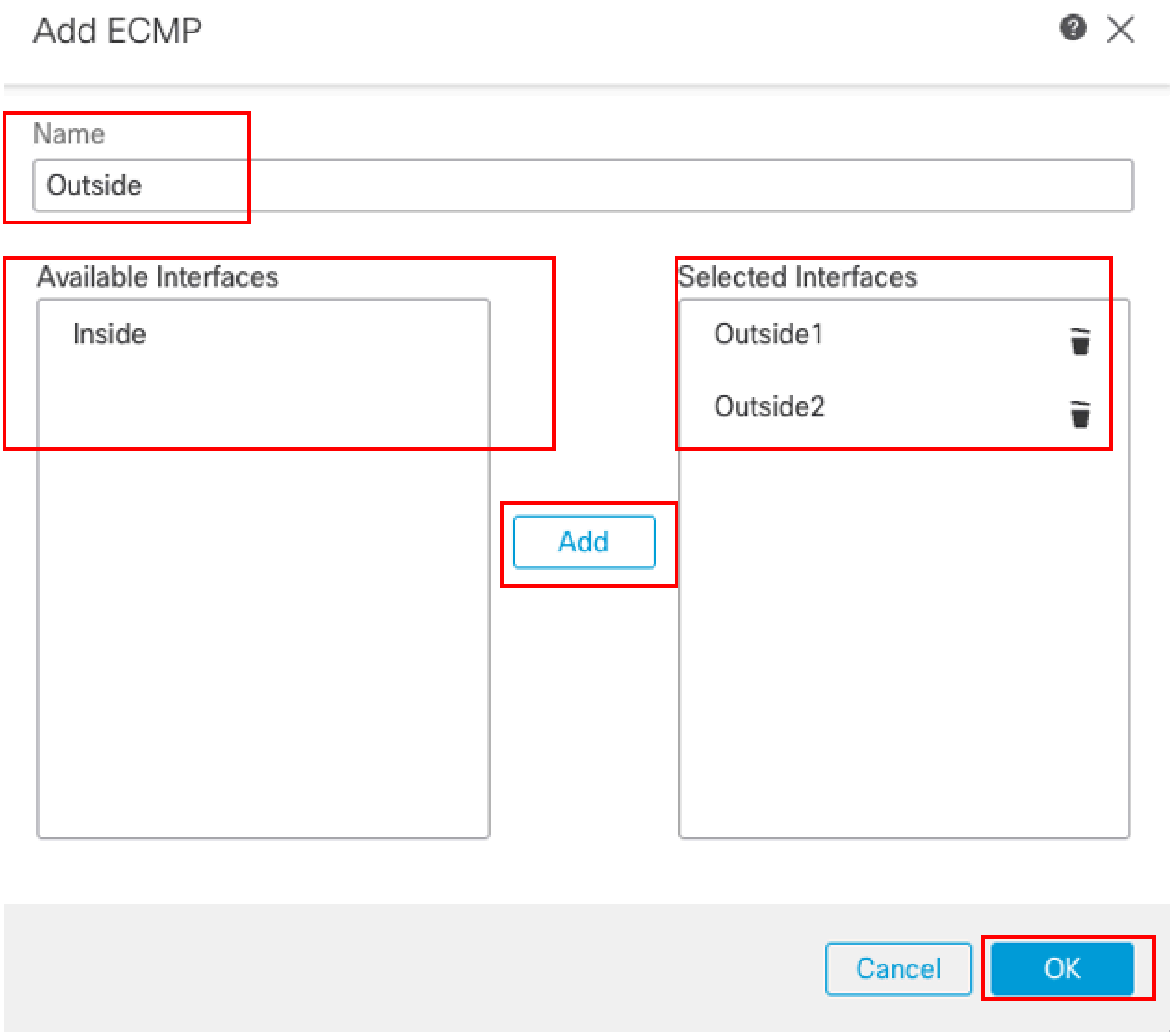
Click **ECMP**, then click **Add**.



Configure ECMP Zone

In the **Add ECMP** window:

1. Set **Name** for ECMP zone, in this example **Outside**.
2. To associate interfaces, select the interface under the **Available Interfaces** box, and then click Add. In this example **Outside1** and **Outside2**.
3. Click **OK**.



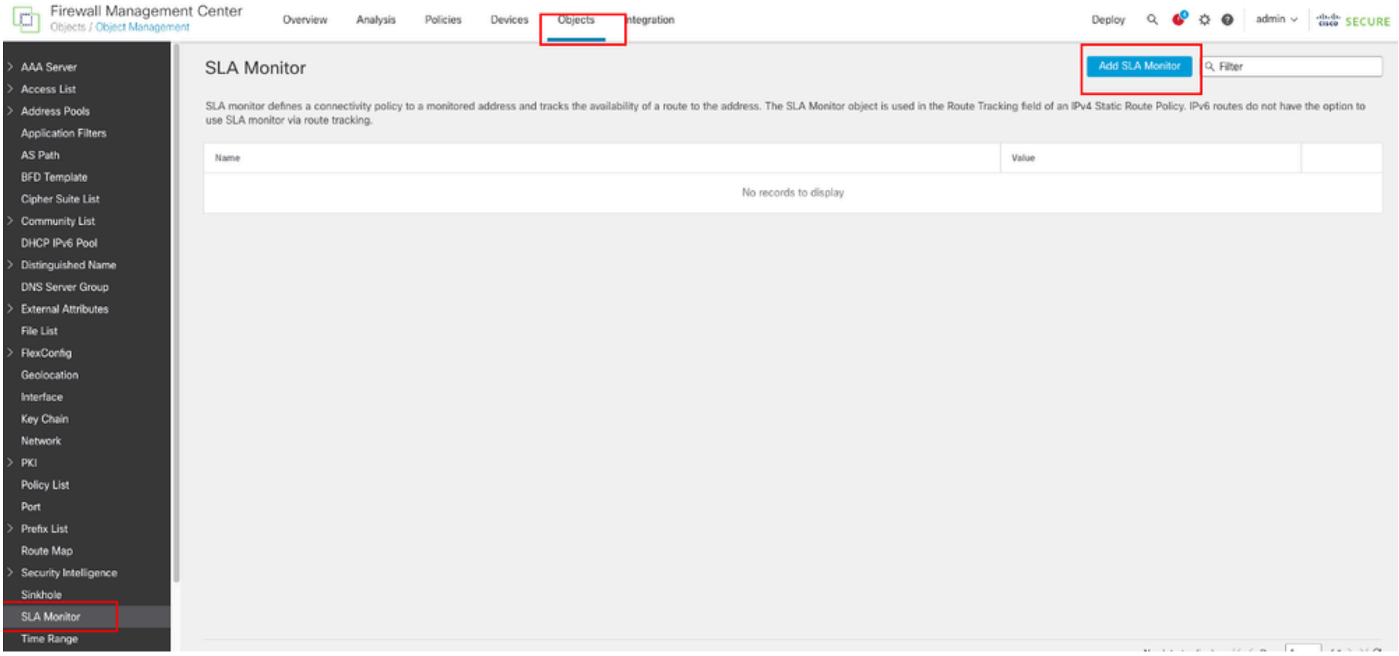
Name: Outside

Configure ECMP Zone Outside

Click **Save** and **Deploy** the configuration.

Step 2. Configure IP SLA Objects

Navigate to **Objects** > **Object Management**, Choose **SLA Monitor** from the list of object types, Click **Add SLA Monitor** to add a new SLA monitor for the first ISP gateway.



SLA Monitor

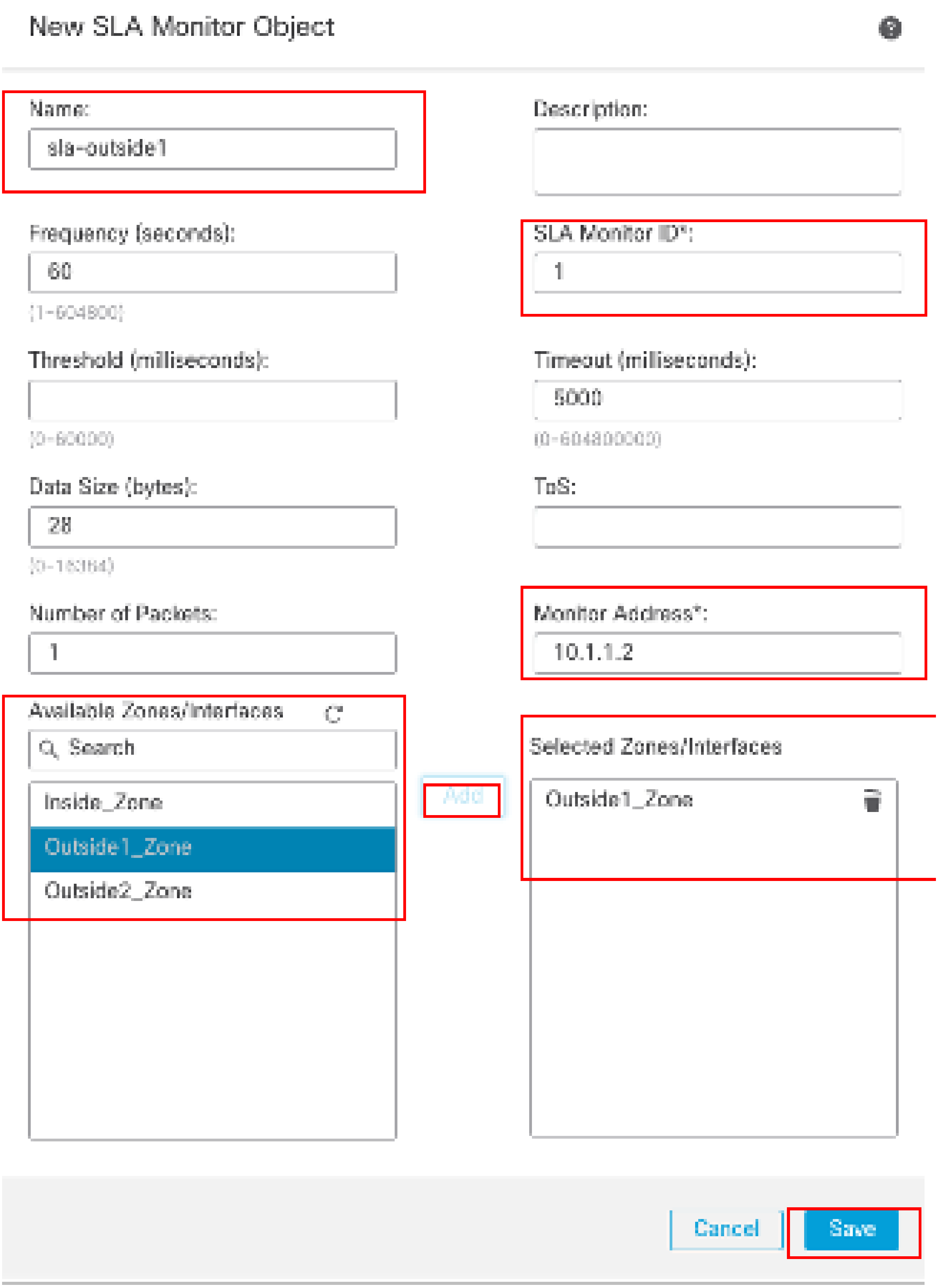
SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
No records to display	

Create SLA Monitor

In the **New SLA Monitor Object** window:

1. Set the **Name** for the SLA monitor object, in this case **sla-outside1**.
2. Enter the ID number of the SLA operation in the **SLA Monitor ID** field. Values range from 1 to 2147483647. You can create a maximum of 2000 SLA operations on a device. Each ID number must be unique to the policy and the device configuration. In this example **1**.
3. Enter the IP address that is being monitored for availability by the SLA operation, in the **Monitored Address** field. In this example **10.1.1.2**.
4. The **Available Zones/Interfaces** list displays both zones and interface groups. In the Zones/Interfaces list, add the zones or interface groups that contain the interfaces through which the device communicates with the management station. To specify a single interface, you need to create a zone or the interface groups for the interface. In this example **Outside1_Zone**.
5. Click **Save**.



New SLA Monitor Object

Name: sla-outside1

Description:

Frequency (seconds): 60 (1-604800)

SLA Monitor ID*: 1

Threshold (milliseconds): (0-60000)

Timeout (milliseconds): 5000 (0-604800000)

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

ToS:

Number of Packets: 1

Monitor Address*: 10.1.1.2

Available Zones/Interfaces: Inside_Zone, Outside1_Zone, Outside2_Zone

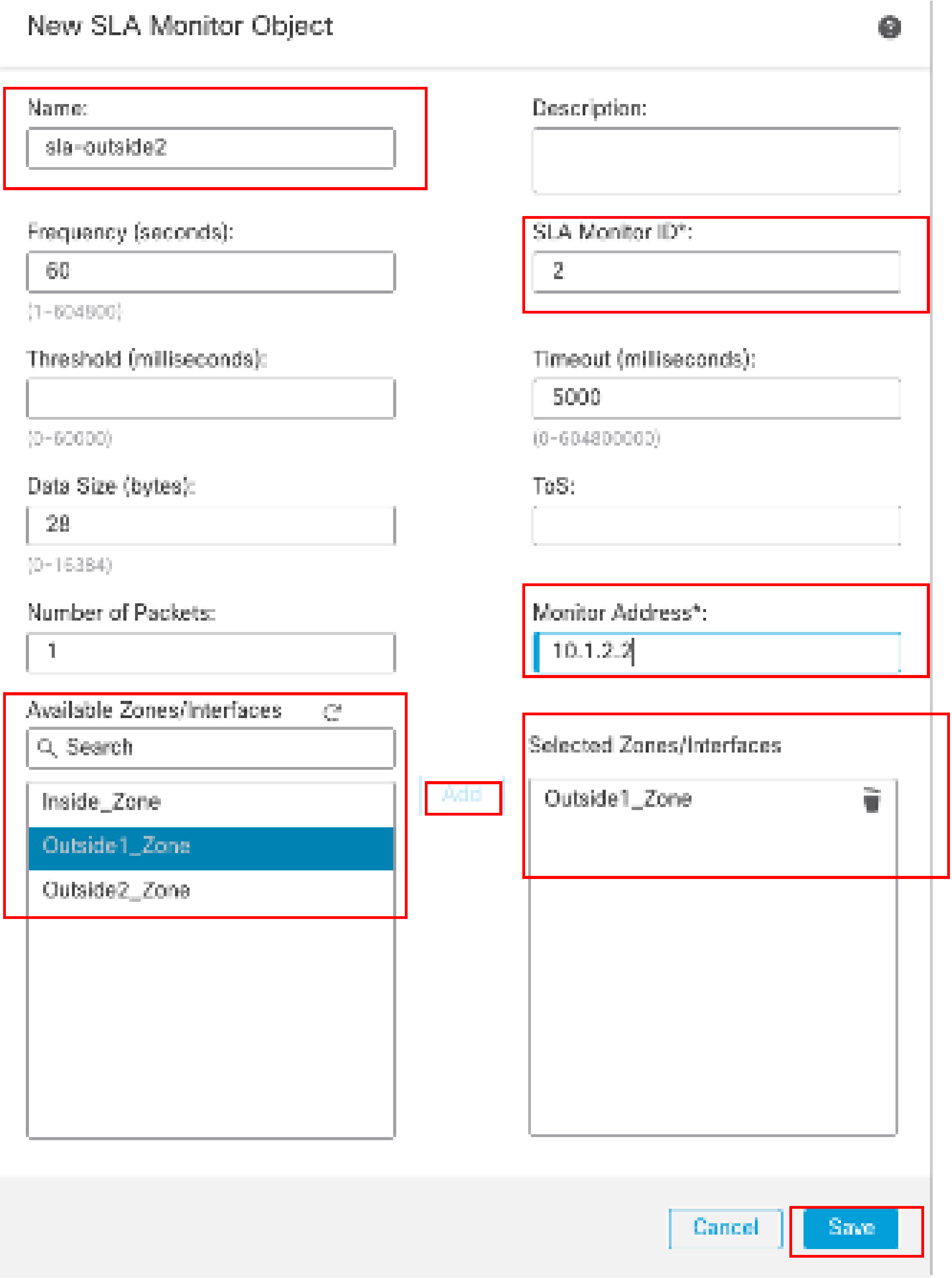
Selected Zones/Interfaces: Outside1_Zone

SLA Object Sla-outside1

Repeat similar steps to create another SLA monitor for the second ISP gateway.

In the **New SLA Monitor Object** window:

1. Set the **Name** for the SLA monitor object, in this case **sla-outside2**.
2. Enter the ID number of the SLA operation in the **SLA Monitor ID** field. Values range from 1 to 2147483647. You can create a maximum of 2000 SLA operations on a device. Each ID number must be unique to the policy and the device configuration. In this example **2**.
3. Enter the IP address that is being monitored for availability by the SLA operation, in the **Monitored Address** field. In this example **10.1.2.2**.
4. The **Available Zones/Interfaces** list displays both zones and interface groups. In the Zones/Interfaces list, add the zones or interface groups that contain the interfaces through which the device communicates with the management station. To specify a single interface, you need to create a zone or the interface groups for the interface. In this example **Outside2_Zone**.
5. Click **Save**.



New SLA Monitor Object

Name: sla-outside2

Description:

Frequency (seconds): 60
(1-604800)

SLA Monitor ID*: 2

Threshold (milliseconds):
(0-60000)

Timeout (milliseconds): 5000
(0-604800000)

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

ToS:

Number of Packets: 1

Monitor Address*: 10.1.2.2

Available Zones/Interfaces
- Inside_Zone
- Outside1_Zone
- Outside2_Zone

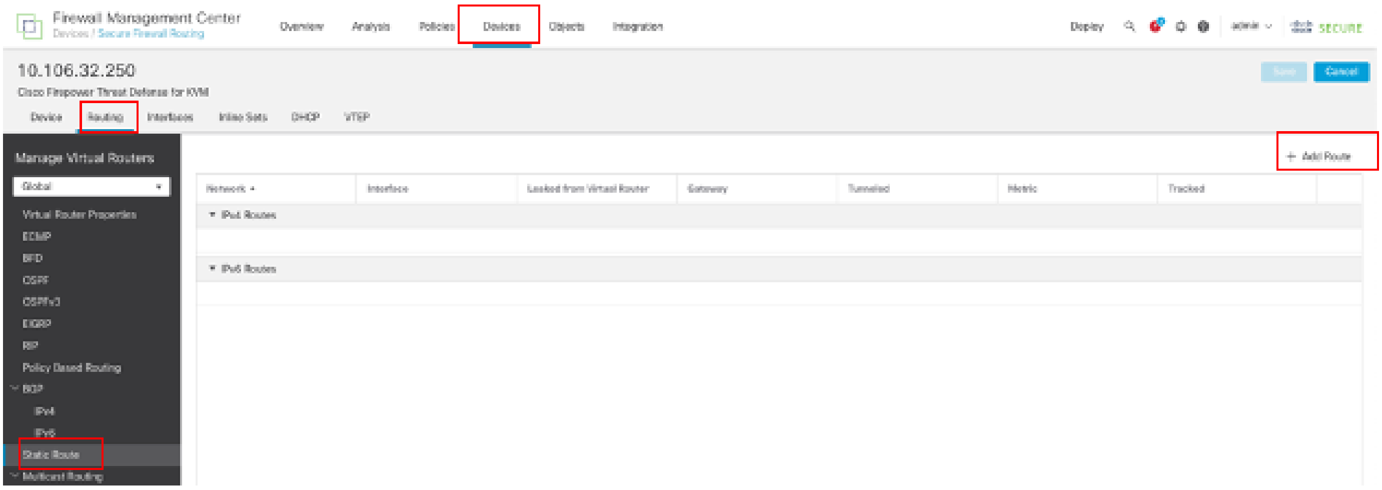
Selected Zones/Interfaces
- Outside1_Zone

SLA Object Sla-outside2

Step 3. Configure Static Routes with Route Track

Navigate to **Devices** > **Device Management**, and edit the threat defense device, click **Routing**, From the **virtual routers** drop-down list, select the virtual router for which you are configuring a static route. In this example **Global**.

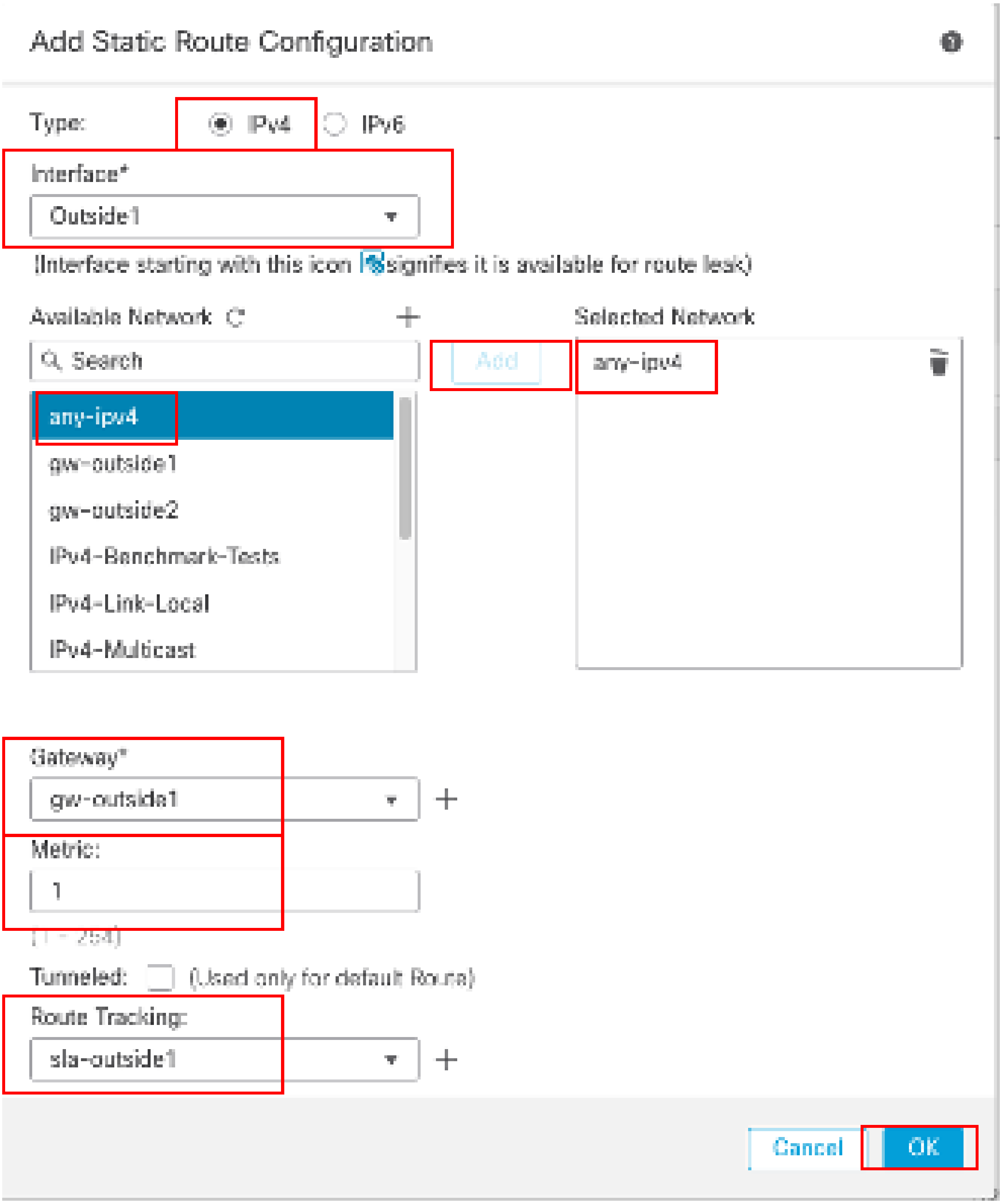
Select **Static Route**, click **Add Route** to add the default route to first ISP gateway.



Configure Static Route

In the **Add Static Route Configuration** window:

1. Click **IPv4** or **IPv6** depending on the type of static route that you are adding. In this example **IPv4**.
2. Choose the **Interface** to which this static route applies. In this example **Outside1**.
3. In the **Available Network** list, choose the destination network. In this example **any-ipv4**.
4. In the **Gateway** or **IPv6 Gateway** field, enter or choose the gateway router which is the next hop for this route. You can provide an IP address or a Networks/Hosts object. In this example **gw-outside1**.
5. In the **Metric** field, enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1. In this example **1**.
6. To monitor route availability, enter or choose the name of an SLA Monitor object that defines the monitoring policy, in the **Route Tracking** field. In this example **sla-outside1**.
7. Click **OK**.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: Outside1

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

Available Network:
- any-ipv4
- gw-outside1
- gw-outside2
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast

Selected Network: any-ipv4

Gateway*: gw-outside1

Metric: 1

(1 - 254)

Tunneled: □ (Used only for default Route)

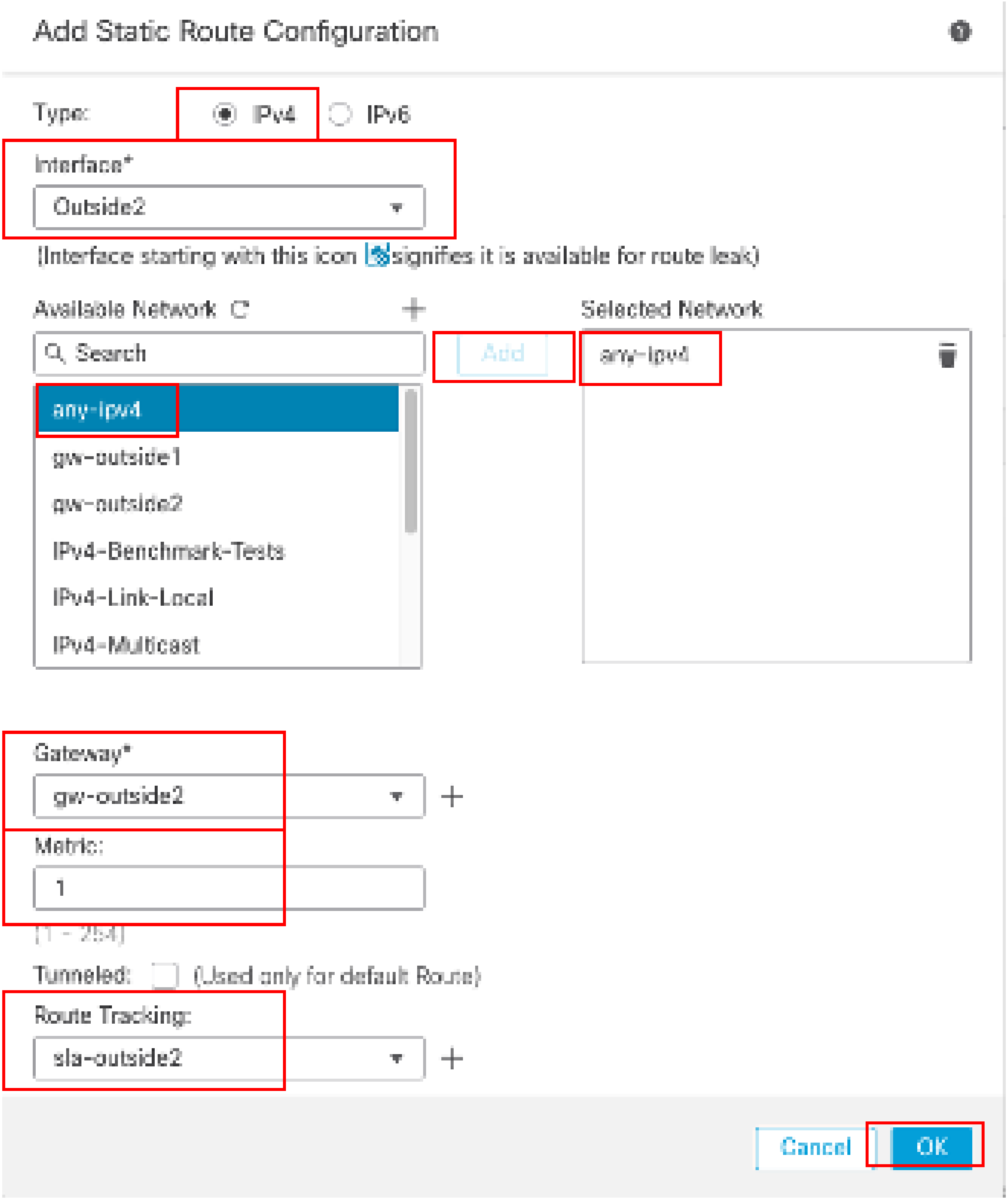
Route Tracking: sla-outside1

Add Static Route First ISP

Repeat similar steps to add the default route to second ISP gateway. In the **Add Static Route Configuration** window:

1. Click **IPv4** or **IPv6** depending on the type of static route that you are adding. In this example **IPv4**.
2. Choose the **Interface** to which this static route applies. In this example Outside2.
3. In the **Available Network** list, choose the destination network. In this example **any-ipv4**.

4. In the **Gateway** or **IPv6 Gateway** field, enter or choose the gateway router which is the next hop for this route. You can provide an IP address or a Networks/Hosts object. In this example **gw-outside2**.
5. In the **Metric** field, enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1. Ensure to specify same metric as the first route, in this example **1**.
6. To monitor route availability, enter or choose the name of an SLA Monitor object that defines the monitoring policy, in the **Route Tracking** field. In this example **sla-outside2**.
7. Click **OK**.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: Outside2

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

Available Network: any-ipv4, gw-outside1, gw-outside2, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast

Selected Network: any-ipv4

Gateway*: gw-outside2

Metric: 1

(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking: sla-outside2

Add Static Route Second ISP

Click **Save** and **Deploy** the configuration.

Verify

Log into the CLI of the FTD, run the command **show zone** to check information about ECMP traffic zones, including the interfaces that are part of each zone.

<#root>

```
> show zone
Zone: Outside ecmp
Security-level: 0

Zone member(s): 2



Outside2 GigabitEthernet0/1



Outside1 GigabitEthernet0/0
```

Run the command show running-config route to check the running configuration for the routing configuration, in this case there are two static routes with route tracks.

<#root>

```
> show running-config route

route Outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1



route Outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2
```

Run the command show route to check the routing table, in this case there are two default routes are via the interface outside1 and outside2 with equal cost, traffic can be distributed between two ISP circuits.

<#root>

```
> 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 10.1.2.2 to network 0.0.0.0


S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2
```

```
                   [1/0] via 10.1.1.2, Outside1

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Run the command **show sla monitor configuration** to check the configuration of the SLA monitor.

<#root>

```
> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1
Owner:
Tag:

Type of operation to perform: echo


Target address: 10.1.1.2


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:

Entry number: 2
Owner:
Tag:

Type of operation to perform: echo


Target address: 10.1.2.2


Interface: Outside2


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:
```

Run the command `show sla monitor operational-state` to confirm the state of the SLA Monitor. In this case you can find “**Timeout occurred: FALSE**” in the command output, it indicates that the ICMP echo to the gateway is replying, so the default route through target interface is active and installed in routing table.

<#root>

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
```

```
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

Load Balancing

Initial traffic through FTD to verify if ECMP load balance the traffic among the gateways in ECMP zone. In this case, initiate telnet connection from Inside-Host1 (10.1.3.2) and Inside-Host2 (10.1.3.4) towards Internet-Host (10.1.5.2), run the command **show conn** to confirm that the traffic is load-balanced between two ISP links, Inside-Host1 (10.1.3.2) goes through interface outside1, Inside-Host2 (10.1.3.4) goes through interface outside2.

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, flags UIO N1
```

Note: Traffic is load balanced among the specified gateways based on an algorithm that hashes the source and destination IP addresses, incoming interface, protocol, source and destination ports. when you run the test, the traffic you simulate can be routed to the same gateway due to the hash algorithm, this is expected, change any value among the 6 tuples (source IP, Destination IP, incoming interface, protocol, source port, destination port) to make change on the hash result.

Lost Route

If the link to the first ISP Gateway is down, in this case, shut down the first gateway router to simulate. If the FTD does not receive an echo reply from first ISP gateway within the threshold timer specified in the SLA Monitor object, the host is considered unreachable and marked as down. Tracked route to first gateway is also removed from routing table.

Run the command `show sla monitor operational-state` to confirm the current state of the SLA Monitor. In this case you can find “Timeout occurred: True” in the command output, it indicates that the ICMP echo to the first ISP gateway is not responding.

<#root>

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: TRUE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

Run the command **show route** to check the current routing table, the route to the first ISP gateway through interface outside1 is removed, there is only one active default route to the second ISP gateway through interface outside2.

<#root>

```
> 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 10.1.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2


C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

Run the command `show conn` , you can find the two connections are still up. telnet sessions are also active on Inside-Host1 (10.1.3.2) and Inside-Host2 (10.1.3.4) without any interruption.

<#root>

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect


TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1



TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```

Note: You can notice in the output of show conn , telnet session from Inside-Host1 (10.1.3.2) is still through interface outside1, although the default route through interface outside1 has been removed from routing table. this is expected and by design, the actual traffic flows through interface outside2. If you initiate new connection from Inside-Host1 (10.1.3.2) to Internet-Host (10.1.5.2), you can find all the traffic are through interface outside2.

Troubleshoot

In order to validate the routing table change, run command debug ip routing.

In this example, when the link to first ISP gateway is down, the route through interface outside1 is removed from routing table.

<#root>

```
> debug ip routing
IP routing debugging is on
```

```
RT: ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, Outside1

ha_cluster_synced 0 routetype 0

RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0



RT(mgmt-only): NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2



NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2
```

Run the command `show route` to confirm the current routing table.

<#root>

```
> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```

When the link to first ISP gateway is up again, the route through interface outside1 is added back to routing table.

<#root>

```
> debug ip routing
IP routing debugging is on

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, Outside2



NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, Outside2
```

```
NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, Outside2

 via 10.1.1.2, Outside1
```

Run the command `show route` to confirm the current routing table.

<#root>

```
> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, Outside2

                   [1/0] via 10.1.1.2, Outside1

C 10.1.1.0 255.255.255.0 is directly connected, Outside1
L 10.1.1.1 255.255.255.255 is directly connected, Outside1
C 10.1.2.0 255.255.255.0 is directly connected, Outside2
L 10.1.2.1 255.255.255.255 is directly connected, Outside2
C 10.1.3.0 255.255.255.0 is directly connected, Inside
L 10.1.3.1 255.255.255.255 is directly connected, Inside
```