在FMC管理的FTD上設定ECMP與IP SLA

目錄

簡介

本檔案介紹如何在由FMC管理的FTD上設定ECMP與IP SLA。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦(FTD)上的ECMP配置
- 思科安全防火牆威脅防禦(FTD)上的IP SLA配置
- 思科安全防火牆管理中心(FMC)

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- Cisco FTD版本7.4.1
- Cisco FMC版本7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本檔案介紹如何在由思科FMC管理的思科FTD上設定等價多重路徑(ECMP)以及網際網路通訊協定服務等級協定(IP SLA)。 ECMP允許您在FTD上將介面組成群組，並在多個介面之間平衡流量負載。 IP SLA是一種透過交換常規資料包來監控端到端連線的機制。IP SLA可與ECMP一起實施，以確保下一跳的可用性。 在本例中，ECMP用於在兩個Internet服務提供商(ISP)電路上平均分配資料包。同時，IP SLA會跟蹤連線，確保在出現故障時能夠無縫過渡到任何可用電路。

本文檔的特定要求包括：

- 使用具有管理員許可權的使用者帳戶訪問裝置
- 思科安全防火牆威脅防禦7.1版或更高版本

- Cisco Secure Firewall Management Center 7.1或更高版本

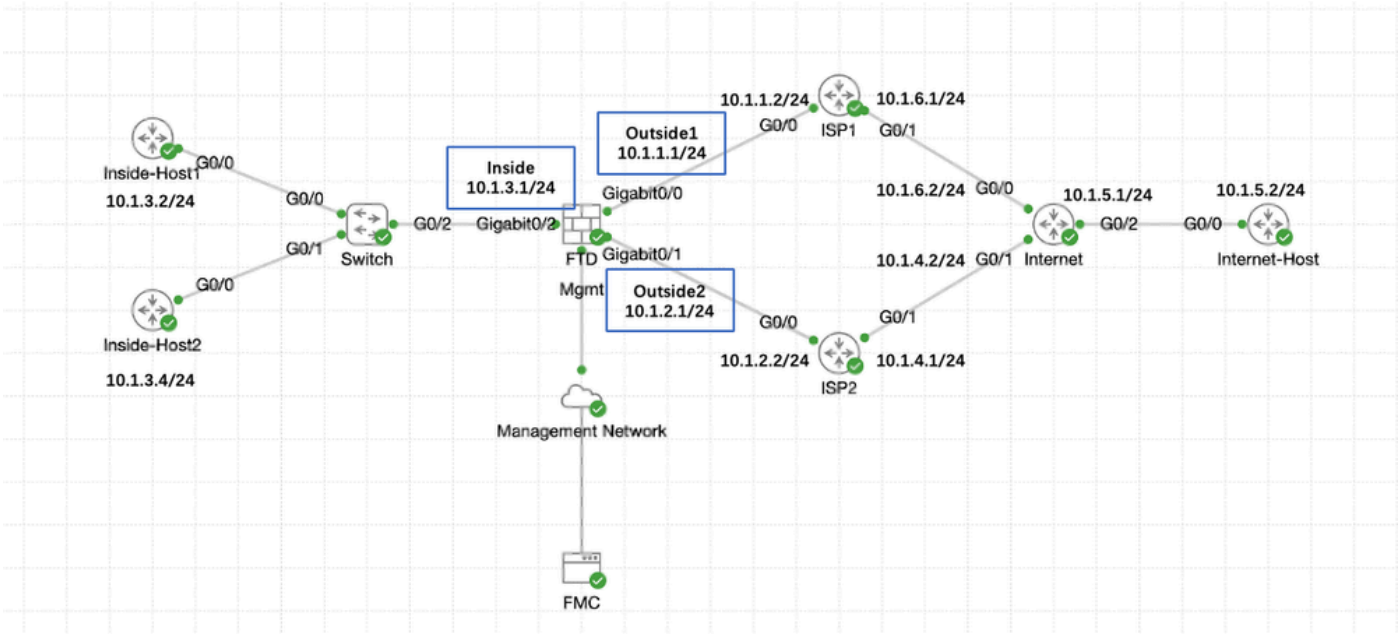
設定

網路圖表

在本例中，Cisco FTD有兩個外部介面：outside1和outside2。每個連線到ISP網關的outside1和outside2屬於名為outside的相同ECMP區域。

來自內部網路的流量會透過FTD進行路由，並透過兩個ISP將負載均衡到網際網路。

同時，FTD使用IP SLA來監控與每個ISP閘道的連線。如果任何ISP電路出現故障，FTD會故障切換到另一個ISP網關以維持業務連續性。

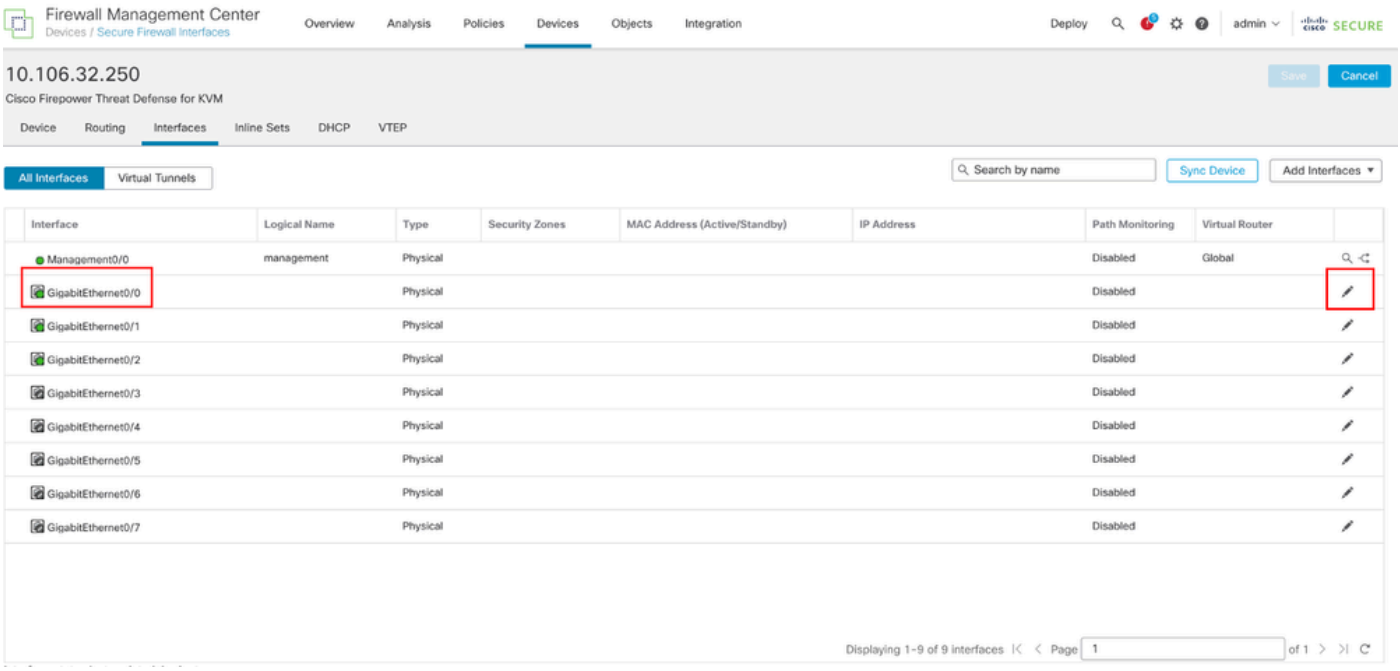


網路圖表

組態

步驟 0.預配置介面/網路對象

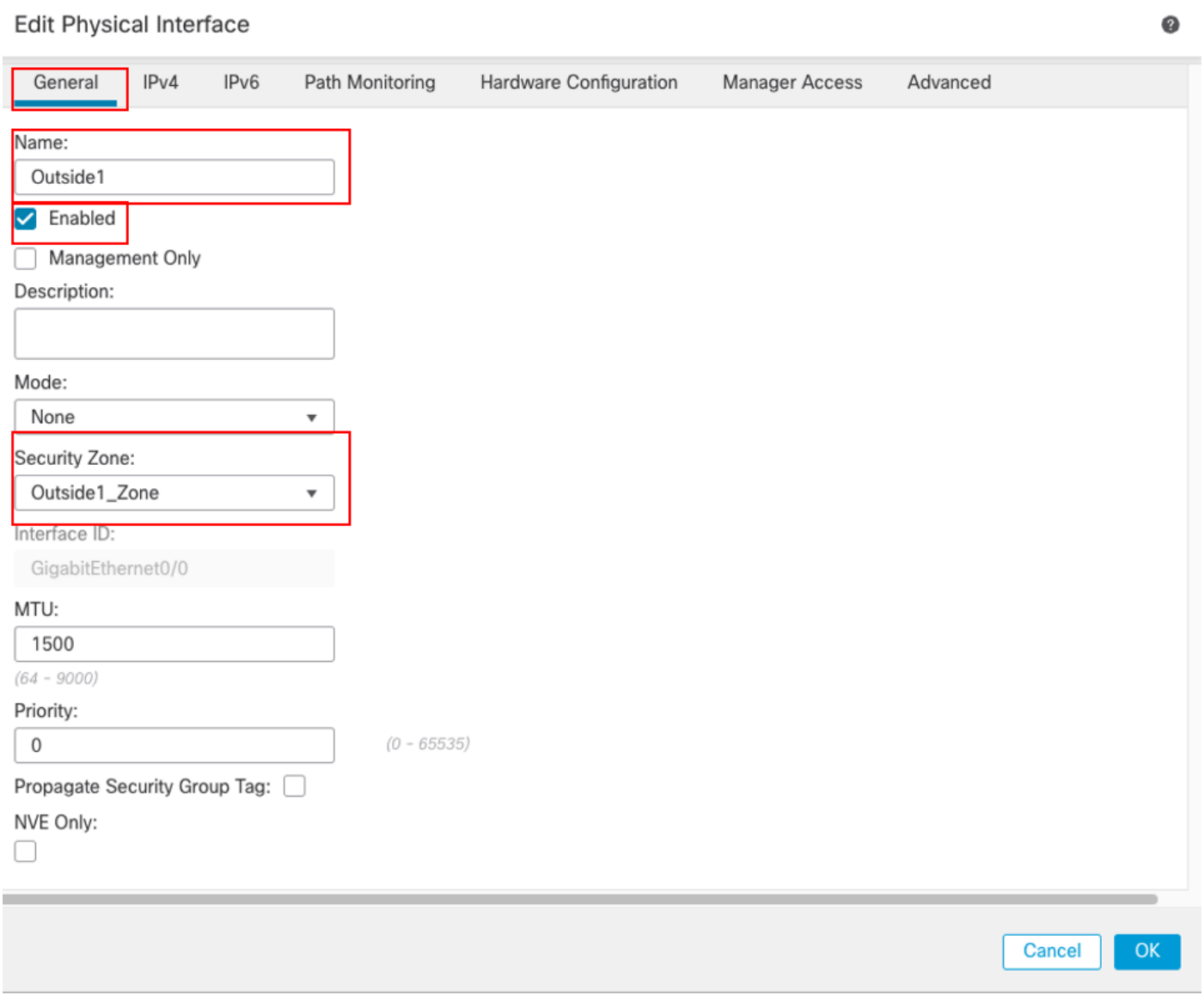
登入FMC Web GUI，選擇Devices > Device Management，然後為威脅防禦裝置點選Edit按鈕。預設情況下，Interfaces頁處於選中狀態。按一下要編輯的介面的Edit按鈕，在此示例中為GigabitEthernet0/0。



編輯介面Gi0/0

在Edit Physical Interface窗口的General頁籤下：

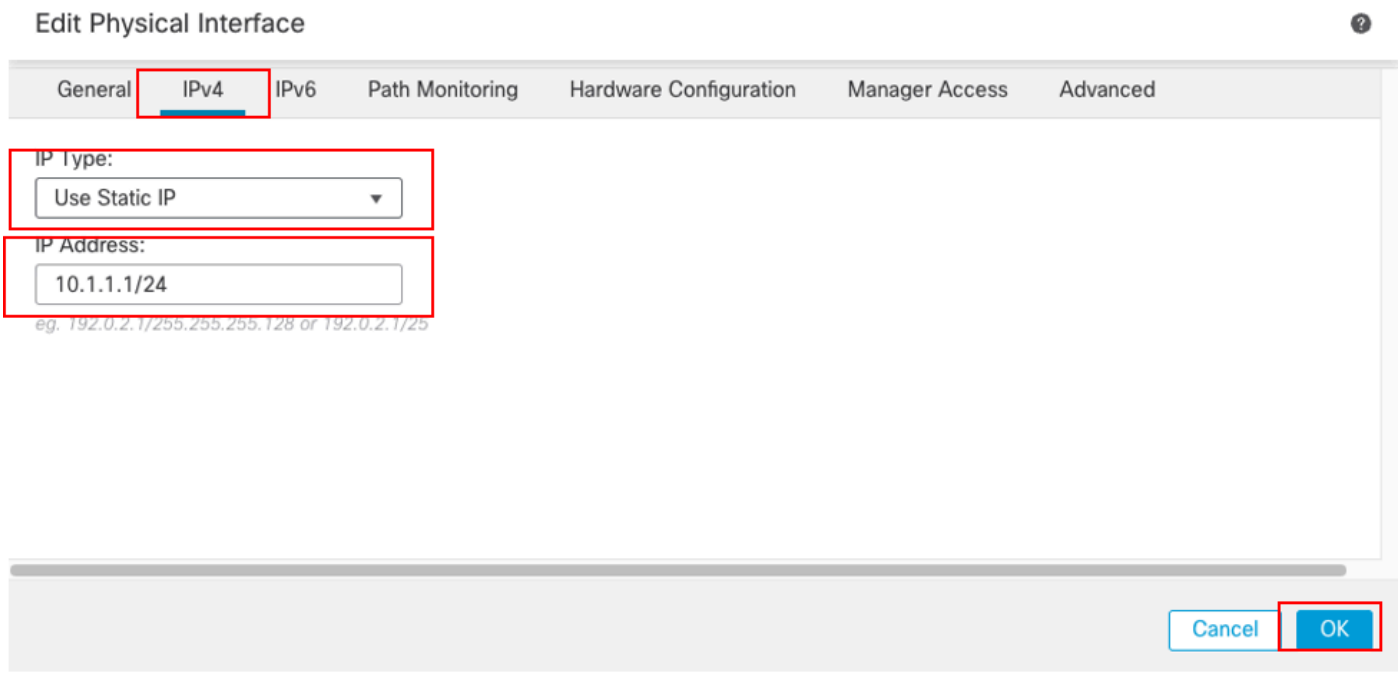
1. 設定Name，在本例中為Outside1。
2. 透過選中Enabled覈取方塊啟用介面。
3. 在安全區域下拉選單中，選擇現有安全區域或建立新區域，在本示例中為Outside1_Zone。



介面Gi0/0常規

在IPv4頁籤下：

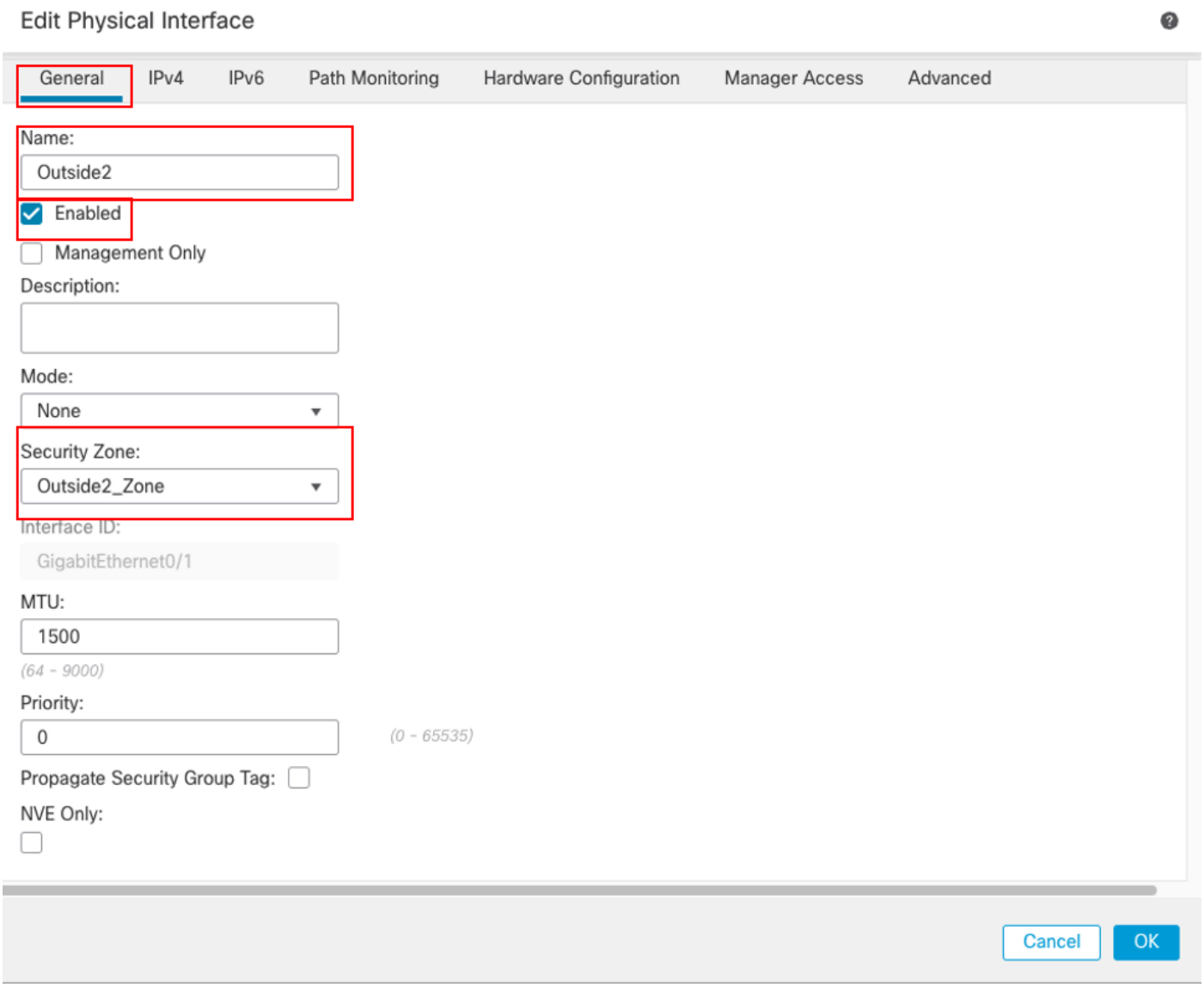
1. 從IP Type下拉選單中選擇其中一個選項，在本示例中為Use Static IP。
2. 設定IP地址，在此示例中為10.1.1.1/24。
3. 按一下「OK」（確定）。



介面Gi0/0 IPv4

在Edit Physical Interface窗口的General頁籤下重複類似步驟配置介面GigabitEthernet0/1：

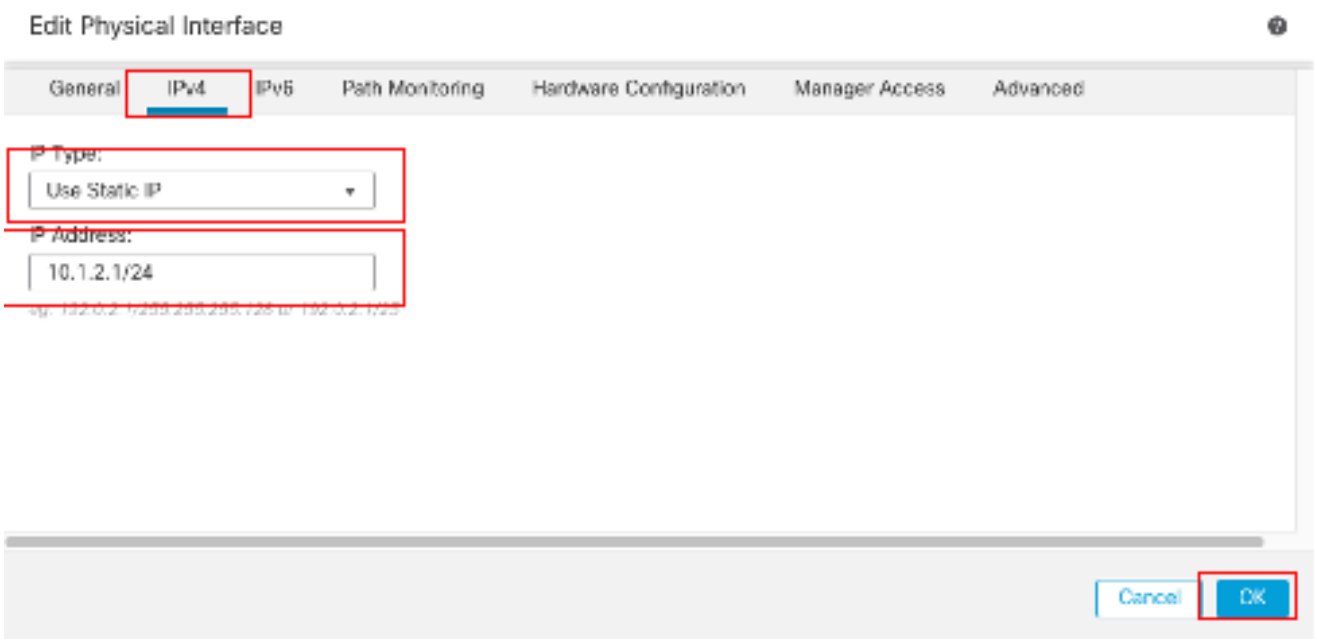
1. 設定Name，在本例中為Outside2。
2. 透過選中Enabled覈取方塊啟用介面。
3. 在安全區域下拉選單中，選擇現有安全區域或建立新區域，在本示例中為Outside2_Zone。



介面Gi0/1常規

在IPv4頁籤下：

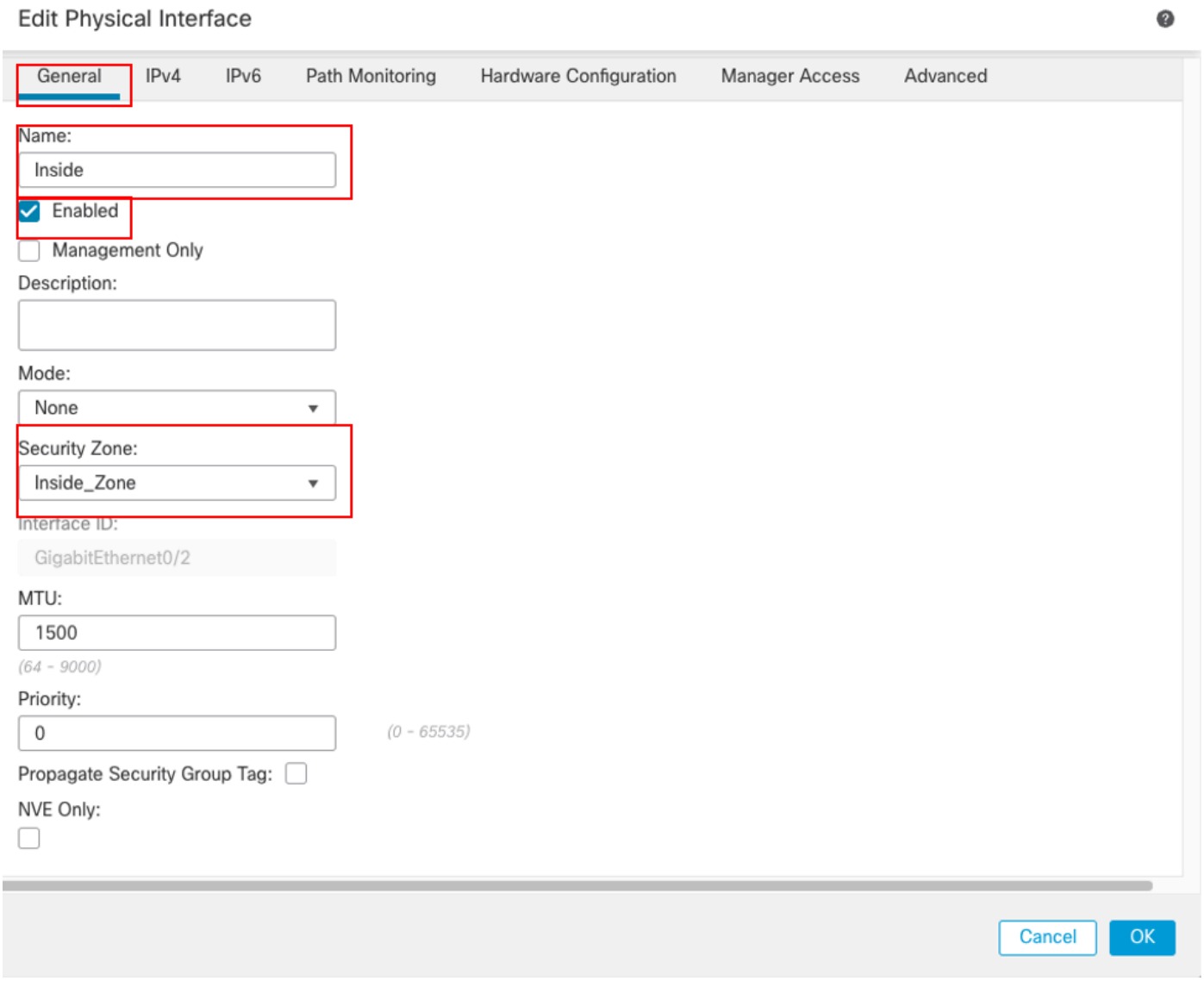
1. 從IP Type下拉選單中選擇其中一個選項，在本示例中為Use Static IP。
2. 設定IP地址，在此示例中為10.1.2.1/24。
3. 按一下「OK」（確定）。



介面Gi0/1 IPv4

在Edit Physical Interface窗口的General頁籤下重複類似步驟配置介面GigabitEthernet0/2：

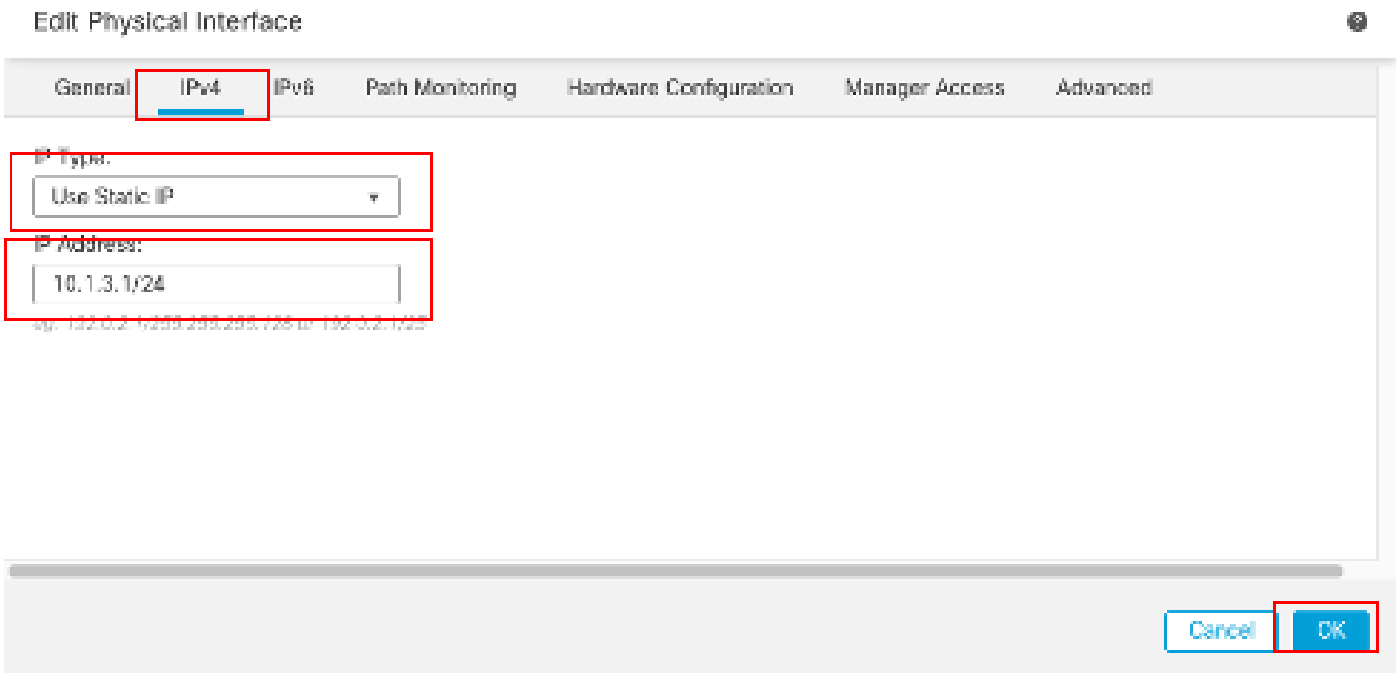
1. 設定Name，在此例中為Inside。
2. 透過選中Enabled覈取方塊啟用介面。
3. 在安全區域下拉選單中，選擇現有安全區域或建立新區域，在本示例中為Inside_Zone。



介面Gi0/2常規

在IPv4頁籤下：

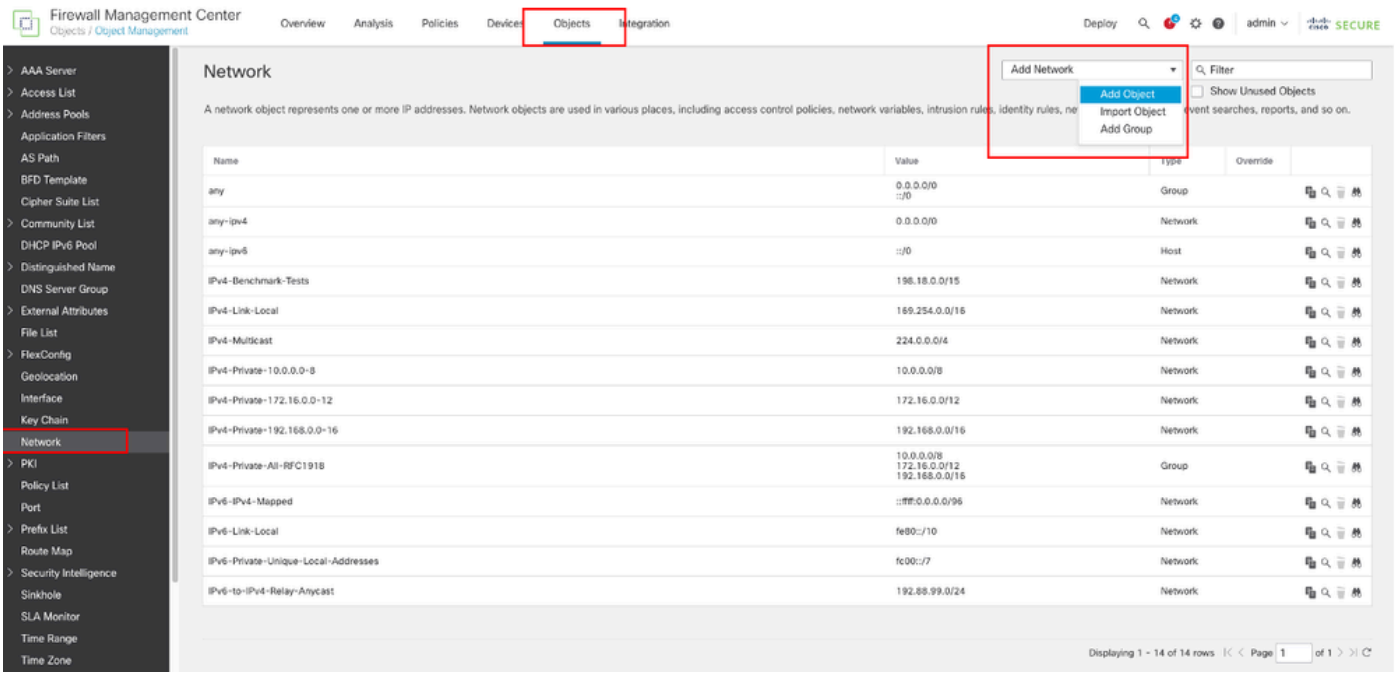
1. 從IP Type下拉選單中選擇其中一個選項，在本示例中為Use Static IP。
2. 設定IP地址，在此示例中為10.1.3.1/24。
3. 按一下「OK」（確定）。



介面Gi0/2 IPv4

按一下Save和Deploy配置。

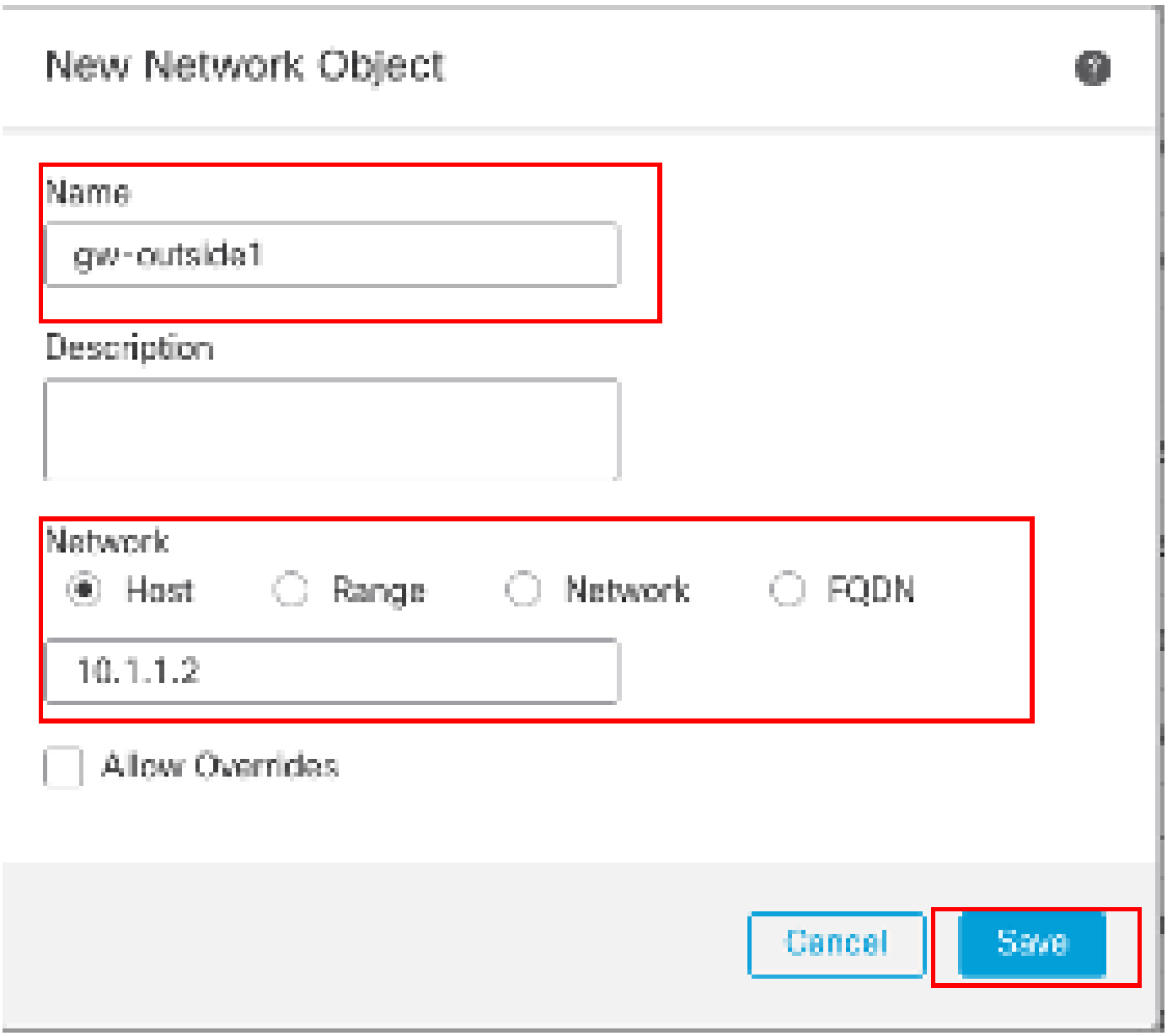
導航到對象>對象管理，從對象型別清單中選擇Network，從Add Network下拉選單中選擇Add Object為第一個ISP網關建立對象。



網路物件

在New Network Object窗口中：

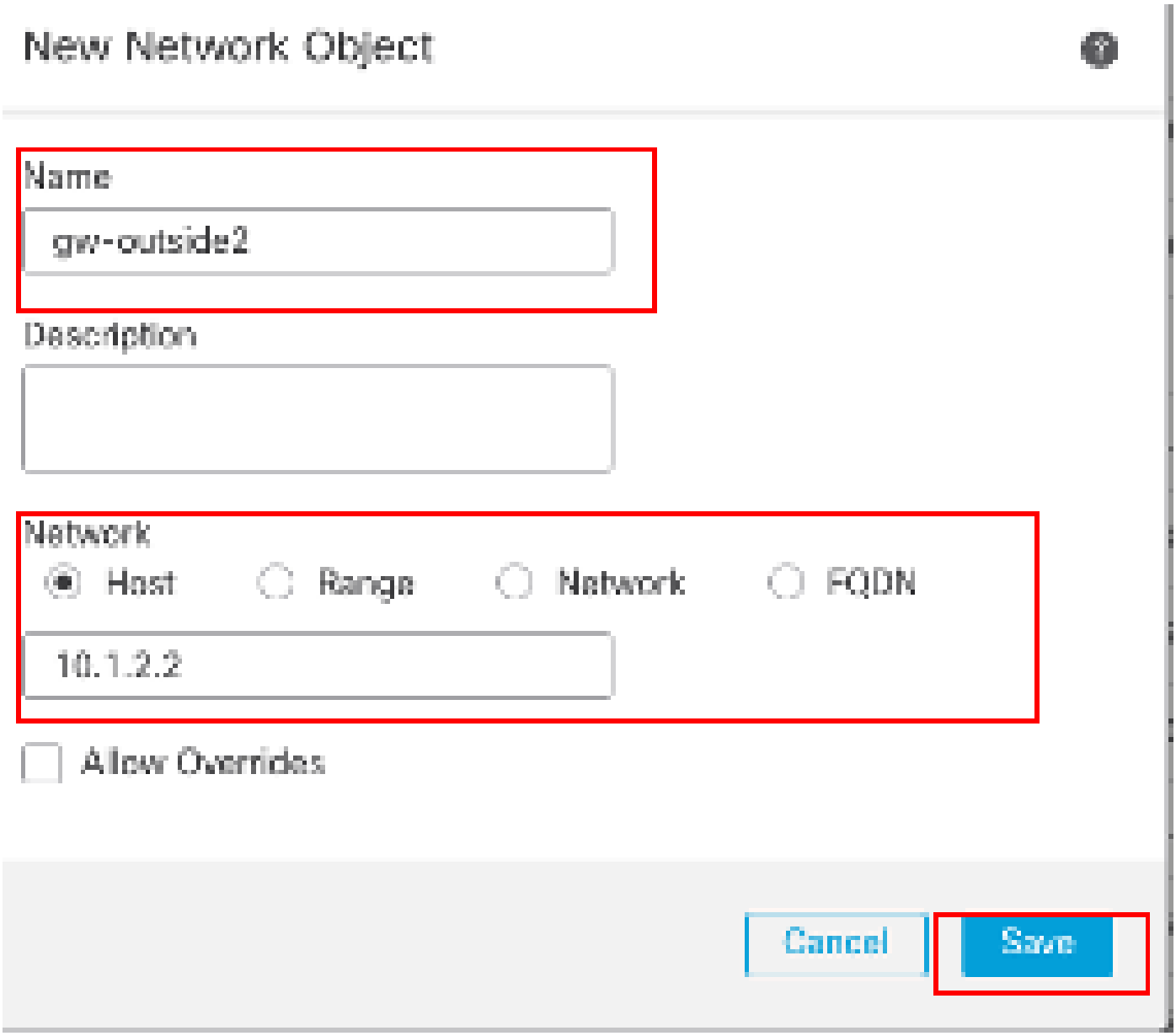
1. 設定Name，在此示例中為gw-outside1。
2. 在網路欄位中，選擇所需的選項並輸入適當的值，在本示例中為主機和10.1.1.2。
3. 按一下Save。



對象Gw-outside1

重複類似步驟，為第二個ISP網關建立另一個對象。在New Network Object窗口中：

1. 設定Name，在此示例中為gw-outside2。
2. 在網路欄位中，選擇所需的選項並輸入適當的值，在本示例中為主機和10.1.2.2。
3. 按一下Save。

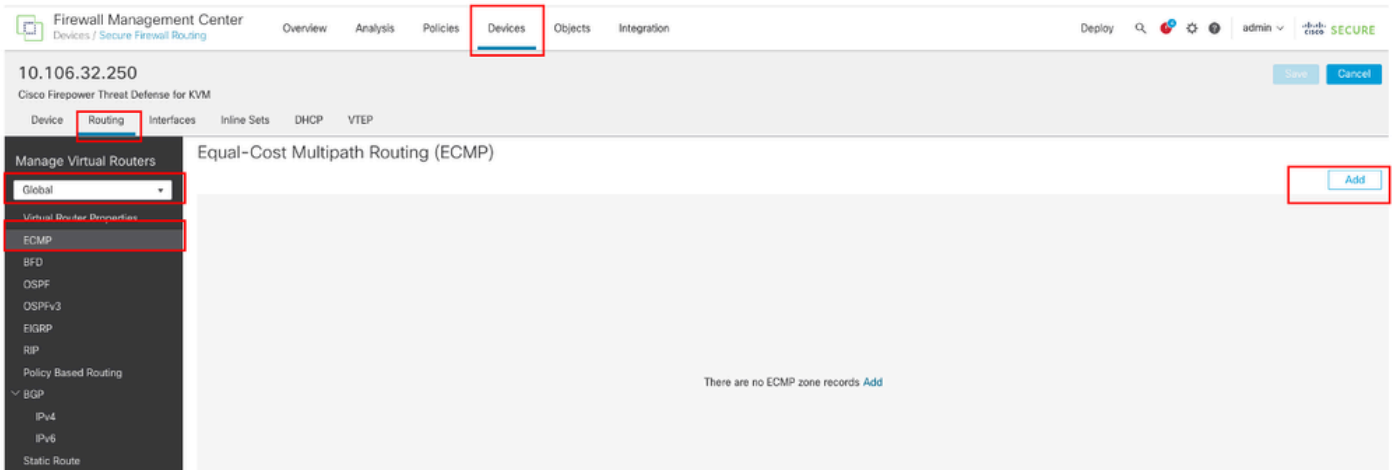


對象Gw-outside2

步驟 1.配置ECMP區域

導航到裝置 > 裝置管理並編輯威脅防禦裝置，點選路由。從virtual router下拉選單中選擇要在其中建立ECMP區域的虛擬路由器。您可以在全局虛擬路由器和使用者定義的虛擬路由器中建立ECMP區域。本示例中選擇Global。

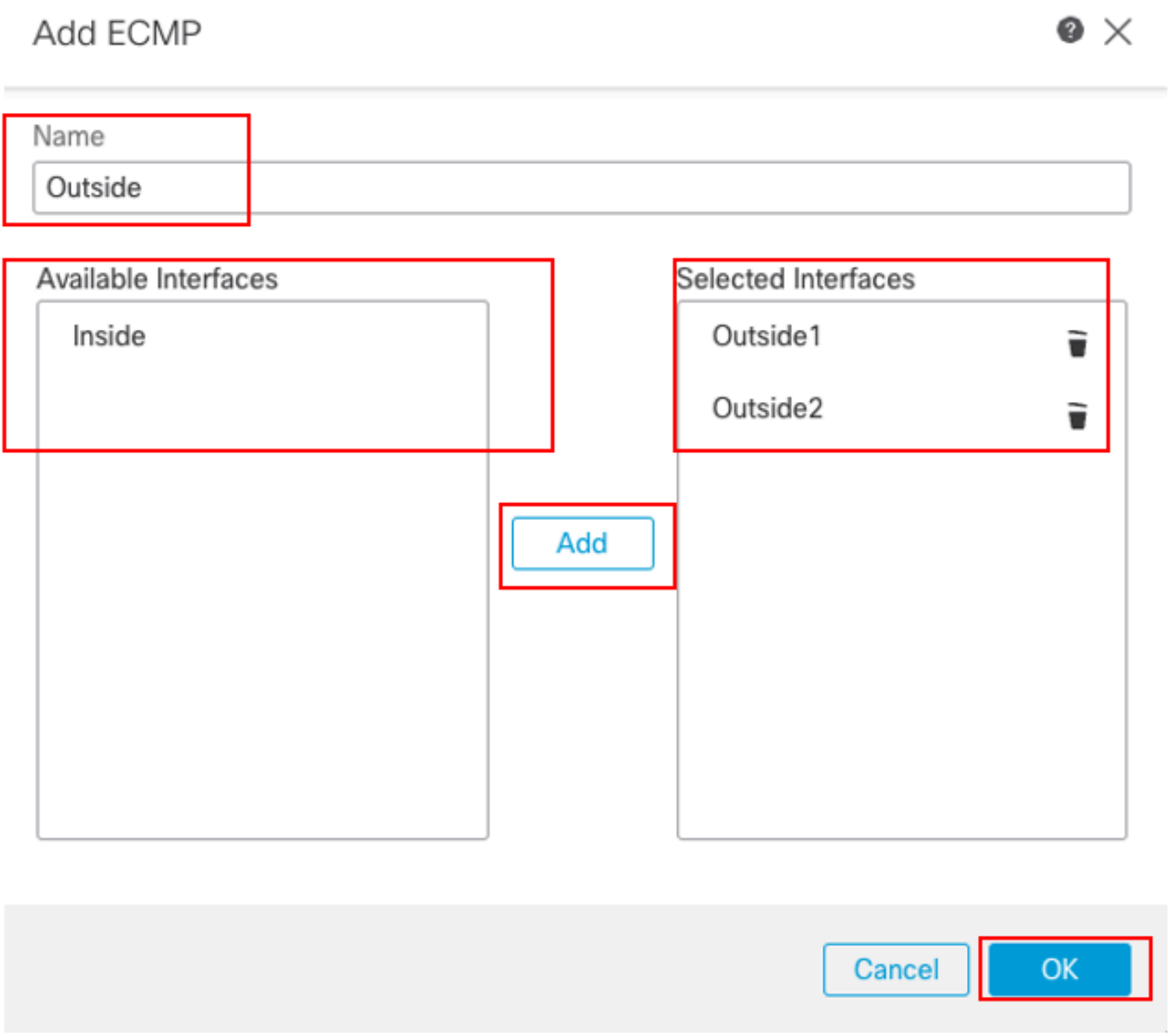
按一下ECMP，然後按一下Add。



配置ECMP區域

在Add ECMP窗口中：

1. 為ECMP區域設定Name，在此示例中為Outside。
2. 要關聯介面，請在Available Interfaces框下選擇介面，然後按一下Add。在本示例中，Outside1和Outside2。
3. 按一下「OK」（確定）。

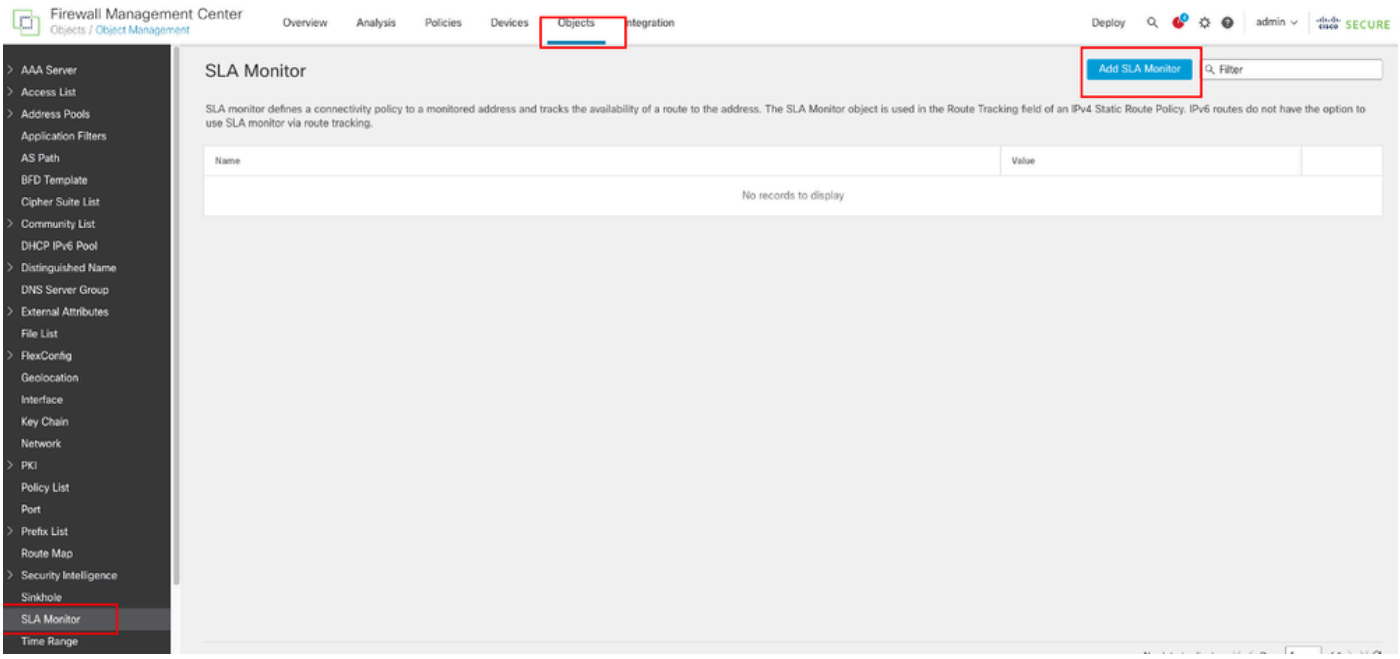


配置外部的ECMP區域

按一下Save和Deploy配置。

步驟 2.配置IP SLA對象

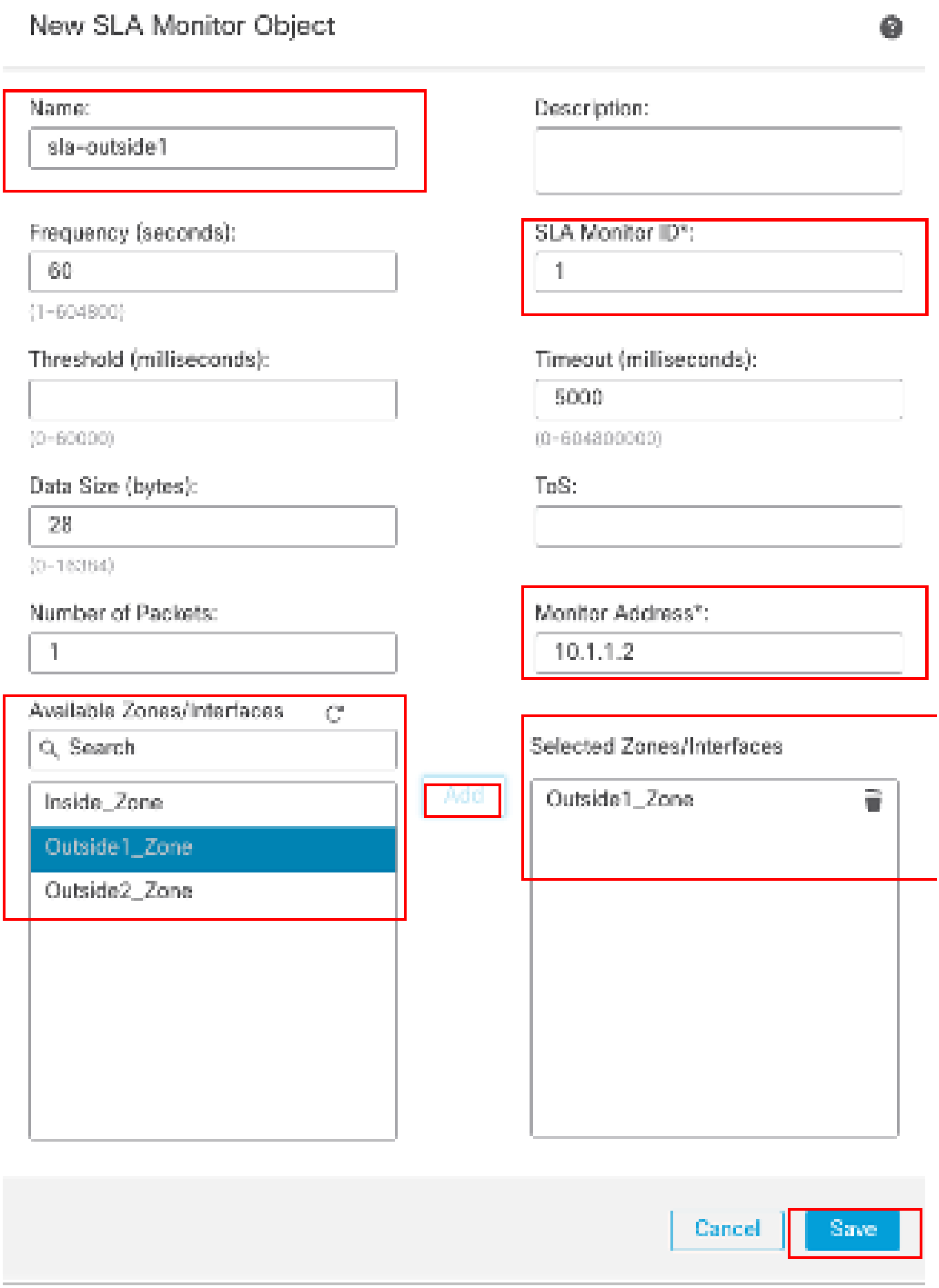
導航到對象 > 對象管理，從對象型別清單中選擇SLA監控，點選增加SLA監控，為第一個ISP網關增加新的SLA監控。



建立SLA監控器

在「新建SLA監控器對象」窗口中：

1. 為SLA監控對象設定Name，在此例中為sla-outside1。
2. 在SLA Monitor ID欄位中輸入SLA操作的ID號。值範圍從1到2147483647。您最多可以在裝置上建立2000個SLA操作。每個ID號對於策略和裝置配置必須是唯一的。在本示例1中。
3. 在Monitored Address欄位中，輸入SLA操作正在監控的可用性的IP地址。在本示例中，10.1.1.2。
4. Available Zones/Interfaces清單可同時顯示區域和介面組。在Zones/Interfaces清單中，增加包含裝置與管理站通訊所用介面的區域或介面組。要指定單個介面，需要為該介面建立一個區域或介面組。在本示例中，Outside1_Zone。
5. 按一下Save。

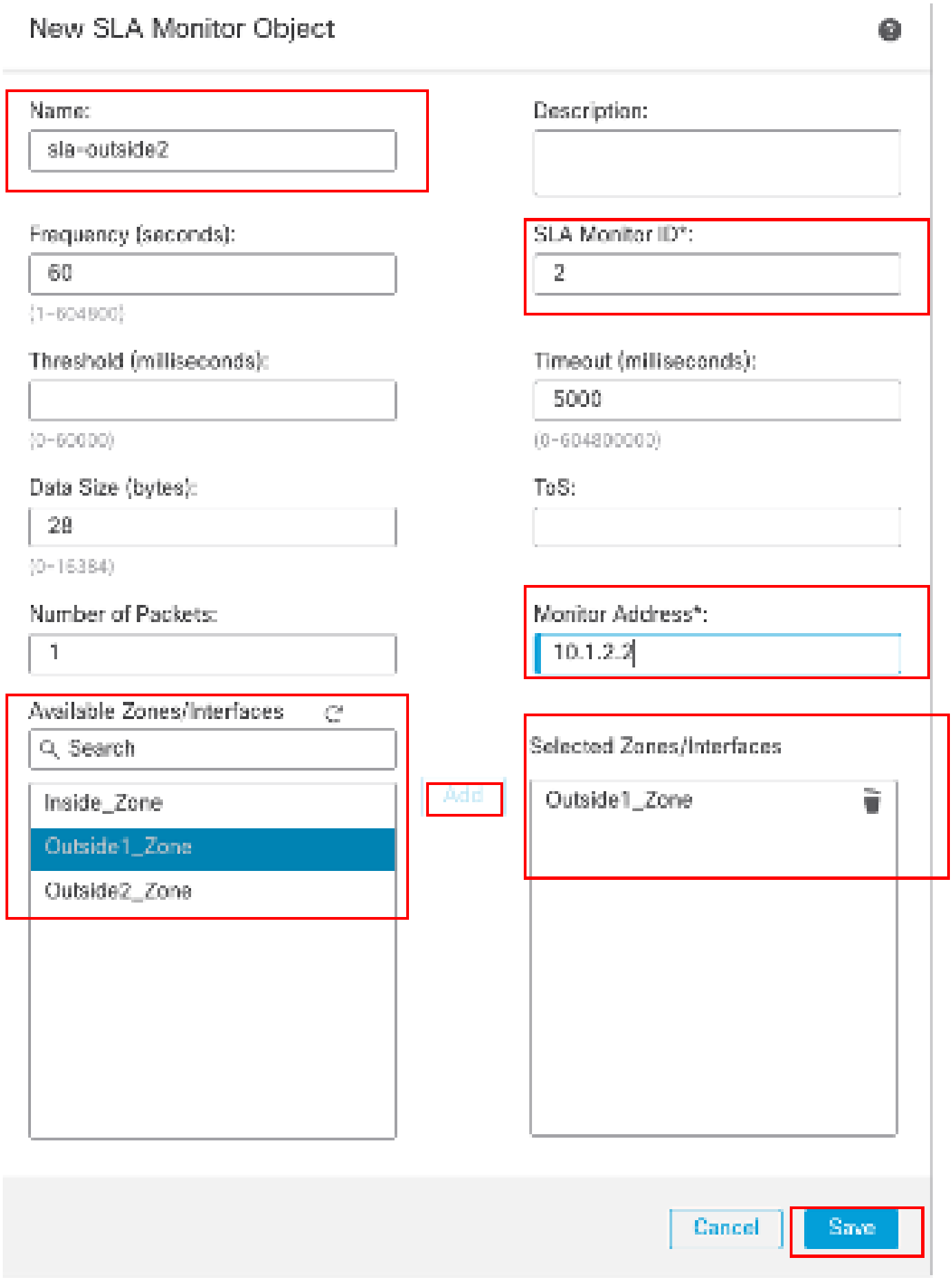


SLA對象Sla-outside1

重複類似步驟，為第二個ISP網關建立另一個SLA監控器。

在「新建SLA監控器對象」窗口中：

1. 為SLA監控對象設定Name，在此例中為sla-outside2。
2. 在SLA Monitor ID欄位中輸入SLA操作的ID號。值範圍從1到2147483647。您最多可以在裝置上建立2000個SLA操作。每個ID號對於策略和裝置配置必須是唯一的。在本示例2中。
3. 在Monitored Address欄位中，輸入SLA操作正在監控的可用性的IP地址。在本示例中，10.1.2.2。
4. Available Zones/Interfaces清單可同時顯示區域和介面組。在Zones/Interfaces清單中，增加包含裝置與管理站通訊所用介面的區域或介面組。要指定單個介面，需要為該介面建立一個區域或介面組。在本示例中，Outside2_Zone。
5. 按一下Save。

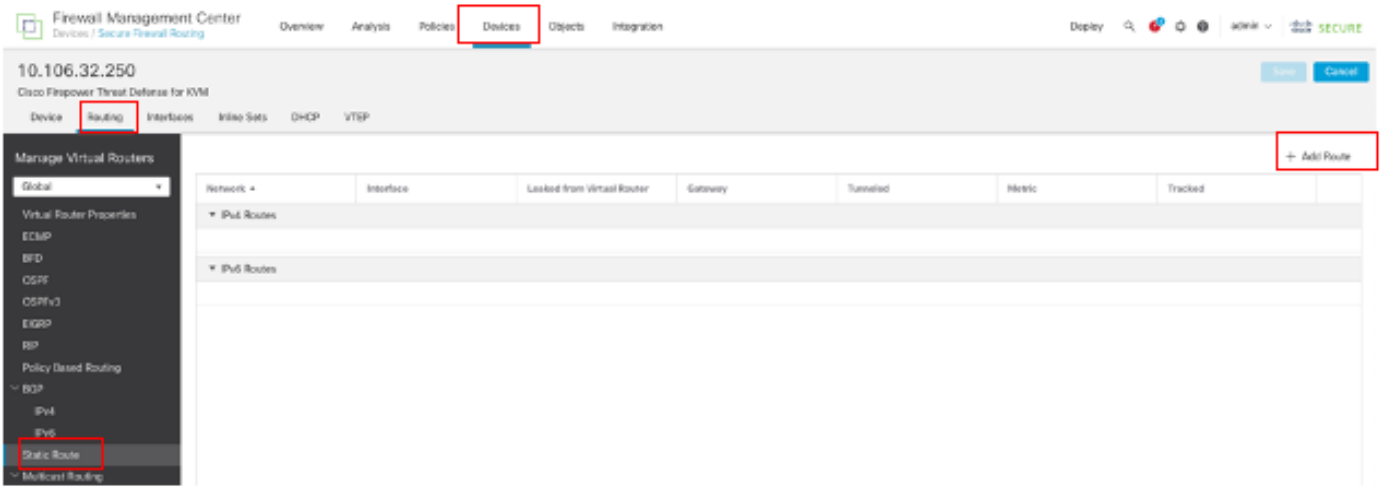


SLA對象Sla-outside2

步驟 3.使用路由跟蹤配置靜態路由

導航到裝置 > 裝置管理，然後編輯威脅防禦裝置，點選路由，從虛擬路由器下拉選單中選擇要為其配置靜態路由的虛擬路由器。在本示例中，Global。

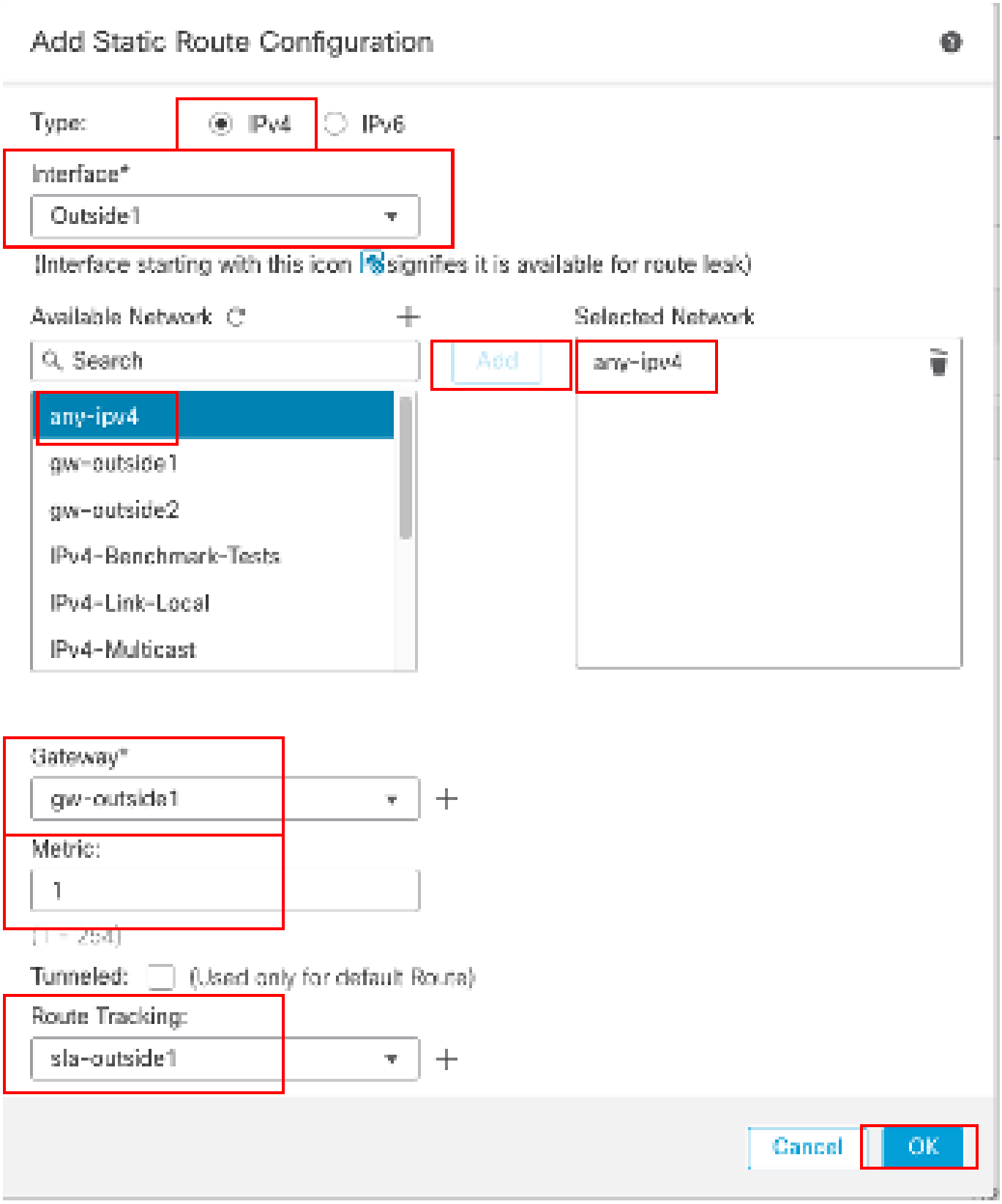
選擇Static Route，點選Add Route，將預設路由增加到第一個ISP網關。



配置靜態路由

在Add Static Route Configuration 窗口中：

1. 根據所增加的靜態路由型別，按一下IPv4或IPv6。在本示例中，IPv4。
2. 選擇此靜態路由所應用的介面。在本示例中，Outside1。
3. 在Available Network清單中，選擇目的網路。在本示例中，any-ipv4。
4. 在Gateway或IPv6 Gateway欄位中，輸入或選擇作為此路由的下一跳的網關路由器。您可以提供IP地址或網路/主機對象。在本示例中，gw-outside1。
5. 在Metric欄位中，輸入到達目標網路的跳數。有效值範圍為1至255；預設值為1。在本示例1中。
6. 要監控路由可用性，請在路由跟蹤欄位中輸入或選擇用於定義監控策略的SLA監控對象名稱。在本示例中，sla-outside1。
7. 按一下「OK」（確定）。



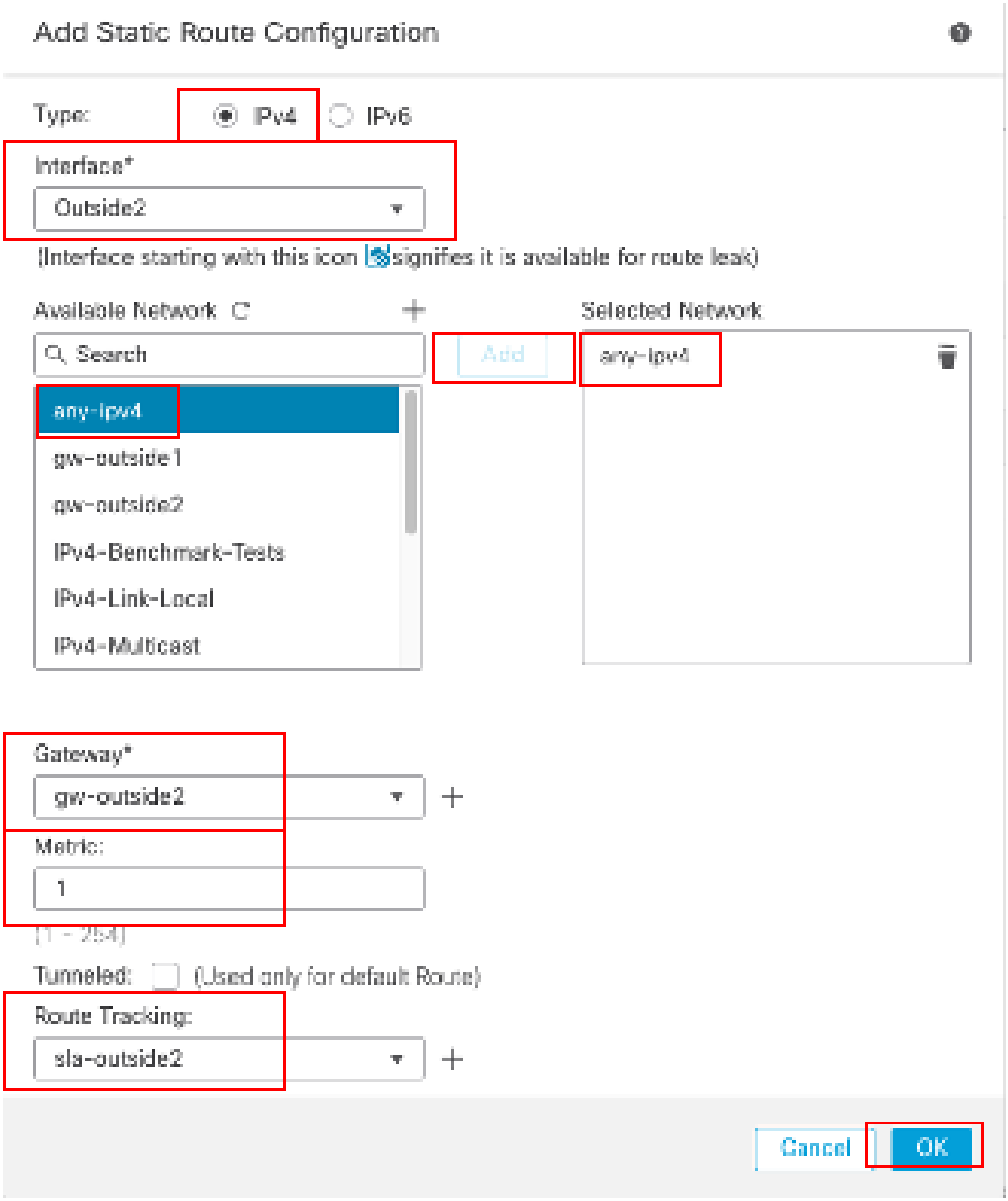
增加靜態路由第一個ISP

重複類似步驟，將預設路由增加到第二個ISP網關。在Add Static Route Configuration 窗口中：

1. 根據所增加的靜態路由型別，按一下IPv4或IPv6。在本示例中，IPv4。
2. 選擇此靜態路由所應用的介面。在本例中，Outside2。
3. 在Available Network清單中，選擇目的網路。在本示例中，any-ipv4。
4. 在Gateway或IPv6 Gateway欄位中，輸入或選擇作為此路由的下一跳的網關路由器。您可以

提供IP地址或網路/主機對象。在本示例中，gw-outside2。

5. 在Metric欄位中，輸入到達目標網路的跳數。有效值範圍為1至255；預設值為1。確保指定與第一個路由相同的度量，在此示例中為1。
6. 要監控路由可用性，請在路由跟蹤欄位中輸入或選擇用於定義監控策略的SLA監控對象名稱。在本示例中，sla-outside2。
7. 按一下「OK」（確定）。



增加第二個ISP靜態路由

按一下Save和Deploy配置。

驗證

登入FTD的CLI，運行命令 **show zone** 以檢查有關ECMP流量區域的資訊，包括屬於每個區域的介面。

```
<#root>

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

Zone member(s): 2

Outside2 GigabitEthernet0/1

Outside1 GigabitEthernet0/0
```

運行show running-config route命令以檢查正在運行的路由配置配置，在這種情況下，存在兩條帶有路由跟蹤的靜態路由。

```
<#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

運行show route命令檢查路由表，如果有兩個預設路由是透過outside1和outside2介面且開銷相等，則流量可以在兩個ISP電路之間分配。

<#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
```

運行 **show sla monitor configuration** 命令以檢查SLA監控器的配置。

<#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:

運行命令show sla monitor operational-state以確認SLA監控器的狀態。在這種情況下，您可以在命令輸出中找到「**Timeout occurred：FALSE**」，表示網關的ICMP響應正在應答，因此透過目標介面的預設路由處於活動狀態並安裝在路由表中。

<#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:
```

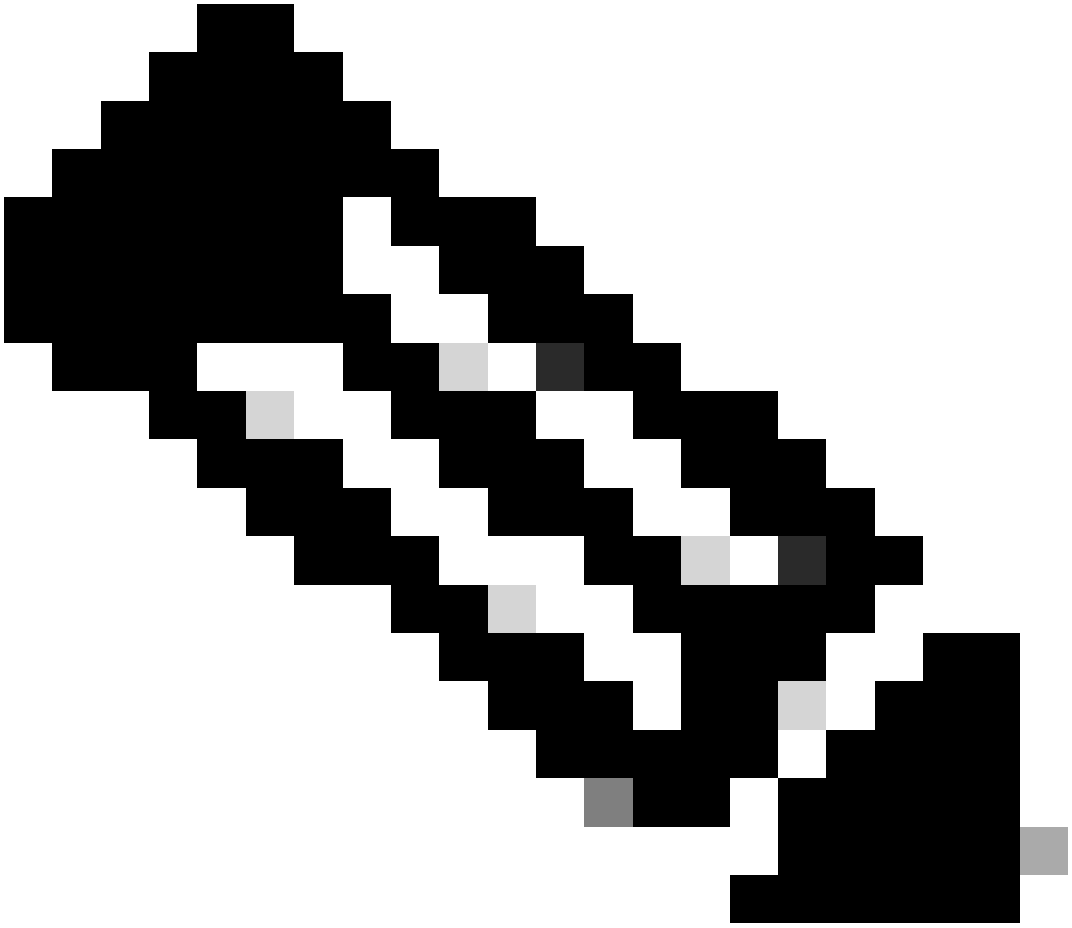
```
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

負載平衡

透過FTD的初始流量，以驗證ECMP是否在ECMP區域中的網關之間對流量進行負載均衡。在這種情況下，起始從Inside-Host1 (10.1.3.2)和Inside-Host2 (10.1.3.4)到Internet-Host (10.1.5.2)的telnet連線，運行命令 **show conn** 以確認兩個ISP鏈路之間的流量處於負載均衡狀態：Inside-Host1 (10.1.3.2)透過interface outside1，Inside-Host2 (10.1.3.4)透過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
```



注意：系統會根據雜湊來源和目的地IP位址、內送介面、通訊協定、來源和目的地連線埠的演演算法，在指定的閘道之間對流量進行負載平衡。執行測試時，您模擬的流量會因為雜湊演演算法而路由到相同的閘道，這是預期的結果，會變更6個元組（來源IP、目的地IP、內送介面、通訊協定、來源連線埠、目的地連線埠）中的任何值，以變更雜湊結果。

遺失的路由

如果連線到第一個ISP網關的鏈路關閉（在本例中）請關閉要模擬的第一個網關路由器。如果FTD在SLA監控器物件中指定的臨界值計時器內，沒有收到來自第一個ISP閘道的回應回覆，就會將主機視為無法連線並標示為關閉。到第一個網關的跟蹤路由也會從路由表中刪除。

運行show sla monitor operational-state命令以確認SLA監控器的當前狀態。在這種情況下，您可以在命令輸出中找到「Timeout occurred： True」，表示發往第一個ISP網關的ICMP響應沒有響應。

<#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
```

運行 **show route** 命令檢查當前路由表，刪除了透過outside1介面到第一個ISP網關的路由，只有一條透過介面outside2到第二個ISP網關的活動預設路由。

<#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
```

運行show conn命令，您可以看到兩個連線仍處於運行狀態。Telnet會話在Inside-Host1 (10.1.3.2)和Inside-Host2 (10.1.3.4)上也處於活動狀態，不會出現任何中斷。

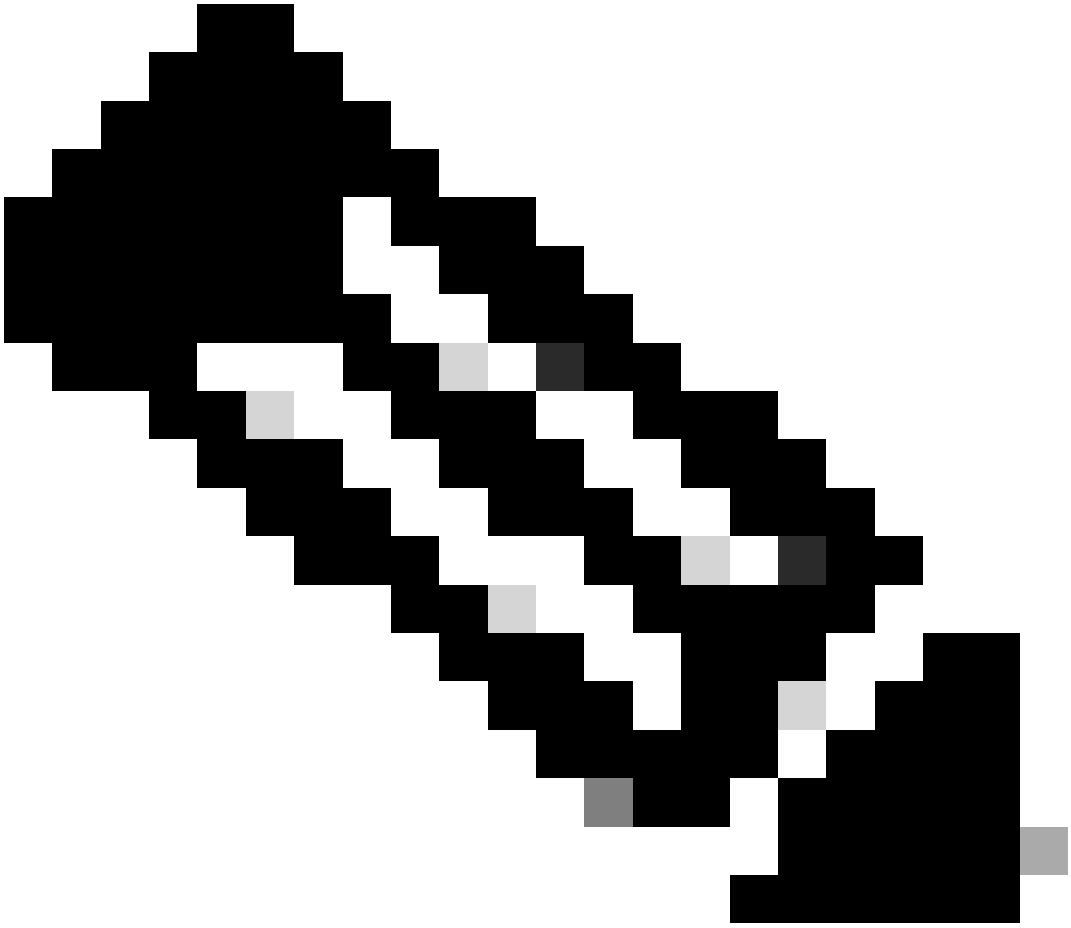
<**#root**>

```
> 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



注意：您可在show conn的輸出中注意到，雖然透過介面outside1的預設路由已從路由表中刪除，但來自Inside-Host1 (10.1.3.2)的telnet會話仍透過interface outside1。這是正常現象，實際流量流經介面outside2。如果啟動從Inside-Host1 (10.1.3.2)到Internet-Host (10.1.5.2)的新連線，則可以發現所有流量都透過interface outside2。

疑難排解

要驗證路由表更改，請運行命令debug ip routing。

在本示例中，當通往第一個ISP網關的鏈路斷開時，透過介面outside1的路由將從路由表中刪除。

<#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
```

運行命令show route以確認當前路由表。

<#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
```

當通往第一個ISP網關的鏈路再次接通時，透過介面outside1的路由將增加迴路由表。

<#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

運行命令show route以確認當前路由表。

<#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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。