

# 在FDM管理的FTD上使用IP SLA設定ECMP

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

#### [背景資訊](#)

### [設定](#)

#### [網路圖表](#)

#### [組態](#)

##### [步驟 0.預配置介面/對象](#)

##### [步驟 1.配置ECMP區域](#)

##### [步驟 2.配置IP SLA對象](#)

##### [步驟 3.使用路由跟蹤配置靜態路由](#)

### [驗證](#)

#### [負載平衡](#)

#### [遺失的路由](#)

### [疑難排解](#)

### [相關資訊](#)

---

## 簡介

本檔案將說明如何在FDM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
- 思科安全防火牆裝置管理員(FDM)

### 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 ( 內部版本172 )

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Cisco FDM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

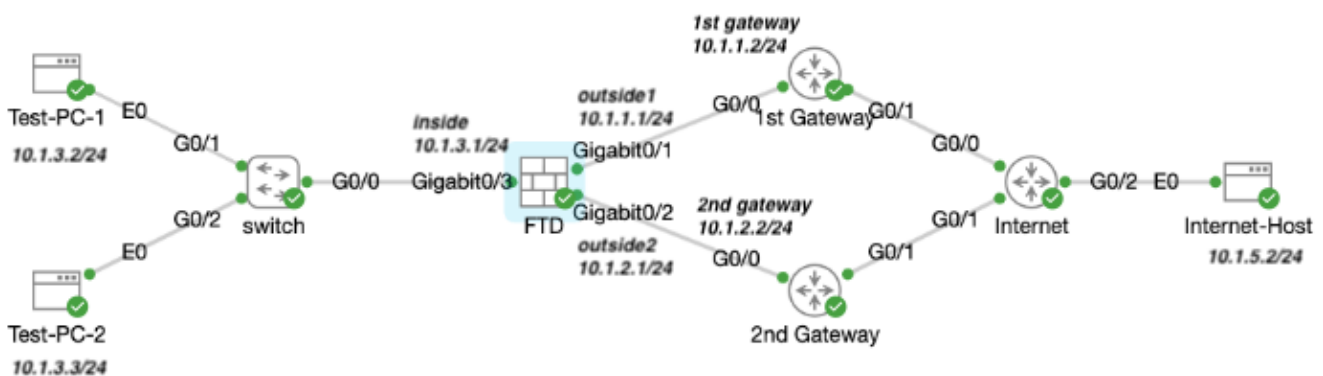
## 設定

### 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。

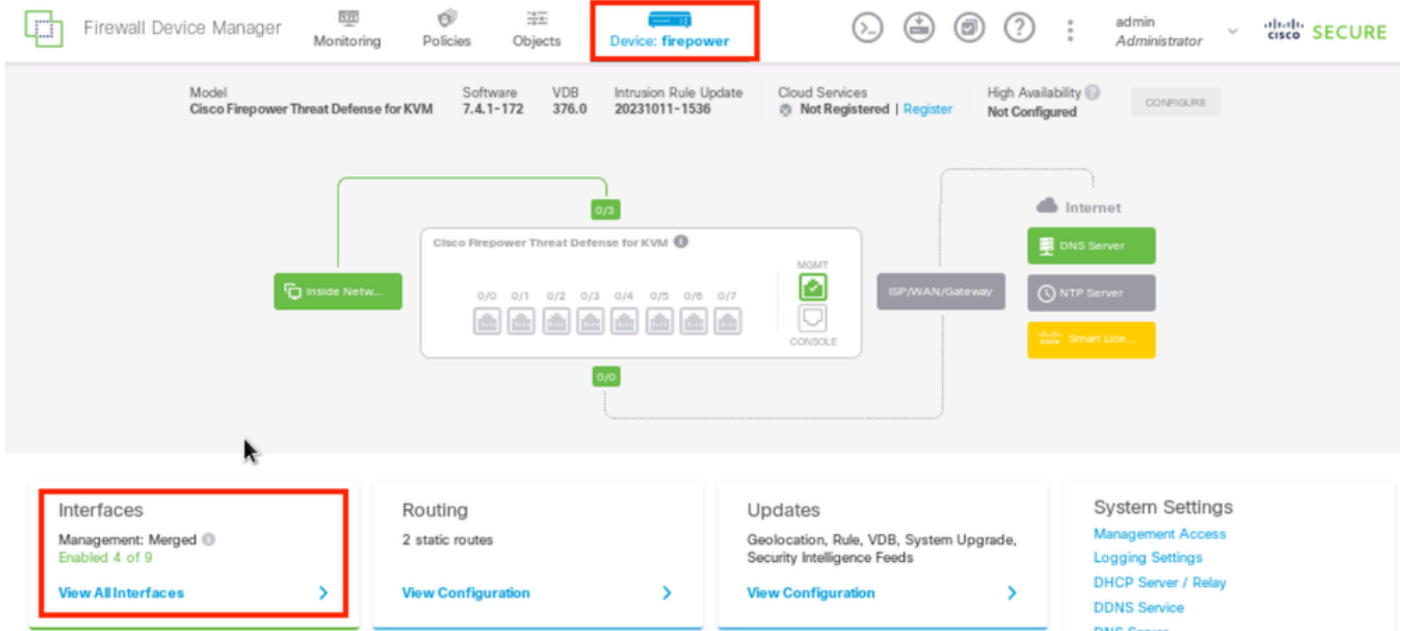


網路圖表

### 組態

#### 步驟 0. 預配置介面/對象

登入到FDM Web GUI，按一下裝置，然後按一下介面摘要中的連結。Interfaces 清單顯示可用介面、其名稱、地址和狀態。



FDM裝置介面



按一下要編輯的物理介面的編輯圖示( )。在本示例中，GigabitEthernet0/1。

Firewall Device Manager

Monitoring Policies Objects Device: firepower

admin Administrator

CISCO SECURE

### Device Summary

#### Interfaces

Cisco Firepower Threat Defense for KVM


0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT

CONSOLE

Interfaces Virtual Tunnel Interfaces

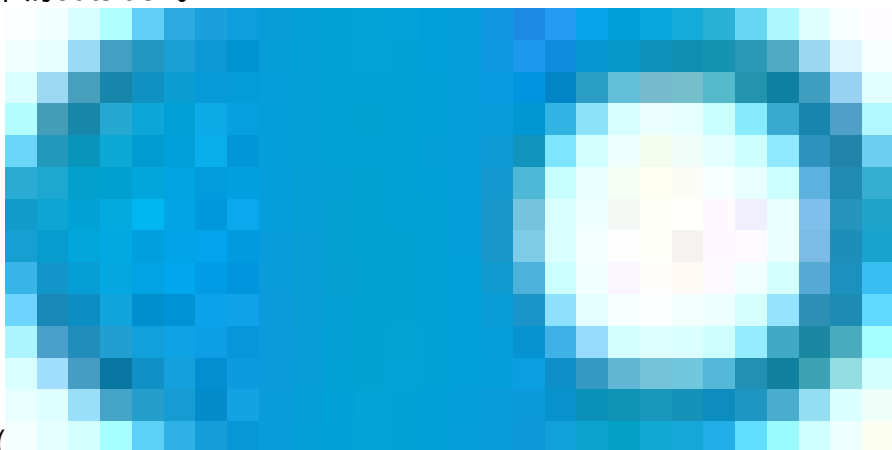
9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STAND BY ADDRESS	MONITOR FOR HA	ACTIONS
> GigabitEthernet0/0	outside	<input type="checkbox"/>	Routed			Enabled	
> GigabitEthernet0/1	outside 1	<input checked="" type="checkbox"/>	Routed	10.1.1.1		Enabled	

步驟0介面Gi0/1

在Edit Physical Interface窗口中：

1. 設定Interface Name，在本例中為outside1。



2. 將狀態滑杆設定為啟用的設定( )。
3. 按一下IPv4 Address頁籤並配置IPv4地址(本例中為10.1.1.1/24)。
4. 按一下「OK」(確定)。

# GigabitEthernet0/1

## Edit Physical Interface



Interface Name

outside1

Mode

Routed

Status



*Most features work with named interfaces only, although some require unnamed interfaces.*

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.1.1

/

255.255.255.0

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

Standby IP Address and Subnet Mask

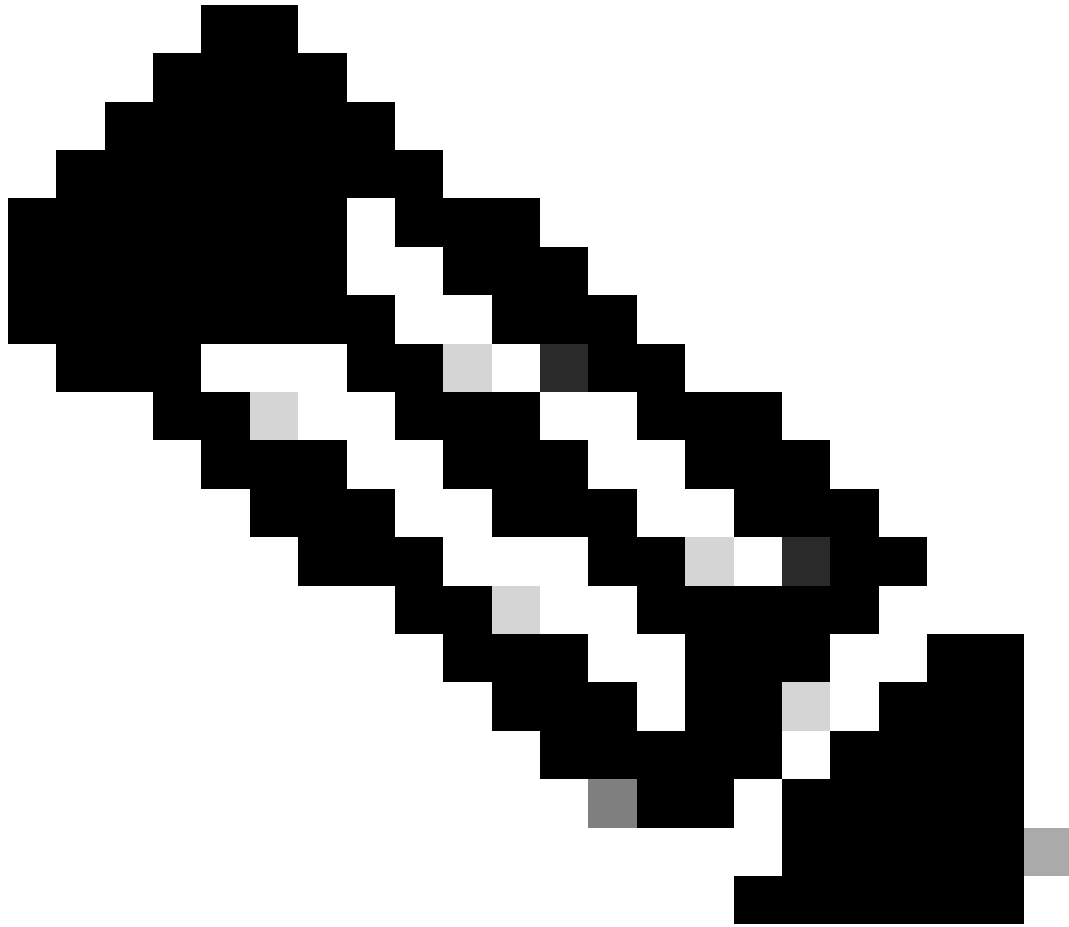
 / 

*e.g. 192.168.5.16*

CANCEL

OK

步驟0編輯介面Gi0/1

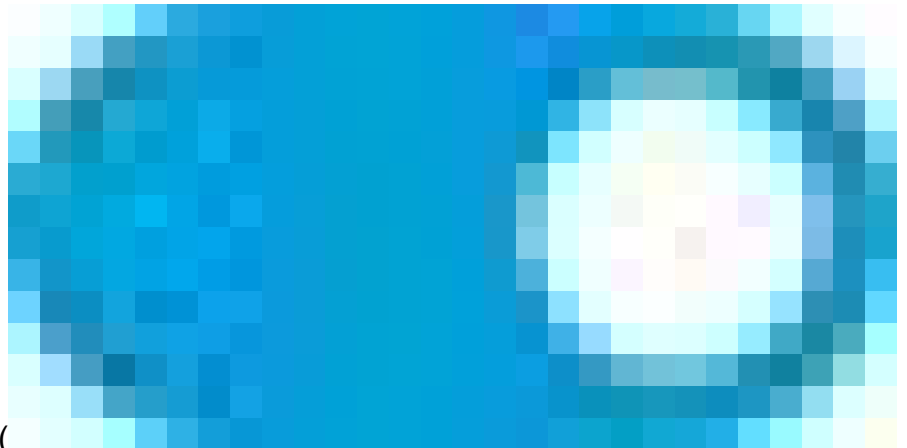


註：只有路由介面可以與ECMP區域關聯。

---

重複類似步驟，為輔助ISP連線配置介面，在此示例中物理介面為GigabitEthernet0/2。在Edit Physical Interface窗口中：

1. 設定Interface Name，在本例中為outside2。



2. 將狀態滑杆設定為啟用的設定(

- )。
- 按一下IPv4 Address頁籤並配置IPv4地址(本例中為10.1.2.1/24)。
  - 按一下「OK」(確定)。

## GigabitEthernet0/2

### Edit Physical Interface

Interface Name:

Mode:

Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask:  /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

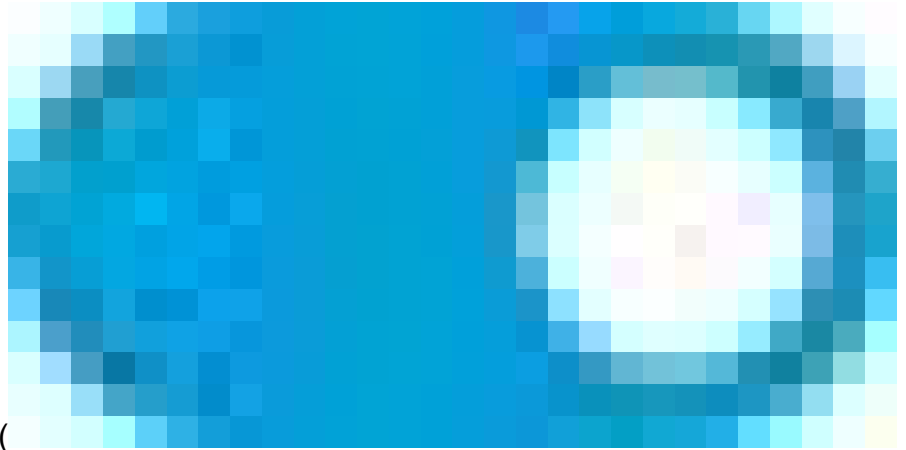
Standby IP Address and Subnet Mask:  /

e.g. 192.168.5.16

步驟0編輯介面Gi0/2

重複類似步驟，為內部連線配置介面，在本示例中，物理介面為GigabitEthernet0/3。在Edit Physical Interface窗口中：

1. 設定Interface Name , 在此例中為inside。



2. 將狀態滑杆設定為啟用的設定( )。

3. 按一下IPv4 Address頁籤並配置IPv4地址(本例中為10.1.3.1/24)。

4. 按一下「OK」(確定)。



# GigabitEthernet0/3 Edit Physical Interface



Interface Name

inside

Mode

Routed

Status



*Most features work with named interfaces only, although some require unnamed interfaces.*

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.3.1

/

24

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

Standby IP Address and Subnet Mask

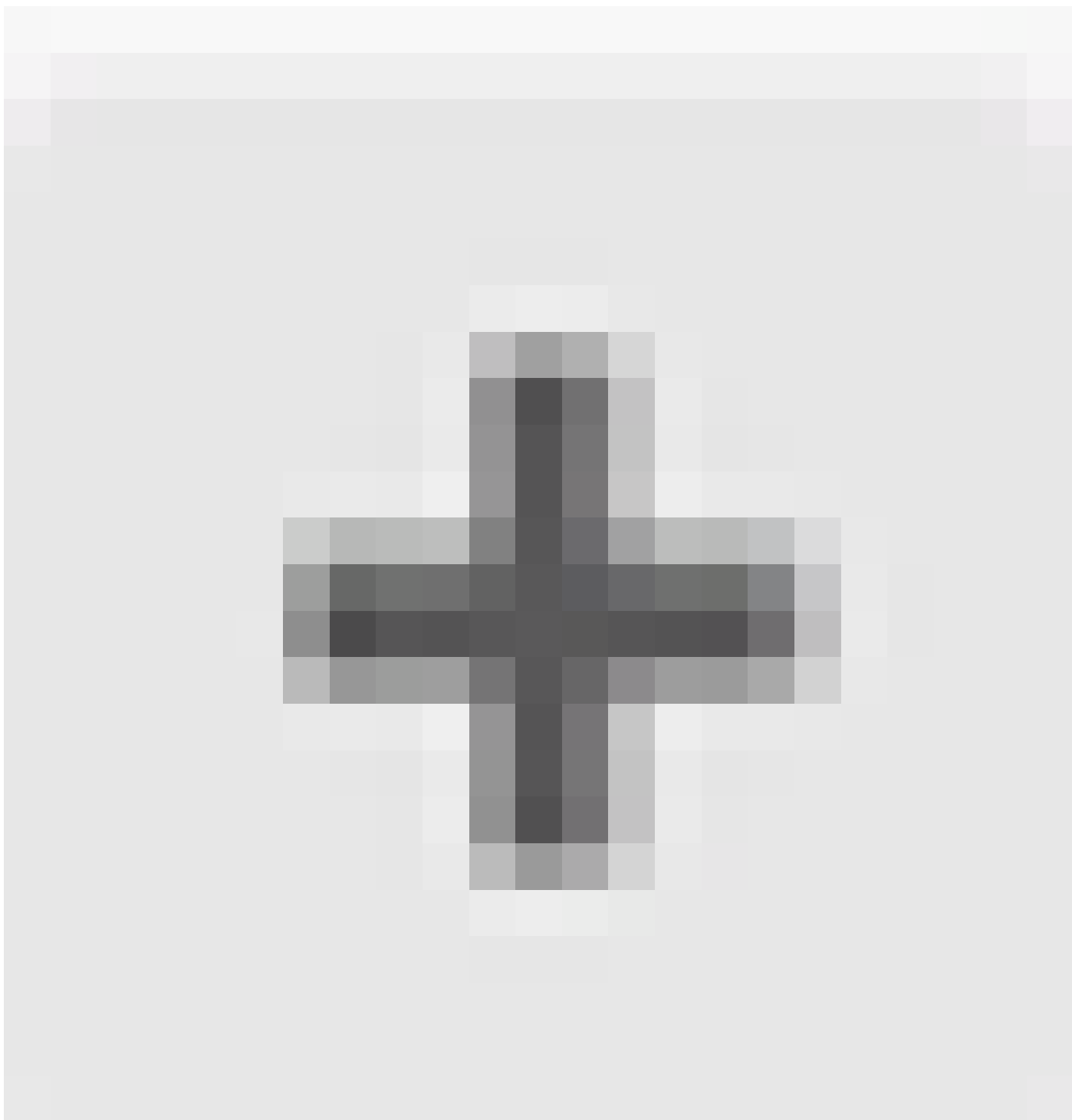
*e.g. 192.168.5.16*

CANCEL

OK

步驟0編輯介面Gi0/3

導航到對象>對象型別>網路，點選增加圖示()



增加新對象。

Firewall Device Manager   Monitoring   Policies   **Objects**   Device: firepower   admin Administrator   CISCO SECURE

Object Types   ←

**Networks**

Ports

Security Zones

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

### Network Objects and Groups

8 objects

Filter +

Preset filters: *System,Applied, User,Applied*

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	
2	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
3	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
4	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
5	any-ipv4	NETWORK	0.0.0.0/0	
6	any-ipv6	NETWORK	::/0	

步驟0對象1

在Add Network Object 窗口中，配置第一個ISP網關：

1. 設定對象的名稱，在本例中為gw-outside1。
2. 選擇對象的型別，此例中為主機。
3. 設定主機的IP地址，在本例中為10.1.1.2。
4. 按一下「OK」（確定）。

# Add Network Object

Name  
gw-outside1

Description

Type  
 Network  Host  FQDN  Range

Host  
10.1.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL OK

步驟0對象2

重複類似步驟，為第二個ISP網關配置另一個網路對象：

1. 設定對象的名稱，在本例中為gw-outside2。
2. 選擇對象的型別，此例中為主機。
3. 設定主機的IP地址，在本例中為10.1.2.2。
4. 按一下「OK」（確定）。

# Add Network Object



Name

gw-outside2

Description

Type



Network



Host



FQDN



Range

Host

10.1.2|2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL

OK

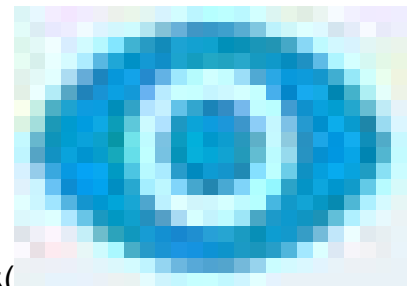


附註：您必須在FTD上設定存取控制原則，才能允許流量，本檔案不涵蓋此部分。

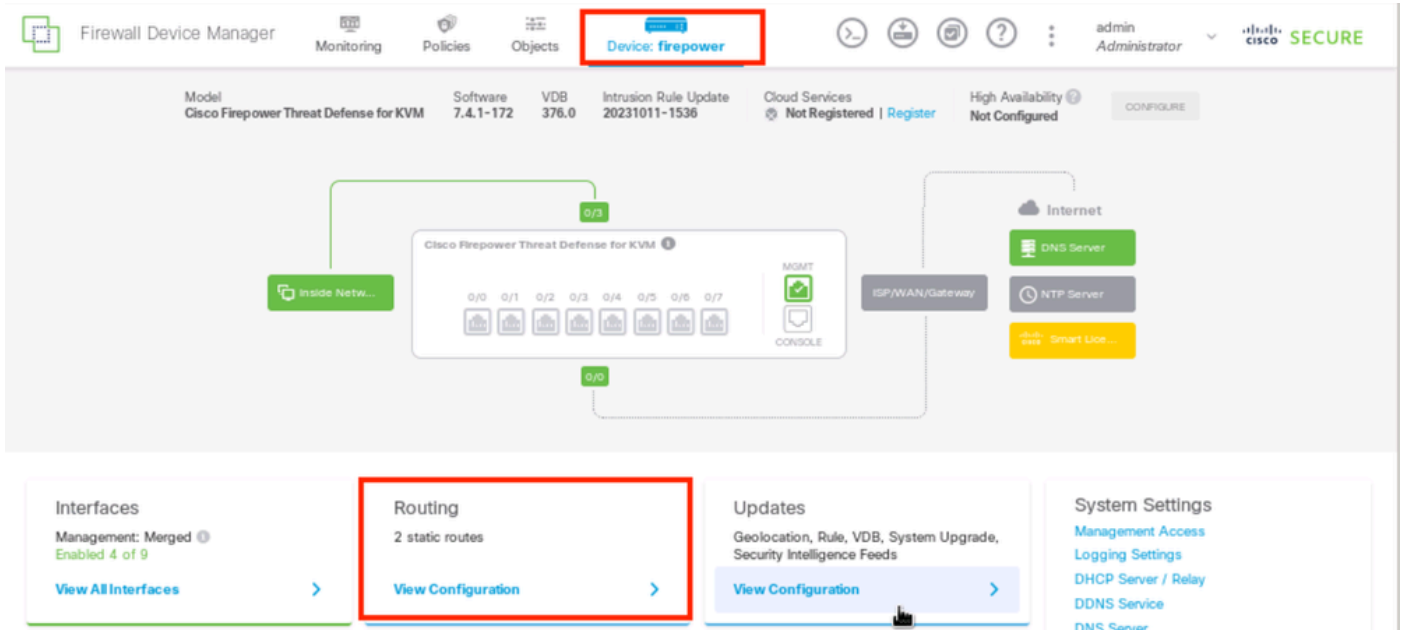
---

### 步驟 1. 配置ECMP區域

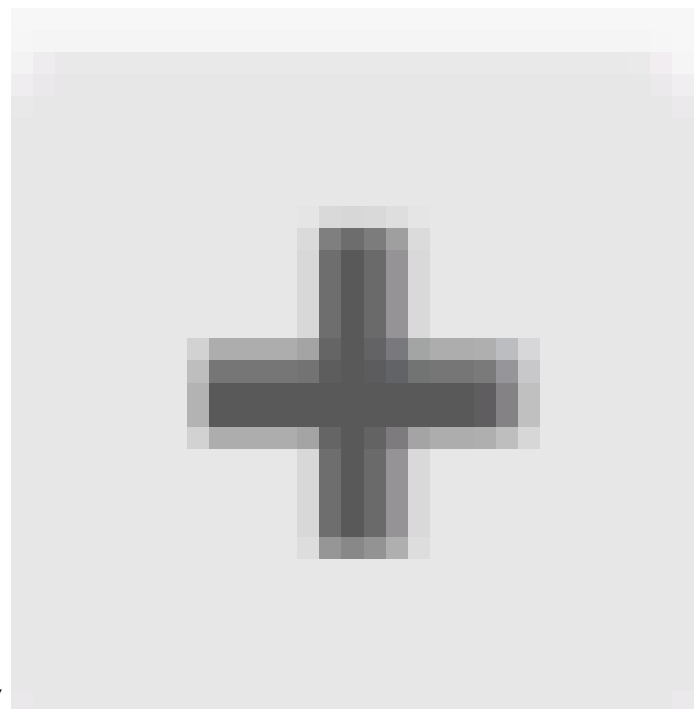
導航到裝置，然後點選路由摘要中的連結。



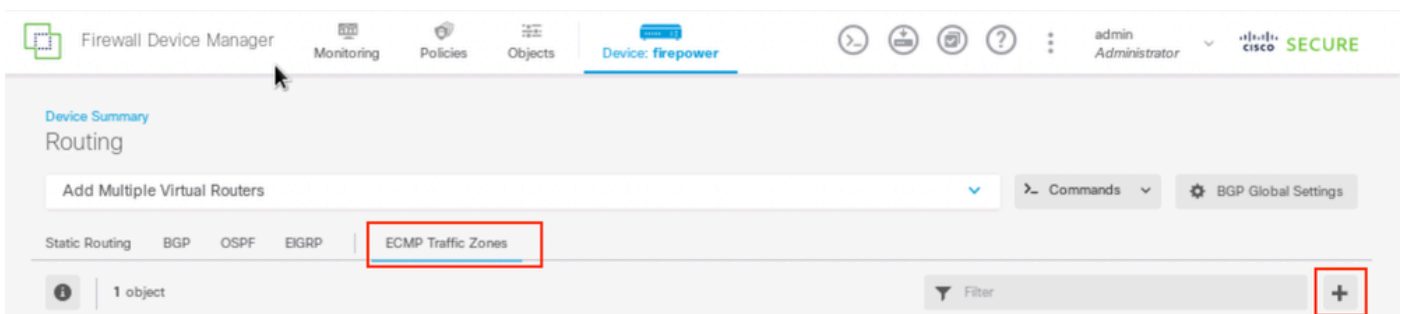
如果啟用了虛擬路由器，請點選正在配置靜態路由的路由器的檢視圖示( )。在這種情況下，虛擬路由器未啟用。



第1步ECMP區域1



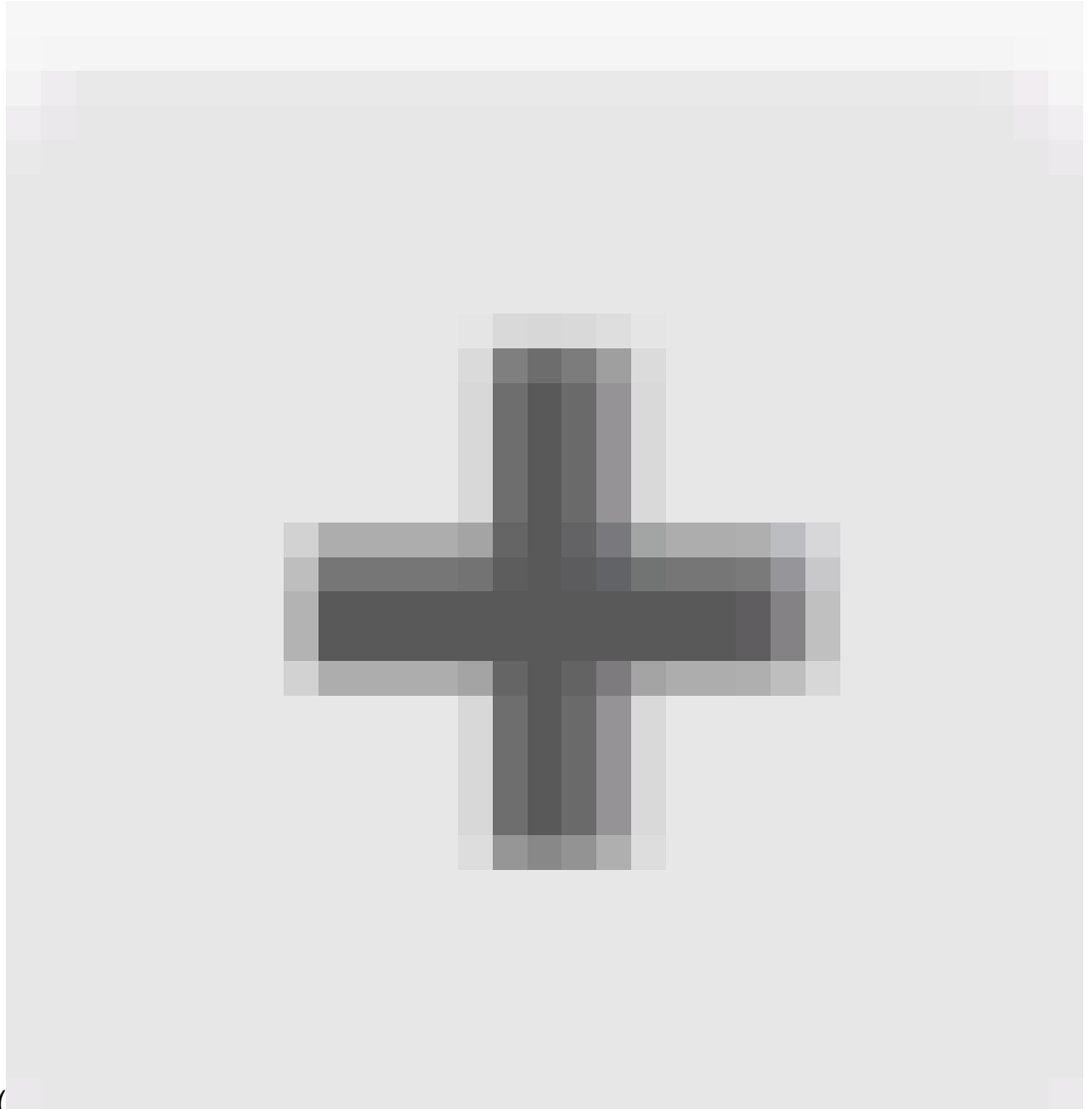
點選ECMP Traffic Zones頁籤，然後點選add圖示( )以增加新區域。




第1步ECMP區域2

在Add ECMP Traffic Zone 窗口中：

1. 設定ECMP區域的名稱，並根據需要設定說明。



2. 點選增加圖示(  )，選擇最多8個介面以將其包含在區域中。在本示例中，ECMP名稱為Outside，介面outside1和outside2增加到區域中。
3. 按一下「OK」( 確定 )。



# Add ECMP Traffic Zone



**i** Keep the member interfaces of a ECMP traffic zone in the same security zone to prevent different access rules being applied to those interfaces.

Name

Outside

Description

Interfaces



- > inside (GigabitEthernet0/3)
- > management (Management0/0)
- > outside (GigabitEthernet0/0)
- > outside1 (GigabitEthernet0/1)
- > outside2 (GigabitEthernet0/2)

2 item(s) selected

Create new Subinterface

CANCEL

OK

CANCEL

OK

NETWORK

INSIDE HOST

ADD ECMP TRAFFIC ZONE

第1步ECMP區域3

介面outside1和outside2均已成功增加到ECMP區域outside。

Device Summary  
Routing

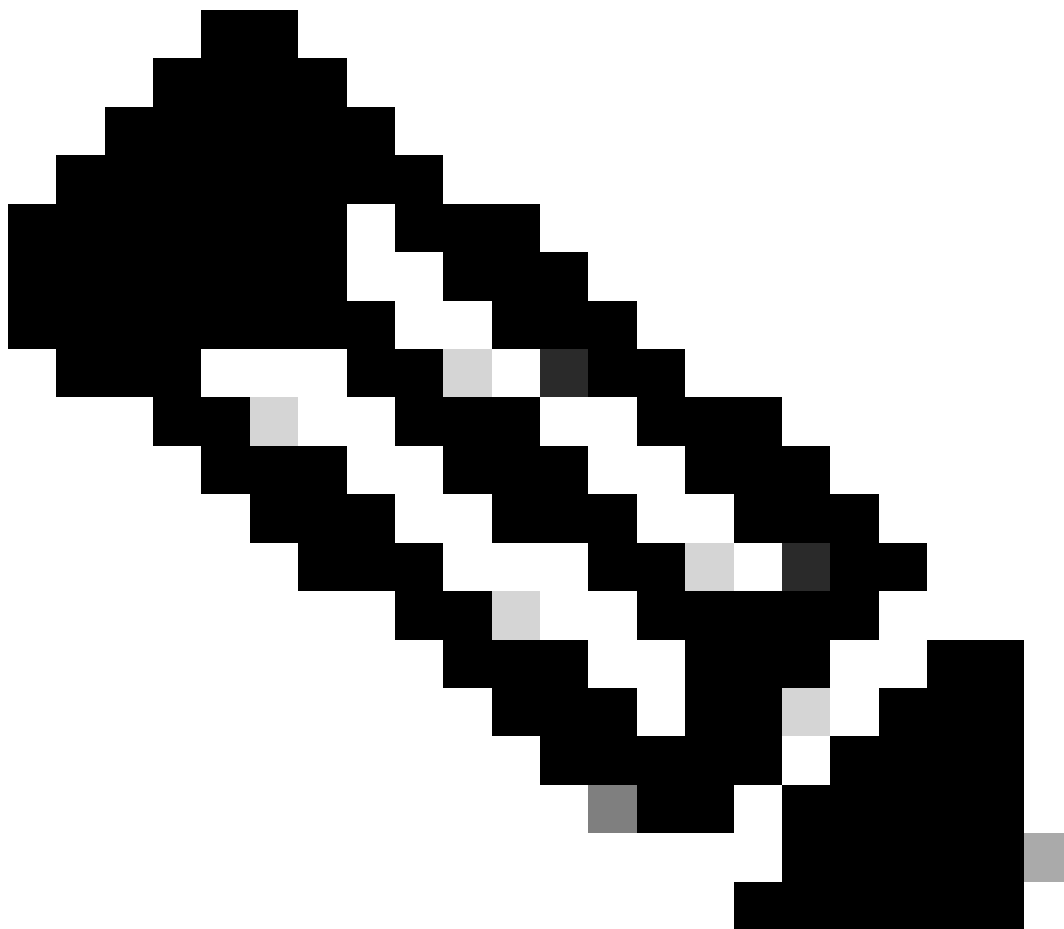
Add Multiple Virtual Routers ▾ Commands ▾ BGP Global Settings

Static Routing | BGP | OSPF | EIGRP | **ECMP Traffic Zones**

1 object Filter +

#	NAME	INTERFACES	ACTIONS
1	Outside	outside1 (GigabitEthernet0/1) outside2 (GigabitEthernet0/2)	

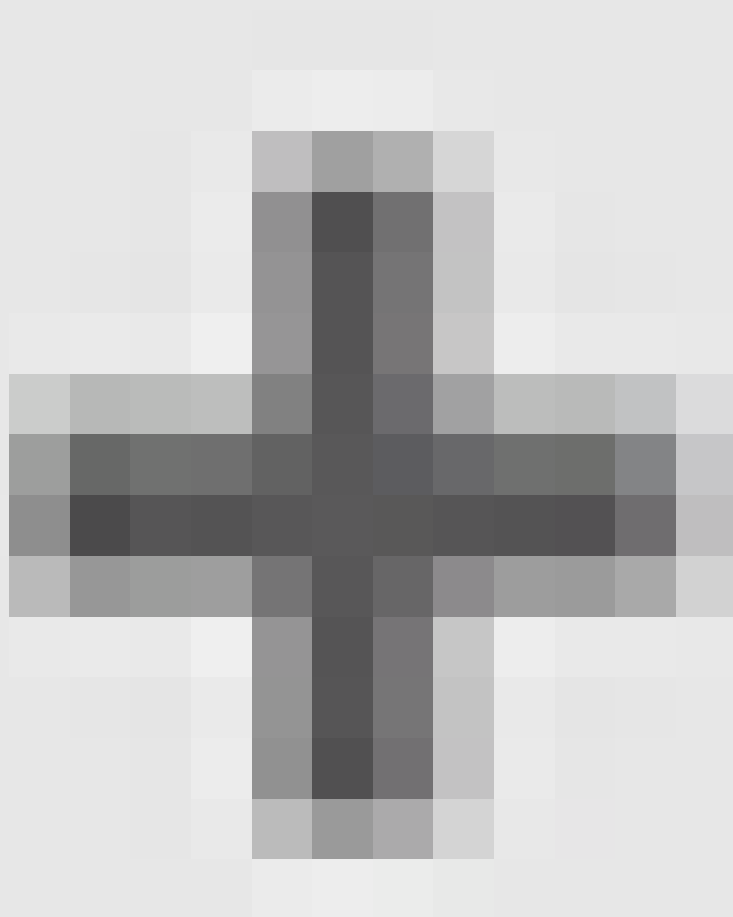
第1步ECMP區域4



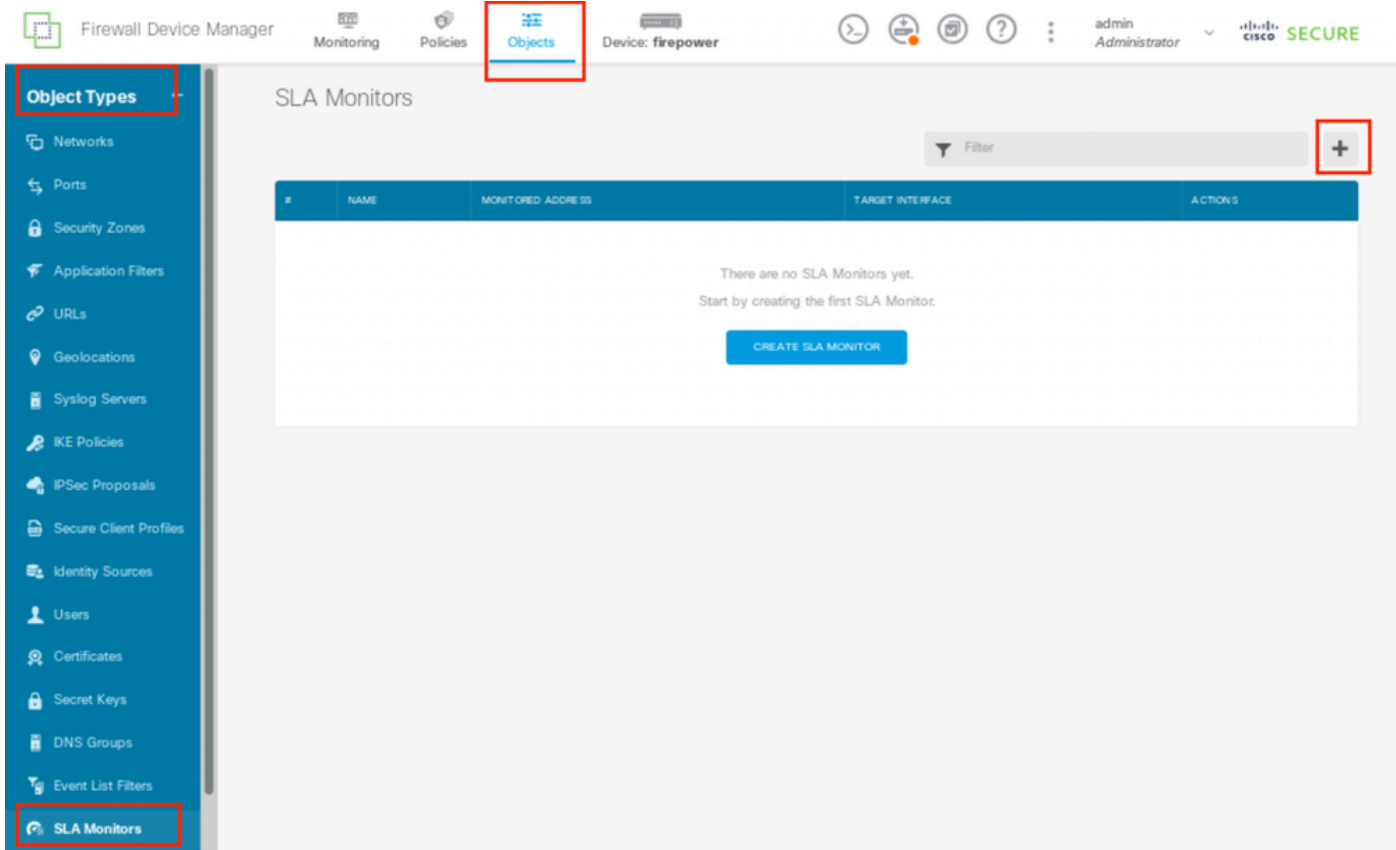
注意：ECMP路由流量區域與安全區域無關。建立包含outside1和outside2介面的安全區域不會為ECMP路由實現流量區域。

步驟 2. 配置IP SLA對象

要定義用於監控到每個網關連線的SLA對象，請導航到對象>對象型別> SLA監控器，點選增加圖示(



)，為第一個ISP連線增加新的SLA監控器。



第2步IP SLA1

在Add SLA Monitor Object 窗口中：

1. 為SLA監控器對象設定Name，並選擇性地設定說明(在本例中為sla-outside1)。
2. 設定Monitor Address，在此例中為gw-outside1 ( 第一個ISP網關 )。
3. 設定可到達監控器地址的目標介面，此例中為outside1。
4. 此外，還可以調整超時和閾值。按一下「OK」( 確定 )。

# Add SLA Monitor Object



Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

## IP ICMP ECHO OPTIONS

**i** Following properties have following correlation: Threshold  $\leq$  Timeout  $\leq$  Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

OK

重複類似步驟，在Add SLA Monitor Object 窗口中為第二個ISP連線配置另一個SLA Monitor Object：

1. 為SLA監控對象設定Name，並選擇性地設定說明(本例中為sla-outside2)。
2. 設定Monitor Address，在本例中為gw-outside2 ( 第二個ISP網關 )。
3. 設定可到達監控器地址的目標介面，此例中為outside2。
4. 此外，還可以調整超時和閾值。按一下「OK」( 確定 )。



# Add SLA Monitor Object



Name

sla-outside2

Description

Monitor Address

gw-outside2

Target Interface

outside2 (GigabitEthernet0/2)

## IP ICMP ECHO OPTIONS

**i** Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

OK

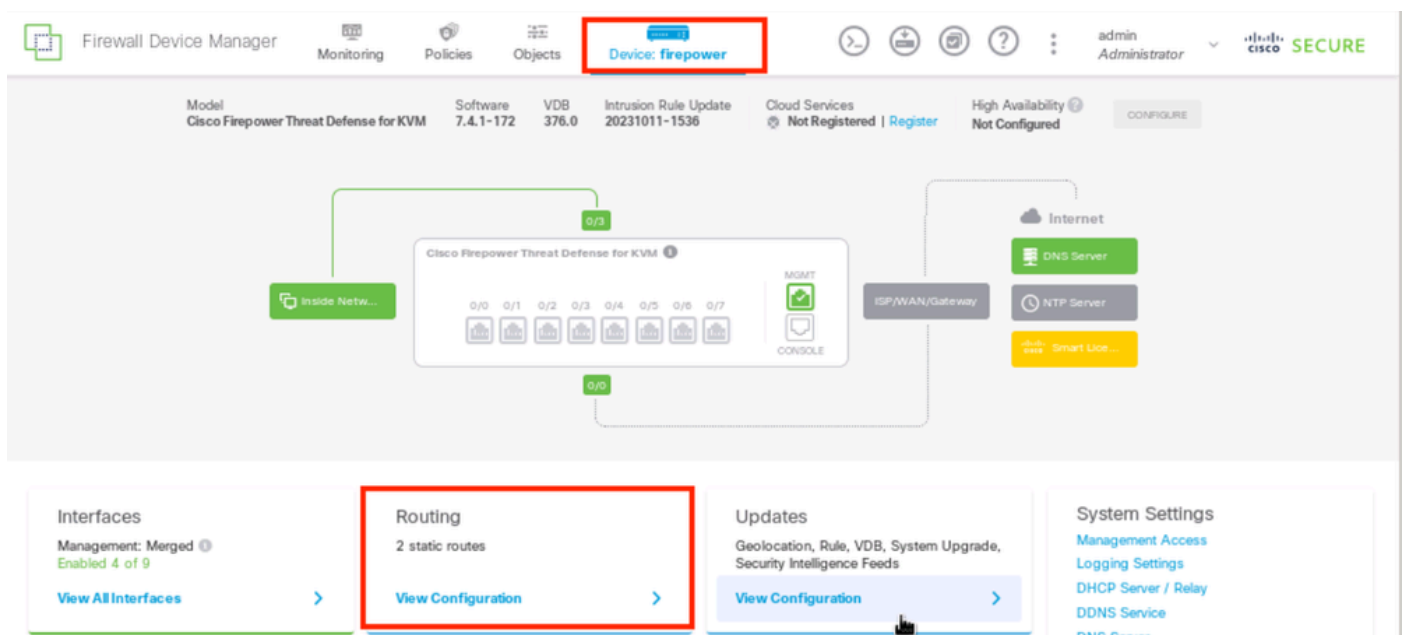
第2步IP SLA3

### 步驟 3.使用路由跟蹤配置靜態路由

導航到裝置，然後點選路由摘要中的連結。



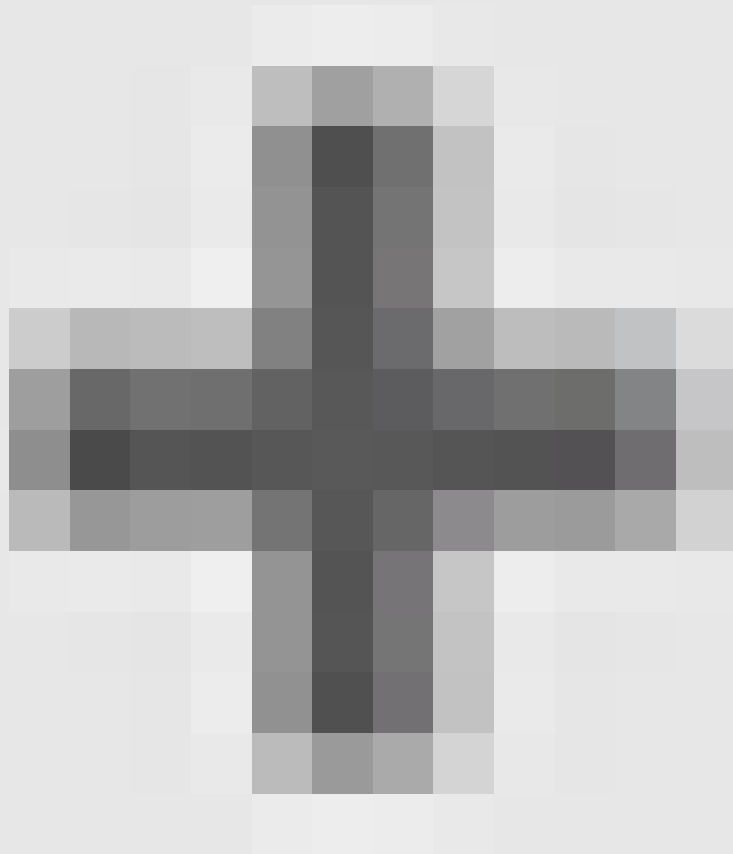
如果啟用了虛擬路由器，請點選正在配置靜態路由的路由器的檢視圖示( )。在這種情況下，虛擬路由器未啟用。



第3步Route1

在靜態路由頁面上，點選增加圖示( )





)，為第一個ISP鏈路增加新的靜態路由。

在Add Static Route 窗口中：

1. 設定路由的Name和說明（可選）。在本示例中，route\_outside1。
2. 從Interface下拉選單中，選擇要透過其傳送流量的介面，需要透過介面訪問網關地址。在本示例中，outside1 (GigabitEthernet0/1)。
3. 選擇網路，標識使用此路由中的網關的目標網路或主機。在本示例中，是預定義的any-ipv4。
4. 從Gateway 下拉選單中，選擇用於辨識網關IP地址的網路對象，Traffic is sent to this address.在本例中，為gw-outside1（第一個ISP網關）。
5. 設定路由的Metric，介於1和254之間。在本示例 1中。
6. 從SLA Monitor下拉選單中選擇SLA監控器對象。在本例中，選擇sla-outside1。

7. 按一下「OK」(確定)。

## Add Static Route

Name  
route\_outside1

Description

Interface  
outside1 (GigabitEthernet0/1)

Protocol  
 IPv4  IPv6

Networks  
+  
any-ipv4

Gateway  
gw-outside1

Metric  
1

SLA Monitor Applicable only for IPv4 Protocol type  
sla-outside1

CANCEL OK

重複類似步驟，在Add Static Route 窗口中為第二個ISP連線配置另一個靜態路由：

1. 設定路由的Name和說明（可選）。在本示例中，route\_outside2。
2. 從Interface下拉選單中，選擇要透過其傳送流量的介面，需要透過介面訪問網關地址。在本示例中，outside2 (GigabitEthernet0/2)。
3. 選擇網路，標識使用此路由中的網關的目標網路或主機。在本示例中，是預定義的any-ipv4。
4. 從Gateway下拉選單中，選擇用於辨識網關IP地址的網路對象，Traffic is sent to this address。在本例中，為gw-outside2（第二個ISP網關）。
5. 設定路由的Metric，介於1和254之間。在本示例 1中。
6. 從SLA Monitor下拉選單中選擇SLA監控器對象。在本場景中，為sla-outside2。
7. 按一下「OK」（確定）。

# Add Static Route



Name

route\_outside2

Description

Interface

outside2 (GigabitEthernet0/2)

Protocol

IPv4

IPv6

Networks



any-ipv4

Gateway

gw-outside2

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

您有2條路由，其透過帶有路由跟蹤的outside1和outside2介面。



#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	route_outside1	outside1	IPv4	0.0.0.0/0	10.1.1.2	sla-outside1	1	
2	route_outside2	outside2	IPv4	0.0.0.0/0	10.1.2.2	sla-outside2	1	

步驟3：路由4

將變更部署到FTD。

## 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 GigabitEthernet0/2
```

```
outside1 GigabitEthernet0/1
```

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
```

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

```
<#root>
```

```
> show sla monitor configuration
```

```
SA Agent, Infrastructure Engine-II
```

```
Entry number: 1037119999
```

```
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: 1631063762  
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」，表示到網關的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: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
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: 05:32:32.791 UTC Tue Jan 30 2024  
Latest operation return code: OK  
RTT Values:  
RTTAvg: 1 RTTMin: 1 RTTMax: 1  
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762  
Modification time: 04:14:32.771 UTC Tue Jan 30 2024  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 79  
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: 05:32:32.791 UTC Tue Jan 30 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，從Test-PC-1 (10.1.3.2)和Test-PC-2 (10.1.3.4)到Internet主機(10.1.5.2)啟動SSH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，Test-PC-1 (10.1.3.2)透過interface outside1，Test-PC-2 (10.1.3.4)透過interface outside2。

<#root>

```
> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect
```

```
TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1
```

```
TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, 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。

運行命令 `show sla monitor operational-state` 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: 1037119999

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 121

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: 06:14:32.801 UTC Tue Jan 30 2024

Latest operation return code: Timeout

RTT Values:

RTTAvg: 0 RTTMin: 0 RTTMax: 0

NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 1631063762

Modification time: 04:14:32.771 UTC Tue Jan 30 2024

Number of Octets Used by this Entry: 2056

Number of operations attempted: 121

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: 06:14:32.802 UTC Tue Jan 30 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然運行。SSH會話在Test-PC-1 (10.1.3.2)和Test-PC-2 (10.1.3.4)上也處於活動狀態，不會出現任何中斷。

```
<#root>
```

```
> show conn  
4 in use, 14 most used  
Inspect Snort:  
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect
```

```
TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1
```

```
TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, 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，但是Test-PC-1 (10.1.3.2)的SSH會話仍透過介面outside1。這是預期的結果，而且根據設計，實際流量流經介面outside2。如果啟動從Test-PC-1 (10.1.3.2)到Internet主機(10.1.5.2)的新連線，則可以發現所有流量都透過介面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 0.0.0.0
```

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
```

RT(mgmt-only):

```
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。

```
> 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
```

相關資訊

- [思科技術支援與下載](#)

## 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）。