Configurazione di ECMP con SLA IP su FTD gestito da FDM

Sommario

Introduzione

In questo documento viene descritto come configurare ECMP con SLA IP su un FTD gestito da FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ECMP su Cisco Secure Firewall Threat Defense (FTD)
- Configurazione dello SLA IP su Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Device Manager (FDM)

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione software e hardware:

- Cisco FTD versione 7.4.1 (build 172)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritto come configurare Equal-Cost Multi-Path (ECMP) con Internet Protocol Service Level Agreement (IP SLA) su un FTD Cisco gestito da Cisco FDM. ECMP consente di raggruppare le interfacce su FTD e di bilanciare il carico del traffico su più interfacce. Lo SLA IP è un meccanismo che monitora la connettività end-to-end attraverso lo scambio di pacchetti regolari. Oltre all'ECMP, è possibile implementare lo SLA IP per garantire la disponibilità dell'hop successivo. Nell'esempio, il protocollo ECMP viene usato per distribuire i pacchetti in modo uniforme su due circuiti ISP (Internet Service Provider). Allo stesso tempo, uno SLA IP tiene traccia della connettività, assicurando una transizione senza problemi a qualsiasi circuito disponibile in caso di guasto.

I requisiti specifici per questo documento includono:

- Accesso ai dispositivi con un account utente con privilegi di amministratore
- Cisco Secure Firewall Threat Defense versione 7.1 o superiore

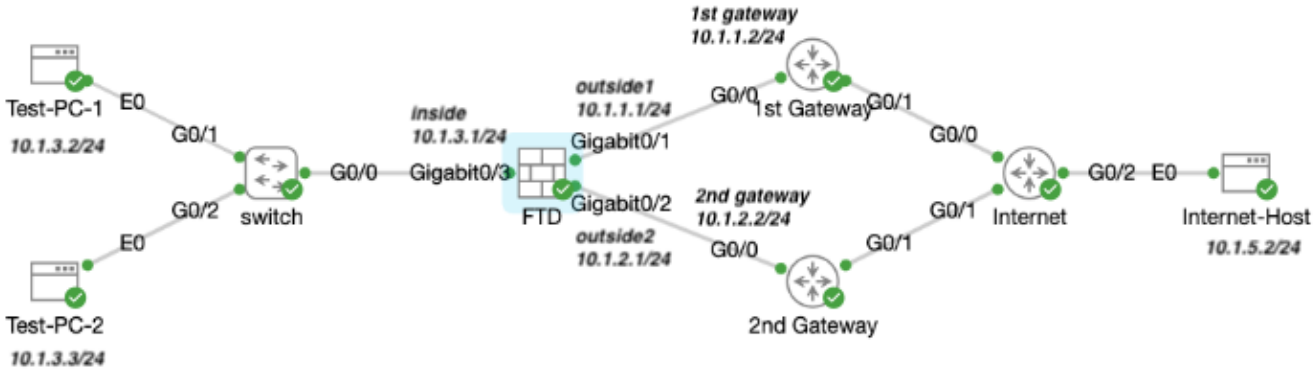
Configurazione

Esempio di rete

In questo esempio, Cisco FTD ha due interfacce esterne: outside1 e outside2. Ognuno di essi si connette a un gateway ISP, l'esterno 1 e l'esterno 2 appartengono alla stessa zona ECMP denominata all'esterno.

Il traffico proveniente dalla rete interna viene instradato attraverso FTD e viene bilanciato dal carico verso Internet attraverso i due ISP.

Allo stesso tempo, FTD usa gli SLA IP per monitorare la connettività a ciascun gateway ISP. In caso di guasto su uno dei circuiti ISP, FTD esegue il failover sull'altro gateway ISP per mantenere la continuità aziendale.

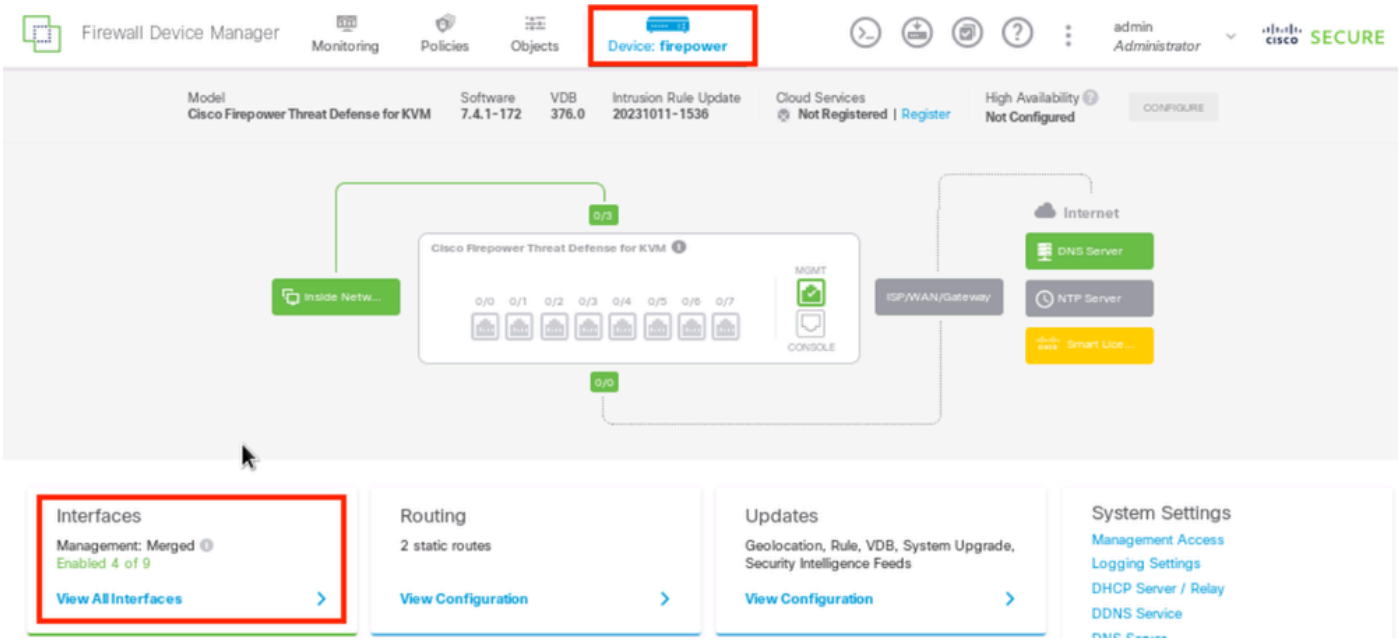


Esempio di rete

Configurazioni

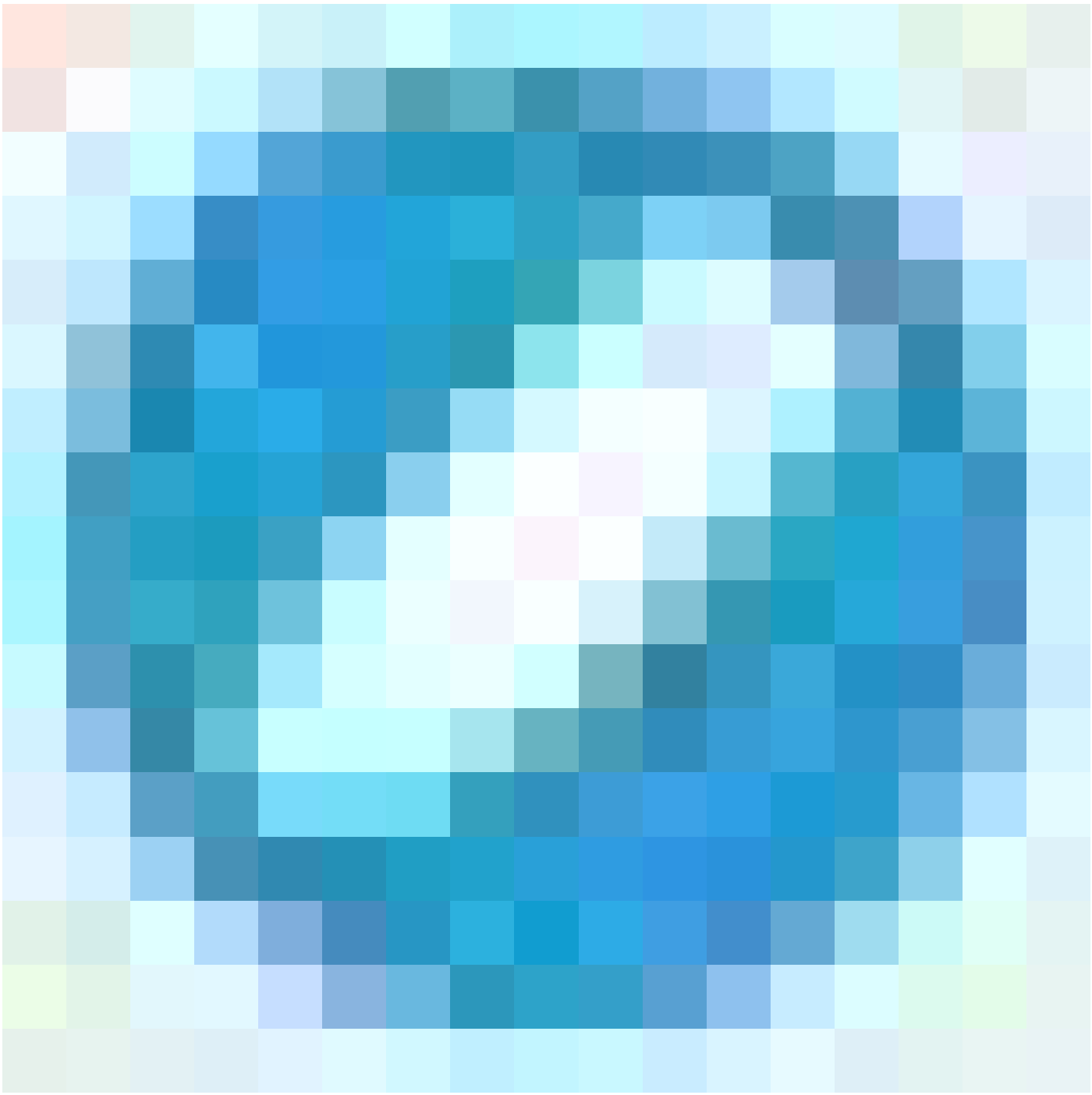
Passaggio 0. Preconfigurazione di interfacce/oggetti

Accedere all'interfaccia utente Web di FDM, fare clic su Dispositivo, quindi fare clic sul collegamento nel riepilogo Interfacce. Nell'elenco Interfacce vengono visualizzate le interfacce disponibili, i relativi nomi, indirizzi e stati.

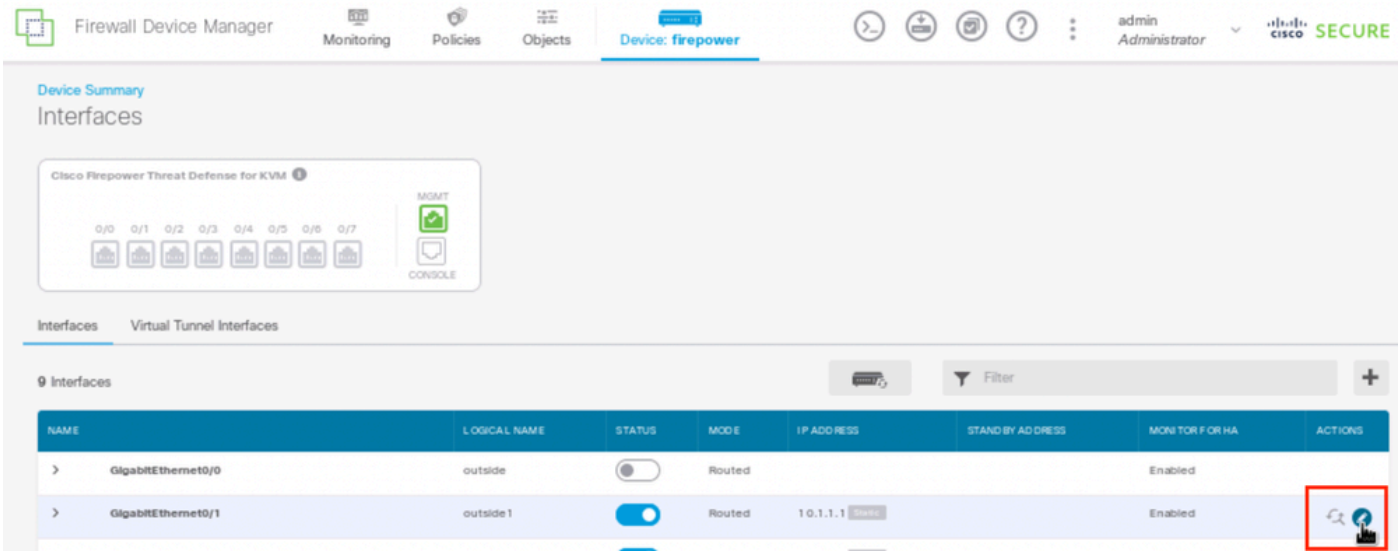


FDM Device Interface

Fare clic sull'icona di modifica (



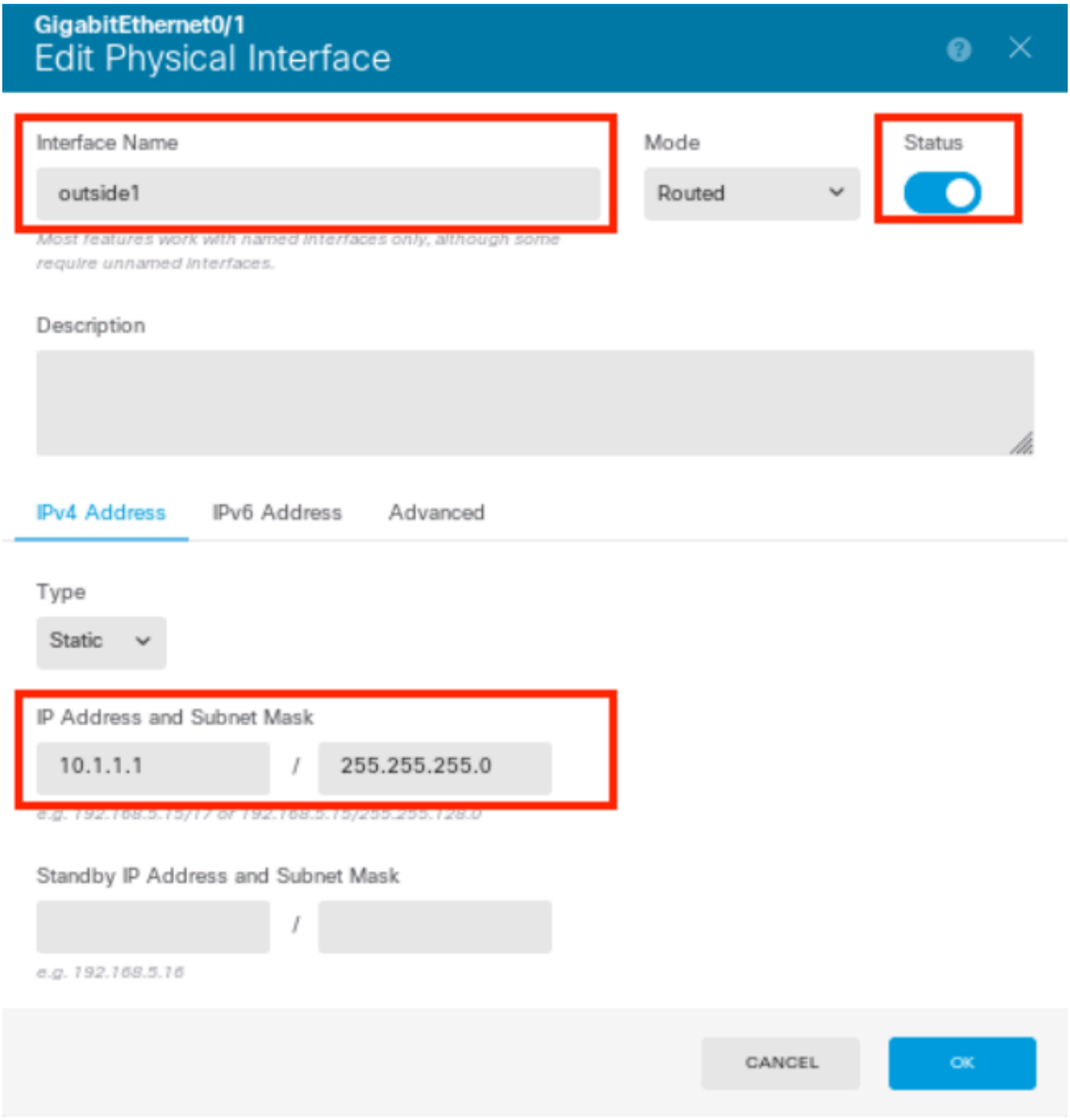
) per l'interfaccia fisica che si desidera modificare. Nell'esempio, Gigabit Ethernet0/1.



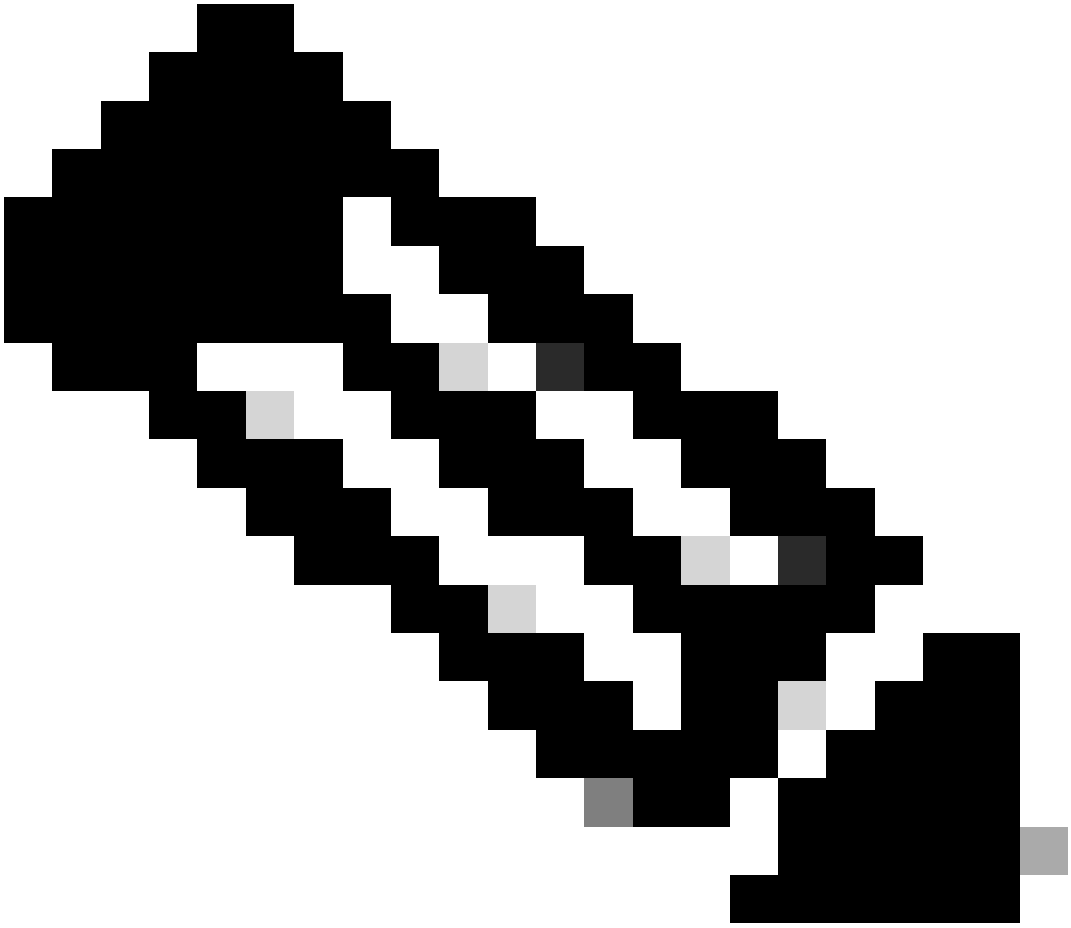
Fase 0 Interfaccia Gi0/1

Nella finestra Modifica interfaccia fisica:

1. Impostare il nome dell'interfaccia, in questo caso esternamente a 1.
2. Impostare il dispositivo di scorrimento Status (Stato) sull'impostazione enabled ().
3. Fare clic sulla scheda Indirizzo IPv4 e configurare l'indirizzo IPv4, in questo caso 10.1.1.1/24.
4. Fare clic su OK.

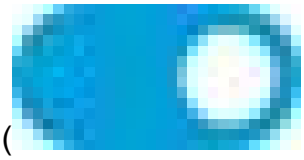


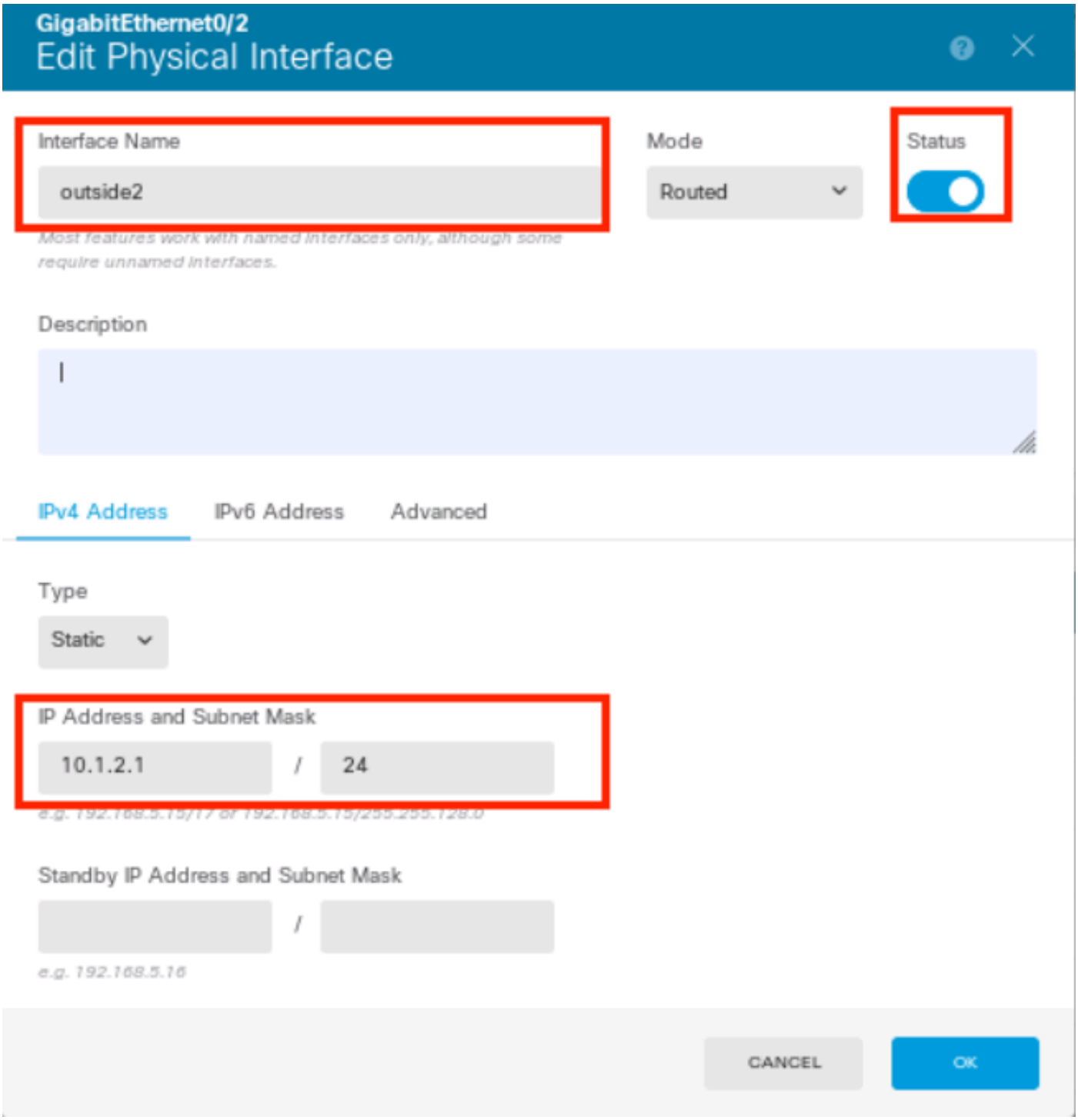
Passaggio 0 Modificare L'Interfaccia Gi0/1



Nota: solo le interfacce instradate possono essere associate a una zona ECMP.

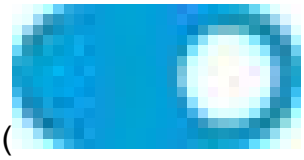
Ripetere la procedura simile per configurare l'interfaccia per la connessione dell'ISP secondario, in questo esempio l'interfaccia fisica è Gigabit Ethernet0/2 . Nella finestra Modifica interfaccia fisica:

1. Impostare il nome dell'interfaccia, in questo caso esternamente2.
2. Impostare il dispositivo di scorrimento Status sull'impostazione enabled ().
3. Fare clic sulla scheda Indirizzo IPv4 e configurare l'indirizzo IPv4, in questo caso 10.1.2.1/24.
4. Fare clic su OK.



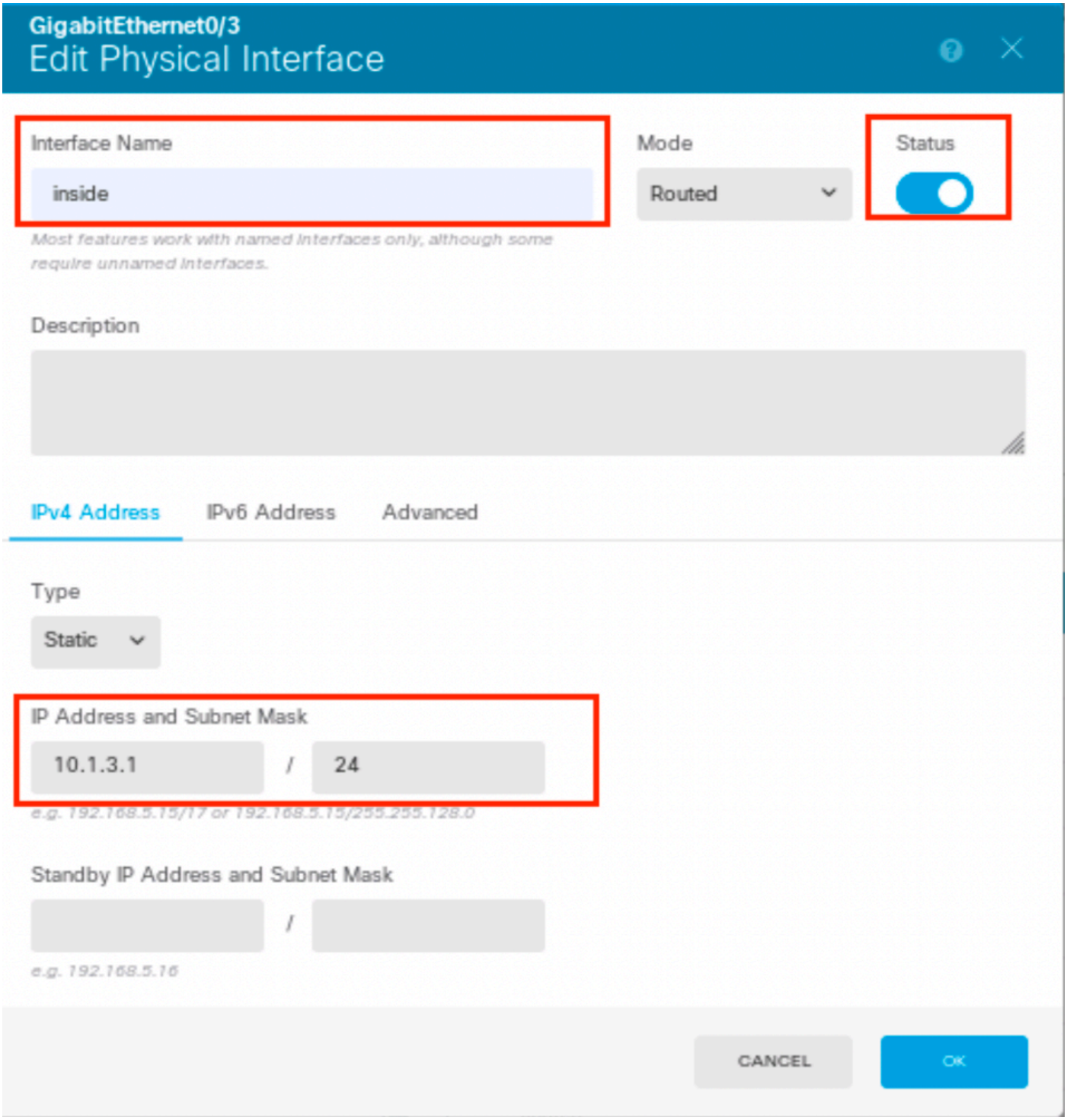
Fase 0: Modifica Interfaccia Gi0/2

Ripetere la procedura simile per configurare l'interfaccia per la connessione interna, in questo esempio l'interfaccia fisica è Gigabit Ethernet0/3. Nella finestra Modifica interfaccia fisica:

1. Impostare il nome dell'interfaccia, in questo caso all'interno di .
2. Impostare il dispositivo di scorrimento Status sull'impostazione enabled (

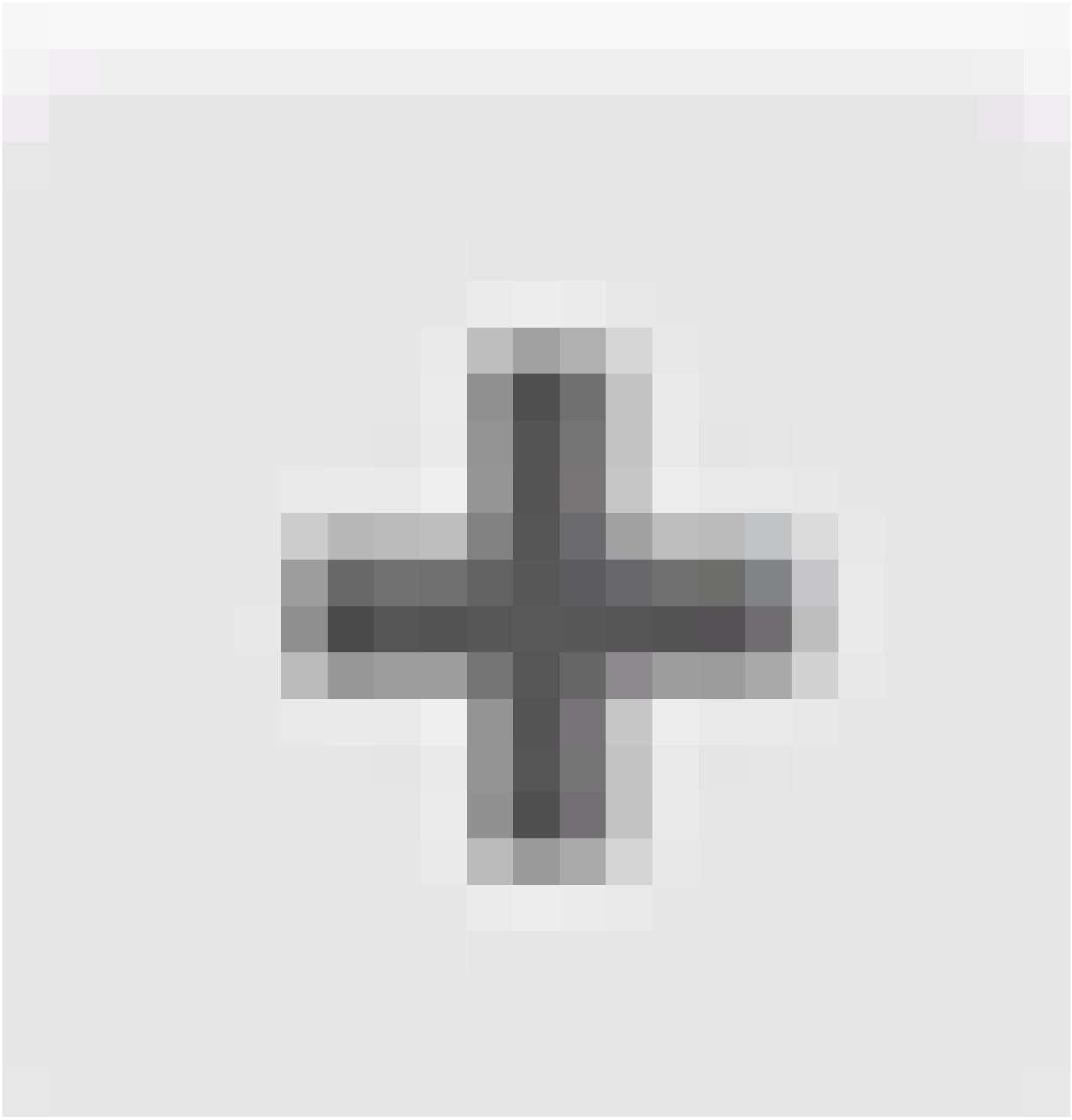
).

3. Fare clic sulla scheda Indirizzo IPv4 e configurare l'indirizzo IPv4, in questo caso 10.1.3.1/24.
4. Fare clic su OK.

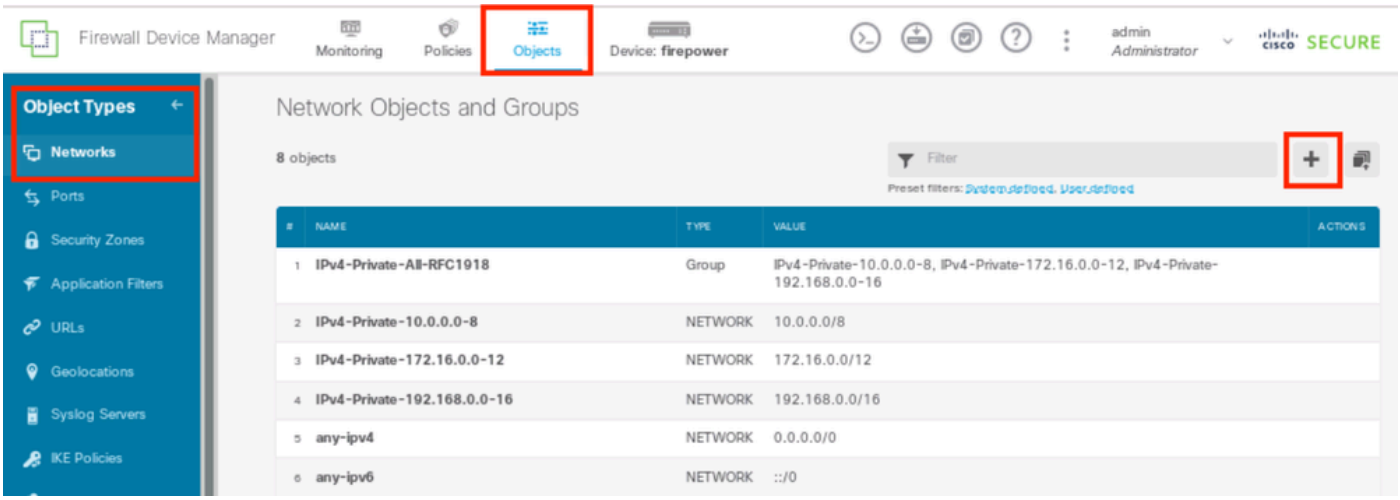


Fase 0: Modifica Interfaccia Gi0/3

Passare a Oggetti > Tipi di oggetto > Reti , fare clic sull'icona di aggiunta (



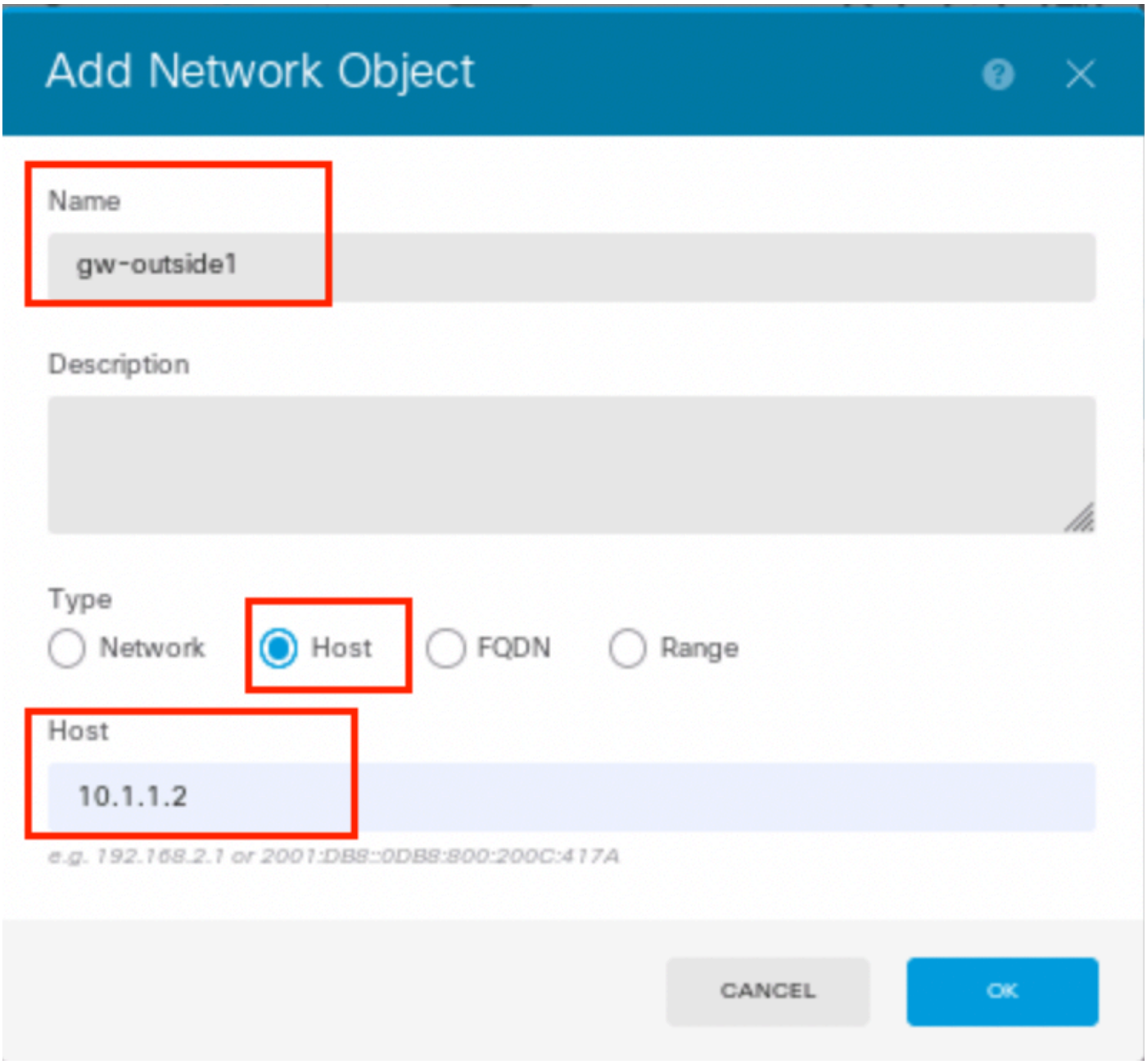
) per aggiungere un nuovo oggetto.



Fase 0 Oggetto1

Nella finestra Add Network Object (Aggiungi oggetto di rete), configurare il primo gateway ISP:

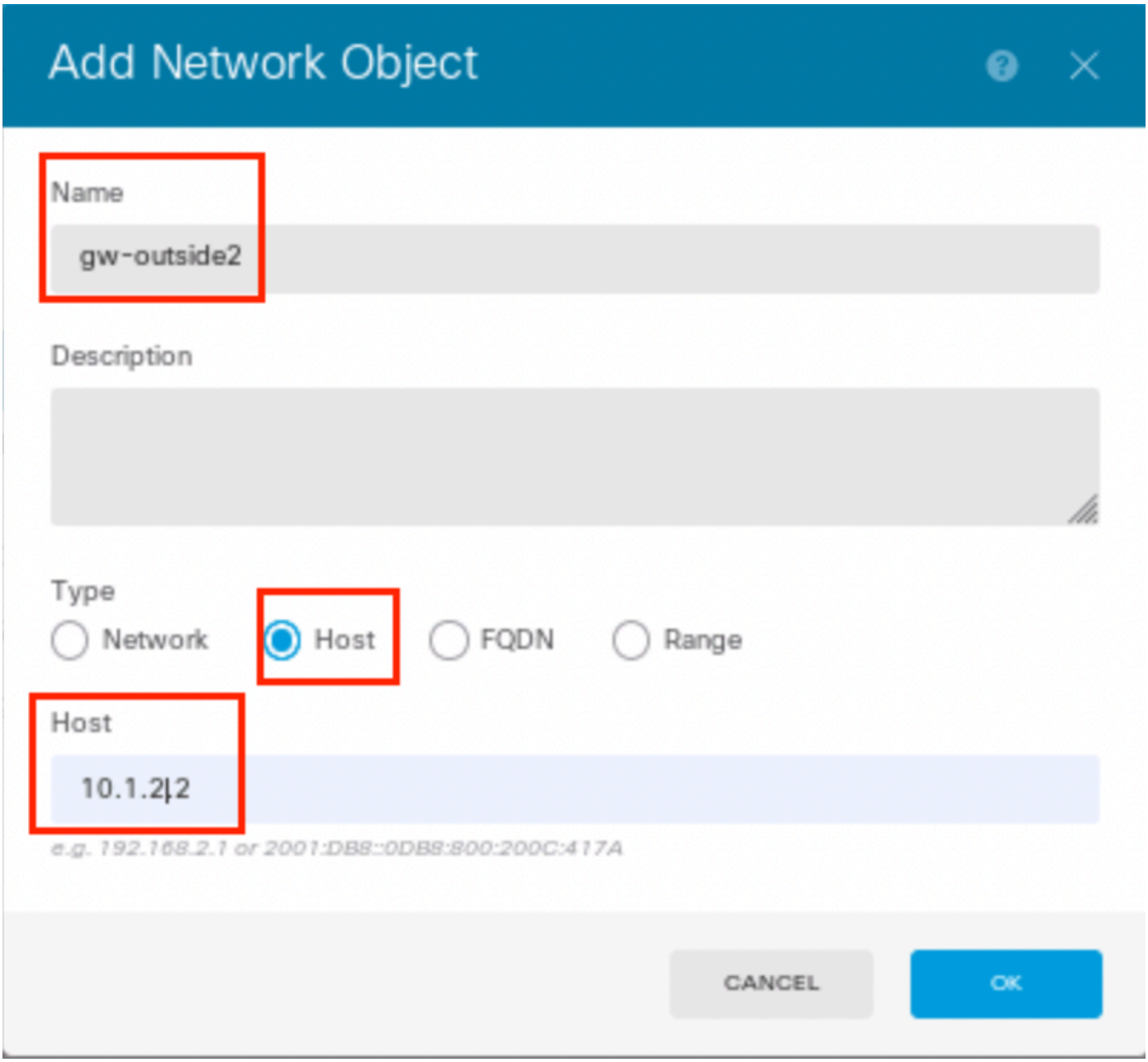
1. Impostare il Nome dell'oggetto, in questo caso gw-outside1.
2. Selezionare il tipo dell'oggetto, in questo caso Host.
3. Impostare l'indirizzo IP dell'host, in questo caso 10.1.1.2.
4. Fare clic su OK.



Fase 0 Oggetto2

Ripetere la procedura simile per configurare un altro oggetto di rete per il secondo gateway ISP:

1. Impostare il Nome dell'oggetto, in questo caso gw-outside2.
2. Selezionare il tipo dell'oggetto, in questo caso Host.
3. Impostare l'indirizzo IP dell'host, in questo caso 10.1.2.2.
4. Fare clic su OK.

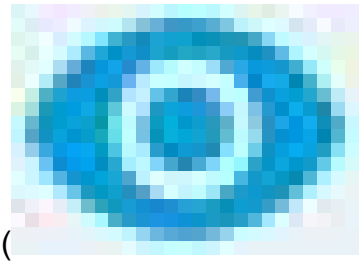


Fase 0 Oggetto3

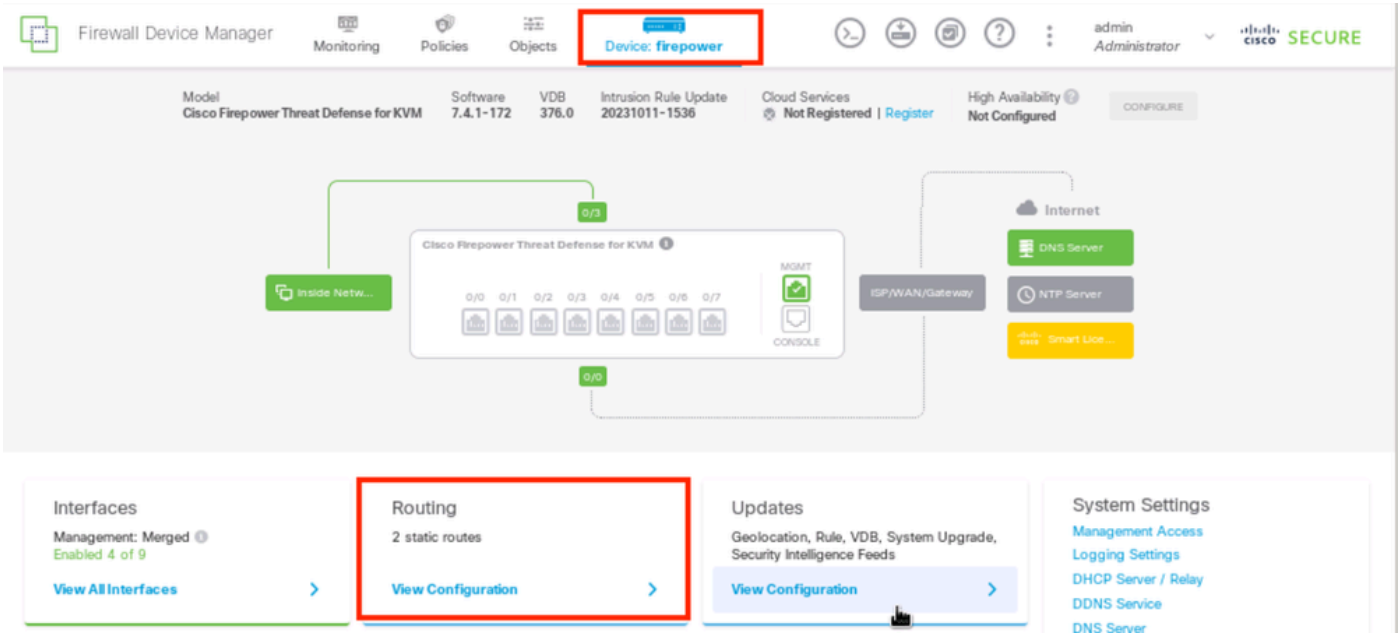
Nota: per autorizzare il traffico, è necessario che la policy di controllo dell'accesso sia configurata su FTD. Questa parte non è inclusa nel presente documento.

Passaggio 1. Configura zona ECMP

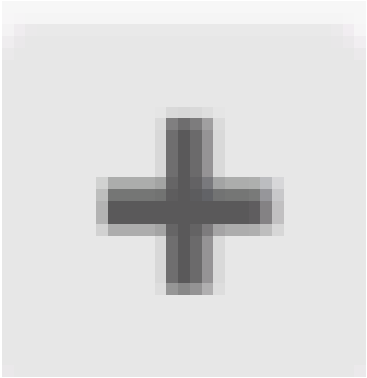
Passare a Periferica, quindi fare clic sul collegamento nel riepilogo Instradamento.



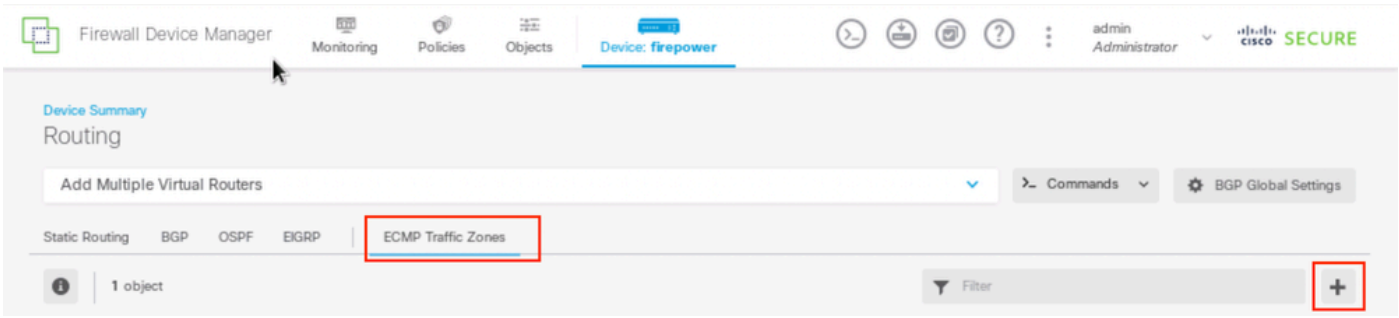
Se sono stati abilitati i router virtuali, fare clic sull'icona di visualizzazione ( ) del router in cui si sta configurando una route statica. In questo caso, i router virtuali non sono abilitati.



Fase 1 ECMP Zone1



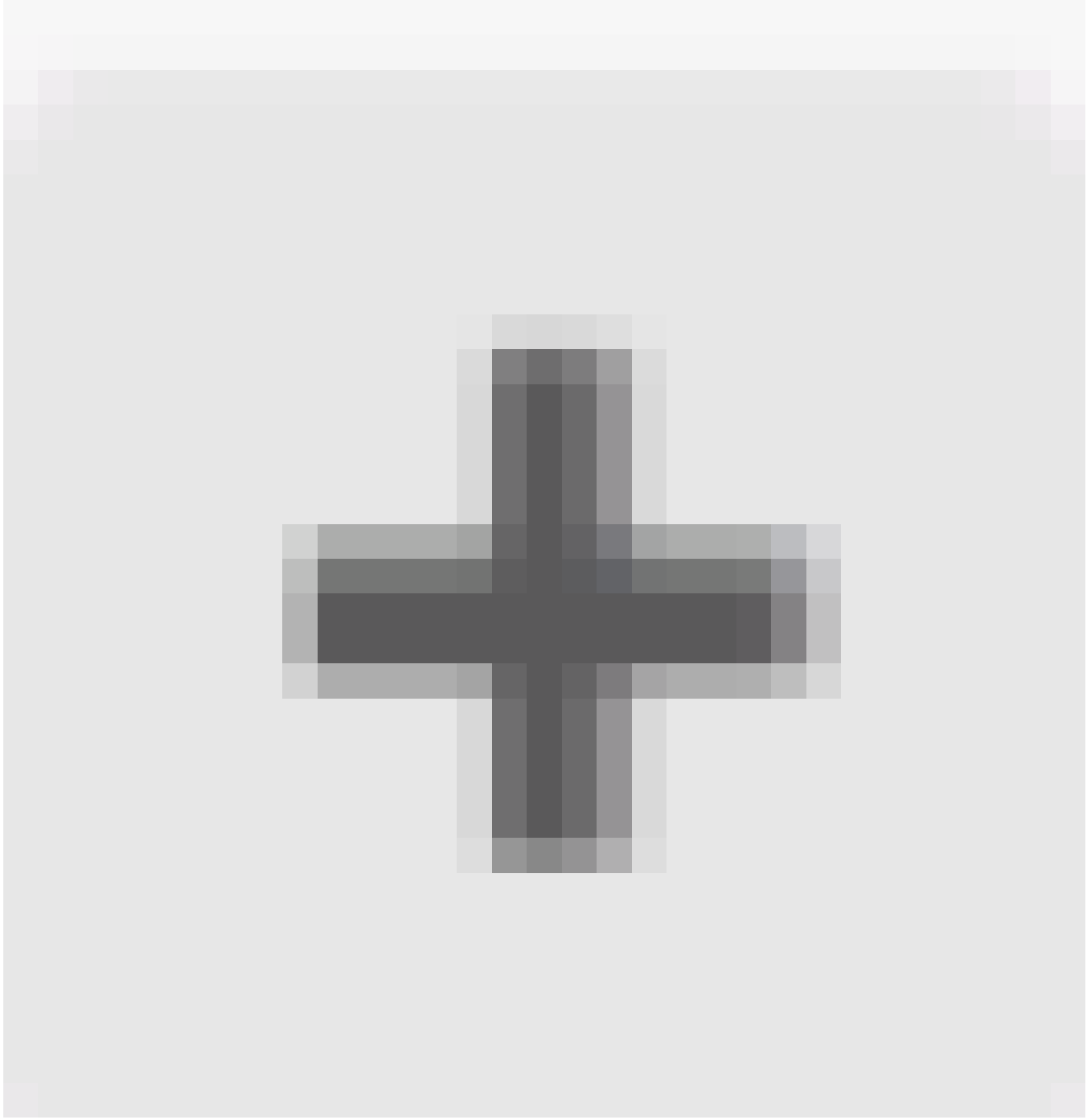
Fare clic sulla scheda Zone traffico ECMP, quindi sull'icona di aggiunta ( ) per aggiungere una nuova zona.



Fase 1 ECMP Zone2

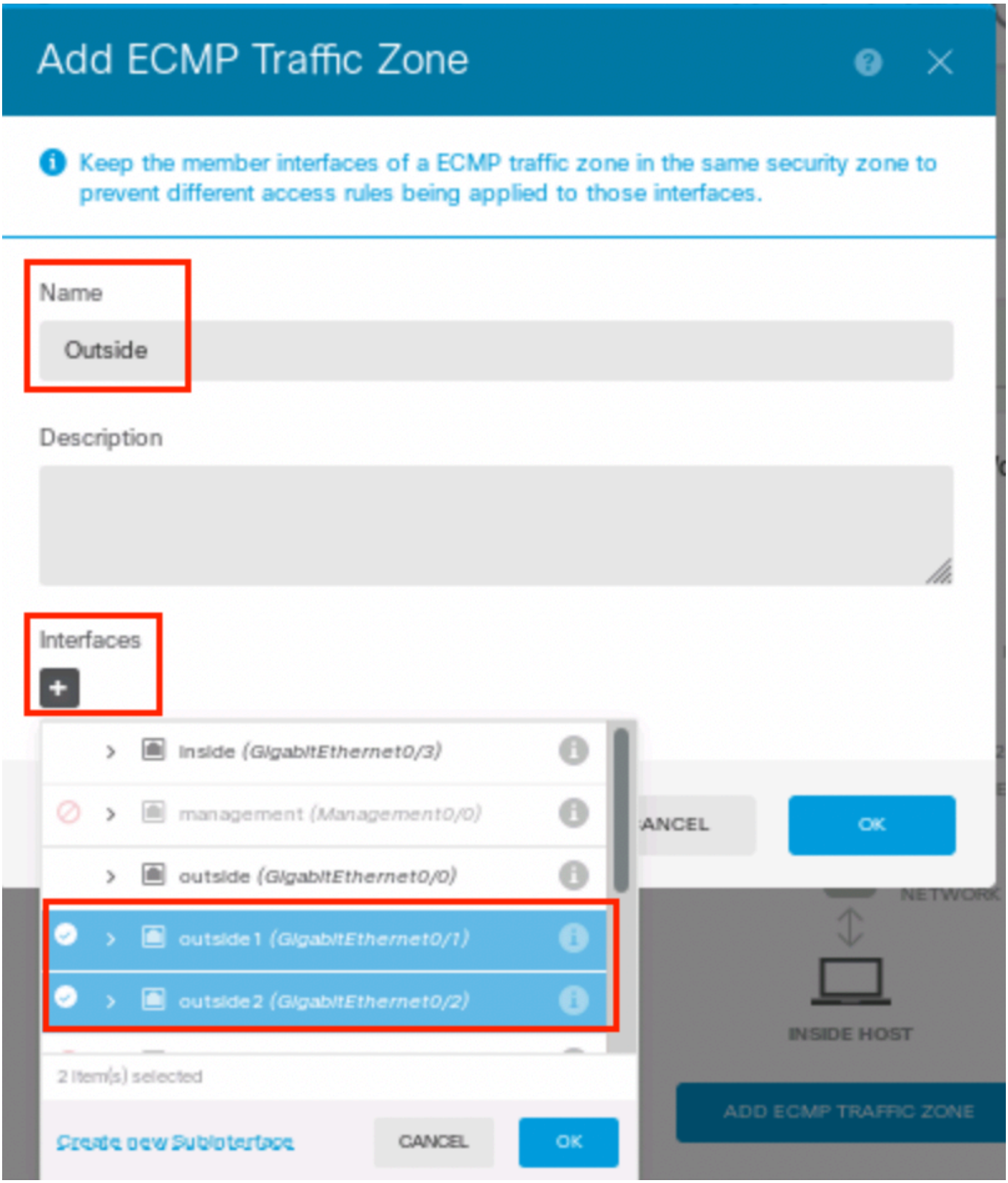
Nella finestra Aggiungi zona traffico ECMP:

1. Impostare il Nome per la zona ECMP e, facoltativamente, una descrizione.
2. Fare clic sull'icona Aggiungi (



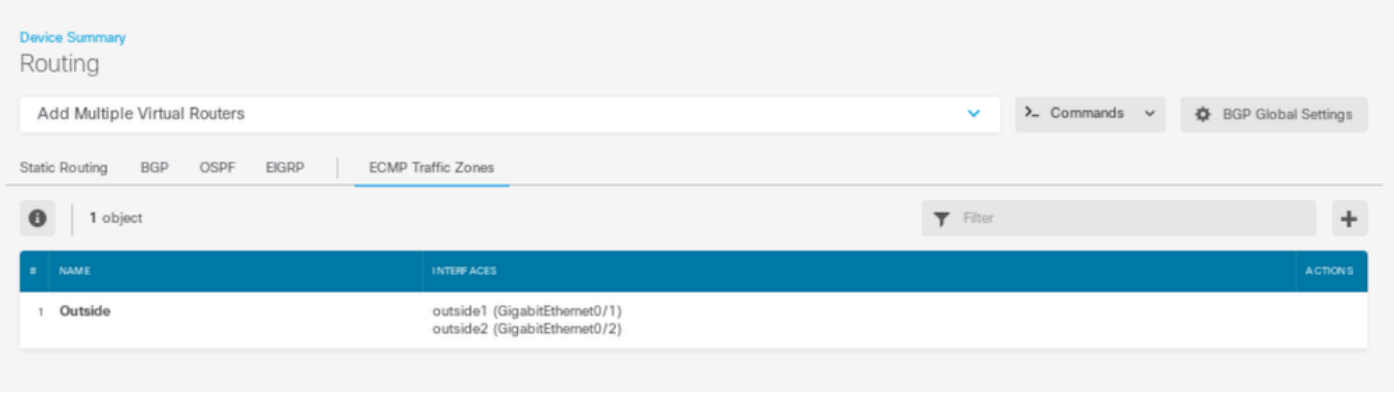
) per selezionare fino a 8 interfacce da includere nella zona. In questo esempio, il nome ECMP è Esterno (Outside), le interfacce esterne1 e esterne2 vengono aggiunte alla zona.

3. Fare clic su OK.

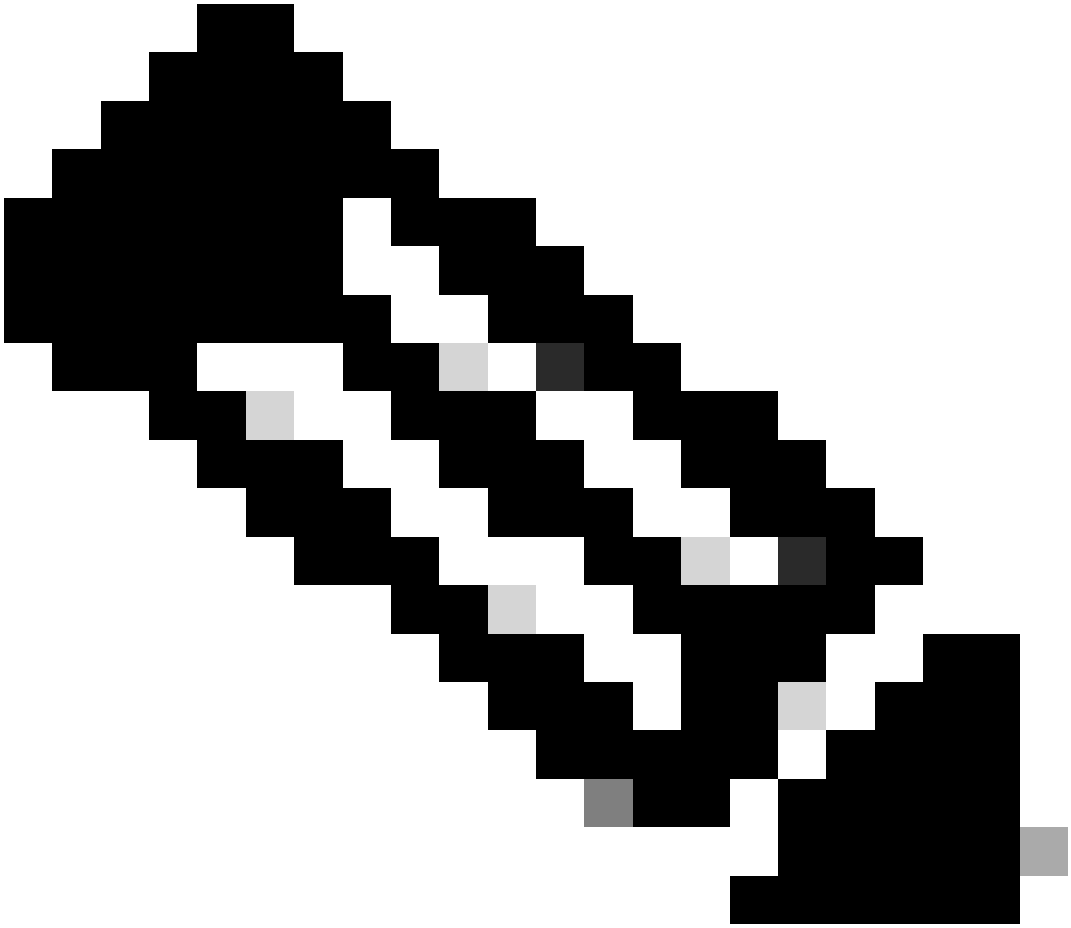


Fase 1 ECMP Zone3

Entrambe le interfacce esterne1 ed esterne2 sono state aggiunte alla zona ECMP all'esterno.



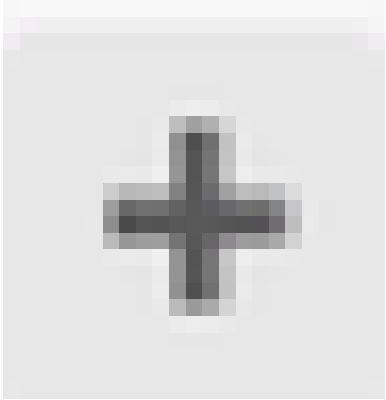
Fase 1: ECMP Zone4



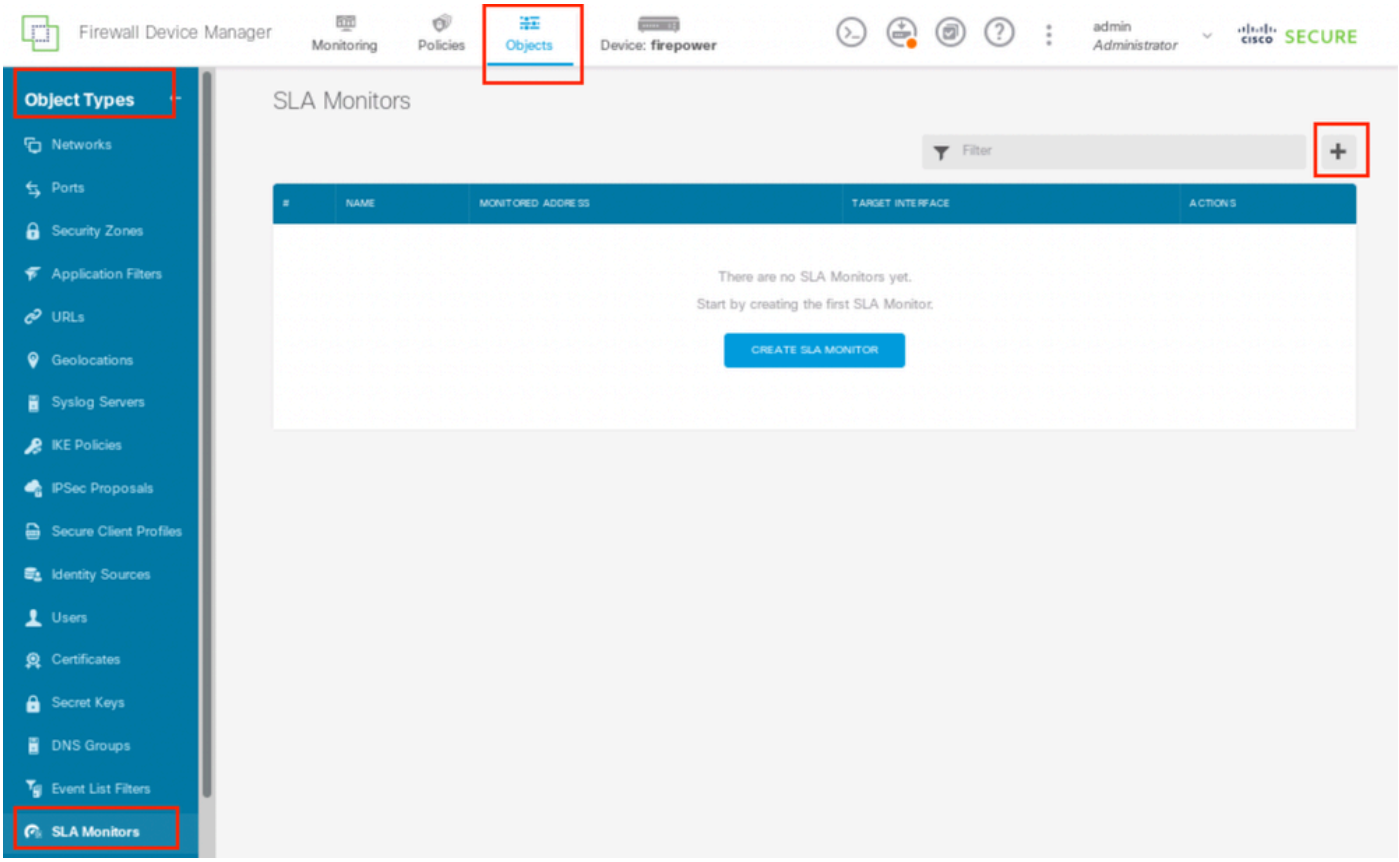
Nota: un'area di traffico di routing ECMP non è correlata alle aree di sicurezza. La creazione di un'area di sicurezza che contiene le interfacce outside1 e outside2 non implementa un'area di traffico per il routing ECMP.

Passaggio 2. Configura oggetti SLA IP

Per definire gli oggetti SLA utilizzati per monitorare la connettività a ciascun gateway, selezionare



Oggetti > Tipi di oggetto > Monitor SLA, fare clic sull'icona di aggiunta ( ) per aggiungere un nuovo monitor SLA per la prima connessione ISP.



Fase 2: IP SLA1

Nella finestra Aggiungi oggetto di monitoraggio SLA:

1. Impostare il Nome per l'oggetto di monitoraggio del contratto di servizio e, facoltativamente, una descrizione, in questo caso sla-outside1.
2. Impostare l'indirizzo del monitor, in questo caso gw-external1 (il primo gateway ISP).
3. Impostare l'interfaccia di destinazione attraverso la quale è possibile raggiungere l'indirizzo del monitor, in questo caso esternamente a 1.
4. Inoltre, è possibile regolare il timeout e la soglia. Fare clic su OK.

Add SLA Monitor Object

Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

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

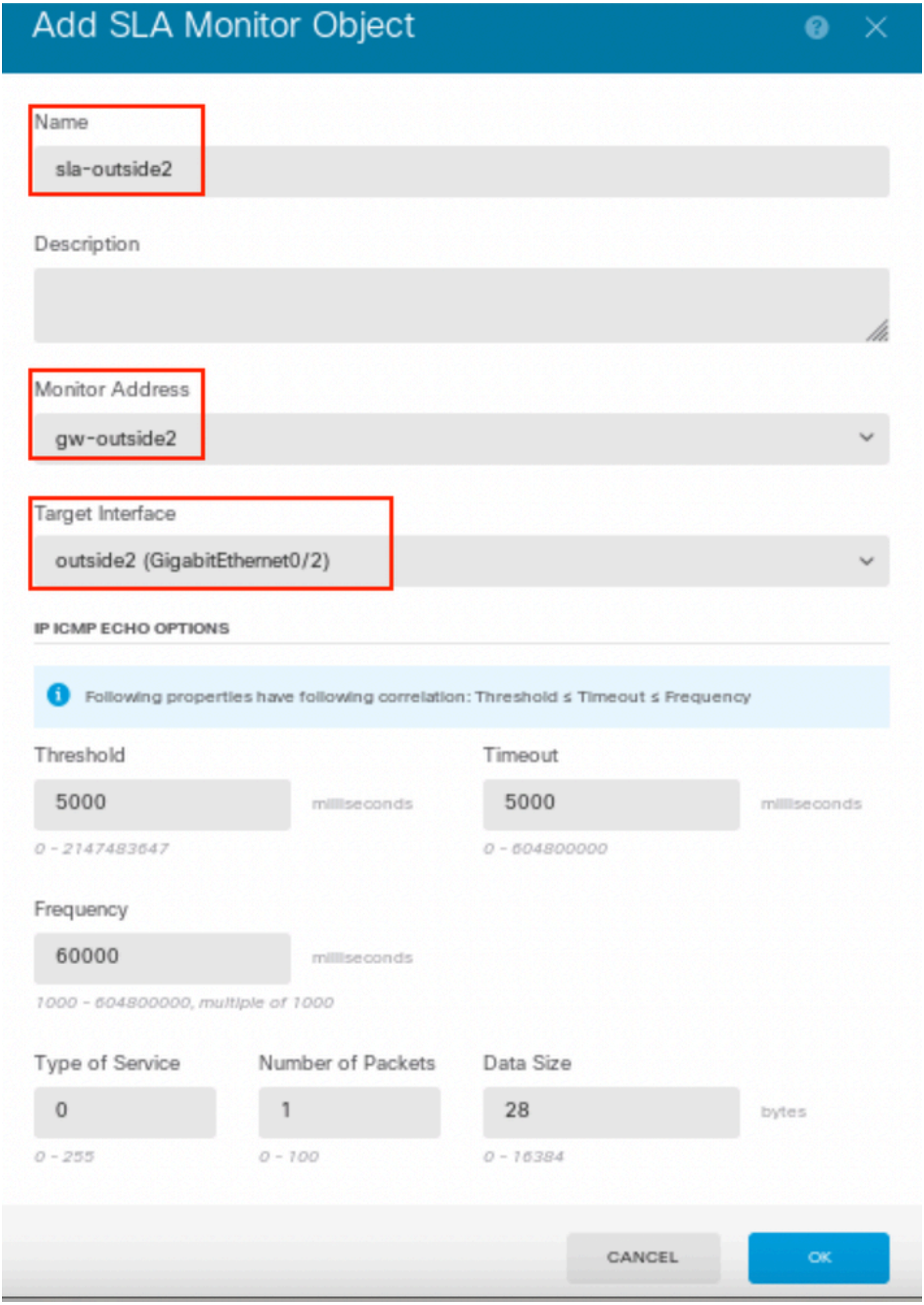
28 bytes

0 - 16384

CANCEL OK

Ripetere la procedura simile per configurare un altro oggetto di monitoraggio SLA per la seconda connessione ISP, nella finestra Aggiungi oggetto di monitoraggio SLA:

1. Impostare il Nome per l'oggetto di monitoraggio dello SLA e, facoltativamente, una descrizione, in questo caso sla-outside2.
2. Impostare l'indirizzo del monitor, in questo caso gw-outside2 (il secondo gateway ISP).
3. Impostare l'interfaccia di destinazione attraverso la quale è possibile raggiungere l'indirizzo del monitor, in questo caso esterno2.
4. Inoltre, è possibile regolare il timeout e la soglia. Fare clic su OK.

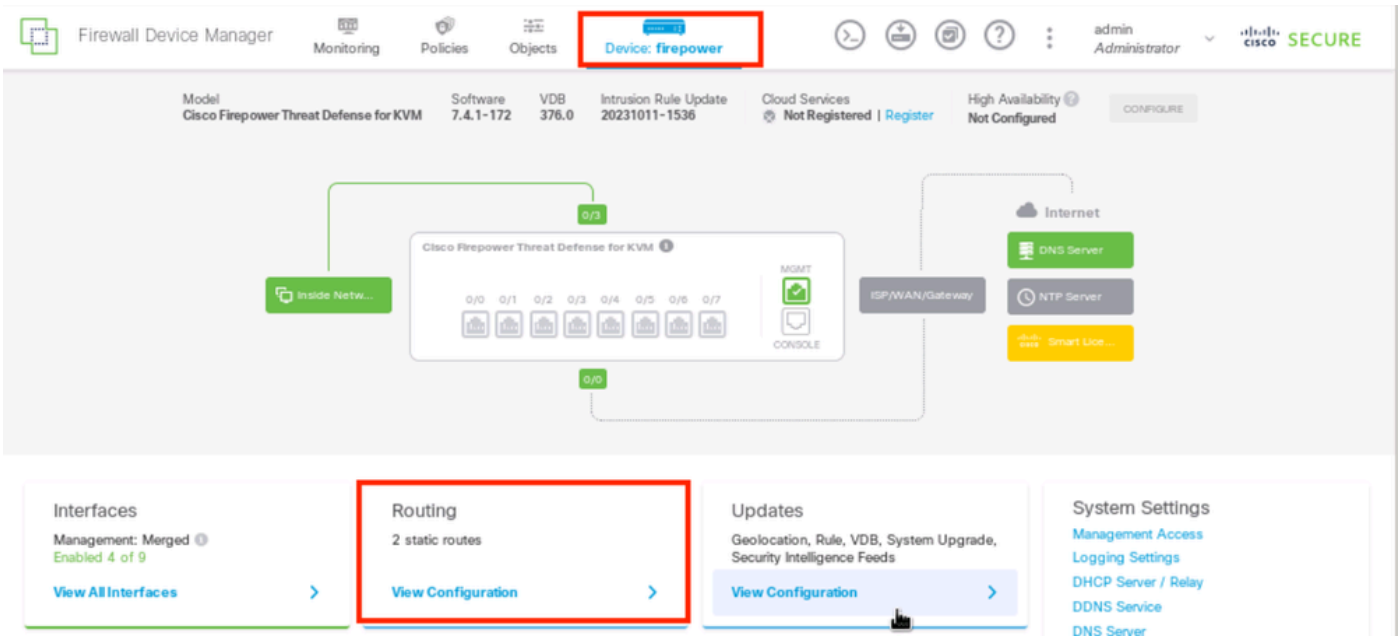

Add SLA Monitor Object
Name
sla-outside2
Description
Monitor Address
gw-outside2
Target Interface
outside2 (GigabitEthernet0/2)
IP ICMP ECHO OPTIONS
Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency
Threshold
5000
milliseconds
0 - 2147483647
Timeout
5000
milliseconds
0 - 604800000
Frequency
60000
milliseconds
1000 - 604800000, multiple of 1000
Type of Service
0
0 - 255
Number of Packets
1
0 - 100
Data Size
28
bytes
0 - 16384
CANCEL
OK

Fase 2: IP SLA3

Passaggio 3. Configura route statiche con route

Passare a Periferica, quindi fare clic sul collegamento nel riepilogo Instradamento.

Se sono stati abilitati i router virtuali, fare clic sull'icona di visualizzazione ( ) del router in cui si sta configurando una route statica. In questo caso, i router virtuali non sono abilitati.

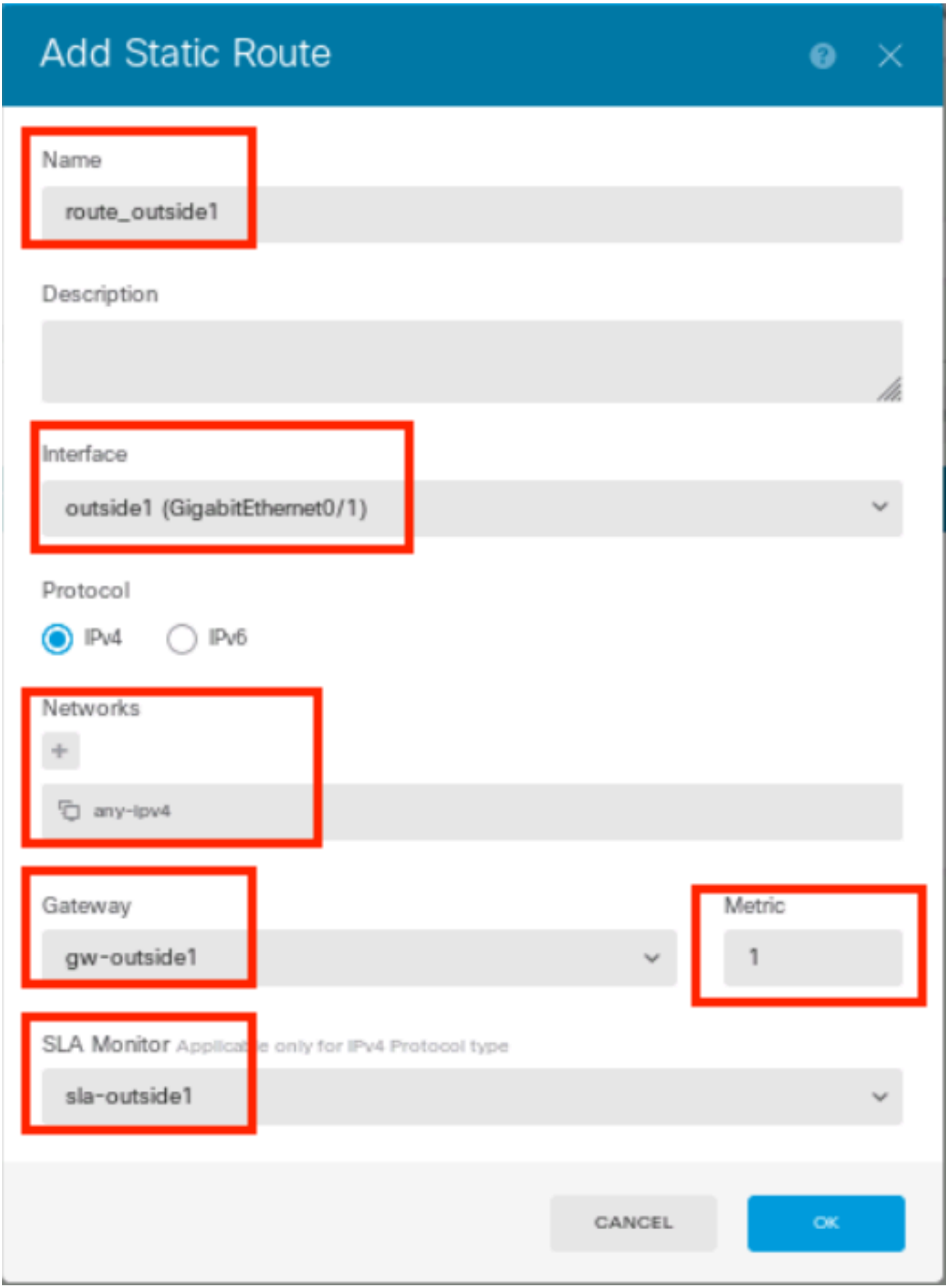


Fase 3 Route1

Nella pagina Instradamento statico fare clic sull'icona di aggiunta ( ) per aggiungere una nuova route statica per il primo collegamento dell'ISP.

Nella finestra Aggiungi instradamento statico:

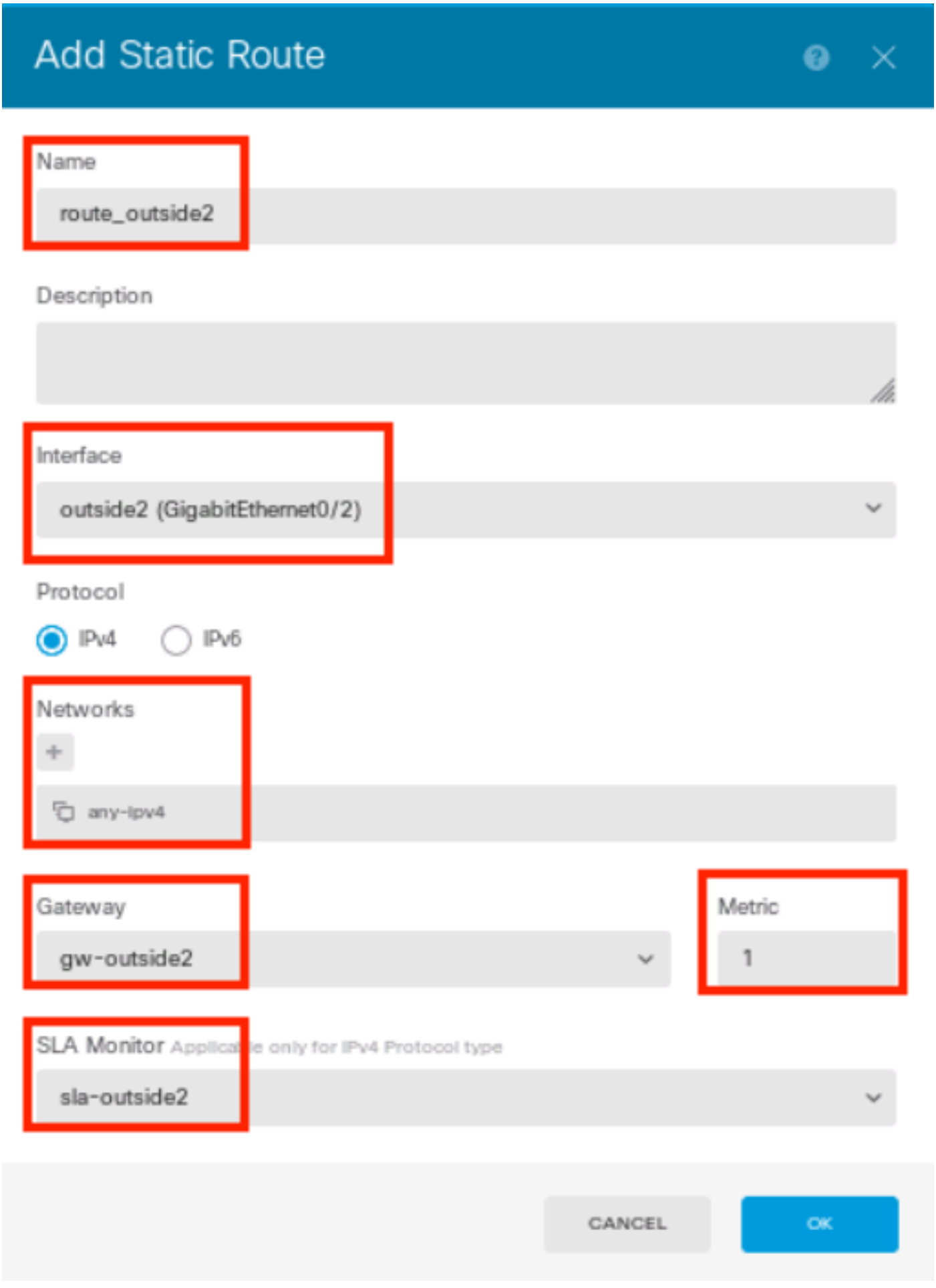
1. Impostare il nome della route e, facoltativamente, la descrizione. In questo caso, route_outside1.
2. Dall'elenco a discesa Interface (Interfaccia), selezionare l'interfaccia attraverso la quale si desidera inviare il traffico. L'indirizzo del gateway deve essere accessibile tramite l'interfaccia. In questo caso, all'esterno di 1 (Gigabit Ethernet0/1).
3. Selezionare le reti che identificano le reti o gli host di destinazione che utilizzano il gateway in questa route. In questo caso, usare il protocollo predefinito any-ipv4.
4. Dall'elenco a discesa Gateway, selezionare l'oggetto di rete che identifica l'indirizzo IP del gateway. Il traffico verrà inviato a questo indirizzo. In questo caso gw-outside1 (il primo gateway ISP).
5. Impostare la metrica della route su un valore compreso tra 1 e 254. In questo esempio 1.
6. Dall'elenco a discesa Monitor contratto di servizio selezionare l'oggetto di monitoraggio del contratto di servizio. In questo caso sla-outside1.
7. Fare clic su OK.



Fase 3 Route2

Ripetere la procedura simile per configurare un'altra route statica per la seconda connessione ISP, nella finestra Aggiungi route statica:

1. Impostare il nome della route e, facoltativamente, la descrizione. In questo caso, route_outside2.
2. Dall'elenco a discesa Interface (Interfaccia), selezionare l'interfaccia attraverso la quale si desidera inviare il traffico. L'indirizzo del gateway deve essere accessibile tramite l'interfaccia. In questo caso, all'esterno2 (Gigabit Ethernet0/2).
3. Selezionare le reti che identificano le reti o gli host di destinazione che utilizzano il gateway in questa route. In questo caso, usare il protocollo predefinito any-ipv4.
4. Dall'elenco a discesa Gateway, selezionare l'oggetto di rete che identifica l'indirizzo IP del gateway. Il traffico verrà inviato a questo indirizzo. In questo caso, gw-outside2 (il secondo gateway ISP).
5. Impostare la metrica della route su un valore compreso tra 1 e 254. In questo esempio 1.
6. Dall'elenco a discesa Monitor contratto di servizio selezionare l'oggetto di monitoraggio del contratto di servizio. In questo scenario, sla-outside2.
7. Fare clic su OK.



Fase 3 Route3

Sono disponibili 2 route tramite l'interfaccia esterna1 e esterna2 con route track.

Fase 3. Instradamento 4

Distribuire la modifica in FTD.

Verifica

Accedere alla CLI dell'FTD, eseguire il comando show zone per controllare le informazioni sulle zone di traffico ECMP, incluse le interfacce che fanno parte di ciascuna zona.

```
<#root>

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

Zone member(s): 2

 outside2 GigabitEthernet0/2

outside1 GigabitEthernet0/1
```

Eseguire il comando show running-config route per verificare la configurazione in esecuzione per la configurazione di routing, in questo caso sono disponibili due route statiche con route track.

```
<#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

Eseguire il comando show route per verificare la tabella di routing. In questo caso, saranno disponibili due route predefinite tramite l'interfaccia outside1 e outside2, con lo stesso costo. Il traffico può essere distribuito tra due circuiti ISP.

<#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
```

Eseguire il comando show sla monitor configuration per verificare la configurazione del monitor del contratto di servizio.

<#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:
```

Eseguire il comando show sla monitor operational-state per confermare lo stato del monitor del contratto di servizio. In questo caso, se l'output del comando restituisce "Timeout: FALSE", l'eco ICMP sul gateway sta rispondendo, quindi il percorso predefinito attraverso l'interfaccia di destinazione è attivo e installato nella tabella di routing.

<#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

Bilanciamento del carico

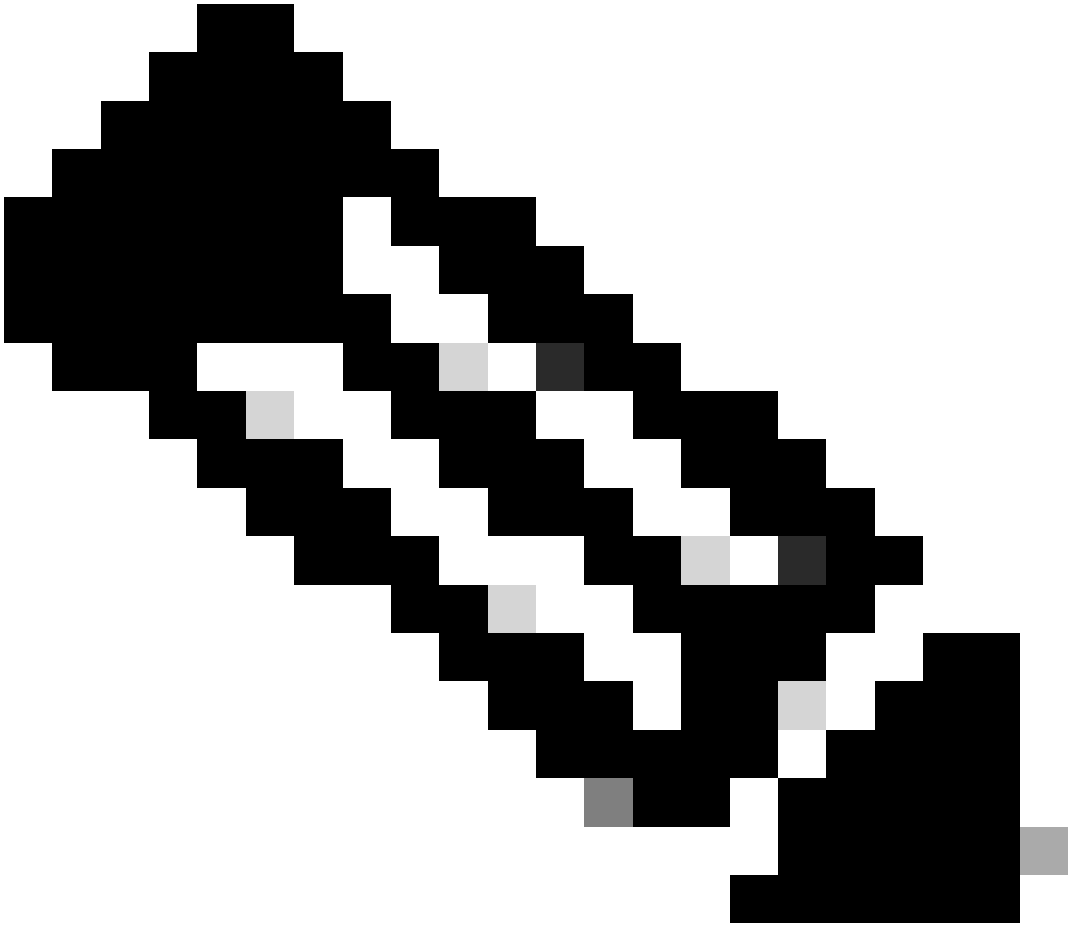
Traffico iniziale attraverso FTD per verificare se il carico ECMP bilancia il traffico tra i gateway nella zona ECMP. In questo caso, avviare la connessione SSH da Test-PC-1 (10.1.3.2) e Test-PC-2 (10.1.3.4) verso Internet-Host (10.1.5.2), eseguire il comando show conn per verificare che il traffico tra due collegamenti ISP sia bilanciato dal carico, mentre Test-PC-1 (10.1.3.2) passa attraverso l'interfaccia esterna1, Test-PC-2 (10.1.3.4) passa attraverso l'interfaccia esterna2.

<#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



Nota: il traffico viene bilanciato dal carico tra i gateway specificati in base a un algoritmo che incapsula gli indirizzi IP di origine e di destinazione, l'interfaccia in entrata, il protocollo, le porte di origine e di destinazione. quando si esegue il test, il traffico simulato può essere instradato allo stesso gateway a causa dell'algoritmo hash. In base alle previsioni, modificare qualsiasi valore tra le 6 tuple (IP di origine, IP di destinazione, interfaccia in entrata, protocollo, porta di origine, porta di destinazione) per apportare modifiche al risultato dell'hash.

Route persa

Se il collegamento al primo gateway ISP è inattivo, in questo caso arrestare il primo router gateway per eseguire la simulazione. Se l'FTD non riceve una risposta echo dal primo gateway ISP entro il timer di soglia specificato nell'oggetto Monitor SLA, l'host viene considerato non raggiungibile e contrassegnato come non attivo. Il percorso tracciato verso il primo gateway viene rimosso anche dalla tabella di routing.

Eseguire il comando show sla monitor operational-state per confermare lo stato corrente di Monitoraggio contratto di servizio. In questo caso,

è possibile trovare "Timeout OCCUR: True" nell'output del comando, per segnalare che l'eco ICMP del primo gateway ISP non risponde.

<#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

Eseguire il comando **show route** per verificare la tabella di routing corrente, la route al primo gateway ISP tramite l'interfaccia esterna1 viene rimossa, esiste solo una route predefinita attiva al secondo gateway ISP tramite l'interfaccia esterna2.

<#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

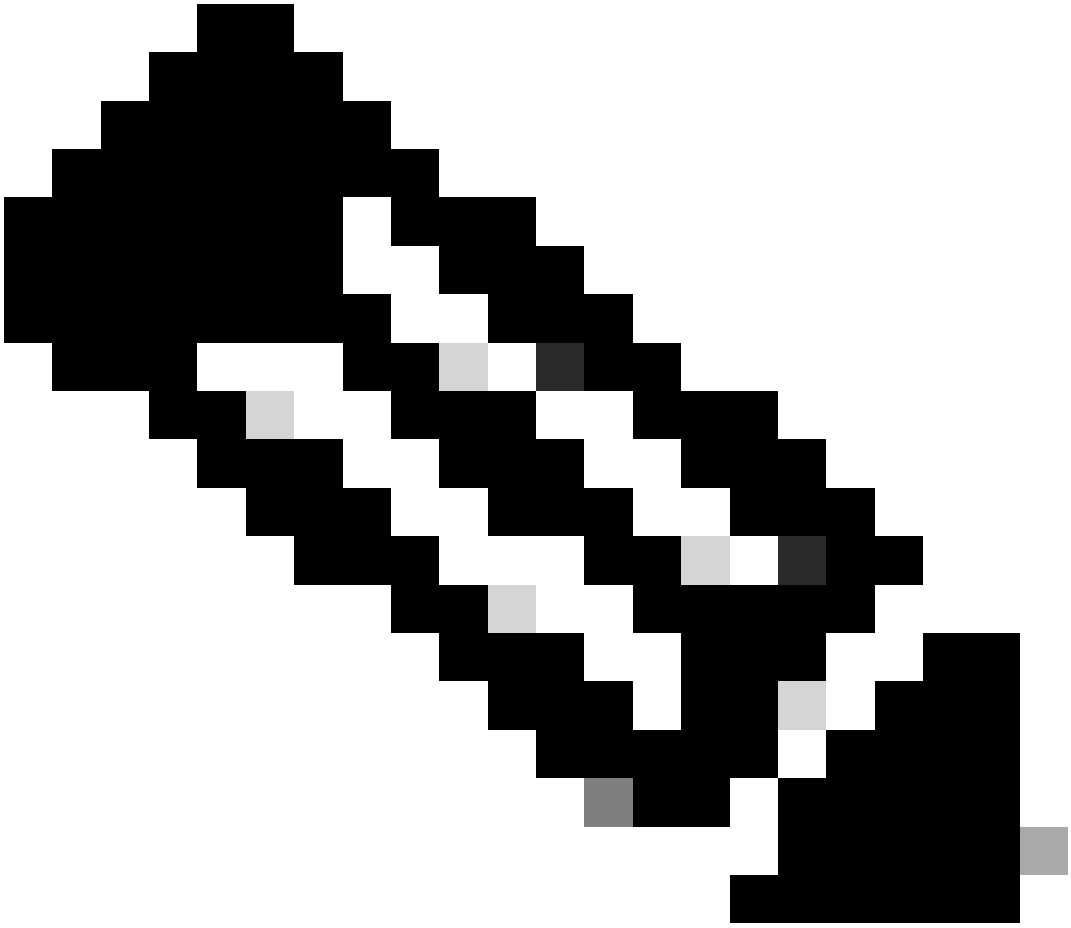
Eseguire il comando show conn per verificare che le due connessioni siano ancora attive. Le sessioni SSH sono attive anche sul Test-PC-1 (10.1.3.2) e sul Test-PC-2 (10.1.3.4) senza interruzioni.

<#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



Nota: come si può notare nell'output di show conn , la sessione SSH di Test-PC-1 (10.1.3.2) utilizza ancora l'interfaccia esterna1, anche se il percorso predefinito che passa attraverso l'interfaccia esterna1 è stato rimosso dalla tabella di routing. In base alle previsioni, il traffico effettivo passa attraverso l'interfaccia esterna2. Se si avvia una nuova connessione da Test-PC-1 (10.1.3.2) a Internet-Host (10.1.5.2), è possibile trovare tutto il traffico attraverso l'interfaccia esterna2.

Risoluzione dei problemi

Per convalidare le modifiche alla tabella di routing, eseguire il comando debug ip routing .

Nell'esempio, quando il collegamento al primo gateway ISP è inattivo, il percorso attraverso l'interfaccia esterna a 1 viene rimosso dalla tabella di routing.

<#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

Eseguire il comando show route per confermare la tabella di routing corrente.

<#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

Quando il collegamento al primo gateway ISP torna attivo, il percorso attraverso l'interfaccia esterna1 viene aggiunto nuovamente alla tabella di routing.

<#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

Eseguire il comando show route per confermare la tabella di routing corrente.

> 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

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).