Configurazione di ECMP con SLA IP su FTD Gestito da FMC

Sommario

Introduzione

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

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 Management Center (FMC)

Componenti usati

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

- Cisco FTD versione 7.4.1

- Cisco FMC versione 7.4.1

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 FMC. 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

- Cisco Secure Firewall Management Center versione 7.1 o successiva

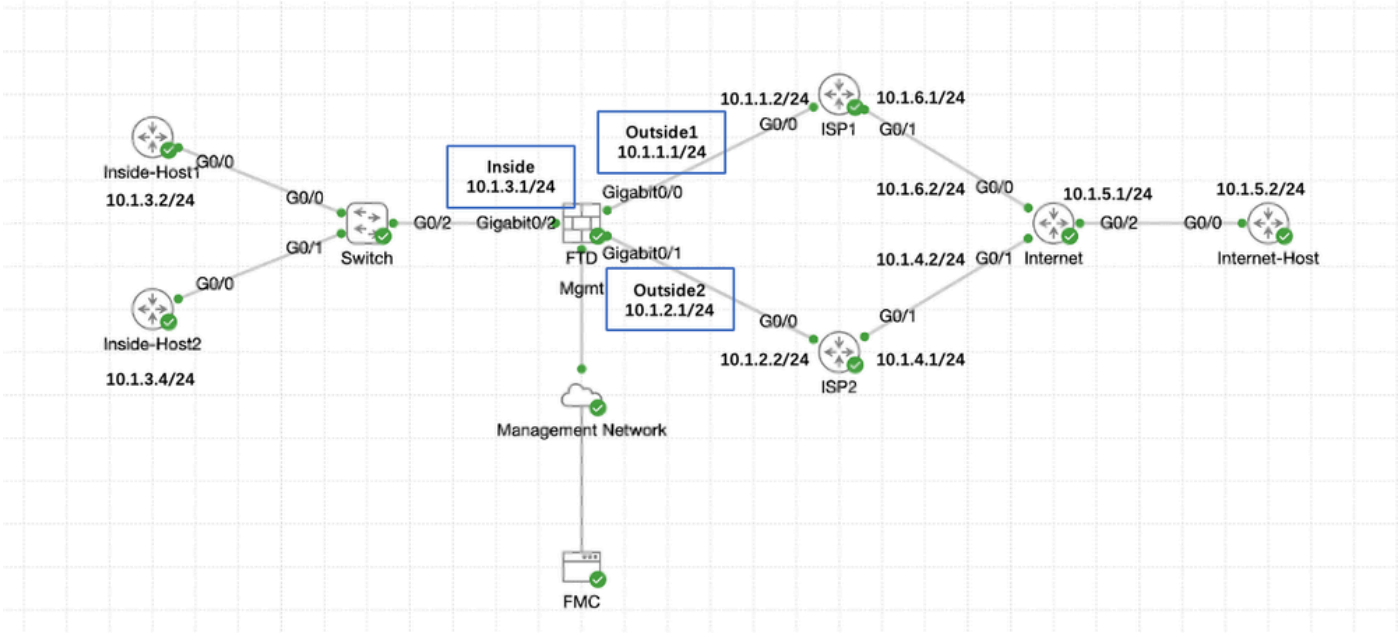
Configurazione

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.

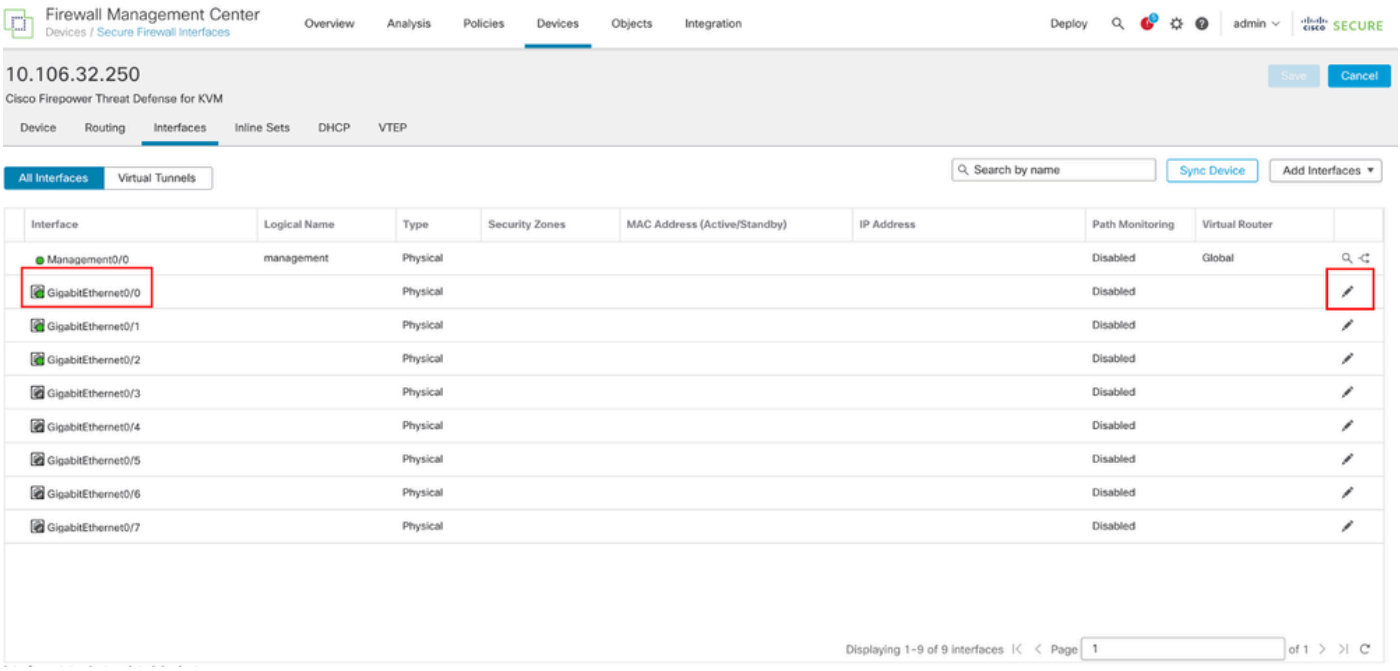


Esempio di rete

Configurazioni

Passaggio 0. Preconfigurazione di interfacce/oggetti di rete

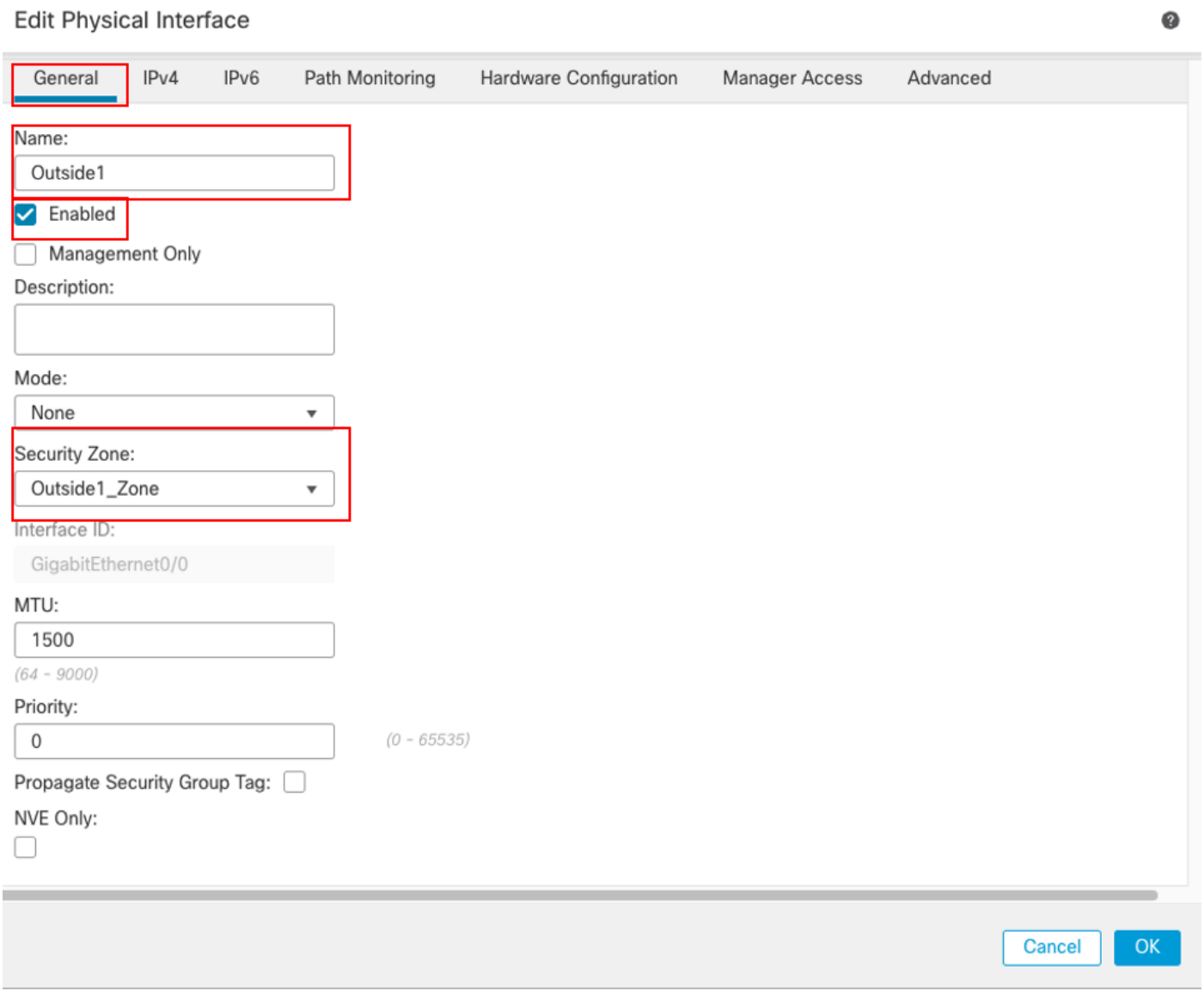
Accedere alla GUI Web di FMC, selezionare Devices>Device Management (Gestione dispositivi) e fare clic sul pulsante Edit (Modifica)per il dispositivo di difesa dalle minacce. La pagina Interfacce è selezionata per impostazione predefinita. Fare clic sul pulsante Edit (Modifica) dell'interfaccia che si desidera modificare, in questo esempio Gigabit Ethernet0/0.



Modifica Interfaccia Gi0/0

Nella scheda Generale della finestra Modifica interfaccia fisica:

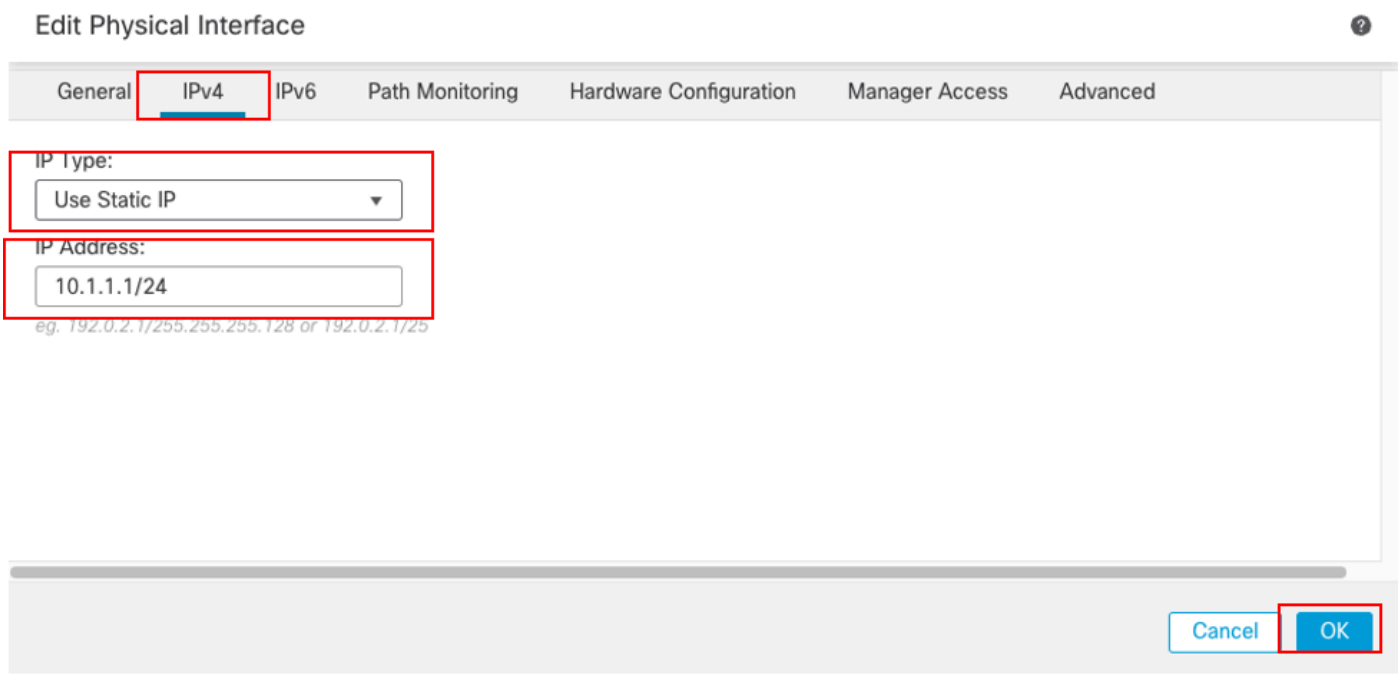
1. Impostare il Nome, in questo caso Esterno1.
2. Abilitare l'interfaccia selezionando la casella di controllo Abilitato.
3. Nell'elenco a discesa Area di protezione selezionare un'area di protezione esistente o crearne una nuova, in questo esempio Outside1_Zone.



Interfaccia Gi0/0 - Generale

Nella scheda IPv4:

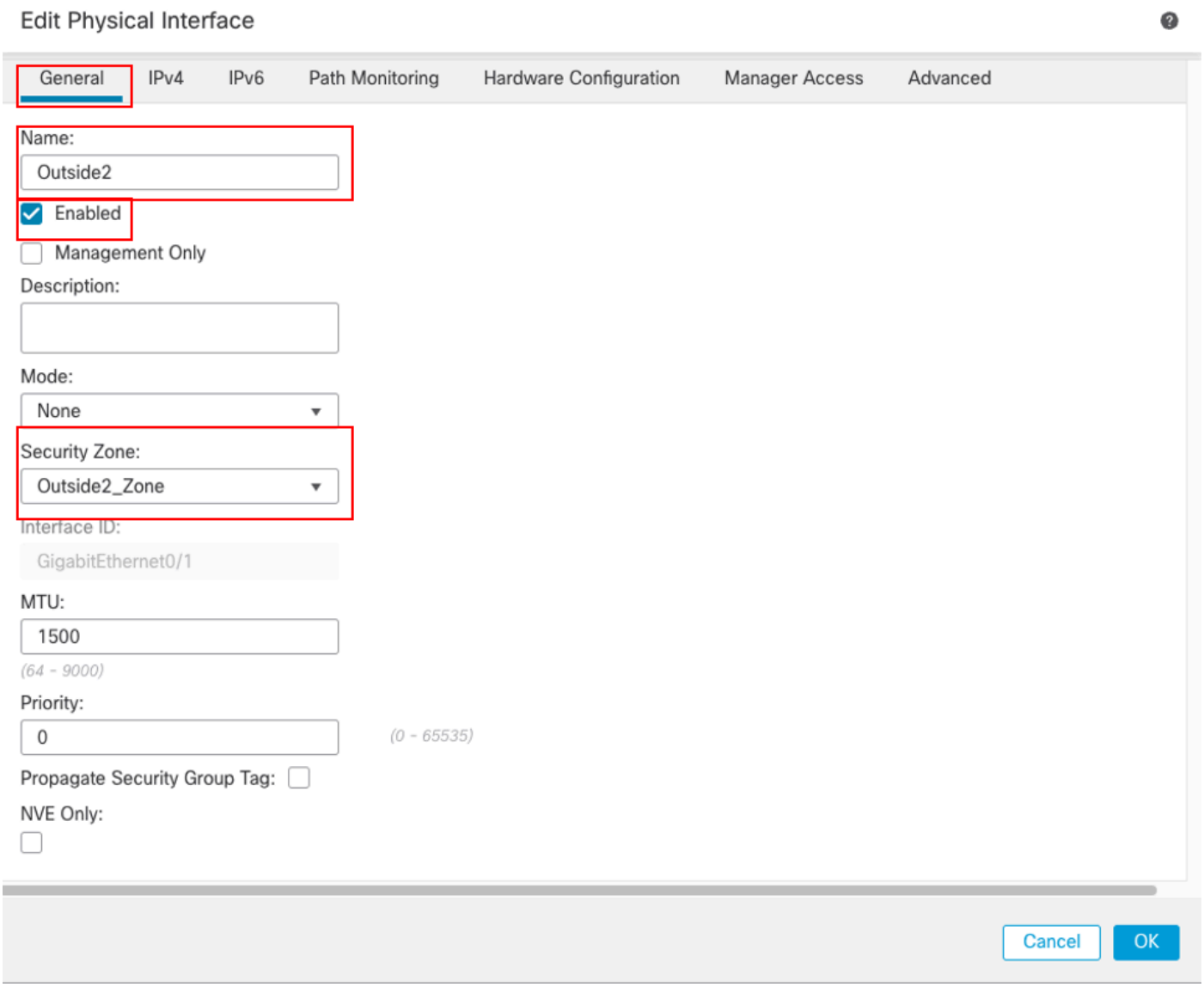
1. Selezionare una delle opzioni dall'elenco a discesa IP Type (Tipo IP), nell'esempio Use Static IP (Usa IP statico).
2. Impostare l'indirizzo IP, in questo esempio 10.1.1.1/24.
3. Fare clic su OK.



Interfaccia Gi0/0 IPv4

Ripetere un passaggio simile per configurare l'interfaccia Gigabit Ethernet0/1, nella scheda General della finestra Edit Physical Interface:

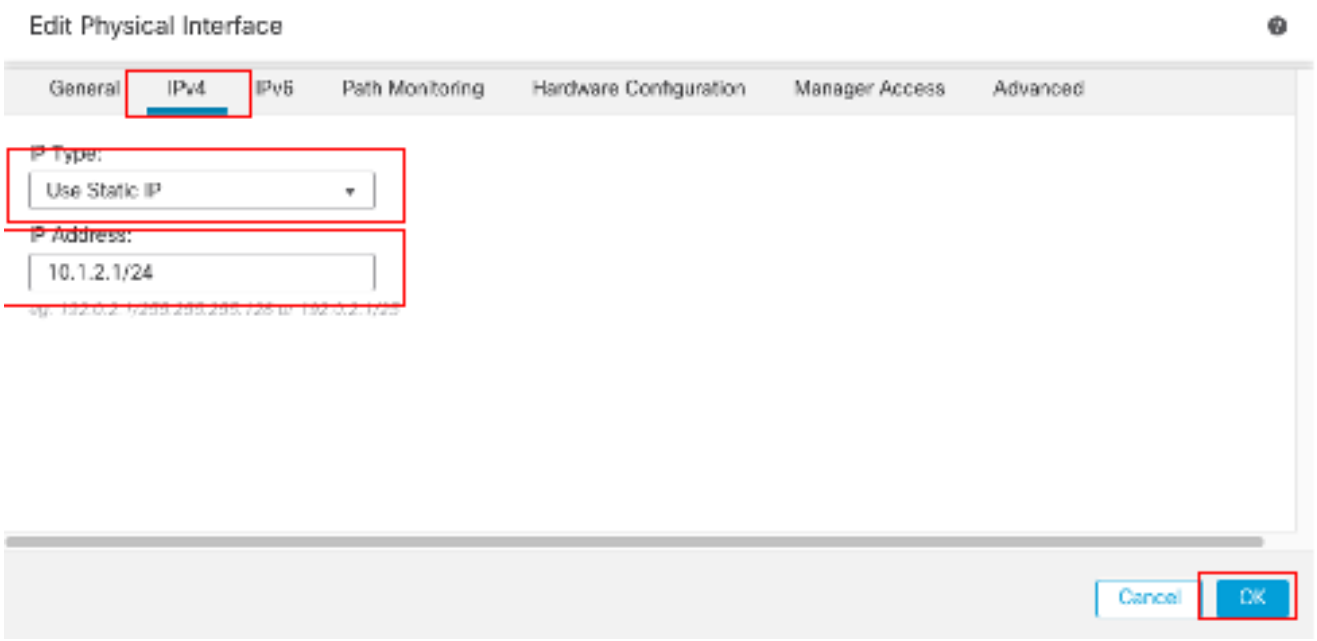
1. Impostare il Nome, in questo caso Esterno2.
2. Abilitare l'interfaccia selezionando la casella di controllo Abilitato.
3. Nell'elenco a discesa Area di sicurezza, selezionare un'area di sicurezza esistente o crearne una nuova, in questo esempio Outside2_Zone.



Interfaccia Gi0/1 - Generale

Nella scheda IPv4:

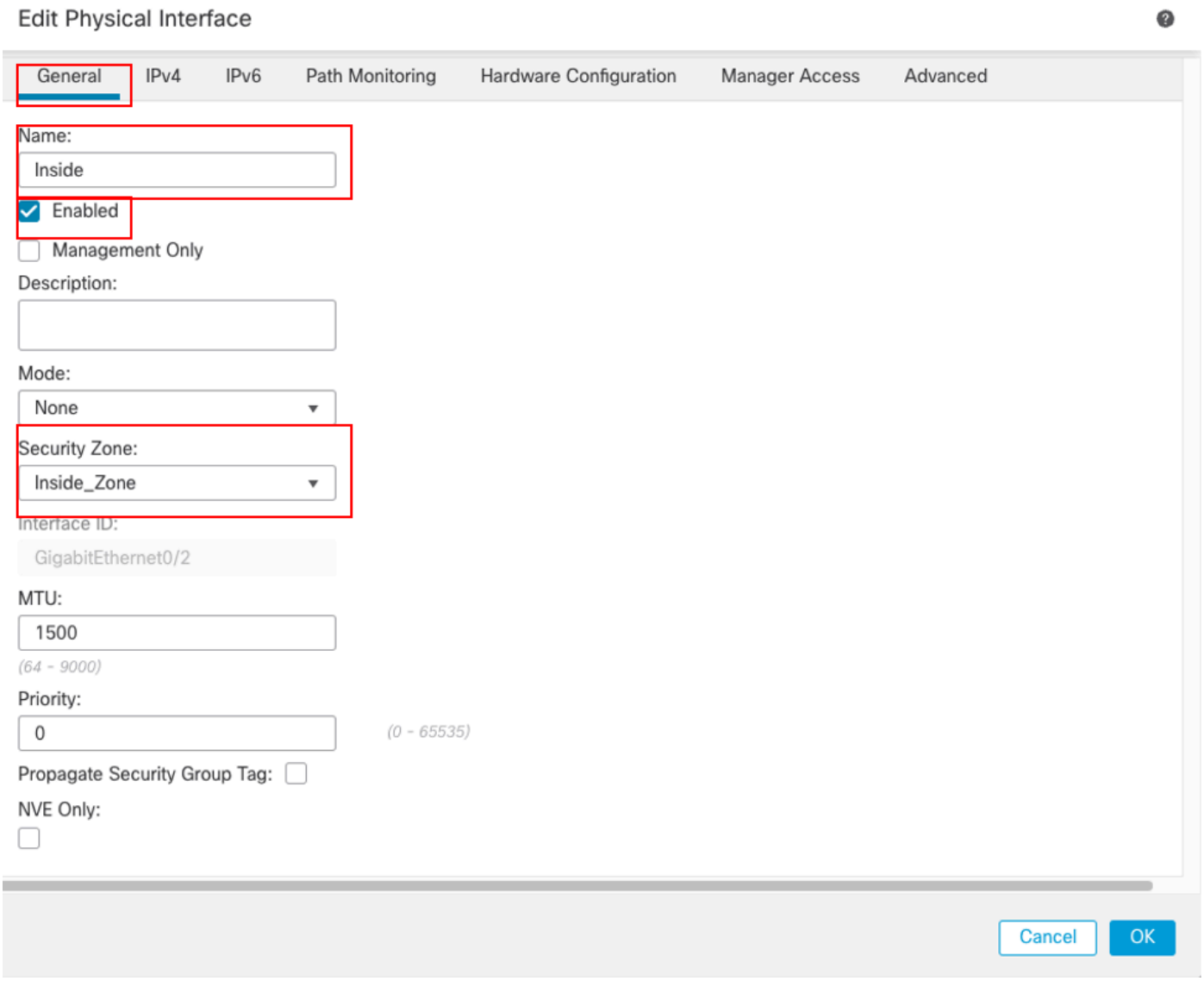
1. Selezionare una delle opzioni dall'elenco a discesa IP Type (Tipo IP), nell'esempio Use Static IP (Usa IP statico).
2. Impostare l'indirizzo IP, in questo esempio 10.1.2.1/24.
3. Fare clic su OK.



Interfaccia Gi0/1 IPv4

Ripetere un passaggio simile per configurare l'interfaccia Gigabit Ethernet0/2, nella finestra Edit Physical Interface (Modifica interfaccia fisica), nella scheda General:

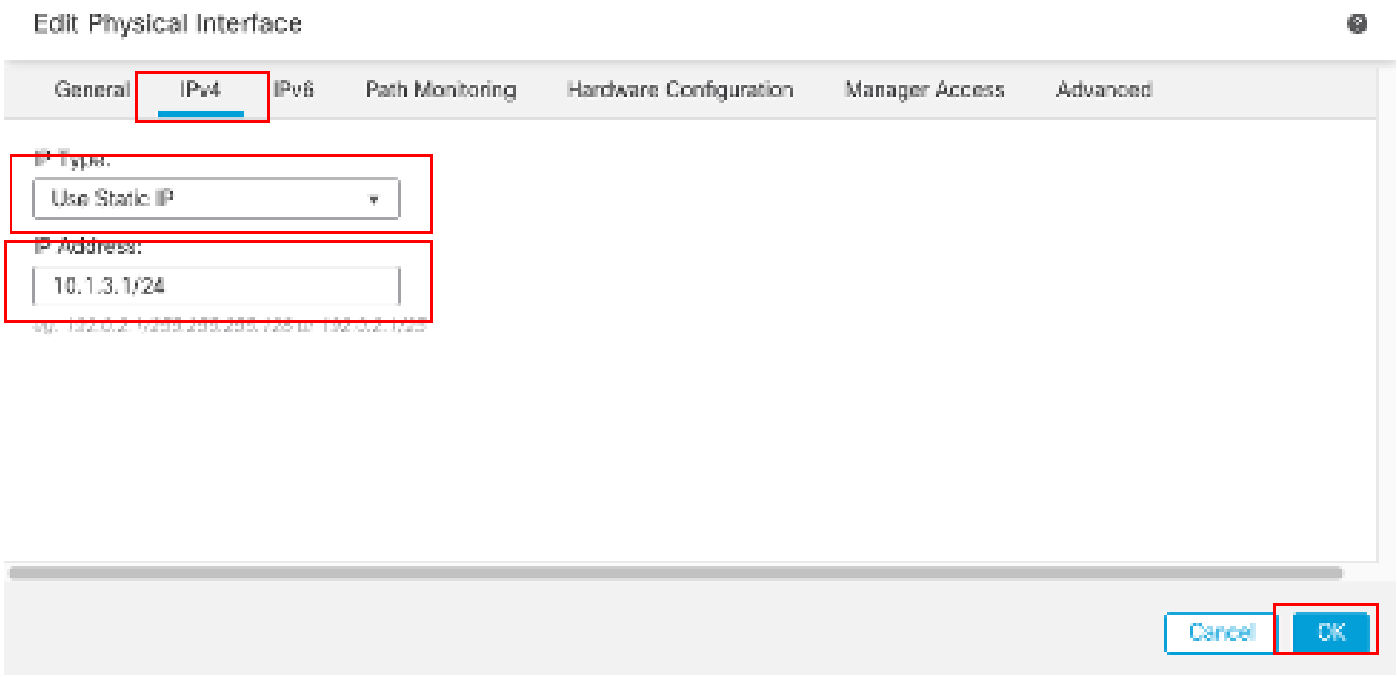
1. Impostare il Nome, in questo caso Interno.
2. Abilitare l'interfaccia selezionando la casella di controllo Abilitato.
3. Nell'elenco a discesa Area di sicurezza, selezionare un'area di sicurezza esistente o crearne una nuova, in questo esempio Inside_Zone.



Interfaccia Gi0/2 - Generale

Nella scheda IPv4:

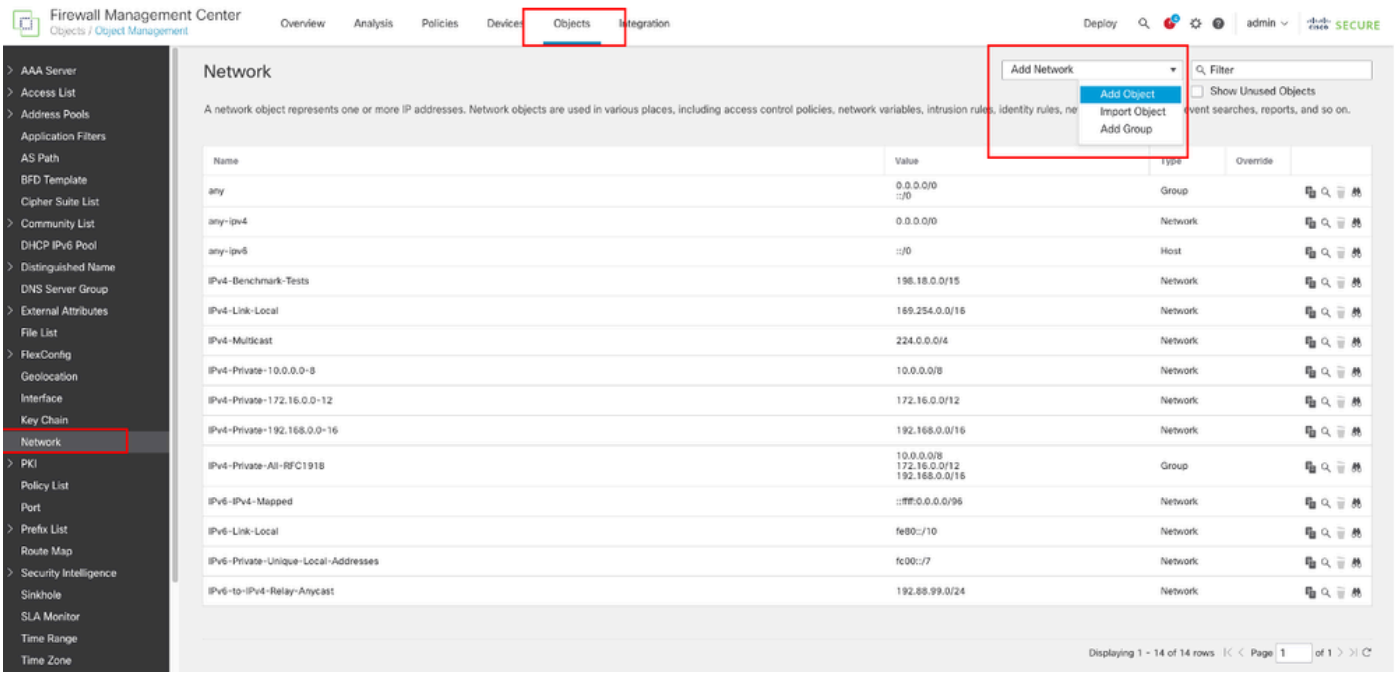
1. Selezionare una delle opzioni dall'elenco a discesa IP Type (Tipo IP), nell'esempio Use Static IP (Usa IP statico).
2. Impostare l'indirizzo IP, in questo esempio 10.1.3.1/24.
3. Fare clic su OK.



Interfaccia Gi0/2 IPv4

Fare clic su Save and Deploy the configuration (Salva e distribuisci).

Passare a Oggetti > Gestione oggetti, Scegliere Rete dall'elenco dei tipi di oggetto, Scegliere Aggiungi oggetto dal menu a discesa Aggiungi rete per creare un oggetto per il primo gateway ISP.

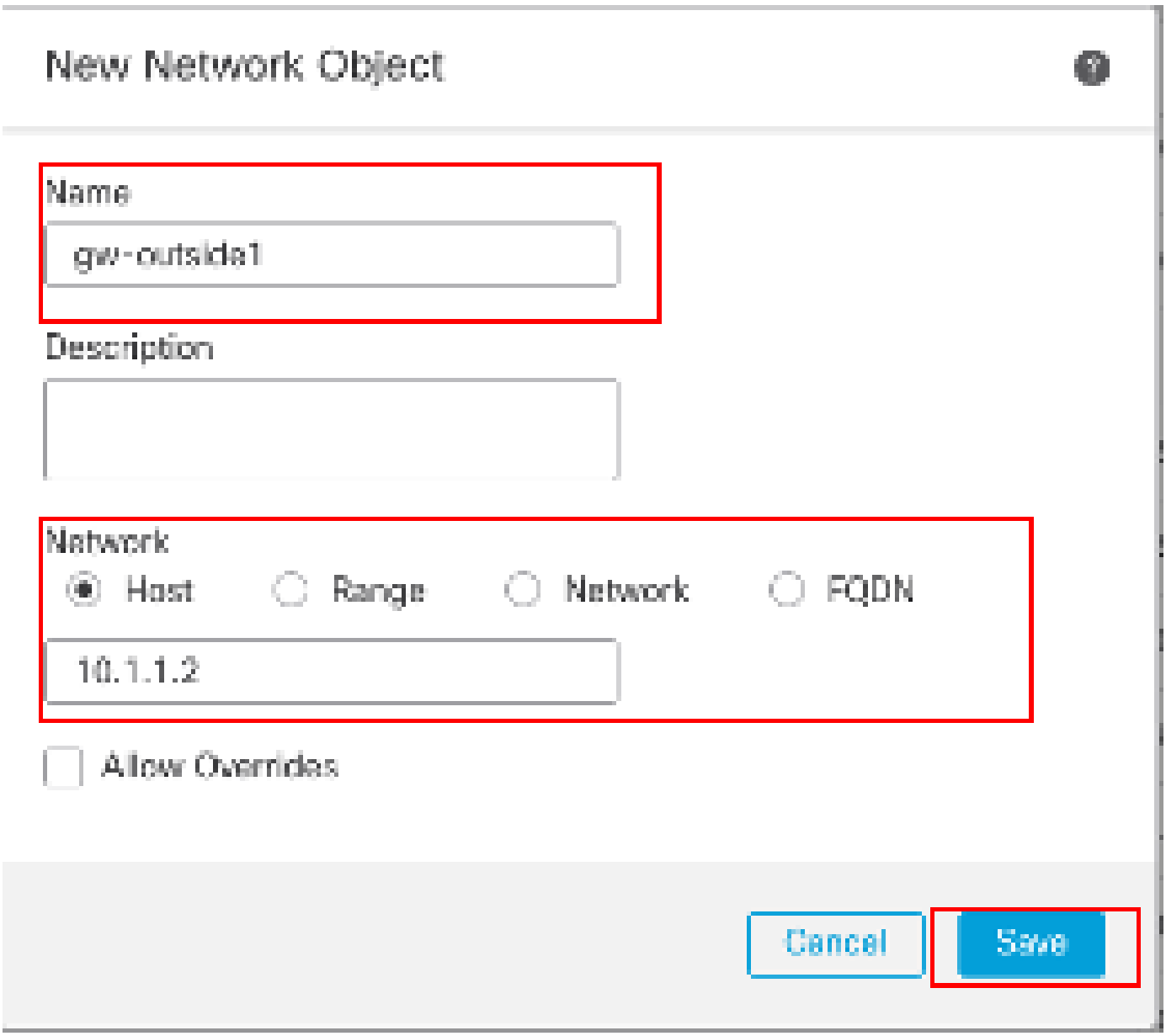


Oggetto di rete

Nella finestra Nuovo oggetto di rete:

1. Impostare il Nome, in questo esempio gw-outside1.
2. Nel campo Network (Rete), selezionare l'opzione richiesta e immettere un valore appropriato, in questo esempio Host e 10.1.1.2.

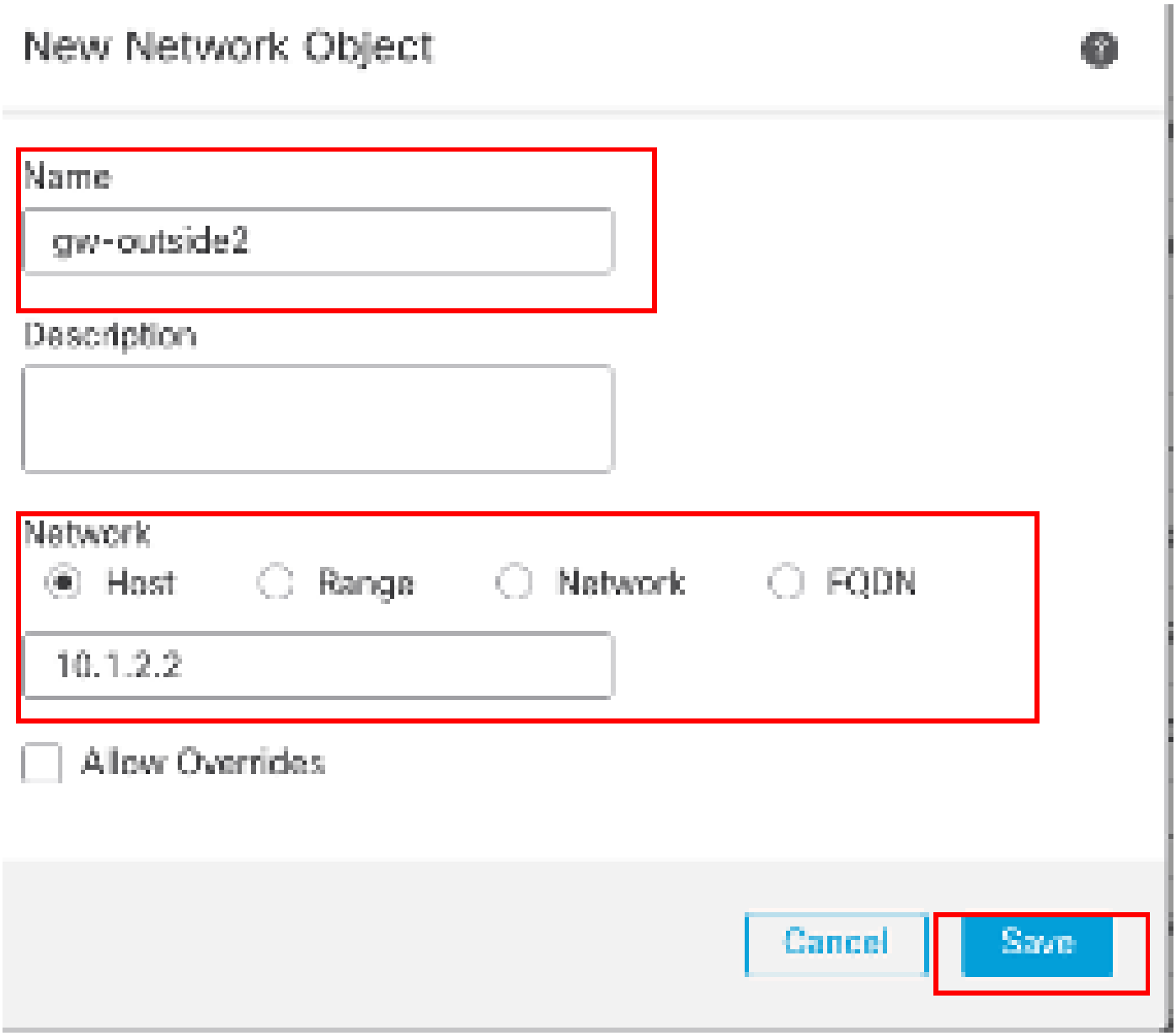
3. Fare clic su Save (Salva).



Oggetto Gw-outside1

Ripetere passaggi simili per creare un altro oggetto per il secondo gateway ISP. Nella finestra Nuovo oggetto di rete:

1. Impostare il Nome, in questo esempio gw-outside2.
2. Nel campo Network (Rete), selezionare l'opzione richiesta e immettere un valore appropriato, in questo esempio Host e 10.1.2.2.
3. Fare clic su Save (Salva).

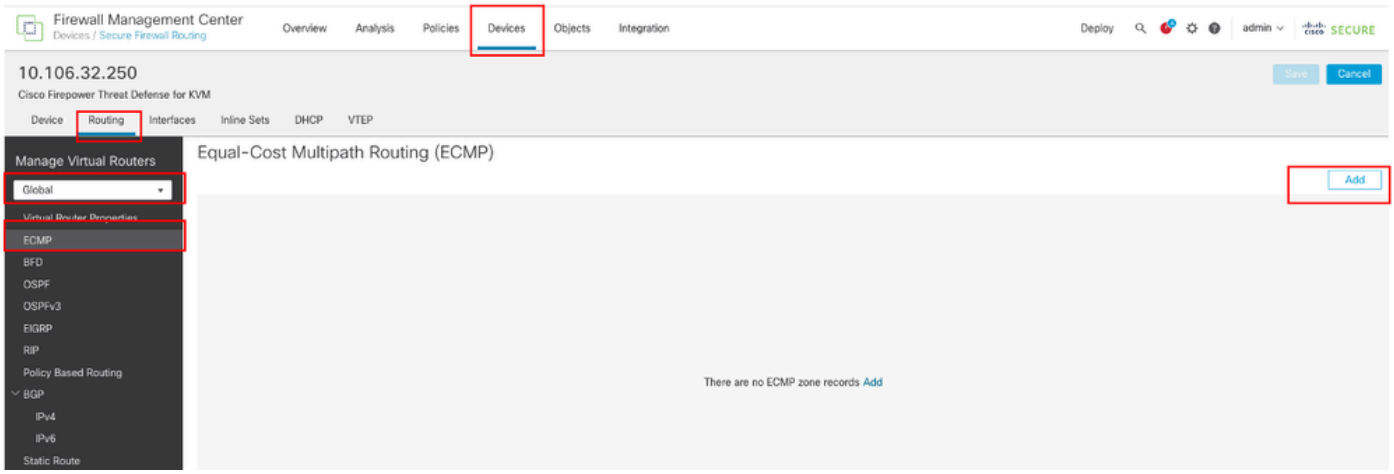


Oggetto Gw-outside2

Passaggio 1. Configura zona ECMP

Selezionare Dispositivi > Gestione dispositivi e modificare il dispositivo di difesa dalle minacce, quindi fare clic su Routing. Dall'elenco a discesa router virtuale, selezionare il router virtuale in cui si desidera creare la zona ECMP. È possibile creare zone ECMP in router virtuali globali e router virtuali definiti dall'utente. In questo esempio, scegliere Globale.

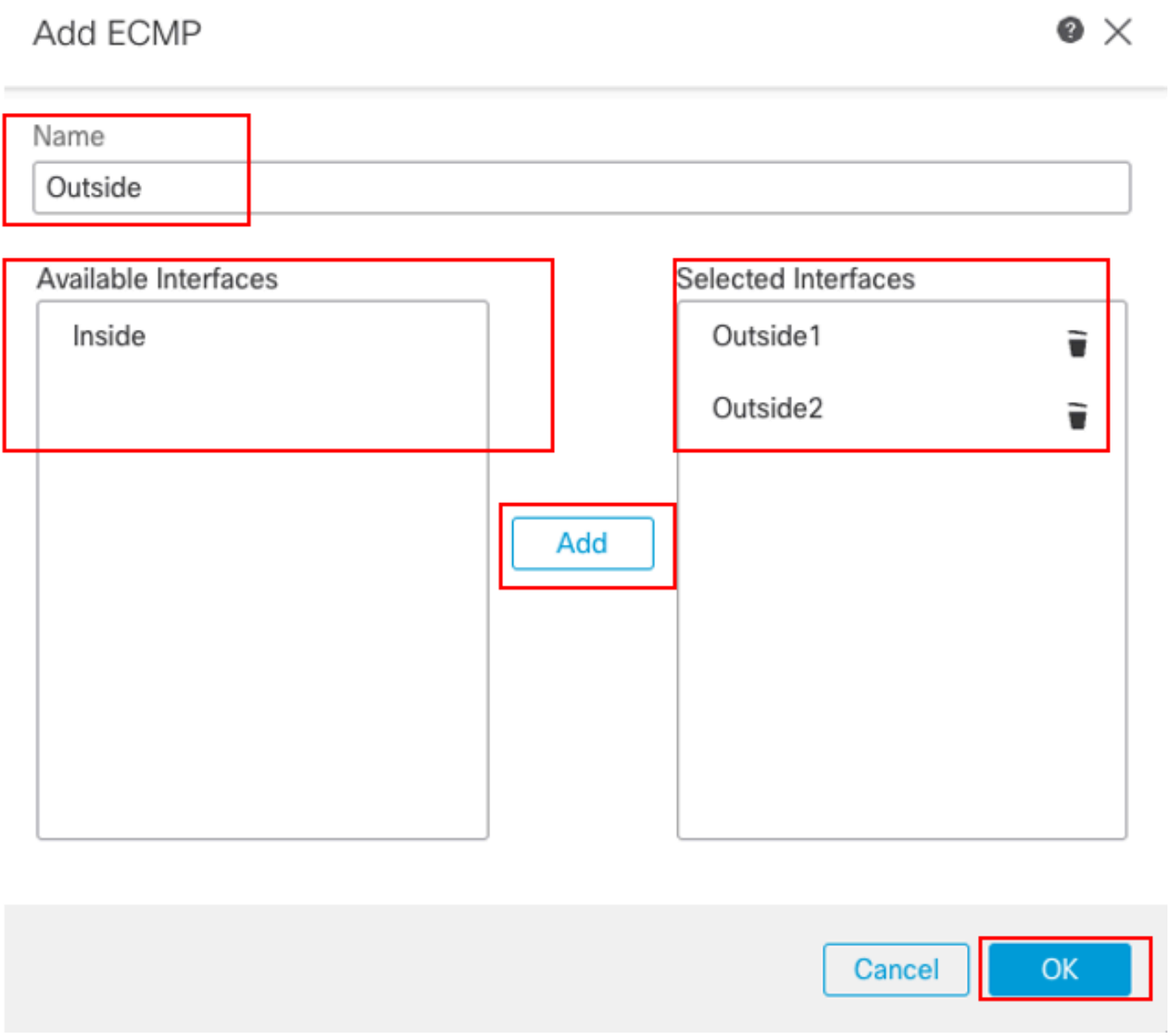
Fare clic su ECMP, quindi su Add (Aggiungi).



Configura zona ECMP

Nella finestra Aggiungi ECMP:

1. Impostare Name per la zona ECMP, in questo esempio Outside.
2. Per associare le interfacce, selezionare l'interfaccia nella casella Interfacce disponibili e quindi fare clic su Aggiungi. In questo esempio, Esterno1 e Esterno2.
3. Fare clic su OK.

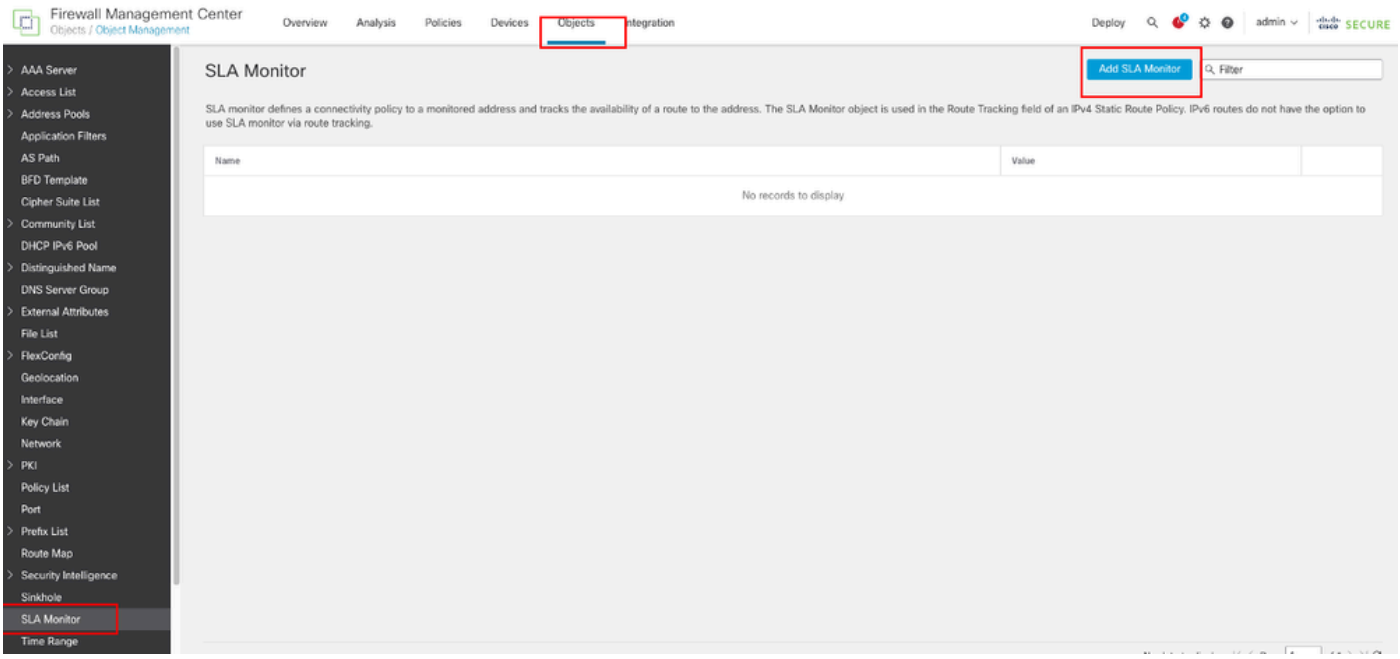


Configura area ECMP all'esterno

Fare clic su Save and Deploy the configuration (Salva e distribuisci).

Passaggio 2. Configura oggetti SLA IP

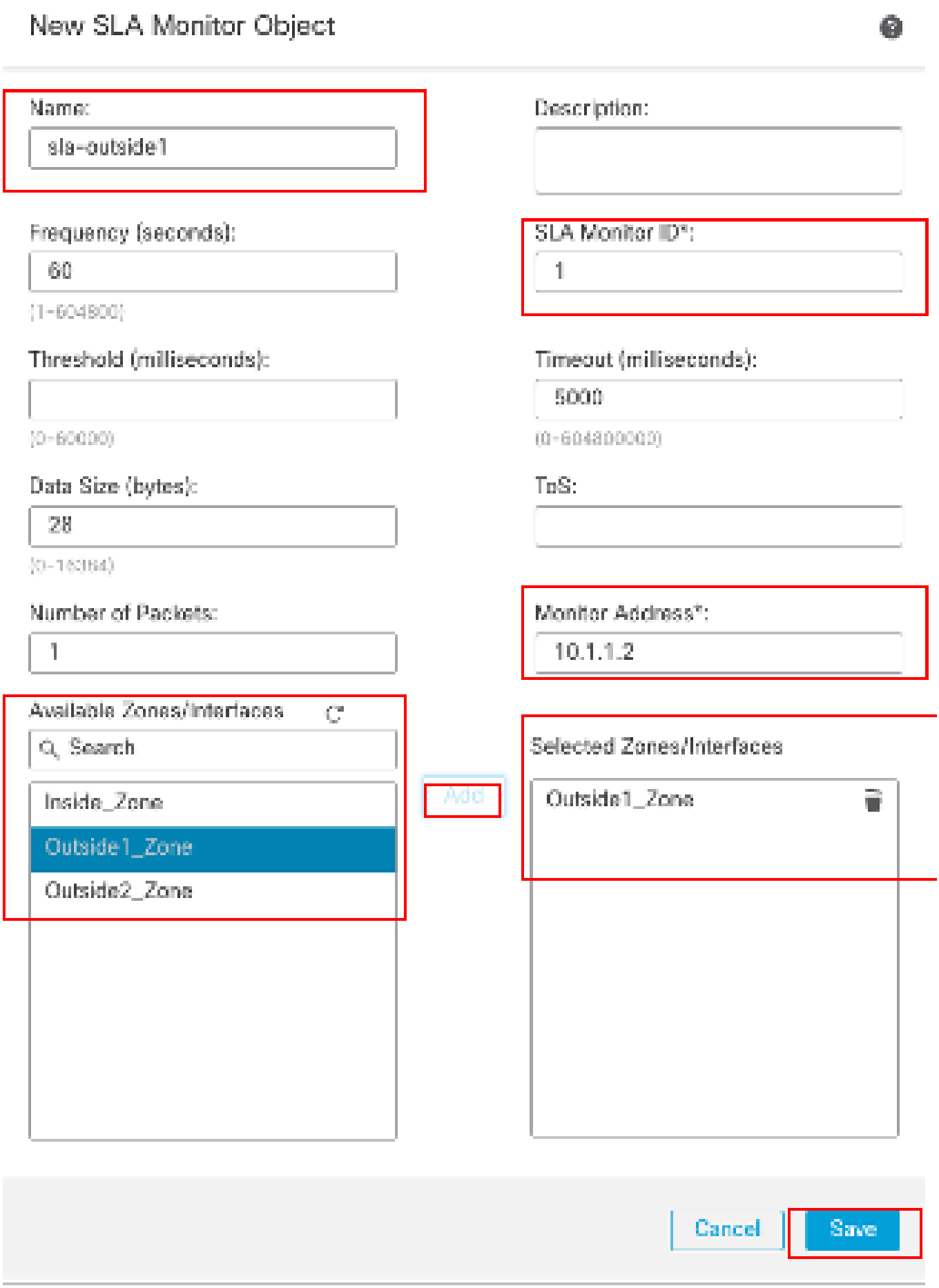
Selezionare Oggetti > Gestione oggetti, Scegliere Monitoraggio SLA dall'elenco dei tipi di oggetto, quindi fare clic su Aggiungi monitoraggio SLA per aggiungere un nuovo monitoraggio per il primo gateway ISP.



Crea monitoraggio contratto di servizio

Nella finestra Nuovo oggetto di monitoraggio SLA:

1. Impostare il Nome per l'oggetto di monitoraggio del contratto di servizio, in questo caso sla-outside1.
2. Immettere il numero ID dell'operazione del contratto di servizio nel campo ID monitor contratto di servizio. I valori sono compresi tra 1 e 2147483647. È possibile creare un massimo di 2000 operazioni SLA su un dispositivo. Ogni numero ID deve essere univoco nel criterio e nella configurazione del dispositivo. In questo esempio 1.
3. Immettere nel campo Indirizzo monitorato l'indirizzo IP monitorato per la disponibilità dall'operazione SLA. Nell'esempio 10.1.1.2.
4. Nell'elenco Zone disponibili/Interfacce vengono visualizzate sia le zone che i gruppi di interfacce. Nell'elenco Zone/Interfacce aggiungere le zone o i gruppi di interfacce che contengono le interfacce attraverso le quali il dispositivo comunica con la stazione di gestione. Per specificare una singola interfaccia, è necessario creare una zona o i gruppi di interfacce per l'interfaccia. In questo esempio, Outside1_Zone.
5. Fare clic su Save (Salva).

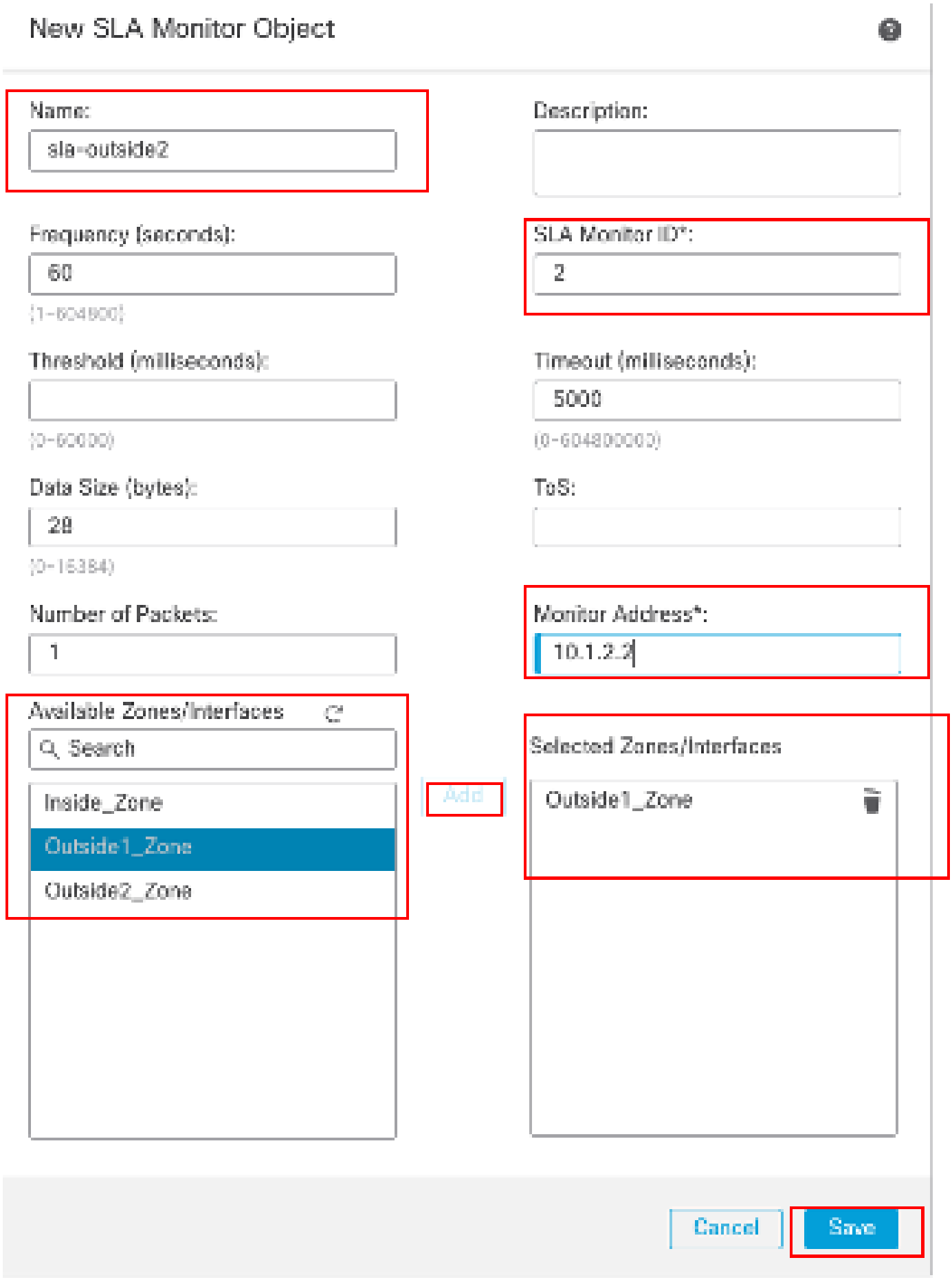


SLA - esterno1 oggetto

Ripetere i passaggi simili per creare un altro monitoraggio SLA per il secondo gateway ISP.

Nella finestra Nuovo oggetto di monitoraggio SLA:

1. Impostare il Nome per l'oggetto di monitoraggio del contratto di servizio, in questo caso sla-outside2.
2. Immettere il numero ID dell'operazione del contratto di servizio nel campo ID monitor contratto di servizio. I valori sono compresi tra 1 e 2147483647. È possibile creare un massimo di 2000 operazioni SLA su un dispositivo. Ogni numero ID deve essere univoco nel criterio e nella configurazione del dispositivo. In questo esempio 2.
3. Immettere nel campo Indirizzo monitorato l'indirizzo IP monitorato per la disponibilità dall'operazione SLA. Nell'esempio 10.1.2.2.
4. Nell'elenco Zone disponibili/Interfacce vengono visualizzate sia le zone che i gruppi di interfacce. Nell'elenco Zone/Interfacce aggiungere le zone o i gruppi di interfacce che contengono le interfacce attraverso le quali il dispositivo comunica con la stazione di gestione. Per specificare una singola interfaccia, è necessario creare una zona o i gruppi di interfacce per l'interfaccia. In questo esempio, Outside2_Zone.
5. Fare clic su Save (Salva).

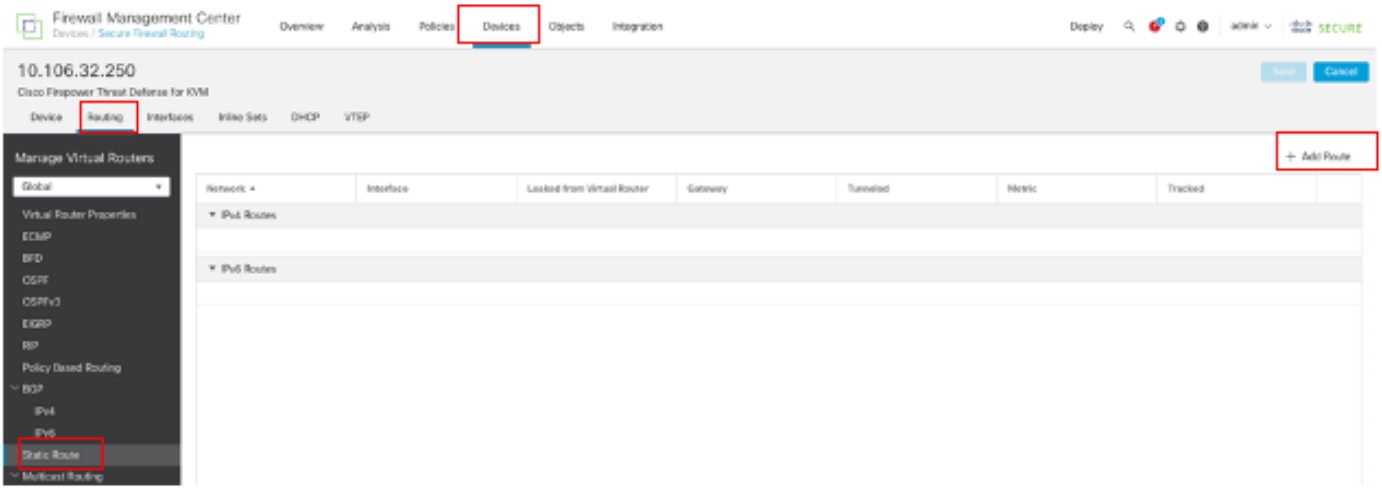


SLA - esterno contratto di servizio2

Passaggio 3. Configura route statiche con route

Passare a Dispositivi > Gestione dispositivi e modificare il dispositivo di difesa dalle minacce, fare clic su Routing. Dall'elenco a discesa Router virtuali, selezionare il router virtuale per il quale si sta configurando un percorso statico. In questo esempio, Global.

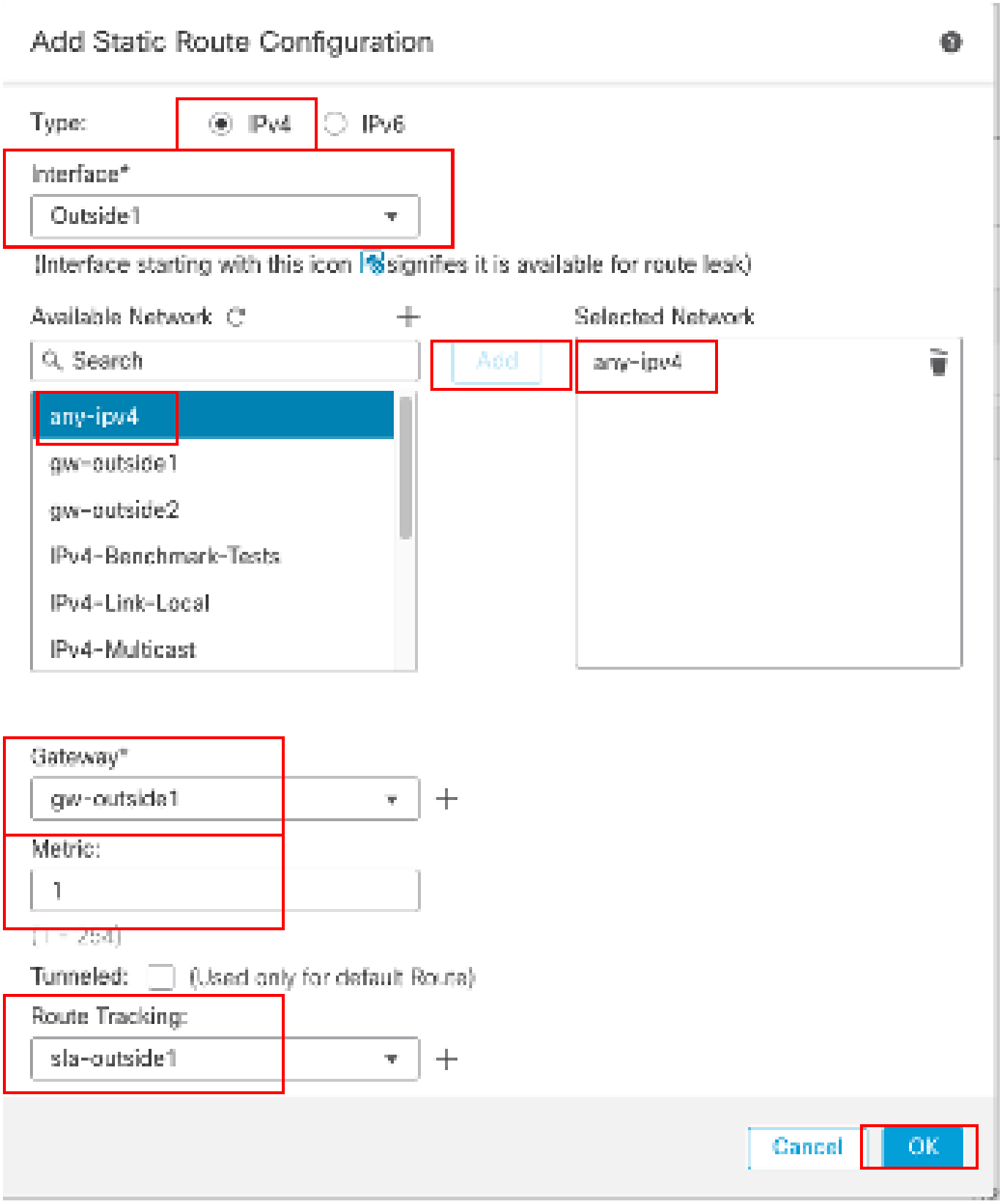
Selezionare Static Route, fare clic su Add Route per aggiungere la route predefinita al primo gateway ISP.



Configura route statica

Nella finestra Aggiungi configurazione route statica:

1. Fare clic su IPv4 o IPv6 a seconda del tipo di route statica che si sta aggiungendo. Nell'esempio, IPv4.
2. Selezionare l'interfaccia a cui applicare la route statica. In questo esempio, Outside1.
3. Nell'elenco Reti disponibili, scegliere la rete di destinazione. Nell'esempio, any-ipv4.
4. Nel campo Gateway o Gateway IPv6, immettere o scegliere il router gateway che rappresenta l'hop successivo per la route. È possibile specificare un indirizzo IP o un oggetto Networks/Hosts. In questo esempio, gw-outside1.
5. Nel campo Metric (Metrica), immettere il numero di hop sulla rete di destinazione. I valori validi sono compresi tra 1 e 255; il valore predefinito è 1. In questo esempio 1.
6. Per monitorare la disponibilità della route, immettere o scegliere il nome di un oggetto di monitoraggio del contratto di servizio che definisce il criterio di monitoraggio nel campo Tracciamento route. In questo esempio, sla-outside1.
7. Fare clic su OK.

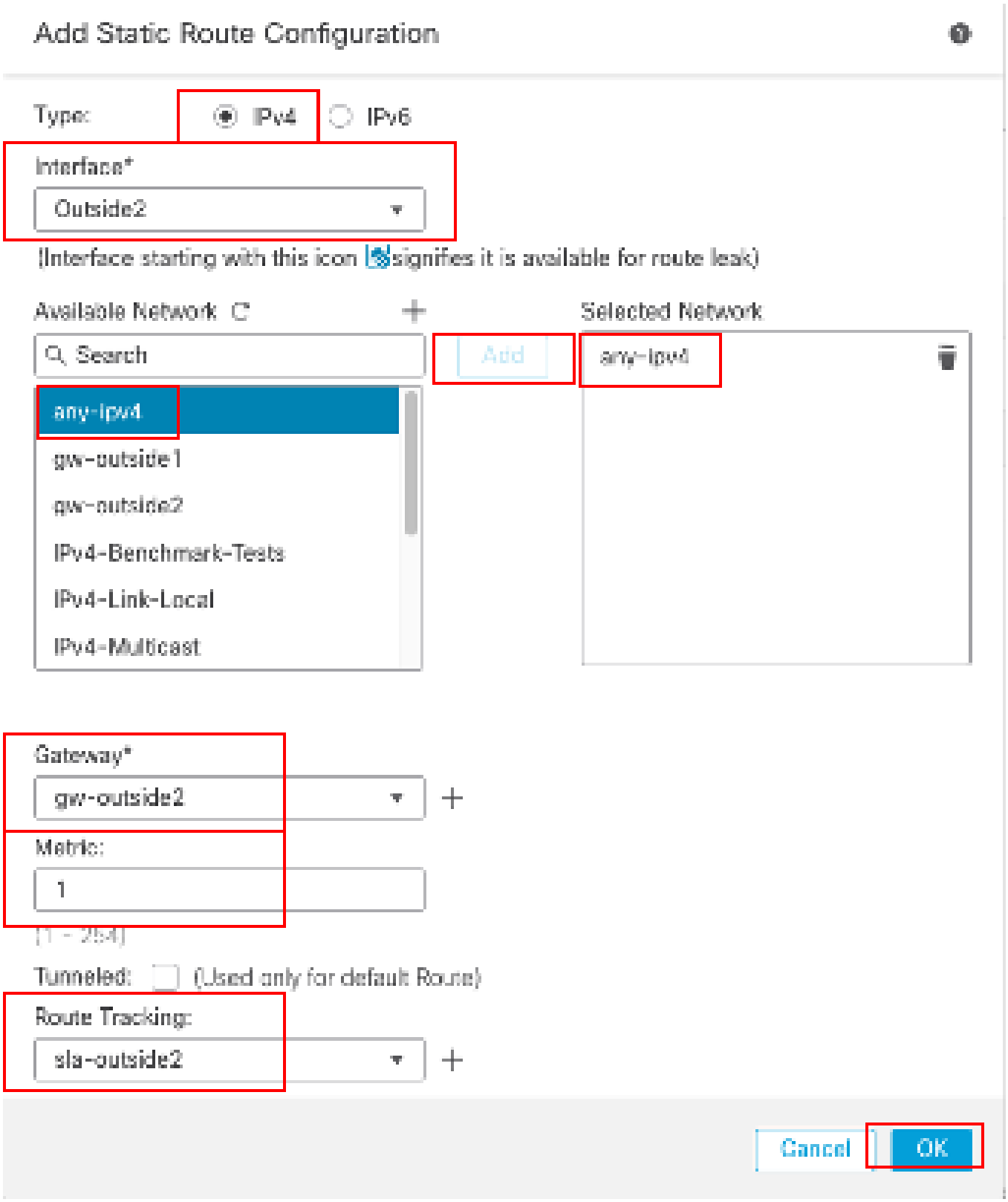


Aggiungi route statica primo ISP

Ripetere una procedura simile per aggiungere la route predefinita al secondo gateway ISP. Nella finestra Aggiungi configurazione route statica:

1. Fare clic su IPv4 o IPv6 a seconda del tipo di route statica che si sta aggiungendo. Nell'esempio, IPv4.
2. Selezionare l'interfaccia a cui applicare la route statica. In questo esempio, Outside2.

3. Nell'elenco Reti disponibili, scegliere la rete di destinazione. Nell'esempio, any-ipv4.
4. Nel campo Gateway o Gateway IPv6, immettere o scegliere il router gateway che rappresenta l'hop successivo per la route. È possibile specificare un indirizzo IP o un oggetto Networks/Hosts. Nell'esempio, gw-outside2.
5. Nel campo Metric (Metrica), immettere il numero di hop sulla rete di destinazione. I valori validi sono compresi tra 1 e 255; il valore predefinito è 1. Assicurarsi di specificare la stessa metrica della prima route, in questo esempio 1.
6. Per monitorare la disponibilità della route, immettere o scegliere il nome di un oggetto di monitoraggio del contratto di servizio che definisce il criterio di monitoraggio nel campo Tracciamento route. In questo esempio, sla-outside2.
7. Fare clic su OK.



Aggiungi route statica secondo ISP

Fare clic su Save and Deploy the configuration (Salva e distribuisci).

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 GigabitEthernet0/1

Outside1 GigabitEthernet0/0

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, a parità di 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: 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:
```

Eseguire il comando show sla monitor operational-state per confermare lo stato del monitor del contratto di servizio. In questo caso, è possibile trovare "**Timeout**: **FALSE**" nell'output del comando, per segnalare che 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: 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

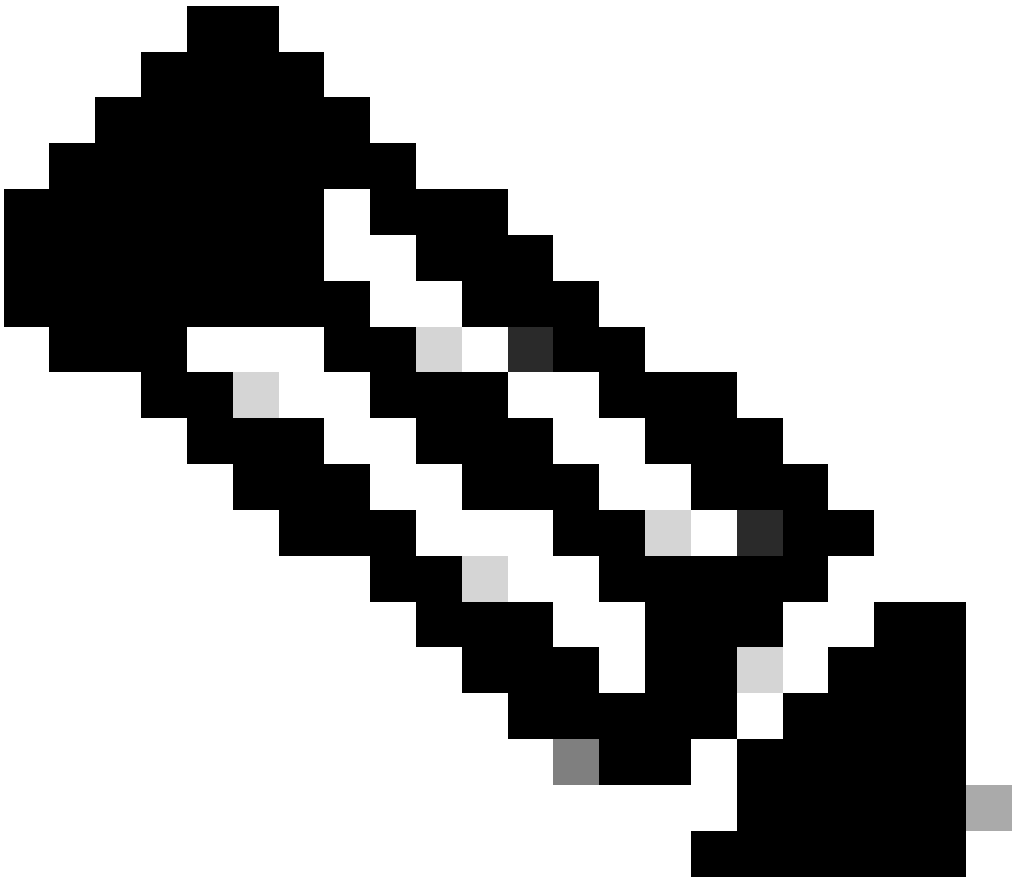
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

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 telnet da Inside-Host1 (10.1.3.2) e da Inside-Host2 (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. Inside-Host1 (10.1.3.2) passa attraverso l'interfaccia esterna1, Inside-Host2 (10.1.3.4) passa attraverso l'interfaccia esterna2.

```
> 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
```



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: 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
```

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
```

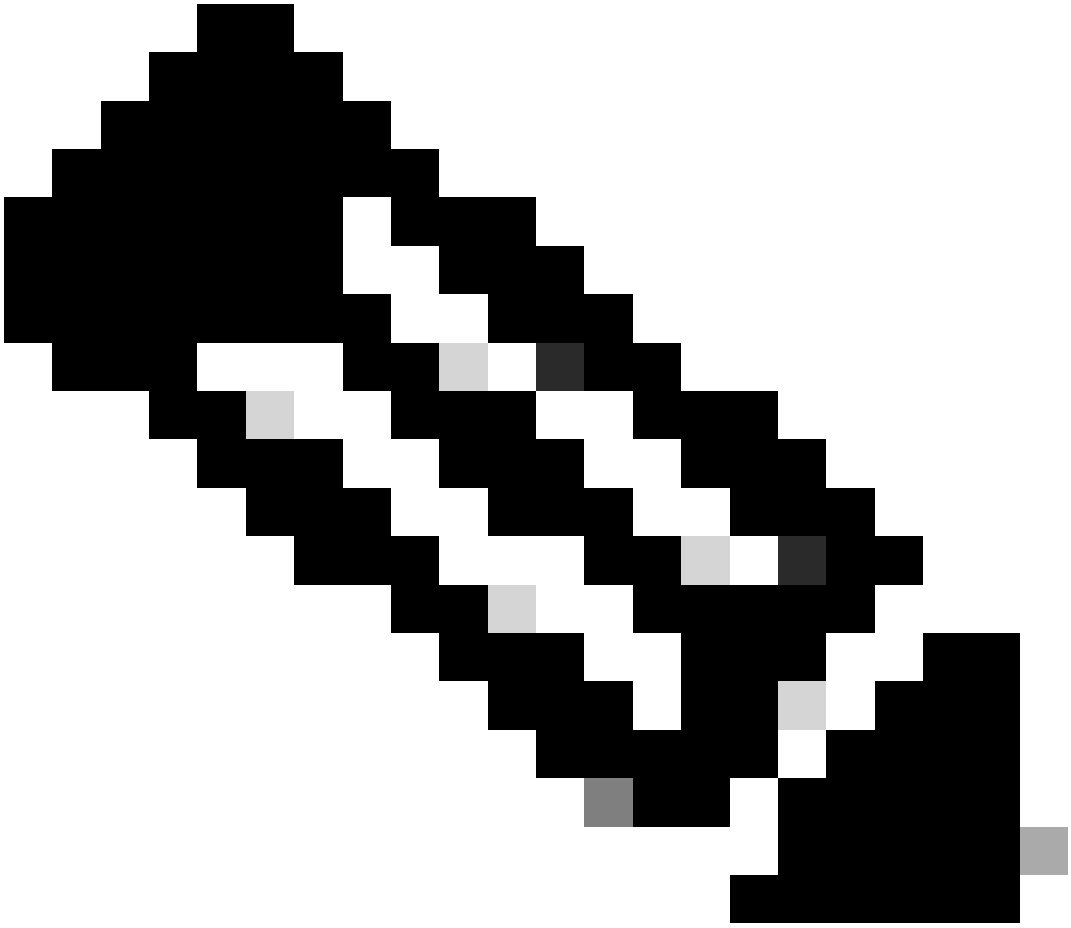
Eseguire il comando show conn per verificare che le due connessioni siano ancora attive. Le sessioni telnet sono attive anche su Inside-Host1 (10.1.3.2) e Inside-Host2 (10.1.3.4) senza alcuna interruzione.

<#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
```



Nota: si noti che nell'output di show conn , la sessione telnet da Inside-Host1 (10.1.3.2) viene ancora eseguita tramite l'interfaccia esterna1, anche se il percorso predefinito attraverso l'interfaccia esterna1 è stato rimosso dalla tabella di routing. Questo è previsto e, in base alla progettazione, il traffico effettivo passa attraverso l'interfaccia esterna2. Se si avvia una nuova connessione da Inside-Host1 (10.1.3.2) a Internet-Host (10.1.5.2), è possibile trovare tutto il traffico che passa 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
```

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.

<#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
```

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).