Konfiguration von ECMP mit IP SLA auf FTD, das von FMC verwaltet wird

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie ECMP zusammen mit IP SLA auf einem FTD konfiguriert wird, das vom FMC verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ECMP-Konfiguration auf Cisco Secure Firewall Threat Defense (FTD)
- IP SLA-Konfiguration auf Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Software- und Hardwareversion:

- Cisco FTD Version 7.4.1

- Cisco FMC Version 7.4.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument beschreibt die Konfiguration von Equal-Cost Multi-Path (ECMP) zusammen mit dem Internet Protocol Service Level Agreement (IP SLA) auf einem Cisco FTD, das von Cisco FMC verwaltet wird. ECMP ermöglicht Ihnen, Schnittstellen in FTD zu gruppieren und Datenverkehr über mehrere Schnittstellen mit Lastausgleich zu übertragen. IP SLA ist ein Mechanismus, der eine End-to-End-Verbindung durch den Austausch regulärer Pakete überwacht. Zusammen mit ECMP kann ein IP SLA implementiert werden, um die Verfügbarkeit des nächsten Hop sicherzustellen. In diesem Beispiel wird ECMP verwendet, um Pakete gleichmäßig über zwei Internet Service Provider (ISP)-Leitungen zu verteilen. Gleichzeitig überwacht ein IP SLA die Verbindungen und stellt einen nahtlosen Übergang zu allen verfügbaren Schaltkreisen bei einem Ausfall sicher.

Spezifische Anforderungen für dieses Dokument:

- Zugriff auf Geräte mit einem Benutzerkonto mit Administratorberechtigungen
- Cisco Secure Firewall Threat Defense Version 7.1 oder höher

- Cisco Secure Firewall Management Center Version 7.1 oder höher

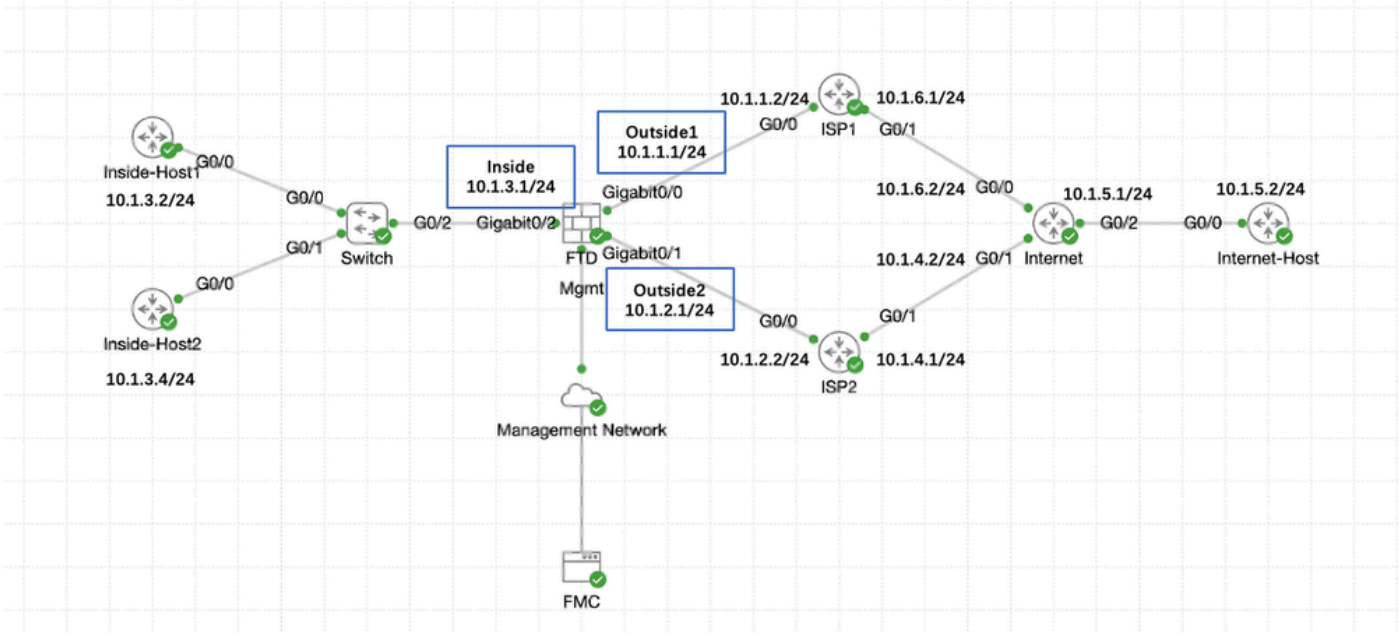
Konfigurieren

Netzwerkdiagramm

In diesem Beispiel hat Cisco FTD zwei externe Schnittstellen: outside1 und outside2 . Jede Verbindung wird mit einem ISP-Gateway hergestellt. outside1 und outside2 gehören zu derselben ECMP-Zone namens outside.

Der Datenverkehr vom internen Netzwerk wird über FTD geroutet und erhält über die beiden ISP ein Load Balancing auf das Internet.

Gleichzeitig verwendet FTD IP SLAs, um die Verbindungen zu den einzelnen ISP-Gateways zu überwachen. Bei einem Ausfall eines ISP-Anschlusses wird die FTD auf den anderen ISP-Gateway umgeschaltet, um die Geschäftskontinuität aufrechtzuerhalten.

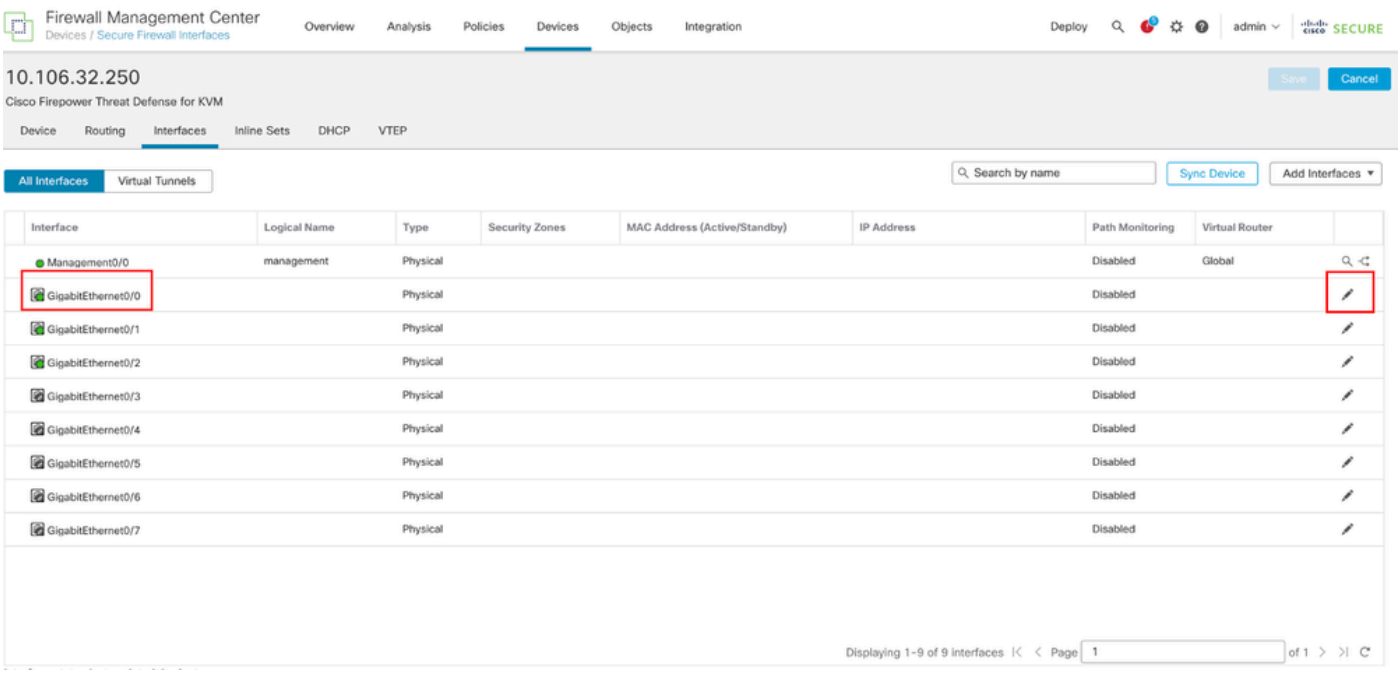


Netzwerkdiagramm

Konfigurationen

Schritt 0: Schnittstellen/Netzwerkobjekte vorkonfigurieren

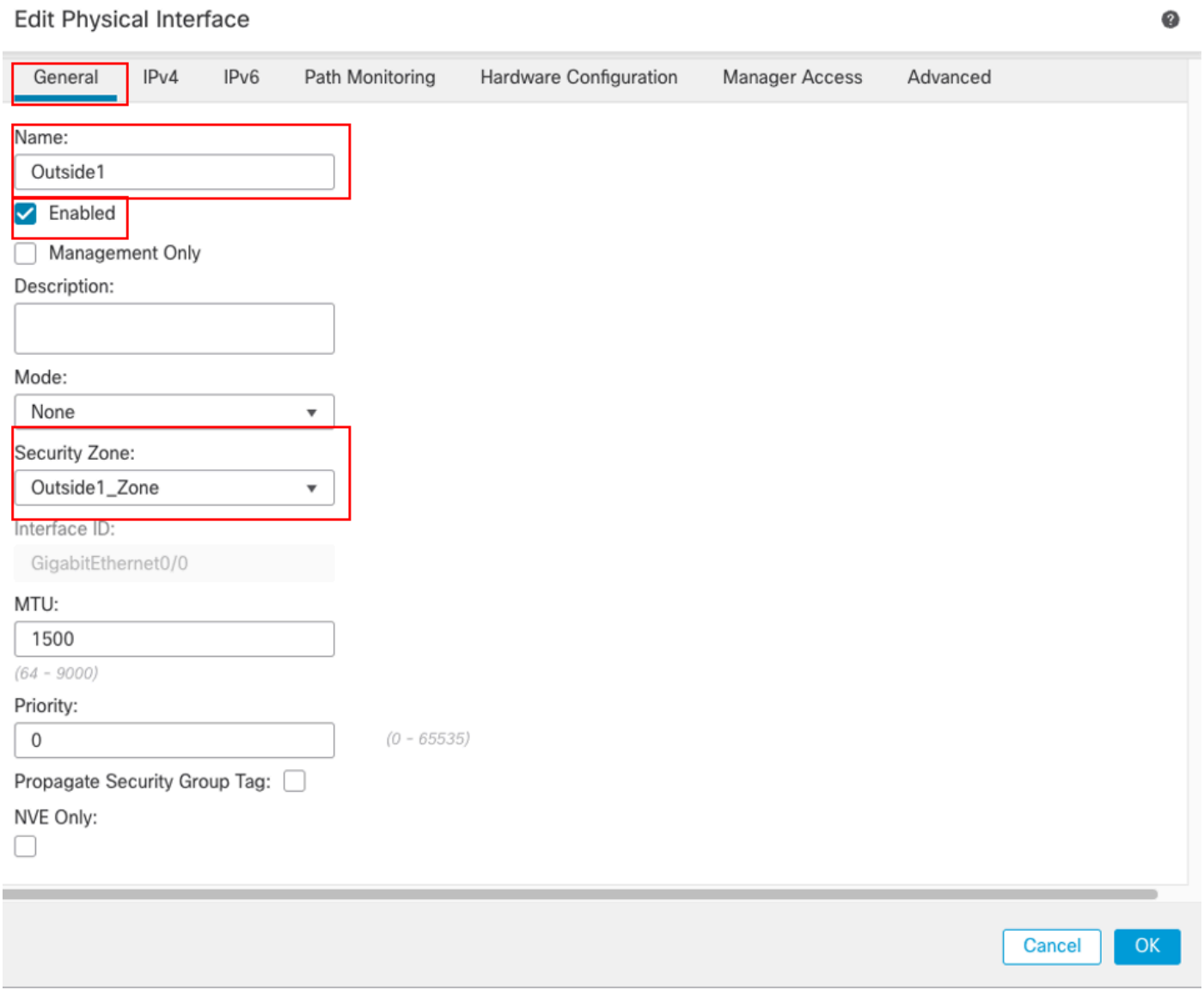
Melden Sie sich bei der FMC Web-GUI an, wählen Sie Devices (Geräte) > Device Management (Geräteverwaltung) aus, und klicken Sie auf die Schaltfläche Edit (Bearbeiten) für Ihr Threat Defense-Gerät. Die Seite Schnittstellen ist standardmäßig ausgewählt. Klicken Sie für die Schnittstelle, die Sie bearbeiten möchten, in diesem Beispiel GigabitEthernet0/0, auf die Schaltfläche Edit.



Schnittstelle Gi0/0 bearbeiten

Im Fenster Edit Physical Interface (Physische Schnittstelle bearbeiten) auf der Registerkarte General (Allgemein):

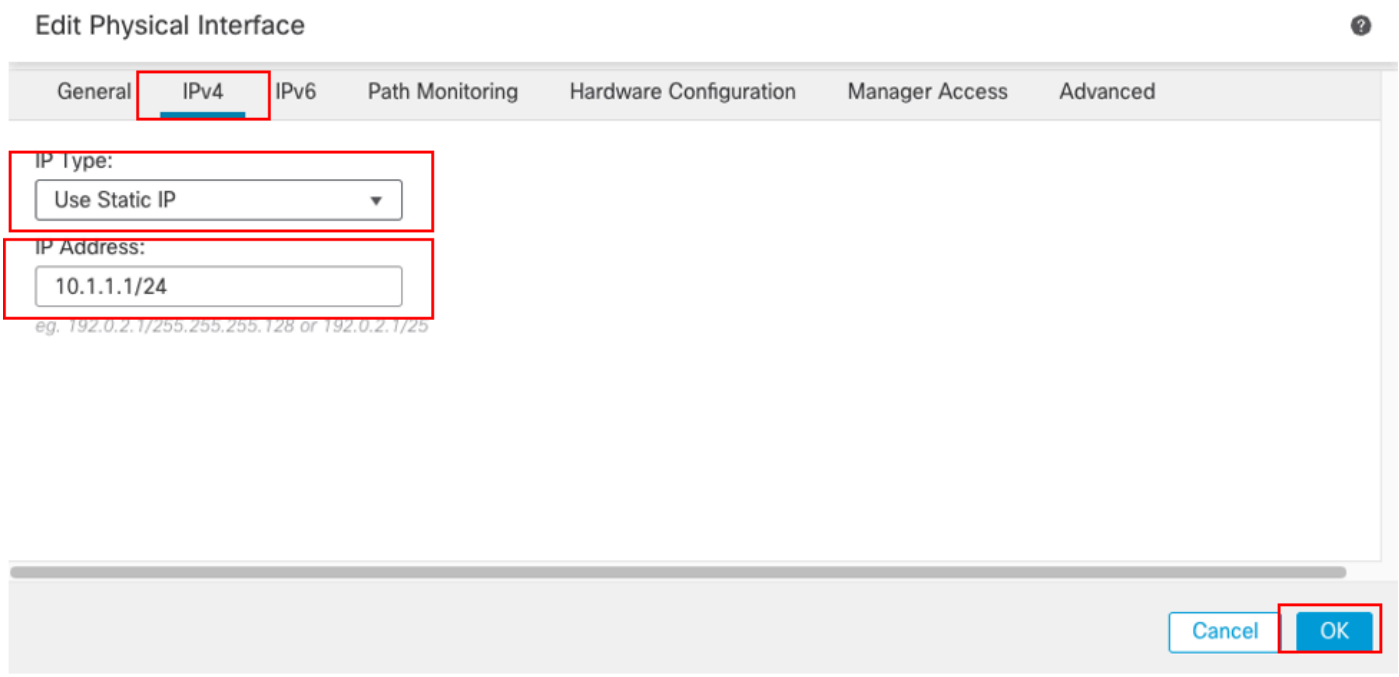
1. Legen Sie den Namen fest, in diesem Fall Outside1.
2. Aktivieren Sie die Schnittstelle, indem Sie das Kontrollkästchen Aktiviert aktivieren.
3. Wählen Sie in der Dropdown-Liste Sicherheitszone eine vorhandene Sicherheitszone aus, oder erstellen Sie eine neue, in diesem Beispiel Outside1_Zone.



Schnittstelle Gi0/0 Allgemein

Auf der Registerkarte IPv4:

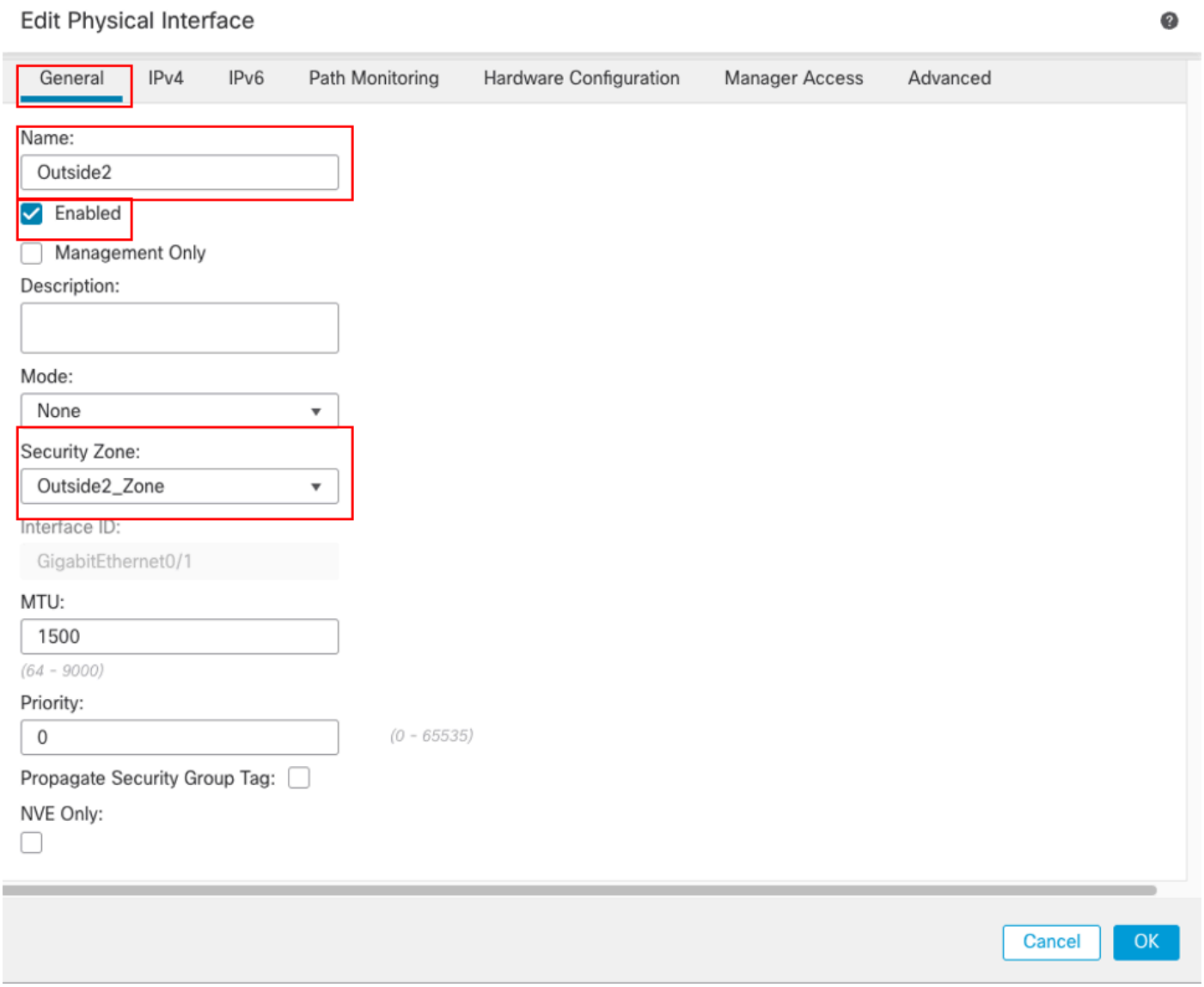
1. Wählen Sie eine der Optionen aus der Dropdown-Liste IP Type (IP-Typ) aus. In diesem Beispiel wird Use Static IP (Statische IP verwenden) verwendet.
2. Legen Sie die IP-Adresse in diesem Beispiel 10.1.1.1/24 fest.
3. Klicken Sie auf OK.



Schnittstelle Gi0/0 IPv4

Wiederholen Sie einen ähnlichen Schritt, um die Schnittstelle GigabitEthernet0/1 zu konfigurieren. Gehen Sie im Fenster Edit Physical Interface (Physische Schnittstelle bearbeiten) unter der Registerkarte General (Allgemein) folgendermaßen vor:

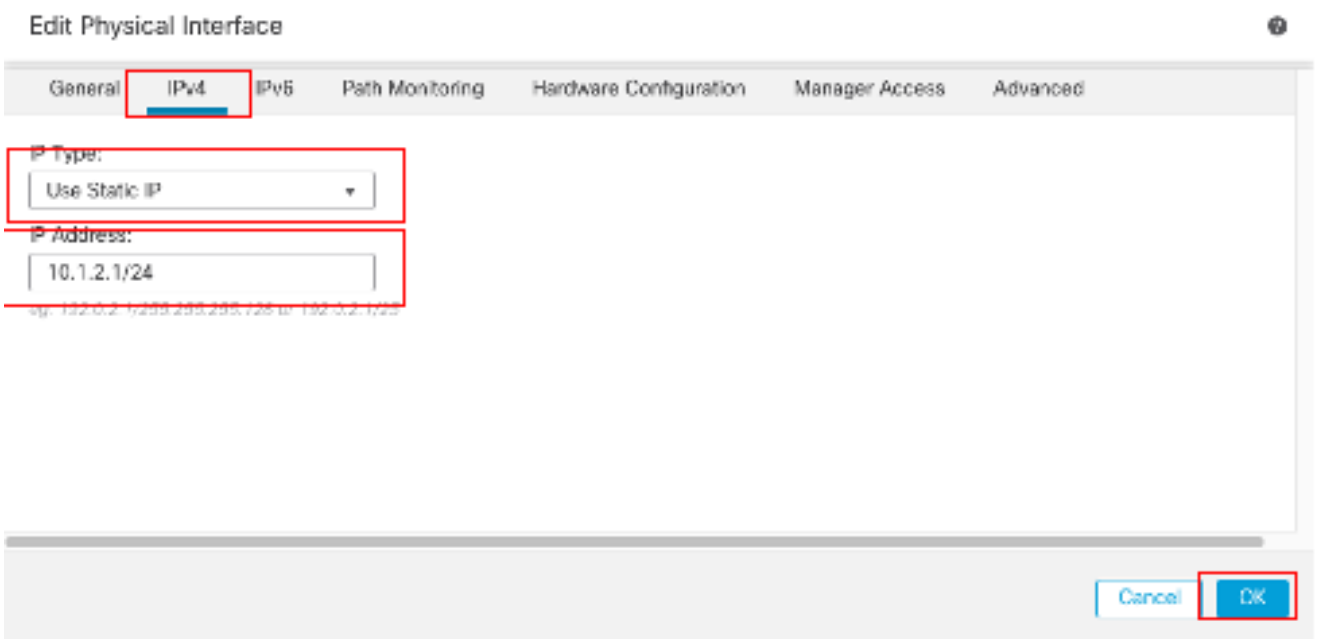
1. Legen Sie den Namen fest, in diesem Fall Outside2.
2. Aktivieren Sie die Schnittstelle, indem Sie das Kontrollkästchen Aktiviert aktivieren.
3. Wählen Sie in der Dropdown-Liste Sicherheitszone eine vorhandene Sicherheitszone aus, oder erstellen Sie eine neue, in diesem Beispiel Outside2_Zone.



Schnittstelle Gi0/1 Allgemein

Auf der Registerkarte IPv4:

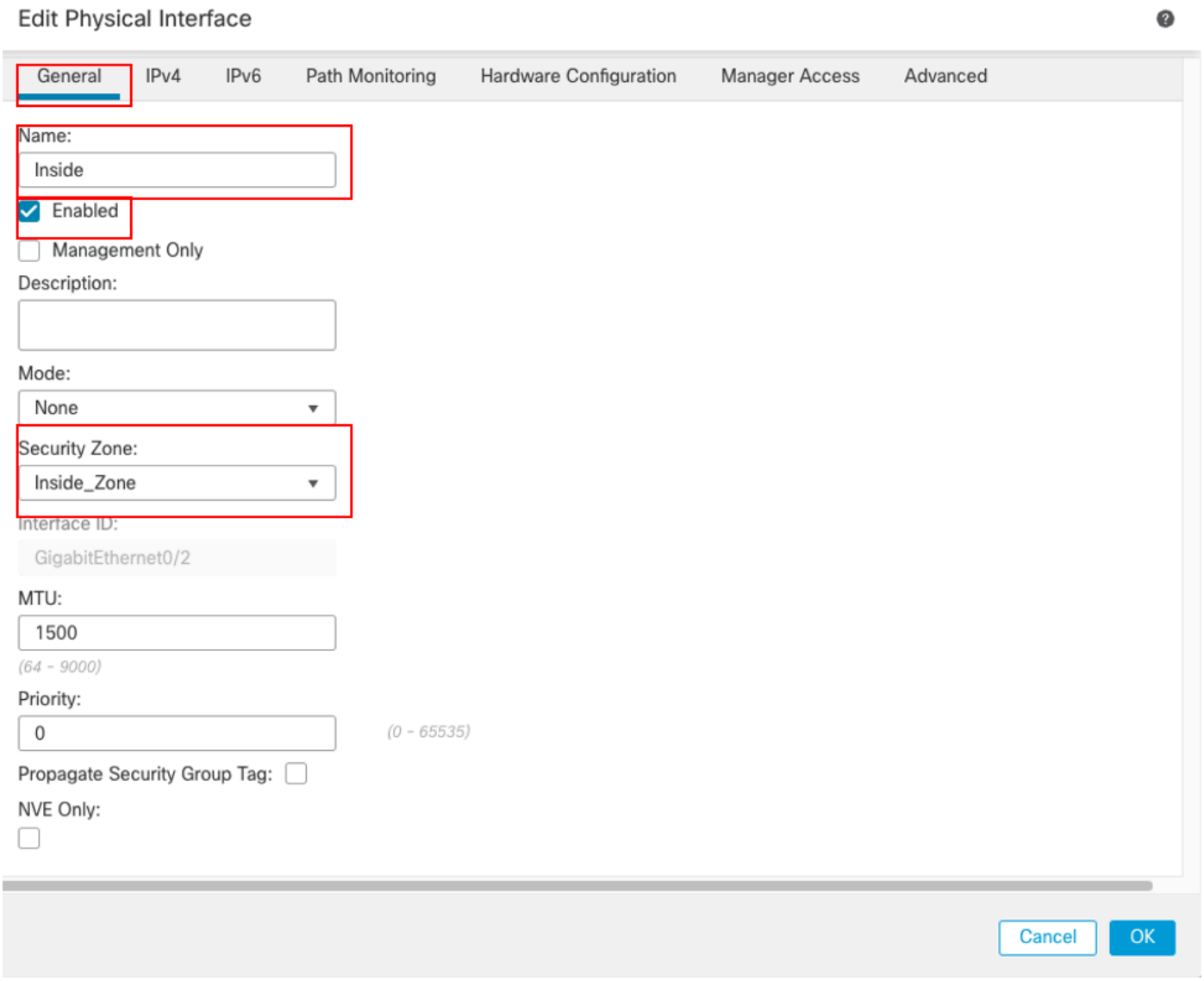
1. Wählen Sie eine der Optionen aus der Dropdown-Liste IP Type (IP-Typ) aus. In diesem Beispiel wird Use Static IP (Statische IP verwenden) verwendet.
2. Legen Sie die IP-Adresse in diesem Beispiel 10.1.2.1/24 fest.
3. Klicken Sie auf OK.



Schnittstelle Gi0/1 IPv4

Wiederholen Sie einen ähnlichen Schritt, um die Schnittstelle GigabitEthernet0/2 zu konfigurieren. Gehen Sie im Fenster Edit Physical Interface (Physische Schnittstelle bearbeiten) unter der Registerkarte General (Allgemein) folgendermaßen vor:

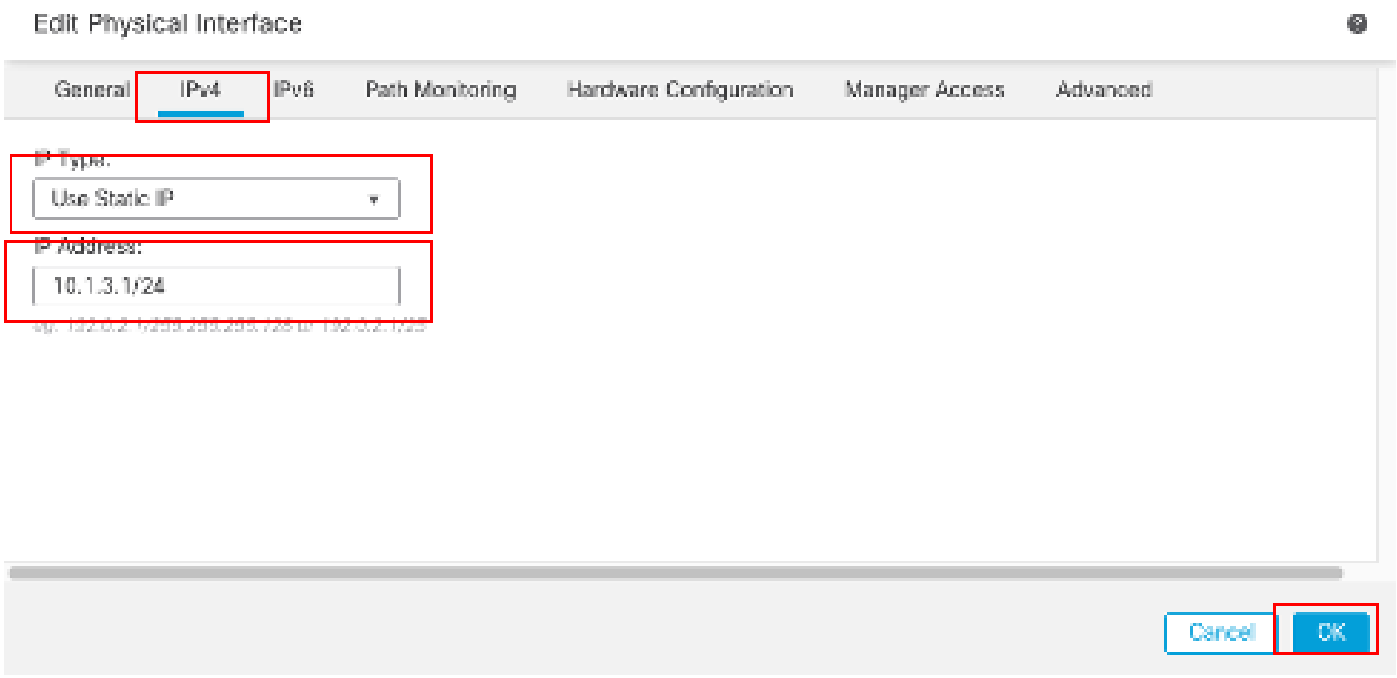
1. Legen Sie den Namen fest, in diesem Fall Inside.
2. Aktivieren Sie die Schnittstelle, indem Sie das Kontrollkästchen Aktiviert aktivieren.
3. Wählen Sie in der Dropdown-Liste Sicherheitszone eine vorhandene Sicherheitszone aus, oder erstellen Sie eine neue, in diesem Beispiel Inside_Zone.



Schnittstelle Gi0/2 Allgemein

Auf der Registerkarte IPv4:

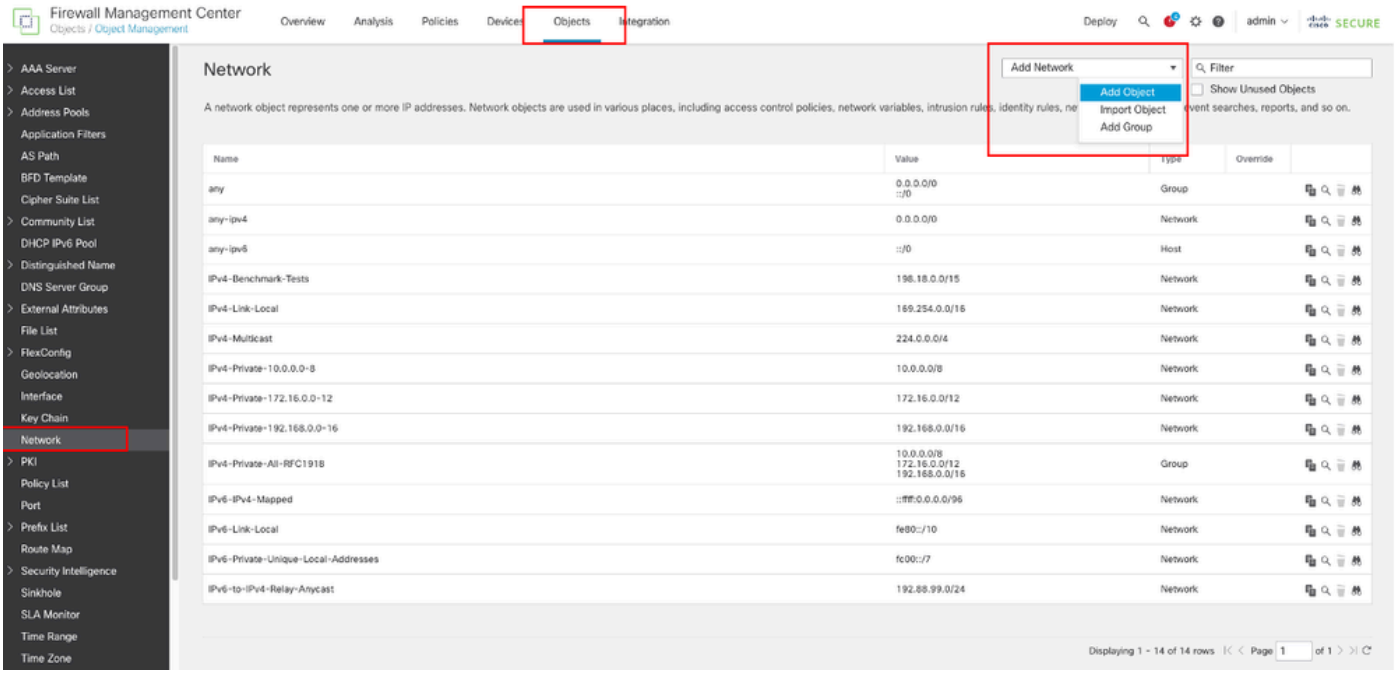
1. Wählen Sie eine der Optionen aus der Dropdown-Liste IP Type (IP-Typ) aus. In diesem Beispiel wird Use Static IP (Statische IP verwenden) verwendet.
2. Legen Sie die IP-Adresse in diesem Beispiel 10.1.3.1/24 fest.
3. Klicken Sie auf OK.



Schnittstelle Gi0/2 IPv4

Klicken Sie auf Speichern und Bereitstellen der Konfiguration.

Navigieren Sie zu Objekte > Objektverwaltung, Wählen Sie Netzwerk aus der Liste der Objekttypen, und wählen Sie Objekt hinzufügen aus dem Dropdown-Menü Netzwerk hinzufügen, um ein Objekt für das erste ISP-Gateway zu erstellen.

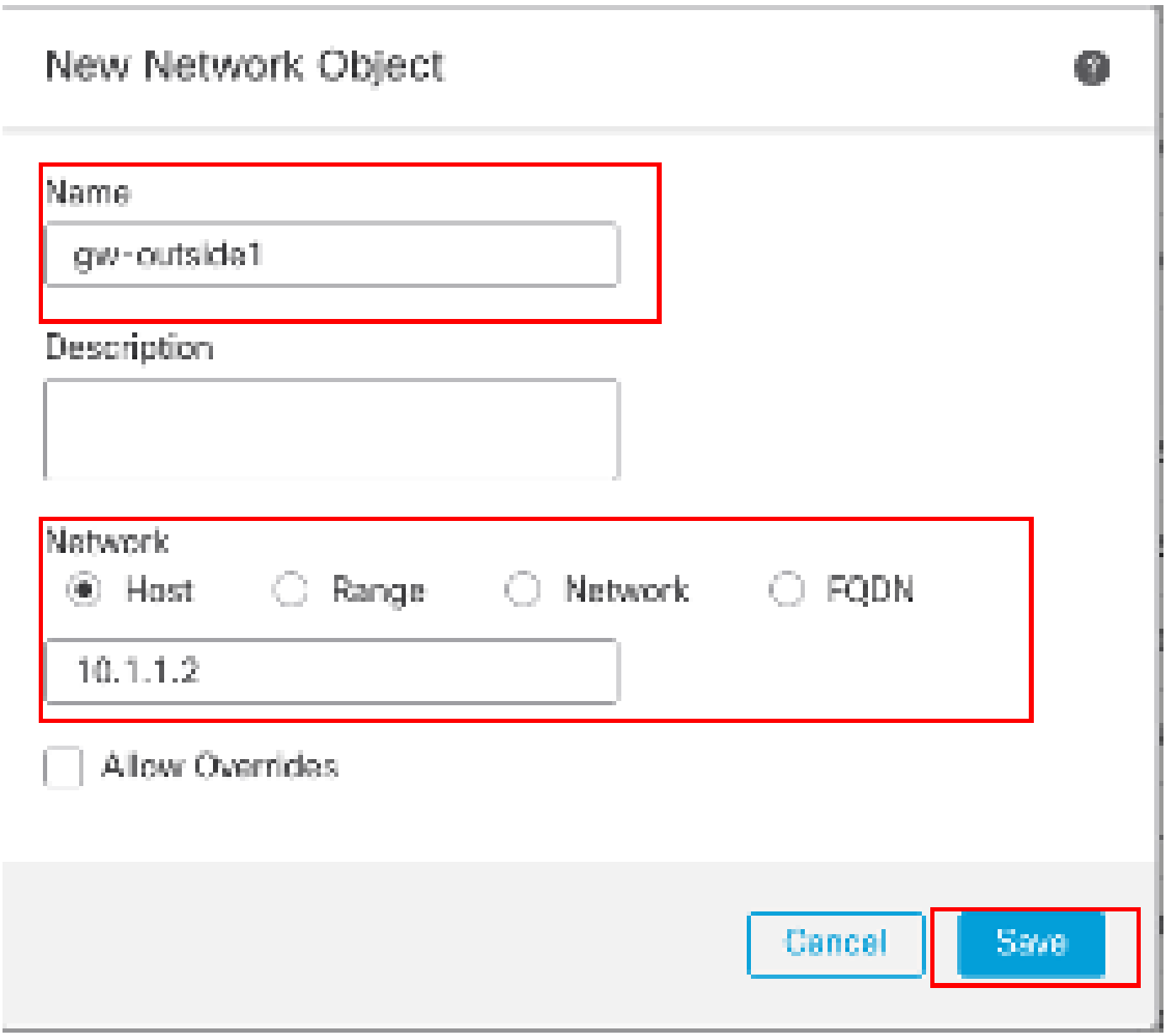


Netzwerkobjekt

Im Fenster Neues Netzwerkobjekt:

1. Legen Sie den Namen fest, in diesem Beispiel gw-outside1.
2. Wählen Sie im Feld Netzwerk die erforderliche Option aus, und geben Sie einen entsprechenden Wert ein, in diesem Beispiel Host und 10.1.1.2.

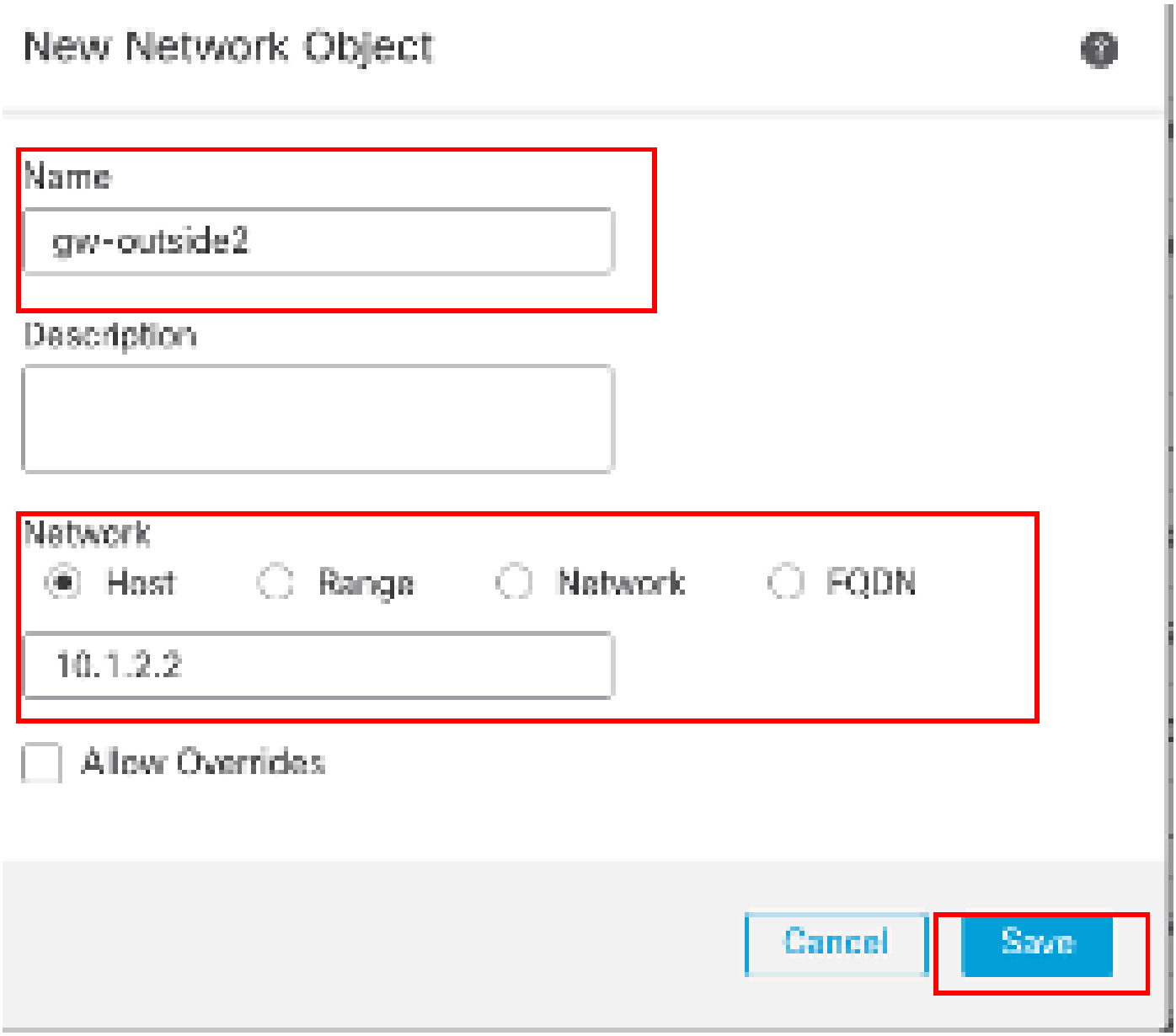
3. Klicken Sie auf Speichern.



Objekt Gw-outside1

Wiederholen Sie ähnliche Schritte, um ein weiteres Objekt für das zweite ISP-Gateway zu erstellen. Im Fenster Neues Netzwerkobjekt:

1. Legen Sie den Namen fest, in diesem Beispiel gw-outside2.
2. Wählen Sie im Feld Netzwerk die erforderliche Option aus, und geben Sie einen entsprechenden Wert ein, in diesem Beispiel Host und 10.1.2.2.
3. Klicken Sie auf Speichern.

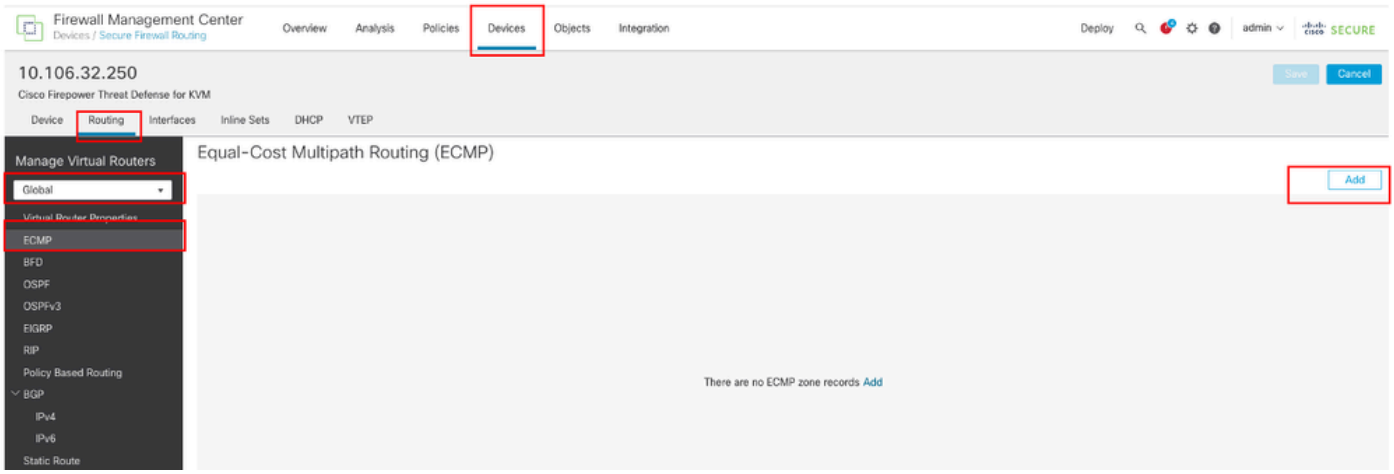


Objekt Gw-outside2

Schritt 1: Konfigurieren der ECMP-Zone

Navigieren Sie zu Devices > Device Management (Geräte > Geräteverwaltung), und bearbeiten Sie das Threat Defense-Gerät, und klicken Sie auf Routing (Routing). Wählen Sie aus dem Dropdown-Menü für den virtuellen Router den virtuellen Router aus, in dem die ECMP-Zone erstellt werden soll. Sie können ECMP-Zonen in globalen virtuellen Routern und benutzerdefinierten virtuellen Routern erstellen. Wählen Sie in diesem Beispiel Global.

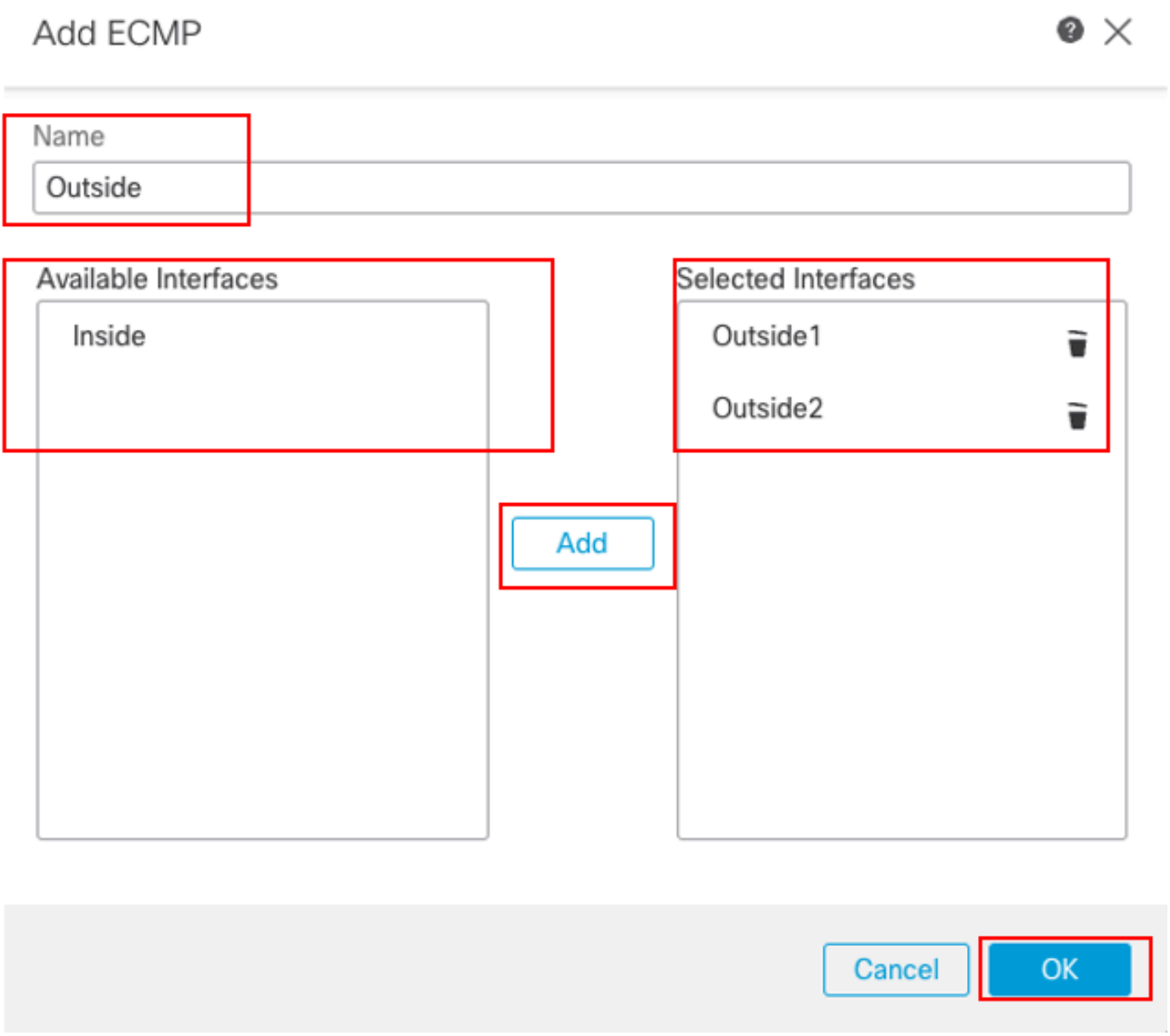
Klicken Sie auf ECMP und dann auf Hinzufügen.



Konfigurieren der ECMP-Zone

Führen Sie im Fenster Add ECMP folgende Schritte aus:

1. Legen Sie Name für die ECMP-Zone fest, in diesem Beispiel Outside.
2. Um Schnittstellen zuzuordnen, wählen Sie die Schnittstelle im Feld Verfügbare Schnittstellen aus, und klicken Sie dann auf Hinzufügen. In diesem Beispiel Outside1 und Outside2.
3. Klicken Sie auf OK.

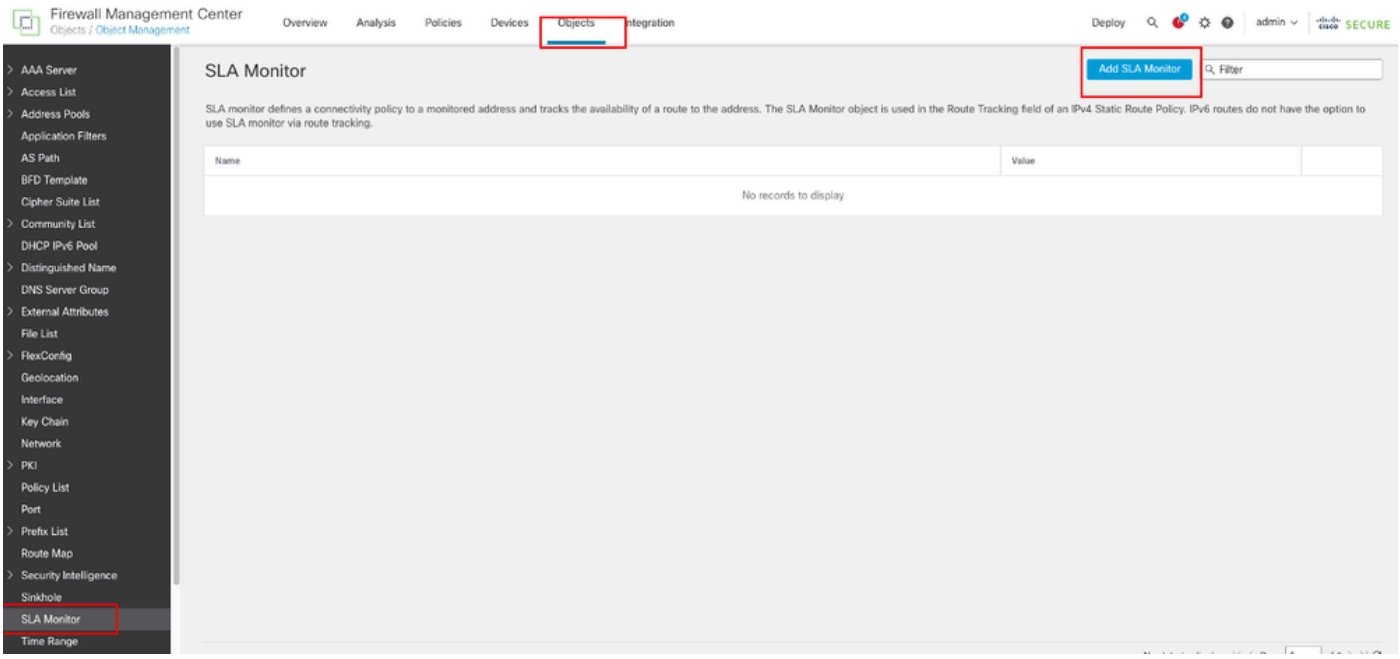


Konfigurieren der externen ECMP-Zone

Klicken Sie auf Speichern und Bereitstellen der Konfiguration.

Schritt 2: IP SLA-Objekte konfigurieren

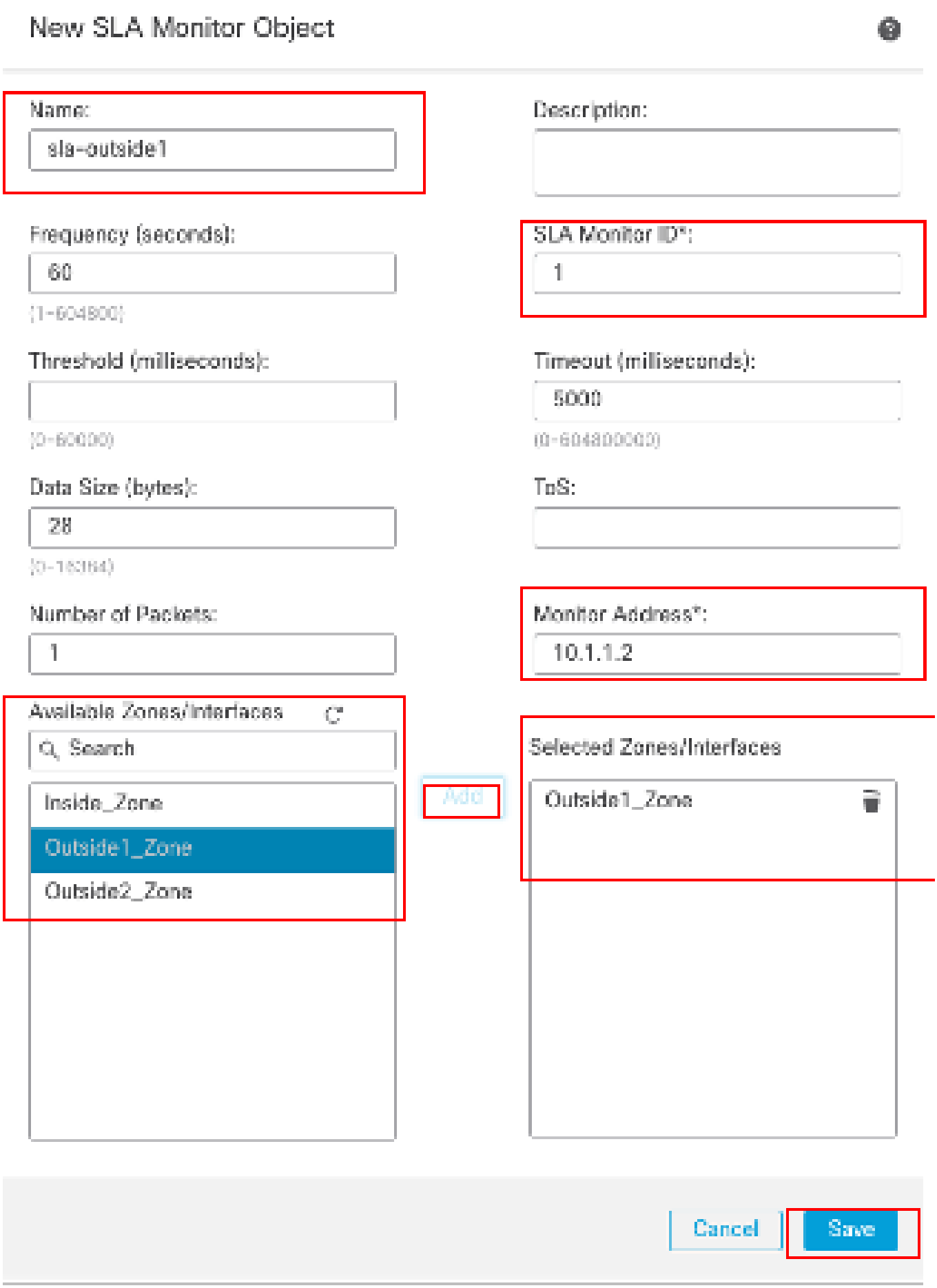
Navigieren Sie zu Objekte > Objektmanagement, Wählen Sie SLA Monitor aus der Liste der Objekttypen aus, und klicken Sie auf SLA Monitor hinzufügen, um einen neuen SLA Monitor für das erste ISP-Gateway hinzuzufügen.



SLA-Monitor erstellen

Im Fenster Neues SLA-Überwachungsobjekt:

1. Legen Sie den Namen für das SLA-Überwachungsobjekt fest, in diesem Fall sla-outside1.
2. Geben Sie die ID-Nummer des SLA-Vorgangs in das Feld SLA Monitor ID (SLA-Monitor-ID) ein. Die Werte liegen zwischen 1 und 2147483647. Sie können maximal 2.000 SLA-Vorgänge auf einem Gerät erstellen. Jede ID-Nummer muss für die Richtlinie und die Gerätekonfiguration eindeutig sein. In diesem Beispiel 1.
3. Geben Sie die IP-Adresse, die im Rahmen des SLA-Vorgangs auf Verfügbarkeit überwacht wird, in das Feld Überwachte Adresse ein. In diesem Beispiel 10.1.1.2.
4. In der Liste Verfügbare Zonen/Schnittstellen werden sowohl Zonen als auch Schnittstellengruppen angezeigt. Fügen Sie in der Liste Zones/Interfaces (Zonen/Schnittstellen) die Zonen oder Schnittstellengruppen hinzu, die die Schnittstellen enthalten, über die das Gerät mit der Managementstation kommuniziert. Um eine einzelne Schnittstelle festzulegen, müssen Sie eine Zone oder die Schnittstellengruppen für die Schnittstelle erstellen. In diesem Beispiel ist Outside1_Zone angegeben.
5. Klicken Sie auf Speichern.



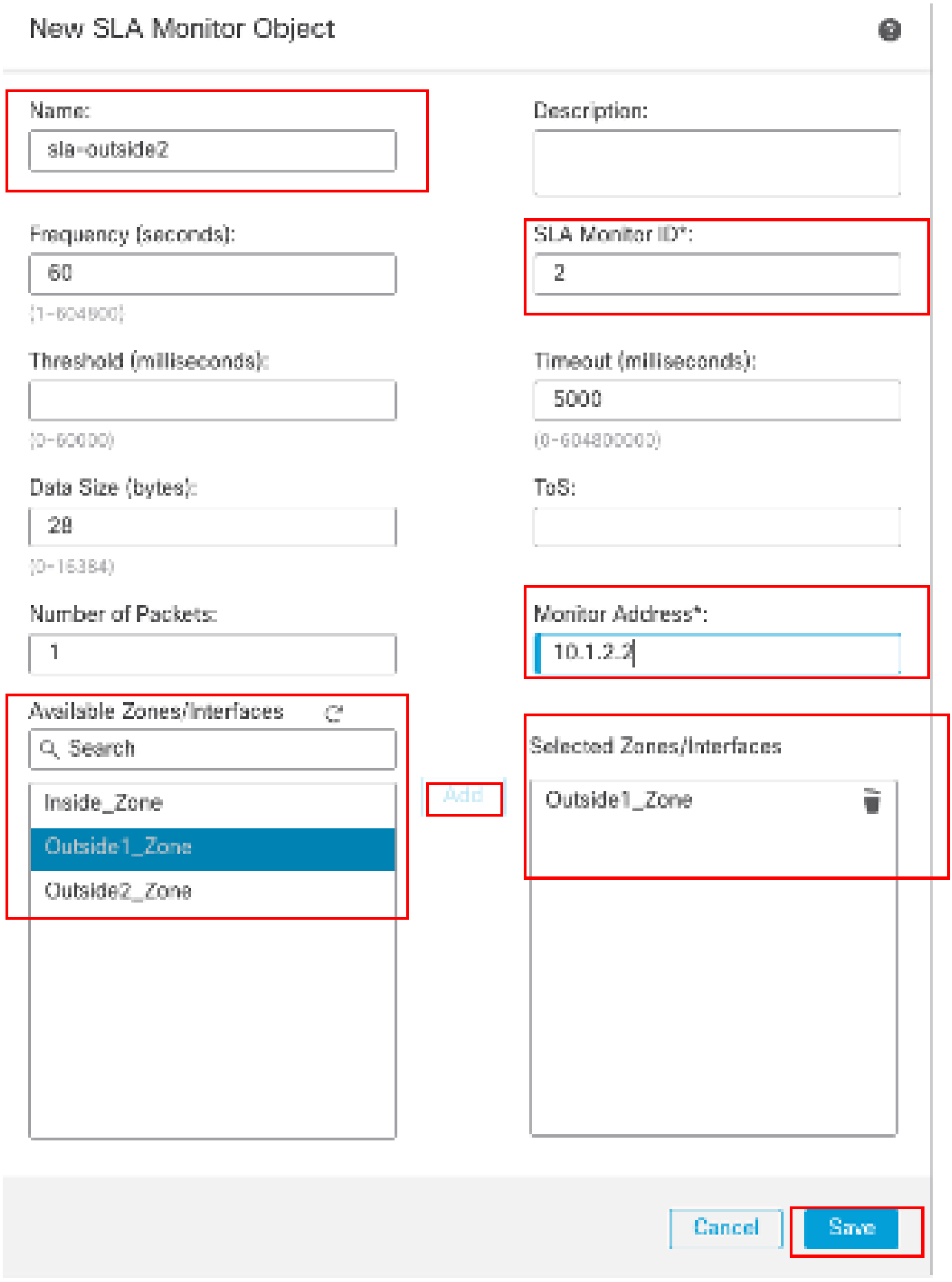
SLA-Objekt Sla-outside1

Wiederholen Sie ähnliche Schritte, um einen weiteren SLA-Monitor für das zweite ISP-Gateway zu

erstellen.

Im Fenster Neues SLA-Überwachungsobjekt:

1. Legen Sie den Namen für das SLA-Überwachungsobjekt fest, in diesem Fall sla-outside2.
2. Geben Sie die ID-Nummer des SLA-Vorgangs in das Feld SLA Monitor ID (SLA-Monitor-ID) ein. Die Werte liegen zwischen 1 und 2147483647. Sie können maximal 2.000 SLA-Vorgänge auf einem Gerät erstellen. Jede ID-Nummer muss für die Richtlinie und die Gerätekonfiguration eindeutig sein. In diesem Beispiel 2.
3. Geben Sie die IP-Adresse, die im Rahmen des SLA-Vorgangs auf Verfügbarkeit überwacht wird, in das Feld Überwachte Adresse ein. In diesem Beispiel 10.1.2.2.
4. In der Liste Verfügbare Zonen/Schnittstellen werden sowohl Zonen als auch Schnittstellengruppen angezeigt. Fügen Sie in der Liste Zones/Interfaces (Zonen/Schnittstellen) die Zonen oder Schnittstellengruppen hinzu, die die Schnittstellen enthalten, über die das Gerät mit der Managementstation kommuniziert. Um eine einzelne Schnittstelle festzulegen, müssen Sie eine Zone oder die Schnittstellengruppen für die Schnittstelle erstellen. In diesem Beispiel ist Outside2_Zone angegeben.
5. Klicken Sie auf Speichern.

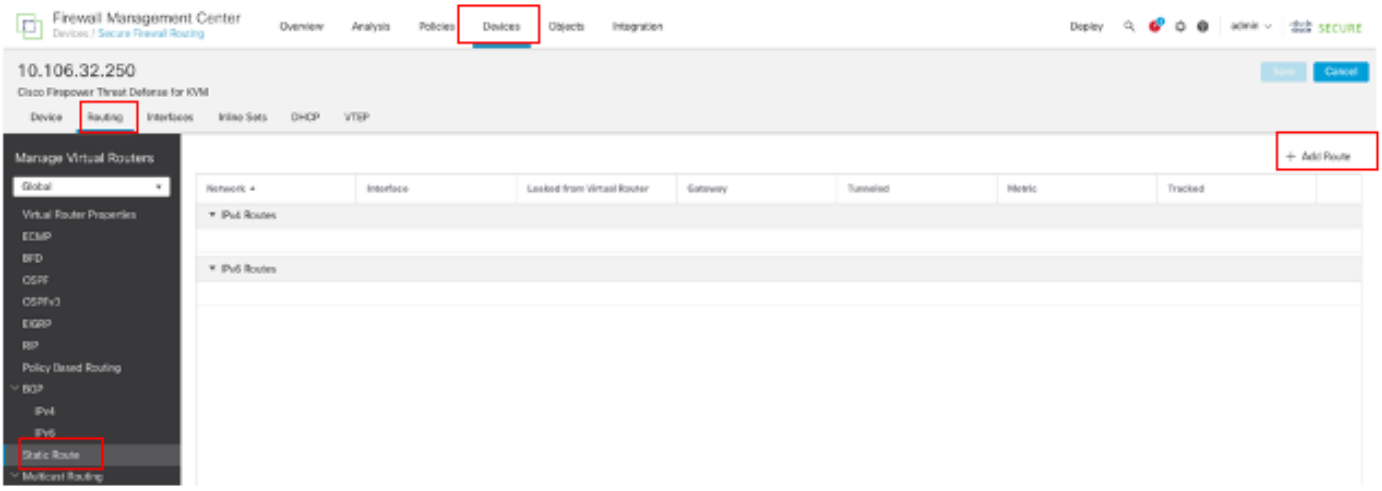


SLA-Objekt Sla-outside2

Schritt 3: Konfigurieren statischer Routen mit Route Track

Navigieren Sie zu Devices > Device Management (Geräte > Gerätemanagement), und bearbeiten Sie das Threat Defense-Gerät. Klicken Sie auf Routing, und wählen Sie in der Dropdown-Liste "Virtual Router" den virtuellen Router aus, für den Sie eine statische Route konfigurieren. In diesem Beispiel Global.

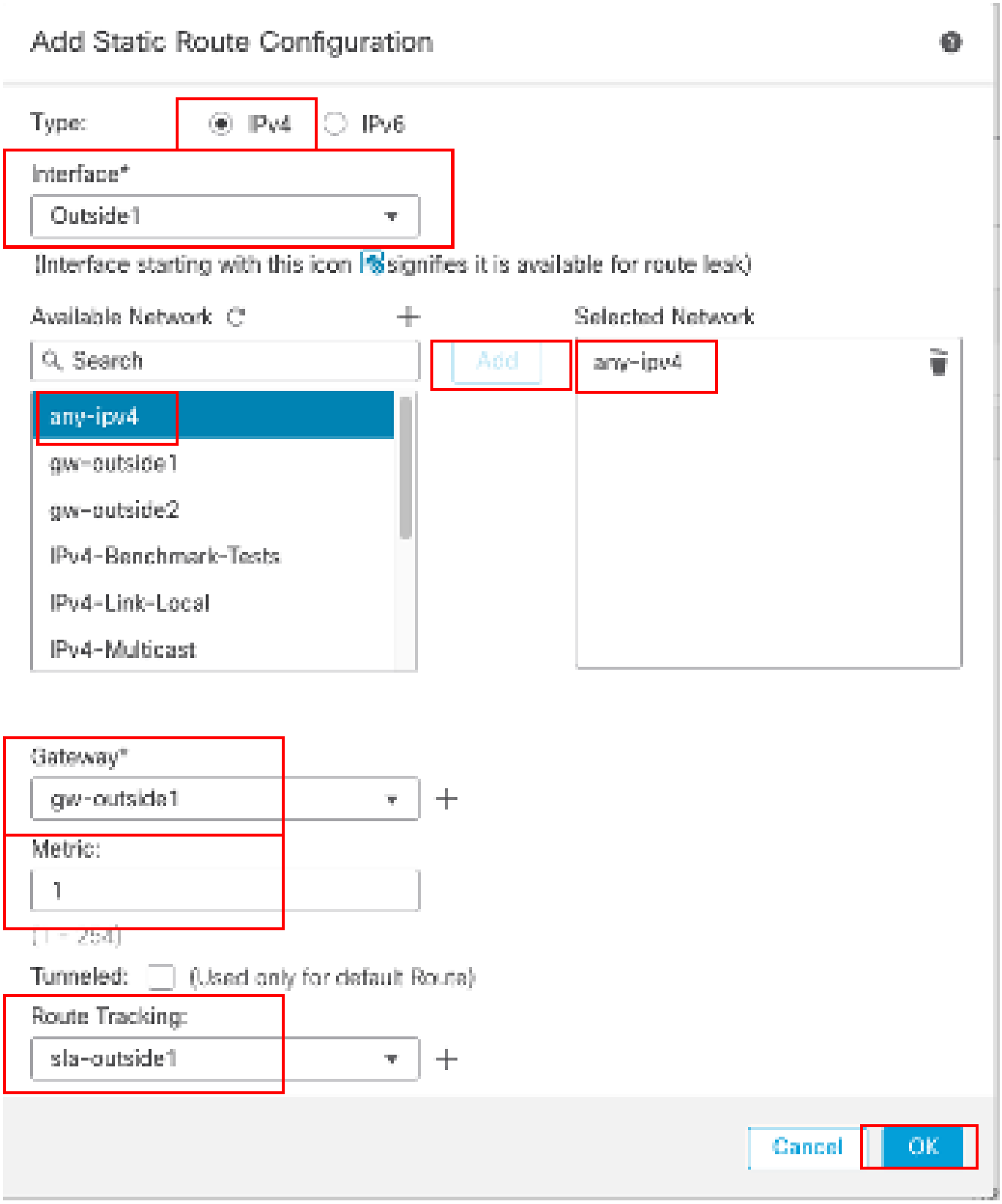
Wählen Sie Statische Route, klicken Sie auf Route hinzufügen, um die Standardroute zum ersten ISP-Gateway hinzuzufügen.



Statische Route konfigurieren

Führen Sie im Fenster Add Static Route Configuration (Statische Routenkonfiguration hinzufügen) folgende Schritte aus:

1. Klicken Sie abhängig vom hinzugefügten Typ der statischen Route auf IPv4 oder IPv6. In diesem Beispiel IPv4.
2. Wählen Sie die Schnittstelle aus, auf die diese statische Route angewendet werden soll. In diesem Beispiel ist Outside1 enthalten.
3. Wählen Sie in der Liste Available Network (Verfügbares Netzwerk) das Zielnetzwerk aus. In diesem Beispiel any-ipv4.
4. Geben Sie im Feld Gateway or IPv6 Gateway (Gateway oder IPv6-Gateway) den Gateway-Router ein, der den nächsten Hop für diese Route darstellt, oder wählen Sie diesen aus. Sie können eine IP-Adresse oder ein Netzwerk-/Hosts-Objekt angeben. In diesem Beispiel gw-outside1.
5. Geben Sie im Feld Metric die Anzahl der Hops zum Zielnetzwerk ein. Gültige Werte liegen zwischen 1 und 255; der Standardwert ist 1. In diesem Beispiel 1.
6. Um die Verfügbarkeit der Route zu überwachen, geben Sie den Namen eines SLA-Überwachungsobjekts, das die Überwachungsrichtlinie definiert, in das Feld Route Tracking (Routenverfolgung) ein, oder wählen Sie diesen aus. In diesem Beispiel sla-outside1.
7. Klicken Sie auf OK.

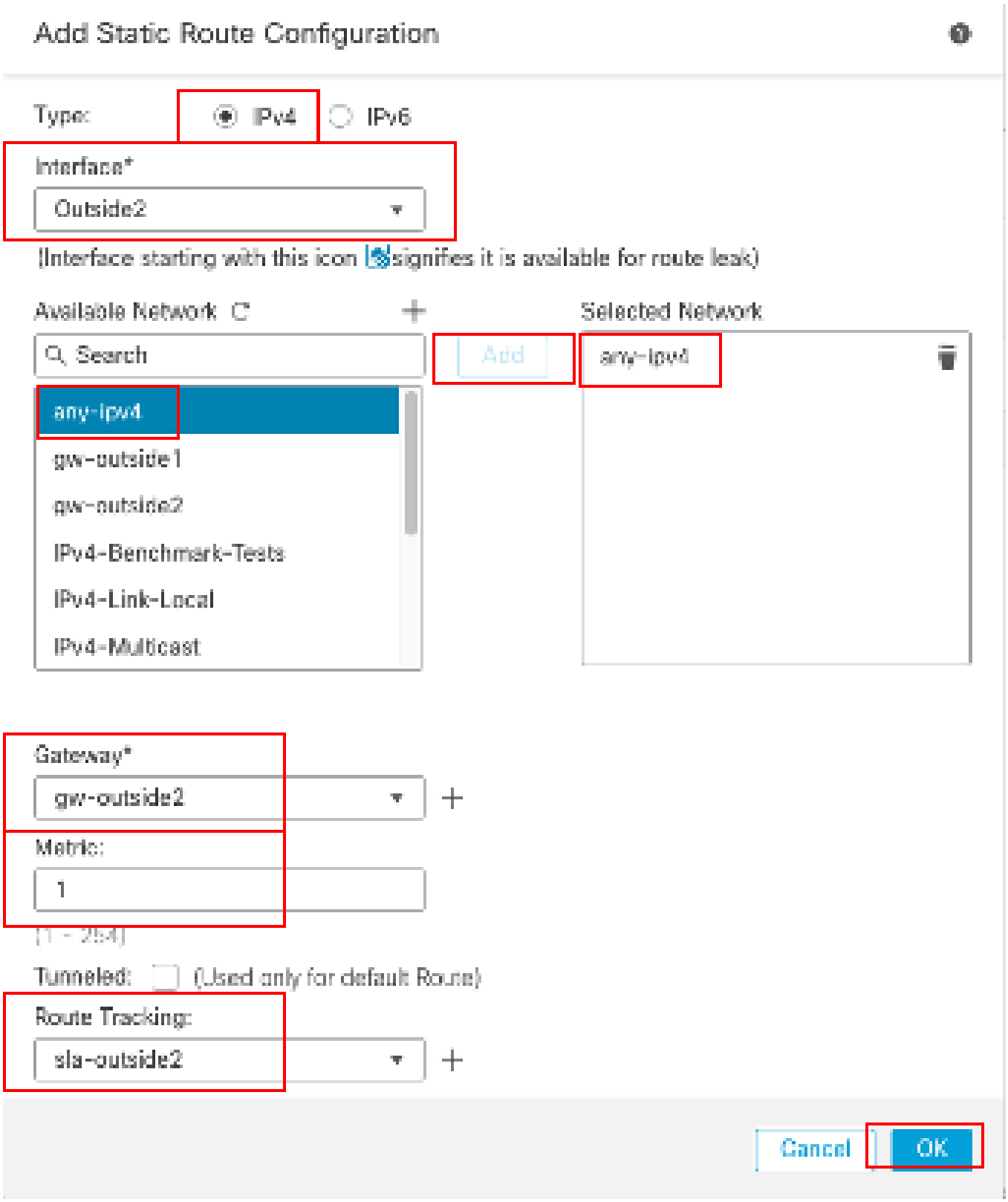


Statische Route ersten ISP hinzufügen

Wiederholen Sie ähnliche Schritte, um die Standardroute zum zweiten ISP-Gateway hinzuzufügen. Führen Sie im Fenster Add Static Route Configuration (Statische Routenkonfiguration hinzufügen) folgende Schritte aus:

1. Klicken Sie abhängig vom hinzugefügten Typ der statischen Route auf IPv4 oder IPv6. In diesem Beispiel IPv4.

2. Wählen Sie die Schnittstelle aus, auf die diese statische Route angewendet werden soll. In diesem Beispiel ist Outside2.
3. Wählen Sie in der Liste Available Network (Verfügbares Netzwerk) das Zielnetzwerk aus. In diesem Beispiel any-ipv4.
4. Geben Sie im Feld Gateway or IPv6 Gateway (Gateway oder IPv6-Gateway) den Gateway-Router ein, der den nächsten Hop für diese Route darstellt, oder wählen Sie diesen aus. Sie können eine IP-Adresse oder ein Netzwerk-/Hosts-Objekt angeben. In diesem Beispiel gw-outside2.
5. Geben Sie im Feld Metric die Anzahl der Hops zum Zielnetzwerk ein. Gültige Werte liegen zwischen 1 und 255; der Standardwert ist 1. Stellen Sie sicher, dass Sie die gleiche Metrik wie die erste Route in diesem Beispiel 1 angeben.
6. Um die Verfügbarkeit der Route zu überwachen, geben Sie den Namen eines SLA-Überwachungsobjekts, das die Überwachungsrichtlinie definiert, in das Feld Route Tracking (Routenverfolgung) ein, oder wählen Sie diesen aus. In diesem Beispiel sla-outside2.
7. Klicken Sie auf OK.



Zweiten ISP mit statischer Route hinzufügen

Klicken Sie auf Speichern und Bereitstellen der Konfiguration.

Überprüfung

Melden Sie sich bei der CLI des FTD an, und führen Sie den Befehl aus, **show zone** um Informationen über die ECMP-Verkehrszonen zu überprüfen, einschließlich der Schnittstellen, die zu jeder Zone gehören.

<#root>

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

Zone member(s): 2

Outside2 GigabitEthernet0/1

Outside1 GigabitEthernet0/0

Führen Sie den Befehl show running-config route aus, um die aktuelle Konfiguration für die Routing-Konfiguration zu überprüfen. In diesem Fall gibt es zwei statische Routen mit Routenspuren.

<#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

Führen Sie den Befehl show route aus, um die Routing-Tabelle zu überprüfen. In diesem Fall gibt es zwei Standardrouten, die zu gleichen Kosten über die Schnittstelle outside1 und outside2 geleitet werden. Der Datenverkehr kann zwischen zwei ISP-Schaltungen verteilt werden.

<#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
```

Führen Sie den Befehl aus, **show sla monitor configuration** um die Konfiguration des SLA-Monitors zu überprüfen.

<#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:

Führen Sie den Befehl show sla monitor operational-state aus, um den Status des SLA-Monitors zu bestätigen. In diesem Fall finden Sie in der Befehlsausgabe "**Timeout failed: FALSE**". Dies zeigt an, dass das ICMP-Echo auf das Gateway antwortet, sodass die Standardroute über die Zielschnittstelle aktiv ist und in der Routing-Tabelle installiert ist.

<#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

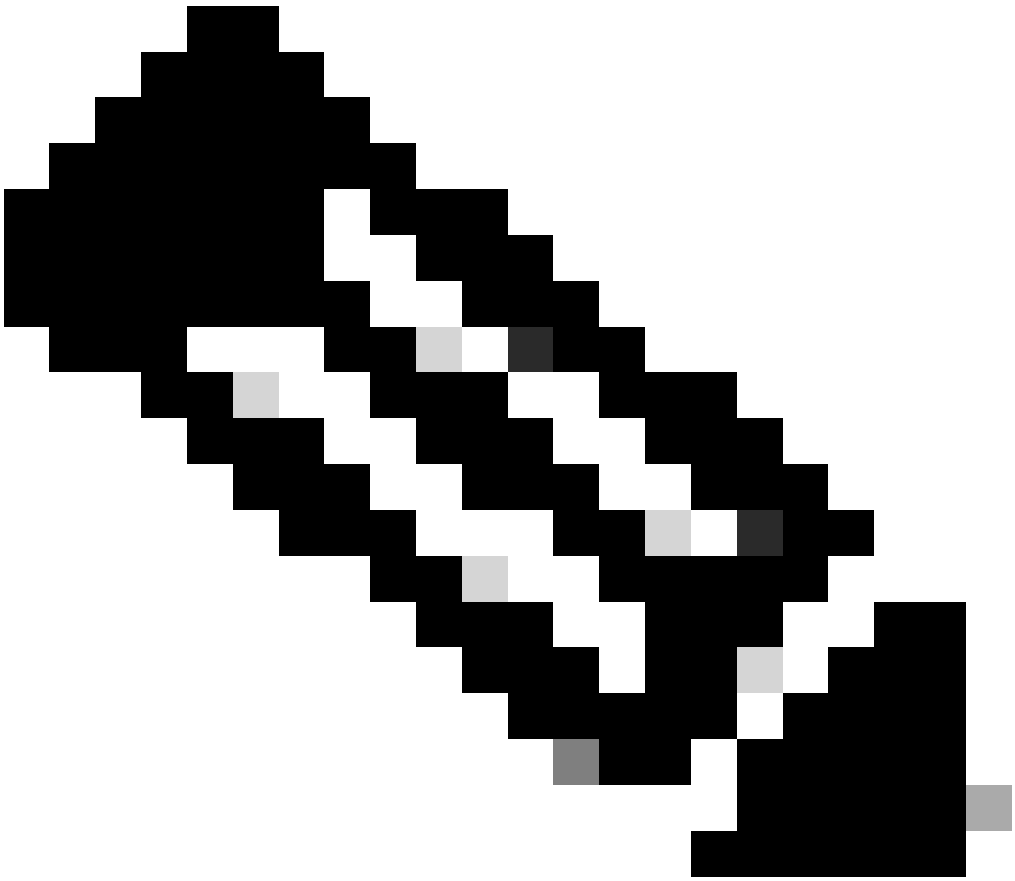
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Lastenausgleich

Ursprünglicher Datenverkehr über FTD, um zu überprüfen, ob ECMP-Lastenausgleich für den Datenverkehr zwischen den Gateways in der ECMP-Zone erfolgt. Initiieren Sie in diesem Fall die Telnet-Verbindung von Inside-Host1 (10.1.3.2) und Inside-Host2 (10.1.3.4) zum Internet-Host (10.1.5.2). Führen Sie den Befehl aus, **show conn** um sicherzustellen, dass der Datenverkehr ein Load Balancing zwischen zwei ISP-Verbindungen durchläuft: Inside-Host1 (10.1.3.2) die Schnittstelle außerhalb1. Inside-Host2 (10.1.3.4) durchläuft die Schnittstelle outside2.

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

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



Hinweis: Der Datenverkehr wird auf der Grundlage eines Algorithmus, der die Quell- und Ziel-IP-Adressen, die eingehende

---

Schnittstelle, das Protokoll, die Quell- und Ziel-Ports hasht, auf die angegebenen Gateways verteilt. Wenn Sie den Test ausführen, kann der von Ihnen simulierte Datenverkehr aufgrund des Hash-Algorithmus an dasselbe Gateway geroutet werden. Dies wird erwartet, indem Sie einen beliebigen Wert zwischen den 6 Tupeln (Quell-IP, Ziel-IP, eingehende Schnittstelle, Protokoll, Quell-Port, Quell-Port) Änderungen am Hashergebnis vornehmen.

Verlorene Route

Wenn die Verbindung zum ersten ISP-Gateway unterbrochen ist, fahren Sie in diesem Fall den ersten Gateway-Router herunter, um die Simulation durchzuführen. Wenn der FTD innerhalb des im SLA Monitor-Objekt angegebenen Timer-Schwellenwerts keine Echoantwort vom ersten ISP-Gateway erhält, gilt der Host als nicht erreichbar und als inaktiv (down) markiert. Die verfolgte Route zum ersten Gateway wird ebenfalls aus der Routing-Tabelle entfernt.

Führen Sie den Befehl show sla monitor operational-state aus, um den aktuellen Status des SLA-Monitors zu bestätigen. In diesem Fall finden Sie in der Befehlsausgabe "Timeout failed: True". Dies zeigt an, dass das ICMP-Echo auf das erste ISP-Gateway nicht reagiert.

<#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
```

Führen Sie den Befehl aus, **show route** um die aktuelle Routing-Tabelle zu überprüfen. Die Route zum ersten ISP-Gateway über die Schnittstelle outside1 wird entfernt. Es gibt nur eine aktive Standardroute zum zweiten ISP-Gateway über die Schnittstelle outside2.

<#root>

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.1.2.2 to network 0.0.0.0
```

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

```
C 10.1.1.0 255.255.255.0 is directly connected, Outside1
```

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

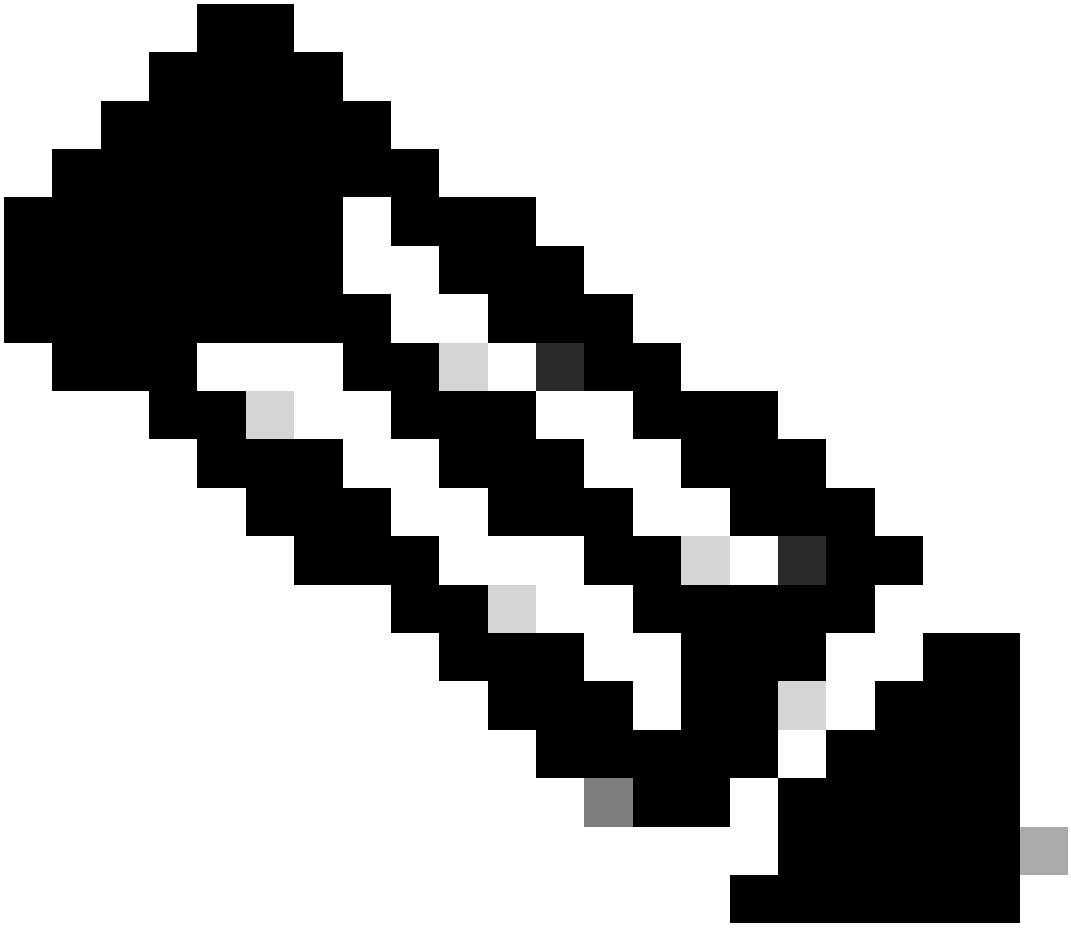
Führen Sie den Befehl show conn aus, um festzustellen, dass die beiden Verbindungen noch aktiv sind. telnet-Sitzungen sind auch auf Inside-Host1 (10.1.3.2) und Inside-Host2 (10.1.3.4) ohne Unterbrechung aktiv.

<#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
```



Hinweis: In der Ausgabe von show conn wird festgestellt, dass die Telnet-Sitzung von Inside-Host1 (10.1.3.2) weiterhin die Schnittstelle outside1 durchläuft, obwohl die Standardroute durch die Schnittstelle outside1 aus der Routing-Tabelle entfernt wurde. Dies wird erwartet, und der tatsächliche Datenverkehr fließt laut Entwurf über die Schnittstelle outside2. Wenn Sie eine neue Verbindung von Inside-Host1 (10.1.3.2) zu Internet-Host (10.1.5.2) initiieren, können Sie feststellen, dass der gesamte Datenverkehr über die Schnittstelle outside2 läuft.

Fehlerbehebung

Führen Sie den Befehl debug ip routing aus, um die Änderung der Routing-Tabelle zu überprüfen.

Wenn in diesem Beispiel die Verbindung zum ersten ISP-Gateway ausfällt, wird die Route über die Schnittstelle outside1 aus der Routing-Tabelle entfernt.

<#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
```

Führen Sie den Befehl show route aus, um die aktuelle Routing-Tabelle zu bestätigen.

<#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
```

Wenn die Verbindung zum ersten ISP-Gateway wieder besteht, wird die Route über die Schnittstelle outside1 wieder der Routing-Tabelle hinzugefügt.

<#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

Führen Sie den Befehl show route aus, um die aktuelle Routing-Tabelle zu bestätigen.

<#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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.