

Konfigurieren von ECMP mit IP SLA auf von FDM verwaltetem FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Schritt 0: Schnittstellen/Objekte vorkonfigurieren](#)

[Schritt 1: Konfigurieren der ECMP-Zone](#)

[Schritt 2: IP SLA-Objekte konfigurieren](#)

[Schritt 3: Konfigurieren statischer Routen mit Route Track](#)

[Überprüfung](#)

[Lastenausgleich](#)

[Verlorene Route](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie ECMP zusammen mit IP SLA auf einem FTD konfiguriert wird, das von FDM 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 Device Manager (FDM)

Verwendete Komponenten

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

- Cisco FTD Version 7.4.1 (Build 172)

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 FDM 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

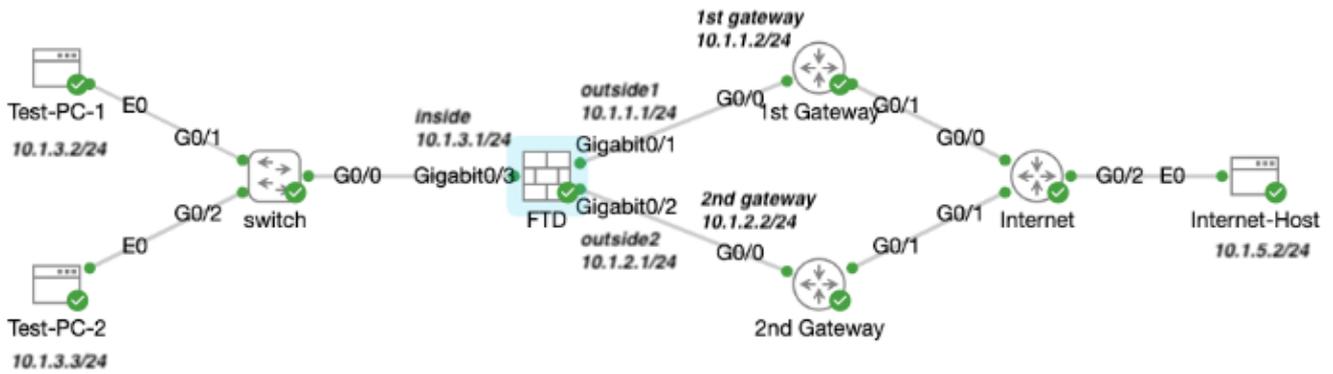
Konfigurieren

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.

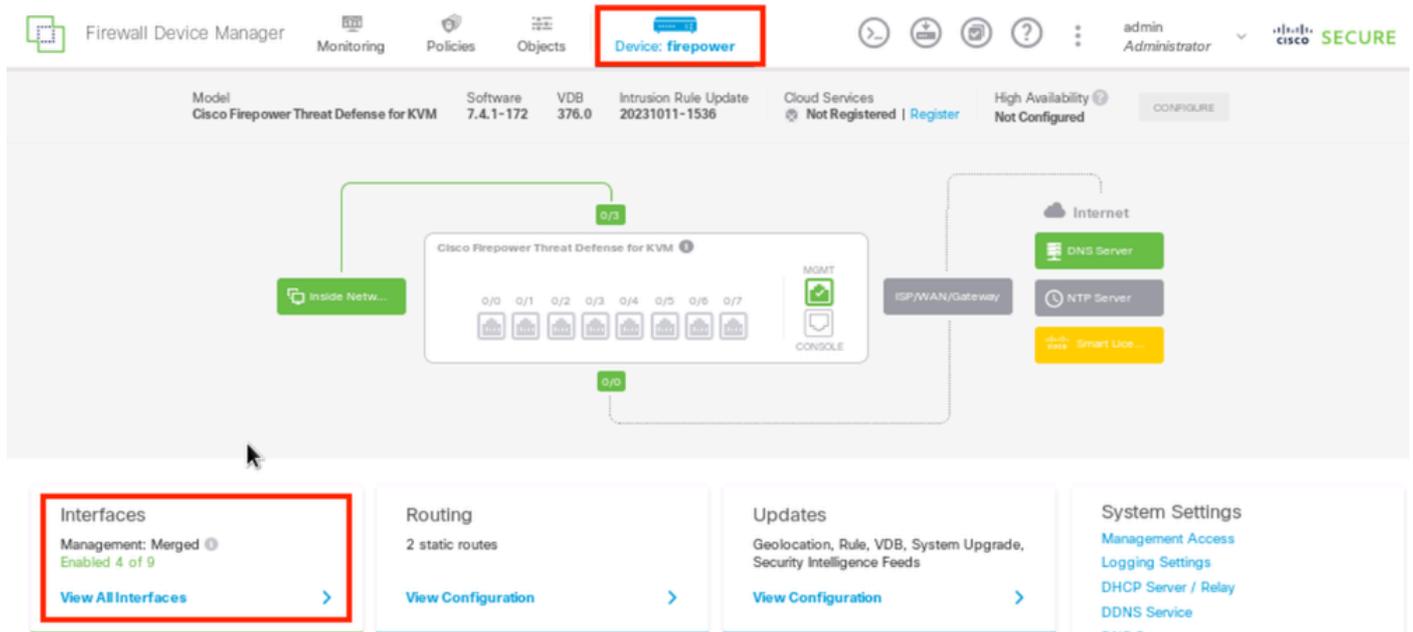


Netzwerkdigramm

Konfigurationen

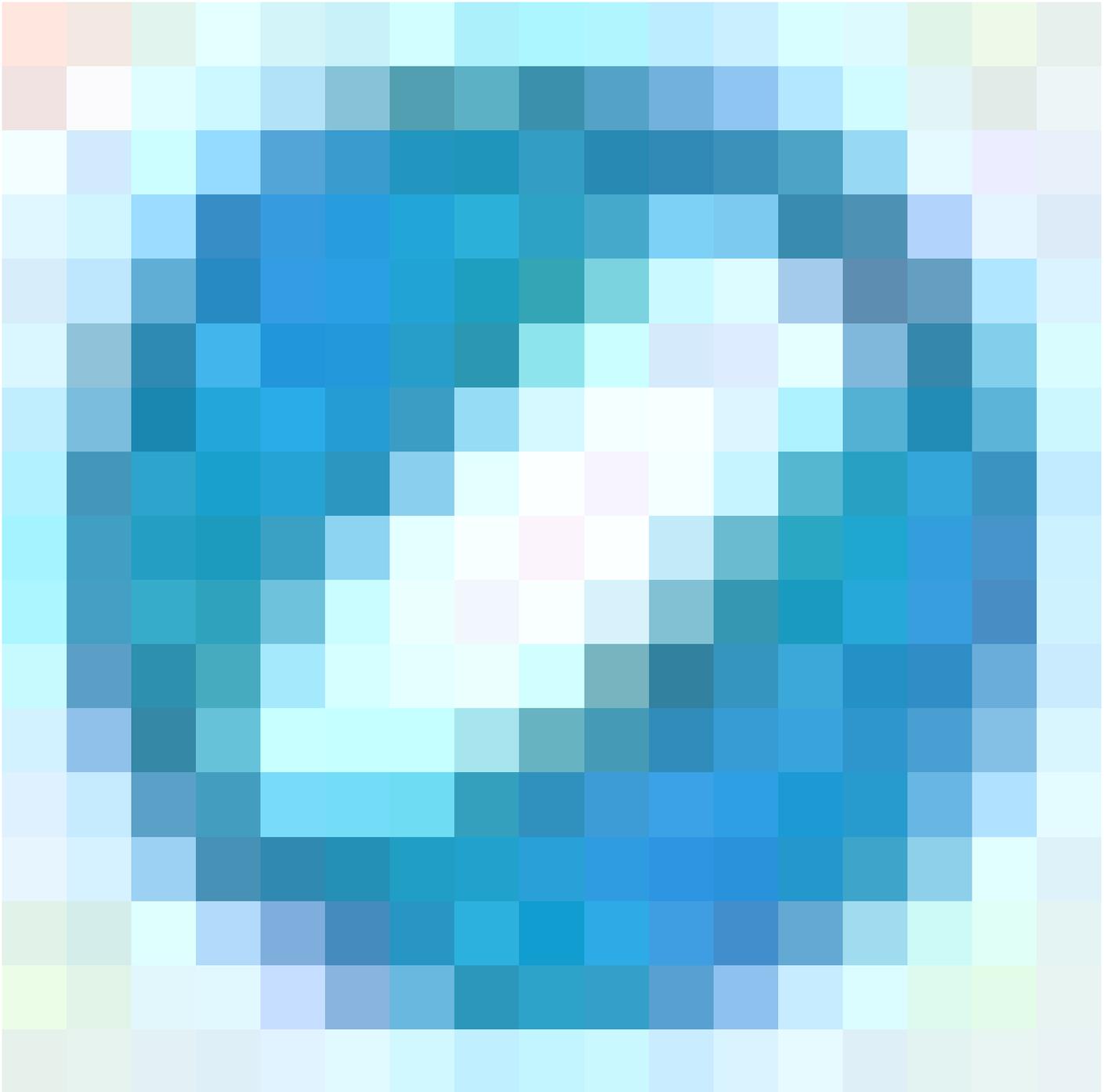
Schritt 0: Schnittstellen/Objekte vorkonfigurieren

Melden Sie sich bei der FDM-Web-GUI an, klicken Sie auf Device (Gerät), und klicken Sie dann auf den Link in der Übersicht der Schnittstellen. Die Schnittstellenliste zeigt die verfügbaren Schnittstellen, deren Namen, Adressen und Status.



FDM-Geräteschnittstelle

Klicken Sie auf das Bearbeitungssymbol (



) für die physische Schnittstelle, die Sie bearbeiten möchten. In diesem Beispiel GigabitEthernet0/1.

Firewall Device Manager

Monitoring Policies Objects Device: firepower

admin Administrator

Device Summary

Interfaces

Cisco Firepower Threat Defense for KVM

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

MGMT

CONSOLE

Interfaces Virtual Tunnel Interfaces

9 Interfaces

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

Schritt 0 Schnittstelle Gi0/1

Führen Sie im Fenster Edit Physical Interface (Physische Schnittstelle bearbeiten) folgende Schritte aus:

1. Legen Sie den Schnittstellennamen fest, in diesem Fall außerhalb1 .



2. Stellen Sie den Schieberegler Status auf die aktivierte Einstellung ein ().

3. Klicken Sie auf die Registerkarte IPv4 Address (IPv4-Adresse), und konfigurieren Sie die IPv4-Adresse, in diesem Fall 10.1.1.1/24.

4. Klicken Sie auf OK.

GigabitEthernet0/1 Edit Physical Interface



Interface Name

outside1

Mode

Routed

Status



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

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.1.1

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

CANCEL

OK

Schritt 0 Schnittstelle Gi0/1 bearbeiten



Hinweis: Nur geroutete Schnittstellen können einer ECMP-Zone zugeordnet werden.

Wiederholen Sie ähnliche Schritte, um die Schnittstelle für die sekundäre ISP-Verbindung zu konfigurieren. In diesem Beispiel ist die physische Schnittstelle GigabitEthernet0/2. Führen Sie im Fenster Edit Physical Interface (Physische Schnittstelle bearbeiten) folgende Schritte aus:

1. Legen Sie den Schnittstellennamen fest, in diesem Fall außerhalb von 2.



2. Stellen Sie den Schieberegler Status auf die aktivierte Einstellung ein ().

3. Klicken Sie auf die Registerkarte IPv4 Address (IPv4-Adresse), und konfigurieren Sie die IPv4-Adresse, in diesem Fall 10.1.2.1/24.

4. Klicken Sie auf OK.

GigabitEthernet0/2 Edit Physical Interface

Interface Name
outside2

Mode
Routed

Status

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

Description
|

IPv4 Address IPv6 Address Advanced

Type
Static

IP Address and Subnet Mask
10.1.2.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

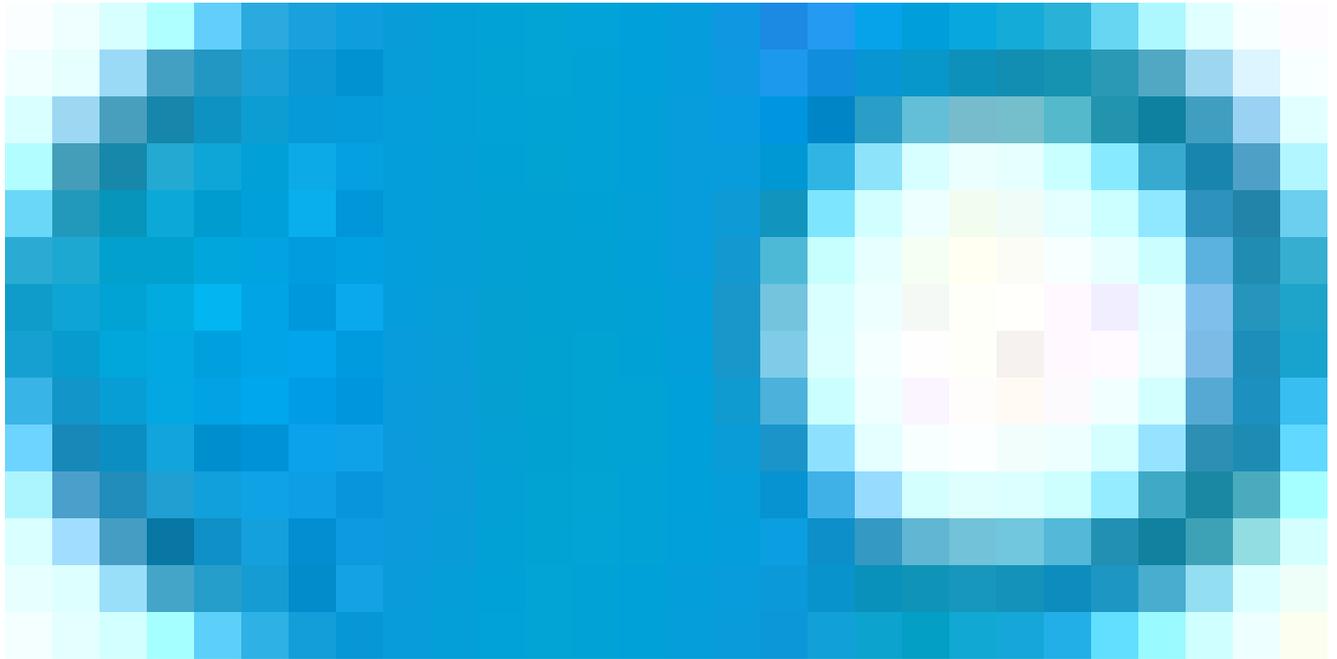
Standby IP Address and Subnet Mask
/
e.g. 192.168.5.16

CANCEL OK

Schritt 0 Schnittstelle Gi0/2 bearbeiten

Wiederholen Sie die ähnlichen Schritte, um die Schnittstelle für die interne Verbindung zu konfigurieren. In diesem Beispiel lautet die physische Schnittstelle GigabitEthernet0/3. Führen Sie im Fenster Edit Physical Interface (Physische Schnittstelle bearbeiten) folgende Schritte aus:

1. Legen Sie den Schnittstellennamen fest, in diesem Fall innerhalb .
2. Stellen Sie den Schieberegler Status auf die aktivierte Einstellung ein (



).

3. Klicken Sie auf die Registerkarte IPv4 Address (IPv4-Adresse), und konfigurieren Sie die IPv4-Adresse, in diesem Fall 10.1.3.1/24.
4. Klicken Sie auf OK.

GigabitEthernet0/3 Edit Physical Interface



Interface Name

inside

Mode

Routed

Status



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

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

10.1.3.1

/

24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

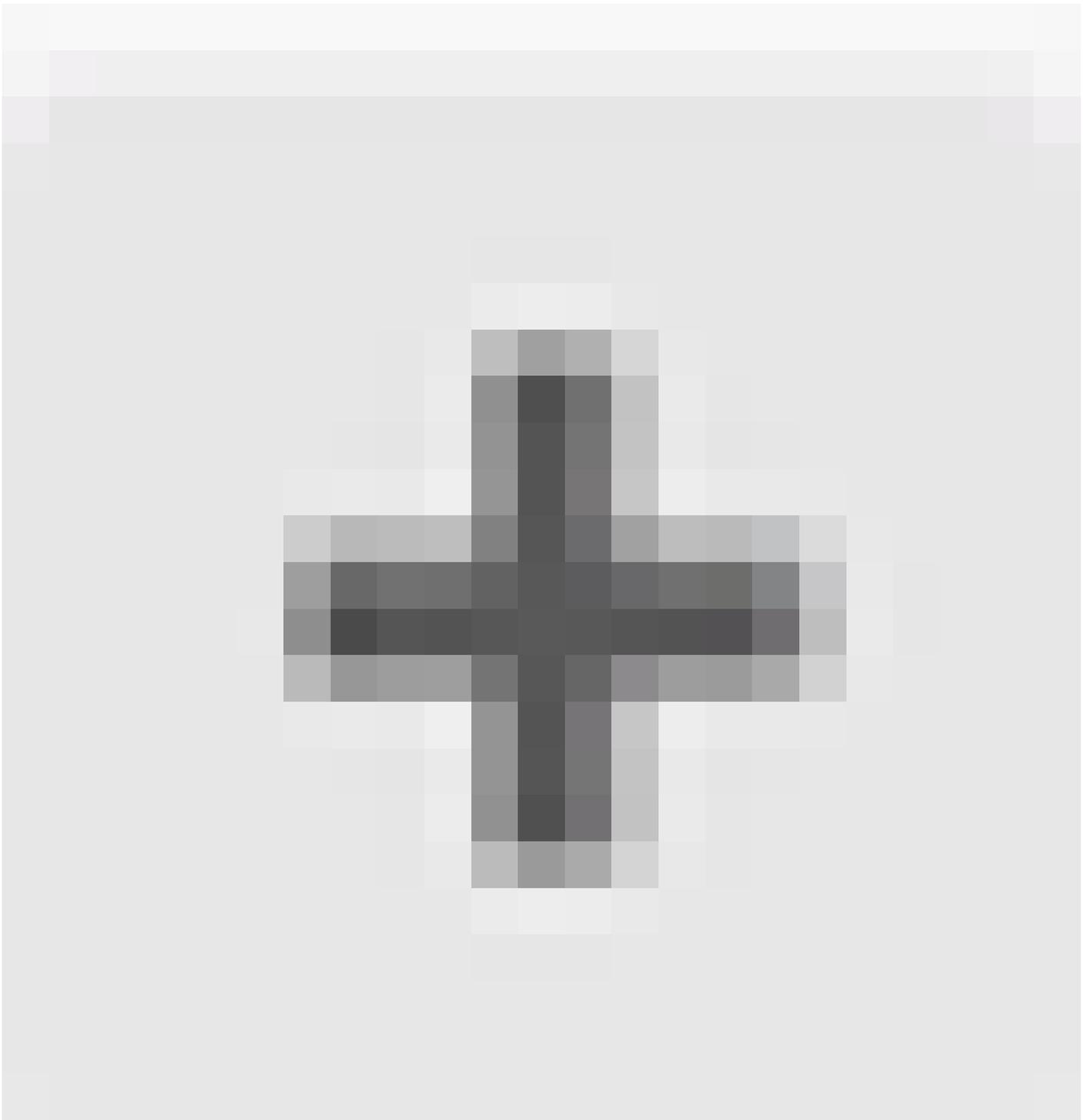
e.g. 192.168.5.16

CANCEL

OK

Schritt 0 Schnittstelle Gi0/3 bearbeiten

Navigieren Sie zu Objekte > Objekttypen > Netzwerke, und klicken Sie auf das Symbol zum Hinzufügen (



), um ein neues Objekt hinzuzufügen.

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

Object Types

- Networks**
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies

Network Objects and Groups

8 objects

Filter +

Preset filters: *Default, Applied, User, Applied*

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

Schritt 0 Objekt 1

Konfigurieren Sie im Fenster Add Network Object (Netzwerkobjekt hinzufügen) den ersten ISP-Gateway:

1. Legen Sie den Namen des Objekts fest, in diesem Fall gw-outside1.
2. Wählen Sie den Typ des Objekts, in diesem Fall Host.
3. Legen Sie die IP-Adresse des Hosts fest, in diesem Fall 10.1.1.2.
4. Klicken Sie auf OK.

Add Network Object



Name

gw-outside1

Description

Type



Network



Host



FQDN



Range

Host

10.1.1.2

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

CANCEL

OK

Schritt 0 Objekt 2

Wiederholen Sie die ähnlichen Schritte, um ein anderes Netzwerkobjekt für das zweite ISP-Gateway zu konfigurieren:

1. Legen Sie den Namen des Objekts fest, in diesem Fall gw-outside2.
2. Wählen Sie den Typ des Objekts, in diesem Fall Host.
3. Legen Sie die IP-Adresse des Hosts fest, in diesem Fall 10.1.2.2.
4. Klicken Sie auf OK.

Add Network Object



Name

gw-outside2

Description

Type



Network



Host



FQDN



Range

Host

10.1.2|2

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

CANCEL

OK

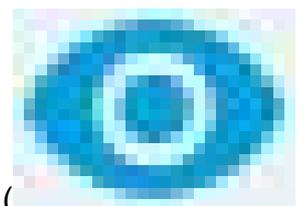


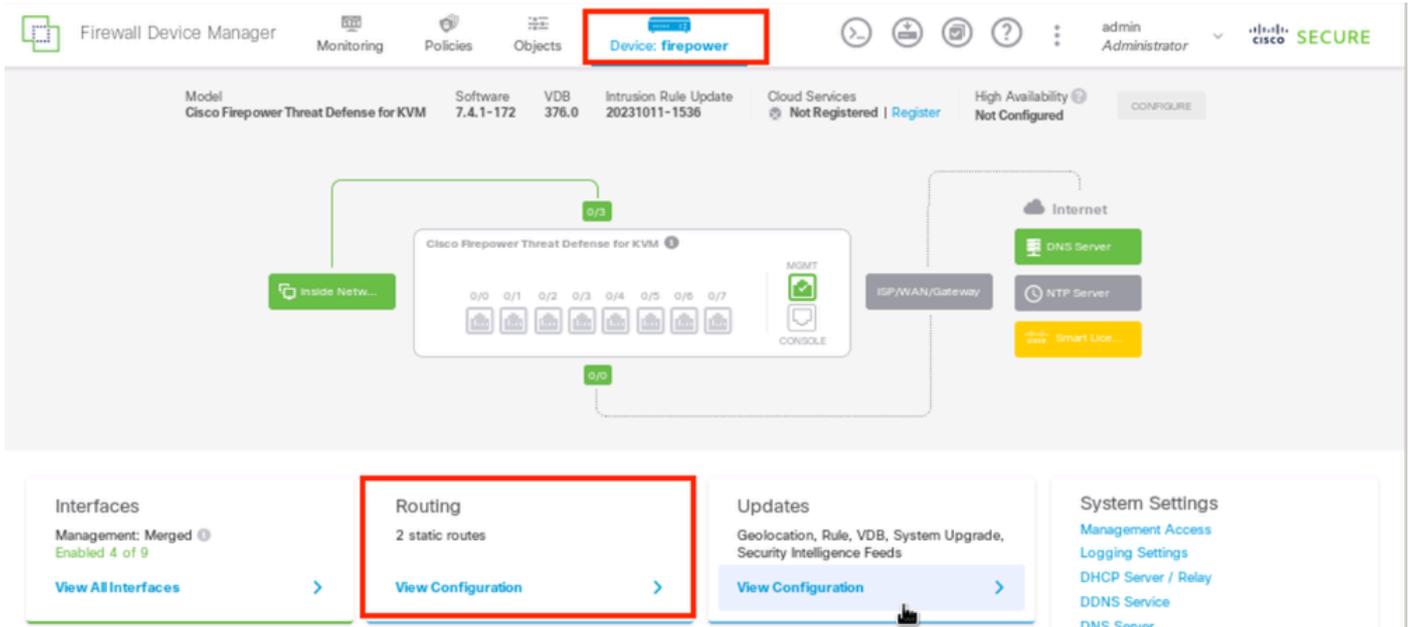
Hinweis: Sie müssen Ihre Zugriffskontrollrichtlinie für FTD konfigurieren, um den Datenverkehr zuzulassen. Dieser Teil ist nicht in diesem Dokument enthalten.

Schritt 1: Konfigurieren der ECMP-Zone

Navigieren Sie zu Device (Gerät), und klicken Sie auf den Link in der Übersicht "Routing".

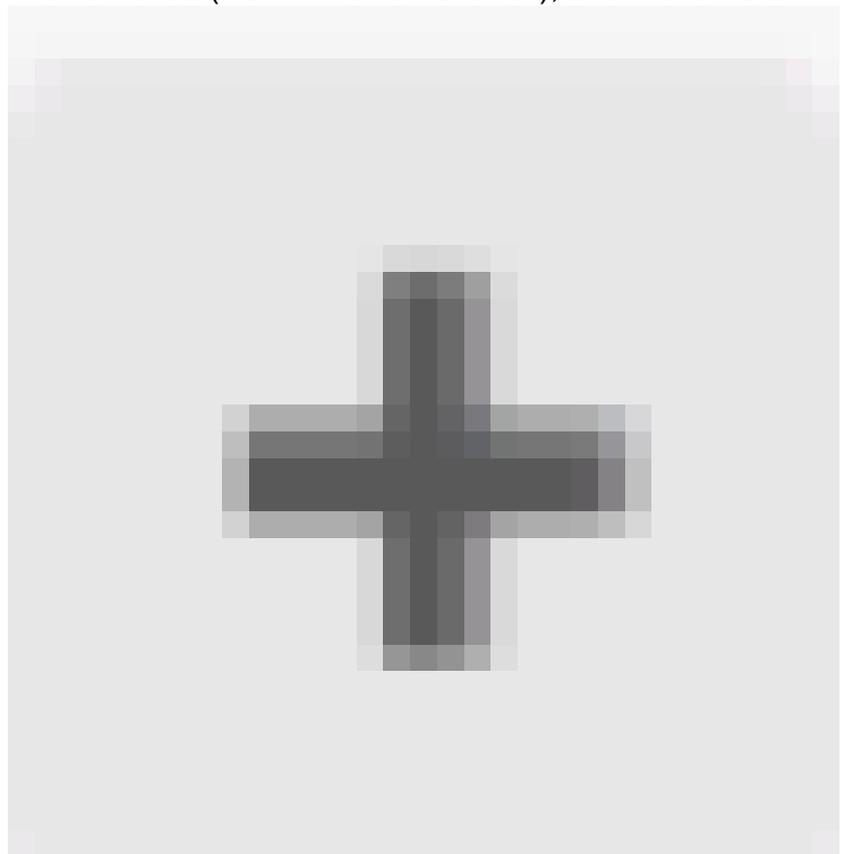


Wenn Sie virtuelle Router aktiviert haben, klicken Sie auf das Ansichtssymbol () für den Router, in dem Sie eine statische Route konfigurieren. In diesem Fall sind virtuelle Router nicht aktiviert.

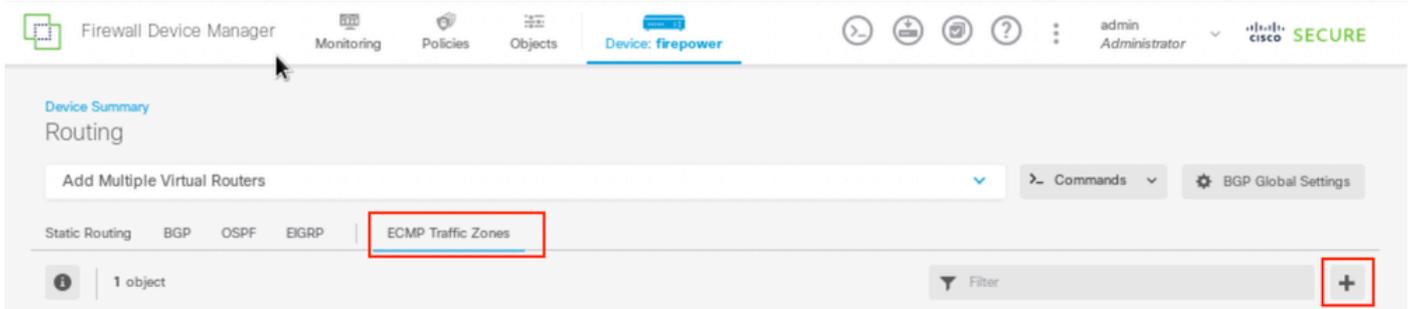


Schritt 1: ECMP-Bereich 1

Klicken Sie auf die Registerkarte ECMP Traffic Zones (ECMP-Verkehrszonen), und klicken Sie



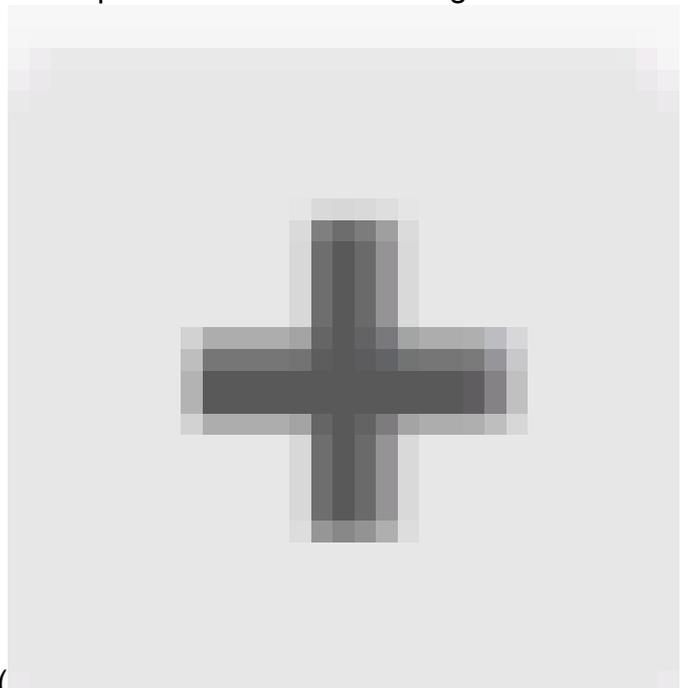
dann auf das Symbol zum Hinzufügen (), um eine neue Zone hinzuzufügen.



Schritt 1: ECMP-Bereich 2

Führen Sie im Fenster Add ECMP Traffic Zone (ECMP-Verkehrszone hinzufügen) folgende Schritte aus:

1. Legen Sie den Namen für den ECMP-Bereich und optional eine Beschreibung fest.



2. Klicken Sie auf das Symbol zum Hinzufügen (), um bis zu 8 Schnittstellen für die Zone auszuwählen. In diesem Beispiel lautet der ECMP-Name Outside, und die Schnittstellen outside1 und outside2 werden der Zone hinzugefügt.
3. Klicken Sie auf OK.

Add ECMP Traffic Zone



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

Name

Outside

Description

Interfaces



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

2 item(s) selected

Create new Subinterface

CANCEL

OK

CANCEL

OK

NETWORK

INSIDE HOST

ADD ECMP TRAFFIC ZONE

Schritt 1: ECMP-Bereich 3

Beide Schnittstellen outside1 und outside2 wurden der ECMP-Zone outside erfolgreich hinzugefügt.

Device Summary
Routing

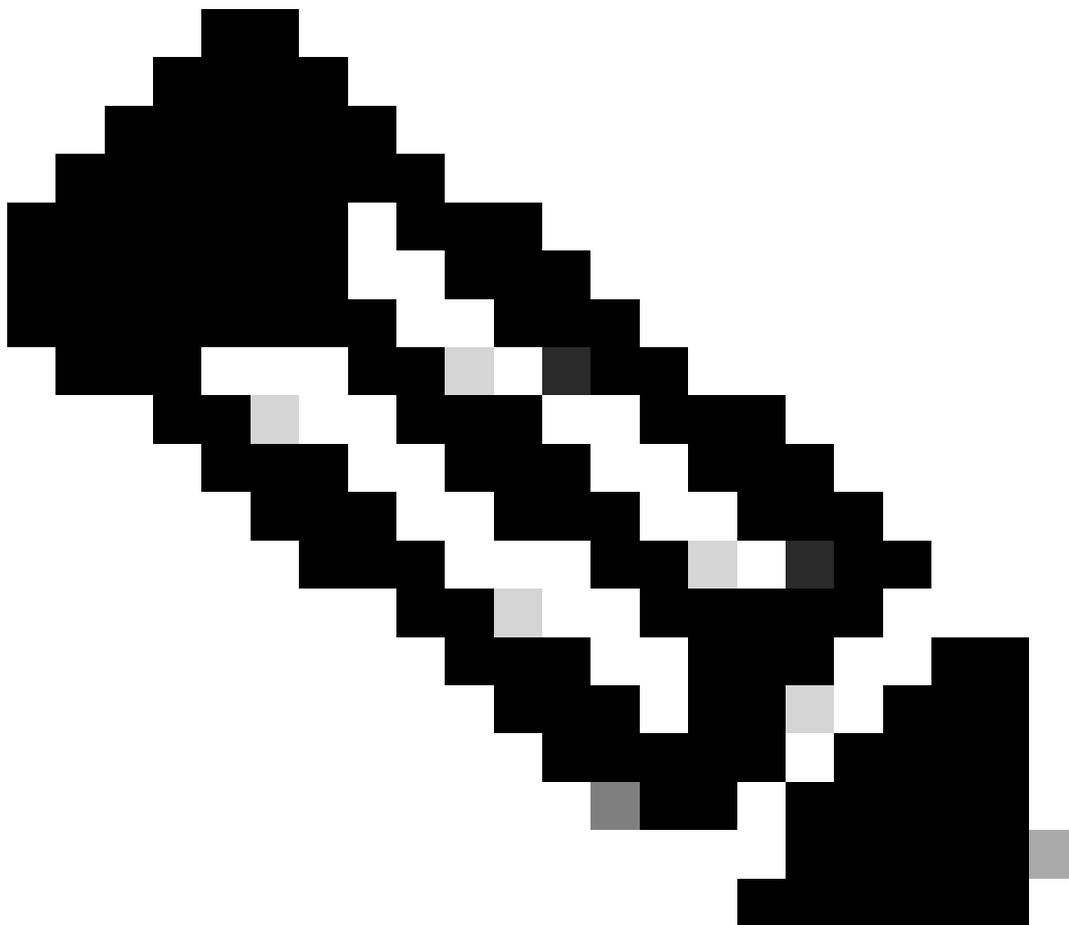
Add Multiple Virtual Routers ⌵ Commands BGP Global Settings

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

1 object Filter +

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

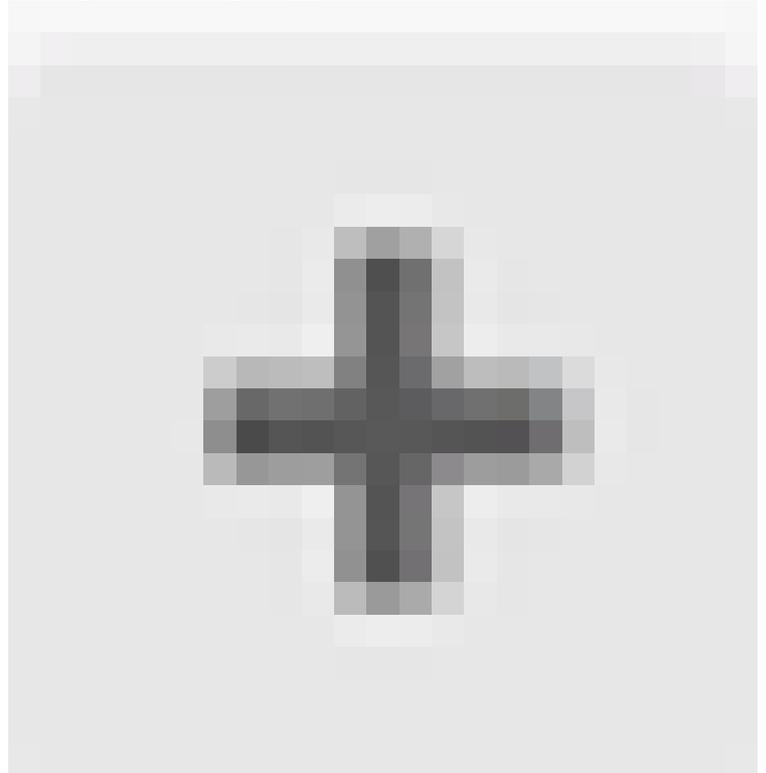
Schritt 1: ECMP-Zone4



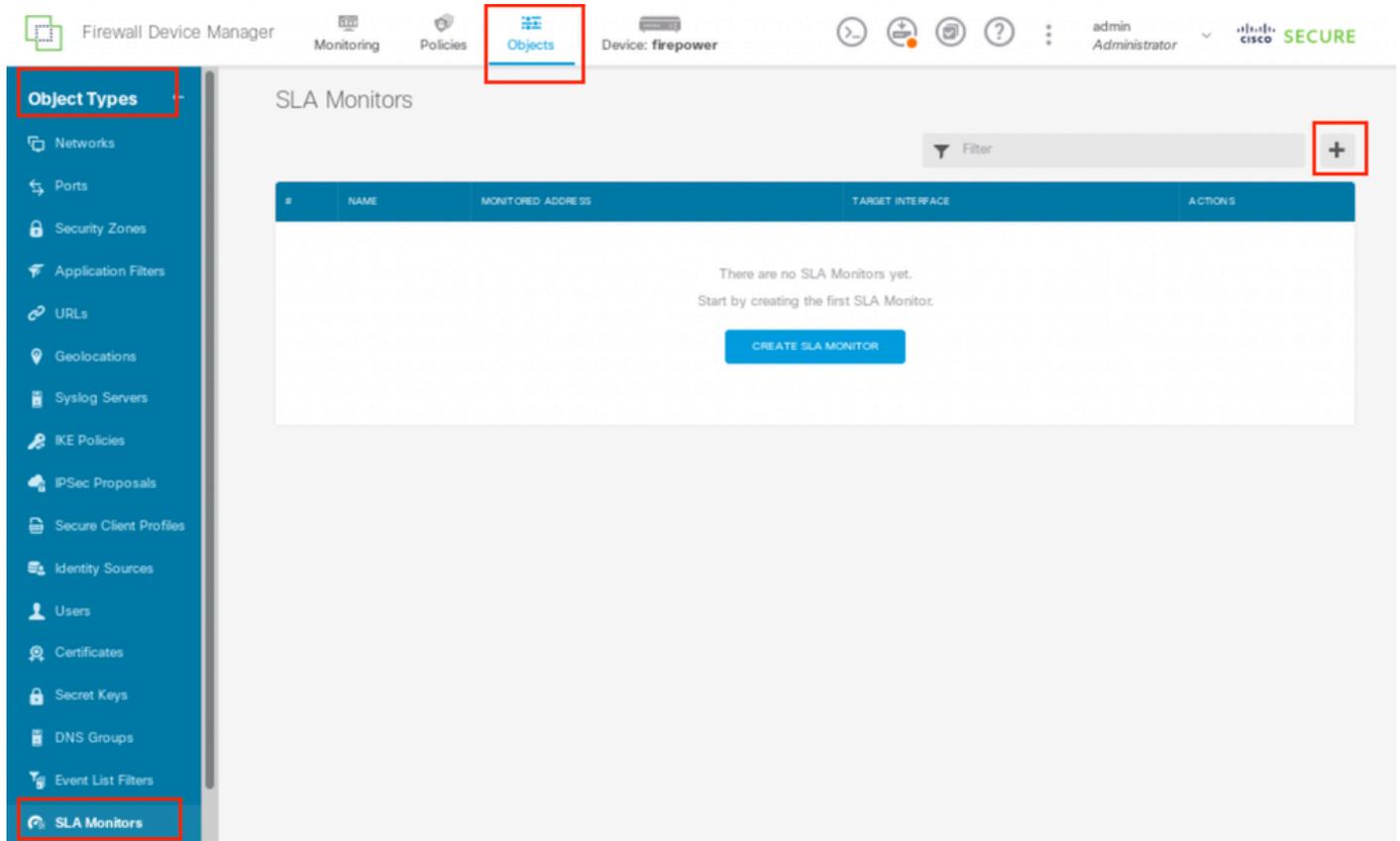
Hinweis: Eine ECMP-Routingverkehrszone hängt nicht mit Sicherheitszonen zusammen. Beim Erstellen einer Sicherheitszone, die die outside1- und outside2-Schnittstellen enthält, wird für das ECMP-Routing keine Datenverkehrszone implementiert.

Schritt 2: IP SLA-Objekte konfigurieren

Um die SLA-Objekte zu definieren, die zum Überwachen der Verbindung zu den einzelnen Gateways verwendet werden, navigieren Sie zu Objekte > Objekttypen > SLA-Monitore, und



klicken Sie auf das Symbol zum Hinzufügen (), um einen neuen SLA-Monitor für die erste ISP-Verbindung hinzuzufügen.



Schritt 2 IP-SLA1

Führen Sie im Fenster Add SLA Monitor Object (SLA-Überwachungsobjekt hinzufügen) folgende Schritte aus:

1. Legen Sie den Namen für das SLA-Überwachungsobjekt und optional eine Beschreibung fest, in diesem Fall sla-outside1.
2. Legen Sie die Überwachungsadresse fest, in diesem Fall gw-outside1 (das erste ISP-Gateway).
3. Legen Sie die Zielschnittstelle fest, über die die Monitoradresse erreichbar ist, in diesem Fall außerhalb1 .
4. Außerdem ist es möglich, die Zeitüberschreitung und den Schwellenwert anzupassen. Klicken Sie auf OK.

Add SLA Monitor Object



Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

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

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

bytes

CANCEL

OK

Wiederholen Sie den ähnlichen Schritt, um ein anderes SLA-Überwachungsobjekt für die zweite ISP-Verbindung im Fenster "SLA-Überwachungsobjekt hinzufügen" zu konfigurieren:

1. Legen Sie den Namen für das SLA-Überwachungsobjekt und optional eine Beschreibung fest, in diesem Fall sla-outside2 .
2. Legen Sie die Überwachungsadresse fest, in diesem Fall gw-outside2 (das zweite ISP-Gateway).
3. Legen Sie die Zielschnittstelle fest, über die die Monitoradresse erreichbar ist, in diesem Fall außerhalb2.
4. Außerdem ist es möglich, die Zeitüberschreitung und den Schwellenwert anzupassen. Klicken Sie auf 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 \leq Timeout \leq Frequency

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

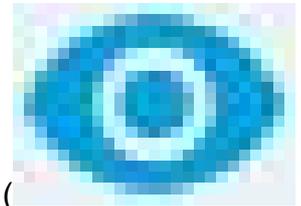
bytes

CANCEL

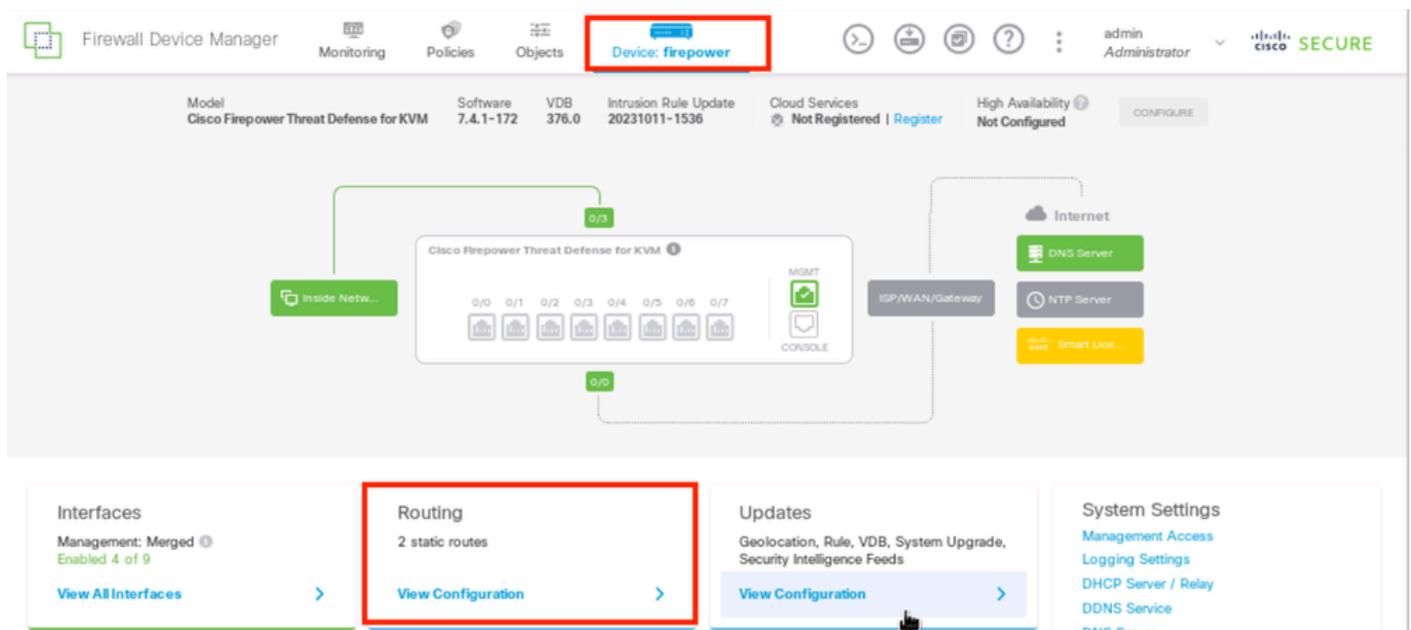
OK

Schritt 3: Konfigurieren statischer Routen mit Route Track

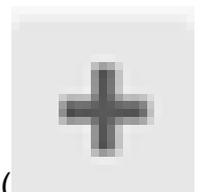
Navigieren Sie zu Device (Gerät), und klicken Sie auf den Link in der Übersicht "Routing".



Wenn Sie virtuelle Router aktiviert haben, klicken Sie auf das Ansichtssymbol () für den Router, in dem Sie eine statische Route konfigurieren. In diesem Fall sind virtuelle Router nicht aktiviert.



Schritt 3 - Route 1



Klicken Sie auf der Seite "Static Routing" (Statisches Routing) auf das Symbol "Add" (), um eine neue statische Route für den ersten ISP-Link hinzuzufügen.

Im Fenster Statische Route hinzufügen:

1. Legen Sie den Namen der Route und optional die Beschreibung fest. In diesem Fall `route_outside1`.
2. Wählen Sie in der Dropdown-Liste Interface (Schnittstelle) die Schnittstelle aus, über die Sie Datenverkehr senden möchten. Die Gateway-Adresse muss über die Schnittstelle zugänglich sein. In diesem Fall außerhalb1 (GigabitEthernet0/1).
3. Wählen Sie die Netzwerke aus, die die Zielnetzwerke oder Hosts identifizieren, die das Gateway in dieser Route verwenden. In diesem Fall ist `any-ipv4` vordefiniert.
4. Wählen Sie aus der Dropdown-Liste Gateway (Gateway) das Netzwerkobjekt aus, das die

IP-Adresse des Gateways identifiziert. Datenverkehr wird an diese Adresse gesendet. In diesem Fall gw-outside1 (das erste ISP-Gateway).

5. Legen Sie die Metrik der Route zwischen 1 und 254 fest. In diesem Beispiel 1.
6. Wählen Sie aus der Dropdown-Liste SLA Monitor (SLA-Monitor) das SLA-Überwachungsobjekt aus. In diesem Fall sla-outside1.
7. Klicken Sie auf OK.

Add Static Route



Name

route_outside1

Description

Interface

outside1 (GigabitEthernet0/1)

Protocol

IPv4 IPv6

Networks



any-ipv4

Gateway

gw-outside1

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside1

CANCEL

OK

Wiederholen Sie den ähnlichen Schritt, um eine weitere statische Route für die zweite ISP-Verbindung im Fenster "Statische Route hinzufügen" zu konfigurieren:

1. Legen Sie den Namen der Route und optional die Beschreibung fest. In diesem Fall `route_outside2`.
2. Wählen Sie in der Dropdown-Liste Interface (Schnittstelle) die Schnittstelle aus, über die Sie Datenverkehr senden möchten. Die Gateway-Adresse muss über die Schnittstelle zugänglich sein. In diesem Fall außerhalb von 2 (GigabitEthernet0/2).
3. Wählen Sie die Netzwerke aus, die die Zielnetzwerke oder Hosts identifizieren, die das Gateway in dieser Route verwenden. In diesem Fall ist `any-ipv4` vordefiniert.
4. Wählen Sie aus der Dropdown-Liste Gateway (Gateway) das Netzwerkobjekt aus, das die IP-Adresse des Gateways identifiziert. Datenverkehr wird an diese Adresse gesendet. In diesem Fall `gw-outside2` (das zweite ISP-Gateway).
5. Legen Sie die Metrik der Route zwischen 1 und 254 fest. In diesem Beispiel 1.
6. Wählen Sie aus der Dropdown-Liste SLA Monitor (SLA-Monitor) das SLA-Überwachungsobjekt aus. In diesem Szenario `sla-outside2`.
7. Klicken Sie auf OK.

Add Static Route



Name

route_outside2

Description

Interface

outside2 (GigabitEthernet0/2)

Protocol

IPv4

IPv6

Networks



any-ipv4

Gateway

gw-outside2

Metric

1

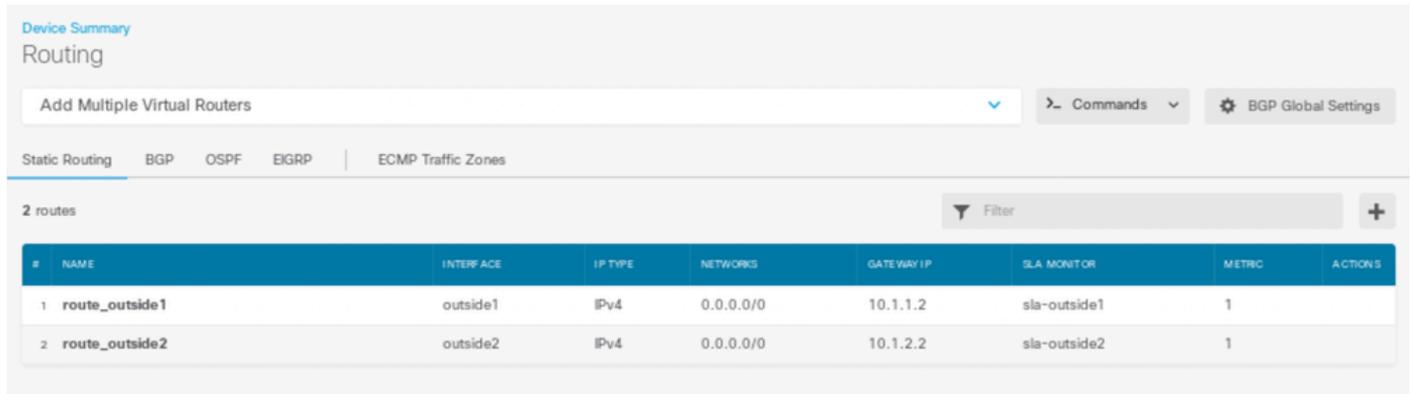
SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

Sie haben 2 Routen über die Schnittstellen Außen1 und Außen2 mit Routengleisen.



The screenshot shows the Cisco ISE Routing configuration page. At the top, there is a 'Device Summary' section with 'Routing' as the main heading. Below this, there are tabs for 'Static Routing', 'BGP', 'OSPF', 'EIGRP', and 'ECMP Traffic Zones'. The 'Static Routing' tab is selected. A search bar contains 'Add Multiple Virtual Routers'. To the right, there are buttons for 'Commands' and 'BGP Global Settings'. Below the tabs, it says '2 routes'. A table lists the routes:

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

Schritt 3 - Route 4

Setzen Sie die Änderung auf FTD ein.

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 den einzelnen Zonen gehören.

```
<#root>
```

```
> show zone
```

```
Zone:
```

```
Outside
```

```
ecmp
```

```
Security-level: 0
```

```
Zone member(s): 2
```

```
outside2 GigabitEthernet0/2
```

```
outside1 GigabitEthernet0/1
```

Führen Sie den Befehl aus, `show running-config route` 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 aus, `show route` 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: 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:

Führen Sie den Befehl `show sla monitor operational-state` aus, um den Status des SLA-Monitors zu bestätigen. In diesem Fall finden Sie im Befehlsausgang "Timeout ist aufgetreten: 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: 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

Lastenausgleich

Ursprünglicher Datenverkehr über FTD, um zu überprüfen, ob ECMP-Lastenausgleich für den Datenverkehr zwischen den Gateways in der ECMP-Zone erfolgt. In diesem Fall starten Sie die SSH-Verbindung von Test-PC-1 (10.1.3.2) und Test-PC-2 (10.1.3.4) zum Internet-Host (10.1.5.2). Führen Sie den Befehl aus, show conn um zu bestätigen, dass der Datenverkehr ein Load Balancing zwischen zwei ISP-Verbindungen aufweist. Test-PC-1 (10.1.3.2) geht durch die Schnittstelle. outside1, Test-PC-2 (10.1.3.4) durchläuft die Schnittstelle outside2.

<#root>

> show conn

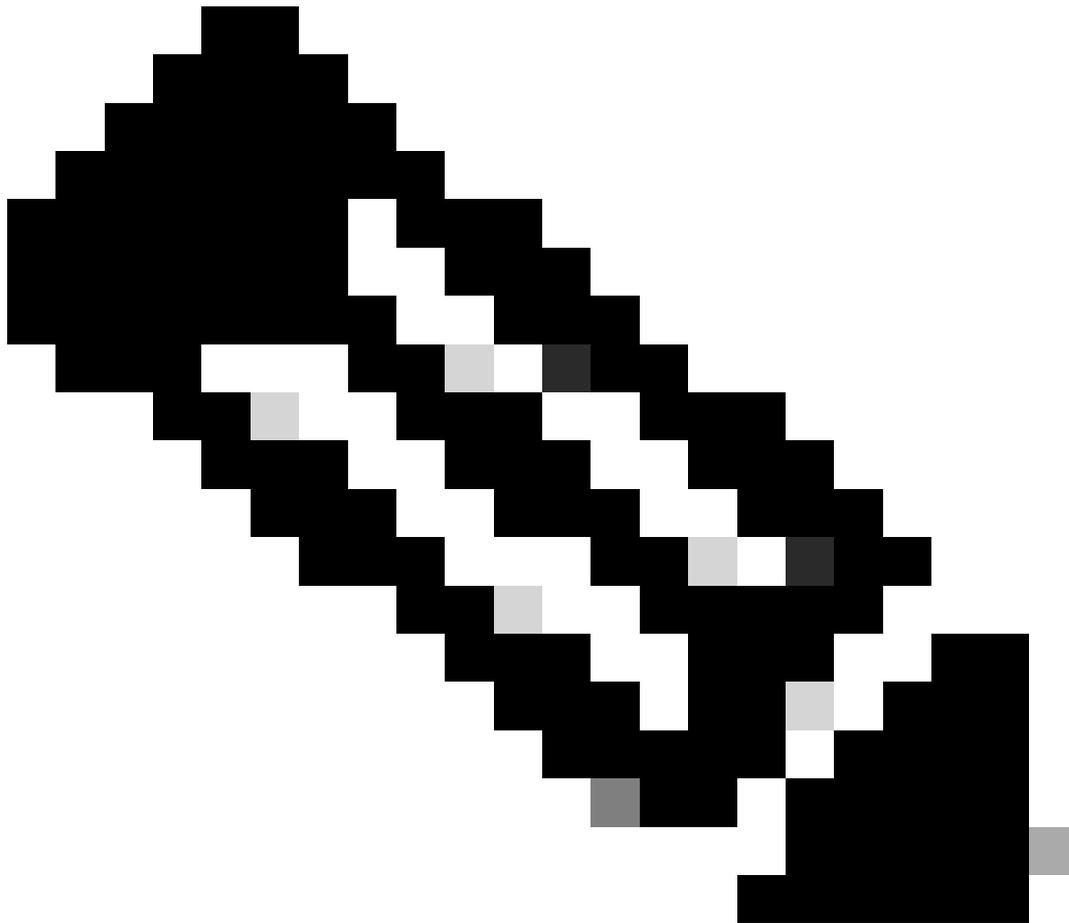
4 in use, 14 most used

Inspect Snort:

preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

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

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, flags UIO N1



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 aus, `show sla monitor operational-state` 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: 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

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
```

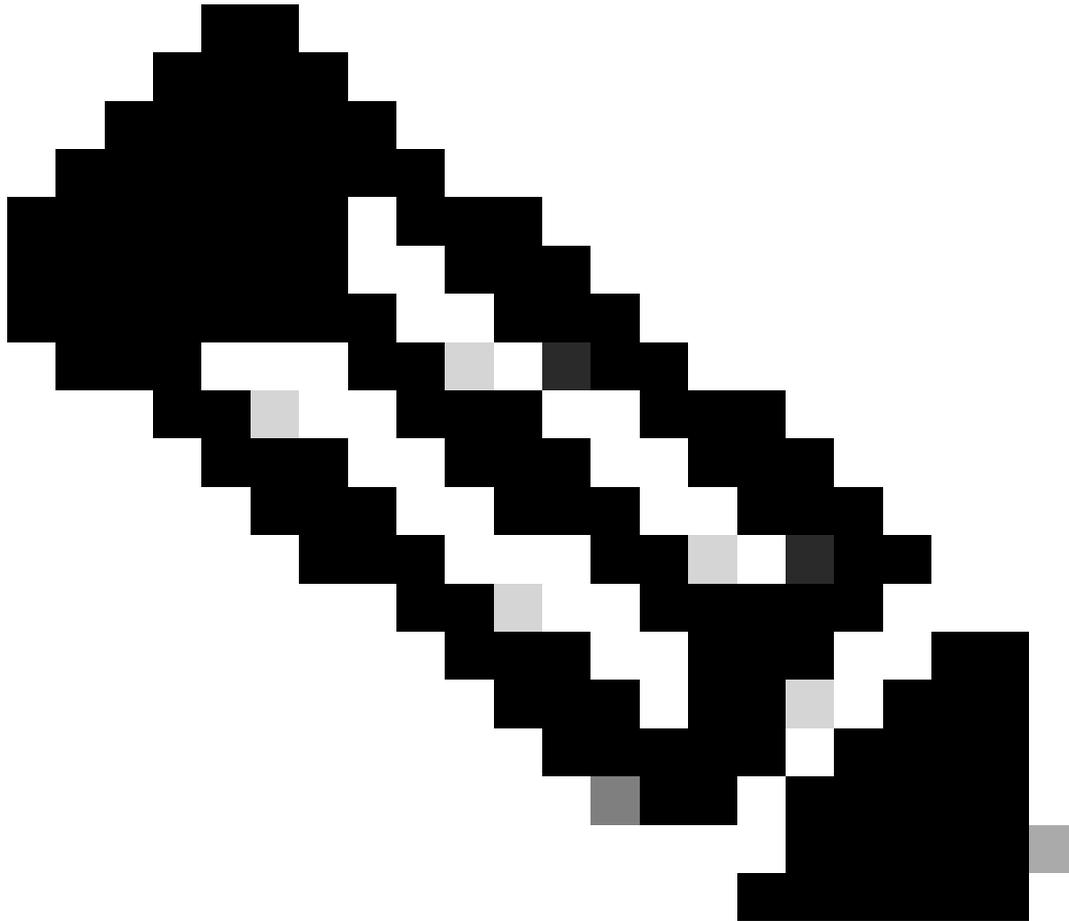
Führen Sie den Befehl `show conn` aus, Sie können feststellen, dass die beiden Verbindungen noch aktiv sind. SSH-Sitzungen sind auch auf Test-PC-1 (10.1.3.2) und Test-PC-2 (10.1.3.4) ohne Unterbrechung aktiv.

```
<#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
```



Hinweis: Sie können in der Ausgabe von `show conn` bemerken, dass die SSH-Sitzung von Test-PC-1 (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 vom Design her durch die Schnittstelle `outside2`. Wenn Sie eine neue Verbindung von Test-PC-1 (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

Um die Änderung der Routing-Tabelle zu überprüfen, führen Sie den Befehl `debug ip routing` aus.

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 0.0.0.0
```

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
```

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
```

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

```
> 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
```

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

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.