ECMP configureren met IP SLA op FTD beheerde via FDM

Inhoud

Inleiding

In dit document wordt beschreven hoe u ECMP samen met IP SLA kunt configureren op een FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ECMP-configuratie op Cisco Secure Firewall Threat Defence (FTD)
- IP SLA-configuratie op Cisco Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Device Manager (FDM)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversie:

- Cisco FTD versie 7.4.1 (Build 172)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft hoe u Equal-Cost Multi-Path (ECMP) kunt configureren in combinatie met een Internet Protocol Service Level Agreement (IP SLA) op een Cisco FTD die wordt beheerd door Cisco FDM. Met het ECMP kunt u interfaces groeperen op FTD-verkeer en taakverdeling over meerdere interfaces. IP SLA is een mechanisme dat end-to-end connectiviteit bewaakt door de uitwisseling van reguliere pakketten. Samen met ECMP kan IP SLA worden geïmplementeerd om de beschikbaarheid van de volgende hop te garanderen. In dit voorbeeld wordt ECMP gebruikt om pakketten gelijkelijk te verdelen over twee internetserviceproviders (ISP's). Tegelijkertijd houdt een IP SLA de connectiviteit bij, waardoor een naadloze overgang naar beschikbare circuits in het geval van een storing wordt gegarandeerd.

Specifieke eisen voor dit document zijn onder meer:

- Toegang tot de apparaten met een gebruikersaccount met beheerdersrechten
- Cisco Secure Firewall Threat Defense versie 7.1 of hoger

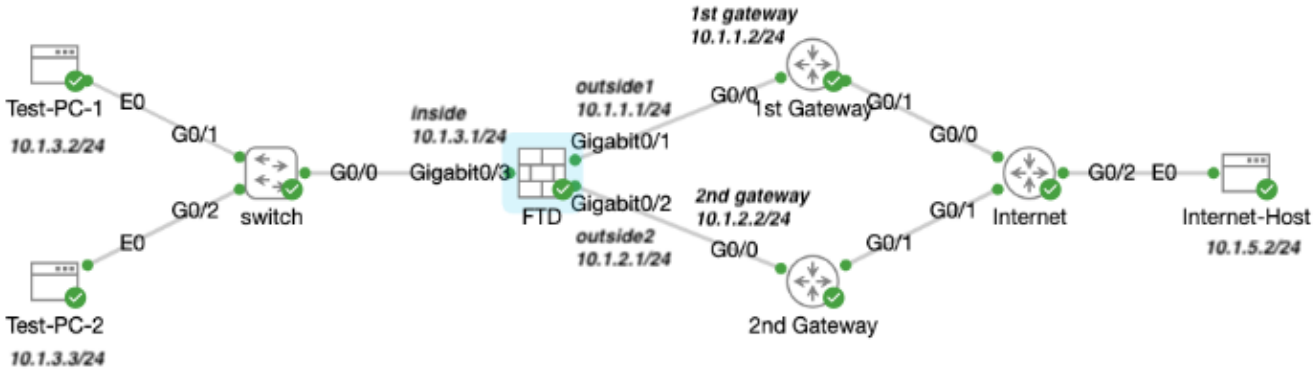
Configureren

Netwerkdiagram

In dit voorbeeld heeft Cisco FTD twee buiteninterfaces: buitenkant1 en buitenkant2 . Elke verbinding met een ISP-gateway, buitenkant1 en buitenkant2 behoren tot dezelfde ECMP-zone die buiten is genoemd.

Het verkeer van het interne netwerk wordt via FTD gerouteerd en wordt via de twee ISP's gebalanceerd met de lading op internet.

Tegelijkertijd maakt FTD gebruik van IP SLA's om de connectiviteit met elke ISP-gateway te bewaken. In het geval van een storing op een van de ISP-circuits, FTD-failovers naar de andere ISP-gateway om de bedrijfscontinuïteit te handhaven.

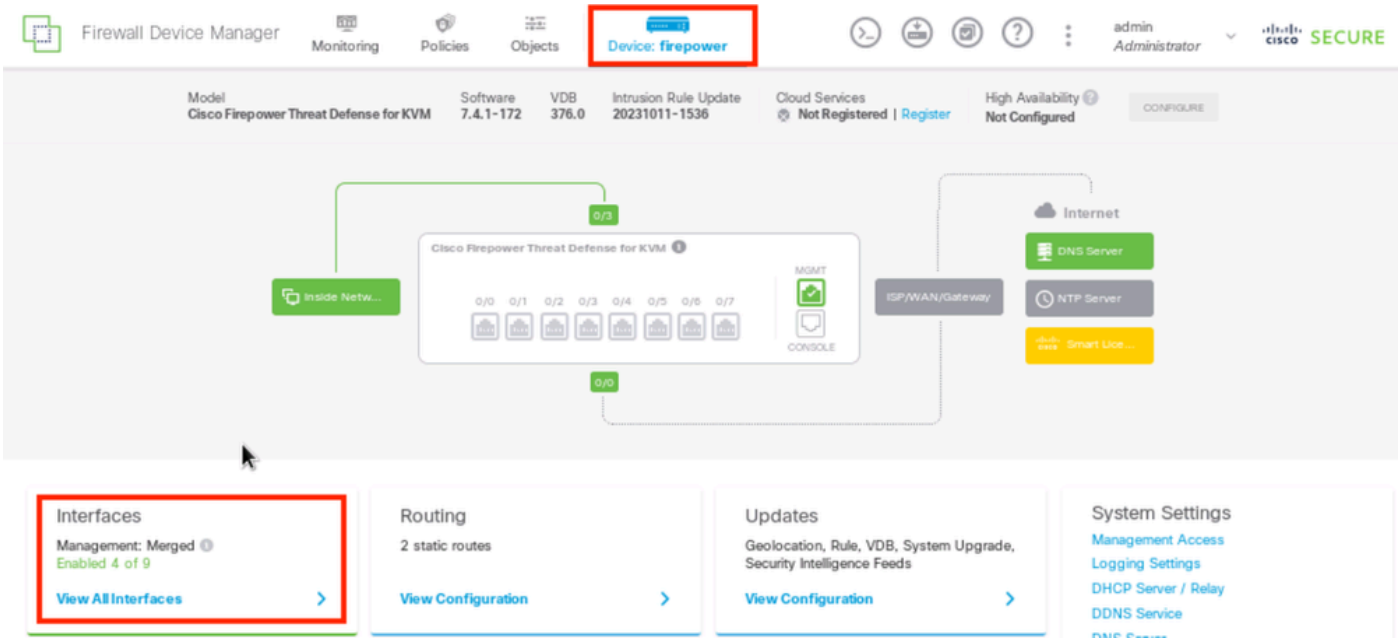


Netwerkdiagram

Configuraties

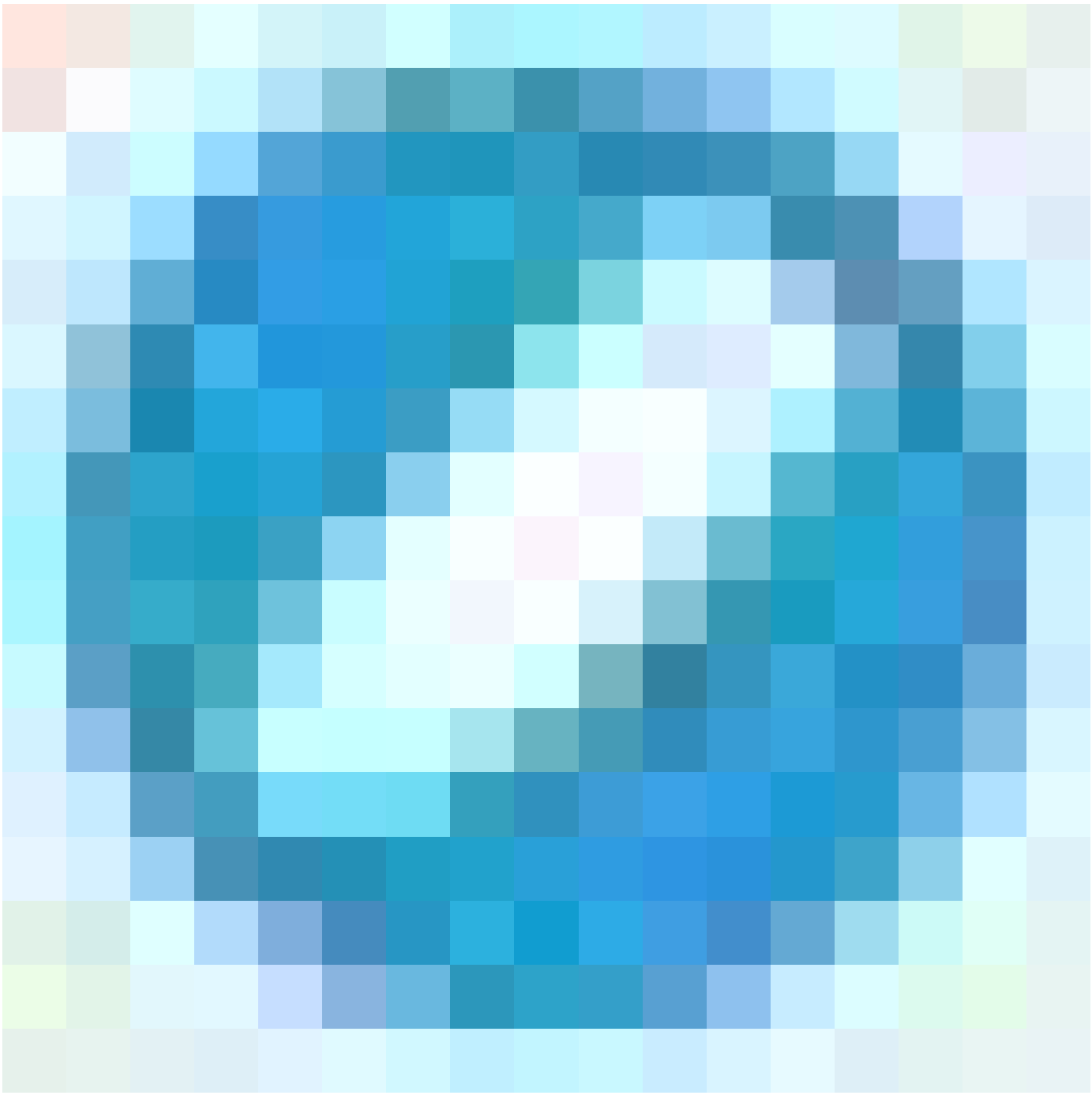
Stap 0. Interfaces/objecten vooraf configureren

Log in de FDM web GUI, klik op Apparaat en klik vervolgens op de link in de samenvatting van Interfaces. De lijst van interfaces toont de beschikbare interfaces, hun namen, adressen, en staten.

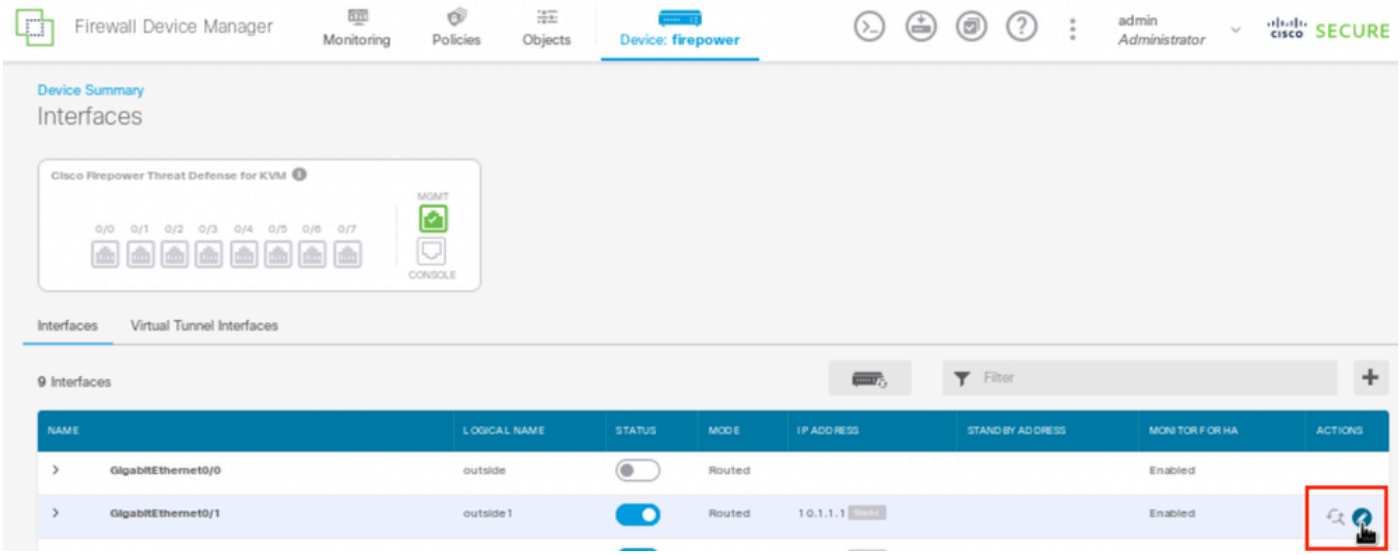


FDM-apparaatinterface

Klik op het pictogram bewerken (

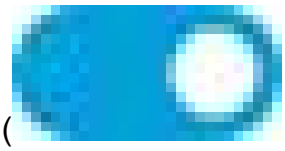


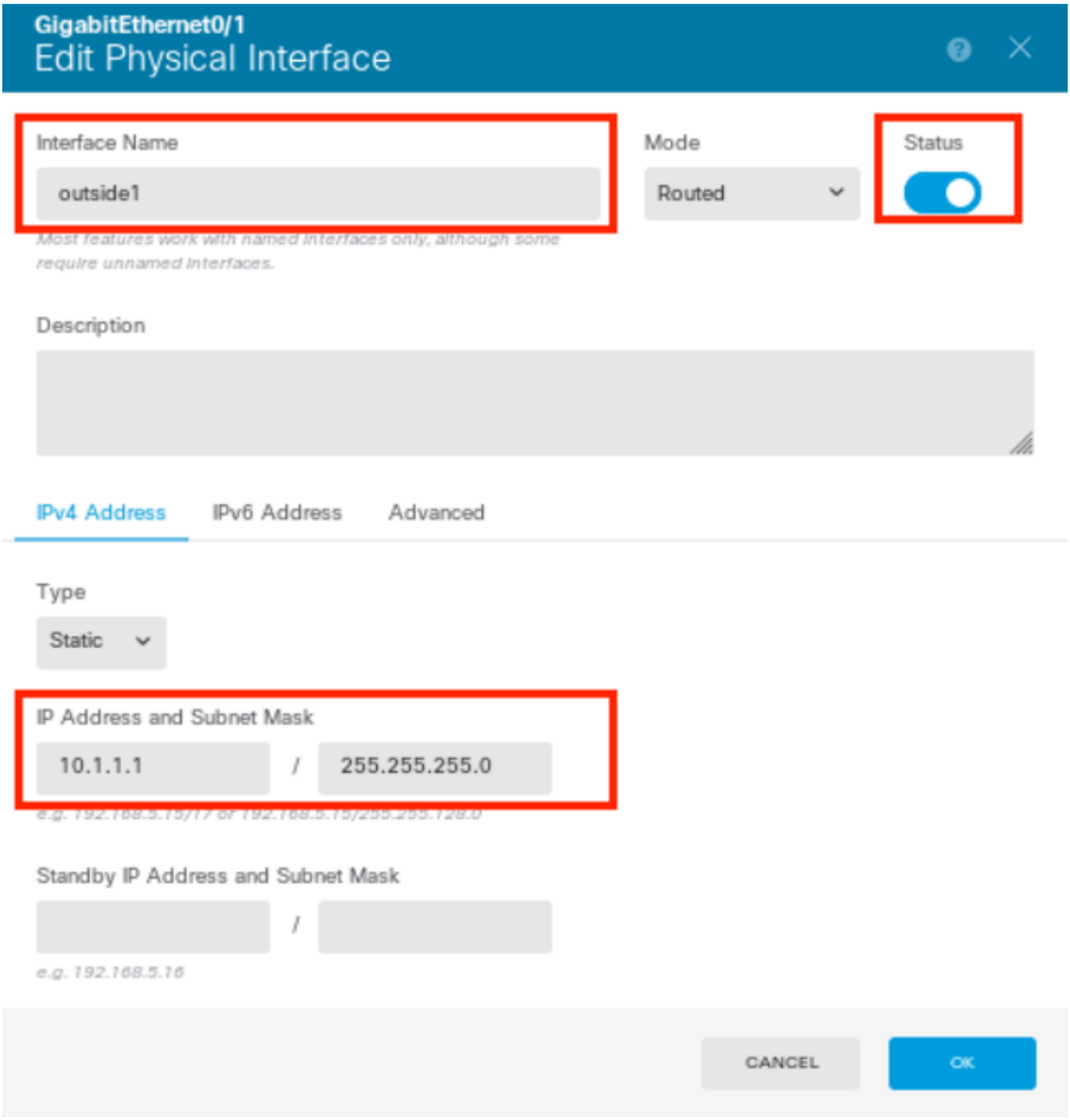
) voor de fysieke interface die u wilt bewerken. In dit voorbeeld Gigabit Ethernet0/1.



Stap 0 interface Gi0/1

In het venster Fysieke interface bewerken:

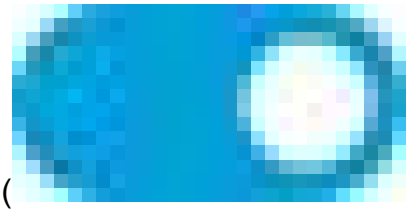
1. Stel de interfacenaam in, in dit geval buitenkant1 .
2. Stel de schuifschakelaar voor de status in op de ingeschakelde instelling ().
3. Klik op het tabblad IPv4-adres en configureer het IPv4-adres, in dit geval 10.1.1.1/24.
4. Klik op OK.

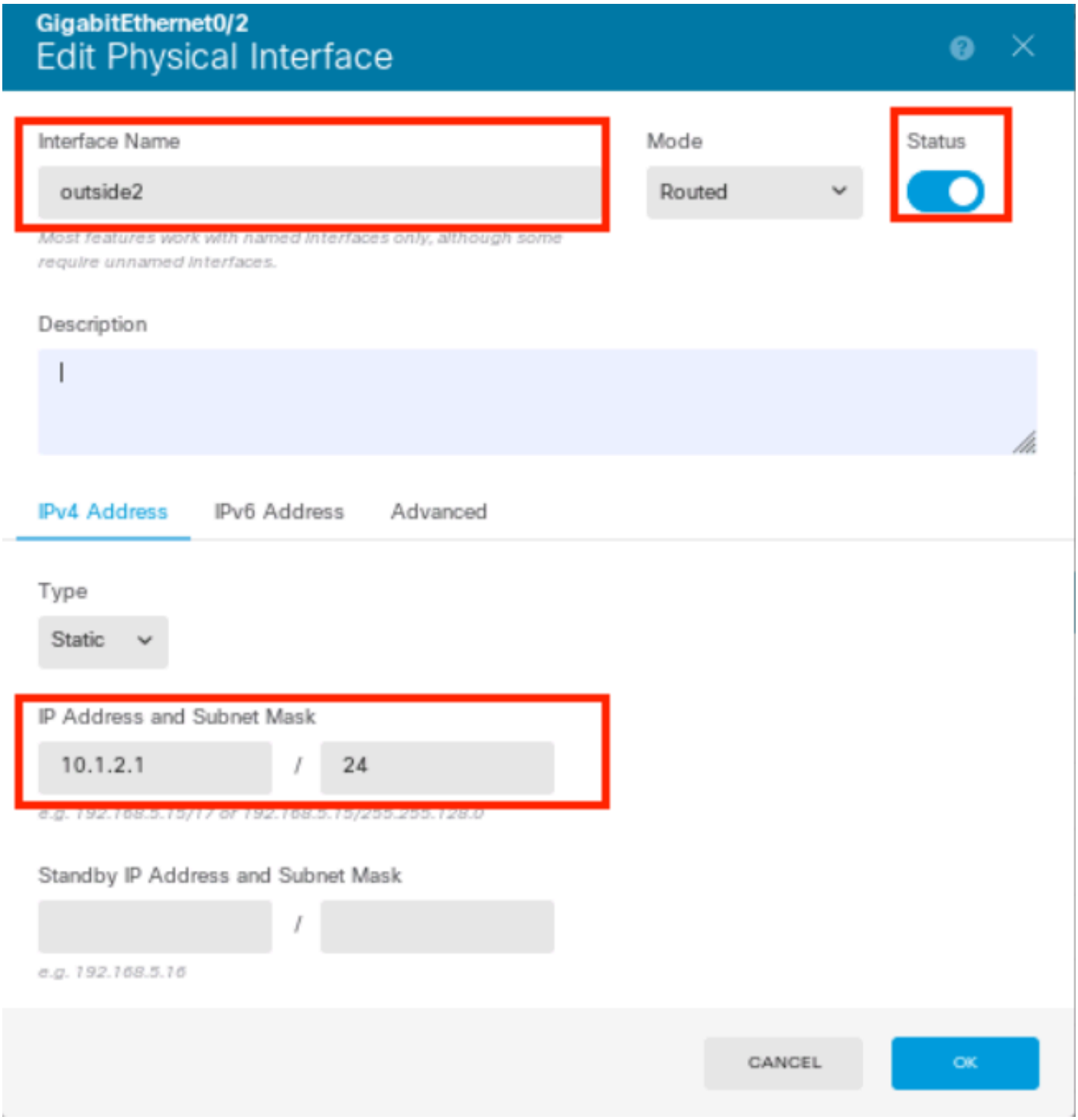


Stap 0 Bewerken interface Gi0/1

Opmerking: alleen routeringsinterfaces kunnen aan een ECMP-zone worden gekoppeld.

Herhaal de soortgelijke stappen om de interface voor de secundaire ISP-verbinding te configureren. In dit voorbeeld is de fysieke interface Gigabit Ethernet0/2 . In het venster Fysieke interface bewerken:

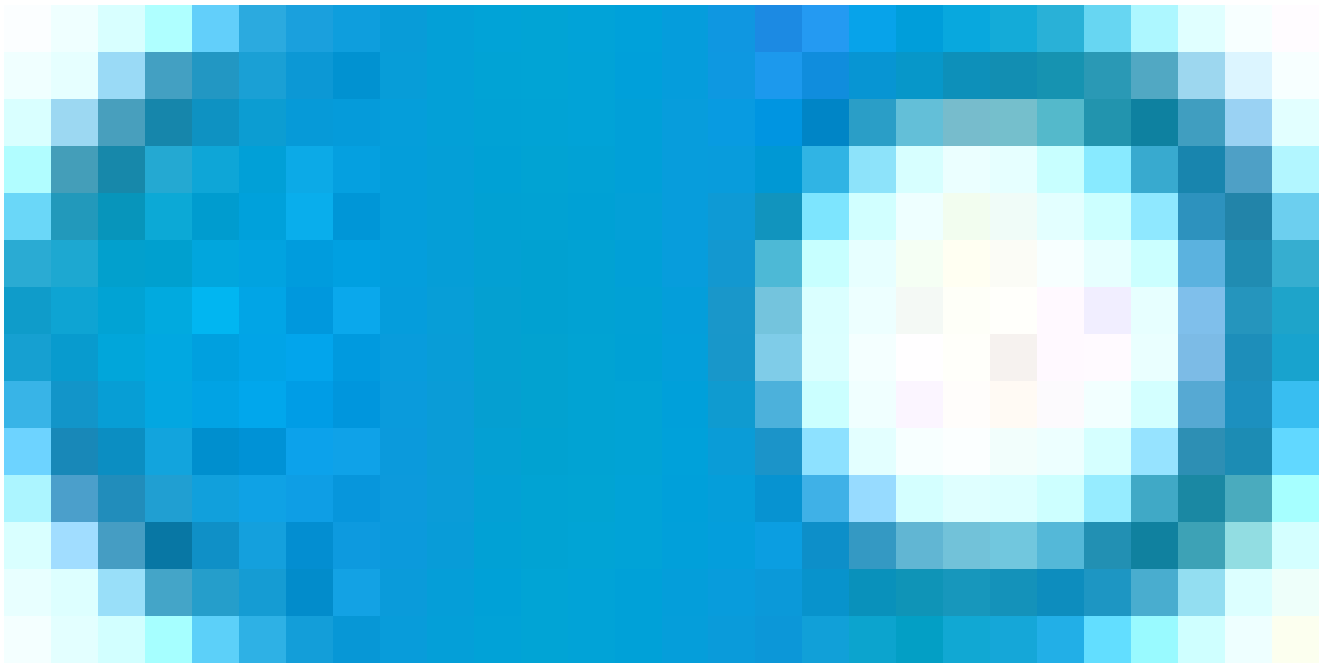
1. Stel de interfacenaam in, in dit geval buitenkant2.
2. Stel de statusschuifschakelaar in op de ingeschakelde instelling ().
3. Klik op het tabblad IPv4-adres en configureer het IPv4-adres, in dit geval 10.1.2.1/24.
4. Klik op OK.



Stap 0 Bewerken interface Gi0/2

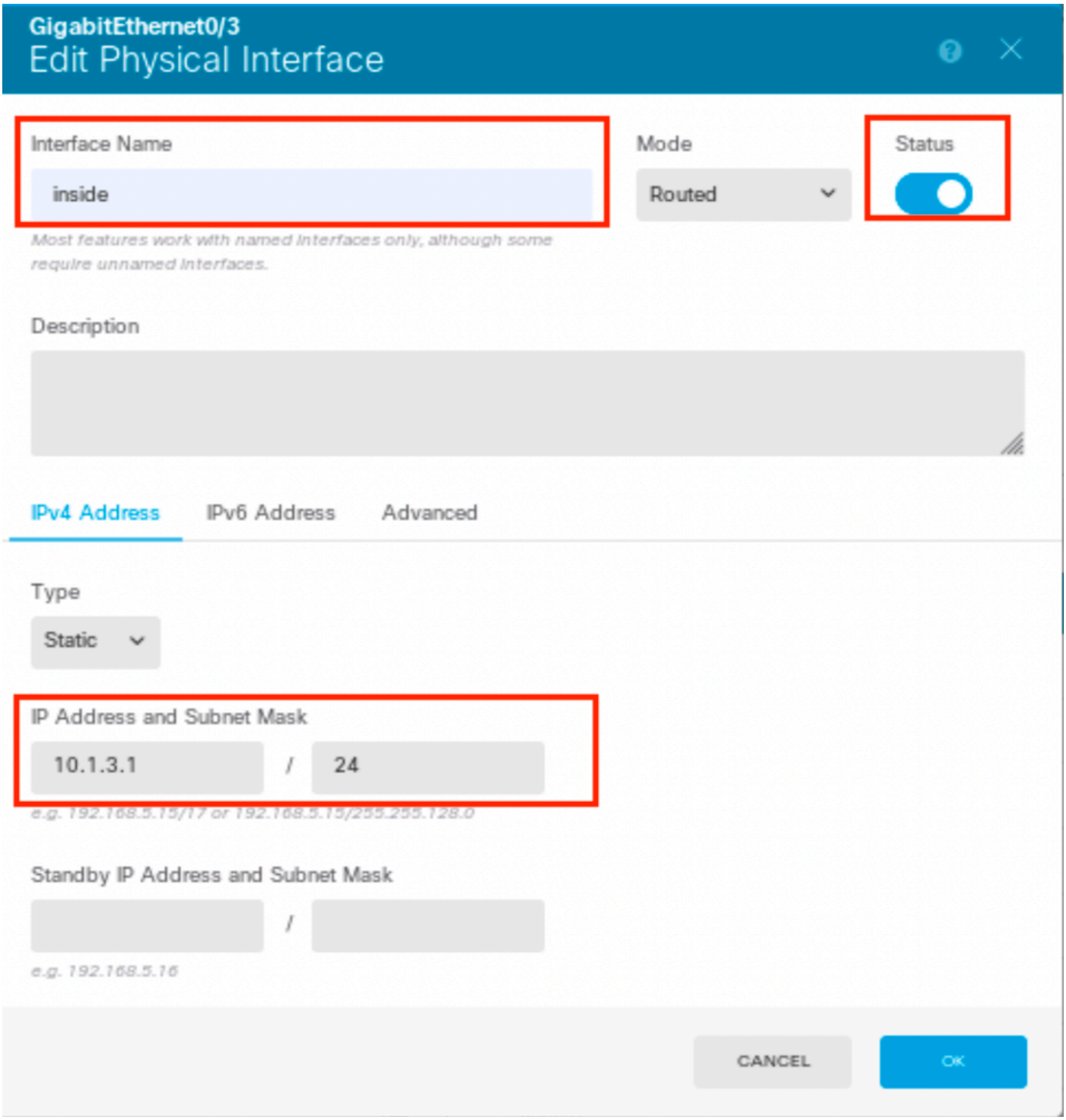
Herhaal de vergelijkbare stappen om de interface te configureren voor de interne verbinding, in dit voorbeeld is de fysieke interface Gigabit Ethernet0/3. In het venster Fysieke interface bewerken:

1. Stel de interfacenaam in, in dit geval binnenin .
2. Stel de statusschuifschakelaar in op de ingeschakelde instelling (



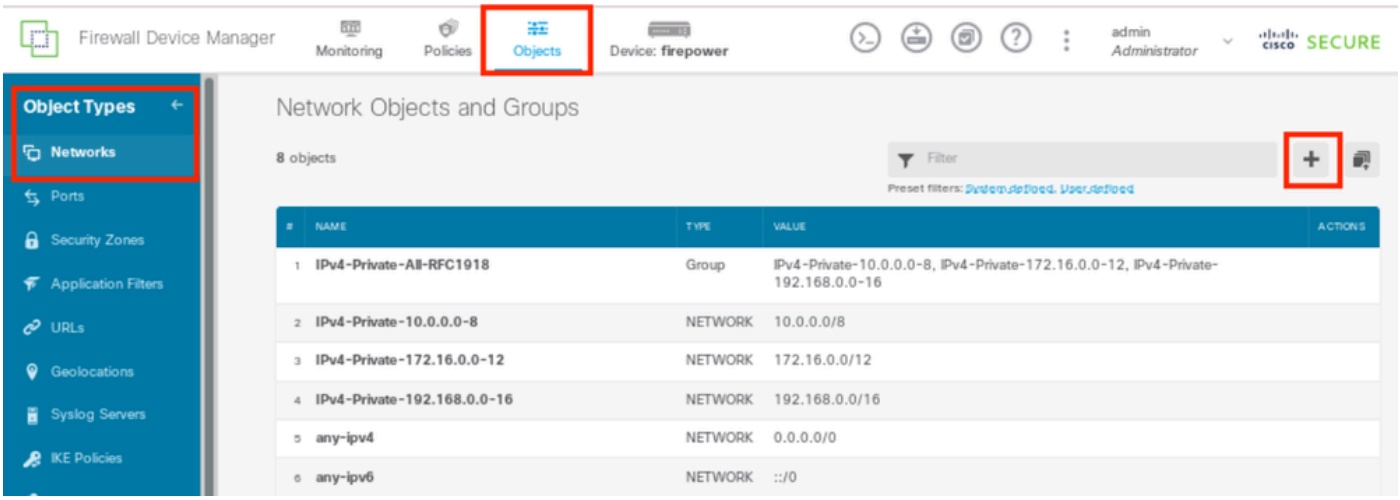
).

3. Klik op het tabblad IPv4-adres en configureer het IPv4-adres, in dit geval 10.1.3.1/24.
4. Klik op OK.



Stap 0 Bewerken interface Gi0/3

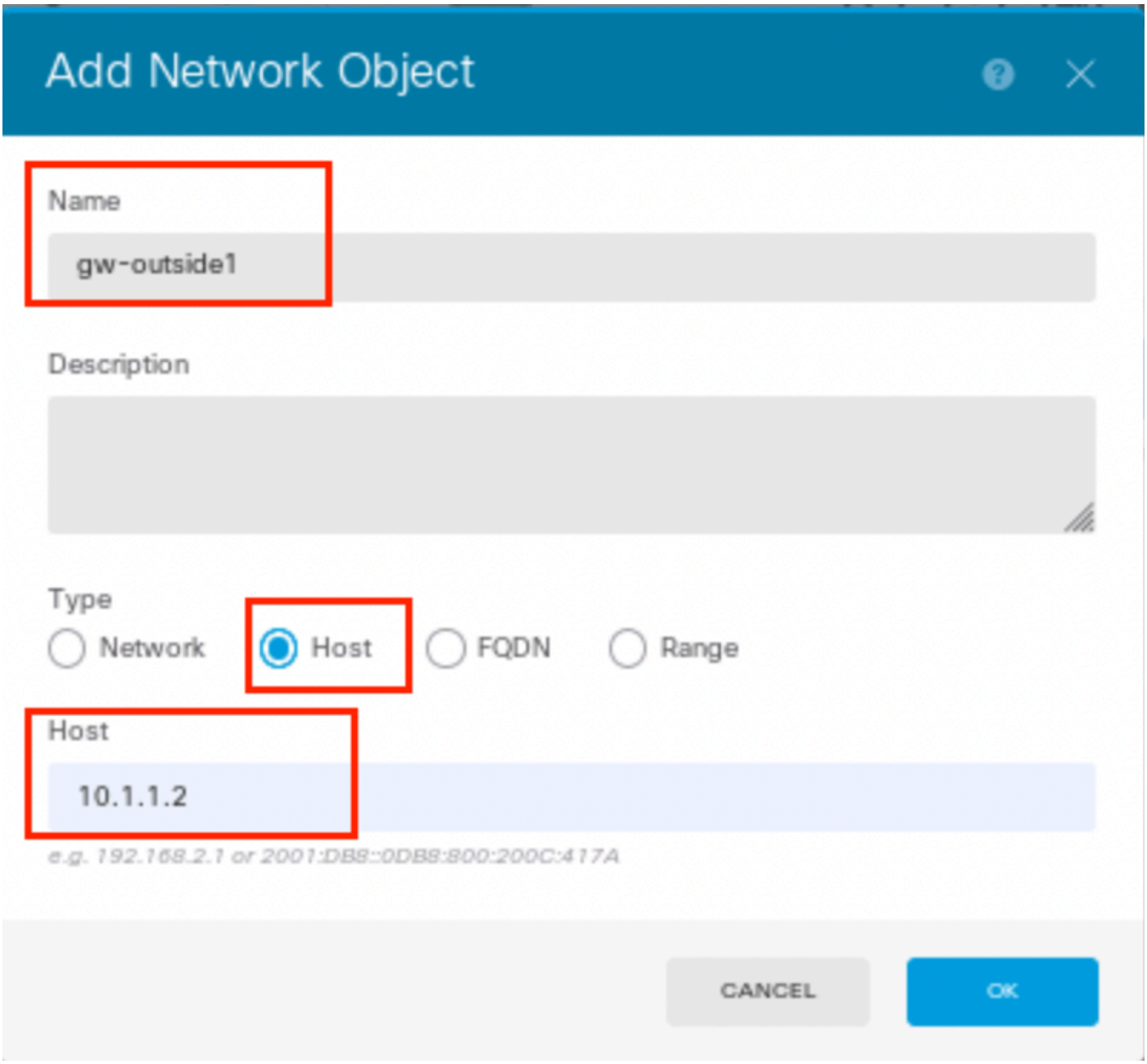
Navigeer naar Objecten > Objecttypen > Netwerken en klik op het pictogram Toevoegen ( ) om een nieuw object toe te voegen.



Stap 0 Object1

In het venster Add Network Object configureer de eerste ISP-gateway:

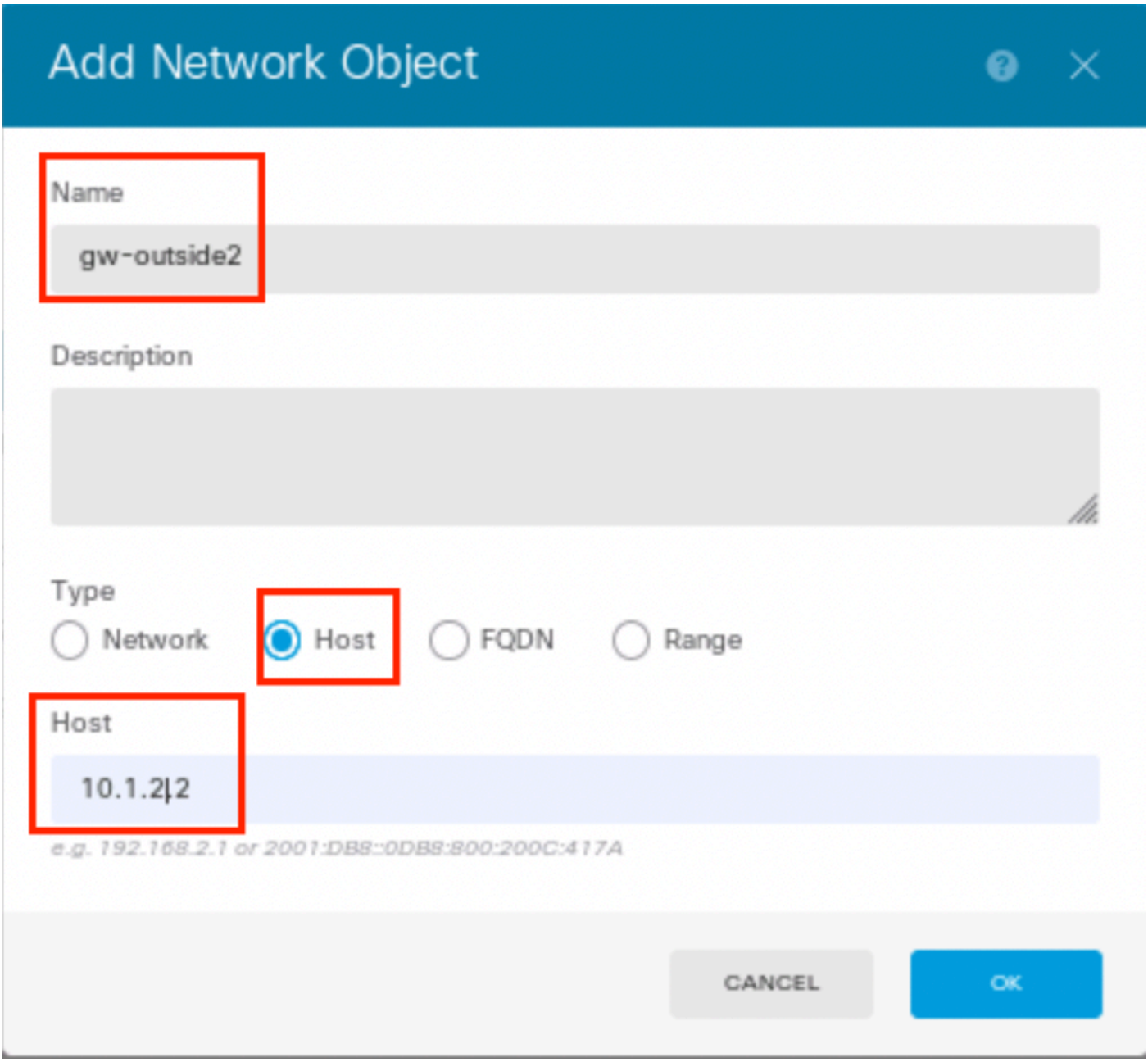
1. Stel de naam van het object in, in dit geval gw-outdoor1.
2. Selecteer het Type van het object, in dit geval Host.
3. Stel het IP-adres van de host in, in dit geval 10.1.1.2.
4. Klik op OK.



Stap 0 Object2

Herhaal de soortgelijke stappen om een ander netwerkobject voor de tweede ISP-gateway te configureren:

1. Stel de naam van het object in, in dit geval gw-outdoor2.
2. Selecteer het Type van het object, in dit geval Host.
3. Stel het IP-adres van de host in, in dit geval 10.1.2.2.
4. Klik op OK.



Stap 0 Object3

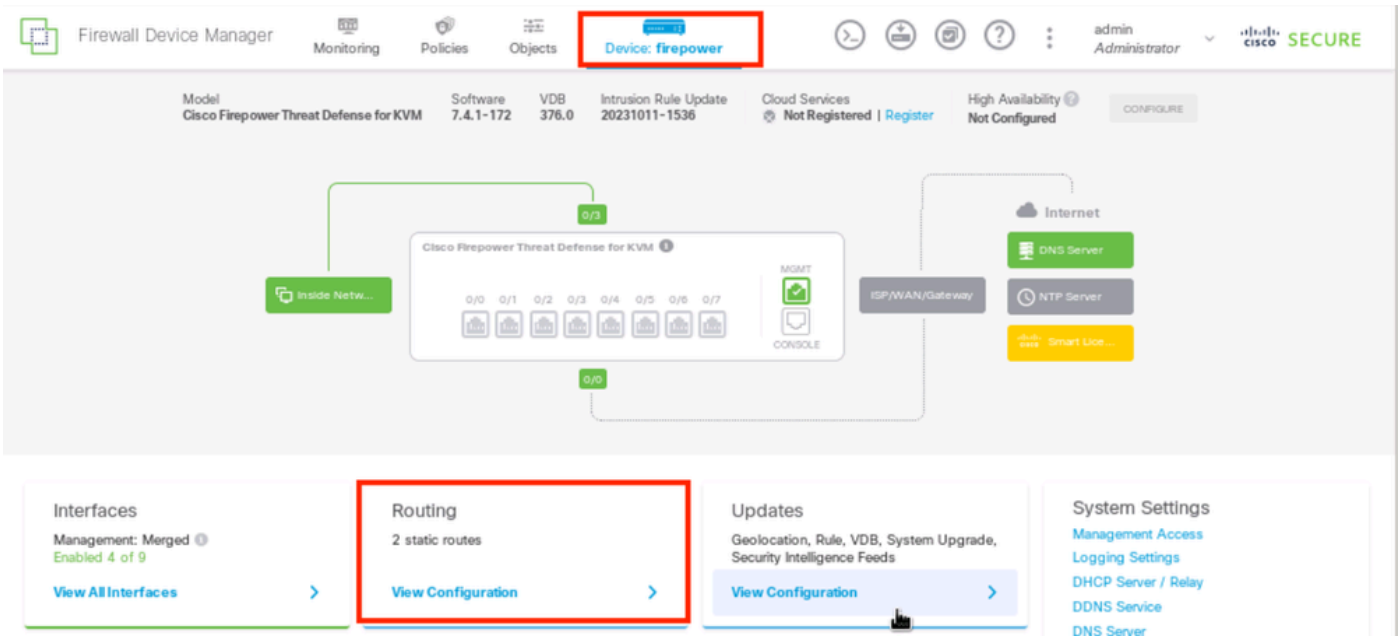
Opmerking: om het verkeer toe te laten, moet uw toegangscontrolebeleid op FTD zijn geconfigureerd. Dit onderdeel is niet in dit document opgenomen.

Stap 1. ECMP-zone configureren

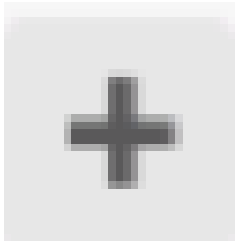
Navigeer naar apparaat en klik vervolgens op de koppeling in de samenvatting Routing.

Als u virtuele routers inschakelt, klikt u op het pictogram 

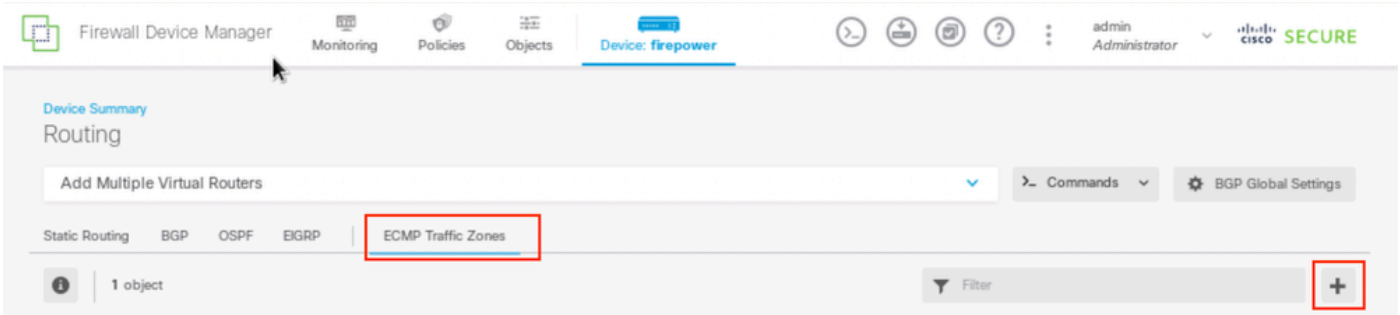
weergave voor de router waarin u een statische route configureert. In dit geval zijn virtuele routers niet ingeschakeld.



Stap 1 ECMP zone 1



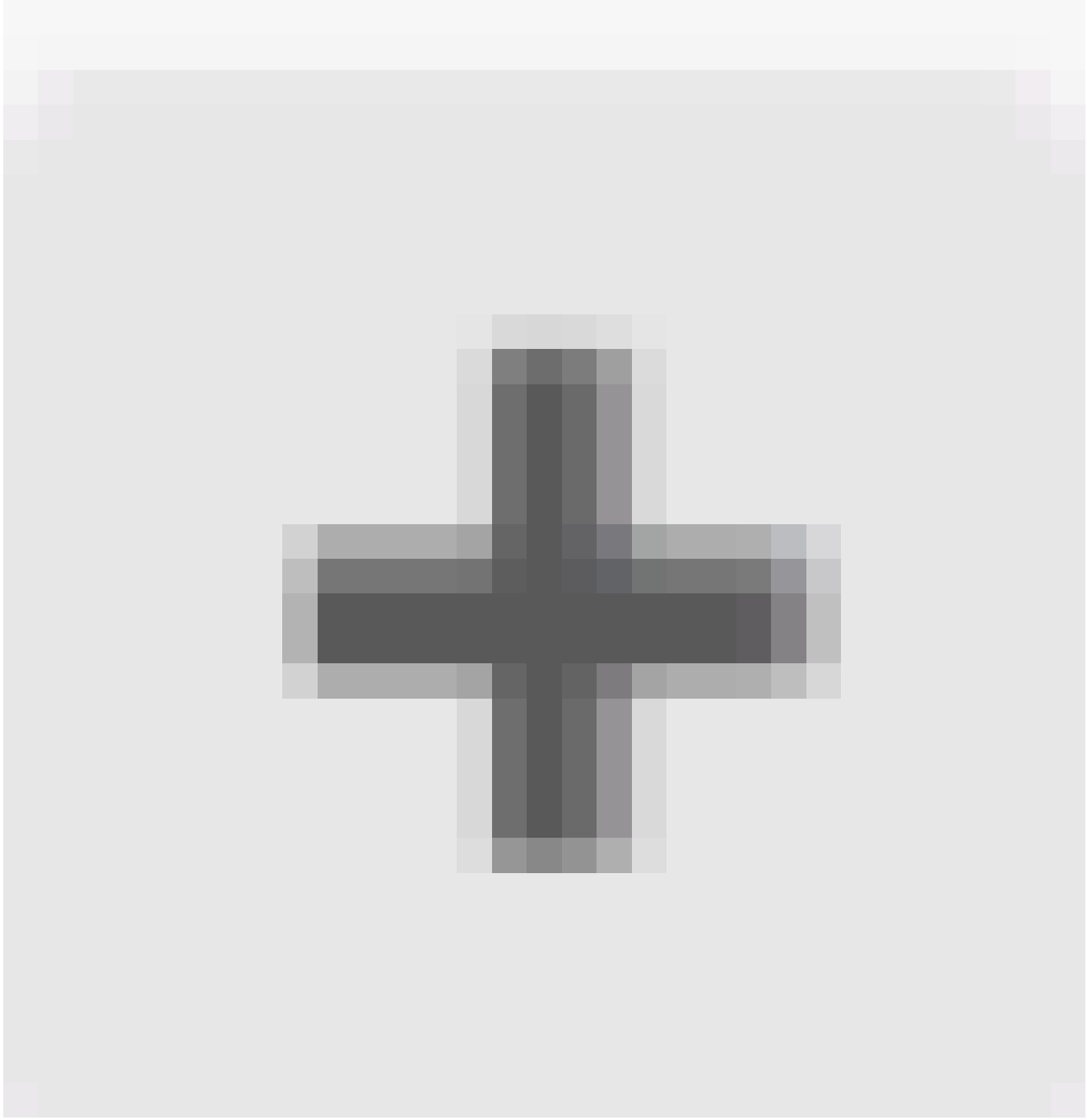
Klik op het tabblad ECMP Traffic Zones en klik vervolgens op het pictogram Add ( ) om een nieuwe zone toe te voegen.



Stap 1 ECMP zone 2

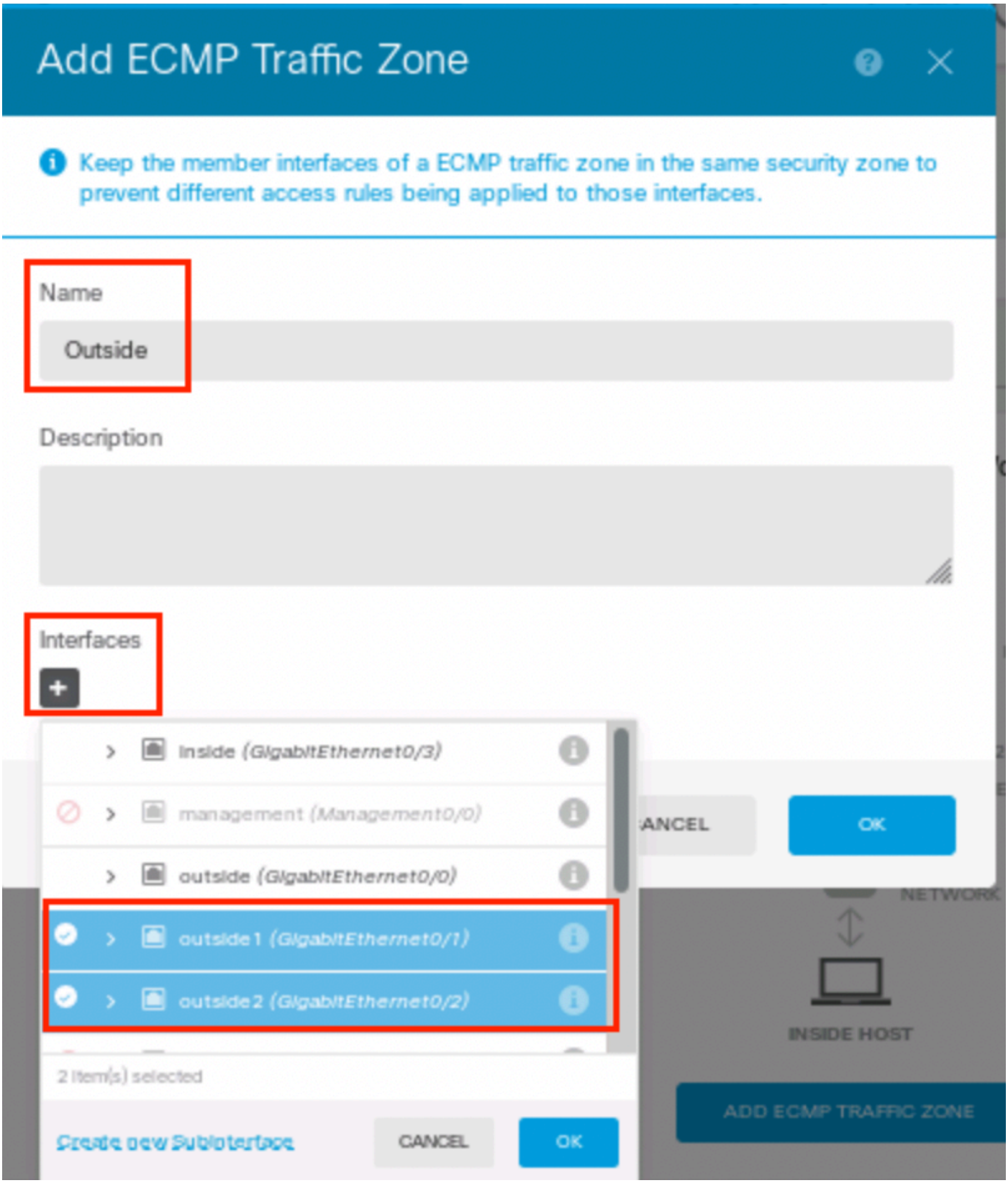
In het venster Add ECMP Traffic Zone:

1. Stel de naam van de ECMP-zone in en desgewenst een beschrijving.
2. Klik op het pictogram Add (



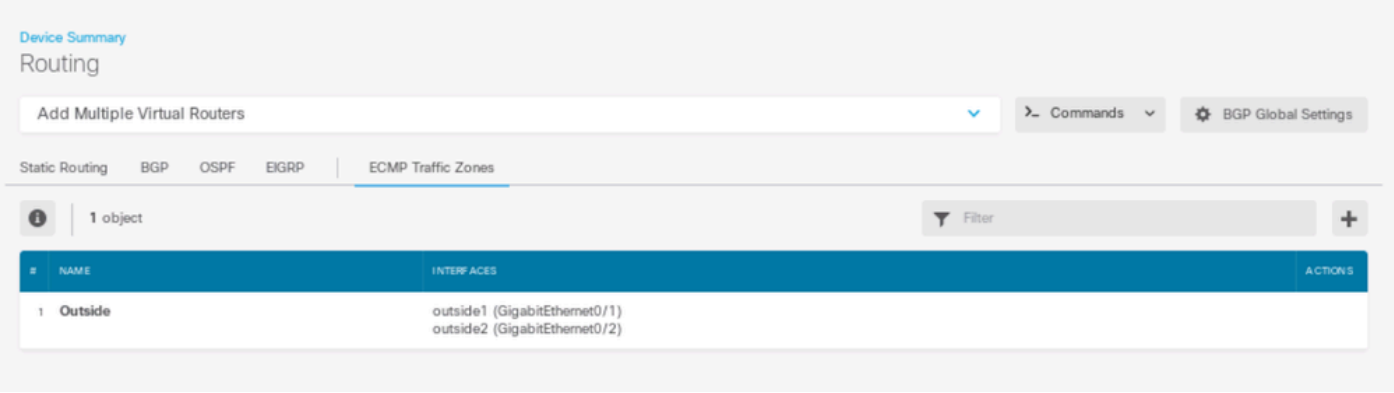
) om maximaal 8 interfaces te selecteren die u in de zone wilt opnemen. In dit voorbeeld, de naam van het ECMP is Buiten , interfaces buiten1 en buiten2 worden aan de zone toegevoegd.

3. Klik op OK.

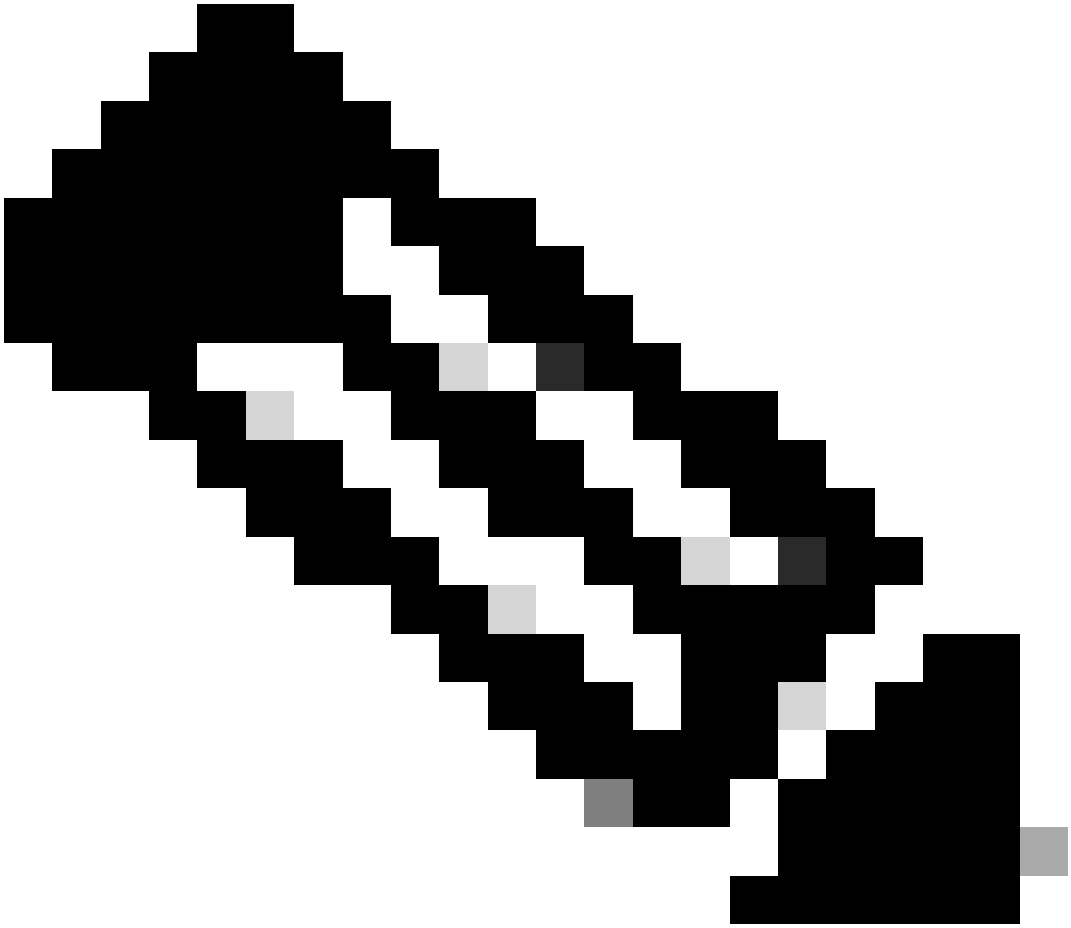


Stap 1 ECMP zone 3

Beide interfaces buiten1 en buiten2 zijn met succes toegevoegd aan de ECMP-zone buiten.



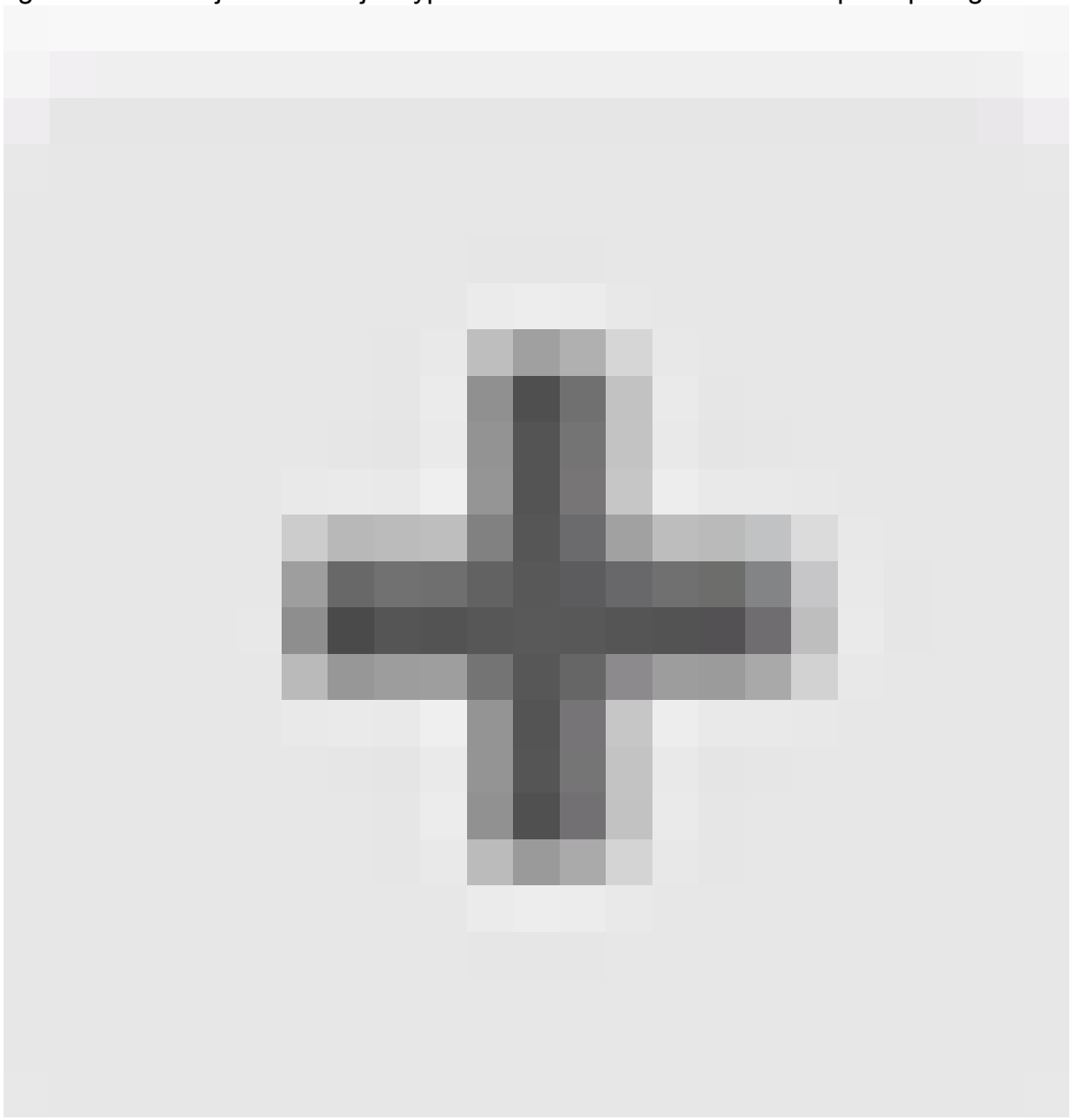
Stap 1 ECMP zone 4



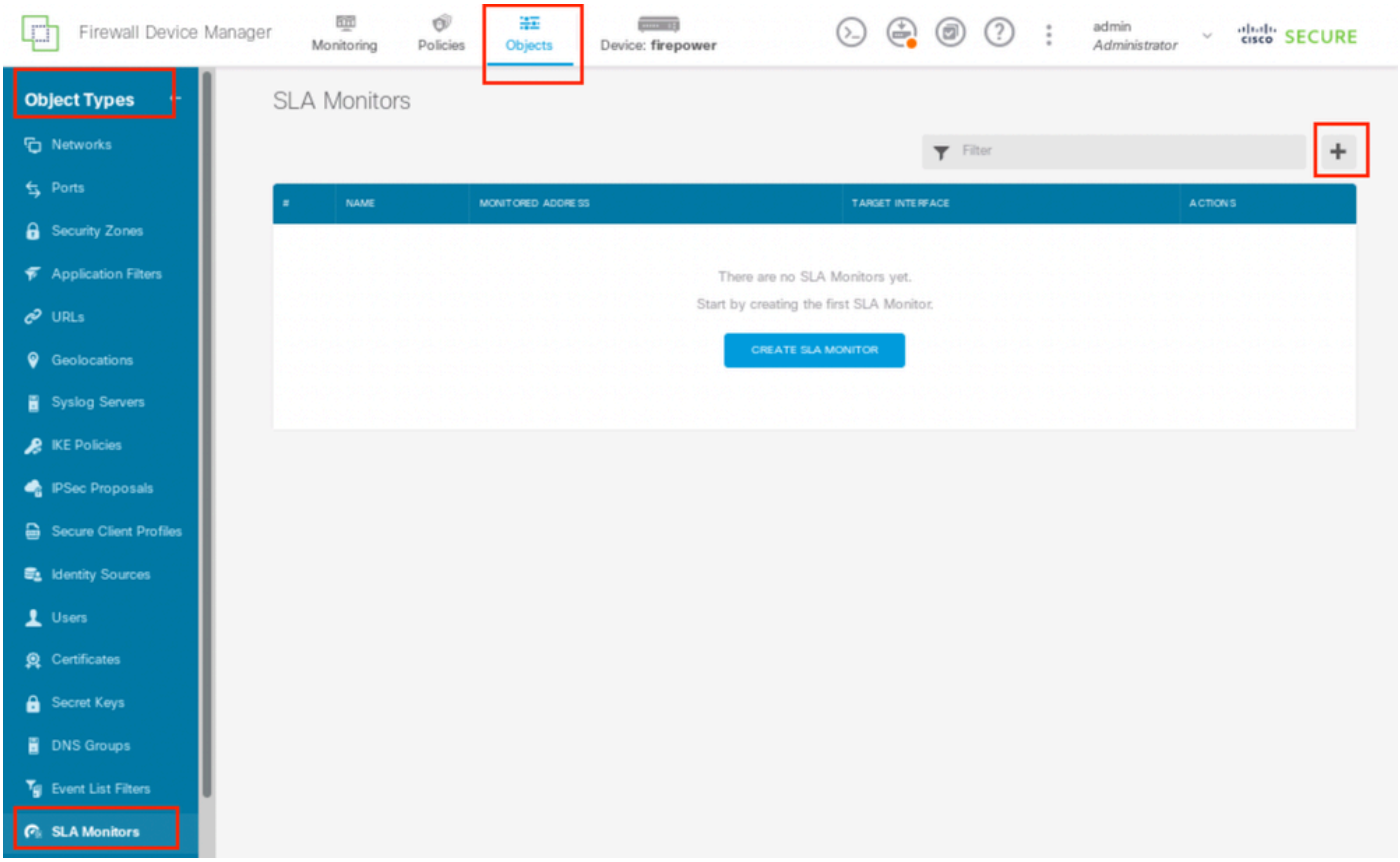
Opmerking: een ECMP-routeringszone is niet gerelateerd aan beveiligingszones. Het creëren van een veiligheidszone die de interfaces external1 en outdoor2 bevat, implementeert geen verkeerszone voor ECMP-routeringsdoeleinden.

Stap 2. IP SLA-objecten configureren

Als u de SLA-objecten wilt definiëren die worden gebruikt om de connectiviteit met elke gateway te bewaken, navigeert u naar Objecten > Objecttypen > SLA-monitoren en klikt u op het pictogram



Toevoegen (
) om een nieuwe SLA-monitor toe te voegen voor de eerste ISP-verbinding.



Stap 2 IP SLA1

In het venster Add SLA Monitor Object:

1. Stel de naam voor het SLA-monitorobject in en eventueel een beschrijving, in dit geval sla-external1.
2. Stel het monitoradres in, in dit geval gw-external1 (de eerste ISP-gateway).
3. Stel de doelinterface in waardoor het monitoradres bereikbaar is, in dit geval buitenkant1 .
4. Daarnaast is het ook mogelijk om de Time-out en de drempelwaarde aan te passen. Klik op OK.

Add SLA Monitor Object

Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000 milliseconds

0 - 2147483647

Timeout

5000 milliseconds

0 - 604800000

Frequency

60000 milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

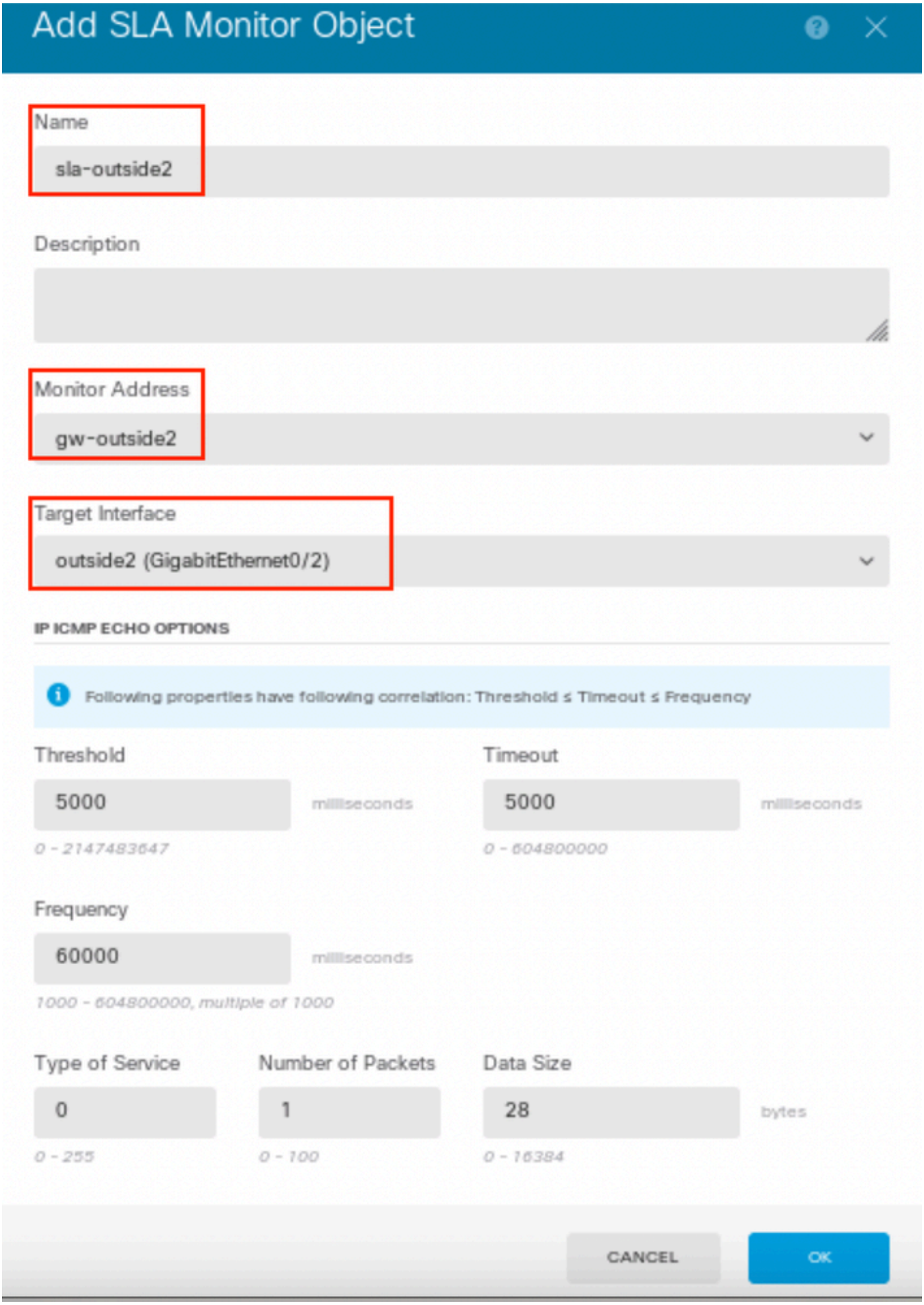
28 bytes

0 - 16384

CANCEL OK

Herhaal de soortgelijke stap om een ander SLA Monitor Object te configureren voor de tweede ISP-verbinding, in het venster Add SLA Monitor Object:

1. Stel de naam voor het SLA-monitorobject in en eventueel een beschrijving, in dit geval sla-outdoor2 .
2. Stel het monitoradres in, in dit geval gw-buitenkant2 (de tweede ISP-gateway).
3. Stel de doelinterface in waardoor het monitoradres bereikbaar is, in dit geval buiten2.
4. Bovendien is het ook mogelijk om de Time-out en de drempelwaarde aan te passen. Klik op OK.

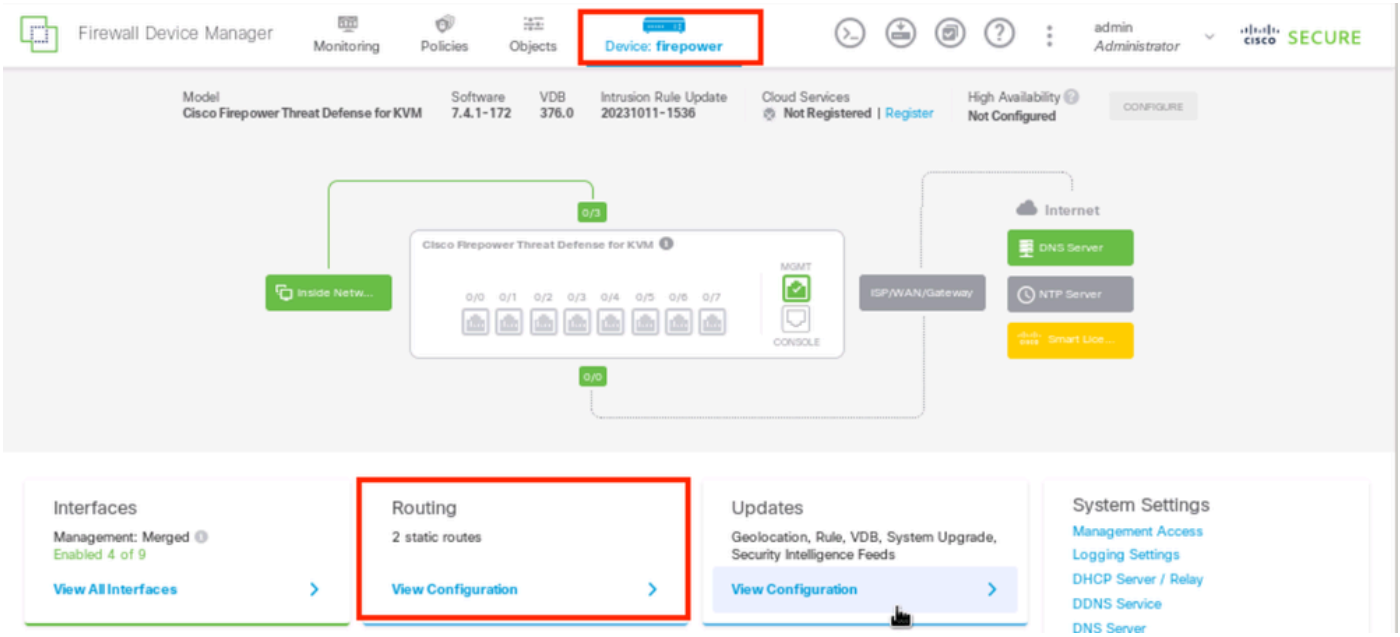

Add SLA Monitor Object
Name
sla-outside2
Description
Monitor Address
gw-outside2
Target Interface
outside2 (GigabitEthernet0/2)
IP ICMP ECHO OPTIONS
Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency
Threshold
5000
milliseconds
0 - 2147483647
Timeout
5000
milliseconds
0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

Stap 2 IP SLA3

Stap 3. Configureer statische routes met routespoor

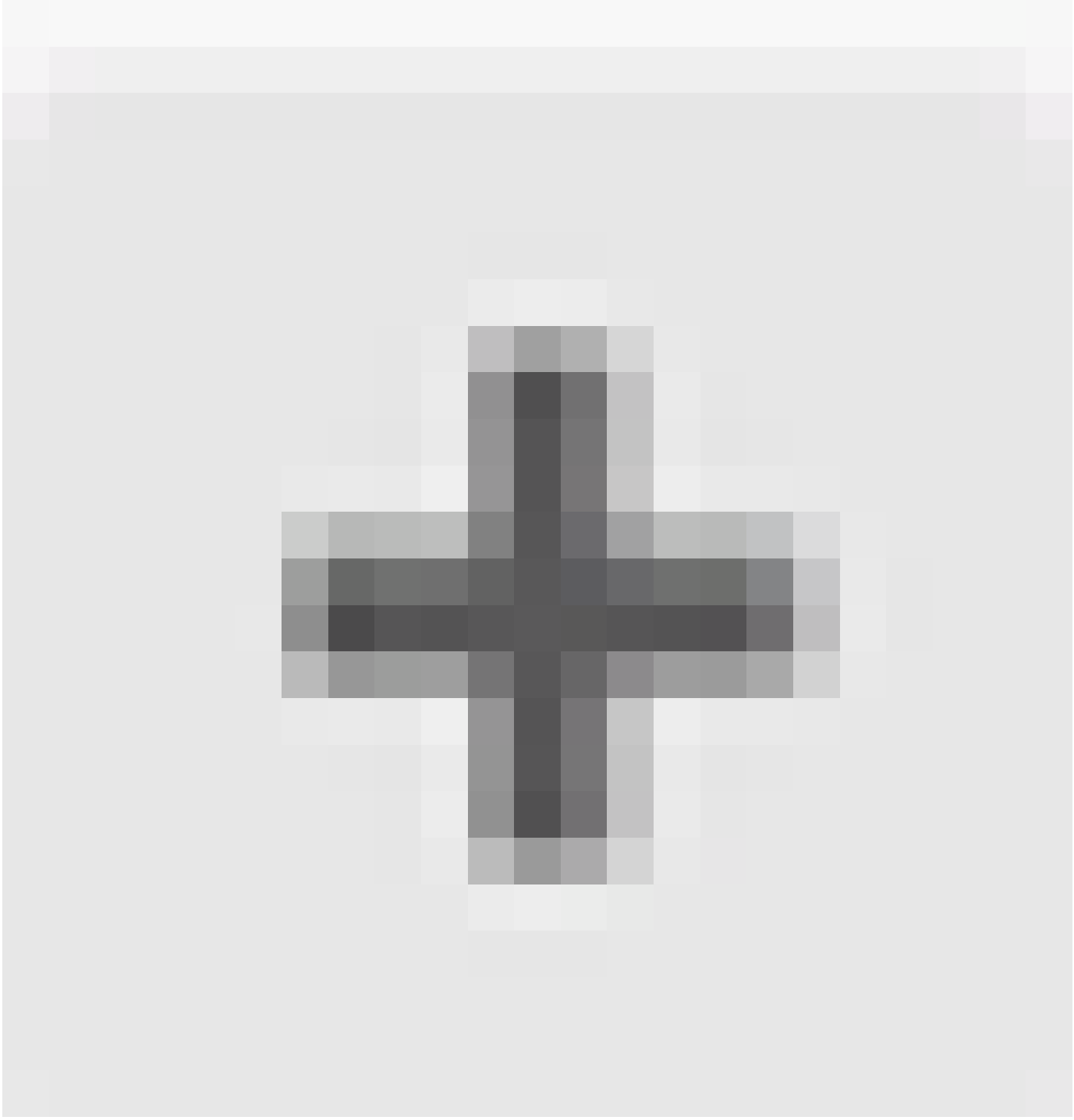
Navigeer naar apparaat en klik vervolgens op de koppeling in de samenvatting Routing.

Als u virtuele routers inschakelt, klikt u op het pictogram weergave voor de router waarin u een statische route configureert. In dit geval zijn virtuele routers niet ingeschakeld.



Stap 3 Route1

Op de Statische Routing pagina klikt u op het pictogram Add (

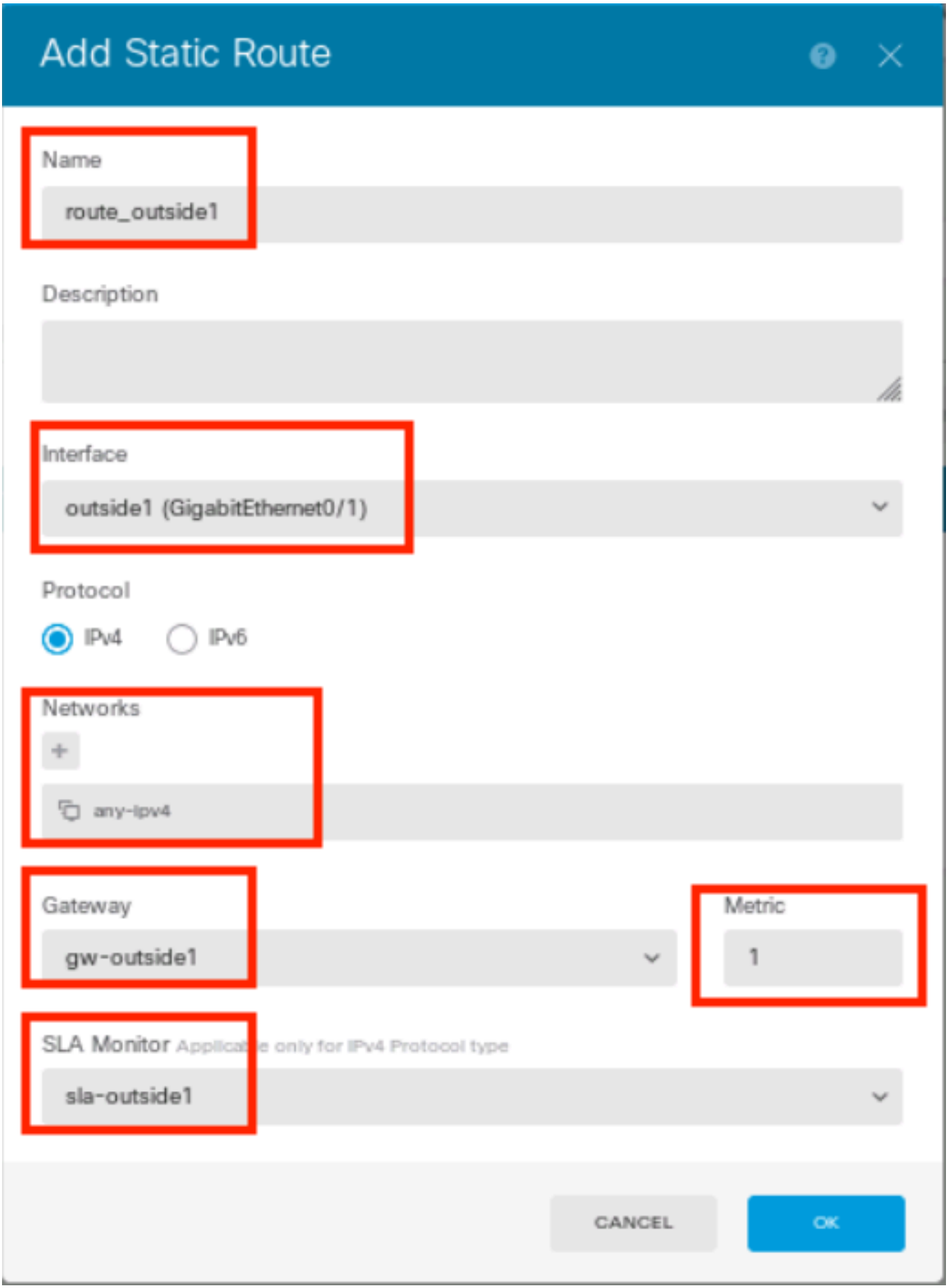


) om een nieuwe statische route toe te voegen voor de eerste ISP-link.

In het venster Statische route toevoegen :

1. Stel de naam van de route en eventueel de beschrijving in. In dit geval route_external1.
2. Van de vervolgkeuzelijst Interface, selecteer de interface waardoor u verkeer wilt verzenden, moet het gatewayadres door de interface toegankelijk zijn. In dit geval buiten1 (Gigabit Ethernet0/1).
3. Selecteer de Netwerken die de doelnetwerken of -hosts identificeren die de gateway in deze route gebruiken. In dit geval de vooraf gedefinieerde willekeurige-ipv4.
4. Selecteer in de vervolgkeuzelijst Gateway het netwerkobject dat het IP-adres van de gateway identificeert. Traffic wordt naar dit adres verzonden. In dit geval gw-external1 (de

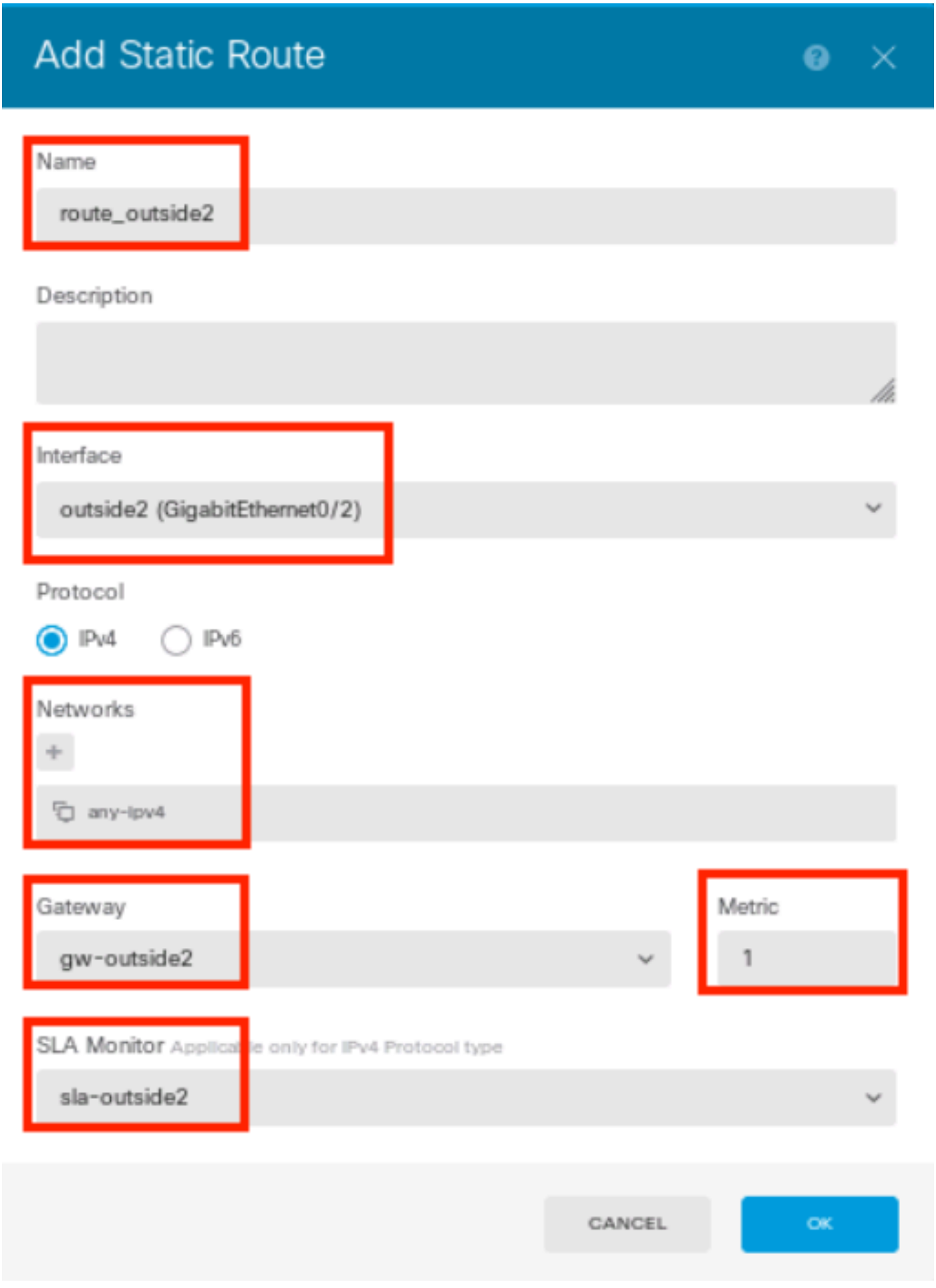
eerste ISP-gateway).
5. Stel de Metriek van de route in, tussen 1 en 254. In dit voorbeeld 1.
6. Selecteer in de vervolgkeuzelijst SLA Monitor het SLA-monitorobject. In dit geval sla-outdoor1.
7. Klik op OK.



Stap 3 Route2

Herhaal de soortgelijke stap om een andere statische route voor de tweede ISP-verbinding te configureren, in het venster Statische route toevoegen:

1. Stel de naam van de route en eventueel de beschrijving in. In dit geval route_external2.
2. Van de vervolgkeuzelijst Interface, selecteer de interface waardoor u verkeer wilt verzenden, moet het gatewayadres door de interface toegankelijk zijn. In dit geval buiten2 (Gigabit Ethernet0/2).
3. Selecteer de Netwerken die de doelnetwerken of -hosts identificeren die de gateway in deze route gebruiken. In dit geval de vooraf gedefinieerde willekeurige-ipv4.
4. Selecteer in de vervolgkeuzelijst Gateway het netwerkobject dat het IP-adres van de gateway identificeert. Traffic wordt naar dit adres verzonden. In dit geval gw-external2 (de tweede ISP-gateway).
5. Stel de Metriek van de route in, tussen 1 en 254. In dit voorbeeld 1.
6. Selecteer in de vervolgkeuzelijst SLA Monitor het SLA-monitorobject. In dit scenario, sla-outdoor2.
7. Klik op OK.



Stap 3 Route3

Je hebt 2 routes via de buiten1 en buiten2 interfaces met routesporen.

Stap 3 router 4

Breng de wijziging in FTD aan.

Verifiëren

Log in op de CLI van de FTD en voer de opdracht uit show zone om informatie over ECMP-verkeerszones te controleren, inclusief de interfaces die deel uitmaken van elke zone.

<#root>

> show zone
Zone:

Outside

ecmp
Security-level: 0

Zone member(s): 2

outside2 GigabitEthernet0/2

outside1 GigabitEthernet0/1

Stel het bevel in werking show running-config route om de lopende configuratie de routerconfiguratie te controleren, in dit geval zijn er twee statische routes met routesporen.

<#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

show route Stel het bevel in werking om de routeringstabel te controleren, in dit geval zijn er twee standaardroutes via de interface buitenkant1 en buitenkant2 met gelijke kosten, kan het verkeer tussen twee ISP kringen worden verdeeld.

<#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

Voer de opdracht uit show sla monitor configuration om de configuratie van de SLA-monitor te controleren.

<#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:
```

Voer de opdracht show sla monitor operational-state uit om de status van de SLA-monitor te bevestigen. In dit geval kunt u vinden "Time-out voorkwam: FALSE" in de opdrachtoutput, het geeft aan dat de ICMP-echo naar de gateway reageert, zodat de standaardroute door doelinterface actief is en geïnstalleerd in routeringstabel.

<#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

Taakverdeling

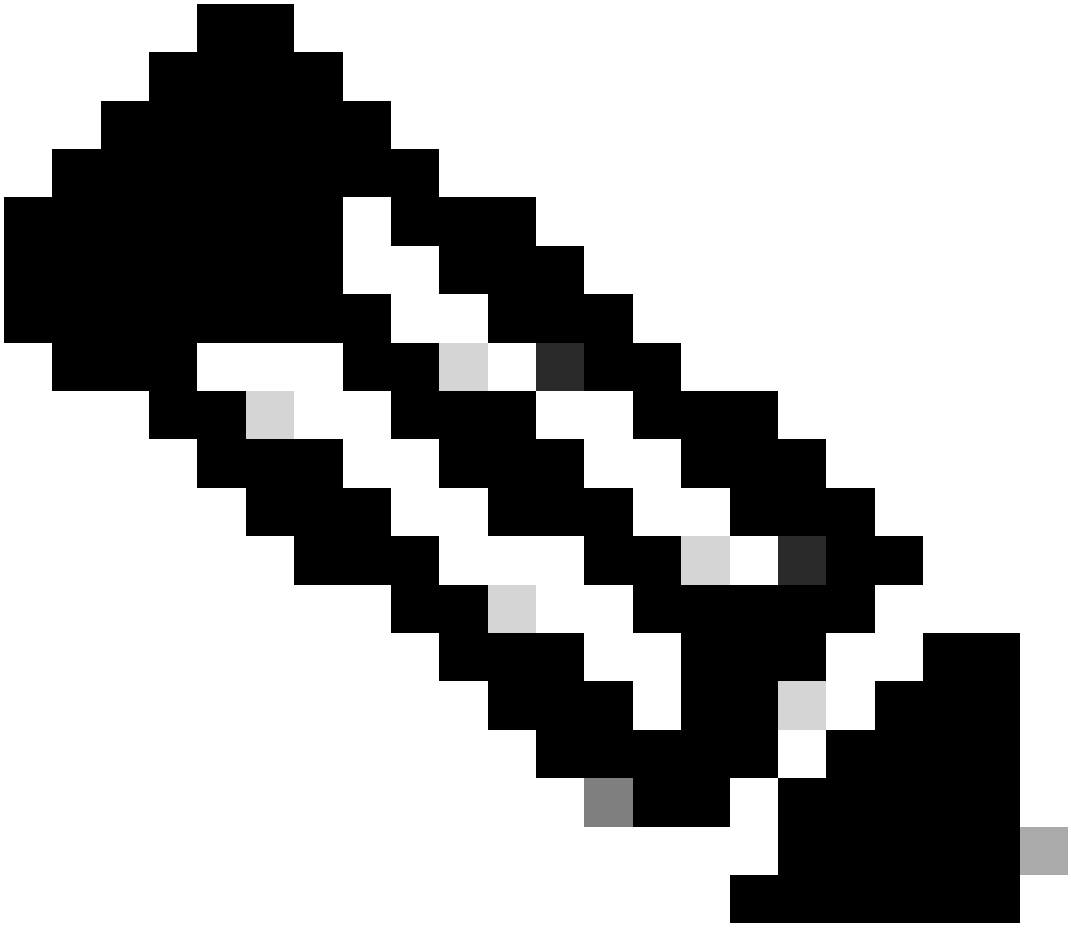
Aanvankelijk verkeer via FTD om te controleren of de ECMP-werklastverdeling gelijk is aan het verkeer tussen de gateways in de ECMP-zone. In dit geval, initieer SSH verbinding van Test-PC-1 (10.1.3.2) en Test-PC-2 (10.1.3.4) naar Internet-Host (10.1.5.2), voer de opdracht show conn uit om te bevestigen dat het verkeer belastingsgebalanceerd is tussen twee ISP-verbindingen, Test-PC-1 (10.1.3.2) gaat door interface buiten1, Test-PC-2 (10.1.3.4) gaat door interface buiten2.

<#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



Opmerking: het verkeer is taakverdeling tussen de gespecificeerde gateways op basis van een algoritme dat de bron- en bestemmingsIP-adressen, inkomende interface, protocol, bron- en bestemmingshavens blokkeert. Wanneer u de test uitvoert, kan het verkeer dat u simuleert naar dezelfde gateway worden gerouteerd vanwege het hashalgoritme, dit wordt verwacht, verandert elke waarde onder de 6 tuples (bron IP, bestemming IP, inkomende interface, protocol, bronpoort, bestemmingshaven) om het hashresultaat te wijzigen.

Verloren route

Als de verbinding met de eerste ISP Gateway is uitgeschakeld, moet u in dit geval de eerste te simuleren gatewayrouter uitschakelen. Als FTD geen echoantwoord van eerste ISP gateway binnen de drempeltijdopnemer ontvangt die in het voorwerp van de SLA Monitor wordt gespecificeerd, wordt de gastheer beschouwd als onbereikbaar en zoals neer gemarkeerd. De gevolgde route aan eerste gateway wordt ook verwijderd uit het verpletteren van lijst.

Start de opdracht show sla monitor operational-state om de huidige status van de SLA-monitor te bevestigen. In dit geval kunt u "Time-out voorgekomen vinden: Waar" in de opdrachtoutput, het geeft aan dat de ICMP-echo naar de eerste ISP-gateway niet reageert.

<#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

Voer de opdracht uit **show route** om de huidige routeringstabel te controleren, de route naar de eerste ISP-gateway via interface buitenkant1 wordt verwijderd, er is slechts één actieve standaardroute naar de tweede ISP-gateway via interface buitenkant2.

<#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

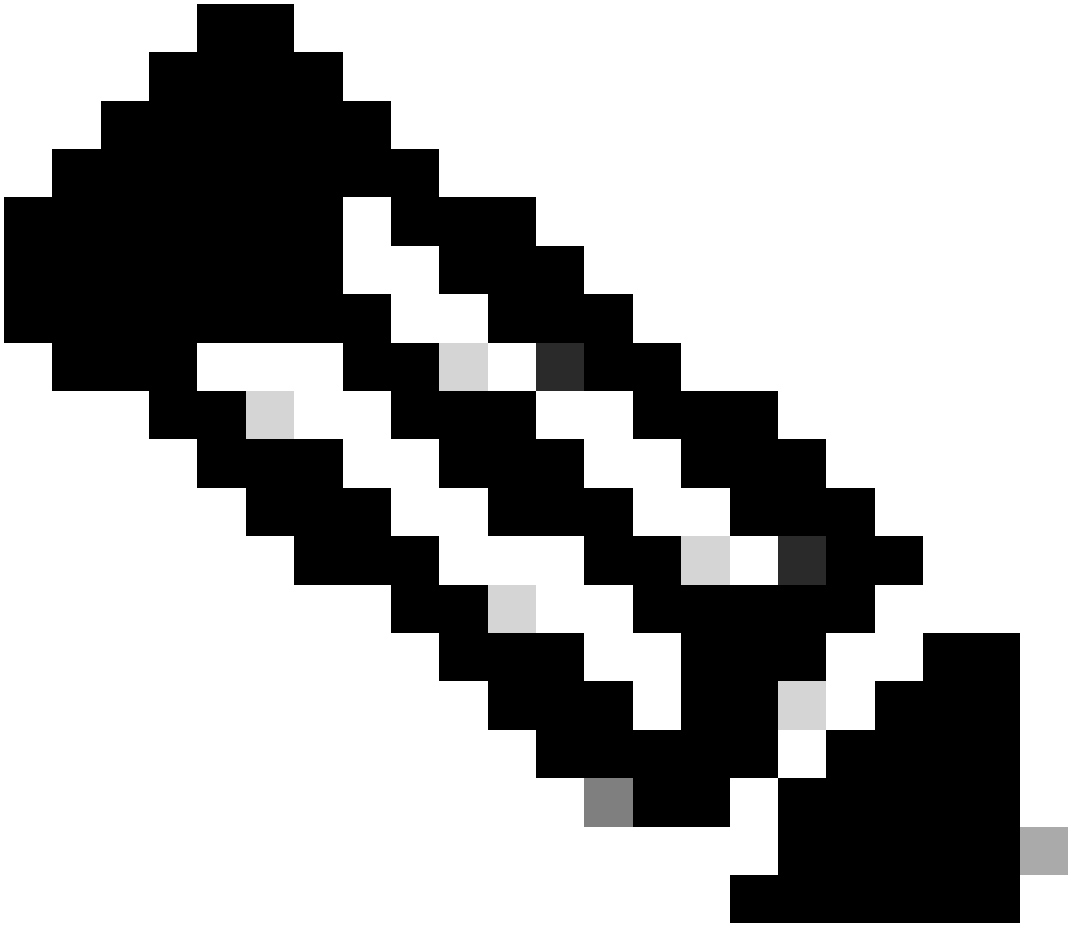
Voer de opdracht uit show conn , je kunt zien dat de twee verbindingen nog steeds actief zijn. SSH-sessies zijn ook zonder enige onderbreking actief op Test-PC-1 (10.1.3.2) en Test-PC-2 (10.1.3.4).

<#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



Opmerking: in de output van show conn , SSH-sessie van Test-PC-1 (10.1.3.2) is nog steeds via interface buitenkant1, hoewel de standaardroute door interface buitenkant1 is verwijderd uit de routeringstabel. Dit wordt verwacht en door ontwerp, het werkelijke verkeer stroomt door interface buitenkant2. Als u een nieuwe verbinding van Test-PC-1 (10.1.3.2) naar Internet-Host (10.1.5.2) start, kunt u al het verkeer vinden via de interface buiten2.

Problemen oplossen

Om de routingstabel te bevestigen verander, stel bevel in werking debug ip routing.

In dit voorbeeld, wanneer de verbinding met eerste ISP gateway neer is, wordt de route door interface outdoor1 verwijderd uit het verpletteren van lijst.

<#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

Voer de opdracht show route uit om de huidige routertabel te bevestigen.

<#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

Wanneer de verbinding met de eerste ISP gateway omhoog opnieuw is, wordt de route door interface external1 toegevoegd terug naar routingstabel.

<#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

Voer de opdracht show route uit om de huidige routertabel te bevestigen.

> 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

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.