Dual ISP op FTD configureren met FDM

Inhoud

Inleiding

In dit document wordt beschreven hoe u de failover van de Dual Internet Service Provider (ISP) kunt configureren met Firewall Device Manager (FDM) voor de Secure Firewall-reeks.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- basisroutering
- Firewall Device Manager-dashboardkennis
- Minstens twee internetserviceproviders zijn verbonden met de beveiligde firewall.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

· Cisco Secure Firewall met versie 7.7.X of hogere versies.

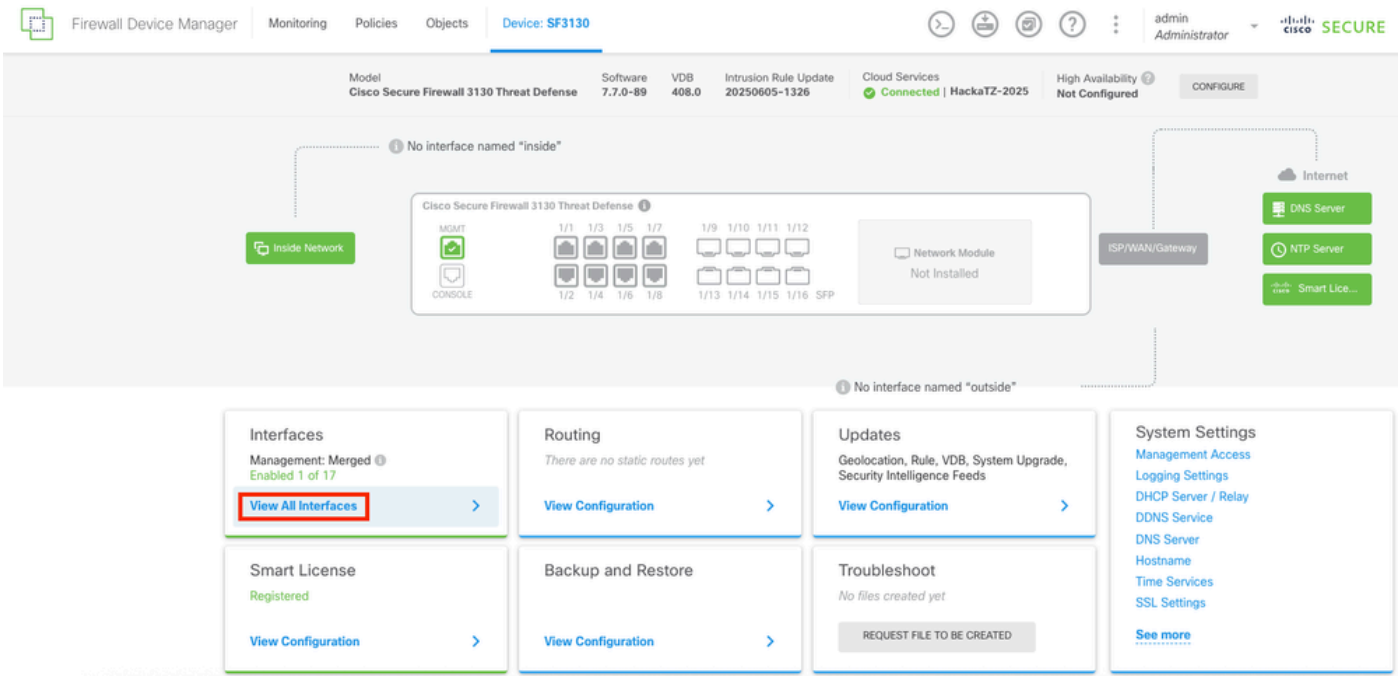
· Beveiligde firewall 3130 met versie 7.7.0.

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.

Configureren

Stap 1.

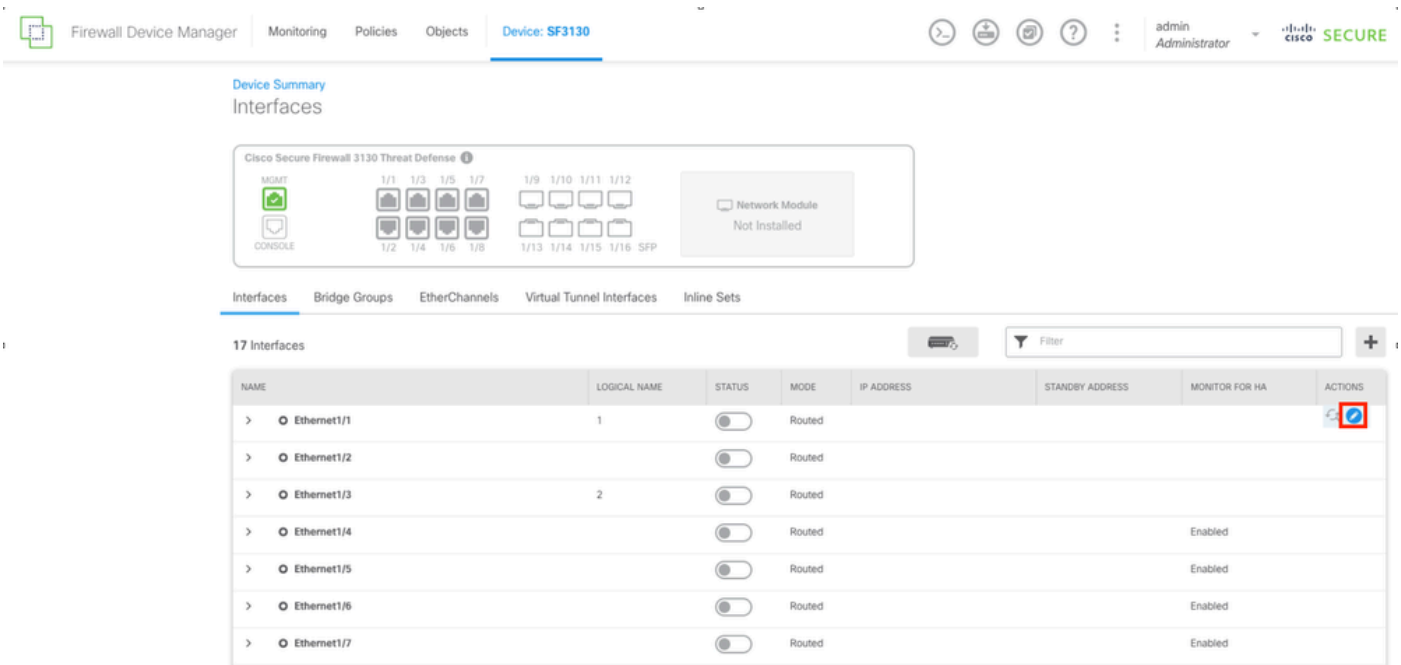
Meld u aan bij de FDM op de beveiligde firewall en navigeer naar de sectie interfaces door de knop Alle interfaces weergeven te selecteren.



Hoofddashboard van FDM

Stap 2.

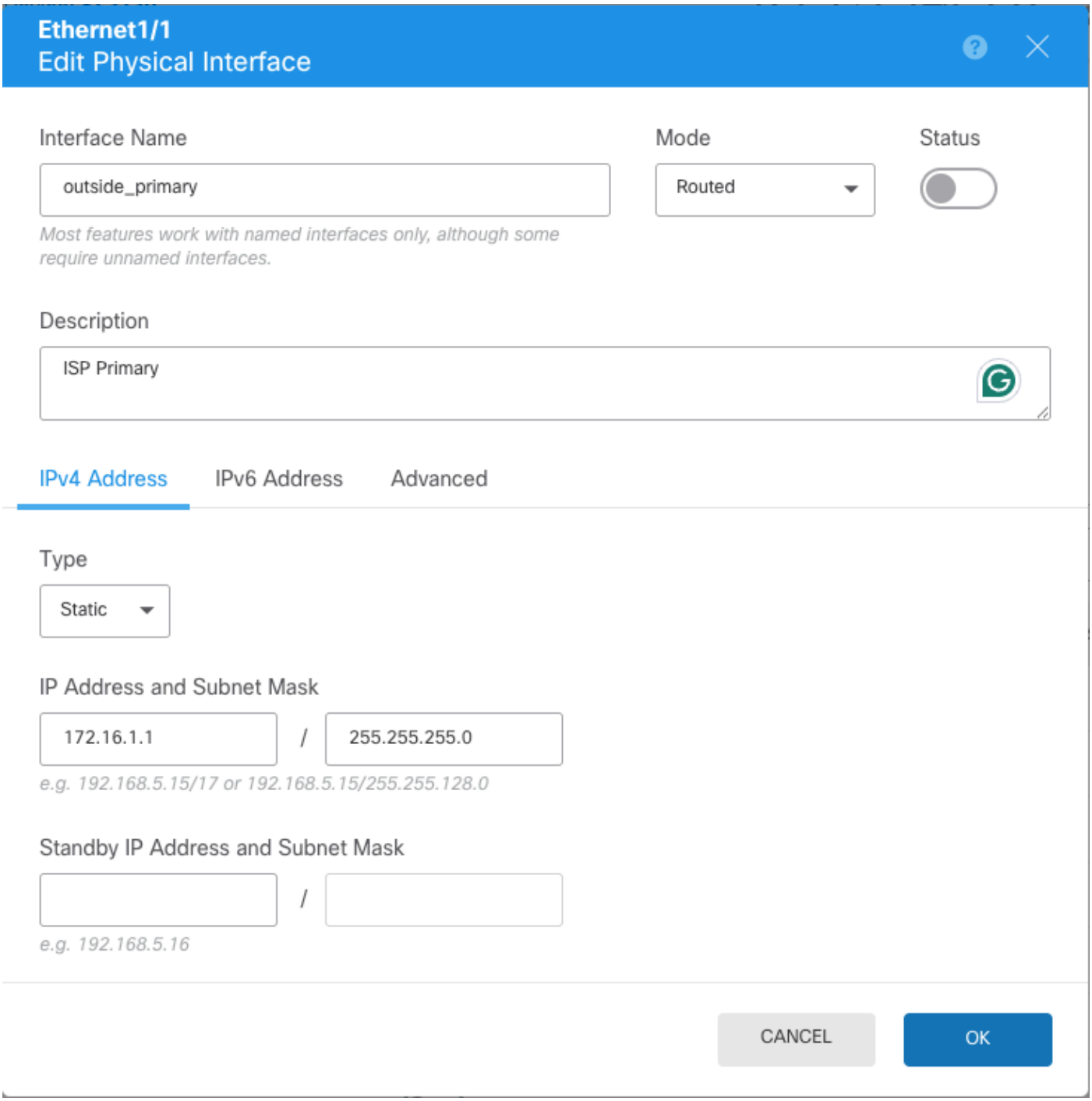
Om de interface voor de primaire ISP-verbinding te configureren, begint u met het selecteren van de gewenste interface. Selecteer de corresponderende knop voor de interface om door te gaan. In dit voorbeeld is de gebruikte interface Ethernet1/1.



Tabblad Interfaces

Stap 3.

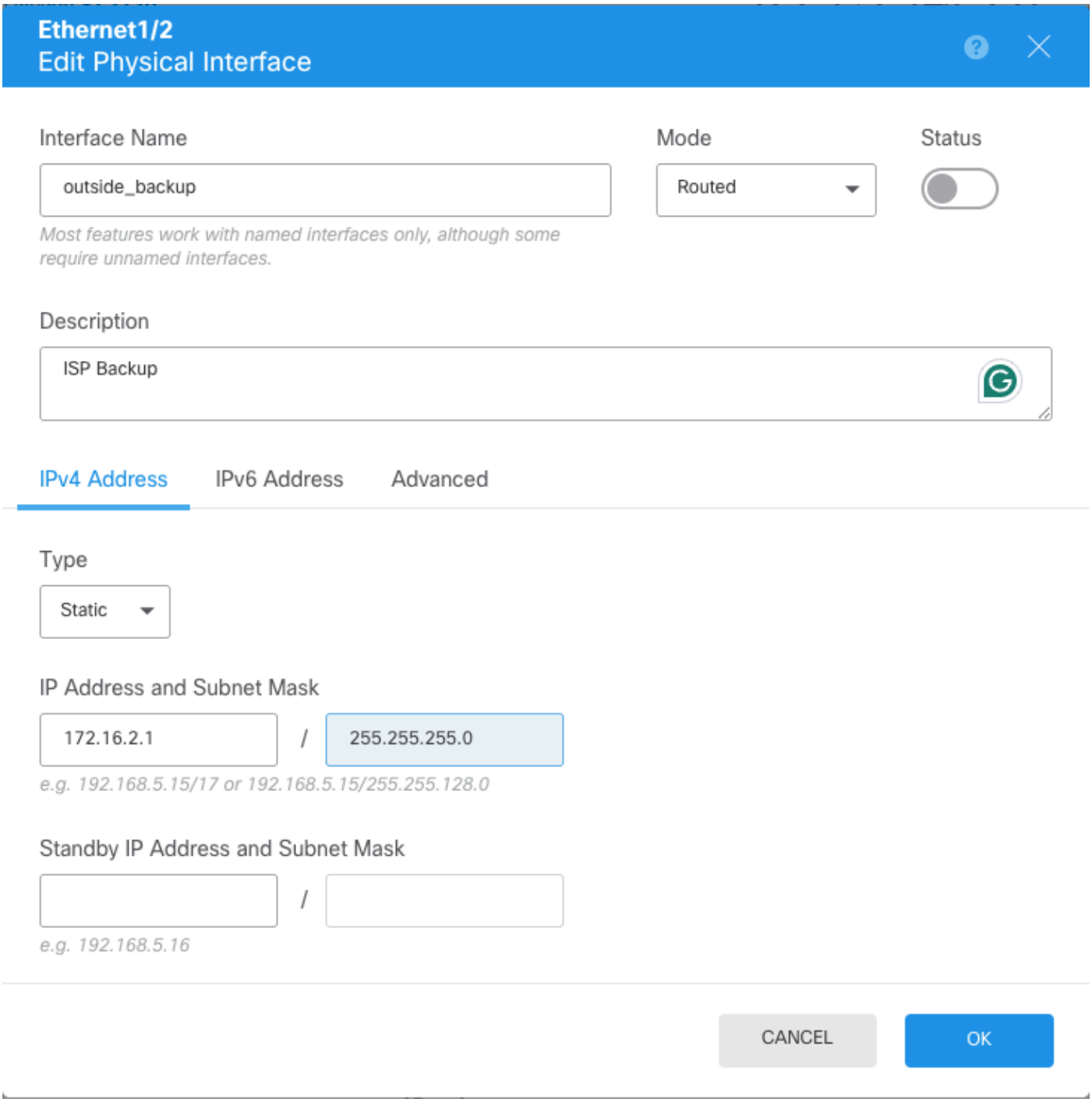
Configureer de interface met de juiste parameters voor uw primaire ISP-verbinding. In dit voorbeeld is de interface outside_primary.



Configuratie van primaire ISP-interface

Stap 4.

Herhaal hetzelfde proces voor de secundaire ISP-interface. In dit voorbeeld wordt de interface Ethernet1/2 gebruikt.

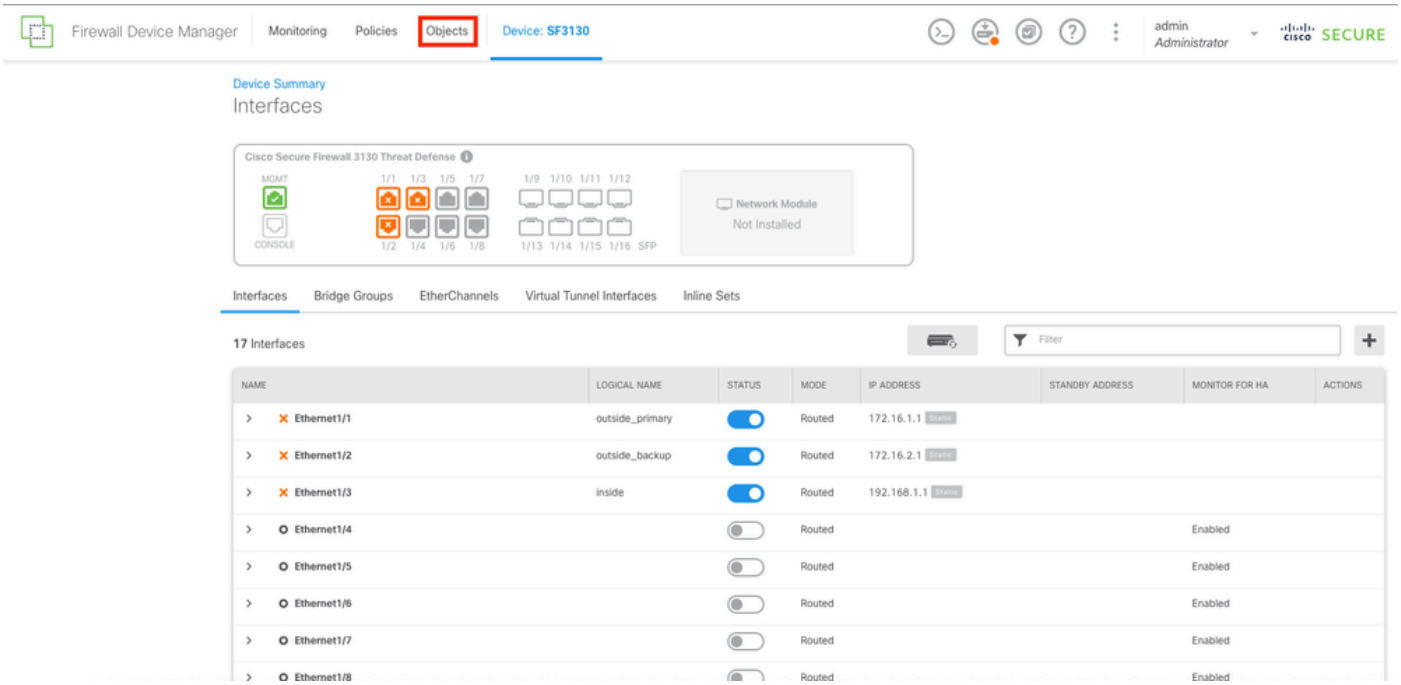


Configuratie van secundaire ISP-interface

Stap 5.

Nadat u de twee interfaces voor de ISP's hebt geconfigureerd, is de volgende stap het instellen van de SLA-monitor voor de primaire interface.

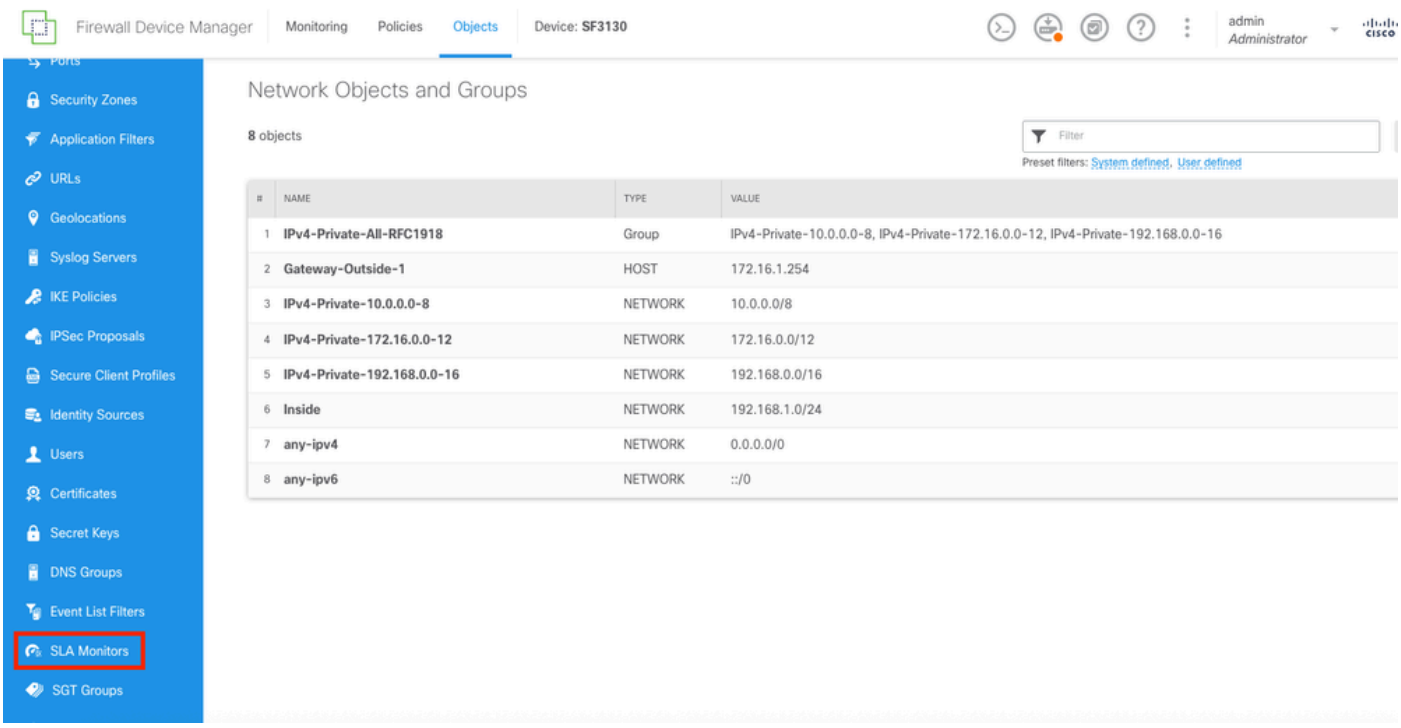
Navigeer naar de sectie Objecten door de knop Objecten boven in het menu te selecteren.



Geconfigureerde interfaces

Stap 6.

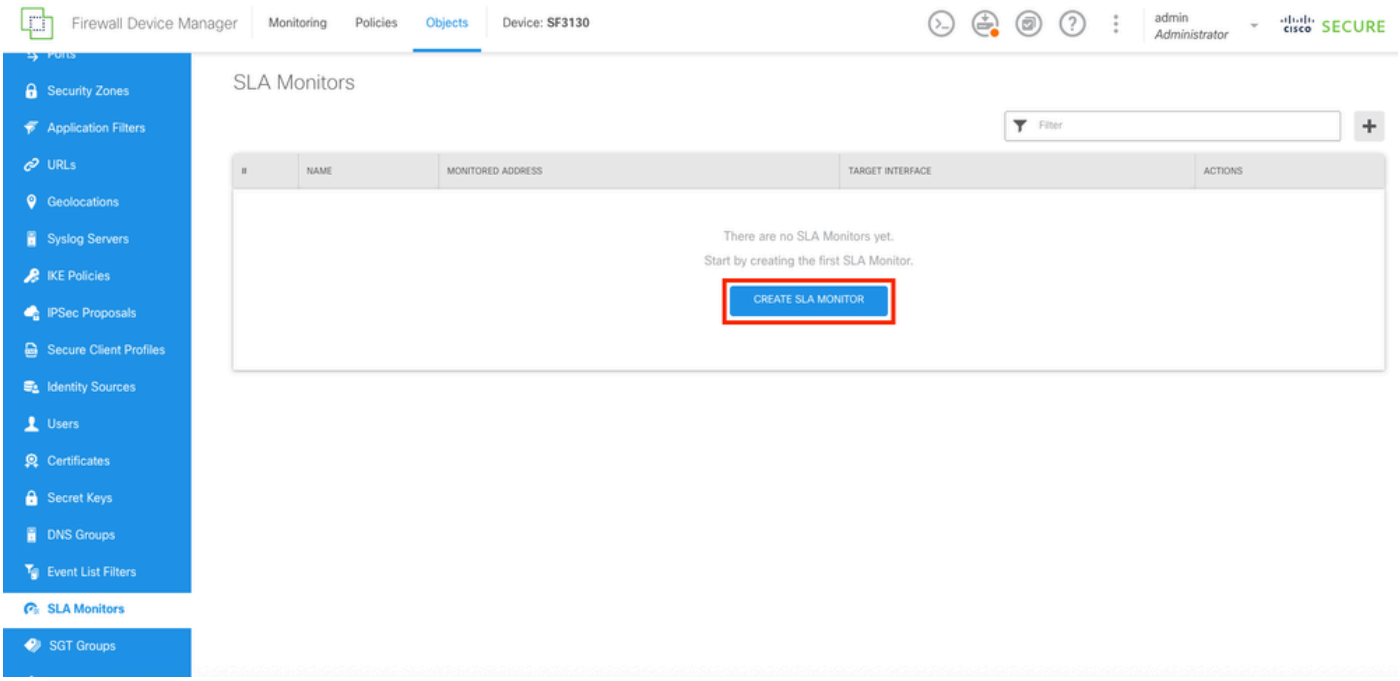
Selecteer in de linkerkolom de knop SLA-monitoren.



Objectenscherm

Stap 7.

Maak een nieuwe SLA-monitor door de knop SLA-monitor maken te selecteren.



Sectie SLA-monitor

Stap 8.

De parameters voor de primaire ISP-verbinding configureren.

Add SLA Monitor Object

Name

Outside_Primary_ISP

Description

Monitor for ISP Primary

Monitor Address

Gateway-Outside-1

Target Interface

outside_primary (Ethernet1/1)

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

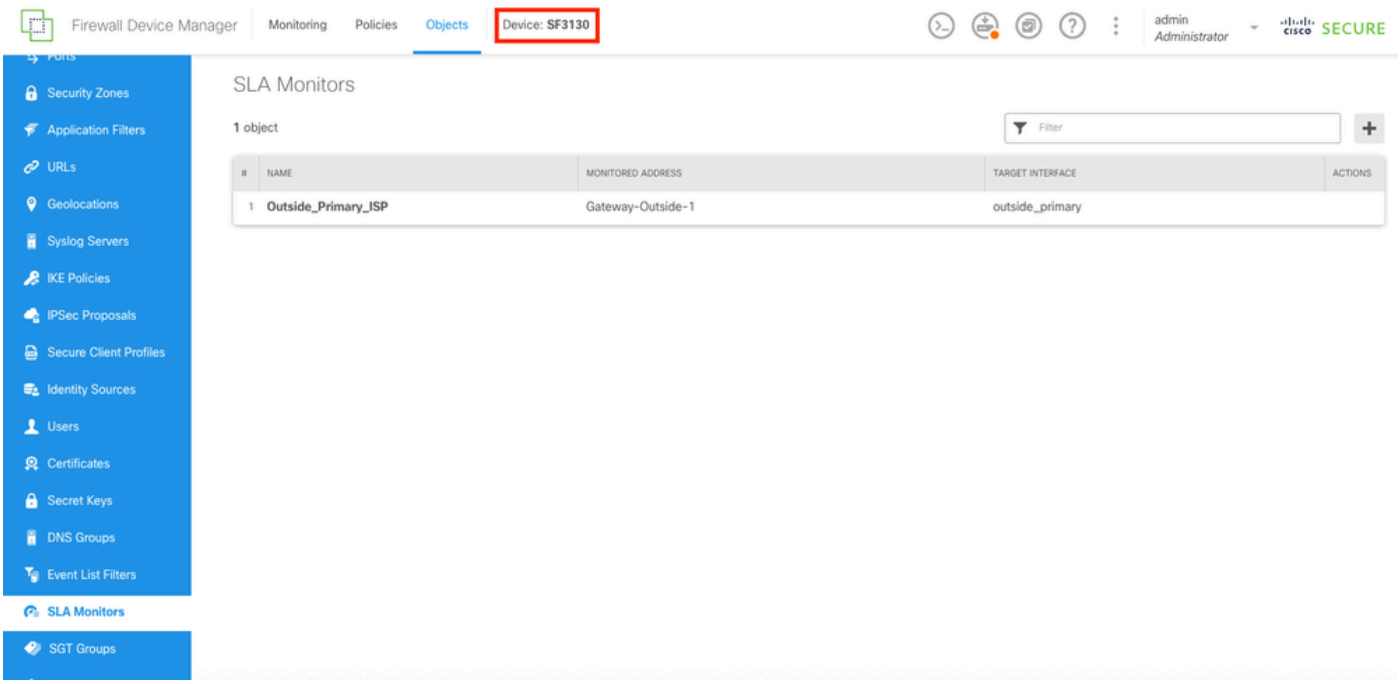
0 - 16384

CANCEL OK

SLA-object maken

Stap 9.

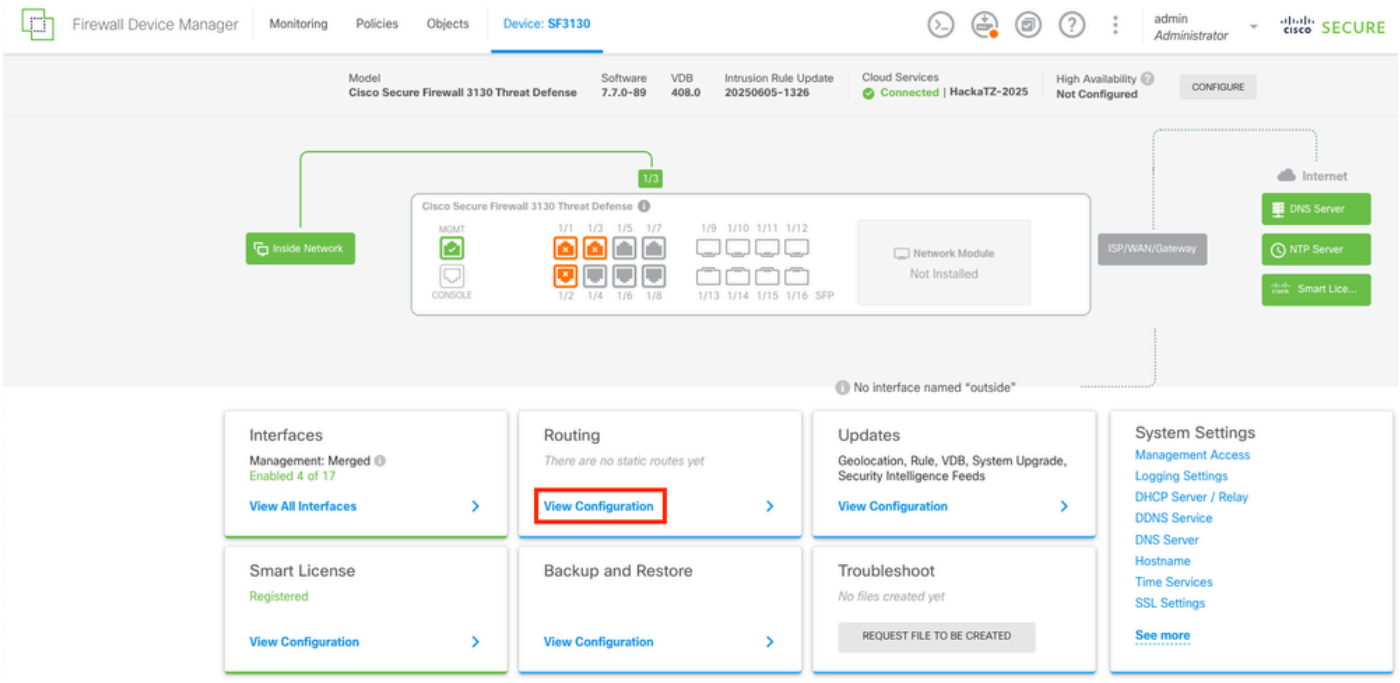
Nadat het object is gemaakt, moet de statische route voor de interfaces het maken. Navigeer naar het hoofddashboard door de knop Apparaat te selecteren.



SLA-monitor gemaakt

Stap 10.

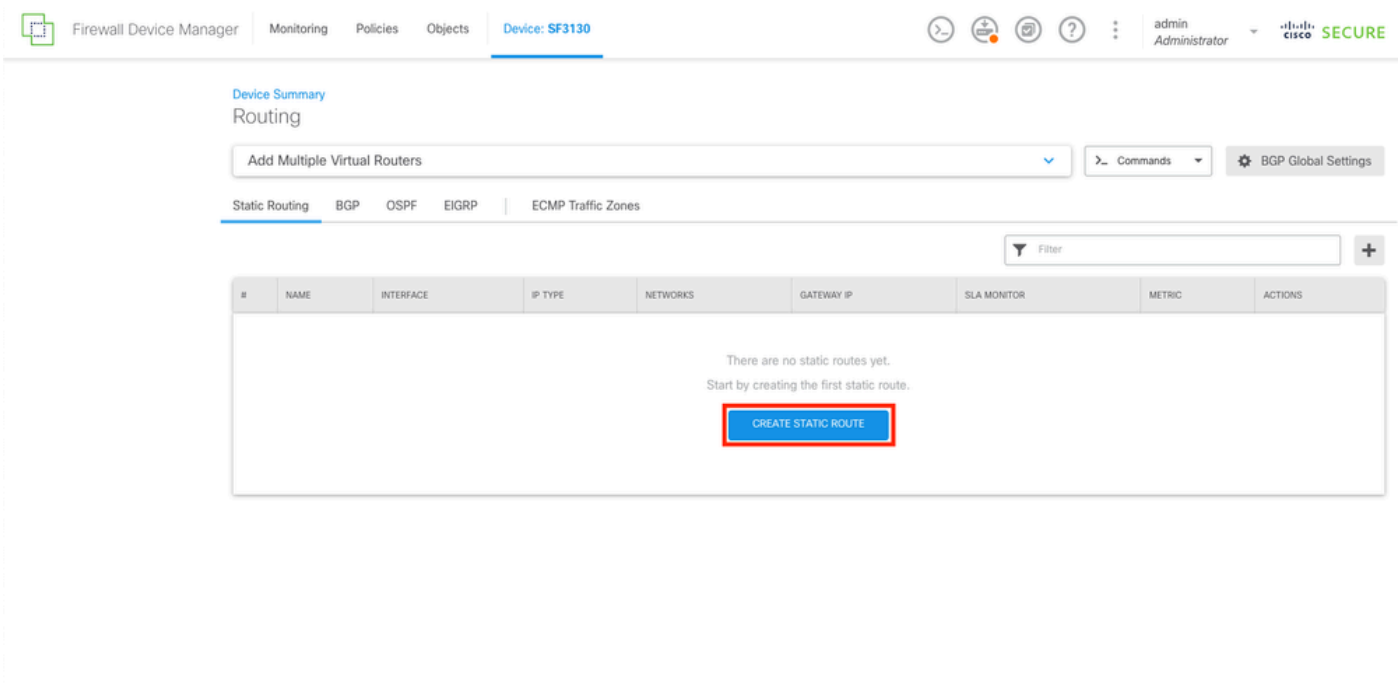
Navigeer naar de routeringssectie door de weergaveconfiguratie te selecteren in het deelvenster Routering.



Hoofddashboard

Stap 11.

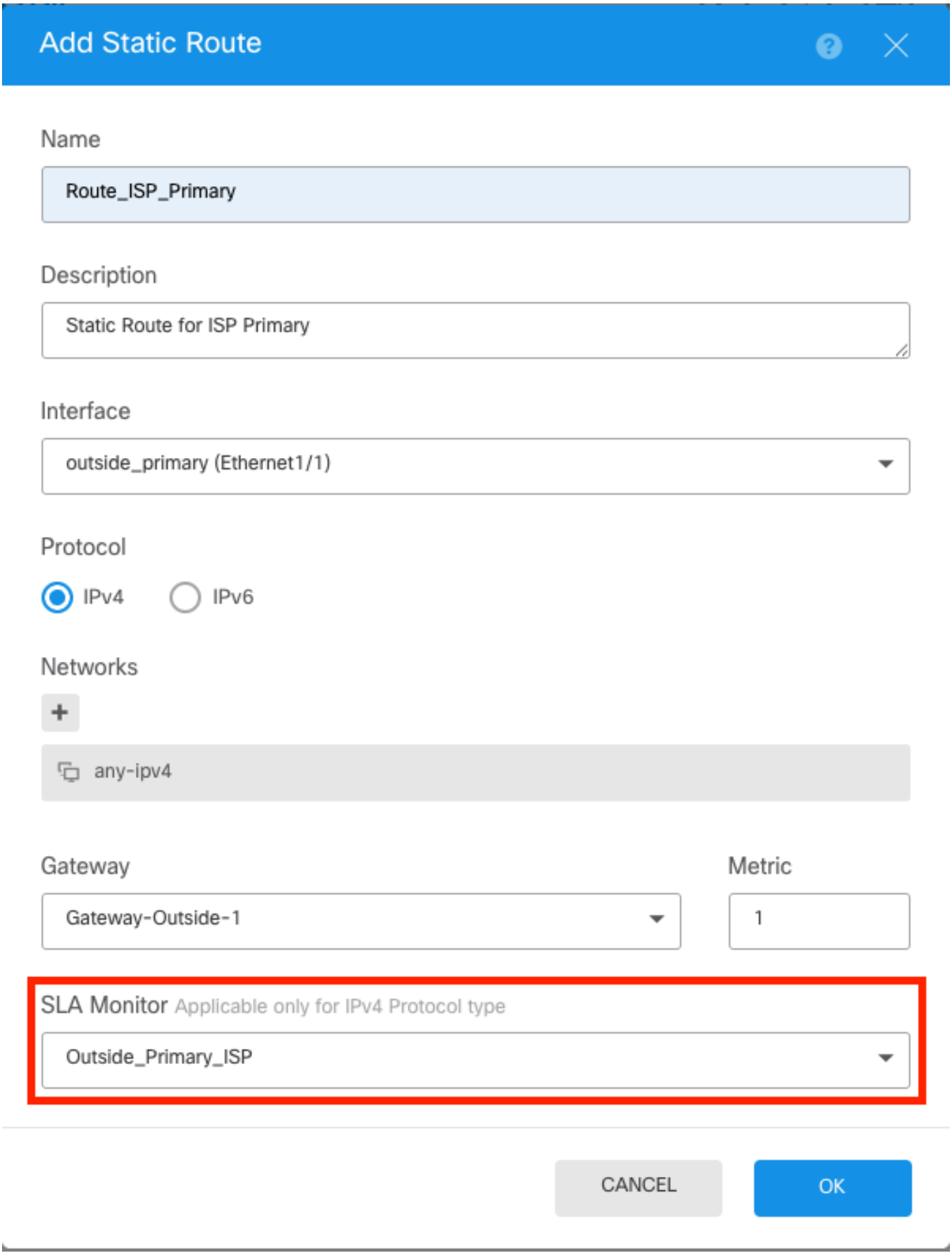
Maak op het tabblad Statische routering de 2 standaard statische routes voor beide ISP's. Als u een nieuwe statische route wilt maken, selecteert u de knop STATISCHE ROUTE MAKEN.



statische routeringssectie

Stap 12.

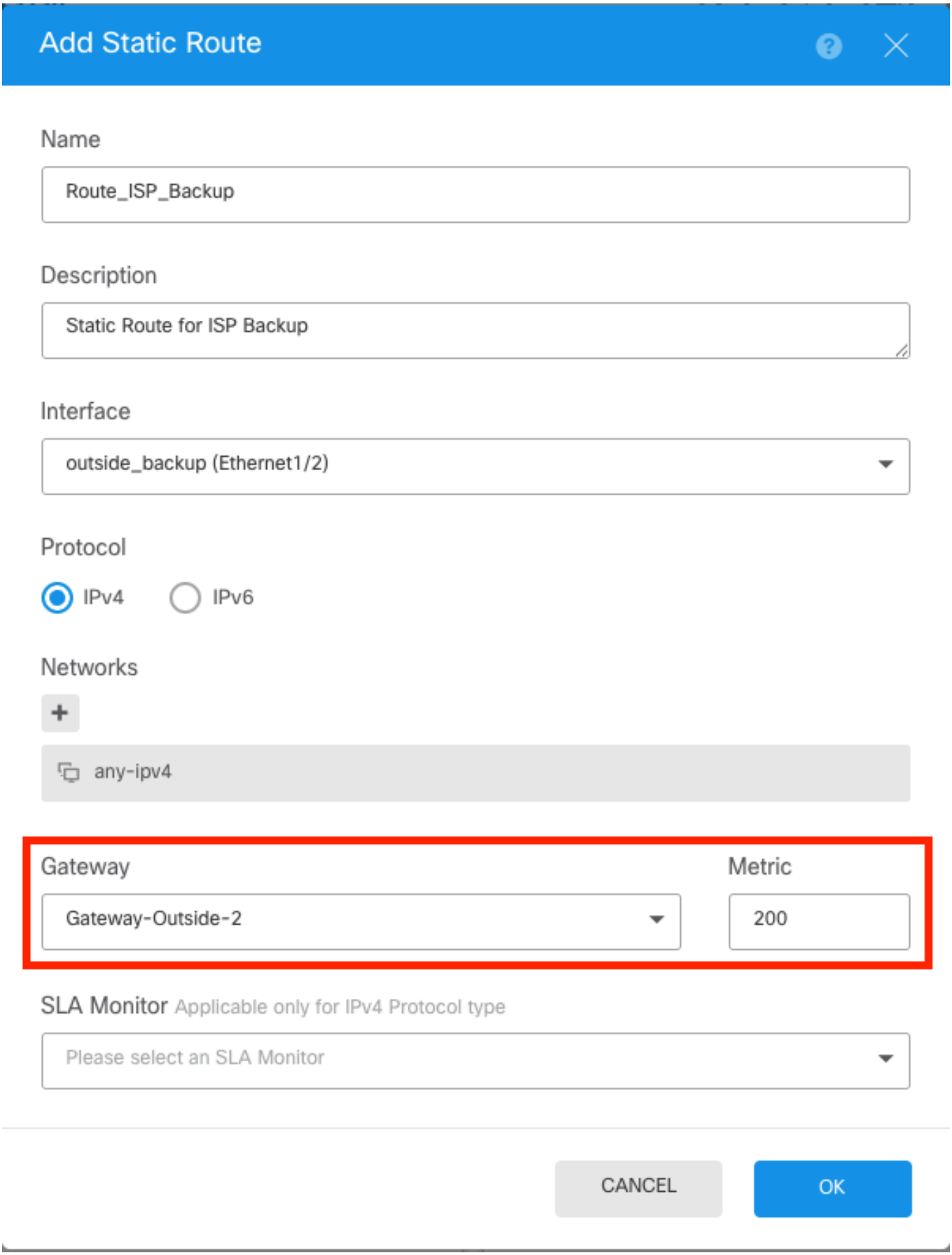
Maak eerst de statische route voor de primaire ISP. Voeg aan het einde het SLA-monitorobject toe dat bij de laatste stap is gemaakt.



Statische route voor primaire ISP

Stap 13.

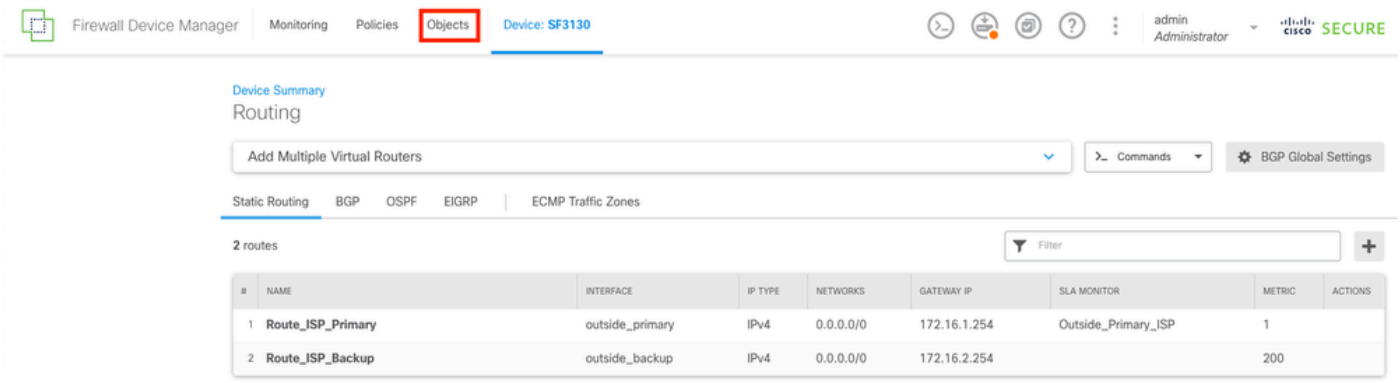
Herhaal de laatste stap en maak een standaardroute, voor de secundaire ISP met de juiste gateway en verschillende Metric. In dit voorbeeld is dit verhoogd naar 200.



Statische route voor secundaire ISP

Stap 14.

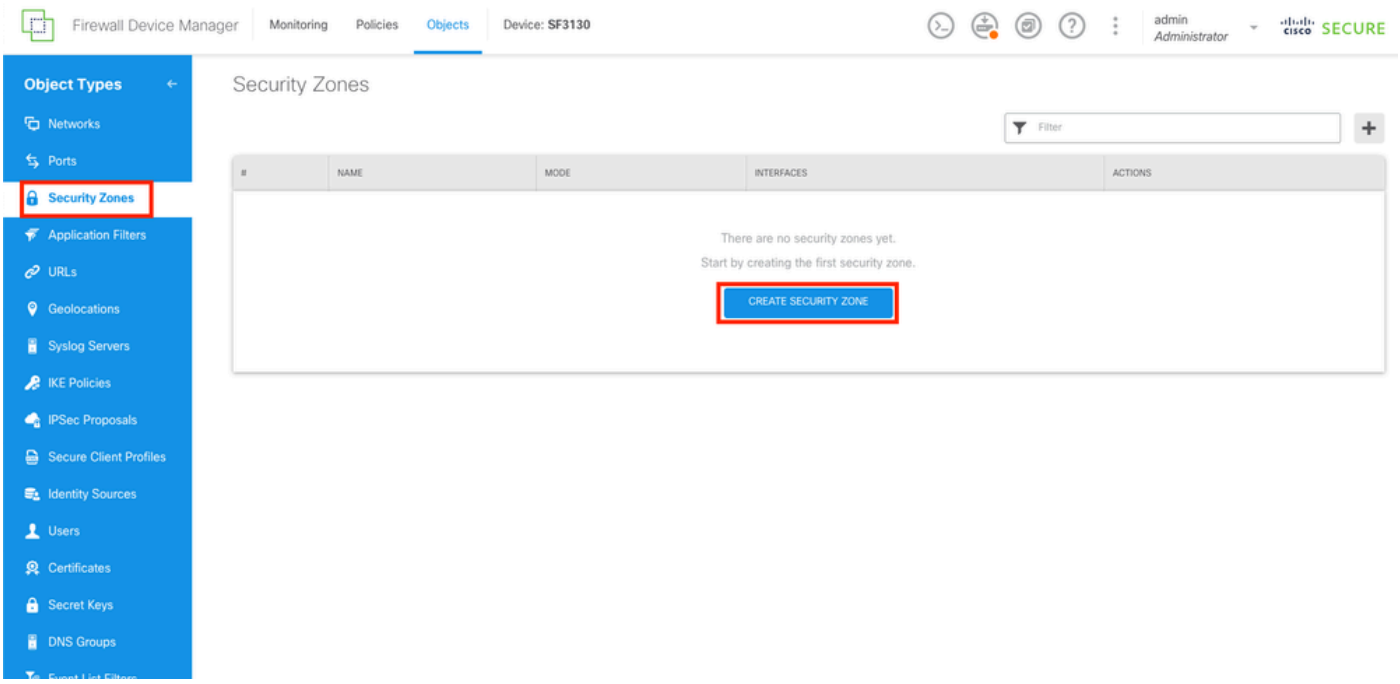
Zodra beide statische routes zijn gemaakt, moet een beveiligingszone worden gemaakt. Navigeer naar de sectie Objecten door de knop Objecten bovenaan te selecteren.



Statische routes aangemaakt

Stap 15.

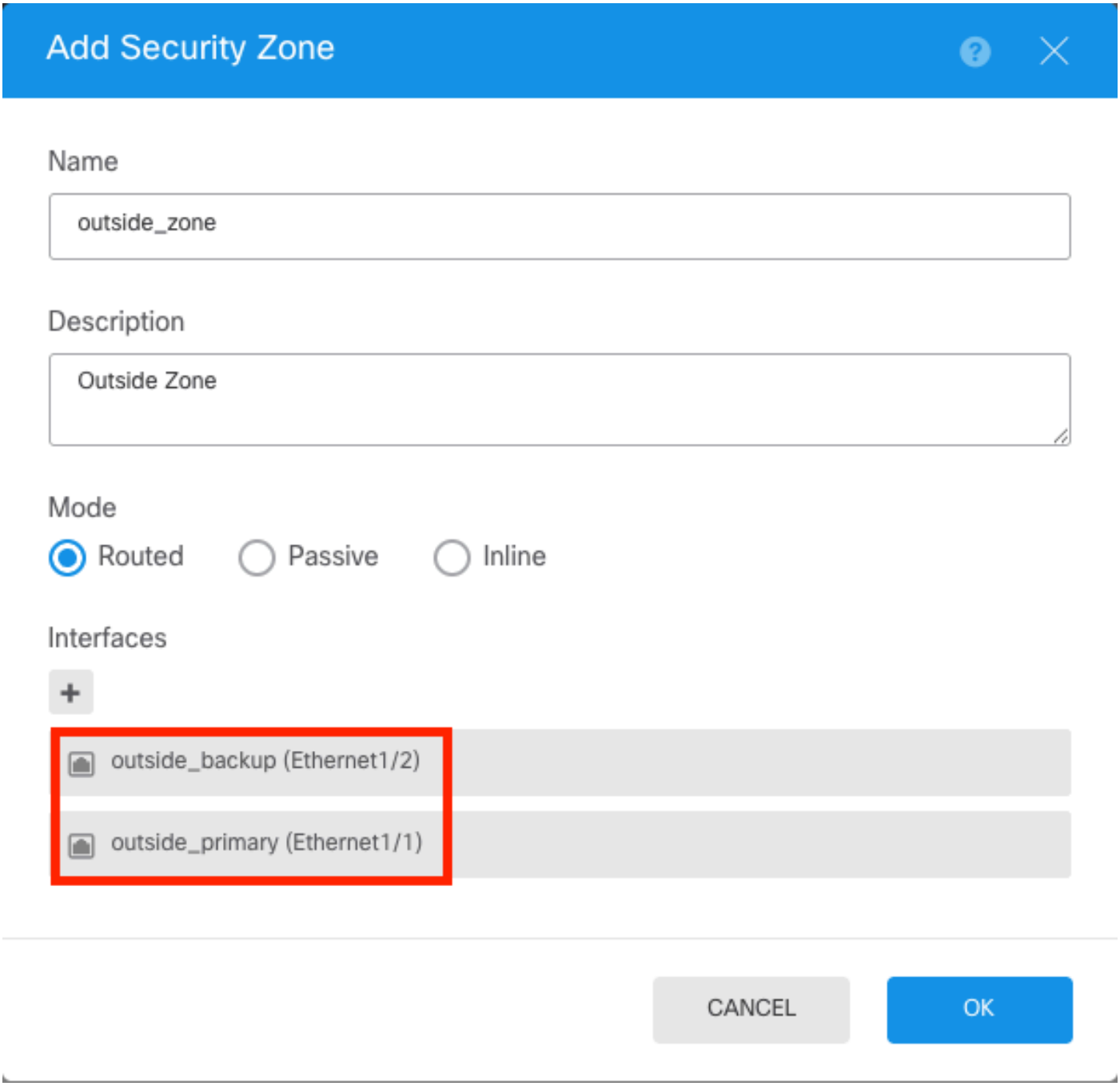
Navigeer naar de sectie Beveiligingszones door in de linkerkolom de knop Beveiligingszones te selecteren en maak vervolgens een nieuwe zone door de knop BEVEILIGINGSZONE MAKEN te selecteren.



Sectie Beveiligingszones

Stap 16.

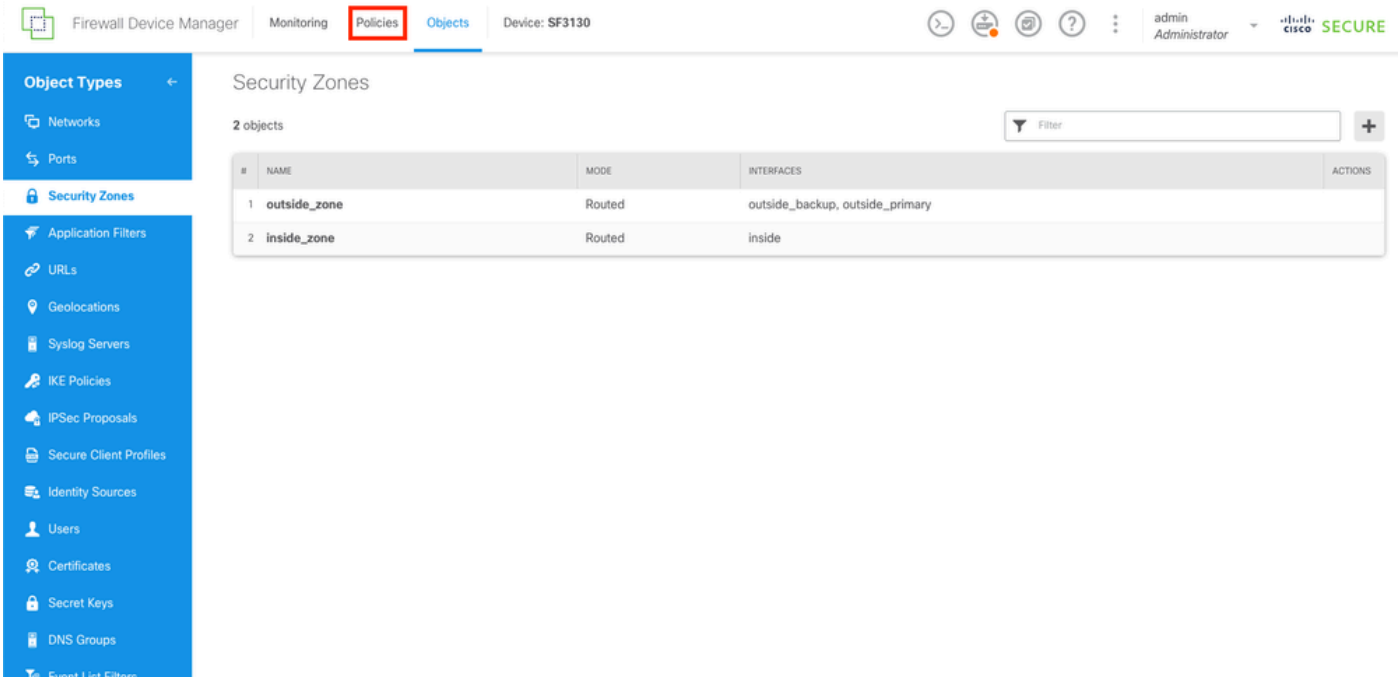
Maak de externe beveiligingszone met de beide externe interfaces voor de ISP-verbindingen.



Veiligheidszone buiten

Stap 17.

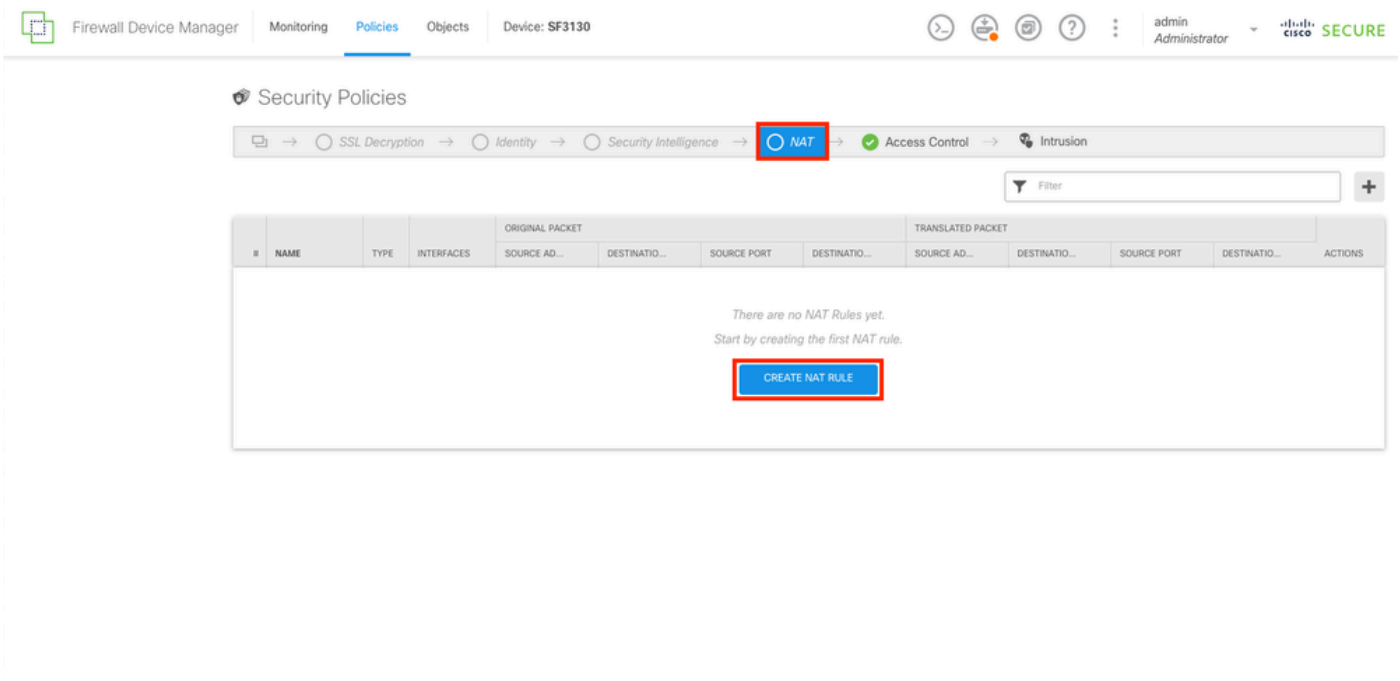
Nadat de veiligheidszone is gecreëerd, moet een NAT worden gecreëerd. Navigeer naar het gedeelte Beleid door bovenaan de knop Beleid te selecteren.



Beveiligingszones gemaakt

Stap 18.

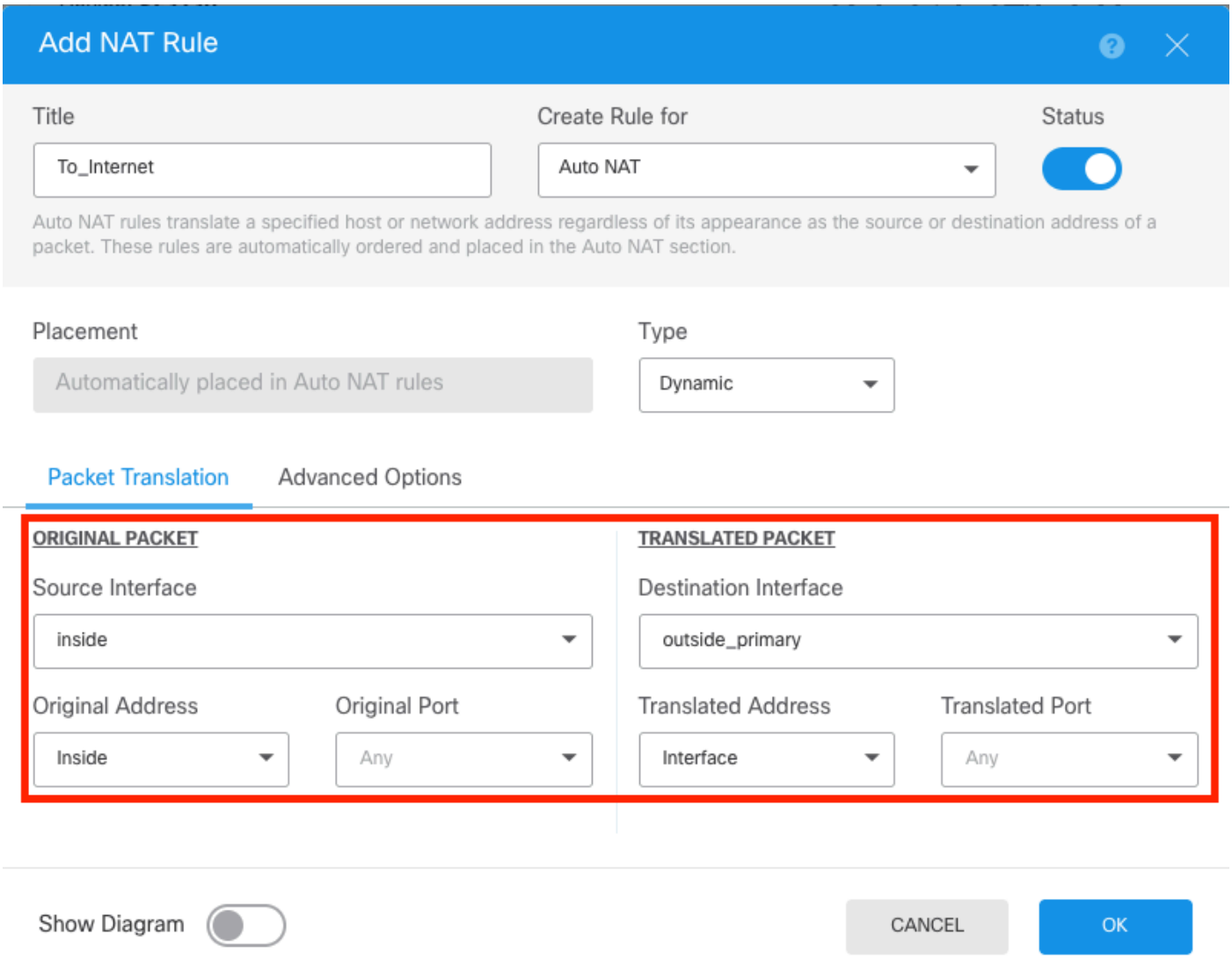
Navigeer naar de NAT-sectie door de knop NAT te selecteren en maak vervolgens een nieuwe regel door de knop NAT-REGEL MAKEN te selecteren.



NAT-sectie

Stap 19.

Voor de ISP-failover moet de configuratie twee routes hebben via externe interfaces. Ten eerste voor de verbinding van de primaire externe interface met de primaire ISP.

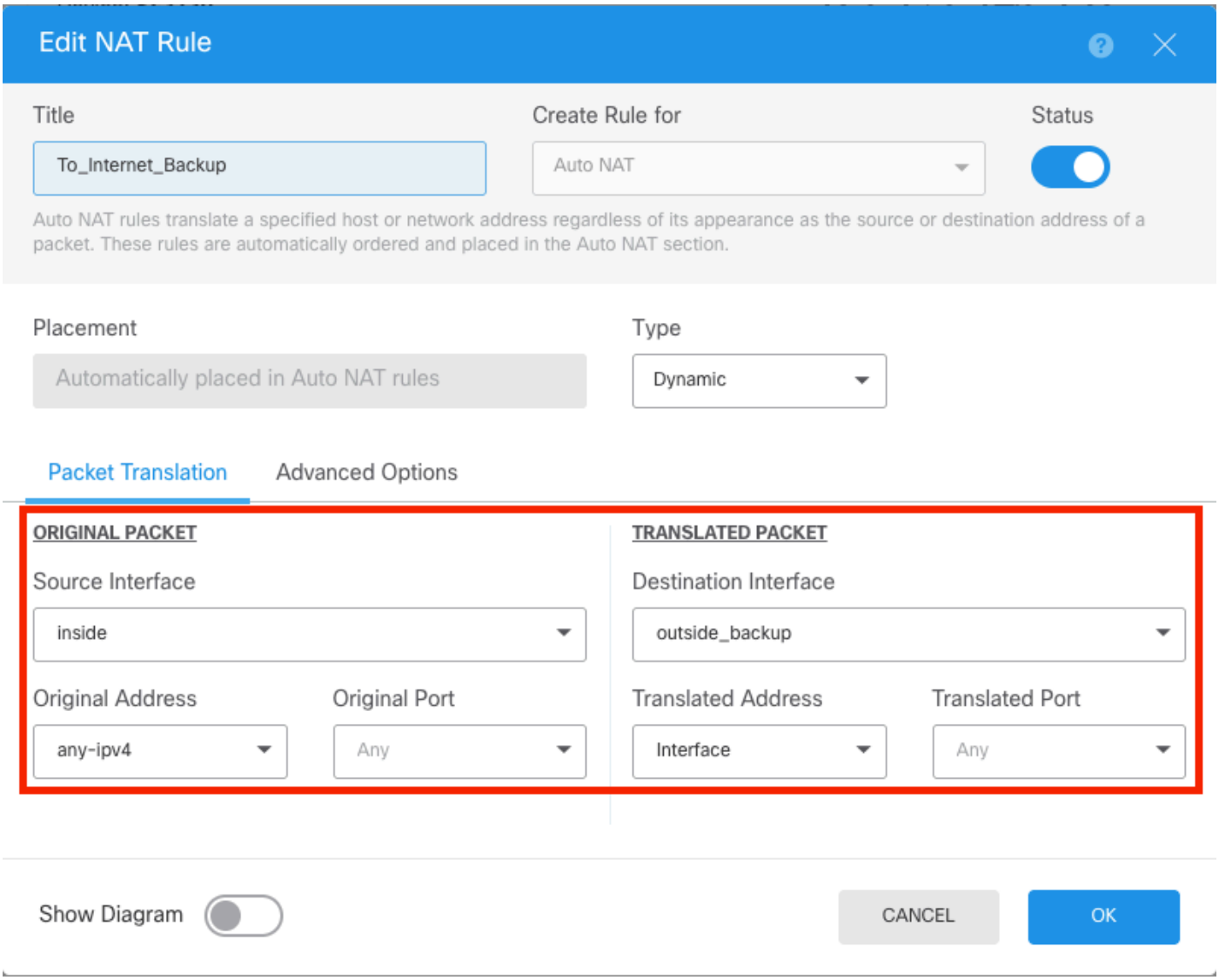


NAT voor primaire ISP

Stap 20.

Nu een tweede NAT voor de Secundaire ISP-verbinding.

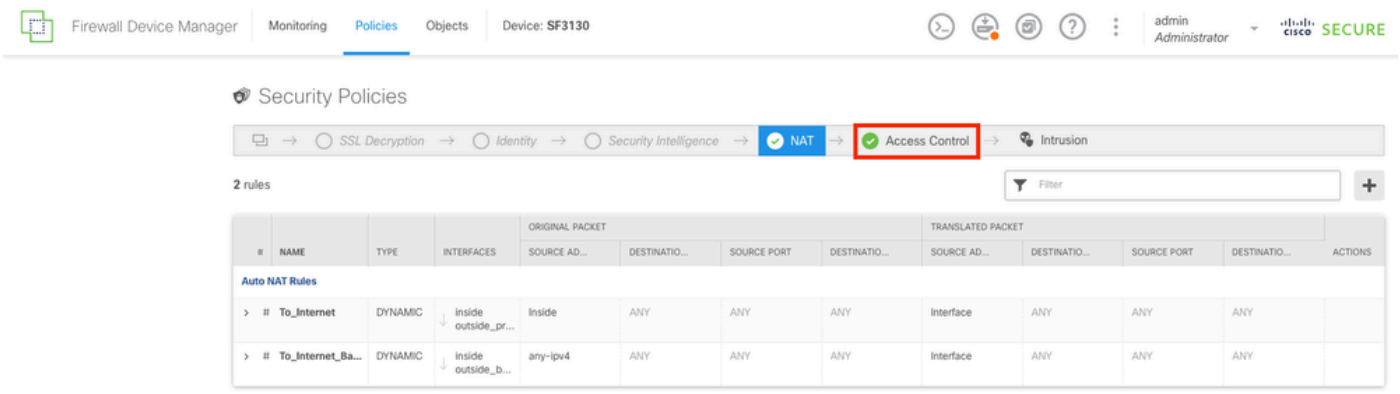
Opmerking: voor het oorspronkelijke adres kan niet hetzelfde netwerk worden gebruikt. In dit voorbeeld, voor de secundaire ISP, is het oorspronkelijke adres het object any-ipv4.



NAT voor secundaire ISP

Stap 21.

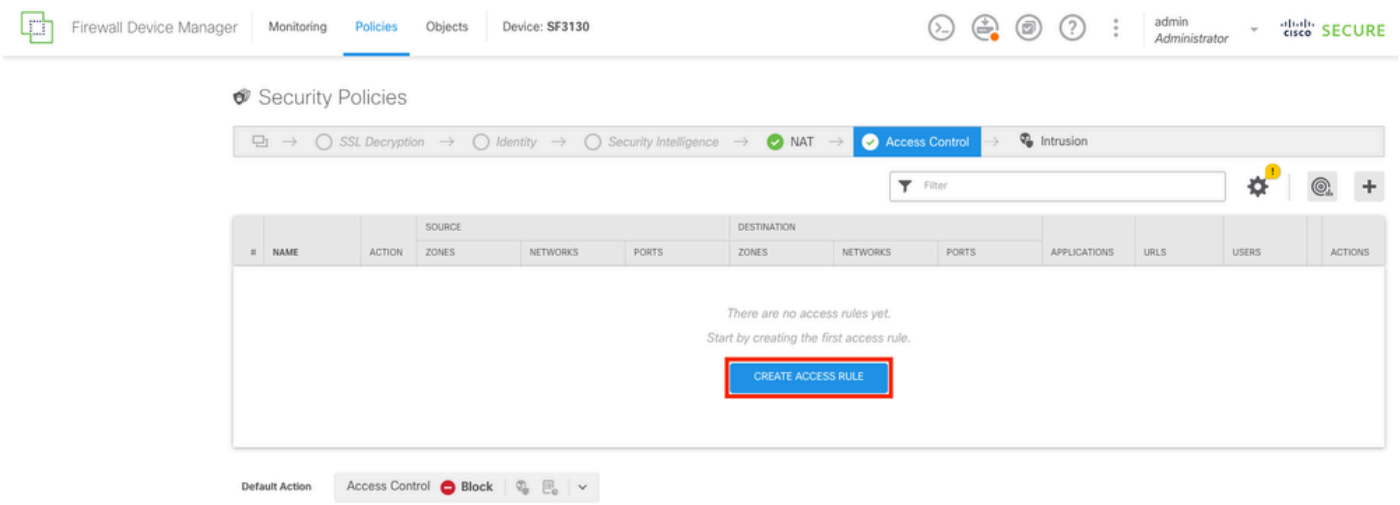
Nadat beide NAT-regels zijn gemaakt, moet een toegangscontroleregels worden vastgesteld om uitgaand verkeer mogelijk te maken. Selecteer de knop Toegangscontrole.



NAT-regels gemaakt

Stap 22.

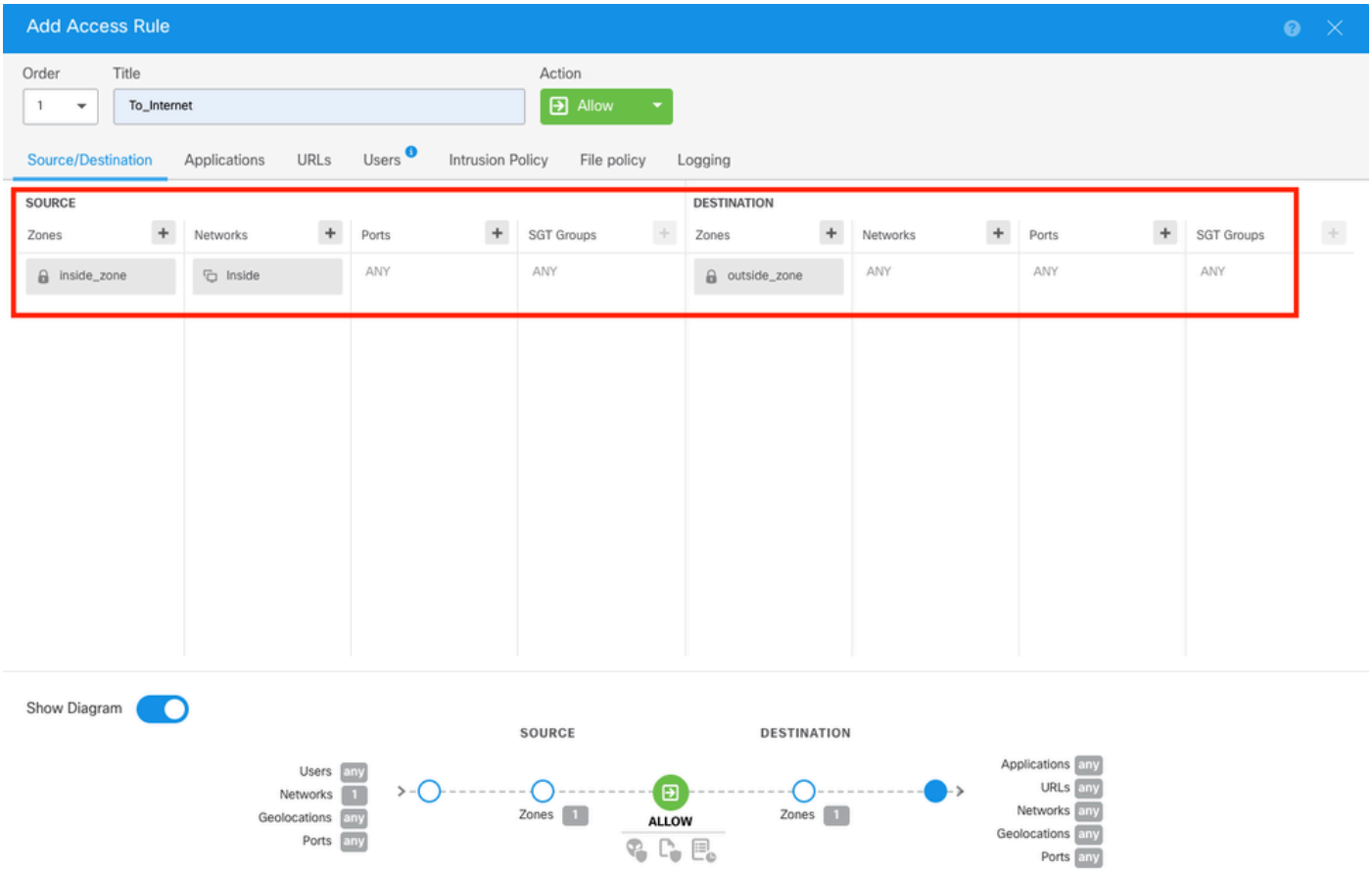
Als u de toegangsregel wilt maken, selecteert u de knop TOEGANGSREGEL MAKEN.



sectie Toegangscontrole

Stap 23.

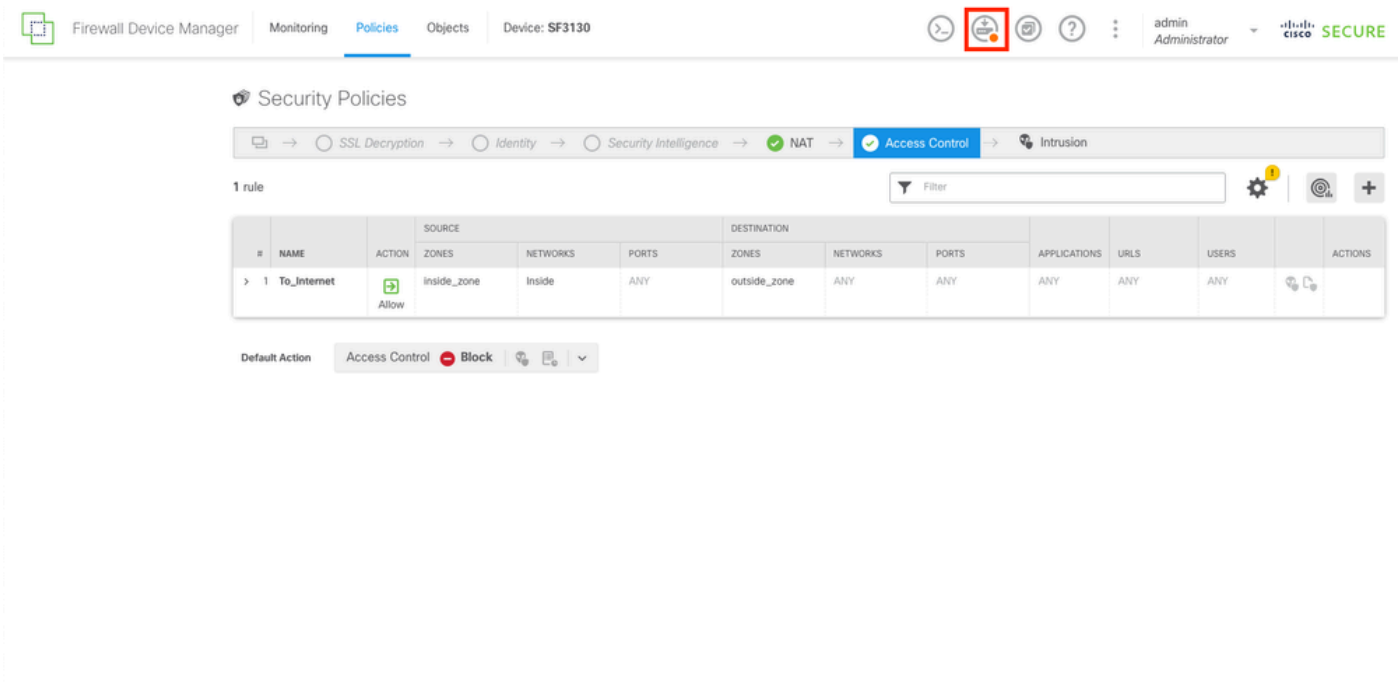
Selecteer de gewenste zones en netwerken.



toegangscontroleregels

Stap 24.

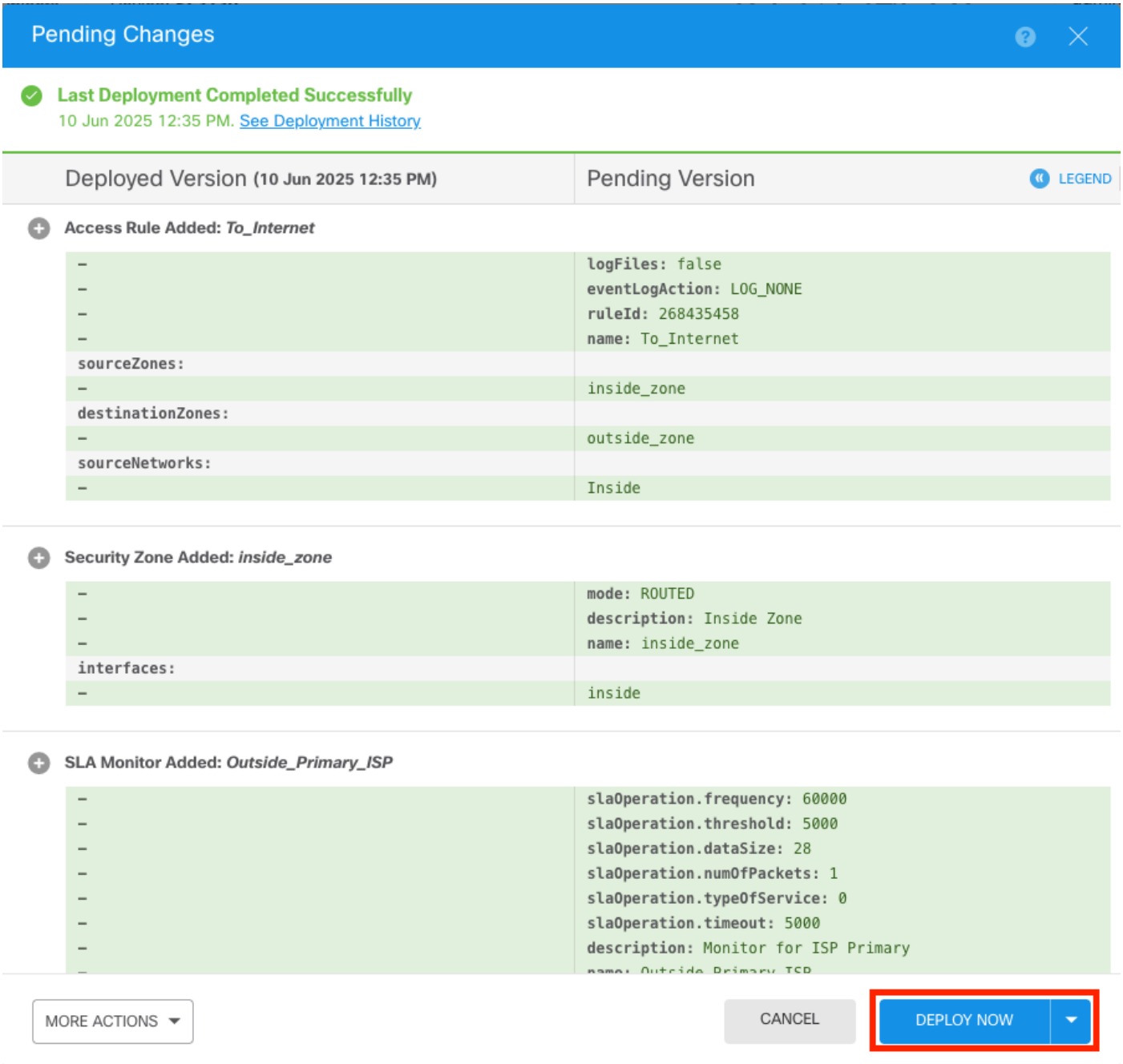
Zodra de toegangsregel is gemaakt, gaat u verder met het implementeren van alle wijzigingen door bovenaan de knop Implementeren te selecteren.



Toegangsregel gemaakt

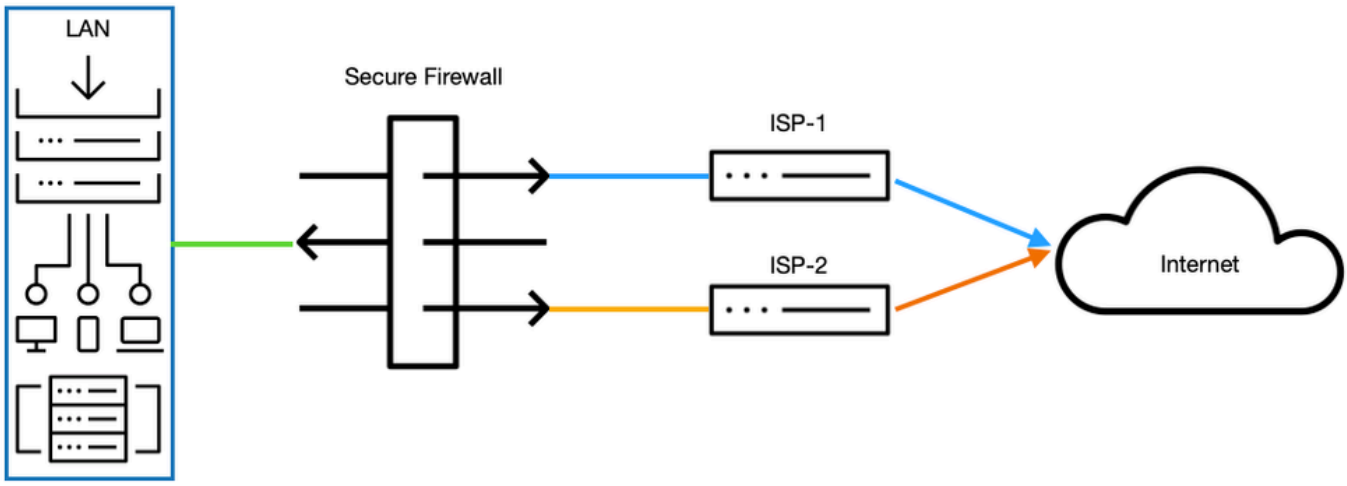
Stap 25.

Controleer de wijzigingen en selecteer vervolgens de knop Nu implementeren.



Verificatie van implementatie

Netwerkdiagram



Netwerkdiagram

Verifiëren

<#root>

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

SF3130#

show ip

System IP Addresses:
Interface Name IP address Subnet mask Method
Ethernet1/1 outside_primary 172.16.1.1 255.255.255.0 manual

------------> THE PRIMARY INTERFACE OF THE ISP IS SET

Ethernet1/2 outside_backup 172.16.2.1 255.255.255.0 manual

------------> THE SECONDARY INTERFACE OF THE ISP IS SET

Ethernet1/3 inside 192.168.1.1 255.255.255.0 manual

SF3130#

show interface ip brief

Interface IP-Address OK? Method Status Protocol
Ethernet1/1 172.16.1.1 YES manual up up

------------------> THE INTERFACE IS UP AND RUNNING

```
Ethernet1/2 172.16.2.1  YES manual   up      up
```

------------------> THE INTERFACE IS UP AND RUNNING

```
Ethernet1/3 192.168.1.1 YES manual   up      up

SF3130#
```

show route

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

----> THE DEFAULT ROUTE IS CONNECTED THROUGH THE PRIMARY ISP

```
C  172.16.1.0  255.255.255.0   is directly connected, outside_primary
L  172.16.1.1  255.255.255.255 is directly connected, outside_primary
C  172.16.2.0  255.255.255.0   is directly connected, outside_backup
L  172.16.2.1  255.255.255.255 is directly connected, outside_backup
C  192.168.1.0 255.255.255.0   is directly connected, inside
L  192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#
```

show run route

```
route outside_primary 0.0.0.0 0.0.0.0 172.16.1.254 1 track 1
route outside_backup  0.0.0.0 0.0.0.0 172.16.2.254 200

SF3130#
```

show sla monitor configuration

---> CHECKING THE SLA MONITOR CONFIGURATION

```
SA Agent, Infrastructure Engine-II
Entry number: 539523651
Owner:
Tag:
Type of operation to perform: echo
Target address: 172.16.1.254
Interface: outside_primary
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 3000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
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:

SF3130#
```

show sla monitor operational-state

```
Entry number: 739848060
Modification time: 01:24:11.029 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
```

---------------------------> THE ISP PRIMARY IS IN A HEALTHY STATE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

AFTERARGBSETHBNDGFSHNDFGSDBFB

SF3130#
```

show interface ip brief

```
Interface   IP-Address  OK? Method Status Protocol
Ethernet1/1 172.16.1.1  YES manual  down   down
```

------------------> THE PRIMARY ISP IS DOWN

```
Ethernet1/2 172.16.2.1  YES manual   up     up
Ethernet1/3 192.168.1.1 YES manual   up     up

SF3130#
```

show route

```
Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [200/0] via 172.16.2.254, outside_backup
```

---------> AFTER THE ISP PRIMARY FAILS, INSTANTLY THE ISP BACKUP IS FAILOVER AND IS INSTALL IN THE ROUTI

```
C  172.16.2.0 255.255.255.0    is directly connected, outside_backup
L  172.16.2.1 255.255.255.255  is directly connected, outside_backup
C  192.168.1.0 255.255.255.0   is directly connected, inside
L  192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#
```

show sla monitor operational-state

```
Entry number: 739848060
Modification time: 01:24:11.140 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
```

```
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
```

----------> AFTER THE DOWNTIME OF THE PRIMARY ISP THE TIMEOUT IS FLAGGED

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

SF3130#
```

show route

```
Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary
```

----------> AFTER A FEW SECONDS ONCE THE PRIMARY INTERFACE IS BACK THE DEFAULT ROUTE INSTALLS AGAIN IN

```
C 172.16.1.0 255.255.255.0    is directly connected, outside_primary
L 172.16.1.1 255.255.255.255  is directly connected, outside_primary
C 172.16.2.0 255.255.255.0    is directly connected, outside_backup
L 172.16.2.1 255.255.255.255  is directly connected, outside_backup
C 192.168.1.0 255.255.255.0   is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside
```

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.