Konfigurieren von zwei ISPs auf FTD mithilfe von FDM

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Dual Internet Service Provider (ISP)-Failover mithilfe des Firewall Device Manager (FDM) für die Secure Firewall Series konfigurieren.

Voraussetzungen

Anforderungen

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

- Grundlegendes Routing
- Kenntnisse über das Firewall Device Manager-Dashboard
- Mindestens zwei Internet Service Provider, die mit der sicheren Firewall verbunden sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

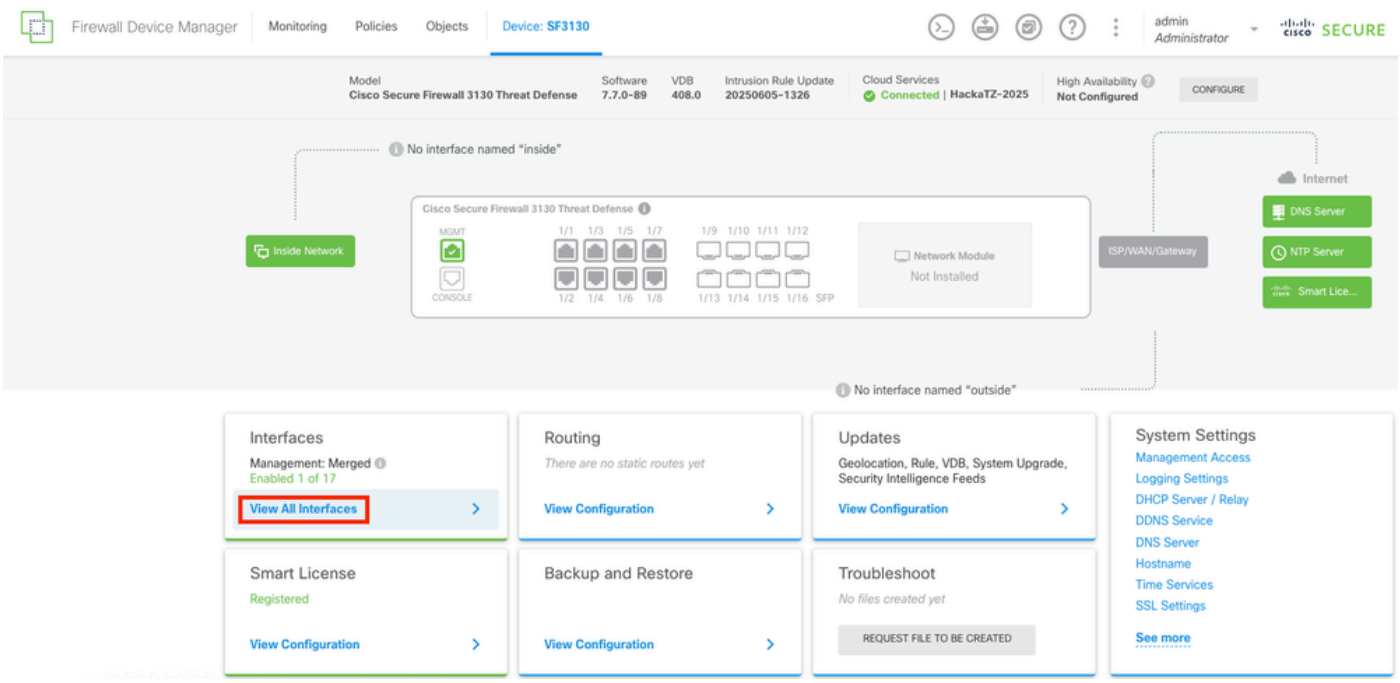
- Cisco Secure Firewall mit Version 7.7.x oder höher
- Secure Firewall 3130 mit Version 7.7.0.

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.

Konfigurieren

Schritt 1:

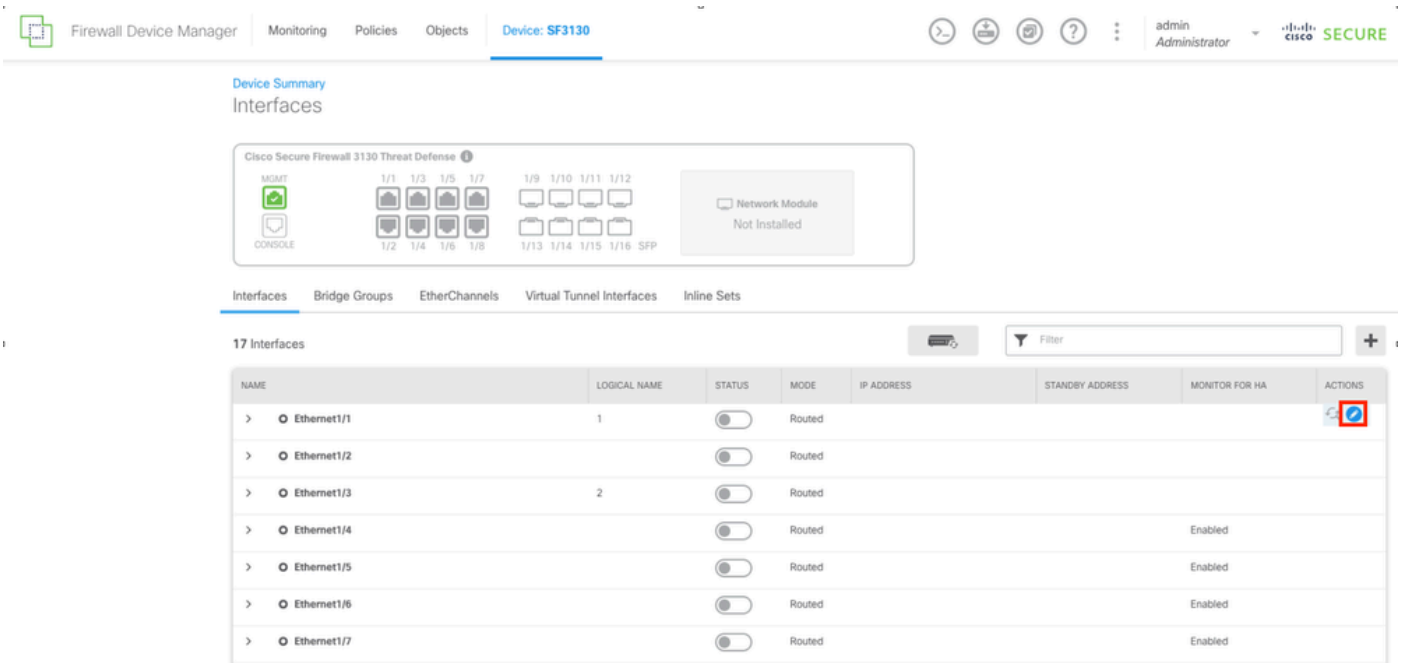
Melden Sie sich beim FDM an der sicheren Firewall an, und navigieren Sie zum Schnittstellenabschnitt, indem Sie auf die Schaltfläche Alle Schnittstellen anzeigen klicken.



FDM-Haupt-Dashboard

Schritt 2:

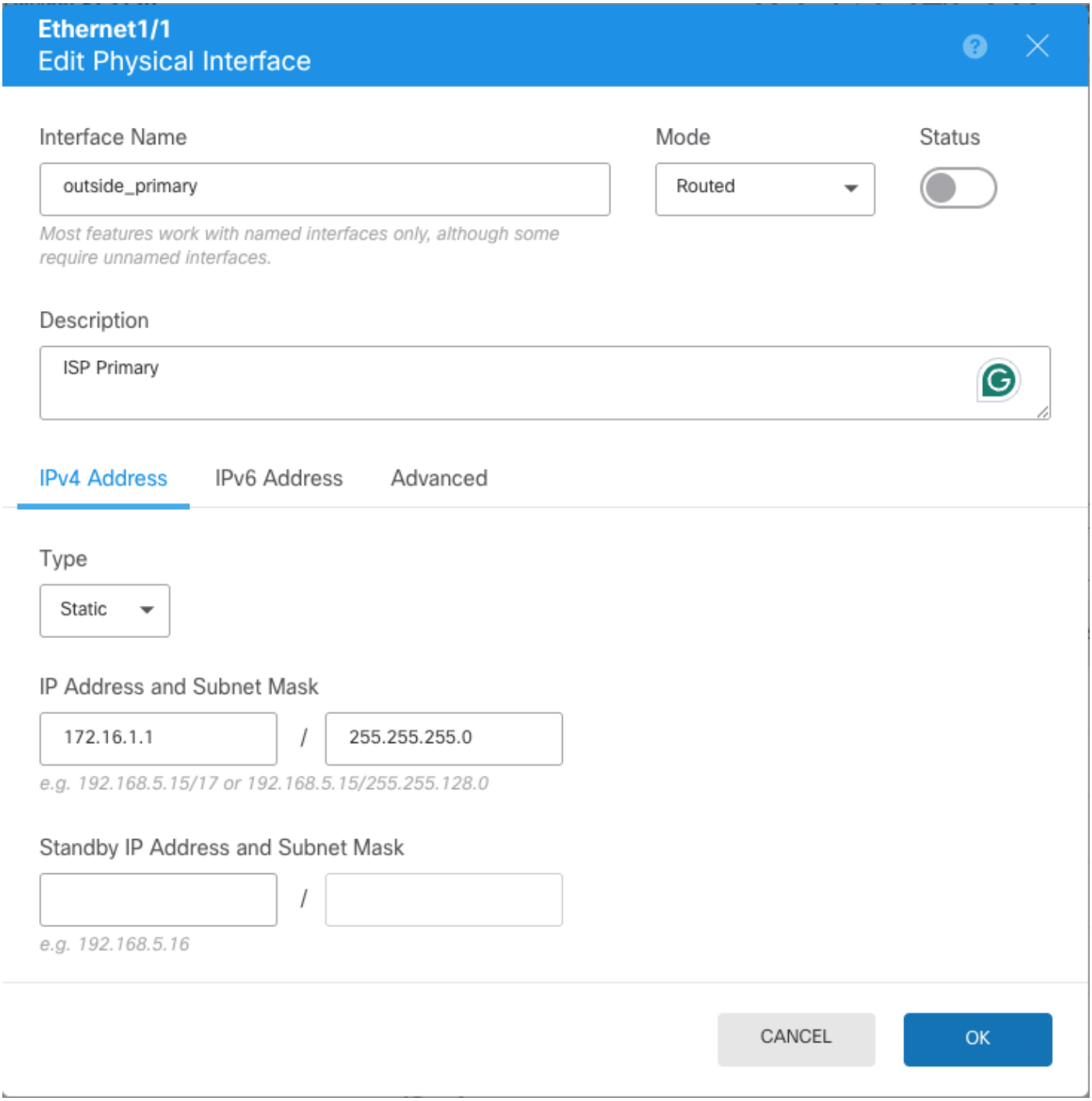
Um die Schnittstelle für die primäre ISP-Verbindung zu konfigurieren, wählen Sie zunächst die gewünschte Schnittstelle aus. Auswählen der entsprechenden Schnittstellentaste, um fortzufahren In diesem Beispiel wird als Schnittstelle Ethernet1/1 verwendet.



Registerkarte Schnittstellen

Schritt 3:

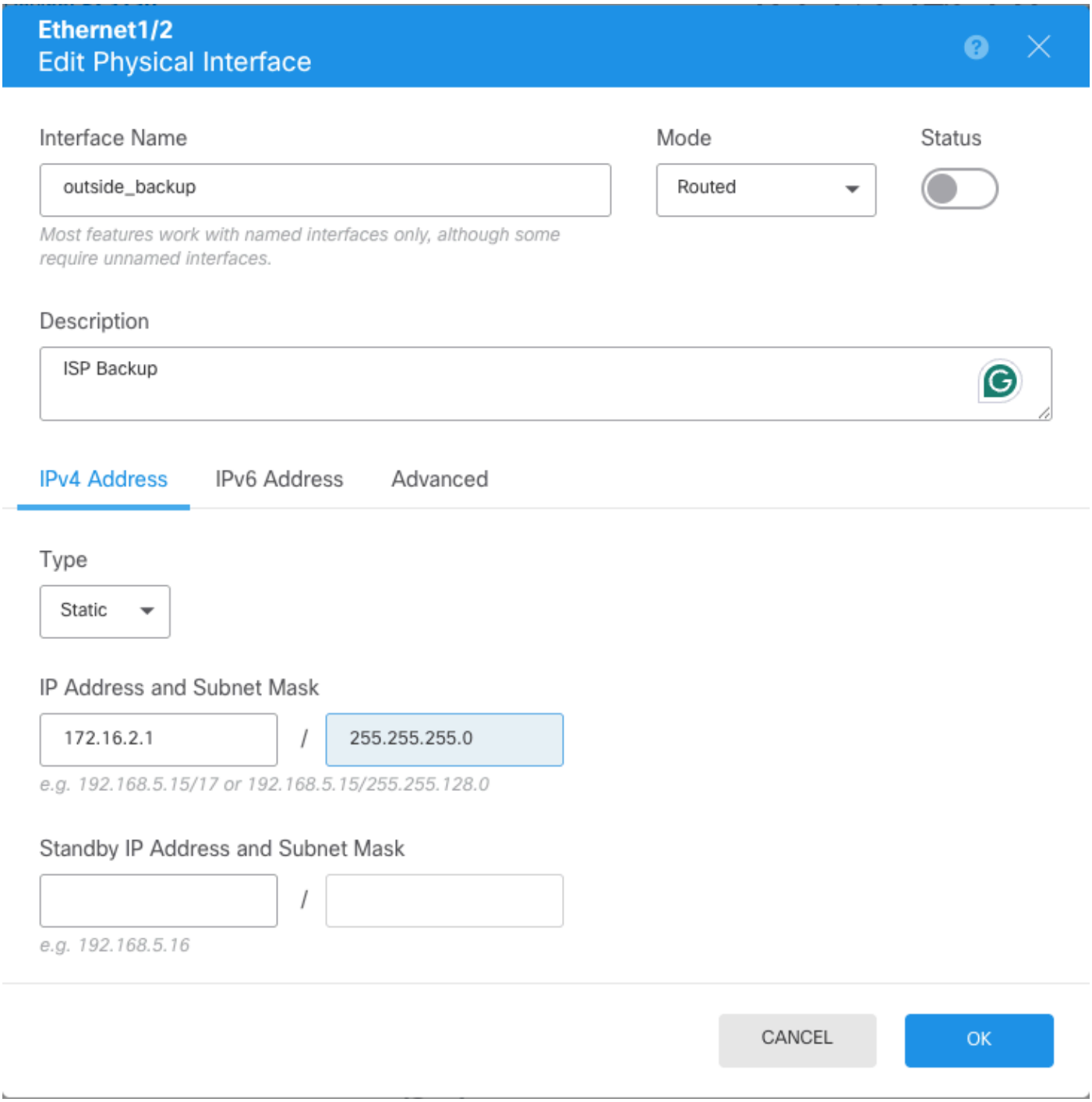
Konfigurieren Sie die Schnittstelle mit den richtigen Parametern für Ihre primäre ISP-Verbindung. In diesem Beispiel ist die Schnittstelle outside_primary.



Konfiguration der primären ISP-Schnittstelle

Schritt 4:

Wiederholen Sie den gleichen Vorgang für die sekundäre ISP-Schnittstelle. In diesem Beispiel wird die Schnittstelle Ethernet1/2 verwendet.

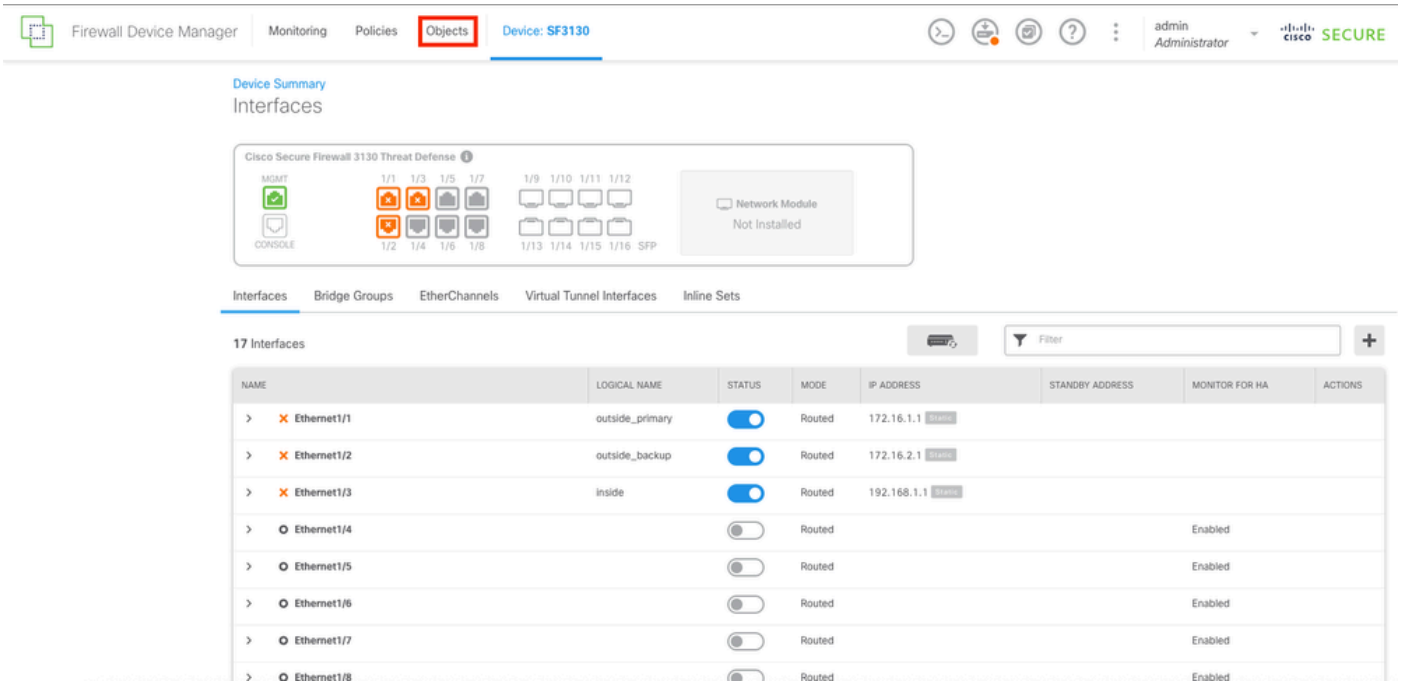


Konfiguration der sekundären ISP-Schnittstelle

Schritt 5:

Nach der Konfiguration der beiden Schnittstellen für die ISPs besteht der nächste Schritt darin, den SLA-Monitor für die primäre Schnittstelle einzurichten.

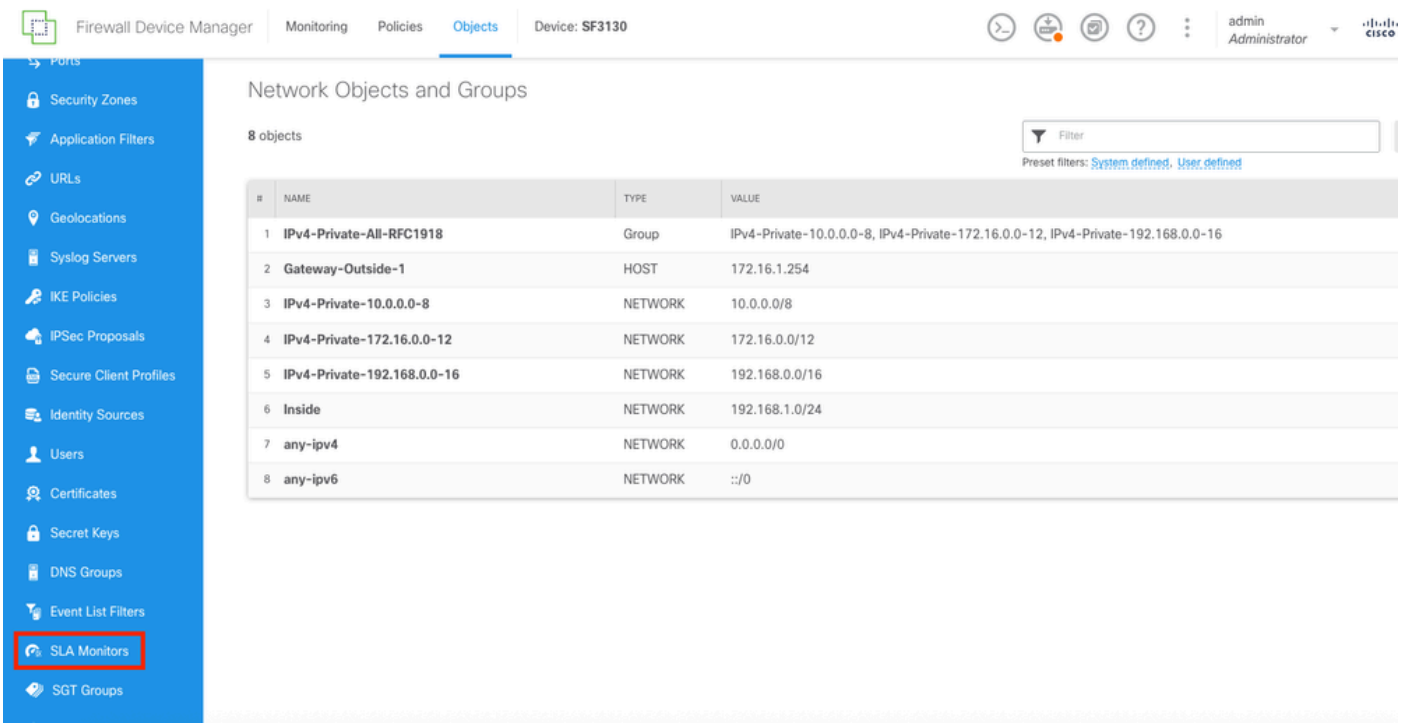
Navigieren Sie zum Abschnitt Objekte, indem Sie die Schaltfläche Objekte oben im Menü auswählen.



Konfigurierte Schnittstellen

Schritt 6:

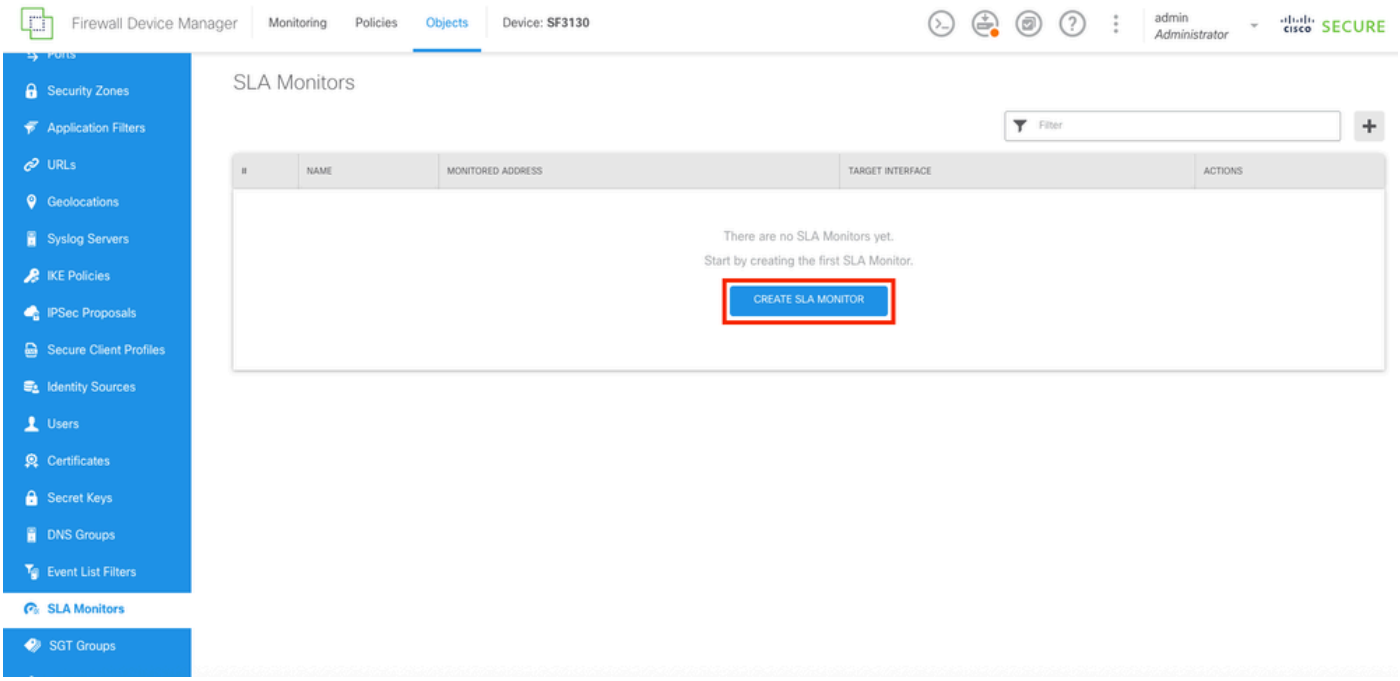
Wählen Sie in der linken Spalte die Schaltfläche SLA Monitors aus.



Bildschirm "Objekte"

Schritt 7.

Erstellen Sie einen neuen SLA-Monitor, indem Sie auf die Schaltfläche SLA-Monitor erstellen klicken.



Abschnitt SLA-Monitor

Schritt 8:

Konfigurieren Sie die Parameter für die primäre ISP-Verbindung.

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

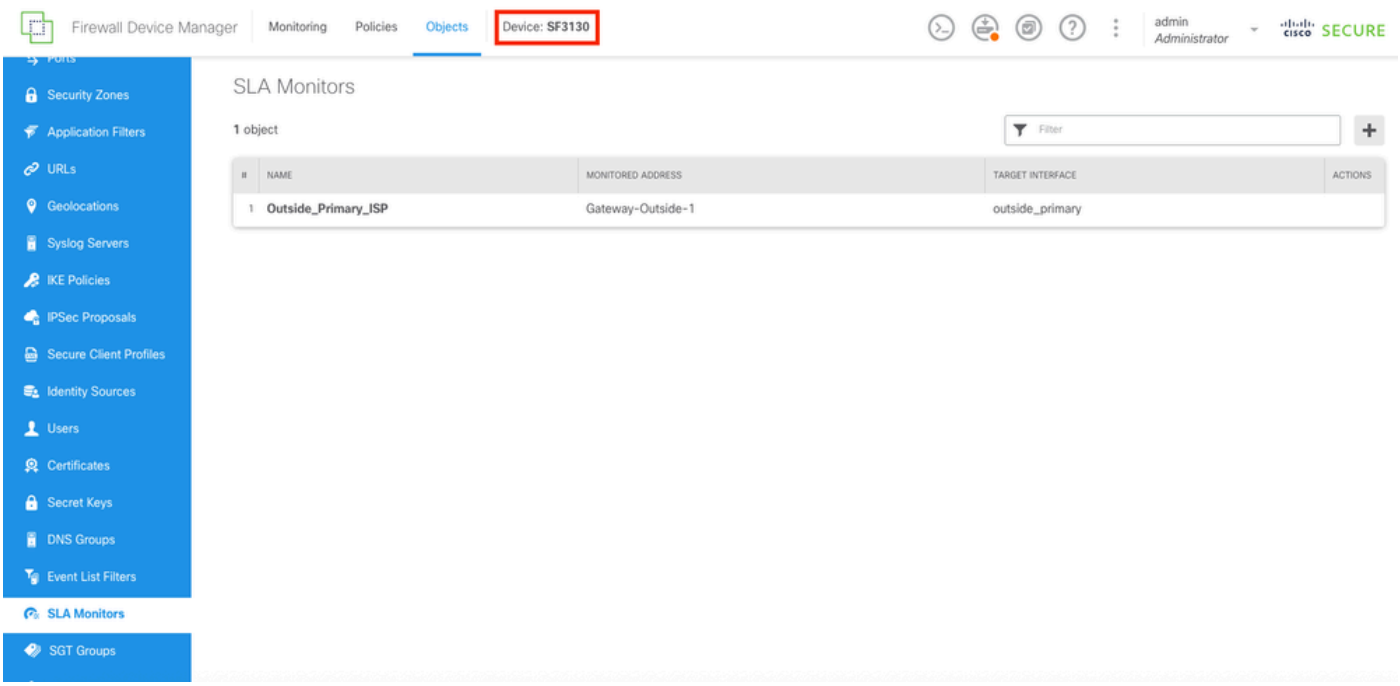
28 bytes

0 - 16384

CANCEL OK

Schritt 9.

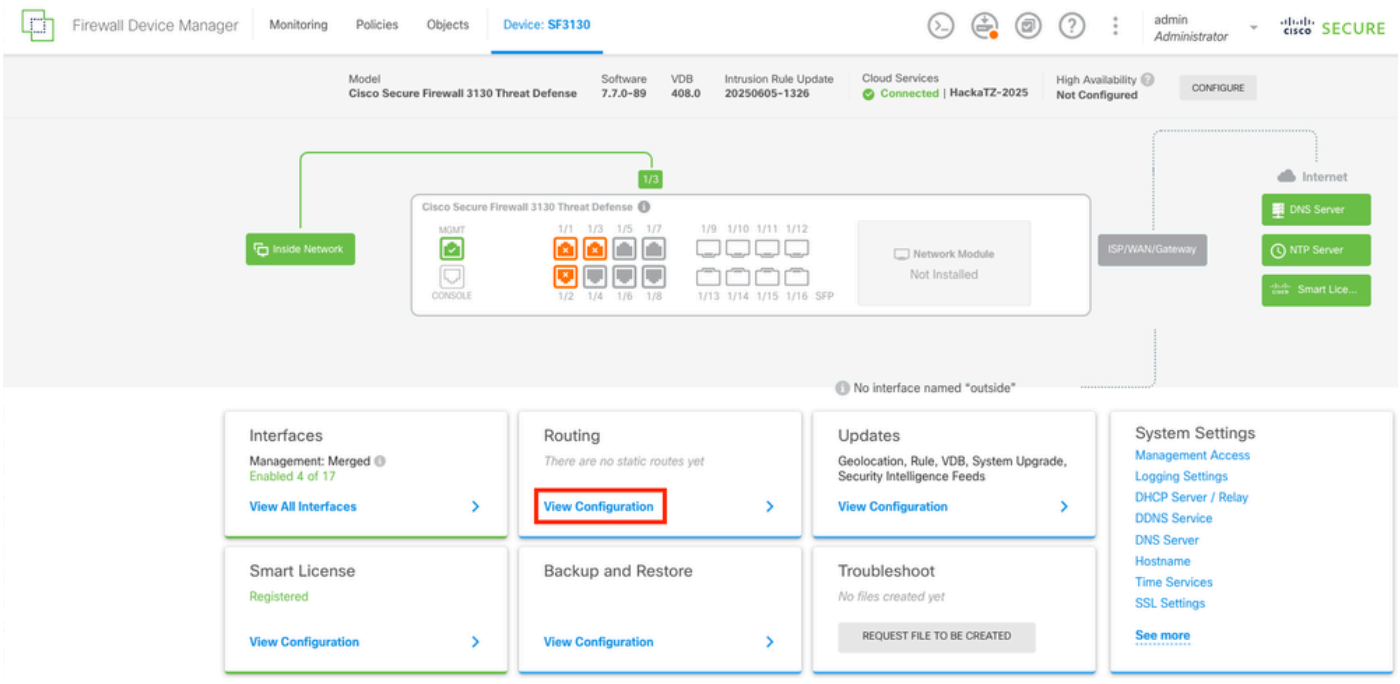
Nachdem das Objekt erstellt wurde, muss es von der statischen Route für die Schnittstellen erstellt werden. Navigieren Sie zum Haupt-Dashboard, indem Sie auf die Schaltfläche Device (Gerät) klicken.



SLA-Monitor erstellt

Schritt 10.

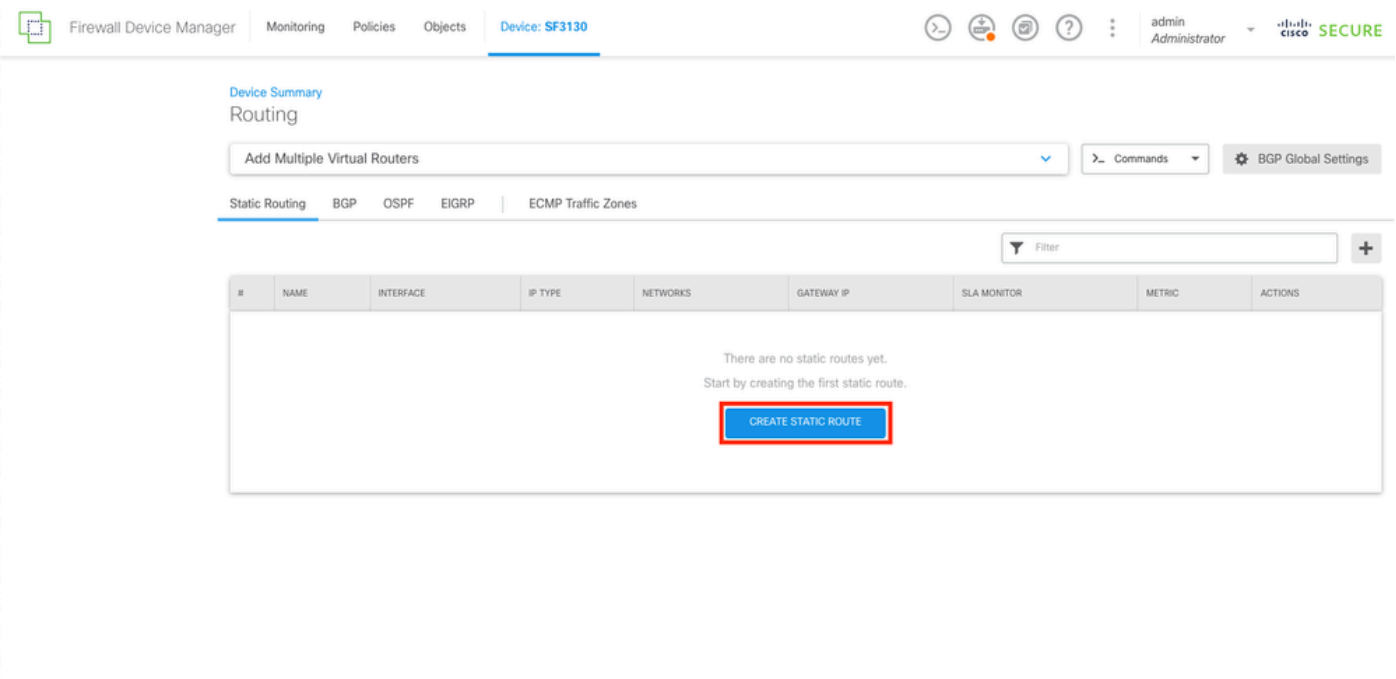
Navigieren Sie zum Abschnitt Routing, indem Sie im Routing-Bereich die Option View Configuration (Konfiguration anzeigen) auswählen.



Haupt-Dashboard

Schritt 11.

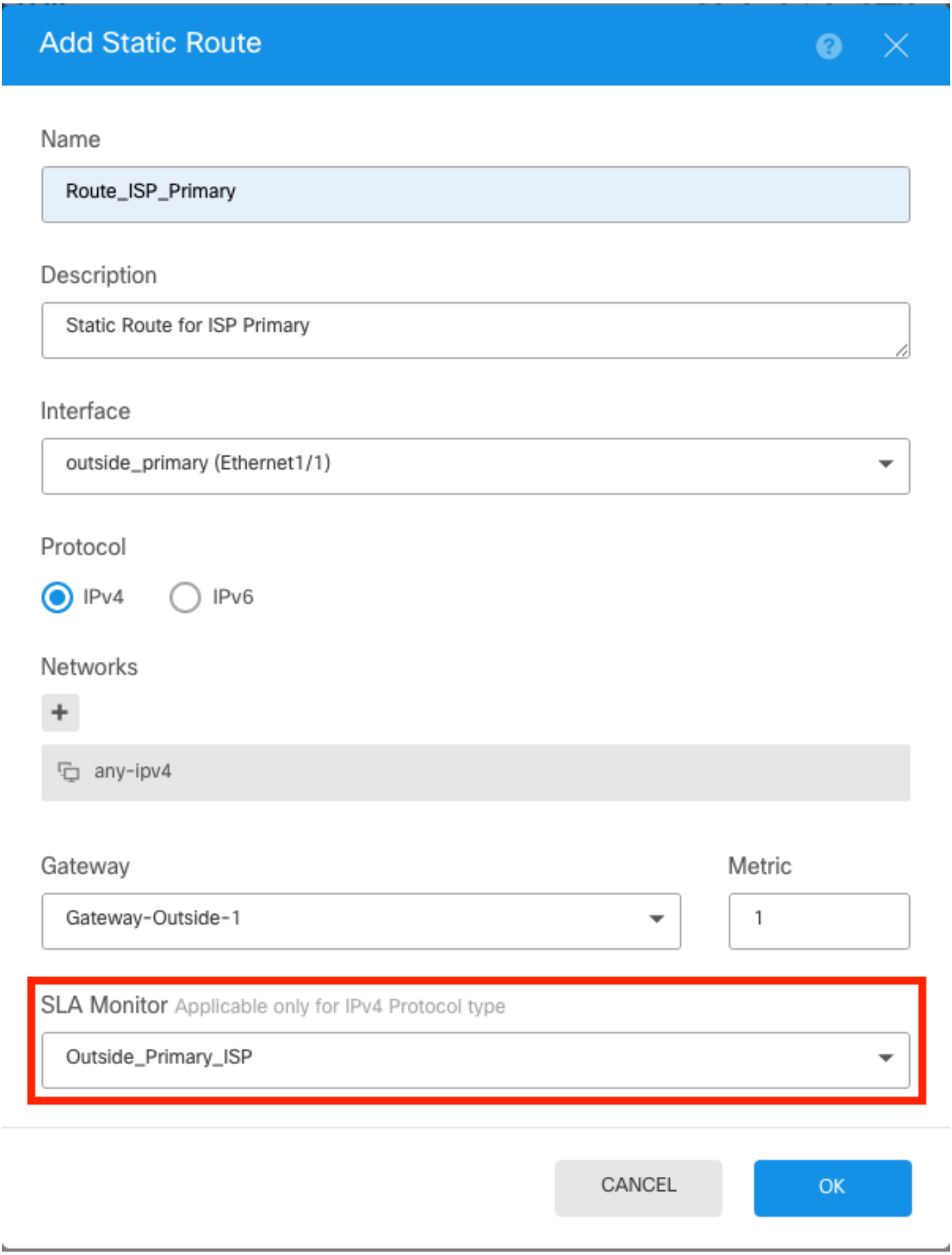
Erstellen Sie auf der Registerkarte Static Routing (Statisches Routing) die beiden statischen Standardrouten für beide ISPs. Um eine neue statische Route zu erstellen, wählen Sie die Schaltfläche STATISCHE Route ERSTELLEN.



Abschnitt für statisches Routing

Schritt 12:

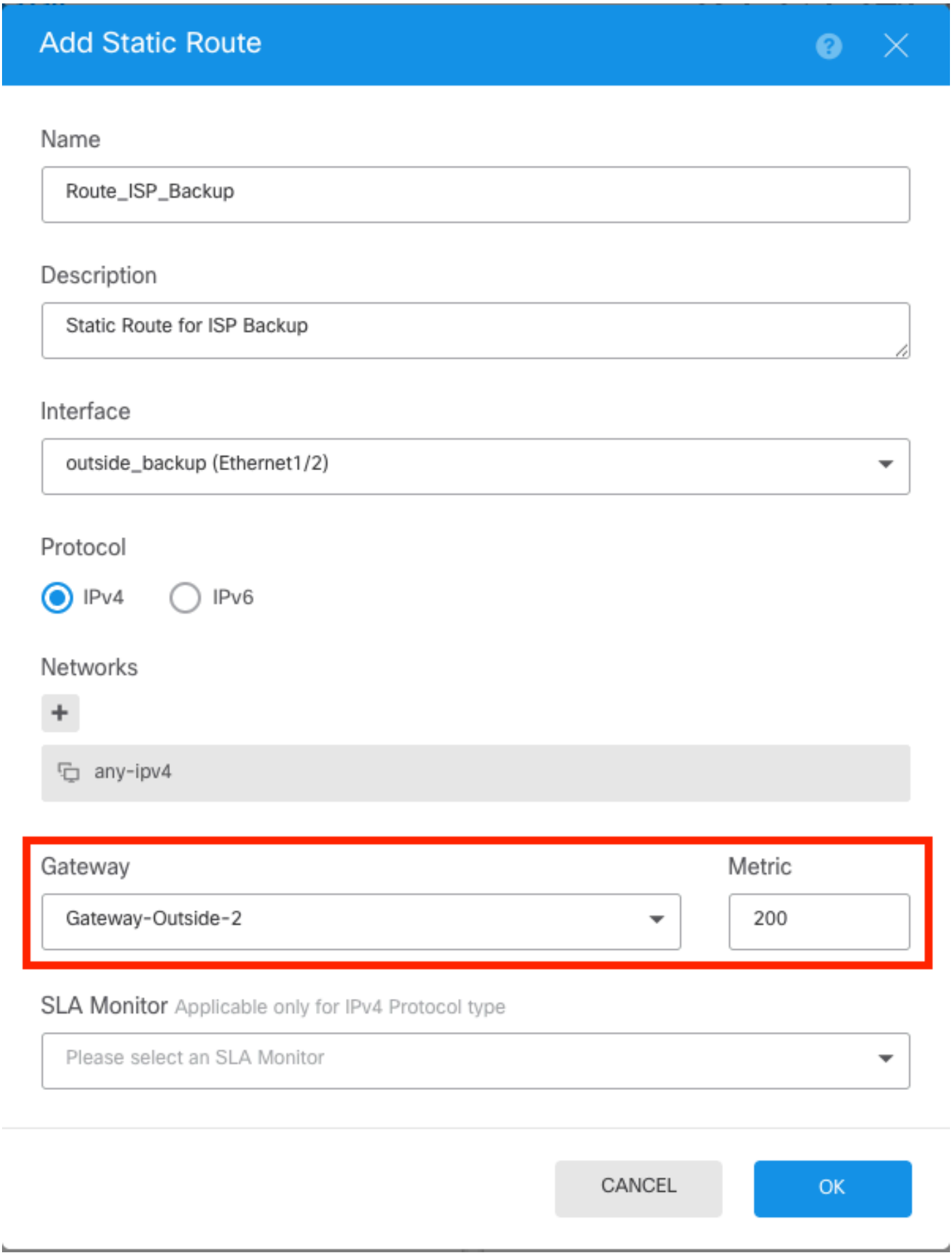
Erstellen Sie zunächst die statische Route für den primären ISP. Fügen Sie am Ende das SLA-Überwachungsobjekt hinzu, das im letzten Schritt erstellt wurde.



Statische Route für primären ISP

Schritt 13:

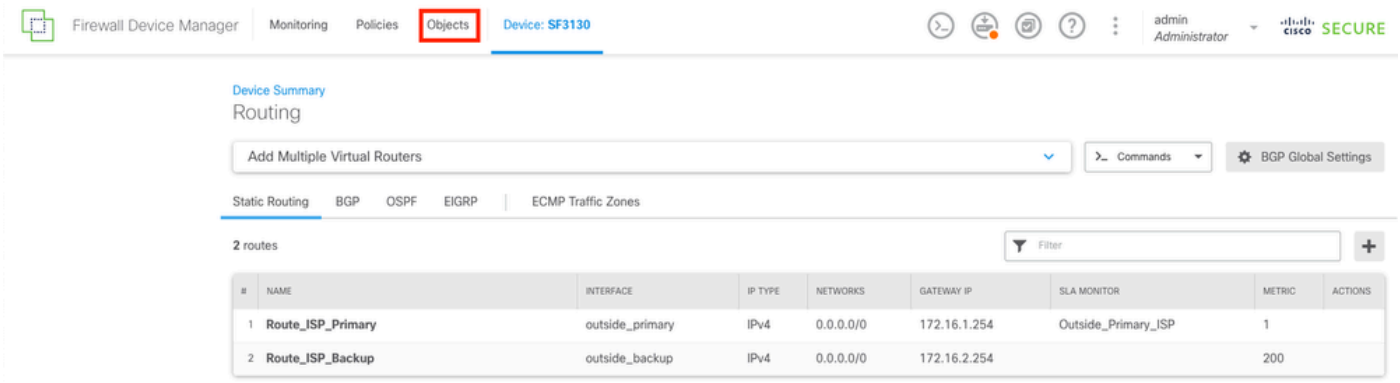
Wiederholen Sie den letzten Schritt, und erstellen Sie eine Standardroute für den sekundären ISP mit dem richtigen Gateway und einer anderen Metrik. In diesem Beispiel wurde sie auf 200 erhöht.



Statische Route für sekundären ISP

Schritt 14:

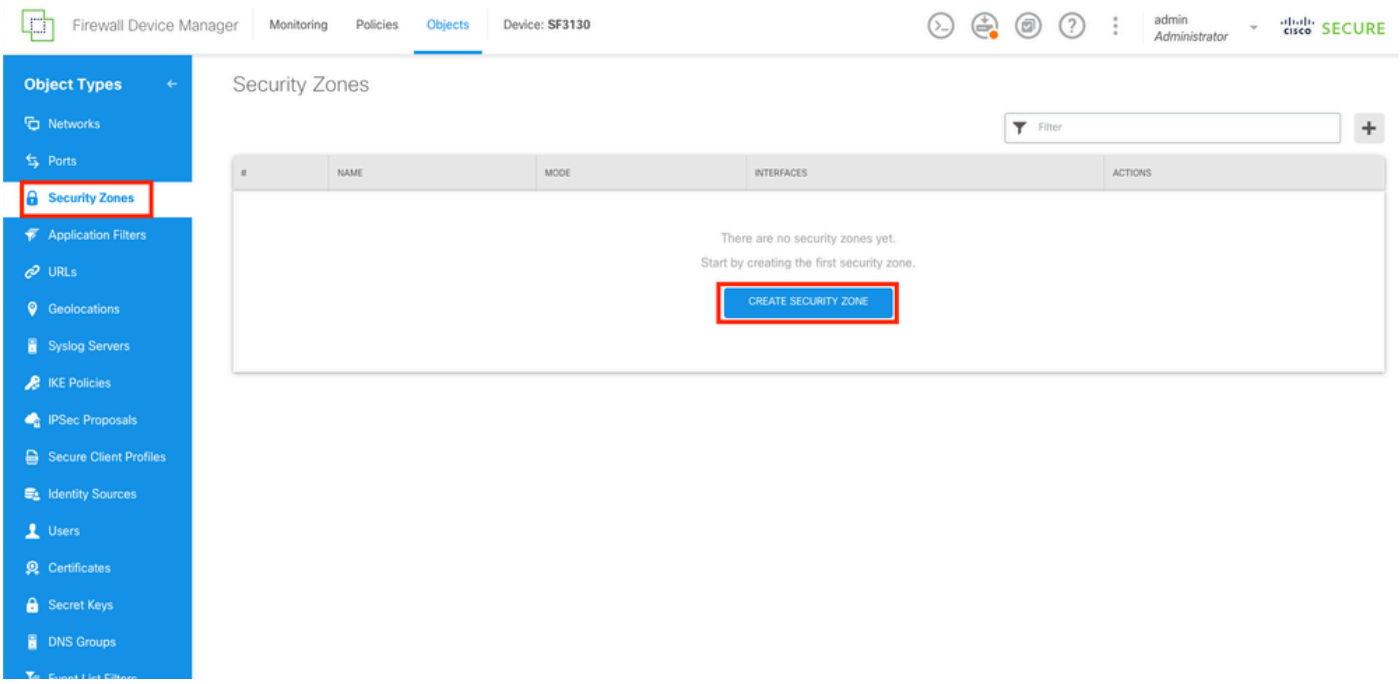
Nachdem beide statischen Routen erstellt wurden, muss eine Sicherheitszone erstellt werden. Navigieren Sie zum Abschnitt Objekte, indem Sie oben auf die Schaltfläche Objekte klicken.



Statische Routen erstellt

Schritt 15:

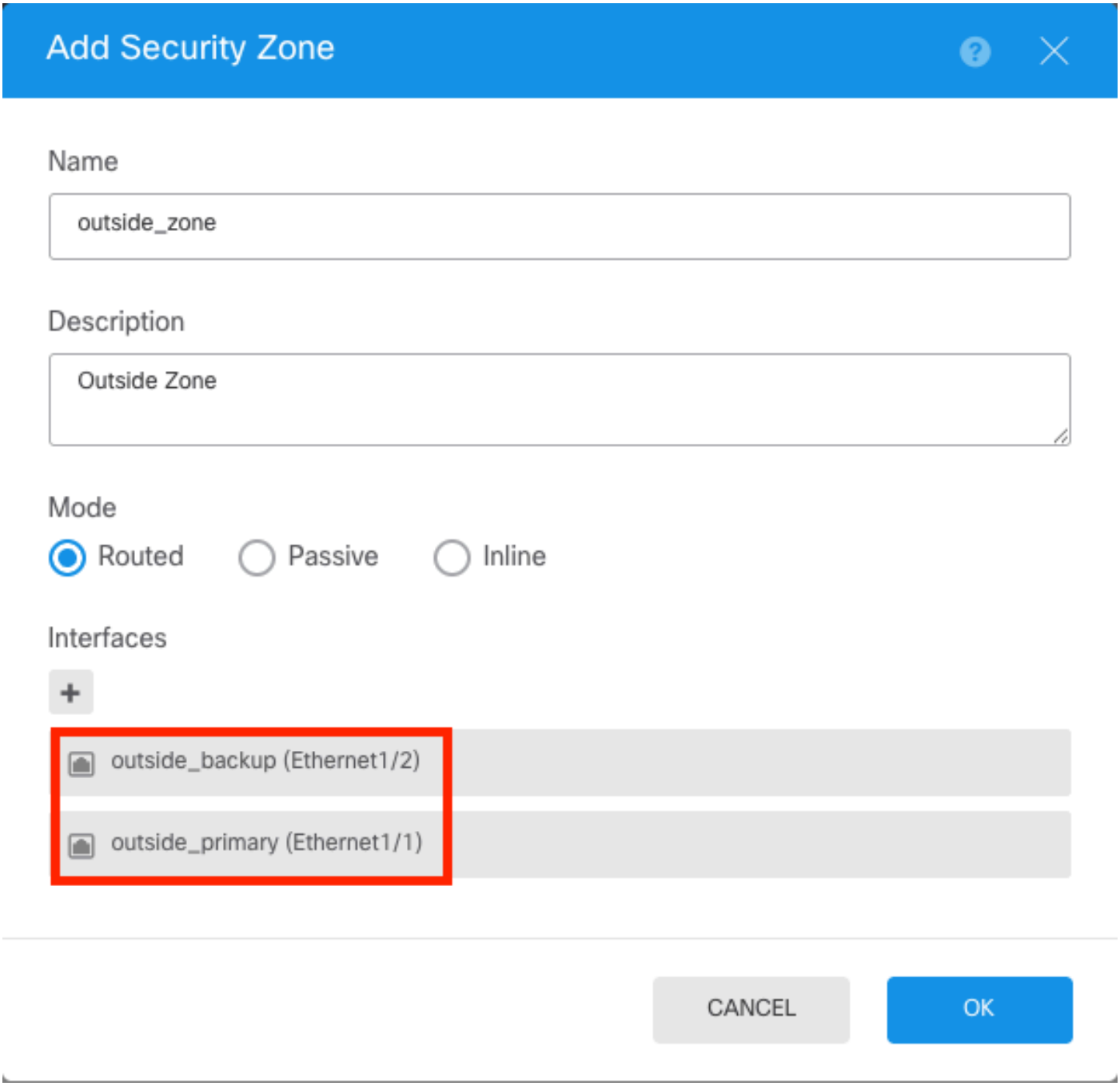
Navigieren Sie zum Abschnitt Sicherheitszonen, indem Sie in der linken Spalte die Schaltfläche Sicherheitszonen auswählen. Erstellen Sie dann eine neue Zone, indem Sie die Schaltfläche SICHERHEITSZONE ERSTELLEN auswählen.



Abschnitt "Sicherheitszonen"

Schritt 16:

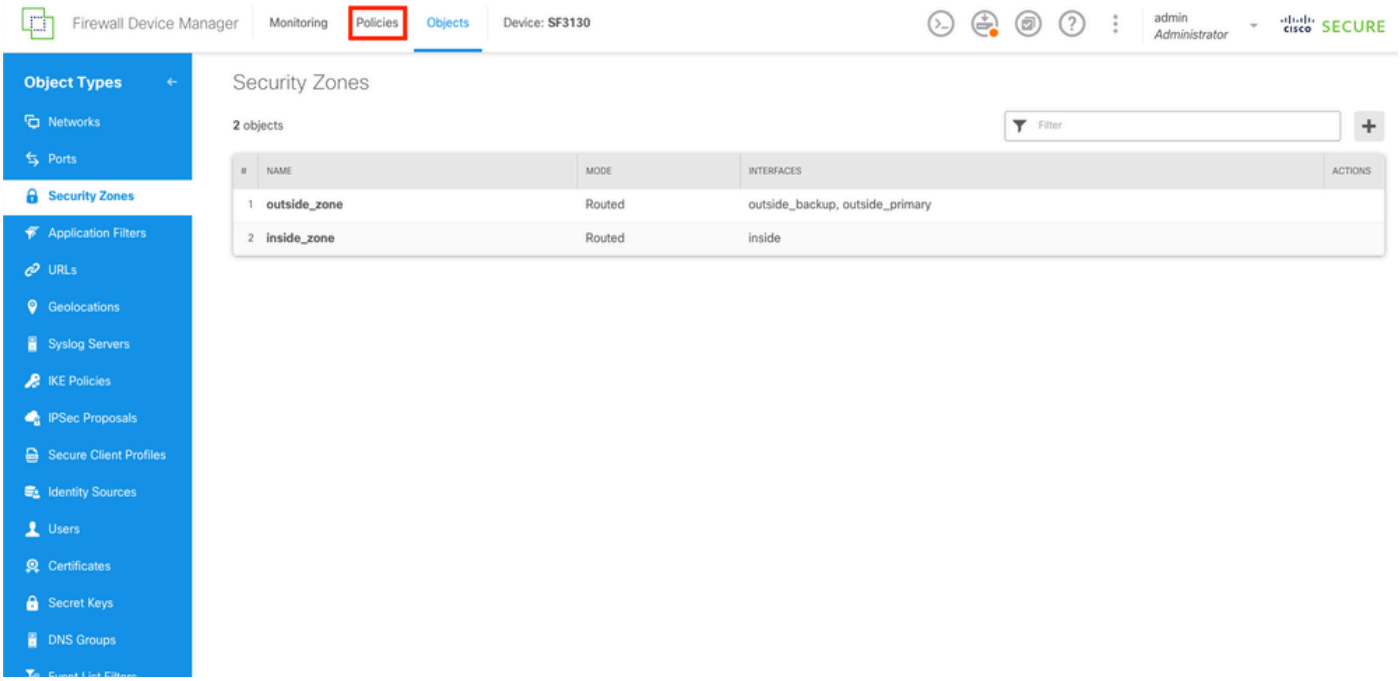
Erstellen Sie die externe Sicherheitszone mit den beiden externen Schnittstellen für die ISP-Verbindungen.



Sicherheitszone außerhalb

Schritt 17:

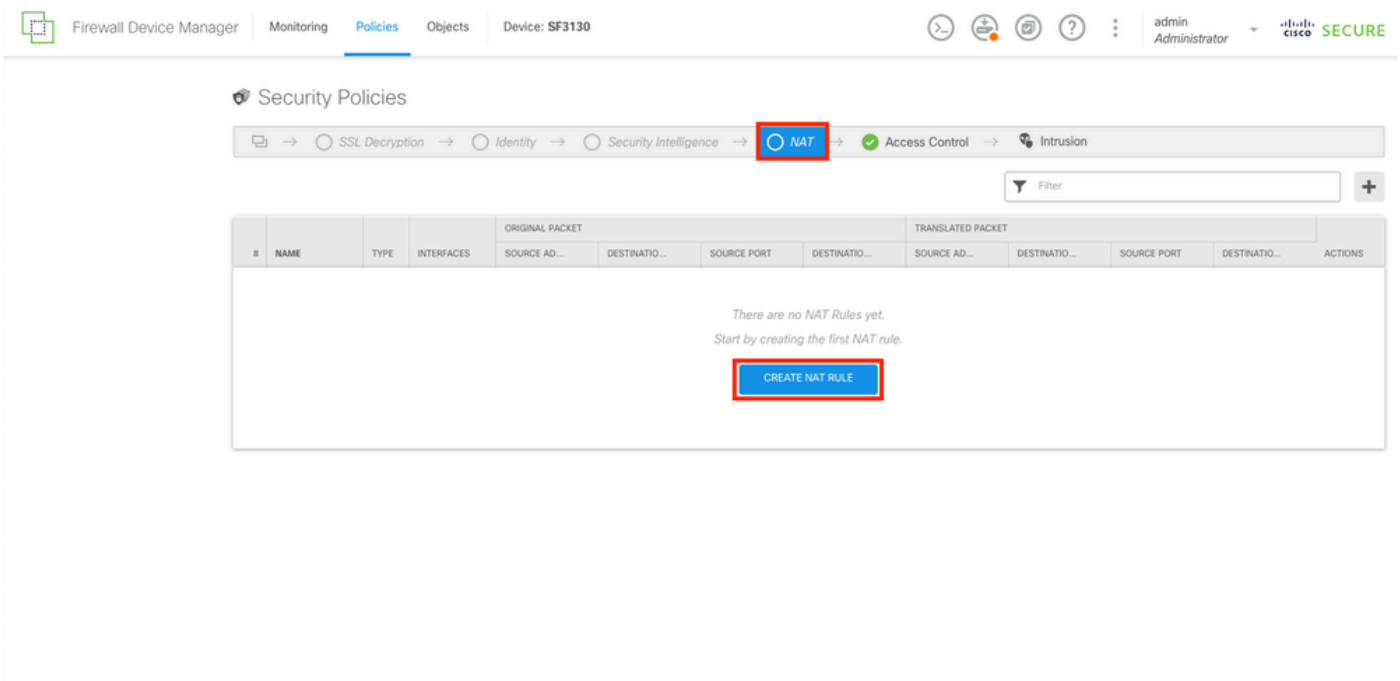
Nachdem die Sicherheitszone erstellt wurde, muss eine NAT erstellt werden. Navigieren Sie zum Abschnitt Policies (Richtlinien), indem Sie oben auf die Schaltfläche Policies (Richtlinien) klicken.



Sicherheitszonen erstellt

Schritt 18:

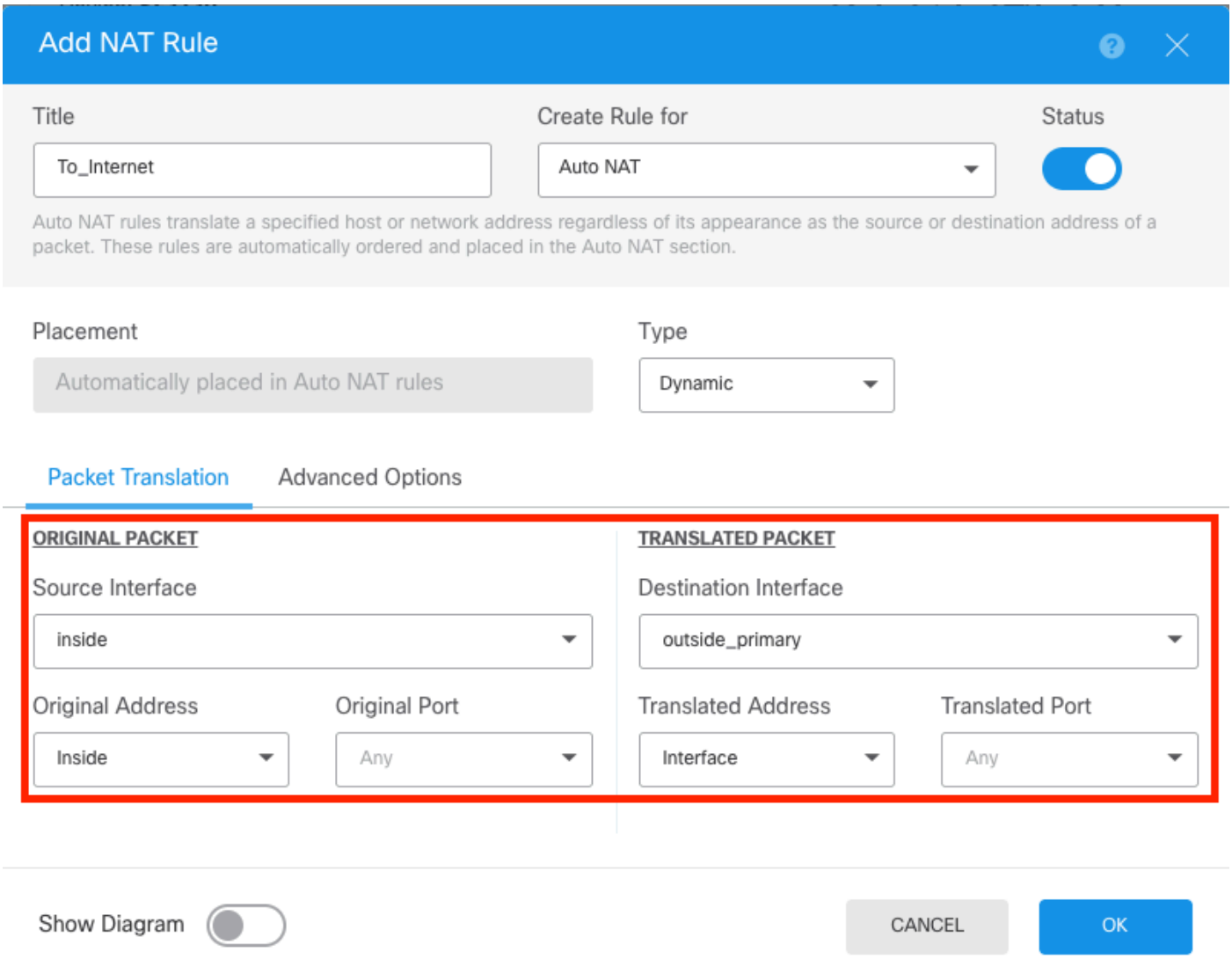
Navigieren Sie zum Abschnitt NAT, indem Sie die Schaltfläche NAT auswählen, und erstellen Sie dann eine neue Regel, indem Sie die Schaltfläche CREATE NAT RULE (NAT-REGEL ERSTELLEN) auswählen.



NAT-Abschnitt

Schritt 19:

Für den ISP-Failover muss die Konfiguration über zwei Routen über externe Schnittstellen verfügen. Zunächst für die primäre externe Schnittstellenverbindung zum primären ISP.

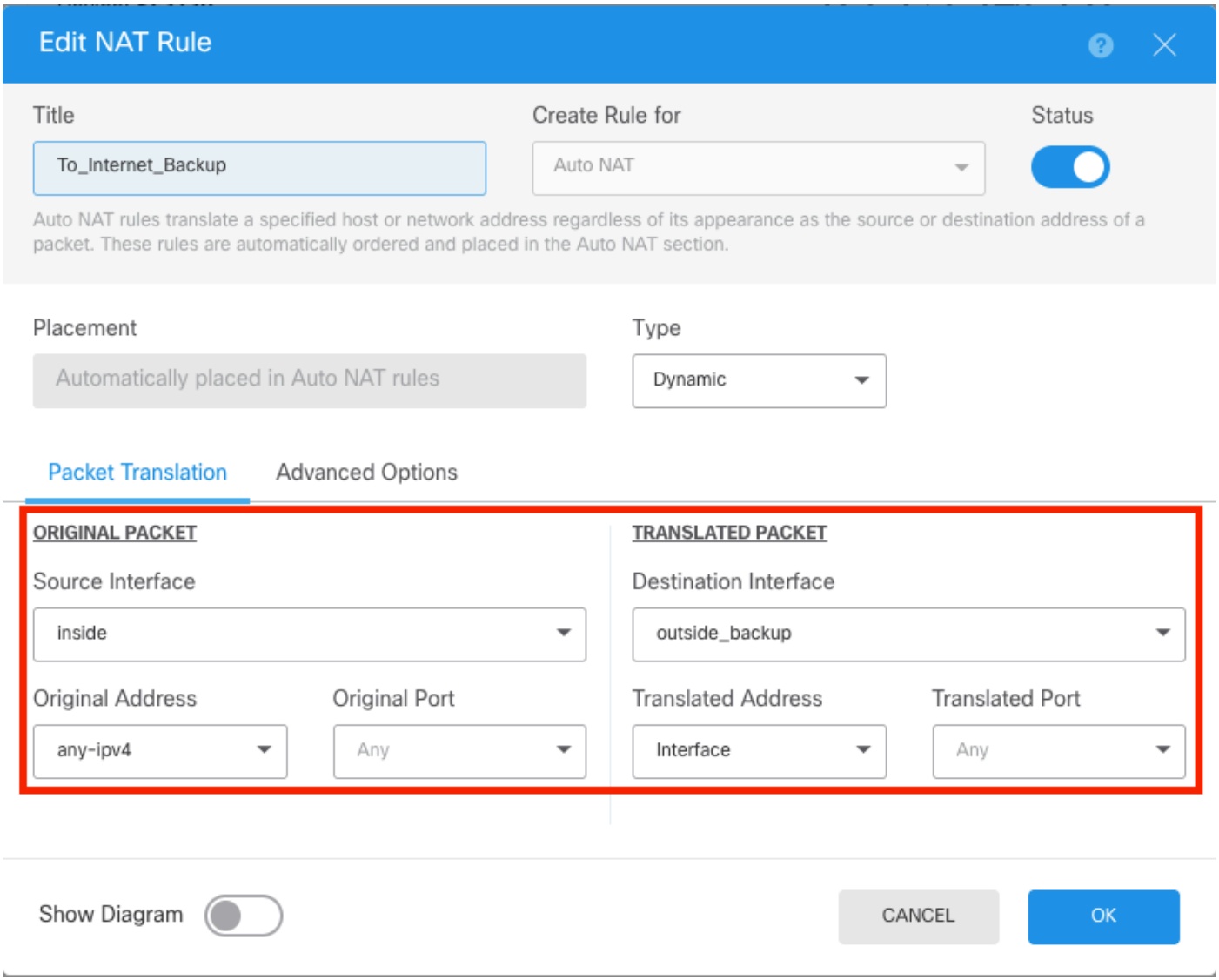


NAT für primären ISP

Schritt 20:

Nun eine zweite NAT für die sekundäre ISP-Verbindung.

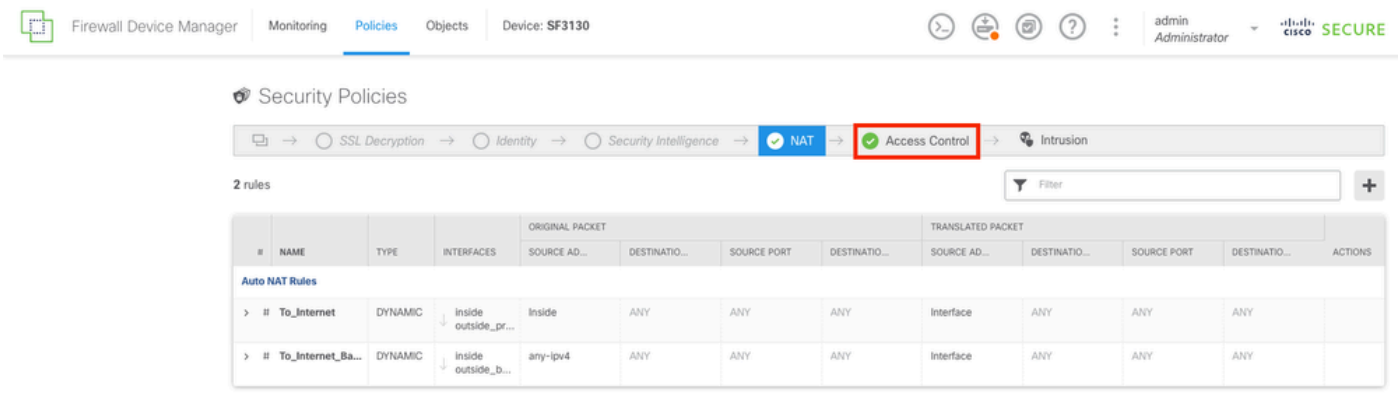
Anmerkung: Für die ursprüngliche Adresse kann nicht dasselbe Netzwerk verwendet werden. In diesem Beispiel ist die ursprüngliche Adresse für den sekundären ISP das Objekt any-ipv4.



NAT für sekundären ISP

Schritt 21:

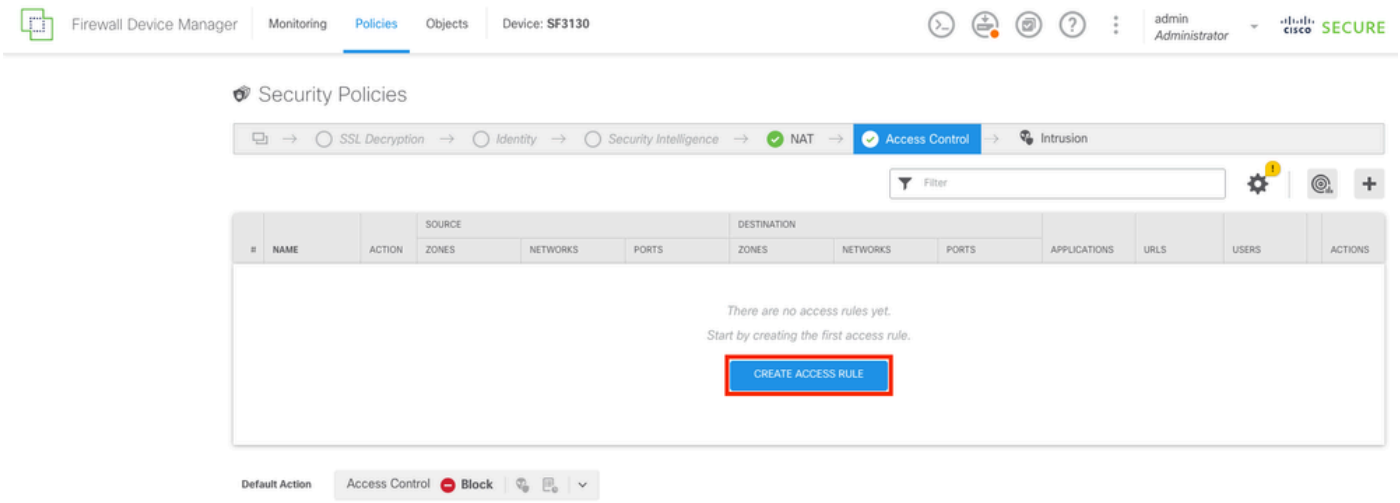
Nachdem beide NAT-Regeln erstellt wurden, muss eine Zugriffskontrollregel eingerichtet werden, die ausgehenden Verkehr zulässt. Wählen Sie die Schaltfläche Zugriffskontrolle aus.



NAT-Regeln erstellt

Schritt 22:

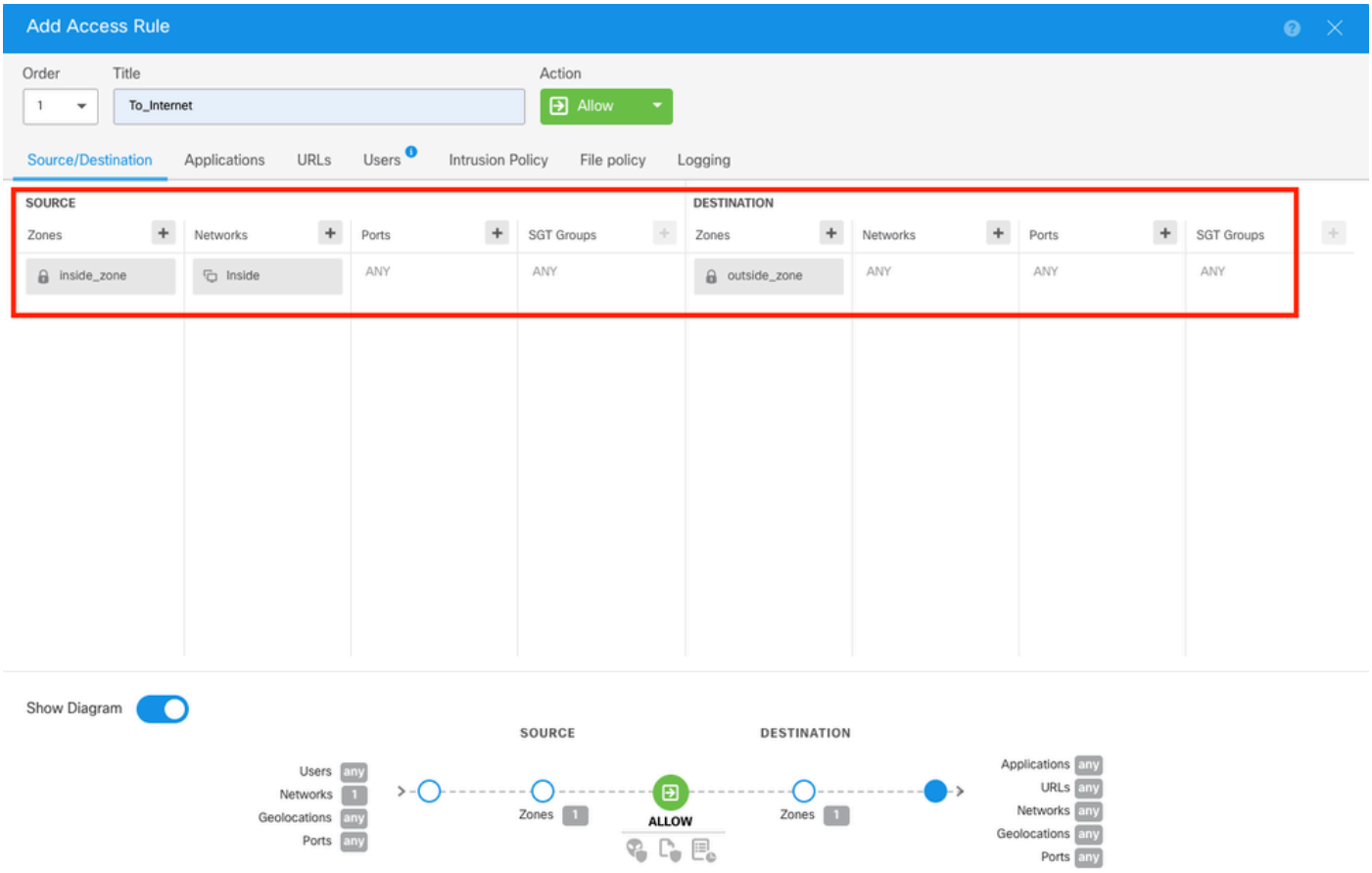
Wählen Sie zum Erstellen der Zugriffskontrollregel die Schaltfläche ZUGRIFFSREGEL ERSTELLEN.



Abschnitt "Zugriffskontrolle"

Schritt 23:

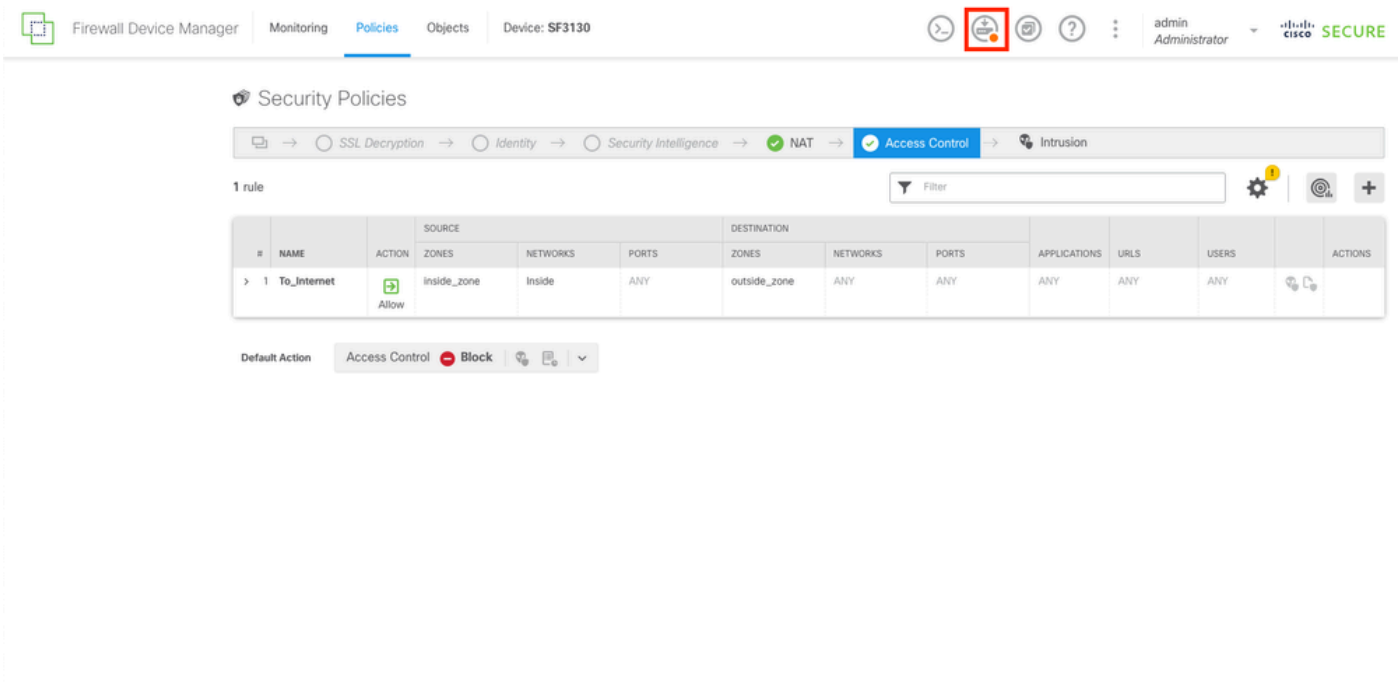
Wählen Sie die gewünschten Zonen und Netzwerke aus.



Zugriffskontrollregel

Schritt 24:

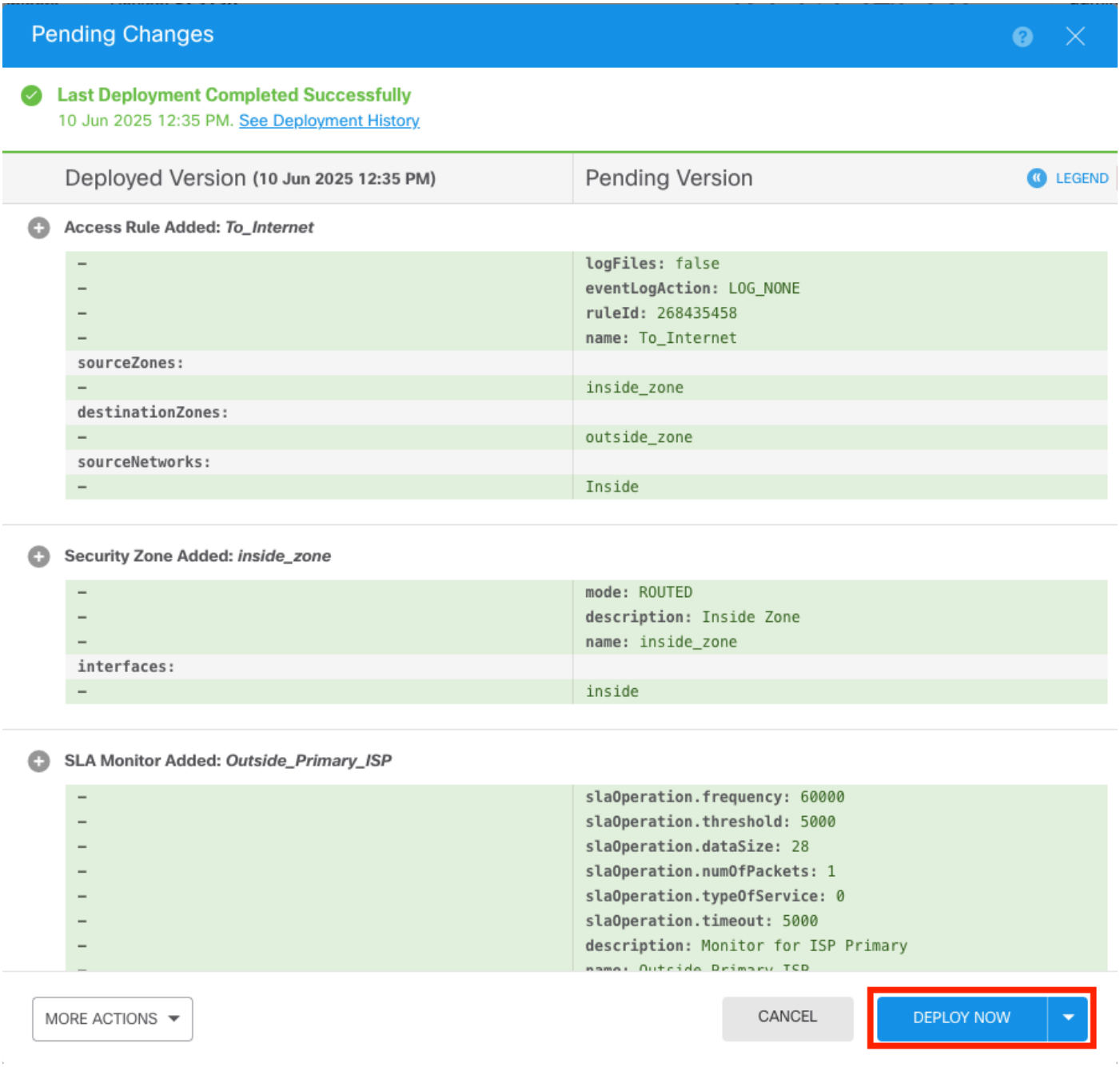
Nachdem die Zugriffskontrollregel erstellt wurde, können Sie mit der Bereitstellung aller Änderungen fortfahren, indem Sie oben auf die Schaltfläche Bereitstellen klicken.



Zugriffskontrollregel erstellt

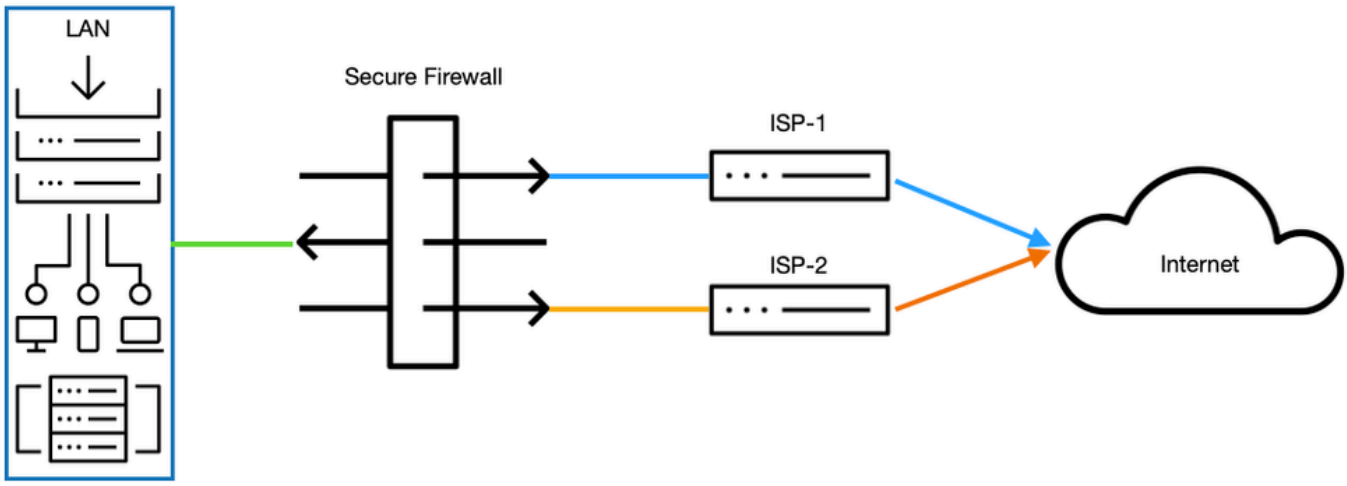
Schritt 25:

Überprüfen Sie die Änderungen, und klicken Sie dann auf die Schaltfläche Jetzt bereitstellen.



Bereitstellungsüberprüfung

Netzwerkdiagramm



Netzwerkdiagramm

Überprüfung

<#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
```

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.