FDMを使用したFTDでのデュアルISPの設定

内容

はじめに

このドキュメントでは、Secure Firewallシリーズのファイアウォールデバイスマネージャ(FDM)を使用して、デュアルインターネットサービスプロバイダー(ISP)フェールオーバーを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 基本的なルーティング
- ファイアウォールデバイスマネージャダッシュボードの知識
- 少なくとも2つのインターネットサービスプロバイダーがセキュアファイアウォールに接続している。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

・ 7.7.X以降のバージョンが稼働するCisco Secure Firewall

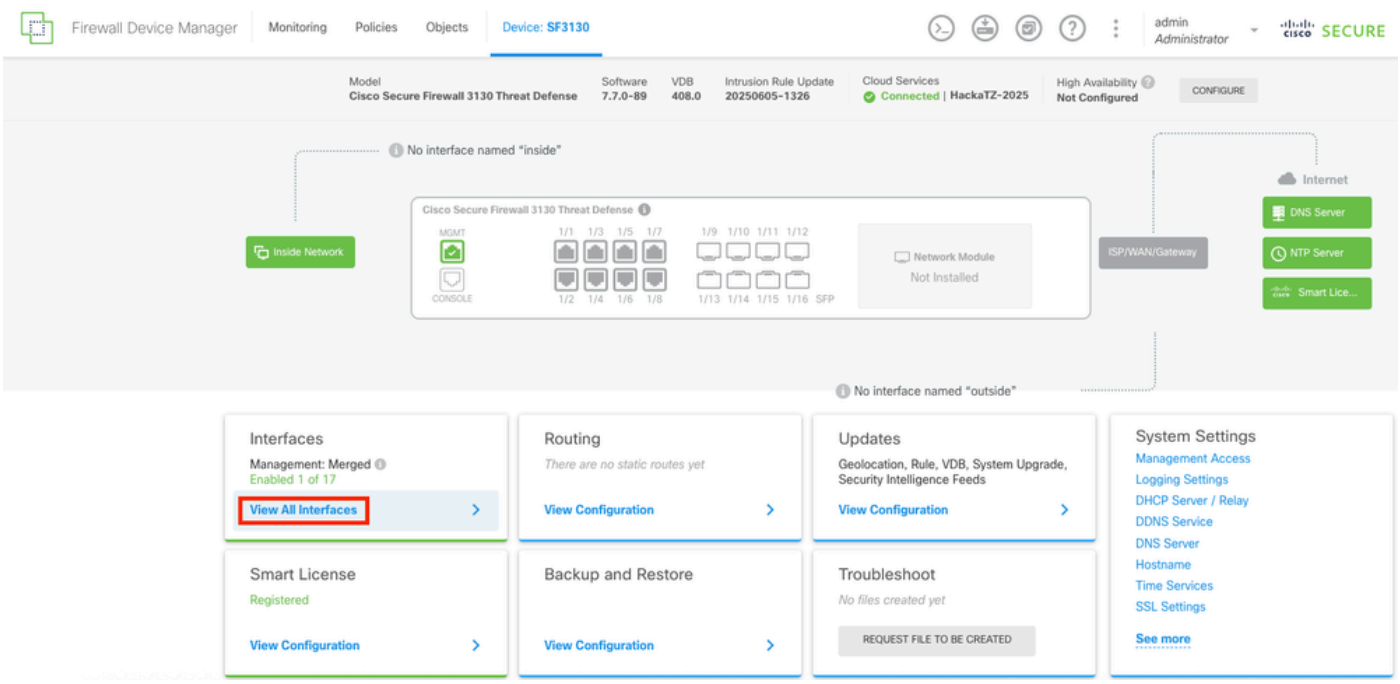
・ 7.7.0バージョンがインストールされたファイアウォール3130を保護します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップ 1：

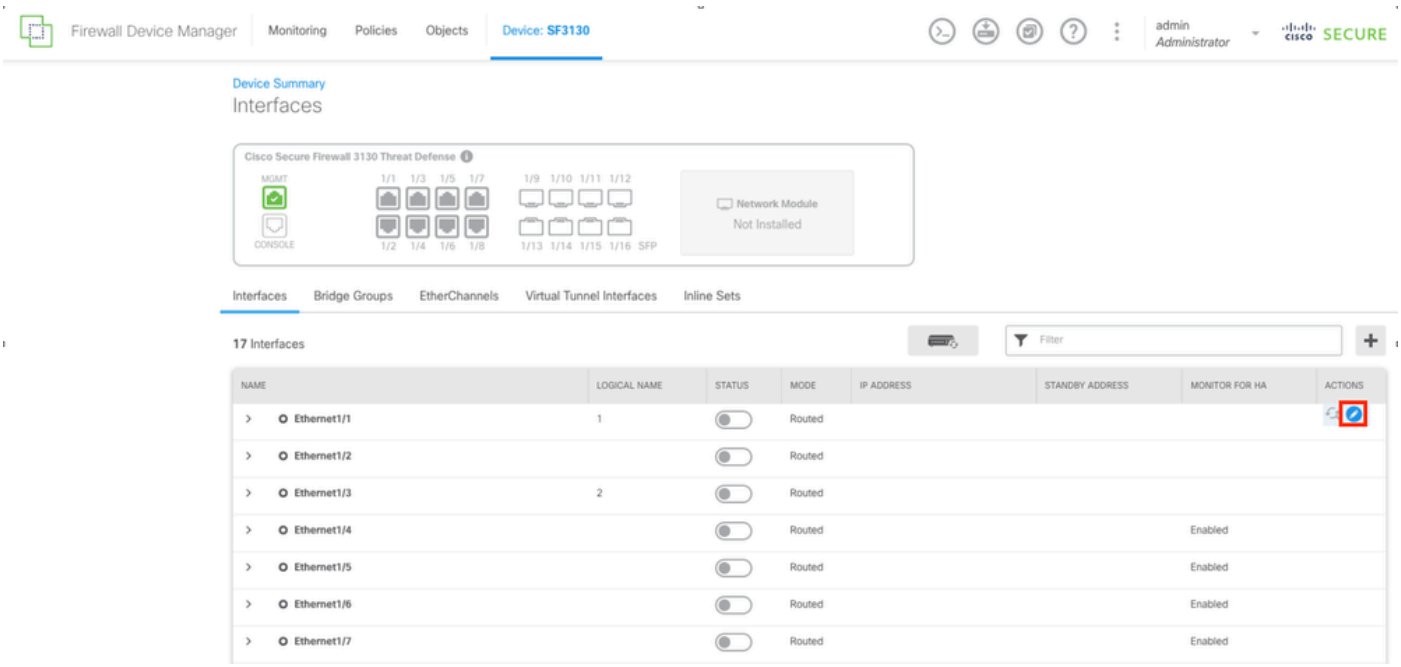
セキュアファイアウォールのFDMにログインし、View All Interfacesボタンを選択してinterfacesセクションに移動します。



FDMメイン・ダッシュボード

ステップ 2：

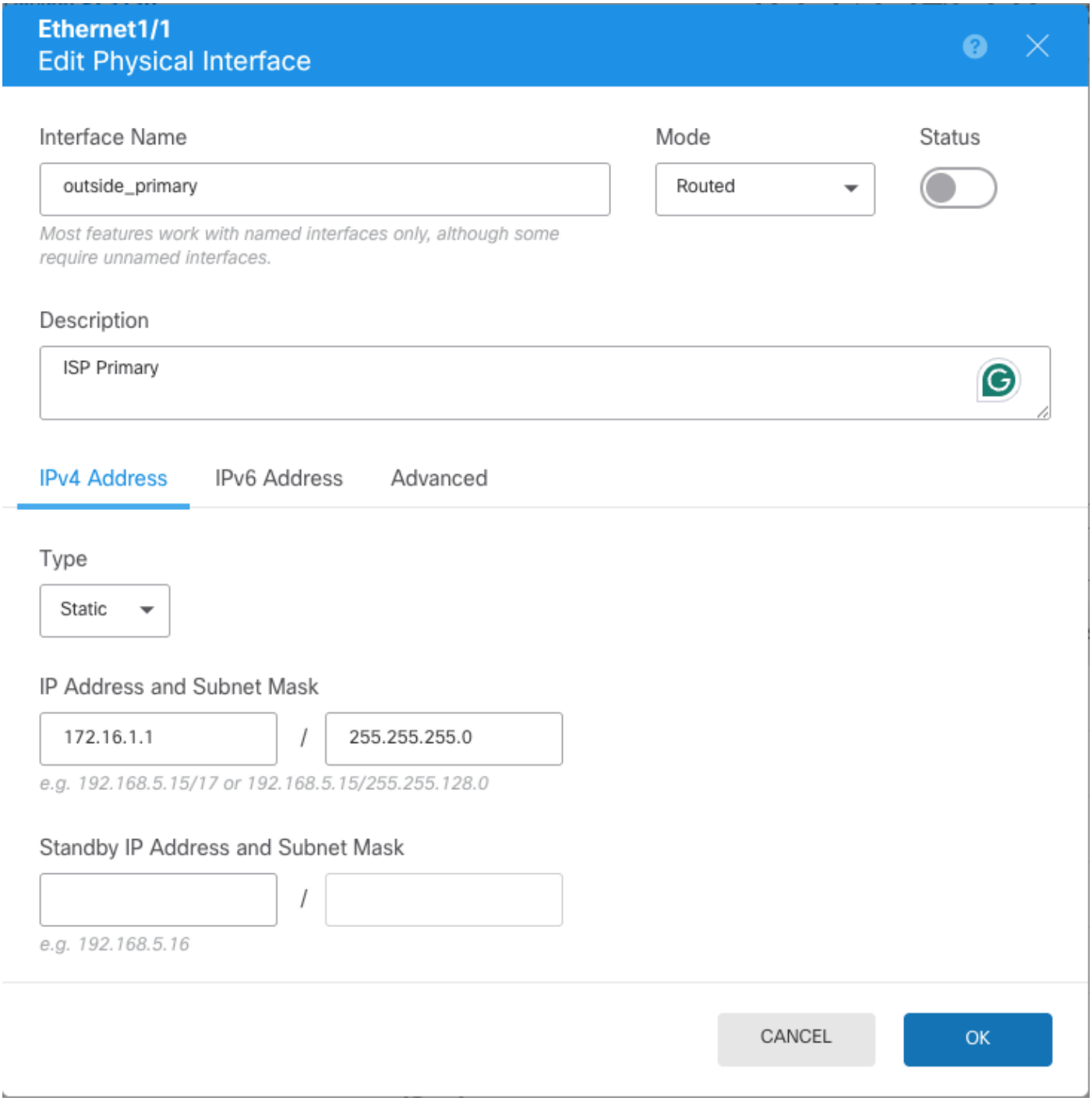
プライマリISP接続のインターフェイスを設定するには、まず目的のインターフェイスを選択します。続行するには、対応するインターフェイスボタンを選択します。この例で使用するインターフェイスはEthernet1/1です。



Interfacesタブ

ステップ 3：

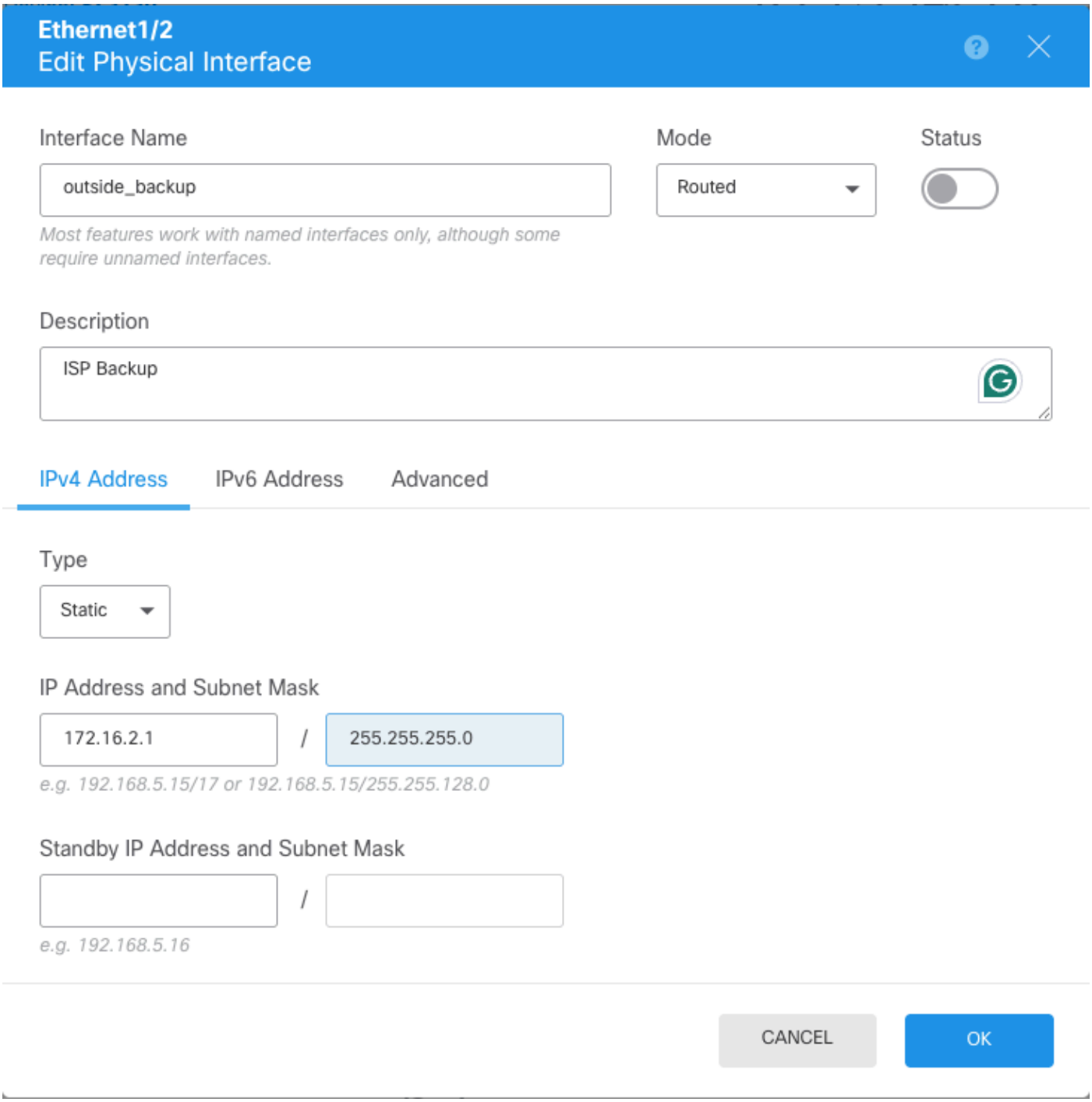
プライマリISP接続の正しいパラメータを使用してインターフェイスを設定します。この例では、インターフェイスはoutside_primaryです。



プライマリISPインターフェイスの設定

ステップ 4：

セカンダリISPインターフェイスに対して同じプロセスを繰り返します。この例では、インターフェイスEthernet1/2が使用されています。

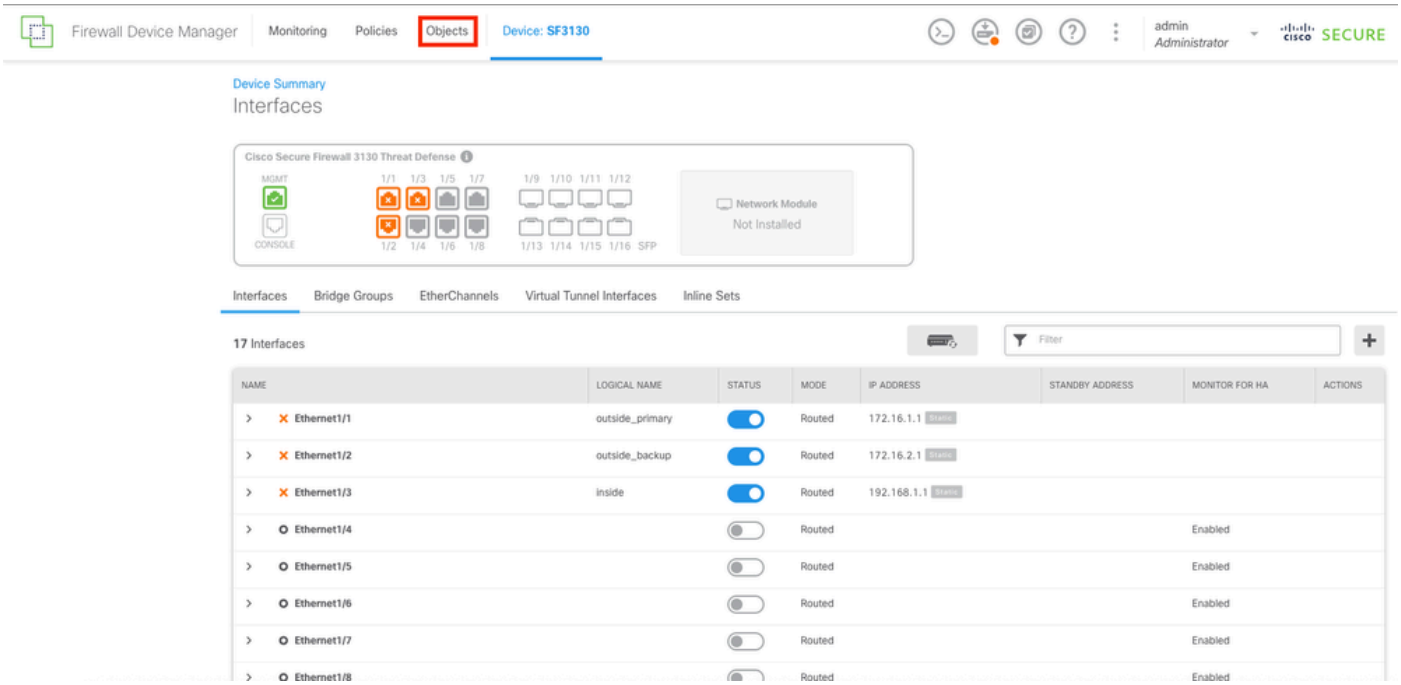


セカンダリISPインターフェイスの設定

ステップ 5：

ISPの2つのインターフェイスを設定した後、次の手順では、プライマリインターフェイスのSLAモニタを設定します。

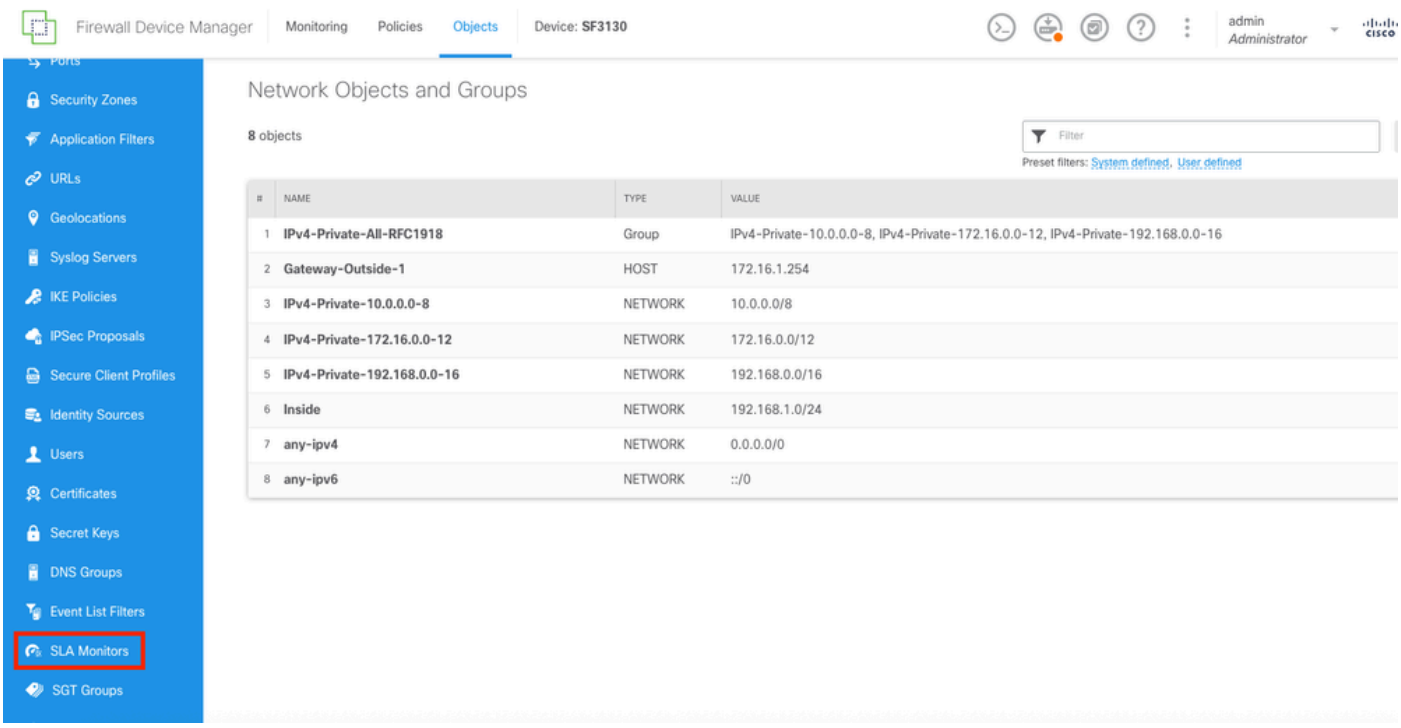
メニューの上部にあるObjectsボタンを選択して、Objectsセクションに移動します。



設定されたインターフェイス

手順 6：

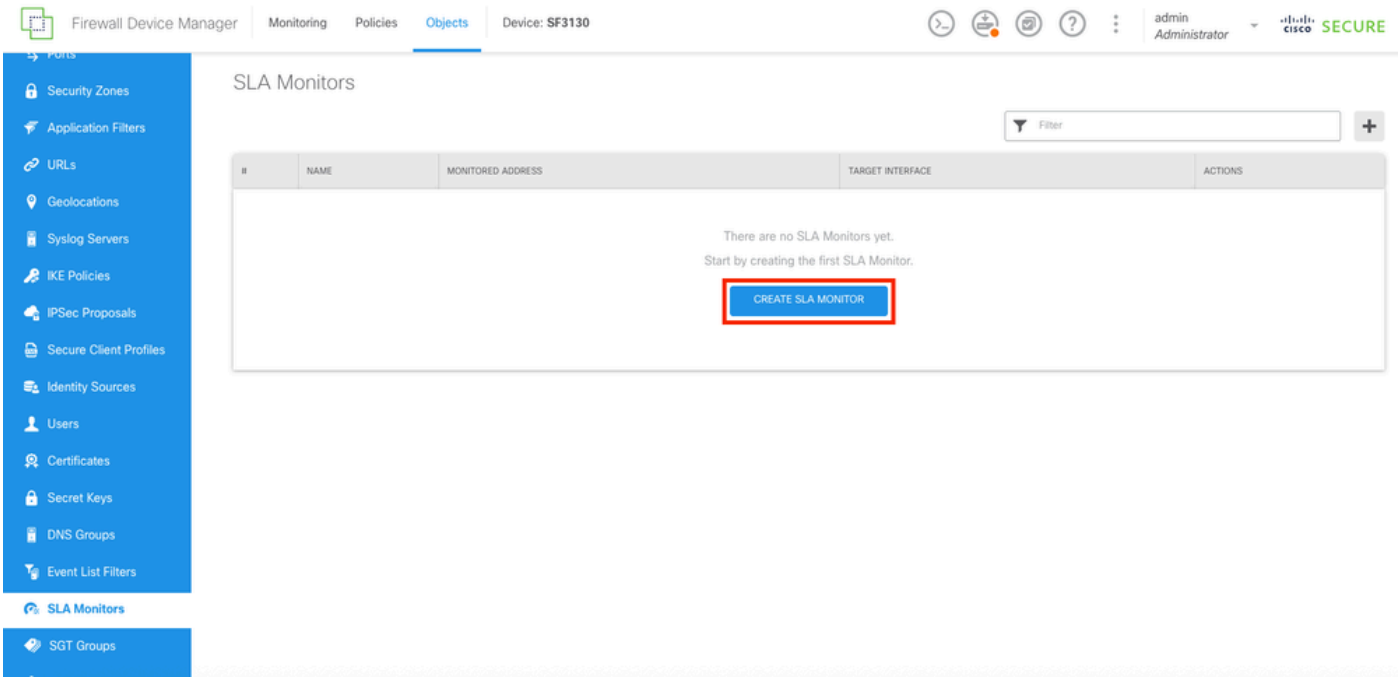
左側の列でSLA Monitorsボタンを選択します。



Objects画面

手順 7：

Create SLA Monitorボタンを選択して、新しいSLAモニタを作成します。



SLA Monitorセクション

ステップ 8：

プライマリISP接続のパラメータを設定します。

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

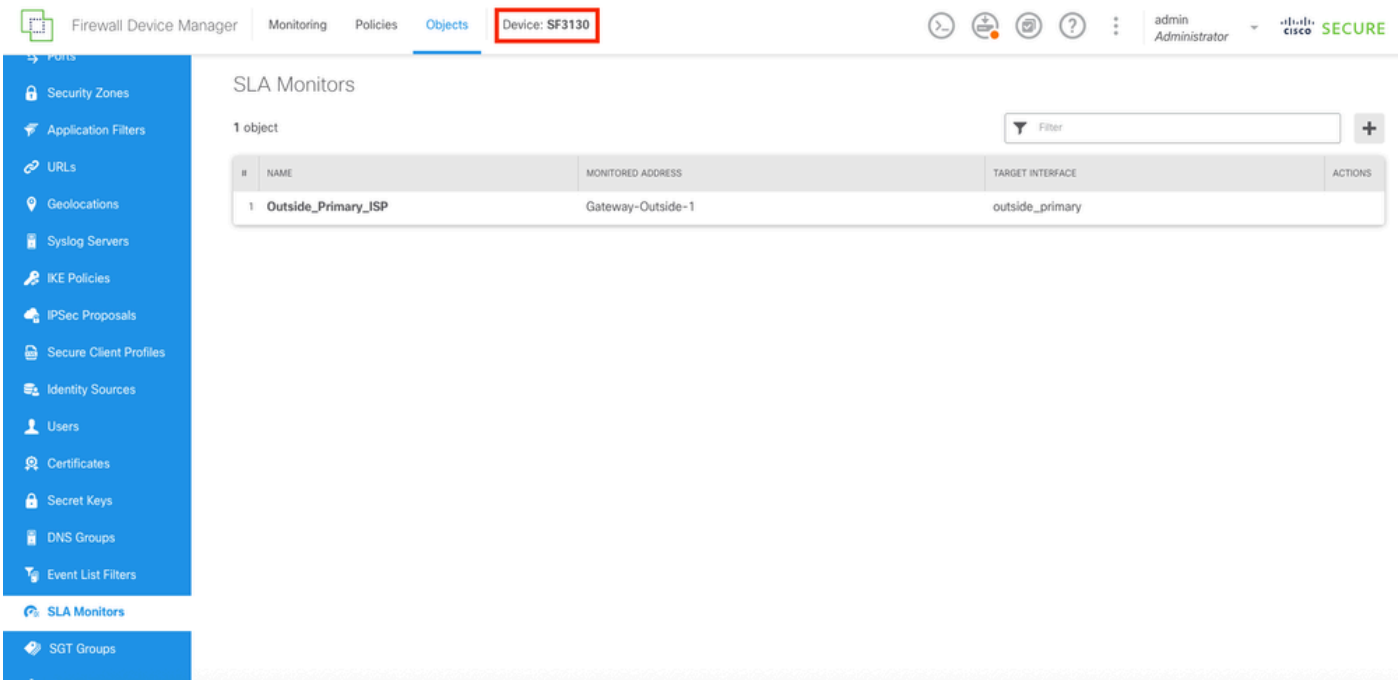
0 - 16384

CANCEL OK

SLAオブジェクトの作成

ステップ 9：

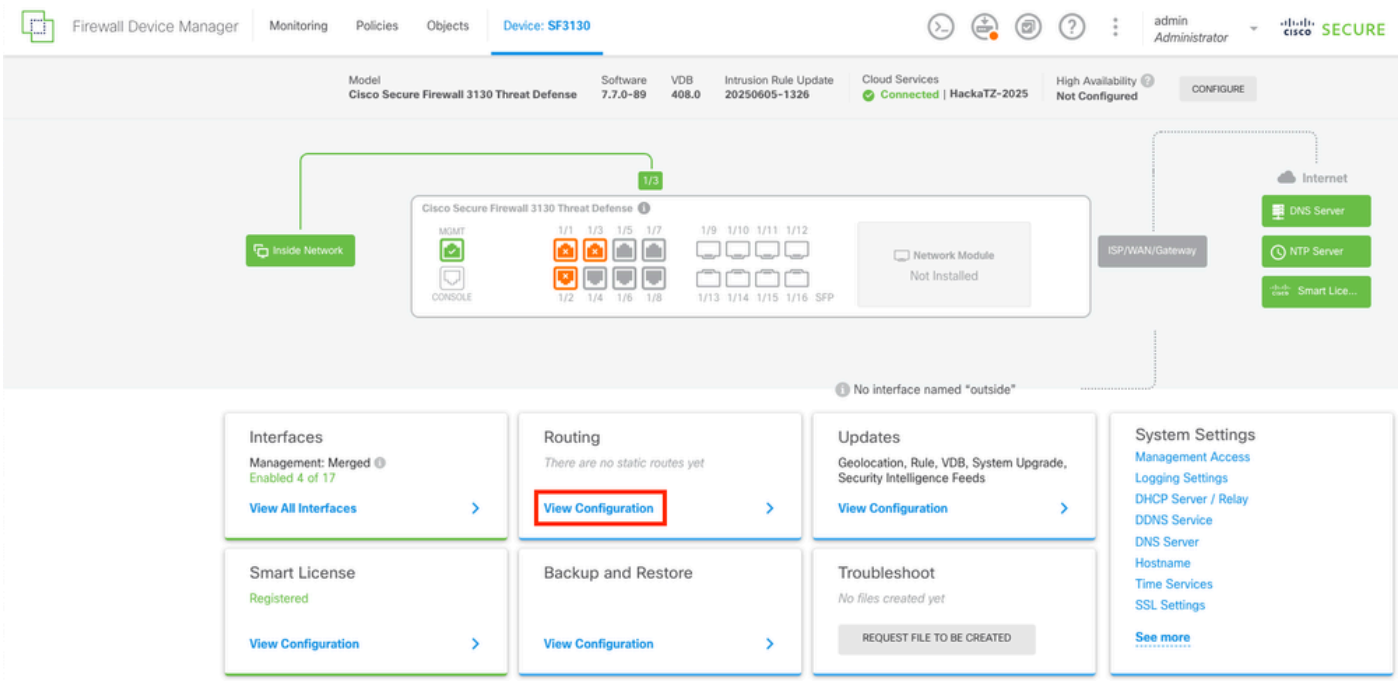
オブジェクトが作成されたら、インターフェイスのスタティックルートでオブジェクトを作成する必要があります。Deviceボタンを選択して、メインダッシュボードに移動します。



SLAモニタが作成されました

ステップ 10：

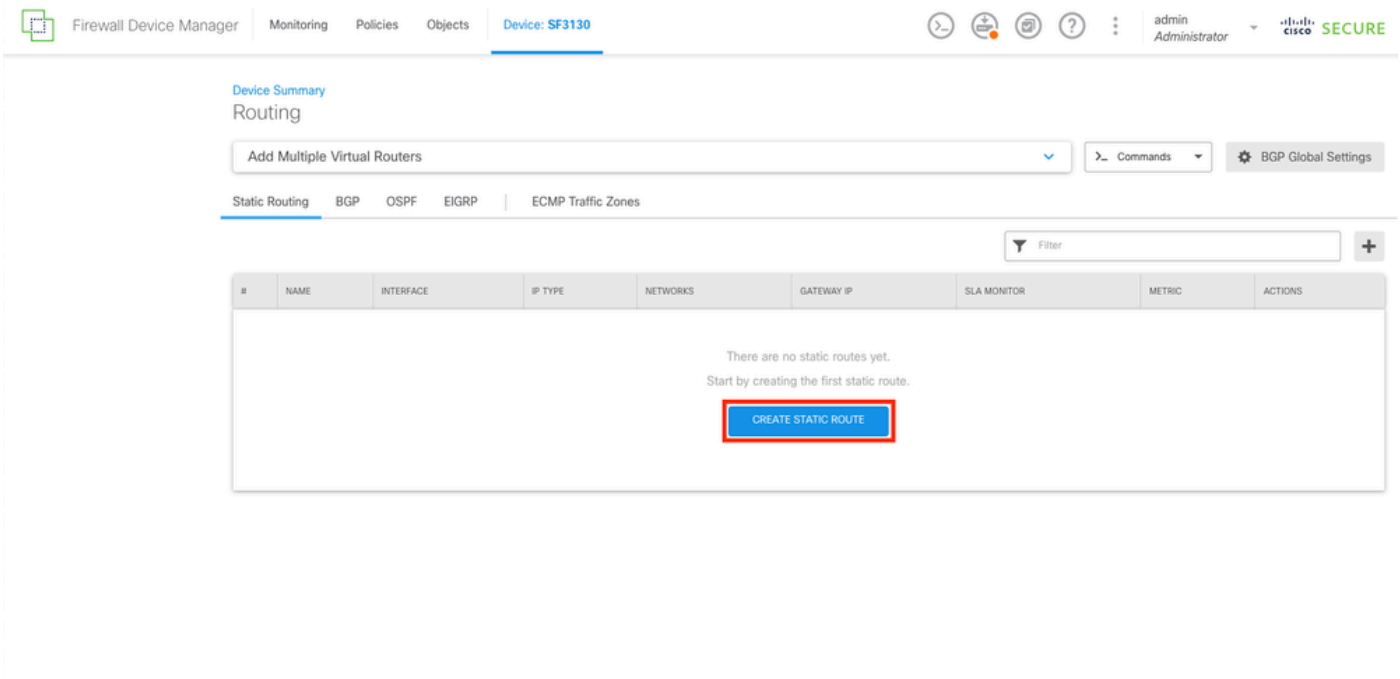
Routing PanelでView Configurationを選択して、Routing Sectionに移動します。



メインダッシュボード

ステップ 11

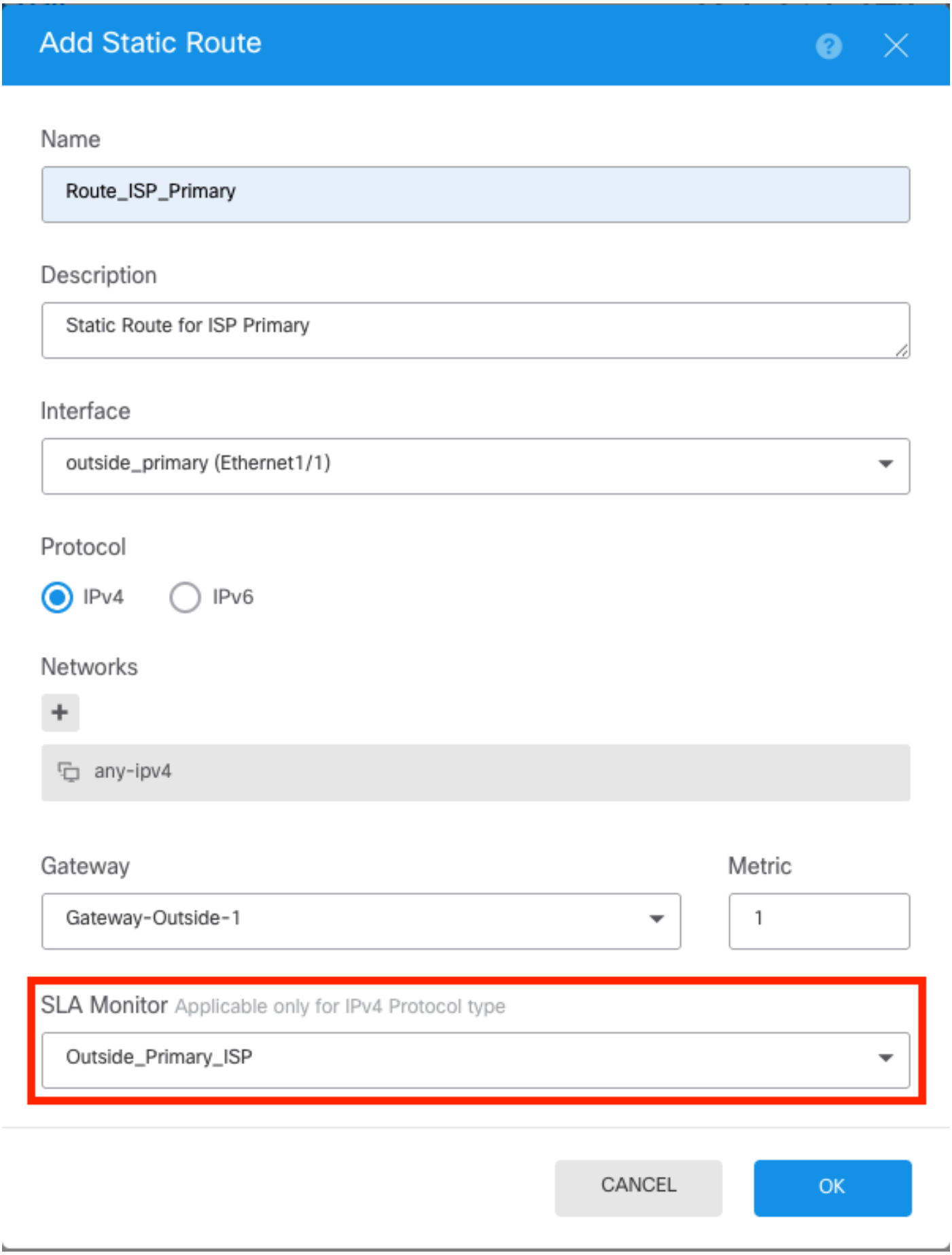
Static Routingタブで、両方のISPの2つのデフォルトスタティックルートを作成します。新しいスタティックルートを作成するには、CREATE STATIC ROUTEボタンを選択します。



Static Routingセクション

ステップ 12

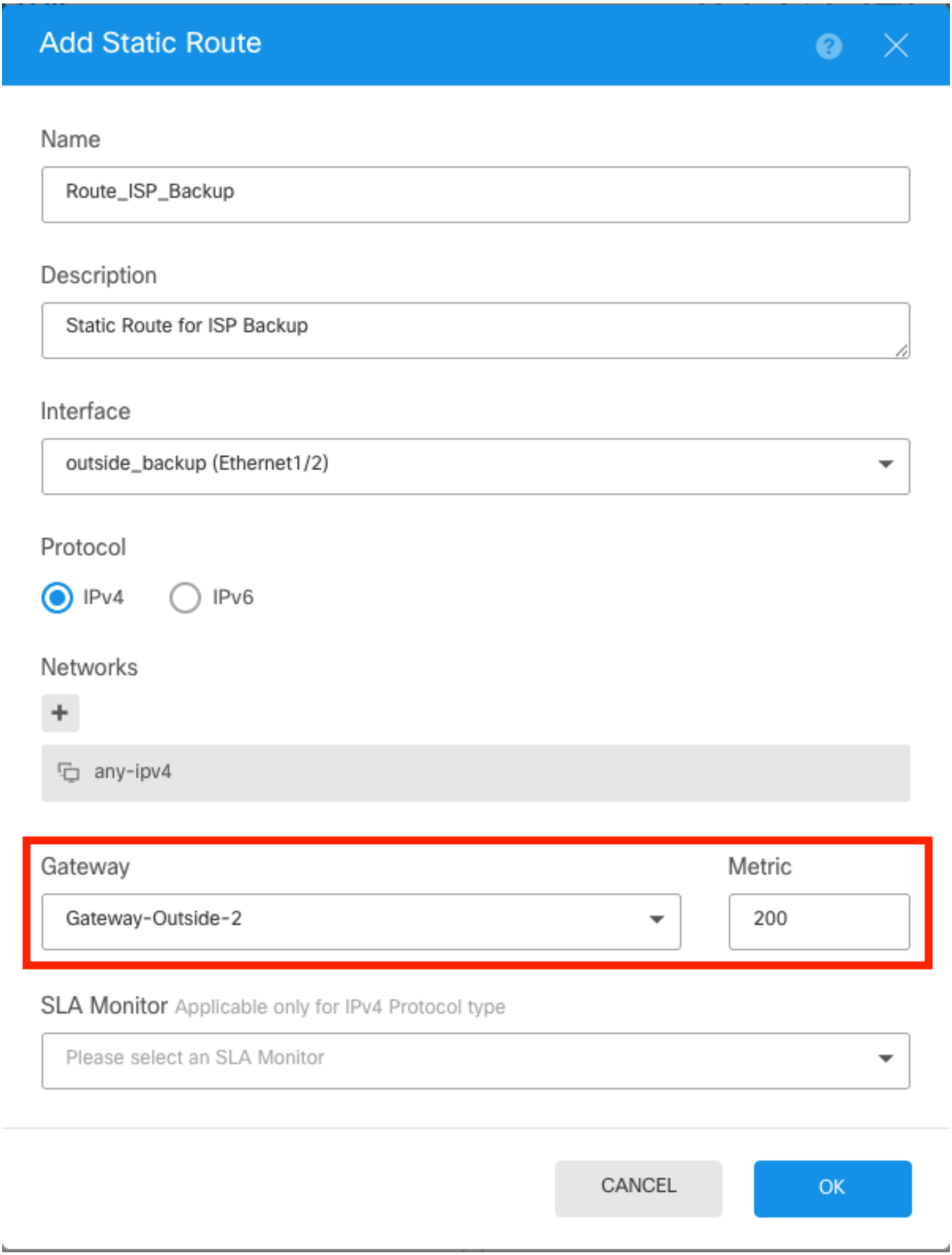
最初に、プライマリISPのスタティックルートを作成します。 最後に、最後の手順で作成したSLAモニタオブジェクトを追加します。



プライマリISPのスタティックルート

ステップ 13

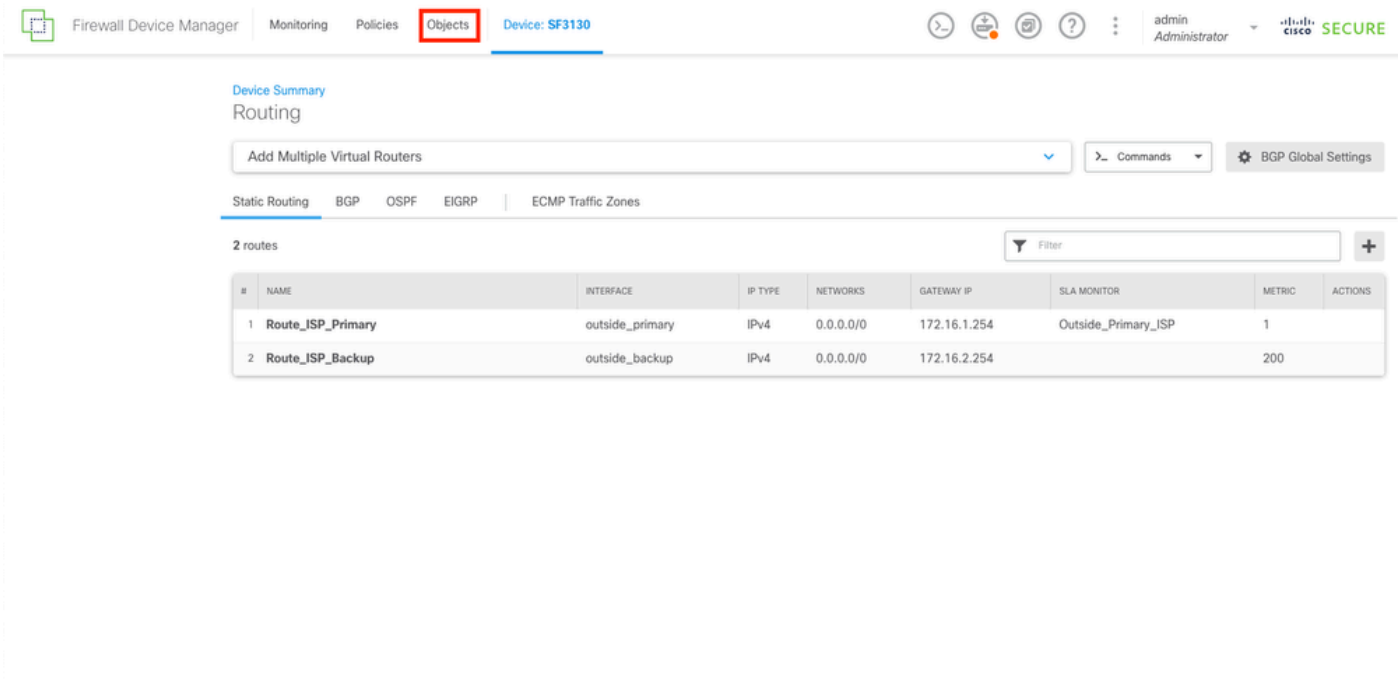
最後の手順を繰り返し、適切なゲートウェイと異なるメトリックを使用するISPセカンダリのデフォルトルートを作成します。この例では、200に増やされています。



セカンダリISPのスタティックルート

ステップ 14：

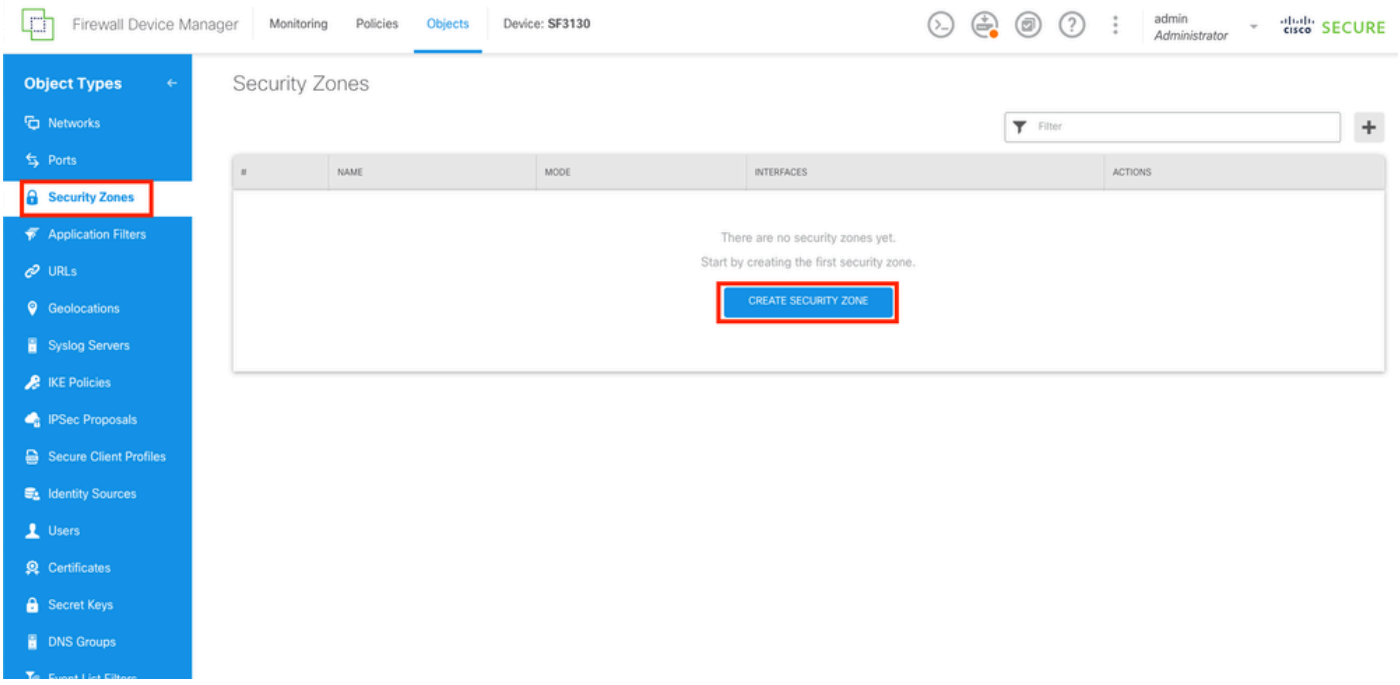
両方のスタティックルートが作成されたら、セキュリティゾーンを作成する必要があります。上部にあるObjectsボタンを選択して、Objectsセクションに移動します。



作成されたスタティックルート

ステップ 15：

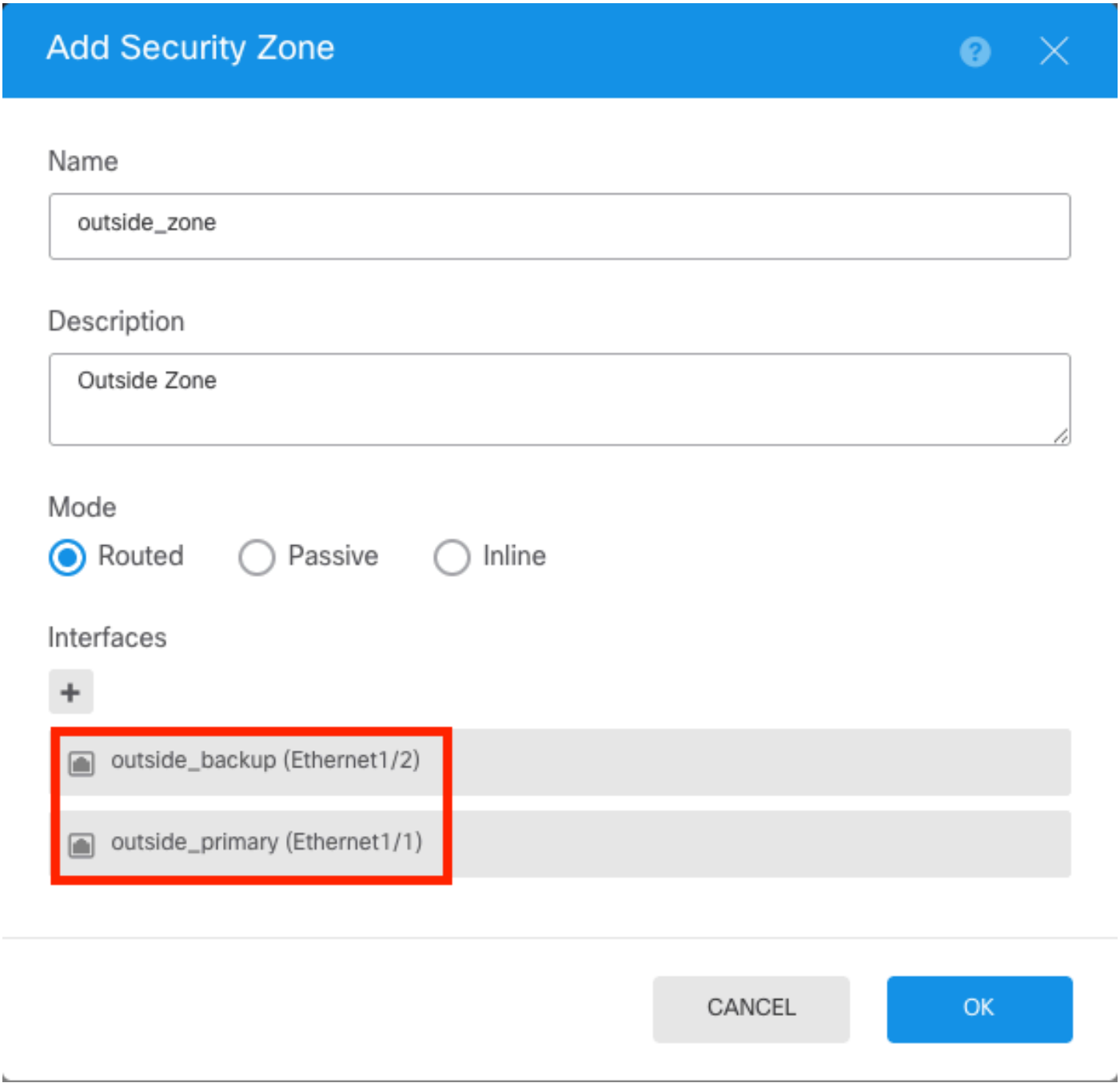
Security Zonesセクションの左側の列でSecurity Zonesボタンを選択してSecurity Zonesセクションに移動し、CREATE SECURITY ZONEボタンを選択して新しいゾーンを作成します。



Security Zonesセクション

ステップ 16：

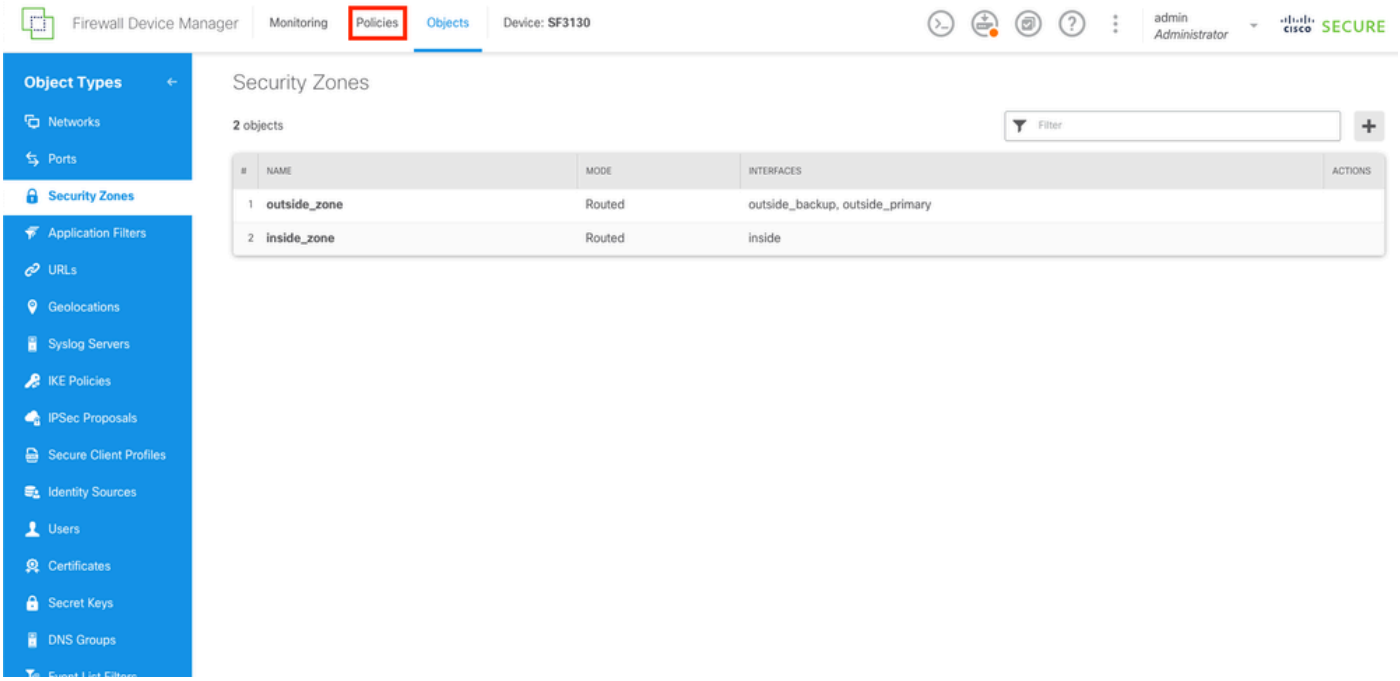
ISP接続の両方の外部インターフェイスを使用して外部セキュリティゾーンを作成します。



外部のセキュリティゾーン

ステップ 17：

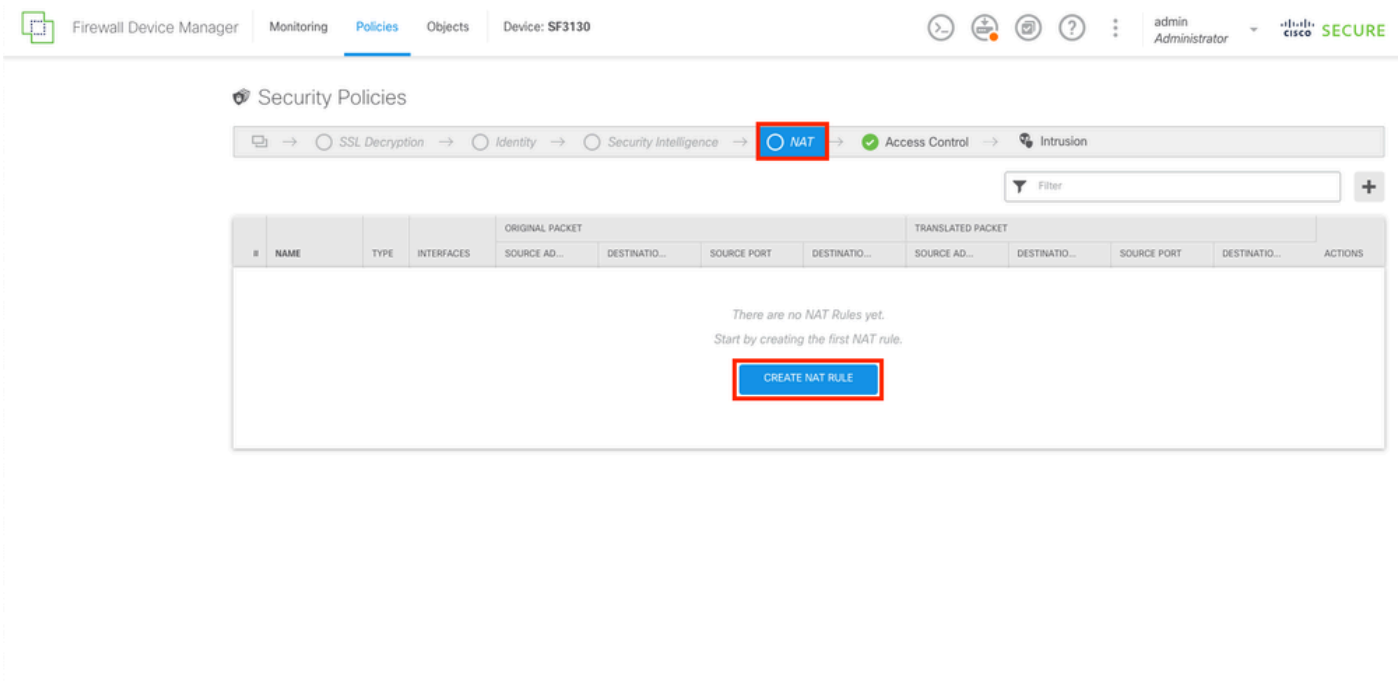
セキュリティゾーンが作成された後、NATを作成する必要があります。上部にあるPoliciesボタンを選択して、Policiesセクションに移動します。



作成されたセキュリティゾーン

ステップ 18 :

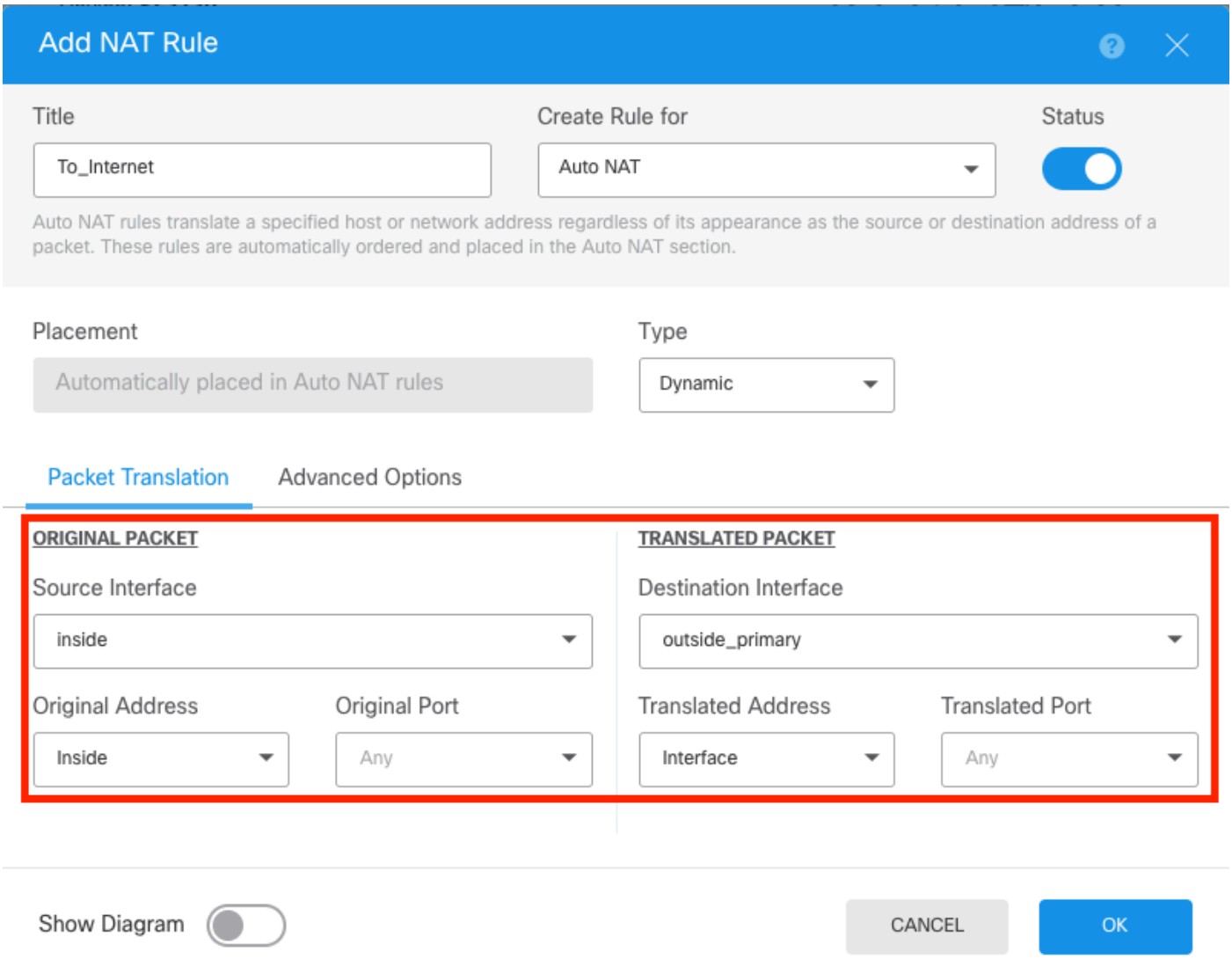
NATボタンを選択してNATセクションに移動してから、CREATE NAT RULEボタンを選択して新しいルールを作成します。



NATセクション

ステップ 19 :

ISPフェールオーバーの場合、設定には外部インターフェイスを経由する2つのルートが必要です。まず、プライマリISPへのプライマリ外部インターフェイス接続が必要です。

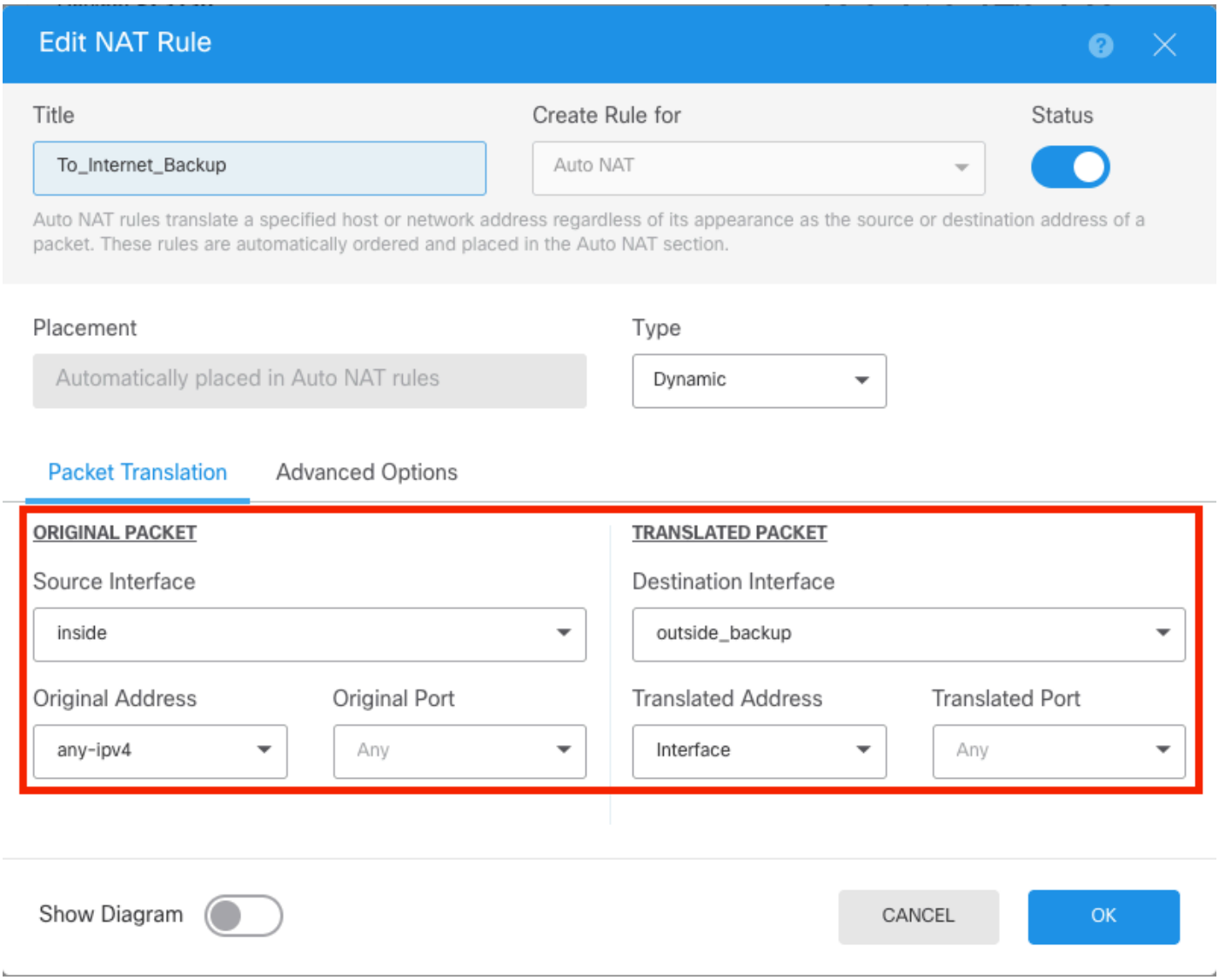


プライマリISPのNAT

ステップ 20：

次に、セカンダリISP接続用の2番目のNATです。

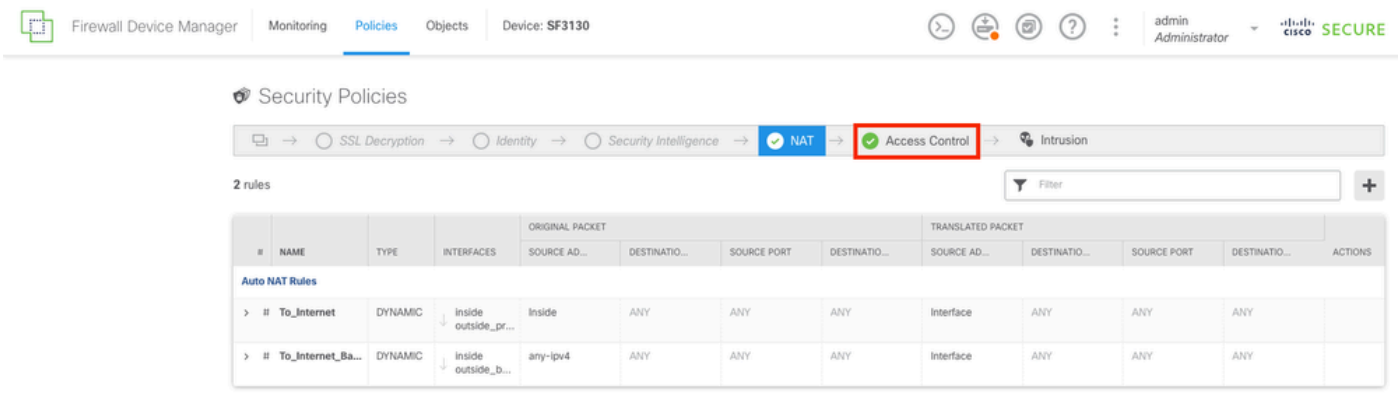
注：元のアドレスに対して、同じネットワークを使用することはできません。この例では、セカンダリISPの場合、元のアドレスはオブジェクトany-ipv4です。



セカンダリISP用NAT

ステップ 21：

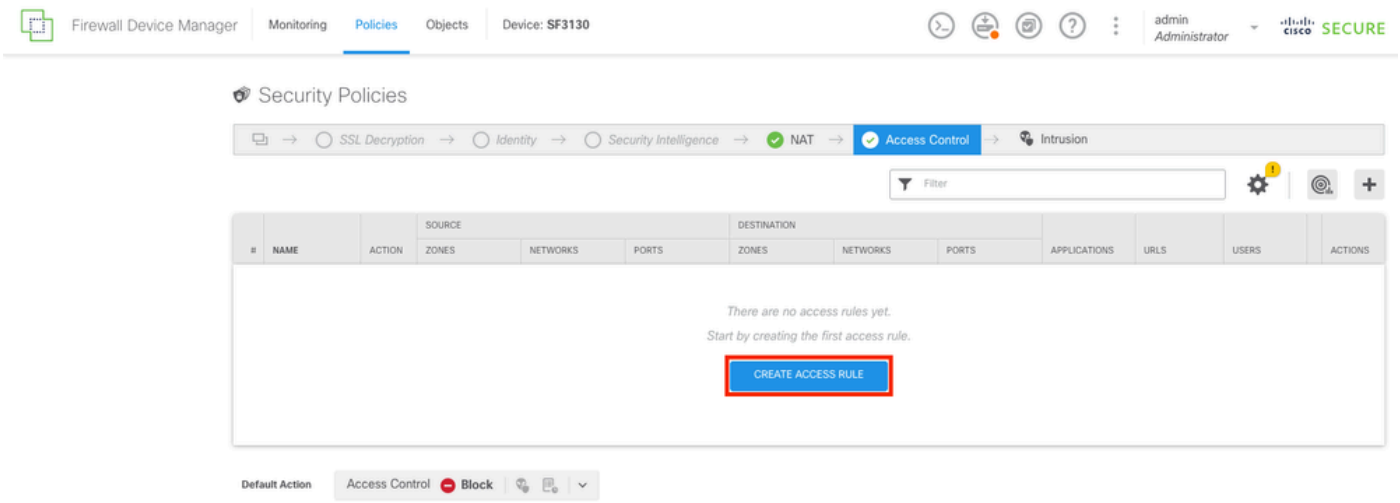
両方のNATルールを作成した後、アウトバウンドトラフィックを許可するためにアクセスコントロールルールを確立する必要があります。Access Controlボタンを選択します。



作成されたNATルール

ステップ 22 :

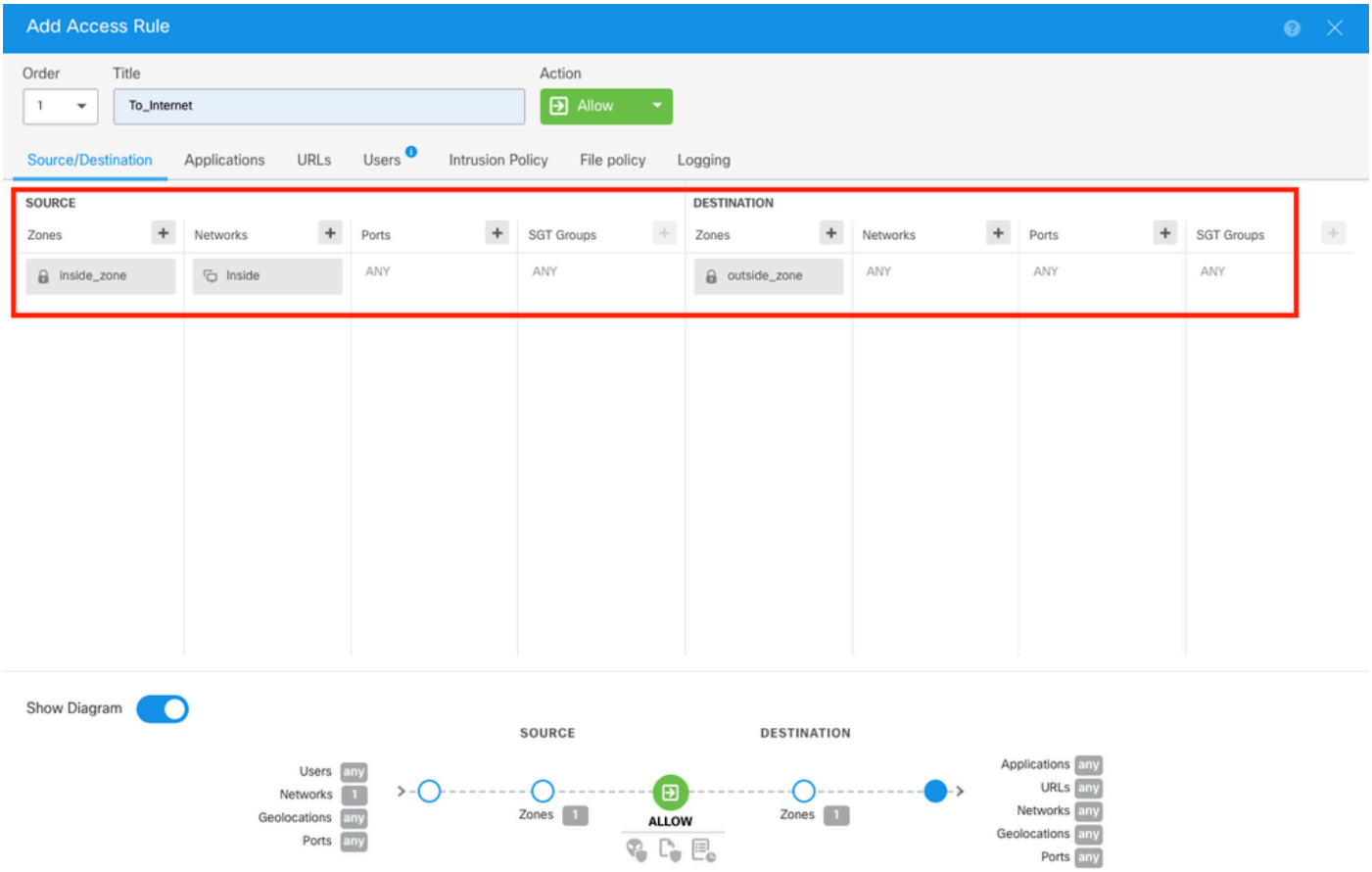
アクセスコントロールルールを作成するには、CREATE ACCESS RULEボタンを選択します。



Access Controlセクション

ステップ 23 :

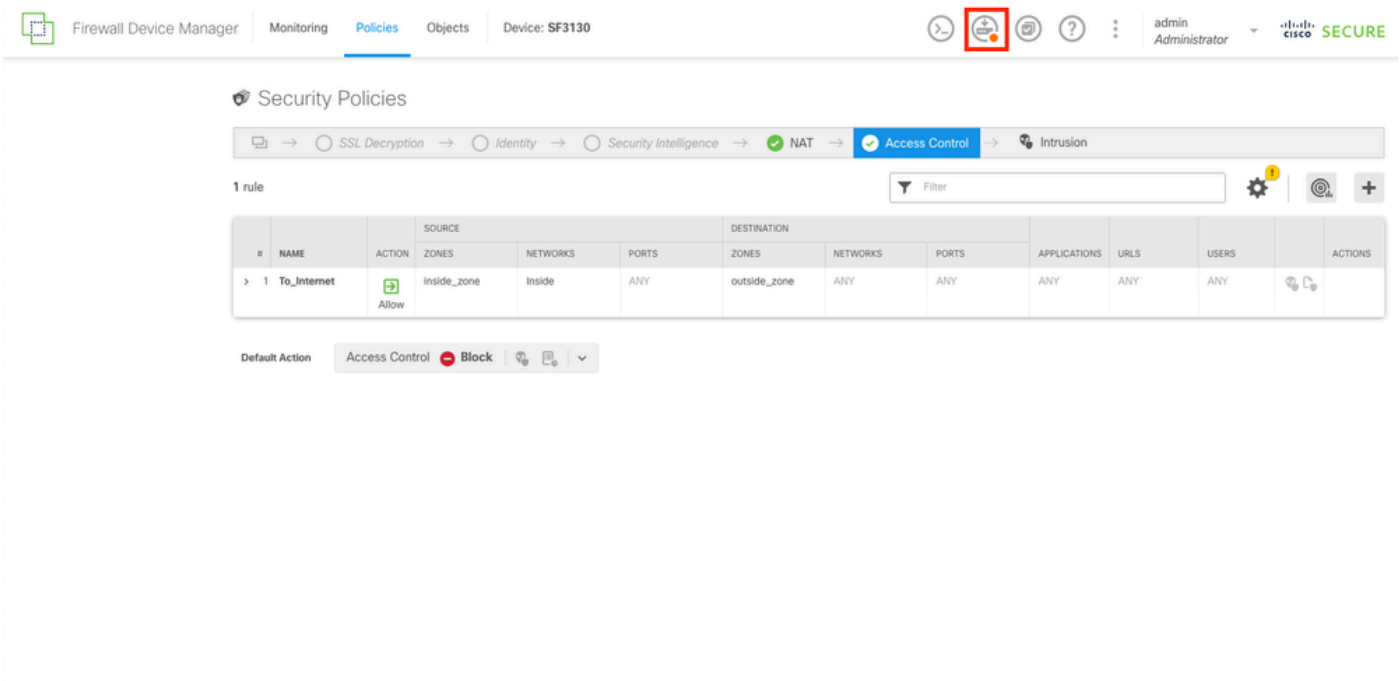
必要なゾーンとネットワークを選択します。



アクセスコントロールルール

ステップ 24：

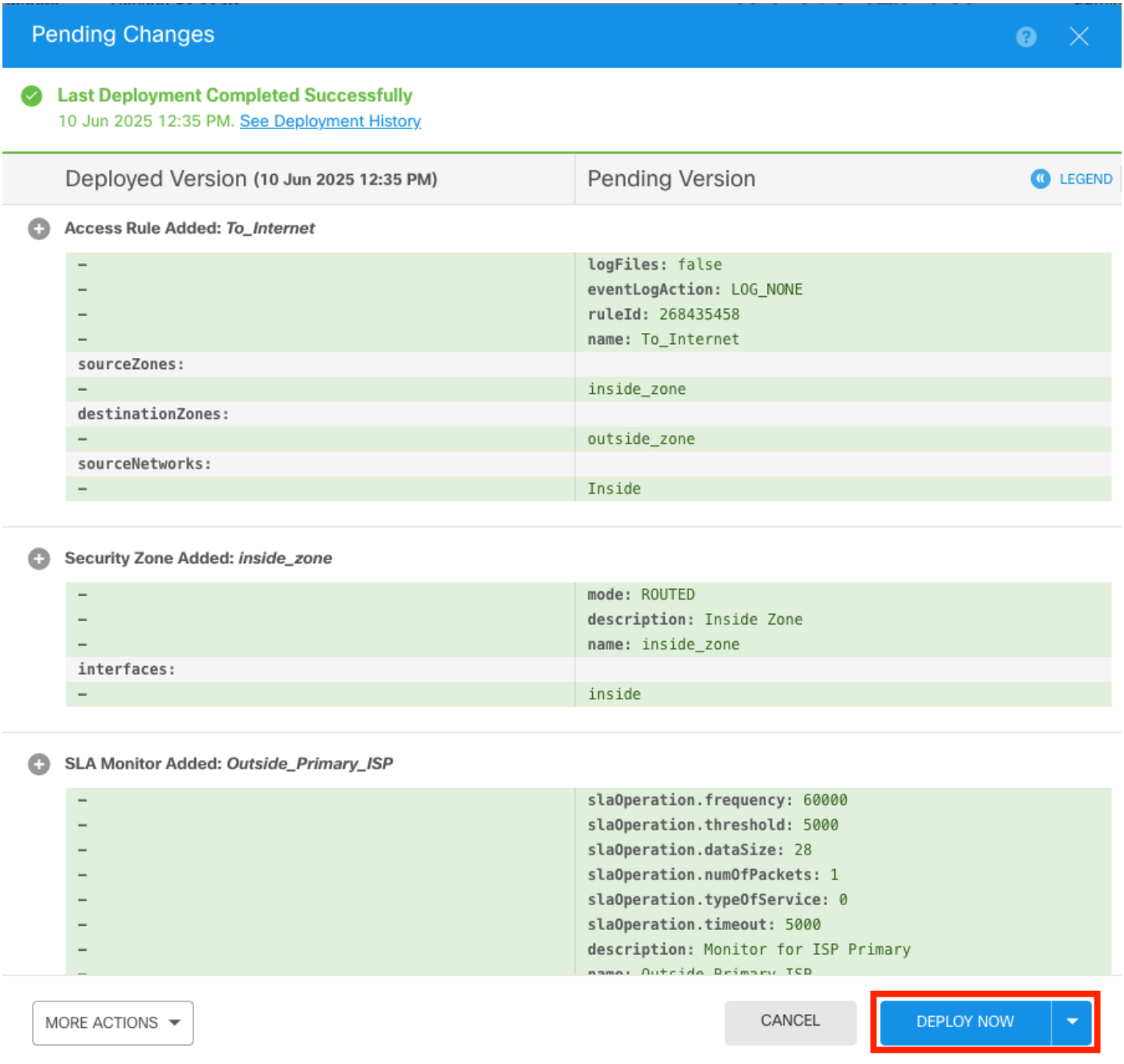
アクセスコントロールルールを作成したら、上部のDeployボタンを選択して、すべての変更の展開に進みます。



アクセスコントロールルールが作成されました

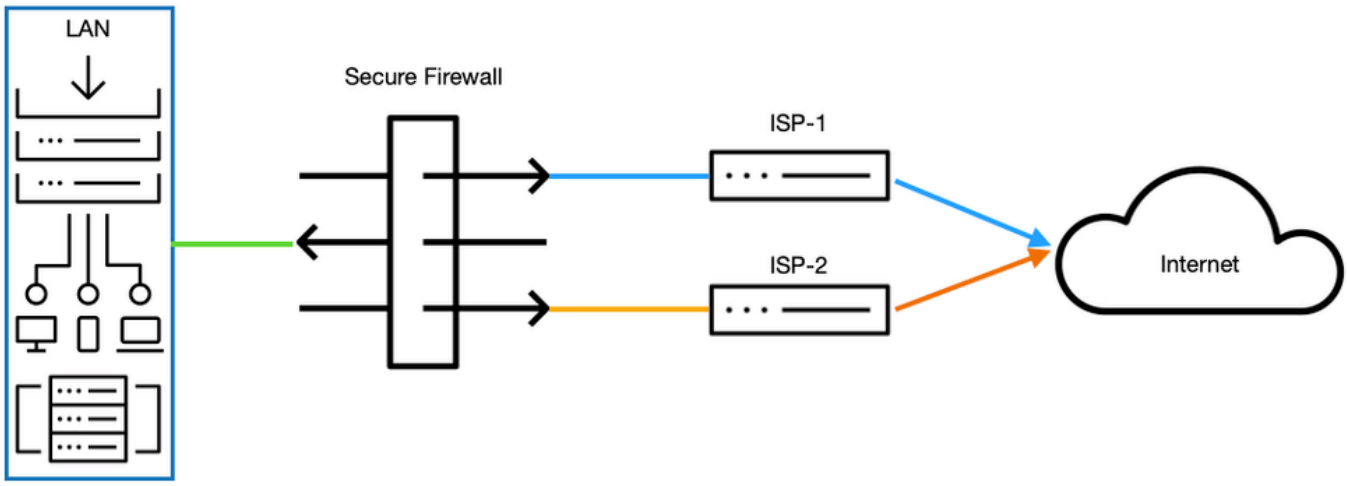
ステップ 25：

変更を確認し、「今すぐ配備」ボタンを選択します。



導入の検証

ネットワーク図



ネットワーク図

確認

<#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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。