Configuration de deux FAI sur FTD à l'aide de FDM

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Diagramme du réseau

Vérifier

Introduction

Ce document décrit comment configurer le basculement de deux fournisseurs d'accès Internet (FAI) à l'aide de Firewall Device Manager (FDM) pour la gamme Secure Firewall.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Routage de base
- Connaissances du tableau de bord du Gestionnaire de pare-feu
- Au moins 2 fournisseurs d'accès Internet connectés au pare-feu sécurisé.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

· Cisco Secure Firewall version 7.7.X ou ultérieure.

· Secure Firewall 3130 avec version 7.7.0.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Étape 1.

Connectez-vous au FDM sur le pare-feu sécurisé et accédez à la section des interfaces en sélectionnant le bouton View All Interfaces (Afficher toutes les interfaces).

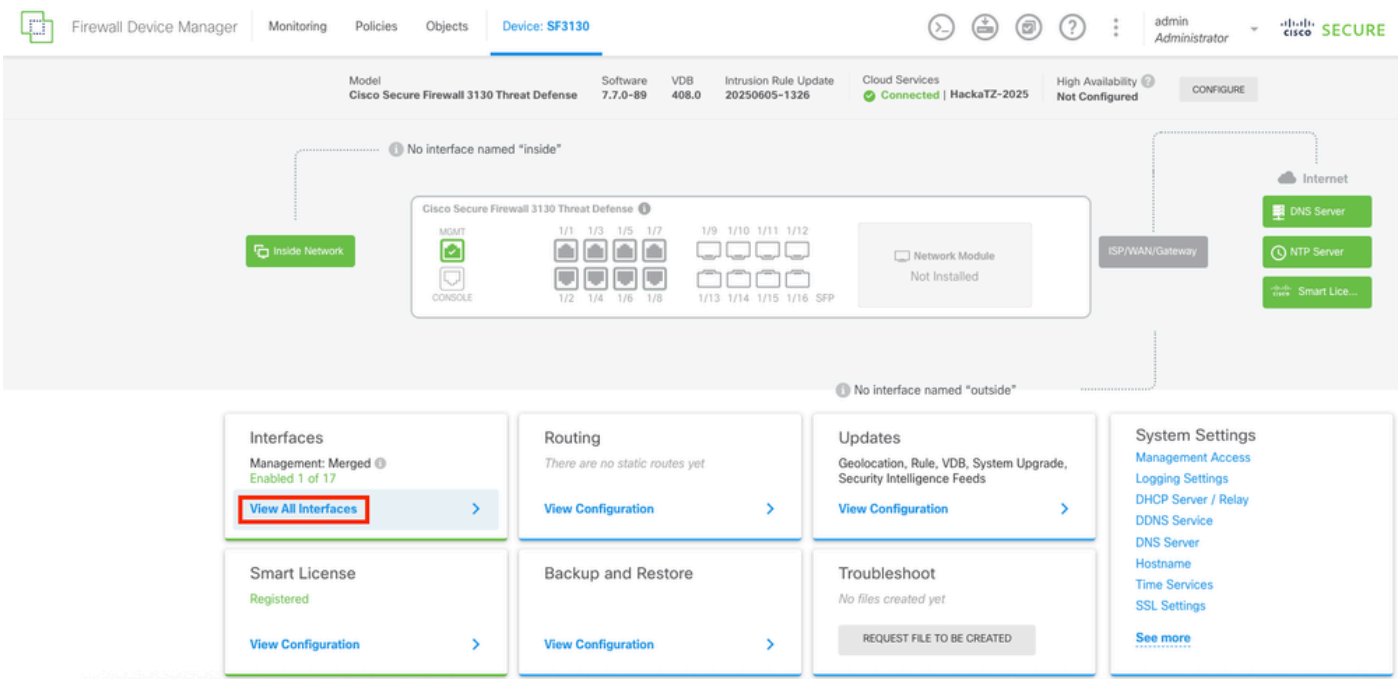
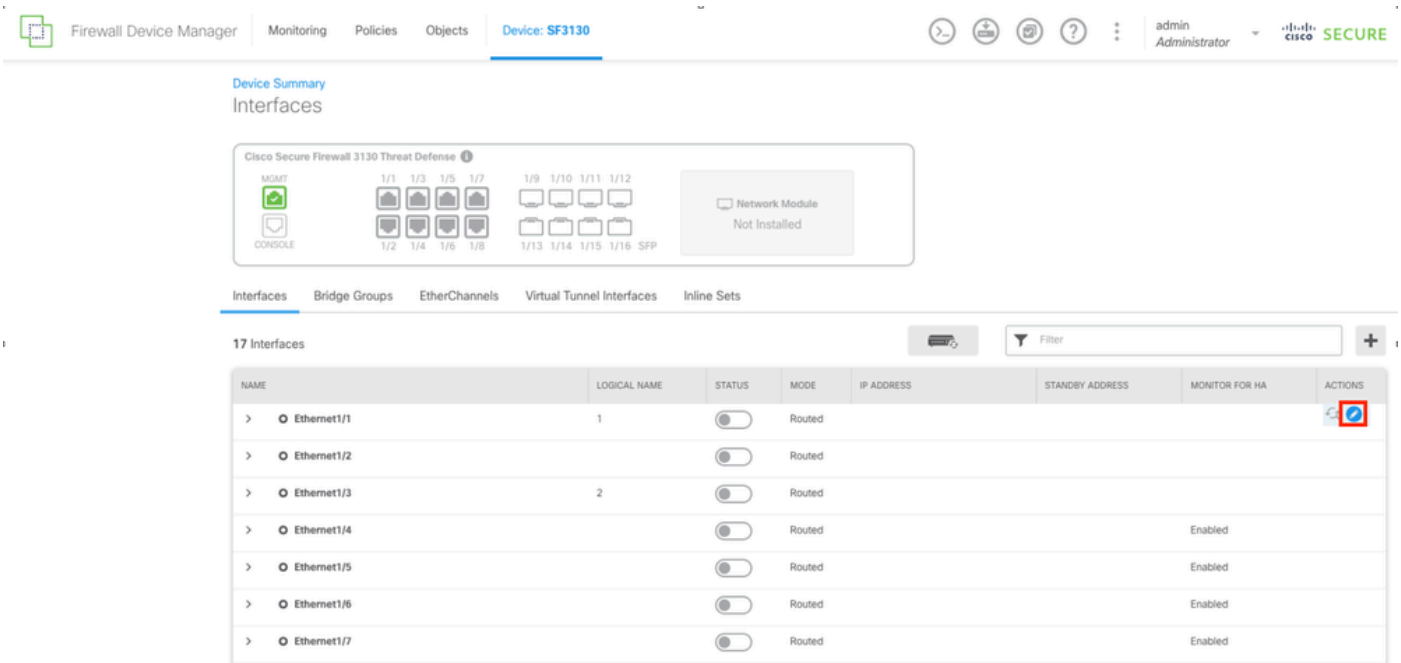


Tableau de bord principal FDM

Étape 2.

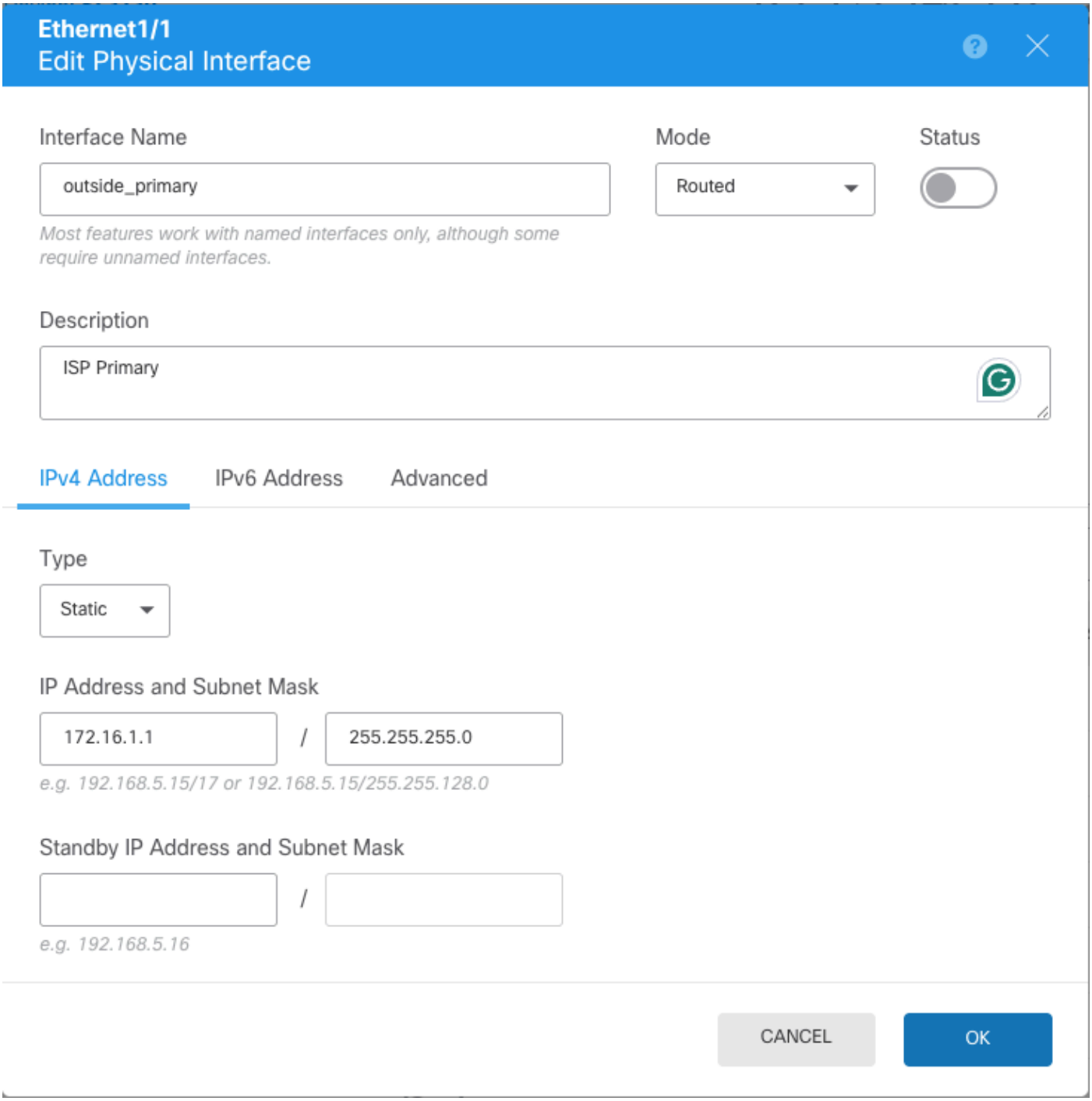
Pour configurer l'interface de la connexion du FAI principal, commencez par sélectionner l'interface de votre choix. Sélection du bouton d'interface correspondant pour continuer. Dans cet exemple, l'interface utilisée est Ethernet1/1.



Onglet Interface

Étape 3.

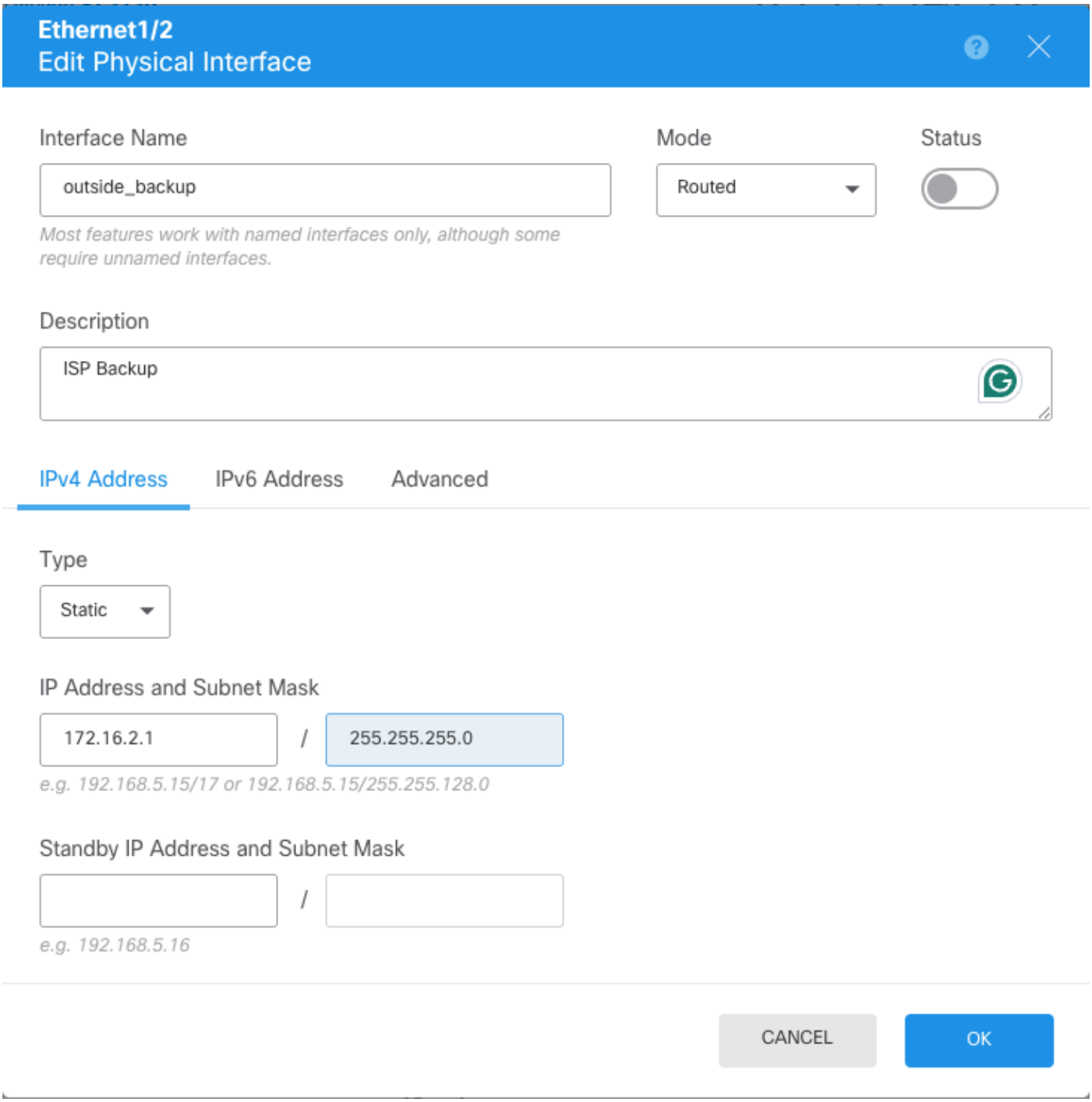
Configurez l'interface avec les paramètres appropriés pour votre connexion au FAI principal. Dans cet exemple, l'interface est outside_primary.



Configuration de l'interface principale du FAI

Étape 4.

Répétez le même processus pour l'interface ISP secondaire. Dans cet exemple, l'interface Ethernet1/2 est utilisée.

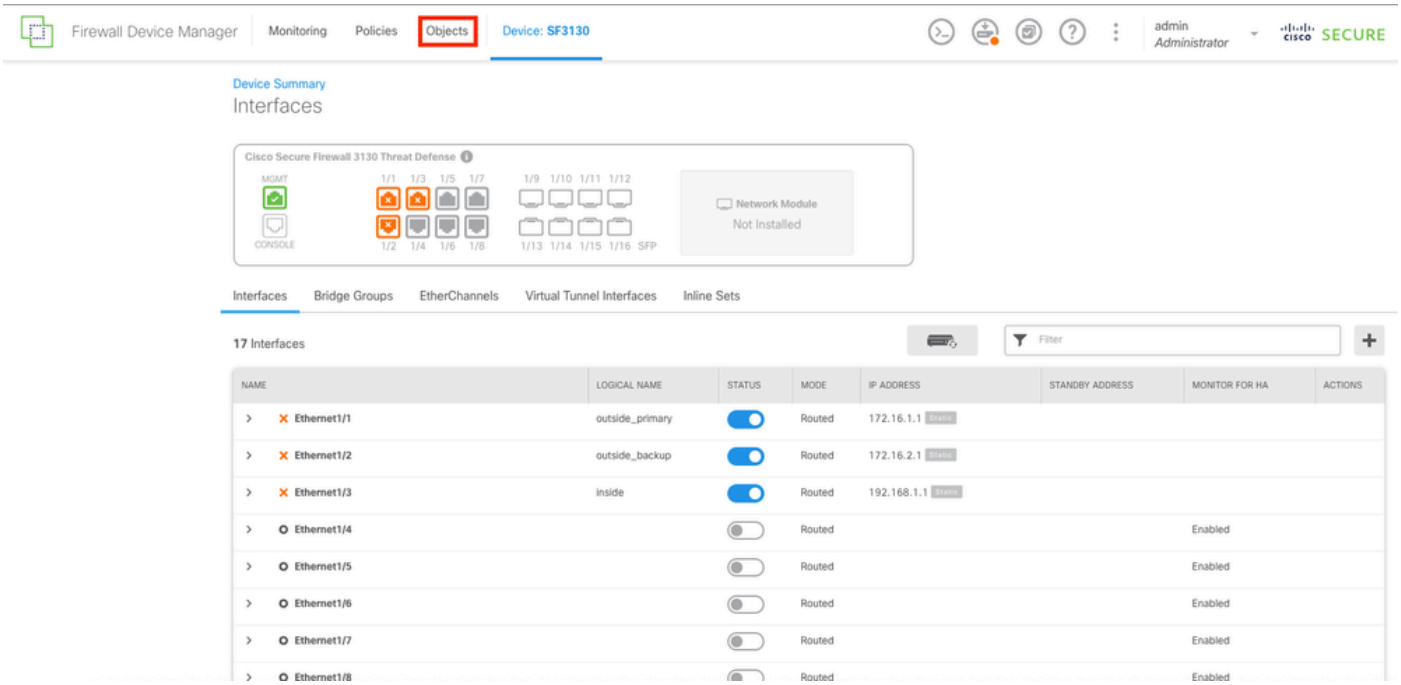


Configuration de l'interface ISP secondaire

Étape 5.

Après avoir configuré les deux interfaces pour les FAI, l'étape suivante consiste à configurer le SLA Monitor pour l'interface principale.

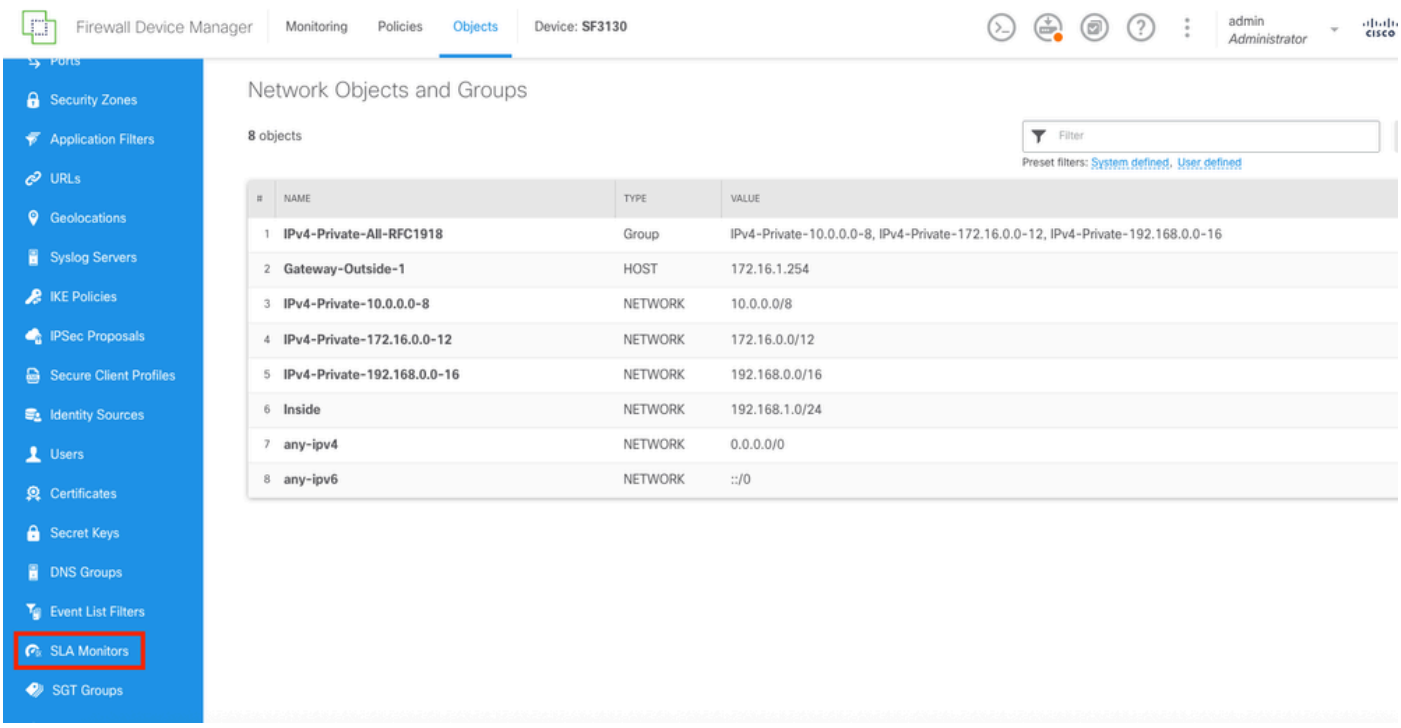
Accédez à la section Objets en sélectionnant le bouton Objets situé en haut du menu.



Interfaces configurées

Étape 6.

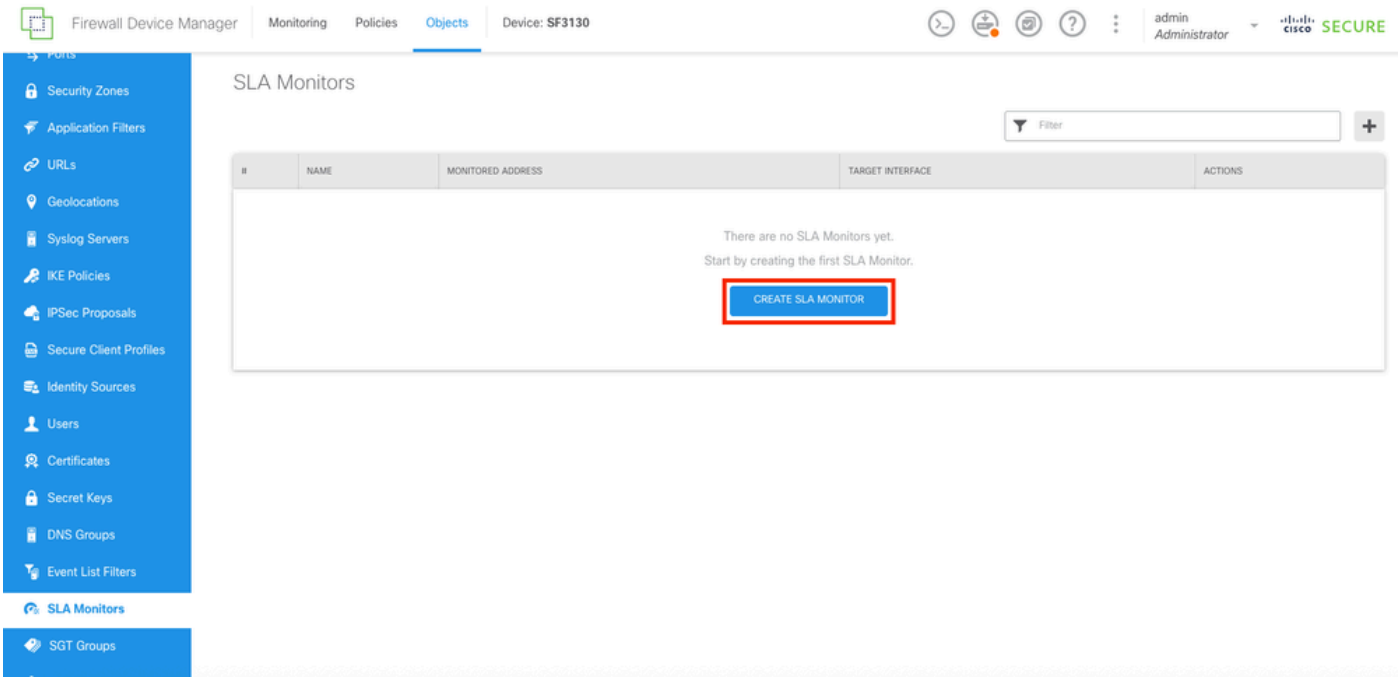
Sélectionnez le bouton SLA Monitors dans la colonne de gauche.



Ecran Objets

Étape 7.

Créez un nouveau SLA Monitor en cliquant sur le bouton Create SLA Monitor.



Section SLA Monitor

Étape 8.

Configurez les paramètres de la connexion du FAI principal.

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

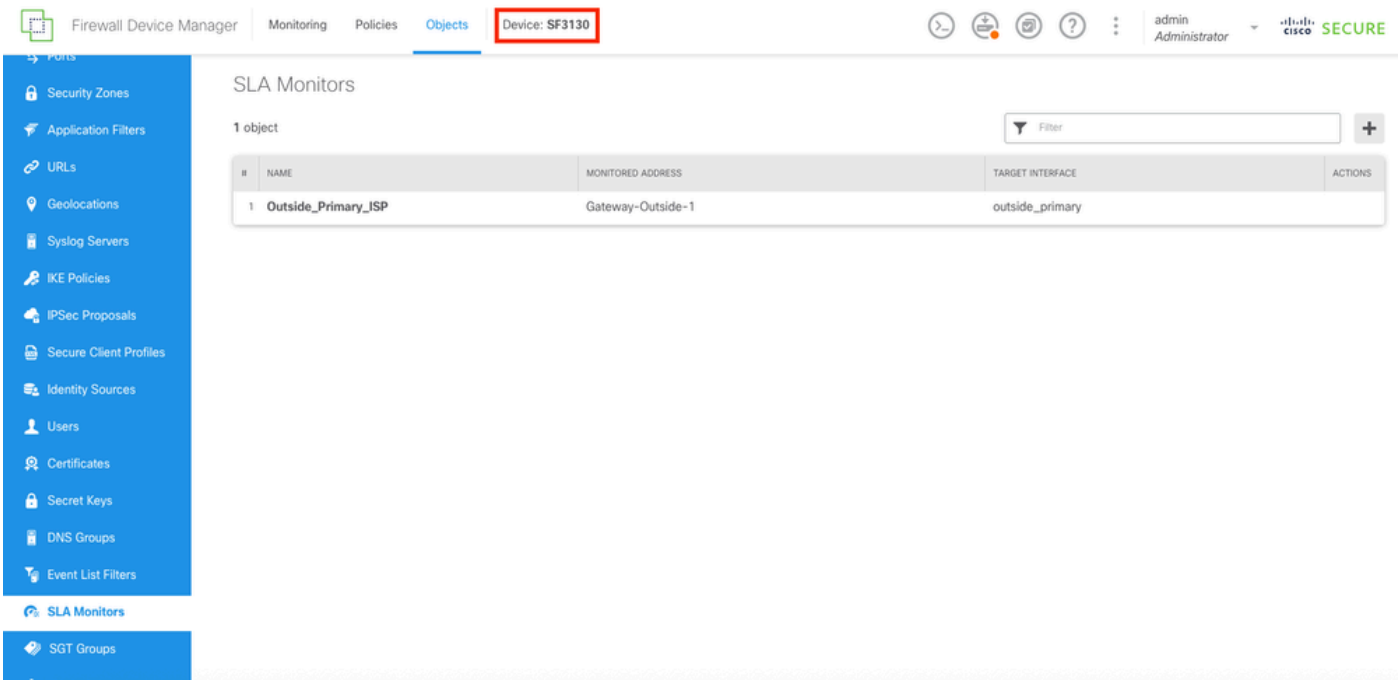
0 - 16384

CANCEL OK

Création d'objets SLA

Étape 9.

Une fois l'objet créé, la route statique pour les interfaces doit la créer. Accédez au tableau de bord principal en sélectionnant le bouton Device (Périphérique).



Moniteur SLA créé

Étape 10.

Accédez à la section Routing en sélectionnant View Configuration dans le panneau de routage.

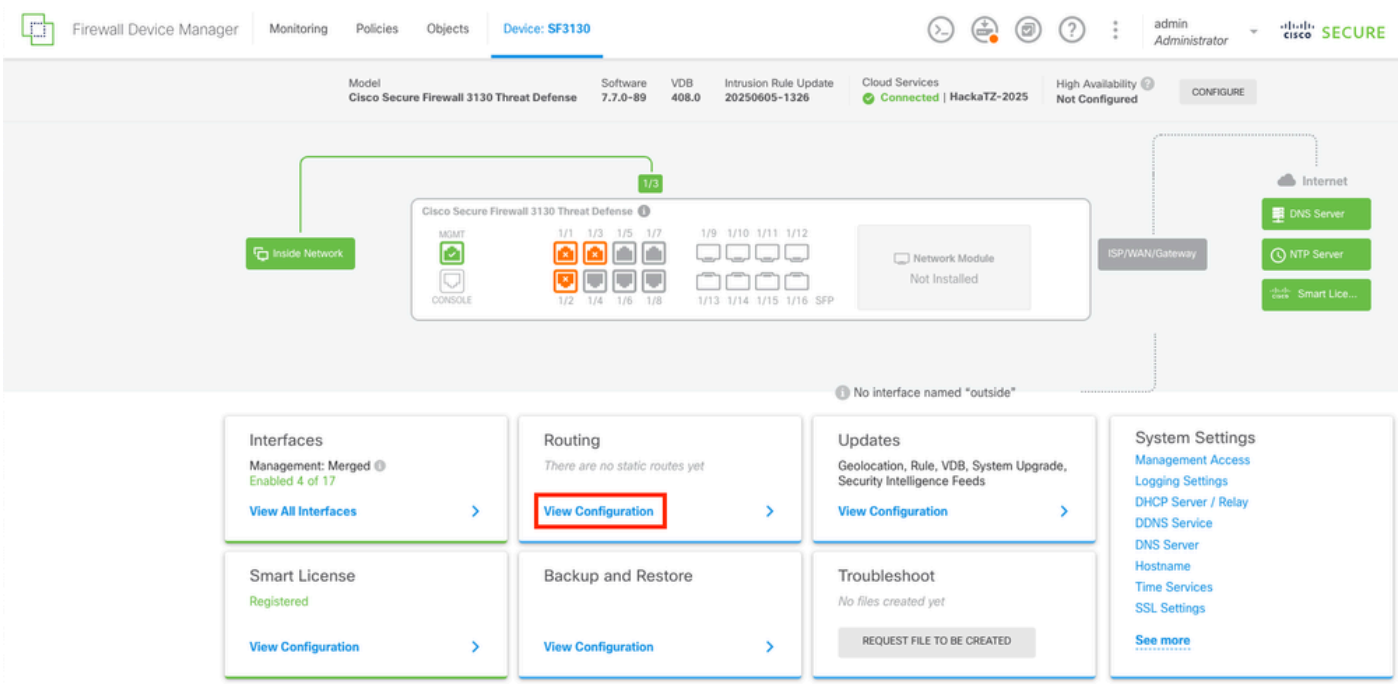
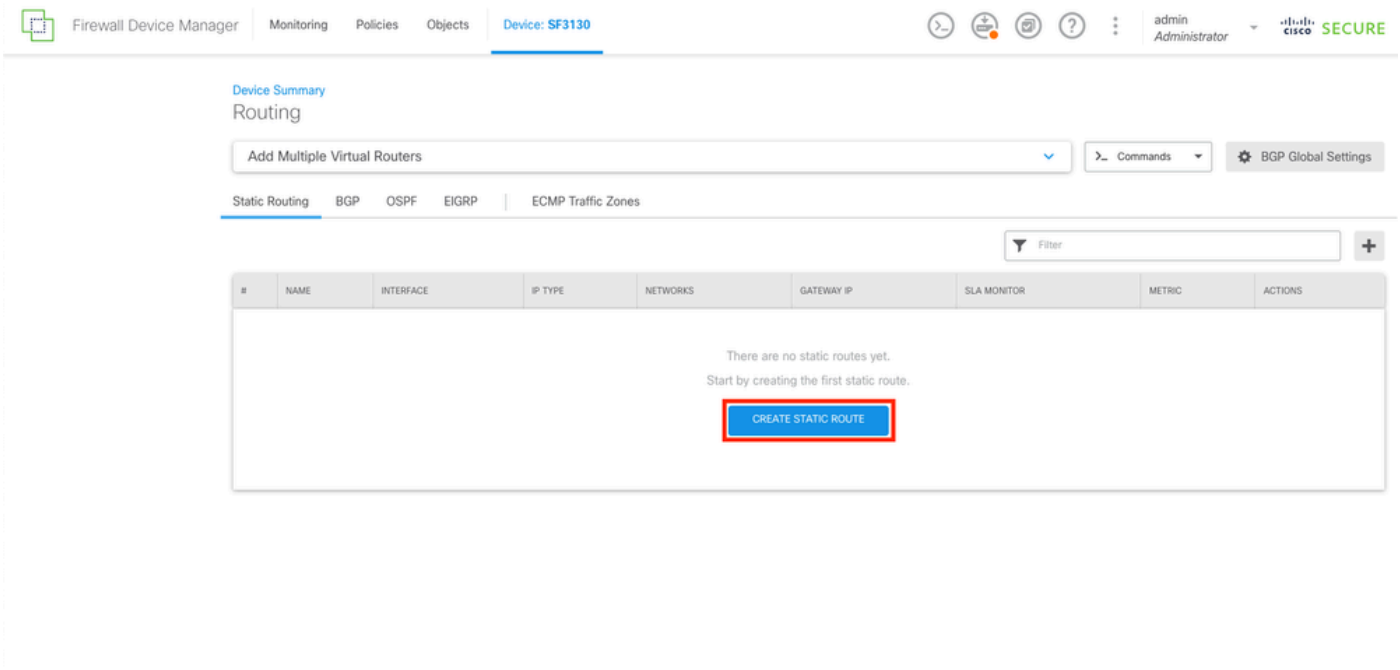


Tableau de bord principal

Étape 11.

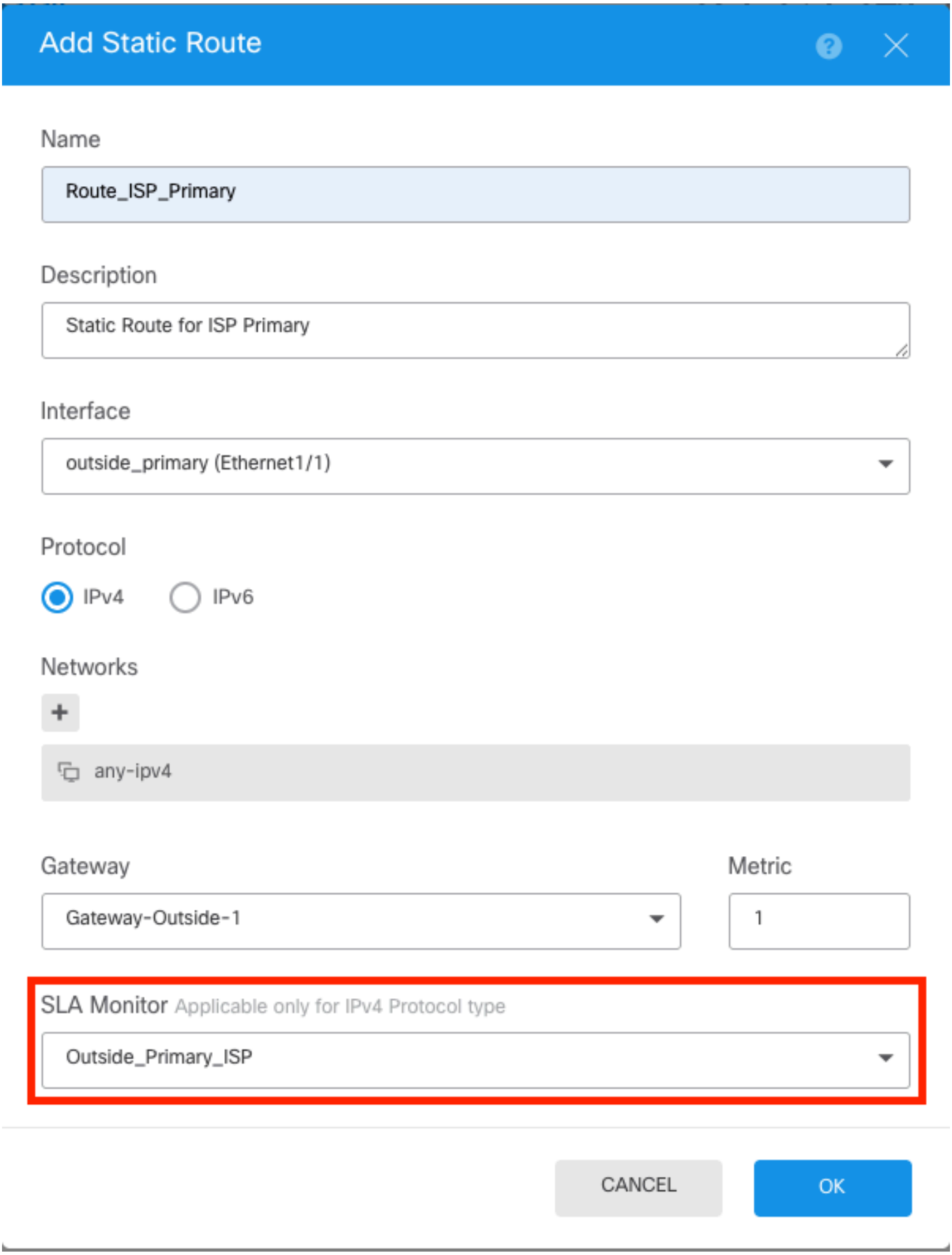
Dans l’onglet Static Routing (Routage statique), créez les deux routes statiques par défaut pour les deux FAI. Pour créer une nouvelle route statique, cliquez sur le bouton CREATE STATIC ROUTE.



Section Routage statique

Étape 12.

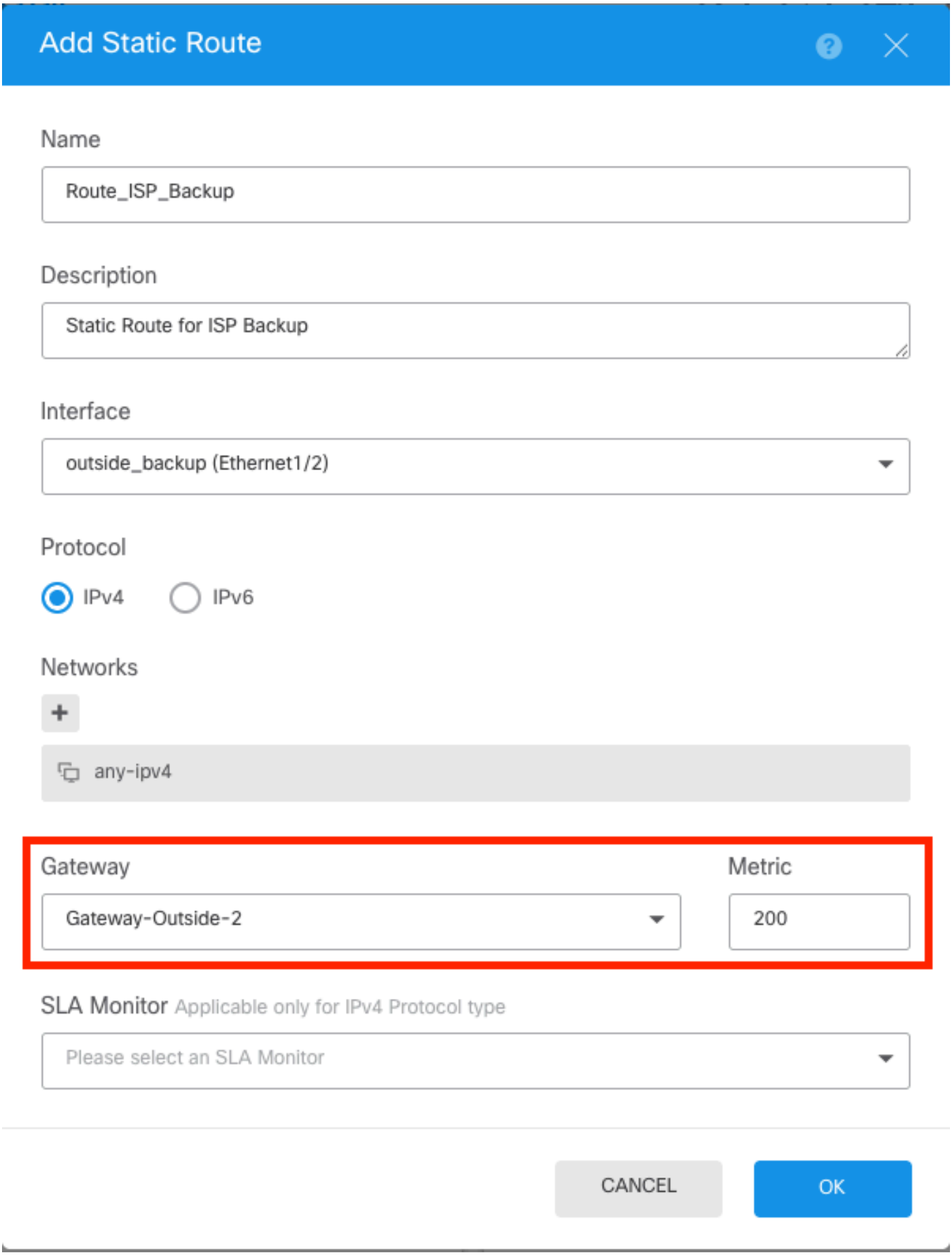
Commencez par créer la route statique pour le FAI principal. À la fin, ajoutez l’objet de surveillance SLA qui a été créé à la dernière étape.



Route statique pour le FAI principal

Étape 13.

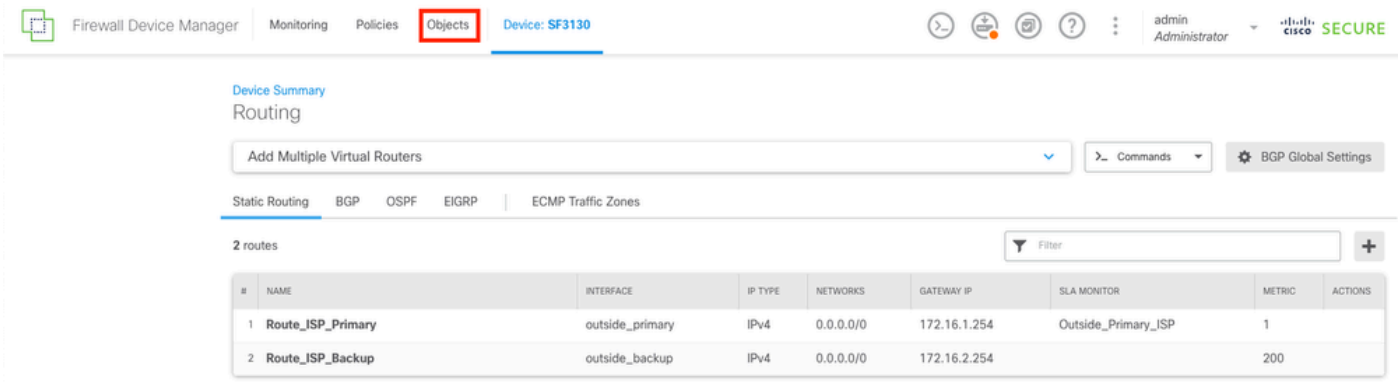
Répétez la dernière étape et créez une route par défaut, pour le routeur secondaire ISP avec la passerelle appropriée et une métrique différente. Dans cet exemple, il a été porté à 200.



Route statique pour ISP secondaire

Étape 14.

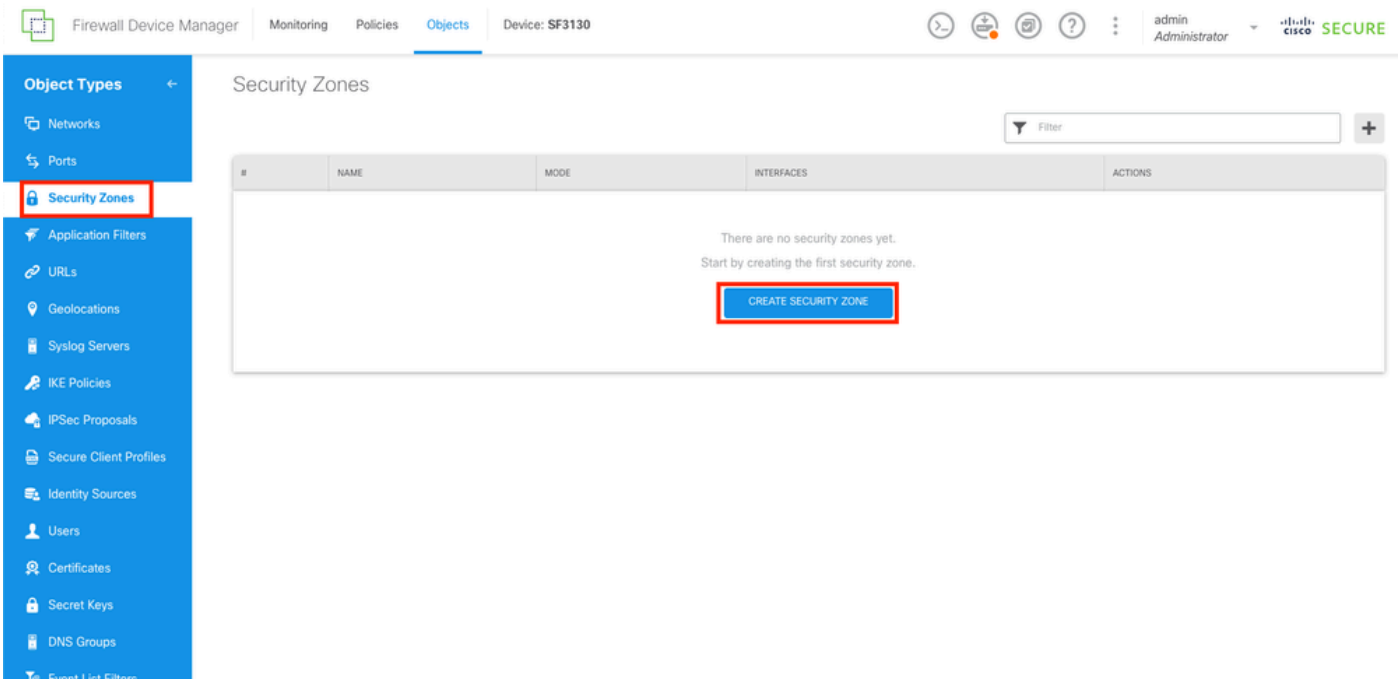
Une fois les deux routes statiques créées, une zone de sécurité doit être créée. Accédez à la section Objets en cliquant sur le bouton Objets en haut de la page.



Routes statiques créées

Étape 15.

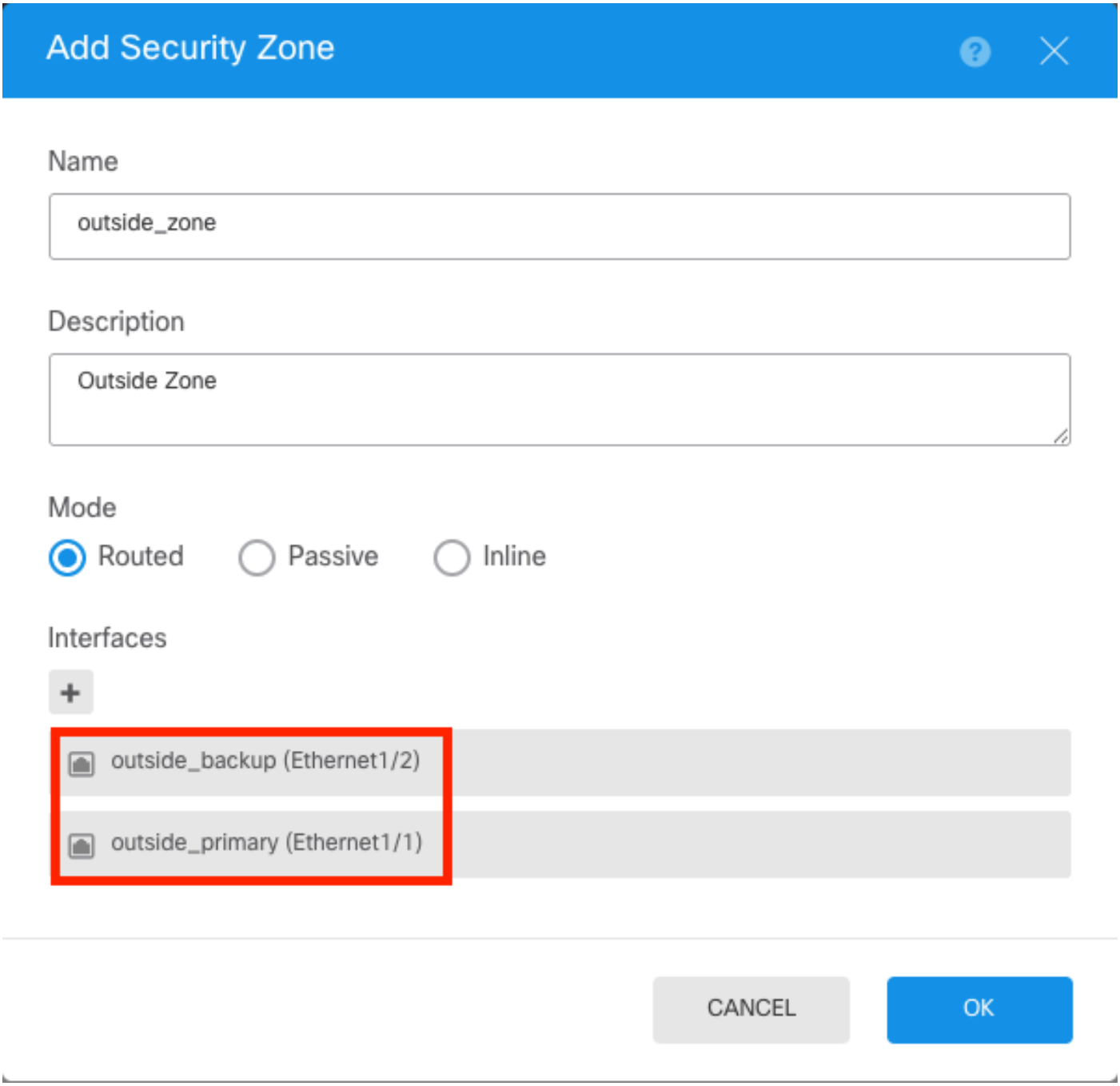
Accédez à la section Zones de sécurité en sélectionnant dans la colonne de gauche le bouton Zones de sécurité, puis créez une nouvelle zone en sélectionnant le bouton CREATE SECURITY ZONE.



Section Zones de sécurité

Étape 16.

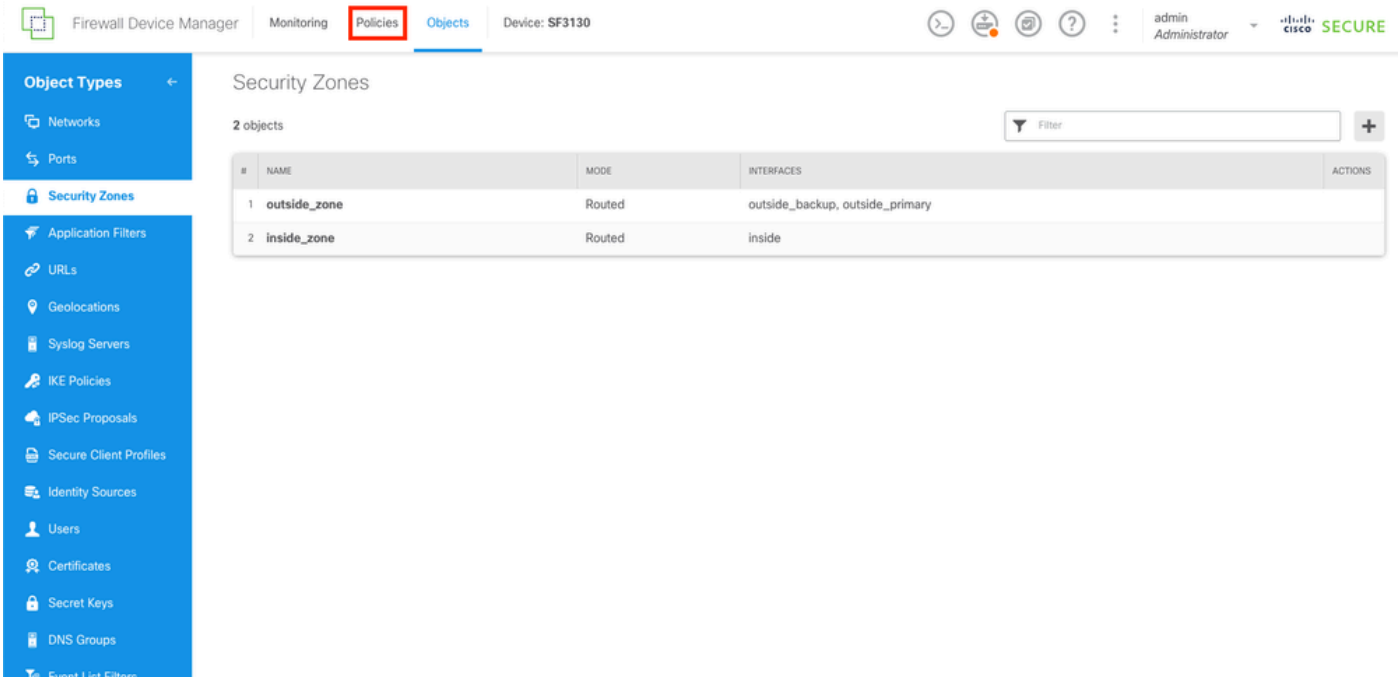
Créez la zone de sécurité externe avec les deux interfaces externes pour les connexions des FAI.



Zone de sécurité externe

Étape 17.

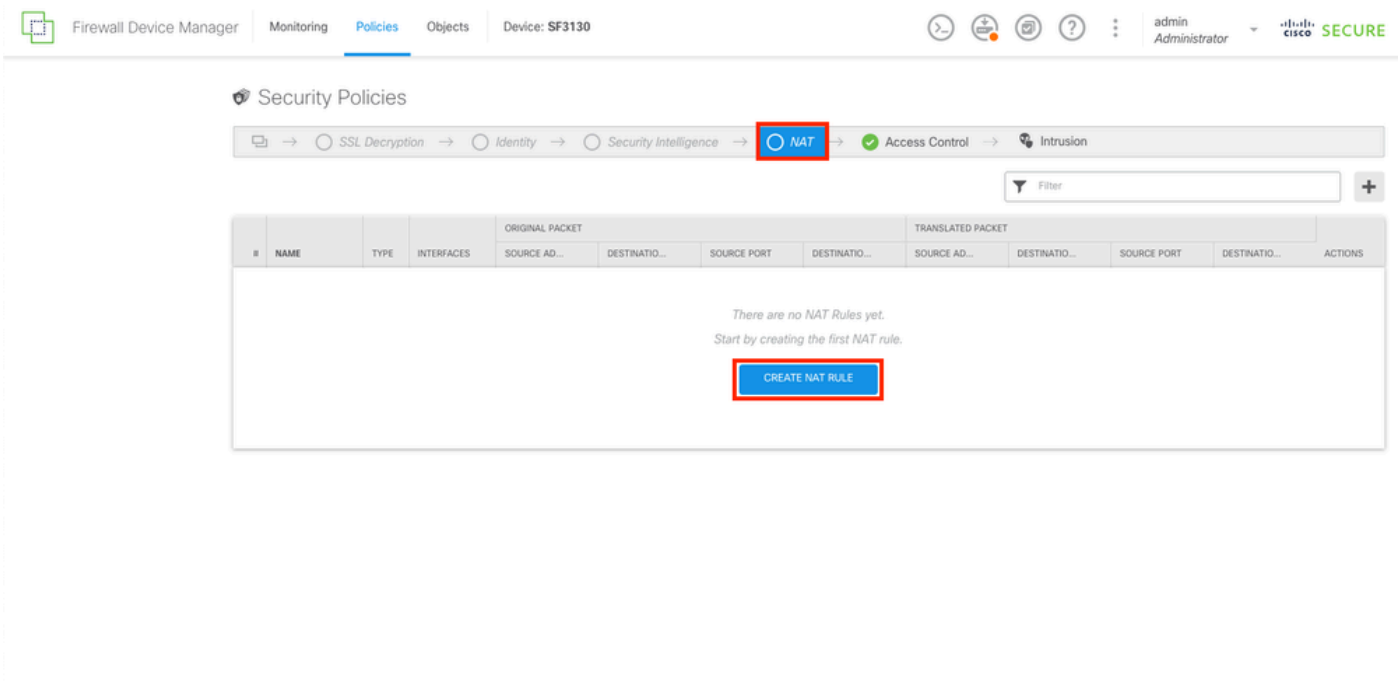
Une fois la zone de sécurité créée, une NAT doit être créée. Accédez à la section Policies en cliquant sur le bouton Policies en haut de la page.



Zones de sécurité créées

Étape 18.

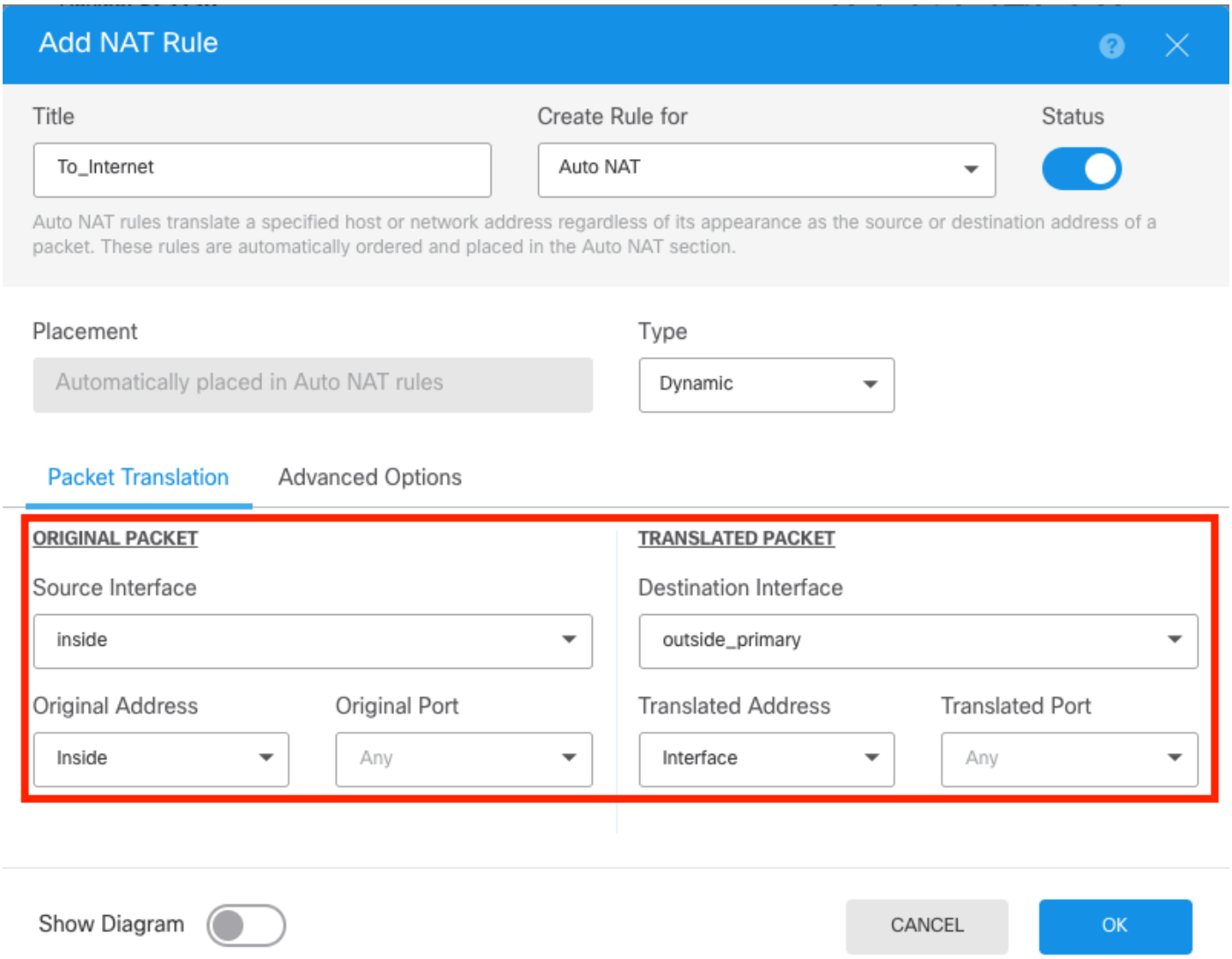
Accédez à la section NAT en sélectionnant le bouton NAT, puis créez une nouvelle règle en sélectionnant le bouton CREATE NAT RULE.



Section NAT

Étape 19.

Pour le basculement du FAI, la configuration doit comporter 2 routes via des interfaces externes. Tout d'abord, pour la connexion de l'interface externe principale au FAI principal.

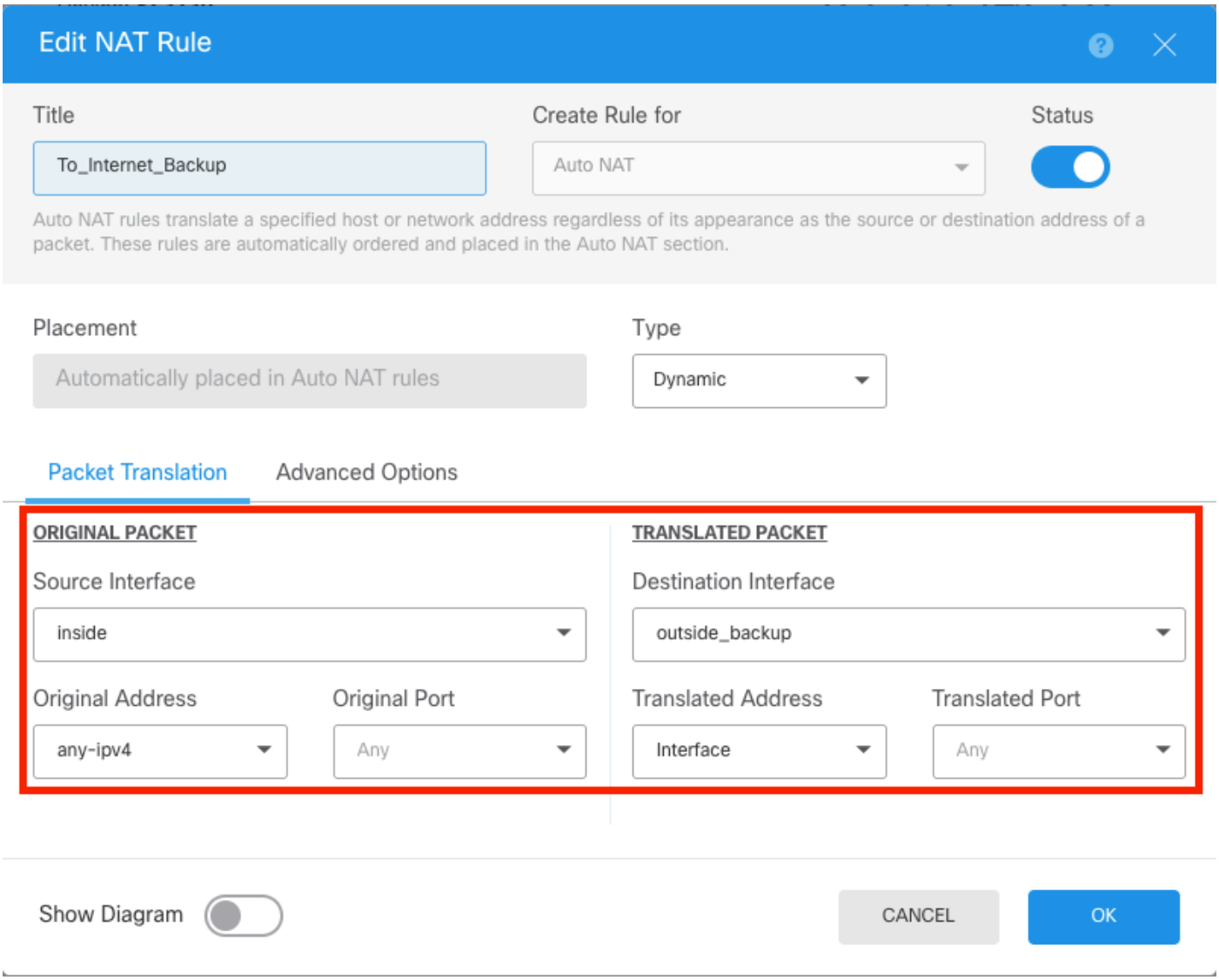


NAT pour ISP principal

Étape 20.

Maintenant, une deuxième NAT pour la connexion ISP secondaire.

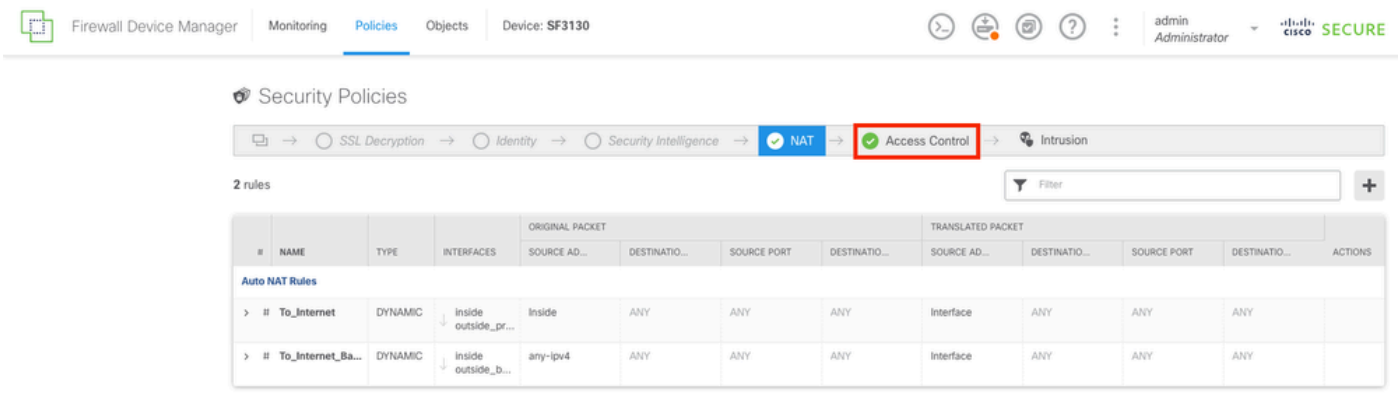
Remarque : Pour l'adresse d'origine, le même réseau ne peut pas être utilisé. Dans cet exemple, pour le FAI secondaire, l'adresse d'origine est l'objet any-ipv4.



NAT pour ISP secondaire

Étape 21.

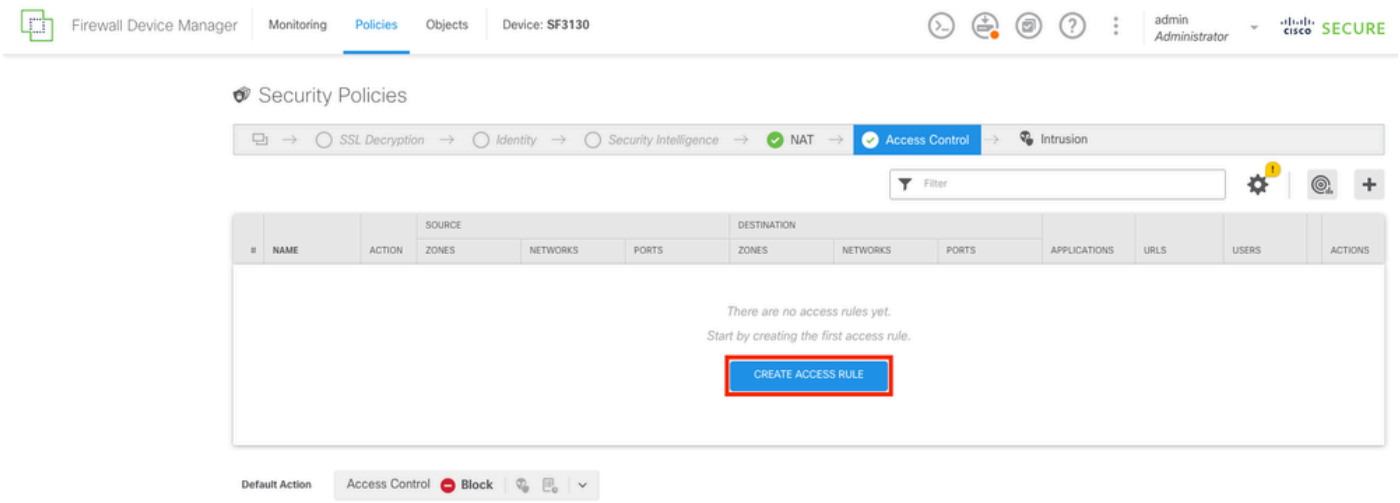
Après avoir créé les deux règles NAT, une règle de contrôle d'accès doit être établie pour autoriser le trafic sortant. Cliquez sur le bouton Contrôle d'accès.



Règles NAT créées

Étape 22.

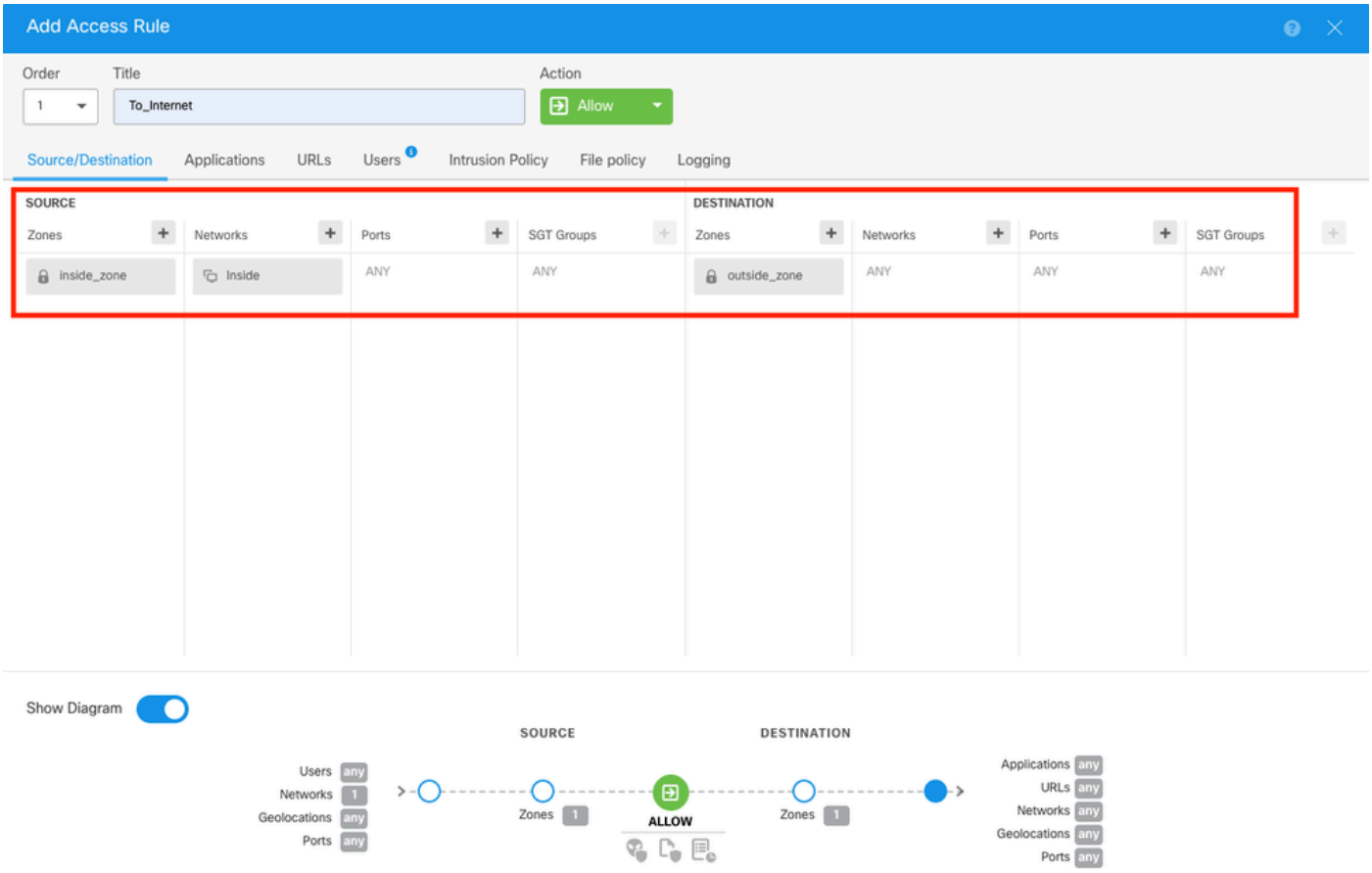
Pour créer la règle de contrôle d'accès, cliquez sur le bouton CREATE ACCESS RULE.



Section de contrôle d'accès

Étape 23.

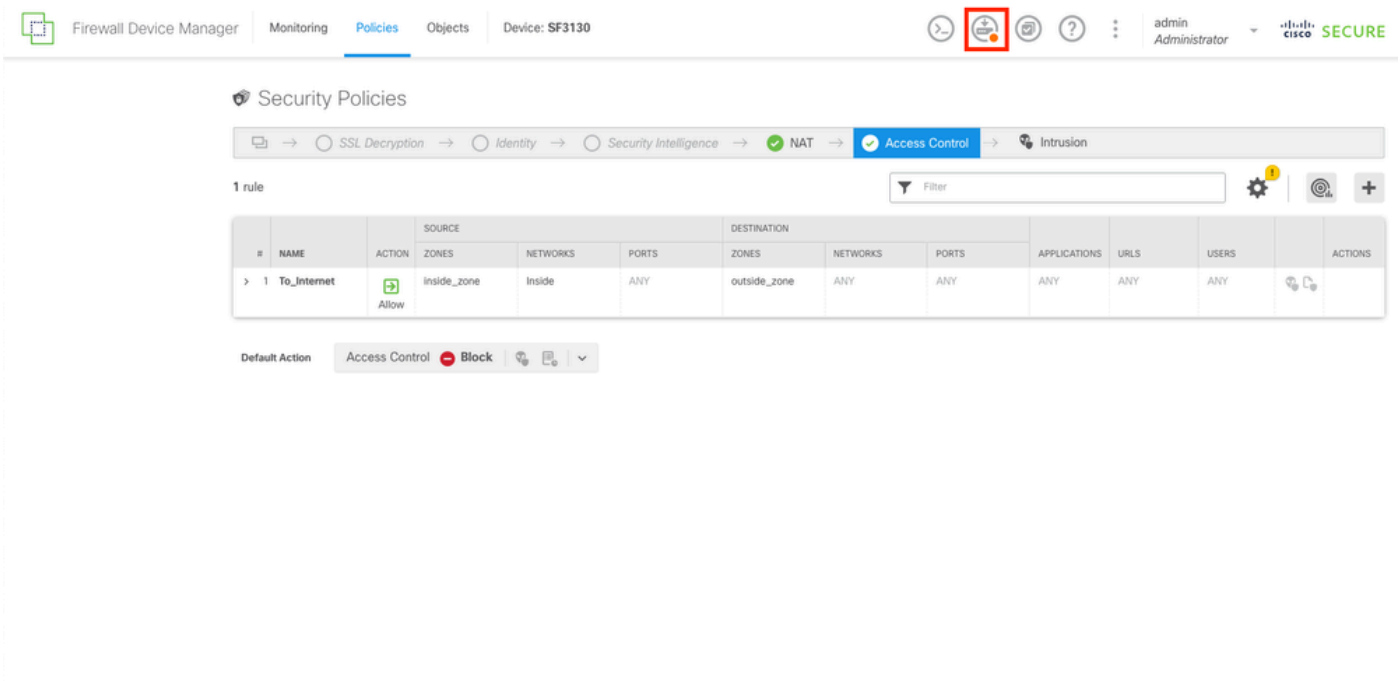
Sélectionnez les zones et les réseaux souhaités.



règle de contrôle d'accès

Étape 24.

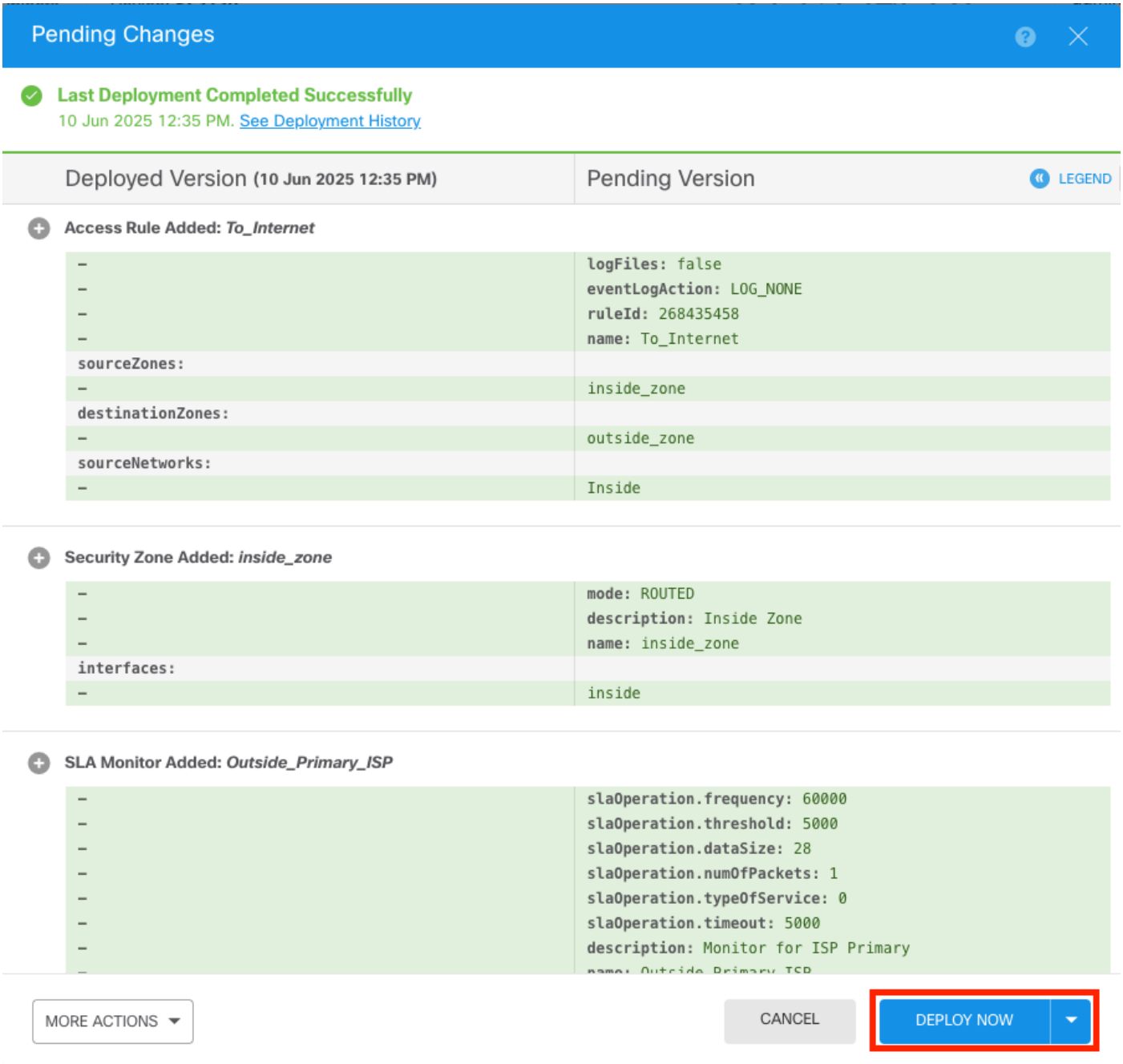
Une fois la règle de contrôle d'accès créée, poursuivez le déploiement de toutes les modifications en sélectionnant le bouton Déployer en haut.



Règle de contrôle d'accès créée

Étape 25.

Vérifiez les modifications, puis cliquez sur le bouton Déployer maintenant.



Vérification du déploiement

Diagramme du réseau

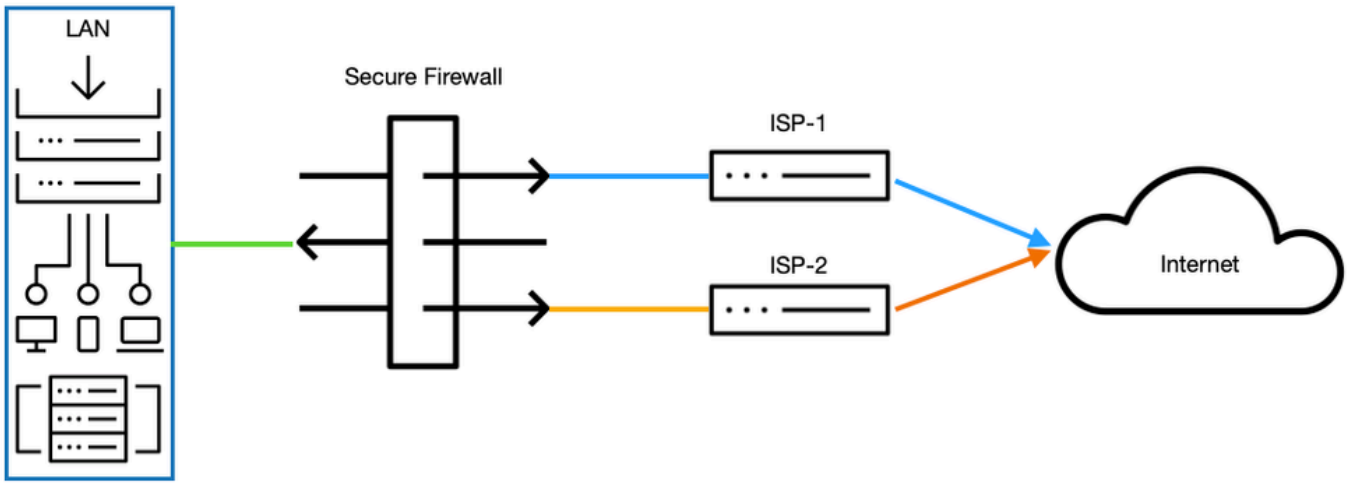


Diagramme du réseau

Vérifier

<#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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.