تكوين ISP المزدوج على FTD باستخدام FDM

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

الرسم التخطيطي للشبكة

التحقق من الصحة

المقدمة

يوضح هذا المستند كيفية تكوين تجاوز فشل موفر خدمة الإنترنت المزدوج (ISP) باستخدام مدير أجهزة جدار الحماية (FDM) لسلسلة جدار الحماية الآمن.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- التوجيه الأساسي
- معرفة لوحة معلومات إدارة أجهزة جدار الحماية

- تم توصيل موفري خدمة إنترنت على الأقل بجدار الحماية الآمن.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

· تشغيل جدار الحماية الآمن من Cisco من الإصدار 7.7.x أو الإصدارات الأحدث.

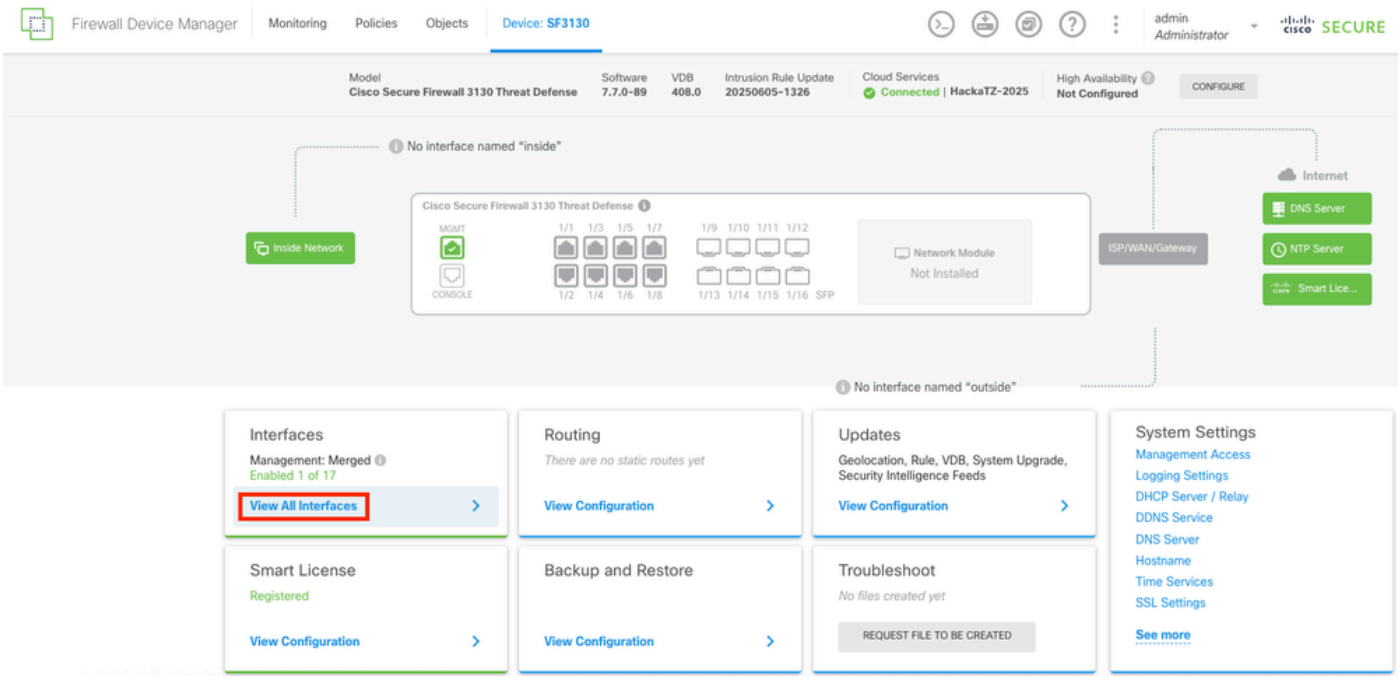
· جدار الحماية الآمن 3130 مع الإصدار 7.7.0.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. تم بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الخطوة 1.

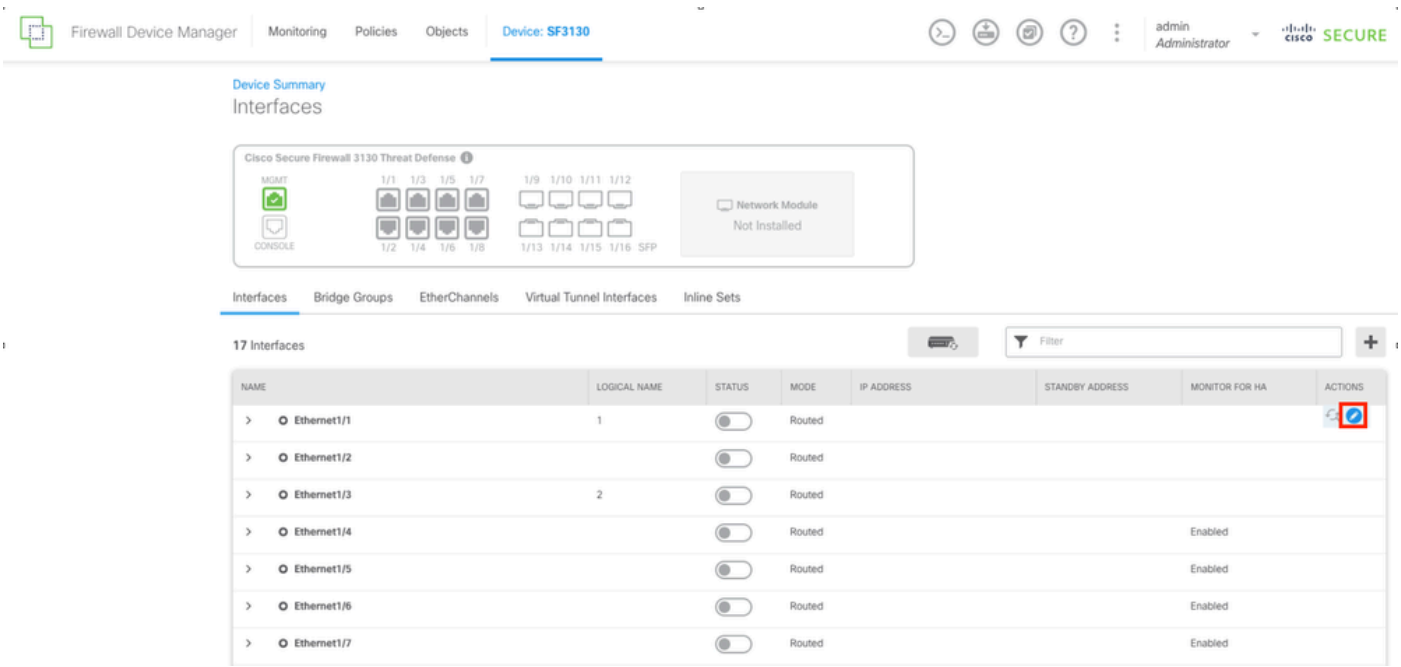
سجل الدخول إلى FDM على جدار الحماية الآمن، وتنقل إلى قسم الواجهات من خلال تحديد الزر عرض جميع الواجهات.



لوحة المعلومات الرئيسية ل FDM

الخطوة 2.

لتكوين الواجهة لاتصال ISP الأساسي، ابدأ بتحديد الواجهة المطلوبة. تحديد زر الواجهة المطابقة للمتابعة. في هذا المثال، الواجهة المستخدمة هي Ethernet1/1.

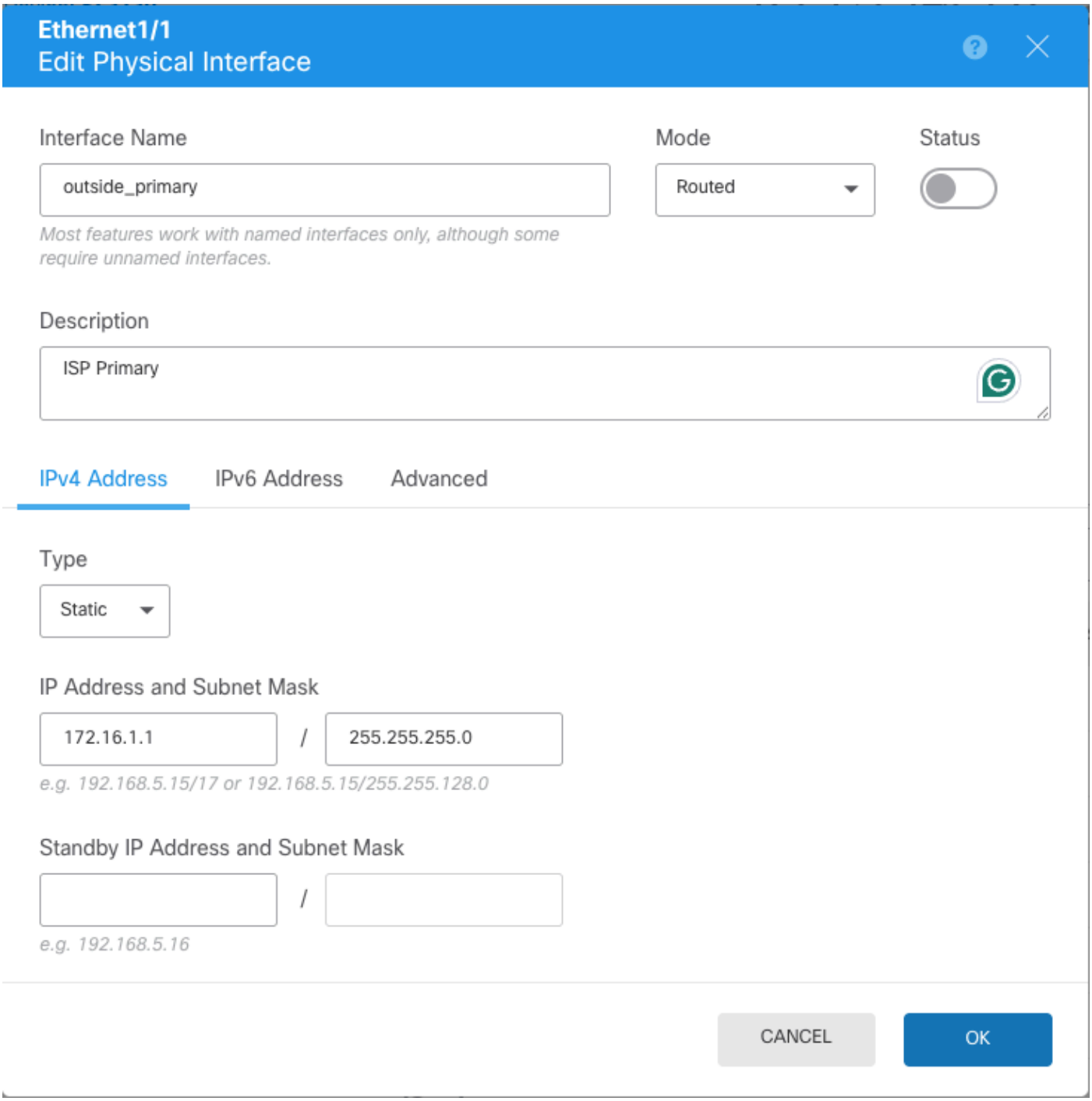


علامة تبويب الواجهات

الخطوة 3.

قم بتكوين الواجهة باستخدام المعلمات الصحيحة لاتصال ISP الأساسي لديك. في هذا

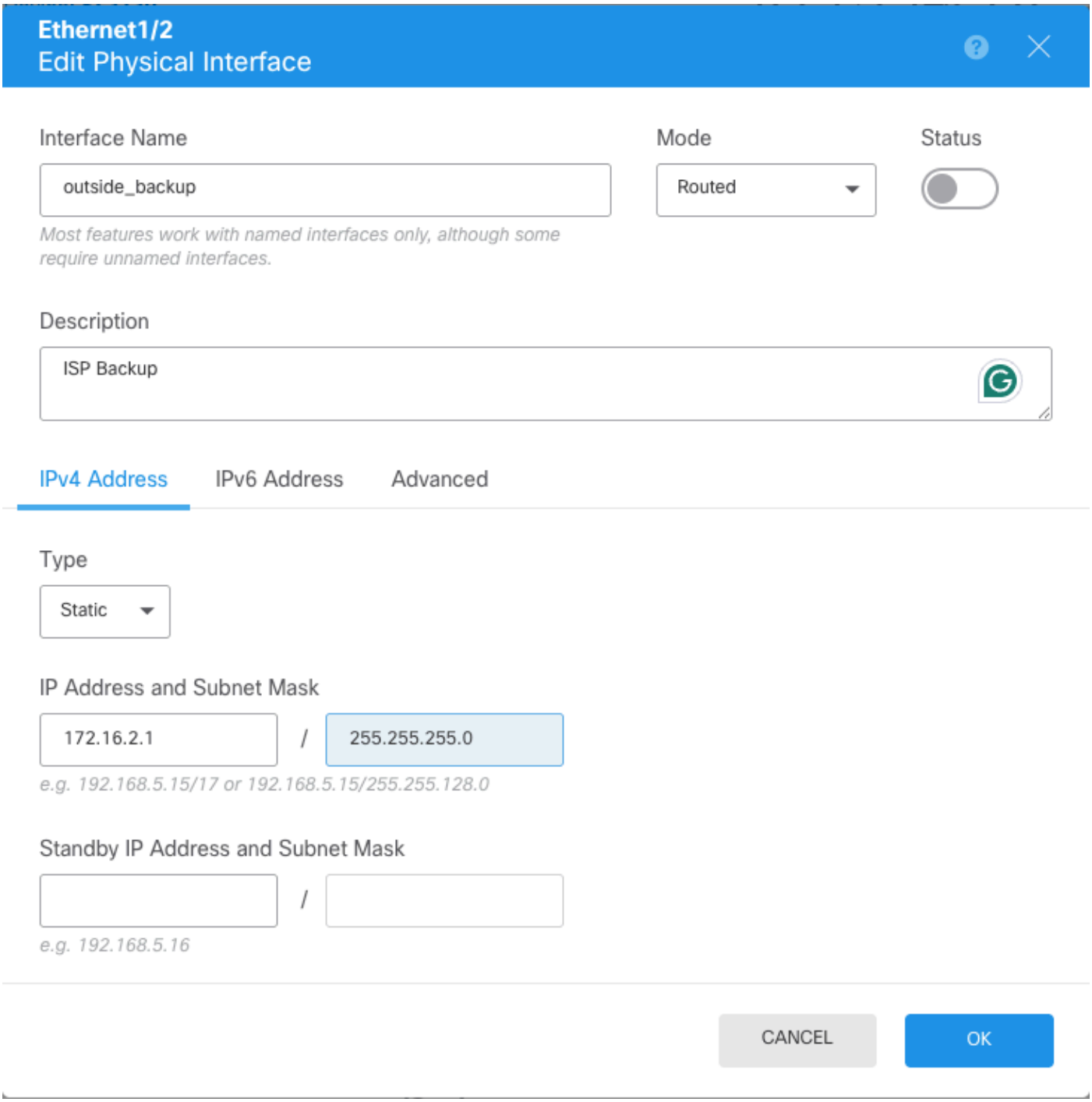
مثال، القارن خارج_أساسي.



تكوين واجهة ISP الأساسية

الخطوة 4.

كرر نفس العملية لواجهة ISP الثانوية. في هذا المثال، يتم إستخدام الواجهة Ethernet1/2.

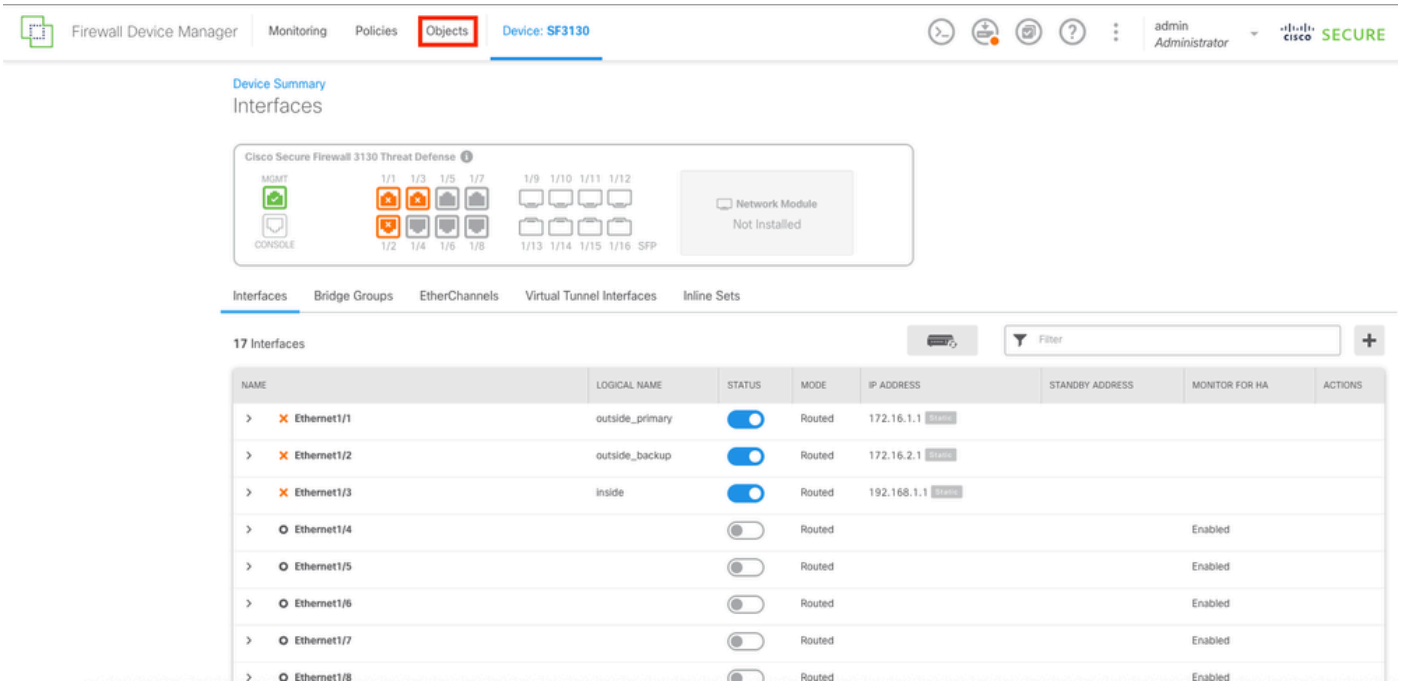


تكوين واجهة ISP الثانوية

الخطوة 5.

بعد تكوين الواجهات ل ISPs، تتمثل الخطوة التالية في إعداد مراقبة SLA للواجهة الأساسية.

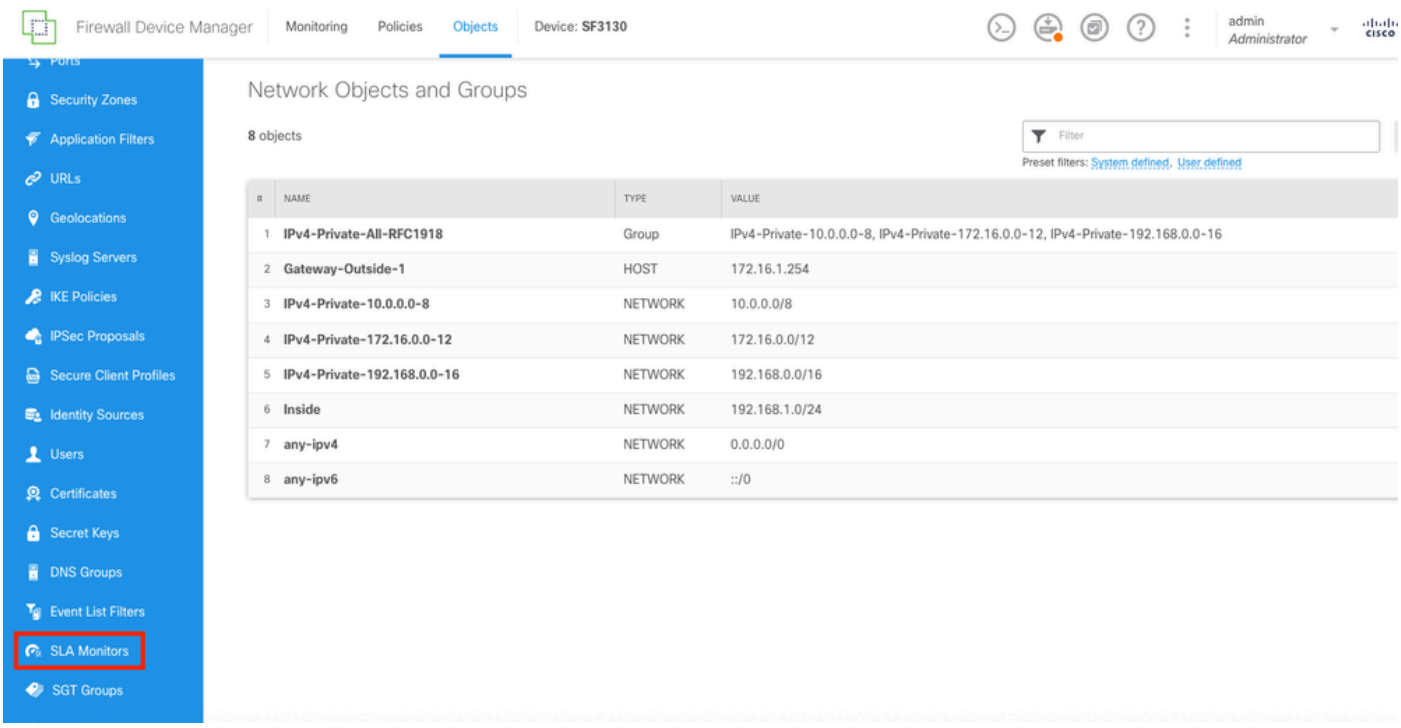
انتقل إلى قسم الكائنات بتحديد زر الكائنات الموجود في أعلى القائمة.



الواجهات التي تم تكوينها

الخطوة 6.

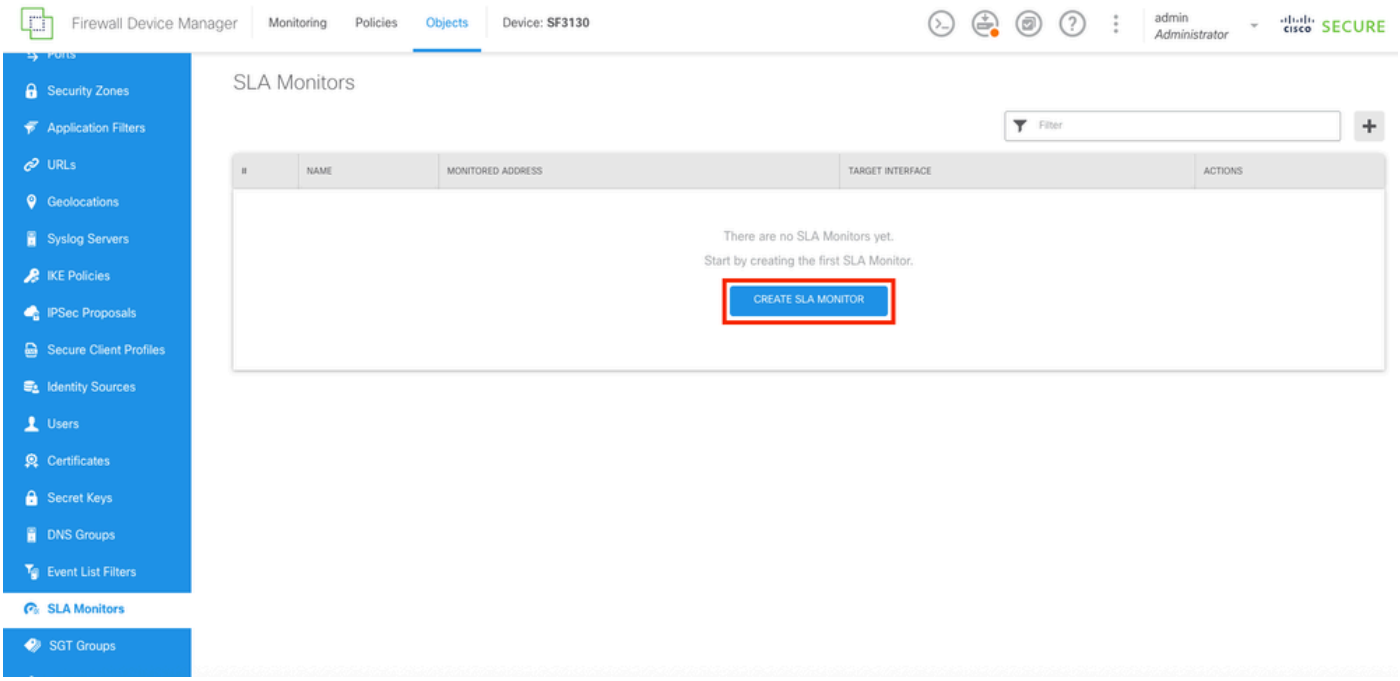
حدد في العمود الأيسر، زر شاشات SLA.



شاشة الكائنات

الخطوة 7.

إنشاء شاشة SLA جديدة عن طريق تحديد الزر إنشاء شاشة SLA.



قسم مراقبة SLA

الخطوة 8.

قم بتكوين معلمات اتصال ISP الأساسي.

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

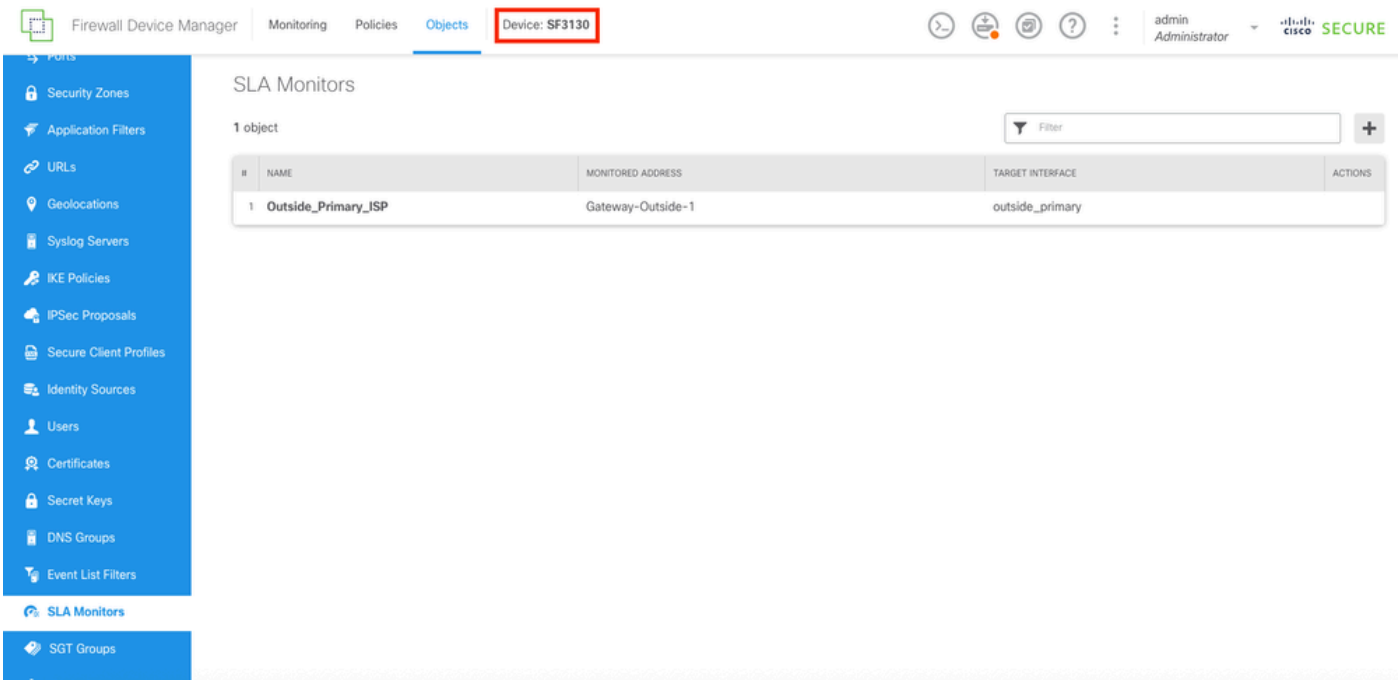
0 - 16384

CANCEL OK

إنشاء كائن SLA

الخطوة 9.

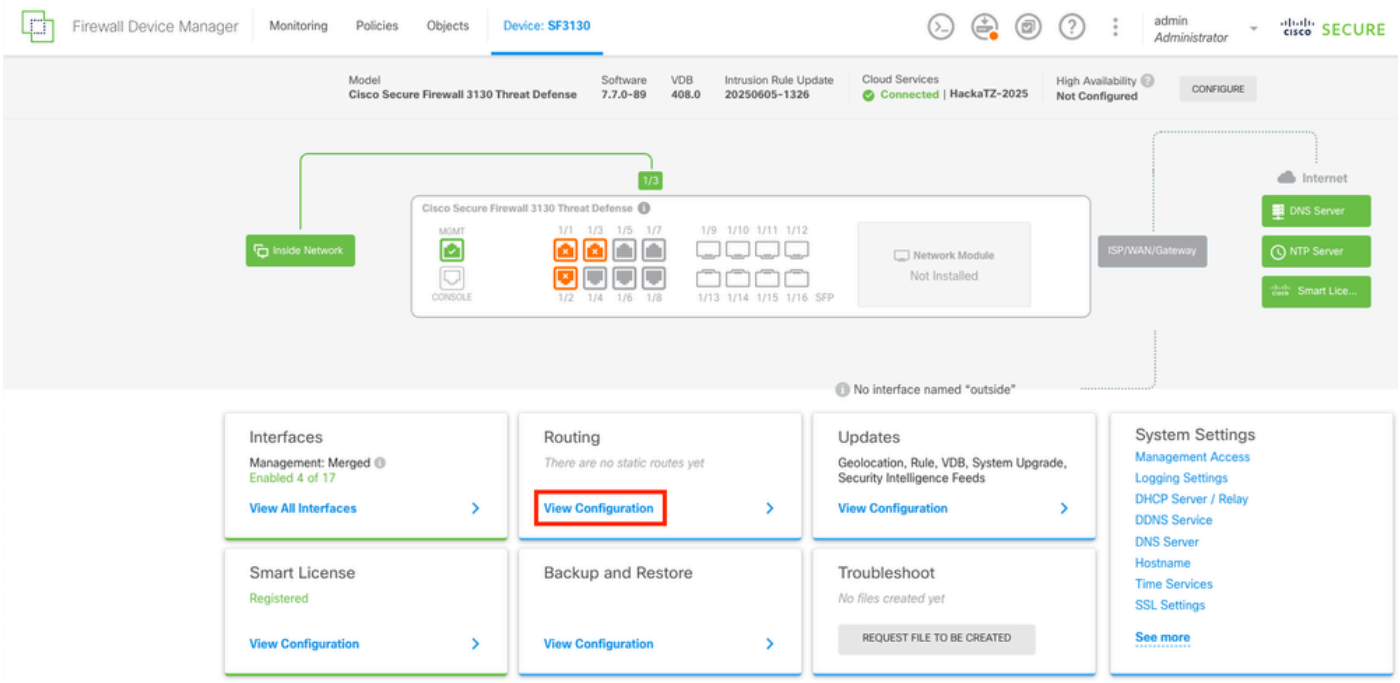
بمجرد إنشاء الكائن، يجب أن يقوم المسار الثابت للواجهات بإنشائه. انتقل إلى لوحة المعلومات الرئيسية بتحديد زر الجهاز.



تم إنشاء شاشة SLA

الخطوة 10.

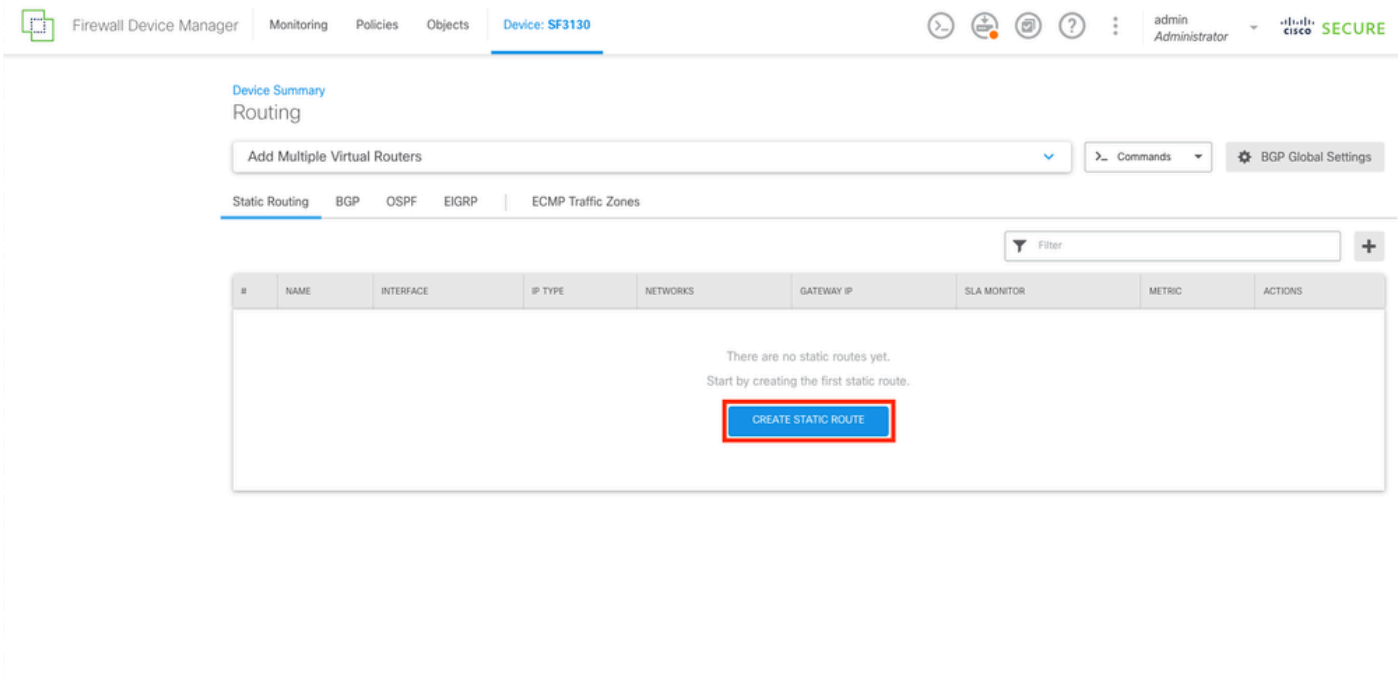
انتقل إلى قسم التوجيه بتحديد تكوين عرض في لوحة التوجيه.



لوحة المعلومات الرئيسية

الخطوة 11.

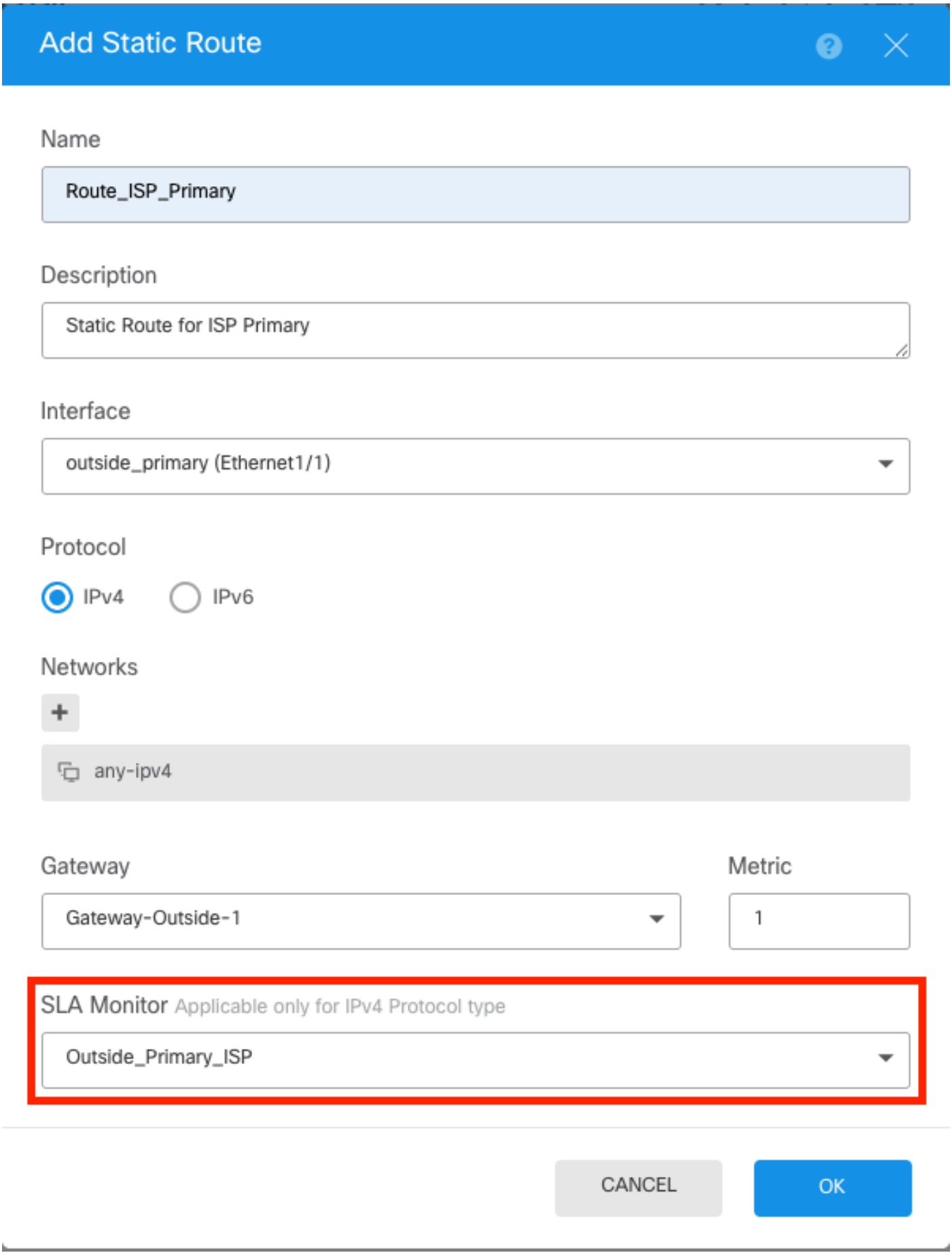
في علامة التبويب "توجيه ثابت"، قم بإنشاء 2 مسارات ثابتة افتراضية لكل من موفري خدمات الإنترنت (ISPs). لإنشاء مسار ثابت جديد، حدد الزر إنشاء مسار ثابت.



قسم التوجيه الثابت

الخطوة 12.

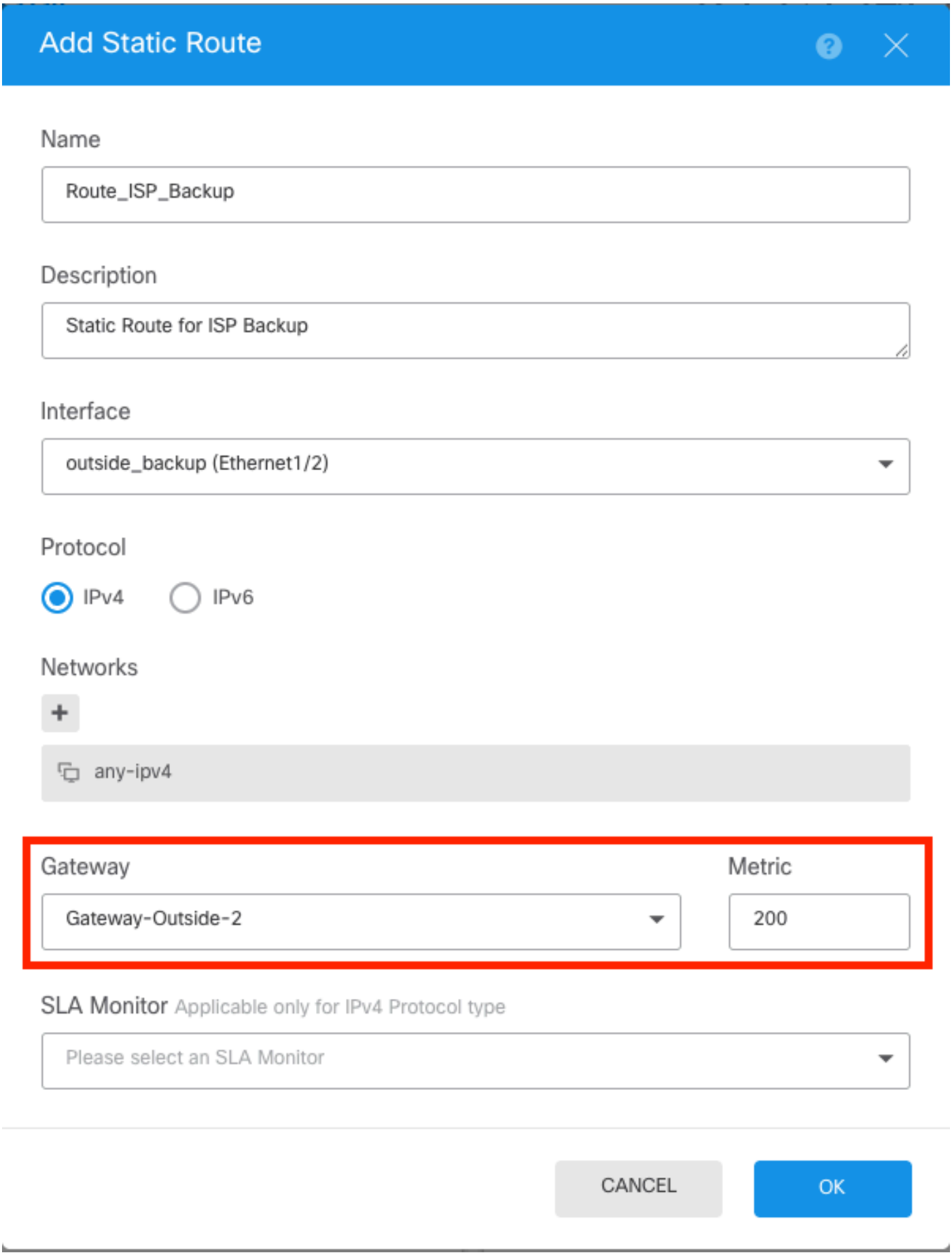
أولا، قم بإنشاء المسار الثابت ل ISP الأساسي. في النهاية، أضف كائن مراقبة SLA الذي تم إنشاؤه في الخطوة الأخيرة.



المسار الثابت ل ISP الأساسي

الخطوة 13.

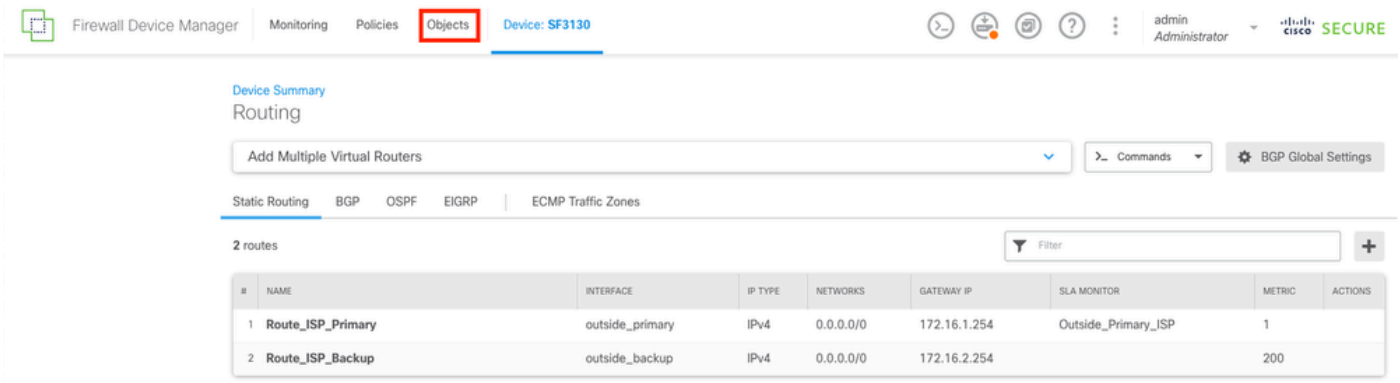
قم بتكرار الخطوة الأخيرة وإنشاء مسار افتراضي، ل ISP الثانوية باستخدام العبارة المناسبة والمقياس المختلف. في هذا المثال، تمت زيادته إلى 200.



المسار الثابت ل ISP الثانوي

الخطوة 14.

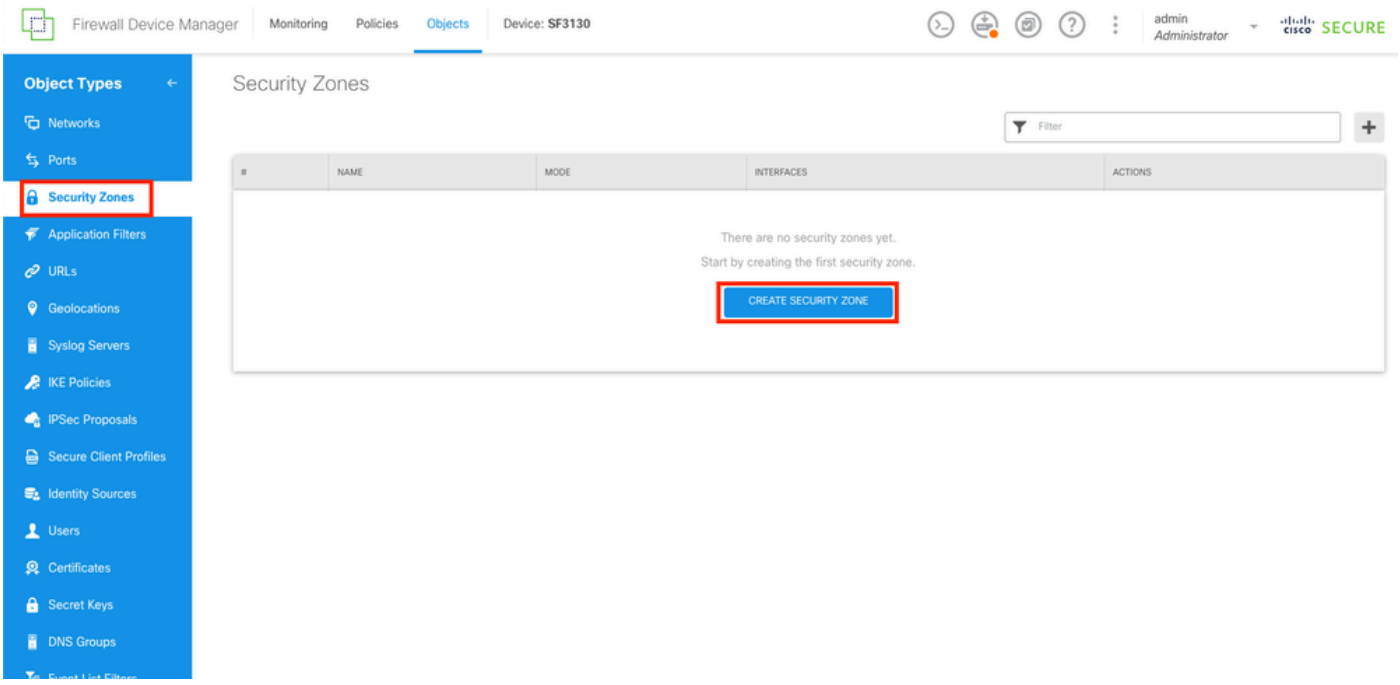
بمجرد إنشاء كل الموجهين الثابتين، يجب إنشاء منطقة أمان. انتقل إلى قسم الكائنات بتحديد زر الكائنات الموجود بالأعلى.



المسارات الثابتة التي تم إنشاؤها

الخطوة 15.

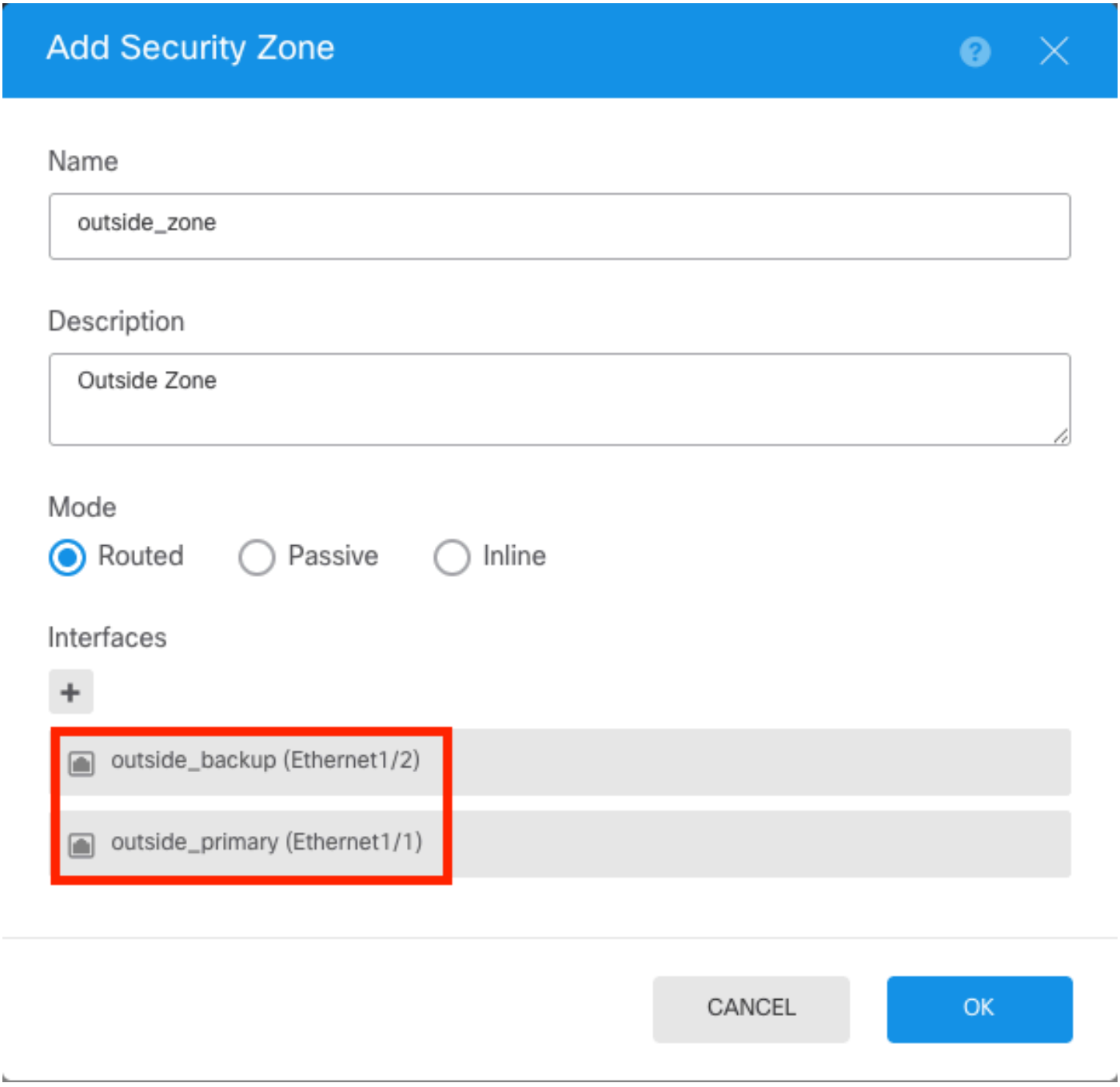
انتقل إلى قسم مناطق الأمان عن طريق تحديد الزر مناطق الأمان في العمود الأيسر، ثم قم بإنشاء منطقة جديدة عن طريق تحديد الزر إنشاء منطقة أمان.



قسم المناطق الأمنية

الخطوة 16.

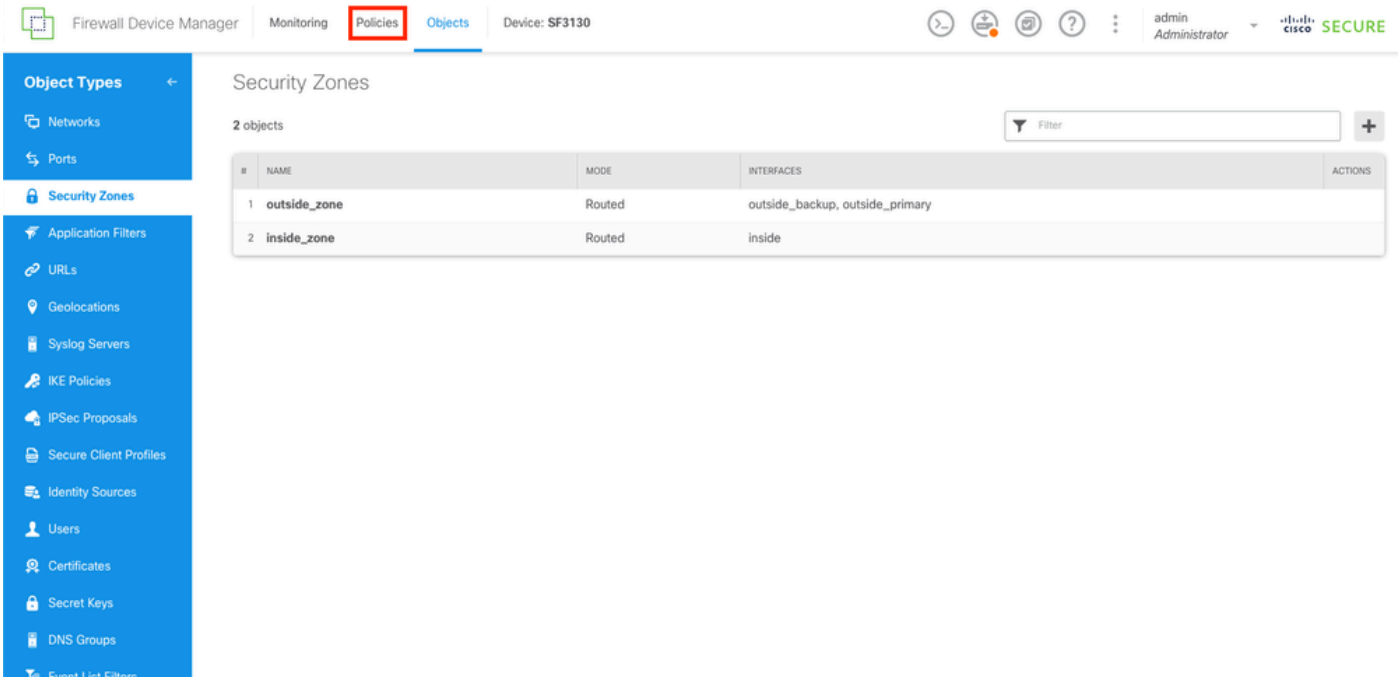
قم بإنشاء منطقة الأمان الخارجية باستخدام كل الواجهات الخارجية لاتصالات ISPs.



المنطقة الأمنية في الخارج

الخطوة 17.

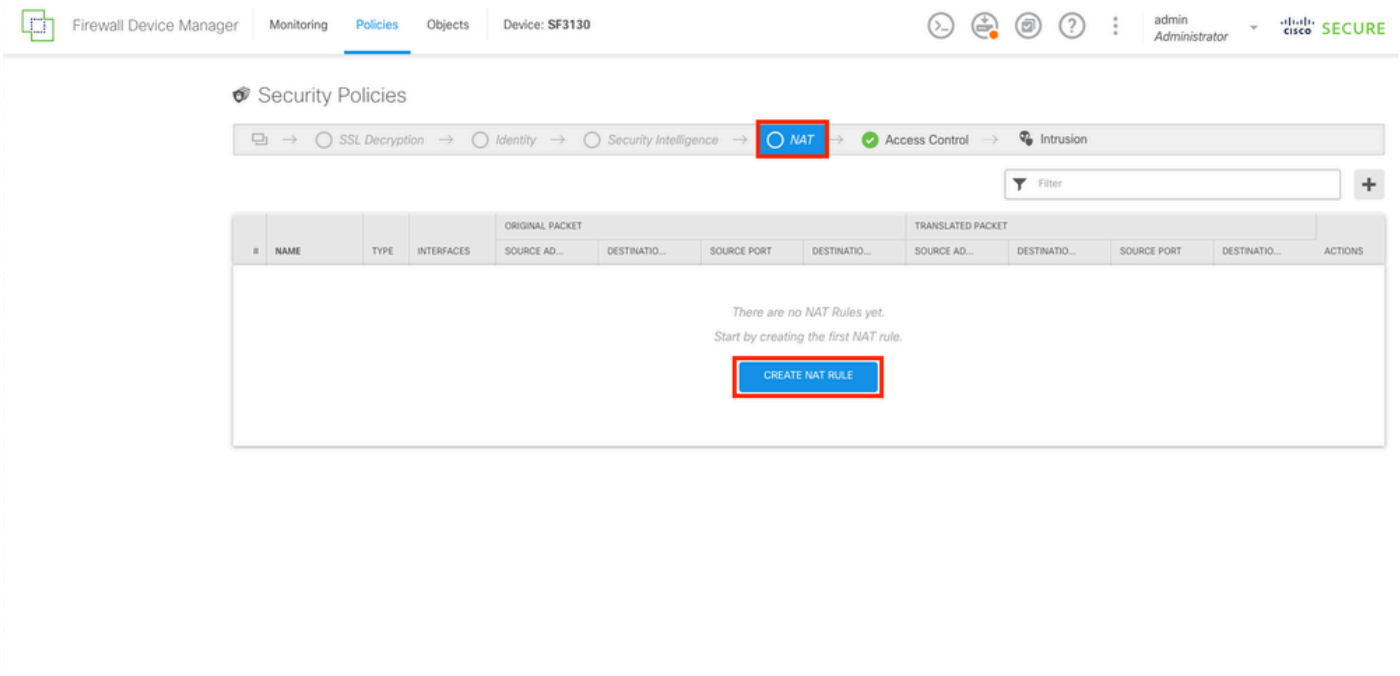
بعد إنشاء منطقة الأمان، يجب إنشاء NAT. انتقل إلى قسم السياسات بتحديد الزر نهج في الأعلى.



إنشاء مناطق الأمان

الخطوة 18.

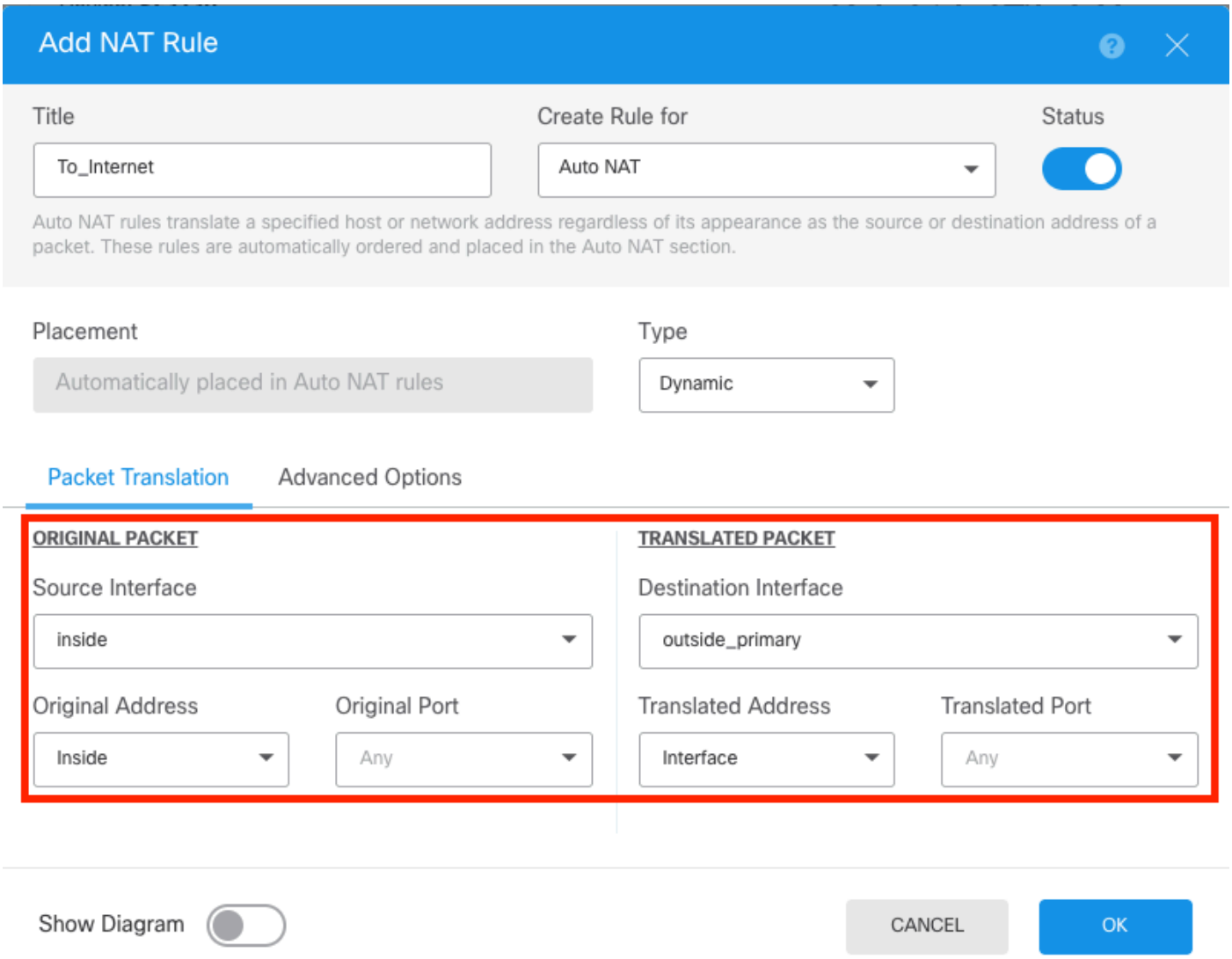
انتقل إلى قسم nat بتحديد زر nat، ثم قم بإنشاء قاعدة جديدة بتحديد الزر إنشاء قاعدة nat.



قسم nat

الخطوة 19.

بالنسبة لتجاوز فشل بروتوكول ISP، يجب أن يكون للتكوين مسحاج تخديد عبر الواجهات الخارجية. أولا، اتصال الواجهة الخارجية الأساسية ب ISP الأساسي.

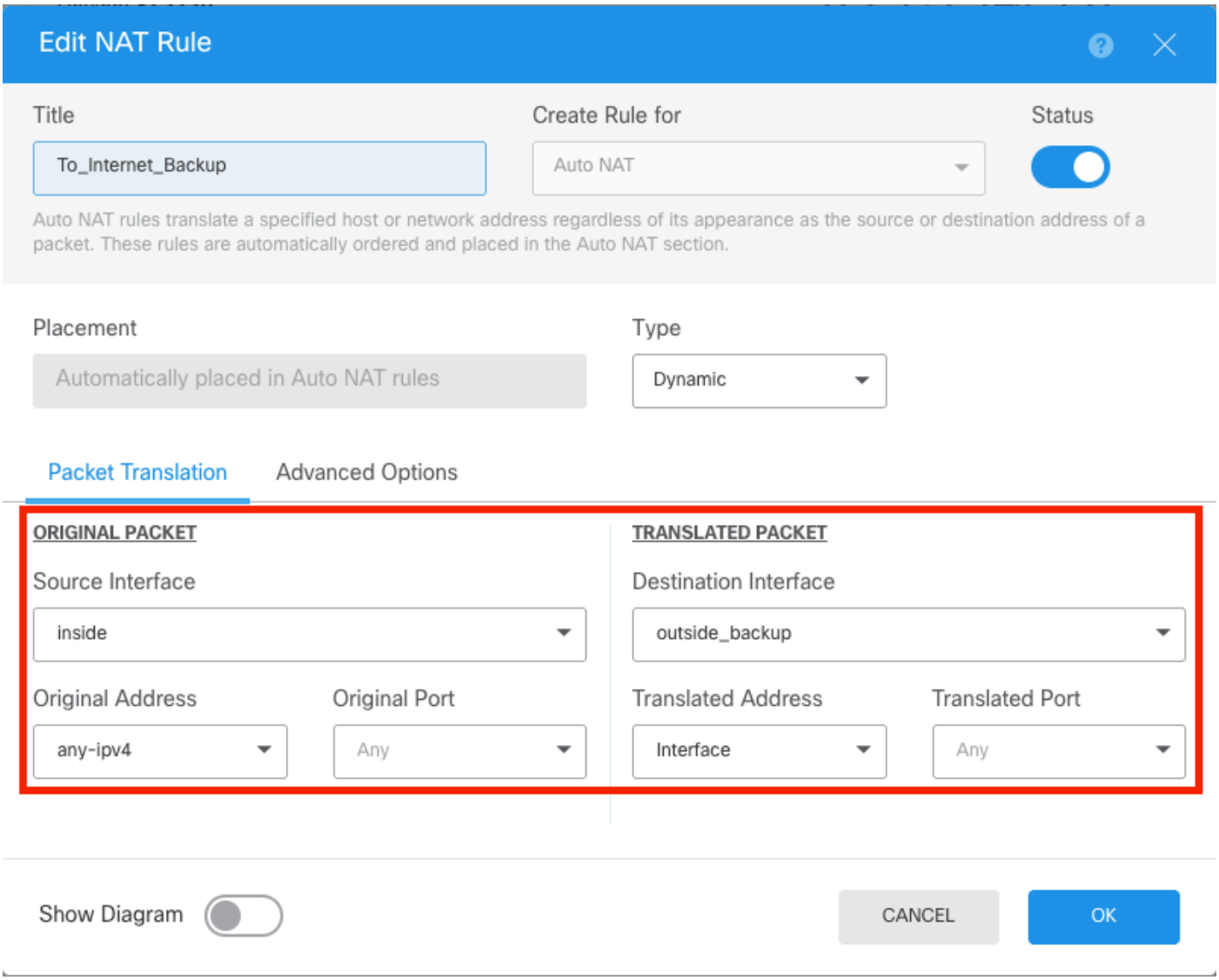


NAT ل ISP أساسي

الخطوة 20.

الآن، nat ثان لاتصال ISP الثانوي.

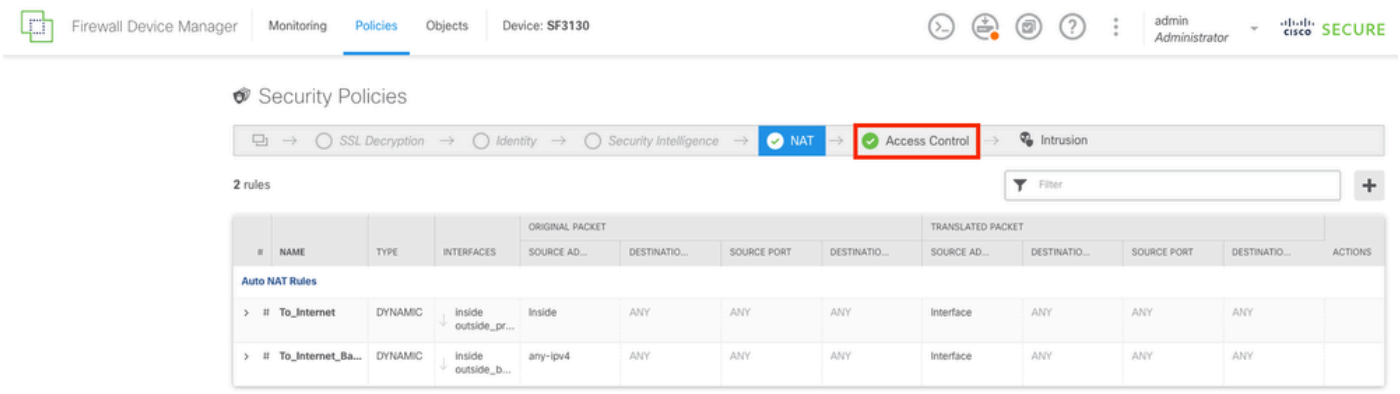
ملاحظة: للعنوان الأصلي، لا يمكن إستخدام نفس الشبكة. في هذا المثال، بالنسبة لموفر خدمات الإنترنت الثانوي، يكون العنوان الأصلي هو الكائن any-IPv4.



NAT ل ISP الثانوي

الخطوة 21.

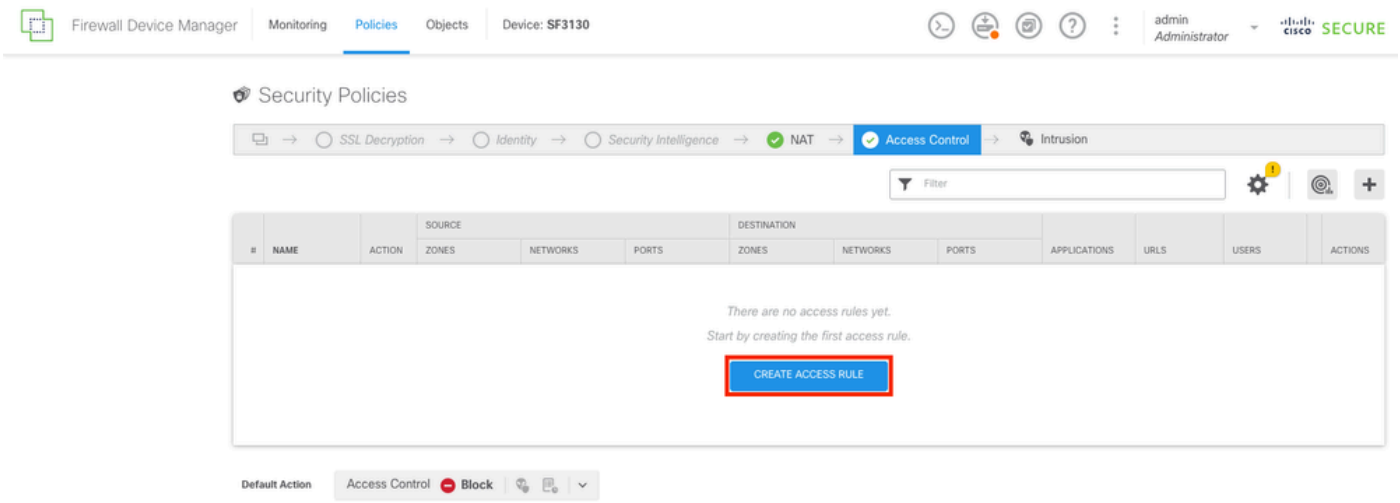
بعد إنشاء كل من قواعد NAT، يجب إنشاء قاعدة التحكم في الوصول للسماح بحركة المرور الصادرة. حدد الزر التحكم في الوصول.



تم إنشاء قواعد NAT

الخطوة 22.

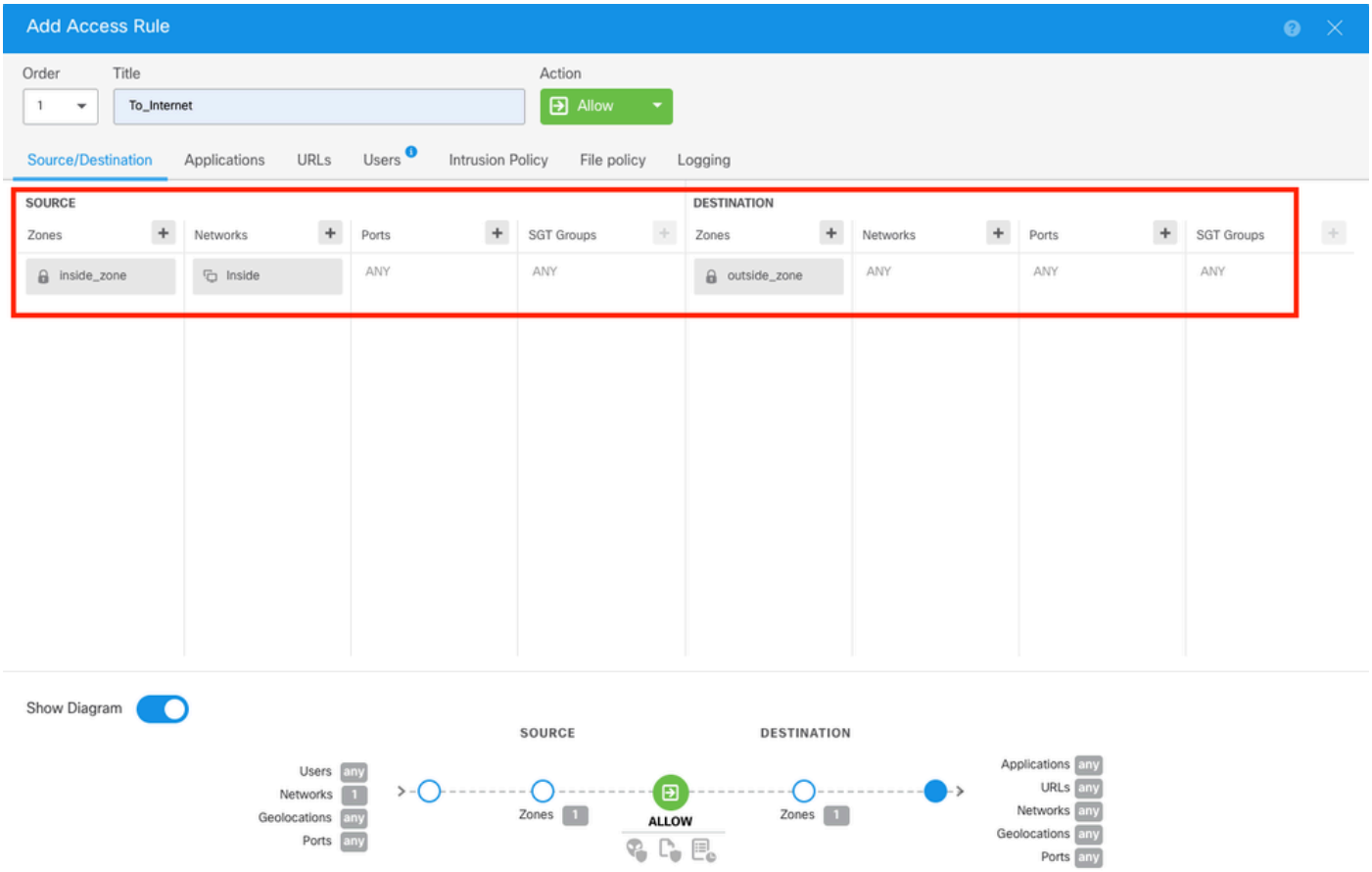
لإنشاء قاعدة التحكم بالوصول، حدد الزر إنشاء قاعدة وصول.



قسم التحكم في الوصول

الخطوة 23.

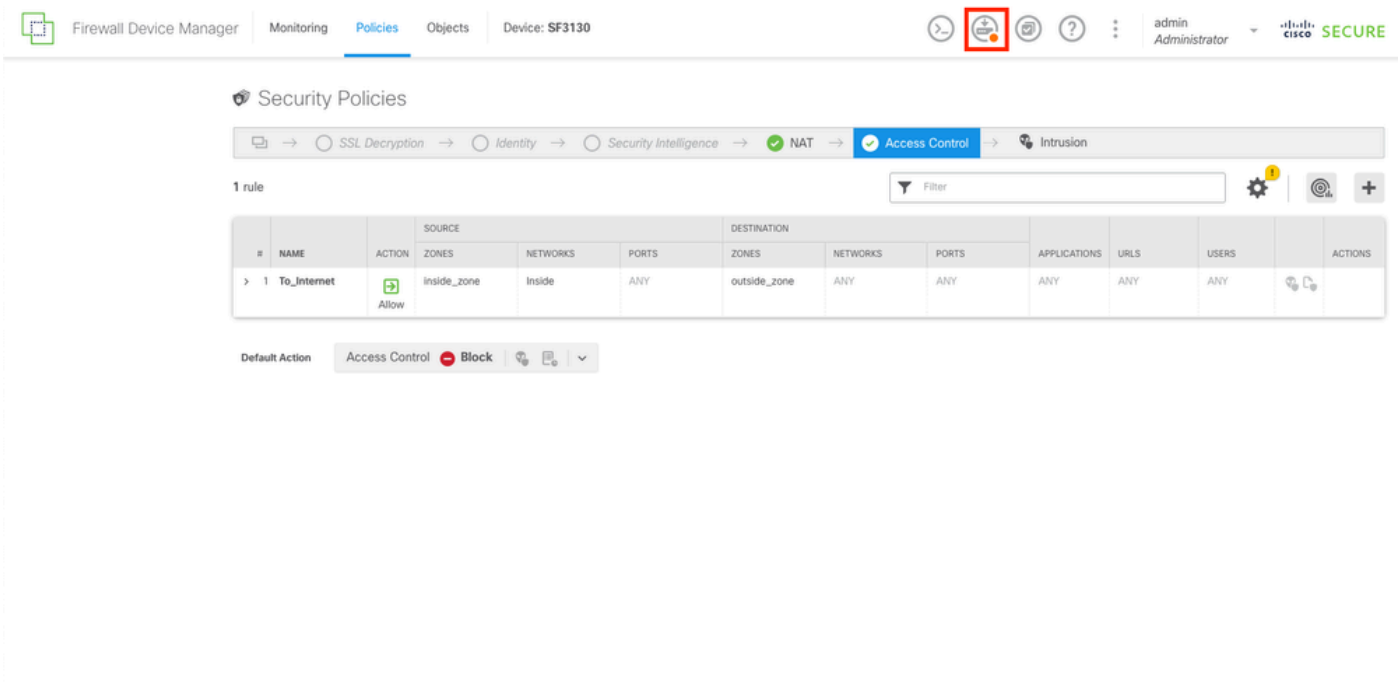
حدد المناطق والشبكات المطلوبة.



قاعدة التحكم في الوصول

الخطوة 24.

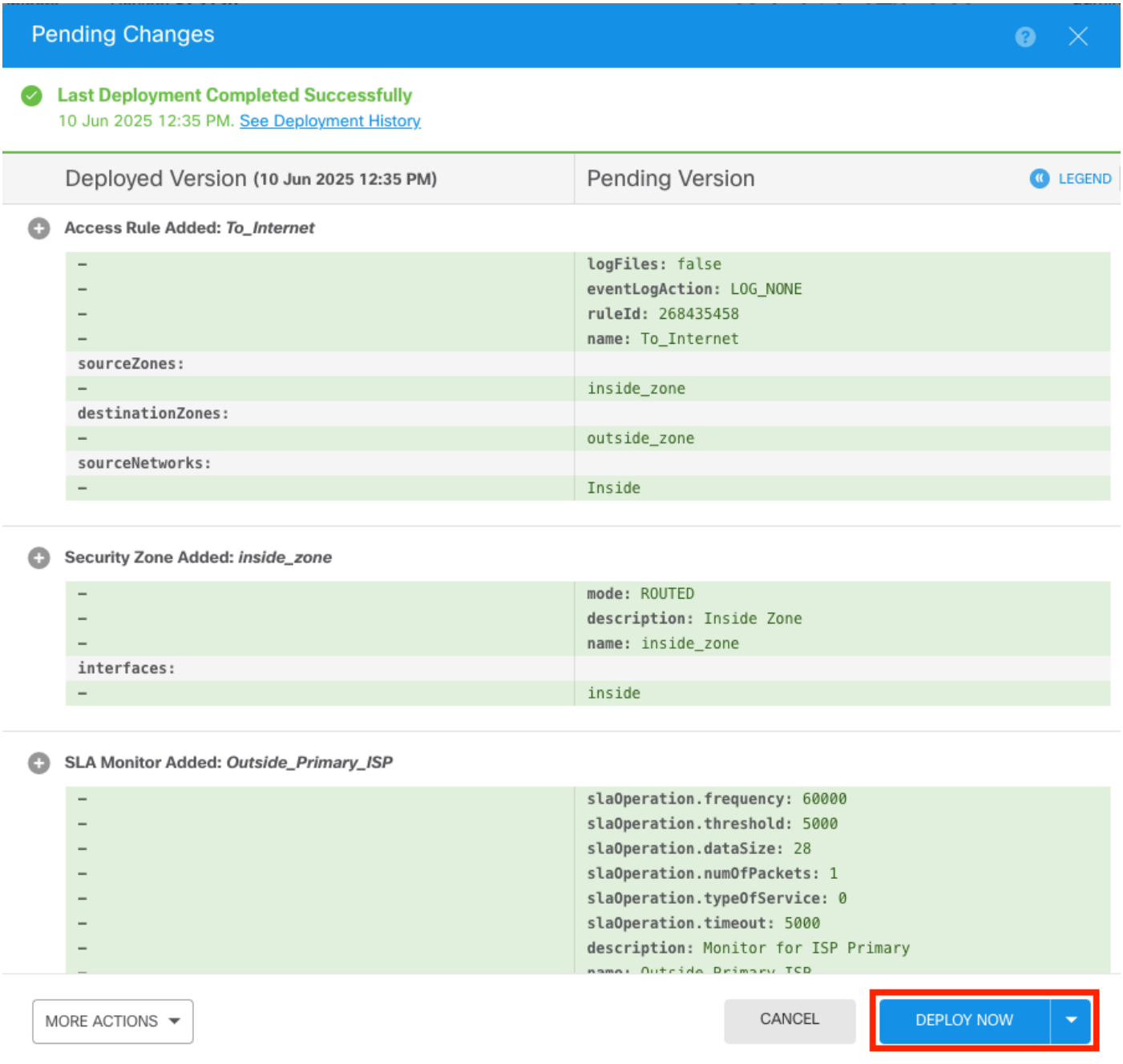
بمجرد إنشاء "قاعدة التحكم بالوصول"، قم بالمتابعة لنشر كافة التغييرات عن طريق تحديد الزر نشر الموجود بالأعلى.



تم إنشاء قاعدة التحكم بالوصول

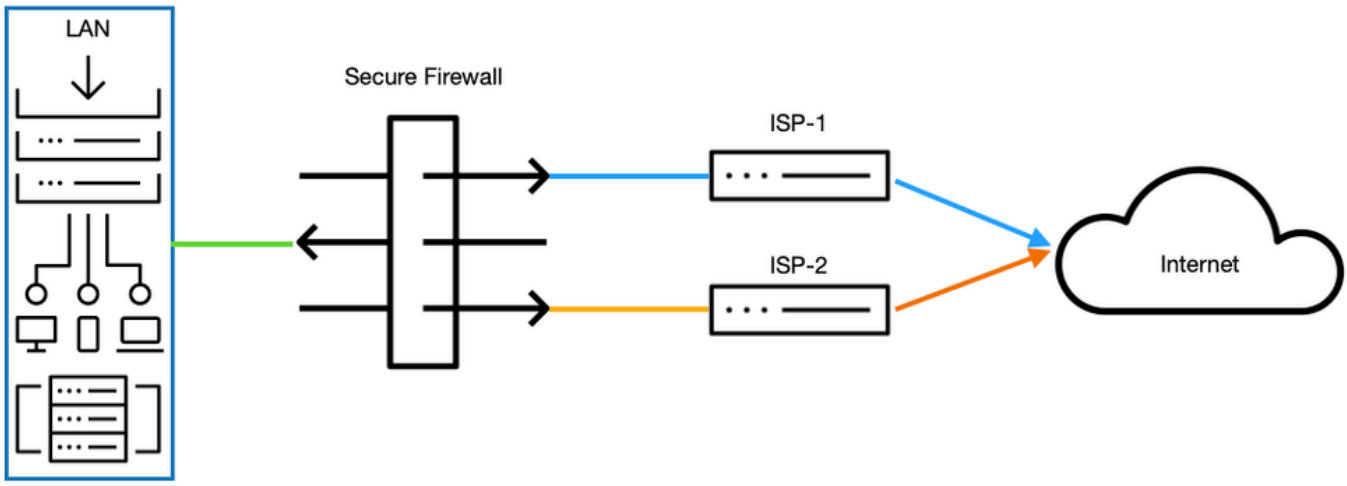
الخطوة 25.

تحقق من التغييرات ثم حدد الزر نشر الآن.



التحقق من النشر

الرسم التخطيطي للشبكة



الرسم التخطيطي للشبكة

التحقق من الصحة

<#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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).