تكوين تجاوز الأعطال لأنفاق IPSec من موقع إلى موقع باستخدام إرتباطات ISP الاحتياطية على FTD المدارة بواسطة FMC

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين تجاوز الفشل المستند إلى خريطة التشفير لارتباط ISP باستخدام ميزة تعقب IP SLA على FTD التي تتم إدارتها بواسطة FMC.

تمت المساهمة من قبل أمانداب ناثاني، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- المفهوم الأساسي لشبكة خاصة ظاهرية (VPN)
- تجربة إستخدام برنامج FTD
- تجربة مع FMC
- تجربة مع سطر أوامر أجهزة الأمان المعدلة (ASA)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- FMC، الإصدار 6.6.0
- FTD، الإصدار 6.6.0
- الإصدار 9.14.1 من أجهزة الأمان التكيفي (ASA)

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

معلومات أساسية

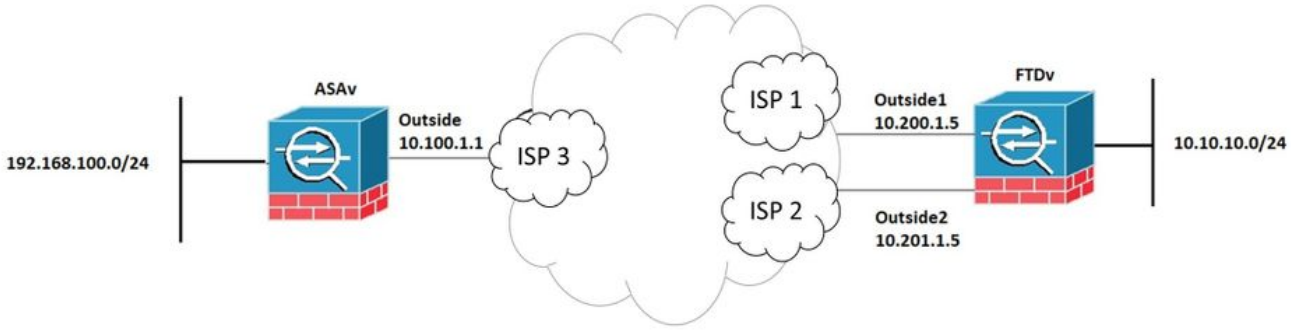
يوضح هذا المستند كيفية تكوين تجاوز الفشل المستند إلى خريطة التشفير للنسخ الاحتياطي لارتباط موزع خدمة الإنترنت (ISP) باستخدام ميزة تعقب "إتفاقية مستوى خدمة (IP SLA)" على "الدفاع عن تهديد الطاقة النارية (FTD)" التي يديرها FirePOWER (FMC). وهو يشرح أيضا كيفية تكوين إعفاء ترجمة عنوان الشبكة (NAT) لحركة مرور الشبكة الخاصة الظاهرية (VPN) عندما يكون هناك موصل خدمات الإنترنت (ISP) ويتطلب تجاوز الفشل بسلاسة.

في هذا السيناريو، يتم إنشاء الشبكة الخاصة الظاهرية (VPN) من FTD تجاه ASA كنظير. يستخدم FTD إرتباط ISP واحد فقط. واجهة ISP باستخدام الشبكة الخاصة الظاهرية (VPN). عند تعطل إرتباط موزد خدمة واحد في ذلك الوقت لإنشاء الشبكة الخاصة الظاهرية (VPN)، يتولى "برنامج الإرسال فائق السرعة (FTD)" الأمر من خلال الأساسي، مزود خدمة الإنترنت (ISP) من خلال أداة المراقبة التابعة لارتباط الثانوي القائم على مزود خدمة الإنترنت (ISP) ويتم إنشاء الشبكة الخاصة الظاهرية (VPN) لاتفاقية مستوى الخدمة (SLA).

التكوين

الرسم التخطيطي للشبكة

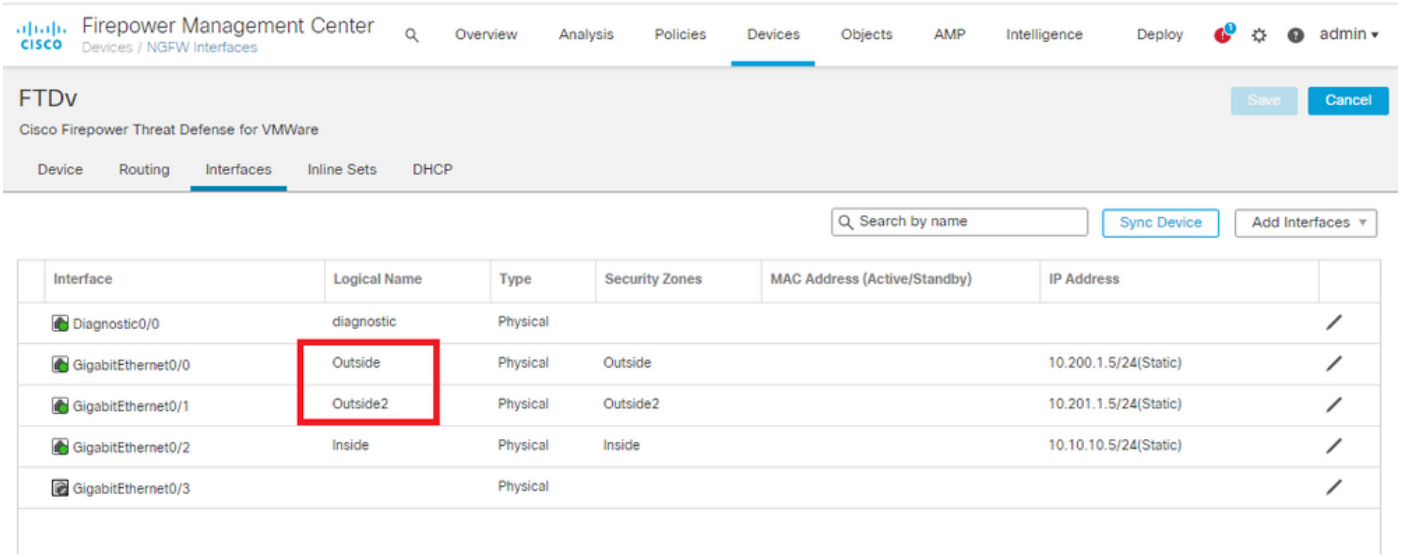
هذا هو المخطط المستخدم للمثال في هذا المستند:



تكوين FTD

الخطوة 1. تحديد واجهات ISP الأساسية والثانوية

1. انتقل إلى الأجهزة > إدارة الأجهزة > الواجهات كما هو موضح في الصورة.

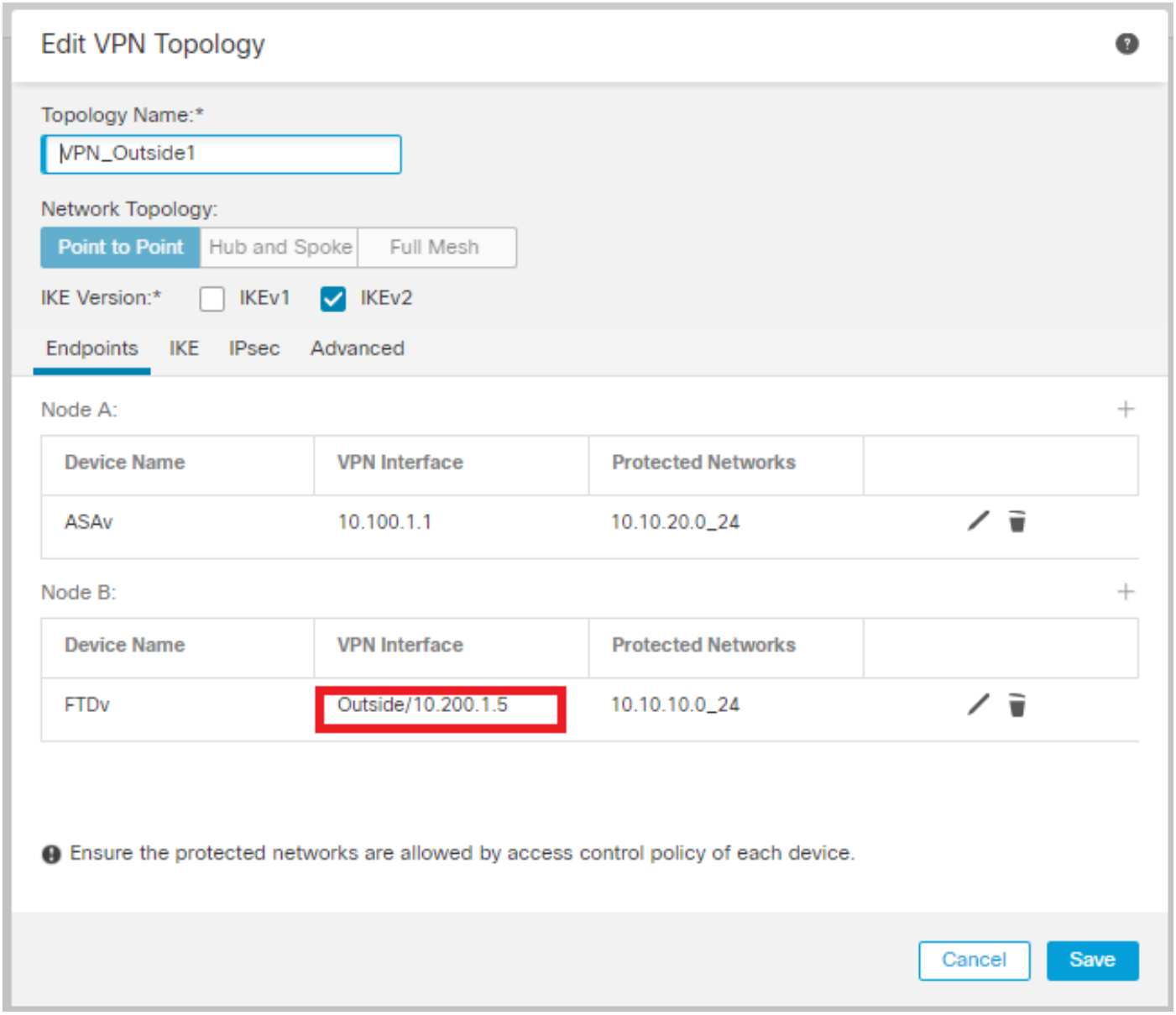


الخطوة 2. تحديد مخطط شبكة VPN لواجهة ISP الأساسية

1. انتقل إلى الأجهزة > VPN > موقع إلى موقع. تحت إضافة شبكة VPN، انقر فوق جهاز الدفاع ضد تهديد FirePOWER، وقم بإنشاء شبكة VPN وحدد الواجهة الخارجية.

ملاحظة: لا يصف هذا المستند كيفية تكوين شبكة VPN S2S من البداية. لمزيد من المرجع لتكوين S2S VPN على FTD، انتقل إلى https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html

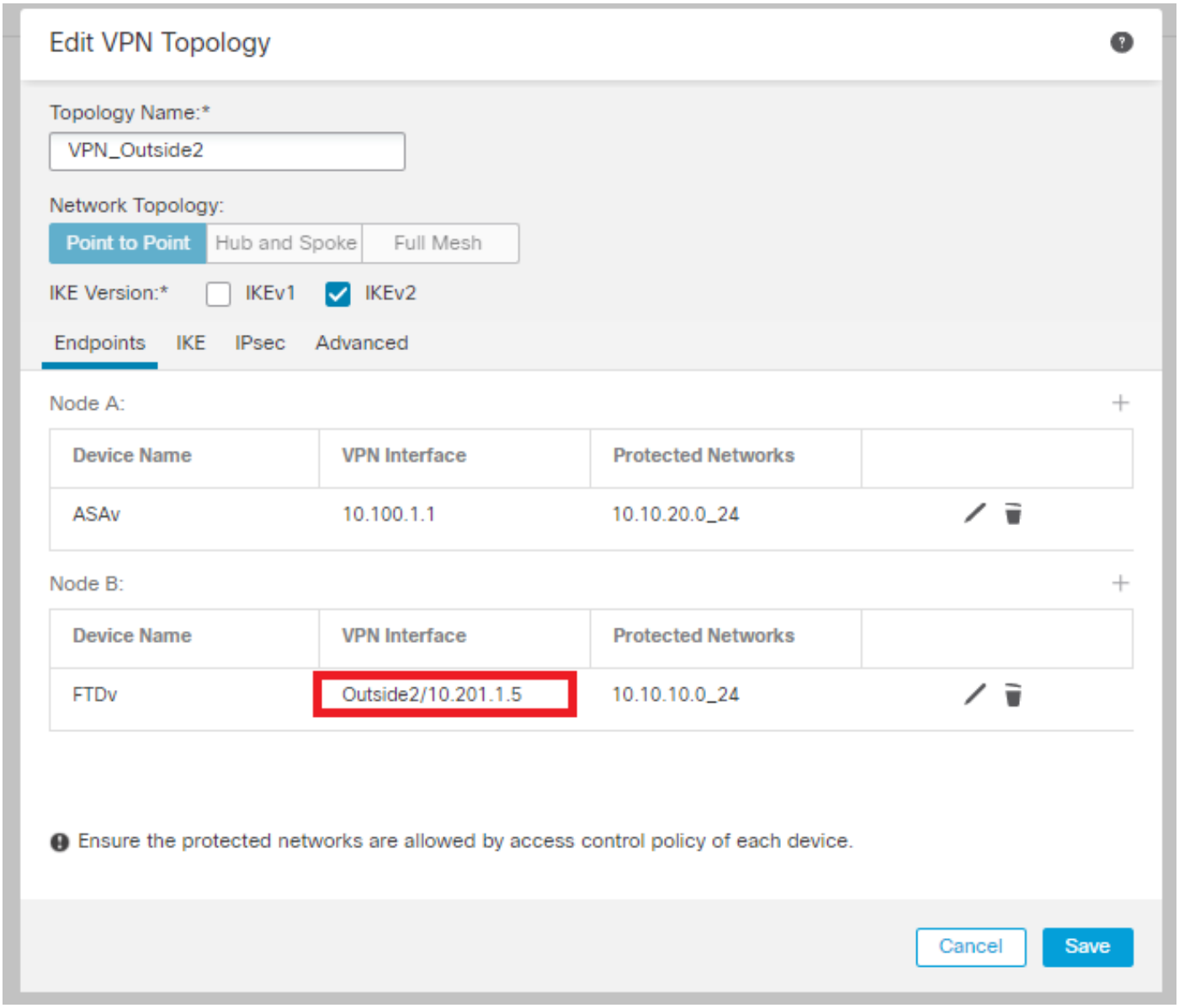
---



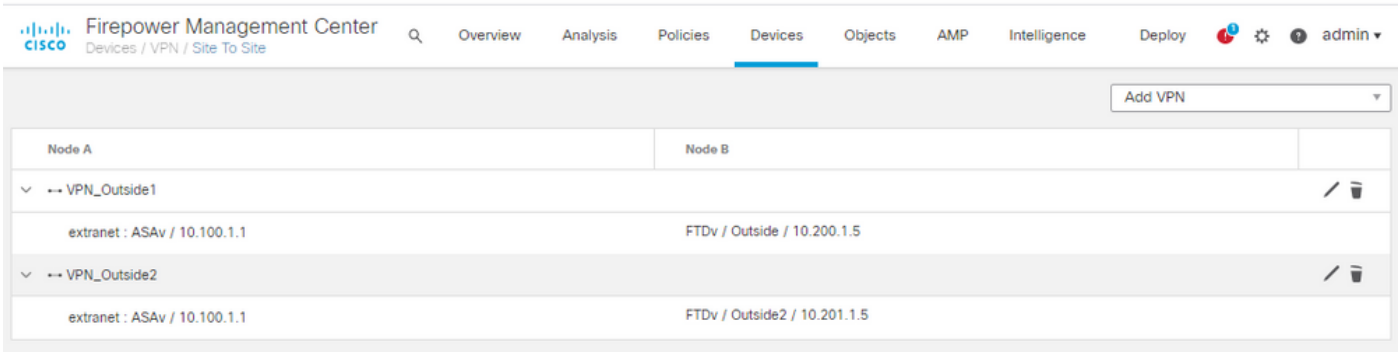
الخطوة 3. تحديد مخطط شبكة VPN لواجهة ISP الثانوية

1. انتقل إلى الأجهزة > VPN > موقع إلى موقع. تحت إضافة شبكة VPN، انقر فوق جهاز الدفاع ضد تهديد FirePOWER، وقم بإنشاء شبكة VPN وحدد الواجهة Outside2.

ملاحظة: يجب أن يكون تكوين الشبكة الخاصة الظاهرية (VPN) الذي يستخدم واجهة Outside2 هو نفسه تمامًا كمخطط الشبكة الخاصة الظاهرية (VPN) الخارجية باستثناء واجهة الشبكة الخاصة الظاهرية (VPN).

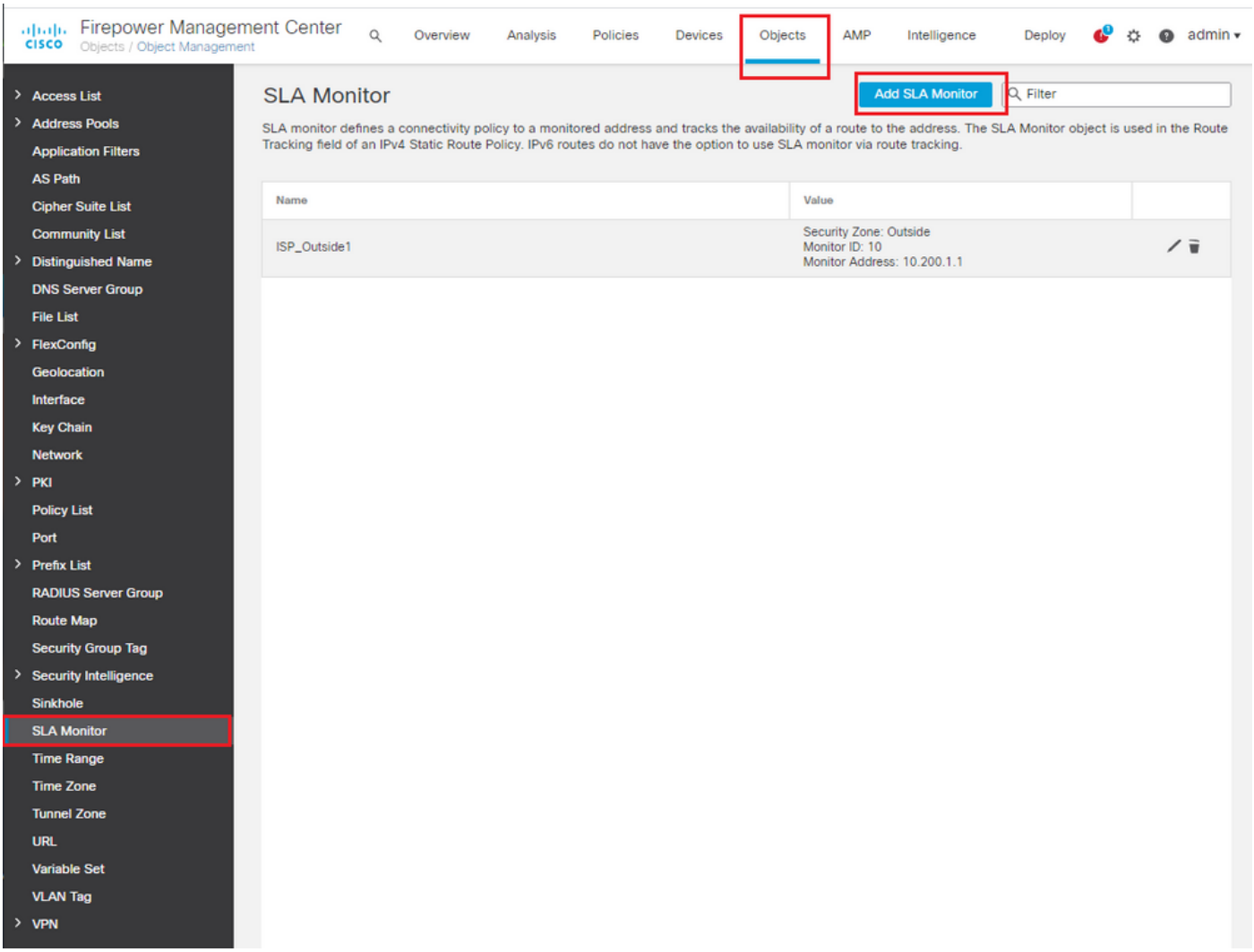


يجب تكوين طبوولوجيا VPN كما هو موضح في الصورة.

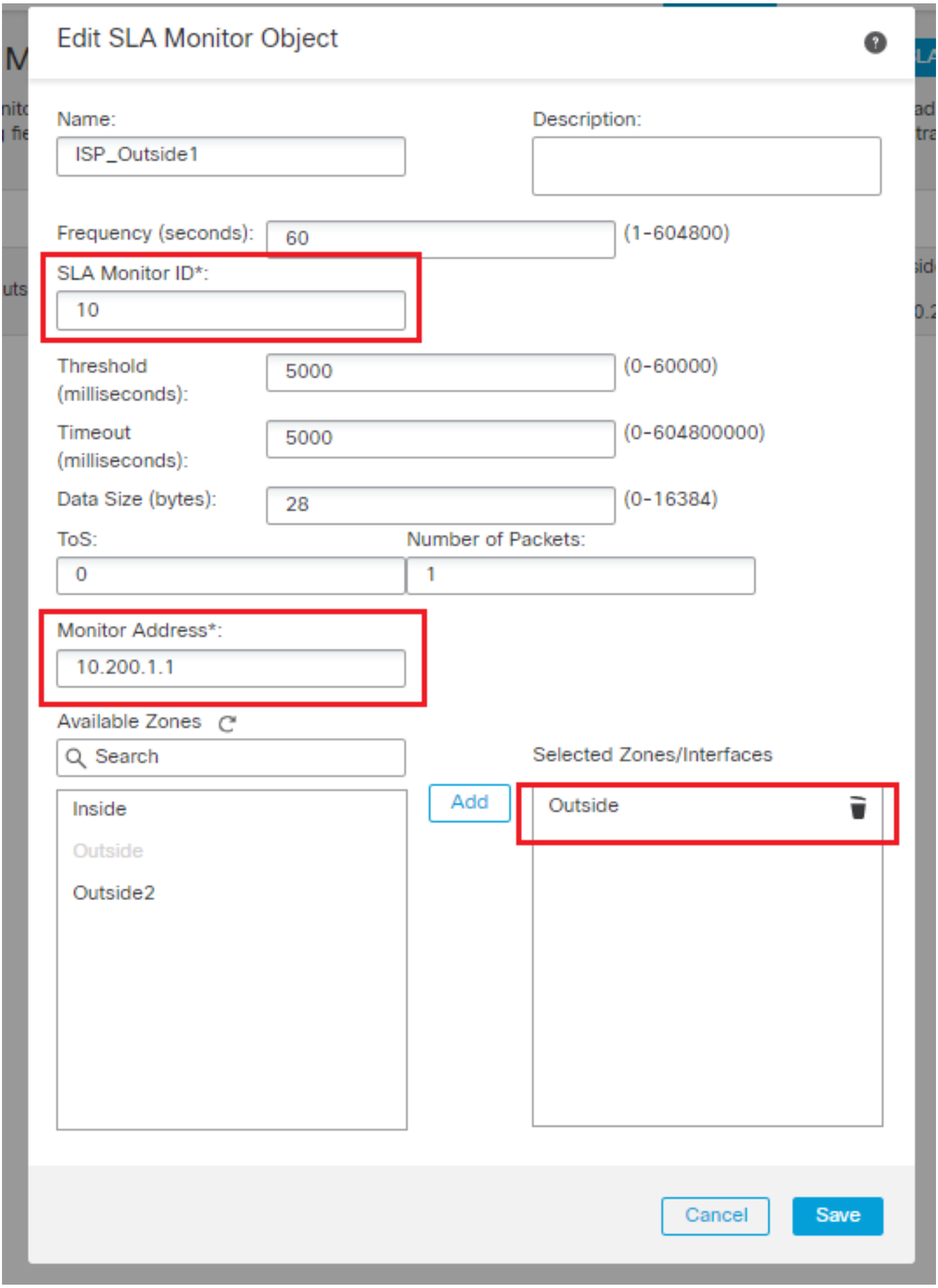


الخطوة 4. تكوين مراقبة SLA

1. انتقل إلى الكائنات > شاشة SLA > إضافة شاشة SLA. تحت إضافة شبكة VPN، انقر فوق جهاز الدفاع ضد تهديد FirePOWER، وقم بتكوين شاشة SLA كما هو موضح في الصورة.

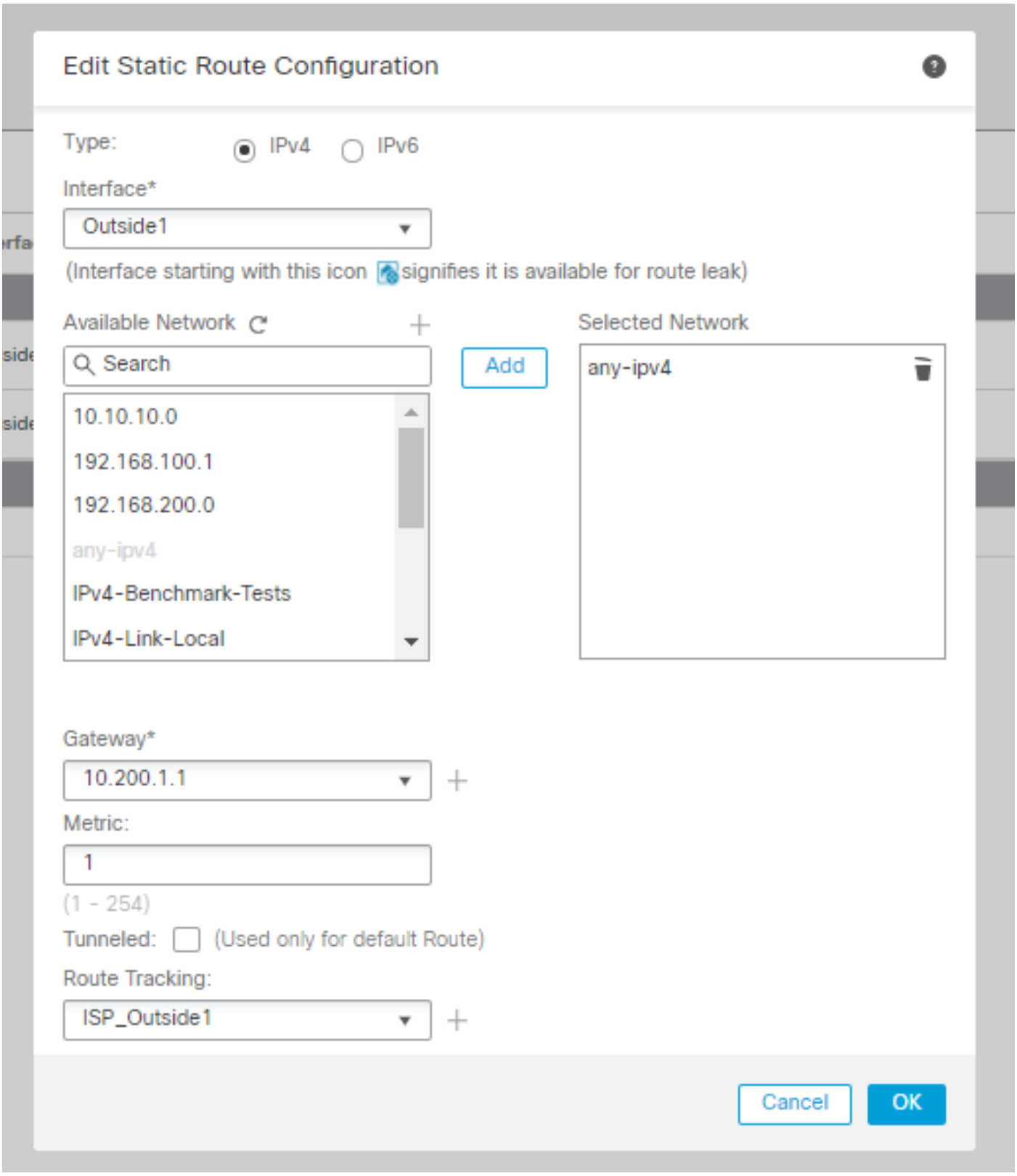


2. بالنسبة لمعرف مراقبة SLA*، أستخدم الحقل عنوان IP الخارجي للخطوة التالية.


Edit SLA Monitor Object
Name:
ISP_Outside1
Description:
Frequency (seconds):
60
(1-604800)
SLA Monitor ID*:
10
Threshold (milliseconds):
5000
(0-60000)
Timeout (milliseconds):
5000
(0-604800000)
Data Size (bytes):
28
(0-16384)
ToS:
0
Number of Packets:
1
Monitor Address*:
10.200.1.1
Available Zones
Search
Inside
Outside
Outside2
Add
Selected Zones/Interfaces
Outside
Cancel
Save

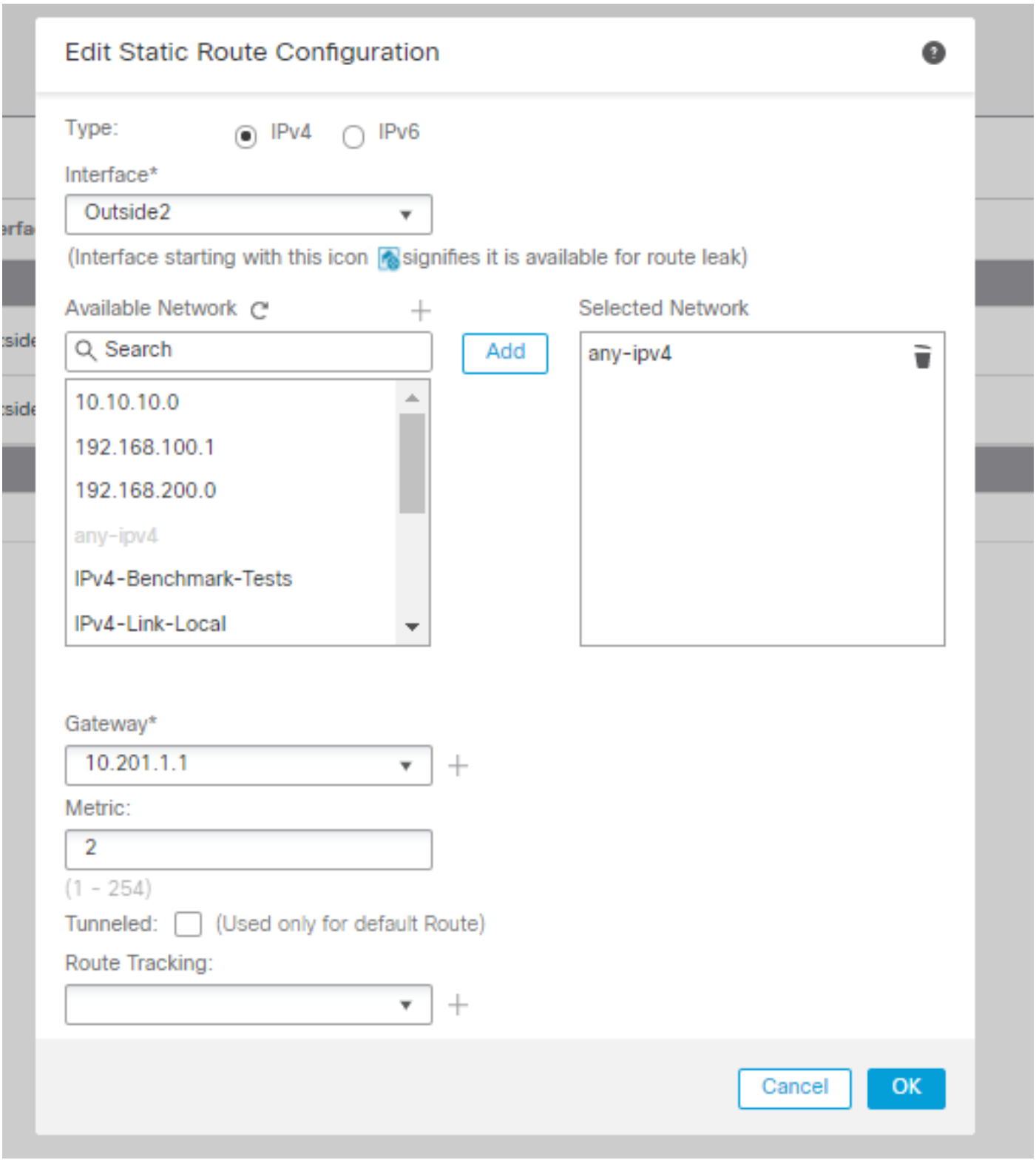
الخطوة 5. تكوين المسارات الثابتة باستخدام شاشة SLA

1. انتقل إلى الأجهزة > التوجيه > المسار الثابت. حدد إضافة مسار، وقم بتكوين المسار الافتراضي للواجهة الخارجية (الأساسية) باستخدام معلومات مراقبة SLA (التي تم إنشاؤها في الخطوة 4) في حقل تعقب المسار.

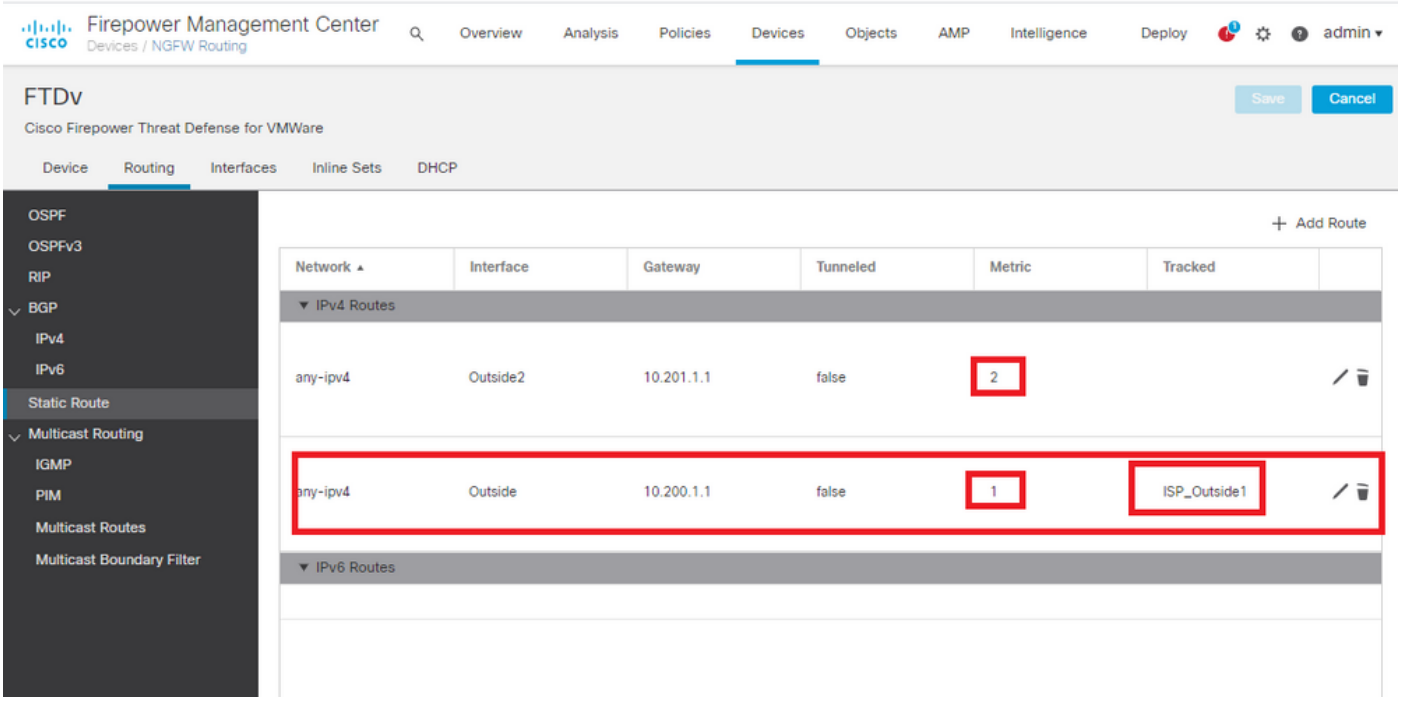


2. تكوين المسار الافتراضي للواجهة الخارجية2 (الثانوية). يجب أن تكون القيمة المتريةة

أعلى من المسار الافتراضي الأساسي. لا توجد حاجة إلى حقل تعقب المسار في هذا القسم.

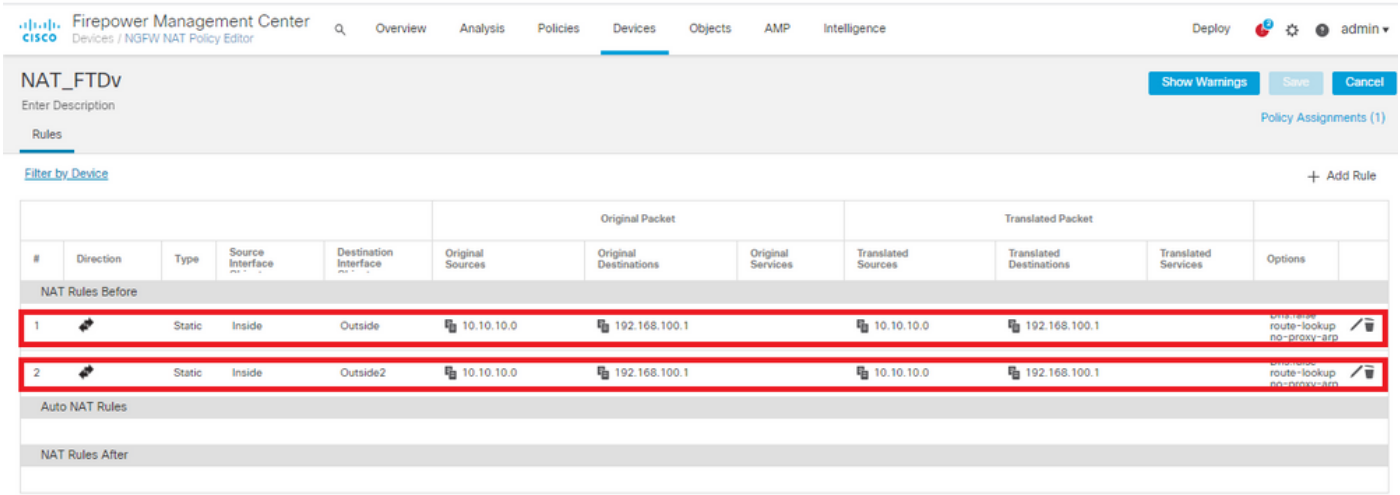


يجب تكوين المسارات كما هو موضح في الصورة.



الخطوة 6. تكوين إستثناء NAT

1. انتقل إلى الأجهزة > NAT > سياسة NAT وحدد السياسة التي تستهدف جهاز FTD. حدد إضافة قاعدة وشكلت إستثناء NAT لكل واجهة ISP (خارج و خارج2). يجب أن تكون قواعد NAT هي نفسها باستثناء واجهة الوجهة.



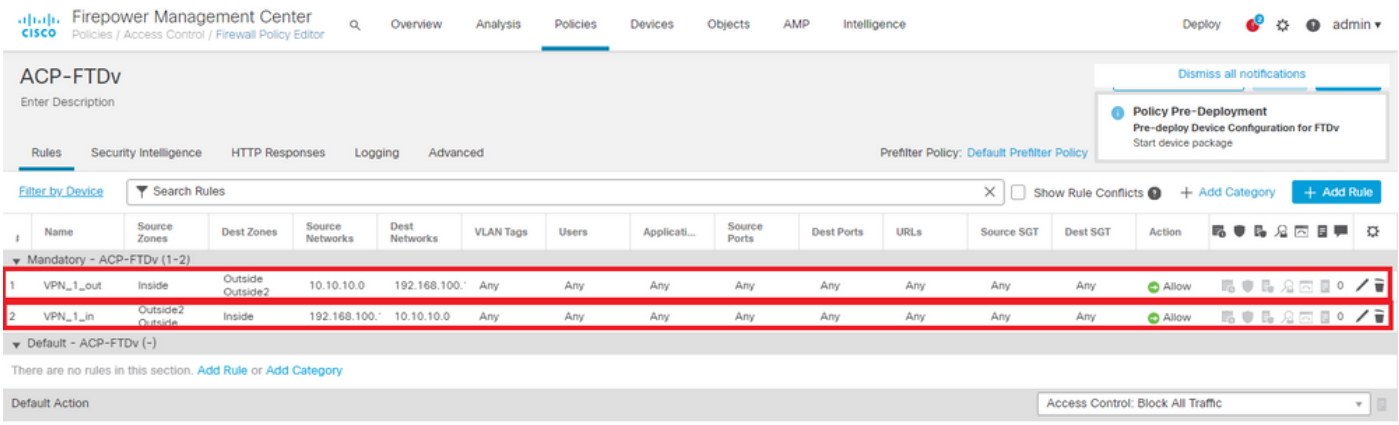
ملاحظة: بالنسبة لهذا السيناريو، تتطلب كل من قواعد NAT تمكين البحث عن المسار. وإلا فإن حركة المرور سوف تضرب القاعدة الأولى ولن تستمر في سلوك مسارات تجاوز الفشل. إذا لم يتم تمكين بحث المسار، فسيتم إرسال حركة المرور دائما باستخدام الواجهة الخارجية (قاعدة nat الأولى). مع تمكين البحث عن المسار، تبقى حركة مرور البيانات دائما في جدول التوجيه الذي يتم التحكم فيه من خلال مراقبة SLA.

الخطوة 7. تكوين سياسة التحكم في الوصول لحركة المرور المفيدة

1. انتقل إلى السياسات > التحكم في الوصول > تحديد سياسة التحكم في الوصول. إلضافة قاعدة، انقر فوق إضافة قاعدة، كما هو موضح في الصورة هنا.

قم بتكوين قاعدة واحدة من الداخل إلى المناطق الخارجية (خارج 1 وخارج 2) والتي تتيح لحركة المرور المهتمة من 10.10.10.0/24 إلى 192.168.100/24.

قم بتكوين قاعدة أخرى من المناطق الخارجية (خارج 1 وخارج 2) إلى الداخل مما يسمح بحركة المرور المثيرة للاهتمام من 192.168.100/24 إلى 10.10.10.0/24.



تكوين ASA

ملاحظة: لهذا السيناريو المحدد، يتم تكوين نظير نسخ إحتياطي على خريطة التشفير IKEv2، وتتطلب هذه الميزة أن يكون ASA على 9.14.1 أو الإصدارات الأحدث. إذا كان ASA الخاص بك يشغل إصدارا قديما، فاستخدم IKEv1 كحل بديل. أحلت ل كثير مرجع إلى cisco بق id CSCud2276.

1. مكنت IKEv2 على القارن خارجي من ال ASA:

```
Crypto ikev2 enable Outside
```

2. قم بإنشاء نهج IKEv2 الذي يحدد نفس المعلمات التي تم تكوينها على FTD:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

3. قم بإنشاء سياسة مجموعة للسماح ببروتوكول iKEV2:

```
group-policy IKEV2 internal
group-policy IKEV2 attributes
 vpn-tunnel-protocol ikev2
```

4. قم بإنشاء مجموعة أنفاق لكل عنوان IP خارجي في FTD (خارج1 وخارج2). راجع نهج المجموعة وحدد المفاتيح المشترك مسبقا:

```
tunnel-group 10.200.1.5 type ipsec-l2l
tunnel-group 10.200.1.5 general-attributes
 default-group-policy IKEV2
tunnel-group 10.200.1.5 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123

tunnel-group 10.201.1.5 type ipsec-l2l
tunnel-group 10.201.1.5 general-attributes
 default-group-policy IKEV2
tunnel-group 10.201.1.5 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123
```

5. قم بإنشاء قائمة وصول تحدد حركة المرور التي سيتم تشفيرها: (FTD-Subnet 10.10.10.0/24) (ASA-Subnet 192.168.100.0/24):

```
Object network FTD-Subnet
 Subnet 10.10.10.0 255.255.255.0
Object network ASA-Subnet
 Subnet 192.168.100.0 255.255.255.0
access-list VPN_1 extended permit ip 192.168.100.0 255.255.255.0 10.10.10.0 255.255.255.0
```

6. إنشاء مقترح ikev2 ipSec للإشارة إلى الخوارزميات المحددة في FTD:

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

7. قم بإنشاء إدخال خريطة تشفير طبق التكوين مع وضع عناوين IP لبروتوكول الإنترنت (FTD) الخارجي1 والخارجي2:

```
crypto map CSM_Outside_map 1 match address VPN_1
crypto map CSM_Outside_map 1 set peer 10.200.1.5 10.201.1.5
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map 1 set reverse-route
crypto map CSM_Outside_map interface Outside
```

8. قم بإنشاء بيان إستثناء NAT يمنع حركة مرور VPN من أن تحدث بواسطة جدار الحماية:

```
Nat (inside,Outside) 1 source static ASA-Subnet ASA-Subnet destination static FTD-Subnet FTD-Subnet
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

نظام Firepower Threat Defense (FTD)

في سطر الأوامر، أستخدم الأمر show crypto ikev2 sa للتحقق من حالة شبكة VPN.

ملاحظة: يتم إنشاء الشبكة الخاصة الظاهرية (VPN) باستخدام عنوان IP الخاص ب Outside1 (10.200.1.5) كعنوان محلي.

```
firepower# sh crypto  ikev2 sa

IKEv2 SAs:

Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
373101057 10.200.1.5/500                                10.100.1.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/37 sec
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
          remote selector 192.168.100.0/0 - 192.168.100.255/65535
          ESP spi in/out: 0x829ed58d/0x2051ccc9
```

طريق

يعرض المسار الافتراضي عنوان IP للخطوة التالية ل External1.

```
firepower# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.200.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.200.1.1, Outside1
C        10.10.10.0 255.255.255.0 is directly connected, Inside
L        10.10.10.5 255.255.255.255 is directly connected, Inside
C        10.200.1.0 255.255.255.0 is directly connected, Outside1
L        10.200.1.5 255.255.255.255 is directly connected, Outside1
C        10.201.1.0 255.255.255.0 is directly connected, Outside2
L        10.201.1.5 255.255.255.255 is directly connected, Outside2
```

رثأ

كمإ يظهر في إخراج show track 1، "تم تشغيل القابلية للوصول".

```
firepower#   sh track 1
Track 1
  Response Time Reporter 10 reachability
  Reachability is Up                        <-----
  36 changes, last change 00:00:04
  Latest operation return code: OK
  Latest RTT (millisecs) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

nat

هناك حاجة إلى أتكيد حركة المرور المفيدة التي تصل إلى قاعدة إستثناء NAT باستخدام الواجهة Outside1.

أستخدم الأمر "packet-tracer input داخل ICMP 10.10.10.1 8 0 192.168.100.10 detail" للتحقق من قاعدة NAT المطبقة على حركة المرور المفيدة.

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det

---------------OMITTED OUTPUT -----------------
Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
```

```
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
NAT divert to egress interface Outside1(vrfid:0)
Untranslate 192.168.100.1/0 to 192.168.100.1/0

---------------OMITTED OUTPUT -----------------

Phase: 7
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
Static translate 10.10.10.1/0 to 10.10.10.1/0
 Forward Flow based lookup yields rule:
 in  id=0x2b3e09576290, priority=6, domain=nat, deny=false
        hits=19, user_data=0x2b3e0c341370, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3596, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c8d0250, priority=70, domain=encrypt, deny=false
        hits=5, user_data=0x16794, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any(vrfid:65535), output_ifc=Outside1

Phase: 13
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e095d49a0, priority=6, domain=nat-reverse, deny=false
        hits=1, user_data=0x2b3e0c3544f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
```

```
        input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)

Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0c8ad890, priority=70, domain=ipsec-tunnel-flow, deny=false
        hits=5, user_data=0x192ec, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
        src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Outside1(vrfid:0), output_ifc=any

Phase: 15
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3598, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------

Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

تنفيذ تجاوز الفشل

على سبيل المثال، يتم تنفيذ تجاوز الفشل بواسطة إيقاف تشغيل عالخطوة التالية ل Outside1 المستخدمة على تكوين شاشة IP SLA.

```
firepower# sh sla monitor configuration 10
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 10
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.200.1.1
Interface: Outside1
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
```

```
Verify data: No
Operation frequency (seconds): 60
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:
```

طريق

يستخدم المسار الافتراضي الآن عنوان IP للخطوة التالية الخاص ب External2 كما أن إمكانية الوصول متوقفة.

```
firepower# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.201.1.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 10.201.1.1, Outside2
C        10.10.10.0 255.255.255.0 is directly connected, Inside
L        10.10.10.5 255.255.255.255 is directly connected, Inside
C        10.200.1.0 255.255.255.0 is directly connected, Outside1
L        10.200.1.5 255.255.255.255 is directly connected, Outside1
C        10.201.1.0 255.255.255.0 is directly connected, Outside2
L        10.201.1.5 255.255.255.255 is directly connected, Outside2
```

رثأ

كما يظهر في إخراج show track 1، "إمكانية الوصول متوقفة" عند هذه النقطة.

```
firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Down <----
37 changes, last change 00:17:02
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

nat

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det
---------------OMITTED OUTPUT -----------------

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
Static translate 10.10.10.1/0 to 10.10.10.1/0
 Forward Flow based lookup yields rule:
 in  id=0x2b3e0c67d470, priority=6, domain=nat, deny=false
        hits=44, user_data=0x2b3e0c3170e0, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

---------------OMITTED OUTPUT -----------------
Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c67bdb0, priority=70, domain=encrypt, deny=false
        hits=1, user_data=0x1d4cfb24, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any(vrfid:65535), output_ifc=Outside2

Phase: 10
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x2b3e0c6d5bb0, priority=6, domain=nat-reverse, deny=false
        hits=1, user_data=0x2b3e0b81bc00, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)

Phase: 11
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0c8a14f0, priority=70, domain=ipsec-tunnel-flow, deny=false
        hits=1, user_data=0x1d4d073c, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
        src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
```

```
        input_ifc=Outside2(vrfid:0), output_ifc=any

Phase: 12
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Reverse Flow based lookup yields rule:
 in  id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
        hits=3669, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

---------------OMITTED OUTPUT -----------------

Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside2(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

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).