Configuration du basculement pour les tunnels IPSec site à site avec les liaisons de sauvegarde ISP sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit comment configurer le basculement basé sur la crypto-carte pour la liaison ISP avec la fonctionnalité IP SLA track sur le FTD géré par FMC.

Contribution d'Amanda Nava, Ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base d'un réseau privé virtuel (VPN)
- Expérience avec FTD
- Expérience avec FMC
- Expérience avec la ligne de commande ASA (Adaptive Security Appliance)

Composants utilisés

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

- FMC version 6.6.0
- FTD version 6.6.0
- ASA version 9.14.1

The information in this document was created from the devices in a specific lab environment. 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.

Informations générales

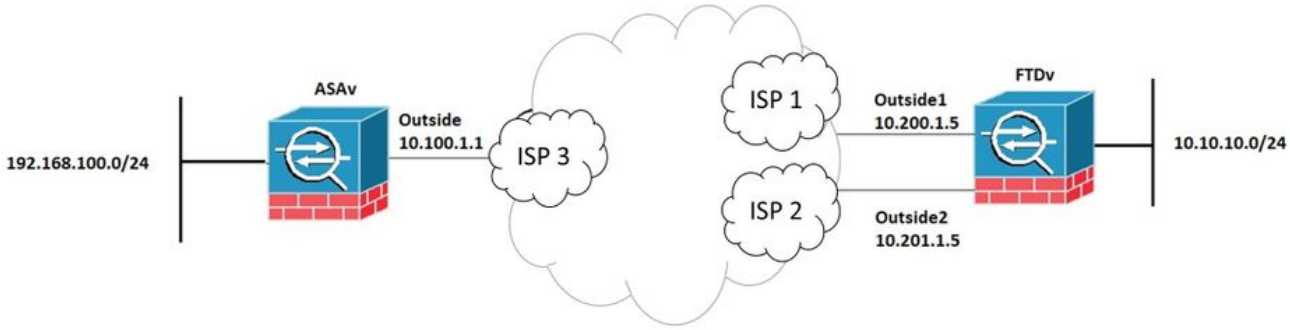
Ce document décrit comment configurer le basculement basé sur une crypto-carte pour la liaison de secours du fournisseur d'accès Internet (FAI) avec la fonctionnalité de suivi IP SLA (Internet Protocol Service Level Agreement) sur le pare-feu Firepower Threat Defense (FTD) géré par le Centre de gestion Firepower (FMC). Il explique également comment configurer l'exemption de traduction d'adresses de réseau (NAT) pour le trafic VPN lorsqu'il y a deux FAI et qu'il nécessite un basculement transparent.

Dans ce scénario, le VPN est établi du FTD vers l'ASA comme homologue VPN avec une seule interface ISP. Le FTD utilise une liaison FAI à ce moment pour établir le VPN. Lorsque la liaison du FAI principal tombe en panne, le FTD prend le relais avec la liaison du FAI secondaire via le SLA Monitor et le VPN est établi.

Configurer

Diagramme du réseau

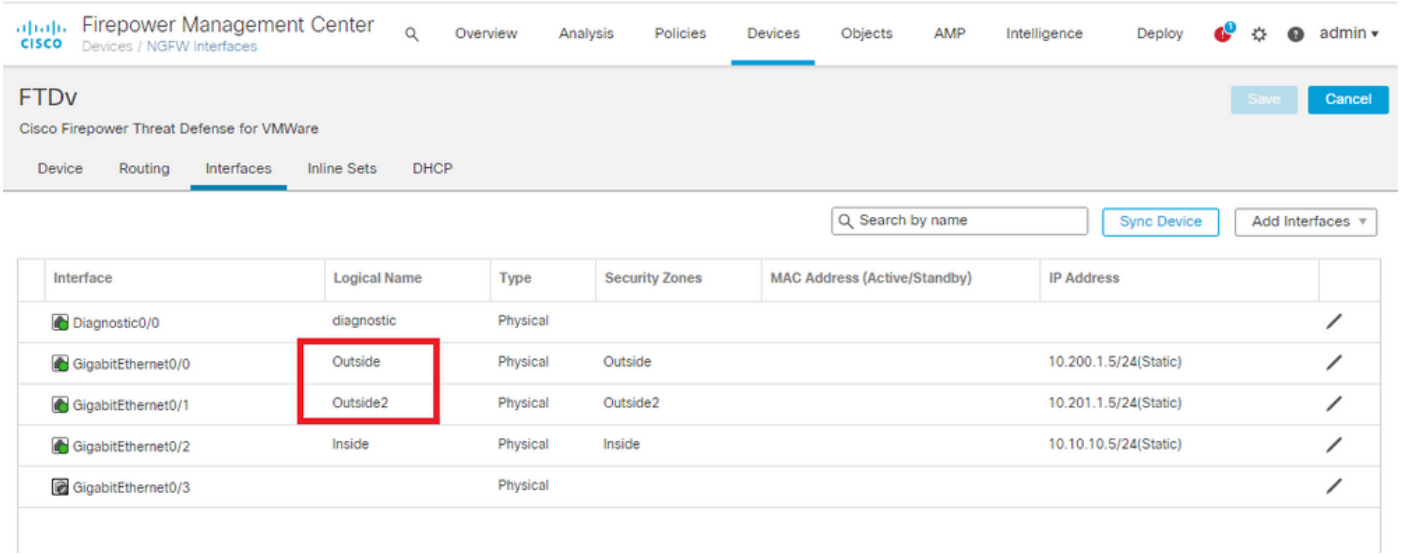
Voici la topologie utilisée pour l'exemple dans ce document :



Configuration du FTD

Étape 1. Définition des interfaces ISP principale et secondaire

1. Accédez à Périphériques > Gestion des périphériques > Interfaces comme indiqué dans l'image.

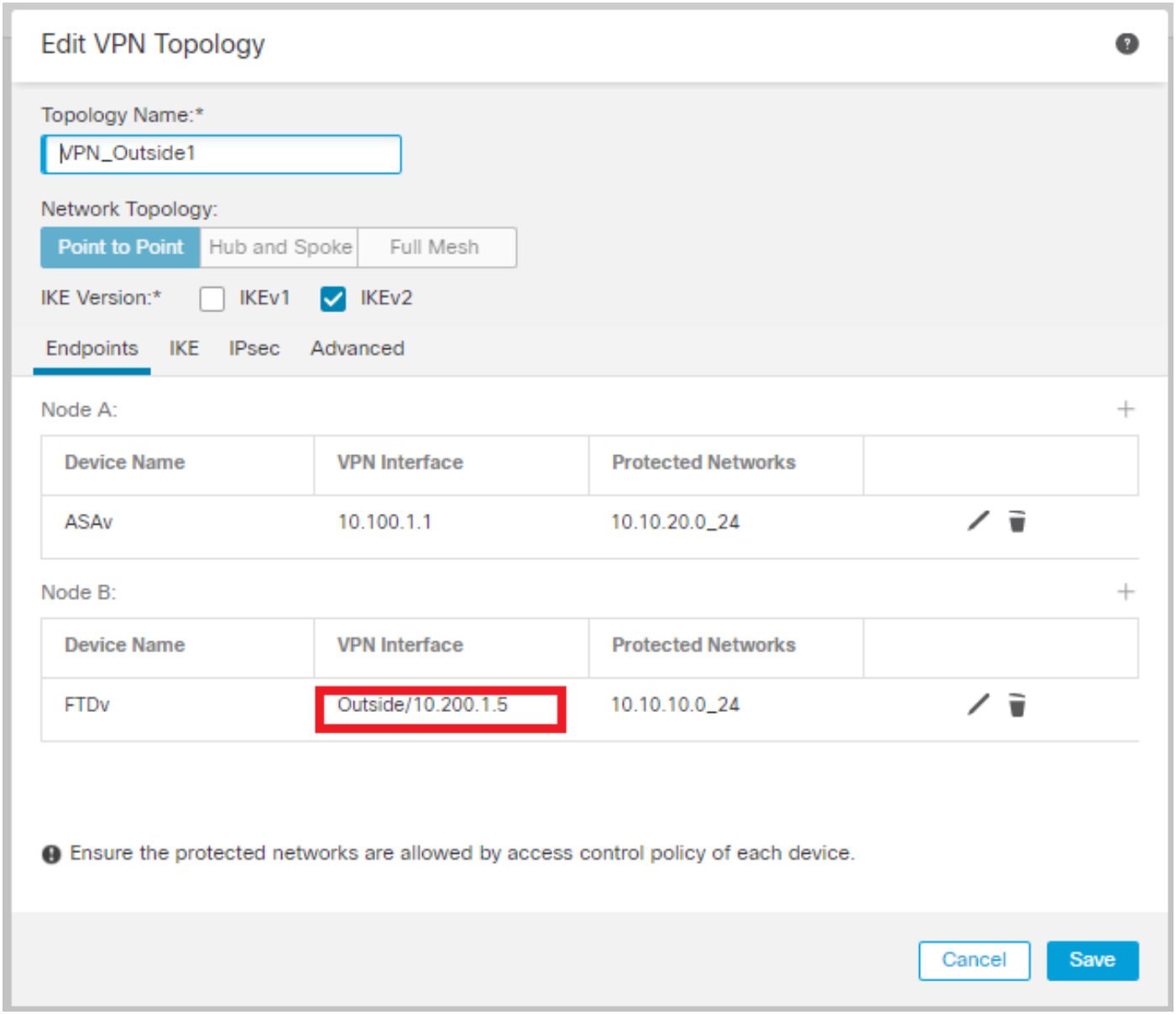


Étape 2. Définition de la topologie VPN pour l'interface principale du FAI

1. Accédez à Devices > VPN > Site To Site. Sous Add VPN, cliquez sur Firepower Threat Defense Device, créez le VPN et sélectionnez l'interface externe.

Remarque : ce document ne décrit pas comment configurer un VPN S2S à partir de zéro. Pour plus de références sur la configuration VPN S2S sur FTD, consultez la page 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

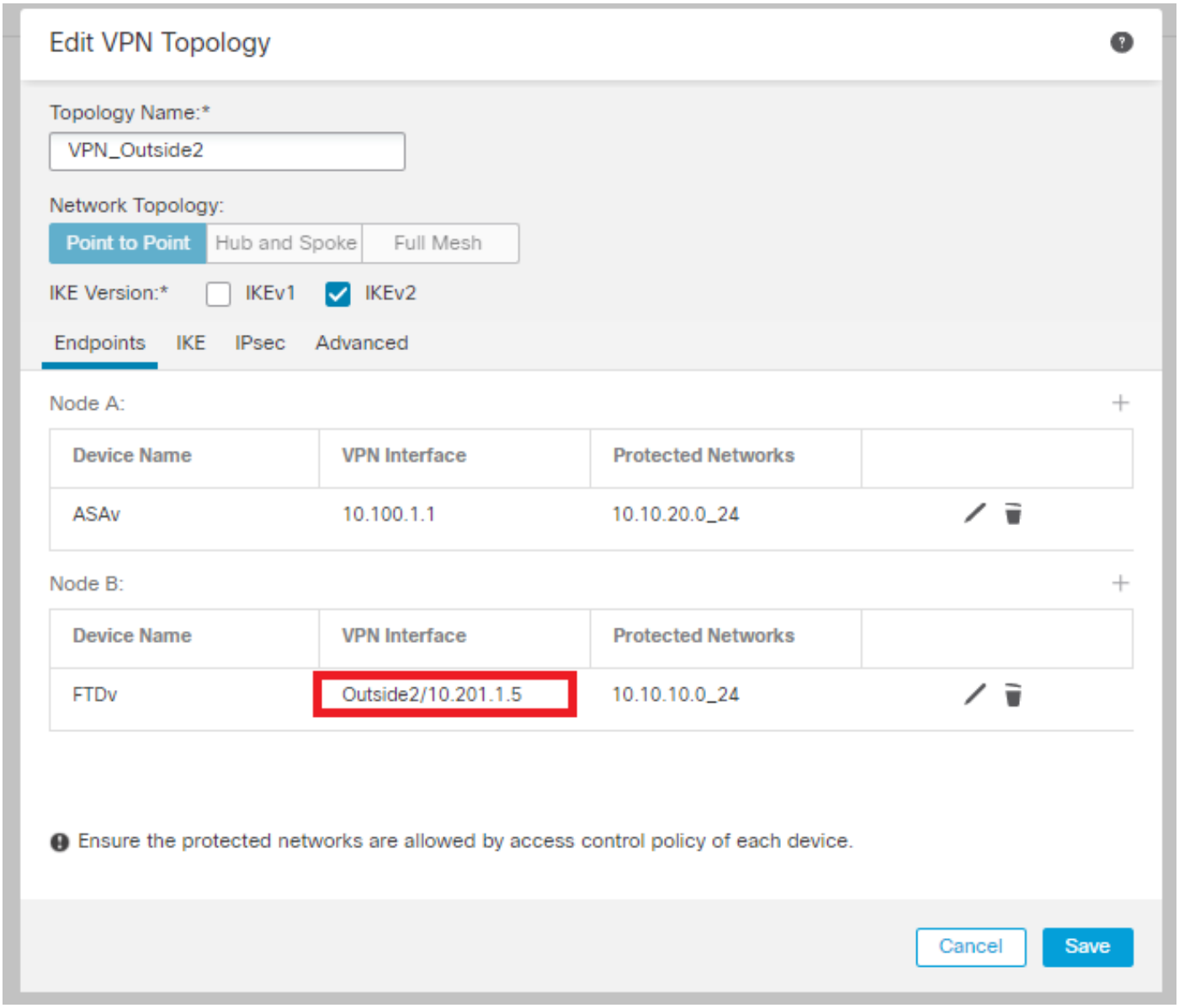
---



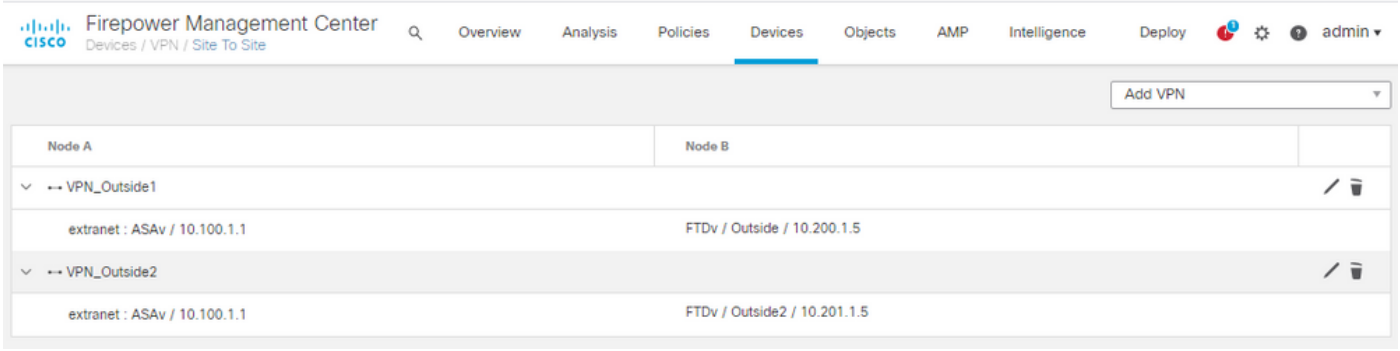
Étape 3. Définition de la topologie VPN pour l'interface ISP secondaire

1. Accédez à Devices > VPN > Site To Site. Sous Add VPN, cliquez sur Firepower Threat Defense Device, créez le VPN et sélectionnez l'interface Outside2.

Remarque : la configuration VPN qui utilise l'interface Outside2 doit être exactement identique à la topologie Outside VPN, à l'exception de l'interface VPN.

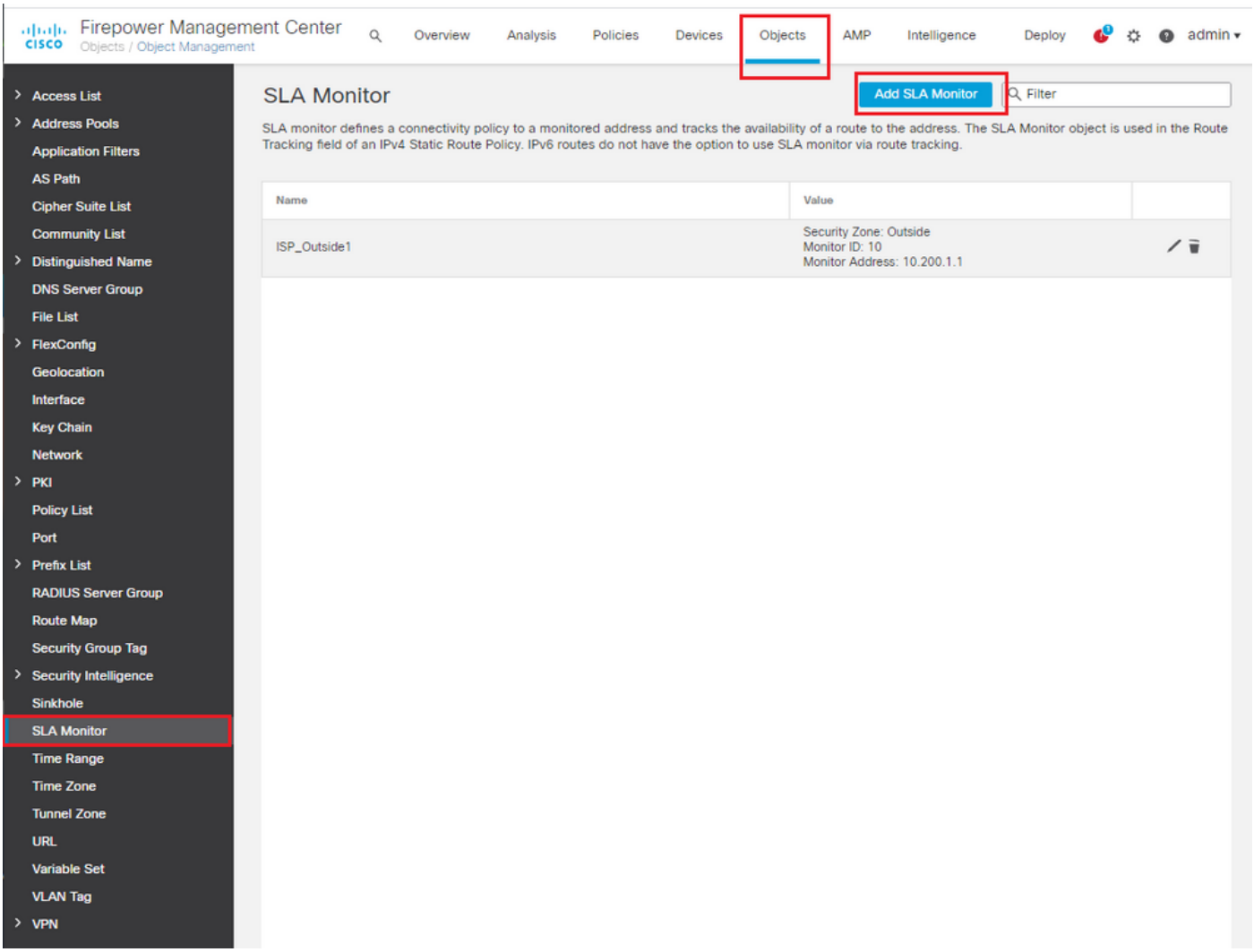


Les topologies VPN doivent être configurées comme indiqué dans l'image.

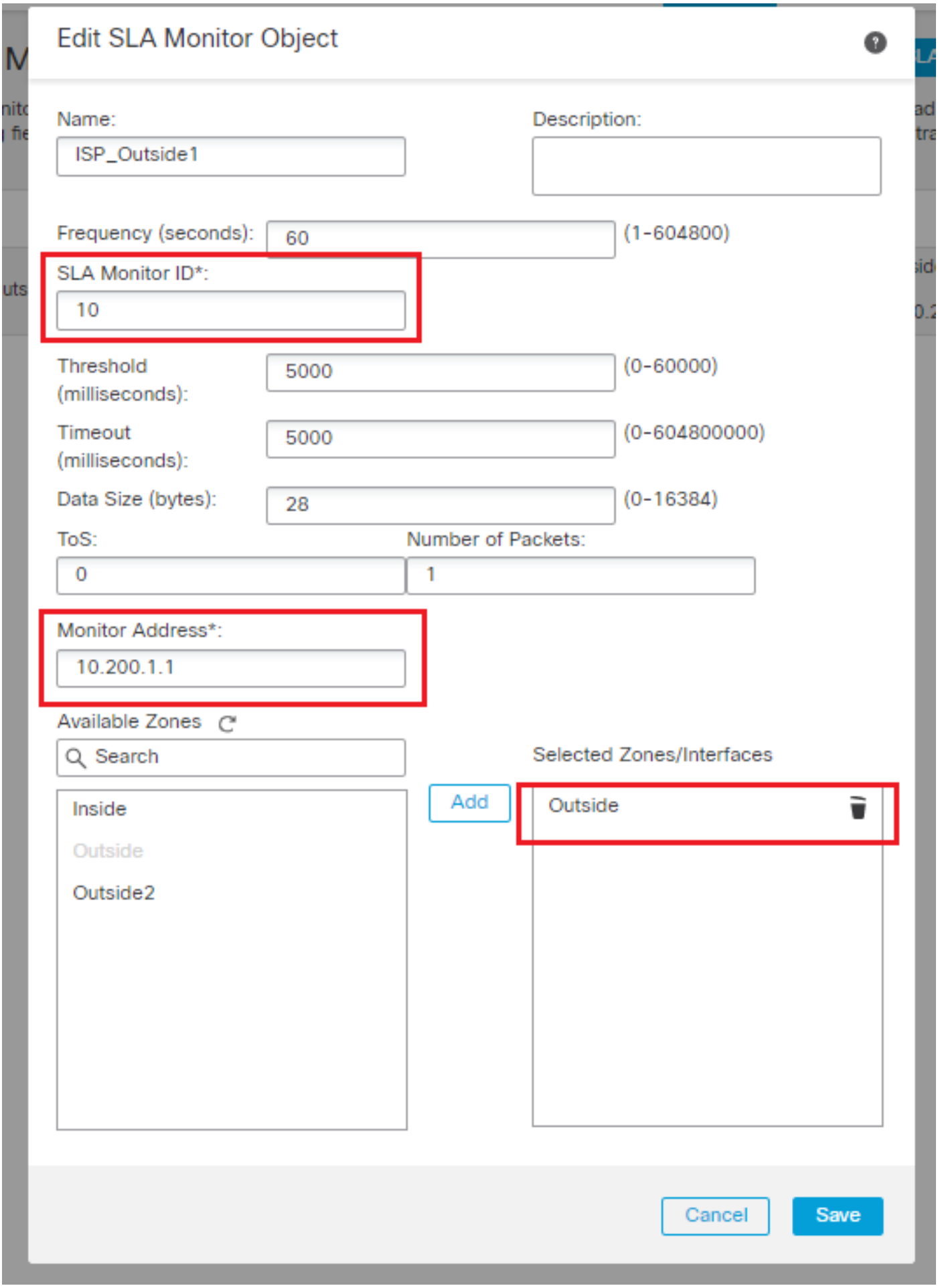


Étape 4. Configurer le SLA Monitor

1. Accédez à Objects > SLA Monitor > Add SLA Monitor. Sous Add VPN, cliquez sur Firepower Threat Defense Device, et configurez le SLA Monitor comme indiqué dans l'image.

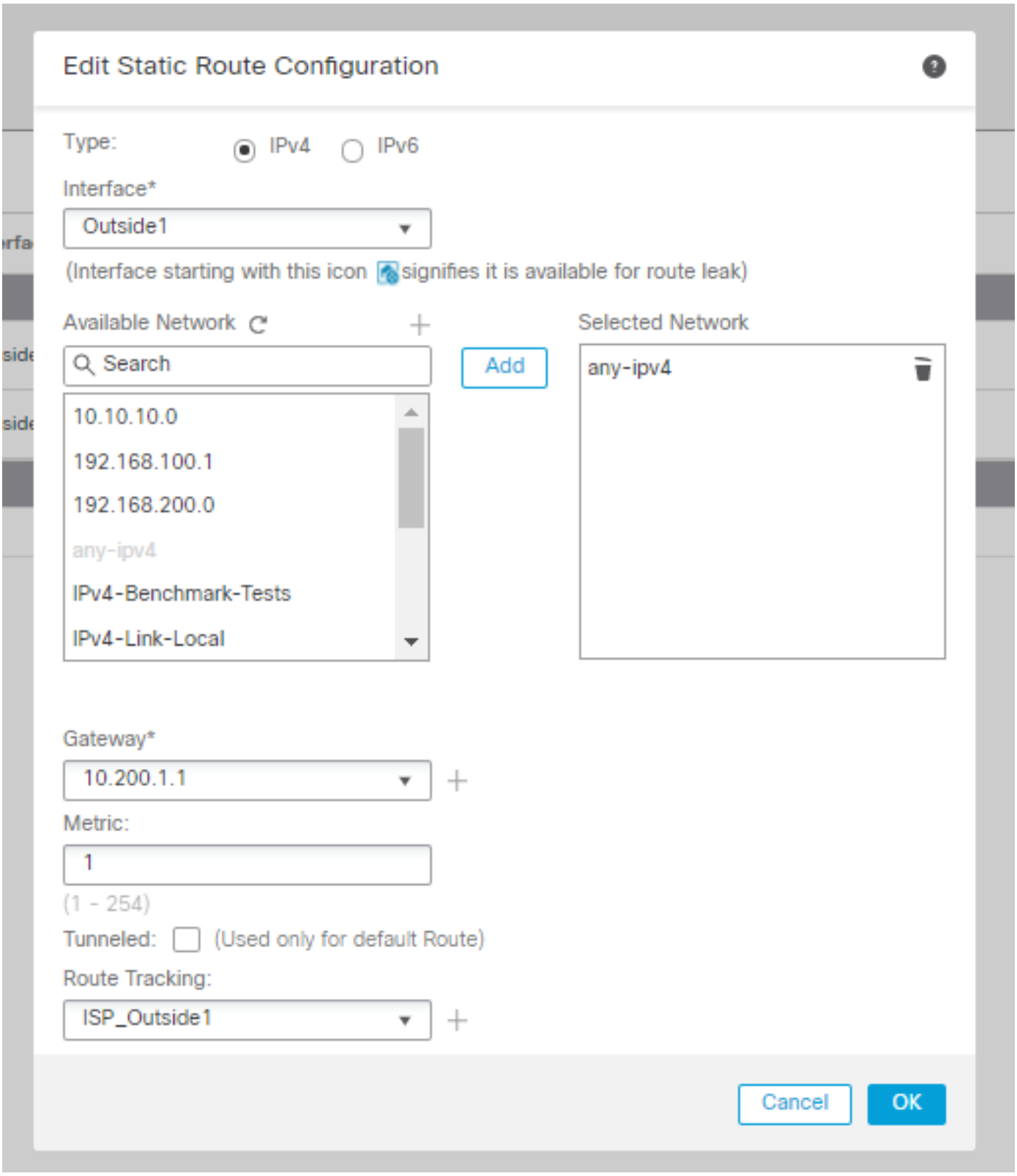


2. Pour le champ SLA Monitor ID*, utilisez l’adresse IP du tronçon suivant externe.


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

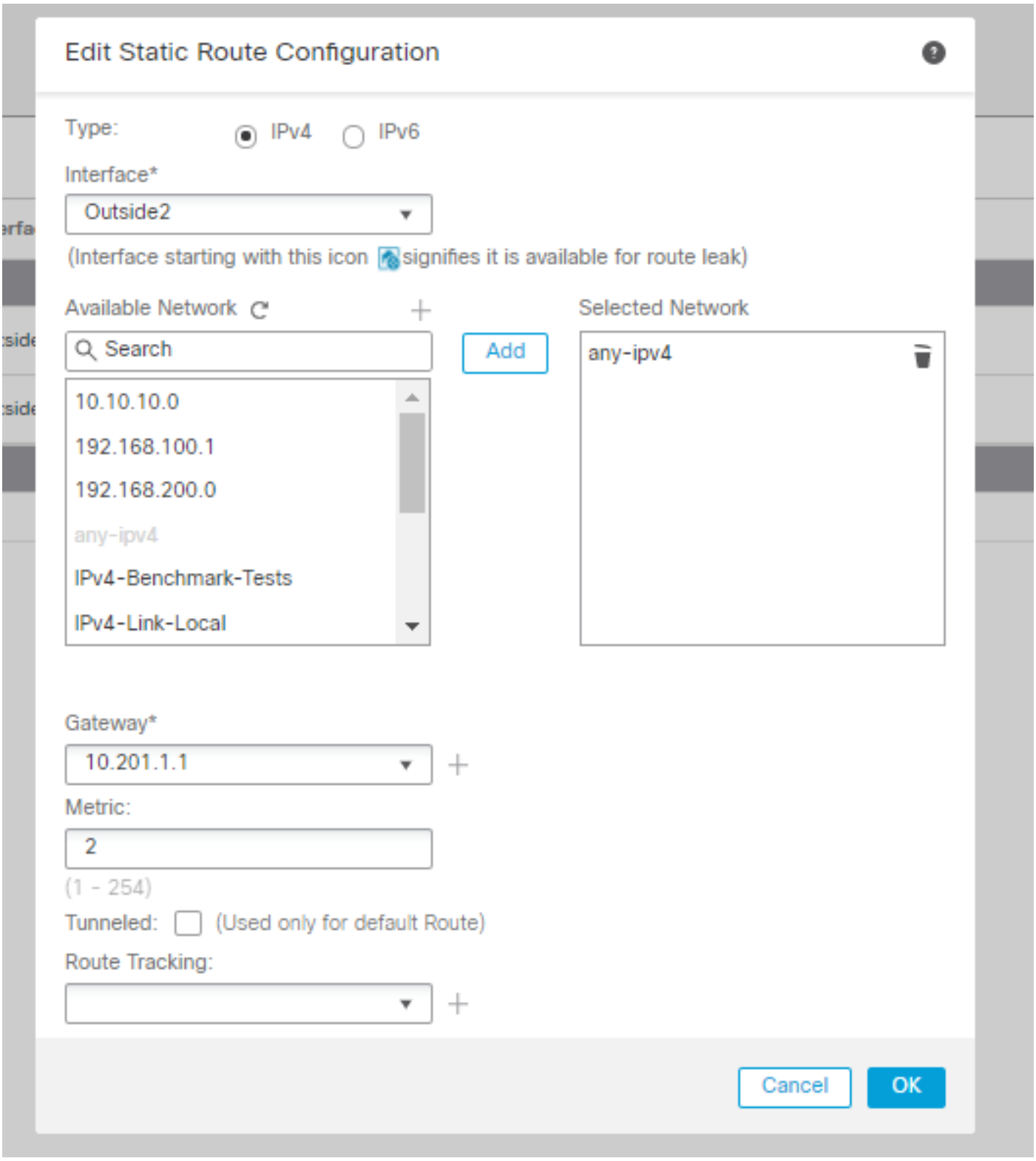
Étape 5. Configurez les routes statiques avec le Moniteur SLA

1. Accédez à Périphériques > Routage > Route statique. Sélectionnez Add Route et configurez la route par défaut pour l'interface externe (principale) avec les informations de surveillance SLA (Créé à l'étape 4) dans le champ Route tracking.

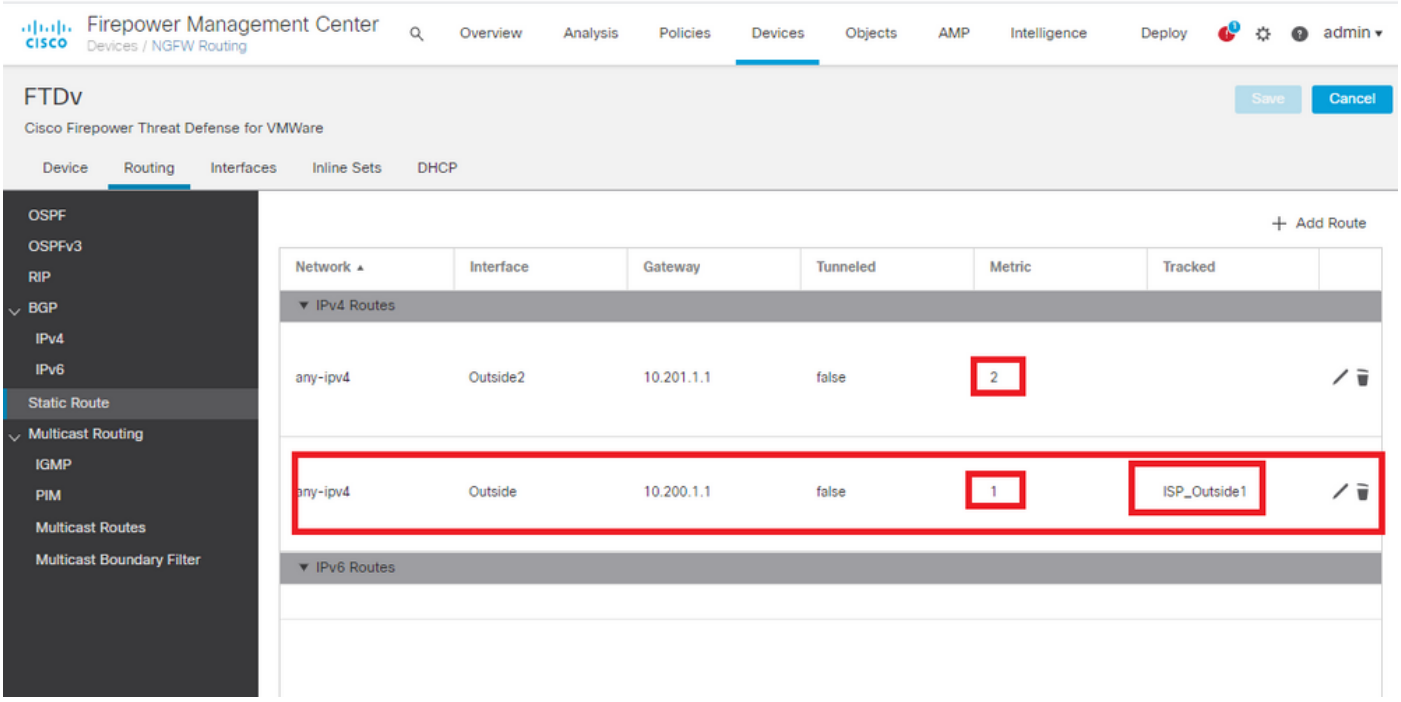


2. Configurez la route par défaut pour l'interface Outside2 (secondaire). La valeur de la mesure

doit être supérieure à la route par défaut principale. Aucun champ de suivi de route n'est nécessaire dans cette section.

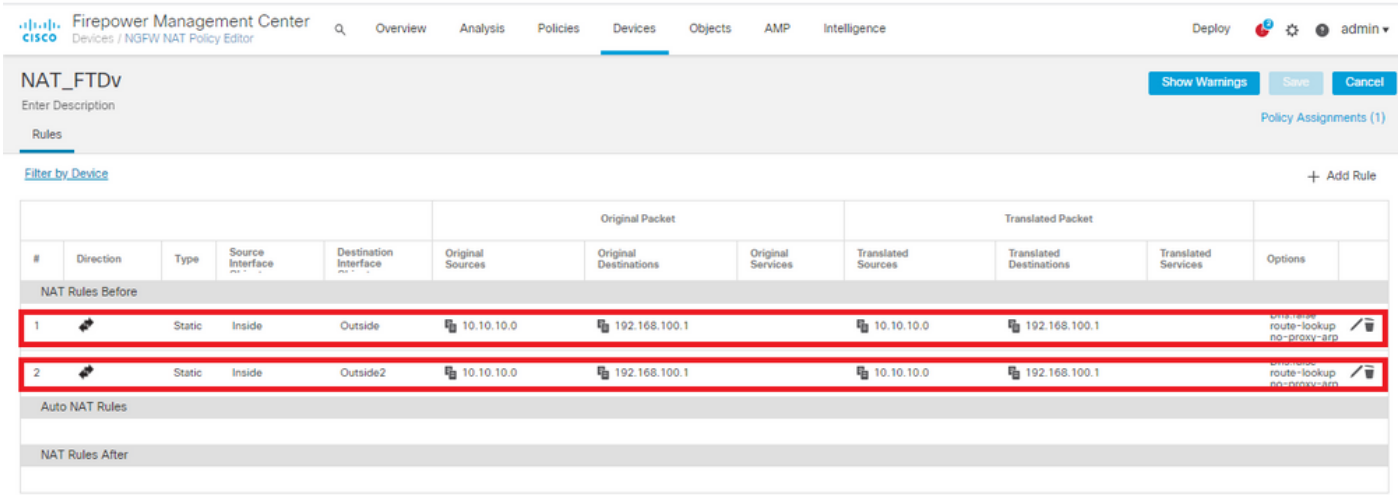


Les routes doivent être configurées comme indiqué dans l’image.



Étape 6. Configuration de l'exemption NAT

1. Accédez à Devices > NAT > NAT Policy et sélectionnez la politique qui cible le périphérique FTD. Sélectionnez Add Rule et configurez une exemption NAT par interface ISP (Outside et Outside2). Les règles NAT doivent être identiques, sauf pour l'interface de destination.



Remarque : pour ce scénario, les deux règles NAT nécessitent l'activation de la recherche de route. Sinon, le trafic atteindrait la première règle et ne se cantonnerait pas aux routes de basculement. Si la recherche de route n'est pas activée, le trafic est toujours envoyé à l'aide de l'interface externe (première règle NAT). Lorsque la recherche de route est activée, le trafic reste toujours dans la table de routage qui est contrôlée par le biais du SLA Monitor.

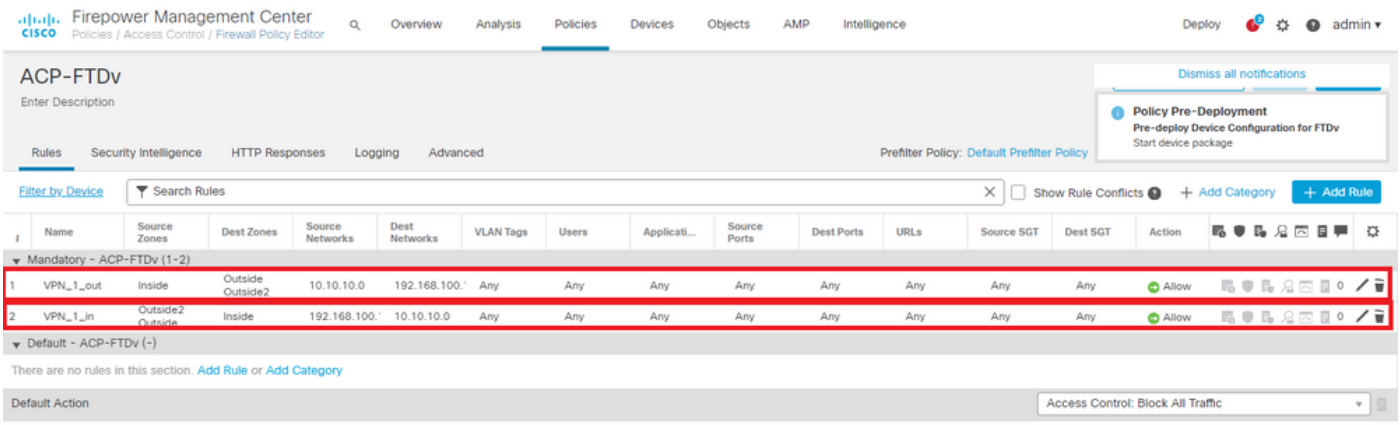
Étape 7. Configurer la politique de contrôle d'accès pour le trafic intéressant

1. Accédez à Stratégies > Contrôle d'accès > Sélectionnez la stratégie de contrôle d'accès. Afin

d'ajouter une règle, cliquez sur Add Rule, comme montré dans l'image ici.

Configurez une règle des zones Interne vers Externe (Outside1 et Outside2) qui autorise le trafic intéressé de 10.10.10.0/24 à 192.168.100/24.

Configurez une autre règle de Outside zones (Outside1 et Outside 2) à Inside qui autorise le trafic intéressant de 192.168.100/24 à 10.10.10.0/24.



Configuration de l'ASA

Remarque : pour ce scénario spécifique, un homologue de sauvegarde est configuré sur la crypto-carte IKEv2. Cette fonctionnalité nécessite que l'ASA soit sur la version 9.14.1 ou ultérieure. Si votre ASA exécute une version antérieure, utilisez IKEv1 comme solution de contournement. Pour plus de référence, allez à l'ID de bogue Cisco CSCud22276.

1. Activez IKEv2 sur l'interface externe de l'ASA :

```
Crypto ikev2 enable Outside
```

2. Créez la stratégie IKEv2 qui définit les mêmes paramètres configurés sur le FTD :

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

3. Créez une stratégie de groupe pour autoriser le protocole ikev2 :

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

4. Créez un groupe de tunnels pour chaque adresse IP FTD externe (Outside1 et Outside2). Faites référence à la stratégie de groupe et spécifiez la clé pré-partagée :

```
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. Créez une liste d'accès qui définit le trafic à chiffrer : (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. Créez une proposition ipsec ikev2 pour référencer les algorithmes spécifiés sur le FTD :

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

7. Créez une entrée de crypto-carte qui lie la configuration et ajoutez les adresses IP FTD

Outside1 et Outside2 :

```
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. Créez une instruction d'exemption NAT qui empêche le trafic VPN d'être NATTED par le pare-feu :

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

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

FTD

Dans la ligne de commande, utilisez la commande show crypto ikev2 sa pour vérifier l'état du VPN.

Remarque : le VPN est établi avec l'adresse IP de Outside1 (10.200.1.5) comme adresse locale.

```
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
```

Route

La route par défaut affiche l'adresse IP du tronçon suivant de Outside1.

```
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
```

Suivre

Comme on le voit dans la sortie de show track 1, "Reachability is Up".

```
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

Il est nécessaire de confirmer que le trafic intéressant atteint la règle d'exemption NAT avec l'interface Outside1.

Utilisez la commande « packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail » pour vérifier la règle NAT appliquée au trafic intéressant.

```
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
```

Effectuer le basculement

Dans cet exemple, le basculement est effectué par un arrêt sur le tronçon suivant Outside1 utilisé dans la configuration du moniteur 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:
```

Route

La route par défaut utilise désormais l'adresse IP du tronçon suivant de Outside2 et l'accessibilité est désactivée.

```
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
```

Suivre

Comme on le voit dans la sortie de show track 1, "Reachability is Down" à ce point.

```
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
```

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.