Configuration du pare-feu basé sur les zones SD-WAN (ZBFW) et des fuites de route

Table des matières

Introduction

Conditions préalables

- Exigences

Composants utilisés

Informations générales

Configurer

- Diagramme du réseau
- Configuration des fuites de route
- Configuration ZBFW

Vérifier

Dépannage

- Méthode 1. Pour rechercher un VPN de destination à partir de la table OMP
- Méthode 2. Pour rechercher un VPN de destination à l'aide des commandes de la plate-forme
- Méthode 3. Pour rechercher un VPN de destination à l'aide de l'outil Packet-Trace
- Problèmes potentiels dus au basculement

Introduction

Ce document décrit comment configurer, vérifier et dépanner un pare-feu basé sur les zones (ZBFW) avec une fuite de route entre des réseaux privés virtuels (VPN).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La superposition SD-WAN Cisco permet d'obtenir une configuration initiale
- Configuration ZBFW à partir de l'interface utilisateur vManage
- Configuration de la stratégie de contrôle des fuites de route à partir de l'interface utilisateur vManage

Composants utilisés

Pour les besoins de la démonstration, ces logiciels ont été utilisés :

- Contrôleur Cisco SD-WAN vSmart avec version logicielle 20.6.2

- Contrôleur Cisco SD-WAN vManage avec version logicielle 20.6.2
- Deux routeurs de plate-forme de périphérie virtuelle Cisco IOS®-XE Catalyst 8000V avec version 17.6.2 qui s'exécutent en mode contrôleur
- Trois routeurs de plate-forme de périphérie virtuelle Cisco IOS-XE Catalyst 8000V avec version 17.6.2 qui s'exécutent en mode autonome

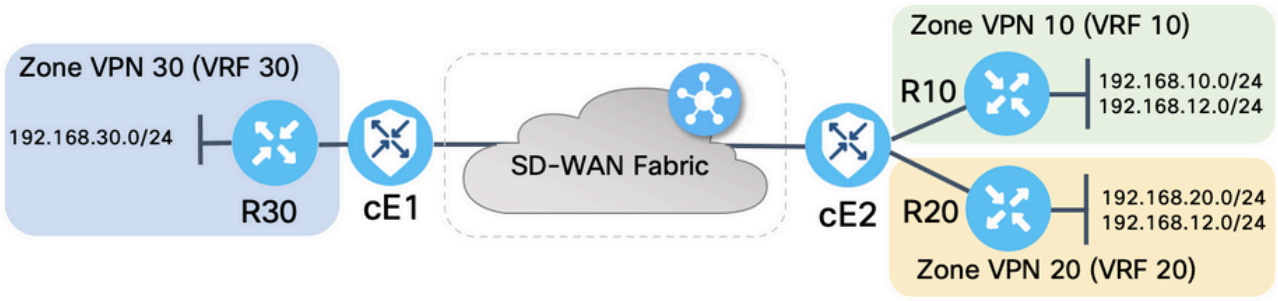
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document explique comment le routeur détermine le mappage VPN de destination dans la superposition SD-WAN et comment vérifier et dépanner les fuites de route entre les VPN. Il décrit également les particularités de la sélection de chemin dans le cas où le même sous-réseau est annoncé à partir d'un VPN différent et quel type de problèmes peuvent survenir à cause de cela.

Configurer

Diagramme du réseau



Les deux routeurs SD-WAN ont été configurés avec des paramètres de base pour établir des connexions de contrôle avec les contrôleurs SD-WAN et des connexions de plan de données entre eux. Les détails de cette configuration ne sont pas abordés dans le cadre de ce document. Le tableau ci-dessous récapitule les affectations VPN, ID de site et Zones.

	cE1	cE2
ID du site	11	12
VPN	30	10,20

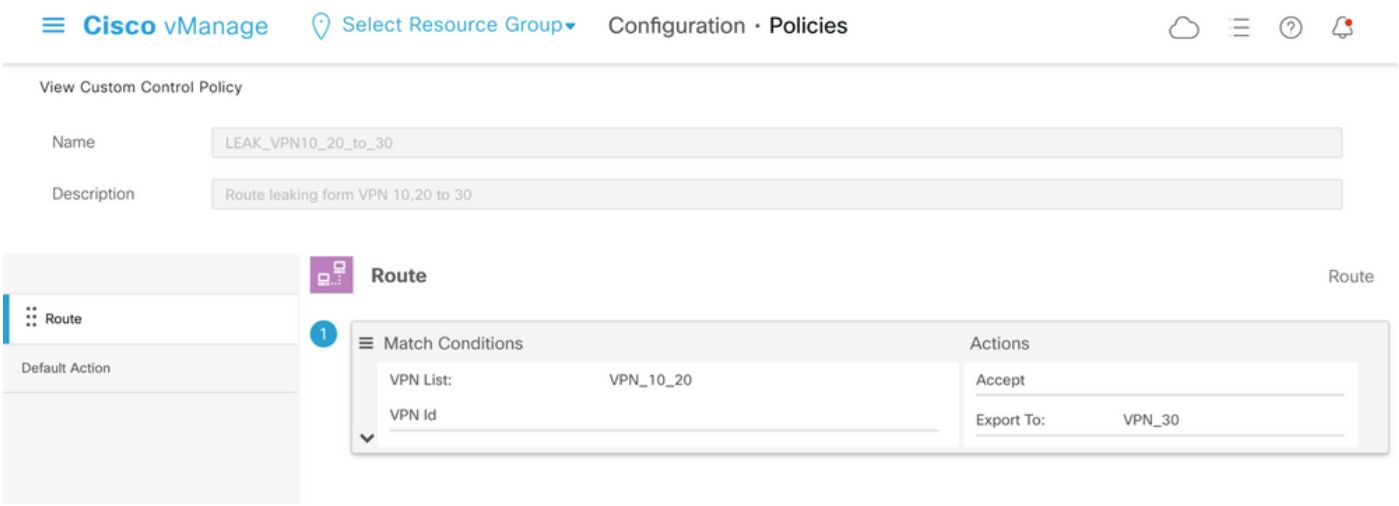
System-IP	169.254.206.11	169.254.206.12

Les routeurs côté service ont été configurés avec des routes statiques par défaut dans chaque VRF (Virtual Routing and Forwarding) qui pointe vers le routeur SD-WAN correspondant. De même, les routeurs SD-WAN Edge ont été configurés avec des routes statiques qui pointent vers les sous-réseaux correspondants. Notez que, dans le but de démontrer les problèmes potentiels de fuite de route et de ZBFW, les routeurs derrière le côté service de cE2 ont le même sous-réseau 192.168.12.0/24. Sur les deux routeurs derrière cE2, il y a une interface de bouclage configurée pour émuler un hôte avec la même adresse IP 192.168.12.12.

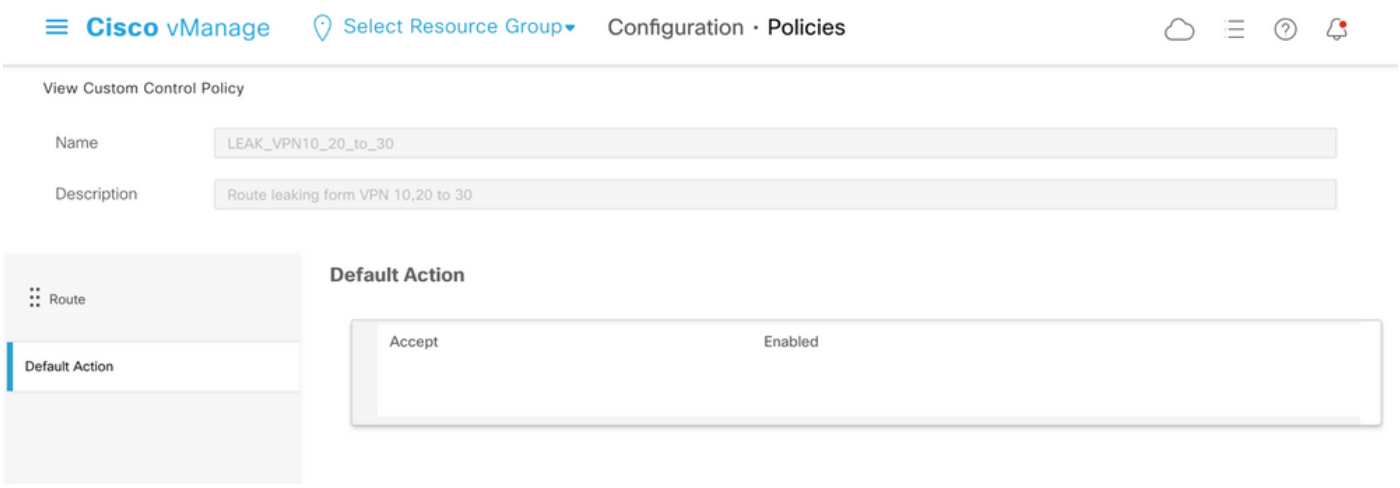
Il est important de noter que les routeurs Cisco IOS-XE R10, R20 et R30 fonctionnent en mode autonome du côté service des routes SD-WAN Edge qui servent principalement à émuler les hôtes finaux dans cette démonstration. Les interfaces de bouclage sur les routes de périphérie SD-WAN ne peuvent pas être utilisées à cette fin au lieu d'hôtes réels comme les routeurs côté service, car le trafic qui provient d'une interface dans un VRF d'un routeur de périphérie SD-WAN n'est pas considéré comme du trafic provenant de la zone ZBFW qui correspond, et appartient plutôt à la zone propre spéciale d'un routeur de périphérie. C'est pourquoi la zone ZBFW ne peut pas être considérée comme la même que la VRF. Une analyse détaillée de la zone auto n'est pas comprise dans cet article.

Configuration des fuites de route

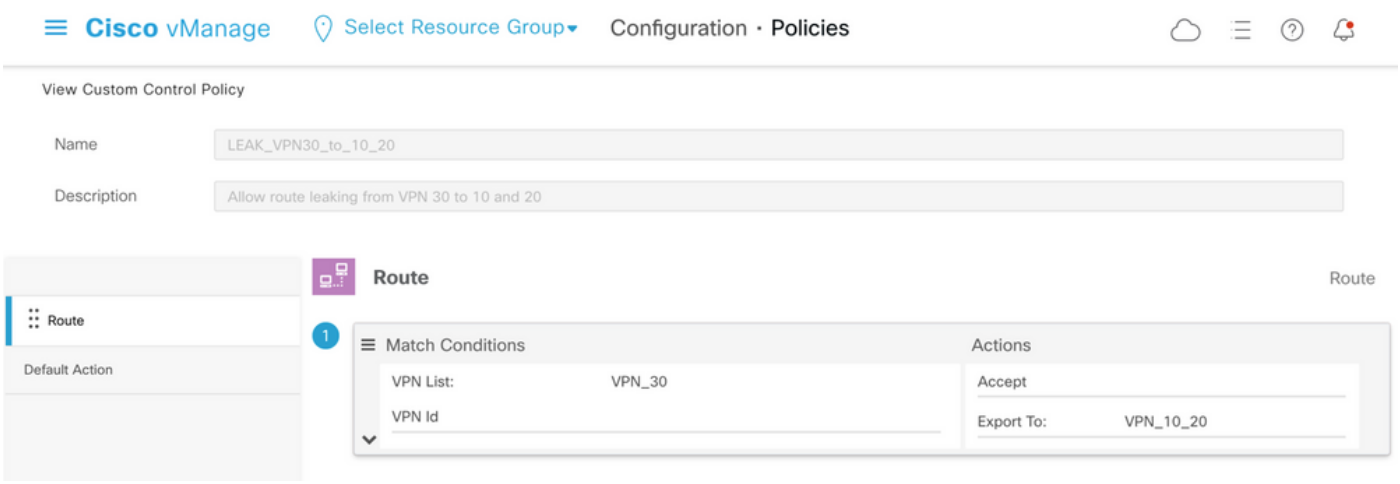
L'objectif principal de la configuration de la stratégie de contrôle est de permettre la fuite de toutes les routes du VPN 10 et 20 vers le VPN 30. Le VRF 30 existe uniquement sur le routeur cE1 et les VRF 10 et 20 sont configurés sur le routeur cE2 uniquement. Pour ce faire, deux stratégies de topologie (contrôle personnalisé) ont été configurées. Voici la topologie pour exporter toutes les routes des VPN 10 et 20 vers le VPN 30.

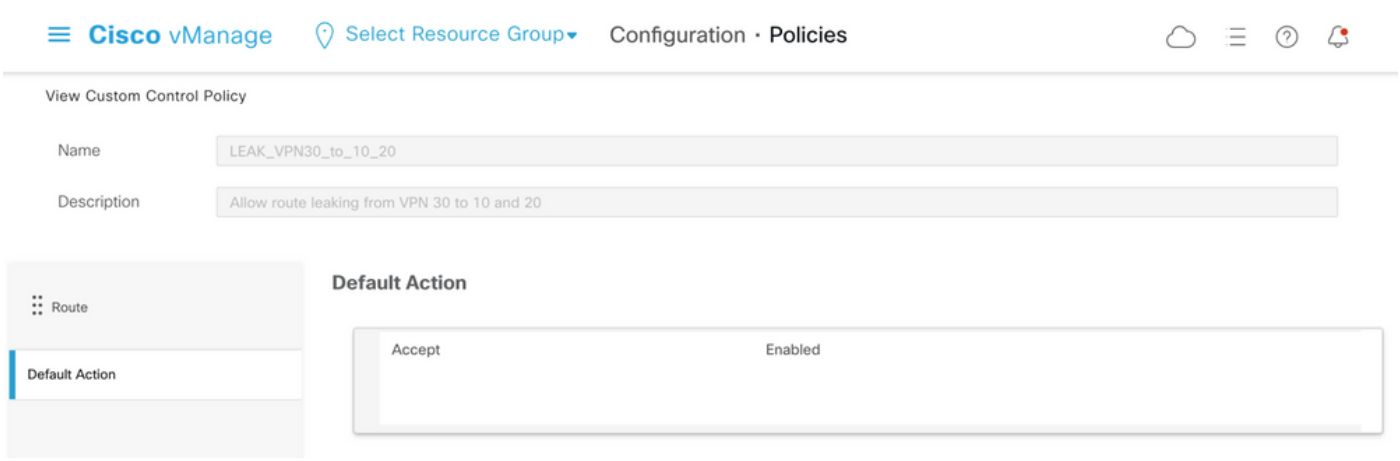


Notez que l'action par défaut est définie sur Allow, pour éviter le blocage accidentel des annonces TLOC ou des annonces de routes intra-VPN normales.

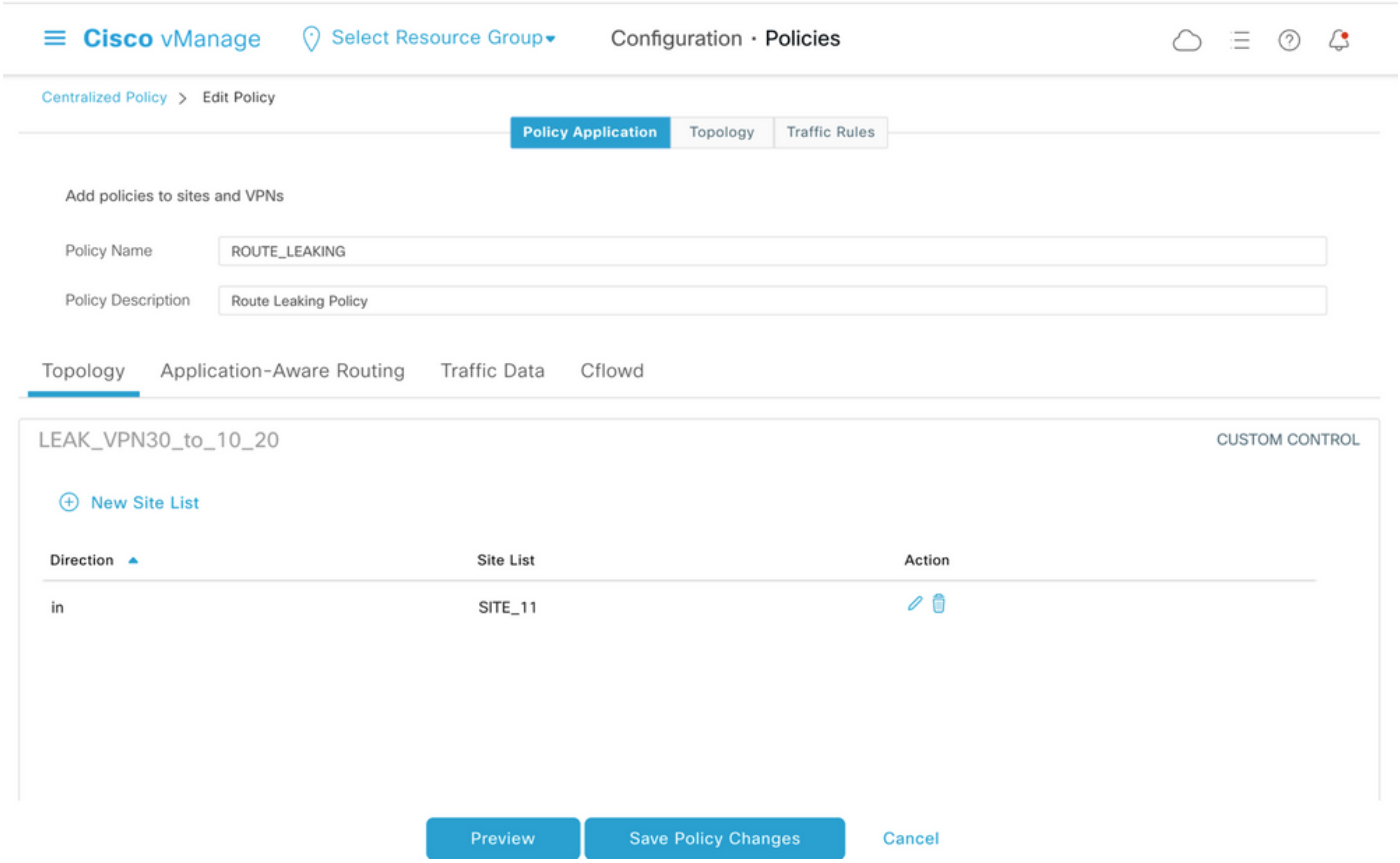


De même, la stratégie de topologie a été configurée pour autoriser l'annonce inverse des informations de routage du VPN 30 vers les VPN 10 et 20.

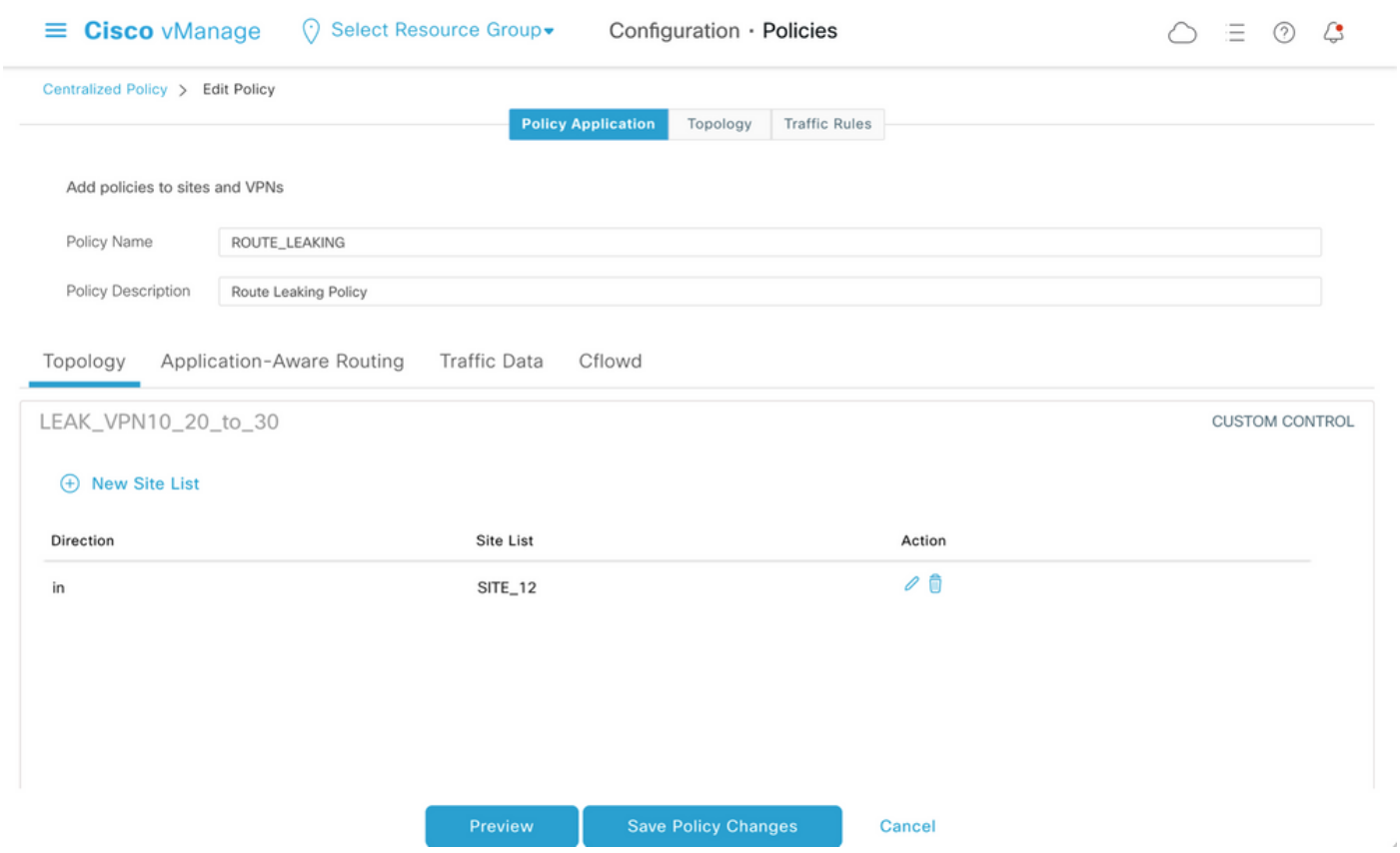




Ensuite, les deux stratégies de topologie sont affectées aux listes de sites correspondantes, dans la direction d'entrée (entrante). Les routes du VPN 30 sont exportées par le contrôleur vSmart dans les tables de protocole de gestion de superposition (OMP) des VPN 10 et 20 lorsqu'elles sont reçues de cE1 (ID de site 11).



De même, les routes provenant des VPN 10 et 20 sont exportées par vSmart dans la table de routage du VPN 30 à la réception des routes VPN 10 et 20 provenant de cE2 (ID de site 12).



Voici également un aperçu complet de la configuration de la stratégie de contrôle pour référence.

```
viptela-policy:policy
 control-policy LEAK_VPN10_20_to_30
    sequence 1
     match route
      vpn-list VPN_10_20
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      export-to vpn-list VPN_30
     !
    !
  default-action accept
 !
 control-policy LEAK_VPN30_to_10_20
    sequence 1
     match route
      vpn-list VPN_30
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      export-to vpn-list VPN_10_20
     !
    !
  default-action accept
 !
 lists
  site-list SITE_11
   site-id 11
  !
  site-list SITE_12
   site-id 12
  !
  vpn-list VPN_10_20
   vpn 10
   vpn 20
  !
  vpn-list VPN_30
   vpn 30
  !
  prefix-list _AnyIpv4PrefixList
   ip-prefix 0.0.0.0/0 le 32
  !
 !
!
apply-policy
 site-list SITE_12
  control-policy LEAK_VPN10_20_to_30 in
 !
 site-list SITE_11
  control-policy LEAK_VPN30_to_10_20 in
 !
!
```

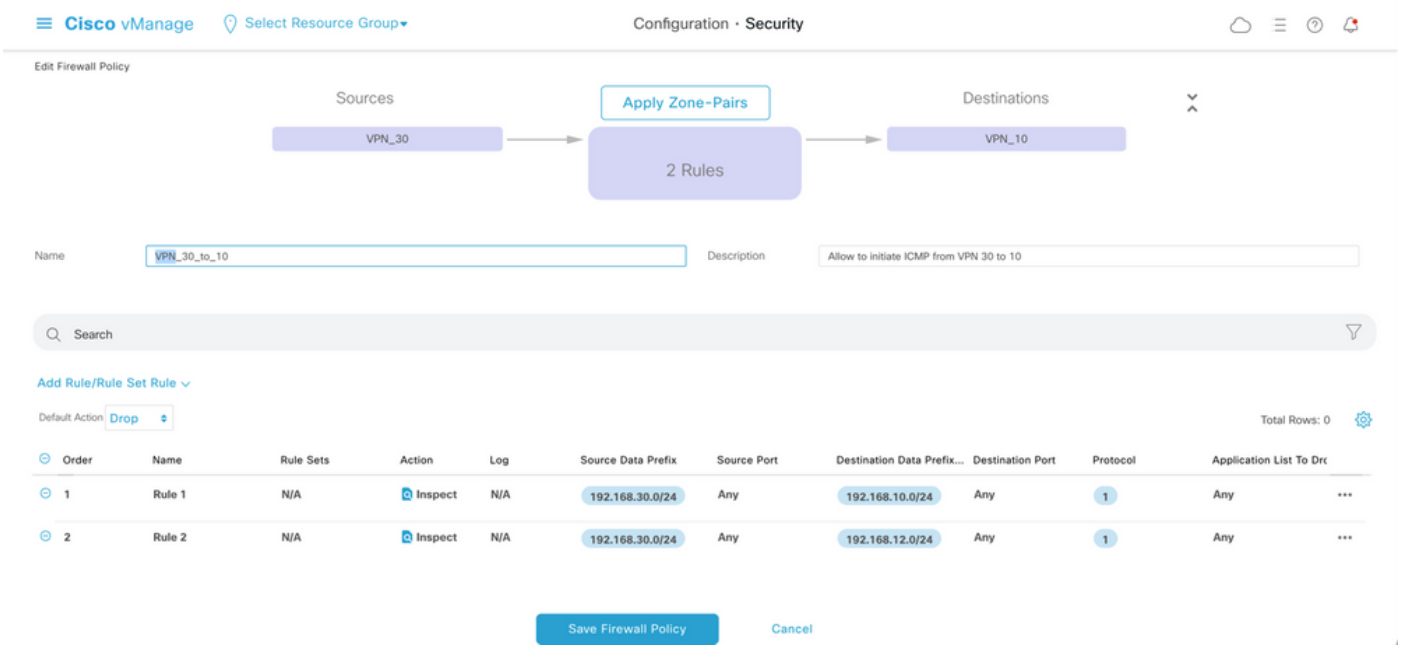
La stratégie doit être activée à partir de la section Configuration > Stratégies du contrôleur vManage pour être effective sur le contrôleur vSmart.

Configuration ZBFW

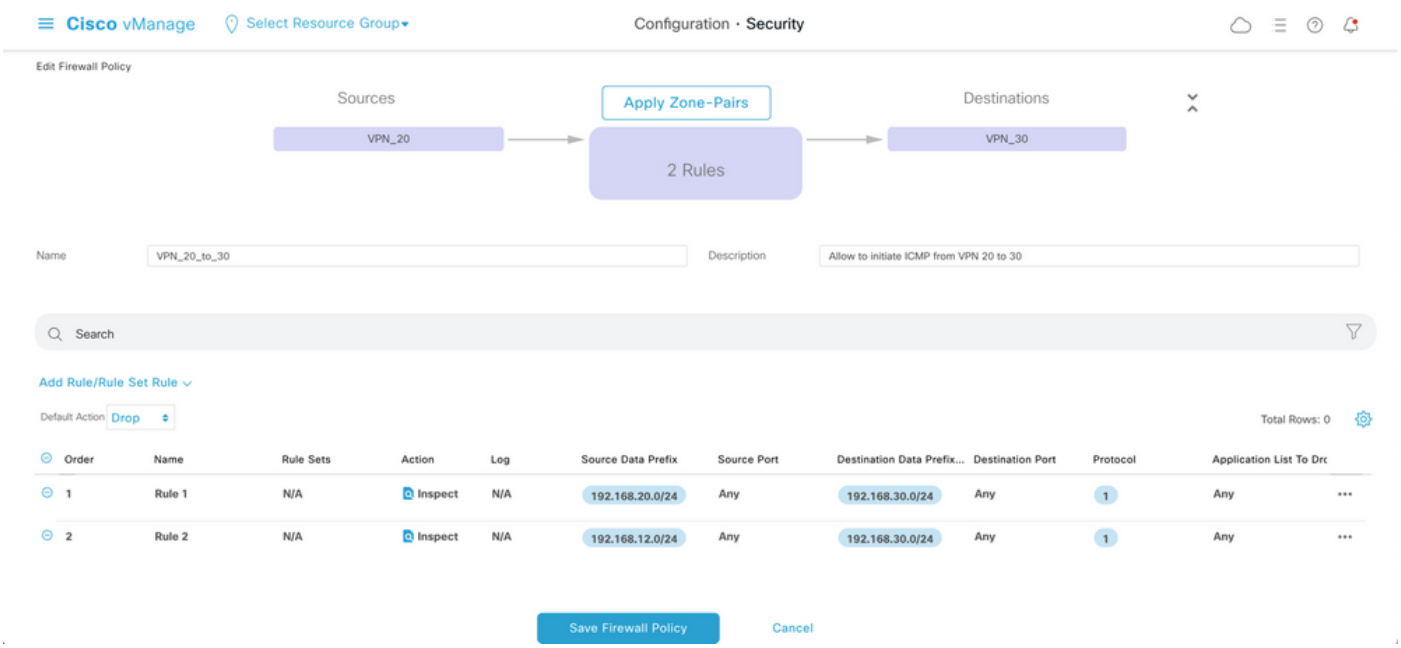
Voici un tableau qui résume ZBFW pour filtrer les exigences à des fins de démonstration dans cet article.

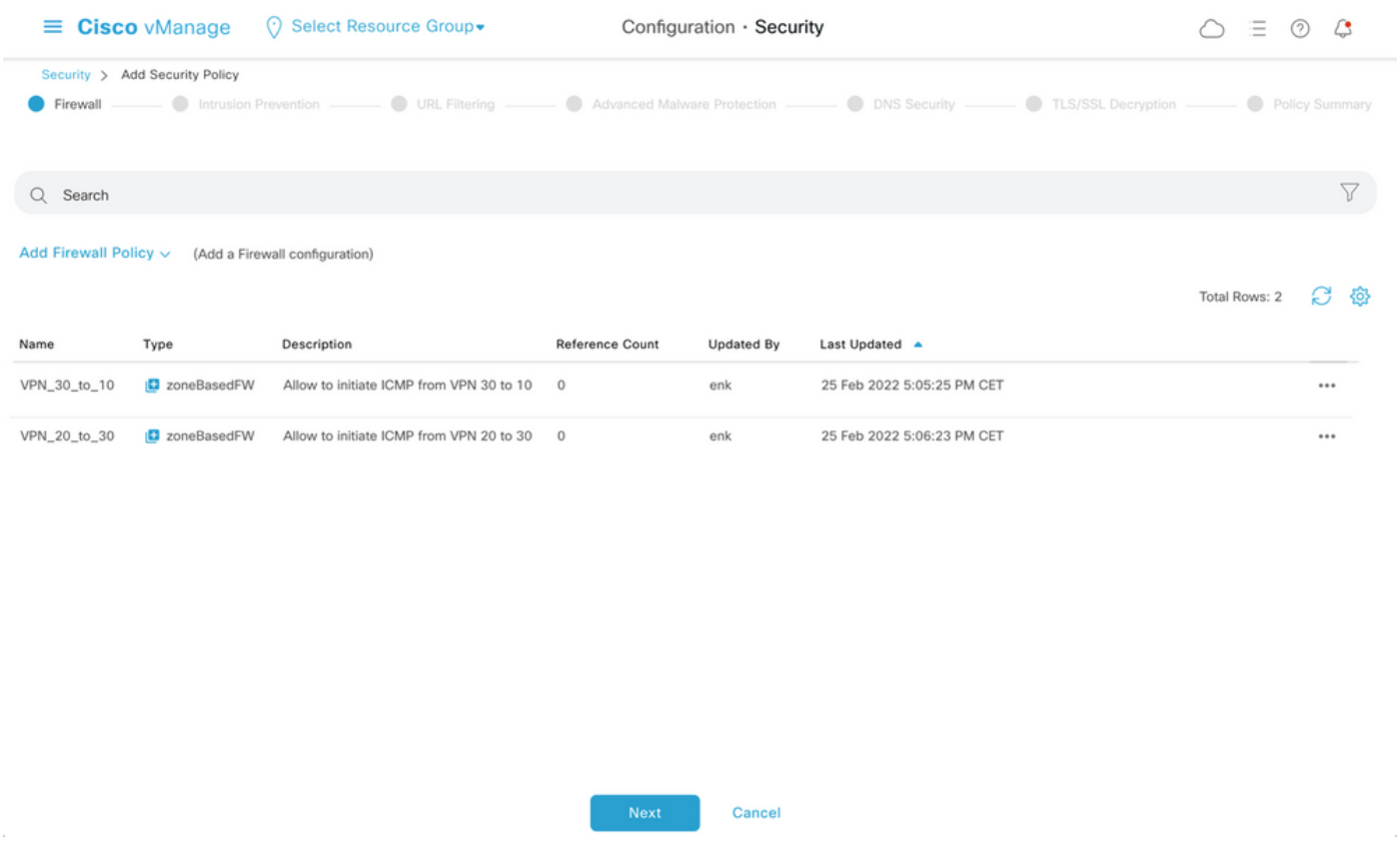
Zone de destination Zone source	VPN_10	VPN_20	VPN_30
VPN_10	autorisation à l'intérieur de la zone	Refuser	Refuser
VPN_20	Refuser	autorisation à l'intérieur de la zone	Allow
VPN_30	Allow	Refuser	autorisation à l'intérieur de la zone

L'objectif principal est d'autoriser tout trafic ICMP (Internet Control Message Protocol) provenant du côté service du routeur cE1 VPN 30 et destiné au VPN 10, mais pas au VPN 20. Le trafic de retour doit être autorisé automatiquement.



En outre, tout trafic ICMP provenant du VPN 20 côté service cE2 du routeur doit être autorisé à transiter vers le VPN 30 côté service de cE1, mais pas à partir du VPN 10. Le trafic de retour du VPN 30 vers le VPN 20 doit être autorisé automatiquement.



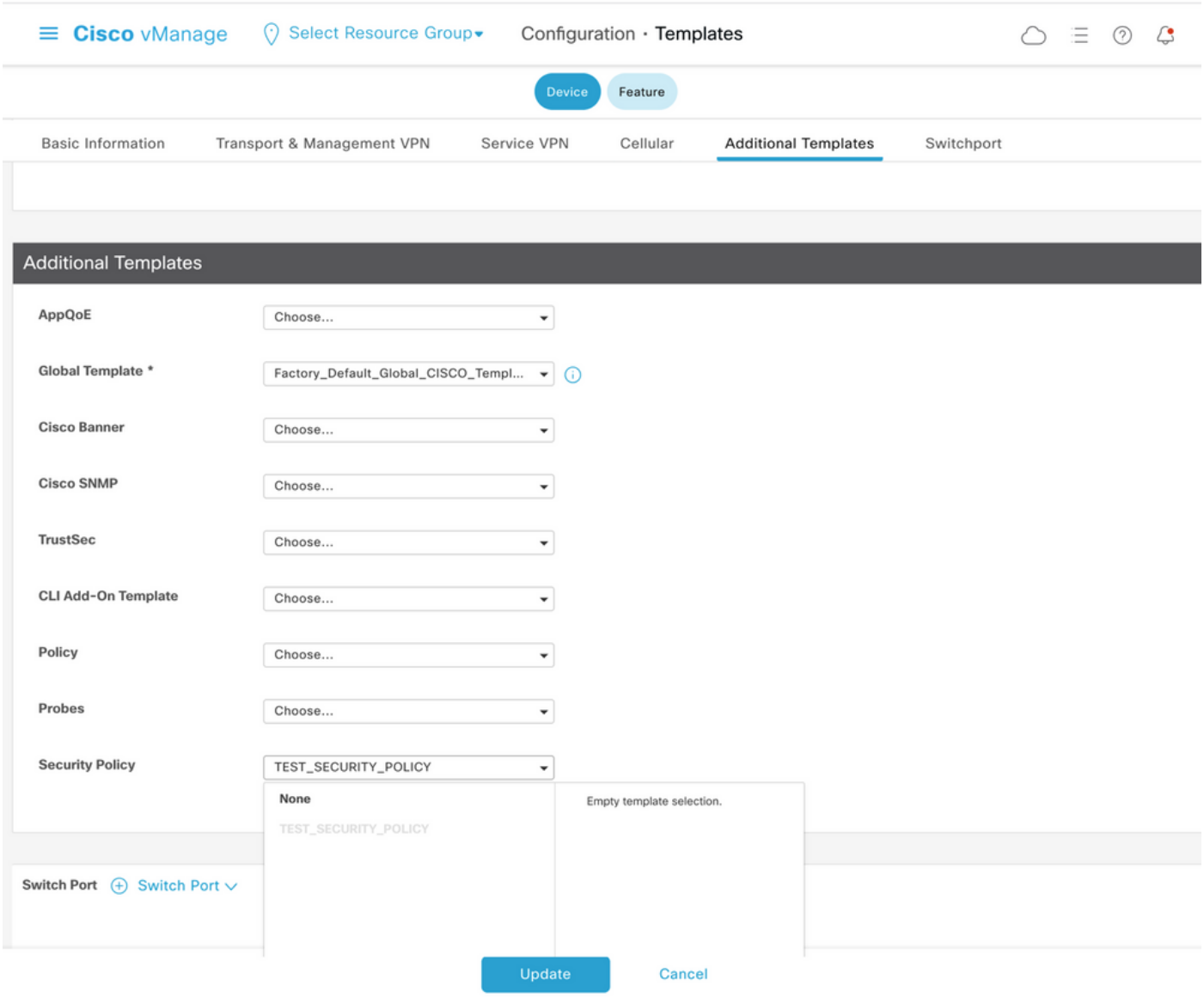


Ici, vous pouvez trouver l'aperçu de la politique ZBFW pour référence.

```
policy
 zone-based-policy VPN_20_to_30
    sequence 1
     seq-name Rule_1
     match
      source-ip 192.168.20.0/24
      destination-ip 192.168.30.0/24
      protocol 1
     !
```

```
     action inspect
     !
    !
    sequence 11
     seq-name Rule_2
     match
      source-ip 192.168.12.0/24
      destination-ip 192.168.30.0/24
      protocol 1
     !
     action inspect
     !
    !
  default-action drop
 !
 zone-based-policy VPN_30_to_10
    sequence 1
     seq-name Rule_1
     match
      source-ip 192.168.30.0/24
      destination-ip 192.168.10.0/24
      protocol 1
     !
     action inspect
     !
    !
    sequence 11
     seq-name Rule_2
     match
      protocol 1
      source-ip 192.168.30.0/24
      destination-ip 192.168.12.0/24
     !
     action inspect
     !
    !
  default-action drop
 !
  zone VPN_10
   vpn 10
  !
  zone VPN_20
   vpn 20
  !
  zone VPN_30
   vpn 30
  !
  zone-pair ZP_VPN_20_VPN_30_VPN_20_to_30
   source-zone VPN_20
   destination-zone VPN_30
   zone-policy VPN_20_to_30
  !
  zone-pair ZP_VPN_30_VPN_10_VPN_30_to_10
   source-zone VPN_30
   destination-zone VPN_10
   zone-policy VPN_30_to_10
  !
 zone-to-nozone-internet deny
!
```

Pour appliquer la stratégie de sécurité, vous devez l'attribuer dans la section du menu déroulant Stratégie de sécurité de la section Modèles supplémentaires du modèle de périphérique.



Une fois le modèle de périphérique mis à jour, la stratégie de sécurité devient active sur le périphérique sur lequel la stratégie de sécurité a été appliquée. Pour les besoins de la démonstration dans ce document, il suffisait d'activer la stratégie de sécurité sur le routeur cE1 uniquement.

Vérifier

Vous devez maintenant vérifier que les objectifs de la stratégie de sécurité (ZBFW) ont été atteints.

Le test avec ping confirme que le trafic de la zone VPN 10 vers VPN 30 est refusé comme prévu parce qu'il n'y a pas de zone-pair configurée pour le trafic de VPN 10 vers VPN 30.

```
R10#ping 192.168.30.30 source 192.168.10.10
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.10
.....
Success rate is 0 percent (0/5)
R10#ping 192.168.30.30 source 192.168.12.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.12.12
.....
Success rate is 0 percent (0/5)
```

De même, le trafic provenant du VPN 20 est autorisé vers le VPN 30 comme prévu par la configuration de la stratégie de sécurité.

```
R20#ping 192.168.30.30 source 192.168.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R20#ping 192.168.30.30 source 192.168.12.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.12.12
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Le trafic du VPN 30 vers le sous-réseau 192.168.10.0/24 dans la zone VPN 10 est autorisé comme prévu par la configuration de la stratégie.

```
R30#ping 192.168.10.10 source 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.30
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Le trafic du VPN 30 vers le sous-réseau 192.168.20.0/24 dans la zone VPN 20 est refusé car aucune paire de zones n'est configurée pour ce trafic, ce qui est attendu.

```
R30#ping 192.168.20.20 source 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.30
.....
Success rate is 0 percent (0/5)
```

Des résultats supplémentaires qui peuvent vous intéresser peuvent être observés lorsque vous essayez d'envoyer une requête ping à l'adresse IP 192.168.12.12 parce qu'elle peut être dans la zone VPN 10 ou VPN 20, et il est impossible de déterminer le VPN de destination du point de vue du routeur R30 situé du côté service du routeur de périphérie SD-WAN cE1.

```
R30#ping 192.168.12.12 source 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.30
.....
Success rate is 0 percent (0/5)
```

Le résultat est le même pour toutes les sources dans VRF 30. Cela confirme qu'il ne dépend pas des résultats de la fonction de hachage ECMP (Equal-Cost Multi-Path) :

```
R30#ping 192.168.12.12 source 192.168.30.31
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.31
.....
Success rate is 0 percent (0/5)
R30#ping 192.168.12.12 source 192.168.30.32
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.32
.....
Success rate is 0 percent (0/5)
```

D'après les résultats des tests pour l'adresse IP de destination 192.168.12.12, vous pouvez seulement deviner qu'elle se trouve dans le VPN 20 parce qu'elle ne répond pas aux requêtes d'écho ICMP et qu'elle est très probablement bloquée parce qu'il n'y a pas de zone-pair configurée pour autoriser le trafic du VPN 30 vers le VPN 20 (comme souhaité). Si une destination avec la même adresse IP 192.168.12.12 se trouve dans le VPN 10 et est supposée répondre à une requête d'écho ICMP, alors conformément à la politique de sécurité ZBFW pour le trafic ICMP du VPN 30 au VPN 20, le trafic doit être autorisé. Vous devez confirmer le VPN de destination.

Dépannage

Méthode 1. Pour rechercher un VPN de destination à partir de la table OMP

Une simple vérification de la table de routage sur cE1 n'aide pas à comprendre le VPN de destination réel. Les informations les plus utiles que vous pouvez obtenir du résultat sont une adresse IP système de la destination (169.254.206.12) et aussi qu'il n'y a pas d'ECMP qui se produit.

```
cE1# show ip route vrf 30 192.168.12.0 255.255.255.0

Routing Table: 30
Routing entry for 192.168.12.0/24
  Known via "omp", distance 251, metric 0, type omp
  Last update from 169.254.206.12 on Sdwan-system-intf, 01:34:24 ago
  Routing Descriptor Blocks:
  * 169.254.206.12 (default), from 169.254.206.12, 01:34:24 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
```

Pour connaître le VPN de destination, vous devez d'abord trouver l'étiquette de service dans la table OMP sur cE1 pour le préfixe d'intérêt.

```
cE1#show sdwan omp routes vpn 30 192.168.12.0/24
Generating output, this might take time, please wait ...
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
                PATH                      ATTRIBUTE
FROM PEER       ID     LABEL    STATUS    TYPE       TLOC IP          COLOR            ENCAP  PREFEREN
-----------------------------------------------------------------------------------------------------
169.254.206.4   12     1007     C,I,R     installed  169.254.206.12   private2         ipsec  -
```

Nous pouvons voir que la valeur d'étiquette est 1007. Enfin, le VPN de destination peut être trouvé si tous les services qui proviennent du routeur qui possède l'adresse IP système 169.254.206.12 sont vérifiés sur le contrôleur vSmart.

```
vsmart1# show omp services family ipv4 service VPN originator 169.254.206.12
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                PATH
```

```
VPN    SERVICE  ORIGINATOR      FROM PEER        ID     LABEL    STATUS
--------------------------------------------------------------------------
1      VPN      169.254.206.12  169.254.206.12   82     1003     C,I,R
2      VPN      169.254.206.12  169.254.206.12   82     1004     C,I,R
10     VPN      169.254.206.12  169.254.206.12   82     1006     C,I,R
17     VPN      169.254.206.12  169.254.206.12   82     1005     C,I,R
20     VPN      169.254.206.12  169.254.206.12   82     1007     C,I,R
```

Sur la base de l'étiquette VPN 1007, il est possible de confirmer que le VPN de destination est 20.

Méthode 2. Pour rechercher un VPN de destination à l’aide des commandes de la plate-forme

Pour découvrir le VPN de destination à l'aide des commandes de plate-forme, vous devez d'abord obtenir un ID VRF interne pour VPN 30 sur le routeur cE1 à l'aide des commandes show ip vrf detail 30 ou show platform software ip f0 cef table * summary.

```
cE1#show ip vrf detail 30 | i Id
VRF 30 (VRF Id = 1); default RD 1:30; default VPNID
```

```
cE1#show platform software ip f0 cef table * summary | i VRF|^30
Name             VRF id  Table id    Protocol         Prefixes    State
30               1       1           IPv4             21          hw: 0x561b60f07a50 (created)
```

Dans ce cas, l’ID VRF 1 a été attribué au VRF nommé 30. Les commandes de la plate-forme révèlent la chaîne d’objets OCE (Output Chain Element) du logiciel SD-WAN qui représente la logique de transfert interne qui détermine le chemin des paquets dans le logiciel Cisco IOS-XE :

```
cE1#show platform software ip F0 cef table index 1 prefix 192.168.12.0/24 oce
=== Prefix OCE ===
Prefix/Len: 192.168.12.0/24
  Next Obj Type: OBJ_SDWAN_NH_SLA_CLASS
  Next Obj Handle: 0xf800045f, urpf: 0
  Prefix Flags: unknown
  aom id: 1717, HW handle: 0x561b60eeba20 (created)
```

Le préfixe d'intérêt pointe vers l'objet de tronçon suivant du type de classe de contrat de niveau de service (SLA) (OBJ_SDWAN_NH_SLA_CLASS) avec l'ID 0xf800045f qui peut être vérifié plus avant est indiqué ici :

```
cE1#show platform software sdwan F0 next-hop sla id 0xf800045f
SDWAN Nexthop OCE

SLA: num_class 16, client_handle 0x561b610c3f10, ppe addr 0xdbce6c10
  SLA_0: num_nhops 1, Fallback_sla_flag TDL_FALSE, nhobj_type SDWAN_NH_INDIRECT
  ECMP: 0xf800044f 0xf800044f 0xf800044f 0xf800044f
        0xf800044f 0xf800044f 0xf800044f 0xf800044f
        0xf800044f 0xf800044f 0xf800044f 0xf800044f
        0xf800044f 0xf800044f 0xf800044f 0xf800044f
  SLA_1: num_nhops 0, Fallback_sla_flag TDL_FALSE, nhobj_type ADJ_DROP
  ECMP: 0xf800000f 0xf800000f 0xf800000f 0xf800000f
        0xf800000f 0xf800000f 0xf800000f 0xf800000f
        0xf800000f 0xf800000f 0xf800000f 0xf800000f
        0xf800000f 0xf800000f 0xf800000f 0xf800000f
```

Il s'agit d'une sortie longue, de sorte que les classes SLA de 2 à 15 ont été ignorées car aucune classe SLA de secours n'est configurée, et toutes pointent vers la même contiguïté DROP spéciale que SLA 1. L'intérêt principal est l'objet de tronçon suivant de type indirect (SDWAN_NH_INDIRECT) à partir de SLA 0. Nous pouvons également noter qu'il n'y a pas d'ECMP et que tous les ID sont identiques (0xf800044f). Il peut être vérifié pour trouver le VPN de destination ultime et l'étiquette de service.

```
cE1#show platform software sdwan F0 next-hop indirect id 0xf800044f
SDWAN Nexthop OCE

Indirect: client_handle 0x561b610f8140, ppe addr 0xd86b4cf0
  nhobj_type: SDWAN_NH_LOCAL_SLA_CLASS, nhobj_handle: 0xf808037f
  label: 1007, vpn: 20, sys-ip: 169.254.206.12, vrf_id: 1, sla_class: 1
```

Méthode 3. Pour rechercher un VPN de destination à l'aide de l'outil Packet-Trace

Un autre moyen de trouver un VPN de destination est un outil de trace de paquets qui peut analyser les paquets réels qui s'exécutent à travers le routeur en temps réel. La condition de débogage est définie pour faire correspondre le trafic uniquement avec l'adresse IP 192.168.12.12.

```
cE1#debug platform condition ipv4 192.168.12.12/32 both
cE1#debug platform packet-trace packet 10
 Please remember to turn on 'debug platform condition start' for packet-trace to work
cE1#debug platform condition start
```

Ensuite, si le trafic a été initié à partir de R30 avec l'aide de ping, vous pouvez voir les paquets correspondants sur cE1 et vérifier chaque détail de paquet. Dans ce cas, il s'agit par exemple du tout premier paquet numéro 0. Les lignes les plus importantes sont mises en évidence par les signes <<<<.

```
cE1#show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
1     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
2     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
3     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
4     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
5     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)


cE1#show platform packet-trace packet 0
Packet: 0           CBUG ID: 0
Summary
  Input     : GigabitEthernet6
  Output    : Tunnel3
  State     : DROP 52  (FirewallL4Insp) <<<<<<<<<<<<<<<<<<<<<<<<<
  Timestamp
    Start   : 161062920614751 ns (03/24/2022 16:19:31.754050 UTC)
    Stop    : 161062920679374 ns (03/24/2022 16:19:31.754114 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet6
    Output      :




    Source      : 192.168.30.30
    Destination : 192.168.12.12
    Protocol    : 1 (ICMP)
  Feature: SDWAN Forwarding
    SDWAN adj OCE:
    Output       : GigabitEthernet3
    Hash Value   : 0xda
    Encap        : ipsec
    SLA          : 0
    SDWAN VPN    : 20
    SDWAN Proto  : IPV4
    Out Label    : 1007 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Local Color  : private2
    Remote Color : private2
    FTM Tun ID   : 218
    SDWAN Session Info
      SRC IP       : 192.168.10.11
      SRC Port     : 12366
      DST IP       : 192.168.10.12
      DST Port     : 12346
      Remote System IP : 169.254.206.12
      Lookup Type : TUN_DEMUX
      Service Type : NONE
  Feature: ZBFW
    Action  : Drop
    Reason  : No Zone-pair found <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Zone-pair name         : N/A <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

```
    Class-map name         : N/A
    Policy    name         : N/A
    Input interface        : GigabitEthernet6
    Egress interface       : Tunnel3
    Input  VPN ID          : 30
    Output VPN ID          : 20 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Input  VRF ID:Name     : 1:30
    Output VRF ID:Name     : 1:30
    AVC Classification ID  : 0
    AVC Classification name: N/A
    UTD Context ID         : 0
```

Un suivi de paquets indique que les cinq paquets d'écho ICMP envoyés par la commande ping ont été abandonnés avec le code d'abandon 52 (FirewallL4). Fonction de section : Le transfert SDWAN indique que le VPN de destination est 20 et que l'étiquette de service 1007 dans l'en-tête interne du paquet tunnelisé est utilisée pour transférer pour désigner le VPN de destination sur cE2. Section Feature : ZBFW confirme en outre que les paquets ont été abandonnés car la paire de zones n'était pas configurée pour le trafic du VPN d'entrée 20 destiné à la zone VPN 30.

Problèmes potentiels dus au basculement

Que se passe-t-il si la route 192.168.12.0/24 est retirée par R20 ou n'est plus accessible à partir de cE2 dans VRF 20 ? Bien que du point de vue du VRF 30, le sous-réseau soit le même, car la politique de sécurité ZBFW traite le trafic de la zone VPN 30 vers les zones VPN 20 et 10 différemment, il peut conduire à des résultats indésirables comme le trafic autorisé, alors qu'il ne doit pas l'être ou vice versa.

Par exemple, si vous simulez une défaillance d'une liaison entre les routeurs cE2 et R20. Cela entraîne le retrait de la route 192.168.12.0/24 de la table de routage VPN 20 sur le contrôleur vSmart et, à la place, la route VPN 10 est filtrée dans la table de routage VPN 30. La connectivité du VPN 30 au VPN 10 est autorisée conformément à la stratégie de sécurité appliquée sur cE1 (ceci est attendu du point de vue de la stratégie de sécurité, mais ne peut pas être souhaitable pour le sous-réseau spécifique présenté dans les deux VPN).

```
cE1#show platform packet-trace packet 0
Packet: 0           CBUG ID: 644
Summary
  Input     : GigabitEthernet6
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 160658983624344 ns (03/24/2022 16:12:47.817059 UTC)
    Stop    : 160658983677282 ns (03/24/2022 16:12:47.817112 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet6
    Output      :
```

```
    Source      : 192.168.30.30
    Destination : 192.168.12.12
    Protocol    : 1 (ICMP)
  Feature: SDWAN Forwarding
    SDWAN adj OCE:
    Output       : GigabitEthernet3
    Hash Value   : 0xda
    Encap        : ipsec
    SLA          : 0
    SDWAN VPN    : 10
    SDWAN Proto  : IPV4
    Out Label    : 1006
    Local Color  : private2
    Remote Color : private2
    FTM Tun ID   : 188
    SDWAN Session Info
      SRC IP       : 192.168.10.11
      SRC Port     : 12366
      DST IP       : 192.168.10.12
      DST Port     : 12346
      Remote System IP : 169.254.206.12
      Lookup Type : TUN_DEMUX
      Service Type : NONE
  Feature: ZBFW
    Action  : Fwd
    Zone-pair name         : ZP_VPN_30_VPN_10_VPN_30_to_10
    Class-map name         : VPN_30_to_10-seq-11-cm_
    Policy    name         : VPN_30_to_10
    Input interface        : GigabitEthernet6
    Egress interface       : Tunnel3
    Input  VPN ID          : 30
    Output VPN ID          : 10
    Input  VRF ID:Name     : 1:30
    Output VRF ID:Name     : 1:30
    AVC Classification ID  : 0
    AVC Classification name: N/A
    UTD Context ID         : 0
  Feature: IPSec
    Result    : IPSEC_RESULT_SA
    Action    : ENCRYPT
    SA Handle : 74
    Peer Addr : 192.168.10.12
    Local Addr: 192.168.10.11
```

Notez que l'étiquette 1006 a été utilisée au lieu de 1007 et que l'ID VPN de sortie est 10 au lieu de 20 maintenant. En outre, le paquet a été autorisé conformément à la politique de sécurité ZBFW, et les noms de zone-paire, class-map et de politique correspondants ont été donnés.

Il y a un problème encore plus important qui peut survenir du fait que la route la plus ancienne est conservée dans la table de routage du VPN 30 et dans ce cas, c'est la route du VPN 10 qui après l'application de la politique de contrôle initiale, la route du VPN 20 a fui dans la table OMP du VPN 30 sur vSmart. Imaginez le scénario où l'idée initiale était exactement le contraire de la logique de

la stratégie de sécurité ZBFW décrite dans cet article. Par exemple, l'objectif était d'autoriser le trafic du VPN 30 vers le VPN 20 et non vers le VPN 10. S'il a été autorisé après une configuration de stratégie initiale, puis après l'échec ou le retrait de la route 192.168.12.0/24 du VPN 20, le trafic reste bloqué vers le sous-réseau 192.168.12.0/24 même après la récupération, car la route 192.168.12.0/24 fuit toujours du VPN 10.

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.