

# Configuration du pare-feu basé sur une zone de SD-WAN (ZBFW) et des fuites de route

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration des fuites de route](#)

[Configuration ZBFW](#)

[Vérification](#)

[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 une zone (ZBFW) avec une fuite de route entre des réseaux privés virtuels (VPN).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La superposition Cisco SD-WAN présente une configuration initiale
- Configuration ZBFW à partir de l'interface utilisateur vManage
- Configuration de stratégie de contrôle de fuite de route à partir de l'interface utilisateur vManage

## Components Used

Aux fins 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 logicielle 17.6.2 fonctionnant en mode contrôleur
- Trois routeurs de plate-forme de périphérie virtuelle Cisco IOS-XE Catalyst 8000V avec version logicielle 17.6.2 fonctionnant en mode autonome

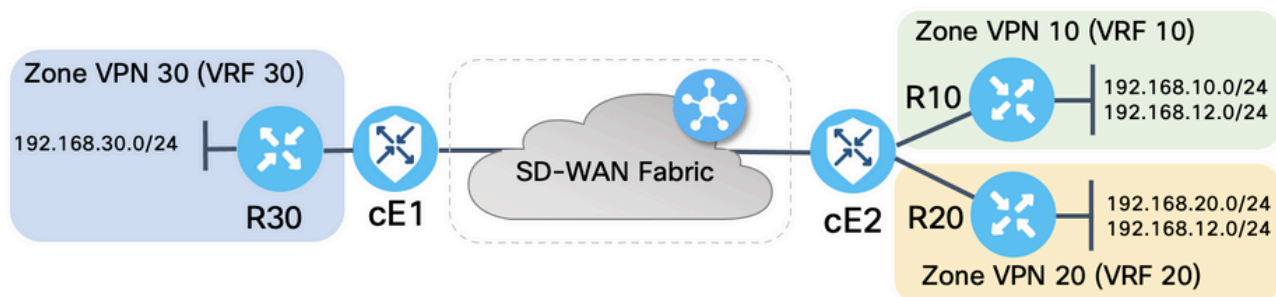
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## 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 du chemin dans le cas où le même sous-réseau est annoncé à partir d'un autre VPN et quel type de problème peut survenir à cause de cela.

## Configuration

### Diagramme du réseau



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

	cE1	cE2
ID de 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 de périphérie SD-WAN ont été configurés avec des routes statiques qui pointent vers les sous-réseaux qui correspondent. Notez que, pour illustrer les problèmes potentiels liés aux fuites de route et au ZBFW, les routeurs situés derrière le côté service de cE2 ont le même sous-réseau 192.168.12.0/24. Sur les deux routeurs derrière cE2, une interface de bouclage est 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 sur les côtés de service des routes de périphérie SD-WAN 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 tels que les routeurs côté service, car le trafic qui provient d'une interface dans un VRF d'un routeur Edge SD-WAN n'est pas considéré comme le trafic provenant de la zone ZBFW qui correspond et appartient plutôt à la zone autonome spéciale d'un routeur de périphérie. C'est pourquoi la zone ZBFW ne peut pas être considérée comme identique à VRF. Une discussion détaillée de la zone d'auto n'entre pas dans le champ d'application de cet article.

## Configuration des fuites de route

L'objectif principal de la configuration de la stratégie de contrôle est de permettre la fuite de route de toutes les routes de VPN 10 et 20 vers VPN 30. 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 de VPN 10 et 20 vers VPN 30.

The screenshot shows the Cisco vManage interface for configuring a Custom Control Policy. The policy name is 'LEAK\_VPN10\_20\_to\_30' and the description is 'Route leaking form VPN 10,20 to 30'. The configuration is for a 'Route' match condition. The match conditions are: VPN List: VPN\_10\_20, and VPN Id: VPN\_30. The action is 'Accept'.

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

The screenshot shows the 'Default Action' configuration for the Custom Control Policy. The action is 'Accept' and it is 'Enabled'.

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

View Custom Control Policy

Name: LEAK\_VPN30\_to\_10\_20  
 Description: Allow route leaking from VPN 30 to 10 and 20

- Route
- Default Action

### Route

**Match Conditions**

VPN List: VPN\_30

VPN Id:

**Actions**

Accept:

Export To: VPN\_10\_20

Route

View Custom Control Policy

Name: LEAK\_VPN30\_to\_10\_20  
 Description: Allow route leaking from VPN 30 to 10 and 20

- Route
- Default Action

### Default Action

Accept: Enabled

Ensuite, les deux stratégies de topologie sont affectées aux listes de sites qui correspondent, dans la direction d'entrée (entrante). Les routes de VPN 30 sont exportées par le contrôleur vSmart dans les tables OMP (Overlay Management Protocol) de VPN 10 et 20 lorsqu'elles sont reçues de cE1 (id de site 11).

Centralized Policy > Edit Policy

Policy Application | Topology | Traffic Rules

Add policies to sites and VPNs

Policy Name: ROUTE\_LEAKING  
 Policy Description: Route Leaking Policy

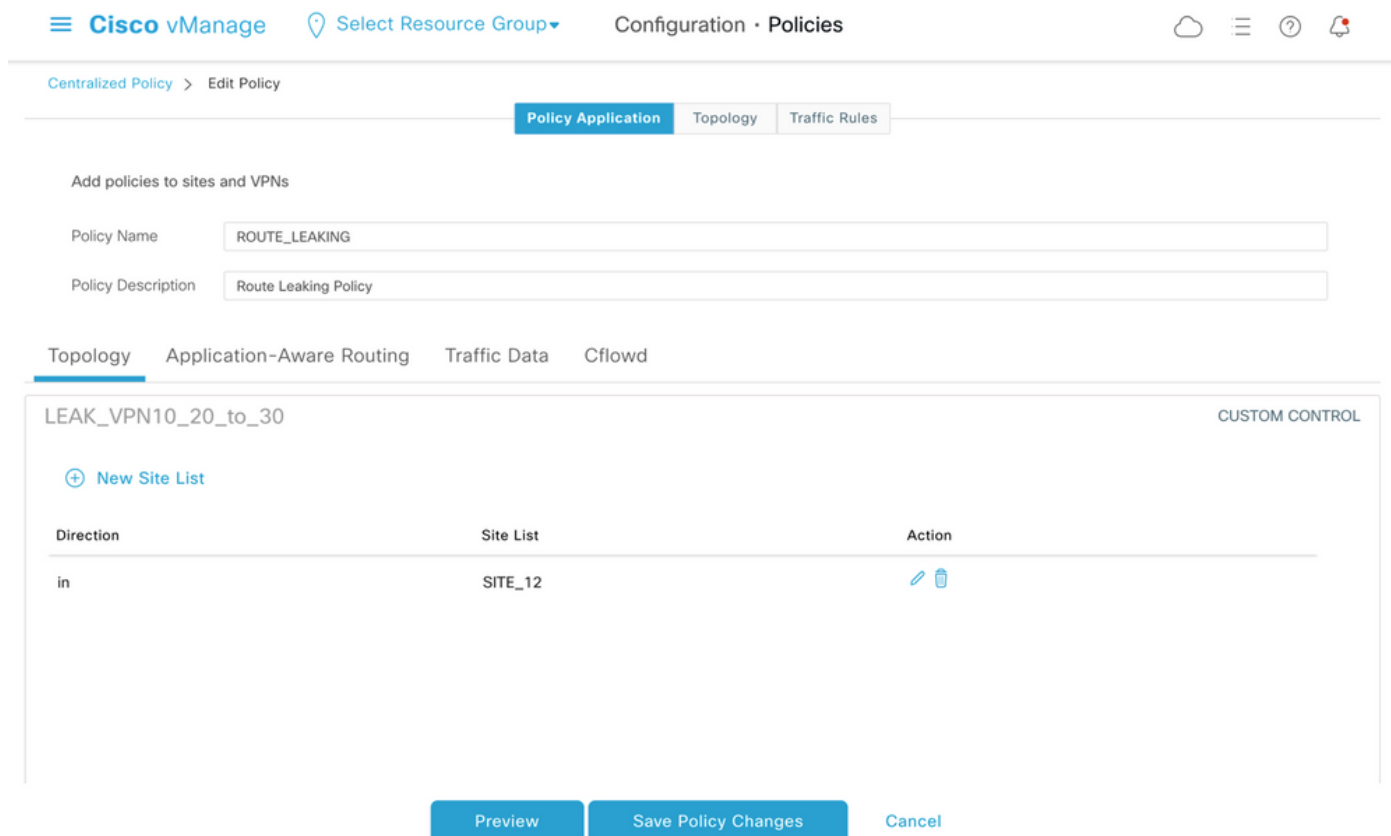
Topology | Application-Aware Routing | Traffic Data | Cflowd

LEAK\_VPN30\_to\_10\_20 CUSTOM CONTROL

[+ New Site List](#)

Direction	Site List	Action
in	SITE_11	<a href="#">✎</a> <a href="#">🗑️</a>

De même, les routes de VPN 10 et 20 sont exportées par vSmart dans la table de routage VPN 30 à la réception des routes VPN 10 et 20 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	VPN_10	VPN_20	VPN_30
Zone source			
VPN_10	intra-zone allow	Refuser	Refuser
VPN_20	Refuser	intra-zone allow	Allow
VPN_30	Allow	Refuser	intra-zone allow

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.

Cisco vManage Configuration · Security

Edit Firewall Policy



Name: VPN\_30\_to\_10 Description: Allow to initiate ICMP from VPN 30 to 10

Search

Add Rule/Rule Set Rule

Default Action: Drop


Order	Name	Rule Sets	Action	Log	Source Data Prefix	Source Port	Destination Data Prefix...	Destination Port	Protocol	Application List To Drc
1	Rule 1	N/A	Inspect	N/A	192.168.30.0/24	Any	192.168.10.0/24	Any	1	Any
2	Rule 2	N/A	Inspect	N/A	192.168.30.0/24	Any	192.168.12.0/24	Any	1	Any

Save Firewall Policy Cancel

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

Cisco vManage Configuration · Security

Edit Firewall Policy



Name: VPN\_20\_to\_30 Description: Allow to initiate ICMP from VPN 20 to 30

Search

Add Rule/Rule Set Rule

Default Action: Drop

Order	Name	Rule Sets	Action	Log	Source Data Prefix	Source Port	Destination Data Prefix...	Destination Port	Protocol	Application List To Drc
1	Rule 1	N/A	Inspect	N/A	192.168.20.0/24	Any	192.168.30.0/24	Any	1	Any
2	Rule 2	N/A	Inspect	N/A	192.168.12.0/24	Any	192.168.30.0/24	Any	1	Any

Save Firewall Policy Cancel

Add Firewall Policy ▼ (Add a Firewall configuration)Total Rows: 2  

Name	Type	Description	Reference Count	Updated By	Last Updated	
VPN_30_to_10	 zoneBasedFW	Allow to initiate ICMP from VPN 30 to 10	0	enk	25 Feb 2022 5:05:25 PM CET	...
VPN_20_to_30	 zoneBasedFW	Allow to initiate ICMP from VPN 20 to 30	0	enk	25 Feb 2022 5:06:23 PM CET	...

[Next](#)[Cancel](#)

Vous trouverez ici l'aperçu de la stratégie 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 une stratégie de sécurité, elle doit être affectée dans la section de menu déroulant **Stratégie de sécurité** de la section **Modèles supplémentaires** du modèle de périphérique.

Cisco vManage Select Resource Group Configuration · Templates

Device Feature

Basic Information Transport & Management VPN Service VPN Cellular **Additional Templates** Switchport

**Additional Templates**

AppQoE Choose...

Global Template \* Factory\_Default\_Global\_CISCO\_Templ... ⓘ

Cisco Banner Choose...

Cisco SNMP Choose...

TrustSec Choose...

CLI Add-On Template Choose...

Policy Choose...

Probes Choose...

Security Policy TEST\_SECURITY\_POLICY

None  
TEST\_SECURITY\_POLICY

Empty template selection.

Switch Port + Switch Port v

Update Cancel

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 présentée dans ce document, il suffisait d'activer la stratégie de sécurité sur le routeur cE1 uniquement.

## Vérification

Maintenant, vous devez vérifier que les objectifs de la stratégie de sécurité requise (ZBFW) ont été atteints.

Le test avec **ping** confirme que le trafic de la zone VPN 10 à VPN 30 est refusé comme prévu car aucune zone-paire n'est configurée pour le trafic de VPN 10 à 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 de VPN 20 est autorisé vers 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 de 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 de 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 peuvent vous intéresser lorsque vous essayez d'envoyer une requête ping à l'adresse IP 192.168.12.12, car elle peut se trouver 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. Ceci 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 du test pour l'adresse IP de destination 192.168.12.12, vous pouvez seulement deviner qu'elle se trouve dans VPN 20 parce qu'elle ne répond pas aux requêtes d'écho ICMP et qu'elle est probablement bloquée parce qu'il n'y a aucune zone-paire configurée pour autoriser le trafic de VPN 30 à VPN 20 (comme souhaité). Si une destination avec la même adresse IP 192.168.12.12 se trouve dans VPN 10 et est supposée répondre à la requête d'écho ICMP, alors conformément à la politique de sécurité ZBFW pour le trafic ICMP de VPN 30 à 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 de la sortie 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, il faut 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 PREFERENCE ---
-----
----- 169.254.206.4 12 1007 C,I,R installed 169.254.206.12 private2 ipsec -
```

Nous pouvons voir que la valeur de l'étiquette est 1007. Enfin, un VPN de destination peut être trouvé si tous les services provenant 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
```

D'après l'étiquette VPN 1007, il peut être confirmé 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 connaître 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
```

Dans ce cas, l'ID VRF 1 a été attribué au VRF nommé 30. Les commandes de plate-forme révèlent la chaîne OCE (Output Chain Element) d'objets dans le 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 SLA (Service Level Agreement) (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
```



Par exemple, si vous simulez une défaillance d'une liaison entre les routeurs cE2 et R20. Cela conduit au 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 divulguée dans la table de routage VPN 30. La connectivité entre VPN 30 et 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 :
```

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 stratégie de sécurité ZBFW, et les noms de zone-paire, de class-map et de stratégie correspondants ont été donnés.

Il y a un problème encore plus grand qui peut se poser en raison du fait que la première route est conservée dans la table de routage de VPN 30 et dans ce cas, c'est la route VPN 10 qui après la fuite de la route VPN 20 de l'application de stratégie de contrôle initiale dans la table VPN 30 OMP sur vSmart. Imaginez le scénario où l'idée initiale était exactement le contraire de la logique de politique de sécurité ZBFW décrite dans cet article. Par exemple, l'objectif était d'autoriser le trafic de VPN 30 à VPN 20 et non à VPN 10. Si elle a été autorisée après une configuration de stratégie initiale, puis après la défaillance ou le retrait de la route 192.168.12.0/24 de 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.