

Configuration des fuites de route pour le chaînage de service dans SD-WAN

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Informations générales](#)

[Configurer](#)

[Fuite De Routage](#)

[Configuration via CLI](#)

[Configuration via un modèle](#)

[Chaînage de service](#)

[Configuration via CLI](#)

[Configuration via un modèle](#)

[Annoncer le service de pare-feu](#)

[Configuration via CLI](#)

[Configuration via un modèle](#)

[Vérifier](#)

[Fuite De Routage](#)

[Chaînage de service](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer et vérifier le chaînage de service pour inspecter le trafic sur différents VRF.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) de Cisco
- Stratégies de contrôle.
- Modèles.

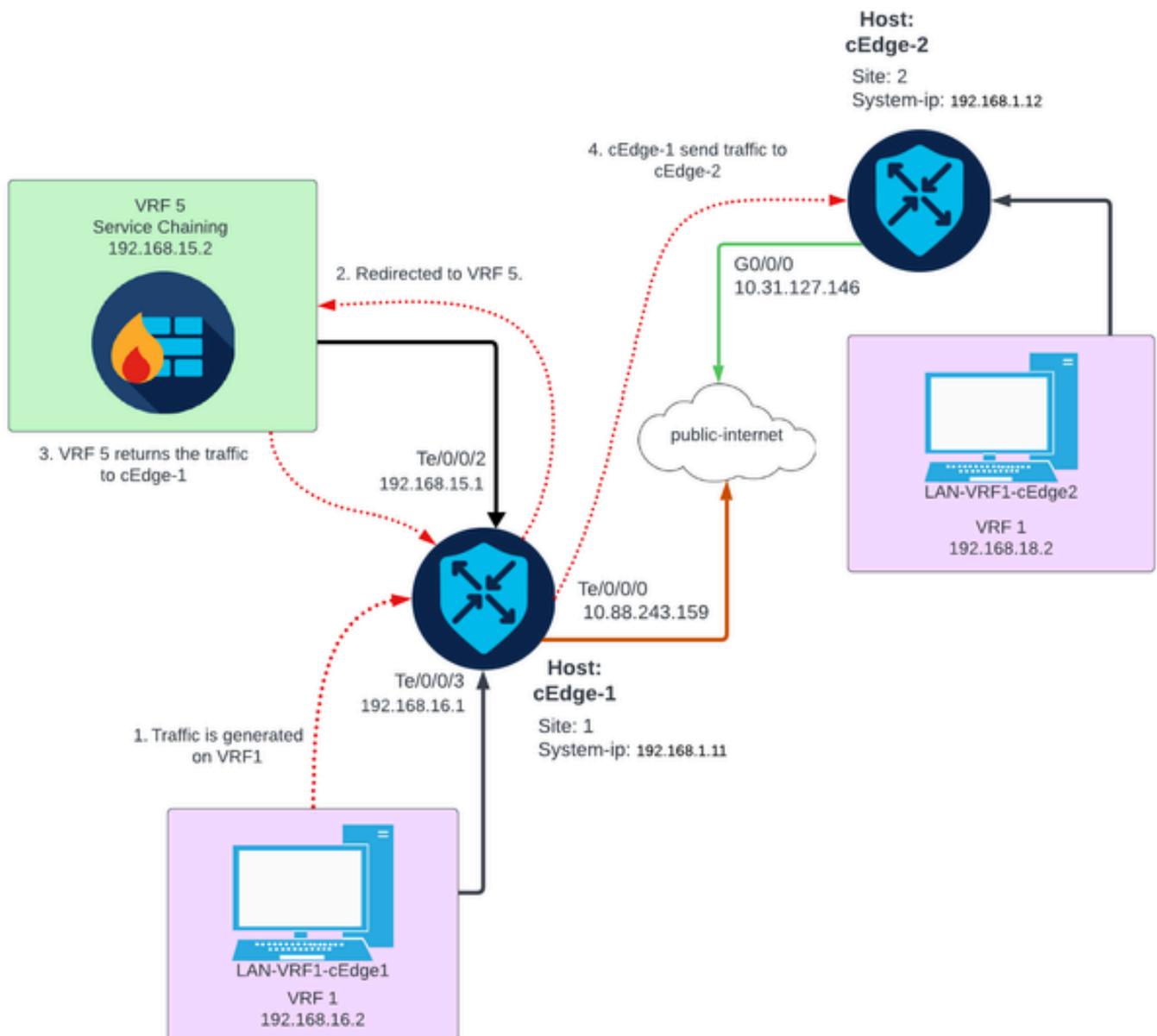
Composants utilisés

Ce document est basé sur les versions logicielles et matérielles suivantes :

- Contrôleurs SD-WAN (20.9.4.1)
- Routeur de périphérie Cisco (17.09.04)

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.

Diagramme du réseau



Informations générales

Sur le schéma du réseau, le service de pare-feu se trouve dans le VRF (Virtual Routing and Forwarding) 5 tandis que les périphériques LAN se trouvent sur le VRF 1. Les informations sur les

routes doivent être partagées entre les VRF afin que l'acheminement et l'inspection du trafic puissent être réalisés. Pour acheminer le trafic via un service, une stratégie de contrôle sur le contrôleur Cisco SD-WAN doit être configurée.

Configurer

Fuite De Routage

Les fuites de route permettent la propagation des informations de routage entre différents VRF. Dans ce scénario, lorsque le chaînage de service (pare-feu) et le côté service LAN se trouvent dans des VRF différents, une fuite de route est nécessaire pour l'inspection du trafic.

Pour assurer le routage entre le côté service LAN et le service pare-feu, une fuite de routes est nécessaire dans les deux VRF et une politique est appliquée dans les sites où une fuite de route est requise.

Configuration via CLI

1. Configurez les listes sur le contrôleur SD-WAN Cisco Catalyst.

La configuration permet d'identifier les sites par le biais d'une liste.

```
<#root>
vSmart#
config
vSmart(config)#
  policy

vSmart(config-policy)#
  lists

vSmart(config-lists)#
  site-list cEdges-1

vSmart(config-site-list-cEdge-1)#
  site-id 1

vSmart(config-site-list-cEdge-1)# exit
vSmart(config-lists)#
  site-list cEdge-2

vSmart(config-site-list- cEdge-2)#
  site-id 2
```

```
vSmart(config-site-list- cEdge-2)# exit
vSmart(config-site-list)#
vpn-list VRF-1
```

```
vSmart(config-vpn-list-VRF-1)#
vpn 1
```

```
vSmart(config-vpn-list-VRF-1)# exit
vSmart(config-site-list)#
vpn-list VRF-5
```

```
vSmart(config-vpn-list-VRF-5)#
vpn 5
vSmart(config-vpn-list-VRF-5)#
commit
```

2. Configurez la stratégie sur le contrôleur SD-WAN Cisco Catalyst.

La configuration permet la propagation des informations de routage entre VRF 1 et VRF 5, afin de garantir le routage entre eux, les deux VRF doivent partager leurs données de routage.

La politique autorise l'acceptation et l'exportation du trafic du VRF 1 vers le VRF 5 et vice versa.

```
<#root>
```

```
vSmart#
config
```

```
vSmart(config)#
policy
```

```
vSmart(config-policy)#
control-policy Route-Leaking
```

```
vSmart(config-control-policy-Route-Leaking)#
sequence 1
```

```
vSmart(config-sequence-1)#
match route
```

```
vSmart(config-match-route)#
vpn 5
```

```
vSmart(config-match-route)# exit
vSmart(config-sequence-1)#
action accept

vSmart(config-action)#
export-to

vSmart(config-export-to)#
vpn-list VRF-1

vSmart(config-action)# exit

vSmart(config-sequence-1)# exit
vSmart(config-control-policy-Route-Leaking)#
sequence 10

vSmart(config-sequence-10)#
match route

vSmart(config-match-route)#
vpn 1

vSmart(config-match-route)# exit
vSmart(config-sequence-10)#
action accept

vSmart(config-action)#
export-to

vSmart(config-export-to)#
vpn-list VRF-5

vSmart(config-action)# exit

vSmart(config-sequence-10)# exit
vSmart(config-control-policy-Route-Leaking)#
default-action accept

vSmart(config-control-policy-Route-Leaking)#
commit
```

3. Appliquez la politique sur le contrôleur SD-WAN Cisco Catalyst.

La politique est appliquée sur les sites 1 et 2 pour permettre le routage entre le VRF 1 situé sur ces sites et le VRF 5.

La politique est mise en oeuvre en entrée, ce qui signifie qu'elle est appliquée aux mises à jour OMP provenant des routeurs de périphérie Cisco vers le contrôleur SD-WAN Cisco Catalyst.

```
<#root>
```

```
vSmart#
```

```
config
```

```
vSmart(config)#
```

```
apply-policy
```

```
vSmart(config-apply-policy)#
```

```
site-list cEdge-1
```

```
vSmart(config-site-list-cEdge-1)#
```

```
control-policy Route-Leaking in
```

```
vSmart(config-site-list-cEdge-1)# exit
```

```
vSmart(config-apply-policy)#
```

```
site-list cEdge-2
```

```
vSmart(config-site-list-cEdge-2)#
```

```
control-policy Route-Leaking in
```

```
vSmart(config-site-list-cEdge-2)#
```

```
commit
```

Configuration via un modèle



Remarque : pour activer la politique via l'interface graphique utilisateur (GUI) de Cisco Catalyst SD-WAN Manager, un modèle doit être associé au contrôleur Cisco Catalyst SD-WAN.

1. Créez la règle permettant la propagation des informations de routage.

Créez une stratégie sur le Cisco Catalyst SD-WAN Manager, accédez à Configuration > Politiques > Centralized Policy.

Sous l'onglet Stratégie centralisée, cliquez sur Ajouter une stratégie.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Créez des listes sur Cisco Catalyst SD-WAN Manager, la configuration permet d'identifier les sites par le biais d'une liste.

Accédez à Site > Nouvelle liste de sites.

Créez la liste des sites où des fuites de route sont nécessaires et ajoutez la liste.

Centralized Policy > Add Policy

● Create Groups of Interest — ● Configure Topology and VPN Membership — ● Configure Traffic Rules — ● Apply Policies to Sites an

Select a list type on the left and start creating your groups of interest

- Data Prefix
- Policer
- Prefix
- Site
- App Probe Class
- SLA Class
- TLOC
- VPN

+ New Site List

Site List Name*

Name of the list

Add Site*

Example: 100 or 200 separated by commas or 1000-2000 by range

Add Cancel

Accédez à VPN > New VPN List.

Créez la liste VPN où la fuite de route doit être appliquée, cliquez sur Next.

Select a list type on the left and start creating your groups of interest

Prefix

Site

App Probe Class

SLA Class

TLOC

VPN

Region

Preferred Color Group

+ New VPN List

VPN List Name*

Name of the list

Add VPN*

Example: 100 or 200 separated by commas or 1000-2000 by range

Add Cancel

3. Configurez la stratégie sur le gestionnaire SD-WAN de Cisco Catalyst.

Cliquez sur l'onglet Topologie, puis sur Ajouter une topologie.

Créer un contrôle personnalisé (route et TLOC).

Search

Add Topology ▾

Hub-and-Spoke

Mesh

Custom Control (Route & TLOC)

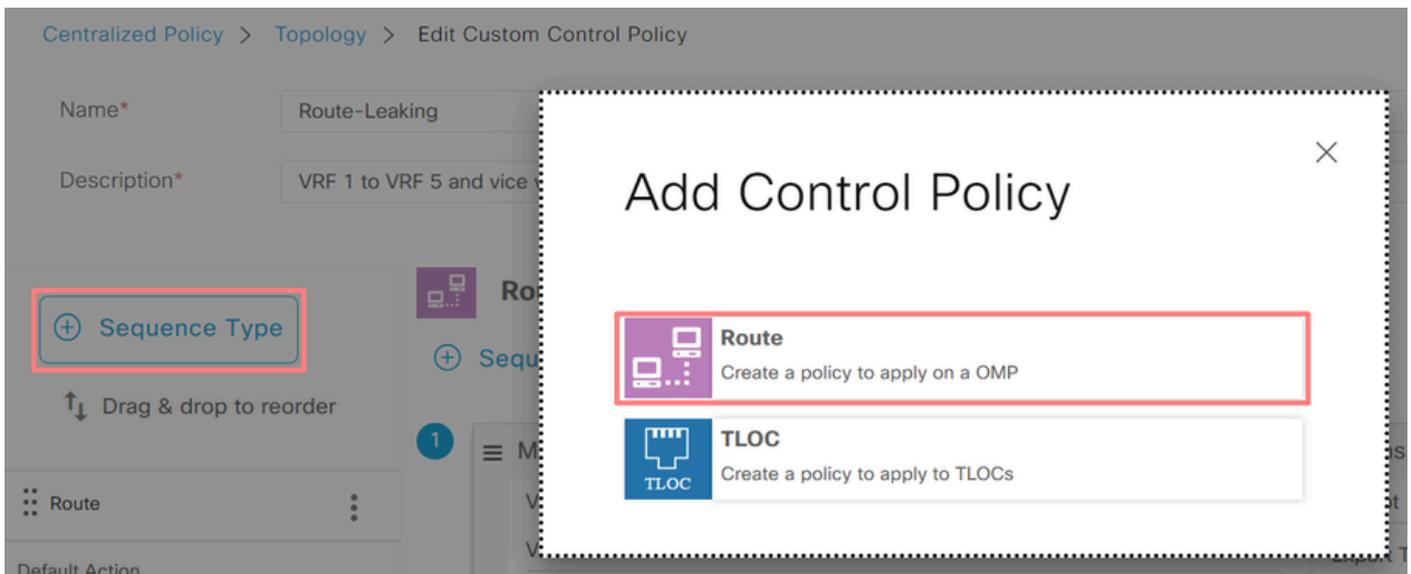
Import Existing Topology

Description

Mode

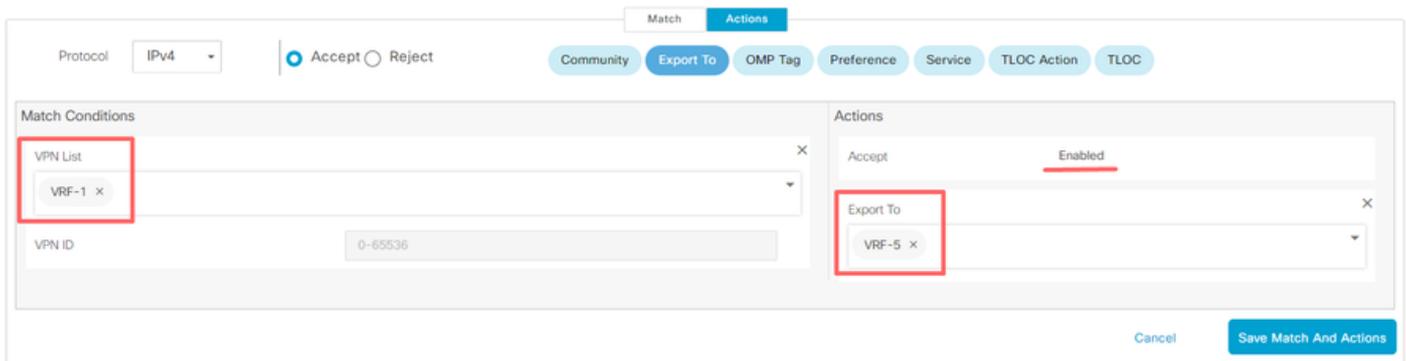
No data available

Cliquez sur Sequence Type et sélectionnez Route sequence.

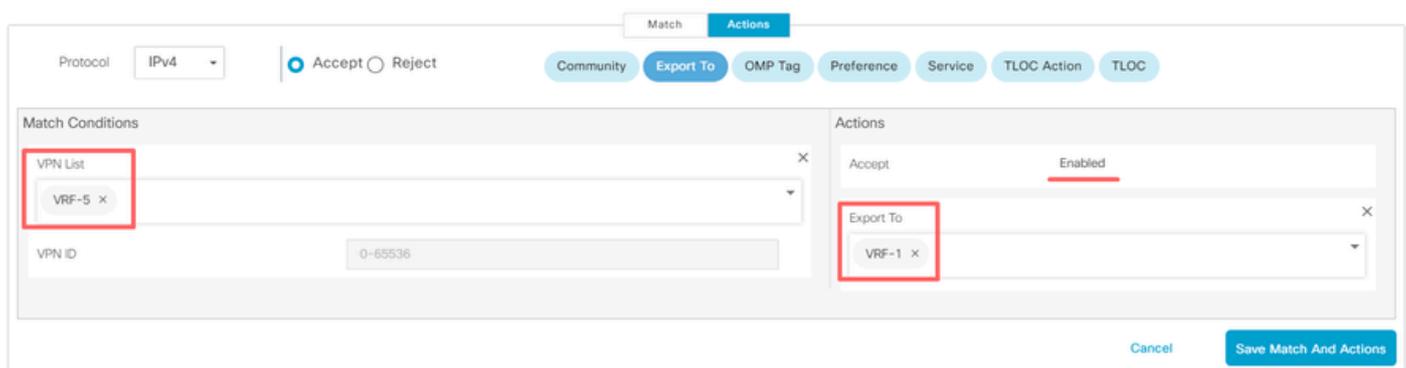


Ajouter une règle de séquence.

Condition 1 : le trafic du VRF 1 est accepté et exporté vers le VRF 5.



Condition 2 : le trafic du VRF 5 est accepté et exporté vers le VRF 1.



Modifiez l'action par défaut de la stratégie sur Accepter.

Cliquez sur Enregistrer la correspondance et les actions, puis sur Enregistrer la stratégie de contrôle.

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel

4. Appliquez la politique sur les sites où des fuites de route sont nécessaires.

Cliquez sur l'onglet Topology, sous la politique de fuite de route, sélectionnez New Site/Region List on Inbound Site List. Sélectionnez les listes de sites où des fuites de route sont nécessaires.

Pour enregistrer les modifications, sélectionnez Enregistrer les modifications de stratégie.

Route-Leaking CUSTOM CONTROL

+ New Site/Region List

Direction	Site/Region List	Region ID	Action
in	cEdge-2, cEdge-1	N/A	 

Preview Save Policy Changes Cancel

Chaînage de service

Le chaînage de services est également appelé insertion de services. Elle implique l'injection d'un service réseau ; les services standard incluent le pare-feu (FW), le système de détection des intrusions (IDS) et le système de prévention des intrusions (IPS). Dans ce cas, un service de pare-feu est inséré dans le chemin de données.

Configuration via CLI

1. Configurez les listes sur le contrôleur SD-WAN Cisco Catalyst.

La configuration permet d'identifier les sites par le biais d'une liste.

Créez une liste pour les sites où chaque VRF 1 est situé.

Dans la liste Emplacement de transport (TLOC), spécifiez l'adresse à laquelle le trafic doit être redirigé pour atteindre le service.

<#root>

```
vSmart#
config

vSmart(config)#
policy

vSmart(config-policy)#
lists

vSmart(config-lists)#
site-list cEdge-1

vSmart(config-site-list-cEdge-1)#
site-id 1

vSmart(config-site-list-cEdge-1)# exit
vSmart(config-lists)#
site-list cEdge-2

vSmart(config-site-list-cEdge-2)#
site-id 2

vSmart(config-site-list-cEdge-2)# exit
vSmart(config-lists)#
tloc-list cEdge-1-TLOC

vSmart(config-tloc-list-cEdge-1-TLOC)#
tloc 192.168.1.11 color public-internet encaps ipsec

vSmart(config-tloc-list-cEdge-1-TLOC)#
commit
```

2. Configurez la stratégie sur le contrôleur SD-WAN Cisco Catalyst.

La séquence filtre le trafic du VRF 1. Le trafic est autorisé et inspecté sur un pare-feu de service situé sur VRF 5.

```
<#root>
```

```
vSmart#
config
```

```
vSmart(config)#  
  policy  
  
vSmart(config-policy)#  
control-policy Service-Chaining  
  
vSmart(config-control-policy-Service-Chaining)#  
sequence 1  
  
vSmart(config-sequence-1)#  
match route  
  
vSmart(config-match-route)#  
vpn 1  
  
vSmart(config-match-route)#  
action accept  
  
vSmart(config-action)#  
set  
  
vSmart(config-set)#  
  service FW vpn 5  
  
vSmart(config-set)#  
  service tloc-list cEdge-1-TLOC  
  
vSmart(config-set)# exit  
vSmart(config-action)# exit  
vSmart(config-sequence-1)# exit  
vSmart(config-control-policy-Service-Chaining)#  
default-action accept  
vSmart(config-control-policy-Service-Chaining)#  
commit
```

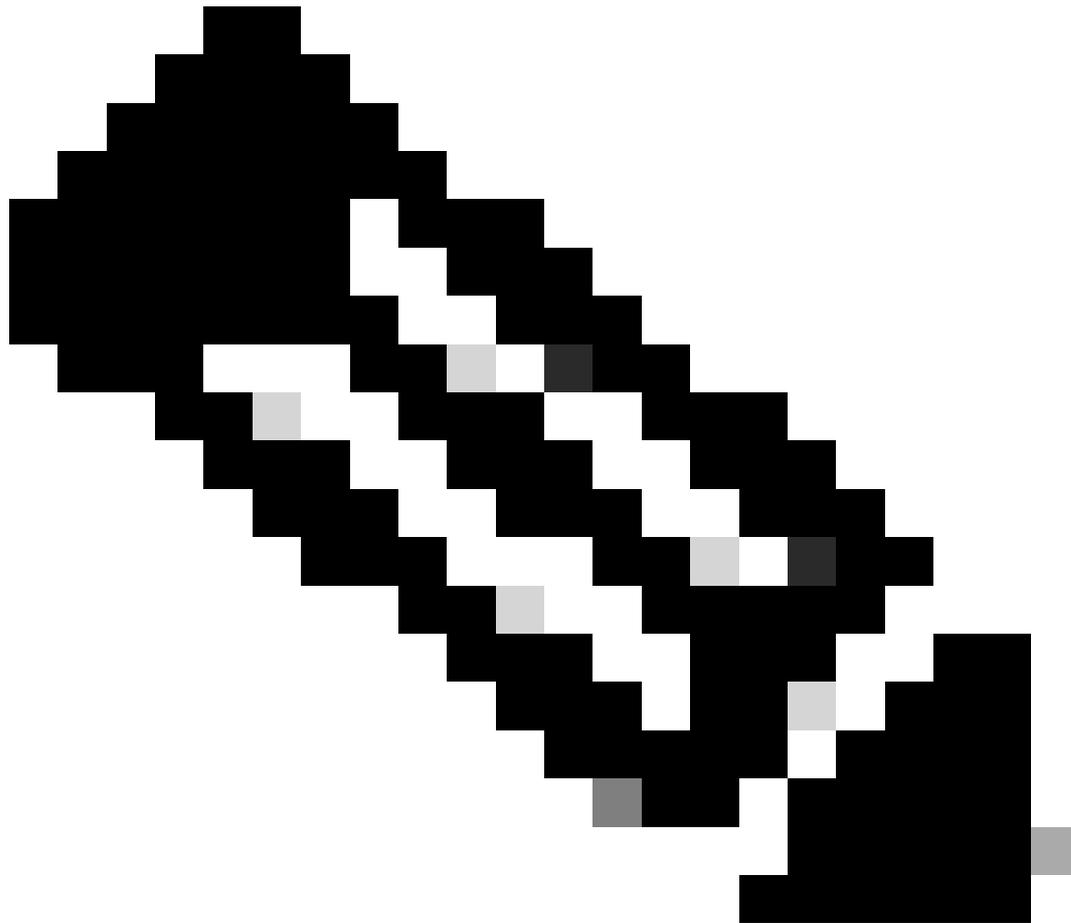
3. Appliquez la politique sur le contrôleur SD-WAN Cisco Catalyst.

La stratégie est configurée sur les sites 1 et 2 pour permettre l'inspection du trafic en provenance du VRF 1.

<#root>

```
vSmart#  
config  
  
vSmart(config)#  
apply-policy  
  
vSmart(config-apply-policy)#  
site-list cEdge-1  
  
vSmart(config-site-list-cEdge-1)#  
control-policy Service-Chaining out  
vSmart(config-site-list-cEdge-1)# exit  
  
vSmart(config-apply-policy)#  
site-list cEdge-2  
  
vSmart(config-site-list-cEdge-1)#  
control-policy Service-Chaining out  
vSmart(config-site-list-cEdge-1)#  
commit
```

Configuration via un modèle



Remarque : pour activer la politique via l'interface graphique utilisateur (GUI) de Cisco Catalyst SD-WAN Manager, un modèle doit être joint au contrôleur SD-WAN Cisco Catalyst.

1. Créez une politique sur le gestionnaire SD-WAN de Cisco Catalyst.

Accédez à Configuration > Politiques > Centralized Policy.

Sous l'onglet Stratégie centralisée, cliquez sur Ajouter une stratégie.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Créez des listes sur le Cisco Catalyst SD-WAN Manager.

Accédez à Site > Nouvelle liste de sites.

Créez la liste des sites sur lesquels se trouve VRF 1 et sélectionnez Add.

Centralized Policy > Add Policy

Create Groups of Interest

Configure Topology and VPN Membership

Configure Traffic Rules

Apply Policies to Sites an

Select a list type on the left and start creating your groups of interest

Data Prefix

Policer

Prefix

Site

App Probe Class

SLA Class

TLOC

VPN

+ New Site List

Site List Name*

Name of the list

Add Site*

Example: 100 or 200 separated by commas or 1000-2000 by range

Add

Cancel

Accédez à TLOC > New TLOC List.

Créez le chaînage de service de liste TLOC situé sur et sélectionnez Enregistrer.

TLOC List

List Name *

TLOC IP*

Color*

Encap*

Preference

+ Add TLOC

Cancel

Save

3. Ajoutez des règles de séquence.

Cliquez sur l'onglet Topology et cliquez sur Add Topology.

Créer un contrôle personnalisé (route et TLOC).

Centralized Policy > Add Policy

✔ Create Groups of Interest ● Configure Topology and VPN Membership

Specify your network topology

Topology

VPN Membership

Search

Add Topology ▾

Hub-and-Spoke

Mesh

Custom Control (Route & TLOC)

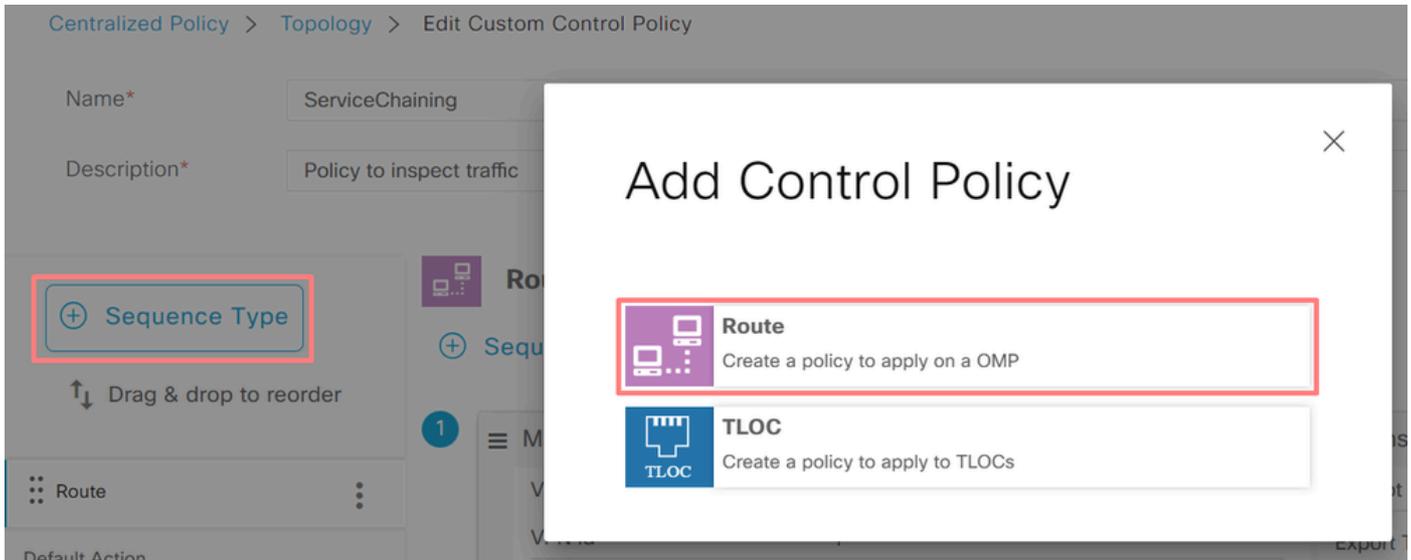
Import Existing Topology

Description

Mode

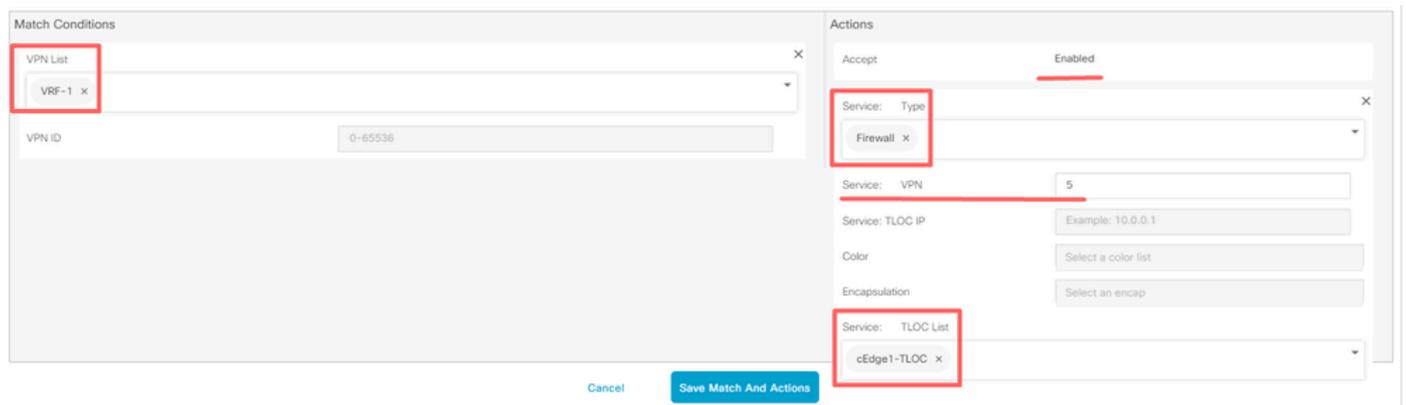
No data available

Cliquez sur Sequence Type et sélectionnez Route sequence.



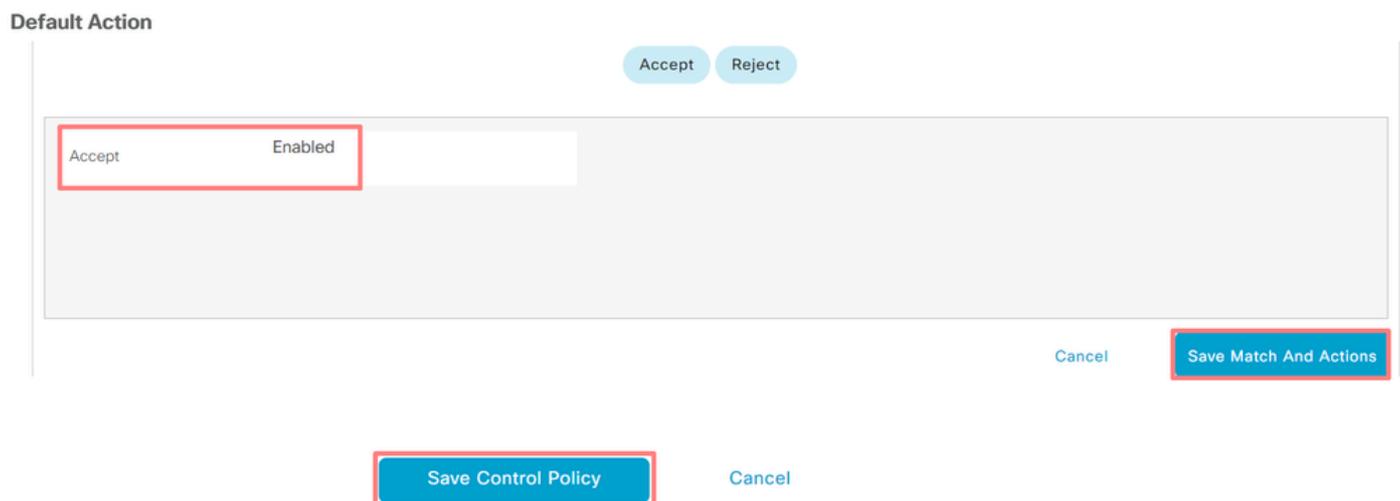
Ajouter une règle de séquence.

La séquence filtre le trafic du VRF 1, l'autorise à passer, puis le redirige vers un service (pare-feu) qui existe dans le VRF 5. Pour ce faire, il suffit d'utiliser le TLOC sur le site 1, qui est l'emplacement du service de pare-feu.



Modifiez l'action par défaut de la stratégie sur Accepter.

Cliquez sur Save Match and Actions, puis sur Save Control Policy.



4. Appliquez la stratégie.

Cliquez sur l'onglet Topology, sous la stratégie de chaînage de services, sélectionnez New Site/Region List on Outbound Site List. Sélectionnez les sites que le trafic VRF 1 doit inspecter, puis cliquez sur Save Policy. Enregistrez les modifications, cliquez sur Save Policy Changes.



Annoncer le service de pare-feu

Configuration via CLI

Pour provisionner le service de pare-feu, spécifiez l'adresse IP du périphérique de pare-feu. Le service est annoncé au contrôleur SD-WAN Cisco Catalyst via une mise à jour OMP.

```
<#root>
```

```
cEdge-01#
```

```
config-transaction
```

```
cEdge-01(config)#
```

```
sdwan
```

```
cEdge-01(config-sdwan)#
```

```
service Firewall vrf 5
```

```
cEdge-01(config-vrf-5)#
```

```
ipv4 address 192.168.15.2
```

```
cEdge-01(config-vrf-5)#
```

```
commit
```

Configuration via un modèle

Accédez au modèle de fonction du VRF 5.

Passez à Configuration > Templates > Feature Template > Add Template > Cisco VPN.

Sous Service Section, cliquez sur New Service. Entrez les valeurs, ajoutez le service et enregistrez le modèle.

SERVICE

New Service

Service Type

 FW 

IPv4 address

 192.168.15.2

Tracking

 On Off

Vérifier

Fuite De Routage

Vérifiez que le contrôleur SD-WAN Cisco Catalyst exporte les routes de VRF 1 vers VRF 5 et inversement.

<#root>

```
vSmart# show omp routes vpn 1 | tab
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP
1	192.168.15.0/24	192.168.3.16	92	1003	C,R,Ext	original	192.168.15.1
						installed	192.168.15.1
1	192.168.16.0/24	192.168.3.16	69	1002	C,R	installed	192.168.16.1
1	192.168.18.0/24	192.168.3.15	69	1002	C,R	installed	192.168.18.1

```
vSmart# show omp routes vpn 5 | tab
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP
5	192.168.15.0/24	192.168.3.16	69	1003	C,R	installed	192.168.15.1
5	192.168.16.0/24	192.168.3.16	92	1002	C,R,Ext	original	192.168.16.1

							installed	192.168.
5	192.168.18.0/24	192.168.3.15	92	1002	C,R,Ext	original		192.168.
							installed	192.168.

Confirmez que les routeurs de périphérie Cisco ont reçu la route ayant fui du VRF 1 au VRF 5.

Confirmez que les routeurs de périphérie Cisco ont reçu la route ayant fui du VRF 5 au VRF 1.

```
<#root>
```

```
cEdge-1#
```

```
show ip route vrf 1
```

```
----- output omitted -----
```

```
m 192.168.15.0/24 [251/0] via 192.168.3.16 (5), 10:12:28, Sdwan-system-intf
```

```
192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 192.168.16.0/24 is directly connected, TenGigabitEthernet0/0/3
```

```
L 192.168.16.1/32 is directly connected, TenGigabitEthernet0/0/3
```

```
m 192.168.18.0/24 [251/0] via 192.168.3.16, 10:12:28, Sdwan-system-intf
```

```
cEdge-1#
```

```
show ip route vrf 5
```

```
----- output omitted -----
```

```
192.168.15.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 192.168.15.0/24 is directly connected, TenGigabitEthernet0/0/2
```

```
L 192.168.15.1/32 is directly connected, TenGigabitEthernet0/0/2
```

```
m 192.168.16.0/24 [251/0] via 192.168.3.16 (1), 10:17:54, Sdwan-system-intf
```

```
m 192.168.18.0/24 [251/0] via 192.168.3.15, 10:17:52, Sdwan-system-intf
```

```
cEdge-2#
```

```
show ip route vrf 1
```

```
----- output omitted -----
```

```
m 192.168.15.0/24 [251/0] via 192.168.3.16, 01:35:15, Sdwan-system-intf
```

```
m 192.168.16.0/24 [251/0] via 192.168.3.16, 01:35:15, Sdwan-system-intf
192.168.18.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C      192.168.18.0/24 is directly connected, GigabitEthernet0/0/1
L      192.168.18.1/32 is directly connected, GigabitEthernet0/0/1
```

Chaînage de service

Vérifiez que le routeur de périphérie Cisco a annoncé le service de pare-feu au contrôleur SD-WAN Cisco Catalyst via la route de service OMP.

```
<#root>
```

```
cEdge-01#
```

```
show sdwan omp services
```

ADDRESS FAMILY	TENANT	VPN	SERVICE	ORIGINATOR	FROM PEER	PATH ID	REGION ID	LABEL	STATUS	VRF
ipv4	0	1	VPN	192.168.1.11	0.0.0.0	69	None	1002	C,Red,R	
	0	5	VPN	192.168.1.11	0.0.0.0	69	None	1003	C,Red,R	
0	5	FW	192.168.1.11	0.0.0.0	69	None	1005	C,Red,R		5

Vérifiez que le contrôleur SD-WAN Cisco Catalyst a bien reçu la route de service.

```
<#root>
```

```
vSmart#
```

```
show omp services
```

ADDRESS					PATH	REGION			
ipv4	1	VPN	192.168.1.12	192.168.1.12	69	None	1002	C,I,R	
	1	VPN	192.168.1.11	192.168.1.11	69	None	1002	C,I,R	
	5	VPN	192.168.1.11	192.168.1.11	69	None	1003	C,I,R	
5	FW	192.168.1.11	192.168.1.11	69	None	1005	C,I,R		

Pour vérifier que le service de pare-feu inspecte le trafic provenant de VRF 1, exécutez une commande traceroute.

```
<#root>
```

```
Service-Side-cEdge1#traceroute 192.168.18.2
```

```
Type escape sequence to abort.  
Tracing the route to 192.168.18.2  
VRF info: (vrf in name/id, vrf out name/id)  
1 192.168.16.1 0 msec 0 msec 0 msec  
2 192.168.16.1 1 msec 0 msec 0 msec  
  
3 192.168.15.2 1 msec 0 msec 0 msec  
  
4 192.168.15.1 0 msec 0 msec 0 msec  
5 10.31.127.146 1 msec 1 msec 1 msec  
6 192.168.18.2 2 msec 2 msec *
```

```
Service-Side-cEdge2#traceroute 192.168.16.2  
Type escape sequence to abort.  
Tracing the route to 192.168.16.2  
VRF info: (vrf in name/id, vrf out name/id)  
1 192.168.18.1 2 msec 1 msec 1 msec  
2 10.88.243.159 2 msec 2 msec 2 msec  
  
3 192.168.15.2 1 msec 1 msec 1 msec  
  
4 192.168.15.1 2 msec 2 msec 1 msec  
5 192.168.16.2 2 msec * 2 msec
```

Informations connexes

- [Chaînage de service](#)
- [Fuite De Routage](#)
- [SD-WAN - Configurer la fuite de route - YouTube](#)

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.