

Route-lekkage voor serviceketting configureren in SD-WAN

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Route voor lekkage](#)

[Configuratie via CLI](#)

[Configuratie via sjabloon](#)

[Serviceketen](#)

[Configuratie via CLI](#)

[Configuratie via sjabloon](#)

[Advertentie-firewallservice](#)

[Configuratie via CLI](#)

[Configuratie via sjabloon](#)

[Verifiëren](#)

[Route voor lekkage](#)

[Serviceketen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Service Chaining kunt configureren en verifiëren om verkeer via verschillende VRF te inspecteren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Beleid inzake controle.
- Sjablonen.

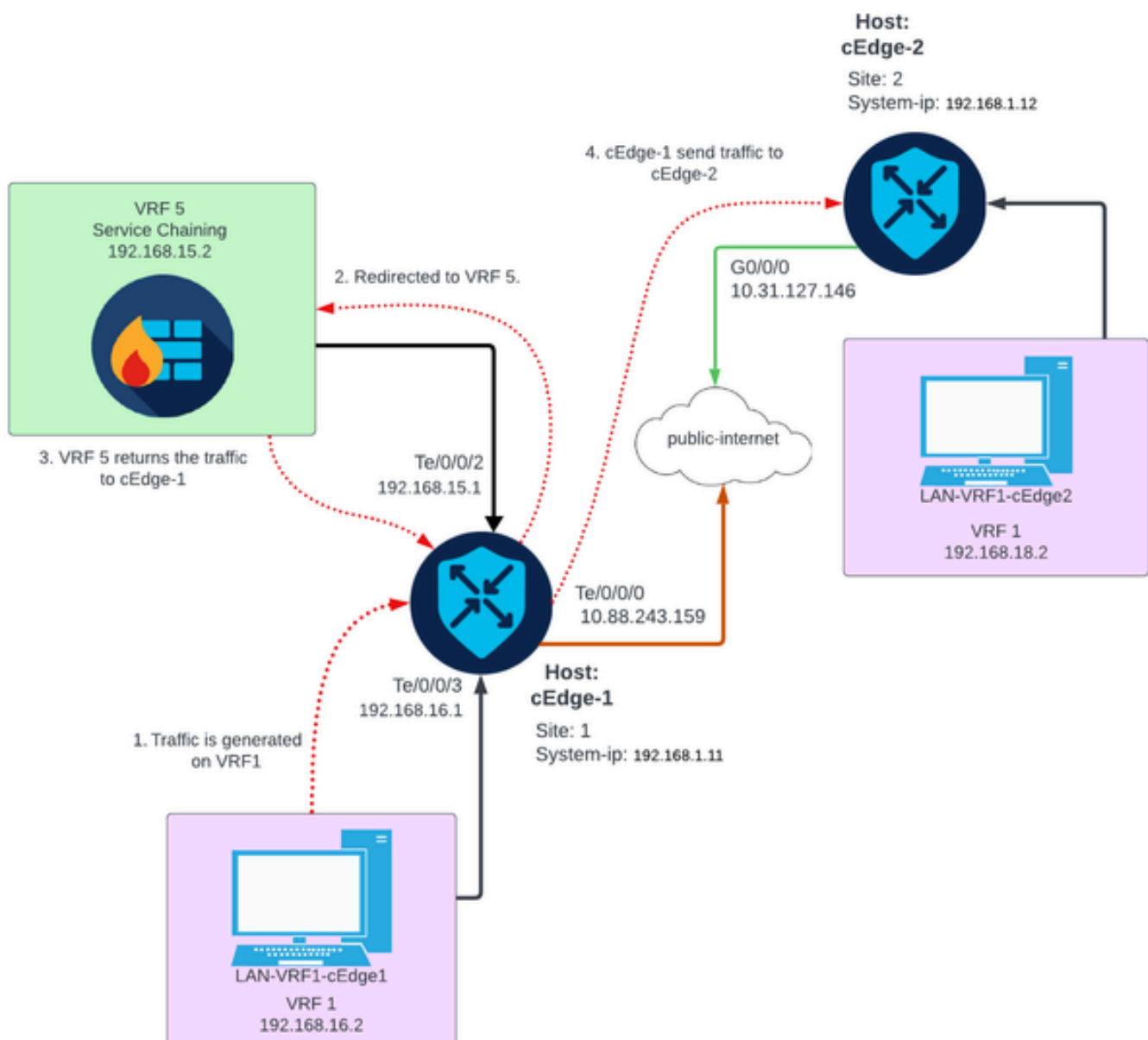
Gebruikte componenten

Dit document is gebaseerd op deze software- en hardwareversies:

- SD-WAN controllers (20.9.4.1)
- Cisco Edge-router (17.09.04)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdigram



Achtergrondinformatie

In het netwerkdigram is de Firewallservice in Virtual Routing and Forwarding (VRF) 5

geïnstalleerd terwijl LAN-apparaten op VRF 1 zich bevinden. Informatie over routes moet worden gedeeld tussen VRF's zodat voorwaarts en inspectie van het verkeer kan worden bereikt. Om verkeer door een service te leiden moet er een controlebeleid op de Cisco SD-WAN controller worden geconfigureerd.

Configureren

Route voor lekkage

Het lekken van de route laat de propagatie van het verpletteren van informatie tussen verschillende VRF's toe. In dit scenario, wanneer Service Chaining (Firewall) en LAN Service kant in verschillende VRF's zijn, is route lekken noodzakelijk voor verkeersinspectie.

Om ervoor te zorgen dat de routing tussen LAN-servicekant en Firewall-service plaatsvindt, is er een lek van routes nodig in zowel VRF-apparatuur als een beleid op de locaties waar routelekkage vereist is.

Configuratie via CLI

1. Configureer lijsten op de Cisco Catalyst SD-WAN controller.

De configuratie maakt het mogelijk locaties te identificeren door middel van een lijst.

```
<#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. Configureer het beleid inzake de Cisco Catalyst SD-WAN controller.

De configuratie staat propagatie van het verpletteren van informatie tussen VRF 1 en VRF 5 toe, om het verpletteren tussen hen te verzekeren, moeten beide VRF hun routeringsgegevens delen.

Het verkeer van de vergunning van het beleid van VRF 1 om aan VRF 5 worden goedgekeurd en worden uitgevoerd en 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. Pas het beleid toe op de Cisco Catalyst SD-WAN controller.

Het beleid wordt toegepast in plaats 1 en plaats 2 om het leiden tussen VRF 1 toe te staan die op die plaatsen en op VRF 5 wordt gevestigd.

Beleid wordt inbound geïmplementeerd en dit betekent dat de OMP-updates van Cisco Edge-routers naar Cisco Catalyst SD-WAN controller worden toegepast.

```
<#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

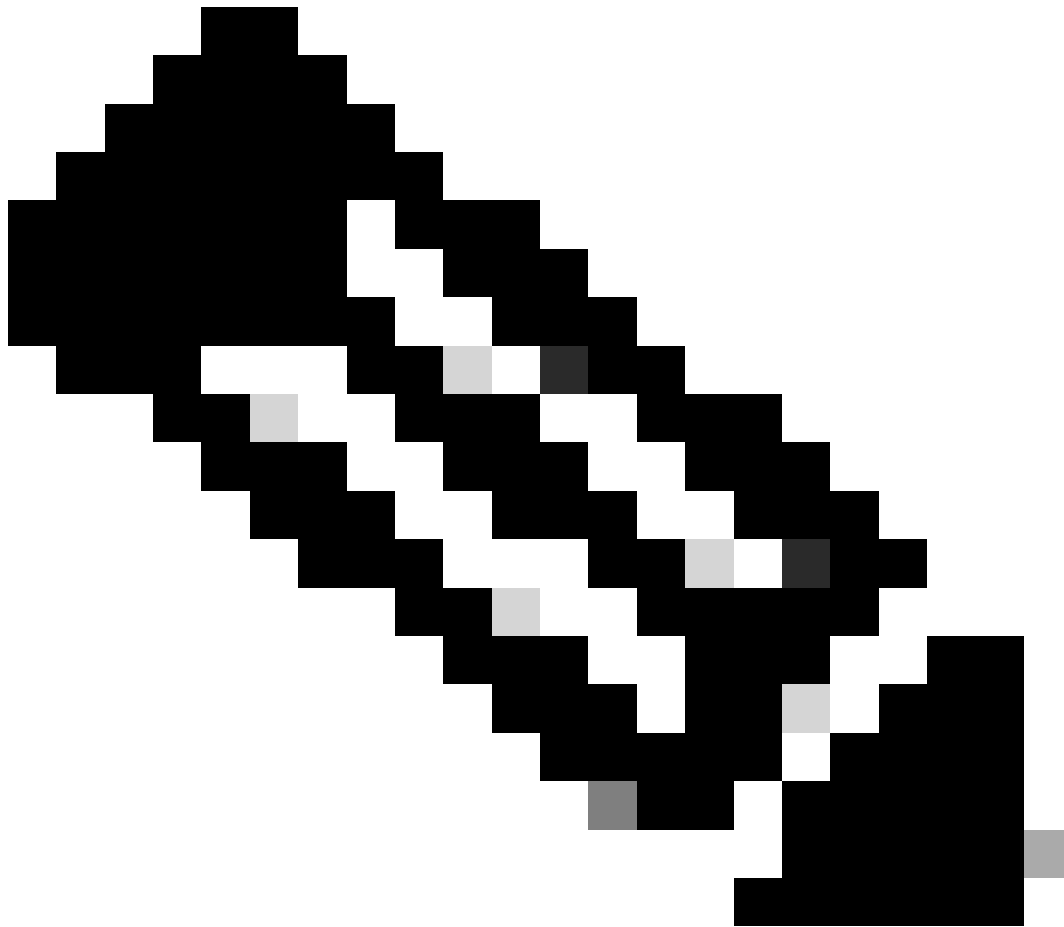
vSmart(config-site-list-cEdge-1)# exit

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
```

Configuratie via sjabloon



Opmerking: om het beleid te activeren via Cisco Catalyst SD-WAN Manager Graphic User Interface (GUI), moet voor Cisco Catalyst SD-WAN controller een sjabloon zijn gekoppeld.

1. Maak het beleid om propagatie van routinginformatie toe te staan.

Maak beleid op de Cisco Catalyst SD-WAN Manager, navigeer naar Configuration> Beleid >Gecentraliseerd beleid.

Klik onder het tabblad Gecentraliseerd beleid op Beleid toevoegen.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Maak lijsten op de Cisco Catalyst SD-WAN Manager, met de configuratie kunnen sites worden geïdentificeerd door middel van een lijst.

Ga naar Site > Nieuwe Site lijst.

Maak de lijst van sites waar route lekken is nodig en voeg de lijst toe.

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

Navigeer naar VPN > Nieuwe VPN-lijst.

Maak de VPN-lijst waarop routelekken moet worden toegepast, klik op Volgende.

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. Configureer het beleid inzake Cisco Catalyst SD-WAN Manager.

Klik op het tabblad Topologie en klik op Topologie toevoegen.

Maak een aangepaste controle (Route & TLOC).

Search

Add Topology ▾

Hub-and-Spoke

Mesh

Custom Control (Route & TLOC)

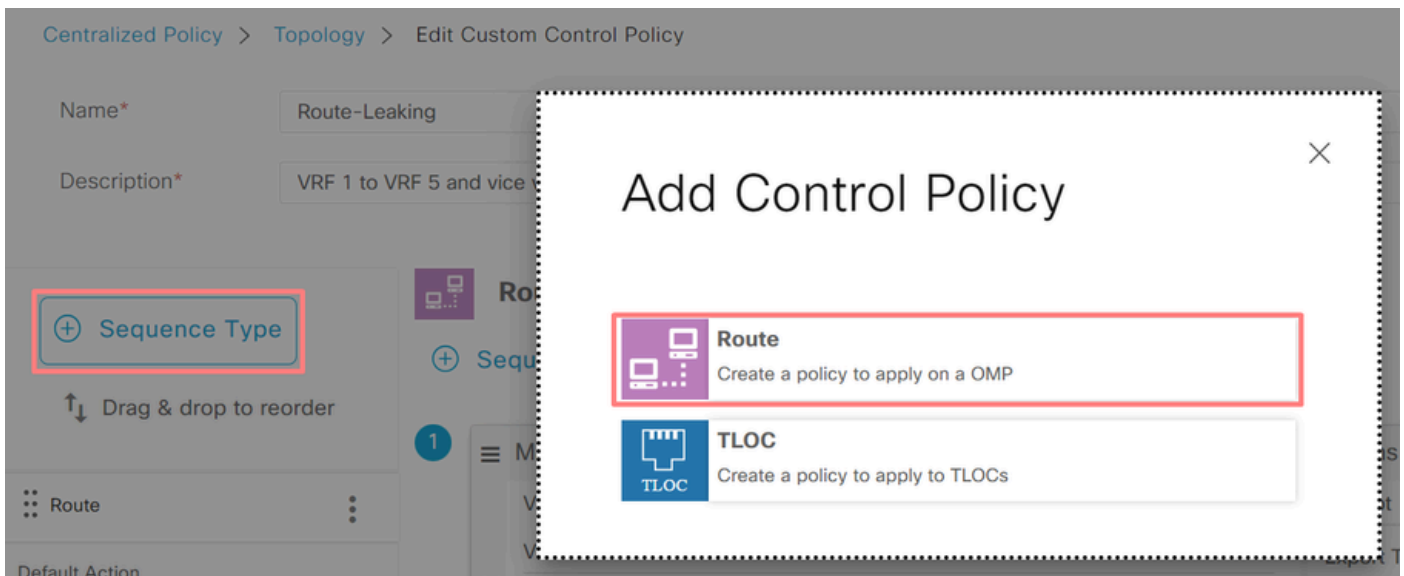
Import Existing Topology

Description

Mode

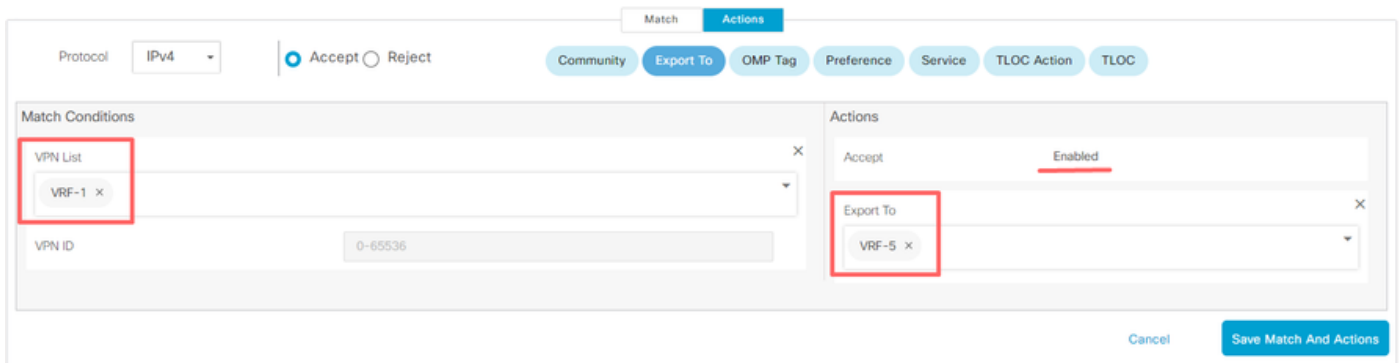
No data available

Klik op Sequence Type en selecteer Route sequentie.

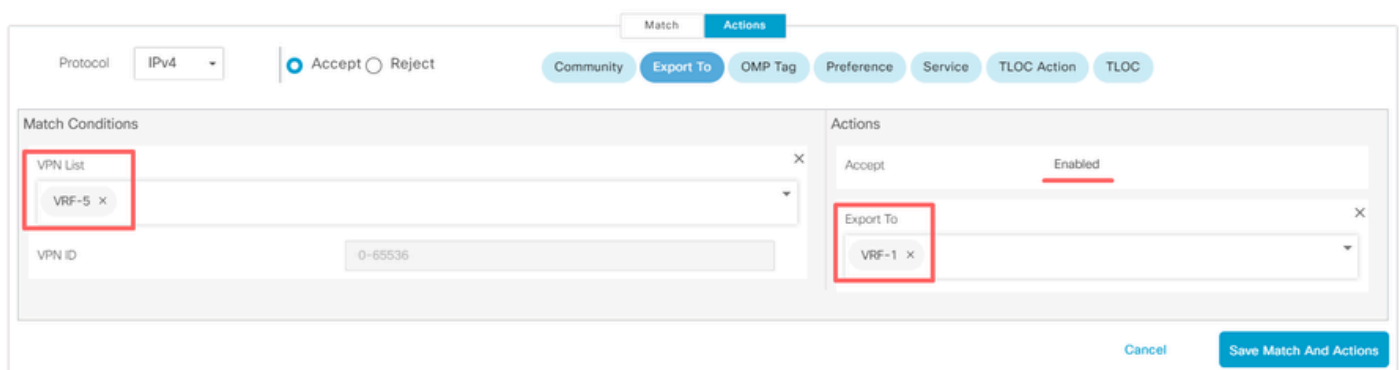


Voeg een sequentieregel toe.

Voorwaarde 1: Verkeer van VRF 1 wordt goedgekeurd en uitgevoerd naar VRF 5.



Voorwaarde 2: Verkeer van VRF 5 wordt goedgekeurd en uitgevoerd naar VRF 1.



Verander de Standaardactie van het te accepteren beleid.

Klik op Overeenkomsten en acties opslaan en klik vervolgens op Configuratiebeleid opslaan.

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel



4. Pas het beleid toe op de plaatsen waar routelekkage nodig is.

Klik op het tabblad Topologie, onder het Route-Leaking Policy selecteer Nieuwe Site/Gebiedslijst op Inkomende Site Lijst. Selecteer de sitelijsten waar route lekken nodig is.

Als u de wijzigingen wilt opslaan, selecteert u Beleidswijzigingen opslaan.

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

Serviceketen

Service Chaining is ook bekend als service insertion. Het impliceert de injectie van de netwerkdienst; de standaarddiensten omvatten Firewall (FW), Inbraakdetectiesysteem (IDS), en Inbraakpreventiesysteem (IPS). In dit geval wordt een firewallservice ingevoegd in het gegevenspad.

Configuratie via CLI

1. Configureer de lijsten met de Cisco Catalyst SD-WAN controller.

De configuratie maakt het mogelijk locaties te identificeren door middel van een lijst.

Maak een lijst voor de locaties waar elke VRF 1 zich bevindt.

Specificeer in de lijst Transport Location (TLOC) het adres waar het verkeer moet worden omgeleid om de service te bereiken.

<#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. Configureer het beleid inzake de Cisco Catalyst SD-WAN controller.

Het verkeer van de opeenvolgingsfilters van VRF 1. Het verkeer is toegestaan en gecontroleerd op een service firewall op 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. Pas het beleid toe op de Cisco Catalyst SD-WAN controller.

Het beleid is ingesteld in site 1 en 2 om verkeer vanaf VRF 1 te kunnen inspecteren.

```
<#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
```

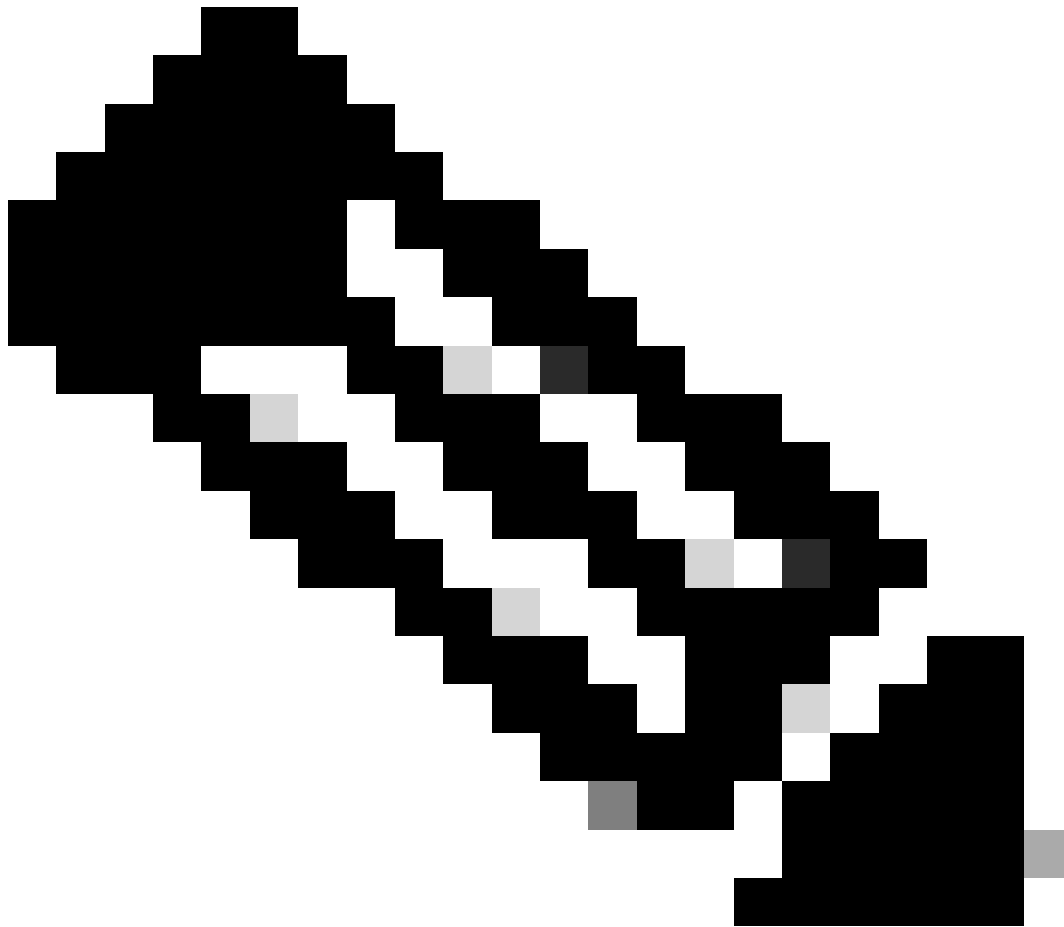
```
vSmart(config-site-list-cEdge-1)#
```

```
control-policy Service-Chaining out
```

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

```
commit
```

Configuratie via sjabloon



Opmerking: om het beleid te activeren via Cisco Catalyst SD-WAN Manager Graphic User Interface (GUI), moet voor Cisco Catalyst SD-WAN Controller een sjabloon zijn gekoppeld.

1. Maak een beleid aan voor Cisco Catalyst SD-WAN Manager.

Ga naar Configuration > Policies > Centralised Policy.

Klik onder het tabblad Gecentraliseerd beleid op Beleid toevoegen.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Maak lijsten aan op de Cisco Catalyst SD-WAN Manager.

Ga naar Site > Nieuwe sitelijst.

Maak de sitelijst van de sites waarop VRF 1 zich bevindt en selecteer Toevoegen.

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

Navigeren naar TLOC > Nieuwe TLOC-lijst.

Ga naar de TLOC-lijst voor de koppeling en selecteer Opslaan.



TLOC List

List Name *

cEdge1-TLOC

TLOC IP*

192.168.1.11

Color*

public-internet ▼

Encap*

ipsec ▼

Preference

0-4294967295

[+ Add TLOC](#)

Cancel

Save

3. Voeg sequentieregels toe.

Klik op het tabblad Topologie en klik op Topologie toevoegen.

Maak een aangepaste controle (Route & 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)

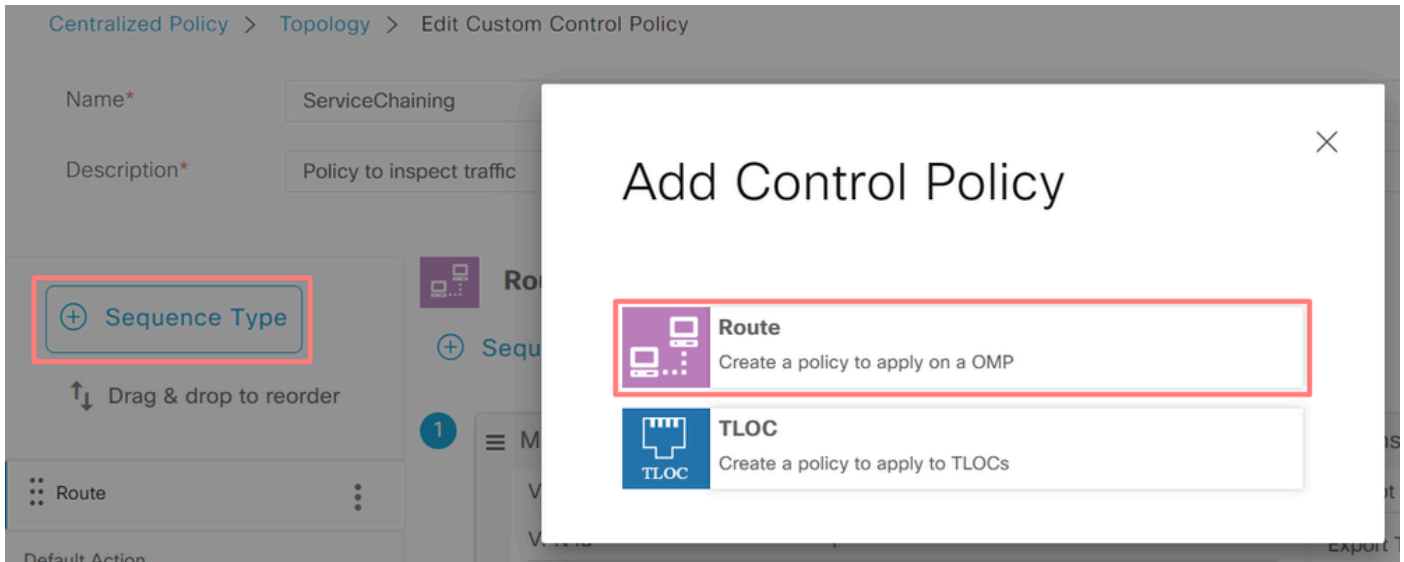
Import Existing Topology

Description

Mode

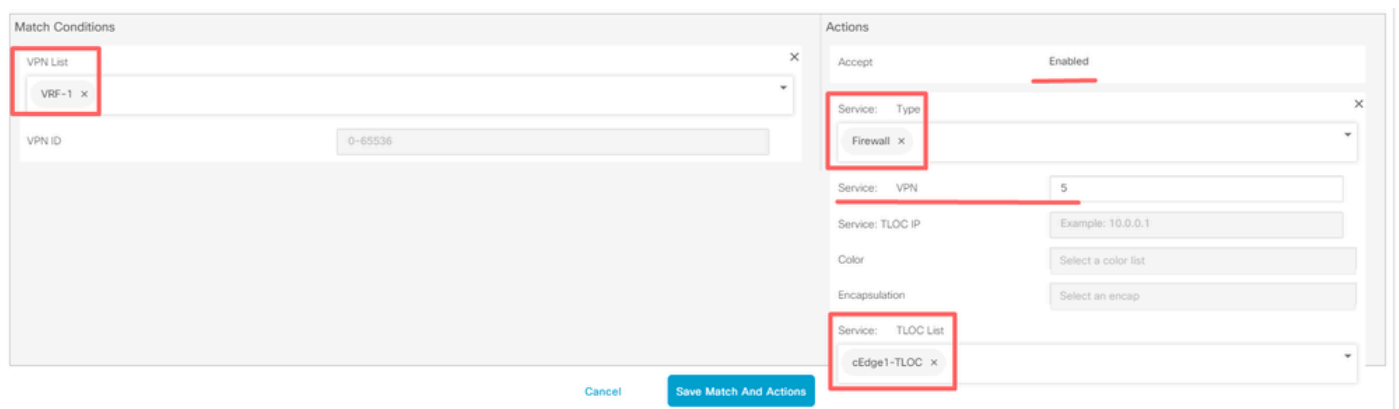
No data available

Klik op Sequence Type en selecteer Route sequentie.



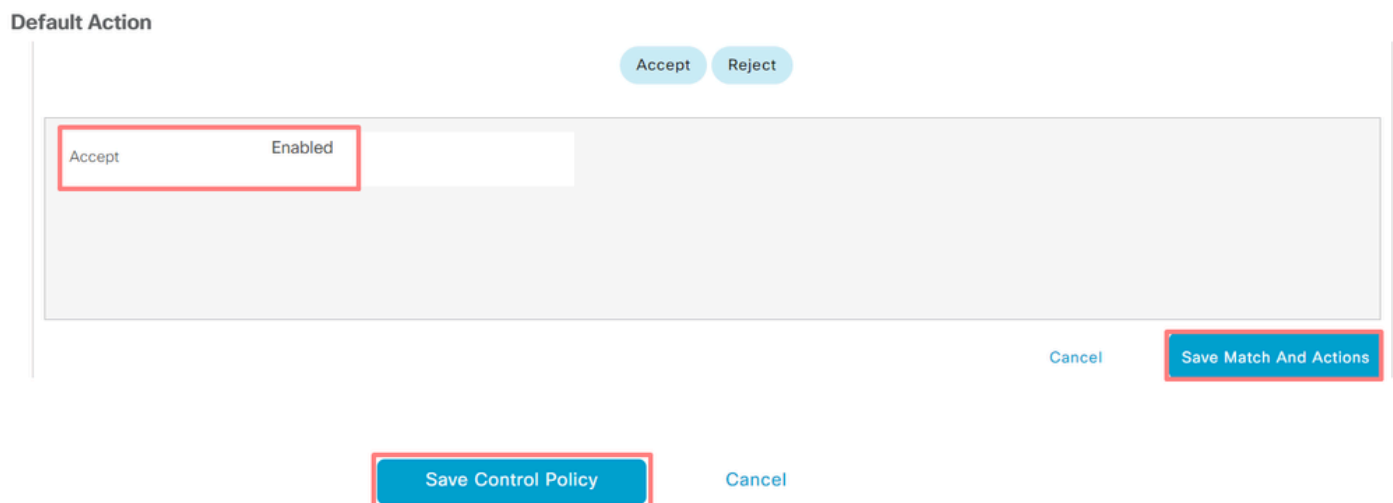
Voeg een sequentieregel toe.

Het verkeer van de opeenvolgingsfilters van VRF 1, staat het door toe, en leidt het dan opnieuw aan de dienst (Firewall) die binnen VRF 5 bestaat. Dit kan worden bereikt door gebruik te maken van de TLOC op site 1, de locatie van de Firewallservice.



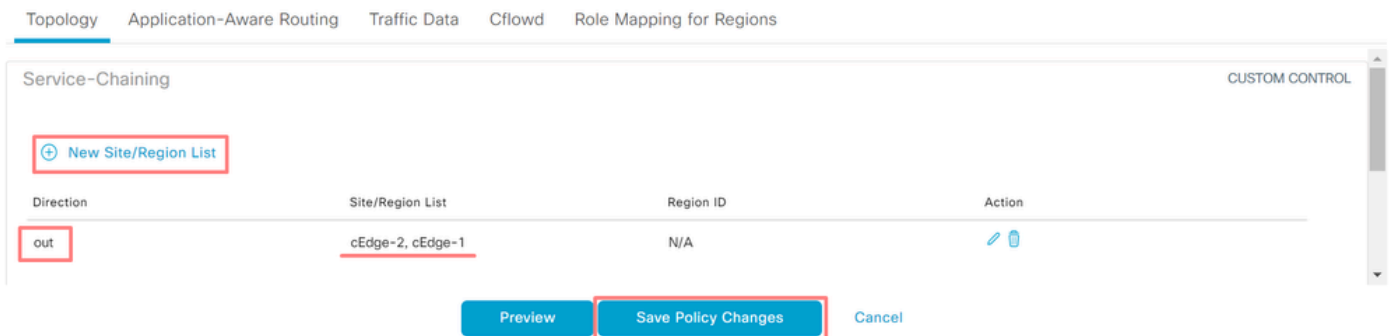
Verander de Standaardactie van het te accepteren beleid.

Klik op Overeenkomsten en acties opslaan en klik vervolgens op Configuratiebeleid opslaan.



4. Pas het beleid toe.

Klik op het tabblad Topologie, onder het Service-Chaining Policy selecteer Nieuwe site/regio lijst op uitgaande site lijst. Selecteer de sites die door het VRF 1-verkeer moeten worden geïnspecteerd en klik vervolgens op Beleid opslaan. Sla de wijzigingen op en klik op Beleidswijzigingen opslaan.



Advertentie-firewallservice

Configuratie via CLI

Specificeer het IP-adres van het firewallapparaat als u de Firewallservice wilt provisioneren. De service wordt via een OMP-update aangekondigd op de Cisco Catalyst SD-WAN controller.

```
<#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
```

Configuratie via sjabloon

Navigeer naar de functiesjabloon van de VRF 5.

Ga verder naar Configuratie > Sjablonen > Functiesjabloon > Sjabloon toevoegen > Cisco VPN.

Klik onder Service op New Service. Voer de waarden in, voeg de service toe en sla de sjabloon op.

✓ SERVICE

New Service

Service Type	<input type="text" value="FW"/>
IPv4 address	<input type="text" value="192.168.15.2"/>
Tracking	<input checked="" type="radio"/> On <input type="radio"/> Off

Verifiëren

Route voor lekkage

Bevestig dat Cisco Catalyst SD-WAN controller routes van VRF 1 naar VRF 5 en andersom exporteert.

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

Bevestig dat Cisco Edge-routers de uitgelekte route van VRF 1 naar VRF 5 hebben ontvangen.

Bevestig dat Cisco Edge-routers de uitgelekte route van VRF 5 naar VRF 1 hebben ontvangen.

<#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

```

Serviceketen

Controleer of Cisco Edge Router de firewallservice via OMP-serviceroute heeft geadverteerd naar de Cisco Catalyst SD-WAN controller.

```
<#root>
```

```
cEdge-01#
```

```
show sdwan omp services
```

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

Bevestig dat de Cisco Catalyst SD-WAN controller de serviceroute met succes heeft ontvangen.

```
<#root>
```

```
vSmart#
```

```
show omp services
```

ADDRESS						PATH	REGION			
FAMILY	TENANT	VPN	SERVICE	ORIGINATOR	FROM PEER	ID	ID	LABEL	STATUS	VRF
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
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			

Om te controleren of de Firewallservice het verkeer vanaf VRF 1 inspecteert, voert u een traceroute uit.

```
<#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
```

Gerelateerde informatie

- [Serviceketen](#)
- [Route voor lekkage](#)
- [SD-WAN - Route-lekkage instellen - YouTube](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.