

Konfigurieren von Route Leaking für Serviceverkettung im SD-WAN

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Route Leaking](#)

[Konfiguration über CLI](#)

[Konfiguration über Vorlage](#)

[Serviceverkettung](#)

[Konfiguration über CLI](#)

[Konfiguration über Vorlage](#)

[Firewall-Dienst ankündigen](#)

[Konfiguration über CLI](#)

[Konfiguration über Vorlage](#)

[Überprüfung](#)

[Route Leaking](#)

[Serviceverkettung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie die Serviceverkettung konfiguriert und verifiziert wird, um den Datenverkehr zwischen verschiedenen VRFs zu überprüfen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Kontrollrichtlinien.
- Vorlagen.

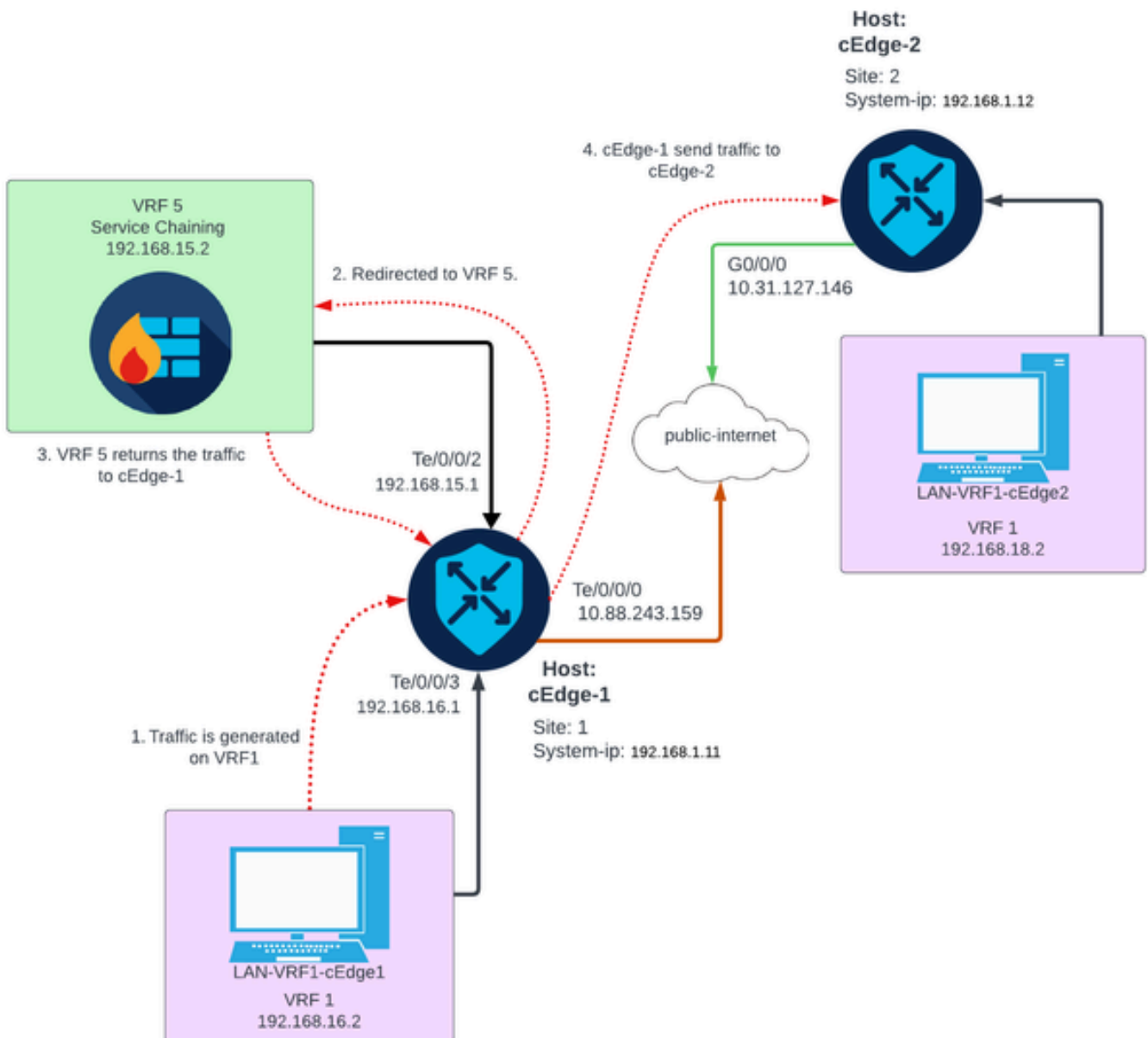
Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- SD-WAN-Controller (20.9.4.1)
- Cisco Edge-Router (17.09.04)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm



Hintergrundinformationen

Im Netzwerkdiagramm befindet sich der Firewall-Service in Virtual Routing and Forwarding (VRF)

5, während sich LAN-Geräte in VRF 1 befinden. Informationen zu Routen müssen von den VRF-Instanzen gemeinsam genutzt werden, damit die Weiterleitung und Überprüfung des Datenverkehrs möglich ist. Um Datenverkehr über einen Service weiterzuleiten, muss eine Steuerungsrichtlinie auf dem Cisco SD-WAN-Controller konfiguriert werden.

Konfigurieren

Route Leaking

Route Leaking ermöglicht die Weitergabe von Routing-Informationen zwischen verschiedenen VRFs. Wenn sich in diesem Szenario die Serviceverkettung (Firewall) und die LAN-Serviceseite in unterschiedlichen VRFs befinden, ist für die Datenverkehrsanalyse ein Route Leaking erforderlich.

Um das Routing zwischen LAN Service Side und Firewall Service sicherzustellen, ist in beiden VRFs ein Verlust von Routen erforderlich, und an den Standorten, an denen ein Verlust von Routen erforderlich ist, wird eine Richtlinie angewendet.

Konfiguration über CLI

1. Konfigurieren Sie Listen auf dem Cisco Catalyst SD-WAN Controller.

Durch die Konfiguration können Standorte anhand einer Liste identifiziert werden.

```
<#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. Konfigurieren der Richtlinie auf dem Cisco Catalyst SD-WAN-Controller

Die Konfiguration ermöglicht die Weitergabe von Routing-Informationen zwischen VRF 1 und VRF 5. Um sicherzustellen, dass das Routing zwischen den VRFs erfolgt, müssen beide VRFs ihre Routing-Daten gemeinsam nutzen.

Die Richtlinie ermöglicht die Annahme und den Export von Datenverkehr von VRF 1 in VRF 5 und umgekehrt.

```
<#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. Wenden Sie die Richtlinie auf den Cisco Catalyst SD-WAN Controller an.

Die Richtlinie wird an Standort 1 und 2 angewendet, um das Routing zwischen der VRF-1 an diesen Standorten und der VRF-5-Instanz zu ermöglichen.

Die Richtlinie wird für eingehenden Datenverkehr implementiert, d. h., sie wird auf OMP-Updates angewendet, die von Cisco Edge-Routern an den Cisco Catalyst SD-WAN-Controller gesendet werden.

```
<#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
```

Konfiguration über Vorlage



Hinweis: Um die Richtlinie über die grafische Benutzeroberfläche (GUI) Cisco Catalyst SD-WAN Manager zu aktivieren, muss dem Cisco Catalyst SD-WAN-Controller eine Vorlage zugeordnet sein.

1. Erstellen Sie die Richtlinie, um die Weitergabe von Routing-Informationen zu ermöglichen.

Erstellen Sie auf dem Cisco Catalyst SD-WAN Manager eine Richtlinie, und navigieren Sie zu Konfiguration > Richtlinien > Zentrale Richtlinie.

Klicken Sie auf der Registerkarte Zentrale Richtlinie auf Richtlinie hinzufügen.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Erstellen Sie Listen auf dem Cisco Catalyst SD-WAN Manager. Durch die Konfiguration können Standorte mithilfe einer Liste identifiziert werden.

Navigieren Sie zu Site > New Site List.

Erstellen Sie die Liste der Standorte, an denen ein Route Leaking erforderlich ist, und fügen Sie die Liste hinzu.

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

Navigieren Sie zu VPN > New VPN List (Neue VPN-Liste).

Erstellen Sie die VPN-Liste, auf die das Route Leaking angewendet werden muss, und klicken Sie auf "Weiter".

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. Konfigurieren Sie die Richtlinie auf dem Cisco Catalyst SD-WAN Manager.

Klicken Sie auf die Registerkarte Topologie und anschließend auf Topologie hinzufügen.

Erstellen eines benutzerdefinierten Steuerelements (Route und TLOC)

Search

Add Topology ▾

Hub-and-Spoke

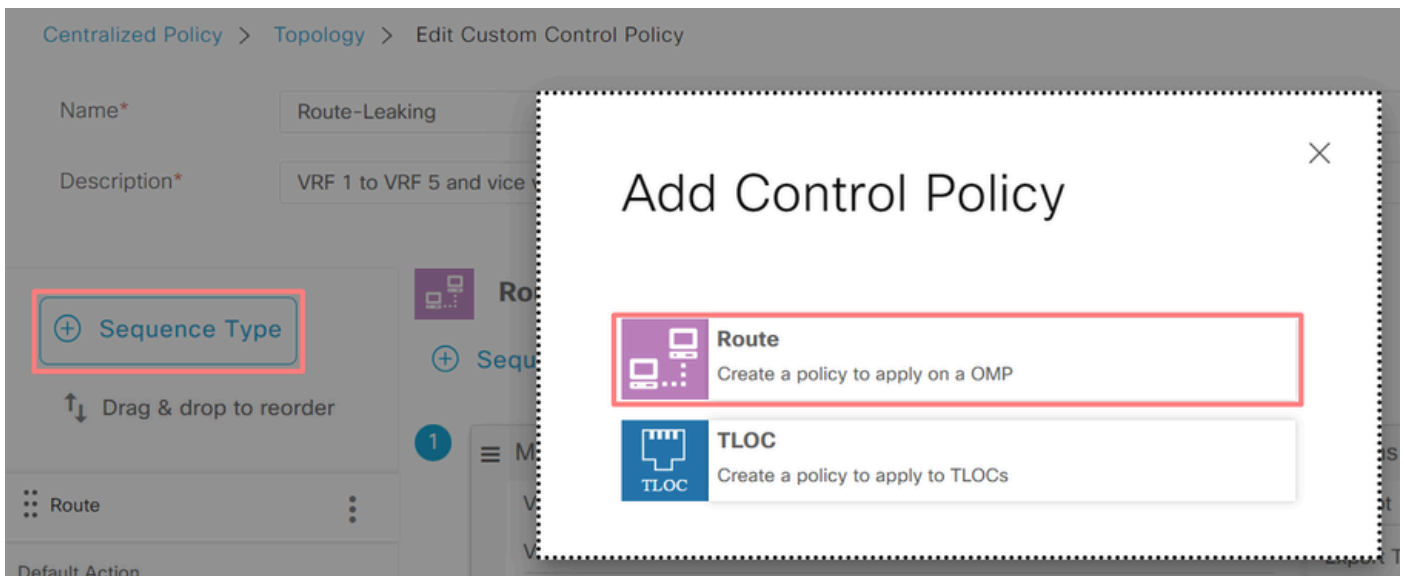
Mesh

Custom Control (Route & TLOC)

Import Existing Topology

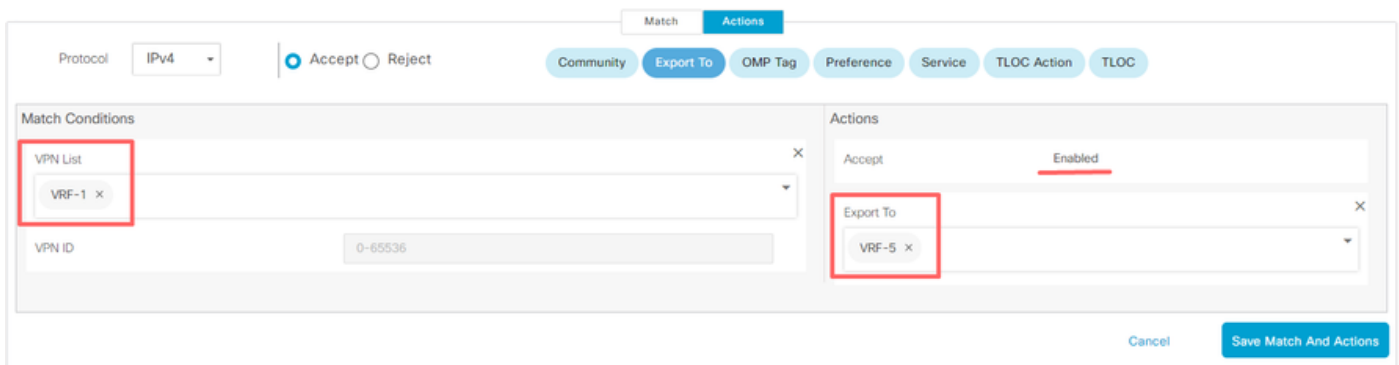
Description	Mode
No data available	

Klicken Sie auf Sequence Type (Sequenztyp), und wählen Sie Route Sequence (Weiterleitungssequenz) aus.

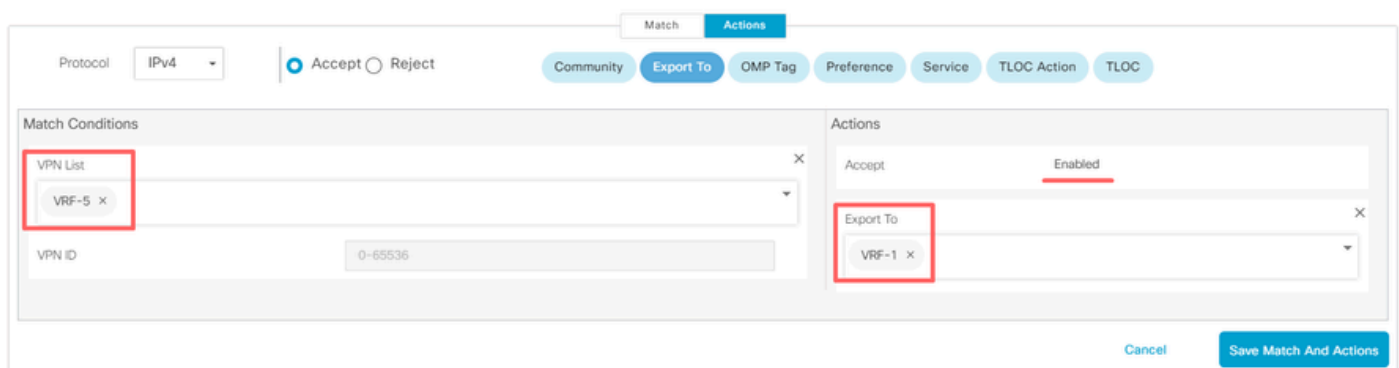


Fügen Sie eine Sequenzregel hinzu.

Bedingung 1: Der Datenverkehr von VRF 1 wird akzeptiert und in die VRF 5 exportiert.



Bedingung 2: Datenverkehr von VRF 5 wird akzeptiert und in VRF 1 exportiert.



Ändern Sie die Standardaktion der Richtlinie in Akzeptieren.

Klicken Sie auf Save Match and Actions (Übereinstimmung und Aktionen speichern) und dann auf Save Control Policy (Kontrollrichtlinie speichern).

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel



4. Wenden Sie die Richtlinie auf die Websites an, auf denen ein Route Leaking erforderlich ist.

Klicken Sie auf die Registerkarte Topologie, und wählen Sie unter "Route-Leaking Policy" (Richtlinie für Weiterleitung) in der Liste eingehender Standorte die Option New Site/Region List (Neue Standort-/Regionsliste). Wählen Sie die Standortlisten aus, wo ein Route Leaking erforderlich ist.

Um die Änderungen zu speichern, wählen Sie Richtlinienänderungen speichern aus.

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

Serviceverkettung

Die Serviceverkettung wird auch als Serviceeinbindung bezeichnet. Dazu gehört die Implementierung eines Netzwerkdienstes. Zu den Standarddiensten gehören Firewall (FW), Intrusion Detection System (IDS) und Intrusion Prevention System (IPS). In diesem Fall wird ein Firewall-Dienst in den Datenpfad eingefügt.

Konfiguration über CLI

1. Konfigurieren Sie die Listen auf dem Cisco Catalyst SD-WAN Controller.

Durch die Konfiguration können Standorte anhand einer Liste identifiziert werden.

Erstellen Sie eine Liste der Standorte, an denen sich die einzelnen VRF 1-Instanzen befinden.

Geben Sie in der TLOC-Liste (Transport Location) die Adresse an, an die der Datenverkehr umgeleitet werden muss, um den Service zu erreichen.

```
<#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. Konfigurieren der Richtlinie auf dem Cisco Catalyst SD-WAN-Controller

Die Sequenz filtert den Datenverkehr von VRF 1. Der Datenverkehr wird über eine Service-Firewall auf VRF 5 zugelassen und überprüft.

```
<#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. Wenden Sie die Richtlinie auf den Cisco Catalyst SD-WAN Controller an.

Die Richtlinie wird an Standort 1 und 2 konfiguriert, um die Überprüfung des Datenverkehrs von VRF 1 zu ermöglichen.

```
<#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
```

Konfiguration über Vorlage



Hinweis: Um die Richtlinie über die grafische Benutzeroberfläche (GUI) des Cisco Catalyst SD-WAN Manager zu aktivieren, muss dem Cisco Catalyst SD-WAN-Controller eine Vorlage zugeordnet sein.

1. Erstellen Sie Richtlinien auf dem Cisco Catalyst SD-WAN Manager.

Navigieren Sie zu Konfiguration > Richtlinien > Zentrale Richtlinie.

Klicken Sie auf der Registerkarte "Zentrale Richtlinie" auf Richtlinie hinzufügen.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Erstellen Sie Listen auf dem Cisco Catalyst SD-WAN Manager.

Navigieren Sie zu Site > New Site List.

Erstellen Sie die Standortliste der Standorte, auf denen sich VRF 1 befindet, und wählen Sie Hinzufügen aus.

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

+ New Site List

Site List Name*

Add Site*

Add Cancel

Navigieren Sie zu TLOC > New TLOC List (Neue TLOC-Liste).

Erstellen Sie die Verkettung des TLOC-Listendienstes am , und wählen Sie Speichern aus.

TLOC List

List Name *

TLOC IP*

Color*

 ▼

Encap*

 ▼

Preference

⊕ Add TLOC

Cancel

Save

3. Sequenzregeln hinzufügen.

Klicken Sie auf die Registerkarte Topologie und anschließend auf Topologie hinzufügen.

Erstellen eines benutzerdefinierten Steuerelements (Route und 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

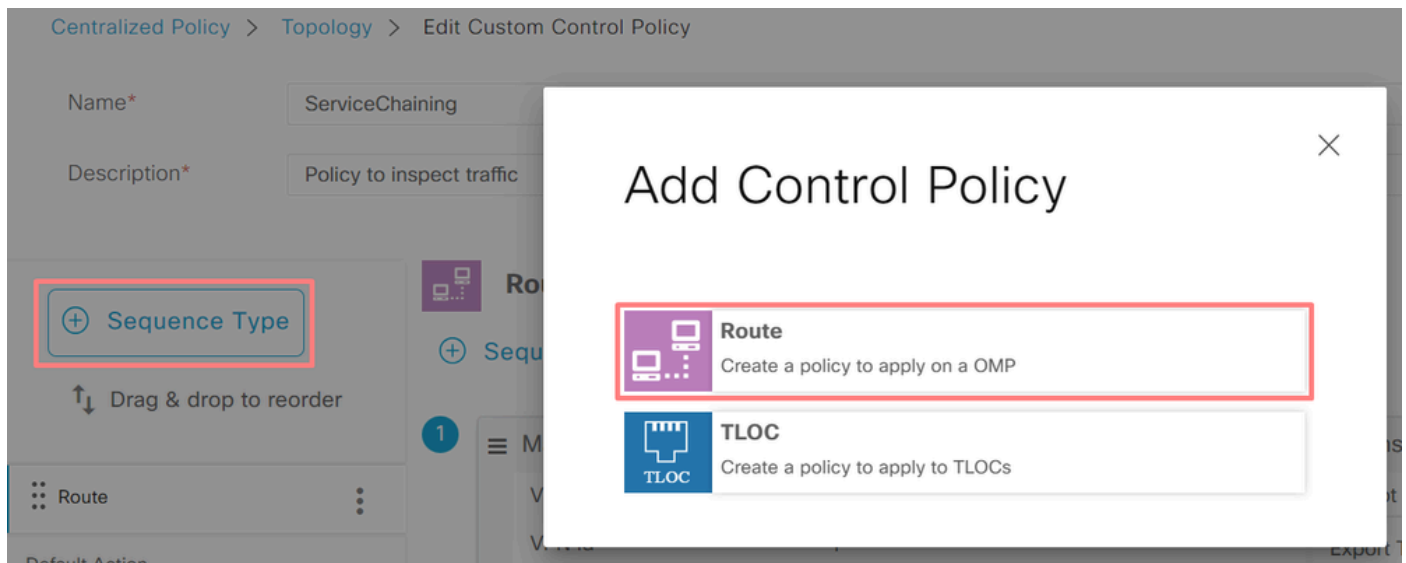
Description

Mode

No data available

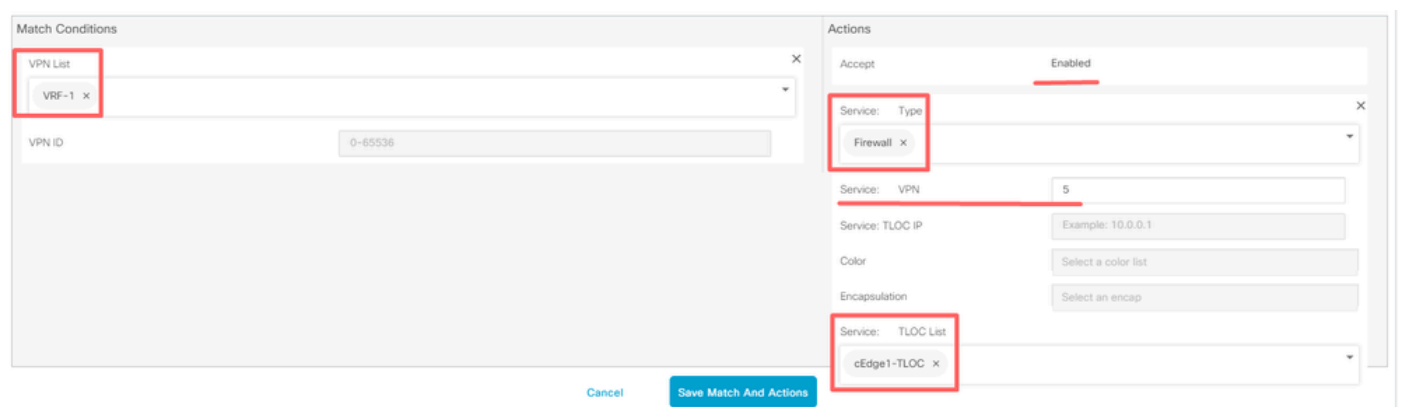
Klicken Sie auf Sequence Type (Sequenztyp), und wählen Sie Route Sequence

(Weiterleitungssequenz) aus.



Fügen Sie eine Sequenzregel hinzu.

Die Sequenz filtert den Datenverkehr von der VRF-Instanz 1, lässt ihn zu und leitet ihn dann an einen Service (Firewall) weiter, der innerhalb der VRF-Instanz 5 vorhanden ist. Dies kann durch die Verwendung des TLOC am Standort 1 erreicht werden, der den Standort des Firewall-Services darstellt.



Ändern Sie die Standardaktion der Richtlinie in Akzeptieren.

Klicken Sie auf Save Match and Actions (Übereinstimmung und Aktionen speichern) und dann auf Save Control Policy (Kontrollrichtlinie speichern).

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel



4. Wenden Sie die Richtlinie an.

Klicken Sie auf die Registerkarte Topologie, und wählen Sie unter der Richtlinie für die Serviceverkettung in der Liste ausgehender Standorte die Option Neue Standort-/Regionsliste aus. Wählen Sie die Standorte aus, die der VRF-1-Datenverkehr überprüfen muss, und klicken Sie dann auf Save Policy (Richtlinie speichern). Speichern Sie die Änderungen, und klicken Sie auf Richtlinienänderungen speichern.

Topology Application-Aware Routing Traffic Data Cflowd Role Mapping for Regions

Service-Chaining CUSTOM CONTROL

+ New Site/Region List

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

Preview Save Policy Changes Cancel

Firewall-Dienst ankündigen

Konfiguration über CLI

Um den Firewall-Service bereitzustellen, geben Sie die IP-Adresse des Firewall-Geräts an. Der Service wird dem Cisco Catalyst SD-WAN-Controller durch ein OMP-Update angekündigt.

```
<#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
```

Konfiguration über Vorlage

Navigieren Sie zur Featurevorlage der VRF-Instanz 5.

Fahren Sie mit Konfiguration > Vorlagen > Funktionsvorlage > Vorlage hinzufügen > Cisco VPN fort.

Klicken Sie unter Service auf New Service (Neuer Service). Geben Sie die Werte ein, fügen Sie den Service hinzu und speichern Sie die Vorlage.

SERVICE

New Service

Service Type



FW



IPv4 address



192.168.15.2

Tracking



On

Off

Überprüfung

Route Leaking

Vergewissern Sie sich, dass der Cisco Catalyst SD-WAN-Controller Routen von VRF 1 zu VRF 5 und umgekehrt exportiert.

```
<#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.
						installed	192.168.
1	192.168.16.0/24	192.168.3.16	69	1002	C,R	installed	192.168
1	192.168.18.0/24	192.168.3.15	69	1002	C,R	installed	192.168

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
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.

Bestätigen Sie, dass die Cisco Edge-Router die geleakte Route von VRF 1 zu VRF 5 erhalten haben.

Bestätigen Sie, dass die Cisco Edge-Router die geleakte Route von VRF 5 zu VRF 1 erhalten haben.

<#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

```

Serviceverkettung

Vergewissern Sie sich, dass der Cisco Edge Router den Firewall-Service über die OMP-Service-Route dem Cisco Catalyst SD-WAN-Controller angekündigt hat.

<#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

Bestätigen Sie, dass der Cisco Catalyst SD-WAN-Controller die Serviceroute erfolgreich erhalten hat.

<#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

Um zu überprüfen, ob der Firewall-Service den Datenverkehr von VRF 1 überprüft, führen Sie eine Traceroute durch.

<#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
```

Zugehörige Informationen

- [Serviceverkettung](#)
- [Route Leaking](#)
- [SD-WAN - Konfigurieren des Route Leaking - YouTube](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.