

Configuración de la fuga de ruta para el encadenamiento de servicios en SD-WAN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Antecedentes](#)

[Configurar](#)

[Fuga de ruta](#)

[Configuración mediante CLI](#)

[Configuración mediante plantilla](#)

[Encadenamiento de servicios](#)

[Configuración mediante CLI](#)

[Configuración mediante plantilla](#)

[Anunciar servicio de firewall](#)

[Configuración mediante CLI](#)

[Configuración mediante plantilla](#)

[Verificación](#)

[Fuga de ruta](#)

[Encadenamiento de servicios](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y verificar el encadenamiento de servicios para inspeccionar el tráfico a través de diferentes VRF.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software de Cisco (SD-WAN)
- Políticas de Control.
- Plantillas.

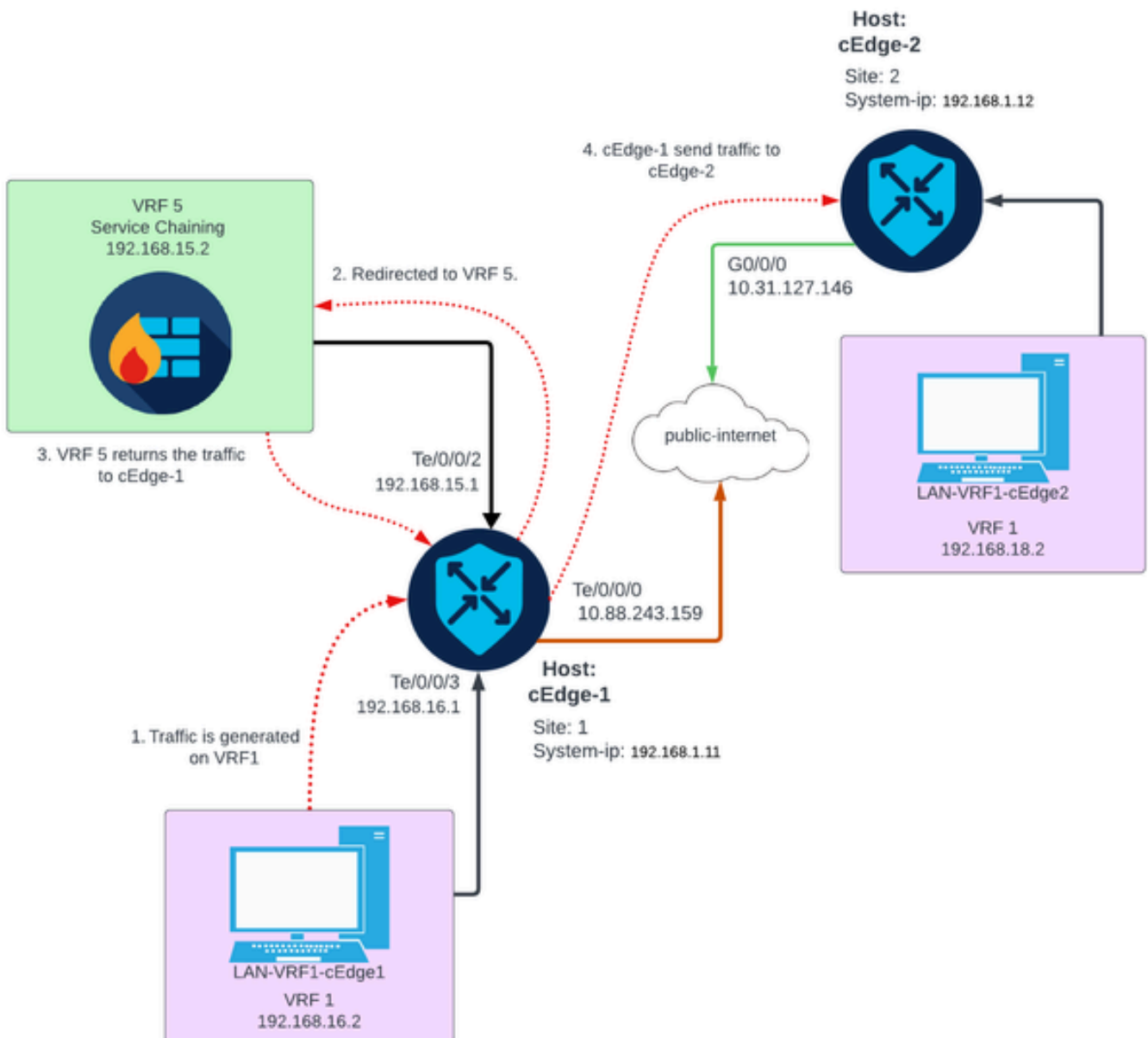
Componentes Utilizados

Este documento se basa en las siguientes versiones de software y hardware:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red



Antecedentes

En el diagrama de red, el servicio de firewall se encuentra en Virtual Routing and Forwarding

(VRF) 5, mientras que los dispositivos LAN se encuentran en VRF 1. La información de las rutas debe ser compartida entre los VRFs para que se pueda lograr el reenvío y la inspección del tráfico. Para enrutar el tráfico a través de un servicio, debe configurarse una política de control en el controlador Cisco SD-WAN.

Configurar

Fuga de ruta

La fuga de ruta habilita la propagación de la información de ruteo entre diferentes VRF. En esta situación, cuando el encadenamiento de servicios (firewall) y el servicio LAN se encuentran en diferentes VRF, es necesario que se produzca una fuga de ruta para la inspección del tráfico.

Para garantizar el ruteo entre el lado del servicio LAN y el servicio Firewall, se necesita la fuga de rutas en ambos VRF y aplicar una política en los sitios donde se requiere la fuga de rutas.

Configuración mediante CLI

1. Configure las listas en el controlador Cisco Catalyst SD-WAN.

La configuración permite identificar los sitios mediante una lista.

```
<#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. Configure la política en el controlador Cisco Catalyst SD-WAN.

La configuración permite la propagación de la información de ruteo entre VRF 1 y VRF 5, para garantizar el ruteo entre ellos, ambos VRF deben compartir sus datos de ruteo.

La política permite que el tráfico de VRF 1 sea aceptado y exportado al VRF 5 y viceversa.

```
<#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. Aplique la política en el controlador Cisco Catalyst SD-WAN.

La política se aplica en el sitio 1 y el sitio 2 para permitir el ruteo entre el VRF 1 ubicado en esos sitios y en el VRF 5.

La política se implementa de forma entrante, lo que significa que se aplica a las actualizaciones de OMP procedentes de los routers periféricos de Cisco al controlador Cisco Catalyst SD-WAN.

```
<#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
```

Configuración mediante plantilla



Nota: para activar la política a través de la interfaz gráfica de usuario (GUI) de Cisco Catalyst SD-WAN Manager, el controlador Cisco Catalyst SD-WAN debe tener una plantilla adjunta.

1. Cree la política para permitir la propagación de la información de enrutamiento.

Cree la política en el Cisco Catalyst SD-WAN Manager, navegue hasta **Configuración > Políticas > Política centralizada**.

En la ficha **Directiva centralizada**, haga clic en **Agregar directiva**.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Crear listas en el Cisco Catalyst SD-WAN Manager, la configuración permite que los sitios se identifiquen a través de una lista.

Vaya a Sitio > Nueva lista de sitios.

Cree la lista de sitios donde se necesita la fuga de rutas y agregue la lista.

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

Vaya a VPN > Lista de VPN nueva.

Cree la lista VPN donde se debe aplicar la fuga de ruta, haga clic en 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. Configure la política en el Cisco Catalyst SD-WAN Manager.

Haga clic en la ficha Topología y haga clic en Agregar topología.

Crear un control personalizado (Route & TLOC).

Search

Add Topology ▾

Hub-and-Spoke

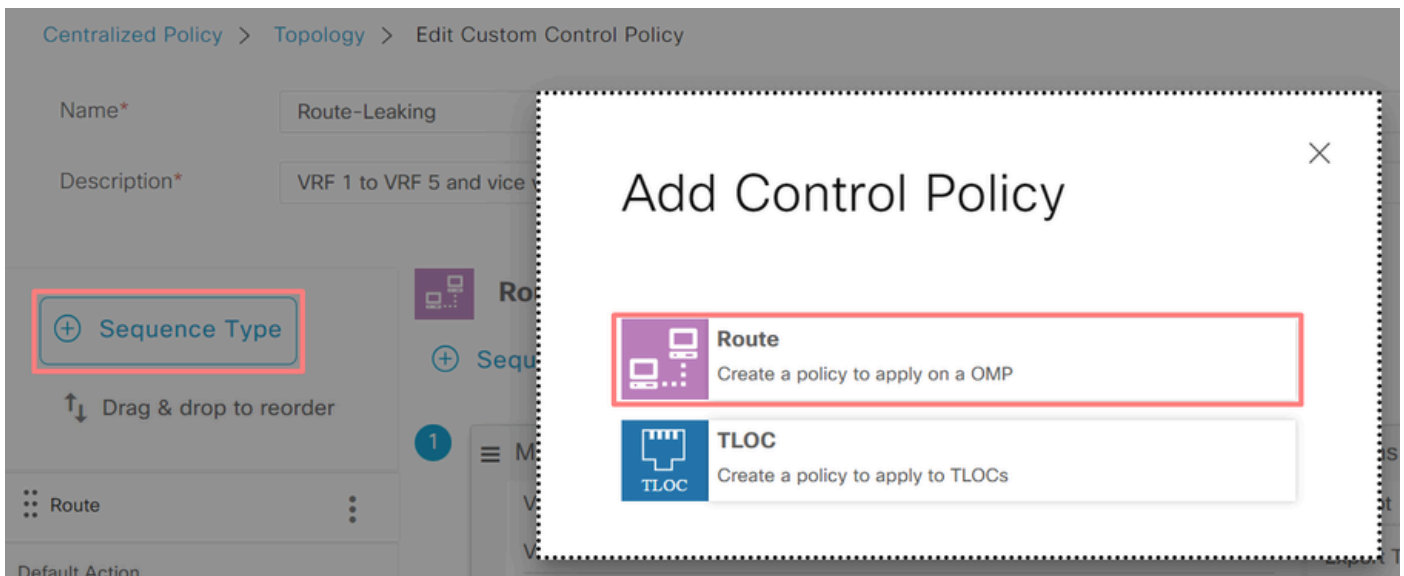
Mesh

Custom Control (Route & TLOC)

Import Existing Topology

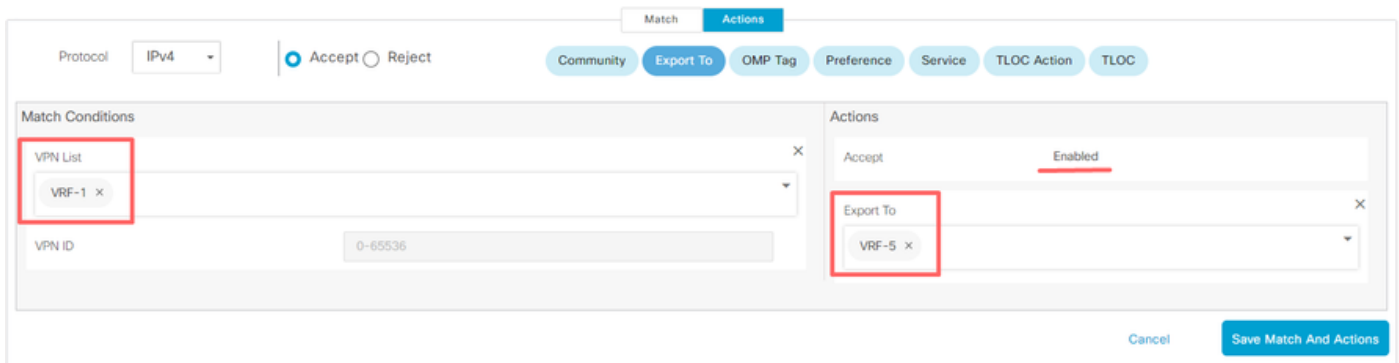
Description	Mode
No data available	

Haga clic en Tipo de secuencia y seleccione Ruta.

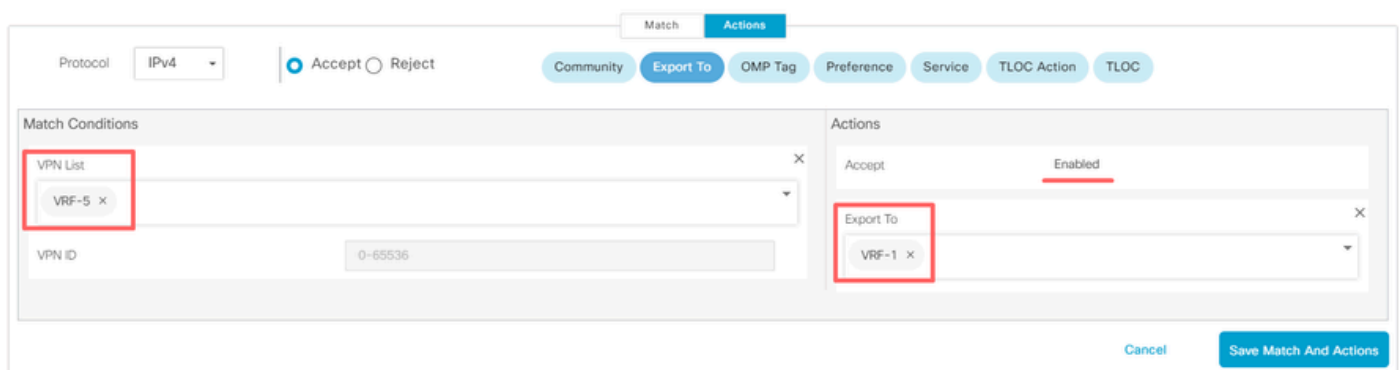


Agregue una regla de secuencia.

Condición 1: Se acepta el tráfico de VRF 1 y se exporta al VRF 5.



Condición 2: Se acepta el tráfico de VRF 5 y se exporta al VRF 1.



Cambie la Acción predeterminada de la política a Aceptar.

Haga clic en Guardar coincidencia y acciones y, a continuación, haga clic en Guardar directiva de control.

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel



4. Aplique la política en los sitios donde se necesita fuga de ruta.

Haga clic en la pestaña Topology, en Route-Leaking Policy, seleccione New Site/Region List en Inbound Site List. Seleccione las listas de sitios en las que se necesita filtrado de rutas.

Para guardar las modificaciones, seleccione Save Policy Changes.

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

Encadenamiento de servicios

El encadenamiento de servicios también se conoce como inserción de servicios. Implica la inyección de un servicio de red; los servicios estándar incluyen firewall (FW), sistema de detección de intrusiones (IDS) y sistema de prevención de intrusiones (IPS). En este caso, se inserta un servicio de firewall en la ruta de datos.

Configuración mediante CLI

1. Configure las listas en el controlador Cisco Catalyst SD-WAN.

La configuración permite identificar los sitios mediante una lista.

Cree una lista para los sitios en los que se encuentra cada VRF 1.

En la lista Ubicación de transporte (TLOC), especifique la dirección a la que se debe redirigir el tráfico para llegar al servicio.

<#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. Configure la política en el controlador Cisco Catalyst SD-WAN.

La secuencia filtra el tráfico de VRF 1. El tráfico se permite e inspecciona en un firewall de servicio ubicado en 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. Aplique la política en el controlador Cisco Catalyst SD-WAN.

La política se configura en los sitios 1 y 2 para permitir que se inspeccione el tráfico de 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
```

Configuración mediante plantilla



Nota: para activar la política a través de la interfaz gráfica de usuario (GUI) de Cisco Catalyst SD-WAN Manager, el controlador Cisco Catalyst SD-WAN debe tener una plantilla adjunta.

1. Crear una política en Cisco Catalyst SD-WAN Manager.

Vaya a Configuración > Políticas > Política centralizada.

En la pestaña Política centralizada, haga clic en Agregar política.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Crear listas en el Cisco Catalyst SD-WAN Manager.

Vaya a Sitio > Nueva lista de sitios.

Cree la lista de sitios de los sitios en los que se encuentra VRF 1 y seleccione Agregar.

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

Vaya a TLOC > Nueva lista TLOC.

Cree la lista TLOC donde se encuentra el encadenamiento de servicios y seleccione Save.



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. Agregue reglas de secuencia.

Haga clic en la pestaña Topology y haga clic en Add Topology.

Crear un control personalizado (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)

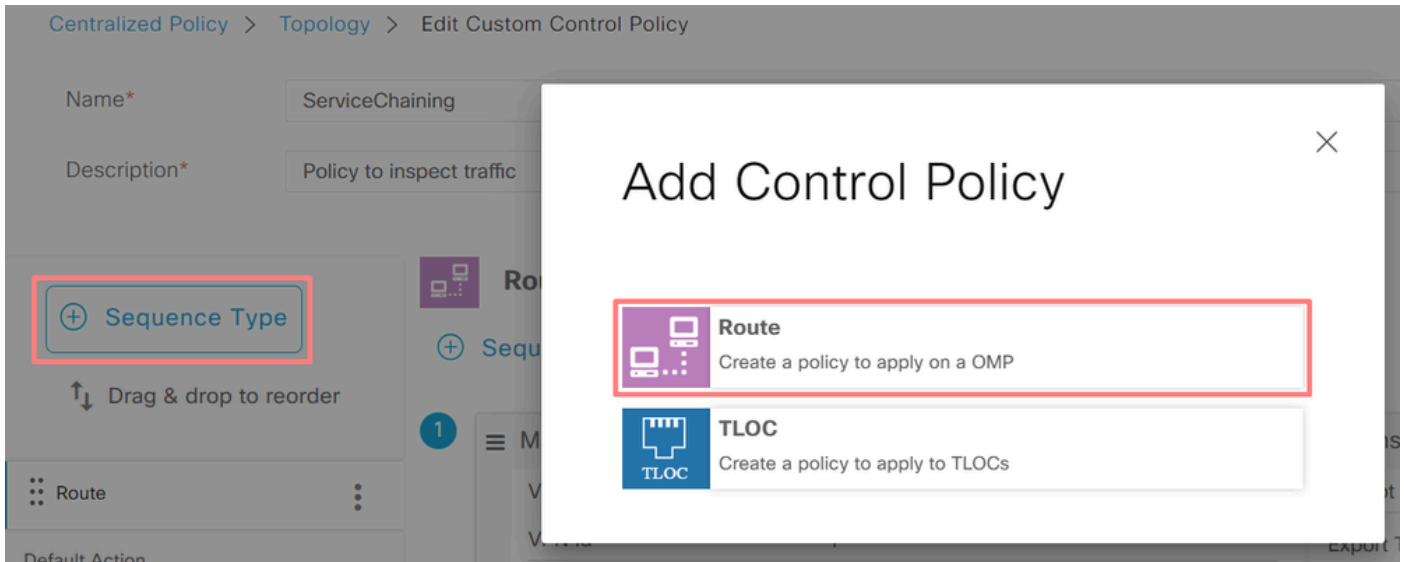
Import Existing Topology

Description

Mode

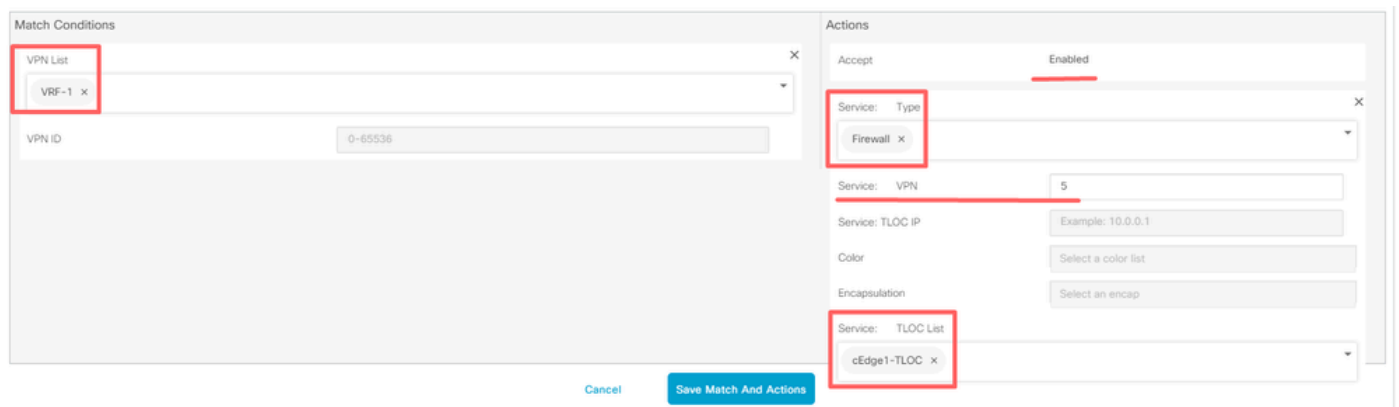
No data available

Haga clic en Tipo de secuencia y seleccione Ruta.



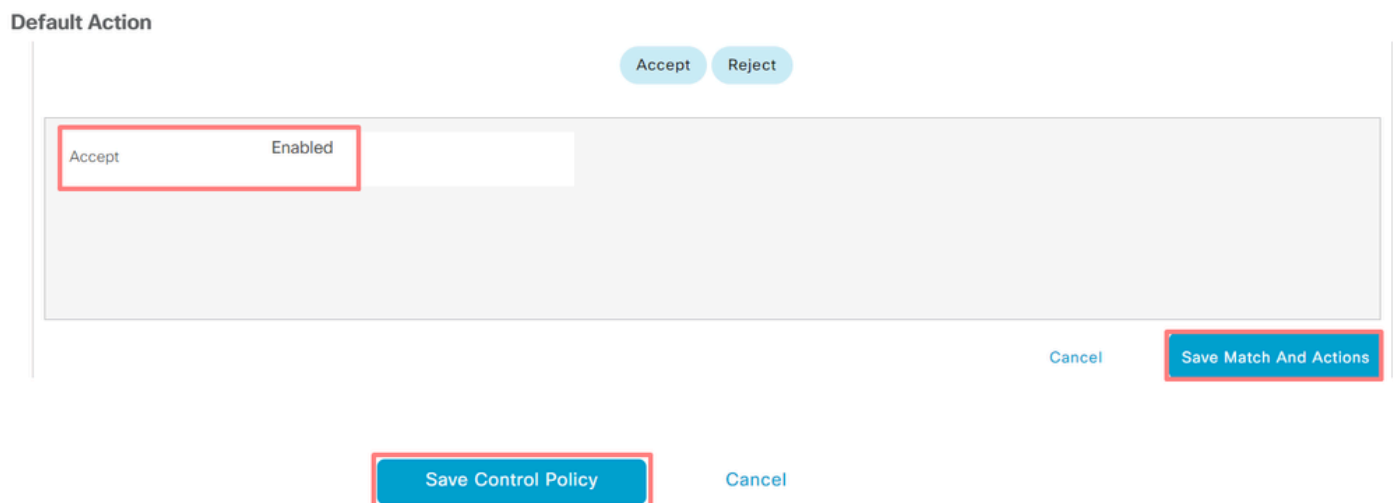
Agregue una regla de secuencia.

La secuencia filtra el tráfico desde el VRF 1, lo permite y, a continuación, lo redirige a un servicio (firewall) que existe en el VRF 5. Esto se puede lograr mediante el TLOC en el sitio 1, que es la ubicación del servicio de firewall.



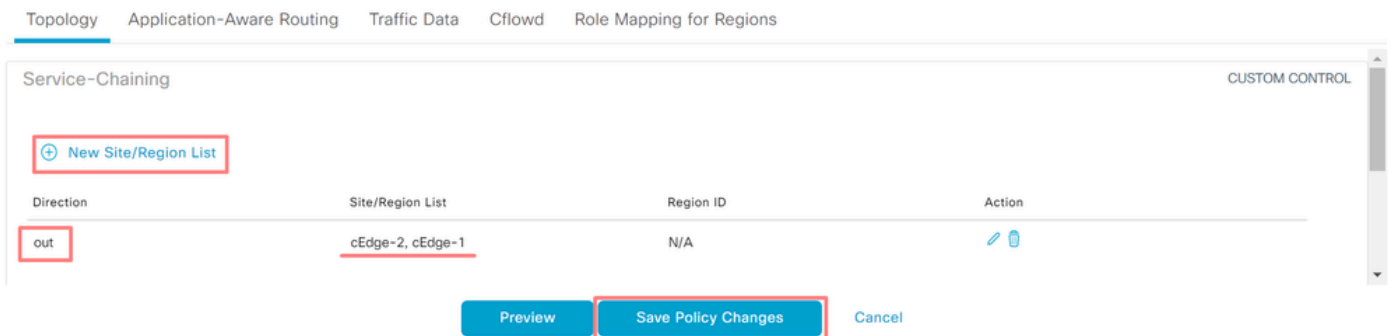
Cambie la Acción predeterminada de la política a Aceptar.

Haga clic en Save Match and Actions y luego haga clic en Save Control Policy.



4. Aplique la política.

Haga clic en la pestaña Topology, en la política de encadenamiento de servicios, seleccione New Site/Region List en la Lista de sitios salientes. Seleccione los sitios que el tráfico VRF 1 debe inspeccionar y luego haga clic en Save Policy. Guarde las modificaciones, haga clic en Save Policy Changes.



Anunciar servicio de firewall

Configuración mediante CLI

Para aprovisionar el servicio de firewall, especifique la dirección IP del dispositivo de firewall. El servicio se anuncia al controlador Cisco Catalyst SD-WAN mediante una actualización de 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
```

Configuración mediante plantilla

Vaya a la plantilla de función del VRF 5.

Vaya a Configuration > Templates > Feature Template > Add Template > Cisco VPN.

En la sección Servicio, haga clic en Nuevo servicio. Introduzca los valores, Add the Service y Save the template.

Service Type: FW

IPv4 address: 192.168.15.2

Tracking: On Off

Verificación

Fuga de ruta

Confirme que Cisco Catalyst SD-WAN Controller exporta rutas de VRF 1 a VRF 5 y viceversa.

<#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	192.168.15.2
						installed	192.168.15.2
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	192.168.15.2
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.

Confirme que los routers periféricos de Cisco recibieron la ruta filtrada de VRF 1 a VRF 5.

Confirme que los routers periféricos de Cisco recibieron la ruta filtrada de VRF 5 a 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
```

Encadenamiento de servicios

Verifique que el router Cisco Edge haya anunciado el servicio de firewall al controlador Cisco Catalyst SD-WAN a través de la ruta de servicio 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

Confirme que el controlador Cisco Catalyst SD-WAN ha recibido correctamente la ruta de servicio.

```
<#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		

Para verificar que el servicio de firewall inspecciona el tráfico de VRF 1, realice un 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
```

Información Relacionada

- [Encadenamiento de servicios](#)
- [Fuga de ruta](#)
- [El Fuego de Rutas - YouTube](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).