

配置SD-WAN中服务链接的路由渗透

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[背景信息](#)

[配置](#)

[路由渗透](#)

[通过CLI配置](#)

[通过模板进行配置](#)

[服务链](#)

[通过CLI配置](#)

[通过模板进行配置](#)

[通告防火墙服务](#)

[通过CLI配置](#)

[通过模板进行配置](#)

[验证](#)

[路由渗透](#)

[服务链](#)

[相关信息](#)

简介

本文档介绍如何配置和验证服务链，以检查不同VRF之间的流量。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- 控制策略。
- 模板。

使用的组件

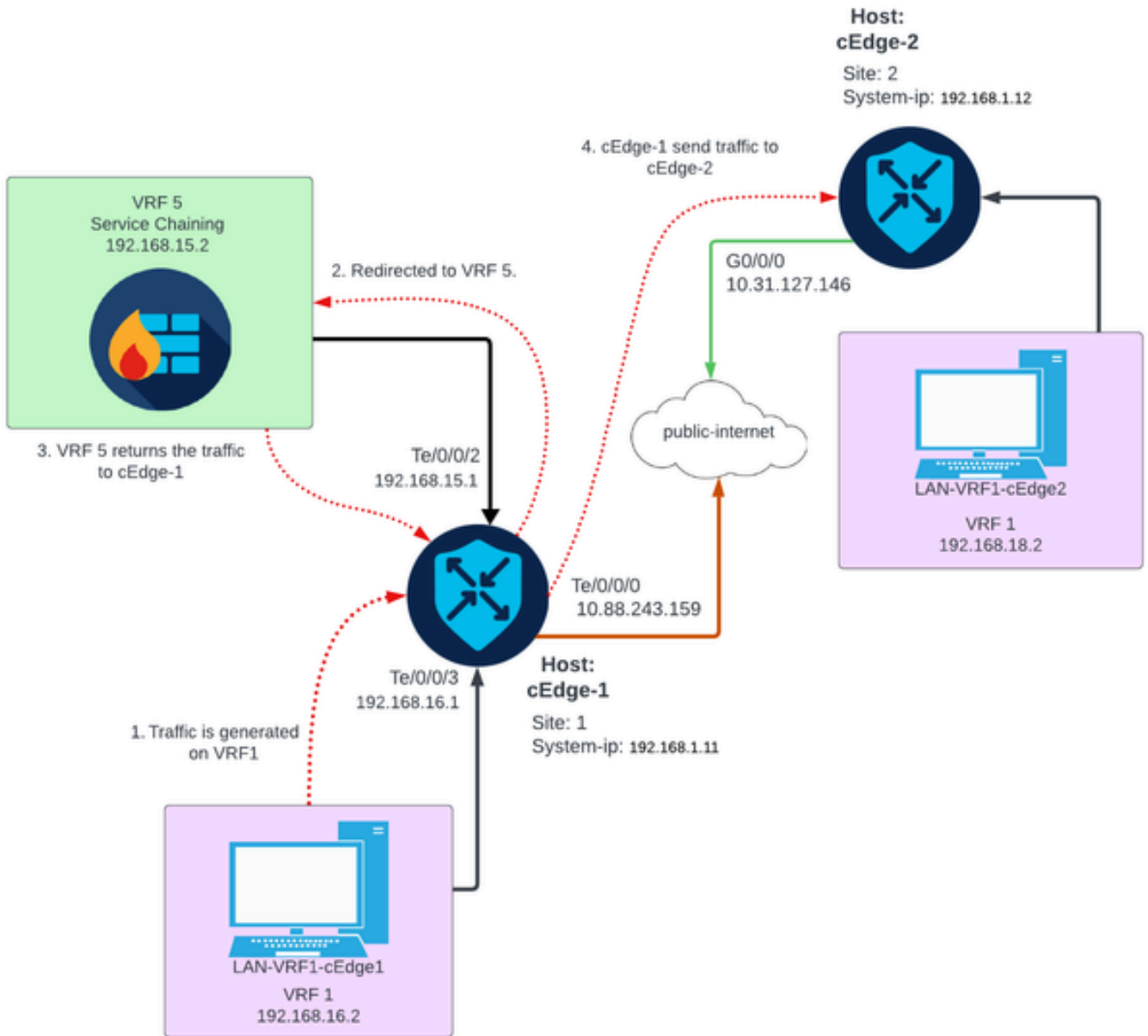
本文档基于以下软件和硬件版本：

- SD-WAN控制器(20.9.4.1)

- 思科边缘路由器(17.09.04)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图



背景信息

在网络图中，防火墙服务处于虚拟路由和转发(VRF) 5中，而LAN设备位于VRF 1中。路由信息必须在VRF之间共享，以便实现流量的转发和检查。要通过服务路由流量，必须在Cisco SD-WAN控制器上配置控制策略。

配置

路由渗透

路由泄漏允许在不同的VRF之间传播路由信息。在这种情况下，当服务链（防火墙）和LAN服务端处于不同的VRF中时，路由泄漏对于流量检测必不可少。

为确保LAN服务端和防火墙服务之间的路由，需要在两个VRF中都泄漏路由，并在需要路由泄漏的站点中应用策略。

通过CLI配置

1. 在Cisco Catalyst SD-WAN控制器上配置列表。

该配置允许通过列表识别站点。

```
<#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. 在Cisco Catalyst SD-WAN控制器上配置策略。

该配置允许在VRF 1和VRF 5之间传播路由信息，以确保两者之间的路由，两个VRF必须共享其路由数据。

策略允许VRF 1的流量被接受并导出到VRF 5，反之亦然。

```
<#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. 在Cisco Catalyst SD-WAN控制器上应用策略。

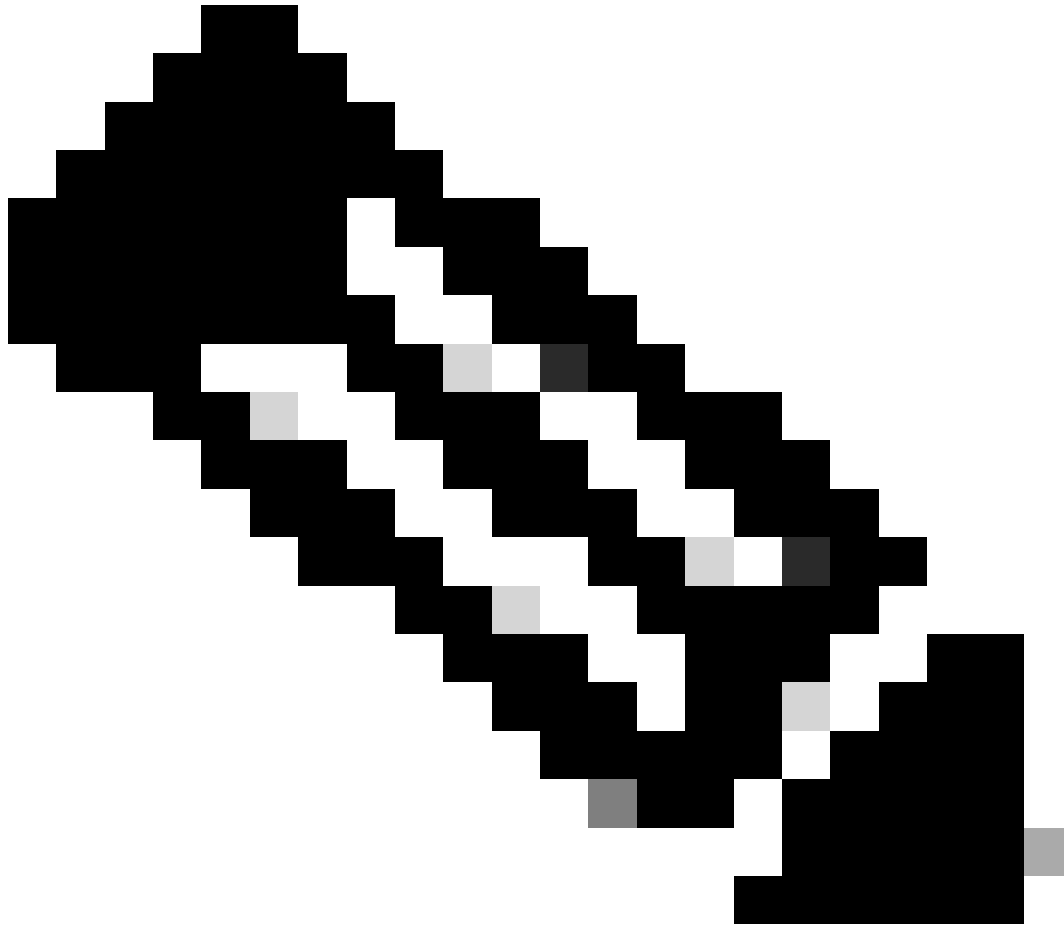
策略应用于站点1和站点2，以允许在这些站点和VRF 5上的VRF 1之间进行路由。

策略是入站实施的，这意味着将应用于从思科边缘路由器到Cisco Catalyst SD-WAN控制器的OMP更新。

<#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
```

通过模板进行配置



注意：要通过Cisco Catalyst SD-WAN Manager图形用户界面(GUI)激活策略，Cisco Catalyst SD-WAN控制器必须附加模板。

1. 创建策略以允许传播路由信息。

在Cisco Catalyst SD-WAN Manager上创建策略，导航至配置>策略>集中策略。

在Centralized Policy (集中策略) 选项卡下，点击Add Policy (添加策略)。

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. 在Cisco Catalyst SD-WAN Manager上创建列表，配置允许通过列表识别站点。

导航到站点>新建站点列表。

创建需要路由泄漏的站点列表并添加该列表。

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*

Add Site*

Add Cancel

导航到VPN > New VPN List。

创建需要应用路由泄漏的VPN列表，然后单击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. 在Cisco Catalyst SD-WAN Manager上配置策略。

点击Topology(拓扑)选项卡，然后点击Add Topology (添加拓扑)。

创建自定义控件(Route & TLOC)。

Search

Add Topology ▾

Hub-and-Spoke

Mesh

Custom Control (Route & TLOC)

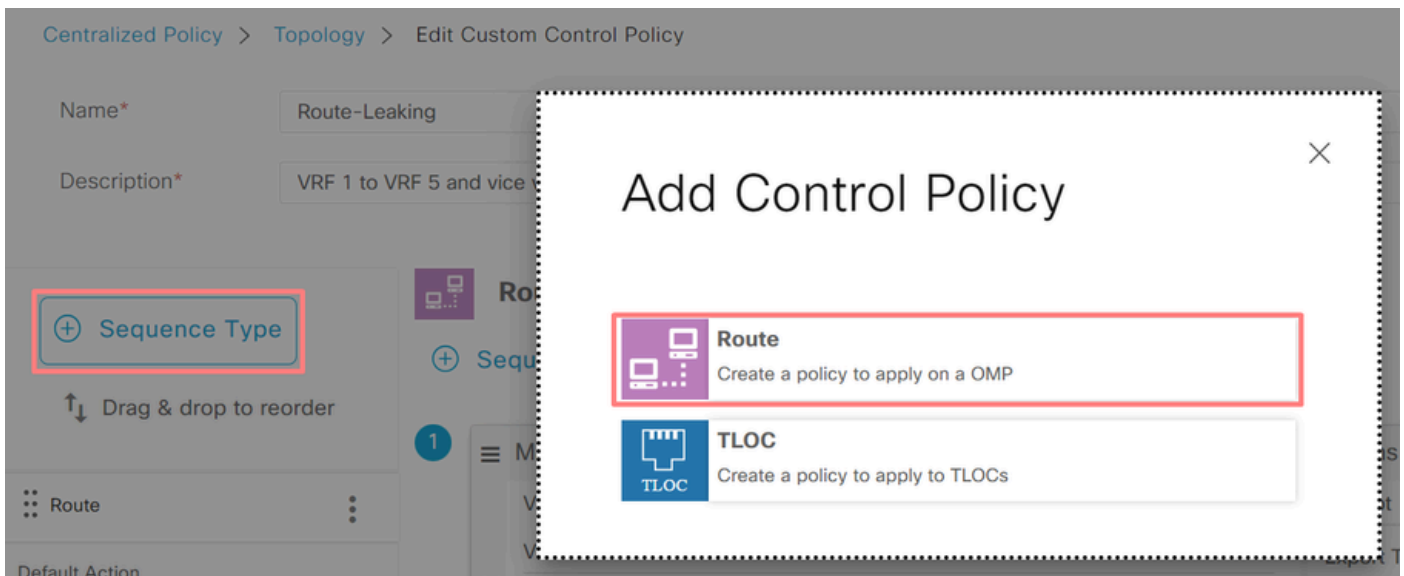
Import Existing Topology

Description

Mode

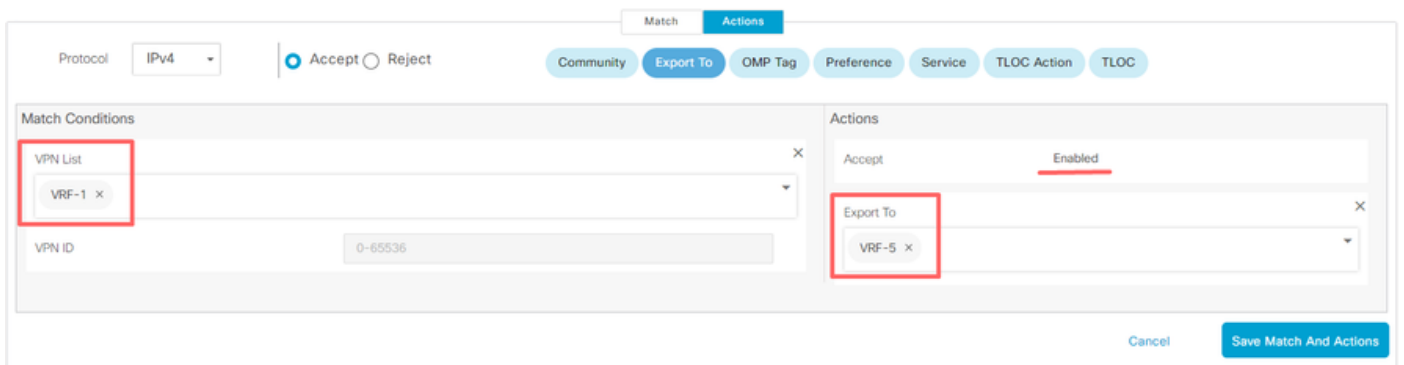
No data available

点击Sequence Type并选择Route sequence。

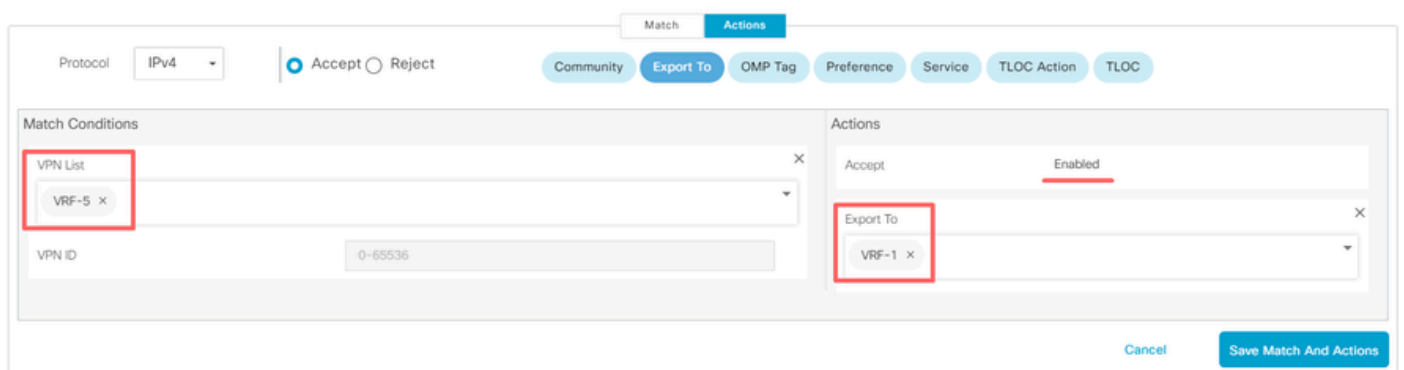


添加序列规则。

条件1：接受VRF 1的流量并将其导出到VRF 5。



条件2：接受VRF 5的流量并将其导出到VRF 1。



将策略的Default Action更改为Accept。

点击Save Match and Actions，然后点击Save Control Policy。

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel

4. 将该策略应用于需要路由泄漏的站点。



点击拓扑选项卡在路由渗透策略下，选择入站站点列表上的新站点/区域列表。选择需要路由泄漏的站点列表。

要保存修改，请选择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

服务链

服务链也称为服务插入。它涉及网络服务的注入；标准服务包括防火墙(FW)、入侵检测系统(IDS)和入侵防御系统(IPS)。在这种情况下，防火墙服务会插入到数据路径中。

通过CLI配置

1. 在Cisco Catalyst SD-WAN控制器上配置列表。

该配置允许通过列表识别站点。

为每个VRF 1所在的站点创建一个列表。

在Transport Location (TLOC)列表中，指定流量必须重定向到哪个地址才能到达该服务。

```
<#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. 在Cisco Catalyst SD-WAN控制器上配置策略。

该序列过滤来自VRF 1的流量。流量在VRF 5上的服务防火墙上被允许和检查。

```
<#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. 在Cisco Catalyst SD-WAN控制器上应用策略。

在站点1和2中配置策略，以允许检查来自VRF 1的流量。

```
<#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
```

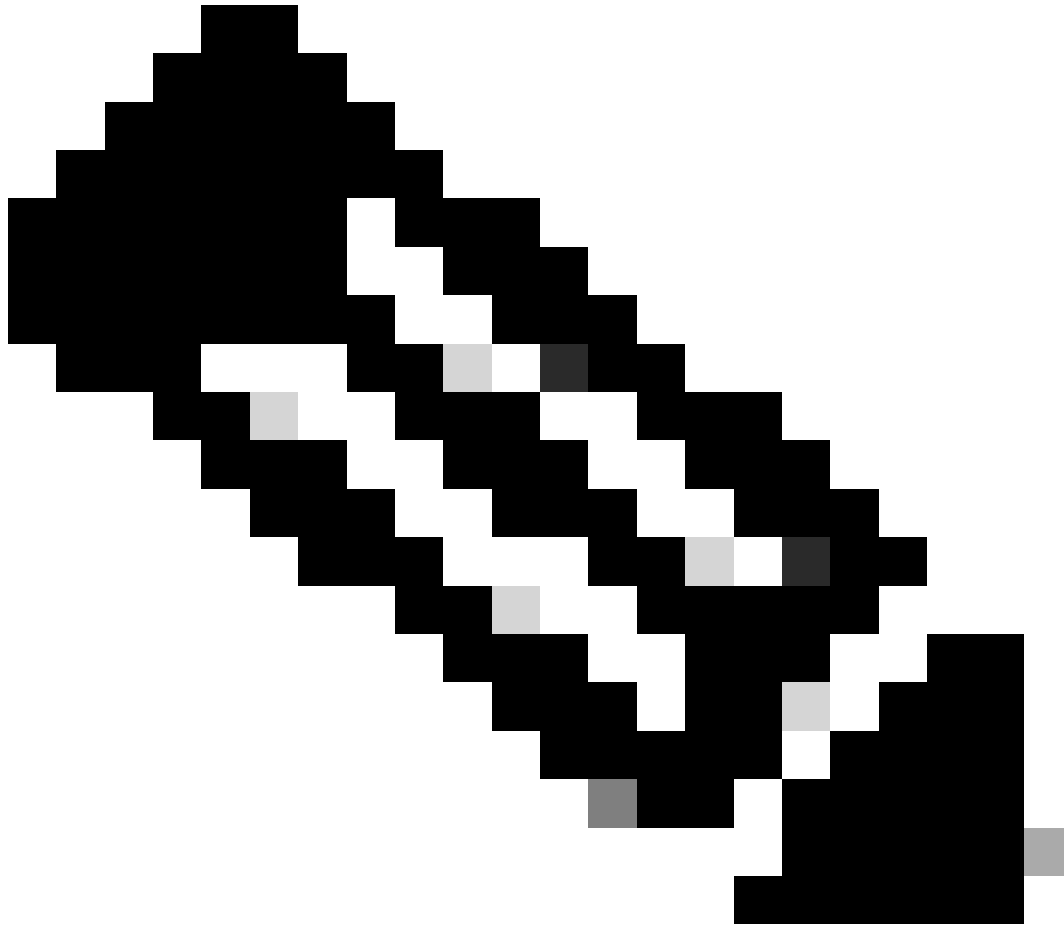
```
vSmart(config-site-list-cEdge-1)#
```

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

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

```
commit
```

通过模板进行配置



注意：要通过Cisco Catalyst SD-WAN Manager图形用户界面(GUI)激活策略，Cisco Catalyst SD-WAN控制器必须附加模板。

1. 在Cisco Catalyst SD-WAN Manager上创建策略。

导航到配置 >策略>集中策略。

在Centralized Policy选项卡下点击Add Policy。

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. 在Cisco Catalyst SD-WAN Manager上创建列表。

导航到站点>新建站点列表。

创建VRF 1所在的站点的站点列表，然后选择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

导航到TLOC > New TLOC List。

创建TLOC列表服务链接位于中，然后选择Save。

TLOC List

List Name *

TLOC IP*

Color*

 ▼

Encap*

 ▼

Preference

⊕ Add TLOC

Cancel

Save

3. 添加序列规则。

单击Topology选项卡，然后单击Add Topology。

创建自定义控件(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)

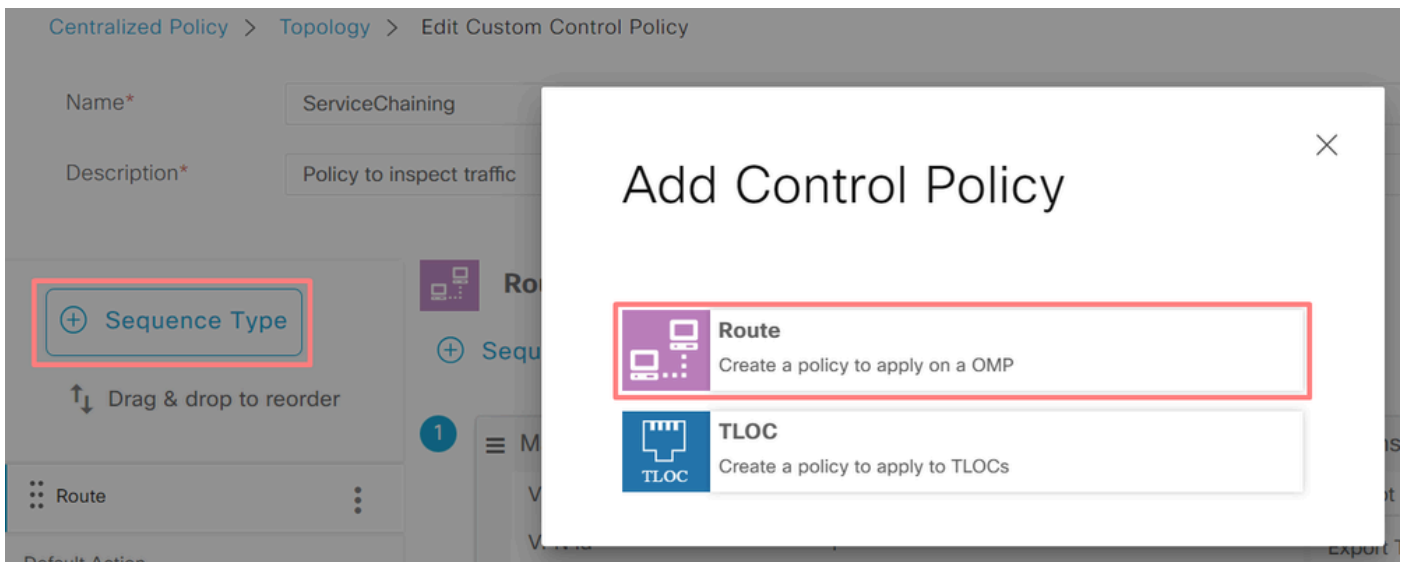
Import Existing Topology

Description

Mode

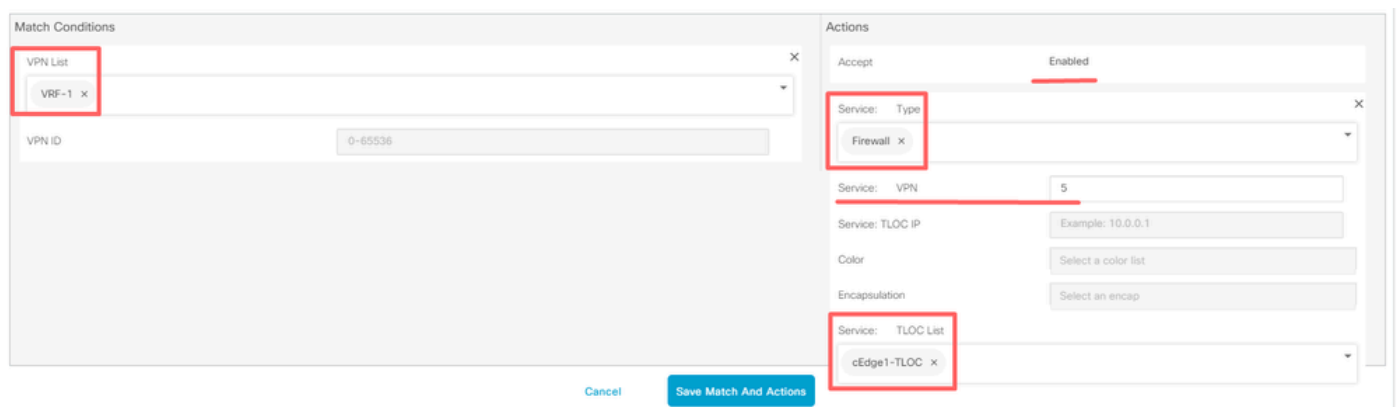
No data available

单击Sequence Type并选择Route sequence。



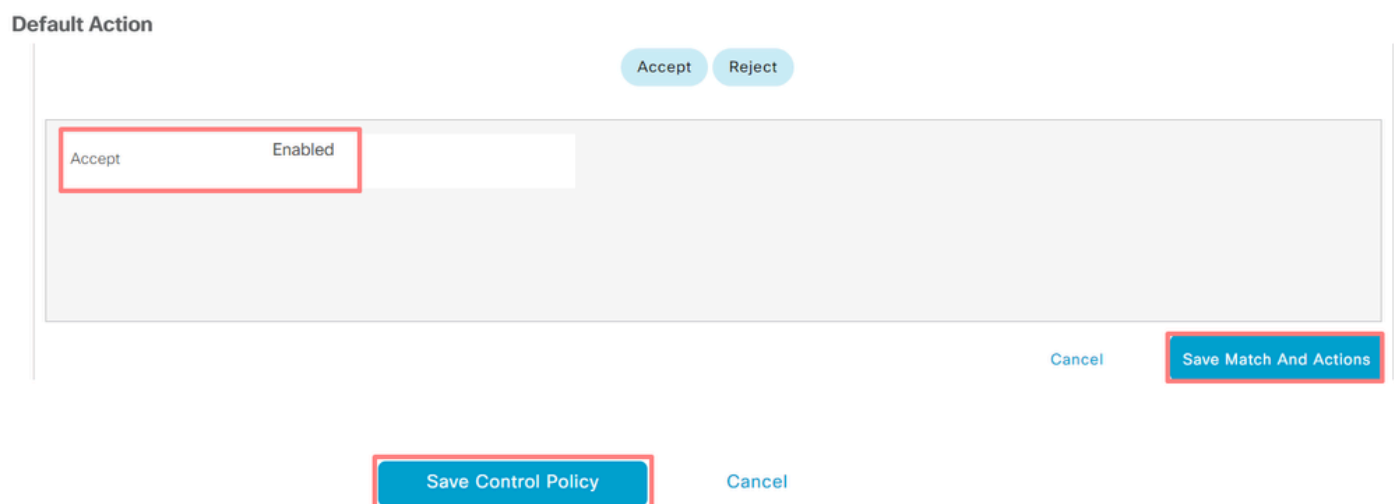
添加序列规则。

该序列过滤来自VRF 1的流量，允许其通过，然后将其重定向到VRF 5中的服务（防火墙）。这可以通过使用站点1（防火墙服务的位置）的TLOC来实现。



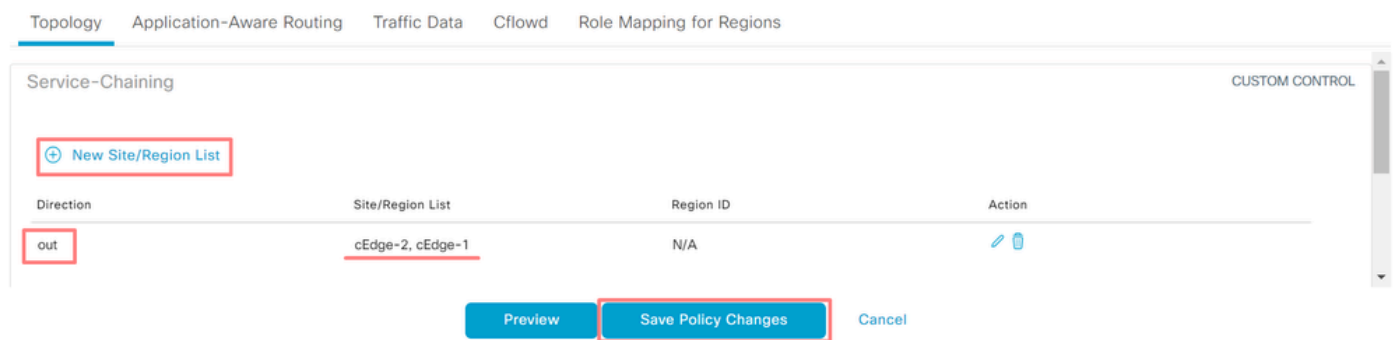
将策略的Default Action更改为Accept。

点击Save Match and Actions，然后点击Save Control Policy。



4. 应用策略。

点击拓扑选项卡在服务链策略下，在出站站点列表上选择新站点/区域列表。选择VRF 1流量必须检查的站点，然后单击Save Policy。保存修改，然后单击Save Policy Changes。



通告防火墙服务

通过CLI配置

要调配防火墙服务，请指定防火墙设备的IP地址。该服务通过OMP更新通告给Cisco Catalyst SD-WAN控制器。

```
<#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
```

通过模板进行配置

导航到VRF 5的功能模板。



继续执行Configuration > Templates > Feature Template > Add Template > Cisco VPN。

在服务部分下，单击新建服务。输入值，添加服务和保存模板。

SERVICE

New Service


Service Type

 FW 

IPv4 address

 192.168.15.2

Tracking

 On Off

验证

路由渗透

确认Cisco Catalyst SD-WAN控制器正在将路由从VRF 1导出到VRF 5，反之亦然。

<#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	192.168.16.1

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

确认云翼路由器已收到从VRF 1到VRF 5的泄漏路由。

确认云翼路由器已收到从VRF 5到VRF 1的泄漏路由。

```
<#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
```

服务链

验证云翼路由器是否已通过OMP服务路由将防火墙服务通告到Cisco Catalyst SD-WAN控制器。

```
<#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

确认Cisco Catalyst SD-WAN控制器已成功收到服务路由。

```
<#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	

要验证防火墙服务是否检查来自VRF 1的流量，请执行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
```

相关信息

- [服务链](#)
- [路由渗透](#)
- [SD-WAN -配置路由泄漏- YouTube](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。