

SD-WANでのサービスチェーンに対するルート漏出の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[背景説明](#)

[設定](#)

[ルート漏出](#)

[CLIを使用した設定](#)

[テンプレートを使用した設定](#)

[サービスチェーン](#)

[CLIを使用した設定](#)

[テンプレートを使用した設定](#)

[ファイアウォールサービスのアドバタイズ](#)

[CLIを使用した設定](#)

[テンプレートを使用した設定](#)

[確認](#)

[ルート漏出](#)

[サービスチェーン](#)

[関連情報](#)

はじめに

このドキュメントでは、異なるVRF間のトラフィックを検査するためにサービスチェーンを設定および確認する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- 制御ポリシー。
- テンプレート。

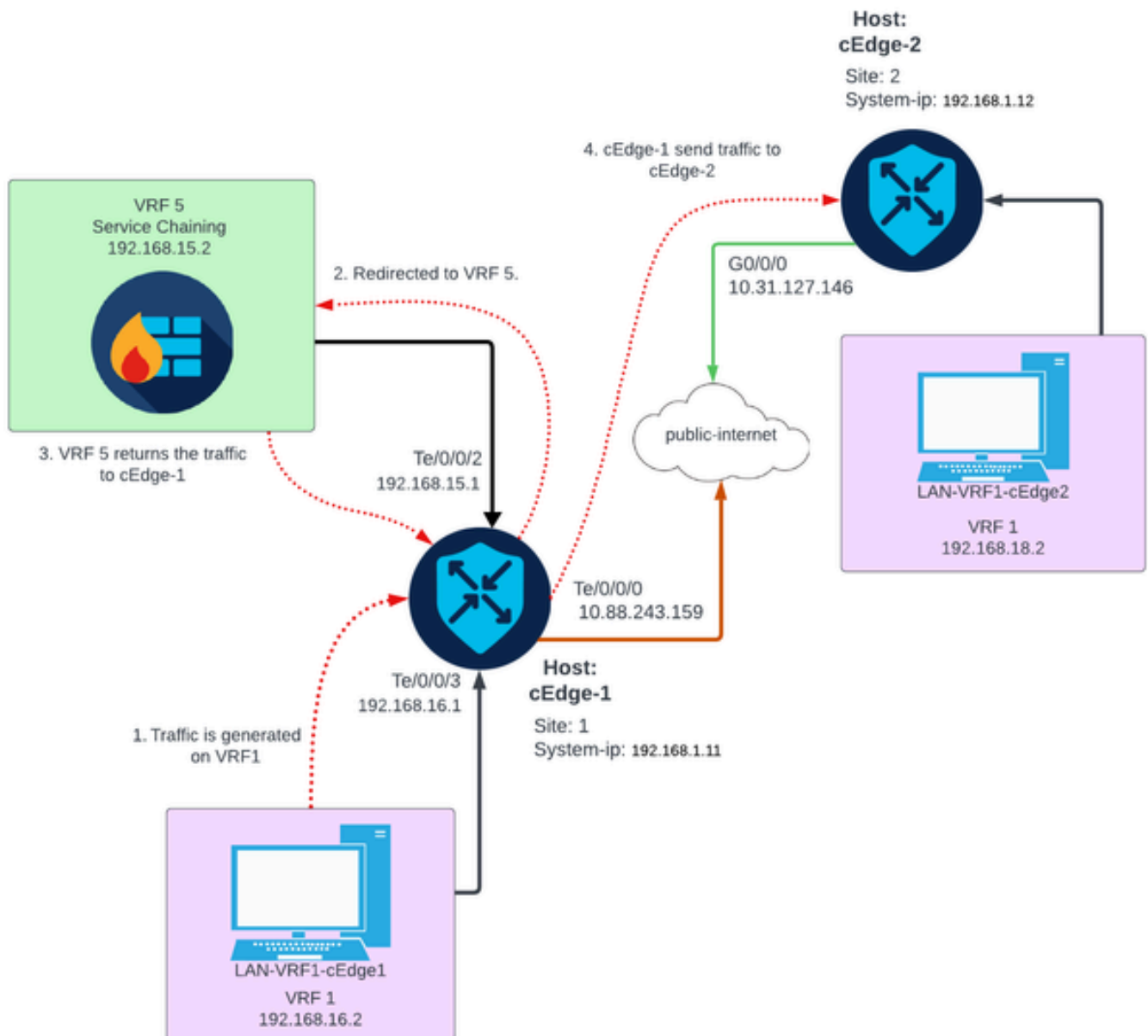
使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- SD-WANコントローラ(20.9.4.1)
- Ciscoエッジルータ(17.09.04)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図



背景説明

このネットワークダイアグラムでは、ファイアウォールサービスはVirtual Routing and

Forwarding(VRF)5内にあり、LANデバイスはVRF 1上にあります。トラフィックの転送と検査を実現できるように、ルートの情報をVRF間で共有する必要があります。サービスを介してトラフィックをルーティングするには、Cisco SD-WANコントローラ上に制御ポリシーを設定する必要があります。

設定

ルート漏出

ルート漏出により、異なるVRF間でのルーティング情報の伝搬が可能になります。このシナリオでは、サービスチェーン（ファイアウォール）とLANサービス側が異なるVRFにある場合、トラフィックの検査にルート漏出が必要になります。

LANサービス側とファイアウォールサービス間のルーティングを保証するには、両方のVRFでルートのリークが必要であり、ルートのリークが必要なサイトでポリシーを適用します。

CLIを使用した設定

1. Cisco Catalyst SD-WANコントローラでリストを設定します。

この設定では、リストを使用してサイトを特定できます。

```
<#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. Cisco Catalyst SD-WANコントローラでポリシーを設定します。

この設定では、VRF 1とVRF 5の間でルーティング情報を伝搬できるため、VRF間のルーティングが確実に行われ、両方のVRFでルーティングデータを共有する必要があります。

ポリシーは、VRF 1のトラフィックを許可してVRF 5にエクスポートし、またその逆も許可します。

```
<#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. Cisco Catalyst SD-WANコントローラにポリシーを適用します。

サイト1とサイト2にポリシーが適用され、これらのサイトにあるVRF 1とVRF 5の間のルーティングが許可されます。

ポリシーはインバウンドで実装されます。つまり、CiscoエッジルータからCisco Catalyst SD-WANコントローラへのOMPアップデートに適用されます。

```
<#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
```

テンプレートを使用した設定



注：Cisco Catalyst SD-WAN Manager Graphic User Interface(GUI)を介してポリシーをアクティブにするには、Cisco Catalyst SD-WAN Controllerにテンプレートが接続されている必要があります。

1. ルーティング情報の伝達を許可するポリシーを作成します。

Cisco Catalyst SD-WAN Managerでポリシーを作成し、Configuration > Policies > Centralized Policyの順に選択します。

Centralized PolicyタブでAdd Policyをクリックします。

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Cisco Catalyst SD-WAN Managerでリストを作成します。この設定では、リストを使用してサイトを特定できます。

Site > New Site Listの順に移動します。

ルート漏出が必要なサイトのリストを作成し、そのリストを追加します。

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

VPN > New VPN Listの順に移動します。

ルート漏出を適用する必要があるVPNリストを作成し、Nextをクリックします。

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

The screenshot shows the 'Add Policy' page with a sidebar on the left containing options: Prefix, Site, App Probe Class, SLA Class, TLOC, VPN (highlighted with a red box), Region, and Preferred Color Group. The main area is titled 'New VPN List' and contains two input fields: 'VPN List Name*' with a placeholder 'Name of the list' and 'Add VPN*' with a placeholder 'Example: 100 or 200 separated by commas or 1000-2000 by range'. At the bottom right, there are 'Add' and 'Cancel' buttons.

3. Cisco Catalyst SD-WAN Managerでポリシーを設定します。

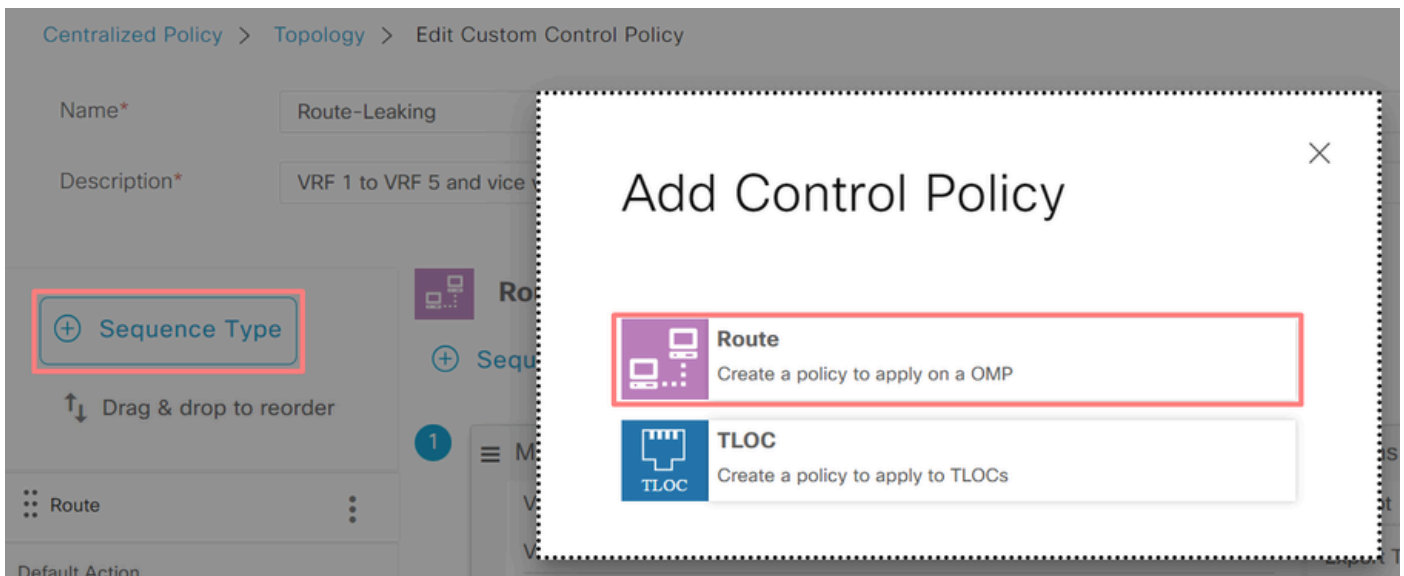
Topologytabをクリックし、Add Topologyをクリックします。

カスタムコントロール (ルートおよびTLOC) を作成します。

Search

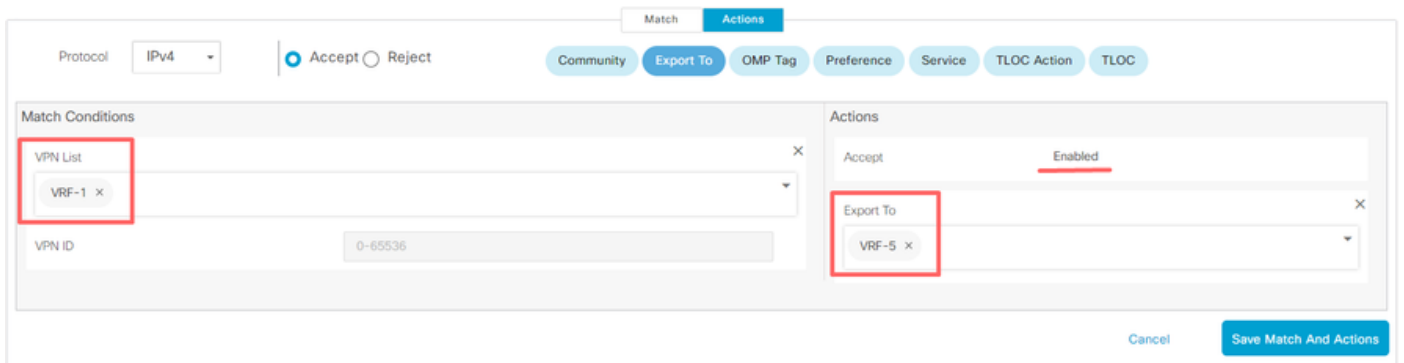
The screenshot shows the 'Add Topology' dropdown menu with options: Hub-and-Spoke, Mesh, Custom Control (Route & TLOC) (highlighted with a red box), and Import Existing Topology. Below the menu is a table with columns 'Description' and 'Mode', and the text 'No data available'.

Sequence Typeをクリックして、Route sequenceを選択します。

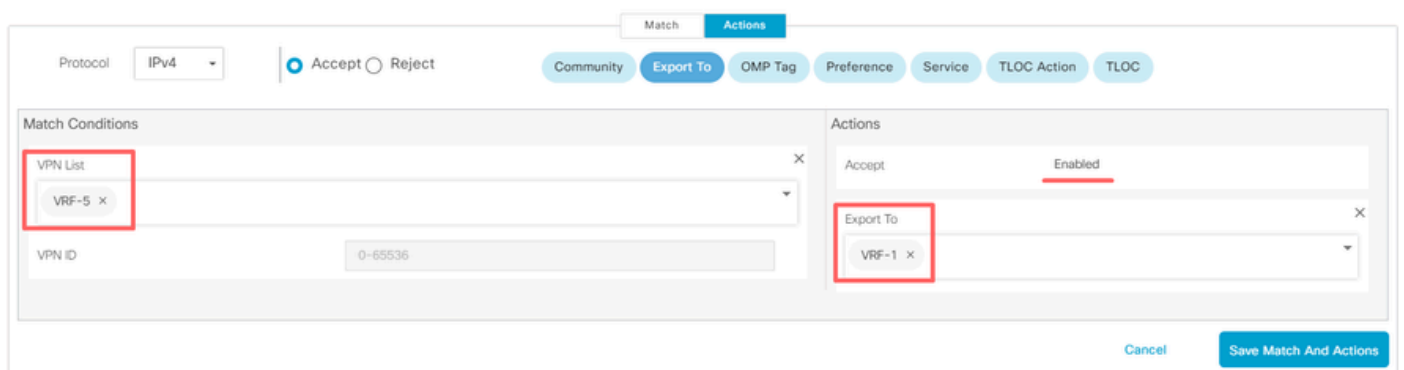


シーケンスルールを追加します。

条件1:VRF 1のトラフィックが受け入れられ、VRF 5にエクスポートされます。



条件2:VRF 5のトラフィックが受け入れられ、VRF 1にエクスポートされます。



ポリシーのデフォルトアクションをAcceptに変更します。

Save Match and Actionsをクリックし、次にSave Control Policyをクリックします。

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel

4. ルート漏出が必要なサイトにポリシーを適用します。



Topologyタブをクリックし、Route-Leaking Policyの下でNew Site/Region List on Inbound Site Listを選択します。ルート漏出が必要なサイトリストを選択します。

変更内容を保存するには、Save Policy Changesを選択します。

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

サービスチェーン

サービスチェーンは、サービス挿入とも呼ばれます。ネットワークサービスの注入が含まれます。標準サービスには、ファイアウォール(FW)、侵入検知システム(IDS)、および侵入防御システム(IPS)が含まれます。この場合、ファイアウォールサービスがデータパスに挿入されます。

CLIを使用した設定

1. Cisco Catalyst SD-WANコントローラでリストを設定します。

この設定では、リストを使用してサイトを特定できます。

各VRF 1が配置されているサイトのリストを作成します。

[トランスポートの場所(TLOC)]の一覧で、サービスに到達するためにトラフィックをリダイレクトする必要があるアドレスを指定します。

```
<#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. Cisco Catalyst SD-WANコントローラでポリシーを設定します。

このシーケンスにより、VRF 1からのトラフィックがフィルタリングされます。トラフィックは、VRF 5にあるサービスファイアウォールで許可され、検査されます。

```
<#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. Cisco Catalyst SD-WANコントローラにポリシーを適用します。

ポリシーは、VRF 1からのトラフィックの検査を許可するようにサイト1と2で設定されます。

```
<#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
```

テンプレートを使用した設定



注: Cisco Catalyst SD-WAN Manager Graphic User Interface(GUI)を介してポリシーをアクティブにするには、Cisco Catalyst SD-WAN Controllerにテンプレートが接続されている必要があります。

1. Cisco Catalyst SD-WAN Managerでポリシーを作成します。

Configuration > Policies > Centralized Policyの順に移動します。

Centralized PolicyタブでAdd Policyをクリックします。

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Cisco Catalyst SD-WAN Managerでリストを作成します。

Site > New Site Listの順に移動します。

VRF 1が配置されているサイトのサイトリストを作成し、Addを選択します。

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

TLOC > New TLOC Listの順に移動します。

TLOCリストサービスチェーンの作成場所を特定し、Saveを選択します。

TLOC List

List Name *

TLOC IP*

Color*

 ▼

Encap*

 ▼

Preference

⊕ Add TLOC

Cancel

Save

3. 順序ルールを追加します。

Topologyタブをクリックして、Add Topologyをクリックします。

カスタムコントロール（ルートおよびTLOC）を作成します。

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)

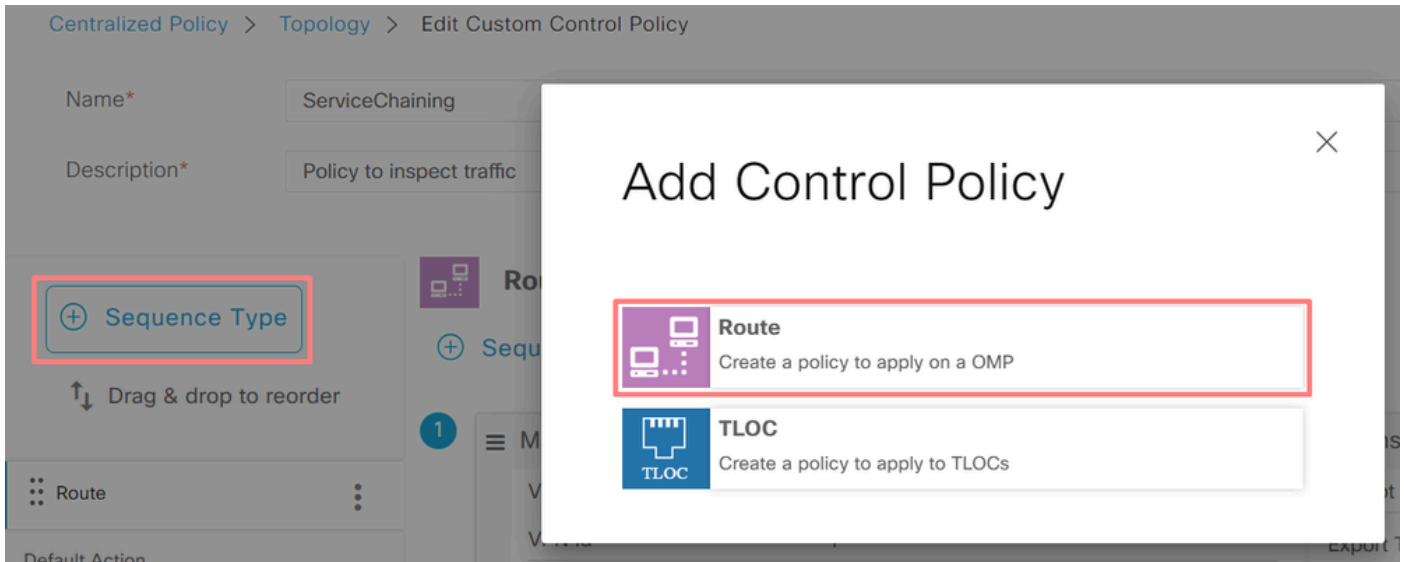
Import Existing Topology

Description

Mode

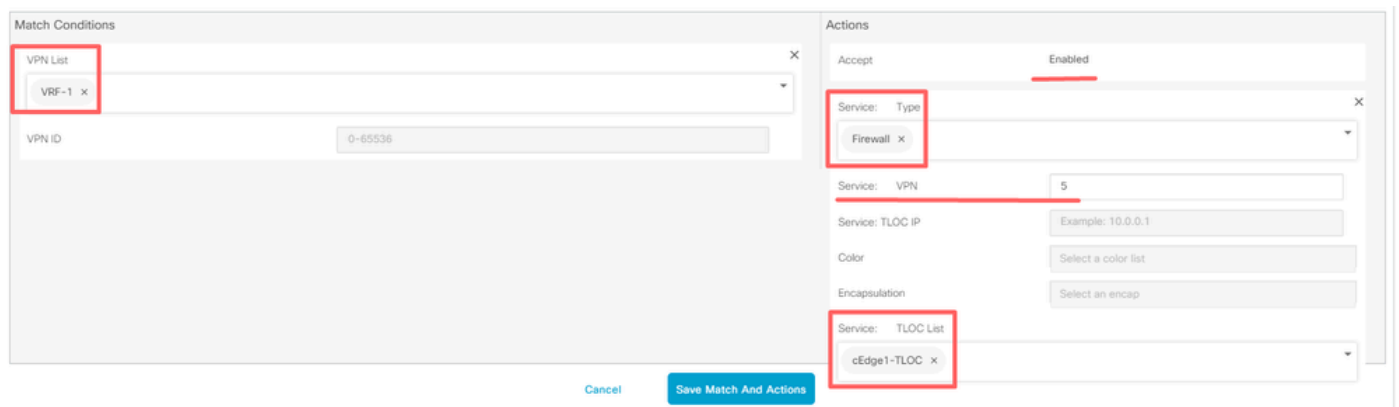
No data available

Sequence Typeをクリックして、Route sequenceを選択します。



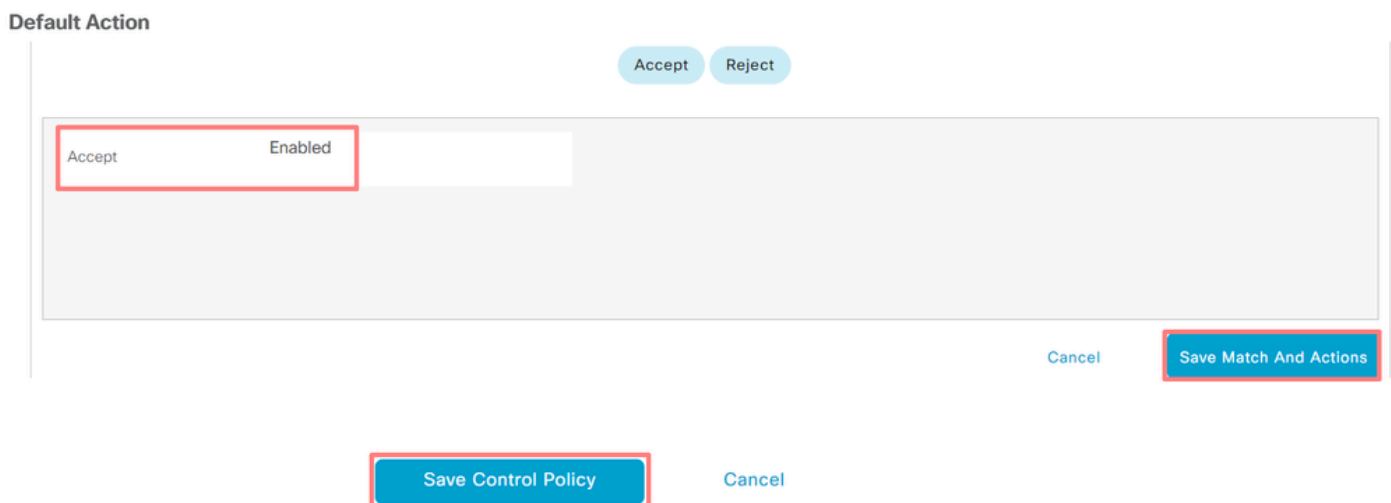
シーケンスルールを追加します。

このシーケンスは、VRF 1からのトラフィックをフィルタリングし、通過を許可してから、VRF 5内に存在するサービス (ファイアウォール) にリダイレクトします。これは、ファイアウォールサービスの場所であるサイト1のTLOCを使用して実現できます。



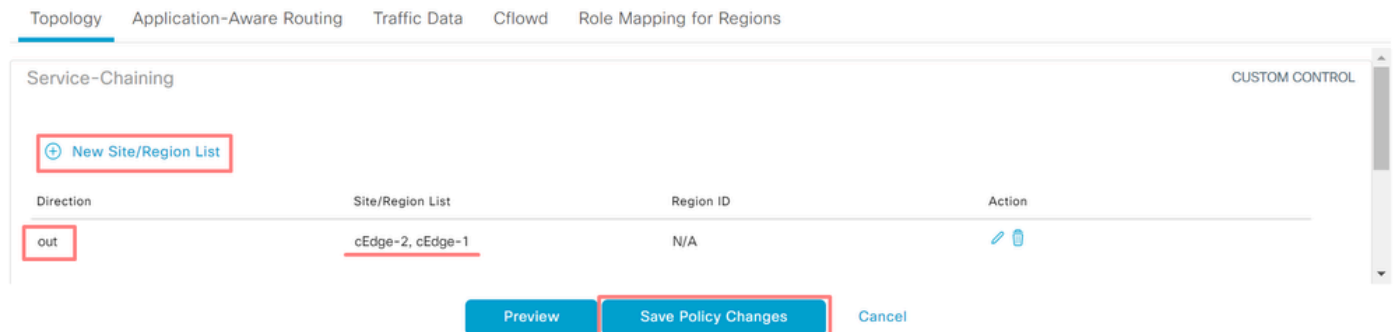
ポリシーのデフォルトアクションをAcceptに変更します。

Save Match and Actionsをクリックし、次にSave Control Policyをクリックします。



4. ポリシーを適用します。

Topologyタブをクリックし、Service-Chaining Policyの下でNew Site/Region List on Outbound Site Listを選択します。VRF 1トラフィックが検査する必要があるサイトを選択して、Save Policyをクリックします。変更を保存し、Save Policy Changesをクリックします。



ファイアウォールサービスのアドバタイズ

CLIを使用した設定

ファイアウォールサービスをプロビジョニングするには、ファイアウォールデバイスのIPアドレスを指定します。このサービスは、OMPアップデートを通じてCisco Catalyst SD-WANコントローラにアナウンスされます。

```
<#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
```

テンプレートを使用した設定

VRF 5の機能テンプレートに移動します。

Configuration > Templates > Feature Template > Add Template > Cisco VPNの順に進みます。

Service SectionでNew Serviceをクリックします。値を入力し、サービスを追加して、テンプレートを保存します。

New Service

Service Type	<div style="border: 1px solid #ccc; padding: 2px;"><div style="display: flex; align-items: center;"><div style="margin-right: 5px;"></div><div style="flex-grow: 1;">FW</div><div style="margin-left: 5px;">▼</div></div></div>
IPv4 address	<div style="border: 1px solid #ccc; padding: 2px;"><div style="display: flex; align-items: center;"><div style="margin-right: 5px;"></div><div style="flex-grow: 1;">192.168.15.2</div><div style="margin-left: 5px;">▼</div></div></div>
Tracking	<div style="display: flex; align-items: center;"><div style="margin-right: 10px;"><input checked="" type="checkbox"/> On</div><div><input type="checkbox"/> Off</div></div>

確認

ルート漏出

Cisco Catalyst SD-WANコントローラがVRF 1からVRF 5へ、およびその逆にルートをエクスポートしていることを確認します。

<#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.

Ciscoエッジルータが、VRF 1からVRF 5への漏出ルートを受信したことを確認します。

Ciscoエッジルータが、VRF 5からVRF 1への漏出ルートを受信したことを確認します。

<#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

```

サービスチェーン

Ciscoエッジルータが、OMPサービスルートを通じてCisco Catalyst SD-WANコントローラにファイアウォールサービスをアドバタイズしたことを確認します。

```
<#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

Cisco Catalyst SD-WANコントローラがサービスルートを正常に受信したことを確認します。

```
<#root>
```

```
vSmart#
```

```
show omp services
```

ADDRESS	TENANT	VPN	SERVICE	ORIGINATOR	FROM PEER	PATH	REGION	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			

ファイアウォールサービスがVRF 1からのトラフィックを検査していることを確認するには、tracertouteを実行します。

```
<#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
```

関連情報

- [サービスチェーン](#)
- [ルート漏出](#)
- [SD-WAN - ルート漏出の設定 - YouTube](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。