

SD-WAN에서 서비스 체이닝에 대한 경로 유출 구성

목차

- [소개](#)
- [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [네트워크 다이어그램](#)

배경 정보

- [구성](#)
 - [경로 유출](#)
 - [CLI를 통한 컨피그레이션](#)
 - [템플릿을 통한 컨피그레이션](#)
 - [서비스 체이닝](#)
 - [CLI를 통한 컨피그레이션](#)
 - [템플릿을 통한 컨피그레이션](#)
 - [방화벽 서비스 알림](#)
 - [CLI를 통한 컨피그레이션](#)
 - [템플릿을 통한 컨피그레이션](#)

[다음을 확인합니다.](#)

- [경로 유출](#)
- [서비스 체이닝](#)

관련 정보

소개

이 문서에서는 서로 다른 VRF에서 트래픽을 검사하도록 서비스 체이닝을 구성하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)
- 제어 정책.
- 템플릿.

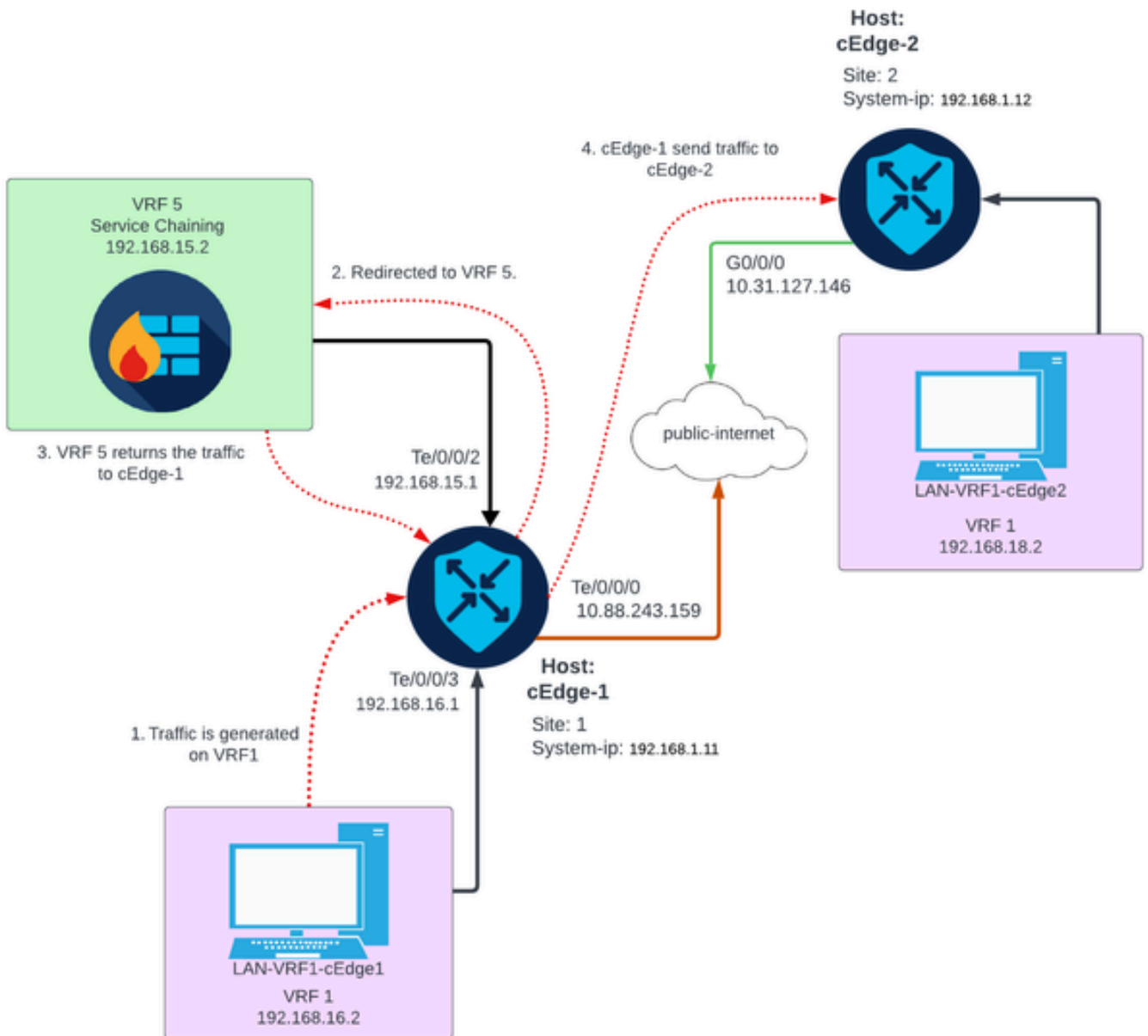
사용되는 구성 요소

이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램



배경 정보

네트워크 다이어그램에서 방화벽 서비스는 VRF(Virtual Routing and Forwarding) 5에 있고 LAN 디바이스는 VRF 1에 있습니다. 트래픽의 전달 및 검사를 수행할 수 있도록 VRF 간에 경로 정보를 공

유해야 합니다. 서비스를 통해 트래픽을 라우팅하려면 Cisco SD-WAN Controller에 대한 제어 정책을 구성해야 합니다.

구성

경로 유출

경로 유출을 통해 서로 다른 VRF 간에 라우팅 정보를 전파할 수 있습니다. 이 시나리오에서 서비스 체이닝(방화벽)과 LAN 서비스 측이 서로 다른 VRF에 있는 경우 트래픽 검사를 위해 경로 유출을 수행해야 합니다.

LAN 서비스 측과 방화벽 서비스 간의 라우팅을 보장하기 위해 두 VRF에서 모두 경로 유출이 필요하며, 경로 유출이 필요한 사이트에 정책을 적용합니다.

CLI를 통한 컨피그레이션

1. Cisco Catalyst SD-WAN 컨트롤러에 목록을 구성합니다.

이 컨피그레이션을 통해 목록을 통해 사이트를 식별할 수 있습니다.

```
<#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 컨트롤러에 대한 정책을 구성합니다.

이 컨피그레이션을 통해 VRF 1과 VRF 5 간의 라우팅 정보 전달이 가능하므로 두 VRF가 모두 라우팅 데이터를 공유해야 합니다.

정책은 VRF 1의 트래픽을 수락하고 VRF 5로 내보내거나 그 반대로 허용합니다.

```
<#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 컨트롤러에 정책을 적용합니다.

정책은 사이트 1과 사이트 2에 적용되어 해당 사이트에 있는 VRF 1과 VRF 5 간의 라우팅을 허용합니다.

정책은 인바운드에서 구현되며, 이는 Cisco Edge Router에서 Cisco Catalyst SD-WAN Controller로 전달되는 OMP 업데이트에 적용되는 것을 의미합니다.

```
<#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
```

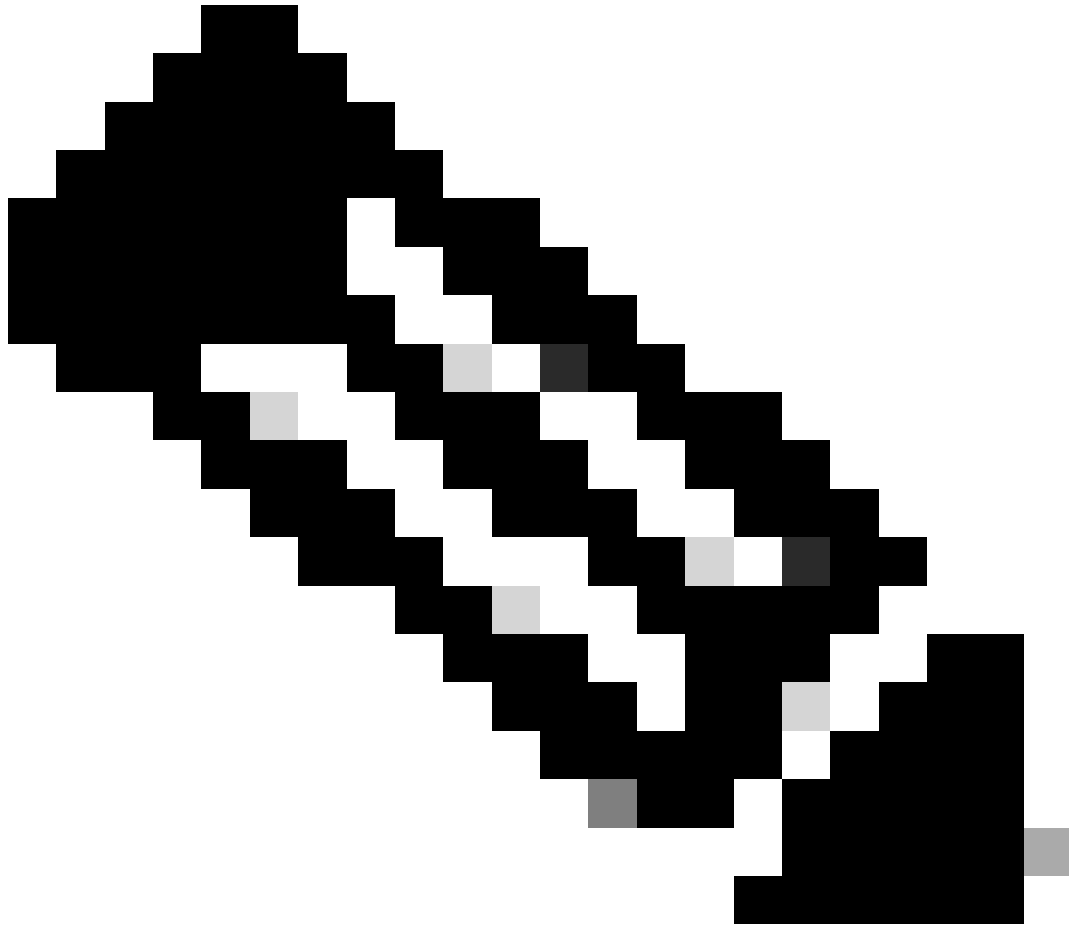
```
vSmart(config-site-list-cEdge-2)#
```

```
control-policy Route-Leaking in
```

```
vSmart(config-site-list-cEdge-2)#
```

```
commit
```

템플릿을 통한 컨피그레이션



참고: Cisco Catalyst SD-WAN Manager Graphic User Interface(GUI)를 통해 정책을 활성화하려면 Cisco Catalyst SD-WAN Controller에 템플릿이 연결되어 있어야 합니다.

1. 라우팅 정보 전파를 허용하는 정책을 생성합니다.

Cisco Catalyst SD-WAN Manager에서 정책을 생성하고 Configuration(컨피그레이션) > Policies(정책) > Centralized Policy(중앙 집중식 정책)로 이동합니다.

Centralized Policy(중앙 집중식 정책) 탭에서 Add Policy(정책 추가)를 클릭합니다.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Cisco Catalyst SD-WAN Manager에서 목록을 생성합니다. 이 구성을 통해 목록을 통해 사이트를 식별할 수 있습니다.

사이트 > 새 사이트 목록으로 이동합니다.

경로 유출이 필요한 사이트 목록을 만들고 목록을 추가합니다.

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(새 VPN 목록)로 이동합니다.

경로 누수를 적용해야 하는 VPN 목록을 생성하고 Next(다음)를 클릭합니다.

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. Cisco Catalyst SD-WAN Manager에서 정책을 구성합니다.

Topologytab(토폴로지 탭)을 클릭하고 Add Topology(토폴로지 추가)를 클릭합니다.

사용자 지정 컨트롤(경로 및 TLOC)을 만듭니다.

Search

Add Topology ▾

Hub-and-Spoke

Mesh

Custom Control (Route & TLOC)

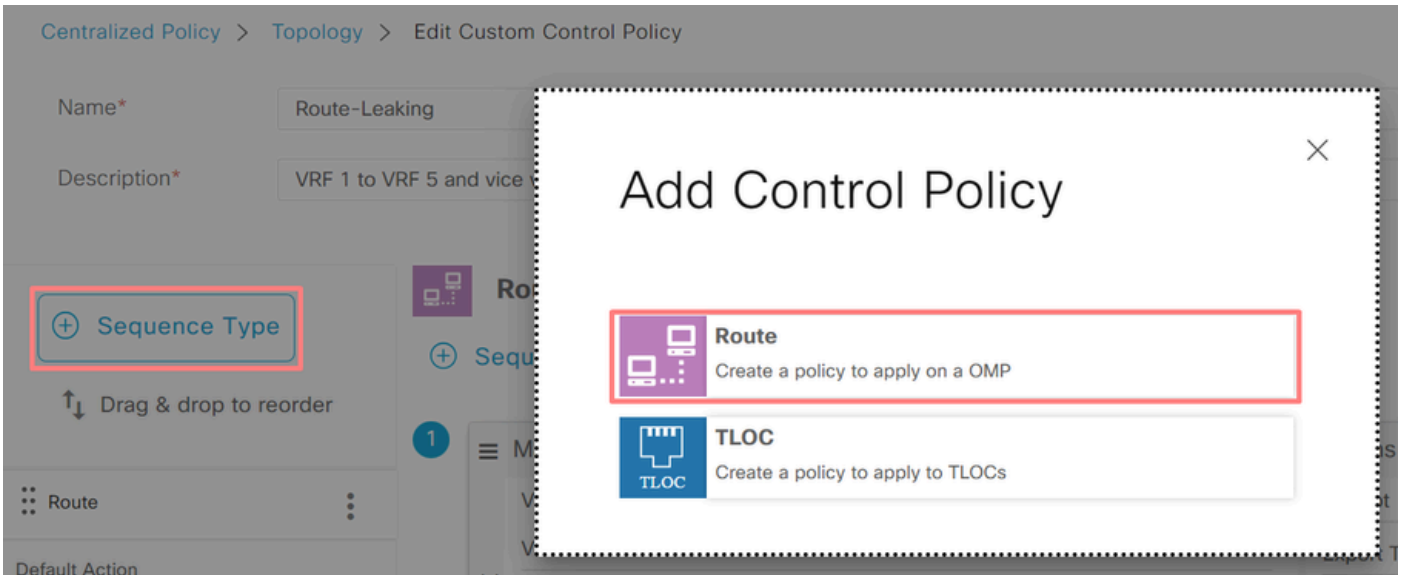
Import Existing Topology

Description

Mode

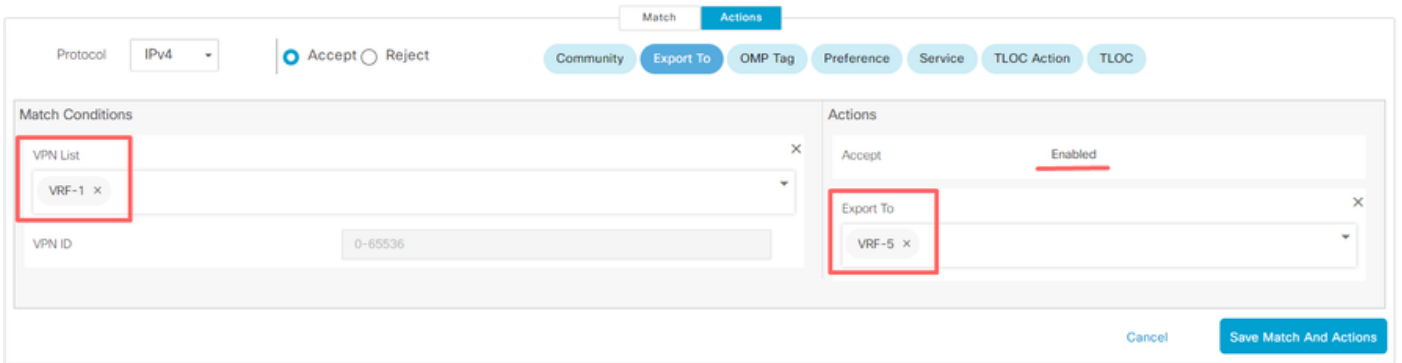
No data available

Sequence Type(시퀀스 유형)을 클릭하고 Route sequence(경로 시퀀스)를 선택합니다.

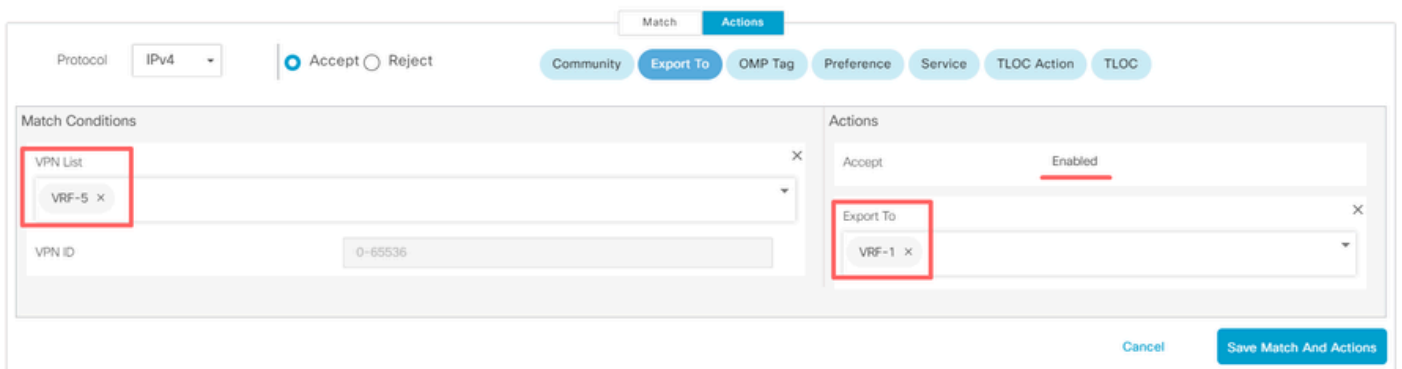


시퀀스 규칙을 추가합니다.

조건 1: VRF 1의 트래픽이 수락되고 VRF 5로 내보내집니다.



조건 2: VRF 5의 트래픽이 수락되고 VRF 1로 내보내집니다.



정책의 Default Action(기본 작업)을 Accept(수락)로 변경합니다.

Save Match and Actions(일치 및 작업 저장)를 클릭한 다음 Save Control Policy(제어 정책 저장)를 클릭합니다.

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel

4. 경로 유출이 필요한 사이트에 대한 정책을 적용할 것



Topology(토폴로지) 탭을 클릭하고 Route-Leaking Policy(경로 유출 정책) 아래에서 Inbound Site List(인바운드 사이트 목록)에서 New Site/Region List(새 사이트/지역 목록)를 선택합니다. 경로 유출이 필요한 사이트 목록을 선택합니다.

수정 사항을 저장하려면 Save Policy Changes(정책 변경 사항 저장)를 선택합니다.

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

서비스 체이닝

서비스 체이닝은 서비스 삽입이라고도 합니다. 여기에는 네트워크 서비스의 삽입이 포함됩니다. 표준 서비스에는 방화벽(FW), IDS(Intrusion Detection System), IPS(Intrusion Prevention System)가 포함됩니다. 이 경우 데이터 경로에 방화벽 서비스가 삽입됩니다.

CLI를 통한 컨피그레이션

1. Cisco Catalyst SD-WAN Controller에서 목록을 구성합니다.

이 컨피그레이션을 통해 목록을 통해 사이트를 식별할 수 있습니다.

각 VRF 1이 있는 사이트의 목록을 생성합니다.

TLOC(Transport Location) 목록에서 서비스에 도달하기 위해 트래픽을 리디렉션해야 하는 주소를 지정합니다.

<#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 컨트롤러에 대한 정책을 구성합니다.

이 시퀀스는 VRF 1에서 트래픽을 필터링합니다. 트래픽은 VRF 5에 위치한 서비스 방화벽에서 허용되고 검사됩니다.

```
<#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 컨트롤러에 정책을 적용합니다.

VRF 1의 트래픽을 검사하도록 사이트 1과 2에 정책이 구성됩니다.

<#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
```

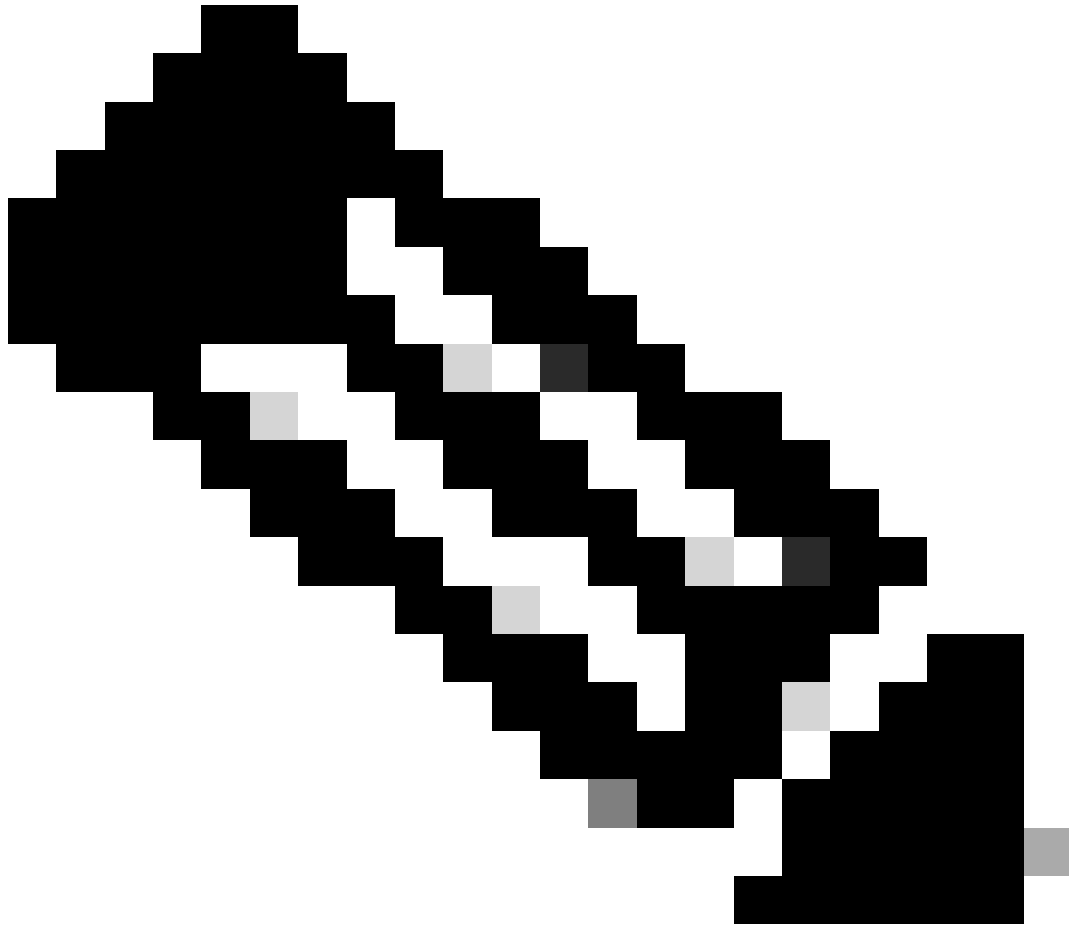
```
vSmart(config-site-list-cEdge-1)#
```

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

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

```
commit
```

템플릿을 통한 컨피그레이션



참고: Cisco Catalyst SD-WAN Manager GUI(Graphic User Interface)를 통해 정책을 활성화하려면 Cisco Catalyst SD-WAN Controller에 템플릿이 연결되어 있어야 합니다.

1. Cisco Catalyst SD-WAN Manager에서 정책을 생성합니다.

Configuration(컨피그레이션) > Policies(정책) > Centralized Policy(중앙 집중식 정책)로 이동합니다

Centralized Policy(중앙 집중식 정책) 탭에서 Add Policy(정책 추가)를 클릭합니다.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Cisco Catalyst SD-WAN Manager에서 목록을 생성합니다.

Site(사이트) > New Site List(새 사이트 목록)로 이동합니다.

VRF 1이 있는 사이트의 사이트 목록을 생성하고 Add(추가)를 선택합니다.

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(새 TLOC 목록)로 이동합니다.

에 있는 TLOC 목록 서비스 체인을 생성하고 저장을 선택합니다.

TLOC List

List Name *

TLOC IP*

Color*

Encap*

Preference

+ Add TLOC

Cancel

Save

3. 순번 규칙을 추가합니다.

Topology(토폴로지) 탭을 클릭하고 Add Topology(토폴로지 추가)를 클릭합니다.

사용자 지정 컨트롤(경로 및 TLOC)을 만듭니다.

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)

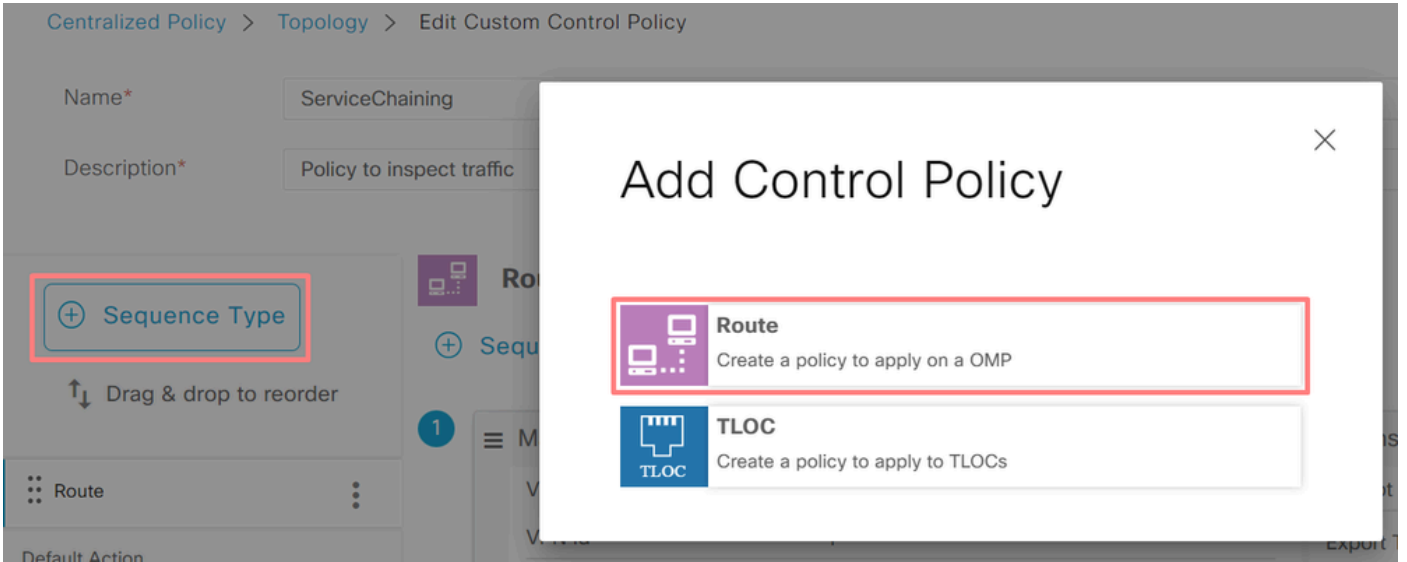
Import Existing Topology

Description

Mode

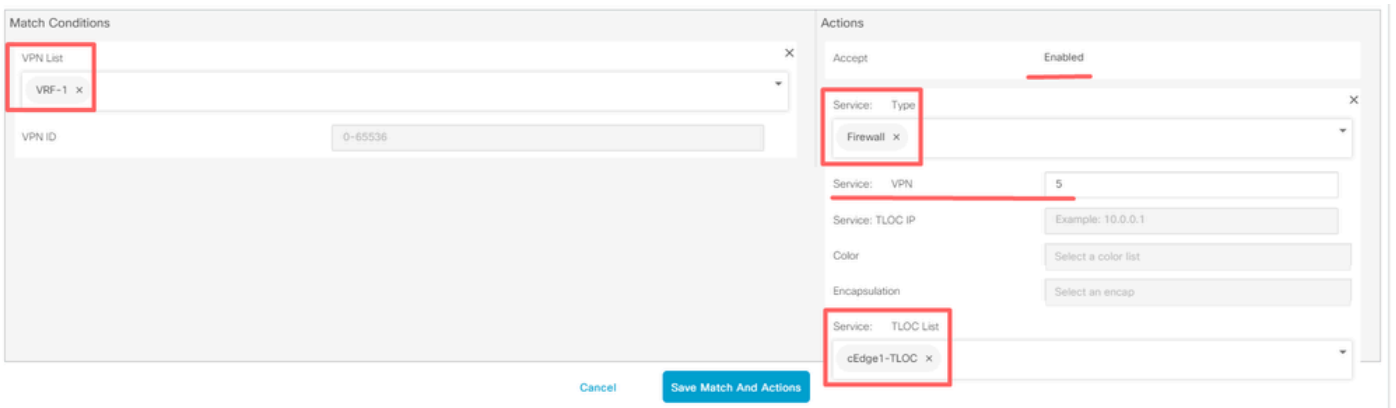
No data available

Sequence Type(시퀀스 유형)을 클릭하고 Route sequence(경로 시퀀스)를 선택합니다.



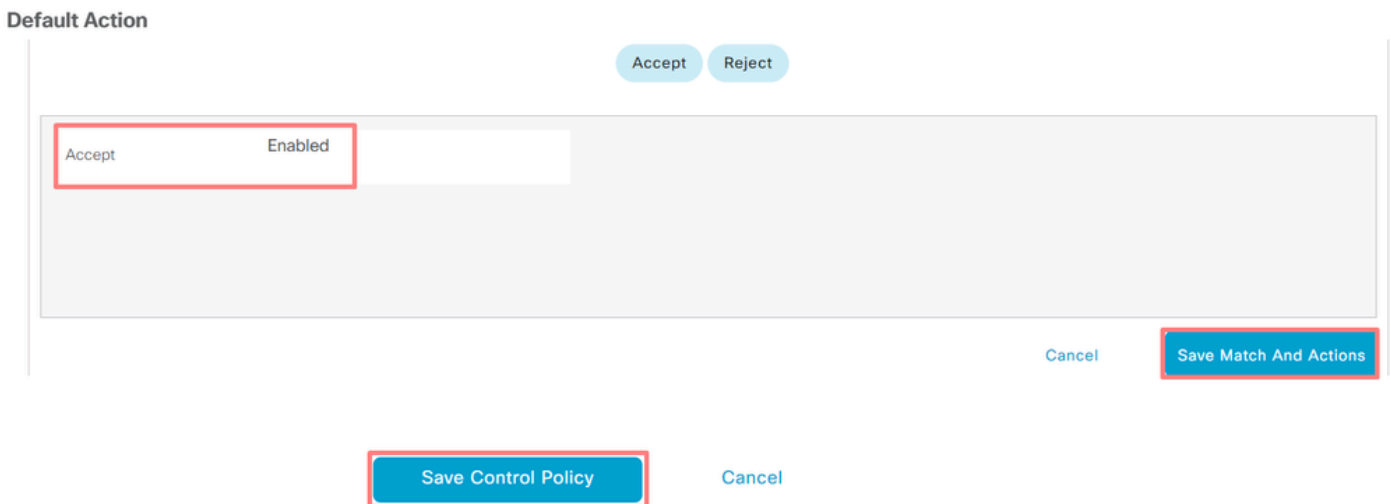
시퀀스 규칙을 추가합니다.

이 시퀀스는 VRF 1에서 트래픽을 필터링하여 통과시킨 다음 VRF 5 내에 있는 서비스(방화벽)로 리디렉션합니다. 이는 방화벽 서비스의 위치인 사이트 1의 TLOC를 사용하여 달성할 수 있습니다.



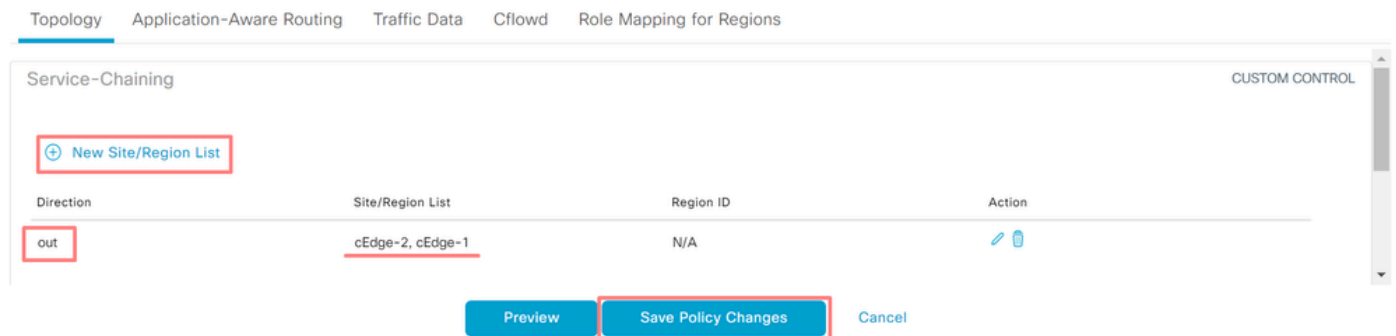
정책의 Default Action(기본 작업)을 Accept(수락)로 변경합니다.

Save Match and Actions(일치 및 작업 저장)를 클릭한 다음 Save Control Policy(제어 정책 저장)를 클릭합니다.



4. 정책을 적용합니다.

Topology(토폴로지) 탭을 클릭하고 Service-Chaining Policy(서비스 체이닝 정책) 아래에서 Outbound Site List(아웃바운드 사이트 목록)에서 New Site/Region List(새 사이트/지역 목록)를 선택합니다. VRF 1 트래픽이 검사해야 하는 사이트를 선택한 다음 Save Policy(정책 저장)를 클릭합니다. 수정 사항을 저장하고 Save Policy Changes(정책 변경 사항 저장)를 클릭합니다.



방화벽 서비스 알림

CLI를 통한 컨피그레이션

방화벽 서비스를 프로비저닝하려면 방화벽 디바이스의 IP 주소를 지정합니다. 이 서비스는 OMP 업데이트를 통해 Cisco Catalyst SD-WAN 컨트롤러에 공지됩니다.

```
<#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
```

템플릿을 통한 컨피그레이션

VRF 5의 Feature 템플릿으로 이동합니다.

Configuration(컨피그레이션) > Templates(템플릿) > Feature Template(기능 템플릿) > Add Template(템플릿 추가) > Cisco VPN으로 이동합니다.

Service Section(서비스 섹션)에서 New Service(새 서비스)를 클릭합니다. 값을 입력하고 Add the Service(서비스 추가)를 선택한 후 템플릿을 저장합니다.

▼ SERVICE

New Service

Service Type

IPv4 address

Tracking

🌐 FW ▼

🌐 192.168.15.2

🕒 On Off

다음을 확인합니다.

경로 유출

Cisco Catalyst SD-WAN Controller가 VRF 1에서 VRF 5로 경로를 내보내고 그 반대로도 경로를 내보내는지 확인합니다.

<#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.

Cisco Edge Router가 VRF 1에서 VRF 5로 유출된 경로를 수신했는지 확인합니다.

Cisco Edge Router가 VRF 5에서 VRF 1로의 누출 경로를 수신했는지 확인합니다.

<#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

```

서비스 체이닝

Cisco Edge Router가 OMP 서비스 경로를 통해 방화벽 서비스를 Cisco Catalyst SD-WAN Controller에 알렸는지 확인합니다.

```
<#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 컨트롤러가 성공적으로 서비스 경로를 수신했는지 확인합니다.

```
<#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			

방화벽 서비스가 VRF 1에서 트래픽을 검사하는지 확인하려면 traceroute를 수행합니다.

```
<#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
```

관련 정보

- [서비스 체이닝](#)
- [경로 유출](#)
- [SD-WAN - 경로 유출 구성 - YouTube](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.