

Configurazione della perdita di route per il concatenamento dei servizi in SD-WAN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Premesse](#)

[Configurazione](#)

[Perdite](#)

[Configurazione tramite CLI](#)

[Configurazione tramite modello](#)

[Concatenamento dei servizi](#)

[Configurazione tramite CLI](#)

[Configurazione tramite modello](#)

[Annuncia servizio firewall](#)

[Configurazione tramite CLI](#)

[Configurazione tramite modello](#)

[Verifica](#)

[Perdite](#)

[Concatenamento dei servizi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e verificare il concatenamento dei servizi per ispezionare il traffico tra diversi VRF.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- Criteri di controllo.
- Modelli.

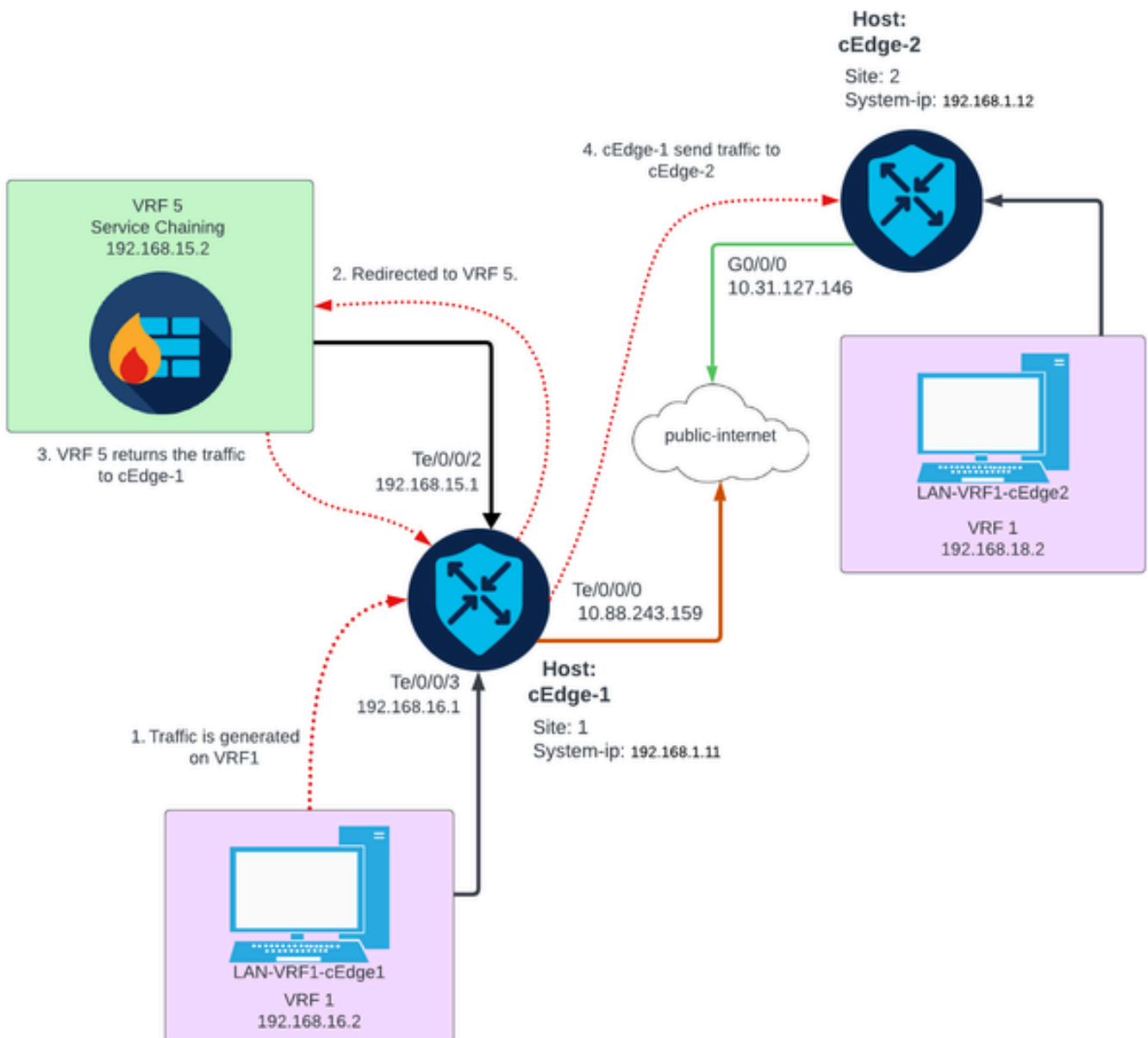
Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete



Premesse

Nel diagramma di rete il servizio firewall è in VRF (Virtual Routing and Forwarding) 5, mentre i

dispositivi LAN sono in VRF 1. Le informazioni relative ai percorsi devono essere condivise tra i VRF in modo da consentire l'inoltro e l'ispezione del traffico. Per instradare il traffico attraverso un servizio, è necessario configurare una policy di controllo sul controller Cisco SD-WAN.

Configurazione

Perdite

La perdita di route consente la propagazione delle informazioni di routing tra VRF diversi. In questo scenario, quando il concatenamento dei servizi (firewall) e il lato del servizio LAN si trovano in VRF diverse, la perdita di percorso è necessaria per l'ispezione del traffico.

Per garantire il routing tra il servizio LAN e il servizio firewall, è necessaria una perdita di route in entrambi i VRF e applicare una policy nei siti in cui è richiesta una perdita di route.

Configurazione tramite CLI

1. Configurare gli elenchi sul controller Cisco Catalyst SD-WAN.

La configurazione consente di identificare i siti tramite un elenco.

```
<#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. Configurare i criteri sul controller Cisco Catalyst SD-WAN.

La configurazione consente la propagazione delle informazioni di routing tra VRF 1 e VRF 5. Per garantire il routing tra di esse, entrambi i VRF devono condividere i dati di routing.

Le regole consentono l'accettazione e l'esportazione del traffico del VRF 1 nel VRF 5 e 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. Applicare la policy sul controller Cisco Catalyst SD-WAN.

La policy viene applicata nel sito 1 e nel sito 2 per consentire il routing tra il VRF 1 situato in tali siti e il VRF 5.

Il criterio viene implementato in entrata, ovvero applicato agli aggiornamenti OMP provenienti dai router perimetrali Cisco al controller SD-WAN Cisco Catalyst.

```
<#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
```

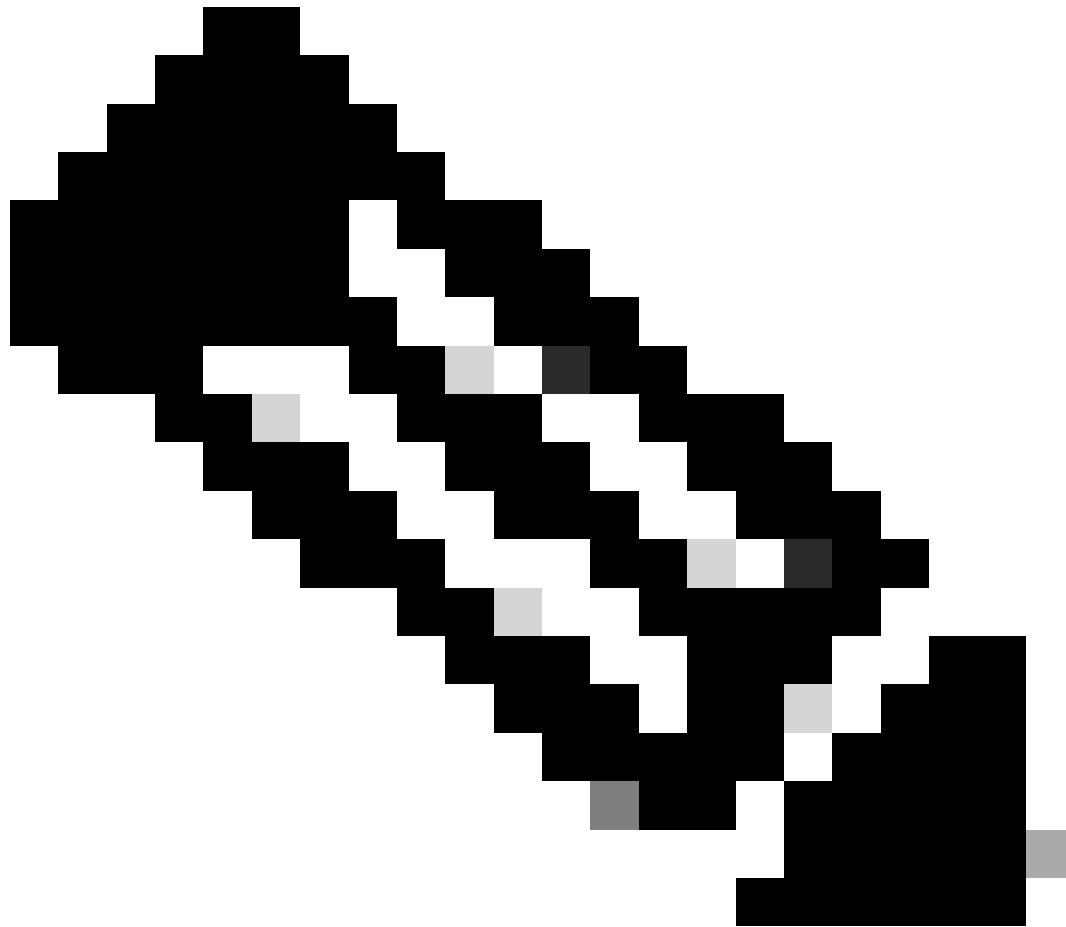
```
vSmart(config-site-list-cEdge-2)#
```

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

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

```
commit
```

Configurazione tramite modello



Nota: per attivare la policy tramite l'interfaccia grafica utente (GUI) di Cisco Catalyst SD-WAN Manager, è necessario associare un modello al controller Cisco Catalyst SD-WAN.

1. Creare il criterio per consentire la propagazione delle informazioni di routing.

Creare la policy sul Cisco Catalyst SD-WAN Manager, selezionare Configuration > Policies > Centralized Policy (Configurazione > Criteri > Criterio centralizzato).

In Scheda Criteri centralizzati fare clic su Aggiungi criterio.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Per creare elenchi sul Cisco Catalyst SD-WAN Manager, la configurazione consente di identificare i siti tramite un elenco.

Passare a Sito > Nuovo elenco siti.

Creare l'elenco dei siti in cui sono necessarie perdite di route e aggiungere l'elenco.

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

Passare a VPN > Nuovo elenco VPN.

Creare l'elenco VPN in cui è necessario applicare le perdite di route, quindi fare clic su Next (Avanti).

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. Configurare la policy sul Cisco Catalyst SD-WAN Manager.

Fare clic sulla scheda Topologia e selezionare Aggiungi topologia.

Creare un controllo personalizzato (Route & TLOC).

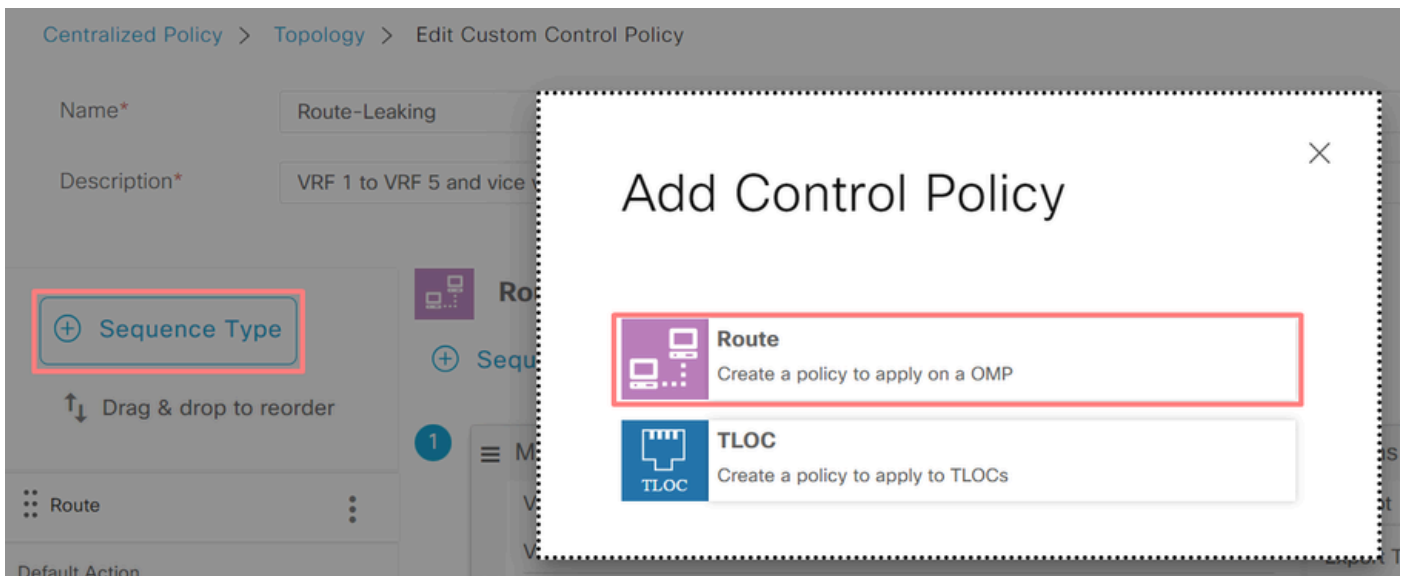
Search

Add Topology ▾

- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)**
- Import Existing Topology

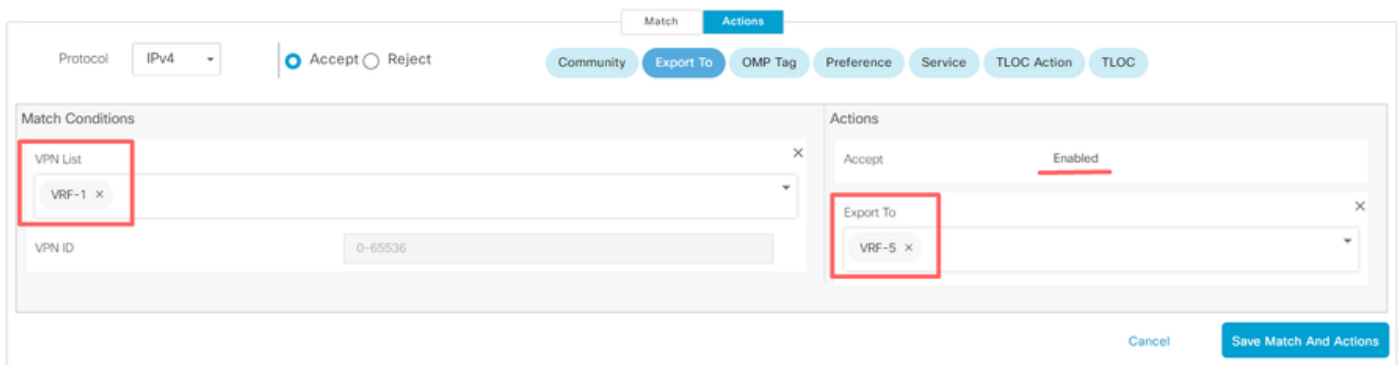
Description	Mode
No data available	

Fate clic su Tipo sequenza (Sequence Type) e selezionate Sequenza stesura (Route Sequence).

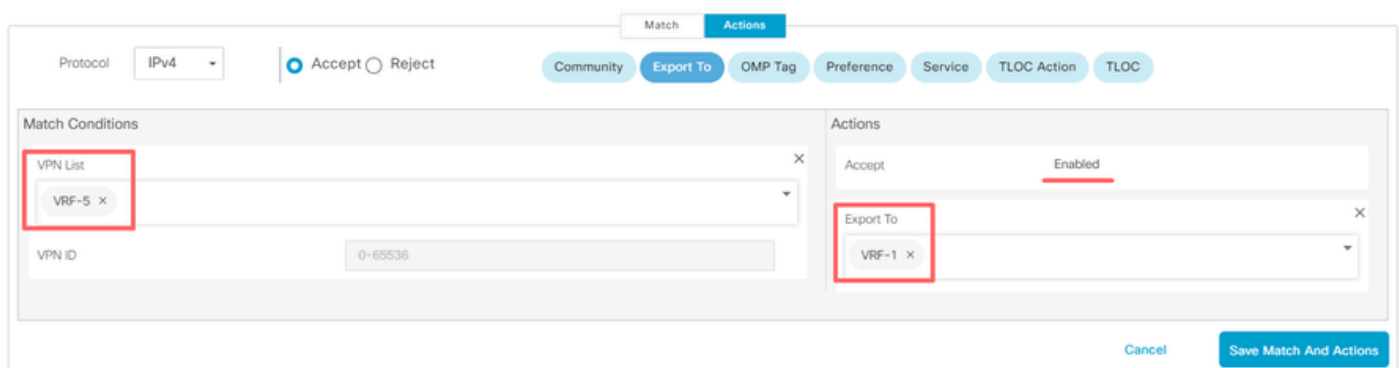


Aggiungere una regola di sequenza.

Condizione 1: il traffico del VRF 1 viene accettato ed esportato nel VRF 5.



Condizione 2: il traffico del VRF 5 viene accettato ed esportato nel VRF 1.



Modificare l'azione predefinita del criterio in Accetta.

Fare clic su Salva corrispondenza e azioni e quindi su Salva criteri di controllo.

Default Action

Accept Reject

Accept Enabled

Cancel Save Match And Actions

Save Control Policy Cancel



4. Applicare i criteri nei siti in cui sono necessarie perdite di percorso.

Fare clic sulla scheda Topologia, in Criterio di perdita dei percorsi selezionare Nuovo elenco sito/area in Elenco siti in ingresso. Selezionare gli elenchi dei siti in cui sono necessarie perdite di route.

Per salvare le modifiche, selezionare Salva modifiche criteri.

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

Concatenamento dei servizi

Il concatenamento dei servizi è noto anche come inserimento di servizi. Prevede l'inserimento di un servizio di rete; i servizi standard includono Firewall (FW), Intrusion Detection System (IDS) e Intrusion Prevention System (IPS). In questo caso, nel percorso dati viene inserito un servizio Firewall.

Configurazione tramite CLI

1. Configurare gli elenchi sul controller Cisco Catalyst SD-WAN.

La configurazione consente di identificare i siti tramite un elenco.

Creare un elenco per i siti in cui si trova ogni VRF 1.

Nell'elenco Percorso di trasporto (TLOC) specificare l'indirizzo a cui deve essere reindirizzato il traffico per raggiungere il servizio.

```
<#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 encap ipsec

vSmart(config-tloc-list-cEdge-1-TLOC)#
  commit
```

2. Configurare i criteri sul controller Cisco Catalyst SD-WAN.

La sequenza filtra il traffico dal VRF 1. Il traffico è autorizzato e ispezionato su un firewall del servizio situato su 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
```

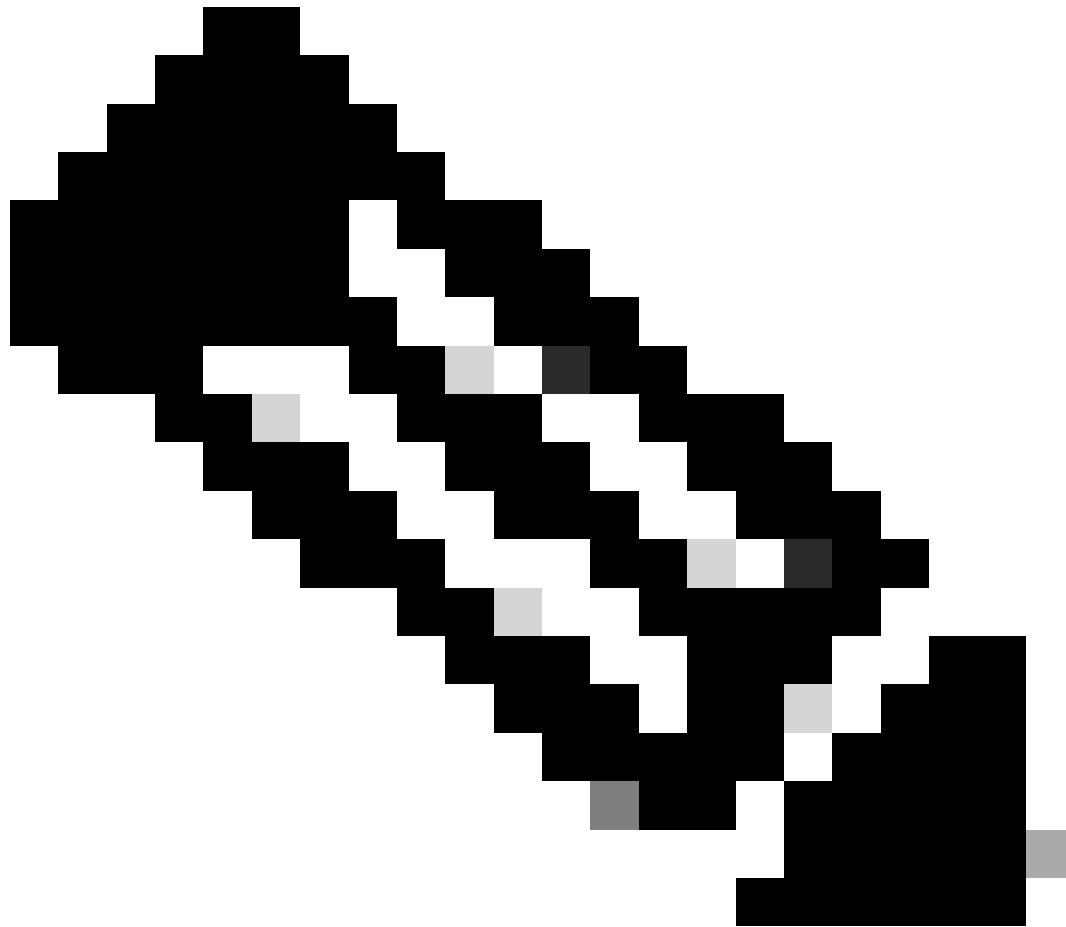
3. Applicare la policy sul controller Cisco Catalyst SD-WAN.

Il criterio è configurato nei siti 1 e 2 per consentire l'ispezione del traffico proveniente dal 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
```

Configurazione tramite modello



Nota: per attivare la policy tramite l'interfaccia grafica utente (GUI) di Cisco Catalyst SD-WAN Manager, è necessario associare un modello al controller Cisco Catalyst SD-WAN.

1. Creare la policy sul Cisco Catalyst SD-WAN Manager.

Passare a Configurazione > Criteri > Criterio centralizzato.

In scheda Criteri centralizzati fare clic su Aggiungi criterio.

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. Creare elenchi sul Cisco Catalyst SD-WAN Manager.

Passare a Sito > Nuovo elenco siti.

Creare l'elenco dei siti in cui si trova VRF 1 e selezionare Aggiungi.

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

Passate a TLOC > Nuovo elenco TLOC.

Creare il concatenamento del servizio elenco TLOC su e selezionare Salva.



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. Aggiungere le regole di sequenza.

Fare clic sulla scheda Topologia e selezionare Aggiungi topologia.

Creare un controllo personalizzato (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)

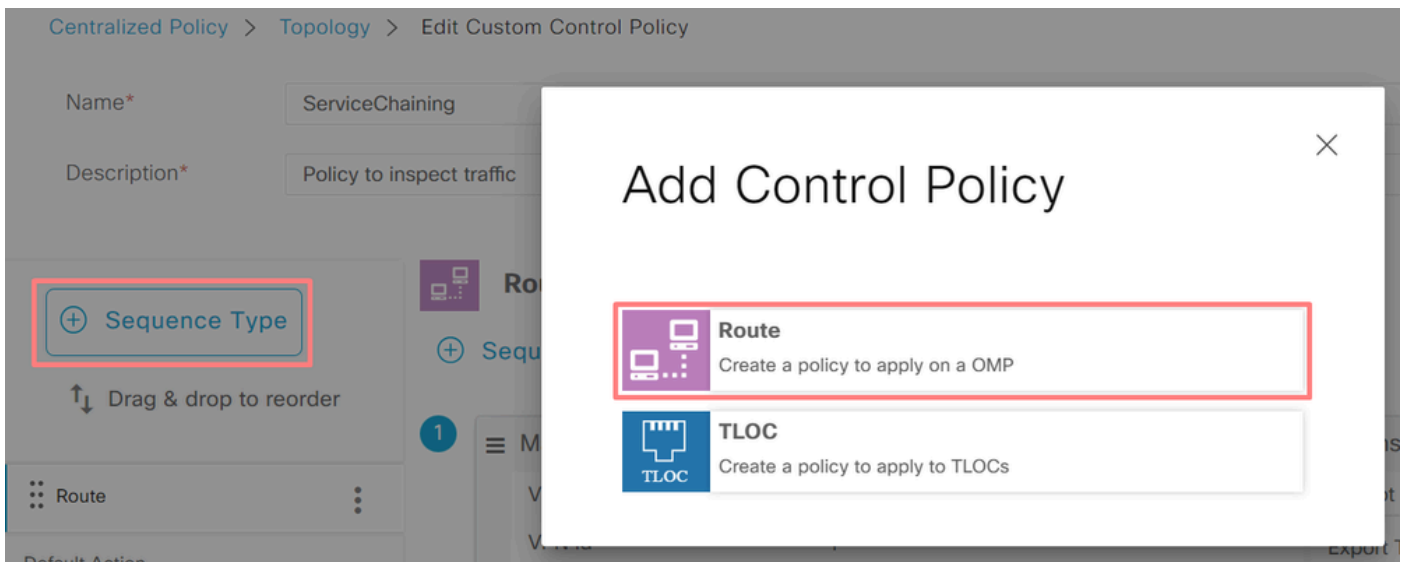
Import Existing Topology

Description

Mode

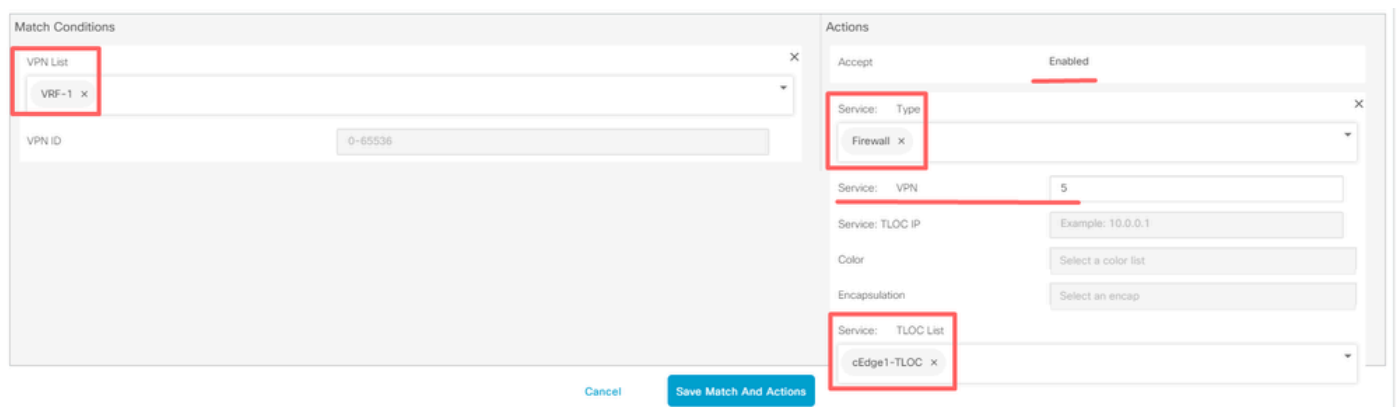
No data available

Fate clic su Tipo sequenza (Sequence Type) e selezionate Sequenza stesura (Route Sequence).



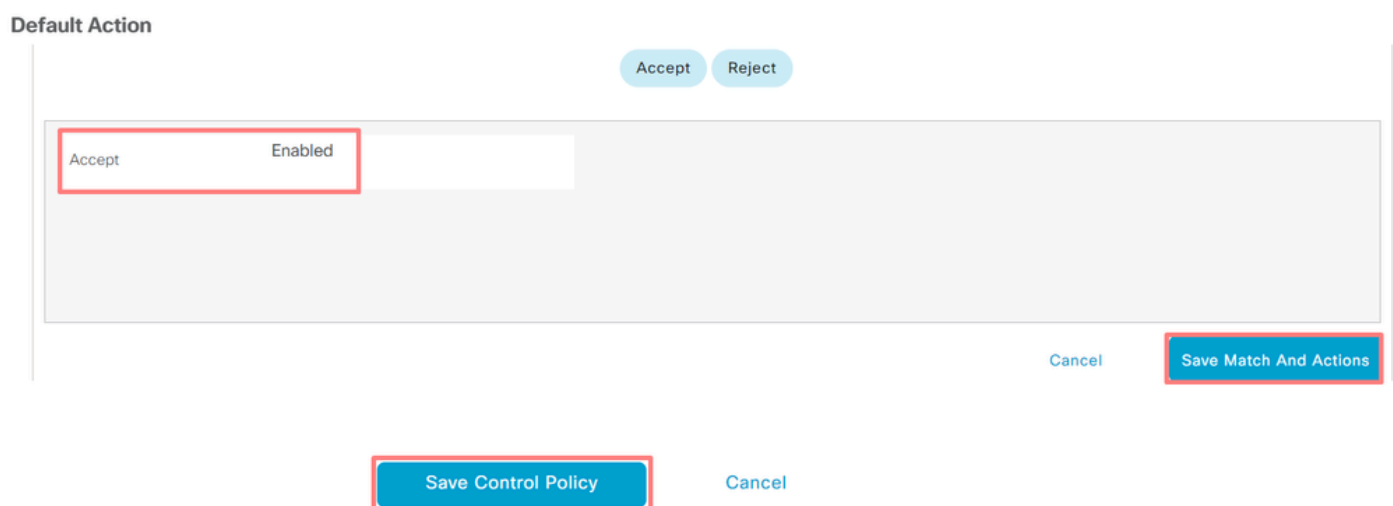
Aggiungere una regola di sequenza.

La sequenza filtra il traffico proveniente dal VRF 1, lo consente di passare e quindi lo reindirizza a un servizio (firewall) esistente all'interno del VRF 5. A tale scopo, è possibile utilizzare il TLOC nel sito 1, che rappresenta la posizione del servizio firewall.



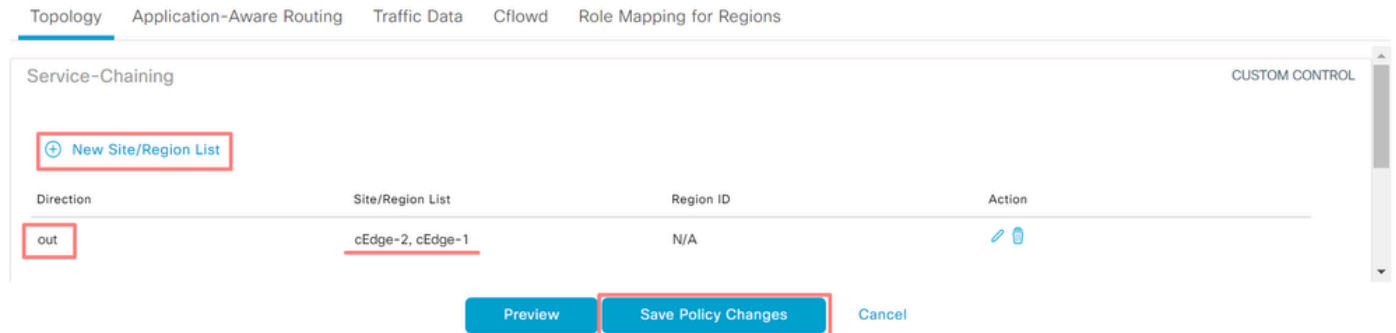
Modificare l'azione predefinita del criterio in Accetta.

Fare clic su Save Match and Actions e quindi su Save Control Policy.



4. Applicare il criterio.

Fare clic sulla scheda Topologia, in Criterio concatenamento servizi selezionare Nuovo elenco sito/area geografica in Elenco siti in uscita. Selezionare i siti che il traffico VRF 1 deve ispezionare e quindi fare clic su Salva criterio. Salvare le modifiche, quindi fare clic su Salva modifiche criteri.



Annuncia servizio firewall

Configurazione tramite CLI

Per effettuare il provisioning del servizio firewall, specificare l'indirizzo IP del dispositivo firewall. Il servizio viene annunciato al controller Cisco Catalyst SD-WAN tramite un aggiornamento 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
```

Configurazione tramite modello

Passare al modello Feature di VRF 5.

Procedere a Configurazione > Modelli > Modello funzionalità > Aggiungi modello > Cisco VPN.

In Sezione assistenza fare clic su Nuovo servizio. Immettere i valori, aggiungere il servizio e salvare il modello.

SERVICE

New Service

Service Type



FW

IPv4 address



192.168.15.2

Tracking



On

Off

Verifica

Perdite

Confermare che il controller Cisco Catalyst SD-WAN sta esportando i percorsi da VRF 1 a VRF 5 e 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	192.168.16.0
1	192.168.18.0/24	192.168.3.15	69	1002	C,R	installed	192.168.18.0

```
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	192.168.16.0

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

Confermare che i router perimetrali Cisco hanno ricevuto il percorso trapelato da VRF 1 a VRF 5.

Confermare che i router perimetrali Cisco hanno ricevuto il percorso trapelato da 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
```

Concatenamento dei servizi

Verificare che Cisco Edge Router abbia annunciato il servizio Firewall al controller Cisco Catalyst SD-WAN tramite il percorso del servizio 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

Confermare che il controller Cisco Catalyst SD-WAN ha ricevuto la route del servizio.

```
<#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		

Per verificare che il servizio Firewall controlli il traffico proveniente dal VRF 1, eseguire 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
```

Informazioni correlate

- [Concatenamento dei servizi](#)
- [Perdite](#)
- [SD-WAN - Configurazione della perdita di percorso - YouTube](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).