

配置SD-WAN中服務鏈結的路由洩漏

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[背景資訊](#)

[設定](#)

[路由洩漏](#)

[透過CLI進行配置](#)

[透過模板進行配置](#)

[服務鏈結](#)

[透過CLI進行配置](#)

[透過模板進行配置](#)

[通告防火牆服務](#)

[透過CLI進行配置](#)

[透過模板進行配置](#)

[驗證](#)

[路由洩漏](#)

[服務鏈結](#)

[相關資訊](#)

簡介

本文檔介紹如何配置和驗證服務鏈以檢查不同VRF之間的流量。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- 控制原則。
- 範本。

採用元件

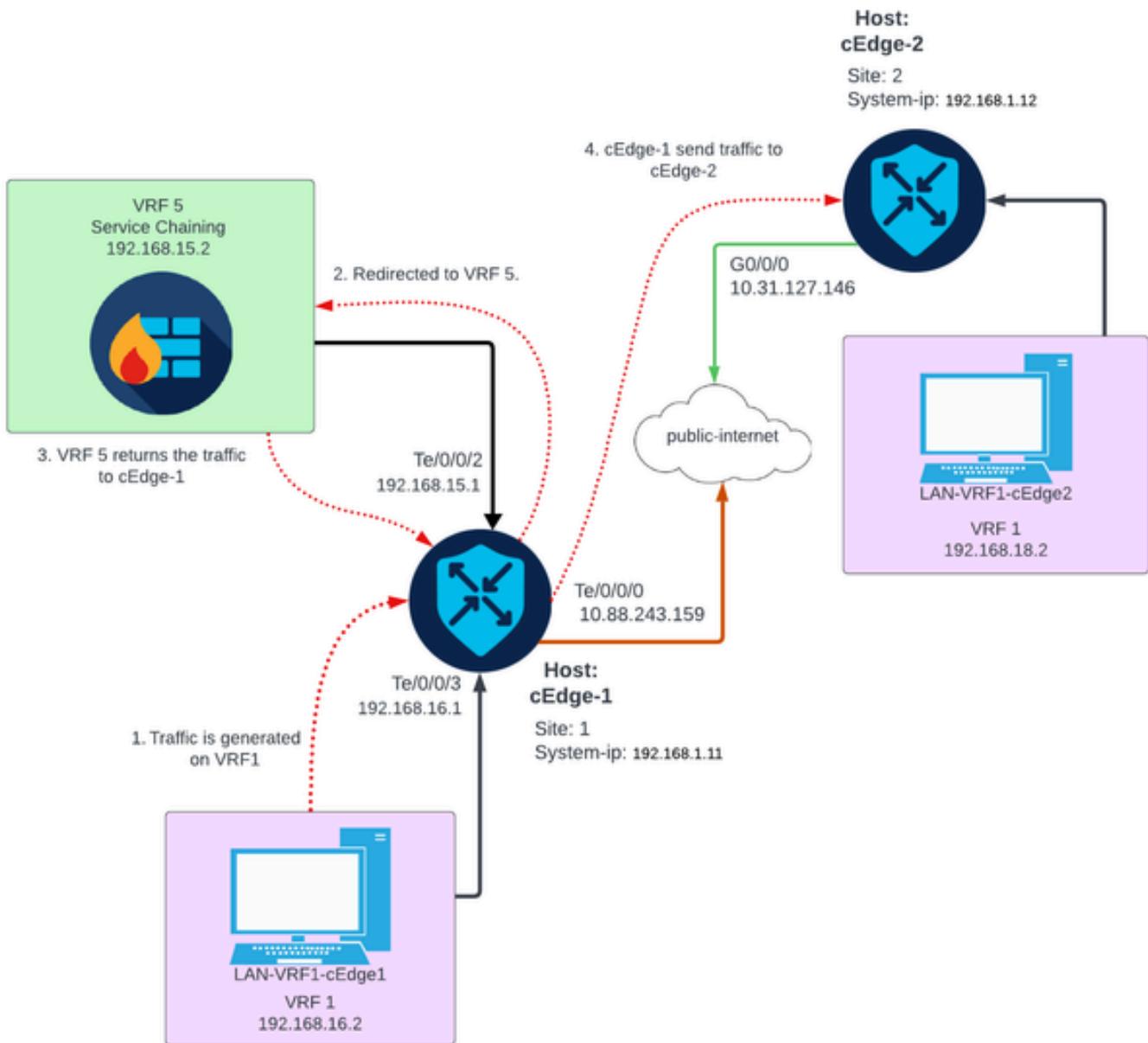
本檔案根據這些軟體和硬體版本：

- SD-WAN控制器(20.9.4.1)

- 思科邊緣路由器(17.09.04)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表



背景資訊

在網路圖中，防火牆服務處於虛擬路由和轉發(VRF) 5中，而LAN裝置位於VRF 1中。必須在VRF之間共用路由資訊，以便實現流量的轉發和檢查。要透過服務路由流量，必須在Cisco SD-WAN控制器上配置控制策略。

設定

路由洩漏

路由洩漏允許不同VRF之間傳播路由資訊。在此場景中，當服務鏈（防火牆）和LAN服務端位於不同的VRF中時，路由洩漏對於流量檢測是必要的。

為確保LAN服務端和防火牆服務之間的路由，兩個VRF都需要路由洩漏，並在需要路由洩漏的站點應用策略。

透過CLI進行配置

1. 在Cisco Catalyst SD-WAN控制器上配置清單。

該配置允許透過清單標識站點。

```
<#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。

此配置允許在VRF 1和VRF 5之間傳播路由資訊，以確保兩者之間的路由，兩個VRF必須共用其路由資料。

策略允許VRF 1的流量被接受並導出到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控制器上應用策略。

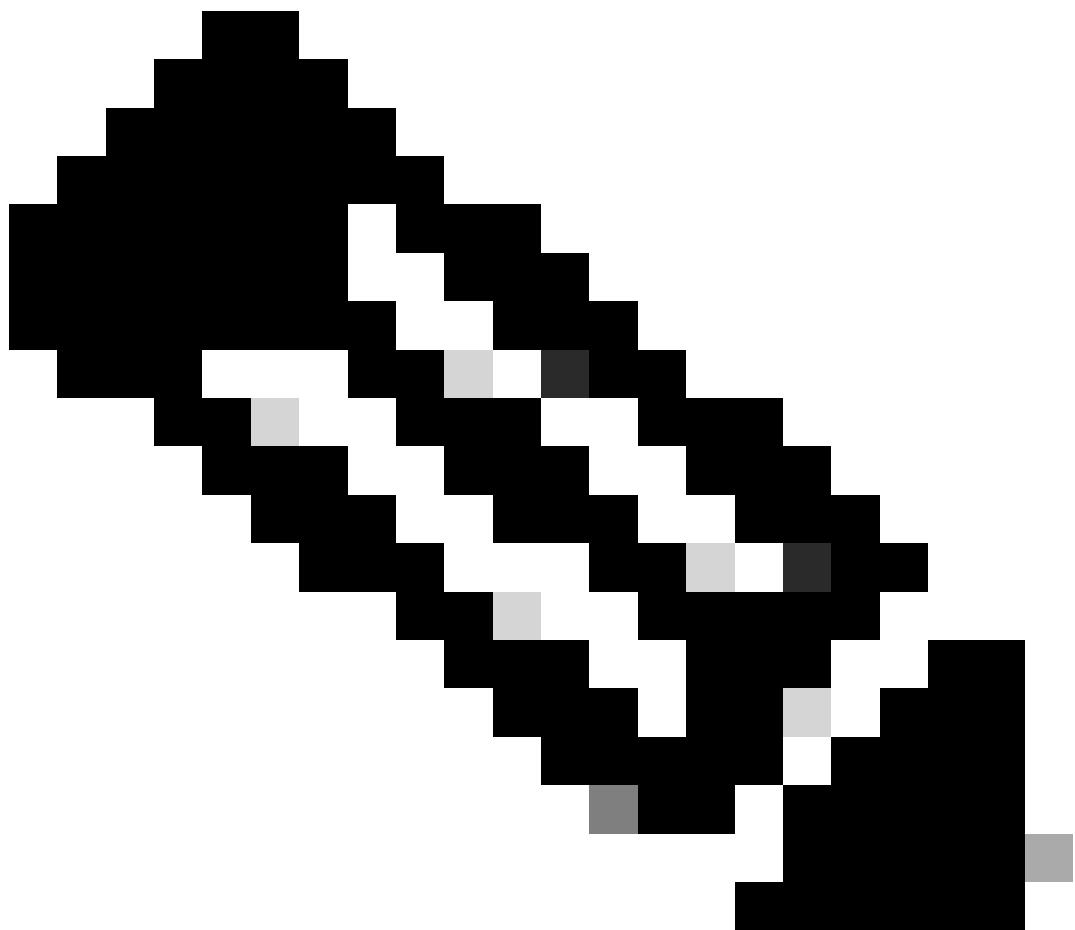
在站點1和站點2中應用策略，以允許位於這些站點和VRF 5上的VRF 1之間進行路由。

策略實施為入站，這意味著將應用到從思科邊緣路由器到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
```

透過模板進行配置



註：要透過Cisco Catalyst SD-WAN Manager圖形使用者介面(GUI)啟用策略，必須附帶Cisco Catalyst SD-WAN控制器模版。

1. 建立允許傳輸路由資訊的策略。

在Cisco Catalyst SD-WAN Manager上建立策略，然後導航至配置>策略>集中策略。

在集中策略頁籤下，按一下增加策略。

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. 在Cisco Catalyst SD-WAN Manager上建立清單，配置允許透過清單標識站點。

導航到站點 > 新建站點清單。

建立需要路由洩漏的站點清單並增加該清單。

Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and Services

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

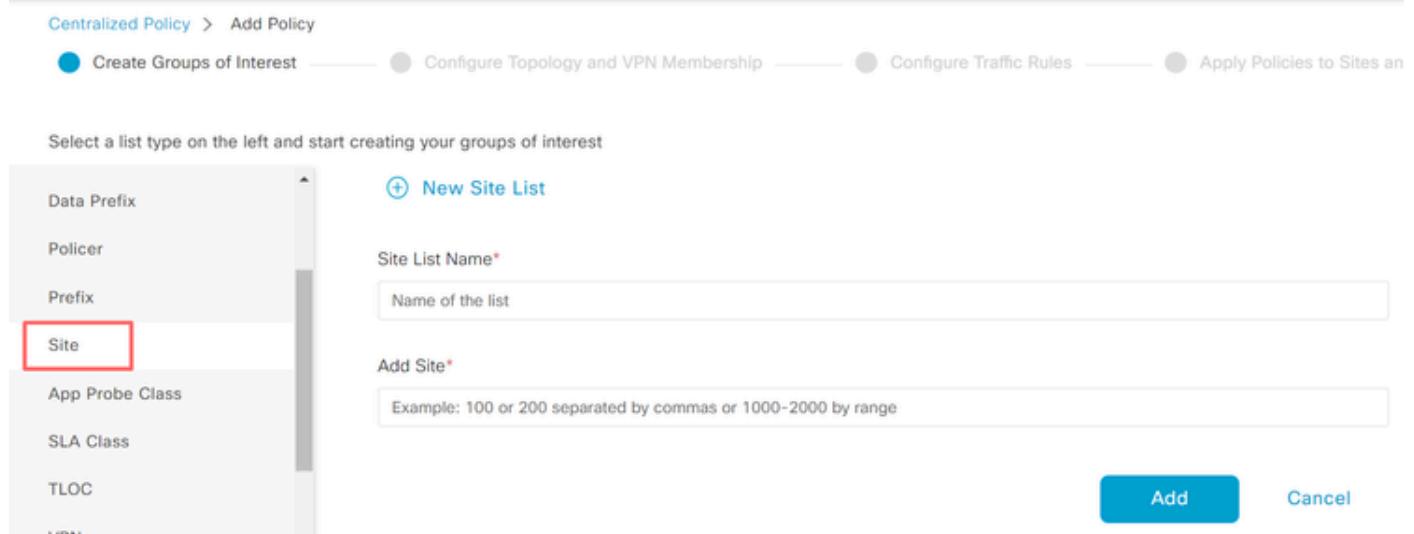
New Site List

Site List Name*
Name of the list

Add Site*
Example: 100 or 200 separated by commas or 1000-2000 by range

Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VLAN

Add Cancel



導航到VPN > New VPN List。

建立需要應用路由洩漏的VPN清單，然後按一下Next。

Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and ...

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。

點選Topology頁籤，然後點選Add Topology。

建立自訂控制項(Route & TLOC)。

Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership

Search

Add Topology ▾

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

Description	Mode
No data available	

點選序列型別並選擇路由序列。

Name*: Route-Leaking

Description*: VRF 1 to VRF 5 and vice versa

Sequence Type

Drag & drop to reorder

Route

Default Action

Add Control Policy

- Route** Create a policy to apply on a OMP
- TLOC** Create a policy to apply to TLOCs

增加序列規則。

條件1：接受VRF 1的流量並將其導出到VRF 5。

Protocol: IPv4 | Accept | Match | Actions

Match Conditions:

- VPN List: VRF-1
- VPN ID: 0-65536

Actions:

- Accept: Enabled
- Export To: VRF-5

Save Match And Actions

條件2：接受VRF 5的流量並將其導出到VRF 1。

Protocol: IPv4 | Accept | Match | Actions

Match Conditions:

- VPN List: VRF-5
- VPN ID: 0-65536

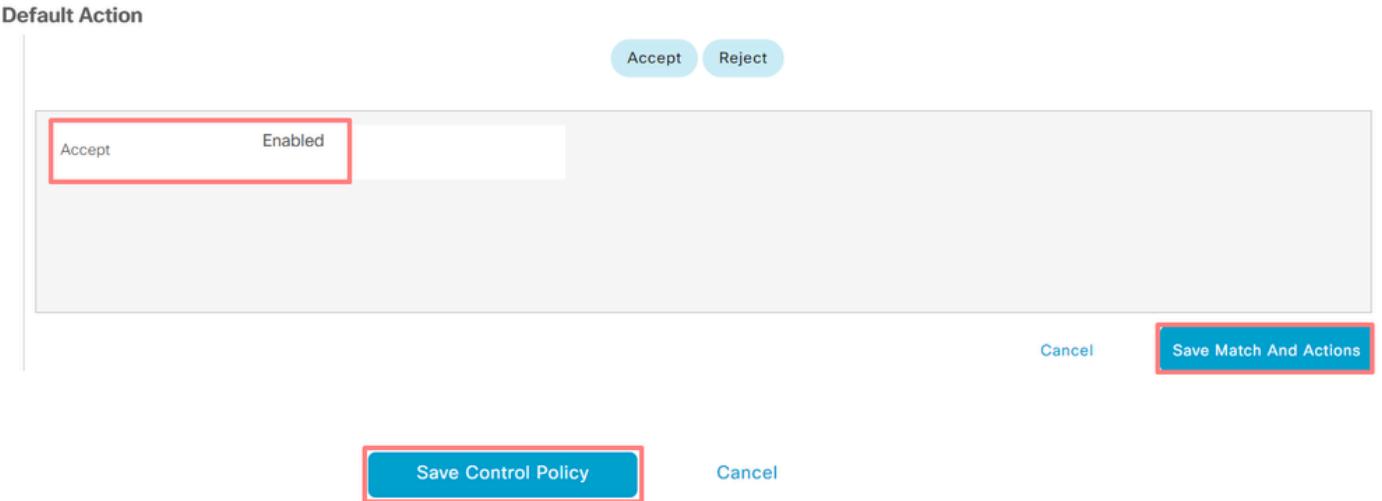
Actions:

- Accept: Enabled
- Export To: VRF-1

Save Match And Actions

將策略的Default Action更改為Accept。

點選Save Match and Actions，然後點選Save Control Policy。



4. 在需要路由洩漏的站點上應用策略。

按一下Topology頁籤上的「Route-Leaking Policy」下，選擇New Site/Region List在「Inbound Site List」上。選擇需要路由洩漏的站點清單。

要儲存修改，請選擇Save Policy Changes。

The screenshot shows the 'Route-Leaking' configuration page. It lists a site 'cEdge-2, cEdge-1' under 'Site/Region List' for direction 'in'. At the bottom are 'Preview', 'Save Policy Changes', and 'Cancel' buttons. A red box highlights the 'Save Policy Changes' button.

服務鏈結

服務鏈也稱為服務插入。它涉及注入網路服務；標準服務包括防火牆(FW)、入侵檢測系統(IDS)和入侵防禦系統(IPS)。在這種情況下，會在資料路徑中插入防火牆服務。

透過CLI進行配置

1. 在Cisco Catalyst SD-WAN控制器上配置清單。

該配置允許透過清單標識站點。

建立每個VRF 1所在站點的清單。

在傳輸位置(TLOC)清單中，指定流量必須重新導向才能到達服務的地址。

```
<#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。

該序列過濾來自VRF 1的流量。流量在VRF 5上的服務防火牆上被允許和檢查。

```

<#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控制器上應用策略。

在站點1和站點2中配置該策略，以允許對來自VRF 1的流量進行檢查。

```

<#root>
vSmart#
config

vSmart(config)#

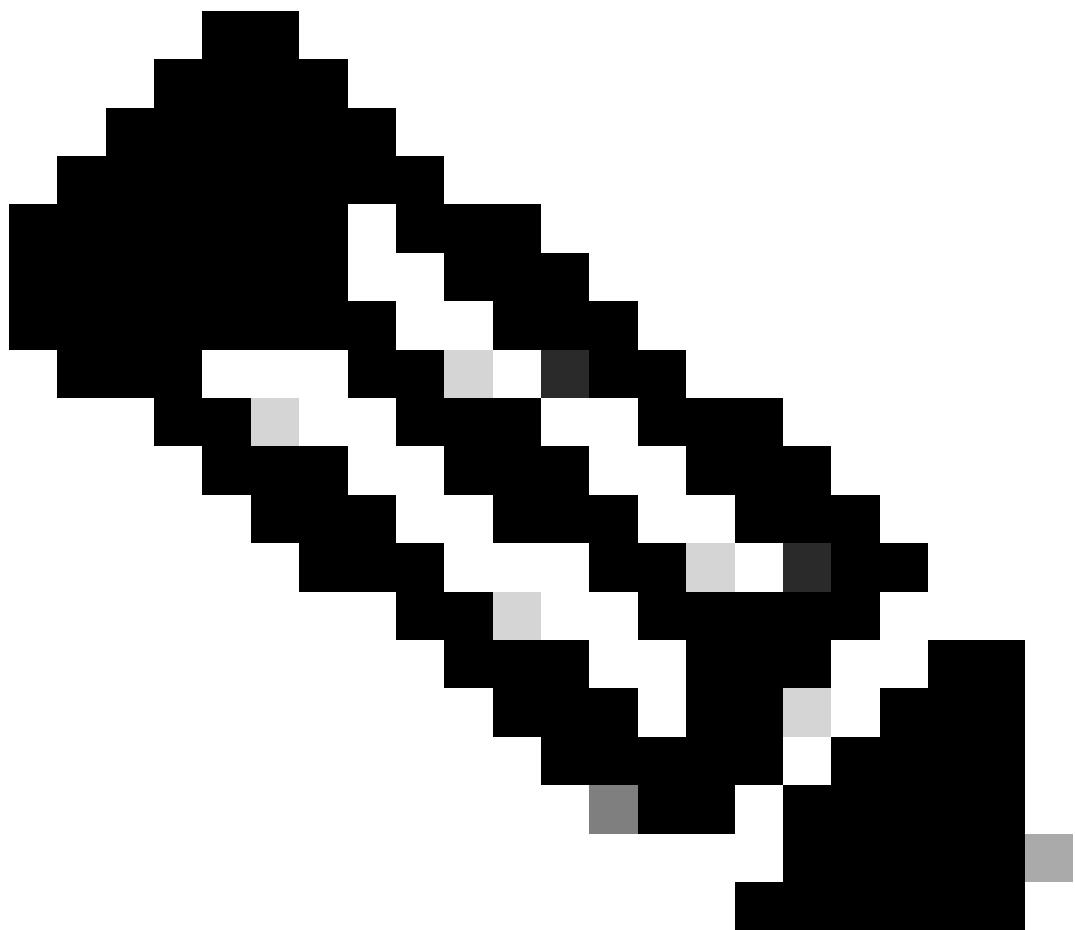
```

```
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
```

透過模板進行配置



注意：要透過Cisco Catalyst SD-WAN Manager圖形使用者介面(GUI)啟用策略，Cisco Catalyst SD-WAN控制器必須連線模板。

-
1. 在Cisco Catalyst SD-WAN Manager上建立策略。

導航到配置 >策略>集中策略。

在Centralized Policy頁籤下按一下Add Policy。

Centralized Policy

Localized Policy

Search

Add Policy

Add Default AAR & QoS

2. 在Cisco Catalyst SD-WAN Manager上建立清單。

導航到站點>新建站點清單。

建立VRF 1所在站點的站點清單，並選擇Add。

Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and Services

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

The screenshot shows the 'Centralized Policy > Add Policy' screen. On the left, there's a vertical list of options: Data Prefix, Policer, Prefix, Site (which is highlighted with a red box), App Probe Class, SLA Class, TLOC, and Link. To the right, there's a 'New Site List' section with a plus icon. Below it, there's a 'Site List Name*' field with 'Name of the list' placeholder text, and an 'Add Site*' field with 'Example: 100 or 200 separated by commas or 1000-2000 by range' placeholder text. At the bottom right are 'Add' and 'Cancel' buttons.

導航到TLOC > New TLOC List。

Create the TLOC list service chaining is on and select Save。

TLOC List

X

List Name *

cEdge1-TLOC

TLOC IP*

Color*

Encap*

Preference

192.168.1.11

public-internet

v

ipsec

v

0-4294967295

 Add TLOC

Cancel

Save

3. 新增序號規則。

按一下Topology頁籤，然後按一下Add Topology。

建立自訂控制項(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

點選序列型別並選擇路由序列。

The screenshot shows the 'Edit Custom Control Policy' page. At the top, there are fields for 'Name*' (ServiceChaining) and 'Description*' (Policy to inspect traffic). Below these, a section titled 'Sequence Type' is highlighted with a red box. A note says 'Drag & drop to reorder'. To the right, a modal window titled 'Add Control Policy' is open, showing two options: 'Route' (Create a policy to apply on a OMP) and 'TLOC' (Create a policy to apply to TLOCs). The 'Route' option is also highlighted with a red box.

增加序列規則。

該序列過濾來自VRF 1的流量，允許其通過，然後將其重定向到VRF 5中存在的服務（防火牆）。這可以透過使用站點1（防火牆服務的位置）的TLOC來實現。

This screenshot shows the 'Match Conditions' and 'Actions' sections of the policy editor. In the 'Match Conditions' section, the 'VPN List' field contains 'VRF-1' and the 'VPN ID' field contains '0-65536'. In the 'Actions' section, under the 'Accept' row, the 'Service: Type' field contains 'Firewall' and the 'Service: VPN' field contains '5'. Under the 'TLOC' row, the 'Service: TLOC List' field contains 'cEdge1-TLOC'. Both the 'Firewall' and 'cEdge1-TLOC' fields are highlighted with red boxes.

將策略的Default Action更改為Accept。

點選Save Match and Actions，然後點選Save Control Policy。

This screenshot shows the 'Default Action' and 'Save Control Policy' sections. In the 'Default Action' section, the 'Accept' button is highlighted with a red box. In the 'Save Control Policy' section, the 'Save Control Policy' button is also highlighted with a red box.

4. 套用政策。

按一下Topology頁籤上的「Service-Chaining Policy」下，選擇New Site/Region List(在Outbound Site List上)。選擇VRF 1流量必須檢查的站點，然後按一下Save Policy。儲存修改，然後按一下Save Policy Changes。

The screenshot shows the Cisco SD-WAN Topology interface. At the top, there are tabs: Topology (selected), Application-Aware Routing, Traffic Data, Cflowd, and Role Mapping for Regions. Below the tabs, under the 'Service-Chaining' section, there is a table with columns: Direction, Site/Region List, Region ID, and Action. A row in the table has 'out' in the Direction column, 'cEdge-2, cEdge-1' in the Site/Region List column, and 'N/A' in the Region ID column. The Action column contains edit and delete icons. At the bottom of the table are three buttons: Preview, Save Policy Changes (highlighted with a red box), and Cancel.

通告防火牆服務

透過CLI進行配置

要設定防火牆服務，請指定防火牆裝置的IP地址。透過OMP更新向Cisco Catalyst SD-WAN控制器通告該服務。

```
<#root>
cEdge-01#
config-transaction

cEdge-01(config)#
sdwan

cEdge-01(config-sdwan)#
service Firewall vrf 5

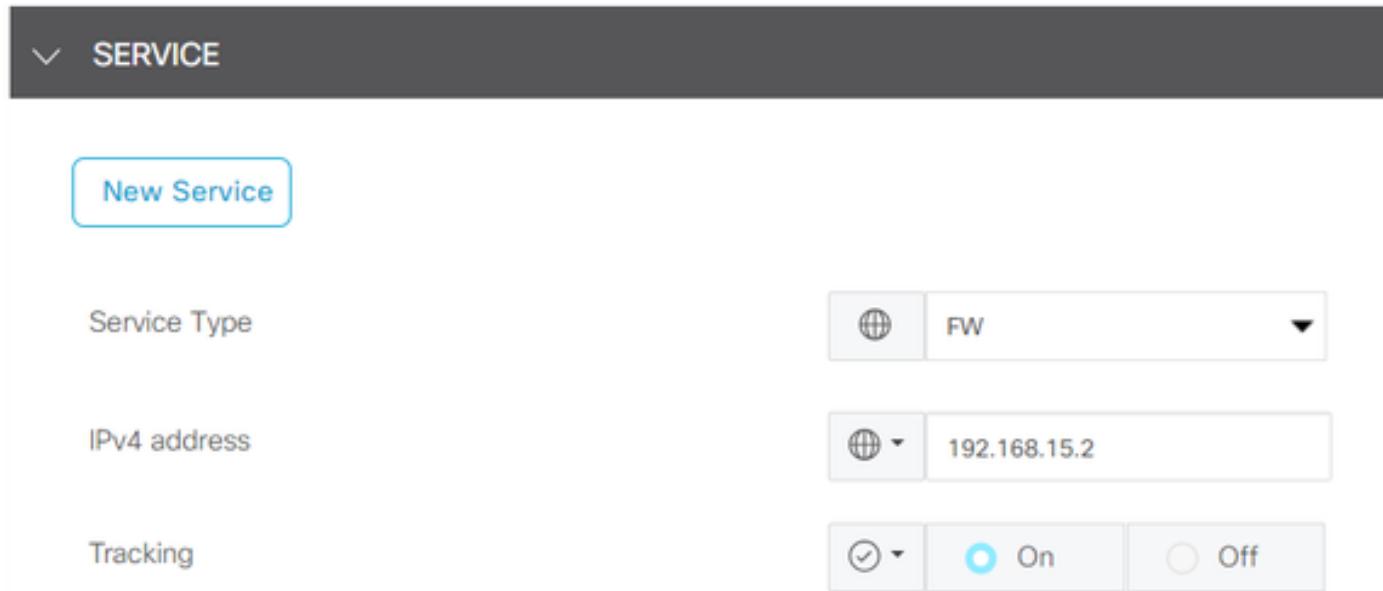
cEdge-01(config-vrf-5)#
ipv4 address 192.168.15.2
cEdge-01(config-vrf-5)#
commit
```

透過模板進行配置

導航到VRF 5的功能模板。

繼續執行Configuration > Templates > Feature Template > Add Template > Cisco VPN。

在服務部分下，按一下新建服務。輸入值Add the Service和Save 模板。



驗證

路由洩漏

確認Cisco Catalyst SD-WAN控制器正在將路由從VRF 1導出到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.
						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.

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

確認思科邊緣路由器收到從VRF 1到VRF 5的洩漏路由。

確認思科邊緣路由器收到從VRF 5到VRF 1的洩漏路由。

```
<#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
C   192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
L     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
```

服務鏈結

驗證思科邊緣路由器是否已透過OMP服務路由將防火牆服務通告給Cisco Catalyst SD-WAN控制器。

<#root>

cEdge-01#

show sdwan omp services

ADDRESS						PATH	REGION			
FAMILY	TENANT	VPN	SERVICE	ORIGINATOR	FROM PEER	ID	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

確認Cisco Catalyst SD-WAN控制器已成功收到服務路由。

<#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	

要驗證防火牆服務是否檢查來自VRF 1的流量，請執行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
```

相關資訊

- [服務鏈結](#)
- [路由洩漏](#)
- [SD-WAN -配置路由洩漏- YouTube](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。