

使用傳輸交換矩陣的L4-L7路由對等 — 配置演練

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[設定](#)

[驗證和疑難排解](#)

簡介

本檔案介紹使用路由對等的L4-L7服務圖的配置演練，其中消費者和提供商均位於以應用為中心的基礎設施(ACI)交換矩陣外部。

作者：思科高級服務工程師Zahid Hassan。

必要條件

需求

思科建議您瞭解以下主題：

- 靜態VLAN池，將用於外部裝置和ACI交換矩陣之間的封裝VLAN
- 將外部裝置的位置（枝葉節點/路徑）與VLAN池結合在一起的外部物理域和路由域
- 到外部網路(L3Out)的第3層連線

本文檔未介紹前面的**交換矩陣訪問**和**L3Out**配置步驟，並假定這些步驟已經完成。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科應用政策基礎架構控制器（思科APIC） — 1.2(1m)
- 自適應安全裝置(ASA)裝置包 — 1.2.4.8
- ASA 5585 - 9.5(1)
- Nexus 3064 - 6.0(2)U3(7)

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

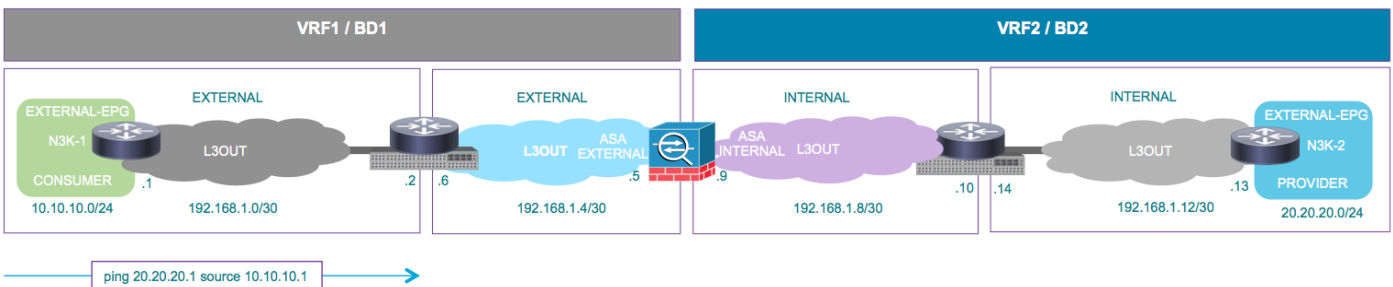
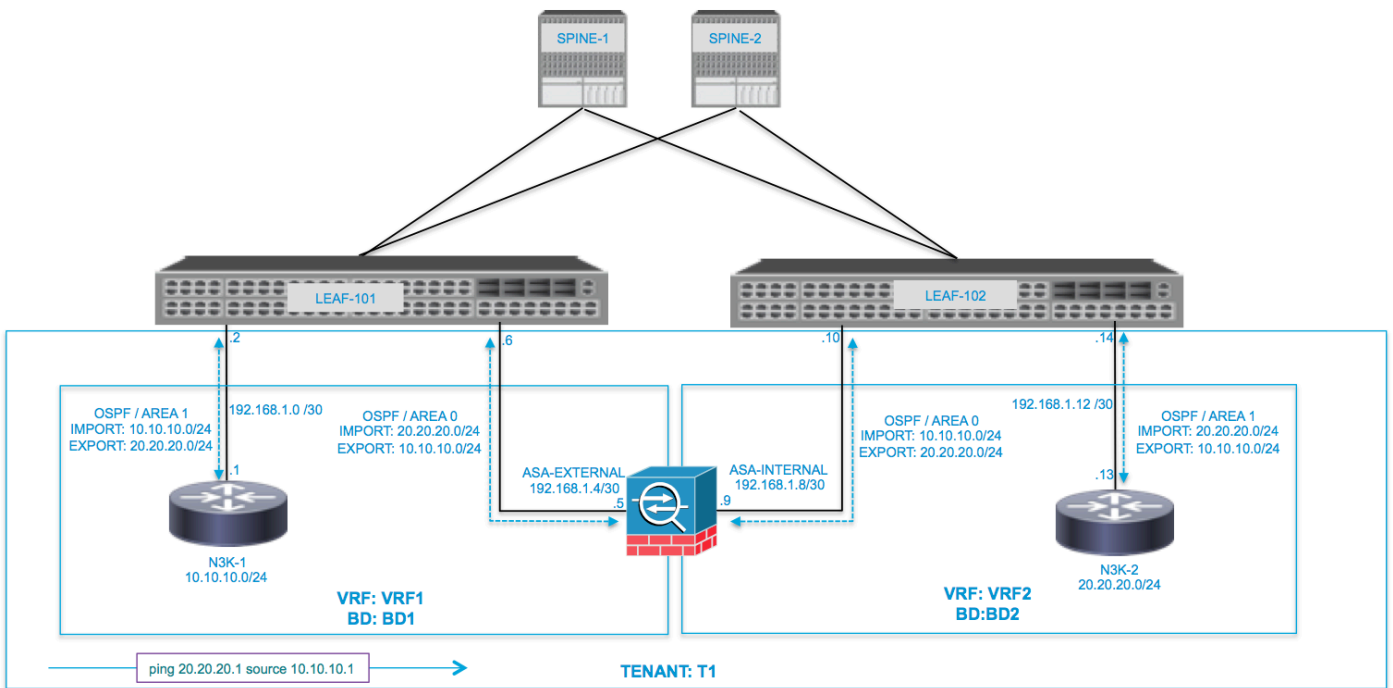
路由對等功能使服務裝置（例如負載均衡器或防火牆）能夠通過ACI交換矩陣向外部網路通告其可達性。

此處提供的使用案例是在兩個L3Outs或外部終端組(EPG)之間部署為雙臂服務圖的物理防火牆。服務圖與枝葉101上的外部EPG(N3K-1)與枝葉102上的外部EPG(N3K-2)之間的合約相關聯。ACI交換矩陣為路由器（N3K-1和N3K-2）提供中轉服務，並且使用路由對等(使用開放最短路徑優先(OSPF)作為路由協定)在防火牆和ACI交換矩陣之間交換路由。

設定

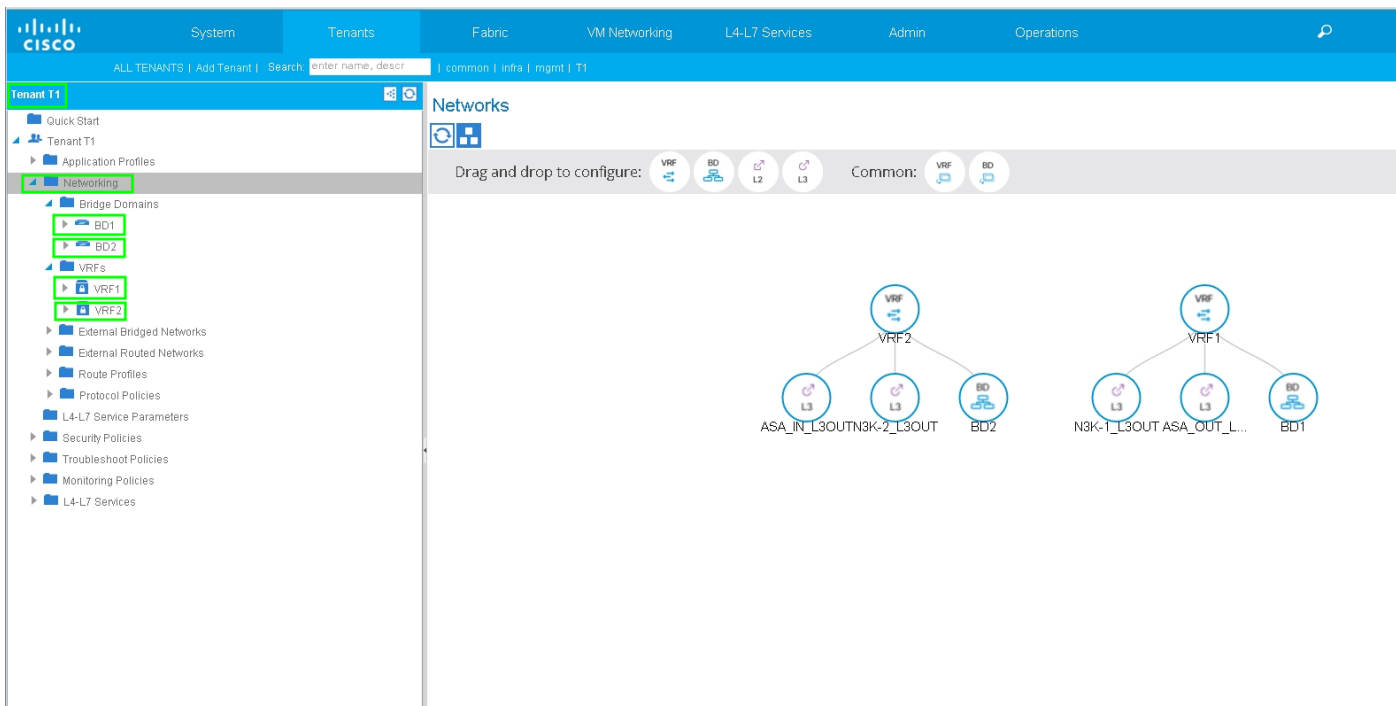
網路圖表

下圖顯示路由對等端如何運作：

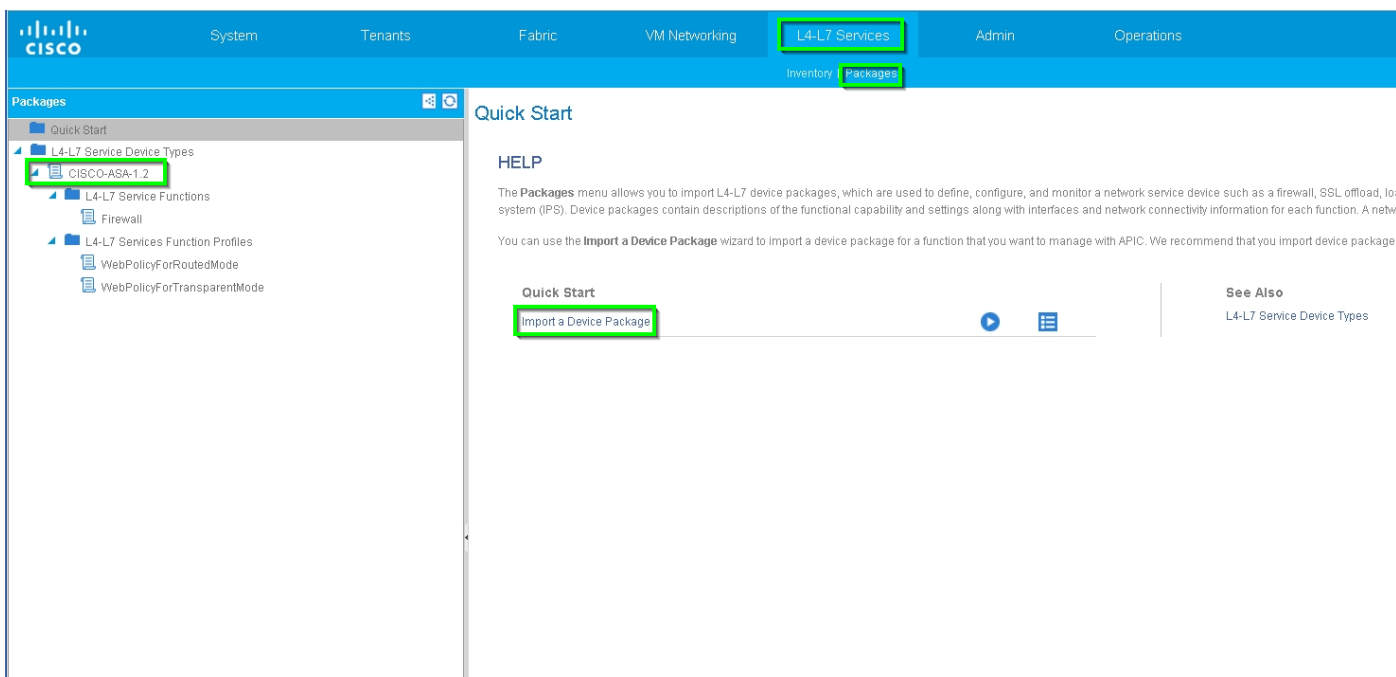


設定

步驟1.配置虛擬路由和轉發1(VRF1)、VRF2、網橋域1(BD1)和BD2。將BD1與VRF1關聯，將BD2與VRF2關聯，如下圖所示：



步驟2.上傳L4-L7裝置下的ASA裝置包，如下圖所示：



為物理ASA 5585 (路由) 配置L4-L7裝置，如下圖所示：

The screenshot shows the Cisco ACI GUI for configuring L4-L7 devices. The left sidebar is expanded to 'L4-L7 Devices'. The main configuration area is titled 'L4-L7 Devices - ASA5585'. It includes sections for 'General' (Name: ASA5585, Device Package: CISCO-ASA-1.2, Service Type: Firewall), 'Credentials' (Username: admin), and 'Configuration State' (Devices State: stable). The 'Device 1' section shows Management IP Address: 172.23.97.1, Management Port: 443, and a table of interfaces:

Name	Path
GigabitEthernet0/0	Node-105/eth1/2
GigabitEthernet0/1	Node-106/eth1/2

The 'Cluster' section shows Management IP Address: 172.23.96.228, Management Port: 443, and a table of cluster interfaces:

Type	Name	Concrete Interfaces
provider	inside	ASA5585_Device_1[GigabitEthernet0/1]
consumer	outside	ASA5585_Device_1[GigabitEthernet0/0]

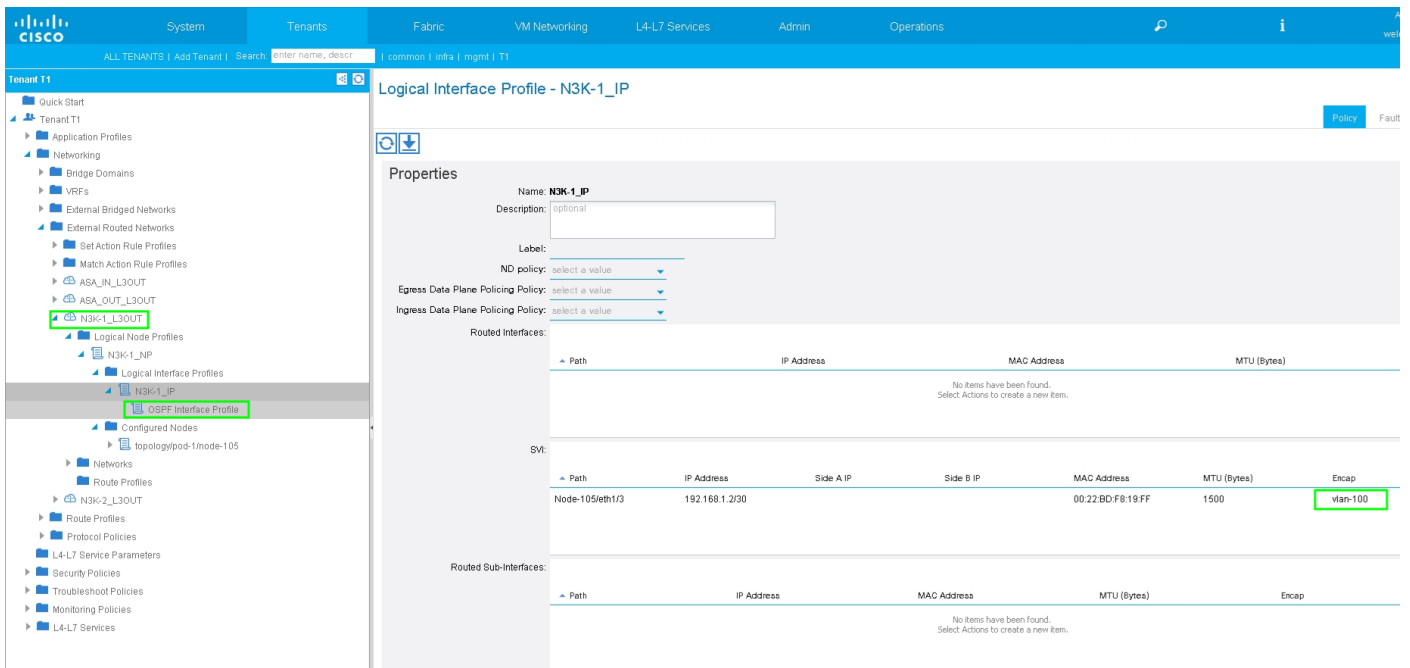
步驟3.為N3K-1配置L3Out並與BD1和VRF1關聯。

外部路由網路用於在ACI交換矩陣中為路由對等指定路由配置，如下圖所示：

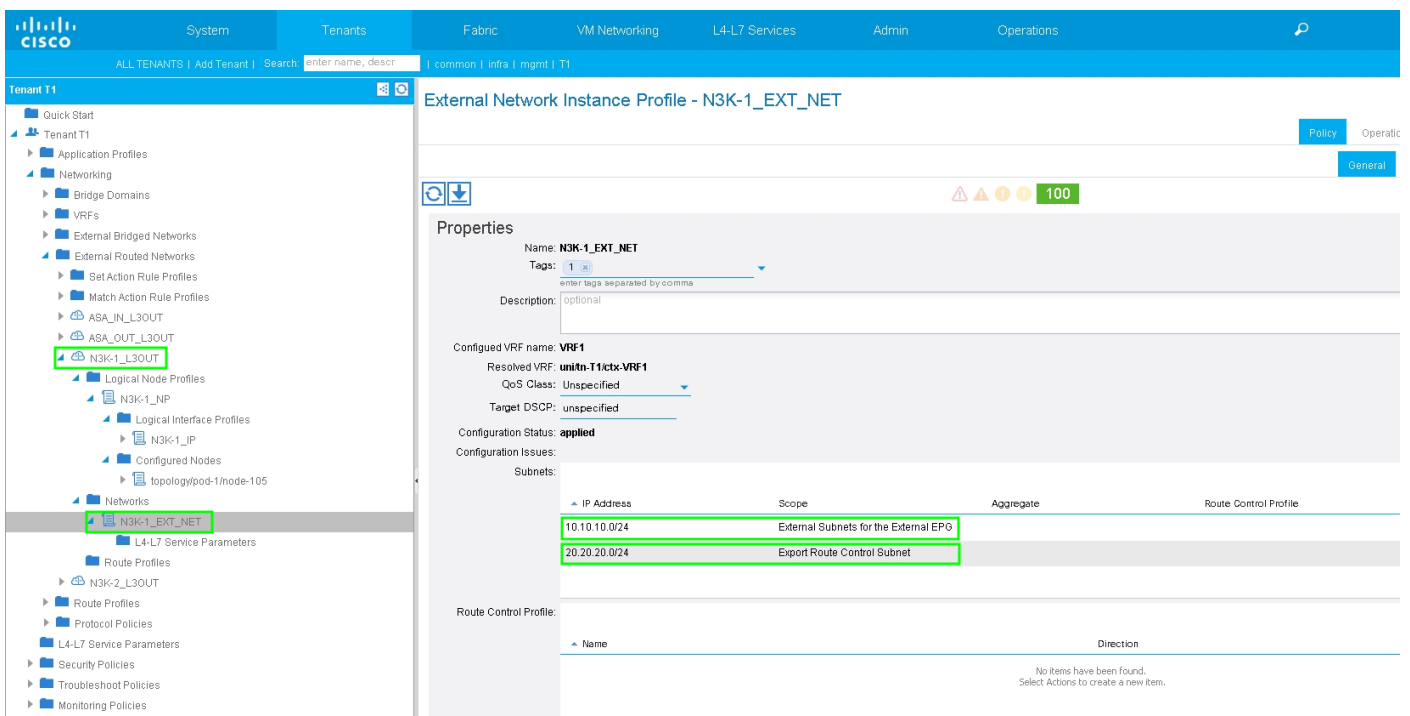
The screenshot shows the Cisco ACI GUI for configuring L3 Outside. The left sidebar is expanded to 'N3K-1_L3OUT'. The main configuration area is titled 'L3 Outside - N3K-1_L3OUT'. The 'Properties' section includes:

- Name: N3K-1_L3OUT
- Description: optional
- Tags: (empty)
- Label: (empty)
- Target DSCP: unspecified
- Route Control Enforcement: Import, Export
- VRF: T1/VRF1
- Resolved VRF: T1/VRF1
- External Routed Domain: T1_L3OUT
- Route Profile for Interleak: (empty)
- Route Control For Dampening: (empty)
- Address Family Type: (empty)
- Enable BGP/EIGRP/OSPF: BGP, OSPF, EIGRP
- OSPF Area ID: 0.0.0.1
- OSPF Area Control: Send redistributed LSAs into NSSA area, Originate summary LSA, Suppress forwarding address in translated LSA
- OSPF Area Type: NSSA area, Regular area, Stub area
- OSPF Area Cost: 1

附註：所有用於路由對等的L3Out介面必須相應地配置為具有VLAN封裝的交換機虛擬介面 (SVI)。



為N3K-1 L3Out外部EPG配置子網的匯入/匯出路由控制，如下圖所示：



為ASA外部介面配置L3Out並與BD1和VRF1關聯，如下圖所示：

L3 Outside - ASA_OUT_L3OUT

Properties

Name: **ASA_OUT_L3OUT**

Description: optional

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: **T1/VRF1**

Resolved VRF: **T1/VRF1**

External Routed Domain: T1_L3OUT

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type:

Route Dampening Policy: No items have been found. Select Actions to create a new item.

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: **0**

OSPF Area Control: Send redistributed LSAs into NSSA area Originate summary LSA Suppress forwarding address in translated LSA

OSPF Area Type: NSSA area **Regular area** Stub area

OSPF Area Cost: 0

Logical Interface Profile - ASA_OUT_IP

Properties

Name: **ASA_OUT_IP**

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed interfaces:

Path	IP Address	MAC Address	MTU (Bytes)
No items have been found. Select Actions to create a new item.			

SVI:

Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-105eth1/2	192.168.1.8/30			00:22:BD:F8:19:FF	1500	vlan-101

Routed Sub-Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)	Encap
No items have been found. Select Actions to create a new item.				

為ASA外部L3Out外部EPG配置子網的匯入/匯出路由控制，如下圖所示：

External Network Instance Profile - ASA_OUT_EXT_NET

Policy Operational Stats

General Contracts

Properties

Name: ASA_OUT_EXT_NET

Tags: enter tags separated by comma

Description: optional

Configured VRF name: VRF1

Resolved VRF: untn-T1/ctx-VRF1

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: applied

Configuration Issues:

IP Address	Scope	Aggregate	Route Control Profile	Route Summa
10.10.10.0/24	Export Route Control Subnet			
20.20.20.0/24	External Subnets for the External EPG			

Route Control Profile:

Name Direction

No items have been found. Select Actions to create a new item.

為ASA-Internal配置L3out並與BD2和VRF2關聯，如下圖所示：

L3 Outside - ASA_IN_L3OUT

Properties

Name: ASA_IN_L3OUT

Description: optional

Tags: 1

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: T1/VRF2

Resolved VRF: T1/VRF2

External Routed Domain: T1_L3OUT

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type Route Dampening Policy

No items have been found. Select Actions to create a new item.

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: 0

OSPF Area Control: Send redistributed LSAs into NSSA area Originate summary LSA Suppress forwarding address in translated LSA

OSPF Area Type: NSSA area Regular area Stub area

OSPF Area Cost: 0

The screenshot displays the Cisco SD-WAN GUI for configuring a Logical Interface Profile named **ASA_IN_IP**. The left-hand navigation pane shows the hierarchy: Tenant T1 > Networking > External Routed Networks > Match Action Rule Profiles > ASA_IN_L3OUT > Logical Node Profiles > ASA_IN_IP > Logical Interface Profiles > ASA_IN_IP. The main configuration area shows the following details:

- Name:** ASA_IN_IP
- Description:** optional
- Label:** (empty field)
- ND policy:** select a value
- Egress Data Plane Policing Policy:** select a value
- Ingress Data Plane Policing Policy:** select a value

Below these properties are three tables:

- Routed Interfaces:** A table with columns Path, IP Address, MAC Address, and MTU (Bytes). It is currently empty with the message: "No items have been found. Select Actions to create a new item."
- SVI:** A table with columns Path, IP Address, Side A IP, Side B IP, MAC Address, MTU (Bytes), and Encap. It contains one entry:

Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-106/eth1/2	192.168.1.10/30			00:22:BD:F8:19:FF	1500	vlan-102
- Routed Sub-Interfaces:** A table with columns Path, IP Address, MAC Address, MTU (Bytes), and Encap. It is currently empty with the message: "No items have been found. Select Actions to create a new item."

為ASA內部L3Out外部EPG配置子網的匯入/匯出路由控制，如下圖所示：

The screenshot displays the Cisco SD-WAN GUI for configuring an External Network Instance Profile named **ASA_IN_EXT_NET**. The left-hand navigation pane shows the hierarchy: Tenant T1 > Networking > External Routed Networks > Match Action Rule Profiles > ASA_IN_L3OUT > Networks > ASA_IN_EXT_NET. The main configuration area shows the following details:

- Name:** ASA_IN_EXT_NET
- Tags:** (empty field)
- Description:** optional
- Configured VRF name:** VRF2
- Resolved VRF:** unln-11ctx-VRF2
- QoS Class:** Unspecified
- Target DSCP:** unspecified
- Configuration Status:** applied

Under **Configuration Issues:**, there is a **Subnets** table:

IP Address	Scope	Aggregate	Route Control Profile
10.10.10.0/24	External Subnets for the External EPG		Shared Route Control Subnet
20.20.20.0/24	Export Route Control Subnet		Shared Route Control Subnet

Below this is the **Route Control Profile** section, which is currently empty with the message: "No items have been found. Select Actions to create a new item."

為N3K-2配置L3Out並與BD2和VRF2關聯，如下圖所示：

L3 Outside - N3K-2_L3OUT

Properties

Name: **N3K-2_L3OUT**

Description: optional

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: **T1/VRF2**

Resolved VRF: **T1/VRF2**

External Routed Domain: T1_L3OUT

Route Profile for Interleak: select a value

Route Control For Dampening:

Address Family Type:

Route Dampening Policy: No items have been found. Select Actions to create a new item.

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: **0.0.0.1**

OSPF Area Control: Send redistributed LSAs into NSSA area Originate summary LSA Suppress forwarding address in translated LSA

OSPF Area Type: NSSA area **Regular area** Stub area

OSPF Area Cost: 0

Logical Interface Profile - N3K-2_IP

Properties

Name: **N3K-2_IP**

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)
No items have been found. Select Actions to create a new item.			

SVI:

Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-1066eth1/4	192.168.1.14/30			00:22:BD:F8:19:FF	1500	vlan-103

Routed Sub-Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)	Encap
No items have been found. Select Actions to create a new item.				

為外部EPG的N3K-2 L3Out配置子網的匯入/匯出路由控制，如下圖所示：

External Network Instance Profile - N3K-2_EXT_NET

Properties

Name: **N3K-2_EXT_NET**

Tags:

Description: optional

Configured VRF name: **VRF2**

Resolved VRF: **unitn-11ctx-VRF2**

QoS Class: **Unspecified**

Target DSCP: **unspecified**

Configuration Status: **applied**

Configuration Issues:

Subnets:

IP Address	Scope	Aggregate	Route Control Profile
10.10.10.0/24	Export Route Control Subnet		
20.20.20.0/24	External Subnets for the External EPG		

Route Control Profile:

Name	Direction
No items have been found. Select Actions to create a new item.	

步驟4.建立功能設定檔群組，並根據現有範本設定功能設定檔，如下圖所示：

L4-L7 Services Function Profile - ASA5585_FP

Properties

Name: **ASA5585_FP**

Description:

Associated Function: **CISCO-ASA-12FWirewall**



FEATURES AND PARAMETERS

Features:

- Interfaces
- AccessLists
- NAT
- TrafficSelectionObjects
- All

Basic Parameters | All Parameters

Meta Folder/Param Key	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
Access List	access-list-inbound			false	false
Interface Related Configuration	externalf			false	false
Interface Related Configuration	internalf			false	false
Function Config	Function				
External Interface Configuration	ExtConfig			false	false
Internal Interface Configuration	IntConfig			false	false



ACTIONS

Properties

Name: **ASA5585_FP**
 Description:
 Associated Function: **CISCO-ASA-1.2Firewall**

FEATURES AND PARAMETERS

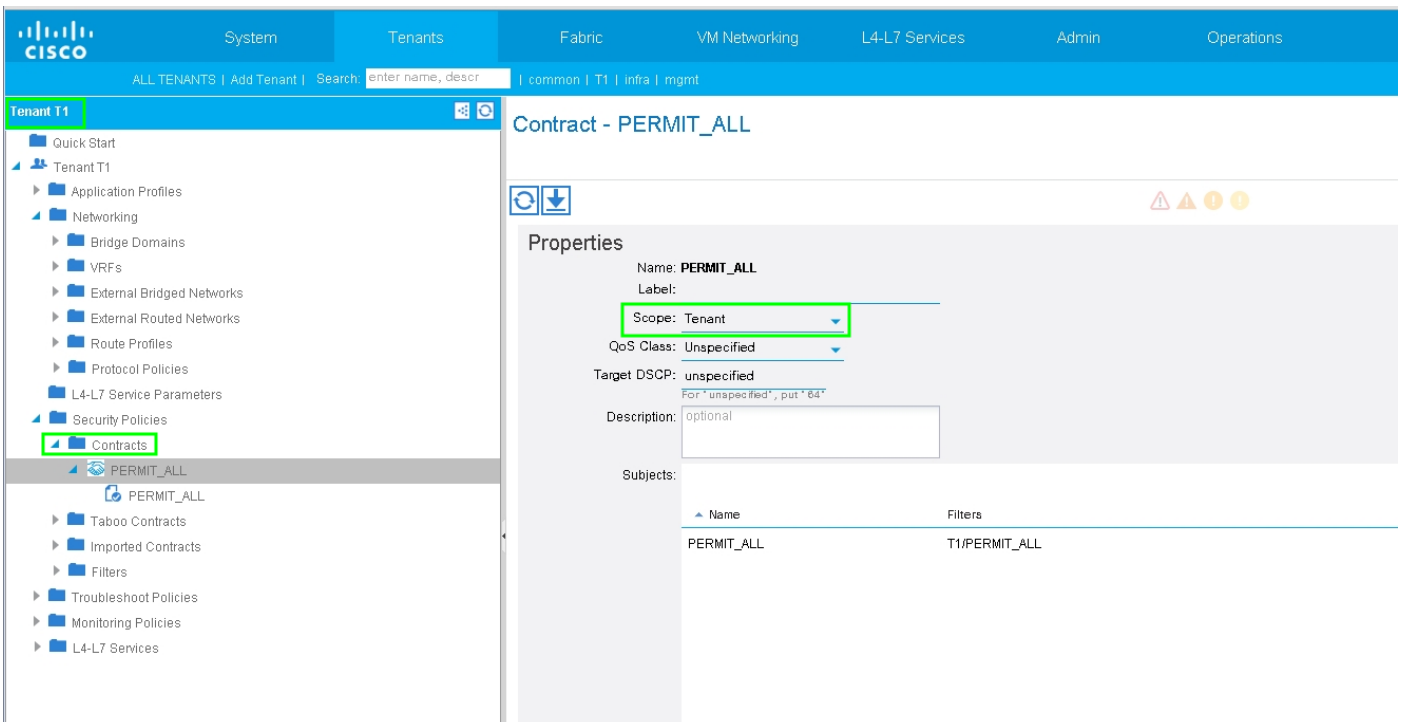
Features:

- [Interfaces](#)
- [AccessLists](#)
- [NAT](#)
- [TrafficSelectionObjects](#)
- All**

Basic Parameters All Parameters

Meta Folder/Param Key	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
Access List	access-list-inbound			false	false
Interface Related Configuration	externalif			false	false
Access Group	ExtAccessGroup			false	
Inbound Access List	name	access-list-inbound	false	false	
Interface Specific Configuration	externalifCfg			false	
IPv4 Address Configuration	IPv4Address			false	
IPv4 Address	ipv4_address	192.168.1.5/30	true	false	
Security Level	external_security_level	50	false	false	
Interface Related Configuration	internalif			false	false
Interface Specific Configuration	internalifCfg			false	
IPv4 Address Configuration	IPv4Address			false	
IPv4 Address	ipv4_address	192.168.1.9/30	true	false	
Security Level	internal_security_level	100	false	false	
Function Config	Function				
External Interface Configuration	ExtConfig			false	false
Interface Configuration	ExtConfigrel	externalif	false	false	
Internal Interface Configuration	IntConfig			false	false
Interface Configuration	InConfigrel	internalif	false	false	

步驟5.建立合約並將「Scope」欄位修改為Tenant，如下圖所示：



The screenshot shows the Cisco ISE configuration page for a contract named 'PERMIT_ALL'. The left sidebar shows a tree view with 'Contracts' highlighted. The main area shows the 'Properties' section for the contract. The 'Scope' dropdown menu is open and set to 'Tenant', which is highlighted with a green box. Other fields include 'Label', 'QoS Class' (set to 'Unspecified'), 'Target DSCP' (set to 'unspecified'), and 'Description' (set to 'optional'). The 'Subjects' table shows one subject named 'PERMIT_ALL' with filters 'T1/PERMIT_ALL'.

步驟6.如圖所示，建立L4-L7服務圖模板，其中服務圖關聯涉及外部路由網路策略和路由器配置與裝置選擇策略的關聯。

:

ALL TENANTS | Add Tenant | Search: enter name, descr | common | T1 | info | mgmt

Tenant T1

Quick Start

- Tenant T1
 - Application Profiles
 - Networking
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services
 - L4-L7 Service Graph Templates
 - ASA5585_SGT
 - Function Node - N1
 - Router configurations
 - Function Profiles
 - L4-L7 Devices
 - Imported Devices
 - Devices Selection Policies
 - Deployed Graph Instances
 - Deployed Devices
 - Inband Management Configuration for L4-L7 devices
 - Device Managers
 - Chassis

L4-L7 Service Graph Template - ASA5585_SGT

Topology Policy

ASA5585 Information

Firewall: Routed Transparent

Profile: ASA5585_FP

Create L4-L7 Service Graph Template

Drag device clusters to create graph nodes.

Device Clusters

- T1 /ASA5585 (Managed Firewall)

Graph Name: ASA5585_SGT

Graph Type: Create A New One Clone An Existing One

Please drag a device from devices table and drop it here to create a service node.

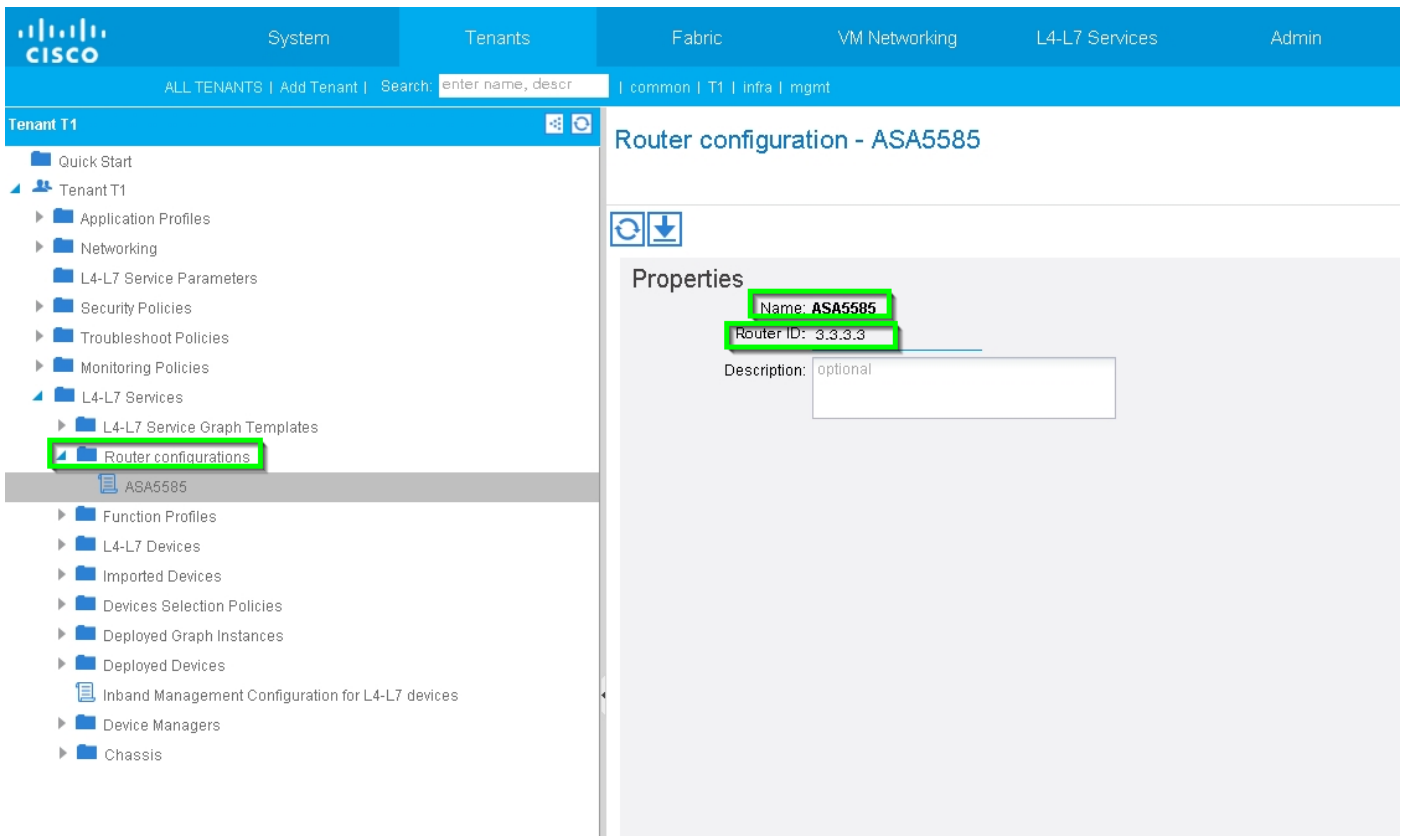
ASA5585 Information

Firewall: Routed Transparent

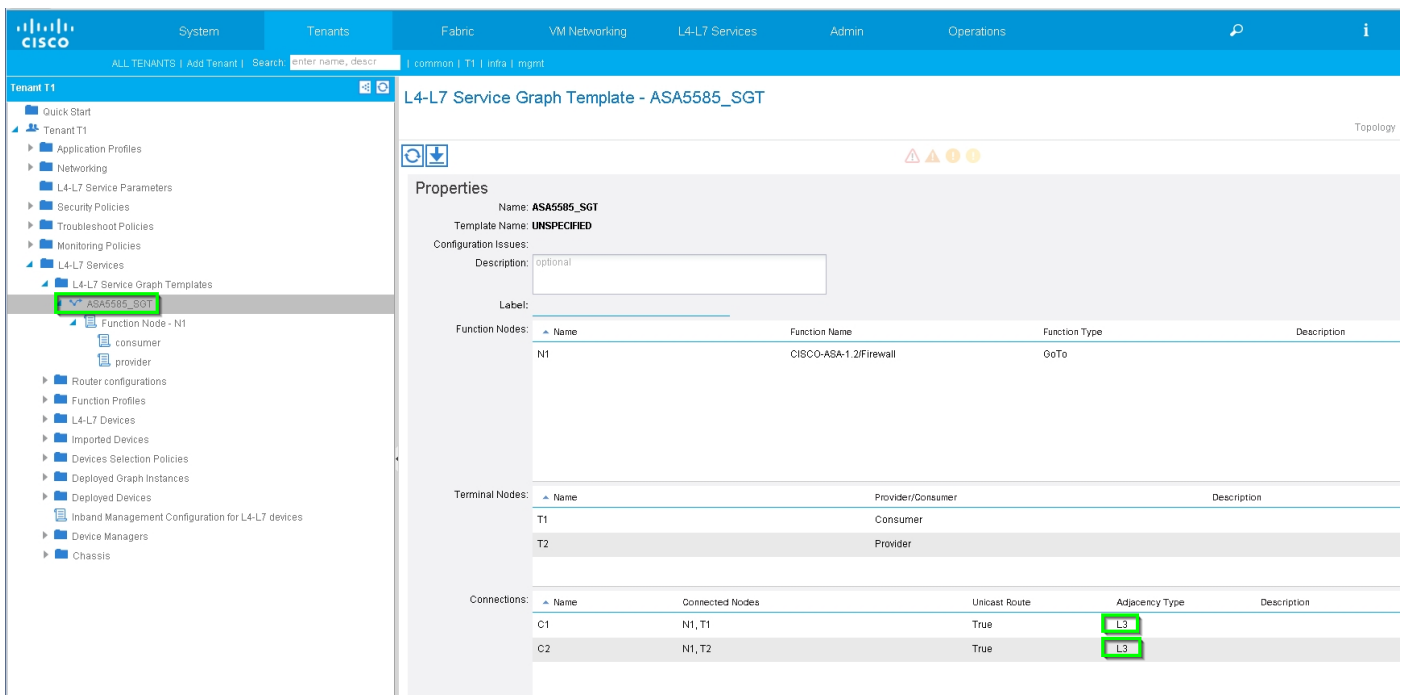
Profile: T1/ASA5585_FP/ASA5585_FP

SUBMIT CANCEL

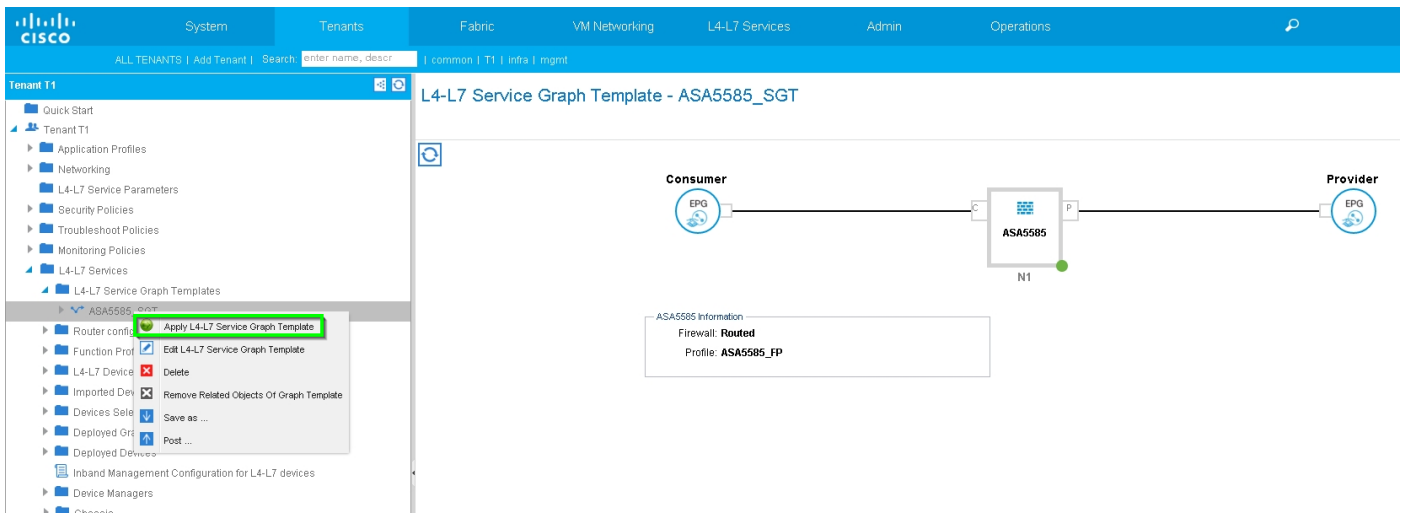
用於指定將在服務裝置(ASA 5585)上使用的路由器ID的路由器配置，如下圖所示：



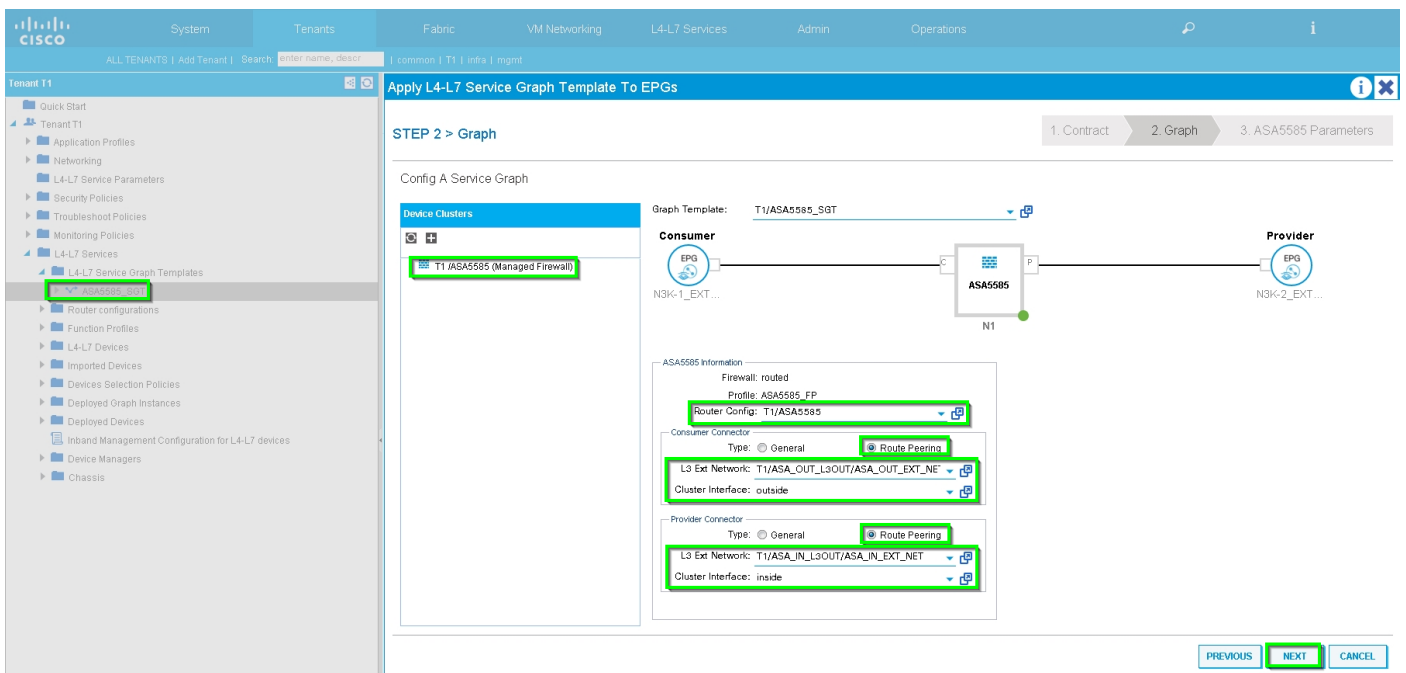
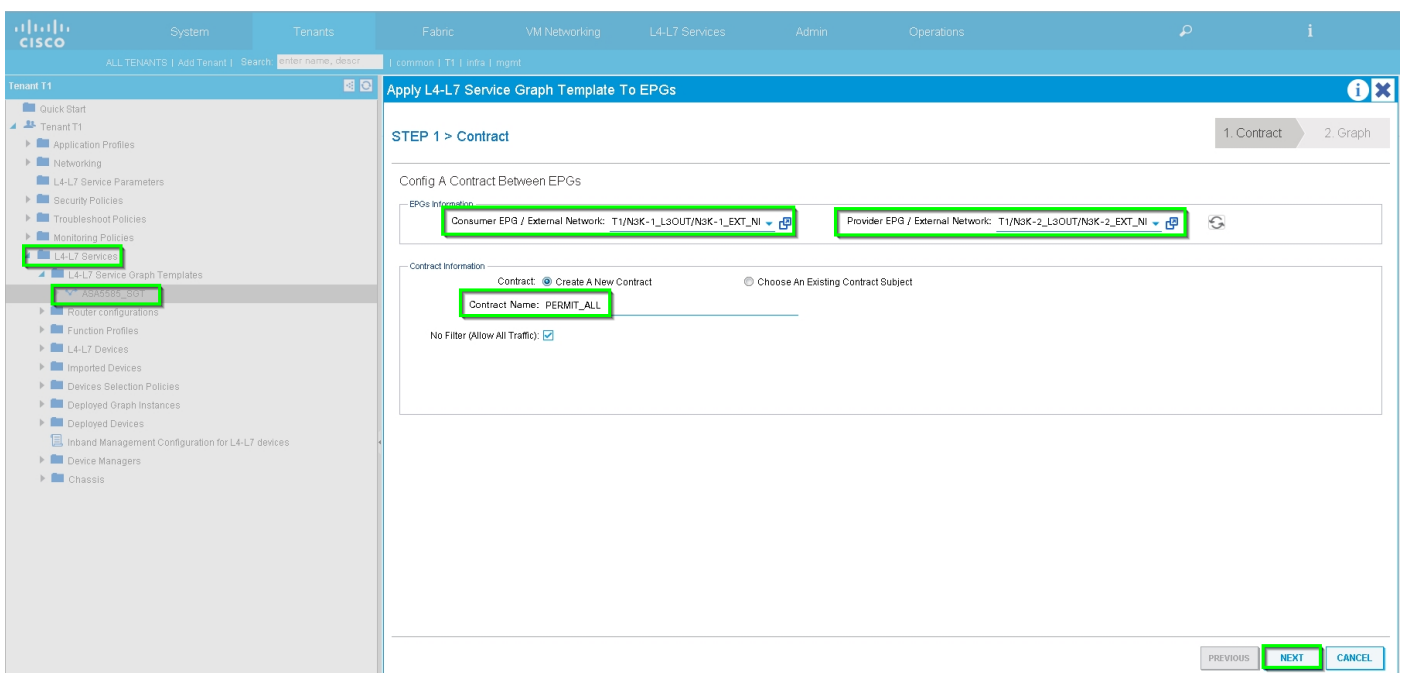
將鄰接型別從L2更改為L3，如下圖所示：



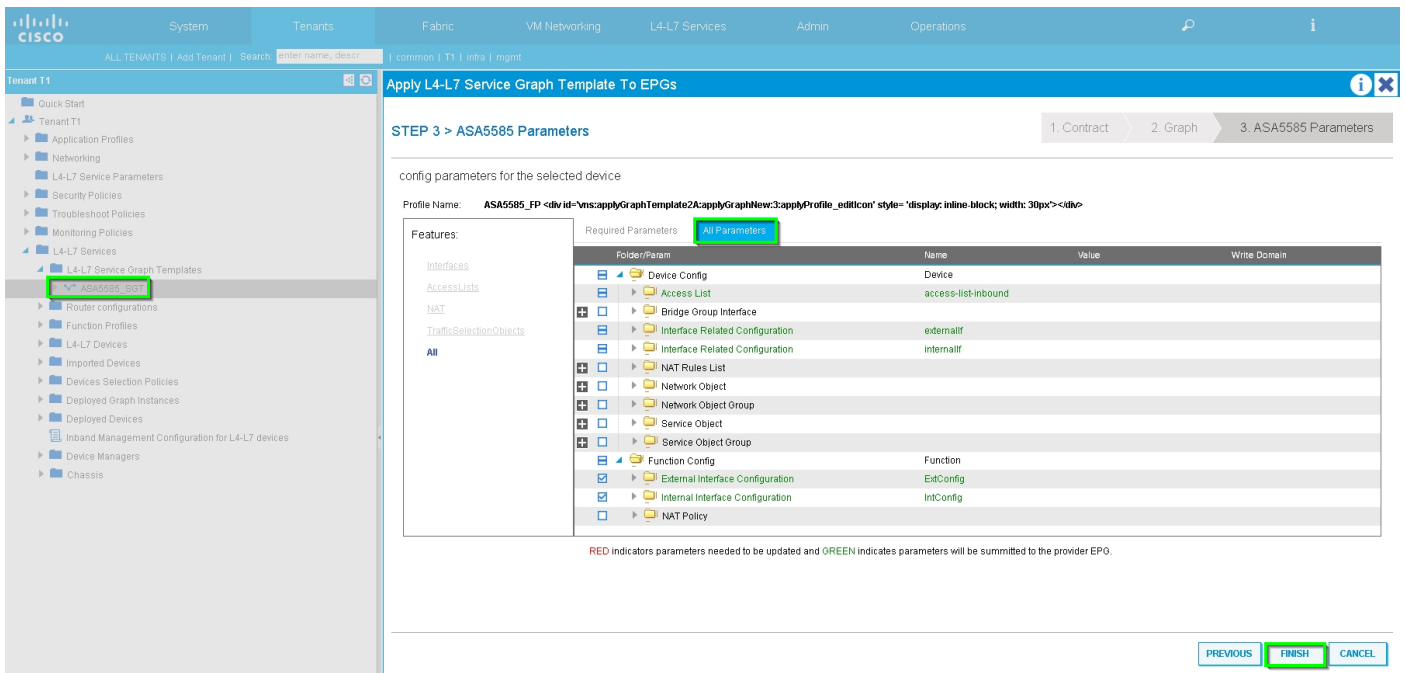
應用服務圖模板，如下圖所示：



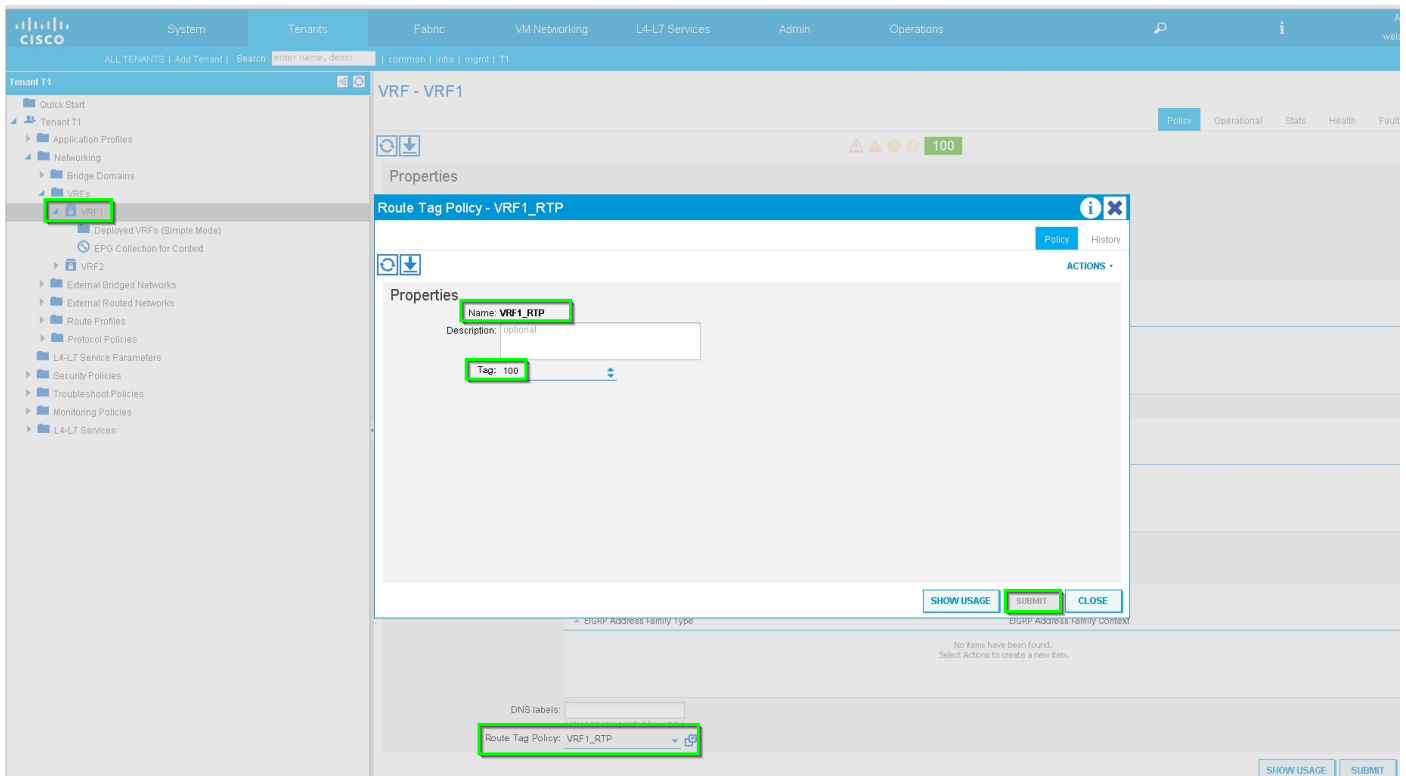
將服務圖附加到合約，如下圖所示：



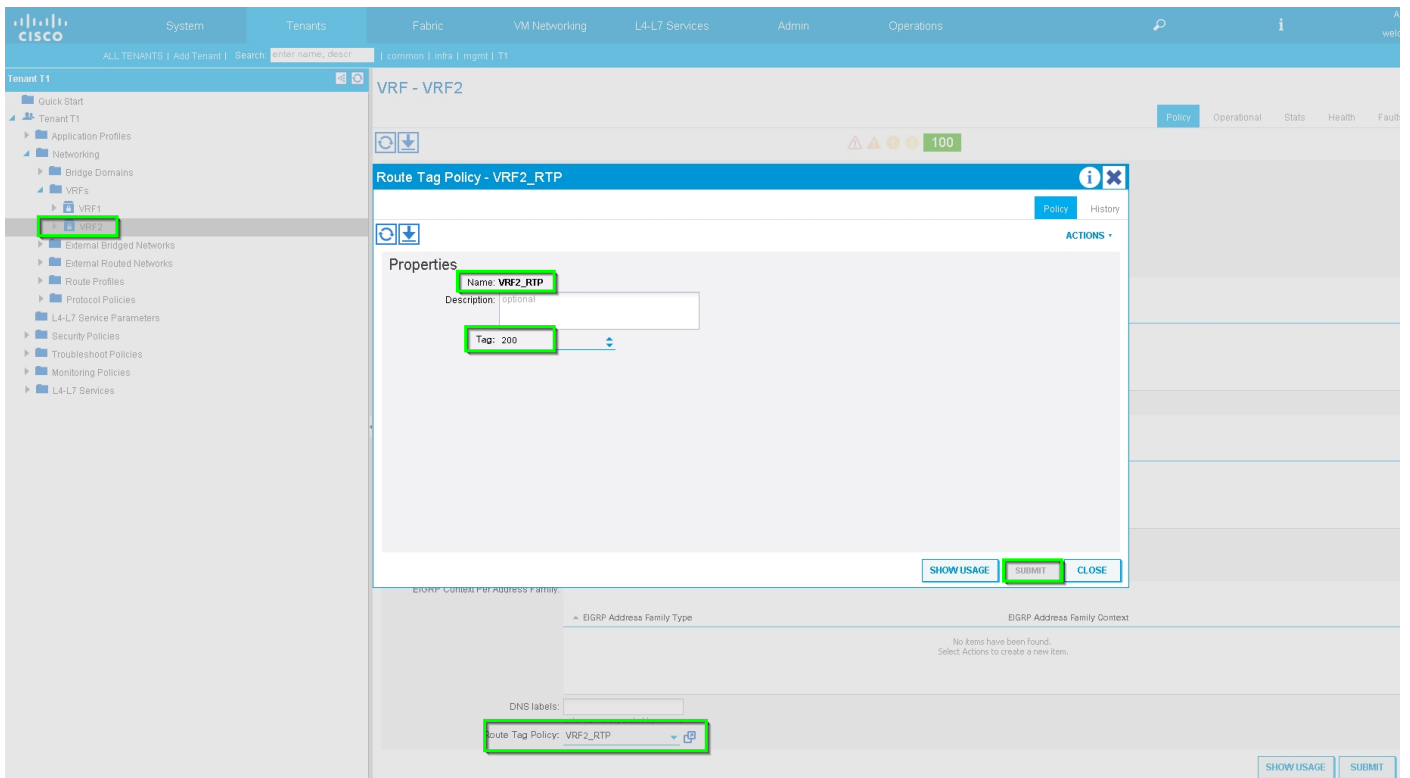
如果需要，請新增/更改L4-L7引數，如下圖所示：



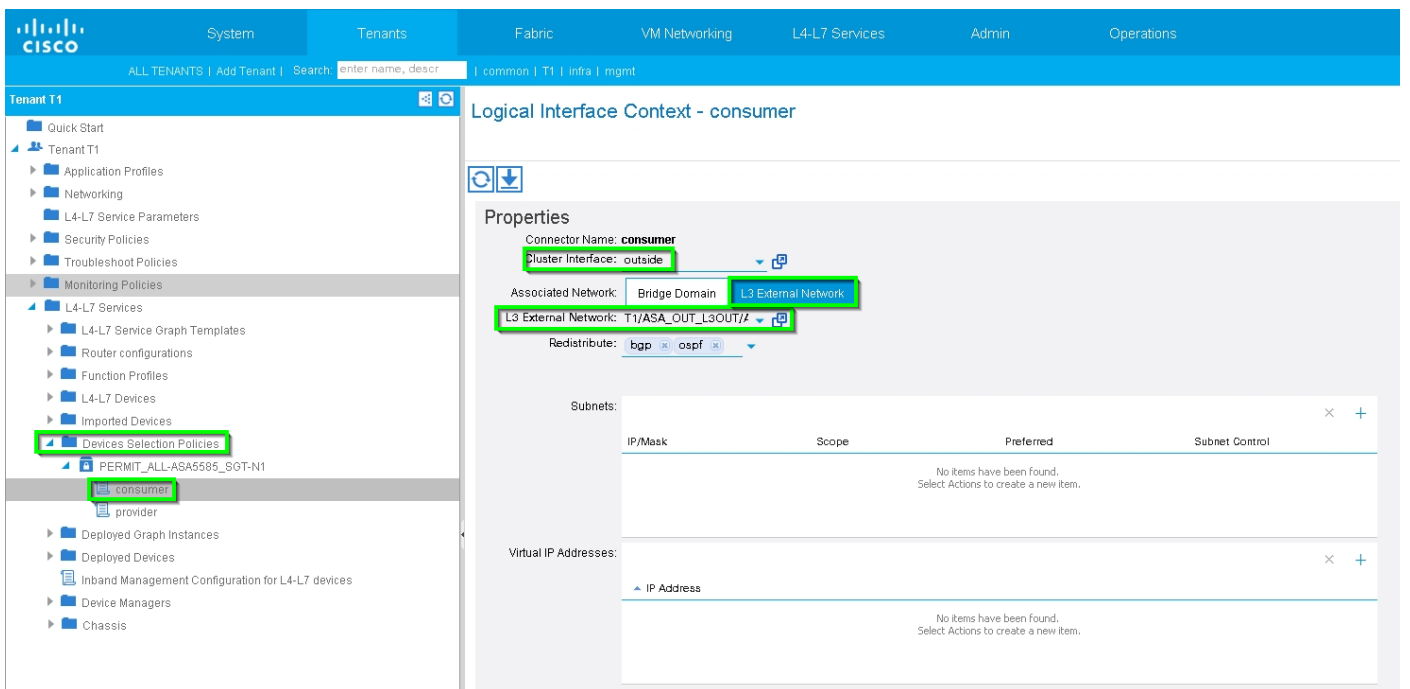
第7步：Route-tag Policy，為VRF1配置Route-tag Policy(Tag:100)，如下圖所示：



配置VRF2的路由標籤策略（標籤：200），如下圖所示：



第8步：檢查狀態並驗證裝置選擇策略，如下圖所示：



System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations

ALL TENANTS | Add Tenant | Search: enter name, descr | common | T1 | infra | mgmt

Tenant T1

- Quick Start
- Tenant T1
 - Application Profiles
 - Networking
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services
 - L4-L7 Service Graph Templates
 - Router configurations
 - Function Profiles
 - L4-L7 Devices
 - Imported Devices
 - Devices Selection Policies
 - PERMIT_ALL-ASA5585_SOT-N1
 - consumer
 - provider
 - Deployed Graph Instances
 - Deployed Devices
 - Inband Management Configuration for L4-L7 devices
 - Device Managers
 - Chassis

Logical Interface Context - provider

Properties

Connector Name: provider
 Cluster Interface: inside
 Associated Network: Bridge Domain L3 External Network
 L3 External Network: T1/ASA_IN_L3OUT/AS
 Redistribute: bgp ospf

Subnets:

IP/Mask	Scope	Preferred	Subnet Control
No items have been found. Select Actions to create a new item.			

Virtual IP Addresses:

IP Address
No items have been found. Select Actions to create a new item.

驗證已部署的圖形例項，如下圖所示：

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations

ALL TENANTS | Add Tenant | Search: enter name, descr | common | T1 | infra | mgmt

Tenant T1

- Quick Start
- Tenant T1
 - Application Profiles
 - Networking
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services
 - L4-L7 Service Graph Templates
 - Router configurations
 - Function Profiles
 - L4-L7 Devices
 - Imported Devices
 - Devices Selection Policies
 - PERMIT_ALL-ASA5585_SOT-N1
 - consumer
 - provider
 - Deployed Graph Instances
 - PERMIT_ALL-ASA5585_SOT-T1
 - Function Node-N1
 - Deployed Devices
 - Inband Management Configuration for L4-L7 devices
 - Device Managers
 - Chassis

Function Node - N1

Policy | Faults | Hist

Properties

Name: N1
 Function Type: GoTo
 Devices: ASA5585

Cluster Interfaces:

Name	Concrete Interfaces	Encap
inside	ASA5585_Device_1(0)igabitEthernet0/1	unknown
outside	ASA5585_Device_1(0)igabitEthernet0/0	unknown

Function Connectors:

Name	Encap	Class ID
consumer	vlan-101	32773
provider	vlan-102	49156

Folders And Parameters

Basic Parameters | All Parameters

Meta Folder/Param Key	Name	Value	Override Name/Value To
Features:			

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations

ALL TENANTS | Add Tenant | Search: enter name, descr | common | T1 | infra | mgmt

Tenant T1

Deployed Devices

Device Name	VRF
ASA5585	none

System | Tenants | Fabric | VM Networking | L4-L7 Services | Admin | Operations

ALL TENANTS | Add Tenant | Search: enter name, descr | common | T1 | infra | mgmt

Tenant T1

Device OSPF Configurations

Name	Enable	Context Name	Address Family	Area	Area Control	Area Type	Networks
ASA_IN_L3OUT_area_0	True	VRF2	IPv4	Backbone area	Send redistributed LSAs into NSSA area Originate customer LSA	Regular area	ASA_IN_EXT_NET (10.10.10.0/24)
ASA_OUT_L3OUT_area_0	True	VRF1	IPv4	Backbone area	Send redistributed LSAs into NSSA area Originate summary LSA	Regular area	ASA_OUT_EXT_NET (20.20.20.0/24)

驗證和疑難排解

租戶的APIC配置：

```
apic1# sh running-config tenant T1
# Command: show running-config tenant T1
# Time: Thu Feb 25 16:05:14 2016
tenant T1
```

```
access-list PERMIT_ALL
  match ip
  exit
contract PERMIT_ALL
  scope tenant
  subject PERMIT_ALL
    access-group PERMIT_ALL both
    1417 graph ASA5585_SGT
  exit
exit
vrf context VRF1
  exit
vrf context VRF2
  exit
l3out ASA_IN_L3OUT
  vrf member VRF2
  exit
l3out ASA_OUT_L3OUT
  vrf member VRF1
  exit
l3out N3K-1_L3OUT
  vrf member VRF1
  exit
l3out N3K-2_L3OUT
  vrf member VRF2
  exit
bridge-domain BD1
  vrf member VRF1
  exit
bridge-domain BD2
  vrf member VRF2
  exit
application AP1
  epg EPG1
    bridge-domain member BD1
  exit
  epg EPG2
    bridge-domain member BD2
  exit
exit
external-l3 epg ASA_IN_EXT_NET l3out ASA_IN_L3OUT
  vrf member VRF2
  match ip 10.10.10.0/24
  exit
external-l3 epg ASA_OUT_EXT_NET l3out ASA_OUT_L3OUT
  vrf member VRF1
  match ip 20.20.20.0/24
  exit
external-l3 epg N3K-1_EXT_NET l3out N3K-1_L3OUT
  vrf member VRF1
  match ip 10.10.10.0/24
  contract consumer PERMIT_ALL
  exit
external-l3 epg N3K-2_EXT_NET l3out N3K-2_L3OUT
  vrf member VRF2
  match ip 20.20.20.0/24
  contract provider PERMIT_ALL
  exit
interface bridge-domain BD1
  exit
interface bridge-domain BD2
  exit
1417 cluster name ASA5585 type physical vlan-domain T1_PHY service FW function go-to
  cluster-device ASA5585_Device_1
```

```

cluster-interface inside
  member device ASA5585_Device_1 device-interface GigabitEthernet0/1
  interface ethernet 1/2 leaf 106
  exit
exit
cluster-interface outside
  member device ASA5585_Device_1 device-interface GigabitEthernet0/0
  interface ethernet 1/2 leaf 105
  exit
exit
exit
1417 graph ASA5585_SGT contract PERMIT_ALL
  service N1 device-cluster-tenant T1 device-cluster ASA5585 mode FW_ROUTED
  connector consumer cluster-interface outside
    1417-peer tenant T1 out ASA_OUT_L3OUT epg ASA_OUT_EXT_NET redistribute bgp,ospf
  exit
  connector provider cluster-interface inside
    1417-peer tenant T1 out ASA_IN_L3OUT epg ASA_IN_EXT_NET redistribute bgp,ospf
  exit
  rtr-cfg ASA5585
  exit
  connection C1 terminal consumer service N1 connector consumer
  connection C2 terminal provider service N1 connector provider
  exit
rtr-cfg ASA5585
  router-id 3.3.3.3
  exit
exit
apic1#

```

驗證枝葉101上的OSPF鄰居關係和路由表：

```

leaf101# show ip ospf neighbors vrf T1:VRF1
OSPF Process ID default VRF T1:VRF1
Total number of neighbors: 2
Neighbor ID      Pri State                Up Time  Address      Interface
1.1.1.1          1 FULL/BDR              02:07:19 192.168.1.1  Vlan8
3.3.3.3          1 FULL/BDR              00:38:35 192.168.1.5  Vlan9

leaf101# show ip route vrf T1:VRF1
IP Route Table for VRF "T1:VRF1"
'*' denotes best ucast next-hop
*** denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.10.0/24, ubest/mbest: 1/0
  *via 192.168.1.1, vlan8, [110/8], 01:59:50, ospf-default, intra
20.20.20.0/24, ubest/mbest: 1/0
  *via 192.168.1.5, vlan9, [110/22], 00:30:20, ospf-default, inter
100.100.100.100/32, ubest/mbest: 2/0, attached, direct
  *via 100.100.100.100, lo1, [1/0], 02:21:22, local, local
  *via 100.100.100.100, lo1, [1/0], 02:21:22, direct
192.168.1.0/30, ubest/mbest: 1/0, attached, direct
  *via 192.168.1.2, vlan8, [1/0], 02:35:53, direct
192.168.1.2/32, ubest/mbest: 1/0, attached
  *via 192.168.1.2, vlan8, [1/0], 02:35:53, local, local
192.168.1.4/30, ubest/mbest: 1/0, attached, direct
  *via 192.168.1.6, vlan9, [1/0], 02:20:53, direct
192.168.1.6/32, ubest/mbest: 1/0, attached
  *via 192.168.1.6, vlan9, [1/0], 02:20:53, local, local

```

```
192.168.1.8/30, ubest/mbest: 1/0
  *via 192.168.1.5, vlan9, [110/14], 00:30:20, ospf-default, intra
200.200.200.200/32, ubest/mbest: 1/0
  *via 192.168.1.5, vlan9, [110/15], 00:30:20, ospf-default, intra
```

驗證枝葉102上的OSPF鄰居關係和路由表：

```
leaf102# show ip ospf neighbors vrf T1:VRF2
OSPF Process ID default VRF T1:VRF2
Total number of neighbors: 2
Neighbor ID      Pri State           Up Time  Address      Interface
3.3.3.3          1 FULL/BDR         00:37:07 192.168.1.9  Vlan14
2.2.2.2          1 FULL/BDR         02:09:59 192.168.1.13 Vlan15
```

```
leaf102# show ip route vrf T1:VRF2
IP Route Table for VRF "T1:VRF2"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
```

```
10.10.10.0/24, ubest/mbest: 1/0
  *via 192.168.1.9, vlan14, [110/22], 00:35:22, ospf-default, inter
20.20.20.0/24, ubest/mbest: 1/0
  *via 192.168.1.13, vlan15, [110/8], 02:08:13, ospf-default, intra
192.168.1.4/30, ubest/mbest: 1/0
  *via 192.168.1.9, vlan14, [110/14], 00:35:22, ospf-default, intra
192.168.1.8/30, ubest/mbest: 1/0, attached, direct
  *via 192.168.1.10, vlan14, [1/0], 02:14:29, direct
192.168.1.10/32, ubest/mbest: 1/0, attached
  *via 192.168.1.10, vlan14, [1/0], 02:14:29, local, local
192.168.1.12/30, ubest/mbest: 1/0, attached, direct
  *via 192.168.1.14, vlan15, [1/0], 02:09:04, direct
192.168.1.14/32, ubest/mbest: 1/0, attached
  *via 192.168.1.14, vlan15, [1/0], 02:09:04, local, local
200.200.200.200/32, ubest/mbest: 2/0, attached, direct
  *via 200.200.200.200, lo4, [1/0], 02:10:02, local, local
  *via 200.200.200.200, lo4, [1/0], 02:10:02, direct
```

驗證ASA 5585上的配置、OSPF鄰居關係和路由表：

```
ASA5585# sh run interface
!
interface GigabitEthernet0/0
  no nameif
  security-level 0
  no ip address
!
interface GigabitEthernet0/0.101
  nameif externalIf
  security-level 50
  ip address 192.168.1.5 255.255.255.252
!
interface GigabitEthernet0/1
  no nameif
  security-level 100
  no ip address
!
interface GigabitEthernet0/1.102
  nameif internalIf
```

```
security-level 100
ip address 192.168.1.9 255.255.255.252
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 172.23.97.1 255.255.254.0
```

```
ASA5585# sh run router
router ospf 1
router-id 3.3.3.3
network 192.168.1.4 255.255.255.252 area 0
network 192.168.1.8 255.255.255.252 area 0
area 0
log-adj-changes
!
```

```
ASA5585# sh ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
100.100.100.100	1	FULL/DR	0:00:38	192.168.1.6	externalIf
200.200.200.200	1	FULL/DR	0:00:33	192.168.1.10	internalIf

```
ASA5585# sh route ospf
```

```
Routing Table: T1
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set
```

```
O IA    10.10.10.0 255.255.255.0
        [110/18] via 192.168.1.6, 00:22:57, externalIf
O IA    20.20.20.0 255.255.255.0
        [110/18] via 192.168.1.10, 00:22:47, internalIf
O       200.200.200.200 255.255.255.255
        [110/11] via 192.168.1.10, 00:22:47, internalIf
```

```
ASA5585# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
        alert-interval 300
access-list access-list-inbound; 3 elements; name hash: 0xcb5bd6c7
access-list access-list-inbound line 1 extended permit tcp any any eq www (hitcnt=0) 0xc873a747
access-list access-list-inbound line 2 extended permit tcp any any eq https (hitcnt=0)
0x48bedbdd
```

```
access-list access-list-inbound line 3 extended permit icmp any any (hitcnt=6) 0xe4b5a75d
```

驗證N3K-1上的配置、OSPF鄰居關係和路由表:

```

N3K-1# sh run ospf

!Command: show running-config ospf
!Time: Thu Feb 25 15:40:55 2016

version 6.0(2)U3(7)
feature ospf

router ospf 1
  router-id 1.1.1.1

interface Ethernet1/21
  ip router ospf 1 area 0.0.0.1

interface Ethernet1/47
  ip router ospf 1 area 0.0.0.1

N3K-1# sh ip ospf neighbors
OSPF Process ID 1 VRF default
Total number of neighbors: 1
Neighbor ID      Pri State                Up Time  Address      Interface
100.100.100.100  1 FULL/DR              01:36:24 192.168.1.2  Eth1/47

N3K-1# sh ip ospf route
OSPF Process ID 1 VRF default, Routing Table
(D) denotes route is directly attached      (R) denotes route is in RIB
10.10.10.0/24 (intra)(D) area 0.0.0.1
  via 10.10.10.0/Eth1/21* , cost 4
20.20.20.0/24 (inter)(R) area 0.0.0.1
  via 192.168.1.2/Eth1/47 , cost 62
100.100.100.100/32 (intra)(R) area 0.0.0.1
  via 192.168.1.2/Eth1/47 , cost 41
192.168.1.0/30 (intra)(D) area 0.0.0.1
  via 192.168.1.1/Eth1/47* , cost 40

```

驗證N3K-2上的配置、OSPF鄰居關係和路由表:

```

N3K-2# sh run ospf

!Command: show running-config ospf
!Time: Thu Feb 25 15:44:47 2016

version 6.0(2)U3(7)
feature ospf

router ospf 1
  router-id 2.2.2.2

interface loopback0
  ip ospf network point-to-point
  ip router ospf 1 area 0.0.0.0

interface Ethernet1/21
  ip router ospf 1 area 0.0.0.1

interface Ethernet1/47
  ip router ospf 1 area 0.0.0.1

```

```
N3K-2# sh ip ospf neighbors
OSPF Process ID 1 VRF default
Total number of neighbors: 1
Neighbor ID      Pri State                Up Time  Address      Interface
200.200.200.200  1 FULL/DR              01:43:50 192.168.1.14 Eth1/47
```

```
N3K-2# sh ip ospf route
OSPF Process ID 1 VRF default, Routing Table
(D) denotes route is directly attached (R) denotes route is in RIB
2.2.2.0/30 (intra)(D) area 0.0.0.0
  via 2.2.2.0/Lo0* , cost 1
10.10.10.0/24 (inter)(R) area 0.0.0.1
  via 192.168.1.14/Eth1/47 , cost 62
20.20.20.0/24 (intra)(D) area 0.0.0.1
  via 20.20.20.0/Eth1/21* , cost 4
192.168.1.12/30 (intra)(D) area 0.0.0.1
  via 192.168.1.13/Eth1/47* , cost 40
```

驗證枝葉和資料包命中計數上的合約過濾器規則：。

```
leaf101# show system internal policy-mgr stats
Requested Rule Statistics
[ CUT ]
Rule (4107) DN (sys/actrl/scope-3112964/rule-3112964-s-32773-d-49158-f-33) Ingress: 1316,
Egress: 0, Pkts: 0 RevPkts: 0
Rule (4108) DN (sys/actrl/scope-3112964/rule-3112964-s-49158-d-32773-f-33) Ingress: 1317,
Egress: 0, Pkts: 0 RevPkts: 0
```

```
leaf101# show system internal policy-mgr stats
Requested Rule Statistics
[ CUT ]
Rule (4107) DN (sys/actrl/scope-3112964/rule-3112964-s-32773-d-49158-f-33) Ingress: 2317,
Egress: 0, Pkts: 0 RevPkts: 0
Rule (4108) DN (sys/actrl/scope-3112964/rule-3112964-s-49158-d-32773-f-33) Ingress: 2317,
Egress: 0, Pkts: 0 RevPkts: 0
```

```
leaf102# show system internal policy-mgr stats Requested Rule Statistics [ CUT ] Rule (4103) DN
(sys/actrl/scope-2752520/rule-2752520-s-49156-d-6019-f-default) Ingress: 3394, Egress: 0, Pkts:
0 RevPkts: 0 Rule (4104) DN (sys/actrl/scope-2752520/rule-2752520-s-6019-d-49156-f-default)
Ingress: 3394, Egress: 0, Pkts: 0 RevPkts: 0 [ CUT ] leaf102# show system internal policy-mgr
stats Requested Rule Statistics [ CUT ] Rule (4103) DN (sys/actrl/scope-2752520/rule-2752520-s-
49156-d-6019-f-default) Ingress: 4392, Egress: 0, Pkts: 0 RevPkts: 0 Rule (4104) DN
(sys/actrl/scope-2752520/rule-2752520-s-6019-d-49156-f-default) Ingress: 4392, Egress: 0, Pkts:
0 RevPkts: 0 [ CUT ]
```

N3K-1與N3K-2的可達性測試：

```
N3K-1# ping 20.20.20.1 source 10.10.10.1
PING 20.20.20.1 (20.20.20.1) from 10.10.10.1: 56 data bytes
64 bytes from 20.20.20.1: icmp_seq=0 ttl=250 time=2.098 ms
64 bytes from 20.20.20.1: icmp_seq=1 ttl=250 time=0.922 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=250 time=0.926 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=250 time=0.893 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=250 time=0.941 ms
```

```
--- 20.20.20.1 ping statistics ---
```



```
5 packets transmitted, 5 packets received, 0.00% packet loss  
round-trip min/avg/max = 0.893/1.156/2.098 ms
```

```
N3K-2# ping 10.10.10.1 source 20.20.20.1
```

```
PING 10.10.10.1 (10.10.10.1) from 20.20.20.1: 56 data bytes
```

```
64 bytes from 10.10.10.1: icmp_seq=0 ttl=250 time=2.075 ms
```

```
64 bytes from 10.10.10.1: icmp_seq=1 ttl=250 time=0.915 ms
```

```
64 bytes from 10.10.10.1: icmp_seq=2 ttl=250 time=0.888 ms
```

```
64 bytes from 10.10.10.1: icmp_seq=3 ttl=250 time=1.747 ms
```

```
64 bytes from 10.10.10.1: icmp_seq=4 ttl=250 time=0.828 ms
```

```
--- 10.10.10.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0.00% packet loss
```

```
round-trip min/avg/max = 0.828/1.29/2.075 ms
```

附件是租戶的XML配置檔案和用於此演示的ASA功能配置檔案。