Homologation de route L4-L7 avec structure de transit - Procédure pas à pas de configuration

Contenu

Introduction

Ce document décrit la procédure pas à pas de configuration du graphique de services L4-L7 avec appairage de route, où le consommateur et le fournisseur sont tous deux externes au fabric ACI (Application Centric Infrastructure).

Contribution de Zahid Hassan, ingénieur des services avancés Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pools de VLAN statiques qui seront utilisés pour le VLAN d'encapsulation entre les périphériques externes et le fabric ACI
- Domaines physiques et routés externes qui relieront l'emplacement (noeud/chemin feuille) des périphériques externes et le pool de VLAN
- Connexion de couche 3 à un réseau externe (L3Out)

Les étapes de configuration **d'accès au fabric** et **L3Out** précédentes ne sont pas couvertes dans ce document et ont été supposées avoir déjà été effectuées.

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Contrôleur Cisco APIC (Application Policy Infrastructure Controller) - 1.2(1m)
- Package de périphériques ASA (Adaptive Security Appliance) - 1.2.4.8
- ASA 5585 - 9.5(1)
- Nexus 3064 - 6.0(2)U3(7)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

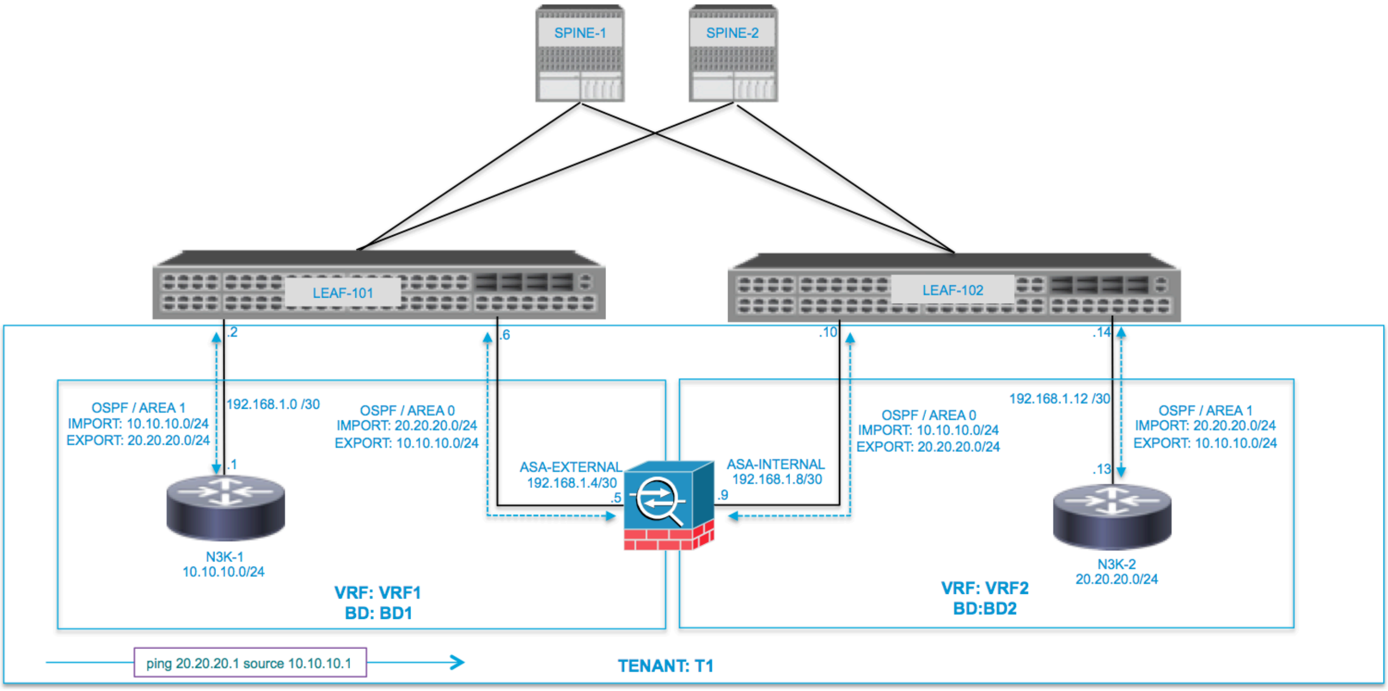
L'appairage de route est une fonctionnalité qui permet à un appareil de service tel qu'un équilibreur de charge ou un pare-feu d'annoncer son accessibilité via le fabric ACI jusqu'à un réseau externe.

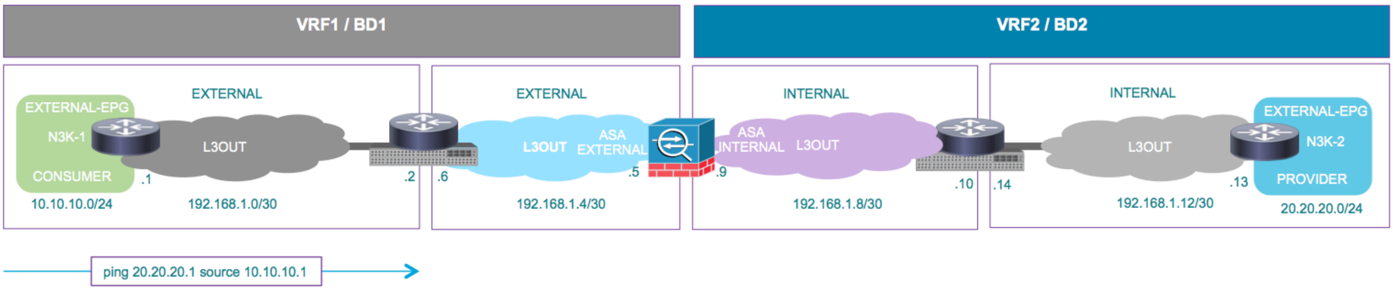
Le cas d'utilisation présenté ici est un pare-feu physique qui est déployé en tant que graphique de service à deux branches, entre deux sorties L3ou groupes de terminaux externes (EPG). Le graphique de service est associé à un contrat entre le groupe de terminaux externe sur Leaf 101 (N3K-1) et le groupe de terminaux externe sur Leaf 102 (N3K-2). Le fabric ACI fournit un service de transit pour les routeurs (N3K-1 et N3K-2) et l'appairage de route est utilisé, avec le protocole de routage OSPF (Open Shortest Path First), pour échanger des routes entre le pare-feu et le fabric ACI.

Configuration

Diagramme du réseau

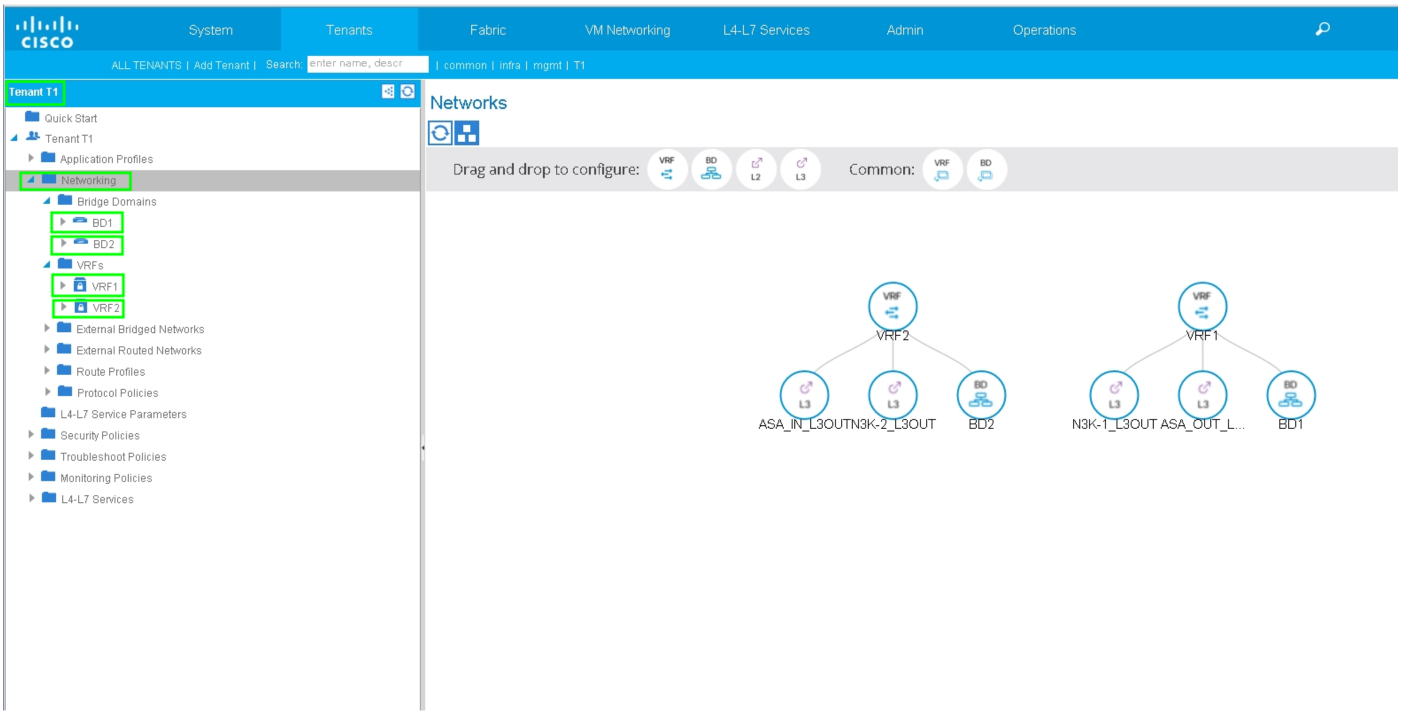
L'image suivante montre comment l'appairage de route fonctionne de bout en bout :



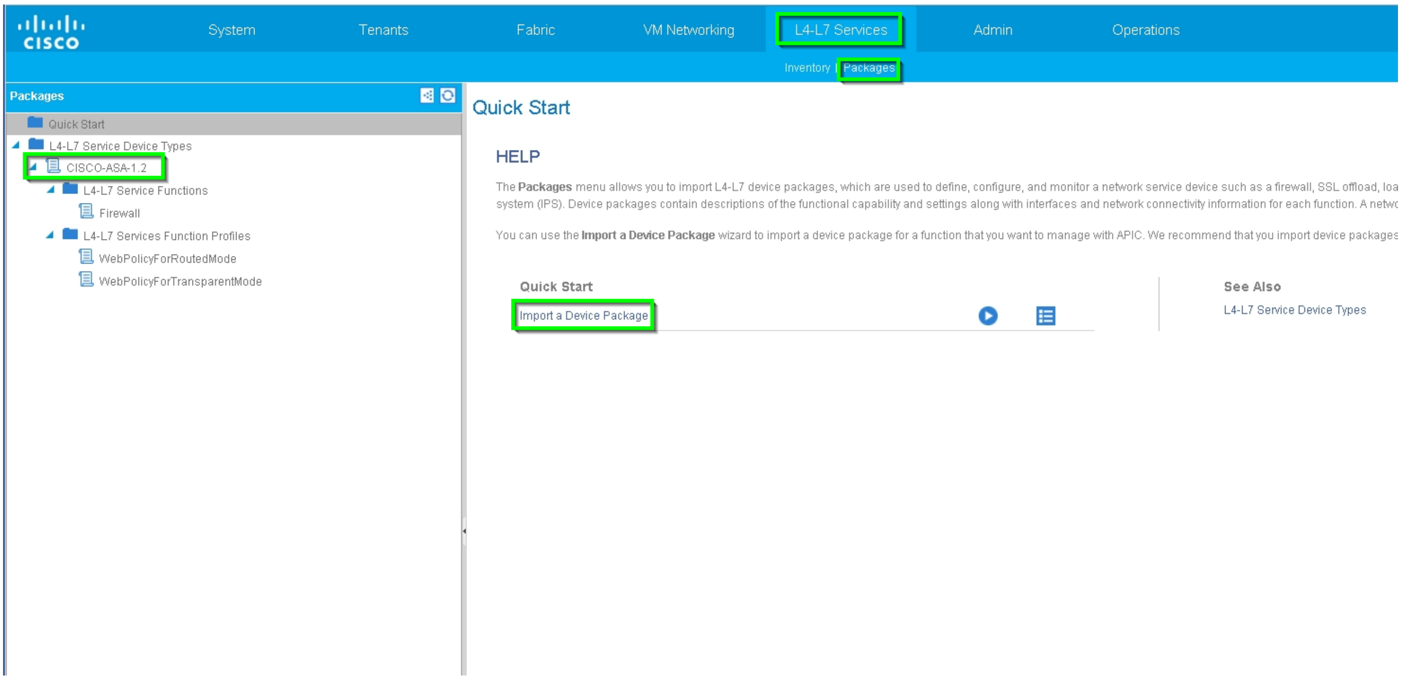


Configuration

Étape 1. Configurez Virtual Routing and Forwarding1 (VRF1), VRF2, Bridge Domain1 (BD1) et BD2. Associez BD1 à VRF1 et BD2 à VRF2, comme illustré sur l'image :



Étape 2. Téléchargez le package de périphériques ASA sous le périphérique L4-L7, comme l'illustre l'image :

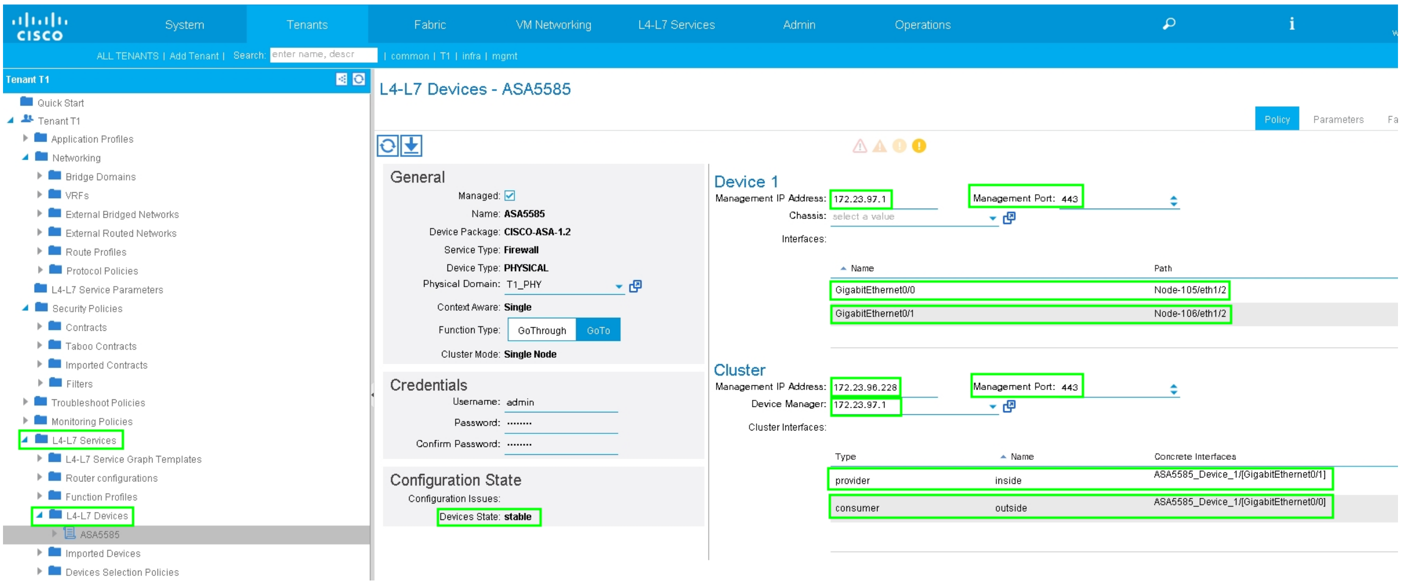


HELP

The **Packages** menu allows you to import L4-L7 device packages, which are used to define, configure, and monitor a network service device such as a firewall, SSL offload, loa system (IPS). Device packages contain descriptions of the functional capability and settings along with interfaces and network connectivity information for each function. A netwo

You can use the **Import a Device Package** wizard to import a device package for a function that you want to manage with APIC. We recommend that you import device packages

Configurez le périphérique L4-L7 pour l'ASA 5585 physique (routé), comme indiqué sur l'image :



L4-L7 Devices - ASA5585

General

Managed: ☑

Name: **ASA5585**

Device Package: **CISCO-ASA-1.2**

Service Type: **Firewall**

Device Type: **PHYSICAL**

Physical Domain: T1_PHY

Context Aware: **Single**

Function Type: GoThrough [✓ GoTo]

Cluster Mode: **Single Node**

Credentials

Username: admin

Password: ········

Confirm Password: ········

Configuration State

Configuration Issues:

Devices State: **stable**

Device 1

Management IP Address: 172.23.97.1 Management Port: 443

Chassis: select a value

Interfaces:

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

Cluster

Management IP Address: 172.23.96.228 Management Port: 443

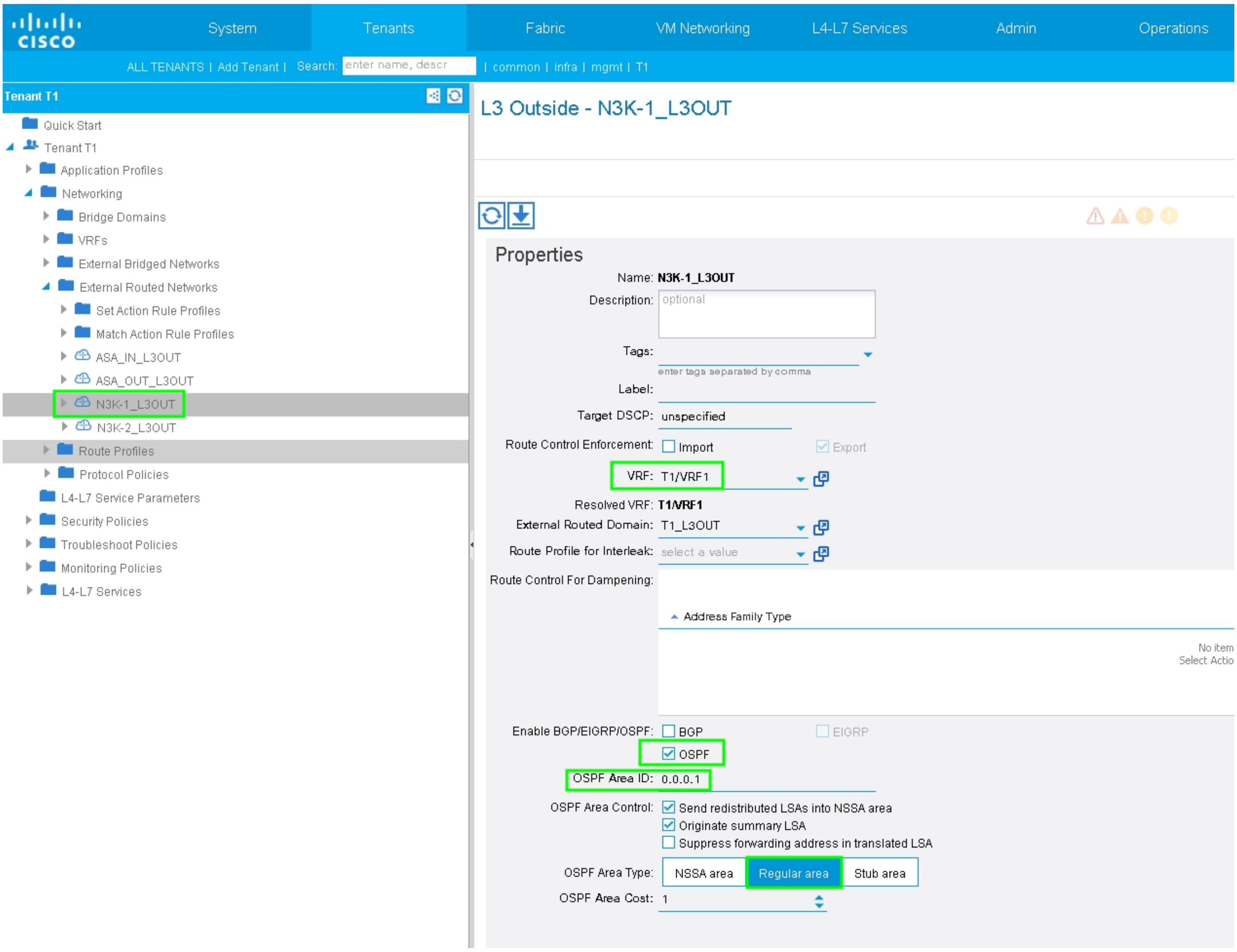
Device Manager: 172.23.97.1

Cluster Interfaces:

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

Étape 3. Configurez L3Out pour N3K-1 et associez-vous à BD1 et VRF1.

Le réseau routé externe est utilisé pour spécifier la configuration de routage dans le fabric ACI pour l'appairage de route, comme l'illustre l'image :



L3 Outside - N3K-1_L3OUT

Properties

Name: N3K-1_L3OUT

Description: optional

Tags: enter tags separated by comma

Label:

Target DSCP: unspecified

Route Control Enforcement: □ Import ☑ Export

VRF: T1/VRF1

Resolved VRF: T1/VRF1

External Routed Domain: T1_L3OUT

Route Profile for Interleak: select a value

Route Control For Dampening:

Address Family Type

No item
Select Actio

Enable BGP/EIGRP/OSPF: □ BGP □ EIGRP
☑ OSPF

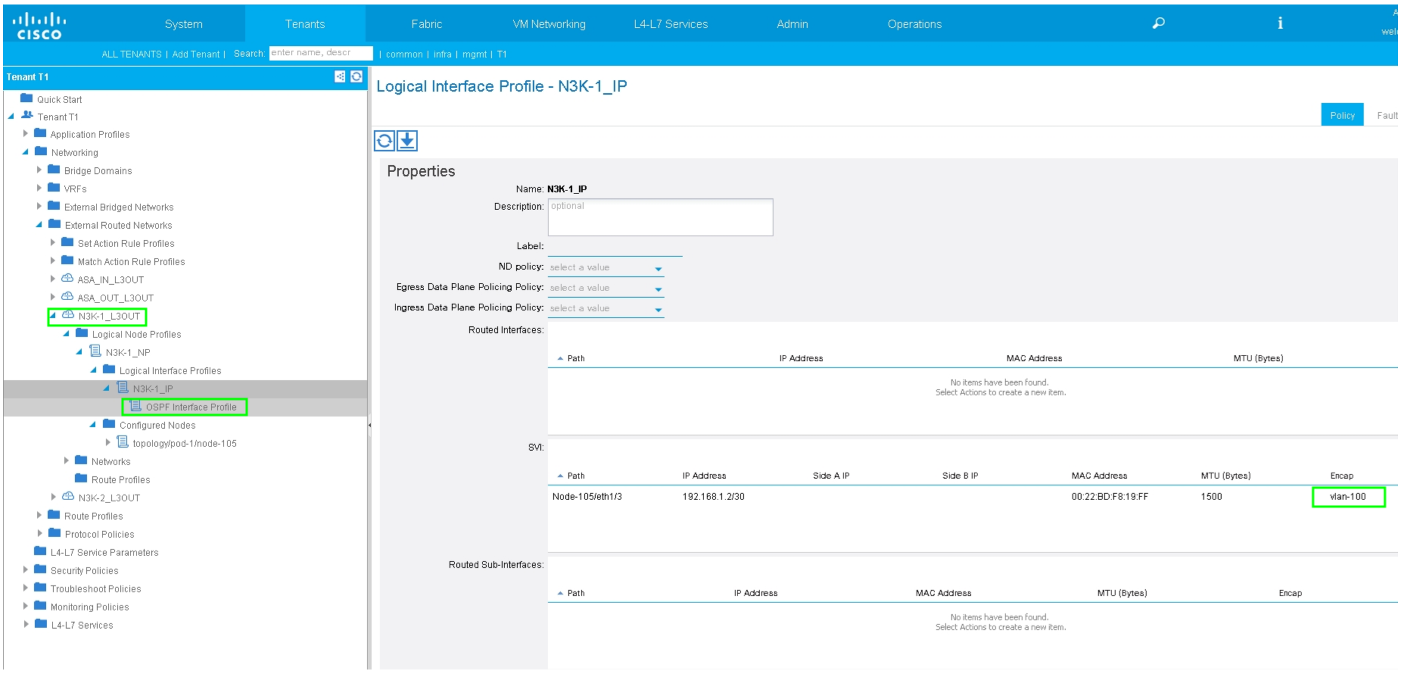
OSPF Area ID: 0.0.0.1

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

Note: Toutes les interfaces L3Out utilisées pour l'appairage de route doivent être configurées en tant qu'interface virtuelle de commutateur (SVI) avec un encap VLAN en conséquence.



Logical Interface Profile - N3K-1_IP

Properties

Name: N3K-1_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:

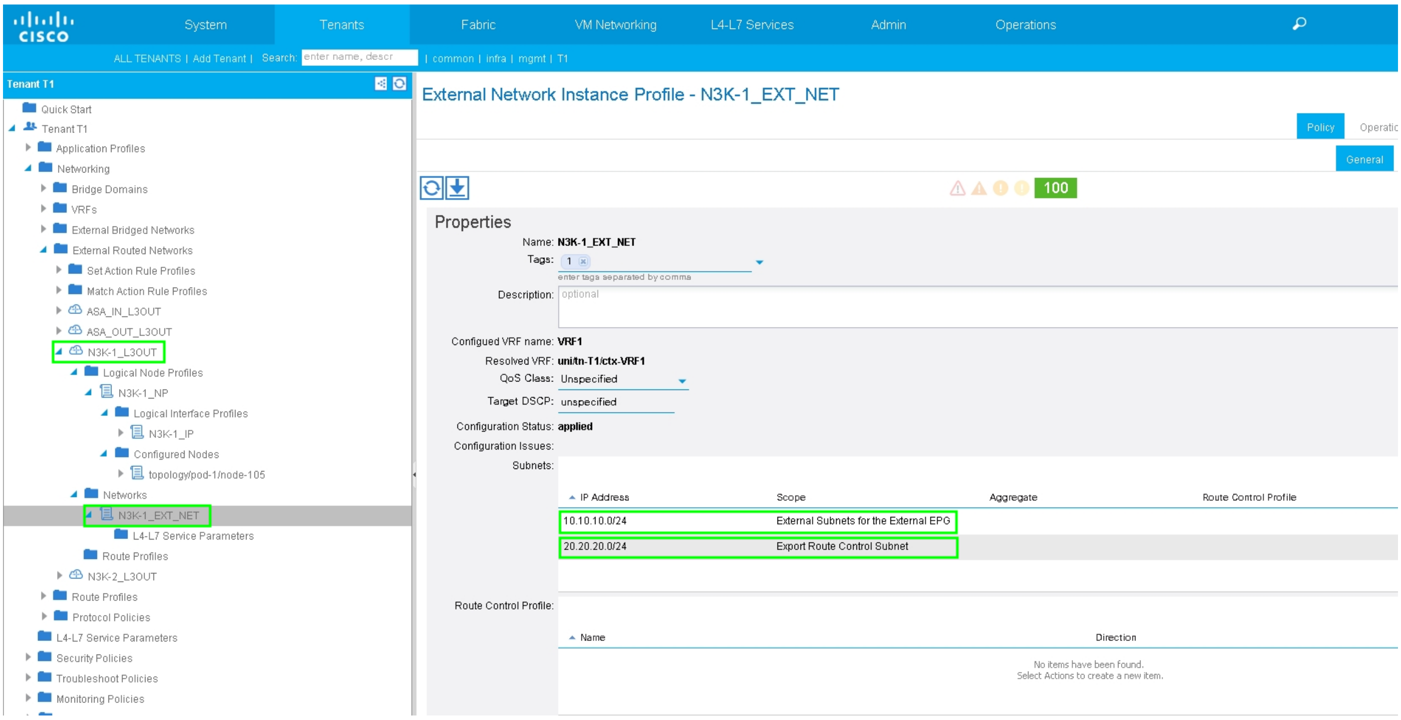
Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-105/eth1/3	192.168.1.2/30			00:22:BD:F8:19:FF	1500	vlan-100

Routed Sub-Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)	Encap

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

Configurez le contrôle de route d'importation/exportation sur les sous-réseaux pour l'EPG externe N3K-1 L3Out, comme illustré dans l'image :



External Network Instance Profile - N3K-1_EXT_NET

Properties

Name: N3K-1_EXT_NET

Tags: 1

enter tags separated by comma

Description: optional

Configued VRF name: VRF1

Resolved VRF: uni/tn-T1/ctx-VRF1

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: applied

Configuration Issues:

Subnets:

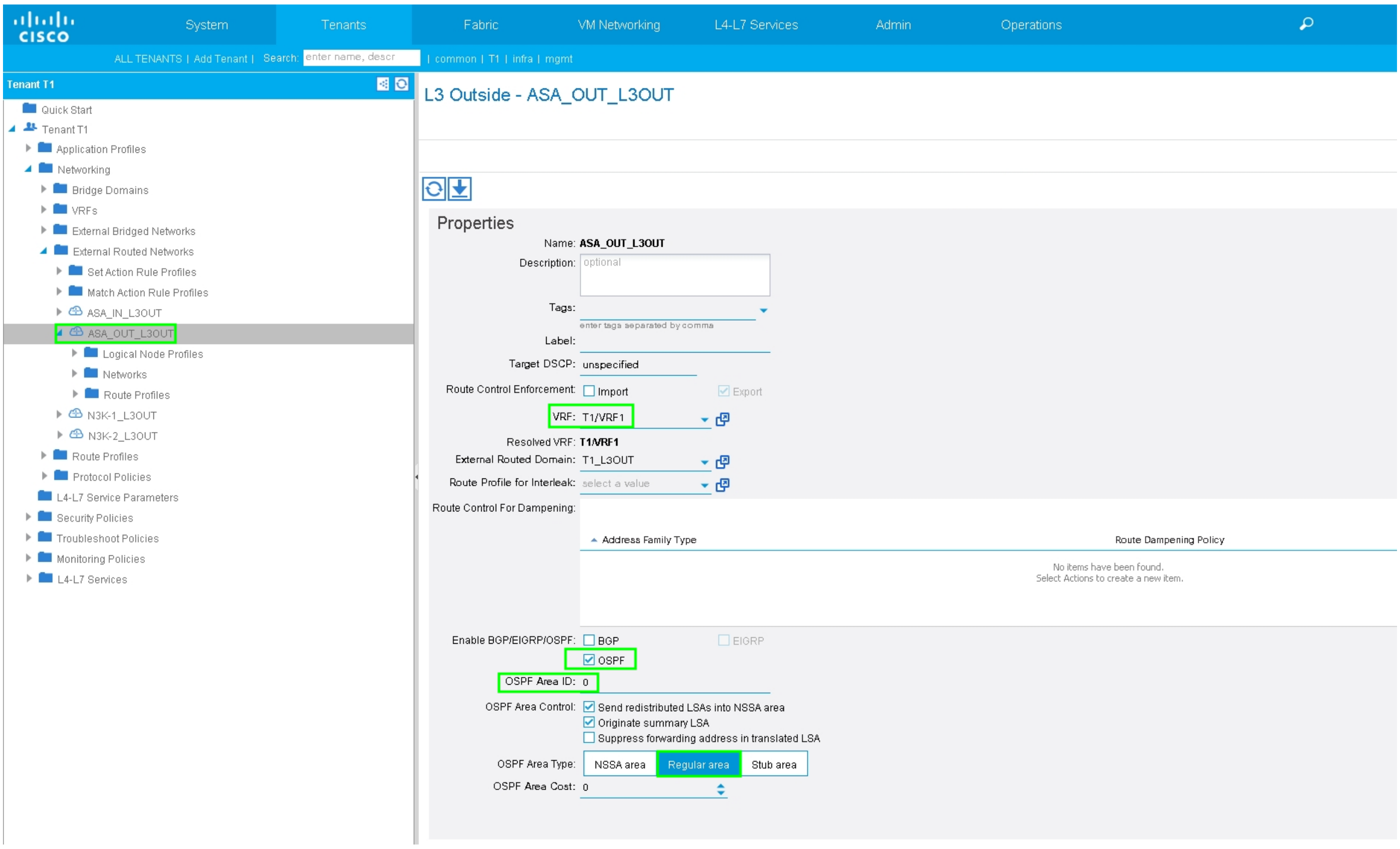
IP Address	Scope	Aggregate	Route Control Profile
10.10.10.0/24	External Subnets for the External EPG		
20.20.20.0/24	Export Route Control Subnet		

Route Control Profile:

Name	Direction

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

Configurez L3Out pour l'interface externe ASA et associez-vous à BD1 et VRF1, comme illustré dans l'image :



L3 Outside - ASA_OUT_L3OUT

Properties

Name: ASA_OUT_L3OUT

Description: optional

Tags:

enter tags separated by comma

Label:

Target DSCP: unspecified

Route Control Enforcement: □ Import ☑ Export

VRF: T1/VRF1

Resolved VRF: T1/VRF1

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.

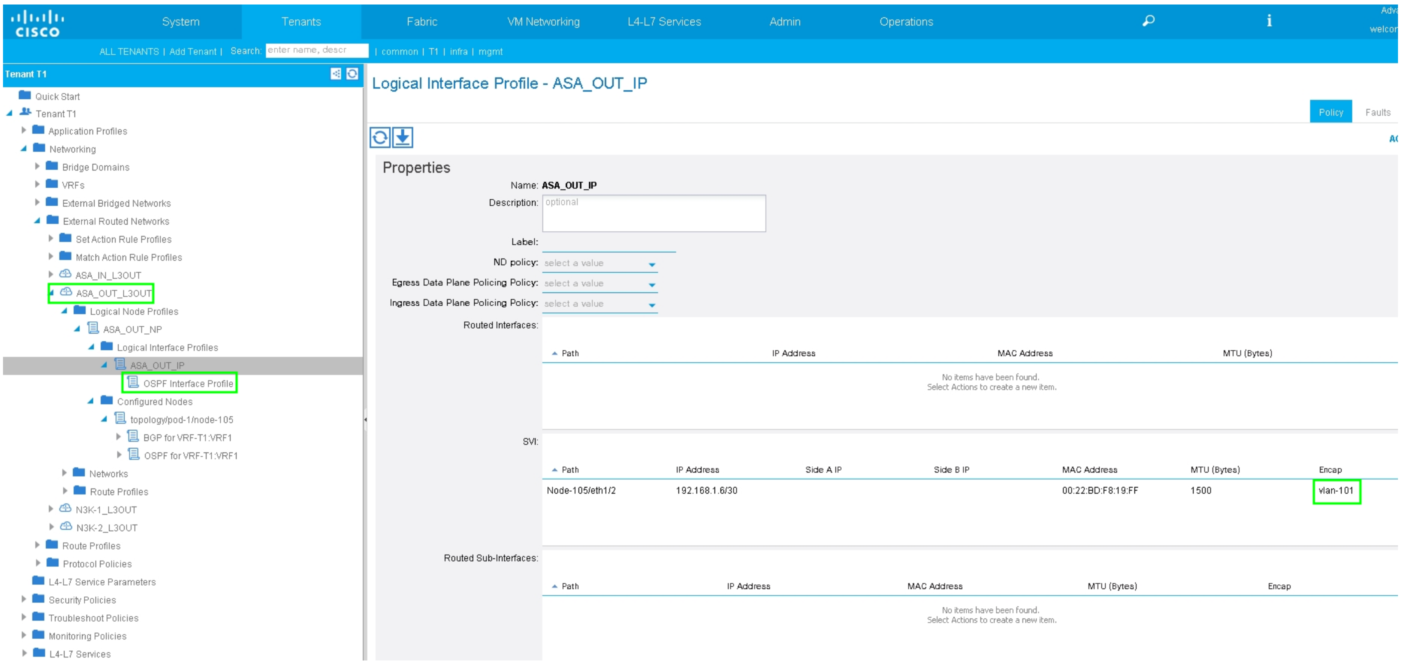
Enable BGP/EIGRP/OSPF: □ BGP □ EIGRP ☑ OSPF

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:

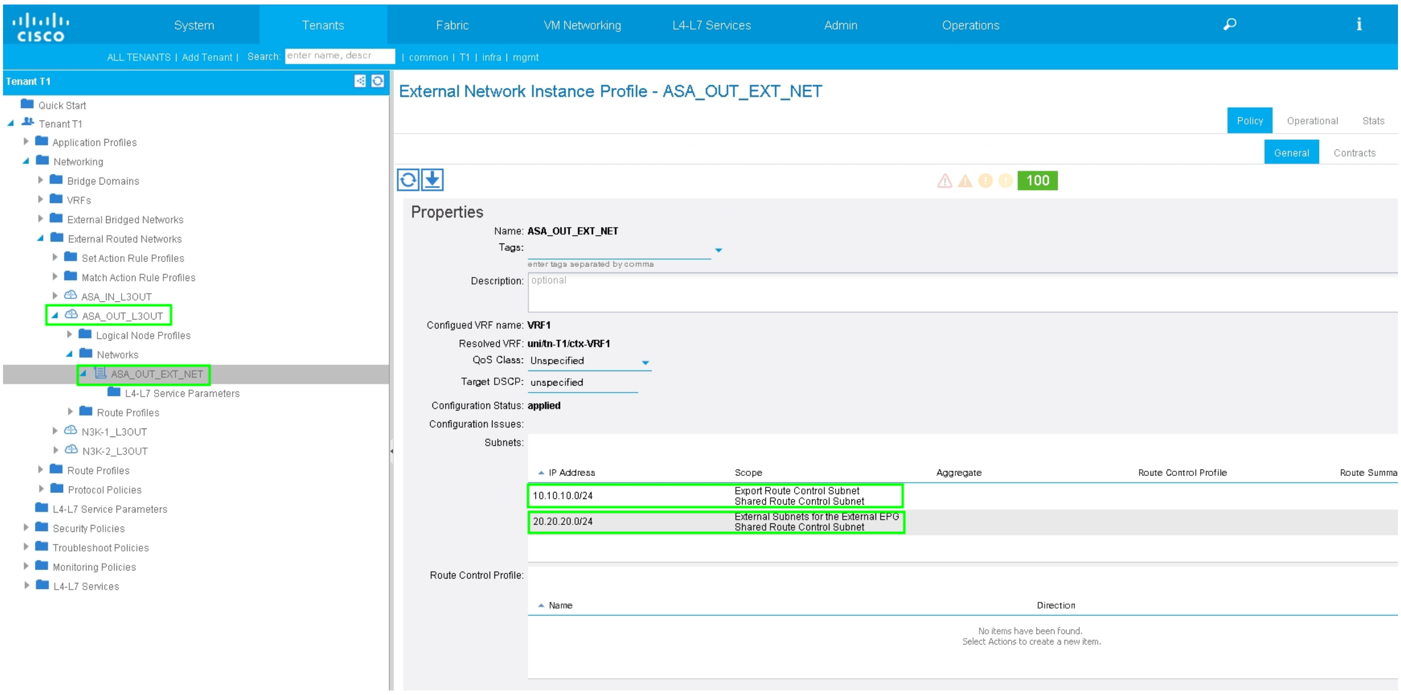
Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-105/eth1/2	192.168.1.6/30			00:22:BD:F8:19:FF	1500	vlan-101

Routed Sub-Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)	Encap

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

Configurez le contrôle de route Import/Export sur les sous-réseaux pour l'EPG externe L3Out ASA-External, comme illustré dans l'image :



External Network Instance Profile - ASA_OUT_EXT_NET

Properties

Name: ASA_OUT_EXT_NET

Tags: enter tags separated by comma

Description: optional

Configued VRF name: VRF1

Resolved VRF: uni/tn-T1/ctx-VRF1

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: applied

Configuration Issues:

Subnets:

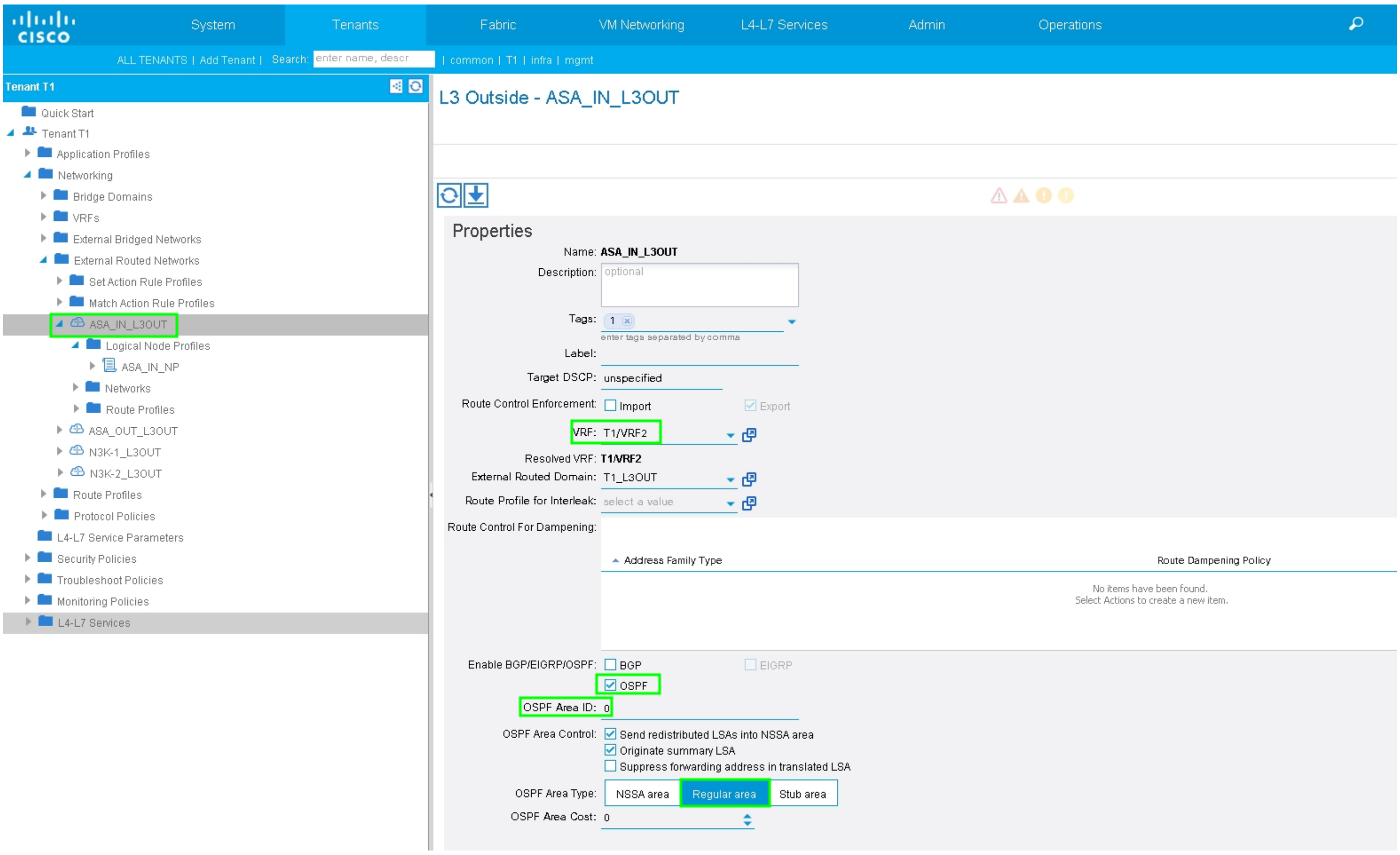
IP Address	Scope	Aggregate	Route Control Profile	Route Summa
10.10.10.0/24	Export Route Control Subnet Shared Route Control Subnet			
20.20.20.0/24	External Subnets for the External EPG Shared Route Control Subnet			

Route Control Profile:

Name	Direction

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

Configurez L3out pour ASA-Internal et associez-le à BD2 et VRF2, comme illustré dans l'image :



L3 Outside - ASA_IN_L3OUT

Properties

Name: ASA_IN_L3OUT

Description: optional

Tags: 1 ×

enter tags separated by comma

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.	

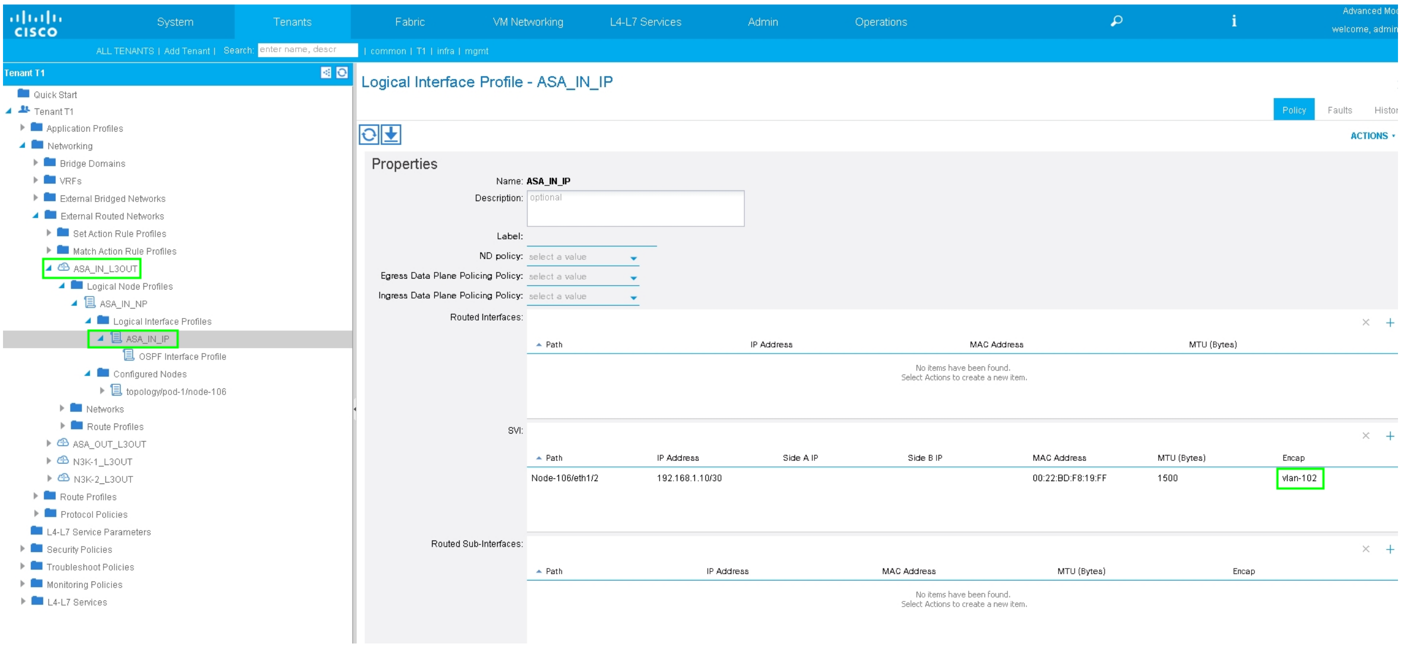
Enable BGP/EIGRP/OSPF: □ BGP □ EIGRP ☑ OSPF

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_IN_IP

Properties

Name: ASA_IN_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.			

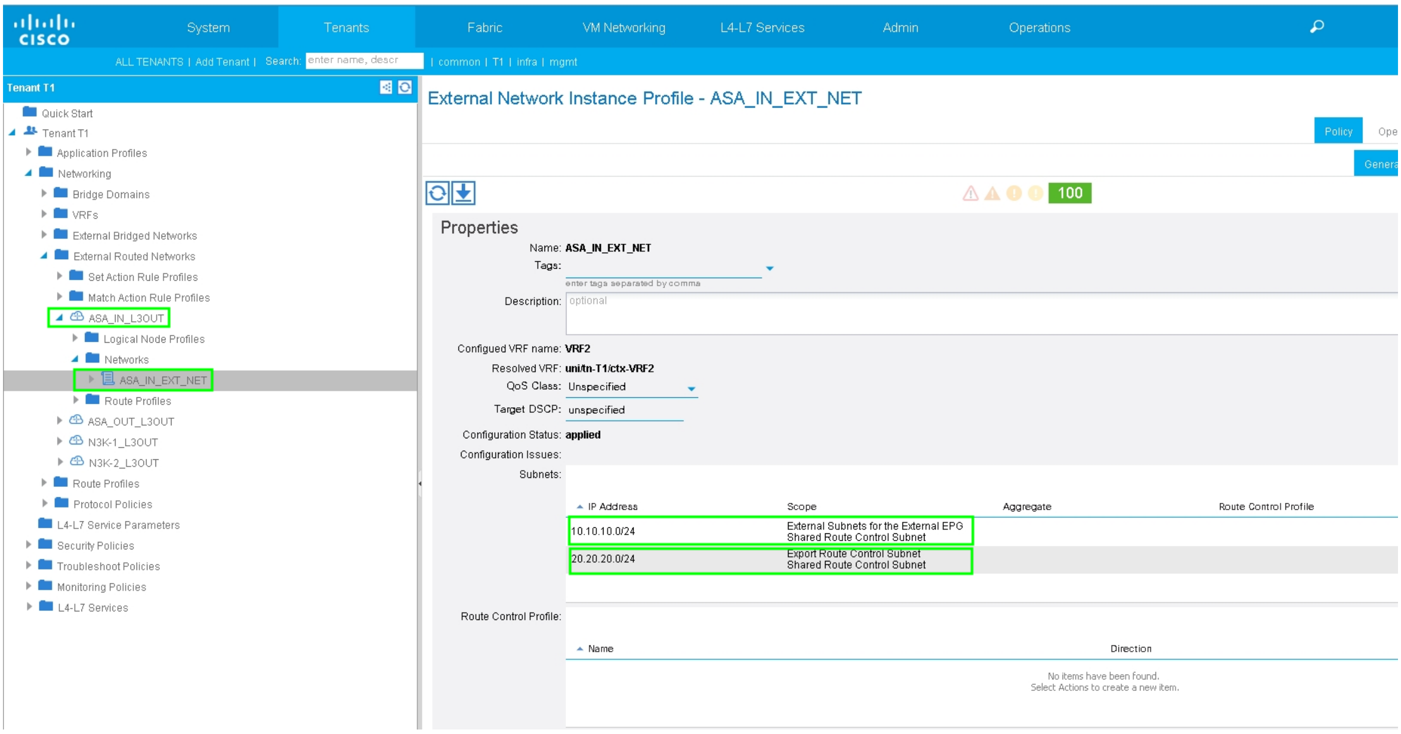
SVI:

Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-106/eth1/2	192.168.1.10/30			00:22:BD:F8:19:FF	1500	vlan-102

Routed Sub-Interfaces:

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

Configurez le contrôle de route Import/Export sur les sous-réseaux pour l'EPG externe L3Out interne ASA, comme illustré dans l'image :



External Network Instance Profile - ASA_IN_EXT_NET

Properties

Name: **ASA_IN_EXT_NET**

Tags:

enter tags separated by comma

Description: optional

Configued VRF name: **VRF2**

Resolved VRF: **uni/tn-T1/ctx-VRF2**

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: **applied**

Configuration Issues:

Subnets:

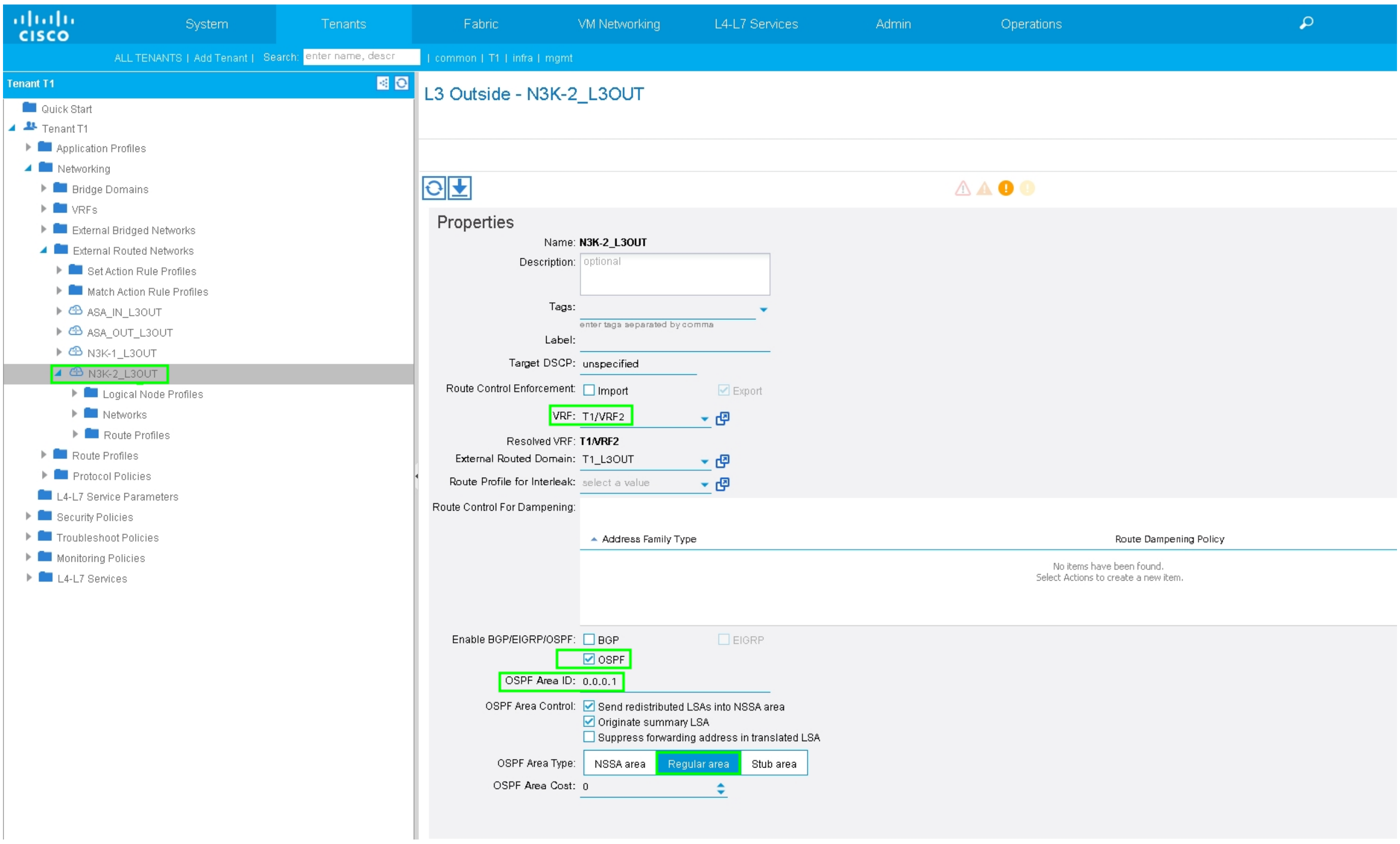
IP Address	Scope	Aggregate	Route Control Profile
10.10.10.0/24	External Subnets for the External EPG Shared Route Control Subnet		
20.20.20.0/24	Export Route Control Subnet Shared Route Control Subnet		

Route Control Profile:

Name	Direction

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

Configurez L3Out pour N3K-2 et associez-vous à BD2 et VRF2, comme illustré dans l'image :



L3 Outside - N3K-2_L3OUT

Properties

Name: **N3K-2_L3OUT**

Description: optional

Tags:

enter tags separated by comma

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 □ EIGRP

☑ OSPF

OSPF Area ID: 0.0.0.1

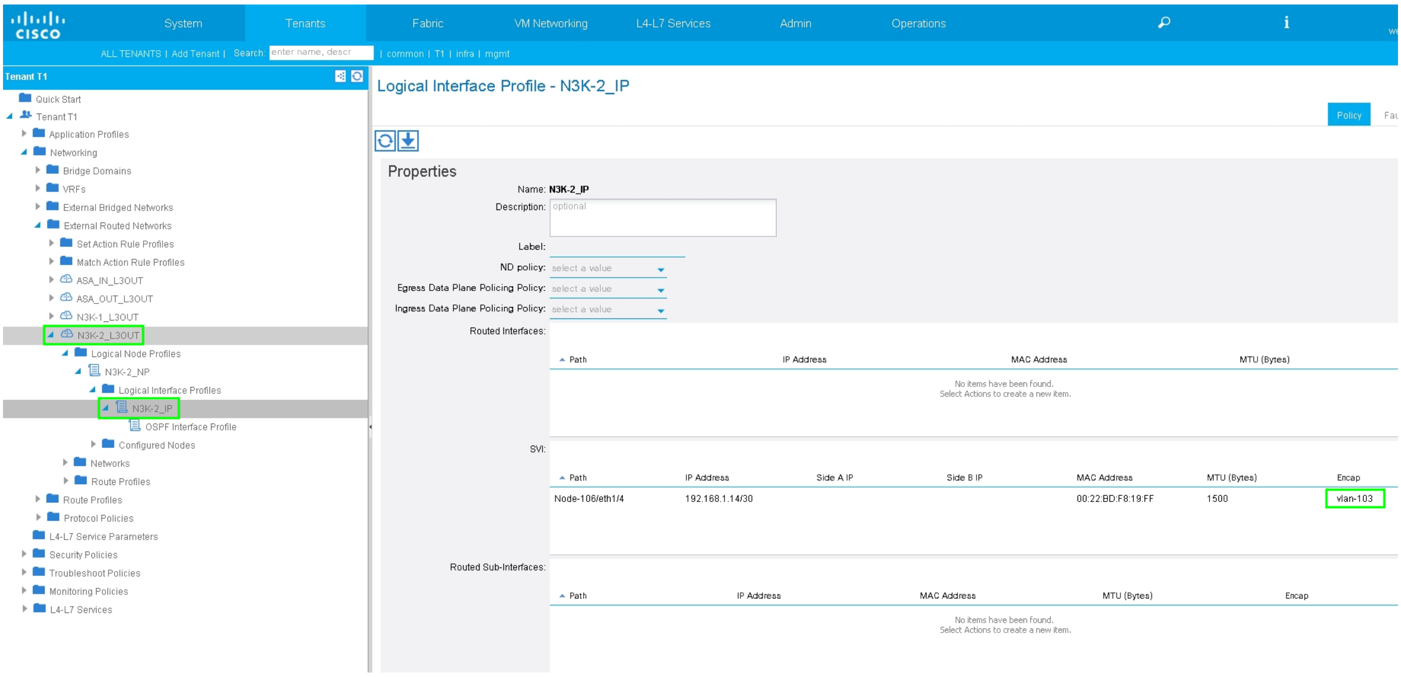
OSPF Area Control: ☑ Send redistributed LSAs into NSSA area

☑ 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:

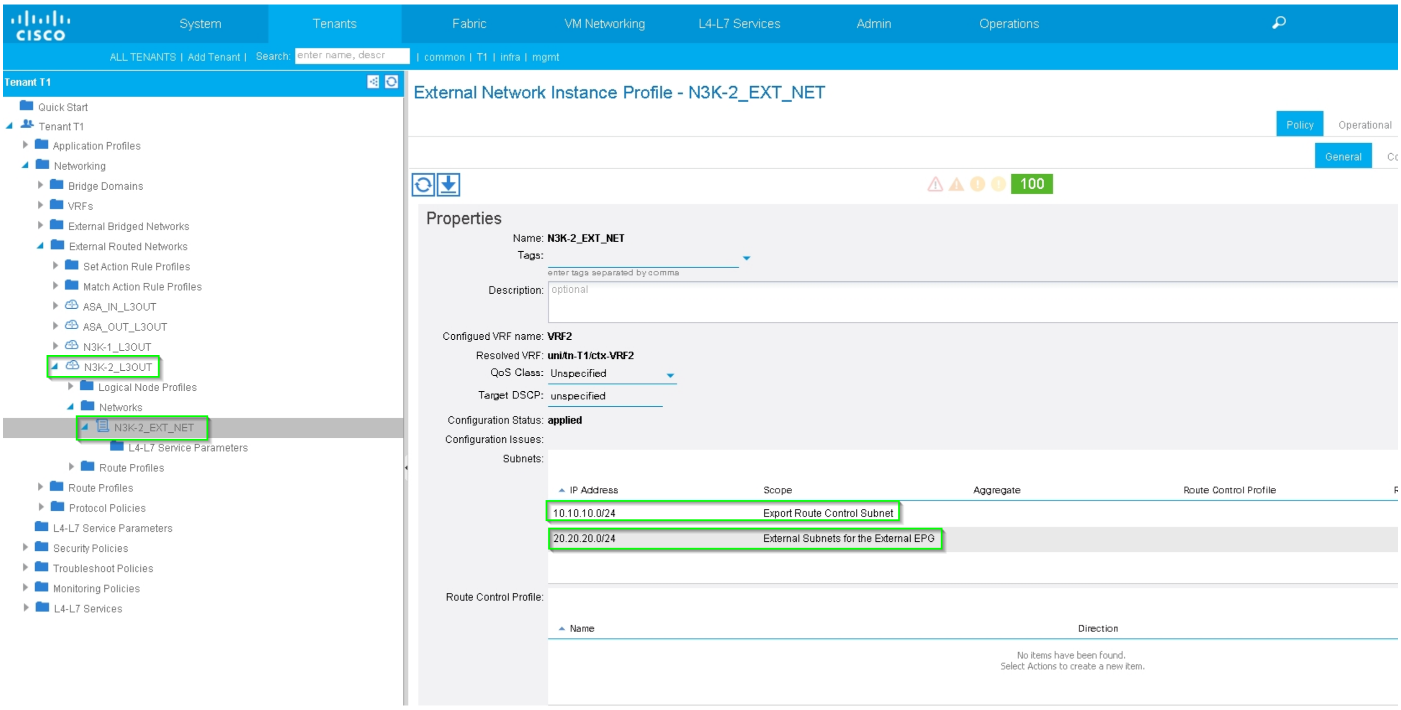
Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-106/eth1/4	192.168.1.14/30			00:22:BD:F8:19:FF	1500	vlan-103

Routed Sub-Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)	Encap

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

Configurez le contrôle de route d'importation/exportation sur les sous-réseaux pour N3K-2 L3Out pour EPG externe, comme illustré dans l'image :



External Network Instance Profile - N3K-2_EXT_NET

Properties

Name: N3K-2_EXT_NET

Tags: enter tags separated by comma

Description: optional

Configued VRF name: VRF2

Resolved VRF: uni/tn-T1/ctx-VRF2

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: applied

Configuration Issues:

Subnets:

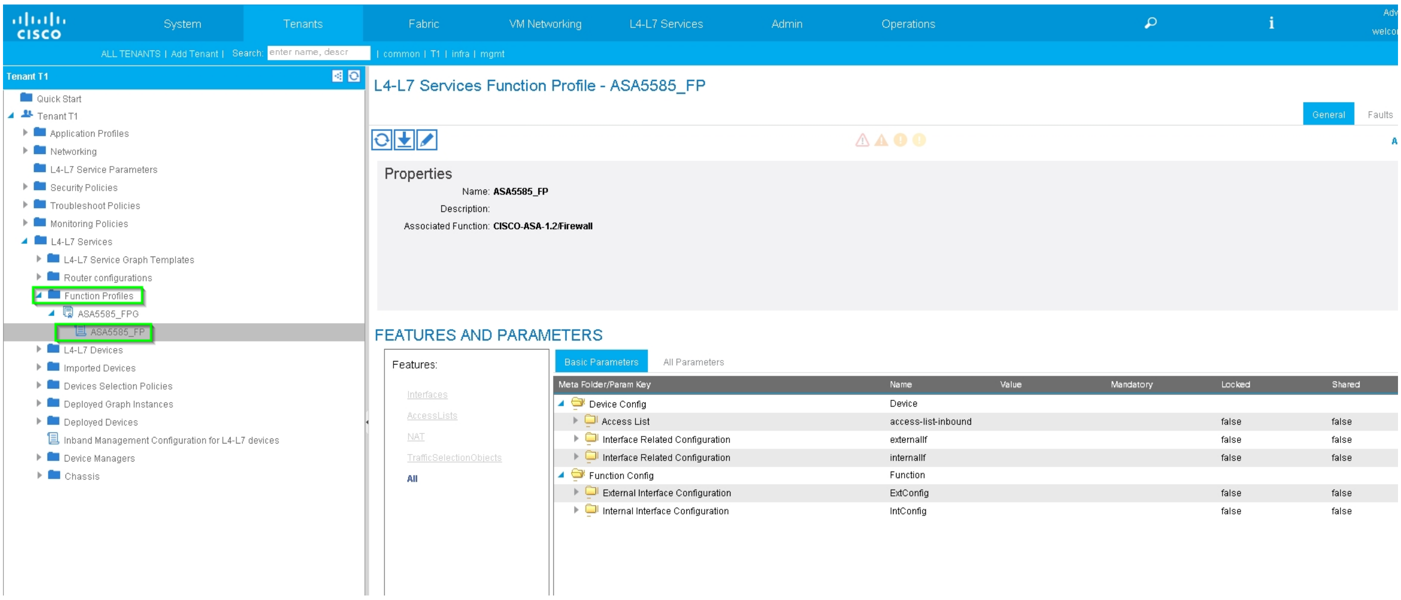
IP Address	Scope	Aggregate	Route Control Profile
10.10.10.0/24	Export Route Control Subnet		
20.20.20.0/24	External Subnets for the External EPG		

Route Control Profile:

Name	Direction

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

Étape 4. Créez un groupe de profils de fonction et configurez un profil de fonction à partir du modèle existant, comme illustré dans l'image :



L4-L7 Services Function Profile - ASA5585_FP

Properties

Name: **ASA5585_FP**

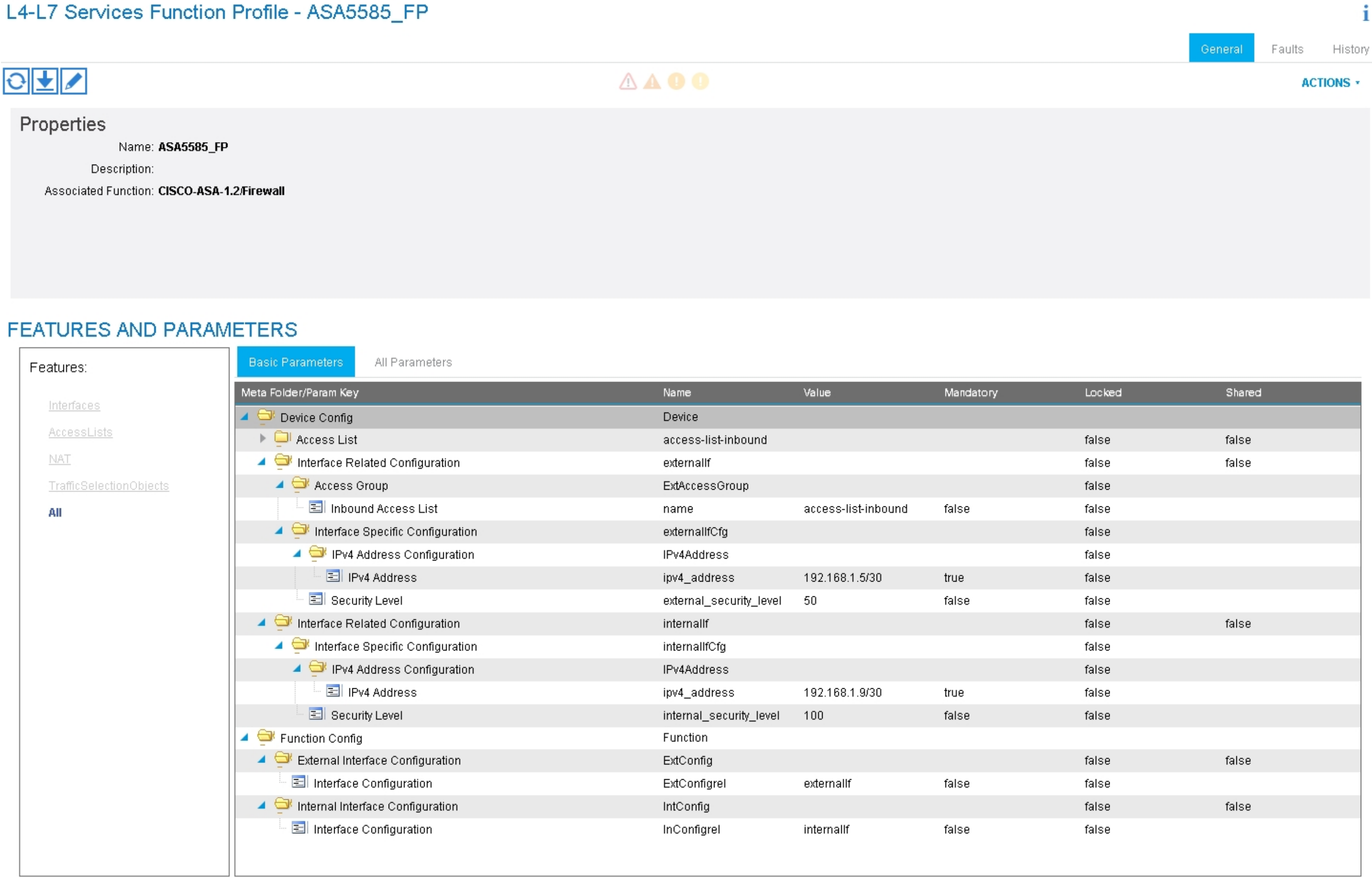
Description:

Associated Function: **CISCO-ASA-1.2/Firewall**

FEATURES AND PARAMETERS

Features:

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
Interface Related Configuration	internalIf			false	false
Function Config	Function				
External Interface Configuration	ExtConfig			false	false
Internal Interface Configuration	IntConfig			false	false



L4-L7 Services Function Profile - ASA5585_FP

Properties

Name: **ASA5585_FP**

Description:

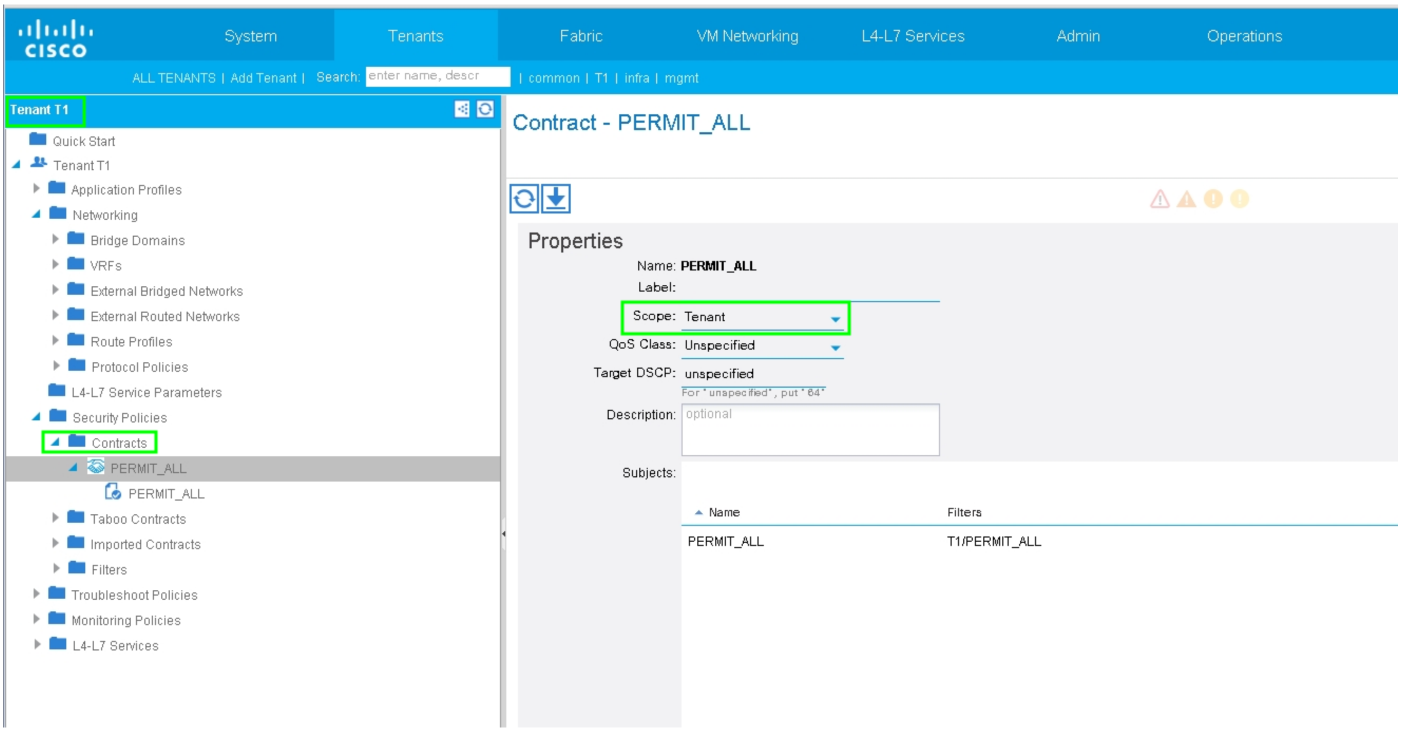
Associated Function: **CISCO-ASA-1.2/Firewall**

FEATURES AND PARAMETERS

Features:

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	

Étape 5. Créez un contrat et modifiez le champ Étendue en Locataire, comme illustré dans l'image :



Contract - PERMIT_ALL

Properties

Name: **PERMIT_ALL**

Label:

Scope: Tenant

QoS Class: Unspecified

Target DSCP: unspecified

For " unspecified" , put " 64"

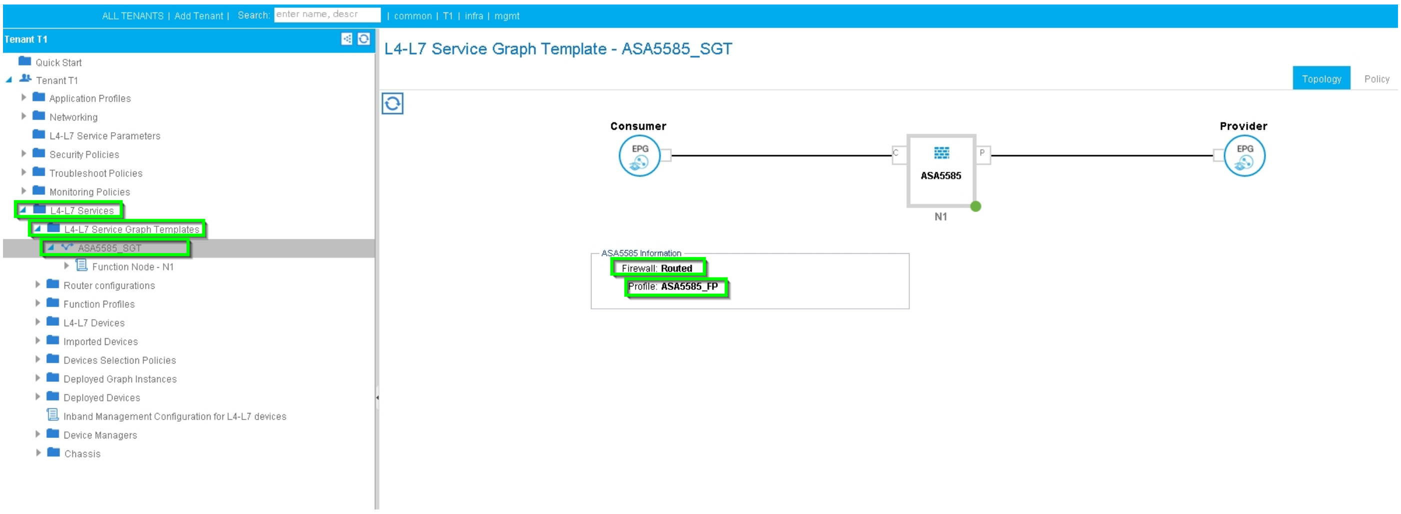
Description: optional

Subjects:

Name	Filters
PERMIT_ALL	T1/PERMIT_ALL

Étape 6. Comme l'illustre l'image, créez un modèle de graphique de service L4-L7 dans lequel l'association de graphique de service implique l'association d'une stratégie réseau routée externe et d'une configuration de routeur avec une stratégie de sélection de périphérique.

: :

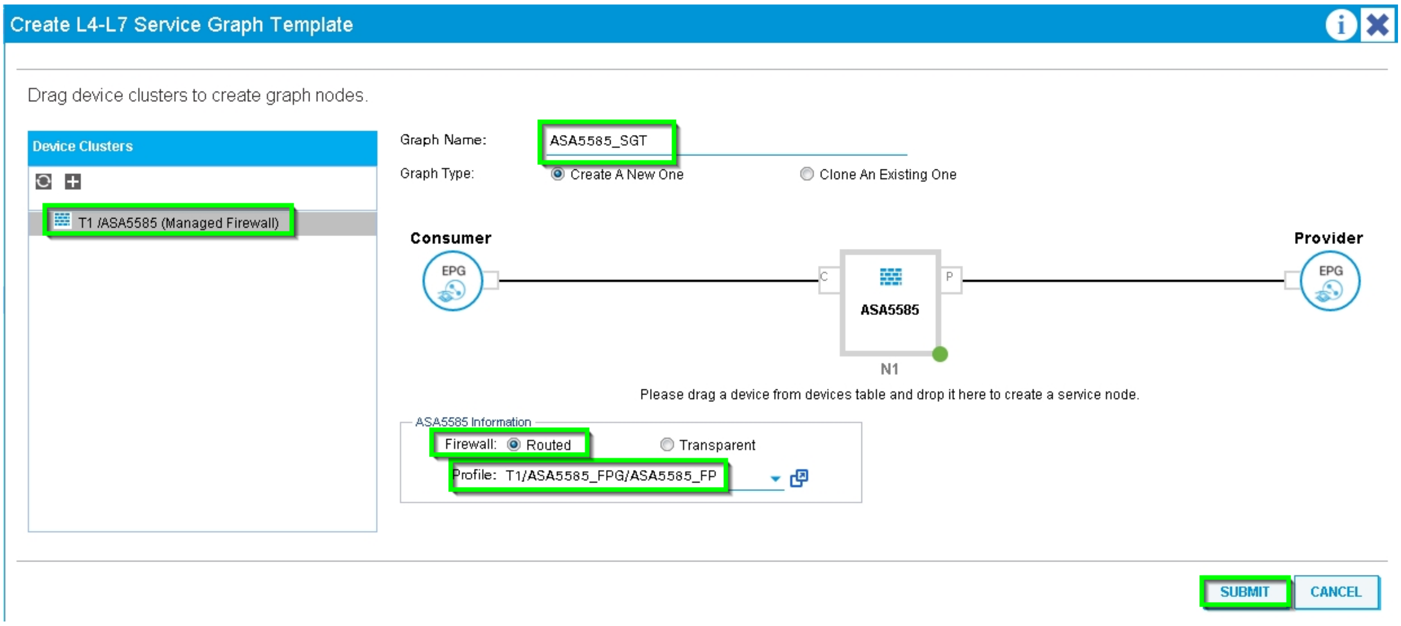


L4-L7 Service Graph Template - ASA5585_SGT

ASA5585 Information

Firewall: **Routed**

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

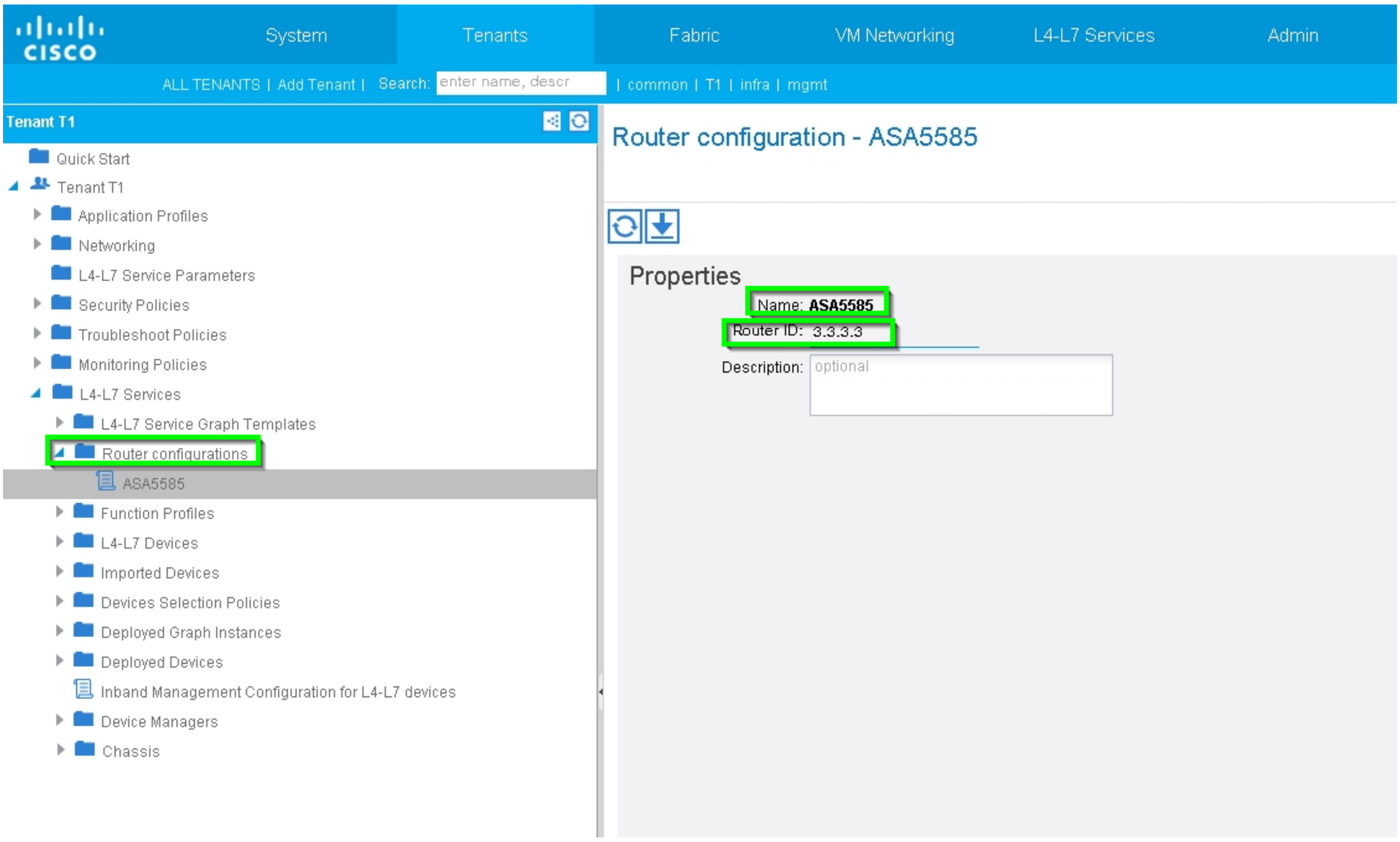
Please drag a device from devices table and drop it here to create a service node.

ASA5585 Information

Firewall: ● Routed ○ Transparent

Profile: T1/ASA5585_FPG/ASA5585_FP

Configuration du routeur pour spécifier l'ID de routeur qui sera utilisé sur l'appareil de service (ASA 5585), comme illustré sur l'image :



Router configuration - ASA5585

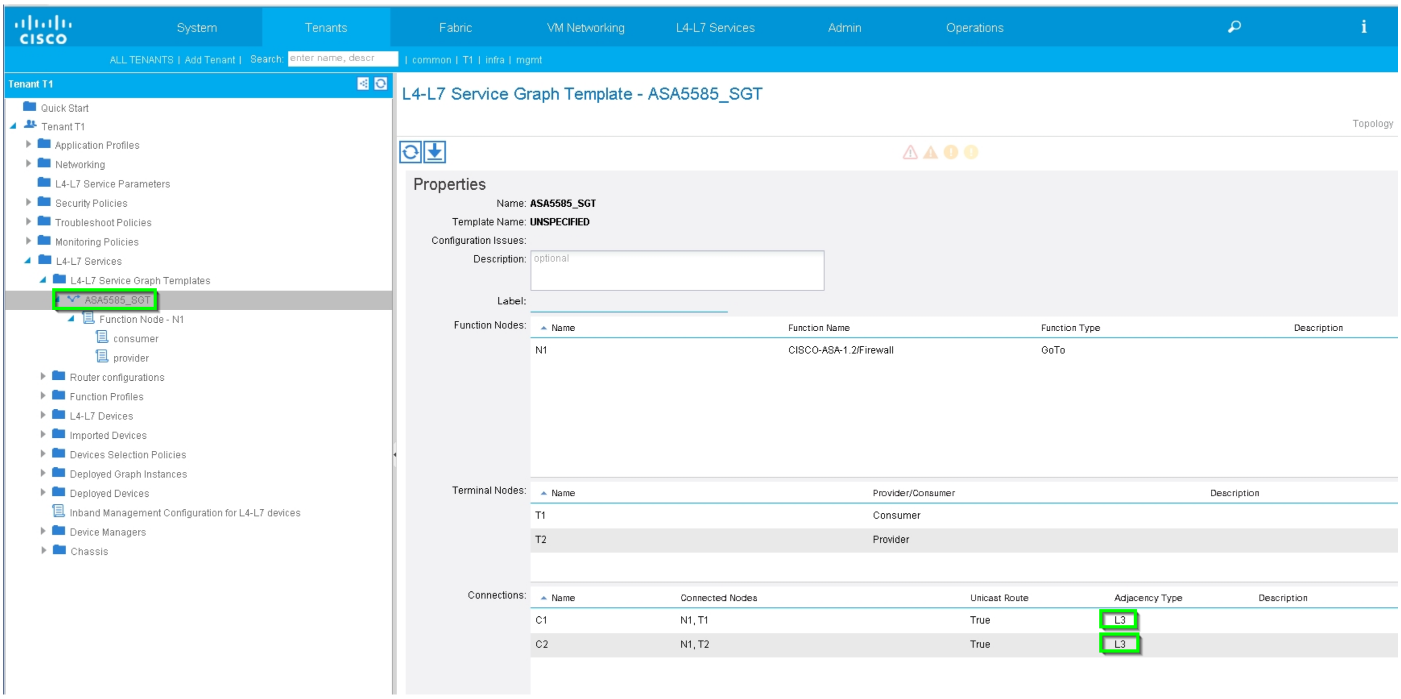
Properties

Name: ASA5585

Router ID: 3.3.3.3

Description: optional

Modifiez le type de contiguïté de L2 à L3, comme illustré sur l'image :



L4-L7 Service Graph Template - ASA5585_SGT

Properties

Name: ASA5585_SGT

Template Name: UNSPECIFIED

Configuration Issues:

Description: optional

Label:

Function Nodes:

Name	Function Name	Function Type	Description
N1	CISCO-ASA-1.2/Firewall	GoTo	

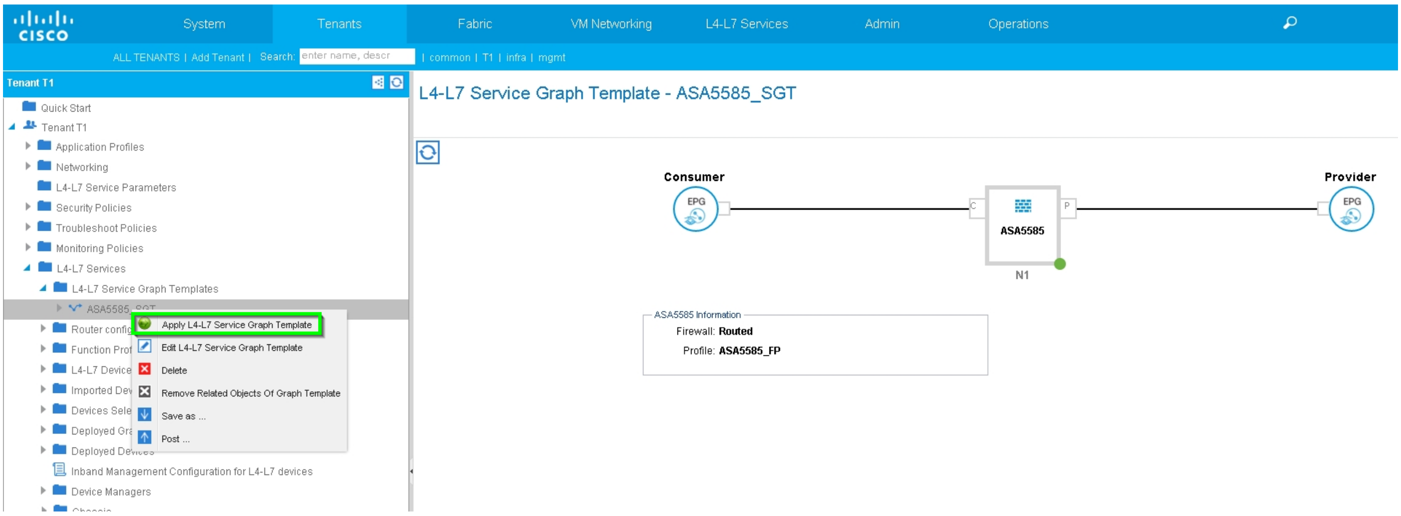
Terminal Nodes:

Name	Provider/Consumer	Description
T1	Consumer	
T2	Provider	

Connections:

Name	Connected Nodes	Unicast Route	Adjacency Type	Description
C1	N1, T1	True	L3	
C2	N1, T2	True	L3	

Appliquer le modèle de graphique de service, comme illustré dans l'image :



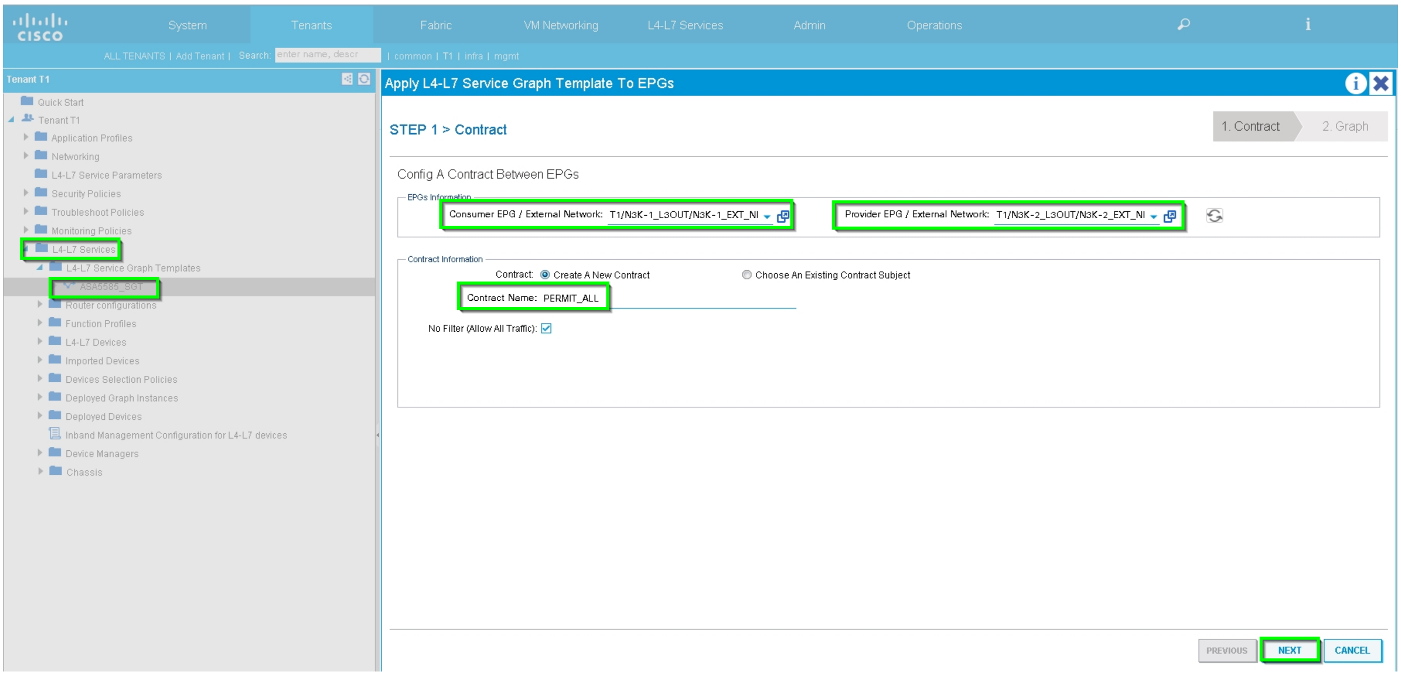
L4-L7 Service Graph Template - ASA5585_SGT

ASA5585 Information

Firewall: Routed

Profile: ASA5585_FP

Associez le graphique de service au contrat, comme illustré sur l'image :



Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: T1/N3K-1_L3OUT/N3K-1_EXT_NI

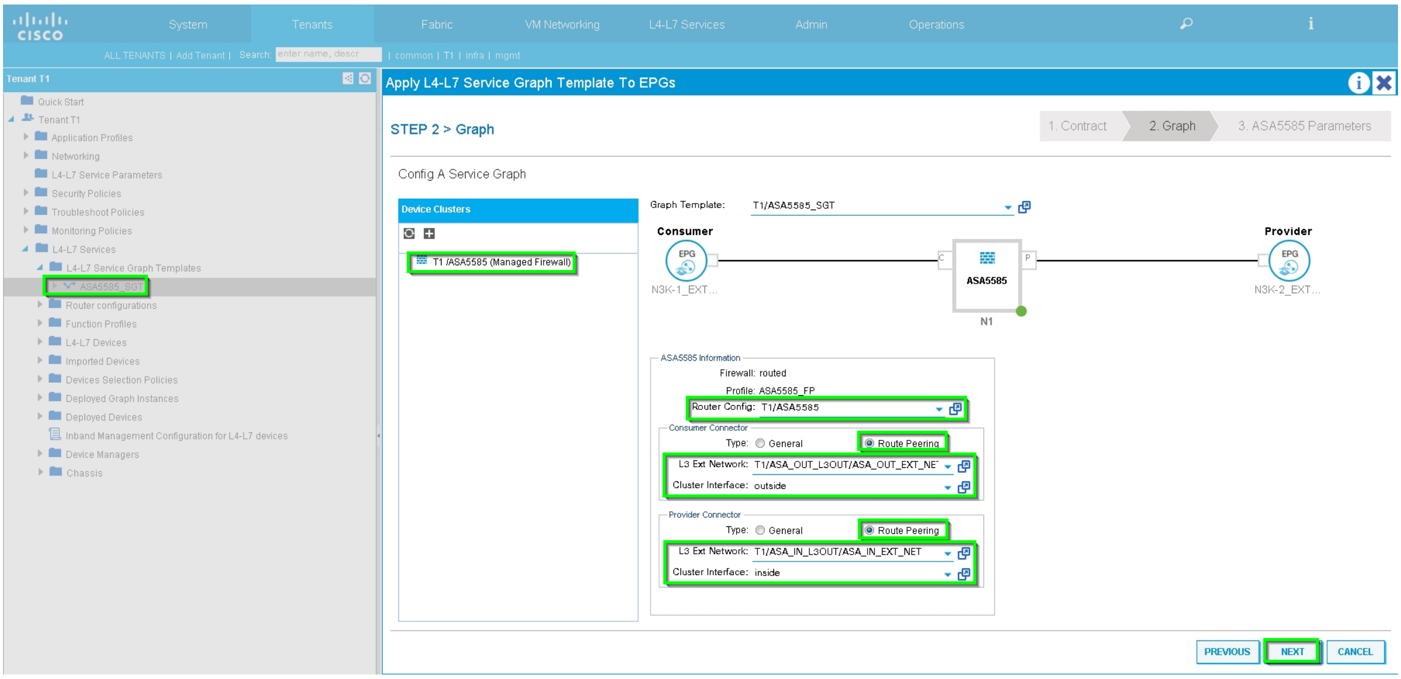
Provider EPG / External Network: T1/N3K-2_L3OUT/N3K-2_EXT_NI

Contract Information

Contract: ● Create A New Contract ○ Choose An Existing Contract Subject

Contract Name: PERMIT_ALL

No Filter (Allow All Traffic): ☑



Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

Config A Service Graph

Graph Template: T1/ASA5585_SGT

ASA5585 Information

Firewall: routed

Profile: ASA5585_FP

Router Config: T1/ASA5585

Consumer Connector

Type: ○ General ● Route Peering

L3 Ext Network: T1/ASA_OUT_L3OUT/ASA_OUT_EXT_NE

Cluster Interface: outside

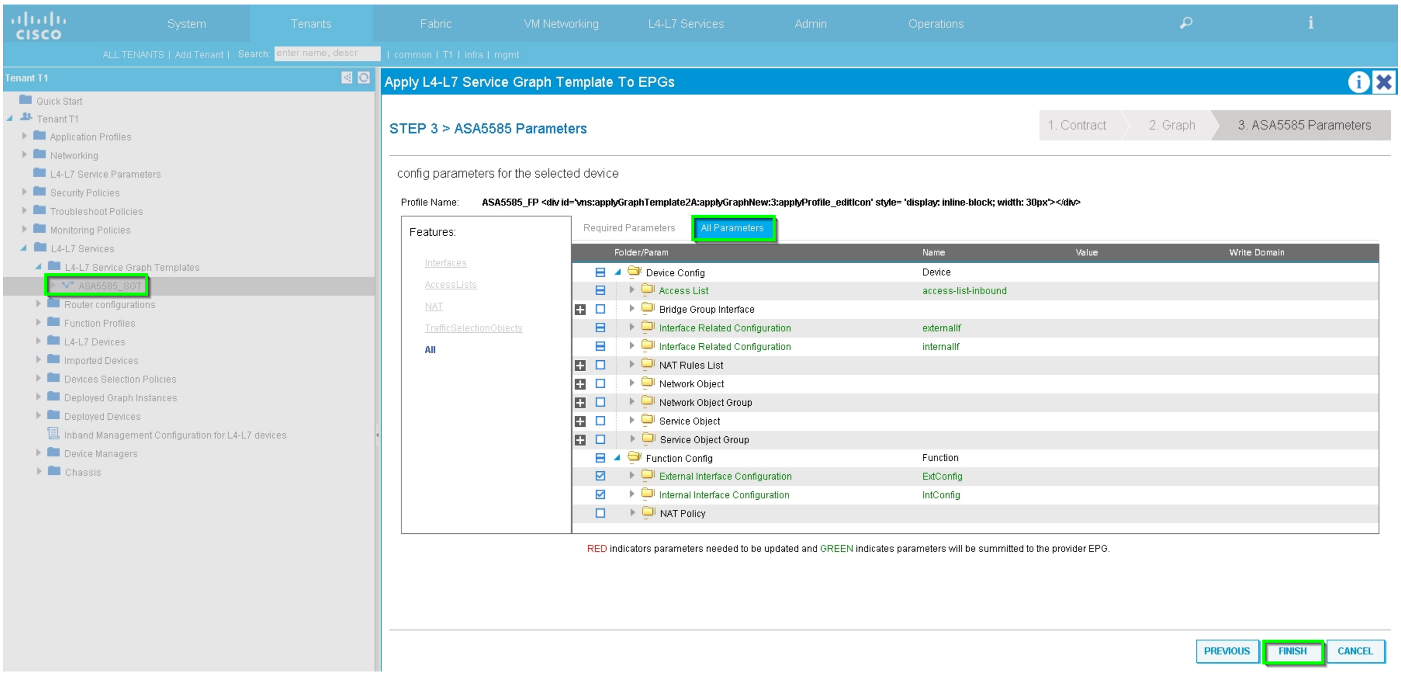
Provider Connector

Type: ○ General ● Route Peering

L3 Ext Network: T1/ASA_IN_L3OUT/ASA_IN_EXT_NET

Cluster Interface: inside

Ajoutez/modifiez le paramètre L4-L7 si nécessaire, comme l'illustre l'image :



Apply L4-L7 Service Graph Template To EPGs

STEP 3 > ASA5585 Parameters

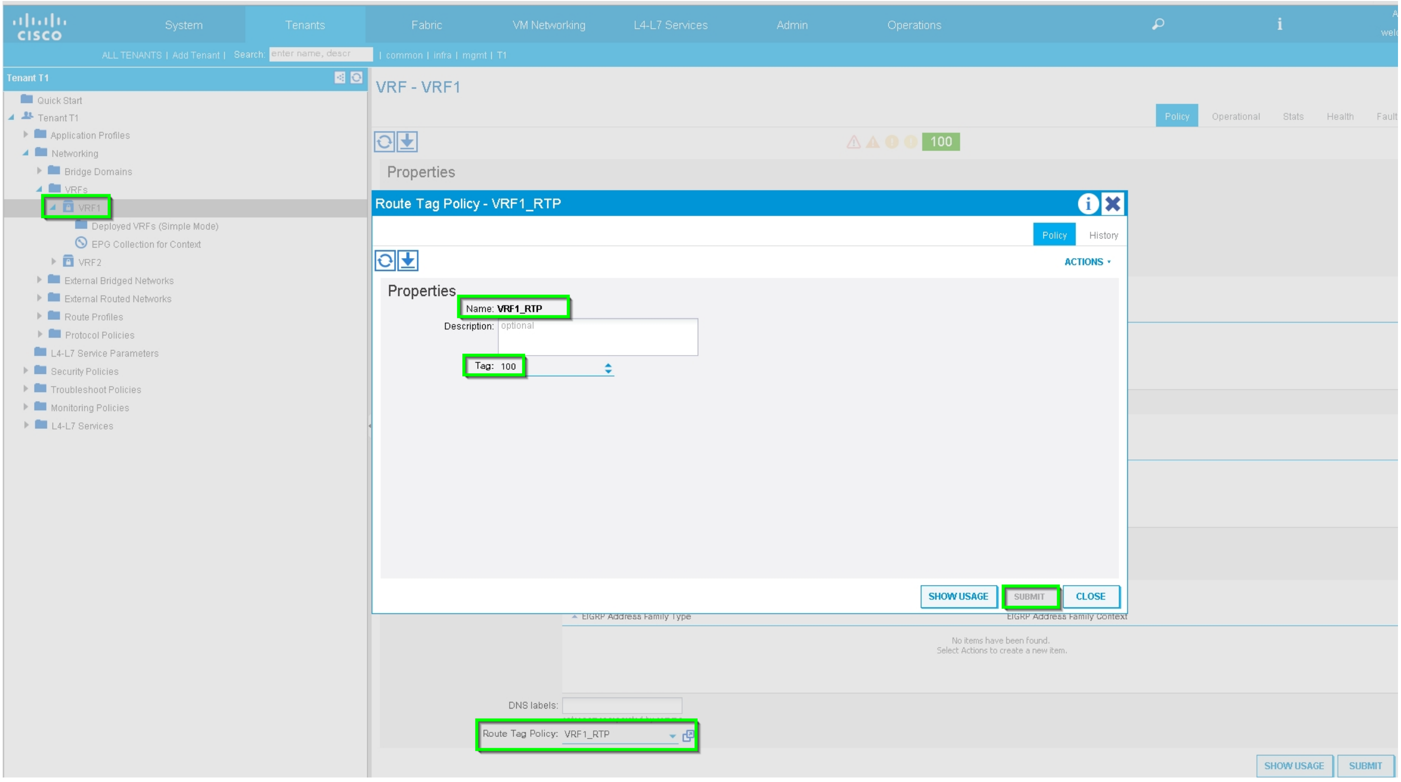
config parameters for the selected device

Profile Name: ASA5585_FP <div id='vns:applyGraphTemplate2A:applyGraphNew:3:applyProfile_editIcon' style= 'display: inline-block; width: 30px'></div>

Folder/Param	Name	Value	Write Domain
Device Config	Device		
Access List	access-list-inbound		
Bridge Group Interface			
Interface Related Configuration	externalIf		
Interface Related Configuration	internalIf		
NAT Rules List			
Network Object			
Network Object Group			
Service Object			
Service Object Group			
Function Config	Function		
☑ External Interface Configuration	ExtConfig		
☑ Internal Interface Configuration	IntConfig		
□ NAT Policy			

RED indicates parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.

Étape 7 : Route-tag Policy, configure Route-tag Policy for VRF1 (Tag:100), comme l'illustre l'image :



VRF - VRF1

Route Tag Policy - VRF1_RTP

Properties

Name: VRF1_RTP

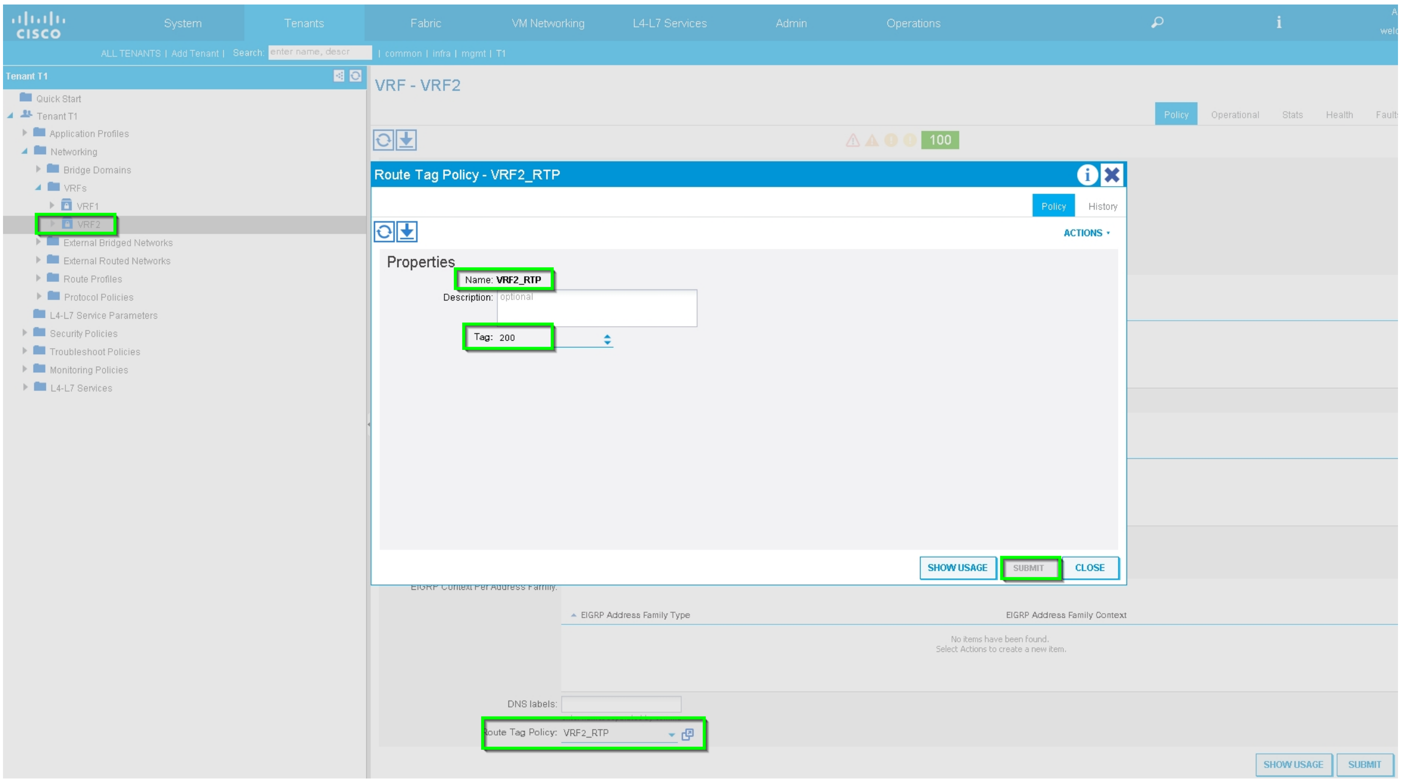
Description: optional

Tag: 100

DNS labels:

Route Tag Policy: VRF1_RTP

Configurez la stratégie de balise de route pour VRF2 (Tag:200), comme indiqué dans l'image :



VRF - VRF2

Route Tag Policy - VRF2_RTP

Properties

Name: VRF2_RTP

Description: optional

Tag: 200

EIGRP Context Per Address Family:

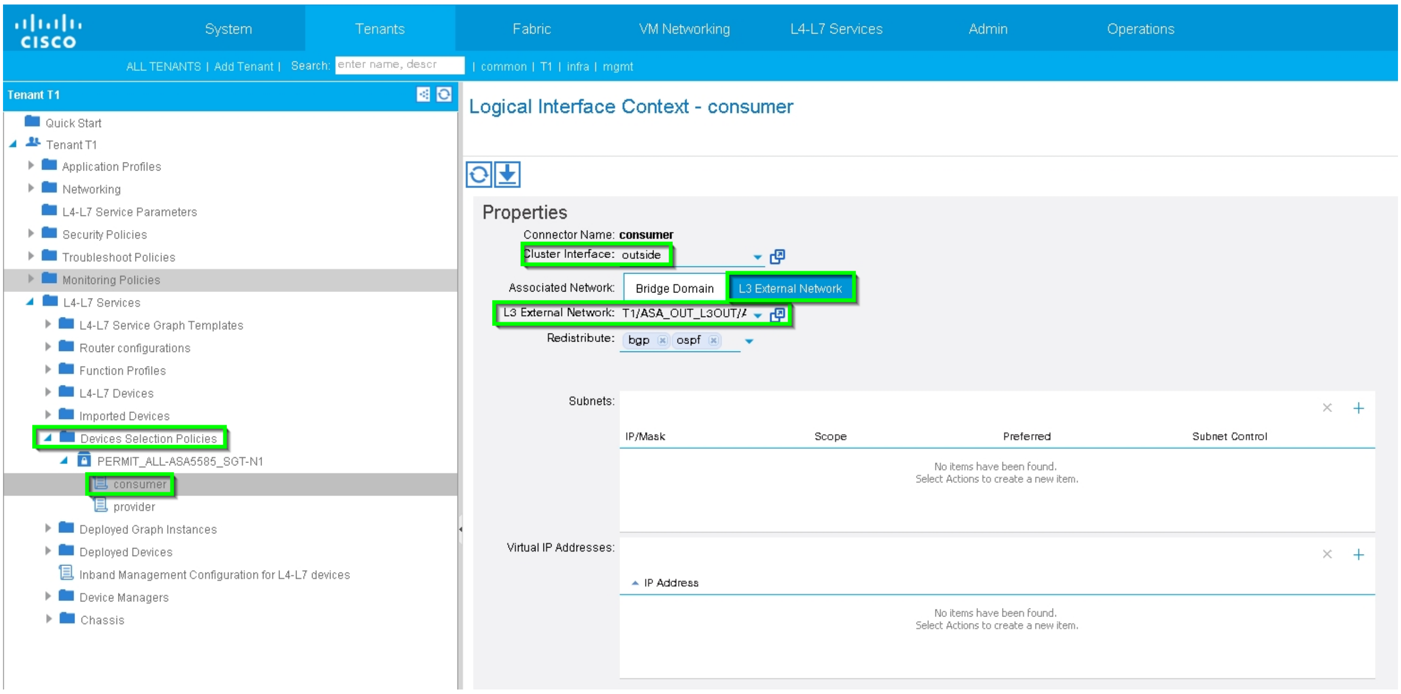
EIGRP Address Family Type	EIGRP Address Family Context

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

DNS labels:

Route Tag Policy: VRF2_RTP

Étape 8 : Vérifiez l'état et vérifiez la stratégie de sélection des périphériques, comme illustré sur l'image :



Logical Interface Context - consumer

Properties

Connector Name: consumer

Cluster Interface: outside

Associated Network: Bridge Domain | L3 External Network

L3 External Network: T1/ASA_OUT_L3OUT/

Redistribute: bgp ospf

Subnets:

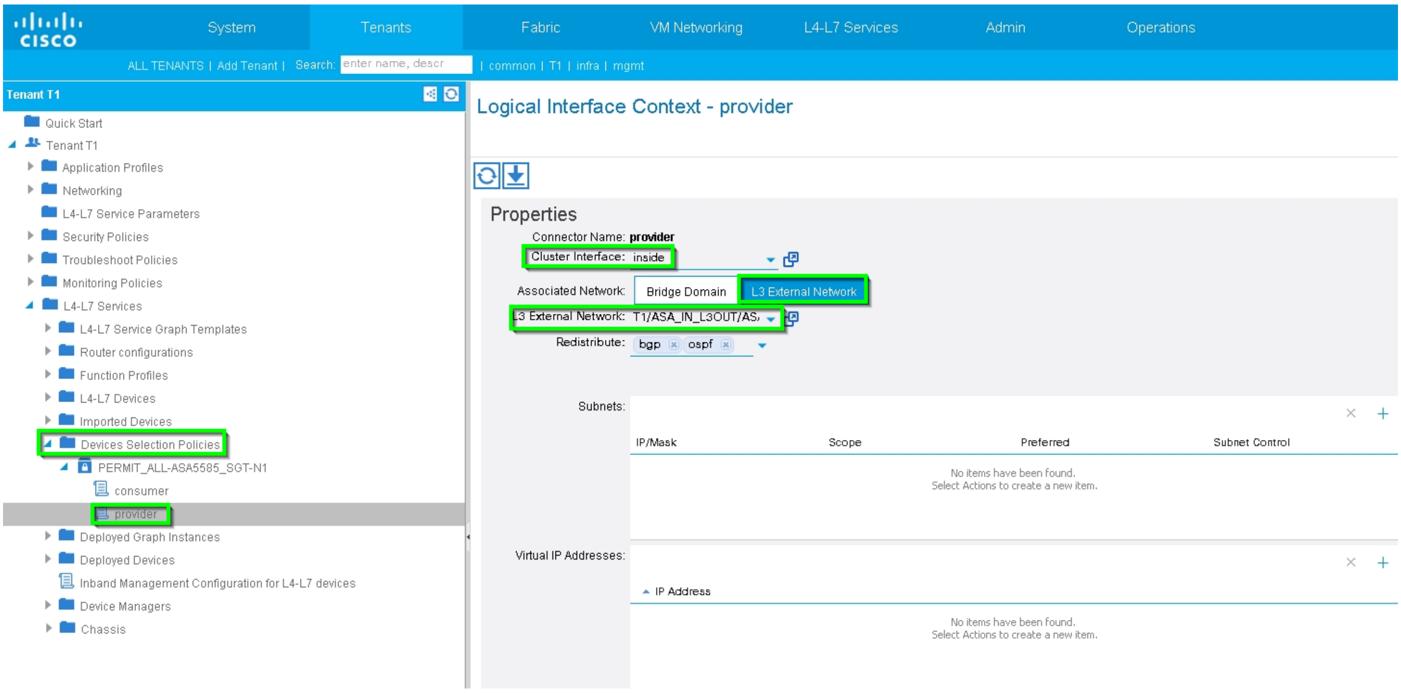
IP/Mask	Scope	Preferred	Subnet Control

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.



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

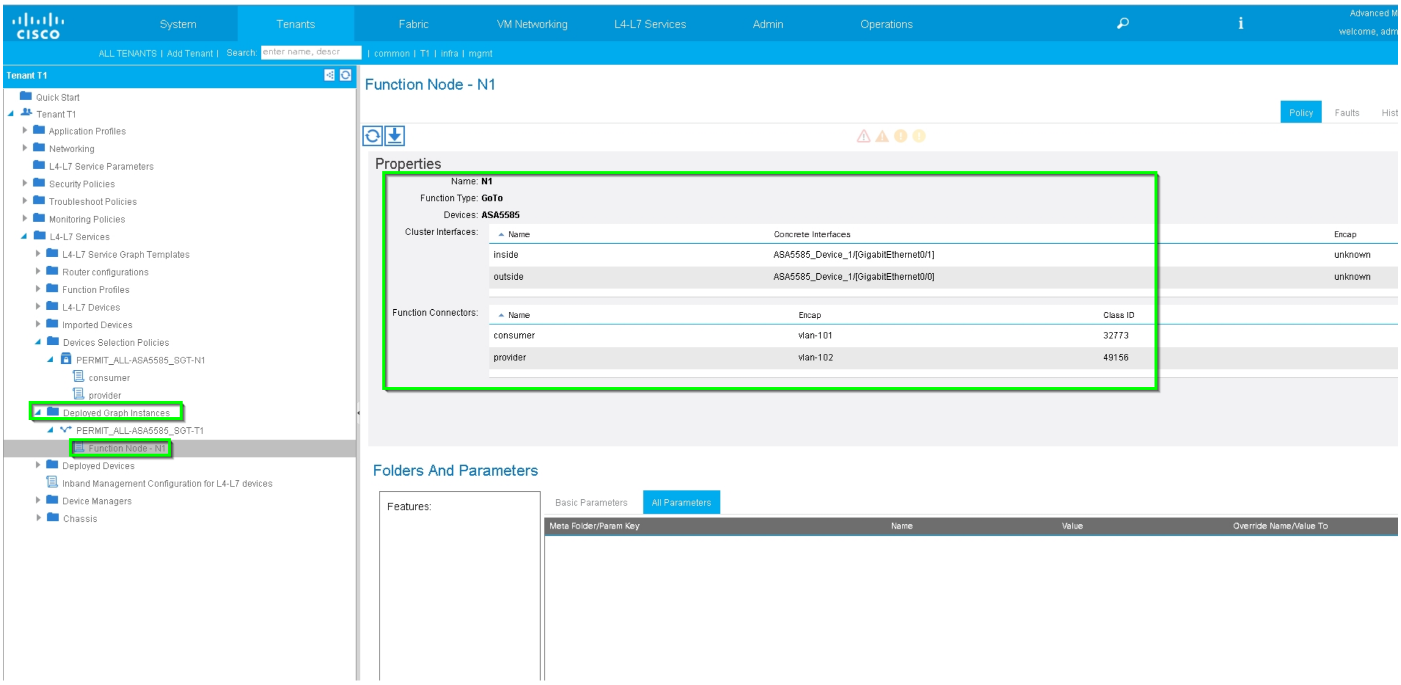
No items have been found.
Select Actions to create a new item.

Virtual IP Addresses:

IP Address

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

Vérifiez l'instance du graphique déployé, comme illustré dans l'image :



Function Node - N1

Properties

Name: **N1**

Function Type: **GoTo**

Devices: **ASA5585**

Cluster Interfaces:

Name	Concrete Interfaces	Encap
inside	ASA5585_Device_1/[GigabitEthernet0/1]	unknown
outside	ASA5585_Device_1/[GigabitEthernet0/0]	unknown

Function Connectors:

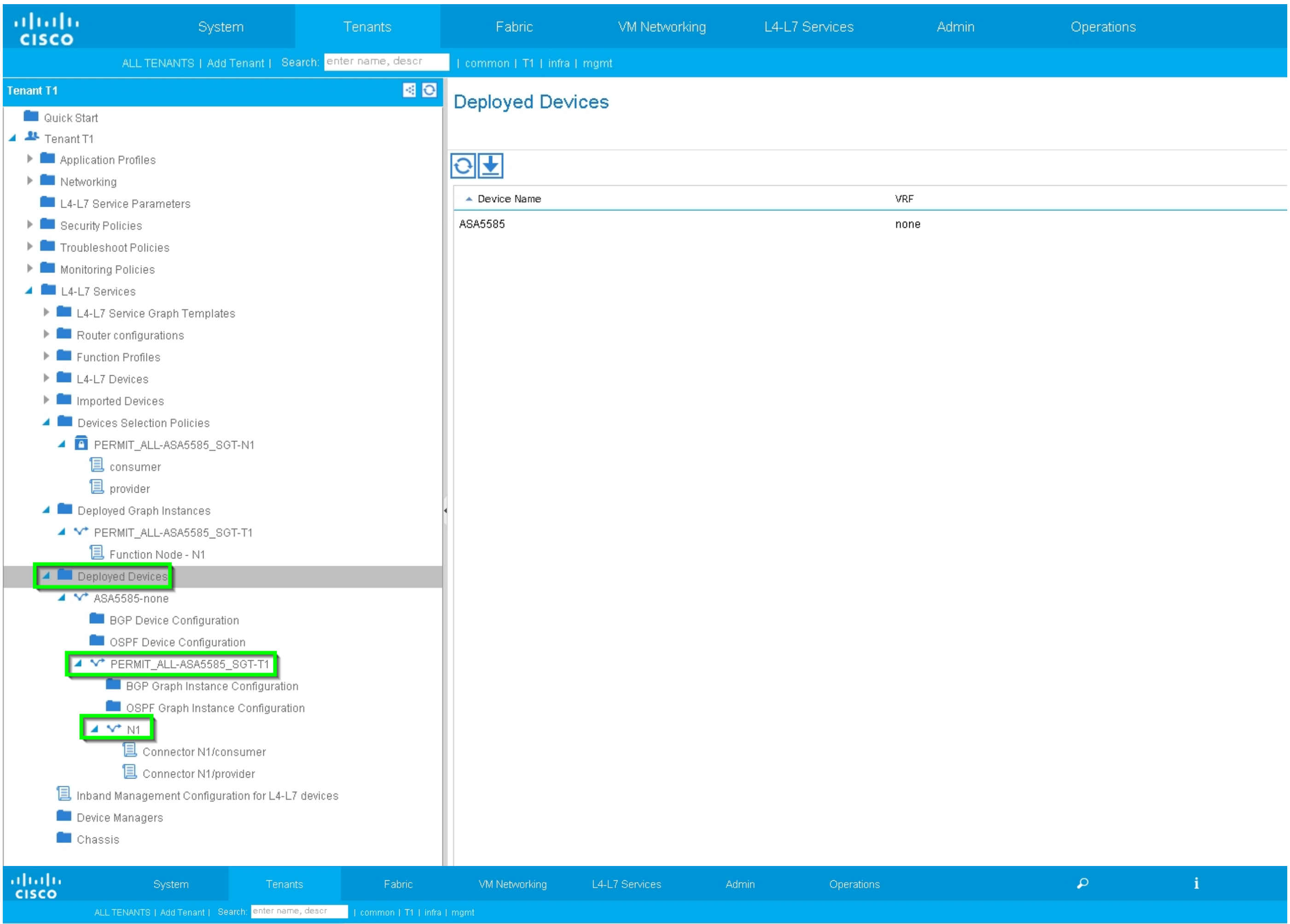
Name	Encap	Class ID
consumer	vlan-101	32773
provider	vlan-102	49156

Folders And Parameters

Features:

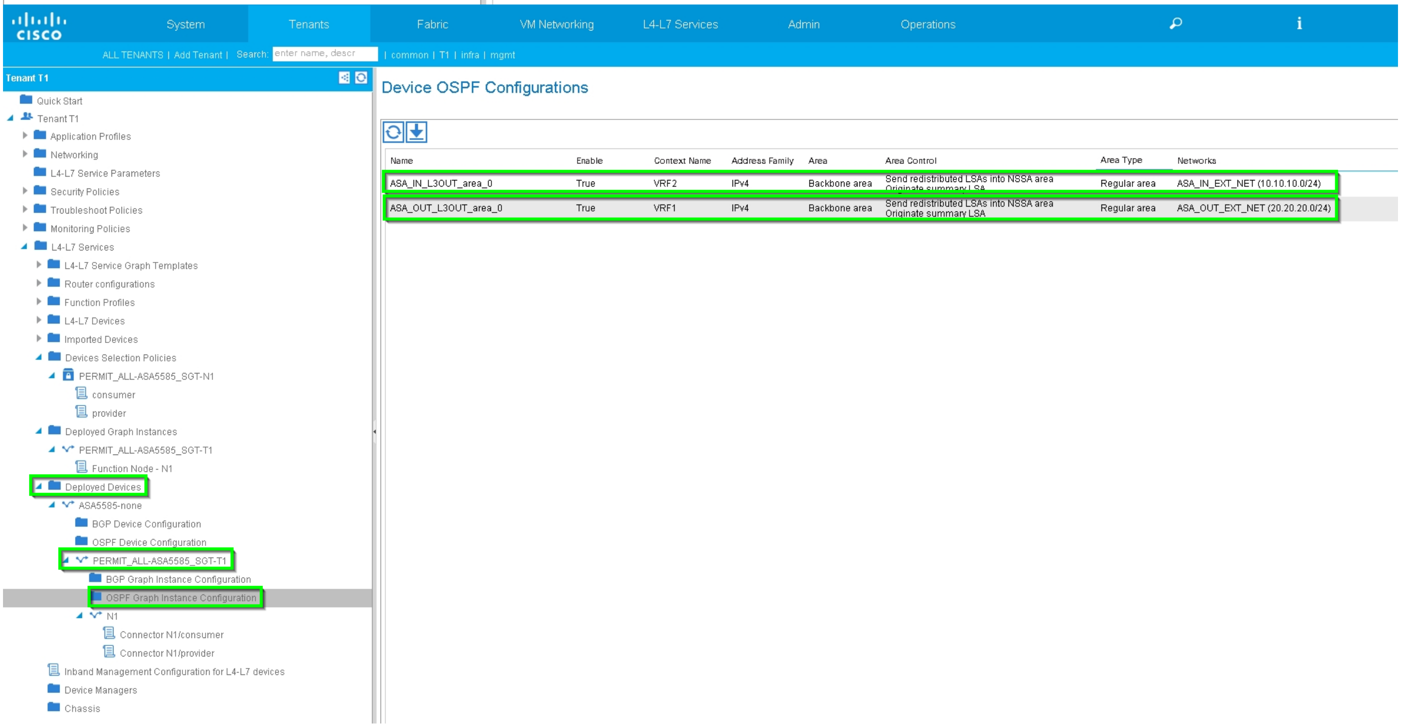
Basic Parameters | All Parameters

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



Deployed Devices

Device Name	VRF
ASA5585	none



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 summary 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)

Vérifiez et dépannez

Configuration APIC pour le locataire :

```
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
    l4l7 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
l4l7 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
    l4l7 graph ASA5585_SGT contract PERMIT_ALL
      service N1 device-cluster-tenant T1 device-cluster ASA5585 mode FW_ROUTED
        connector consumer cluster-interface outside
          l4l7-peer tenant T1 out ASA_OUT_L3OUT epg ASA_OUT_EXT_NET redistribute bgp,ospf
          exit
        connector provider cluster-interface inside
          l4l7-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#
```

Vérifiez la relation de voisinage OSPF et la table de routage sur la feuille 101 :

```
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
```

Vérifiez la relation de voisinage OSPF et la table de routage sur la feuille 102 :

```
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
```

Vérifiez la configuration, la relation de voisinage OSPF et la table de routage sur ASA 5585 :

```
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
```

Vérifiez la configuration, la relation de voisinage OSPF et la table de routage sur N3K-1 :

```
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
```

Vérifiez la configuration, la relation de voisinage OSPF et la table de routage sur N3K-2 :

```
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
```

Vérifiez les règles de filtre de contrat sur leaf et le nombre de succès de paquet : .

```
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]
```

Test d'accessibilité entre N3K-1 et N3K-2 :

```
    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
```

Vous trouverez ci-joint le fichier de configuration XML du locataire et le profil de fonction ASA, utilisés pour cette démonstration.