

Peering de rota L4-L7 com estrutura de trânsito - Introdução à configuração

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar](#)

[Verificar e solucionar problemas](#)

Introduction

Este documento descreve a configuração do Service Graph L4-L7 com Route Peering, em que o consumidor e o provedor são externos à estrutura da Application Centric Infrastructure (ACI).

Contribuído por Zahid Hassan, engenheiro de serviços avançados da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Grupos estáticos de VLAN que serão usados para a VLAN de encapsulamento entre os dispositivos externos e a estrutura ACI
- Domínios físicos e roteados externos que unirão o local (nó/caminho de folha) dos dispositivos externos e o pool de VLANs
- Conexão da camada 3 a uma rede externa (L3Out)

As etapas anteriores das configurações **de acesso à estrutura** e **L3Out** não são abordadas neste documento e foram presumidas que elas já foram concluídas.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Application Policy Infrastructure Controller (Cisco APIC) - 1.2(1m)

- Pacote de dispositivos do Adaptive Security Appliance (ASA) - 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.

Informações de Apoio

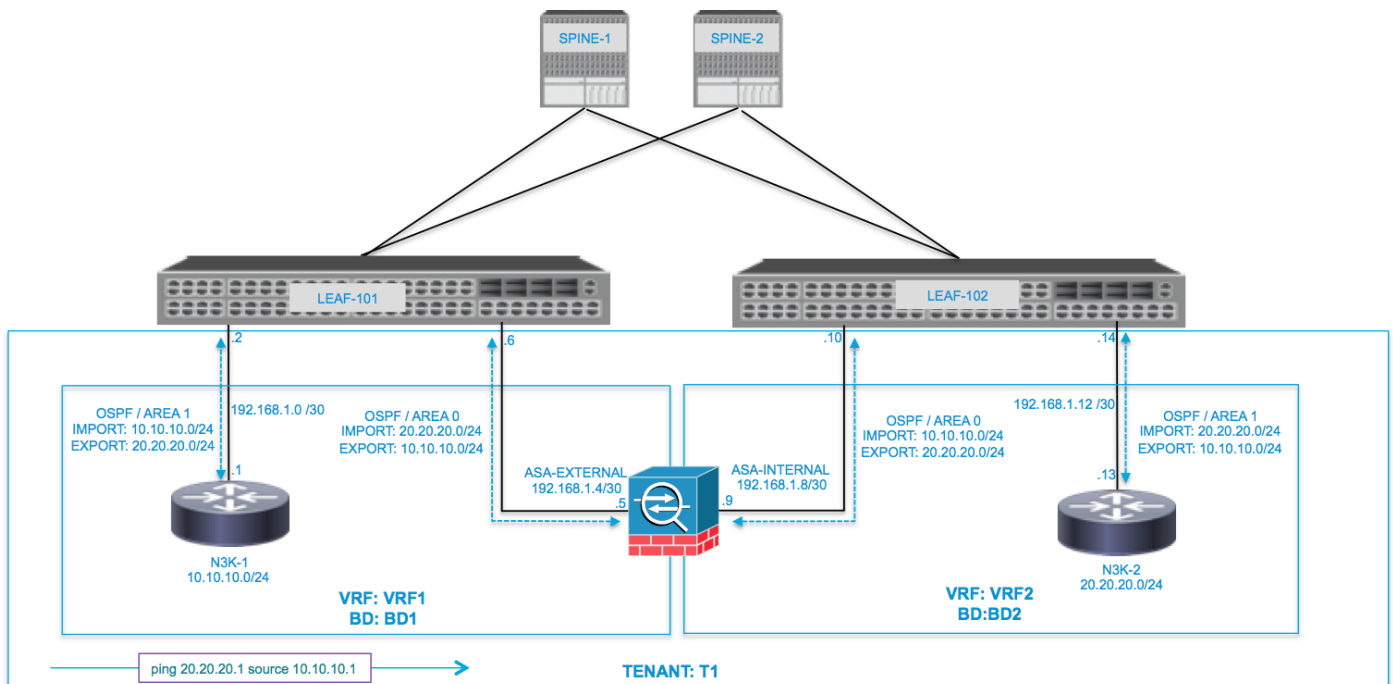
O Route Peering é um recurso que permite que um dispositivo de serviço, como um balanceador de carga ou um firewall, anuncie sua acessibilidade por meio da estrutura da ACI até uma rede externa.

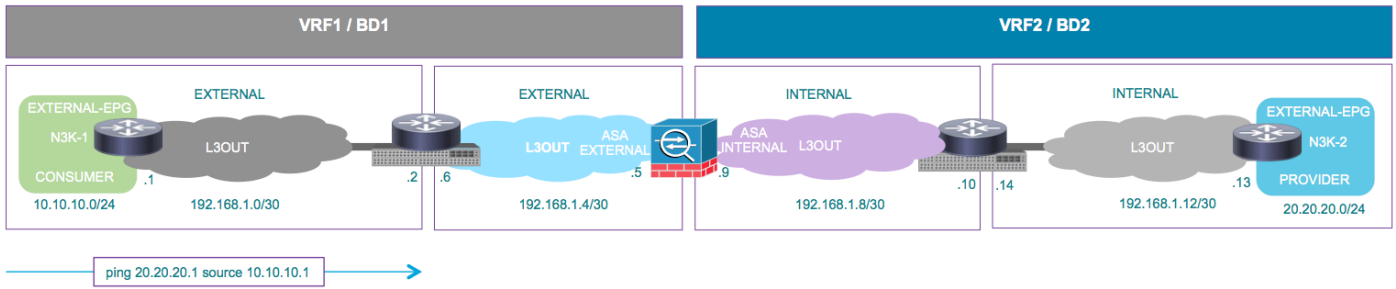
O caso de uso apresentado aqui é um firewall físico que é implantado como um Gráfico de serviços de dois braços, entre dois L3Outs ou Grupos de terminais externos (EPGs). O Service Graph está associado a um contrato entre o EPG externo no Leaf 101 (N3K-1) e o EPG externo no Leaf 102 (N3K-2). A estrutura da ACI está fornecendo um serviço de trânsito para os roteadores (N3K-1 e N3K-2) e a Peering de Rota é usada, com o OSPF (Open Shortest Path First) como protocolo de roteamento, para trocar rotas entre o firewall e a estrutura da ACI.

Configurar

Diagrama de Rede

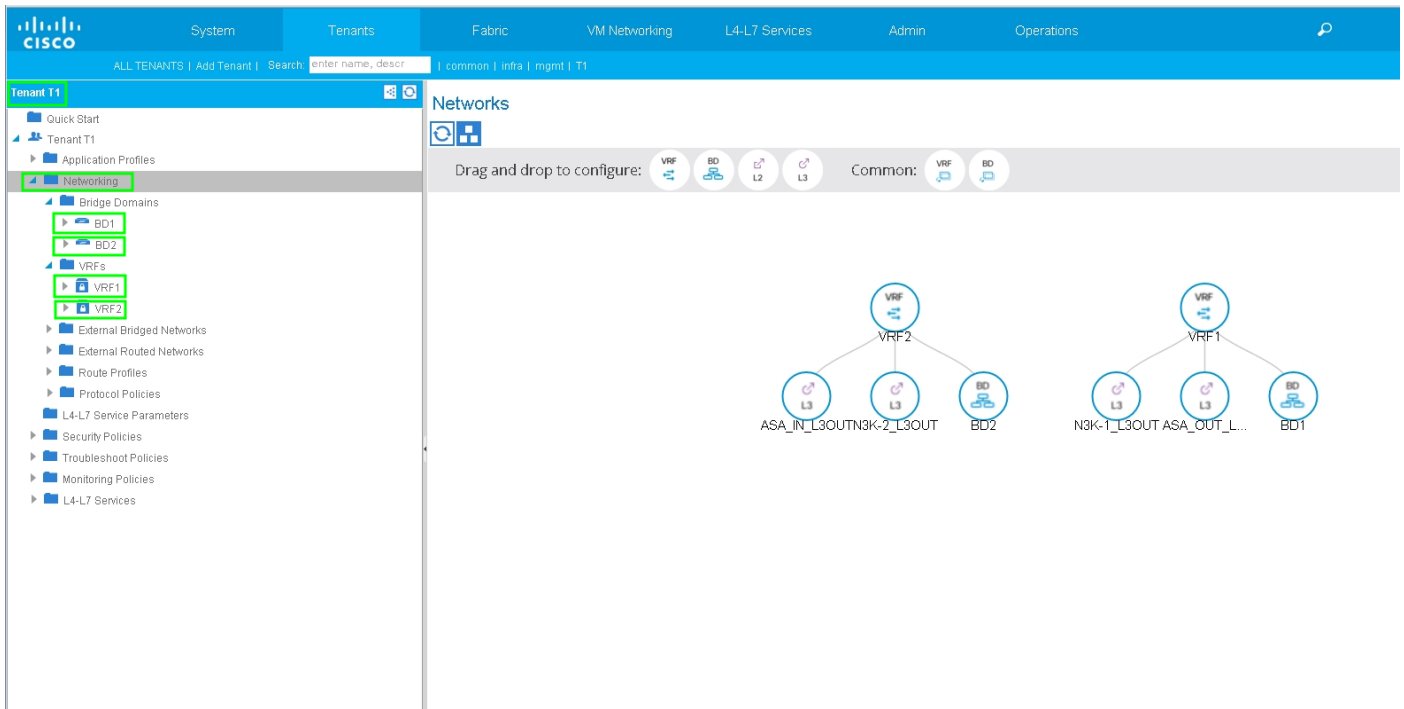
A imagem a seguir mostra como o Route Peering funciona de ponta a ponta:



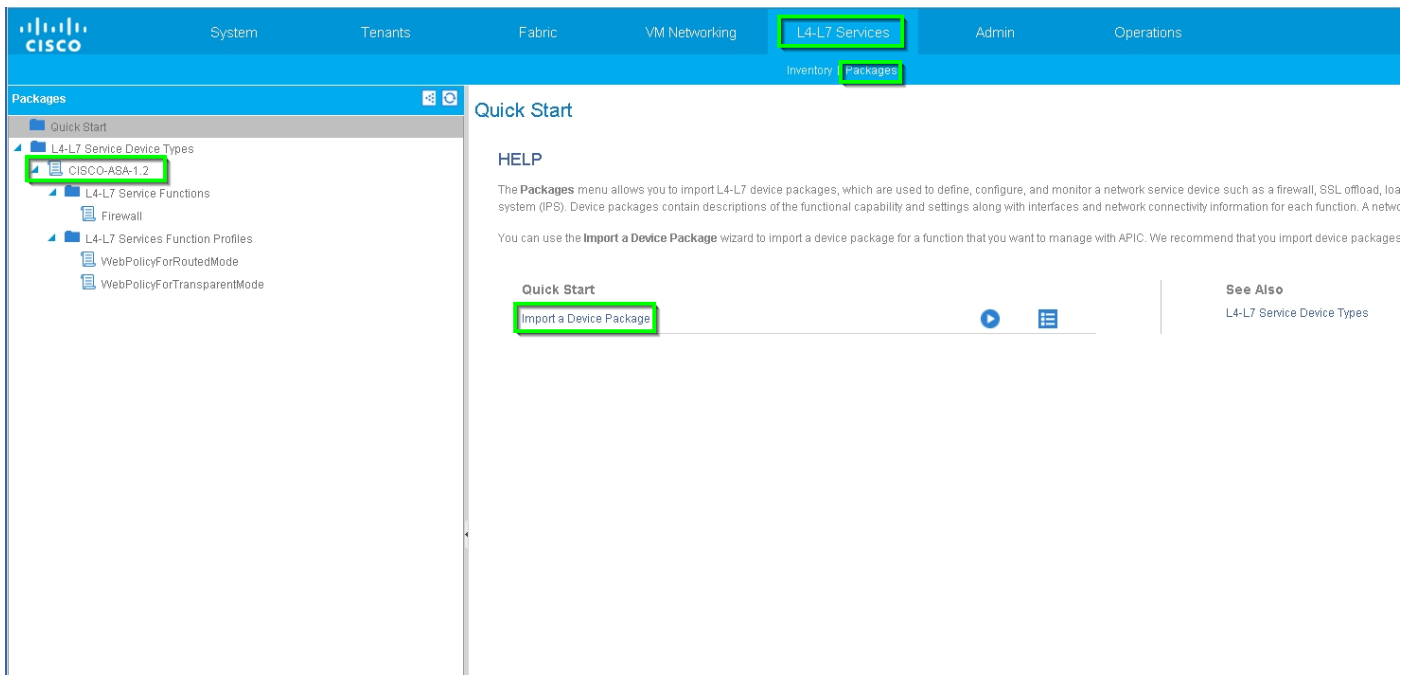


Configurar

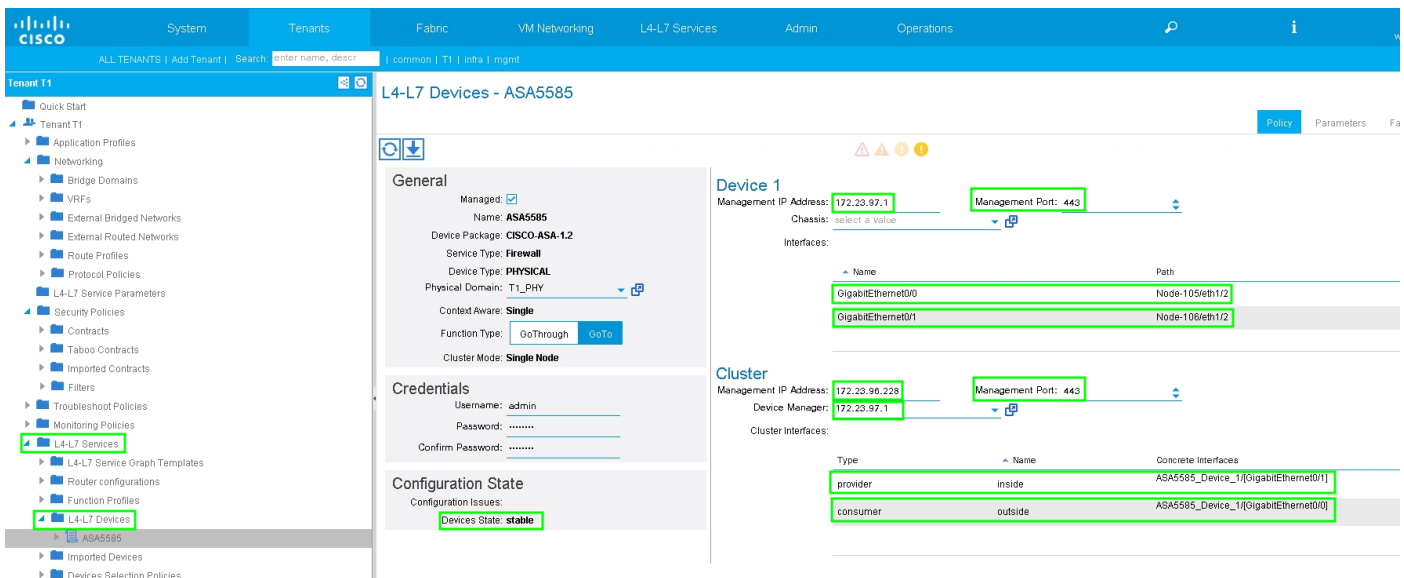
Etapa 1. Configure o Virtual Routing and Forwarding1 (VRF1), VRF2, Bridge Domain1 (BD1) e BD2. Associe BD1 a VRF1 e BD2 a VRF2, como mostrado na imagem:



Etapa 2. Carregue o pacote de dispositivos ASA em Dispositivo L4-L7, conforme mostrado na imagem, :



Configure o dispositivo L4-L7 para o ASA 5585 físico (roteado), como mostrado na imagem:



Etapa 3. Configure L3Out para N3K-1 e associe com BD1 e VRF1.

A rede roteada externa é usada para especificar a configuração de roteamento na estrutura da ACI para o Route Peering, como mostrado na imagem:

Properties

Name: **N3K-1_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 Interleak: select a value

Route Control For Dampening:

Address Family Type

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

Note: Todas as interfaces L3Out que são usadas para o Peering de Rota, precisam ser configuradas como uma Interface Virtual de Switch (SVI) com encapsulamento de VLAN de acordo.

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.				

Configure o controle de rota de importação/exportação em sub-redes para N3K-1 L3Out External

EPG, como mostrado na imagem:

The screenshot displays the Cisco SD-WAN GUI for Tenant T1. The left sidebar shows a navigation tree with 'N3K-1_EXT_NET' selected under 'Networks'. The main panel is titled 'External Network Instance Profile - N3K-1_EXT_NET' and shows the 'Properties' tab. The configuration includes:

- Name: N3K-1_EXT_NET
- Tags: 1
- Description: optional
- Configured VRF name: VRF1
- Resolved VRF: untn-T1ctx-VRF1
- QoS Class: Unspecified
- Target DSCP: unspecified
- Configuration Status: applied
- Subnets table:

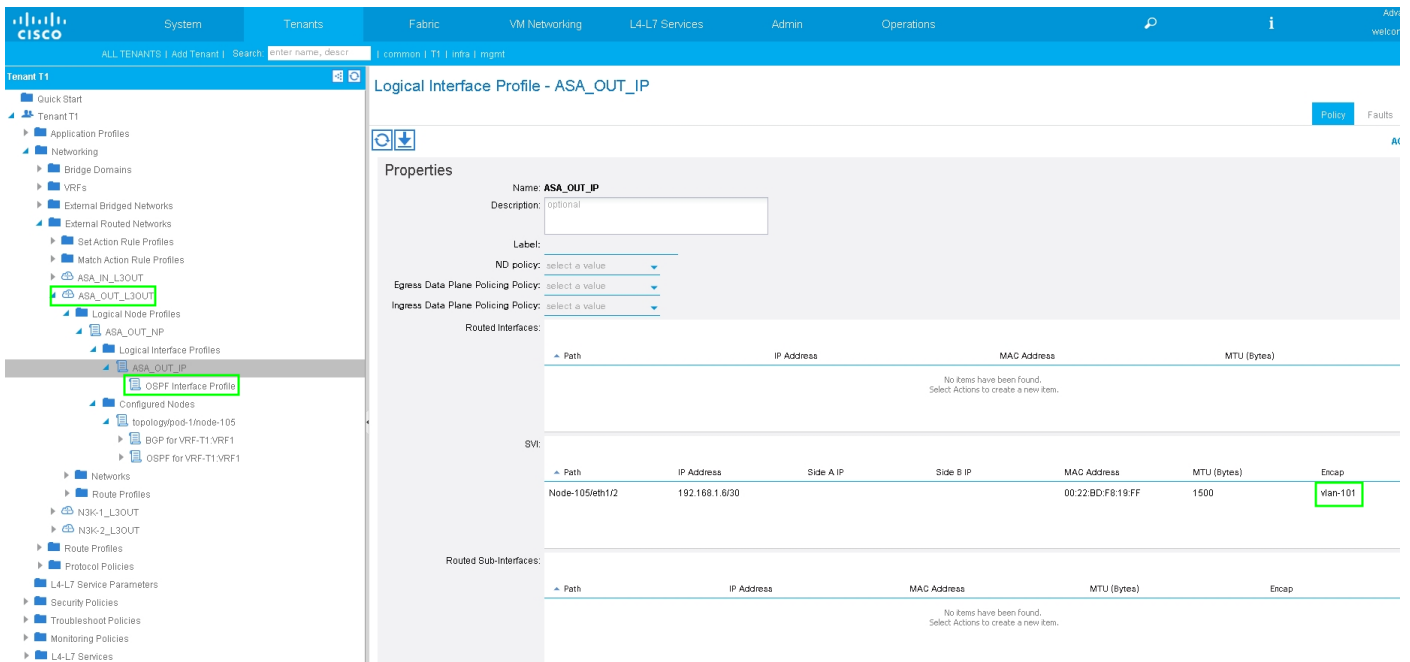
IP Address	Scope	Aggregate	Route Control Profile
10.10.10.0/24	External Subnets for the External EPO		
20.20.20.0/24	Export Route Control Subnet		

Below the subnets table, there is a 'Route Control Profile' section with a table for Name and Direction, which is currently empty.

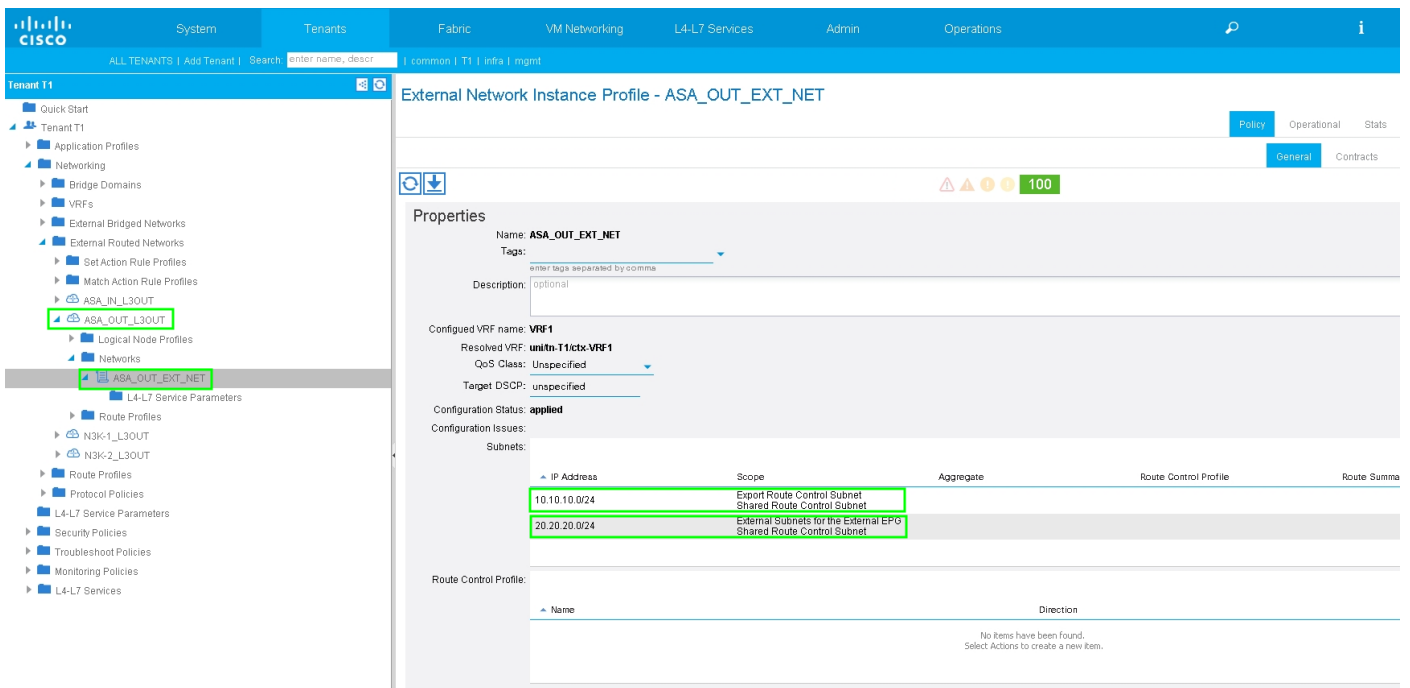
Configure L3Out para a interface ASA-External e associe-se a BD1 e VRF1, como mostrado na imagem:

The screenshot displays the Cisco SD-WAN GUI for Tenant T1. The left sidebar shows a navigation tree with 'ASA_OUT_L3OUT' selected under 'Networks'. The main panel is titled 'L3 Outside - ASA_OUT_L3OUT' and shows the 'Properties' tab. The configuration includes:

- Name: ASA_OUT_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)
- 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



Configure o controle de rota de importação/exportação em sub-redes para ASA-External L3Out External EPG, como mostrado na imagem:



Configure L3out para ASA-Internal e associe com BD2 e VRF2, como mostrado na imagem:

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 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**

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

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

Configure o controle de rota de importação/exportação em sub-redes para ASA-Internal L3Out External EPG, como mostrado na imagem:

External Network Instance Profile - ASA_IN_EXT_NET

Properties

Name: **ASA_IN_EXT_NET**

Tags:

Description:

Configured VRF name: **VRF2**

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

QoS Class: **Unspecified**

Target DSCP: **unspecified**

Configuration Status: **applied**

Configuration Issues:

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.	

Configure L3Out para N3K-2 e associe com BD2 e VRF2, como mostrado na imagem:

L3 Outside - N3K-2_L3OUT

Properties

Name: **N3K-2_L3OUT**

Description:

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 Interleaf:

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:

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.				

Configure o controle de rota de importação/exportação em sub-redes para N3K-2 L3Out para EPG externo, como mostrado na imagem:

External Network Instance Profile - N3K-2_EXT_NET

Properties

Name: **N3K-2_EXT_NET**

Tags:

Description: optional

Configured VRF name: **VRF2**

Resolved VRF: **uni/tn-1/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.	

Etapa 4. Crie um grupo de perfis de função e configure o perfil de função a partir do modelo existente, como mostrado na imagem:

Properties

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

FEATURES AND 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
Interface Related Configuration	internalif			false	false
Function Config	Function				
External interface Configuration	ExtConfig			false	false
Internal interface Configuration	IntConfig			false	false

Properties

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

FEATURES AND 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
Interface Related Configuration	internalif			false	false
Function Config	Function				
External interface Configuration	ExtConfig			false	false
Internal interface Configuration	IntConfig			false	false

Properties

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

FEATURES AND 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	IntConfigrel	internalif	false	false	

Etapa 5. Crie um Contrato e modifique o campo Escopo para Espaço, conforme mostrado na imagem:

Contract - PERMIT_ALL

Properties

Name: PERMIT_ALL
 Label:
 Scope: Tenant
 QoS Class: Unspecified
 Target DSCP: unspecified
 Description: optional
 Subjects:

Name	Filters
PERMIT_ALL	T1/PERMIT_ALL

Etapa 6. Como mostrado na imagem, crie o Modelo de Gráfico de Serviços L4-L7 no qual a associação do Gráfico de Serviços envolve a associação de uma política de rede roteada externa e a configuração do roteador com uma Política de Seleção de Dispositivos.

:

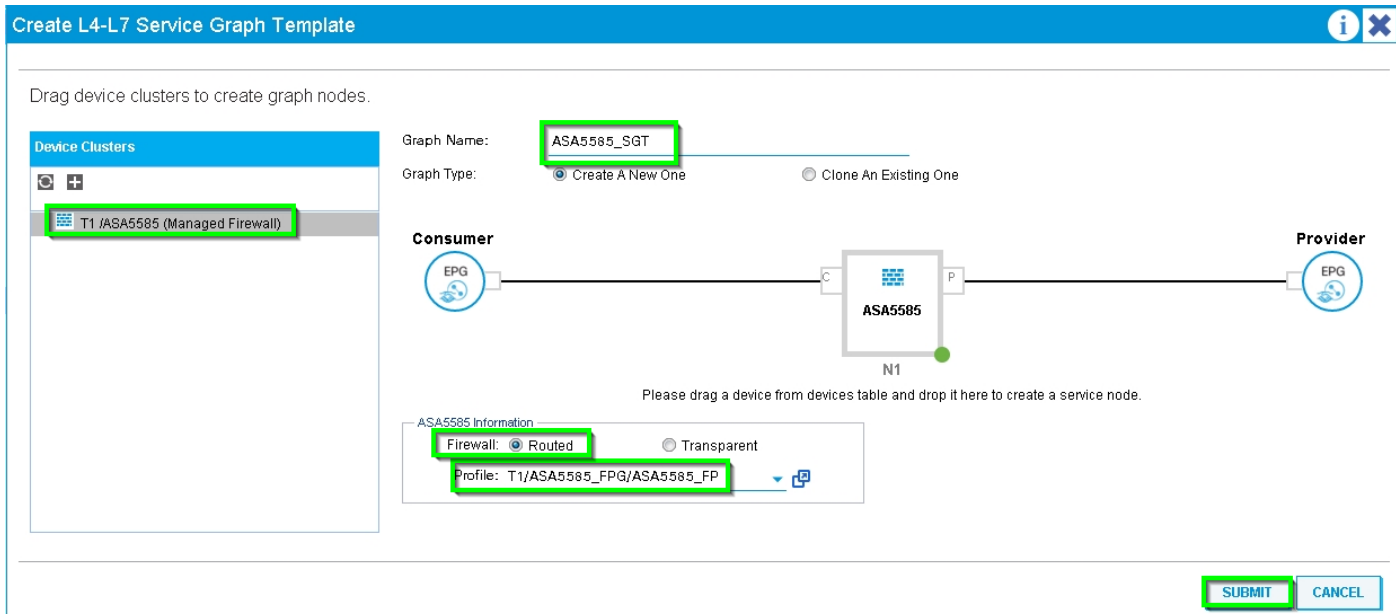
L4-L7 Service Graph Template - ASA5585_SGT

Topology Policy

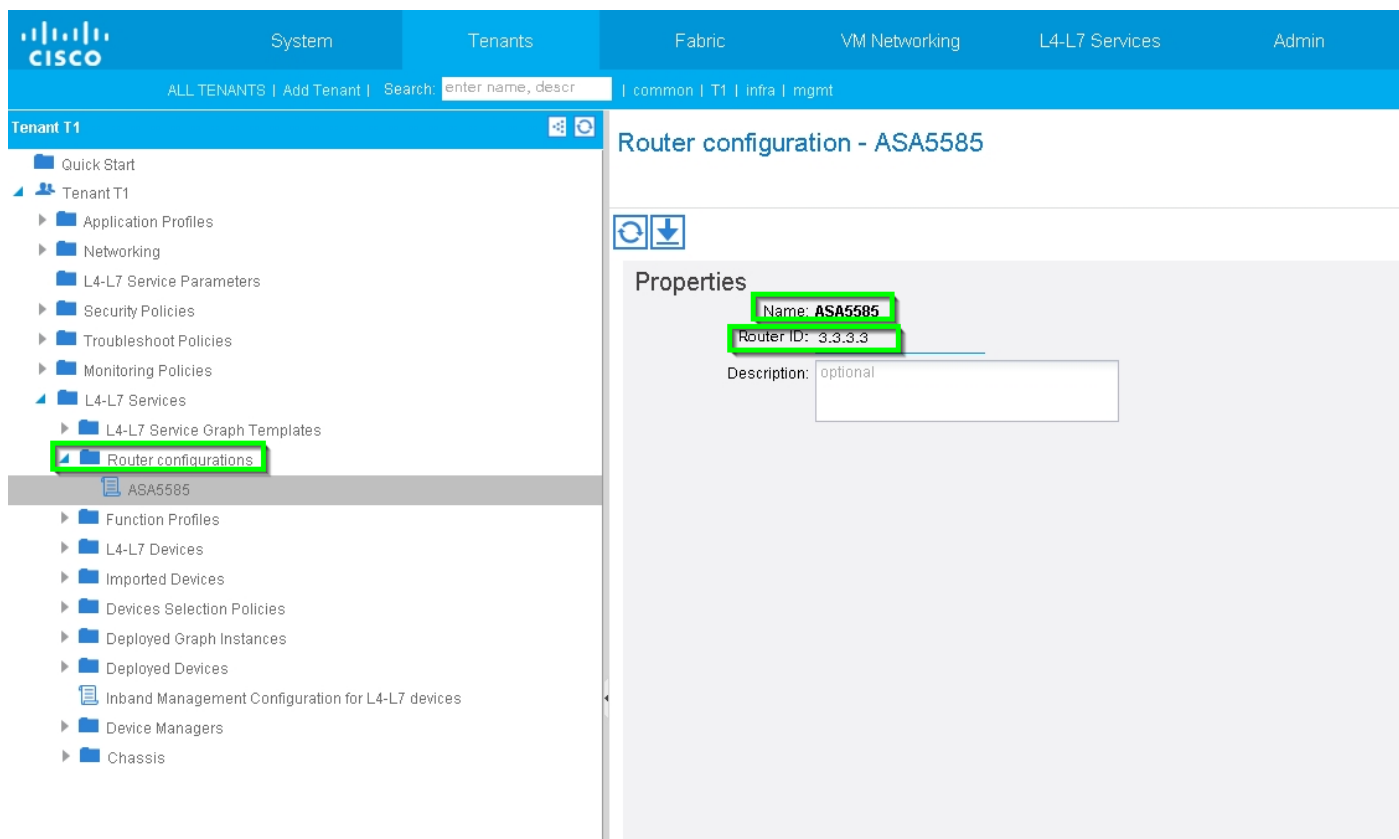
Consumer (EPG) --- ASA5585 (N1) --- Provider (EPG)

ASA5585 Information

- Firewall: Routed
- Profile: ASA5585_IP



Configuração do roteador para especificar o ID do roteador que será usado no Service Appliance (ASA 5585), como mostrado na imagem:



Altere o tipo de adjacência de L2 para L3, conforme mostrado na imagem:

Properties

Name: **ASA5585_SGT**
 Template Name: **UNSPECIFIED**

Configuration Issues:

Description: optional

Label:

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

Name	Provider/Consumer	Description
T1	Consumer	
T2	Provider	

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

Aplicar modelo de gráfico de serviço, como mostrado na imagem:

ASA5585 Information

Firewall: **Routed**
 Profile: **ASA5585_FP**

Anexe o Service Graph ao Contrato, conforme mostrado na imagem:

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

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
 - T1/ASA5585_SGT
 - 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

Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

1. Contract 2. Graph

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)

PREVIOUS NEXT CANCEL

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

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
 - T1/ASA5585_SGT
 - 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

Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

1. Contract 2. Graph 3. ASA5585 Parameters

Config A Service Graph

Device Clusters

- T1/ASA5585 (Managed Firewall)

Graph Template: T1/ASA5585_SGT

Consumer EPG N3K-1_EXT...

ASA5585 N1

Provider EPG N3K-2_EXT...

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

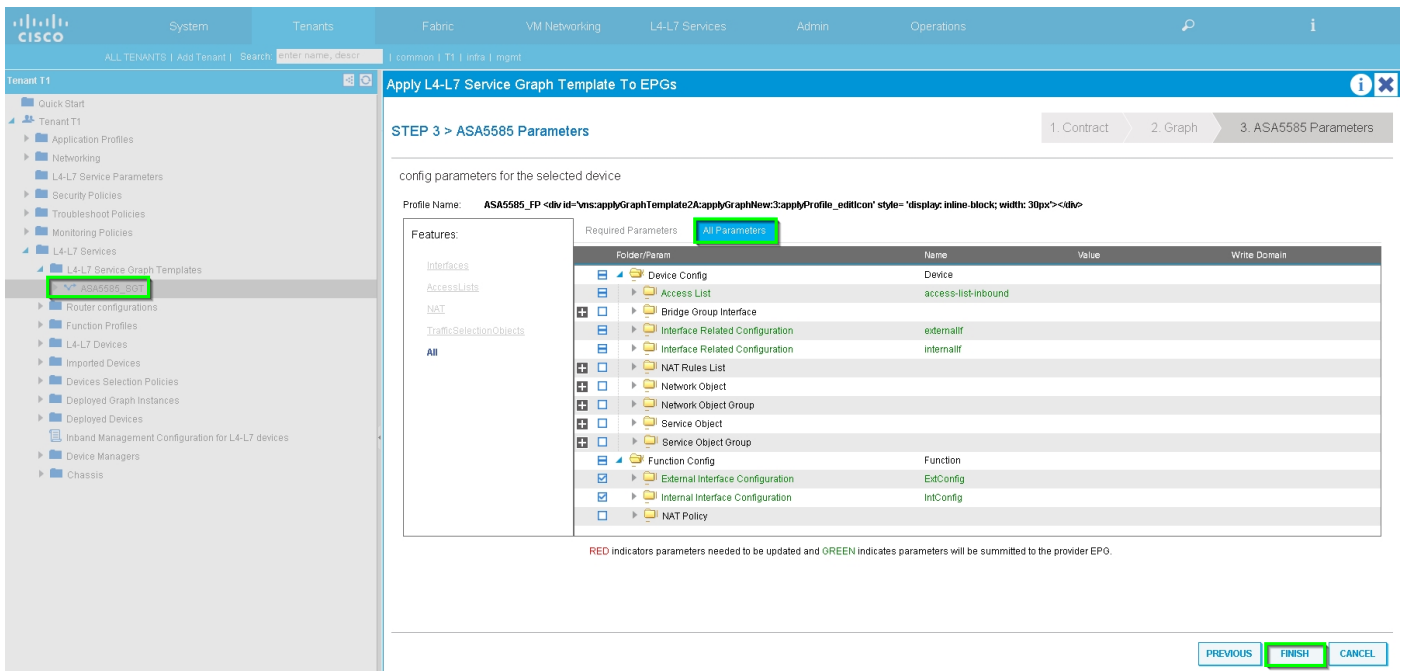
Type: General Route Peering

L3 Ext Network: T1/ASA_IN_L3OUT/ASA_IN_EXT_NET

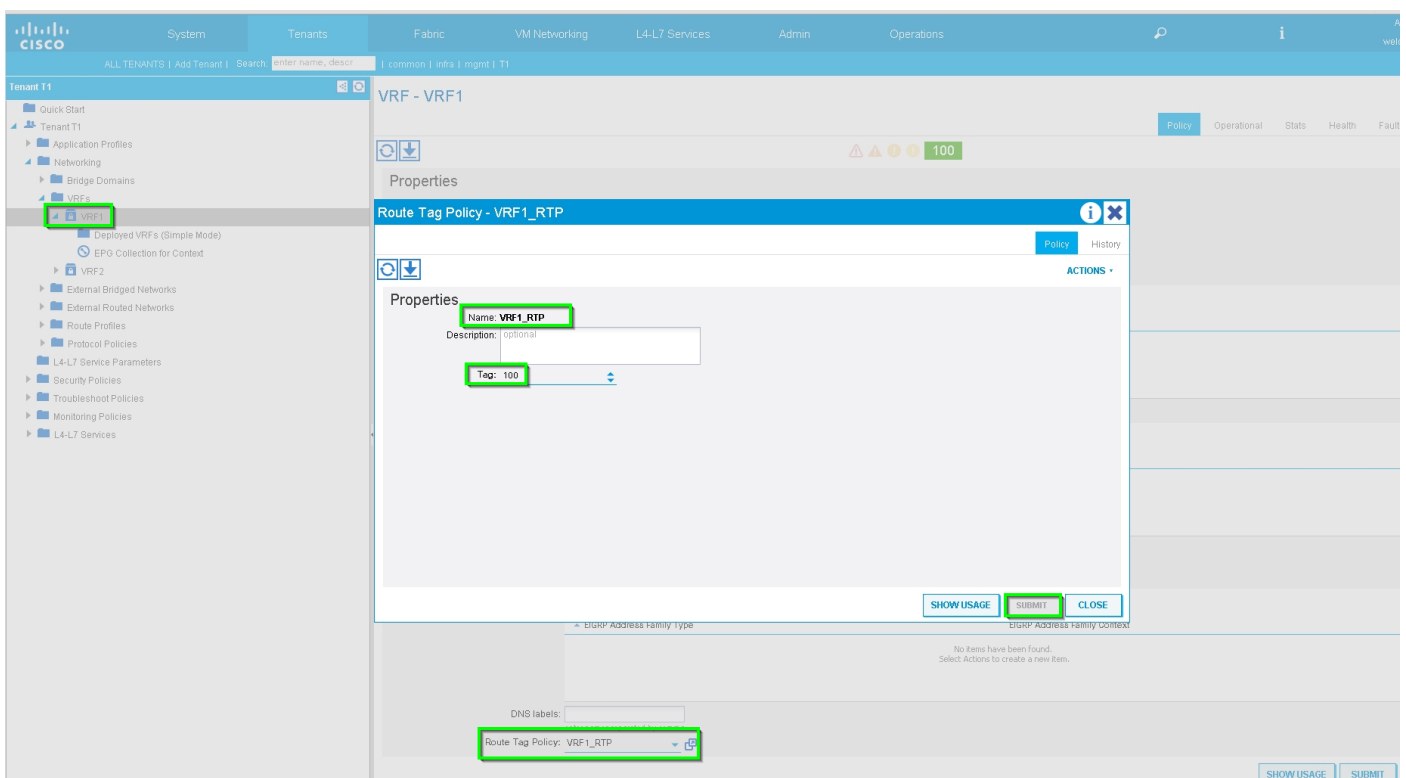
Cluster Interface: inside

PREVIOUS NEXT CANCEL

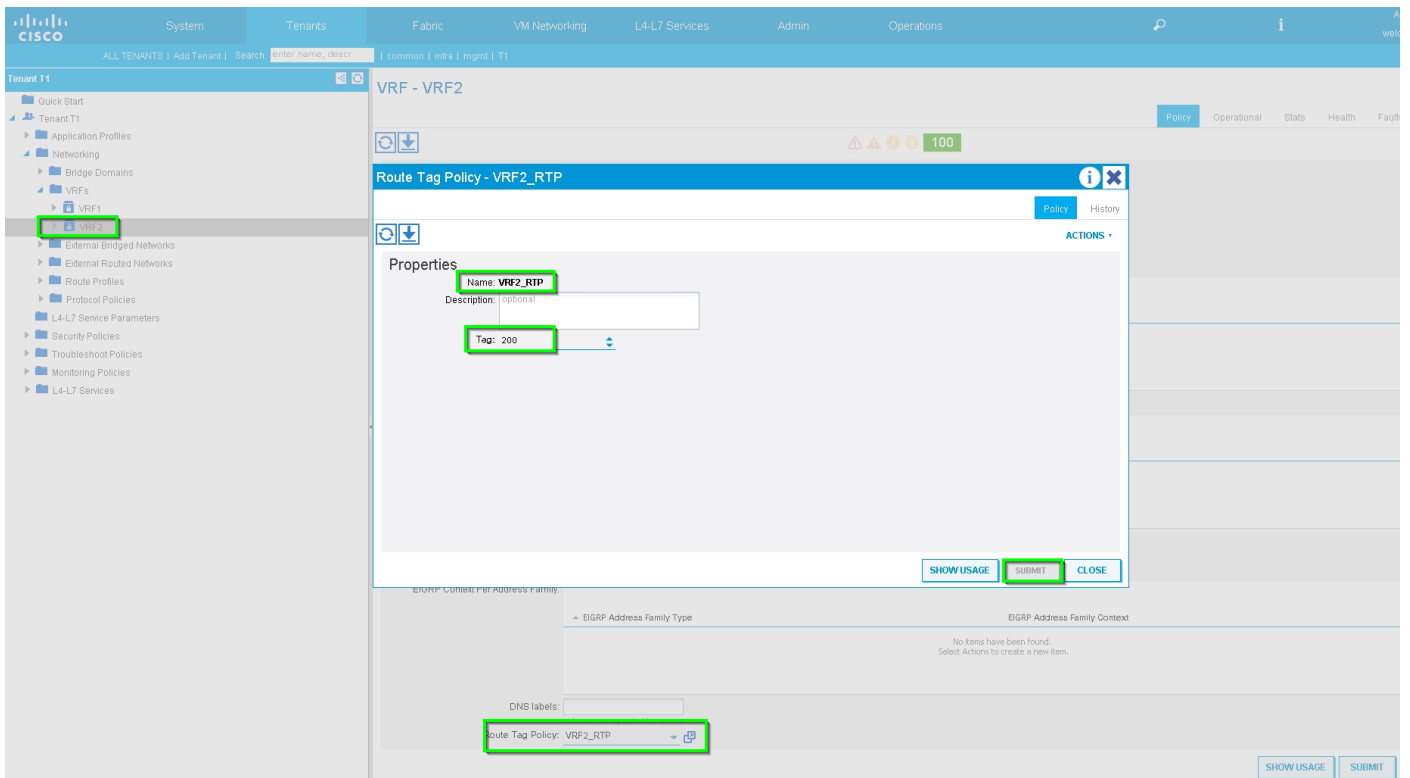
Adicione/altere o parâmetro L4-L7, se necessário, conforme mostrado na imagem:



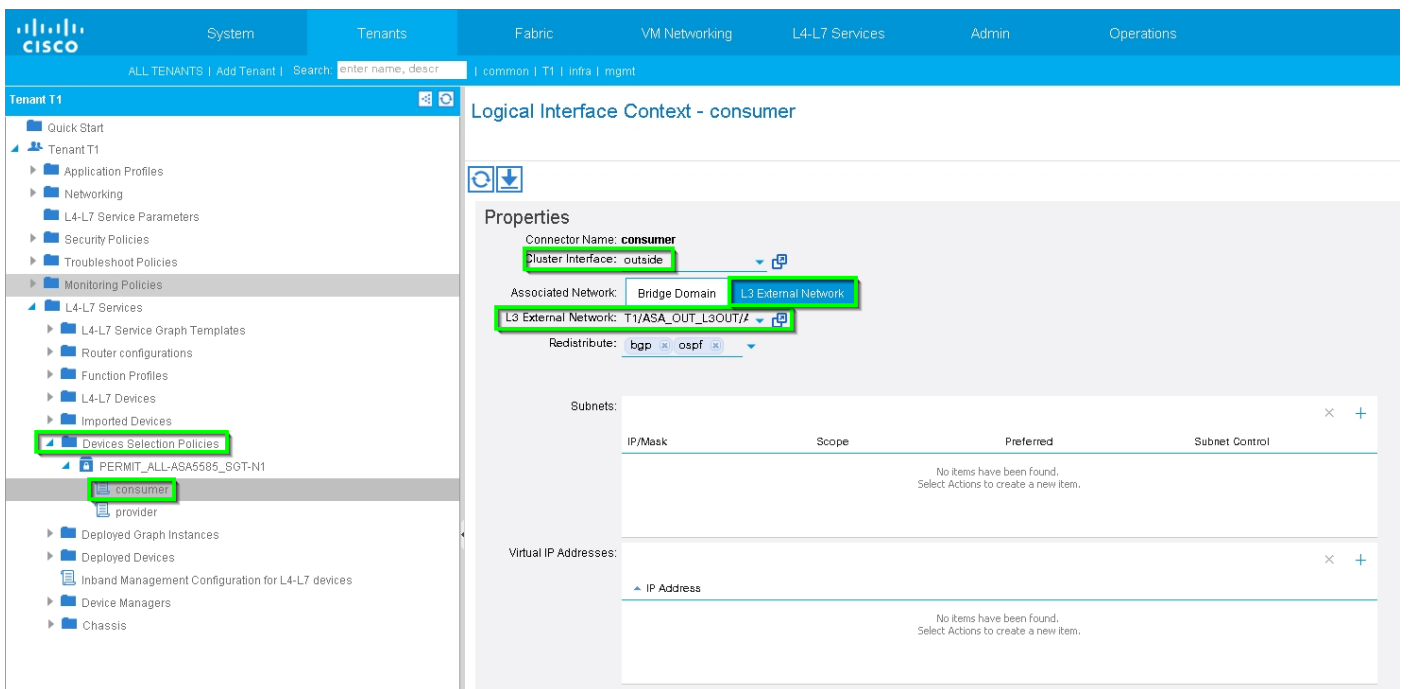
Passo 7: Política de tag de rota, configurar Política de tag de rota para VRF1 (Tag:100), como mostrado na imagem:



Configure a política de etiqueta de rota para VRF2 (Tag:200), como mostrado na imagem:



Passo 8: Verifique o status e verifique a Política de seleção de dispositivo, conforme mostrado na imagem:



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.

Verifique a instância do gráfico implantado, como mostrado na imagem:

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(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

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)

Verificar e solucionar problemas

Configuração APIC para o espaço:

```
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#

```

Verifique a relação de vizinhança do OSPF e a tabela de roteamento na folha 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
```

Verifique a relação de vizinhança do OSPF e a tabela de roteamento na folha 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
```

Verifique a configuração, a relação de vizinhança OSPF e a tabela de roteamento no 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
```

Verifique a configuração, a relação de vizinhança OSPF e a tabela de roteamento em 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

```

Verifique a configuração, a relação de vizinhança OSPF e a tabela de roteamento em 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
```

Verifique as regras de filtro do contrato no leaf e as contagens de ocorrências do pacote..

```
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]
```

Ensaio de acessibilidade entre N3K-1 e 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
```

O arquivo de configuração XML do Espaço e o perfil de função do ASA, usados para esta demonstração, estão anexados.