

# Peering della route L4-L7 con fabric di transito - Procedura dettagliata per la configurazione

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Verifica e risoluzione dei problemi](#)

## Introduzione

Questo documento descrive la procedura dettagliata per la configurazione del grafico dei servizi L4-L7 con peer route, in cui sia il consumer che il provider sono esterni alla struttura ACI (Application Centric Infrastructure).

Contributo di Zahid Hassan, Cisco Advanced Services Engineer.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Pool di VLAN statiche che verranno utilizzati per l'incapsulamento della VLAN tra i dispositivi esterni e la struttura ACI
- Domini fisici e di routing esterni che conetteranno la posizione (nodo/percorso foglia) dei dispositivi esterni e il pool di VLAN
- Connessione di livello 3 a una rete esterna (L3Out)

I passaggi precedenti relativi alle configurazioni **Fabric Access** e **L3Out** non sono illustrati in questo documento e si presume che siano già stati completati.

## Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

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

## Premesse

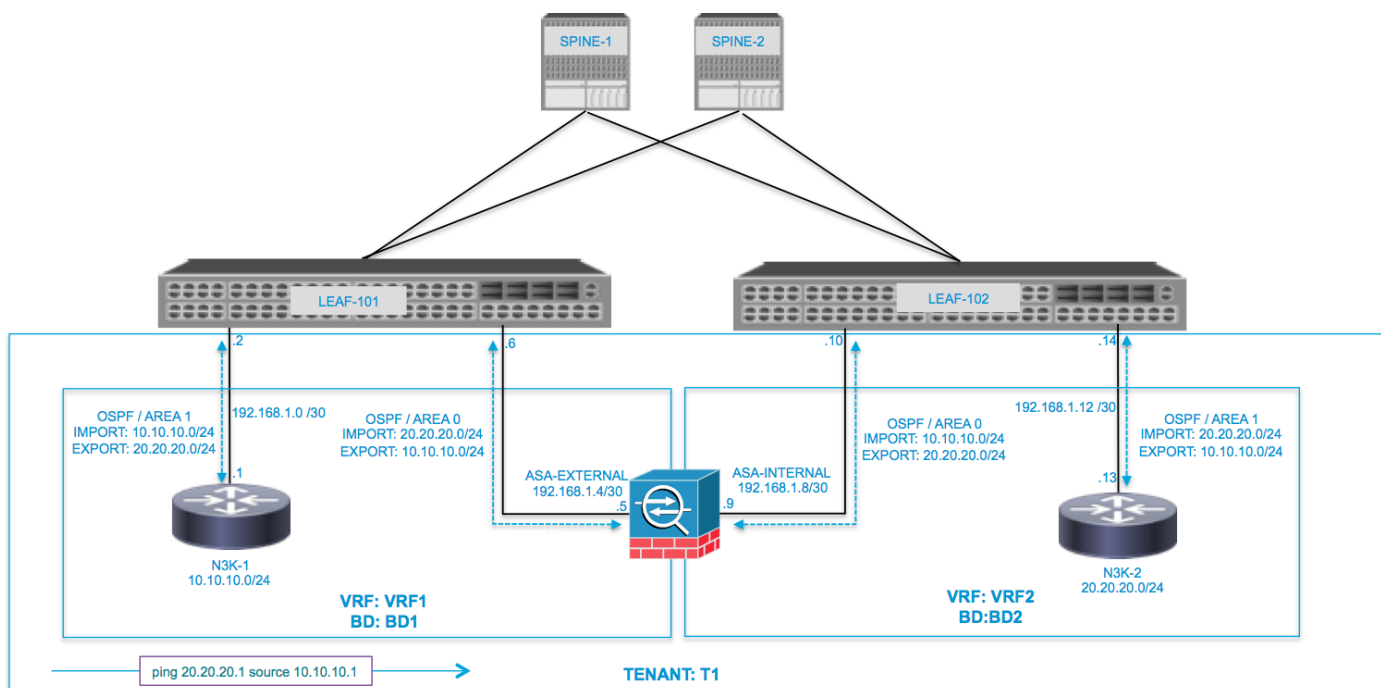
Route Peering è una funzionalità che consente a un'appliance di servizio, ad esempio un servizio di bilanciamento del carico o un firewall, di annunciare la raggiungibilità del dispositivo attraverso la struttura ACI fino a una rete esterna.

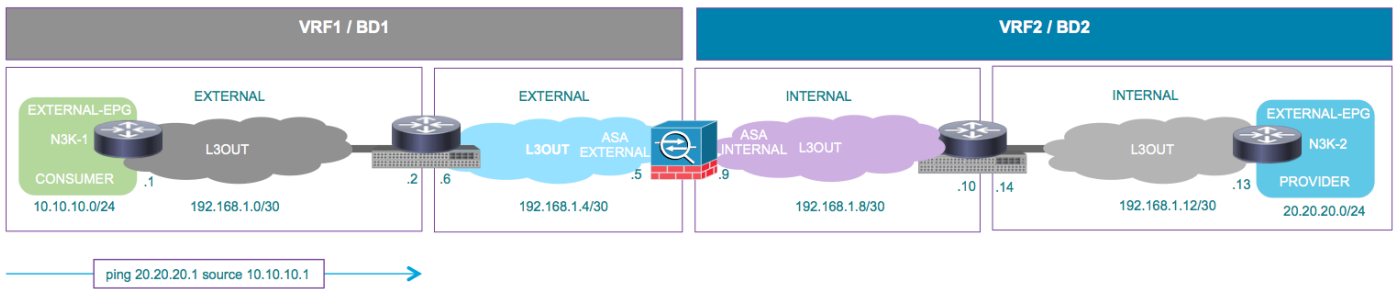
Lo scenario di utilizzo presentato qui è un firewall fisico distribuito come un Service Graph a due bracci, tra due L3Out o gruppi di endpoint esterni (EPG, External End Point Group). Il grafico del servizio è associato a un contratto tra l'EPG esterno sulla foglia 101 (N3K-1) e l'EPG esterno sulla foglia 102 (N3K-2). L'infrastruttura ACI fornisce un servizio di transito per i router (N3K-1 e N3K-2) e viene utilizzato Route Peering, con Open Shortest Path First (OSPF) come protocollo di routing, per scambiare le route tra il firewall e l'infrastruttura ACI.

## Configurazione

### Esempio di rete

Nell'immagine seguente viene illustrato il funzionamento end-to-end di Peering route:

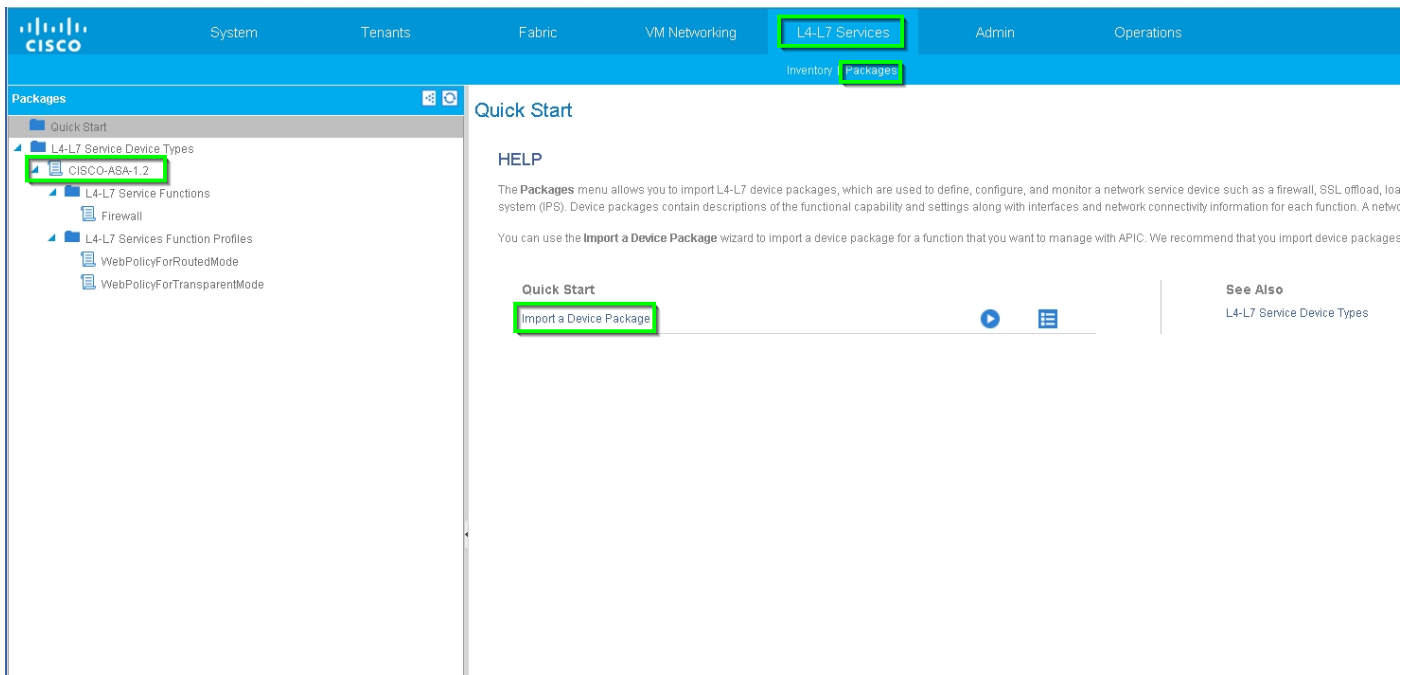




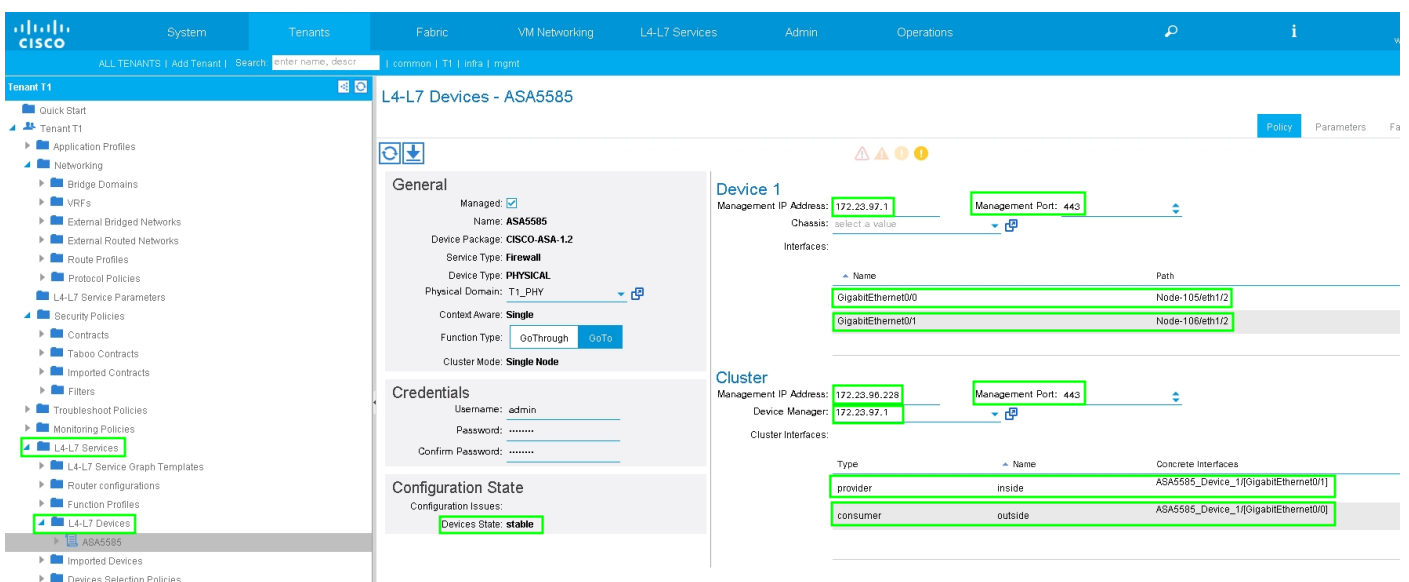
## Configurazione

**Passaggio 1. Configurare Virtual Routing and Forwarding1 (VRF1), VRF2, Bridge Domain1 (BD1) e BD2. Associare BD1 a VRF1 e BD2 a VRF2, come mostrato nell'immagine:**

**Passaggio 2. Caricare il pacchetto del dispositivo ASA in un dispositivo L4-L7, come mostrato nell'immagine, :**



Configurare il dispositivo L4-L7 per l'appliance ASA 5585 (routing) fisica, come mostrato nell'immagine:



### Passaggio 3. Configurare L3Out per N3K-1 e associarlo a BD1 e VRF1.

La rete con routing esterno viene utilizzata per specificare la configurazione di routing nella struttura ACI per il peer route, come mostrato nell'immagine:

**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:  **Regular area**

OSPF Area Cost: 1

**Nota:** Tutte le interfacce L3Out utilizzate per il routing peer devono essere configurate come interfaccia virtuale dello switch (SVI) con l'encap VLAN corrispondente.

**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	<b>wan-100</b>

Routed Sub-Interfaces:

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

Configurare il controllo route di importazione/esportazione nelle subnet per l'EPG esterno N3K-1 L3Out, come mostrato nell'immagine:

**External Network Instance Profile - N3K-1\_EXT\_NET**

**Properties**

Name: **N3K-1\_EXT\_NET**

Tags: 1

Description: optional

Configured VRF name: **VRF1**

Resolved VRF: **unitn-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.

Configurare L3Out per l'interfaccia esterna ASA e associarlo a BD1 e VRF1, come mostrato nell'immagine:

**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 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: **Regular area** (NSSA 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	192.168.1.8/30			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.				

Configurare il controllo route di importazione/esportazione nelle subnet per l'EPG esterno L3Out ASA, come mostrato nell'immagine:

**External Network Instance Profile - ASA\_OUT\_EXT\_NET**

**Properties**

Name: **ASA\_OUT\_EXT\_NET**

Tags: enter tags separated by comma

Description: optional

Configured 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			
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.	

Configurare L3out per ASA-Internal e associarlo a BD2 e VRF2, come mostrato nell'immagine:

**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	<b>vlan-102</b>

Routed Sub-interfaces:

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

Configurare il controllo route di importazione/esportazione sulle subnet per l'EPG esterno L3Out interno ASA, come mostrato nell'immagine:



**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.	

Configurare L3Out per N3K-2 e associarlo a BD2 e VRF2, come mostrato nell'immagine:

**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: **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-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.				

Configurare il controllo route di importazione/esportazione nelle subnet per N3K-2 L3Out per EPG esterno, come mostrato nell'immagine:

**External Network Instance Profile - N3K-2\_EXT\_NET**

**Properties**

Name: **N3K-2\_EXT\_NET**

Tags:

Description: optional

Configured VRF name: **VRF2**

Resolved VRF: **unitn-T1ctx-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.	

**Passaggio 4. Creare il gruppo di profili di funzione e configurare il profilo di funzione dal modello esistente, come mostrato nell'immagine:**

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
        - ASA5585\_FP
  - Imported Devices
  - Devices Selection Policies
  - Deployed Graph Instances
  - Deployed Devices
  - Inband Management Configuration for L4-L7 devices
  - Device Managers
  - Chassis

L4-L7 Services Function Profile - ASA5585\_FP

General | Faults

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
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

General | Faults | History

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

### 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	IntConfigrel	internalif	false	false	

Passaggio 5. Creare un contratto e modificare il campo Ambito in Tenant, come mostrato nell'immagine:

**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

**Passaggio 6.** Come mostrato nell'immagine, creare un modello di Service Graph L4-L7 in cui l'associazione di Service Graph implica l'associazione di un criterio di rete con routing esterno e la configurazione del router a un criterio di selezione del dispositivo.

:

**L4-L7 Service Graph Template - ASA5585\_SGT**

Topology Policy

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

ASA5585 Information

Firewall: Routed  
 Profile: ASA5585\_IP

## 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

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

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

**SUBMIT** **CANCEL**

Configurazione del router per specificare l'ID del router che verrà utilizzato sull'appliance Service (ASA 5585), come mostrato nell'immagine:

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

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**
- ASA5585
  - 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

### Router configuration - ASA5585

Properties

Name: **ASA5585**

Router ID: **3.3.3.3**

Description: optional

Modificate il tipo di adiacenza da L2 a L3, come mostrato nell'immagine:

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  
 ASA5585\_SGT  
 Function Node - N1  
 consumer  
 provider  
 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

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	

Applica modello di Service Graph, come mostrato nell'immagine:

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  
 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

### L4-L7 Service Graph Template - ASA5585\_SGT

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

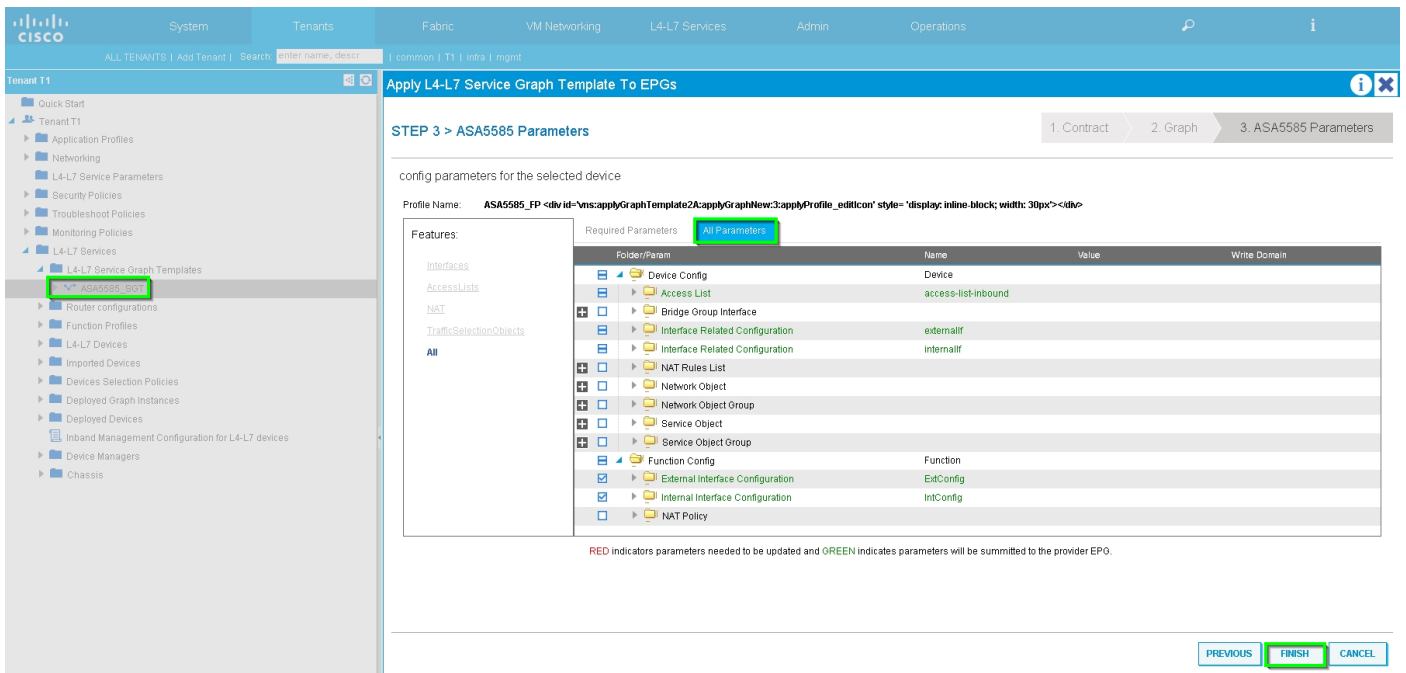
ASA5585 Information  
 Firewall: **Routed**  
 Profile: **ASA5585\_FP**

Allegare il diagramma assistenza al contratto, come mostrato nell'immagine:

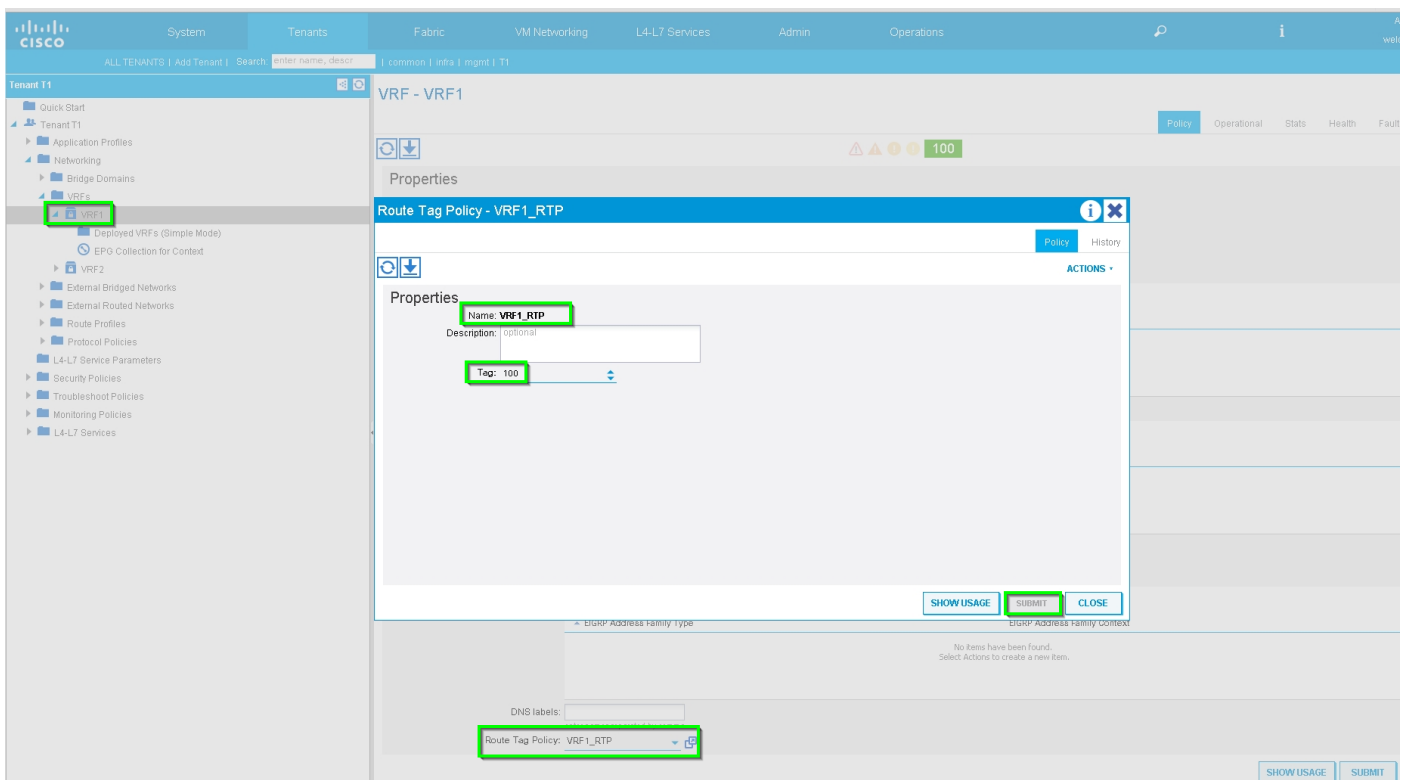
The screenshot shows the Cisco SD-WAN configuration interface for a tenant named 'Tenant T1'. The left sidebar contains a navigation tree with 'L4-L7 Services' and 'L4-L7 Service Graph Templates' highlighted. The main panel is titled 'Apply L4-L7 Service Graph Template To EPGs' and is in 'STEP 1 > Contract' mode. The configuration steps are: 1. Contract, 2. Graph. The 'Config A Contract Between EPGs' section includes 'EPGs Information' with 'Consumer EPG / External Network: T1/NSK-1\_L3OUT/NSK-1\_EXT\_NI' and 'Provider EPG / External Network: T1/NSK-2\_L3OUT/NSK-2\_EXT\_NI'. The 'Contract Information' section shows 'Contract: Create A New Contract' and 'Contract Name: PERMIT\_ALL'. A 'No Filter (Allow All Traffic)' checkbox is checked. At the bottom right, there are 'PREVIOUS', 'NEXT', and 'CANCEL' buttons.

The screenshot shows the same configuration interface in 'STEP 2 > Graph' mode. The configuration steps are: 1. Contract, 2. Graph, 3. ASA5585 Parameters. The 'Config A Service Graph' section includes a 'Device Clusters' list with 'T1/ASA5585 (Managed Firewall)' selected. A diagram shows a central 'ASA5585' device (N1) connected to a 'Consumer' EPG (N3K-1\_EXT...) and a 'Provider' EPG (N3K-2\_EXT...). The 'ASA5585 Information' section includes 'Firewall: routed', 'Profile: ASA5585\_FP', and 'Router Config: T1/ASA5585'. The 'Consumer Connector' section shows 'Type: Route Peering', 'L3 Ext Network: T1/ASA\_OUT\_L3OUT/ASA\_OUT\_EXT\_NE', and 'Cluster Interface: outside'. The 'Provider Connector' section shows 'Type: Route Peering', 'L3 Ext Network: T1/ASA\_IN\_L3OUT/ASA\_IN\_EXT\_NET', and 'Cluster Interface: inside'. At the bottom right, there are 'PREVIOUS', 'NEXT', and 'CANCEL' buttons.

Se necessario, aggiungere/modificare il parametro L4-L7, come mostrato nell'immagine:

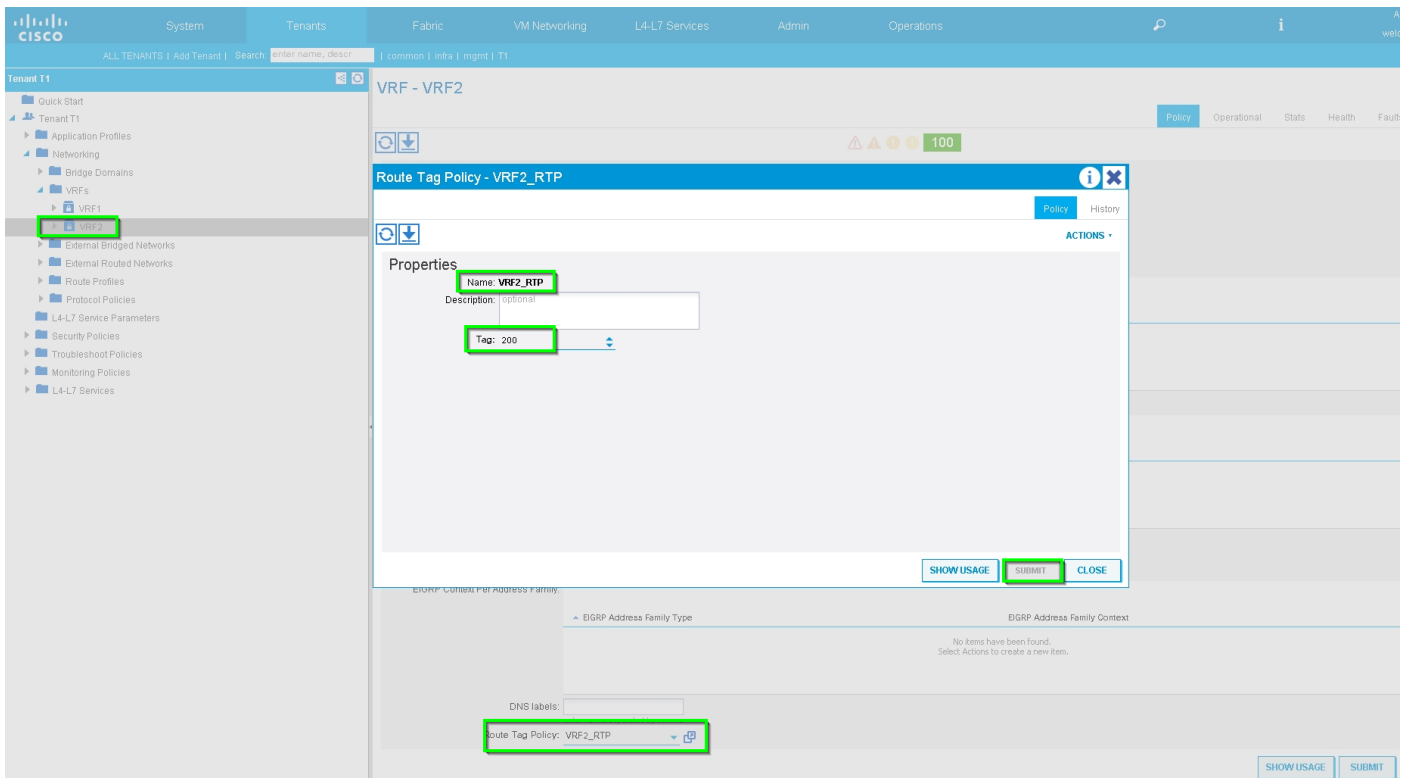


Passaggio 7: Criteri tag route, configurare i criteri tag route per VRF1 (tag:100), come mostrato nell'immagine:

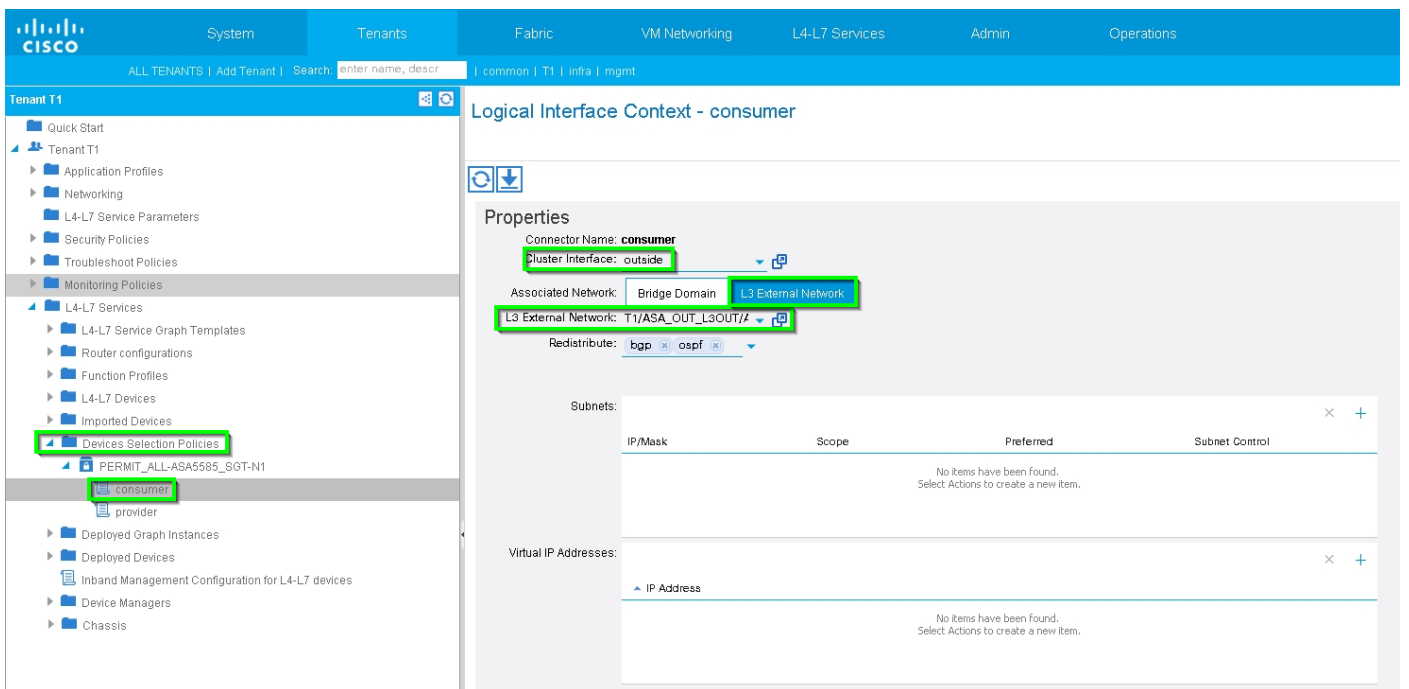


Configurare il criterio Route-Tag per VRF2 (Tag:200), come mostrato nell'immagine:





**Passaggio 8: Controllare lo stato e verificare il criterio di selezione del dispositivo, come mostrato nell'immagine:**



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/ASA

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.

Verificare l'istanza di Deployed Graph, come mostrato nell'immagine:

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)gabitEthernet0/1	unknown
outside		ASA5585_Device_1(0)gabitEthernet0/0	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 consumer 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)

## Verifica e risoluzione dei problemi

Configurazione APIC per tenant:

```
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#

```

Verificare la relazione tra nodi adiacenti OSPF e la tabella di routing nella foglia 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
```

**Verificare la relazione di router adiacente OSPF e la tabella di routing nella foglia 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
```

**Verificare la configurazione, la relazione tra nodi adiacenti OSPF e la tabella di routing su 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
```

Verificare la configurazione, la relazione tra nodi adiacenti OSPF e la tabella di routing in 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
```

## Verificare la configurazione, la relazione tra nodi adiacenti OSPF e la tabella di routing in 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
```

**Verificare le regole di filtro del contratto sulla foglia e il numero di riscontri del pacchetto:.**

```
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]
```

**Prova di raggiungibilità tra 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
```

In allegato è il file di configurazione XML per il tenant e il profilo delle funzioni ASA, utilizzato per questa dimostrazione.