

L4-L7-Routen-Peering mit Transit-Fabric - Konfigurationsanleitung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Überprüfung und Fehlerbehebung](#)

Einführung

In diesem Dokument wird die Konfigurationsanleitung für L4-L7-Servicediagramme mit Route Peering beschrieben, in der sowohl der Consumer als auch der Provider sich außerhalb der ACI-Fabric befinden.

Unterstützt von Zahid Hassan, Cisco Advanced Services Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Statische VLAN-Pools für das Kapselungs-VLAN zwischen den externen Geräten und der ACI-Fabric
- Externe physische und geroutete Domänen, die den Standort (Leaf-Knoten/Pfad) der externen Geräte und den VLAN-Pool verbinden.
- Layer-3-Verbindung mit einem externen Netzwerk (L3Out)

Die vorhergehenden **Fabric Access**- und **L3Out**-Konfigurationsschritte werden in diesem Dokument nicht behandelt, und es wird davon ausgegangen, dass sie bereits abgeschlossen wurden.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco Application Policy Infrastructure Controller (Cisco APIC) - 1.2(1 m)
- Adaptive Security Appliance (ASA)-Gerätepaket - 1,2/4,8
- ASA 5585 - 9.5(1)
- Nexus 3064 - 6.0(2)U3(7)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

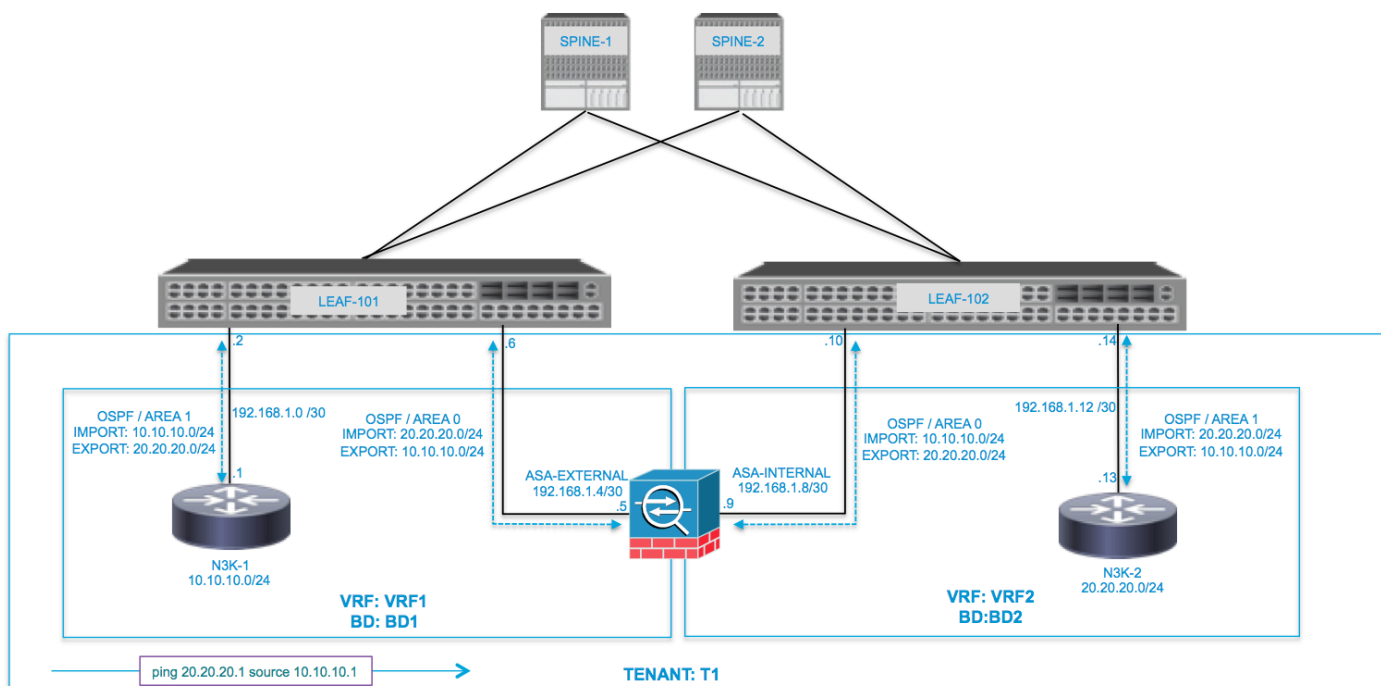
Route Peering ist eine Funktion, mit der eine Service-Appliance wie ein Load Balancer oder eine Firewall die Erreichbarkeit über die ACI-Fabric bis hin zu einem externen Netzwerk ankündigen kann.

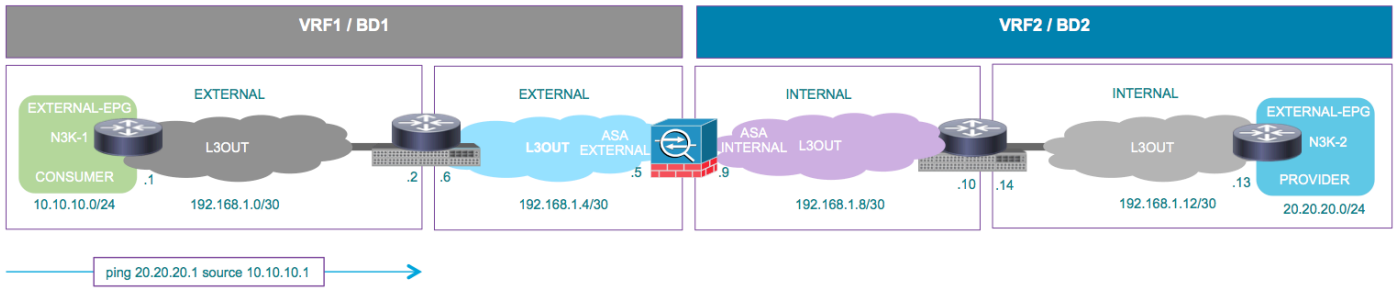
Der hier vorgestellte Anwendungsfall ist eine physische Firewall, die als zweiartiger Servicediagramm zwischen zwei L3Outs oder externen Endpunktgruppen (EPGs) bereitgestellt wird. Der Servicediagramm ist mit einem Vertrag zwischen der externen EPG auf Leaf 101 (N3K-1) und der externen EPG auf Leaf 102 (N3K-2) verknüpft. Die ACI-Fabric stellt einen Transit-Service für die Router (N3K-1 und N3K-2) bereit, und Routen-Peering wird mit Open Shortest Path First (OSPF) als Routing-Protokoll für den Austausch von Routen zwischen der Firewall und der ACI-Fabric verwendet.

Konfigurieren

Netzwerkdiagramm

Das folgende Bild zeigt die End-to-End-Funktionsweise von Routen-Peering:



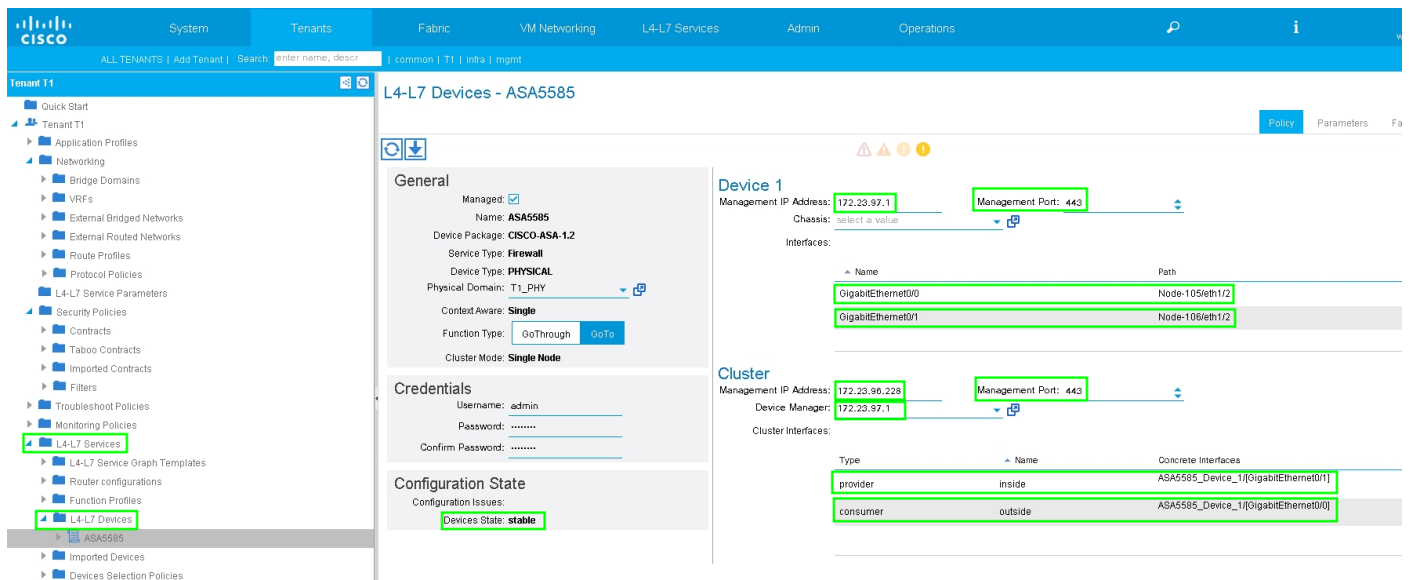


Konfigurieren

Schritt 1: Konfigurieren Sie Virtual Routing and Forwarding1 (VRF1), VRF2, Bridge Domain1 (BD1) und BD2. Ordnen Sie BD1 VRF1 und BD2 VRF2 zu, wie im Bild gezeigt:

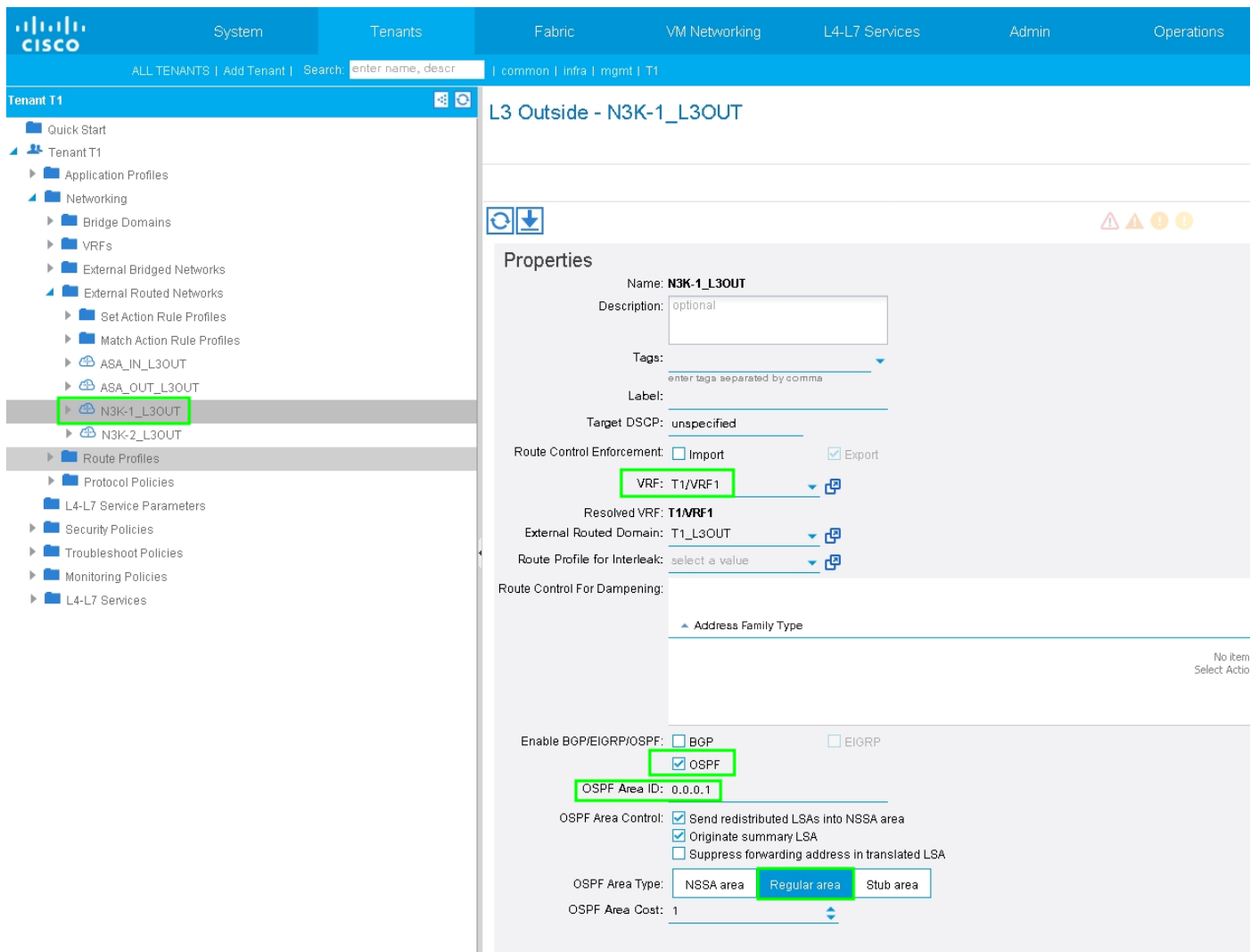
Schritt 2: Laden Sie das ASA-Gerätepaket unter L4-L7-Gerät hoch, wie im Bild gezeigt:

Konfigurieren Sie das L4-L7-Gerät für die physische ASA 5585 (geroutet), wie im Bild gezeigt:



Schritt 3: L3Out für N3K-1 konfigurieren und BD1 und VRF1 verknüpfen.

Externes geroutetes Netzwerk wird verwendet, um die Routing-Konfiguration in der ACI-Fabric für Routen-Peering anzugeben, wie im Bild gezeigt:



Hinweis: Alle L3Out-Schnittstellen, die für das Routen-Peering verwendet werden, müssen

als Switch Virtual Interface (SVI) mit VLAN-Encap konfiguriert werden.

The screenshot displays the configuration page for the Logical Interface Profile 'N3K-1_IP'. The left-hand navigation pane shows the hierarchy: Tenant T1 > Networking > External Routed Networks > N3K-1_L3OUT > Logical Interface Profiles > N3K-1_IP. The main configuration area includes the following sections:

- Properties:** Name: N3K-1_IP, Description: optional, Label: (empty), ND policy: select a value, Egress Data Plane Policing Policy: select a value, Ingress Data Plane Policing Policy: select a value.
- Routed Interfaces:** A table with columns Path, IP Address, MAC Address, and MTU (Bytes). It contains no data rows.
- SVI:** A table with columns Path, IP Address, Side A IP, Side B IP, MAC Address, MTU (Bytes), and Encap. It contains one row: Node-105/eth1/3, 192.168.1.2/30, (empty), (empty), 00:22:BD:F8:19:FF, 1500, and vlan-100.
- Routed Sub-Interfaces:** A table with columns Path, IP Address, MAC Address, MTU (Bytes), and Encap. It contains no data rows.

Konfigurieren Sie die Import-/Export-Route-Control für Subnetze für N3K-1 L3Out External EPG, wie im Bild gezeigt:

The screenshot displays the configuration page for the External Network Instance Profile 'N3K-1_EXT_NET'. The left-hand navigation pane shows the hierarchy: Tenant T1 > Networking > External Routed Networks > N3K-1_L3OUT > Networks > N3K-1_EXT_NET. The main configuration area includes the following sections:

- Properties:** Name: N3K-1_EXT_NET, Tags: 1, Description: optional, Configured VRF name: VRF1, Resolved VRF: uni:tn-11:ctx-vrf1, QoS Class: Unspecified, Target DSCP: unspecified, Configuration Status: applied.
- Subnets:** A table with columns IP Address, Scope, Aggregate, and Route Control Profile. It contains two rows: 10.10.10.0/24 (External Subnets for the External EPG) and 20.20.20.0/24 (Export Route Control Subnet).
- Route Control Profile:** A table with columns Name and Direction. It contains no data rows.

Konfigurieren Sie L3Out für die ASA-externe Schnittstelle, und ordnen Sie es BD1 und VRF1 zu, wie im Bild gezeigt:

L3 Outside - ASA_OUT_L3OUT

Properties

Name: **ASA_OUT_L3OUT**

Description: optional

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: **T1/VRF1**

Resolved VRF: **T1/VRF1**

External Routed Domain: T1_L3OUT

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type:

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

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: **0**

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

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

OSPF Area Cost:

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. | | | | |

Konfigurieren Sie die Import-/Export-Routenkontrolle für Subnetze für ASA-External L3Out External EPG, wie im Bild gezeigt:

System Tenants Fabric VM Networking L4-L7 Services Admin Operations

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

Tenant T1

External Network Instance Profile - ASA_OUT_EXT_NET

Policy Operational Stats

General Contracts

Properties

Name: ASA_OUT_EXT_NET

Tags: enter tags separated by comma

Description: optional

Configured VRF name: VRF1

Resolved VRF: unitn-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 EPoS Shared Route Control Subnet | | | |

Route Control Profile:

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

Konfigurieren Sie L3out für ASA-Internal, und ordnen Sie es BD2 und VRF2 zu, wie im Bild gezeigt:

System Tenants Fabric VM Networking L4-L7 Services Admin Operations

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

Tenant T1

L3 Outside - ASA_IN_L3OUT

Properties

Name: ASA_IN_L3OUT

Description: optional

Tags: 1

Label: enter tags separated by comma

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

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. | | | | |

Konfigurieren Sie die Import-/Export-Routenkontrolle für Subnetze für ASA-Internal L3Out External EPG, wie im Bild gezeigt:

External Network Instance Profile - ASA_IN_EXT_NET

Properties

Name: **ASA_IN_EXT_NET**

Tags: enter tags separated by comma

Description: optional

Configured 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. | |

Konfigurieren Sie L3Out für N3K-2, und ordnen Sie es BD2 und VRF2 zu, wie im Bild gezeigt:

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
 - Bridge Domains
 - VRFs
 - External Bridged Networks
 - External Routed Networks
 - Set Action Rule Profiles
 - Match Action Rule Profiles
 - ASA_IN_L3OUT
 - ASA_OUT_L3OUT
 - N3K-1_L3OUT
 - N3K-2_L3OUT**
 - Logical Node Profiles
 - Networks
 - Route Profiles
 - Route Profiles
 - Protocol Policies
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services

L3 Outside - N3K-2_L3OUT

Properties

Name: **N3K-2_L3OUT**

Description: optional

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: **T1/VRF2**

Resolved VRF: **T1/VRF2**

External Routed Domain: T1_L3OUT

Route Profile for Interleak: select a value

Route Control For Dampening:

Address Family Type:

Route Dampening Policy:

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

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: **0.0.0.1**

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

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

OSPF Area Cost: 0

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
 - Bridge Domains
 - VRFs
 - External Bridged Networks
 - External Routed Networks
 - Set Action Rule Profiles
 - Match Action Rule Profiles
 - ASA_IN_L3OUT
 - ASA_OUT_L3OUT
 - N3K-1_L3OUT
 - N3K-2_L3OUT**
 - Logical Node Profiles
 - N3K-2_IP**
 - Logical Interface Profiles
 - N3K-2_IP**
 - OSPF Interface Profile
 - Configured Nodes
 - Networks
 - Route Profiles
 - Route Profiles
 - Protocol Policies
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services

Logical Interface Profile - N3K-2_IP

Properties

Name: **N3K-2_IP**

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed Interfaces:

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

SVI:

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

Routed Sub-Interfaces:

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

Konfigurieren Sie die Import-/Export-Routenkontrolle für Subnetze für N3K-2 L3Out für externe EPG, wie im Bild gezeigt:

External Network Instance Profile - N3K-2_EXT_NET

Properties

Name: **N3K-2_EXT_NET**

Tags:

Description: optional

Configured VRF name: **VRF2**

Resolved VRF: **uni1tn-11ctx-VRF2**

QoS Class: **Unspecified**

Target DSCP: **unspecified**

Configuration Status: **applied**

Configuration Issues:

Subnets:

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

Route Control Profile:

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

Schritt 4: Erstellen Sie die Funktionsprofilgruppe, und konfigurieren Sie das Funktionsprofil aus der vorhandenen Vorlage, wie im Bild gezeigt:

L4-L7 Services Function Profile - ASA5585_FP

Properties

Name: **ASA5585_FP**

Description:

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

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 |



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 | |

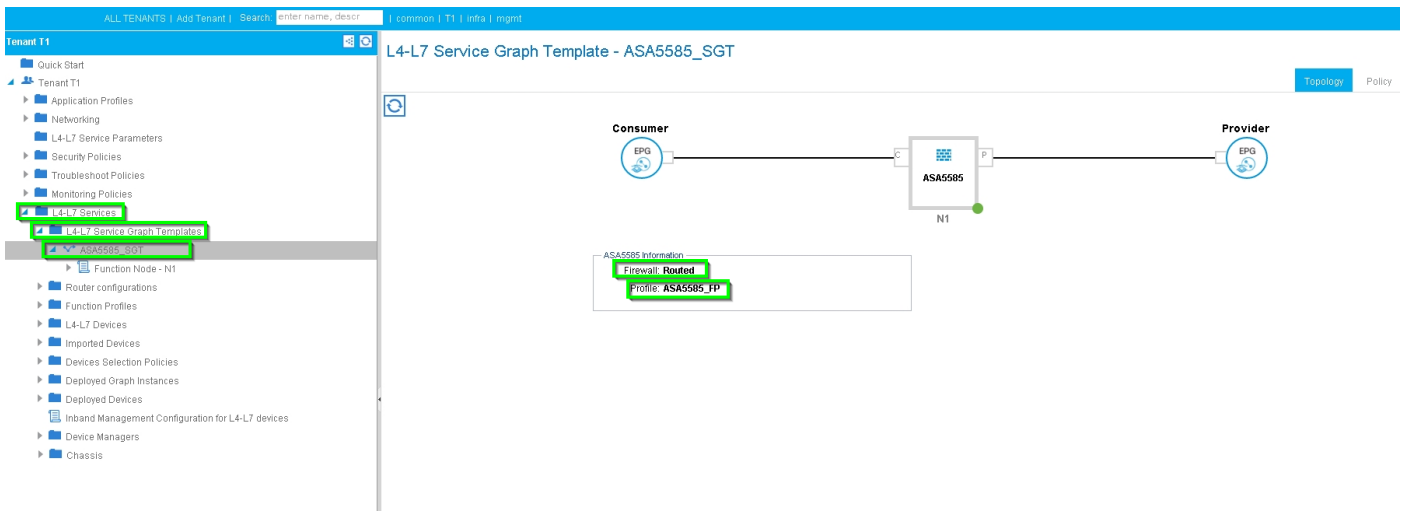
Schritt 5: Erstellen Sie einen Vertrag, und ändern Sie das Feld "Scope" (Umfang) in "Tenant" (Tenant), wie im Bild gezeigt:

The screenshot shows the Cisco ICM interface for configuring a contract. The left sidebar shows a tree view with 'Contracts' selected under 'Tenant T1'. The main area displays the configuration for 'Contract - PERMIT_ALL'. The 'Properties' section includes:

- Name: PERMIT_ALL
- Label: (empty)
- Scope: Tenant (highlighted in green)
- QoS Class: Unspecified
- Target DSCP: unspecified
- Description: optional
- Subjects: A table with columns 'Name' and 'Filters'. The entry is PERMIT_ALL with filters T1/PERMIT_ALL.

Schritt 6: Erstellen Sie, wie im Bild gezeigt, eine L4-L7-Servicediagrammvorlage, bei der die Zuordnung von Servicediagrammen zu einer externen gerouteten Netzwerkrichlinie und einer Routerkonfiguration mit einer Richtlinie für die Geräteauswahl beinhaltet.

:



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_FP/ASA5585_FP

SUBMIT CANCEL

Router-Konfiguration zur Angabe der Router-ID, die auf der Service Appliance (ASA 5585) verwendet wird, wie in der Abbildung gezeigt:

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

Ändern Sie den Adjacency-Typ von L2 in L3, wie in der Abbildung gezeigt:

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

Properties

Name: **ASA5585_SGT**

Template Name: **UNSPECIFIED**

Configuration Issues:

Description: optional

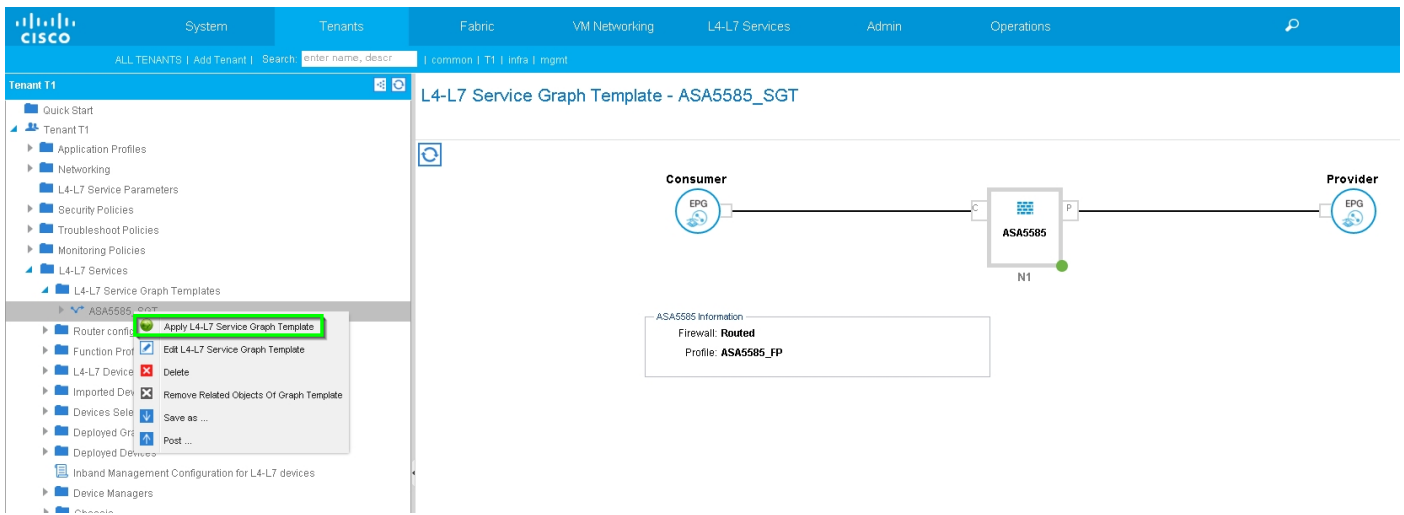
Label:

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

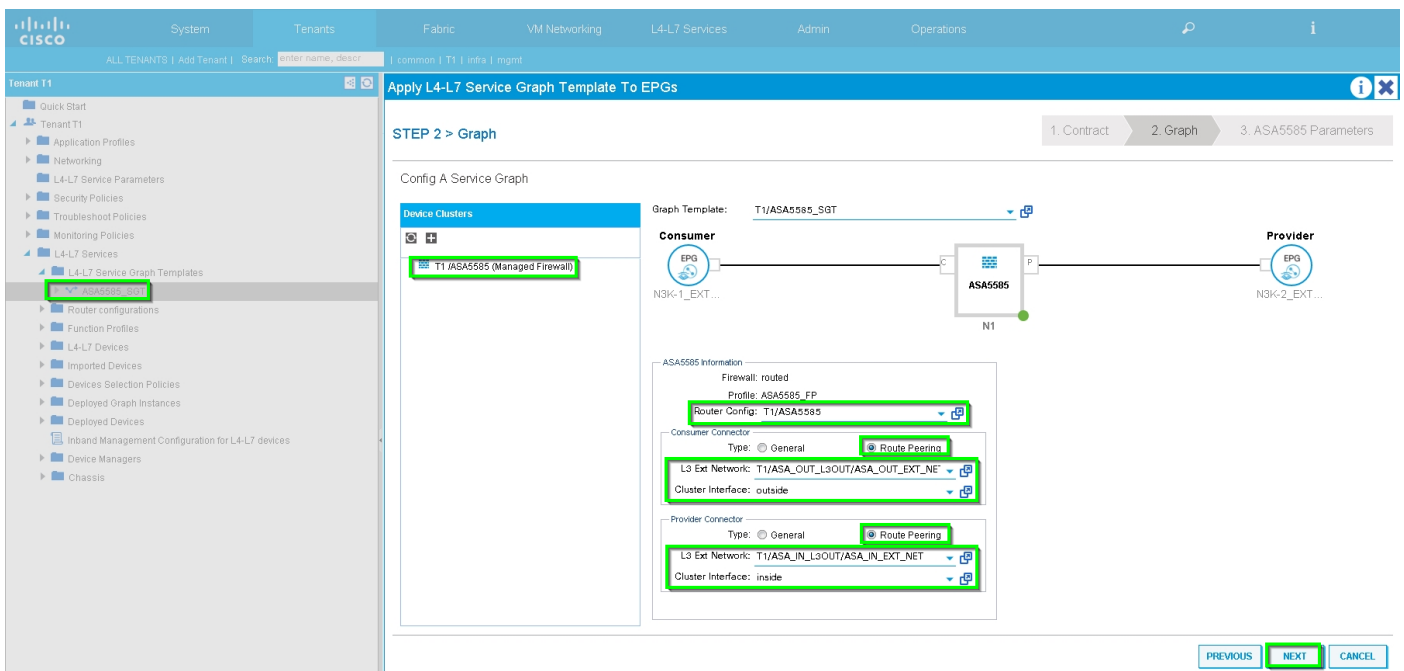
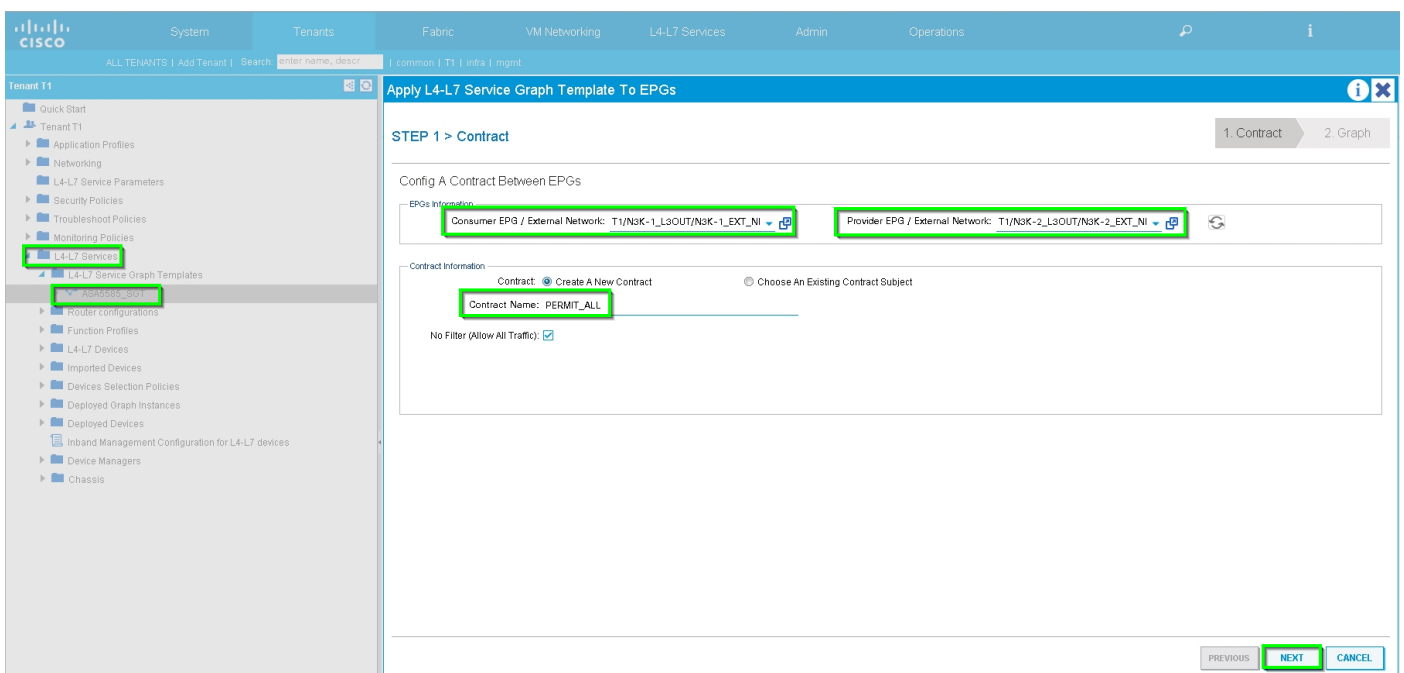
| Terminal Nodes: | Name | Provider/Consumer | Description |
|-----------------|------|-------------------|-------------|
| | T1 | Consumer | |
| | T2 | Provider | |

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

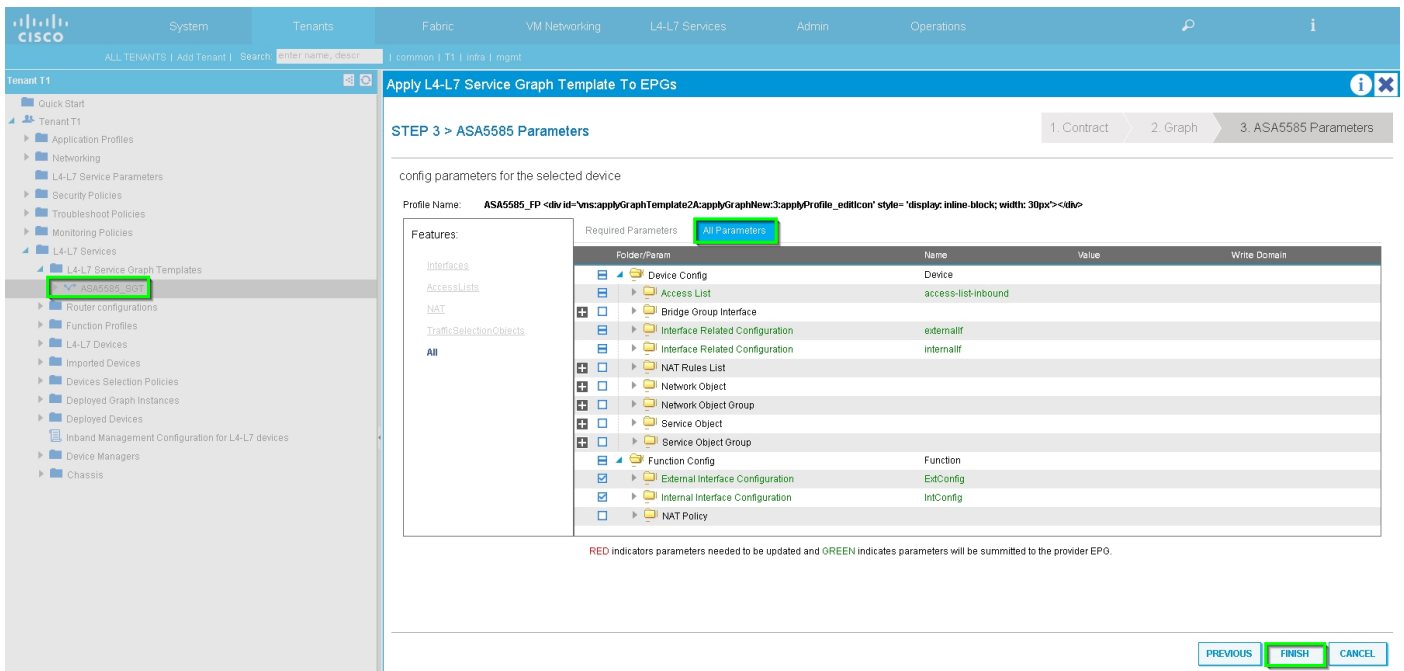
Vorlage für Servicediagramme anwenden, wie im Bild gezeigt:



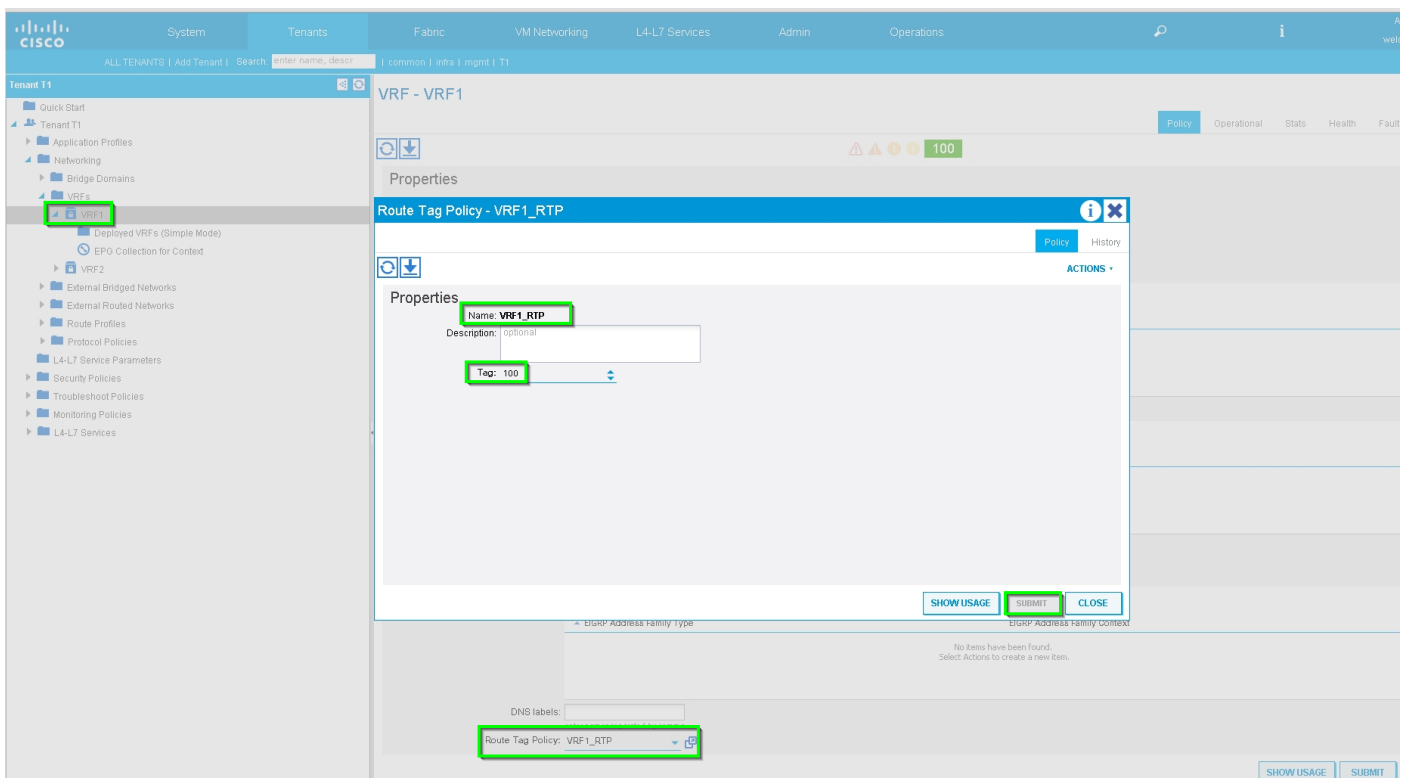
Hinzufügen des Servicediagramms zum Vertrag, wie im Bild gezeigt:



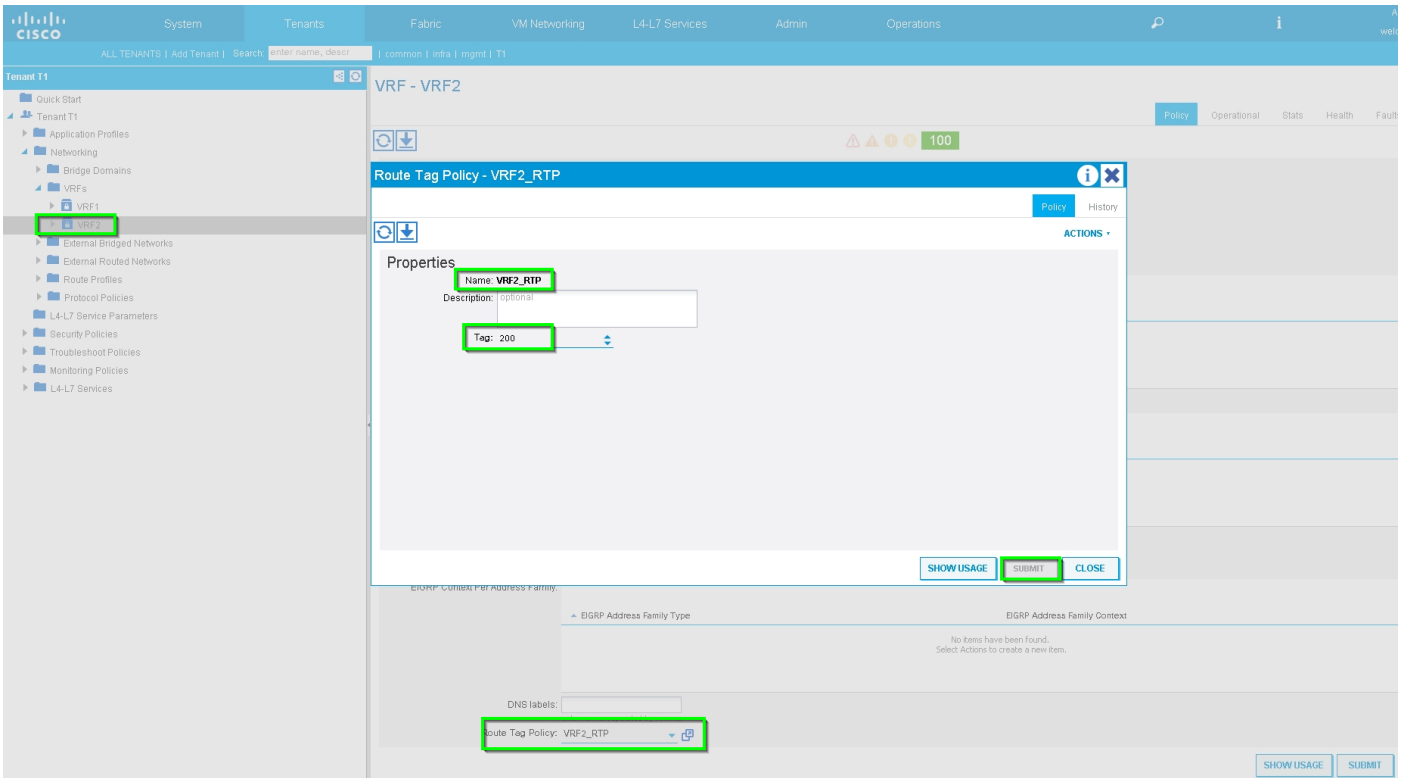
Fügen Sie ggf. den L4-L7-Parameter hinzu bzw. ändern Sie ihn, wie im Bild gezeigt:



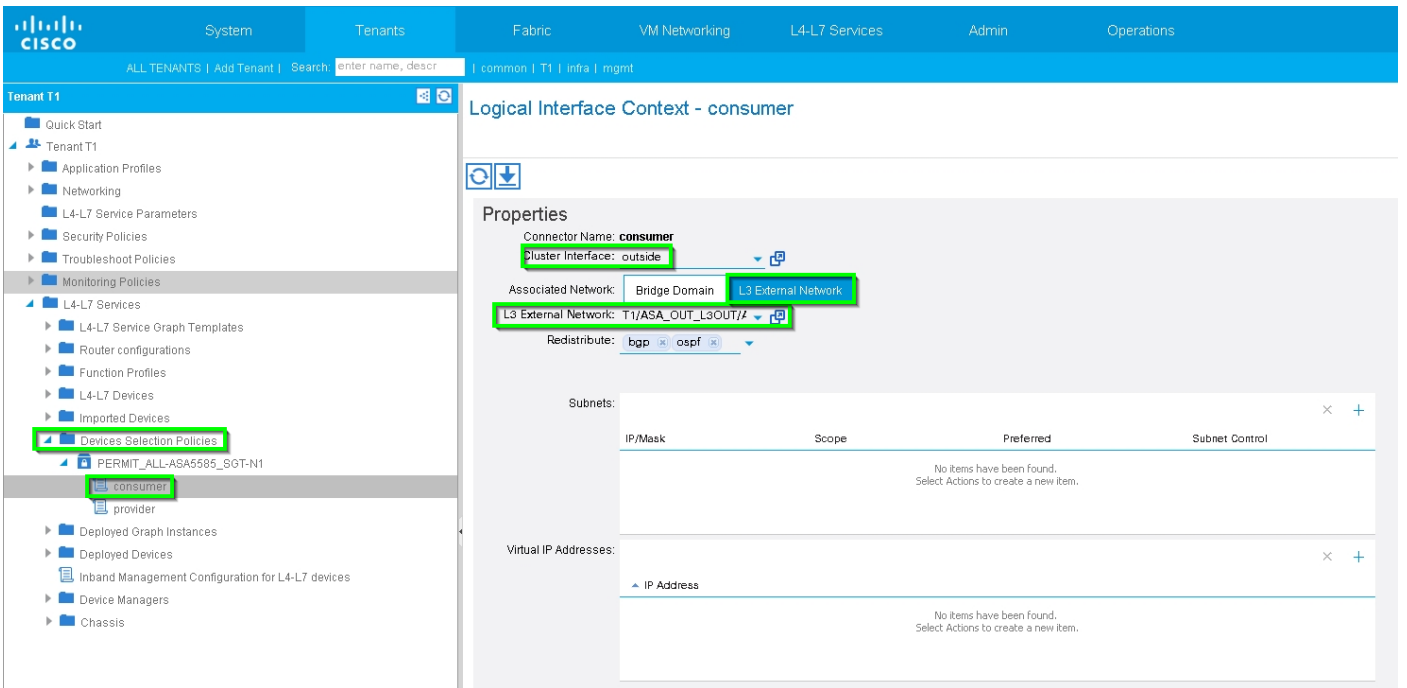
Schritt 7: Route-Tag-Richtlinie, Konfigurieren der Route-Tag-Richtlinie für VRF1 (Tag:100), wie im Bild gezeigt:



Konfigurieren Sie die Route-Tag-Richtlinie für VRF2 (Tag:200), wie im Bild gezeigt:



Schritt 8: Überprüfen Sie den Status, und überprüfen Sie die Richtlinie für die Geräteauswahl, wie im Bild gezeigt:



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. |

Überprüfen Sie die Instanz des bereitgestellten Diagramms, wie im Bild gezeigt:

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 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) |

Überprüfung und Fehlerbehebung

APIC-Konfiguration für Tenant:

```
apicl# 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#

```

Überprüfen Sie die OSPF-Nachbarbeziehung und die Routing-Tabelle auf Blatt 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
```

Überprüfen Sie die OSPF-Nachbarbeziehung und die Routing-Tabelle auf Blatt 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
```

Überprüfen Sie die Konfiguration, die OSPF-Nachbarbeziehung und die Routing-Tabelle auf der 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
```

Überprüfung der Konfiguration, der OSPF-Nachbarbeziehung und der Routing-Tabelle auf 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
```

Überprüfung der Konfiguration, der OSPF-Nachbarbeziehung und der Routing-Tabelle auf 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
```

Überprüfen Sie die Vertragsfilterregeln für das Leaf und die Anzahl der Paketergebnisse:.

```
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 ]
```

Erreichbarkeitstest zwischen N3K-1 und 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
```

Angehängt ist die XML-Konfigurationsdatei für den Tenant und das ASA-Funktionsprofil, die für diese Demonstration verwendet wird.