

트랜짓 패브릭을 사용한 L4-L7 경로 피어링 - 구성 연습

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[확인 및 문제 해결](#)

소개

이 문서에서는 소비자 및 공급자 모두 ACI(Application Centric Infrastructure) 패브릭의 외부에 있는 경로 피어링을 사용하는 L4-L7 서비스 그래프의 컨피그레이션 연습을 설명합니다.

기고자: Zahid Hassan, Cisco Advanced Services 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 외부 디바이스와 ACI 패브릭 간의 캡슐화 VLAN에 사용할 고정 VLAN 풀
- 외부 장치 및 VLAN 풀의 위치(리프 노드/경로)를 연결하는 외부 물리적 및 라우티드 도메인
- 외부 네트워크에 대한 레이어 3 연결(L3Out)

앞의 패브릭 액세스 및 L3Out 구성 단계는 이 문서에서 다루지 않으며 이미 완료된 것으로 간주되었습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco APIC(Application Policy Infrastructure Controller) - 1.2(1m)
- ASA(Adaptive Security Appliance) 디바이스 패키지 - 1.2.4.8
- ASA 5585 - 9.5(1)

- Nexus 3064 - 6.0(2)U3(7)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

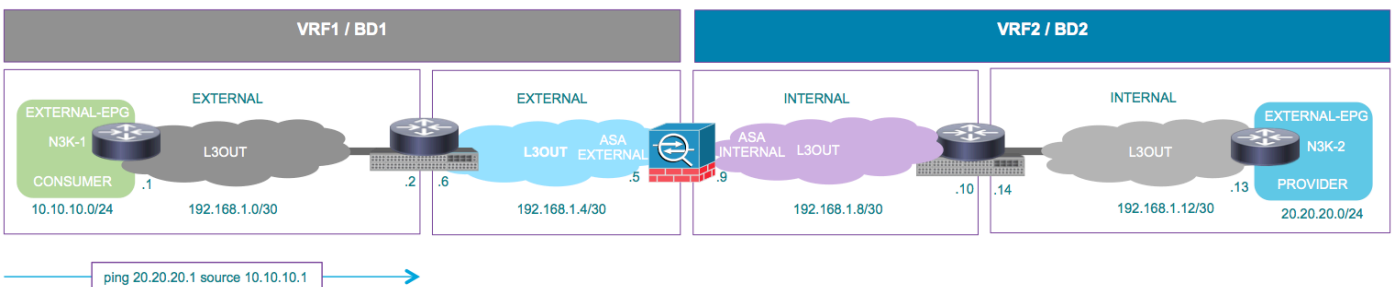
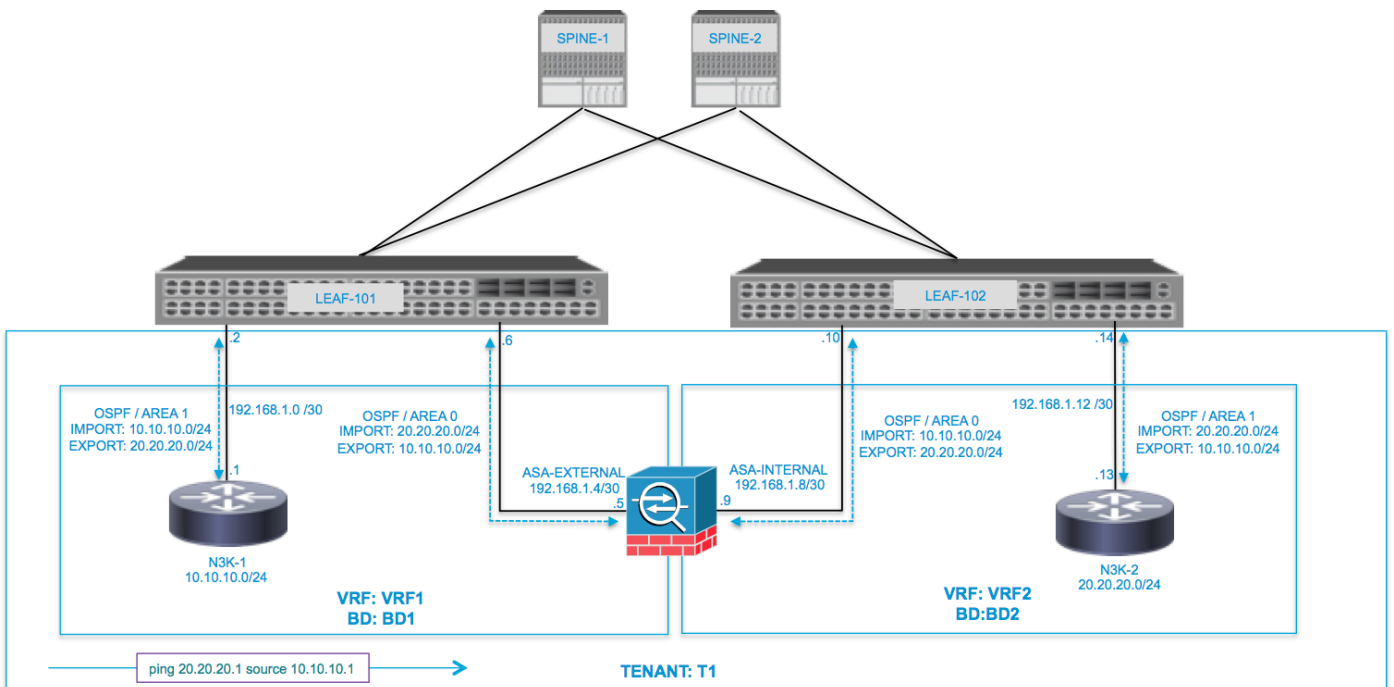
Route Peering은 로드 밸런서 또는 방화벽과 같은 서비스 어플라이언스에서 ACI 패브릭을 통해 외부 네트워크로 연결할 수 있는 연결성을 알릴 수 있는 기능입니다.

여기에 제시된 활용 사례는 2개의 L3Outs 또는 외부 EPG(End Point Groups) 사이에 2암 서비스 그래프로 구축된 물리적 방화벽입니다. 서비스 그래프는 Leaf 101(N3K-1)의 외부 EPG와 Leaf 102(N3K-2)의 외부 EPG 간의 계약과 연결됩니다. ACI 패브릭은 라우터에 트랜짓 서비스(N3K-1 및 N3K-2)를 제공하고 라우팅 프로토콜로 OSPF(Open Shortest Path First)를 사용하여 방화벽과 ACI 패브릭 간의 경로를 교환합니다.

구성

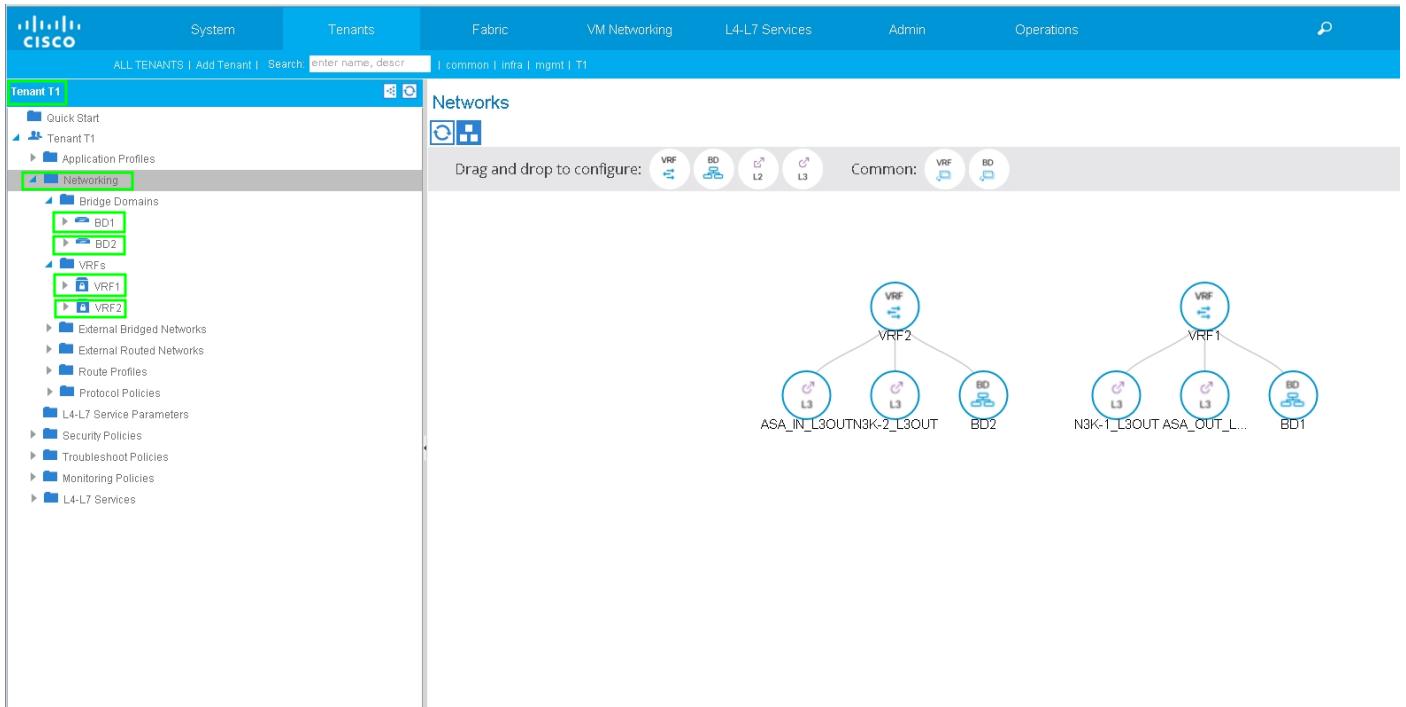
네트워크 다이어그램

다음 이미지는 경로 피어링이 엔드 투 엔드 방식으로 작동하는 방식을 보여줍니다.

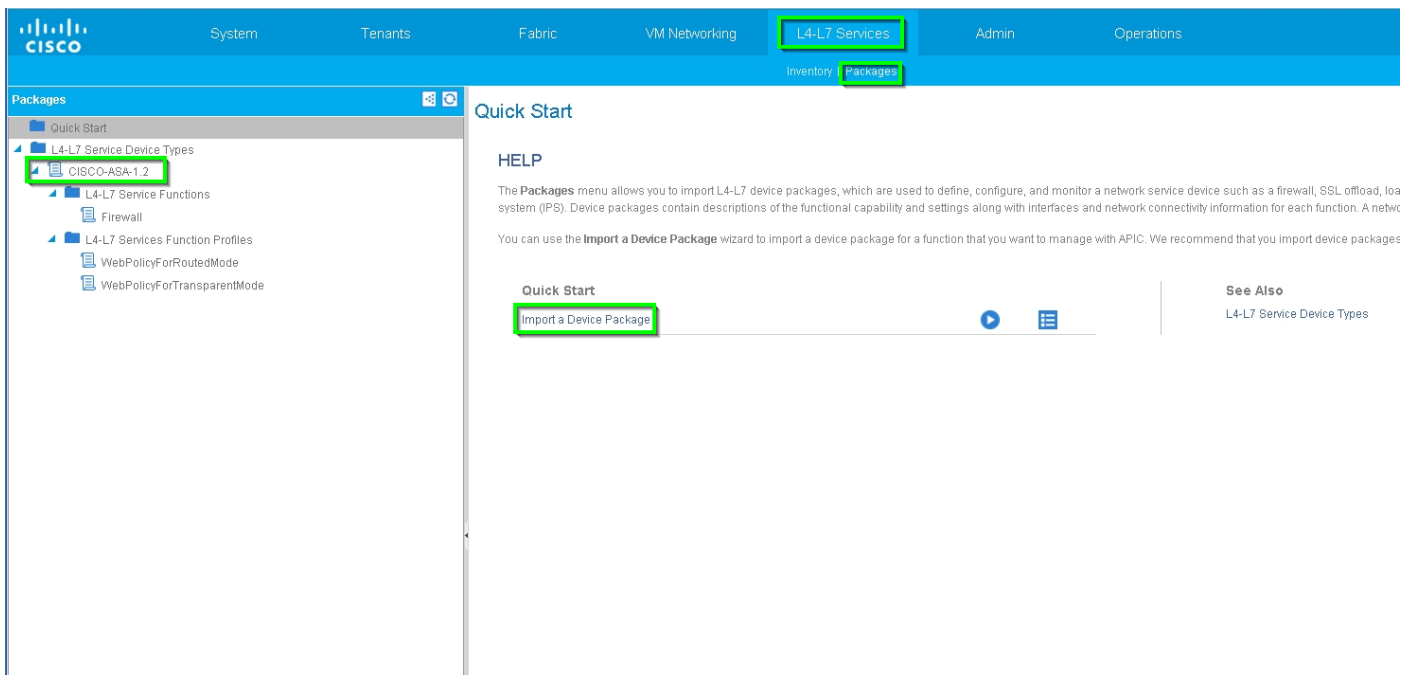


구성

1단계. 가상 라우팅 및 포워딩(VRF1), VRF2, 브리지 도메인1(BD1) 및 BD2를 구성합니다. 이미지에 표시된 대로 BD1을 VRF1에 연결하고 BD2를 VRF2에 연결합니다.



2단계. 이미지에 표시된 대로 L4-L7 디바이스 아래에 ASA 디바이스 패키지를 업로드합니다.



이미지에 표시된 대로 물리적 ASA 5585(라우터드)에 대해 L4-L7 디바이스를 구성합니다.

The screenshot shows the Cisco ACI GUI for configuring L4-L7 devices. The left sidebar is expanded to 'L4-L7 Devices' under 'Tenant T1'. The main configuration area is titled 'L4-L7 Devices - ASA5585'. It includes sections for 'General' (Name: ASA5585, Device Package: CISCO-ASA-1.2, Service Type: Firewall), 'Credentials' (Username: admin), and 'Configuration State' (Devices State: stable). The 'Device 1' section shows Management IP Address: 172.23.97.1, Management Port: 443, and a table of interfaces:

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

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

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

3단계. N3K-1에 대해 L3Out을 구성하고 BD1 및 VRF1과 연결합니다.

외부 라우티드 네트워크는 다음 이미지에 표시된 것처럼 경로 피어링을 위한 ACI 패브릭에서 라우팅 컨피그레이션을 지정하는 데 사용됩니다.

The screenshot shows the Cisco ACI GUI for configuring L3 Outside. The left sidebar is expanded to 'N3K-1_L3OUT' under 'Tenant T1'. The main configuration area is titled 'L3 Outside - N3K-1_L3OUT'. The 'Properties' section includes:

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

참고: Route Peering에 사용되는 모든 L3Out 인터페이스는 그에 따라 VLAN 캡슐화가 포함된 SVI(Switch Virtual Interface)로 구성해야 합니다.

Logical Interface Profile - N3K-1_IP

Properties

Name: **N3K-1_IP**

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed Interfaces:

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

SVI:

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

Routed Sub-Interfaces:

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

이미지에 표시된 대로 N3K-1 L3Out 외부 EPG에 대한 서브넷에서 Import/Export Route Control을 구성합니다.

External Network Instance Profile - N3K-1_EXT_NET

Properties

Name: **N3K-1_EXT_NET**

Tags: 1

Description: optional

Configured VRF name: **VRF1**

Resolved VRF: **uni4tn-T1ctx-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.	

ASA 외부 인터페이스에 대해 L3Out을 구성하고 이미지에 표시된 대로 BD1 및 VRF1과 연결합니다

L3 Outside - ASA_OUT_L3OUT

Properties

Name: **ASA_OUT_L3OUT**

Description: optional

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: **T1/VRF1**

Resolved VRF: **T1/VRF1**

External Routed Domain: T1_L3OUT

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type:

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

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: **0**

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

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

OSPF Area Cost: 0

Logical Interface Profile - ASA_OUT_IP

Properties

Name: **ASA_OUT_IP**

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed interfaces:

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

SVI:

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

Routed Sub-Interfaces:

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

이미지에 표시된 대로 ASA-External L3Out External EPG용 서브넷에서 Import/Export Route Control을 구성합니다.

External Network Instance Profile - ASA_OUT_EXT_NET

Policy Operational Stats

General Contracts

Properties

Name: ASA_OUT_EXT_NET

Tags: enter tags separated by comma

Description: optional

Configured VRF name: VRF1

Resolved VRF: untn-T1/ctx-VRF1

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: applied

Configuration Issues:

Subnets:

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

Route Control Profile:

Name Direction

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

이미지에 표시된 대로 ASA-Internal에 대해 L3out을 구성하고 BD2 및 VRF2와 연결합니다.

L3 Outside - ASA_IN_L3OUT

Properties

Name: ASA_IN_L3OUT

Description: optional

Tags: 1

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: T1/VRF2

Resolved VRF: T1/VRF2

External Routed Domain: T1_L3OUT

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type Route Dampening Policy

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

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: 0

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

OSPF Area Type: NSSA area Regular area Stub area

OSPF Area Cost: 0

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.				

이미지에 표시된 대로 ASA-Internal L3Out External EPG용 서브넷에서 Import/Export Route Control을 구성합니다.

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.	

이미지에 표시된 대로 N3K-2에 대해 L3Out을 구성하고 BD2 및 VRF2와 연결합니다.

L3 Outside - N3K-2_L3OUT

Properties

Name: **N3K-2_L3OUT**

Description: optional

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: Import Export

VRF: **T1/VRF2**

Resolved VRF: **T1/VRF2**

External Routed Domain: T1_L3OUT

Route Profile for Interleak: select a value

Route Control For Dampening:

Address Family Type:

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

Enable BGP/EIGRP/OSPF: BGP OSPF EIGRP

OSPF Area ID: **0.0.0.1**

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

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

OSPF Area Cost: 0

Logical Interface Profile - N3K-2_IP

Properties

Name: **N3K-2_IP**

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed Interfaces:

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

SVI:

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

Routed Sub-Interfaces:

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

이미지에 표시된 대로 N3K-2 L3Out for External EPG에 대해 서브넷에서 Import/Export Route Control을 구성합니다.

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.	

4단계. 이미지에 표시된 대로 기능 프로파일 그룹을 생성하고 기존 템플릿에서 기능 프로파일을 구성합니다.

L4-L7 Services Function Profile - ASA585_FP

Properties

Name: **ASA585_FP**

Description:

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

FEATURES AND PARAMETERS

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

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	

5단계. 다음 이미지에 표시된 대로 계약을 생성하고 범위 필드를 테넌트로 수정합니다.

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

6단계. 이미지에 표시된 대로 L4-L7 서비스 그래프 템플릿을 생성합니다. 여기서 서비스 그래프 연결은 외부 라우팅 네트워크 정책 및 라우터 컨피그레이션을 디바이스 선택 정책과 연결합니다.

:

ALL TENANTS | Add Tenant | Search: enter name, descr | Common | T1 | Info | mgmt

Tenant T1

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

L4-L7 Service Graph Template - ASA5585_SGT

Topology Policy

ASA5585 Information

Firewall: **Routed**

Profile: **ASA5585_FP**

Create L4-L7 Service Graph Template

Drag device clusters to create graph nodes.

Device Clusters

- T1 /ASA5585 (Managed Firewall)

Graph Name: **ASA5585_SGT**

Graph Type: Create A New One Clone An Existing One

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

ASA5585 Information

Firewall: Routed Transparent

Profile: **T1/ASA5585_FP/ASA5585_FP**

SUBMIT **CANCEL**

이미지에 표시된 대로 서비스 어플라이언스(ASA 5585)에서 사용할 라우터 ID를 지정하기 위한 라우터 컨피그레이션:

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

이미지에 표시된 대로 인접성 유형을 L2에서 L3으로 변경합니다.

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

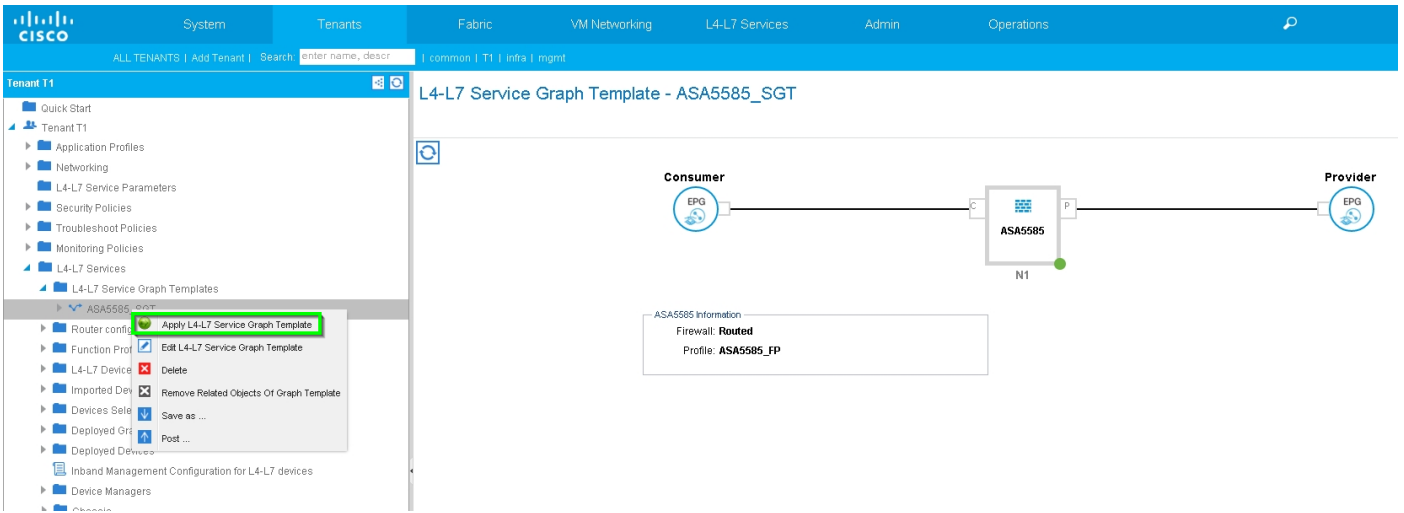
Label:

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

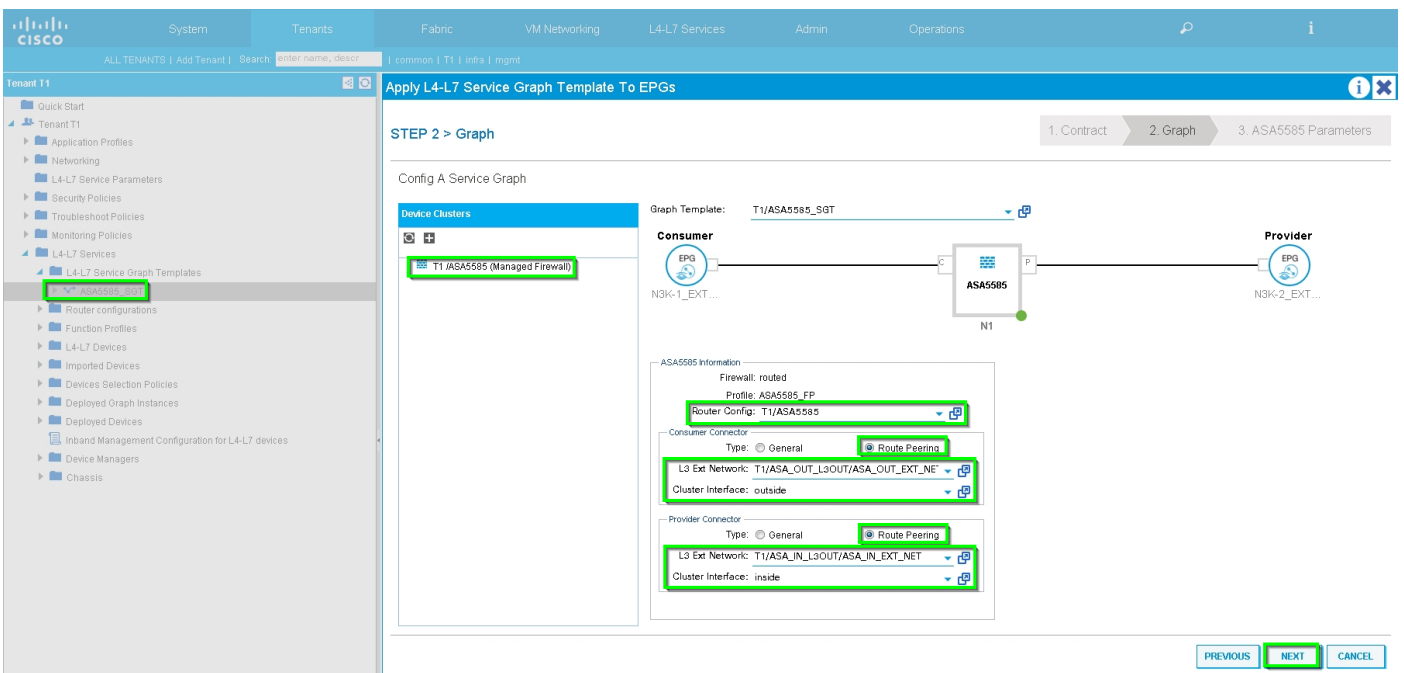
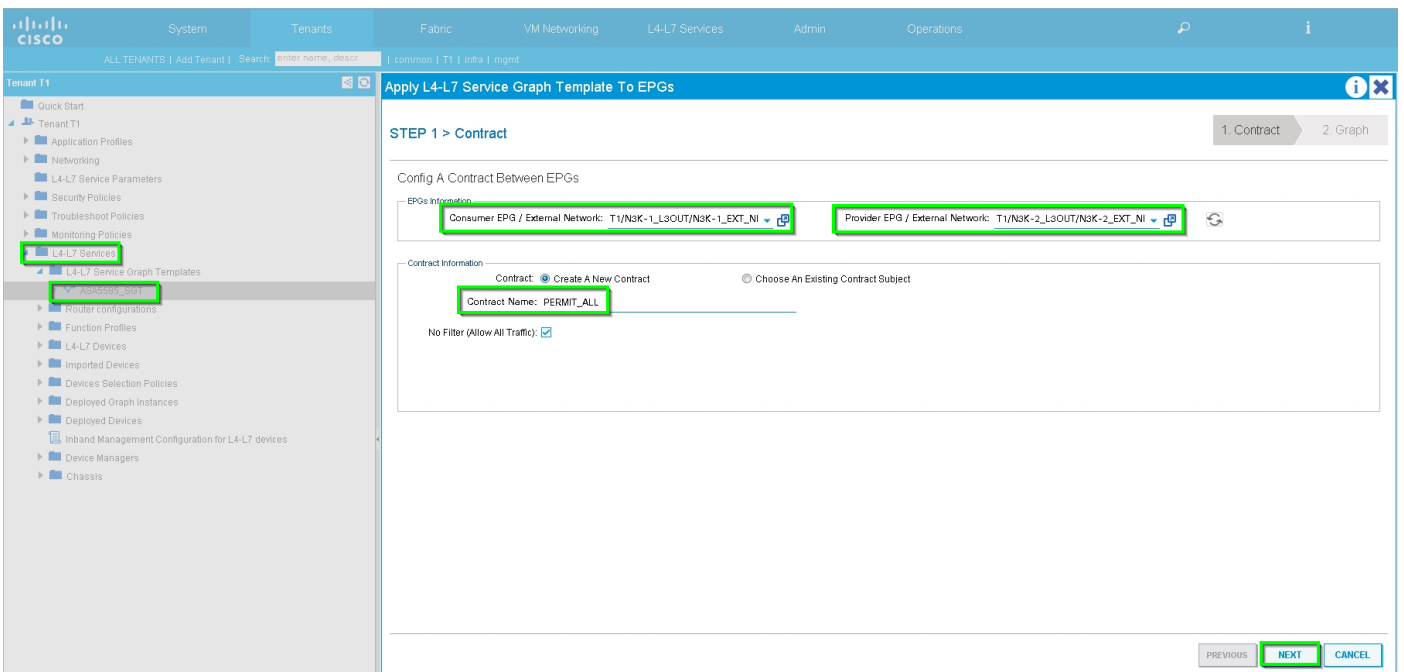
Terminal Nodes:	Name	Provider/Consumer	Description
T1		Consumer	
T2		Provider	

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

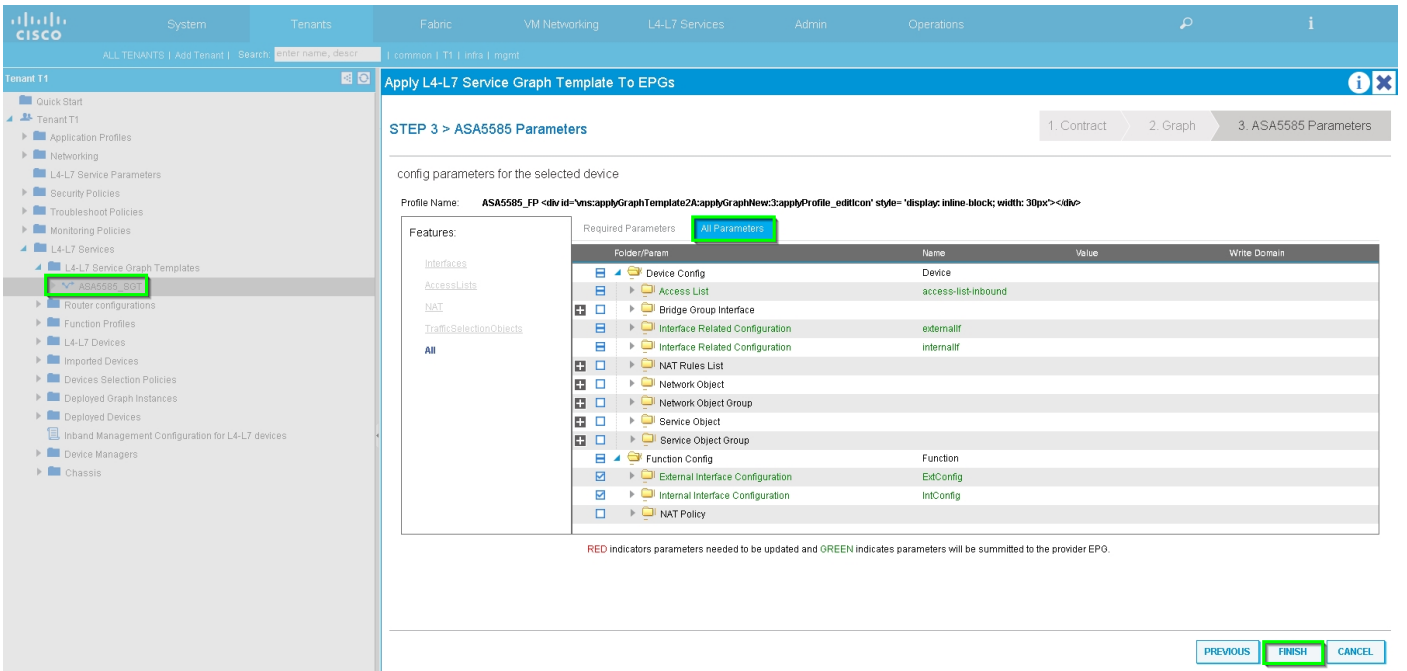
이미지에 표시된 대로 서비스 그래프 템플릿 적용:



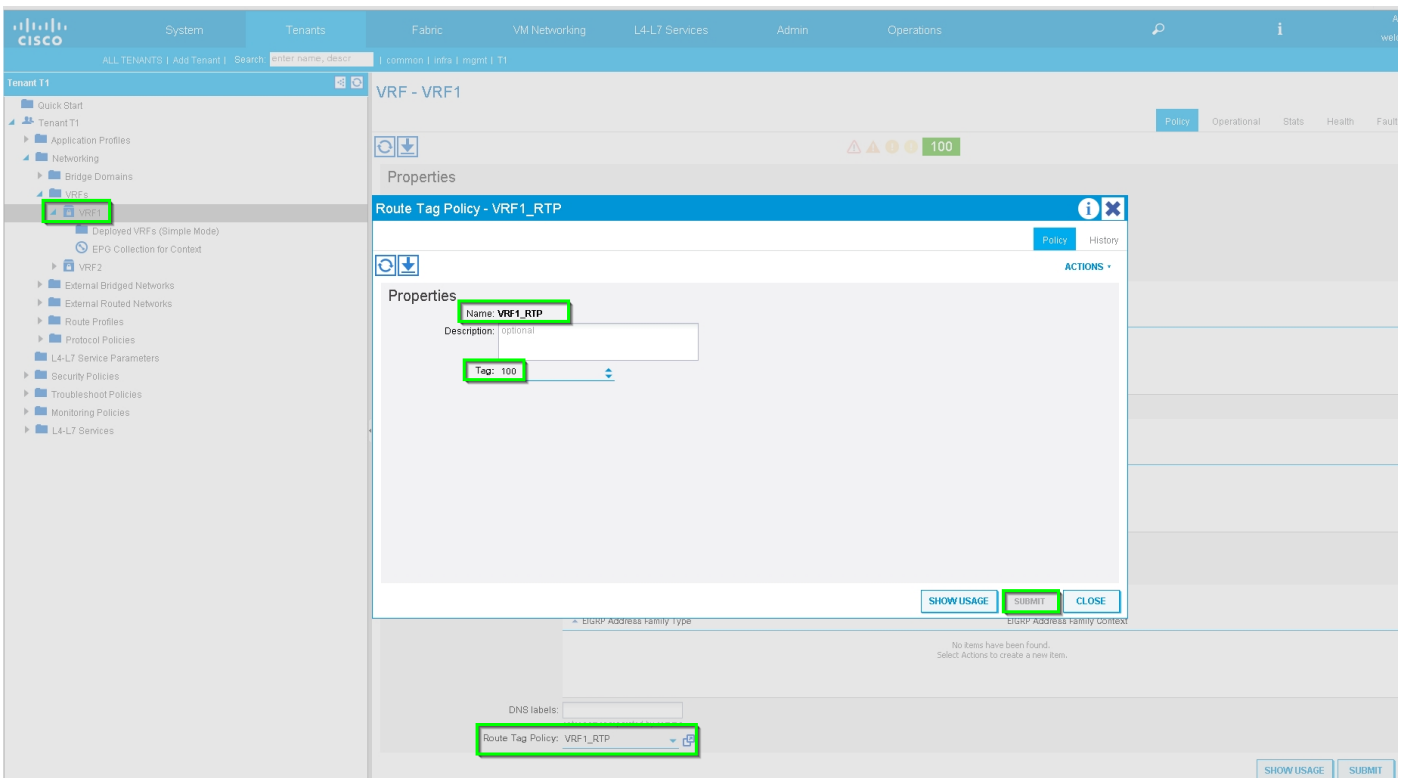
이미지에 표시된 대로 서비스 그래프를 계약에 연결합니다.



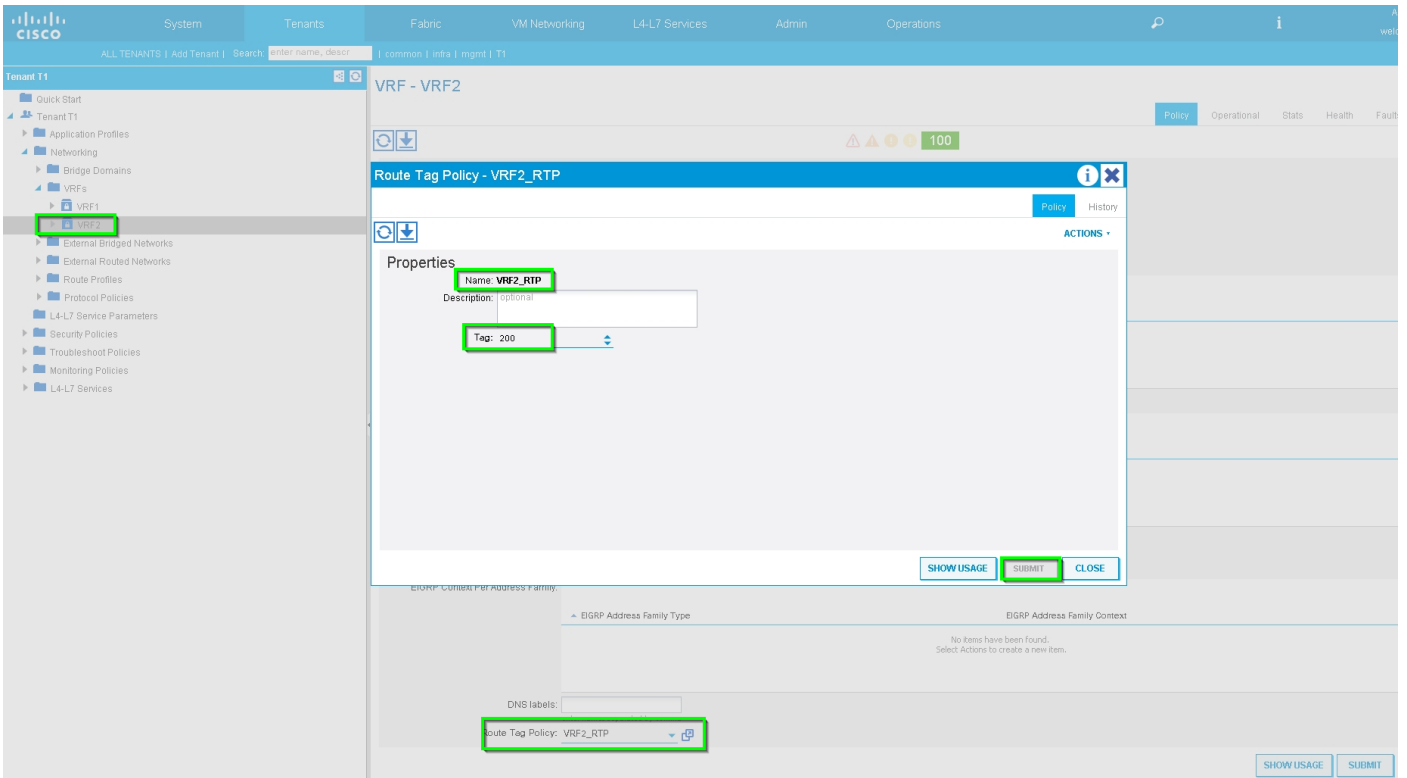
필요한 경우 이미지에 표시된 대로 L4-L7 매개 변수 추가/변경:



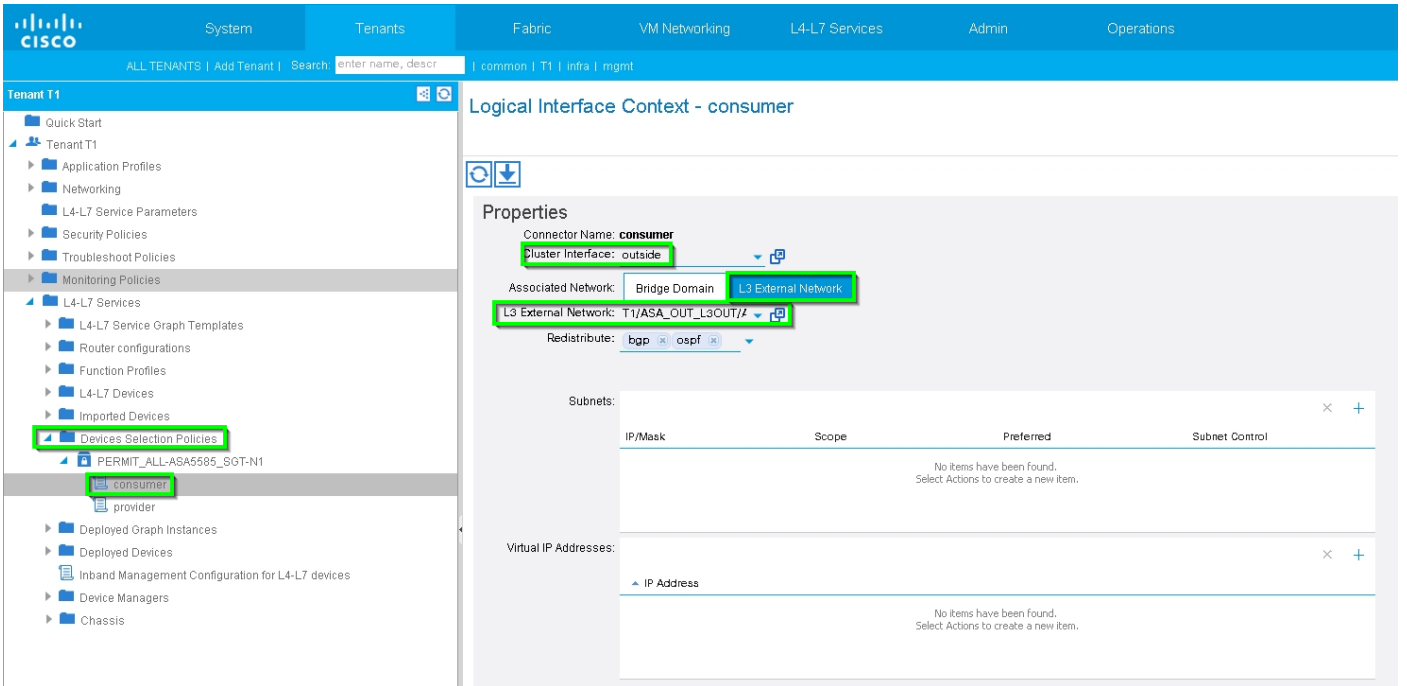
7단계:Route-tag Policy, 이미지에 표시된 대로 VRF1(Tag:100)에 대한 Route-tag Policy를 구성합니다.



이미지에 표시된 대로 VRF2(Tag:200)에 대한 Route-tag 정책을 구성합니다.



8단계: 다음 이미지에 표시된 대로 상태를 확인하고 디바이스 선택 정책을 확인합니다.



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.

이미지에 표시된 대로 Deployed Graph 인스턴스를 확인합니다.

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)

확인 및 문제 해결

테넌트에 대한 APIC 컨피그레이션:

```
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#

```

leaf 101에서 OSPF 인접 디바이스 관계 및 라우팅 테이블을 확인합니다.

```

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
```

leaf 102에서 OSPF 인접 디바이스 관계 및 라우팅 테이블을 확인합니다.

```
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
```

ASA 5585에서 컨피그레이션, OSPF 네이버 관계 및 라우팅 테이블을 확인합니다.

```
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
```

N3K-1에서 컨피그레이션, OSPF 네이버 관계 및 라우팅 테이블을 확인합니다.

```
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
```

N3K-2에서 컨피그레이션, OSPF 네이버 관계 및 라우팅 테이블을 확인합니다.

```
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
```

leaf의 계약 필터 규칙 및 패킷 적중 횟수를 확인합니다.

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

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

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

N3K-1과 N3K-2 간의 연결 가능성 테스트:

```
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
```

이 데모에 사용되는 테넌트 및 ASA 기능 프로파일의 XML 컨피그레이션 파일이 첨부되었습니다.