AVS 사용 시 GoTo(L3) 모드의 ASAv - ACI 1.2(x) 릴리스

목차

소개

이 문서에서는 라우티드/GOTO 모드에서 ASAv(Adaptive Security Virtual Appliance) 단일 방화벽을 사용하여 AVS(Application Virtual Switch) 스위치를 L4-L7 서비스 그래프로 구축하여 ACI 1.2(x) 릴리스를 사용하여 클라이언트-서버 통신을 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 알고 있는 것이 좋습니다.

- 액세스 정책이 구성되고 작동 및 작동 중
- EPG, BD(Bridge Domain) 및 VRF(Virtual Routing and Forwarding)가 이미 구성되어 있음

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

하드웨어 및 소프트웨어:

- UCS C220 - 2.0(6d)
- ESXi/vCenter - 5.5
- ASAv - asa-device-pkg-1.2.4.8
- AVS - 5.2.1.SV3.1.10
- APIC - 1.2(1i)
- 리프/스파인 - 11.2(1i)
- 장치 패키지 *.zip이 이미 다운로드됨

기능:

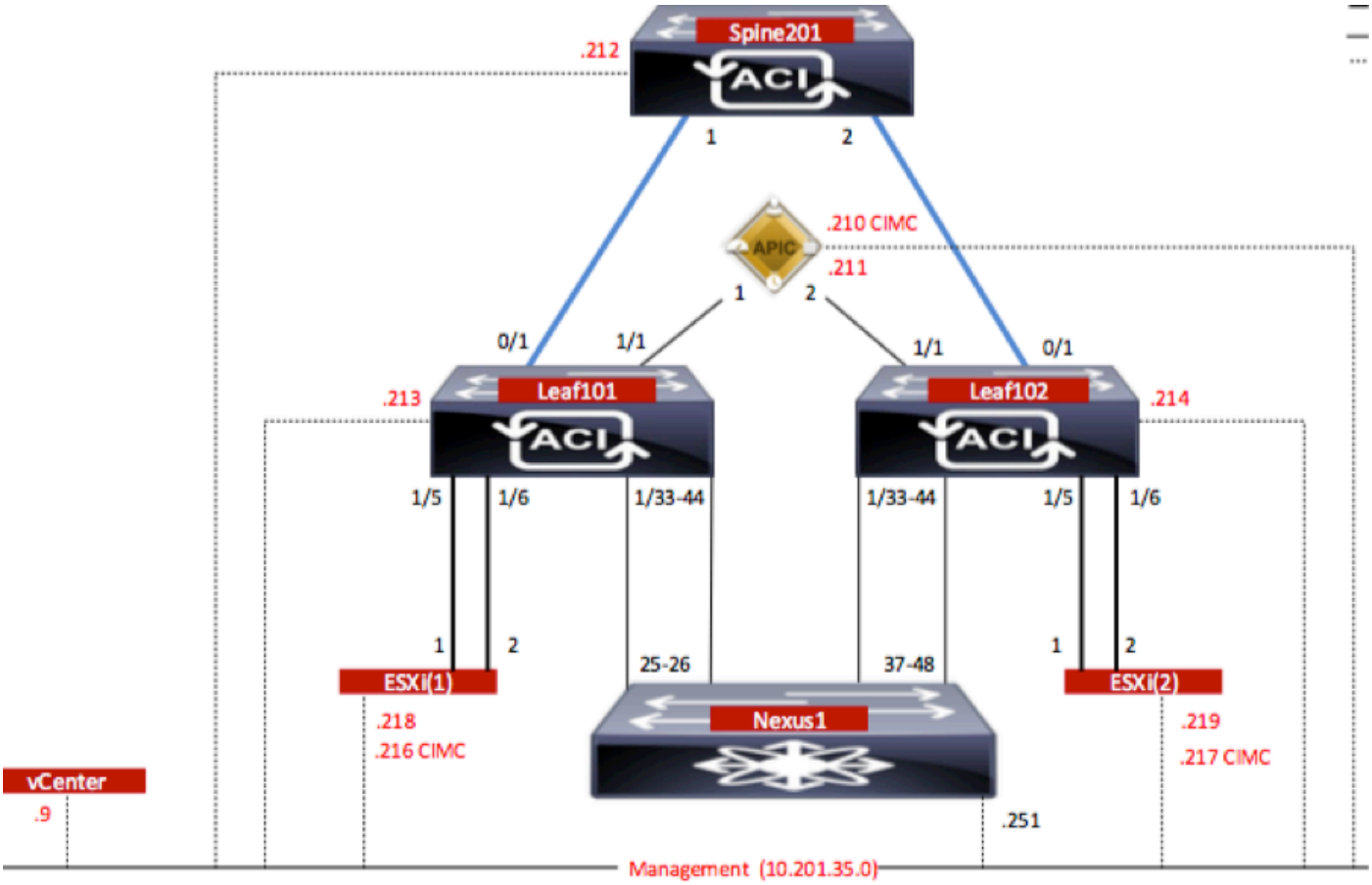
- AVS
- ASAv
- EPG, BD, VRF
- ACL(Access Control List)
- L4-L7 서비스 그래프
- vCenter

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 지워진(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램

이미지에 표시된 것처럼



구성

AVS 초기 설정: VMware vCenter 도메인 생성(VMM 통합)2

참고:

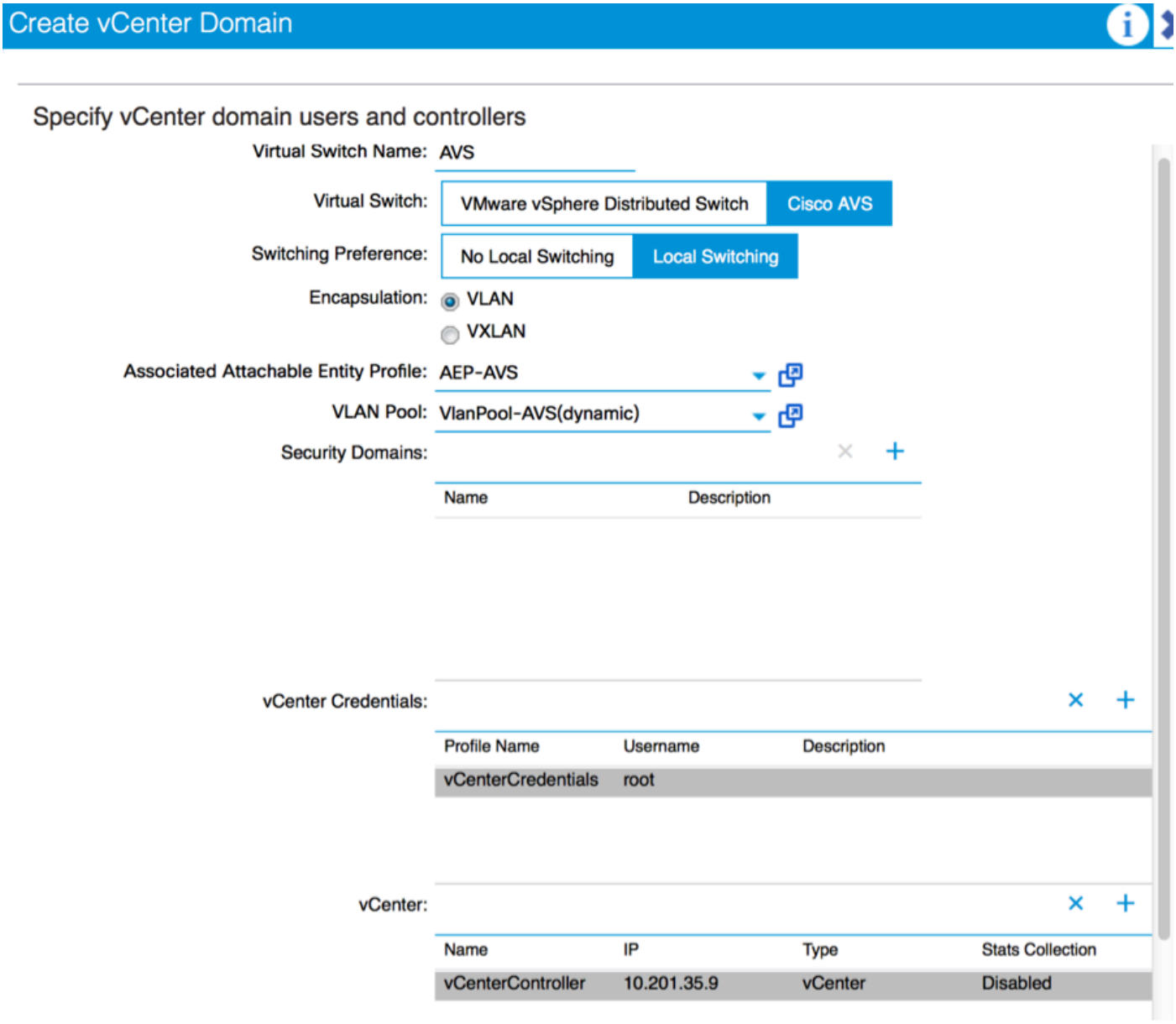
- 단일 도메인 아래에 여러 데이터 센터 및 DVS(Distributed Virtual Switch) 항목을 생성할 수 있습니다.그러나 각 데이터센터에 Cisco AVS를 하나만 할당할 수 있습니다.

- Cisco AVS를 통한 서비스 그래프 구축은 Cisco AVS 릴리스 5.2(1)SV3(1.10)의 Cisco ACI 릴리스 1.2(1i)에서 지원됩니다. 전체 서비스 그래프 컨피그레이션은 Cisco APIC(Cisco Application Policy Infrastructure Controller)에서 수행됩니다.

- Cisco AVS를 사용하는 VM(서비스 가상 머신) 배포는 VLAN(Virtual Local Area Network) 캡슐화 모드가 있는 VMM(Virtual Machine Manager) 도메인에서만 지원됩니다.그러나 컴퓨팅 VM(공급자 및 소비자 VM)은 VXLAN(Virtual Extensible LAN) 또는 VLAN 캡슐화가 포함된 VMM 도메인의 일부가 될 수 있습니다.

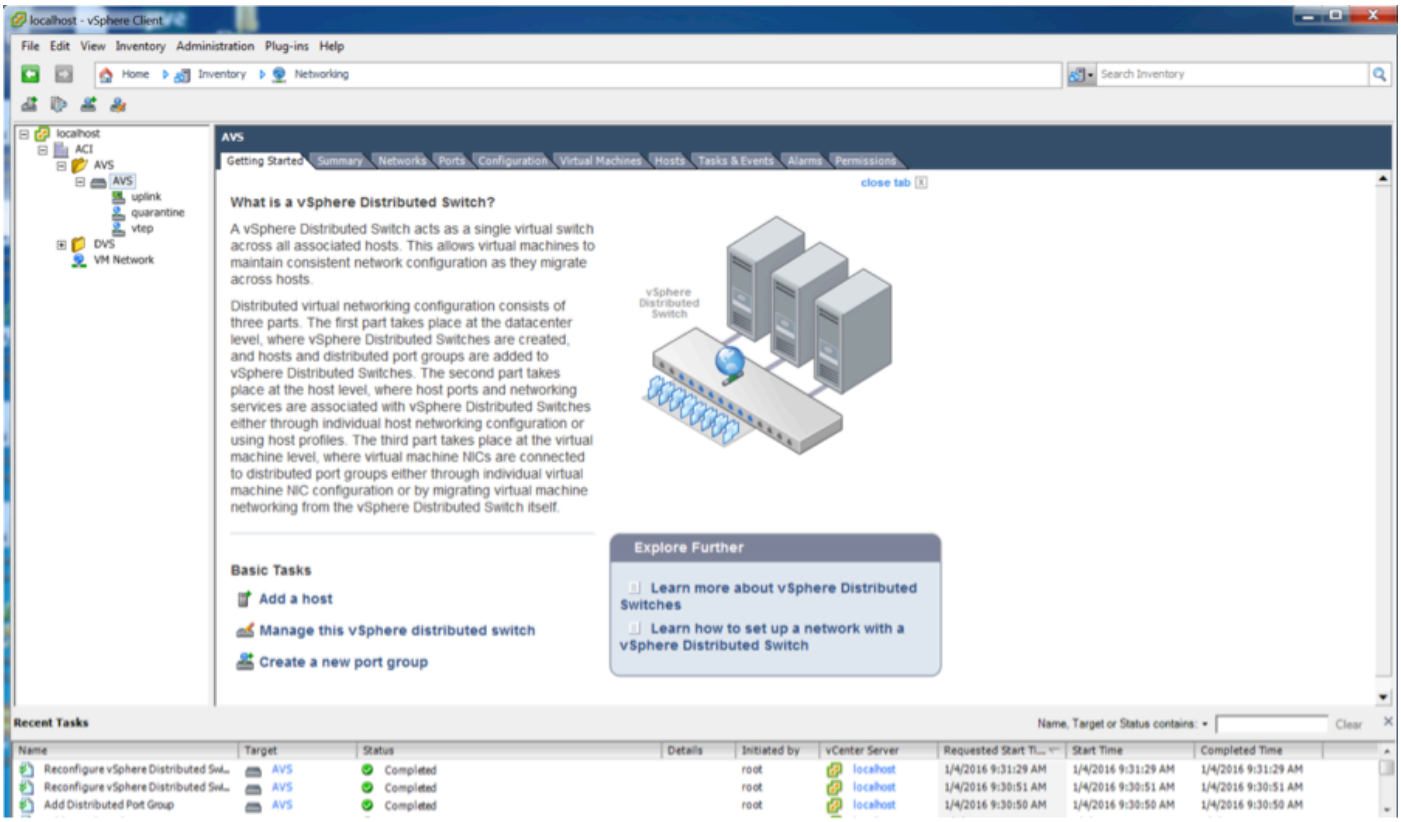
- 또한 로컬 스위칭이 사용되는 경우 멀티캐스트 주소와 풀이 필요하지 않습니다.로컬 스위칭을 선택하지 않은 경우 멀티캐스트 풀을 구성해야 하며 AVS 패브릭 전체의 멀티캐스트 주소는 멀티캐스트 풀의 일부가 아니어야 합니다.AVS에서 시작된 모든 트래픽은 VLAN 또는 VXLAN이 캡슐화됩니다.

이미지에 표시된 대로 **VM Networking(VM 네트워킹) > VMWare > Create vCenter Domain(vCenter 도메인 생성)**으로 이동합니다.

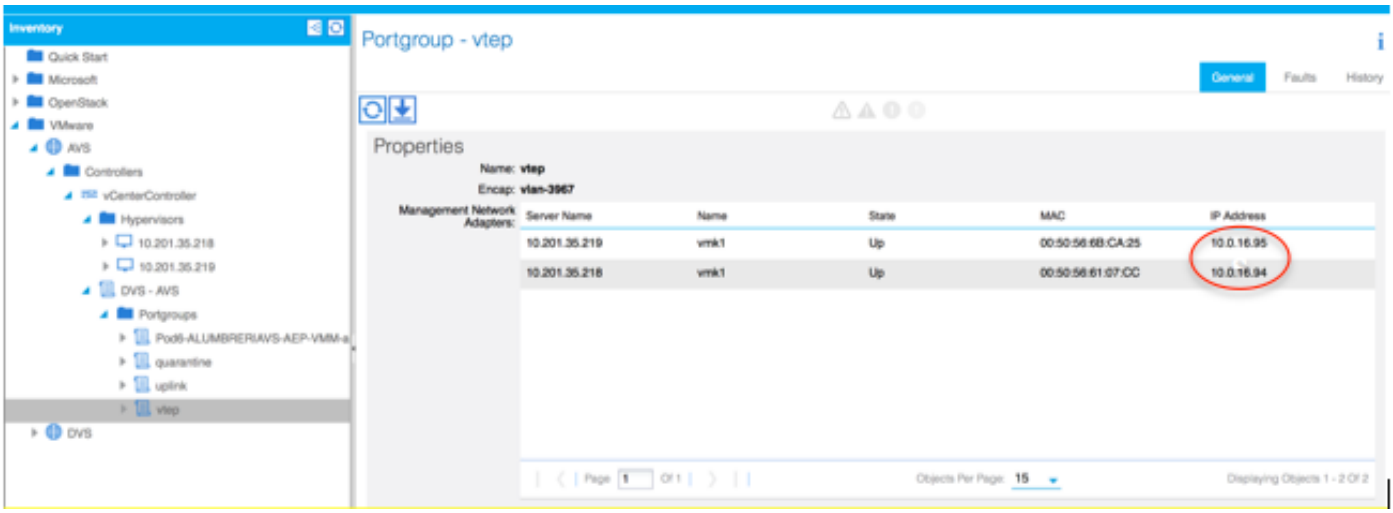


Port-channel 또는 VPC(Virtual Port-channel)를 사용하는 경우 Mac 피닝을 사용하도록 vSwitch 정책을 설정하는 것이 좋습니다.

이 후 APIC는 다음과 같이 AVS 스위치 컨피그레이션을 vCenter에 푸시해야 합니다.



APIC에서 VTEP(VXLAN Tunnel Endpoint) 주소가 AVS용 VTEP 포트 그룹에 할당되어 있음을 알 수 있습니다.연결 모드(VLAN 또는 VXLAN)에 관계없이 이 주소가 할당됩니다.



vCenter에 Cisco AVS 소프트웨어 설치

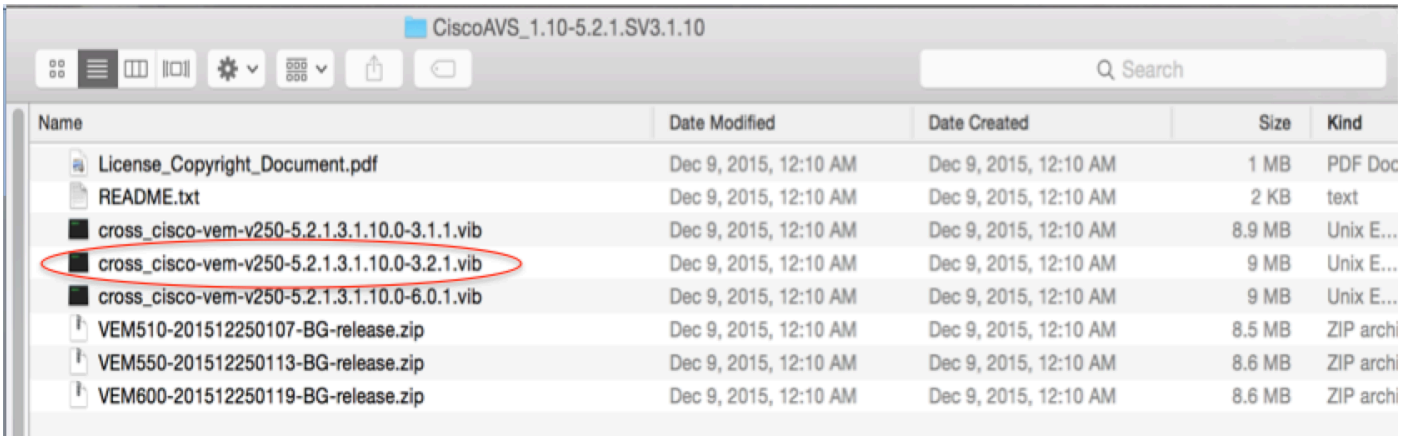
- 이 링크를 사용하여 CCO에서 vSphere 설치 번들(VIB)을 다운로드합니다.

  참고:이 경우 ESX 5.5, 표 1에는 ESXi 6.0, 5.5, 5.1 및 5.0의 호환성 매트릭스가 나와 있습니다 .

표 1 - ESXi 6.0, 5.5, 5.1 및 5.0의 호스트 소프트웨어 버전 호환성

VMware	VIB	VEM Bundle	Windows VC Installer	Linux vCenter Server Appliance
ESXi 6.0	cross_cisco-vem- v250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-BG- release.zip (Offline) VEM600-201512250119-BG (Online)	6.0	6.0
ESXi 5.5	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG- release.zip (Offline) VEM550-201512250113-BG (Online)	5.5	5.5
ESXi 5.1	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.1.1.vib	VEM510-201512250107-BG- release.zip (Offline) VEM510-201512250107-BG (Online)	5.1	5.1
ESXi 5.0	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.0.1.vib	VEM500-201512250101-BG- release.zip (Offline) VEM500-201512250101-BG (Online)	5.0	5.0

ZIP 파일에는 3개의 VIB 파일이 있으며, ESXi 호스트 버전마다 하나씩, 이미지에 표시된 대로 ESX 5.5에 적합한 파일을 선택합니다.



- VIB 파일을 ESX Datastore에 복사 - CLI를 통해 또는 vCenter에서 직접 복사

  참고:호스트에 VIB 파일이 있는 경우 esxcli **소프트웨어 vib** remove 명령을 사용하여 제거합니다.

esxcli 소프트웨어 vib 제거 -n cross_cisco-vem-v197-5.2.1.3.1.5.0-3.2.1.vib

데이터 저장소를 직접 찾아보는 것입니다

- ESXi 호스트에서 다음 명령을 사용하여 AVS 소프트웨어를 설치합니다.

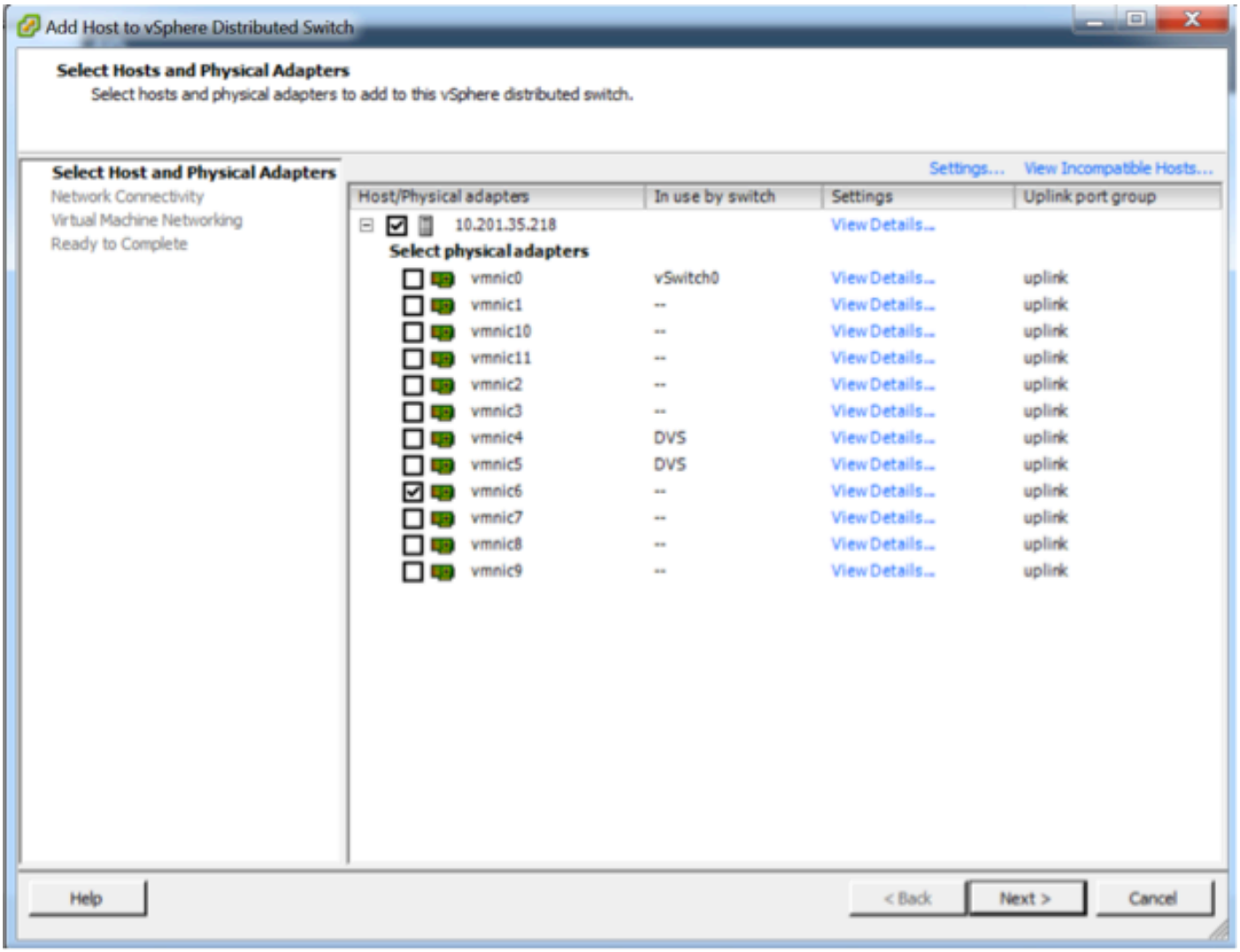
esxcli 소프트웨어 vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib —maintenance-mode —no-sig-check

```
~ # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib --maintenance-mode --no-sig-check
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v250-esx_5.2.1.3.1.10.0-3.2.1
   VIBs Removed: Cisco_bootbank_cisco-vem-v197-esx_5.2.1.3.1.5.0-3.2.1
   VIBs Skipped:
~ # vem status

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         5632        8           128               1500    vmnic0
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
DVS              5632        10          512               9000    vmnic5,vmnic4

VEM Agent (vemdpa) is running

~ #
```

- VEM(Virtual Ethernet module)이 작동되면 AVS에 호스트를 추가할 수 있습니다.

Add Host to vSphere Distributed Switch(vSphere 분산형 스위치에 호스트 추가) 대화 상자에서 리프 스위치에 연결된 가상 NIC 포트를 선택합니다(이 예에서는 vmnic6만 이동함). 이미지는 다음과

같습니다.



- **다음**을 클릭합니다.
- Network Connectivity(네트워크 연결) 대화 상자에서 Next(**다음**)를 클릭합니다.
- Virtual Machine Networking(가상 머신 네트워킹) 대화 상자에서 Next(다음)를 클릭합니다.
- 완료 준비 대화 상자에서 마침을 클릭합니다.

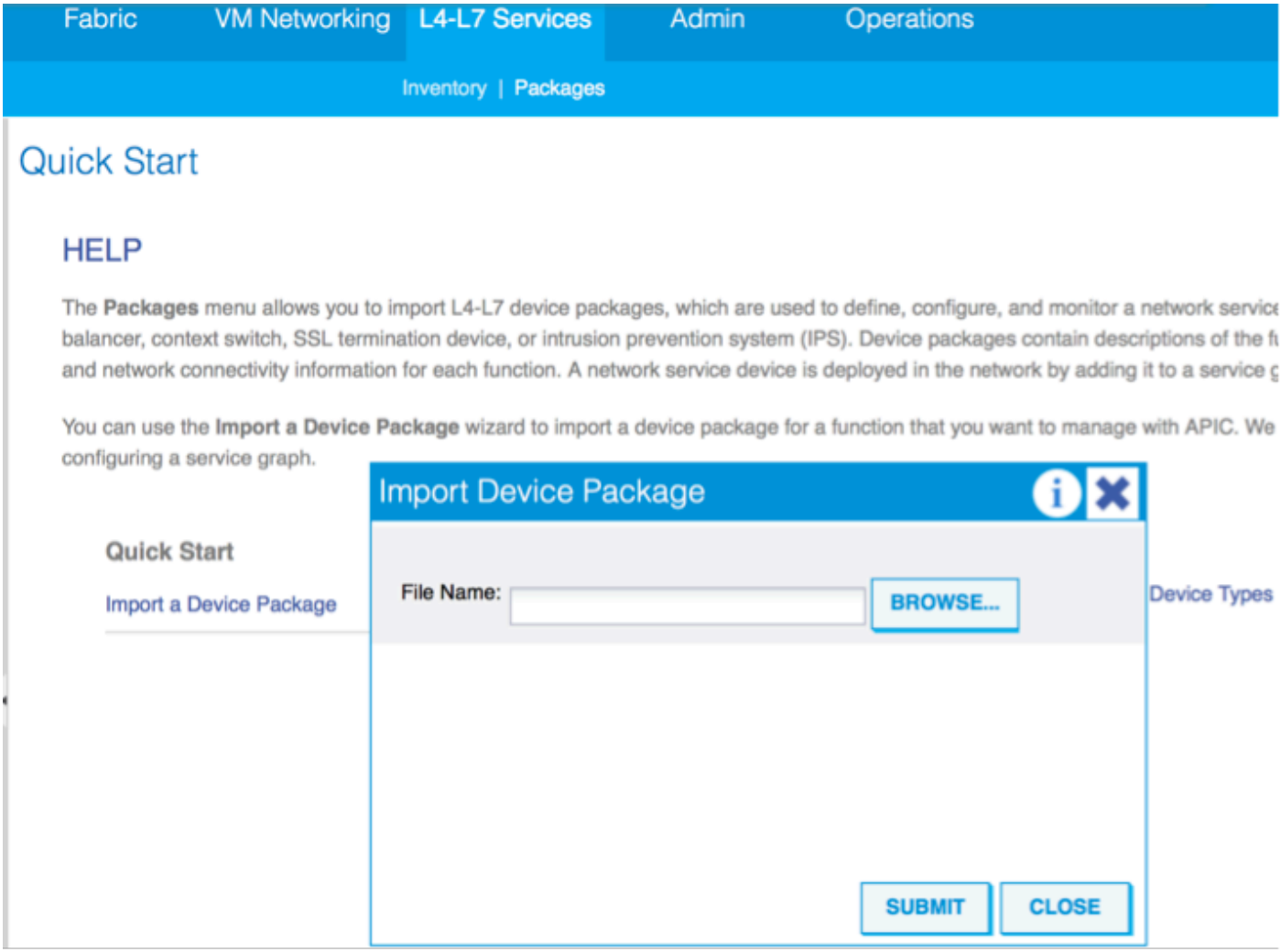
  참고:여러 ESXi 호스트를 사용하는 경우, 모두 AVS/VEM을 실행하여 표준 스위치에서 DVS 또는 AVS로 관리할 수 있어야 합니다.

이를 통해 AVS 통합이 완료되었으며 L4-L7 ASAv 구축을 계속할 준비가 되었습니다.

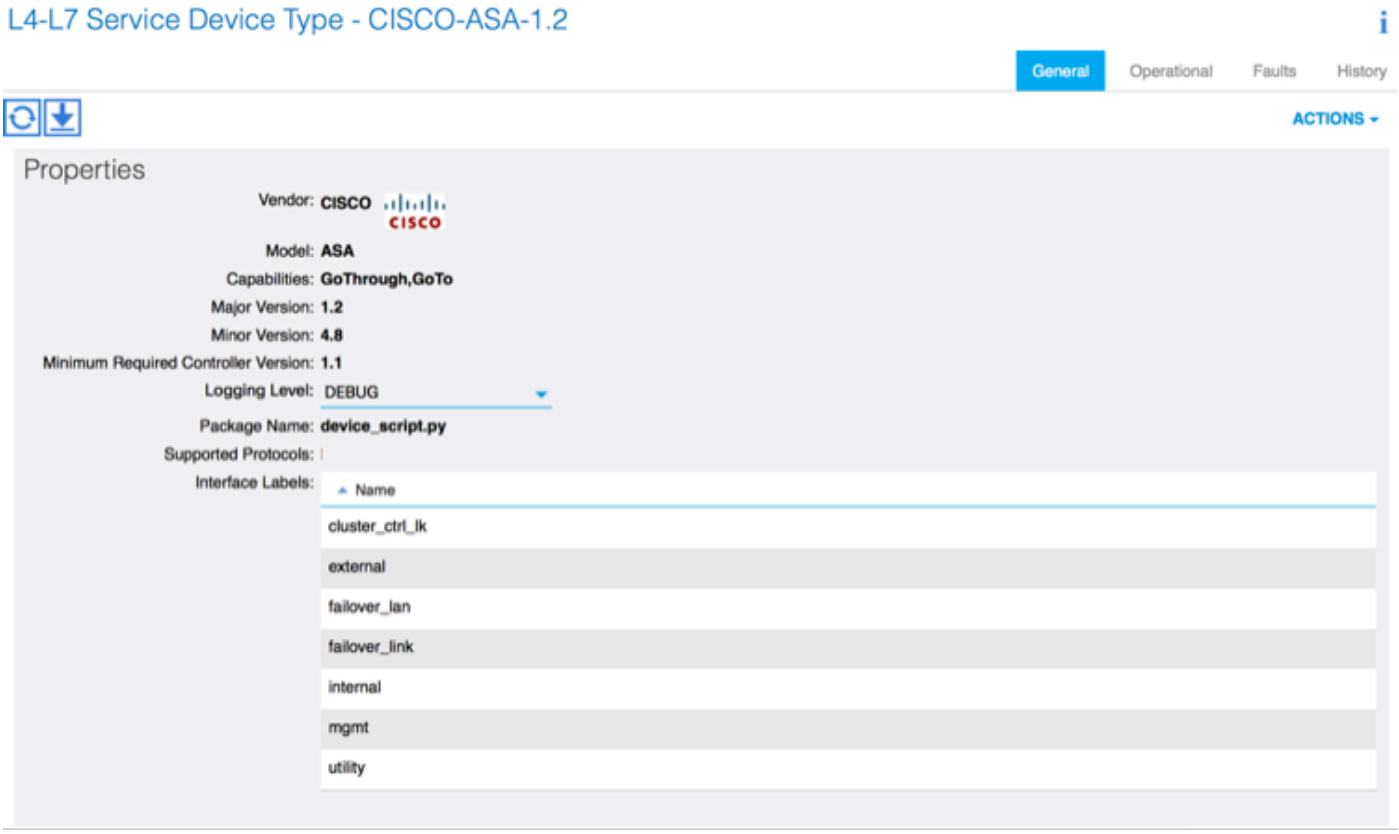
ASAv 초기 설정

- Cisco ASAv 디바이스 패키지를 다운로드하여 APIC로 가져옵니다.

이미지에 표시된 대로 **L4-L7 Services > Packages > Import Device Package**로 이동합니다.



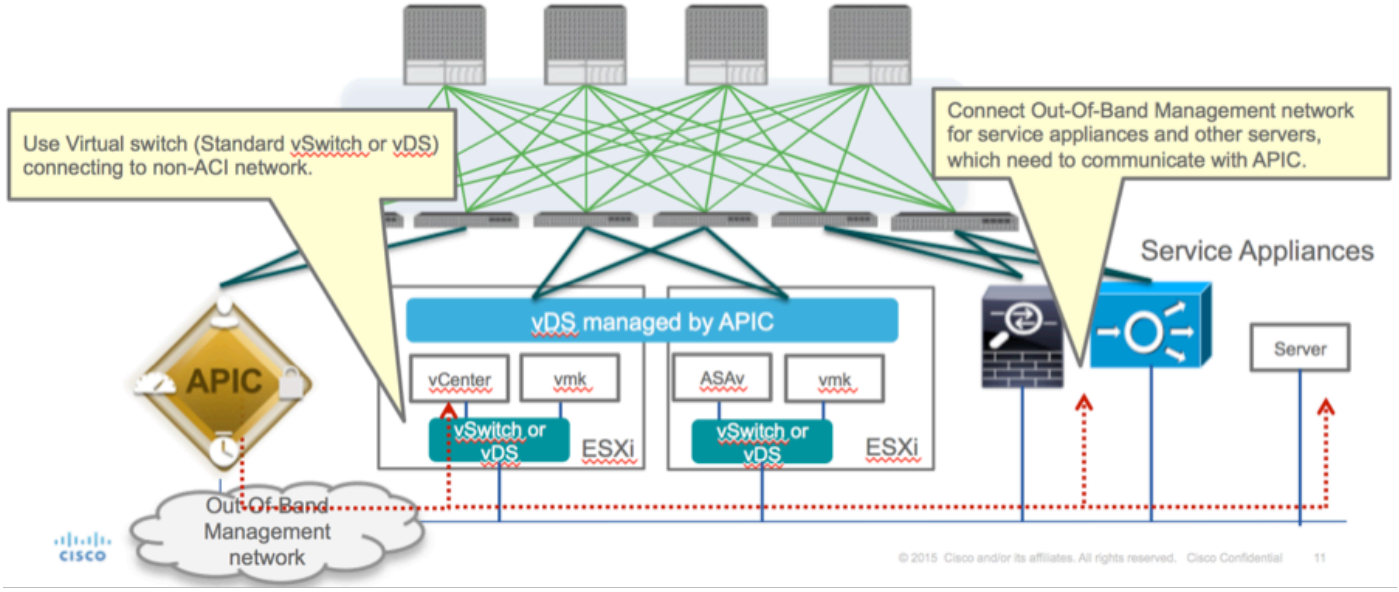
- 모든 것이 제대로 작동하는 경우 다음 이미지에 표시된 것처럼 가져온 디바이스 패키지가 L4-L7 서비스 디바이스 유형 폴더를 확장하는 것을 볼 수 있습니다.



계속하기 전에 실제 L4-L7 통합이 수행되기 전에 확인해야 할 설치 측면이 몇 가지 있습니다.

관리 네트워크에는 OOB(In-Band Management)와 OOB(Out-of-Band)라는 두 가지 유형이 있습니다. 이러한 유형은 기본 ACI(Application Centric Infrastructure)에 속하지 않는 장치(리프, 스파인 또는 apic 컨트롤러)를 관리하는 데 사용할 수 있으며, 여기에는 ASAv, 로더밸런서 등이 포함됩니다.

이 경우 ASAv용 OOB는 표준 vSwitch를 사용하여 구축됩니다.베어 메탈 ASA 또는 기타 서비스 어플라이언스 및/또는 서버의 경우 이미지에 표시된 대로 OOB 관리 포트를 OOB 스위치 또는 네트워크에 연결합니다.



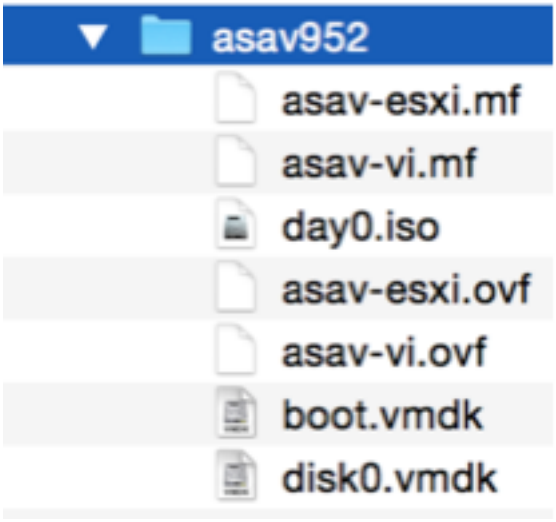
ASAv OOB 관리 포트 관리 연결은 OOB를 통해 APIC와 통신하려면 ESXi 업링크 포트를 사용해야 합니다. vNIC 인터페이스를 매핑하면 네트워크 어댑터1은 항상 ASAv의 Management0/0 인터페이스와 일치하며 나머지 데이터 플레인 인터페이스는 Network adapter2에서 시작됩니다.

표 2는 네트워크 어댑터 ID 및 ASAv 인터페이스 ID의 일치입니다.

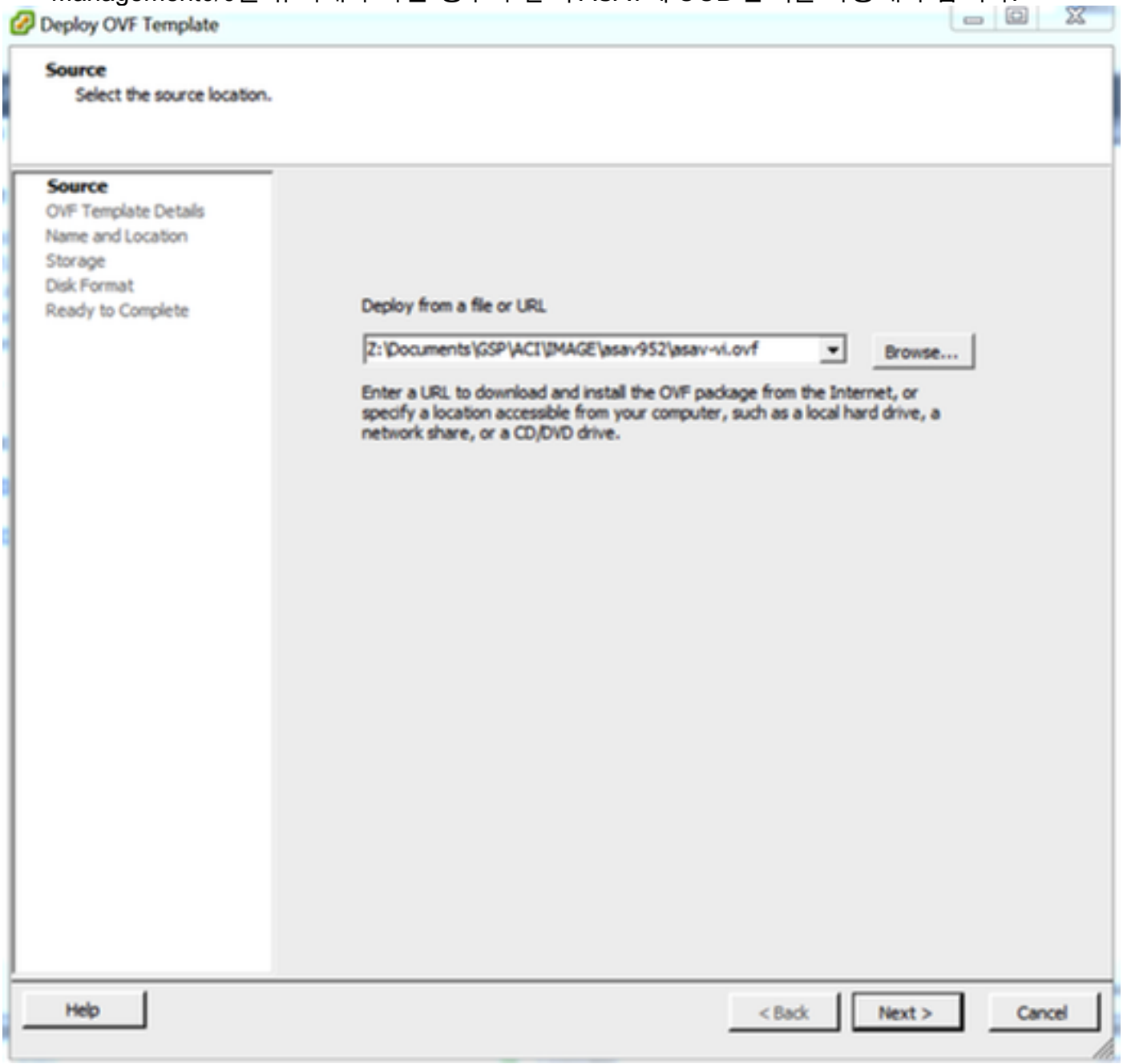
표 2

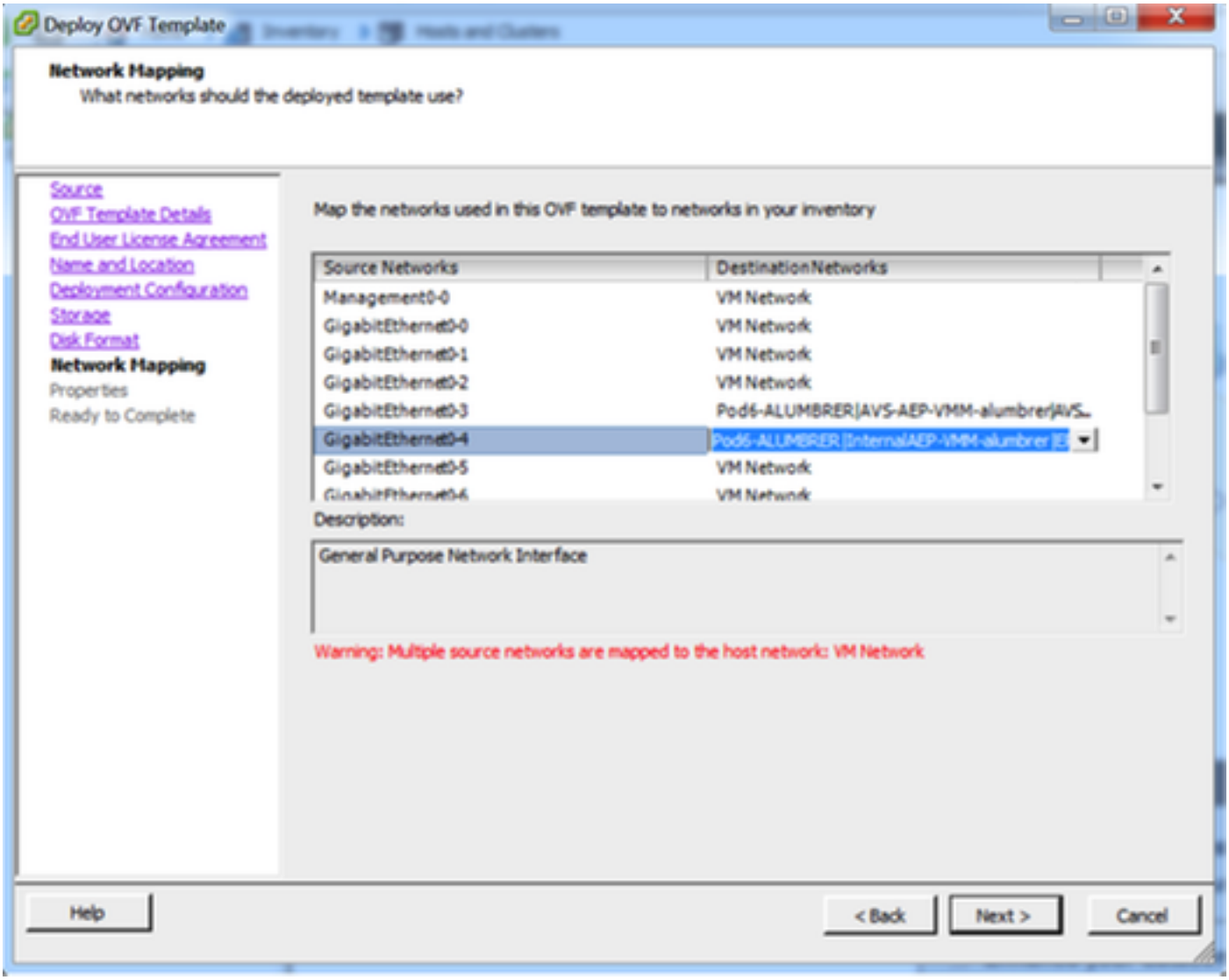
Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter 8	GigabitEthernet0/6
Network Adapter 9	GigabitEthernet0/7
Network Adapter 10	GigabitEthernet0/8

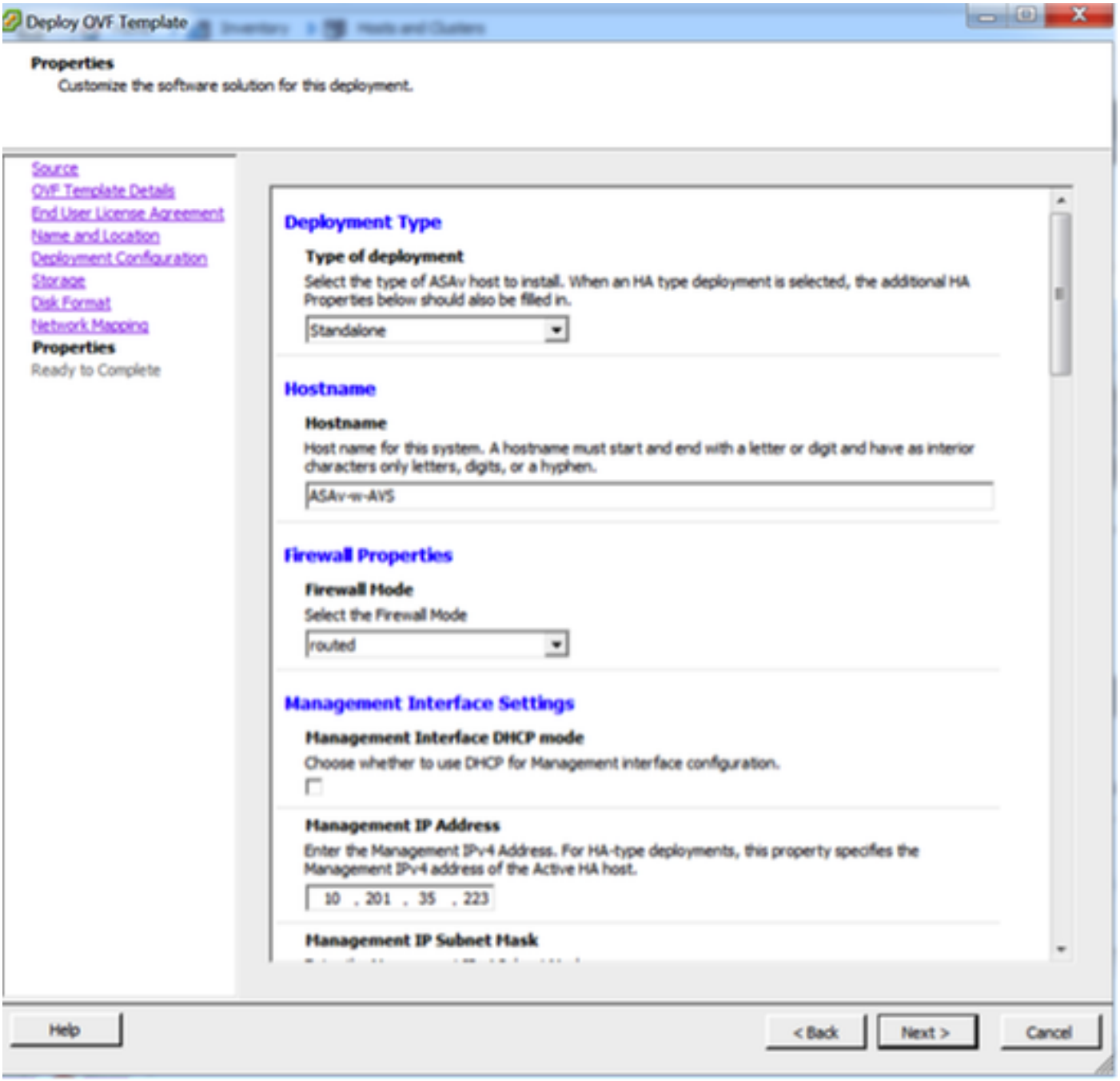
- File(파일)>Deploy OVF **(Open Virtualization Format) Template(OVF 구축) 템플릿을** 통해 ASAv VM **구축**
- 독립형 **ESX** Server 또는 vCenter용 asav**-vi**를 사용하려면 asav-esxi를 선택합니다.이 경우 vCenter가 사용됩니다.

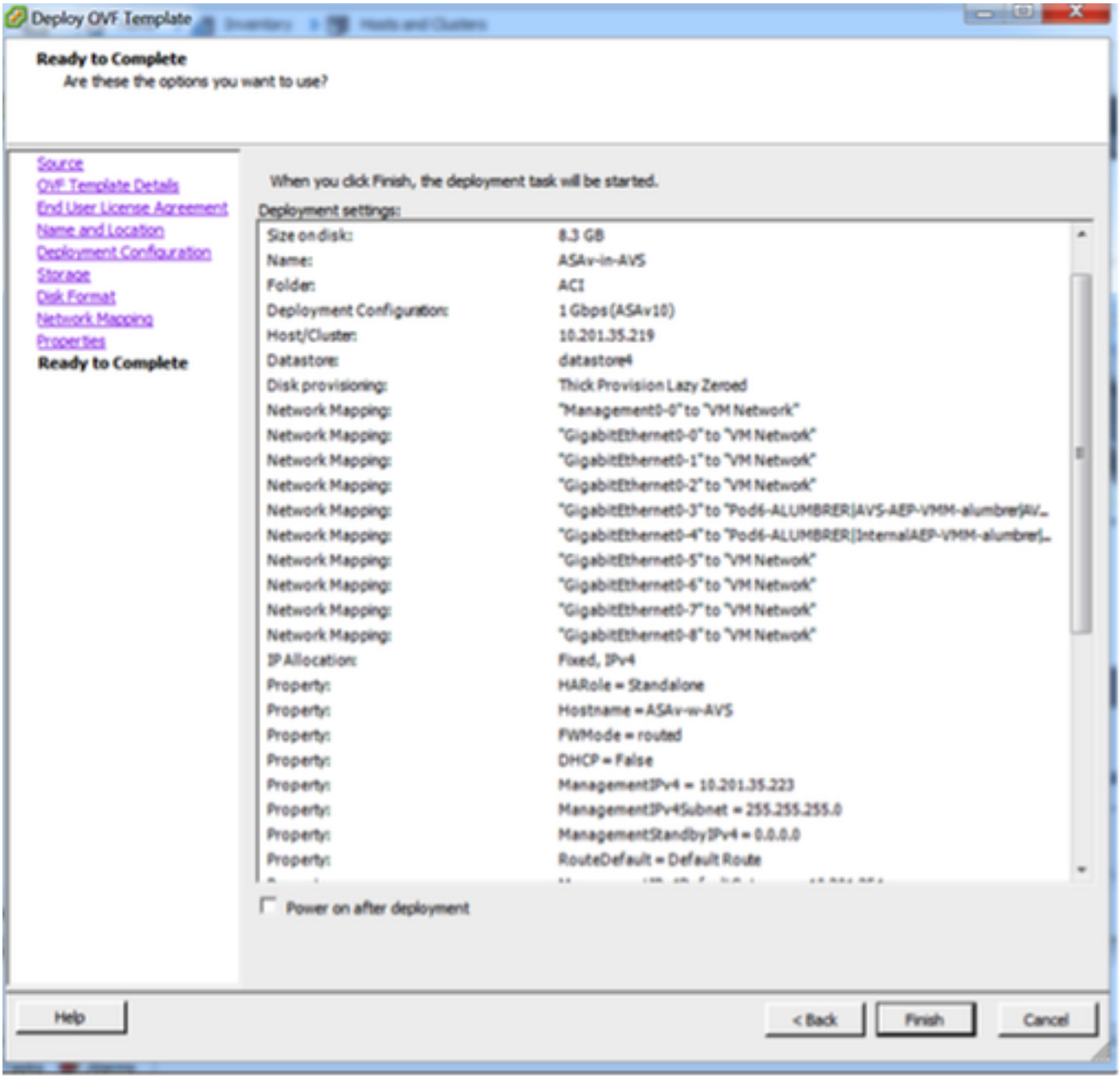


- 설치 마법사를 통해 약관에 동의합니다. 마법사 중간에 호스트 이름, 관리, IP 주소, 방화벽 모드 및 ASAv와 관련된 기타 특정 정보와 같은 여러 옵션을 결정할 수 있습니다.VM 네트워크(표준 스위치)를 사용하고 GigabitEthernet0-8이 기본 네트워크 포트인 경우 인터페이스 Management0/0을 유지해야 하는 경우와 같이 ASAv에 OOB 관리를 사용해야 합니다.

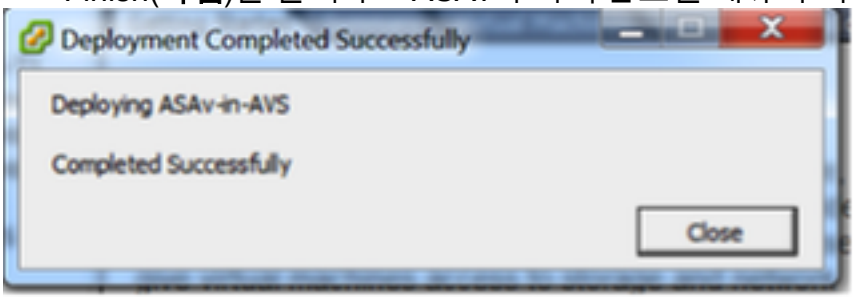



Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
Management0-0
VM Network
GigabitEthernet0-0
VM Network
GigabitEthernet0-1
VM Network
GigabitEthernet0-2
VM Network
GigabitEthernet0-3
Pod6-ALUMBRER|AVS-AEP-VMM-alumbrer|AVS...
GigabitEthernet0-4
Pod6-ALUMBRER|InternalAEP-VMM-alumbrer|E
GigabitEthernet0-5
VM Network
Description:
General Purpose Network Interface
Warning: Multiple source networks are mapped to the host network: VM Network
Help
< Back
Next >
Cancel

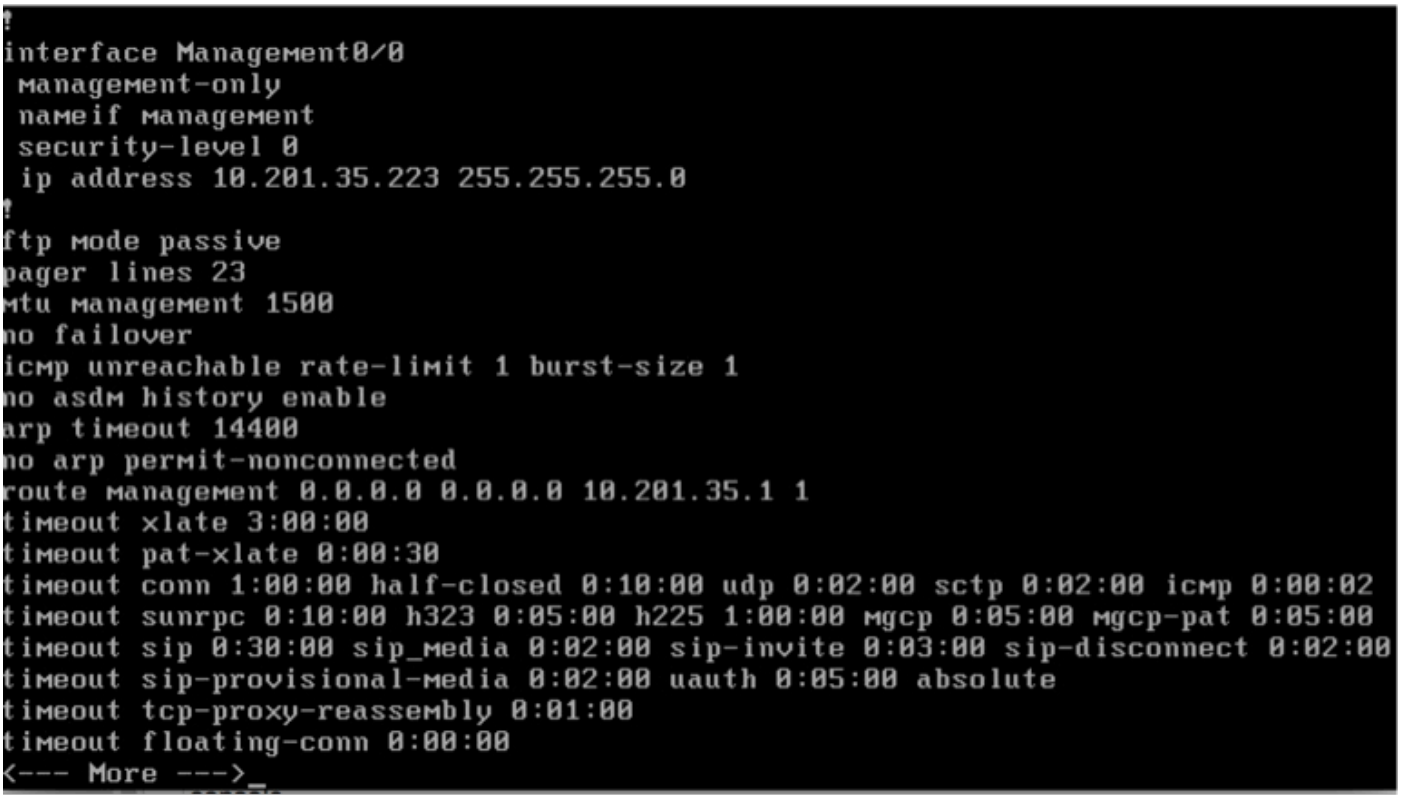

Deploy OVF Template
Properties
Customize the software solution for this deployment.
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Deployment Type
Type of deployment
Select the type of ASAv host to install. When an HA type deployment is selected, the additional HA Properties below should also be filled in.
Standalone
Hostname
Hostname
Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.
ASAv-w-AVS
Firewall Properties
Firewall Mode
Select the Firewall Mode
routed
Management Interface Settings
Management Interface DHCP mode
Choose whether to use DHCP for Management interface configuration.
Management IP Address
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.
10 . 201 . 35 . 223
Management IP Subnet Mask
Help
< Back
Next >
Cancel



- Finish(**마침**)를 클릭하고 ASAv 구축이 완료될 때까지 기다립니다.

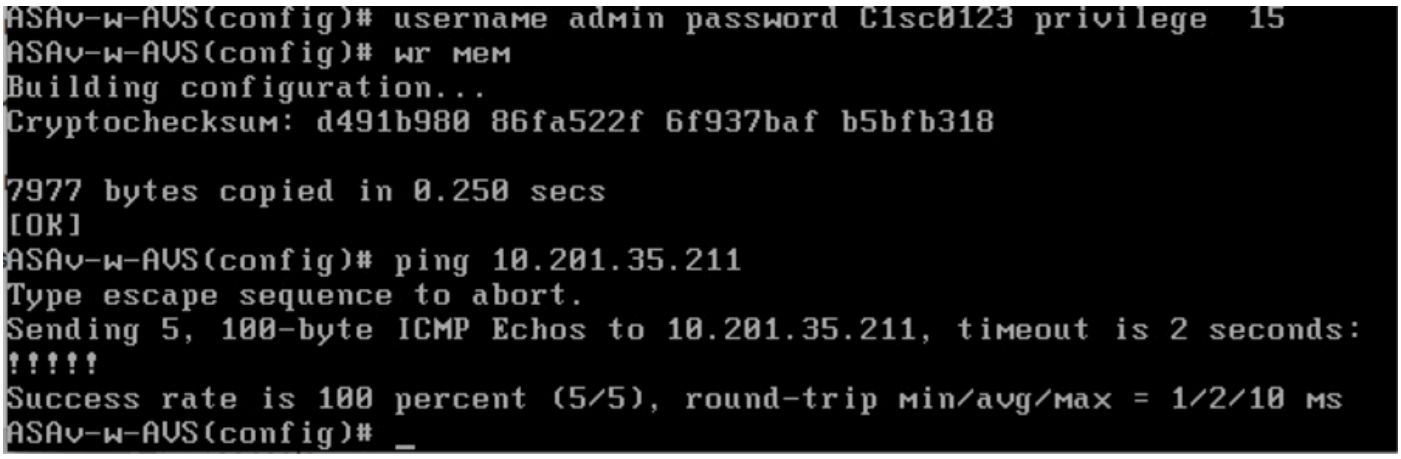


- ASAv VM 전원을 켜고 콘솔을 통해 로그인하여 초기 컨피그레이션을 확인합니다.



- 이미지에 표시된 대로 일부 관리 컨피그레이션은 이미 ASAv 방화벽에 푸시됩니다.관리자 사용자 이름 및 비밀번호를 구성합니다. 이 사용자 이름 및 비밀번호는 APIC에서 ASA에 로그인하고 구성하는 데 사용됩니다.ASA는 OOB 네트워크에 연결되어 있어야 하며 APIC에 연결할 수 있어야 합니다.

사용자 이름 admin 비밀번호 <device_password> 암호화된 권한 15



또한 전역 컨피그레이션 모드에서 http 서버를 활성화합니다.

http 서버 활성화

http 0.0.0.0 0.0.0.0 관리

APIC에서 ASAv 통합을 위한 L4-L7:

- ACI GUI에 로그인하고 서비스 그래프가 구축될 테넌트를 클릭합니다.탐색 창 하단의 L4-L7 서비스를 확장하고 **L4-L7 Devices**를 마우스 오른쪽 버튼으로 클릭한 다음 **Create L4-L7 devices(L4-L7 디바이스 생성)를** 클릭하여 마법사를 엽니다.

- 이 구현의 경우 다음 설정이 적용됩니다.
  - 관리 모드

  -방화벽 서비스

  - 가상 디바이스

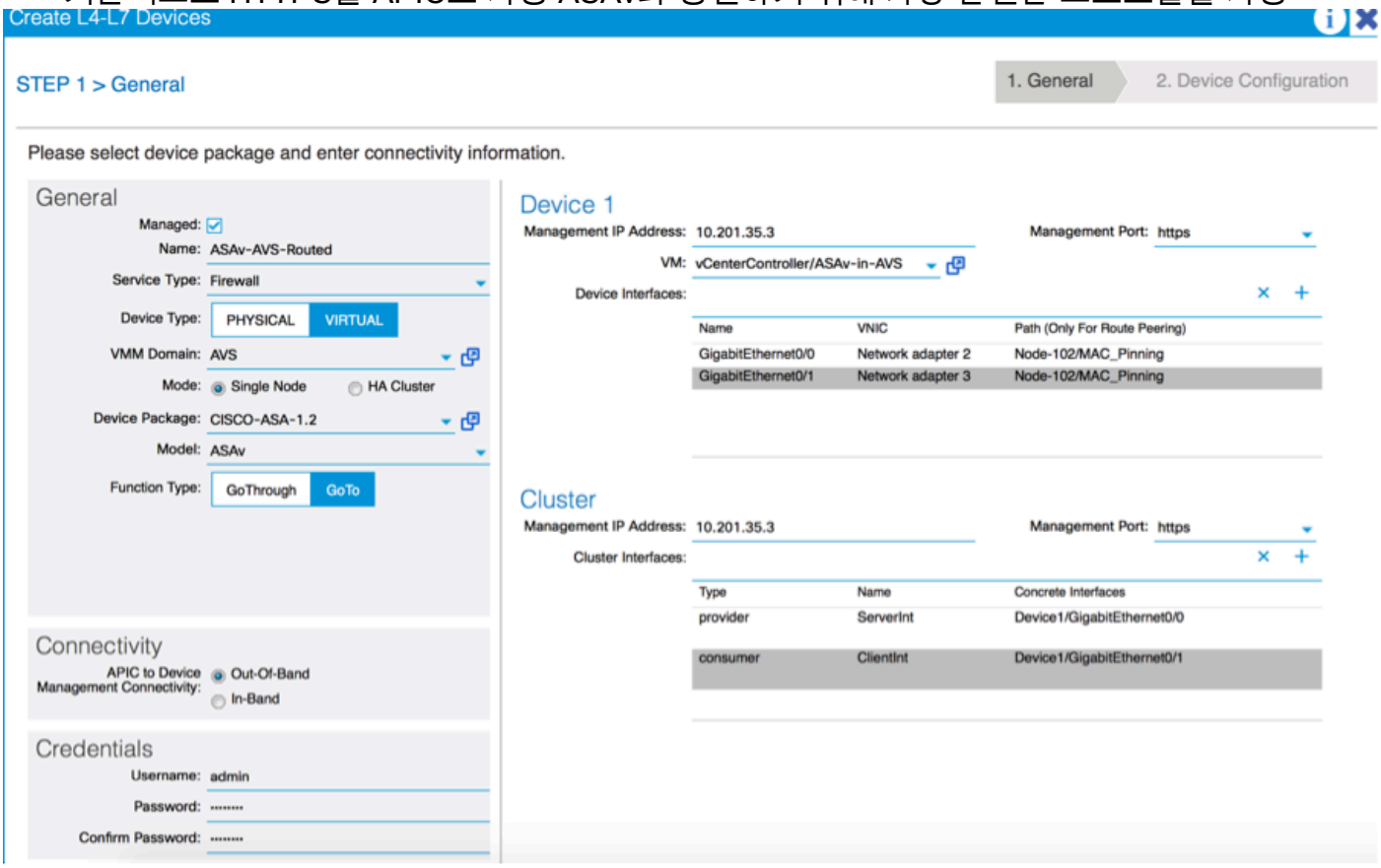
  - 단일 노드를 사용하여 AVS 도메인에 연결됨

  -ASAv 모델

  -라우팅된 모드(GoTo)

  -관리 주소(Mgmt0/0 인터페이스에 할당된 이전 주소와 일치해야 함)

- 기본적으로 HTTPS를 APIC로 사용 ASAv와 통신하기 위해 가장 안전한 프로토콜을 사용



- 성공적인 구축을 위해서는 디바이스 인터페이스 및 클러스터 인터페이스의 올바른 정의가 중요합니다

첫 번째 부분에서는 이전 섹션에 나와 있는 표 2를 사용하여 사용하려는 ASAv 인터페이스 ID와 네트워크 어댑터 ID를 올바르게 일치시킵니다.경로는 방화벽 인터페이스를 드나들 수 있는 물리적 포트, 포트 채널 또는 VPC를 나타냅니다.이 경우 ASA는 ESX 호스트에 있으며, 여기서 in과 out은 두 인터페이스에서 동일합니다.물리적 어플라이언스에서 방화벽 내부 및 외부(FW)는 물리적 포트와 다릅니다.

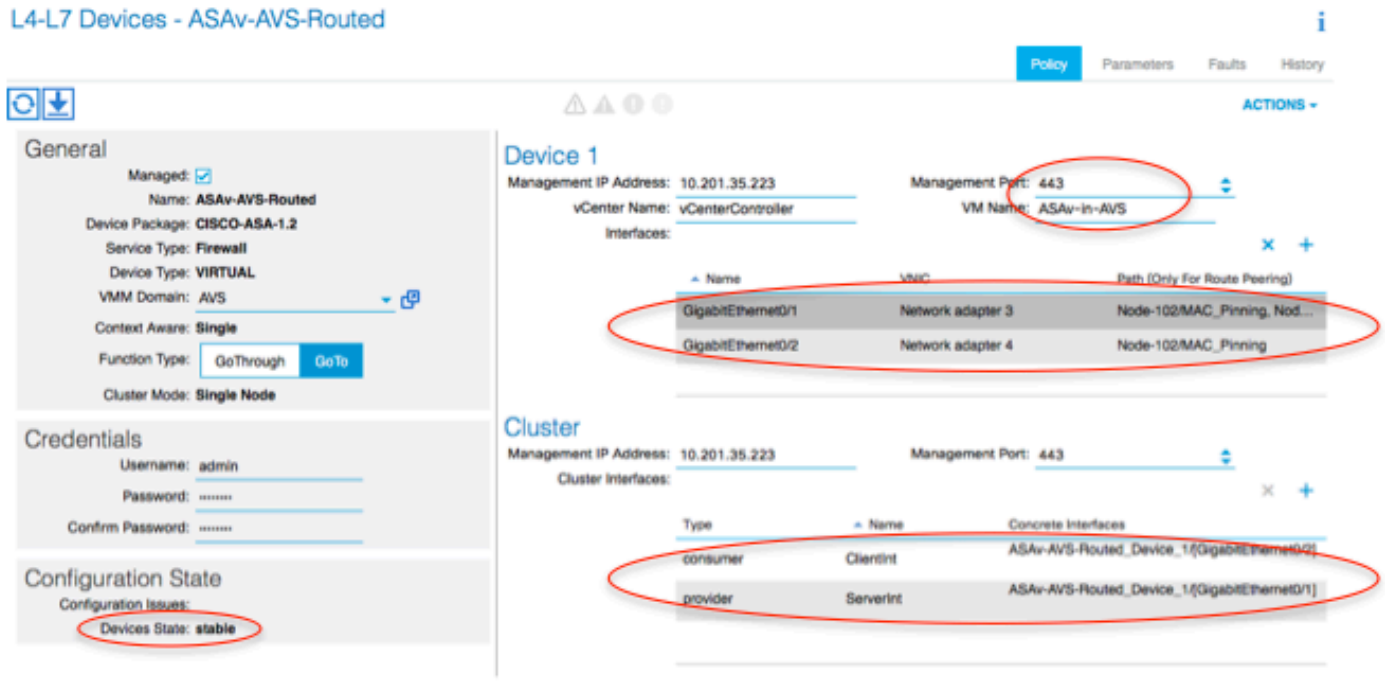
두 번째 부분에서는 클러스터 인터페이스를 항상 예외 없이 정의해야 합니다(클러스터 HA가 사용되지 않는 경우에도). 이는 개체 모델이 mIf 인터페이스(디바이스 패키지의 메타 인터페이스), LIf 인터페이스(예: 외부, 내부, 내부 등 리프 인터페이스) 및 **CIf**(콘크리트 인터페이스) 간를 가지고 있기 때문입니다. L4-L7 콘크리트 디바이스는 디바이스 클러스터 컨피그레이션에서 구성해야 하며 이러한 추상화를 논리적 디바이스라고 합니다.논리적 디바이스에는 콘크리트 디바이스의 콘크리트 인

터페이스에 매핑된 논리적 인터페이스가 있습니다.

이 예에서는 다음 연결이 사용됩니다.

Gi0/0 = vmnic2 = ServerInt/provider/server > EPG1

Gi0/1 = vmnic3 = ClientInt/consumer/client > EPG2

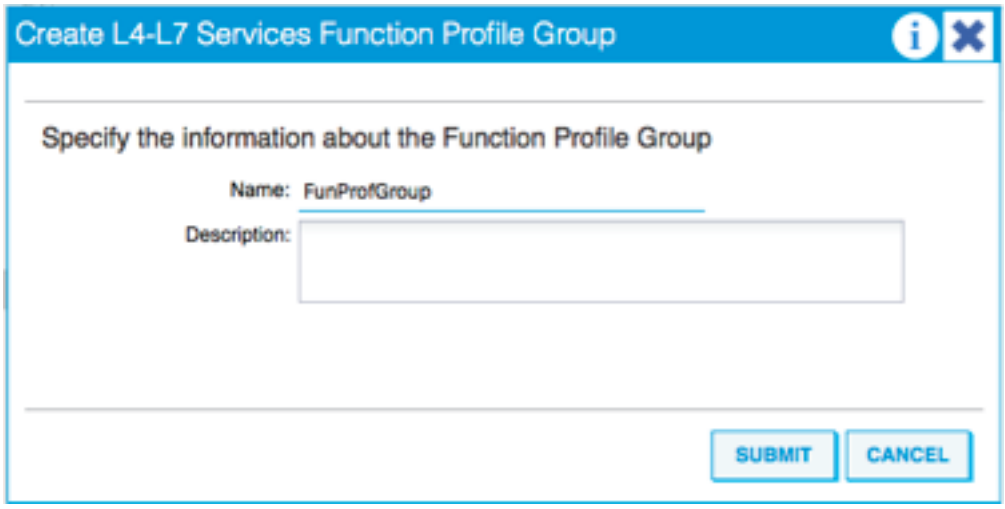


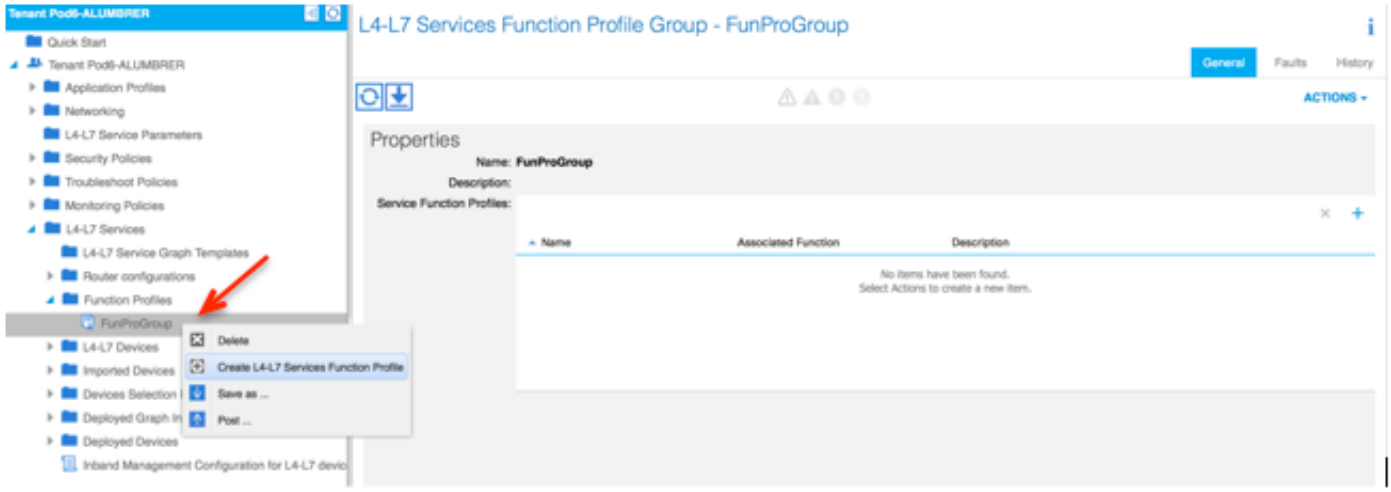
참고:장애 조치/HA 구축의 경우 GigabitEthernet 0/8이 장애 조치 인터페이스로 사전 구성됩니다.

디바이스 상태는 안정적이어야 하며 기능 프로파일 및 서비스 그래프 템플릿을 구축할 준비가 되어 있어야 합니다.

서비스 그래프 사원

첫째, ASAv용 기능 프로파일을 생성하지만 그 전에 이미지에 표시된 대로 해당 폴더 아래에 기능 프로파일 그룹을 생성한 다음 L4-L7 서비스 기능 프로파일을 생성해야 합니다.

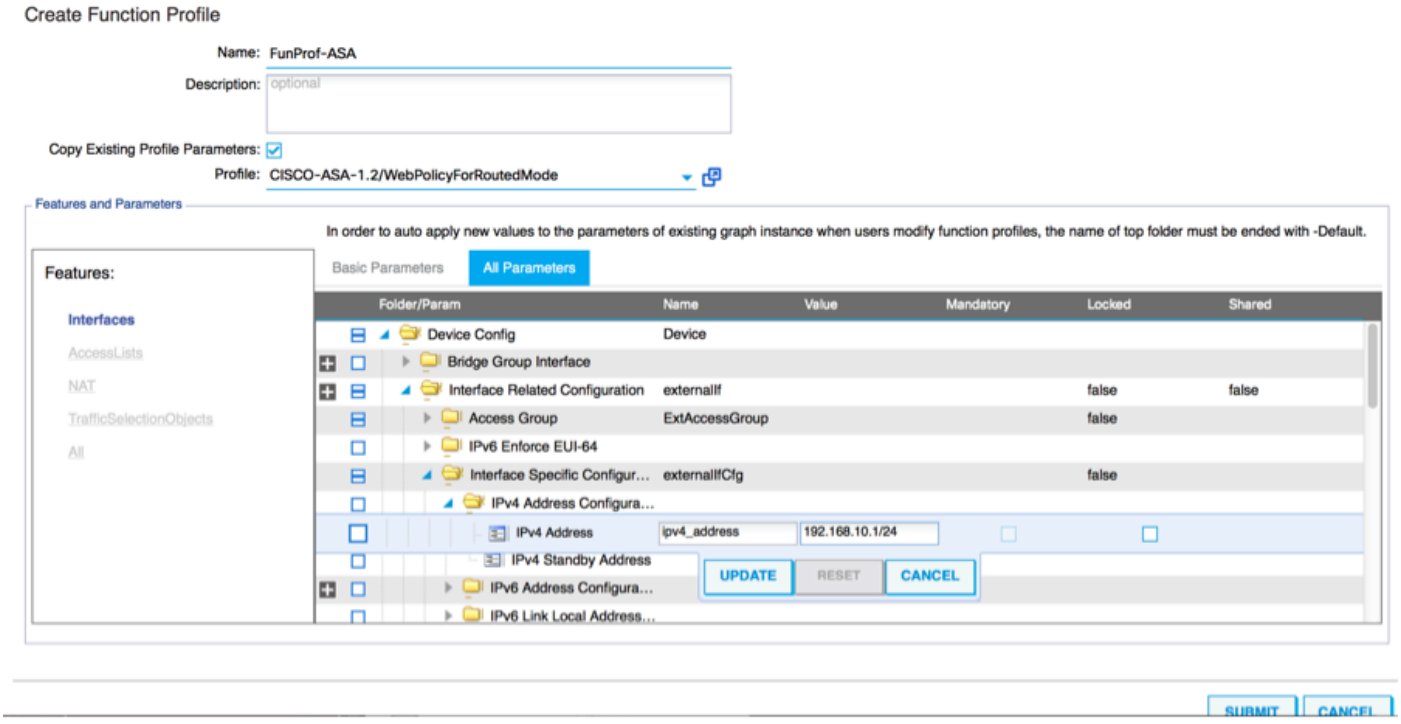




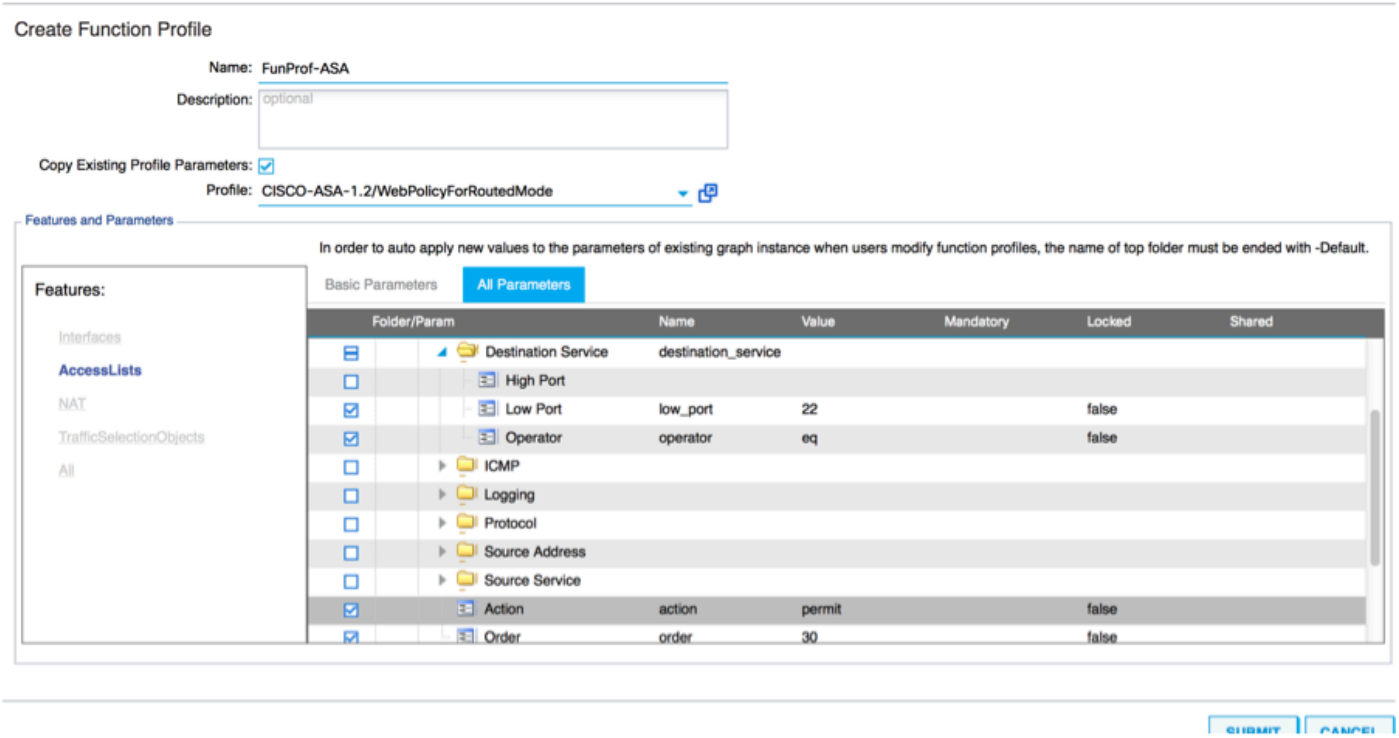
- 드롭다운 메뉴에서 **WebPolicyForRoutedMode** Profile을 선택하고 방화벽에서 인터페이스를 구성합니다.여기에서 단계는 선택 사항이며 나중에 구현/수정할 수 있습니다.이러한 단계는 서비스 그래프의 재사용 가능 또는 사용자 정의 방법에 따라 구축의 몇 가지 다른 단계에서 수행할 수 있습니다.

이 연습에서는 라우팅된 방화벽(GoTo 모드)을 사용하려면 각 인터페이스에 고유한 IP 주소가 있어야 합니다.또한 표준 ASA 컨피그레이션에는 인터페이스 보안 레벨이 있습니다(외부 인터페이스는 안전하지 않고 내부 인터페이스는 더 안전함). 요구 사항에 따라 인터페이스의 이름을 변경할 수도 있습니다.이 예에서는 기본값이 사용됩니다.

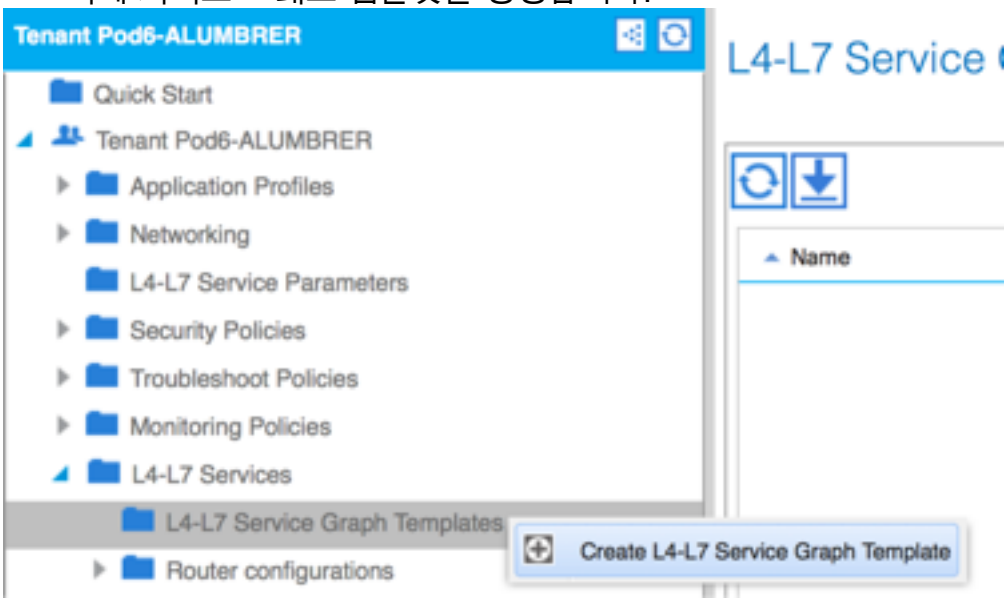
- Interface Specific Configuration(인터페이스별 컨피그레이션)을 확장하고 IP 주소 **x.x.x.x/y.y.y.y 또는 x.x.x.x/yy**의 다음 형식으로 ServerInt의 IP 주소 및 보안 수준**을 추가합니다** .ClientInt 인터페이스에 대해 프로세스를 반복합니다.



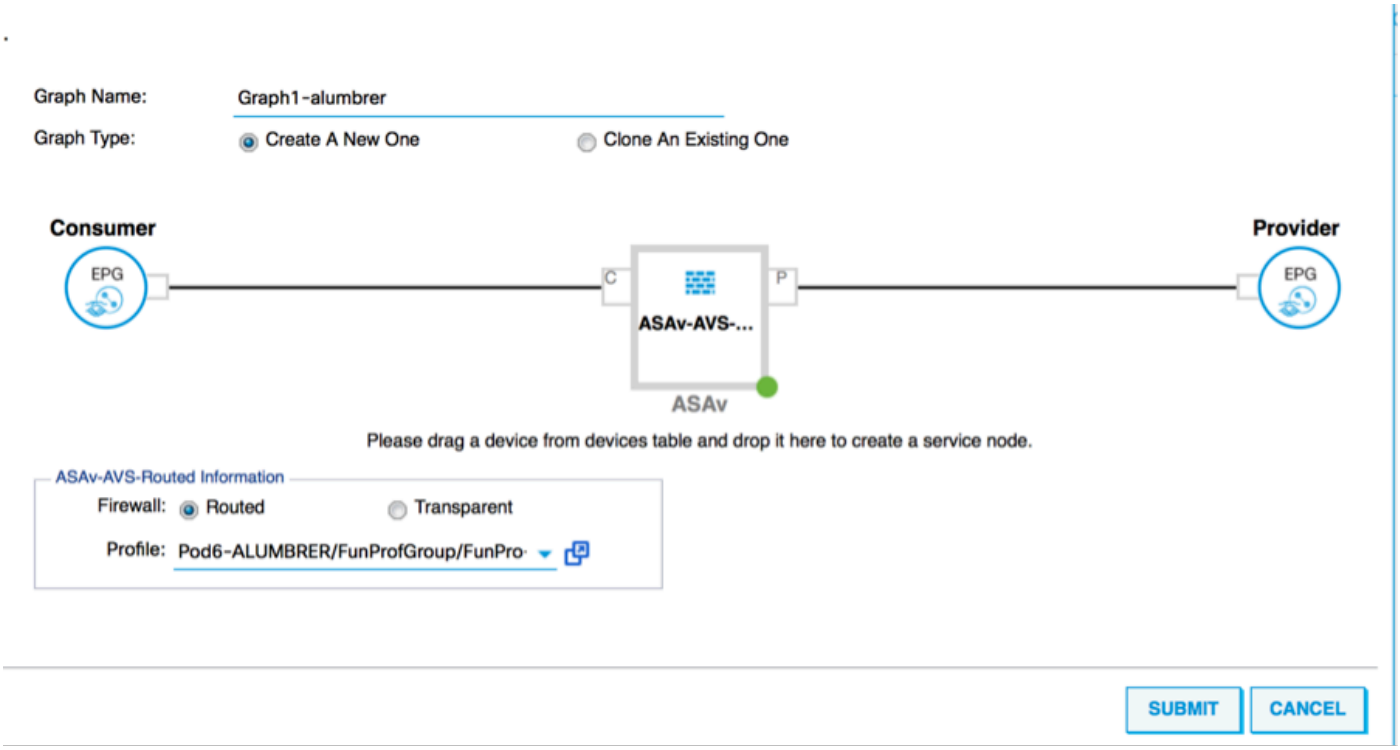
참고:기본 액세스 목록 설정을 수정하고 사용자 고유의 기본 템플릿을 만들 수도 있습니다.기본적으로 RoutedMode 템플릿에는 HTTP 및 HTTPS에 대한 규칙이 포함됩니다.이 연습에서는 SSH 및 ICMP가 허용된 외부 액세스 목록에 추가됩니다.



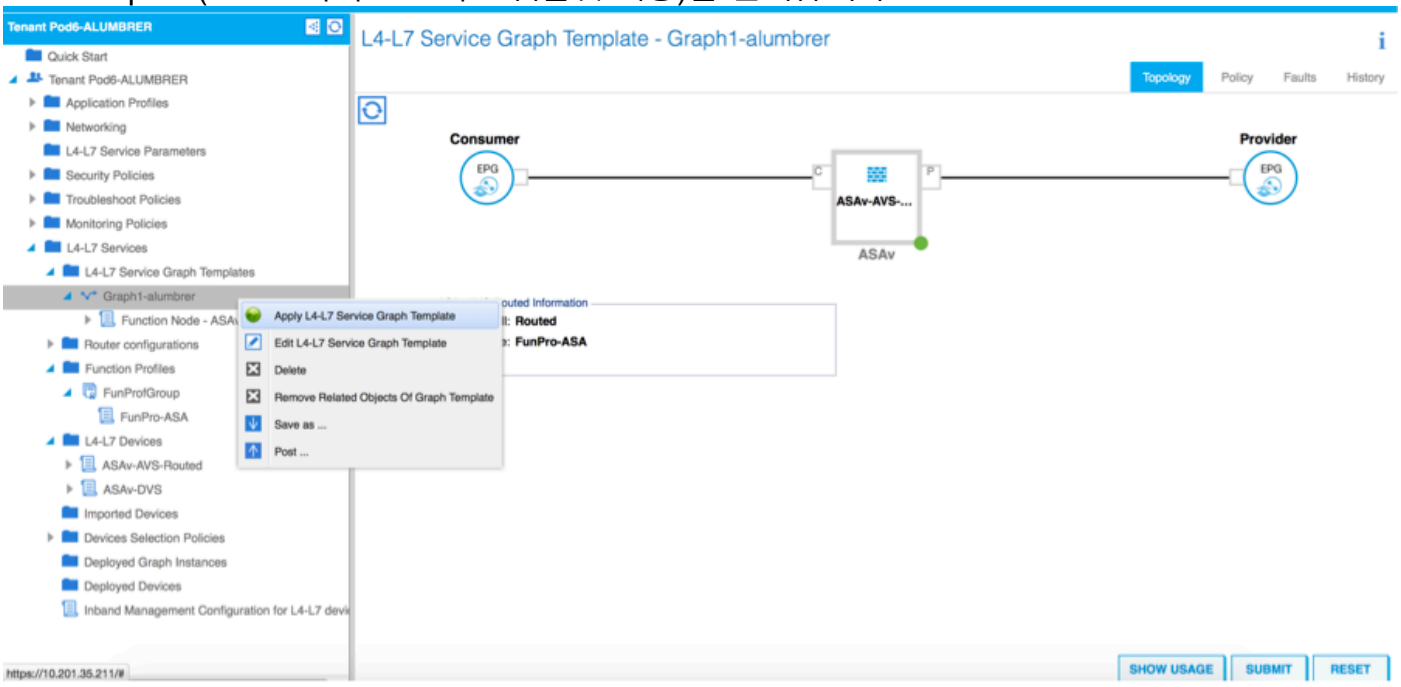
- 그런 다음 Submit(제출)을 **클릭합니다.**
- 이제 서비스 그래프 템플릿을 생성합니다.



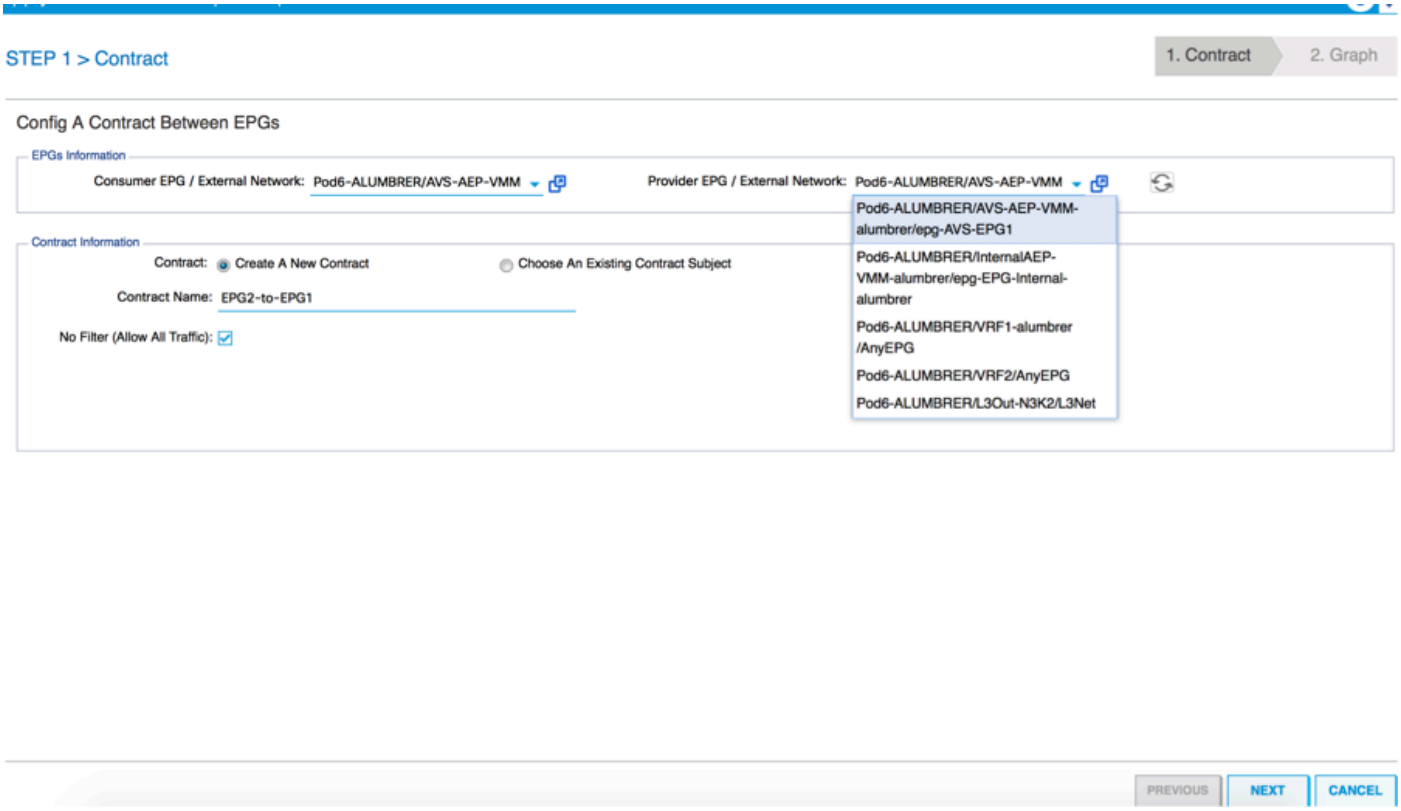
- 장치 클러스터를 오른쪽으로 끌어서 놓아 소비자와 공급자 간의 관계를 형성하고 라우팅 모드와 이전에 생성한 기능 프로파일을 선택합니다.



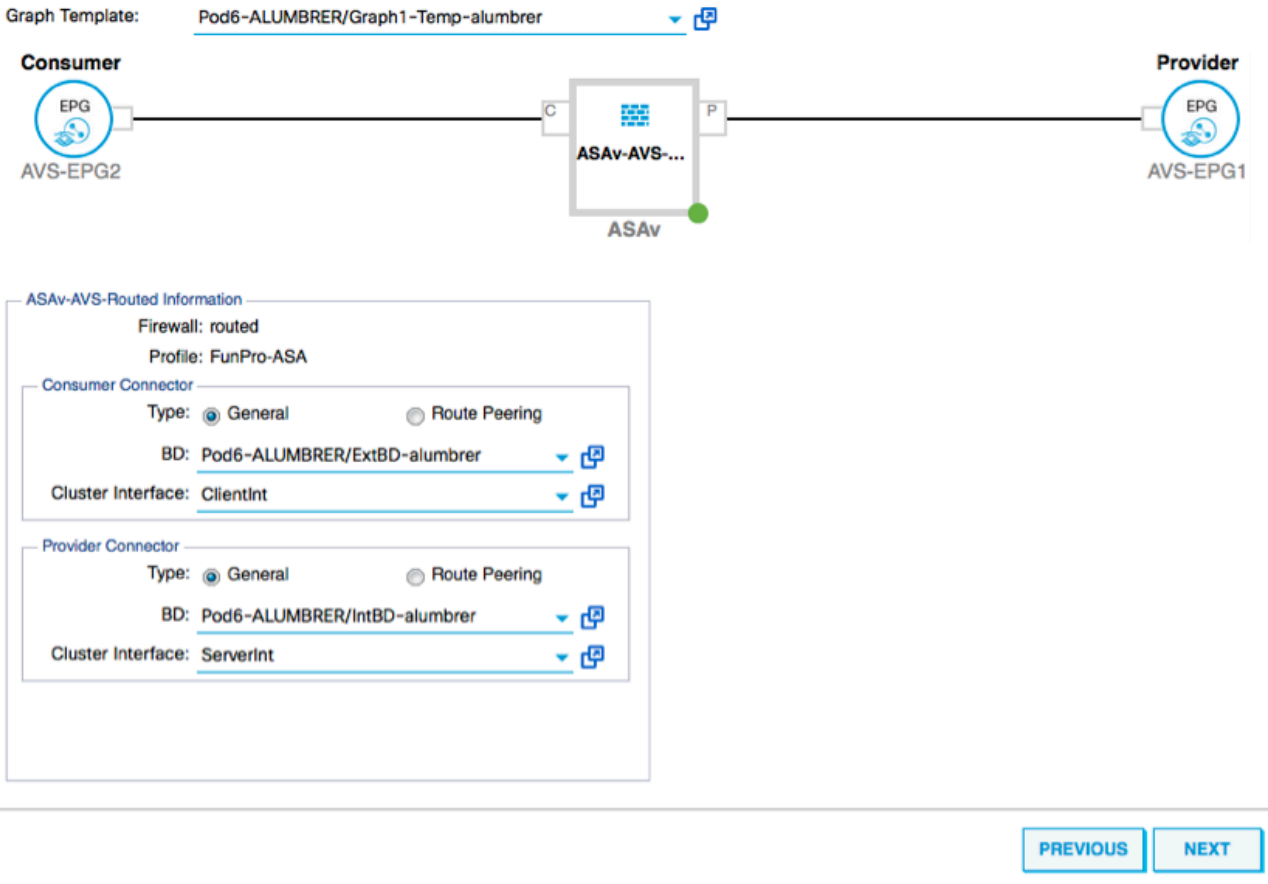
- 템플릿에 결함이 있는지 확인합니다.템플릿은 재사용 가능하도록 생성되며 특정 EPG 등에 적용해야 합니다.
- 템플릿을 적용하려면 마우스 오른쪽 버튼을 클릭하고 Apply L4-L7 Service Graph Template(L4-L7 서비스 그래프 템플릿 적용)을 선택합니다.



- 소비자 측 및 공급자 측에 어떤 EPG가 될지 정의합니다.이 연습에서는 AVS-EPG2가 소비자(클라이언트)이고 AVS-EPG1은 제공자(서버)입니다. 필터가 적용되지 않습니다. 그러면 방화벽에서 이 마법사의 마지막 섹션에 정의된 액세스 목록을 기반으로 모든 필터링을 수행할 수 있습니다.
- **다음**을 클릭합니다.

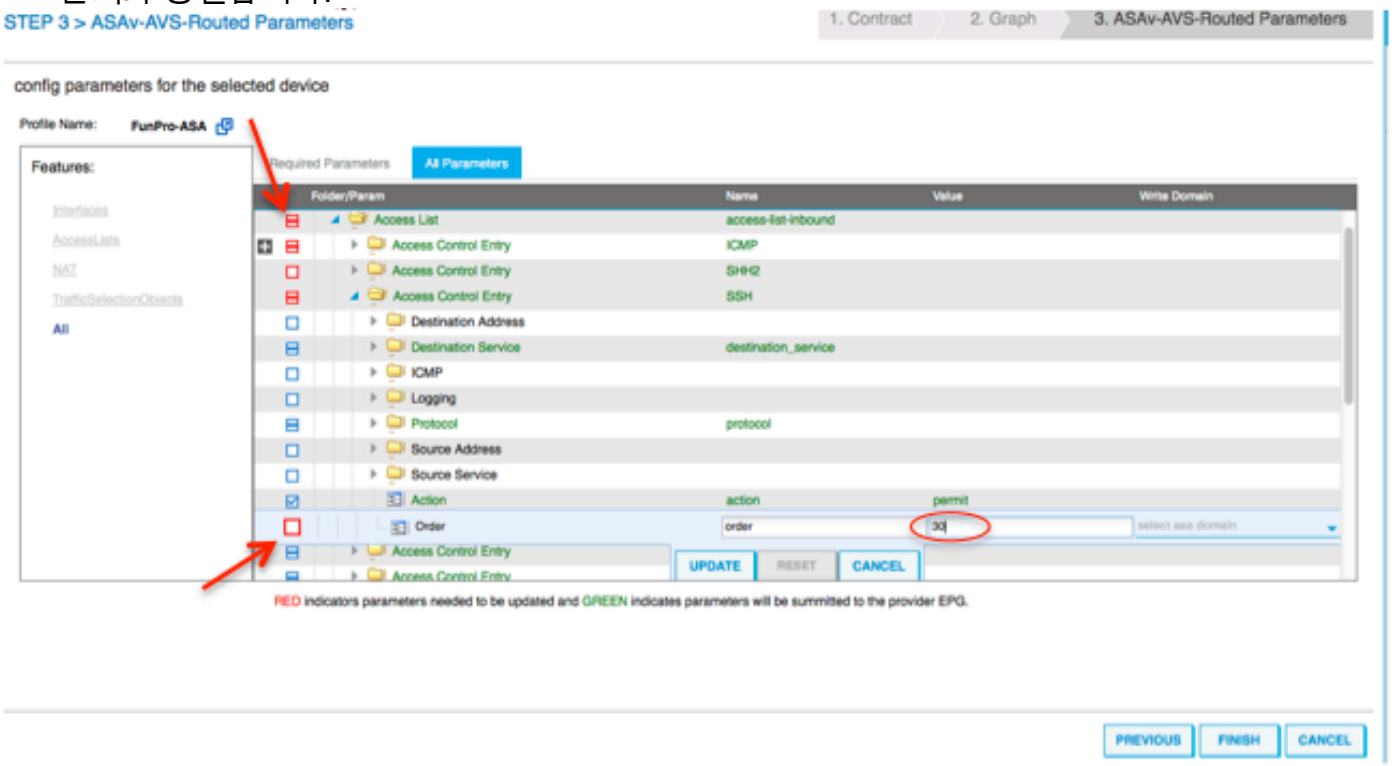


- 각 EPG에 대한 BD 정보를 확인합니다.이 경우 EPG1은 IntBD DB의 제공자이고 EPG2는 BD ExtBD의 소비자입니다.EPG1은 방화벽 인터페이스에서 연결되며 ServerInt 및 EPG2는 인터페이스 ClientInt에 연결됩니다.두 FW 인터페이스 모두 각 EPG의 DG가 되므로 트래픽은 항상 방화벽을 통과해야 합니다.
- **다음**을 클릭합니다.

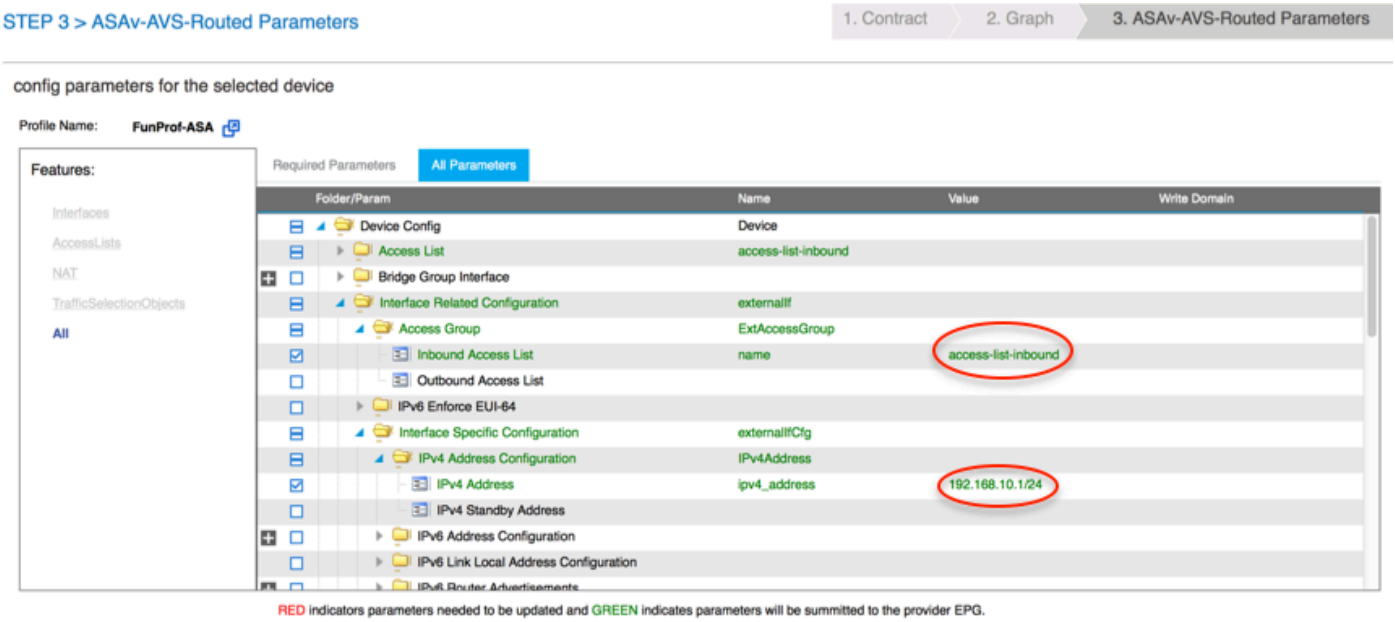


- Config Parameters(컨피그레이션 매개변수) 섹션에서 **All Parameters(모든 매개변수)**를 클릭하

고 업데이트/구성해야 하는 RED 지표가 있는지 확인합니다.이미지에 표시된 대로 출력에서 access-list의 순서가 누락되었음을 알 수 있습니다.이는 show ip access-list X에 표시되는 라인 순서와 동일합니다.



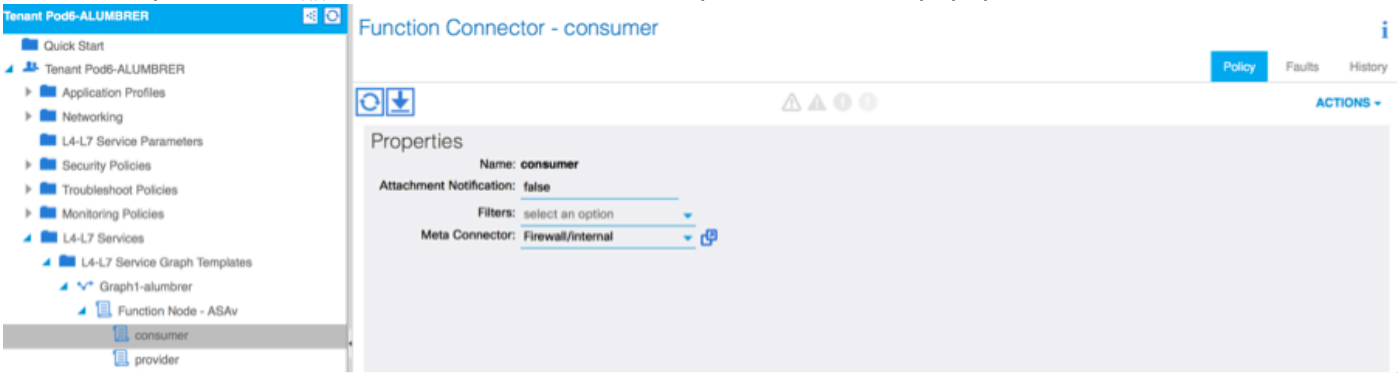
- 앞서 정의된 기능 프로필에서 할당한 IP 주소 지정을 확인할 수도 있습니다. 필요한 경우 정보를 변경할 수 있는 좋은 기회입니다.모든 매개 변수를 설정한 후에는 이미지에 표시된 대로 **마침**을 클릭합니다.



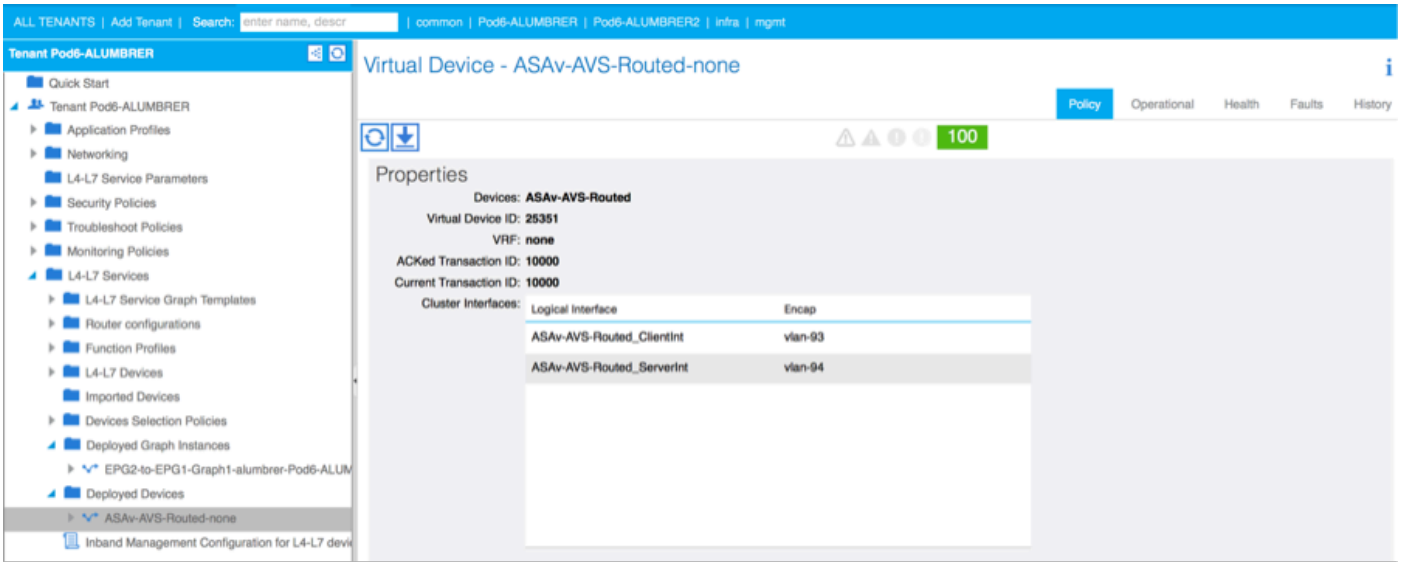
- 모든 것이 제대로 작동하면 새로운 Deployed 디바이스 및 Graph Instance 가 나타납니다.

확인

- 서비스 그래프를 작성한 후 확인해야 할 중요한 한 가지는 소비자/공급자 관계가 적절한 메타 커넥터로 생성되었다는 것입니다.함수 커넥터 등록 정보 아래에서 확인합니다.



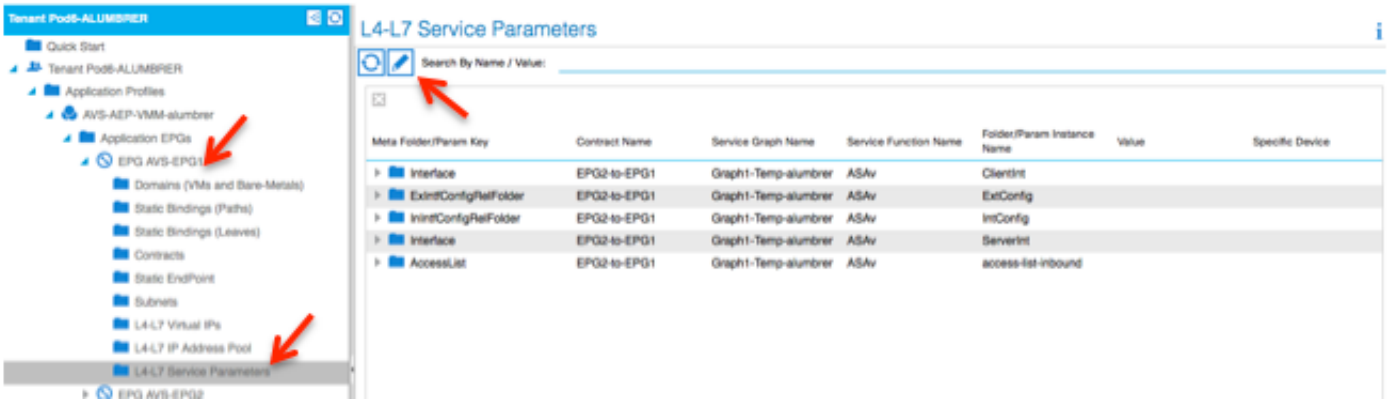
참고:방화벽의 각 인터페이스에는 AVS 동적 풀의 캡슐화-vlan이 할당됩니다.결함이 없는지 확인합니다.



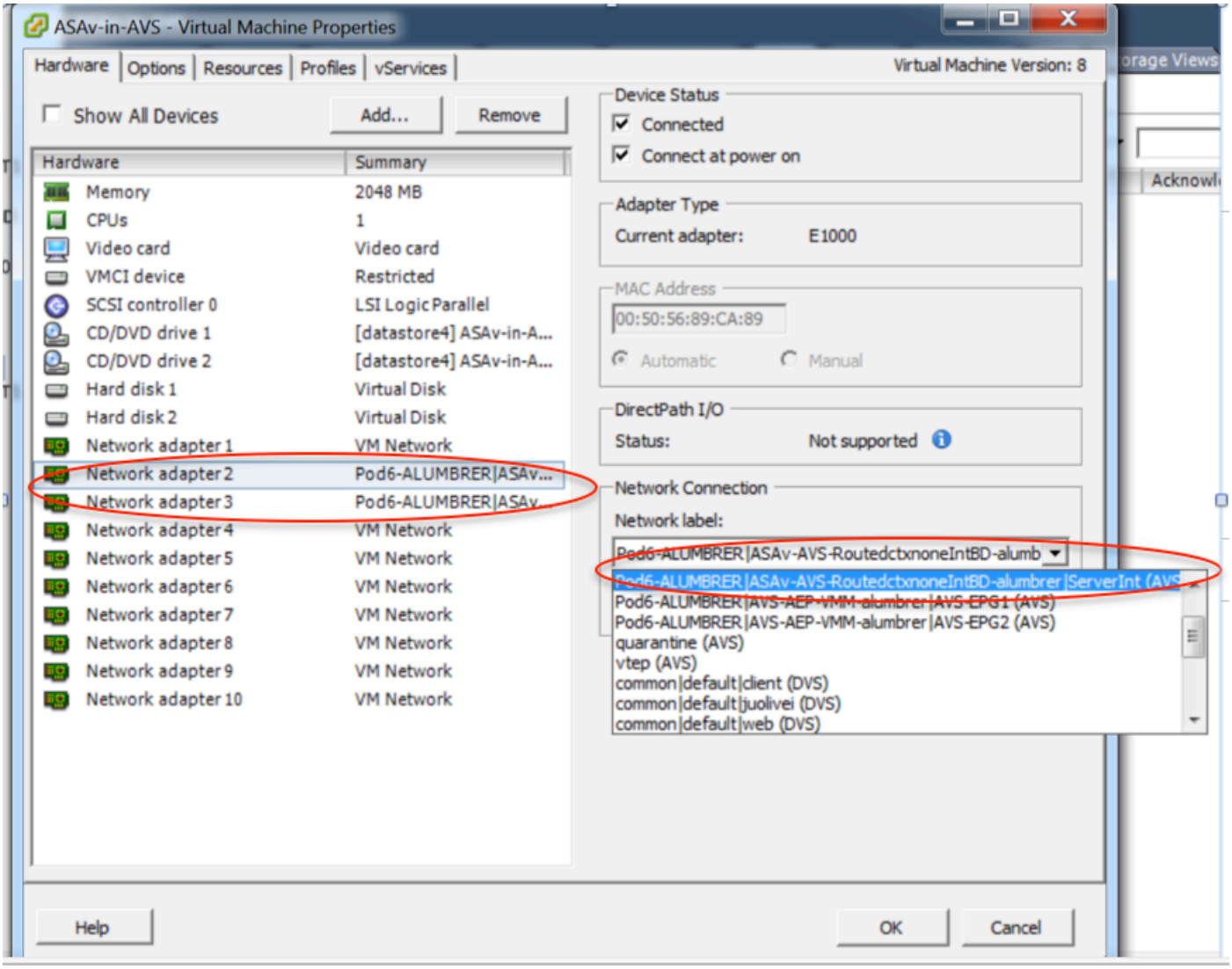
- 이제 ASAv로 푸시된 정보를 확인할 수도 있습니다

```
ASAv-w-AVS# show interface ip brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         192.168.10.1    YES manual up                    up
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down up
GigabitEthernet0/3         unassigned      YES unset  administratively down up
GigabitEthernet0/4         unassigned      YES unset  administratively down up
GigabitEthernet0/5         unassigned      YES unset  administratively down up
GigabitEthernet0/6         unassigned      YES unset  administratively down up
GigabitEthernet0/7         unassigned      YES unset  administratively down up
GigabitEthernet0/8         unassigned      YES unset  administratively down up
Management0/0              10.201.35.223   YES CONFIG up                    up
ASAv-w-AVS# show run access-list
access-list access-list-inbound extended permit tcp any any eq www
access-list access-list-inbound extended permit tcp any any eq https
access-list access-list-inbound extended permit tcp any any eq ssh
access-list access-list-inbound extended permit icmp any any
ASAv-w-AVS#
```

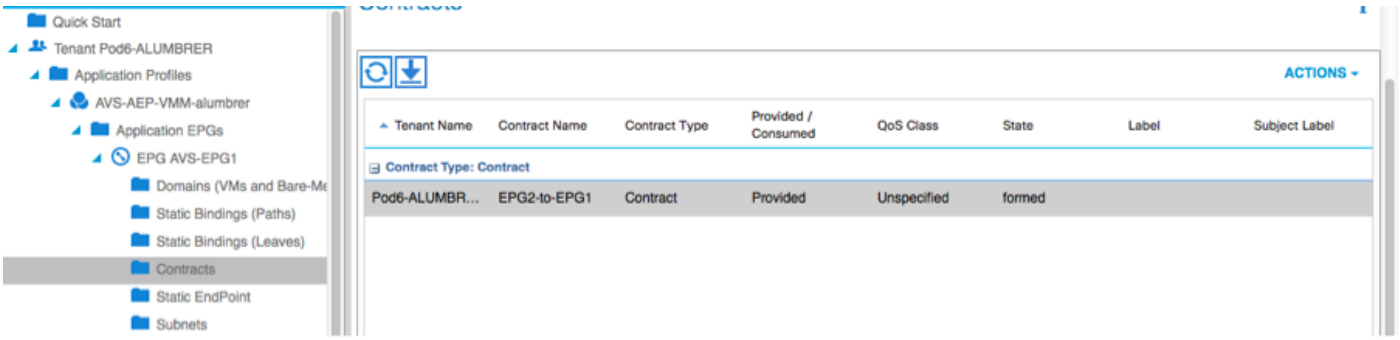
- EPG에 새 계약이 할당됩니다.지금부터 access-list에서 수정할 사항이 있으면 Provider EPG의 L4-L7 Service 매개변수에서 변경해야 합니다.



- vCenter에서 섀도우 EPG가 각 FW 인터페이스에 할당되었는지 확인할 수도 있습니다.



이 테스트에서는 2개의 EPG가 표준 계약과 통신했으며, 이 2개의 EPG는 서로 다른 도메인과 서로 다른 VRF에 있으므로, 두 EPG 간에 경로 누수가 이전에 구성되었습니다.이는 FW가 2개의 EPG 간에 라우팅 및 필터링을 설정할 때 서비스 그래프를 삽입한 후 약간 간소화됩니다.이전에 EPG 및 BD에 구성된 DG를 이제 계약과 동일하게 제거할 수 있습니다.L4-L7에서 푸시된 계약만 EPG에 남아 있어야 합니다.



표준 계약이 제거되면 이제 트래픽이 ASAv를 통해 이동하는지 확인할 수 있습니다. show access-list 명령은 클라이언트가 서버에 요청을 전송할 때마다 증가되는 규칙의 적중 횟수를 표시해야 합니다.

```
ASAv-w-AVS#
ASAv-w-AVS# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list access-list-inbound; 4 elements; name hash: 0xcb5bd6c7
access-list access-list-inbound line 1 extended permit tcp any any eq www (hitcn
t=0) 0xc873a747
access-list access-list-inbound line 2 extended permit tcp any any eq https (hit
cnt=0) 0x48bedbdd
access-list access-list-inbound line 3 extended permit tcp any any eq ssh (hitcn
t=4) 0x532fd57a
access-list access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0
xe4b5a75d
ASAv-w-AVS# _
```

leaf에서 엔드포인트는 클라이언트 및 서버 VM과 ASAv 인터페이스에 대해 학습해야 합니다.

```
leaf2# show endpoint
Legend:
 O - peer-attached    H - vtep            a - locally-aged     S - static
 V - vpc-attached     p - peer-aged       L - local            M - span
 s - static-arp       B - bounce
+------------------------------------+---------------+-----------------+-------------+-------------+
      VLAN/                          Encap           MAC Address       MAC Info/     Interface
      Domain                         VLAN            IP Address        IP Info
+------------------------------------+---------------+-----------------+-------------+-------------+
Pod6-ALUMBRER:VRF1-alumbrer                                50.50.50.50 L
14/Pod6-ALUMBRER:VRF1-alumbrer       vxlan-14778359     5897.bda4.f9bc L                eth1/13
30                                                      0050.5689.fa08 L                eth1/7
Pod6-ALUMBRER:VRF1-alumbrer          vlan-98            192.168.10.10 L
25                                   vlan-94            0050.5689.ca89 L                po4
Pod6-ALUMBRER:VRF1-alumbrer          vlan-94            192.168.10.1 L
mgmt:inb                                                192.168.2.11 S
21                                   vlan-97            0050.5689.3fca L                eth1/7
Pod6-ALUMBRER:VRF2                   vlan-97            172.16.1.10 L
26                                   vlan-93            0050.5689.e7dd L                po4
Pod6-ALUMBRER:VRF2                   vlan-93            172.16.1.1 L
overlay-1                                               10.0.104.93 L
overlay-1                                               10.0.96.67 L
13                                   vxlan-16777209     0050.5677.18a5 H                unspecified
overlay-1                            vxlan-16777209     10.0.32.93 H
13                                   vxlan-16777209     0050.5660.ddab H                unspecified
overlay-1                            vxlan-16777209     10.0.32.64 H
```


VEM에 연결된 방화벽 인터페이스를 모두 참조하십시오.

ESX-1

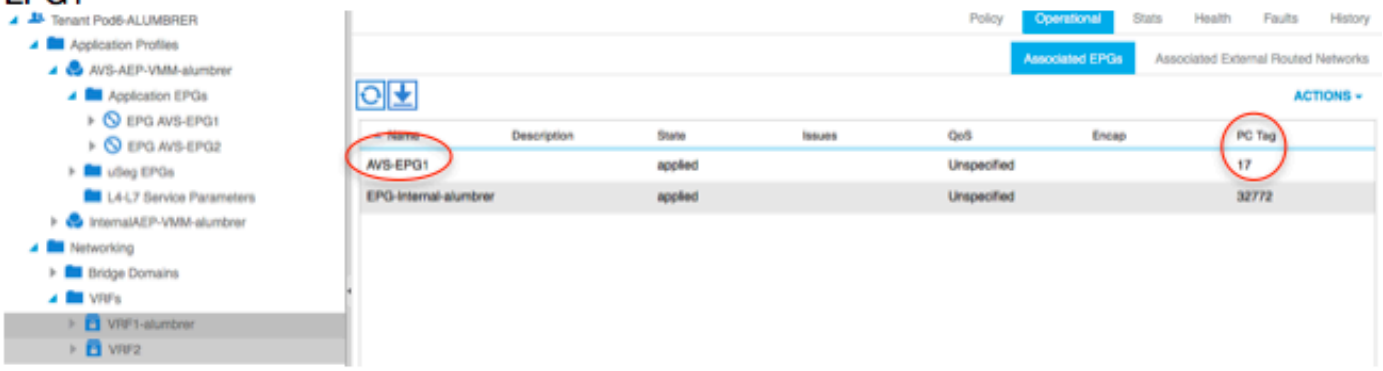
```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State   Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   22     Eth1/5     UP   UP    FWD       -    1040     4    0        0              vmnic4
   23     Eth1/6     UP   UP    FWD       -    1040     5    0        0              vmnic5
   50                UP   UP    FWD       -       0     4    0        0               vmk1
   51                UP   UP    FWD       -       0     4    0        0       ASAv-in-AVS.eth1
   52                UP   UP    FWD       -       0     4    0        0       ASAv-in-AVS.eth2
 1040        Po1     UP   UP    FWD       -       0          0        0
```

ESX-2

```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State   Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   24     Eth1/7     UP   UP    FWD       -    1040     6    0        0                vmnic6
   50                UP   UP    FWD       -       0     6    0        0                  vmk1
   51                UP   UP    FWD       -       0     6    0        0       Client1-AVS.eth0
   52                UP   UP    FWD       -       0     6    0        0       Server1-AVS.eth0
 1040        Po1     UP   UP    FWD       -       0          0        0
~ #
```

마지막으로, 소스 및 대상 EPG에 대한 PC 태그를 알고 있는 경우 리프 레벨에서 방화벽 규칙을 확인할 수 있습니다.

EPG1



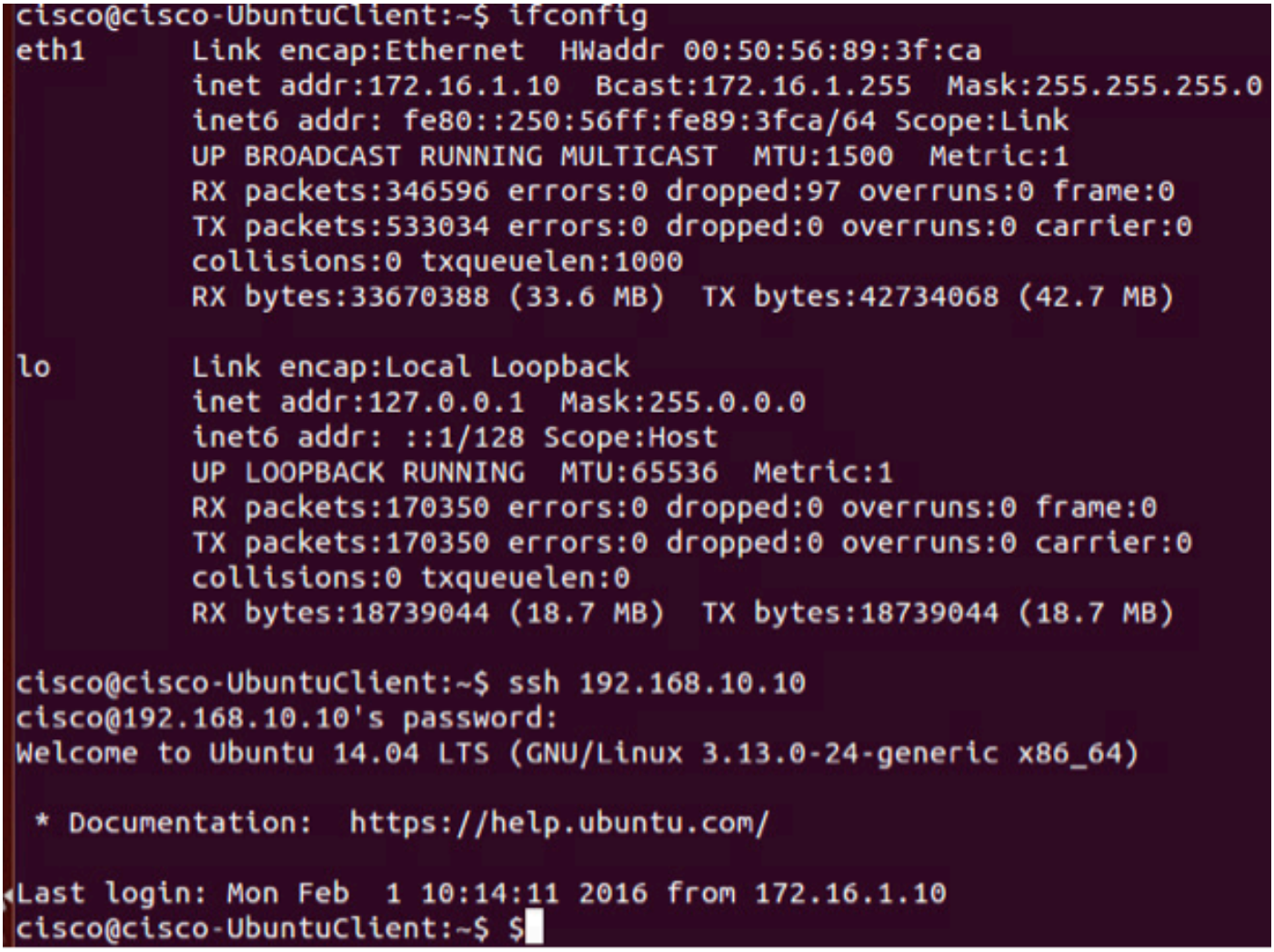
EPG2

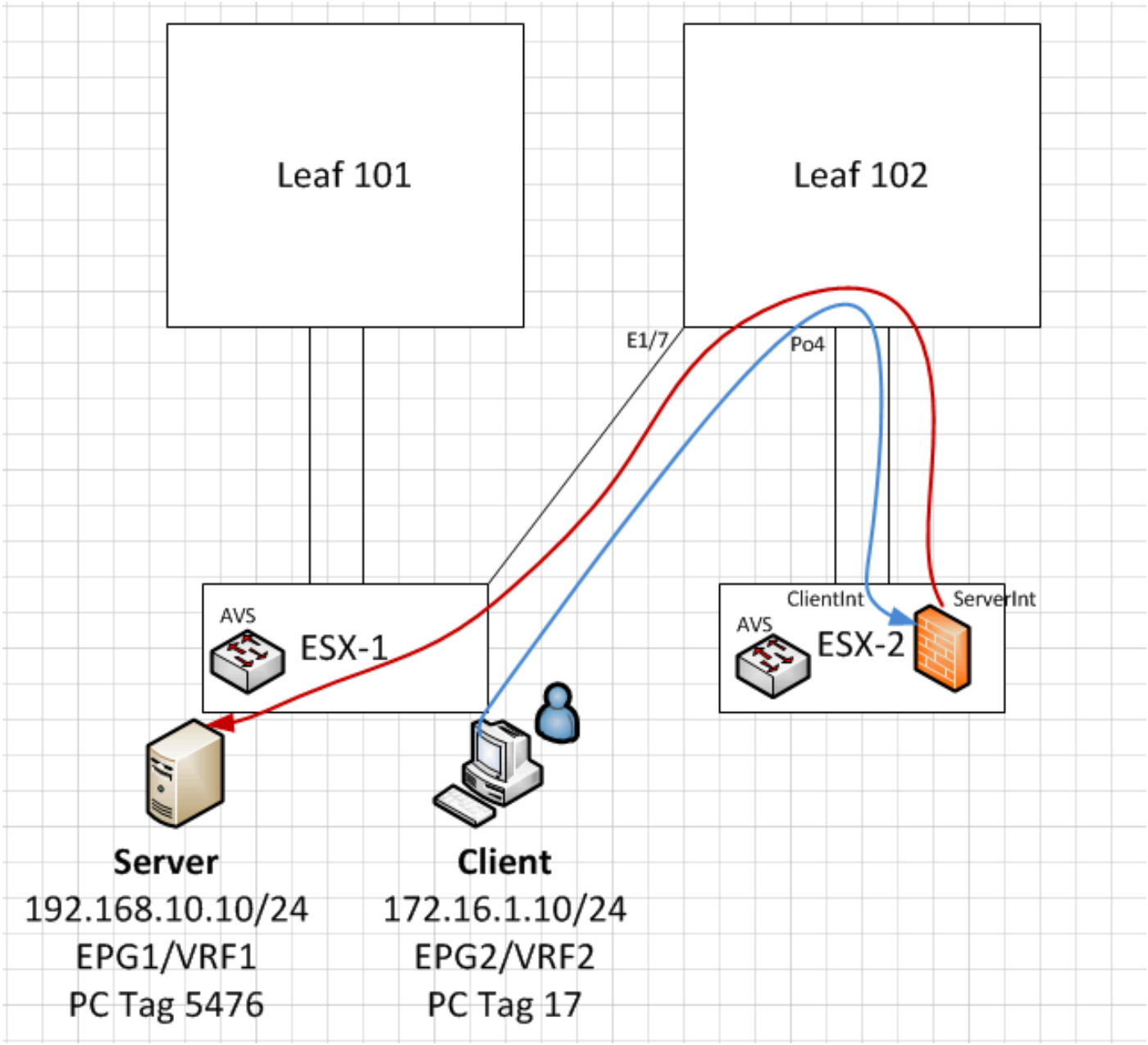
필터 ID를 leaf의 PC 태그와 일치시켜 FW 규칙을 확인할 수 있습니다.

```
leaf2# show zoning-rule | grep '17\|5476'
4141        17          32775       default     enabled     2916352     permit      src_dst_any(5)
4142        32775       17          default     enabled     2916352     permit      src_dst_any(5)
4139        5476        49156       14          enabled     2555904     permit      src_dst_any(5)
4140        49156       5476        14          enabled     2555904     permit      src_dst_any(5)
leaf2#
```

> **참고**:EPG PCTags/Sclass는 직접 통신하지 않습니다.L4-L7 서비스 그래프 삽입에 의해 생성된 섀도우 EPG를 통해 통신이 중단되거나 연결됩니다.

통신 클라이언트와 서버 간의 통신이 작동합니다.

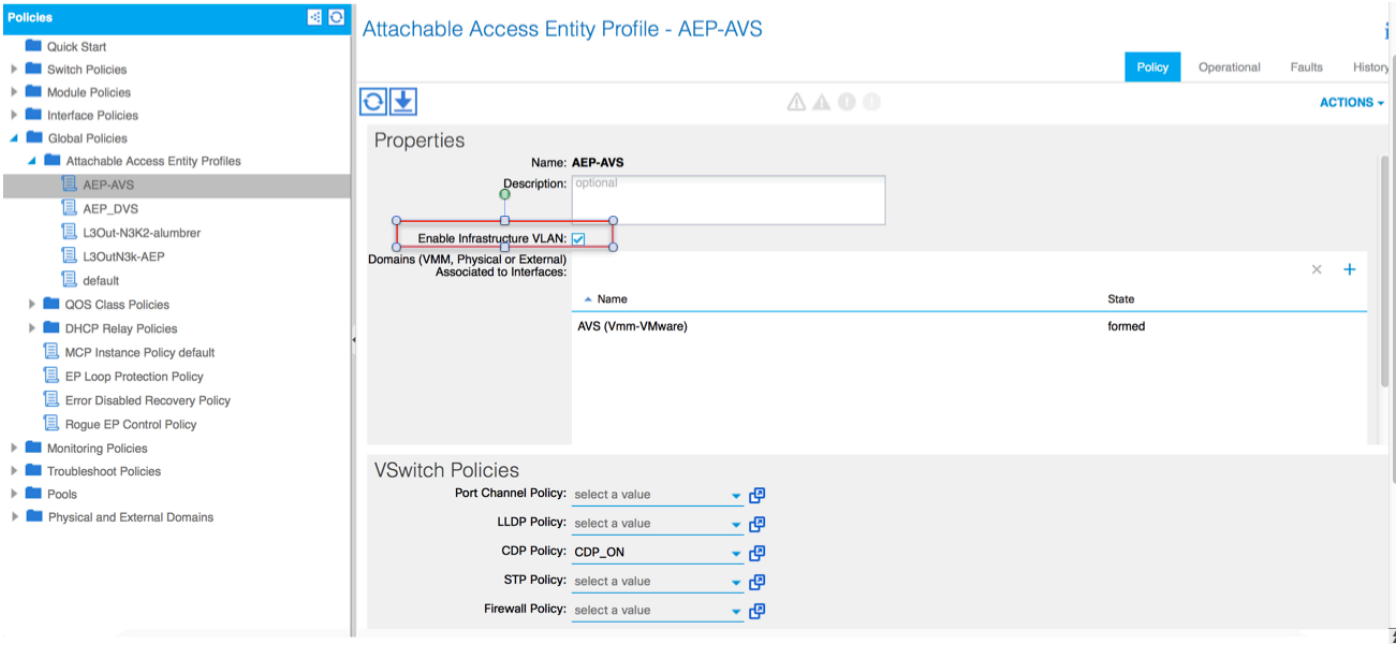

cisco@cisco-UbuntuClient:~$ ifconfig
eth1 Link encap:Ethernet HWaddr 00:50:56:89:3f:ca
inet addr:172.16.1.10 Bcast:172.16.1.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:346596 errors:0 dropped:97 overruns:0 frame:0
TX packets:533034 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:33670388 (33.6 MB) TX bytes:42734068 (42.7 MB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:170350 errors:0 dropped:0 overruns:0 frame:0
TX packets:170350 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:18739044 (18.7 MB) TX bytes:18739044 (18.7 MB)
cisco@cisco-UbuntuClient:~$ ssh 192.168.10.10
cisco@192.168.10.10's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
* Documentation: https://help.ubuntu.com/
Last login: Mon Feb 1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~$ $



문제 해결

VTEP 주소가 할당되지 않았습니다.

AEP에서 인프라 VLAN이 선택되어 있는지 확인합니다.



지원되지 않는 버전

VEM 버전이 올바른지 확인하고 적절한 ESXi VMWare 시스템을 지원합니다.

```
~ # vem version
Running esx version -1746974 x86_64
VEM Version: 5.2.1.3.1.10.0-3.2.1
OpFlex SDK Version: 1.2(1i)
System Version: VMware ESXi 5.5.0 Releasebuild-1746974
ESX Version Update Level: 0
```

VEM 및 패브릭 통신이 작동하지 않음

```
- Check VEM status
vem status

- Try reloading or restating the VEM at the host:
vem reload
vem restart

- Check if there's connectivity towards the Fabric. You can try pinging 10.0.0.30 which is
(infra:default) with 10.0.0.30 (shared address, for both Leafs)

~ # vmkping -I vmk1 10.0.0.30
PING 10.0.0.30 (10.0.0.30): 56 data bytes

--- 10.0.0.30 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss

If ping fails, check:

- Check OpFlex status - The DPA (DataPathAgent) handles all the control traffic between AVS and
APIC (talks to the immediate Leaf switch that is connecting to) using OpFlex (opflex
client/agent).
All EPG communication will go thru this opflex connection. ~ # vemcmd show opflex Status: 0
(Discovering) Channel0: 0 (Discovering), Channel1: 0 (Discovering) Dvs name: comp/prov-
VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129 Remote IP: 10.0.0.30 Port: 8000 Infra vlan: 3967
FTEP IP: 10.0.0.32 Switching Mode: unknown Encap Type: unknown NS GIPO: 0.0.0.0 you can also
check the status of the vmnics at the host level: ~ # esxcfg-vmknic -l Interface Port
Group/DVPort IP Family IP Address Netmask Broadcast MAC Address MTU TSO MSS Enabled Type vmk0
```

```
Management Network IPv4 10.201.35.219 255.255.255.0 10.201.35.255 e4:aa:5d:ad:06:3e 1500 65535
true STATIC vmk0 Management Network IPv6 fe80::e6aa:5dff:fead:63e 64 e4:aa:5d:ad:06:3e 1500
65535 true STATIC, PREFERRED vmk1 160 IPv4 10.0.32.65 255.255.0.0 10.0.255.255 00:50:56:6b:ca:25
1500 65535 true STATIC vmk1 160 IPv6 fe80::250:56ff:fe6b:ca25 64 00:50:56:6b:ca:25 1500 65535
true STATIC, PREFERRED ~ # - Also on the host, verify if DHCP requests are sent back and forth:
~ # tcpdump-uw -i vmk1 tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol
decode listening on vmk1, link-type EN10MB (Ethernet), capture size 96 bytes 12:46:08.818776 IP
truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:50:56:6b:ca:25 (oui Unknown), length 300 12:46:13.002342 IP truncated-ip - 246 bytes
missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25
(oui Unknown), length 300 12:46:21.002532 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc >
255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300
12:46:30.002753 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps:
BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300
```

이때 ESXi 호스트와 Leaf 간의 Fabric 통신이 제대로 작동하지 않는지 확인할 수 있습니다.일부 확인 명령은 leaf 측에서 확인하여 근본 원인을 확인할 수 있습니다.

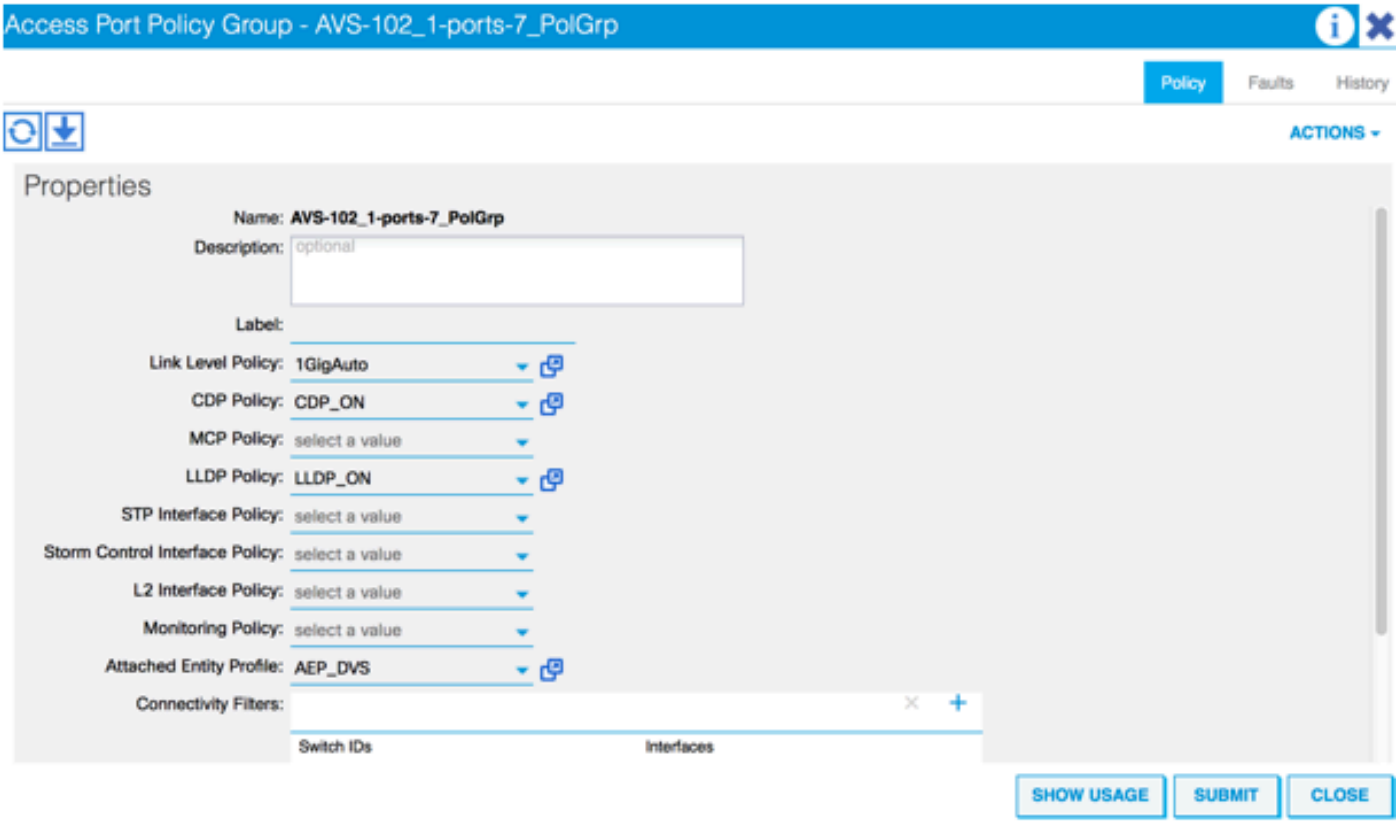
```
leaf2# show cdp ne

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme  Capability  Platform      Port ID
AVS:localhost.localdomainmain
                     Eth1/5          169     S I s      VMware ESXi    vmnic4
AVS:localhost.localdomainmain
                     Eth1/6          169     S I s      VMware ESXi    vmnic5
N3K-2(FOC1938R02L)
                     Eth1/13         166     R S I s    N3K-C3172PQ-1  Eth1/13

leaf2# show port-c sum
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
        F - Configuration failed
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
5     Po5(SU)     Eth      LACP      Eth1/5(P)    Eth1/6(P)
```

Po5를 통해 연결된 ESXi에는 2개의 포트가 사용됩니다.

```
leaf2# show vlan extended

 VLAN Name                             Status    Ports
 ---- -------------------------------- --------- -------------------------------
 13   infra:default                    active    Eth1/1, Eth1/20
 19   --                               active    Eth1/13
 22   mgmt:inb                         active    Eth1/1
 26   --                               active    Eth1/5, Eth1/6, Po5
 27   --                               active    Eth1/1
 28   ::                               active    Eth1/5, Eth1/6, Po5
 36   common:pod6_BD                   active    Eth1/5, Eth1/6, Po5
```

```
VLAN Type  Vlan-mode  Encap
---- ----- ---------- --------------------------------
13   enet  CE         vxlan-16777209, vlan-3967
19   enet  CE         vxlan-14680064, vlan-150
22   enet  CE         vxlan-16383902
26   enet  CE         vxlan-15531929, vlan-200
27   enet  CE         vlan-11
28   enet  CE         vlan-14
36   enet  CE         vxlan-15662984
```

위의 출력에서 ESXi 호스트(1/5-6)로 이동하는 업링크 포트를 통해 Infra VLAN이 허용되지 않거나 전달되지 않음을 확인할 수 있습니다. 이는 인터페이스 정책 또는 스위치 정책이 APIC에 구성된 컨피그레이션이 잘못되었음을 나타냅니다.
모두 확인:
액세스 정책 > 인터페이스 정책 > 프로파일 액세스 정책 > 스위치 정책 > 프로파일
이 경우 인터페이스 프로파일은 이미지에 표시된 대로 잘못된 AEP(DVS에 사용된 이전 AEP)에 연결됩니다.



AVS에 대한 올바른 AEP를 설정한 후 Leaf의 적절한 Unlink를 통해 Infra Vlan이 표시되는 것을 확인할 수 있습니다.

```
leaf2# show vlan extended

VLAN Name                             Status    Ports
---- -------------------------------- --------- --------------------------------
13   infra:default                    active    Eth1/1, Eth1/5, Eth1/6,
                                                Eth1/20, Po5
19   --                               active    Eth1/13
22   mgmt:inb                         active    Eth1/1
26   --                               active    Eth1/5, Eth1/6, Po5
27   --                               active    Eth1/1
28   ::                               active    Eth1/5, Eth1/6, Po5
36   common:pod6_BD                   active    Eth1/5, Eth1/6, Po5

VLAN Type  Vlan-mode  Encap
---- ----- ---------- --------------------------------
```

```
 13    enet  CE         vxlan-16777209, vlan-3967
 19    enet  CE         vxlan-14680064, vlan-150
 22    enet  CE         vxlan-16383902
 26    enet  CE         vxlan-15531929, vlan-200
 27    enet  CE         vlan-11
 28    enet  CE         vlan-14
 36    enet  CE         vxlan-15662984
```

and Opflex connection is restablised after restarting the VEM module:

```
~ # vem restart
stopDpa
VEM SwISCSI PID is
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
watchdog-vemdpa: Terminating watchdog process with PID 213974

~ # vemcmd show opflex
Status: 0 (Discovering)
Channel0: 14 (Connection attempt), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: unknown
Encap Type: unknown
NS GIPO: 0.0.0.0

~ # vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: unknown
NS GIPO: 0.0.0.0
```

관련 정보

애플리케이션 가상 스위치 설치

Cisco Systems, Inc. Cisco Application Virtual Switch 설치 가이드, 릴리스 5.2(1)SV3(1.2)
VMware를 사용하여 ASAv 구축

Cisco Systems, Inc. Cisco ASAv(Adaptive Security Virtual Appliance) 빠른 시작 가이드, 9.4

Cisco ACI 및 Cisco AVS

Cisco Systems, Inc. Cisco ACI 가상화 가이드, 릴리스 1.2(1i)

Cisco Application Centric Infrastructure를 사용한 서비스 그래프 설계 백서

Cisco Application Centric Infrastructure를 사용한 서비스 그래프 설계 백서

기술 지원 및 문서 - Cisco Systems