ASAv en el modo GoTo (L3) con el uso de AVS-ACI 1.2(x) versión

Contenido

Introducción

Este documento describe cómo implementar un switch Application Virtual Switch (AVS) con un firewall único Adaptive Security Virtual Appliance (ASAv) en modo Routed/GOTO como un gráfico de servicio L4-L7 entre dos grupos de punto final (EPG) para establecer la comunicación cliente-servidor mediante la versión ACI 1.2(x).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Políticas de acceso configuradas e interconectadas en servicio
- EPG, dominio de puente (BD) y routing y reenvío virtual (VRF) ya configurados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Hardware y software:

- UCS C220 - 2.0(6 d)
- ESXi/vCenter - 5.5
- ASAv - asa-device-pkg-1.2.4.8
- AVS - 5.2.1.SV3.1.10
- APIC - 1.2(1i)
- Hoja/espinas - 11.2(1i)
- Paquetes de dispositivos *.zip ya descargados

Funciones:

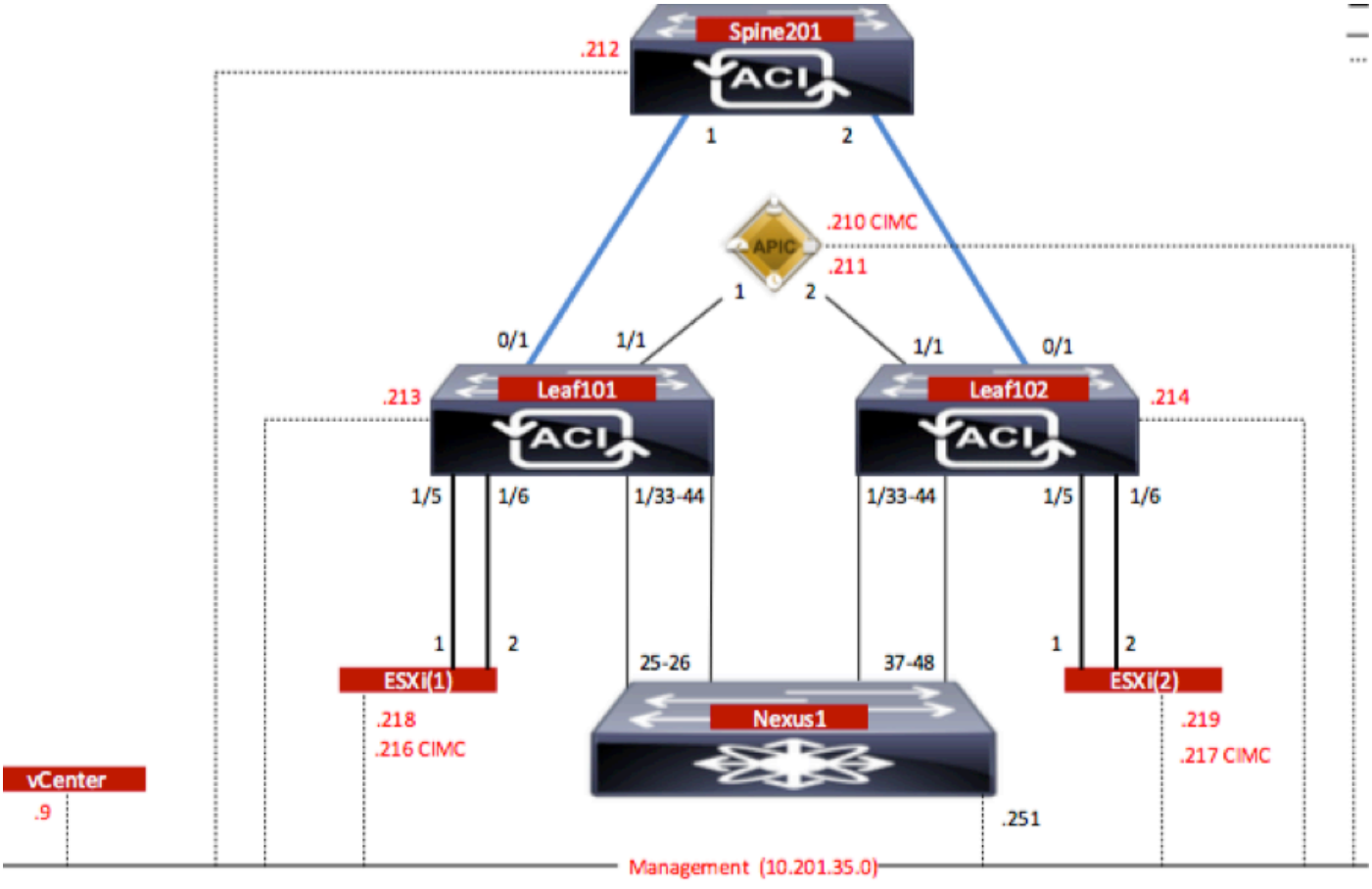
- AVS
- ASAv
- EPG, BD, VRF
- Lista de control de acceso (ACL)
- Gráfico de servicios L4-L7
- vCenter

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de la red

Como se muestra en la imagen,



Configuraciones

La configuración inicial de AVS crea un dominio VMware vCenter (integración de VMware)2

Nota:

- Puede crear varios Data Centers y entradas de switch virtual distribuido (DVS) bajo un único

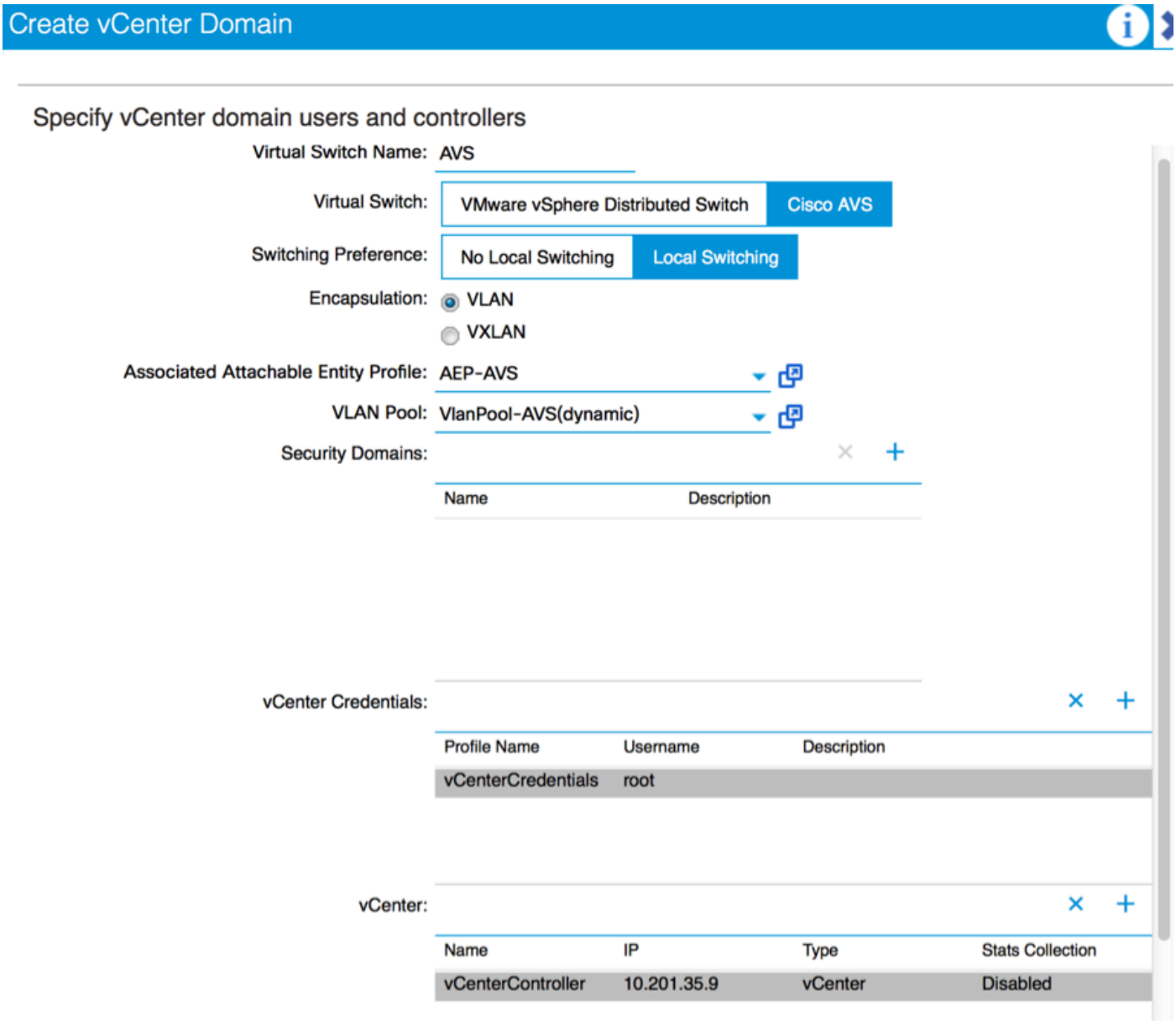
dominio. Sin embargo, sólo puede tener asignado un AVS de Cisco a cada Data Center.

- La implementación de gráficos de servicios con Cisco AVS es compatible con Cisco ACI versión 1.2(1i) con Cisco AVS versión 5.2(1)SV3(1.10). Toda la configuración del gráfico de servicios se realiza en el Cisco Application Policy Infrastructure Controller (Cisco APIC).

- La implementación de la máquina virtual de servicios (VM) con Cisco AVS solo se admite en dominios de Virtual Machine Manager (VM) con modo de encapsulación de redes de área local virtuales (VLAN). Sin embargo, las VM informáticas (las VM de proveedor y de consumidor) pueden formar parte de dominios de VM con Virtual Extensible LAN (VXLAN) o encapsulación de VLAN.

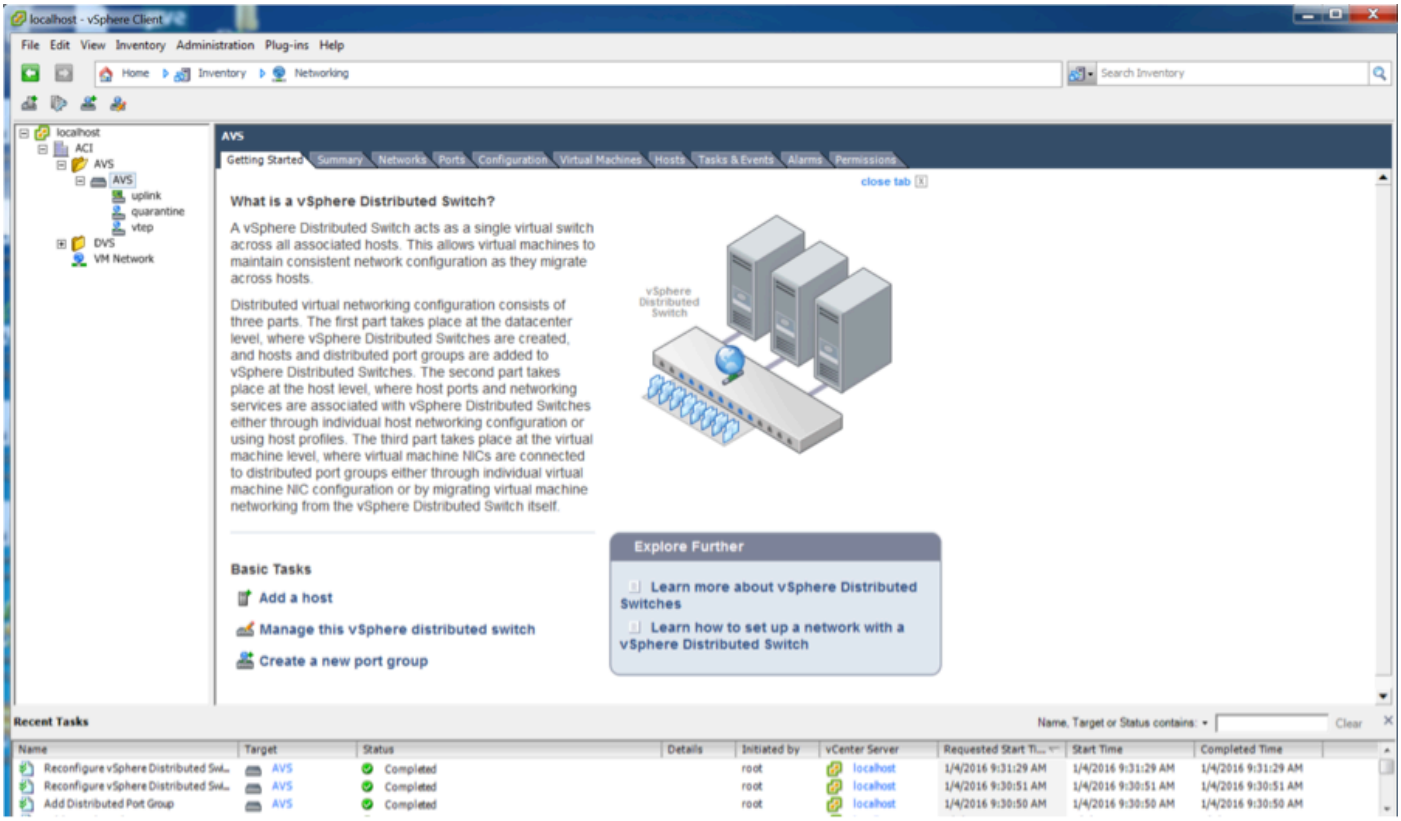
- Tenga en cuenta también que si se utiliza el switching local, no se requieren la dirección de multidifusión ni el conjunto. Si no se selecciona ninguna conmutación local, se debe configurar el conjunto de multidifusión y la dirección de multidifusión de AVS Fabric-wide no debe formar parte del conjunto de multidifusión. Todo el tráfico originado desde el AVS será VLAN o VXLAN encapsulado.

Navegue hasta **VM Networking > VMWare > Create vCenter Domain,** como se muestra en la imagen:

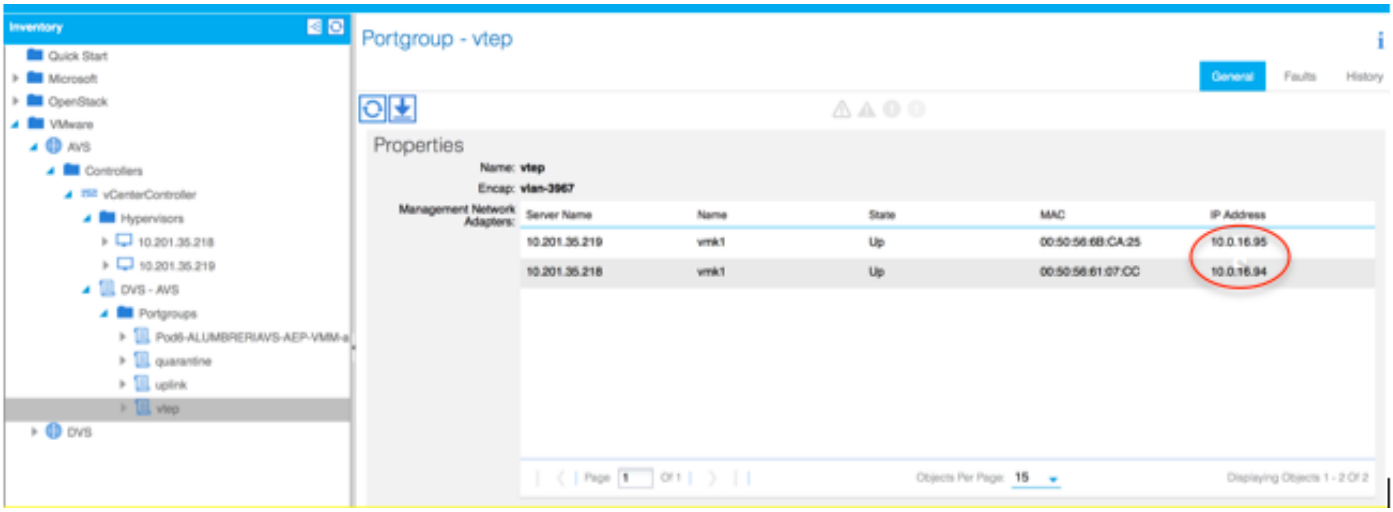


Si utiliza Port-Channel o VPC (Virtual Port-Channel), se recomienda establecer las políticas de vSwitch para utilizar Mac Pinning.

Después de esto, APIC debe enviar la configuración del switch AVS a vCenter, como se muestra en la imagen:



En APIC, puede observar que una dirección VXLAN Tunnel Endpoint (VTEP) se asigna al grupo de puertos VTEP para AVS. Esta dirección se asigna independientemente del modo de conectividad utilizado (VLAN o VXLAN)



Instale el software Cisco AVS en vCenter

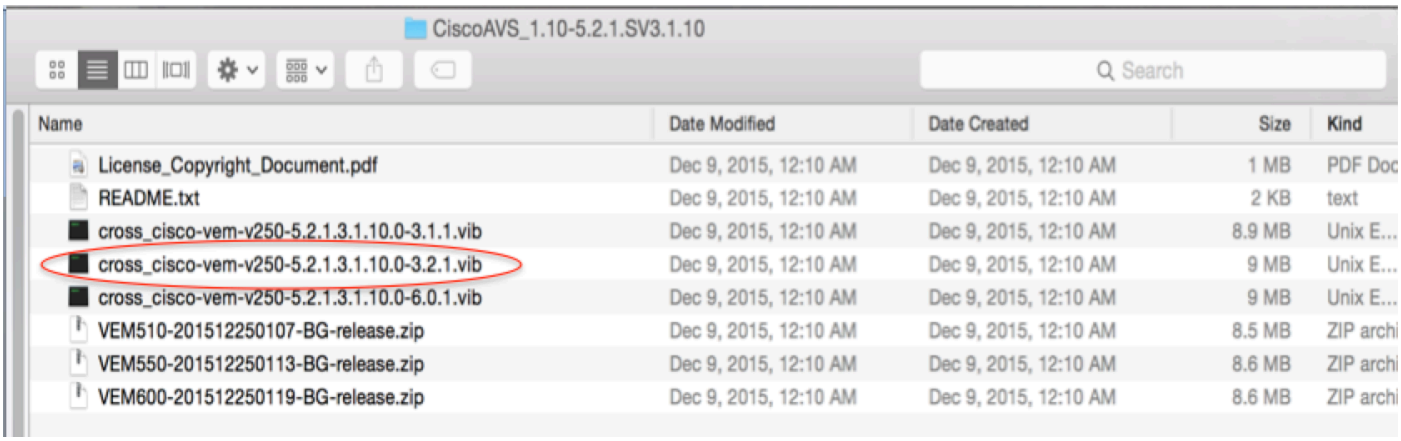
- Descargue vSphere Installation Bundle (VIB) de CCO mediante este enlace

  Nota: En este caso, utilizamos ESX 5.5, Tabla 1, que muestra la matriz de compatibilidad para ESXi 6.0, 5.5, 5.1 y 5.0

Tabla 1: Compatibilidad de la versión de software host para ESXi 6.0, 5.5, 5.1 y 5.0

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

Dentro del archivo ZIP hay 3 archivos VIB, uno para cada una de las versiones de host ESXi, seleccione el apropiado para ESX 5.5, como se muestra en la imagen:



- Copie el archivo VIB en ESX Datastore; esto se puede hacer a través de CLI o directamente desde vCenter

  Nota: Si existe un archivo VIB en el host, retírelo usando el comando **esxcli software vib** remove.

esxcli software vib remove -n cross_cisco-vem-v197-5.2.1.3.1.5.0-3.2.1.vib

o explorando el almacén de datos directamente.

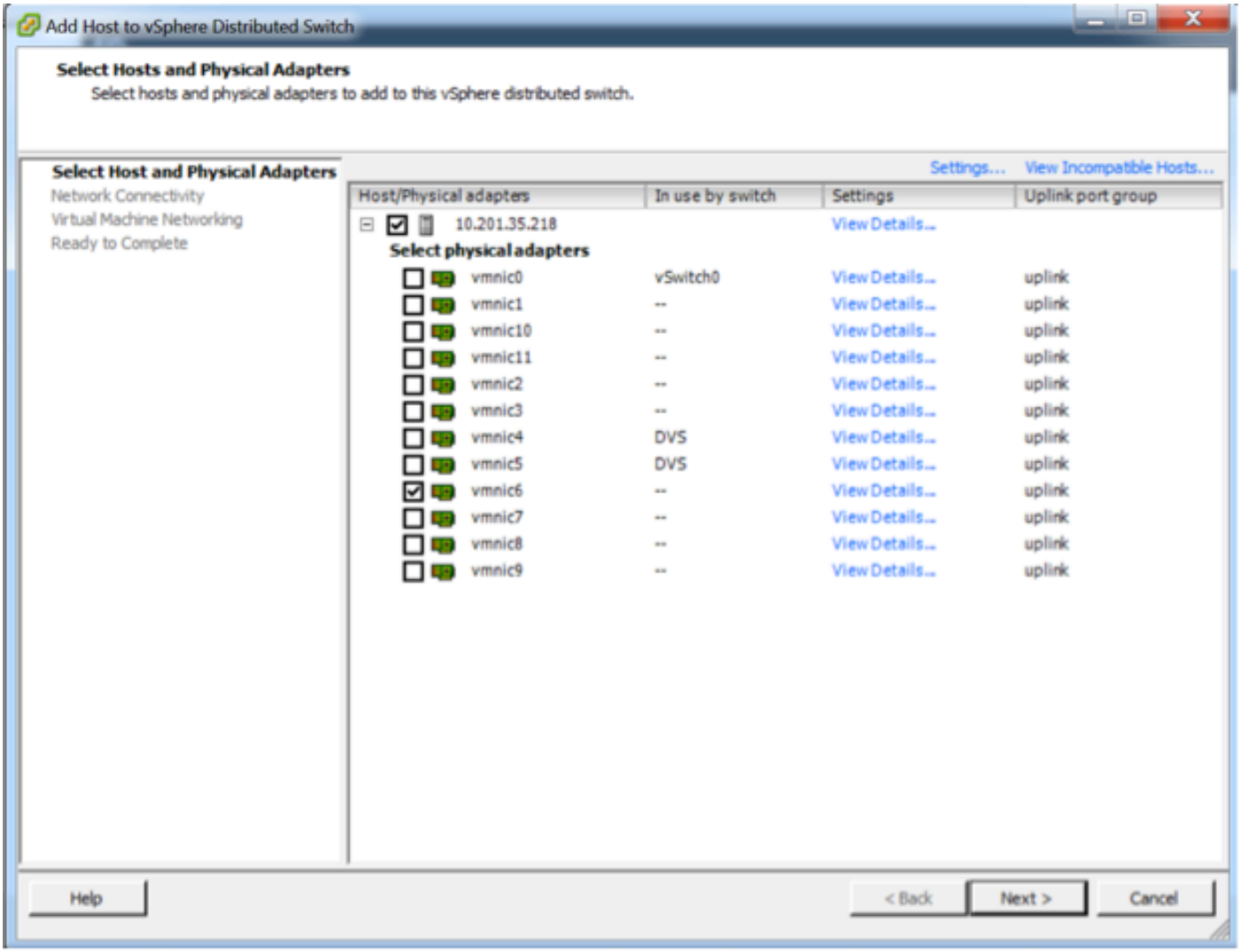
- Instale el software AVS mediante el siguiente comando en el host ESXi:

esxcli software vib install -v /vmfs/tomes/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

~ #
```

- Una vez que el módulo Ethernet virtual (VEM) esté activo, puede agregar hosts a su AVS:

En el cuadro de diálogo Add Host to vSphere Distributed Switch (Agregar host a switch distribuido de vSphere), elija los puertos NIC virtuales que están conectados al switch de hoja (en este ejemplo, sólo mueve vmnic6), como se muestra en la imagen:



- Haga clic en Next (Siguiente)
- En el cuadro de diálogo Conectividad de red, haga clic en **Siguiente**
- En el cuadro de diálogo Red de máquina virtual, haga clic en **Siguiente**
- En el cuadro de diálogo Preparado para completar, haga clic en **Finalizar**

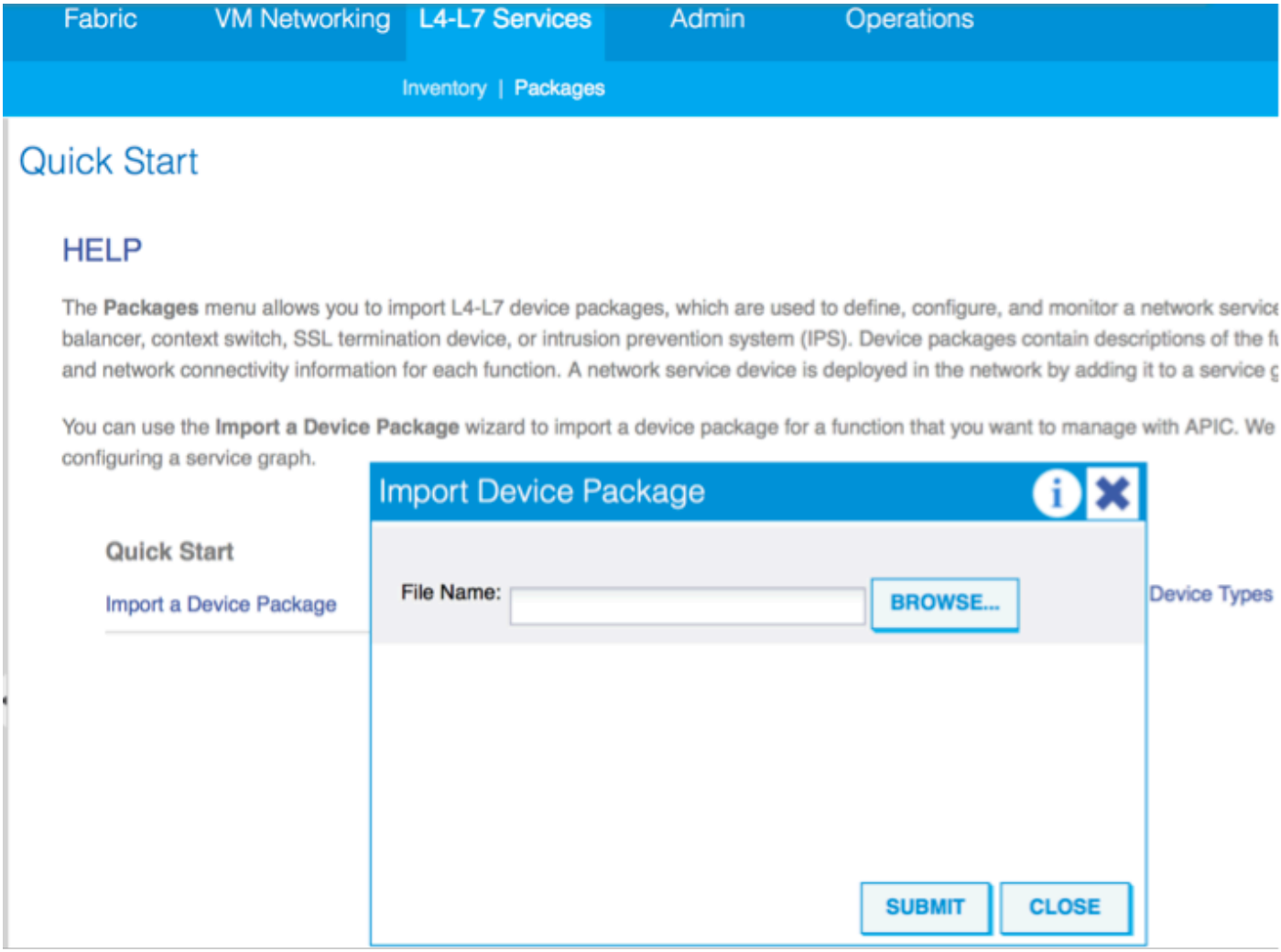
Nota: Si se utilizan varios hosts ESXi, todos ellos necesitan ejecutar AVS/VEM para que puedan administrarse desde el switch estándar a DVS o AVS.

Con esto, se ha completado la integración de AVS y estamos preparados para continuar con la implementación de ASAv L4-L7:

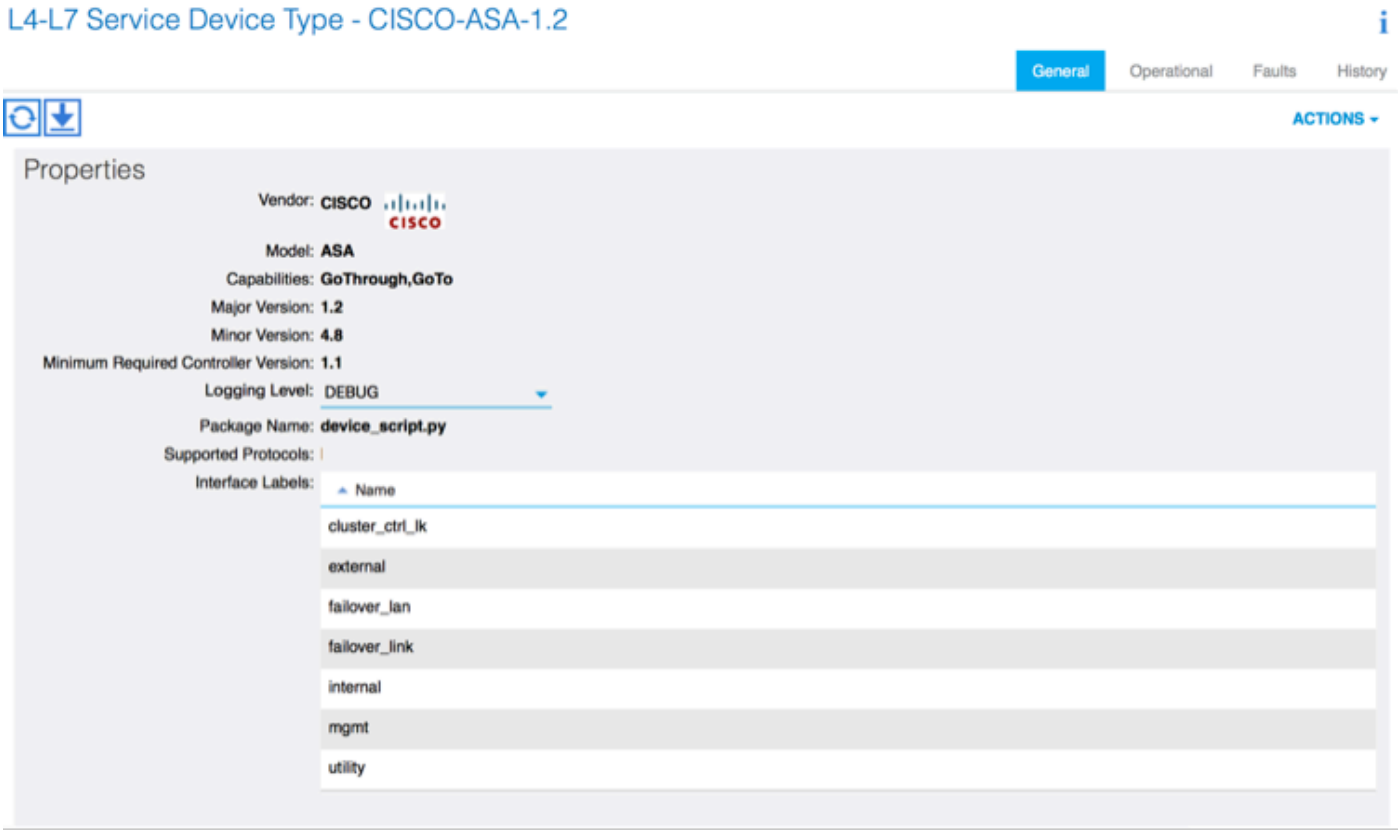
Configuración inicial de ASAv

- Descargue el paquete de dispositivos Cisco ASAv e importe en APIC:

Navegue hasta **Servicios L4-L7 > Paquetes > Importar paquete de dispositivos,** como se muestra en la imagen:



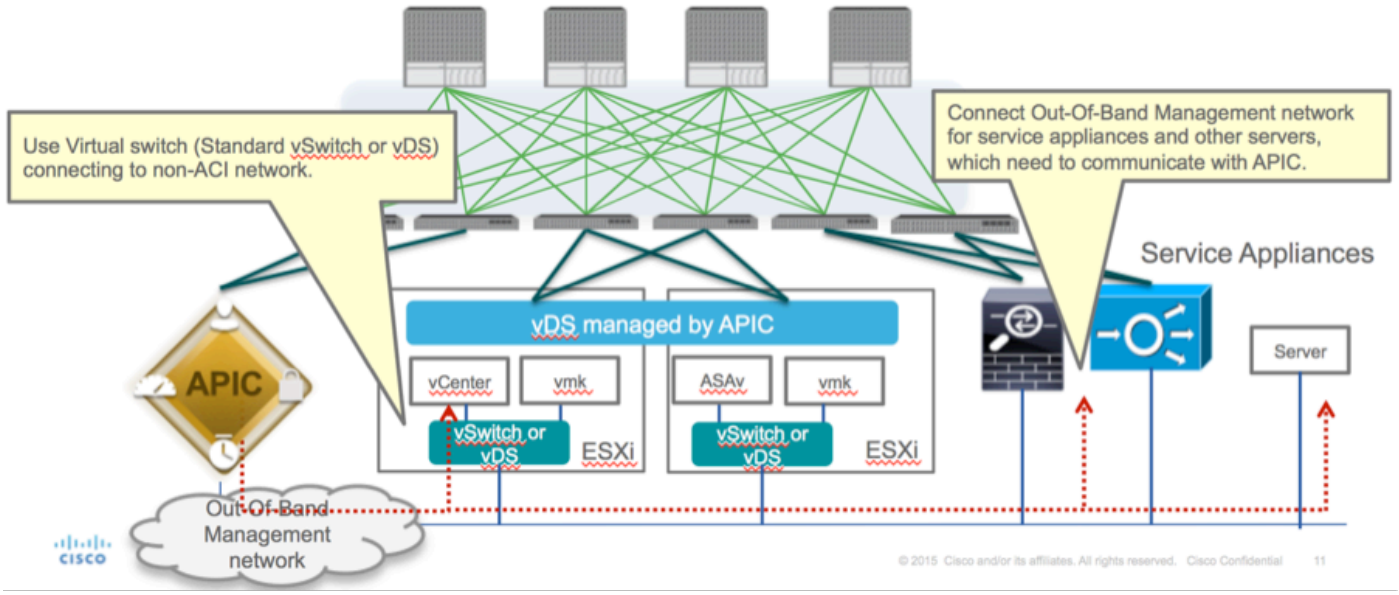
- Si todo funciona bien, puede ver el paquete de dispositivos importado expandiendo la carpeta Tipos de dispositivos de servicio L4-L7, como se muestra en la imagen:



Antes de continuar, hay algunos aspectos de la instalación que deben determinarse antes de realizar la integración L4-L7:

Existen dos tipos de redes de gestión: administración en banda y fuera de banda (OOB), que se pueden utilizar para administrar dispositivos que no forman parte de la infraestructura centrada en aplicaciones (ACI) básica (hoja, columna o controlador apic) que incluiría ASAv, equilibradores de carga, etc.

En este caso, OOB para ASAv se implementa con el uso de vSwitch estándar. Para el ASA sin software específico u otros dispositivos de servicio o servidores, conecte el puerto de administración OOB al switch OOB o a la red, como se muestra en la imagen.



La conexión de administración del puerto de administración de OOB ASAv necesita utilizar los puertos de enlace ascendente ESXi para comunicarse con APIC a través de OOB. Al mapear interfaces vNIC, el adaptador de red1 siempre coincide con la interfaz Management0/0 en ASAv, y el resto de las interfaces del plano de datos se inician desde el adaptador de red2.

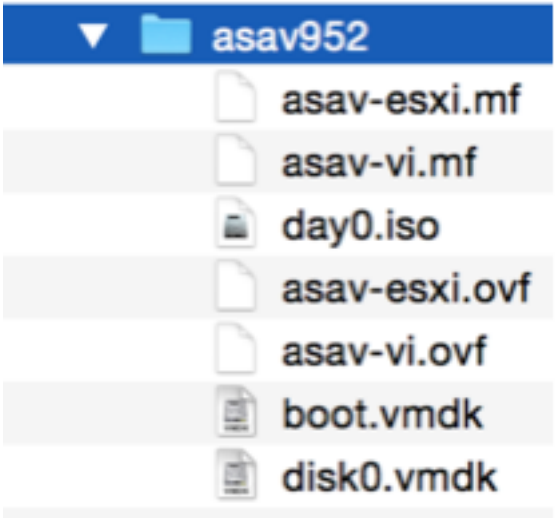
La tabla 2 muestra la concordancia de ID de adaptador de red e ID de interfaz ASAv:

Tabla 2

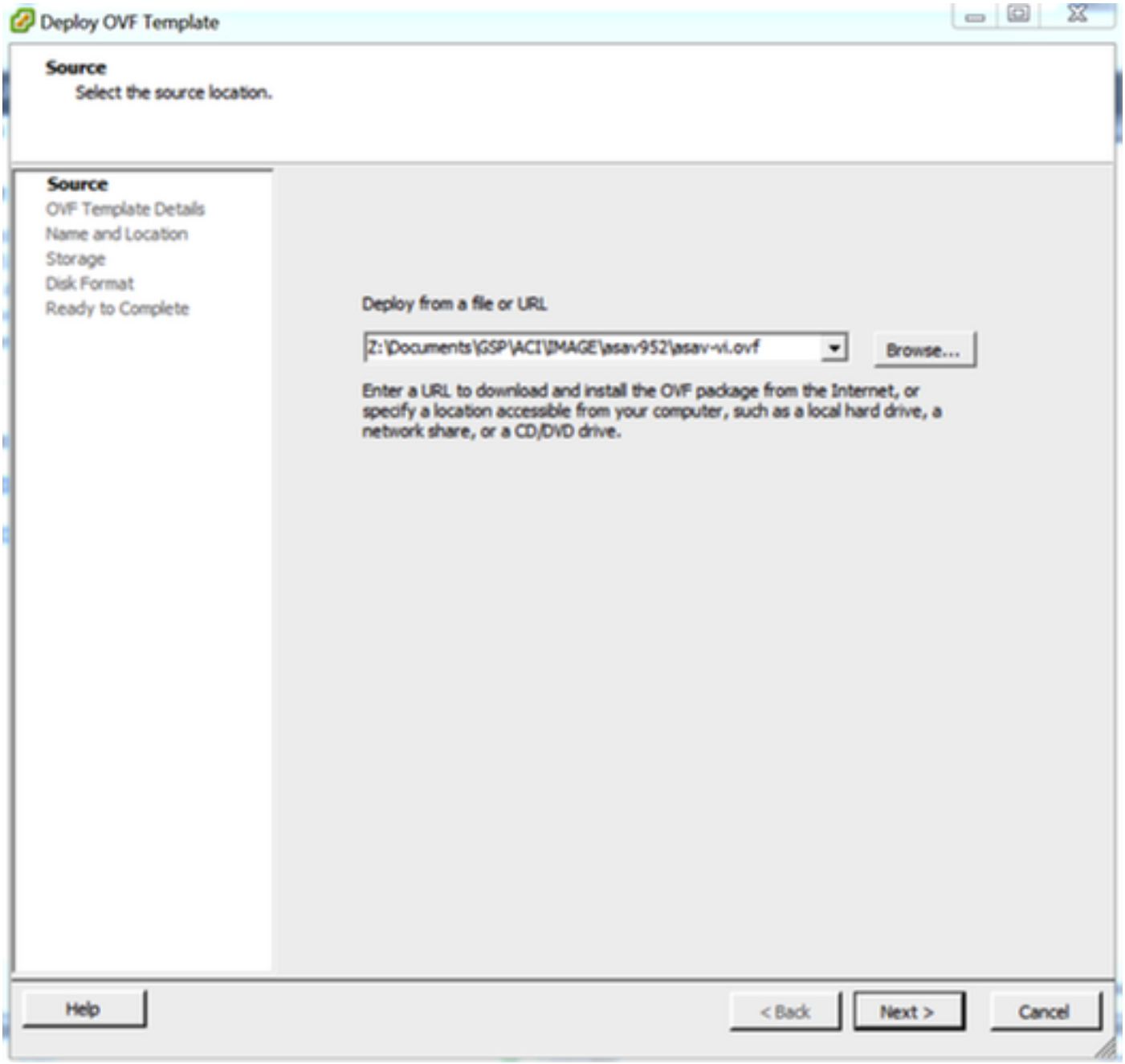
Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter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

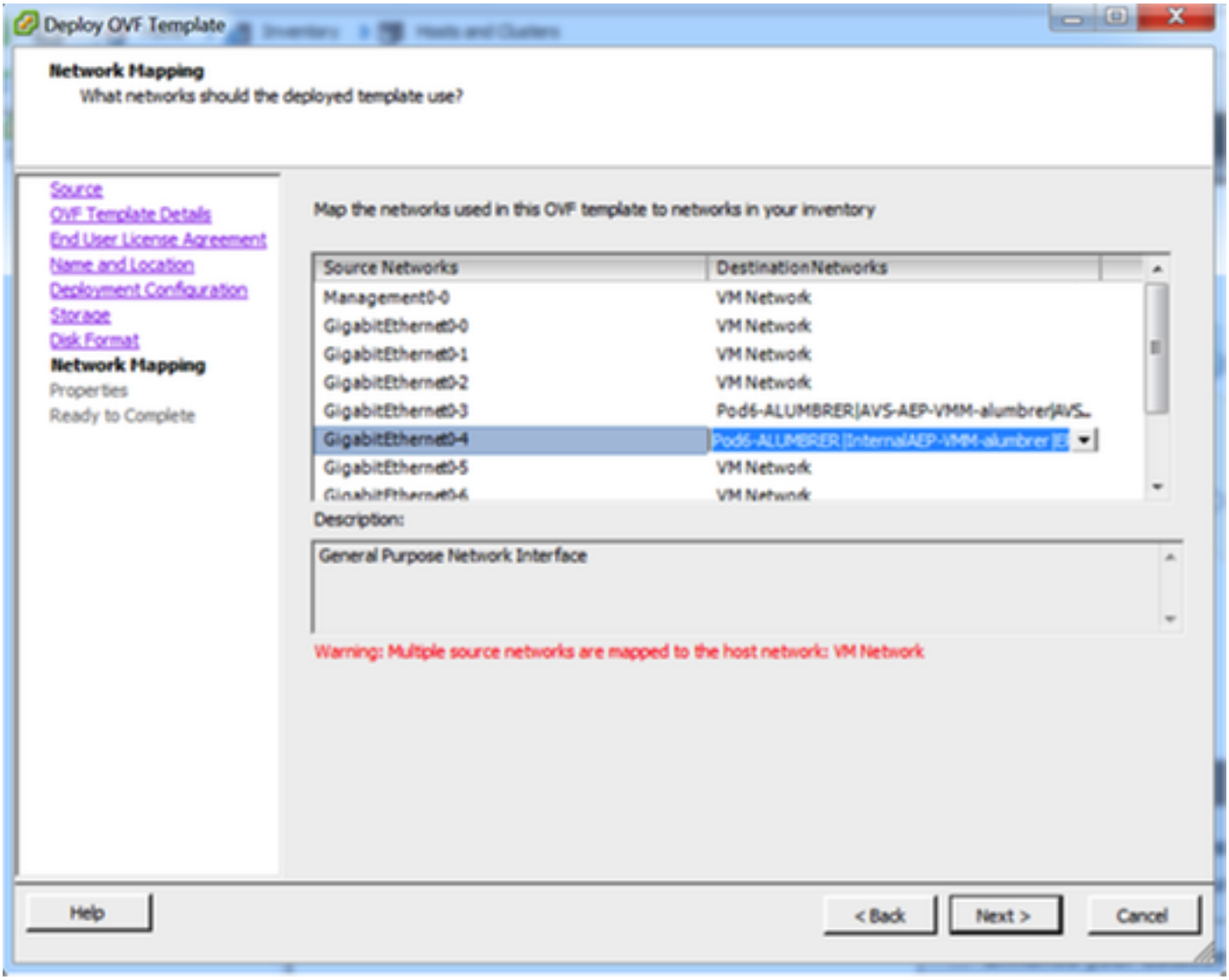
- Implemente la máquina virtual ASAv a través del asistente desde **File>Deploy OVF (Open Virtualization Format) Template**
- Seleccione **asav-esxi** si desea utilizar ESX Server independiente o **asav-vi** para vCenter. En

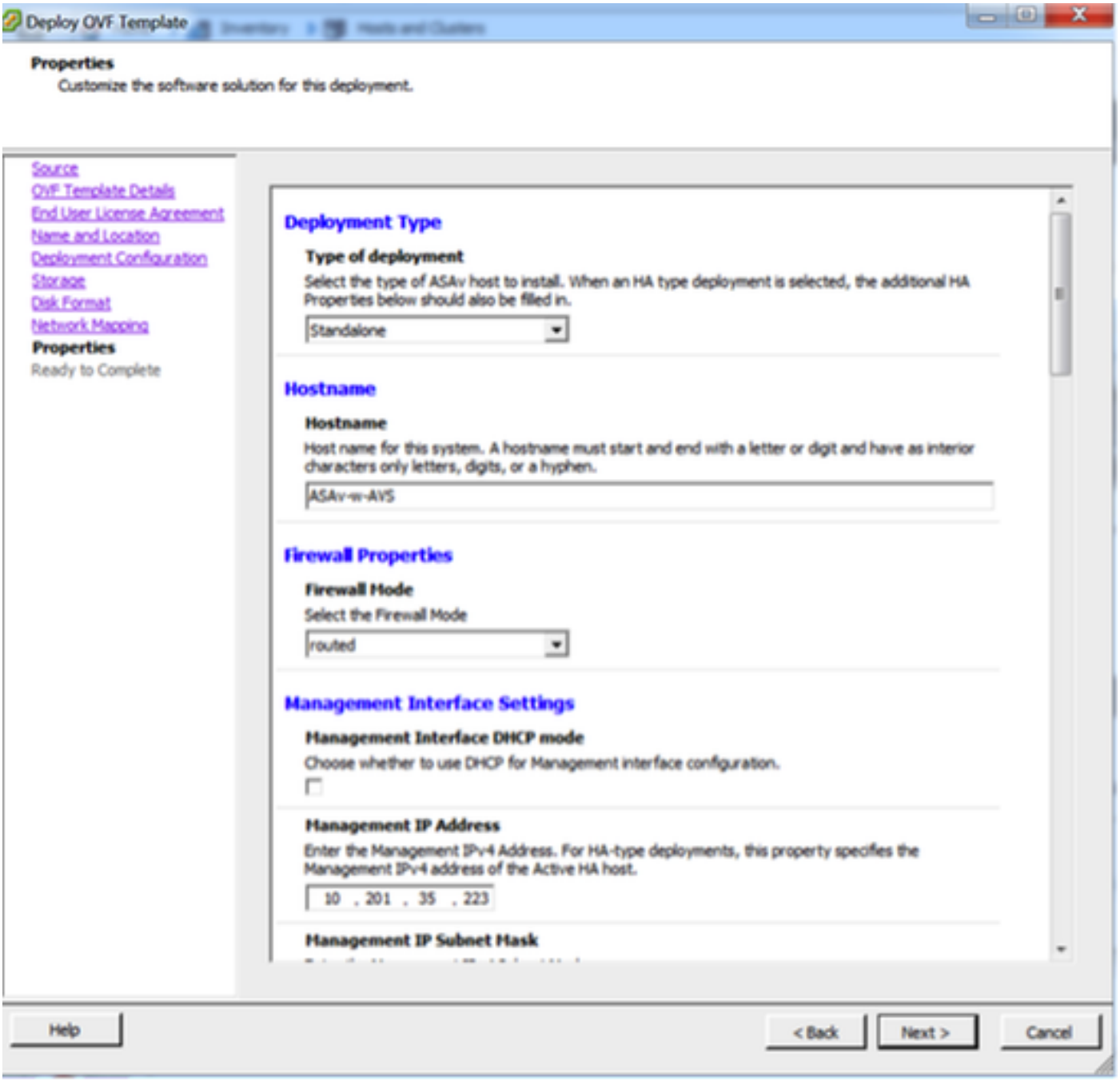
este caso, se utiliza vCenter.

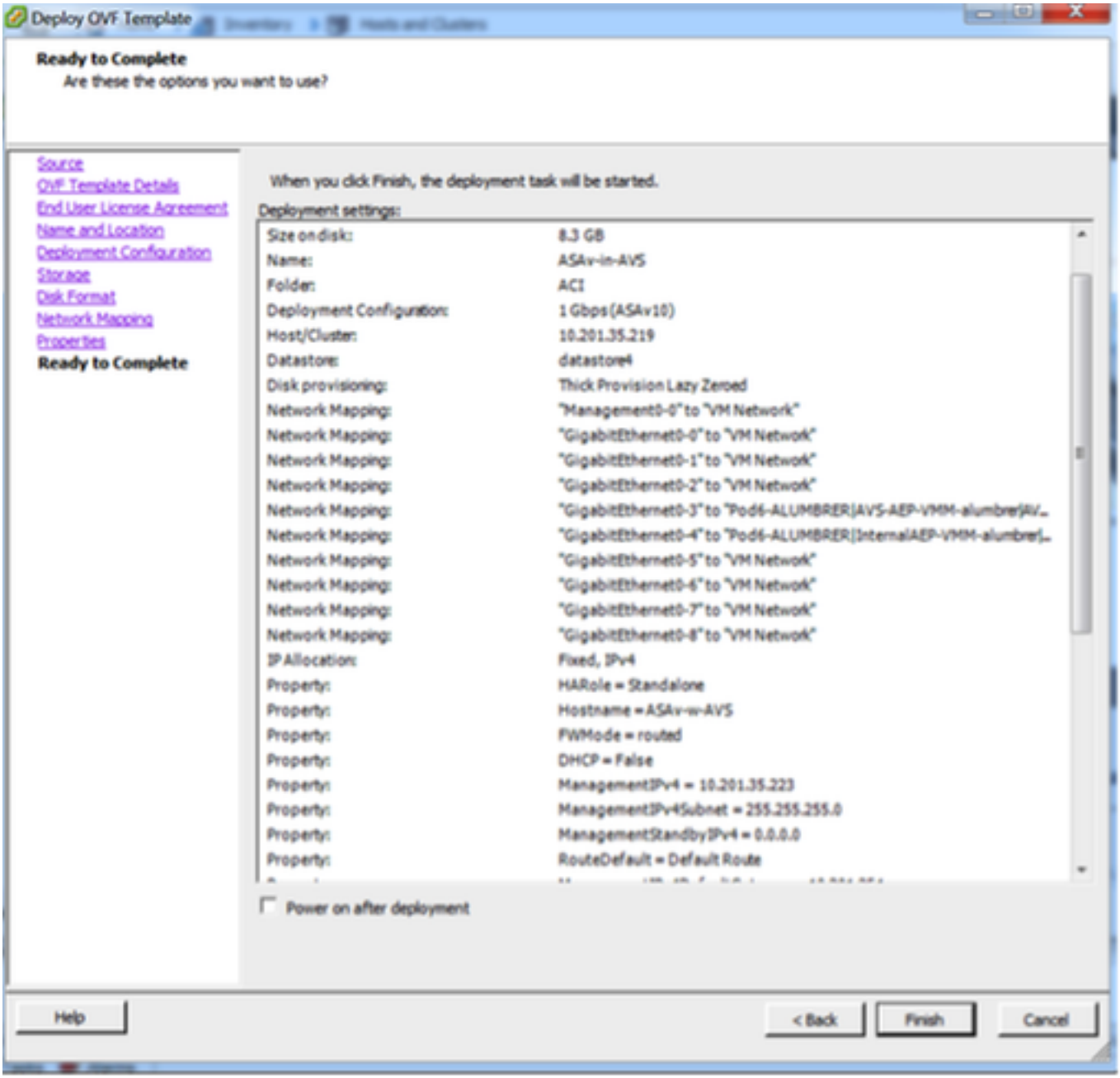


- Vaya al asistente de instalación, acepte términos y condiciones. En medio del asistente puede determinar varias opciones, como nombre de host, administración, dirección ip, modo de firewall y otra información específica relacionada con ASAv. Recuerde utilizar la administración OOB para ASAv, como en este caso, debe mantener la interfaz Management0/0 mientras utiliza la red VM (switch estándar) y la interfaz GigabitEthernet0-8 son los puertos de red predeterminados.

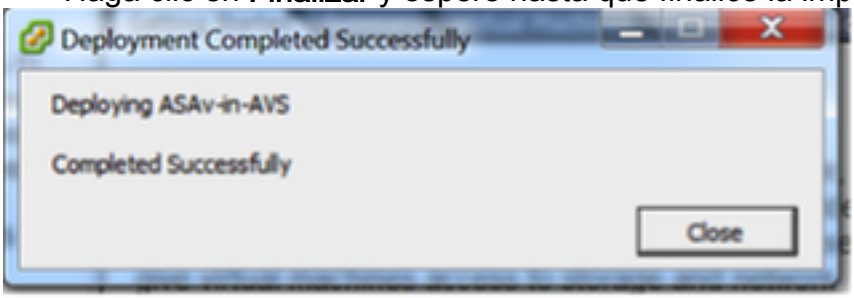

Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete
Deploy from a file or URL
Z:\Documents\GSP\ACI\IMAGE\asav952\asav-vi.ovf
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help
< Back
Next >
Cancel


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



- Haga clic en **Finalizar** y espere hasta que finalice la implementación de ASAv



- Encienda su máquina virtual ASAv e inicie sesión a través de la consola para verificar la configuración inicial

```
!
interface Management0/0
 management-only
 nameif management
 security-level 0
 ip address 10.201.35.223 255.255.255.0
!
ftp mode passive
pager lines 23
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route management 0.0.0.0 0.0.0.0 10.201.35.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
<--- More --->_
```

- Como se muestra en la imagen, ya se ha enviado parte de la configuración de administración al firewall ASAv. Configure el nombre de usuario y la contraseña del administrador. El APIC utiliza este nombre de usuario y contraseña para iniciar sesión y configurar el ASA. El ASA debe tener conectividad con la red OOB y debe poder alcanzar el APIC.

nombre de usuario admin password <device_password> privilegio cifrado 15

```
ASAv-w-AVS(config)# username admin password C1sc0123 privilege  15
ASAv-w-AVS(config)# wr mem
Building configuration...
Cryptochecksum: d491b980 86fa522f 6f937baf b5bfb318

7977 bytes copied in 0.250 secs
[OK]
ASAv-w-AVS(config)# ping 10.201.35.211
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.201.35.211, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASAv-w-AVS(config)# _
```

Además, desde el modo de configuración global, habilite el servidor http:

http server enable

http 0.0.0.0 0.0.0.0

L4-L7 para la integración de ASAv en APIC:

- Inicie sesión en la GUI de ACI, haga clic en el arrendatario en el que se implementará el gráfico de servicios. Expanda los servicios L4-L7 en la parte inferior del panel de navegación y haga clic con el botón derecho en **Dispositivos L4-L7** y haga clic en **Crear dispositivos L4-L7** para abrir el asistente

- Para esta implementación, se aplicarán las siguientes configuraciones:
  -Modo administrado

  -Servicio de firewall

  -Dispositivo virtual

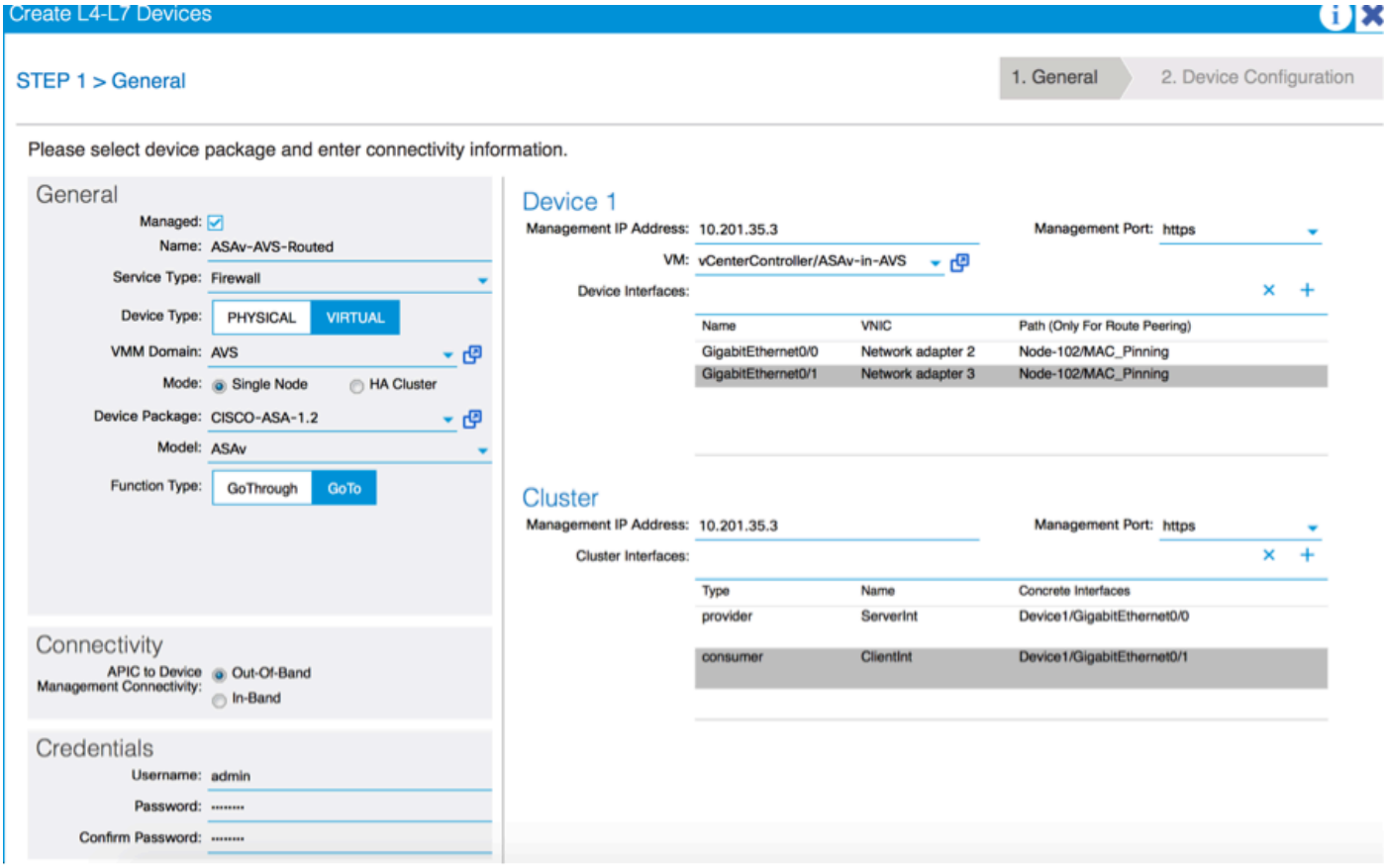
  -Conectado al dominio AVS con un solo nodo

  -Modelo ASAv

  -Modo enrutado (GoTo)

  -Dirección de administración (debe coincidir con la dirección asignada anteriormente a la interfaz Mgmt0/0)

- Utilice HTTPS como APIC de forma predeterminada utiliza el protocolo más seguro para comunicarse con ASAv



- La definición correcta de las interfaces de dispositivo y de las interfaces de clúster es fundamental para una implementación correcta

Para la primera parte, utilice la tabla 2 mostrada en la sección anterior para hacer coincidir correctamente los ID de adaptador de red con los ID de interfaz ASAv que desea utilizar. La ruta hace referencia al puerto físico, al canal de puerto o al VPC que habilita la entrada y salida de las interfaces de firewall. En este caso, ASA se encuentra en un host ESX, donde el ingreso y la salida son los mismos para ambas interfaces. En un dispositivo físico, el interior y el exterior del firewall (FW) serían puertos físicos diferentes.

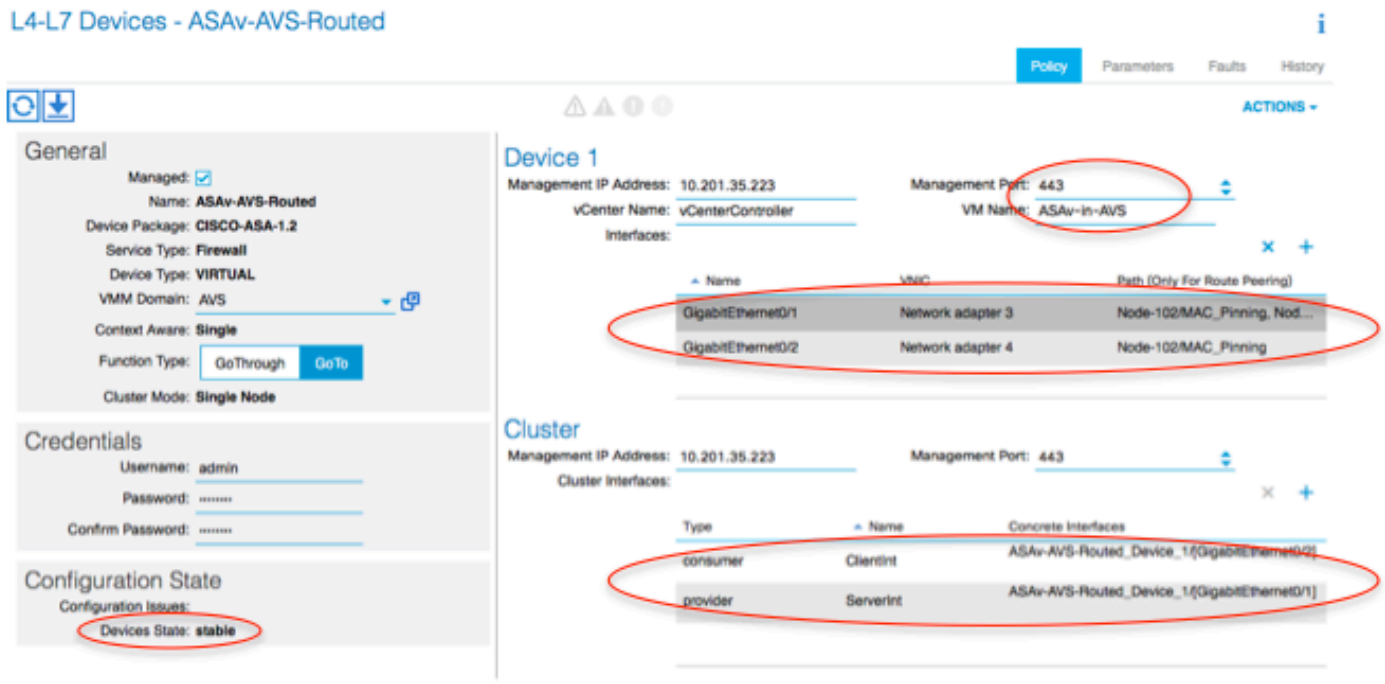
Para la segunda parte, las interfaces de clúster deben definirse siempre sin excepciones (incluso

si no se utiliza Cluster HA), esto se debe a que el modelo de objetos tiene una asociación entre la interfaz **mIf** (metainterfaz en el paquete de dispositivos), la interfaz **LIf** (interfaz hoja como, por ejemplo, externa, interna, interna, interna, etc.) y la **CIf** (interfaz de hormigemento). Los dispositivos concretos L4-L7 deben configurarse en una configuración de clúster de dispositivos y esta abstracción se denomina dispositivo lógico. El dispositivo lógico tiene interfaces lógicas asignadas a interfaces concretas en el dispositivo concreto.

Para este ejemplo, se utilizará la asociación siguiente:

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

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

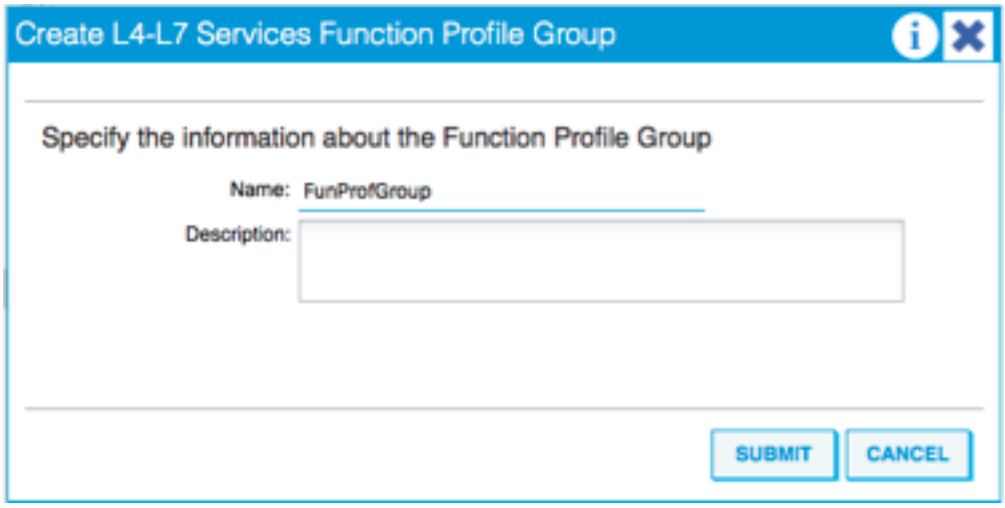


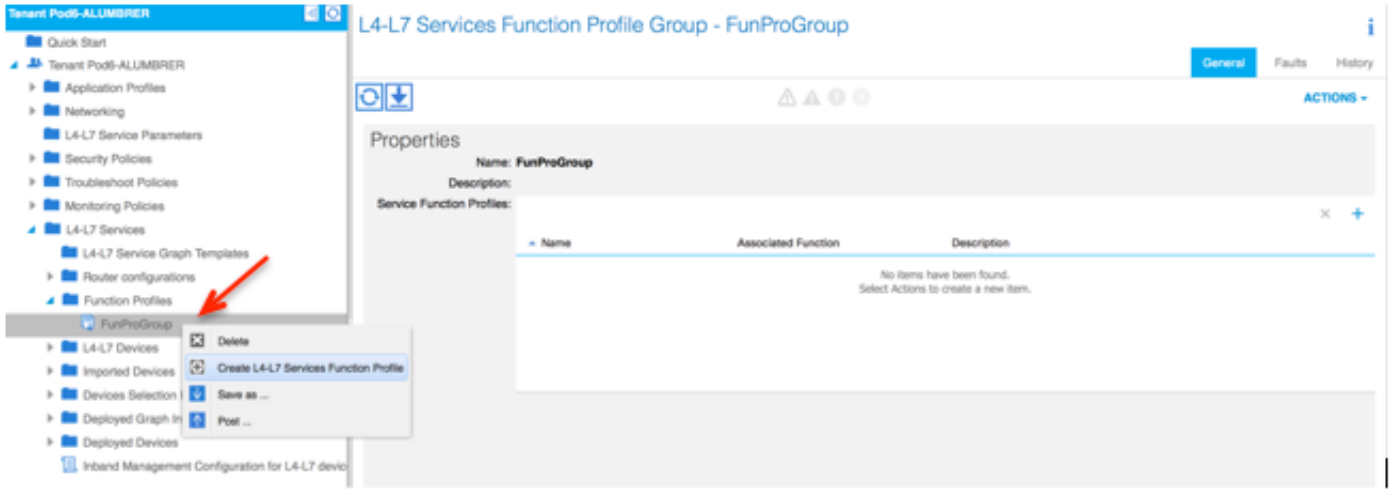
> **Nota:** Para implementaciones de failover/HA, GigabitEthernet 0/8 está preconfigurado como interfaz de failover.

El estado del dispositivo debe ser Estable y debe estar preparado para implementar el perfil de función y la plantilla de gráfico de servicios

Templo de gráfico de servicio

En primer lugar, cree un perfil de función para ASAv, pero antes de eso debe crear un grupo de perfiles de función y, a continuación, un perfil de función de servicios L4-L7 debajo de esa carpeta, como se muestra en la imagen:

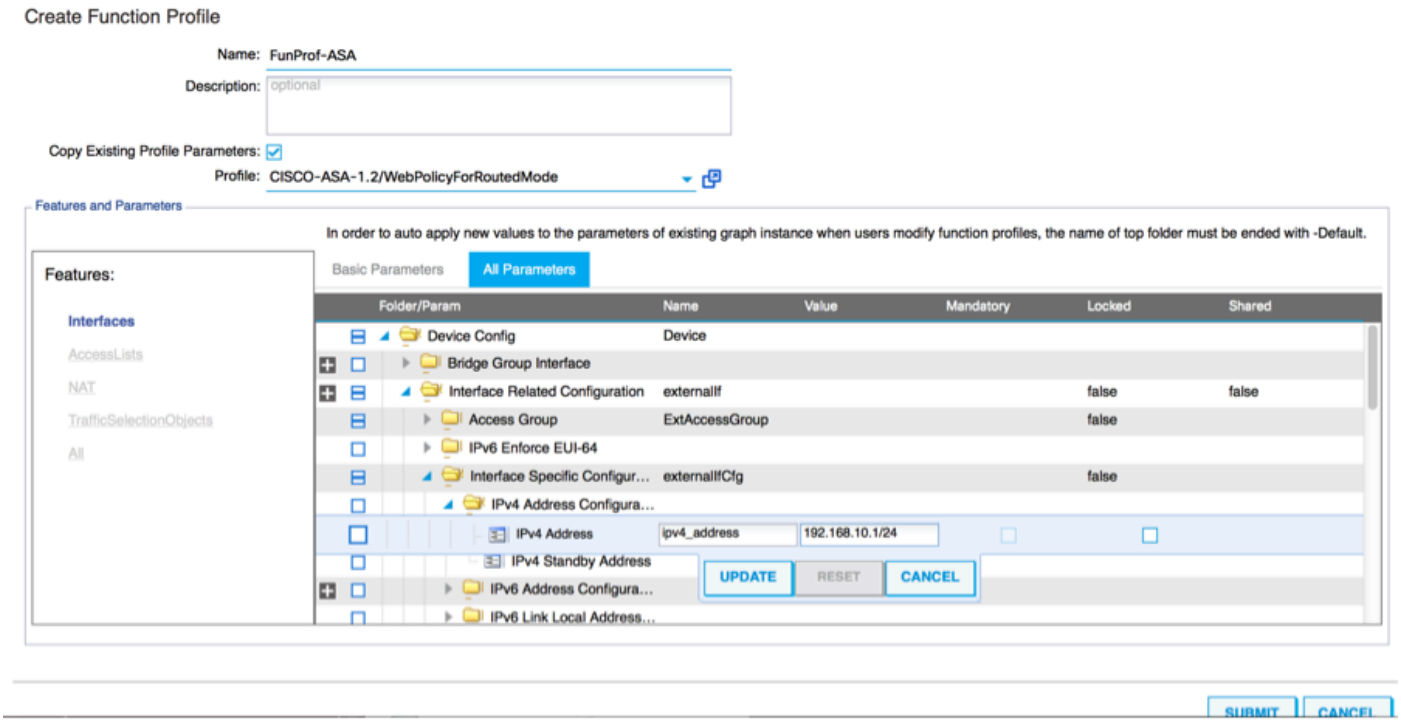




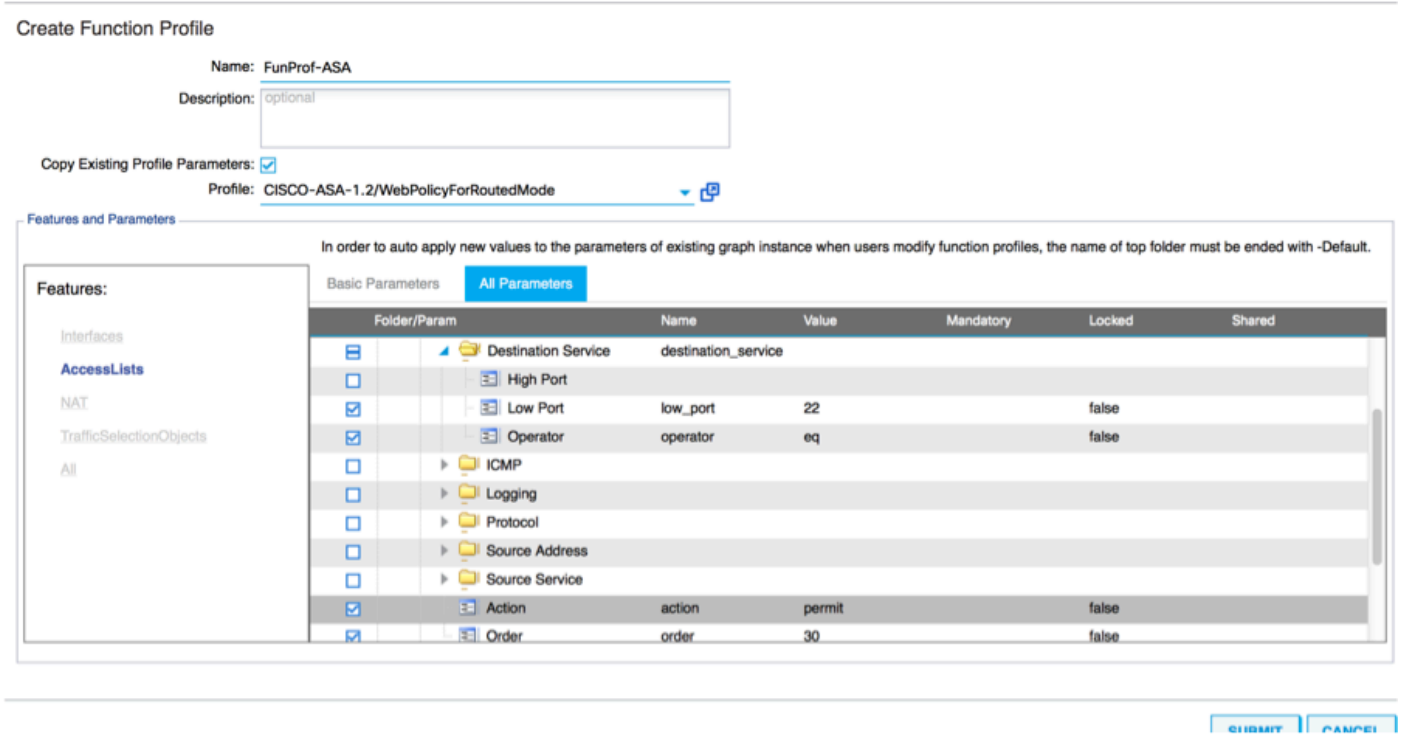
- Seleccione el perfil **WebPolicyForRoutedMode** en el menú desplegable y proceda a configurar las interfaces en el firewall. A partir de aquí, los pasos son opcionales y se pueden implementar/modificar más adelante. Estos pasos se pueden realizar en varias etapas diferentes de la implementación en función de la reutilización o personalización del Gráfico de servicios.

Para este ejercicio, un firewall enrutado (modo GoTo) requiere que cada interfaz tenga una dirección IP única. La configuración estándar de ASA también tiene un nivel de seguridad de la interfaz (la interfaz externa es menos segura, la interfaz interna es más segura). También puede cambiar el nombre de la interfaz según sus requisitos. Los valores predeterminados se utilizan en este ejemplo.

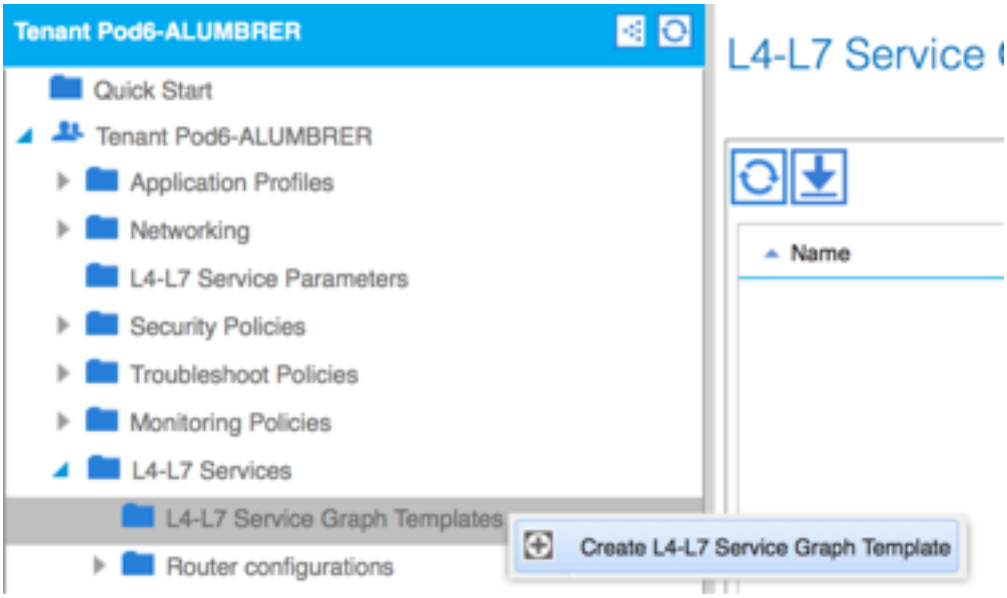
- Expanda Interface Specific Configuration, agregue la dirección IP y el nivel de seguridad para ServerInt con el siguiente formato para la dirección IP **x.x.x.x/y.y.y.y o x.x.x.x/yy**. Repita el proceso para la interfaz ClientInt.



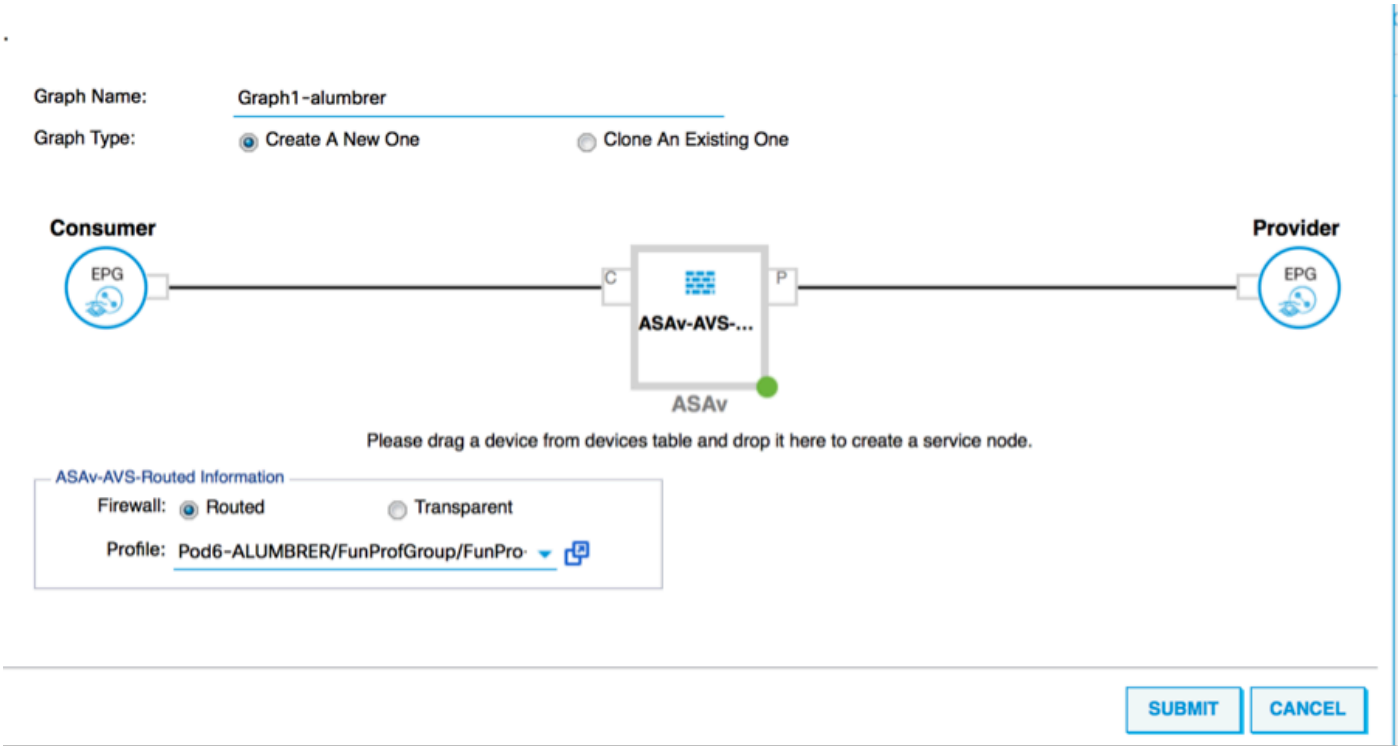
Nota: También puede modificar la configuración predeterminada de la lista de acceso y crear su propia plantilla base. De forma predeterminada, la plantilla RoutedMode incluirá reglas para HTTP y HTTPS. Para este ejercicio, SSH e ICMP se agregarán a la lista de acceso externa permitida.



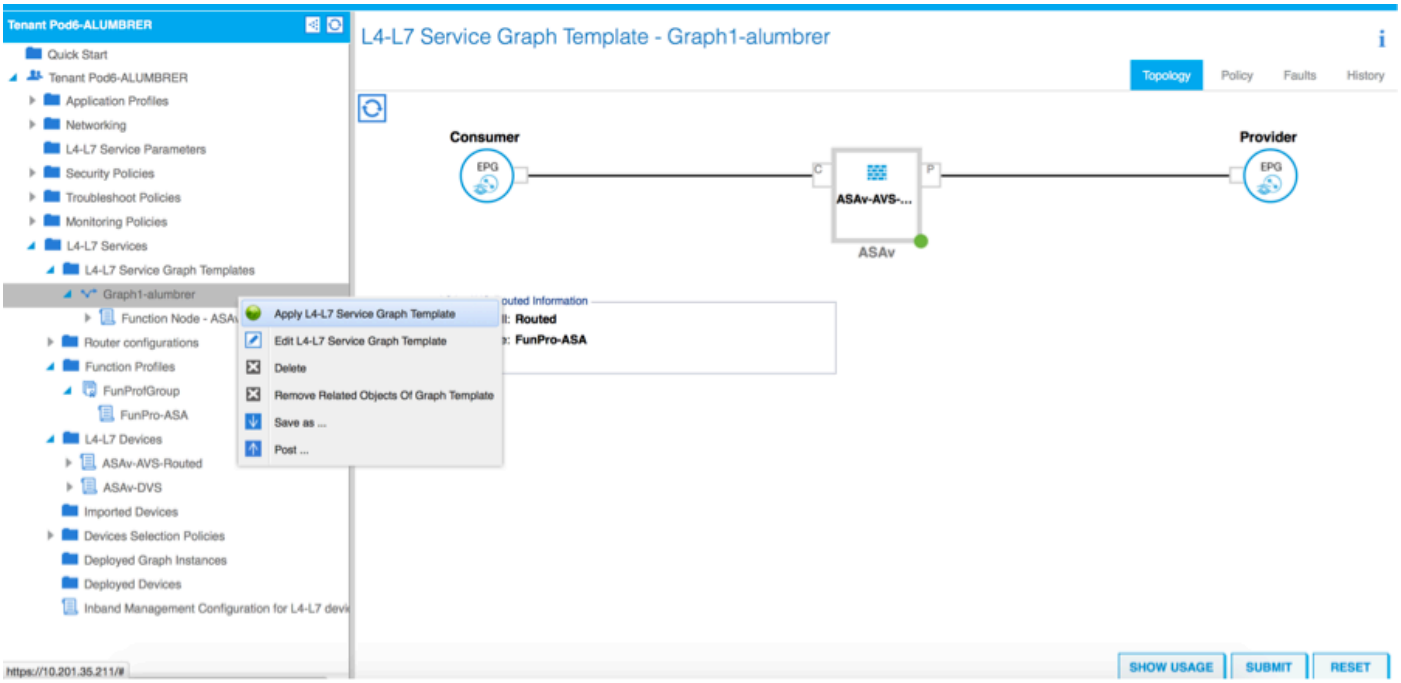
- A continuación, haga clic en **Enviar**
- Ahora, cree la plantilla de gráficos de servicios



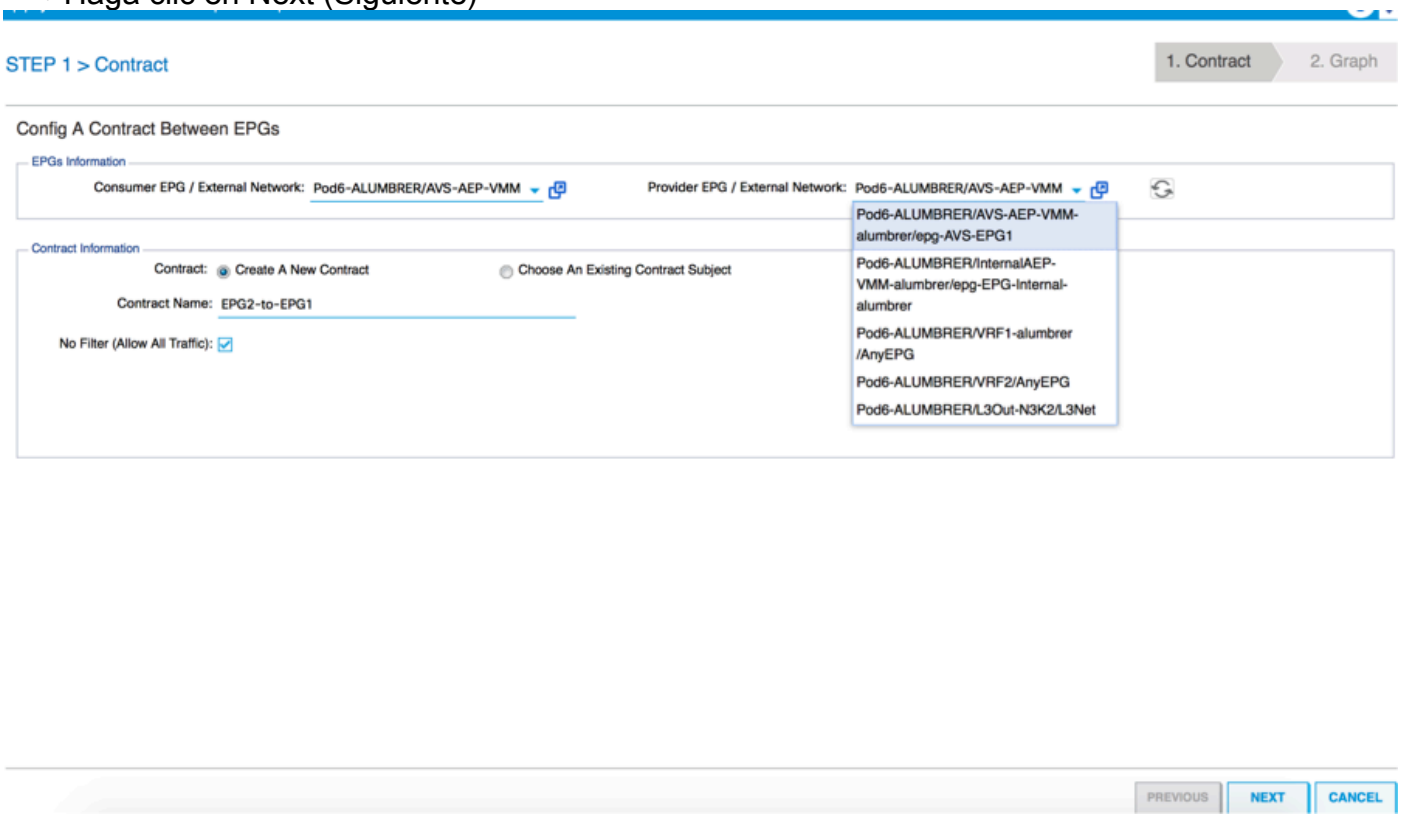
- Arrastre y suelte el clúster de dispositivos a la derecha para formar la relación entre consumidor y proveedor, seleccione Modo enrutado y el perfil de función creado anteriormente.



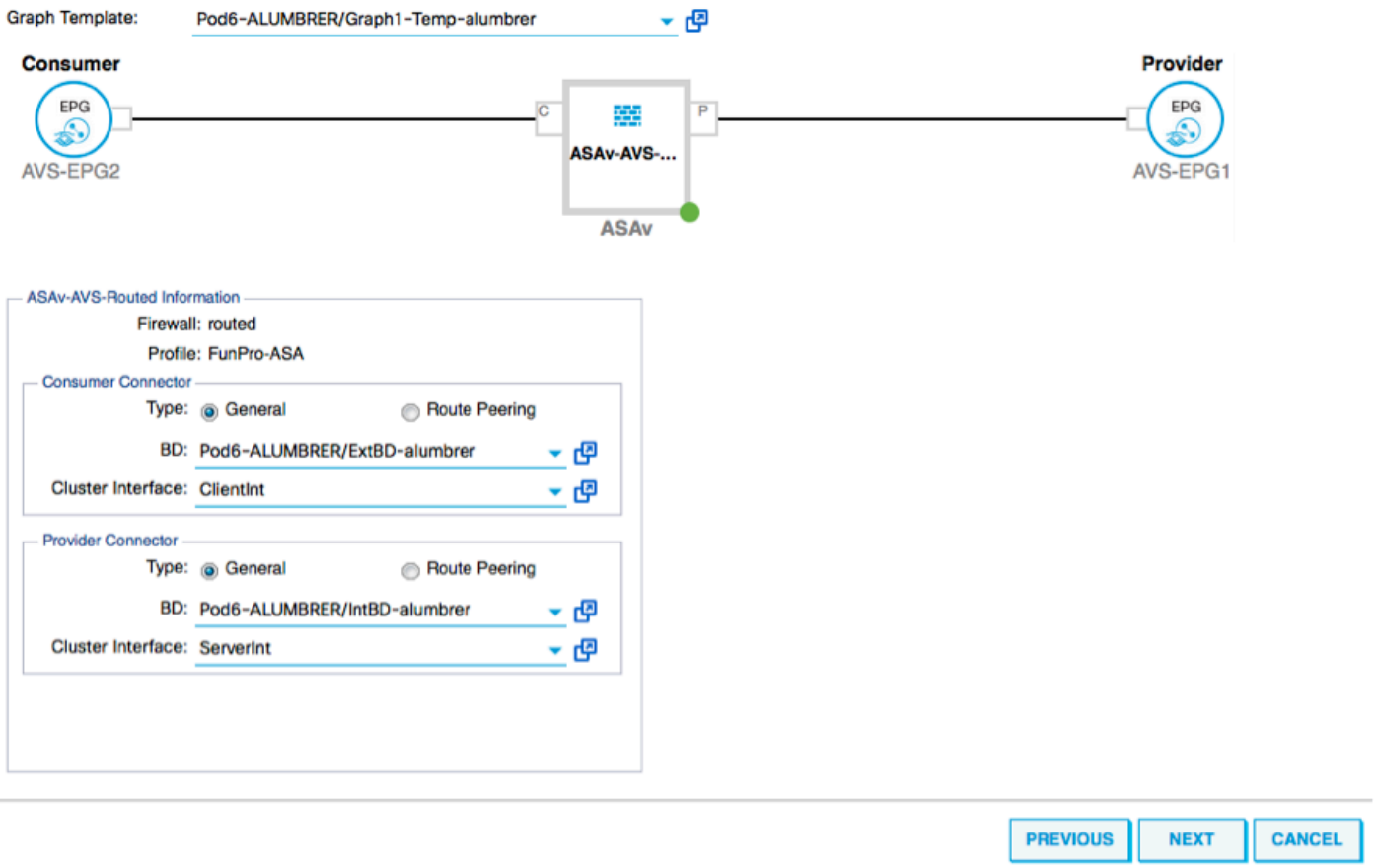
- Verifique la plantilla para ver si hay fallos. Las plantillas se crean para reutilizables, y después se deben aplicar a EPG particulares, etc.
- Para aplicar una plantilla, haga clic con el botón derecho del ratón y seleccione Aplicar plantilla de gráficos de servicios L4-L7



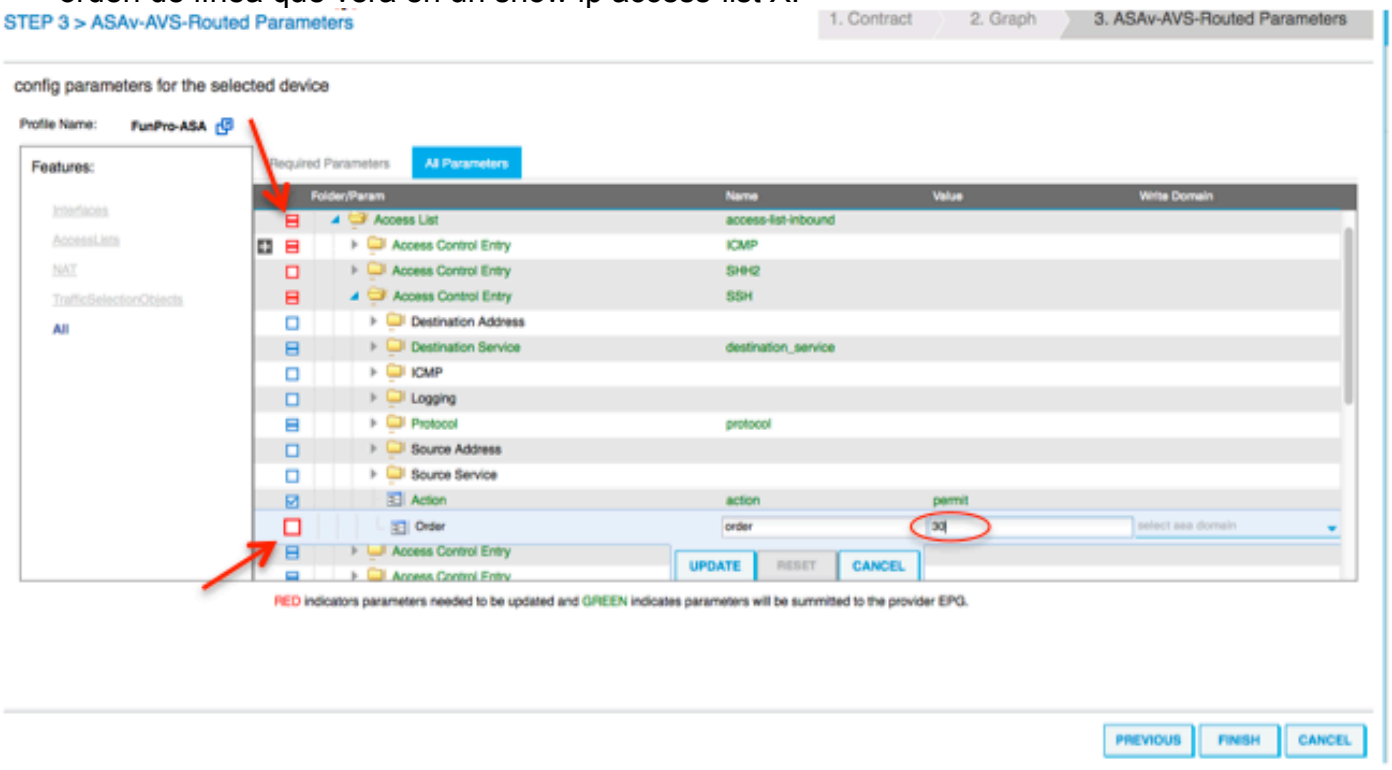
- Defina qué EPG estará en el lado del consumidor y del proveedor. En este ejercicio, AVS-EPG2 es el consumidor (cliente) y AVS-EPG1 es el proveedor (servidor). Recuerde que no se aplica ningún filtro, esto permitirá que el firewall realice todo el filtrado basado en la lista de acceso definida en la última sección de este asistente.
- Haga clic en Next (Siguiente)



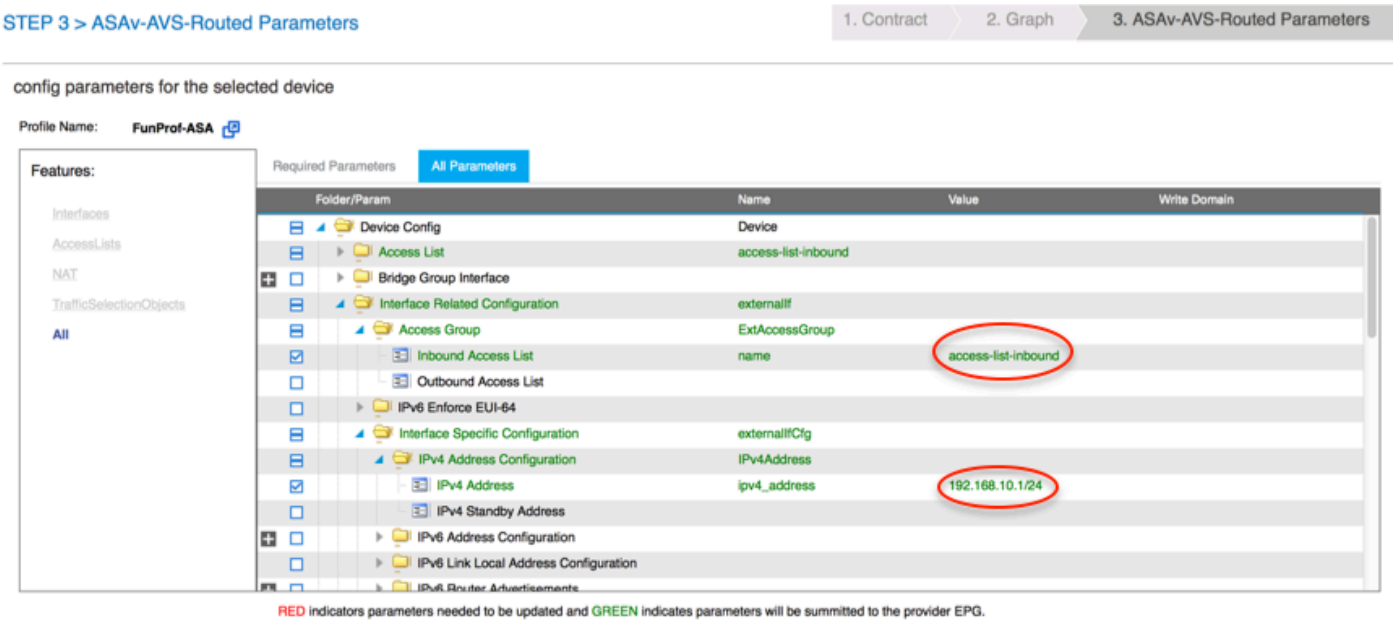
- Verifique la información de BD para cada uno de los EPG. En este caso, EPG1 es el proveedor en la base de datos IntBD y EPG2 es el consumidor en BD ExtBD. EPG1 se conectará en la interfaz de firewall ServerInt y EPG2 se conectará en la interfaz ClientInt. Ambas interfaces FW se convertirán en la DG para cada uno de los EPG, por lo que el tráfico se verá obligado a cruzar el firewall en todo momento.
- Haga clic en Next (Siguiente)



- En la sección Config Parameters, haga clic en **All Parameters** y verifique si hay indicadores RED que necesitan actualizarse/configurarse. En el resultado, como se muestra en la imagen, se puede observar que se ha perdido el orden en la lista de acceso. Esto equivale al orden de línea que verá en un show ip access-list X.



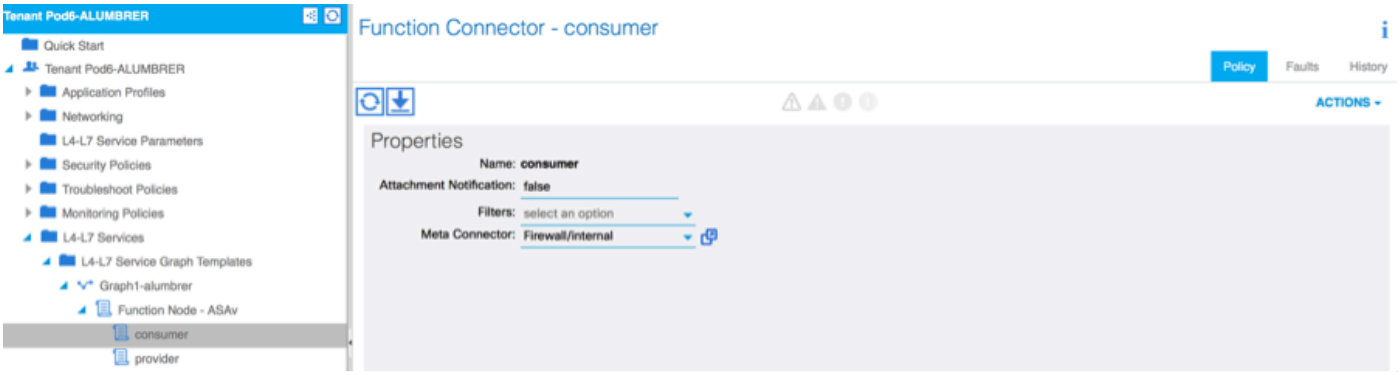
- También puede verificar el direccionamiento IP asignado desde el perfil de función definido anteriormente. Hay una buena oportunidad de cambiar la información si es necesario. Una vez configurados todos los parámetros, haga clic en **Finalizar**, como se muestra en la imagen:



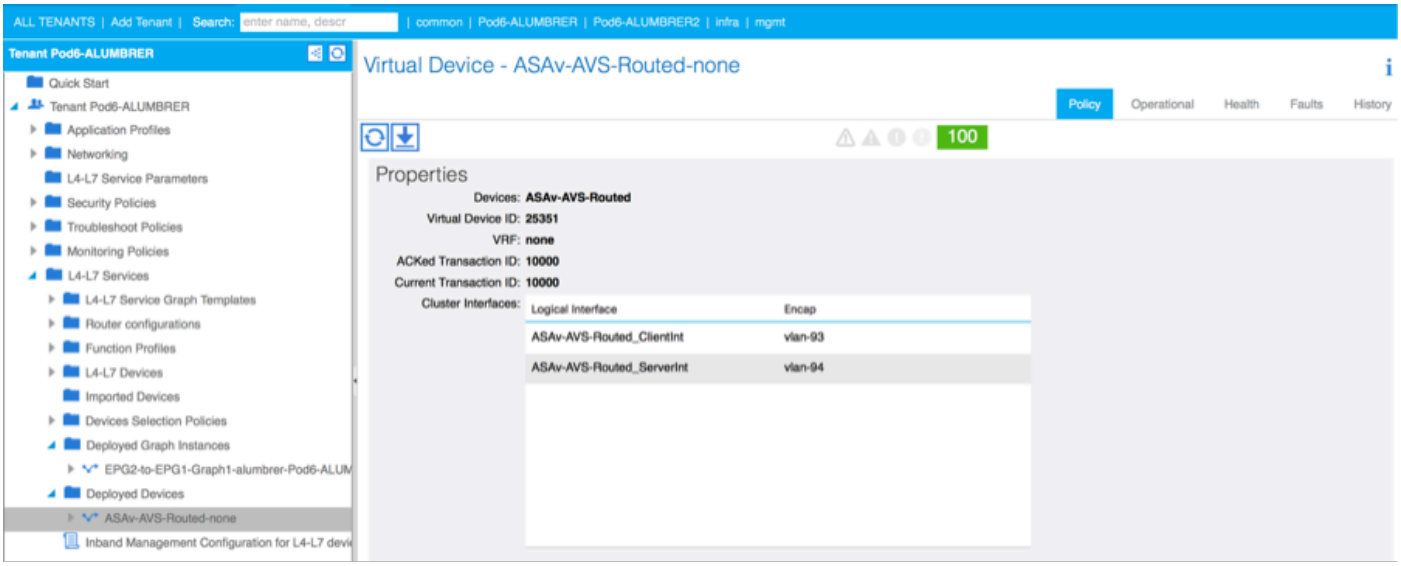
- Si todo va bien, debería aparecer un nuevo dispositivo implementado e instancia de gráfico.

Verificación

- Una cosa importante para verificar después de crear el gráfico de servicios es que la relación consumidor/proveedor se creó con el Meta Connector adecuado. Verifique bajo Propiedades del Conector de Función.



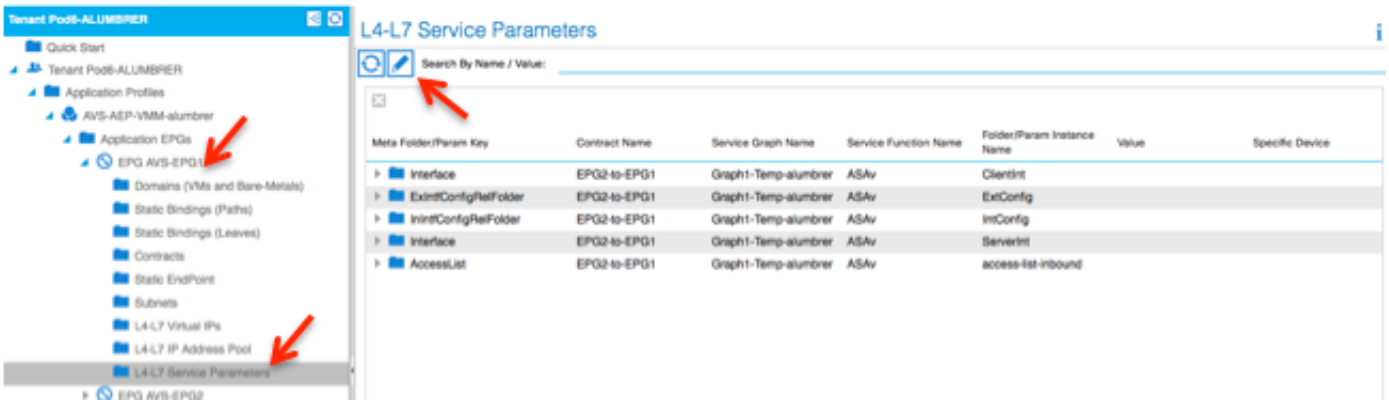
Nota: Cada interfaz del firewall se asignará con una vlan encap del grupo dinámico AVS. Verifique que no haya fallas.



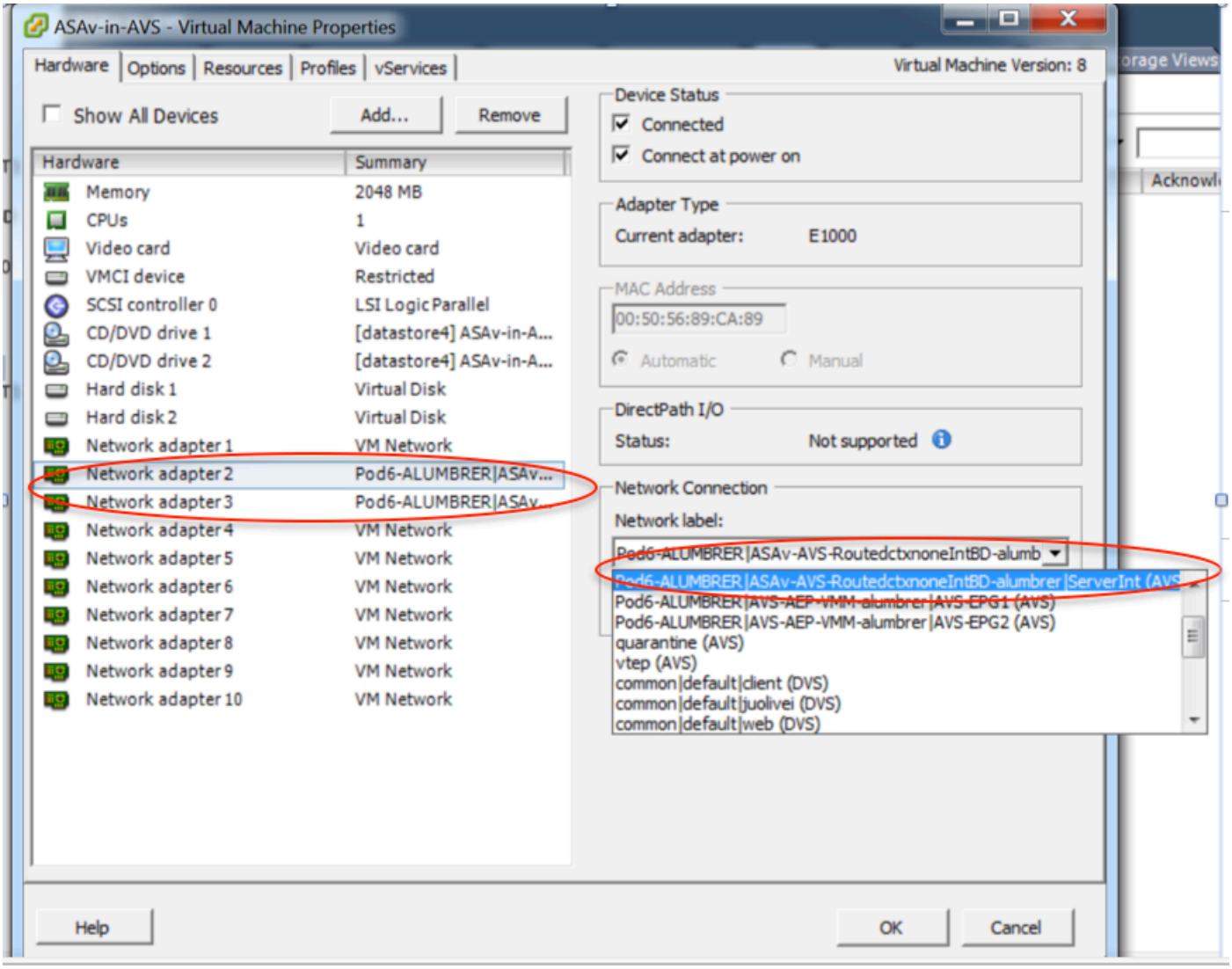
- Ahora, también puede verificar la información enviada al ASAv

```
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#
```

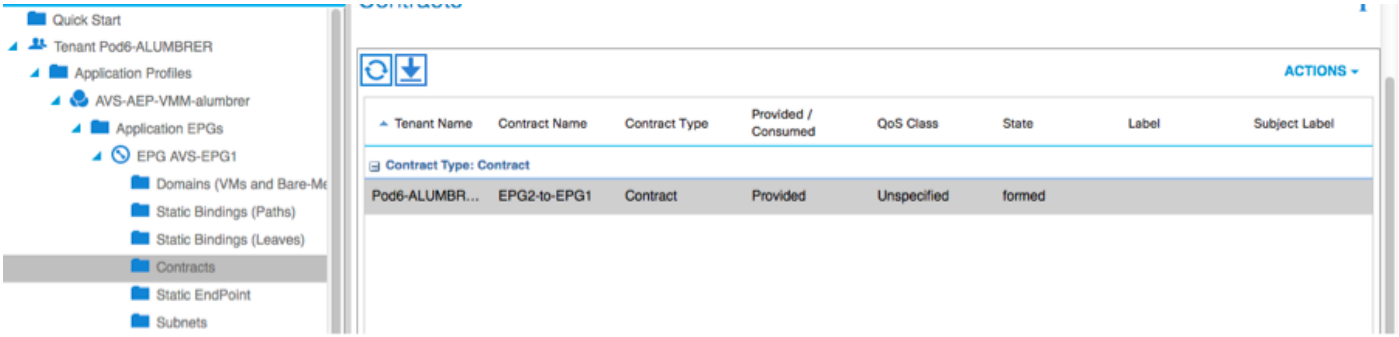
- Se asigna un nuevo contrato en los EPG. A partir de ahora, si necesita modificar algo de la lista de acceso, el cambio debe hacerse a partir de los parámetros de servicio L4-L7 de la EPG del proveedor.



- En vCenter, también puede verificar que los EPG de la sombra estén asignados a cada una de las interfaces FW:



Para esta prueba, tuve los 2 EPG comunicándose con los contratos estándar, estos 2 EPG están en diferentes dominios y VRF diferentes, por lo que la fuga de ruta entre ellos se configuró previamente. Esto simplifica un poco después de insertar el Gráfico de servicios, ya que el firewall configura el enrutamiento y el filtrado entre los 2 EPG. La DG configurada anteriormente en el EPG y el BD ahora puede eliminarse del mismo modo que los contratos. Sólo el contrato impulsado por la L4-L7 debe permanecer bajo los EPG.



A medida que se elimina el contrato estándar, puede confirmar que el tráfico ahora fluye a través de ASAv, el comando show access-list debería mostrar el recuento de aciertos para la regla que aumenta cada vez que el cliente envía una solicitud al servidor.

```
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# _
```

En la hoja, se deben aprender los terminales para las VM de cliente y servidor, así como para las interfaces ASAv

```
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                                     vlan-98     0050.5689.fa08 L                      eth1/7
Pod6-ALUMBRER:VRF1-alumbrer      Server IP         vlan-98   192.168.10.10 L
25                               & MAC             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               Client IP &       vlan-97     172.16.1.10 L
26                               MAC               vlan-93     0050.5689.e7dd L                      po4
Pod6-ALUMBRER:VRF2                                 vlan-93       172.16.1.1 L
overlay-1                                                      10.0.104.93
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
```

FW interface (ServerInt)

FW interface (ClientInt)

vea ambas interfaces de firewall conectadas al VEM.

ESX-1

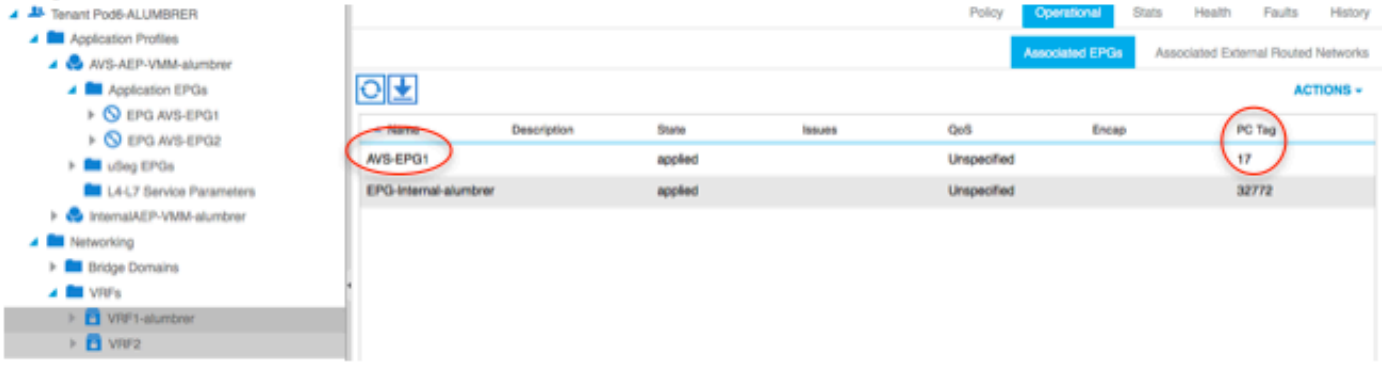
```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State    Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   22     Eth1/5     UP   UP    FWD        -    1040     4    0        0                vmnic4
   23     Eth1/6     UP   UP    FWD        -    1040     5    0        0                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

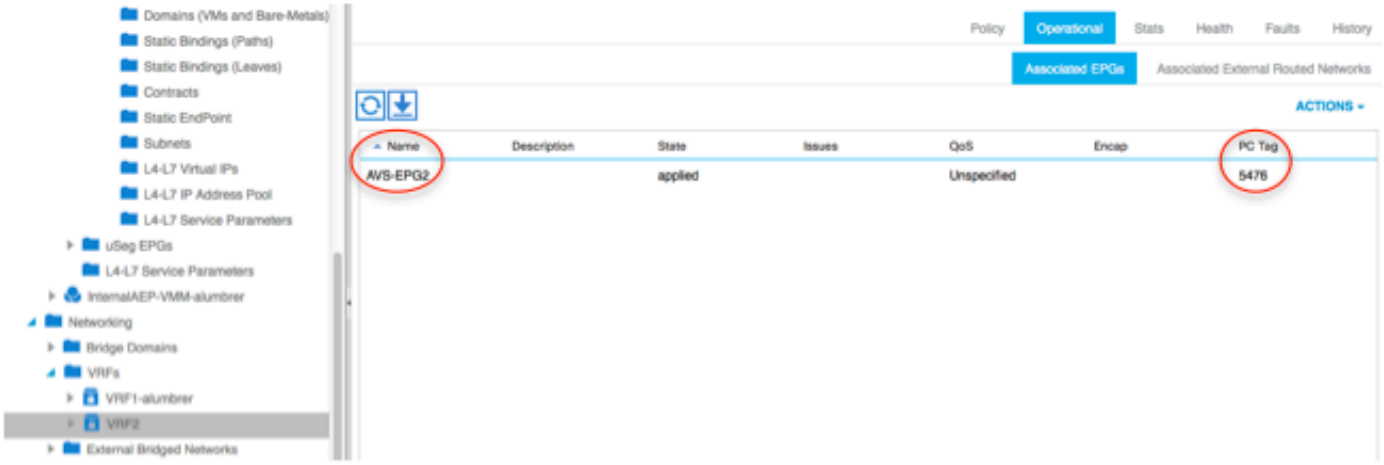
```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State    Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   24     Eth1/7     UP   UP    FWD        -    1040     6    0        0                vmnic6
   50                UP   UP    FWD        -       0     6    0        0                 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
~ #
```

Por último, las reglas del firewall también se pueden verificar en el nivel de hoja si conocemos las etiquetas de PC para los EPG de origen y destino:

EPG1



EPG2



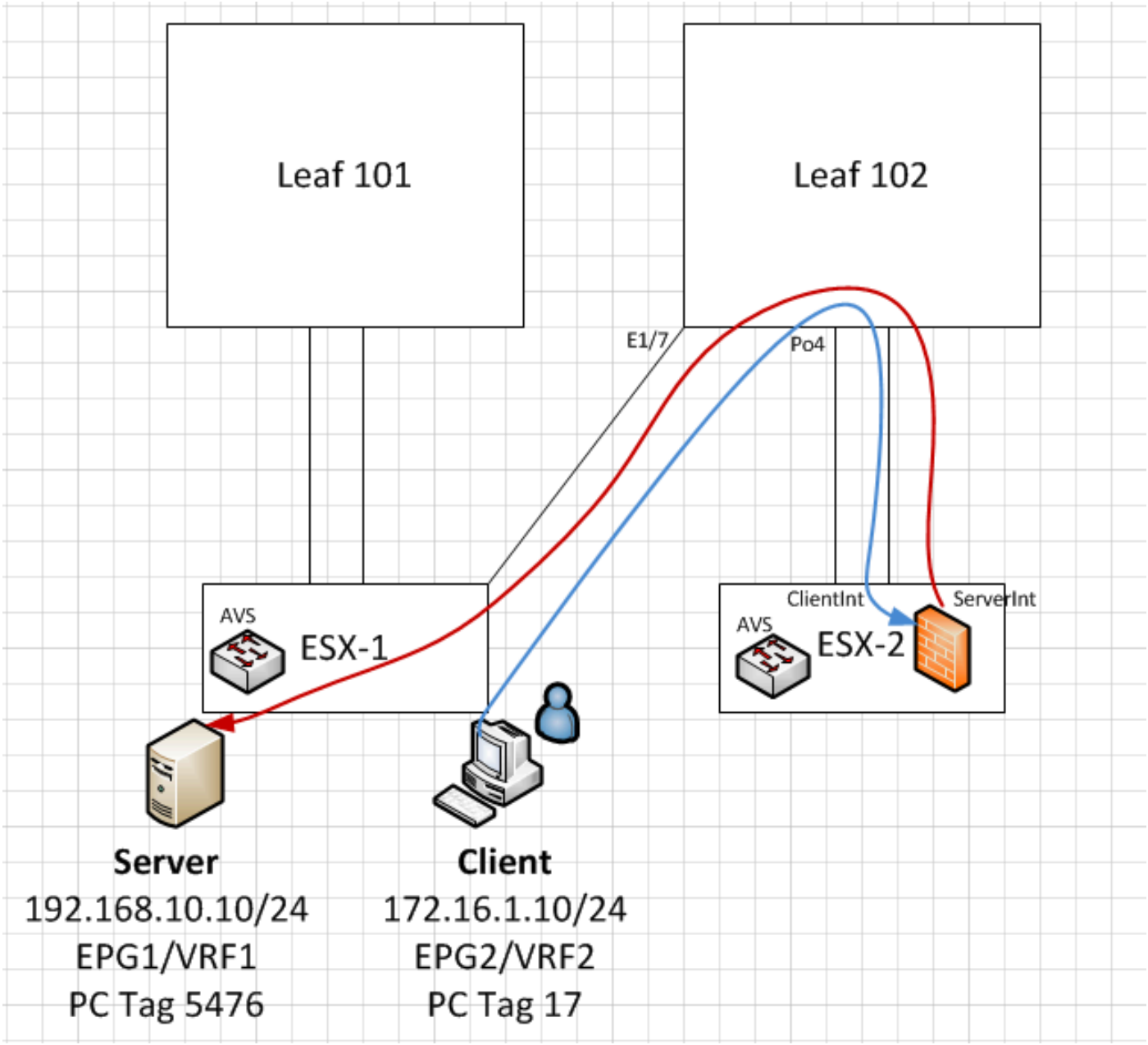
Los ID de filtro pueden coincidir con las etiquetas de PC de la hoja para verificar las reglas de FW.

```
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#
```

Nota: El PCTags/Sclass de EPG nunca se comunica directamente. La comunicación se interrumpe o se une a través de los EPG de sombra creados por la inserción del gráfico de servicio L4-L7.

Y la comunicación Cliente a Servidor funciona.

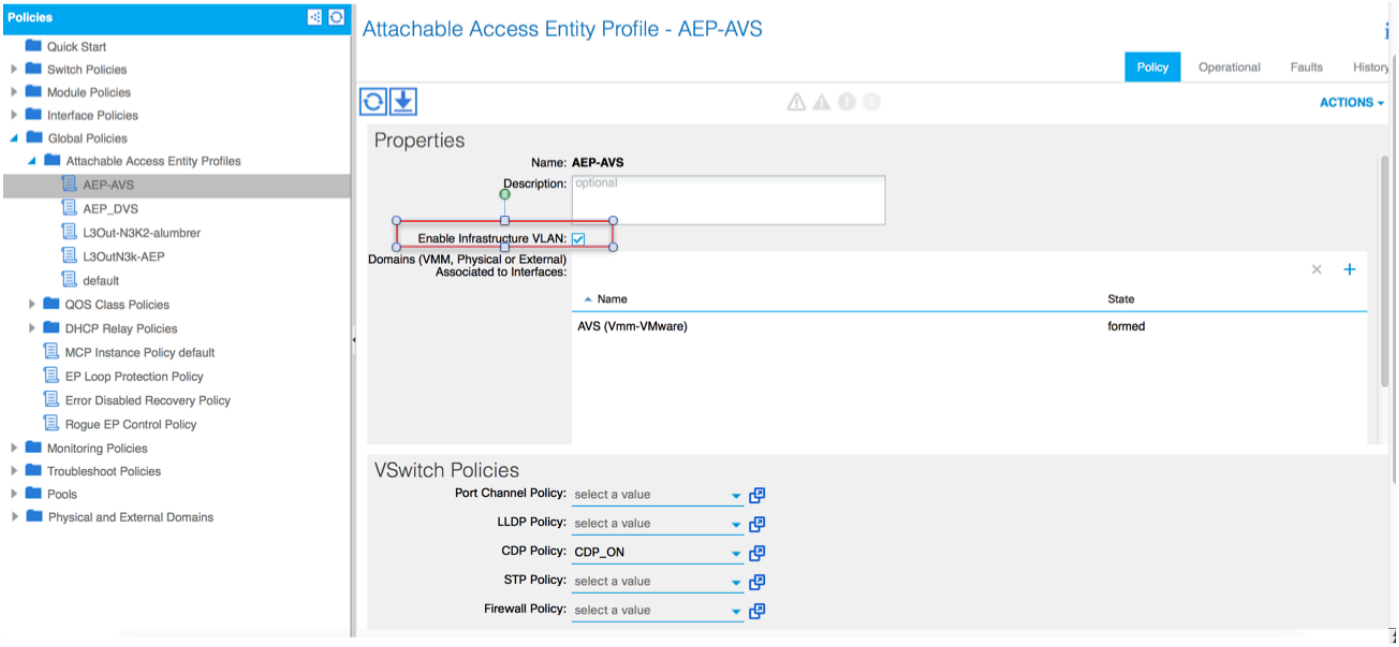
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          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:~$ $
```



Troubleshoot

La dirección VTEP no está asignada

Verifique que la VLAN de infraestructura esté verificada bajo AEP:



Versión no admitida

Verifique que la versión de VEM sea correcta y admita el sistema VMWare de ESXi adecuado.

```
~ # 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
```

No funciona la comunicación de VEM y fabric

```
- 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
```

En este punto, se puede determinar que la comunicación del fabric entre el host ESXi y la hoja no funciona correctamente. Algunos comandos de verificación se pueden verificar en el lado de la hoja para determinar la causa raíz.

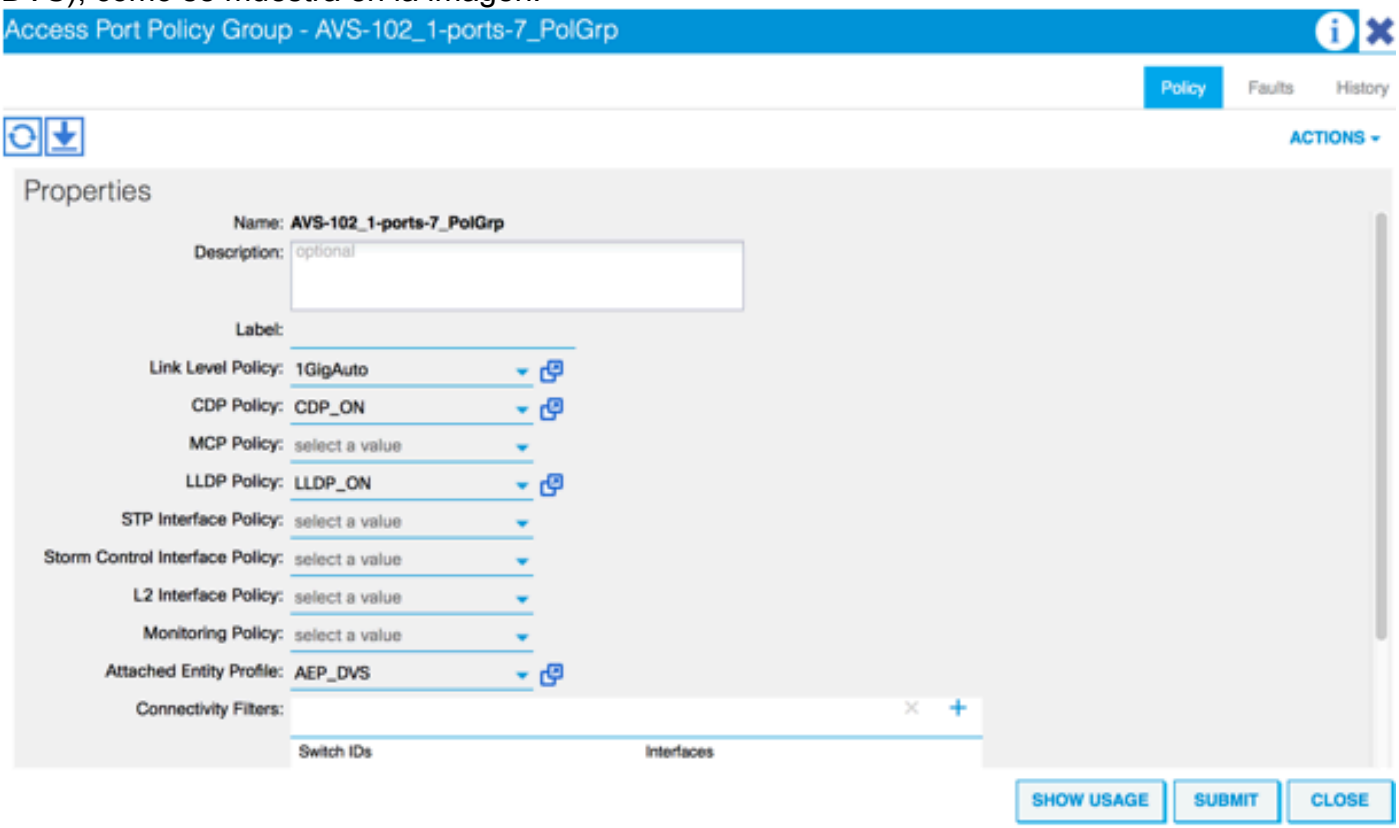
```
leaf2# show cdp ne

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)
```

Hay 2 puertos que se utilizan en el ESXi conectados a través de un Po5

```
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
```

A partir del resultado anterior, se puede observar que la Vlan Infra no está permitida ni pasa a través de los puertos Uplinks que van al host ESXi (1/5-6). Esto indica un error de configuración con la política de interfaz o la política de switch configurada en APIC.
Verifique ambos:
Políticas de acceso > Políticas de interfaz > Perfiles Políticas de acceso > Políticas de switch > Perfiles
En este caso, los perfiles de interfaz se conectan al AEP incorrecto (antiguo AEP utilizado para DVS), como se muestra en la imagen:



Después de configurar el AEP correcto para AVS, ahora podemos ver que la Vlan Infra se ve a través de los Unlinks adecuados en la hoja:

```
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
```

Información Relacionada

Instalación del switch virtual de la aplicación

Cisco Systems, Inc. Guía de Instalación de Cisco Application Virtual Switch, Versión 5.2(1)SV3(1.2)

Implemente ASAv con VMware

Guía de inicio rápido de Cisco Systems, Inc. Cisco Adaptive Security Virtual Appliance (ASAv), 9.4

Cisco ACI y Cisco AVS

Cisco Systems, Inc. Guía de virtualización de Cisco ACI, versión 1.2(1i)

Informe técnico sobre diseño de gráficos de servicios con Cisco Application Centric Infrastructure

Informe técnico sobre diseño de gráficos de servicios con Cisco Application Centric Infrastructure

Soporte Técnico y Documentación - Cisco Systems