Servicios de FirePOWER de la configuración en el dispositivo ISR con la cuchilla UCS-E

Contenido

Introducción

Este documento describe cómo instalar y desplegar el software de Cisco FirePOWER en una plataforma de la cuchilla de la serie del Cisco Unified Computing System E (UCS-E) en el modo del sistema de la detección de intrusos (IDS). El ejemplo de configuración que se describe en este documento es un suplemento al guía del usuario oficial.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Imagen 3.14 del Routers de los Servicios integrados de Cisco (ISR) XE o más adelante
- Versión 2.3 o posterior del regulador de la administración integrada de Cisco (CIMC)
- Versión 5.2 o posterior del centro de administración de Cisco FireSIGHT (FMC)
- Versión 5.2 o posterior del dispositivo virtual de Cisco FirePOWER (NGIPSv)
- Versión 5.0 o posterior de VMware ESXi

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

> **Note**: Antes de que usted actualice el código a la versión 3.14 o posterior, asegúrese de que el sistema tenga memoria suficiente, el espacio en disco, y una licencia para la actualización. Refiera al ejemplo 1: Copie la imagen para contellear: de la sección del servidor TFTP del documento de Cisco de los procedimientos de actualización de software de los routeres de acceso para aprender más sobre las actualizaciones de código.

> **Note**: Para actualizar el CIMC, BIOS, y otros componentes de firmware, usted puede utilizar o la utilidad de la actualización del host de Cisco (HUU), o usted puede actualizar a los componentes de firmware manualmente. Para aprender más sobre la actualización del firmware, refiera a actualizar el firmware en la sección de los servidores del E-series de Cisco UCS del guía del usuario utilitario de la actualización del host para los servidores del E-series de Cisco UCS y el motor del cálculo de la red del E-series de Cisco UCS.

Antecedentes

Esta sección proporciona la información sobre las Plataformas de hardware admitido, las licencias, y las limitaciones con respecto a los componentes y a los procedimientos que se describen en este documento.

Plataformas de hardware admitido

Esta sección enumera las Plataformas de hardware admitido para el G2 y los dispositivos de las 4000 Series.

Dispositivos ISR G2 con las cuchillas UCS-E

Estos dispositivos de las G2 Series ISR con las cuchillas de la serie UCS-E se soportan:

Producto	Platform	Modelo UCS-E
Cisco 2900 Series ISR	2911	Sola opción amplia UCS-E 120/140
	2921	Opción amplia simple o doble UCS-E 120/140/160/180
	2951	Opción amplia simple o doble UCS-E 120/140/160
Cisco 3900 Series ISR	3925	UCS-E opción amplia sola y doble de 120/140/160 o 180 anchos dobles
	3925E	UCS-E opción amplia sola y doble de 120/140/160 o 180 anchos dobles
	3945	UCS-E opción amplia sola y doble de 120/140/160 o 180 anchos dobles
	3945E	UCS-E opción amplia sola y doble de 120/140/160 o 180 anchos dobles

Dispositivos ISR 4000 con las cuchillas UCS-E

Estos dispositivos de las 4000 Series ISR con las cuchillas de la serie UCS-E se soportan:

Producto	Platform	Modelo UCS-E
Cisco 4400 Series ISR	4451	UCS-E opción amplia sola y doble de 120/140/160 o 180 anchos dobles
	4431	Módulo de interfaz de la red UCS-E
Cisco 4300 Series ISR	4351	UCS-E opción amplia sola y doble de 120/140/160/180 o 180 anchos dob
	4331	Sola opción amplia UCS-E 120/140
	4321	Módulo de interfaz de la red UCS-E

Licencias

El ISR debe tener una licencia del k9 de la Seguridad, así como una licencia del appx, para habilitar el servicio.

Limitaciones

Aquí están las dos limitaciones en lo que respecta a la información que se describe en este documento:

- El Multicast no se soporta
- Solamente 4,096 interfaces del dominio de Bridge (BDI) se soportan para cada sistema

Los BDI no soportan estas características:

- Protocolo bidireccional de la detección de la expedición (BFD)
- Netflow
- Quality of Service (QoS)
- Network-Based Application Recognition (NBAR) o codificación video avanzada (AVC)
- La zona basó el Firewall (ZBF)
- VPN criptográficos
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) sobre los Ethernetes (PPPoE)

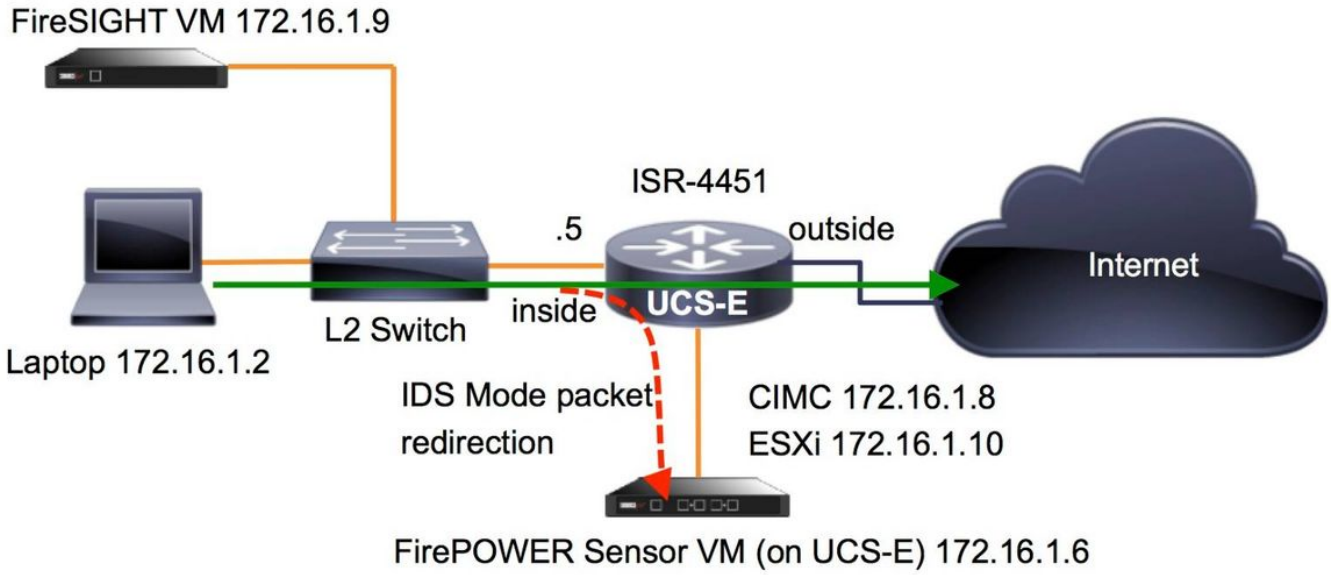
> **Note**: Para un BDI, el Tamaño de la unidad máxima de transmisión (MTU) se puede configurar con cualquier valor entre 1,500 y 9,216 bytes.

Configurar

Esta sección describe cómo configurar los componentes que están implicados con este despliegue.

Diagrama de la red

La configuración que se describe en este documento utiliza esta topología de red:



Flujo de trabajo para los servicios de FirePOWER en UCS-E

Aquí está el flujo de trabajo para los servicios de FirePOWER que se ejecutan en un UCS-E:

1. Los empujes del DATA-avión trafican para el examen hacia fuera de la interfaz BDI/UCS-E (trabajos para los dispositivos G2 y de las G3 Series).
2. Cisco IOS®-XE CLI activa la redirección de paquete para el análisis (opciones para todas las interfaces o por interface).
3. La secuencia de mandos del inicio de la **configuración del** sensor CLI simplifica la configuración.

Configuración CIMC

Esta sección describe cómo configurar el CIMC.

Conecte con CIMC

Hay diferentes formas de conectar con el CIMC. En este ejemplo, la conexión al CIMC se completa vía un puerto de la administración dedicado. Asegúrese de que usted conecte el puerto **M** (dedicado) con la red con el uso de un cable Ethernet. Una vez que está conectado, funcione con el comando del **subslot del módulo del hw del** prompt de router:

```
ISR-4451#hw-module subslot 2/0 session imc

IMC ACK: UCSE session successful for IMC
```

```
Establishing session connect to subslot 2/0
To exit, type ^a^q

picocom v1.4

port is : /dev/ttyDASH1
flowcontrol : none
baudrate is : 9600
parity is : none
databits are : 8
escape is : C-a
noinit is : no
noreset is : no
nolock is : yes
send_cmd is : ascii_xfr -s -v -l10
receive_cmd is : rz -vv

Terminal ready
```

Extremidad 1: Para salir, ejecute **^a^q.**

Extremidad 2: El nombre de usuario predeterminado es <password> **admin** y de la contraseña. El proceso de reinicio de la contraseña se describe aquí: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/3-1-1/gs/guide/b_Getting_Started_Guide/b_3_x_Getting_Started_Guide_appendix_01011.html#GUID-73551F9A-4C79-4692-838A-F99C80E20A28

Configuración CIMC

Utilice esta información para completar la configuración del CIMC:

```
Unknown# scope cimc
Unknown /cimc # scope network
Unknown /cimc/network # set dhcp-enabled no
Unknown /cimc/network *# set dns-use-dhcp no
Unknown /cimc/network *# set mode dedicated
Unknown /cimc/network *# set v4-addr 172.16.1.8
Unknown /cimc/network *# set v4-netmask 255.255.255.0
Unknown /cimc/network *# set v4-gateway 172.16.1.1
Unknown /cimc/network *# set preferred-dns-server 64.102.6.247
Unknown /cimc/network *# set hostname 4451-UCS-E
Unknown /cimc/network *# commit
```

Precaución: Asegúrese de que usted funcione con el **comando commit** para salvar los cambios.

Note: El modo se fija **dedicado** cuando se utiliza el puerto de administración.

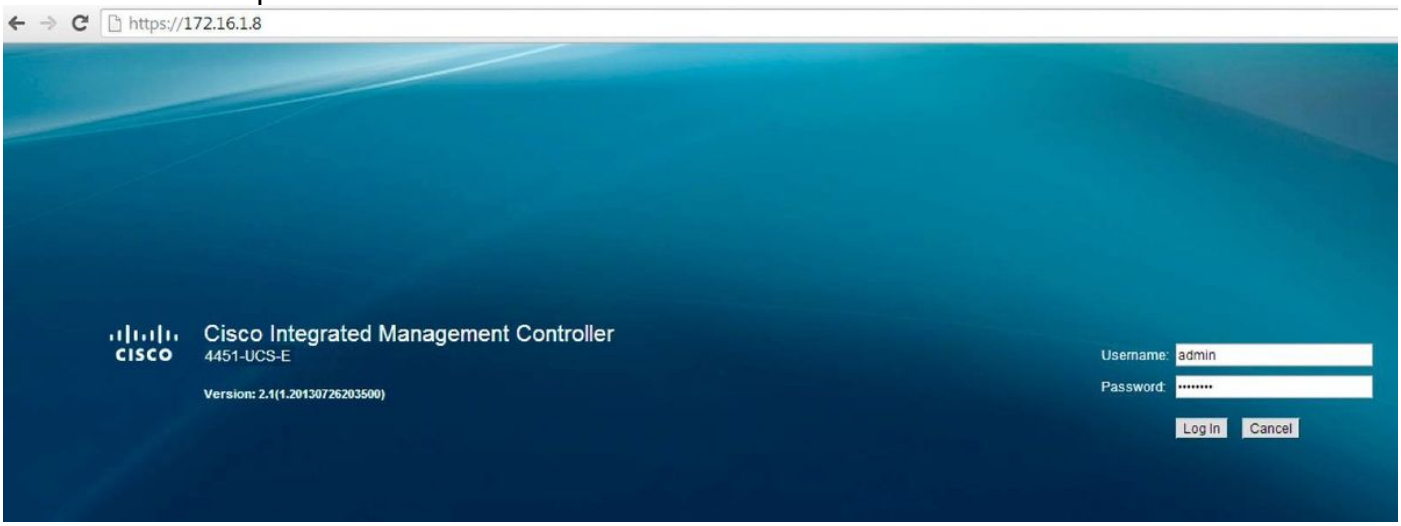
Funcione con el **comando detail de la demostración** para verificar las configuraciones del detalle:

```
4451-UCS-E /cimc/network # show detail
Network Setting:
IPv4 Address: 172.16.1.8
IPv4 Netmask: 255.255.255.0
```

```
IPv4 Gateway: 172.16.1.1
DHCP Enabled: no
Obtain DNS Server by DHCP: no
Preferred DNS: 64.102.6.247
Alternate DNS: 0.0.0.0
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Hostname: 4451-UCS-E
MAC Address: E0:2F:6D:E0:F8:8A
NIC Mode: dedicated
NIC Redundancy: none
NIC Interface: console
4451-UCS-E /cimc/network #
```

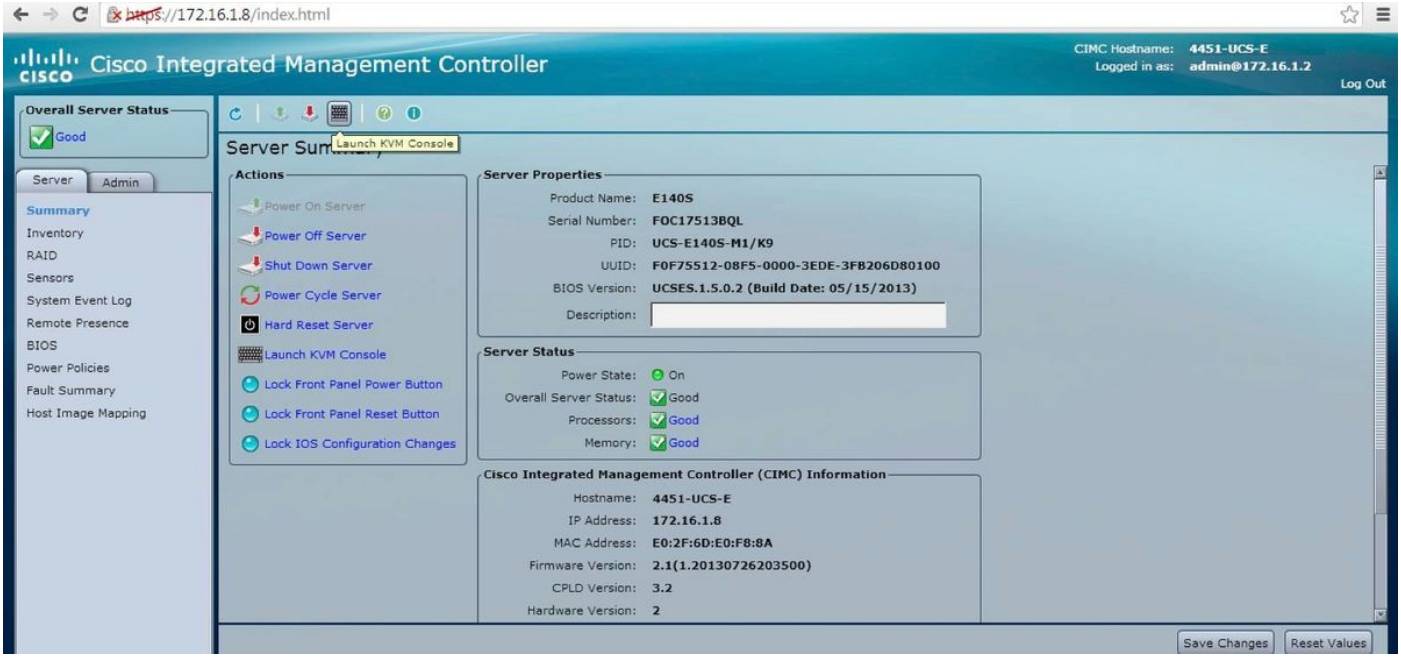
Ponga en marcha la interfaz Web del CIMC de un navegador con el nombre de usuario predeterminado y de la contraseña tal y como se muestra en de la imagen. El nombre de usuario predeterminado y la contraseña son:

- Nombre de usuario: **admin**
- Contraseña <password>

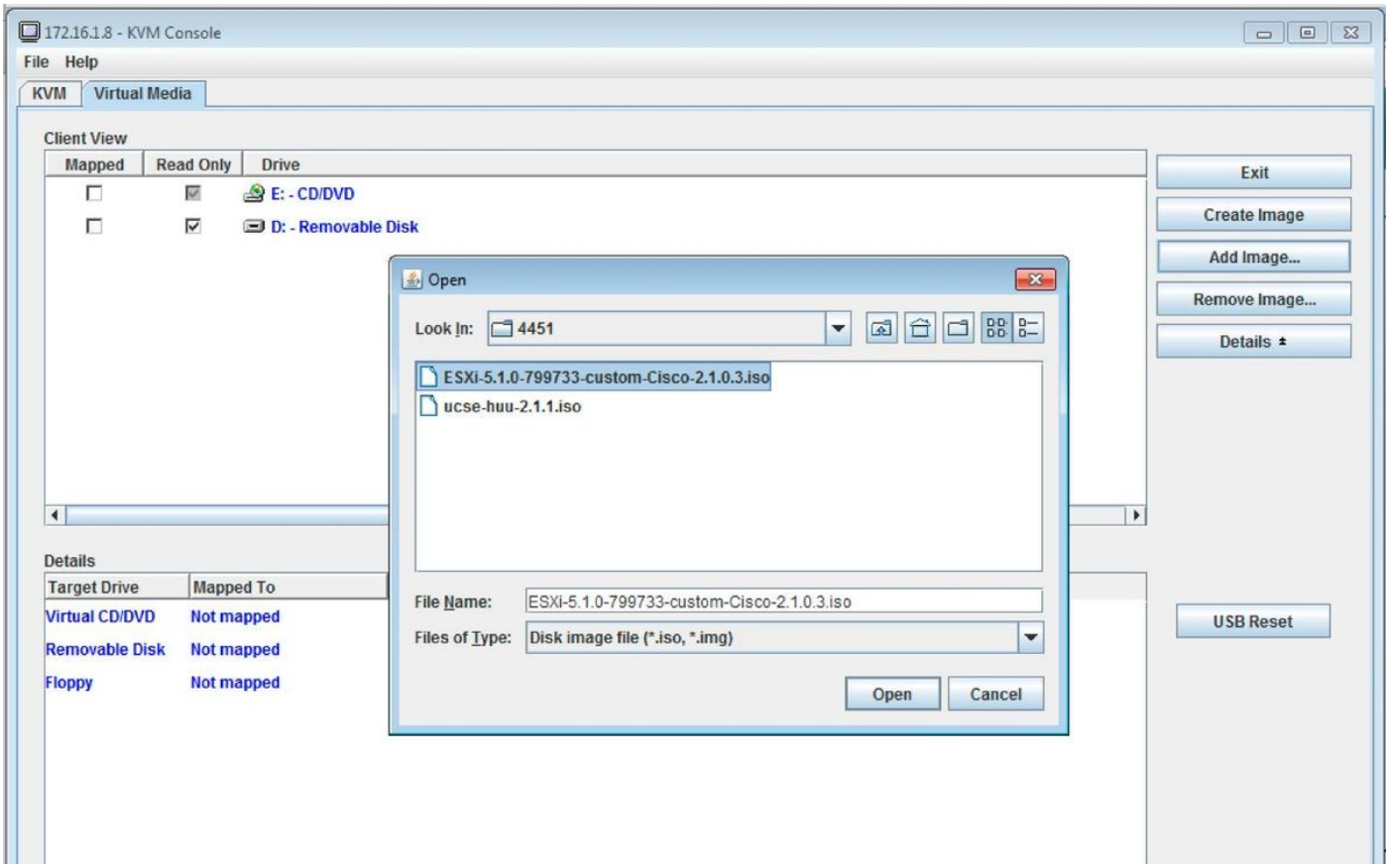


Instale ESXi

Después de que usted registre en la interfaz de usuario del CIMC, usted puede ver una página similar a ésa mostrada en esta imagen. Haga clic el icono de la **consola del lanzamiento KVM**, el tecleo **agrega la imagen**, y después asocia el ESXi ISO como los media virtuales:



Haga clic la lengueta de los **medios virtuales**, y después haga clic **agregan la imagen** para asociar los media virtuales tal y como se muestra en de la imagen.



Después de que se asocie el media virtual, haga clic el **servidor del ciclo del poder del** ciclo de la potencia del Home Page CIMC para el UCS-E. Los lanzamientos de la configuración de ESXi de los media virtuales. Complete al ESXi instalan.

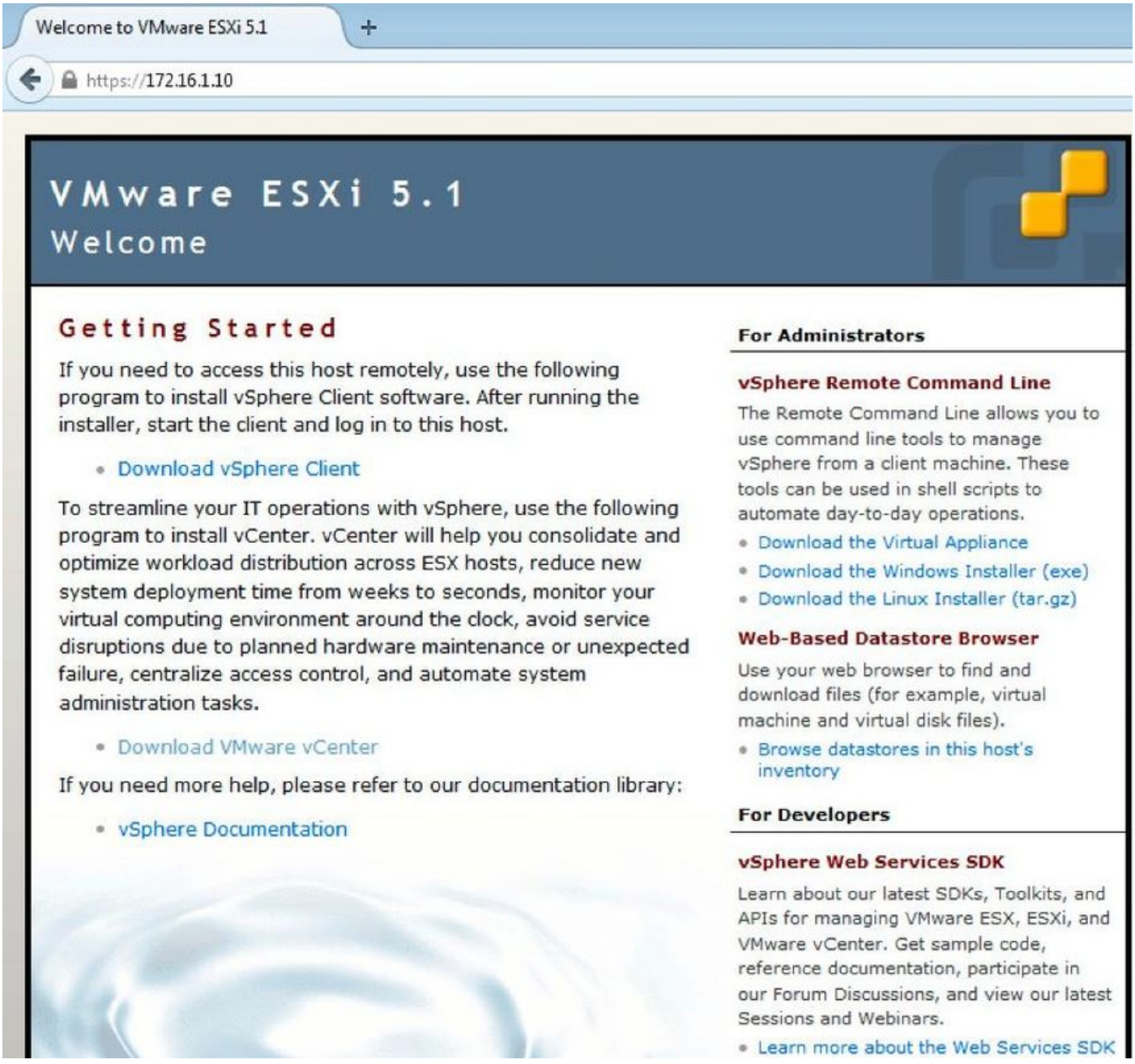
> **Note**: Registre la dirección IP, el nombre de usuario, y la contraseña de ESXi para la referencia futura.

Instale al cliente del vSphere

Esta sección describe cómo instalar al cliente del vSphere.

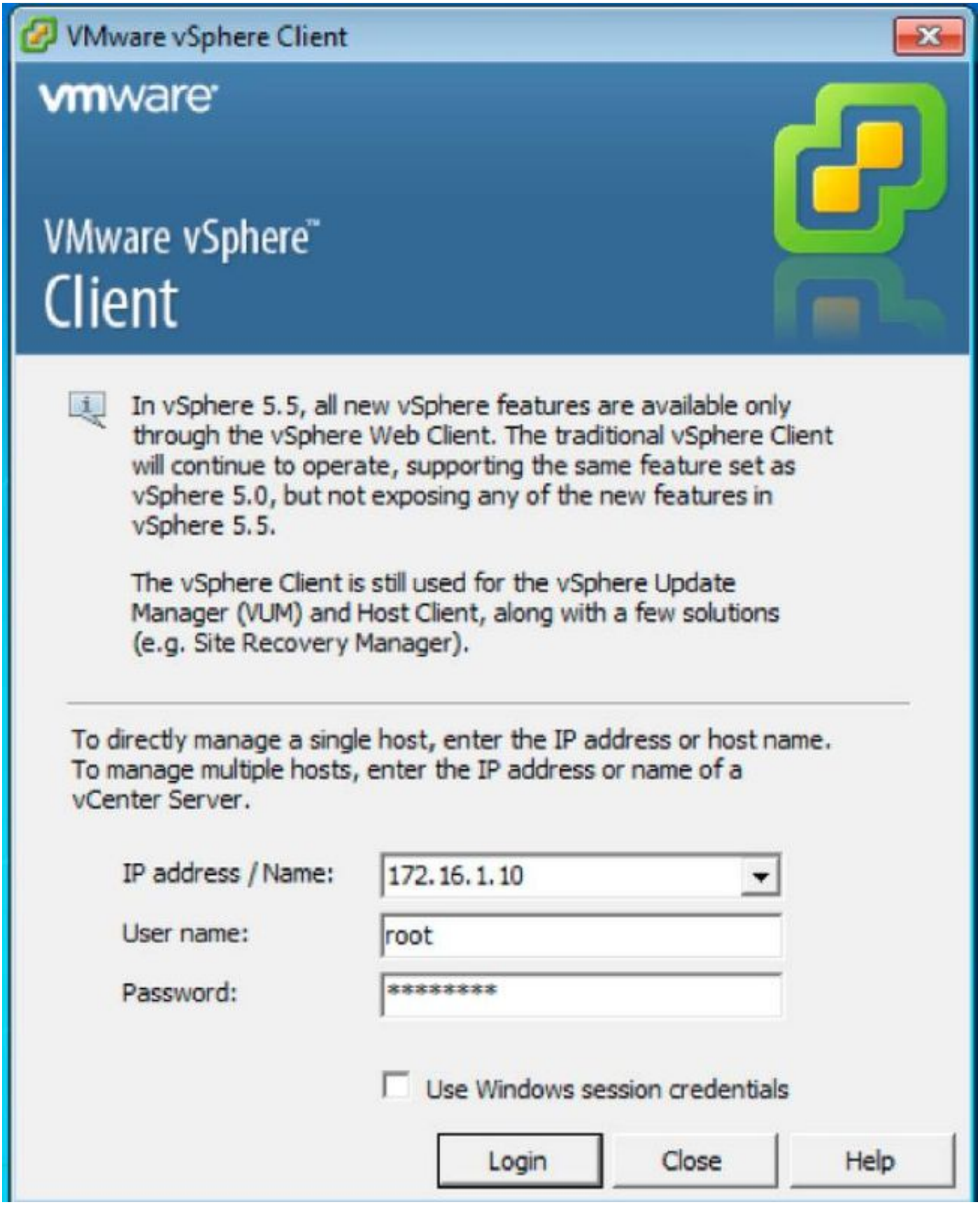
Cliente del vSphere de la descarga

Inicie ESXi y utilice el link del **cliente de VSphere de la descarga** para descargar al cliente del vSphere. Instalelo en su ordenador.



Inicie al cliente del vSphere

Inicie al cliente del vSphere de su ordenador. Inicie sesión con el nombre de usuario y contraseña que usted creó durante la instalación y tal y como se muestra en de la imagen:



Despliegue el centro de administración de FireSIGHT y los dispositivos de FirePOWER

Complete los procedimientos que se describen en el despliegue del centro de administración de FireSIGHT en el documento de Cisco de VMware ESXi para desplegar un centro de administración de FireSIGHT en el ESXi.

Note: El proceso que se utiliza para desplegar un dispositivo de FirePOWER NGIPSv es similar al proceso que se utiliza para desplegar un centro de administración.

Interfaces

En el ancho dual UCS-E, hay cuatro interfaces:

- La interfaz más alta de la dirección MAC es Gi3 en el panel frontal
- La segunda interfaz más alta de la dirección MAC es Gi2 en el panel frontal
- Los dos más recientes que aparecen son las interfaces internas

En el solo ancho UCS-E, hay tres interfaces:

- La interfaz más alta de la dirección MAC es Gi2 en el panel frontal
- Los dos más recientes que aparecen son las interfaces internas

Ambas interfaces UCS-E en el ISR4K son puertos troncales.

Los UCS-E 120S y 140S tienen adaptador de red tres más los puertos de administración:

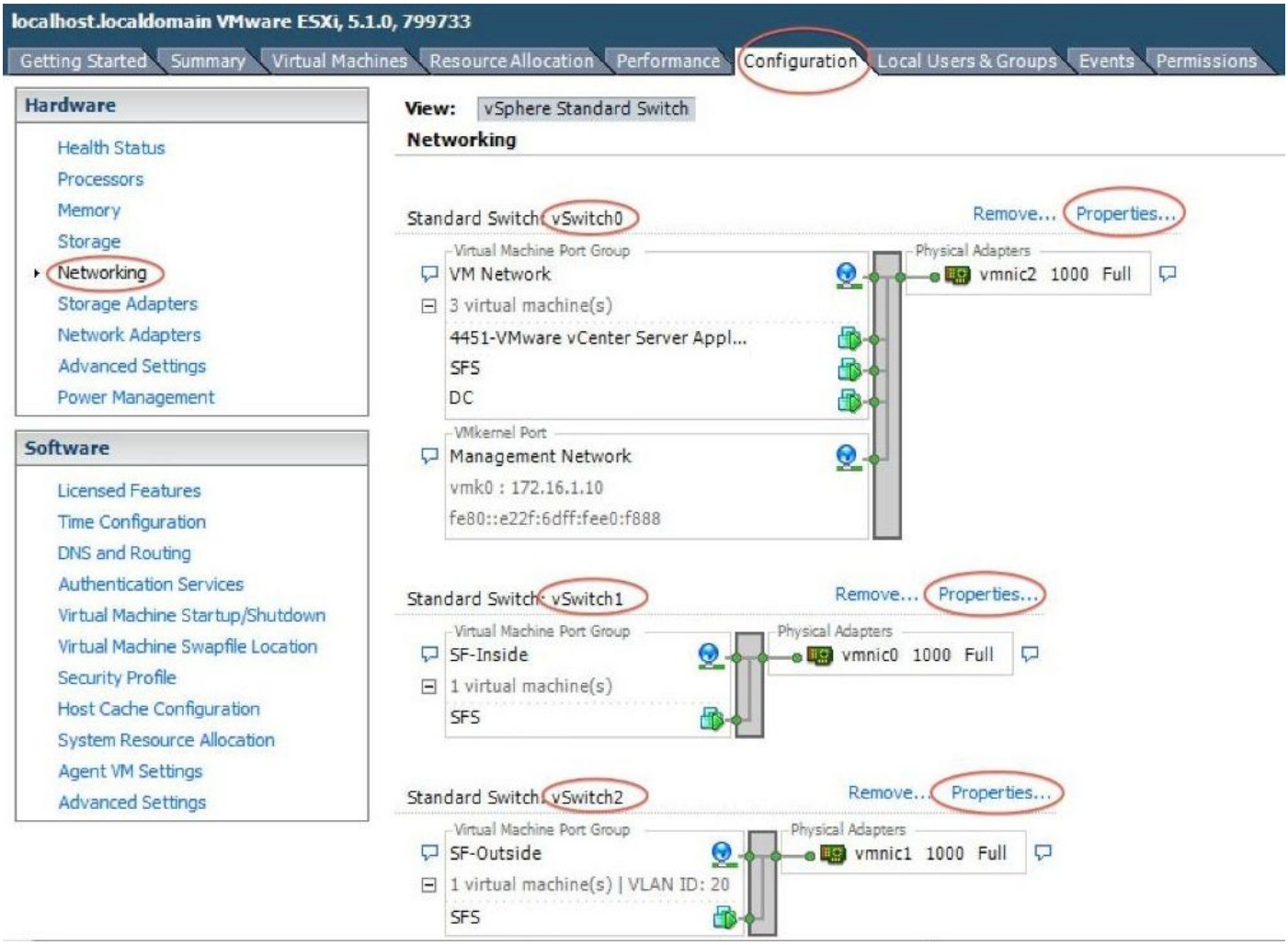
- *El vmnic0* se asocia a *UCSEx/0/0* en la placa de interconexiones del router
- *El vmnic1* se asocia a *UCSEx/0/1* en la placa de interconexiones del router
- *El vmnic2* se asocia a la interfaz del avión GE2 del frente UCS-E
- El puerto de la Administración del panel de delante (m) se puede utilizar solamente para el CIMC.

Los UCS-E 140D, 160D, y 180D tienen cuatro adaptadores de red:

- *El vmnic0* se asocia a *UCSEx/0/0* en la placa de interconexiones del router.
- *El vmnic1* se asocia a *UCSEx/0/1* en la placa de interconexiones del router.
- *El vmnic2* se asocia a la interfaz del avión GE2 del frente UCS-E.
- *El vminc3* se asocia a la interfaz del avión GE3 del frente UCS-E.
- El puerto de la Administración del panel de delante (m) se puede utilizar solamente para el CIMC.

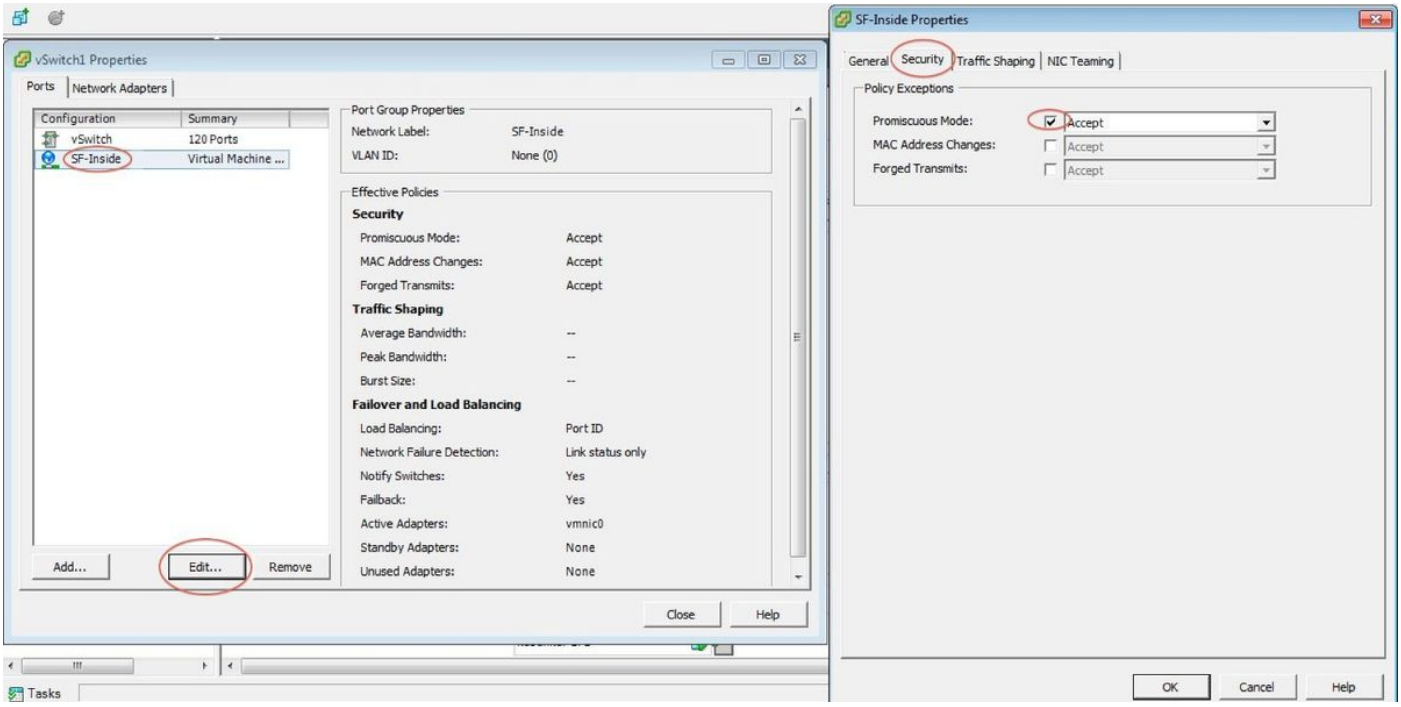
interfaces del vSwitch en ESXi

El vSwitch0 en el ESXi es la interfaz de administración a través de la cual el ESXi, el centro de administración de FireSIGHT, y el dispositivo de FirePOWER NGIPSv comunican a la red. **Propiedades del** tecleo para el vSwitch1 (Sf-dentro de) y el vSwitch2 (Sf-exterior) para realizar ningunos los cambios.



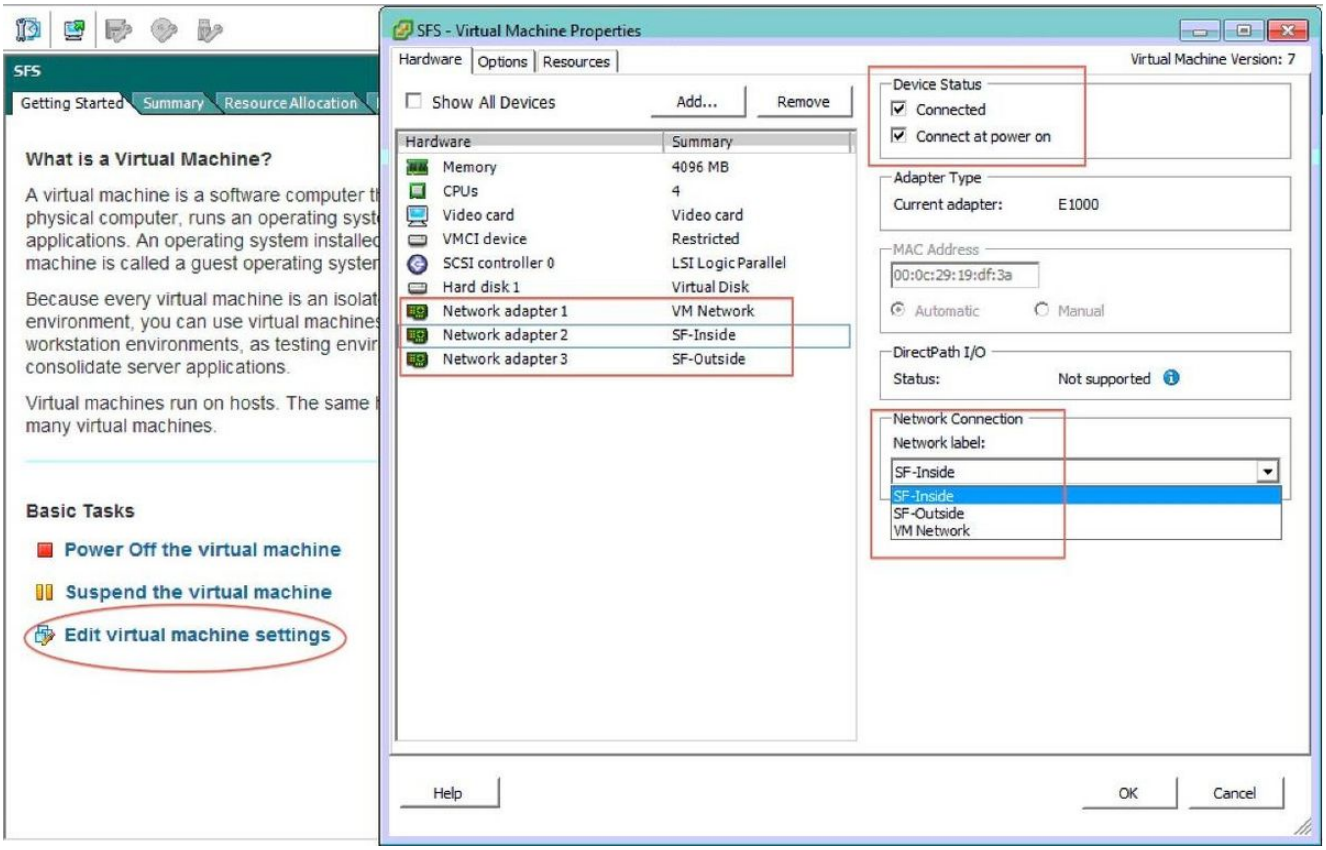
Esta imagen muestra las propiedades del vSwitch1 (usted debe completar los mismos pasos para el vSwitch2):

> **Note**: Asegúrese de que el VLAN ID está configurado a 4095 para NGIPSv, esto está requerida según el documento de NGIPSv: http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



La configuración del vSwtich en el ESXi es completa. Ahora usted debe verificar las configuraciones de la interfaz:

1. Navegue a la máquina virtual para el dispositivo de FirePOWER.
2. El tecleo **edita las configuraciones de la máquina virtual**.
3. Verifique todos los tres adaptadores de red.
4. Asegúrese de que estén elegidos correctamente, tal y como se muestra en de la imagen aquí:



Registre el dispositivo de FirePOWER con el centro de administración de

FireSIGHT

Complete los procedimientos que se describen en el documento de Cisco para registrar un dispositivo de FirePOWER con un centro de administración de FireSIGHT.

Reoriente y verifique el tráfico

Utilize esta sección para confirmar que su configuración funcione correctamente.

Esta sección describe cómo reorientar el tráfico y cómo verificar los paquetes.

Reoriente el tráfico del ISR al sensor en UCS-E

Utilice esta información para reorientar el tráfico:

```
interface GigabitEthernet0/0/1
ip address dhcp
negotiation auto
!
interface ucse2/0/0
no ip address
no negotiation auto
switchport mode trunk
no mop enabled
no mop sysid
service instance 1 ethernet
encapsulation untagged
bridge-domain 1
!
interface BDI1
ip unnumbered GigabitEthernet0/0/1
end
!
utd
mode ids-global
ids redirect interface BDI1
```

> **Note**: Si usted funciona con actualmente la versión 3.16.1 o posterior, funcione con el comando **avanzado motor UTD** en vez del comando **UTD**.

Verifique la redirección de paquete

De la consola ISR, funcione con este comando para verificar si los contadores de paquetes incrementan:

```
cisco-ISR4451#  show plat hardware qfp active feature utd stats

Drop Statistics:
Stats were all zero
General Statistics:
Pkts Entered Policy 6
Pkts Entered Divert 6
Pkts Entered Recycle Path 6
```

```
Pkts already diverted 6
Pkts replicated 6
Pkt already inspected, policy check skipped 6
Pkt set up for diversion 6
```

Verificación

Usted puede funcionar con estos **comandos show** para verificar que su configuración trabaja correctamente:

- **la demostración plat UTD del software global**
- **la demostración plat las interfaces UTD del software**
- **la demostración plat global activo UTD rp del software**
- **la demostración plat global activo punto de congelación UTD del software**
- **la demostración plat el stats activo UTD de la característica del qfp del hardware**
- **muestre a qfp del hardware de plataforma UTD activo de la característica**

Troubleshooting

Esta sección brinda información que puede utilizar para la solución de problemas en su configuración.

Usted puede funcionar con estos **comandos debug** para resolver problemas su configuración:

- **controlplane UTD de la característica de la condición de la plataforma del debug**
- **submode del dataplane UTD de la característica de la condición de la plataforma del debug**

Información Relacionada

- Guía de introducción para los servidores del E-series de Cisco UCS y el motor del cálculo de la red del E-series de Cisco UCS, versión 2.x
- Guía de Troubleshooting para los servidores del E-series de Cisco UCS y el motor del cálculo de la red del E-series de Cisco UCS
- Guía de introducción para los servidores del E-series de Cisco UCS y el motor del cálculo de la red del E-series de Cisco UCS, versión 2.x – actualizar el firmware
- Guía de configuración de software del Routers de servicios de agregación Cisco ASR de la serie 1000 – Configurar las interfaces del dominio de Bridge
- Guía del usuario utilitario de la actualización del host para los servidores del E-series de Cisco UCS y el motor del cálculo de la red del E-series de Cisco UCS – actualizar el firmware en los servidores del E-series de Cisco UCS
- Soporte Técnico y Documentación - Cisco Systems