# Configure FirePOWER Services en un dispositivo ISR con el blade UCS-E

## Contenido



## Introducción

Este documento describe cómo instalar e implementar el software Cisco FirePOWER en una plataforma blade Cisco Unified Computing System serie E (UCS-E) en modo de sistema de detección de intrusiones (IDS). El ejemplo de configuración que se describe en este documento es un complemento de la guía oficial del usuario.

# Prerequisites

## Requirements

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.

- Routers de servicios integrados (ISR) de Cisco, imagen 3.14 o posterior
- Cisco Integrated Management Controller (CIMC) versión 2.3 o posterior
- Cisco FireSIGHT Management Center (FMC) versión 5.2 o posterior
- Dispositivo virtual Cisco FirePOWER (NGIPSv) versión 5.2 o posterior
- VMware ESXi versión 5.0 o posterior

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

> **Nota:** Antes de actualizar el código a la versión 3.14 o posterior, asegúrese de que el sistema tenga suficiente memoria, espacio en disco y una licencia para la actualización. Consulte el Ejemplo 1: Copiar la imagen en flash: desde la sección del servidor TFTP del documento Procedimientos de actualización del software del router de acceso Cisco para obtener más información sobre las actualizaciones del código.

> **Nota:** Para actualizar el CIMC, el BIOS y otros componentes de firmware, puede utilizar la utilidad de actualización de host de Cisco (HUU) o actualizar los componentes de firmware manualmente. Para obtener más información sobre la actualización del firmware, consulte la sección Actualización del firmware en los servidores Cisco UCS serie E de la Guía del usuario de la utilidad de actualización del host para los servidores Cisco UCS serie E y Cisco UCS serie E Network Compute Engine.

# Antecedentes

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

## Plataformas de hardware compatibles

Esta sección enumera las plataformas de hardware soportadas para los dispositivos G2 y 4000 Series.

### Dispositivos ISR G2 con blades UCS-E

Estos dispositivos ISR G2 Series con blades UCS-E son compatibles:

| Producto | Platform | Modelo UCS-E |
|---|---|---|
| ISR de Cisco serie 2900 | 2911 | Opción de ancho único UCS-E 120/140 |
| | 2921 | Opción de ancho único o doble UCS-E 120/140/160/180 |
| | 2951 | Opción de ancho único o doble UCS-E 120/140/160 |
| ISR de Cisco serie 3900 | 3925 | UCS-E 120/140/160 de ancho sencillo y doble o 180 de ancho doble |
| | 3925E | UCS-E 120/140/160 de ancho sencillo y doble o 180 de ancho doble |
| | 3945 | UCS-E 120/140/160 de ancho sencillo y doble o 180 de ancho doble |
| | 3945E | UCS-E 120/140/160 de ancho sencillo y doble o 180 de ancho doble |

#### Dispositivos ISR 4000 con blades UCS-E

Estos dispositivos ISR serie 4000 con blades UCS serie E son compatibles con:

| Producto | Platform | Modelo UCS-E |
|---|---|---|
| ISR de Cisco serie 4400 | 4451 | UCS-E 120/140/160 de ancho sencillo y doble o 180 de ancho doble |
| | 4431 | Módulo de interfaz de red UCS-E |
| ISR de Cisco serie 4300 | 4351 | UCS-E 120/140/160/180 de ancho sencillo y doble o 180 de ancho dob |
| | 4331 | Opción de ancho único UCS-E 120/140 |
| | 4321 | Módulo de interfaz de red UCS-E |

### Licencias

El ISR debe tener una licencia K9 de seguridad, así como una licencia appx, para habilitar el servicio.

### Limitaciones

Estas son las dos limitaciones con respecto a la información que se describe en este documento:

- No se admite la multidifusión
- Solo se admiten 4096 interfaces de dominio de puente (BDI) para cada sistema

Los BDI no admiten estas funciones:

- Protocolo de detección de reenvío bidireccional (BFD)
- Netflow
- Quality of Service (QoS)
- Reconocimiento de aplicaciones basadas en la red (NBAR) o codificación de vídeo avanzada (AVC)
- Firewall basado en zonas (ZBF)
- VPN criptográficas
- Multiprotocol Label Switching (MPLS)
- Protocolo punto a punto (PPP) sobre Ethernet (PPPoE)

> **Nota:** Para un BDI, se puede configurar el tamaño de la unidad máxima de transmisión (MTU) con cualquier valor entre 1500 y 9216 bytes.

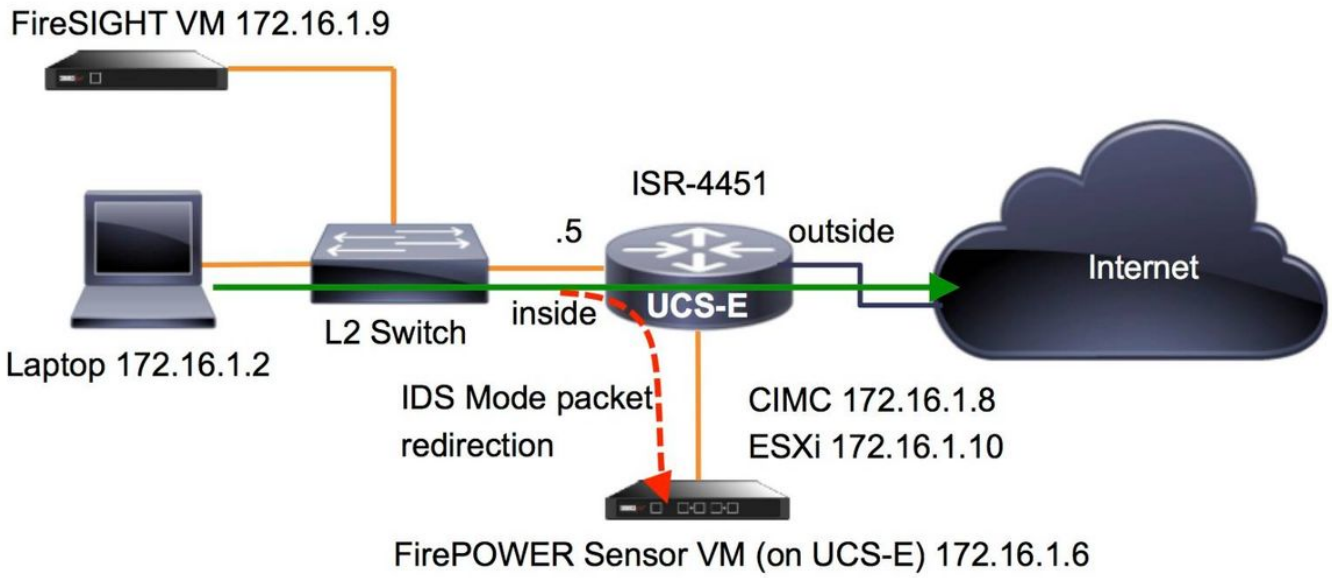
## Configurar

En esta sección se describe cómo configurar los componentes que participan en esta

implementación.

## Diagrama de la red

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




## Flujo de trabajo para FirePOWER Services en UCS-E

Este es el flujo de trabajo para los servicios FirePOWER que se ejecutan en UCS-E:

1. El plano de datos expulsa el tráfico para su inspección desde la interfaz BDI/UCS-E (funciona para los dispositivos de las series G2 y G3).
2. La CLI de Cisco IOS®-XE activa la redirección de paquetes para el análisis (opciones para todas las interfaces o por interfaz).
3. El script de inicio de **configuración** CLI del sensor simplifica la configuración.

## Configurar CIMC

Esta sección describe cómo configurar el CIMC.

### Conexión a CIMC

Hay varias formas de conectarse al CIMC. En este ejemplo, la conexión al CIMC se completa a través de un puerto de administración dedicado. Asegúrese de conectar el puerto **M** (dedicado) a la red mediante un cable Ethernet. Una vez conectado, ejecute el comando **hw-module subslot** desde el mensaje del 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
```

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

**Sugerencia 2**: El nombre de usuario predeterminado es **admin** y password <password>. El proceso de restablecimiento de 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

## Configurar 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 ejecutar el comando **commit** para guardar los cambios.

**Nota:** El modo se configura en **dedicado** cuando se utiliza el puerto de administración.

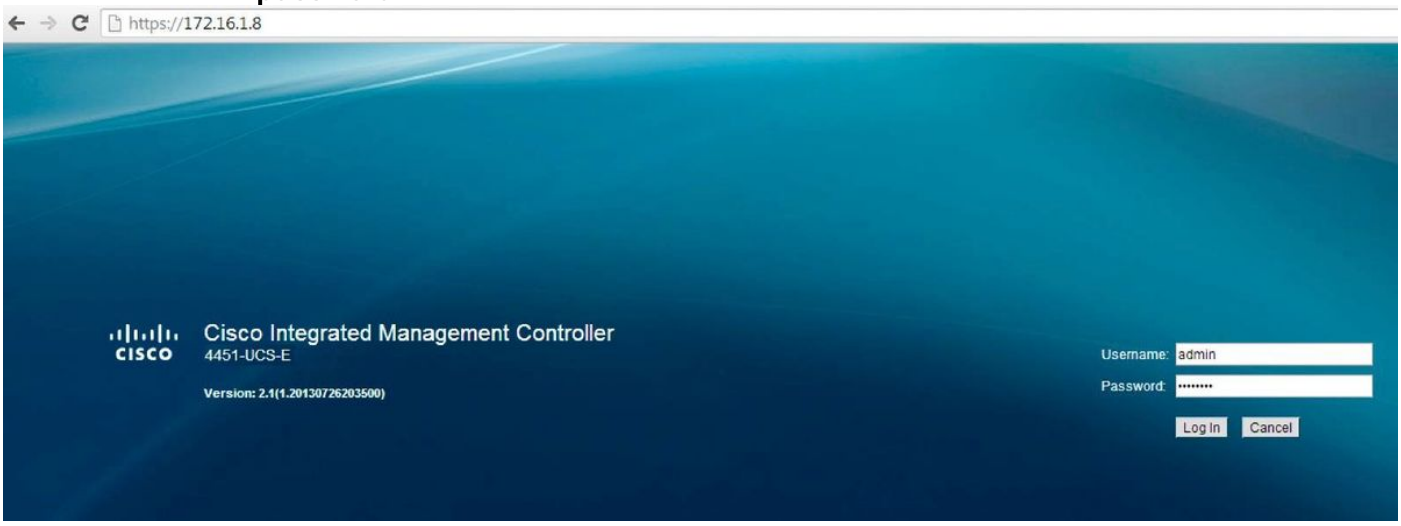
Ejecute el comando **show detail** para verificar la configuración detallada:

```
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 #
```

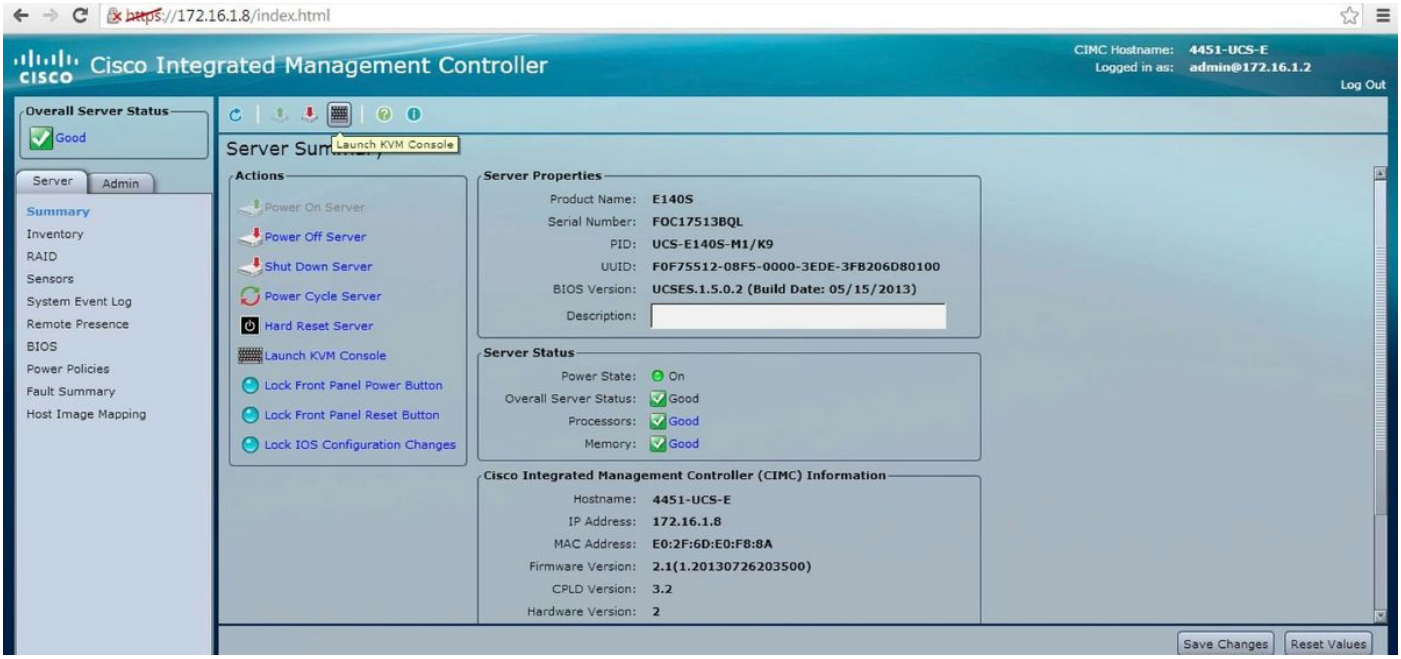
Inicie la interfaz web del CIMC desde un navegador con el nombre de usuario y la contraseña predeterminados como se muestra en la imagen. El nombre de usuario y la contraseña predeterminados son:

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

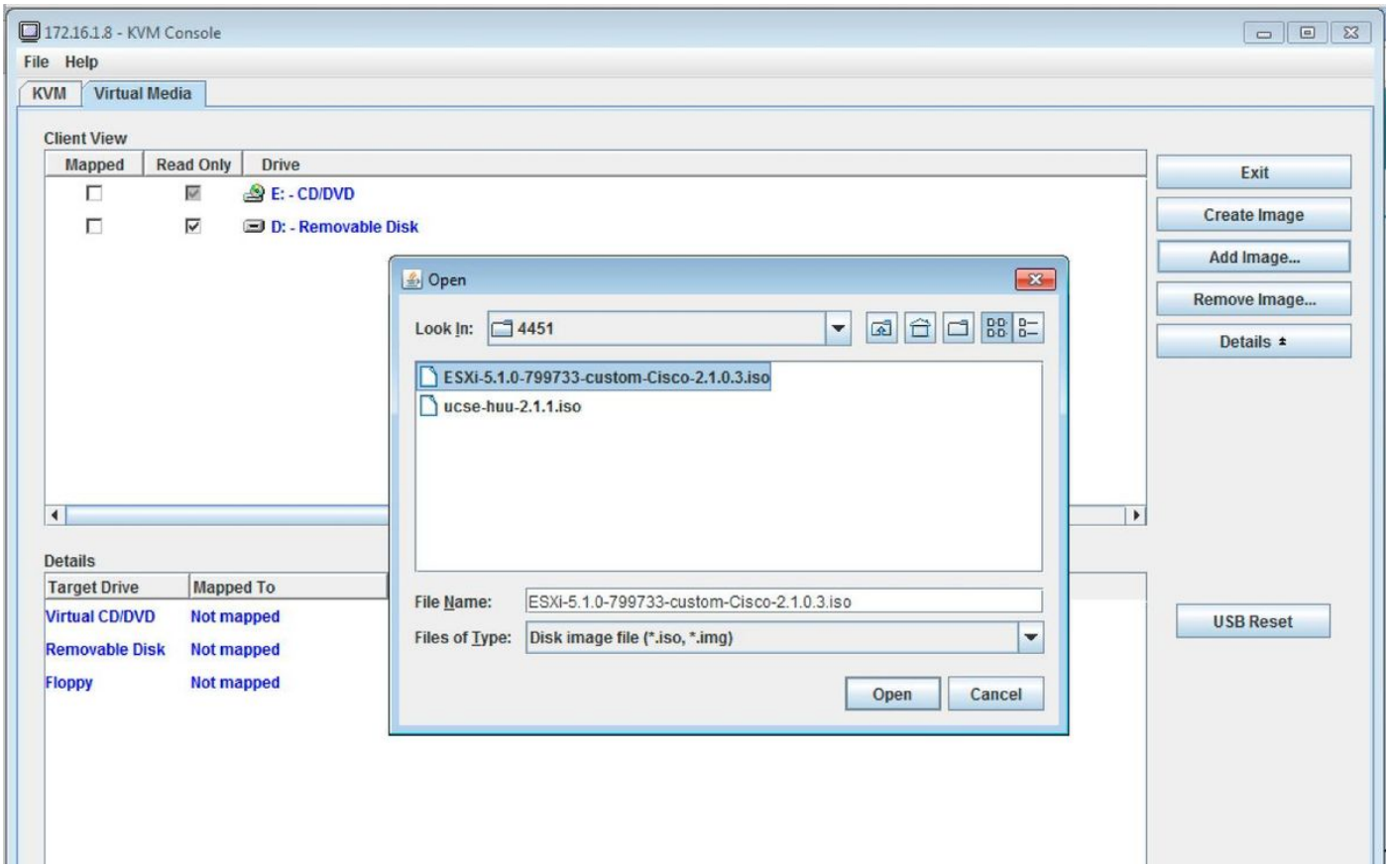



## Instalación de ESXi

Después de iniciar sesión en la interfaz de usuario del CIMC, podrá ver una página similar a la que se muestra en esta imagen. Haga clic en el icono **Iniciar consola KVM**, haga clic en **agregar imagen** y, a continuación, asigne el ISO de ESXi como medio virtual:



Haga clic en la ficha **Virtual Media** y luego haga clic en **Add Image** para asignar los medios virtuales como se muestra en la imagen.




Después de mapear el medio virtual, haga clic en **Power Cycle Server** desde la página de inicio de CIMC para apagar y encender el UCS-E. La configuración de ESXi se inicia desde los medios virtuales. Complete la instalación de ESXi.

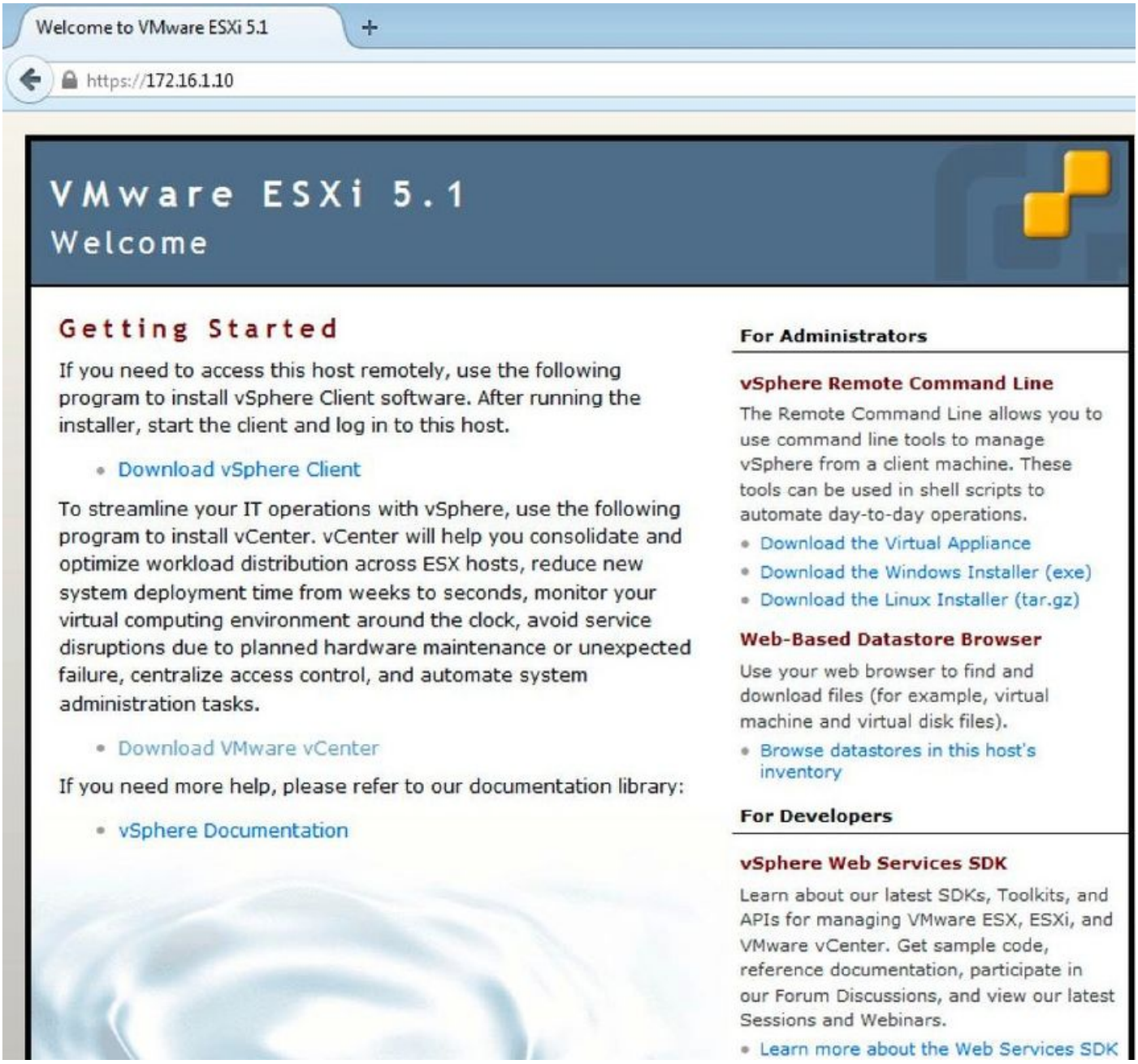
> **Nota:** Registre la dirección IP, el nombre de usuario y la contraseña de ESXi para futuras referencias.

## Instalación del cliente vSphere

En esta sección se describe cómo instalar el cliente vSphere.

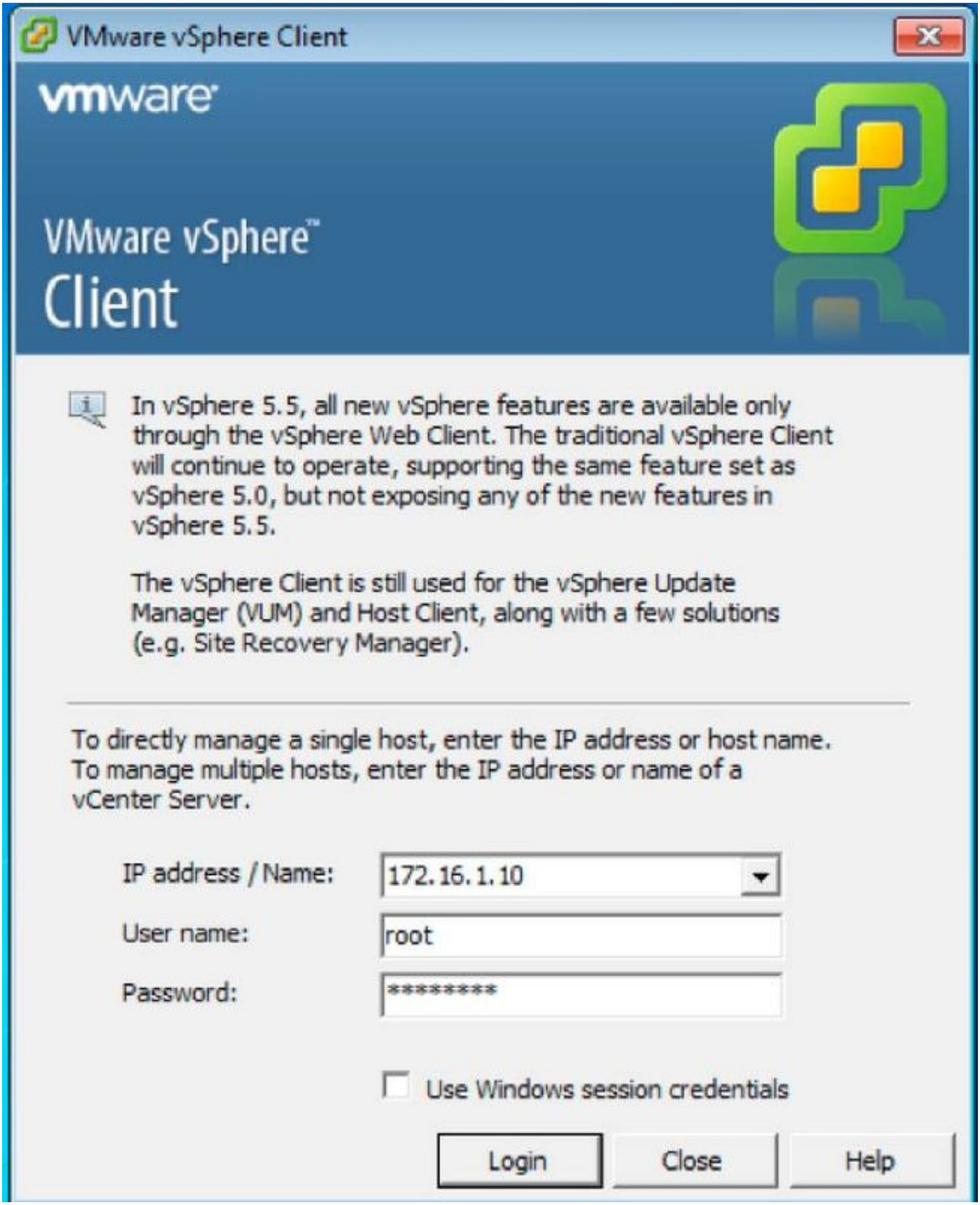
### Descargar cliente vSphere

Inicie ESXi y use el enlace **Download VSphere Client** para descargar el cliente vSphere. Instálelo en el ordenador.




### Iniciar cliente vSphere

Inicie vSphere Client desde su equipo. Inicie sesión con el nombre de usuario y la contraseña que creó durante la instalación y como se muestra en la imagen:




**Implemente FireSIGHT Management Center y dispositivos FirePOWER**

Complete los procedimientos descritos en el documento Implementación de FireSIGHT Management Center en VMware ESXi Cisco para implementar un FireSIGHT Management Center en ESXi.

**Nota:** El proceso que se utiliza para implementar un dispositivo NGIPSv FirePOWER es similar al proceso que se utiliza para implementar un centro de administración.

## Interfaces

En el UCS-E de doble ancho, hay cuatro interfaces:

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

En el UCS-E de ancho único, hay tres interfaces:

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

Las dos interfaces UCS-E del ISR4K son puertos troncales.

Los modelos UCS-E 120S y 140S cuentan con tres adaptadores de red y puertos de gestión:

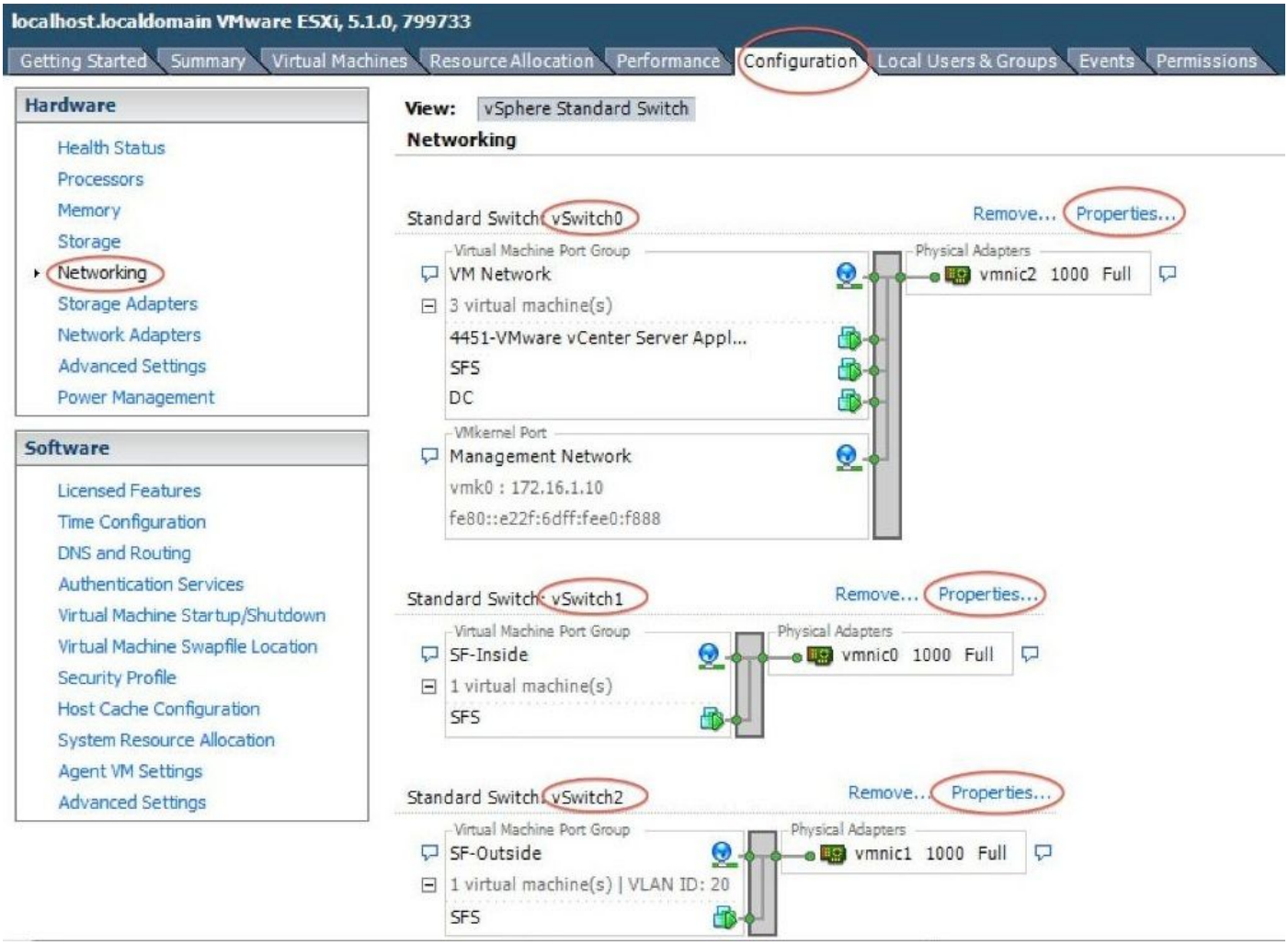
- El *vmnic0* se asigna a *UCSEx/0/0* en la placa de interconexiones del router
- El *vmnic1* se asigna a *UCSEx/0/1* en la placa de interconexiones del router
- El *vmnic2* se asigna a la interfaz GE2 del plano frontal UCS-E
- El puerto de gestión (M) del panel frontal sólo se puede utilizar para el CIMC.

Los modelos UCS-E 140D, 160D y 180D cuentan con cuatro adaptadores de red:

- El *vmnic0* se asigna a *UCSEx/0/0* en la placa de interconexiones del router.
- El *vmnic1* se mapea a *UCSEx/0/1* en la placa de interconexiones del router.
- El *vmnic2* se asigna a la interfaz GE2 del plano frontal UCS-E.
- El *vminc3* se asigna a la interfaz GE3 del plano frontal UCS-E.
- El puerto de gestión (M) del panel frontal sólo se puede utilizar para el CIMC.

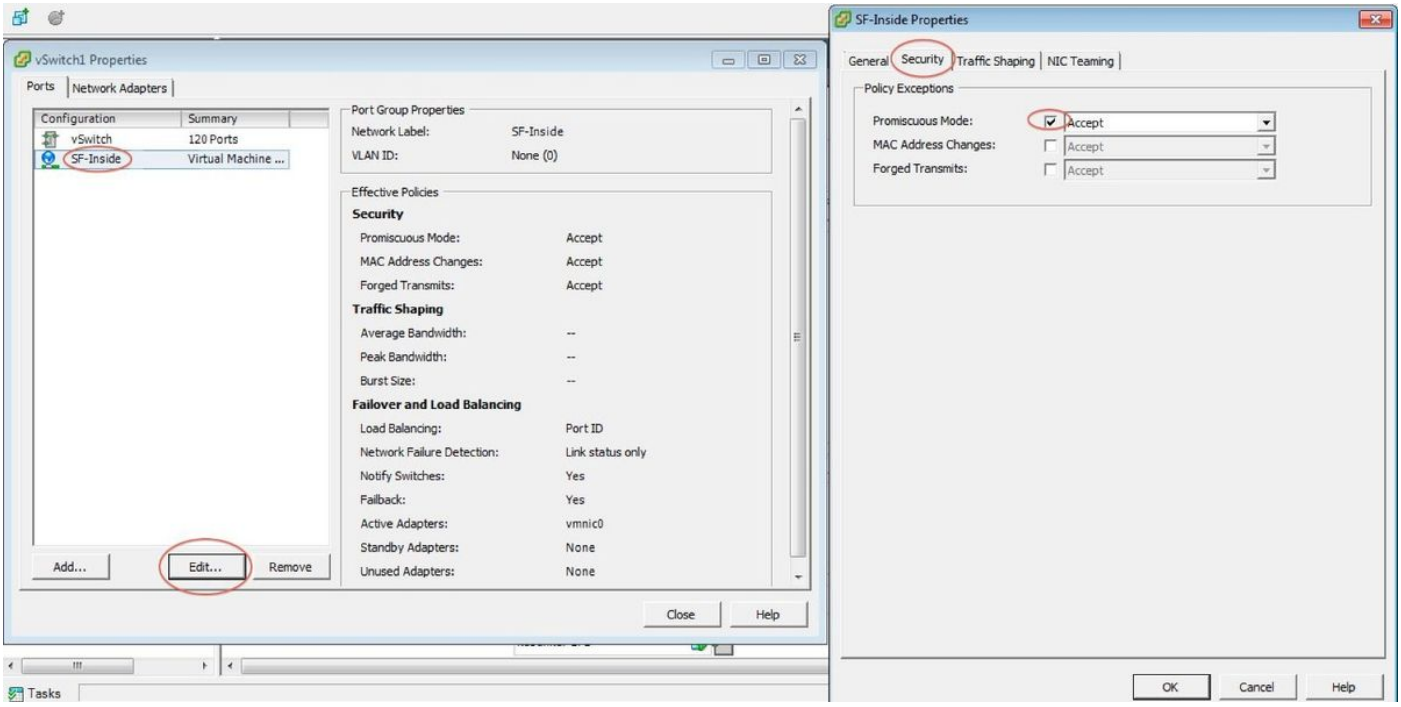
### Interfaces vSwitch en ESXi

El vSwitch0 en el ESXi es la interfaz de administración a través de la cual ESXi, FireSIGHT Management Center y el dispositivo NGIPSv FirePOWER se comunican a la red. Haga clic en **Properties** para vSwitch1 (SF-Inside) y vSwitch2 (SF-Outside) para realizar cualquier cambio.



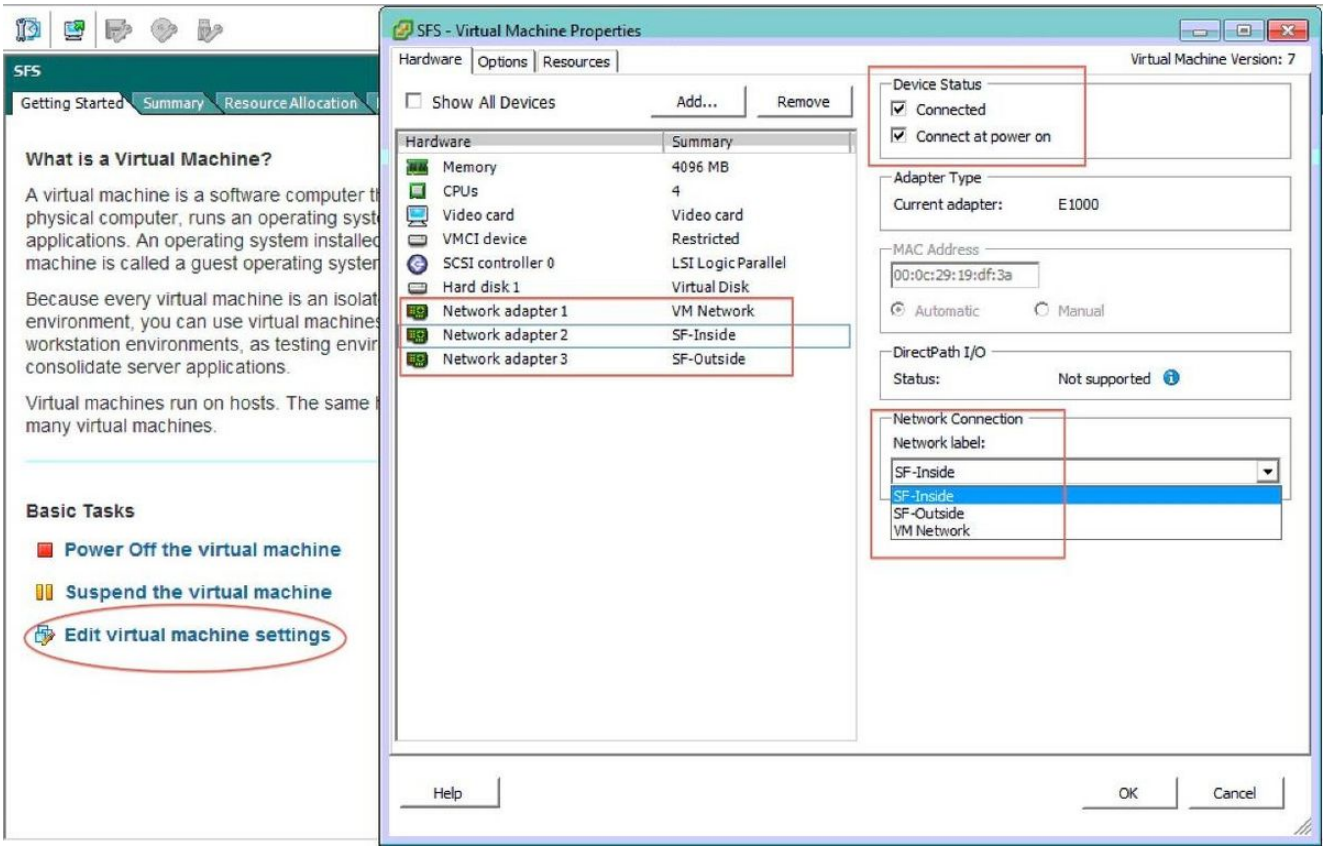

Esta imagen muestra las propiedades del vSwitch1 (debe completar los mismos pasos para el vSwitch2):

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




La configuración de vSwitch en el ESXi ha finalizado. Ahora debe verificar la configuración de la interfaz:

1. Vaya a la máquina virtual para el dispositivo FirePOWER.
2. Haga clic en **Editar configuración de máquina virtual**.
3. Verifique los tres adaptadores de red.
4. Asegúrese de que se han elegido correctamente, como se muestra en la imagen aquí:




## Registre el dispositivo FirePOWER con FireSIGHT Management Center

Complete los procedimientos descritos en el documento de Cisco para registrar un dispositivo FirePOWER con FireSIGHT Management Center.

# Redirigir y verificar el tráfico

Utilize esta sección para confirmar que su configuración funcione correctamente.

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

## Redirigir el tráfico de ISR a sensor en UCS-E

Utilice esta información para redirigir 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
```

> **Nota:** Si actualmente ejecuta la versión 3.16.1 o posterior, ejecute el comando **utd engine advanced** en lugar del comando **utd**.

## Verificar redirección de paquetes

Desde la consola ISR, ejecute este comando para verificar si los contadores de paquetes aumentan:

```
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

Puede ejecutar estos comandos **show** para verificar que su configuración funcione correctamente:

- **show plat software utd global**
- **show plat software utd interfaces**
- **show plat software utd rp active global**
- **show plat software utd fp active global**
- **show plat hardware qfp active feature utd stats**
- **show platform hardware qfp active feature utd**

# Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Puede ejecutar estos comandos **debug** para resolver problemas de su configuración:

- **debug platform condition feature utd controller plane**
- **debug platform condition feature utd dataplane submode**

# Información Relacionada

- Guía de introducción para los servidores Cisco UCS serie E y Cisco UCS serie E Network Compute Engine, versión 2.x
- Guía de solución de problemas de los servidores Cisco UCS serie E y el motor informático de red Cisco UCS serie E
- Guía de introducción para los servidores Cisco UCS serie E y Cisco UCS serie E Network Compute Engine, versión 2.x: actualización del firmware
- Guía de Configuración de Software de Routers de Servicios de Agregación de la Serie ASR 1000 de Cisco - Configuración de Interfaces de Dominio de Bridge
- Guía del usuario de la utilidad de actualización de host para los servidores Cisco UCS serie E y el motor de cálculo de red Cisco UCS serie E: actualización del firmware en los servidores Cisco UCS serie E
- Soporte Técnico y Documentación - Cisco Systems