Configurar serviços de FirePOWER em um dispositivo ISR com uma lâmina UCS-E

Índice

Introdução

Este documento descreve como instalar e distribuir o software de Cisco FirePOWER em uma plataforma da lâmina da série do Cisco Unified Computing System E (UCS-E) no modo do sistema de detecção de Instusion (IDS). O exemplo de configuração que é descrito neste documento é um suplemento ao Guia do Usuário oficial.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Imagem 3.14 do Roteadores dos Serviços integrados de Cisco (ISR) XE ou mais atrasado
- Versão 2.3 ou mais recente do controlador do gerenciamento integrado de Cisco (CIMC)
- Versão 5.2 ou mais recente do centro de gerenciamento de Cisco FireSIGHT (FMC)
- Versão 5.2 ou mais recente do dispositivo virtual de Cisco FirePOWER (NGIPSv)
- Versão 5.0 ou mais recente de VMware ESXi

Note: Antes que você promova o código à versão 3.14 ou mais recente, assegure-se de que o sistema tenha a memória suficiente, o espaço de disco, e uma licença para a elevação. Refira o exemplo 1: Copie a imagem para piscar: da seção do servidor TFTP do documento Cisco dos *procedimentos de upgrade de software dos roteadores de acesso* a fim aprender mais sobre upgrades de código.

A fim promover o CIMC, BIOS, e outros componentes de firmware, você pode usar ou Cisco hospeda a utilidade da elevação (HUU), ou você pode promover os componentes de firmware manualmente. A fim aprender mais sobre a upgrade de firmware, refira o melhoramento do firmware na seção dos server das E-séries de Cisco UCS do *Guia do Usuário de serviço público da elevação do host para server das E-séries de Cisco UCS e o motor do cálculo da rede das E-séries de Cisco UCS*.

Informações de Apoio

Esta seção fornecem a informação sobre as Plataformas de hardware suportado, as licenças, e as limitações com respeito aos componentes e aos procedimentos que são descritos neste documento.

Plataformas de hardware suportado

Esta seção alista as Plataformas de hardware suportado para o G2 e os dispositivos do 4000 Series.

Dispositivos ISR G2 com lâminas UCS-E

Estes dispositivos do G2 Series ISR com as lâminas da série UCS-E são apoiados:

Produto	Plataforma	Modelo UCS-E
Cisco 2900 Series ISR	2911	Única opção larga UCS-E 120/140
	2921	Opção larga simples ou duplo UCS-E 120/140/160/180
	2951	Opção larga simples ou duplo UCS-E 120/140/160
Cisco 3900 Series ISR	3925	UCS-E única e opção larga dobro de 120/140/160 ou 180 largos dobro
	3925E	UCS-E única e opção larga dobro de 120/140/160 ou 180 largos dobro
	3945	UCS-E única e opção larga dobro de 120/140/160 ou 180 largos dobro
	3945E	UCS-E única e opção larga dobro de 120/140/160 ou 180 largos dobro

Dispositivos ISR 4000 com lâminas UCS-E

Estes dispositivos do 4000 Series ISR com as lâminas da série UCS-E são apoiados:

Produto	Plataforma	Modelo UCS-E
Cisco 4400 Series ISR	4451	UCS-E única e opção larga dobro de 120/140/160 ou 180 largos dobro
	4431	Módulo de interface de rede UCS-E
Cisco 4300 Series ISR	4351	UCS-E única e opção larga dobro de 120/140/160/180 ou 180 largos d
	4331	Única opção larga UCS-E 120/140
	4321	Módulo de interface de rede UCS-E

Licenças

O ISR deve ter uma licença da Segurança K9, assim como uma licença do *appx*, a fim permitir o serviço.

Limitações

Estão aqui duas limitações com respeito à informação que é descrita neste documento:

- O Multicast não é apoiado.
- Somente 4,096 relações do domínio de Bridge (BDI) são apoiadas para cada sistema.

Os BDI não apoiam estas características:

- Protocolo bidirecional da detecção da transmissão (BFD)
- Netflow
- Quality of Service (QoS)
- Network-Based Application Recognition (NBAR) ou codificação video avançada (AVC)
- A zona baseou o Firewall (ZBF)
- VPN criptograficamente
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) sobre os Ethernet (PPPoE)

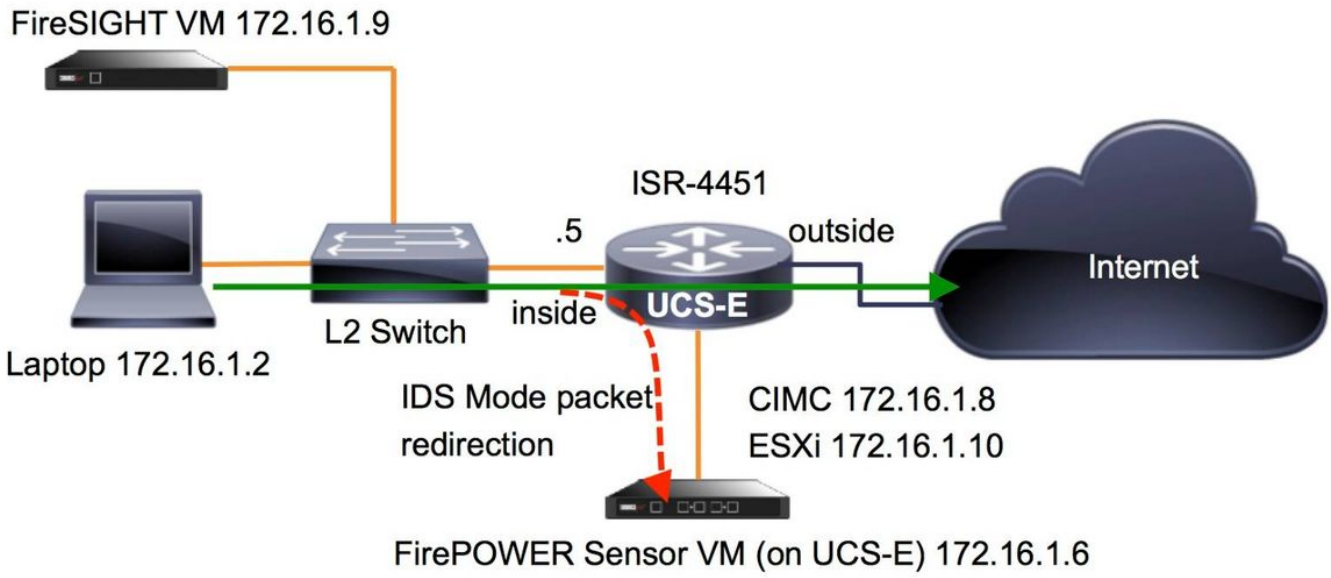
Note: Para um BDI, o tamanho da unidade de transmissão máxima (MTU) pode ser configurado com qualquer valor entre 1,500 e 9,216 bytes.

Configurar

Esta seção descreve como configurar os componentes que são envolvidos com este desenvolvimento.

Diagrama de Rede

A configuração que é descrita neste documento usa esta topologia de rede:



Trabalhos para serviços de FirePOWER em UCS-E

Estão aqui os trabalhos para os serviços de FirePOWER que são executado em um UCS-E:

1. O data-plano empurra o tráfego para a inspeção para fora da relação BDI/UCS-E (trabalhos para dispositivos G2 e de G3 Series).

2. O Cisco IOS XE CLI ativa o redirecionamento de pacote para a análise (opções para todas as relações ou interface per.).

3. O script de inicialização da *instalação do* sensor CLI simplifica a configuração.

Configurar o CIMC

Esta seção descreve como configurar o CIMC.

Conecte ao CIMC

Há umas formas múltiplas conectar ao CIMC. Neste exemplo, a conexão ao CIMC é terminada

através de uma porta do gerenciamento dedicado. Assegure-se de que você conecte a porta **M** (dedicada) à rede com o uso de um cabo do Ethernet. Uma vez que conectado, incorpore o comando do **subslot do módulo HW da** alerta de roteador:

```
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
```

Tip: A fim retirar, incorpore **^a^q.**

Configurar o CIMC

Use esta informação a fim terminar a configuração do 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
```

Caution: Assegure-se de que você inscreva o **comando commit** a fim salvar as mudanças.

Note: *O modo* está ajustado **dedicado** quando a porta de gerenciamento é usada.

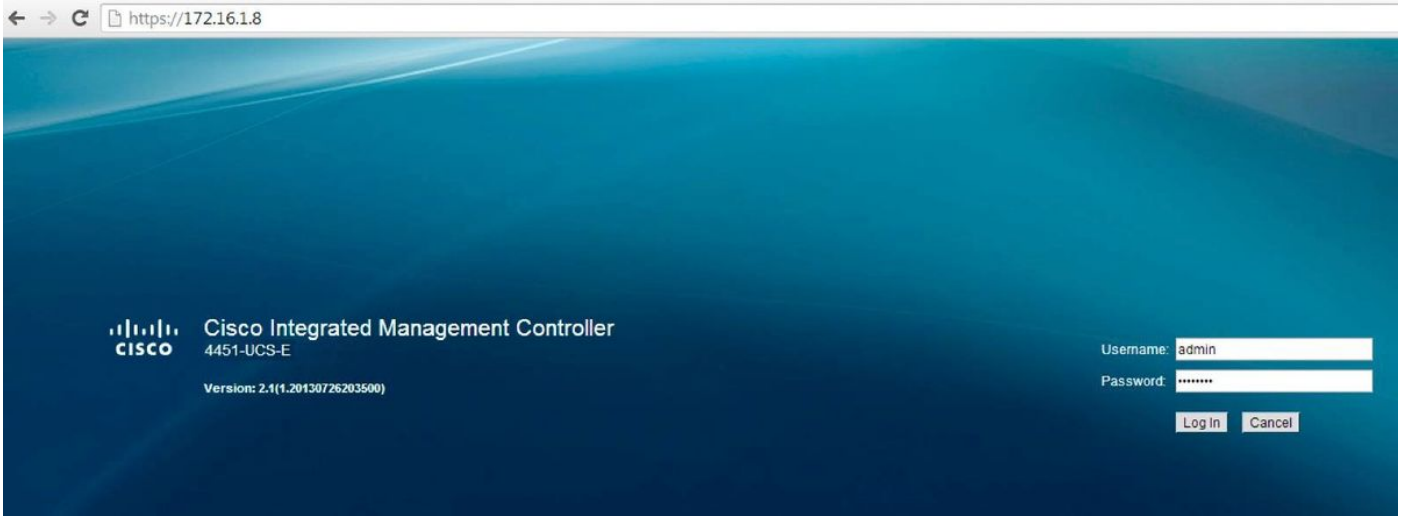
Inscreva o **comando detail da mostra** a fim verificar os ajustes do detalhe:

```
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 #
```

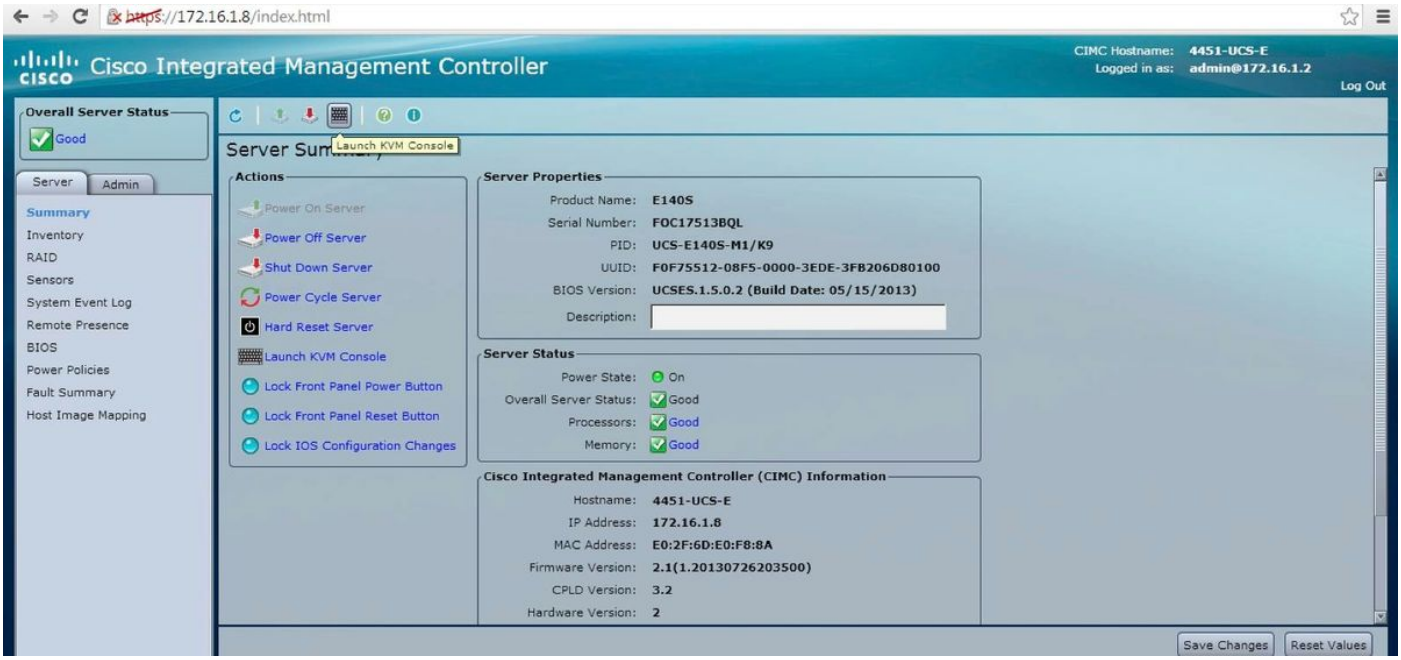
Lance a interface da WEB do CIMC de um navegador com o nome de usuário padrão e a senha. O nome de usuário padrão e a senha são:

- Nome de usuário: **admin**
- Senha: **senha**

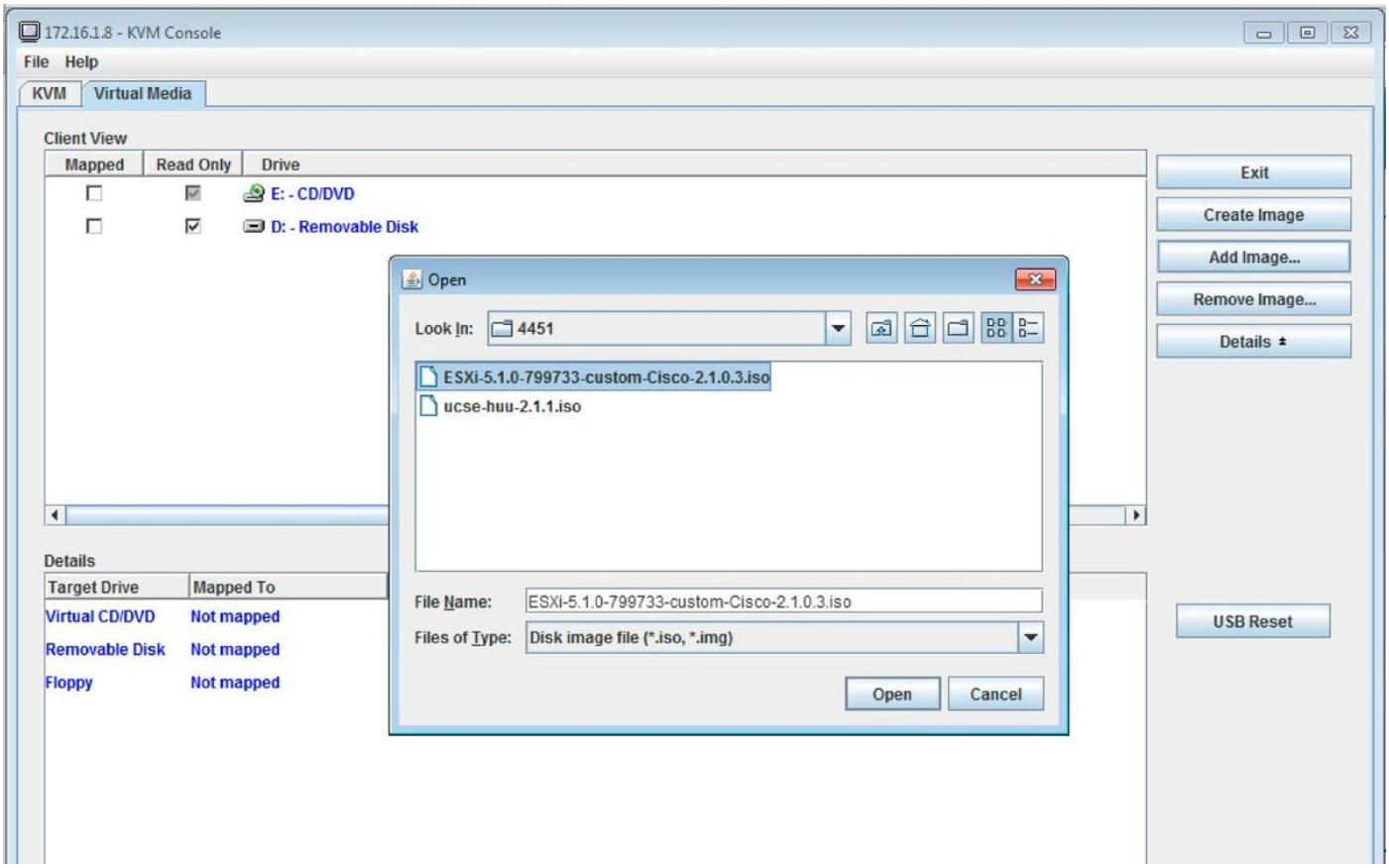


Instale ESXi

Depois que você registra na interface do utilizador do CIMC, você pode ver uma página similar àquela mostrada na imagem seguinte. Clique o ícone do **console do lançamento KVM**, o clique **adiciona a imagem**, e traça então o ESXi ISO como os media virtuais:



Clique a aba dos **Meios virtuais**, e clique-a então **adicionam a imagem** a fim traçar os media virtuais:



Depois que o media virtual é traçado, clique o **server do ciclo da potência do** ciclo de energia do Home Page CIMC o UCS-E. A instalação de ESXi lança-se dos media virtuais. Termine o ESXi instalam.

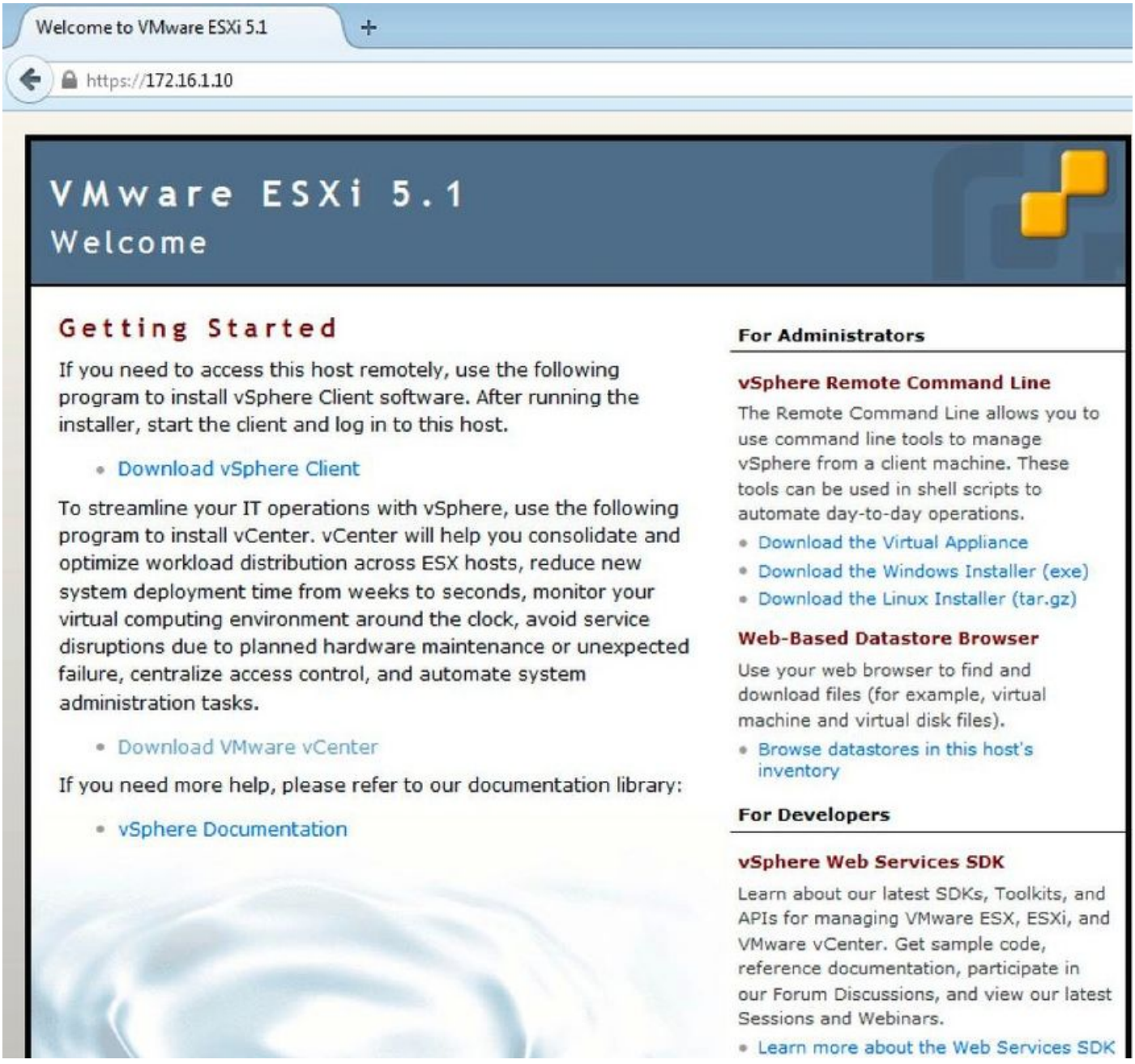
> **Note**: Grave o *endereço IP de Um ou Mais Servidores Cisco ICM NT de ESXi*, o *username*, e a *senha* para a referência futura.

Instale o cliente do vSphere

Esta seção descreve como instalar o cliente do vSphere.

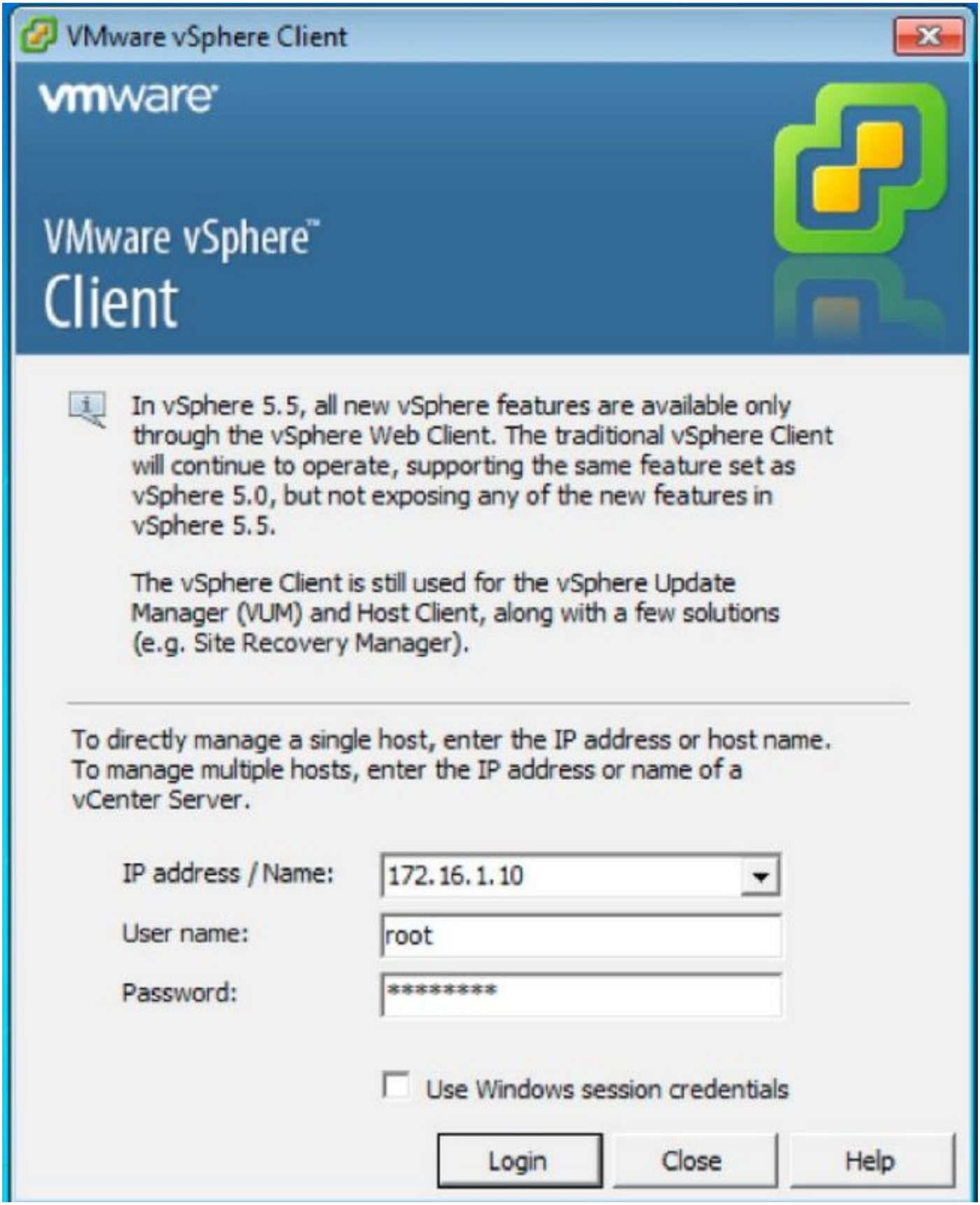
Transfira o cliente do vSphere

Lance ESXi e use o link do **cliente de VSphere da transferência** a fim transferir o cliente do vSphere. Instale-o em seu computador.



Lance o cliente do vSphere

Lance o cliente do vSphere de seu computador. Entre com o nome de usuário e senha que você criou durante a instalação:



Distribua o centro de gerenciamento de FireSIGHT e os dispositivos de FirePOWER

Termine os procedimentos que são descritos no desenvolvimento do centro de gerenciamento de FireSIGHT no documento Cisco de VMware ESXi a fim distribuir um centro de gerenciamento de FireSIGHT no ESXi.

Note: O processo que é usado a fim distribuir um dispositivo de FirePOWER NGIPSv é similar ao processo que é usado a fim distribuir um centro de gerenciamento.

Configurar as relações

No UCS-E dual-wide, há quatro relações:

- A relação a mais alta do MAC address é Gi3 no painel dianteiro.
- A segunda relação a mais alta do MAC address é Gi2 no painel dianteiro.
- Os últimos dois que aparecem são as interfaces internas.

No UCS-E single-wide, há três relações:

- A relação a mais alta do MAC address é Gi2 no painel dianteiro.
- Os últimos dois que aparecem são as interfaces internas.

Ambas as relações UCS-E no ISR4K são portas de tronco.

Os UCS-E 120S e 140S têm o adaptador de rede três mais portas de gerenciamento:

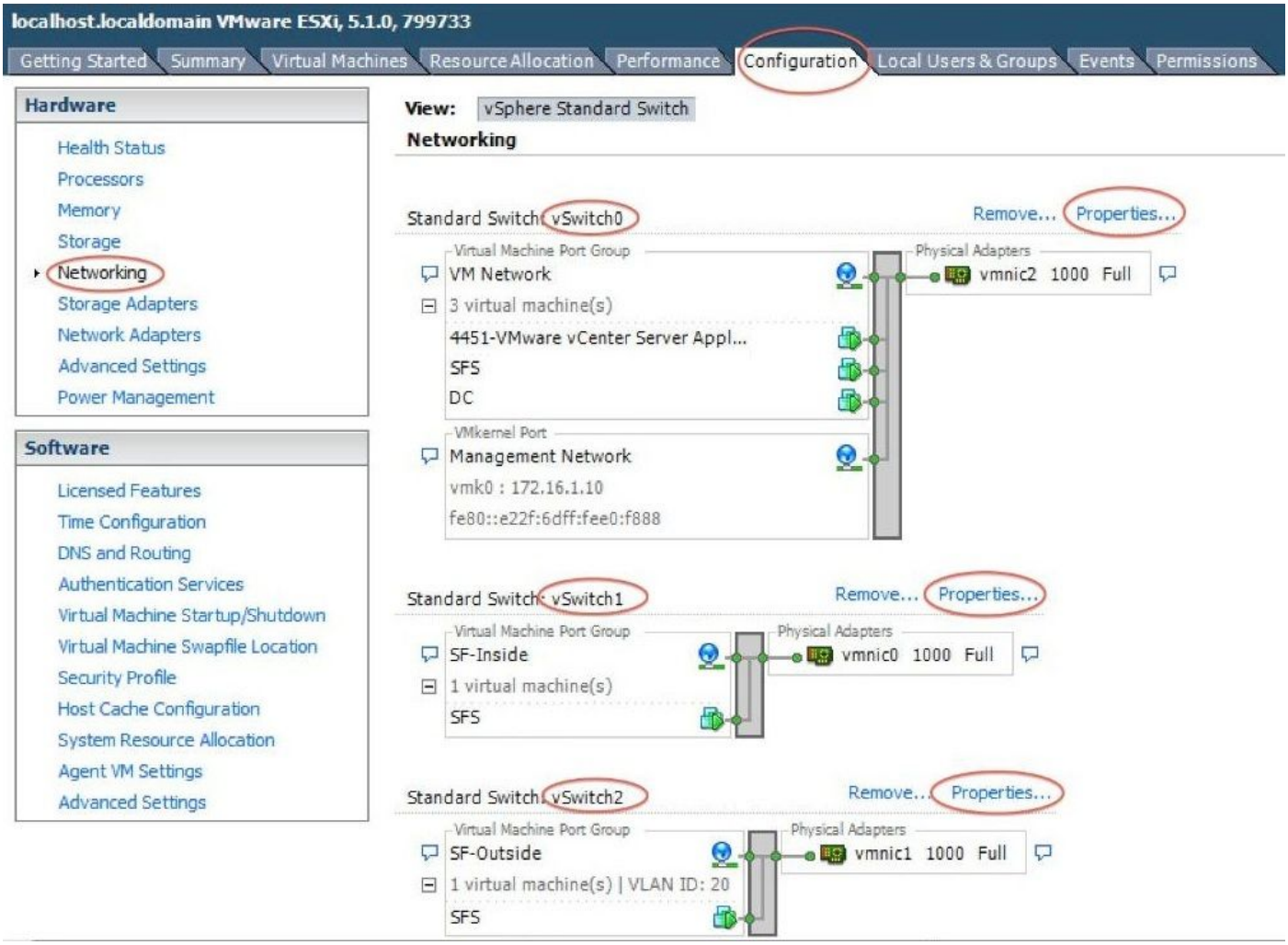
- *O vmnic0* é traçado a *UCSEx/0/0 no* backplane do roteador.
- *O vmnic1* é traçado a *UCSEx/0/1 no* backplane do roteador.
- *O vmnic2* é traçado à relação do plano GE2 da parte dianteira UCS-E.
- O Gerenciamento do painel frontal (M) a porta pode somente ser usada para o CIMC.

Os UCS-E 140D, 160D, e 180D têm quatro adaptadores de rede:

- *O vmnic0* é traçado a *UCSEx/0/0 no* backplane do roteador.
- *O vmnic1* é traçado a *UCSEx/0/1 no* backplane do roteador.
- *O vmnic2* é traçado à relação do plano GE2 da parte dianteira UCS-E.
- *O vminc3* é traçado à relação do plano GE3 da parte dianteira UCS-E.
- O Gerenciamento do painel frontal (M) a porta pode somente ser usada para o CIMC.

Configurar as relações do vSwitch no ESXi

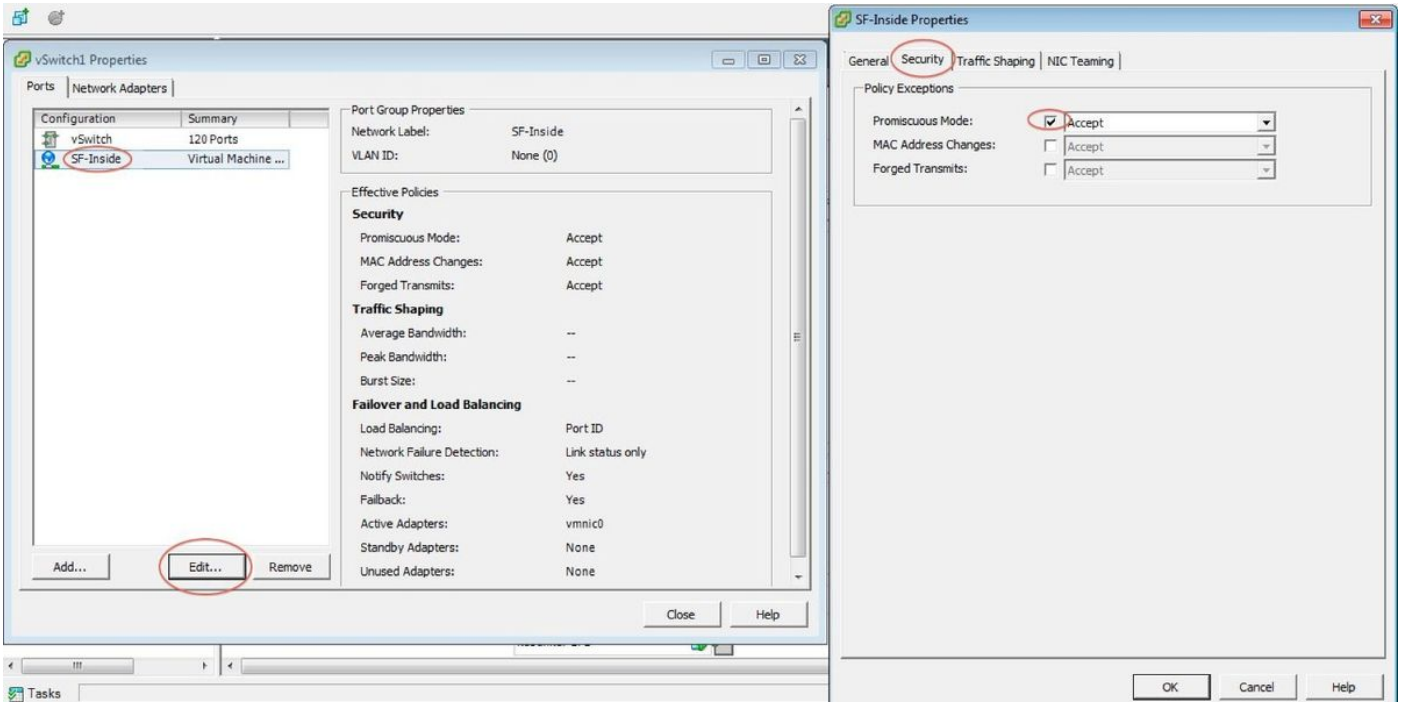
O vSwitch0 no ESXi é a interface de gerenciamento através de que o ESXi, o centro de gerenciamento de FireSIGHT, e o dispositivo de FirePOWER NGIPSv se comunicam à rede. **Propriedades do** clique para o vSwitch1 (SF-dentro de) e o vSwitch2 (SF-parte externa) a fim fazer a alguns mudanças.



Esta imagem mostra as propriedades do vSwitch1 (você deve terminar as mesmas etapas para o vSwitch2):

NOTE: Assegure-se de por favor que o ID de VLAN esteja configurado a 4095 para NGIPSv, isto esteja exigido de acordo com o documento de NGIPSv:

http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



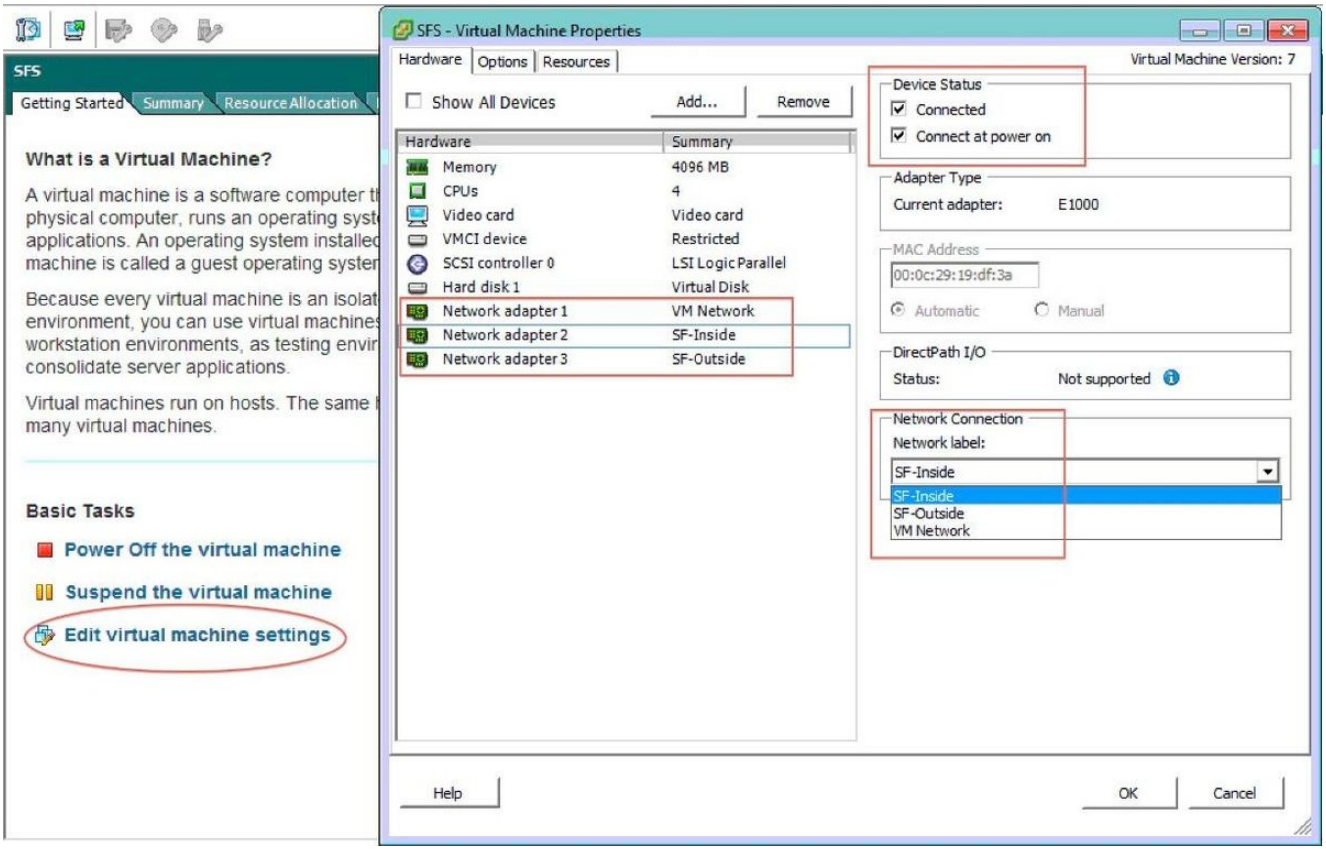
A configuração do vSwtich no ESXi está completa. Agora você deve verificar os ajustes da relação:

1. Navegue à máquina virtual para o dispositivo de FirePOWER.

2. O clique **edita ajustes da máquina virtual**.

3. Verifique todos os três adaptadores de rede.

4. Assegure-se de que estejam escolhidos corretamente, como mostrado aqui:



Registrar o dispositivo de FirePOWER com o centro de gerenciamento de FireSIGHT

Termine os procedimentos que são descritos no documento Cisco a fim registrar um dispositivo de FirePOWER com um centro de gerenciamento de FireSIGHT.

Reoriente e verifique o tráfego

Esta seção descreve como reorientar o tráfego e como verificar os pacotes.

Reoriente o tráfego do ISR ao sensor no UCS-E

Use esta informação a fim reorientar o tráfego:

```
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**: Se você executa atualmente a versão 3.16.1 ou mais recente, use o comando **avançado motor use até esgotar** em vez do comando **use até esgotar**.

Verifique o redirecionamento de pacote

Do console ISR, incorpore este comando a fim verificar se os contadores de pacote de informação incrementam:

```
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
```

Verificar

Você pode usar estes **comandos show** a fim verificar que sua configuração trabalha corretamente:

- **a mostra plat o use até esgotar do software global**
- **a mostra plat relações use até esgotar do software**
- **a mostra plat global ativo use até esgotar rp do software**
- **a mostra plat global ativo use até esgotar fp do software**
- **a mostra plat o stats ativo use até esgotar da característica do qfp do hardware**
- **mostre a qfp do hardware da plataforma o use até esgotar ativo da característica**

Troubleshooting

Você pode usar estes **comandos debug** a fim pesquisar defeitos sua configuração:

- **debugar o controlplane use até esgotar da característica da condição da plataforma**
- **debugar o submode do dataplane use até esgotar da característica da condição da plataforma**

Informações Relacionadas

- Obtendo o guia começado para server das E-séries de Cisco UCS e o motor do cálculo da rede das E-séries de Cisco UCS, libere 2.x
- Guia de Troubleshooting para server das E-séries de Cisco UCS e o motor do cálculo da rede das E-séries de Cisco UCS
- Obtendo o guia começado para server das E-séries de Cisco UCS e o motor do cálculo da rede das E-séries de Cisco UCS, libere 2.x – promovendo o firmware
- Manual de configuração do software do Roteadores de serviços de agregação Cisco ASR série 1000 – Configurando relações do domínio de Bridge
- Guia do Usuário de serviço público da elevação do host para server das E-séries de Cisco UCS e o motor do cálculo da rede das E-séries de Cisco UCS – promovendo o firmware em server das E-séries de Cisco UCS
- Suporte Técnico e Documentação - Cisco Systems