

Configurar o FirePOWER Services no dispositivo ISR com blade UCS-E

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Plataformas de hardware suportadas](#)

[Dispositivos ISR G2 com blades UCS-E](#)

[Dispositivos ISR 4000 com blades UCS-E](#)

[Licenças](#)

[Limitações](#)

[Configurar](#)

[Diagrama de Rede](#)

[Fluxo de trabalho dos FirePOWER Services no UCS-E](#)

[Configurar o CIMC](#)

[Conectar ao CIMC](#)

[Configurar o CIMC](#)

[Instalar o ESXi](#)

[Instalar o vSphere Client](#)

[Fazer download do vSphere Client](#)

[Iniciar o vSphere Client](#)

[Implante o FireSIGHT Management Center e os dispositivos FirePOWER](#)

[Interfaces](#)

[Interfaces do vSwitch no ESXi](#)

[Registre o dispositivo FirePOWER com o FireSIGHT Management Center](#)

[Redirecionar e verificar o tráfego](#)

[Redirecionar tráfego do ISR para o sensor no UCS-E](#)

[Verificar o redirecionamento de pacote](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como instalar e implantar o software Cisco FirePOWER em uma plataforma blade Cisco Unified Computing System E Series (UCS-E) no modo IDS (Intrusion Detection System). O exemplo de configuração descrito neste documento é um suplemento ao guia oficial do usuário.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Imagem do Cisco Integrated Services Routers (ISR) XE 3.14 ou posterior
- Cisco Integrated Management Controller (CIMC) versão 2.3 ou posterior
- Cisco FireSIGHT Management Center (FMC) versão 5.2 ou posterior
- Cisco FirePOWER Virtual Device (NGIPSv) versão 5.2 ou posterior
- VMware ESXi versão 5.0 ou 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Note: Antes de atualizar o código para a versão 3.14 ou posterior, verifique se o sistema tem memória suficiente, espaço em disco e uma licença para a atualização. Consulte o [Exemplo 1: Copie a imagem para a flash: na seção do servidor TFTP](#) do documento Procedimentos de Upgrade de Software dos Roteadores de Acesso da Cisco para saber mais sobre atualizações de código.

Note: Para atualizar o CIMC, o BIOS e outros componentes de firmware, você pode usar o Cisco Host Upgrade Utility (HUU) ou atualizar os componentes do firmware manualmente. Para saber mais sobre a atualização do firmware, consulte a seção [Upgrading the Firmware on Cisco UCS E-Series Servers](#) do Host Upgrade Utility User Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.

Informações de Apoio

Esta seção fornece informações sobre as plataformas de hardware suportadas, licenças e limitações em relação aos componentes e procedimentos descritos neste documento.

Plataformas de hardware suportadas

Esta seção lista as plataformas de hardware suportadas para os dispositivos G2 e 4000 Series.

Dispositivos ISR G2 com blades UCS-E

Esses dispositivos ISR G2 Series com blades UCS-E Series são compatíveis:

Produto	Platform	Modelo UCS-E
ISR Cisco 2900 Series	2911	Opção UCS-E 120/140 single wide
	2921	Opção UCS-E 120/140/160/180 single ou double wide

ISR Cisco 3900 Series	2951	Opção UCS-E 120/140/160 single ou double wide
	3925	Opção UCS-E 120/140/160 single e double wide ou 180 double wide
	3925E	Opção UCS-E 120/140/160 single e double wide ou 180 double wide
	3945	Opção UCS-E 120/140/160 single e double wide ou 180 double wide
	3945E	Opção UCS-E 120/140/160 single e double wide ou 180 double wide

Dispositivos ISR 4000 com blades UCS-E

Esses dispositivos ISR 4000 Series com blades UCS-E Series são compatíveis:

Produto	Platform	Modelo UCS-E
ISR Cisco 4400 Series	4451	Opção UCS-E 120/140/160 single e double wide ou 180 double wide
	4431	Módulo de interface de rede UCS-E
	4351	Opção UCS-E 120/140/160/180 single e double wide ou 180 double wide
ISR Cisco 4300 Series	4331	Opção UCS-E 120/140 single wide
	4321	Módulo de interface de rede UCS-E

Licenças

O ISR deve ter uma licença K9 de segurança, bem como uma licença appx, para habilitar o serviço.

Limitações

Aqui estão as duas limitações em relação às informações descritas neste documento:

- Multicast não é compatível
- Apenas 4.096 BDI (Bridge Domain Interfaces) são suportadas para cada sistema

Os BDIs não suportam estes recursos:

- Protocolo Bidirectional Forwarding Detection (BFD)
- Netflow
- Quality of Service (QoS)
- Reconhecimento de aplicativos baseado em rede (NBAR) ou código de vídeo avançado (AVC)
- Firewall baseado em zona (ZBF)
- VPNs criptográficas
- Multiprotocol Label Switching (MPLS)
- Protocolo Ponto a Ponto (PPP - Point-to-Point Protocol) sobre Ethernet (PPPoE)

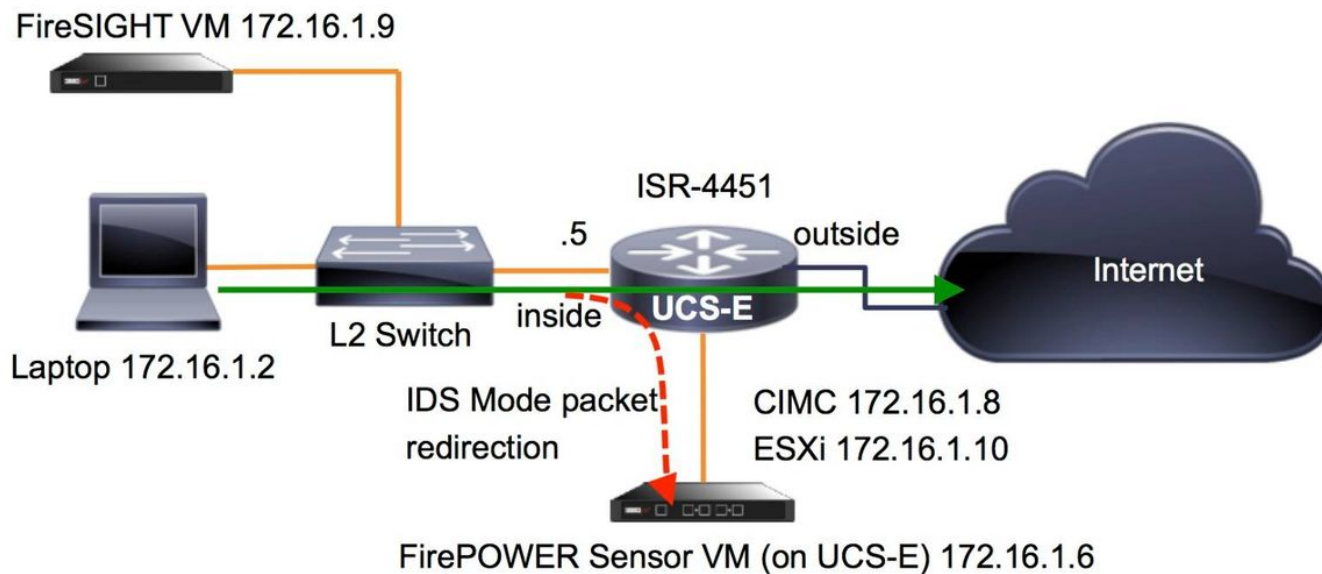
Note: Para um BDI, o tamanho da Unidade de Transmissão Máxima (MTU - Maximum Transmission Unit) pode ser configurado com qualquer valor entre 1.500 e 9.216 bytes.

Configurar

Esta seção descreve como configurar os componentes envolvidos com esta implantação.

Diagrama de Rede

A configuração descrita neste documento usa esta topologia de rede:



Fluxo de trabalho dos FirePOWER Services no UCS-E

Aqui está o fluxo de trabalho dos serviços FirePOWER executados em um UCS-E:

1. O plano de dados empurra o tráfego para fora da interface BDI/UCS-E (funciona para dispositivos G2 e G3 Series).
2. A CLI do Cisco IOS®-XE ativa o redirecionamento de pacotes para análise (opções para todas as interfaces ou por interface).
3. O script de inicialização **de configuração CLI** do sensor simplifica a configuração.

Configurar o CIMC

Esta seção descreve como configurar o CIMC.

Conectar ao CIMC

Há várias maneiras de se conectar ao CIMC. Neste exemplo, a conexão com o CIMC é concluída por meio de uma porta de gerenciamento dedicada. Certifique-se de conectar a porta **M** (dedicada) à rede com o uso de um cabo Ethernet. Depois de conectado, execute o comando **hw-module subslot** no prompt do 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

Dica 1: Para sair, execute **^a^q**.

Dica 2: O nome de usuário padrão é **admin** e password <password>. O processo de redefinição de senha está descrito aqui:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/3-1-1/guide/b_Getting_Started_Guide/b_3_x_Getting_Started_Guide_appendix_01011.html#GUID-73551F9A-4C79-4692-838A-F99C80E20A28

Configurar o CIMC

Use essas informações para concluir 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: Certifique-se de executar o comando **commit** para salvar as alterações.

Note: O modo é definido como **dedicado** quando a porta de gerenciamento é usada.

Execute o comando **show detail** para verificar as configurações detalhadas:

```
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**

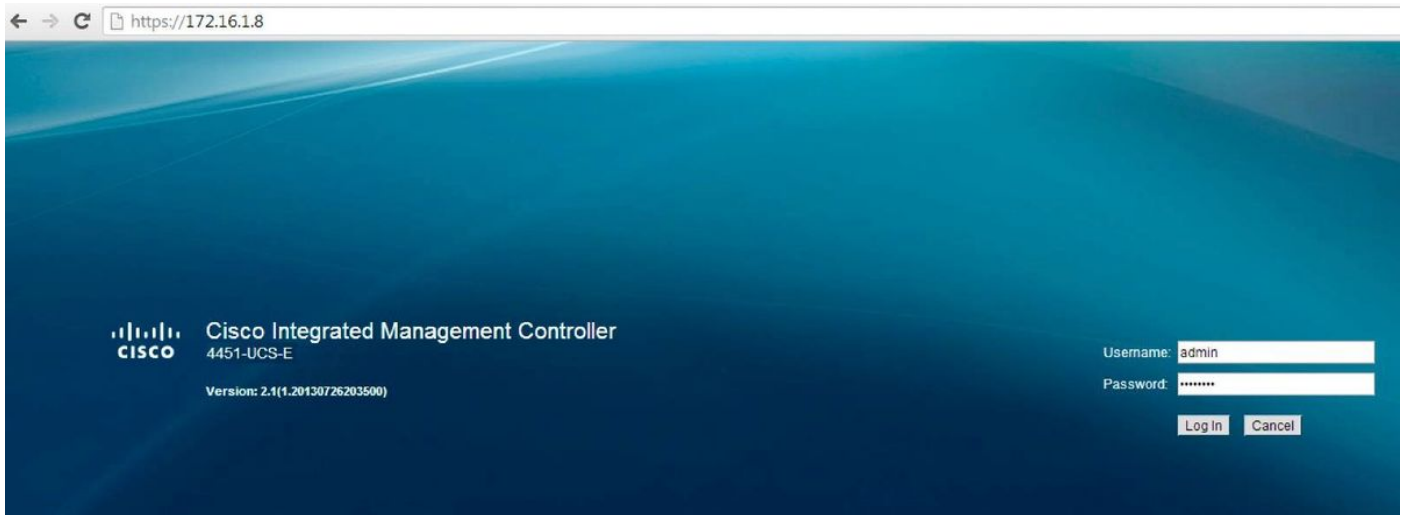
NIC Redundancy: **none**

NIC Interface: **console**

4451-UCS-E /cimc/network #

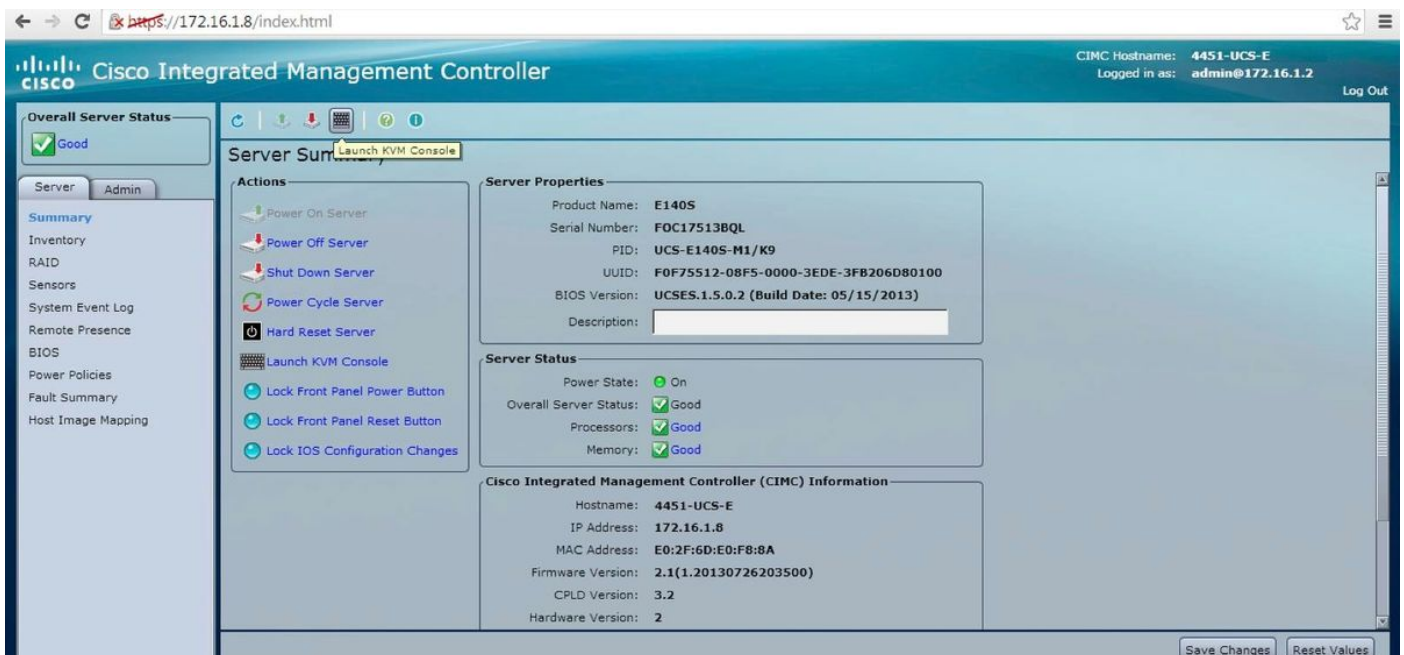
Inicie a interface da Web do CIMC a partir de um navegador com o nome de usuário e a senha padrão, como mostrado na imagem. O nome de usuário e a senha padrão são:

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

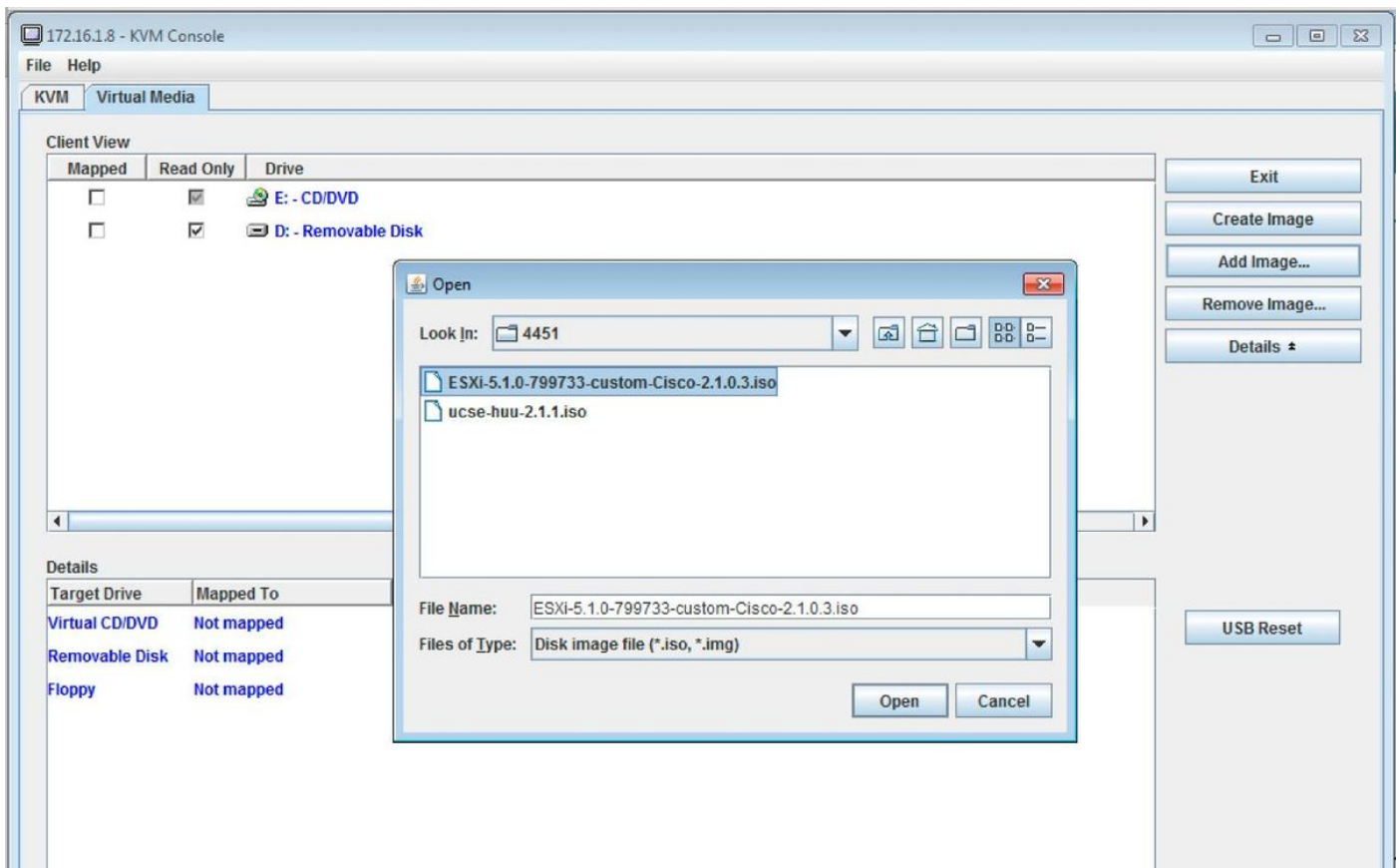


Instalar o ESXi

Depois de fazer login na interface de usuário do CIMC, você poderá visualizar uma página semelhante à mostrada nessa imagem. Clique no ícone **Iniciar console KVM**, clique em **adicionar imagem** e mapeie o ESXi ISO como a mídia virtual:



Clique na guia **Virtual Media** e, em seguida, clique em **Add Image** para mapear a mídia virtual como mostrado na imagem.



Depois que a mídia virtual for mapeada, clique em **Power Cycle Server** na página inicial do CIMC para executar o ciclo de energia do UCS-E. A configuração do ESXi é iniciada a partir da mídia virtual. Conclua a instalação do ESXi.

Note: Registre o endereço IP, o nome de usuário e a senha do ESXi para referência futura.

Instalar o vSphere Client

Esta seção descreve como instalar o cliente vSphere.

Fazer download do vSphere Client

Inicie o ESXi e use o link **Download vSphere Client** para fazer o download do cliente vSphere. Instale-o no computador.

Welcome to VMware ESXi 5.1

https://172.16.1.10

VMware ESXi 5.1

Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

- [Download vSphere Client](#)

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- [Download VMware vCenter](#)

If you need more help, please refer to our documentation library:

- [vSphere Documentation](#)

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- [Download the Virtual Appliance](#)
- [Download the Windows Installer \(exe\)](#)
- [Download the Linux Installer \(tar.gz\)](#)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- [Browse datastores in this host's inventory](#)

For Developers

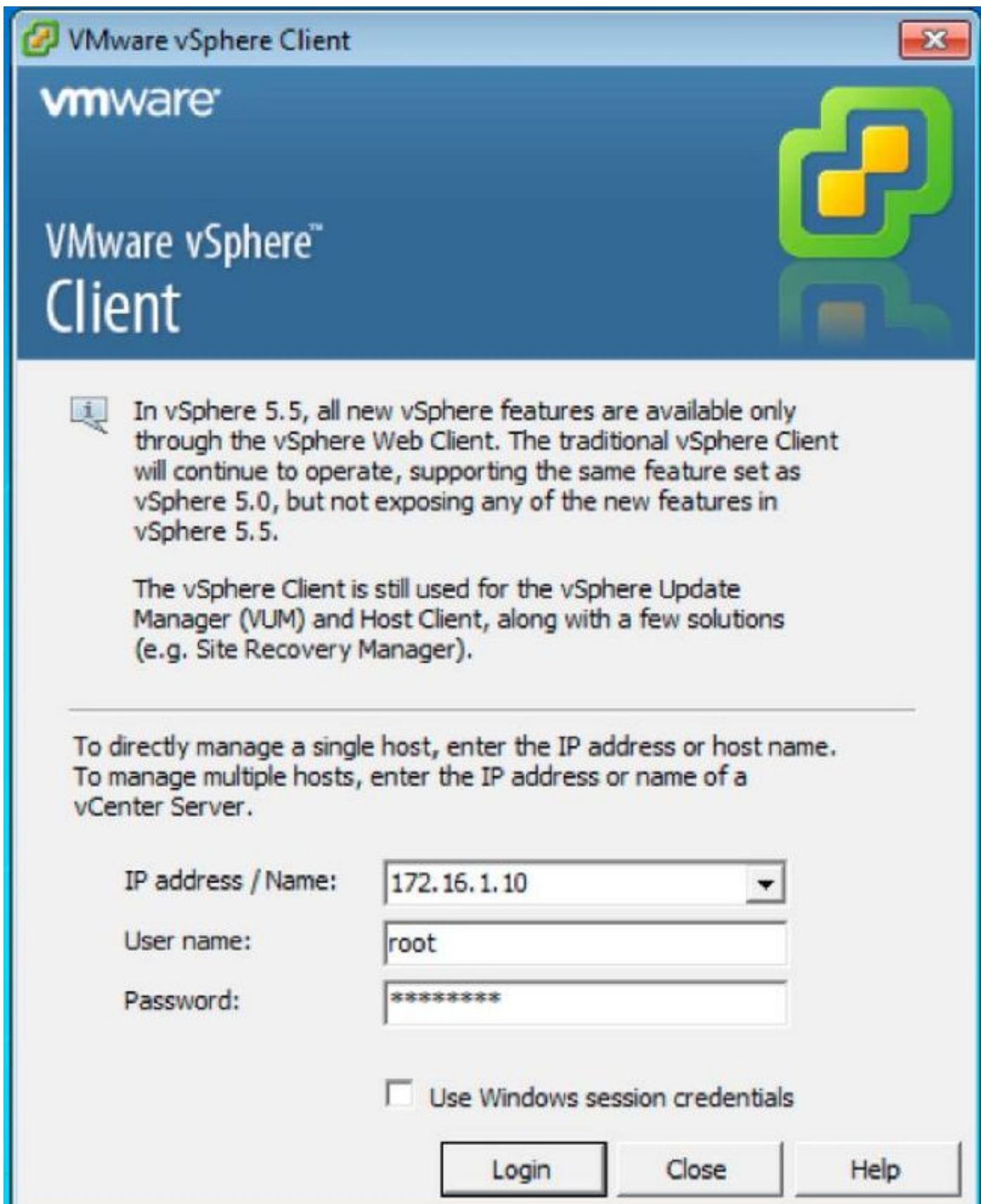
vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- [Learn more about the Web Services SDK](#)

Iniciar o vSphere Client

Inicie o vSphere Client do seu computador. Faça login com o nome de usuário e a senha que você criou durante a instalação e conforme mostrado na imagem:



Implante o FireSIGHT Management Center e os dispositivos FirePOWER

Conclua os procedimentos descritos no documento [Deployment of FireSIGHT Management Center on VMware ESXi](#) Cisco para implantar um FireSIGHT Management Center no ESXi.

Note: O processo usado para implantar um dispositivo FirePOWER NGIPSv é semelhante

ao processo usado para implantar um Management Center.

Interfaces

No UCS-E de largura dupla, há quatro interfaces:

- A interface de endereço MAC mais alta é Gi3 no painel frontal
- A segunda interface de endereço MAC mais alta é Gi2 no painel frontal
- As duas últimas que aparecem são as interfaces internas

No UCS-E Single-Wide, há três interfaces:

- A interface de endereço MAC mais alta é Gi2 no painel frontal
- As duas últimas que aparecem são as interfaces internas

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

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

- A *vmnic0* é mapeada para *UCSEx/0/0* no painel traseiro do roteador
- O *vmnic1* é mapeado para *UCSEx/0/1* no painel traseiro do roteador
- O *vmnic2* é mapeado para a interface GE2 do painel frontal do UCS-E
- A porta de gerenciamento do painel frontal (M) só pode ser usada para o CIMC.

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

- A *vmnic0* é mapeada para *UCSEx/0/0* no backplane do roteador.
- O *vmnic1* é mapeado para *UCSEx/0/1* no painel traseiro do roteador.
- O *vmnic2* é mapeado para a interface GE2 do painel frontal do UCS-E.
- O *vmnic3* é mapeado para a interface GE3 do painel frontal do UCS-E.
- A porta de gerenciamento do painel frontal (M) só pode ser usada para o CIMC.

Interfaces do vSwitch no ESXi

O vSwitch0 no ESXi é a interface de gerenciamento através da qual o ESXi, o FireSIGHT Management Center e o dispositivo FirePOWER NGIPSv se comunicam com a rede. Clique em **Propriedades** do vSwitch1 (SF-Inside) e do vSwitch2 (SF-Outside) para fazer alterações.

localhost.localdomain VMware ESXi, 5.1.0, 799733

Getting Started Summary Virtual Machines Resource Allocation Performance **Configuration** Local Users & Groups Events Permissions

Hardware

- Health Status
- Processors
- Memory
- Storage
- Networking**
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile
- Host Cache Configuration
- System Resource Allocation
- Agent VM Settings
- Advanced Settings

View: vSphere Standard Switch

Networking

Standard Switch **vSwitch0** Remove... **Properties...**

Virtual Machine Port Group

- VM Network
- 3 virtual machine(s)
- 4451-VMware vCenter Server Appl...
- SFS
- DC

Physical Adapters

- vmnic2 1000 Full

VMkernel Port

- Management Network
- vmk0 : 172.16.1.10
- fe80::e22f:6dff:fee0:f888

Standard Switch **vSwitch1** Remove... **Properties...**

Virtual Machine Port Group

- SF-Inside
- 1 virtual machine(s)
- SFS

Physical Adapters

- vmnic0 1000 Full

Standard Switch **vSwitch2** Remove... **Properties...**

Virtual Machine Port Group

- SF-Outside
- 1 virtual machine(s) | VLAN ID: 20
- SFS

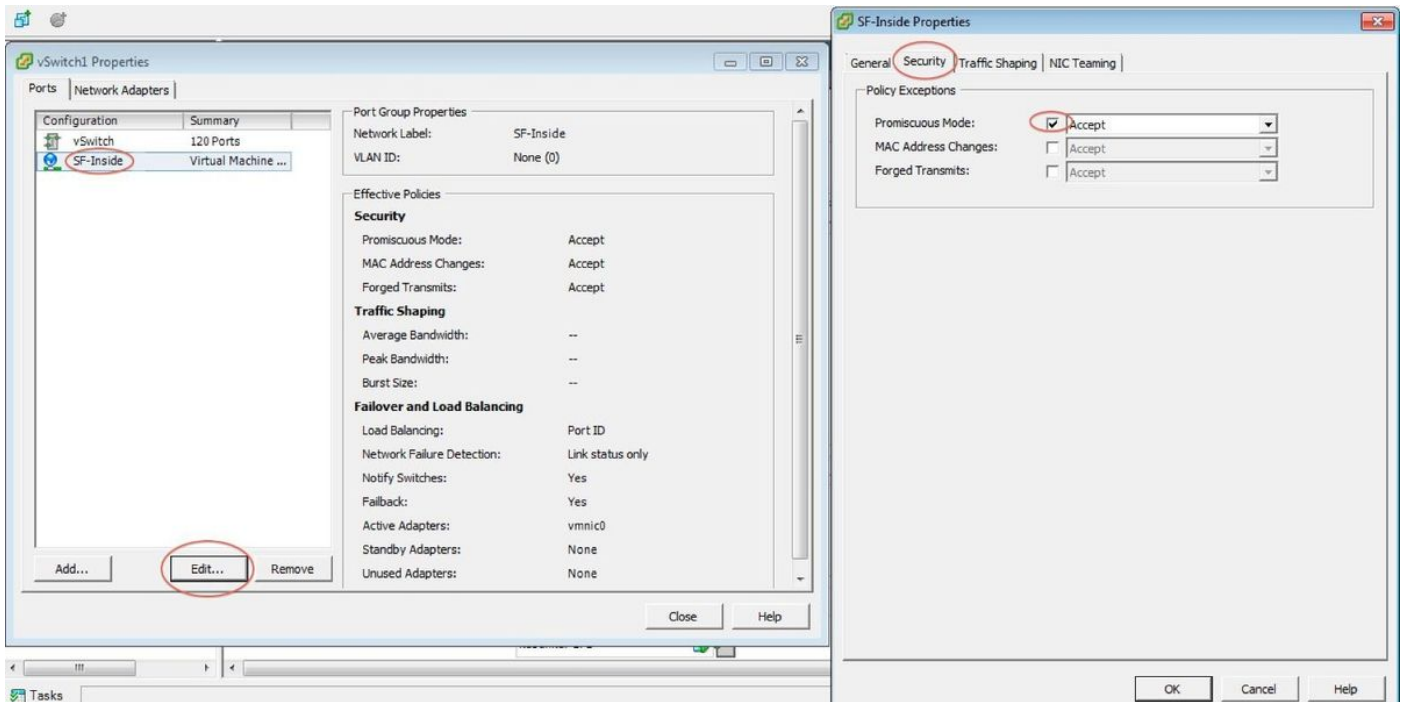
Physical Adapters

- vmnic1 1000 Full

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

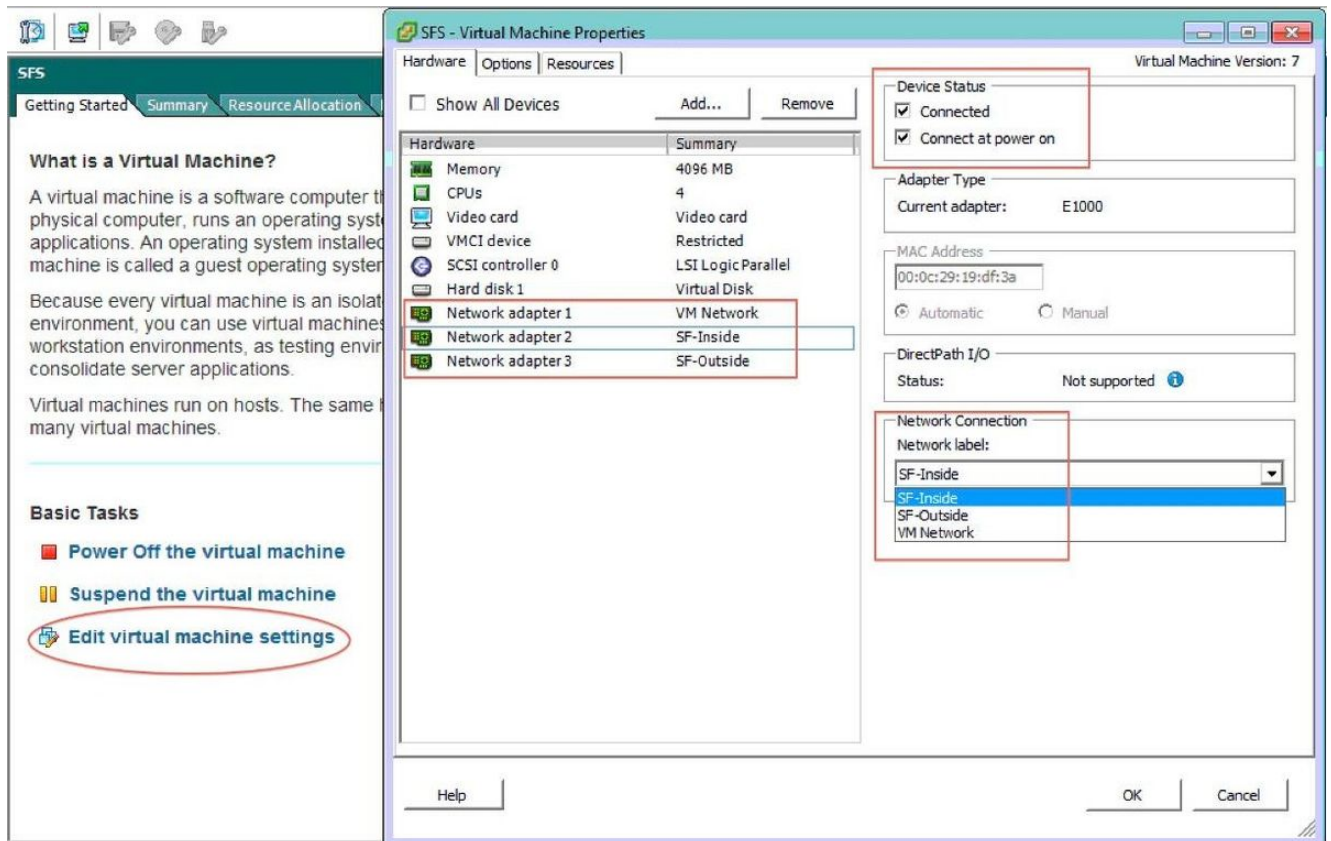
Note: Certifique-se de que a ID da VLAN esteja configurada para 4095 para NGIPSv, isso é necessário de acordo com o documento NGIPSv:

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



A configuração do vSwitch no ESXi está concluída. Agora você deve verificar as configurações da interface:

1. Navegue até a máquina virtual do dispositivo FirePOWER.
2. Clique em **Editar configurações da máquina virtual**.
3. Verifique todos os três adaptadores de rede.
4. Verifique se eles foram escolhidos corretamente, como mostrado na imagem aqui:



Registre o dispositivo FirePOWER com o FireSIGHT Management Center

Conclua os procedimentos descritos no documento da Cisco para registrar um dispositivo FirePOWER com um FireSIGHT Management Center.

Redirecionar e verificar o tráfego

Use esta seção para confirmar se a sua configuração funciona corretamente.

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

Redirecionar tráfego do ISR para o sensor no UCS-E

Use estas informações para redirecionar 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 posterior, execute o comando **utd engine advanced** em vez do comando **utd**.

Verificar o redirecionamento de pacote

No console do ISR, execute este comando para verificar se os contadores de pacotes 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
```

Verificar

Você pode executar estes comandos **show** para verificar se sua configuração funciona corretamente:

- **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

Esta seção disponibiliza informações para a solução de problemas de configuração.

Você pode executar estes comandos **debug** para solucionar problemas de sua configuração:

- **debug platform condition feature utd controlplane**
- **debug platform condition feature utd dataplane submode**

Informações Relacionadas

- [Guia de introdução aos servidores Cisco UCS E-Series e ao Cisco UCS E-Series Network Compute Engine, versão 2.x](#)
- [Guia de solução de problemas para servidores Cisco UCS E-Series e o Cisco UCS E-Series Network Computing Engine](#)
- [Guia de introdução aos servidores Cisco UCS E-Series e ao Cisco UCS E-Series Network Compute Engine, versão 2.x - Atualização do firmware](#)
- [Guia de configuração de software dos roteadores de serviços de agregação Cisco ASR 1000 Series - Configurando interfaces de domínio de bridge](#)
- [Guia do usuário do utilitário de atualização de host para servidores Cisco UCS E-Series e o Cisco UCS E-Series Network Compute Engine - Atualização do firmware em servidores Cisco UCS E-Series](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)