用UCS-E前端配置在ISR设备的Firepower服务

Contents

Introduction

本文在入侵检测系统(IDS)模式描述如何安装和配置Cisco Firepower软件在思科统一计算系统E系列(UCS-E)前端平台。在本文描述的配置示例是补充对于正式用户指南。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco集成服务路由器(ISR) XE镜像3.14或以上
- Cisco集成管理控制器(CIMC)版本2.3或以上
- Cisco FireSIGHT管理中心(FMC)版本5.2或以上
- Cisco Firepower虚拟设备(NGIPSv)版本5.2或以上
- VMware ESXi版本5.0或以上

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.如果您的网络实际，请保证您了解所有命令的潜在影响。

> **Note**:在您升级代码到版本3.14或以上前，请保证系统有充足的内存、磁盘空间和一个许可证的升级。请参见示例1 ：将映像从 TFTP 服务器复制到 flash:从接入路由器软件升级程序Cisco文档的TFTP server部分为了得知更多代码升级。

> **Note**:为了升级CIMC， BIOS和其他固件组件，您能使用或者Cisco主机升级工具(HUU)，或者您能手工升级固件组件。为了得知更多固件升级，请参见升级在Cisco UCS电子系列主机升级工具用户指南的服务器部分的固件Cisco UCS电子系列服务器和Cisco UCS电子系列网络估计引擎的。

背景信息

此部分关于在本文描述的组件和程序提供关于支持的硬件平台的信息，许可证和限制。

支持的硬件平台

此部分列出G2和4000系列设备的支持的硬件平台。

ISR G2设备用UCS-E前端

用UCS-E系列前端支持这些ISR G2系列设备：

产品	Platform	UCS-E型号
Cisco 2900系列ISR	2911	UCS-E 120/140单个宽选项
	2921	UCS-E 120/140/160/180单或双宽选项
	2951	UCS-E 120/140/160单或双宽选项
Cisco 3900系列ISR	3925	UCS-E 120/140/160单个和双宽选项或180双宽
	3925E	UCS-E 120/140/160单个和双宽选项或180双宽
	3945	UCS-E 120/140/160单个和双宽选项或180双宽
	3945E	UCS-E 120/140/160单个和双宽选项或180双宽

ISR 4000个设备用UCS-E前端

用UCS-E系列前端支持这些ISR 4000系列设备：

产品	Platform	UCS-E型号
Cisco 4400系列ISR	4451	UCS-E 120/140/160单个和双宽选项或180双宽
	4431	UCS-E网络接口模块
Cisco 4300系列ISR	4351	UCS-E 120/140/160/180单个和双宽选项或180双宽
	4331	UCS-E 120/140单个宽选项
	4321	UCS-E网络接口模块

许可证

ISR必须有安全K9许可证，以及appx许可证，为了enable (event)服务。

限制

这是两个限制关于在本文描述的信息：

- 不支持组播
- 仅4,096个网桥域接口(BDI)为每个系统支持

BDIs不支持这些功能：

- 双向转发检测(BFD)协议
- Netflow
- Quality of Service (QoS)
- 基于网络应用的识别(NBAR)或先进的视频编码(AVC)
- 区域根据防火墙(ZBF)
- 密码VPN
- 多协议标签交换(MPLS)
- 以太网上的点对点协议(PPPoE)

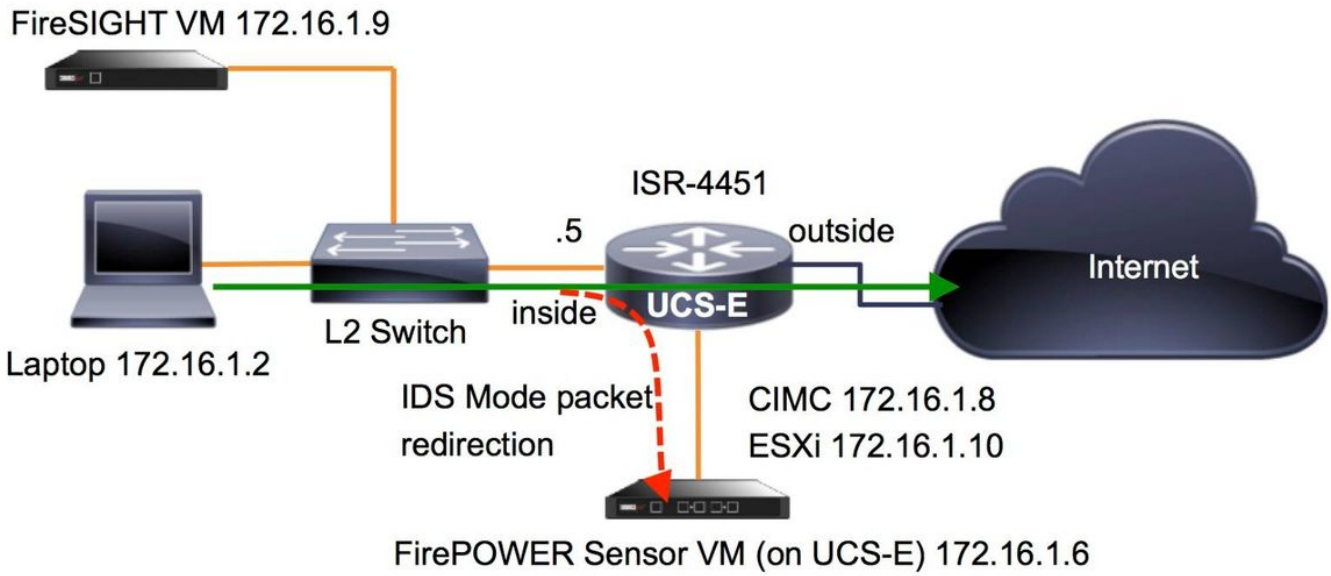
Note:对于BDI，最大传输单元(MTU)大小可以配置有在1,500个和9,216个字节范围的任何值。

Configure

此部分描述如何配置涉及与此配置的组件。

Network Diagram

在本文描述的配置使用此网络拓扑：



Firepower服务的工作流在UCS-E

这是在UCS-E运作的Firepower服务的工作流：

1. 数据平面推进检查的数据流从BDI/UCS-E接口(为G2和G3系列设备工作)。
2. Cisco IOS XE CLI激活分析的(所有接口的选项信息包重定向或单个接口的)。
3. 传感器CLI来设置启动脚本简单化配置。

配置CIMC

此部分描述如何配置CIMC。

连接到CIMC

有多种方式连接到CIMC。在本例中，连接到CIMC通过一个专用管理端口完成。保证您连接**M**端口(投入)到网络用使用以太网电缆。一旦连接，从路由器提示请运行**hw-module子插槽**命令：

```
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
```

提示1 ：为了退出，请运行**^a^q。**

提示2 ：默认用户名是**admin**和密码<password>。密码重设进程被描述得这里：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

配置CIMC

请使用此信息为了完成配置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
```

警告：保证您运行**commit命令**为了保存更改。

Note:当使用时，设置模式**专用**管理端口。

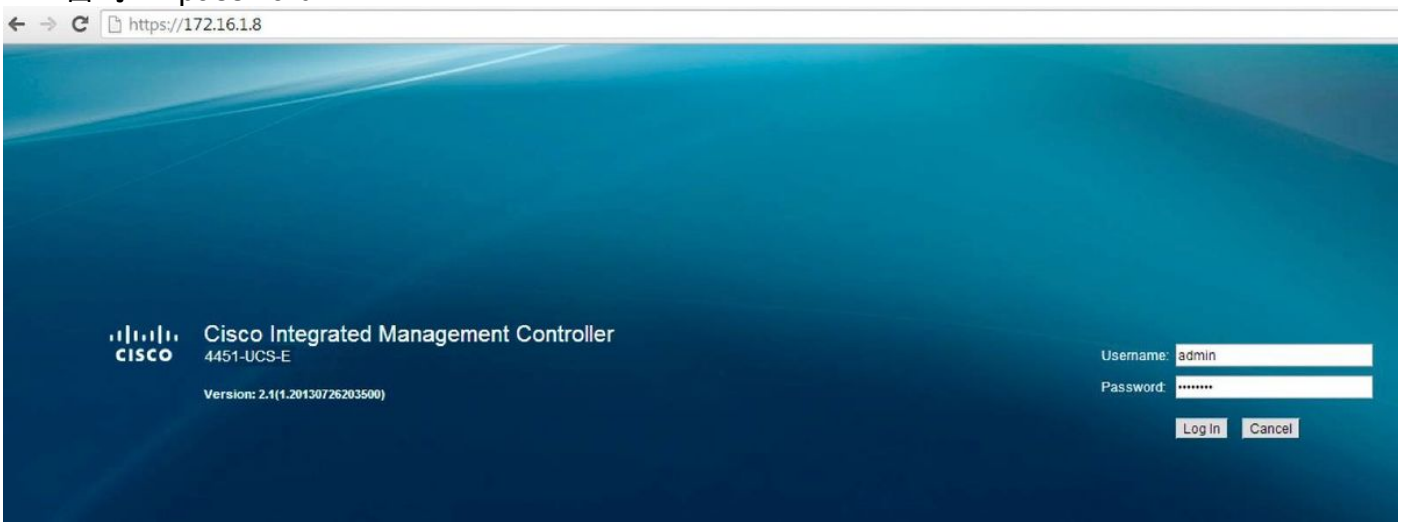
运行**detail命令的显示**为了验证详细资料设置：

```
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 #
```

如镜像所显示，启动Web接口CIMC从浏览器与默认用户名和密码。默认用户名和密码是：

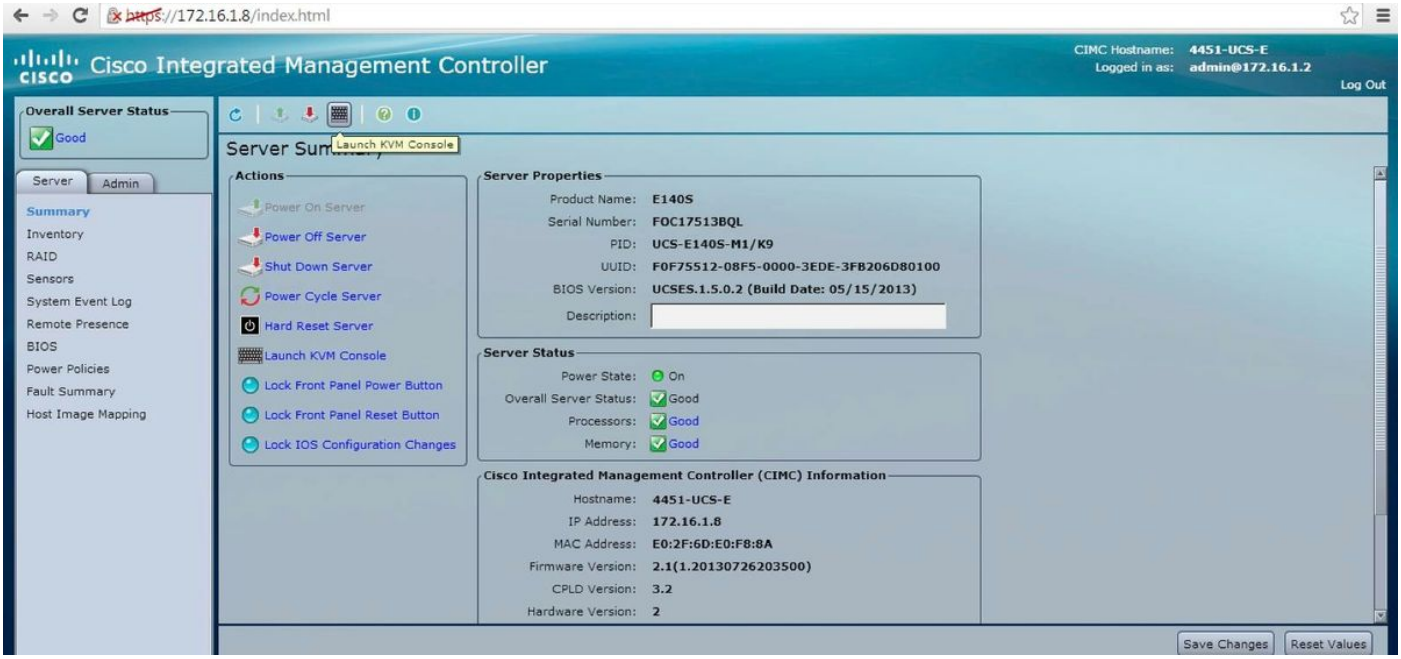
- 用户名：**admin**

- 密码：<password>

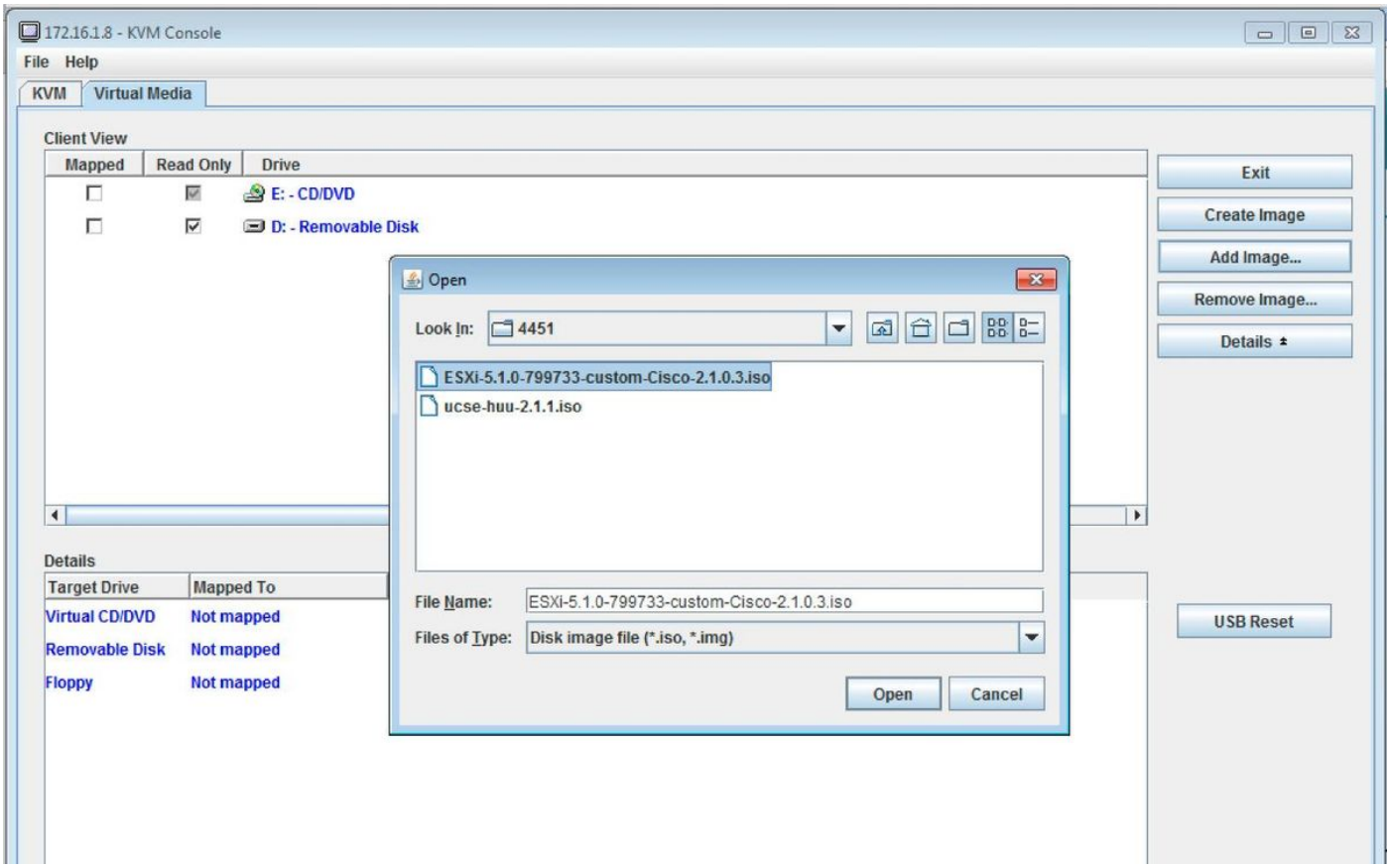


安装ESXi

在您记录到用户界面CIMC后，您能查看页类似于在此镜像显示的那。点击**生成KVM控制台**图标，点击**添加镜像**，然后映射ESXi ISO作为虚拟媒体：



如镜像所显示，点击**虚拟媒体**选项，然后点击**添加镜像**为了映射虚拟媒体。



在虚拟媒体被映射后，请点击**功率**从CIMC主页的**循环服务器**为了关机并重新开机UCS-E。ESXi设置从虚拟媒体启动。完成ESXi安装。

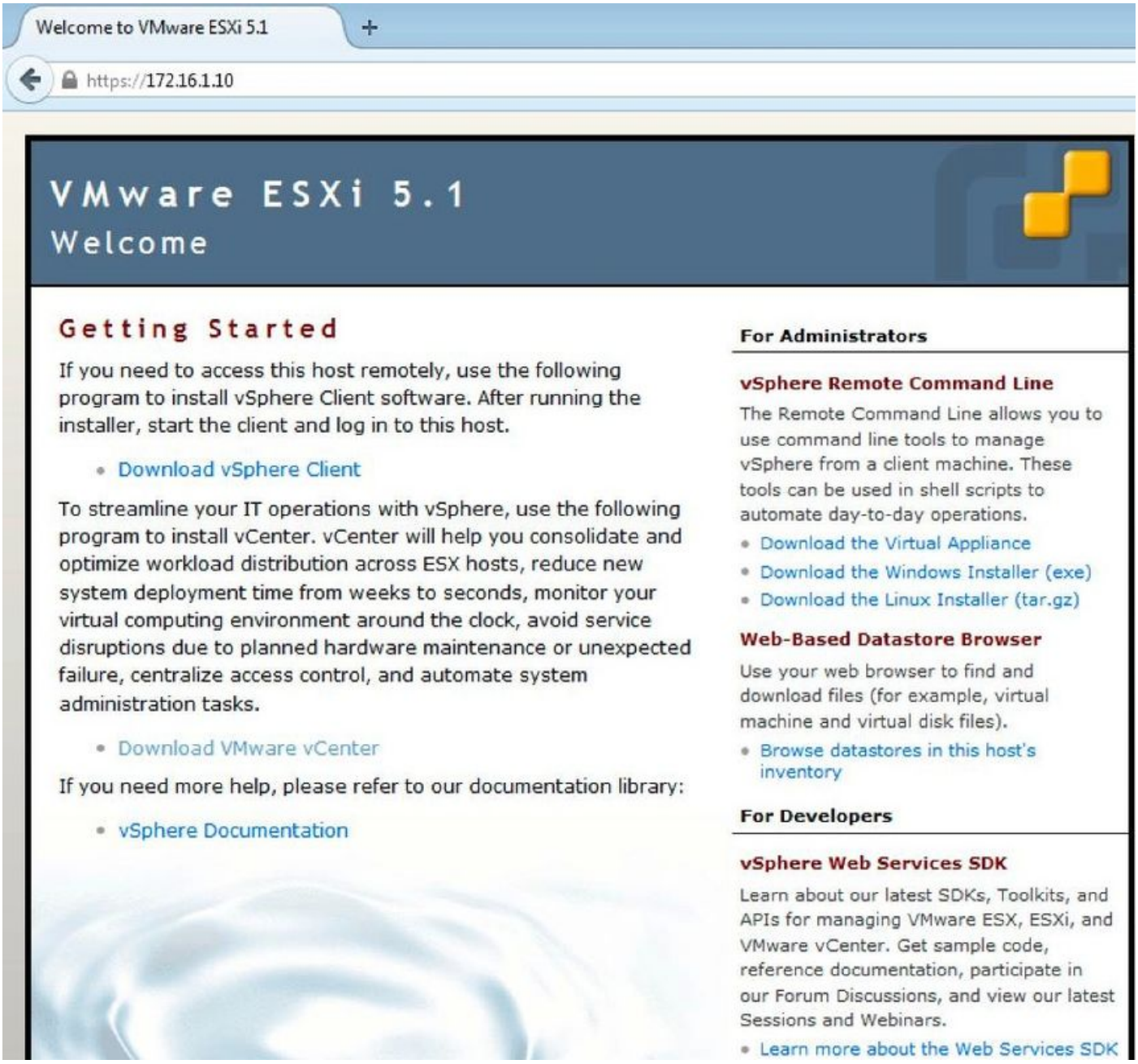
Note:记录ESXi IP地址、用户名和密码供将来参考。

安装vSphere客户端

此部分描述如何安装vSphere客户端。

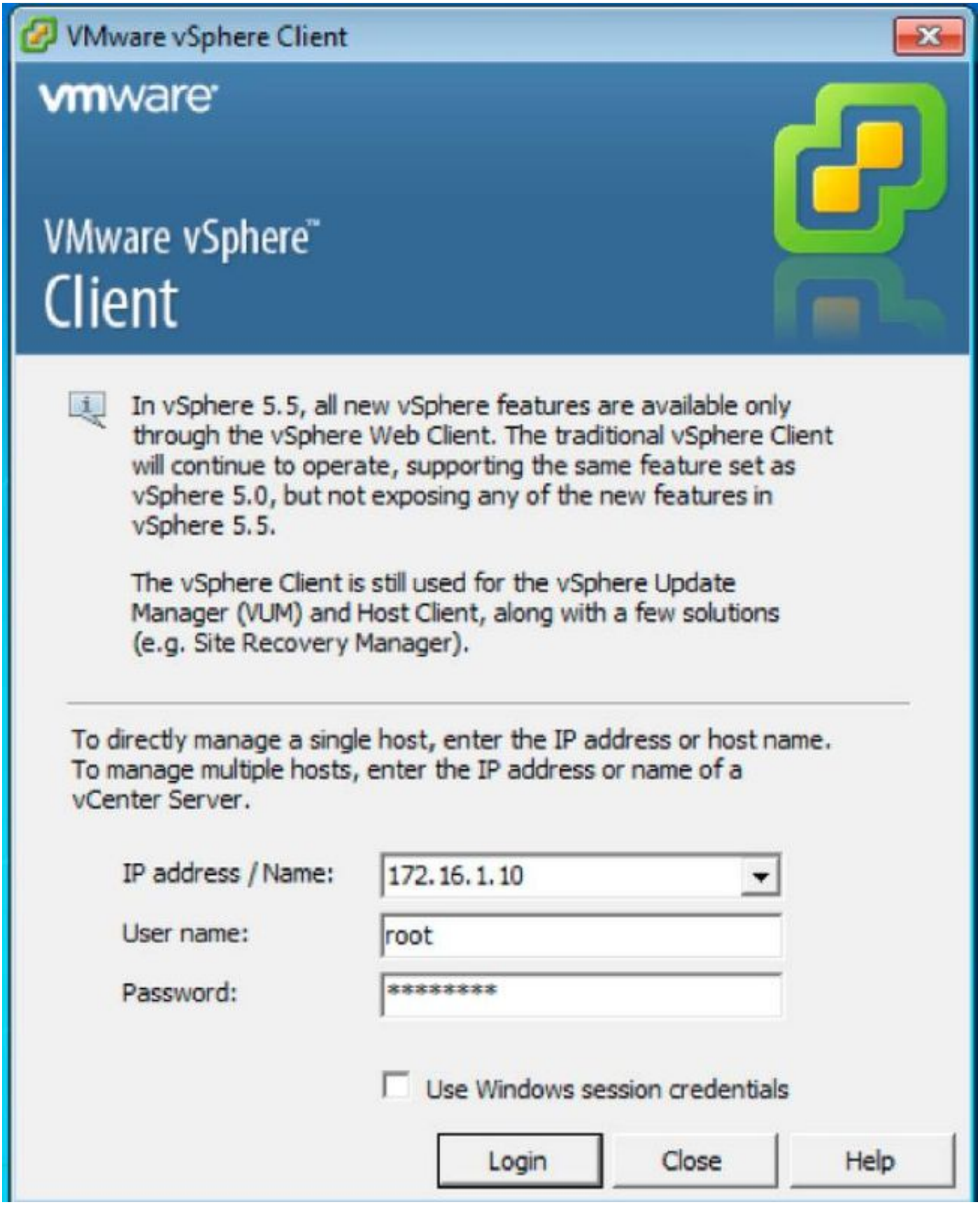
下载vSphere客户端

启动ESXi并且请使用**下载VSphere客户端**链路为了下载vSphere客户端。在您的计算机上安装它。



启动vSphere客户端

启动vSphere客户端从您的计算机。登陆与如镜像所显示，您创建在安装时和的用户名和密码：



配置FireSIGHT管理中心和Firepower设备

完成在FireSIGHT在VMware ESXi Cisco文档的管理中心配置描述为了配置在ESXi的一个FireSIGHT管理中心的程序。

Note:使用为了配置Firepower NGIPSv设备的进程类似于使用为了配置管理中心的进程。

接口

在双重范围UCS-E，有四个接口：

- 最高的MAC地址接口是在前面板的Gi3
- 第二个高MAC地址接口是在前面板的Gi2
- 出现的最后两个是内部界面

在单一范围UCS-E，有三个接口：

- 最高的MAC地址接口是在前面板的Gi2
- 出现的最后两个是内部界面

两个在ISR4K的UCS-E接口是中继端口。

UCS-E 120S和140S有三网络适配器加上管理端口：

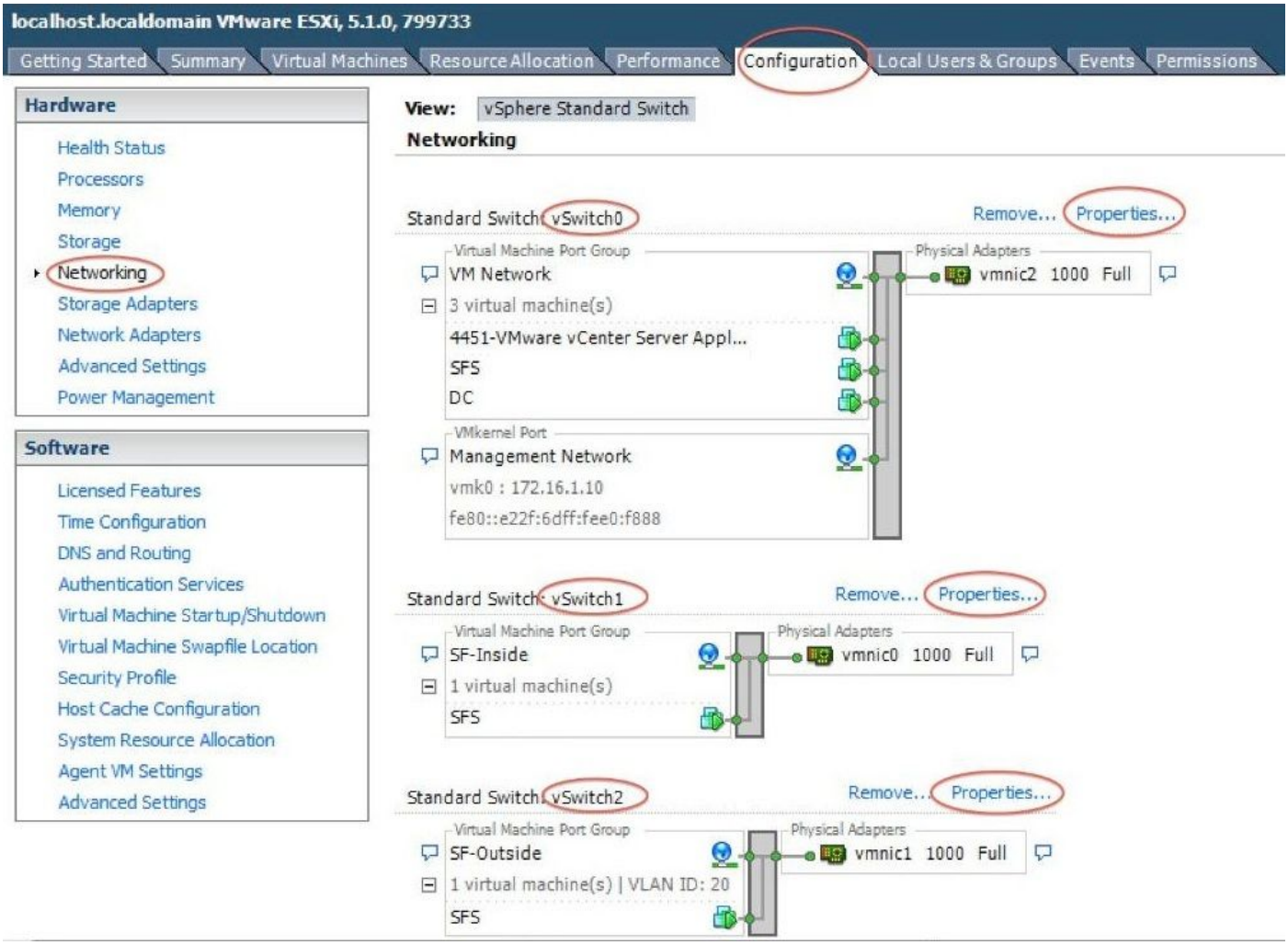
- *vmnic0*被映射对在路由器背板的*UCSEx/0/0*
- *vmnic1*被映射对在路由器背板的*UCSEx/0/1*
- *vmnic2*被映射对UCS-E前面飞机GE2接口
- 前面板管理(m)端口可能只用于CIMC。

UCS-E 140D、160D和180D有四个网络适配器：

- *vmnic0*被映射对在路由器背板的*UCSEx/0/0*。
- *vmnic1*被映射对在路由器背板的*UCSEx/0/1*。
- *vmnic2*被映射对UCS-E前面飞机GE2接口。
- *vminc3*被映射对UCS-E前面飞机GE3接口。
- 前面板管理(m)端口可能只用于CIMC。

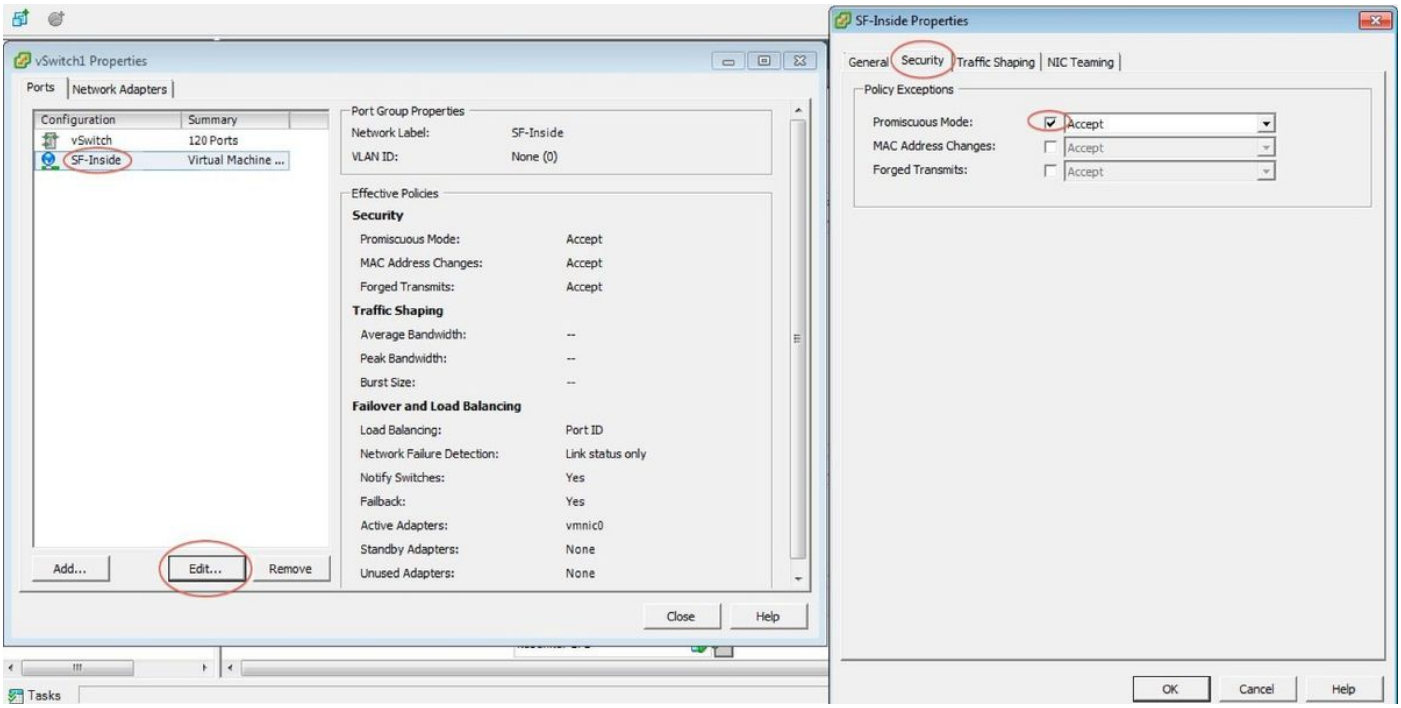
在ESXi的vSwitch接口

在ESXi的vSwitch0是ESXi、FireSIGHT管理中心和Firepower NGIPSv设备沟通对网络的管理接口。点击vSwitch1 (SF里面)和vSwitch2的(SF外部)**属性**为了做其中任一变动。



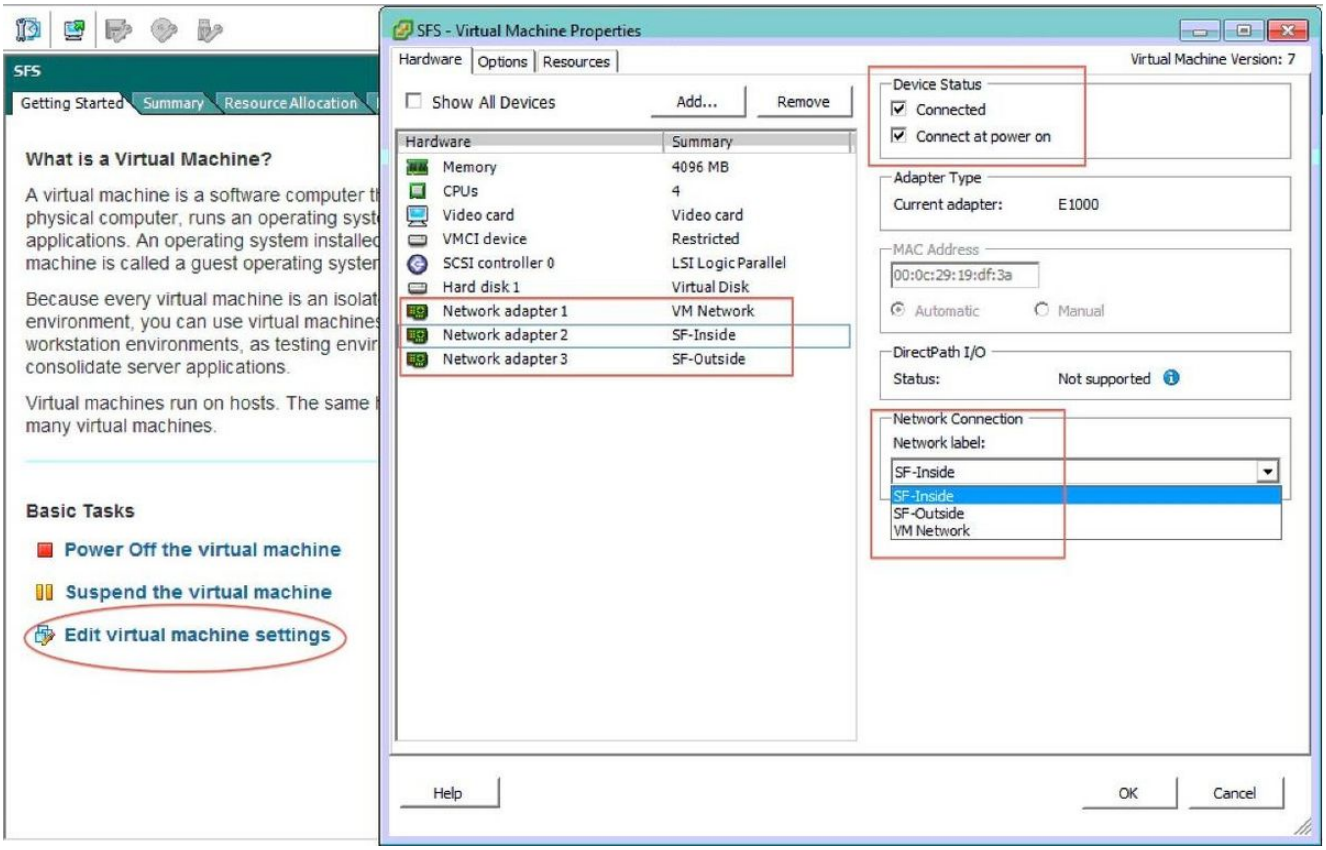
此镜像显示vSwitch1 (您的属性必须完成vSwitch2的同样步骤) ：

Note:保证VLAN ID被配置到4095 NGIPSv的，这根据NGIPSv文件需要：http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



在ESXi的vSwtich配置完成。现在您必须验证接口设置：

1. 连接到Firepower设备的虚拟机。
2. 点击**编辑虚拟机设置**。
3. 验证所有三个网络适配器。
4. 保证他们适当地被选择，如这里镜像所显示：



注册有FireSIGHT管理中心的Firepower设备

完成在Cisco文档描述为了注册有FireSIGHT管理中心的一个Firepower设备的程序。

重定向并且验证数据流

使用本部分可确认配置能否正常运行。

此部分描述如何重定向数据流和如何验证信息包。

重定向数据流从ISR到在UCS-E的传感器

请使用此信息为了重定向数据流：

```
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:如果当前运行3.16.1或以后，运行**utd引擎提前的**命令而不是utd命令。

验证信息包重定向

从ISR控制台，请运行此命令为了验证信息包计数器是否增加：

```
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
```

Verify

您能运行这些**显示**命令为了验证您的配置适当地工作：

- **显示制地图全局软件utd**
- **显示制地图软件utd接口**
- **显示制地图软件utd RP活动全局**
- **显示制地图软件utd fp活动全局**
- **显示制地图硬件qfp活动功能utd stats**
- **显示平台硬件qfp活动功能utd**

Troubleshoot

本部分提供了可用于对配置进行故障排除的信息。

您能运行这些调试指令为了排除您的配置故障：

- **调试平台情况功能utd controlplane**
- **调试平台情况功能utd dataplane从属方式**

Related Information

- Cisco UCS电子系列服务器和Cisco UCS电子系列网络估计引擎的入门指南，版本2.x
- Cisco UCS电子系列服务器和Cisco UCS电子系列网络估计引擎的故障排除指南
- Cisco UCS电子系列服务器和Cisco UCS电子系列网络估计引擎的入门指南，版本2.x –升级固件
- Cisco ASR 1000系列汇聚服务路由器软件配置指南–配置网桥域接口
- 主机升级Cisco UCS电子系列服务器和Cisco UCS电子系列网络估计引擎的工具用户指南–升级在Cisco UCS电子系列服务器的固件
- Technical Support & Documentation - Cisco Systems