

Настройте сервисы FirePOWER на устройстве ISR с блейдом UCS-E

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Поддерживаемые аппаратные платформы](#)

[Устройства ISR G2 с блейдами UCS-E](#)

[ISR 4000 устройств с блейдами UCS-E](#)

[Лицензии](#)

[Ограничения](#)

[Настройка](#)

[Схема сети](#)

[Поток операций для FirePOWER Services на UCS-E](#)

[Настройте CIMC](#)

[Соединитесь с CIMC](#)

[Настройте CIMC](#)

[Установите ESXi](#)

[Установите vSphere Клиента](#)

[Загрузите vSphere Клиента](#)

[Запустите vSphere Клиента](#)

[Разверните центр управления FireSIGHT и устройства FirePOWER](#)

[Настройте интерфейсы](#)

[Настройте Интерфейсы vSwitch на ESXi](#)

[Зарегистрируйте устройство FirePOWER в центре управления FireSIGHT](#)

[Перенаправьте и проверьте трафик](#)

[Трафик перенаправления с ISR на Датчик на UCS-E](#)

[Проверьте перенаправление пакетов](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как установить и развернуть программное обеспечение Cisco FirePOWER на системе Cisco UCS, Серии E (UCS-E) платформа блейда в режиме Системы обнаружения Intrusion (IDS). Пример конфигурации, который описан в этом документе, является дополнением к официальному руководству пользователя.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco ISR (ISR) образ XE 3.14 или позже
- Интегрированный контроллер управления Cisco (CIMC) Версия 2.3 или позже
- Центр управления FireSIGHT (FMC) Cisco Версия 5.2 или позже
- Виртуальное устройство Cisco FirePOWER (NGIPSv) Версия 5.2 или позже
- VMware Версия 5.0 ESXi или позже

Примечание: Прежде чем вы обновите код к Версии 3.14 или позже, гарантируете, что система имеет достаточно памяти, дисковое пространство и лицензию на обновление. См. [Пример 1: Скопируйте образ для мигания: от раздела сервера TFTP](#) Документа *Cisco Процедур модернизации программного обеспечения Маршрутизаторов доступа* для узнавания больше об обновлениях кода.

Для обновления CIMC, BIOS и других компонентов микропрограммного обеспечения, можно использовать или Утилиту обновления хоста (HUU) Cisco, или можно обновить компоненты микропрограммного обеспечения вручную. Для узнавания больше об обновлении микропрограммного обеспечения обратитесь к [Обновлению Микропрограммного обеспечения на UCS Cisco](#) раздел [Серверов Серии E](#) Руководства пользователя Утилиты Обновления Хоста для UCS Cisco Серверы Серии E и UCS Cisco, Сеть Серии E Вычисляет Механизм.

Общие сведения

Этот раздел предоставляет сведения о поддерживаемых аппаратных платформах, лицензиях и ограничениях в отношении компонентов и процедур, которые описаны в этом документе.

Поддерживаемые аппаратные платформы

Этот раздел перечисляет поддерживаемые аппаратные платформы для G2 и устройств серии 4000.

Устройства ISR G2 с блейдами UCS-E

Они ISR устройства Серии G2 с блейдами Серии E UCS поддерживаются:

Продукт	Платформа	Модель UCS-E
ISR серии Cisco 2900	2911	UCS-E 120/140 одиночная широкая опция
	2921	UCS-E 120/140/160/180 одиночная или двойная широкая опция
	2951	UCS-E 120/140/160 одиночная или двойная широкая опция
	3925	UCS-E 120/140/160 одиночная и двойная широкая опция или 180 удваивается широкий
Cisco ISR серии 3900	3925E	UCS-E 120/140/160 одиночная и двойная широкая опция или 180 удваивается широкий
	3945	UCS-E 120/140/160 одиночная и двойная широкая опция или 180 удваивается широкий
	3945E	UCS-E 120/140/160 одиночная и двойная широкая опция или 180 удваивается широкий

ISR 4000 устройств с блейдами UCS-E

Они ISR устройства серии 4000 с блейдами Серии E UCS поддерживаются:

Продукт	Платформа	Модель UCS-E
Cisco ISR серии 4400	4451	UCS-E 120/140/160 одиночная и двойная широкая опция или 180 удваивается широкий
	4431	Модуль сетевых интерфейсов UCS-E
	4351	UCS-E 120/140/160/180 одиночная и двойная широкая опция или 180 удваивается широкий
ISR серии Cisco 4300	4331	UCS-E 120/140 одиночная широкая опция
	4321	Модуль сетевых интерфейсов UCS-E

Лицензии

ISR должен иметь лицензию K9 безопасности, а также *аррх* лицензию, для включения сервиса.

Ограничения

Вот два ограничения в отношении информации, которая описана в этом документе:

- Групповая адресация не поддерживается.
- Только 4,096 Интерфейсов домена моста (BDI) поддерживаются для каждой системы. BDI не поддерживают эти функции:
 - Протокол Обнаружения двунаправленной передачи данных (BFD)
 - Netflow
 - Качество обслуживания (QOS)
 - Сетевое распознавание приложений (NBAR) или усовершенствованное кодирование видео (AVC)

- Зональный базирующийся межсетевой экран (ZBF)
- Криптографические VPN
- Многопротокольная коммутация по меткам (MPLS)
- Протокол PPP по Ethernet (PPPoE)

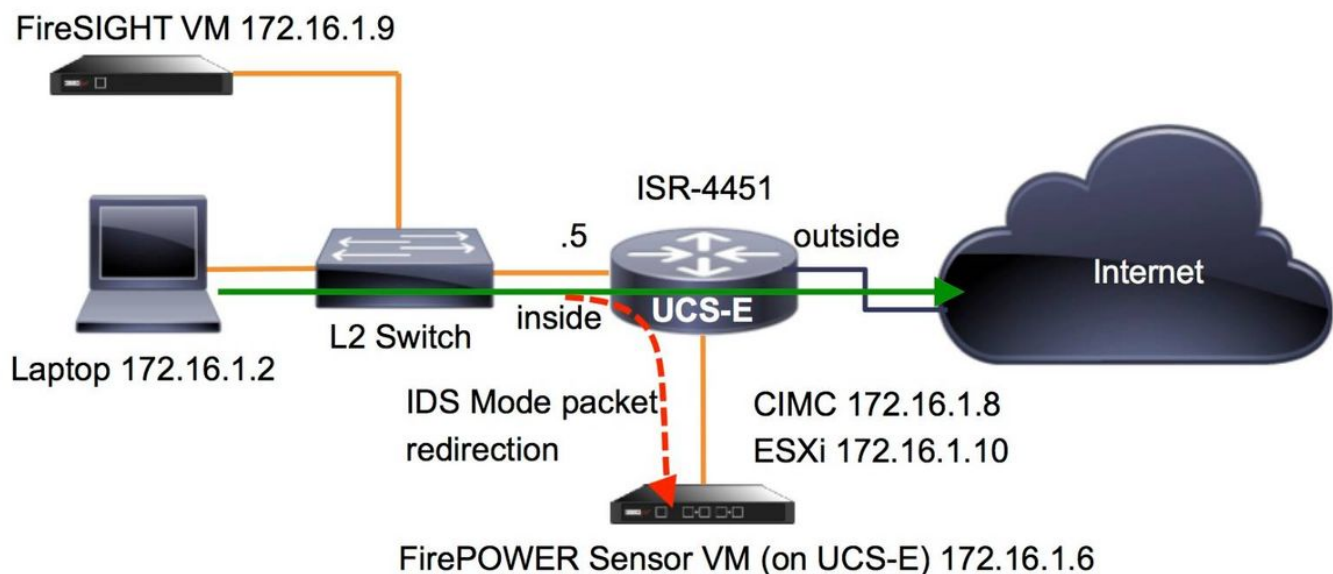
Примечание: Для BDI Максимальный размер передаваемого блока данных (MTU) может быть настроен с любым значением между 1,500 и 9,216 байтами.

Настройка

В этом разделе описывается настроить компоненты, которые связаны с этими развертываниями.

Схема сети

Конфигурация, которая описана в этом документе, использует эту топологию сети:



Поток операций для FirePOWER Services на UCS-E

Вот поток операций для сервисов FirePOWER, которые работают на UCS-E:

1. Плоскость данных требует у трафика контроль из интерфейса BDI/UCS-E (работает для G2 и Устройств серии G3).
2. CLI Cisco IOS XE активирует перенаправление пакетов для анализа (опции для всех интерфейсов или поинтерфейсный).

3. Сценарий запуска *настройки* CLI датчика упрощает конфигурацию.

Настройте CIMC

В этом разделе описывается настроить CIMC.

Соединитесь с CIMC

Существуют несколько способов для соединения с CIMC. В данном примере соединение с CIMC завершено через порт выделенного управления. Гарантируйте соединение порта **M** (выделенного) сети с использованием Кабеля Ethernet. После того, как связанный, введите команду **subslot hw-module** от командной строки маршрутизатора:

```
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
```

Совет: Для выхода введите **^a^q**.

Настройте CIMC

Используйте эту информацию для завершения конфигурации 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
```

Внимание. : Действуйте, что вы вводите команду **передачи** для сохранения изменений.

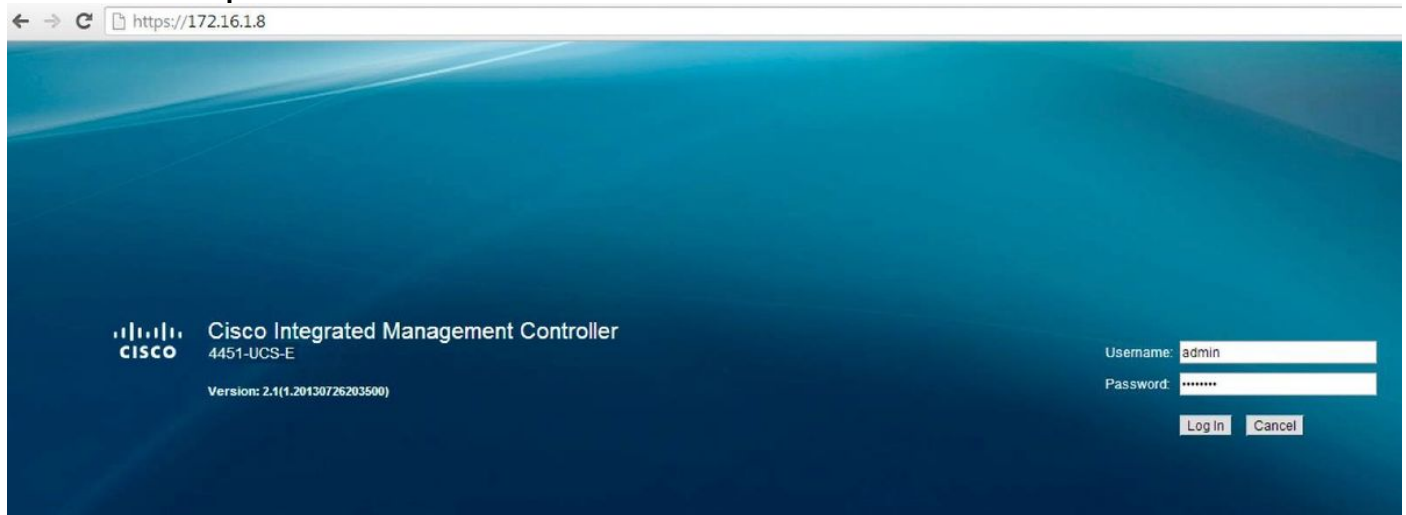
Примечание: Когда порт управления используется, *режим* установлен в **специализированный**.

Введите **подробную** команду **показа** для проверки подробных параметров настройки:

```
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 #
```

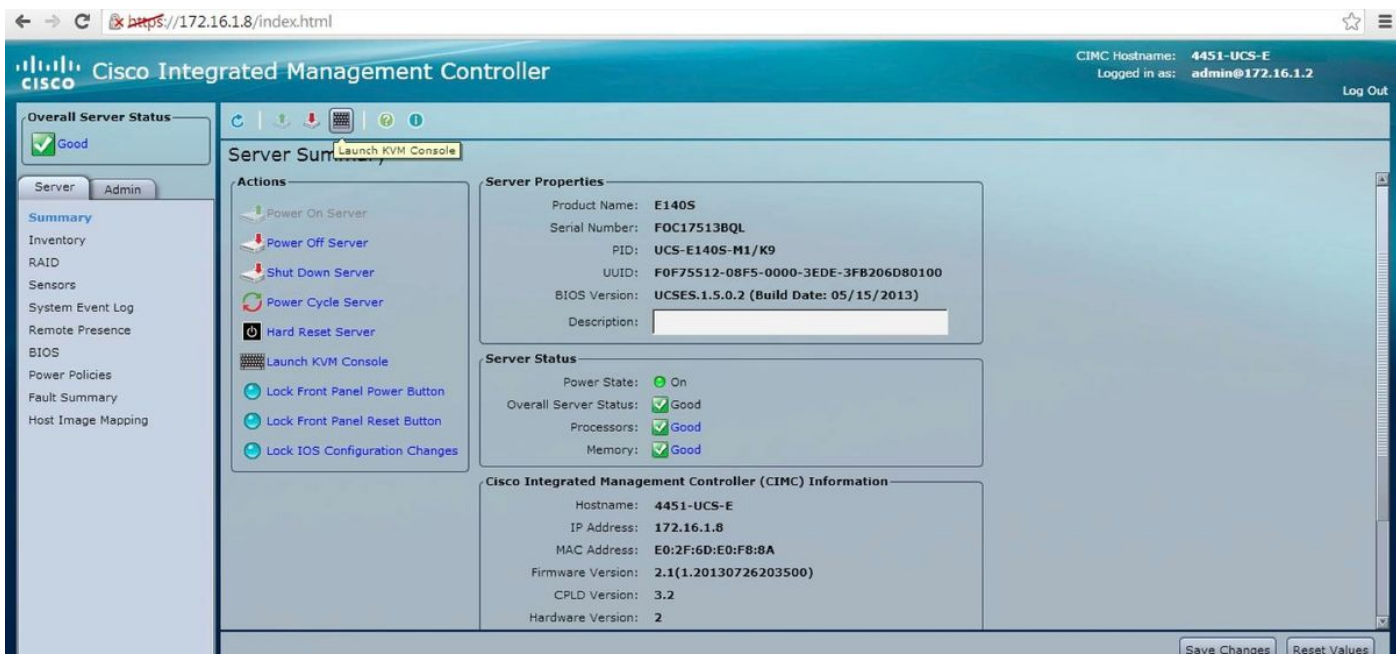
Запустите веб-интерфейс CIMC от браузера с именем пользователя по умолчанию и паролем. Имя пользователя по умолчанию и пароль:

- Username: **admin**
- Password: **password**

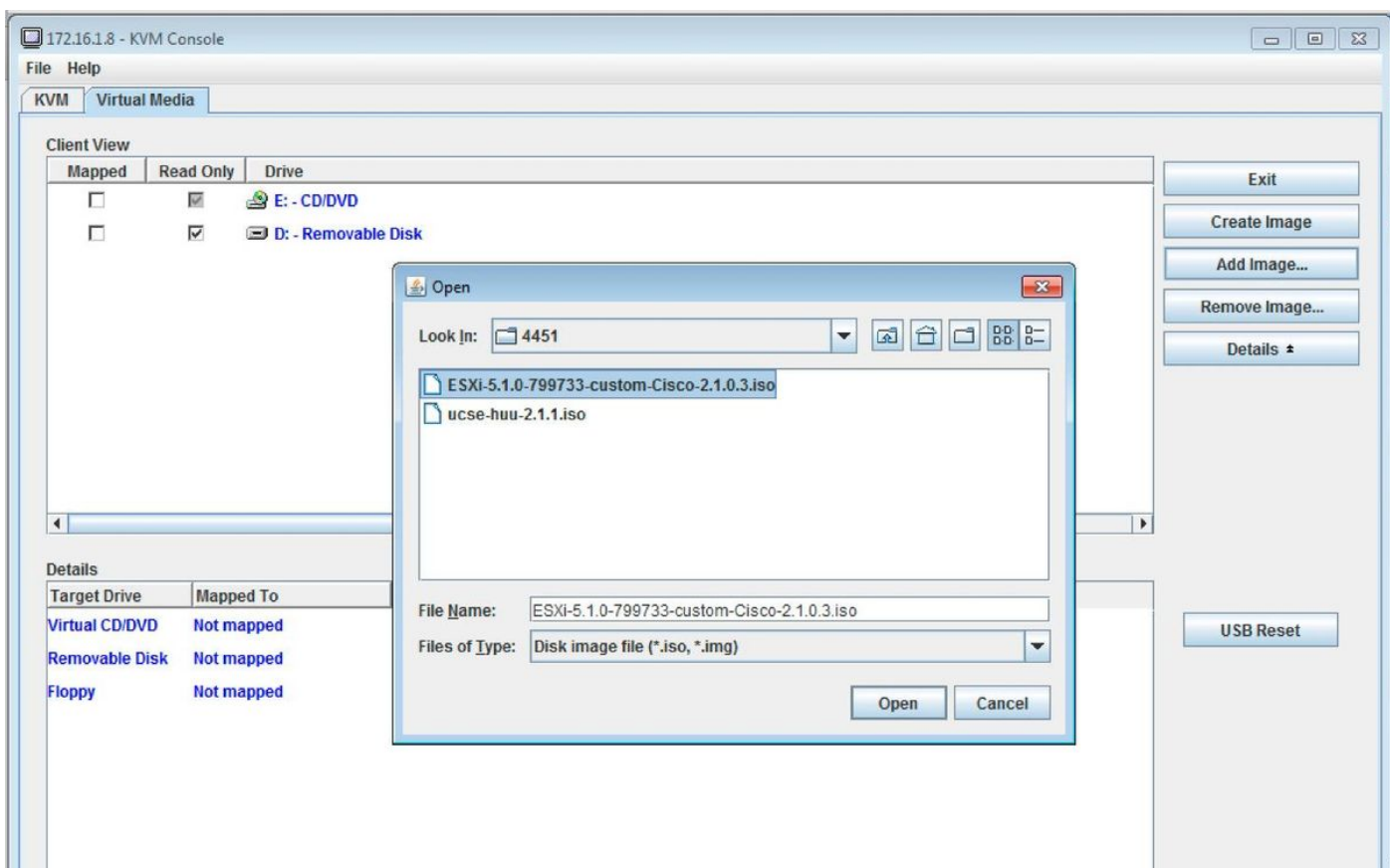


Установите ESXi

После того, как вы войдете в интерфейс пользователя CIMC, вы в состоянии просмотреть страницу, подобную показанному в следующем образе. Нажмите значок **Консоли KVM Запуска**, щелчок **добавляют образ**, и затем сопоставляют ISO ESXi как действительные среды:



Нажмите вкладку **Virtual Media**, и затем нажмите **Add Образ** для сопоставления действительных сред:



После действительных сред сопоставлен, нажмите **Power Cycle Server** от домашней страницы CIMC для выключения UCS-E. ESXi устанавливает запуски от действительных сред. Завершите установку ESXi.

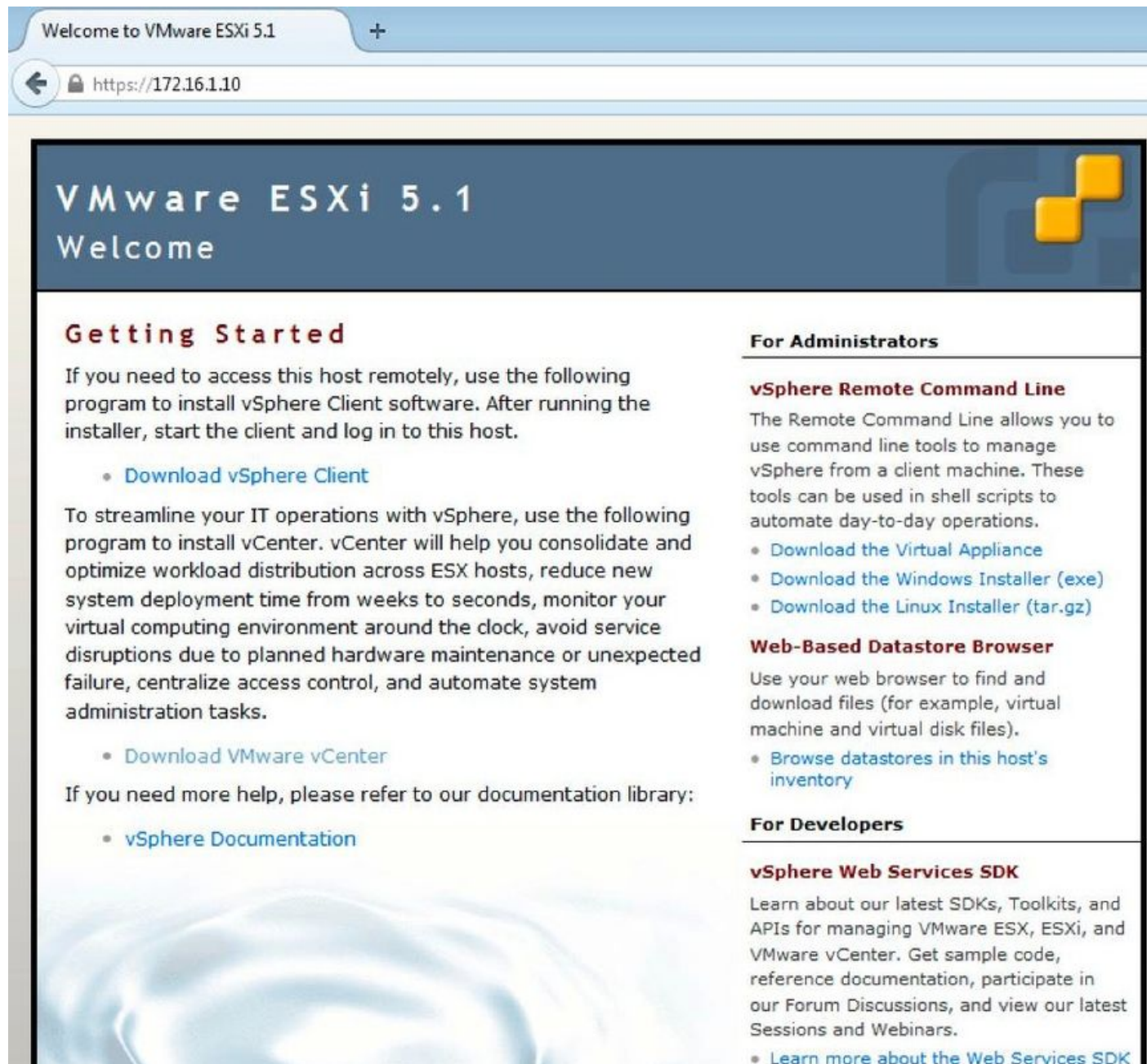
Примечание: Сделайте запись *IP-адреса ESXi, Имени пользователя и Пароля* для дальнейшего использования.

Установите vSphere Клиента

В этом разделе описывается установить vSphere клиента.

Загрузите vSphere Клиента

Запустите ESXi и используйте [Загрузку ссылка Клиента VSphere](#) для загрузки vSphere клиента. Установите его на своем компьютере.



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

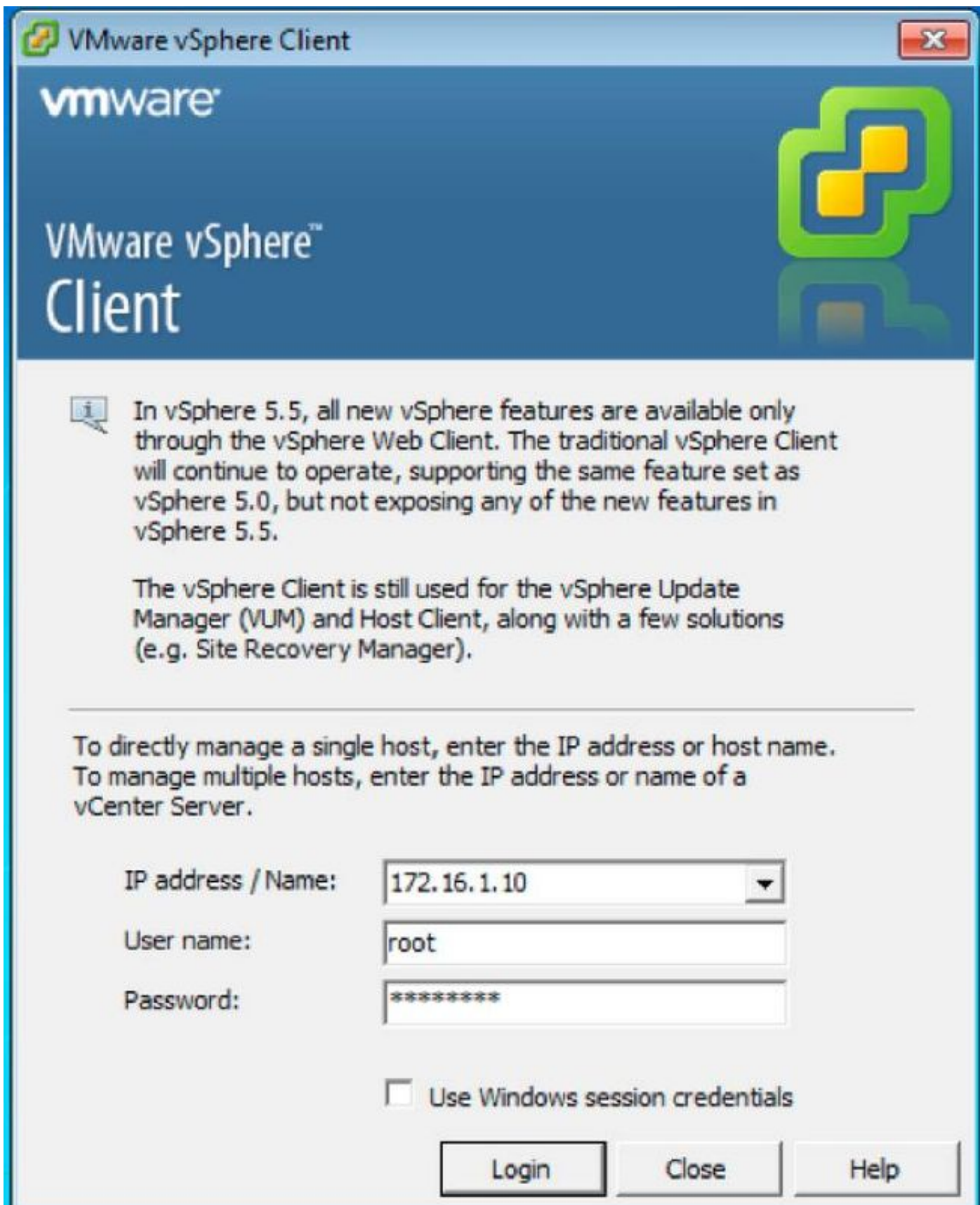
vSphere Web Services SDK

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](#)

Запустите vSphere Клиента

Запустите vSphere Клиента от своего компьютера. Войдите с именем пользователя и паролем, которое вы создали во время установки:



Разверните центр управления FireSIGHT и устройства FirePOWER

Завершите процедуры, которые описаны в [Развертываниях Центра управления FireSIGHT на VMware](#) Документ Cisco [ESXi](#) для развертывания Центра управления FireSIGHT на ESXi.

Примечание: Процесс, который используется для развертывания устройства

FirePOWER NGIPSv подобен процессу, который используется для развертывания Центра управления.

Настройте интерфейсы

На Двойном ширины UCS-E существует четыре интерфейса:

- Самый высокий интерфейс MAC-адреса является Gi3 на лицевой панели.
- Второй по высоте интерфейс MAC-адреса является Gi2 на лицевой панели.
- Последние два, которые появляются, являются внутренними интерфейсами.

На Одинарном UCS-E существует три интерфейса:

- Самый высокий интерфейс MAC-адреса является Gi2 на лицевой панели.
- Последние два, которые появляются, являются внутренними интерфейсами.

Оба из интерфейсов UCS-E на ISR4K являются магистральными портами.

UCS-E 120S и 140S имеет три Сетевых адаптера плюс Порты управления:

- *vmnic0* сопоставлен с *UCSEx/0/0* на объединительной плате маршрутизатора.
- *vmnic1* сопоставлен с *UCSEx/0/1* на объединительной плате маршрутизатора.
- *vmnic2* сопоставлен с передней плоскостью UCS-E интерфейс GE2.
- Управление лицевой панели (M) порт может только использоваться для CIMC.

UCS-E 140D, 160D, и 180D имеет четыре Сетевых адаптера:

- *vmnic0* сопоставлен с *UCSEx/0/0* на объединительной плате маршрутизатора.
- *vmnic1* сопоставлен с *UCSEx/0/1* на объединительной плате маршрутизатора.
- *vmnic2* сопоставлен с передней плоскостью UCS-E интерфейс GE2.
- *vmnic3* сопоставлен с передней стороной UCS-E плоский интерфейс GE3.
- Управление лицевой панели (M) порт может только использоваться для CIMC.

Настройте Интерфейсы vSwitch на ESXi

vSwitch0 на ESXi является интерфейсом управления, через который ESXi, Центр управления FireSIGHT и устройство FirePOWER NGIPSv связываются с сетью. Нажмите **Properties** для vSwitch1 (SF - Внутри) и vSwitch2 (SF - Снаружи) для внесения любых изменений.

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

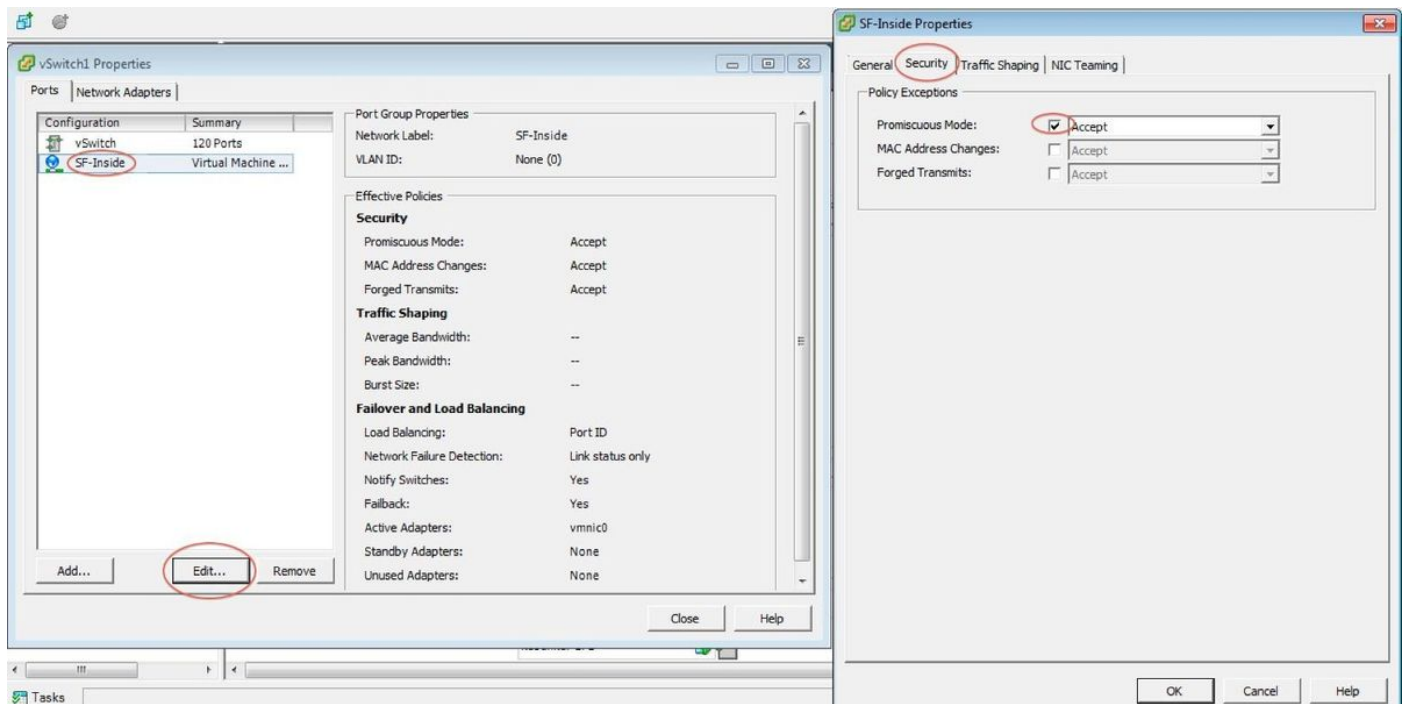
Physical Adapters

- vmnic1 1000 Full

Этот образ показывает свойства vSwitch1 (необходимо выполнить те же шаги для vSwitch2):

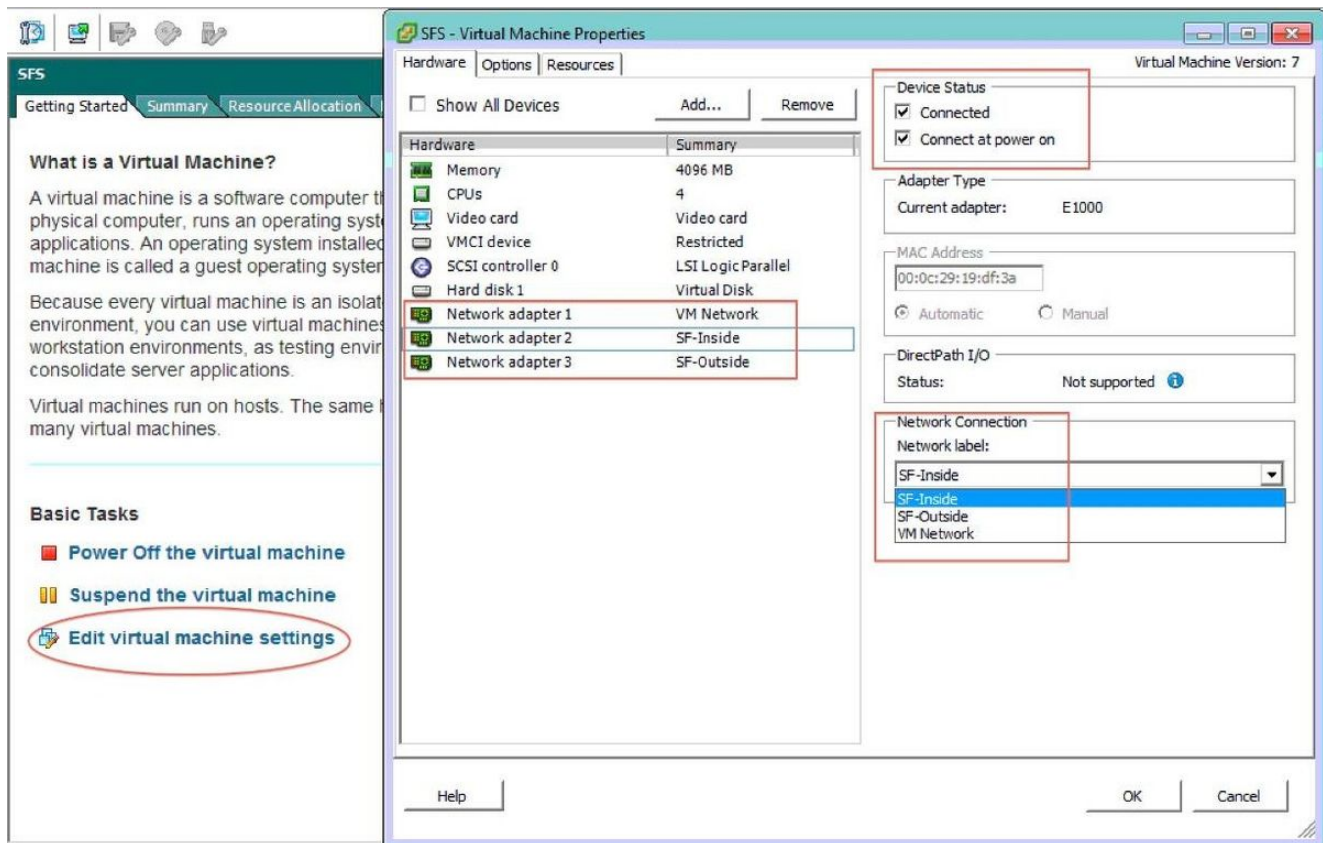
Примечание: Гарантируйте, что ИДЕНТИФИКАТОР VLAN настроен к 4095 для NGIPsv, это требуется согласно документу NGIPsv:

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



vSwitch конфигурация на ESXi завершена. Теперь необходимо проверить интерфейсные параметры настройки:

1. Перейдите к виртуальной машине для устройства FirePOWER.
2. Нажмите параметры настройки виртуальной машины **Edit**.
3. Проверьте все эти три адаптера сети.
4. Гарантируйте, что они должным образом выбраны, как показано здесь:



Зарегистрируйте устройство FirePOWER в центре управления FireSIGHT

Завершите процедуры, которые описаны в Документе Cisco для регистрации устройства FirePOWER в Центре управления FireSIGHT.

Перенаправьте и проверьте трафик

В этом разделе описывается перенаправить трафик и как проверить пакеты.

Трафик перенаправления с ISR на Датчик на UCS-E

Используйте эту информацию для перенаправления трафика:

```
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
```

Примечание: При текущем выполнении Версии 3.16.1 или позже используйте усовершенствованную команду `utd механизма` вместо `utd` команды.

Проверьте перенаправление пакетов

От консоли ISR введите эту команду, чтобы проверить, инкрементно увеличиваются ли счетчики пакетов:

```
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
```

Проверка

Можно использовать эти команды показа, чтобы проверить, что конфигурация работает должным образом:

- покажите программное обеспечение плата utd глобальный
- покажите программное обеспечение плата utd интерфейсы
- покажите программное обеспечение плата utd армированный пластик активный глобальный
- покажите программное обеспечение плата utd fp активный глобальный
- покажите аппаратные средства плата qfp активная функция utd stats
- show platform hardware qfp активная функция utd

Устранение неполадок

Можно использовать эти команды отладки для устранения проблем конфигурации:

- функция условия платформы отладки utd controlplane
- функция условия платформы отладки utd dataplane подрежим

Дополнительные сведения

- [Начинающее работу руководство для UCS Cisco серверы серии E и UCS Cisco сеть серии E вычисляет механизм, выпуск 2. x](#)
- [Руководство по поиску и устранению проблем для UCS Cisco серверы серии E и UCS Cisco сеть серии E вычисляет механизм](#)
- [Начинающее работу руководство для UCS Cisco серверы серии E и UCS Cisco сеть серии E вычисляет механизм, выпуск 2.x – обновление микропрограммного обеспечения](#)
- [Руководство по конфигурации программного обеспечения сервисных маршрутизаторов агрегации Cisco ASR серии 1000 – интерфейсы домена моста Настройки](#)
- [Руководство пользователя утилиты обновления хоста для UCS Cisco серверы серии E и UCS Cisco сеть серии E вычисляет механизм – обновление микропрограммного обеспечения на UCS Cisco серверы серии E](#)
- [Cisco Systems – техническая поддержка и документация](#)