Konfigurieren von FirePOWER-Services auf ISR-Geräten mit dem UCS-E-Blade

Inhalt

Einführung

Dieses Dokument beschreibt die Installation und Bereitstellung der Cisco FirePOWER-Software auf einer Cisco Unified Computing System Blade-Plattform der E-Serie (UCS-E) im IDS-Modus (Intrusion Detection System). Das in diesem Dokument beschriebene Konfigurationsbeispiel ist eine Ergänzung zum offiziellen Benutzerhandbuch.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Integrated Services Router (ISR) XE-Image 3.14 oder höher
- Cisco Integrated Management Controller (CIMC) Version 2.3 oder höher
- Cisco FireSIGHT Management Center (FMC) Version 5.2 oder höher
- Cisco FirePOWER Virtual Device (NGIPSv) Version 5.2 oder höher
- VMware ESXi Version 5.0 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

> **Hinweis**: Bevor Sie den Code auf Version 3.14 oder höher aktualisieren, stellen Sie sicher, dass das System über ausreichend Speicherplatz, Speicherplatz und eine Lizenz für das Upgrade verfügt. Siehe Beispiel 1: Kopieren Sie das Bild in den Flash-Speicher: im Abschnitt "TFTP-Server" des Dokuments "Access Router Software Upgrade Procedures Cisco" (Softwareaktualisierungsverfahren für Access Router), um mehr über Code-Upgrades zu erfahren.

> **Hinweis**: Zur Aktualisierung von CIMC, BIOS und anderen Firmware-Komponenten können Sie entweder das Cisco Host Upgrade Utility (HUU) verwenden oder die Firmware-Komponenten manuell aktualisieren. Weitere Informationen zum Firmware-Upgrade finden Sie im Abschnitt Firmware-Aktualisierung für Cisco UCS Server der E-Serie im Benutzerhandbuch für das Host Upgrade Utility für Cisco UCS Server der E-Serie und die Cisco UCS Network Compute Engine der E-Serie.

Hintergrundinformationen

Dieser Abschnitt enthält Informationen zu den unterstützten Hardwareplattformen, Lizenzen und Einschränkungen hinsichtlich der in diesem Dokument beschriebenen Komponenten und Verfahren.

Unterstützte Hardwareplattformen

In diesem Abschnitt werden die unterstützten Hardwareplattformen für Geräte der Serien G2 und 4000 aufgeführt.

ISR G2-Geräte mit UCS-E-Blades

Diese Geräte der ISR G2-Serie mit Blades der UCS E-Serie werden unterstützt:

Produkt	Plattform	UCS-E-Modell
Cisco ISR der Serie 2900	2911	UCS-E 120/140 Single-Wide-Option
	2921	UCS-E 120/140/160/180 Option mit einfacher oder doppelter Breite
	2951	UCS-E 120/140/160 Option mit einfacher oder doppelter Breite
Cisco ISR der Serie 3900	3925	UCS-E 120/140/160 mit einfacher und doppelter Breite oder 180 mit doppelter Breite
	3925E	UCS-E 120/140/160 mit einfacher und doppelter Breite oder 180 mit doppelter Breite
	3945	UCS-E 120/140/160 mit einfacher und doppelter Breite oder 180 mit doppelter Breite
	3945E	UCS-E 120/140/160 mit einfacher und doppelter Breite oder 180 mit doppelter Breite

ISR 4000-Geräte mit UCS-E-Blades

Diese Geräte der Serie ISR 4000 mit Blades der Serie UCS-E werden unterstützt:

Produkt	Plattform	UCS-E-Modell
Cisco ISR der Serie 4400	4451	UCS-E 120/140/160 mit einfacher und doppelter Breite oder 180 mit dop Breite
	4431	UCS-E-Netzwerkschnittstellenmodul
Cisco ISR der Serie 4300	4351	UCS-E 120/140/160/180 mit einfacher und doppelter Breite oder 180 mit doppelter Breite
	4331	UCS-E 120/140 Single-Wide-Option
	4321	UCS-E-Netzwerkschnittstellenmodul

Lizenzen

Der ISR muss über eine Sicherheits-K9-Lizenz und eine Appx-Lizenz verfügen, um den Service zu aktivieren.

Einschränkungen

Im Folgenden sind zwei Einschränkungen hinsichtlich der in diesem Dokument beschriebenen Informationen aufgeführt:

- Multicast wird nicht unterstützt.
- Pro System werden nur 4.096 Bridge Domain Interfaces (BDI) unterstützt.

Die BDIs unterstützen folgende Funktionen nicht:

- BFD-Protokoll (Bidirectional Forwarding Detection)
- NetFlow
- Quality of Service (QoS)
- Network-Based Application Recognition (NBAR) oder Advanced Video Coding (AVC)
- Zonenbasierte Firewall (ZBF)
- Kryptografische VPNs
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) over Ethernet (PPPoE)

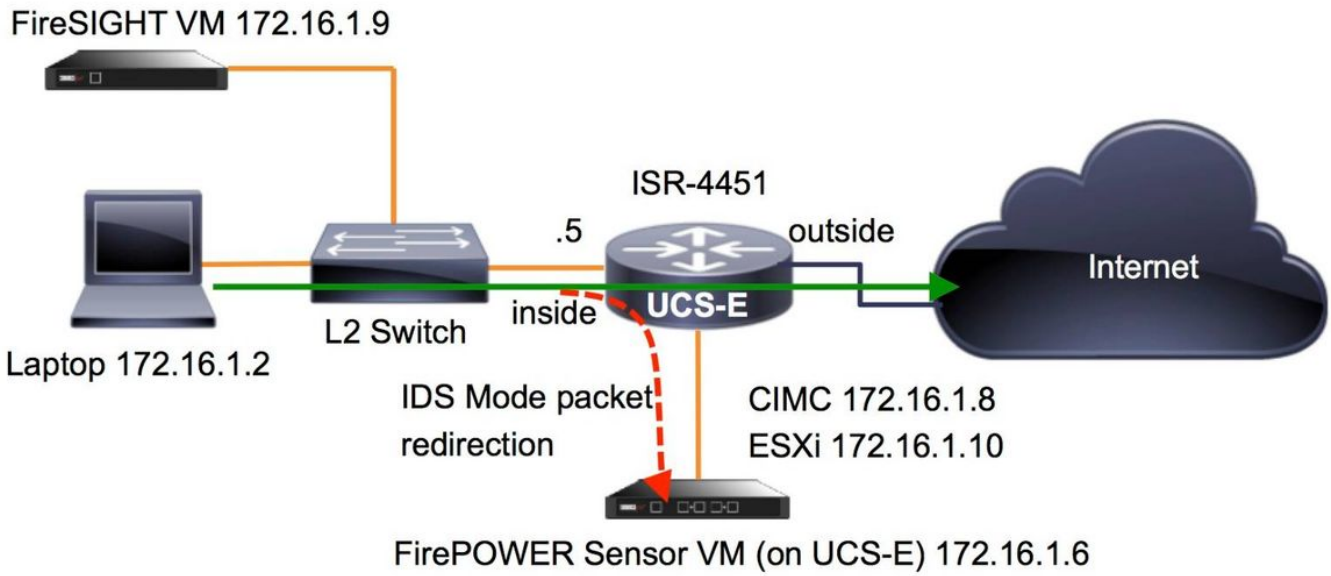
Hinweis: Für eine BDI kann die Größe der Maximum Transmission Unit (MTU) mit einem beliebigen Wert zwischen 1.500 und 9.216 Byte konfiguriert werden.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die Komponenten konfigurieren, die an dieser Bereitstellung beteiligt sind.

Netzwerkdiagramm

Die in diesem Dokument beschriebene Konfiguration verwendet folgende Netzwerktopologie:



Workflow für FirePOWER Services auf UCS-E

Nachfolgend finden Sie den Workflow für FirePOWER-Services, die auf einem UCS-E ausgeführt werden:

1. Die Datenebene leitet den Datenverkehr zur Überprüfung von der BDI/UCS-E-Schnittstelle aus (funktioniert für Geräte der Serien G2 und G3).
2. Die Cisco IOS®-XE CLI aktiviert die Paketweiterleitung für die Analyse (Optionen für alle Schnittstellen oder pro Schnittstelle).
3. Das CLI-**Setup-**Startup-Skript für den Sensor vereinfacht die Konfiguration.

CIMC konfigurieren

In diesem Abschnitt wird die Konfiguration des CIMC beschrieben.

Verbindung mit CIMC herstellen

Es gibt mehrere Möglichkeiten, eine Verbindung zum CIMC herzustellen. In diesem Beispiel wird die Verbindung zum CIMC über einen dedizierten Management-Port hergestellt. Stellen Sie

sicher, dass Sie den **M**-Port (dediziert) mithilfe eines Ethernet-Kabels mit dem Netzwerk verbinden. Führen Sie nach der Verbindung den Befehl **hw-module subslot** über die Router-Eingabeaufforderung aus:

```
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
```

Tipp 1: Zum Beenden führen Sie **^a^q aus**.

Tipp 2: Der Standard-Benutzername lautet **admin** und password <password>. Das Verfahren zum Zurücksetzen von Kennwörtern wird hier beschrieben: 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

CIMC konfigurieren

Verwenden Sie diese Informationen, um die Konfiguration des CIMC abzuschließen:

```
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
```

Vorsicht: Stellen Sie sicher, dass Sie den Befehl **commit** ausführen, um die Änderungen zu speichern.

Hinweis: Der Modus wird bei Verwendung des Management-Ports auf **dedizierte** Werte

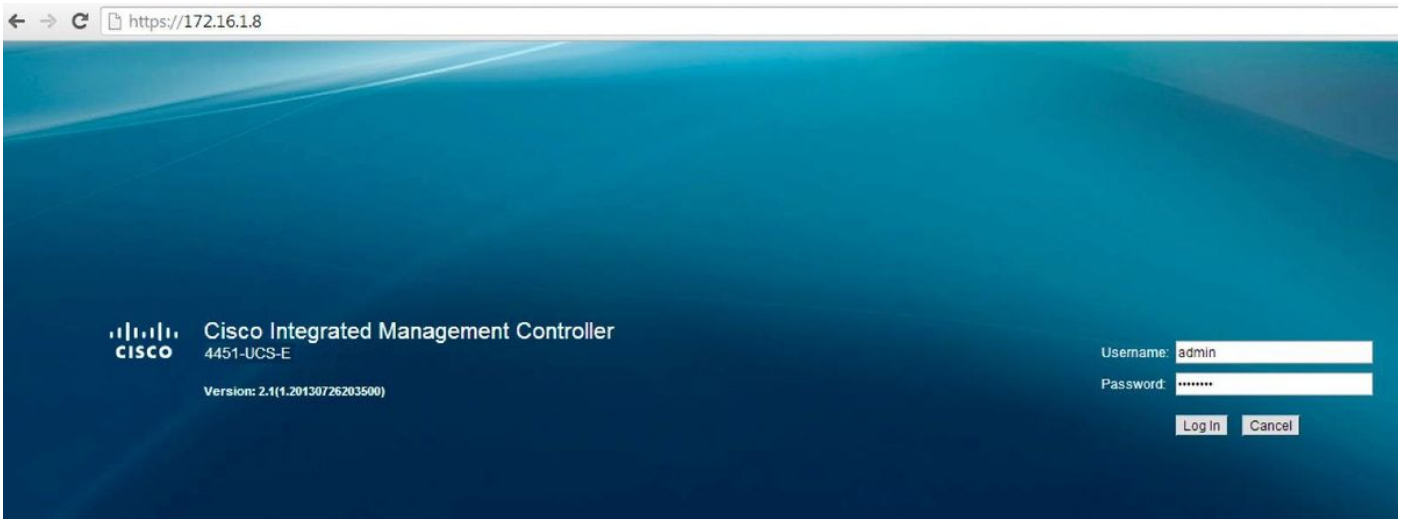
festgelegt.

Führen Sie den Befehl **show detail** aus, um die Detaileinstellungen zu überprüfen:

```
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 #
```

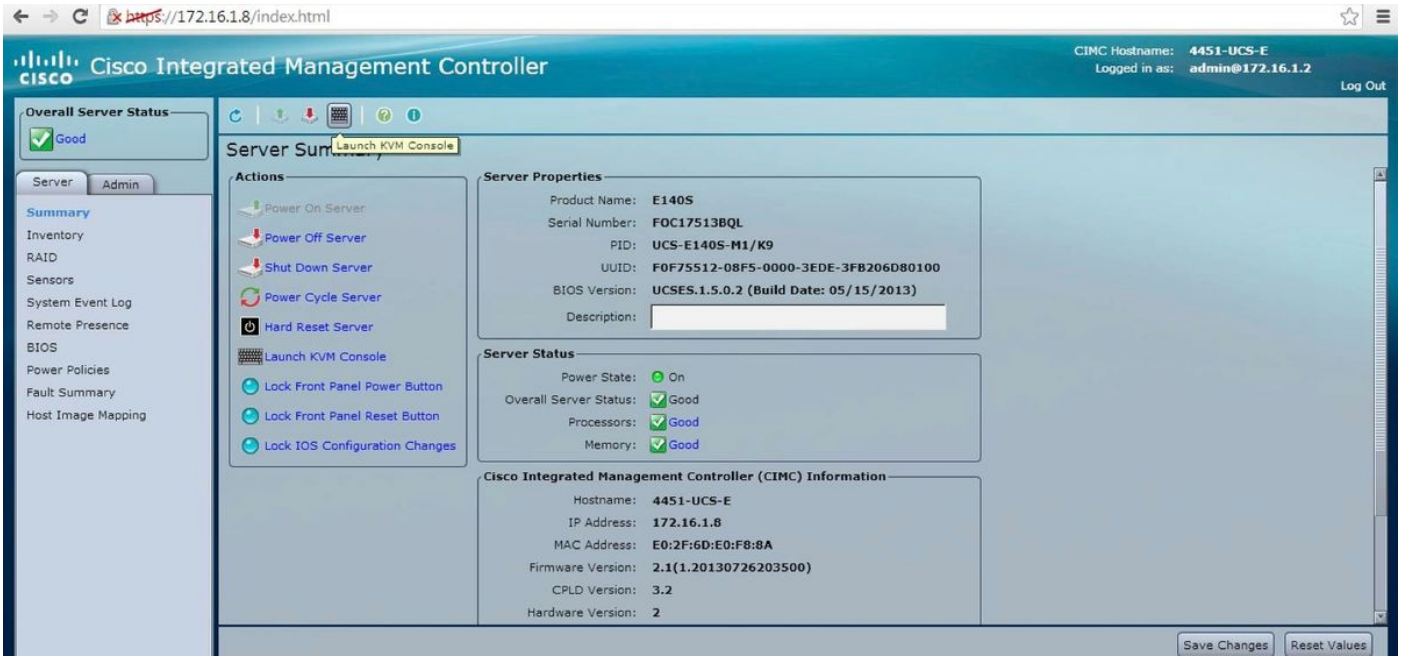
Starten Sie die Webschnittstelle des CIMC über einen Browser mit dem Standardbenutzernamen und -kennwort, wie im Bild gezeigt. Der Standardbenutzername und das Standardkennwort sind:

- Benutzername: **Administrator**
- Kennwort: **<Kennwort>**

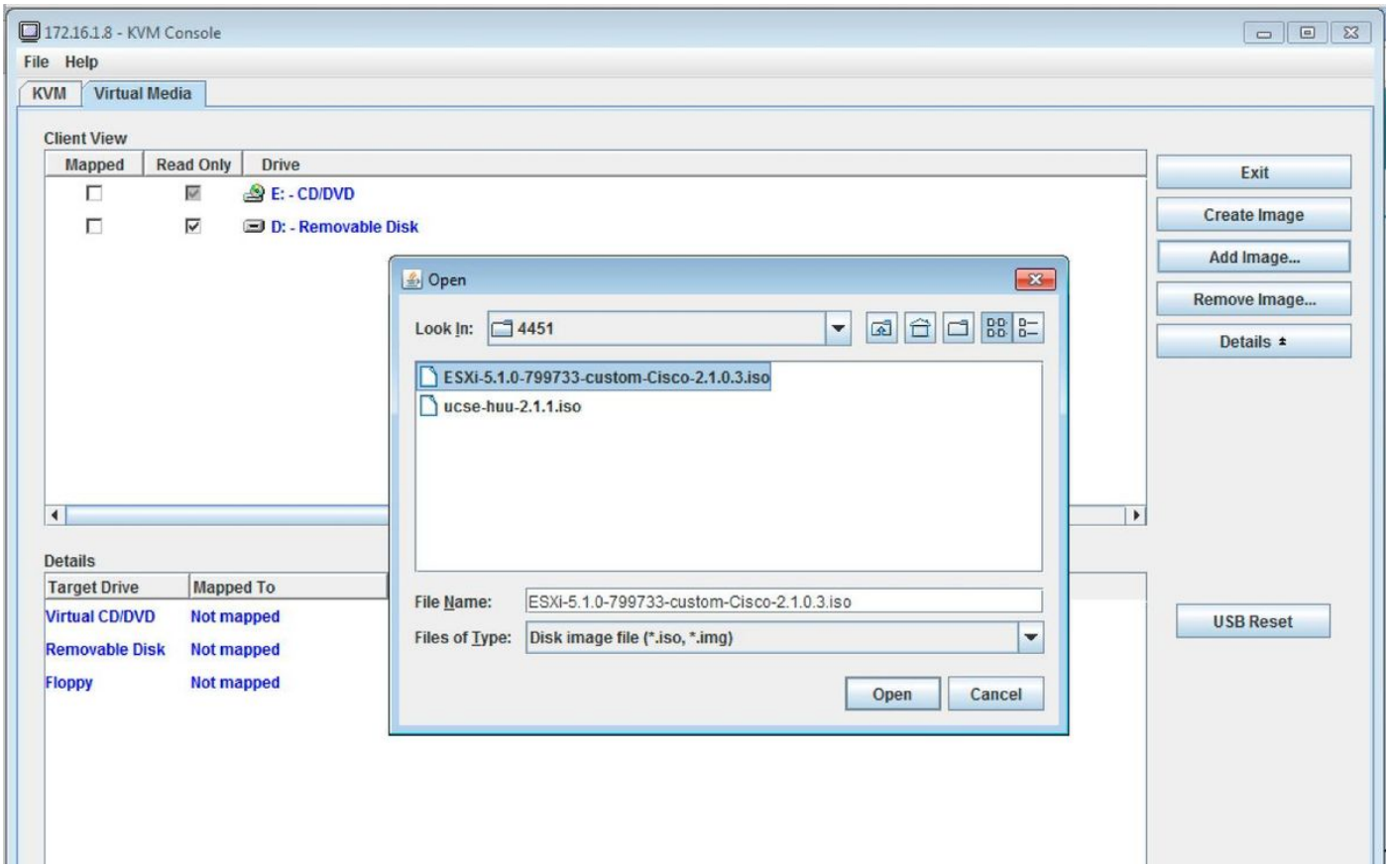


Installieren von ESXi

Nachdem Sie sich bei der Benutzeroberfläche des CIMC angemeldet haben, können Sie eine Seite anzeigen, die der in diesem Bild gezeigten Seite ähnelt. Klicken Sie auf das Symbol **KVM Console starten**, klicken Sie auf **Bild hinzufügen**, und ordnen Sie dann dem ESXi ISO das virtuelle Medium zu:



Klicken Sie auf die Registerkarte **Virtual Media** und dann auf **Add Image (Bild hinzufügen)**, um die virtuellen Medien wie im Bild dargestellt zuzuordnen.



Nachdem die virtuellen Medien zugeordnet wurden, klicken Sie auf der CIMC-Startseite auf **Power Cycle Server**, um das UCS-E aus- und wieder einzuschalten. Die ESXi-Konfiguration wird über Virtual Media gestartet. Schließen Sie die ESXi-Installation ab.

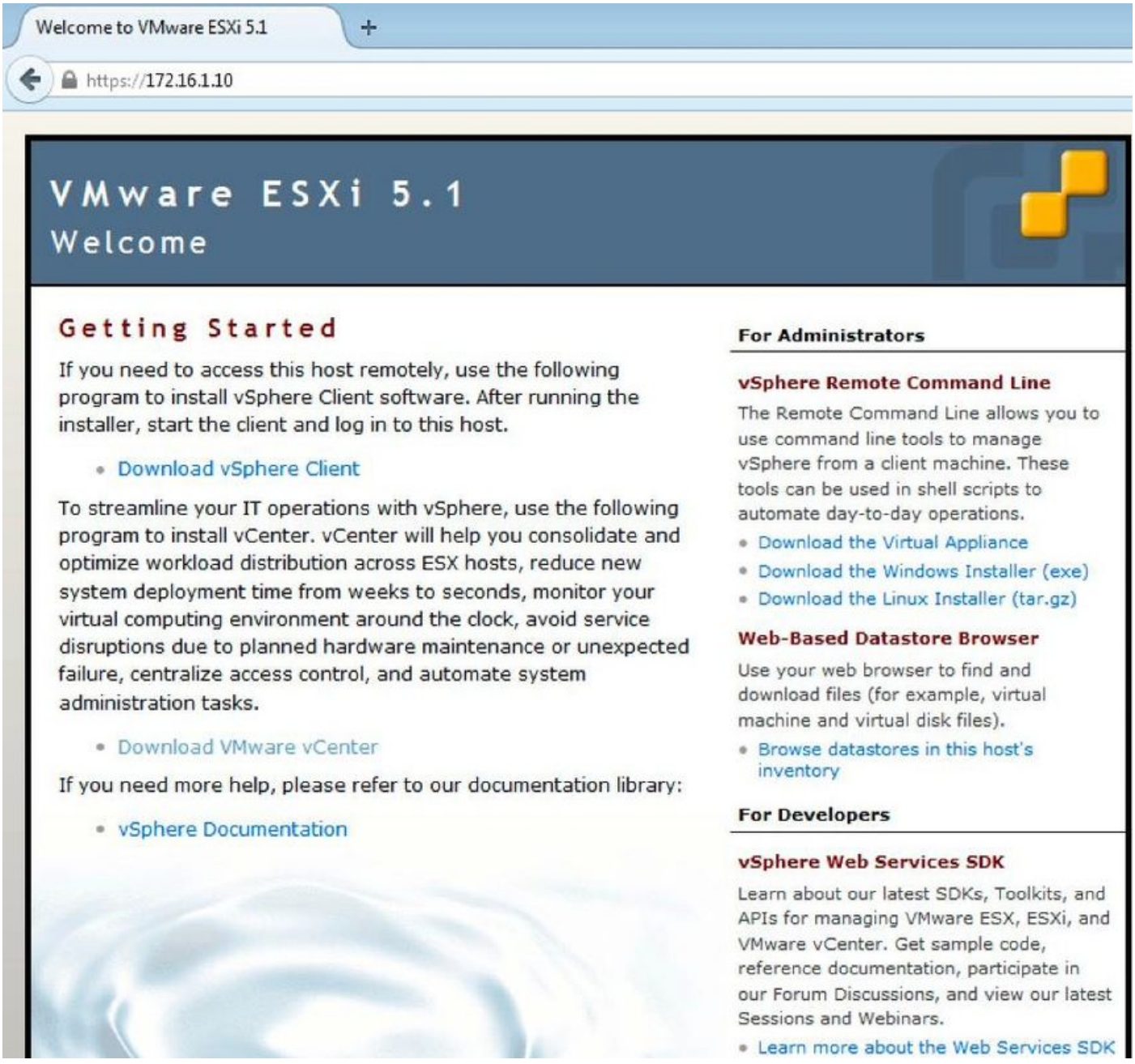
> **Hinweis**: Notieren Sie die ESXi-IP-Adresse, den Benutzernamen und das Kennwort, um später darauf zurückgreifen zu können.

vSphere-Client installieren

In diesem Abschnitt wird beschrieben, wie der vSphere-Client installiert wird.

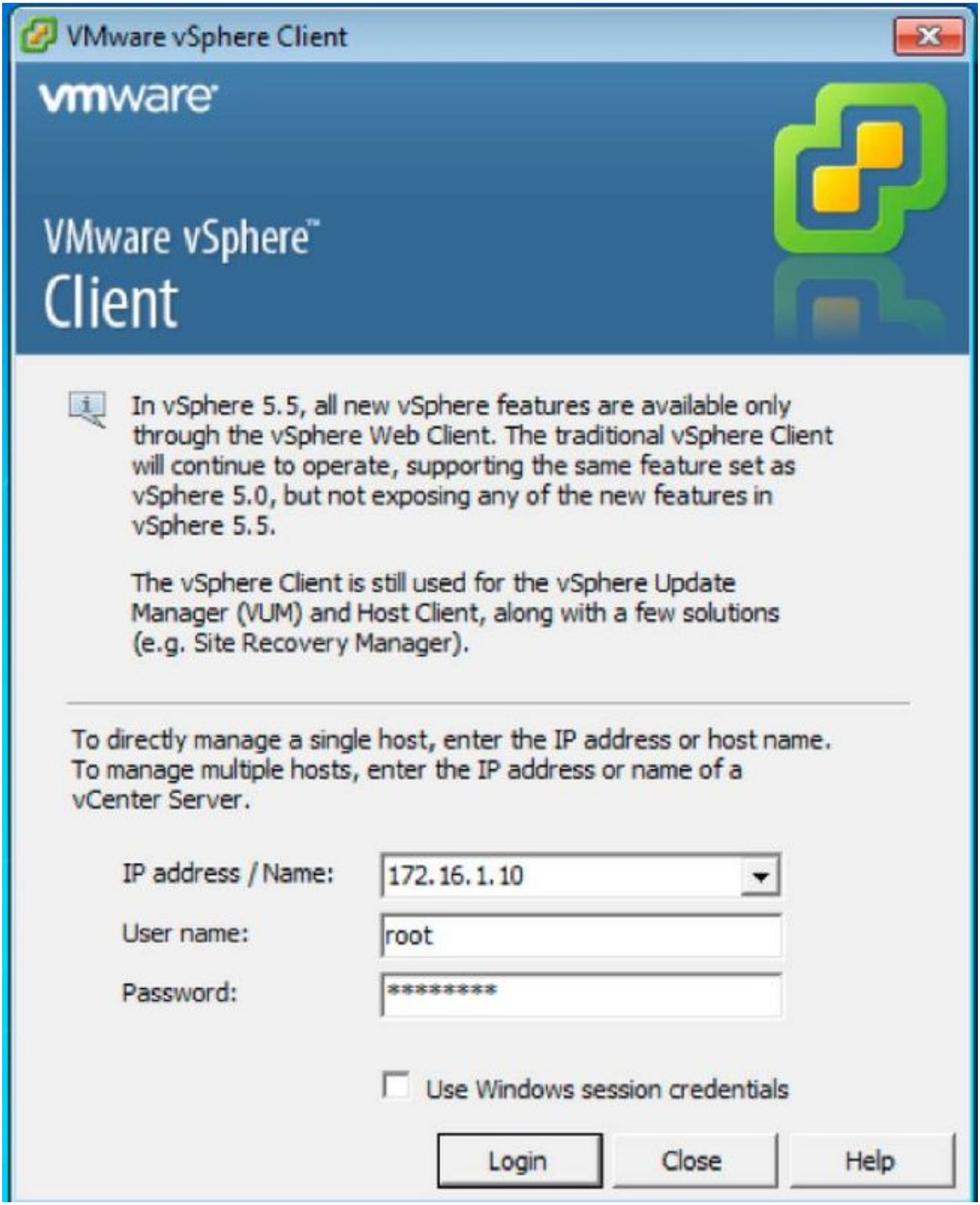
vSphere-Client herunterladen

Starten Sie ESXi und verwenden Sie den Link **Download VSphere Client**, um den vSphere Client herunterzuladen. Installieren Sie es auf Ihrem Computer.



vSphere-Client starten

Starten Sie den vSphere-Client von Ihrem Computer aus. Melden Sie sich mit dem Benutzernamen und dem Kennwort an, die Sie während der Installation erstellt haben und wie im Abbild gezeigt:



Bereitstellung von FireSIGHT Management Center und FirePOWER-Geräten

Führen Sie die im Dokument Bereitstellung von FireSIGHT Management Center auf VMware ESXi Cisco beschriebenen Verfahren aus, um ein FireSIGHT Management Center auf dem ESXi bereitzustellen.

Hinweis: Der Prozess für die Bereitstellung eines FirePOWER NGIPSv-Geräts ähnelt dem Prozess für die Bereitstellung eines Management Center.

Schnittstellen

Auf dem Dual-Wide UCS-E gibt es vier Schnittstellen:

- Die höchste MAC-Adressenschnittstelle ist Gi3 auf der Vorderseite.
- Die zweithöchste MAC-Adressenschnittstelle ist Gi2 auf der Vorderseite.
- Die letzten beiden werden als interne Schnittstellen angezeigt.

Auf dem Single-Wide UCS-E gibt es drei Schnittstellen:

- Die höchste MAC-Adressenschnittstelle ist Gi2 an der Vorderseite
- Die letzten beiden werden als interne Schnittstellen angezeigt.

Beide UCS-E-Schnittstellen des ISR4K sind Trunk-Ports.

Das UCS-E 120S und 140S verfügt über drei Netzwerkadapter plus Management-Ports:

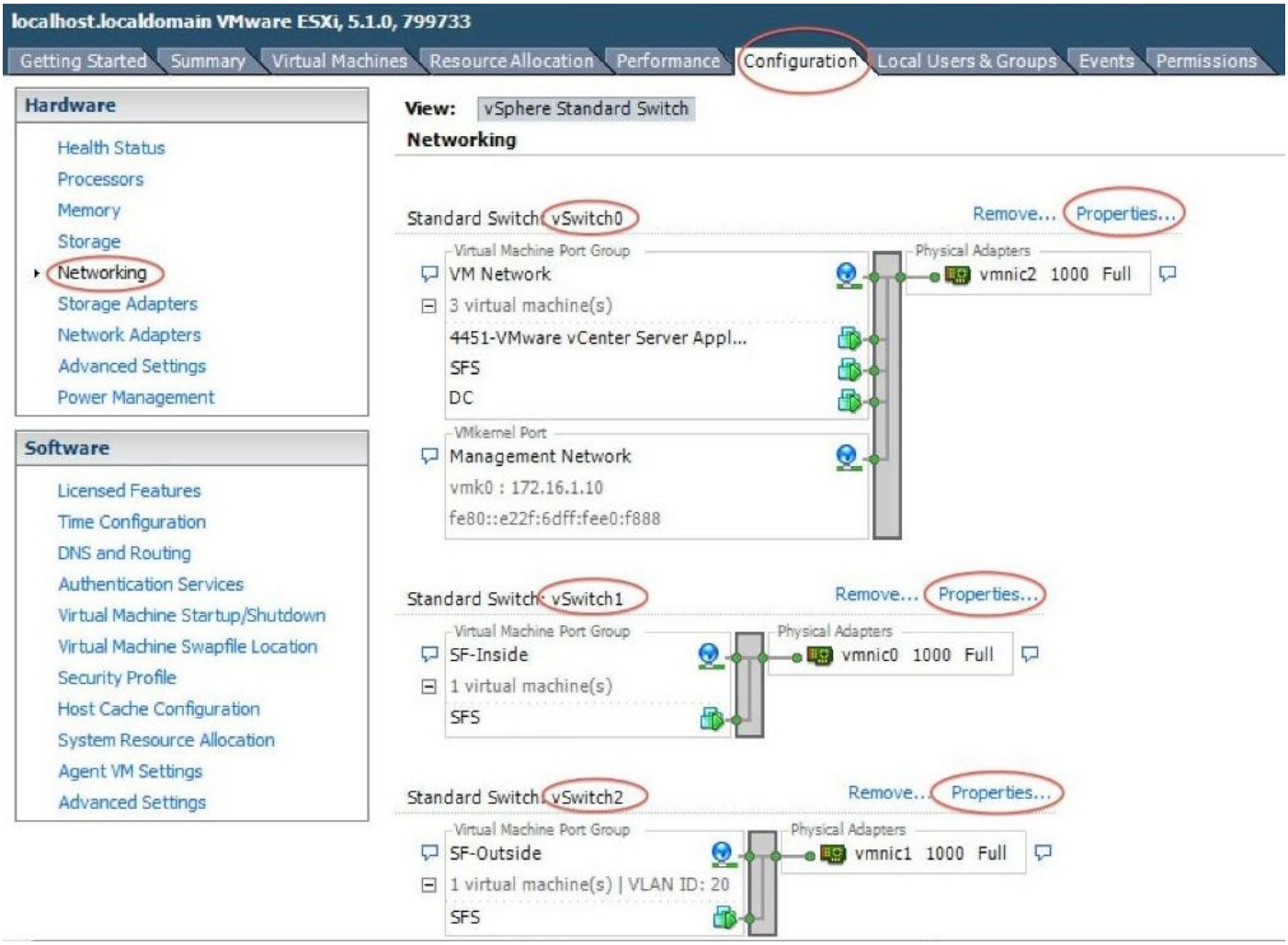
- Das *vmnic0* ist *UCSEx/0/0* auf der Router-Backplane zugeordnet.
- Die *vmnic1* ist *UCSEx/0/1* auf der Router-Backplane zugeordnet.
- Die *vmnic2* ist der GE2-Schnittstelle auf der UCS-E-Fronplane zugeordnet.
- Der Port für die Frontabdeckung (M) kann nur für den CIMC verwendet werden.

UCS-E 140D, 160D und 180D verfügen über vier Netzwerkadapter:

- Das *vmnic0* ist *UCSEx/0/0* auf der Router-Backplane zugeordnet.
- Die *vmnic1* ist *UCSEx/0/1* auf der Router-Backplane zugeordnet.
- Die *vmnic2* ist der GE2-Schnittstelle auf der UCS-E-Fronplane zugeordnet.
- Der *vminc3* ist der GE3-Schnittstelle auf der UCS-E-Frontebene zugeordnet.
- Der Port für die Frontabdeckung (M) kann nur für den CIMC verwendet werden.

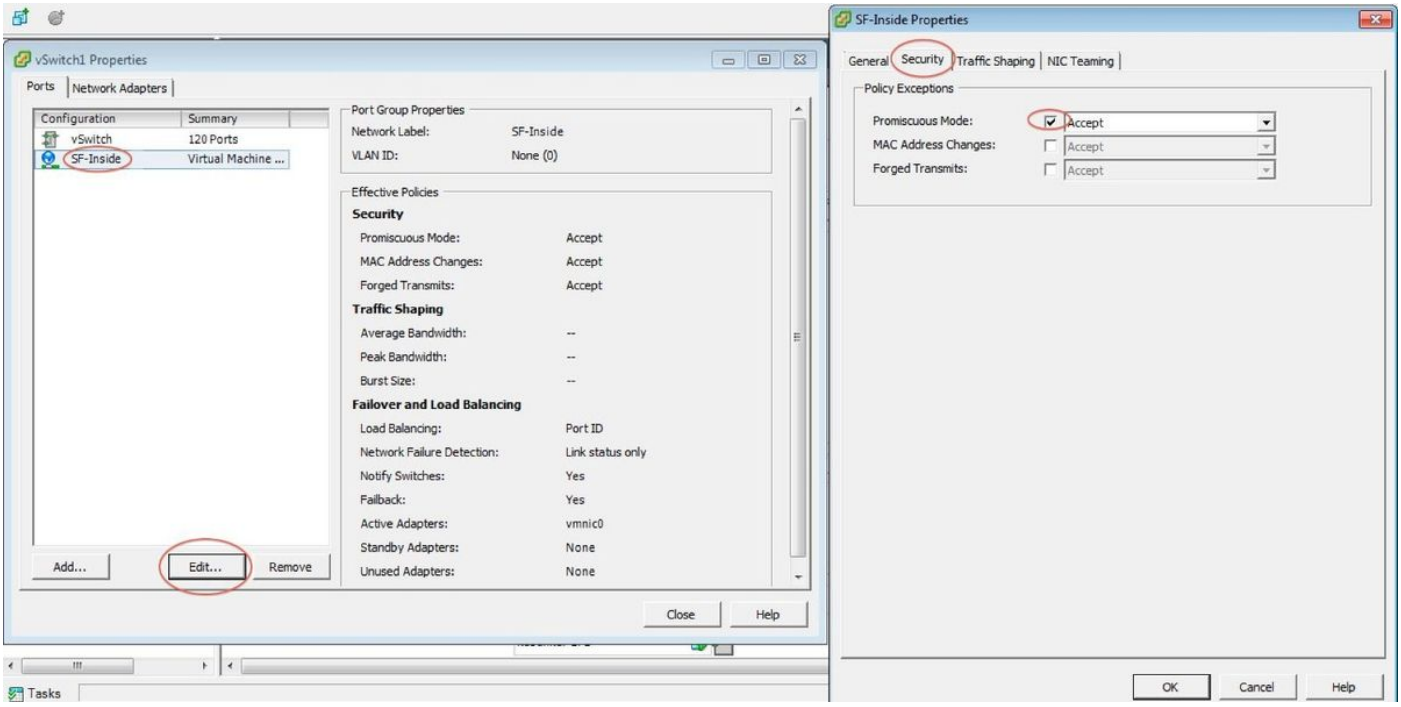
vSwitch-Schnittstellen auf ESXi

Der vSwitch0 auf dem ESXi ist die Verwaltungsschnittstelle, über die das ESXi, das FireSIGHT Management Center und das FirePOWER NGIPSv-Gerät mit dem Netzwerk kommunizieren. Klicken Sie auf **Eigenschaften** für den vSwitch1 (SF-Inside) und den vSwitch2 (SF-Outside), um Änderungen vorzunehmen.



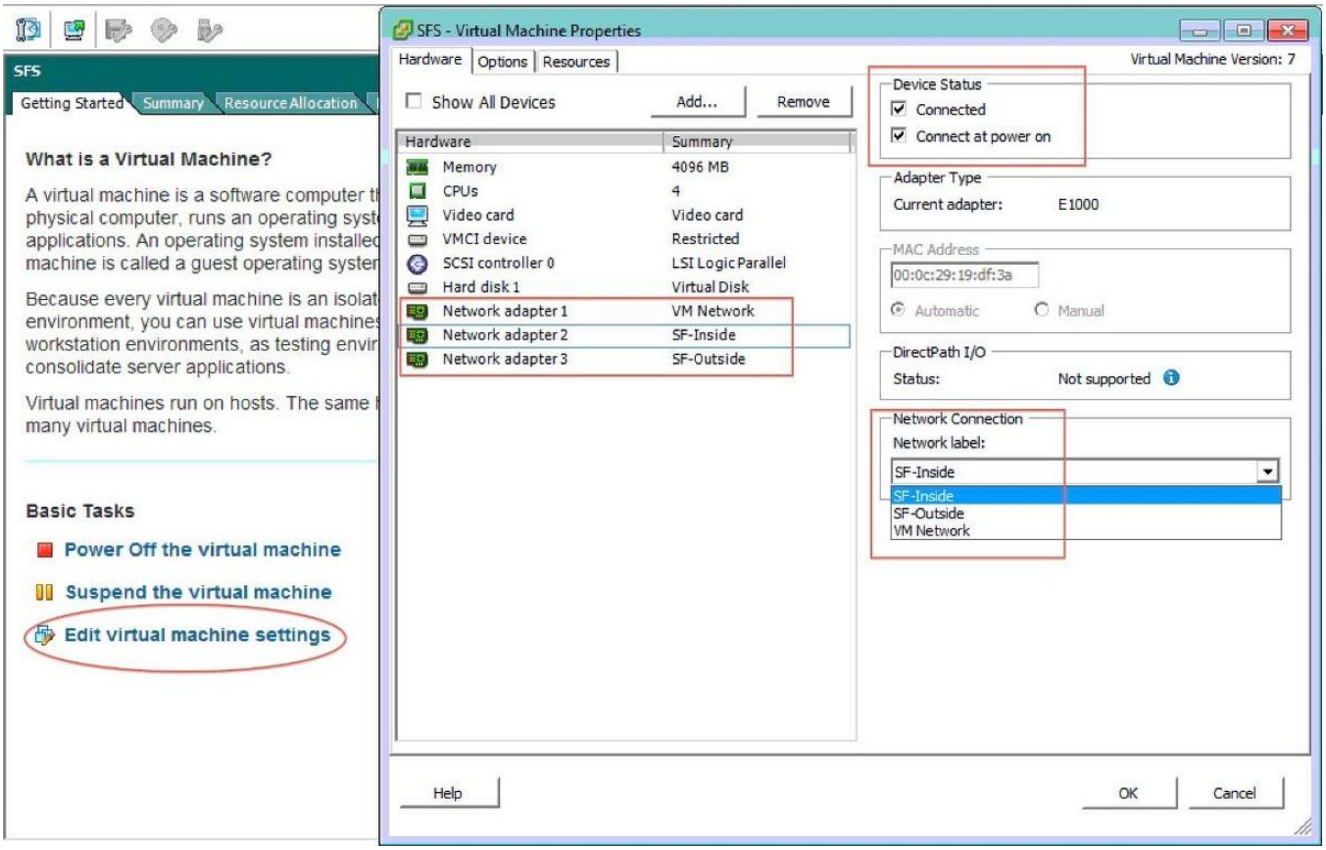
Dieses Bild zeigt die Eigenschaften des vSwitch1 (Sie müssen die gleichen Schritte für den vSwitch2 ausführen):

> **Hinweis**: Stellen Sie sicher, dass die VLAN-ID für NGIPSv auf 4095 konfiguriert ist. Dies ist gemäß NGIPSv-Dokument erforderlich: http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



Die vSwitch-Konfiguration auf dem ESXi ist abgeschlossen. Jetzt müssen Sie die Schnittstelleneinstellungen überprüfen:

1. Navigieren Sie zum virtuellen System für das FirePOWER-Gerät.
2. Klicken Sie auf **Einstellungen für virtuelle Systeme bearbeiten**.
3. Überprüfen Sie alle drei Netzwerkadapter.
4. Stellen Sie sicher, dass sie korrekt ausgewählt sind, wie in der Abbildung hier gezeigt:



Registrierung von FirePOWER-Geräten mit FireSIGHT Management Center

Führen Sie die im Cisco Dokument beschriebenen Verfahren aus, um ein FirePOWER-Gerät bei einem FireSIGHT Management Center zu registrieren.

Umleiten und Überprüfen von Datenverkehr

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

In diesem Abschnitt wird beschrieben, wie Datenverkehr umgeleitet wird und wie die Pakete verifiziert werden.

Umleitung des Datenverkehrs vom ISR zum Sensor auf dem UCS-E

Verwenden Sie diese Informationen, um den Datenverkehr umzuleiten:

```
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
```

> **Hinweis**: Wenn Sie derzeit Version 3.16.1 oder höher ausführen, führen Sie den Befehl **utd engine advanced** anstelle des Befehls **utd aus**.

Paketweiterleitung überprüfen

Führen Sie diesen Befehl in der ISR-Konsole aus, um zu überprüfen, ob die Paketzähler inkrementell sind:

```
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
```

Überprüfen

Sie können die folgenden **show**-Befehle ausführen, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert:

- **show plat software utglobal**
- **show plat software utschnittstellen**
- **show plat software utrp active global**
- **show plat software utfp active global**
- **show plat hardware qfp active feature utstats**
- **show platform hardware qfp active feature uth**

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Sie können diese **Debugbefehle** ausführen, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen:

- **Fehlerbehebungszustandsfunktion für die Steuerungsplattform**
- **Debug-Plattformzustandsfunktion UTD DataGane Submodus**

Zugehörige Informationen

- Erste Schritte für Cisco UCS Server der E-Serie und die Cisco UCS Network Compute Engine der E-Serie, Version 2.x
- Leitfaden zur Fehlerbehebung für Cisco UCS Server der E-Serie und die Cisco UCS Network Compute Engine der E-Serie
- Erste Schritte für Cisco UCS Server der E-Serie und die Cisco UCS Network Compute Engine der E-Serie, Version 2.x - Firmware-Aktualisierung
- Software-Konfigurationsleitfaden für Cisco Aggregation Services Router der Serie ASR 1000 - Konfigurieren von Bridge Domain-Schnittstellen
- Host Upgrade Utility - Benutzerhandbuch für Cisco UCS Server der E-Serie und die Cisco UCS Network Compute Engine der E-Serie - Aktualisieren der Firmware auf Cisco UCS Servern der E-Serie
- Technischer Support und Dokumentation - Cisco Systems