Configurazione dei servizi FirePOWER sui dispositivi ISR con blade UCS-E

Sommario

Introduzione

In questo documento viene descritto come installare e distribuire il software Cisco FirePOWER su una piattaforma blade Cisco Unified Computing System serie E (UCS-E) in modalità Intrusion Detection System (IDS). L'esempio di configurazione descritto in questo documento è un supplemento alla guida dell'utente ufficiale.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Integrated Services Router (ISR) XE immagine 3.14 o successiva
- Cisco Integrated Management Controller (CIMC) versione 2.3 o successiva
- Cisco FireSIGHT Management Center (FMC) versione 5.2 o successiva
- Cisco FirePOWER Virtual Device (NGIPSv) versione 5.2 o successive
- VMware ESXi versione 5.0 o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota:** Prima di aggiornare il codice alla versione 3.14 o successiva, verificare che il sistema disponga di memoria sufficiente, spazio su disco e una licenza per l'aggiornamento. Fare riferimento all'esempio 1: Copiare l'immagine su flash: dalla sezione server TFTP del documento Access Router Software Upgrade Procedures (Procedure di aggiornamento del software dei router di accesso) di Cisco per ulteriori informazioni sugli aggiornamenti del codice.

> **Nota:** Per aggiornare CIMC, BIOS e altri componenti del firmware, è possibile usare l'utility Cisco Host Upgrade (HUU) oppure aggiornare manualmente i componenti del firmware. Per ulteriori informazioni sull'aggiornamento del firmware, fare riferimento alla sezione Aggiornamento del firmware sui Cisco UCS serie E della guida per l'utente della Host Upgrade Utility per Cisco UCS serie E Server e a Cisco UCS serie E Network Compute Engine.

Premesse

In questa sezione vengono fornite informazioni sulle piattaforme hardware supportate, sulle licenze e sulle limitazioni relative ai componenti e alle procedure descritti nel presente documento.

Piattaforme hardware supportate

In questa sezione vengono elencate le piattaforme hardware supportate per i dispositivi serie G2 e 4000.

Dispositivi ISR G2 con blade UCS-E

Sono supportati i seguenti dispositivi ISR serie G2 con blade UCS-E:

Prodotto	Piattaforma	Modello UCS-E
Cisco serie 2900 ISR	2911	UCS-E 120/140 con singola opzione wide
	2921	UCS-E 120/140/160/180 single o double wide option
	2951	UCS-E 120/140/160 single o double wide option
Cisco serie 3900 ISR	3925	UCS-E 120/140/160 single e double wide option o 180 double wide
	3925E	UCS-E 120/140/160 single e double wide option o 180 double wide
	3945	UCS-E 120/140/160 single e double wide option o 180 double wide
	3945E	UCS-E 120/140/160 single e double wide option o 180 double wide

Dispositivi ISR 4000 con blade UCS-E

Sono supportati i seguenti dispositivi ISR serie 4000 con blade UCS serie E:

Prodotto	Piattaforma	Modello UCS-E
Cisco serie 4400 ISR	4451	UCS-E 120/140/160 single e double wide option o 180 double wide
	4431	UCS-E Network Interface Module
Cisco serie 4300 ISR	4351	UCS-E 120/140/160/180 single e double wide option o 180 double wide
	4331	UCS-E 120/140 con singola opzione wide
	4321	UCS-E Network Interface Module

Licenze

Per abilitare il servizio, l'ISR deve avere una licenza K9 di sicurezza, nonché una licenza appx.

Limitazioni

Di seguito sono riportati due limiti relativi alle informazioni descritte nel presente documento:

- Multicast non supportato
- Per ogni sistema sono supportate solo 4.096 interfacce di dominio con bridging (BDI)

Le BDI non supportano le seguenti funzioni:

- Protocollo BFD (Bidirectional Forwarding Detection)
- NetFlow
- QoS (Quality of Service)
- Riconoscimento delle applicazioni in rete (NBAR) o Advanced Video Coding (AVC)
- ZBF (Zone Based Firewall)
- VPN crittografiche
- Multiprotocol Label Switching (MPLS)
- Protocollo PPP (Point-to-Point) over Ethernet (PPPoE)

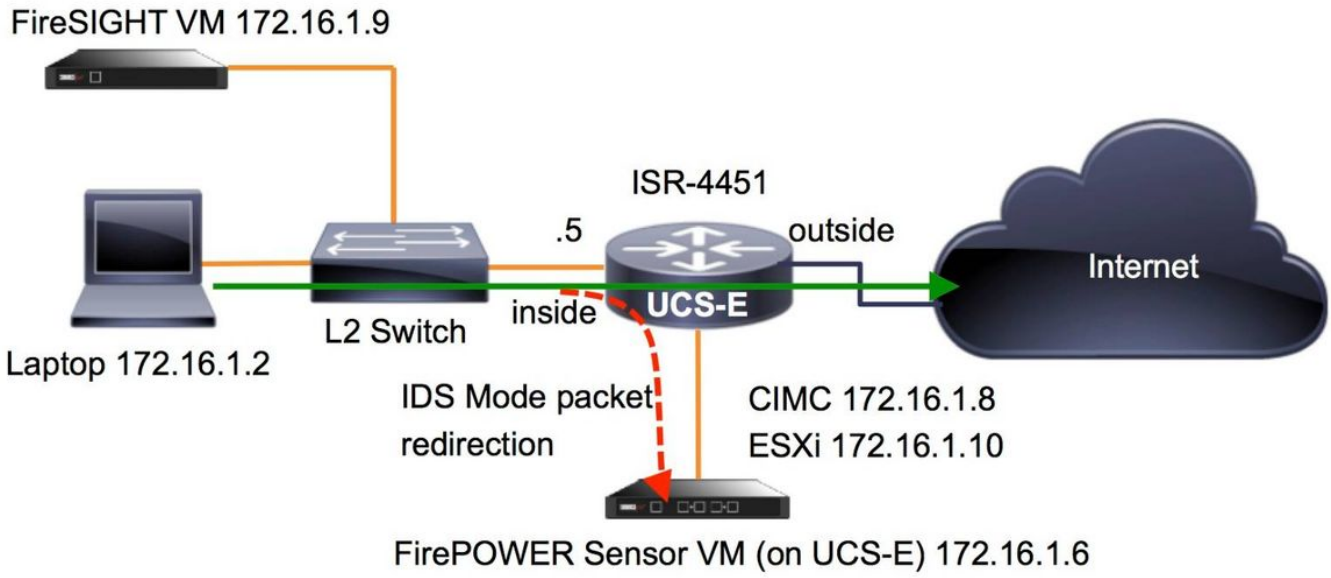
> **Nota:** Per una BDI, le dimensioni della MTU (Maximum Transmission Unit) possono essere configurate con un valore compreso tra 1.500 e 9.216 byte.

Configurazione

In questa sezione viene descritto come configurare i componenti coinvolti nella distribuzione.

Esempio di rete

La configurazione descritta in questo documento utilizza la seguente topologia di rete:



Flusso di lavoro per i servizi FirePOWER su UCS-E

Di seguito è riportato il flusso di lavoro per i servizi FirePOWER eseguiti su un UCS-E:

1. Il data-plane sposta il traffico per l'ispezione dall'interfaccia BDI/UCS-E (funziona con i dispositivi serie G2 e G3).
2. La CLI di Cisco IOS®-XE attiva il reindirizzamento dei pacchetti per l'analisi (opzioni per tutte le interfacce o per singola interfaccia).
3. Lo script di avvio dell'**installazione della** CLI del sensore semplifica la configurazione.

Configurazione di CIMC

Questa sezione descrive come configurare CIMC.

Connetti a CIMC

Èpossibile connettersi al CIMC in diversi modi. Nell'esempio, la connessione al CIMC viene completata tramite una porta di gestione dedicata. Accertarsi di collegare la porta **M** (dedicata) alla rete utilizzando un cavo Ethernet. Una volta connessi, eseguire il comando **hw-module subslot** dal prompt del router:

```
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
```

Suggerimento 1: Per uscire, eseguire **^a^q**.

Suggerimento 2: Il nome utente predefinito è **admin** e la password <password>. Il processo di reimpostazione della password è descritto di seguito: 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

Configurazione di CIMC

Utilizzare queste informazioni per completare la configurazione del 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
```

Attenzione: Accertarsi di eseguire il comando **commit** per salvare le modifiche.

Nota: La modalità è impostata su **dedicata** quando si utilizza la porta di gestione.

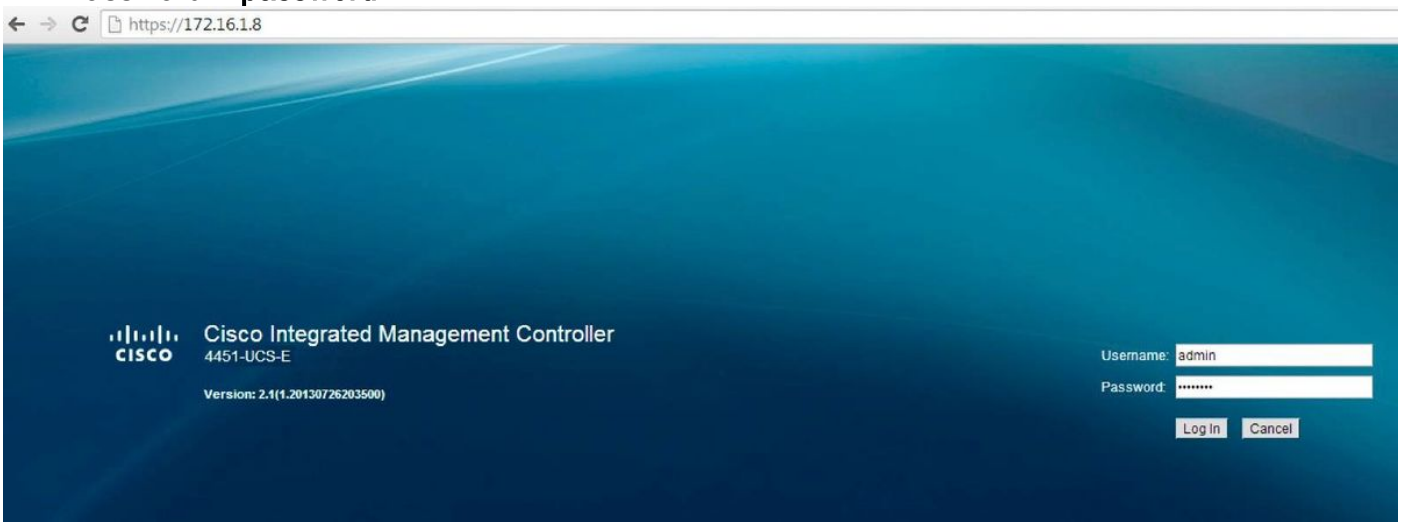
Eseguire il comando **show detail** per verificare le impostazioni di dettaglio:

```
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 #
```

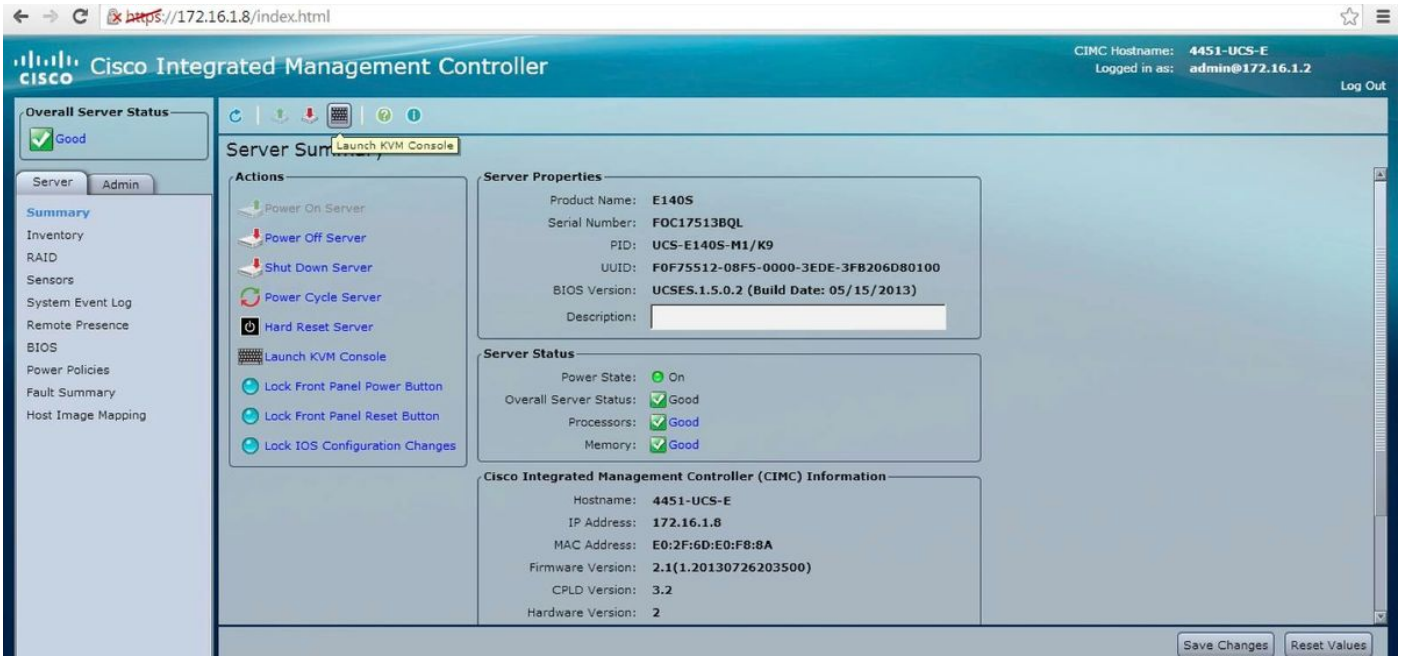
Avviare l'interfaccia Web del CIMC da un browser con il nome utente e la password predefiniti, come mostrato nell'immagine. Il nome utente e la password predefiniti sono:

- Username: **admin**
- Password: **<password>**

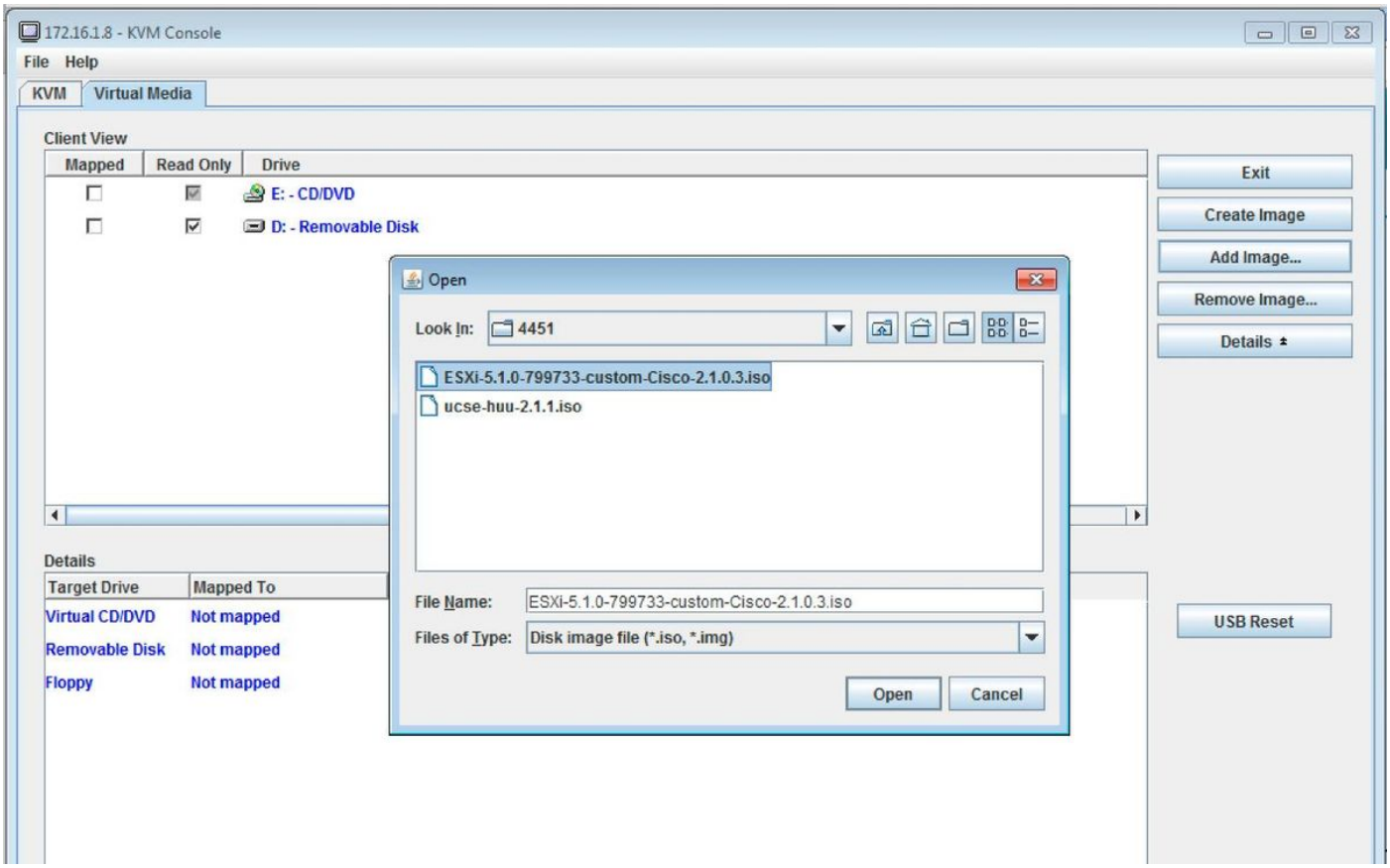


Installazione di ESXi

Dopo aver effettuato l'accesso all'interfaccia utente del CIMC, è possibile visualizzare una pagina simile a quella mostrata in questa immagine. Fare clic sull'icona **Avvia console KVM**, fare clic su **Aggiungi immagine**, quindi mappare ESXi ISO come supporto virtuale:



Fare clic sulla scheda **Supporto virtuale** e quindi su **Aggiungi immagine** per mappare il supporto virtuale come mostrato nell'immagine.



Una volta mappato il supporto virtuale, fare clic su **Power Cycle Server** nella home page di CIMC per spegnere e riaccendere UCS-E. La configurazione di ESXi viene avviata dal supporto virtuale. Completare l'installazione di ESXi.

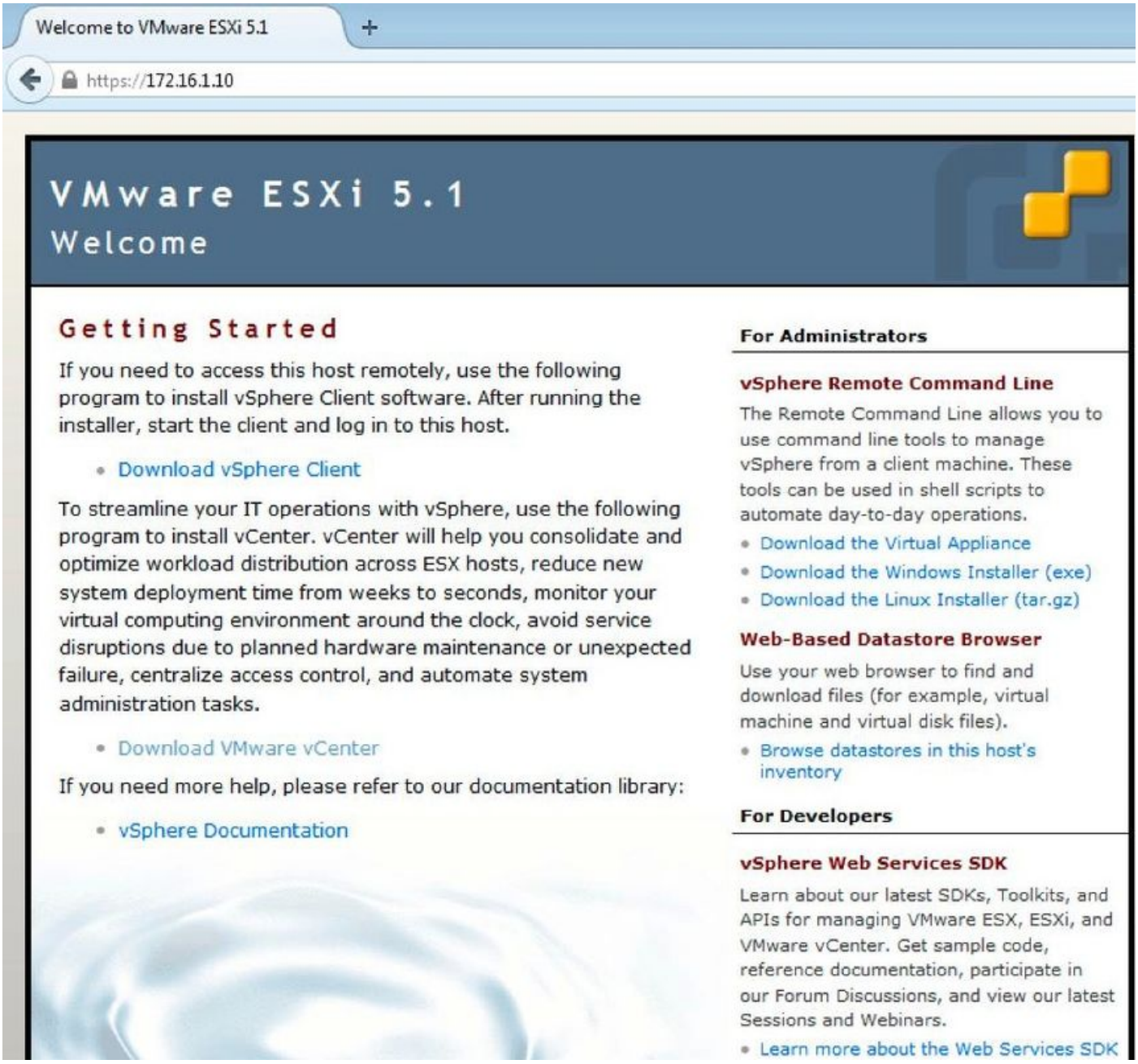
Nota: Registrare l'indirizzo IP, il nome utente e la password ESXi per riferimento futuro.

Installa client vSphere

Questa sezione descrive come installare il client vSphere.

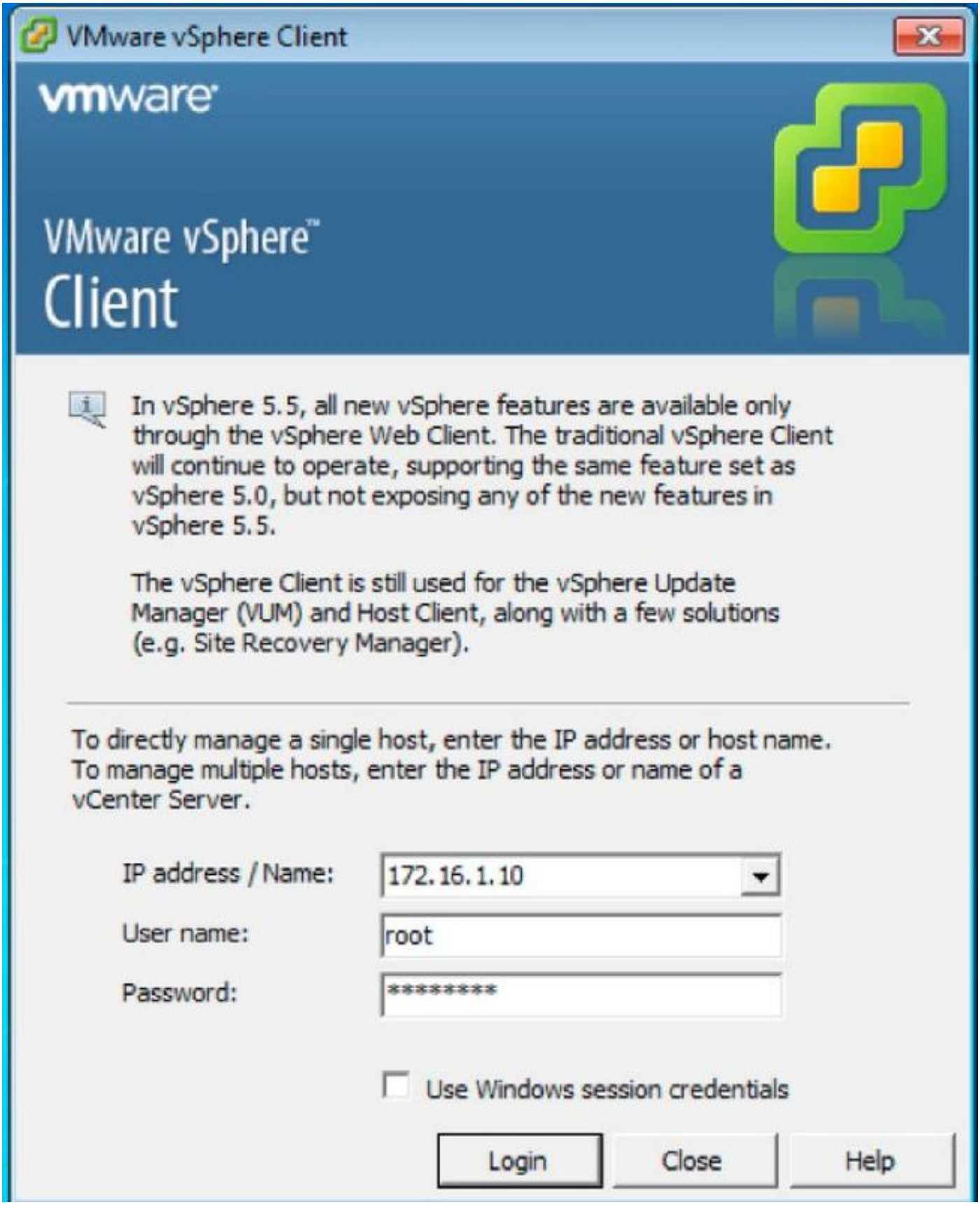
Scarica vSphere Client

Avviare ESXi e utilizzare il collegamento **Scarica client VSphere** per scaricare il client vSphere. Installarlo nel computer.



Avvia client vSphere

Avviare il client vSphere dal computer. Accedere con il nome utente e la password creati durante l'installazione e come mostrato nell'immagine:



Installazione di FireSIGHT Management Center e dei dispositivi FirePOWER

Completare le procedure descritte nel documento Installazione di FireSIGHT Management Center su VMware ESXi Cisco per installare un centro di gestione FireSIGHT su ESXi.

Nota: Il processo utilizzato per distribuire un dispositivo FirePOWER NGIPSv è simile al

processo utilizzato per installare un centro di gestione.

Interfacce

Sul modello UCS-E a doppio schermo sono presenti quattro interfacce:

- L'interfaccia dell'indirizzo MAC più alta è Gi3 sul pannello anteriore
- La seconda interfaccia più alta per gli indirizzi MAC è Gi2 sul pannello anteriore
- Le ultime due visualizzate sono le interfacce interne

Nell'UCS-E single-wide sono disponibili tre interfacce:

- L'interfaccia dell'indirizzo MAC più alta è Gi2 sul pannello anteriore
- Le ultime due visualizzate sono le interfacce interne

Entrambe le interfacce UCS-E sull'ISR4K sono porte trunk.

UCS-E 120S e 140S hanno tre adattatori di rete più porte di gestione:

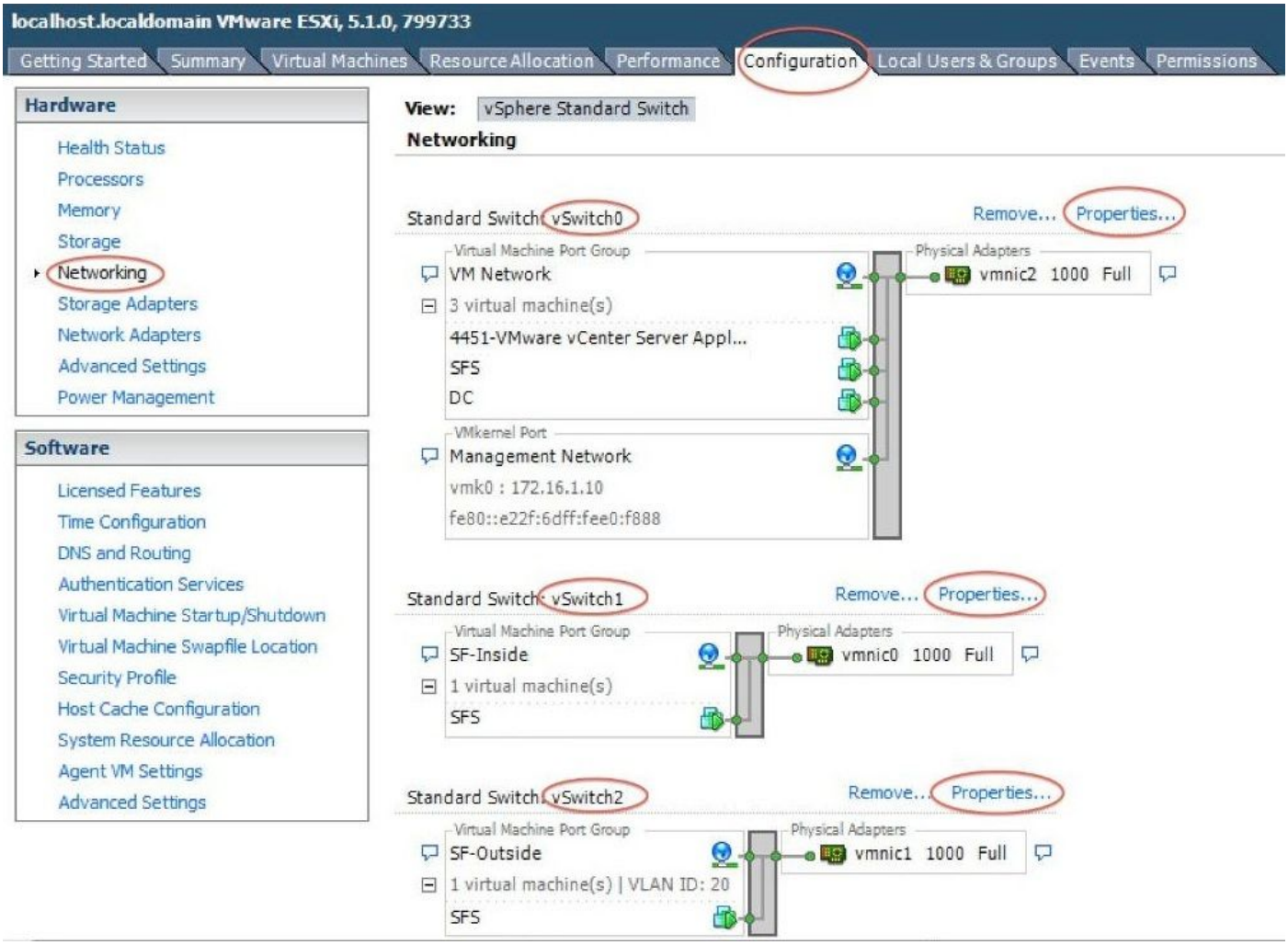
- Il comando *vmnic0* viene mappato su *UCSEx/0/0* sul backplane del router
- Il comando *vmnic1* è mappato su *UCSEx/0/1* sul backplane del router
- Il comando *vmnic2* viene mappato sul piano anteriore UCS-E dell'interfaccia GE2
- La porta di gestione del pannello anteriore (M) può essere utilizzata solo per il CIMC.

UCS-E 140D, 160D e 180D hanno quattro adattatori di rete:

- Il valore *vmnic0* viene mappato su *UCSEx/0/0* sul backplane del router.
- Il comando *vmnic1* viene mappato su *UCSEx/0/1* sul backplane del router.
- Il valore *vmnic2* viene mappato sull'interfaccia GE2 del piano anteriore UCS-E.
- Il comando *vminc3* è associato all'interfaccia GE3 del piano anteriore dell'UCS-E.
- La porta di gestione del pannello anteriore (M) può essere utilizzata solo per il CIMC.

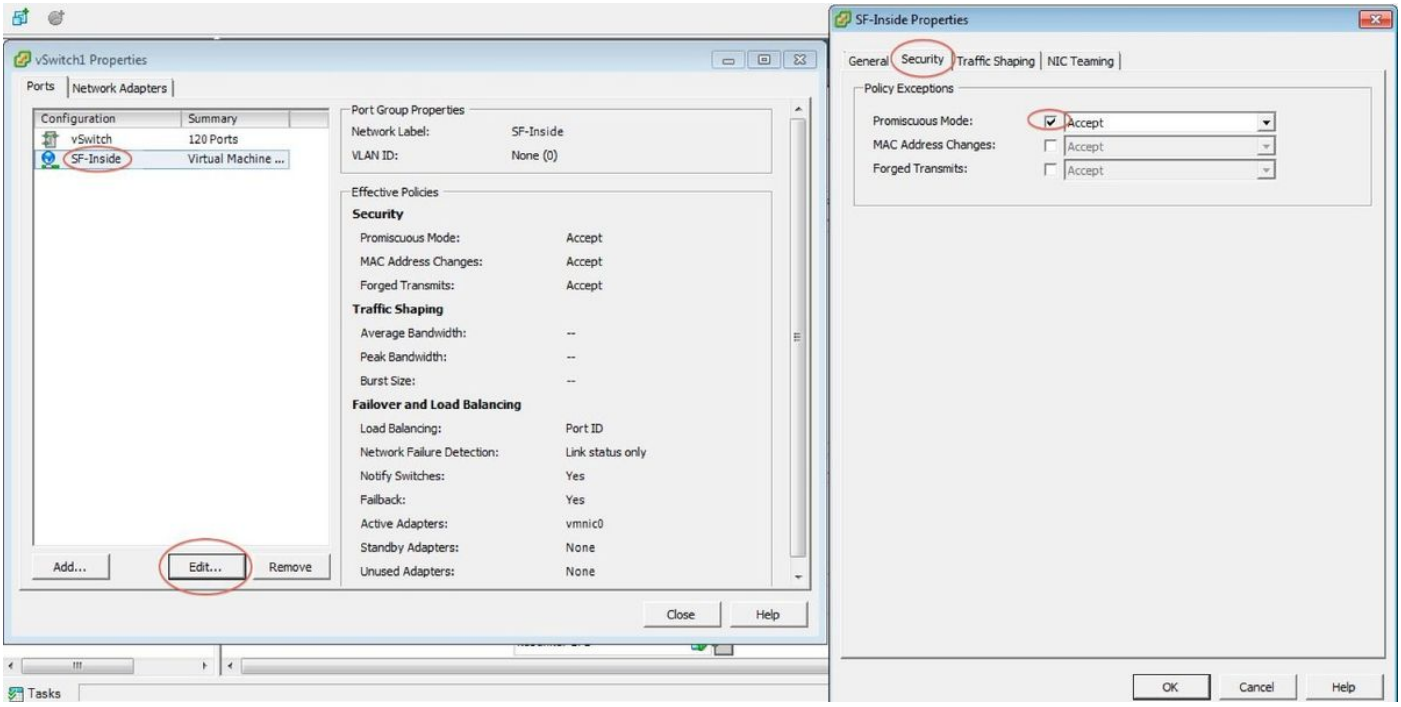
Interfacce vSwitch su ESXi

Il vSwitch0 su ESXi è l'interfaccia di gestione attraverso la quale ESXi, FireSIGHT Management Center e il dispositivo FirePOWER NGIPSv comunicano alla rete. Per apportare modifiche, fare clic su **Proprietà** per vSwitch1 (SF-Inside) e vSwitch2 (SF-Outside).



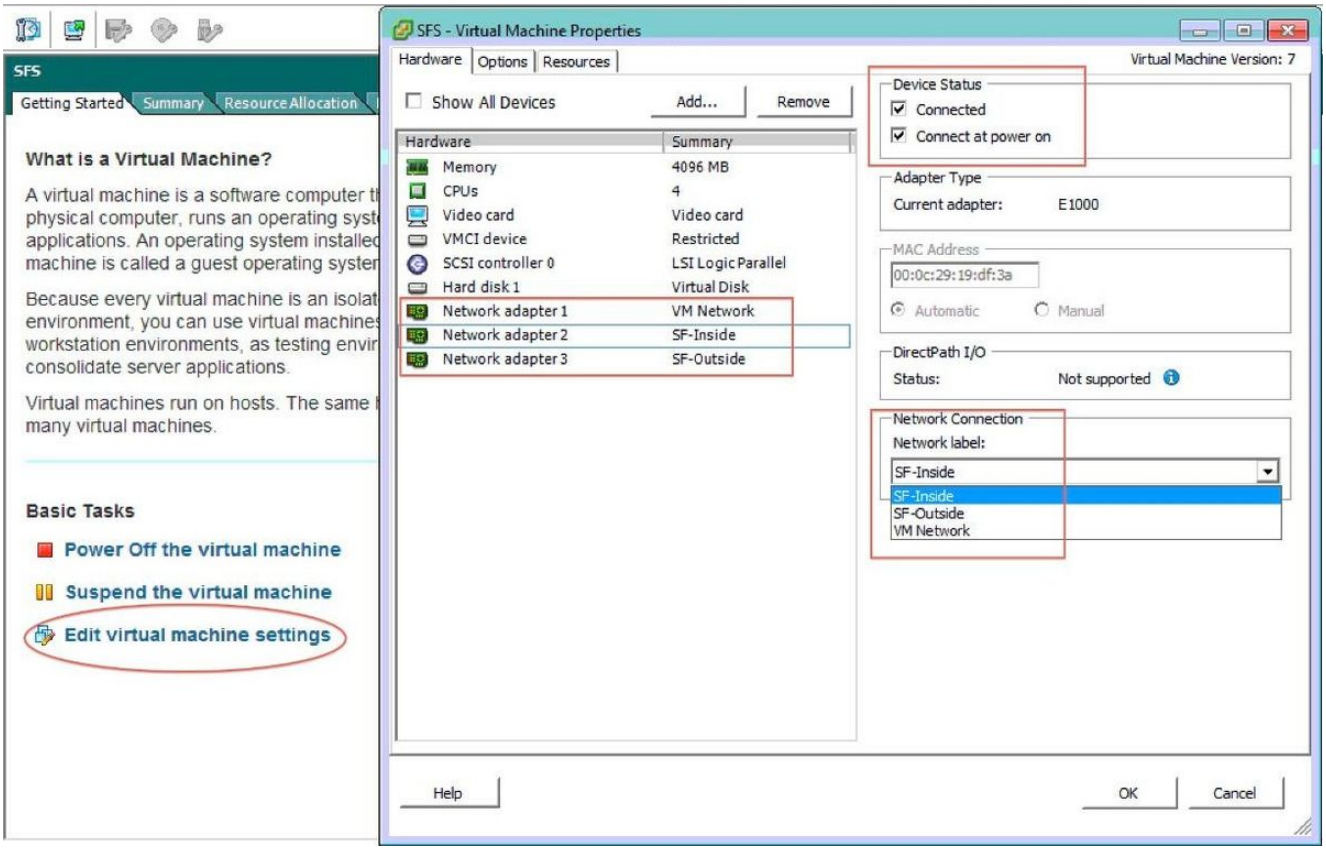
Nell'immagine sono illustrate le proprietà dello switch v1 (è necessario completare la stessa procedura per lo switch v2):

> **Nota:** Verificare che l'ID VLAN sia configurato su 4095 per NGIPSv, come richiesto dal documento NGIPSv: http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



La configurazione di vSwitch su ESXi è completa. A questo punto è necessario verificare le impostazioni dell'interfaccia:

1. Passare alla macchina virtuale per il dispositivo FirePOWER.
2. Fare clic su **Modifica impostazioni macchina virtuale**.
3. Verificare tutte e tre le schede di rete.
4. Verificare che siano stati scelti correttamente, come mostrato nell'immagine seguente:



Registrazione del dispositivo FirePOWER con FireSIGHT Management Center

Completare le procedure descritte nel documento Cisco per registrare un dispositivo FirePOWER con un centro di gestione FireSIGHT.

Reindirizzamento e verifica del traffico

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Questa sezione descrive come reindirizzare il traffico e come verificare i pacchetti.

Reindirizza il traffico dall'ISR al sensore su UCS-E

Utilizzare queste informazioni per reindirizzare il traffico:

```
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
```

> **Nota:** Se al momento si esegue la versione 3.16.1 o successiva, eseguire il comando **utd engine advanced** anziché il comando **utd**.

Verifica reindirizzamento pacchetti

Dalla console ISR, eseguire questo comando per verificare se i contatori del pacchetto incrementano:

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, è possibile eseguire i seguenti comandi **show**:

- **mostra globale utd software plat**
- **show platform software utd interfaces**
- **show platform software rp active global**
- **show plat software utd fp active global**
- **mostra stato utd funzionalità qfp attiva hardware plat**
- **mostra funzionalità attiva qfp hardware piattaforma utd**

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Èpossibile eseguire questi comandi di **debug** per risolvere i problemi relativi alla configurazione:

- **debug platform condition feature utd controlplane**
- **modalità secondaria della funzione di condizione della piattaforma di debug utd**

Informazioni correlate

- Guida introduttiva per Cisco UCS serie E Server e Cisco UCS serie E Network Compute Engine, versione 2.x
- Guida alla risoluzione dei problemi per Cisco UCS serie E Server e Cisco UCS serie E Network Compute Engine
- Guida introduttiva per Cisco UCS serie E Server e Cisco UCS serie E Network Compute Engine, versione 2.x - Aggiornamento firmware
- Cisco ASR serie 1000 Aggregation Services Router - Guida alla configurazione del software - Configurazione delle interfacce di dominio bridge
- Guida per l'utente di Host Upgrade Utility per Cisco UCS serie E Server e Cisco UCS serie E Network Compute Engine - Aggiornamento del firmware sui server Cisco UCS serie E
- Documentazione e supporto tecnico – Cisco Systems