UCS-E 블레이드를 사용하여 ISR 디바이스에서 FirePOWER Services 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[지원되는 하드웨어 플랫폼](#)
[UCS-E 블레이드가 포함된 ISR G2 디바이스](#)
[UCS-E 블레이드가 포함된 ISR 4000 장치](#)
[라이센스](#)
[제한 사항](#)
[구성](#)
[네트워크 다이어그램](#)
[UCS-E의 FirePOWER Services 워크플로](#)
[CIMC 구성](#)
[CIMC에 연결](#)
[CIMC 구성](#)
[ESXi 설치](#)
[vSphere 클라이언트 설치](#)
[vSphere 클라이언트 다운로드](#)
[vSphere 클라이언트 시작](#)
[FireSIGHT Management Center 및 FirePOWER 디바이스 구축](#)
[인터페이스](#)
[ESXi의 vSwitch 인터페이스](#)
[FireSIGHT Management Center에 FirePOWER 디바이스 등록](#)
[트래픽 리디렉션 및 확인](#)
[ISR에서 UCS-E의 센서로 트래픽 리디렉션](#)
[패킷 리디렉션 확인](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 IDS(Intrusion Detection System) 모드에서 Cisco UCS-E(Unified Computing System E Series) 블레이드 플랫폼에 Cisco FirePOWER 소프트웨어를 설치하고 구축하는 방법에 대해 설명합니다.이 문서에 설명된 구성 예제는 공식 사용 설명서를 보완하는 것입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISR(Integrated Services Router) XE 이미지 3.14 이상
- Cisco CIMC(Integrated Management Controller) 버전 2.3 이상
- Cisco FMC(FireSIGHT Management Center) 버전 5.2 이상
- Cisco FirePOWER NGIPSv(Virtual Device) 버전 5.2 이상
- VMware ESXi 버전 5.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

> **참고:**코드를 버전 3.14 이상으로 업그레이드하기 전에 시스템의 메모리, 디스크 공간 및 업그레이드 라이센스가 충분한지 확인하십시오.예 1을 참조하십시오.이미지를 플래시에 복사합니다.코드 업그레이드에 대한 자세한 내용을 보려면 Access Routers Software Upgrade Procedures Cisco 문서의 TFTP 서버 섹션에서 확인하십시오.

> **참고:**CIMC, BIOS 및 기타 펌웨어 구성 요소를 업그레이드하려면 Cisco HUU(Host Upgrade Utility)를 사용하거나 펌웨어 구성 요소를 수동으로 업그레이드할 수 있습니다.펌웨어 업그레이드에 대한 자세한 내용은 Cisco UCS E-Series Servers 및 Cisco UCS E-Series Network Compute Engine용 Host Upgrade Utility 사용 설명서의 Upgrading the Firmware on Cisco UCS E-Series Servers 섹션을 참조하십시오.

배경 정보

이 섹션에서는 이 문서에 설명된 구성 요소 및 절차에 대해 지원되는 하드웨어 플랫폼, 라이센스 및 제한 사항에 대해 설명합니다.

지원되는 하드웨어 플랫폼

이 섹션에서는 G2 및 4000 Series 디바이스에 대해 지원되는 하드웨어 플랫폼을 소개합니다.

UCS-E 블레이드가 포함된 ISR G2 디바이스

UCS-E Series 블레이드를 사용하는 ISR G2 Series 디바이스는 다음과 같이 지원됩니다.

제품	플랫폼	UCS-E 모델
Cisco 2900 Series ISR	2911	UCS-E 120/140 싱글 와이드 옵션
	2921	UCS-E 120/140/160/180 싱글 또는 더블 와이드 옵션
	2951	UCS-E 120/140/160 싱글 또는 더블 와이드 옵션
Cisco 3900 Series ISR	3925	UCS-E 120/140/160 싱글 및 더블 와이드 옵션 또는 180 더블 와이드
	3925E	UCS-E 120/140/160 싱글 및 더블 와이드 옵션 또는 180 더블 와이드
	3945	UCS-E 120/140/160 싱글 및 더블 와이드 옵션 또는 180 더블 와이드

		3945E UCS-E 120/140/160 싱글 및 더블 와이드 옵션 또는 180 더블 와이드

UCS-E 블레이드가 포함된 ISR 4000 장치

UCS-E Series 블레이드를 사용하는 ISR 4000 Series 디바이스는 다음과 같이 지원됩니다.

제품	플랫폼	UCS-E 모델
Cisco 4400 Series ISR	4451	UCS-E 120/140/160 싱글 및 더블 와이드 옵션 또는 180 더블 와이드
	4431	UCS-E Network Interface Module
	4351	UCS-E 120/140/160/180 싱글 및 더블 와이드 옵션 또는 180 더블 와이드
Cisco 4300 Series ISR	4331	UCS-E 120/140 싱글 와이드 옵션
	4321	UCS-E Network Interface Module

라이센스

서비스를 사용하려면 ISR에 보안 K9 라이선스와 appx 라이선스가 있어야 합니다.

제한 사항

이 문서에 설명된 정보와 관련된 두 가지 제한 사항은 다음과 같습니다.

- 멀티캐스트가 지원되지 않습니다.
- 각 시스템에 대해 4,096개의 BDI(Bridge Domain Interfaces)만 지원됩니다.

BDI는 다음 기능을 지원하지 않습니다.

- BFD(Bidirectional Forwarding Detection) 프로토콜
- Netflow
- QoS(Quality of Service)
- NBAR(Network-Based Application Recognition) 또는 AVC(Advanced Video Coding)
- ZBF(Zone Based Firewall)
- 암호화 VPN
- MPLS(Multiprotocol Label Switching)
- PPP(Point-to-Point Protocol) over Ethernet(PPPoE)

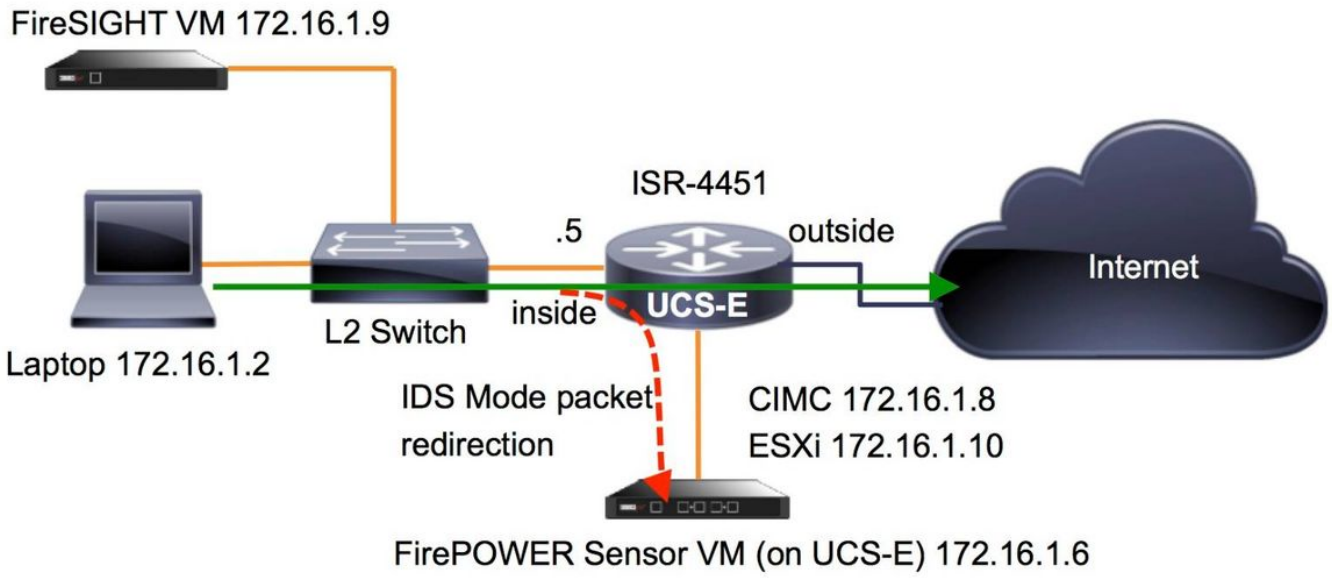
참고:BDI의 경우 MTU(Maximum Transmission Unit) 크기는 1,500~9,216바이트 사이의 임의의 값으로 구성할 수 있습니다.

구성

이 섹션에서는 이 구축과 관련된 구성 요소를 구성하는 방법에 대해 설명합니다.

네트워크 다이어그램

이 문서에 설명된 컨피그레이션에서는 다음 네트워크 토폴로지를 사용합니다.



UCS-E의 FirePOWER Services 워크플로

다음은 UCS-E에서 실행되는 FirePOWER 서비스의 워크플로입니다.

1. 데이터 플레인은 BDI/UCS-E 인터페이스에서 검사할 트래픽을 푸시합니다(G2 및 G3 Series 디바이스에서 작동).
2. Cisco IOS®-XE CLI는 분석을 위해 패킷 리디렉션을 활성화합니다(모든 인터페이스 또는 인터페이스당 옵션).
3. 센서 CLI **설정** 시작 스크립트는 컨피그레이션을 간소화합니다.

CIMC 구성

이 섹션에서는 CIMC를 구성하는 방법에 대해 설명합니다.

CIMC에 연결

CIMC에 연결하는 방법은 여러 가지가 있습니다.이 예에서는 전용 관리 포트를 통해 CIMC에 대한 연결이 완료됩니다.이더넷 케이블을 사용하여 **M** 포트(전용)를 네트워크에 연결해야 합니다.연결되면 라우터 프롬프트**에서 hw-module subslot** 명령을 실행합니다.

```
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
```

팁 1:종료하려면 **^a^q를 실행합니다**.

팁 2:기본 사용자 이름은 **admin** 및 password <password>입니다.비밀번호 재설정 프로세스는 다음과 같습니다. 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 구성

CIMC의 컨피그레이션을 완료하려면 다음 정보를 사용하십시오.

```
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
```

주의:변경 사항을 저장하려면 **commit** 명령을 실행해야 합니다.

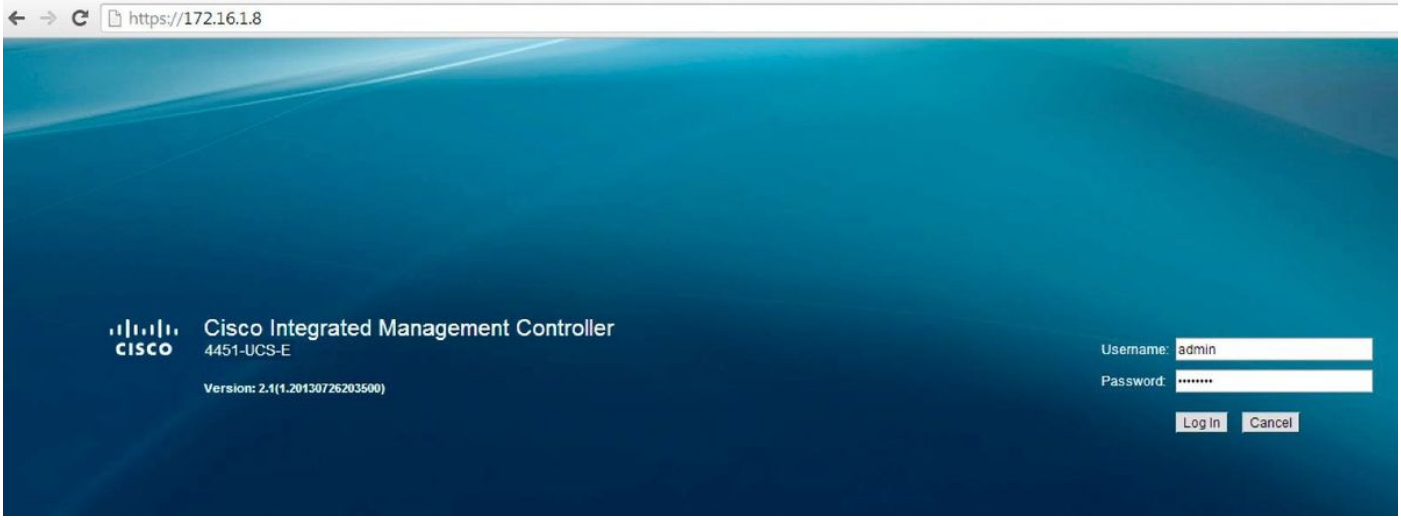
참고:관리 포트를 사용할 때 모드가 **전용**으로 설정됩니다.

show detail 명령을 실행하여 세부 설정을 확인합니다.

```
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 #
```

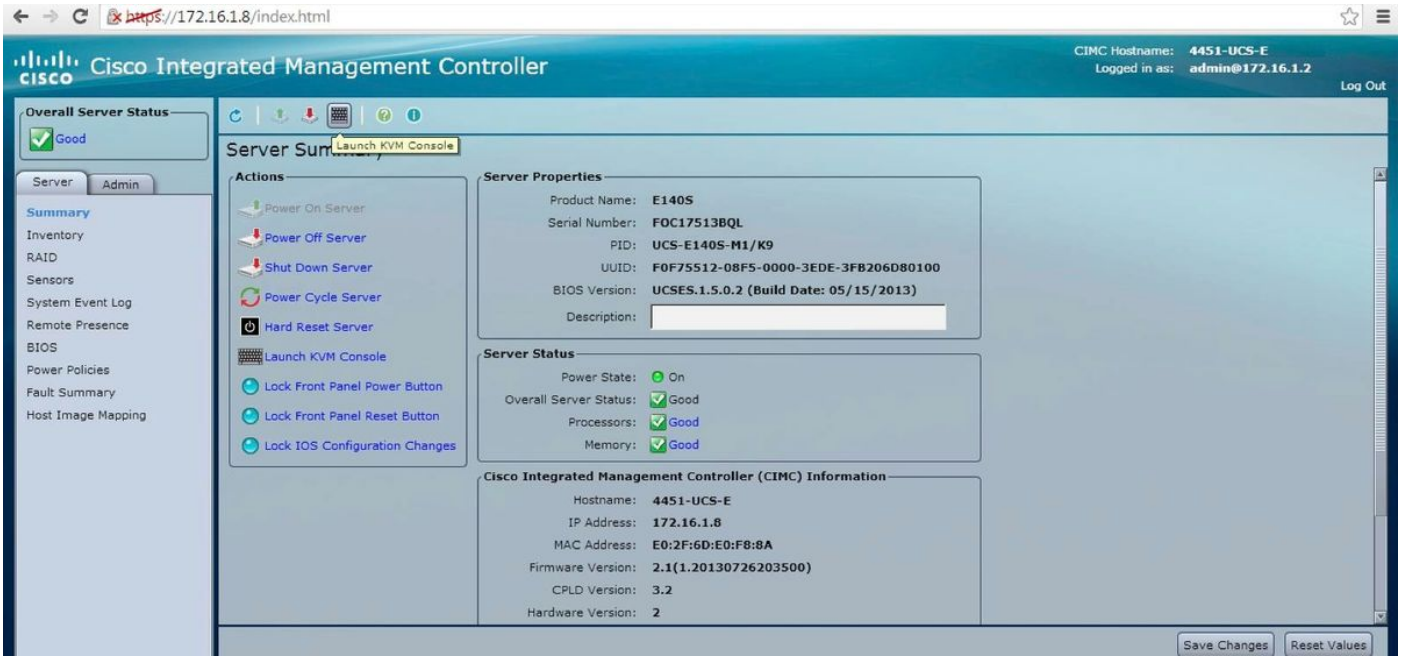
이미지에 표시된 대로 기본 사용자 이름과 비밀번호를 사용하여 브라우저에서 CIMC의 웹 인터페이스를 시작합니다.기본 사용자 이름 및 비밀번호는 다음과 같습니다.

- 사용자 이름:**관리자**
- 암호:**<비밀번호>**

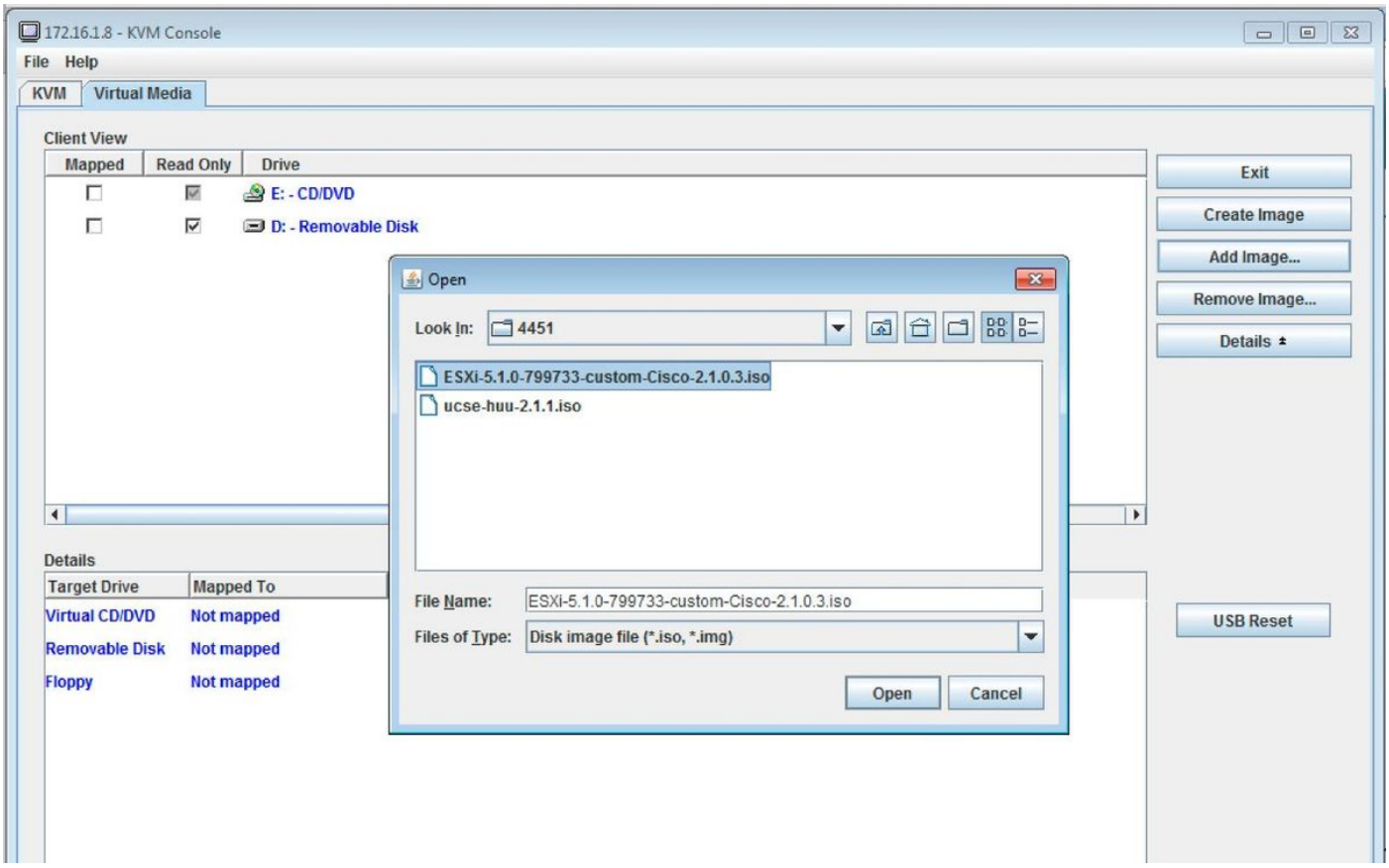


ESXi 설치

CIMC의 사용자 인터페이스에 로그인하면 이 이미지에 표시된 것과 비슷한 페이지를 볼 수 있습니다.Launch **KVM Console(KVM 콘솔 시작**) 아이콘을 클릭하고 **이미지 추가**를 클릭한 다음 ESXi ISO를 가상 미디어로 매핑합니다.



Virtual **Media** 탭을 클릭한 다음 **Add Image(이미지 추가)를** 클릭하여 이미지에 표시된 대로 가상 미디어를 매핑합니다.



가상 미디어가 매핑된 후 CIMC 홈 페이지에서 **Power Cycle Server**를 클릭하여 UCS-E의 전원을 껐다 켜십시오.ESXi 설정이 가상 미디어에서 시작됩니다.ESXi 설치를 완료합니다.

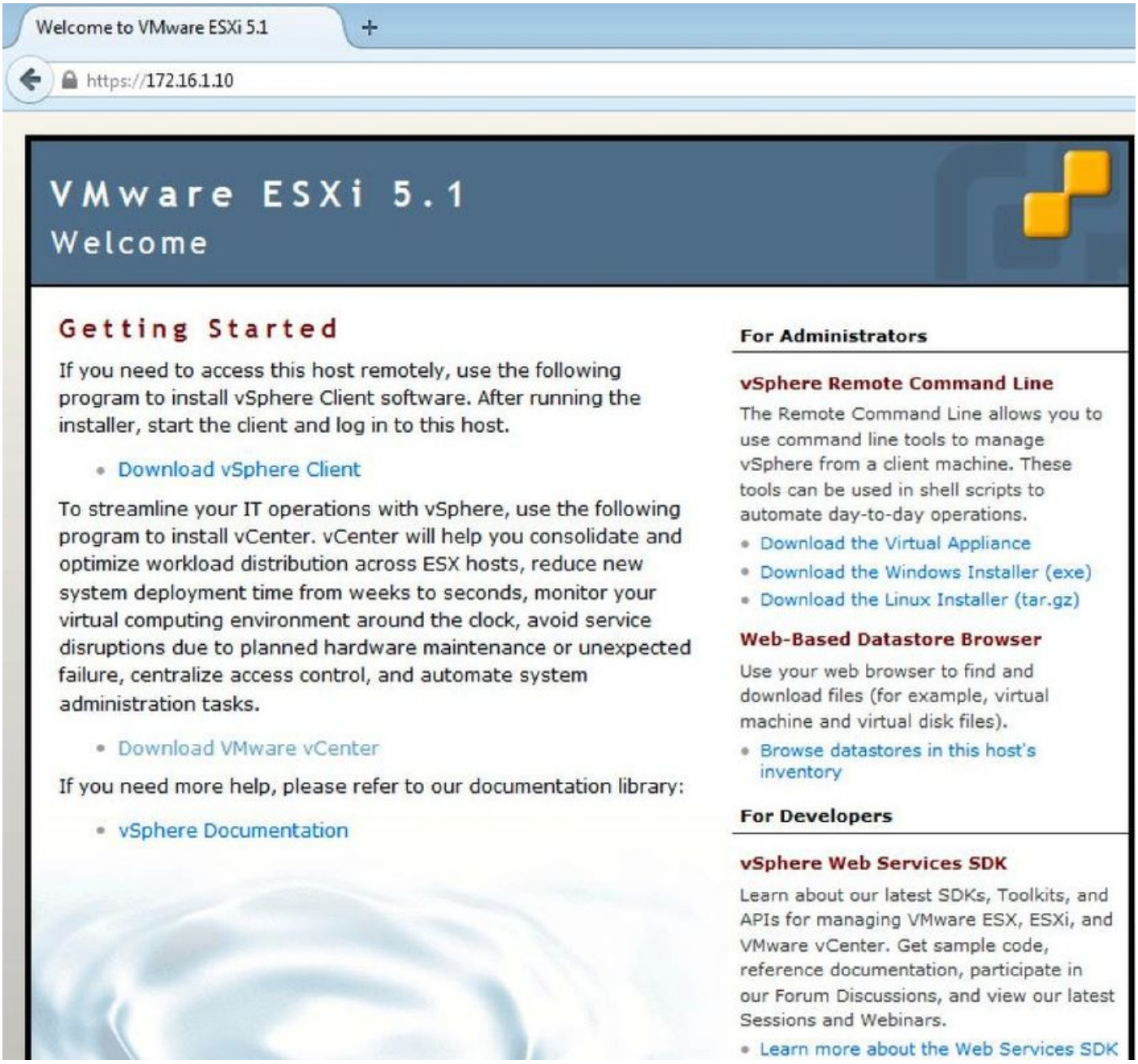
참고:나중에 참조할 수 있도록 ESXi IP 주소, 사용자 이름 및 비밀번호를 기록합니다.

vSphere 클라이언트 설치

이 섹션에서는 vSphere 클라이언트를 설치하는 방법에 대해 설명합니다.

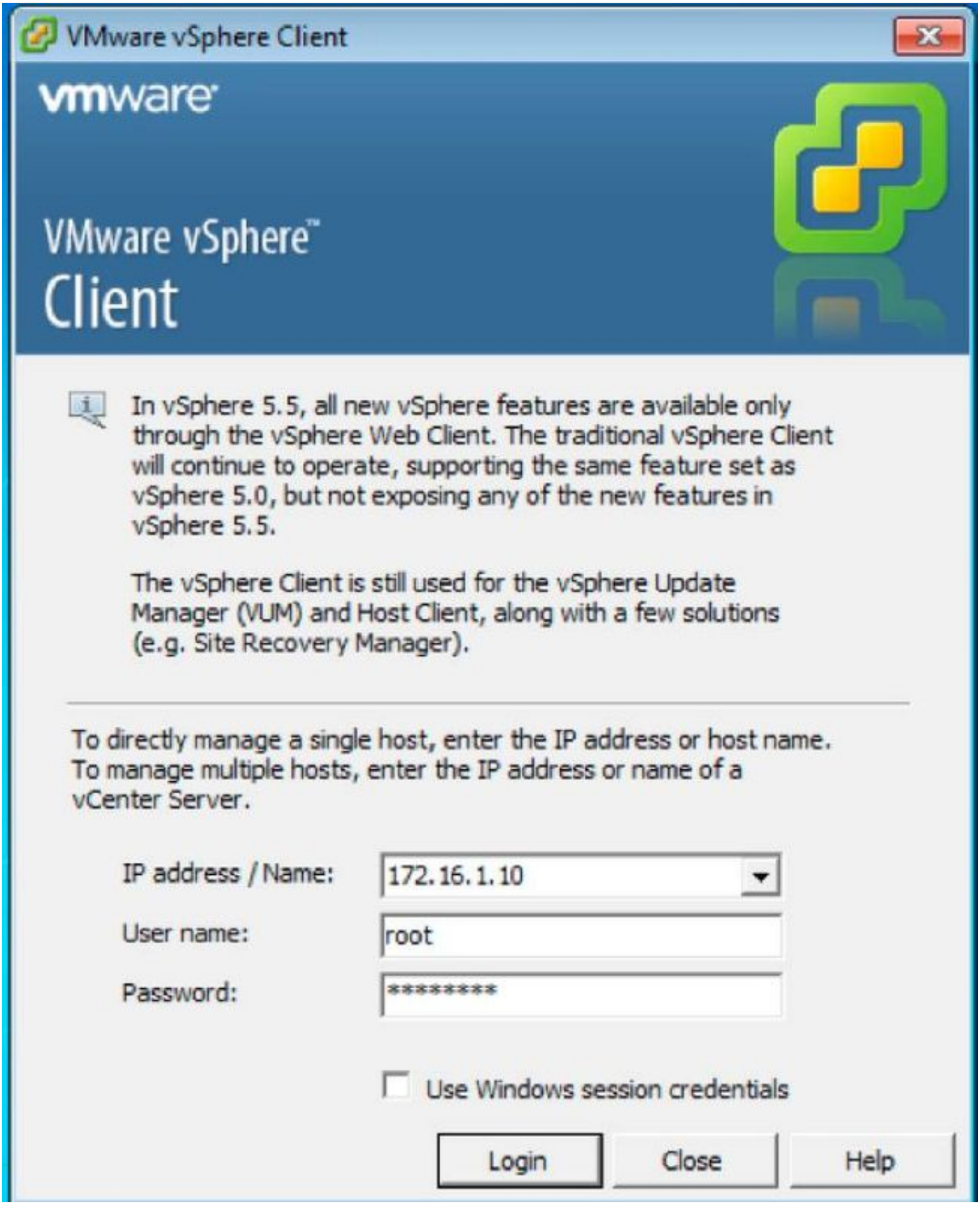
vSphere 클라이언트 다운로드

vSphere 클라이언트를 다운로드하려면 ESXi를 시작하고 **Download VSphere Client**(vSphere 클라이언트 다운로드) 링크를 사용합니다.컴퓨터에 설치합니다.



vSphere 클라이언트 시작

컴퓨터에서 vSphere 클라이언트를 시작합니다.설치 중에 생성한 사용자 이름 및 비밀번호와 이미지에 표시된 대로 로그인합니다.



FireSIGHT Management Center 및 FirePOWER 디바이스 구축

ESXi에 FireSIGHT Management Center를 구축하려면 VMware ESXi Cisco에 FireSIGHT Management Center 구축 문서에 설명된 절차를 완료합니다.

참고: FirePOWER NGIPSv 디바이스를 구축하는 데 사용되는 프로세스는 Management

Center 구축에 사용되는 프로세스와 유사합니다.

인터페이스

듀얼 와이드 UCS-E에는 다음 4개의 인터페이스가 있습니다.

- 가장 높은 MAC 주소 인터페이스는 전면 패널의 Gi3입니다.
- 두 번째로 높은 MAC 주소 인터페이스는 전면 패널의 Gi2입니다.
- 마지막으로 나타나는 두 인터페이스는 내부 인터페이스입니다.

Single-Wide UCS-E에는 세 가지 인터페이스가 있습니다.

- 가장 높은 MAC 주소 인터페이스는 전면 패널의 Gi2입니다.
- 마지막으로 나타나는 두 인터페이스는 내부 인터페이스입니다.

ISR4K의 UCS-E 인터페이스는 모두 트렁크 포트입니다.

UCS-E 120S 및 140S에는 3개의 네트워크 어댑터와 관리 포트가 있습니다.

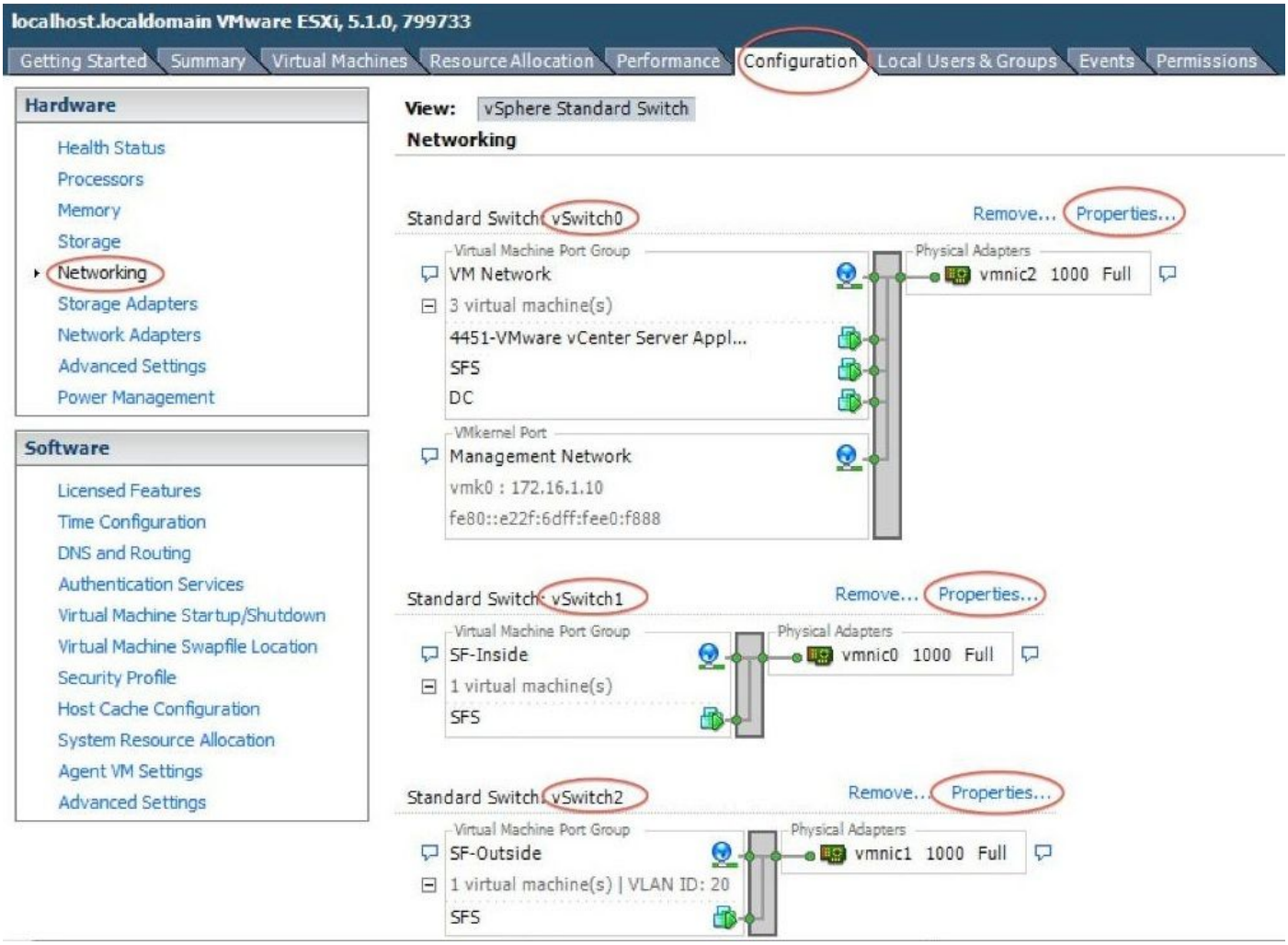
- vmnic *0*은 라우터 백플레인의 *UCSEx/0/0*에 매핑됩니다.
- vmnic*1은* 라우터 백플레인의 *UCSEx/0/1*에 매핑됩니다.
- vmnic*2는* UCS-E 전면 평면 GE2 인터페이스에 매핑됩니다.
- 전면 패널 관리(M) 포트는 CIMC에만 사용할 수 있습니다.

UCS-E 140D, 160D 및 180D에는 4개의 네트워크 어댑터가 있습니다.

- vmnic *0*은 라우터 백플레인의 *UCSEx/0/0*에 매핑됩니다.
- vmnic*1은* 라우터 백플레인의 *UCSEx/0/1*에 매핑됩니다.
- vmnic*2는* UCS-E 전면 평면 GE2 인터페이스에 매핑됩니다.
- vminc*3*은 UCS-E 전면 평면 GE3 인터페이스에 매핑됩니다.
- 전면 패널 관리(M) 포트는 CIMC에만 사용할 수 있습니다.

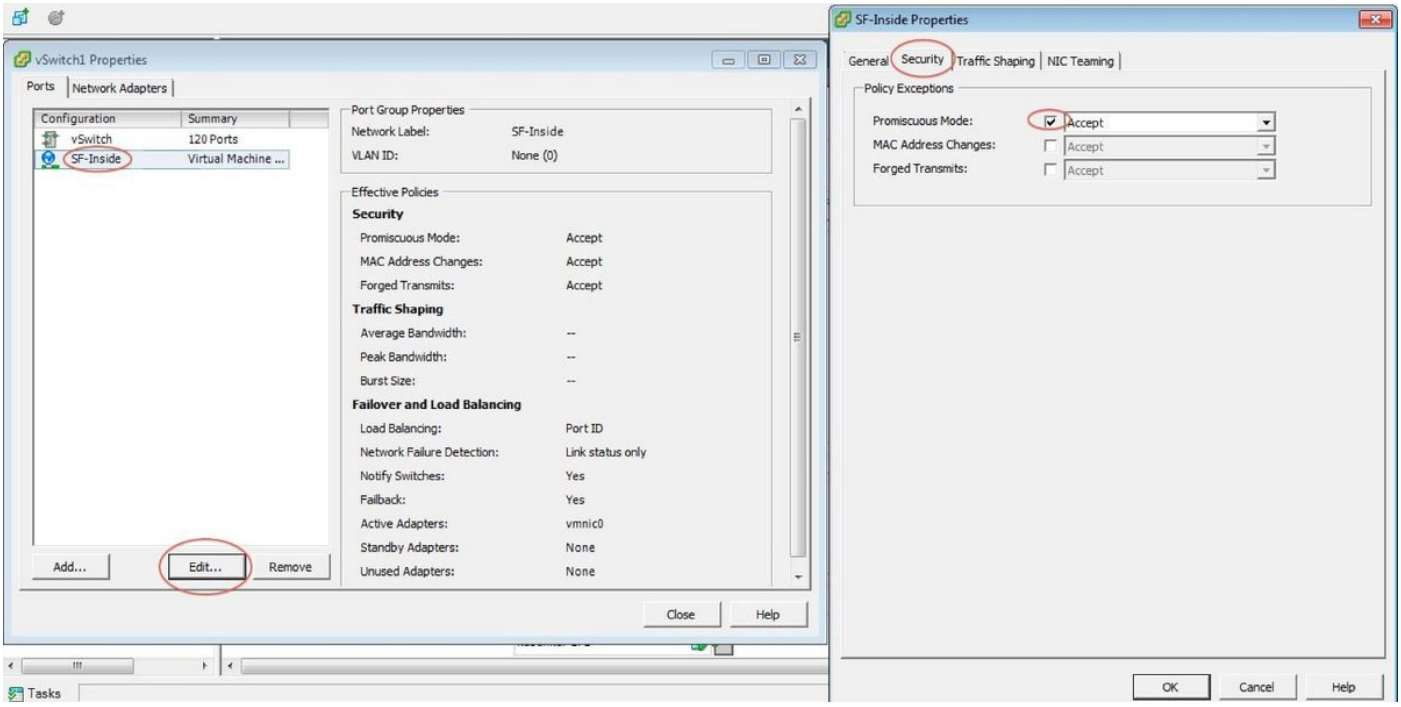
ESXi의 vSwitch 인터페이스

ESXi의 vSwitch0은 ESXi, FireSIGHT Management Center 및 FirePOWER NGIPSv 디바이스가 네트워크와 통신하는 관리 인터페이스입니다.변경하려면 vSwitch1(SF-Inside) 및 vSwitch2(SF-Outside)의 속성을 클릭합니다.



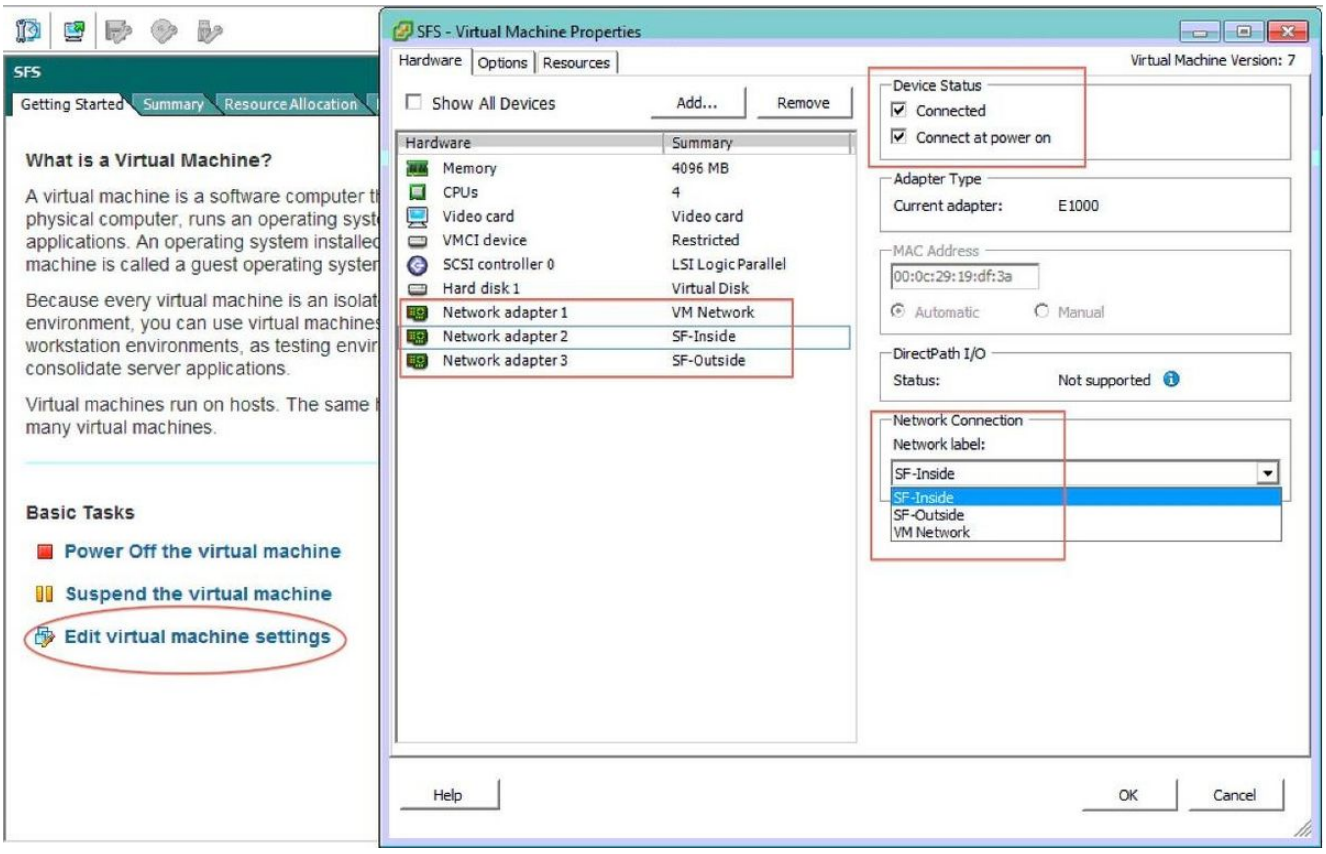
이 그림에서는 vSwitch1의 속성을 보여 줍니다(vSwitch2에 대해 동일한 단계를 완료해야 함).

참고:NGIPSv에 대해 VLAN ID가 4095로 구성되었는지 확인합니다. NGIPSv 문서에 따라 필요합니다 .http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/install-ngipsv.html



ESXi의 vSwitch 컨피그레이션이 완료되었습니다.이제 인터페이스 설정을 확인해야 합니다.

1. FirePOWER 디바이스의 가상 머신으로 이동합니다.
2. **가상 머신 설정 편집을 클릭합니다**.
3. 3개의 네트워크 어댑터를 모두 확인합니다.
4. 다음 이미지에 표시된 대로 올바르게 선택되었는지 확인합니다.



FireSIGHT Management Center에 FirePOWER 디바이스 등록

FirePOWER 디바이스를 FireSIGHT Management Center에 등록하려면 Cisco 문서에 설명된 절차

를 완료합니다.

트래픽 리디렉션 및 확인

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

이 섹션에서는 트래픽을 리디렉션하는 방법과 패킷을 확인하는 방법에 대해 설명합니다.

ISR에서 UCS-E의 센서로 트래픽 리디렉션

이 정보를 사용하여 트래픽을 리디렉션합니다.

```
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
```

> **참고:**현재 버전 3.16.1 이상을 실행하는 경우 utd 명령 대신 **utd engine advanced** 명령**을** 실행합니다.

패킷 리디렉션 확인

ISR 콘솔에서 이 명령을 실행하여 패킷 카운터가 증가하는지 확인합니다.

```
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
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하기 위해 다음 **show** 명령을 실행할 수 있습니다.

- **show plat software utglobal**
- **show plat software utinterface**
- **show plat software utd rp active global**
- **show plat software utd fp active global**
- **show plat hardware qfp active feature uts stats**
- **show platform hardware qfp active feature utt**

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

컨피그레이션을 트러블슈팅하기 위해 다음 **debug** 명령을 실행할 수 있습니다.

- **디버그 플랫폼 조건 기능 utd 제어 평면**
- **디버그 플랫폼 조건 기능 utd dataplane 하위 모드**

관련 정보

- Cisco UCS E-Series Server 및 Cisco UCS E-Series Network Compute Engine, 릴리스 2.x 시작하기 가이드
- Cisco UCS E-Series 서버 및 Cisco UCS E-Series Network Compute Engine 문제 해결 가이드
- Cisco UCS E-Series 서버 및 Cisco UCS E-Series Network Compute Engine, 릴리스 2.x - 펌웨어 업그레이드 시작 가이드
- Cisco ASR 1000 Series Aggregation Services Routers 소프트웨어 구성 설명서 - 브리지 도메인 인터페이스 구성
- Cisco UCS E-Series 서버 및 Cisco UCS E-Series Network Compute Engine용 호스트 업그레이드 유틸리티 사용 설명서 - Cisco UCS E-Series 서버의 펌웨어 업그레이드
- 기술 지원 및 문서 – Cisco Systems