VMware 구축을 위한 Cisco Firepower Threat Defense Virtual

수정: 2016년 6월 1일

VMware를 사용하여 Cisco Firepower Threat Defense Virtual을 구축할 수 있습니다.

Firepower Threat Defense Virtual 및 VMware 사전 요구 사항

Firepower Threat Defense Virtual을 VMware vSphere Web Client 또는 vSphere 독립형 클라이언트를 사용하여 ESXi에 구축할 수 있습니다. 시스템 요건은 Cisco Firepower Threat Defense 호환성을 참고하십시오.

가상 어플라이언스는 기본적으로 e1000(1Gbit/s) 인터페이스를 사용합니다. 기본 인터페이스를 vmxnet3 또는 ixgbe(10Gbit/s) 인터페이스로 교체할 수 있습니다.

vSphere 표준 스위치에 대한 보안 정책 설정 수정

vSphere 표준 스위치의 레이어 2 보안 정책의 3가지 요소는 무차별 모드, MAC 주소 변경 및 위조된 전송입니다. Firepower Threat Defense Virtual은 무차별 모드를 사용하여 작동하며 올바르게 작동하기 위해 액티브 및 스탠바이 간의 MAC 주소가 어떻게 전환되느냐에 따라 Firepower Threat Defense Virtual의 고가용성(HA)이 결정됩니다.

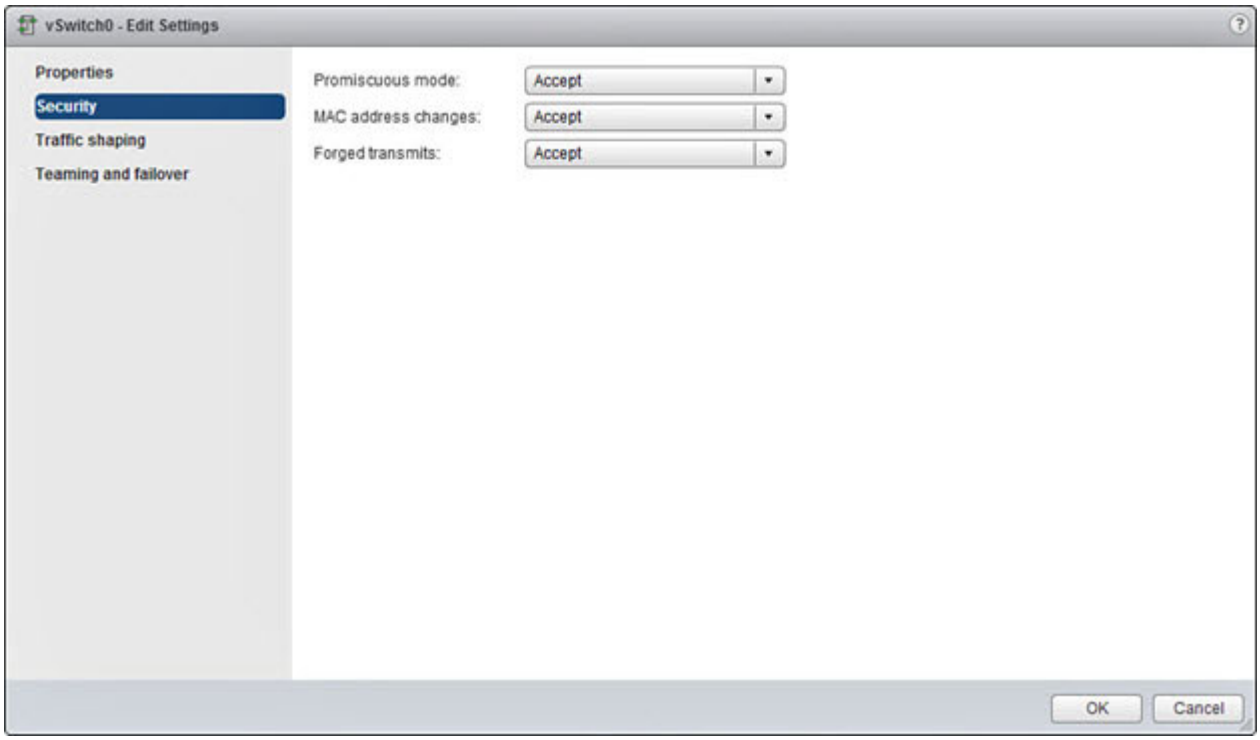
기본 설정은 Firepower Threat Defense Virtual의 올바른 작동을 차단합니다. 다음의 필수 설정을 확인합니다.

표 1 vSphere 표준 스위치 보안 정책 옵션

옵션	필수 설정	작업
무차별 모드	수락	vSphere 표준 스위치에 대한 보안 정책을 vSphere Web Client에서 편집하고 **무차별 모드** 옵션을 **수락**으로 설정**해야 합니다**. 방화벽, 포트 스캐너, 침입 탐지 시스템 등을 무차별 모드에서 실행해야 합니다.
MAC 주소 변경	수락	vSphere 표준 스위치에 대한 보안 정책을 vSphere Web Client에서 확인하고 **MAC 주소 변경** 옵션이 **수락**으로 설정되었는지 확인해야 합니다.
위조된 전송	수락	vSphere 표준 스위치에 대한 보안 정책을 vSphere Web Client에서 확인하고 **위조된 전송** 옵션이 **수락**으로 설정되었는지 확인해야 합니다.

절차

1. vSphere Web Client에서 호스트로 이동합니다.
2. **Manage(관리)** 탭에서 **Networking(네트워킹)**을 클릭하고 **Virtual switches(가상 스위치)**를 선택합니다.
3. 목록에서 표준 스위치를 선택하고 **Edit settings(설정 수정)**를 클릭합니다.
4. **Security(보안)**를 선택하고 현재 설정을 확인합니다.
5. 표준 스위치에 연결된 가상 머신의 게스트 운영 체제에서 무차별 모드 활성화, MAC 주소 변경 및 위조된 전송을 **Accept(수락)**합니다.



6. **OK(확인)**를 클릭합니다.

다음 작업

다음 설정이 Firepower Threat Defense Virtual 센서의 관리 및 장애 조치(HA) 인터페이스에 구성된 모든 네트워크에서 동일한지 확인합니다.

Firepower Threat Defense Virtual 및 VMware에 대한 지침

- Firepower Threat Defense Virtual은 **최소 4개의 인터페이스로 첫 부팅 시 전원이 공급되어야 합니다.**
- e1000 드라이버의 관리 인터페이스(br1)는 2개의 MAC 주소가 있는 브리지된 인터페이스입니다. 하나는 관리용이고 나머지 하나는 진단용입니다.
- vmxnet3 드라이버는 2개의 관리 인터페이스를 사용합니다. 첫 번째 2개의 이더넷 어댑터는 관리 인터페이스로 구성되어야 합니다. 즉, 하나는 장치 관리 및 등록용(eth0)이고 나머지 하나는 진단용(eth1)입니다.
- ixgbe 드라이버는 2개의 관리 인터페이스를 사용합니다. 첫 번째 2개의 PCI 장치는 관리 인터페이스로 구성되어야 합니다. 즉, 하나는 장치 관리 및 등록용(eth0)이고 나머지 하나는 진단용(eth1)입니다.
- 버전 6.0에서 지원되는 유일한 ixgbe 트래픽 인터페이스 유형은 ERSPAN 패시브이며 라우팅됩니다. 이것은 MAC 주소 필터링과 관련된 VMware 제한 때문입니다.

  참고: ixgbe 드라이버는 이 릴리스에서 Firepower Threat Defense Virtual의 장애 조치(HA) 구축을 지원하지 않습니다.

- Cisco는 4개 이상의 vmxnet3 네트워크 카드를 사용할 때 VMware vCenter에서 관리하는 호스트를 사용할 것을 권장합니다. 독립형 ESXi에서 구축할 경우 추가 네트워크 카드는 순차적 PCI 버스 주소가 있는 가상 머신에 추가되지 않습니다. VMWare 인터페이스 추가 및 구성, 7페이지를 참조하십시오.
- vMotion은 지원되지 않습니다.
- 가상 머신 복제는 지원되지 않습니다.
- 스냅샷을 사용한 가상 머신 복원은 지원되지 않습니다.
- 백업 복원은 지원되지 않습니다.

OVF 파일 지침

Firepower Threat Defense Virtual 어플라이언스 설치에 대해 다음 설치 옵션이 있습니다.

```
Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

여기서 *X.X.X-xxx*는 사용하려는 파일의 버전 및 빌드 번호입니다.

- VI OVF 템플릿을 사용하여 구축할 경우, 설치 프로세스에서 Firepower Threat Defense Virtual 어플라이언스의 전체 초기 설정을 수행할 수 있습니다. 다음을 지정할 수 있습니다.
  - 관리자 어카운트의 새 비밀번호
  - 어플라이언스가 관리 네트워크에서 통신하도록 지원하는 네트워크 설정
  - 초기 방화벽 모드
  - Cisco Firepower Management Center 관리

  참고: VMware vCenter를 사용하여 이 가상 어플라이언스를 관리해야 합니다.
- ESXi OVF 템플릿을 사용하여 구축할 경우 설치 후 Firepower System의 필수 설정을 구성해야 합니다. 이 가상 어플라이언스를 VMware vCenter를 사용하여 관리하거나 독립형 어플라이언스로 사용할 수 있습니다. 자세한 내용은 CLI를 사용하여 Firepower Threat Defense Virtual 장치 설정, 8페이지를 참고하십시오.

OVF 템플릿을 구축할 때 다음 정보를 제공합니다.

표 2 VMWare OVF 템플릿

설정	ESXi 또는 VI	조치
OVF 템플릿 가져오기/구축	모두	이전 절차에서 사용하기 위해 다운로드한 OVF 템플릿을 찾습니다.
OVF 템플릿 세부 정보	모두	설치할 어플라이언스(Cisco Firepower Threat Defense Virtual) 및 구축 옵션(VI 또는 ESXi)을 확인합니다.
EULA 수락	VI만	OVF 템플릿에 포함된 라이센스 약관을 수락하려면 동의합니다.
이름 및 위치	모두	가상 어플라이언스에 고유하고 의미 있는 이름을 입력하고 어플라이언스의 인벤토리 위치를 선택합니다.
호스트 / 클러스터	모두	가상 어플라이언스를 구축할 호스트 또는 클러스터를 선택합니다.
리소스 풀	모두	컴퓨팅 리소스를 의미 있는 계층 구조로 설정하는 방식으로 호스트 또는 클러스터 내에서 컴퓨팅 리소스를 관리합니다. 가상 머신 및 하위 리소스 풀은 상위 리소스 풀의 리소스를 공유합니다.
스토리지	모두	가상 머신과 관련된 모든 파일을 저장합니다.

표 2 VMWare OVF 템플릿 (계속)

설정	ESXi 또는 VI	조치
디스크 형식	모두	가상 디스크를 저장할 형식(thick provision lazy zeroed, thick provision eager zeroed 또는 thin provision)을 선택합니다.
네트워크 매핑	모두	가상 어플라이언스의 관리 인터페이스를 선택합니다.
속성	VI만	가상 머신 초기 컨피그레이션 설정을 맞춤화합니다.

Firepower Threat Defense Virtual을 VMware vSphere Web Client 또는 vSphere 하이퍼바이저를 사용하여 구축

VMware vSphere Web Client를 사용하여 Firepower Threat Defense Virtual을 구축할 수 있습니다. Web Client에는 vCenter가 필요합니다. 또한 독립형 ESXi 구축에 vSphere 하이퍼바이저를 사용할 수 있습니다. vSphere를 사용하여 VI OVF 또는 ESXi OVF 템플릿으로 구축할 수 있습니다.

- VI OVF 템플릿을 사용하여 구축할 경우 VMware vCenter로 어플라이언스를 관리해야 합니다.
- ESXi OVF 템플릿을 사용하여 구축할 경우 VMware vCenter로 어플라이언스를 관리하거나 독립형 호스트에 구축할 수 있습니다. 어떤 경우든 설치 후 Firepower System의 필수 설정을 구성해야 합니다.

시작하기 전에

- Firepower Threat Defense Virtual의 아카이브 파일을 Cisco 지원 사이트(https://software.cisco.com/download/navigator.html)의 다운로드 영역에서 다운로드하십시오.

  참고: Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.
- 작업 디렉토리에 아카이브 파일의 압축을 풉니다. 이 디렉터리의 어떤 파일도 삭제하지 마십시오.

절차

1. vSphere Client를 사용하여 **File(파일) > Deploy OVF Template(OVF 템플릿 구축)**을 클릭하여 이전에 다운로드한 OVF 템플릿 파일을 구축합니다.
2. 드롭다운 목록에서 Firepower Threat Defense Virtual 장치에 구축할 OVF 템플릿 중 하나를 선택합니다.

   ```
   Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
   Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
   ```

   여기서 *X.X.X-xxx*는 다운로드하려는 아카이브 파일의 버전 및 빌드 번호입니다.
3. OVF 템플릿 세부 정보 페이지를 확인하고 **Next(다음)**를 클릭합니다.
4. 라이센스 계약서가 OVF 템플릿(VI 템플릿 전용)과 함께 패키지된 경우, 최종 사용자 라이센스 계약 페이지가 나타납니다. 라이센스 약관을 수락하려면 동의하고 **Next(다음)**를 클릭합니다.
5. 선택적으로, 이름을 편집하고 Firepower Threat Defense Virtual을 저장할 인벤토리 내부의 폴더 위치를 선택하고 **다음**을 클릭합니다.

   참고: vSphere Client가 ESXi 호스트에 직접 연결될 경우, 폴더 위치를 선택하는 옵션이 나타나지 않습니다.
6. Firepower Threat Defense Virtual을 구축할 호스트 또는 클러스터를 선택하고 **다음**을 클릭합니다.
7. Firepower Threat Defense Virtual을 실행할 리소스 풀로 이동하여 선택하고 **다음**을 클릭합니다.

   참고: 이 페이지는 클러스터에 리소스 풀이 포함되어 있는 경우에만 나타납니다.
8. 가상 머신 파일을 저장할 스토리지 위치를 선택하고 **다음**을 클릭합니다.

   이 페이지에서 이미 대상 클러스터 또는 호스트에 구성되어 있는 데이터 저장소에서 선택합니다. 가상 머신 컨피그레이션 파일 및 가상 디스크 파일은 해당 데이터 저장소에 저장되어 있습니다. 가상 머신과 모든 가상 디스크 파일을 수용할 만큼 큰 데이터 저장소를 선택합니다.

9. 가상 머신 가상 디스크를 저장할 디스크 형식을 선택하고 **다음**을 클릭합니다.

   Thick Provisioned(씩 프로비저닝)를 선택할 경우, 모든 스토리지가 즉시 할당됩니다. **Thin Provisioned(씬 프로비저닝)**를 선택할 경우, 데이터가 가상 디스크에 쓰여질 때 요청 시 스토리지가 할당됩니다. 또한 씬 프로비저닝은 가상 어플라이언스를 구축하는 데 걸리는 시간을 줄일 수 있습니다.

10. OVF 템플릿에 지정되어 있는 각 네트워크의 경우, 각 Firepower Threat Defense Virtual 인터페이스의 네트워크 매핑을 설정하려면 인프라에서 **Destination Networks(대상 네트워크)** 열을 마우스 오른쪽 버튼으로 클릭하여 네트워크를 선택하고 **다음**을 클릭합니다.

    참고: Firepower Threat Defense Virtual에서는 네트워크를 **최소 4개의 인터페이스**에 **할당해야 합니다**. 시스템은 4개의 인터페이스 없이는 구축하지 않습니다.

    Management0-0 인터페이스가 Firepower Management Center에서 연결할 수 있는 VM 네트워크에 연결되었는지 확인하십시오. 비관리 인터페이스는 Firepower Management Center에서 구성할 수 있습니다.

    네트워크는 사전 순이 아닐 수도 있습니다. 네트워크를 찾기 어려운 경우 나중에 설정 수정 대화 상자에서 네트워크를 변경할 수 있습니다. 구축 후 Firepower Threat Defense Virtual 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings(설정 수정)**를 선택하면 **Edit Settings(설정 수정)** 대화 상자에 액세스할 수 있습니다. 그러나 Firepower Threat Defense Virtual 인터페이스 ID는 이 화면에 표시되지 않습니다(네트워크 어댑터 ID만 표시됨). Firepower Threat Defense Virtual 인터페이스에 대해 다음의 소스 네트워크 및 대상 네트워크를 참고하십시오.

소스 네트워크	대상 네트워크	기능
Management0-0	Diagnostic0/0	진단 및 관리
GigabitEthernet0-0	GigabitEthernet0/0	트래픽
GigabitEthernet0-1	GigabitEthernet0/1	트래픽
GigabitEthernet0-2	GigabitEthernet0/2	트래픽

    Firepower Threat Defense Virtual을 구축한 후 선택적으로 설정 수정 대화 상자에서 인터페이스를 더 추가하려면 vSphere Client로 돌아갈 수 있습니다. Firepower Threat Defense Virtual을 구축할 때 총 10개의 인터페이스를 사용할 수 있습니다. 자세한 내용은 vSphere Client 온라인 도움말을 참고하십시오.

    참고: vSphere Client에서는 네트워크를 최소 4개의 인터페이스에 할당해야 합니다. 모든 Firepower Threat Defense Virtual 인터페이스를 사용할 필요는 없습니다. 사용하지 않으려는 인터페이스는 Firepower Threat Defense Virtual 컨피그레이션 내에서 비활성화된 상태 그대로 두면 됩니다.

11. 사용자가 구성 가능한 속성이 OVF 템플릿(VI 템플릿 전용)과 함께 패키지된 경우, 구성 가능한 속성을 설정하고 **다음**을 클릭합니다.

12. **Ready to Complete(완료 준비)** 창에서 설정을 검토하고 확인합니다. 선택적으로 Firepower Threat Defense Virtual의 전원을 켜려면 **Power on after deployment(구축 후 전원 켜기)** 옵션을 선택한 다음 **Finish(마침)**를 클릭합니다.

    마법사를 완료하면 vSphere Web Client에서 VM을 처리합니다. **Recent Tasks(최근 작업)** 창의 **Global Information(전체 정보)** 영역에서 "OVF 구축 초기화" 상태를 볼 수 있습니다.

    작업이 완료되면 Deploy OVF Template(OVF 템플릿 구축) 완료 상태가 표시됩니다.

    그런 다음 인벤토리의 지정된 데이터 센터 아래에 Firepower Threat Defense Virtual VM 인스턴스가 표시됩니다. 새 VM을 부팅하는 데 최대 30분이 소요될 수 있습니다.

    참고: Firepower Threat Defense Virtual를 Cisco Licensing Authority에 성공적으로 등록하려면 Firepower Threat Defense Virtual에 인터넷 액세스가 필요합니다. 구축 후 인터넷 액세스 및 성공적인 라이센스 등록을 위해 추가 컨피그레이션이 필요할 수 있습니다.

다음 작업

- 가상 어플라이언스의 하드웨어 및 메모리 설정을 수정하거나 인터페이스를 구성해야 하는지를 판단합니다. 자세한 내용은 설치 후 컨피그레이션, 6페이지를 참고하십시오.
- Firepower Threat Defense Virtual을 Firepower Management Center에 등록합니다. 자세한 내용은 Firepower Threat Defense Virtual을 Firepower Management Center에 등록, 9페이지를 참고하십시오.

설치 후 컨피그레이션

가상 어플라이언스를 구축한 다음 가상 어플라이언스의 하드웨어 및 메모리 설정이 구축 요건에 부합하는지 확인하십시오. 기본 설정은 시스템 소프트웨어를 실행하는 데 필요한 최소 설정이므로 기본 설정을 줄이지 **마십시오**. 다음 표에는 기본 어플라이언스 설정이 나와 있습니다.

표 3 기본 가상 어플라이언스 설정

설정	기본	설정의 조정 가능 여부
메모리	8GB	아니요
가상 CPU	4	아니요
하드 디스크 프로비저닝 크기	48.24GB	아니요, 디스크 형식 선택 사항을 따름(씬 프로비저닝의 경우 48.24GB)

가상 머신 속성 확인

VMWare 가상 머신 속성 대화 상자를 사용하여 선택한 가상 머신에 대한 호스트 리소스 할당을 조정합니다. 이 탭에서 CPU, 메모리, 디스크 및 고급 CPU 리소스를 변경할 수 있습니다. 또한 가상 머신에 대한 전원 켜기 연결 설정, MAC 주소, 가상 이더넷 어댑터 컨피그레이션의 네트워크 연결을 변경할 수 있습니다.

절차

1. 새 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 컨텍스트 메뉴에서 **Edit Settings(설정 수정)**를 선택하거나 기본 창의 **Getting Started(시작하기)** 탭에서 **Edit virtual machine settings(가상 머신 설정 수정)**를 클릭합니다.
2. **메모리**, **CPU**, **하드 디스크 1** 설정이 표 3 기본 가상 어플라이언스 설정, 6페이지에 설명된 대로 기본값으로 설정되어 있는지 확인합니다.

   어플라이언스의 메모리 설정 및 가상 CPU 수가 창 왼쪽에 나열됩니다. 하드 디스크의 **프로비저닝된 크기**를 보려면 **Hard disk 1(하드 디스크 1)**을 클릭합니다.
3. **네트워크 어댑터 1** 설정이 다음과 같은지 확인하고, 필요한 경우 변경합니다.
   a. **Device Status(장치 상태)** 아래에서 **Connect at power on(전원이 켜진 상태에서 연결)** 확인란을 활성화합니다.
   b. **MAC Address(MAC 주소)** 아래에서 가상 어플라이언스 관리 인터페이스의 MAC 주소를 수동으로 설정합니다.

      MAC 주소가 변경되거나 동적 풀의 다른 시스템과 충돌하지 않도록 MAC 주소를 가상 어플라이언스에 수동으로 할당합니다.

      또한, 가상 Cisco Firepower Management Center에서 MAC 주소를 수동으로 설정하면 어플라이언스를 이미지로 다시 설치해야 할 경우 Cisco에서 라이센스를 다시 요청하지 않아도 됩니다.
   c. **Network Connection(네트워크 연결)** 아래에서 **Network label(네트워크 레이블)**을 가상 어플라이언스의 관리 네트워크 이름으로 설정합니다.
4. **OK(확인)**를 클릭합니다.

다음 작업

- 가상 어플라이언스를 초기화합니다. 자세한 내용은 가상 어플라이언스 초기화, 8페이지를 참고하십시오.
- 선택적으로, 어플라이언스의 전원을 켜기 전에 기본 e1000 인터페이스를 vnxnet3 인터페이스로 교체하거나, 추가 관리 인터페이스를 생성하거나 두 방식을 모두 수행합니다. 자세한 내용은 VMWare 인터페이스 추가 및 구성, 7페이지를 참고하십시오.

VMWare 인터페이스 추가 및 구성

VMWare는 가상 머신을 생성할 때 e1000 (1Gbit/s) 인터페이스에 기본값을 설정합니다. 가상 머신 작업이 완료되고 Firepower Threat Defense Virtual이 완전히 설치되면 이후에 더 많은 네트워크 처리량을 위해 e1000에서 vmxnet3(10Gbit/s) 또는 ixgbe(10Gbit/s) 인터페이스 중 하나로 전환할 수 있습니다. 다음 지침은 기본 e1000 인터페이스를 대체할 때 중요합니다.

- vmxnet3의 경우, Cisco는 4개 이상의 vmxnet3 네트워크 인터페이스를 사용할 때 VMware vCenter에서 관리하는 호스트를 사용할 것을 권장합니다. 독립형 ESXi에서 구축할 경우 추가 네트워크 인터페이스는 순차적 PCI 버스 주소가 있는 가상 머신에 추가되지 않습니다. 호스트가 VMware vCenter로 관리되면 컨피그레이션 CD-ROM에 있는 XML에서 올바른 순서를 획득할 수 있습니다. 호스트가 독립형 ESXi를 실행 중인 경우, 네트워크 인터페이스의 순서를 결정하는 유일한 방법은 Firepower Threat Defense Virtual에서 보이는 MAC 주소를 VMware 컨피그레이션 툴에서 보이는 MAC 주소와 직접 비교하는 것입니다.
- vmxnet3 드라이버는 2개의 관리 인터페이스를 사용합니다. 첫 번째 2개의 이더넷 어댑터는 관리 인터페이스로 구성되어야 합니다. 즉, 하나는 장치 관리 및 등록용이고 나머지 하나는 진단용입니다.
- ixgbe의 경우, ESXi 플랫폼에서는 ixgbe NIC가 ixgbe PCI 장치를 지원해야 합니다. 또한, ESXi 플랫폼에는 특정한 BIOS와 ixgbe PCI 장치를 지원하는 데 필요한 컨피그레이션 요건이 있습니다. 자세한 내용은 Intel 기술 요약인 *Intel® 이더넷 통합 네트워크 어댑터를 사용하는 가상 기능을 VMware* ESXi* 5.1에 구성하는 방법*을 참고하십시오.
- ixgbe 드라이버는 2개의 관리 인터페이스를 사용합니다. 첫 번째 2개의 PCI 장치는 관리 인터페이스로 구성되어야 합니다. 즉, 하나는 장치 관리 및 등록용이고 나머지 하나는 진단용입니다.

  참고: ixgbe 드라이버는 이 릴리스에서 Firepower Threat Defense Virtual의 장애 조치(HA) 구축을 지원하지 않습니다.

모든 e1000 인터페이스를 삭제하고 이를 vmxnet3 또는 ixgbe 인터페이스로 교체하여 기본 e1000 인터페이스를 교체할 수 있습니다.

구축 과정에서 인터페이스를 혼합할 수 있는 경우에도(예: 가상 Cisco Firepower Management Center의 e1000 인터페이스 및 해당 관리되는 가상 장치의 vmxnet3 인터페이스) 동일한 어플라이언스에서 인터페이스를 혼합할 수 없습니다. 어플라이언스의 모든 센싱 및 관리 인터페이스는 동일한 유형이어야 합니다.

e1000 인터페이스를 교체하려면 vSphere Client를 사용하여 우선 기존의 e1000 인터페이스를 제거한 다음 새로운 인터페이스를 추가하고 적절한 어댑터 유형 및 네트워크 연결을 선택합니다.

또한 두 개의 서로 다른 네트워크에서 트래픽을 별도로 관리하려면 동일한 가상 Firepower Management Center에서 추가 관리 인터페이스를 추가할 수 있습니다. 추가 가상 스위치를 구성하여 두 번째 관리 인터페이스를 두 번째 네트워크의 관리되는 장치에 연결합니다. vSphere Client를 사용하여 두 번째 관리 인터페이스를 가상 어플라이언스에 추가합니다.

참고: 어플라이언스를 켜기 전에 인터페이스에 대한 모든 변경 사항을 적용합니다. 인터페이스를 변경하려면 어플라이언스 전원을 끈 다음 인터페이스를 삭제하고 새 인터페이스를 추가한 다음 어플라이언스 전원을 켜야 합니다.

vSphere Client 사용에 대한 자세한 내용은 VMWare 웹 사이트(http://vmware.com)를 참고하십시오. 다중 관리 인터페이스에 대한 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*의 장치 관리를 참고하십시오.

가상 어플라이언스 초기화

가상 어플라이언스를 설치한 다음 처음으로 가상 어플라이언스의 전원을 켜면 초기화가 자동으로 시작됩니다.

주의: 시작 시간은 서버 리소스 가용성을 포함한 여러 요소에 따라 달라집니다. 초기화가 완료될 때까지 최대 40분이 소요될 수 있습니다. 초기화를 중단하지 마십시오. 초기화를 중단할 경우 어플라이언스를 삭제하고 다시 시작해야 할 수 있습니다.

다음 절차를 사용하여 가상 어플라이언스를 초기화합니다.

절차

1. 어플라이언스의 전원을 켭니다. vSphere Client의 인벤토리 목록에서 가져온 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음, 컨텍스트 메뉴에서 **Power(전원) > Power On(전원 켜기)**을 선택합니다.
2. VMWare 콘솔 탭에서 초기화를 모니터링합니다.

다음 작업

- 구축 과정에서 VI OVF 템플릿을 사용하고 Firepower System의 필수 설정을 구성한 경우, 추가 컨피그레이션이 필요하지 않습니다. 자세한 내용은 Firepower Threat Defense Virtual을 Firepower Management Center에 등록, 9페이지를 참고하십시오.
- VI OVF 템플릿으로 구축할 때 ESXi OVF 템플릿을 사용했거나 Firepower System의 필수 설정을 구성하지 않은 경우, 계속해서 CLI를 사용하여 Firepower Threat Defense Virtual 장치 설정, 8페이지를 수행합니다.

CLI를 사용하여 Firepower Threat Defense Virtual 장치 설정

Firepower Threat Defense Virtual 어플라이언스에는 웹 인터페이스가 없으므로 ESXi OVF 템플릿으로 구축한 경우 CLI를 사용하여 가상 장치를 설정해야 합니다. 또한 구축 과정에서 VI OVF 템플릿으로 구축하고 설정 마법사를 사용하지 않은 경우에도 CLI를 사용하여 Firepower System의 필수 설정을 구성해야 합니다.

참고: VI OVF 템플릿으로 구축하면서 설정 마법사를 사용한 경우, 가상 장치가 구성되어 있으며 추가 작업이 필요하지 않습니다.

새로 구성된 장치에 처음으로 로그인하면 EULA를 읽고 동의해야 합니다. 그 다음 설정 프롬프트에 따라 관리자 비밀번호를 변경하고 장치의 네트워크 설정 및 방화벽 모드를 구성합니다.

설정 프롬프트를 진행하는 동안 선택형 질문의 경우 `(y/n)`과 같이 선택 사항이 괄호 안에 나열됩니다. 기본값은 `[y]`와 같이 대괄호에 나열됩니다. Enter 키를 눌러 선택을 확인합니다.

CLI의 프롬프트에 입력해야 할 설정 정보는 물리적 장치의 설정 웹 페이지와 거의 동일합니다. 자세한 내용은 *Firepower System 설치 가이드*를 참조하십시오.

참고: 초기 설정을 완료한 후 가상 장치의 이러한 설정을 변경하려면 CLI를 사용해야 합니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*의 명령행 참조 장을 참고하십시오.

절차

1. VMWare 콘솔을 엽니다.
2. VMWare 콘솔에서 사용자 이름으로 `admin`을 사용하고 구축 설정 마법사에서 지정한 새로운 관리자 어카운트 비밀번호를 사용하여 가상 어플라이언스에 로그인합니다.

   마법사를 사용하여 비밀번호를 변경하지 않은 경우 또는 ESXi OVF 템플릿으로 구축하는 경우 Admin123을 비밀번호로 사용합니다.

   EULA를 읽으라는 메시지가 장치에 즉시 표시됩니다.
3. EULA를 읽고 그 내용에 동의합니다.
4. `admin` 어카운트의 비밀번호를 변경합니다. 이 계정은 컨피그레이션 CLI 액세스 레벨을 보유하며 삭제할 수 없습니다.

참고: Cisco대문자, 소문자, 1개 이상의 숫자가 포함된 8자 이상의 영숫자로 만든 강력한 비밀번호를 사용하는 것이 좋습니다. 사전에 나오는 단어를 사용하지 마십시오.

5. 표시되는 화면 컨피그레이션을 완료합니다.

   설정이 구현되면 VMWare 콘솔에 메시지가 표시될 수 있습니다. 완료되면 이 장치를 Cisco Firepower Management Center에 등록하라는 알림이 장치에 나타나고 CLI 프롬프트가 표시됩니다.

6. 콘솔이 Firepower **#** 프롬프트로 돌아갈 때 설정이 성공적으로 완료되었는지 확인합니다.

   참고: Firepower Threat Defense Virtual를 Cisco Licensing Authority에 성공적으로 등록하려면 Firepower Threat Defense Virtual에 인터넷 액세스가 필요합니다. 구축 후 인터넷 액세스 및 성공적인 라이센스 등록을 위해 추가 컨피그레이션이 필요할 수 있습니다.

다음 작업

- Firepower Threat Defense Virtual을 Firepower Management Center에 등록합니다. 자세한 내용은 Firepower Threat Defense Virtual을 Firepower Management Center에 등록, 9페이지를 참고하십시오.

Firepower Threat Defense Virtual을 Firepower Management Center에 등록

가상 장치에는 웹 인터페이스가 없으므로 CLI를 사용하여 가상 장치를 물리적 또는 가상 Cisco Firepower Management Center에 등록해야 합니다. 장치의 CLI에 이미 로그인되어 있으므로, 초기 설정 프로세스 중에 장치를 Firepower Management Center에 등록하는 것이 가장 쉬운 방법입니다.

장치를 등록하려면 `configure manager add` 명령을 사용합니다. 장치를 Firepower Management Center에 등록하려면 항상 자체 생성된 고유한 영숫자 등록 키가 필요합니다. 등록 키는 사용자가 지정할 수 있는 간단한 키이며, 라이센스 키와는 다릅니다.

대부분의 경우 등록 키와 함께 Firepower Management Center의 IP 주소를 입력해야 합니다. 예를 들면 다음과 같습니다.

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

여기서 *XXX.XXX.XXX.XXX*는 관리하는 Firepower Management Center의 IP 주소이며 *my_reg_key*는 가상 장치에 입력한 등록 키입니다.

참고: ESXi 플랫폼에서 vSphere Client를 사용하여 가상 장치를 Firepower Management Center에 등록할 때 DNS 정보가 설정하는 동안 제공되지 않은 경우, 관리하는 Firepower Management Center의 IP 주소(호스트 이름이 아님)를 사용해야 합니다.

그러나 장치와 Firepower Management Center가 NAT(Network Address Translation) 장치에 의해 분리되고 Firepower Management Center가 NAT 장치 뒤에 있는 경우, 등록 키와 고유한 NAT ID를 함께 입력하고 IP 주소 대신 `DONTRESOLVE`를 지정합니다. 예를 들면 다음과 같습니다.

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

여기서 *my_reg_key*는 가상 장치에 입력한 등록 키이며 *my_nat_id* 는 NAT 장치의 NAT ID입니다.

장치가 Firepower Management Center 대신 NAT 장치 뒤에 있는 경우, 등록 키와 고유한 NAT ID를 함께 입력하고 Firepower Management Center의 호스트 이름 또는 IP 주소를 지정합니다. 예를 들면 다음과 같습니다.

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

여기서 *my_reg_key*는 가상 장치에 입력한 등록 키이며 *my_nat_id* 는 NAT 장치의 NAT ID입니다.

절차

1. CLI 컨피그레이션(관리자) 권한이 있는 사용자로 가상 장치에 로그인합니다.

- VMWare 콘솔에서 초기 설정을 수행 중인 경우, 필요한 액세스 레벨이 있는 `admin` 사용자로 이미 로그인되어 있습니다.
- 그렇지 않을 경우 VMWare 콘솔을 사용하여 장치에 로그인합니다. 장치의 네트워크 설정을 이미 구성한 경우에는 장치의 IP 주소 또는 호스트 이름으로 SSH를 통해 연결합니다.

2. 프롬프트에서 다음과 같은 구문의 `configure manager add` 명령을 사용하여 장치를 Cisco Firepower Management Center에 등록합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE}는 Firepower Management Center의 IP 주소를 지정합니다. Firepower Management Center의 주소를 직접 지정할 수 없는 경우 `DONTRESOLVE`를 사용합니다.
- *reg_key*는 장치를 Firepower Management Center에 등록하는 데 필요한 영숫자 등록 키입니다.

참고: 등록 키는 사용자가 생성한 일회용 키로, 37자를 초과하지 않아야 합니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 장치를 Firepower Management Center에 추가할 때 이 등록 키를 기억해야 합니다.

- *nat_id*는 Cisco Firepower Management Center와 장치 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 이 문자열은 호스트 이름이 `DONTRESOLVE`로 설정된 경우 필요합니다.

참고: 장치 등록 상태를 모니터링하려면 `show managers` 명령을 사용합니다.

3. 어플라이언스에서 로그아웃합니다.

다음 작업

- Firepower Management Center를 이미 설정한 상태에서 장치를 추가하려면 웹 인터페이스에 로그인하고 장치 관리(**Devices(장치) > Device Management(장치 관리)**) 페이지를 사용합니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*의 장치 관리 장을 참고하십시오.