Firepower 2100용 FDM On-Box Management Service 구성

목차

소개

이 문서에서는 FTD가 설치된 Firepower 2100 Series용 Firepower FDM(Device Management) On-Box Management 서비스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Firepower 2100, FTD 소프트웨어 설치
- Cisco FTD(Firepower Threat Defense) 기본 구성 및 문제 해결

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 2100 Series.
- Cisco FTD 버전 6.2.3

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

배경 정보

이 문서의 주된 목적은 firepower 2100 Series에 대해 FDM On-Box 관리를 활성화하는 데 필요한 단계를 안내하는 것입니다.

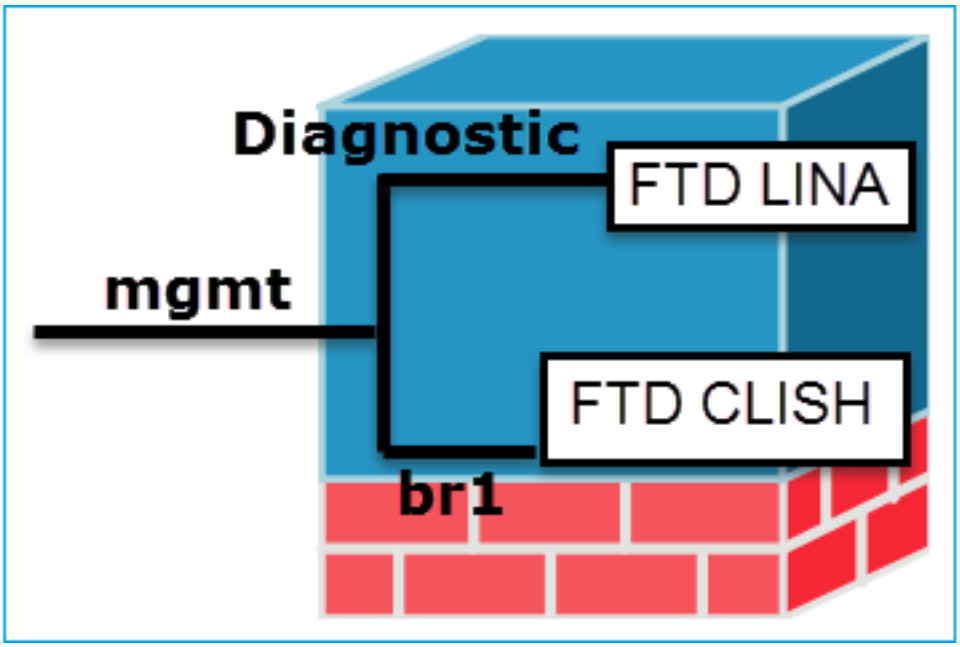
Firepower 2100에 설치된 FTD(Firepower Threat Defense)를 관리하는 옵션은 두 가지입니다.

- FDM On-Box 관리.
- Cisco FMC(Firepower Management Center).

참고: FDM과 FMC를 모두 사용하여 Firepower 2100에 설치된 FTD를 관리할 수는 없습니다. Firepower 2100 FTD에서 FDM On-Box 관리가 활성화되면 로컬 관리를 비활성화하고 FMC를 사용하도록 관리를 재구성하지 않는 한 FMC를 사용하여 FTD를 관리할 수 없습니다. 반면 FTD를 FMC에 등록하면 FTD에서 FDM On-Box 관리 서비스가 비활성화됩니다.

주의: 현재 Cisco는 FDM Firepower 컨피그레이션을 FMC로 마이그레이션하거나 그 반대로 마이그레이션할 수 있는 옵션이 없습니다. Firepower 2100에 설치된 FTD에 대해 구성하는 관리 유형을 선택할 때 이 점을 고려해야 합니다.

관리 인터페이스는 br1(FPR2100/4100/9300 어플라이언스의 management0) 및 진단 등 2개의 논리적 인터페이스로 나뉩니다.



	관리 - br1/management0	관리 - 진단
목적	• 이 인터페이스는 FTD/FMC 통신에 사용되는 FTD IP를 할당하기 위해 사용됩니다. • FMC/FTD 간의 sftunnel을 종료합니다. • 규칙 기반 syslog의 소스로 사용됩니다. • FTD 상자에 대한 SSH 및 HTTPS 액세스를 제공합니다.	• ASA 엔진에 대한 원격 액세스(예: SNMP)를 제공합 • LINA 레벨 syslogs, AAA, SNMP 등의 메시지 소스. 용됩니다.
필수	예. FTD/FMC 통신에 사용되므로(sftunnel은 그 위에서 종료됩니다).	아니요, 구성하는 것은 권장되지 않습니다. 대신 데이터 페이스를 사용하는 것이 좋습니다(아래 참고 사항 확인

참고: 진단 인터페이스에서 IP 주소를 해제하면 다른 데이터 인터페이스와 동일한 네트워크에 관리 인터페이스를 배치할 수 있다는 이점이 있습니다. 진단 인터페이스를 구성하는 경우 해당 IP 주소는 관리 IP 주소와 동일한 네트워크에 있어야 하며, 다른 데이터 인터페이스와 동일한 네트워크에 있을 수 없는 일반 인터페이스로 간주됩니다. 관리 인터페이스에는 업데이트를 위한 인터넷 액세스가 필요하므로, 관리 인터페이스를 내부 FTD 인터페이스와 동일한 네트워

크에 배치하려면 LAN의 스위치만으로 FTD를 구축하고 내부 인터페이스를 관리 인터페이스의 기본 게이트웨이로 지정할 수 있습니다(이는 FTD가 라우팅 모드로 구축된 경우에만 적용됨).

FTD는 Firepower 2100 어플라이언스에 설치할 수 있습니다. Firepower 섀시는 FXOS(Firepower eXtensible Operating System)라는 자체 운영 체제를 실행하여 디바이스의 기본 작업을 제어하는 반면, FTD 논리적 디바이스는 모듈/블레이드에 설치됩니다.

참고: FCM(Firepower Chassis Manager)이라는 FXOS GUI(Graphic User Interface) 또는 FXOS CLI(Command Line Interface)를 사용하여 firepower 섀시 기능을 구성할 수 있습니다. 그러나 FTD가 Firepower 2100 Series에 설치되어 있는 경우에는 FXOS CLI만 GUI FCM을 사용할 수 없습니다.

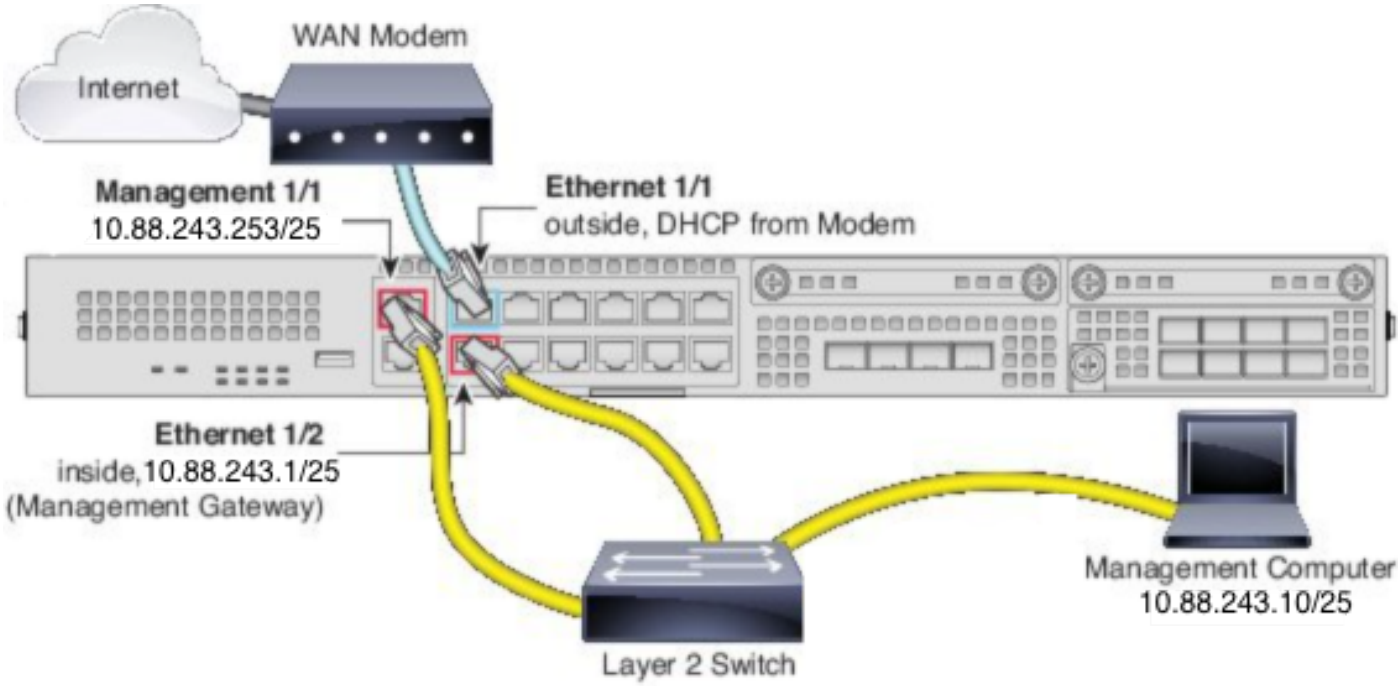
Firepower 21xx 어플라이언스:

참고: Firepower 2100 Series에서 관리 인터페이스는 섀시 FXOS와 FTD 논리적 디바이스 간에 공유됩니다.

구성

네트워크 다이어그램

기본 컨피그레이션에서는 특정 firepower 2100 인터페이스가 내부 및 외부 네트워크에 사용된다고 가정합니다. 이러한 기대치를 기반으로 네트워크 케이블을 인터페이스에 연결하면 초기 컨피그레이션을 보다 쉽게 완료할 수 있습니다. Firepower 2100 Series의 케이블을 연결하려면 다음 이미지를 참조하십시오.



참고: 이 그림에서는 레이어 2 스위치를 사용하는 간단한 토폴로지를 보여줍니다. 다른 토폴로지를 사용할 수 있으며, 구축은 기본 논리적 네트워크 연결, 포트, 주소 지정 및 컨피그레이션 요구 사항에 따라 달라질 수 있습니다.

설정

firepower 2100 시리즈에서 FDM On-Box 관리를 활성화하려면 다음과 같이 진행합니다.

1. FPR2100 섀시에 대한 콘솔 액세스 및 FTD 애플리케이션에 연결합니다.

```
firepower# connect ftd
>
```

2. FTD 관리 IP 주소를 구성합니다.

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

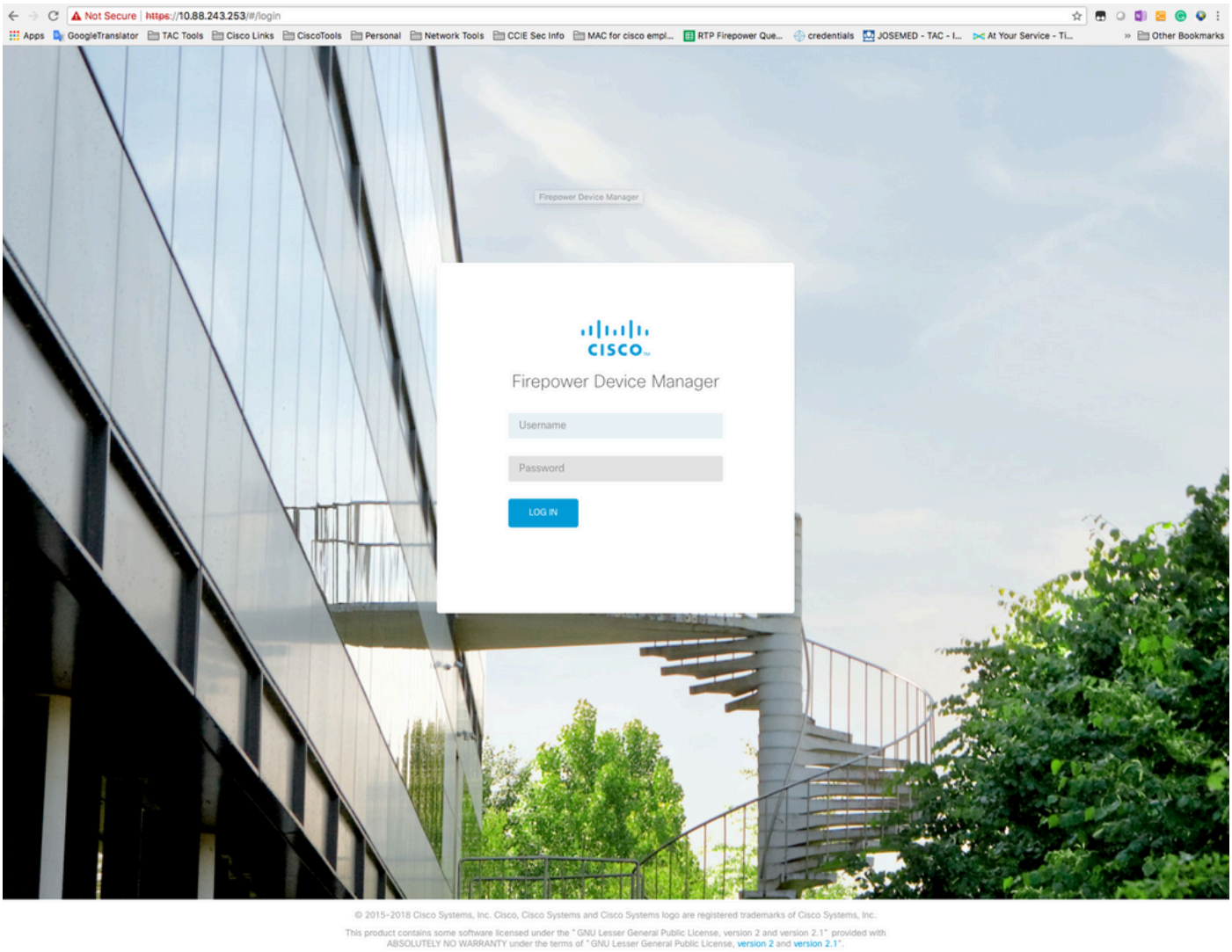
3. 관리 유형을 로컬로 구성합니다.

```
>configure manager local
```

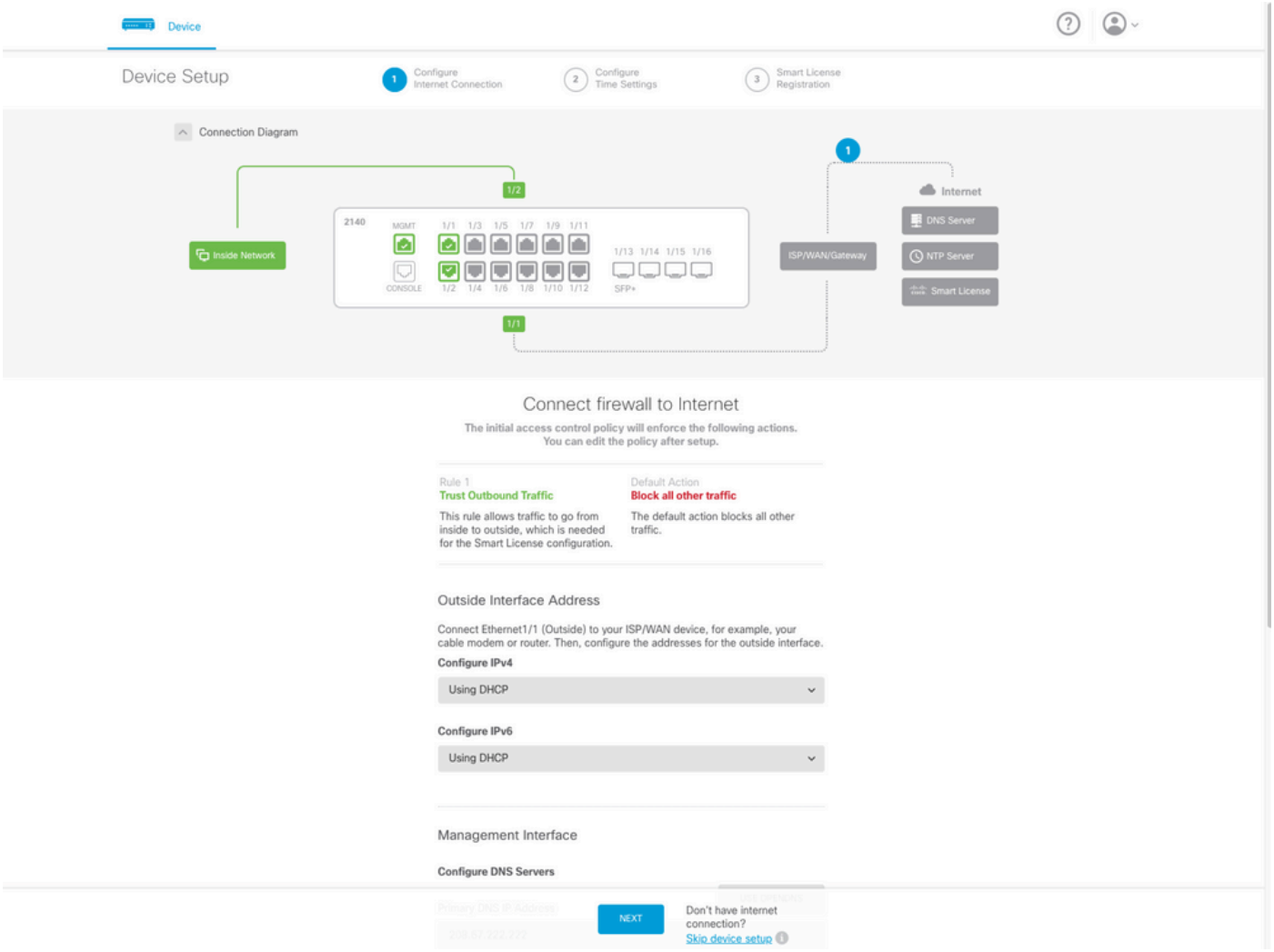
4. FTD에 대한 온박스 관리 액세스를 허용할 IP 주소/서브넷을 구성합니다.

```
>configure https-access-list 0.0.0.0/0
```

5. FTD를 관리하도록 구성한 IP 주소에 대한 브라우저 및 https를 엽니다. 이렇게 하면 FDM(On-Box) 관리자를 열 수 있습니다.



6. 로그인하고 기본 firepower 자격 증명, 사용자 이름 admin 및 비밀번호 Admin123을 사용합니다.



다음을 확인합니다.

1. 다음 명령으로 FTD에 대해 구성한 네트워크 설정을 확인합니다.

```
> show network
===============[ System Information ]===============
Hostname                  : firepower
DNS Servers               : 208.67.222.222
                            208.67.220.220
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.88.243.129

==================[ management0 ]===================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:2C:C8:41:09:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.88.243.253
Netmask                   : 255.255.255.128
Broadcast                 : 10.88.243.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

```
===============[ Proxy Information ]================
State                        : Disabled
Authentication               : Disabled
```

2. 다음 명령으로 FTD에 대해 구성한 관리 유형을 확인합니다.

```
> show managers
Managed locally.
```

관련 정보

Cisco Firepower Device Manager

Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center 빠른 시작 설명서

FTD(Firepower Threat Defense) 관리 인터페이스 설정

Firepower 2100 Series 재이미지화

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.