# 보안 방화벽 용어 해독(Firepower이 처음인 사용자를 위한)

## 목차



## 소개

이 문서에서는 여러 가지 인기 있는 Cisco Firewall Jargons에 대해 설명합니다. 이 문서에서는 CLI 모드 간에 전환하는 방법에 대해서도 설명합니다.

## 사전 요구 사항

### 요구 사항

이 항목을 학습하기 위한 사전 요구 사항은 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Firepower 위협 방어)
- Cisco FDM(Firepower Device Management)
- FXOS(Firepower eXtensible Operating System)
- FCM(Firepower Chassis Manager)
- ASA(Adaptive Security Appliance)

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.

## 일반적으로 사용되는 기술 용어

### FTD: Firepower 위협 방어

FTD는 기존 방화벽을 뛰어넘는 기능을 제공하는 차세대 방화벽입니다. 여기에는 IPS(Intrusion Prevention System), AMP(Advanced Malware Protection), URL 필터링, 보안 인텔리전스 등의 서비스가 포함됩니다. FTD는 ASA(Adaptive Security Appliance)와 매우 유사하지만 기능이 추가되었습니다. FTD는 LINA와 SNORT의 2개 엔진에서 실행됩니다.

### LINA: Linux 기반 통합 네트워크 아키텍처

FTD 디바이스에서는 ASA를 Lina라고 합니다. LINA는 단순히 FTD가 실행되는 ASA 코드에 불과합니다. Lina는 주로 네트워크 레이어 보안에 중점을 두고 있습니다. 애플리케이션 검사 및 제어 기능을 통해 일부 레이어 7 방화벽 기능을 통합합니다.

### SNORT

Snort 엔진은 네트워크 침입 탐지 및 방지 시스템입니다. Snort의 주요 기능으로는 이상 징후를 식별하는 패킷 검사, 규칙 기반 탐지, 실시간 알림, 로깅 및 분석, 기타 보안 툴과의 통합 등이 있습니다. Snort는 패킷 헤더뿐만 아니라 패킷의 내용을 기반으로 L7 검사(애플리케이션 레이어 트래픽)를 수행할 수 있습니다.

애플리케이션 레이어에서 특정 패턴 또는 시그니처를 정의하기 위한 사용자 지정 규칙을 유연하게 작성할 수 있어 탐지 기능이 향상됩니다. 패킷의 페이로드를 평가하여 심층 패킷 검사를 수행합니다. 여기에서 암호화된 패킷의 해독도 수행할 수 있습니다.

### FXOS: 확장 가능한 운영 체제 Firepower

FTD 디바이스가 실행되는 운영 체제입니다. 플랫폼에 따라 FXOS는 기능 구성, 섀시 상태 모니터링, 고급 문제 해결 기능 액세스에 사용됩니다.

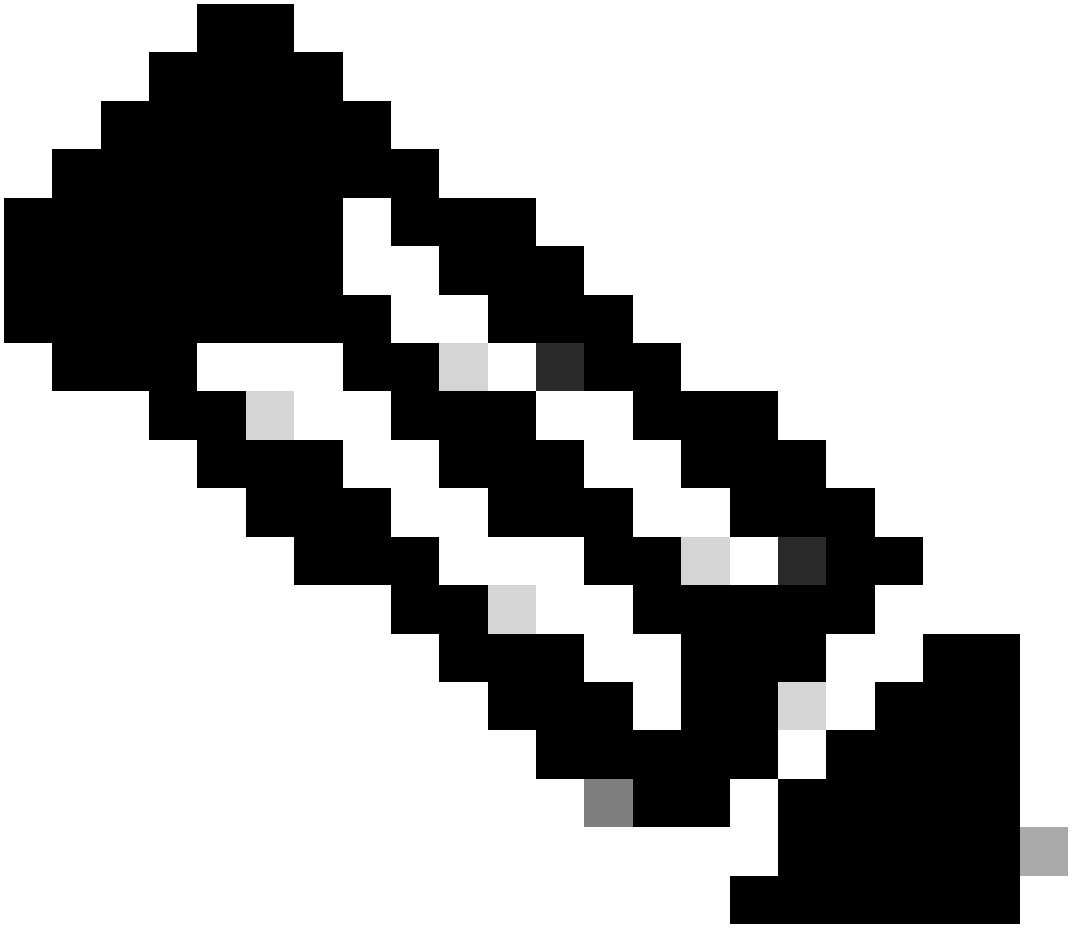
플랫폼 모드의 Adaptive Secure Appliance 소프트웨어가 포함된 Firepower 4100/9300 및

Firepower 2100의 FXOS는 구성 변경을 허용하지만, 특정 기능을 제외한 다른 플랫폼에서는 읽기 전용입니다.

## FCM: Firepower 섀시 관리자

FCM은 섀시를 관리하는 데 사용되는 GUI입니다. 플랫폼 모드에서 ASA를 실행하는 9300, 4100, 2100에서만 사용할 수 있습니다.

---



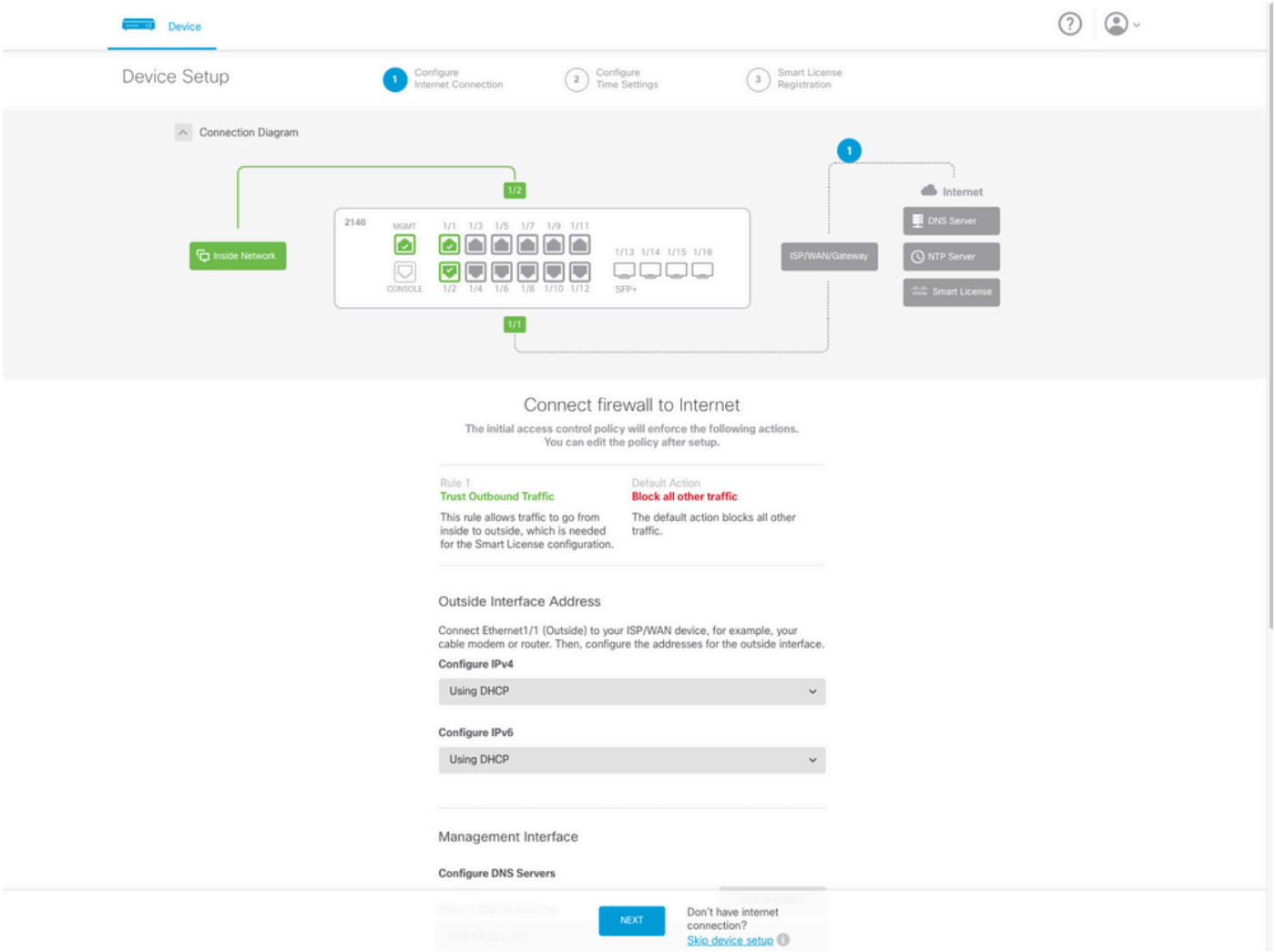
참고: 랩톱을 비유할 수 있습니다. FXOS는 운영 체제(랩톱의 Windows OS)로, 섀시(랩톱)에서 실행됩니다. Lina 및 Snort(구성 요소)에서 실행되는 FTD(애플리케이션 인스턴스)를 설치할 수 있습니다.

---

ASA와 달리 CLI를 통해 FTD를 관리할 수 없습니다. 별도의 GUI 기반 관리가 필요합니다. 이러한 서비스에는 FDM과 FMC의 2가지 유형이 있습니다.

## FDM: Firepower 장치 관리

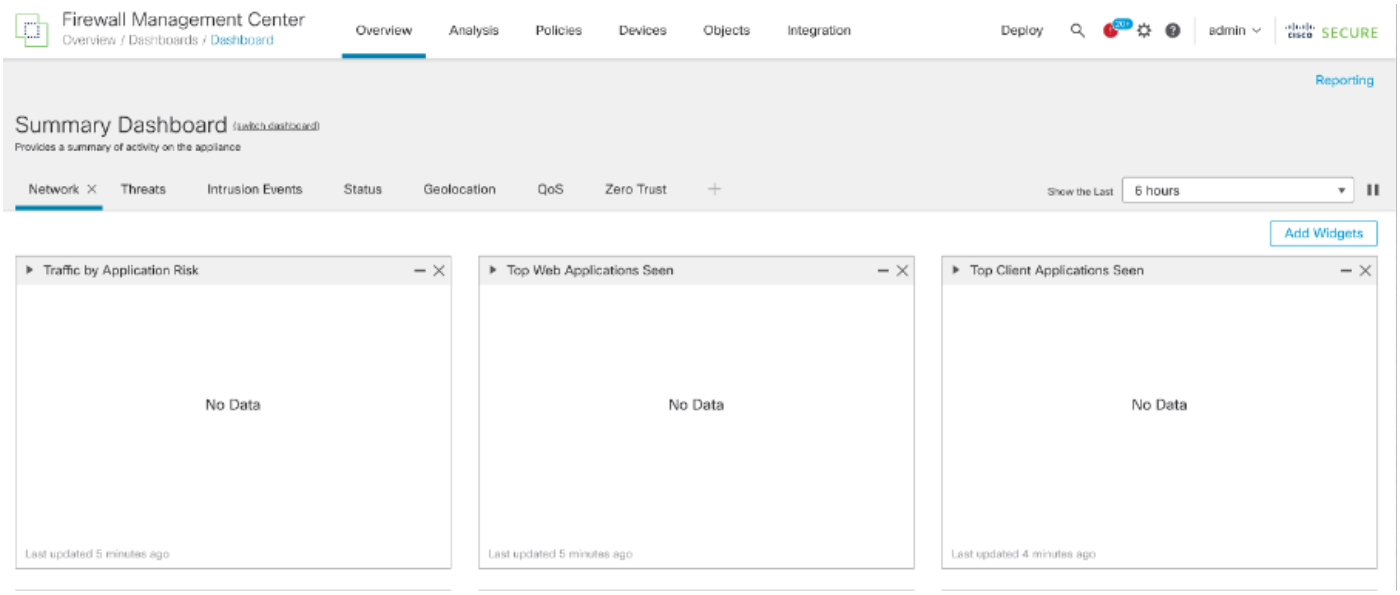
- FDM은 온박스 관리 도구입니다. 보안 정책 및 시스템 설정을 구성, 관리 및 모니터링하기 위한 웹 기반 인터페이스를 제공합니다.
- FDM을 사용할 때 얻을 수 있는 큰 이점 중 하나는 이 기능에 대한 추가 라이센스가 없다는 것입니다.
- FTD는 FDM 1개로 하나만 관리할 수 있습니다.



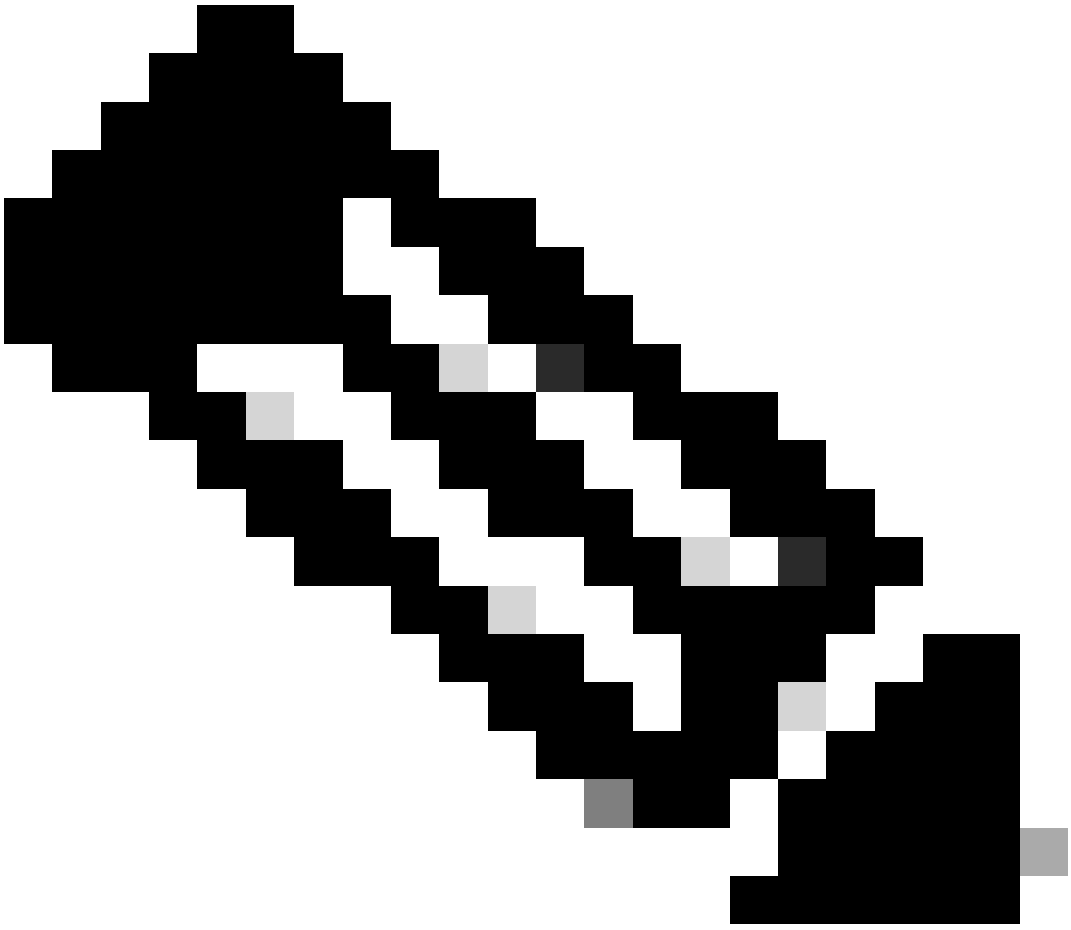

FDM

## FMC: Firepower 관리 센터

- FMC는 Cisco FTD 디바이스, Cisco ASA 디바이스(Firepower 서비스 포함)를 위한 중앙 집중식 관리 솔루션입니다. 또한 FTD 디바이스를 구성, 관리 및 모니터링하는 데 사용할 수 있는 GUI도 제공합니다.
- 하드웨어 FMC 디바이스 또는 가상 FMC 디바이스를 사용할 수 있습니다.
- 이를 위해서는 별도의 라이센스가 필요합니다.
- FMC의 장점 중 하나는 여러 FTD 디바이스를 하나의 FMC 디바이스로 관리할 수 있다는 것입니다.




FMC



참고: FTD 디바이스를 관리하는 데 FDM과 FMC를 모두 사용할 수는 없습니다. FDM On-Box 관리가 활성화되면 로컬 관리를 비활성화하고 FMC를 사용하도록 관리를 다시 구성하

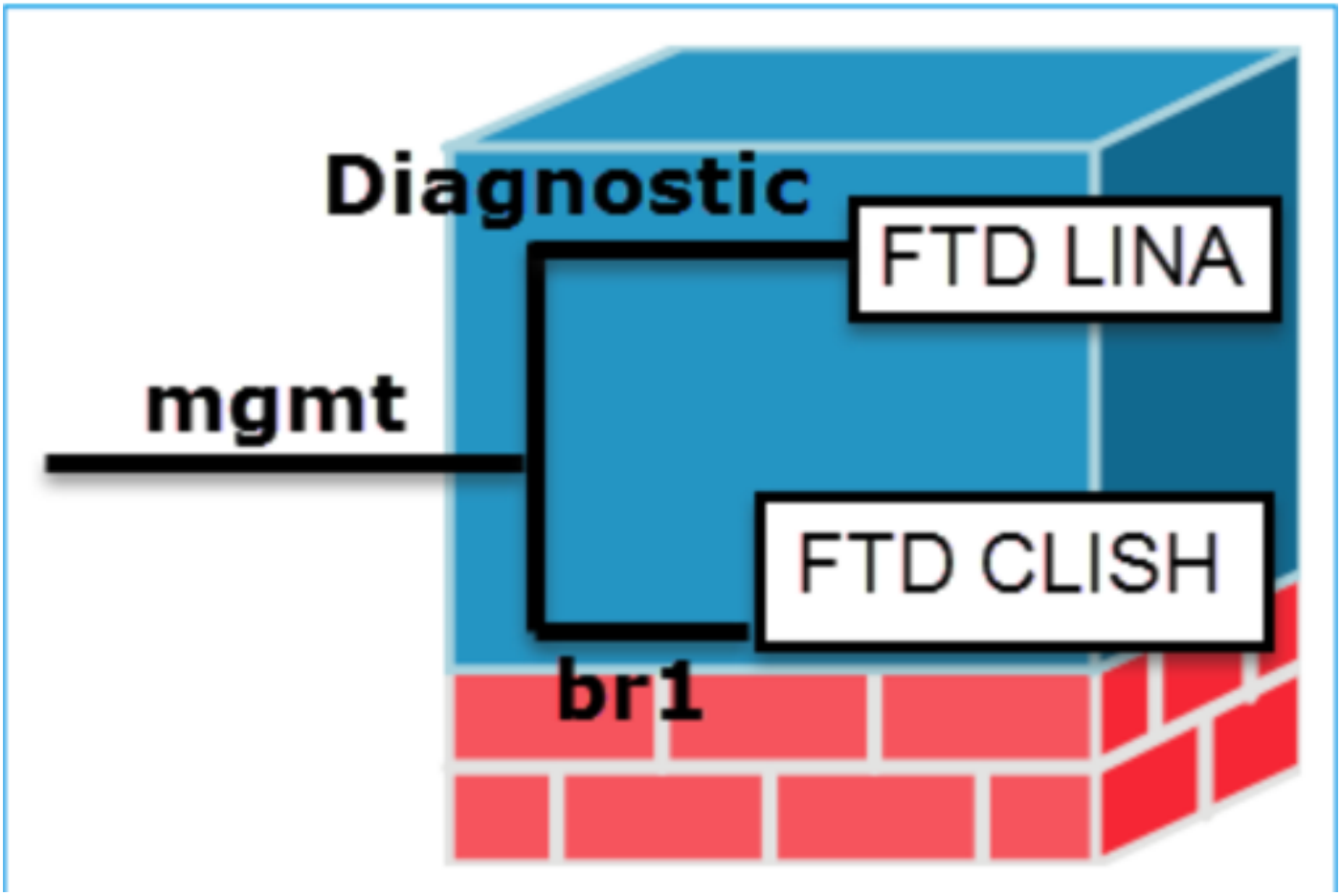
지 않는 한 FMC를 사용하여 FTD를 관리할 수 없습니다. 반면 FTD를 FMC에 등록하면 FTD에서 FDM On-Box 관리 서비스가 비활성화됩니다.

## CLISH: 명령줄 인터페이스 셸

CLISH는 Cisco FTD(Firepower Threat Defense) 디바이스에서 사용되는 명령줄 인터페이스입니다. 이 CLISH 모드를 사용하여 FTD에서 명령을 실행할 수 있습니다.

## 진단 관리

FTD 디바이스에는 진단 관리 인터페이스 및 FTD 관리 인터페이스인 2개의 관리 인터페이스가 있습니다. LINA 엔진에 액세스해야 하는 경우 진단 관리 인터페이스를 사용합니다. SNORT 엔진에 액세스해야 하는 경우 FTD 관리 인터페이스를 사용합니다. 둘 다 서로 다른 인터페이스이며 서로 다른 인터페이스 IP 주소가 필요합니다.




관리 인터페이스

## ASA 플랫폼 모드

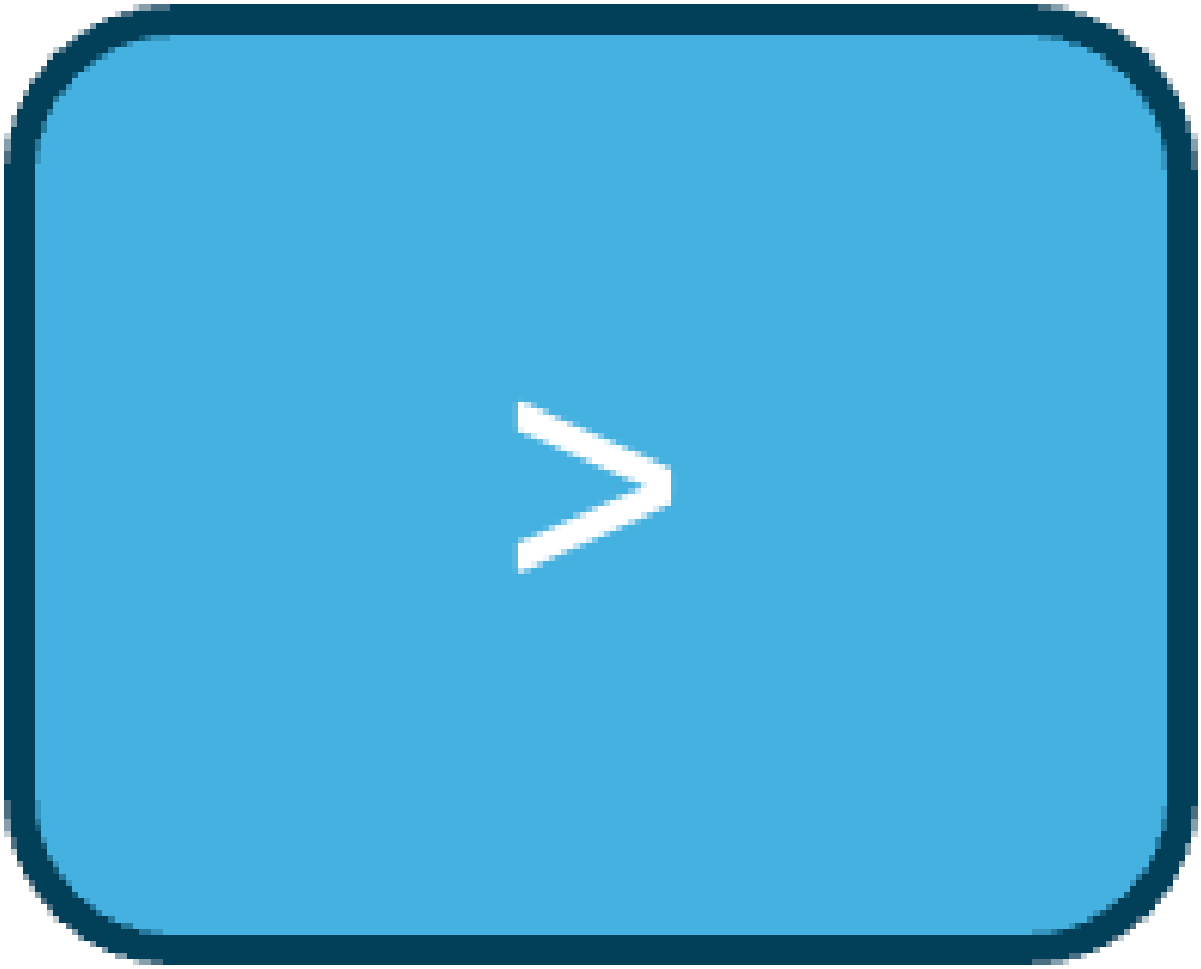
1. 플랫폼 모드에서는 인터페이스 활성화, EtherChannel 설정, NTP, 이미지 관리 등과 같은 FXOS의 기본 운영 매개변수 및 하드웨어 인터페이스 설정을 구성해야 합니다.
2. 다른 모든 컨피그레이션은 ASA CLI/ASDM을 통해 수행해야 합니다.
3. FCM 액세스 권한이 있습니다.

ASA 어플라이언스 모드

1. firepower 2100에서는 어플라이언스 모드의 ASA가 9.13(포함) 이상 도입되었습니다.
2. 어플라이언스 모드를 사용하면 ASA의 모든 설정을 구성할 수 있습니다. 고급 문제 해결 명령만 FXOS CLI에서 사용할 수 있습니다.
3. 이 모드에서는 FCM이 없습니다.

# FTD의 다른 프롬프트

낭비해




낭비해

루트 모드/전문가 모드

Expert 모드

리나 모드


리나 모드

FXOS 모드


FXOS 모드

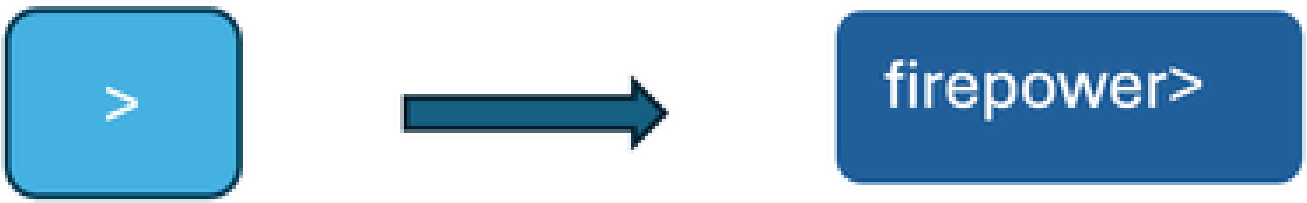
## 다른 프롬프트 사이를 이동하는 방법

FTD 루트 모드로 전환

Expert 모드로 전환

```
> expert
admin@firepower:~$  sudo su
Password:
root@firepower:/home/admin#
```

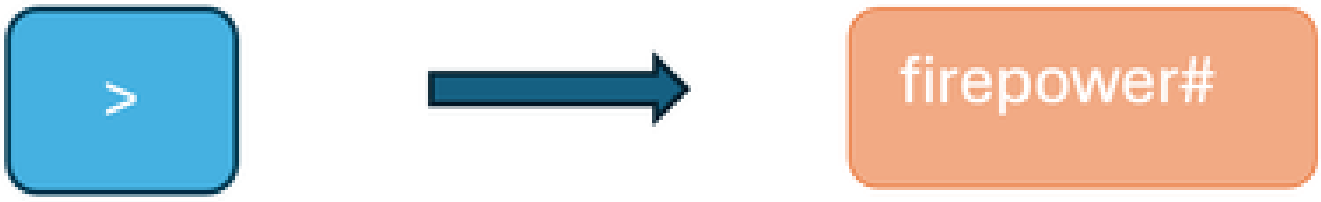
## CLISH 모드에서 Lina 모드로




Clish Mode에서 Lina Mode로

```
> system support diagnostic-cli
Attaching to Diagnostic CLI . . . Press 'Ctrl+a then d' to detach .
Type help or '?' for a list of available commands .
firepower> enable
Password :
firepower#
```

## CLI 모드에서 FXOS 모드로




FXOS 모드로 전환

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.
(------ cropped output -------)
firepower#
```

## 루트 모드에서 LINA 모드로


Expert에서 Lina 모드로

```
root@firepower:/home/admin#
root@firepower:/home/admin#   exit
exit
admin@firepower:~$ exit
logout
>
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

또는

```
root@firepower:/home/admin#
root@firepower:/home/admin#   sfconsole
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

## FXOS에서 FTD CLISH 모드(1000/2100/3100 Series 디바이스)


FXOS에서 Clish Mode로

```
firepower# connect ftd
>
```

```
To exit the fxos console
> exit
firepower#
```

### FXOS에서 FTD CLISH 모드(4100/9300 Series 디바이스)

다음 예에서는 모듈 1에서 위협 방어 CLI에 연결하는 방법을 보여 줍니다.

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1> connect ftd
>
```

콘솔을 종료합니다.

텔넷 애플리케이션을 종료하려면 ~를 입력한 다음 종료합니다.

```
Example:
>exit
Firepower-module1> ~
telnet> quit
firepower#
```

## 관련 문서

firepower 디바이스에서 실행할 수 있는 다양한 명령에 대한 자세한 내용은 FXOS 명령 참조, FTD 명령 참조를 참조하십시오.

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.