



Secure Firewall 200 Threat Defense : Firewall Device Manager

Cisco Secure Firewall Threat Defense
Updated NaN,

제

1

장

:

- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)
- [Cisco Secure Firewall Threat Defense](#) [ASA](#) [CLI](#) [FAQ](#)

소프트웨어 버전을 확인하고, 필요한 경우 이미지를 재설치하고, 라이선스를 획득한 후에 연결할 수 있는지 확인합니다.

Secure Firewall 200은 분산된 엔터프라이즈 및 소규모 브랜치용으로 설계된 차세대 방화벽 기능을 제공합니다. 소형 폼 팩터에서 강력하고 비용 효율적인 보안 및 간소화된 관리를 제공하여 네트워크 엣지에서 안전하고 최적화된 연결성을 보장합니다. **Secure Firewall 200:**

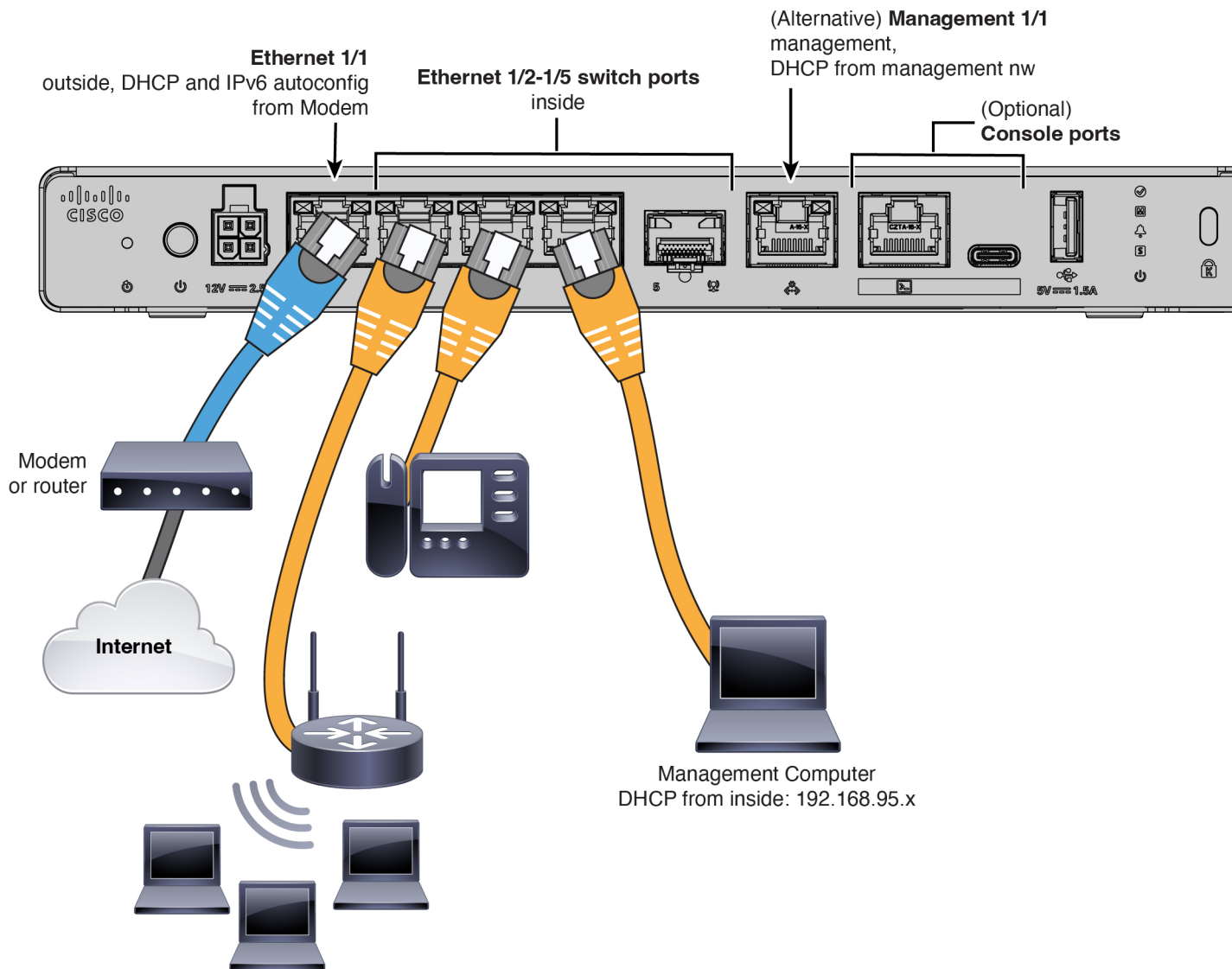
- Cisco의 하이브리드 메시 방화벽 아키텍처를 브랜치 엣지로 확장
- AI 기반 검사 및 일관된 보안 정책 제공
- SD-WAN 기능을 통합하여 성능 및 안정적인 사용자 액세스
- 민감한 환경에 맞게 조정된 애플리케이션 및 사용자 제어, 효율적인 세그멘테이션 및 고급 보안 기능 제공

로컬 **Secure Firewall Device Manager**를 사용하여 방화벽을 관리합니다.

성공적인 하드웨어 설정 및 네트워크 연결성을 보장하기 위한 **Secure Firewall 200**에 대한 케이블 연결 요구 사항을 설명합니다. 이 프로세스에서는 설정에 필요한 포트를 준비합니다.

방화벽 관리 센터를 전용 관리 1/1 인터페이스에 연결하여 업데이트를 위한 인터넷 액세스를 활성화합니다.

- SFP를 Ethernet 1/5에 설치 - SFP 모듈이 필요한 1Gbps SFP 포트입니다.
- 자세한 내용은 [하드웨어 설치 가이드](#)를 참조하십시오.



Secure Firewall 200의 전원을 켜는 방법을 구성하고, 전원 및 시스템 상태의 전면 패널 LED를 확인하여 성공적으로 시작되었는지 확인합니다.

이 작업을 통해 방화벽의 전원을 켜고 LED 상태 표시기를 통해 성공적인 시작을 확인할 수 있습니다.

시스템 전원은 디바이스 뒷면에 있는 전원 버튼로 제어됩니다. 전원 버튼은 부드러운 알림 기능을 제공하여 시스템의 정상적인 종료 과정을 지원함으로써 시스템 소프트웨어 및 데이터 손상 위험을 줄입니다.

주

방화벽을 처음 부팅할 때는 **Firewall Threat Defense** 초기화에 약 15~30분이 소요될 수 있습니다.

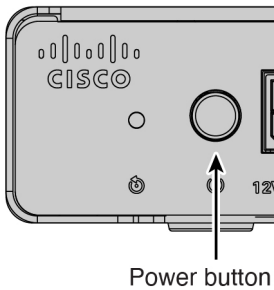
Before you begin

디바이스에 안정적인 전원을 제공하는 것이 중요합니다(예: UPS(Uninterruptable Power Supply) 사용). 먼저 켜다 운하지 않고 전력이 손실되면 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전력이 손실되면 시스템이 정상적으로 종료되지 않습니다.

방화벽의 전원을 켜려면 다음 단계를 따르십시오.

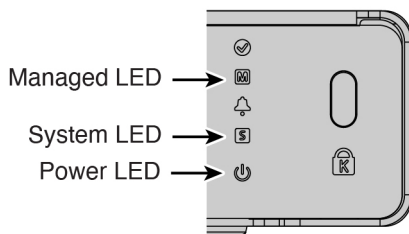
1. 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.
2. 전원 코드 옆에 위치한 새시 후면의 전원 버튼을 사용하여 전원을 켭니다.

1:



3. LED에서 현재 상태를 확인합니다.

2: LED



- 전원 LED - 녹색으로 켜져 있으면 방화벽 전원이 켜져 있음을 의미합니다.
- 시스템 (S) LED - 다음 동작을 참조하십시오.

1: (S) LED

LED 동작	설명	디바이스 전원이 켜진 후의 시간 (분:초)
녹색으로 빠르게 깜박임	부팅	01:00
황색으로 빠르게 깜박임(오류 상태)	부팅 실패	01:00
녹색	애플리케이션 로드됨	15:00 - 30:00
황색 고정(오류 상태)	애플리케이션 로드 실패	15:00 - 30:00

방화벽 전원이 성공적으로 켜지면 전원 LED가 녹색으로 고정되고 시스템 LED가 적절한 애플리케이션 로딩 상태를 나타냅니다. 디바이스의 설정 및 작동 준비가 완료되었습니다.

Firewall Threat Defense ASA ?

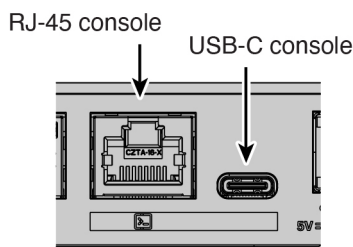
콘솔 포트에 연결하고 CLI 프롬프트를 식별하여 Secure Firewall 200에서 Firewall Threat Defense 또는 ASA가 실행 중인지를 확인합니다.

이 작업은 현재 하드웨어 플랫폼에 설치되어 있는 방화벽 애플리케이션을 식별하는 데 도움이 됩니다.

애플리케이션 Firewall Threat Defense 또는 ASA 모두 하드웨어에서 지원됩니다. 콘솔 포트에 연결하고 공장에서 설치된 애플리케이션이 무엇인지 확인합니다.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

3:



2. CLI 프롬프트를 참조하여 방화벽 Firewall Threat Defense 또는 ASA를 실행 중인지 확인합니다.

Firewall Threat Defense

Firepower 로그인(FXOS) 프롬프트가 표시됩니다. 로그인하고 새 비밀번호 설정하지 않고 연결을 끊을 수 있습니다. 끝까지 로그인해야 하는 경우에는 [Firewall Threat Defense CLI에 액세스 페이지 6](#)를 참조하십시오.

```
firepower login:
```

ASA

ASA 프롬프트가 표시됩니다.

```
ciscoasa>
```

3. 잘못된 애플리케이션을 실행 중인 경우 [Cisco Secure Firewall ASA](#) 및 [Secure Firewall Threat Defense 이미지 재 설치 가이드](#)를 참조하십시오.

CLI 프롬프트 모양을 기반으로 하드웨어에 설치된 방화벽 애플리케이션을 식별했습니다.

Firewall Threat Defense CLI

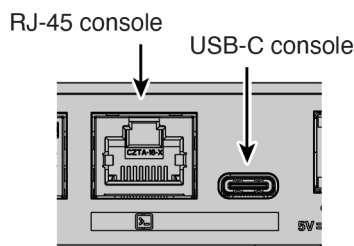
필요 시 FXOS에 로그인하거나 FTD CLI로 전환하는 등의 설정 또는 문제 해결 작업이 포함됩니다.

CLI에 액세스하여 디바이스 구성, 설정 및 문제 해결 작업을 수행합니다.

구성 또는 문제 해결을 위해 CLI에 액세스해야 할 수 있습니다.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

4:



2. FXOS에 연결합니다. **admin** 사용자 이름 및 비밀번호(기본값은 **Admin123**)를 사용하여 CLI에 로그인합니다. 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다.

Example

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

3. Firewall Threat Defense CLI로 변경합니다.



초기 설정에 **Firewall Device Manager**를 사용하려면 **Firewall Threat Defense CLI**에 액세스하지 마십시오. 그러면 **CLI** 설정이 시작됩니다.

connect FTD

Firewall Threat Defense CLI에 처음 연결할 때는 초기 구성을 완료하라는 프롬프트가 표시됩니다.

Example

```
firepower# connect ftd
>
```

Firewall Threat Defense CLI를 종료하려면 **exit** 또는 **logout** 명령을 입력합니다. 그러면 **FXOS** 프롬프트로 돌아갑니다.

Example

```
> exit
firepower#
```

구성을 시작하기 전에, **Firewall Threat Defense** 소프트웨어 버전을 구성하고, **Secure Firewall 200**을(를) 대상 릴리스로 이미지 재설치합니다.

현재 소프트웨어 버전을 확인하고 필요한 경우 이미지를 재설치하여 구성 전에 방화벽이 권장 버전을 실행 중인지 확인하십시오.

방화벽을 구성하기 전에 대상 버전을 설치하는 것이 좋습니다. 또는 가동을 시작한 후 업그레이드를 수행할 수 있지만, 구성을 유지하는 업그레이드는 이 절차를 사용하는 것보다 시간이 더 오래 걸릴 수 있습니다.

어떤 버전을 실행해야 하나요?

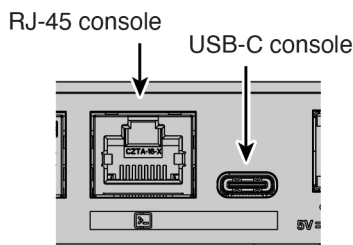
Cisco는 소프트웨어 다운로드 페이지에서 릴리스 번호 옆에 금색 별표로 표시된 **Gold Star** 릴리스를 실행할 것을 권장합니다. <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html>에 설명된 릴리스 전략을 참조할 수도 있습니다.

Before you begin

다음 단계에 따라 버전을 확인하고 디바이스의 이미지를 재설치하십시오.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

5:



2. FXOS CLI에서 실행 중인 버전을 표시합니다.

scope ssa

show app-instance

Example

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name Slot ID Admin State Operational State Running Version Startup
Version Cluster Oper State
-----
ftd              1      Enabled      Online      7.6.0.65      7.6.0.65
                Not Applicable
```

3. 새 버전을 설치하려면 다음 단계를 수행합니다.

기본적으로 관리 인터페이스는 **DHCP**를 사용합니다. 관리 인터페이스에 대한 고정 **IP** 주소를 설정해야 하는 경우 다음 명령을 입력합니다.

scope fabric-interconnect a

set out-of-band static IP /IP netmask 넷마스크 **gw** 게이트웨이

commit-buffer

다음 오류가 발생하면 변경 사항을 커밋하기 전에 **DHCP** 서버를 비활성화해야 합니다. 아래 명령어를 따라 **DHCP**를 서버를 비활성화합니다.

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask>) is not
) is not
in the same network of current DHCP server IP range <ip - ip>.
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

a) 이미지 재설치 절차는 [FXOS 문제 해결 설명서](#)를 참조하십시오.

관리 인터페이스에서 액세스할 수 있는 서버에서 새 이미지를 다운로드해야 합니다.

방화벽이 재부팅된 후 **FXOS CLI**에 다시 연결됩니다

b) **FXOS CLI**에서 관리자 비밀번호를 다시 설정하라는 메시지가 표시됩니다.

현재 소프트웨어 버전을 확인하고, 필요한 경우 방화벽 대상 릴리스로 이미지를 재설치했습니다. 이제 방화벽이 적절한 소프트웨어 버전으로 구성할 준비가 되었습니다.

CLI

기본 주소 지정이 작동하지 않을 때 **CLI**에서 **Secure Firewall 200** 관리 1/1 네트워크 설정을 구성하므로, 네트워크에서 **Secure Firewall Device Manager**에 연결할 수 있습니다.

이 작업을 수행하면 네트워크 환경에서 기본 IP 주소를 사용할 수 없는 경우 관리 1/1 인터페이스에 대한 고정 IP 주소를 설정할 수 있습니다.

기본적으로 다음 인터페이스 중 하나에서 방화벽을 관리할 수 있습니다.

- Ethernet 1/2 및 이상 - 192.168.95.1/24
- Management 1/1 - DHCP로부터 할당된 IP 주소

기본 IP 주소를 사용할 수 없는 경우 콘솔 포트에 연결하여 **CLI**에서 초기 설정을 수행하고 관리 1/1 IP 주소를 정적 주소로 설정할 수 있습니다.

-
1. 콘솔 포트에 연결합니다. [Firewall Threat Defense와 ASA 중 어떤 애플리케이션이 설치되나요?](#) 페이지 5을 참조하십시오.
 2. **Firewall Threat Defense CLI**에 연결합니다.

connect ftd

Example

```
firepower# connect ftd
>
```

3. 그러면 관리 인터페이스 설정을 위한 **CLI** 설정 스크립트가 표시됩니다.

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
```

```
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

지침: 다음 주소 유형 중 하나 이상에 대해 **y**를 입력합니다.

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

지침: 정적 IP 주소를 설정하려면 **manual**을 선택합니다.

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]:
255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
10.10.10.1
```

지침: 게이트웨이의 IP 주소를 설정합니다.

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
```

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on
management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

지침: Firewall Device Manager 명령을 사용하려면 **yes**를 입력합니다.

4. 새 관리 IP 주소에서 Firewall Device Manager에 로그인합니다.

이제 관리 1/1 인터페이스가 고정 IP 주소로 설정되었으며 새 IP 주소를 사용하여 Firewall Device Manager에 액세스할 수 있습니다.

Cisco Smart Software Manager 및 Cisco Commerce Workspace에서 Secure Firewall 200 라이선스를 구성합니다. 여기에는 필요한 라이선스 유형을 파악하고, 추가 사용 권한을 주문하는 데 사용되는 라이선스 PID를 확인하는 작업이 포함됩니다.

Cisco 디바이스에 필요한 라이선스를 확보하고 적절한 작동과 컴플라이언스를 보장하여 다양한 기능과 성능을 활성화합니다.

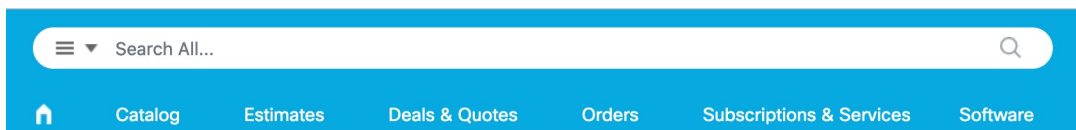
Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 **Smart Software License** 어카운트에 연결되어 있어야 합니다. 초기에 제공된 라이선스 외에 추가 라이선스가 필요한 경우, **Cisco Commerce Workspace**를 통해 취득할 수 있습니다.

Firewall Threat Defense에는 다음 라이선스가 있습니다.

- 표준—필수
- IPS
- 멀웨어 방어
- URL 필터링
- Cisco Secure Client

1. **Cisco Commerce Workspace**로 이동하여 **Search All**(모두 검색) 필드를 사용합니다.

6:

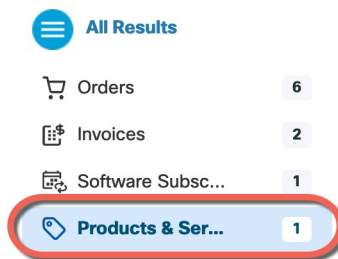


2. 라이선스 PID를 검색합니다.

원하는 PID는 주문 안내서를 확인하십시오.

3. 결과에서 **Products & Services**(제품 및 서비스)를 선택합니다.

7:



Cisco Commerce Workspace에서 필요한 라이선스 PID를 확인했으므로, 이제 해당 디바이스에 대한 추가 사용 권한을 주문할 수 있습니다.

FXOS CLI 셧다운 명령 또는 **Firewall Device Manager** 셧다운 워크플로우를 사용하여 파일 시스템 손상을 방지하기 위해, 효과적으로 **Secure Firewall 200** 전원을 차단하는 방법을 설명합니다.

방화벽 전원 차단 절차란, 실행 중인 모든 프로세스가

- 정상적으로 셧다운되도록 보장하고, 부적절한 셧다운으로 인해

- 발생할 수 있는 파일 시스템 손상을 방지하며, 전원이 차단되기 전에 백그라운드 프로세스가
- 제대로 완료될 수 있도록 하는 시스템 셧다운 프로세스입니다.

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 방화벽 시스템이 정상적으로 종료되지 않습니다.

CLI

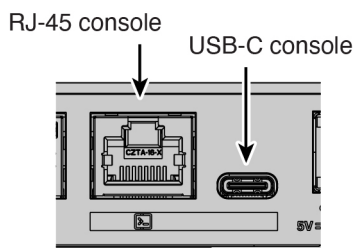
전원을 제거하거나 디바이스를 이동하기 전에 시스템을 정상적으로 중지할 수 있도록 **FXOS CLI**에서 **Secure Firewall 200**를 종료하는 방법을 구성합니다.

명령줄 인터페이스에서 물리적으로 전원을 끄거나 디바이스를 재배포하기 전에 이 절차를 사용하여 방화벽 시스템을 안전하게 종료합니다.

FXOS를 사용하여 시스템을 안전하게 종료하고 **Firewall**의 전원을 끌 수 있습니다.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

8:



2. **FXOS CLI**에서 **local-mgmt**에 연결합니다.

```
Firepower # connect local-mgmt
```

3. 시스템을 종료합니다.

```
firepower(local-mgmt) # shutdown
```

Example

```
firepower(local-mgmt) # shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
```

4. 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 종료가 완료되면 다음 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

5. 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

방화벽 시스템이 안전하게 종료되었으며 물리적 전원 제거 또는 재배치를 수행할 준비가 되었습니다.

Device Manager Firewall

원격으로 관리하는 경우에도 디바이스의 전원을 안전하게 차단할 수 있도록, **Firewall Device Manager**를 통해 **Secure Firewall 200**의 안전 종료를 구성합니다.

이 작업을 통해 방화벽 시스템을 올바르게 종료하여 데이터 손상을 방지하고 안전한 전원 제거를 보장할 수 있습니다.

Firewall Device Manager를 사용하여 시스템을 올바르게 종료할 수 있습니다.

1. 방화벽을 종료합니다.

- a) 디바이스를 클릭한 다음, **System Settings(시스템 설정) > Reboot/Shutdown(리부팅/종료) > 링크**를 클릭합니다.
- b) **Shut Down(종료)**을 클릭합니다.

2. 방화벽에 대한 콘솔 연결이 있는 경우 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 종료가 완료되면 이 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

콘솔에 연결되지 않은 경우 시스템이 종료될 때까지 약 **3분** 동안 기다리십시오.

3. 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

방화벽이 안전하게 종료되며 데이터 손상 위험 없이 전원을 제거할 수 있습니다.

제

2

장

:

- Firewall Device Manager □ □ □ □
- □ □ □ □ □ □
- □ □ □ □ □ □ □ □ □ □

초기 구성을 완료한 다음 추가 인터페이스 및 네트워크 설정을 구성하고 정책을 맞춤화합니다.

Firewall Device Manager

기본 내부 URL 또는 관리 1/1 주소를 사용하여 구성을 시작할 수 있도록 Secure Firewall 200에서 Secure Firewall Device Manager에 로그인하는 방법.

Firewall Threat Defense를 구성하려면 Firewall Device Manager에 로그인합니다.

1. 컴퓨터가 연결되는 인터페이스에 따라 브라우저에 다음 URL을 입력합니다.

- Ethernet 1/2 및 이상—<https://192.168.95.1>
- 관리 1/1—https://management_ip(DHCP에서)

2. 사용자 이름 **admin** 및 기본 비밀번호 **Admin123**으로 로그인합니다.

Secure Firewall 디바이스 관리자에서 초기 Secure Firewall 200 설정을 완료하여 디바이스가 기본 외부 연결성 및 내부-외부 정책이 작동하도록 하는 방법을 알아봅니다.

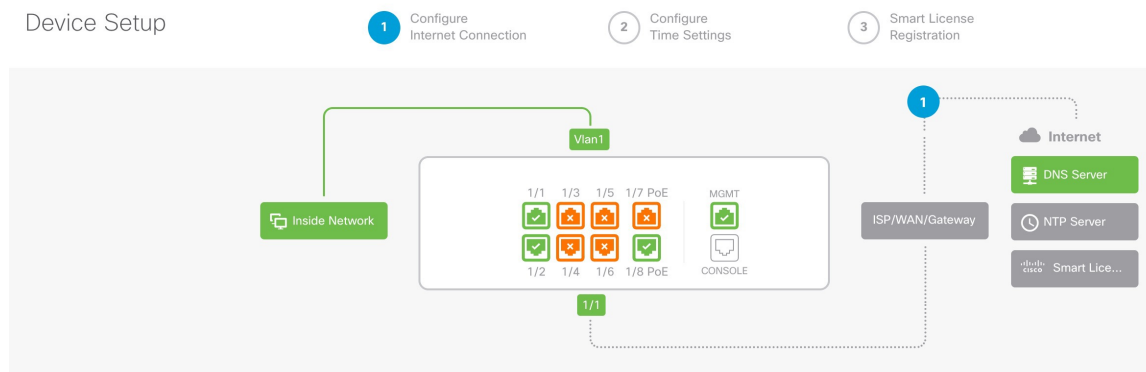
초기 설정을 완료하기 전에 처음으로 Firewall Device Manager에 로그인할 때 설정 마법사를 사용합니다. 설치 마법사를 완료하고 나면 작동 중인 디바이스에 몇 가지 기본 정책이 갖추어져 있어야 합니다.

- 내부→외부 트래픽 흐름
- 외부로 가는 모든 트래픽을 위한 인터페이스 PAT.

1. 일반 약관에 동의하고 관리자 비밀번호를 변경합니다.

Device Setup(디바이스 설정) 화면이 나타납니다.

9:





정확한 포트 구성은 모델에 따라 다릅니다.

2. 외부 및 관리 인터페이스에 대한 네트워크 설정을 구성합니다.

10:

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1 Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	Default Action Block all other traffic The default action blocks all other traffic.
---	---

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP ▼

Configure IPv6

Using DHCP ▼

NEXT

Don't have internet connection?
[Skip device setup](#) i

a) 외부 인터페이스 - 이더넷 1/1. 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다.

IPv4 구성— PPPoE가 필요한 경우 마법사를 완료한 후 PPPoE를 구성할 수 있습니다.

IPv6 구성

b) 관리 인터페이스 - 전용 관리 1/1 인터페이스에 대한 매개변수를 설정합니다. CLI에서 IP 주소를 변경한 경우, 이러한 설정은 이미 구성했으므로 표시되지 않습니다.

DNS 서버 - 기본값은 OpenDNS 공개 DNS 서버입니다.

방화벽 호스트 이름

c) **Next(다음)**를 클릭합니다.

3. 시스템 시간 설정을 구성합니다.

11: (NTP)

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC

NTP Time Server

Default NTP Servers

Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

NEXT

- a) 표준 시간대
- b) **NTP** 시간 서버
- c) **Next(다음)**를 클릭합니다.

4. 스마트 라이선싱 구성.

Register with Cisco Smart Software Manager

Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.

[What is smart license? ↗](#)

- ☐ **Continue with evaluation period: Start 90-day evaluation period without registration**
Recommended if device will be cloud managed. [Learn More ↗](#)
 Please make sure you register with Cisco before the evaluation period ends.
 Otherwise you will not be able to make any changes to the device configuration.

- ☒ **Register device with Cisco Smart Software Manager**
 Please register your device at this time. If you do not register now, you can register later from the Device > Smart License page.

- 1 Create or log in into your [Cisco Smart Software Manager](#) account.
↓
 - 2 On your assigned virtual account, under "General tab", click on **"New Token"** to create token.
↓
 - 3 Copy the token and paste it here:
↓
 Token

```
MDM4MTdhNWetNmExMC00NzMyLWE3YWVtMzY1MWViOTM2NmE0LTE3NDU0MzI2%0ANjQyMjV8dUNPZnRLWDJhSFJ6bWc0YkFqVWZWQzJzd2JDN2dwRkxhbUhQeHhj%0AZUtnUT0%3D%0A|
```
 - 4 Select the region in which your device is operating.
↓
 Region

US Region
▼
i
 - 5 Enroll Cisco Success Network.
 Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.
 Check out the [Sample Data](#) that will be sent to Cisco. [See more ▼](#)
☒ Enroll Cisco Success Network
- [?](#) For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide ↗

BACK

FINISH

- a) **Register device with Cisco Smart Software Manager**(Cisco Smart Software Manager에 디바이스 등록)를 클릭합니다.
- b) [Cisco Smart Software Manager](#) 링크를 클릭합니다.
- c) **Inventory**(인벤토리)를 클릭합니다.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts

Inventory

Convert to Smart Licensing

d) **General(일반)** 탭에서 **New Token(새 토큰)**을 클릭합니다.

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances t

New Token...		
Token	Expiration Date	Uses
OWFINTZiYtGtY2Ew...	2024-May-18 17:41:53 (in 30 days)	0 of 10

e) **Create Registration Token(등록 토큰 생성)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(토큰 생성)**을 클릭합니다.

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

* Expire After: Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

☒ Allow export-controlled functionality on the products registered with this token

Create Token

Cancel

- 설명
- **Expire After(다음 이후에 만료)** — 30일로 설정하는 것이 좋습니다.
- 최대 사용 개수
- **Allow export-controlled functionality on the products registered with this token(이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용)** — 강력한 암호화를 허용하는 국가에 있는 경우 내보내기-규정 준수 플래그를 활성화합니다. 해당 기능을 사용하려는 경우 이 옵션을 지금 선택해야 합니다. 나중에 이 기능을 활성화하는 경우 새 제품 키로 디바이스를 다시 등록하고 디바이스를 다시 로드해야 합니다. 이 옵션이 표시되지 않으면 어카운트가 내보내기 제어 기능을 지원하지 않는 것입니다.

토큰이 인벤토리에 추가됩니다.

f) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(토큰)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 **Firewall Threat Defense**를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

12:

General Licenses Product Instances Event Log

Virtual Account

Description: [Redacted]

Default Virtual Account: No

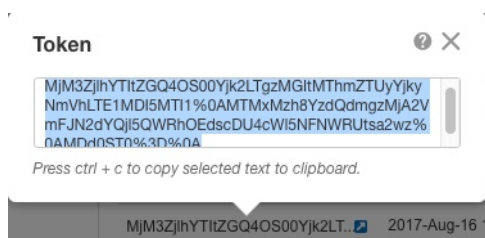
Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled
OWFINTZYtY2Ew...	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

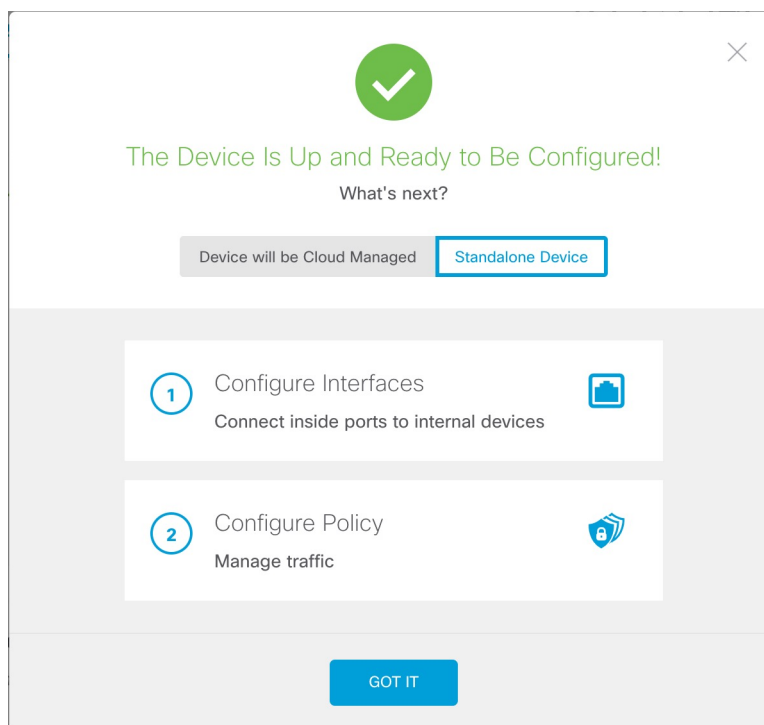
13:



- g) Firewall Device Manager에서 , 토큰을 토큰 필드에 붙여넣습니다.
 h) 다른 옵션을 설정하고 **Finish(마침)**를 클릭합니다.

5. 설정 마법사를 마칩니다.

14:



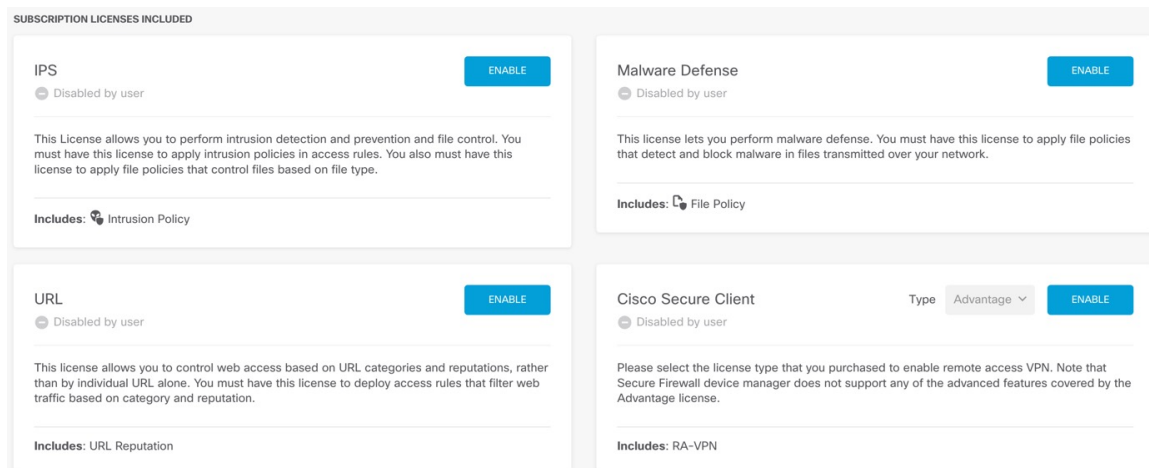
- a) Firewall Device Manager를 사용하려면 **Standalone Device(독립형 디바이스)**를 클릭합니다.

- b) **Configure Interfaces**(인터페이스 구성)를 클릭하여 **Interfaces**(인터페이스) 페이지로 직접 이동하거나, **Configure Policy**(정책 구성)를 클릭하여 **Policies**(정책) 페이지로 이동하거나, **Get It**(확인)을 클릭하여 **Device**(디바이스) 페이지로 이동합니다.

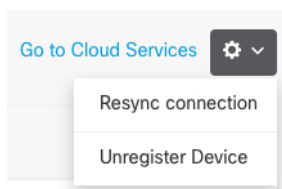
인터페이스 또는 정책 구성은 [네트워크 설정 및 정책 구성](#) 페이지 21의 내용을 참조하십시오.

6. 기능 라이선스를 활성화합니다.

- a) **Device**(디바이스) 페이지에서 **Smart License**(스마트 라이선스) > > **View Configuration**(구성 보기)을 클릭합니다.
- b) 선택 가능한 각 라이선스에 대해 **Enable**(활성화)/**Disable**(비활성화) 컨트롤을 클릭합니다.



- c) Cisco Smart Software Manager와 라이선스 정보를 동기화하려면 기어 드롭다운 목록에서 **Resync Connection**(연결 다시 동기화)를 선택합니다.



Secure Secure Firewall Device Manager에서 인터페이스, 보안 영역, DHCP 및 보안 정책을 설정하는 방법을 통해 보안 정책을 적용하여 Secure Firewall 200는 네트워크 설계 및 트래픽 요구 사항을 충족할 수 있습니다.

추가 인터페이스와 DHCP 서버를 구성하고 보안 정책을 맞춤화합니다.

1. 스위치 포트를 방화벽 인터페이스를 변환하려면 **Device**(디바이스)를 선택한 다음 **Interface**(인터페이스) 요약의 링크를 클릭합니다.

- a) 스위치 포트의 편집 아이콘(🔧)을 클릭합니다.
- b) 모드를 **Switch Port**(스위치 포트)에서 **Routed**(라우팅)으로 변경합니다.

15:

Ethernet1/3
Edit Physical Interface

Interface Name

Mode

Switch Port
Routed
Passive
Switch Port

Status

Description

IPv4 Address
IPv6 Address
Advanced
VLAN

Protected Port

Usage Type

Access
Trunk

Access VLAN

inside (Vlan1)

CANCEL
OK

c) 이름 및 IP 주소를 설정합니다.

16:

Ethernet1/3
Edit Physical Interface

Interface Name

dmz

Mode

Routed

Status

☒

Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address
IPv6 Address
Advanced

Type

Static

IP Address and Subnet Mask

192.168.1.4

 /

24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask
 /

e.g. 192.168.5.16

CANCEL

OK

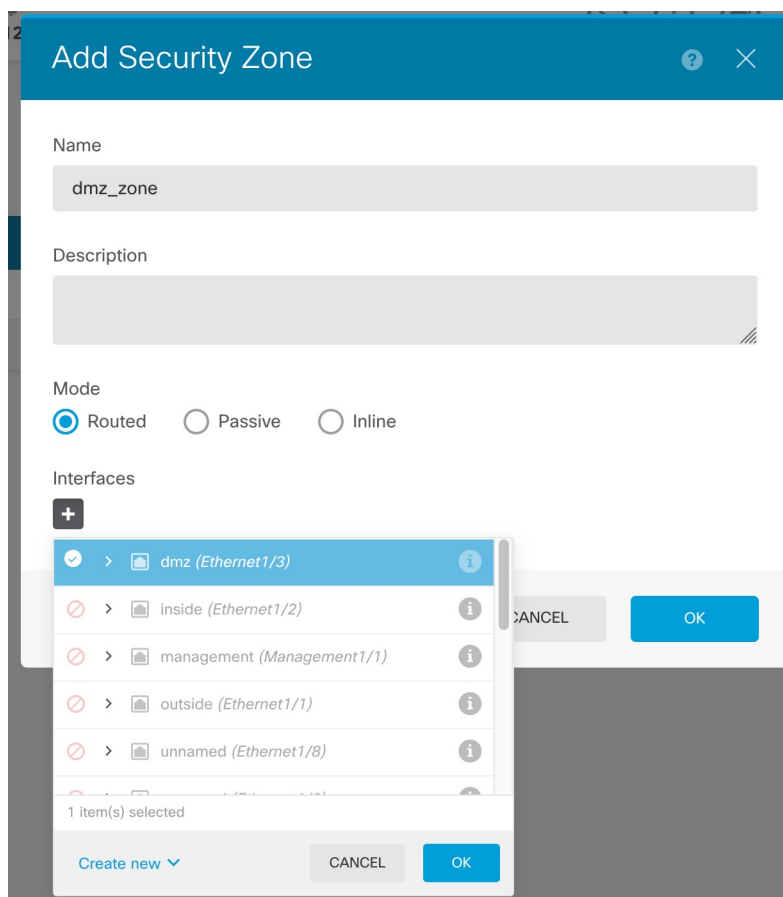
d) **OK(확인)**를 클릭합니다.

- 새로운 인터페이스를 구성한 경우 **Objects(개체)**를 선택한 다음 **Security Zones(보안 영역)**를 선택합니다.

필요에 따라 새 영역을 편집하거나 생성하고 영역에 인터페이스를 할당합니다. 각 인터페이스는 정책을 구성하는 영역에 속해야 합니다.

다음 예에서는 새 **dmz_zone**을 생성한 다음 여기에 **dmz** 인터페이스를 할당합니다.

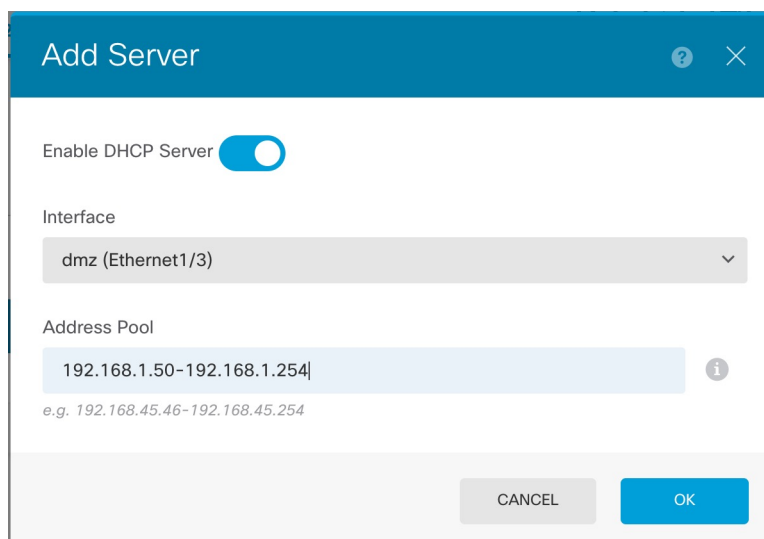
17:



3. 내부 클라이언트가 DHCP를 사용해 디바이스에서 IP 주소를 가져오도록 하려면 **Device(디바이스) > System Settings(시스템 설정) > DHCP Server(DHCP 서버)**을 선택하고 **DHCP Servers(DHCP 서버)** 탭을 선택합니다.

내부 인터페이스에 대해 구성된 DHCP 서버가 이미 있습니다.

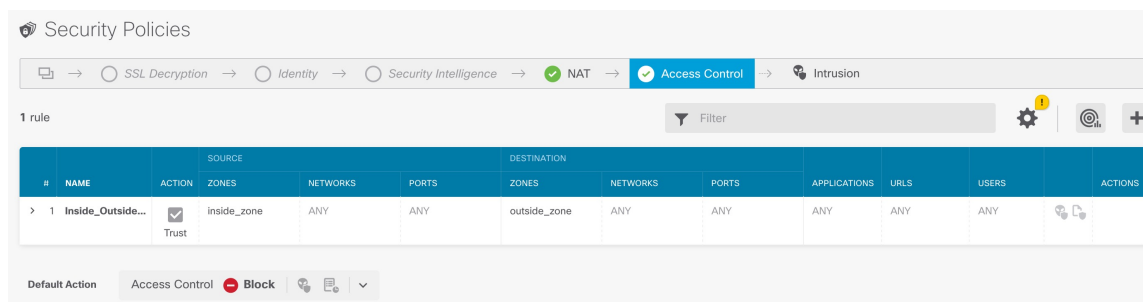
18: DHCP



4. **Policies(정책)**를 선택하고 네트워크의 보안 정책을 구성합니다.

디바이스 설정 마법사 신뢰 규칙을 사용하여 **inside_zone**과 **outside_zone** 간의 트래픽 플로우를 활성화합니다. 신뢰 규칙은 침입 정책을 적용하지 않습니다. 침입을 사용하려면 규칙에 허용 작업을 지정합니다. 정책은 외부 인터페이스로 이동할 때 모든 인터페이스에 대한 인터페이스 **PAT**도 포함합니다.

19:



그러나 서로 다른 영역에 인터페이스가 있는 경우에는 해당 영역에서 들어오고 나가는 트래픽을 허용하는 액세스 제어 규칙이 필요합니다.

또한, 다른 정책을 구성하여 추가 서비스를 제공할 수 있으며 **NAT** 및 액세스 규칙을 조정하여 조직에 필요한 결과를 얻을 수 있습니다. 툴바에서 정책 유형을 클릭하여 다음 정책을 구성할 수 있습니다.

- **SSL Decryption(SSL 암호 해독)** — 침입, 악성코드 등에 대한 암호화된 연결(예: **HTTPS**)을 검사하려는 경우, 연결을 암호 해독해야 합니다. **SSL** 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 **ID** 정책을 사용하여 지정된 소스 **IP** 주소와 연결된 사용자를 확인합니다.
- **Security Intelligence(보안 인텔리전스)** — (**IPS** 라이선스 필요) 보안 인텔리전스 정책을 사용하여 블랙리스트에 추가된 **IP** 주소 또는 **URL**를 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 블랙리스트에 추가함으로써 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. **Cisco**는 알려진 유해 주소 및 **URL**에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 블랙리스트가 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 블랙리스트에서 항목을 추가하거나 제거하기 위해 정책을 편집할 필요가 없습니다.
- **NAT(Network Address Translation)** - **NAT** 정책을 사용하여 내부 **IP** 주소를 외부에서 라우팅 가능한 주소로 변환합니다.
- **Access Control(액세스 제어)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, **IP** 주소, 프로토콜, 포트, 애플리케이션, **URL**, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 **URL** 필터링을 구현할 수 있습니다.
- **Intrusion(침입)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다.

다음 예에는 액세스 제어 정책에서 **inside_zone** 및 **dmz_zone** 간의 트래픽을 허용하는 방법이 나와 있습니다. 이 예에서는 **Logging(로깅)**(**At End of Connection(연결 종료 시)**이 선택된 경우)을 제외하고는 다른 어떤 탭에도 옵션이 설정되어 있지 않습니다.

20:

The screenshot shows the 'Add Access Rule' configuration interface. At the top, there's a header bar with the title 'Add Access Rule' and a close button. Below the header, there's a table with columns: Order, Title, and Action. The first row shows Order '2', Title 'inside-dmz', and Action 'Allow'. Below this table, there are tabs for 'Source/Destination', 'Applications', 'URLs', 'Users', 'Intrusion Policy', 'File policy', and 'Logging'. The 'Source/Destination' tab is selected. Under this tab, there are two main sections: 'SOURCE' and 'DESTINATION'. Each section has a table with columns: Zones, Networks, Ports, and SGT Groups. In the 'SOURCE' section, 'inside_zone' is selected for Zones, and 'ANY' is selected for Networks, Ports, and SGT Groups. In the 'DESTINATION' section, 'dmz_zone' is selected for Zones, and 'ANY' is selected for Networks, Ports, and SGT Groups.

5. **Device**(디바이스)를 선택한 다음 **Updates**(업데이트) 그룹에서 **View Configuration**(구성 보기)를 클릭하고 시스템 데이터베이스에 대한 업데이트 일정을 구성합니다.

침입 정책을 사용하는 경우 규칙 및 VDB 데이터베이스에 대한 정기 업데이트를 설정합니다. 보안 인텔리전스 피드를 사용하는 경우 피드의 업데이트 일정을 설정합니다. 모든 보안 정책의 일치 기준으로 지리적 위치를 사용하는 경우 해당 데이터베이스에 대한 업데이트 일정을 설정합니다.

6. 메뉴에서 **Deploy**(구축) 버튼을 클릭한 다음 **Deploy Now**(지금 구축) 버튼()을 클릭하여 디바이스에 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다.



© 2026 Cisco Systems, Inc. All rights reserved.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.