FDM을 통해 FTD에서 SSH 및 HTTPS에 대한 관리 액세스 구성

목차

소개

이 문서에서는 로컬로 또는 원격으로 관리되는 FTD에서 SSH 및 HTTPS에 대한 관리 액세스 목록을 구성하고 확인하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

- FDM에서 관리하는 버전 7.4.1을 실행하는 Cisco Secure Firewall Threat Defense

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.

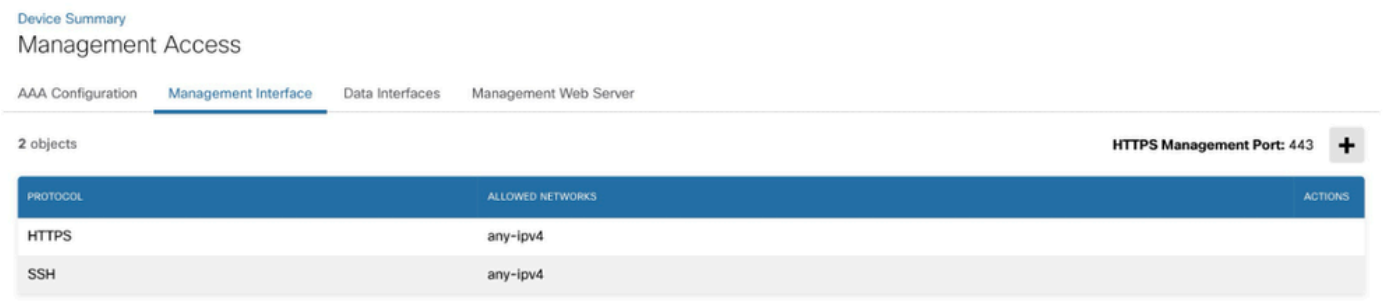
구성

FTD는 FDM을 사용하거나 FMC를 통해 로컬에서 관리할 수 있습니다. 이 문서에서는 FDM 및 CLI를 통한 관리 액세스에 중점을 둡니다. CLI를 사용하면 시나리오 FDM과 FMC를 모두 변경할 수 있습니다.

주의: 세션 잠금을 방지하기 위해 SSH 또는 HTTPS 액세스 목록을 한 번에 하나씩 구성합니다. 먼저 한 프로토콜을 업데이트하고 구축하고 액세스를 확인한 다음 다른 프로토콜을 계속 진행합니다.

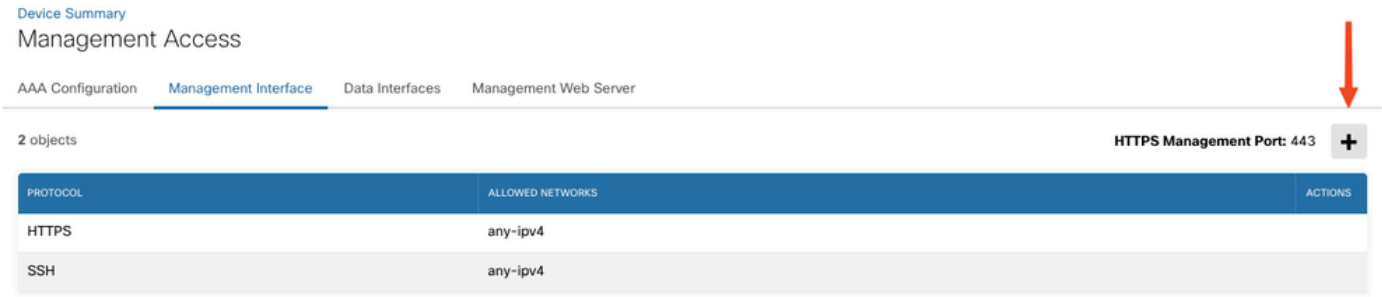
FDM 단계:

1단계: FDM(Firepower 장치 관리자)에 로그인하고 System Settings(시스템 설정) > Management Access(관리 액세스) > Management Interface(관리 인터페이스)로 이동합니다.



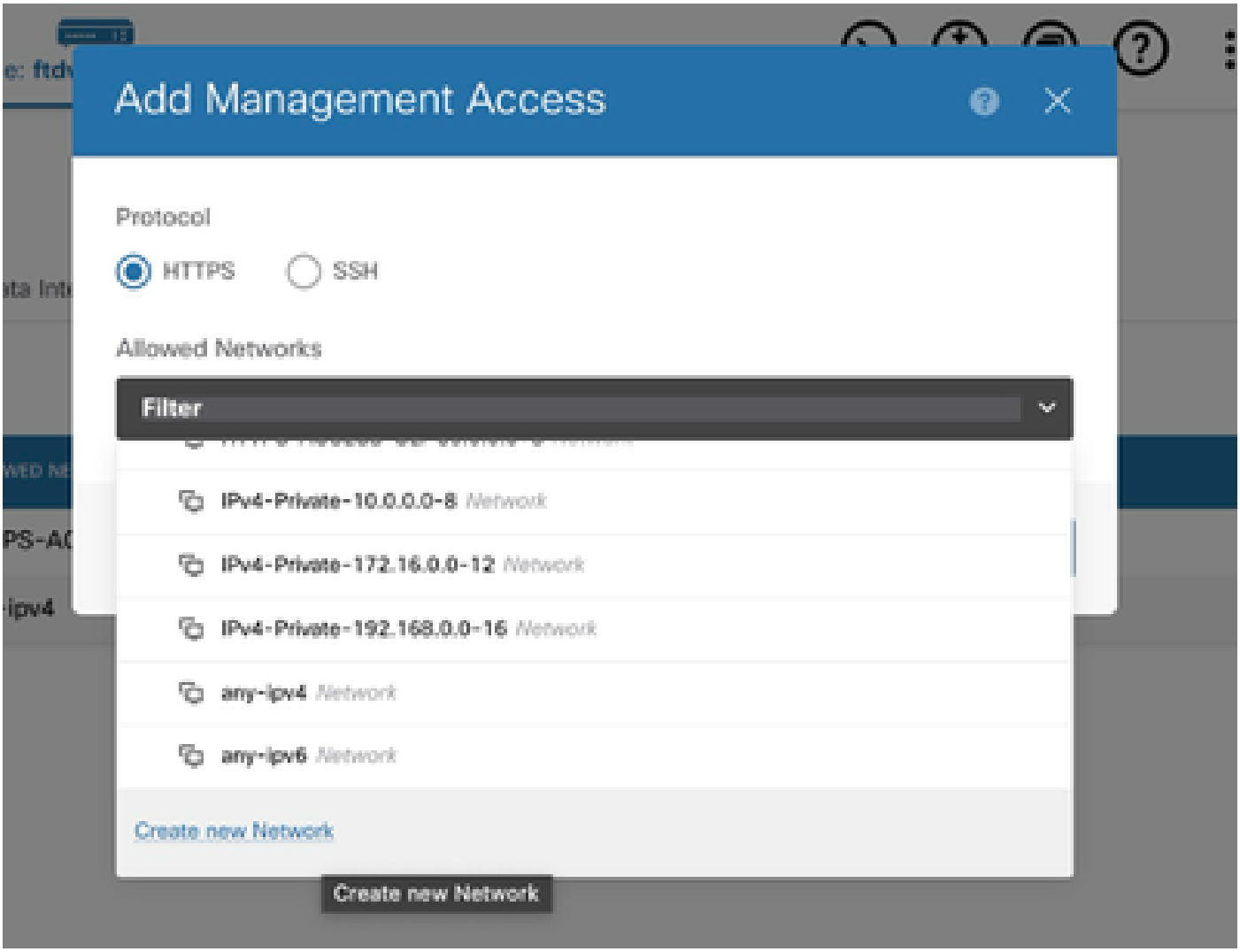
기본적으로 SSH 및 HTTPS용 관리 포트에서는 any-ipv4 액세스가 허용됩니다

2단계: 네트워크 추가를 위한 창을 열려면 + 아이콘을 클릭합니다.



오른쪽 위에서 Add(추가) 버튼을 클릭합니다.

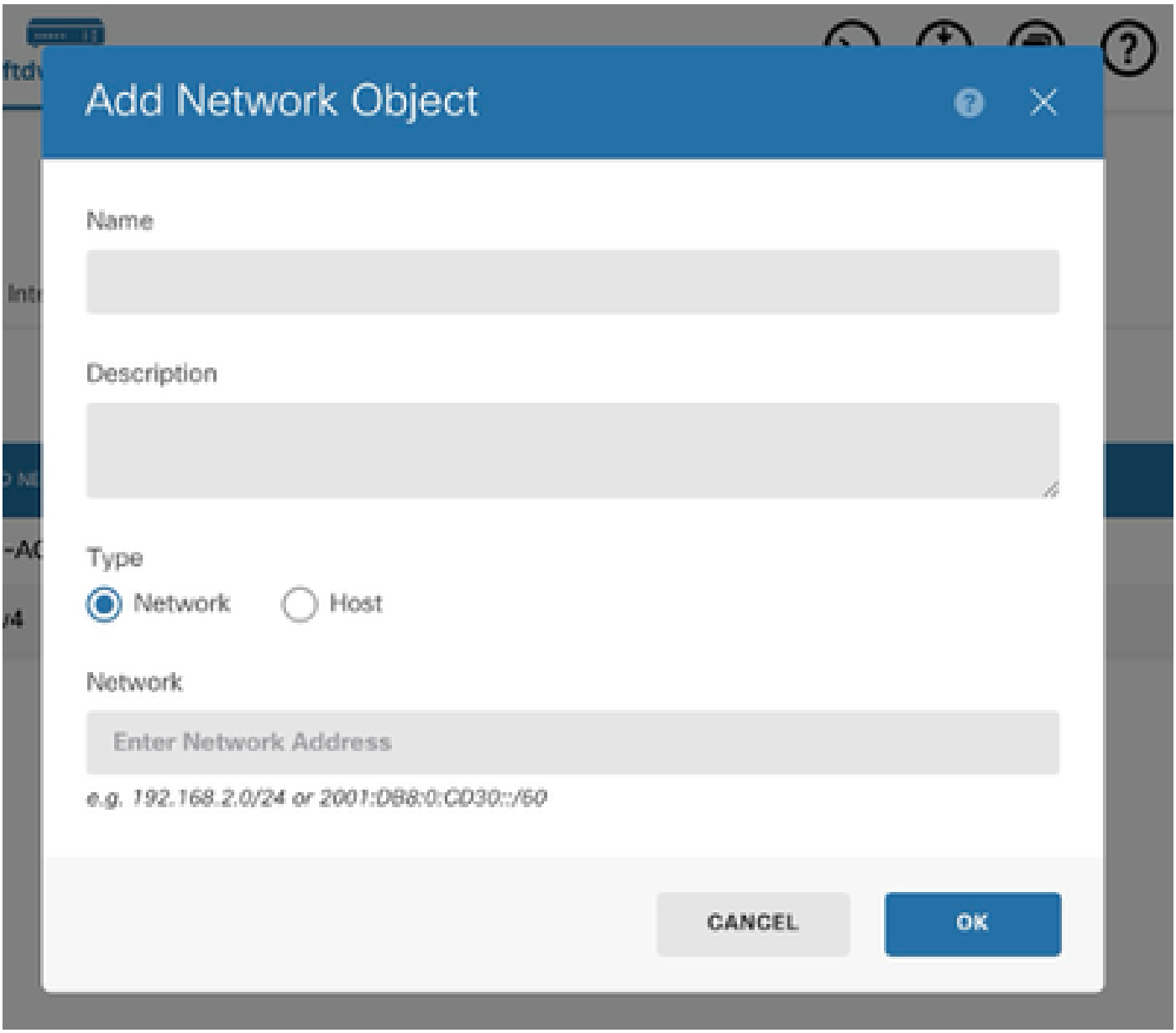
3단계: SSH 또는 HTTPS 액세스를 가질 네트워크 객체를 추가합니다. 새 네트워크를 생성해야 하는 경우 Create new Network(새 네트워크 생성) 옵션을 선택합니다. 관리 액세스에서 네트워크 또는 호스트에 대해 여러 항목을 추가할 수 있습니다.



네트워크를 선택합니다.

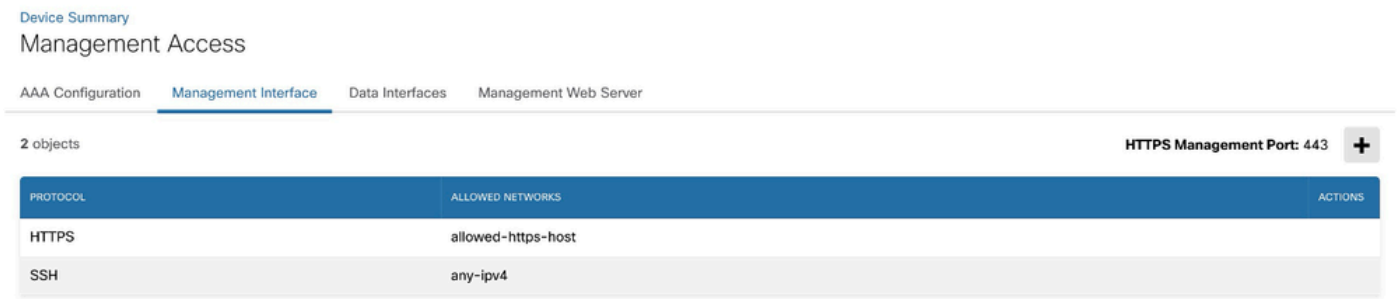
4단계(선택 사항): Create new Network(새 네트워크 생성) 옵션은 Add Network Object(네트워크 개

체 추가) 창을 엽니다.

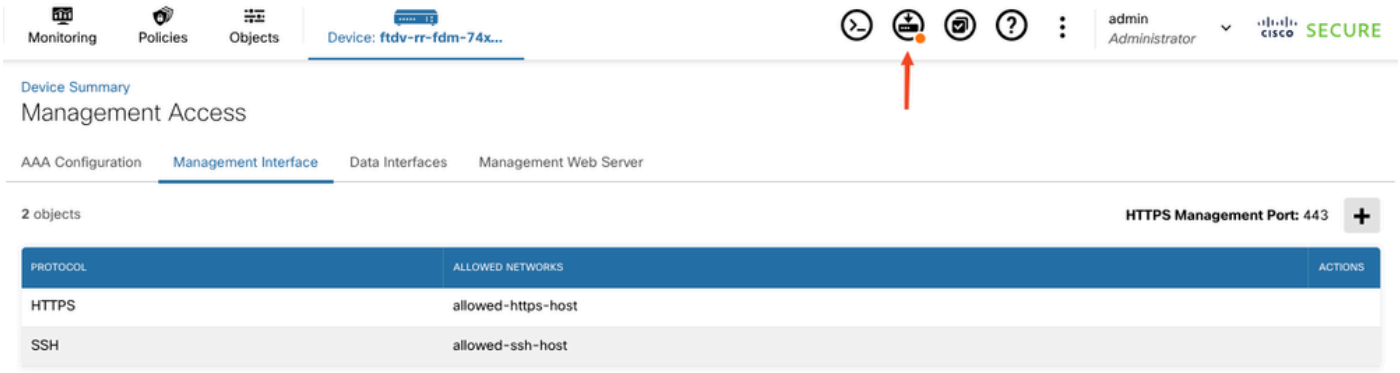


필요에 따라 호스트 네트워크를 생성합니다.

5단계: 변경 사항을 확인하고 배포합니다.

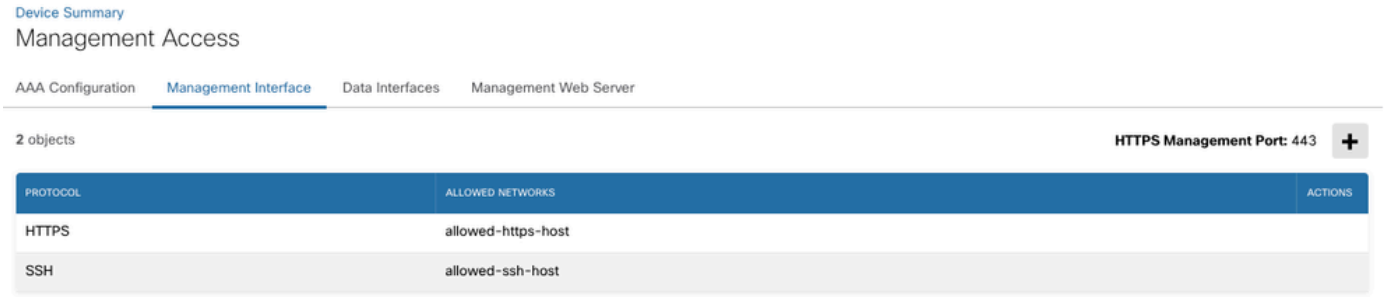


HTTPS 관리 액세스가 변경되고 any-ipv4가 제거됩니다.



FDM에 배포

6단계(선택 사항): HTTPS에 대해 이전에 변경한 사항이 확인되면 SSH에 대해 동일한 작업을 반복합니다.



SSH 및 HTTPS용 네트워크 개체를 추가했습니다.

7단계: 마지막으로 변경 사항을 구축하고 허용된 네트워크 및 호스트에서 FTD에 대한 액세스를 확인합니다.

CLISH 단계:

FDM 또는 FMC를 모두 관리하는 경우 CLI 단계를 사용할 수 있습니다.

지정된 IP 주소 또는 네트워크의 HTTPS 또는 SSH 연결을 허용하도록 디바이스를 구성하려면 theorcommand를configure https-access-listconfigure ssh-access-list사용합니다.

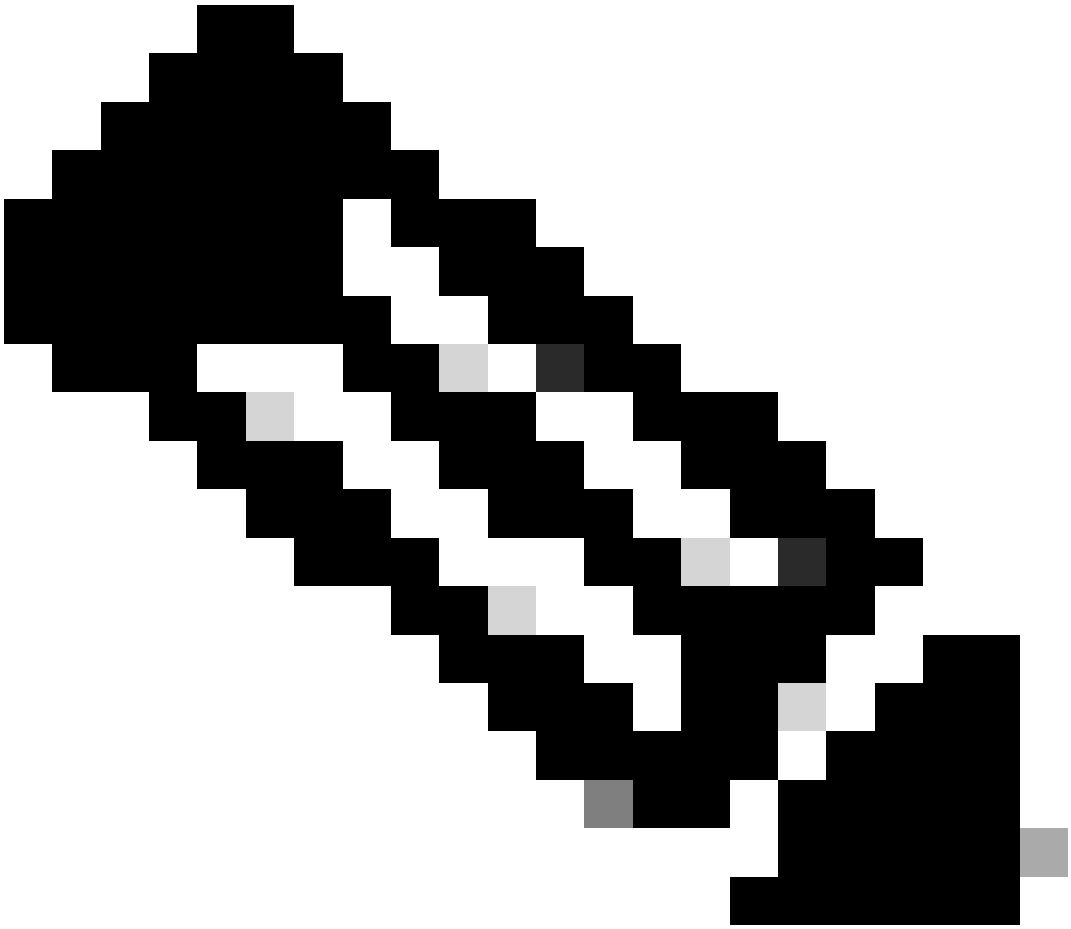
- 지원되는 모든 호스트 또는 네트워크를 단일 명령에 포함해야 합니다. 이 명령에 지정된 주소는 각 액세스 목록의 현재 내용을 덮어씁니다.
- 디바이스가 로컬에서 관리되는 고가용성 그룹의 유닛인 경우, 활성 유닛에서 다음에 구성 업데이트를 배포할 때 변경 내용이 덮어씁니다. 활성 유닛인 경우 배포 중에 변경 내용이 피어에 전파됩니다.

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.

> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
```

```
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```



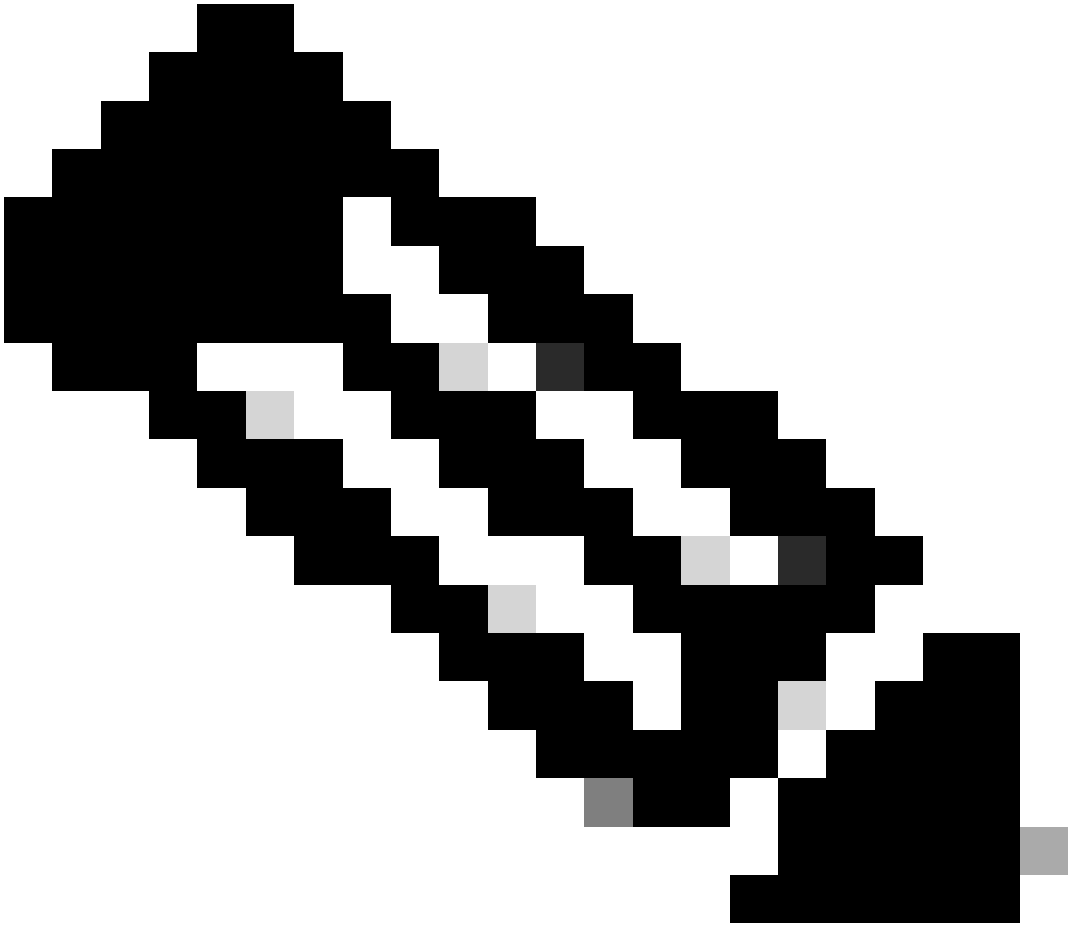
참고: x.x.x.x/x 및 y.y.y.y/y는 CIDR 표기법을 사용하는 ipv4 주소를 나타냅니다.

마찬가지로, SSH 연결의 경우 단일configure ssh-access-list명령 또는 다중 명령이 분리된 명령을 사용합니다.

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:ssh
```



참고: 또는 명령을 사용하여 **configure disable-https-access** HTTPS 또configure disable-ssh-access는 SSH 액세스를 각각 비활성화할 수 있습니다. 이러한 변경 사항이 세션에서 잠길 수 있으므로 이를 숙지해야 합니다.

다음을 확인합니다.

CLISH에서 확인하려면 다음 명령을 사용할 수 있습니다.

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:https
```

참조

Cisco Secure Firewall Threat Defense 명령 참조

firepower 디바이스 관리자용 Cisco Firepower Threat Defense 컨피그레이션 가이드

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.