

보안 방화벽 위협 방어 및 ASA를 위한 컨트롤 플레인 액세스 제어 정책 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[설정](#)

[FMC에서 관리하는 FTD에 대한 컨트롤 플레인 ACL 구성](#)

[FDM에서 관리하는 FTD에 대한 제어 평면 ACL 구성](#)

[CLI를 사용하여 ASA에 대한 컨트롤 플레인 ACL 구성](#)

['shun' 명령을 사용하여 보안 방화벽의 공격을 차단하는 대체 컨피그레이션](#)

[다음을 확인합니다.](#)

[관련 버그](#)

소개

이 문서에서는 Secure Firewall Threat Defense 및 ASA(Adaptive Security Appliance)에 대한 컨트롤 플레인 액세스 규칙을 구성하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(보안 방화벽 위협 방어)
- 보안 방화벽 장치 관리자(FDM)
- FMC(Secure Firewall Management Center)
- 보안 방화벽 ASA
- ACL(Access Control List)
- Flex구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Secure Firewall Threat Defense 버전 7.2.5
- Secure Firewall Manager Center 버전 7.2.5

- Secure Firewall Device Manager 버전 7.2.5
- Secure Firewall ASA 버전 9.18.3

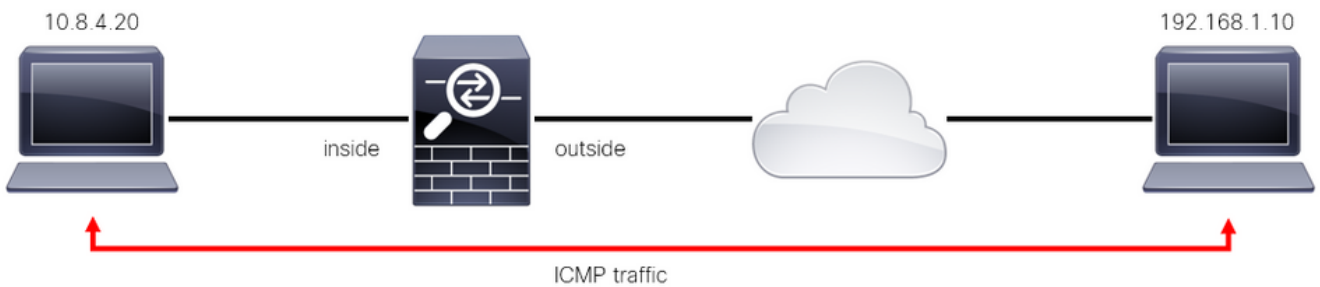
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

일반적으로 트래픽은 방화벽을 통과하고 데이터 인터페이스 간에 라우팅됩니다. 경우에 따라 보안 방화벽으로 '가는' 트래픽을 거부하는 것이 좋습니다. Cisco 보안 방화벽은 컨트롤 플레인 ACL(Access Control List)을 사용하여 'to-the-box' 트래픽을 제한할 수 있습니다. 컨트롤 플레인 ACL이 유용할 수 있는 예를 들면 어떤 피어가 보안 방화벽에 대한 VPN(Site-to-Site 또는 Remote Access VPN) 터널을 설정할 수 있는지 제어하는 것입니다.

보안 방화벽 'through-the-box' 트래픽

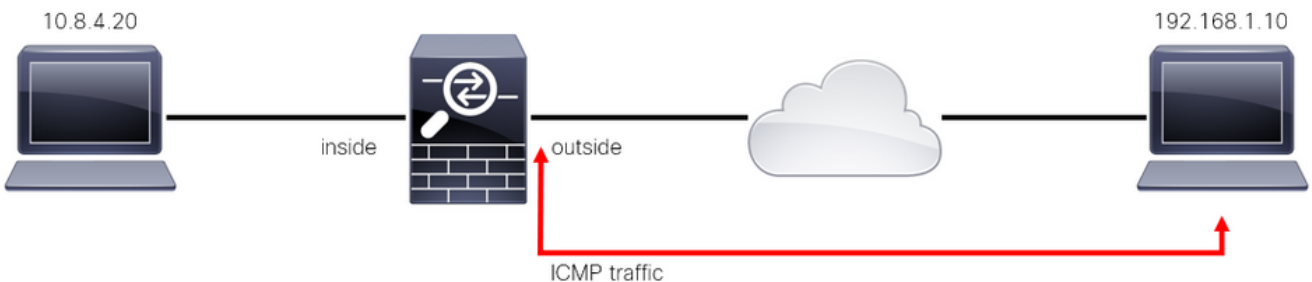
일반적으로 트래픽은 한 인터페이스(인바운드)에서 다른 인터페이스(아웃바운드)로 방화벽을 통과하며, 이를 'through-the-box' 트래픽이라고 하며 ACP(Access Control Policies) 및 사전 필터 규칙 모두에 의해 관리됩니다.



이미지 1. Through-the-box 트래픽 예

보안 방화벽 'to-the-box' 트래픽

트래픽이 FTD 인터페이스(Site-to-Site 또는 Remote Access VPN)로 직접 전달되는 경우가 있습니다. 이를 'to-the-box' 트래픽이라고 하며 해당 특정 인터페이스의 컨트롤 플레인에 의해 관리됩니다.



이미지 2. To-the-box 트래픽 예

컨트롤 플레인 ACL과 관련하여 중요한 고려 사항

- FMC/FTD 버전 7.0부터는 ASA에서 사용되는 것과 동일한 명령 구문을 사용하여 FlexConfig를 사용하여 컨트롤 플레인 ACL을 구성해야 합니다.
- control-plane 키워드가 access-group 컨피그레이션에 추가되어 보안 방화벽 인터페이스에 'to' 트래픽을 적용합니다. 명령에 컨트롤 플레인 단어가 추가되지 않으면 ACL은 보안 방화벽을 '통과'하는 트래픽을 제한합니다.
- 컨트롤 플레인 ACL은 SSH, ICMP 또는 TELNET 인바운드를 보안 방화벽 인터페이스로 제한하지 않습니다. 플랫폼 설정 정책에 따라 처리되며(허용/거부) 우선순위가 더 높습니다.
- 컨트롤 플레인 ACL은 보안 방화벽 자체에서 '대상' 트래픽을 제한하는 반면, FTD에 대한 액세스 제어 정책 또는 ASA에 대한 일반 ACL은 보안 방화벽을 '통과' 트래픽을 제어합니다.
- 일반 ACL과 달리 ACL의 끝에는 암시적 '거부'가 없습니다.
- 이 문서를 만들 때 FTD 지오로케이션 기능을 사용하여 FTD에 대한 액세스를 제한할 수 없습니다.

구성

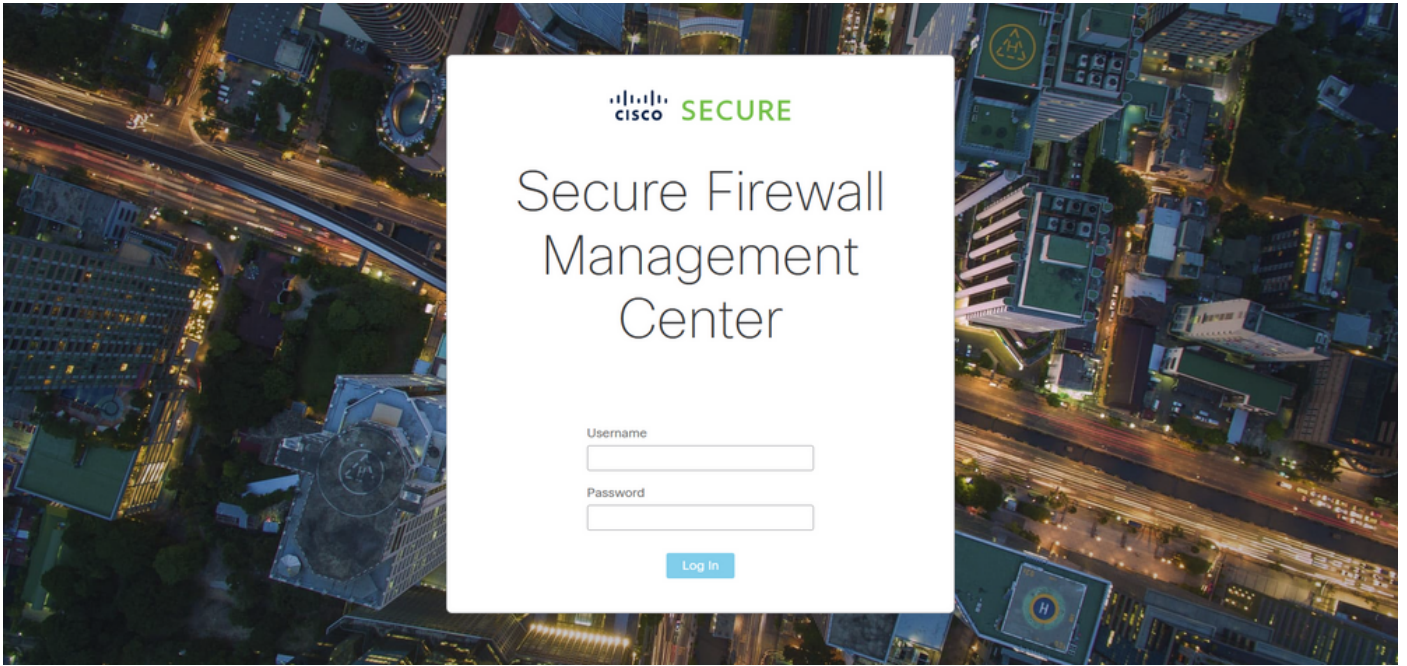
다음 예에서는 특정 국가의 IP 주소 집합이 FTD RAVPN에 로그인을 시도하여 네트워크에 강제로 VPN을 시도합니다. 이러한 VPN 무작위 대입 공격으로부터 FTD를 보호하는 최상의 옵션은 외부 FTD 인터페이스에 대한 이러한 연결을 차단하도록 컨트롤 플레인 ACL을 구성하는 것입니다.

설정

FMC에서 관리하는 FTD에 대한 컨트롤 플레인 ACL 구성

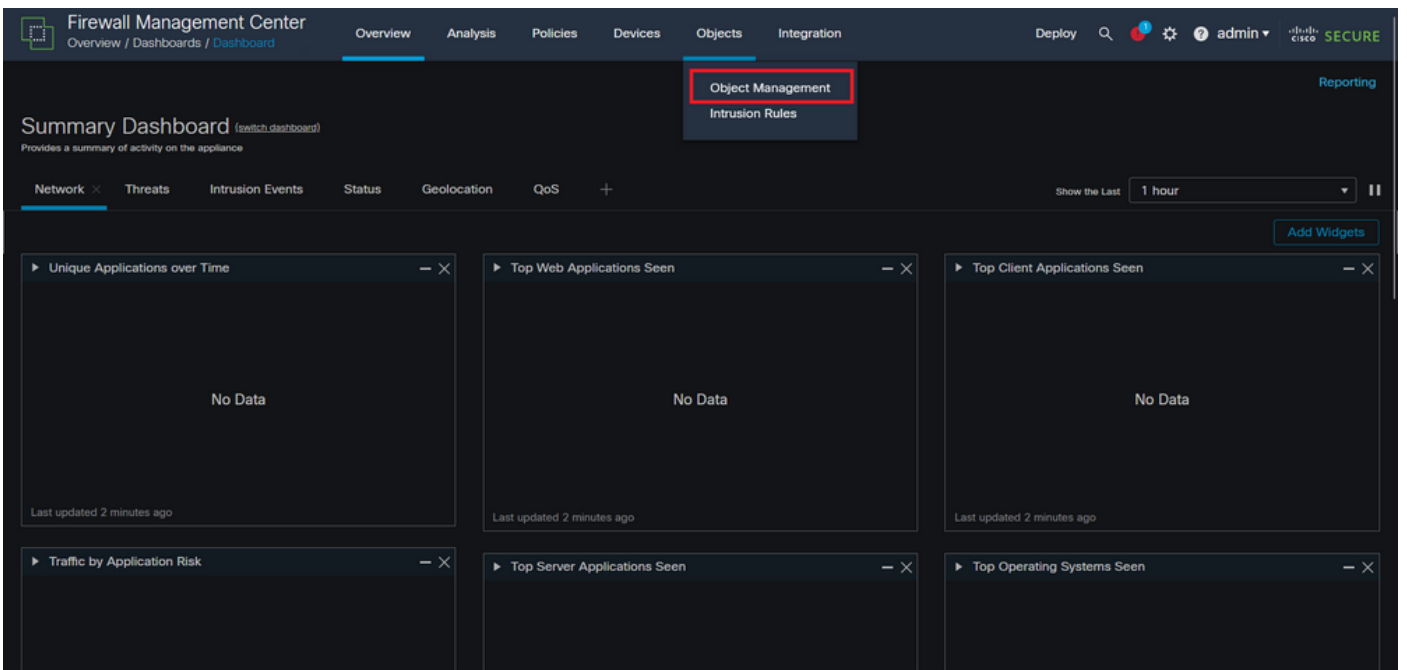
이는 외부 FTD 인터페이스에 대한 수신 VPN 무작위 대입 공격을 차단하기 위해 제어 평면 ACL을 구성하기 위해 FMC에서 수행해야 하는 절차입니다.

1단계. HTTPS를 통해 FMC 그래픽 사용자 인터페이스(GUI)를 열고 자격 증명으로 로그인합니다.



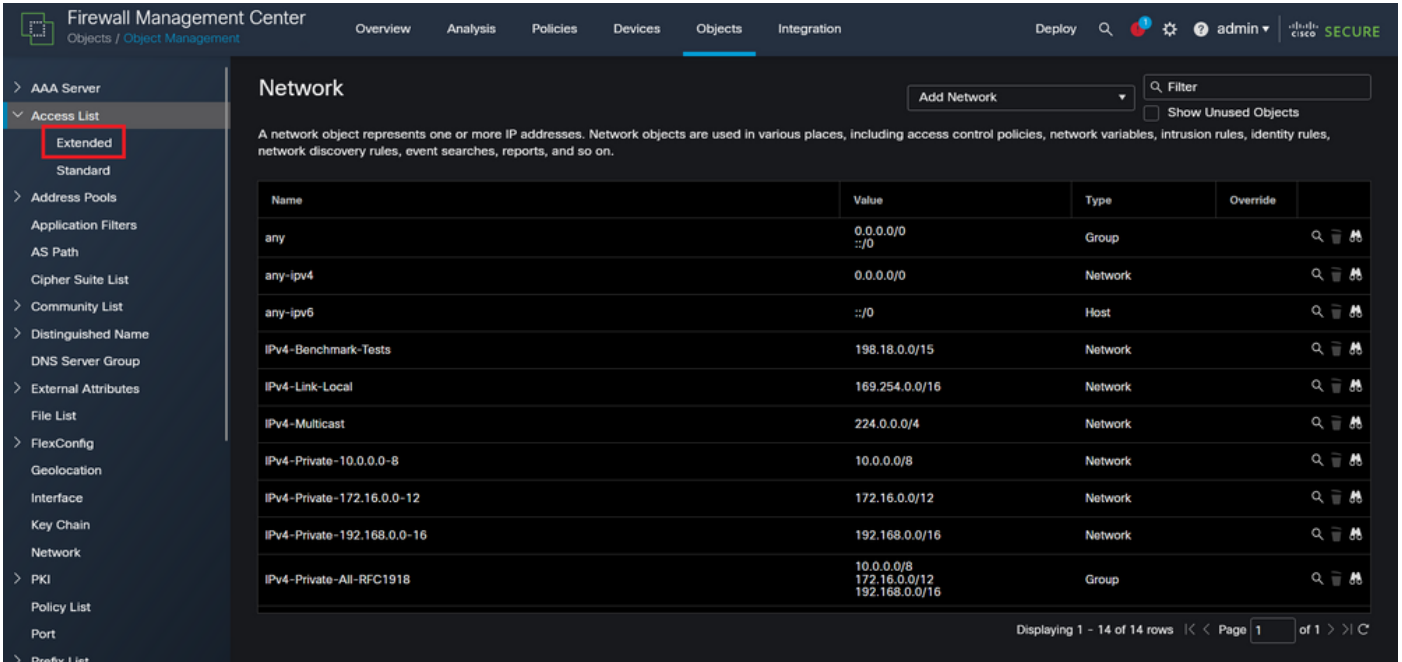
이미지 3. FMC 로그인 페이지

2단계. 확장 ACL을 생성해야 합니다. 이를 위해 Objects > Object Management로 이동합니다.



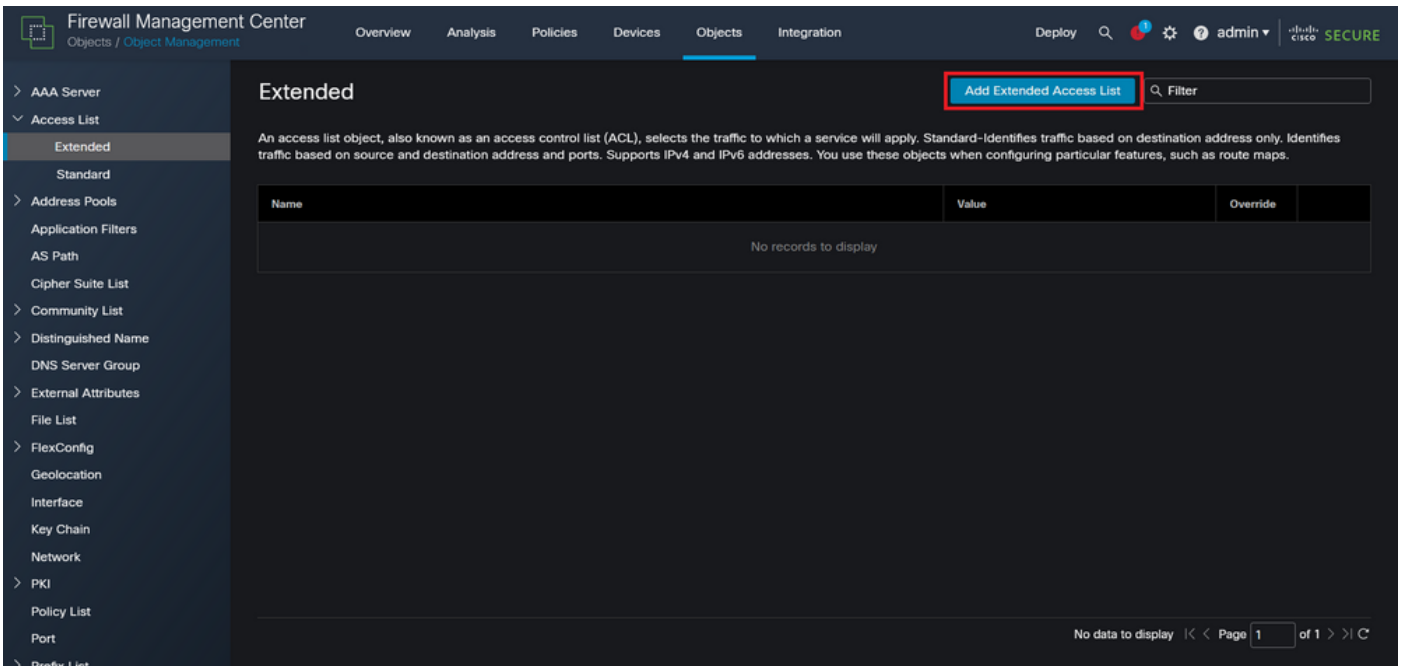
이미지 4. 객체 관리

2.1단계. 왼쪽 패널에서 Access List(액세스 목록) > Extended(확장)로 이동하여 확장 ACL을 생성합니다.



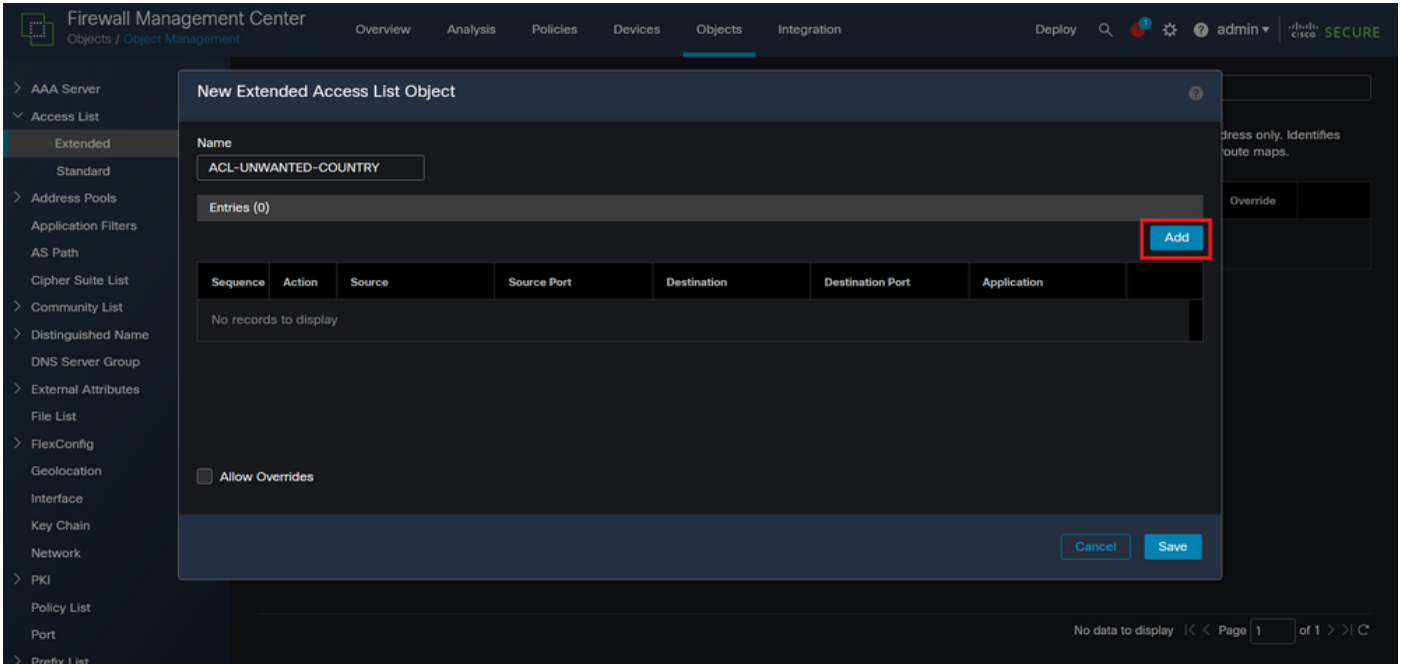
이미지 5. 확장 ACL 메뉴

2.2단계. 그런 다음 Add Extended Access List를 선택합니다.



이미지 6. 확장 ACL 추가

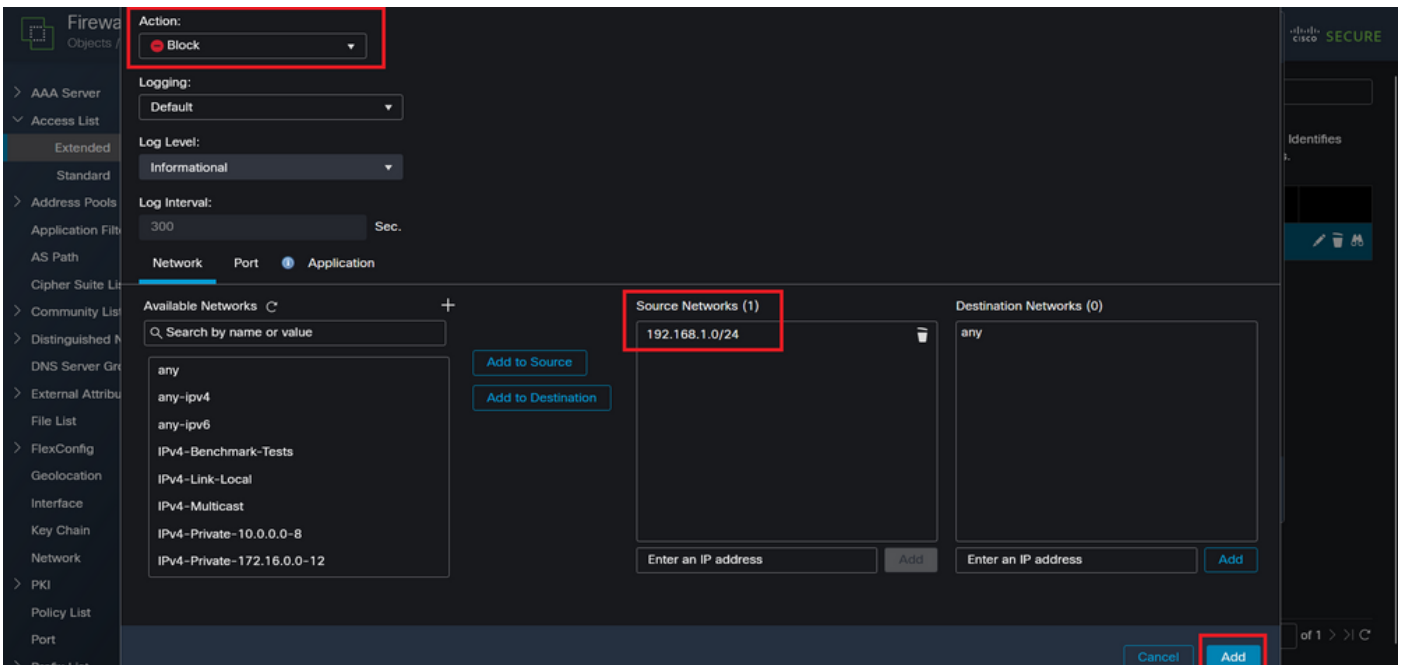
2.3단계. 확장 ACL의 이름을 입력한 다음 Add(추가) 버튼을 클릭하여 ACE(액세스 제어 항목)를 생성합니다.



이미지 7. 확장 ACL 항목

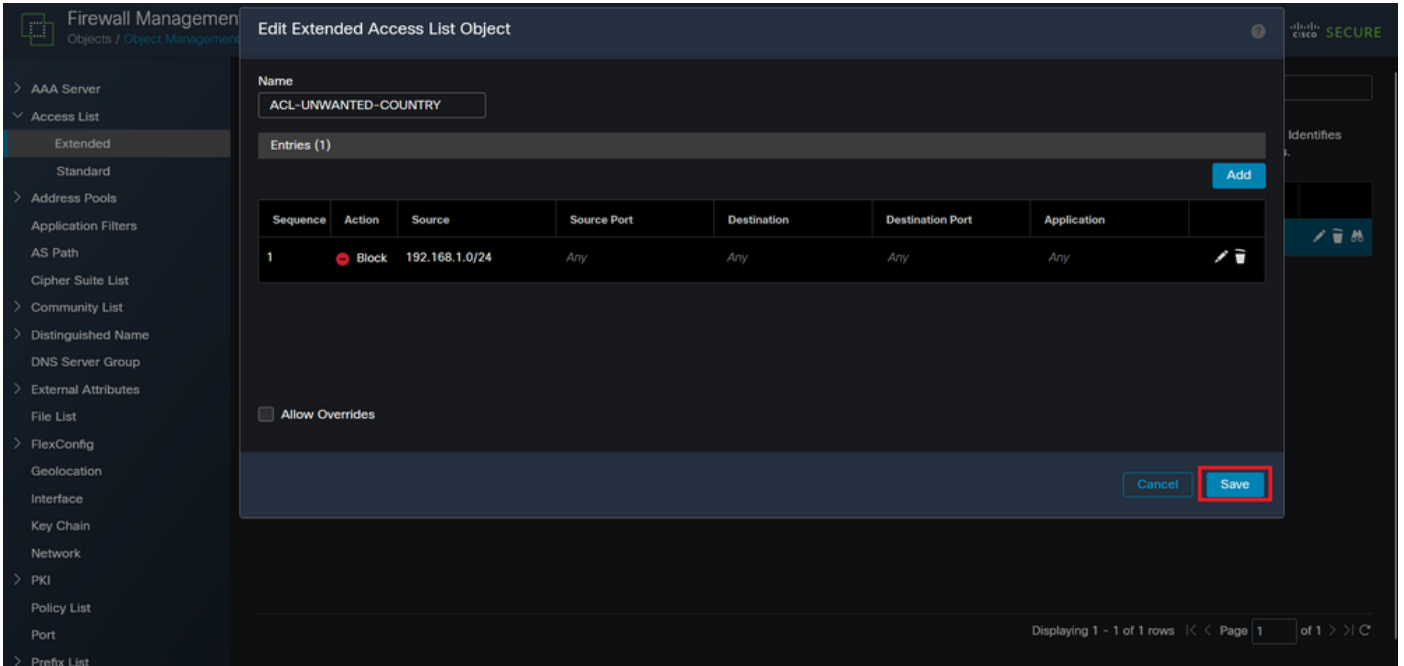
2.4단계. ACE 작업을 Block(차단)으로 변경한 다음 FTD에 거부해야 하는 트래픽과 일치하도록 소스 네트워크를 추가하고, 대상 네트워크를 Any(임의)로 유지한 다음 Add(추가) 버튼을 클릭하여 ACE 항목을 완료합니다.

- 이 예에서 구성된 ACE 항목은 192.168.1.0/24 서브넷에서 오는 VPN 무차별 대입 공격을 차단합니다.



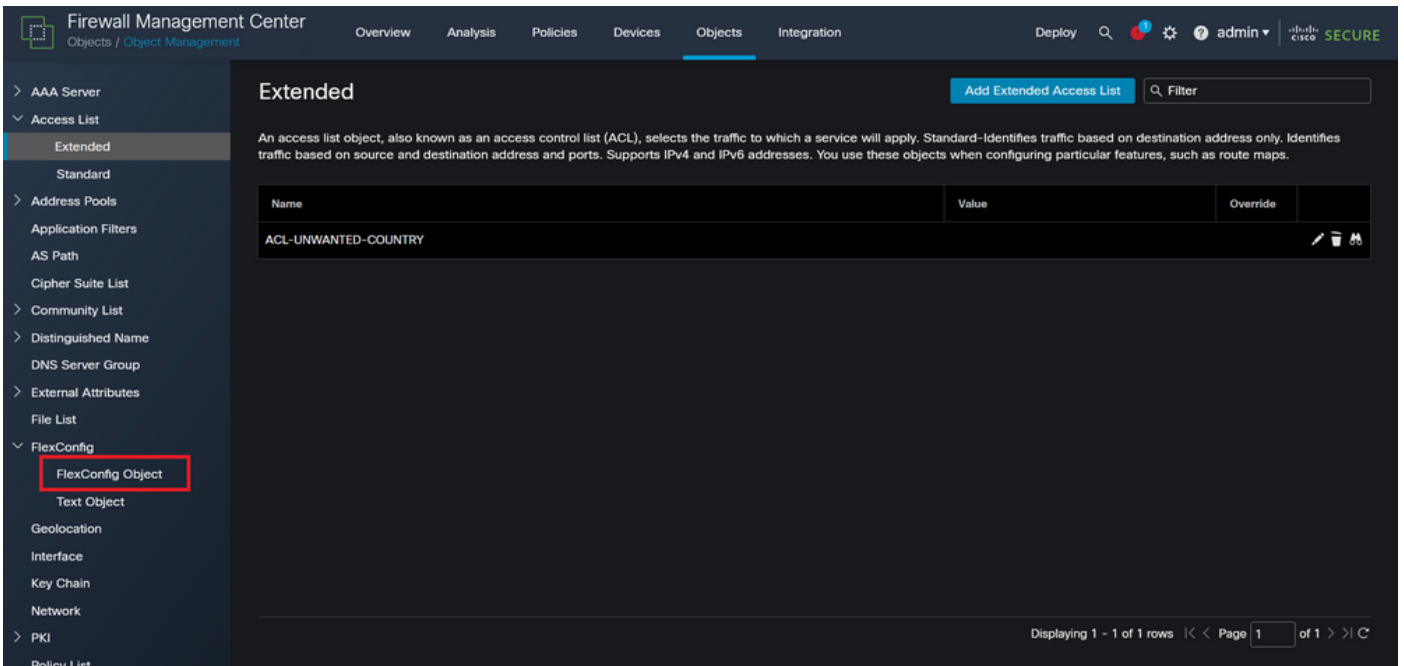
이미지 8. 거부된 네트워크

2.5단계. ACE 항목을 더 추가해야 하는 경우 Add(추가) 버튼을 다시 클릭하고 2.4단계를 반복합니다. 그런 다음 Save(저장) 버튼을 클릭하여 ACL 컨피그레이션을 완료합니다.



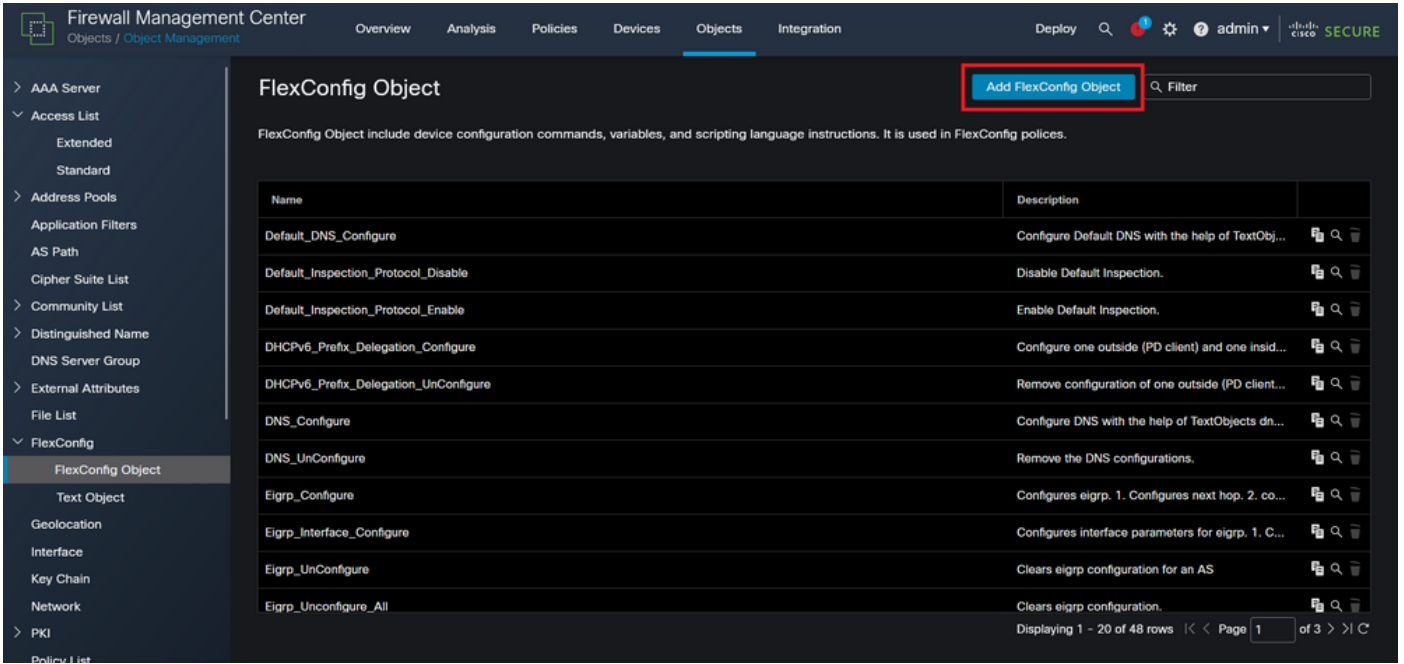
이미지 9. 완료된 확장 ACL 항목

3단계. 그런 다음 제어 평면 ACL을 외부 FTD 인터페이스에 적용하도록 Flex-Config 객체를 구성해야 합니다. 이를 위해 왼쪽 패널로 이동하여 FlexConfig > FlexConfig Object 옵션을 선택합니다.



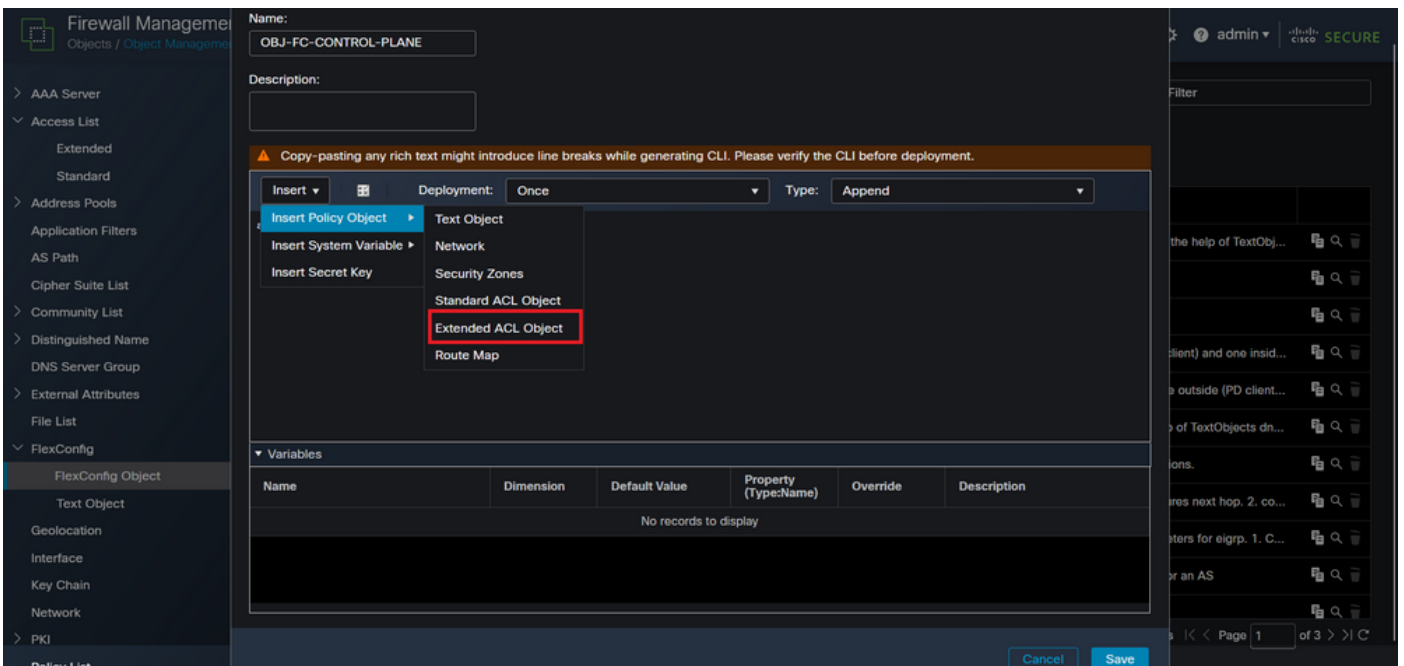
이미지 10. FlexConfig 개체 메뉴

3.1단계. Add FlexConfig Object(FlexConfig 개체 추가)를 클릭합니다.



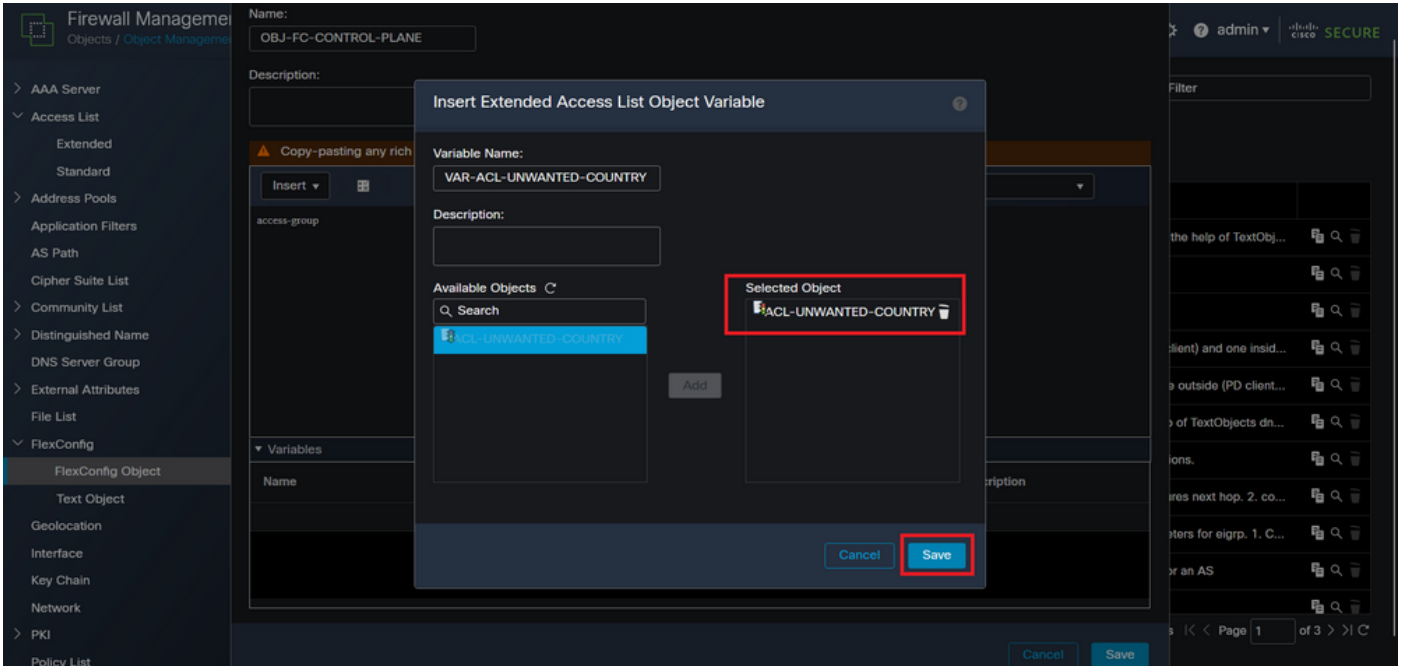
이미지 11. Flexconfig 개체 추가

3.2단계. FlexConfig 개체의 이름을 추가한 다음 ACL 정책 개체를 삽입합니다. 이를 위해 Insert > Insert Policy Object > Extended ACL Object를 선택합니다.



이미지 12. FlexConfig 개체 변수

3.3단계. ACL 객체 변수의 이름을 추가한 다음 2.3단계에서 생성한 확장 ACL을 선택하고 Save(저장) 버튼을 클릭합니다.



이미지 13. FlexConfig 개체 변수 ACL 할당

3.4단계. 그런 다음 제어 평면 ACL을 다음과 같이 외부 인터페이스에 대한 인바운드로 구성합니다.

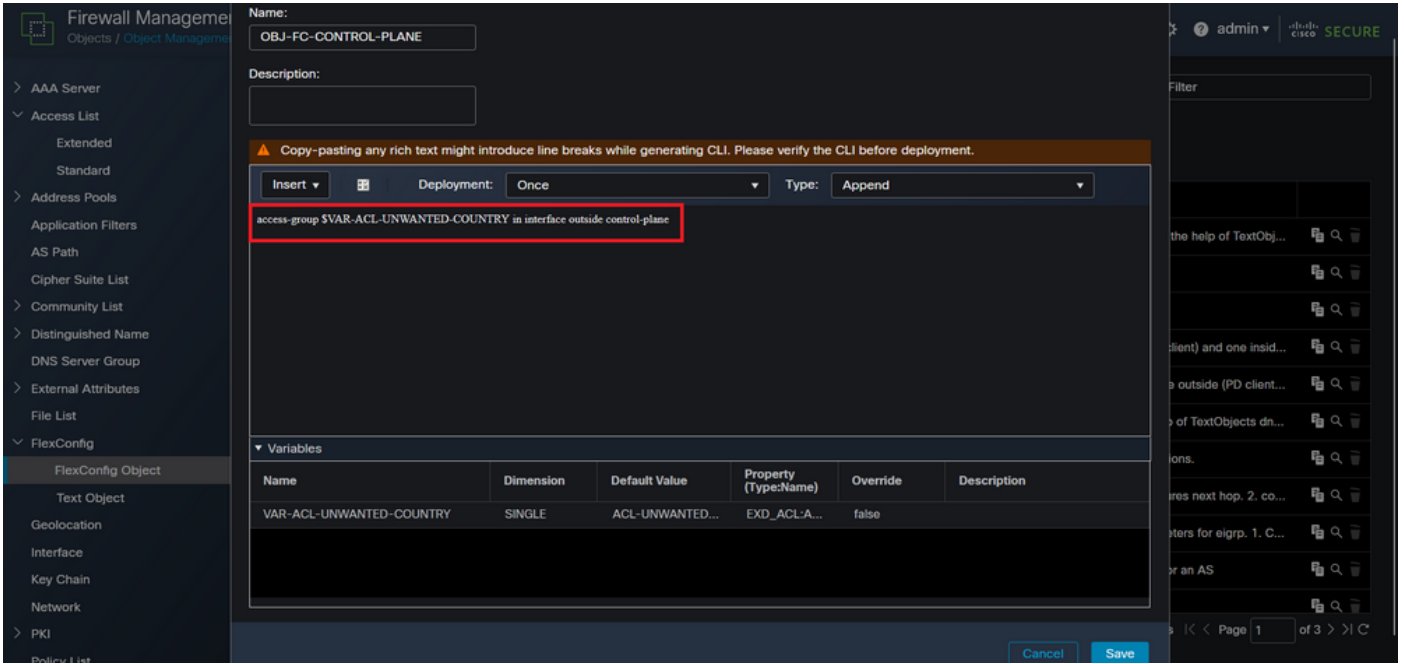
명령줄 구문:

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

이는 다음 명령 예제로 변환되며, 위의 2.3단계 'VAR-ACL-UNWANTED-COUNTRY'에서 생성된 ACL 변수를 다음과 같이 사용합니다.

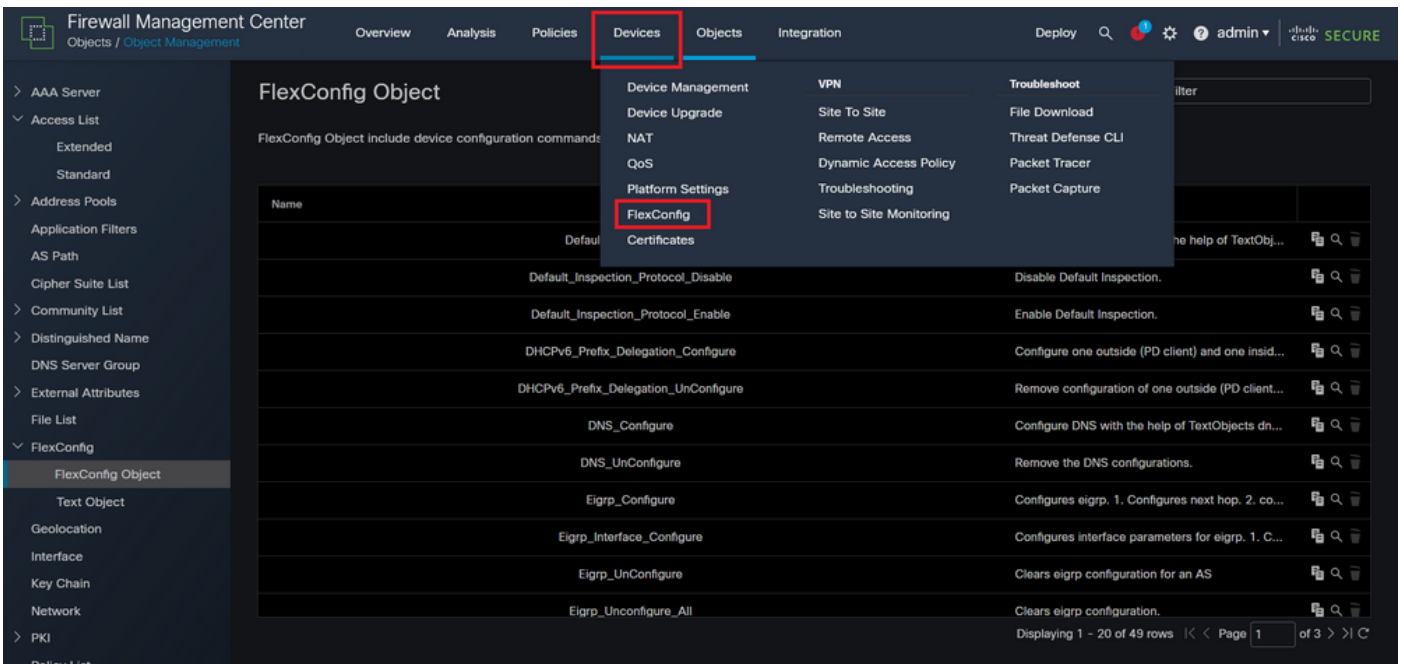
```
access-group $VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane
```

이렇게 하려면 FlexConfig 개체 창에 구성해야 합니다. 그런 다음 [저장] 단추를 선택하여 FlexConfig 개체를 완료합니다.



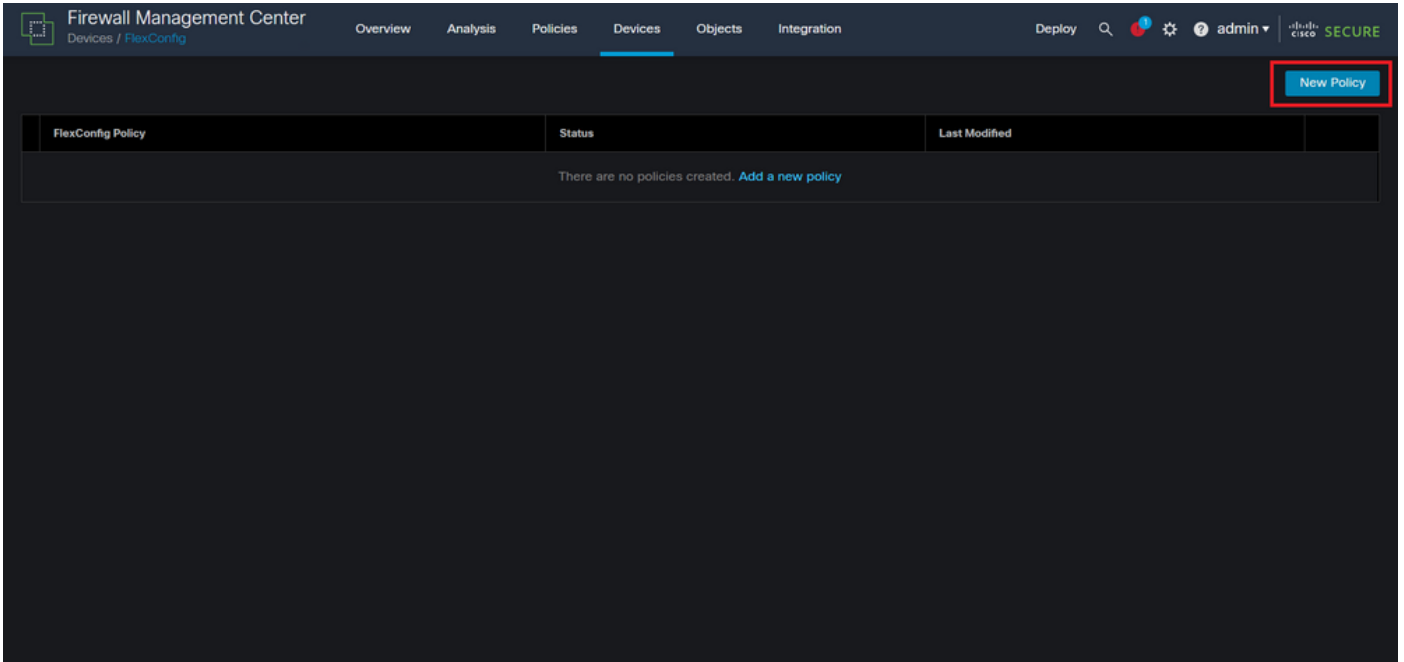
이미지 14. Flexconfig 개체 완료 명령줄

4단계. FlexConfig 개체 컨피그레이션을 FTD에 적용해야 합니다. 이를 위해 Devices(디바이스) > FlexConfig(FlexConfig)로 이동합니다.



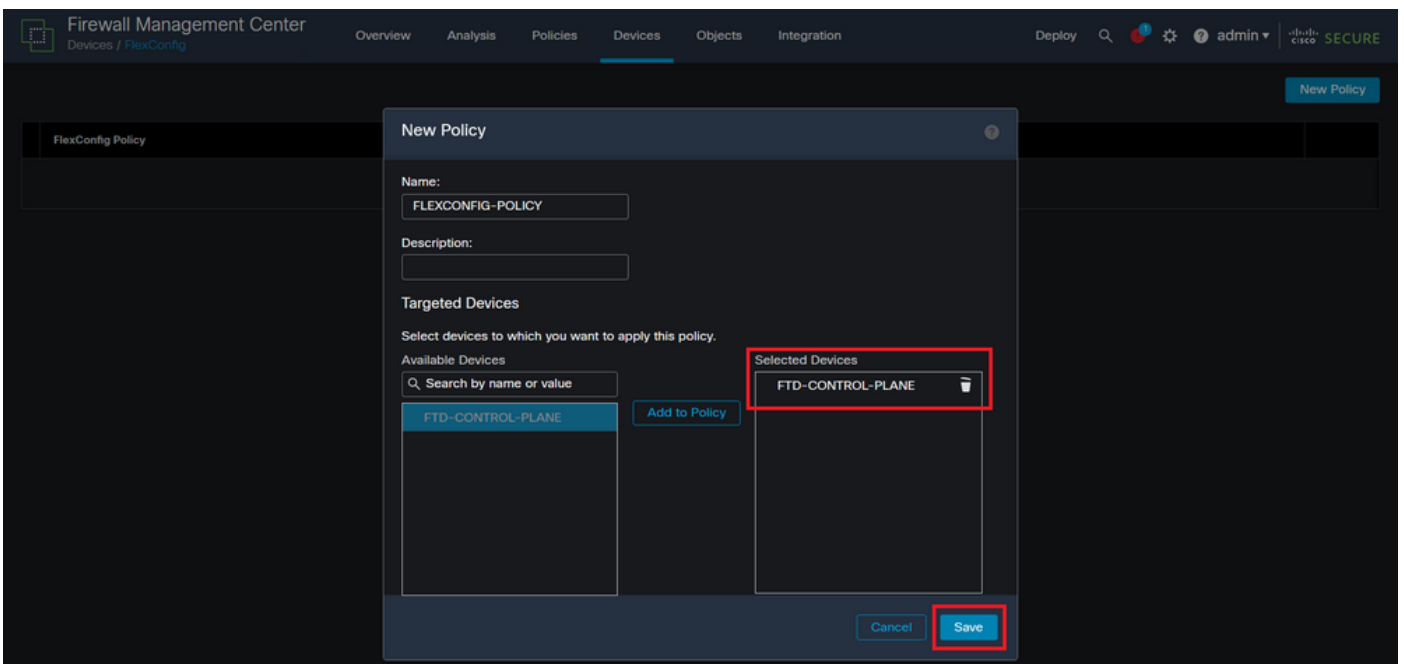
이미지 15. FlexConfig 정책 메뉴

4.1단계. 그런 다음 FTD에 대해 생성된 FlexConfig가 없는 경우 New Policy(새 정책)를 클릭하거나 기존 FlexConfig 정책을 수정합니다.



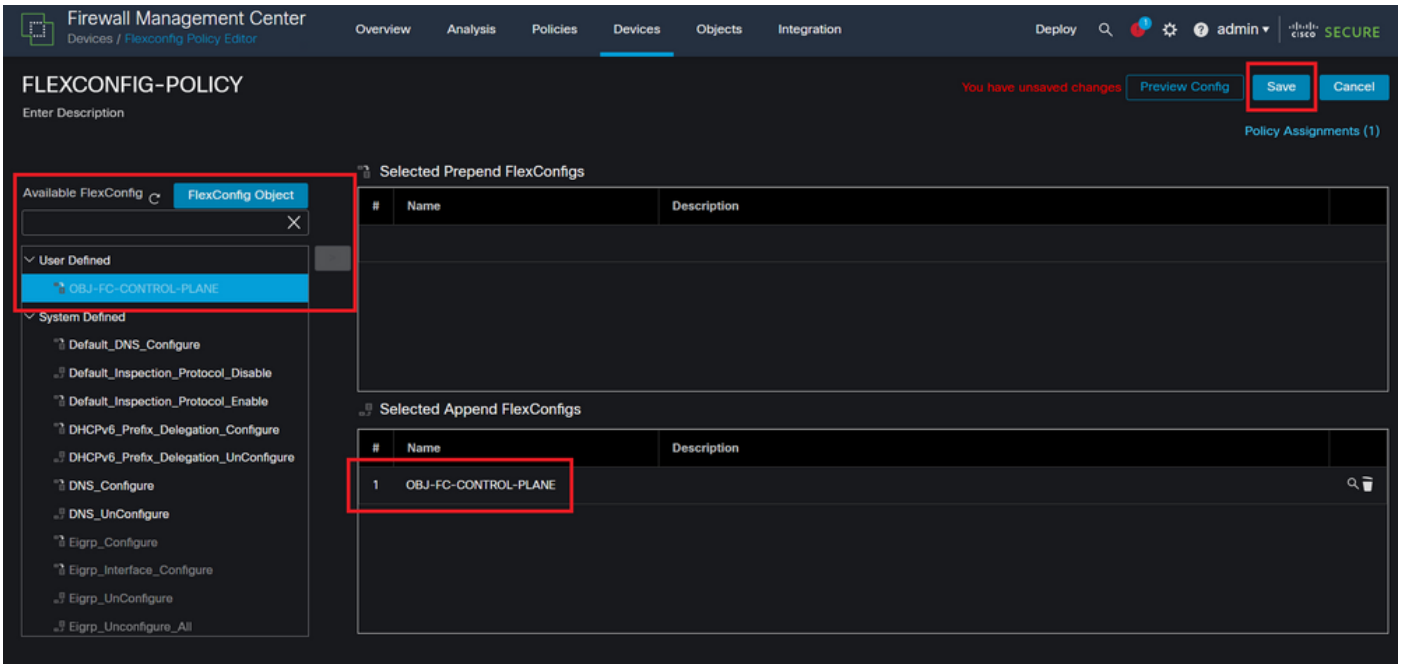
이미지 16. FlexConfig 정책 생성

4.2단계. 새 FlexConfig 정책의 이름을 추가하고 생성된 컨트롤 플레인 ACL을 적용할 FTD를 선택합니다.



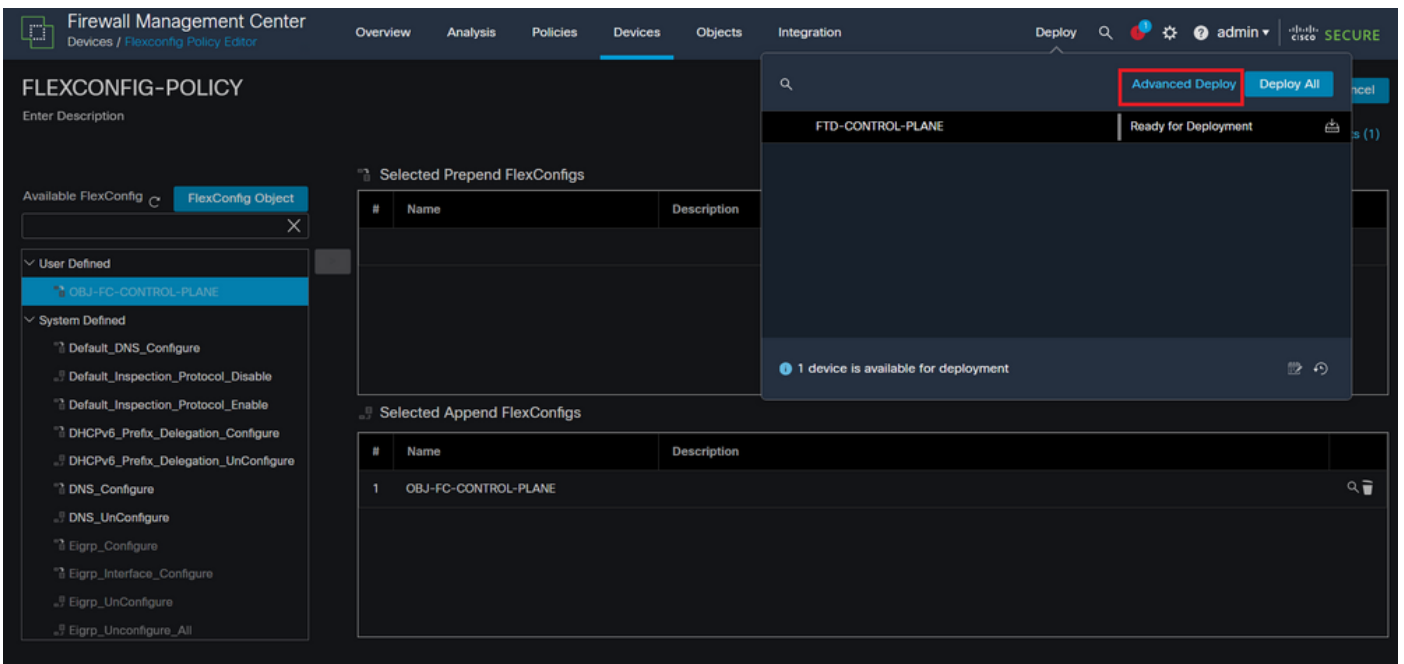
이미지 17. FlexConfig 정책 디바이스 할당

4.3단계. 왼쪽 패널에서 위 3.2단계에서 생성한 FlexConfig 객체를 검색한 다음 창 가운데에 있는 오른쪽 화살표를 클릭하여 FlexConfig 정책에 추가하고 Save(저장) 버튼을 클릭합니다.



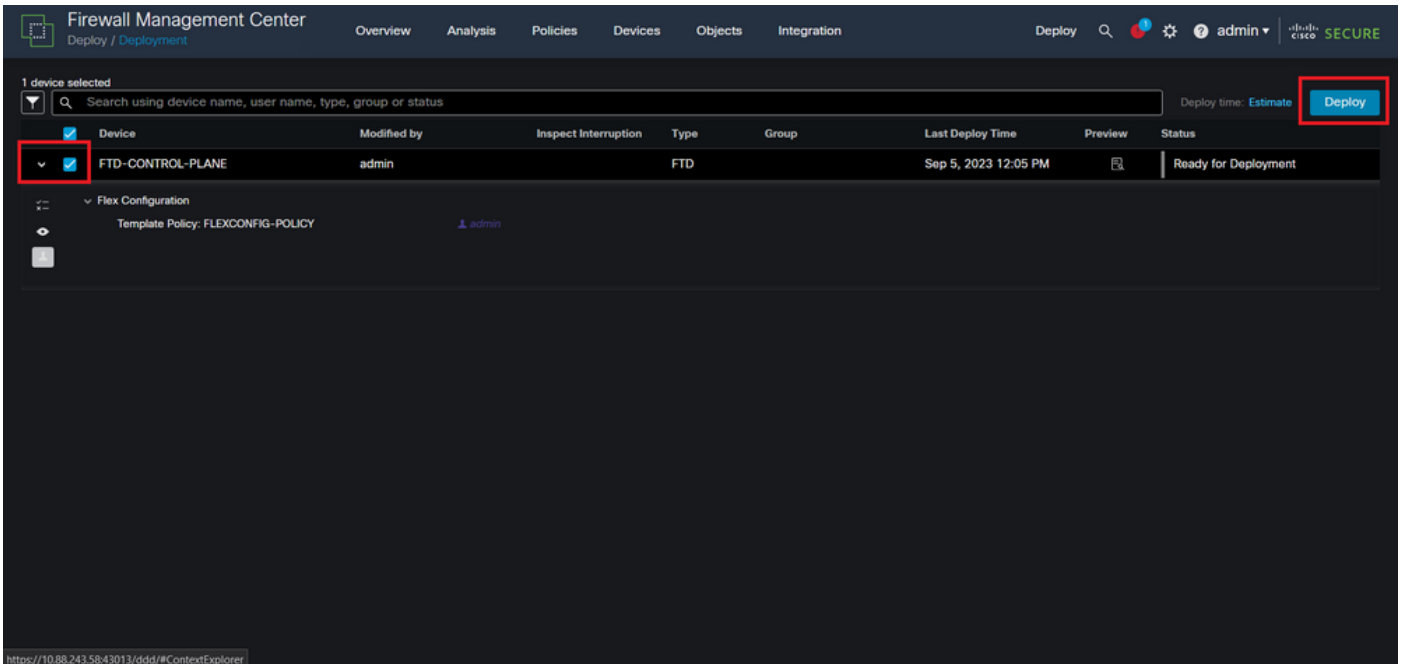
이미지 18. FlexConfig 정책 개체 할당

5단계. 계속해서 FTD에 컨피그레이션 변경 사항을 구축합니다. 이렇게 하려면 Deploy(구축) > Advanced Deploy(고급 구축)로 이동합니다.



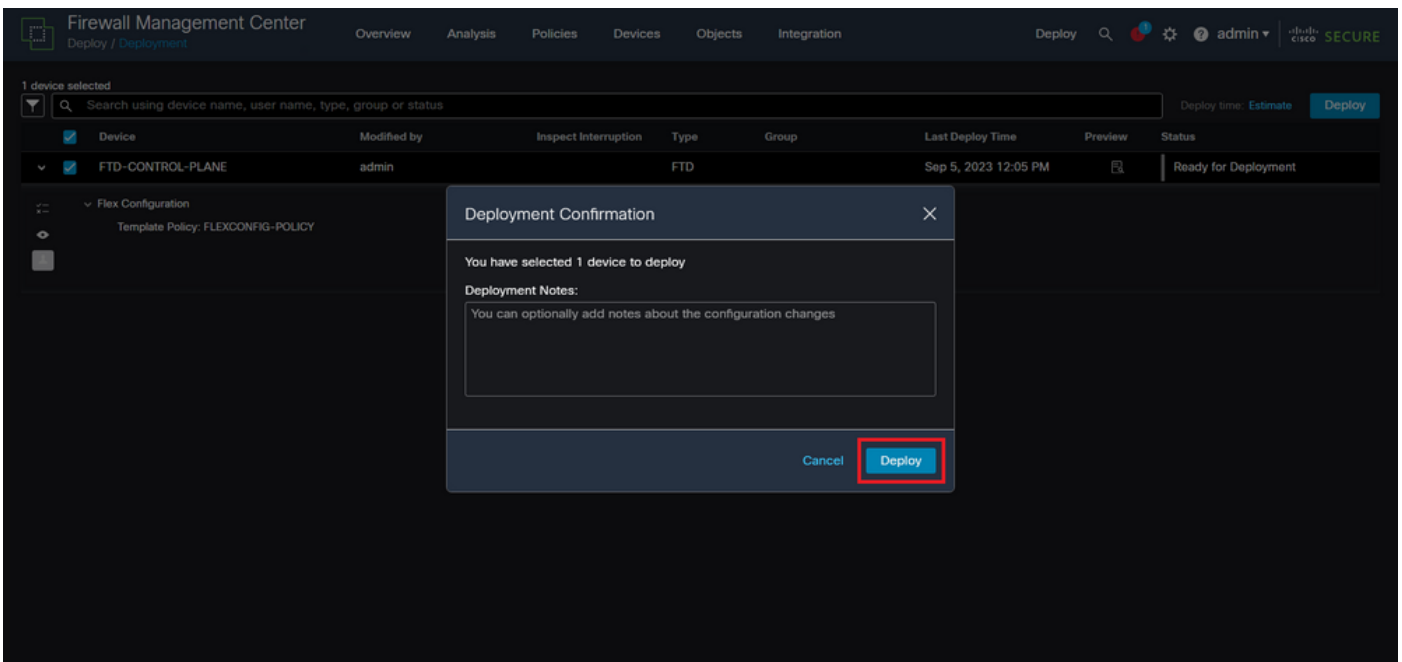
이미지 19. FTD 고급 구축

5.1단계. 그런 다음 FlexConfig 정책을 적용할 FTD를 선택합니다. 모든 것이 올바르게 Deploy(구축)를 클릭합니다.



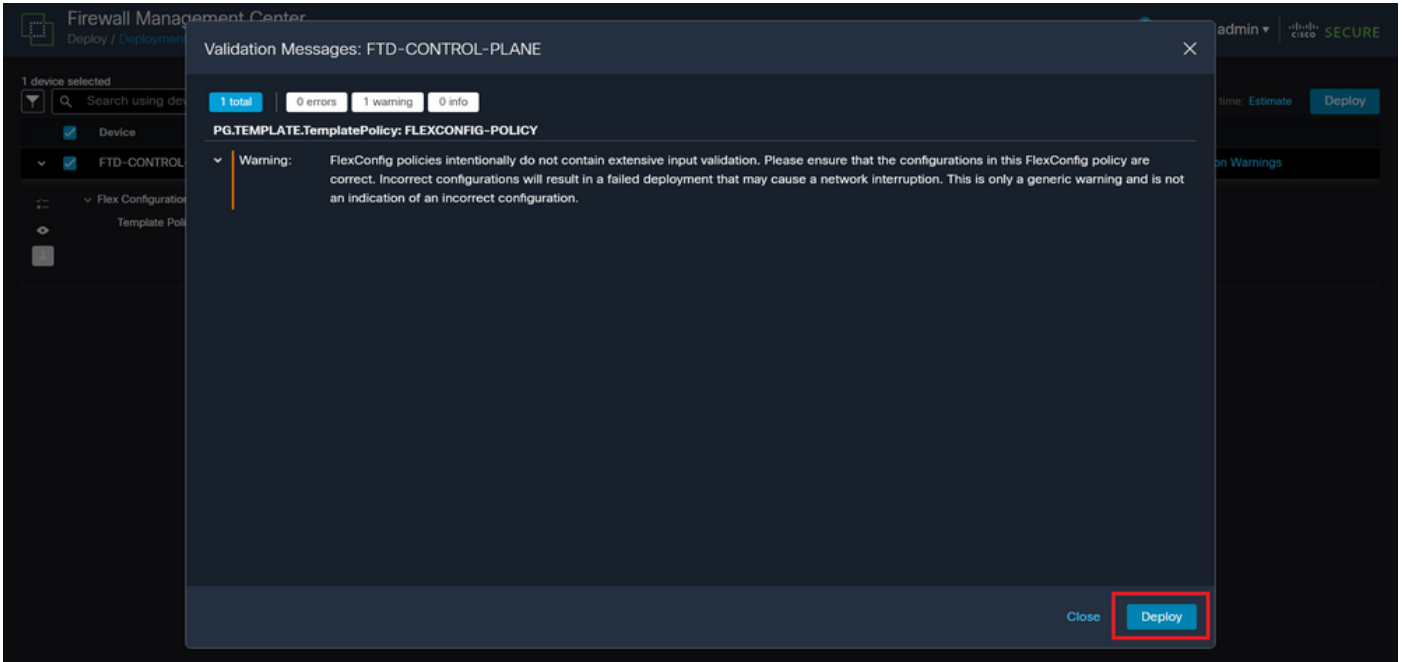
이미지 20. FTD 구축 검증

5.2단계. 그런 다음 Deployment Confirmation(구축 확인) 창이 팝업되고, 설명을 추가하여 구축을 추적하고 Deploy(구축)를 진행합니다.



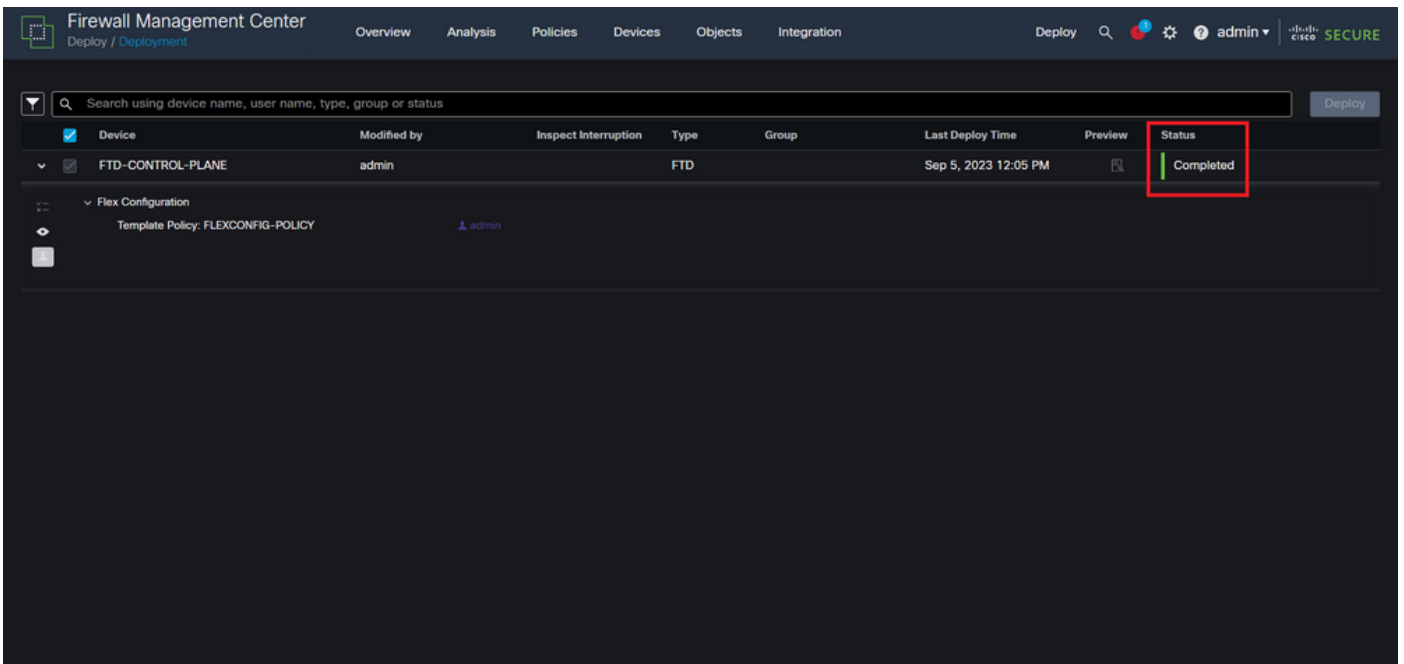
이미지 21. FTD 구축 의견

5.3단계. FlexConfig 변경 내용을 배포할 때 경고 메시지가 나타날 수 있습니다. 정책 컨피그레이션이 올바른지 완전히 확인한 경우에만 Deploy(구축)를 클릭합니다.



이미지 22. FTD 배포 Flexconfig 경고

5.4단계. FTD에 대한 정책 구축이 성공적인지 확인합니다.



이미지 23. FTD 구축 성공

6단계. FTD에 대한 새 컨트롤 플레인 ACL을 생성하거나 현재 사용 중인 기존 ACL을 편집한 경우, 컨피그레이션 변경 사항이 이미 설정된 FTD 연결에 적용되지 않으므로 FTD에 대한 활성 연결 시도를 수동으로 지워야 합니다. 이를 위해 FTD의 CLI에 연결하고 다음과 같이 활성 연결을 지웁니다.

특정 호스트 IP 주소에 대한 활성 연결을 지우려면


```
> clear conn address 192.168.1.10 all
```

전체 서브넷 네트워크에 대한 활성 연결을 지우려면

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

IP 주소 범위에 대한 활성 연결을 지우려면

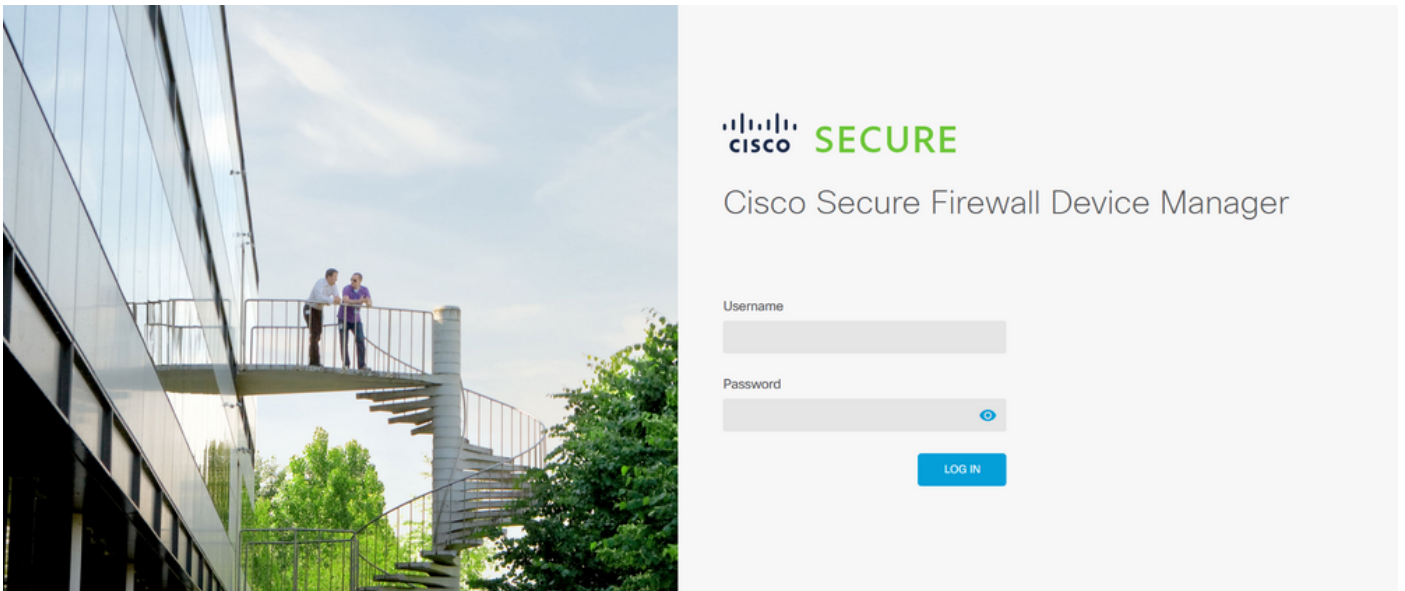
```
> clear conn address 192.168.1.1-192.168.1.10 all
```

 참고: 주로 VPN 무작위 대입 공격의 특성에서 지속적인 연결 시도가 급증할 때 활성 VPN 무작위 대입 연결 시도를 보안 방화벽에 강제로 지우려면 clear conn address 명령의 끝에 'all' 키워드를 사용하는 것이 좋습니다.

FDM에서 관리하는 FTD에 대한 제어 평면 ACL 구성

이는 외부 FTD 인터페이스에 대한 수신 VPN 무작위 대입 공격을 차단하기 위해 제어 평면 ACL을 구성하기 위해 FDM에서 수행해야 하는 절차입니다.

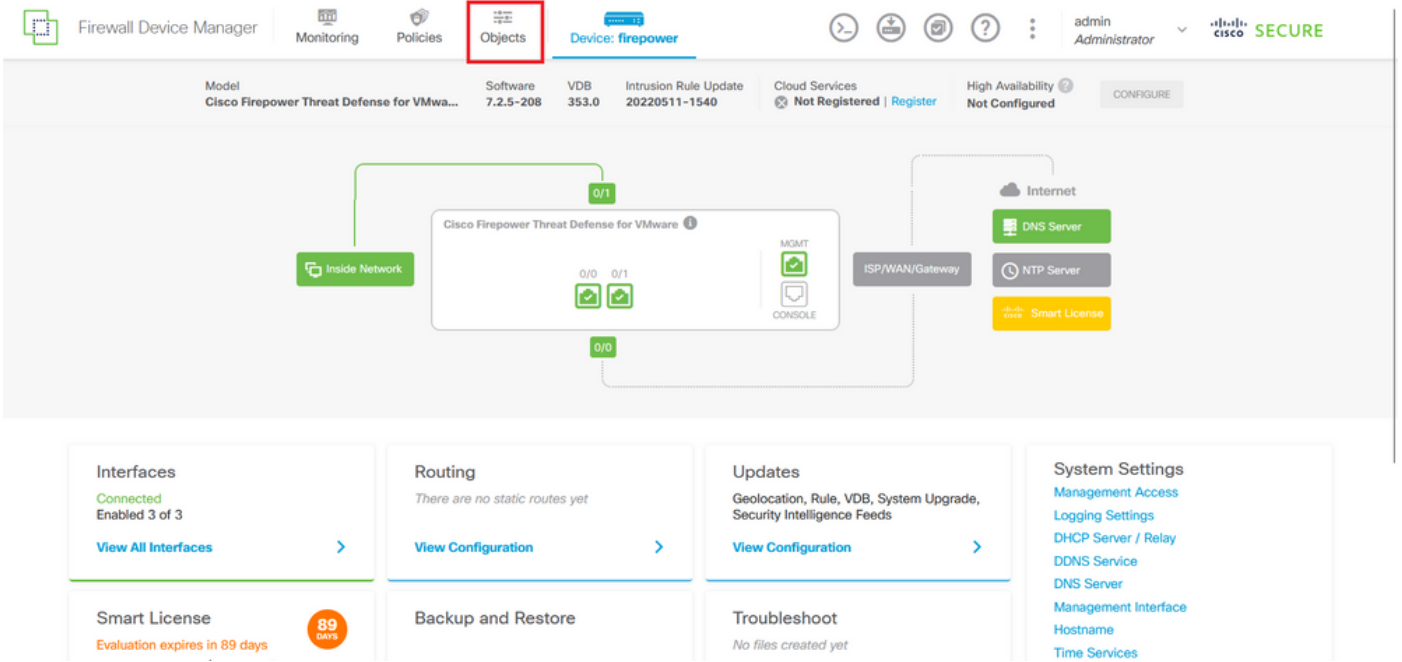
1단계. HTTPS를 통해 FDM GUI를 열고 인증서로 로그인합니다.



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2 [↗](#), version 2.1 [↗](#) and version 3 [↗](#)".

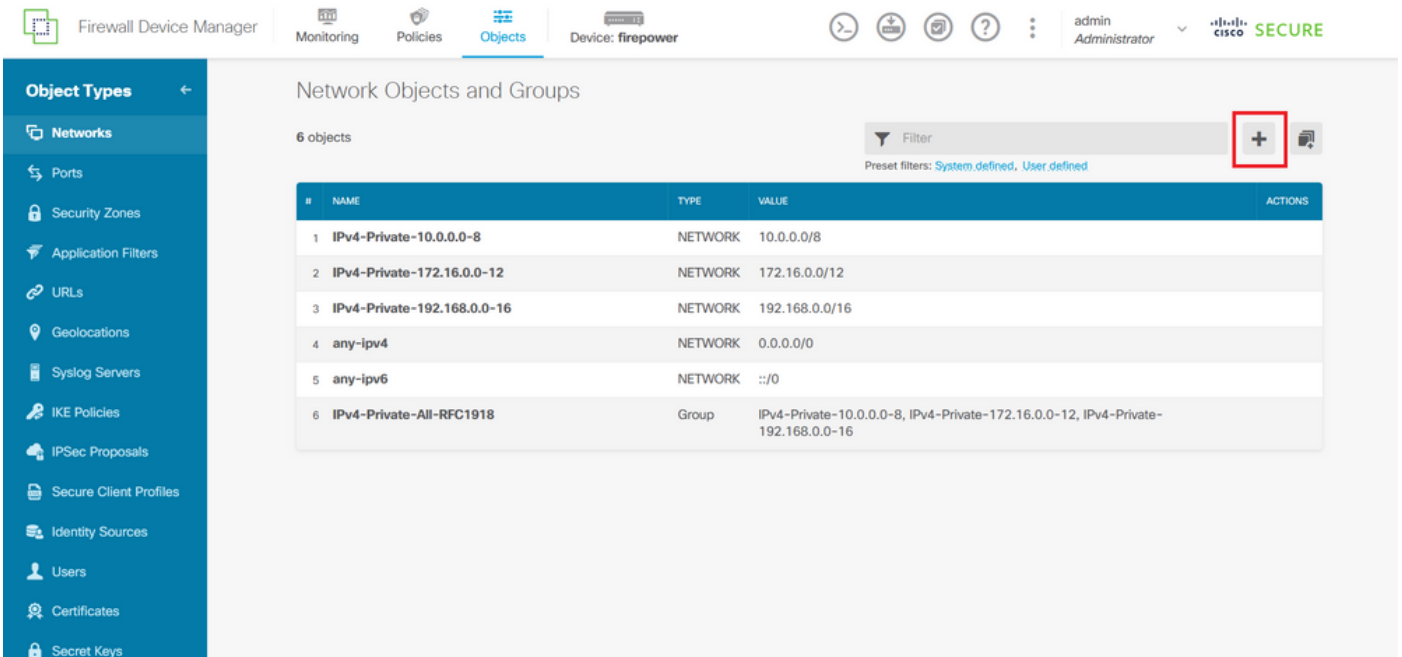
이미지 24. FDM 로그인 페이지

2단계. 객체 네트워크를 생성해야 합니다. 이를 위해 Objects(객체)로 이동합니다.



이미지 25. FDM 기본 대시보드

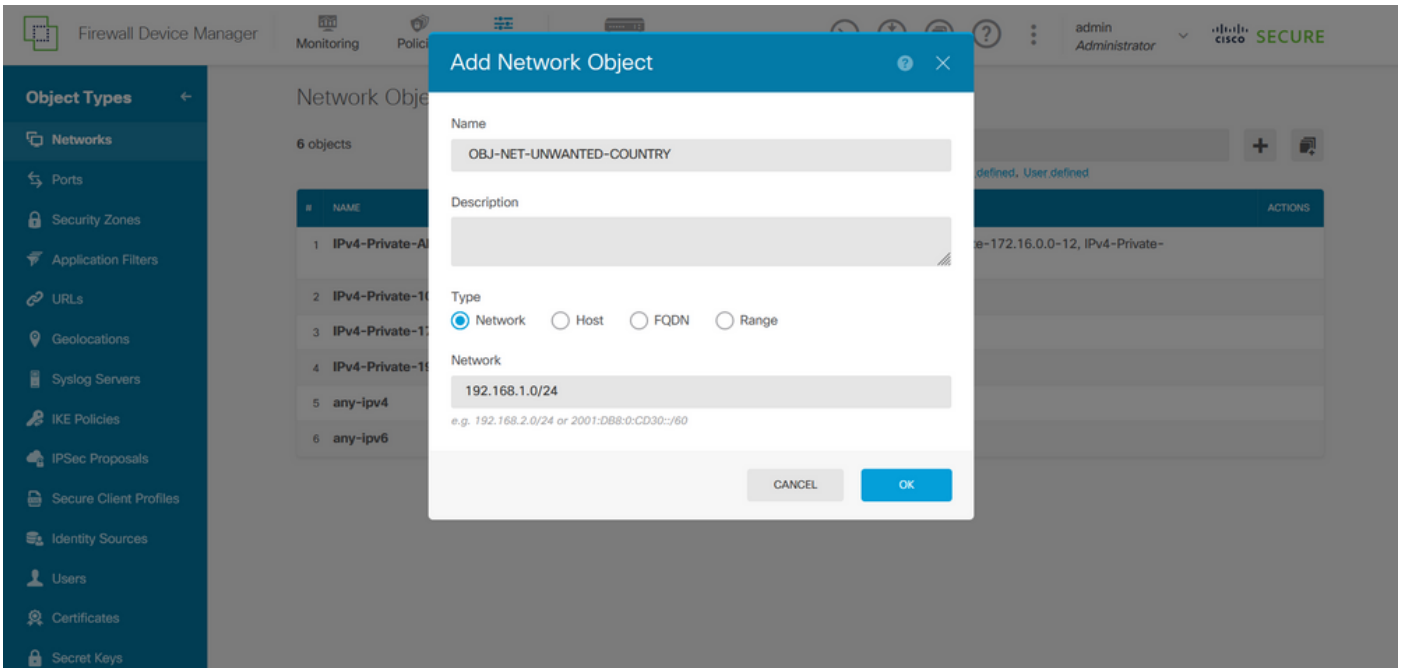
2.1단계. 왼쪽 패널에서 네트워크를 선택한 다음 '+' 버튼을 클릭하여 새 네트워크 객체를 만듭니다.



이미지 26. 객체 생성

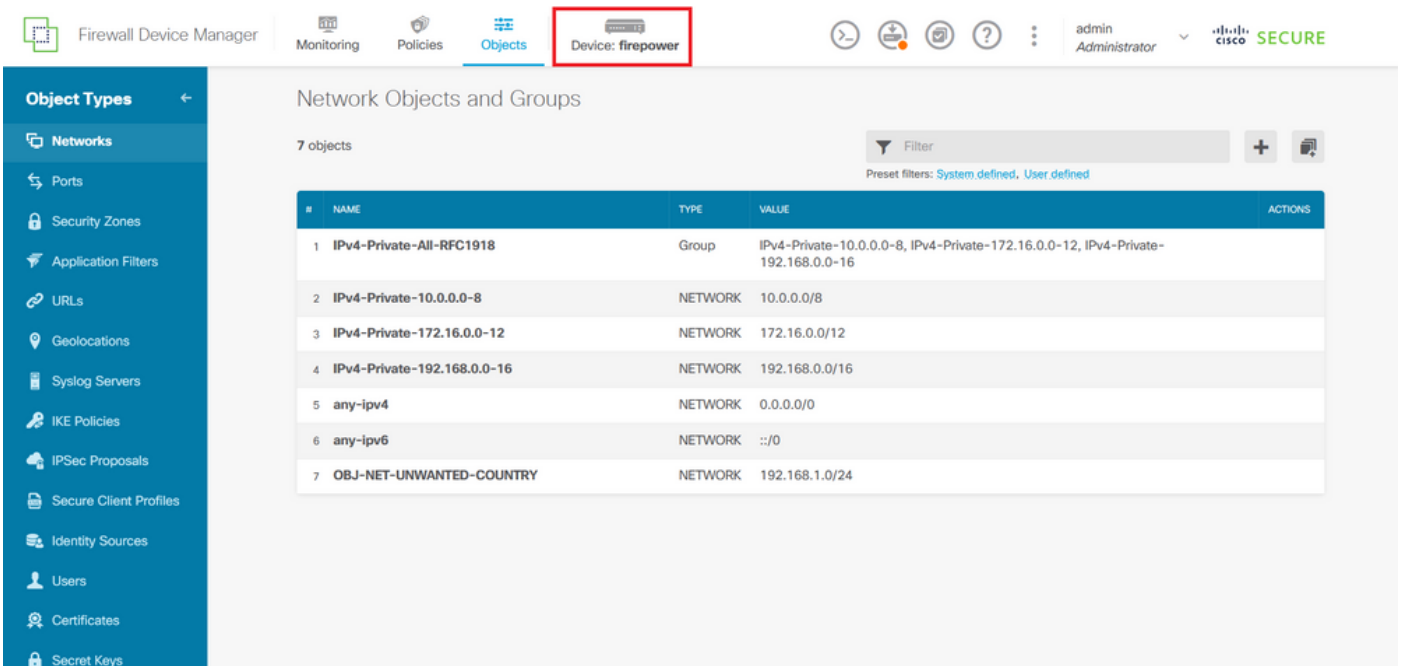
2.2단계. 네트워크 객체의 이름을 추가하고, 객체의 네트워크 유형을 선택하고, FTD에 거부해야 하는 트래픽과 일치하도록 IP 주소, 네트워크 주소 또는 IP 범위를 추가합니다. 그런 다음 OK(확인) 버튼을 클릭하여 개체 네트워크를 완료합니다.

- 이 예에서 구성된 개체 네트워크는 192.168.1.0/24 서브넷에서 오는 VPN 무작위 대입 공격을 차단하기 위한 것입니다.



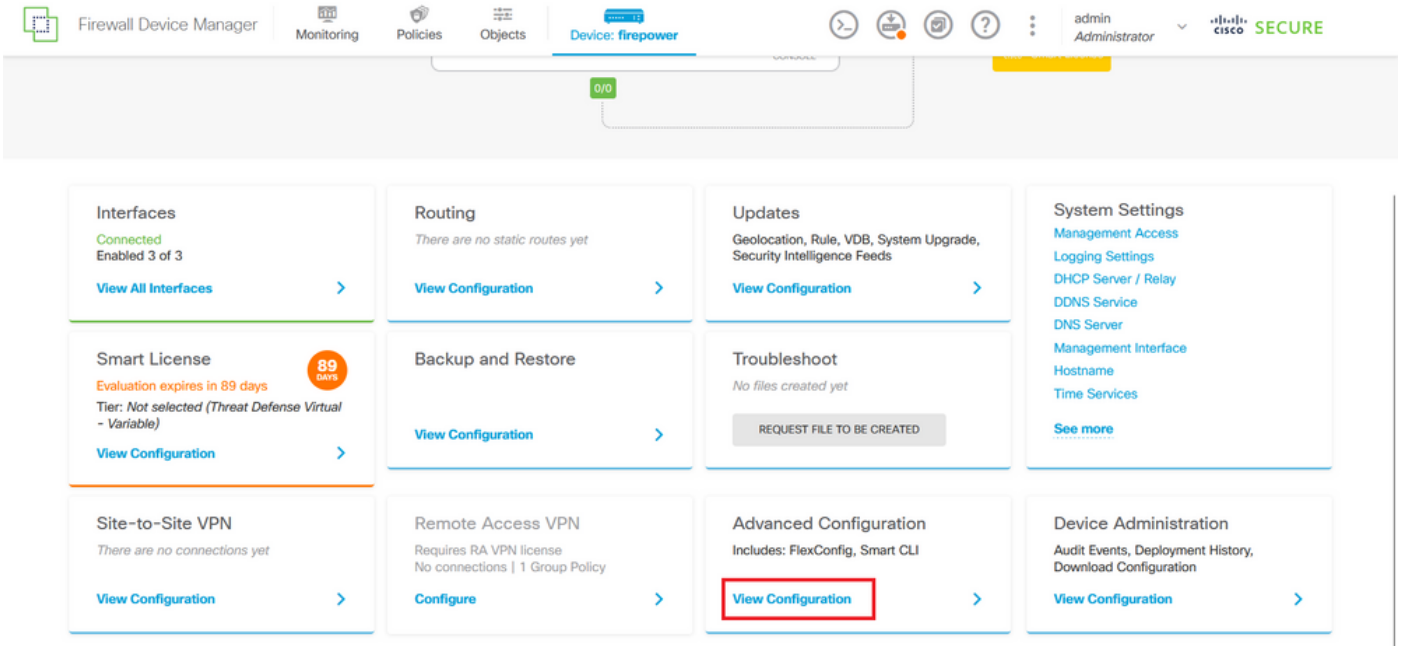
이미지 27. 네트워크 개체 추가

3단계. 그런 다음 확장 ACL을 생성해야 합니다. 이를 위해 상단 메뉴의 Device(디바이스) 탭으로 이동합니다.



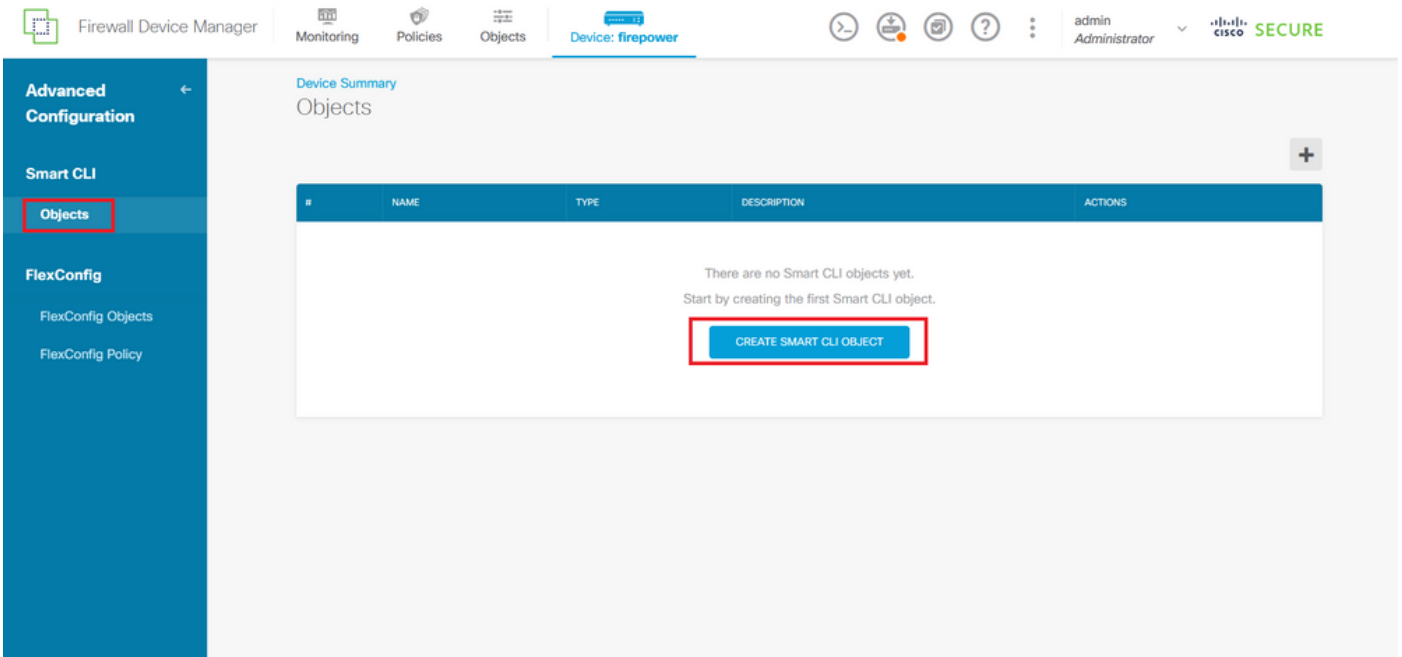
이미지 28. Device settings(디바이스 설정) 페이지

3.1단계. 아래로 스크롤하여 Advanced Configuration(고급 컨피그레이션) 사각형에서 View Configuration(컨피그레이션 보기)을 다음과 같이 선택합니다.



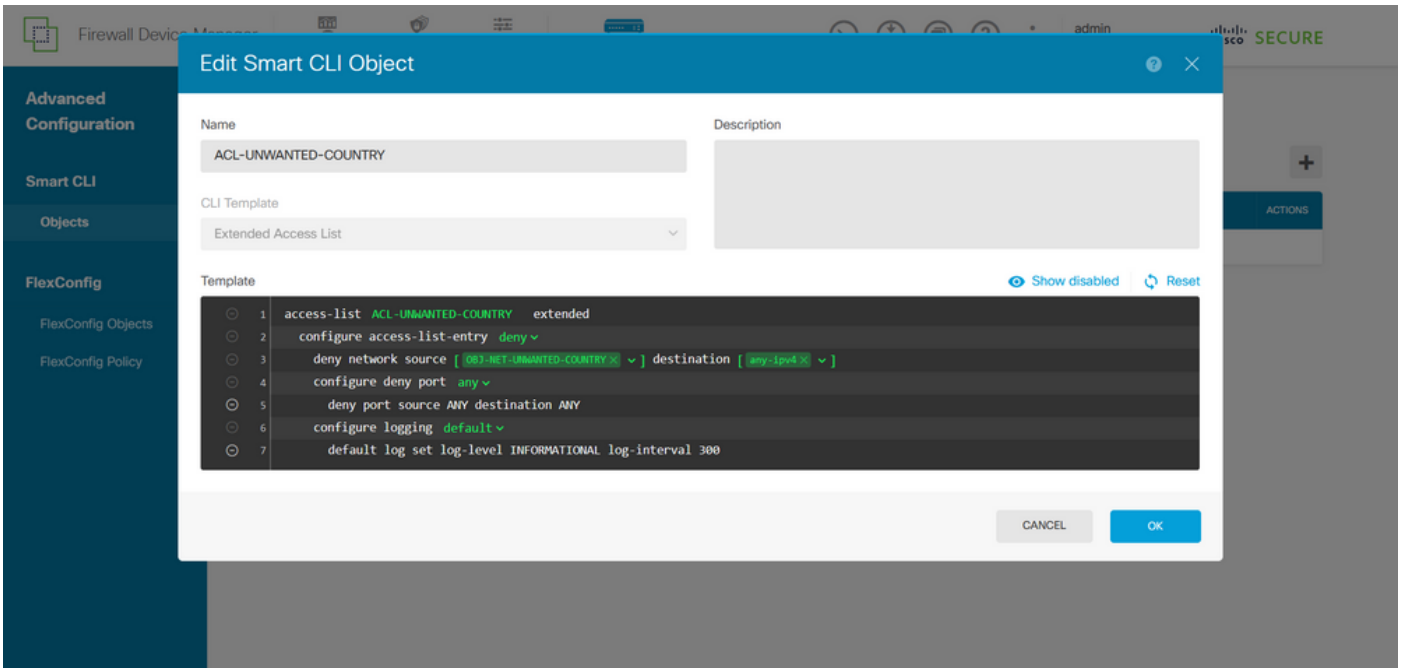
이미지 29. FDM 고급 구성

3.2단계. 그런 다음 왼쪽 패널에서 Smart CLI > Objects(개체)로 이동하고 CREATE SMART CLI OBJECT(SMART CLI 개체 생성)를 클릭합니다.




이미지 30. Smart CLI 객체

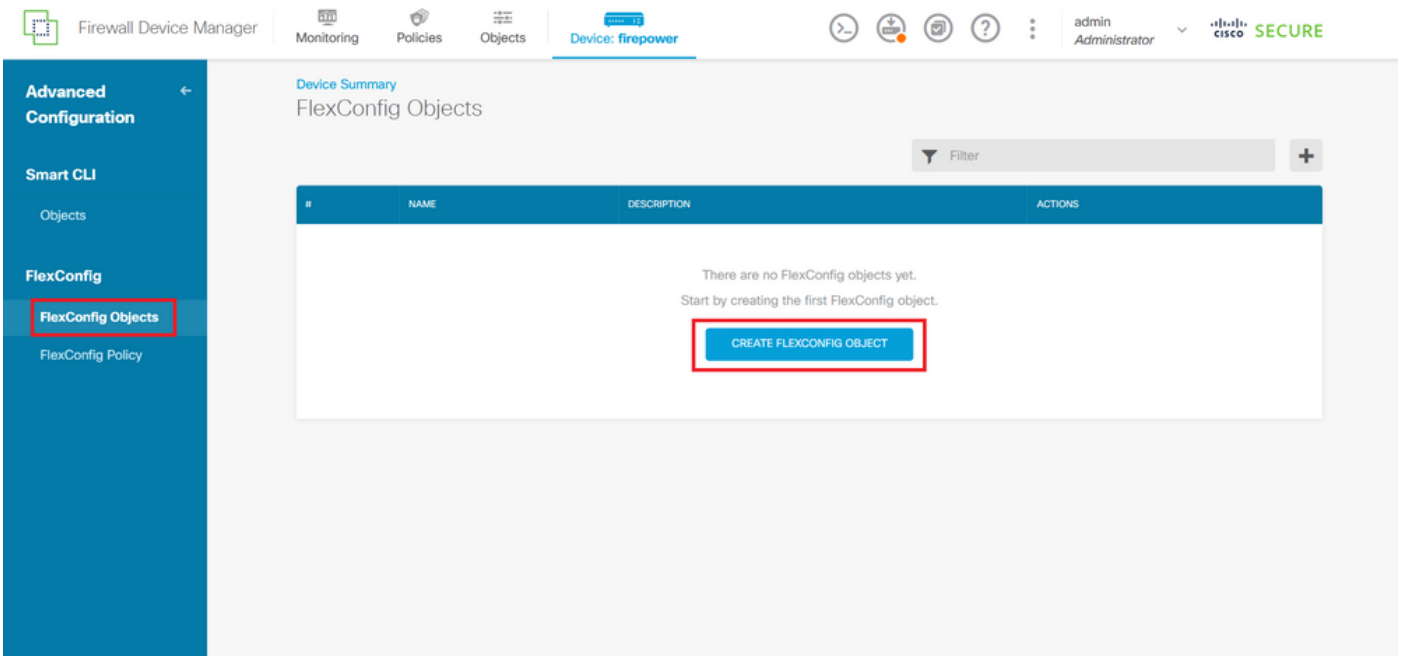
3.3단계. 생성할 확장 ACL의 이름을 추가하고, CLI 템플릿 드롭다운 메뉴에서 Extended Access List(확장 액세스 목록)를 선택하고, 위의 2.2단계에서 생성한 네트워크 객체를 사용하여 필요한 ACE를 구성한 다음 OK(확인) 버튼을 클릭하여 ACL을 완료합니다.



이미지 31. 확장 ACL 생성

 참고: ACL에 대한 ACE를 더 추가해야 하는 경우 마우스를 현재 ACE의 왼쪽 위로 이동하면 클릭할 수 있는 점 3개가 나타납니다. ACE를 더 추가하려면 해당 ACE를 클릭하고 Duplicate(복제)를 선택합니다.

4단계. 그런 다음 FlexConfig 객체를 생성해야 합니다. 이를 위해 왼쪽 패널로 이동하여 FlexConfig > FlexConfig Objects를 선택하고 CREATE FLEXCONFIG OBJECT를 클릭합니다.



이미지 32. FlexConfig 개체

4.1단계. 다음과 같이 FlexConfig 객체의 이름을 추가하여 제어 평면 ACL을 생성하고 외부 인터페이스에 대한 인바운드로 구성합니다.

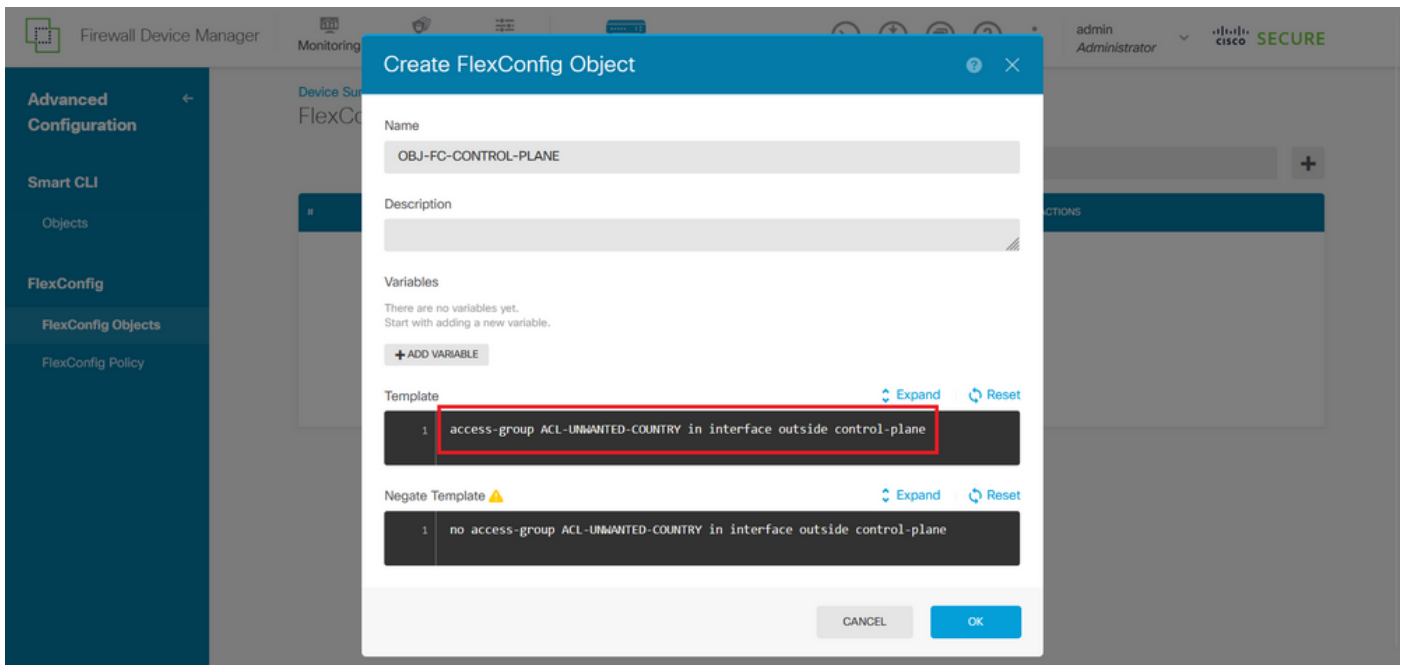
명령줄 구문:

```
access-group "ACL-name" in interface "interface-name" control-plane
```

이는 다음 명령 예제로 변환되며, 위의 3.3단계 'ACL-UNWANTED-COUNTRY'에서 생성된 확장 ACL을 다음과 같이 사용합니다.

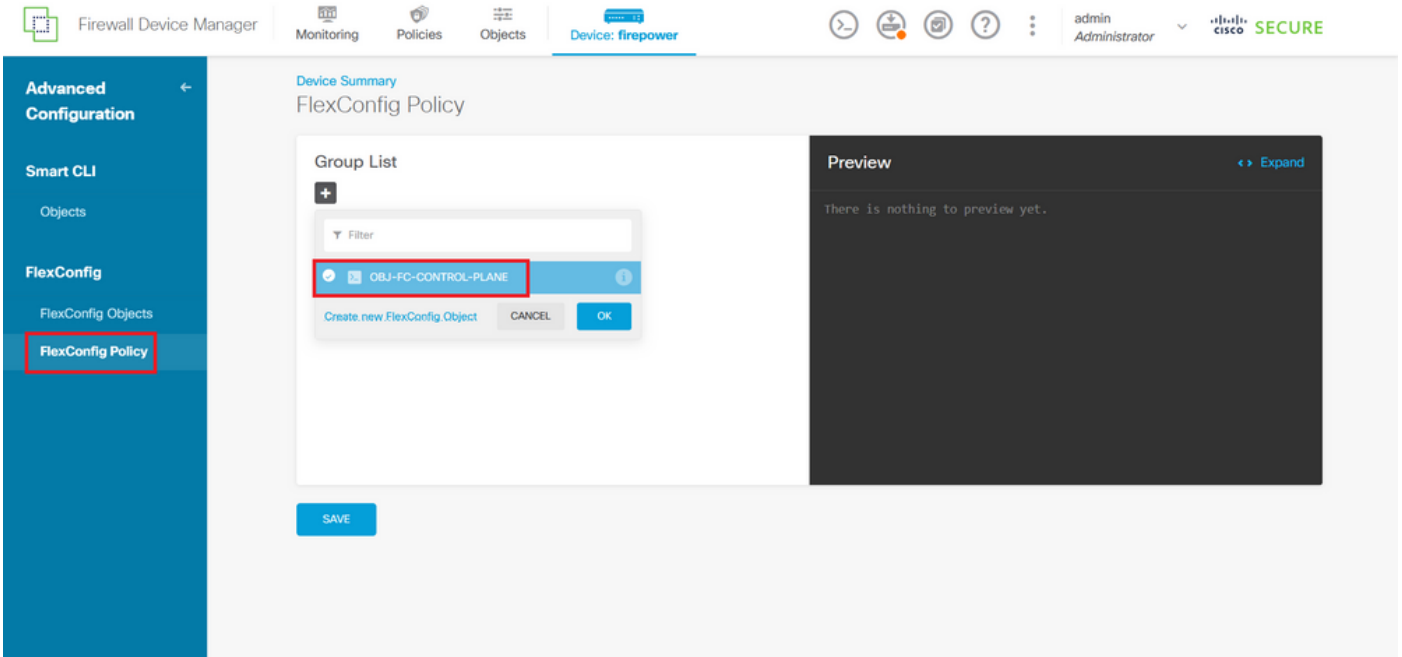
```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

이렇게 하면 FlexConfig 개체 창으로 구성되어야 합니다. 그런 다음 확인 단추를 선택하여 FlexConfig 개체를 완료합니다.



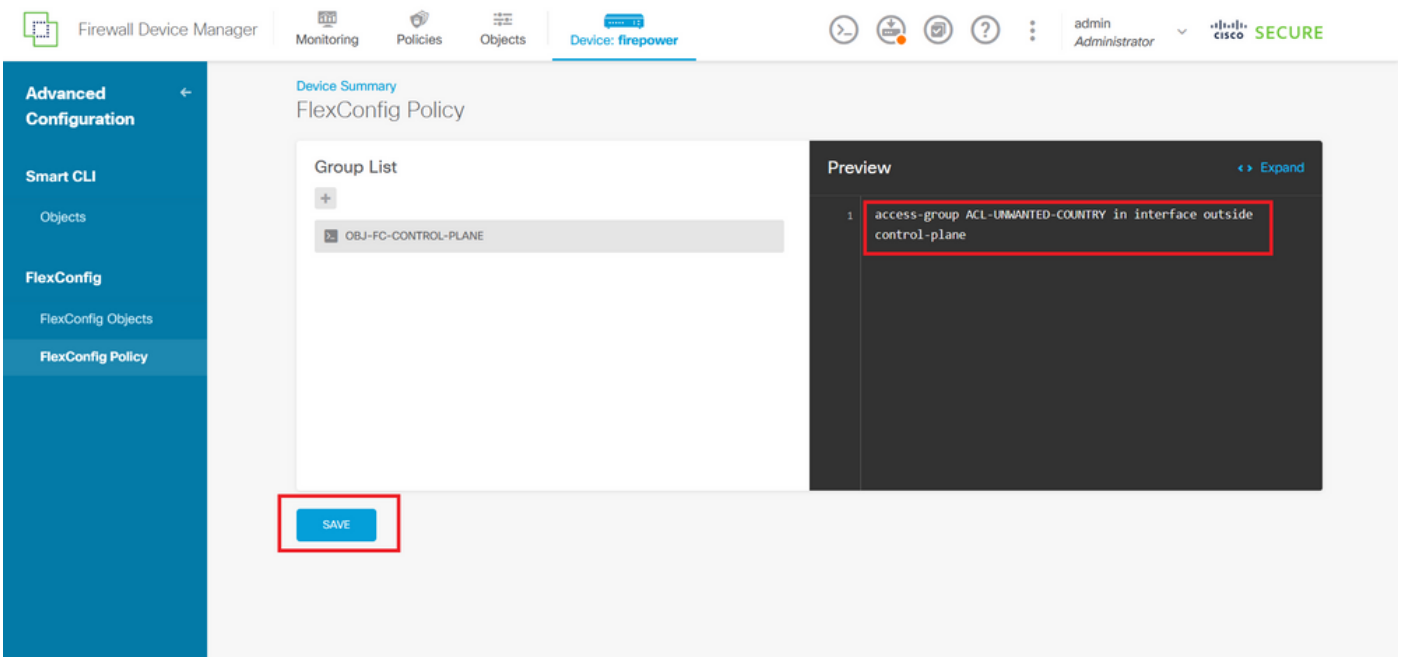
이미지 33. FlexConfig 개체 만들기

5단계. 계속해서 FlexConfig Policy를 생성합니다. 이를 위해 Flexconfig > FlexConfig Policy로 이동하고 '+' 버튼을 클릭한 다음 위 4.1단계에서 생성한 FlexConfig 객체를 선택합니다.



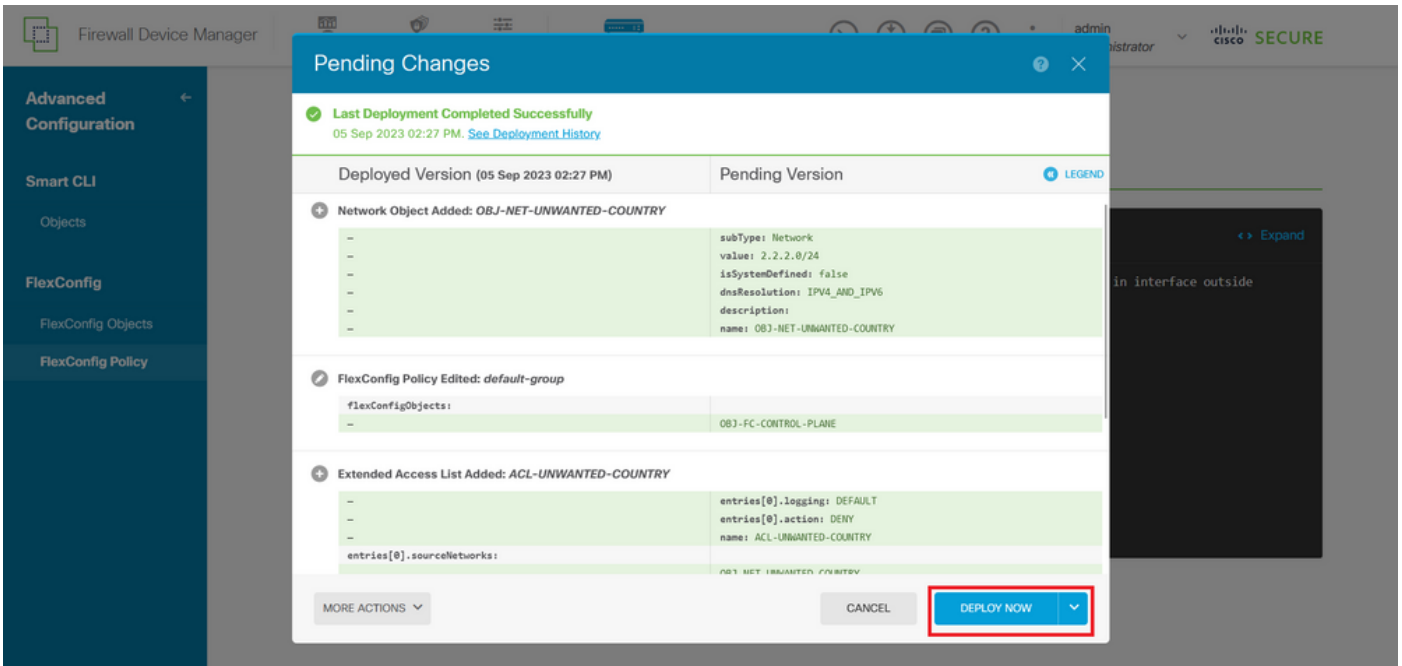
이미지 34. FlexConfig 정책

5.1단계. FlexConfig 미리 보기에 생성된 컨트롤 플레인 ACL에 대한 올바른 컨피그레이션이 표시되는지 확인하고 Save(저장) 버튼을 클릭합니다.



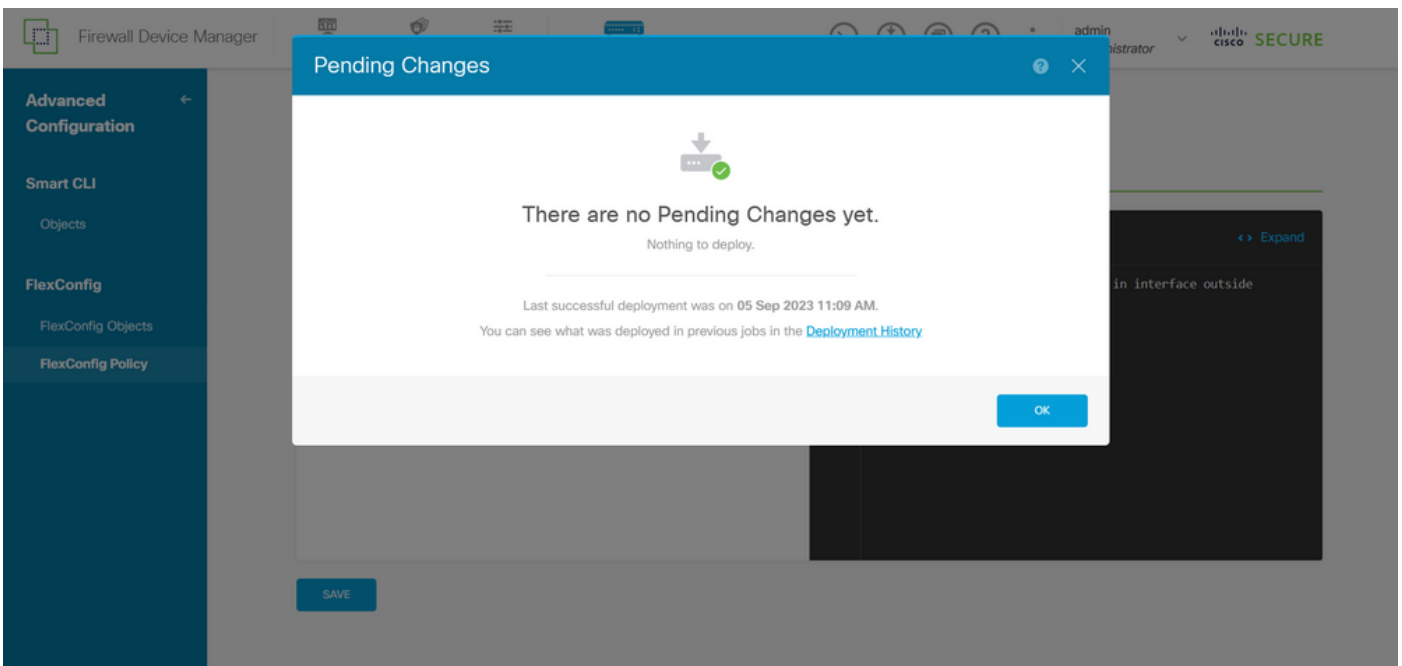
이미지 35. FlexConfig 정책 미리 보기

6단계. VPN 무차별 대입 공격으로부터 보호하려는 FTD에 컨피그레이션 변경 사항을 구축합니다. 이를 위해 상단 메뉴에서 Deployment(구축) 버튼을 클릭하고 구축할 컨피그레이션 변경 사항이 올바른지 확인한 다음 DEPLOY NOW(지금 구축)를 클릭합니다.



이미지 36. 배포 보류 중

6.1단계. 정책 배포가 성공적인지 확인합니다.



이미지 37. 배포 성공

7단계. FTD에 대한 새 컨트를 플레인 ACL을 생성하거나 현재 사용 중인 기존 ACL을 편집한 경우, 컨피그레이션 변경 사항이 이미 설정된 FTD 연결에 적용되지 않으므로 FTD에 대한 활성 연결 시도를 수동으로 지워야 합니다. 이를 위해 FTD의 CLI에 연결하고 다음과 같이 활성 연결을 지웁니다.

특정 호스트 IP 주소에 대한 활성 연결을 지우려면


```
> clear conn address 192.168.1.10 all
```

전체 서브넷 네트워크에 대한 활성 연결을 지우려면

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

IP 주소 범위에 대한 활성 연결을 지우려면

```
> clear conn address 192.168.1.1-192.168.1.10 all
```

 참고: 주로 VPN 무작위 대입 공격의 특성에서 지속적인 연결 시도가 급증할 때 활성 VPN 무작위 대입 연결 시도를 보안 방화벽에 강제로 지우려면 clear conn address 명령의 끝에 'all' 키워드를 사용하는 것이 좋습니다.

CLI를 사용하여 ASA에 대한 컨트롤 플레인 ACL 구성

이는 외부 인터페이스에 대한 수신 VPN 무차별 대입 공격을 차단하기 위해 제어 평면 ACL을 구성하기 위해 ASA CLI에서 수행해야 하는 절차입니다.

1단계. CLI를 통해 보안 방화벽 ASA에 로그인하고 다음과 같이 'configure terminal'에 액세스합니다

```
asa# configure terminal
```

2단계. ASA에 대해 차단해야 하는 트래픽에 대한 호스트 IP 주소 또는 네트워크 주소를 차단하도록 확장 ACL을 구성하려면 next 명령을 사용합니다.

- 이 예에서는 'ACL-UNWANTED-COUNTRY'라는 새 ACL을 생성하면 구성된 ACE 항목이 192.168.1.0/24 서브넷에서 오는 VPN 무차별 대입 공격을 차단합니다.

```
asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

3단계. 다음 access-group 명령을 사용하여 'ACL-UNWANTED-COUNTRY' ACL을 외부 ASA 인터페이스에 대한 컨트롤 플레인 ACL로 구성합니다.

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

4단계. 새 제어 평면 ACL을 생성하거나 현재 사용 중인 기존 ACL을 편집한 경우, 컨피그레이션 변경 사항이 이미 설정된 ASA 연결에 적용되지 않으므로 ASA에 대한 활성 연결 시도를 수동으로 지워야 합니다. 이를 위해 다음과 같이 활성 연결을 지웁니다.

특정 호스트 IP 주소에 대한 활성 연결을 지우려면


```
asa# clear conn address 192.168.1.10 all
```

전체 서브넷 네트워크에 대한 활성 연결을 지우려면

```
asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

IP 주소 범위에 대한 활성 연결을 지우려면

```
asa# clear conn address 192.168.1.1-192.168.1.10 all
```

 참고: 주로 VPN 무작위 대입 공격의 특성에서 지속적인 연결 시도가 급증할 때 활성 VPN 무작위 대입 연결 시도를 보안 방화벽에 강제로 지우려면 clear conn address 명령의 끝에 'all' 키워드를 사용하는 것이 좋습니다.

'shun' 명령을 사용하여 보안 방화벽의 공격을 차단하는 대체 컨피그레이션

보안 방화벽에 대한 공격을 차단하는 즉각적인 옵션의 경우 'shun' 명령을 사용할 수 있습니다. shuncommand를 사용하면 공격 호스트로부터의 연결을 차단할 수 있습니다.

- IP 주소를 해제하면 차단 기능이 수동으로 제거될 때까지 소스 IP 주소에서 향후 모든 연결이 삭제되고 기록됩니다.

- 지정된 호스트 주소와의 연결이 현재 활성 상태인지 여부에 관계없이 theshuncommand의 차단 기능이 적용됩니다.

- 대상 주소, 소스 및 대상 포트, 프로토콜을 지정하면 일치하는 연결을 삭제하고 소스 IP에서 향후 모든 연결을 차단할 수 있습니다

주소: 이러한 특정 연결 매개변수와 일치하는 연결뿐만 아니라 향후 모든 연결이 차단됩니다.

- 소스 IP 주소당 oneshuncommand만 가질 수 있습니다.

- shuncommand는 공격을 동적으로 차단하는 데 사용되므로 위협 방어 디바이스 컨피그레이션에 표시되지 않습니다.

- 인터페이스 컨피그레이션이 제거될 때마다 해당 인터페이스에 연결된 모든 단락도 제거됩니다.

- 명령 구문 차단:

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- shun을 비활성화하려면 이 명령의 no 형식을 사용합니다.

```
no shun source_ip [ vlan vlan_id]
```

호스트 IP 주소를 차단하려면 보안 방화벽에 대해 다음과 같이 진행합니다. 이 예에서는 'shun' 명령을 사용하여 소스 IP 주소 192.168.1.10에서 오는 VPN 무차별 대입 공격을 차단합니다.

FTD의 컨피그레이션 예

1단계. CLI를 통해 FTD에 로그인하고 다음과 같이 shun 명령을 적용합니다.

```
<#root>
```

```
>
```

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

2단계. 다음 show 명령을 사용하여 FTD에서 shun IP 주소를 확인하고 IP 주소당 shun hit 횟수를 모니터링할 수 있습니다.

```
<#root>
```

```
>
```

```
show shun
```

```
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
```

```
>
```

```
show shun statistics
```

```
diagnostic=OFF, cnt=0  
outside=ON, cnt=0
```

```
Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

ASA의 컨피그레이션 예

1단계. CLI를 통해 ASA에 로그인하고 다음과 같이 shun 명령을 적용합니다.

```
<#root>
```

```
asa#
```

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

2단계. 다음 show 명령을 사용하여 ASA에서 shun IP 주소를 확인하고 IP 주소당 shun hit 횟수를 모니터링할 수 있습니다.

```
<#root>
```

```
asa#
```

```
show shun
```


```
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
```

```
asa#
```

```
show shun statistics
```

```
outside=ON, cnt=0  
inside=OFF, cnt=0  
dmz=OFF, cnt=0  
outside1=OFF, cnt=0  
mgmt=OFF, cnt=0
```

```
Shun 192.168.1.10 cnt=0, time=(0:01:39)
```

 참고: secure firewall shun 명령에 대한 자세한 내용은 [Cisco Secure Firewall Threat Defense 명령 참조를 확인하십시오](#)

다음을 확인합니다.

보안 방화벽에 대한 제어 평면 ACL 컨피그레이션이 있는지 확인하려면 다음과 같이 진행합니다.

1단계. CLI를 통해 보안 방화벽에 로그인하고 다음 명령을 실행하여 컨트롤 플레인 ACL 컨피그레이션이 적용되었는지 확인합니다.

FMC에서 관리하는 FTD의 출력 예:

```
<#root>
```

```
>
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

```
>
```

```
show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

FDM에서 관리되는 FTD의 출력 예:

```
<#root>
```

```
> show running-config object id OBJ-NET-UNWANTED-COUNTRY
```

```
object network OBJ-NET-UNWANTED-COUNTRY
```

```
subnet 192.168.1.0 255.255.255.0
```

```
>
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default
```

```
> show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

ASA의 출력 예:

```
<#root>
```

```
asa#
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

```
asa#
```

```
show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

2단계. 컨트롤 플레인 ACL이 필요한 트래픽을 차단하고 있는지 확인하려면 packet-tracer 명령을 사용하여 보안 방화벽의 외부 인터페이스에 대한 수신 TCP 443 연결을 시뮬레이션한 다음 show access-list <acl-name> 명령을 사용하면 보안 방화벽에 대한 VPN 무작위 강제 연결이 컨트롤 플레인 ACL에 의해 차단될 때마다 ACL 히트 수가 증가해야 합니다.

- 이 예에서 packet-tracer 명령은 호스트 192.168.1.10에서 소싱되고 보안 방화벽의 외부 IP 주소로 전달되는 수신 TCP 443 연결을 시뮬레이션합니다. 'packet-tracer' 출력에서는 트래픽이 삭제되고 있음을 확인하고, 'show access-list' 출력에서는 컨트롤 플레인 ACL에 대한 적중 횟수 증가분이 표시됩니다.

FTD의 출력 예

```
<#root>
```

```
>
```

```
packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443
```

```
Phase: 1
```

```
Type:
```

```
ACCESS-LIST
```

```
Subtype: log
```

```
Result: DROP
```

```
Elapsed time: 21700 ns
```

```
Config:
```

```
Additional Information:
```

```
Result:
```

```
input-interface: outside(vrfid:0)
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: drop
```

Time Taken: 21700 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA

>

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f

access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf

ASA의 출력 예

<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 19688 ns

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 17833 ns

Config:

Additional Information:

Result:

input-interface: outside

input-status: up

input-line-status: up

Action: drop

Time Taken: 37521 ns

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA

```
asa#
```


```
show access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
```

```
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any
```

```
(hitcnt=1)
```

```
0x9b4d26ac
```

 참고: Cisco Secure Client VPN과 같은 RAVPN 솔루션이 보안 방화벽에 구현된 경우, 필요한 트래픽을 차단하기 위해 컨트롤 플레인 ACL이 예상대로 작동하는지 확인하기 위해 보안 방화벽에 대한 실제 연결 시도를 수행할 수 있습니다.

관련 버그

- 엔터 | 지리적 위치 기반 AnyConnect 클라이언트 연결: Cisco 버그 ID [CSCvs65322](#)

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.