Firepower Migration Tool을 사용하여 ASA 구성 파일에서 FTD 구성

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance)에서 FPR4145의 FTD(Firepower Threat Defense)로의 마이그레이션의 예를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA에 대한 기본 지식
- FMC(Firepower Management Center) 및 FTD 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 버전 9.12(2)
- FTD 버전 6.7.0
- FMC 버전 6.7.0
- Firepower Migration Tool 버전 2.5.0

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

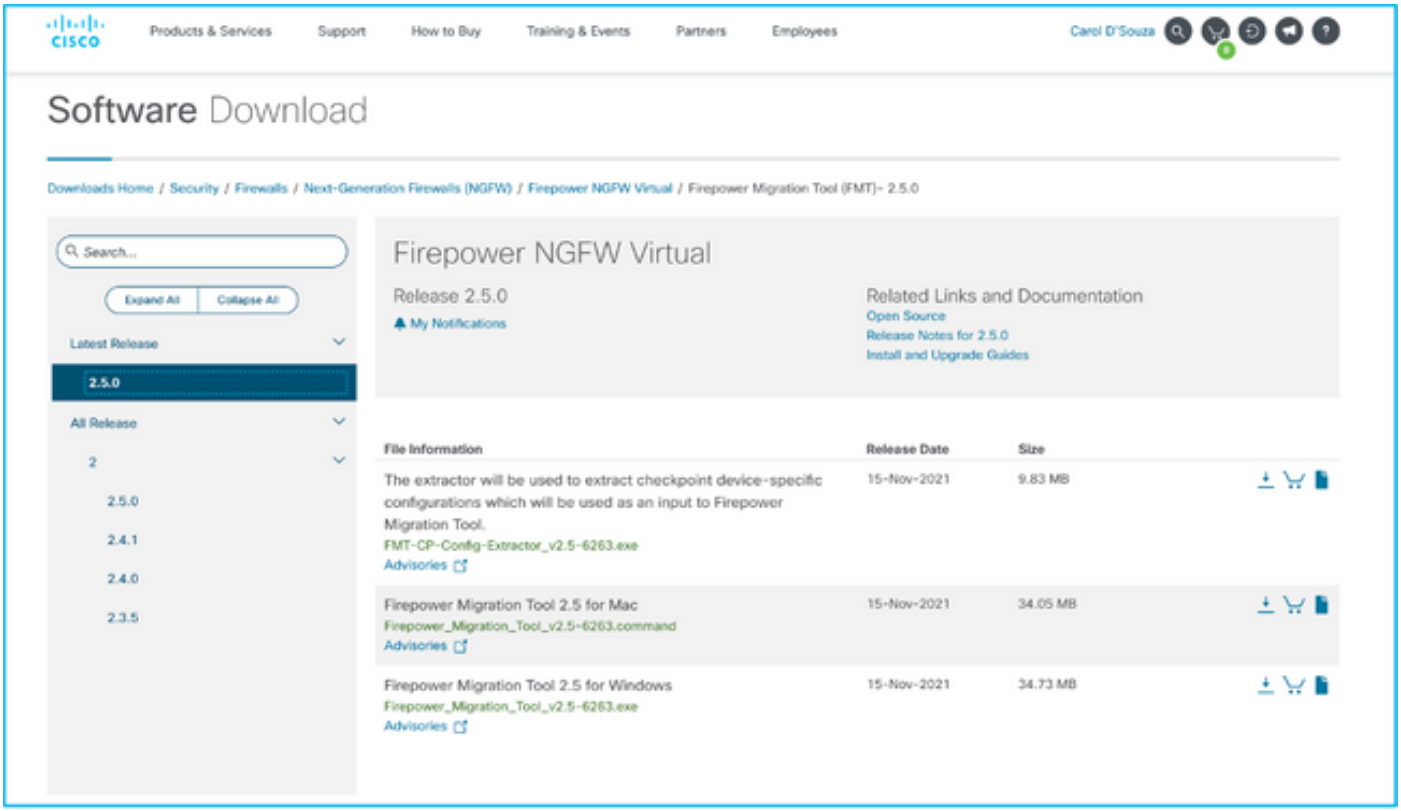
배경 정보

ASA 구성 파일을 **.cfg** 또는 **.txt** 형식**으로** 내보냅니다. FMC는 FTD가 등록된 상태로 구축되어야 합

니다.

구성

1. 이미지에 표시된 대로 software.cisco.com에서 Firepower Migration Tool을 다운로드합니다.



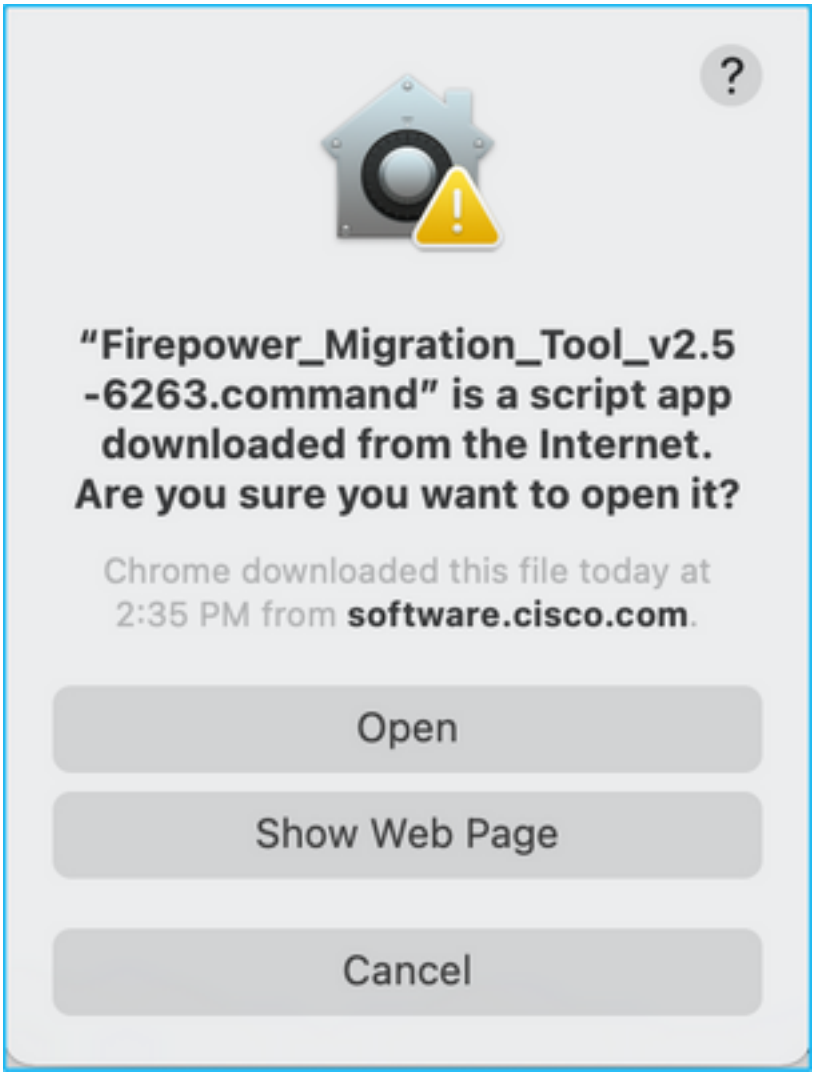
2. Firepower Migration Tool 섹션의 지침 및 제한 사항을 검토하고 확인합니다.

3. 대규모 구성 파일을 마이그레이션하려는 경우 마이그레이션 푸시 중에 시스템이 절전 모드로 전환되지 않도록 절전 설정을 구성합니다.

3.1. Windows의 경우 제어판의 전원 옵션으로 이동합니다. 현재 전원 계획 옆에 있는 **계획 설정 변경**을 클릭합니다. 변경 **컴퓨터를 절전 모드로** 전환합니다**. 변경 내용 저장을 클릭합니다**.

3.2. MAC의 경우 **[시스템 환경 설정] > [에너지 절약]**으로 이동합니다. 디스플레이가 꺼져 있을 때 컴퓨터가 자동으로 절전 모드로 전환되지 않도록 하려면 다음 상자를 선택하고 **[**슬라이더 이후 **표시** 해제]를 [안 함]으로 끕니다.

> **참고:** 이 경고 메시지는 MAC 사용자가 다운로드한 파일을 열려고 하면 대화 상자가 나타납니다. 이를 무시하고 4단계 A를 따릅니다.



4. A. MAC용 - 터미널을 사용하여 이 명령을 실행합니다.

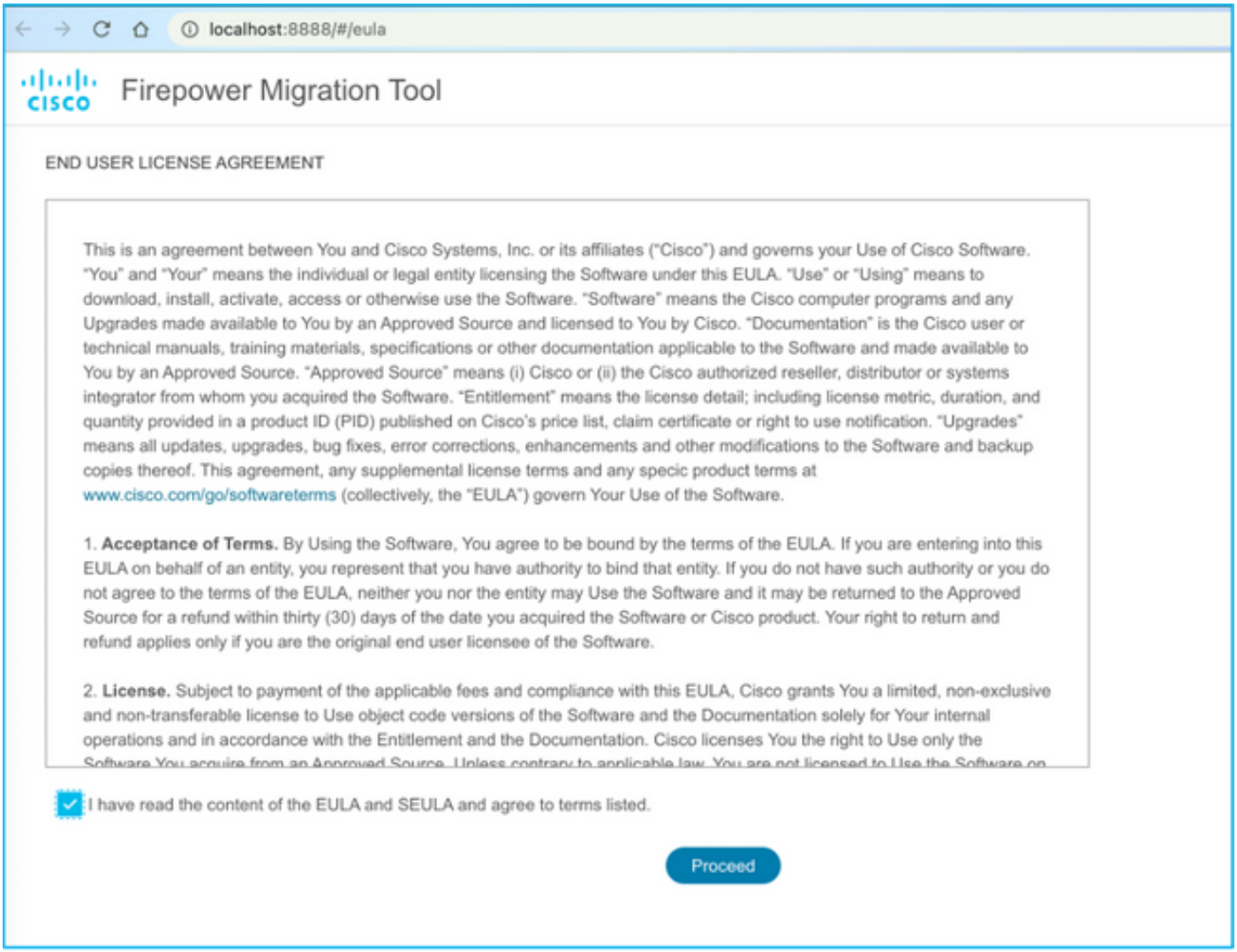
```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263
.command
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command

[75653] PyInstaller Bootloader 3.x
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool
_v2.5-6263.command
[75653] LOADER: homepath is /Users/caroldso/Downloads
[75653] LOADER: _MEIPASS2 is NULL
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too
l_v2.5-6263.command
[75653] LOADER: Cookie found at offset 0x219AE08
[75653] LOADER: Extracting binaries
[75653] LOADER: Executing self as child
```

```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js
 HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H
TTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO    | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG   | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200
-
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4. B. Windows의 경우 Firepower Migration Tool을 더블 클릭하여 Google Chrome 브라우저에서 시작합니다.

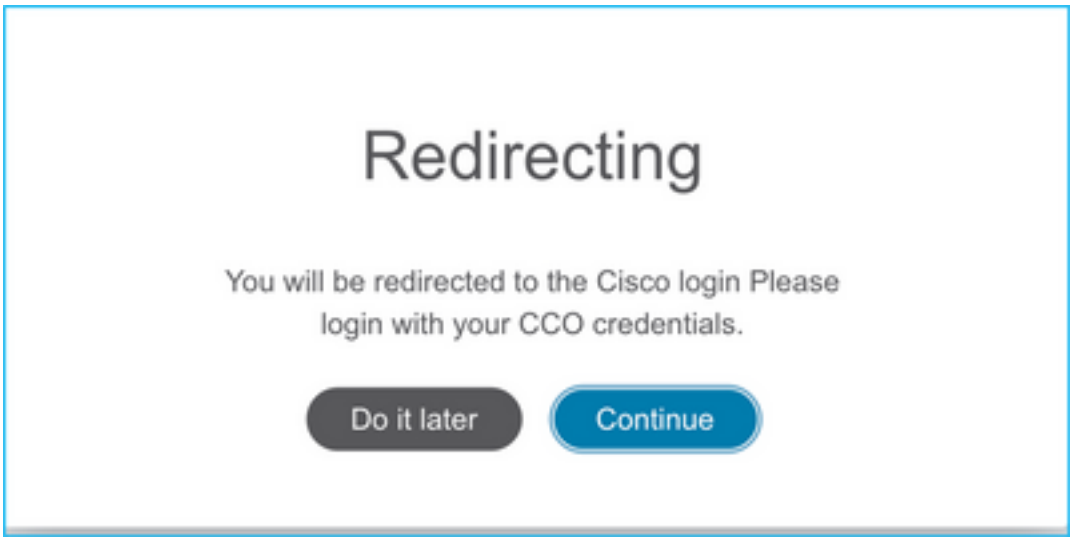
5. 이미지에 표시된 대로 라이센스를 수락합니다.



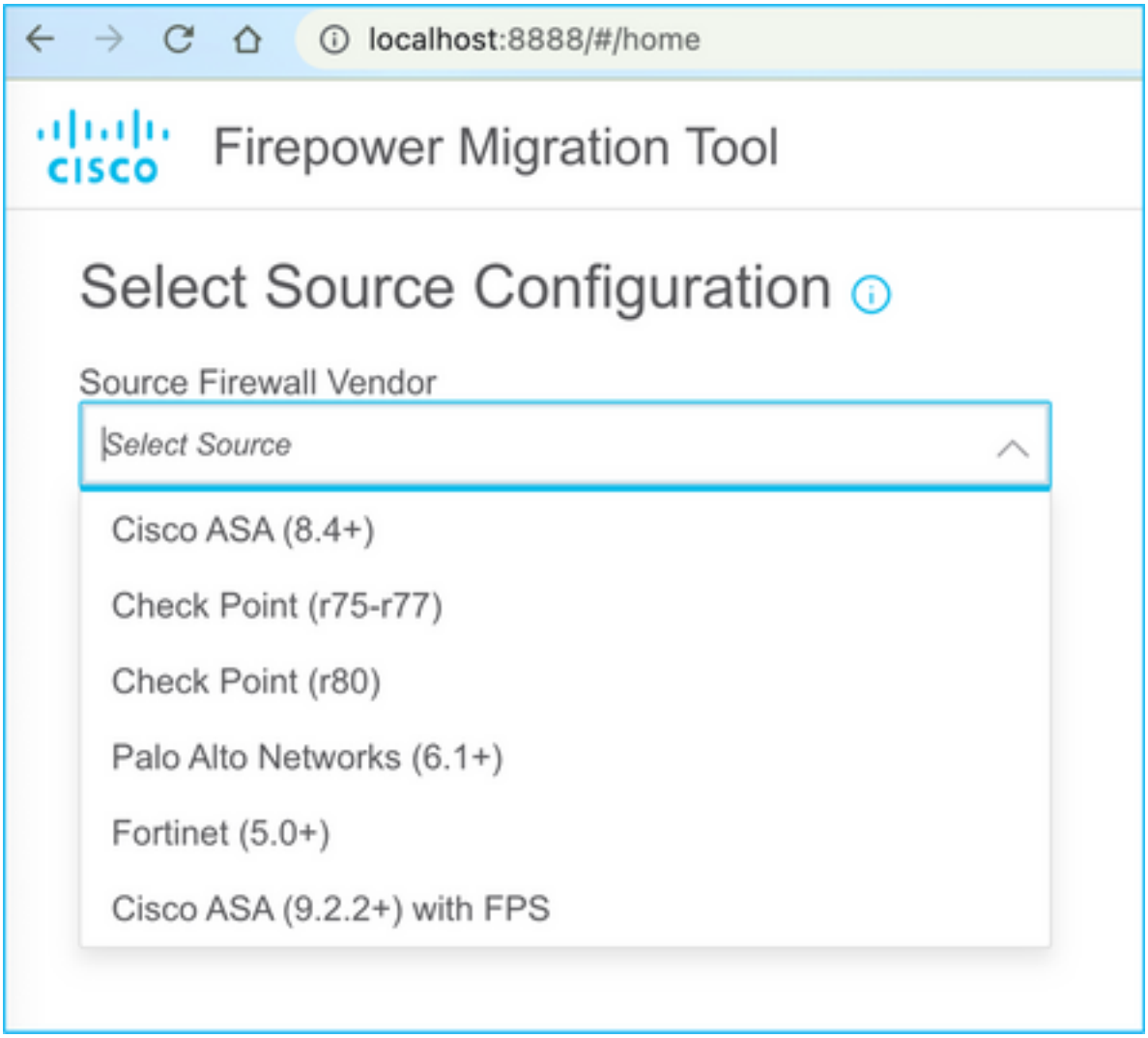
6. Firepower Migration Tool의 로그인 페이지에서 CCO로 로그인 링크를 클릭하여 Cisco.com 계정에 Single Sign-On 자격 증명을 사용하여 로그인합니다.

참고: Cisco.com 계정이 없는 경우 Cisco.com 로그인 페이지에서 계정을 생성합니다. 다음 기

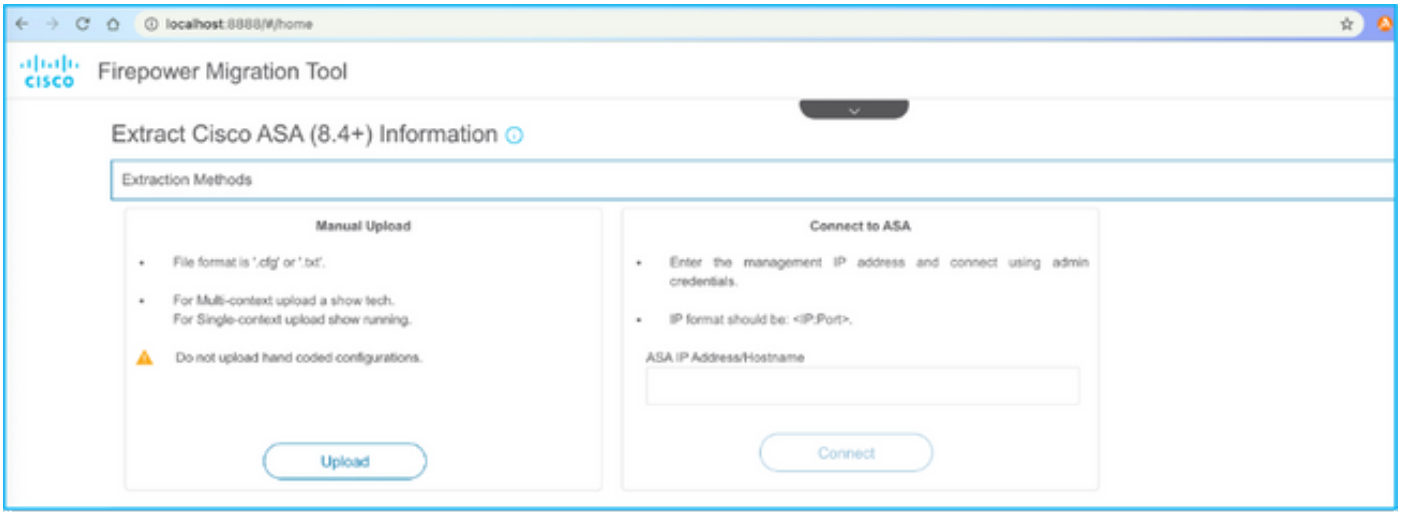
본 자격 증명으로 로그인합니다. Username(사용자 이름) - admin Password(관리자 비밀번호) - Admin123.



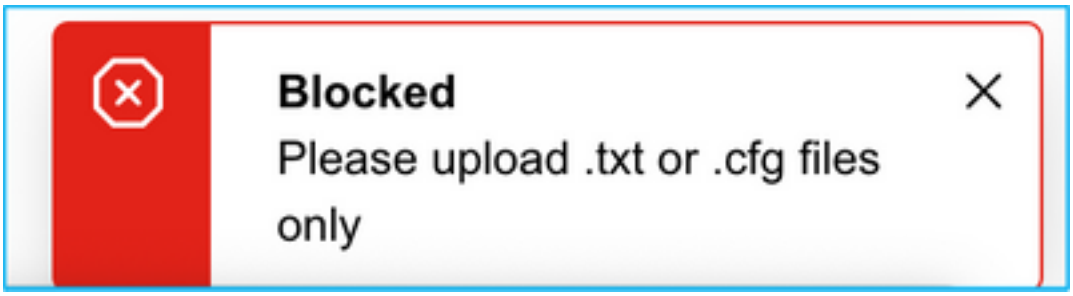
7. 출처 구성을 선택합니다. 이 시나리오에서는 Cisco ASA(8.4 이상)입니다.

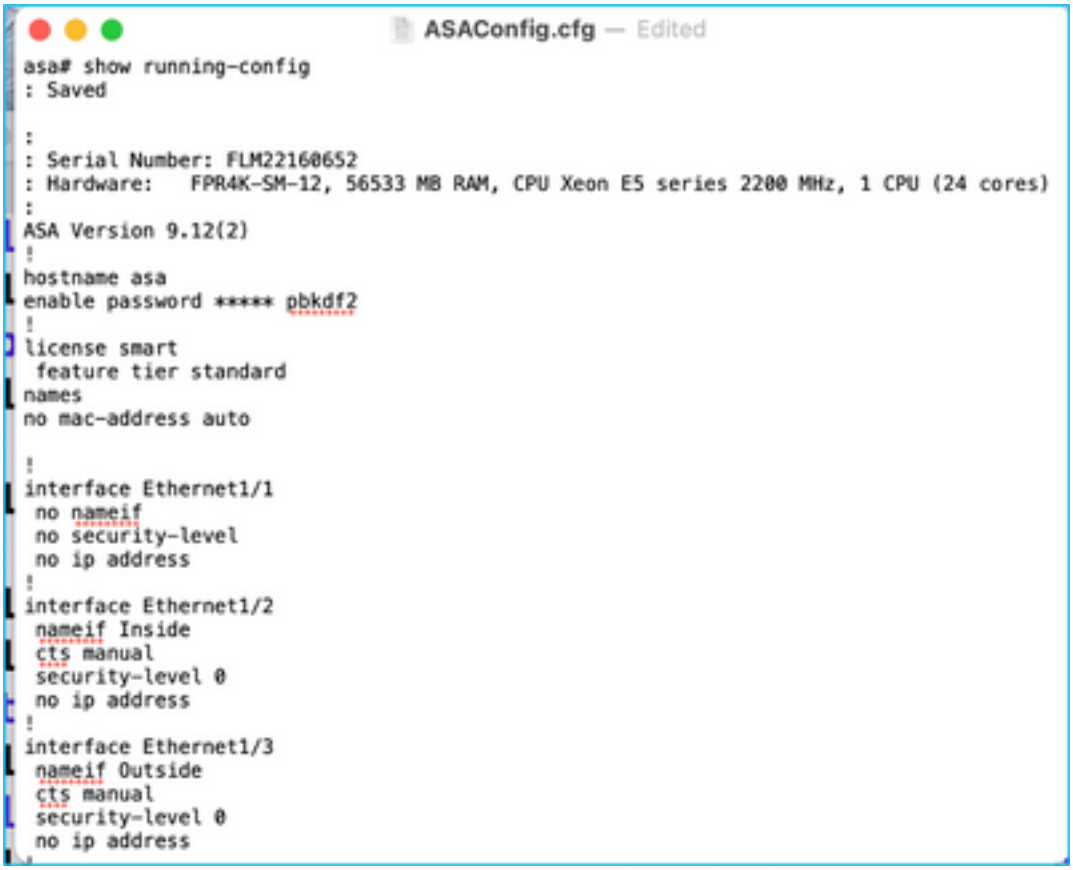


8. ASA에 연결되지 않은 경우 수동 업로드를 선택합니다. 그렇지 않으면 ASA에서 실행 중인 구성을 검색하고 관리 IP 및 로그인 세부 정보를 입력할 수 있습니다. 시나리오에서 수동 업로드가 수행되었습니다.



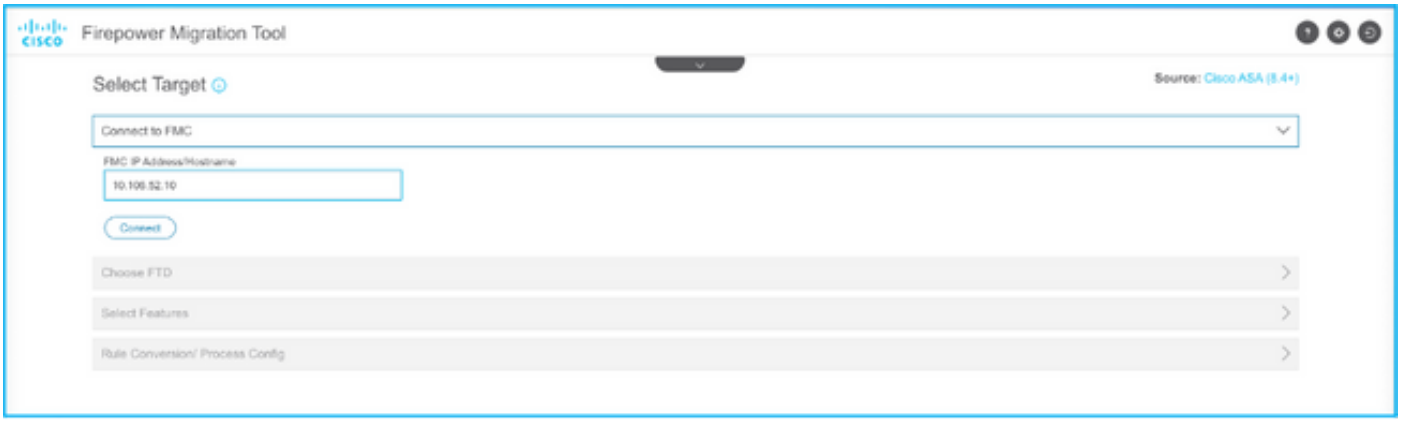
참고: 이 오류는 파일이 지원되지 않는 경우에 나타납니다. 형식을 일반 텍스트로 변경해야 합니다. 확장명이 .cfg에도 불구하고 오류가 표시됩니다.



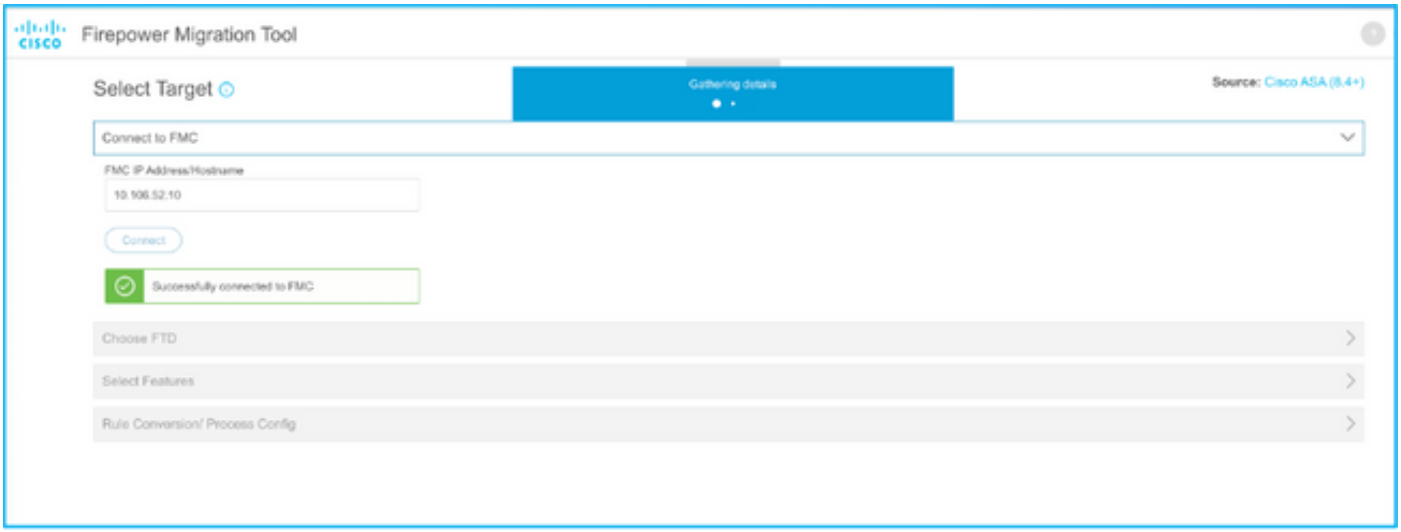


9. 파일이 업로드되면 이미지에 표시된 것처럼 요약을 제공하는 요소를 구문 분석합니다.

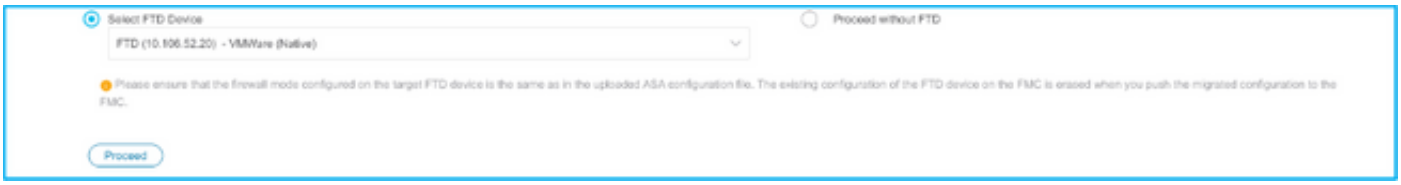
10. ASA 구성을 마이그레이션할 FMC IP 및 로그인 자격 증명을 입력합니다. 워크스테이션에서 FMC IP에 연결할 수 있는지 확인합니다.



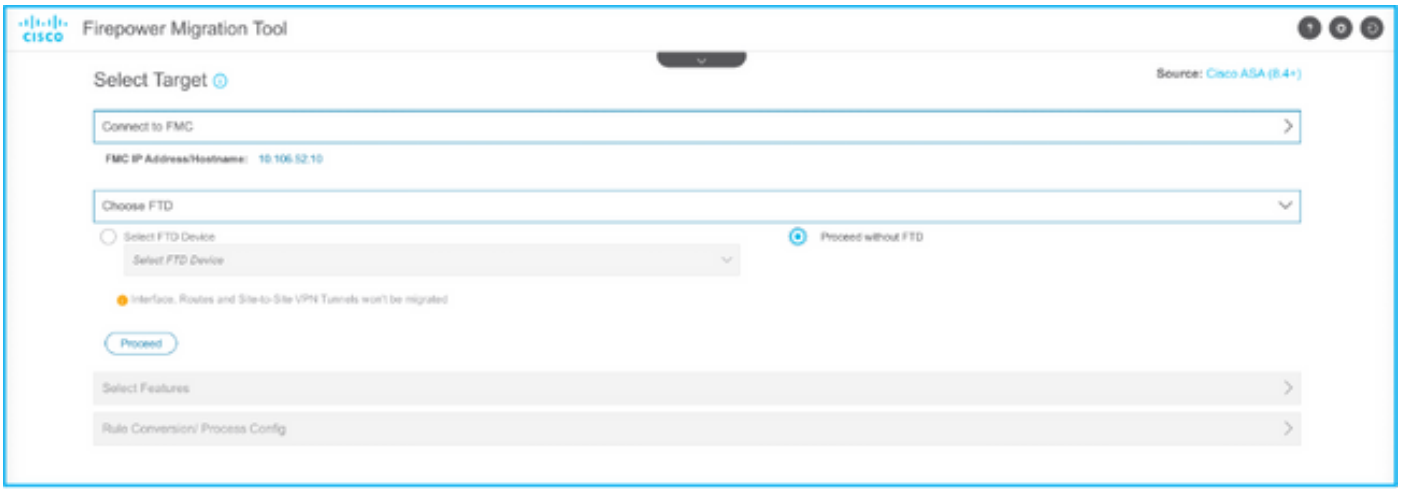
11. FMC가 연결되면 그 아래에 관리되는 FTD가 표시됩니다.



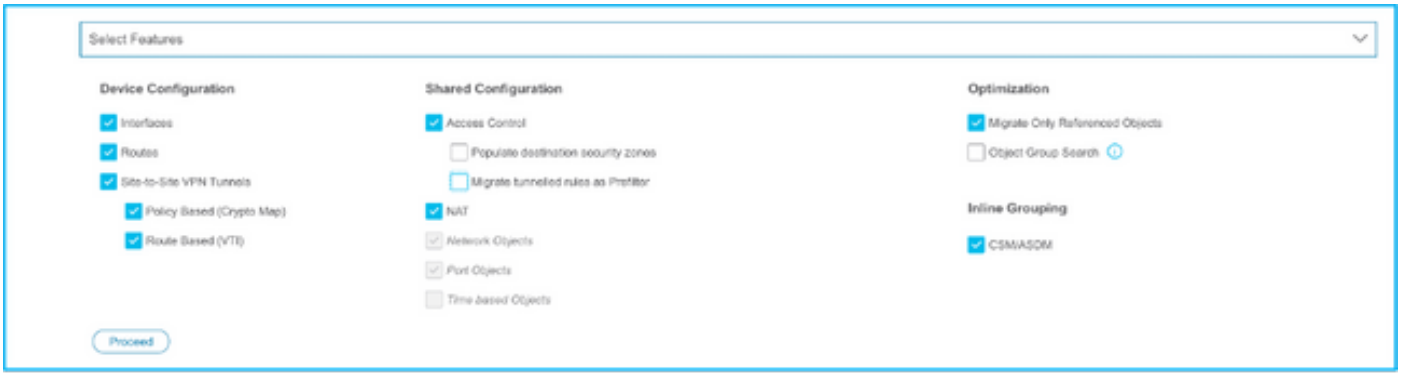
12. ASA 컨피그레이션의 마이그레이션을 수행할 FTD를 선택합니다.



참고: FTD 디바이스를 선택하는 것이 좋습니다. 그렇지 않으면 인터페이스, 경로 및 Site-to-Site VPN 컨피그레이션을 수동으로 수행해야 합니다.

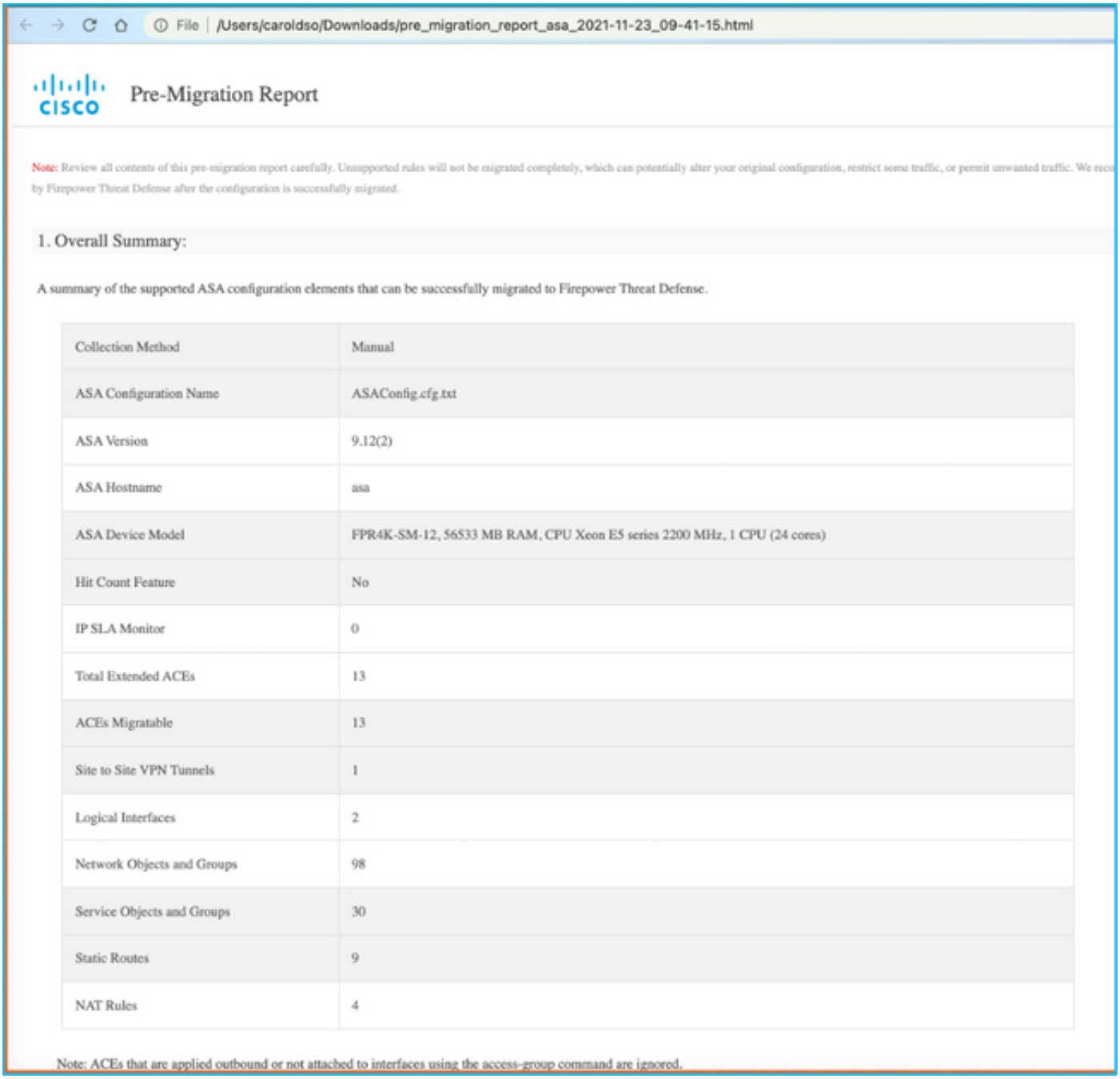


13. 이미지에 표시된 대로 마이그레이션해야 하는 기능을 선택합니다.



14. **변환 시작**을 선택하여 FTD 구성과 관련된 요소를 채우는 사전 마이그레이션을 시작합니다.

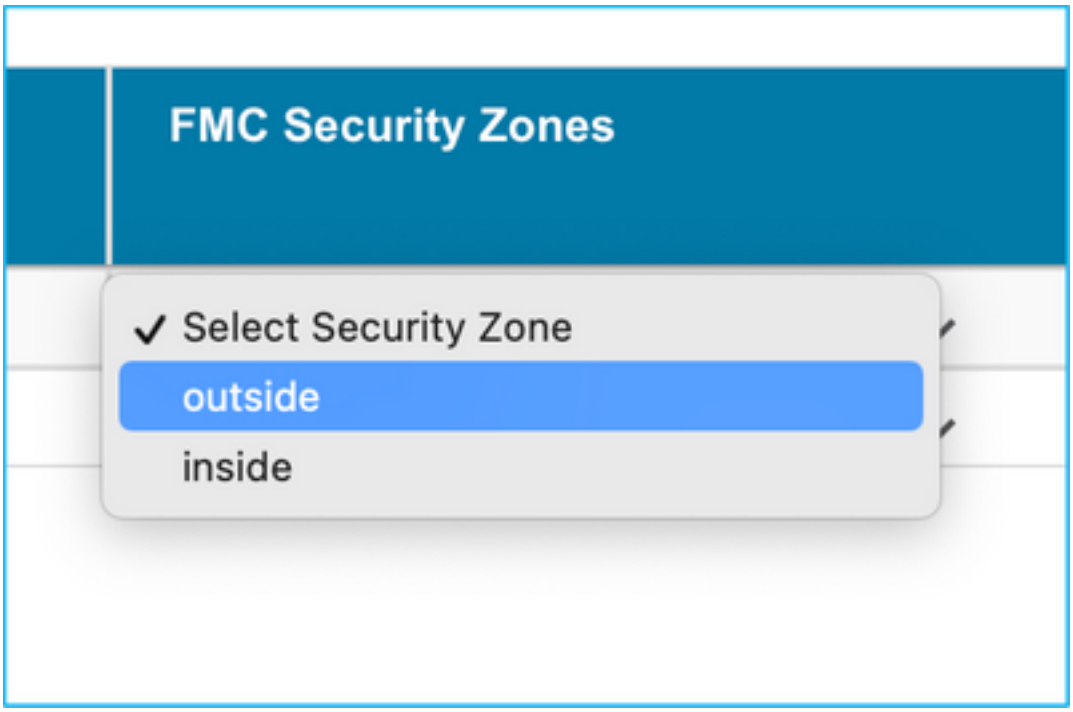
15. 이미지에 표시된 대로 마이그레이션 전 보고서를 보려면 이전에 표시된 **보고서 다운로드**를 클릭합니다.



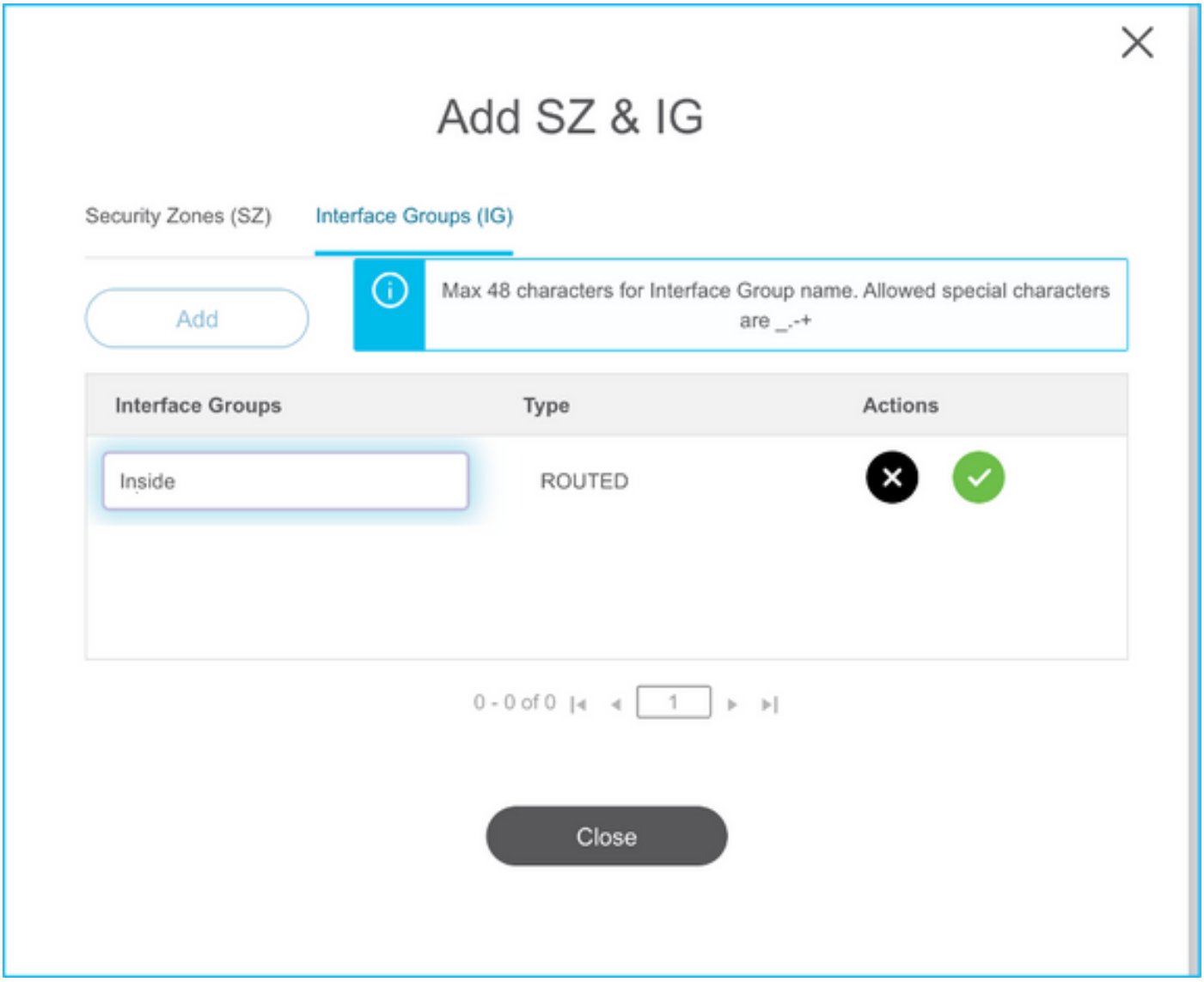
16. 이미지에 표시된 대로 필요에 따라 ASA 인터페이스를 FTD 인터페이스에 매핑합니다.

17. 보안 영역 및 인터페이스 그룹을 FTD 인터페이스에 할당합니다.

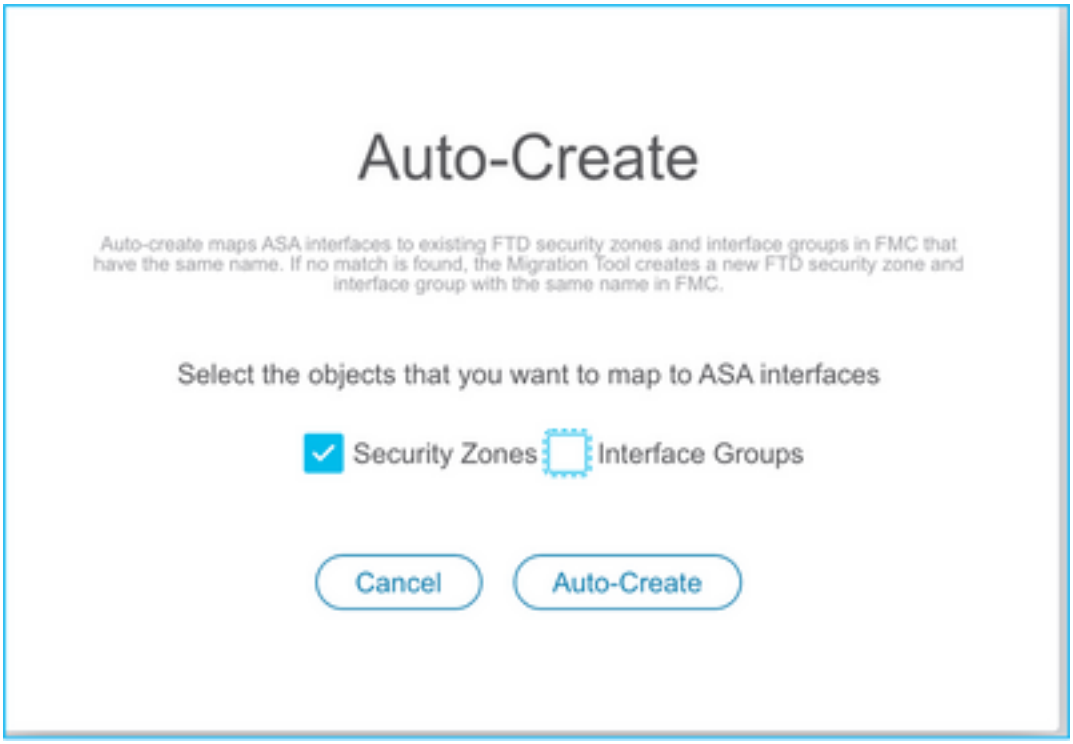
A. FMC에 이미 생성된 보안 영역 및 인터페이스 그룹이 있는 경우 필요에 따라 선택할 수 있습니다.



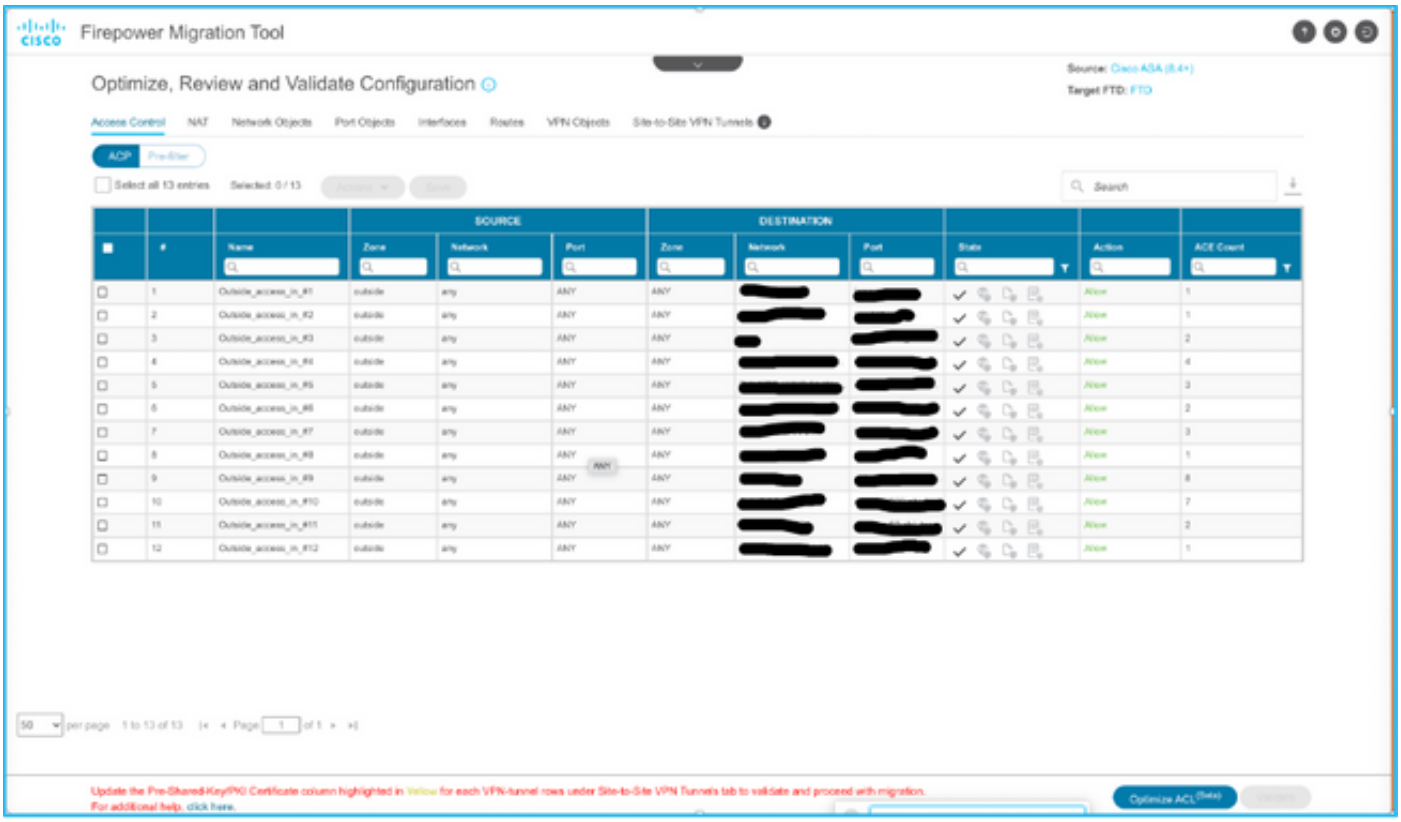
B. 보안 영역 및 인터페이스 그룹을 생성해야 하는 경우 이미지에 표시된 대로 **Add SZ & IG(SZ 및 IG 추가)를** 클릭합니다.



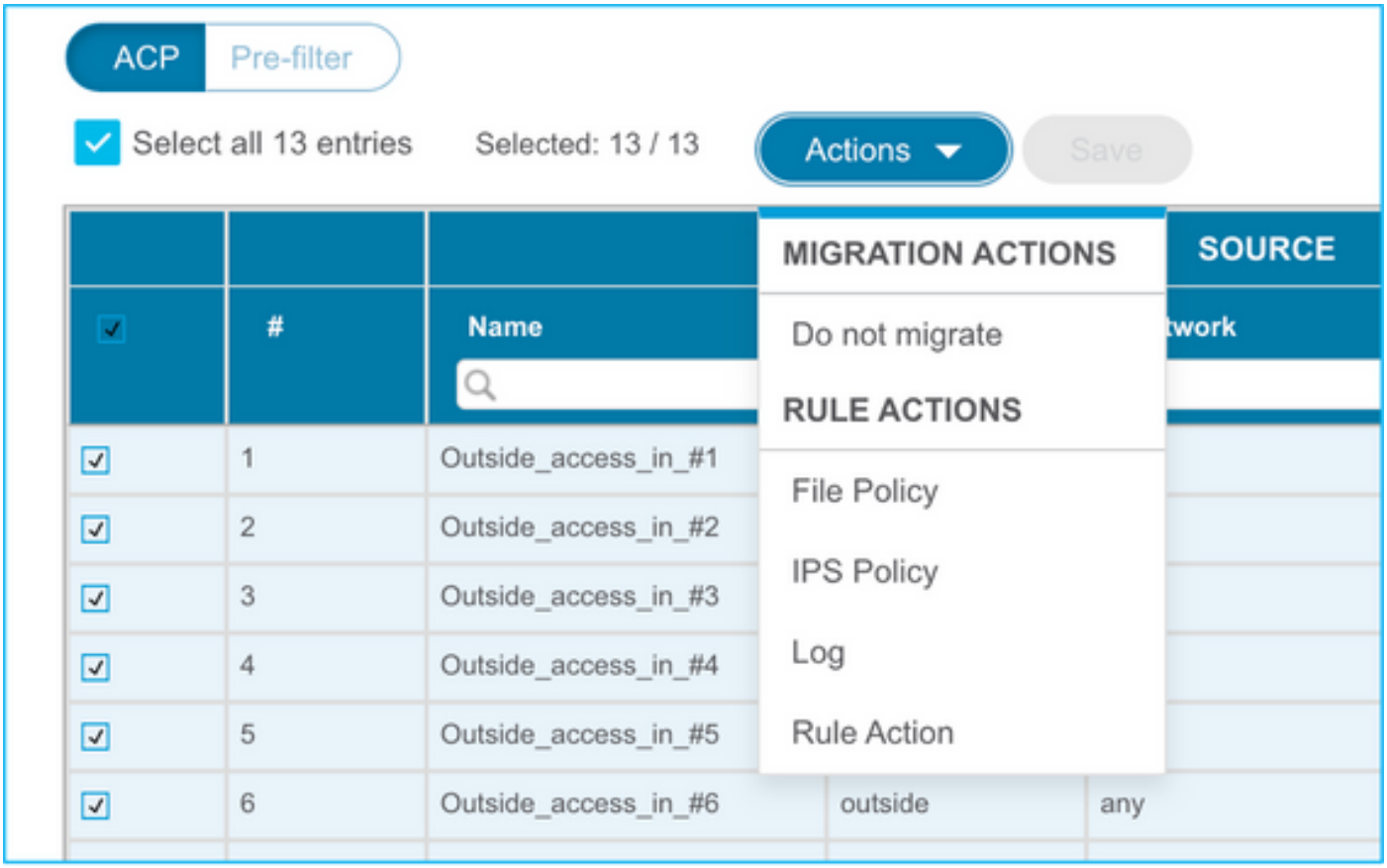
C. 그렇지 않으면 각각 이름이 **ASA 논리적 interface_sz** 및 **ASA 논리적 interface_ig**인 보안 영역 및 인터페이스 그룹을 생성하는 **자동 생성** 옵션으로 이동할 수 있습니다.



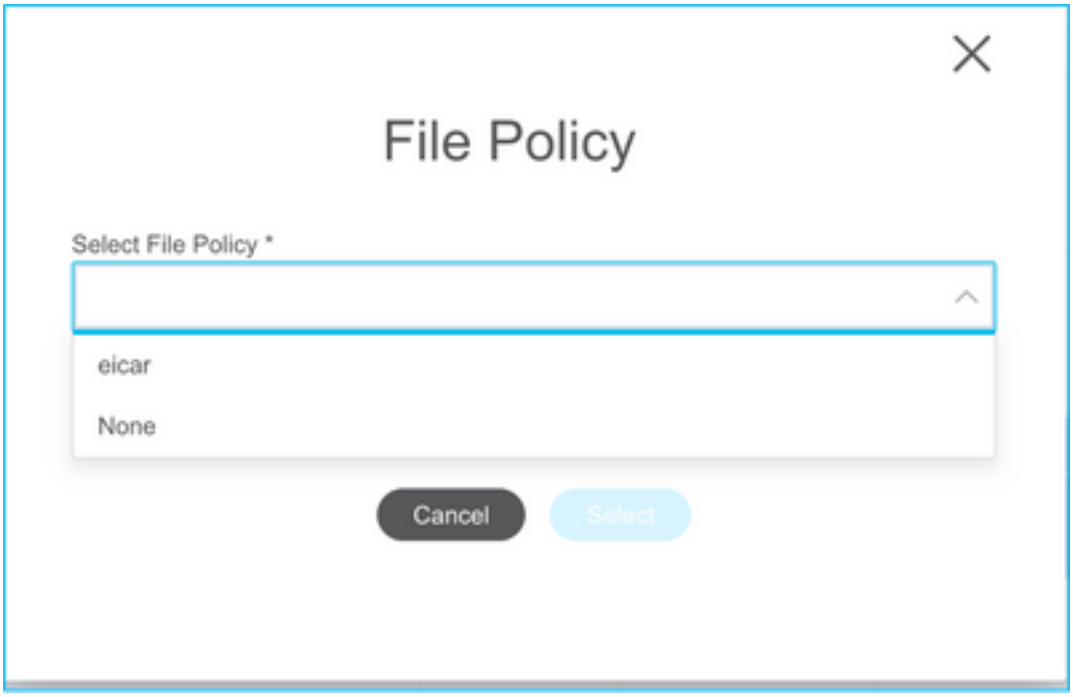
18. 생성된 각 FTD 요소를 검토하고 검증합니다. 경보는 이미지에 표시된 빨간색으로 표시됩니다.



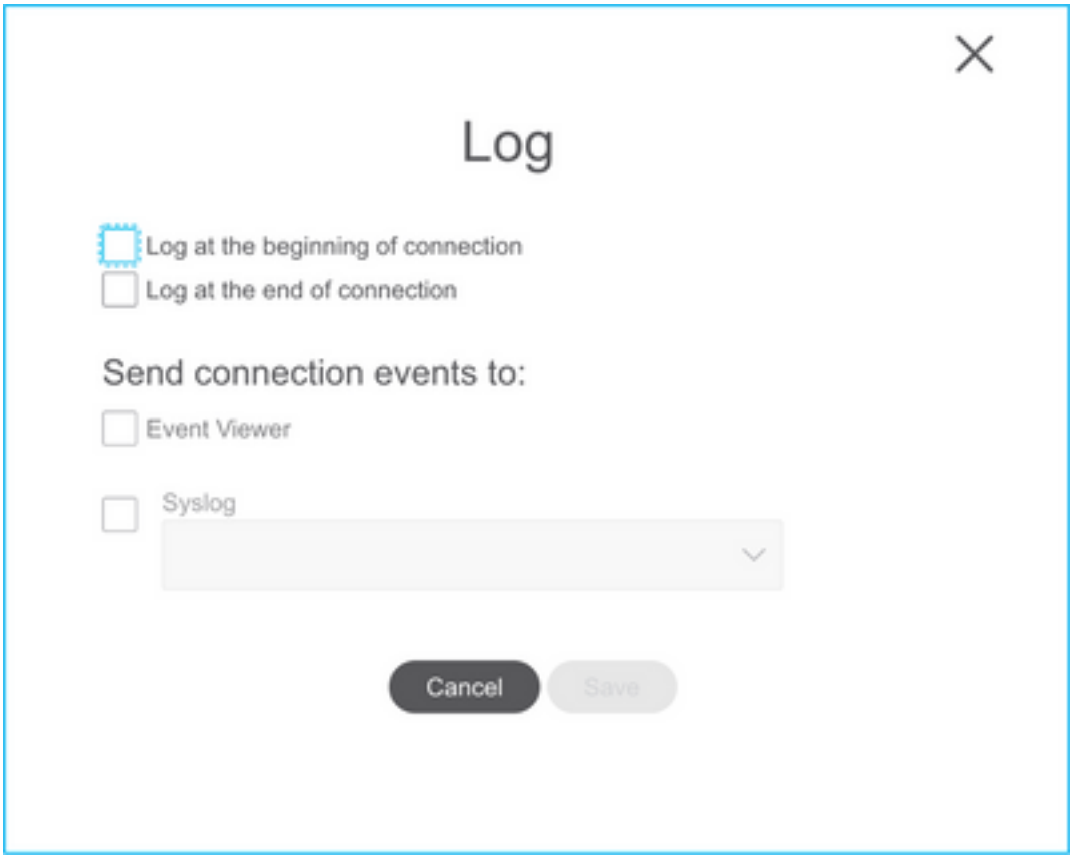
19. 규칙을 편집하려면 이미지에 표시된 대로 마이그레이션 작업을 선택할 수 있습니다. 이 단계에서는 파일 및 IPS 정책을 추가하는 FTD 기능을 수행할 수 있습니다.



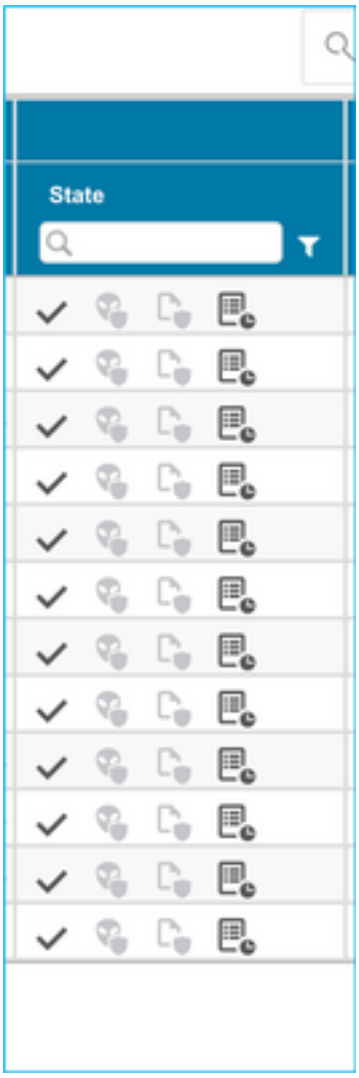
참고: 파일 정책이 FMC에 이미 존재하는 경우 이미지에 표시된 대로 채워집니다. 기본 정책과 함께 IPS 정책에 대해서도 마찬가지입니다.



필요한 규칙에 대해 로그 컨피그레이션을 수행할 수 있습니다. 이 단계에서 FMC에 존재하는 Syslog 서버 컨피그레이션을 선택할 수 있습니다.

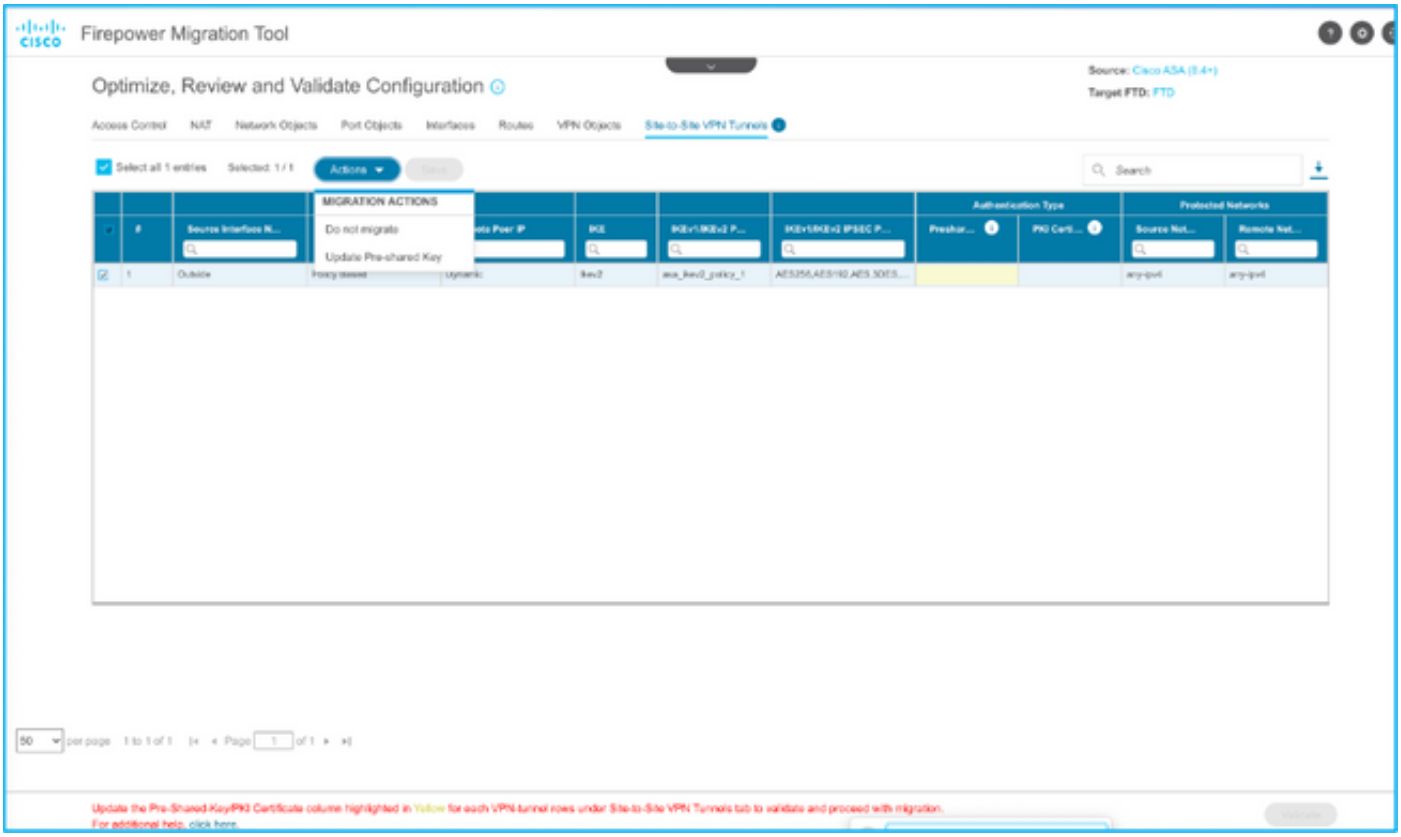


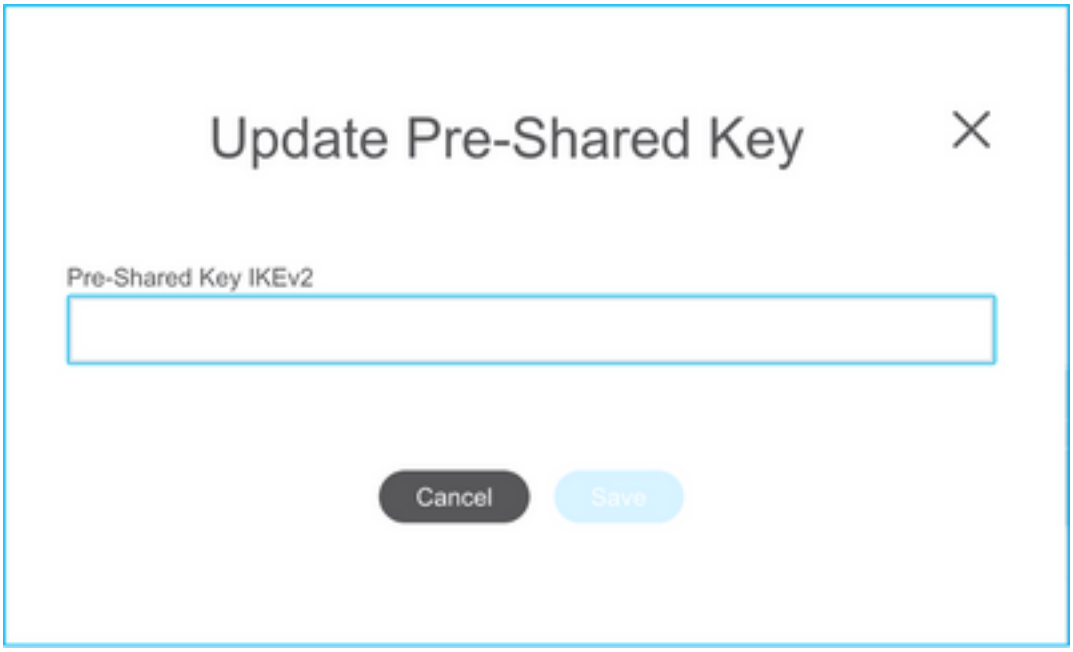
선택한 규칙 작업은 각 규칙에 따라 강조 표시됩니다.



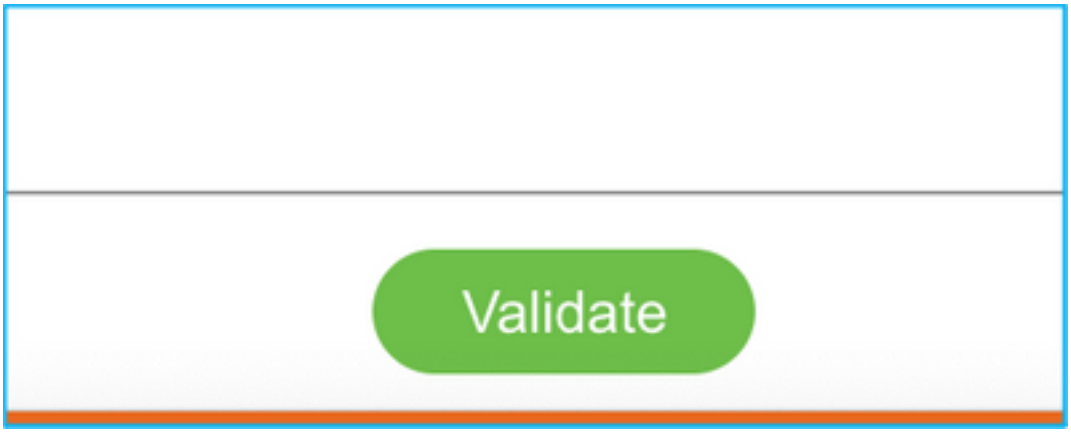
20. 마찬가지로 구성에 따라 NAT, 네트워크 객체, 포트 객체, 인터페이스, 경로, VPN 객체, 사이트 대 사이트 VPN 터널 및 기타 요소를 단계별로 검토할 수 있습니다.

참고: ASA 컨피그레이션 파일에서 복사되지 않으므로 사전 공유 키를 업데이트하라는 경고가 이미지에 표시된 대로 표시됩니다. Actions(**작업) > Update Pre-Shared Key(사전 공유 키 업데이트)**를 선택하여 값을 입력합니다.

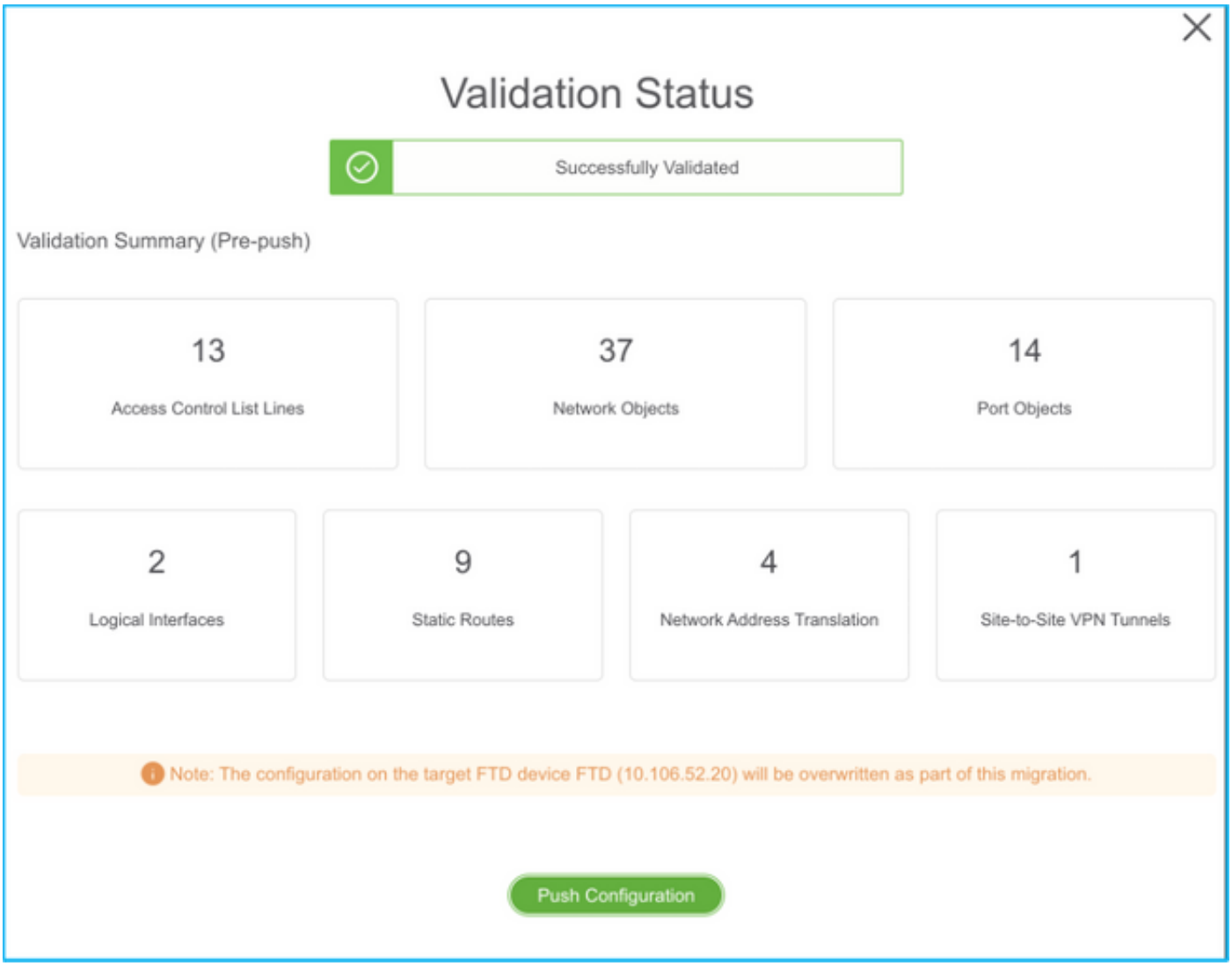


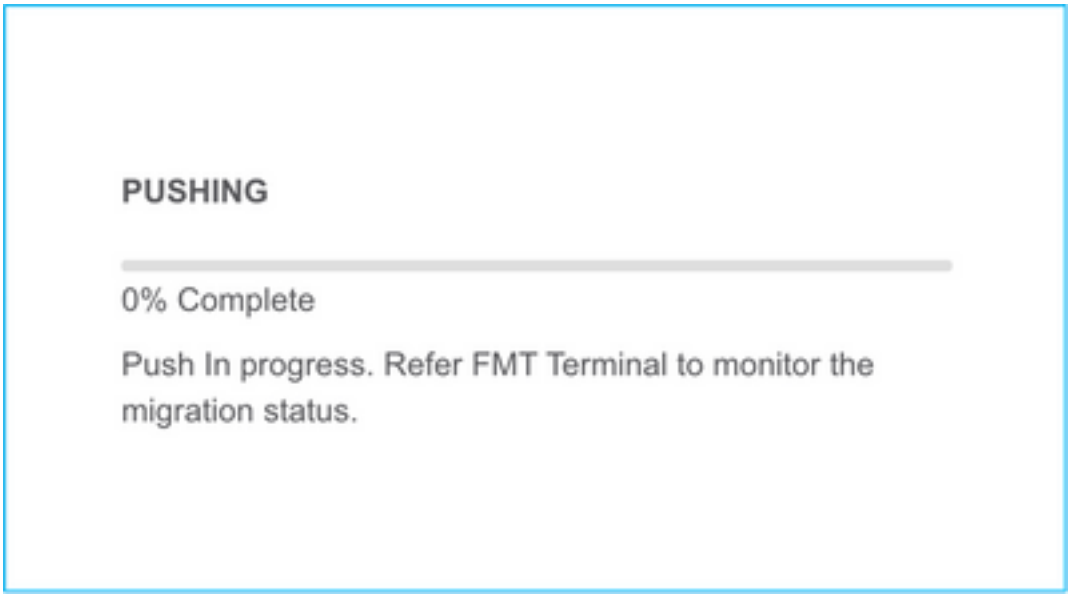


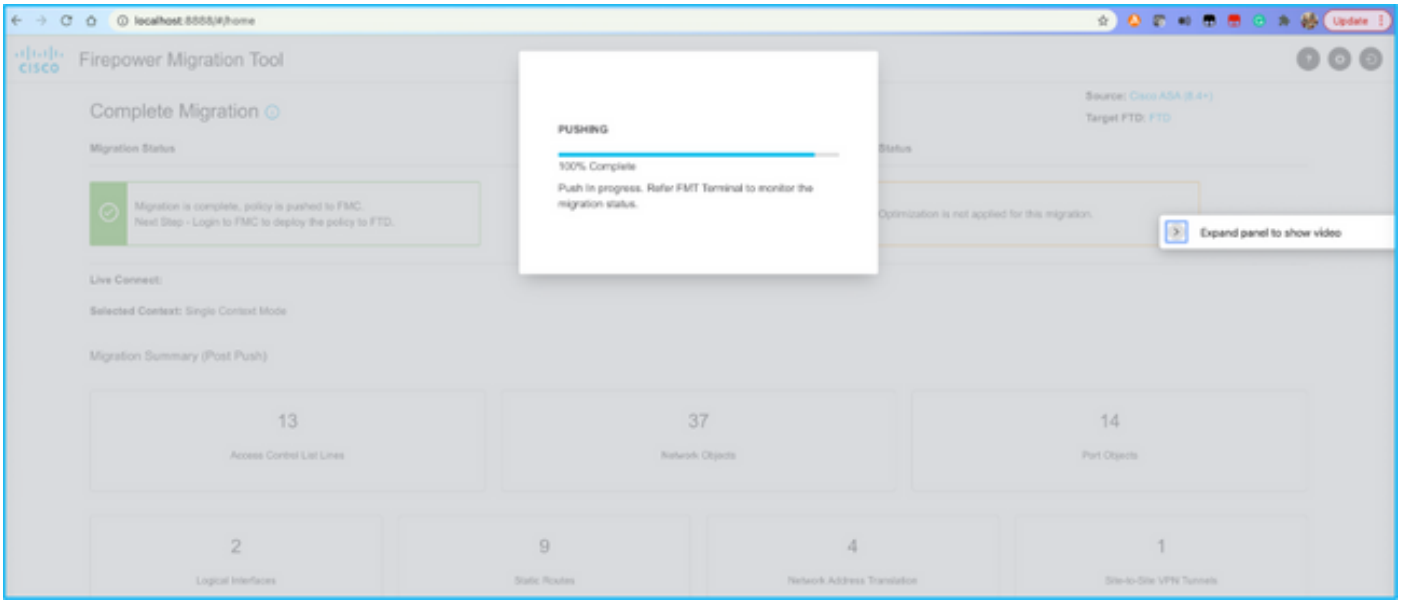
21. 마지막으로, 이미지에 표시된 화면 오른쪽 하단에 있는 **검증** 아이콘을 클릭합니다.



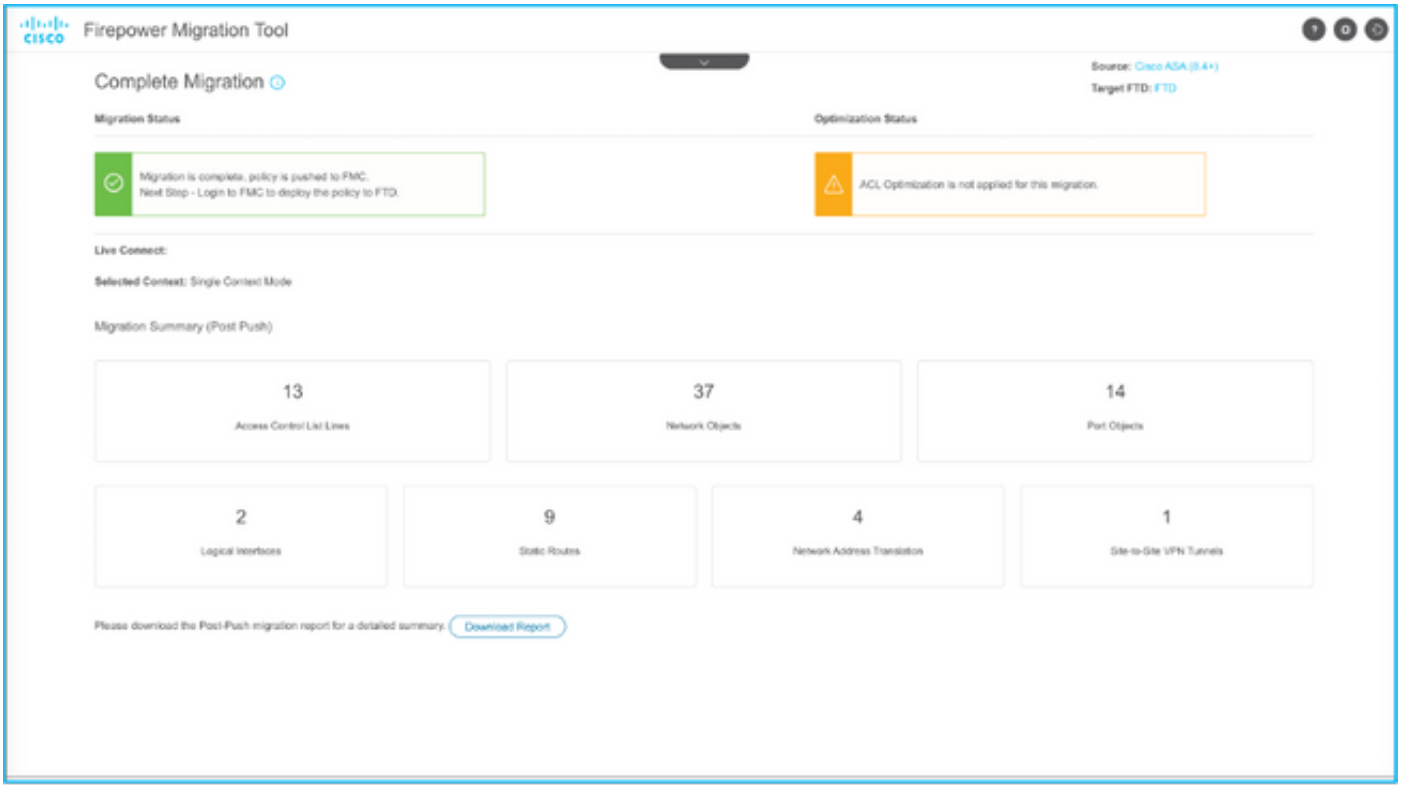
22. 검증이 성공되면 이미지에 표시된 대로 **Push Configuration**을 클릭합니다.



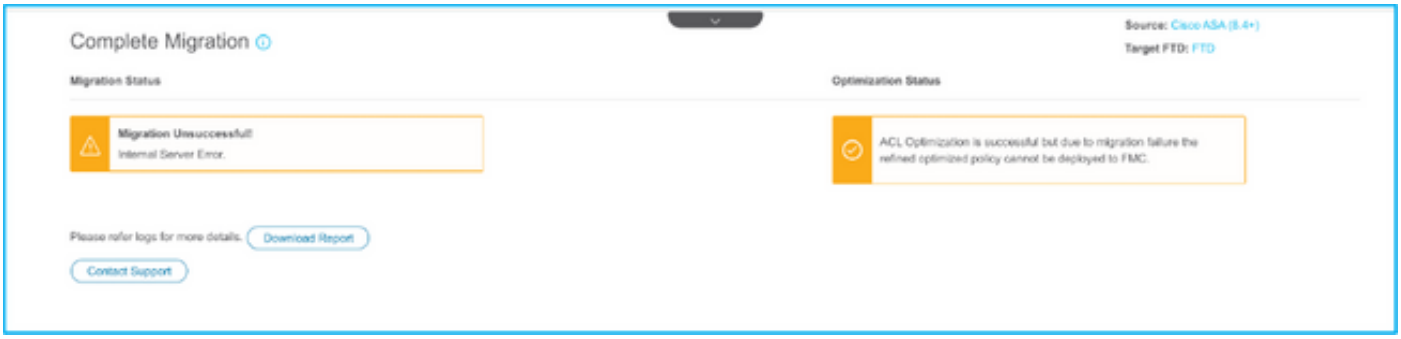




23. 마이그레이션에 성공하면 표시되는 메시지가 이미지에 표시됩니다.



참고: 마이그레이션이 실패하면 **Download Report(보고서 다운로드)**를 클릭하여 마이그레이션 후 보고서를 봅니다.

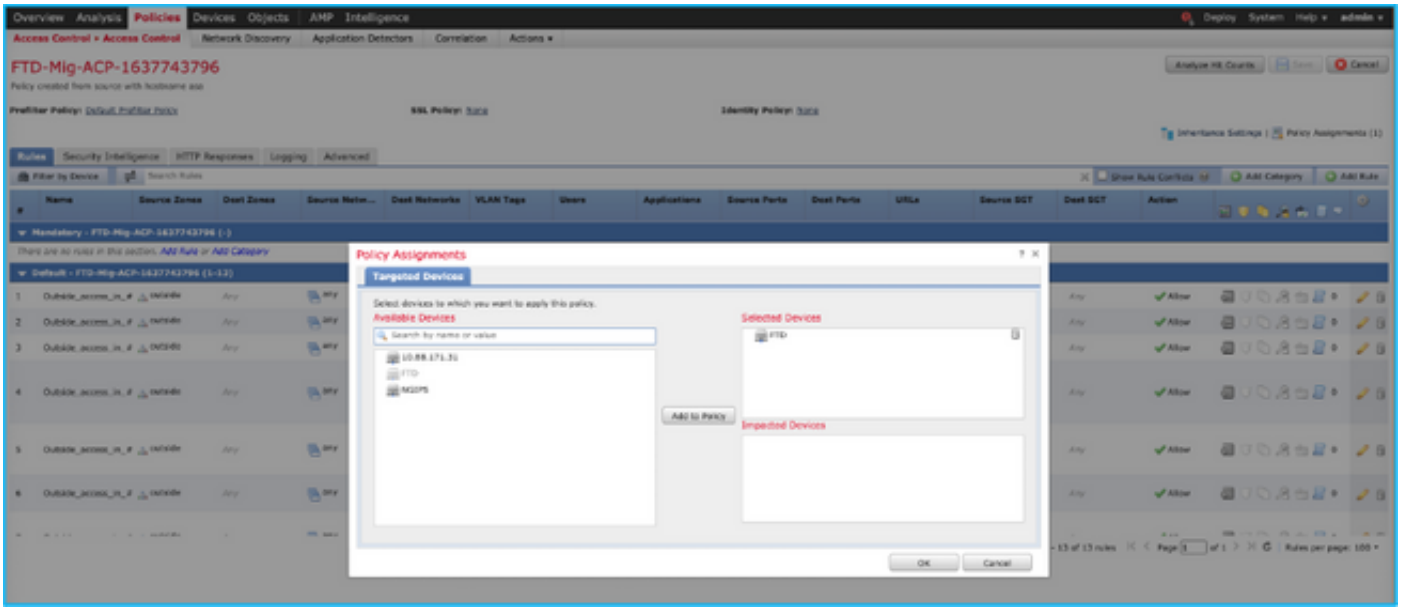


다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

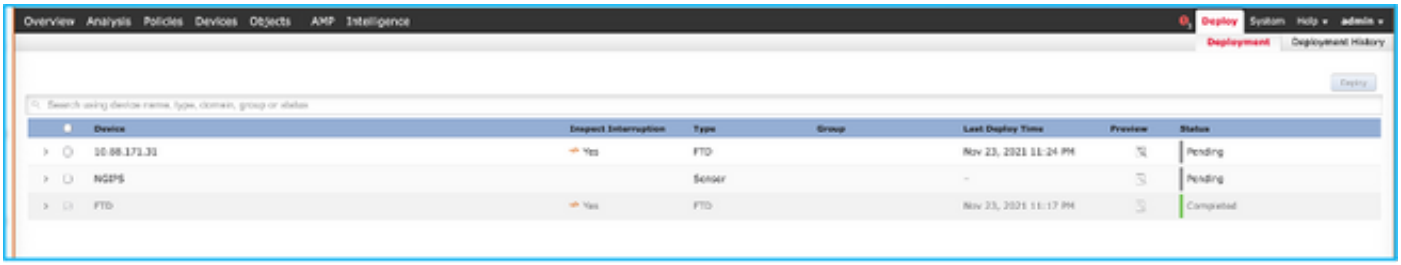
FMC에 대한 검증

1. Policies(**정책) > Access Control(액세스 제어) > Access Control Policy(액세스 제어 정책) > Policy Assignment(정책 할당)로 이동하여** 선택한 FTD가 채워졌는지 확인합니다.



참고: 마이그레이션 액세스 제어 정책에는 접두사 FTD-Mig-ACP가 있는 이름이 있습니다. 단계 2.8에서 FTD를 선택하지 않은 경우 FMC에서 FTD를 선택해야 합니다.

2. 정책을 FTD로 푸시합니다. 이미지에 표시된 대로 **Deploy(구축) > Deployment(구축) > FTD Name(FTD 이름) > Deploy(구축)**로 이동합니다.



Firepower Migration Tool과 관련된 알려진 버그

- Cisco 버그 ID CSCwa56374 - FMT 툴이 영역 매핑 페이지에서 중단되며 메모리 사용률이 높습니다.
- Cisco 버그 ID CSCvz88730 - FTD 포트 채널 관리 인터페이스 유형에 대한 인터페이스 푸시 실패
- Cisco 버그 ID CSCvx21986 - 대상 플랫폼으로의 포트 채널 마이그레이션 - 가상 FTD는 지원되지 않습니다.
- Cisco 버그 ID CSCvy63003 - FTD가 이미 클러스터의 일부인 경우 마이그레이션 툴에서 인터페이스 기능을 비활성화해야 합니다.
- Cisco 버그 ID CSCvx08199 - 애플리케이션 참조가 50을 초과하는 경우 ACL을 분할해야 합니다.

관련 정보

- 방화벽 마이그레이션 툴을 사용하여 ASA 방화벽을 위협 방어로 마이그레이션
- 기술 지원 및 문서 – Cisco Systems