FMT를 사용하여 ASA를 FTD(Firepower Threat Defense)로 마이그레이션

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)를 Cisco Firepower 위협 디바이스로 마이그레이션하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 Cisco FTD(Firewall Threat Defense) 및 ASA(Adaptive Security Appliance)에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMT(Firepower 마이그레이션 도구) v7.0.1을 사용하는 Mac OS
- ASA(Adaptive Security Appliance) v9.16(1)
- FMCv(Secure Firewall Management Center) v7.4.2
- FTDv(Secure Firewall Threat Defense Virtual) v7.4.1

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.

개요

이 문서의 구체적인 요구 사항은 다음과 같습니다.

- Cisco ASA(Adaptive Security Appliance) 버전 8.4 이상
- FMCv(Secure Firewall Management Center) 버전 6.2.3 이상

Firewall Migration Tool은 다음 디바이스 목록을 지원합니다.

- Cisco ASA(8.4+)
- Cisco ASA(9.2.2+) with FPS
- Cisco Secure Firewall Device Manager(7.2+)
- 검사점(r75-r77)
- Check Point(r80)
- Fortinet(5.0+)

· Palo Alto Networks(6.1+)

배경 정보

ASA 컨피그레이션을 마이그레이션하기 전에 다음 작업을 실행합니다.

ASA 컨피그레이션 파일 가져오기

ASA 디바이스를 마이그레이션하려면 단일 컨텍스트에 show running-config를 사용하거나 다중 컨텍스트 모드에 show tech-support를 사용하여 컨피그레이션을 가져온 다음 .cfg 또는 .txt 파일로 저장하고 Secure Firewall 마이그레이션 도구를 사용하여 컴퓨터에 전송합니다.

ASA에서 PKI 인증서 내보내기 및 Management Center로 가져오기

소스 ASA 컨피그레이션에서 CLI를 통해 키를 사용하여 PKCS12 파일로 PKI 인증서를 내보내려면 다음 명령을 사용합니다.
ASA(config)#crypto <trust-point-name> pkcs12 <passphrase>를 내보낼 수 있습니다.
그런 다음 PKI 인증서를 관리 센터(Object Management PKI Objects)로 가져옵니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 PKI 객체를 참조하십시오.

AnyConnect 패키지 및 프로파일 검색

AnyConnect 프로파일은 선택 사항이며 관리 센터 또는 Secure Firewall 마이그레이션 툴을 통해 업로드할 수 있습니다.

소스 ASA에서 FTP 또는 TFTP 서버로 필요한 패키지를 복사하려면 다음 명령을 사용합니다.

<소스 파일 위치:/소스 파일 이름> <대상> 복사

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Anyconnect 패키지 복사의 예.

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- 외부 브라우저 패키지 복사의 예.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Hostscan 패키지 복사의 예.

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Dap.xml 복사의 예

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Data.xml 복사의 예

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Anyconnect 프로파일 복사의 예.

다운로드한 패키지를 관리 센터로 가져옵니다(Object Management > VPN > AnyConnect File).

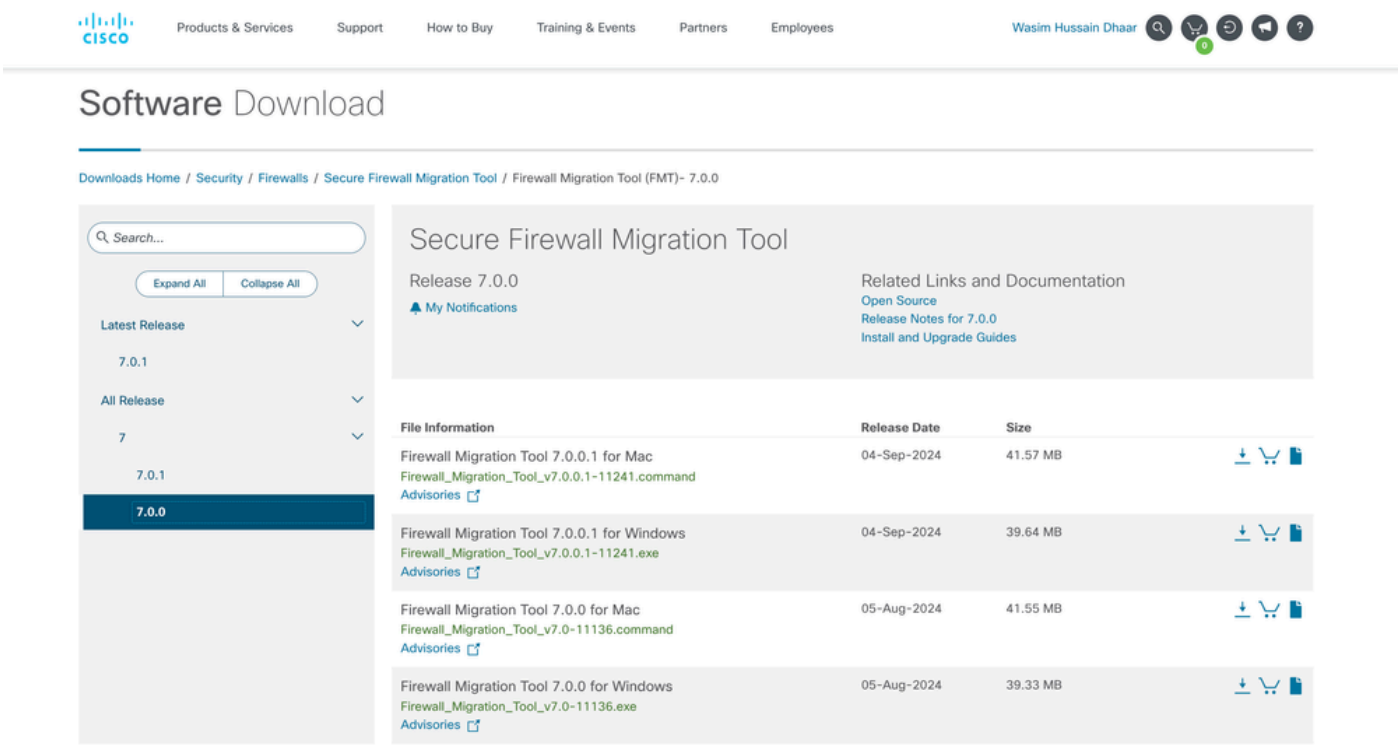
a-Dap.xml 및 Data.xml은 Review and Validate(검토 및 검증) > Remote Access VPN(원격 액세스 VPN) > AnyConnect File(AnyConnect 파일) 섹션의 Secure Firewall(보안 방화벽) 마이그레이션 툴에서 관리 센터로 업로드해야 합니다.

b-AnyConnect 프로필은 관리 센터에 직접 업로드하거나 Review and Validate(검토 및 검증) > Remote Access VPN(원격 액세스 VPN) > AnyConnect File(AnyConnect 파일) 섹션의 Secure Firewall 마이그레이션 툴을 통해 업로드할 수 있습니다.

구성

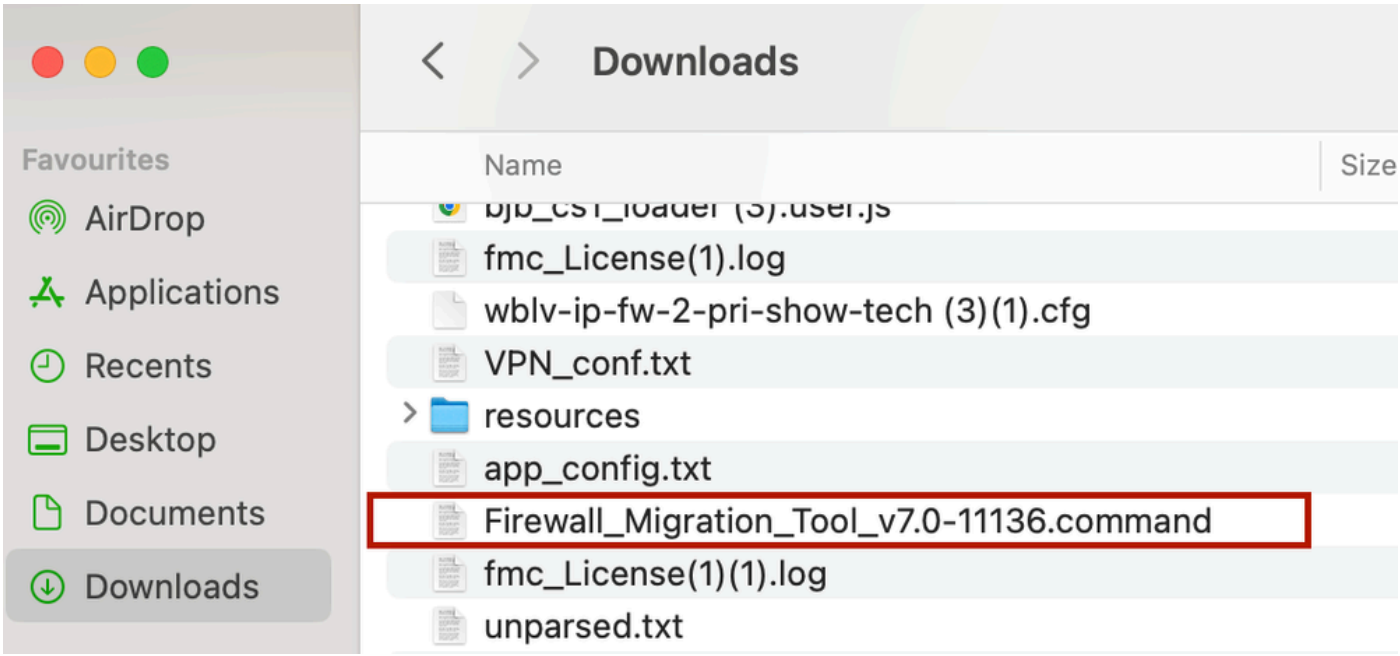
컨피그레이션 단계:

1.다운로드 cisco Software Central의 최신 Firepower 마이그레이션 툴:

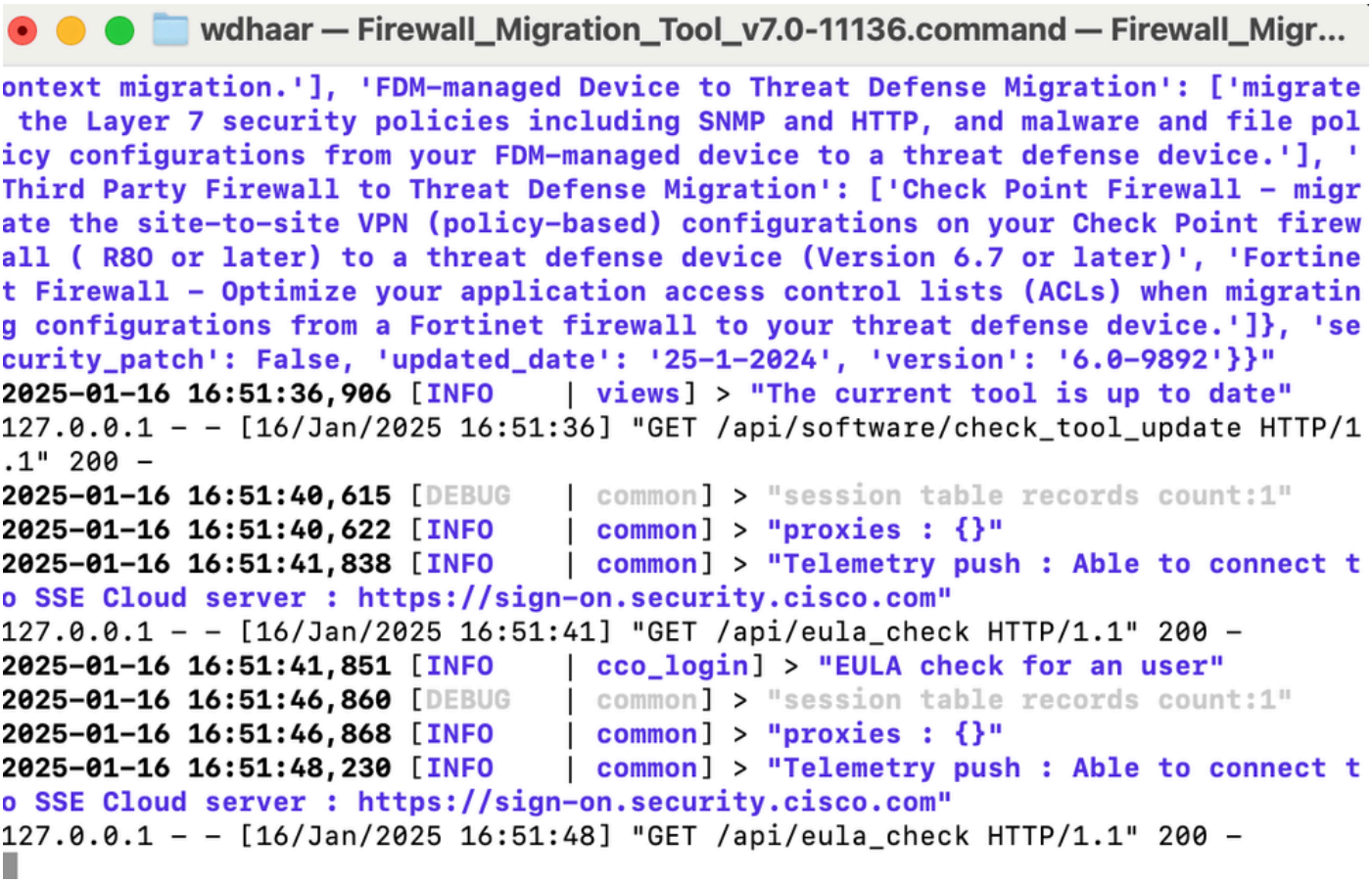


소프트웨어 다운로드

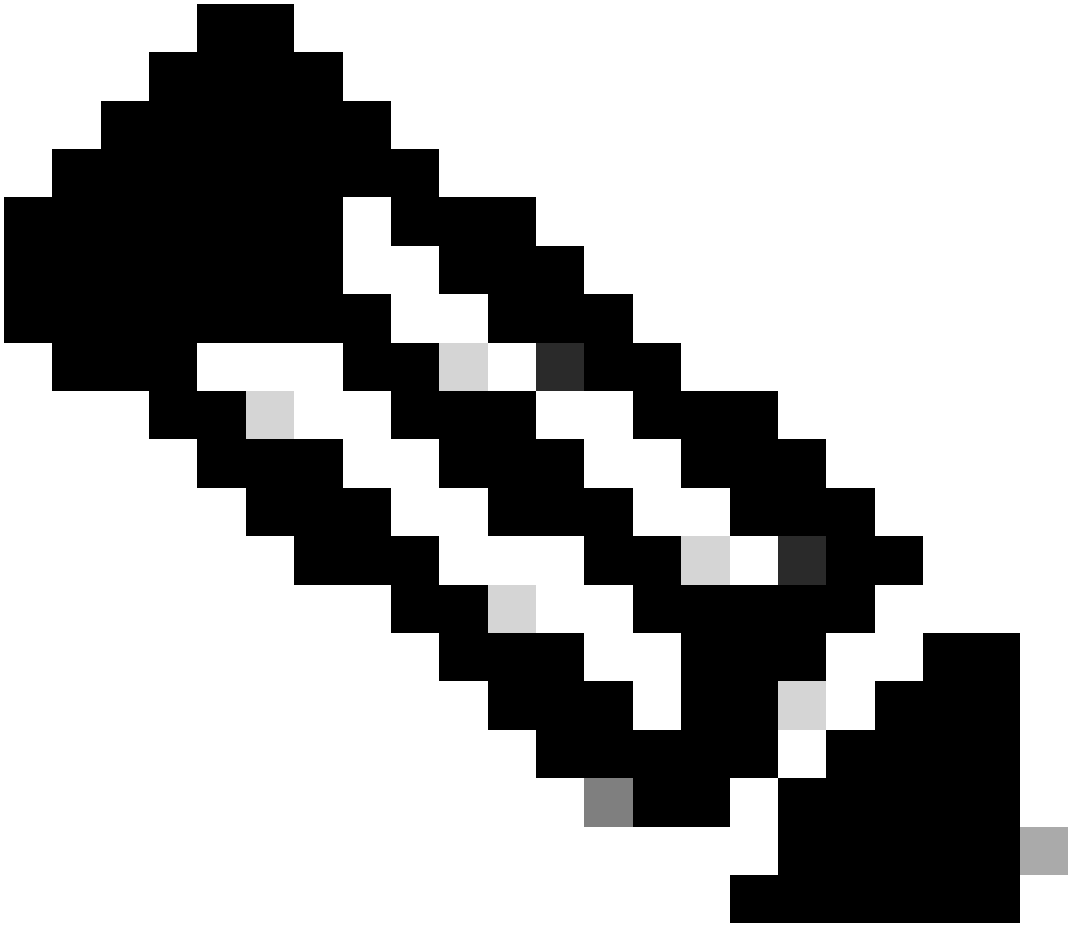
2. 이전에 컴퓨터에 다운로드한 파일을 클릭합니다.



파일


wdhaar — Firewall_Migration_Tool_v7.0-11136.command — Firewall_Migr...
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate the Layer 7 security policies including SNMP and HTTP, and malware and file policy configurations from your FDM-managed device to a threat defense device.'], 'Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migrate the site-to-site VPN (policy-based) configurations on your Check Point firewall (R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortinet Firewall - Optimize your application access control lists (ACLs) when migrating configurations from a Fortinet firewall to your threat defense device.']}, 'security_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INFO | views] > "The current tool is up to date"
127.0.0.1 - - [16/Jan/2025 16:51:36] "GET /api/software/check_tool_update HTTP/1.1" 200 -
2025-01-16 16:51:40,615 [DEBUG | common] > "session table records count:1"
2025-01-16 16:51:40,622 [INFO | common] > "proxies : {}"
2025-01-16 16:51:41,838 [INFO | common] > "Telemetry push : Able to connect to SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:41] "GET /api/eula_check HTTP/1.1" 200 -
2025-01-16 16:51:41,851 [INFO | cco_login] > "EULA check for an user"
2025-01-16 16:51:46,860 [DEBUG | common] > "session table records count:1"
2025-01-16 16:51:46,868 [INFO | common] > "proxies : {}"
2025-01-16 16:51:48,230 [INFO | common] > "Telemetry push : Able to connect to SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:48] "GET /api/eula_check HTTP/1.1" 200 -

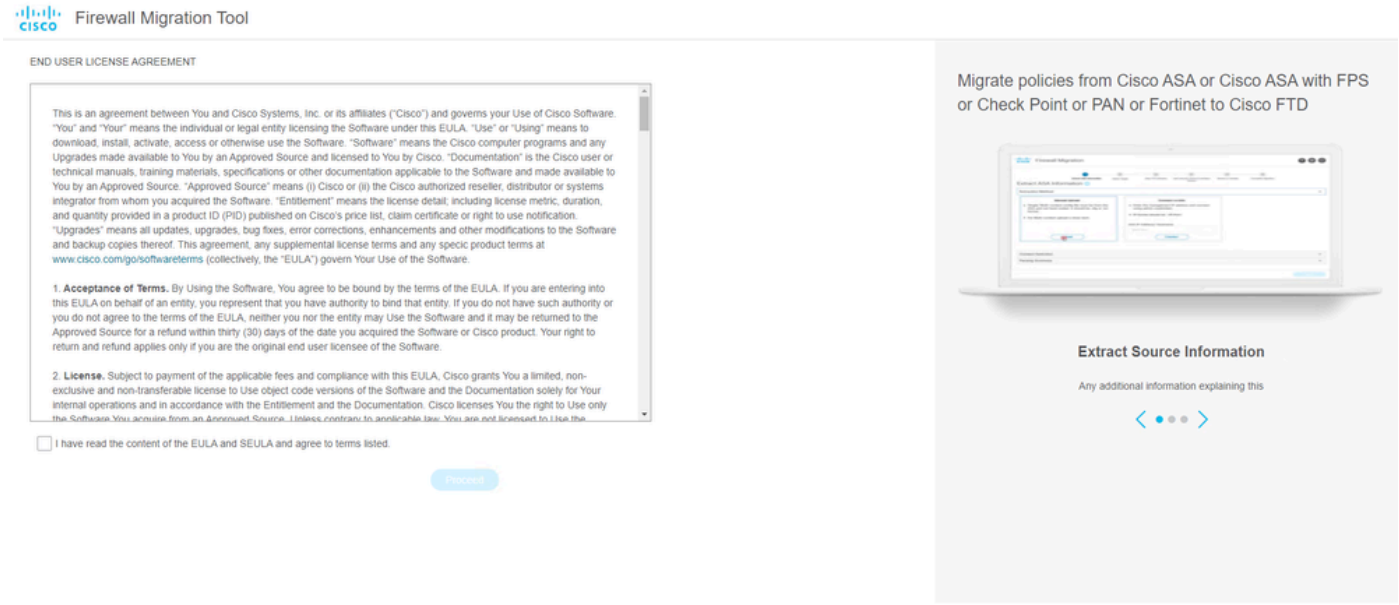
콘솔 로그



참고: 프로그램이 자동으로 열리고 콘솔이 파일을 실행한 디렉토리에 내용을 자동으로 생성합니다.

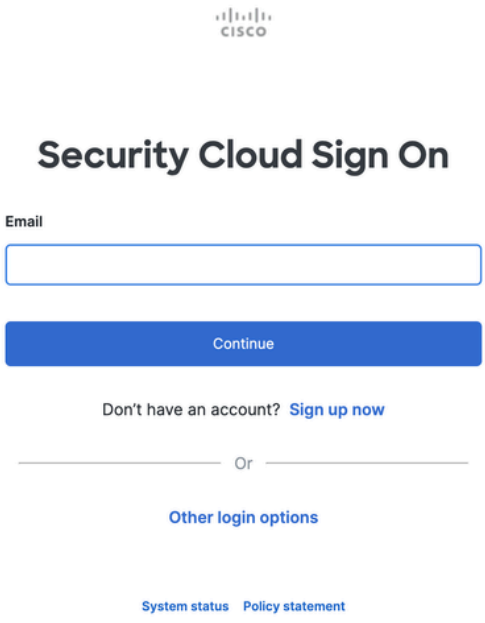
---

3. 프로그램을 실행하면 "End User License Agreement(최종 사용자 사용권 계약)"가 표시된 웹 브라우저가 열립니다.
    1. 약관에 동의하려면 확인란을 선택합니다.
    2. Proceed(진행)를 클릭합니다.



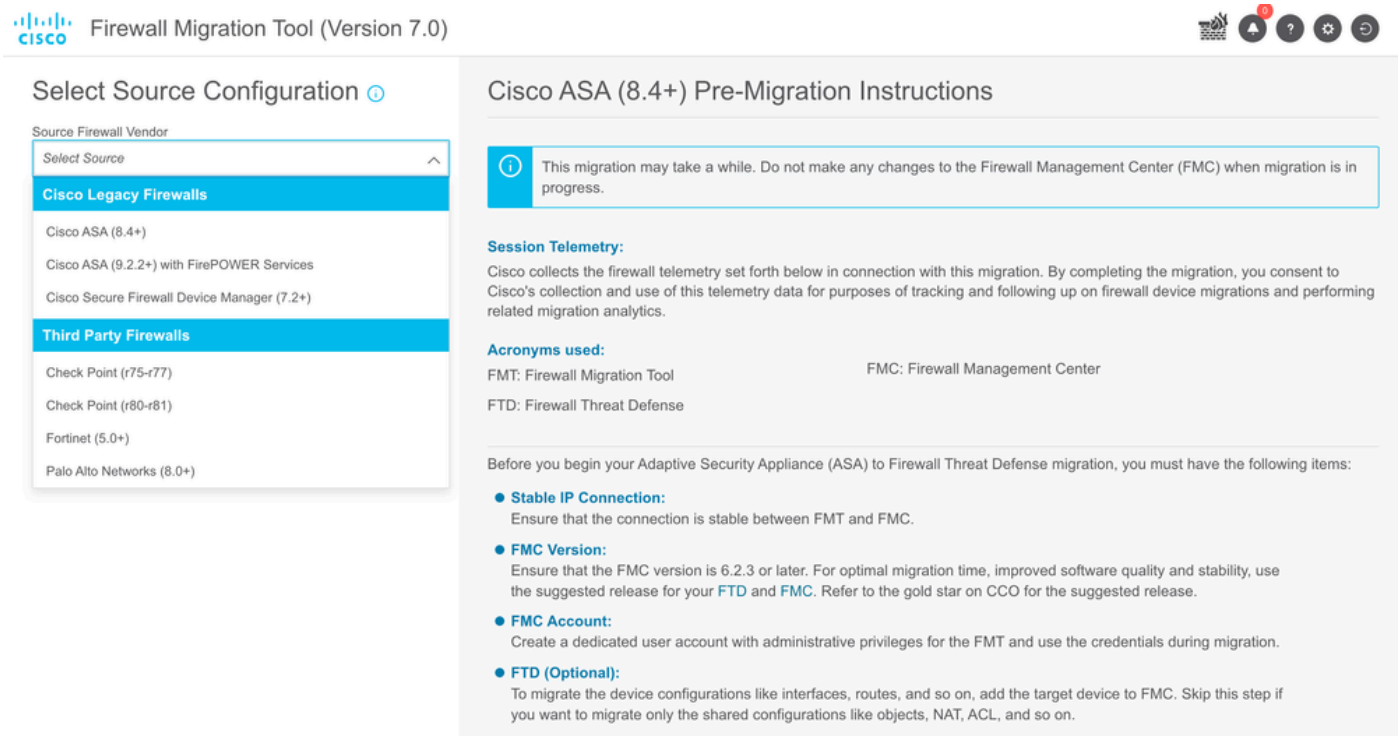
EULA

4. 유효한 CCO 계정을 사용하여 로그인하면 FMT GUI 인터페이스가 웹 브라우저에 나타납니다 .



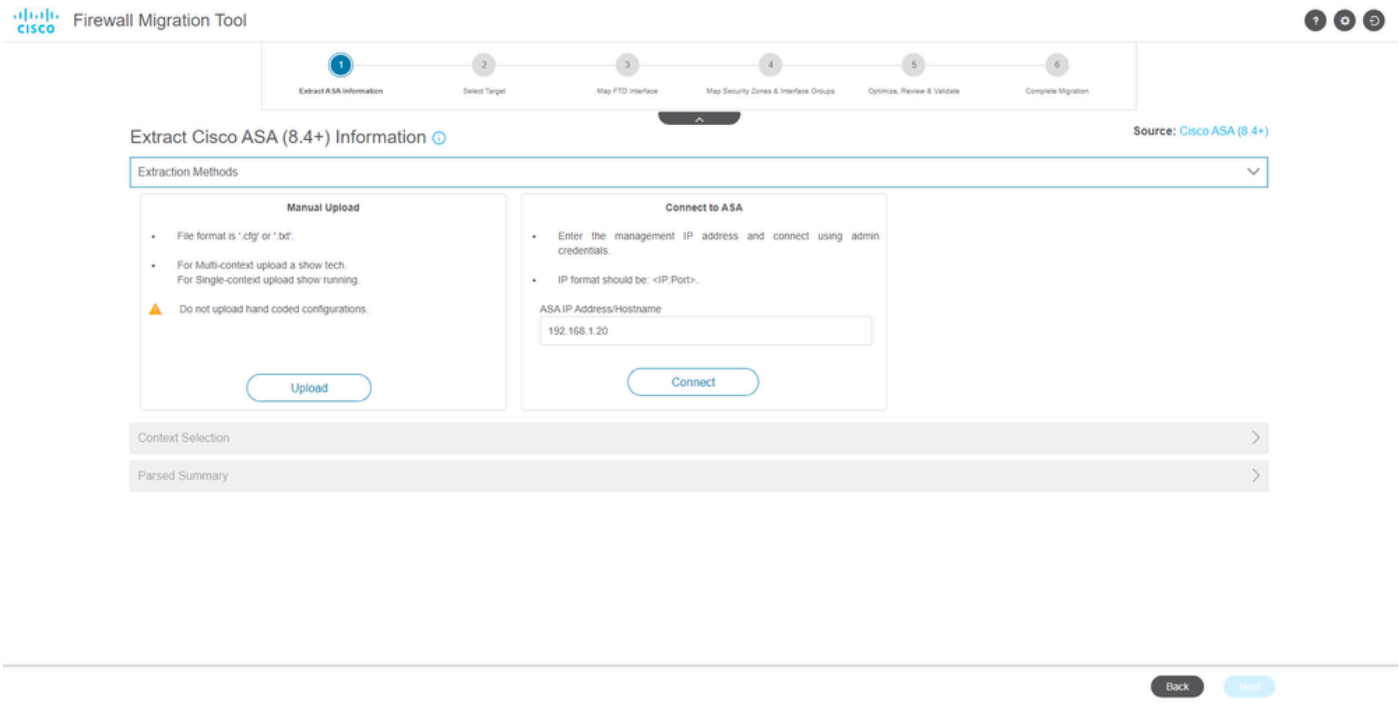
FMT 로그인

5. 마이그레이션할 소스 방화벽을 선택합니다.

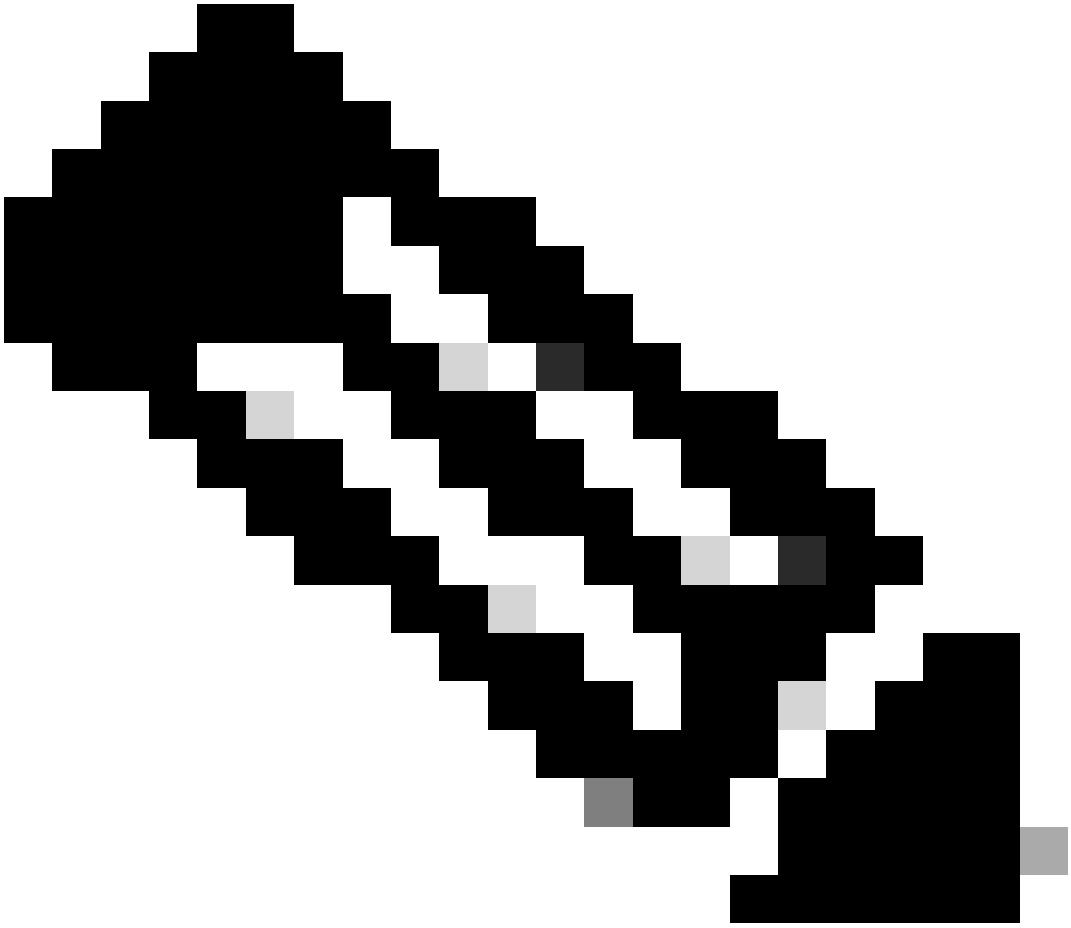


소스 방화벽

6. 컨피그레이션을 가져오는 데 사용할 추출 방법을 선택합니다.
    1. 수동 업로드를 수행하려면 ASA의 **Running Config** 파일을 ".cfg" 또는 ".txt" 형식으로 업로드해야 합니다.
    2. ASA에 연결하여 방화벽에서 직접 컨피그레이션을 추출합니다.

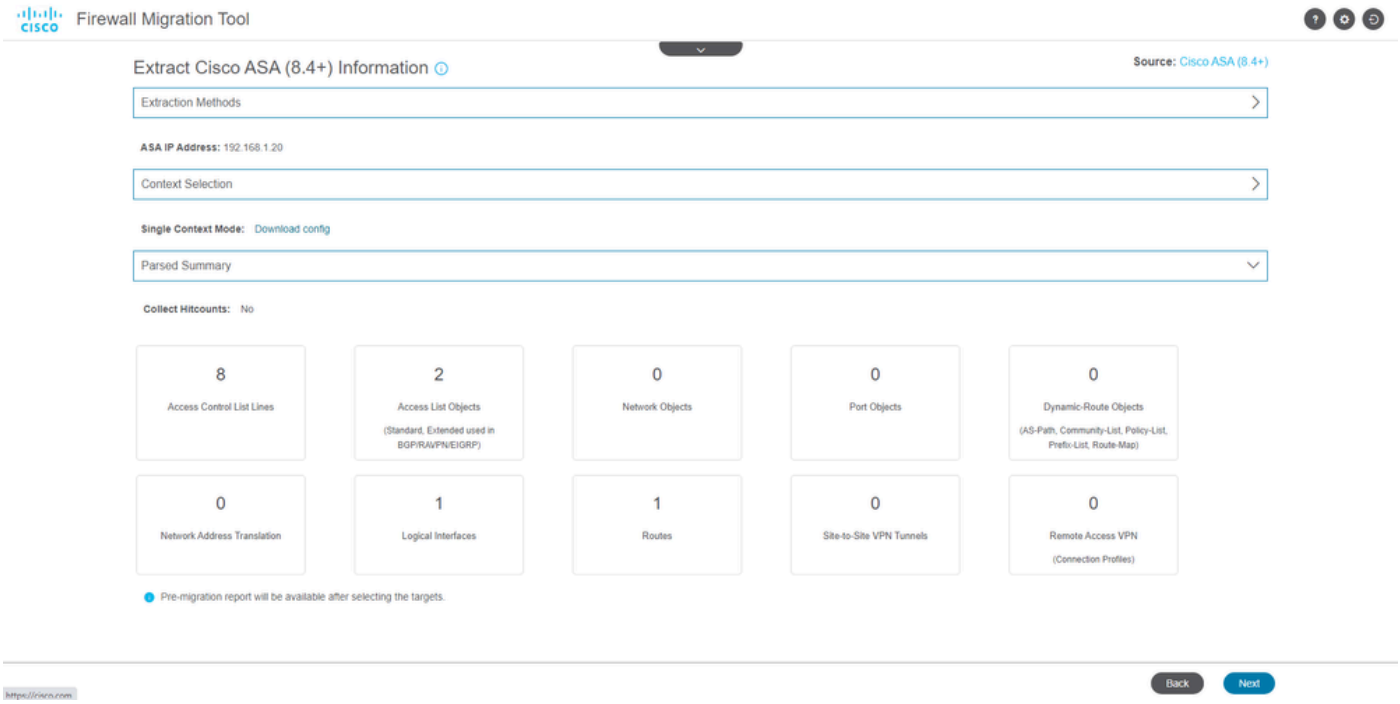


추출



참고: 이 예에서는 ASA에 직접 연결합니다.

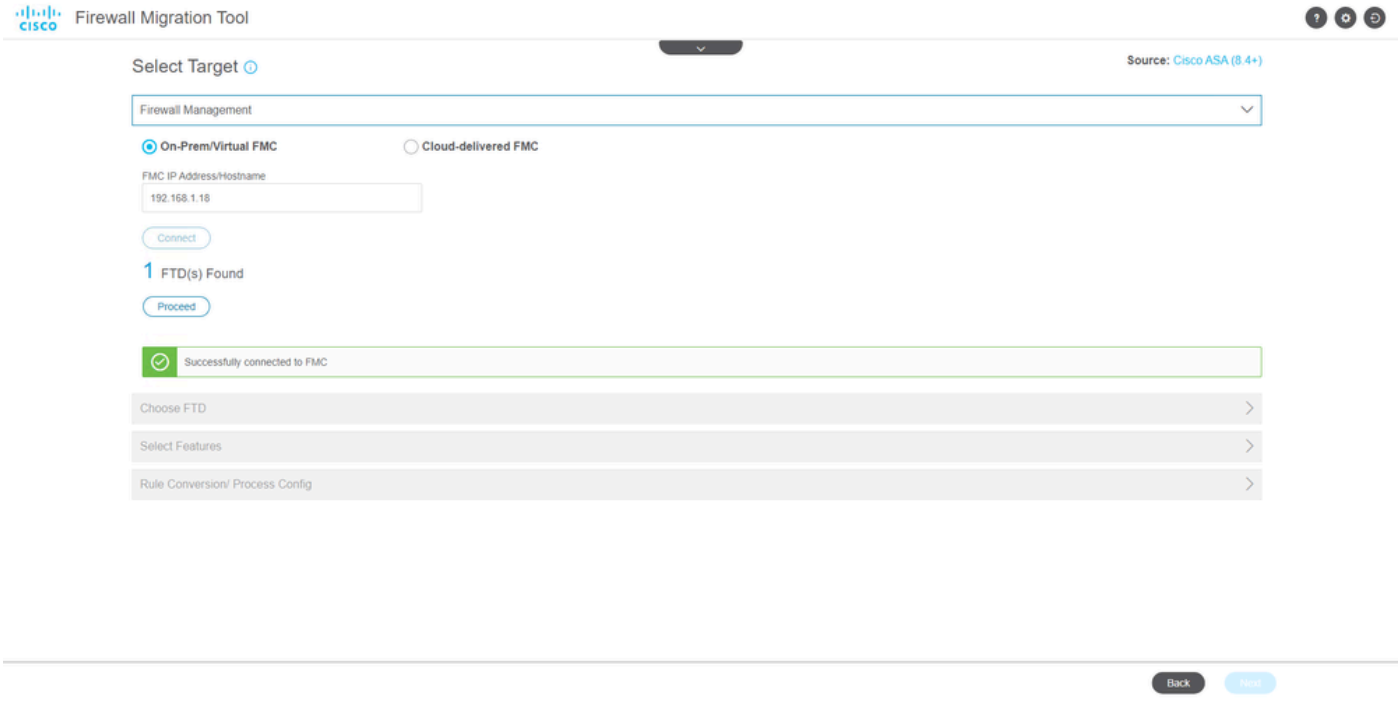
7. 방화벽에 있는 컨피그레이션의 요약이 대시보드로 표시됩니다. Next(다음)를 클릭하십시오.



요약

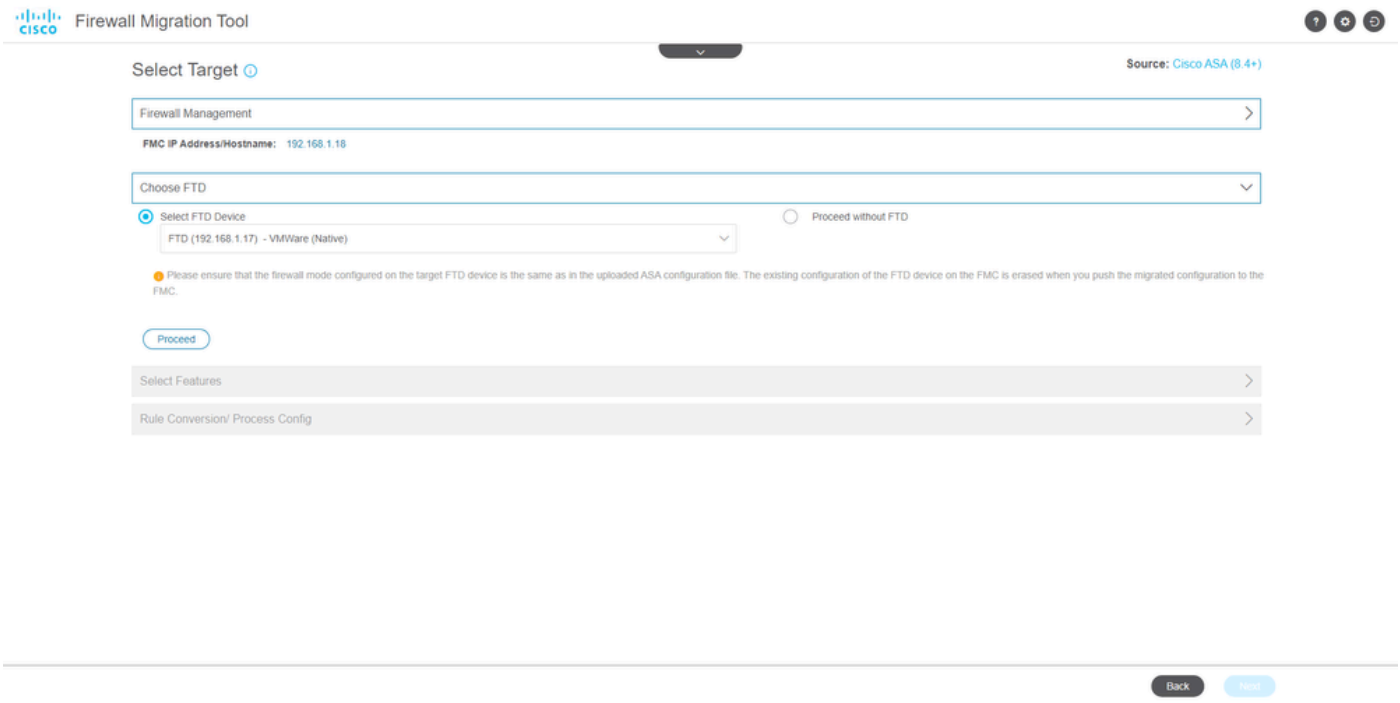
8. 마이그레이션에 사용할 대상 FMC를 선택합니다.

FMC의 IP를 제공합니다.FMC의 로그인 자격 증명을 묻는 팝업 창이 열립니다.



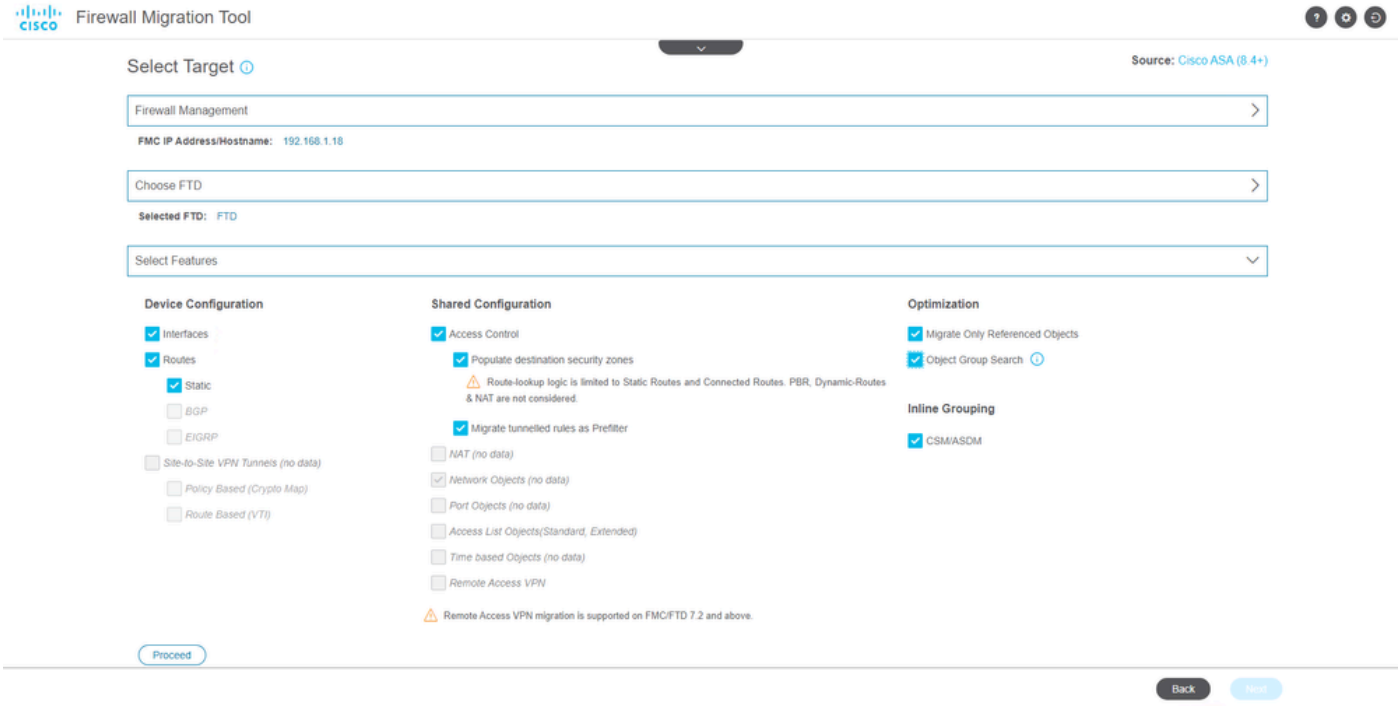
FMC IP

9. (선택 사항)사용할 대상 FTD를 선택합니다.
    1. FTD로 마이그레이션하도록 선택하는 경우 사용할 FTD를 선택합니다.
    2. FTD를 사용하지 않으려면 확인란을 채울 수 있습니다 Proceed without FTD



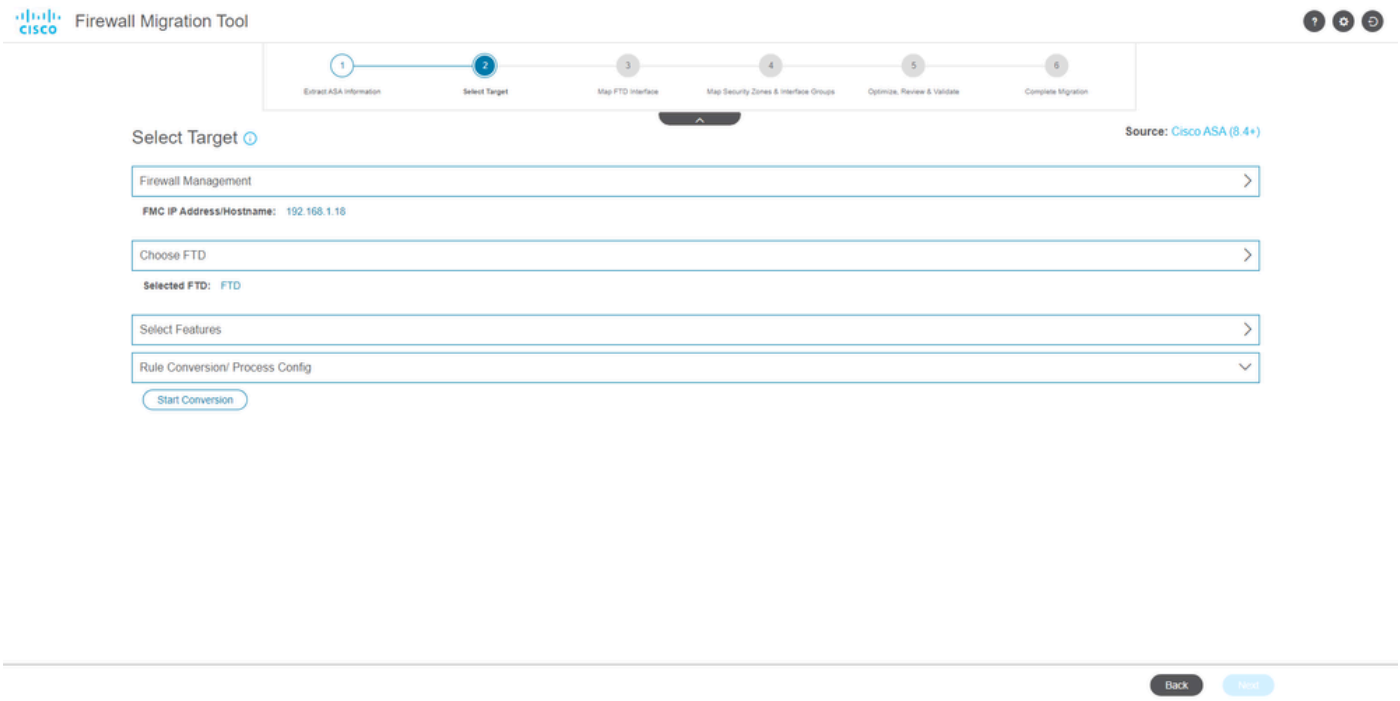
대상 FTD

10. 마이그레이션할 컨피그레이션을 선택하면 옵션이 스크린샷에 표시됩니다.



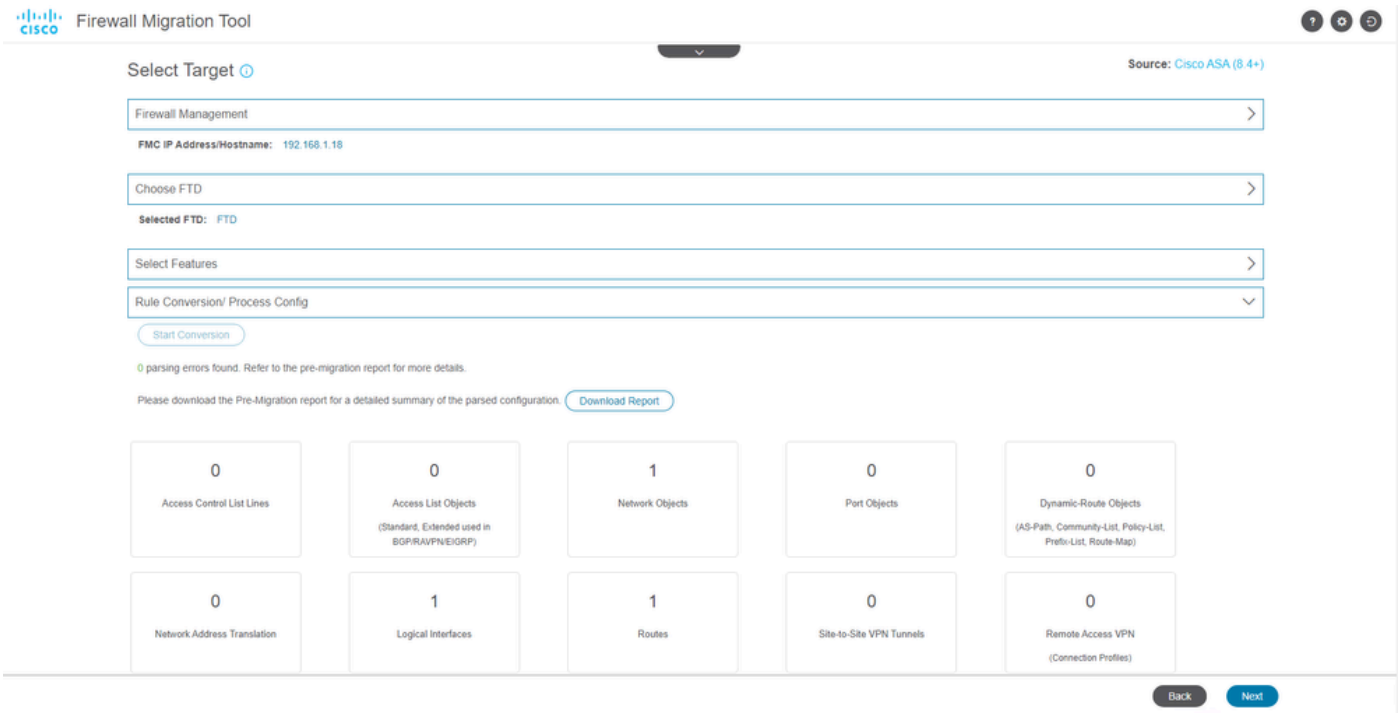
설정

11. ASA에서 FTD로의 컨피그레이션 변환을 시작합니다.



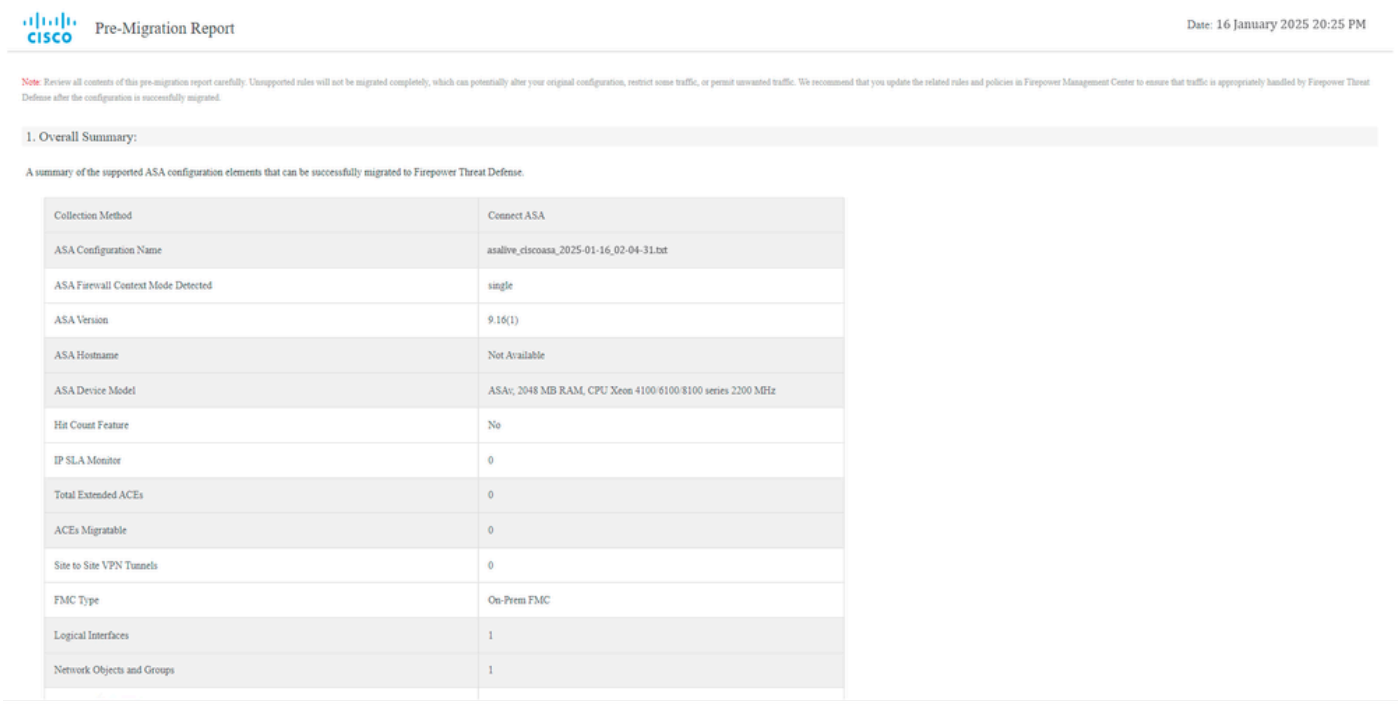
변환 시작

12. 변환이 완료되면 마이그레이션할 객체의 요약이 포함된 대시보드가 표시됩니다(호환성으로 제한).
    1. 선택적으로 클릭하여 마이그레이션할 컨피그레이션의 요약을 받을 수 **Download Report** 있습니다.



보고서 다운로드

그림과 같은 마이그레이션 전 보고서 예:



Pre-Migration Report

Date: 16 January 2025 20:25 PM

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

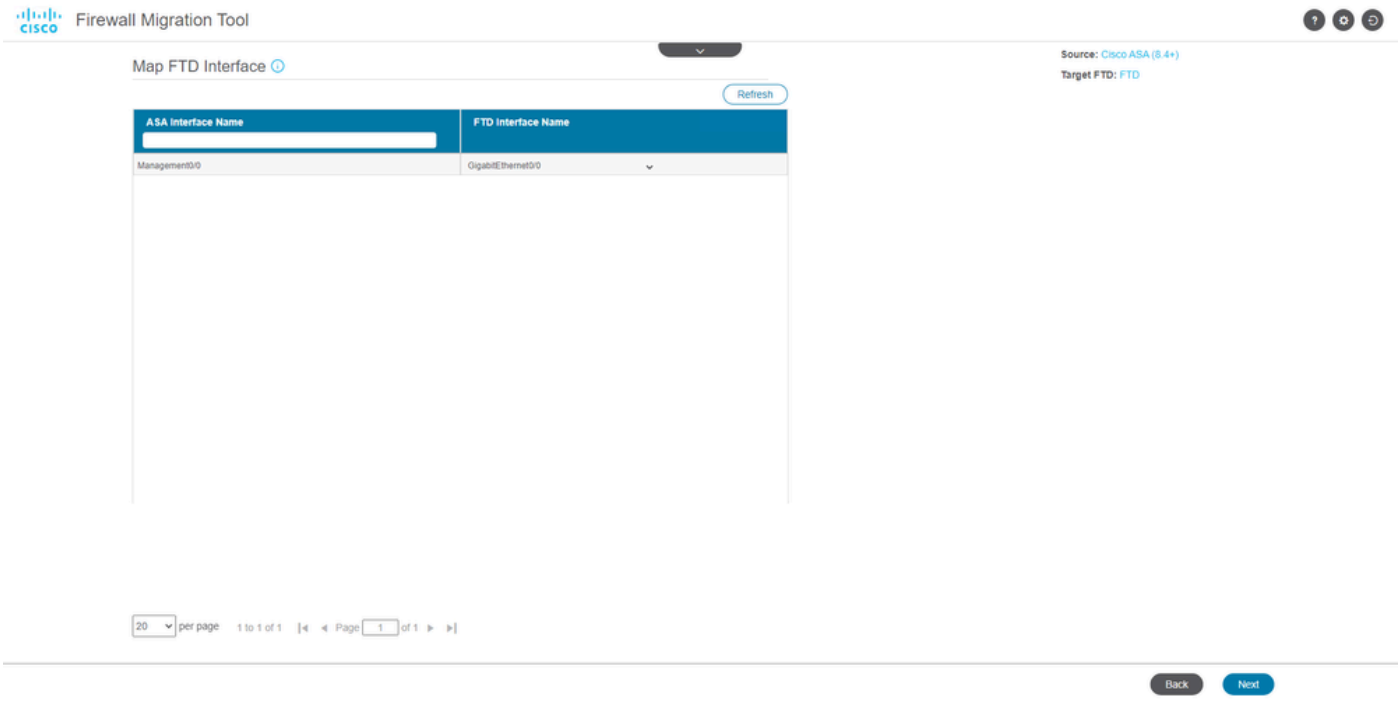
1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_2025-01-16_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

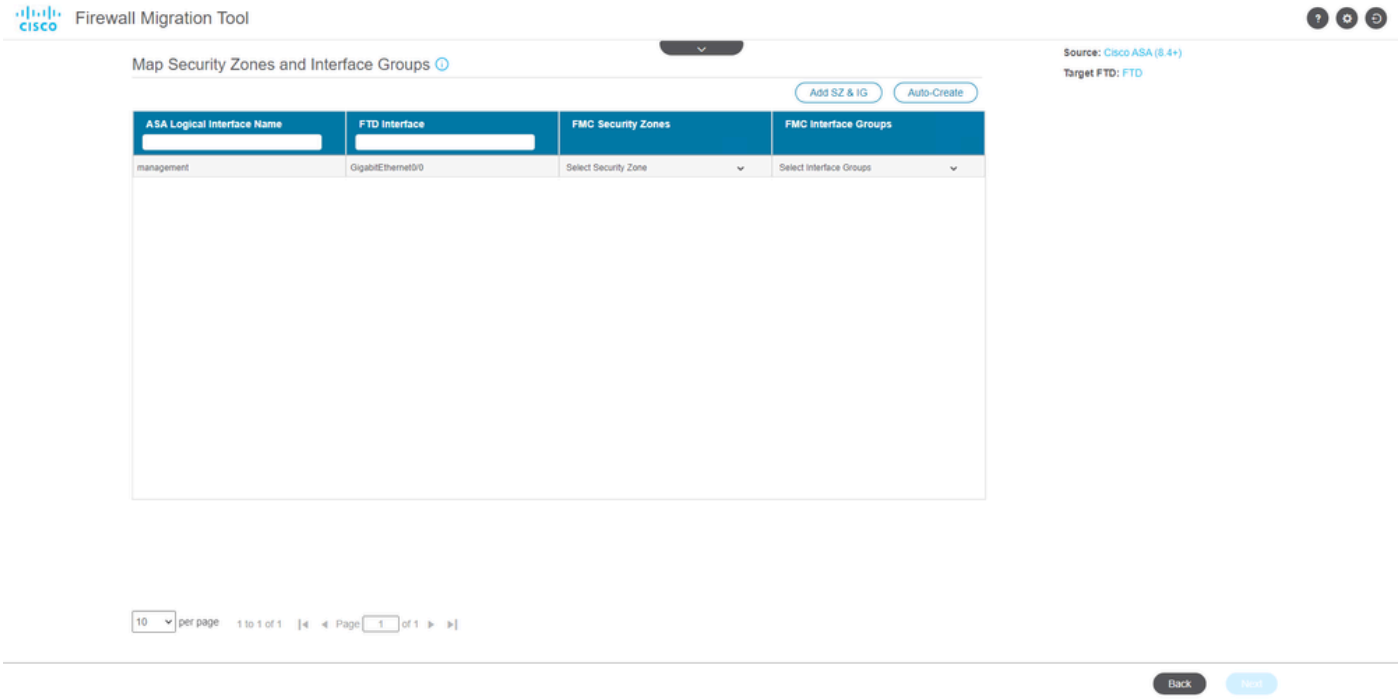
마이그레이션 전 보고서

13. ASA 인터페이스를 마이그레이션 툴의 FTD 인터페이스와 매핑합니다.



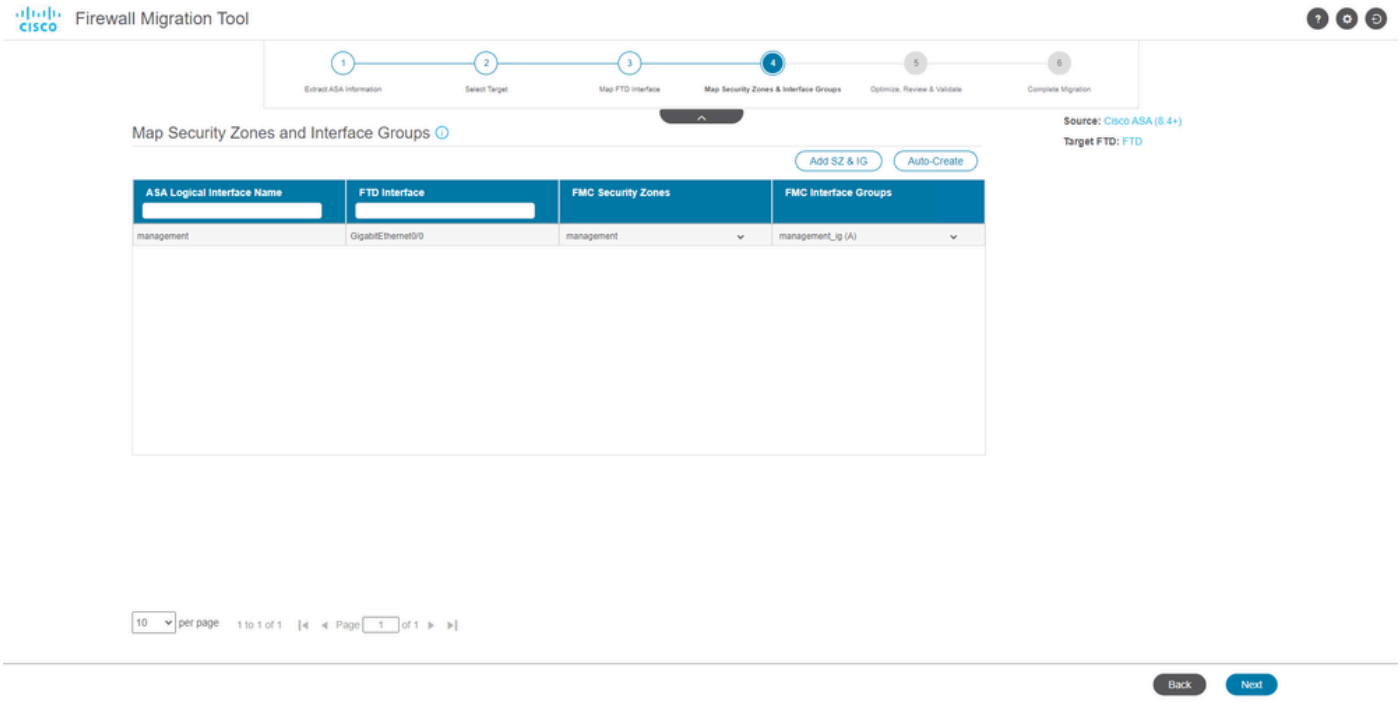
인터페이스 매핑

14. FTD에서 인터페이스에 대한 보안 영역 및 인터페이스 그룹 생성



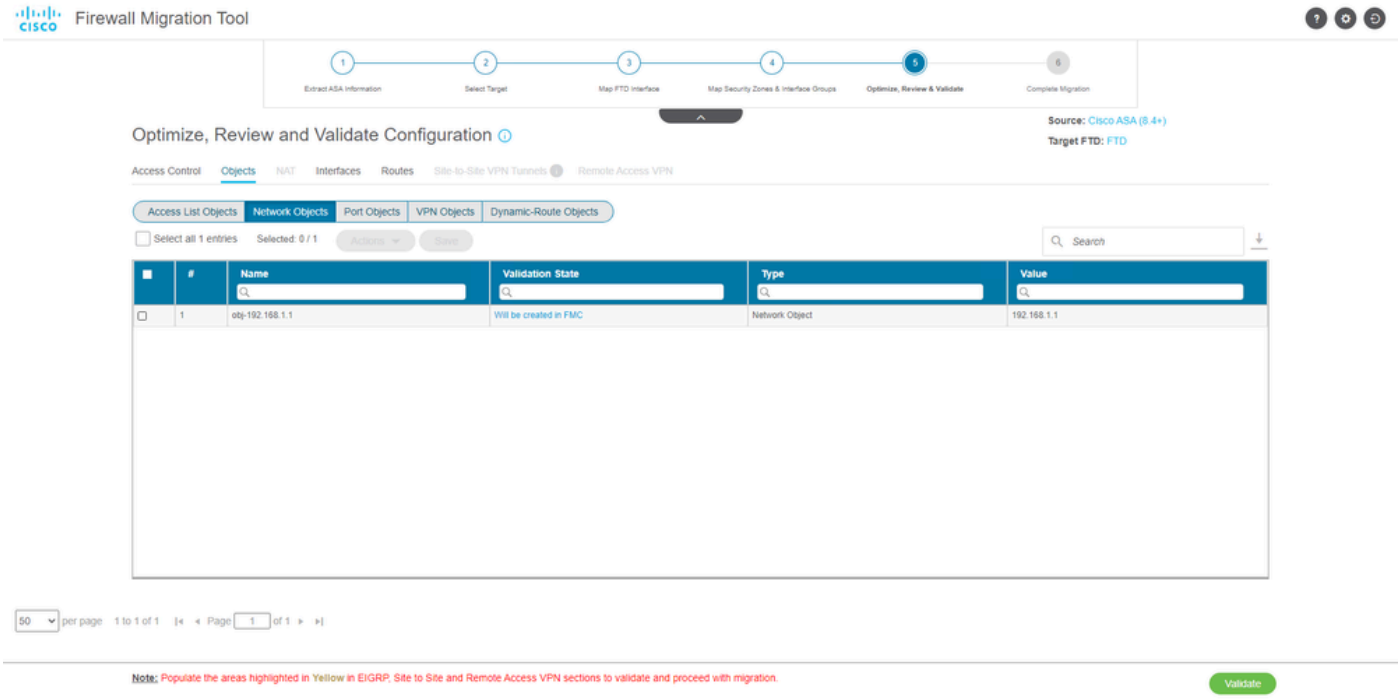
보안 영역 및 인터페이스 그룹

SZ(Security Zones) 및 IG(Interface Groups)는 그림과 같이 툴에 의해 자동으로 생성됩니다.



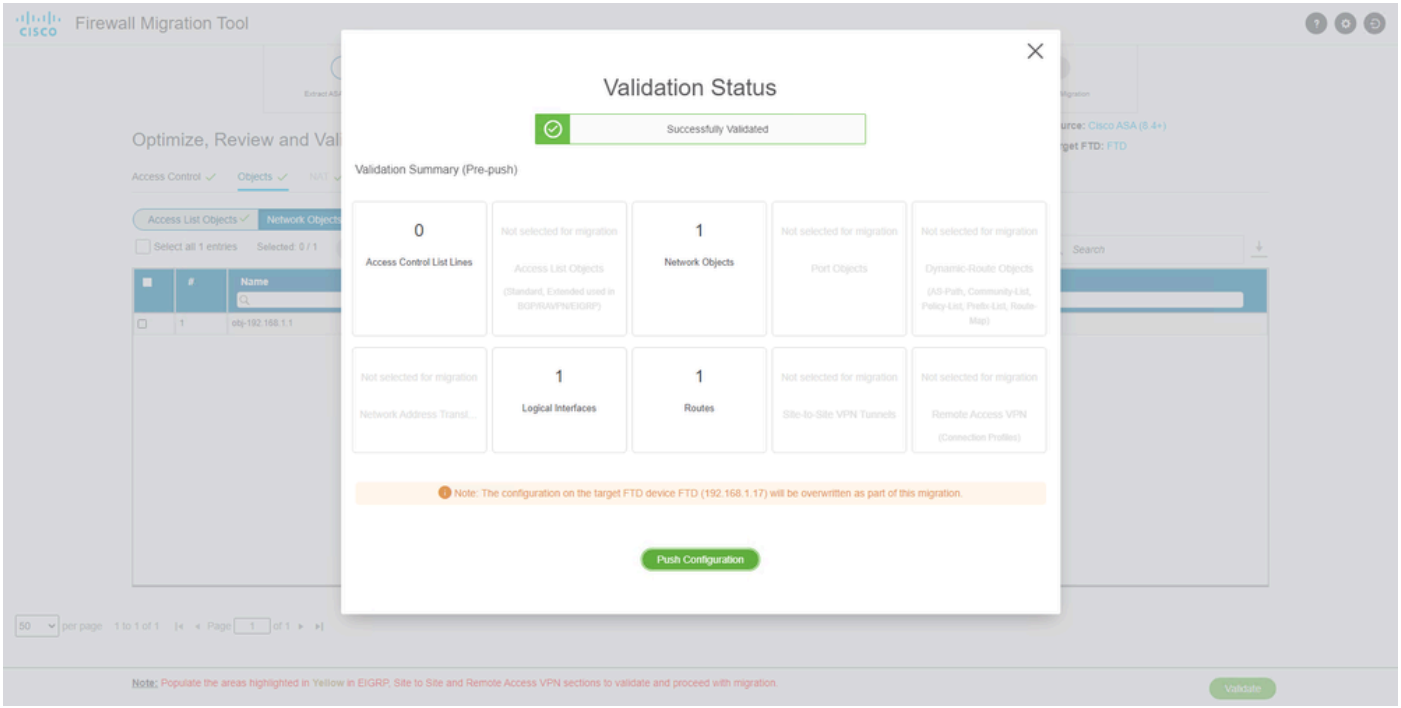
자동 만들기 도구

15. 마이그레이션 툴에서 마이그레이션할 구성을 검토하고 검증합니다.
    1. 컨피그레이션의 검토 및 최적화를 이미 완료한 경우 을 클릭합니다Validate.



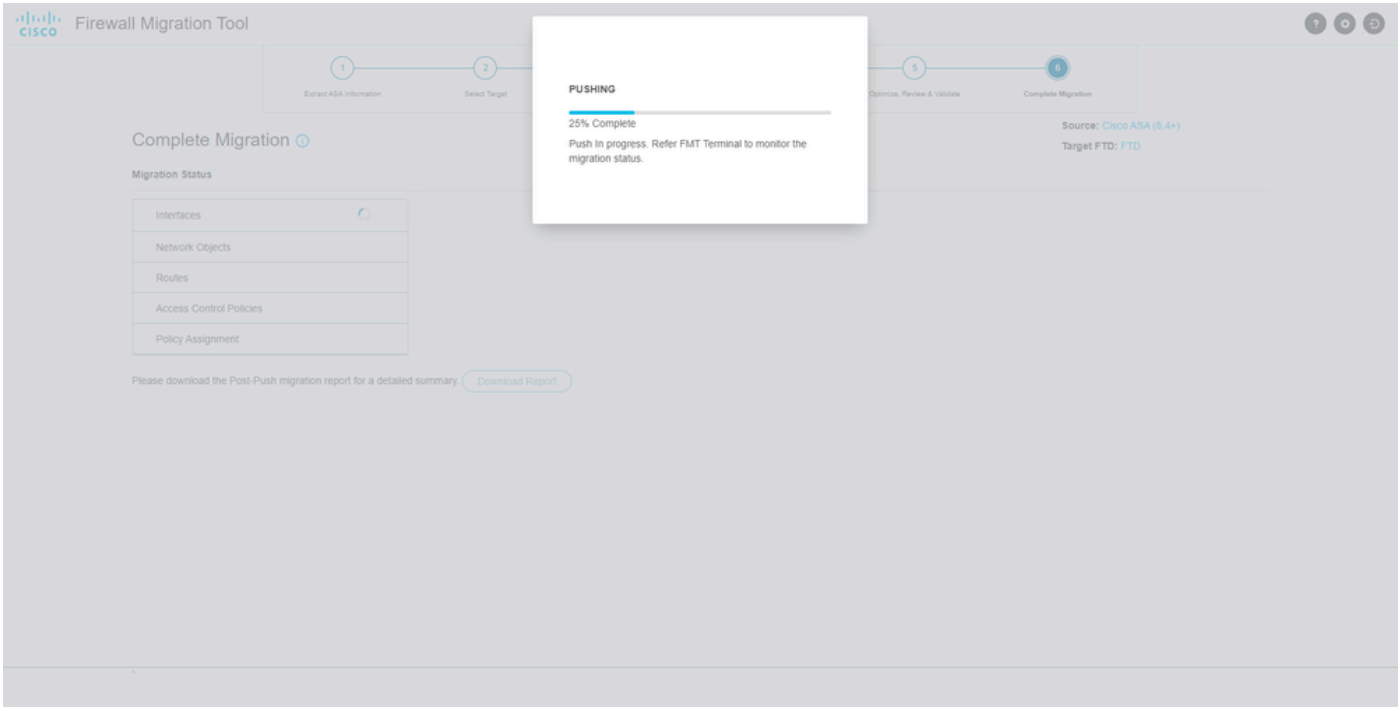
검토 및 검증

16. 검증 상태가 성공적이면 대상 디바이스에 컨피그레이션을 푸시합니다.



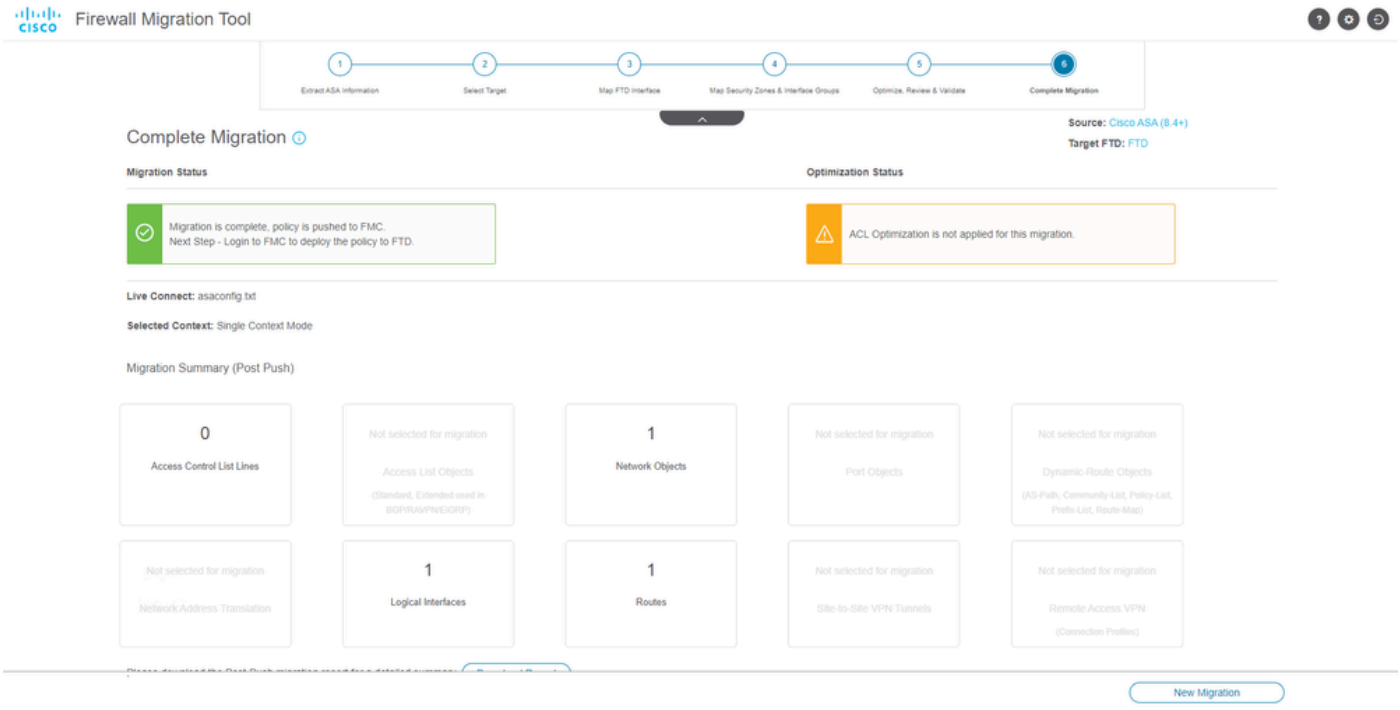
검증

그림과 같이 마이그레이션 툴을 통해 전달된 컨피그레이션의 예:



푸시

이미지에 표시된 대로 성공적인 마이그레이션의 예:



마이그레이션 성공

(선택 사항) 컨피그레이션을 FTD로 마이그레이션하도록 선택한 경우 FMC에서 방화벽으로 사용 가능한 컨피그레이션을 푸시하려면 구축이 필요합니다.

컨피그레이션을 구축하려면

1. FMC GUI에 로그인합니다.
2. 탭으로Deploy이동합니다.

3. 방화벽에 컨피그레이션을 푸시하려면 구축을 선택합니다.
4. 을 클릭합니다. Deploy

문제 해결

Secure Firewall 마이그레이션 툴 트러블슈팅

- 일반적인 마이그레이션 실패:
  - ASA 구성 파일에 알 수 없거나 잘못된 문자가 있습니다.
  - 구성 요소가 없거나 불완전합니다.
  - 네트워크 연결 문제 또는 레이턴시.
  - ASA 컨피그레이션 파일 업로드 중 또는 컨피그레이션을 관리 센터로 푸시하는 동안 문제가 발생합니다.
  - 일반적인 문제는 다음과 같습니다.
- 문제 해결을 위해 지원 번들 사용:
  - "마이그레이션 완료" 화면에서 지원 버튼을 클릭합니다.
  - Support Bundle(지원 번들)을 선택하고 다운로드할 컨피그레이션 파일을 선택합니다.
  - 로그 및 DB 파일은 기본적으로 선택되어 있습니다.
  - Download(다운로드)를 클릭하여 .zip 파일을 가져옵니다.
  - 로그, DB 및 컨피그레이션 파일을 보려면 .zip의 압축을 풉니다.
  - Email us(이메일)를 클릭하여 기술 팀에 실패 세부 정보를 보냅니다.
  - 이메일에 지원 번들을 첨부합니다.
  - TAC 방문 페이지를 클릭하여 지원을 위한 Cisco TAC 케이스를 생성합니다.
  - 이 도구를 사용하면 로그 파일, 데이터베이스 및 컨피그레이션 파일에 대한 지원 번들을 다운로드할 수 있습니다.
  - 다운로드 단계:
  - 추가 지원:

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.