

ASA 마이그레이션을 위한 보안 방화벽 마이그레이션 도구 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[컨피그레이션 단계](#)

[문제 해결](#)

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)를 Cisco Firepower로 마이그레이션하는 절차에 대해 설명합니다.

기고자: Cisco TAC 엔지니어 Ricardo Vera

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.

- Windows PC with Firepower Migration Tool(FMT) v3.0.1
- ASA(Adaptive Security Appliance) v9.16.1
- FMCv(Secure Firewall Management Center) v7.0.1
- FTDv(Secure Firewall Threat Defense Virtual) v7.0.1

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.

이 문서의 구체적인 요구 사항은 다음과 같습니다.

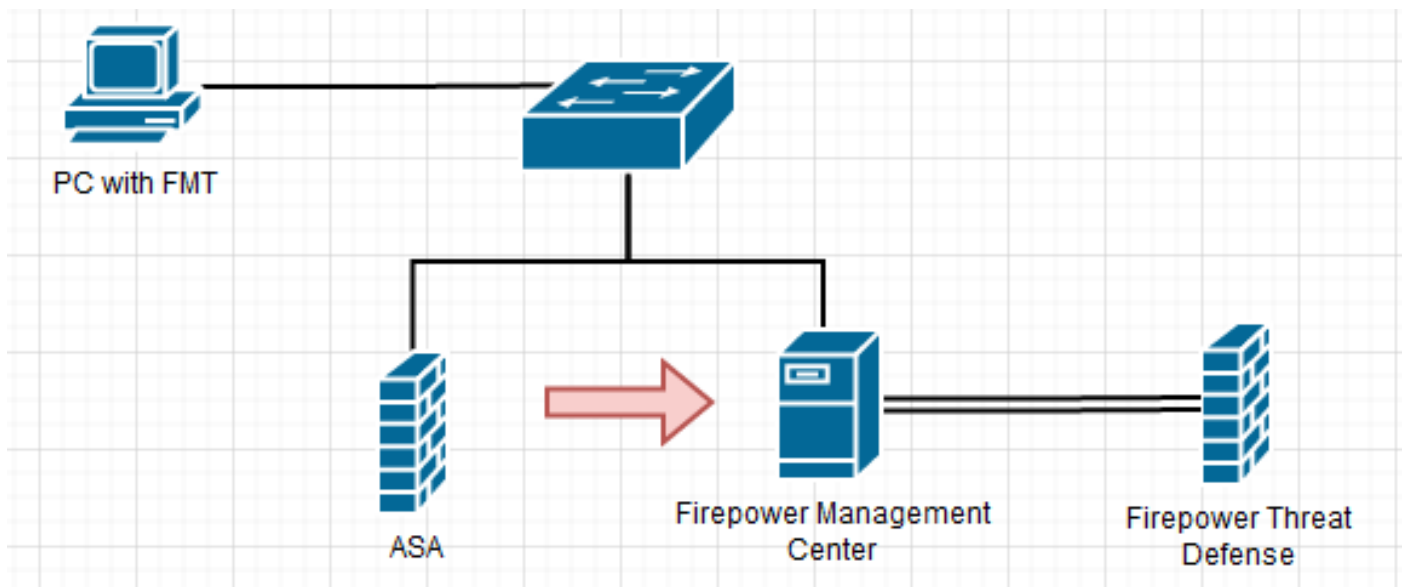
- Cisco ASA(Adaptive Security Appliance) 버전 8.4 이상
- FMCv(Secure Firewall Management Center) 버전 6.2.3 이상

Firewall Migration Tool은 다음 디바이스 목록을 지원합니다.

- Cisco ASA(8.4+)
- Cisco ASA(9.2.2+) with FPS
- 검사점(r75-r77)
- 검사점(r80)
- Fortinet(5.0+)
- Palo Alto Networks(6.1+)

마이그레이션을 진행하기 전에 방화벽 마이그레이션 툴에 [대한 지침 및 제한을 고려하십시오.](#)

구성



1. Cisco Software Central에서 최신 Firepower Migration Tool을 다운로드합니다.

Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall Threat Defense Virtual / Firepower Migration Tool (FMT) - 3.0.1

Search...

Expand All Collapse All

Latest Release

3.0.1

2.5.3

All Release

3

2

Secure Firewall Threat Defense Virtual

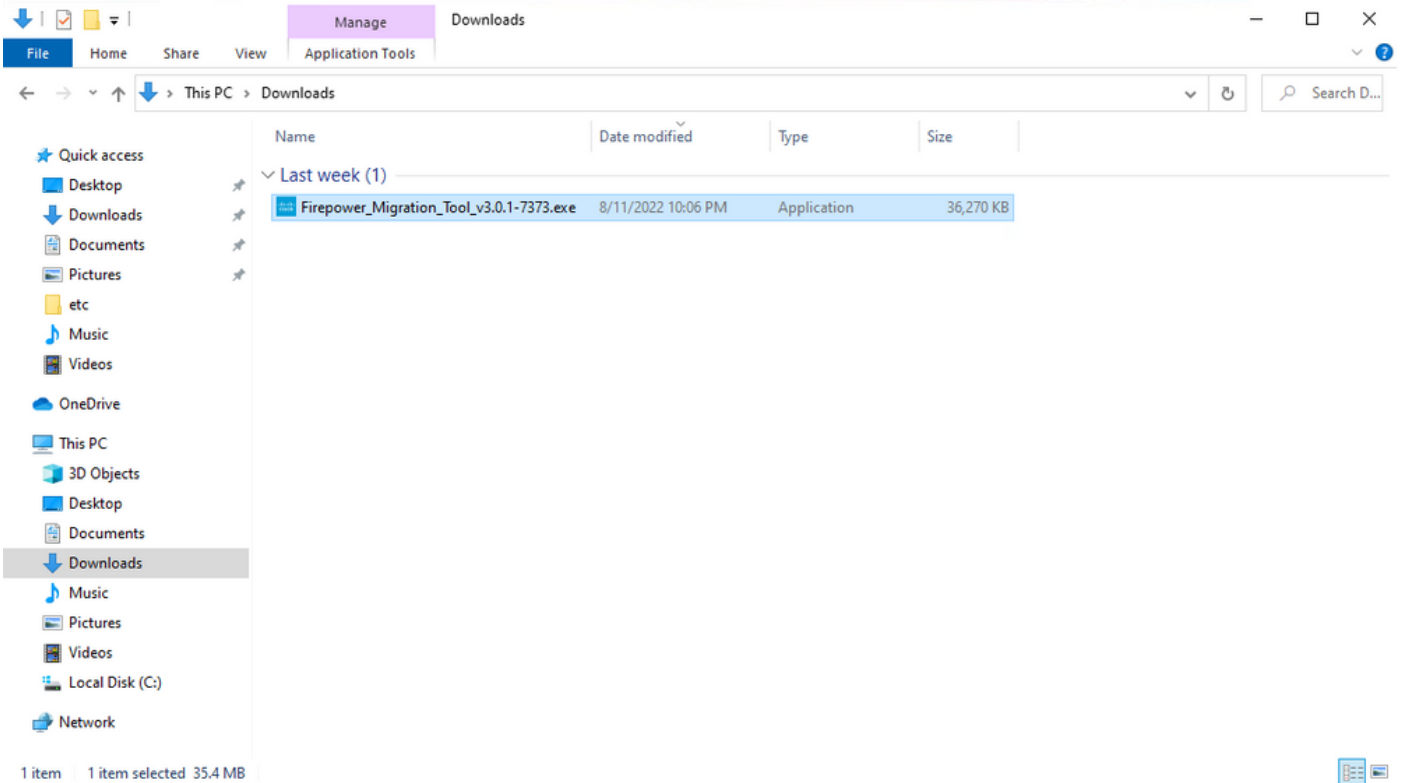
Release 3.0.1

[My Notifications](#)

[Related Links and Documentation](#)
[Open Source](#)
[Release Notes for 3.0.1](#)
[Install and Upgrade Guides](#)

File Information	Release Date	Size	
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v3.0.1-7373.exe Advisories	10-Aug-2022	9.83 MB	Download Add to cart Share
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command Advisories	10-Aug-2022	34.75 MB	Download Add to cart Share
Firepower Migration Tool 3.0.1 for Windows Firepower_Migration_Tool_v3.0.1-7373.exe Advisories	10-Aug-2022	35.42 MB	Download Add to cart Share

2. 이전에 컴퓨터에 다운로드한 파일을 클릭합니다.



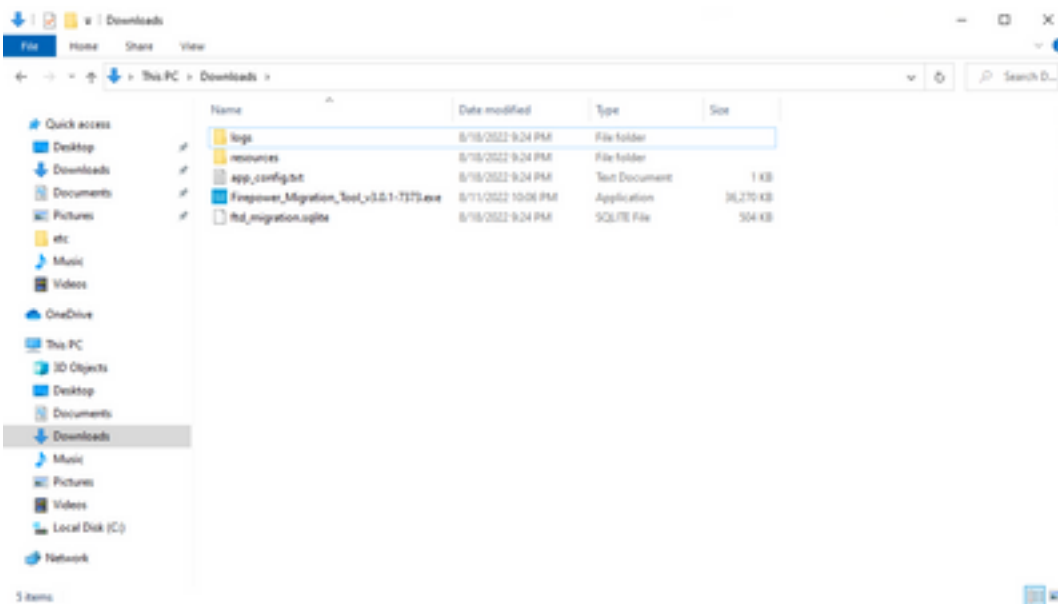
참고: 프로그램이 자동으로 열리고 콘솔이 파일을 실행한 디렉토리에 내용을 자동으로 생성합니다.

```

C:\Users\cali\Downloads\Firepower_Migration_Tool_v3.0.1-7373.exe
2022-08-18 21:24:49,752 [INFO] __init__ > "Initializing..."
2022-08-18 21:24:49,767 [INFO] settings > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO] tool_version > "ToolVersion:[3017373]"
2022-08-18 21:24:50,252 [INFO] __init__ > "Initializing..."
2022-08-18 21:24:51,252 [INFO] config > "loading settings"
2022-08-18 21:24:51,268 [INFO] client > "Getting ssl context for south server"
2022-08-18 21:24:51,299 [INFO] tools > "Not verifying ssl certificates"
2022-08-18 21:24:51,299 [INFO] client > "No discovery url configured, all endpoints needs to be configured manually"

2022-08-18 21:24:51,314 [INFO] settings > "Disabled console quick edit mode"
2022-08-18 21:24:51,314 [DEBUG] common > "session table records count:1"
2022-08-18 21:24:51,314 [INFO] common > "Using port: 8888"
2022-08-18 21:24:51,799 [INFO] run > "***** Starting server at http://localhost:8888 <****"
 * Running on http://localhost:8888/ (Press CTRL+C to quit)
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /styles.a0d79d0031ca159b236f.bundle.css HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /inline.318b50c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /cwi-font.800241c8aa87aa899c6a.woff2 HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /polyfills.76c2f23d4e2a1188f46c.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /main.777e77bd49fe82694a1a.bundle.js HTTP/1.1" 200 -
2022-08-18 21:24:57,075127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/cisco.svg HTTP/1.1" 200 -
[INFO] cco_login > "USA check for an user"
2022-08-18 21:24:57,704 [DEBUG] common > "session table records count:1"
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /favicon.ico HTTP/1.1" 200 -

```



3. 프로그램을 실행하면 "최종 사용자 사용권 계약"이 표시된 웹 브라우저가 열립니다. 약관에 동의하려면 확인란을 선택합니다.Proceed(진행)를 클릭합니다.

Firewall Migration Tool

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail, including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specific product terms at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. It does not extend to any other applicable law. You are not licensed to Use the

I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD

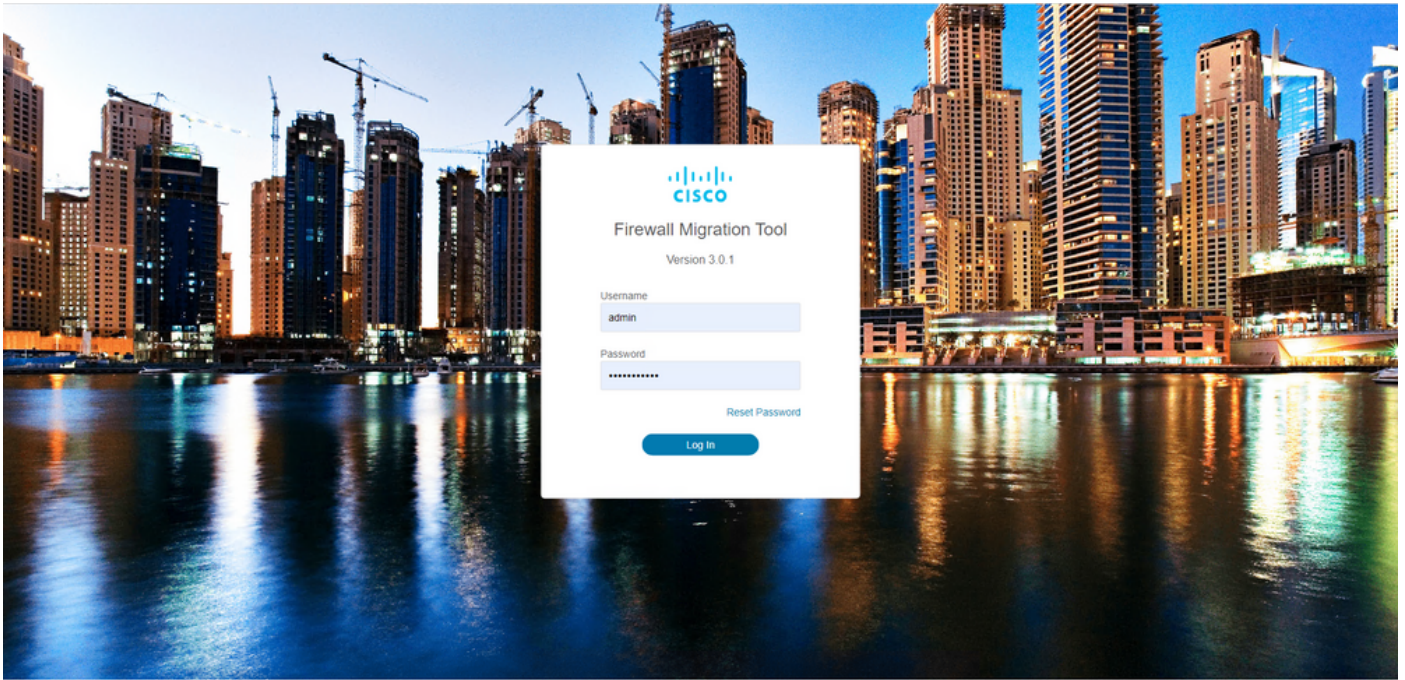


Extract Source Information

Any additional information explaining this



4. 마이그레이션 툴에 로그인합니다. CCO 계정 또는 로컬 기본 계정으로 로그인할 수 있습니다. 로컬 기본 계정 자격 증명은 다음과 같습니다. admin/Admin123



© 2015-2022 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.

5. 마이그레이션할 소스 방화벽을 선택합니다. 이 예에서는 Cisco ASA(8.4+)가 소스로 사용됩니다.

Select Source Configuration

Source Firewall Vendor

- Select Source
- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FPS
- Check Point (r75-r77)
- Check Point (r80)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Cisco ASA (8.4+) Pre-Migration Instructions

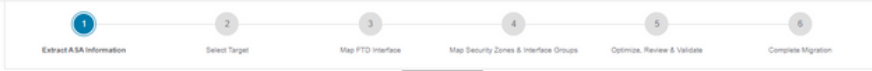
This migration may take a while. Do not make any changes to the Firepower Management Center (FMC) when migration is in progress.

Acronyms used:
 FMT: Firewall Migration Tool FMC: Firepower Management Center
 FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense migration, you must have the following items:

- Stable IP Connection:** Ensure that the connection is stable between FMT and FMC.
- FMC Version:** Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCD for the suggested release.
- FMC Account:** Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.
- FTD (Optional):** To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.
- ASA Configuration Requirements:** Export configuration file from ASA to .cfg or .txt format. Connect to live ASA to extract the configuration file for one or more contexts. To migrate following features in ASA:
 - Time Based ACLs:** FMC and FTD must be on 6.6 or later versions.
 - IP SLA Monitor:** FMC must be on 6.6 or later and FTD must be on 6.2.3 or later.
 - Object Group Search:** FMC and FTD must be on 6.6 or later versions.
 - ASA5505 Support:** FMC and FTD must be on 6.6 or later versions.
 - Remote Deployment:** FMC and FTD must be on 6.7 or later versions. If remote deployment is enabled, Firewall Migration Tool will only migrate ACLs, Network Object and Port Objects. Interface and Route configuration have to be migrated manually on to FMC.
 - Site-to-Site VPN Tunnels:** Policy Based (Crypto Map) VPN needs FMC and FTD to be on 6.6 or later. Route Based (VTI) Support, FMC and FTD to be on 6.7 or later. Ensure FTD must be added to FMC before migration. Firewall Migration Tool will migrate VPN tunnels as Point-to-Point network.

6. 컨피그레이션을 가져오는 데 사용할 추출 방법을 선택합니다. 수동 업로드를 수행하려면 **Running Config ".cfg"** 또는 **".txt"** 형식의 ASA 파일ASA에 연결하여 방화벽에서 직접 컨피그레이션을 추출합니다.



Extract Cisco ASA (8.4+) Information Source: Cisco ASA (8.4+)

Extraction Methods v

Manual Upload

- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech. For Single-context upload show running.

▲ Do not upload hand coded configurations.

[Upload](#)

Connect to ASA

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP Port>.

ASA IP Address/Hostname

192.168.1.20

[Connect](#)

Context Selection >

Parsed Summary >

[Back](#) [Next](#)

참고: 이 예에서는 ASA에 직접 연결합니다.

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

Extract Cisco ASA (8.4+) Information Source: Cisco ASA (8.4+)

Extraction Methods >

ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: [Download config](#)

Parsed Summary v

Collect Hitcounts: No

8 Access Control List Lines	2 Access List Objects <small>(Standard, Extended used in BGP/RAVPN/EIGRP)</small>	0 Network Objects	0 Port Objects	0 Dynamic-Route Objects <small>(AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)</small>
0 Network Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN <small>(Connection Profiles)</small>

● Pre-migration report will be available after selecting the targets.

[Back](#) [Next](#)

8. 마이그레이션에 사용할 대상 FMC를 선택합니다. FMC의 IP를 제공합니다. FMC의 로그인 자격 증명을 묻는 팝업 창이 열립니다.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

On-Prem/Virtual FMC Cloud-delivered FMC

FMC IP Address/Hostname
192.168.1.18

Connect

1 FTD(s) Found

Proceed

Successfully connected to FMC

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

Back

Next

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

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Select FTD Device Proceed without FTD

FTD (192.168.1.17) - VMWare (Native)

Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features >

Rule Conversion/ Process Config >

Back

Next

10. 마이그레이션할 구성을 선택하면 옵션이 스크린샷에 표시됩니다.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Device Configuration

- Interfaces
- Routes
 - Static
 - BGP
 - EIGRP
 - Site-to-Site VPN Tunnels (no data)
 - Policy Based (Crypto Map)
 - Route Based (VTI)

Shared Configuration

- Access Control
 - Populate destination security zones
 - Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.
 - Migrate tunnelled rules as Prefilter
 - NAT (no data)
 - Network Objects (no data)
 - Port Objects (no data)
 - Access List Objects(Standard, Extended)
 - Time based Objects (no data)
 - Remote Access VPN
- Remote Access VPN migration is supported on FMC/FTD 7.2 and above.

Optimization

- Migrate Only Referenced Objects
- Object Group Search

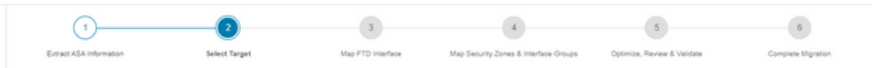
Inline Grouping

- CSM/ASDM

Proceed

Back Next

11. ASA에서 FTD로의 컨피그레이션 변환을 시작합니다.



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

12. 변환이 완료되면 마이그레이션할 객체의 요약이 포함된 대시보드가 표시됩니다(호환성으로 제한). 필요에 따라 **Download Report** 마이그레이션할 컨피그레이션의 요약을 수신합니다.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

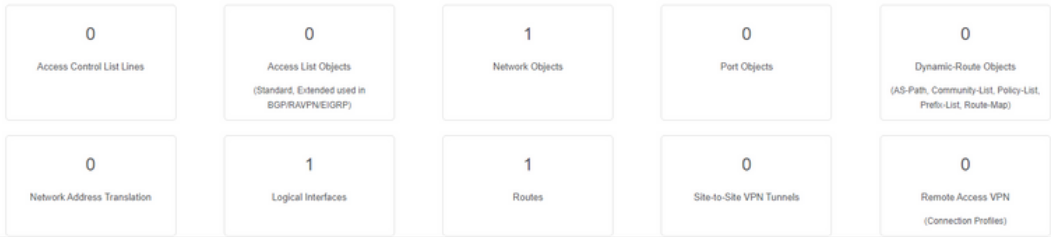
Select Features

Rule Conversion/ Process Config

Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration [Download Report](#)



Back Next

그림과 같은 마이그레이션 전 보고서 예:

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	aaalive_ciscoasa_2022-08-19_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASA; 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

13. ASA 인터페이스를 마이그레이션 툴의 FTD 인터페이스와 매핑합니다.

Map FTD Interface

Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

20 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

14. FTD에서 인터페이스에 대한 보안 영역 및 인터페이스 그룹 생성

Map Security Zones and Interface Groups

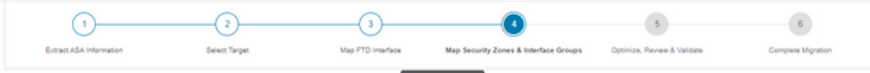
Source: Cisco ASA (8.4+)
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

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



Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)
Target FTD: FTD

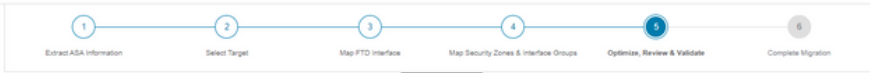
Add SZ & IG Auto-Create

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_ig (A)

10 per page 1 to 1 of 1 |< Page 1 of 1 >|

Back Next

15. 마이그레이션 툴에서 마이그레이션할 구성을 검토하고 검증합니다.
컨피그레이션 검토 및 최적화를 이미 완료한 경우 Validate.



Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)
Target FTD: FTD

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN

Access List Objects Network Objects Port Objects VPN Objects Dynamic-Route Objects

Select all 1 entries Selected: 0 / 1 Actions Save

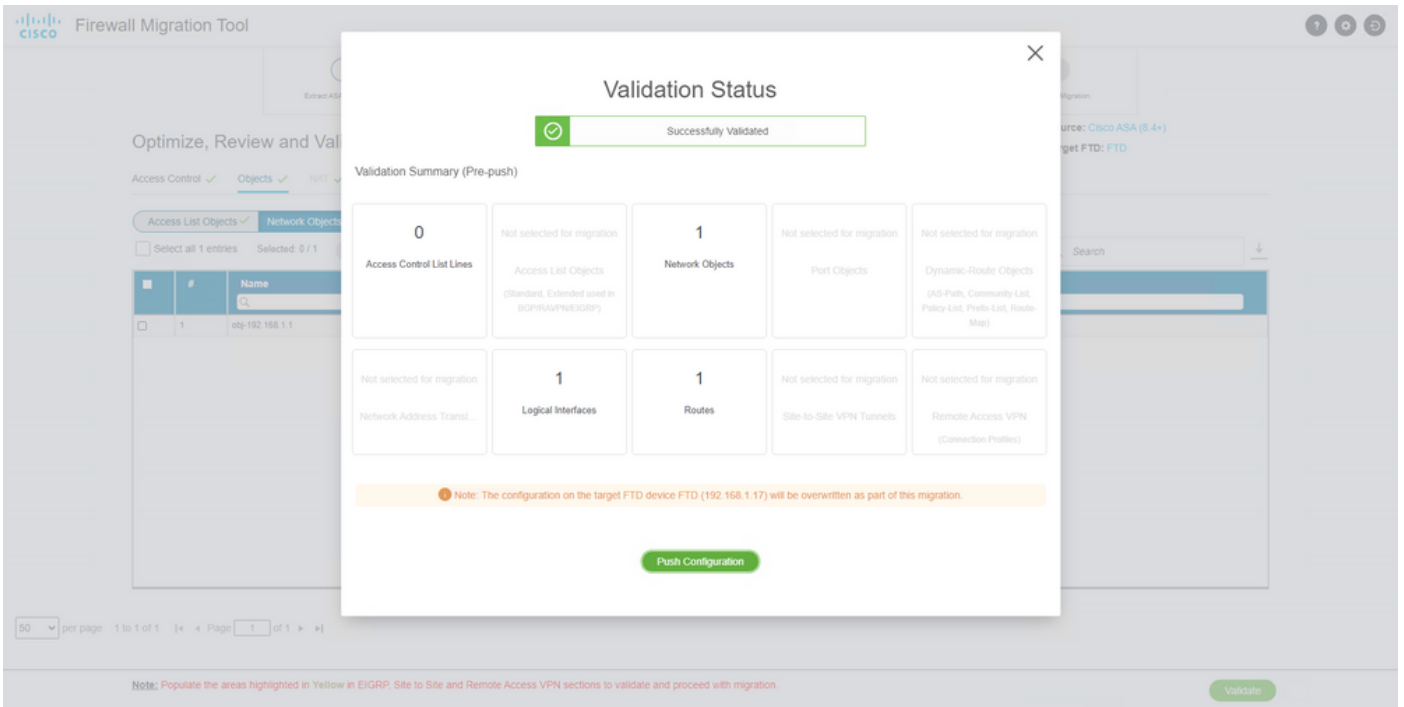
#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

50 per page 1 to 1 of 1 |< Page 1 of 1 >|

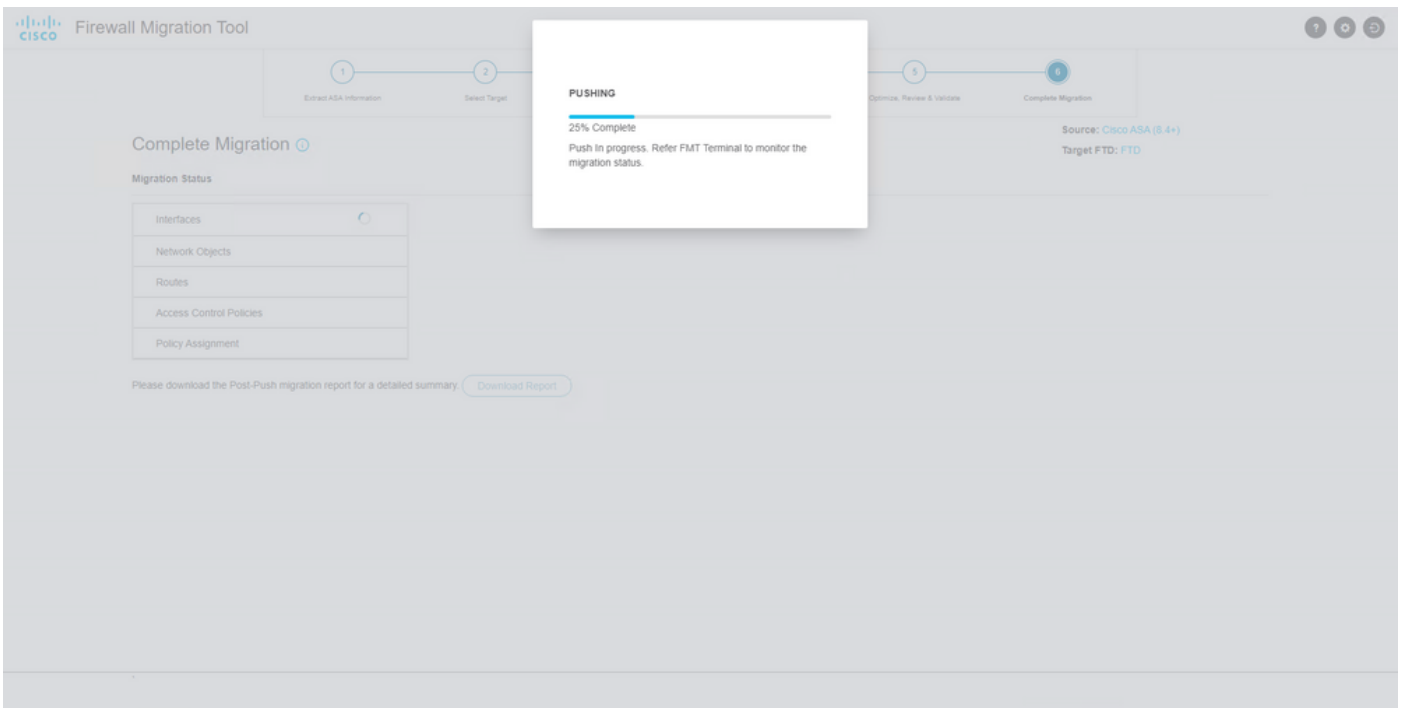
Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration.

Validate

16. 검증 상태가 성공하면 컨피그레이션을 대상 디바이스에 푸시합니다.



그림과 같이 마이그레이션 툴을 통해 전달된 컨피그레이션의 예:



이미지에 표시된 대로 성공적인 마이그레이션의 예:



Source: Cisco ASA (8.4+)
Target FTD: FTD

Complete Migration

Migration Status

✔ Migration is complete, policy is pushed to FMC.
Next Step - Login to FMC to deploy the policy to FTD.

Optimization Status

⚠ ACL Optimization is not applied for this migration.

Live Connect: asaconfig.txt

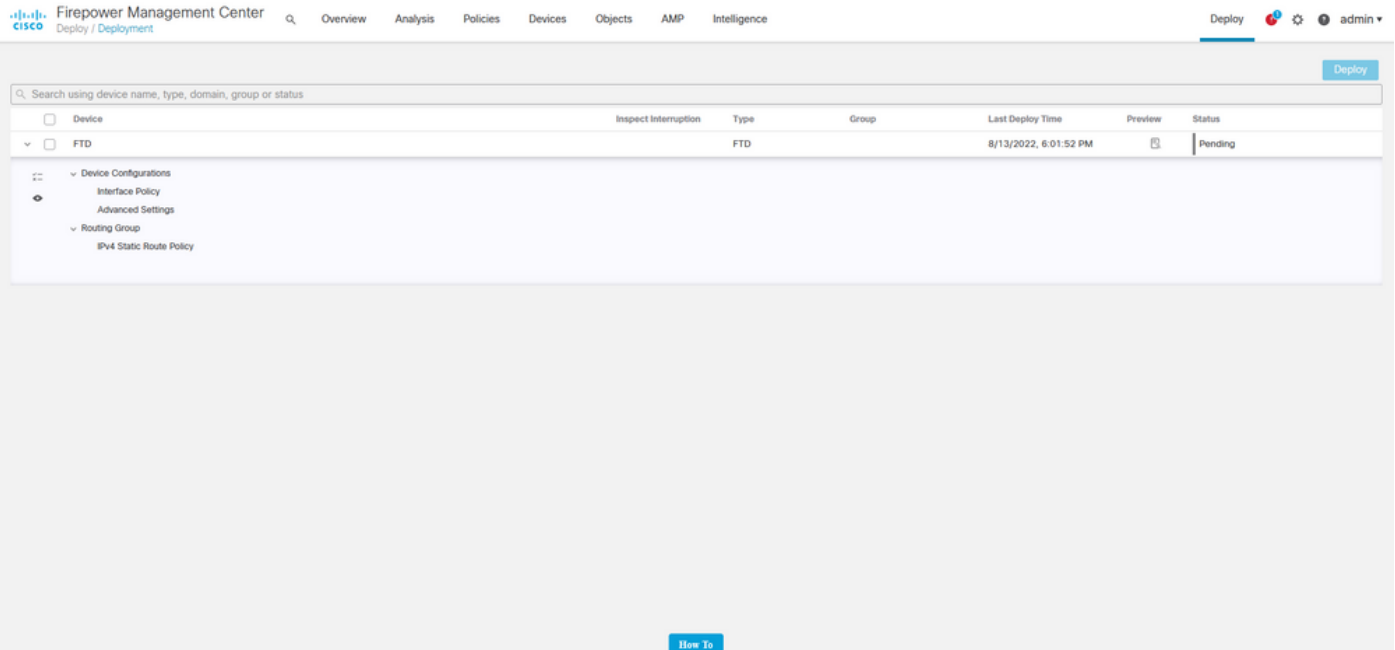
Selected Context: Single Context Mode

Migration Summary (Post Push)

0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RA/PNEIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects V4S-Path, Community List, Policy-List, PreB-List, Route-Map
Not selected for migration Network Address Translation	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

[New Migration](#)

17. (선택 사항) 컨피그레이션을 FTD로 마이그레이션하도록 선택한 경우, 컨피그레이션을 구축하려면 FMC에서 방화벽으로 사용 가능한 컨피그레이션을 푸시하는 구축이 필요합니다. FMC GUI에 로그인합니다. 탐색 Deploy 탭. 방화벽에 컨피그레이션을 푸시하려면 구축을 선택합니다. 클릭 Deploy.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

Firepower Migration Tool 파일이 배치된 디렉토리의 로그를 확인합니다. 예를 들면 다음과 같습니다.

Firepower_Migration_Tool_v3.0.1-7373.exe/logs/log_2022-08-18-21-24-46.log

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.