配置用于ASA迁移的安全防火墙迁移工具

目录

简介

本文档介绍将思科自适应安全设备(ASA)迁移到Cisco Firepower的过程。

作者：Cisco TAC工程师Ricardo Vera。

先决条件

要求

思科建议您了解思科防火墙威胁防御(FTD)和自适应安全设备(ASA)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带Firepower迁移工具(FMT)v3.0.1的Windows PC
- 自适应安全设备(ASA)v9.16.1
- 安全防火墙管理中心(FMCv)v7.0.1
- 安全防火墙威胁防御虚拟(FTDv)v7.0.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

本文档的具体要求包括：

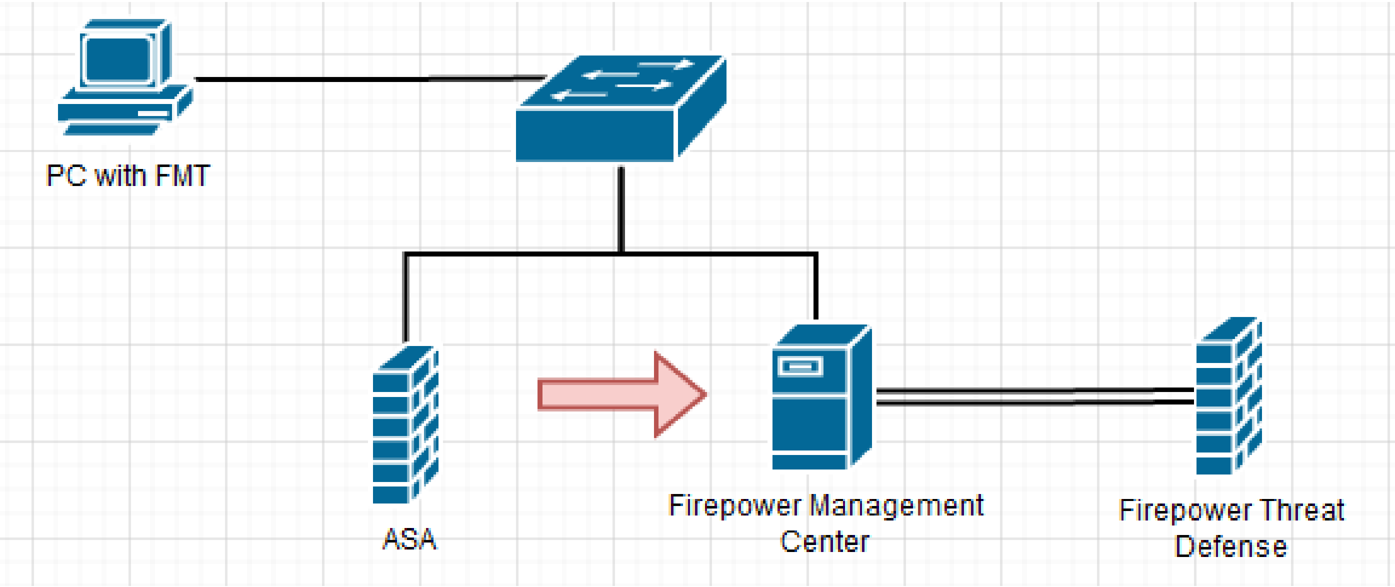
- 思科自适应安全设备(ASA)8.4版或更高版本
- 安全防火墙管理中心(FMCv)版本6.2.3或更高版本

防火墙迁移工具支持以下设备列表：

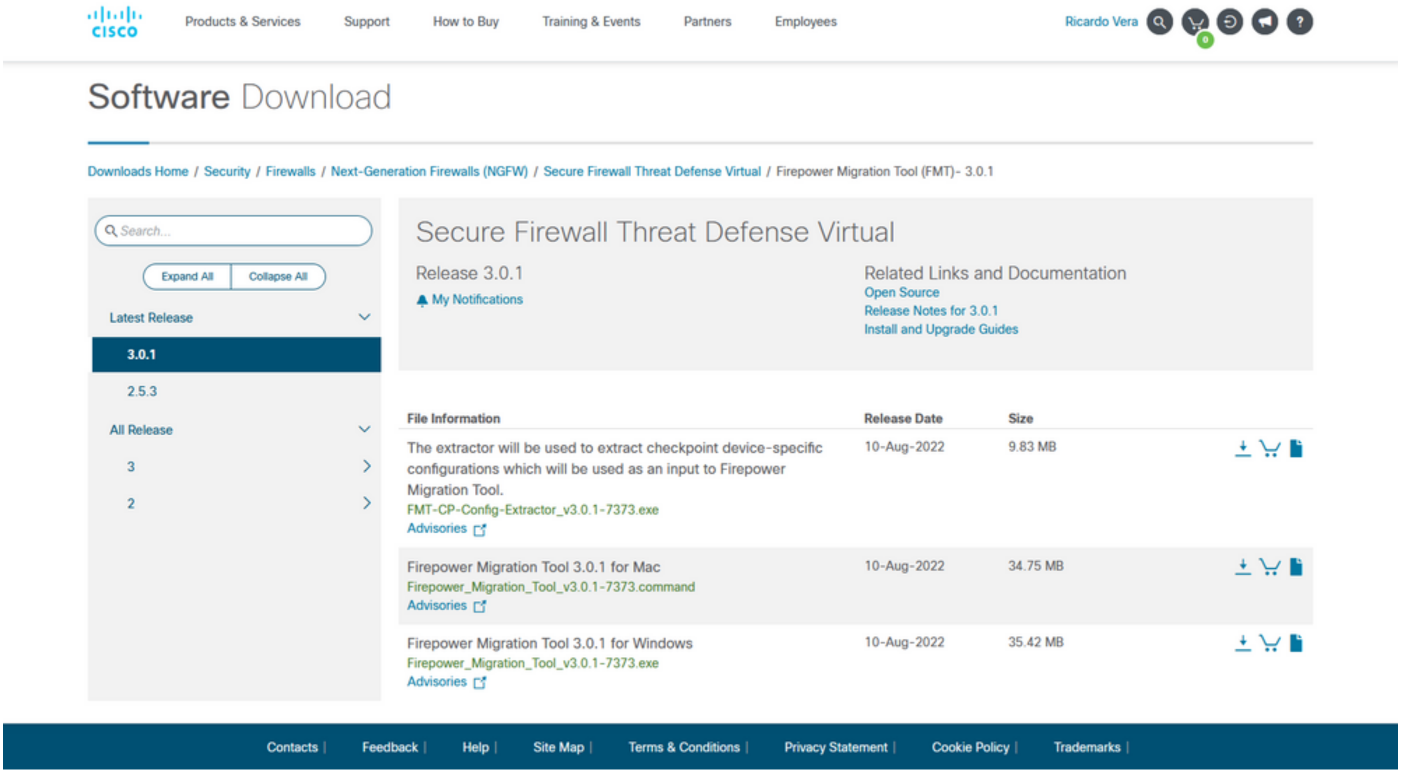
- 思科ASA(8.4+)
- 带FPS的Cisco ASA(9.2.2+)
- 检查点(r75-r77)
- 检查点(r80)
- Fortinet(5.0+)
- Palo Alto Networks(6.1+)

在继续迁移之前，请考虑防火墙迁移工具的准则和限制。

配置



1. 从思科软件中心下载最新的Firepower迁移工具：



Software Download

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

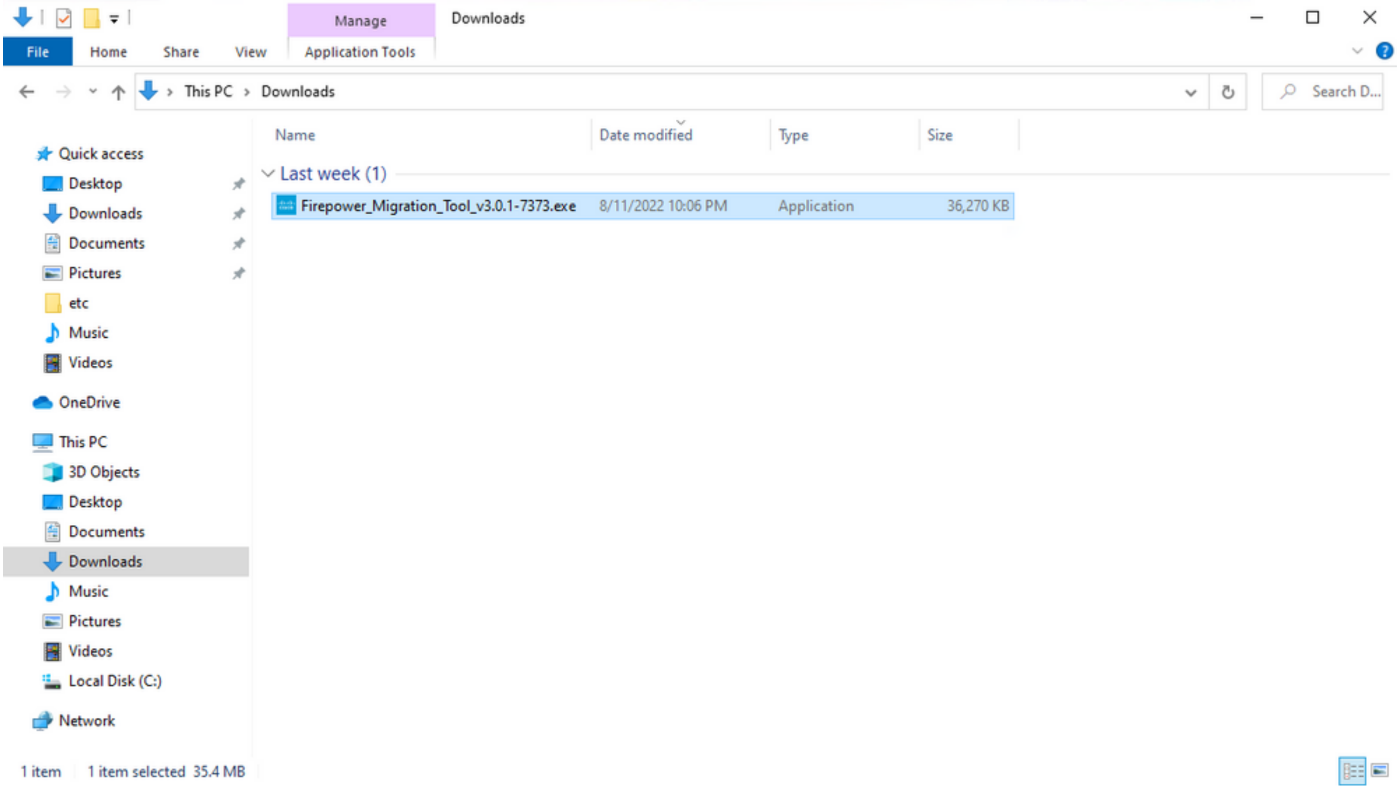
Secure Firewall Threat Defense Virtual

Release 3.0.1

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
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command Advisories	10-Aug-2022	34.75 MB
Firepower Migration Tool 3.0.1 for Windows Firepower_Migration_Tool_v3.0.1-7373.exe Advisories	10-Aug-2022	35.42 MB

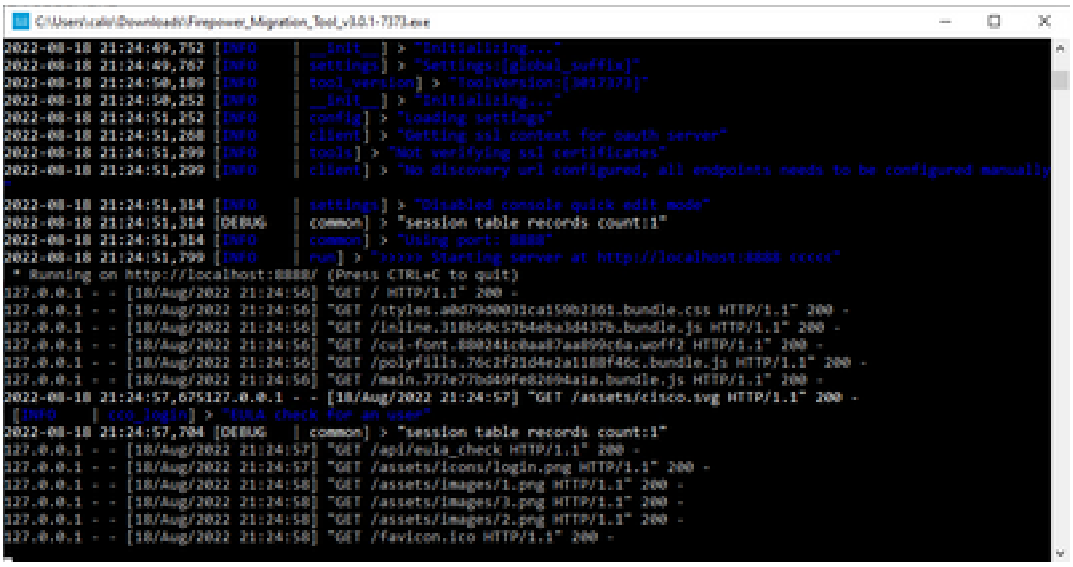
2. 单击之前下载到计算机的文件。



Name	Date modified	Type	Size
Last week (1)			
Firepower_Migration_Tool_v3.0.1-7373.exe	8/11/2022 10:06 PM	Application	36,270 KB

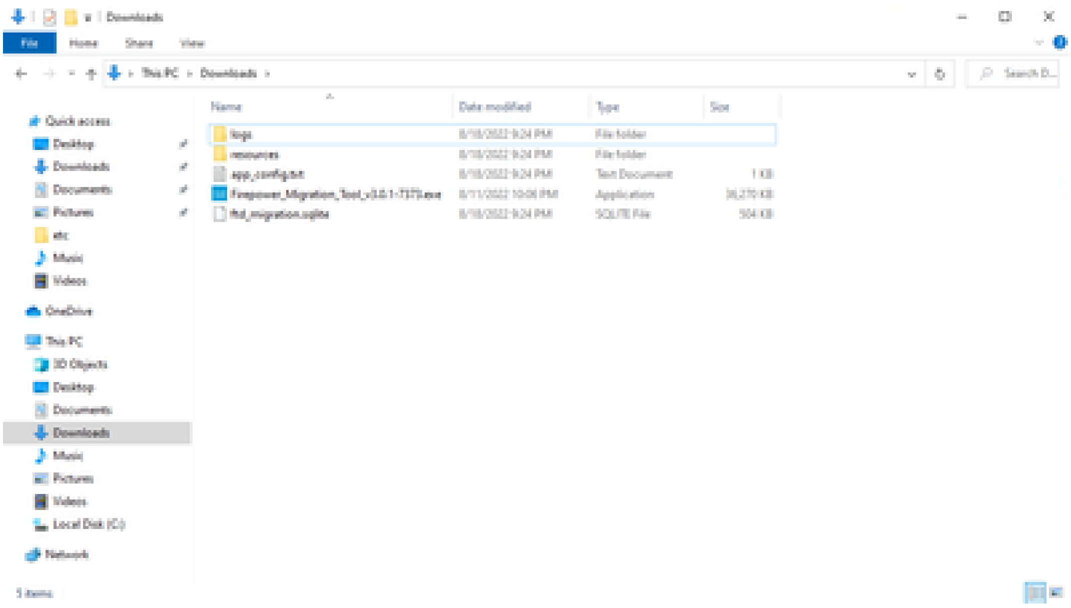
1 item   1 item selected 35.4 MB

注意：该程序会自动打开，控制台会在您运行文件的目录上自动生成内容。


C:\Users\calo\Downloads\Firepower_Migration_Tool_v3.0.1-7373.exe

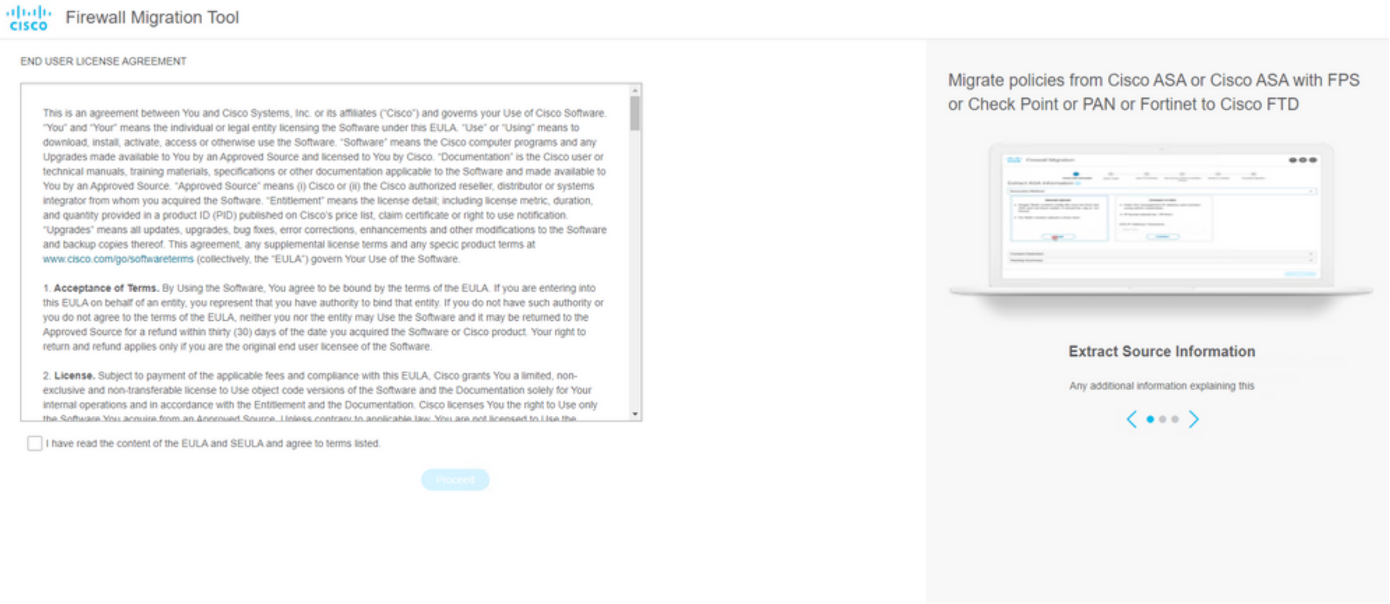
```
2022-08-18 21:24:49,752 [INFO     | __init__] > "Initializing..."
2022-08-18 21:24:49,767 [INFO     | settings] > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO     | tool_version] > "ToolVersion:[3017373]"
2022-08-18 21:24:50,252 [INFO     | __init__] > "Initializing..."
2022-08-18 21:24:51,252 [INFO     | config] > "Loading settings"
2022-08-18 21:24:51,268 [INFO     | client] > "Getting ssl context for oauth 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.a0d79d0031ca159b2361.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 /cui-font.880241c0aa87aa899c6a.woff2 HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /polyfills.76c2f21d4e2a1188f46c.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /main.777e77bd49fe8269 4a1a.bundle.js HTTP/1.1" 200 -
2022-08-18 21:24:57,675127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/cisco.svg HTTP/1.1" 200 -
 [INFO     | cco_login] > "EULA 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 -
```



Name	Date modified	Type	Size
logs	8/18/2022 9:24 PM	File folder	
resources	8/18/2022 9:24 PM	File folder	
app_config.txt	8/18/2022 9:24 PM	Text Document	1 KB
Firepower_Migration_Tool_v3.0.1-7373.exe	8/11/2022 10:06 PM	Application	36,270 KB
ftd_migration.sqlite	8/18/2022 9:24 PM	SQLITE File	504 KB

3. 运行该程序后，它会打开一个显示“最终用户许可协议”的Web浏览器。 选中此复选框可接受条款和条件。单击**Proceed**。


cisco
Firewall Migration Tool
Proceed
Extract Source Information
Any additional information explaining this

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 specic product terms at www.cisco.com/go/softwareterms (collectively, the "EULA") govern Your Use of the Software.

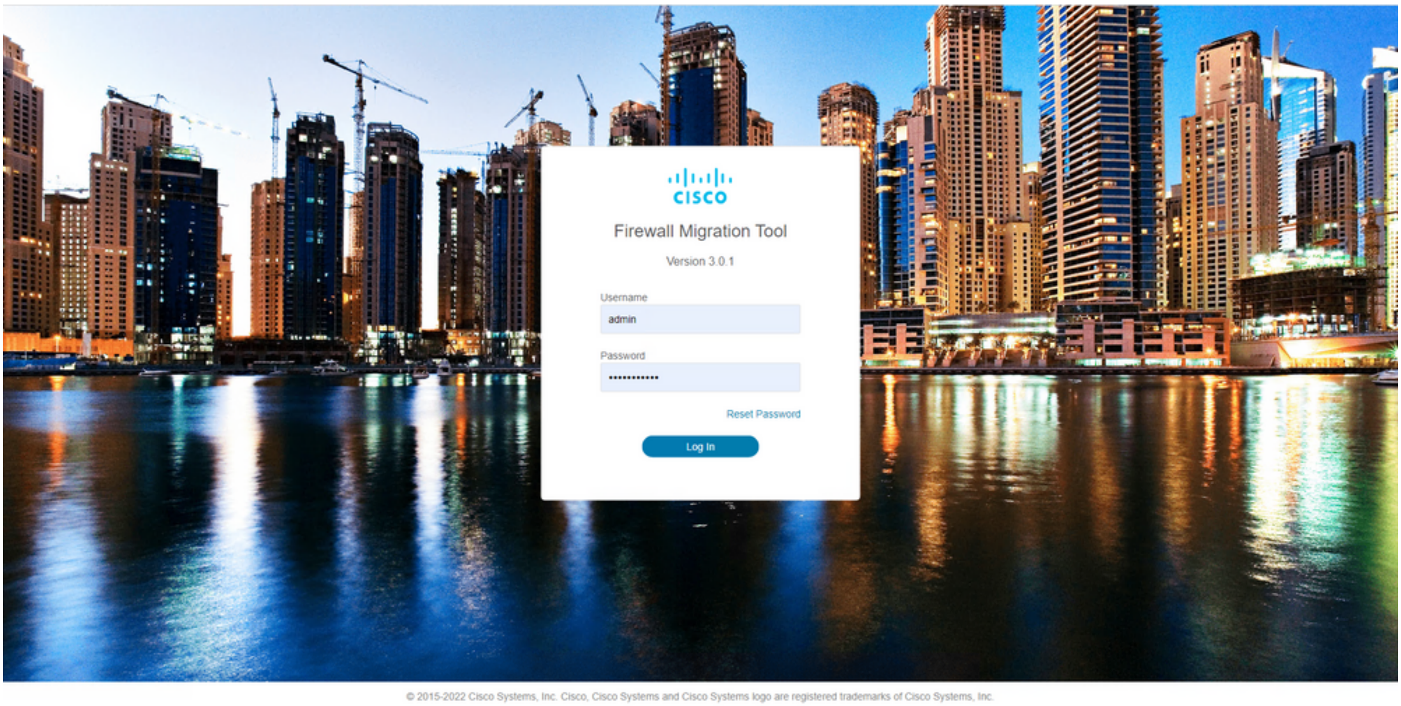
1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither 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. Unless contrary to applicable law, You are not licensed to Use the

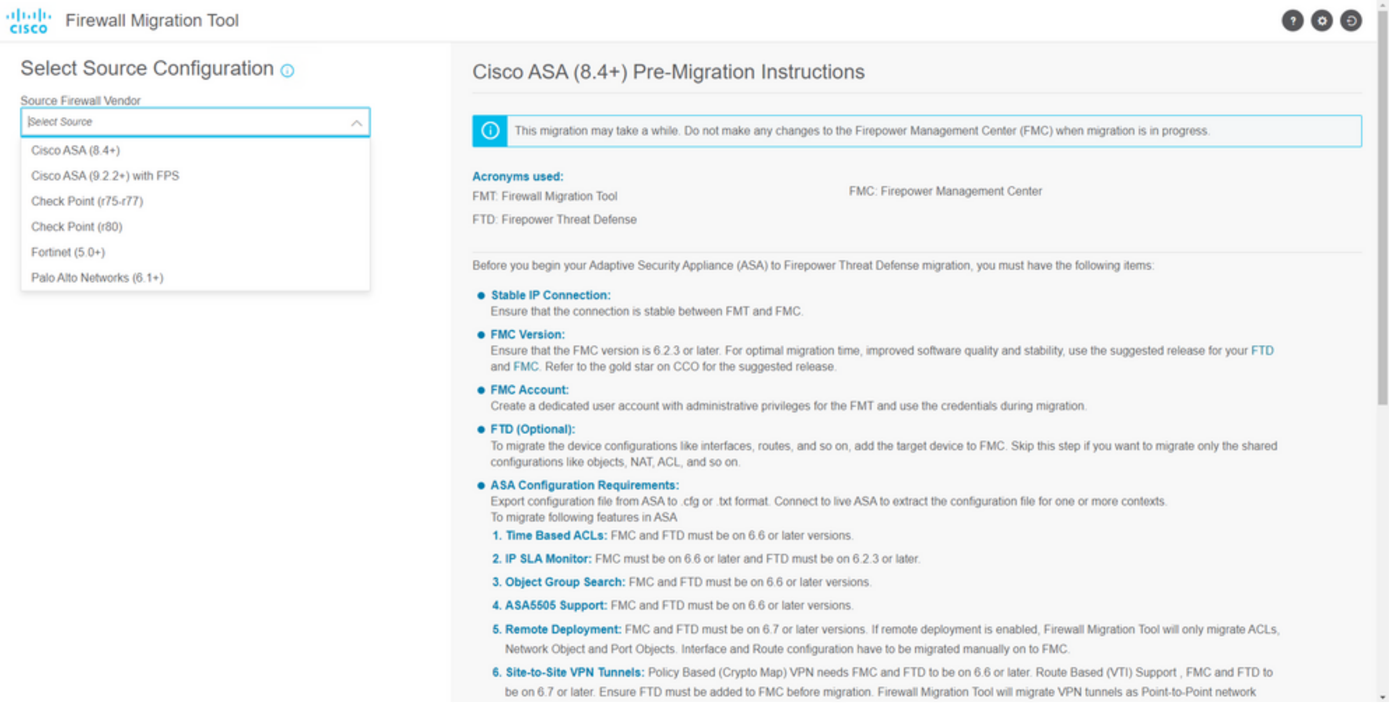
□ I have read the content of the EULA and SEULA and agree to terms listed.

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

4. 登录迁移工具。 您可以使用CCO帐户或本地默认帐户登录。 本地默认帐户凭据为：admin/Admin123


Firewall Migration Tool
Version 3.0.1
Username
admin
Password
Reset Password
Log In
© 2015-2022 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.

5. 选择要迁移的源防火墙。 在本示例中，Cisco ASA(8.4+)用作源。



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

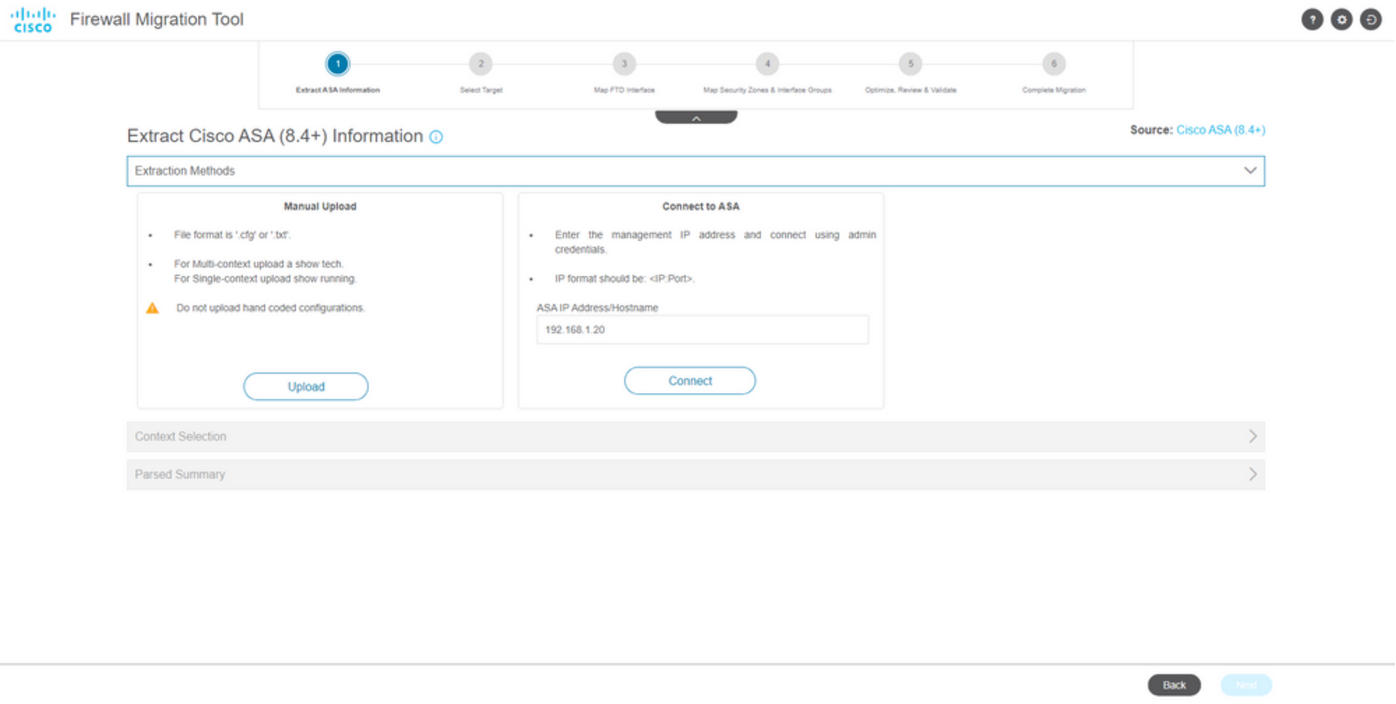
FMC: Firepower Management Center

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 CCO 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
  1. **Time Based ACLs:** FMC and FTD must be on 6.6 or later versions.
  2. **IP SLA Monitor:** FMC must be on 6.6 or later and FTD must be on 6.2.3 or later.
  3. **Object Group Search:** FMC and FTD must be on 6.6 or later versions.
  4. **ASA5505 Support:** FMC and FTD must be on 6.6 or later versions.
  5. **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.
  6. **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. 选择用于获取配置的提取方法。 手动上传要求您上传 **Running Config** ASA文件，格式为“.cfg”或“.txt”。连接到ASA以直接从防火墙提取配置。



Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods

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.

Connect to ASA

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

ASA IP Address/Hostname

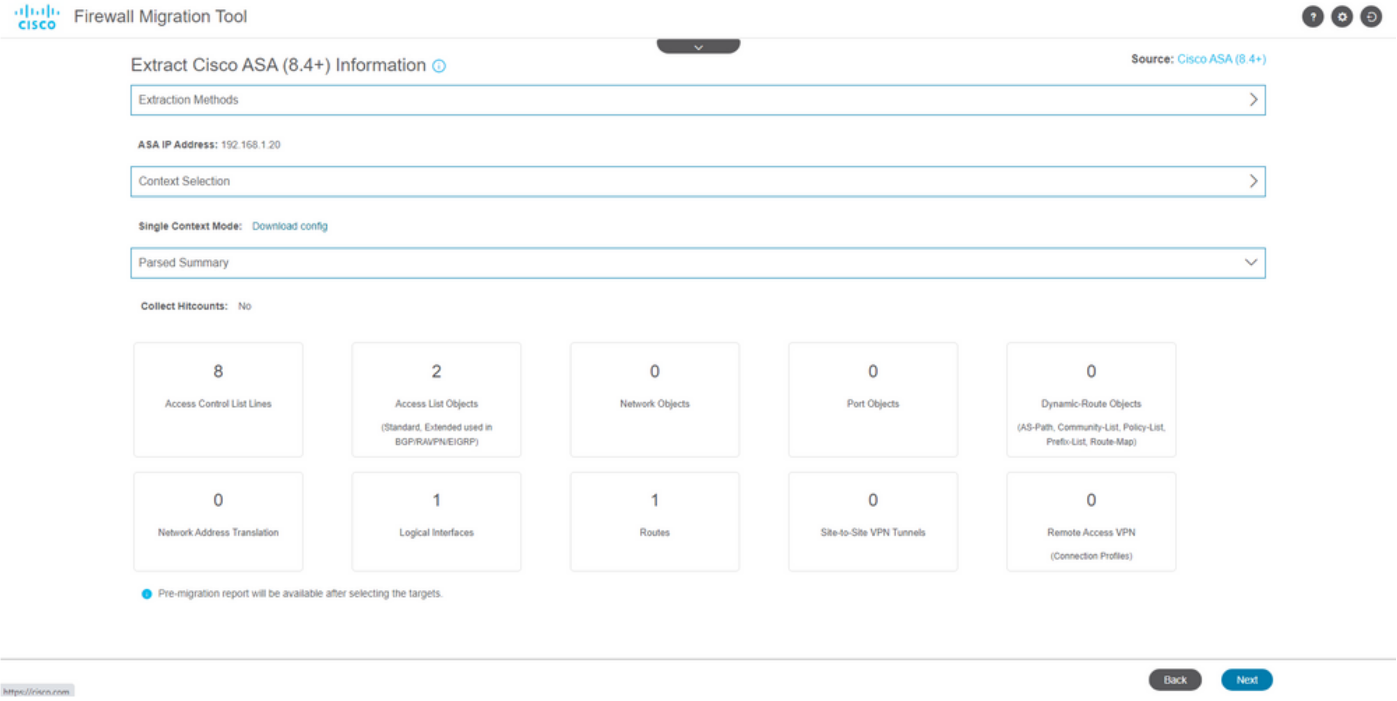
192.168.1.20

Context Selection

Parsed Summary

注意：在本示例中，直接连接到ASA。

7. 在防火墙上找到的配置摘要显示为控制面板，请点击**下一步**。



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

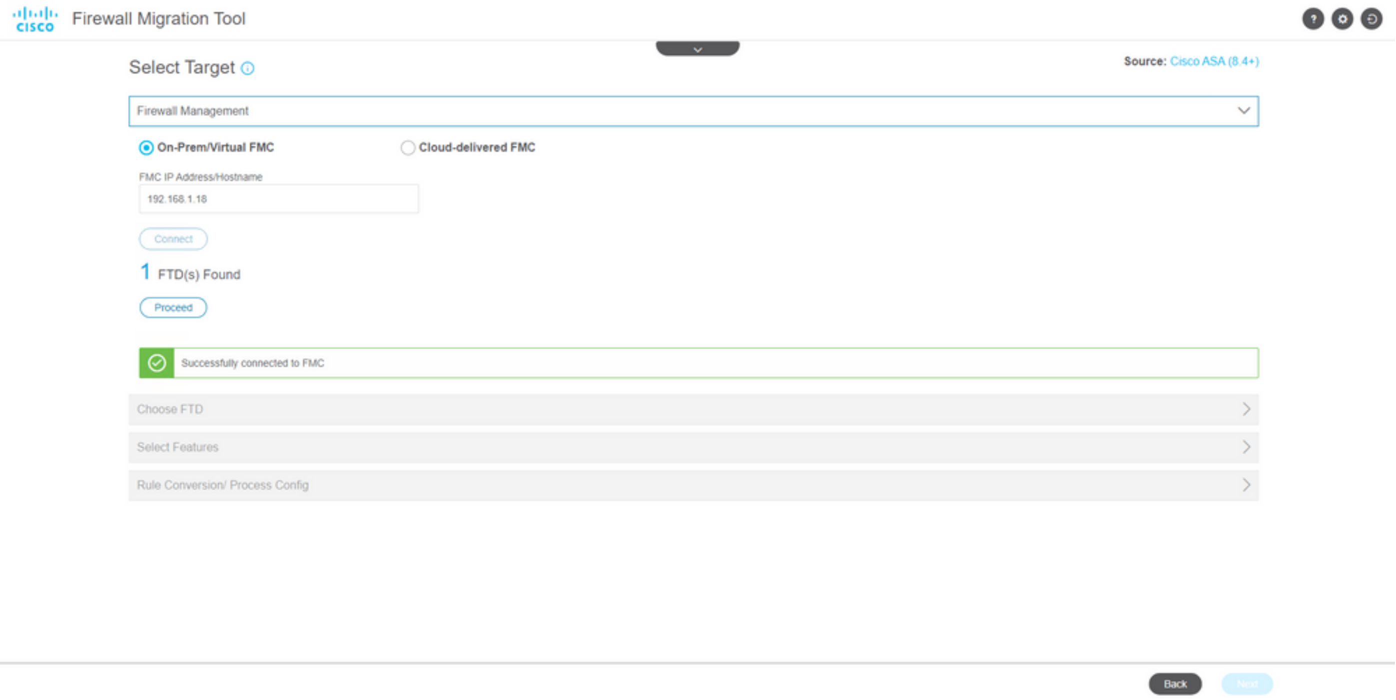
Parsed Summary

Collect Hitcounts: No

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

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

8. 选择要用于迁移的目标FMC。 提供FMC的IP。 它会打开一个弹出窗口，提示您输入FMC的登录凭证。



Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

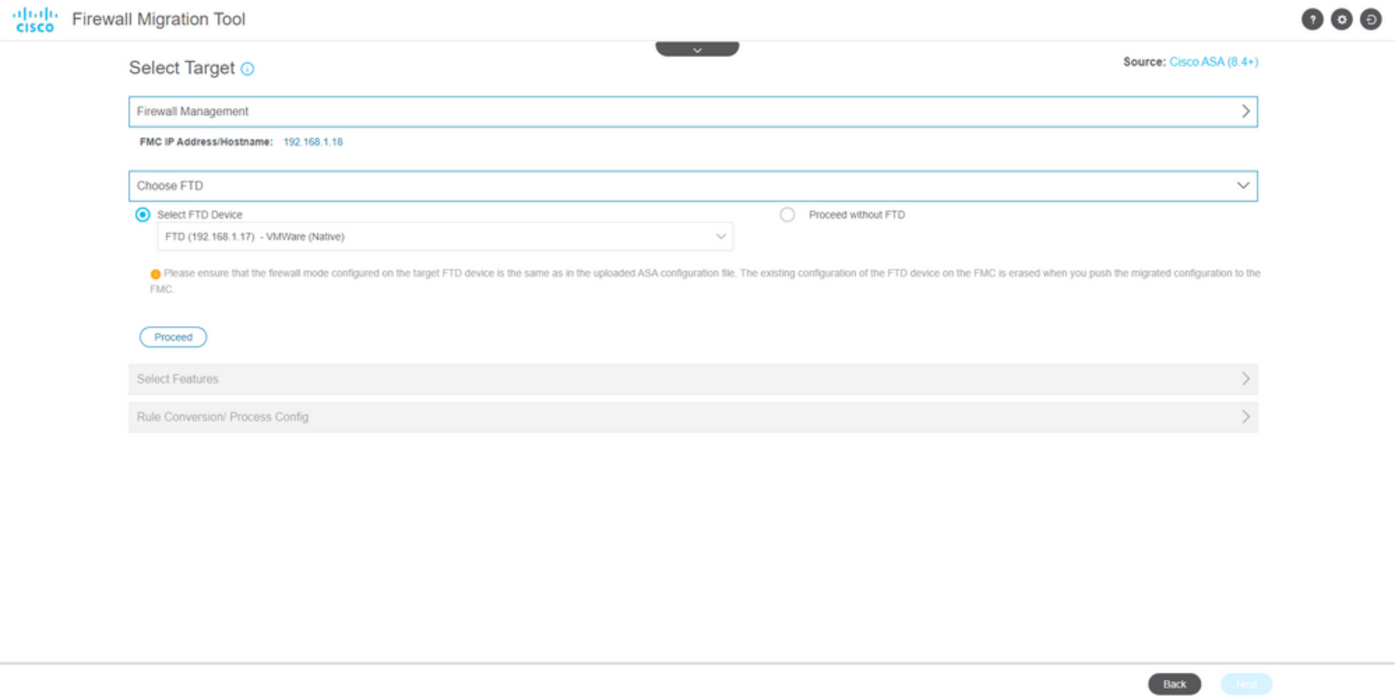
● On-Prem/Virtual FMC ○ Cloud-delivered FMC

FMC IP Address/Hostname: 192.168.1.18

1 FTD(s) Found

Successfully connected to FMC

9. *（可选）*选择要使用的目标FTD。 如果选择迁移到FTD，请选择要使用的FTD。如果不想使用FTD，可以填写此复选框 Proceed without FTD



Firewall Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

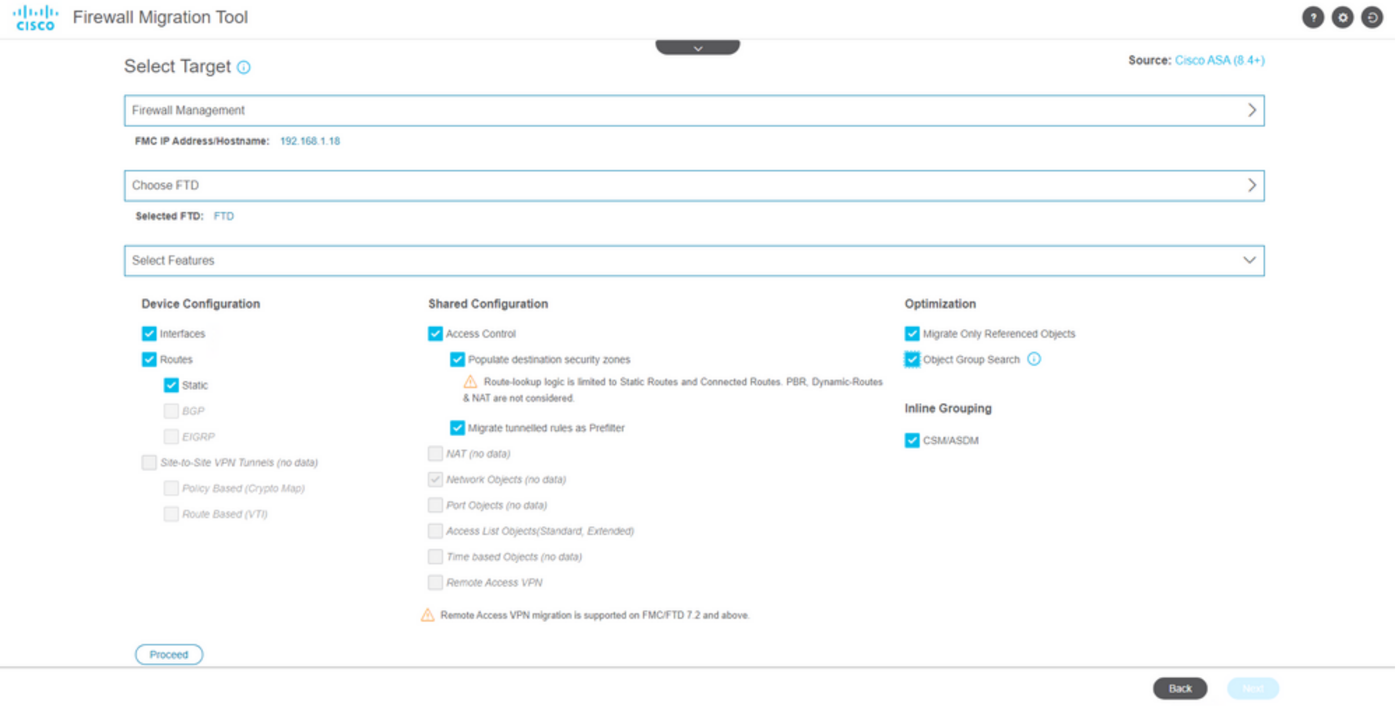
Choose FTD

● 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.

10. 选择要迁移的配置，屏幕截图上显示选项。



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.

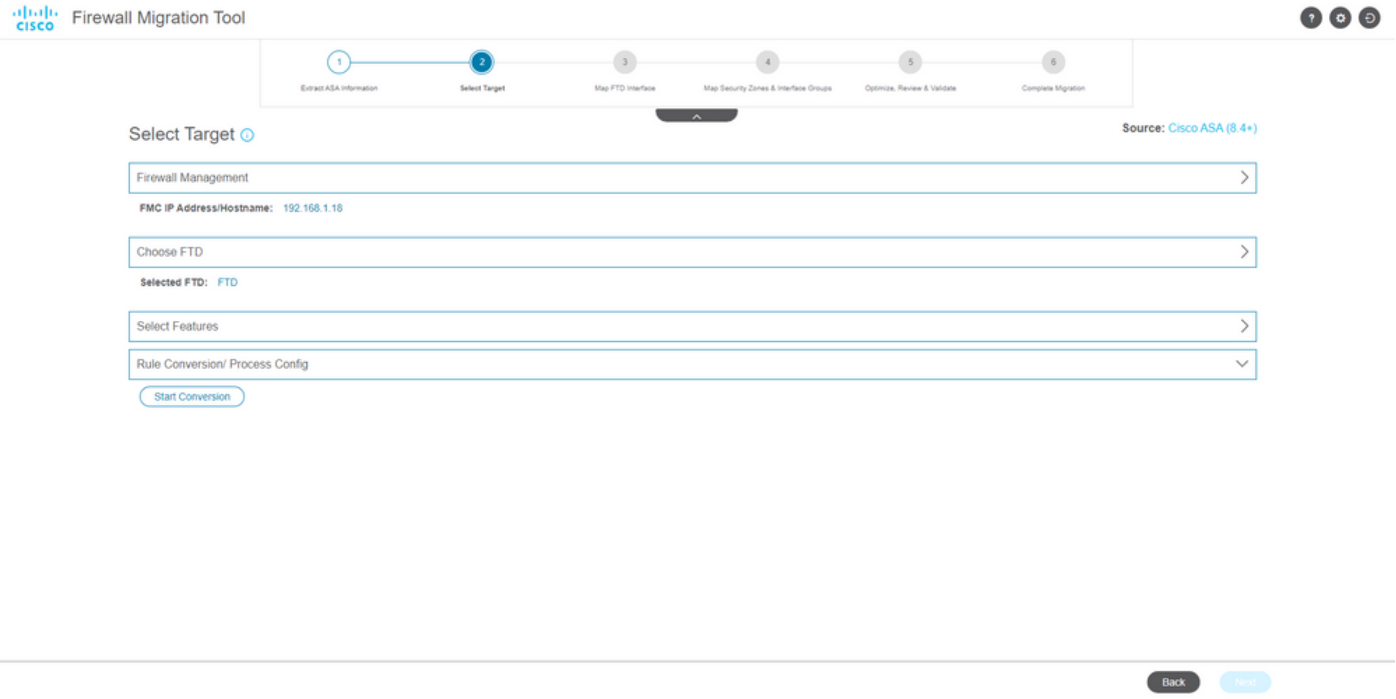
Optimization

☑ Migrate Only Referenced Objects
☑ Object Group Search

Inline Grouping

☑ CSM/ASDM

11. 开始将配置从ASA转换为FTD。



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

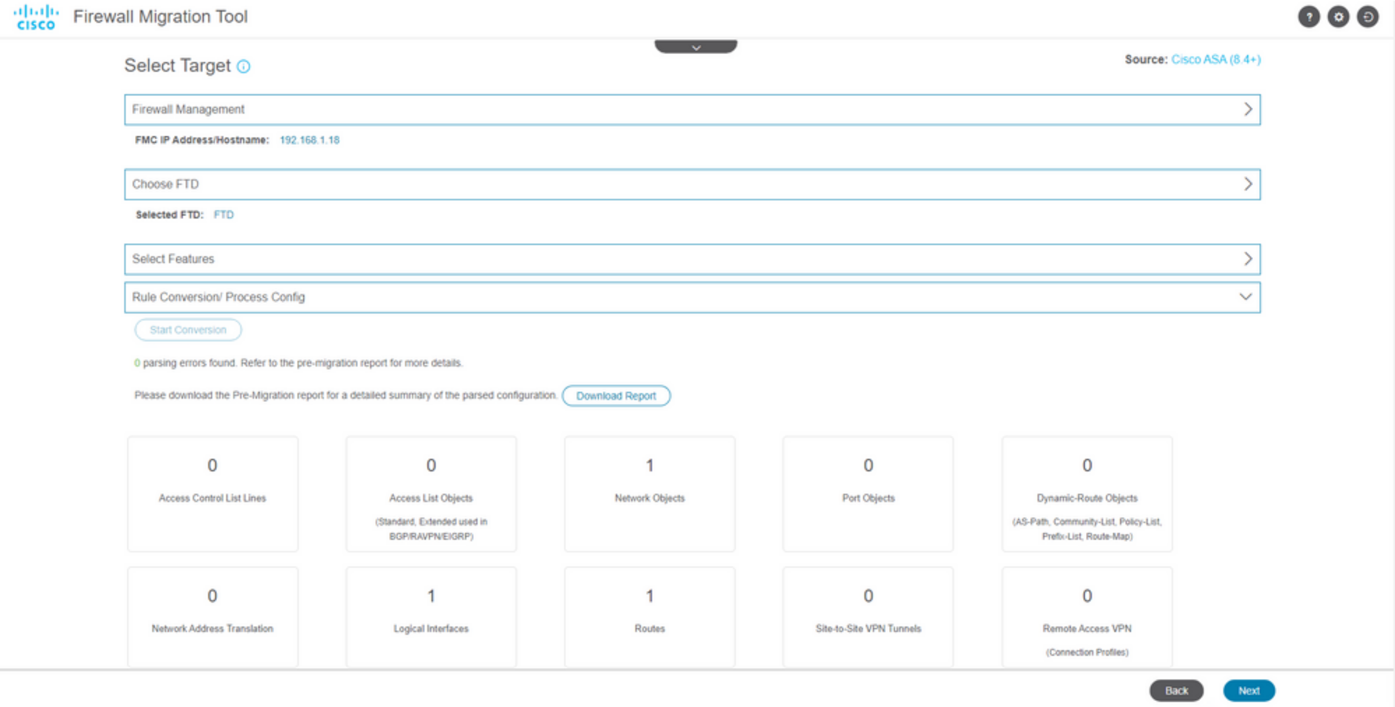
Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

12. 转换完成后，将显示一个控制面板，其中包含要迁移的对象（仅限于兼容性）的摘要。 您也可以点击 **Download Report** 接收要迁移的配置摘要。



Firewall Migration Tool

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

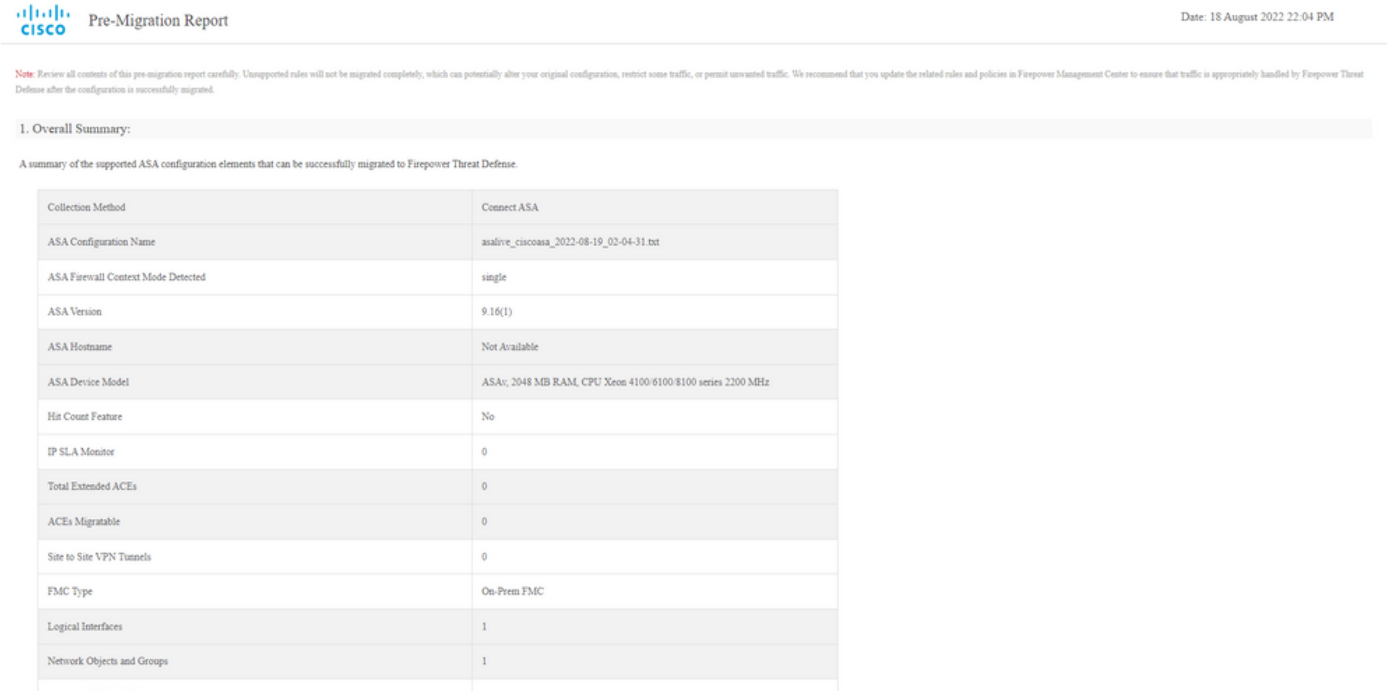
Start Conversion

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

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

迁移前报告示例，如图所示：



Pre-Migration Report

Date: 18 August 2022 22:04 PM

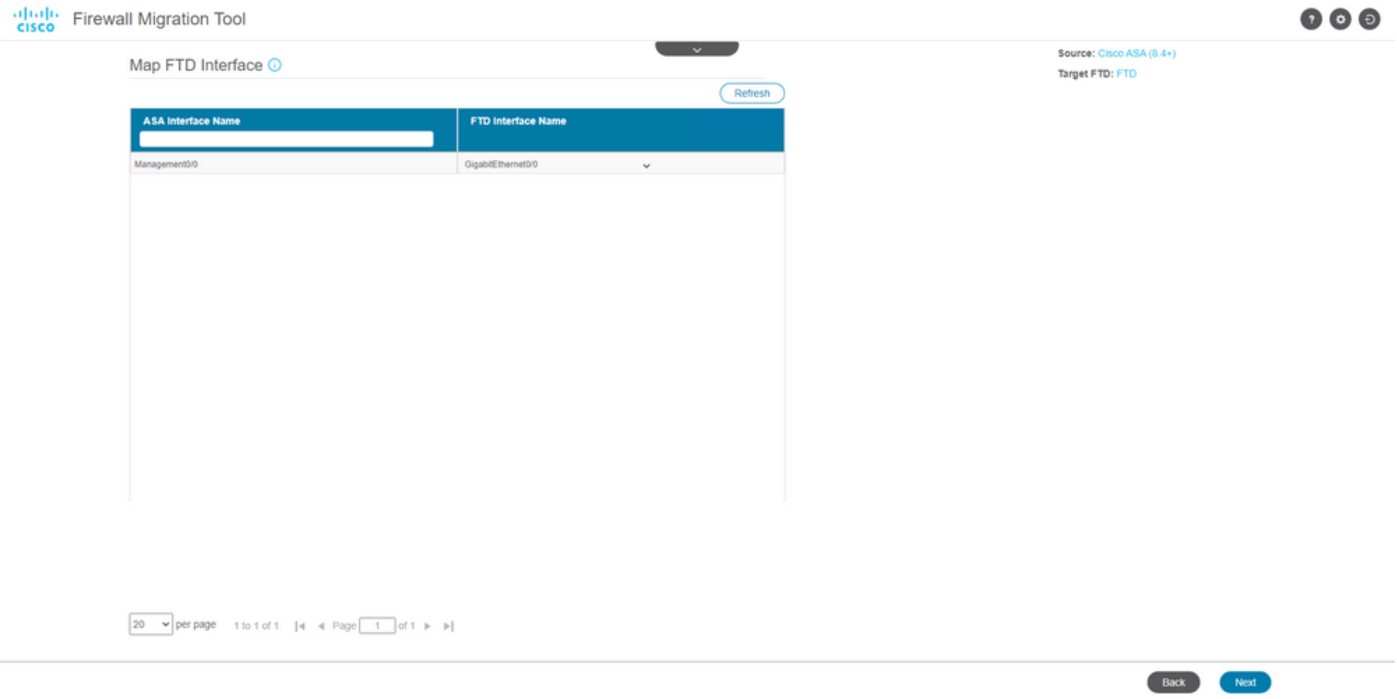
Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management 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_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	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

13. 将ASA接口与迁移工具上的FTD接口映射。



Firewall Migration Tool

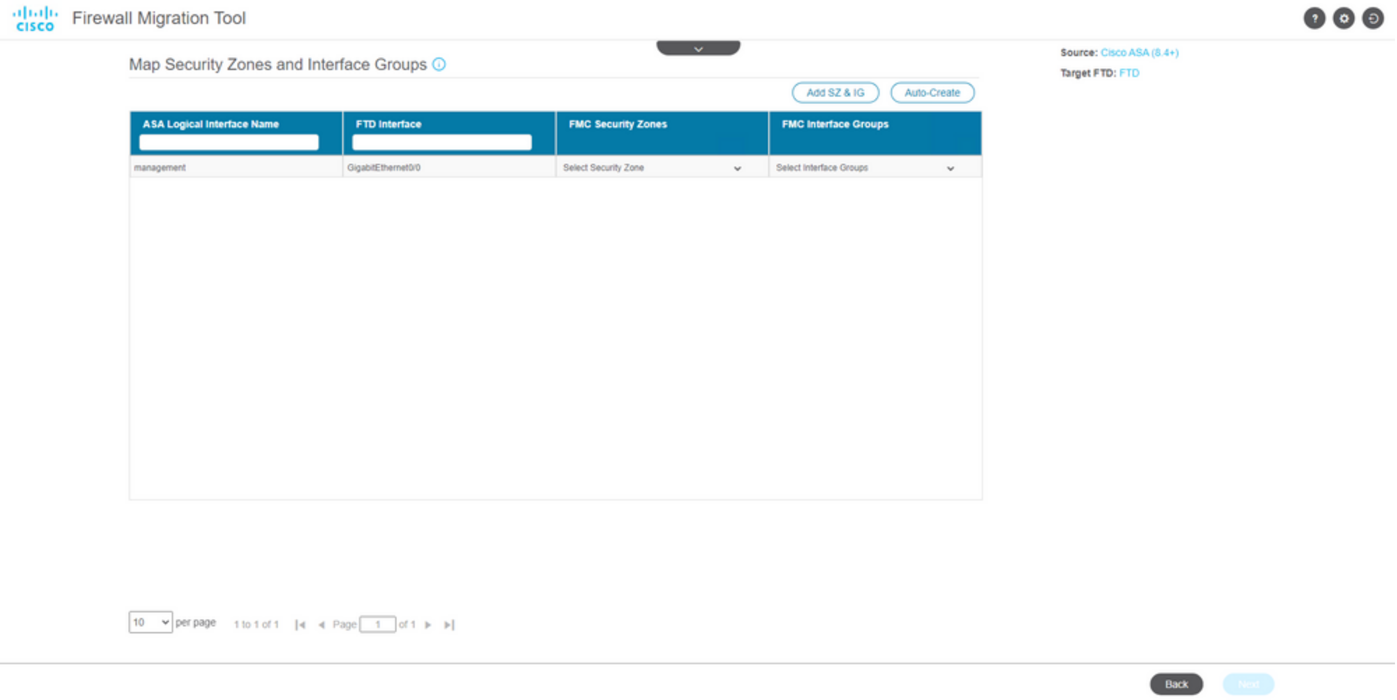
Map FTD Interface

Source: Cisco ASA (8.4+)

Target FTD: FTD

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

14. 为FTD上的接口创建安全区域和接口组



Firewall Migration Tool

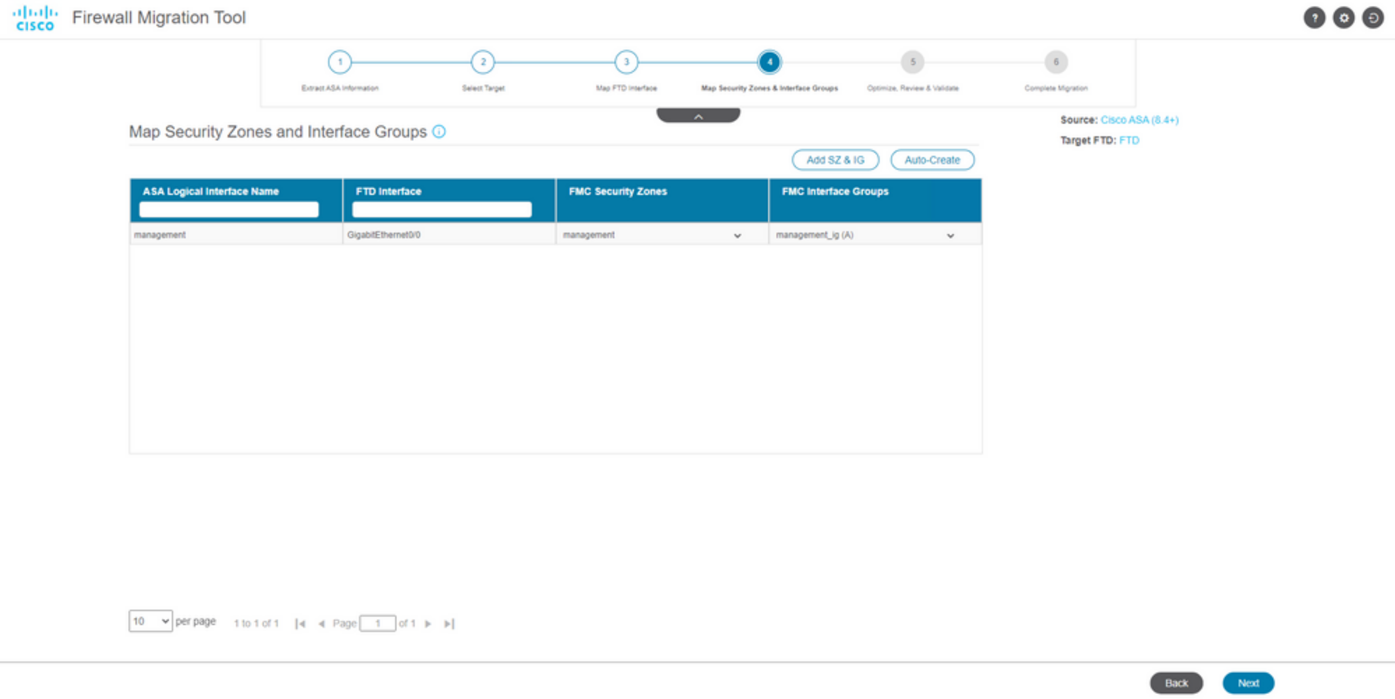
Map Security Zones and Interface Groups

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

安全区域(SZ)和接口组(IG)由该工具自动创建，如图所示：

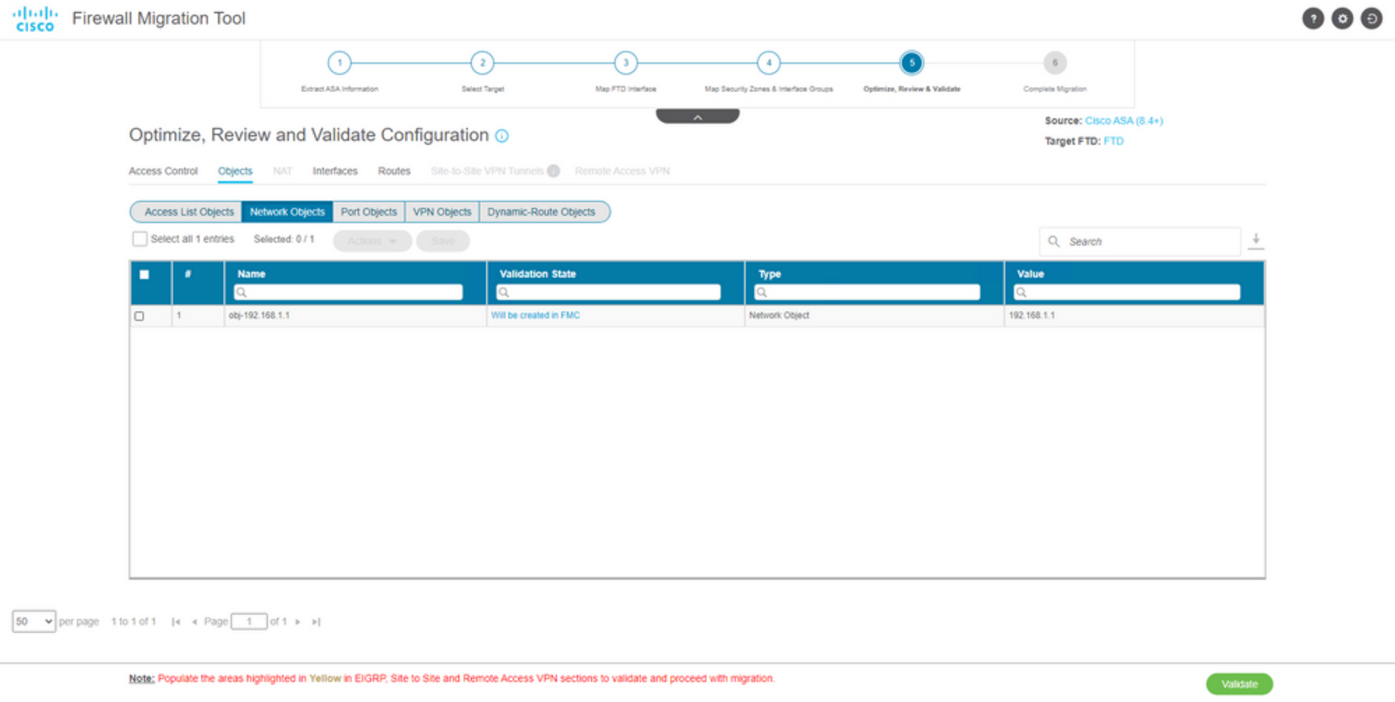

Firewall Migration Tool
1 Extract ASA Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Optimize, Review & Validate
6 Complete Migration
Add SZ & IG
Auto-Create
10 per page 1 to 1 of 1 Page 1 of 1
Back
Next

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	management	management_ig (A)

15. 查看并验证要在迁移工具上迁移的配置。
    如果您已完成配置的审核和优化，请单击 Validate.



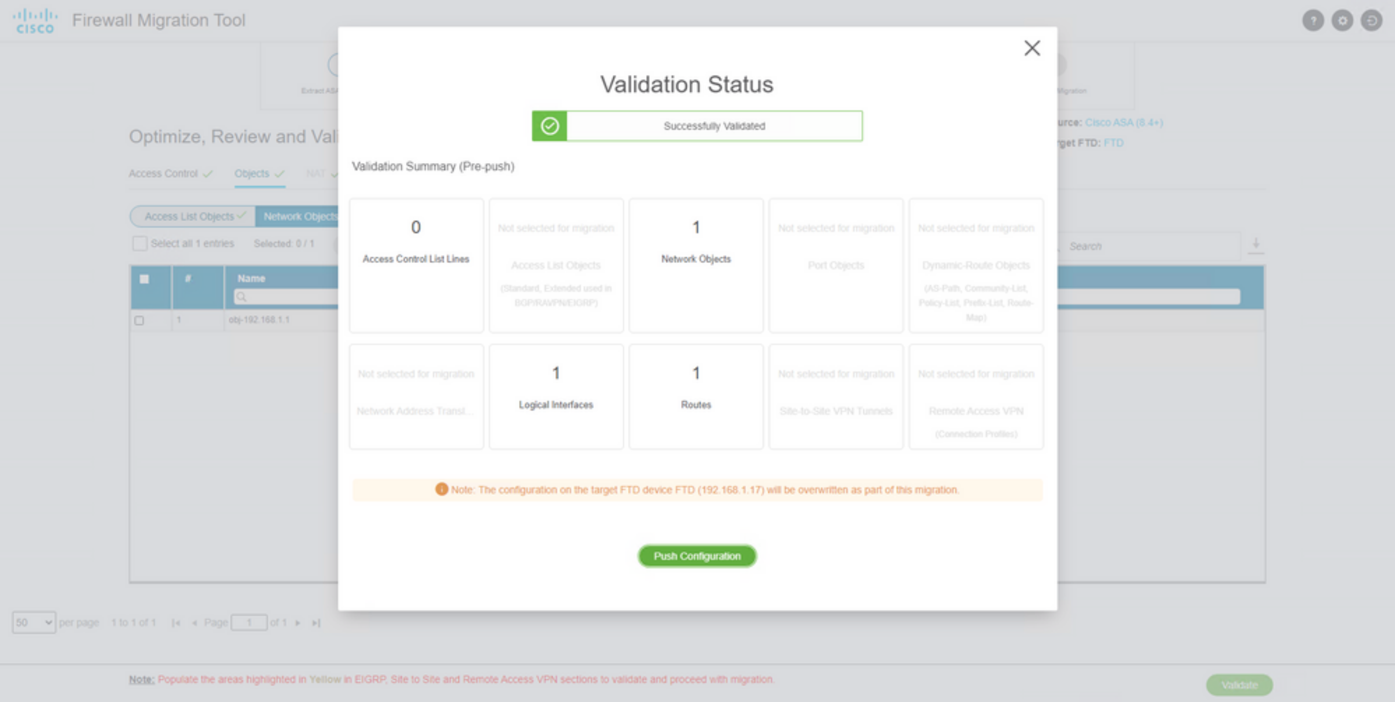
Optimize, Review and Validate Configuration

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

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

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

16. 如果验证状态成功，将配置推送到目标设备。



Validation Status

Successfully Validated

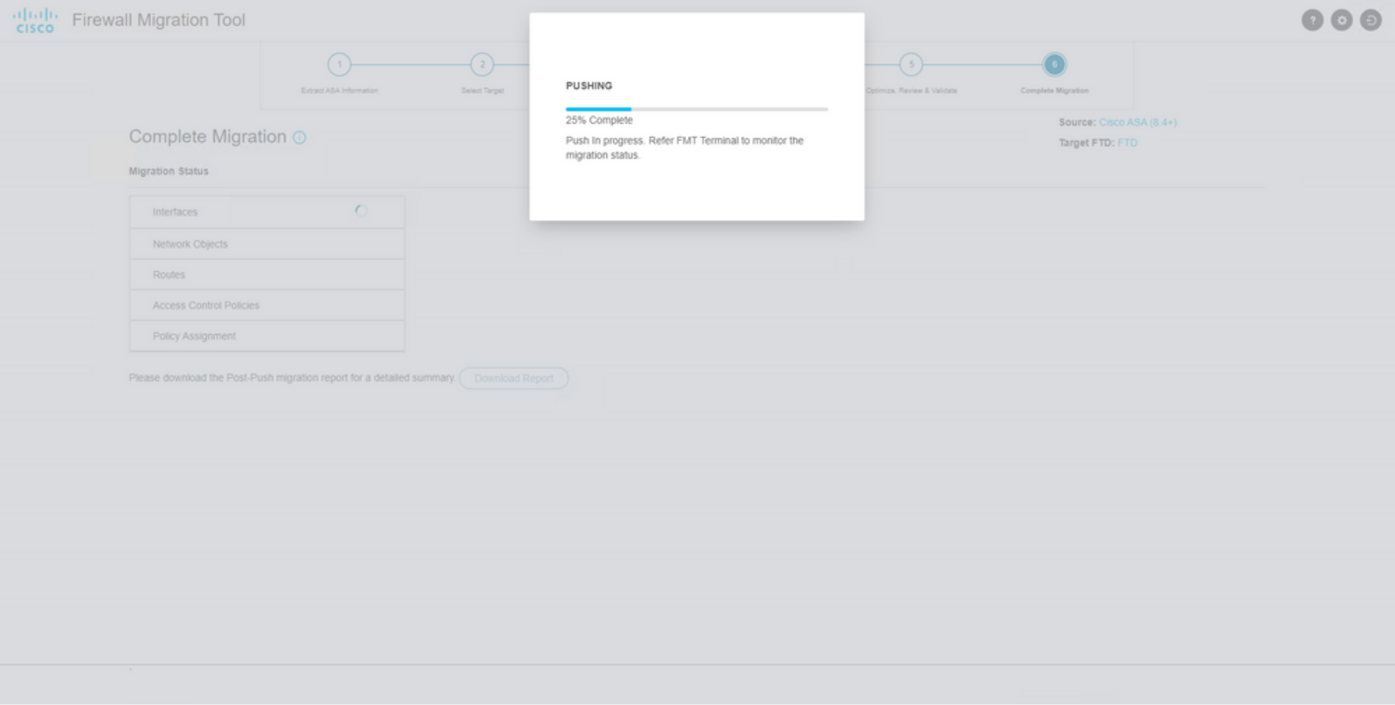
Validation Summary (Pre-push)

0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration Network Address Transl...	1 Logical Interfaces	1 Routes	Not selected for migration Site-to-Site VPN Tunnels	Not selected for migration Remote Access VPN (Connection Profiles)

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

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

通过迁移工具推送的配置示例，如图所示：



PUSHING

25% Complete

Push In progress. Refer FMT Terminal to monitor the migration status.

Source: Cisco ASA (8.4+)

Target FTD: FTD

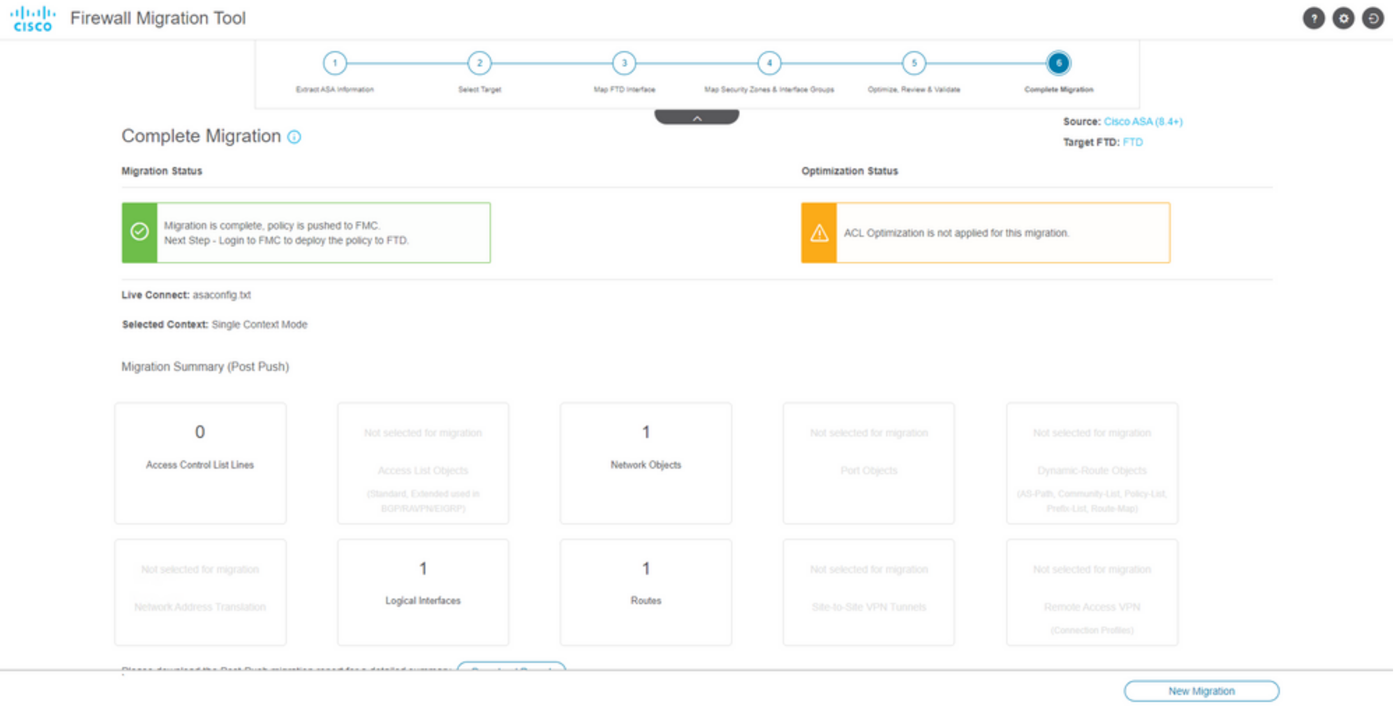
Complete Migration

Migration Status

- Interfaces
- Network Objects
- Routes
- Access Control Policies
- Policy Assignment

Please download the Post-Push migration report for a detailed summary.

成功迁移的示例，如图所示：


Firewall Migration Tool

1 Extract ASA Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Optimize, Review & Validate
6 Complete Migration

Complete Migration

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

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.

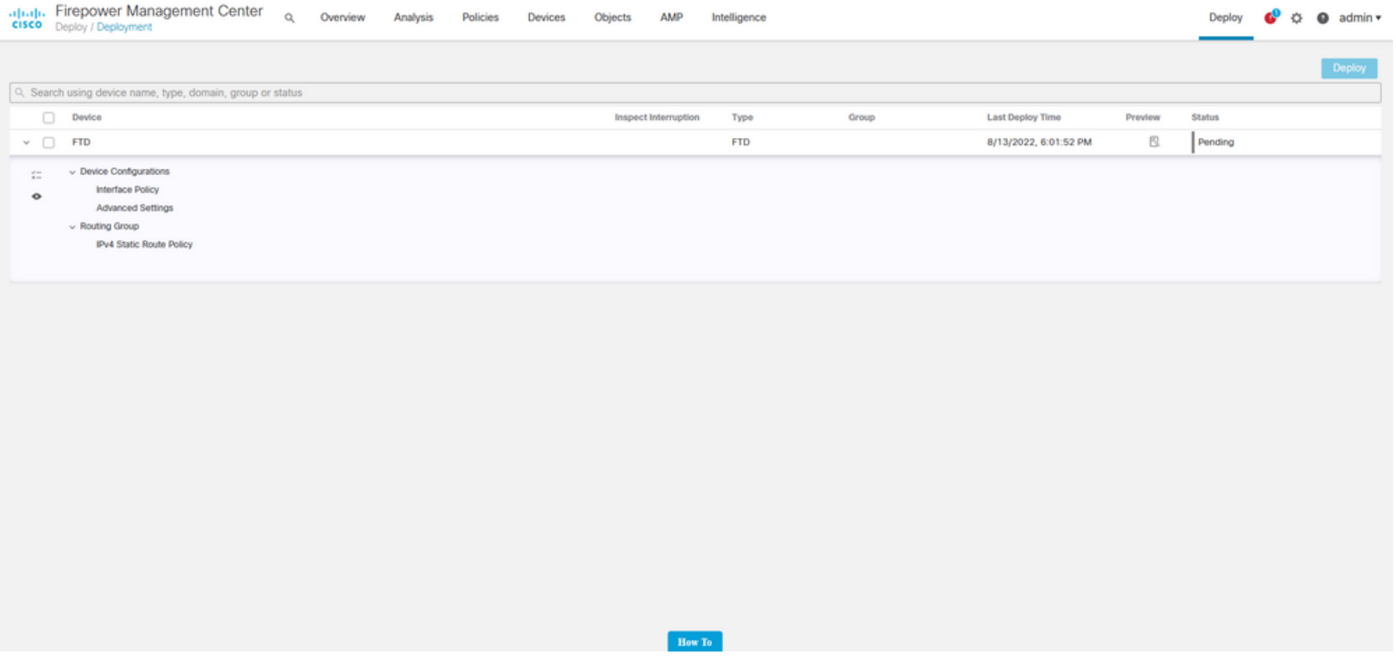
Live Connect: asaconfig.txt

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/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-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)

17. *(可选)*如果选择将配置迁移到FTD，则需要部署将可用配置从FMC推送到防火墙，以便部署配置： 登录到FMC GUI。导航至 Deploy 选项卡。选择要将配置推送到防火墙的部署。点击 Deploy。


Firepower Management Center
Deploy / Deployment

	Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
□	FTD		FTD		8/13/2022, 6:01:52 PM		Pending

- Device Configurations
  - Interface Policy
  - Advanced Settings
- Routing Group
  - IPv4 Static Route Policy

故障排除

本部分提供的信息可用于对配置进行故障排除。

验证放置了Firepower迁移工具文件的目录中的日志，例如：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。