

使用FMT将ASA迁移到Firepower威胁防御(FTD)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[概述](#)

[背景信息](#)

[获取ASAConfiguration文件](#)

[从ASA导出PKI证书并导入管理中心](#)

[检索AnyConnect软件包和配置文件](#)

[配置](#)

[配置步骤:](#)

[故障排除](#)

[安全防火墙迁移工具故障排除](#)

简介

本文档介绍将Cisco自适应安全设备(ASA)迁移到Cisco Firepower威胁设备的过程。

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)v7.0.1的Mac OS
- 自适应安全设备(ASA)v9.16(1)
- 安全防火墙管理中心(FMCv)v7.4.2
- 安全防火墙威胁防御虚拟(FTDv)v7.4.1

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。

概述

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+)
 - 思科安全防火墙设备管理器(7.2+)
 - 检查点(r75-r77)
 - 检查点(r80)
 - Fortinet(5.0+)
- Palo Alto Networks(6.1+)

背景信息

在迁移ASA配置之前，请执行以下活动：

获取ASA配置文件

要迁移ASA设备，请使用单情景的show running-config或多情景模式的show tech-support获取配置，将其另存为.cfg或.txt文件，然后使用安全防火墙迁移工具将其传输到计算机。

从ASA导出PKI证书并导入管理中心

使用此命令通过CLI将带密钥的PKI证书从源ASA配置导出到PKCS12文件：

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

然后，将PKI证书导入管理中心（对象管理PKI对象）。有关详细信息，请参阅[Firepower管理中心配置指南](#)中的PKI对象。

检索AnyConnect软件包和配置文件

AnyConnect配置文件是可选的，可以通过管理中心或安全防火墙迁移工具上传。

使用此命令将所需的软件包从源ASA复制到FTP或TFTP服务器：

```
复制<源文件位置：/源文件名> <目标>
```

```
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <-----复制  
Anyconnect软件包的示例。
```

```
ASA# copy disk0:/ external-ss0- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <-----复制外部浏览器软  
件包的示例。
```

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <-----复制Hostscan软件包的示例。

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <-----复制Dap.xml的示例

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <-----复制Data.xml的示例

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <复制Anyconnect配-----文件的示例。

将下载的软件包导入管理中心(对象管理 > VPN > AnyConnect文件)。

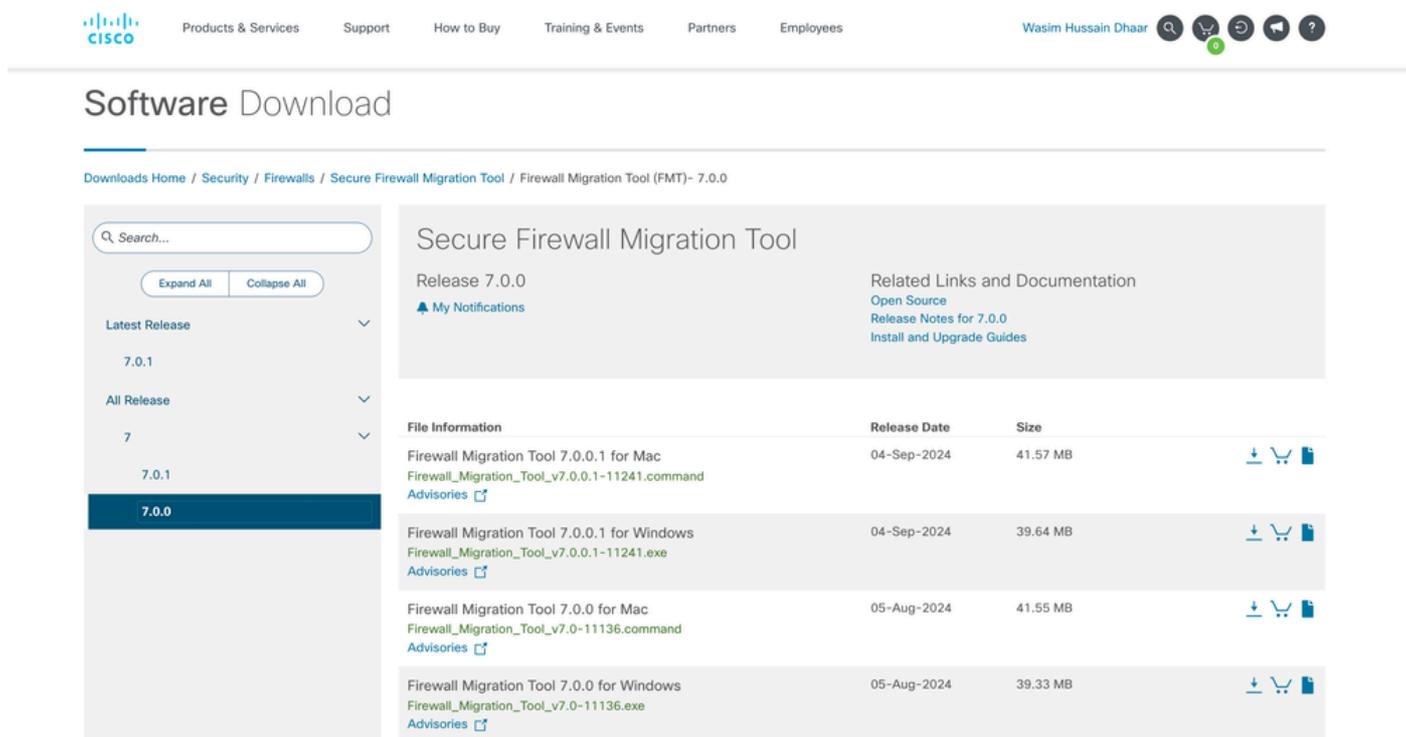
a-Dap.xml和Data.xml必须从Review and Validate > Remote Access VPN > AnyConnect File部分的安全防火墙迁移工具上传到管理中心。

b-AnyConnect配置文件可以直接上传到管理中心，也可以通过审核和验证 > 远程访问VPN > AnyConnect文件部分中的安全防火墙迁移工具上传。

配置

配置步骤:

1.下载 思科软件中心最新的Firepower迁移工具：

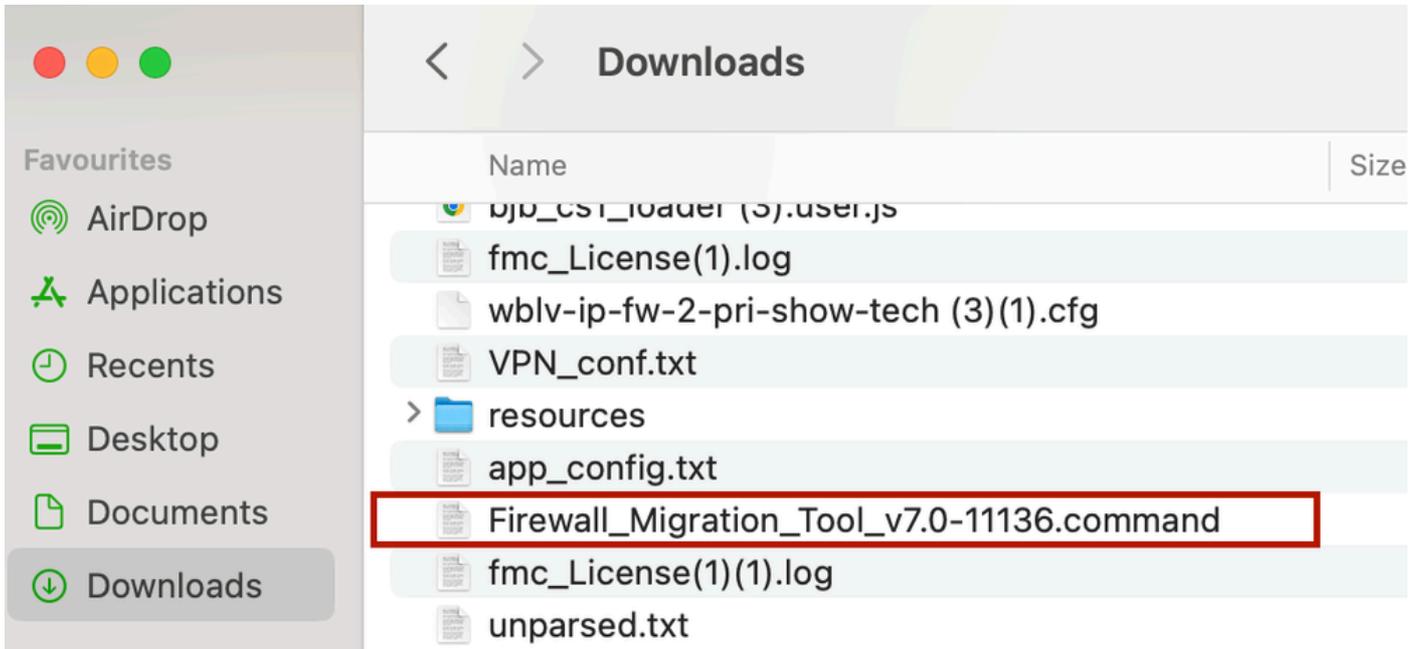


The screenshot shows the Cisco Software Download page for the Secure Firewall Migration Tool (FMT) 7.0.0. The page includes a search bar, navigation tabs (Products & Services, Support, How to Buy, Training & Events, Partners, Employees), and a user profile (Wasim Hussain Dhaar). The main content area displays the title "Secure Firewall Migration Tool" and "Release 7.0.0". Below this, there is a table of file information with columns for File Information, Release Date, and Size. The table lists four download options for Mac and Windows, with their respective release dates and sizes. A sidebar on the left shows a search bar and a list of release versions (7.0.1, 7.0.0) with expand/collapse buttons.

File Information	Release Date	Size	
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command Advisories	04-Sep-2024	41.57 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe Advisories	04-Sep-2024	39.64 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command Advisories	05-Aug-2024	41.55 MB	↓ 🛒 📄
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe Advisories	05-Aug-2024	39.33 MB	↓ 🛒 📄

软件下载

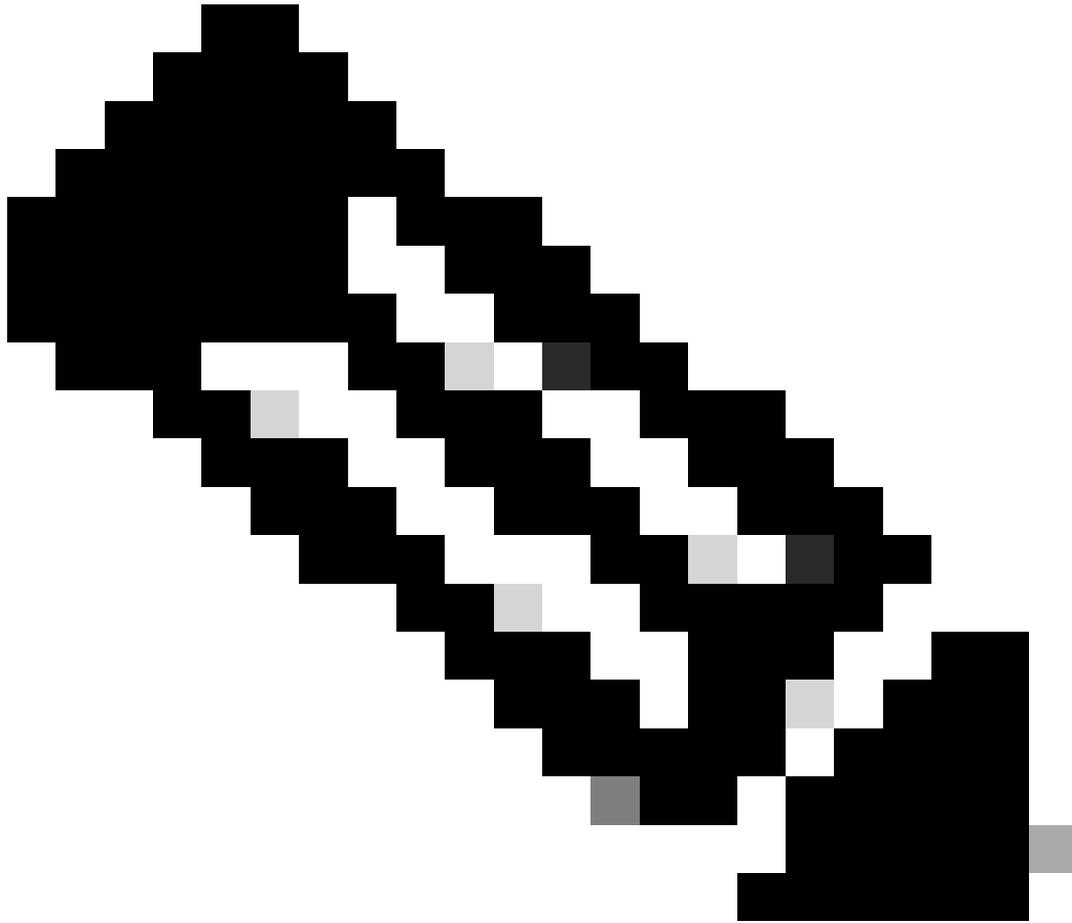
2. 单击之前下载到计算机的文件。



文件

```
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 pol
icy configurations from your FDM-managed device to a threat defense device.'], '
Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migr
ate the site-to-site VPN (policy-based) configurations on your Check Point firew
all ( R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortinet
Firewall - Optimize your application access control lists (ACLs) when migratin
g configurations from a Fortinet firewall to your threat defense device.']], 'se
curity_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 t
o 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 t
o 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 -
```

控制台记录



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。

-
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。
 1. 选中此复选框可接受条款和条件。
 2. 点击Proceed。

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/software/terms (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 makes no warranty, in any 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



EULA

4. 使用有效的CCO帐户登录，并且FMT GUI界面显示在Web浏览器上。



Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

FMT登录

5. 选择要迁移的源防火墙。



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，请单击Next。

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

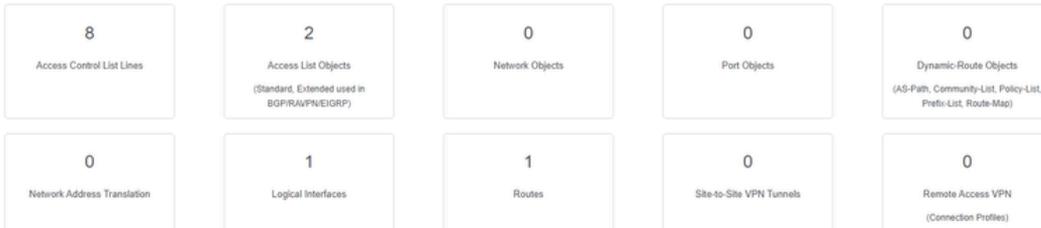
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary ▾

Collect Hitcounts: No



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

https://cisco.com

Back

Next

摘要

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。

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

FMC IP

9. (可选) 选择要使用的目标FTD。

1. 如果选择迁移到FTD，请选择要使用的FTD。
2. 如果不想使用FTD，可以填写此复选框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

FTD (192.168.1.17) - VMWare (Native) v

 Proceed without FTD

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

目标FTD

10. 选择要迁移的配置，屏幕截图上会显示选项。

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

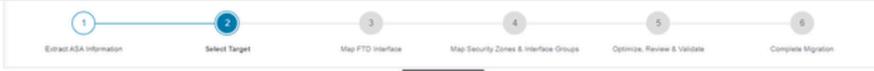
Proceed

Back

Next

配置

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

Start Conversion

Back Next

开始转换

- 转换完成后，它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。

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 BGPRAVP/NEIGRP)	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)

Back Next

下载报告

迁移前报告示例，如图所示：

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	ASA; 2048 MB RAM, CPU Xeon 4100 6100 8100 series 2200 MHz
Hat 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

迁移前报告

13. 将ASA接口映射到迁移工具上的FTD接口。

The screenshot shows the 'Map FTD Interface' screen in the Cisco Firewall Migration Tool. The interface includes a table with two columns: 'ASA Interface Name' and 'FTD Interface Name'. The first row shows 'Management0/0' mapped to 'GigabitEthernet0/0'. The tool also displays 'Source: Cisco ASA (8.4+)' and 'Target FTD: FTD'. Navigation buttons for 'Back' and 'Next' are visible at the bottom right, and a pagination control is at the bottom left.

映射接口

14. 为FTD上的接口创建安全区域和接口组

Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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

安全区域和接口组

安全区域(SZ)和接口组(IG)由该工具自动创建，如图所示：



Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

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)

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

Back Next

自动创建工具

15. 查看并验证要在迁移工具上迁移的配置。

1. 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

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

#	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

审核和验证

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)

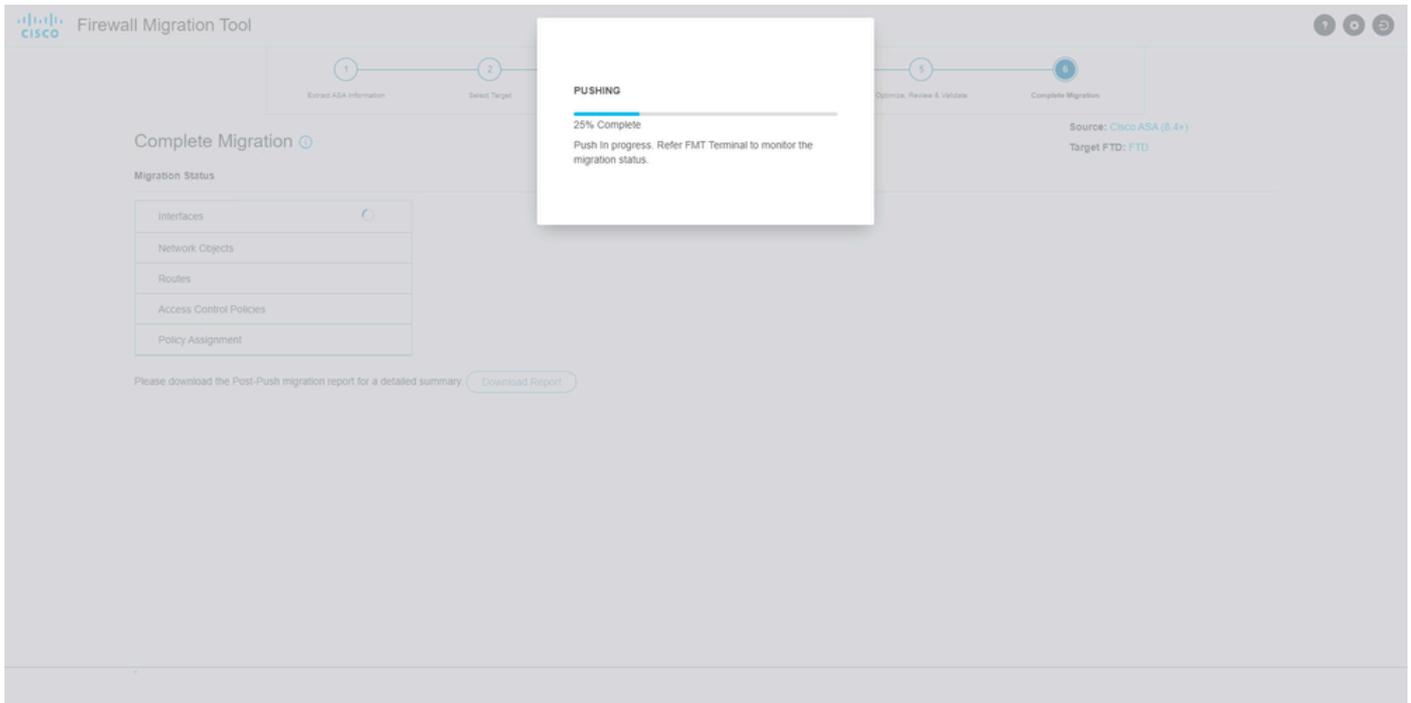
0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected 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.

Push Configuration

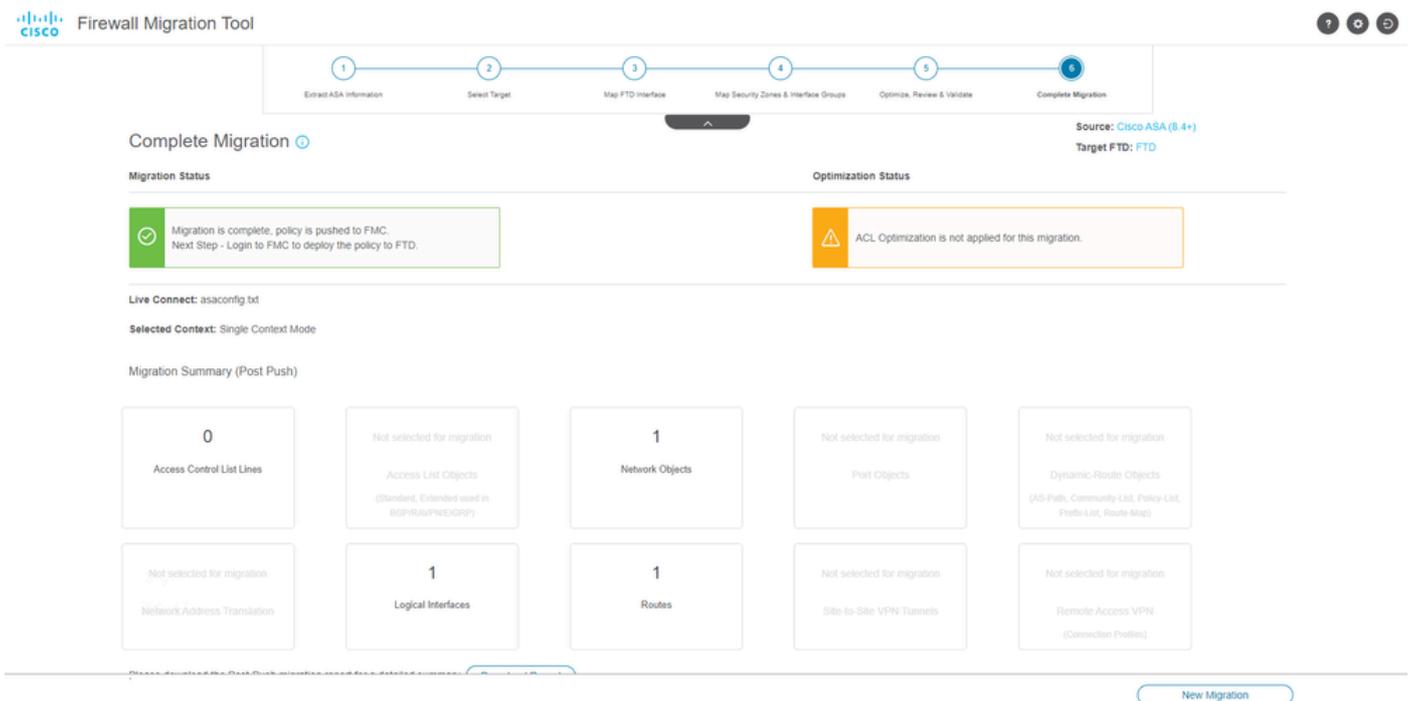
验证

通过迁移工具推送的配置示例，如图所示：



推送

成功迁移的示例，如图所示：



成功迁移

(可选) 如果选择将配置迁移到FTD，则需要部署以将可用配置从FMC推送到防火墙。

要部署配置，请执行以下操作：

1. 登录到FMC GUI。
2. 导航到选Deploy项卡。
3. 选择要将配置推送到防火墙的部署。

4. 单击。Deploy

故障排除

安全防火墙迁移工具故障排除

- 常见迁移失败：
 - ASA配置文件中未知或无效的字符。
 - 配置元素缺失或不完整。
 - 网络连接问题或延迟。
 - ASA配置文件上传或将配置推送到管理中心时出现问题。
 - 常见问题包括：
- 使用支持捆绑包进行故障排除：
 - 在“Complete Migration”（完成迁移）屏幕上，单击Support按钮。
 - 选择Support Bundle并选择要下载的配置文件。
 - 默认情况下会选择日志文件和数据库文件。
 - 单击Download获取.zip文件。
 - 解压缩.zip以查看日志、数据库和配置文件。
 - 单击Email us将故障详细信息发送给技术团队。
 - 在邮件中附加支持捆绑包。
 - 单击访问TAC页面以创建思科TAC案例以获取帮助。
 - 该工具允许您下载日志文件、数据库和配置文件的支持捆绑包。
 - 下载步骤：
 - 如需更多支持：

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）。