

Configurar a Secure Firewall Migration Tool para migração do ASA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuration Steps](#)

[Troubleshoot](#)

Introduction

Este documento descreve o procedimento para migrar o Cisco Adaptive Security Appliance (ASA) para o Cisco Firepower.

Contribuição de Ricardo Vera, engenheiro do Cisco TAC.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do Cisco Firewall Threat Defense (FTD) e do Adaptive Security Appliance (ASA).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os requisitos específicos deste documento incluem:

- Cisco Adaptive Security Appliance (ASA) versão 8.4 ou posterior
- Secure Firewall Management Center (FMCv) versão 6.2.3 ou posterior

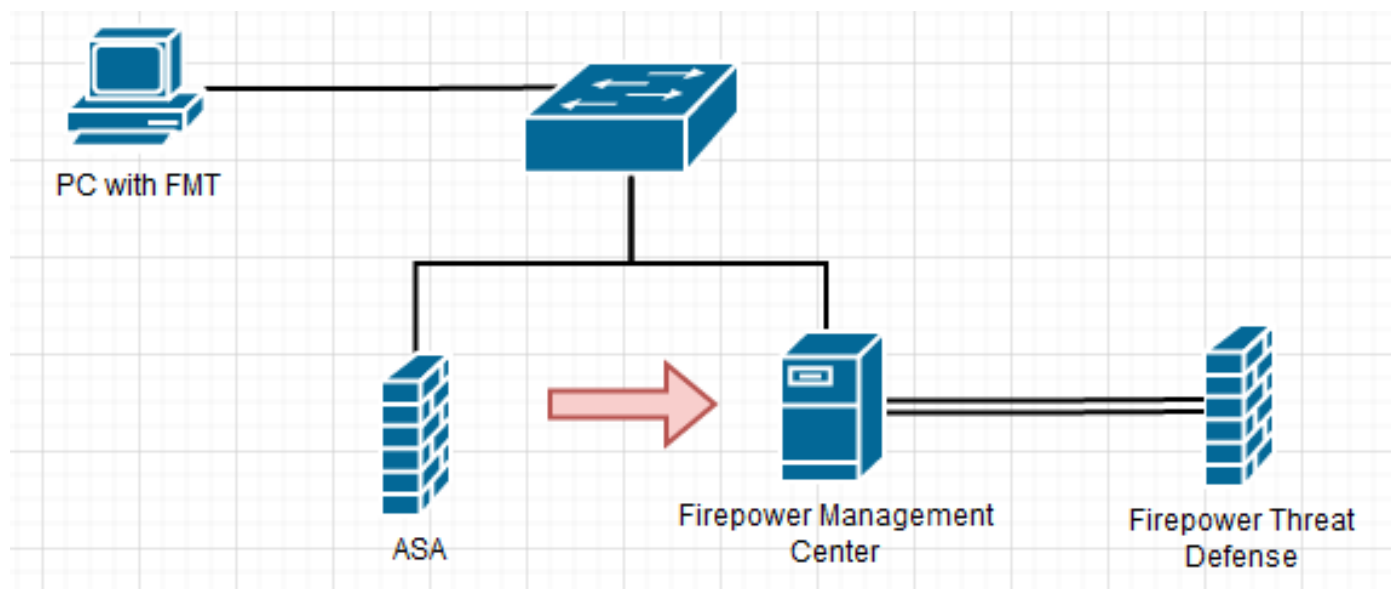
A Ferramenta de Migração de Firewall suporta esta lista de dispositivos:

- Cisco ASA (8,4+)
- Cisco ASA (9.2.2+) com FPS
- Ponto de verificação (r75-r77)
- Ponto de verificação (r80)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Antes de prosseguir com a migração, considere as [Diretrizes e Limitações da Ferramenta de Migração de Firewall](#).

Configurar

Diagrama de Rede



Configuration Steps

1. **Faça o download** da ferramenta de migração do Firepower mais recente na Cisco Software Central:

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

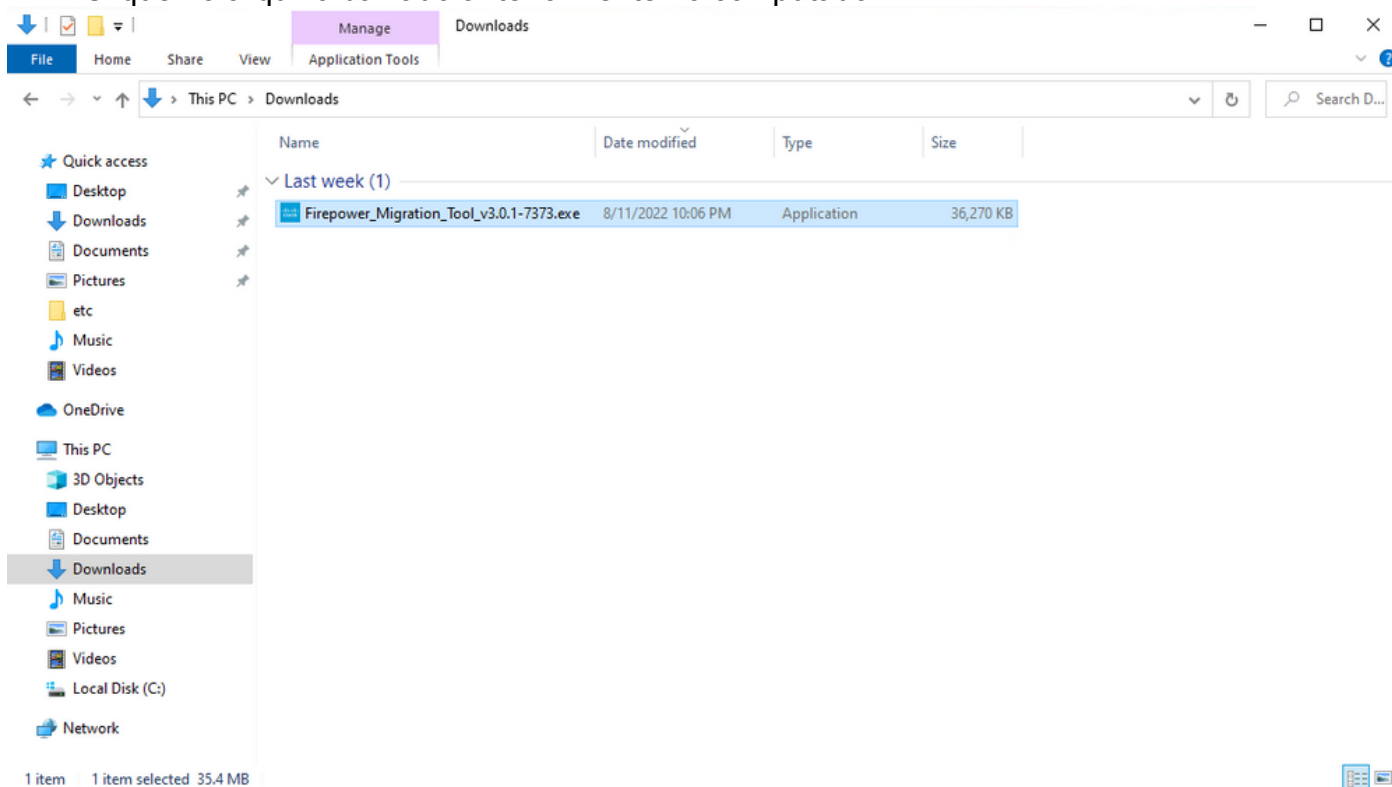
[Open Source](#)

[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 Shopping 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 Shopping 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 Shopping Cart Share

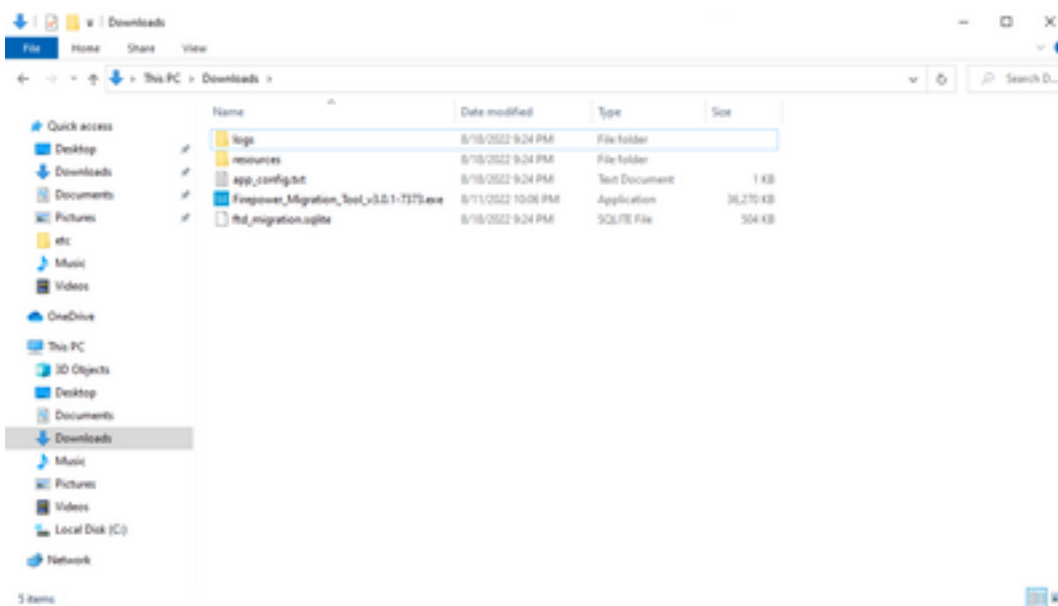
2. Clique no arquivo baixado anteriormente no computador.



Note: O programa é aberto automaticamente e um console gera automaticamente o conteúdo no diretório onde você executou o arquivo.

```
C:\Users\cali\Downloads\Firepower_Migration_Tool_v1.0.1-7171.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:[0817373]"
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 auth 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.a0d79d8031ca159b236f.bundle.css HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /inline.318b58c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /cui-font.880241c8aa87aa899c6a.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. Depois de executar o programa, ele abre um navegador que exibe o "Contrato de licença de usuário final". Marque a caixa de seleção para aceitar termos e condições. Clique em **Continuar**.

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 is not intended to be a license to Use the Software. You are not licensed to Use the Software for any other purpose.

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

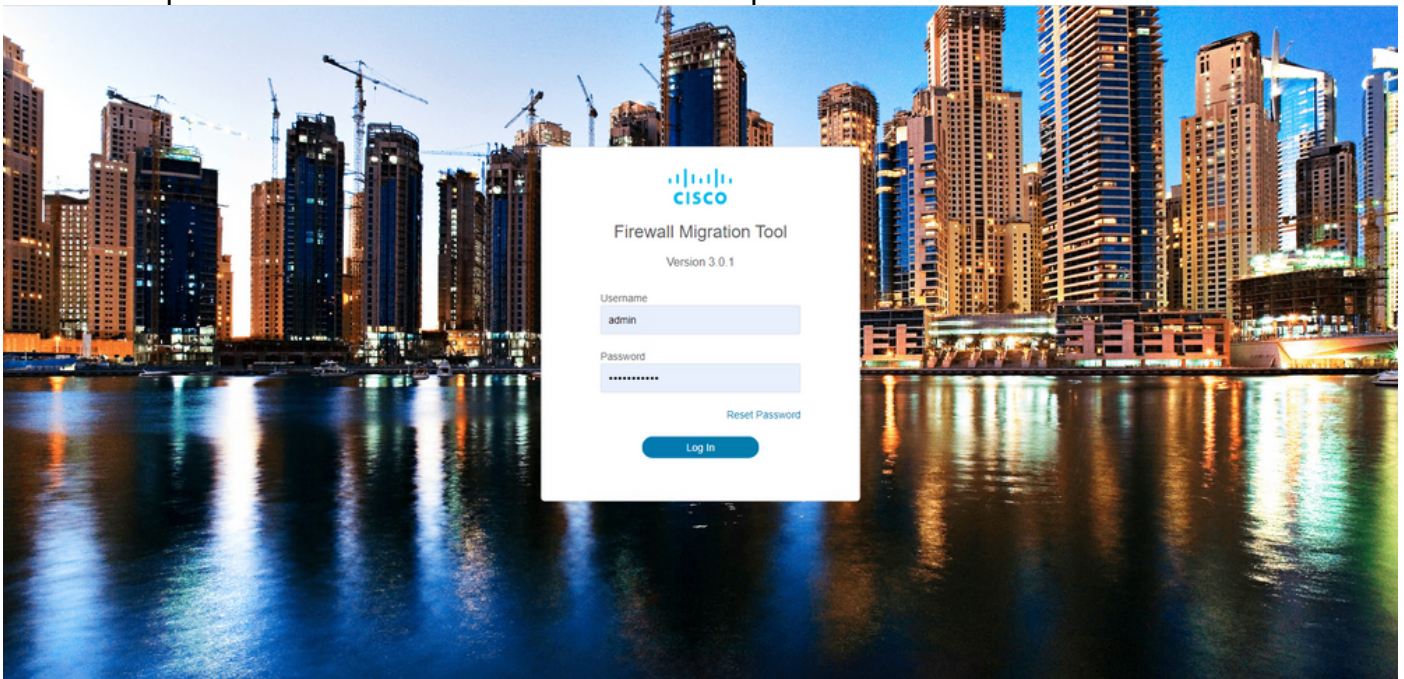


Extract Source Information

Any additional information explaining this



4. Faça login na ferramenta de migração. Você pode fazer login com a conta CCO ou com a conta padrão local. As credenciais da conta padrão local são: admin/Admin123



5. Selecione o firewall de origem a ser migrado. Neste exemplo, o Cisco ASA (8.4+) é usado como origem.

Select Source Configuration

Source Firewall Vendor

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FPS
- Check Point (75-77)
- Check Point (80)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Cisco ASA (8.4+) Pre-Migration Instructions

1 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. Selecione o método de extração a ser usado para obter a configuração. O carregamento manual requer que você carregue o Running Config arquivo do ASA no formato ".cfg" ou ".txt". Conecte-se ao ASA para extrair configurações diretamente do firewall.

1 2 3 4 5 6

Extract ASA Information Select Target Map FTD Interface Map Security Zones & Interface Groups Optimize, Review & Validate Complete Migration

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.

Upload

Connect to ASA

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

ASA IP Address/Hostname

Connect

Context Selection >

Parsed Summary >

Back

Next

Note: Para este exemplo, conecte-se diretamente ao ASA.

7. Um resumo da configuração encontrada no firewall é exibido como um painel. Clique em **Avançar**.

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

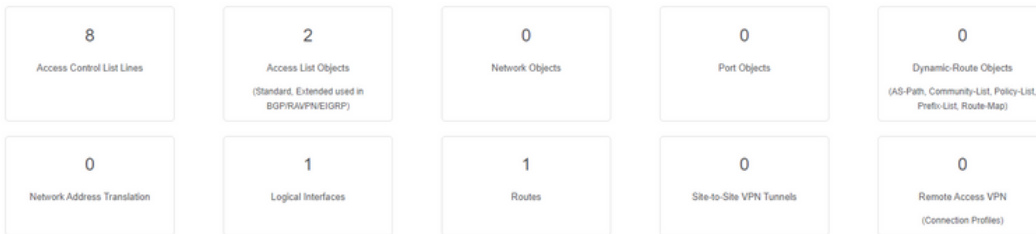
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



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

8. Selecione o FMC de destino a ser usado na migração. Indicar o IP do CVP. Ele abre uma janela pop-up na qual solicita as credenciais de login do FMC.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management v

 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 >

9. (Opcional) Selecione o FTD de Destino que deseja usar. Se você optar por migrar para um FTD, selecione o FTD que deseja usar. Se você não quiser usar um FTD, poderá preencher a caixa de seleção 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

10. Selecione as configurações que deseja migrar, as opções são exibidas nas capturas de tela.

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

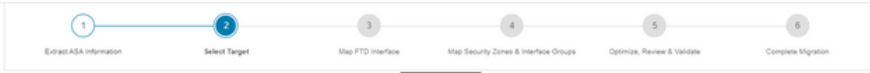
- CSM/ASDM

Proceed

Back

Next

11. Inicie a conversão das configurações do ASA para o 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

12. Quando a conversão for concluída, ele exibirá um painel com o resumo dos objetos a serem migrados (restrito à compatibilidade). Você pode clicar em **Download Report** para receber um resumo das configurações a serem migradas.

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/RAVP/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

Exemplo de relatório de pré-migração, como mostrado na imagem:

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.

I. 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. Mapeie as interfaces do ASA com as interfaces do FTD na Ferramenta de Migração.

Firewall Migration Tool

Map FTD Interface

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

Refresh

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

20 per page 1 to 1 of 1 |< 4 Page 1 of 1 >|

Back Next

14. Crie as zonas de segurança e os grupos de interface para as interfaces no FTD

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

Add SZ & IG Auto-Create

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

Back Next

Zonas de segurança (SZ) e Grupos de interface (IG) são criados automaticamente pela ferramenta, como mostrado na imagem:



Map Security Zones and Interface Groups

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

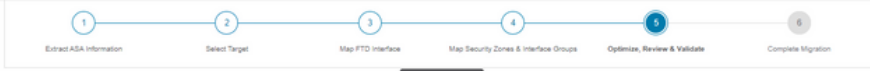
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_ig (A)

Add SZ & IG Auto-Create

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

Back Next

- Revise e valide as configurações a serem migradas na Ferramenta de Migração. Se já tiver concluído a revisão e otimização das configurações, clique em 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

16. Se o status da validação for bem-sucedido, envie as configurações aos dispositivos de destino.

Validation Status

Successfully Validated

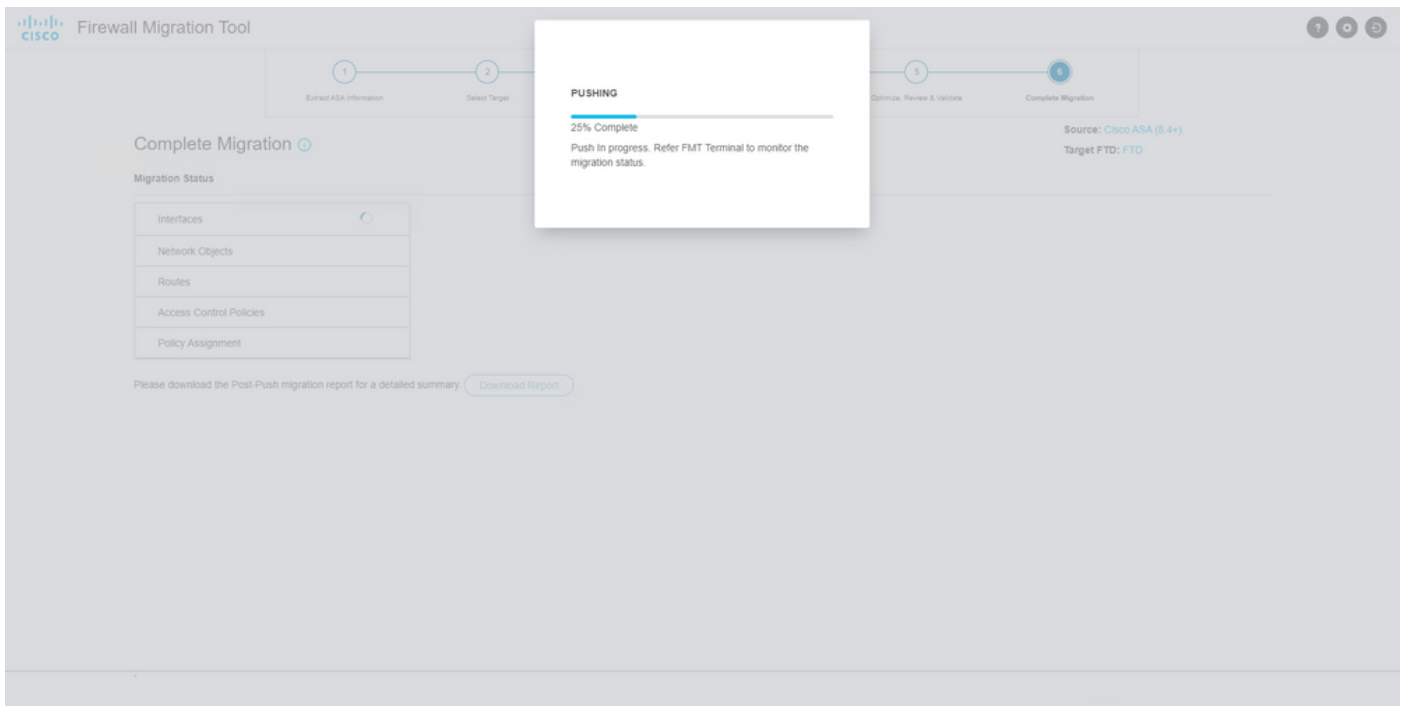
Validation Summary (Pre-push)

0 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RA/VPN/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)

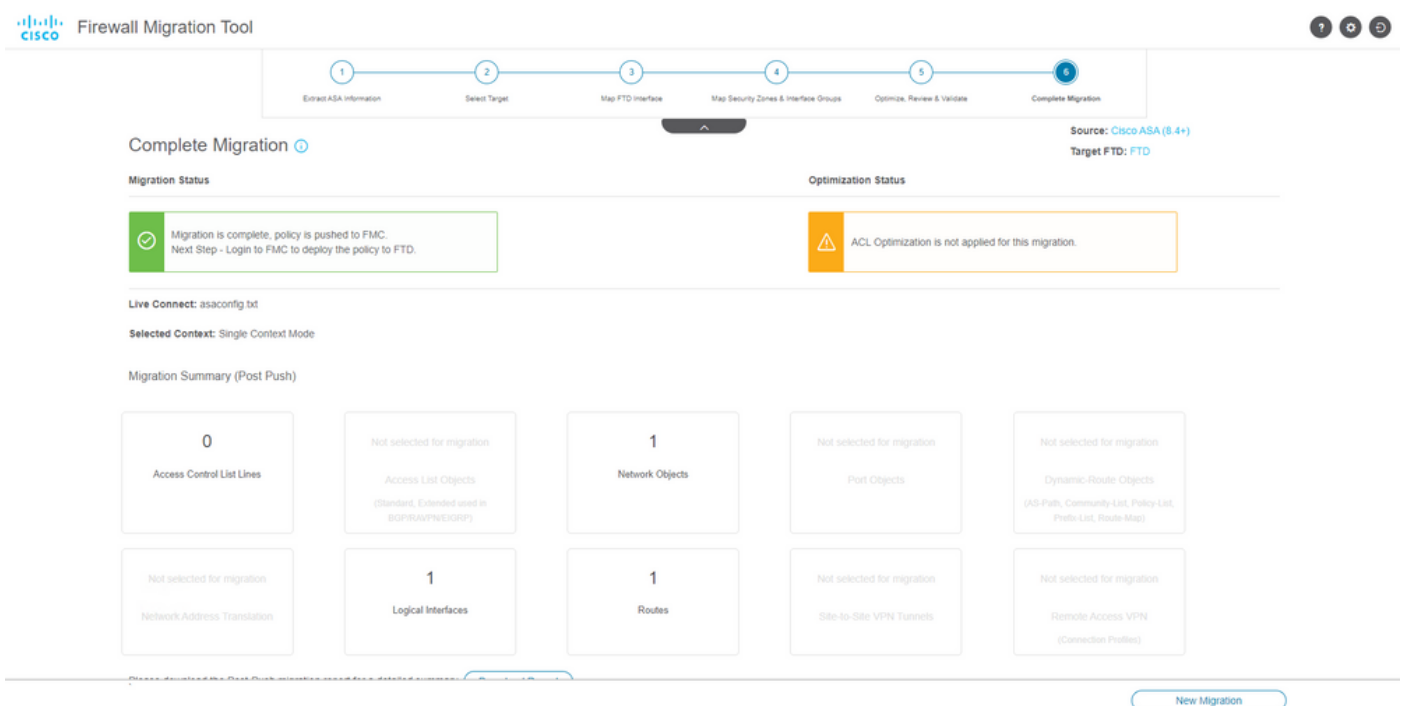
Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

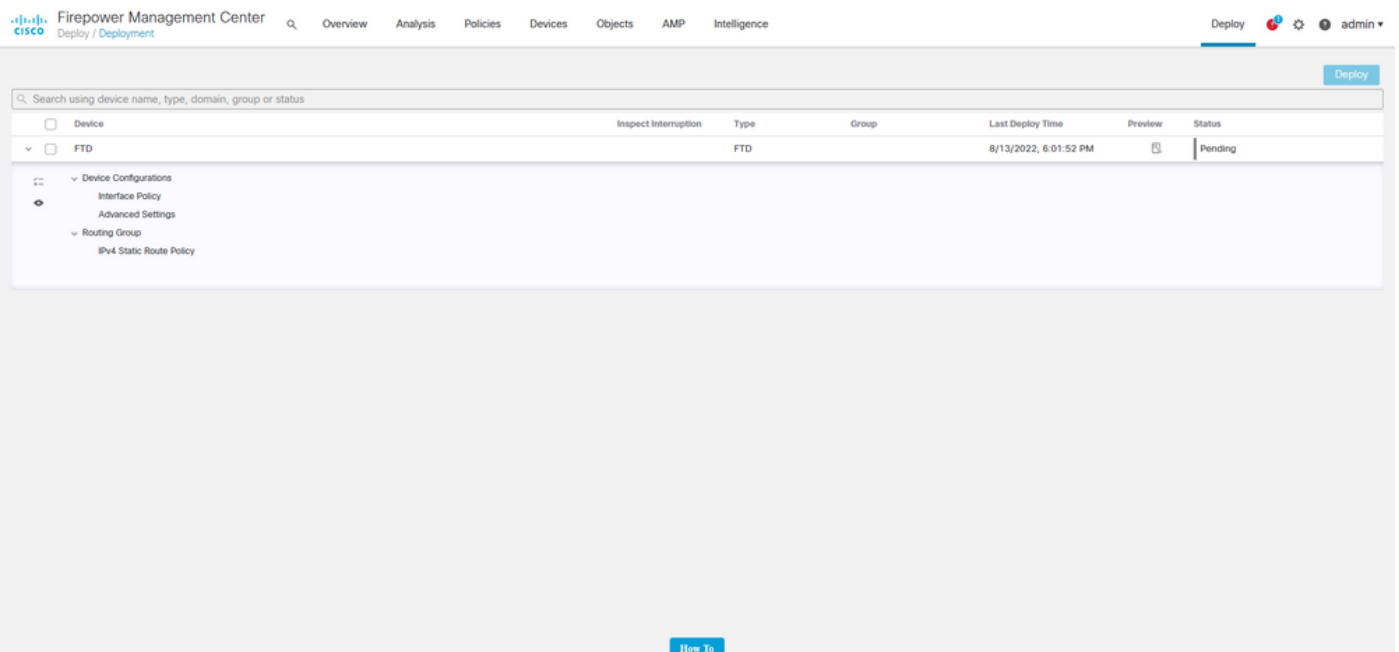
Exemplo de configuração distribuída pela ferramenta de migração, como mostrado na imagem:



Exemplo de uma migração bem-sucedida, como mostrado na imagem:



17. (Opcional) Se você optou por migrar a configuração para um FTD, é necessária uma implantação para enviar a configuração disponível do FMC para o firewall, a fim de implantar a configuração: Faça login na GUI do FMC. Navegue até a página Deploy guia. Selecione a implantação para enviar a configuração para o firewall. Clique em Deploy.



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Verifique os logs no diretório em que o arquivo da ferramenta de migração do Firepower foi colocado, por exemplo:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.