

Migre o ASA para o Firepower Threat Defense (FTD) usando o FMT

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Informações de Apoio](#)

[Obter o arquivo de configuração do ASA](#)

[Exportar o certificado PKI do ASA e importar para o Management Center](#)

[Recuperar pacotes e perfis do AnyConnect](#)

[Configurar](#)

[Configuration Steps:](#)

[Troubleshooting](#)

[Solução de problemas da ferramenta Secure Firewall Migration](#)

Introdução

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

Pré-requisitos

Requisitos

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:

- Mac OS com Firepower Migration Tool (FMT) v7.0.1
- Adaptive Security Appliance (ASA) v9.16(1)
- Centro de gerenciamento seguro de firewall (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

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
 - Gerenciador de dispositivos do Cisco Secure Firewall (7.2+)
 - Ponto de verificação (r75-r77)
 - Ponto de verificação (r80)
 - Fortinet (5.0+)
- Palo Alto Networks (6,1+)

Informações de Apoio

Antes de migrar sua configuração do ASA, execute estas atividades:

Obter o arquivo de configuração do ASA

Para migrar um dispositivo ASA, use `show running-config` para contexto único ou `show tech-support` para modo multicontexto para obter a configuração, salve-a como um arquivo `.cfg` ou `.txt` e transfira-a para o computador com a ferramenta de migração Secure Firewall.

Exportar o certificado PKI do ASA e importar para o Management Center

Use este comando para exportar o certificado PKI através da CLI da configuração do ASA de origem com as chaves para um arquivo PKCS12:

```
ASA(config)#crypto pode exportar <trust-point-name> pkcs12 <passphrase>
```

Em seguida, importe o certificado PKI para um centro de gerenciamento (Object Management PKI Objects). Para obter mais informações, consulte Objetos PKI no [Guia de configuração do Firepower Management Center](#).

Recuperar pacotes e perfis do AnyConnect

Os perfis do AnyConnect são opcionais e podem ser carregados por meio do centro de gerenciamento ou da ferramenta de migração do Secure Firewall.

Use este comando para copiar o pacote necessário do ASA de origem para um servidor FTP ou TFTP:

Copiar <local do arquivo de origem:/nome do arquivo de origem> <destino>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Exemplo de cópia do Pacote Anyconnect.

ASA# copy disk0:/ external-ss0- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Exemplo de cópia do Pacote do Navegador Externo.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Exemplo de cópia do Pacote Hostscan.

ASA#copy disk0:/ dap.xml tftp://1.1.1.1. <----- Exemplo de cópia de Dap.xml

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Exemplo de cópia de Dados.xml

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Exemplo de cópia do perfil do Anyconnect.

Importe os pacotes baixados para o centro de gerenciamento (Object Management > VPN > AnyConnect File).

Os arquivos a-Dap.xml e Data.xml devem ser carregados no centro de gerenciamento a partir da ferramenta de migração do Secure Firewall na seção Revisar e validar > VPN de acesso remoto > Arquivo do AnyConnect.

Os perfis b-AnyConnect podem ser carregados diretamente no centro de gerenciamento ou através da ferramenta de migração do Secure Firewall na seção Revisar e validar > VPN de acesso remoto > Arquivo do AnyConnect.

Configurar

Configuration Steps:

1.Download a mais recente ferramenta de migração Firepower da Cisco Software Central:

Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.0.0

Expand All Collapse All

Latest Release ▼

7.0.1

All Release ▼

7 ▼

7.0.1

7.0.0

Secure Firewall Migration Tool

Release 7.0.0

[My Notifications](#)

Related Links and Documentation

[Open Source](#)

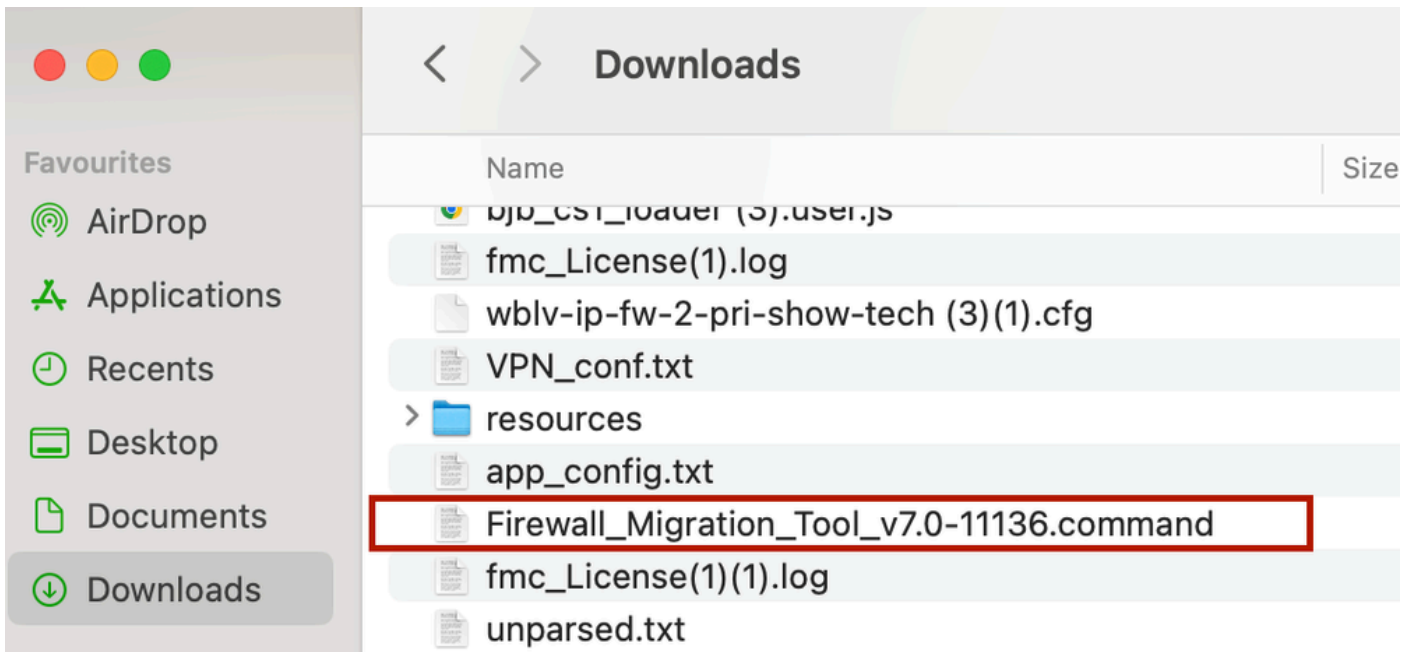
[Release Notes for 7.0.0](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	Icons
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	

Download de software

2. Clique no arquivo baixado anteriormente no computador.



O arquivo

```
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)', 'Fortine
t 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 -
```

Logs de console



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

-
3. Depois de executar o programa, ele abre um navegador que exibe o "Contrato de licença de usuário final".
 1. Marque a caixa de seleção para aceitar termos e condições.
 2. 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 makes no warranty, no 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. Faça login usando uma conta CCO válida e a interface GUI do FMT será exibida no navegador da Web.



Security Cloud Sign On

Email

Continue

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

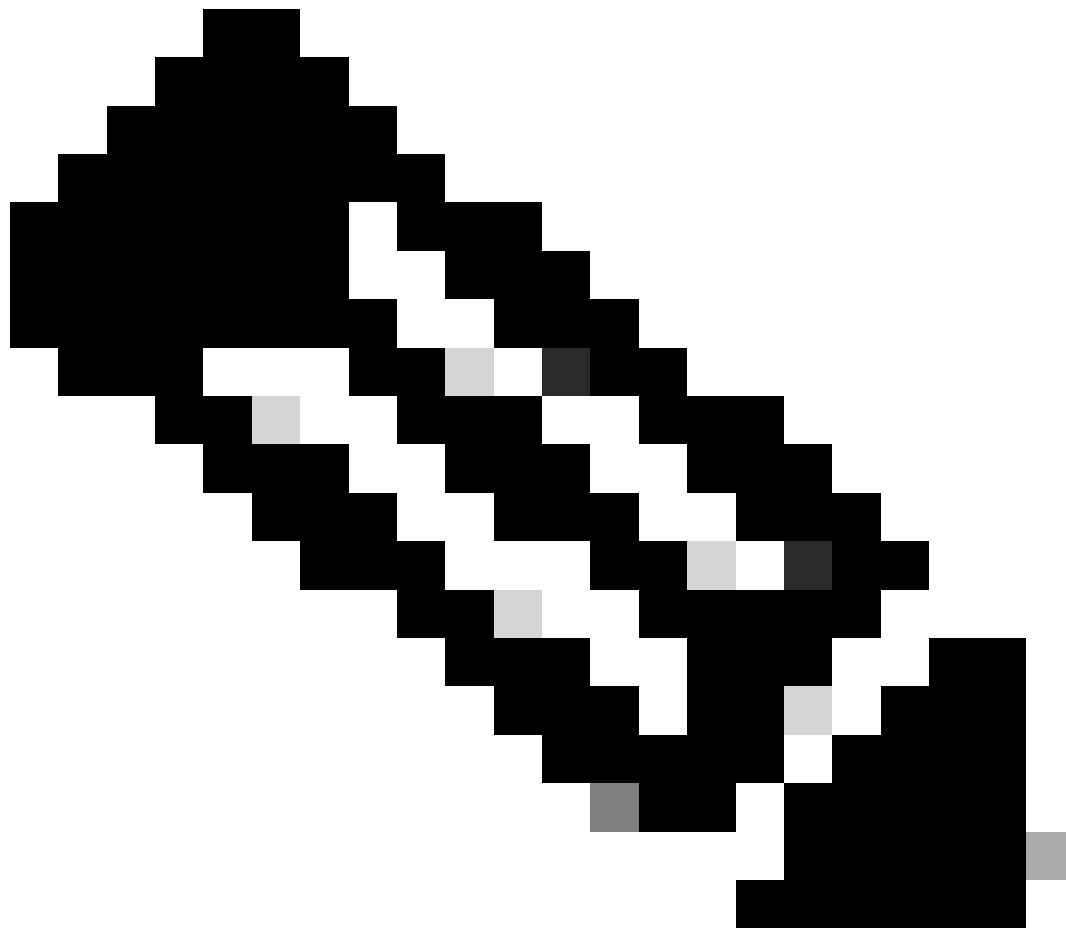
Or

[Other login options](#)

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

Login no FMT

5. Selecione o firewall de origem a ser migrado.



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 >

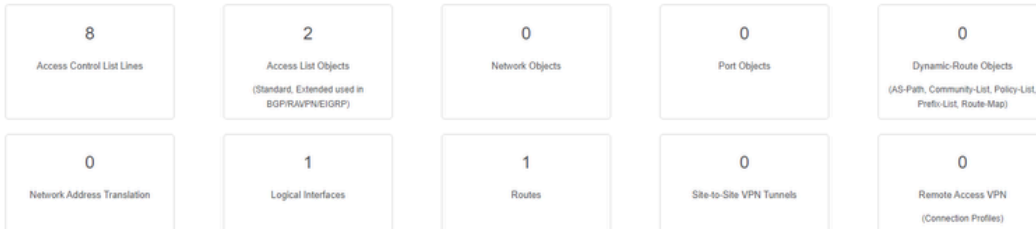
ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



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

<https://cisco.com>

Back

Next

Summary

8. Selecione o FMC de destino a ser usado na migração.

Forneça o IP do FMC. 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 >

Back

Next

IP FMC

9. (Opcional)Selecione o FTD de Destino que deseja usar.

1. Se você optar por migrar para um FTD, selecione o FTD que deseja usar.

2. 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
 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

FTD de destino

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 >

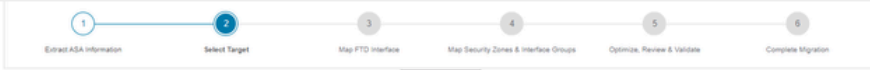
<p>Device Configuration</p> <p><input checked="" type="checkbox"/> Interfaces</p> <p><input checked="" type="checkbox"/> Routes</p> <p> <input checked="" type="checkbox"/> Static</p> <p> <input type="checkbox"/> BGP</p> <p> <input type="checkbox"/> EIGRP</p> <p><input type="checkbox"/> Site-to-Site VPN Tunnels (no data)</p> <p> <input type="checkbox"/> Policy Based (Crypto Map)</p> <p> <input type="checkbox"/> Route Based (VTI)</p>	<p>Shared Configuration</p> <p><input checked="" type="checkbox"/> Access Control</p> <p> <input checked="" type="checkbox"/> Populate destination security zones</p> <p> ⚠️ Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.</p> <p> <input checked="" type="checkbox"/> Migrate tunnelled rules as Prefilter</p> <p> <input type="checkbox"/> NAT (no data)</p> <p> <input checked="" type="checkbox"/> Network Objects (no data)</p> <p> <input type="checkbox"/> Port Objects (no data)</p> <p> <input type="checkbox"/> Access List Objects(Standard, Extended)</p> <p> <input type="checkbox"/> Time based Objects (no data)</p> <p> <input type="checkbox"/> Remote Access VPN</p> <p> ⚠️ Remote Access VPN migration is supported on FMC/FTD 7.2 and above.</p>	<p>Optimization</p> <p><input checked="" type="checkbox"/> Migrate Only Referenced Objects</p> <p><input checked="" type="checkbox"/> Object Group Search</p> <p>Inline Grouping</p> <p><input checked="" type="checkbox"/> CSM/ASDM</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Proceed

Back Next

Configurações

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

Iniciar conversão

12. Quando a conversão for concluída, ele exibirá um painel com o resumo dos objetos a serem migrados (restrito à compatibilidade).

1. Você também 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/VEIGRP)	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

Download do relatório

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.

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

Relatório de pré-migração

13. Mapeie as interfaces ASA com as interfaces FTD na Ferramenta de Migração.

The screenshot shows the 'Map FTD Interface' screen in the Cisco Firewall Migration Tool. At the top left is the Cisco logo and 'Firewall Migration Tool'. On the right, it says 'Source: Cisco ASA (8.4+)' and 'Target FTD: FTD'. The main area is a table with two columns: 'ASA Interface Name' and 'FTD Interface Name'. The first row shows 'Management0/0' under ASA and 'GigabitEthernet0/0' under FTD. There is a 'Refresh' button above the table. At the bottom, there is a pagination control showing '20 per page', '1 to 1 of 1', and 'Page 1 of 1'. At the very bottom right, there are 'Back' and 'Next' buttons.

Mapear interfaces

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

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

Back Next

Zonas de segurança e grupos de interface

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_lg (A)

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

Back Next

ferramenta Criação Automática

15. Revise e valide as configurações a serem migradas na Ferramenta de Migração.

1. Se você já tiver concluído a revisão e a 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

Revisar e validar

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

Validation Status

Successfully Validated

Validation Summary (Pre-push)

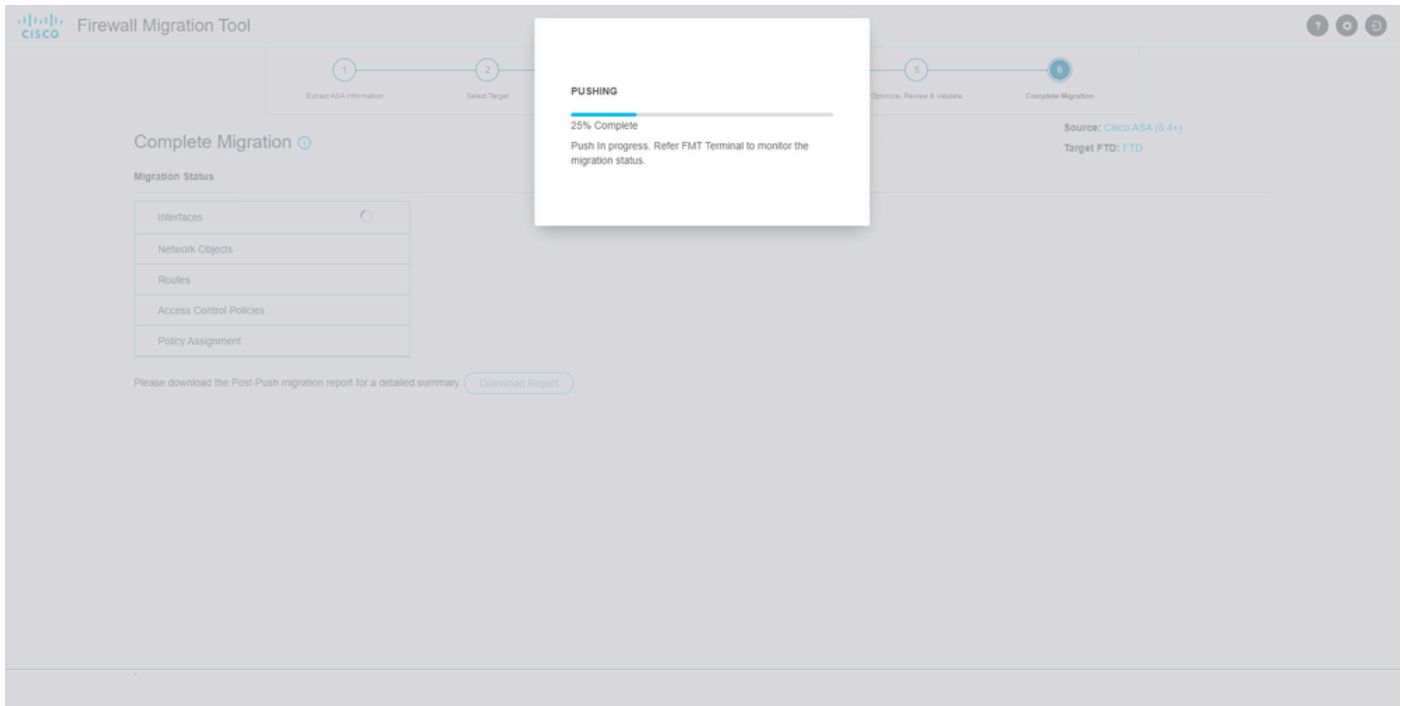
0	Not selected for migration	1	Not selected for migration	Not selected for migration
Access Control List Lines	Access List Objects (Standard, Extended used in BGP/HA/VPN/EIGRP)	Network Objects	Port Objects	Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected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

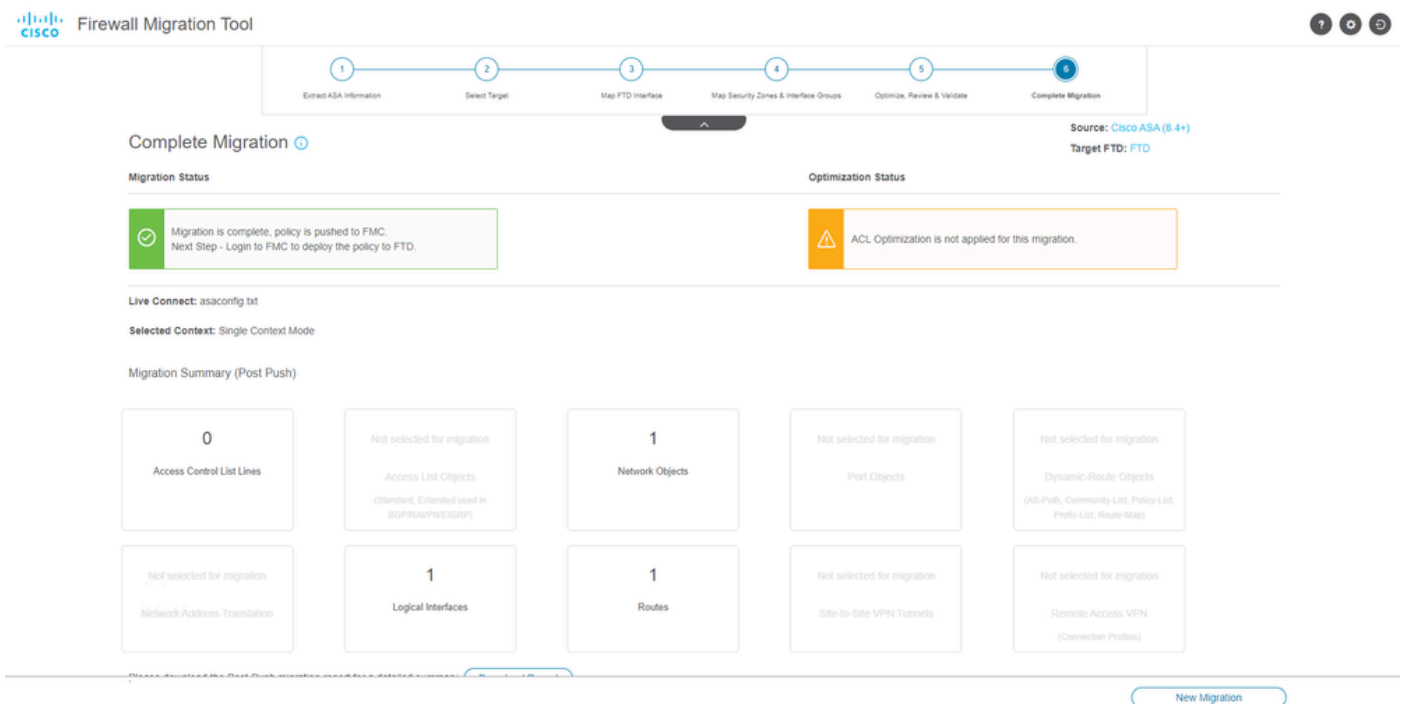
Validação

Exemplo de configuração enviado por meio da ferramenta de migração, como mostrado na imagem:



Enviar por push

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



Migração bem-sucedida

(Opcional) Se você optou por migrar a configuração para um FTD, será necessária uma implantação para enviar a configuração disponível do FMC para o firewall.

Para implantar a configuração:

1. Faça login na GUI do FMC.
2. Navegue até aDeployguia.

3. Selecione a implantação para enviar a configuração para o firewall.
4. Clique em `. Deploy`

Troubleshooting

Solução de problemas da ferramenta Secure Firewall Migration

- Falhas comuns de migração:
 - Caracteres desconhecidos ou inválidos no arquivo de configuração ASA.
 - Elementos de configuração ausentes ou incompletos.
 - Problemas de conectividade de rede ou latência.
- Problemas durante o carregamento do arquivo de configuração do ASA ou o envio da configuração para o centro de gerenciamento.
- Os problemas comuns incluem:
 - Na tela "Migração completa", clique no botão Suporte.
 - Selecione Support Bundle e escolha os arquivos de configuração para download.
 - Os arquivos de log e de banco de dados são selecionados por padrão.
 - Clique em Download para obter um arquivo .zip.
 - Extraia o .zip para exibir logs, BD e arquivos de configuração.
 - Clique em Envie um e-mail para enviar os detalhes da falha para a equipe técnica.
 - Anexe o pacote de suporte em seu e-mail.
 - Clique em Visitar a página TAC para criar um caso de TAC da Cisco para obter assistência.
- A ferramenta permite que você faça download de um pacote de suporte para arquivos de log, banco de dados e arquivos de configuração.
- Etapas para fazer download:
- Para obter mais suporte:

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.