Configurar o FTD do arquivo de configuração do ASA com a ferramenta de migração Firepower

Contents

Introduction

Este documento descreve um exemplo de migração do Adaptive Security Appliance (ASA) para Firepower Threat Defense (FTD) no FPR4145.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do ASA
- Conhecimento do Firepower Management Center (FMC) e do FTD

Componentes Utilizados

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

- ASA versão 9.12(2)
- FTD versão 6.7.0
- FMC versão 6.7.0
- Firepower Migration Tool versão 2.5.0

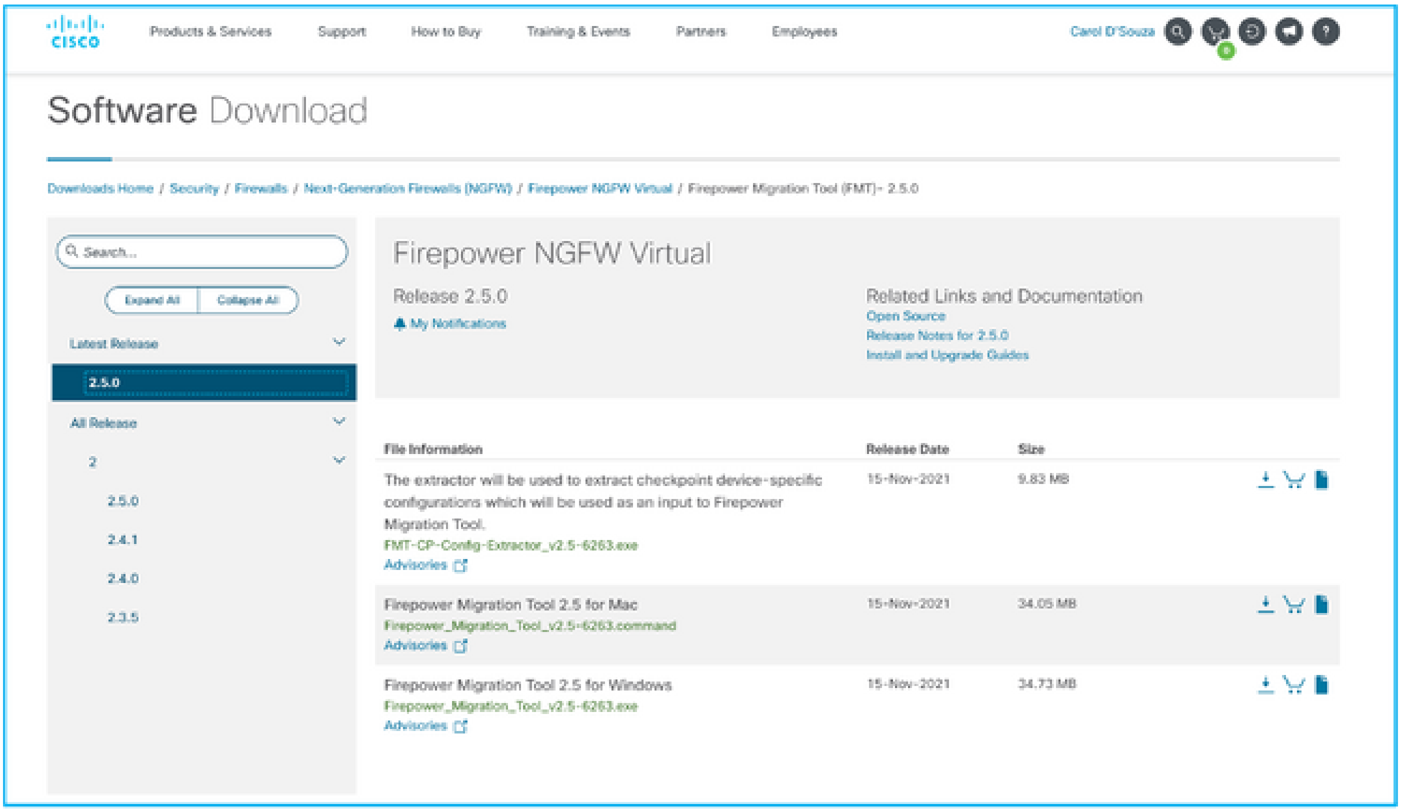
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Exporte o arquivo de configuração do ASA no formato **.cfg** ou **.txt**. O FMC deve ser implantado com o FTD registrado nele.

Configurar

1. Baixe a Firepower Migration Tool de software.cisco.com, como mostrado na imagem.



Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Firepower NGFW Virtual / Firepower Migration Tool (FMT)- 2.5.0

Firepower NGFW Virtual

Release 2.5.0

My Notifications

Related Links and Documentation
Open Source
Release Notes for 2.5.0
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_v2.5-6263.exe Advisories	15-Nov-2021	9.83 MB
Firepower Migration Tool 2.5 for Mac Firepower_Migration_Tool_v2.5-6263.command Advisories	15-Nov-2021	34.05 MB
Firepower Migration Tool 2.5 for Windows Firepower_Migration_Tool_v2.5-6263.exe Advisories	15-Nov-2021	34.73 MB

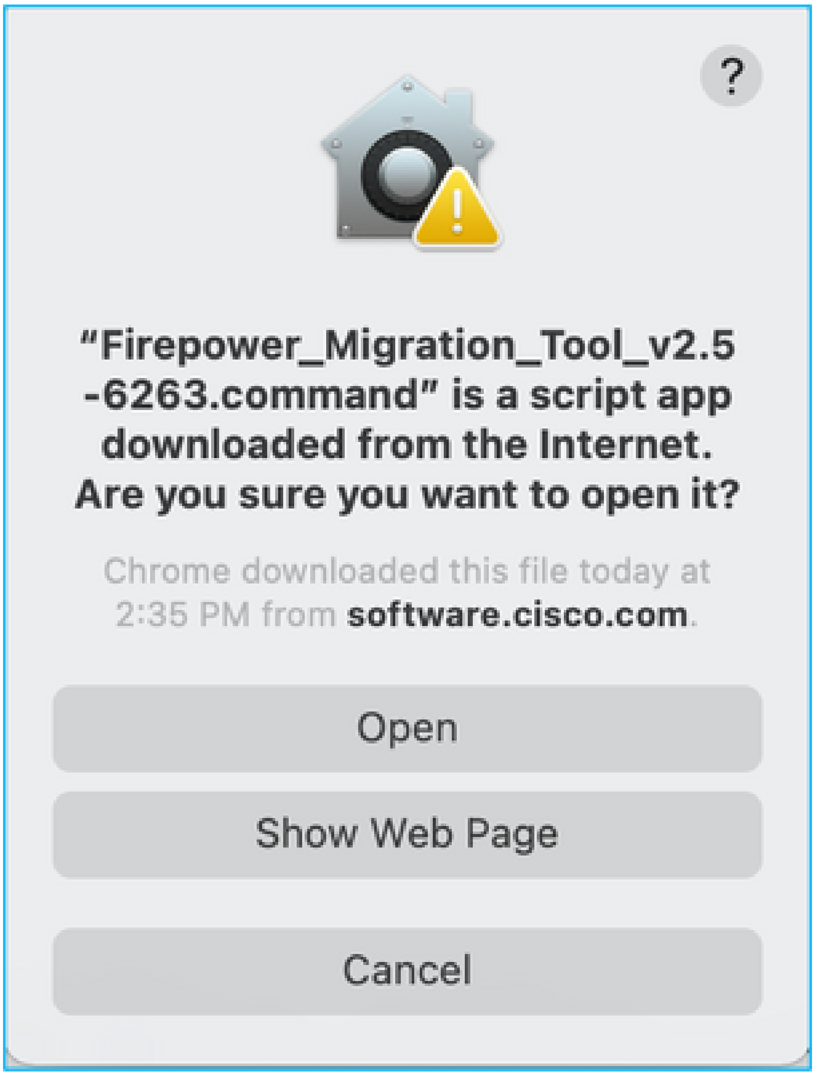
2. Revise e verifique os requisitos na seção Diretrizes e Limitações da ferramenta de migração Firepower.

3. Se você estiver planejando migrar um arquivo de configuração grande, configure as configurações de espera para que o sistema não fique em espera durante um envio de migração.

3.1. No Windows, navegue até Opções de energia no Painel de controle. Clique em **Alterar configurações do plano** próximo ao seu plano de energia atual. Alteração **Coloque o computador para dormir** para **Nunca**. Clique em **Salvar alterações**.

3.2. Para MAC, navegue até **System Preferences > Energy Saver**. Marque a caixa ao lado para evitar que o computador fique dormindo automaticamente quando a tela estiver desligada e arraste a tecla **Turn Off (Desligar exibição)** depois do controle deslizante para Nunca.

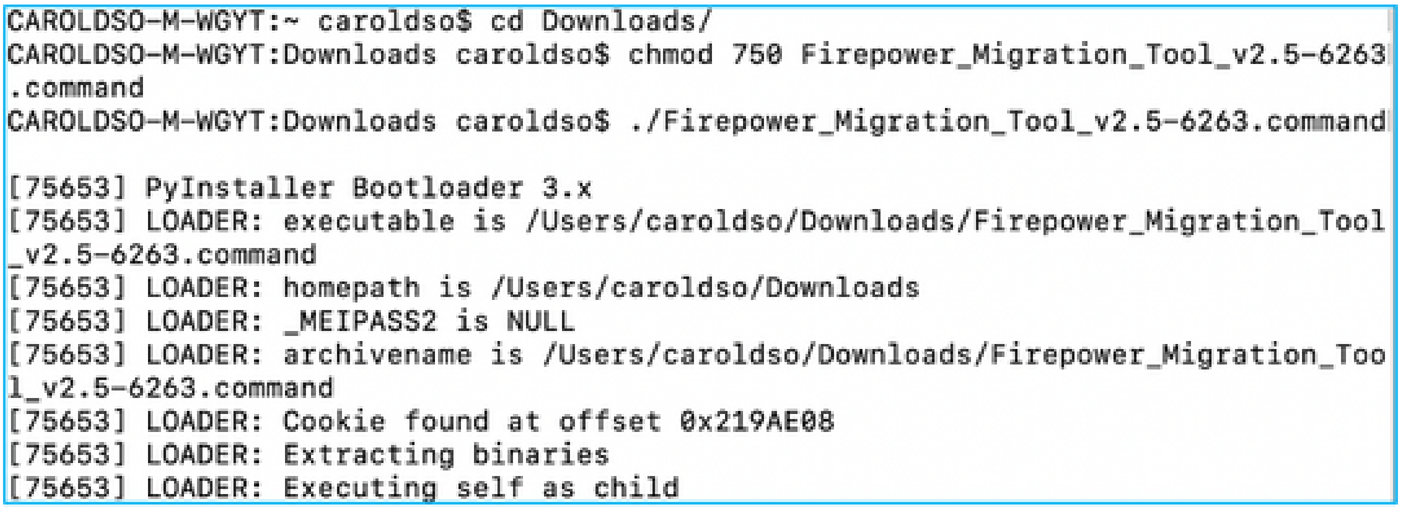
> **Note**: Esse aviso abre a caixa de diálogo quando os usuários MAC tentam abrir o arquivo baixado. Ignore isso e siga a Etapa 4 A.



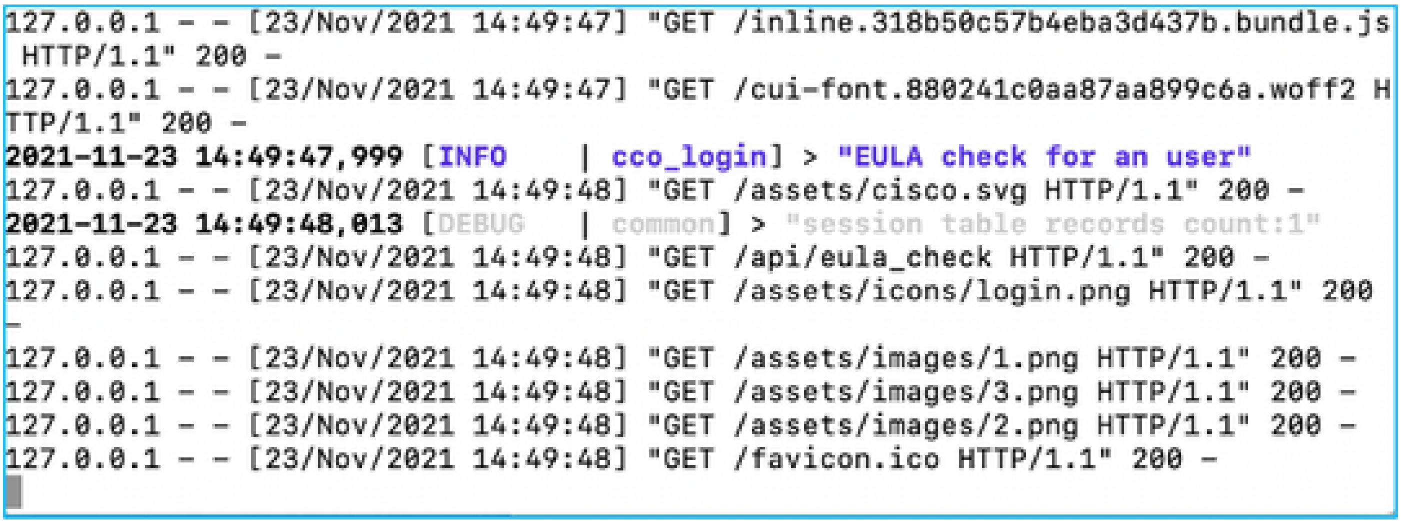
"Firepower_Migration_Tool_v2.5-6263.command" is a script app downloaded from the Internet. Are you sure you want to open it?

Chrome downloaded this file today at 2:35 PM from software.cisco.com.

4. A. Para MAC - Use o terminal e execute esses comandos.



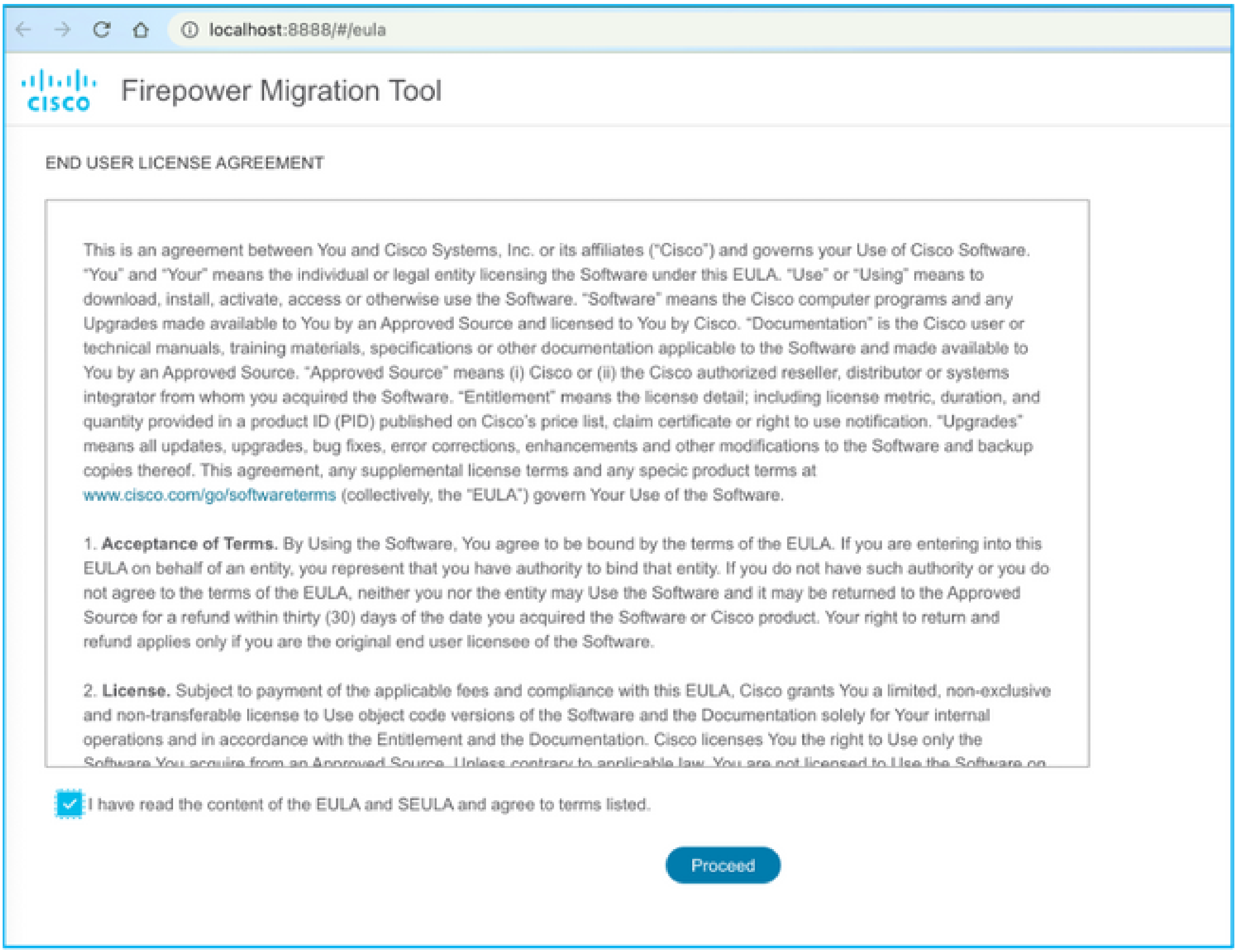
```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263
.command
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command

[75653] PyInstaller Bootloader 3.x
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool
_v2.5-6263.command
[75653] LOADER: homepath is /Users/caroldso/Downloads
[75653] LOADER: _MEIPASS2 is NULL
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too
l_v2.5-6263.command
[75653] LOADER: Cookie found at offset 0x219AE08
[75653] LOADER: Extracting binaries
[75653] LOADER: Executing self as child
```



```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js
 HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 H
TTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO    | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG   | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200
-
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4. B. No Windows - clique duas vezes na Firepower Migration Tool para iniciá-la em um navegador Google Chrome.

5. Aceite a licença conforme mostrado na imagem.



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.

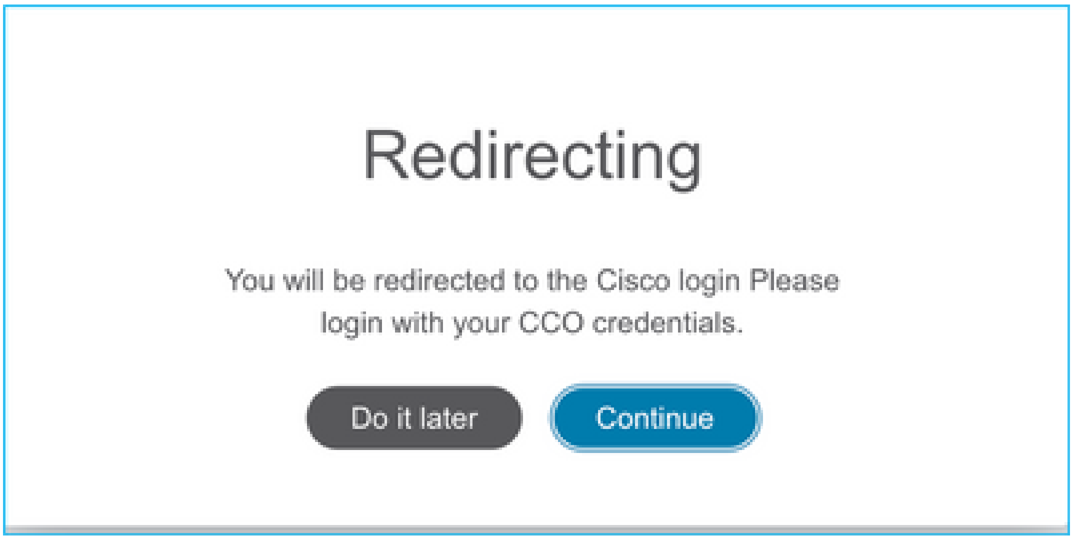
2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement 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 Software on

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

6. Na página de login da Firepower Migration Tool, clique no link de login com CCO para fazer login em sua conta Cisco.com com suas credenciais de login único.

Note: Se você não tiver uma conta do Cisco.com, crie-a na página de login do Cisco.com.

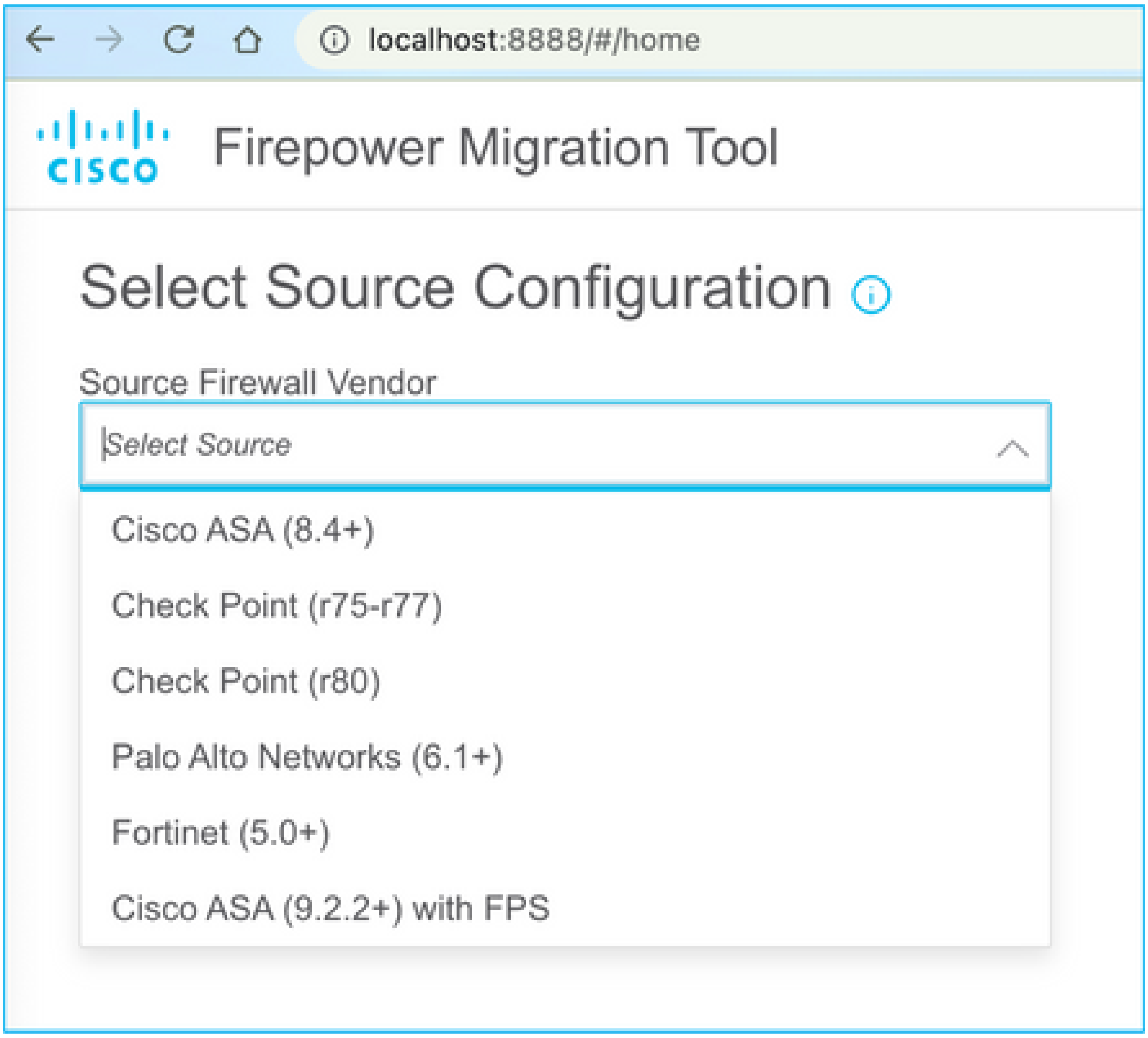
Faça login com as seguintes credenciais padrão: Nome de usuário—senha admin—Admin123.



Redirecting

You will be redirected to the Cisco login Please login with your CCO credentials.

7. Selecione a configuração de origem. Nesse cenário, é o Cisco ASA (8.4+).



localhost:8888/#/home

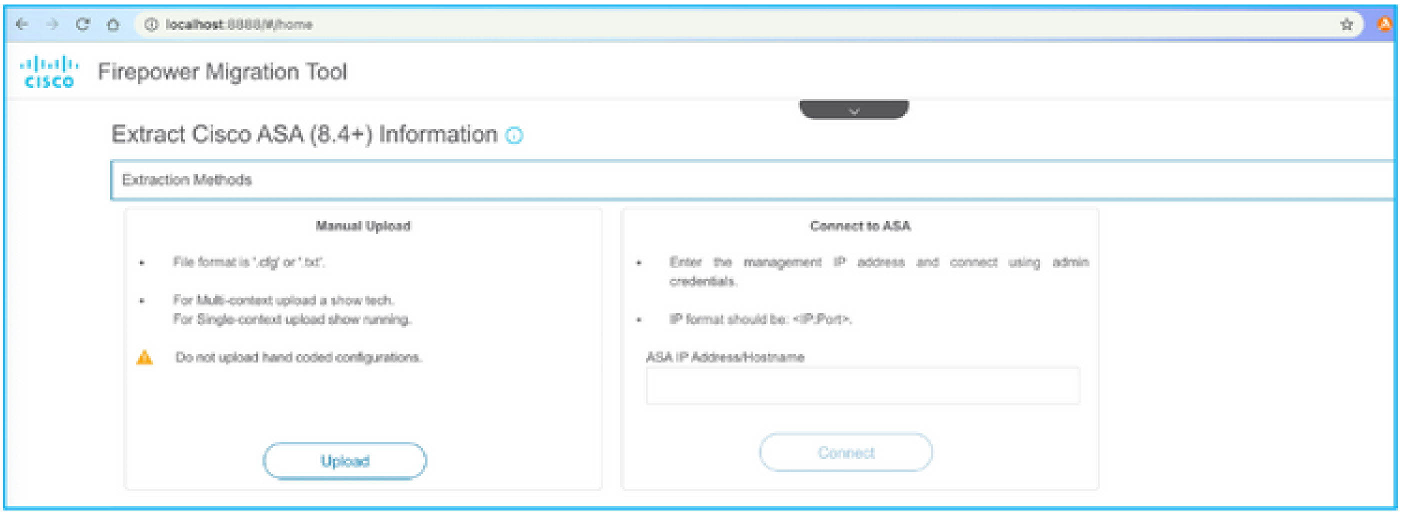
Firepower Migration Tool

Select Source Configuration

Source Firewall Vendor

Select Source

8. Selecione Manual Upload se você não tiver conectividade com o ASA. Caso contrário, você pode recuperar a configuração atual do ASA e inserir o IP de gerenciamento e os detalhes de login. Em nosso cenário, foi feito um upload manual.



Extract Cisco ASA (8.4+) Information

Extraction Methods

Manual Upload

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

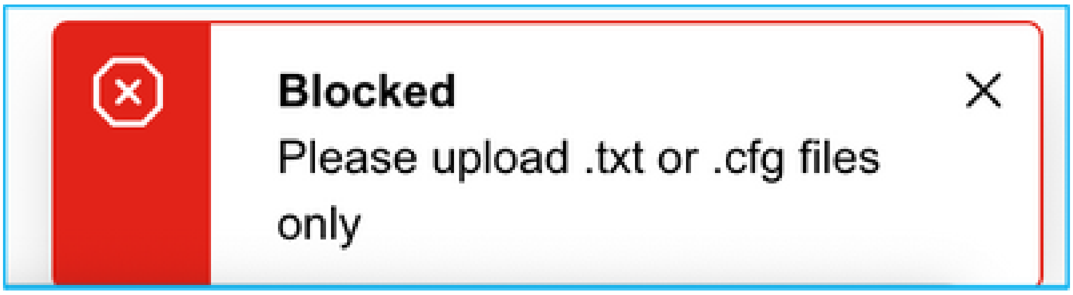
⚠ Do not upload hand coded configurations.

Connect to ASA

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

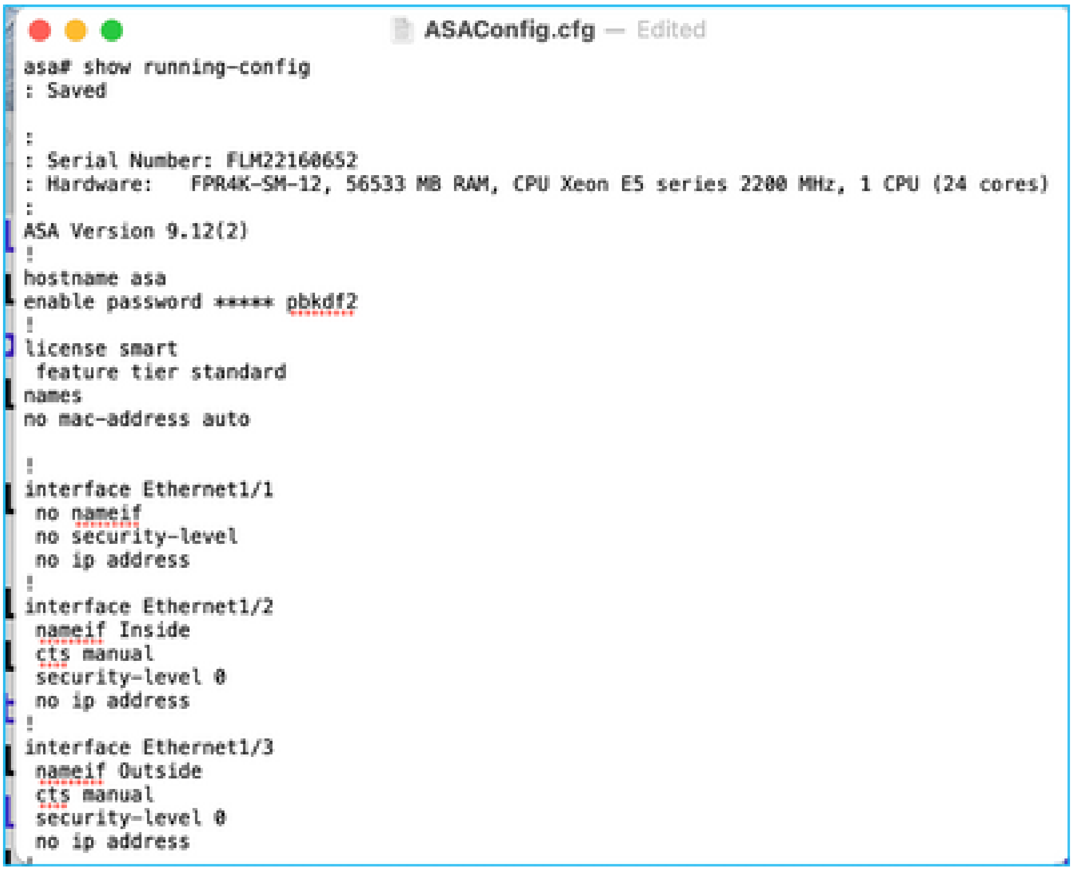
ASA IP Address/Hostname

Note: Esse erro será exibido se o arquivo não for suportado. Certifique-se de alterar o formato para texto simples. (Erro apesar da extensão .cfg).



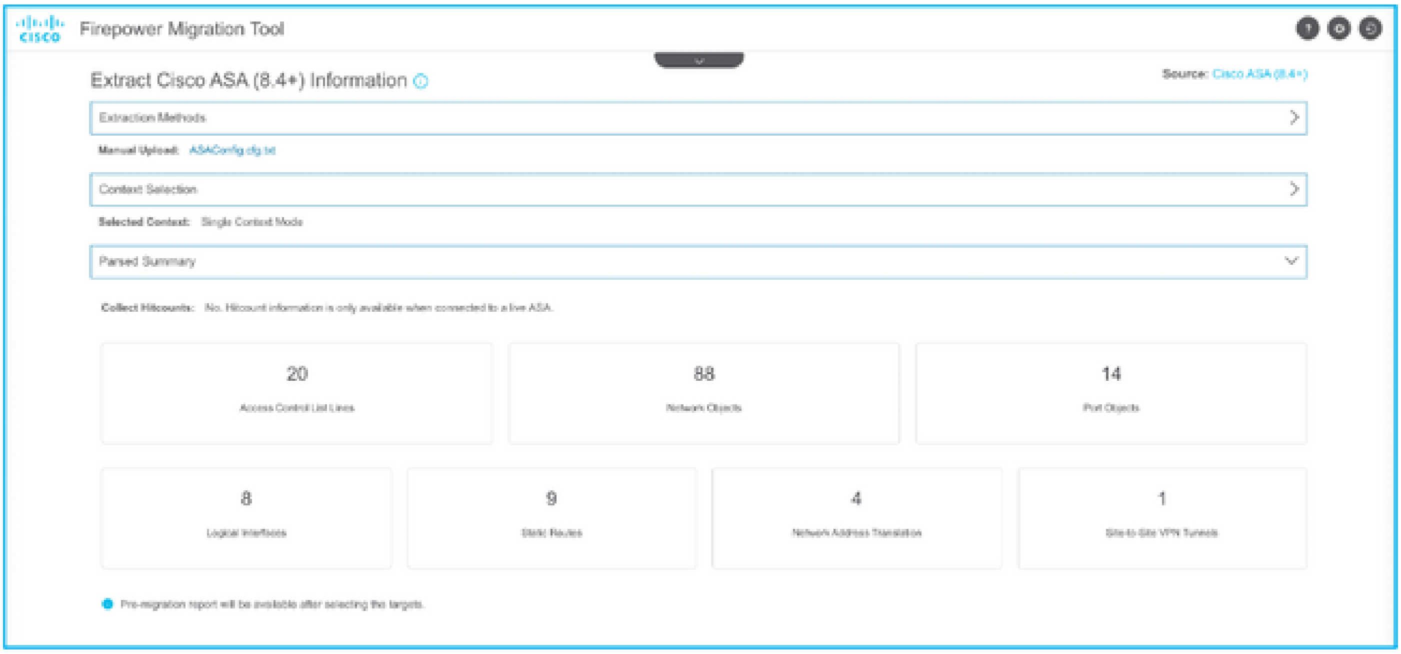
Blocked

Please upload .txt or .cfg files only



```
asa# show running-config
: Saved

:
: Serial Number: FLM22160652
: Hardware:   FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
!
hostname asa
enable password ***** pbkdf2
!
license smart
 feature tier standard
names
no mac-address auto

!
interface Ethernet1/1
 no nameif
 no security-level
 no ip address
!
interface Ethernet1/2
 nameif Inside
 cts manual
 security-level 0
 no ip address
!
interface Ethernet1/3
 nameif Outside
 cts manual
 security-level 0
 no ip address
```

9. Após o upload do arquivo, os elementos serão analisados fornecendo um resumo como mostrado na imagem:



Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods

Manual Upload: ASAConfig.cfg.txt

Context Selection

Selected Context: Single Context Mode

Parsed Summary

Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

20 Access Control List Lines

88 Network Objects

14 Port Objects

8 Logical Interfaces

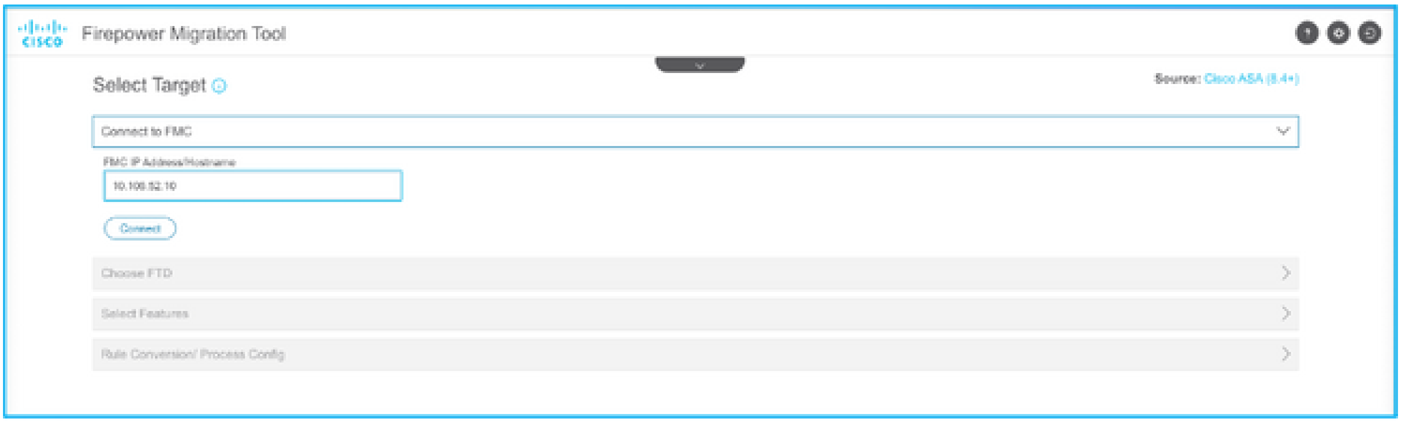
9 Static Routes

4 Network Address Translation

1 Site-to-Site VPN Tunnels

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

10. Insira o IP do FMC e as credenciais de login para as quais a configuração do ASA será migrada. Certifique-se de que o IP do FMC esteja acessível a partir da sua estação de trabalho.



Firepower Migration Tool

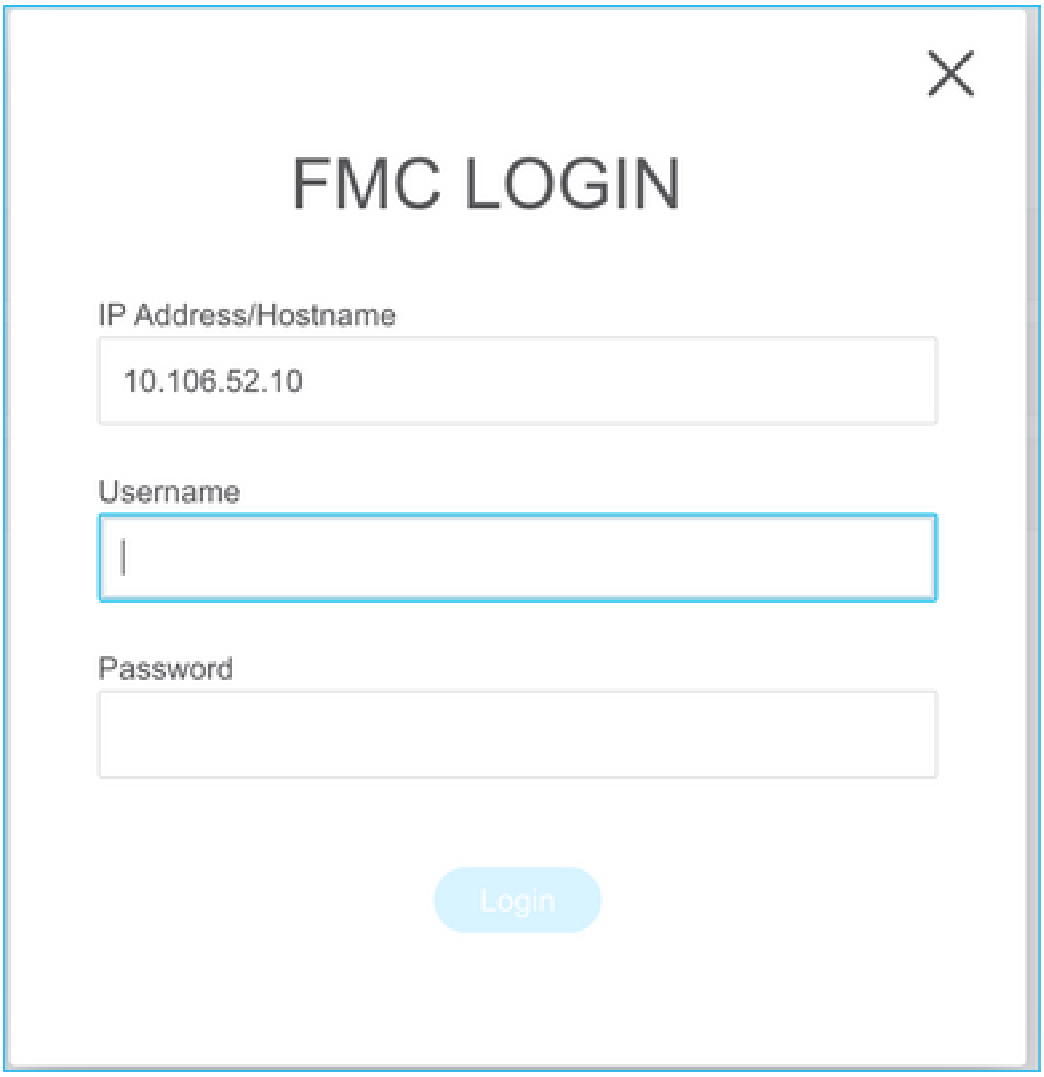
Select Target

Source: Cisco ASA (8.4+)

Connect to FMC

FMC IP Address/Hostname

10.106.52.10



FMC LOGIN

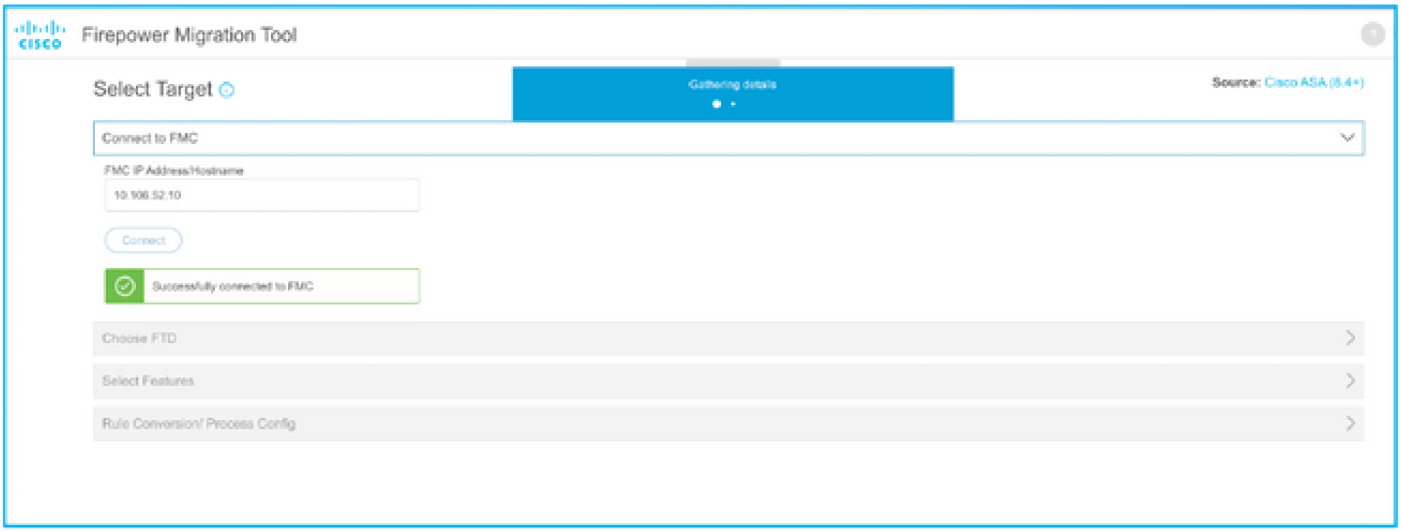
IP Address/Hostname

10.106.52.10

Username

Password

11. Quando o FMC estiver conectado, os FTDs gerenciados abaixo dele serão exibidos.



Firepower Migration Tool

Select Target

Gathering details

Source: Cisco ASA (8.4+)

Connect to FMC

FMC IP Address/Hostname: 10.106.52.10

Connect

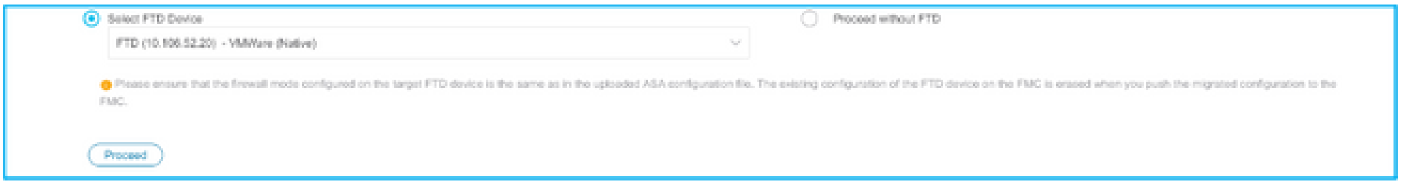
Successfully connected to FMC

Choose FTD

Select Features

Rule Conversion/ Process Config

12. Escolha o FTD para o qual deseja executar a migração da configuração do ASA.



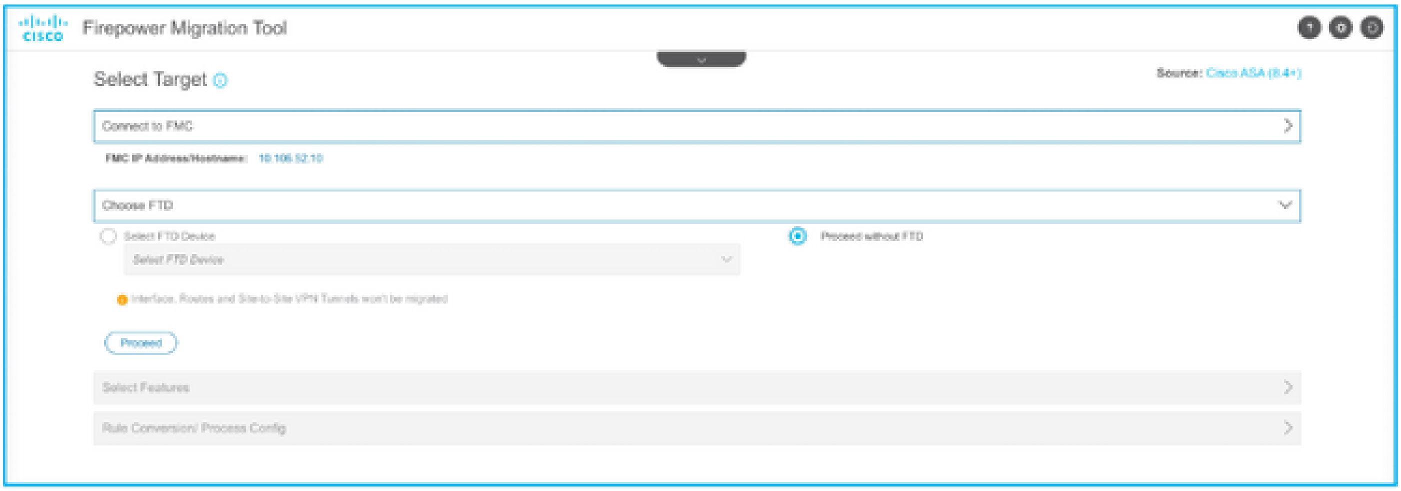
● Select FTD Device　　○ Proceed without FTD

FTD (10.106.52.20) - 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

Note: Recomenda-se selecionar o dispositivo FTD, caso contrário, as interfaces, rotas e a configuração de VPN site a site terão que ser feitas manualmente.



Firepower Migration Tool

Select Target

Source: Cisco ASA (8.4+)

Connect to FMC

FMC IP Address/Hostname: 10.106.52.10

Choose FTD

○ Select FTD Device　　● Proceed without FTD

Select FTD Device

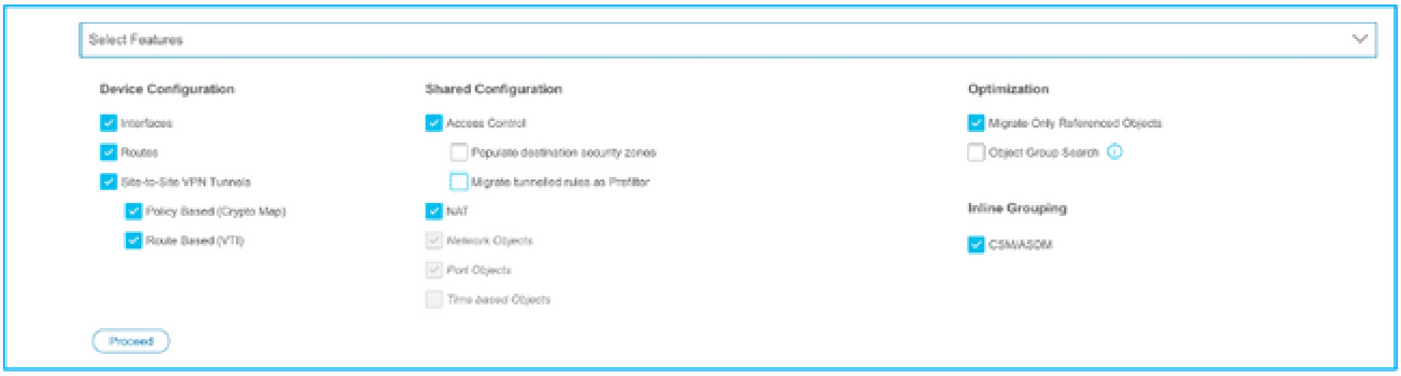
Interface, Routes and Site-to-Site VPN Tunnels won't be migrated

Proceed

Select Features

Rule Conversion/ Process Config

13. Selecione os recursos que devem ser migrados conforme mostrado na imagem.



Select Features

Device Configuration

☑ Interfaces
☑ Routes
☑ Site-to-Site VPN Tunnels
☑ Policy Based (Crypto Map)
☑ Route Based (VTI)

Shared Configuration

☑ Access Control
□ Populate destination security zones
□ Migrate tunnelled rules as Prefilter
☑ NAT
☑ Network Objects
☑ Port Objects
□ Time based Objects

Optimization

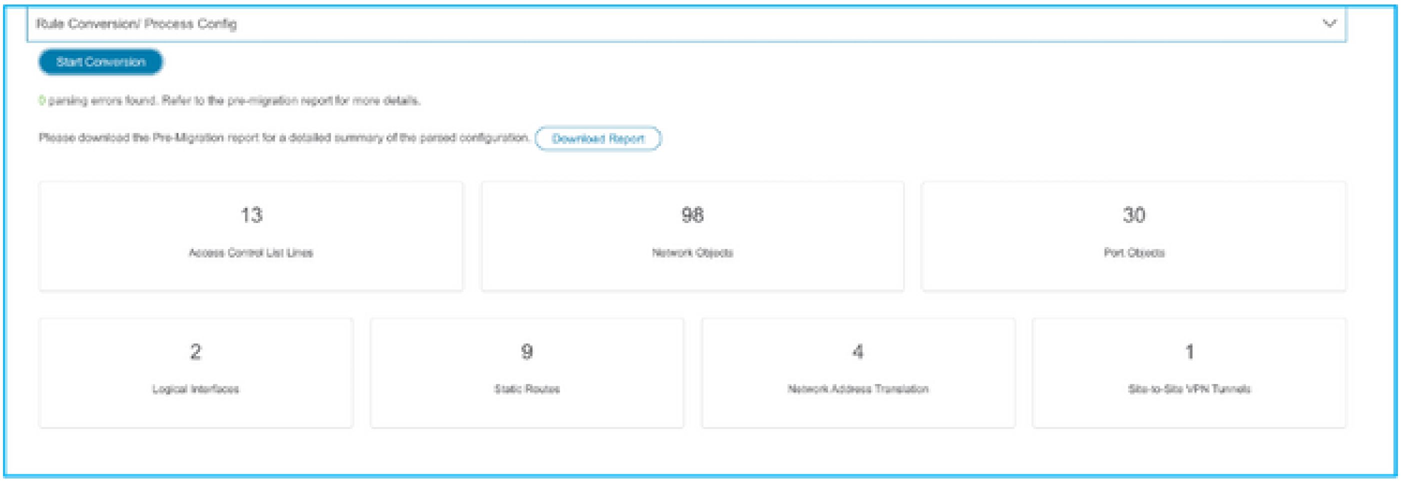
☑ Migrate Only Referenced Objects
□ Object Group Search

Inline Grouping

☑ CSM/ASDM

Proceed

14. Selecione **Start Conversion** para iniciar a pré-migração que preencherá os elementos referentes à configuração do FTD.



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.

13 Access Control List Lines

98 Network Objects

30 Port Objects

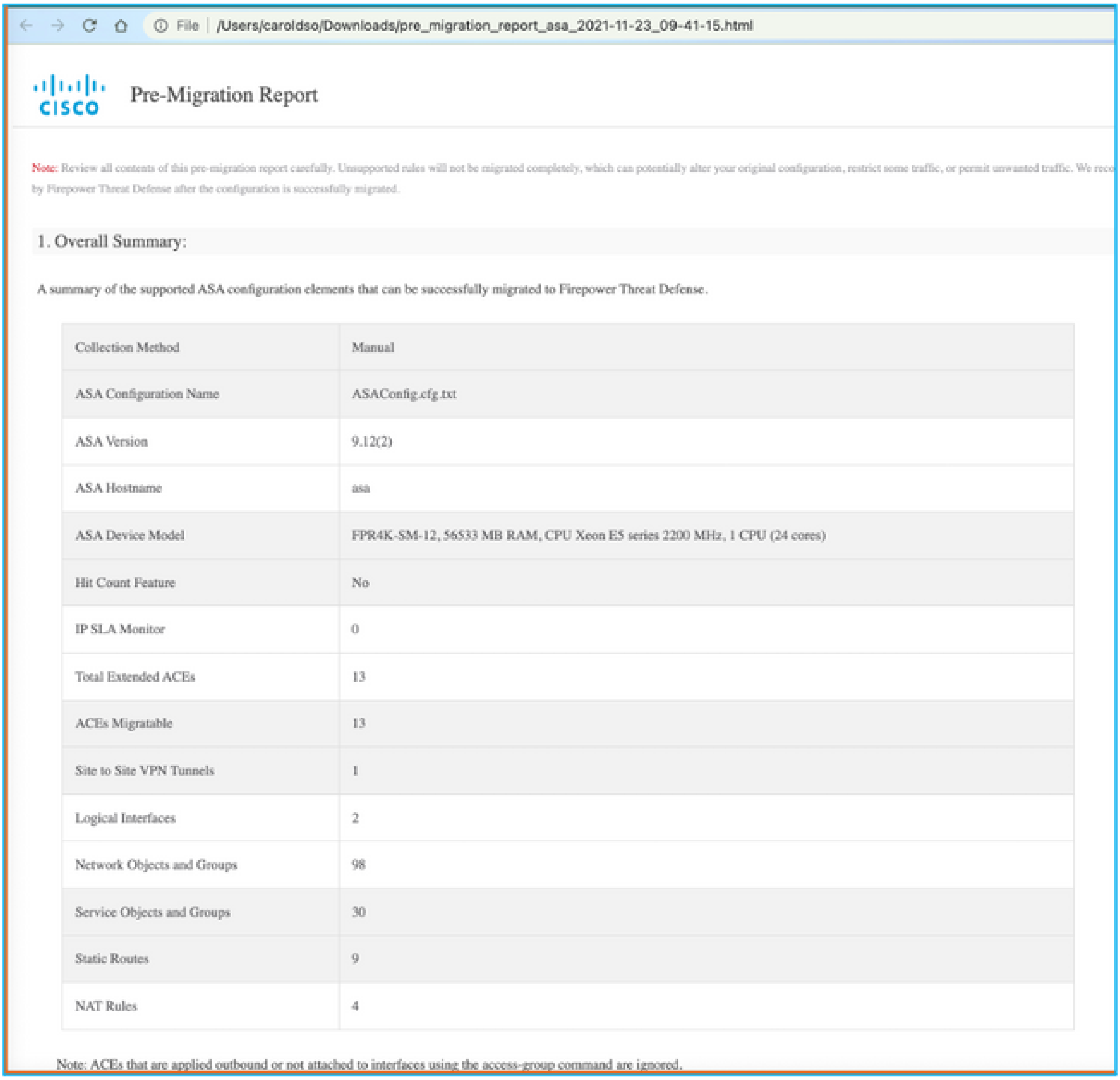
2 Logical Interfaces

9 Static Routes

4 Network Address Translation

1 Site-to-Site VPN Tunnels

15. Clique em **Download Report** visto anteriormente para exibir o Pre-Migration Report, como mostrado na imagem.



/Users/caroldso/Downloads/pre_migration_report_asa_2021-11-23_09-41-15.html

Pre-Migration Report

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 reco
by Firepower Threat Defense after the configuration is successfully migrated.

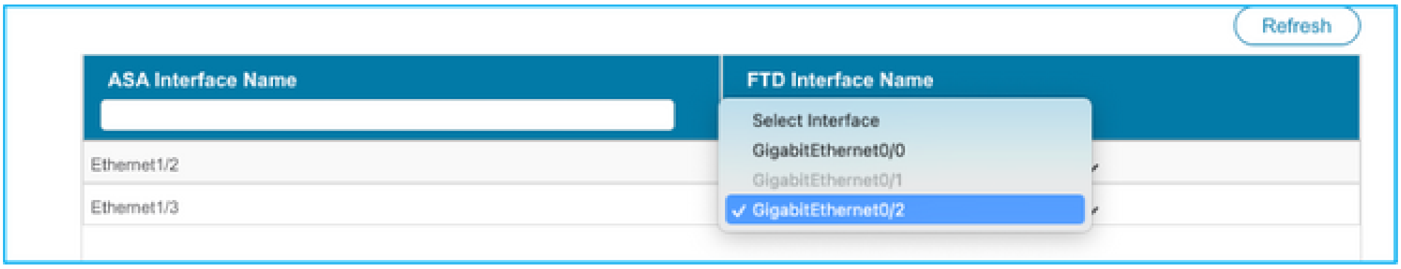
1. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

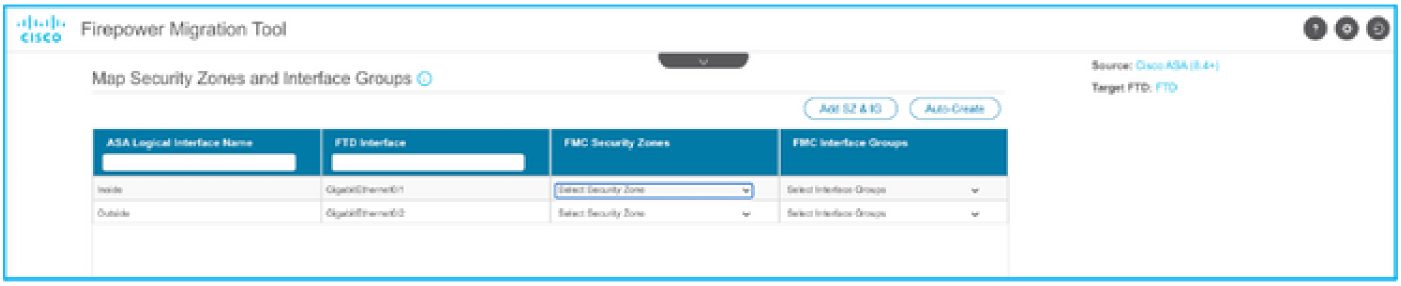
Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

16. Mapeie as interfaces ASA com as interfaces FTD conforme necessário, conforme mostrado na imagem.



ASA Interface Name	FTD Interface Name
Ethernet1/2	
Ethernet1/3	GigabitEthernet0/2

17. Atribua zonas de segurança e grupos de interface às interfaces FTD.



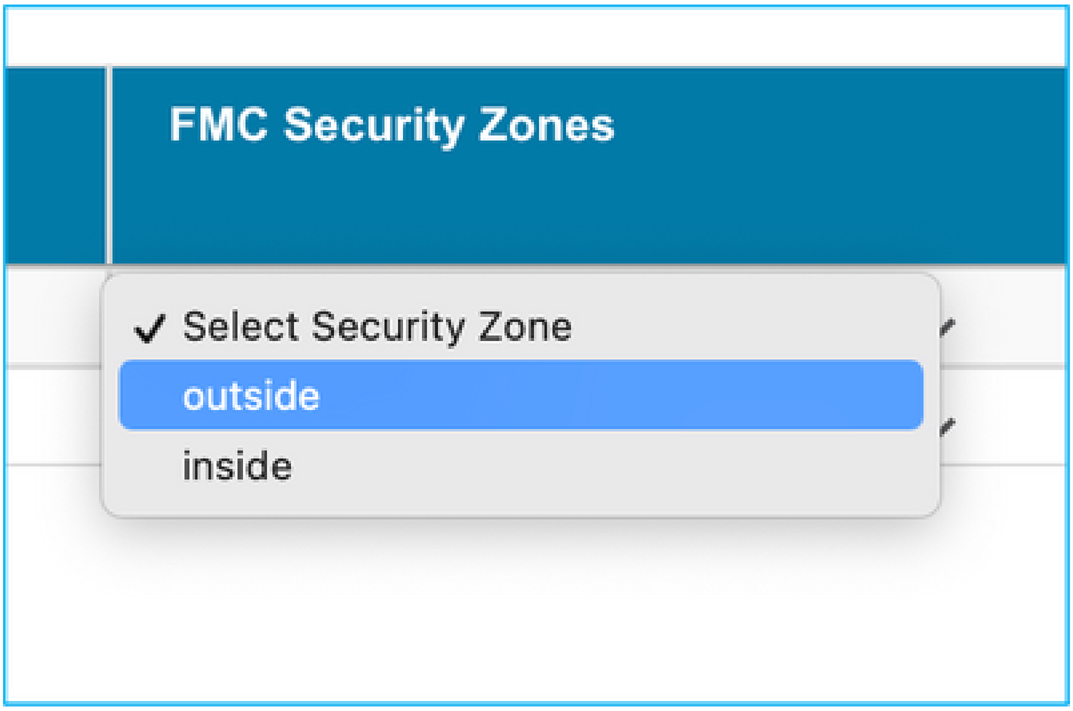
Firepower Migration Tool

Map Security Zones and Interface Groups

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

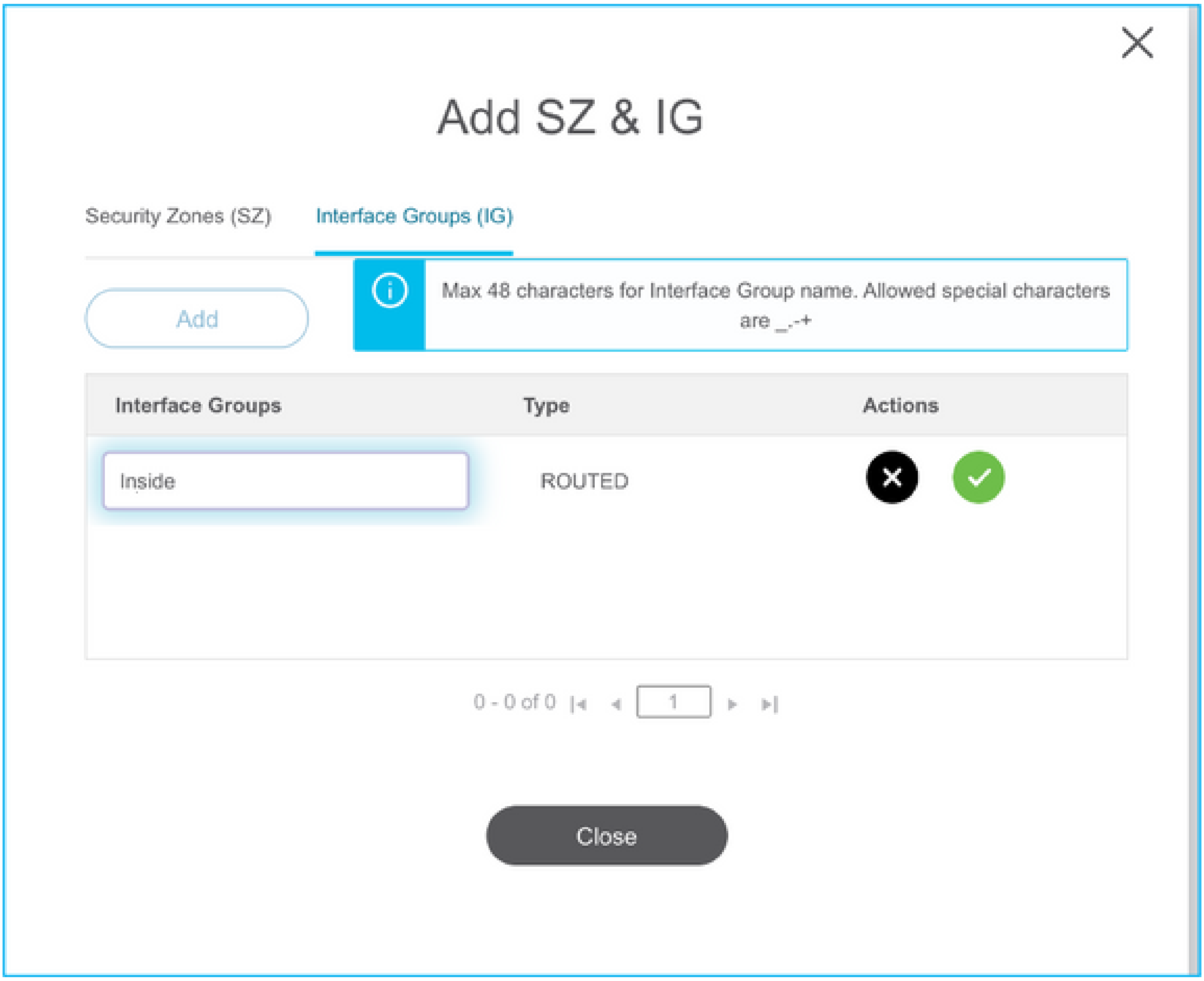
ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	Select Security Zone	Select Interface Groups
Outside	GigabitEthernet0/2	Select Security Zone	Select Interface Groups

A. Se o FMC tiver zonas de segurança e grupos de interface já criados, você poderá selecioná-los conforme necessário:



FMC Security Zones

B. Se houver necessidade de criar zonas de segurança e um grupo de interface, clique em **Adicionar SZ e IG** como mostrado na imagem.



Add SZ & IG

Security Zones (SZ)	Interface Groups (IG)

Add

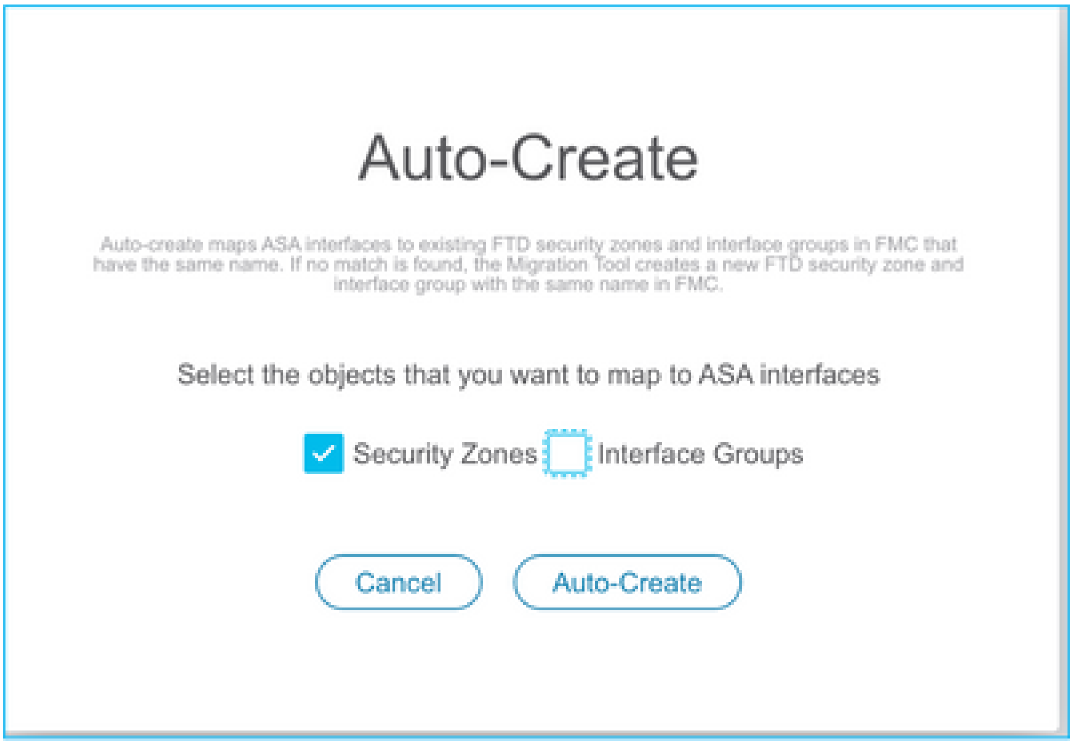
Max 48 characters for Interface Group name. Allowed special characters are _.-+

Interface Groups	Type	Actions
Inside	ROUTED	✕ ✓

0 - 0 of 0 |◂ ◂ 1 ▸ ▸|

Close

C. Caso contrário, você pode optar pela opção **Criação automática** que criará zonas de segurança e grupos de interface com o nome **ASA logical interface_sz** e **ASA logical interface_ig** respectivamente.

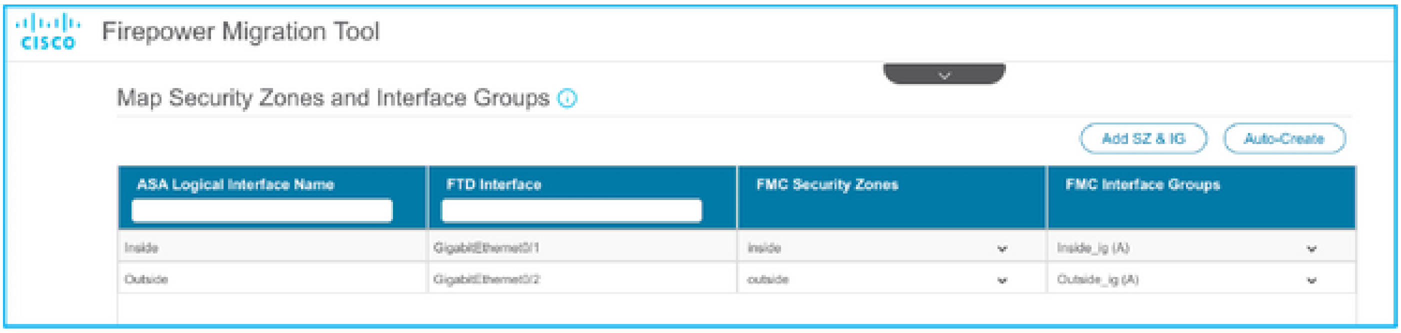


Auto-Create

Auto-create maps ASA interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to ASA interfaces

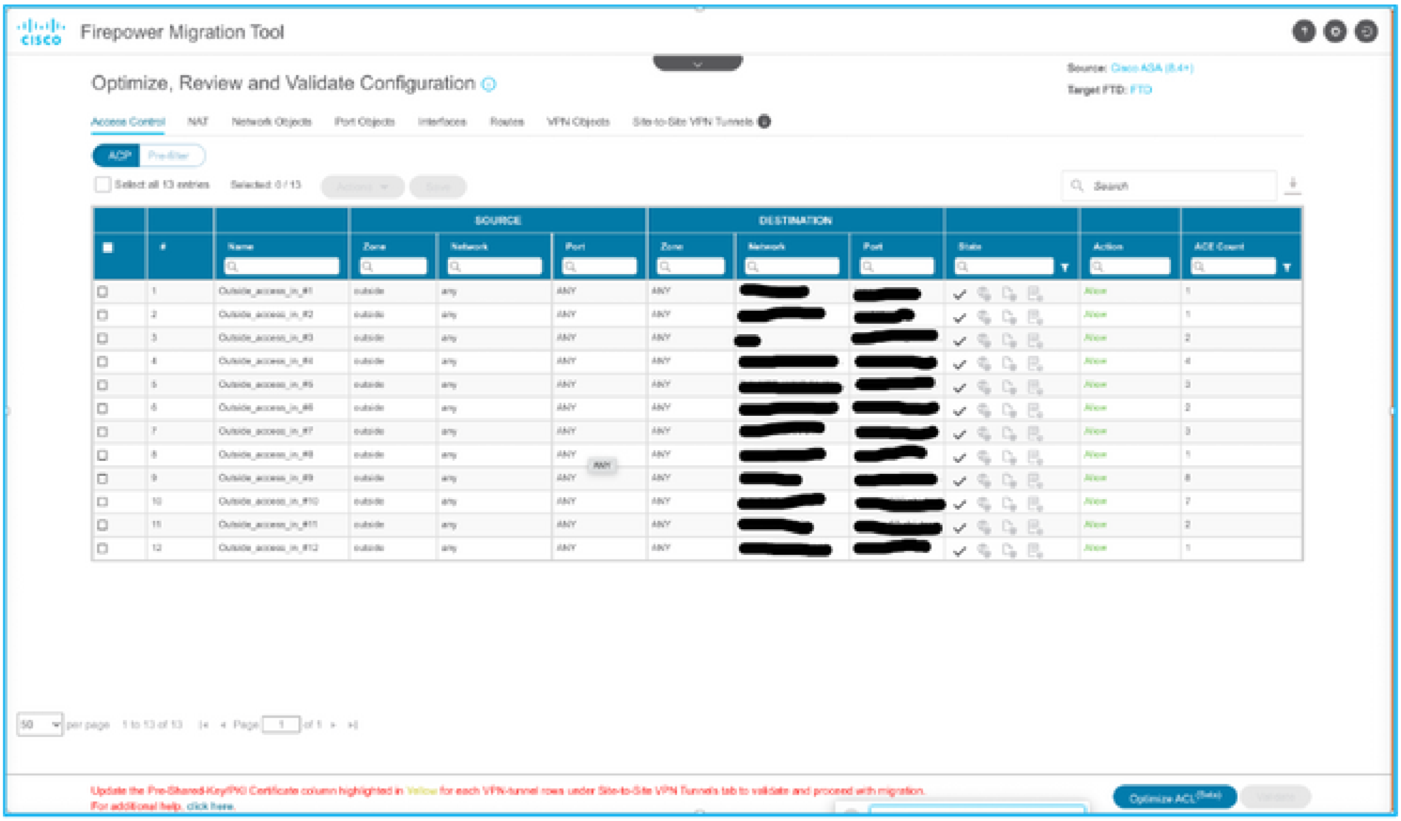
☑ Security Zones ☐ Interface Groups



Map Security Zones and Interface Groups

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
Inside	GigabitEthernet0/1	inside	Inside_ig (A)
Outside	GigabitEthernet0/2	outside	Outside_ig (A)

18. Revise e valide cada um dos elementos FTD criados. Os alertas são vistos em vermelho como mostrado na imagem.



Optimize, Review and Validate Configuration

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

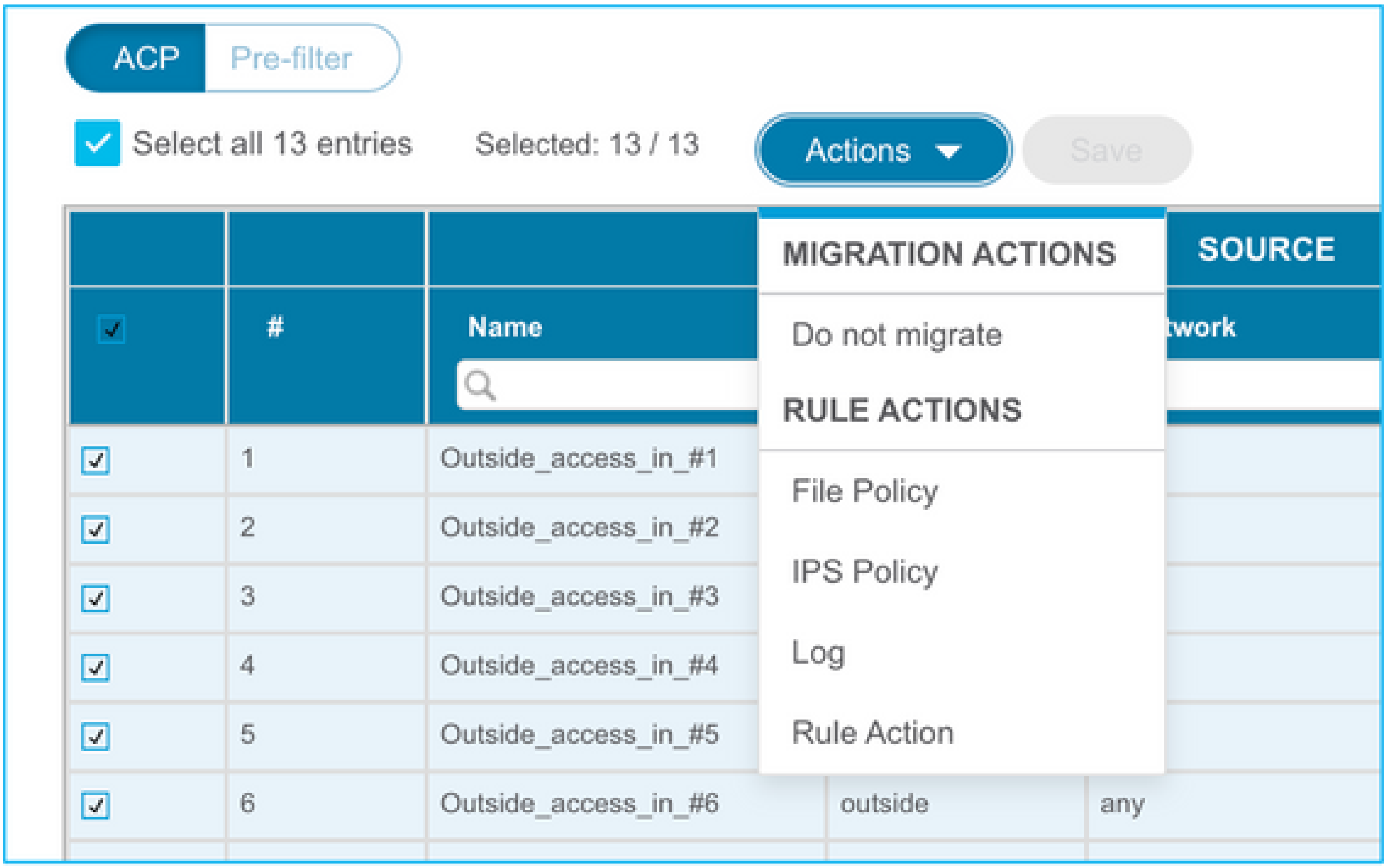
☐ Select all 13 entries   Selected: 0 / 13

			SOURCE			DESTINATION					
☐	#	Name	Zone	Network	Port	Zone	Network	Port	State	Action	ACE Count
☐	1	Outside_access_in_#1	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1
☐	2	Outside_access_in_#2	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1
☐	3	Outside_access_in_#3	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	2
☐	4	Outside_access_in_#4	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	4
☐	5	Outside_access_in_#5	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	3
☐	6	Outside_access_in_#6	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	2
☐	7	Outside_access_in_#7	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	3
☐	8	Outside_access_in_#8	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1
☐	9	Outside_access_in_#9	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	8
☐	10	Outside_access_in_#10	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	7
☐	11	Outside_access_in_#11	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	2
☐	12	Outside_access_in_#12	outside	any	ANY	ANY	[redacted]	[redacted]	✓	Allow	1

50 per page 1 to 13 of 13 |< < Page 1 of 1 > >|

Update the Pre-Shared-Key/PKI Certificate column highlighted in Yellow for each VPN-tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration.
For additional help, click here.

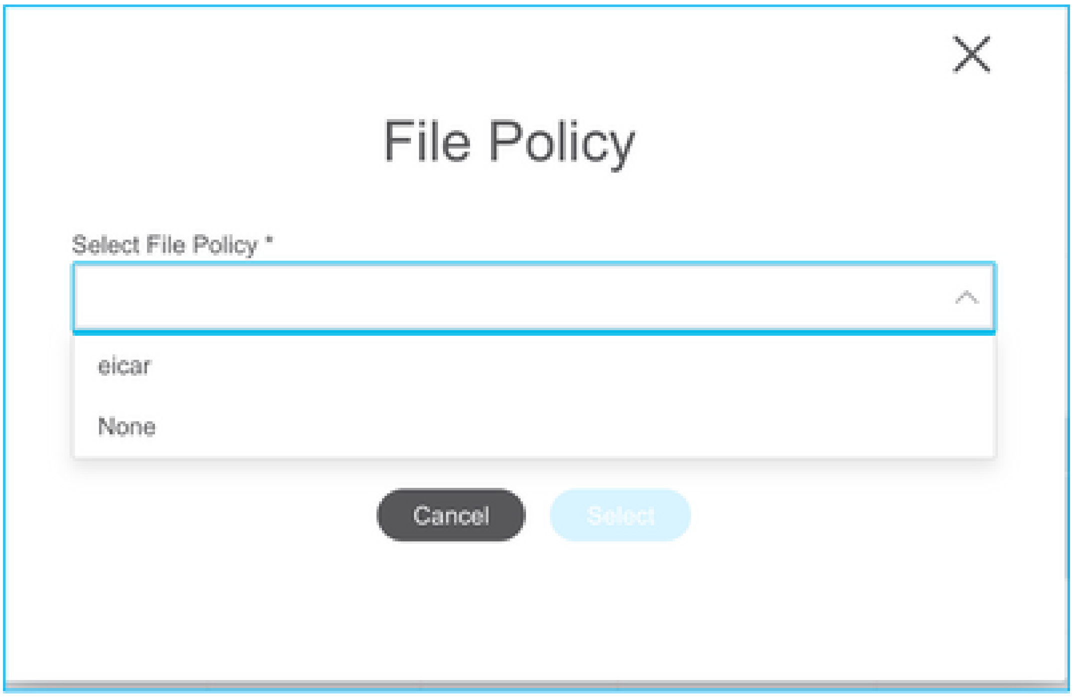
19. As ações de migração podem ser selecionadas conforme mostrado na imagem se você quiser editar qualquer regra. Os recursos FTD de adição de arquivos e política de IPS podem ser feitos nesta etapa.



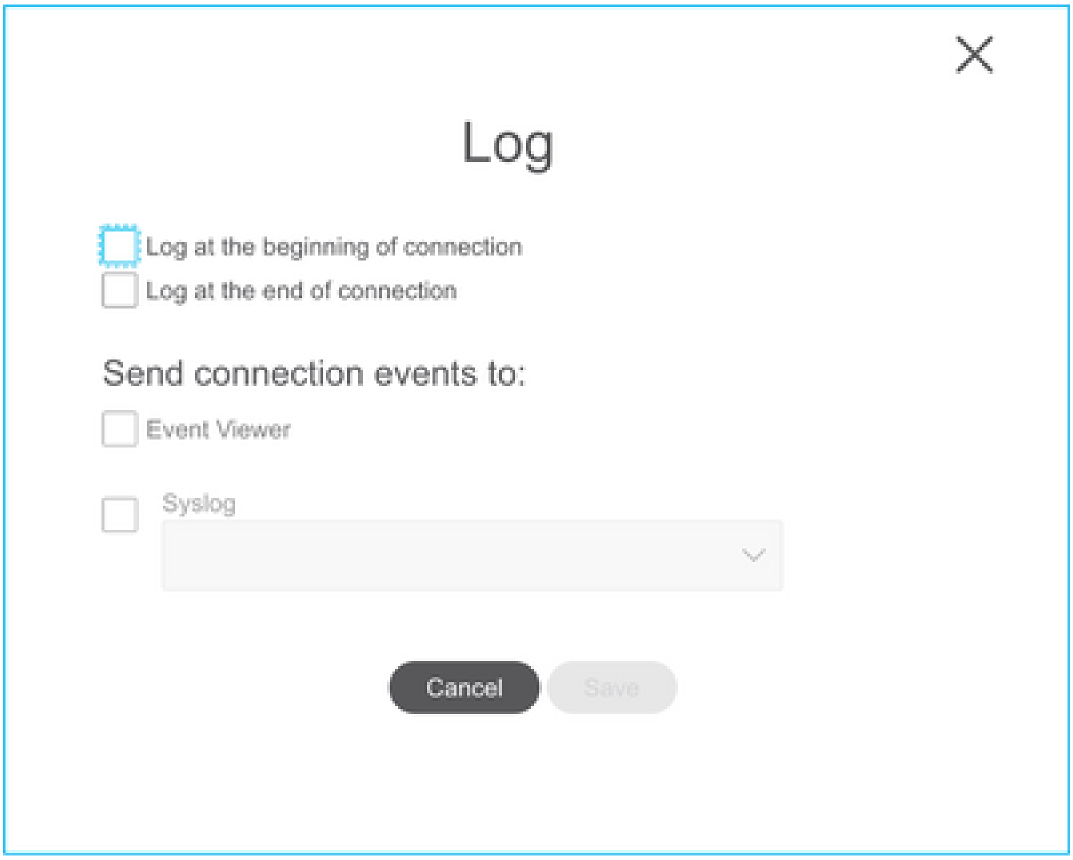
☑ Select all 13 entries Selected: 13 / 13

☑	#	Name			twork
☑	1	Outside_access_in_#1			
☑	2	Outside_access_in_#2			
☑	3	Outside_access_in_#3			
☑	4	Outside_access_in_#4			
☑	5	Outside_access_in_#5			
☑	6	Outside_access_in_#6	outside	any	

Note: Se as Políticas de arquivo já existirem no FMC, elas serão preenchidas como mostrado na imagem. O mesmo se aplica às políticas de IPS junto com as políticas padrão.



A configuração do log pode ser feita para as regras necessárias. A configuração do servidor syslog existente no FMC pode ser selecionada neste estágio.



Log

□ Log at the beginning of connection

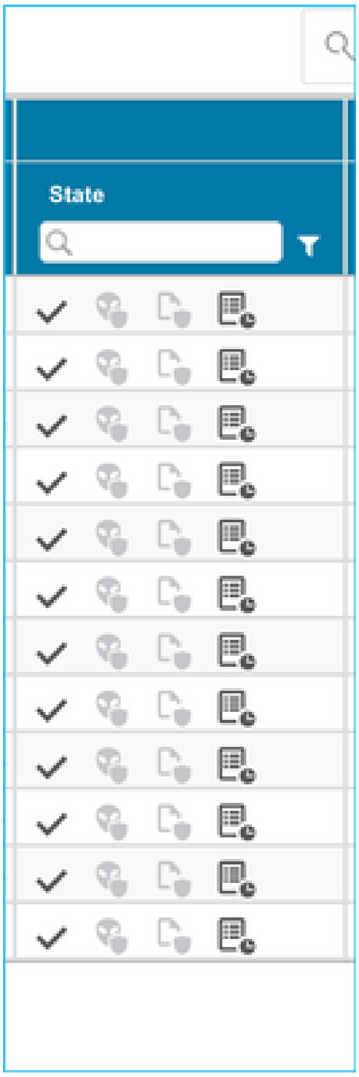
□ Log at the end of connection

Send connection events to:

□ Event Viewer

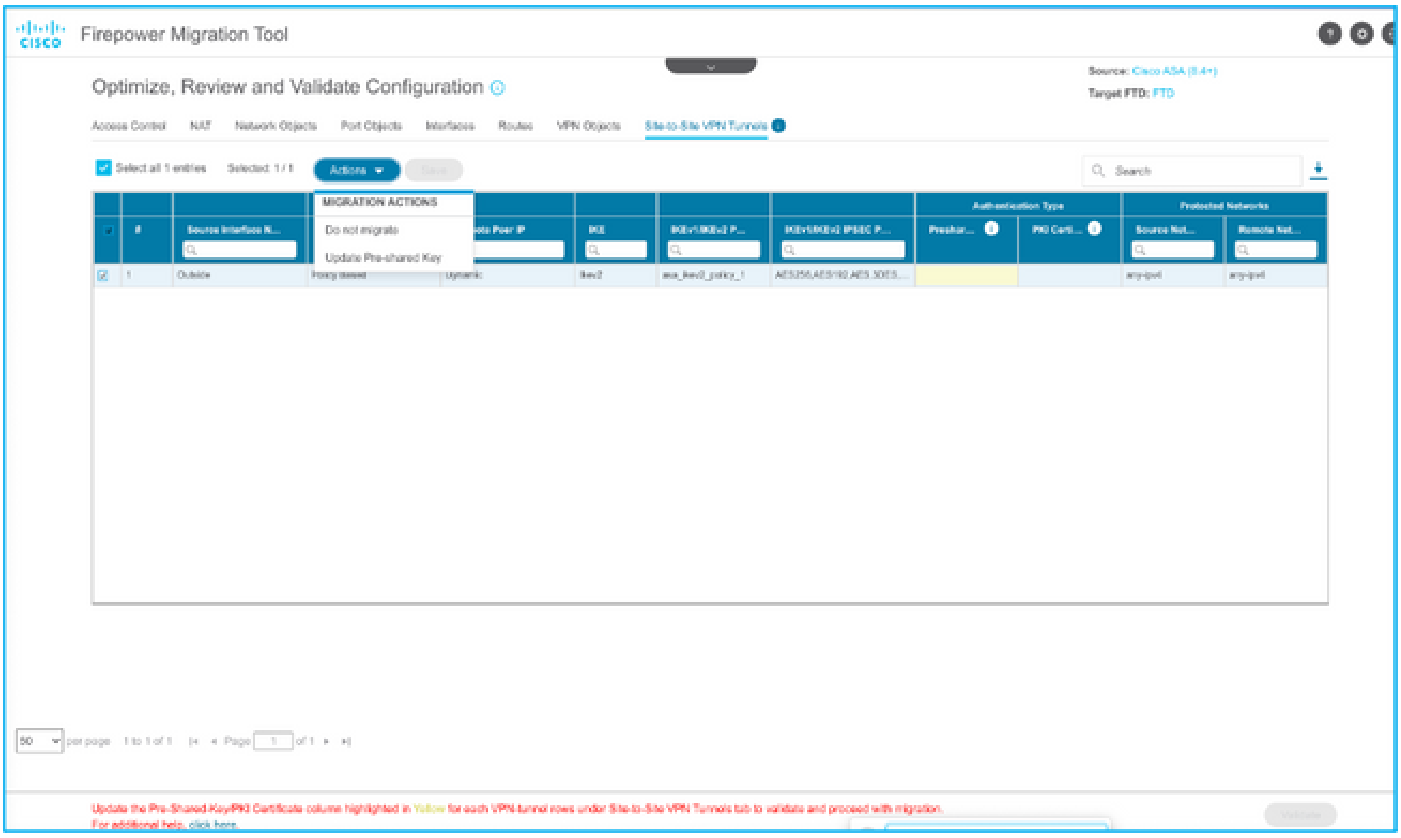
□ Syslog

As ações de regra selecionadas serão destacadas de acordo com cada regra.



20. Da mesma forma, NAT, Objeto de Rede, Objetos de Porta, Interfaces, Rotas, Objetos VPN, Túneis VPN Site a Site e outros elementos de acordo com sua configuração podem ser revisados passo a passo.

> **Note**: O alerta será notificado conforme mostrado na imagem para atualizar a chave pré-compartilhada, pois ela não é copiada no arquivo de configuração do ASA. Selecione **Ações > Atualizar chave pré-compartilhada** para inserir o valor.



Firepower Migration Tool

Optimize, Review and Validate Configuration

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

Access Control | NAT | Network Objects | Port Objects | Interfaces | Routes | VPN Objects | Site-to-Site VPN Tunnels

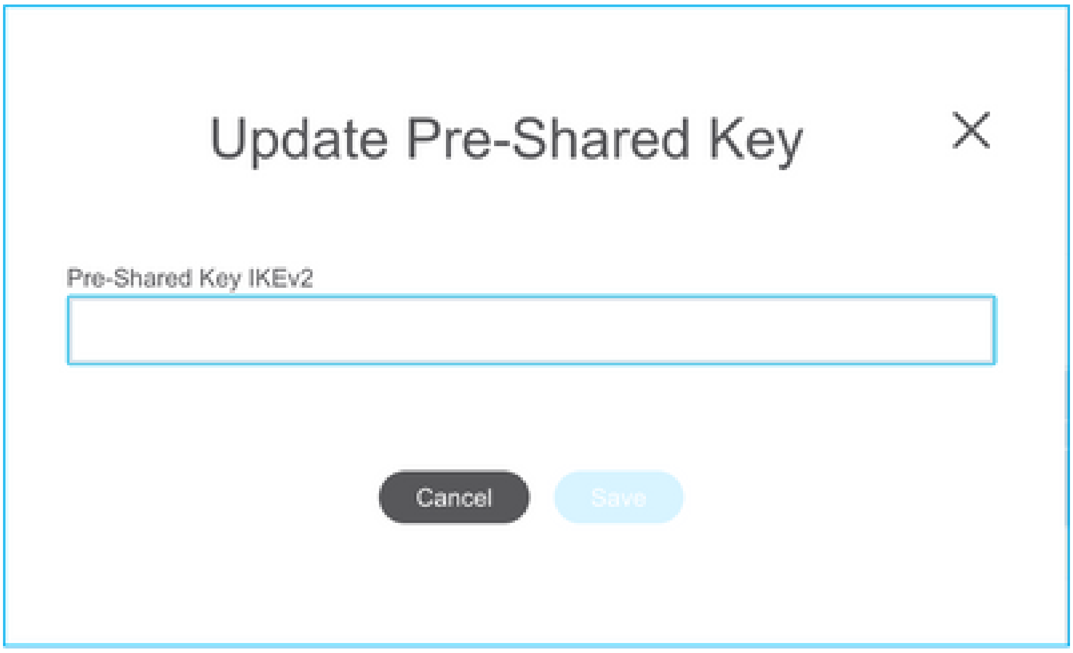
☑ Select all 1 entries   Selected: 1 / 1   Actions ▾   Save

								Authentication Type		Protected Networks	
☑	#	Source Interface N...		...ote Peer IP	IKE	IKEv1/IKEv2 P...	IKEv1/IKEv2 IPSEC P...	Preshar...	PKI Certi...	Source Net...	Remote Net...
☑	1	Outside	Policy Based	Dynamic	ikev2	asa_ikev2_policy_1	AES256,AES192,AES,3DES...			any-ipv4	any-ipv4

50 per page 1 to 1 of 1 |◂ ◂ Page 1 of 1 ▸ ▸|

Update the Pre-Shared-Key/PKI Certificate column highlighted in Yellow for each VPN tunnel rows under Site-to-Site VPN Tunnels tab to validate and proceed with migration.
For additional help, click here.

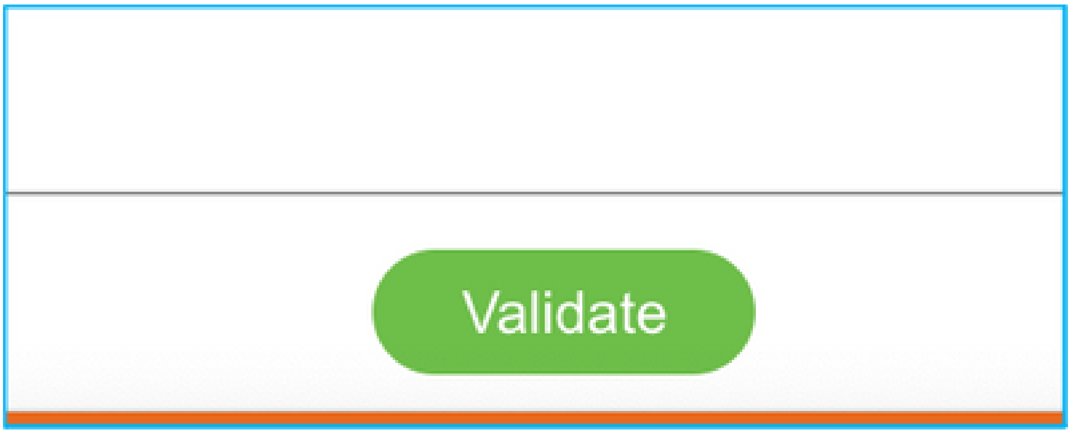
Validate



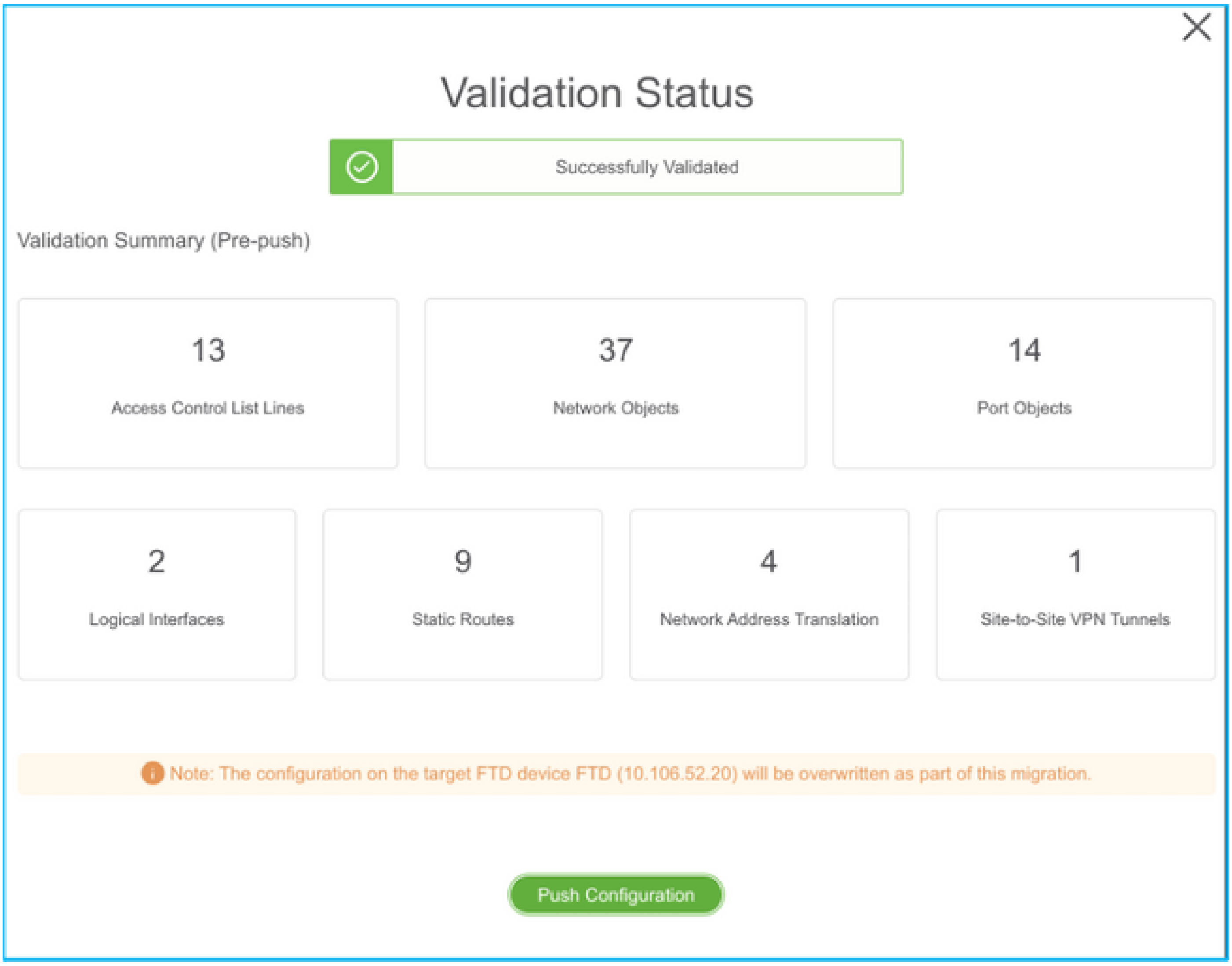
Update Pre-Shared Key

Pre-Shared Key IKEv2

21. Finalmente, clique no ícone **Validar** na parte inferior direita da tela, como mostrado na imagem.



22. Depois que a validação for bem-sucedida, clique em **Push Configuration** como mostrado na imagem.



Validation Status

Successfully Validated

Validation Summary (Pre-push)

13 Access Control List Lines

37 Network Objects

14 Port Objects

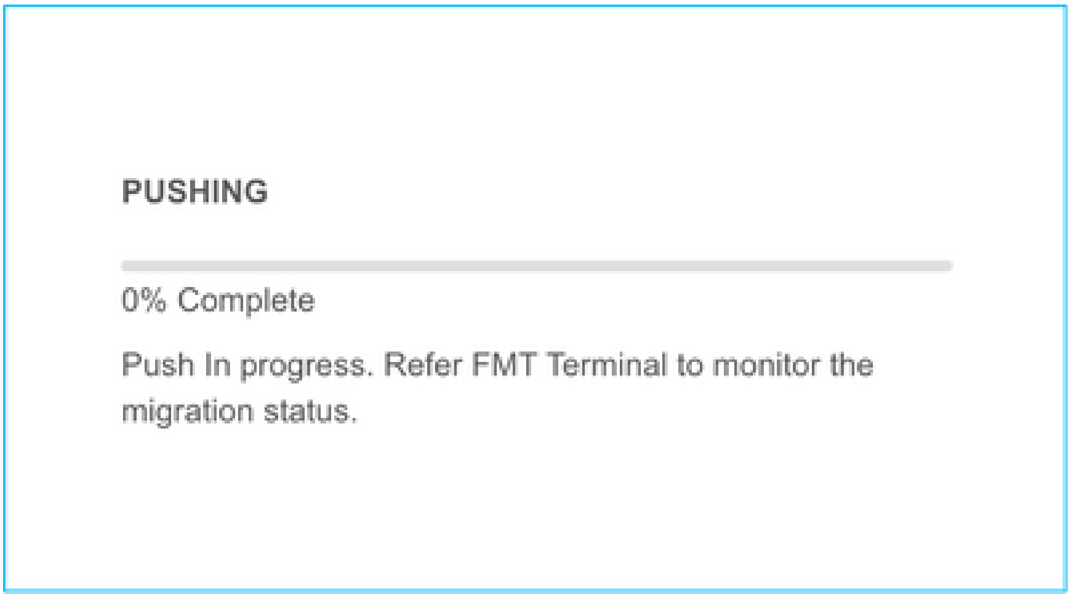
2 Logical Interfaces

9 Static Routes

4 Network Address Translation

1 Site-to-Site VPN Tunnels

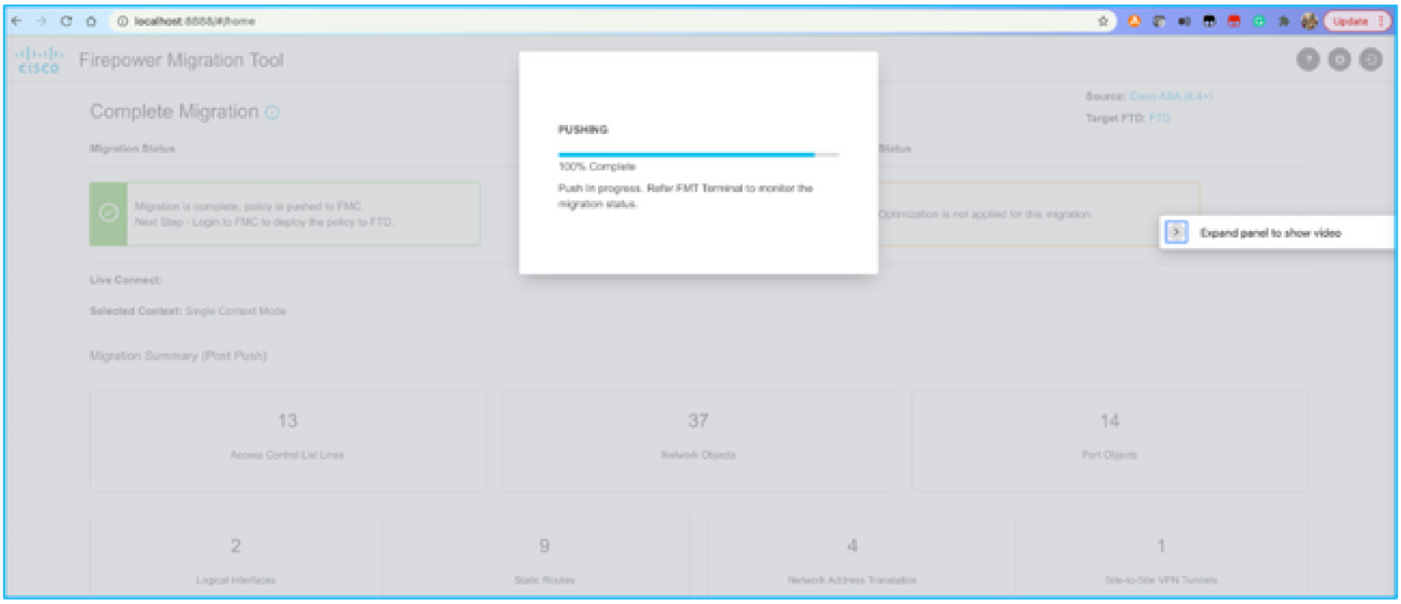
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.



PUSHING

0% Complete

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



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.

Status

Optimization is not applied for this migration.

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

13 Access Control List Lines

37 Network Objects

14 Port Objects

2 Logical Interfaces

9 Static Routes

4 Network Address Translation

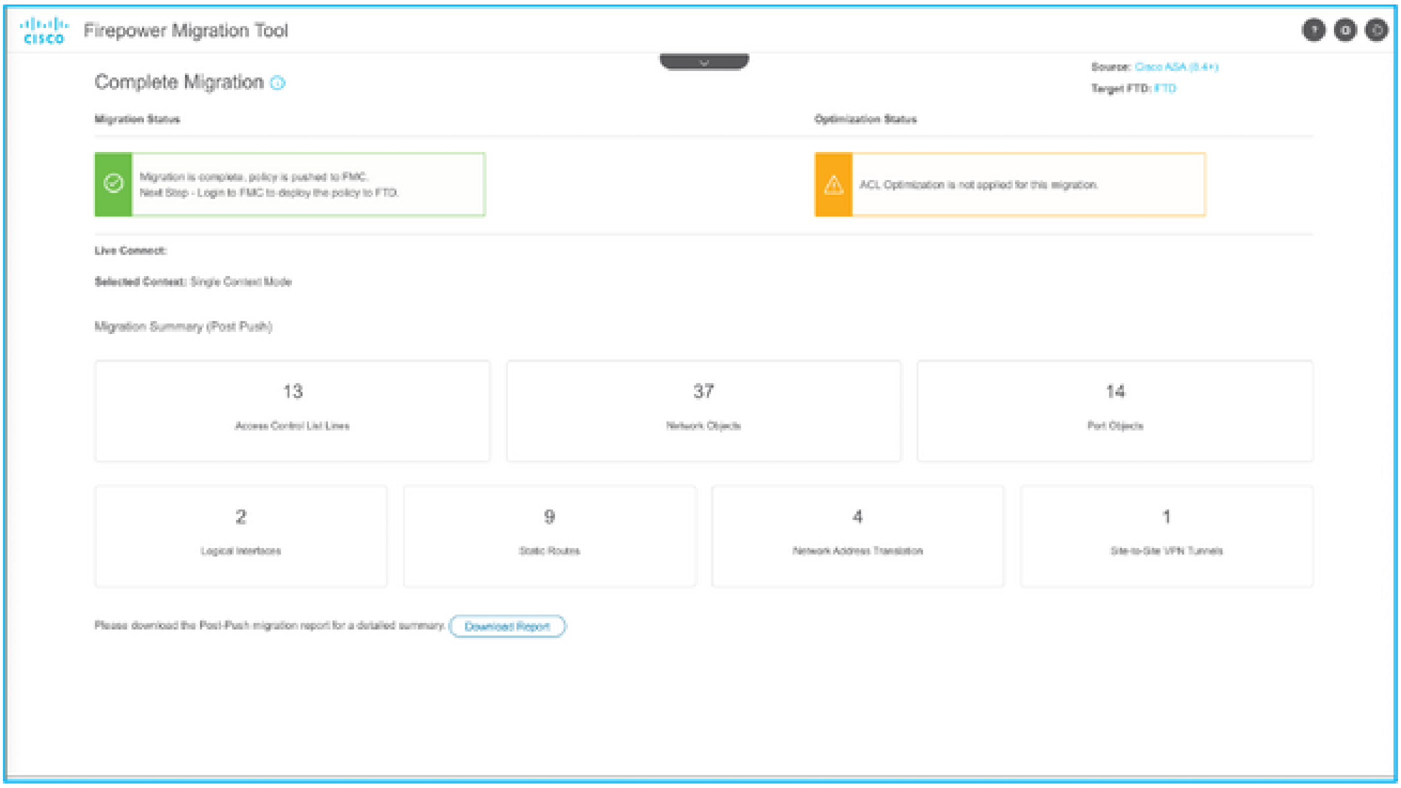
1 Site-to-Site VPN Tunnels

PUSHING

100% Complete

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

23. Quando a migração for bem-sucedida, a mensagem que será exibida será mostrada na imagem.



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:

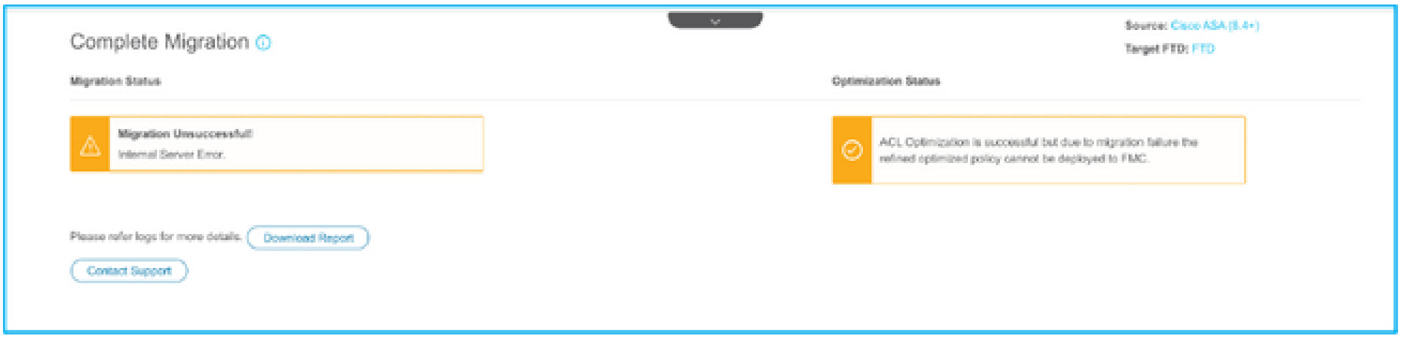
Selected Context: Single Context Mode

Migration Summary (Post Push)

13	Access Control List Lines
37	Network Objects
14	Port Objects
2	Logical Interfaces
9	Static Routes
4	Network Address Translation
1	Site-to-Site VPN Tunnels

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

Note: Se a migração não for bem-sucedida, clique em **Download Report** para exibir o relatório pós-migração.



Complete Migration

Source: Cisco ASA (8.4+)

Target FTD: FTD

Migration Status

Migration Unsuccessful!
Internal Server Error.

Optimization Status

ACL Optimization is successful but due to migration failure the refined optimized policy cannot be deployed to FMC.

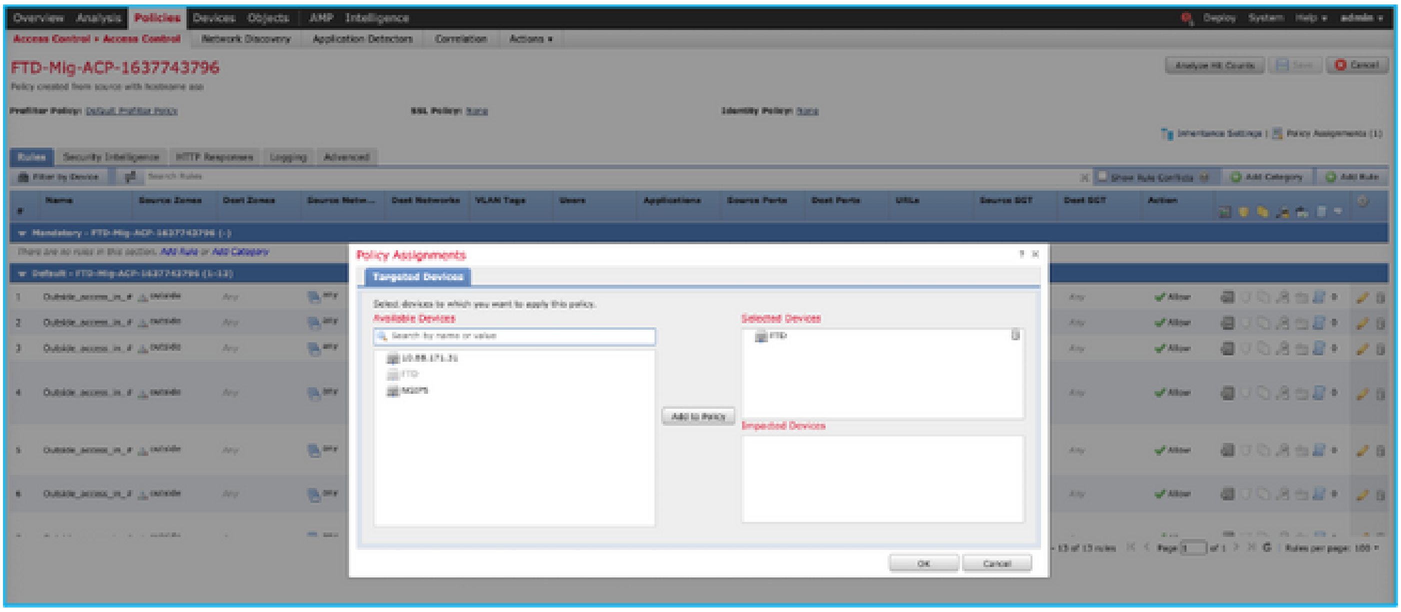
Please refer logs for more details.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Validação no CVP.

1. Navegue para **Políticas > Controle de Acesso > Política de Controle de Acesso > Atribuição de Política** para confirmar se o FTD selecionado está preenchido.



FTD-Mig-ACP-1637743796

Policy created from source with hostname asa

Policy Assignments

Targeted Devices

Select devices to which you want to apply this policy.

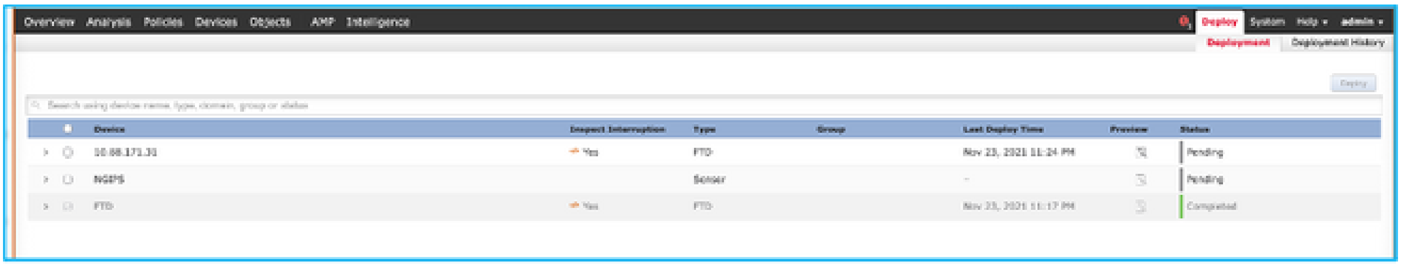
Available Devices: 10.88.171.31, FTD, NGIPS

Selected Devices: FTD

Impacted Devices

Note: A política de controle de acesso à migração teria um nome com o prefixo **FTD-Mig-ACP**. Se não tiver sido selecionado um DTF na etapa 2.8, o DTF deve ser selecionado no CVP.

2. Empurre a política para o FTD. Navegue até **Implantar > Implantação > Nome do FTD > Implantar** como mostrado na imagem.



Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
10.88.171.31	Yes	FTD		Nov 23, 2021 11:24 PM		Pending
NGIPS		Sensor		-		Pending
FTD	Yes	FTD		Nov 23, 2021 11:17 PM		Completed

Erros conhecidos relacionados à ferramenta de migração Firepower

- ID de bug da Cisco CSCwa56374 - ferramenta FMT trava na página de mapeamento de zona com erro com alta utilização de memória
- ID de bug da Cisco CSCvz88730 - Falha de envio de interface para o tipo de interface de gerenciamento de canal de porta FTD
- ID de bug da Cisco CSCvx21986 - Migração do canal de porta para a plataforma de destino - o FTD virtual não é suportado
- ID de bug da Cisco CSCvy63003 - A ferramenta de migração deve desativar o recurso de interface se o FTD já fizer parte do cluster
- ID de bug da Cisco CSCvx08199 - a ACL precisa ser dividida quando a referência do aplicativo for superior a 50

Informações Relacionadas

- Migração do ASA Firewall para a Threat Defense com a ferramenta Firewall Migration

- Suporte Técnico e Documentação - Cisco Systems