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

Contents

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-sso- 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).

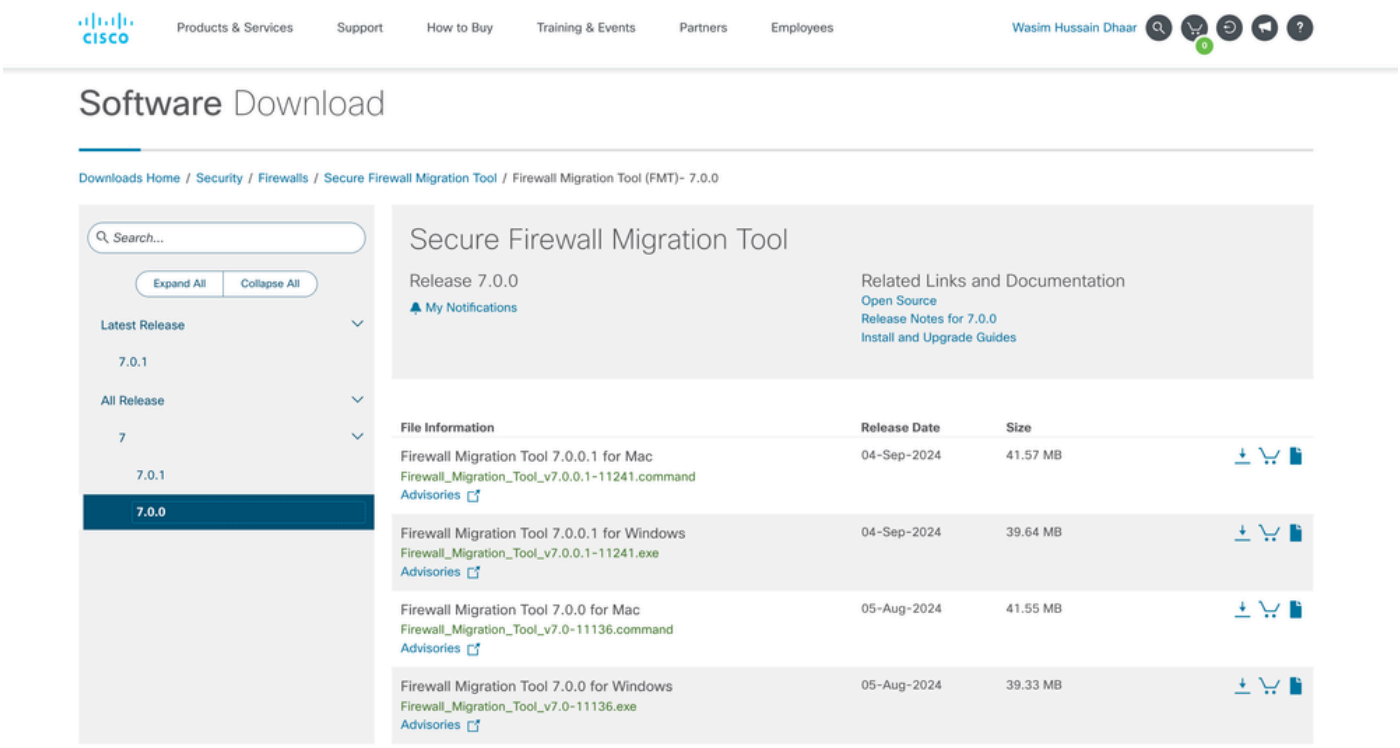
Os arquivos a-Dap.xml e Data.xml devem ser carregados no centro de gerenciamento a partir da ferramenta de migração do Secure Firewall na seção Revisar e validar > VPN de acesso remoto > Arquivo do AnyConnect.

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

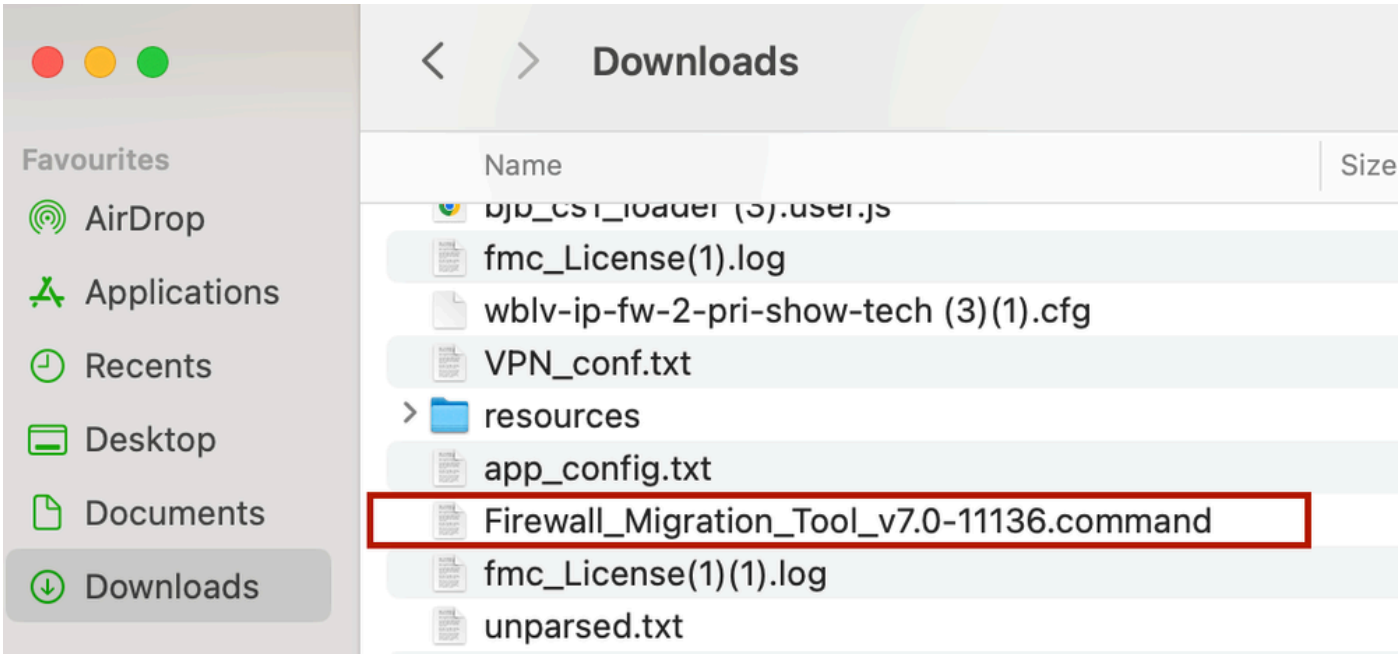
Configuration Steps:

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

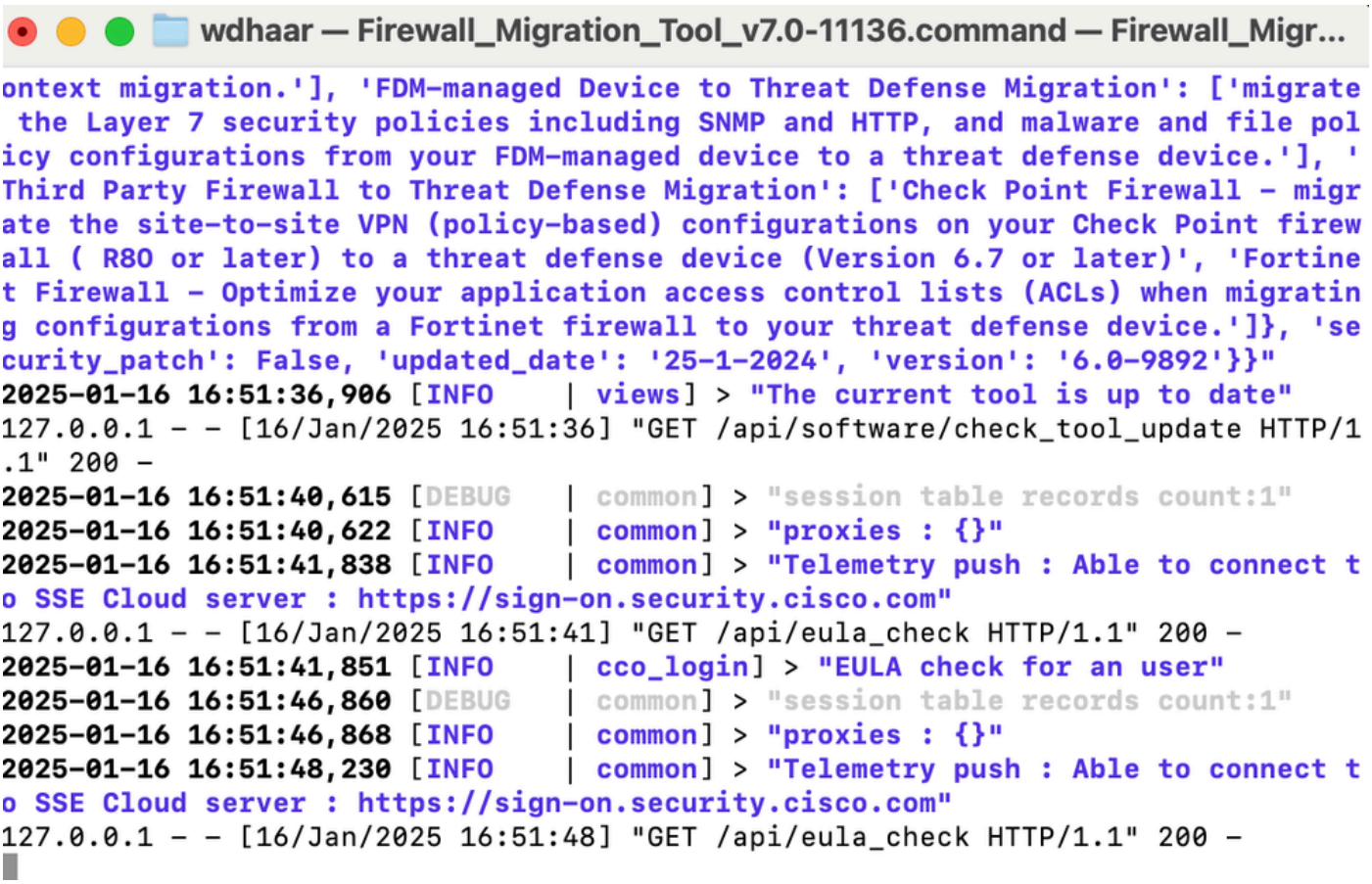


Download de software

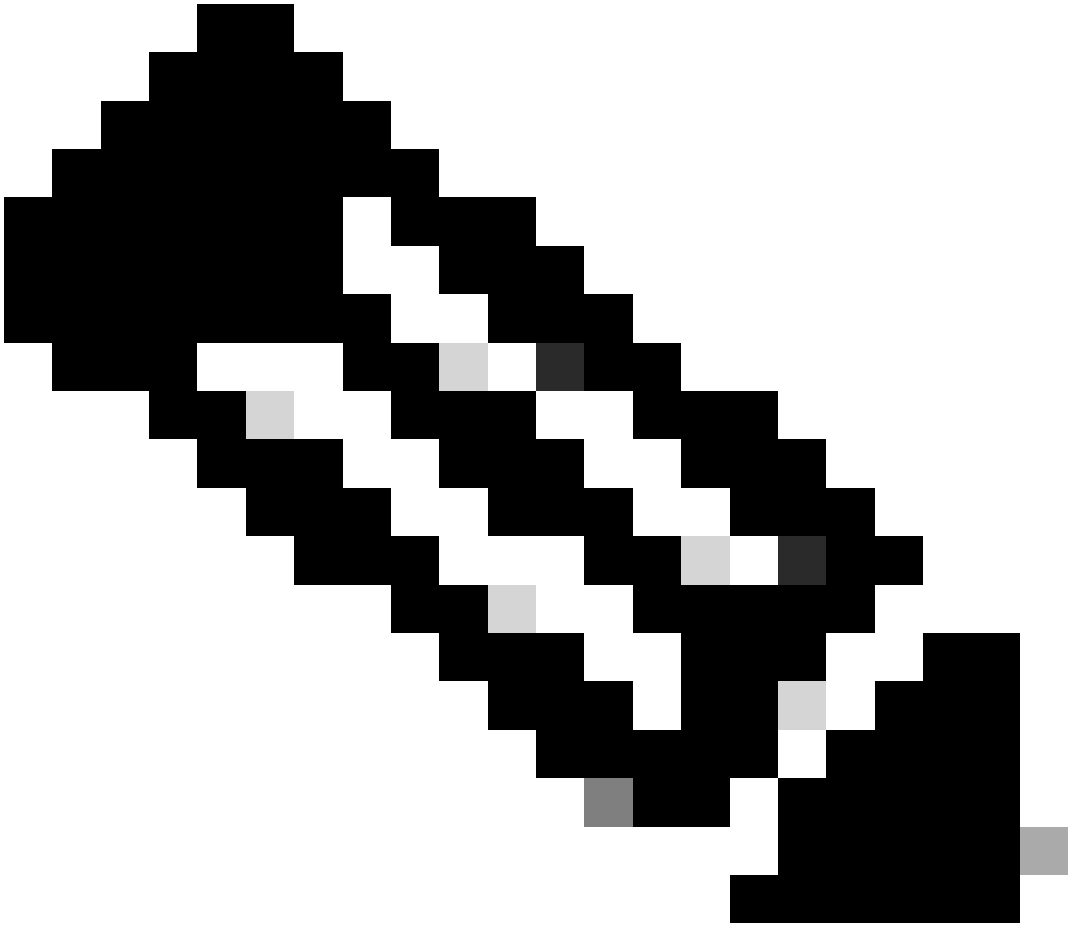
2. Clique no arquivo baixado anteriormente no computador.



O arquivo

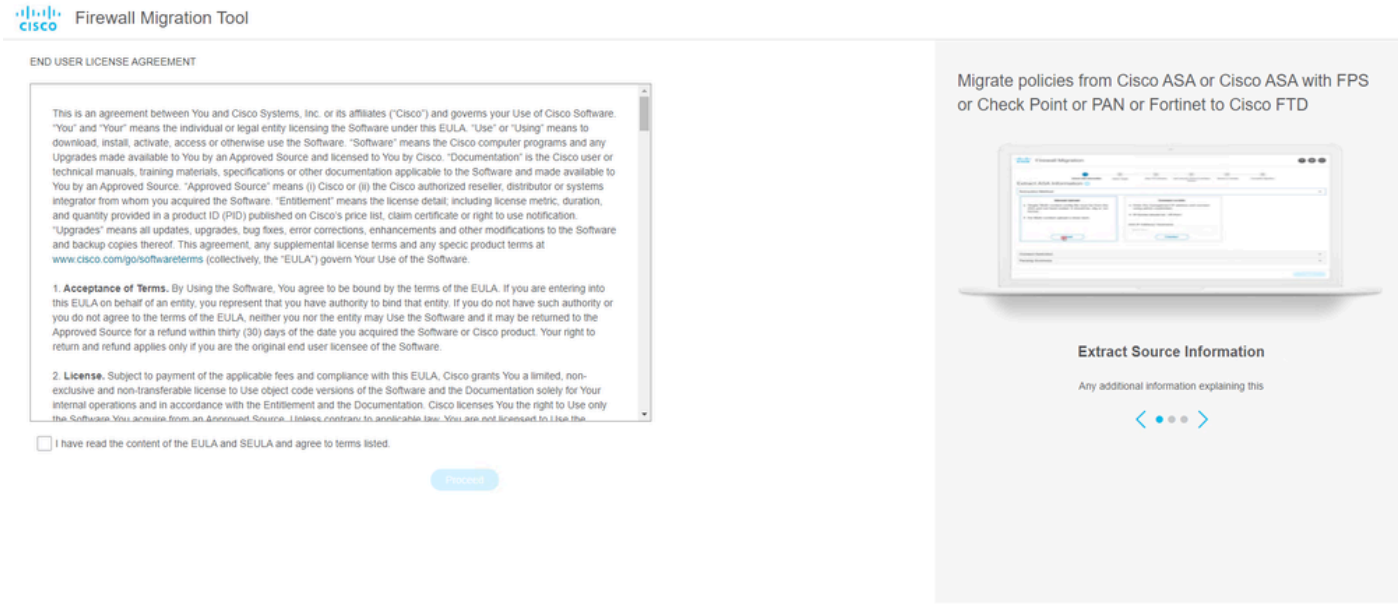


Logs de console



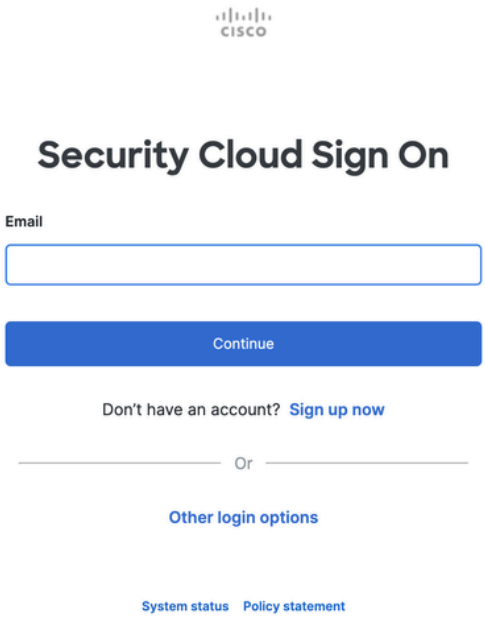
Note: O programa é aberto automaticamente e um console gera automaticamente o conteúdo no diretório onde você executou o arquivo.

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.



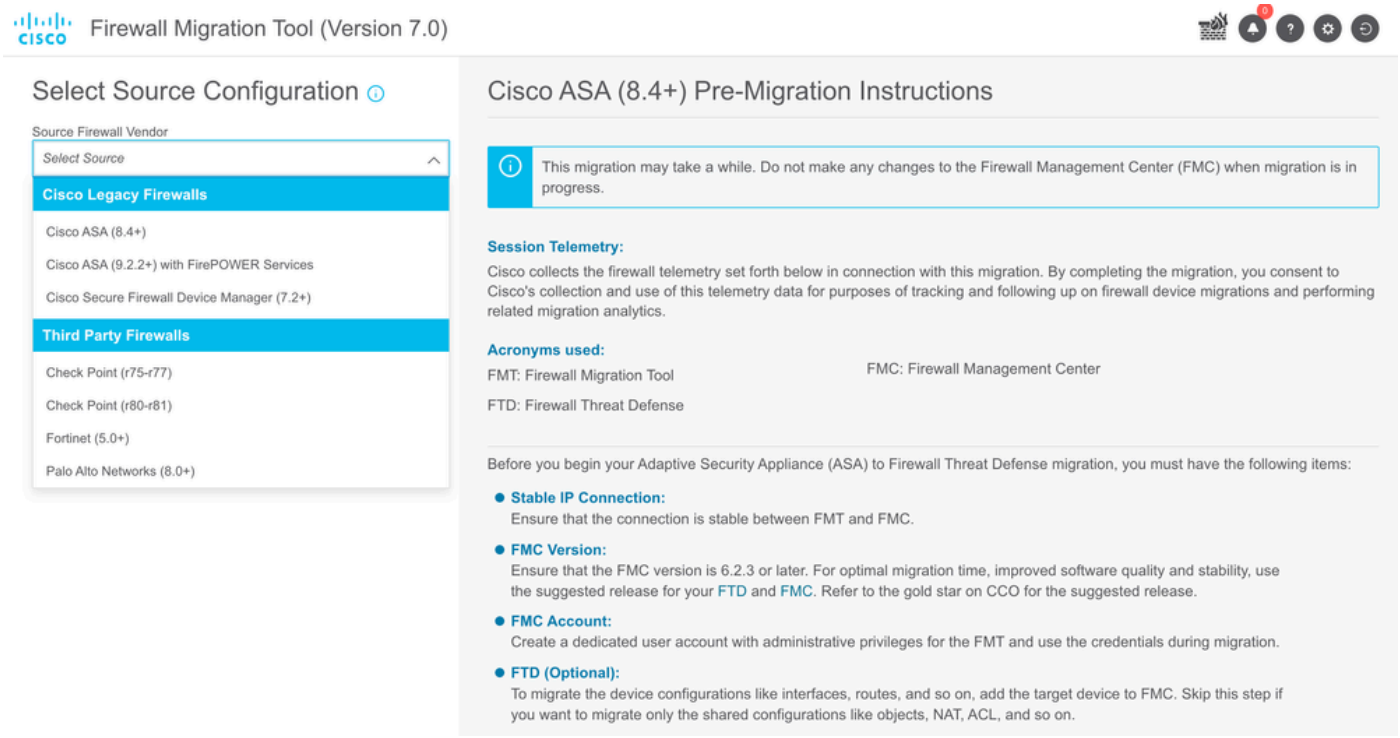
EULA

4. Faça login usando uma conta CCO válida e a interface GUI do FMT será exibida no navegador da Web.



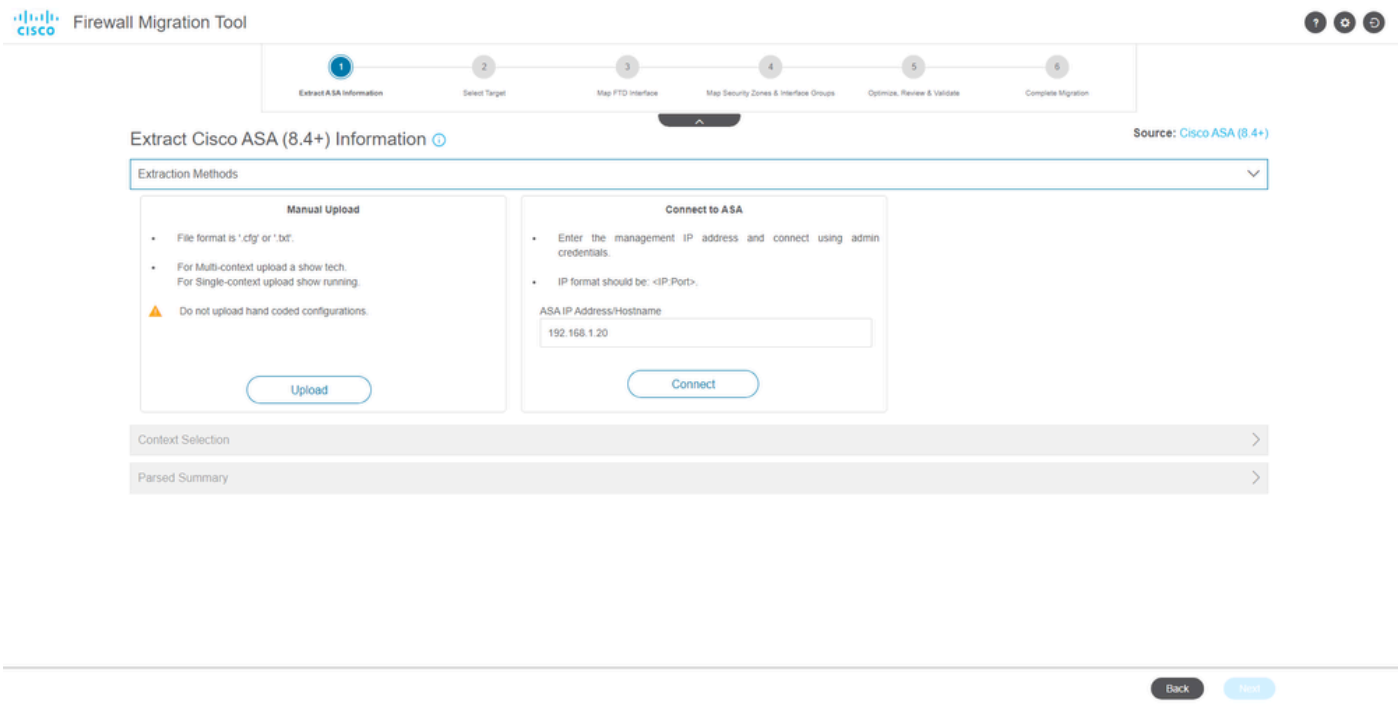
Login no FMT

5. Selecione o firewall de origem a ser migrado.

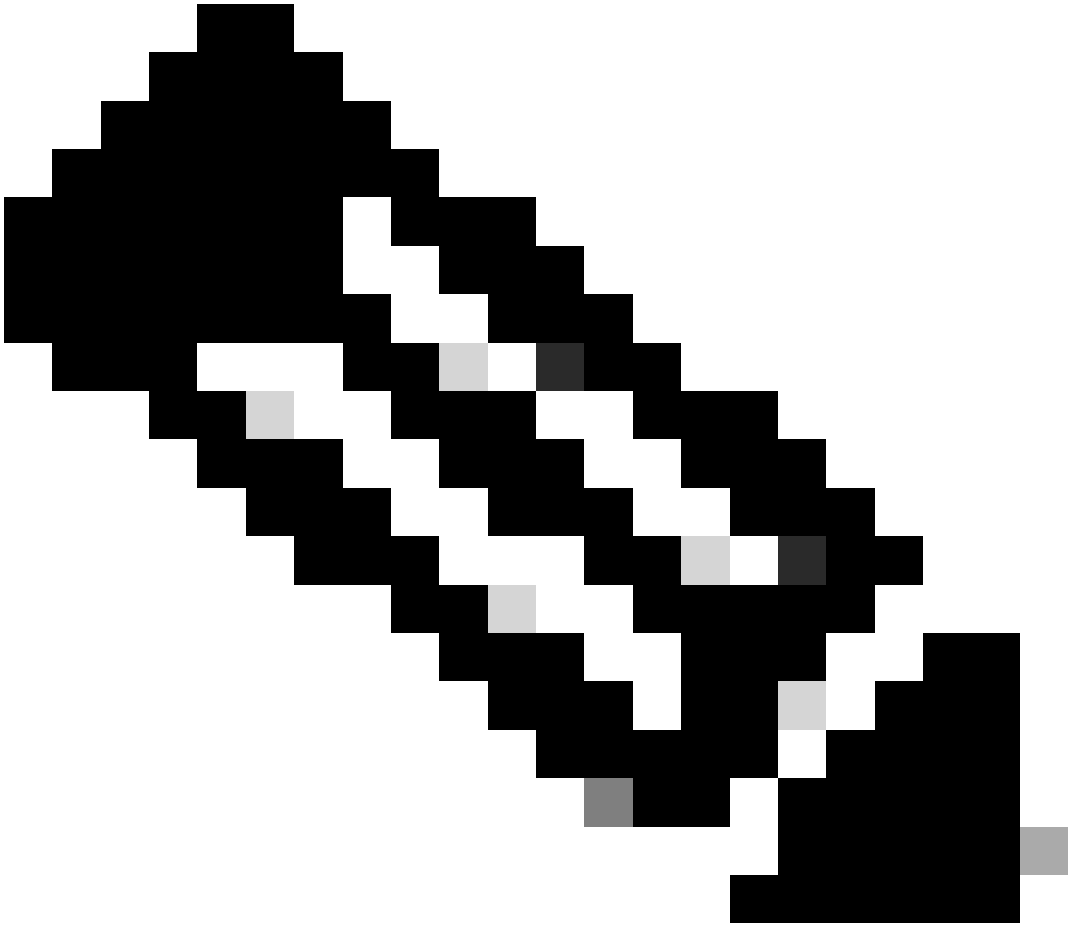


Firewall de origem

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

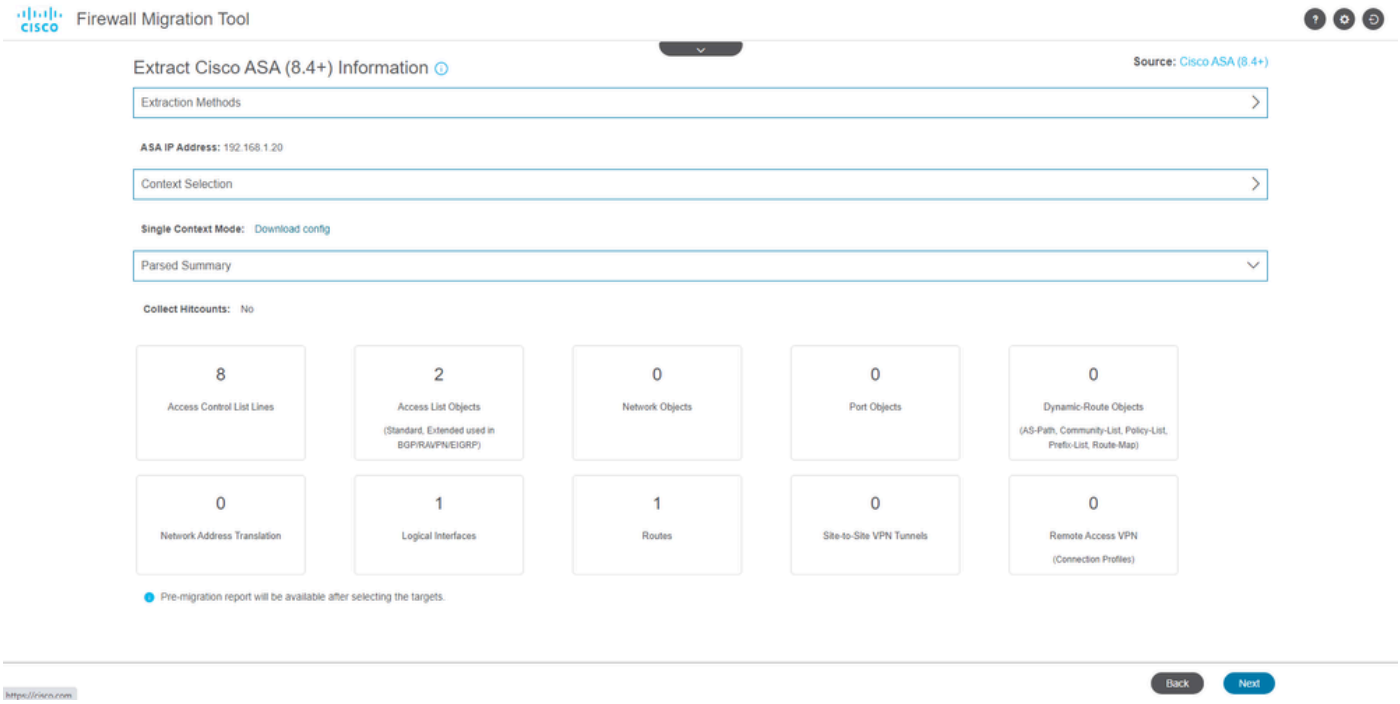


Extração



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

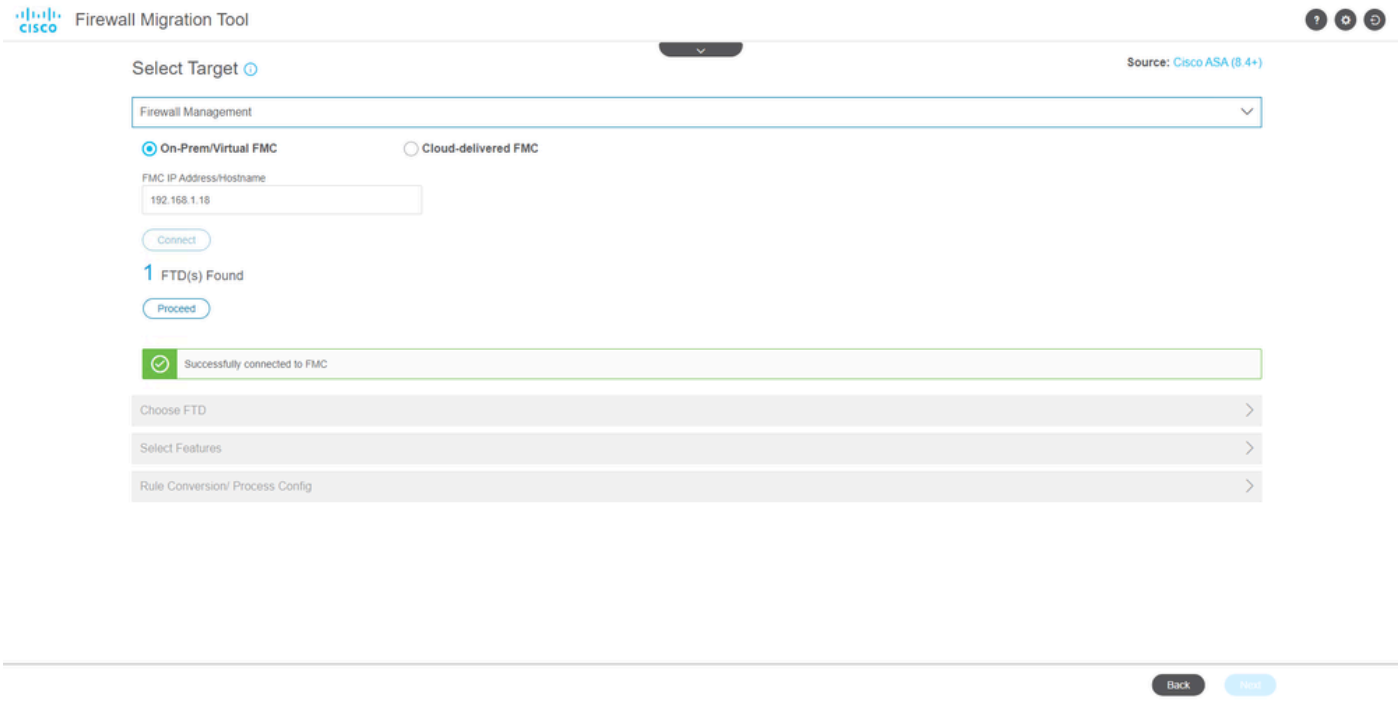
7. Um resumo da configuração encontrada no firewall é exibido como um painel. Clique em Avançar.



Summary

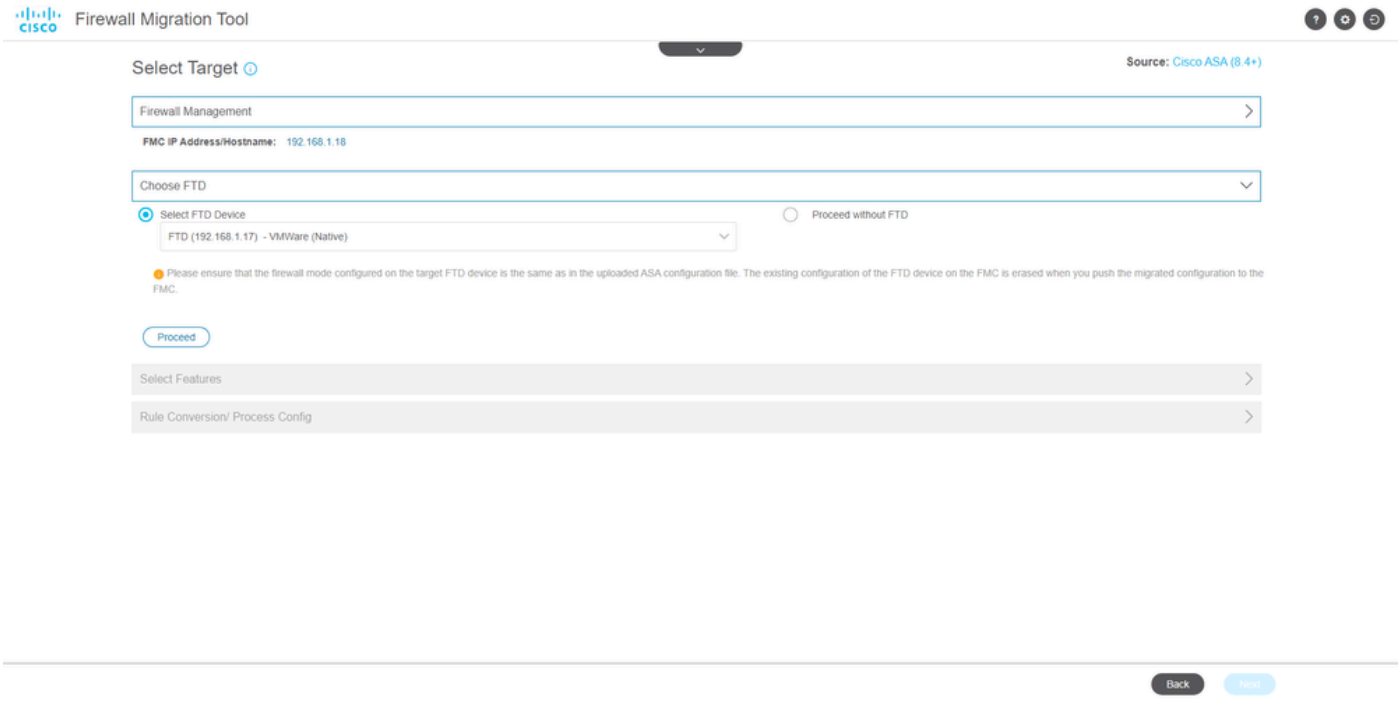
8. Selecione o FMC de destino a ser usado na migração.

Forneça o IP do FMC. Ele abre uma janela pop-up na qual solicita as credenciais de login do FMC.



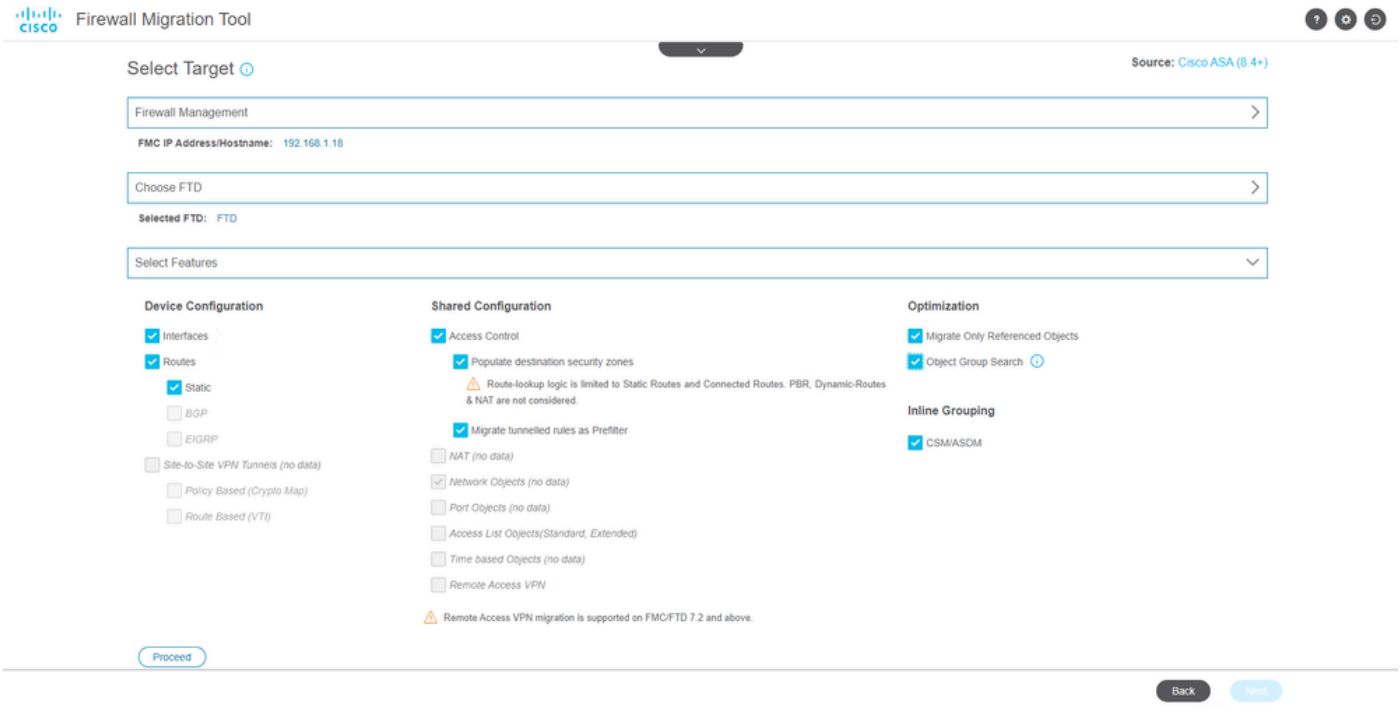
IP FMC

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



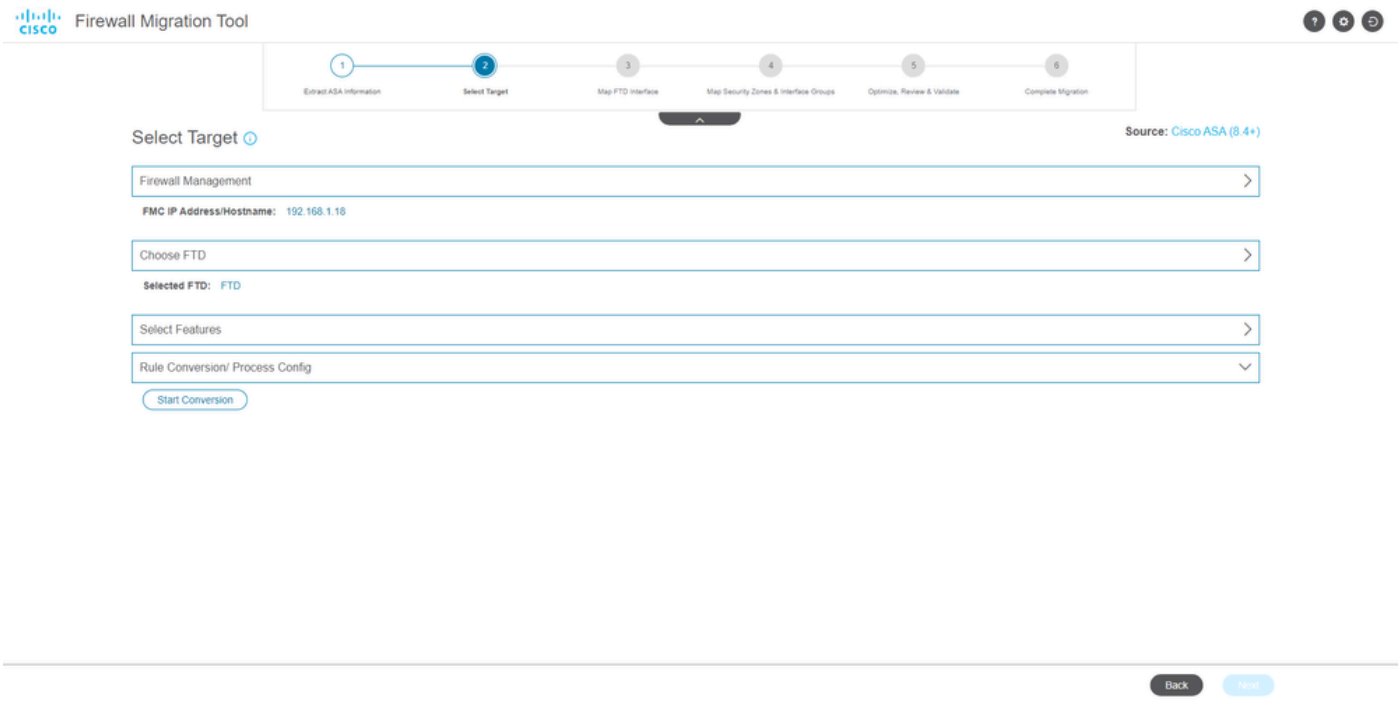
FTD de destino

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



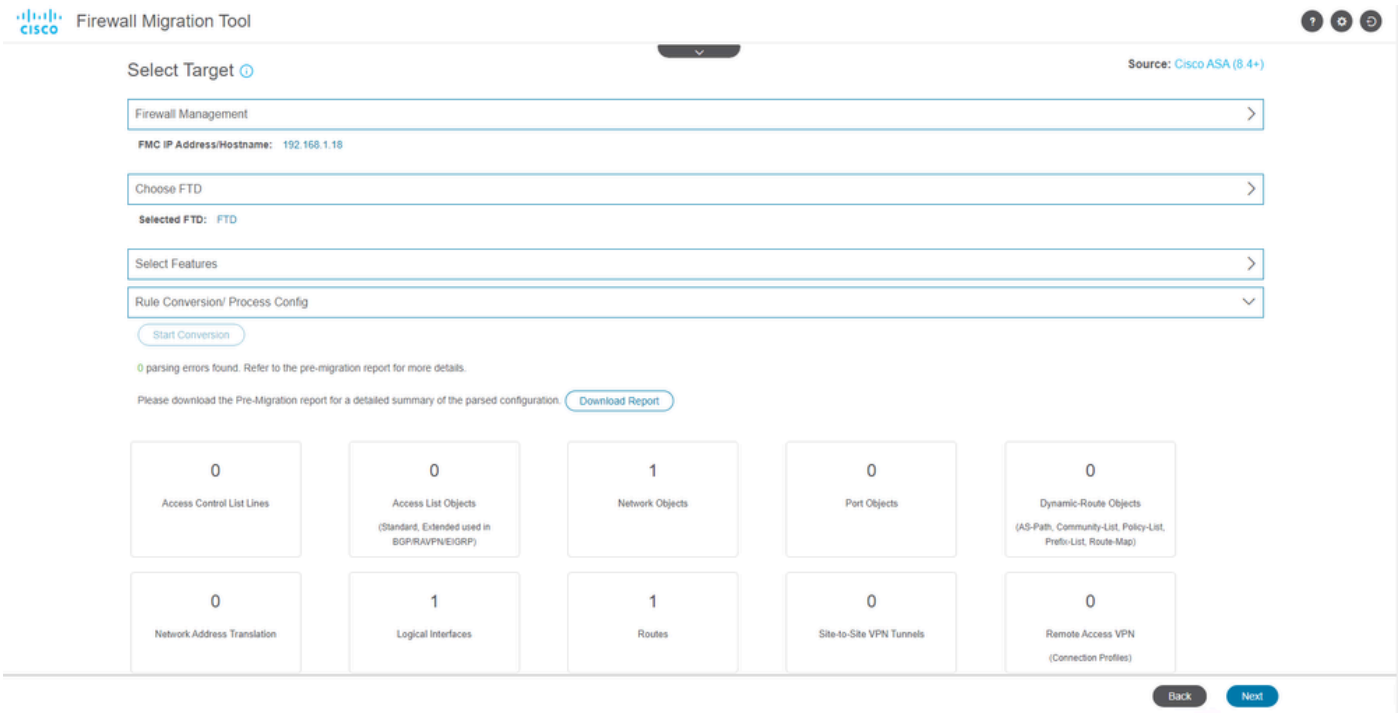
Configurações

11. Inicie a conversão das configurações do ASA para o FTD.



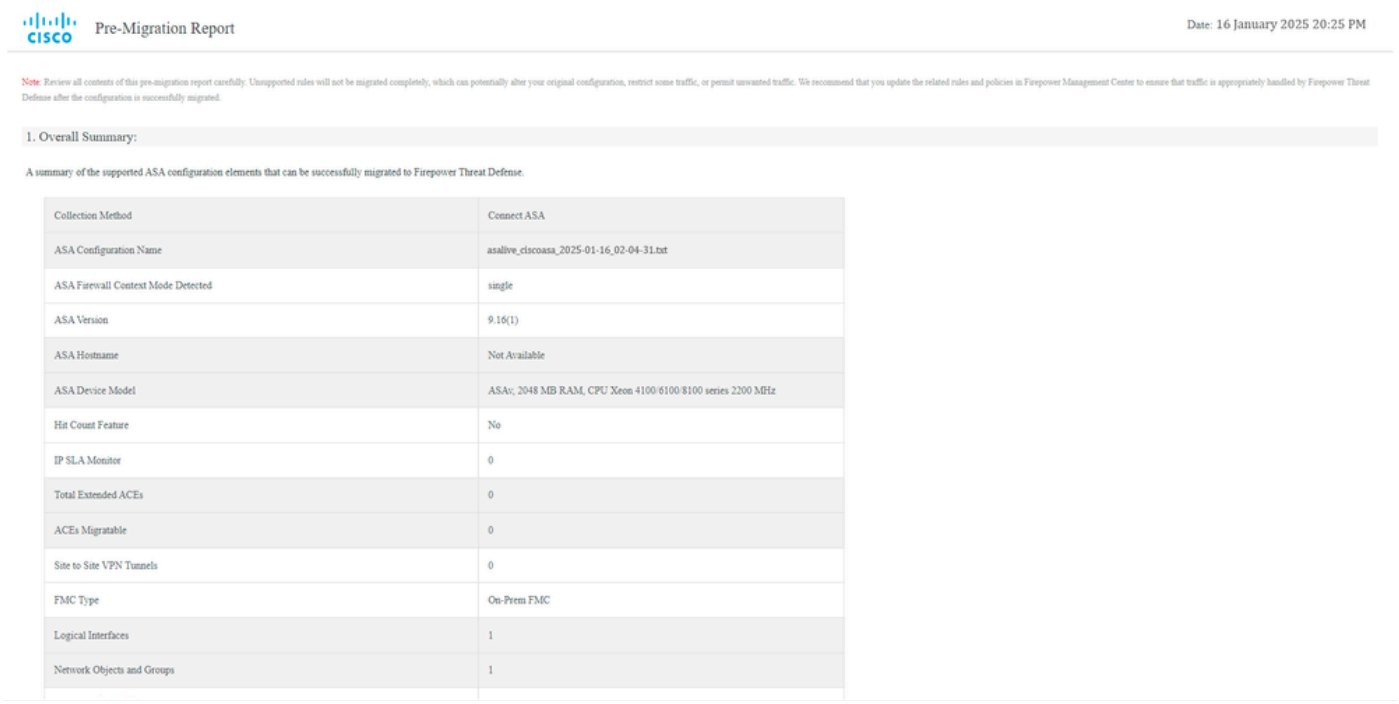
Iniciar conversão

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.



Download do relatório

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



Pre-Migration Report

Date: 16 January 2025 20:25 PM

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

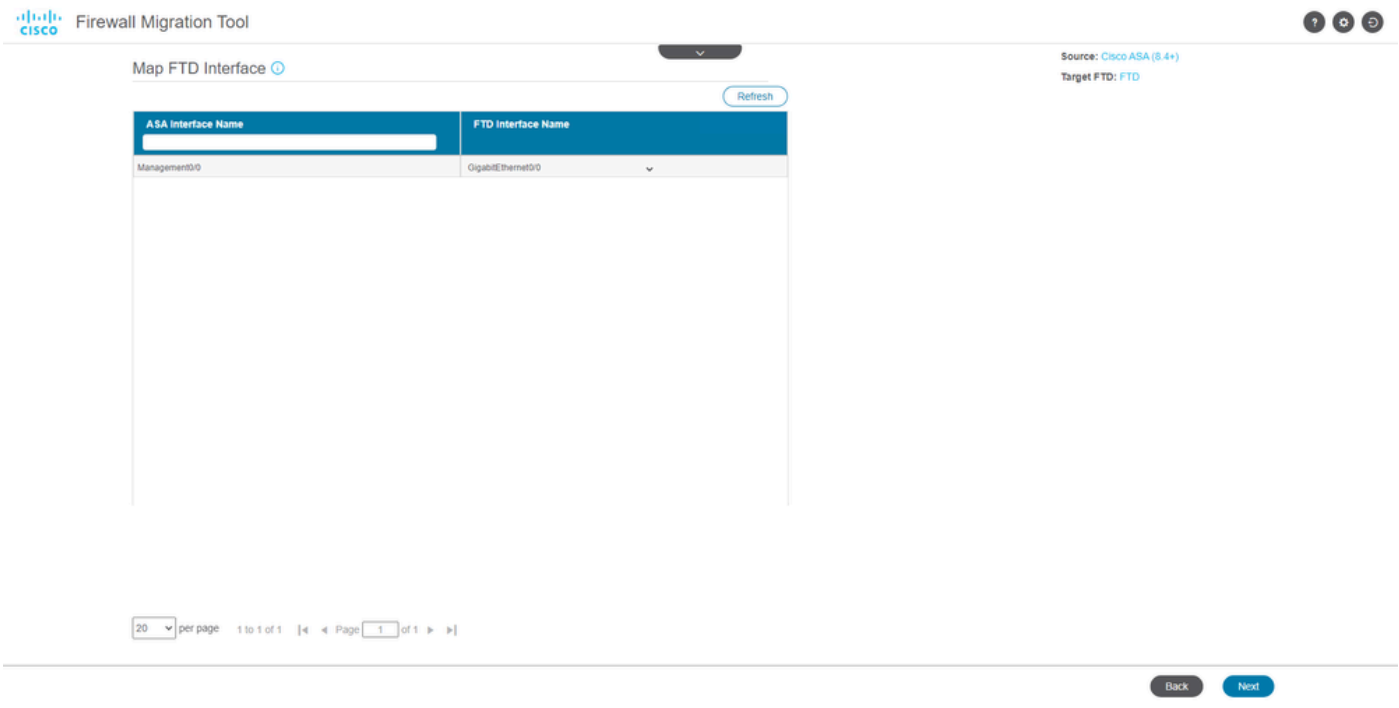
1. Overall Summary:

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

Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_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	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

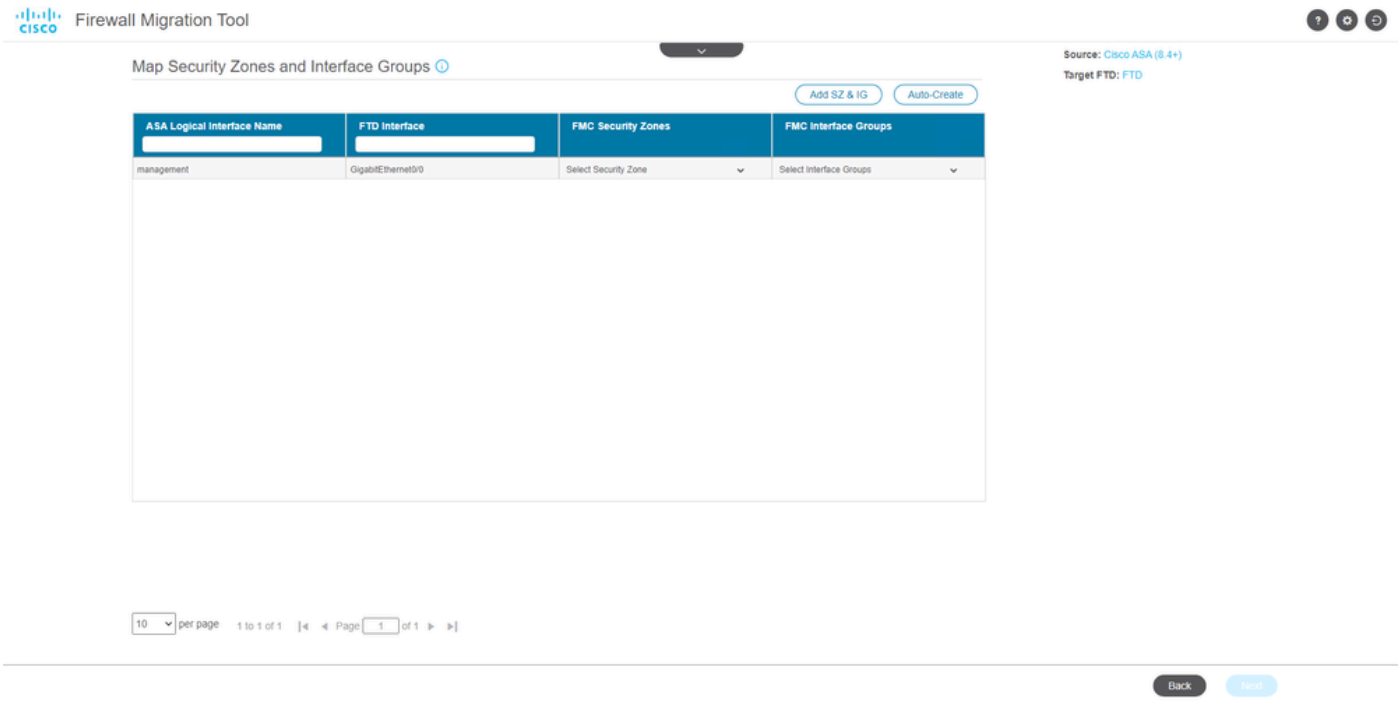
Relatório de pré-migração

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



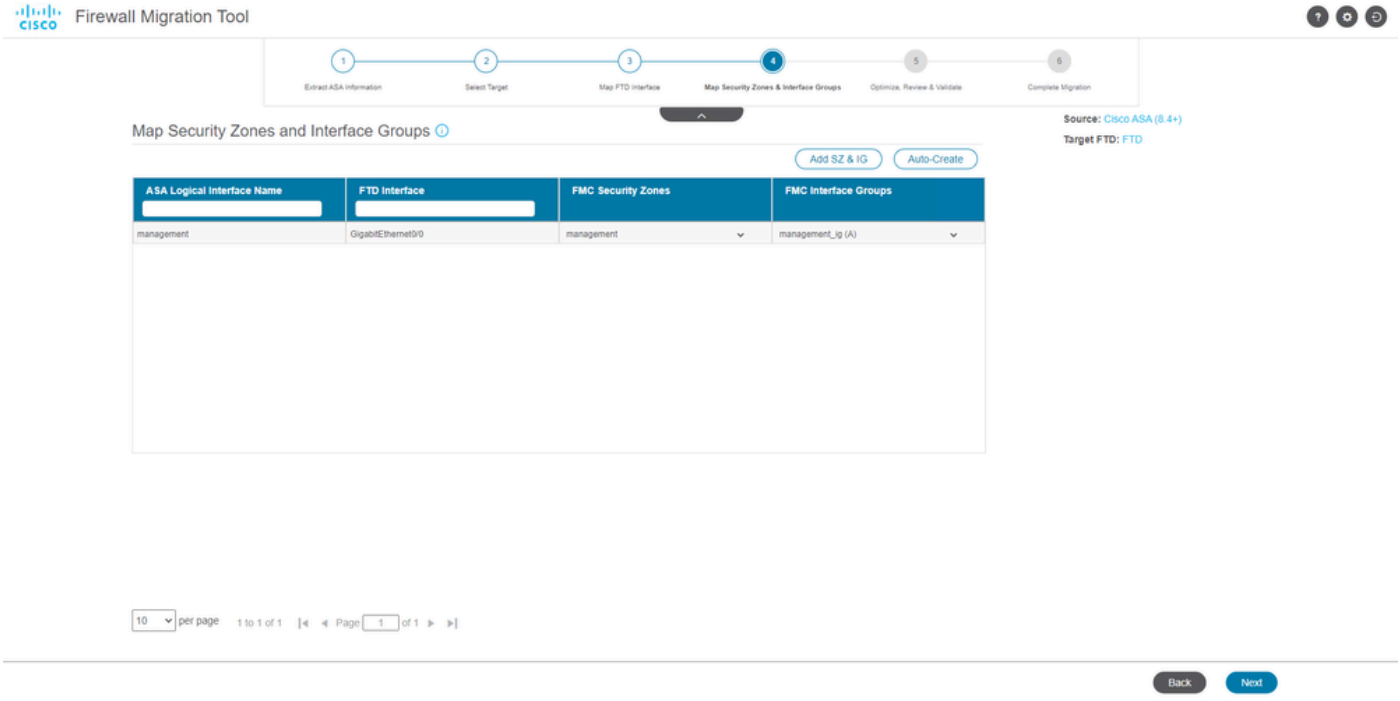
Mapear interfaces

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



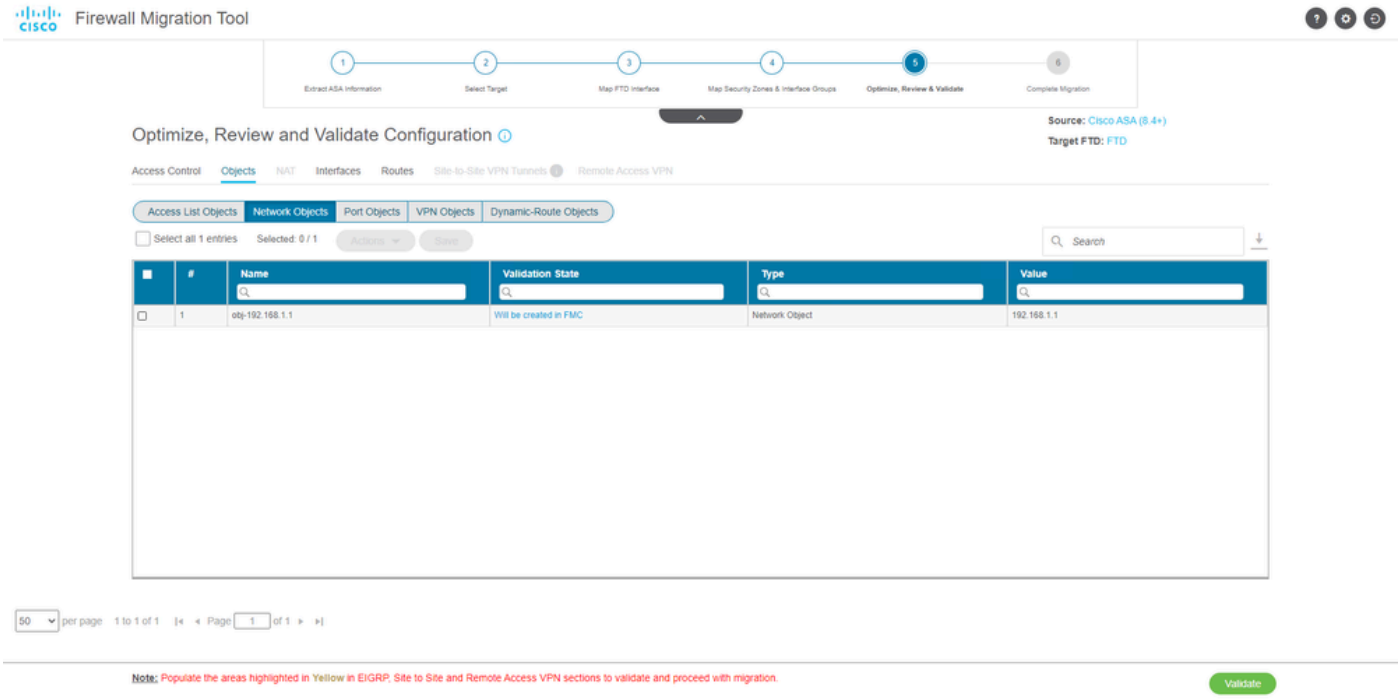
Zonas de segurança e grupos de interface

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



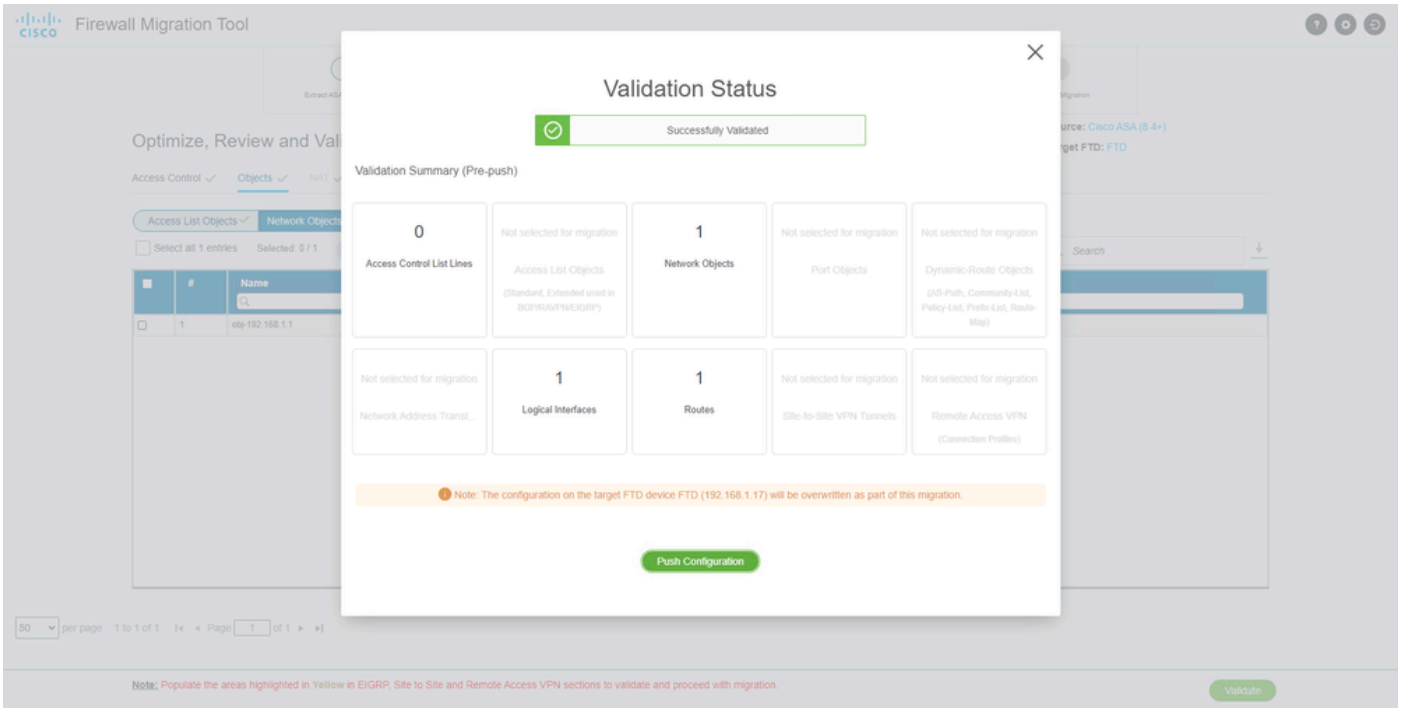
ferramenta Criação Automática

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 emValidate.



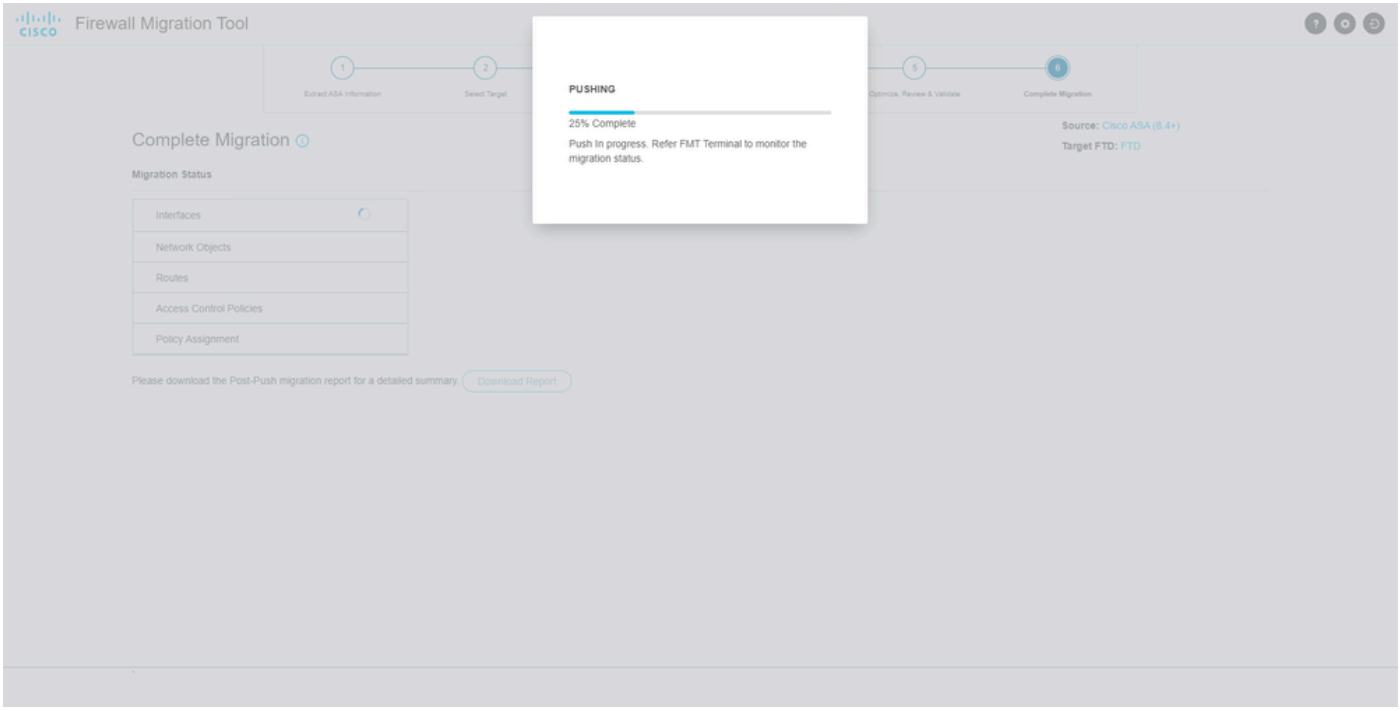
Revisar e validar

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



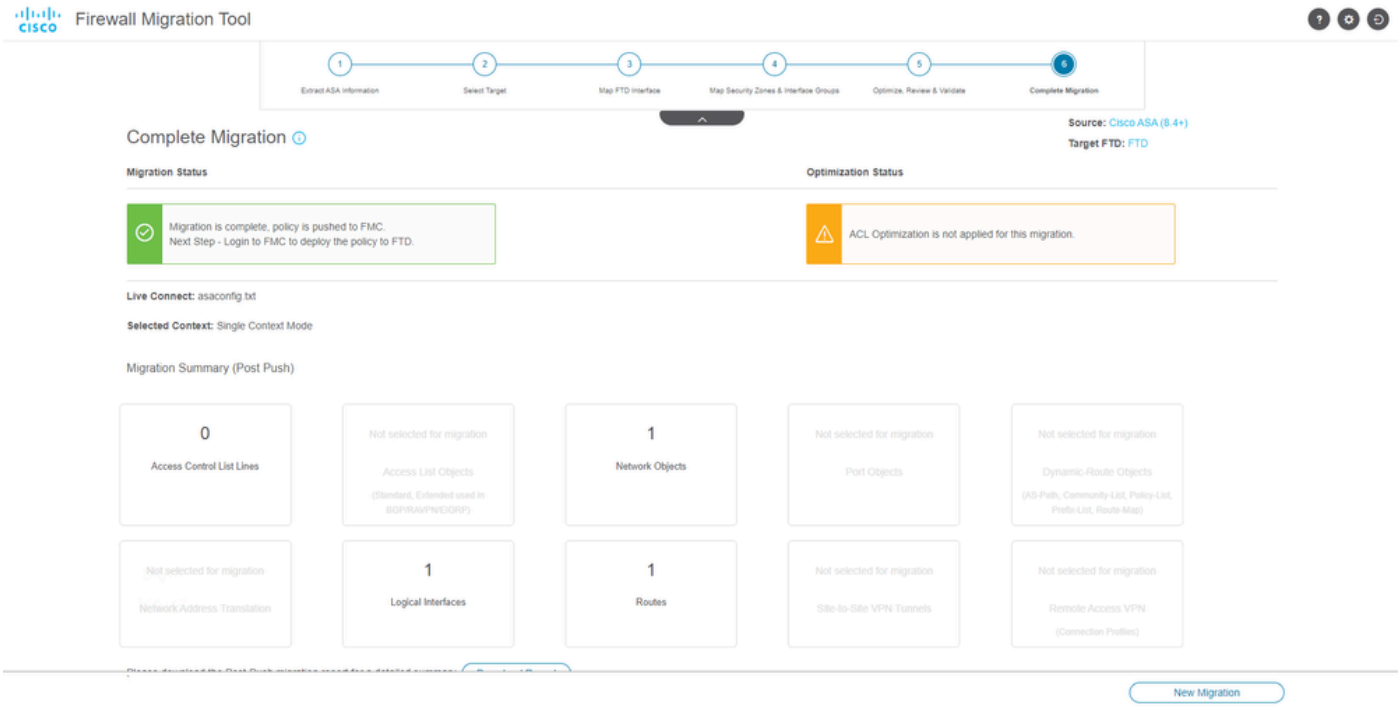
Validação

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:
- Uso do pacote de suporte para solução de problemas:
    - 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.