Migre do Paloalto para o Firepower Threat Defense usando o FMT

Contents

Introdução

Este documento descreve o procedimento para migrar o Palalto Firewall para o Dispositivo de ameaça do Cisco Firepower .

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta de migração do Firepower
- Firewall Paloalto
- Defesa contra ameaças de firewall (FTD) segura
- Cisco Secure Firewall Management Center (FMC)

Componentes Utilizados

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

- Mac OS com Firepower Migration Tool (FMT) v7.7
- PAN NGFW versão 8.0+
- Centro de gerenciamento seguro de firewall (FMCv) v7.6
- Secure Firewall Threat Defense versão 7.4.2

Ressalva: As redes e os endereços IP mencionados neste documento não estão associados a nenhum usuário, grupo ou organização individual. Essa configuração foi criada exclusivamente para uso em um ambiente de laboratório.

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:

- PAN NGFW 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-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8,0+)

Informações de Apoio

Antes de migrar sua configuração do Palo Alto Firewall, execute estas atividades:

Obter o arquivo zip de configuração do Palalto Firewall

- O Paloalto Firewall deve ser da versão 8.4+.
- Exporte a configuração atual em execução do firewall Palo Alto (*.xml deve estar no formato xml).
- Faça login no Paloalto Firewall Cli para executar show routing route e salvar a saída no formato txt (*.txt).
- Compacte o arquivo de configuração atual (*.xml) e o arquivo de roteamento (*.txt) com a extensão *.zip.

Lista de verificação pré-migração

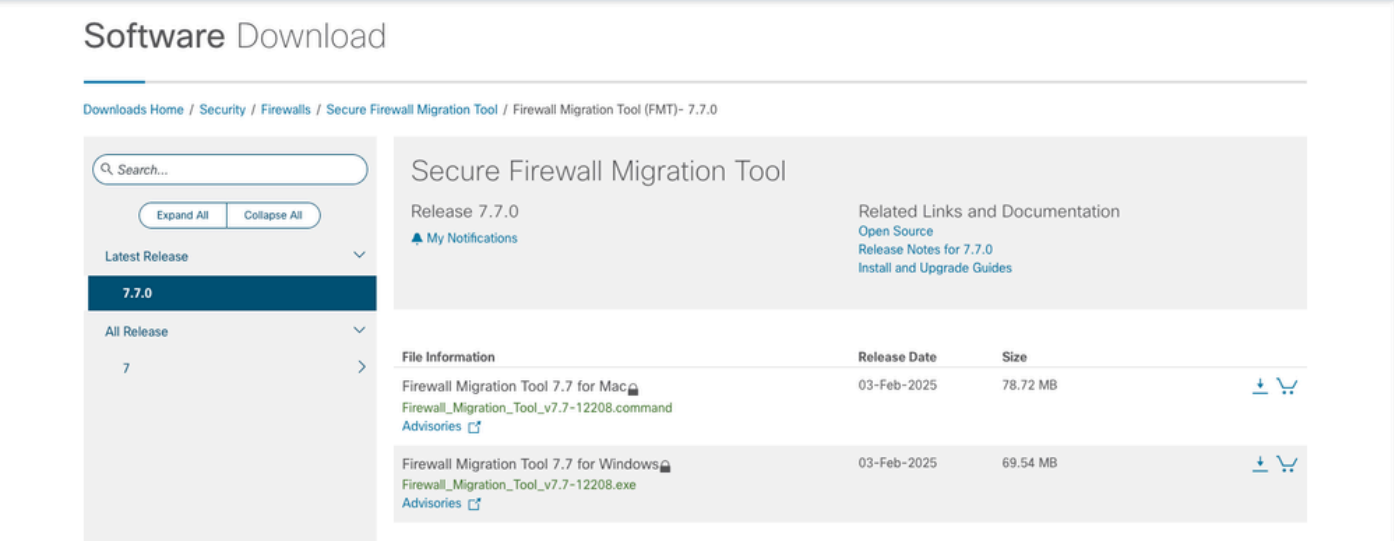
- Verificar se o FTD foi registrado no FMC antes de iniciar o processo de migração.
- Foi criada no CVP uma nova conta de utilizador com privilégios administrativos. Ou as credenciais de administrador existentes podem ser usadas.

- O arquivo de configuração de execução .xml da Palo Alto exportado deve ser compactado com uma extensão .zip (siga o procedimento mencionado na seção anterior).
- O dispositivo Firepower deve ter o mesmo número ou mais de canais de porta ou de subinterface física ou secundária em comparação às interfaces do Palo Alto Firewall.

Configurar

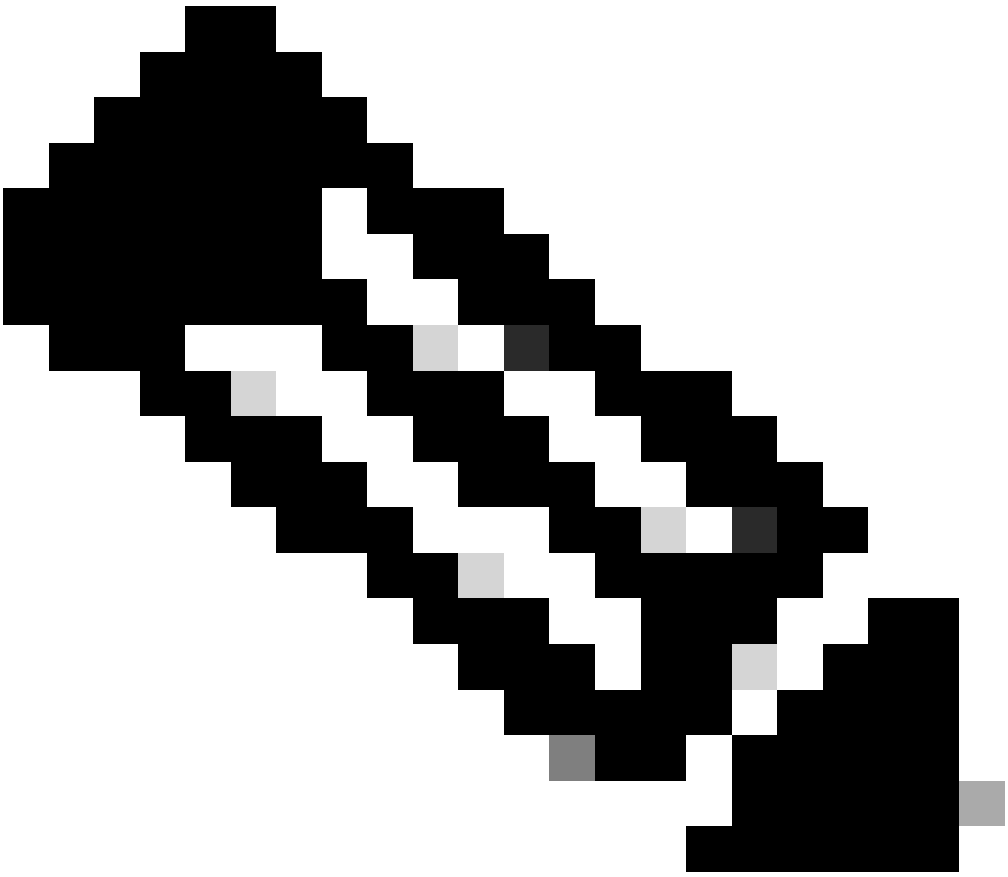
Etapas da migração

1. Faça download da ferramenta de migração mais recente do Firepower do Cisco Software Central que é compatível com o seu computador:



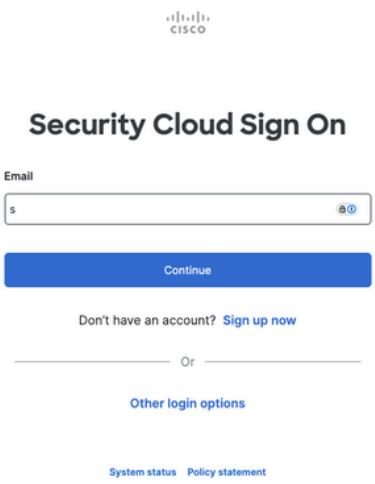
Download do FMT

3. Abra o arquivo baixado anteriormente no computador.



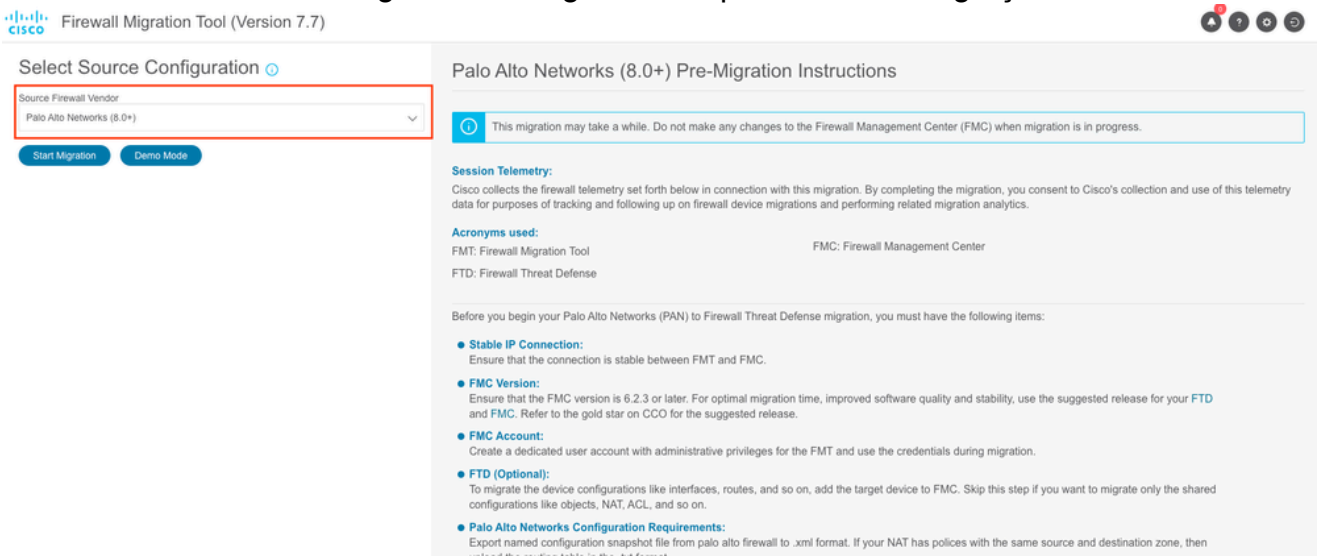
Note: O programa é aberto automaticamente e um console gera automaticamente o conteúdo no diretório onde você executou o arquivo.

4. Após 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.
5. Faça login usando credenciais CCO válidas para acessar a GUI do FMT.



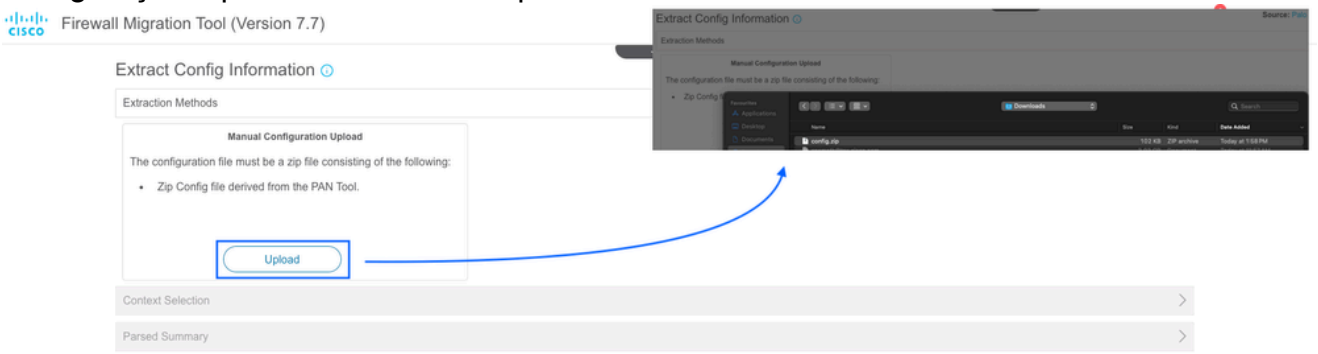
Prompt de login do FMT

6. Selecione o Firewall de origem a ser migrado e clique em Iniciar migração.



GUI FMT

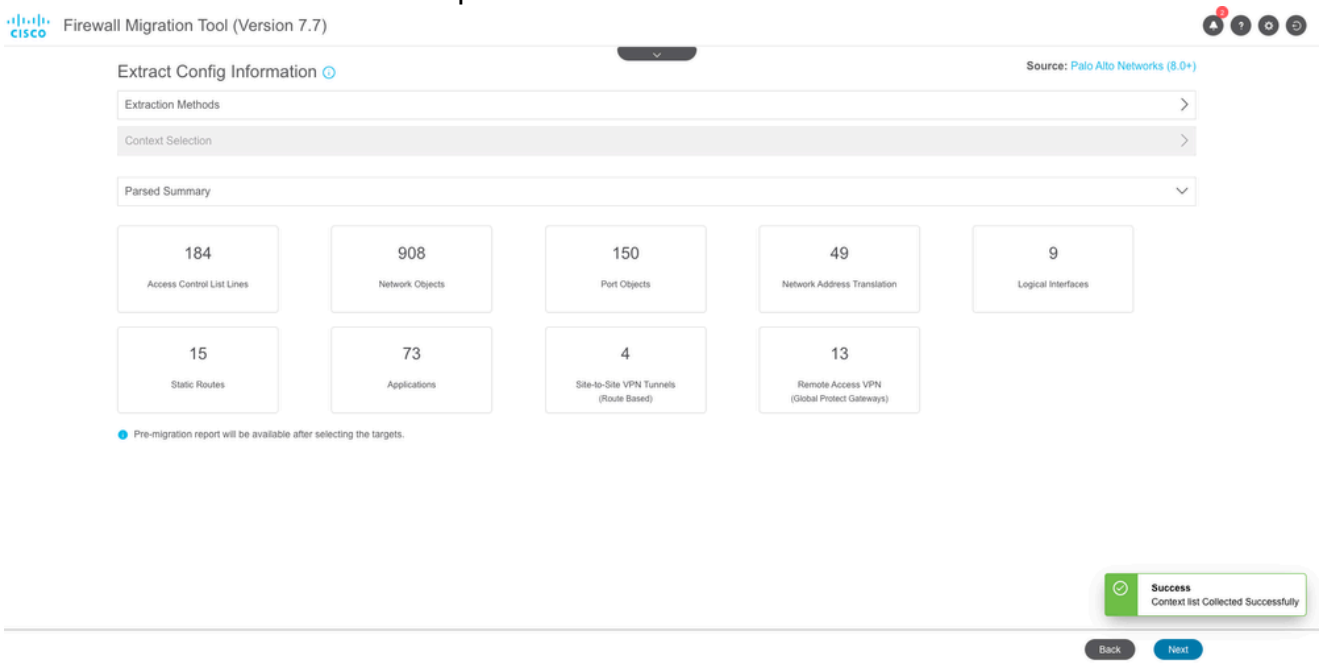
7. A seção Métodos de extração agora é exibida, onde você deve carregar o arquivo de configuração Zip do Palalto Firewall para o FMT.



Assistente de carregamento de configuração

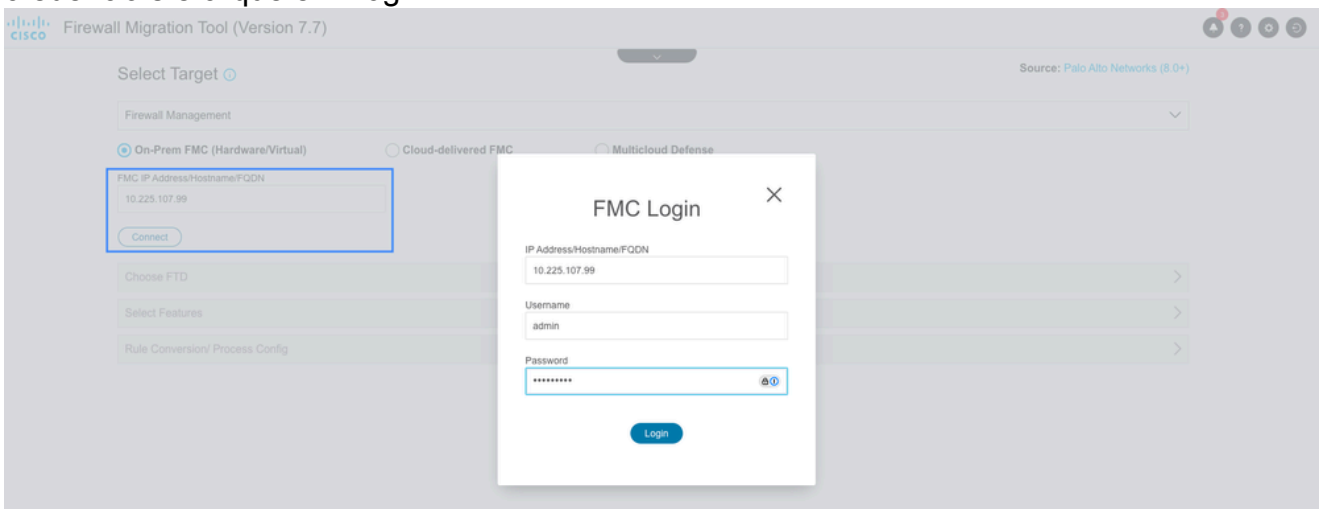
8. O resumo da configuração analisada é exibido depois que o arquivo de configuração é carregado. No caso de VSYS, seleções de VSYS separadas estão disponíveis. Cada um

deles deve ser analisado e migrado um após o outro.
Valide o resumo analisado e clique no ícone Próximo.



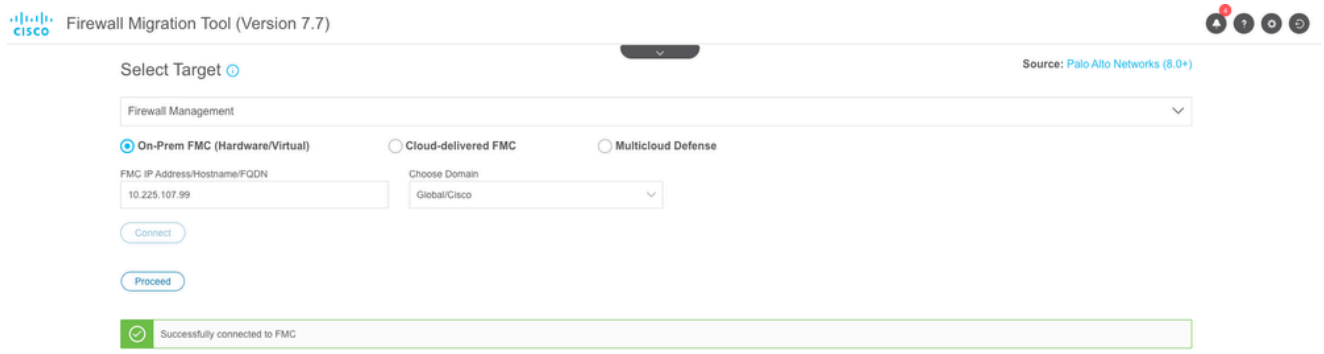
Resumo da validação da configuração

9. Você pode escolher o tipo de FMC nesta seção. Forneça o endereço IP de gerenciamento e clique em Connect.
   Um pop-up é exibido solicitando o fornecimento de credenciais do FMC. Insira as credenciais e clique em Login.



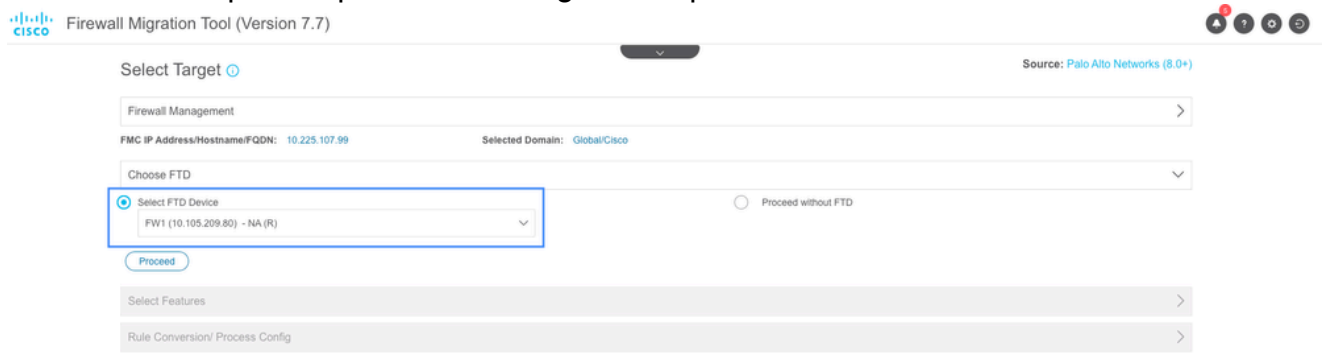
Login no FMC

10. Após se conectar ao FMC com êxito, você pode escolher o Domínio (se houver) e clicar em Continuar.



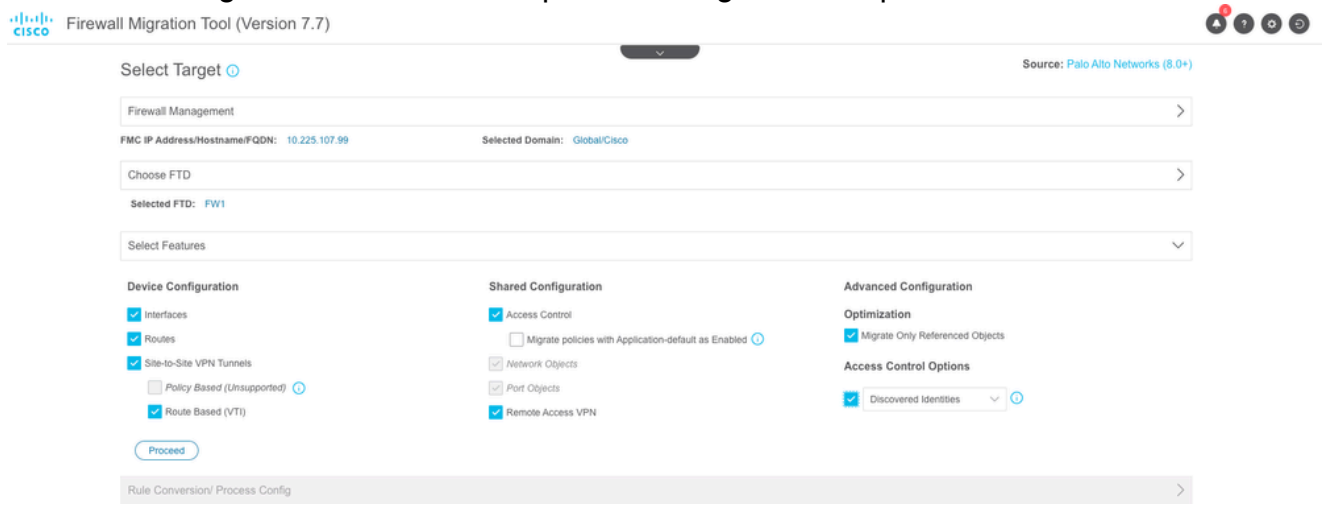
Seleção de domínio

11. Escolha o FTD para o qual você vai migrar e clique em Continuar.



Selecionar FTD de Destino

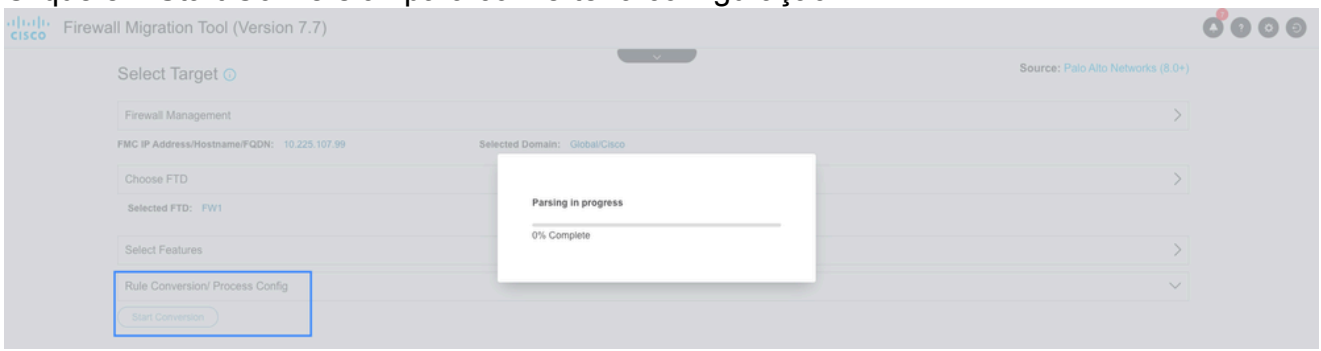
12. A ferramenta agora lista os recursos que serão migrados. Clique em Continuar.



Seleção de recursos

Note: Todos os recursos são selecionados por padrão. Você pode desmarcar qualquer configuração que não deva ser migrada.

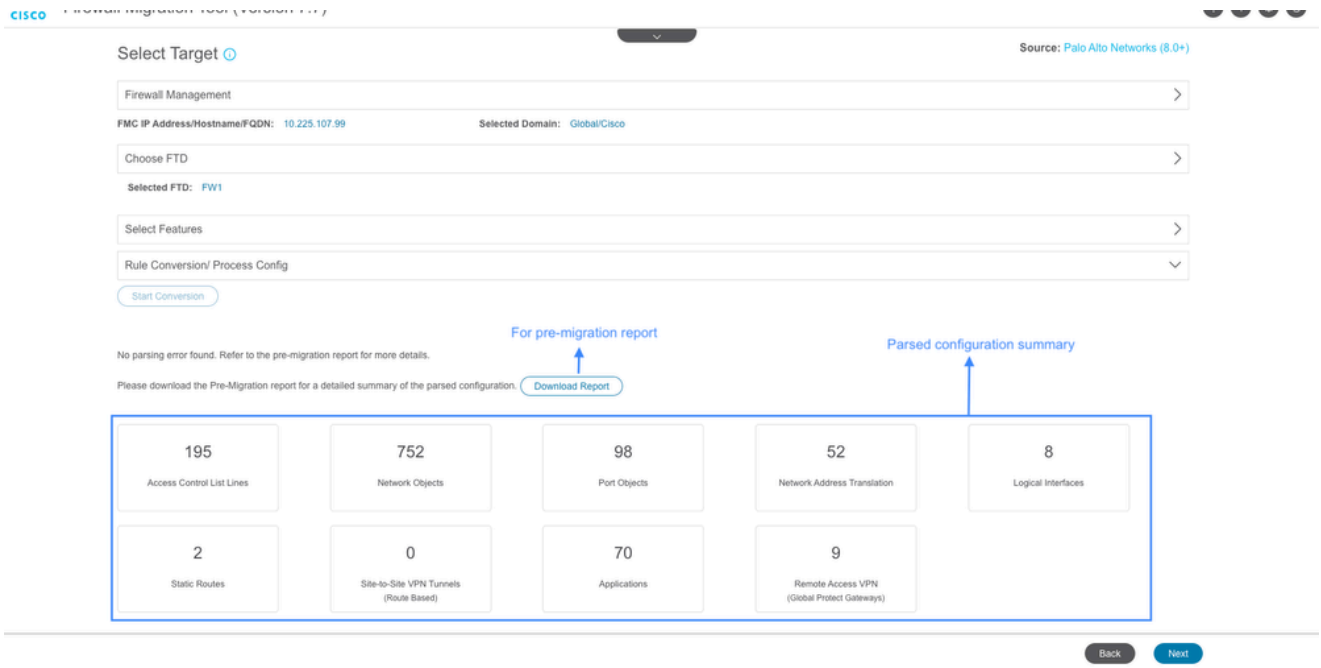
13. Clique em Start Conversion para converter a configuração.



Configuração de análise

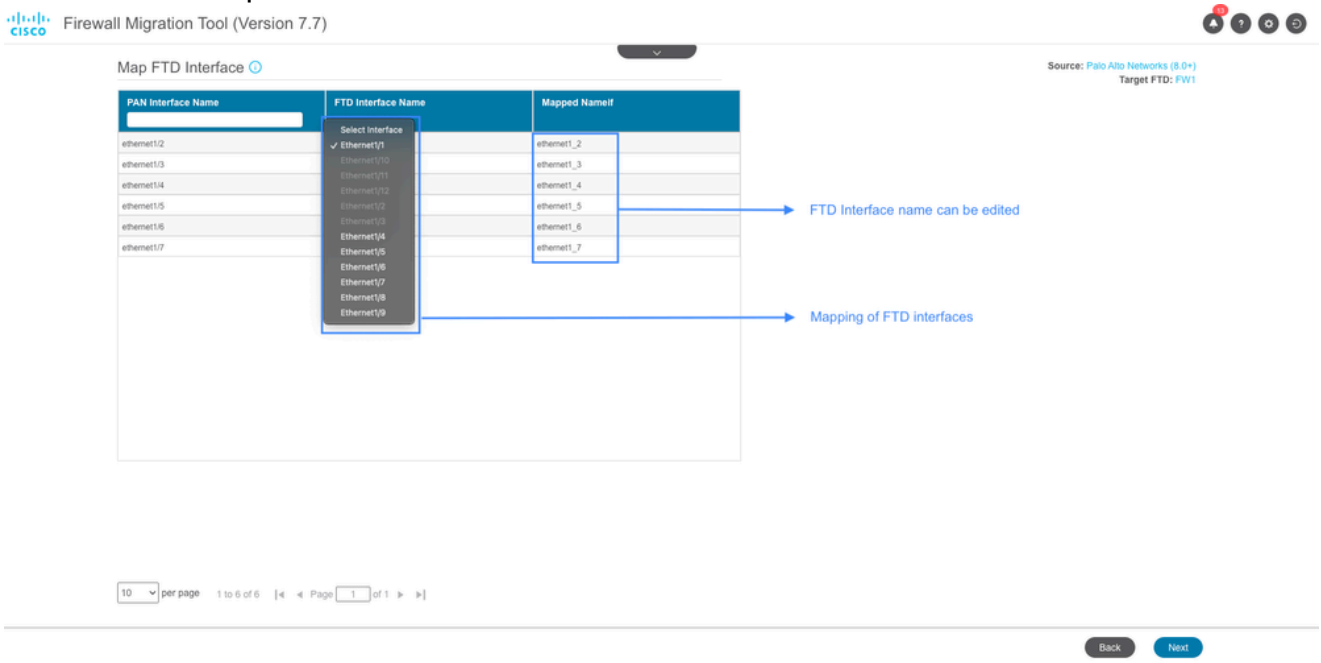
A ferramenta analisa a configuração e exibe o resumo da conversão como mostrado na imagem. Você também pode fazer download do Relatório de pré-migração para validar a configuração migrada para quaisquer Erros ou Avisos, se houver. Navegue até a próxima

página clicando em Avançar.



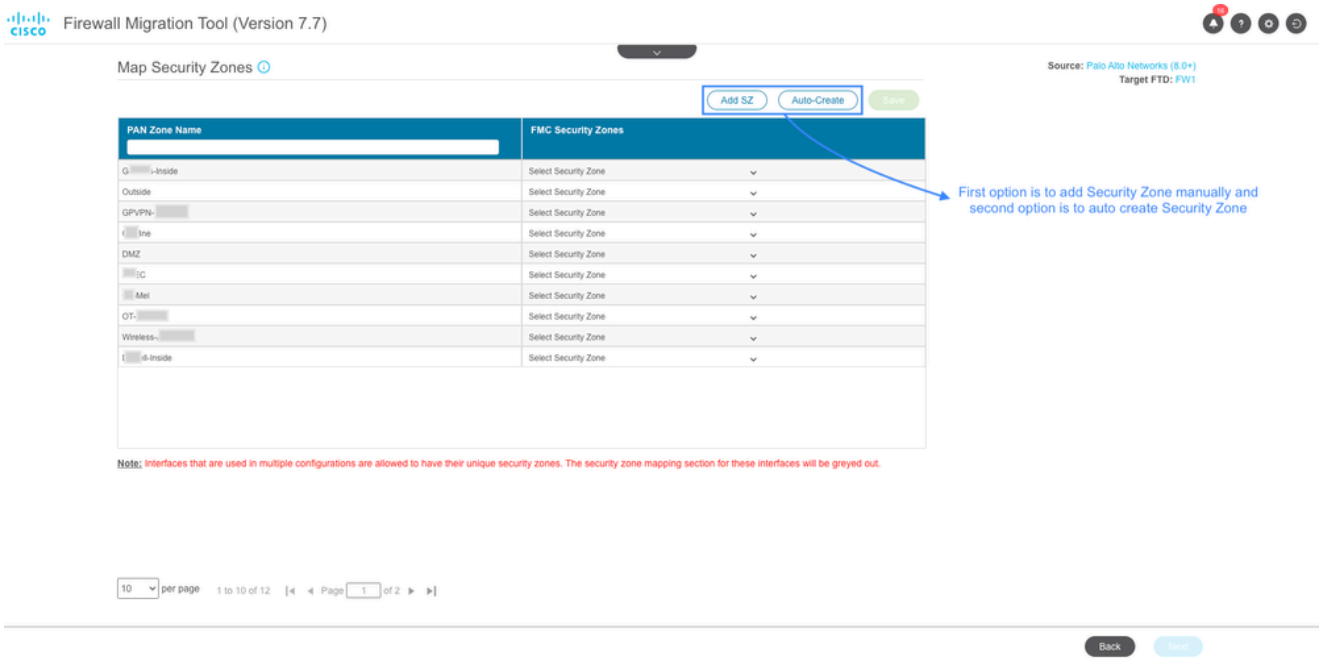
Resumo da configuração analisada

14. Você pode definir o mapeamento de interface do Paloalto para o FTD, bem como editar o nome de cada interface na seção Mapeamento de interface. Clique em Avançar após a conclusão do Mapeamento de interface.



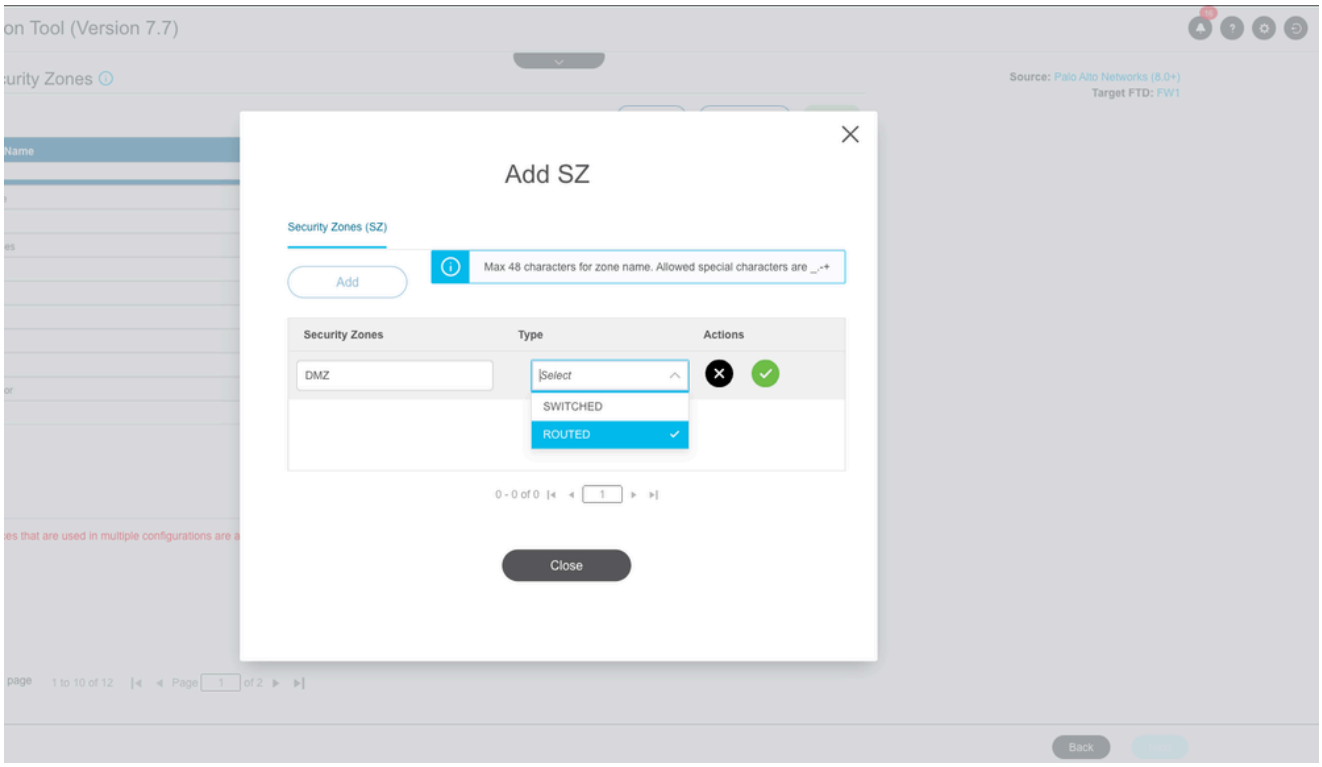
Mapeamento de interfaces

15. Você pode Adicionar a zona de segurança manualmente para cada interface ou Criá-la automaticamente na seção Mapear a zona de segurança . Clique em Próximo após criar e mapear Zonas de Segurança.



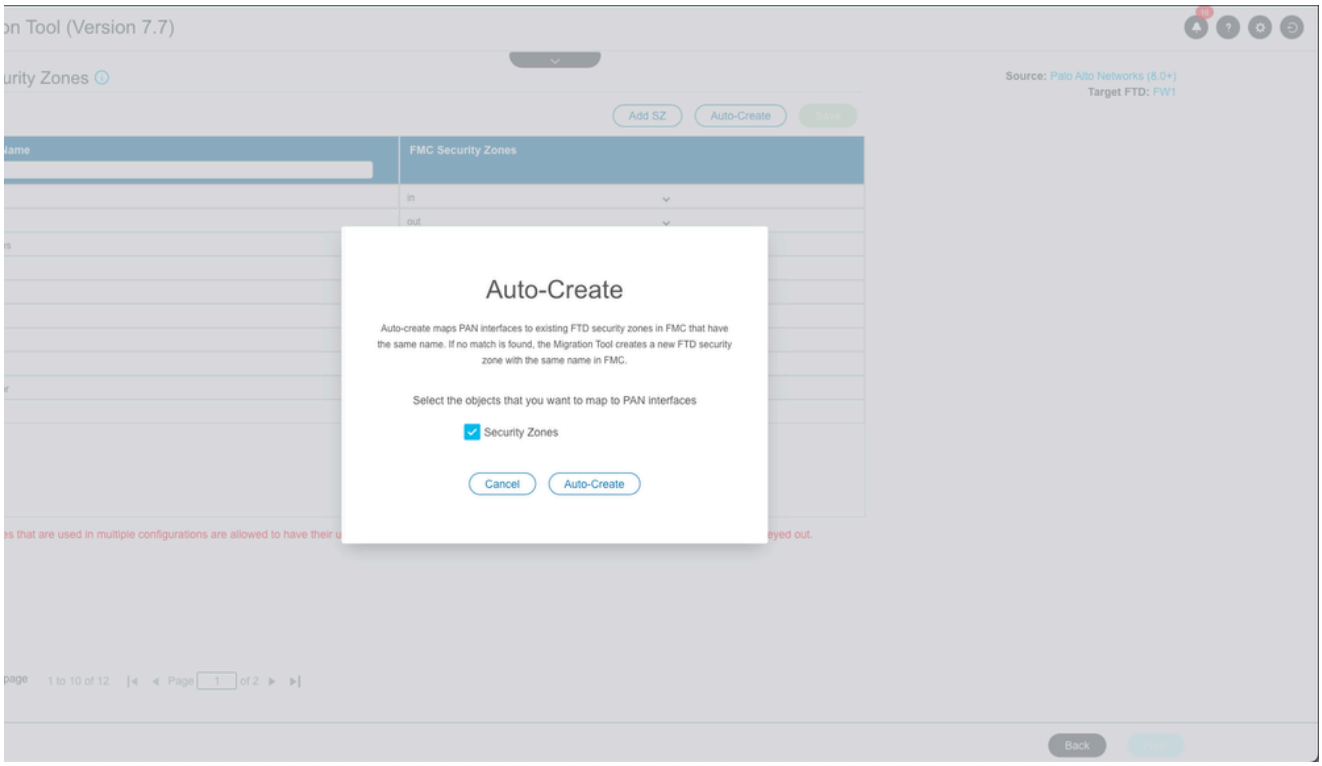
Criação de zona de segurança

Criação manual de zonas de segurança:



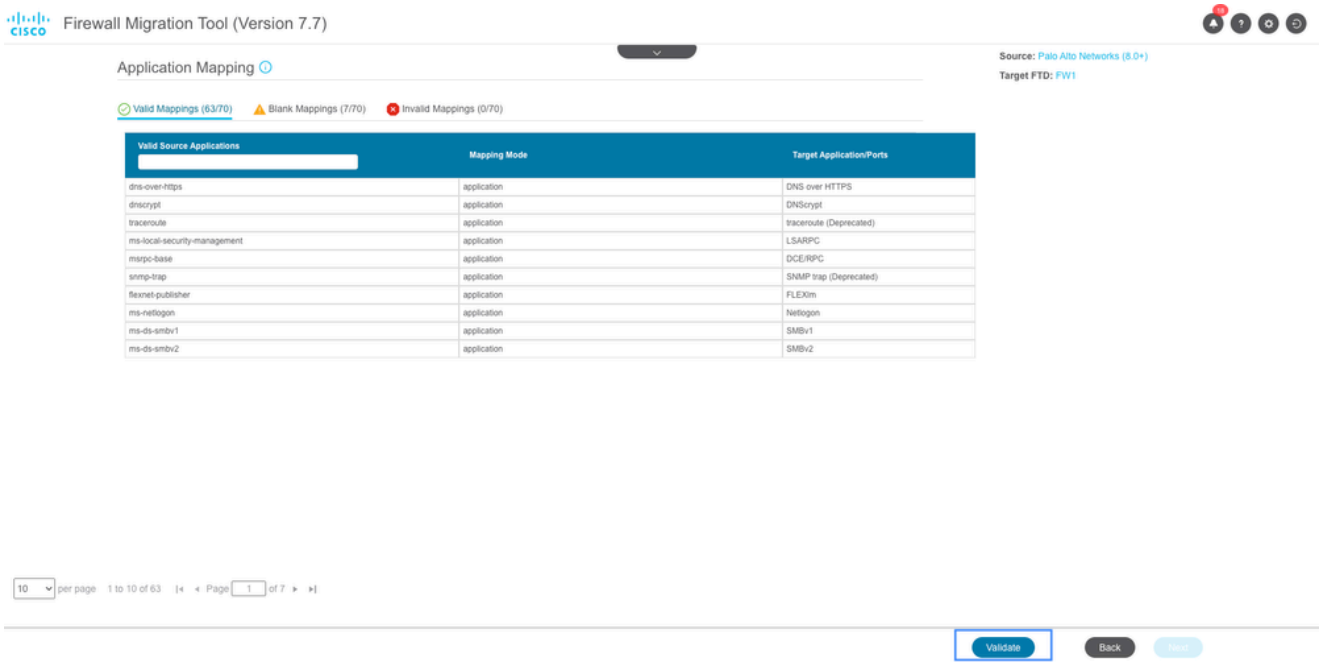
Criação manual de zona de segurança

Criar zonas de segurança automaticamente:

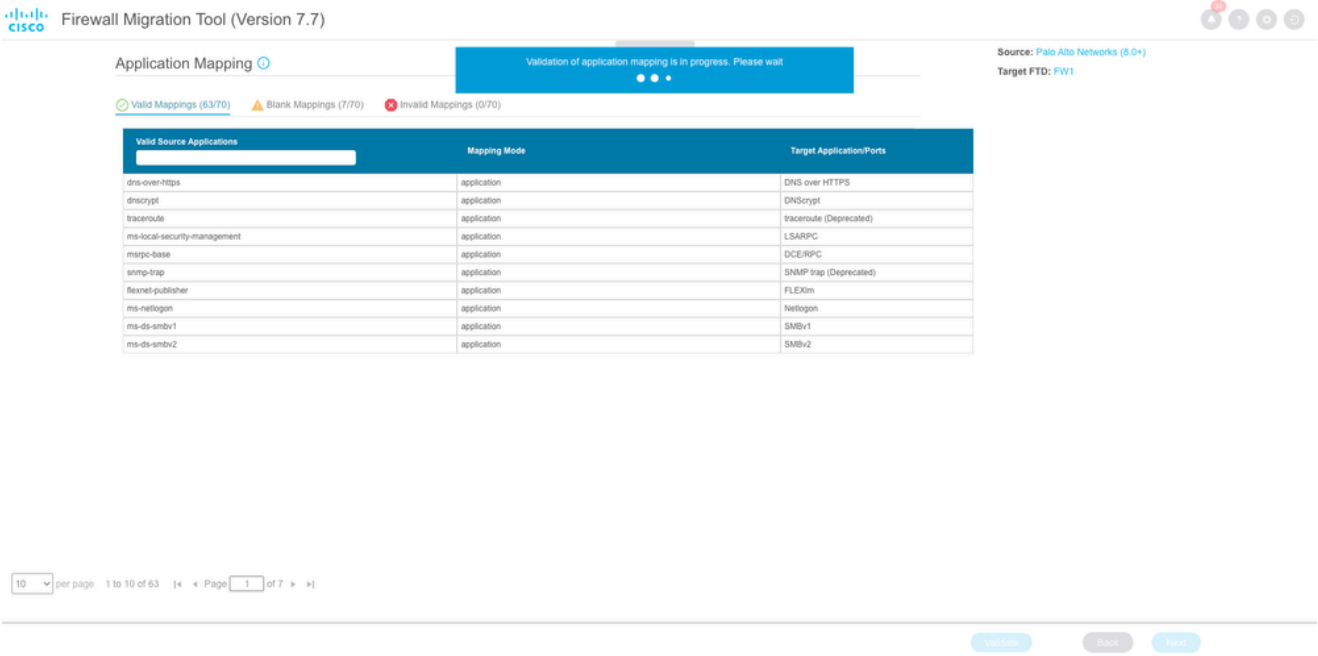


Criação Automática de Zona de Segurança

16. Agora você pode prosseguir para a seção Mapeamento de Aplicativos. Clique no botão Validar para validar o mapeamento do aplicativo.



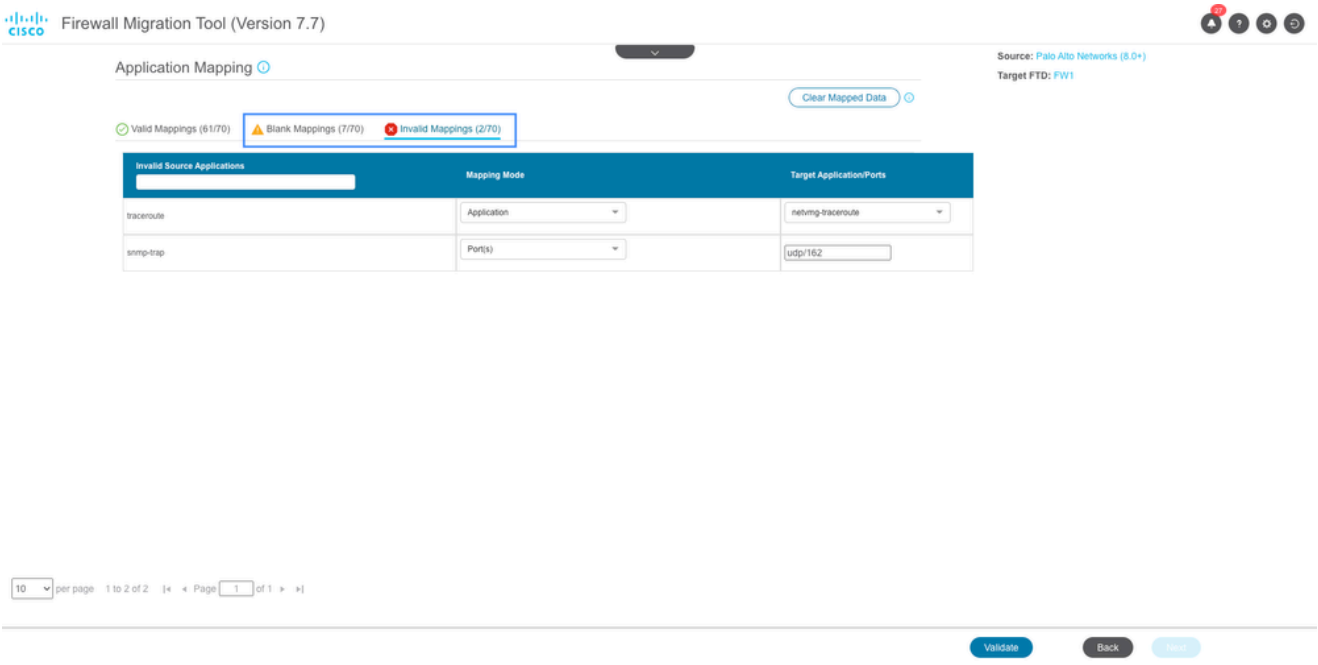
Mapeamento de aplicativos



Validação do mapeamento de aplicativos

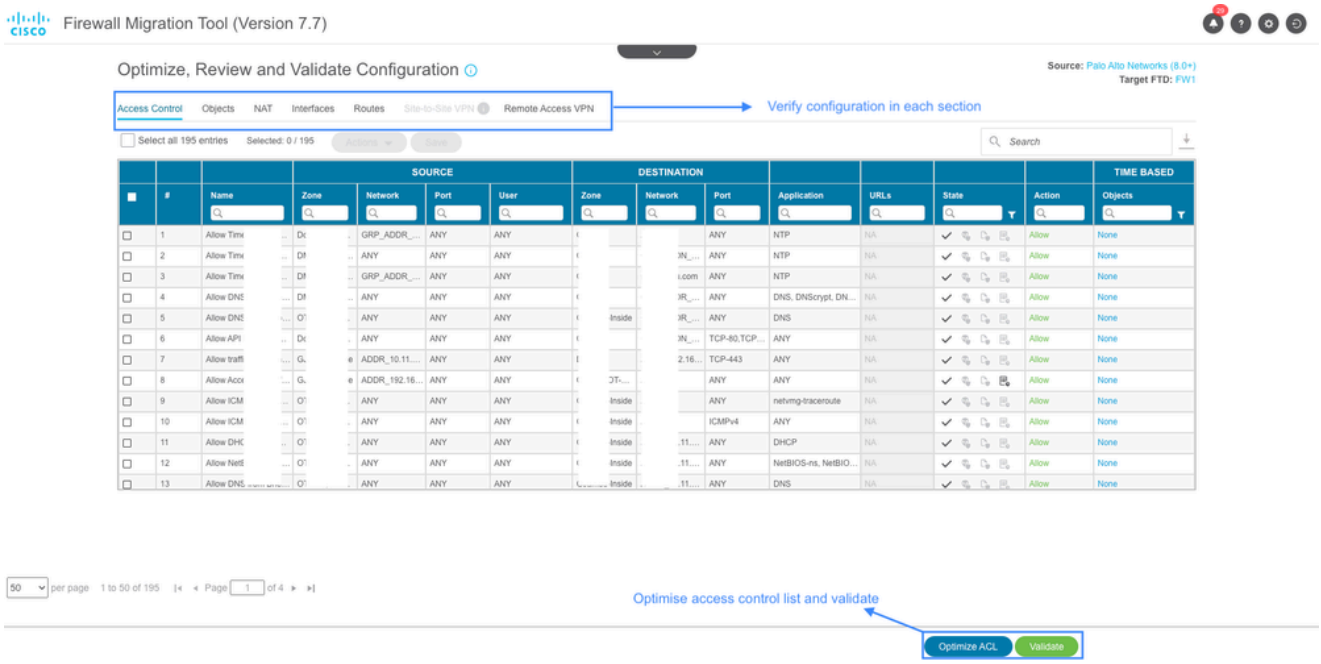
Após a validação, o FMT lista os Mapeamentos em Branco e inválidos. Mapeamentos inválidos devem ser corrigidos antes de continuar e a correção de mapeamentos em branco é opcional.

Clique em Validar novamente para validar os mapeamentos corrigidos. Clique em Avançar após a validação ser bem-sucedida.



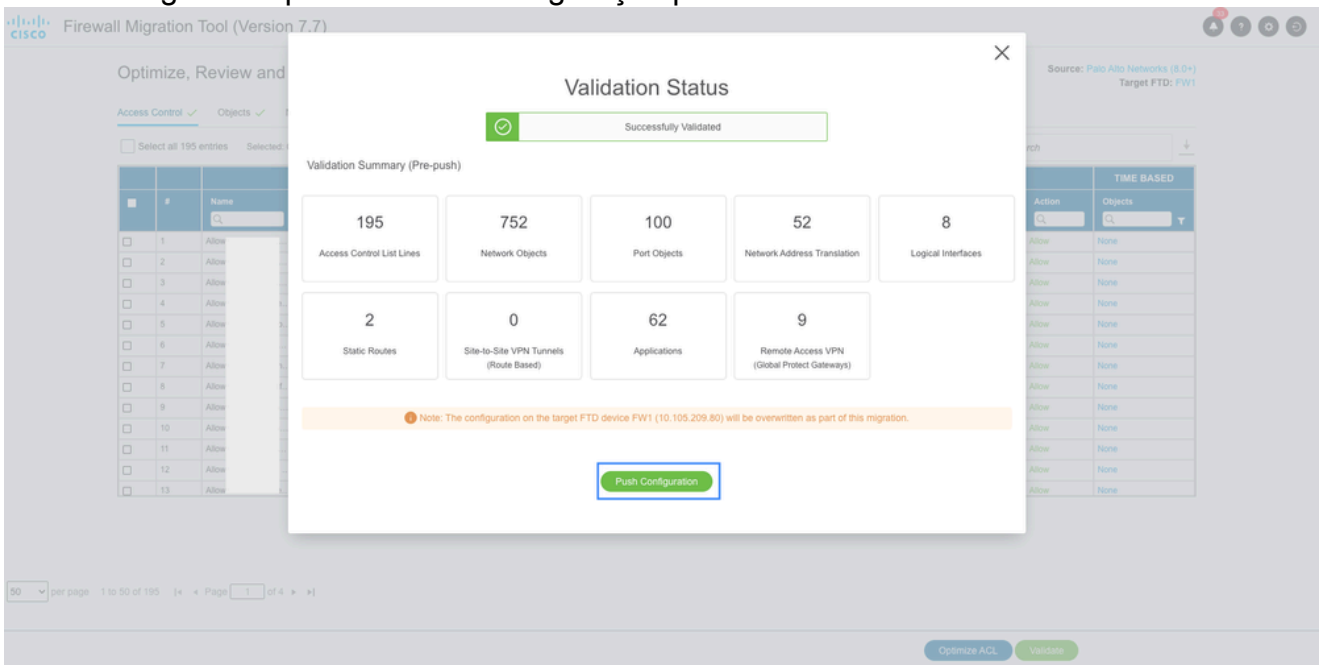
Mapeamento de aplicativos em branco e inválido

17. A ACL pode ser otimizada na próxima seção, se necessário. Revise a configuração em cada seção, como Controle de acesso, Objetos, NAT, Interfaces, Rotas e VPN de acesso remoto. Clique em Validate após examinar as configurações.



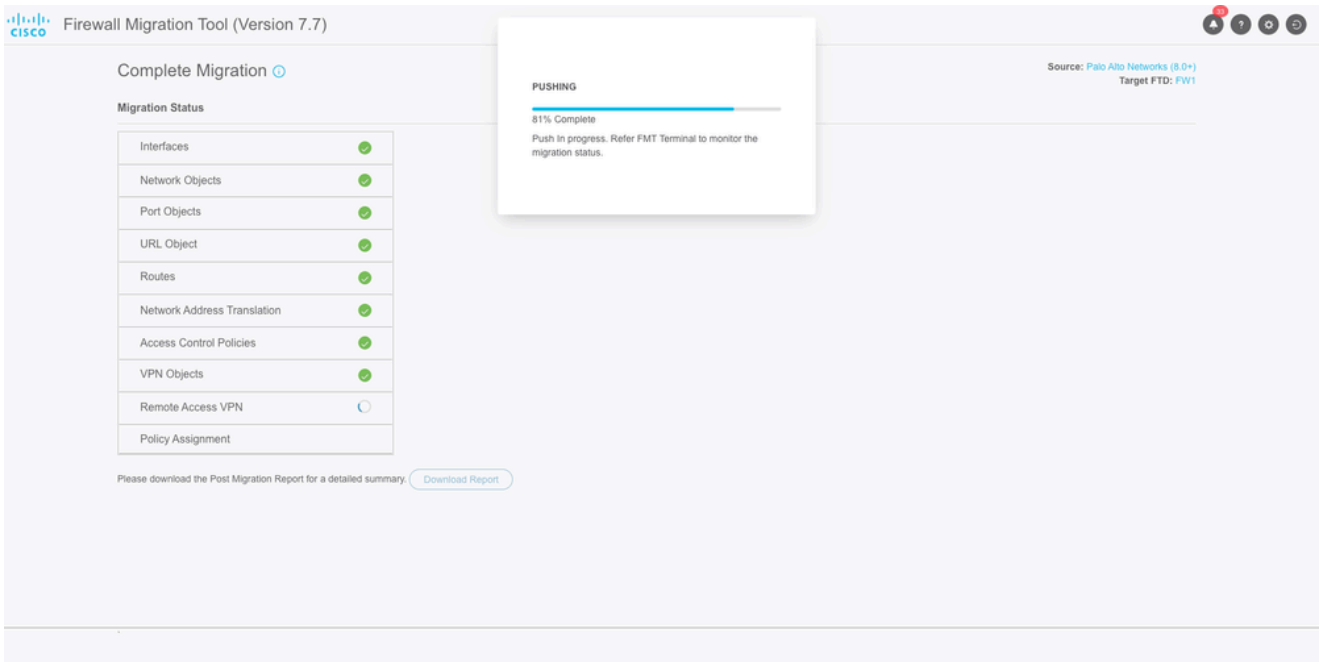
Validação da configuração

18. Um resumo de validação é exibido após a validação ser concluída com êxito. Clique em Push Configuration para enviar a configuração para o FMC de destino.



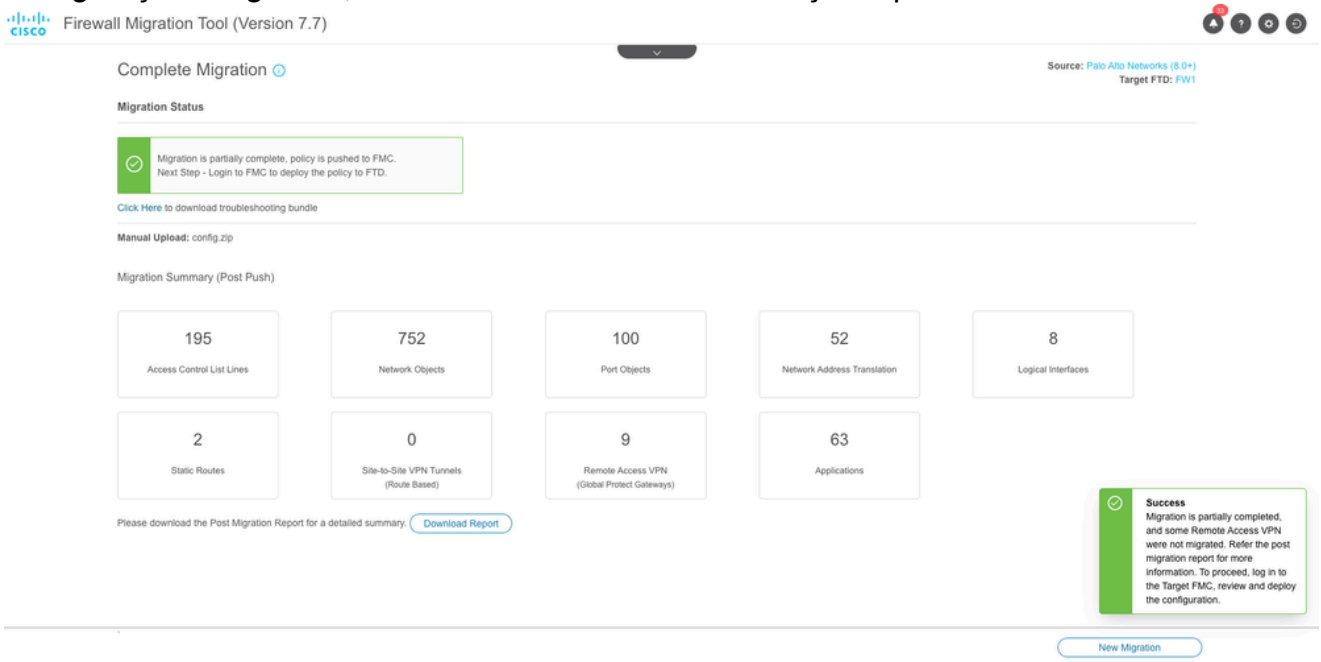
Resumo da validação da configuração

19. O progresso do envio da configuração para o FMC agora está visível na seção Status da migração. Você também pode usar a janela do terminal FMT para monitorar o status da migração.



Status da migração

20. Um Resumo da migração é exibido pela ferramenta quando a migração é bem-sucedida. Ele também lista as configurações parcialmente migradas, se houver. Por exemplo, configuração de VPN de acesso remoto neste cenário devido à ausência do Pacote de Cliente Seguro.
    Você também pode fazer o download do Relatório de pós-migração para revisar as configurações migradas, bem como se há erros ou correções que devem ser feitas.



Resumo da migração bem-sucedida

21. A última etapa é revisar a configuração migrada do FMC e implantar a configuração no FTD. Para implantar a configuração:
    1. Faça login na GUI do FMC.
    2. Navegue até a guia Implantar.
    3. Selecione a implantação para enviar a configuração para o firewall.

4. Clique em Implantar.

Troubleshooting

Solução de problemas da ferramenta Secure Firewall Migration

Falhas comuns de migração:

- Caracteres desconhecidos ou inválidos no arquivo de configuração do PaloAlto.
- Elementos de configuração ausentes ou incompletos.
- Problemas de conectividade de rede ou latência.
- Problemas durante o upload do arquivo de configuração da PaloAlto ou durante o envio da configuração para o FMC.

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.

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.