

Migre do Paloalto para o Firepower Threat Defense usando o FMT

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Informações de Apoio](#)

[Obter o arquivo zip de configuração do Paloalto Firewall](#)

[Lista de verificação pré-migração](#)

[Configurar](#)

[Etapas da migração](#)

[Troubleshooting](#)

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

[Falhas comuns de migração:](#)

[Uso do pacote de suporte para solução de problemas:](#)

Introdução

Este documento descreve o procedimento para migrar o Paloalto 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 Palo Alto 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:

Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.7.0

[Expand All](#) [Collapse All](#)
Latest Release
7.7.0
All Release
7

Secure Firewall Migration Tool

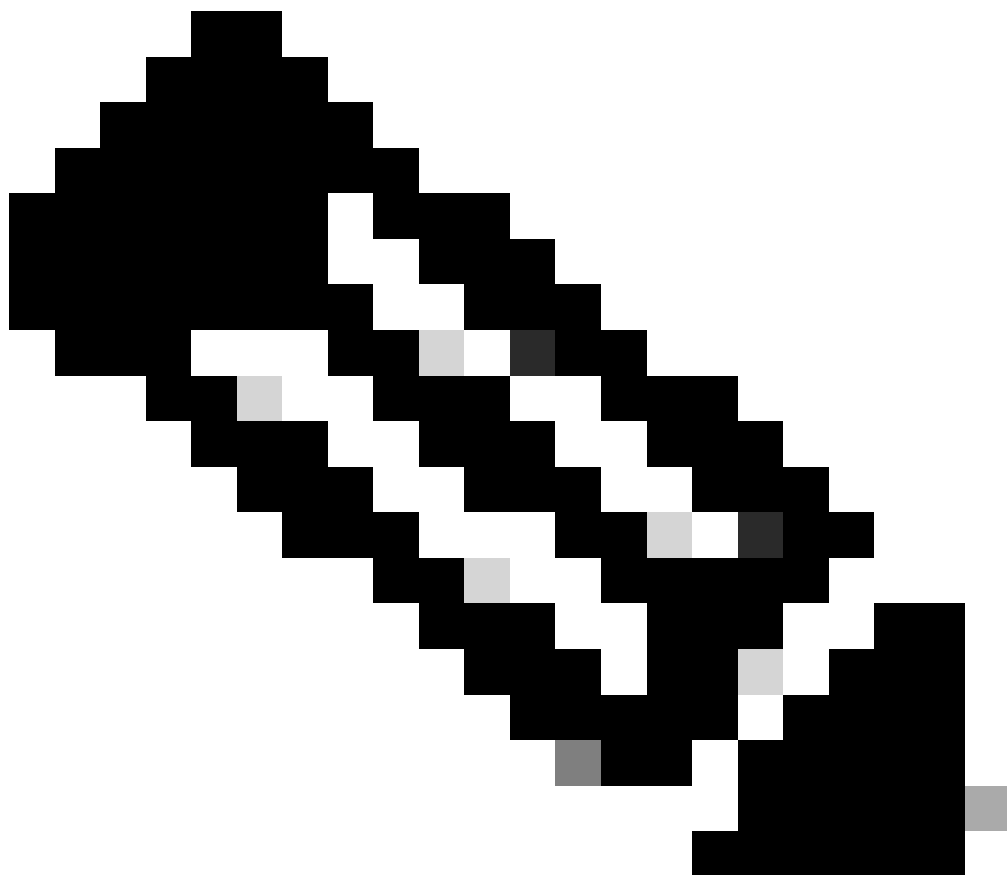
Release 7.7.0
[▲ My Notifications](#)

Related Links and Documentation
[Open Source](#)
[Release Notes for 7.7.0](#)
[Install and Upgrade Guides](#)

File Information	Release Date	Size	
Firewall Migration Tool 7.7 for Mac Firewall_Migration_Tool_v7.7-12208.command Advisories	03-Feb-2025	78.72 MB	↓ 🛒
Firewall Migration Tool 7.7 for Windows Firewall_Migration_Tool_v7.7-12208.exe Advisories	03-Feb-2025	69.54 MB	↓ 🛒

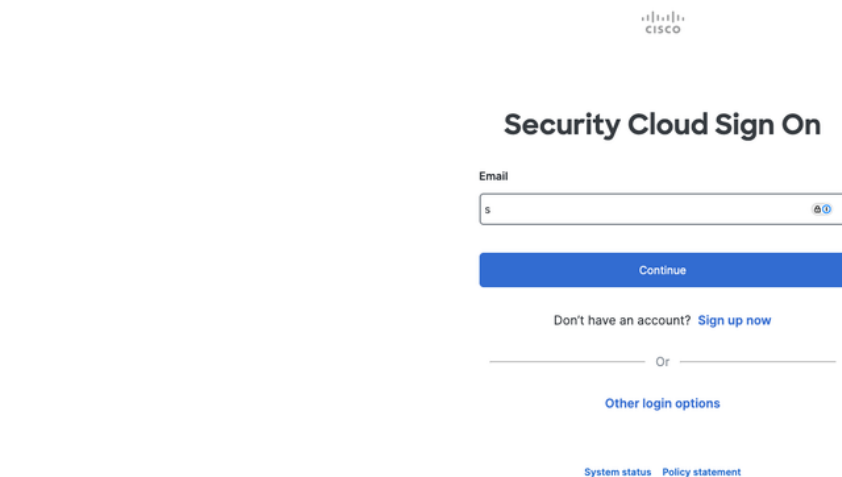
Download do FMT

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.

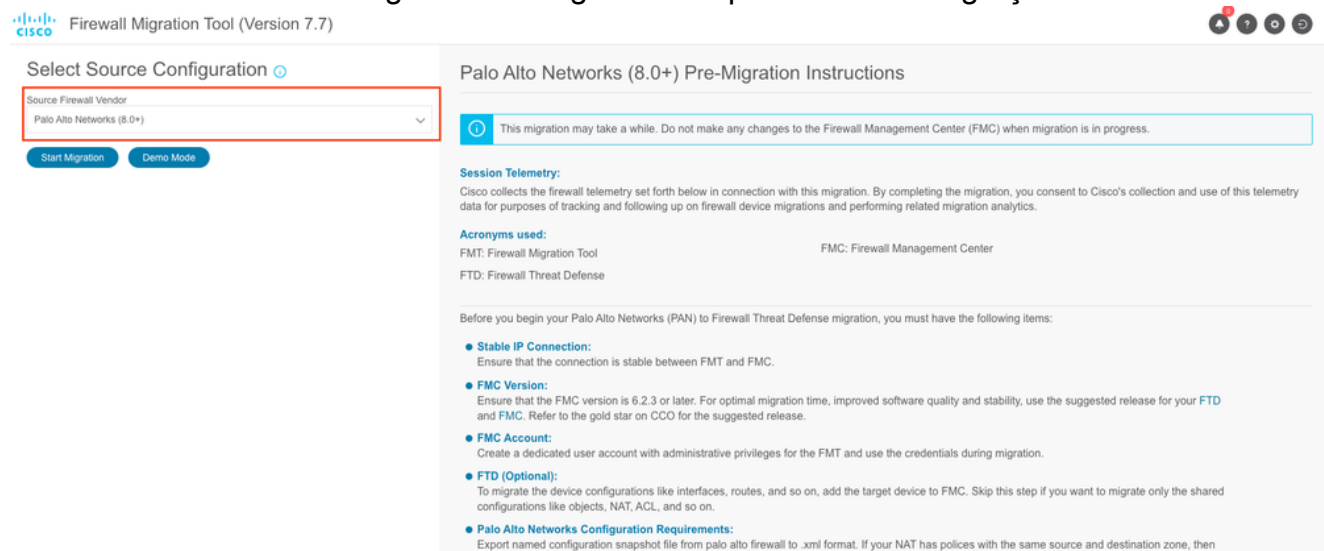
-
4. Após executar o programa, ele abre um navegador que exibe o Contrato de licença de usuário final.
 1. Marque a caixa de seleção para aceitar termos e condições.
 2. Clique em Continuar.
 5. Faça login usando credenciais CCO válidas para acessar a GUI do FMT.



The image shows the Cisco Security Cloud Sign On page. At the top is the Cisco logo. Below it is the heading "Security Cloud Sign On". There is an "Email" input field with the letter "s" and a "Continue" button. Below the button is a link "Don't have an account? Sign up now". There is a horizontal line with "Or" in the center. Below the line is a link "Other login options". At the bottom are links "System status" and "Policy statement".

Prompt de login do FMT

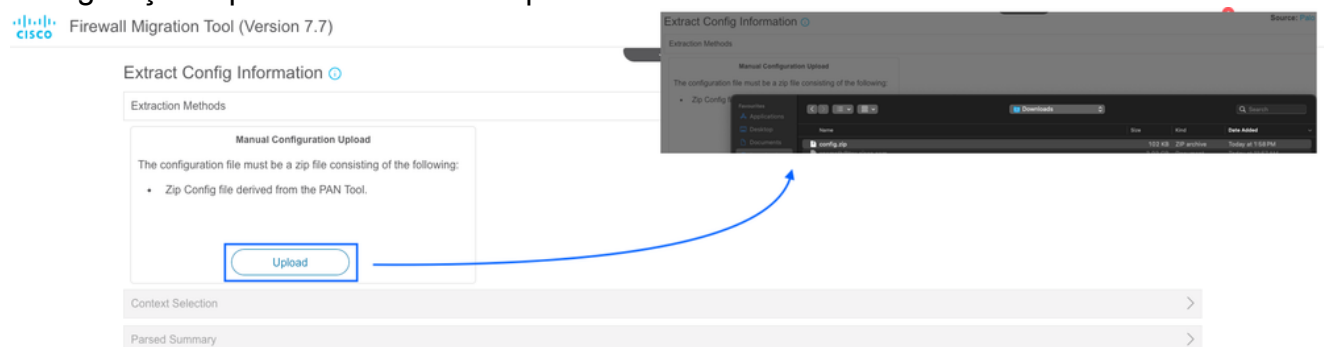
6. Selecione o Firewall de origem a ser migrado e clique em Iniciar migração.



The image shows the Firewall Migration Tool (Version 7.7) interface. On the left, under "Select Source Configuration", there is a dropdown menu for "Source Firewall Vendor" with "Palo Alto Networks (8.0+)" selected. Below it are "Start Migration" and "Demo Mode" buttons. On the right, under "Palo Alto Networks (8.0+) Pre-Migration Instructions", there is a warning box: "This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress." Below this are sections for "Session Telemetry", "Acronyms used" (FMT: Firewall Migration Tool, FMC: Firewall Management Center, FTD: Firewall Threat Defense), and a list of requirements for migration, including "Stable IP Connection", "FMC Version", "FMC Account", "FTD (Optional)", and "Palo Alto Networks Configuration Requirements".

GUI FMT

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

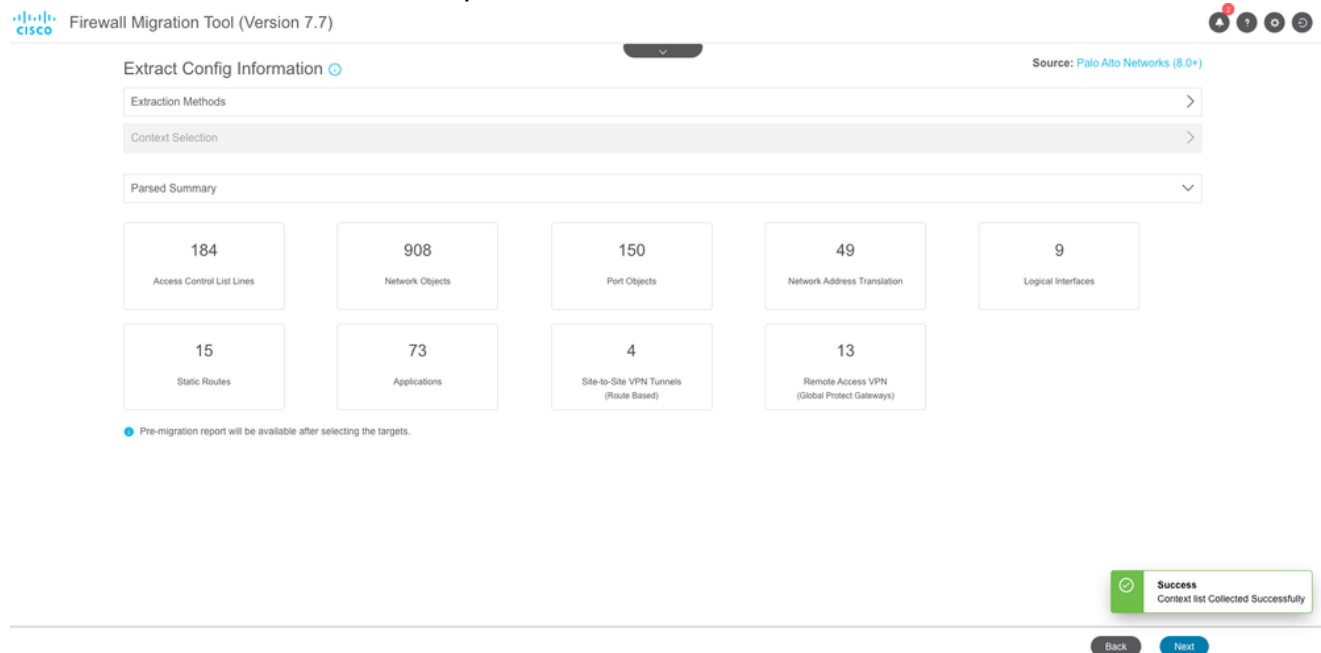


The image shows the Firewall Migration Tool (Version 7.7) interface. On the left, under "Extract Config Information", there is a section for "Extraction Methods" with a "Manual Configuration Upload" subsection. It states: "The configuration file must be a zip file consisting of the following: Zip Config file derived from the PAN Tool." Below this is an "Upload" button. On the right, there is a screenshot of a file manager showing a "config.zip" file. A blue arrow points from the "Upload" button to the "config.zip" file.

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

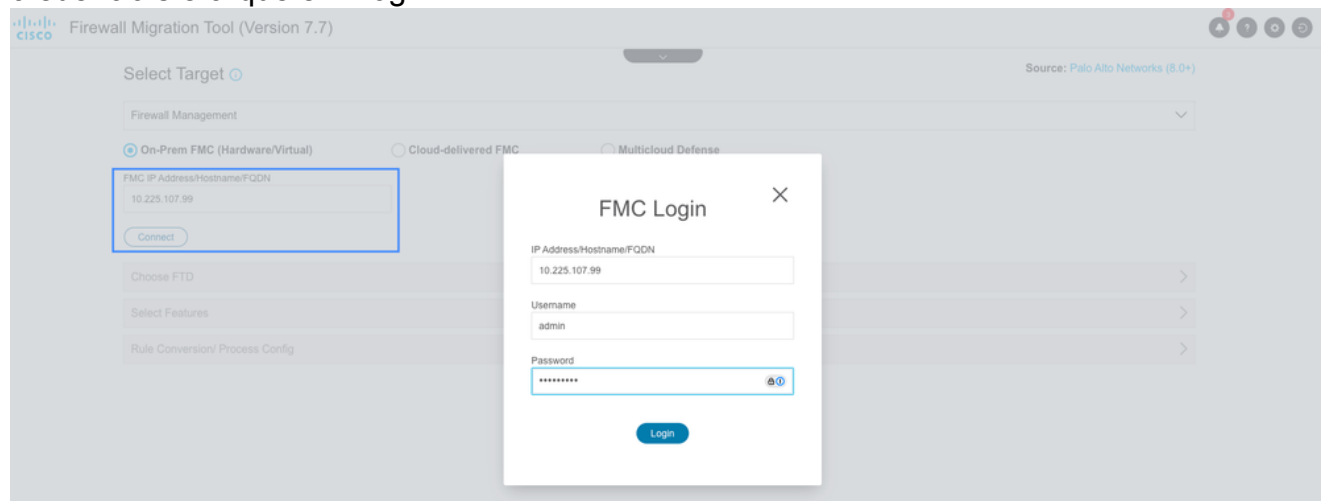
deles deve ser analisado e migrado um após o outro.
Valide o resumo analisado e clique no ícone Próximo.



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.

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

☒ On-Prem FMC (Hardware/Virtual) ☐ Cloud-delivered FMC ☐ Multicloud Defense

FMC IP Address/Hostname/FQDN: 10.225.107.99

Choose Domain: Global/Cisco

Connect

Proceed

Successfully connected to FMC

Seleção de domínio

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

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

☒ Select FTD Device ☐ Proceed without FTD

FW1 (10.105.209.80) - NA (R)

Proceed

Select Features

Rule Conversion/ Process Config

Selecionar FTD de Destino

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

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

Selected FTD: FW1

Select Features

Device Configuration

- ☒ Interfaces
- ☒ Routes
- ☒ Site-to-Site VPN Tunnels
- ☐ Policy Based (Unsupported)
- ☒ Route Based (VTI)

Shared Configuration

- ☒ Access Control
- ☐ Migrate policies with Application-default as Enabled
- ☒ Network Objects
- ☒ Port Objects
- ☒ Remote Access VPN

Advanced Configuration

Optimization

- ☒ Migrate Only Referenced Objects

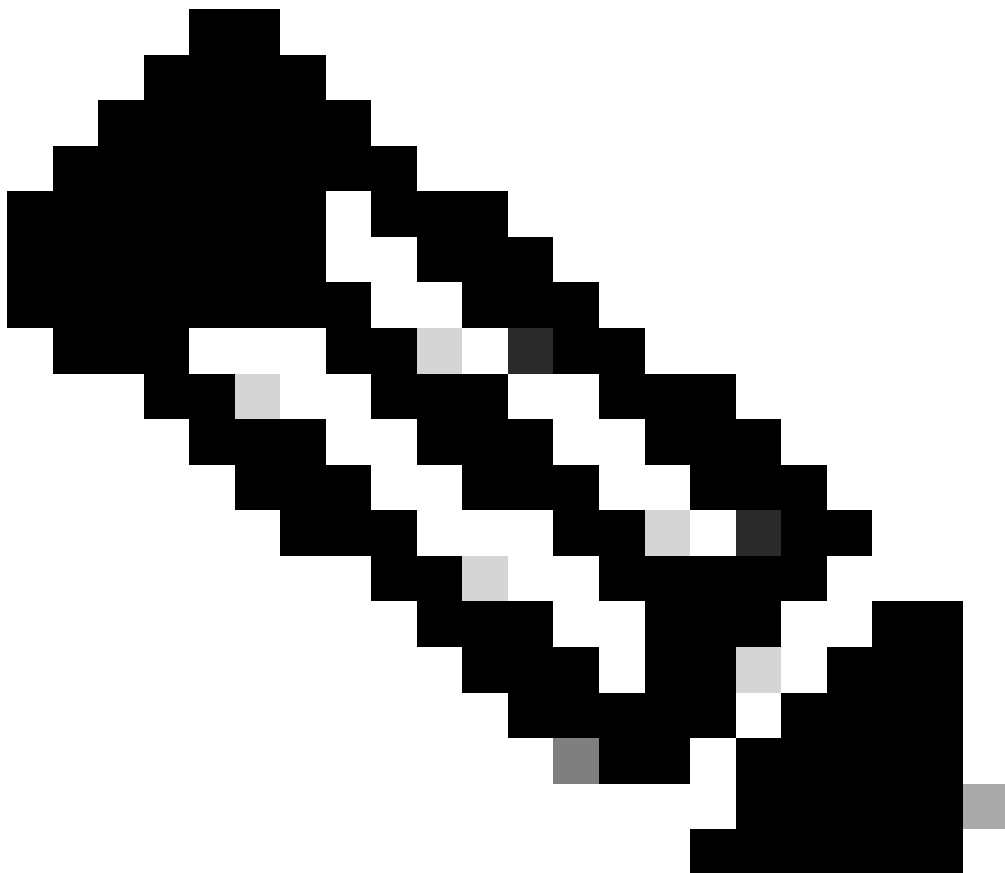
Access Control Options

- ☒ Discovered Identities

Proceed

Rule Conversion/ Process Config

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.

Select Target

Source: Palo Alto Networks (8.0+)

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD

Selected FTD: FW1

Select Features

Rule Conversion/ Process Config

Start Conversion

No parsing error 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

For pre-migration report

Parsed configuration summary

195	752	98	52	8
Access Control List Lines	Network Objects	Port Objects	Network Address Translation	Logical Interfaces
2	0	70	9	
Static Routes	Site-to-Site VPN Tunnels (Route Based)	Applications	Remote Access VPN (Global Protect Gateways)	

Back Next

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.

Map FTD Interface

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

PAN Interface Name	FTD Interface Name	Mapped Name
ethernet1/2	Select Interface	ethernet_2
ethernet1/3	✓ Ethernet1/1	ethernet_3
ethernet1/4	Ethernet1/10	ethernet_4
ethernet1/5	Ethernet1/11	ethernet_5
ethernet1/6	Ethernet1/12	ethernet_6
ethernet1/7	Ethernet1/13	ethernet_7
	Ethernet1/14	
	Ethernet1/15	
	Ethernet1/16	
	Ethernet1/17	
	Ethernet1/18	
	Ethernet1/19	

FTD Interface name can be edited

Mapping of FTD interfaces

10 per page 1 to 6 of 6 Page 1 of 1

Back Next

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.

Map Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

PAN Zone Name	FMC Security Zones
G-Inside	Select Security Zone
Outside	Select Security Zone
GPV-Inside	Select Security Zone
Inside	Select Security Zone
DMZ	Select Security Zone
ISC	Select Security Zone
Mel	Select Security Zone
OT-Inside	Select Security Zone
Wireless-Inside	Select Security Zone
4-Inside	Select Security Zone

Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be grayed out.

10 per page 1 to 10 of 12 |< < Page 1 of 2 > >|

Back

Next

Criação de zona de segurança

Criação manual de zonas de segurança:

on Tool (Version 7.7)

Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Add SZ

Security Zones (SZ)

Add

Max 48 characters for zone name. Allowed special characters are _-+*

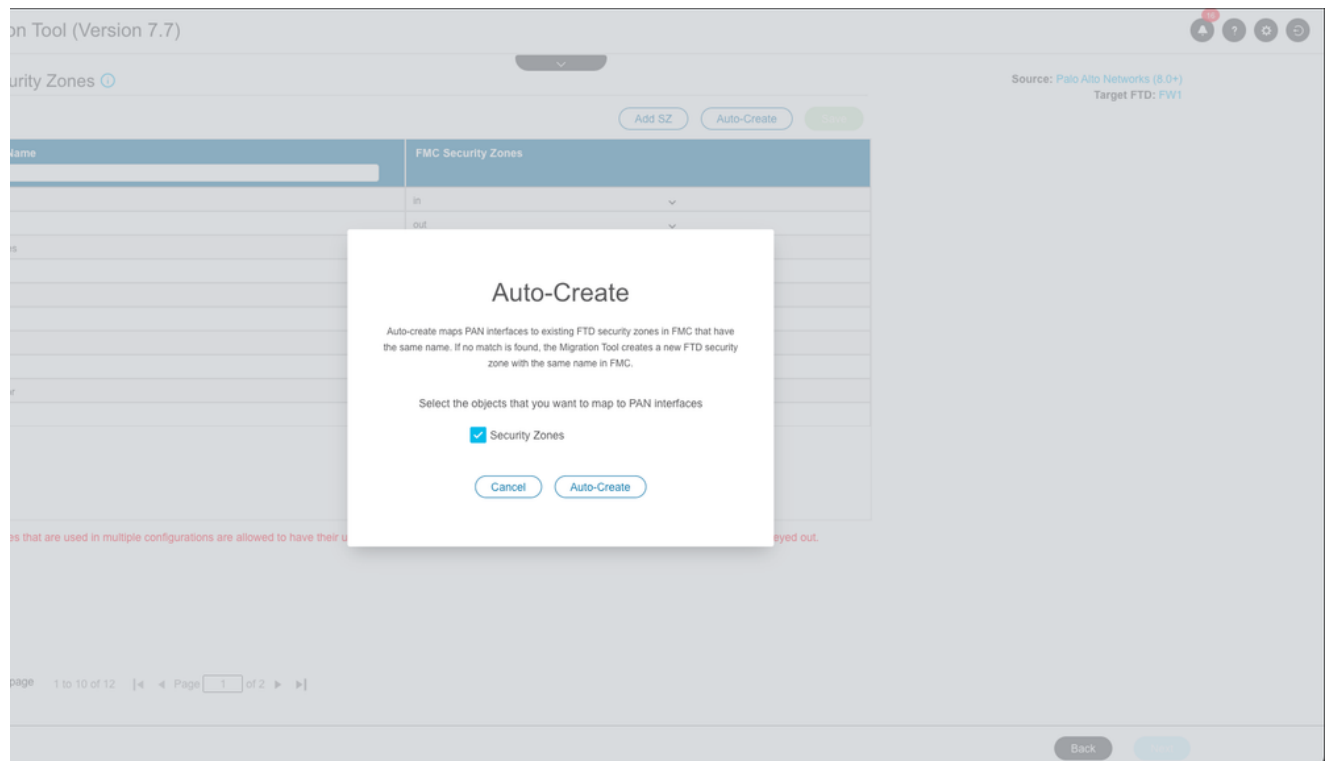
Security Zones	Type	Actions
DMZ	Select	 
	SWITCHED	
	ROUTED	

0 - 0 of 0 |< < 1 > >|

Close

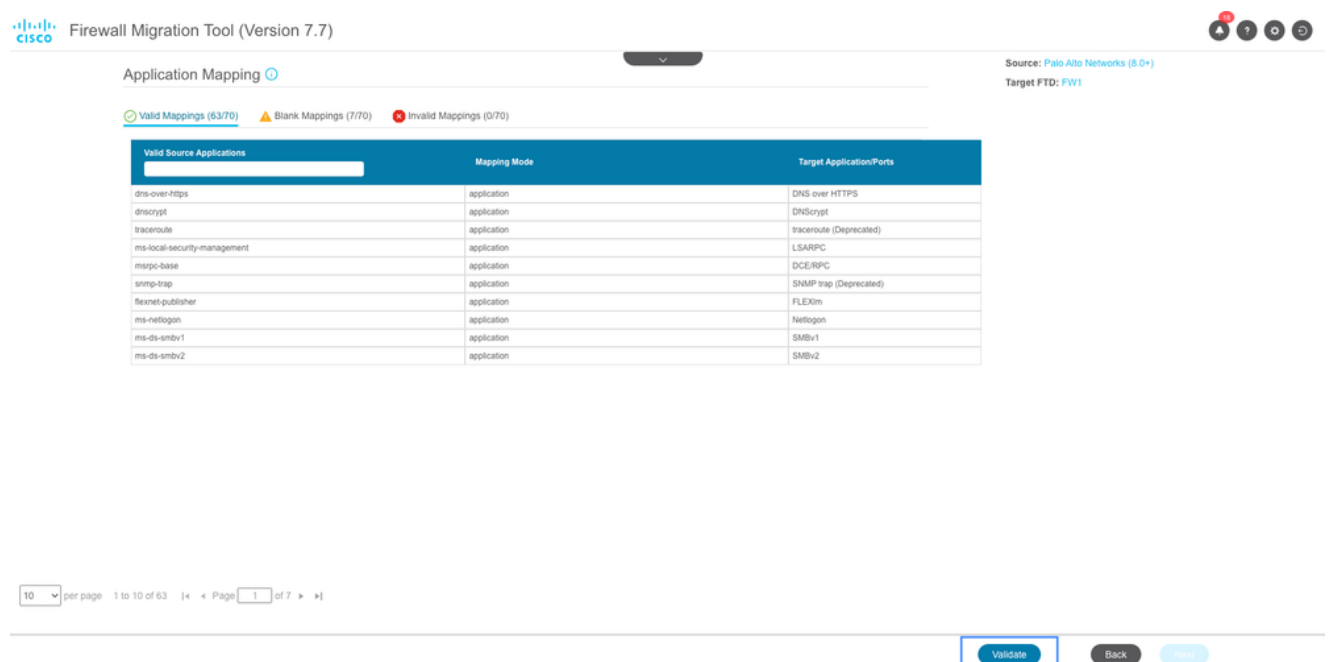
Criação manual de zona de segurança

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

Firewall Migration Tool (Version 7.7)

Application Mapping

Validation of application mapping is in progress. Please wait

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

Valid Mappings (63/70)

Blank Mappings (7/70)

Invalid Mappings (0/70)

Valid Source Applications	Mapping Mode	Target Application/Ports
dns-over-https	application	DNS over HTTPS
dnscrypt	application	DNScrypt
traceroute	application	traceroute (Deprecated)
ms-local-security-management	application	LSARPC
snmp-base	application	DCE/RPC
snmp-trap	application	SNMP trap (Deprecated)
flexnet-publisher	application	FLEXlm
ms-netlogon	application	Netlogon
ms-ds-smbv1	application	SMBv1
ms-ds-smbv2	application	SMBv2

10

per page

1 to 10 of 63

<

Page 1

>

Validate

Back

Next

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.

Firewall Migration Tool (Version 7.7)

Application Mapping

Clear Mapped Data

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

Valid Mappings (61/70)

Blank Mappings (7/70)

Invalid Mappings (2/70)

Invalid Source Applications	Mapping Mode	Target Application/Ports
traceroute	Application	netmg-traceroute
snmp-trap	Port(s)	udp/162

10

per page

1 to 2 of 2

<

Page 1

>

Validate

Back

Next

Mapeamento de aplicativos em branco e inválido

- 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.

Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Remote Access VPN

Verify configuration in each section

Select all 195 entries Selected: 0 / 195

#	Name	Zone	SOURCE			Zone	DESTINATION		Application	URLs	State	Action	TIME BASED
			Network	Port	User		Network	Port					
☐	1	Allow Time	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None
☐	2	Allow Time	ANY	ANY	ANY		2M...	ANY	NTP	NA	✓	Allow	None
☐	3	Allow Time	GRP_ADDR...	ANY	ANY		com	ANY	NTP	NA	✓	Allow	None
☐	4	Allow DNS	ANY	ANY	ANY		3R...	ANY	DNS, DNSCrypt, DN...	NA	✓	Allow	None
☐	5	Allow DNS	ANY	ANY	ANY		3R...	ANY	DNS	NA	✓	Allow	None
☐	6	Allow API	ANY	ANY	ANY		3M...	TCP-80, TCP...	ANY	NA	✓	Allow	None
☐	7	Allow traffi	ADDR_10.11...	ANY	ANY		2.16...	TCP-443	ANY	NA	✓	Allow	None
☐	8	Allow Acco	ADDR_192.16...	ANY	ANY		2T...	ANY	ANY	NA	✓	Allow	None
☐	9	Allow ICM	ANY	ANY	ANY		Inside	ANY	netmg-traceroute	NA	✓	Allow	None
☐	10	Allow ICM	ANY	ANY	ANY		Inside	ICMPv4	ANY	NA	✓	Allow	None
☐	11	Allow DHCP	ANY	ANY	ANY		Inside	ANY	DHCP	NA	✓	Allow	None
☐	12	Allow NetB	ANY	ANY	ANY		Inside	ANY	NetBIOS-ns, NetBIO...	NA	✓	Allow	None
☐	13	Allow DNS	ANY	ANY	ANY		Inside	ANY	DNS	NA	✓	Allow	None

50 per page 1 to 50 of 195 Page 1 of 4

Optimise access control list and validate

Optimize ACL Validate

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.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

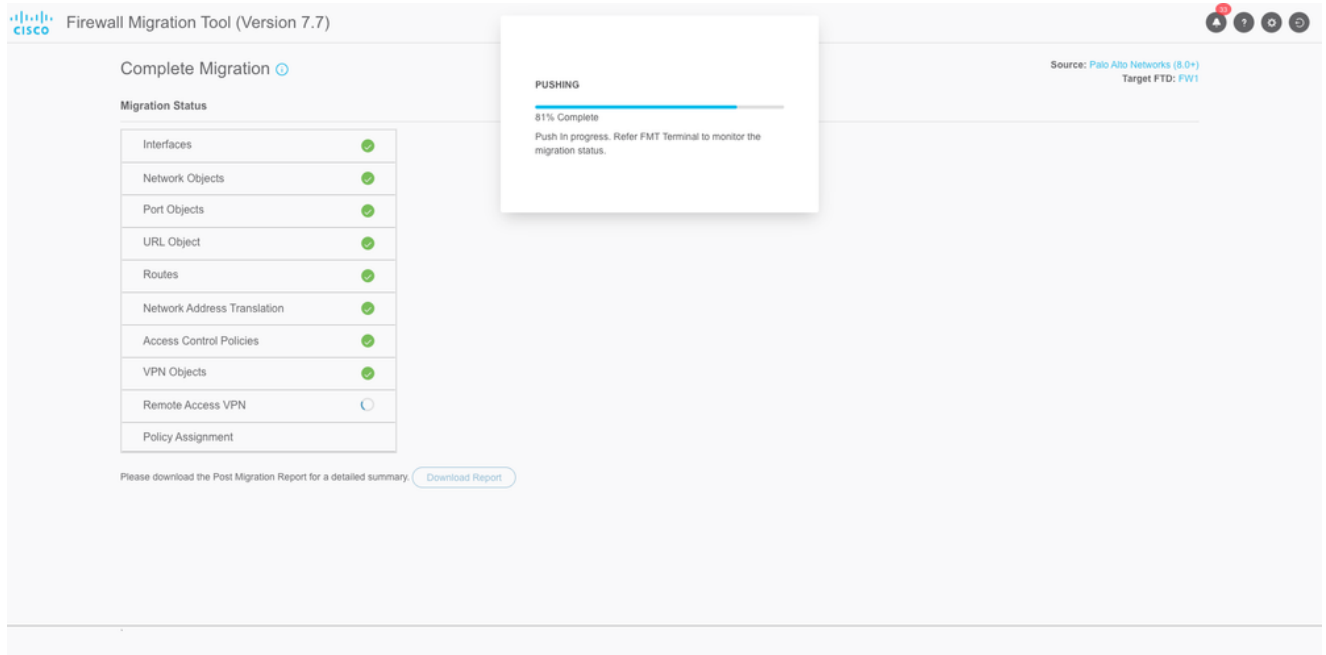
195 Access Control List Lines	752 Network Objects	100 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	62 Applications	9 Remote Access VPN (Global Protect Gateways)	

Note: The configuration on the target FTD device FW1 (10.105.209.80) will be overwritten as part of this migration.

Push Configuration

Resumo da validação da configuração

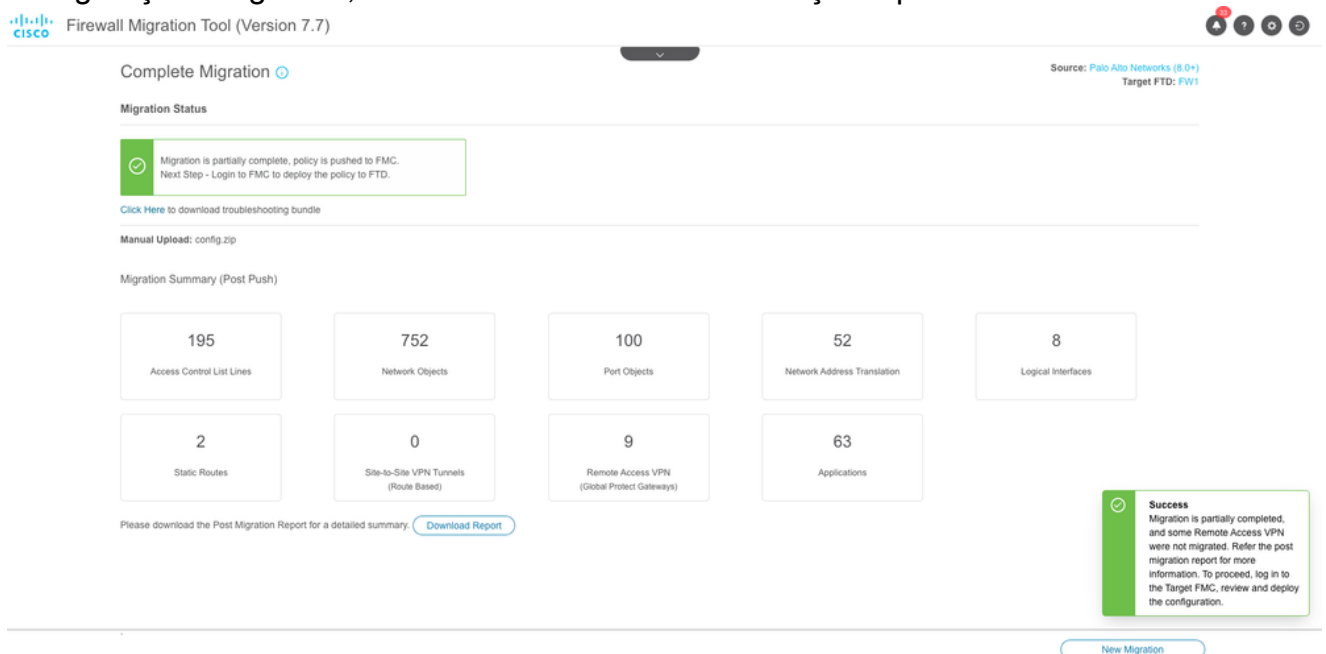
19. O progresso do envio da configuração para o FMC agora está visível na seção Status da migração. Você também pode usar a janela do terminal FMT para monitorar o status da migração.



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.