

Migrar um FTD de um CVP para outro CVP

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como migrar um dispositivo Cisco Firepower Threat Defense (FTD) entre os Firepower Management Centers.

Pré-requisitos

Antes de iniciar o processo de migração, certifique-se de que estes pré-requisitos estejam em vigor:

- Acesso aos CVP de origem e de destino.
- Credenciais administrativas para os CVP e o DTF.
- Faça backup da configuração atual do FMC.
- Certifique-se de que os dispositivos FTD que executam uma versão de software compatível com o FMC de destino.
- Assegurar que o CVP de destino tem a mesma versão que o CVP de origem.

Requisitos

- Ambos os FMCs devem estar executando versões de software compatíveis.
- Conectividade de rede entre o dispositivo FTD e ambos os FMC.
- Armazenamento e recursos adequados no CVP de destino para acomodar o dispositivo de DTF.

Componentes Utilizados

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

Cisco Firepower Threat Defense Virtual (FTDv) versão 7.2.5

Firepower Management Center Virtual (FMCv) versão 7.2.5

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.

Informações de Apoio

A migração de um dispositivo FTD de um CVP para outro envolve várias etapas, incluindo o cancelamento do registro do dispositivo no CVP de origem, a preparação do CVP de destino e o novo registro do dispositivo. Esse processo garante que todas as políticas e configurações sejam corretamente transferidas e aplicadas.

Configurar

Configurações

1. Iniciar sessão no CVP de origem.



Secure Firewall Management Center

Username

Password

Log In

2. Navegue até Devices > Device Management e selecione o dispositivo a ser migrado.



View By: Group

All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (0) Upgrade (0) Snort 3 (1)

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (1)			
<input type="checkbox"/>	192.168.15.31 Snort 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A

3. Na seção do dispositivo, navegue até o dispositivo e clique em exportar para exportar suas configurações de dispositivo.

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General



Name: FTD1
Transfer Packets: Yes
Mode: Routed
Compliance Mode: None
TLS Crypto Acceleration: Disabled

Device Configuration:

[Import](#) [Export](#) [Download](#)

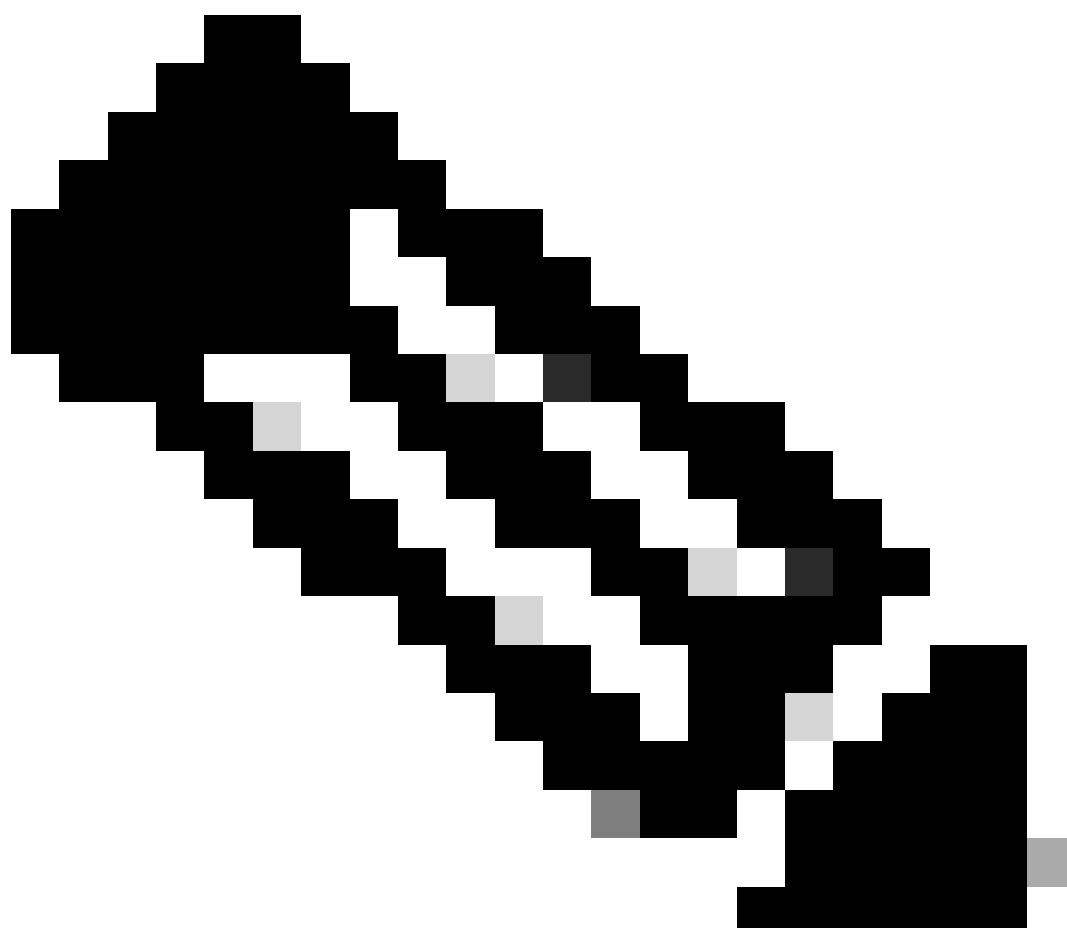
4. Depois que a configuração tiver sido exportada, você deverá baixá-la.

Device Configuration Download

Backup taken on **14-Oct-2024 07:05 PM** is available.

[Click here to download the package](#)

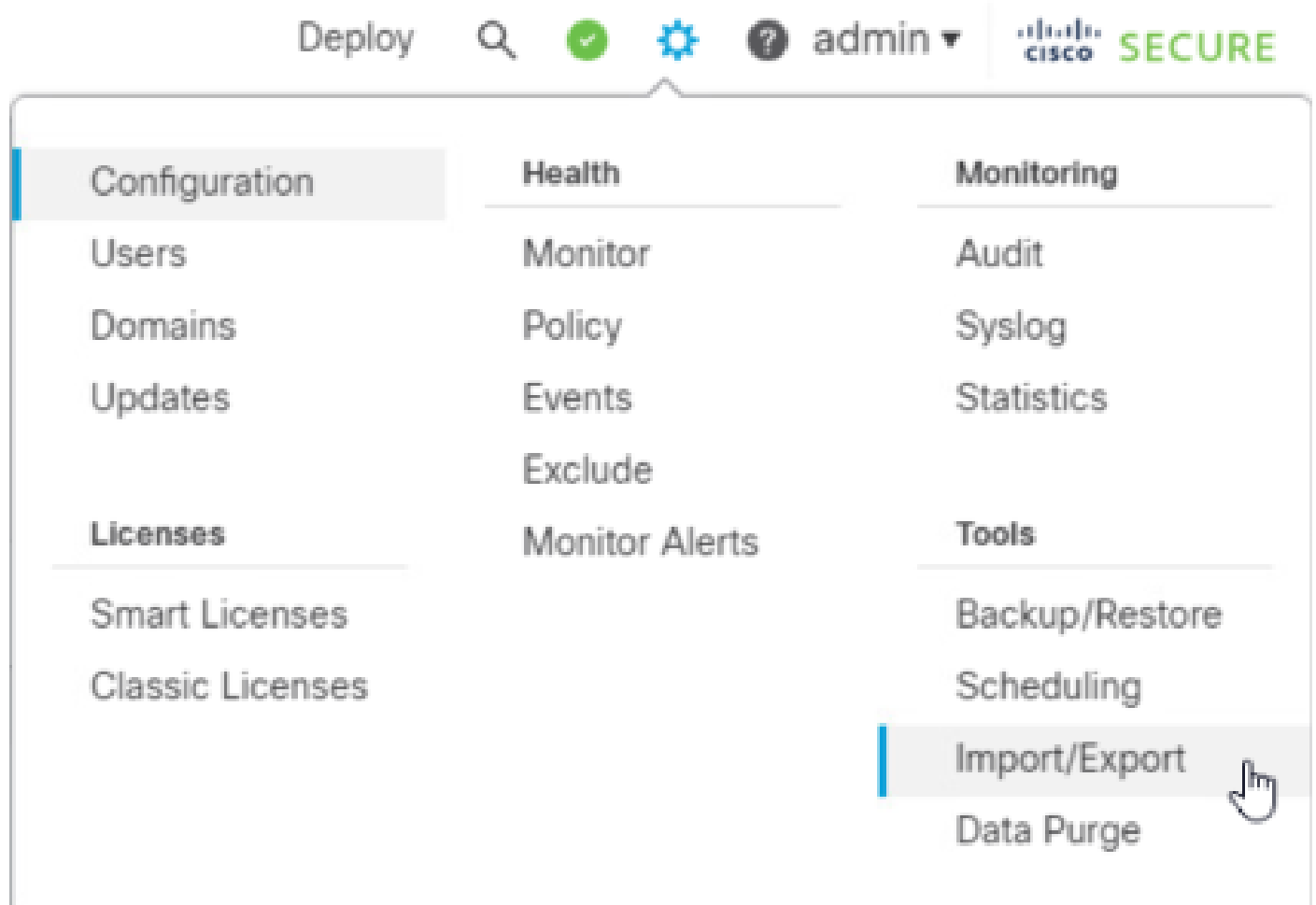
OK



Observação: o arquivo baixado deve conter a extensão .SFO e conter informações de

configuração do dispositivo, como endereços IP, zonas de segurança, rotas estáticas e outras configurações do dispositivo.

5. Você deve exportar as políticas associadas ao dispositivo, navegar para Sistema > Ferramentas > Importar/Exportar, selecionar as políticas que deseja exportar e clicar em exportar.



∨ Access Control Policy



test

Access Control Policy

> Contextual Cross-launch

> Custom Table View

> Custom Workflow

> Dashboard

> Health Policy

∨ NAT Threat Defense



NAT

NAT Threat Defense

∨ Platform Settings Threat Defense



test

Platform Settings Threat Defense

> Report Template

Export



Observação: verifique se o arquivo .SFO foi baixado com êxito. O download é feito automaticamente após clicar em exportar. Esse arquivo contém as políticas de controle de acesso, configurações de plataforma, políticas de NAT e outras políticas que são indispensáveis para a migração, pois não são exportadas junto com a configuração do dispositivo e precisam ser carregadas manualmente no FMC de destino.

6. Cancele o registro do dispositivo FTD no FMC, navegue para Devices > Device management, clique nos três pontos verticais no lado direito e selecione delete.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin | **Secure**

View By: Group

All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (1) Upgrade (0) Short 3 (1)

Deployment History

Search Device Add

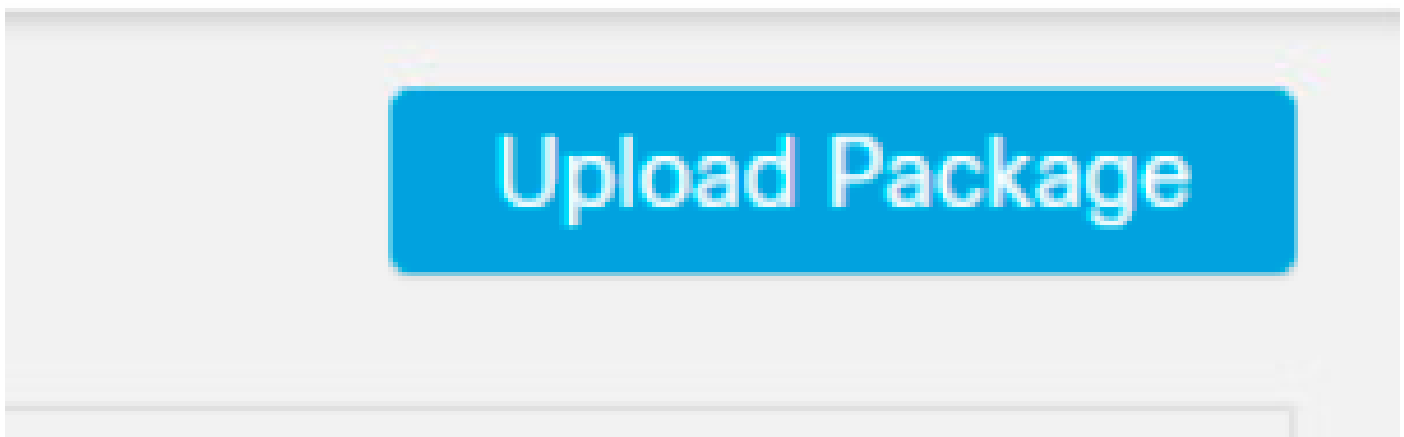
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD1 Short 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A	Base, Threat (2 more...)	test	

Context Menu:

- Delete
- Packet Tracer
- Packet Capture
- Revert Upgrade
- Health Monitor
- Troubleshoot Files

7. Preparar o CVP de destino:

- Inicie sessão no FMC de destino.
- Certifique-se de que o FMC está pronto para aceitar o novo dispositivo importando as políticas do FMC de origem que você baixou na etapa 5. Navegue até System > Tools > Import/Export e clique em upload package. Carregue o arquivo a ser importado e clique em upload.

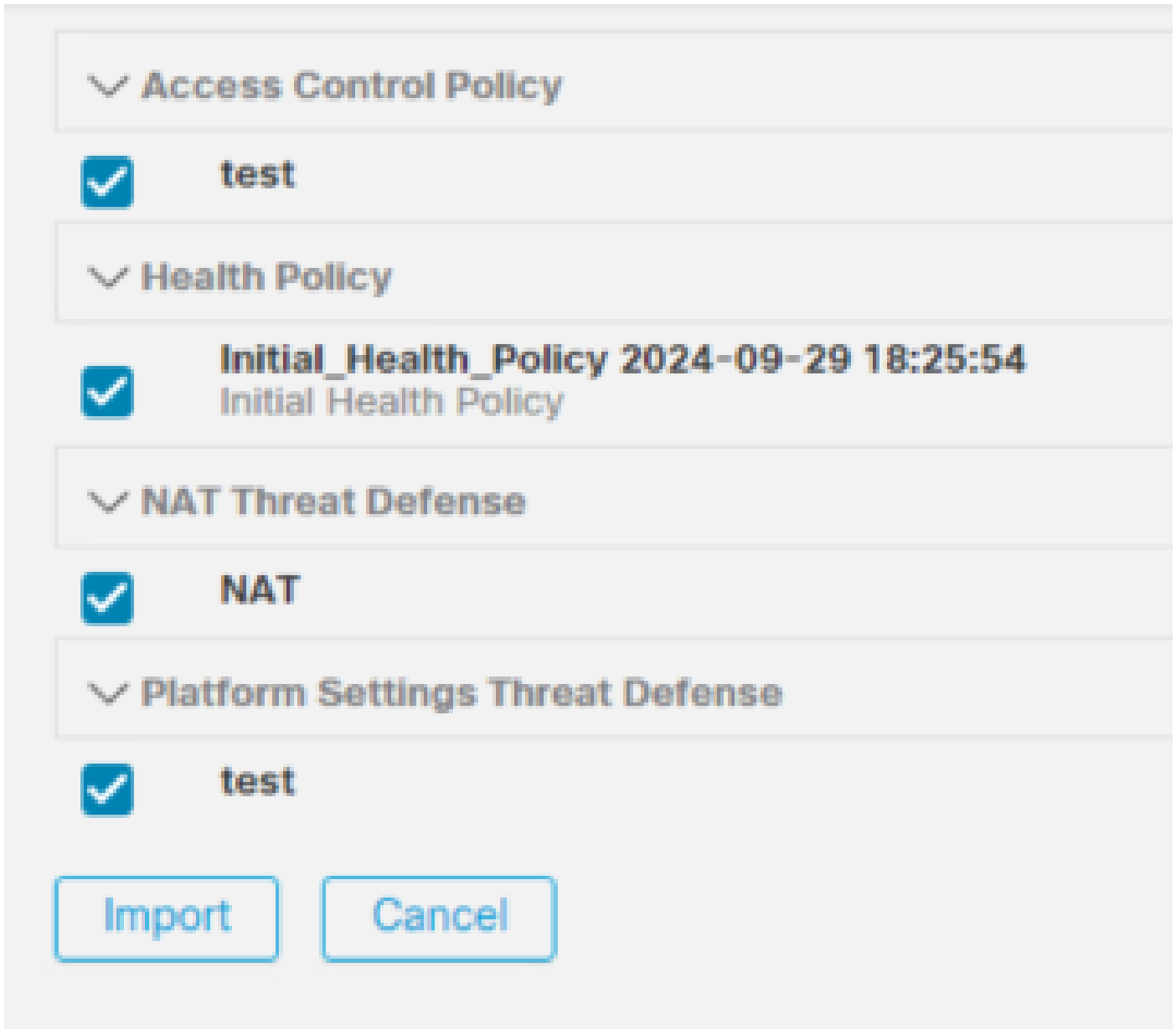


Firewall Management Center
System / Tools / Upload Package

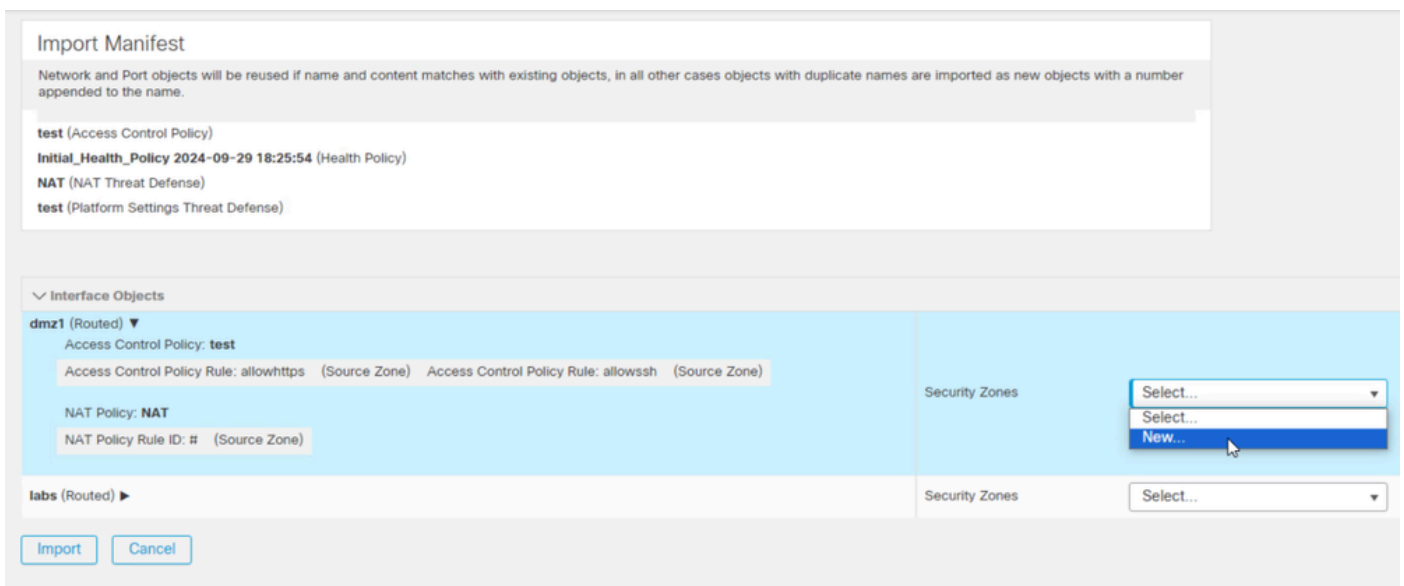
Overview Analysis Policies Devices Objects Integration

Package Name ObjectExport...4235208.sfo

8. Selecione as políticas para importar no FMC de destino.

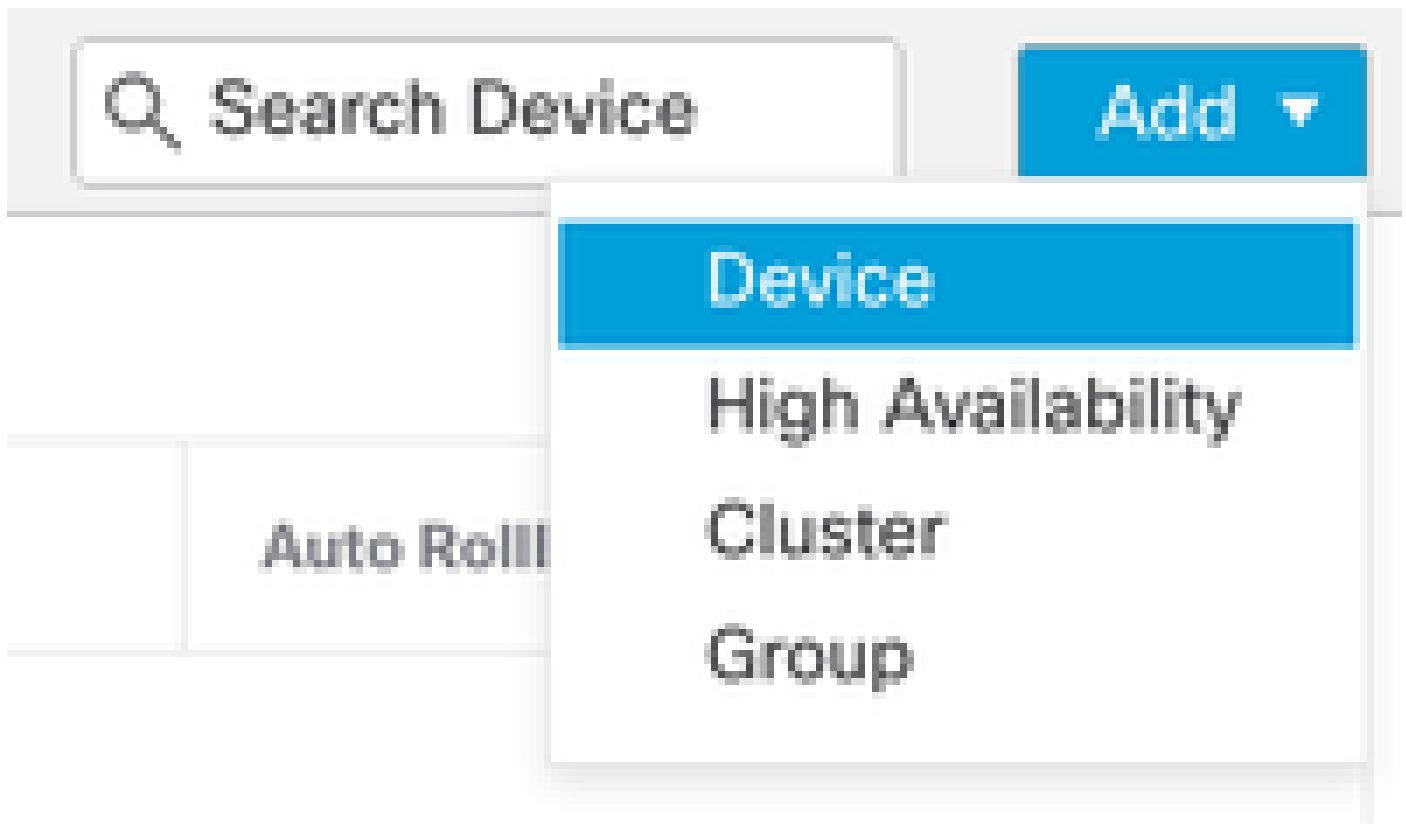


9. No manifesto de importação, selecione uma zona de segurança ou crie uma nova para atribuir ao objeto de interface e clique em importar.



10. Registrar o FTD no CVP de destino:

- No FMC de destino, navegue até a guia Device > Management e selecione Add > Device.
- Conclua o processo de registro respondendo aos avisos.



Add Device



CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

† Either host or NAT ID is required.

Cancel

Register




Para obter detalhes adicionais, consulte o Guia de configuração do Firepower Management Center, [Adicionar dispositivos ao Firepower Management Center](#)

11. Navegue até Device > Device Management > selecione o FTD > Device e clique em import. Um aviso aparece solicitando sua confirmação para substituir a configuração do dispositivo. Clique em yes.

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General		  
Name:		FTD1
Transfer Packets:		Yes
Mode:		Routed
Compliance Mode:		None
TLS Crypto Acceleration:		Disabled
Device Configuration:	<input type="button" value="Import"/>	<input type="button" value="Export"/> <input type="button" value="Download"/>

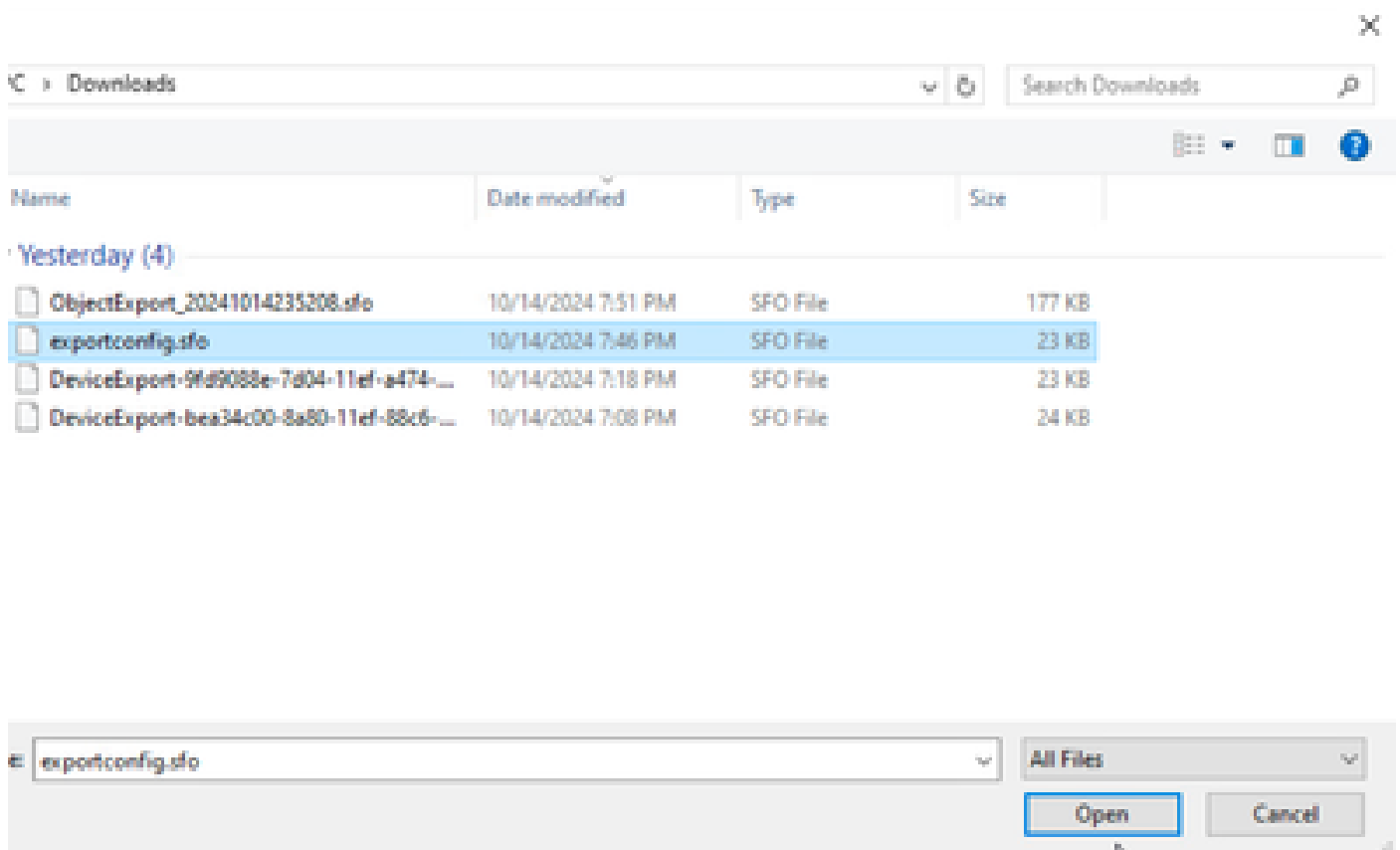
Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

No

Yes

12. Selecione o arquivo de configuração de importação que deve ser a extensão .SFO, clique em carregar e uma mensagem será exibida indicando que a importação foi iniciada.



The screenshot shows a Windows File Explorer window with the address bar set to 'Downloads'. The search bar contains 'Search Downloads'. The file list is sorted by 'Date modified' and shows four files from 'Yesterday (4)'. The file 'exportconfig.sfo' is selected. Below the list, a file selection dialog is open, showing the selected file 'exportconfig.sfo' and the 'Open' button.

Name	Date modified	Type	Size
Yesterday (4)			
ObjectExport_20241014235208.sfo	10/14/2024 7:51 PM	SFO File	177 KB
exportconfig.sfo	10/14/2024 7:46 PM	SFO File	23 KB
DeviceExport-9fd9088e-7d04-11ef-a474-...	10/14/2024 7:18 PM	SFO File	23 KB
DeviceExport-bea34c00-8a80-11ef-88c6-...	10/14/2024 7:08 PM	SFO File	24 KB

File selection dialog details:

- File name: exportconfig.sfo
- File type: All Files
- Buttons: Open, Cancel

Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

OK

Only:

13. Finalmente, um alerta é exibido e um relatório é gerado automaticamente quando a importação é concluída, permitindo que você revise os objetos e políticas que foram importados.

The screenshot shows the Cisco Secure interface. At the top, there is a navigation bar with 'Deploy', a search icon, a notification bell with '2', a gear icon, a user profile 'admin', and the 'CISCO SECURE' logo. Below this is a main navigation area with tabs for 'Deployments', 'Upgrades', 'Health' (with a red indicator), and 'Tasks' (with a red indicator and a blue underline). To the right of these tabs is a 'Show Notifications' toggle switch. Below the navigation is a summary bar for the 'Tasks' section, showing '20+ total' in a blue box, followed by '0 waiting', '0 running', '0 retrying', '20+ success', and '1 failure'. A search box labeled 'Filter' is also present. The main content area displays a notification for 'Device Configuration Import' with a green checkmark icon. The message reads 'Device configurations imported successfully' and includes a link to 'View Import Report'. A '6s' timer and a close 'X' icon are visible in the bottom right corner of the notification.

Configuration Import Summary

Initiated by:
Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

Type	Name
PG.PLATFORM.AutomaticApplicationBypassPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage
PG.PLATFORM.PixInterface	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface
PG.PLATFORM.NgfwinlineSetPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwinlineSetPage

Verificar

Após concluir a migração, verifique se o dispositivo FTD está corretamente registrado e funcionando com o FMC de destino:

- Verifique o status do dispositivo no FMC de destino.
- Verifique se todas as políticas e configurações foram aplicadas corretamente.
- Execute um teste para confirmar se o dispositivo está operacional.

Troubleshooting

Se você encontrar algum problema durante o processo de migração, considere estas etapas de solução de problemas:

- Verifique a conectividade de rede entre o dispositivo FTD e ambos os FMCs.
- Verifique se a versão do software em ambos os FMCs é a mesma.
- Verificar se há mensagens de erro ou avisos nos alertas dos dois CVP.

Informações Relacionadas

- [Guia de administração do Cisco Secure Firewall Management Center](#)
- [Configurar, verificar e solucionar problemas de registro de dispositivos do Firepower](#)

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.