Transição perfeita: Migração do Palo Alto Firewall para o Cisco FTD

Contents

Introdução

Este documento descreve o processo de transição de um firewall Palo Alto para um sistema Cisco FTD utilizando o FMT versão 6.0.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Exportando a configuração atual em execução do firewall Palo Alto no formato XML (*.xml).
- Acessando a CLI do Firewall Palo Alto e executando o comando show routing route, salvando a saída como um arquivo de texto (*.txt).
- Compactando o arquivo de configuração (*.xml) e o arquivo de saída de roteamento (*.txt) em um único arquivo ZIP (*.zip).

Componentes Utilizados

As informações neste documento são baseadas no Palo Alto Firewall versão 8.4.x ou posterior.

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.

Ferramenta de migração Firepower (FMT)

O FMT auxilia as equipes de engenharia na transição de qualquer firewall de fornecedor existente para o firewall de próxima geração (NGFW)/defesa contra ameaças (FTD) do Firepower da Cisco. Certifique-se de operar a versão mais recente do FMT, baixada do site da Cisco.

Diretriz de migração

1. Lista de verificação pré-migração

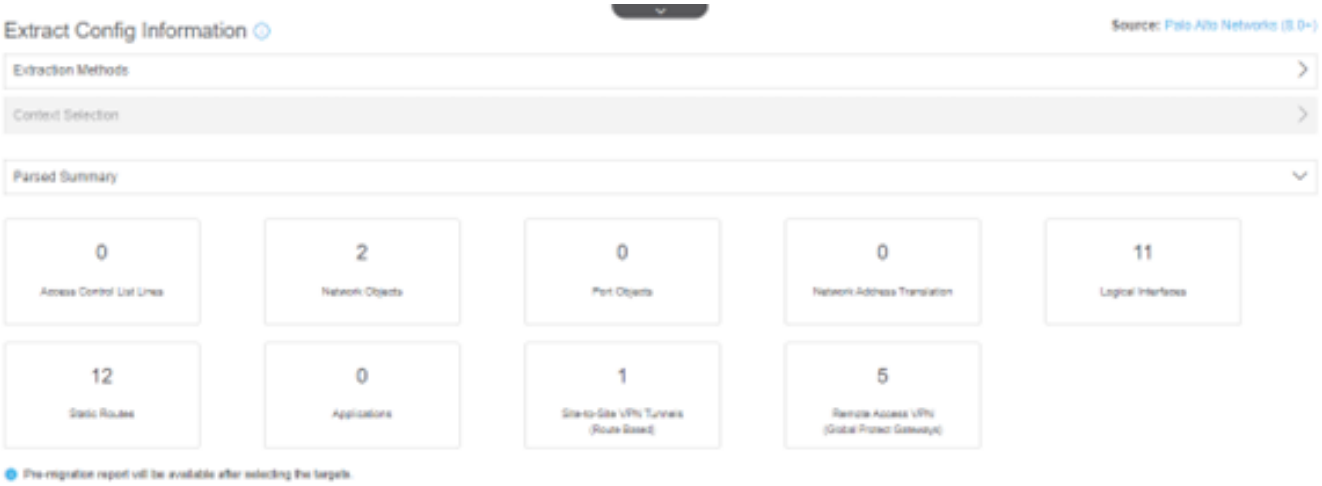
- Verificar se o FTD foi adicionado ao FMC antes de iniciar o processo de migração.
- Foi criada no CVP uma nova conta de utilizador com privilégios administrativos.
- O arquivo de configuração de execução exportado do Palo Alto.xml deve ser compactado com uma extensão de .zip.
- O NGFW/FTD deve ter o mesmo número de Physical ou Sub-interface ou canal de porta igual às interfaces do Palo Alto Firewall.

2. Uso da Ferramenta de Migração

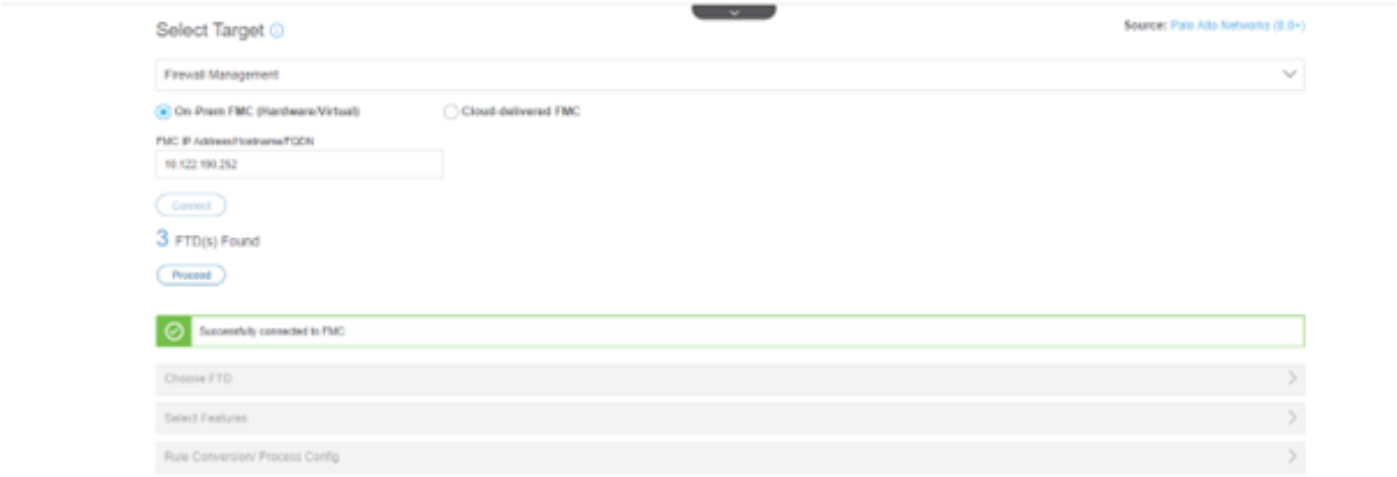
- Baixe o arquivo FMT tool .exe e execute-o como administrador.
- O FMT exigirá a ID do CEC ou a conta de usuário da Cisco para fazer login.
- Após o login bem-sucedido, a ferramenta exibirá um painel onde você pode escolher o fornecedor do firewall e fazer o upload do arquivo *.zip correspondente; consulte a próxima imagem.

- Revise cuidadosamente as instruções fornecidas no lado direito antes de prosseguir com a

migração.
- Clique em Iniciar migração quando estiver pronto para começar.
- Carregue o arquivo *.zip salvo que contém as configurações do seu firewall Palo Alto.
- Depois que o arquivo de configuração for carregado, você poderá ver um Resumo analisado do conteúdo e clicar em avançar; consulte a próxima imagem.

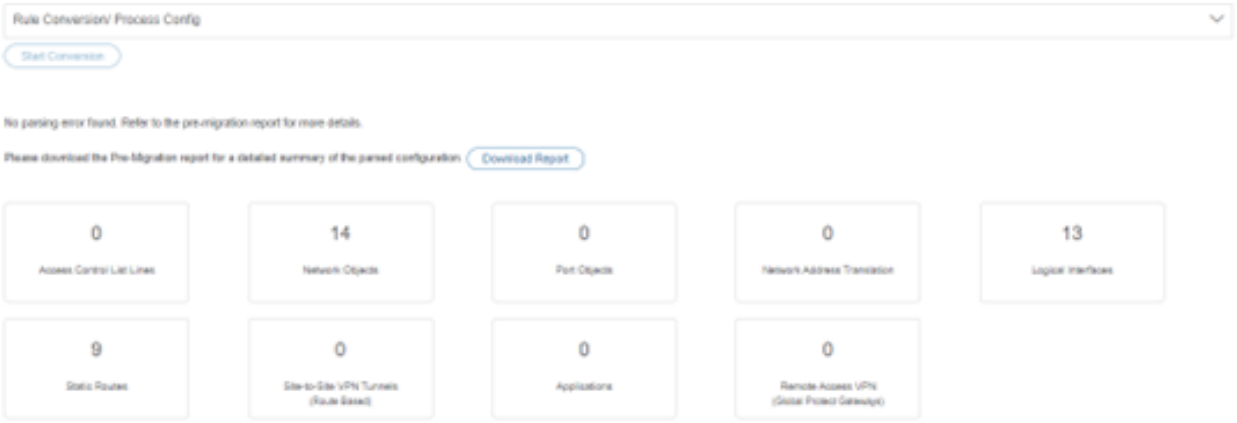


- Introduza o endereço IP do FMC e inicie sessão.
- A ferramenta procurará um FTD ativo que tenha sido registrado no FMC.
- Escolha o FTD que deseja migrar e clique em Prosseguir, como mostrado na imagem a seguir.

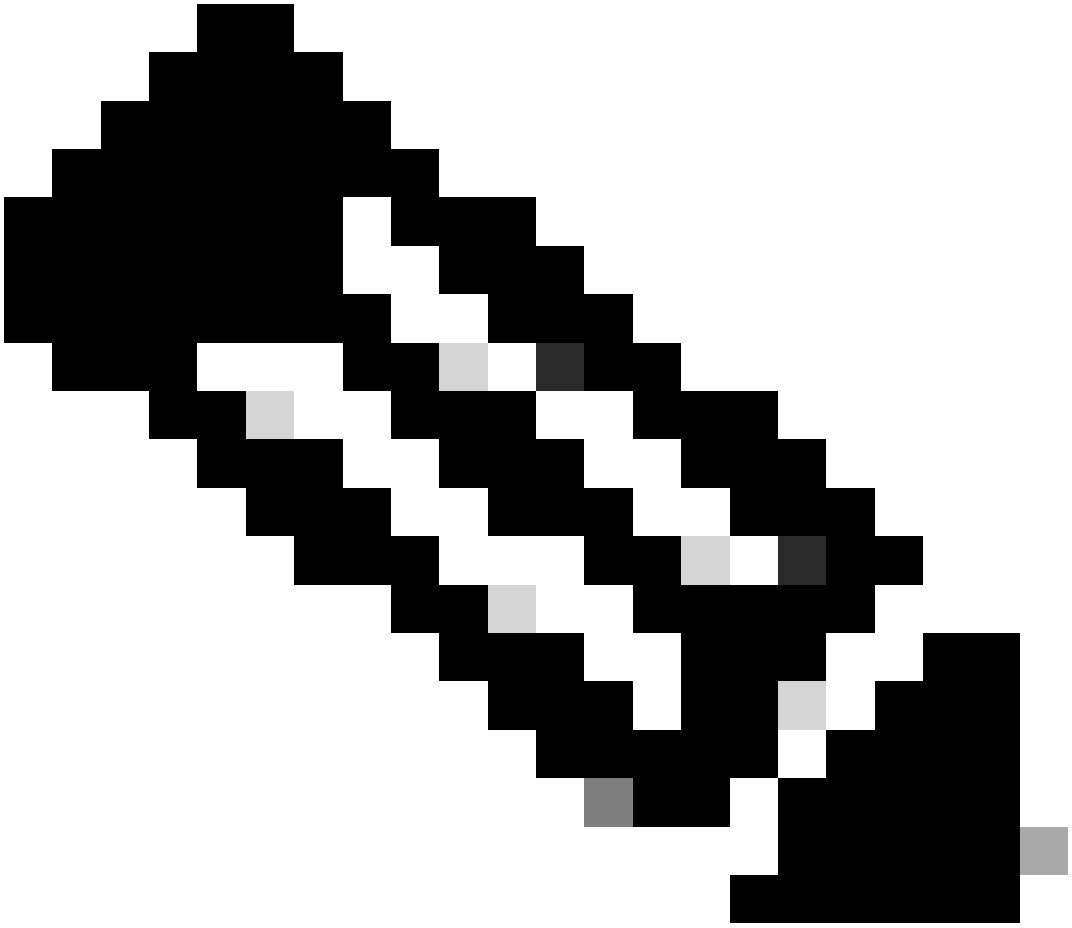


- Escolha os recursos específicos para migrar com base nos requisitos do cliente. Observe que os firewalls Palo Alto têm um conjunto de recursos diferente em comparação ao FTD.
- Clique em Continuar e consulte a próxima imagem para referência.

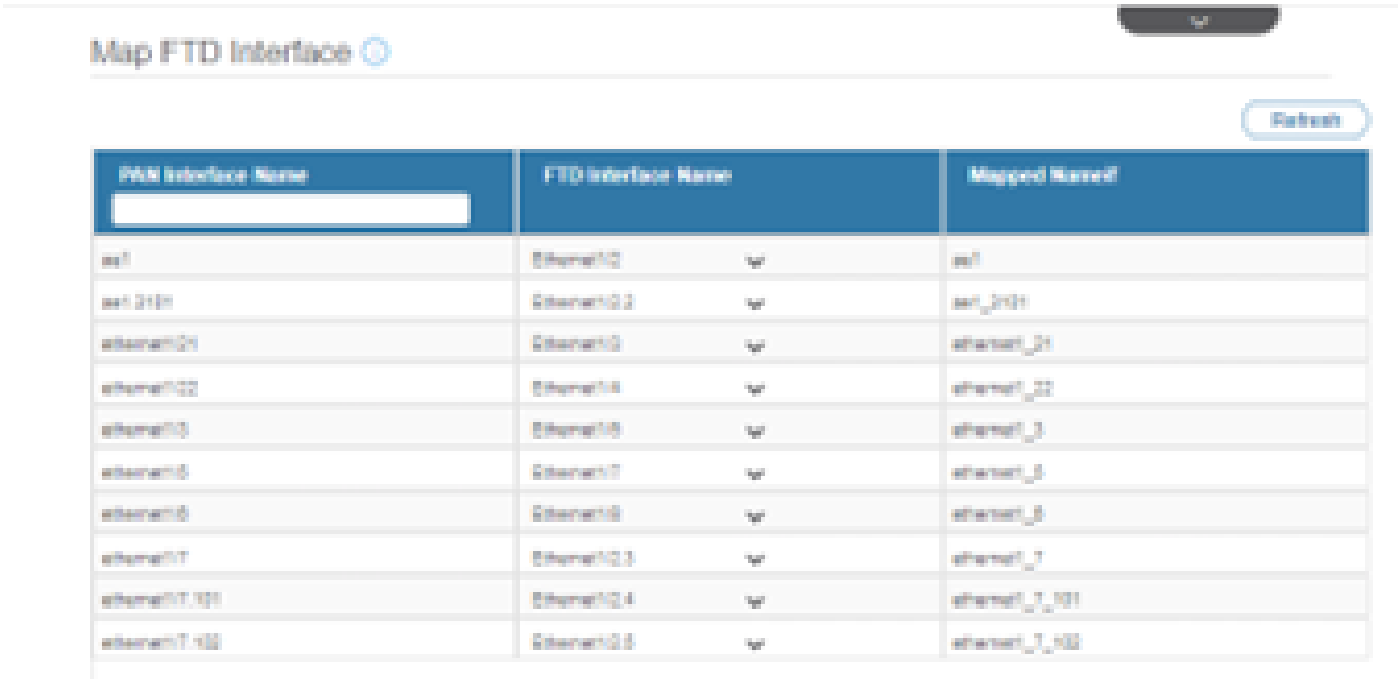
- O FMT executará a conversão de acordo com suas seleções. Revise as alterações no Relatório de Pré-Migração e clique em Continuar. Consulte a próxima imagem para obter orientação.



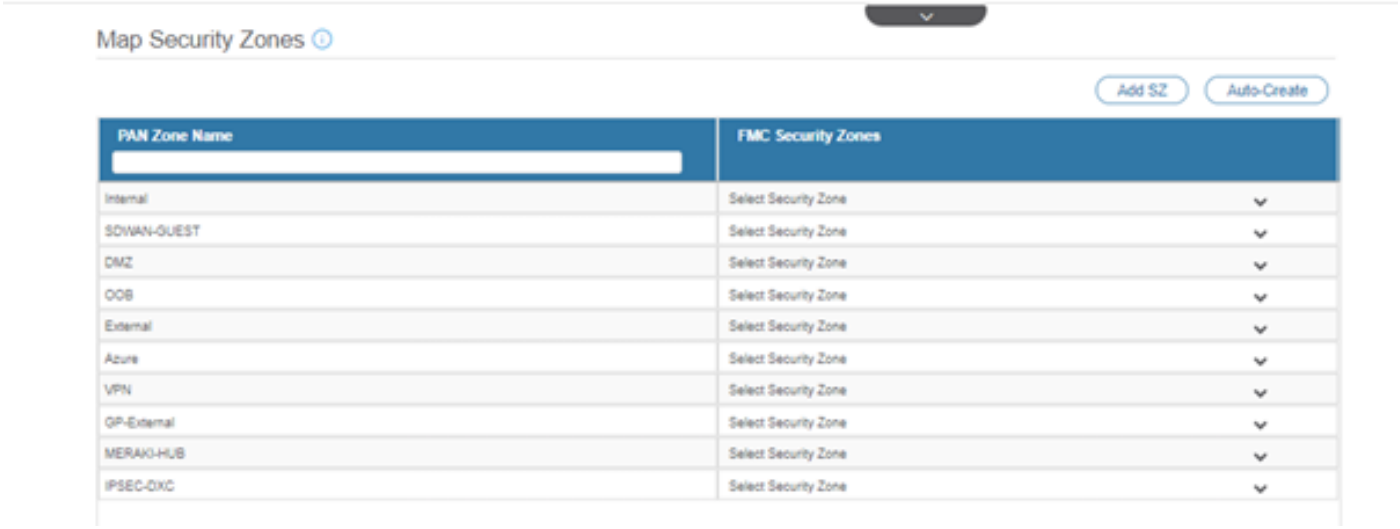
  - Mapeie as interfaces do firewall Palo Alto para as do FTD. Consulte a próxima imagem para obter detalhes.



Note: O NGFW/FTD deve ter o mesmo número de Physical ou Sub-interface ou canal de porta igual às interfaces do Palo Alto Firewall, incluindo Sub-interfaces.



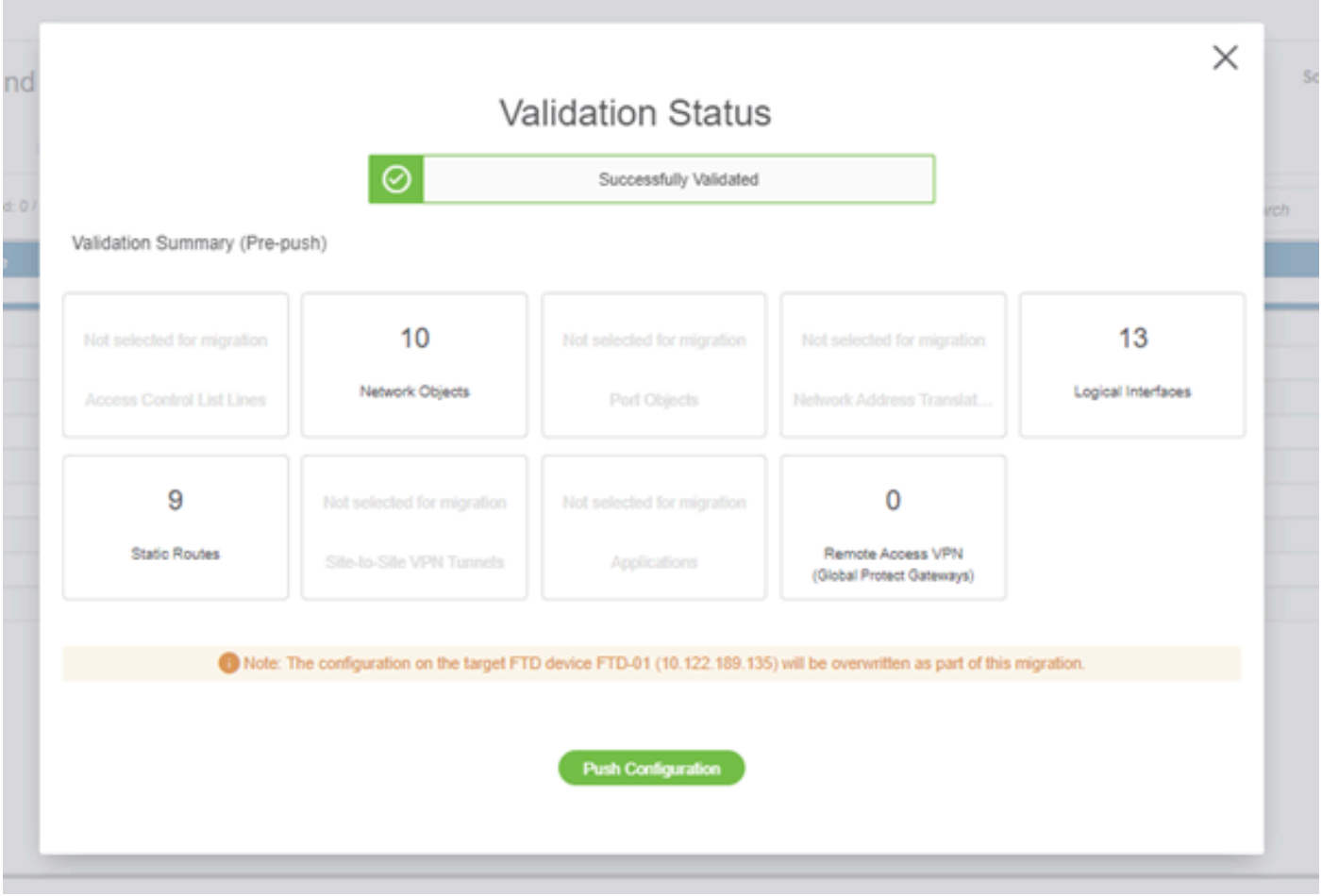
- Determine o mapeamento para regiões, que pode ser feito manualmente ou usando o recurso de criação automática. Para visualização, consulte a próxima imagem.



- Atribua seu perfil de bloqueio de aplicativos. Como este é um dispositivo de laboratório sem mapeamento de aplicativo, você pode continuar com as configurações padrão. Clique em Next e consulte a imagem fornecida.

- Otimize ACLs, objetos, interfaces e rotas conforme necessário. Como esta é uma configuração de laboratório com configurações mínimas, você pode prosseguir com as opções padrão. Em seguida, clique em Validar, fazendo referência à próxima imagem.

- Após a validação bem-sucedida, a configuração está pronta para ser implantada no FTD de destino. Consulte a próxima imagem para obter mais instruções.



- A configuração push salvará as configurações migradas no FMC e será implantada no FTD automaticamente.
- Em caso de qualquer problema durante a migração, abra um caso de TAC para obter assistência adicional.

3. Validação pós - migração

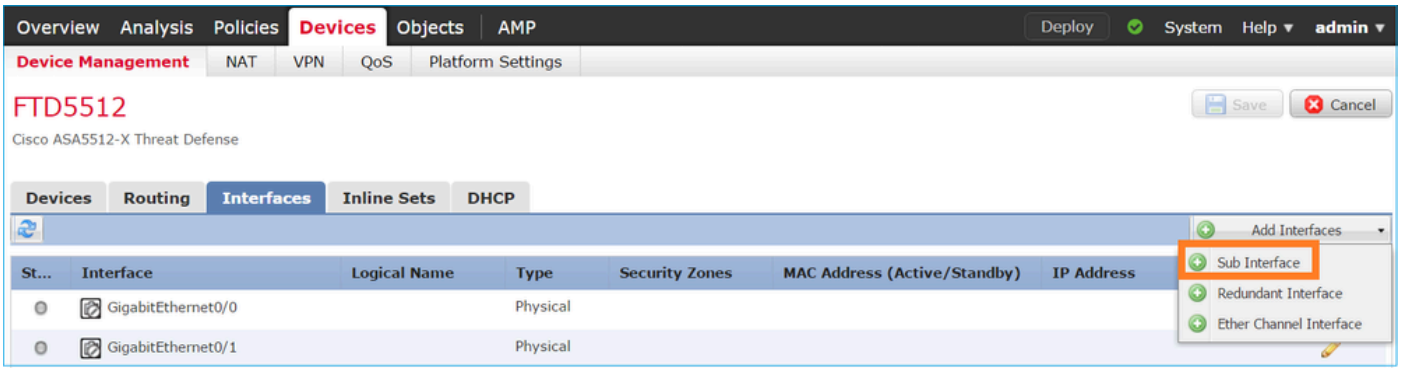
- Validação da configuração no FTD e no FMC.
- Testando as ACLs, a política, a conectividade e outros recursos avançados do dispositivo.
- Crie um ponto de reversão antes de executar qualquer alteração.
- Teste da migração no ambiente de laboratório antes do lançamento no ambiente de produção.

Problemas conhecidos

1. Interfaces Ausentes no FTD

- Faça login na CLI Palo Alto e execute o comando show interface all. Você deve ter um número igual ou maior que o número de interfaces no FTD.
- Crie um número igual ou maior de interfaces - subinterface, canal de porta ou interface física via GUI do FMC.
- Navegue até FMC GUI Device > Device Management, clique no FTD no qual a interface necessária será criada. Na seção Interface, no menu suspenso do canto direito, escolha

Create Sub-interface/BVI adequadamente e crie a interface e associe as interfaces correspondentes. Salve a configuração e sincronize com o dispositivo.



- Verifique se as interfaces são criadas no FTD executando Show interface ip brief e prossiga com a migração para o mapeamento de interface.

2. Tabela de Roteamento

- Verifique a tabela de roteamento no firewall Palo Alto executando Show routing route ou Show routing route summary.
- Antes de migrar as rotas para o FTD, verifique a tabela e escolha as rotas necessárias de acordo com a necessidade do projeto.
- Valide a mesma tabela de roteamento no FTD usando Show route all e show route summary.

3. Otimizar

- O painel Otimização de objetos está esmaecido. Às vezes, você deve criar um objeto manual no FMC e mapeá-lo. Para visualizar o objeto no FTD, use Show Running | em objetos e em Palo Alto, use Show address <object name>.
- A migração de aplicativos exige uma auditoria do firewall Palo Alto antes da migração, o FTD tem um dispositivo IPS dedicado ou você pode habilitar o recurso no FTD para que seja necessário planejar a tarefa de migração de aplicativos de acordo com os requisitos do cliente.
- A configuração NAT do firewall Palo Alto deve ser verificada por show running nat-policy e você deve ter uma política NAT personalizada em FTD, que pode ser visualizada em FTD por Show Running nat.

Conclusão

O firewall Palo Alto foi migrado com êxito para o Cisco FTD com a ajuda do FMT. Em caso de qualquer problema após a migração no FTD e para solução de problemas, abra um caso no TAC.

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.