Configurar a migração de VPN entre FTDs gerenciados por um único FMC

Contents

Introdução

Este documento descreve a migração de uma VPN Site a Site de um FTD para outro, gerenciado pelo mesmo FMC, enquanto mantém a conexão VPN com o roteador.

Pré-requisitos

Requisitos

Para realizar o processo de migração com eficiência, a Cisco recomenda estar familiarizada com os seguintes tópicos:
· Registro do FTD junto do FMC: Compreendendo como registrar dispositivos de Defesa contra ameaças (FTD) do Firepower com o Firepower Management Center (FMC).
· Configuração de VPN site a site: Experiência na configuração de VPNs site a site em dispositivos FTD gerenciados pelo FMC.

Componentes Utilizados

Este documento é baseado nas versões de software e hardware fornecidas:
· Defesa contra ameaças do Firepower Virtual (FTDv): Duas instâncias executando a versão 7.3.1.
· Firepower Management Center (FMC): Versão 7.4.0.

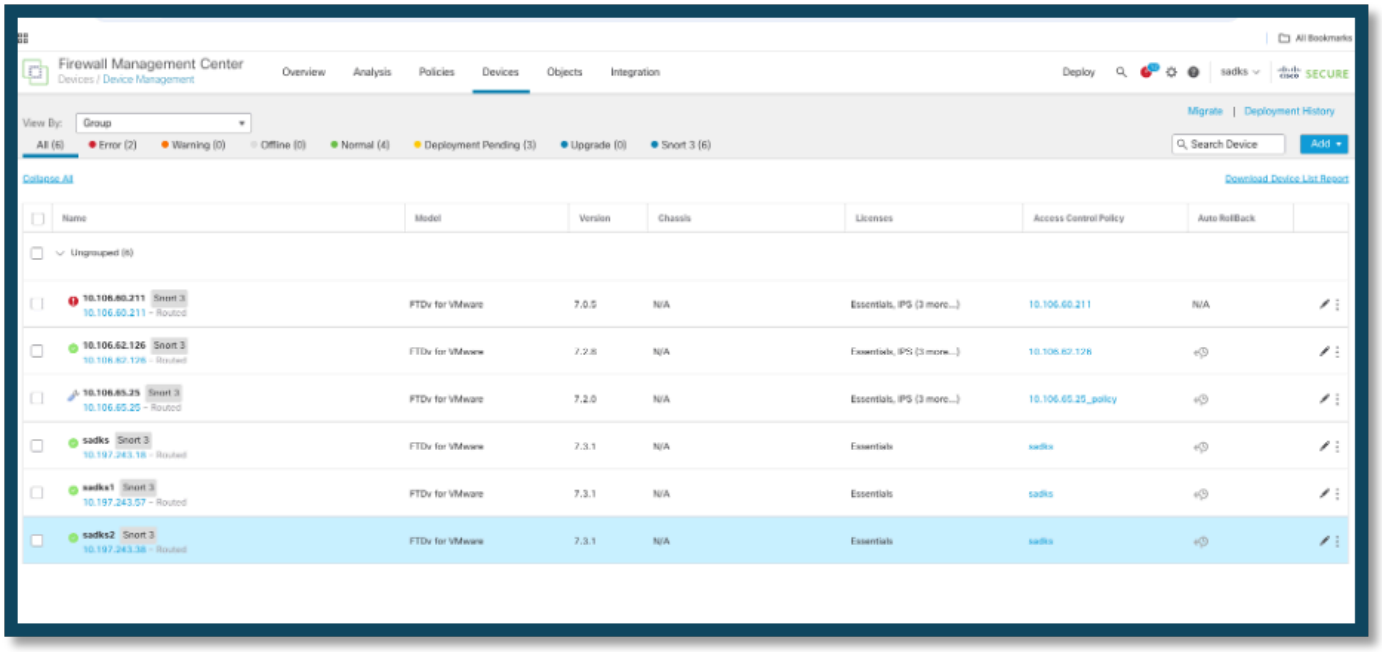
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Configurar

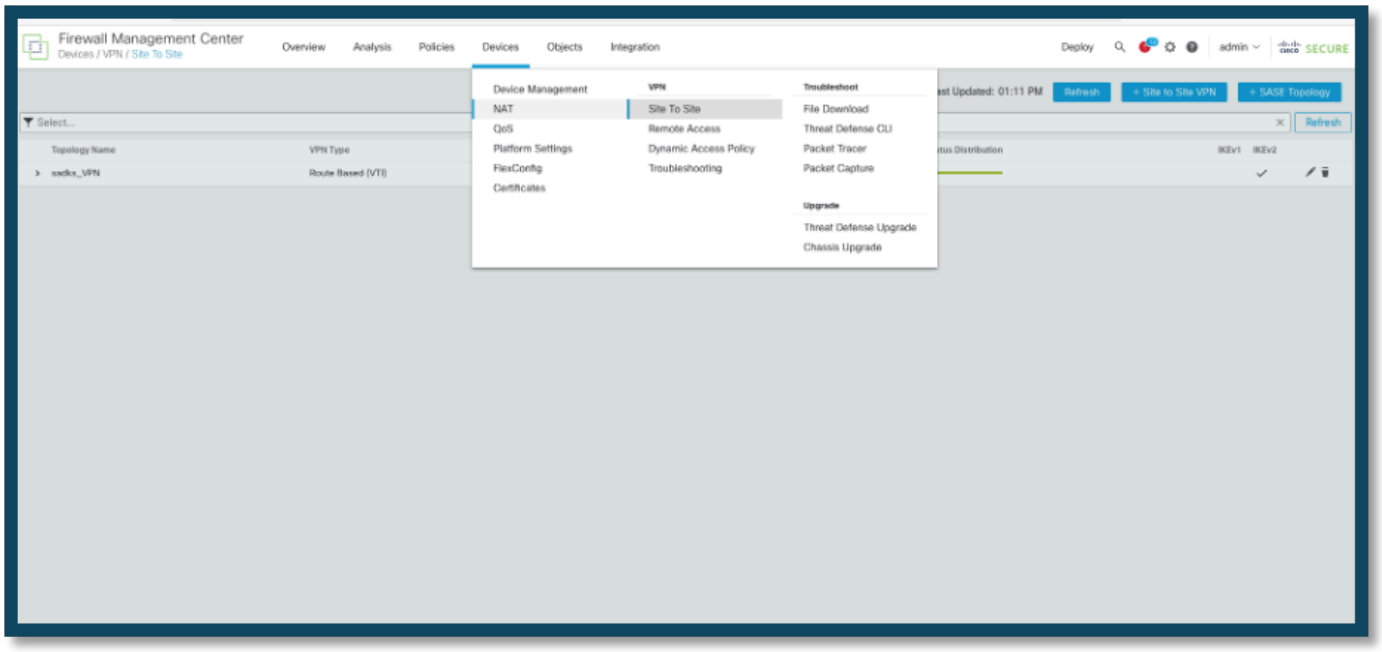
Procedimento

1. Registrar o novo DTF junto do CVP:
   · Comece registrando o novo dispositivo Firepower Threat Defense (FTD) no Firepower Management Center (FMC) em Devices > Device Management.
   · Neste exemplo, o novo dispositivo registrado é chamado "sadks2".



Novo FTD registrado

2. Acesse a configuração do túnel de site a site:
   · Navegue até as configurações de túnel de site a site em Devices > Site to Site na interface do FMC.

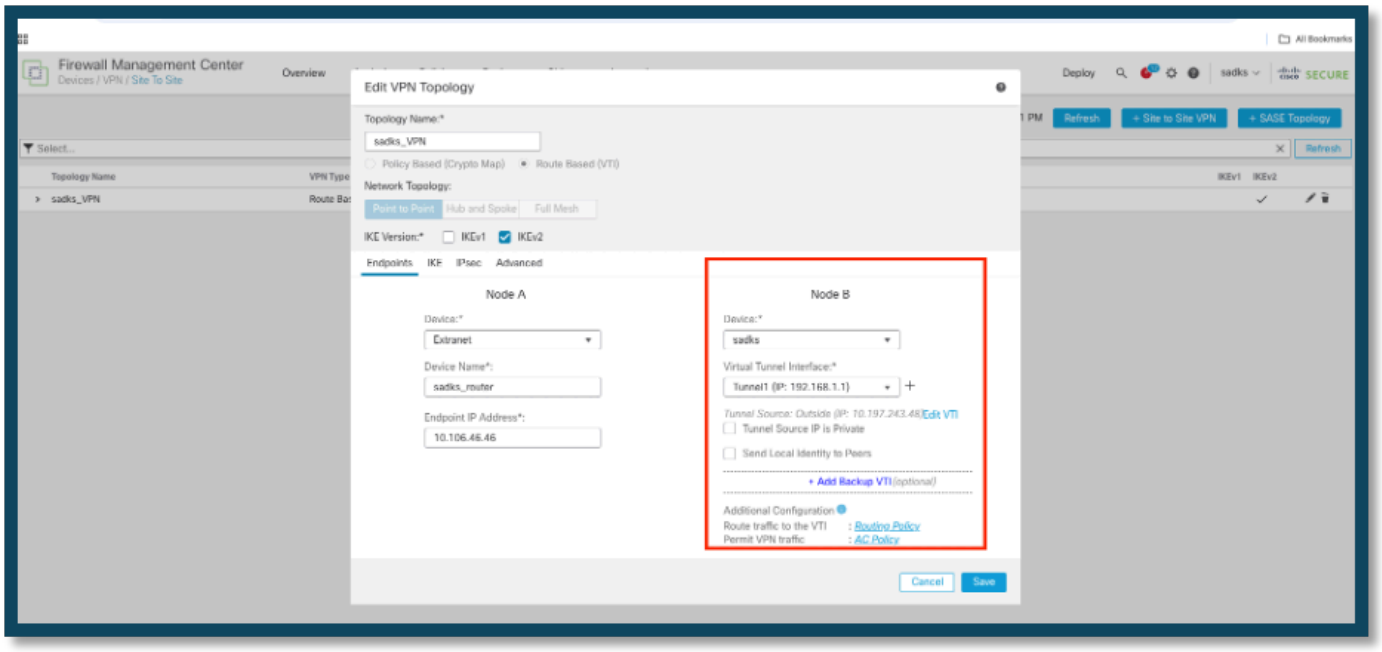


Navegue até VPN Config

3. Modificar a configuração da VPN:

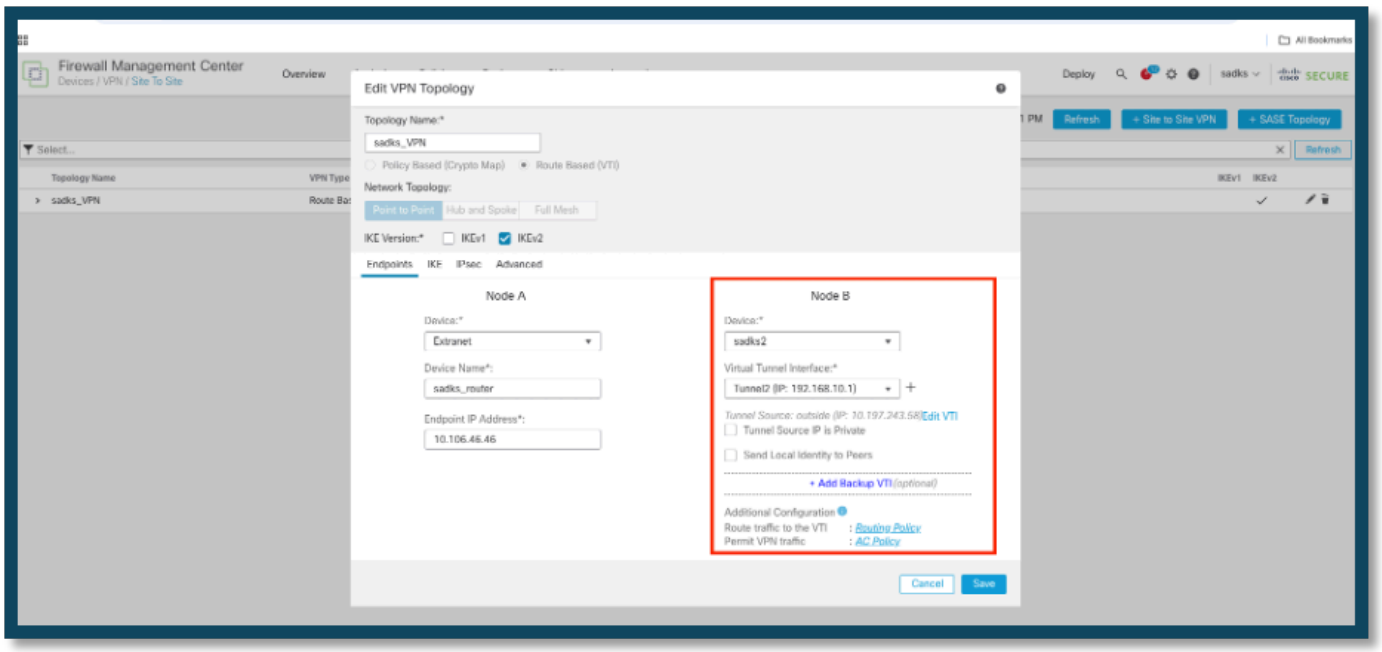
· Selecione a configuração VPN que pretende atualizar.

•Exemplo: Neste cenário, a configuração da VPN envolve um dispositivo FTD e um roteador. Aqui, o Nó B representa o dispositivo FTD, e a configuração foi atualizada para alterar a associação do dispositivo de "sadks" para "sadks2".



Dispositivo FTD antigo

PARA



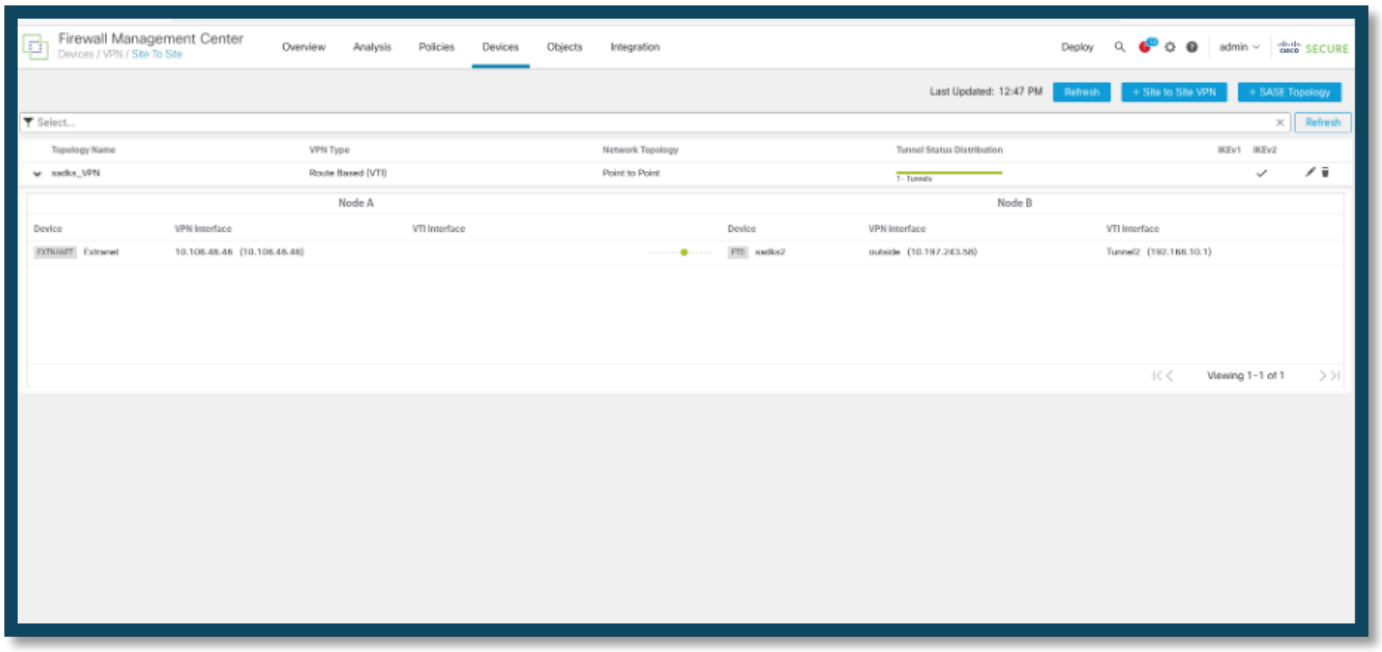
Novo dispositivo FTD

4. Salvar e Implantar a Configuração:

· Depois de fazer as alterações necessárias, salve a configuração e implante-a para ativar as atualizações.

Verificar

O túnel é ativado após a implantação.



Status do túnel

Troubleshooting

Problemas iniciais de conectividade

Ao construir uma VPN, há dois lados negociando o túnel. Portanto, é melhor obter ambos os lados da conversa quando você solucionar qualquer tipo de falha de túnel. Um guia detalhado sobre como depurar túneis IKEv2 pode ser encontrado aqui: Como depurar VPNs IKEv2

A causa mais comum de falhas de túnel é um problema de conectividade. A melhor maneira de determinar isso é fazer capturas de pacotes no dispositivo. Use este comando para fazer capturas de pacotes no dispositivo:

<#root>

capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58

Quando a captura estiver em vigor, tente enviar o tráfego pela VPN e verifique o tráfego bidirecional na captura de pacotes.

Revise a captura de pacotes com este comando:

<#root>

show cap capout

Problemas específicos de tráfego

Os problemas comuns de tráfego que você enfrenta são:

- Problemas de roteamento por trás do FTD — a rede interna não consegue rotear os pacotes de volta para os endereços IP e clientes VPN atribuídos.
- Listas de controle de acesso bloqueando o tráfego.
- A Tradução de Endereço de Rede não está sendo ignorada para tráfego VPN.

Para obter mais informações sobre VPNs no FTD gerenciado pelo FMC, você pode encontrar o guia de configuração completo aqui: FTD gerido pelo guia de configuração do FMC

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.