Configure o acesso seguro com o Secure Firewall Threat Defense para acesso privado com roteamento baseado em políticas

Contents

Introdução

Este documento descreve como configurar o Acesso Seguro com FTD via IPsec para Acesso Privado Seguro com Roteamento Baseado em Política.

Pré-requisitos

Requisitos

- Conhecimento sobre o Cisco Secure Access
- Painel/locatário do Cisco Secure Access
- Conhecimento do Secure Firewall Threat Defense e do Firewall Management Center
- conhecimento de IPsec
- Conhecimento de roteamento baseado em políticas

Componentes Utilizados

- Secure Firewall executando o código 7.7.10
- Centro de gerenciamento de firewall fornecido em nuvem. A configuração também se aplica ao FMC virtual típico
- Painel do Cisco Secure Access

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

Os túneis de rede no Secure Access podem ser usados para duas finalidades principais: Acesso seguro à Internet e acesso privado seguro.

Para acesso privado seguro, as organizações podem aproveitar o acesso zero confiável (ZTA) e/ou VPN como serviço (VPNaaS) para conectar usuários a recursos privados, como aplicativos internos ou data centers. Os túneis IPsec desempenham um papel fundamental nessa arquitetura, criptografando com segurança o tráfego de rede entre usuários e recursos privados, garantindo que os dados confidenciais permaneçam protegidos enquanto atravessam redes não confiáveis. Ao integrar túneis IPsec com ZTA ou VPNaaS, as organizações podem fornecer acesso seguro e contínuo a recursos internos, mantendo controles de segurança e visibilidade robustos.

Este documento descreve como configurar o Acesso Seguro com o Secure Firewall Threat Defense (FTD) via IPsec para Acesso Privado Seguro.
Além disso, este guia fornece etapas para configurar o Roteamento Baseado em Políticas.

Embora este documento aborde a configuração de túneis IPsec para acesso privado seguro, a configuração de acesso zero confiável (ZTA) ou VPN como um serviço (VPNaaS) para acessar aplicativos privados está fora do escopo deste guia.

Configurar

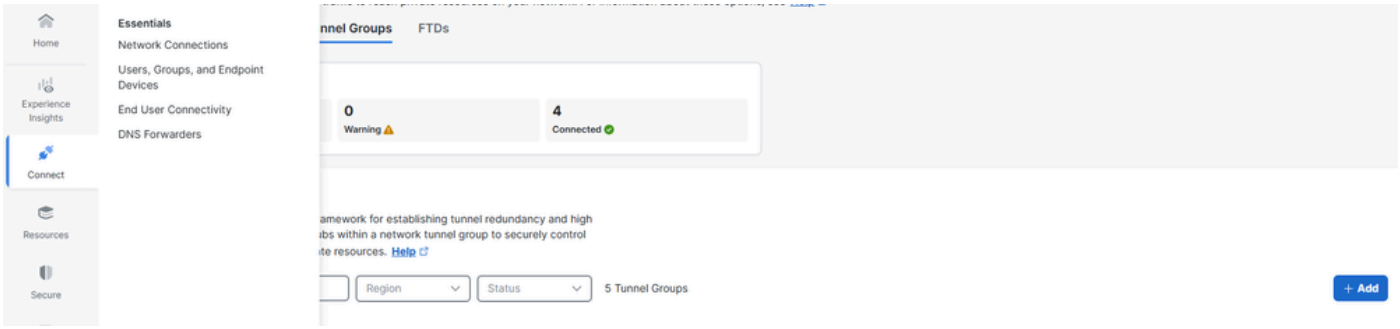
Configuração de acesso seguro

Configuração do grupo de túneis de rede

1. Navegue até o painel de administração do Secure Access.

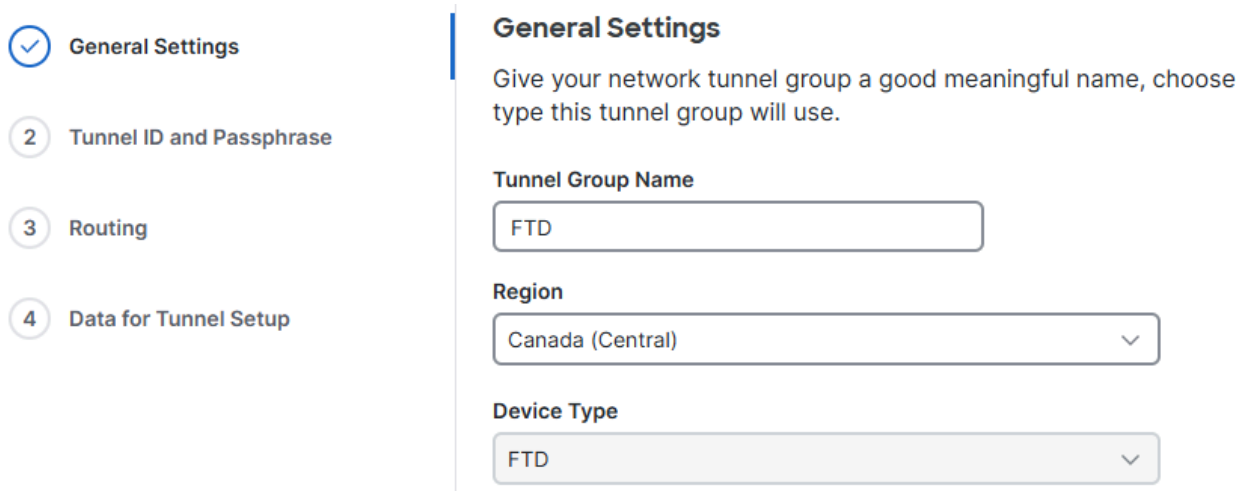
2. Adicione um Grupo de Túneis de Rede.

- Clique emConnect> Network Connections
  - Em Network Tunnel Groups , clique em > Add



3. General Settings Configuração.

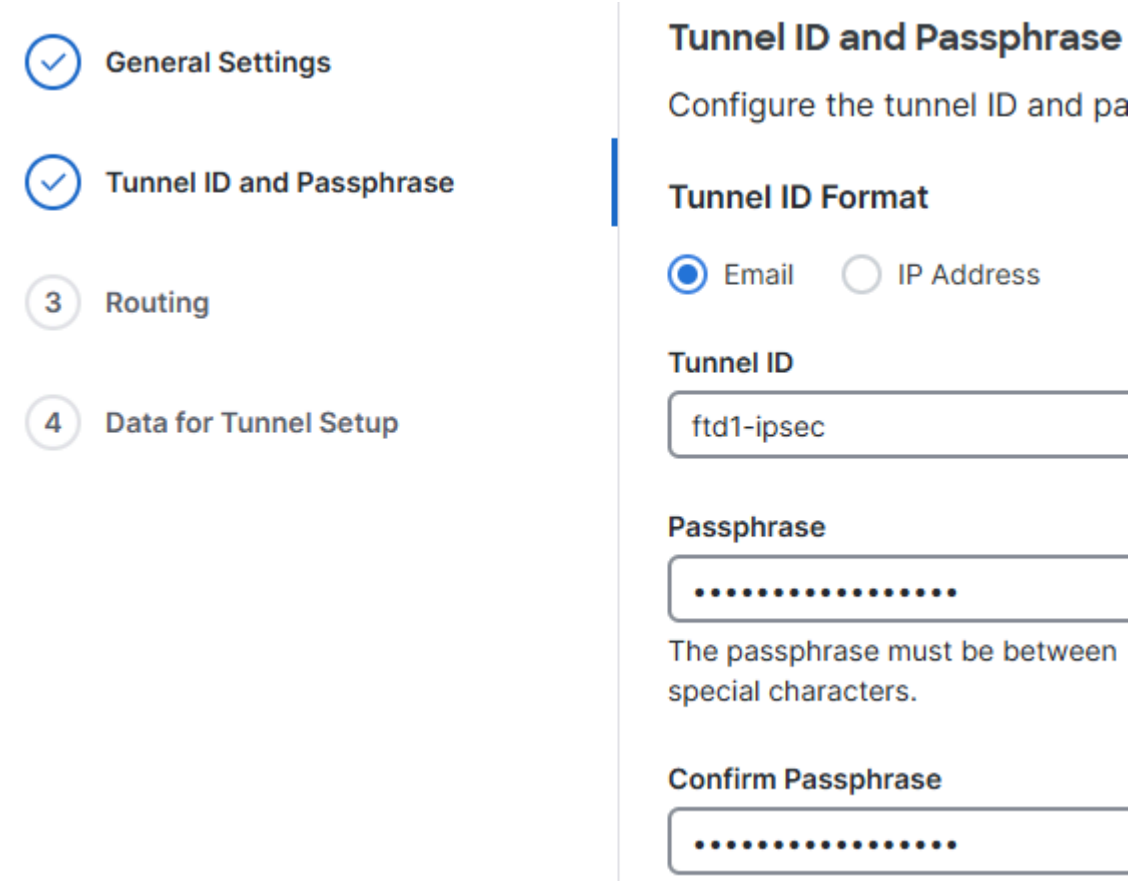
- Configure o Tunnel Group Name **Region** e Device Type
  - Clique em Next



Configurações gerais

4. Configure Tunnel ID e Passphrase.

- Configure o **Tunnel ID**ePassphrase. Esse ID é importante, pois é necessário para a configuração do FTD
- Clique em Next



ID e PSK

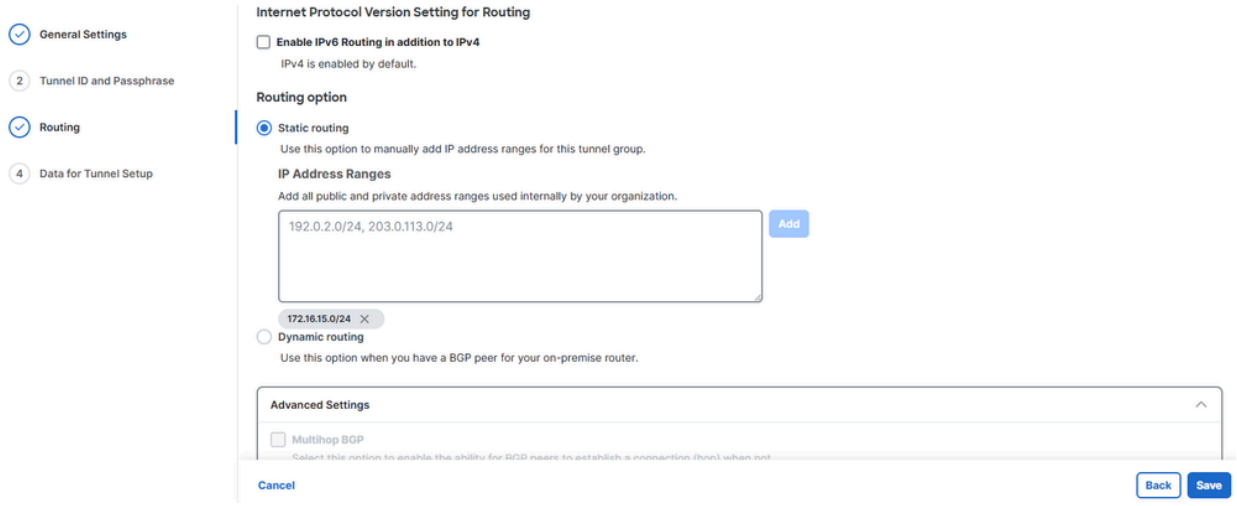
5. Configure o Roteamento Estático.

Roteamento de acesso seguro

Roteamento baseado em políticas

Adicione a(s) rede(s) protegida(s) pelo FTD que você deseja que os usuários remotos acessem via ZTA e/ou VPNaaS e clique em Salvar.

- Clique em Routing> **Static routing**
  - Adicione os intervalos de endereços IP ou hosts configurados na rede e deseje passar o tráfego pelo Secure Access e clique emAdd
  - Clique emSave

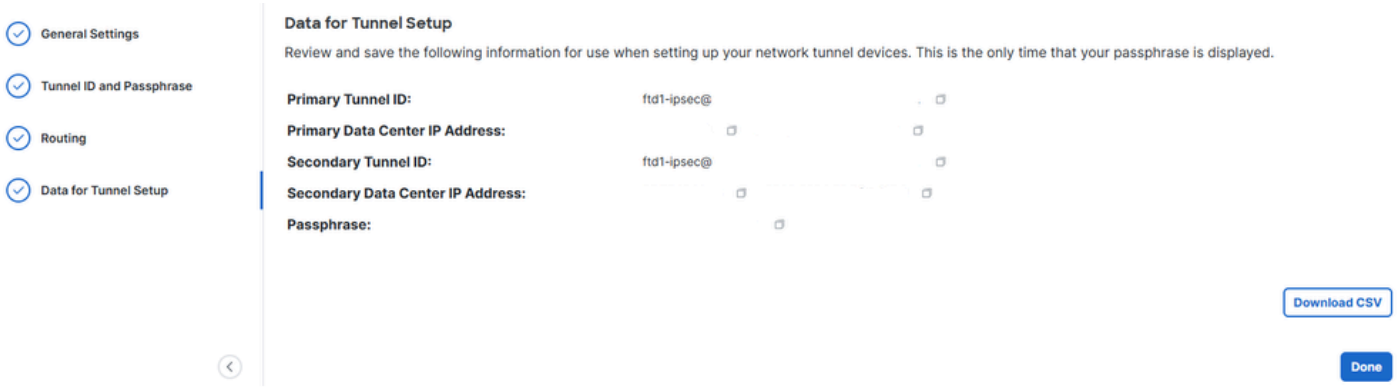


Roteamento estático CSA

Salvar configuração do grupo de túneis de rede

Faça o download e salve os dados de configuração do túnel, conforme necessário para a configuração do FTD.

- Clique em Download CSV
- Clique em Done



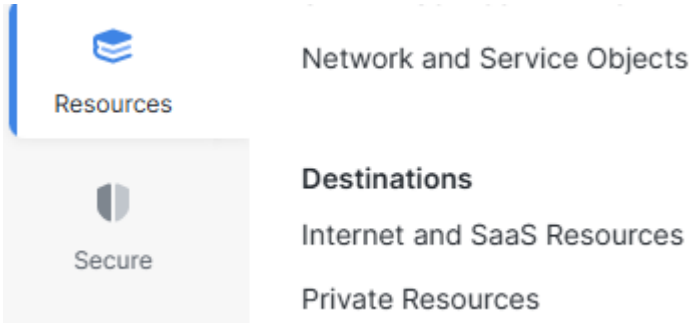
Dados de NTG

Criar um recurso privado

Os recursos privados são aplicativos internos, redes ou sub-redes hospedadas no seu ambiente de data center ou nuvem privada. Esses recursos não são acessíveis publicamente e são protegidos por trás da infraestrutura da sua organização.

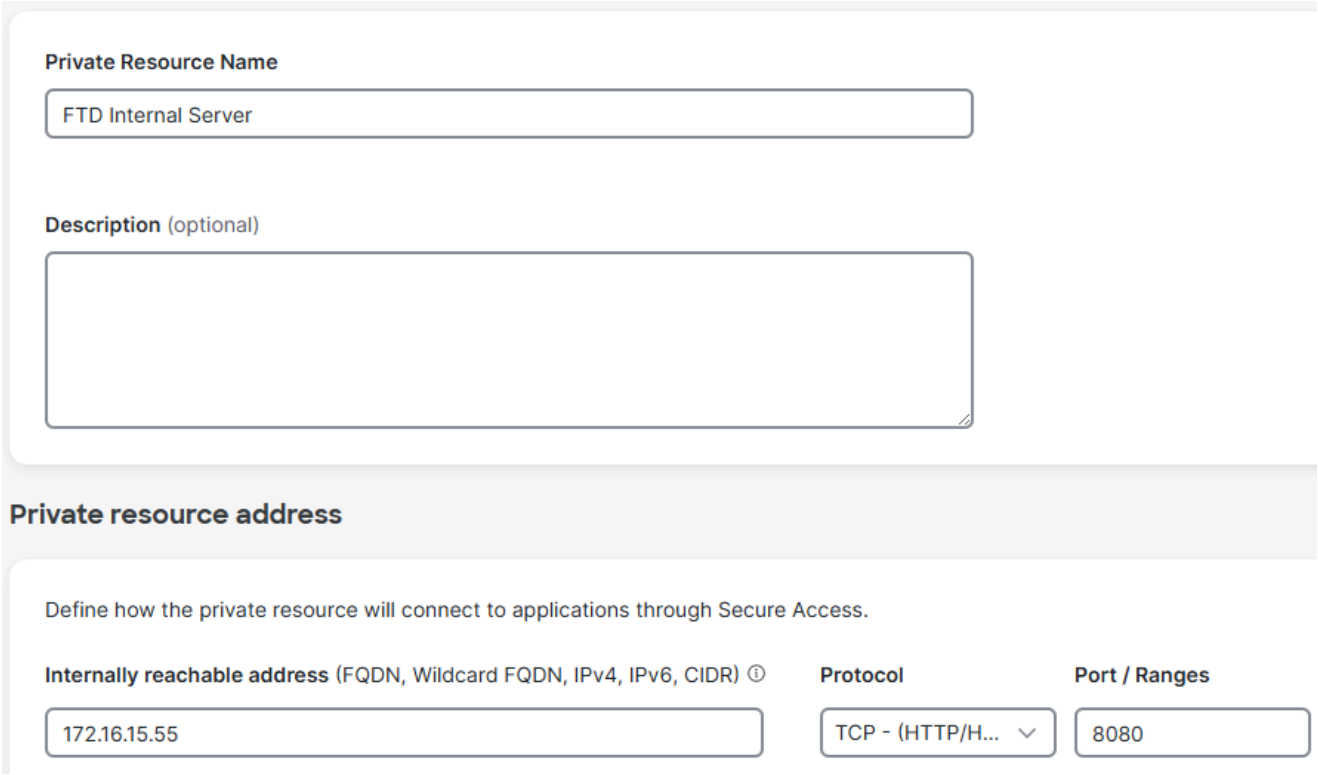
Ao defini-los como recursos privados no acesso seguro, você pode habilitar o acesso controlado por meio de soluções como ZTA (Zero Trust Access) ou VPN como serviço (VPNaaS). Isso garante que os usuários possam se conectar com segurança a sistemas internos com base em identidade, postura de dispositivo e políticas de acesso, sem expor os recursos diretamente à Internet.

Navegue para **Resources** > **Private Resources**> clique em Add.



PR

- Especifique **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Especificar portas e protocolos e adicionar recursos privados adicionais conforme necessário
- Selecione as conexões desejadas Connection Method com base em suas necessidades, por exemplo, conexões Zero-trust e/ou conexões VPN, de acordo com seus requisitos
- Clique em Save



Recurso privado

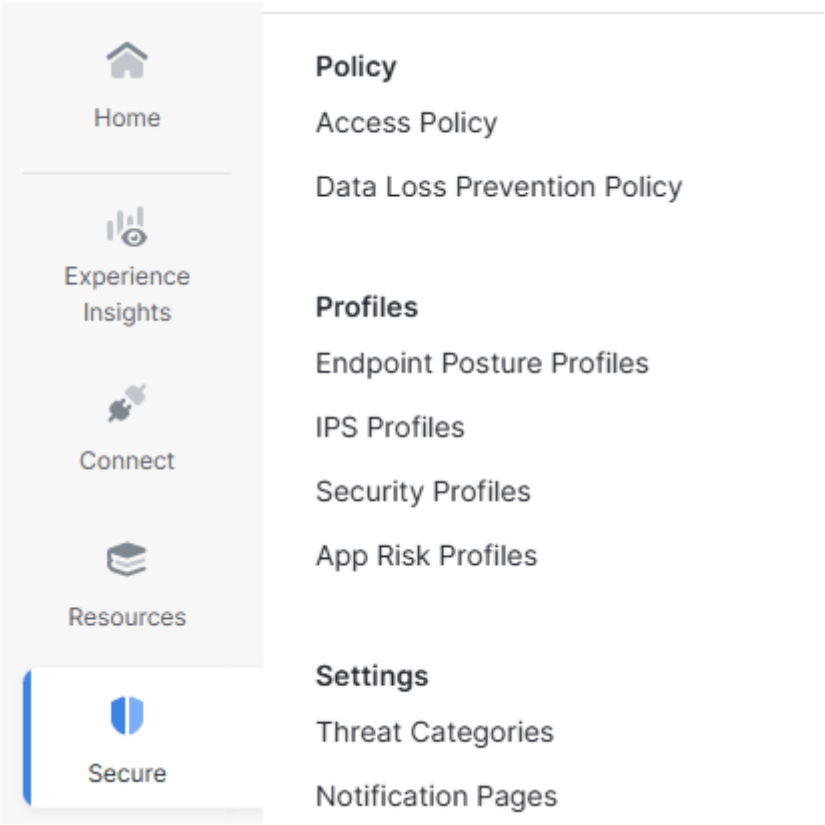
Criar uma Regra de Política de Acesso

As regras de acesso privado definem como os usuários podem se conectar com segurança a recursos internos e aplicativos que não são acessíveis publicamente.

Essas regras reforçam a segurança ao controlar quem pode acessar recursos privados específicos com base em fatores como identidade do usuário, associação do grupo, postura do

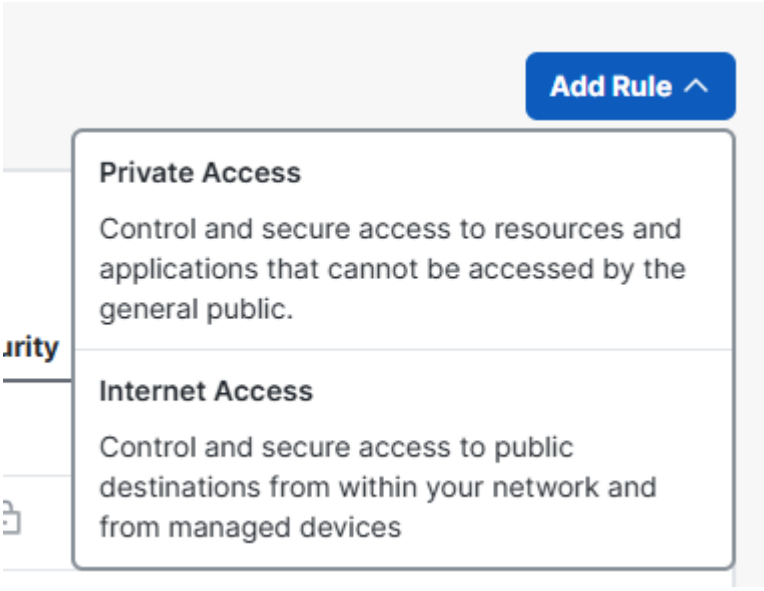
dispositivo, local ou outras condições da política. Isso garante que os sistemas internos confidenciais permaneçam protegidos do acesso público geral enquanto ainda estão disponíveis com segurança para usuários autorizados por meio de ZTA ou VPNaaS.

Navegue até Secure>Access Policy



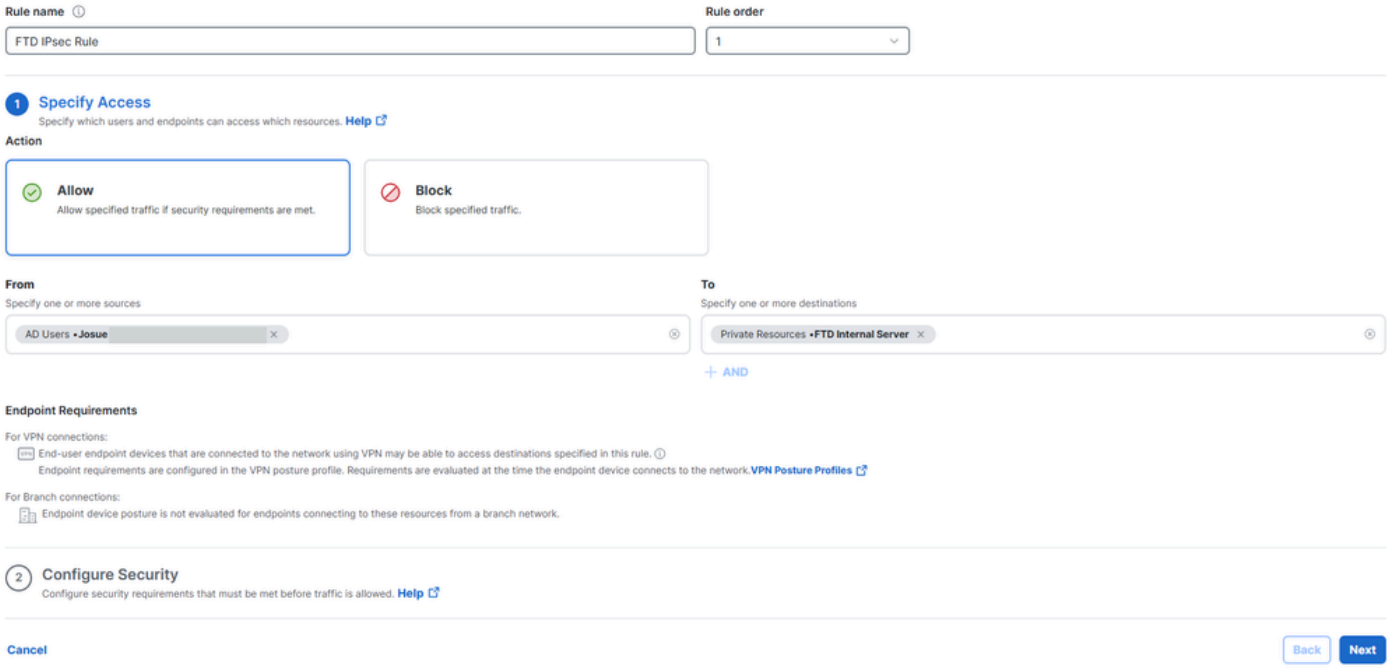
ACP

- Clique em Add Rule
  - Clique em Private Access



Adicionar ACP

- Clique em Rule Name e dê um nome a ele
- Clique emAction, selecione para permitir Allowo tráfego
- CliqueFromem e especifique os usuários que recebem permissão
- Clique em Toe especifique o acesso que esses usuários têm com base nesta regra
- Clique emNexte, em seguida, Savena próxima página



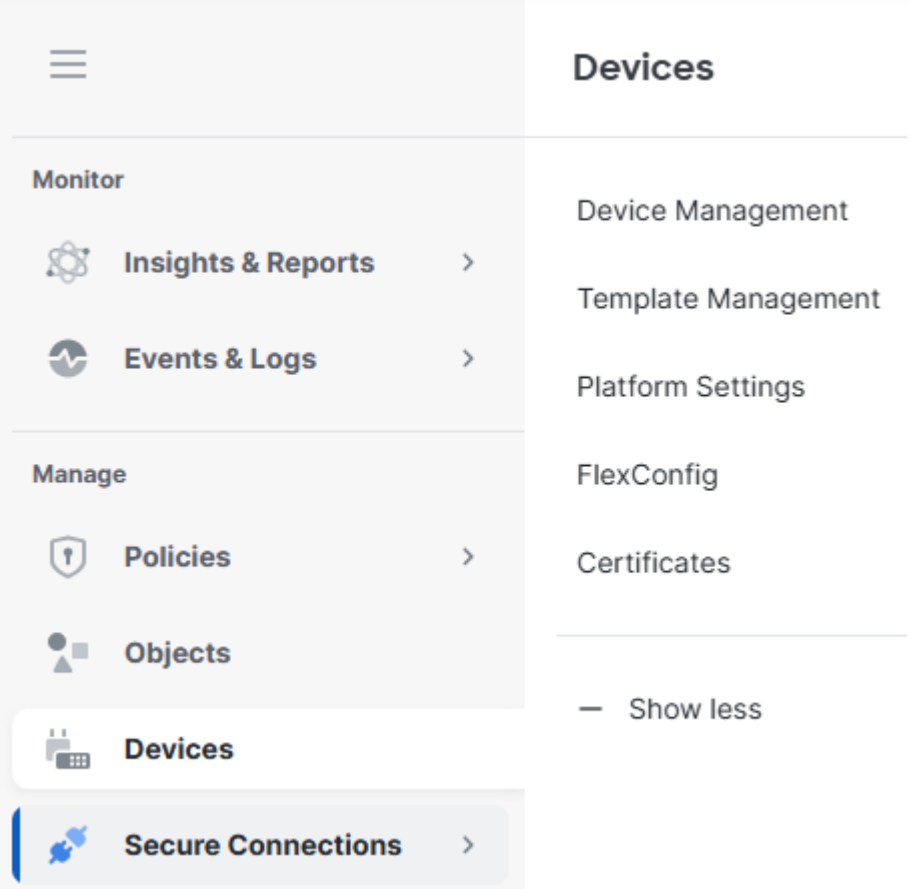
configuração de ACP

Configuração do Secure Firewall Threat Defense (FTD)

Configuração de interfaces de túnel virtual

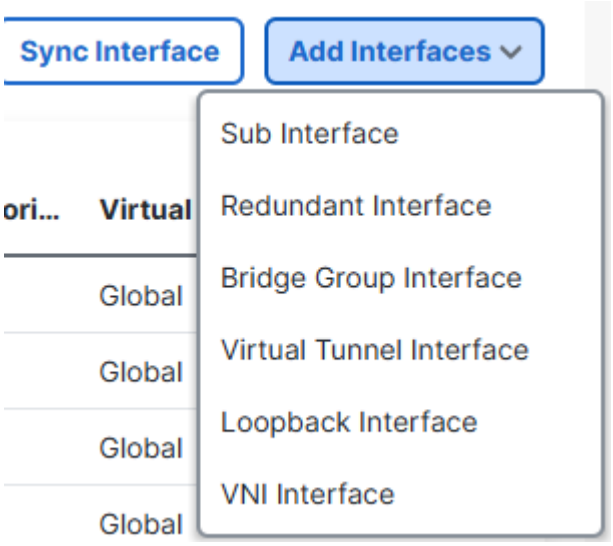
Uma Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) em FTD é uma interface lógica de Camada 3 usada para configurar túneis VPN IPsec baseados em rota.

1. Navegue até Devices> Device Management.



Dispositivos FTD

- Clique no dispositivo FTD, Interfaces
  - Clique em Add Interfaces
  - Clique em Virtual Tunnel Interface
  - Crie duas interfaces de túnel virtual, uma para o hub de acesso seguro primário e outra para o hub de acesso seguro secundário

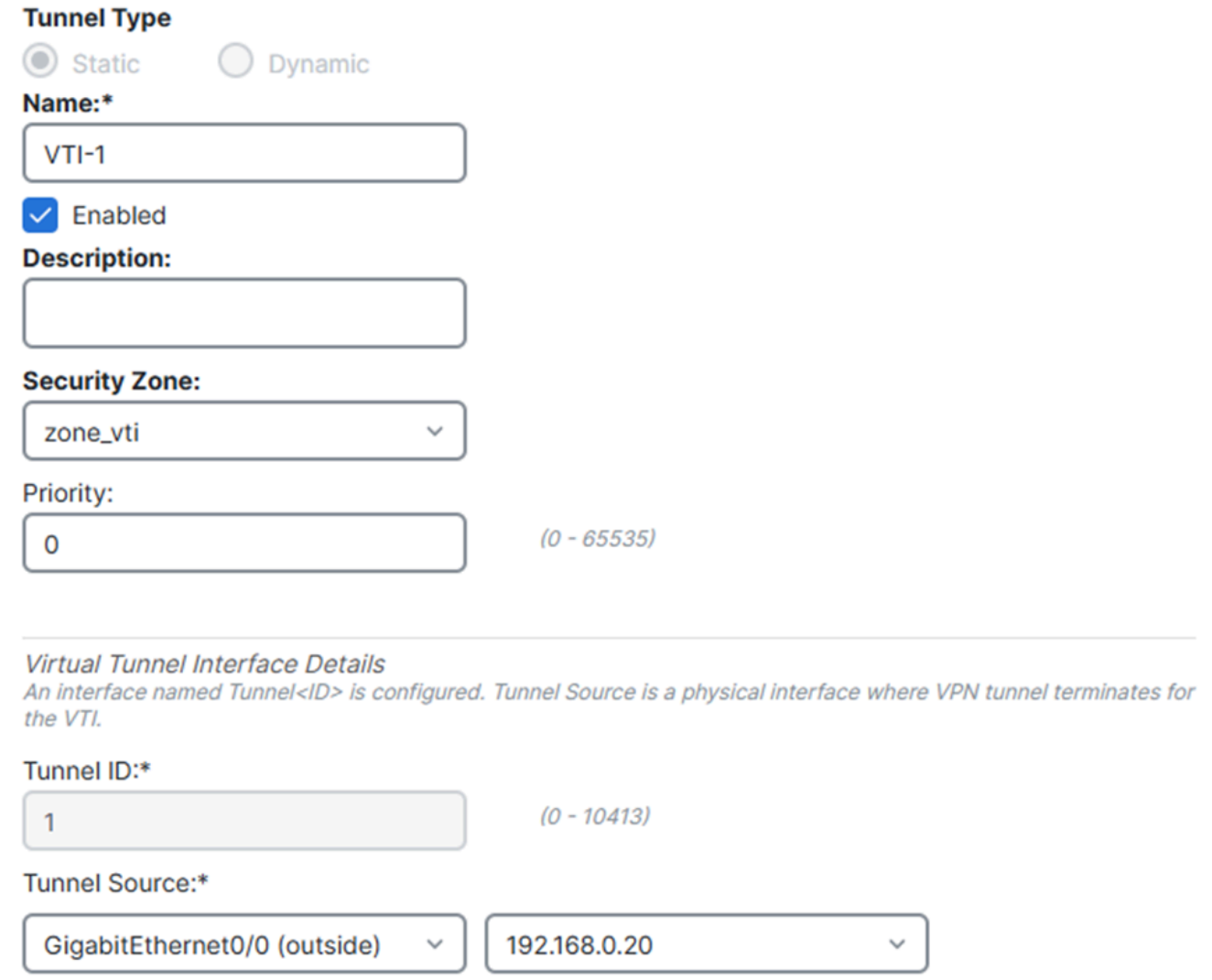


Adicionar VTIs

Interface de túnel virtual 1:

- Dê um nome, clique em Enable

- Selecione ou crie um Security Zone
- Clique em Tunnel ID e atribua um valor a ele.
- Clique Tunnel Source e especifique a interface WAN a partir da qual o túnel será estabelecido
- Clique em IPsec Tunnel Modee selecioneIPv4
- Clique em IP Address e configure o endereço IP para o VTI
- Clique emOK

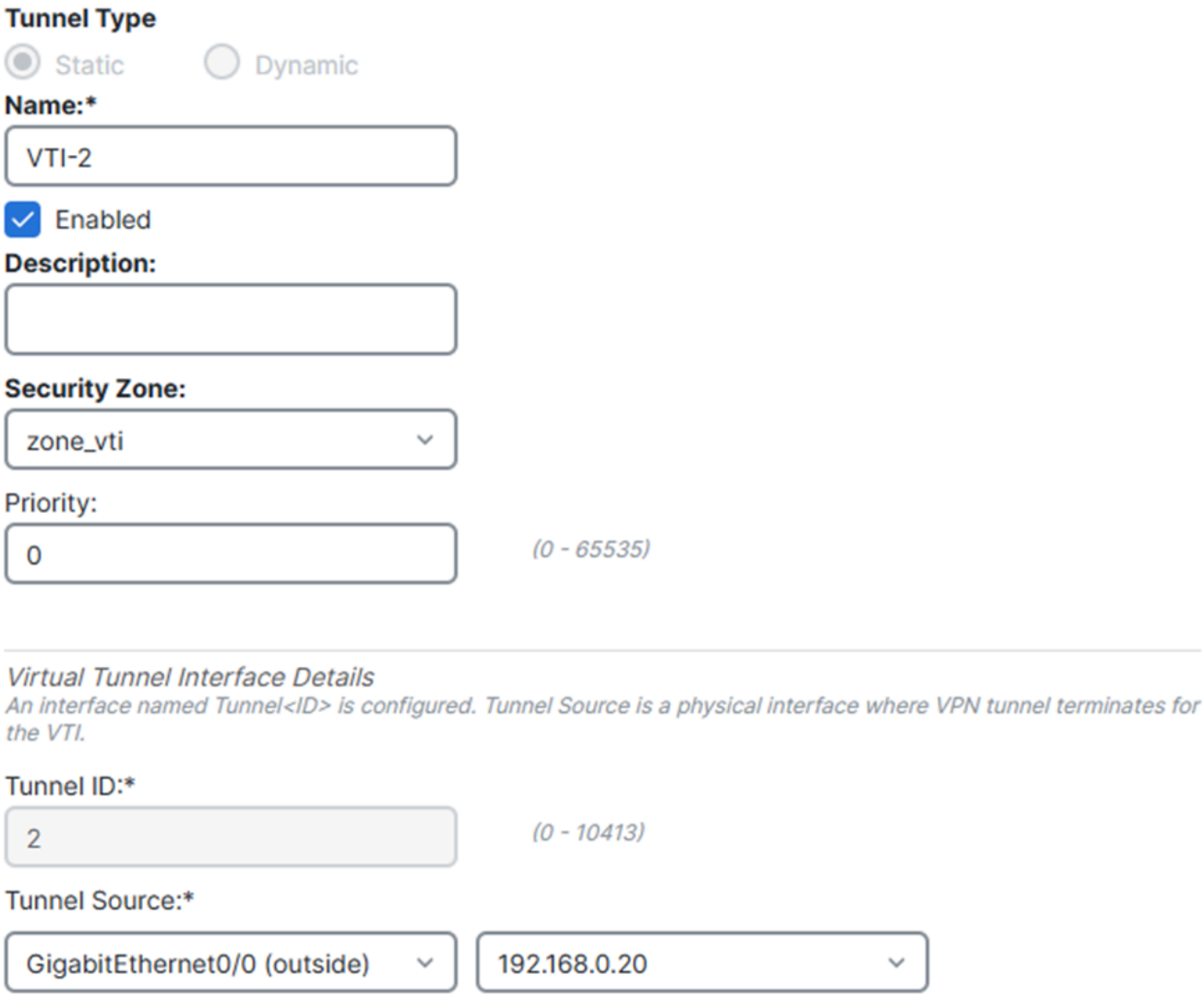


VTI1.1

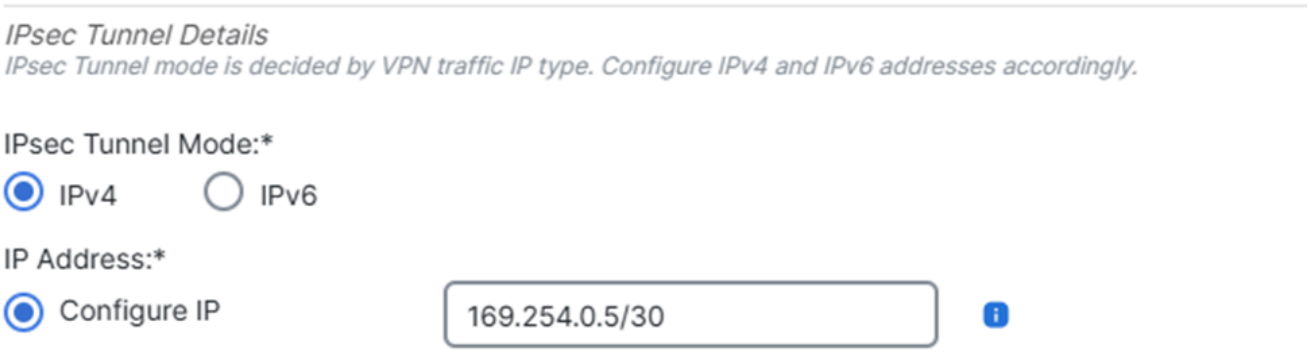
VTI1.2

Interface de túnel virtual 2:

- Dê um nome, clique em Enable
- Selecione ou crie um Security Zone
- Clique em Tunnel ID e atribua um valor
- Clique Tunnel Source e especifique a interface WAN a partir da qual o túnel será estabelecido
- Clique em IPsec Tunnel Modee selecioneIPv4
- Clique em IP Address e configure o endereço IP para o VTI
- Clique emOK

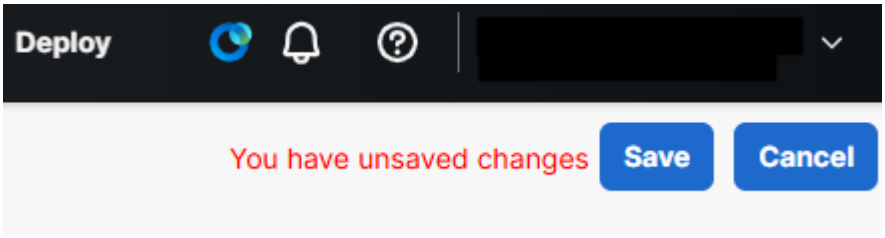


VTI2.1



VTI2.2

- Clique em Save.

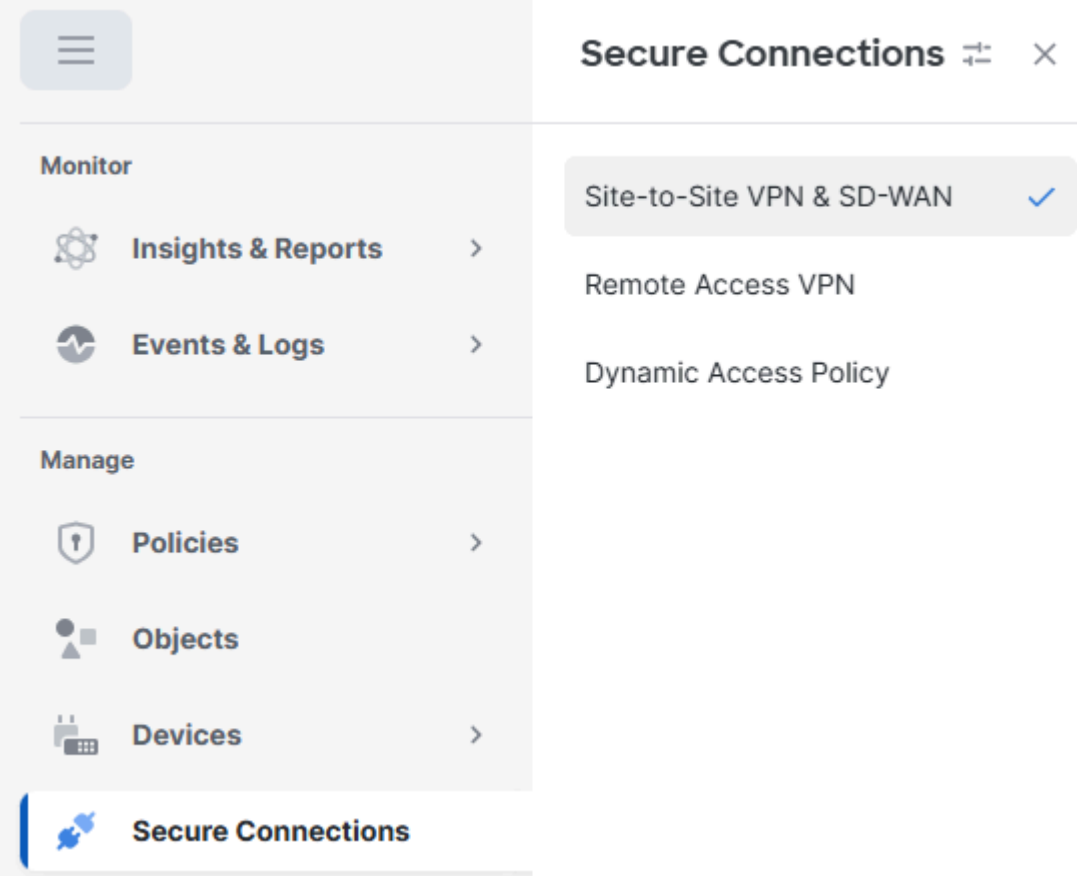


Salvar alterações de VTI

Configuração de túnel IPsec

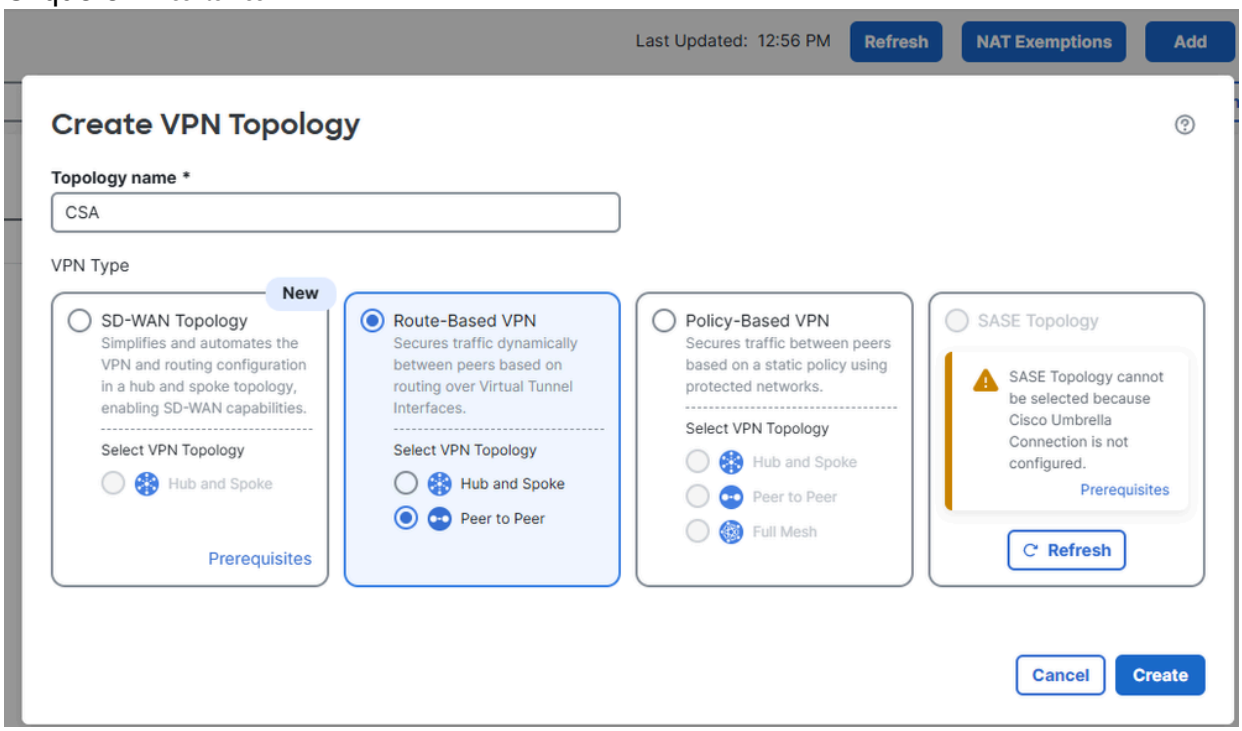
Navegue até o painel do cdFMC.

- Clique em Secure Connection> Site-to-Site VPN & SD-WAN



S2S

- Clique emAdd
  - Clique em Route-Based VPN
  - Clique em Peer to Peer

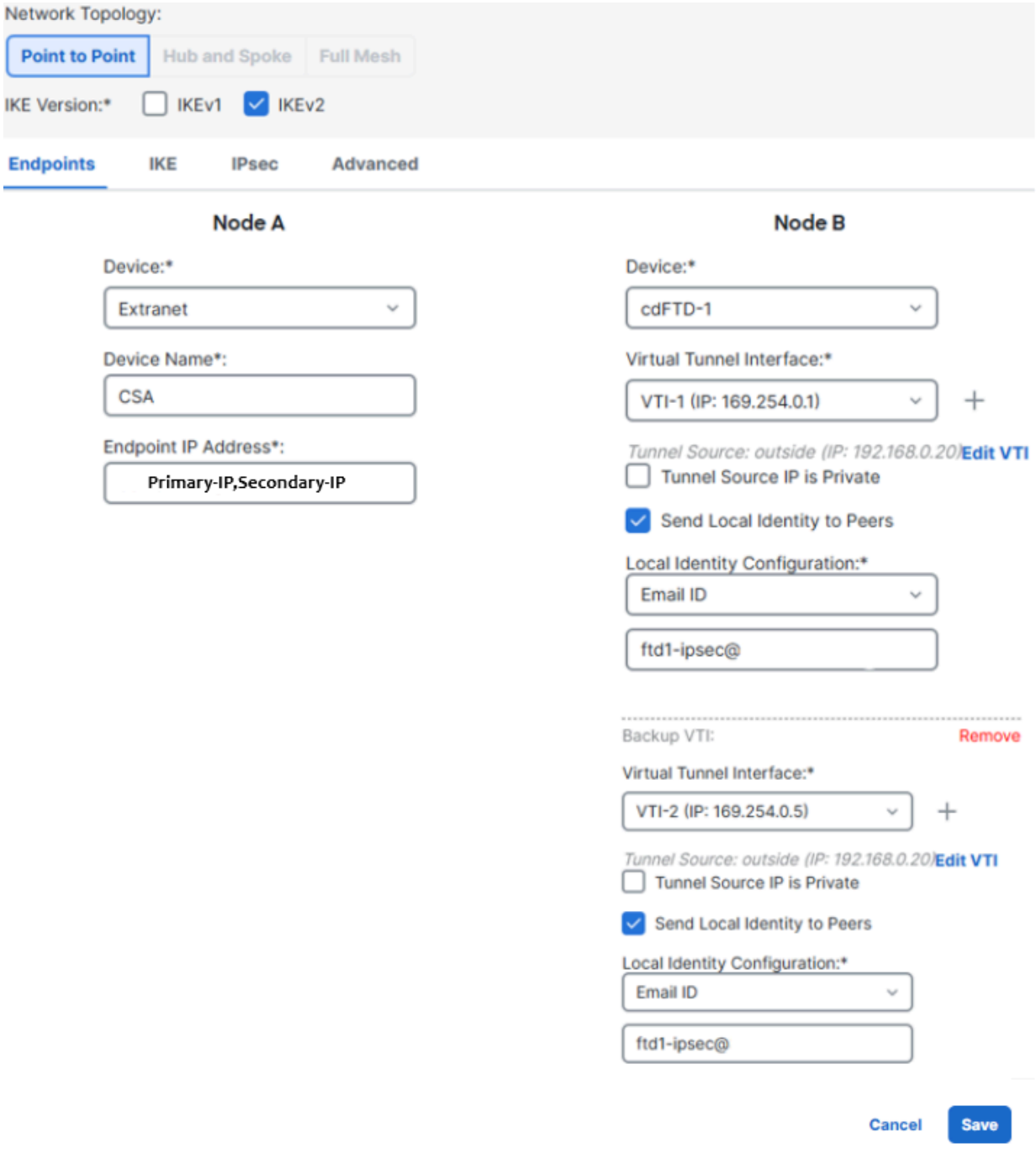


Adicionar VPN

- Na etapa 5 da configuração Secure Access, obtenha as IDs do túnel e os endereços IP dos

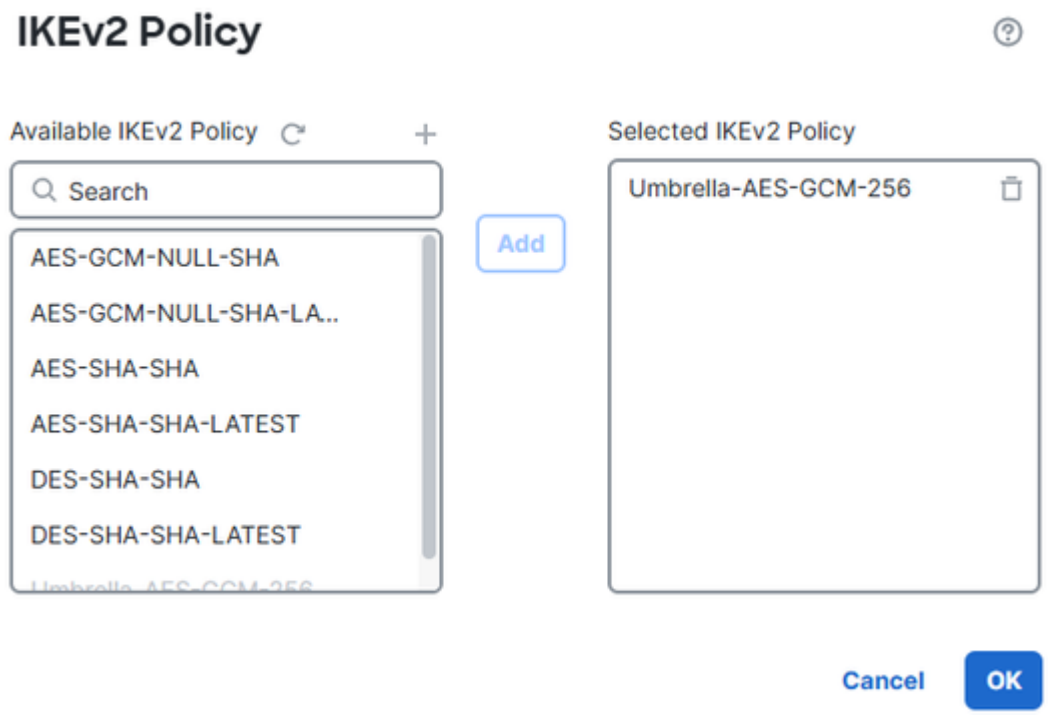
data centers principal e secundário

- Clique emEndpoints
  - EmNode A, cliqueDeviceem e selecione Extranet
  - Clique em Device Namee dê um nome a ele
  - Clique em Enpoint IP Addresses e insira os endereços IP primários e secundários de acesso seguro separados por vírgula (em "Save Network Tunnel Group Configuration", em Acesso seguro
    Configuração)
  - Em Node B, clique emDevicee selecione seu dispositivo FTD
  - Clique em Virtual Tunnel Interface e selecione a primeira interface VTI criada na etapa anterior
  - Clique na Send Local Identity to Peers opção e selecioneEmail ID, insira o ID do túnel principal (em "Save Network Tunnel Group Configuration" na Secure Access Configuration)
  - Clique em Add Backup VTI
  - Clique em Virtual Tunnel Interface e selecione a segunda interface VTI criada na etapa anterior
  - Clique emSend Local Identity to Peersonoption e selecioneEmail ID, enter the secondary tunnel ID (from "Save Network Tunnel Group Configuration" under the Secure Access Configuration)
  - Clique em Salvar



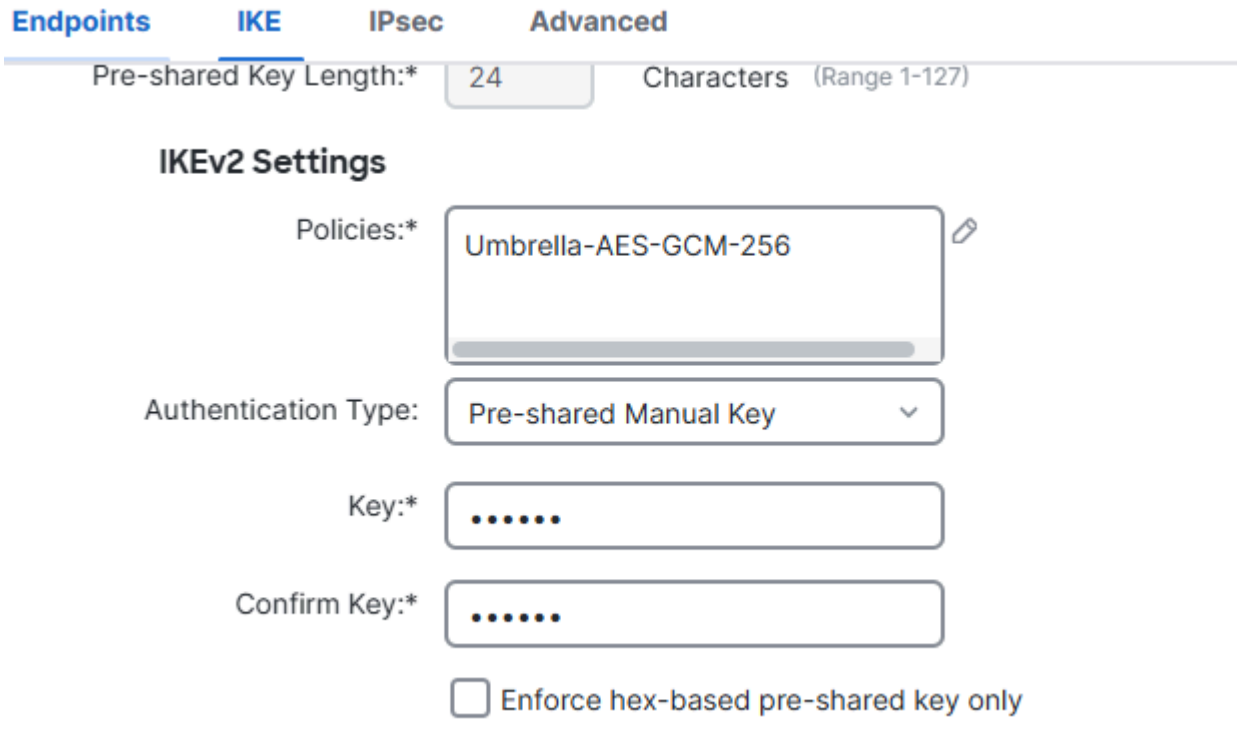
configuração de FTD VTI

- Clique emIKE
  - Clique em **IKEv2 Settings >** Policies
  - Selecione aUmbrella-AES-GCM-256opção
  - Clique em OK



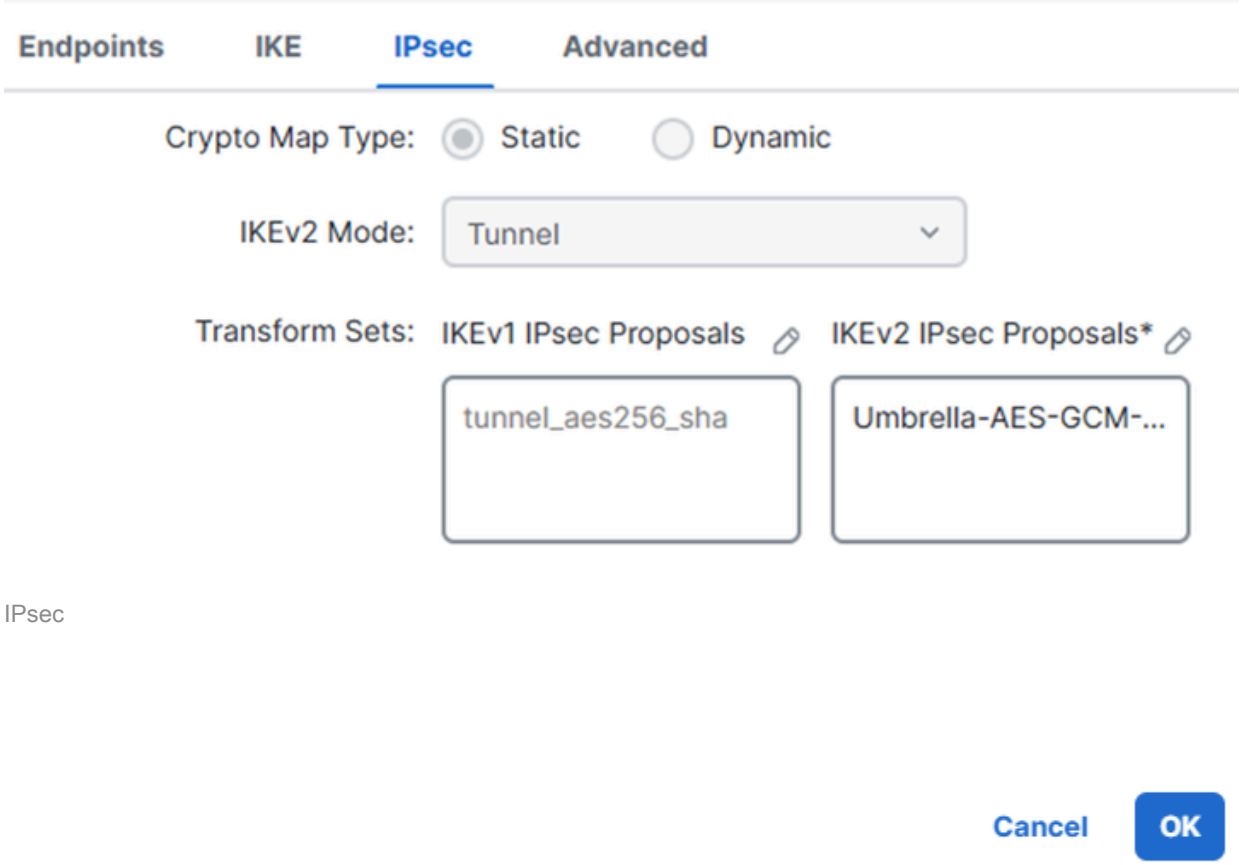
Política IKEv2

- Clique em Authentication Type e selecionePre Shared Manual Key, insira a PSK configurada em Secure Access (senha)



IKE

- Clique em IPSEC
  - Clique em IKEv2 Proposals
  - Selecionar Umbrella-AES-GCM-256
  - Clique em OK



IPsec

Salvar propostas IKEv2

Configuração de roteamento FTD

O Roteamento Baseado em Políticas (PBR - Policy-Based Routing) permite que você controle o encaminhamento de tráfego com base em critérios além do endereço IP de destino. Em vez de depender exclusivamente da tabela de roteamento, o PBR pode rotear o tráfego com base na origem, no aplicativo, no protocolo, nas portas ou em outras políticas definidas.

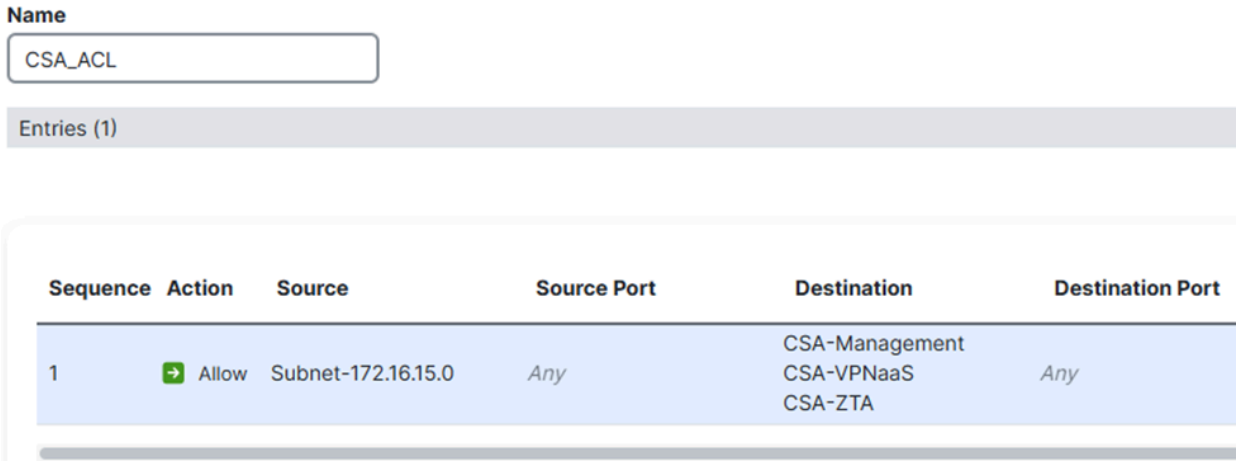
Isso permite que as organizações direcionem o tráfego específico ou de alta prioridade sobre os links preferenciais (como um link de Internet direto ou de alta largura de banda), otimizem o desempenho e dividam com segurança os aplicativos selecionados sem enviar todo o tráfego através de um túnel VPN.

Roteamento baseado em políticas

- Navegue atéObjects
  - Clique em Access List
  - Clique em Extended
  - Clique emAdd Extended Access List

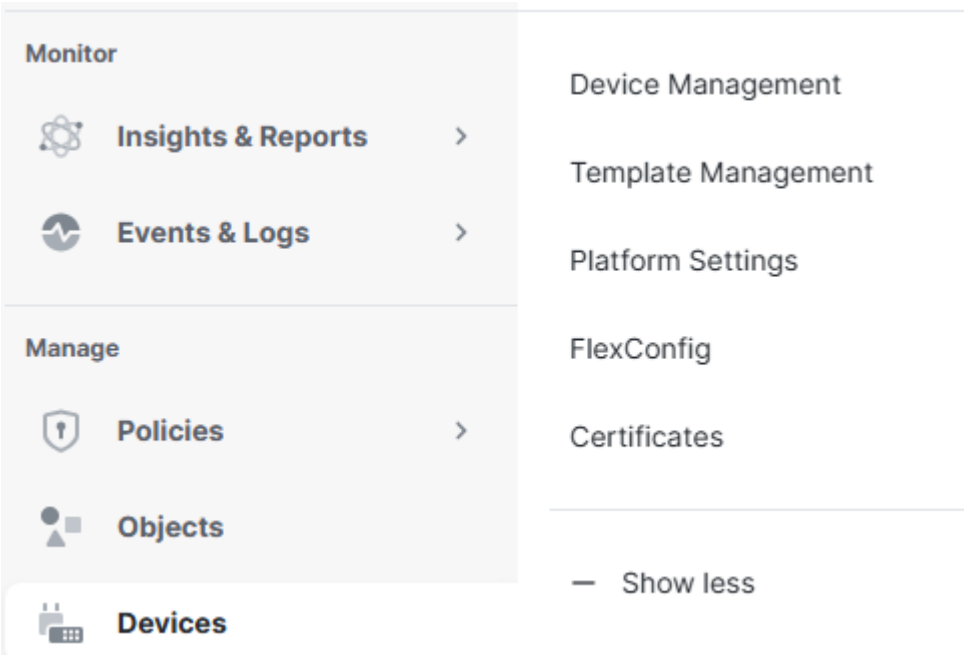
Adicionar ACL

Crie uma lista de controle de acesso estendida (ACL) que corresponda à rede de origem protegida pelo FTD (por exemplo, 172.16.15.0/24) para ser enviada pelo túnel. Para o destino, adicione as redes usadas por ZTA (intervalo CGNAT) e a rede usada por seu VPNaaS (verifique Virtual Private Network IP Pool).



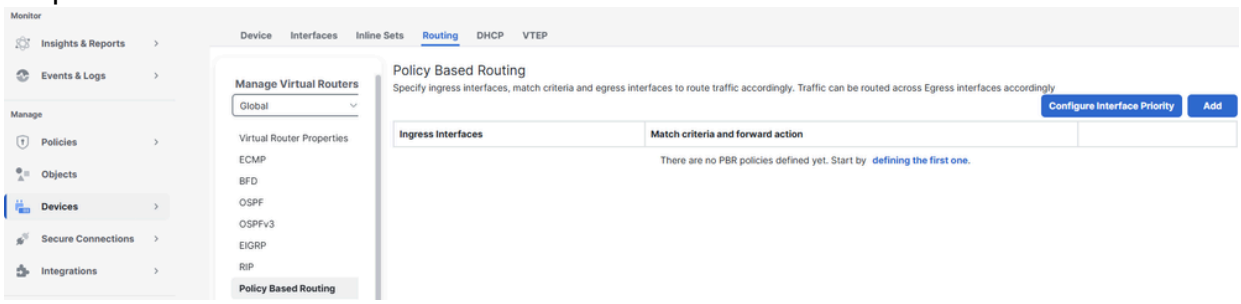
ACL

- Clique em Devices> Device Management



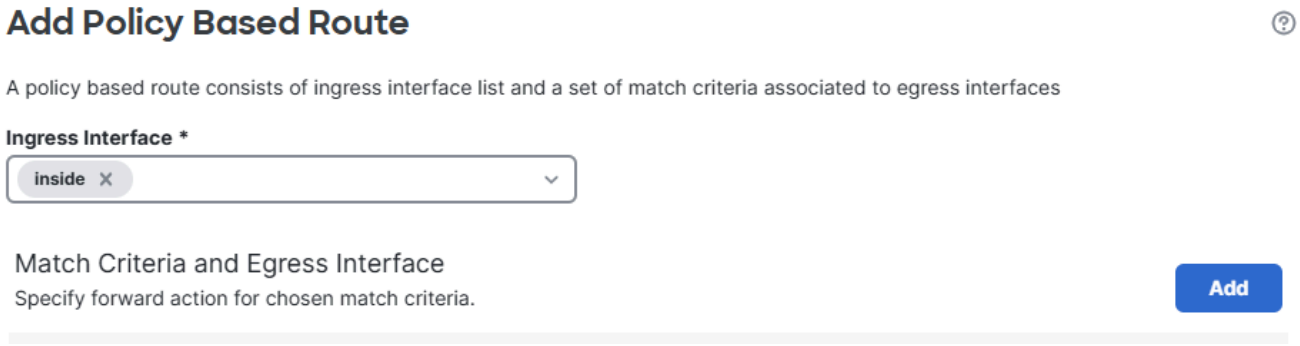
Dispositivo

- Clique no FTD
  - Clique emRouting
  - Clique em Policy Based Routing
  - Clique em Add



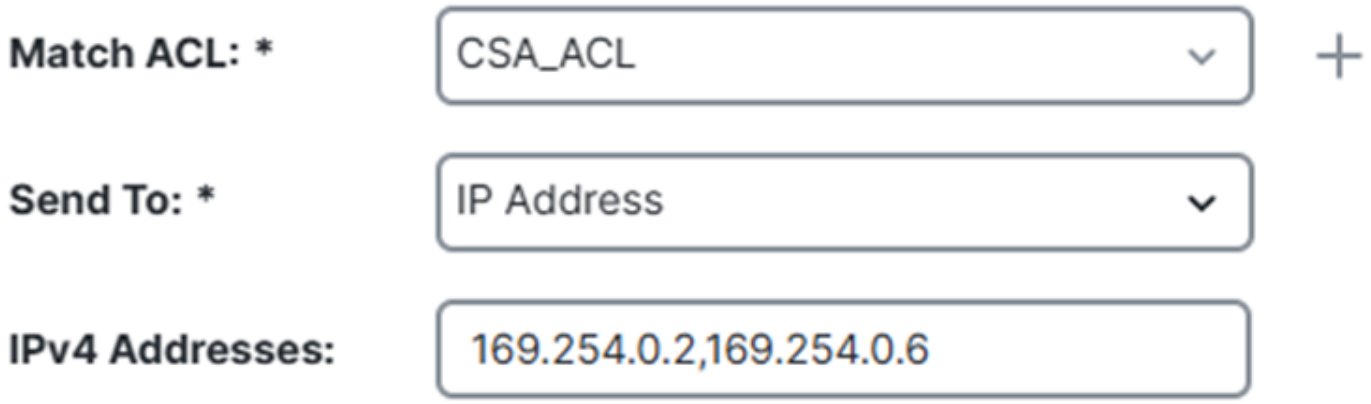
Adicionar PBR

- Clique Ingress Interface e selecione a interface de entrada onde o tráfego de redes internas entra
- Em Match Criteria and Egress Interface, clique em Add



Interface de entrada

- Clique em Match ACL e selecione a ACL estendida criada anteriormente
- Clique em Send To and select IP Address
- Clique em IPv4 Addresses e defina como próximos saltos os endereços IP dentro das sub-redes da interface VTI configuradas anteriormente no FTD (169.254.0.2 e 169.254.0.6)
- Clique em Save



Configuração baseada em política

Salvar PBR

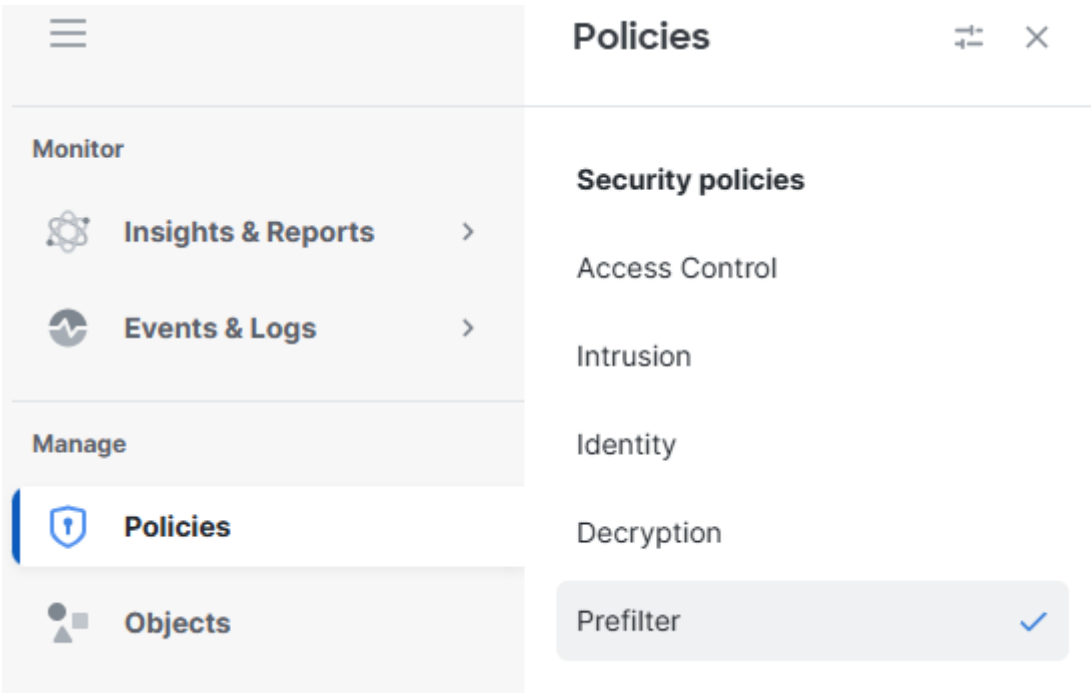
Certifique-se de selecionar a opção Send To > IP Address , e não a Egress Interface opção.

Configuração da política de acesso

Para permitir o tráfego em um Cisco Firepower Threat Defense (FTD) e permitir o acesso a recursos privados, o tráfego deve primeiro passar pelo estágio inicial de controle de acesso conhecido como Pré-filtragem.

A pré-filtragem é processada antes que ocorra uma inspeção mais profunda e é projetada para ser simples e rápida. Ele avalia o tráfego usando critérios básicos de cabeçalho externo (como endereços IP origem e destino e portas) para permitir, bloquear ou desviar rapidamente o tráfego. Quando o tráfego é permitido nesse estágio, ele pode pular mais inspeções intensivas de recursos, como inspeção profunda de pacotes ou políticas de invasão, melhorando o desempenho e mantendo o controle de segurança.

- Navegue até Policies> Prefilter

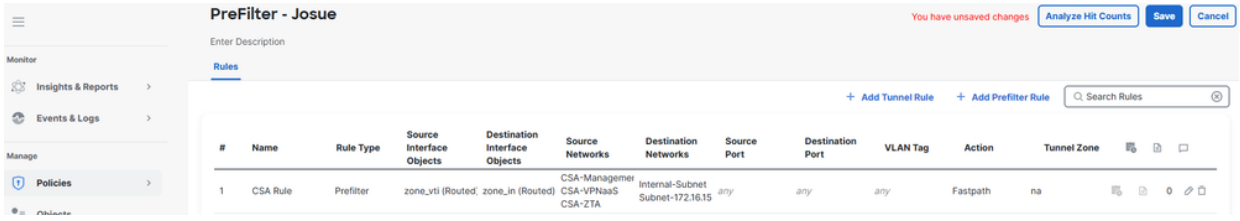


Pré-filtro

- Clique em editar a política de pré-filtro que está sendo usada pela sua política de acesso

clicar no pré-filtro

- Clique em Add Tunnel Rule
  - Adicione e permita o tráfego da rede VPNaaS e/ou da sub-rede ZTA para seus recursos privados
  - Clique emSave



Salvar regra

Neste ponto, uma vez concluída e verificada a configuração no FTD, você poderá prosseguir com a implantação. Após a implantação, os túneis IPsec são ativados com êxito, confirmando que a conectividade segura aos recursos privados está estabelecida.

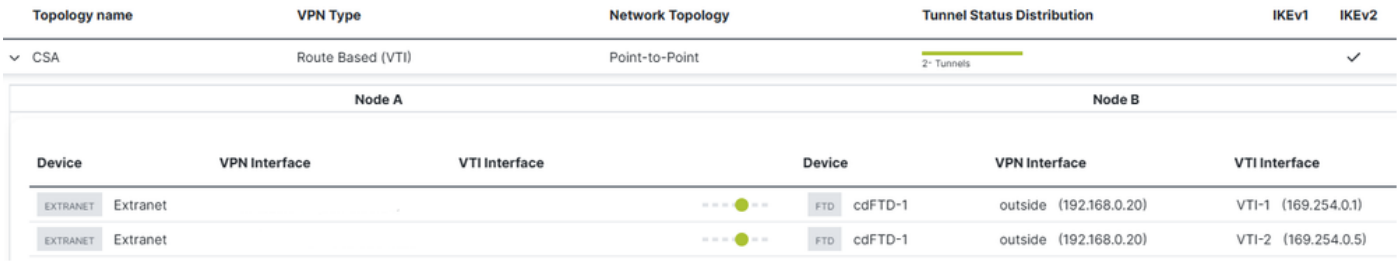
Verificar

Verificar no FTD

Status do túnel em FTD

Você pode visualizar o status atual do túnel, inclusive se ele está ativo ou inativo. Isso ajuda a verificar se o túnel IPsec está estabelecido corretamente.

- Clique em Conexões seguras.
- Clique em VPN site a site e SD-WAN.
- Clique no Nome da Topologia.



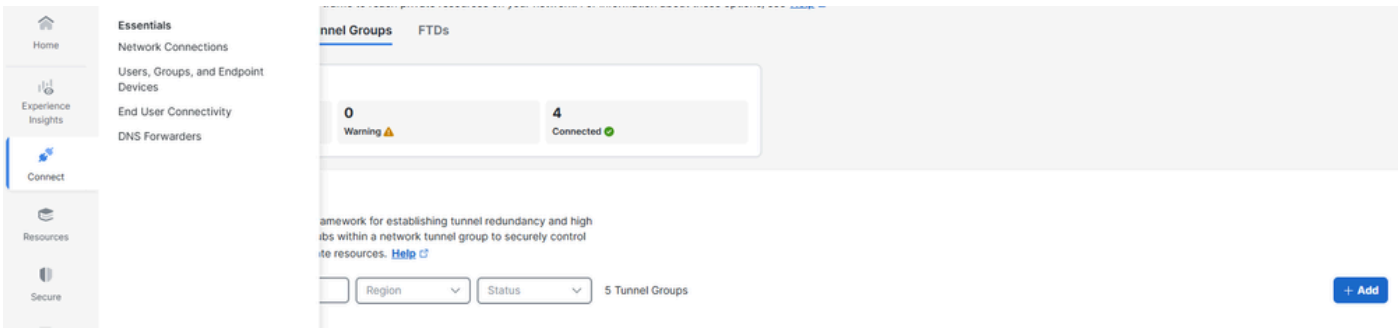
Status do túnel FTD

Verificar no acesso seguro

Status do túnel no acesso seguro

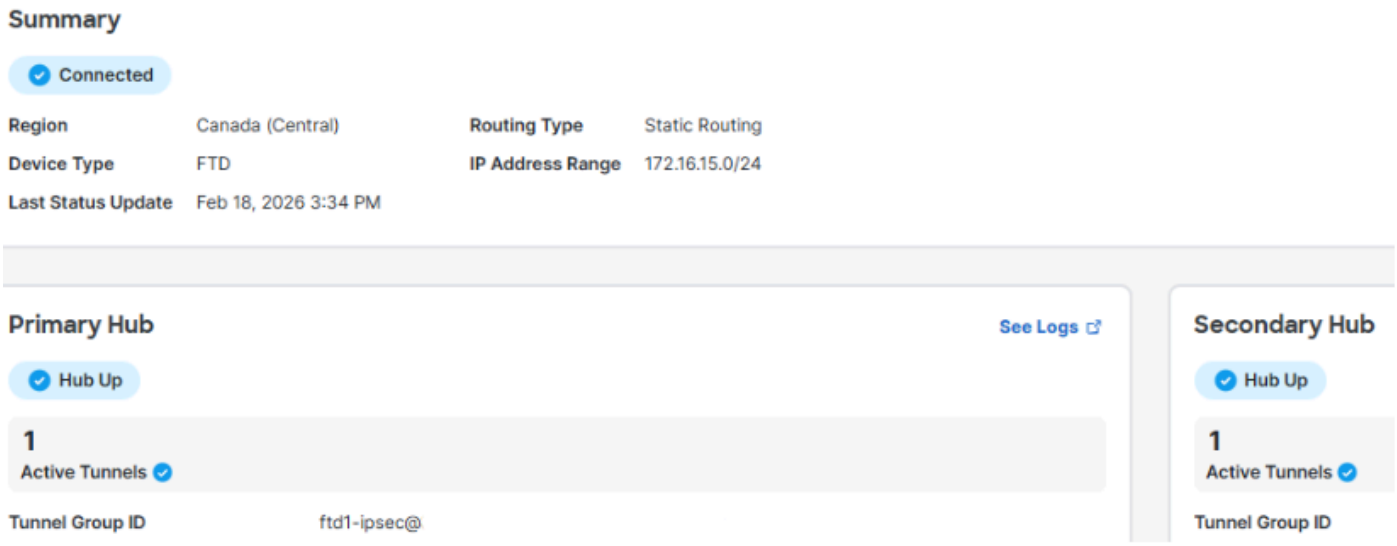
Você pode exibir o status atual do túnel, inclusive se ele está Desconectado, Aviso ou Conectado. Isso ajuda a verificar se o túnel IPsec está estabelecido corretamente.

- Clique em Connect > Network Connections
- Clique em Network Tunnel Groups



Verificar NTG

- Clique em Network Tunnel Group

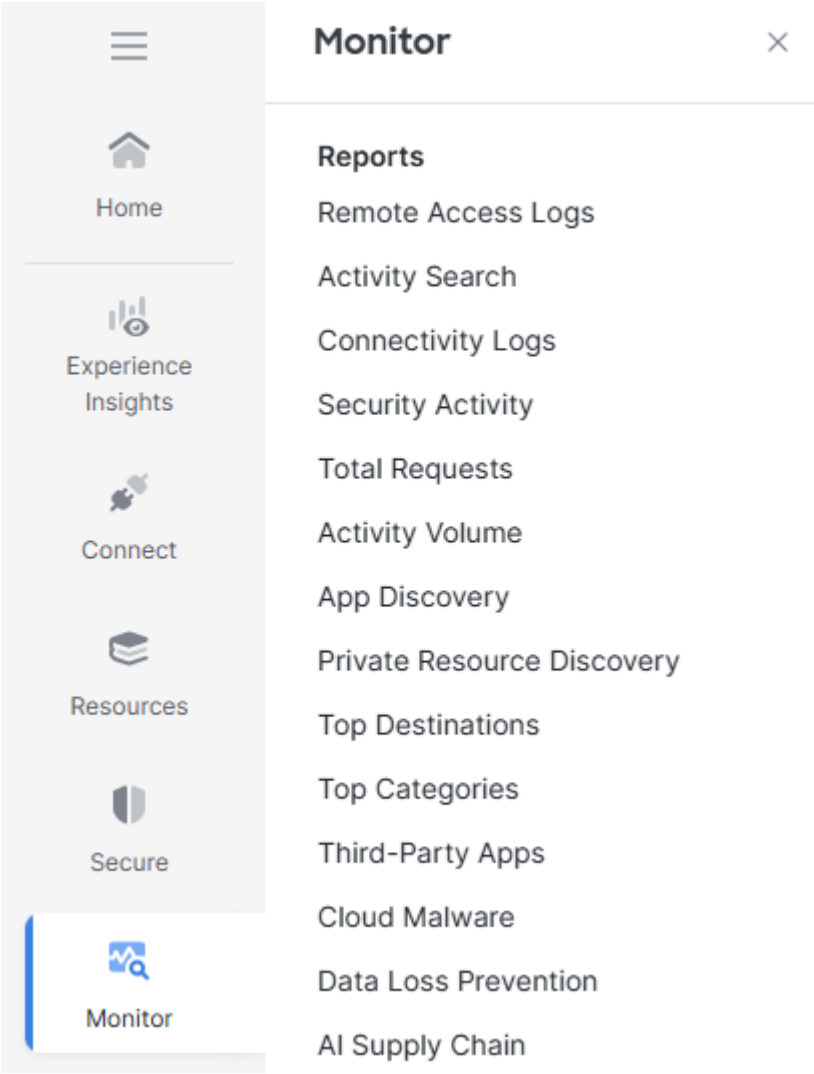


Status do túnel CSA

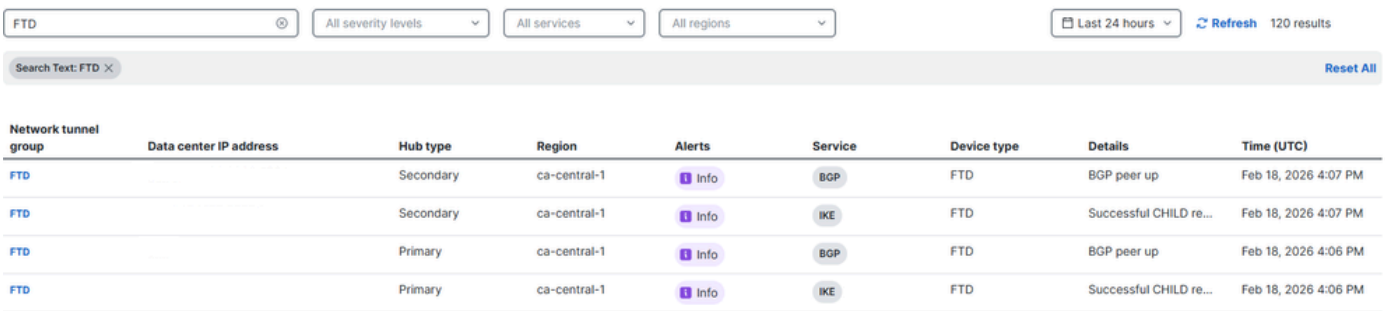
Eventos no acesso seguro

Você pode visualizar eventos de túnel e confirmar se o status dos túneis IPsec está ativo e estável.

Clique em Monitor > Network Connectivity.

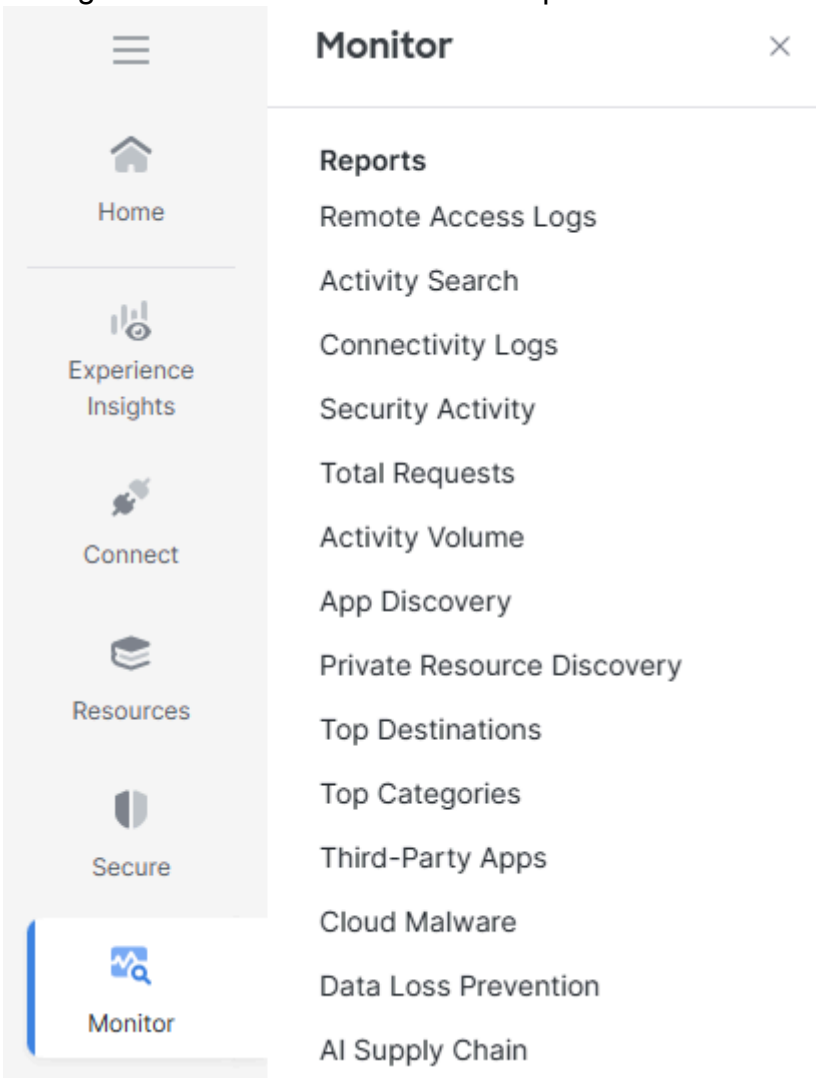


Logs de conexão do monitor



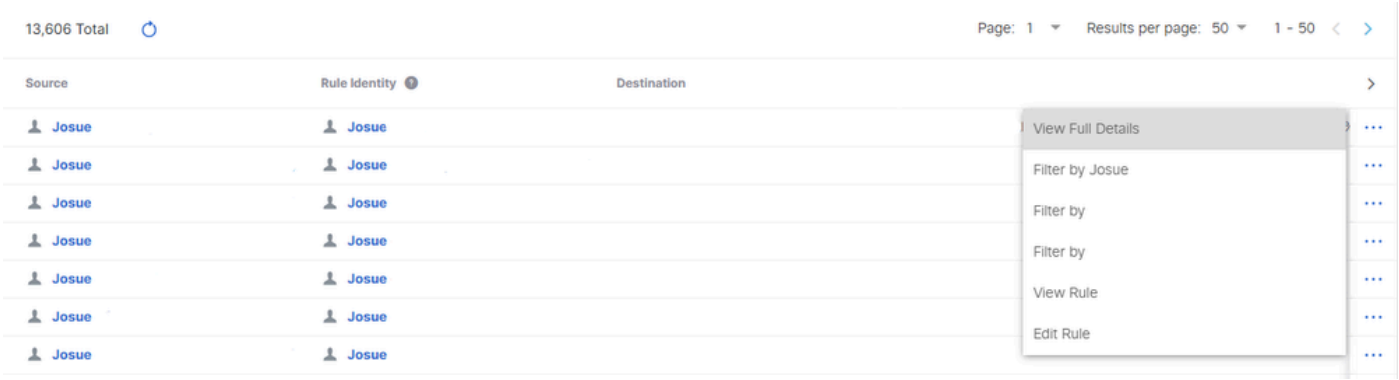
Logs de conexão

Navegue até Monitor > Atividade Pesquisar.

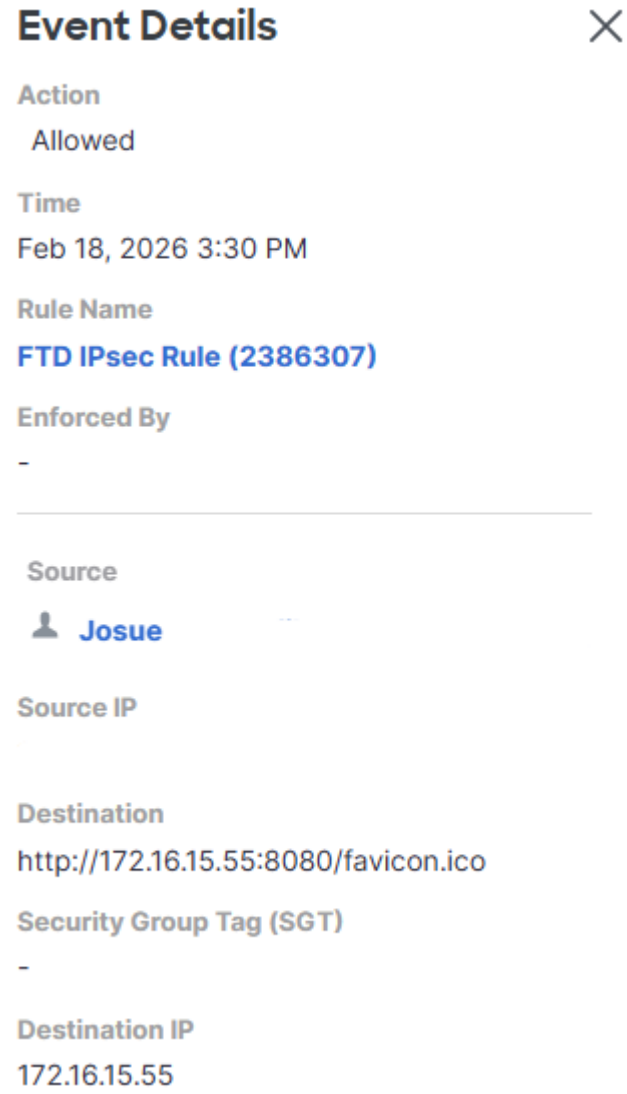


Logs de conexão do monitor

Em qualquer um dos eventos relacionados, clique em View Full Details.



Detalhes completos



Pesquisa de atividade

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.7

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.