

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configuração de acesso seguro](#)

[Configuração do grupo de túneis de rede](#)

[Roteamento de acesso seguro](#)

[Roteamento baseado em políticas](#)

[Salvar configuração do grupo de túneis de rede](#)

[Criar um recurso privado](#)

[Criar uma Regra de Política de Acesso](#)

[Configuração do Secure Firewall Threat Defense \(FTD\)](#)

[Configuração de interfaces de túnel virtual](#)

[Configuração de túnel IPsec](#)

[Configuração de roteamento FTD](#)

[Roteamento baseado em políticas](#)

[Configuração da política de acesso](#)

[Verificar](#)

[Verificar no FTD](#)

[Status do túnel em FTD](#)

[Verificar no acesso seguro](#)

[Status do túnel no acesso seguro](#)

[Eventos no acesso seguro](#)

[Informações Relacionadas](#)

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

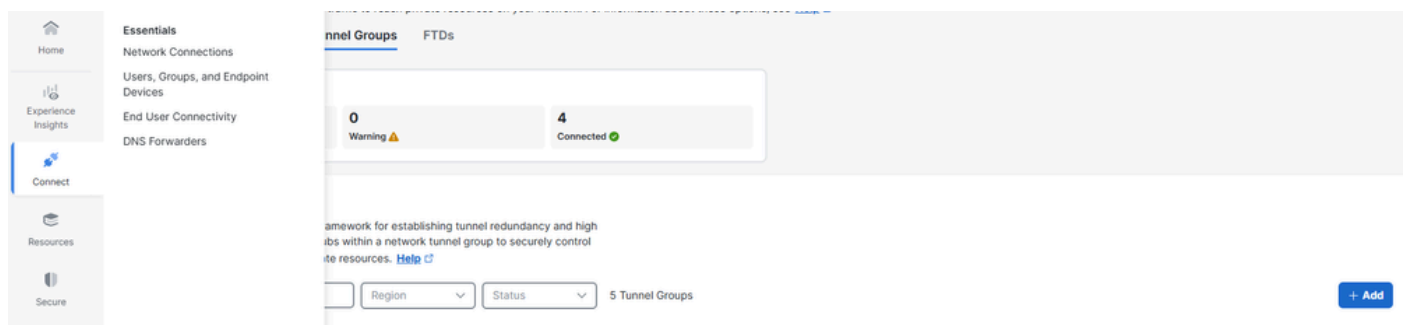
Configuração do grupo de túneis de rede

1. Navegue até o painel de administração do [Secure Access](#).



2. Adicione um Grupo de Túneis de Rede.

- Clique em **Connect** > **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**

1 General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

General Settings

Give your network tunnel group a good meaningful name, choose the type this tunnel group will use.

Tunnel Group Name

FTD

Region

Canada (Central)

Device Type

FTD

Configurações gerais

4. Configure Tunnel ID e Passphrase.

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

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

ftd1-ipsec

Passphrase

.....

The passphrase must be between special characters.

Confirm Passphrase

.....

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 em **Add**
 - Clique em **Save**

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**

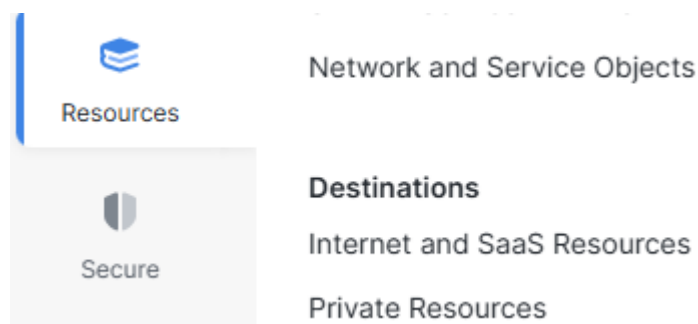
Dados de NTG

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**

Private Resource Name

Description (optional)

Private resource address
Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges
172.16.15.55	TCP - (HTTP/H...	8080

Recurso privado

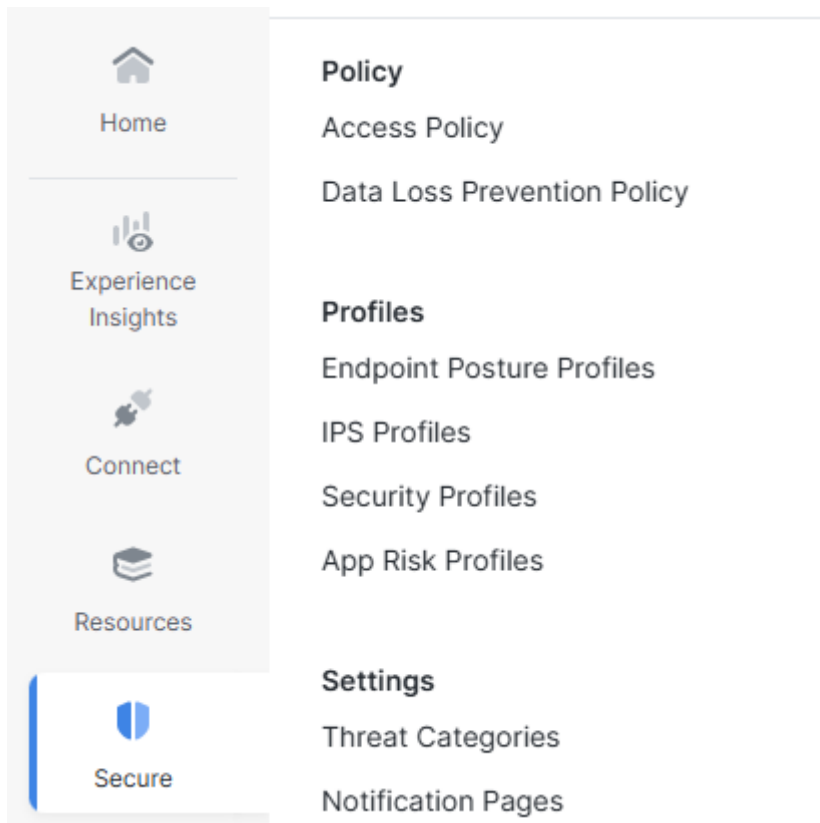
Criar uma Regra de Política de Acesso

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

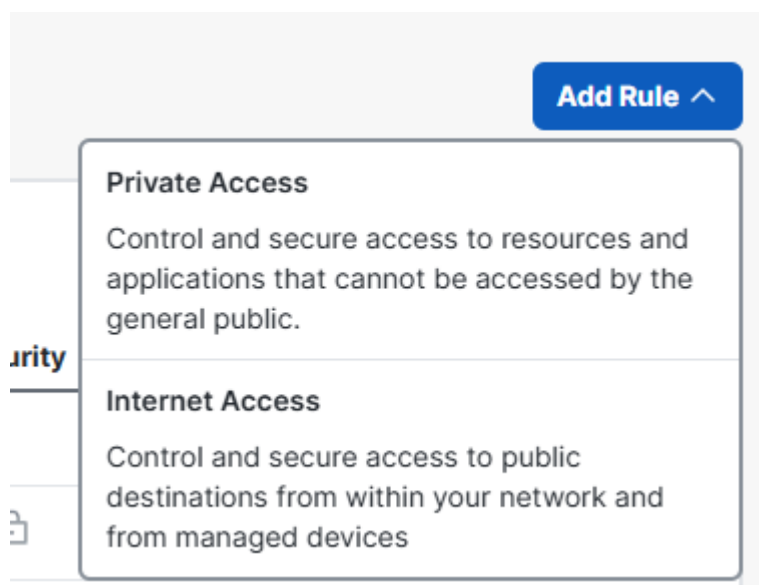
dispositivo, local ou outras condições da política. Isso garante que os sistemas internos confidenciais permaneçam protegidos do acesso público geral enquanto ainda estão disponíveis com segurança para usuários autorizados por meio de ZTA ou VPNaaS.

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 em **Action**, selecione para permitir **Allow** o tráfego
- Clique **From** em e especifique os usuários que recebem permissão
- Clique em **To** e especifique o acesso que esses usuários têm com base nesta regra
- Clique em **Next**, em seguida, **Save** na próxima página

Rule name ⓘ Rule order

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#) ⓘ

Action

☒ **Allow**
Allow specified traffic if security requirements are met.

☐ **Block**
Block specified traffic.

From
Specify one or more sources

AD Users • Josue x

To
Specify one or more destinations

Private Resources • FTD Internal Server x

+ AND

Endpoint Requirements

For VPN connections:

☒ End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#) ⓘ

For Branch connections:

☐ Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security
Configure security requirements that must be met before traffic is allowed. [Help](#) ⓘ

Cancel Back Next

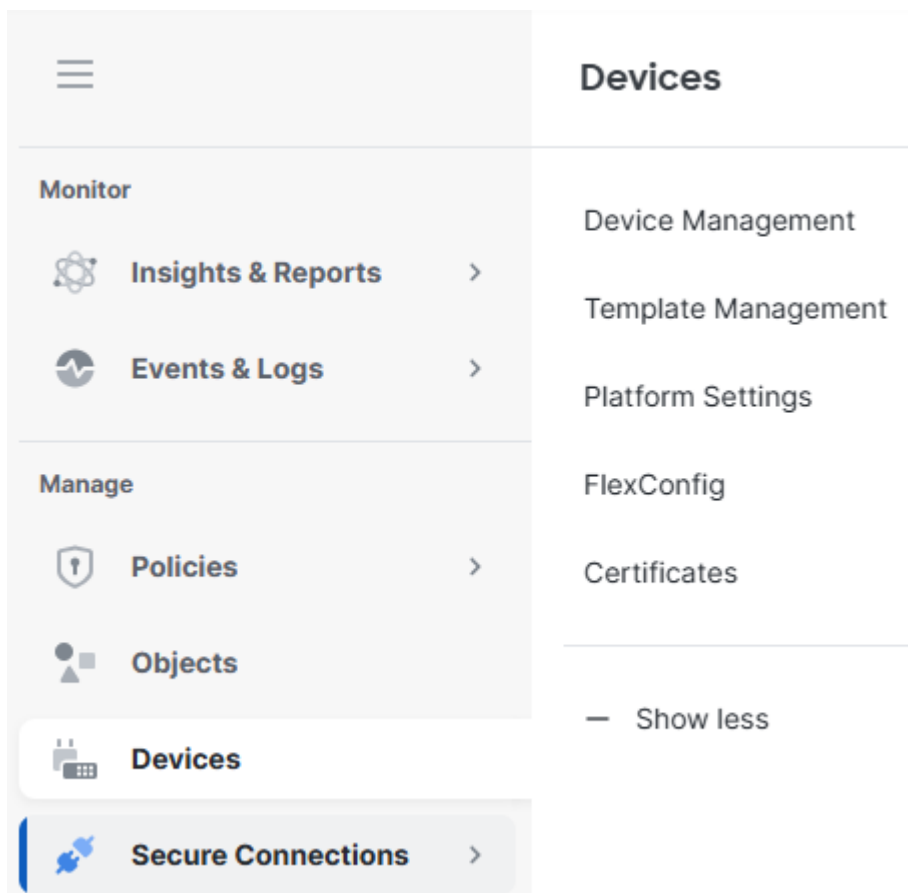
configuração de ACP

Configuração do Secure Firewall Threat Defense (FTD)

Configuração de interfaces de túnel virtual

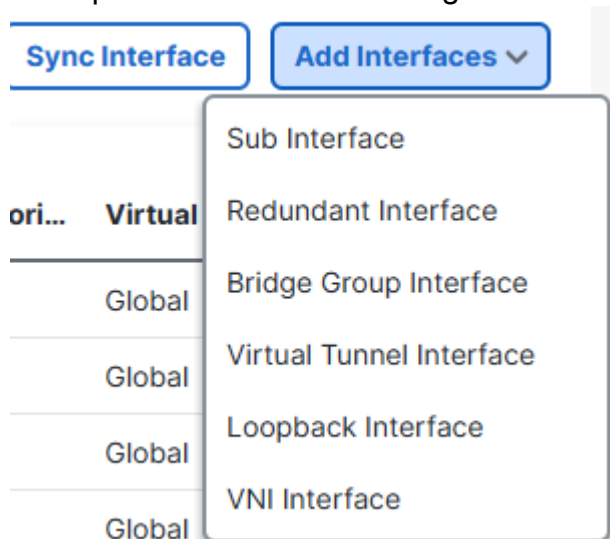
Uma Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) em FTD é uma interface lógica de Camada 3 usada para configurar túneis VPN IPsec baseados em rota.

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 Mode e selecione IPv4
- Clique em IP Address e configure o endereço IP para o VTI
- Clique em OK

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI1.1

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.0.1/30



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 em **Tunnel Source** e especifique a interface WAN a partir da qual o túnel será estabelecido
- Clique em **IPsec Tunnel Mode** e selecione **IPv4**
- Clique em **IP Address** e configure o endereço IP para o VTI
- Clique em **OK**

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-2

☒ Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

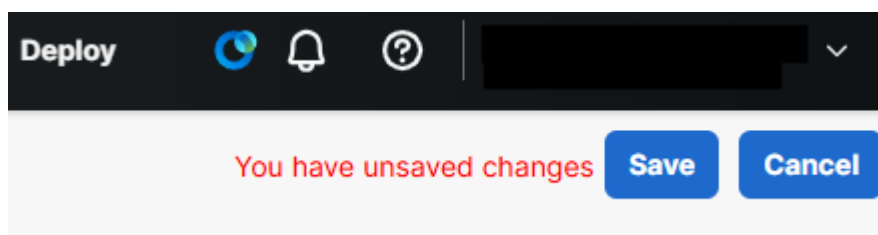
☒ Configure IP

169.254.0.5/30



VTI2.2

- Clique em Save.

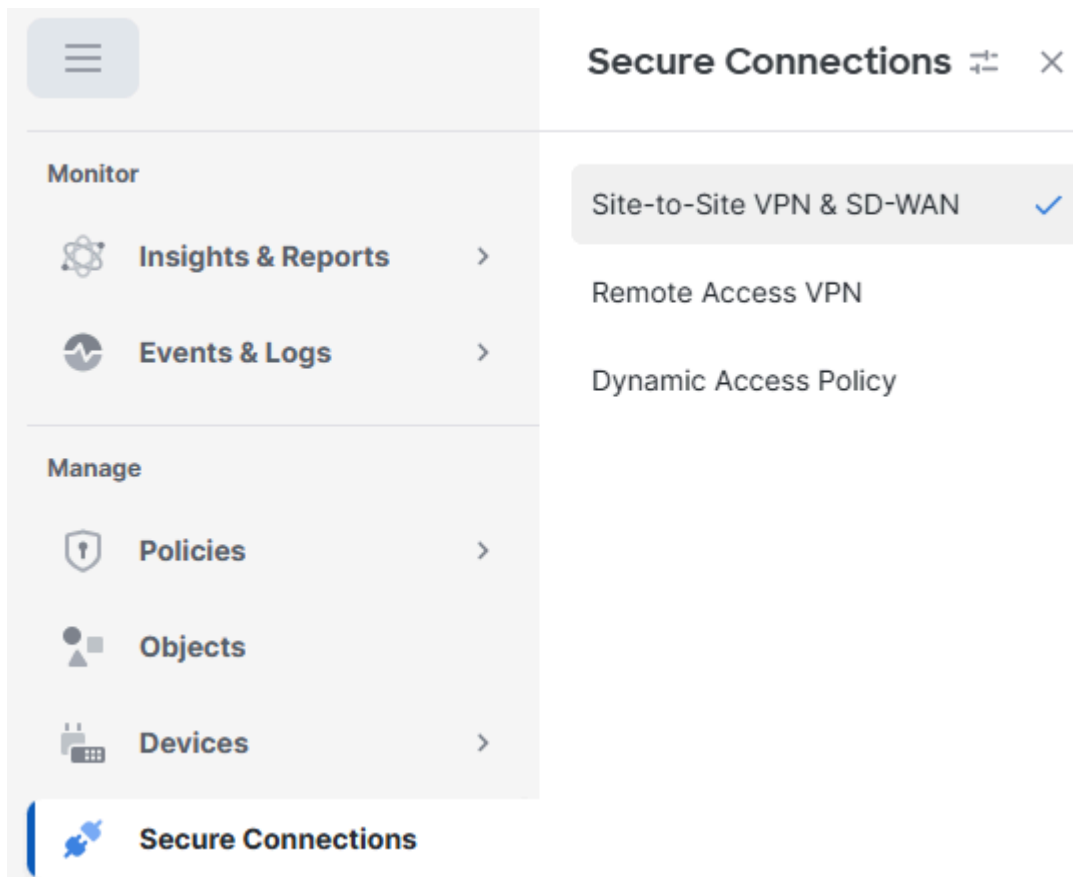


Salvar alterações de VTI

Configuração de túnel IPsec

Navegue até o painel do cdFMC.

- Clique em [Secure Connection](#) > [Site-to-Site VPN & SD-WAN](#)



S2S

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

Last Updated: 12:56 PM [Refresh](#) [NAT Exemptions](#) [Add](#)

Create VPN Topology

Topology name *
CSA

VPN Type

New

☐ SD-WAN Topology
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☐ Hub and Spoke
[Prerequisites](#)

☒ **Route-Based VPN**
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ Hub and Spoke
☒ Peer to Peer

☐ Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh

☐ SASE Topology
⚠ SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.
[Prerequisites](#)
[Refresh](#)

[Cancel](#) [Create](#)

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 em Endpoints
 - Em Node A, clique em Device e selecione Extranet
 - Clique em Device Name e dê um nome a ele
 - Clique em Endpoint 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 em Device e 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 selecione Email 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 em Send Local Identity to Peers option e selecione Email ID, enter the secondary tunnel ID (from "Save Network Tunnel Group Configuration" under the Secure Access Configuration)
 - Clique em Salvar

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

Extranet ▾

Device Name*:

CSA

Endpoint IP Address*:

Primary-IP,Secondary-IP

Node B

Device:*

cdFTD-1 ▾

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.0.1) ▾

 +

Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*:

Email ID ▾

ftd1-ipsec@

Backup VTI: Remove

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.0.5) ▾

 +

Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*:

Email ID ▾

ftd1-ipsec@

[Cancel](#)
[Save](#)

configuração de FTD VTI

- Clique em **IKE**
 - Clique em **IKEv2 Settings** > Policies
 - Selecione a **Umbrella-AES-GCM-256** opção
 - Clique em **OK**

IKEv2 Policy



Available IKEv2 Policy  +

AES-GCM-NULL-SHA
AES-GCM-NULL-SHA-LA..
AES-SHA-SHA
AES-SHA-SHA-LATEST
DES-SHA-SHA
DES-SHA-SHA-LATEST
Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256 

Cancel

OK

Política IKEv2

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

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256 

Authentication Type:

Pre-shared Manual Key 

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

IKE

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

EndpointsIKEIPsecAdvanced

Crypto Map Type:

☒ Static☐ Dynamic

IKEv2 Mode:

Tunnel

Transform Sets:

IKEv1 IPsec ProposalsIKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

IPsec

Cancel

OK

Salvar propostas IKEv2

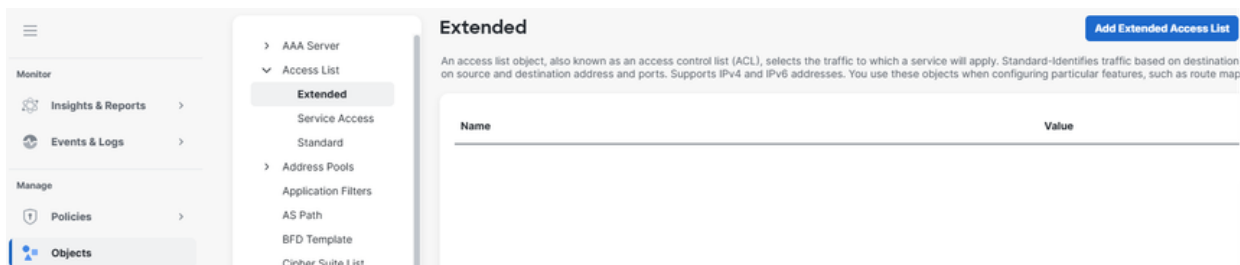
Configuração de roteamento FTD

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).

Name

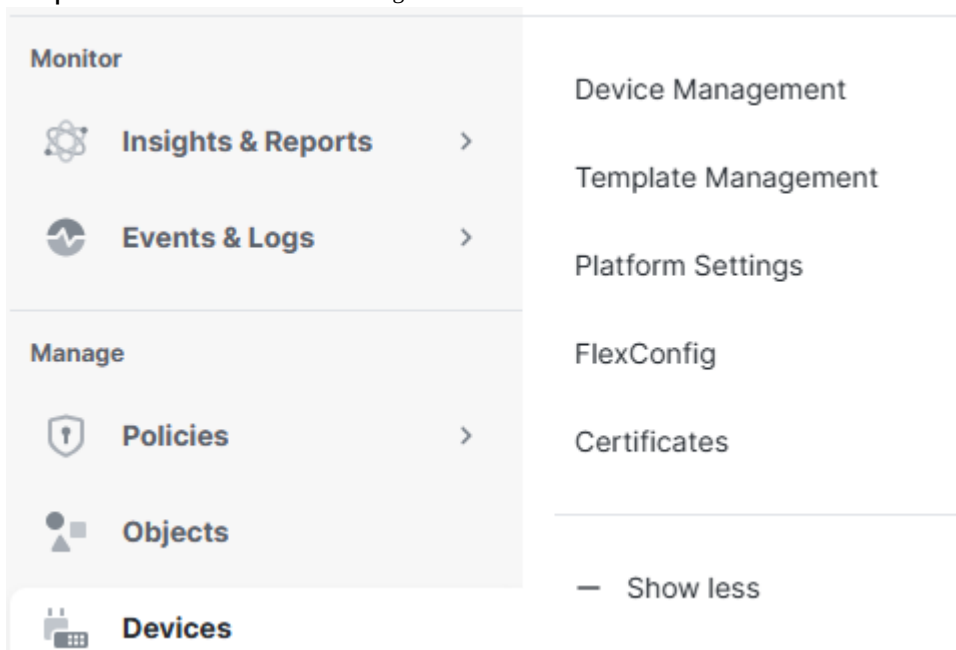
CSA_ACL

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	 Allow	Subnet-172.16.15.0	Any	CSA-Management CSA-VPNaaS CSA-ZTA	Any

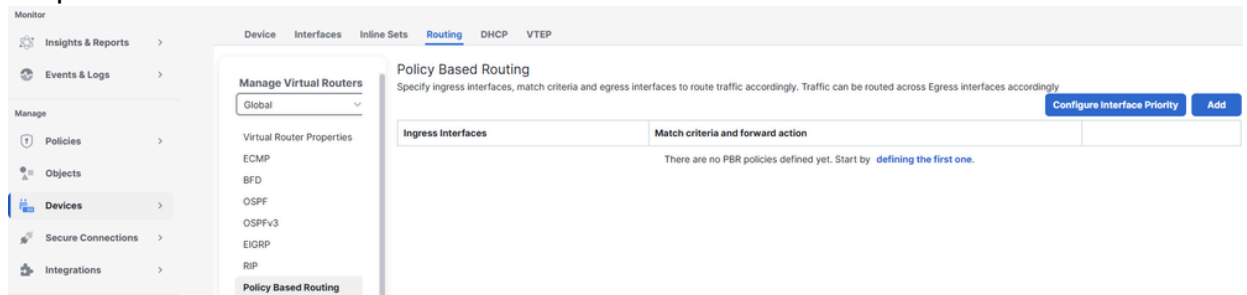
ACL

- Clique em **Devices** > **Device Management**



Dispositivo

- Clique no FTD
 - Clique em Routing
 - 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

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

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

Match ACL: *

CSA_ACL



Send To: *

IP Address



IPv4 Addresses:

169.254.0.2,169.254.0.6

Configuração baseada em política

Cancel

Save

Salvar PBR

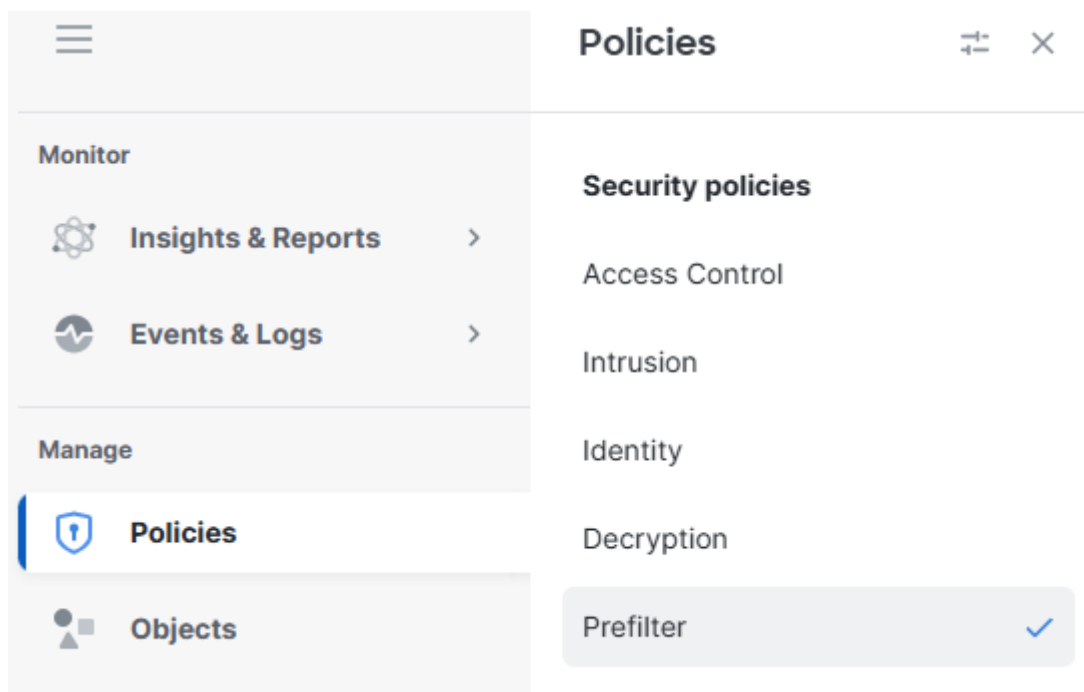
Certifique-se de selecionar a opção **Send To > IP Address** , e não a **Egress Interface** opção.

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

Prefilter Policy			Domain	Last Modified	
Default Prefilter Policy			Global	2025-07-24 08:27:51 Modified by "admin"	 
Prefilter - Josue			Global	2026-02-18 15:26:37 Modified by	 

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 em Save

Monitor

Insights & Reports

Events & Logs

Manage

Policies

PreFilter - Josue

You have unsaved changes

Analyze Hit Counts

Save

Cancel

Enter Description

Rules

+ Add Tunnel Rule

+ Add Prefilter Rule

Search Rules

#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone			
1	CSA Rule	Prefilter	zone_vrt1 (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na			0

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.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
▼ CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

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

Home

Essentials

Network Connections

Users, Groups, and Endpoint Devices

End User Connectivity

DNS Forwarders

Connect

Resources

Secure

Network Tunnel Groups

FTDs

0 Warning

4 Connected

Framework for establishing tunnel redundancy and high availability within a network tunnel group to securely control its resources. [Help](#)

Region

Status

5 Tunnel Groups

+ Add

Verificar NTG

- Clique em Network Tunnel Group

Summary

Connected

Region

Canada (Central)

Routing Type

Static Routing

Device Type

FTD

IP Address Range

172.16.15.0/24

Last Status Update

Feb 18, 2026 3:34 PM

Primary Hub

See Logs

Hub Up

1 Active Tunnels

Tunnel Group ID

ftd1-ipsec@

Secondary Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

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.

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

×

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Logs de conexão do monitor

FTD

All severity levels

All services

All regions

Last 24 hours

Refresh

120 results

Search Text: FTD

Reset All

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

Logs de conexão

Navegue até Monitor > Atividade Pesquisar.

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

×

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Logs de conexão do monitor

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

13,606 Total

Page: 1 Results per page: 50 1 - 50 < >

Source	Rule Identity ⓘ	Destination	
Josue	Josue		View Full Details
Josue	Josue		Filter by Josue
Josue	Josue		Filter by
Josue	Josue		Filter by
Josue	Josue		View Rule
Josue	Josue		Edit Rule
Josue	Josue		

Detalhes completos

Event Details



Action

Allowed

Time

Feb 18, 2026 3:30 PM

Rule Name

FTD IPsec Rule (2386307)

Enforced By

-

Source

 **Josue**

Source IP

-

Destination

http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)

-

Destination IP

172.16.15.55

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.