

Configure o acesso seguro com firewall seguro com alta disponibilidade

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configurar a VPN no acesso seguro](#)

[Dados para configuração de túnel](#)

[Configurar o túnel no Firewall Seguro](#)

[Configurar a interface do túnel](#)

[Configurar a rota estática para a interface secundária](#)

[Configurar a VPN para proteger o acesso no modo VTI](#)

[Configuração de endpoints](#)

[Configuração de IKE](#)

[Configuração de IPSEC](#)

[Configuração avançada](#)

[Cenários de configuração da política de acesso](#)

[Cenário de acesso à Internet](#)

[Cenário de RA-VPN](#)

[Cenário ZTNA CLAP-BAP](#)

[Configurar o Roteamento Base da Política](#)

[Configurar a Diretiva de Acesso à Internet no Acesso Seguro](#)

[Configurar o acesso a recursos privados para ZTNA e RA-VPN](#)

[Troubleshooting](#)

[Verificar Fase1 \(IKEv2\)](#)

[Verificar Fase2 \(IPSEC\)](#)

[Função de alta disponibilidade](#)

[Verificar o roteamento de tráfego para proteger o acesso](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o acesso seguro com firewall seguro com alta disponibilidade.

Pré-requisitos

- [Configurar Provisionamento de Usuário](#)
- [Configuração de Autenticação ZTNA SSO](#)
- [Configurar o acesso seguro da VPN de acesso remoto](#)

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center 7.2
- Firepower Threat Defense 7.2
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA sem cliente

Componentes Utilizados

As informações neste documento são baseadas em:

- Firepower Management Center 7.2
- Firepower Threat Defense 7.2
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

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



CISCO

Secure

Access

Secure Firewall

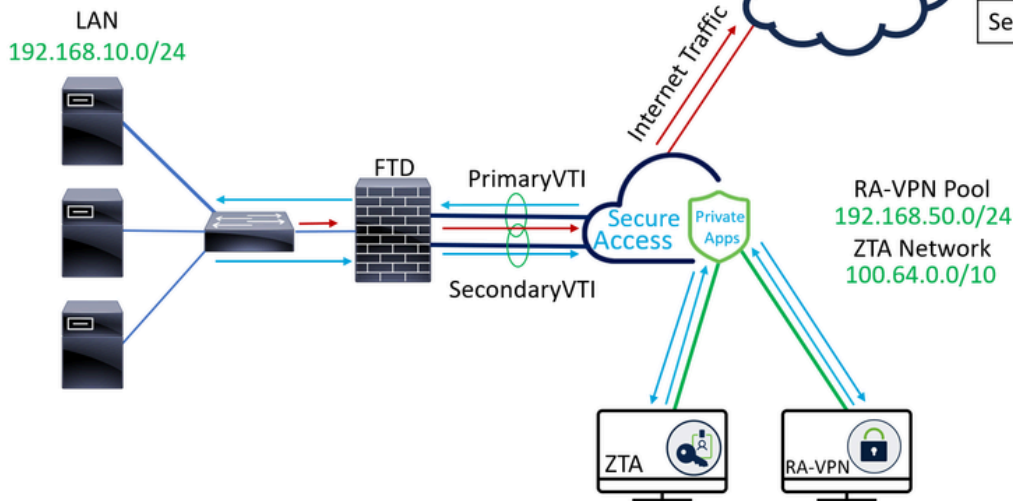
FTD

A Cisco projetou o Secure Access para proteger e fornecer acesso a aplicativos privados, no local e baseados em nuvem. Ele também protege a conexão da rede à Internet. Isso é obtido por meio da implementação de vários métodos e camadas de segurança, todos voltados para preservar as informações à medida que elas são acessadas pela nuvem.

Diagrama de Rede

Internet Access Traffic —
Private Apps Traffic —

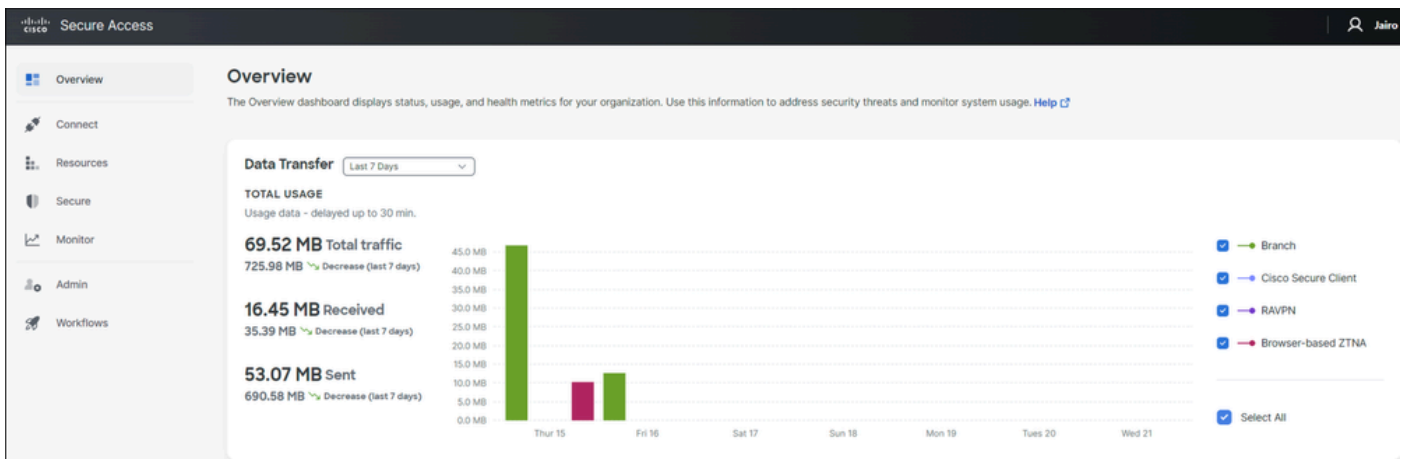
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



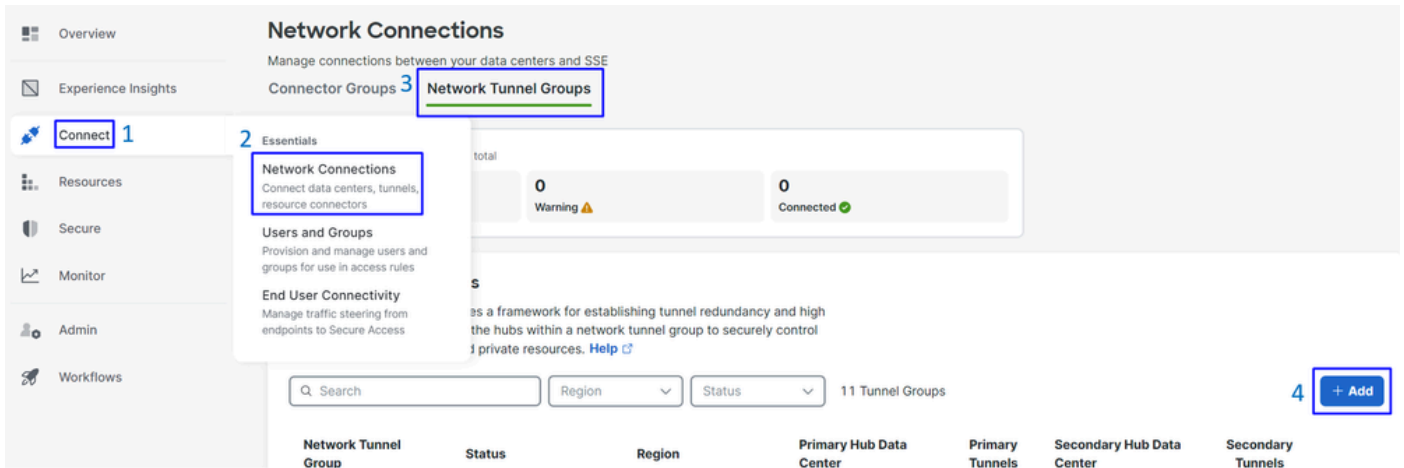
Configurar

Configurar a VPN no acesso seguro

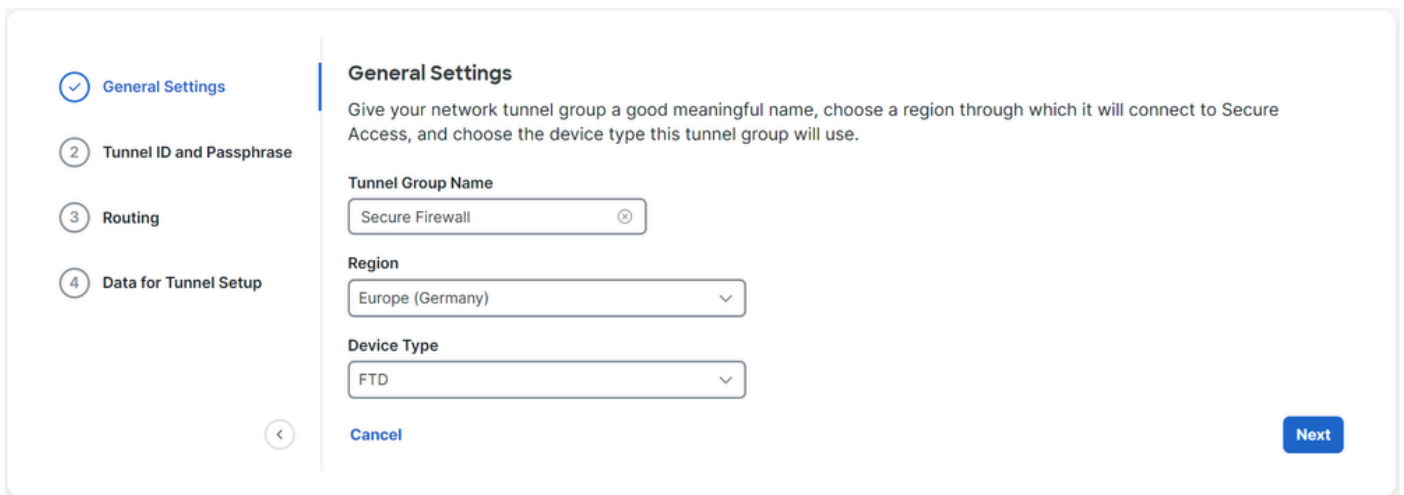
Navegue até o painel de administração do [Acesso seguro](#).



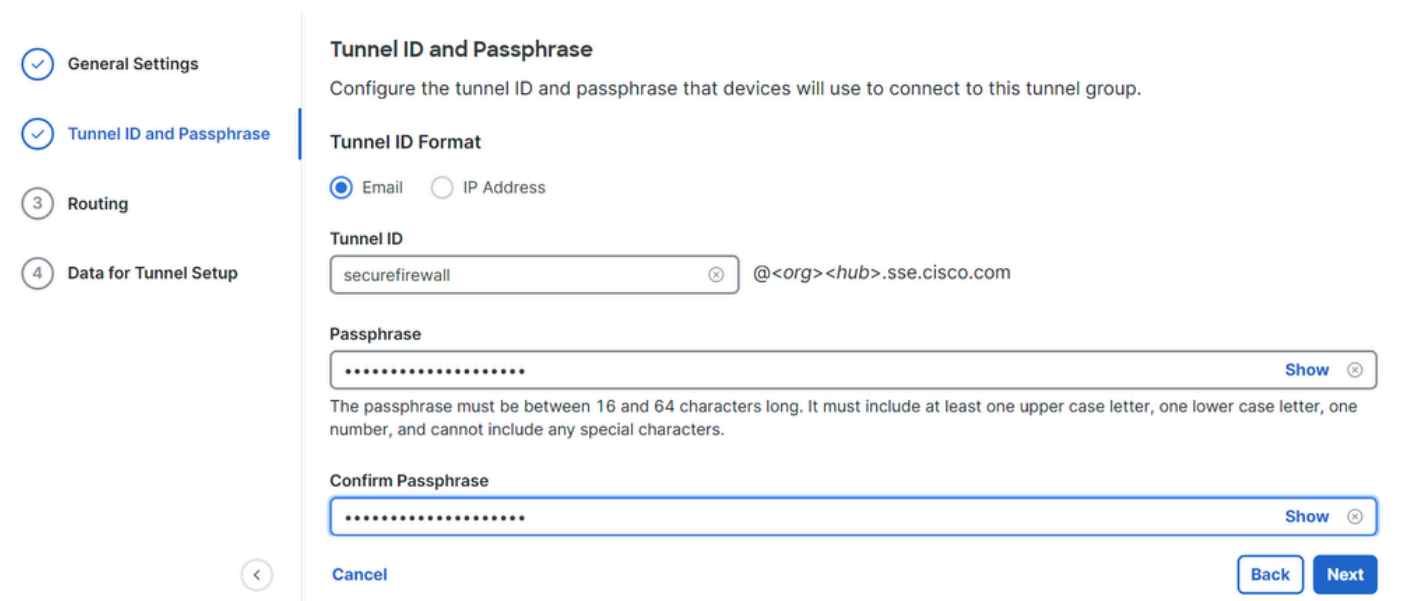
- Clique em **Connect > Network Connections**
- Em **Network Tunnel Groups** clique em **+ Add**



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



- Configure Tunnel ID Format e Passphrase
- Clique em Next



- Configure os intervalos de endereços IP ou hosts que você configurou na sua rede e deseja

passar o tráfego pelo Secure Access

- Clique em **Save**

Routing option

Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24 **Add**

192.168.0.0/24 X 192.168.10.0/24 X

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

[Cancel](#)

[Back](#) [Save](#)

Depois de clicar **save** nas informações sobre o túnel que são exibidas, salve essas informações para a próxima etapa, **Configure the tunnel on Secure Firewall**.

Dados para configuração de túnel

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID: securefirewall@[redacted]-sse.cisco.com

Primary Data Center IP Address: 18.156.145.74

Secondary Tunnel ID: securefirewall@[redacted]-sse.cisco.com

Secondary Data Center IP Address: 3.120.45.23

Passphrase: [redacted]

[Download CSV](#)

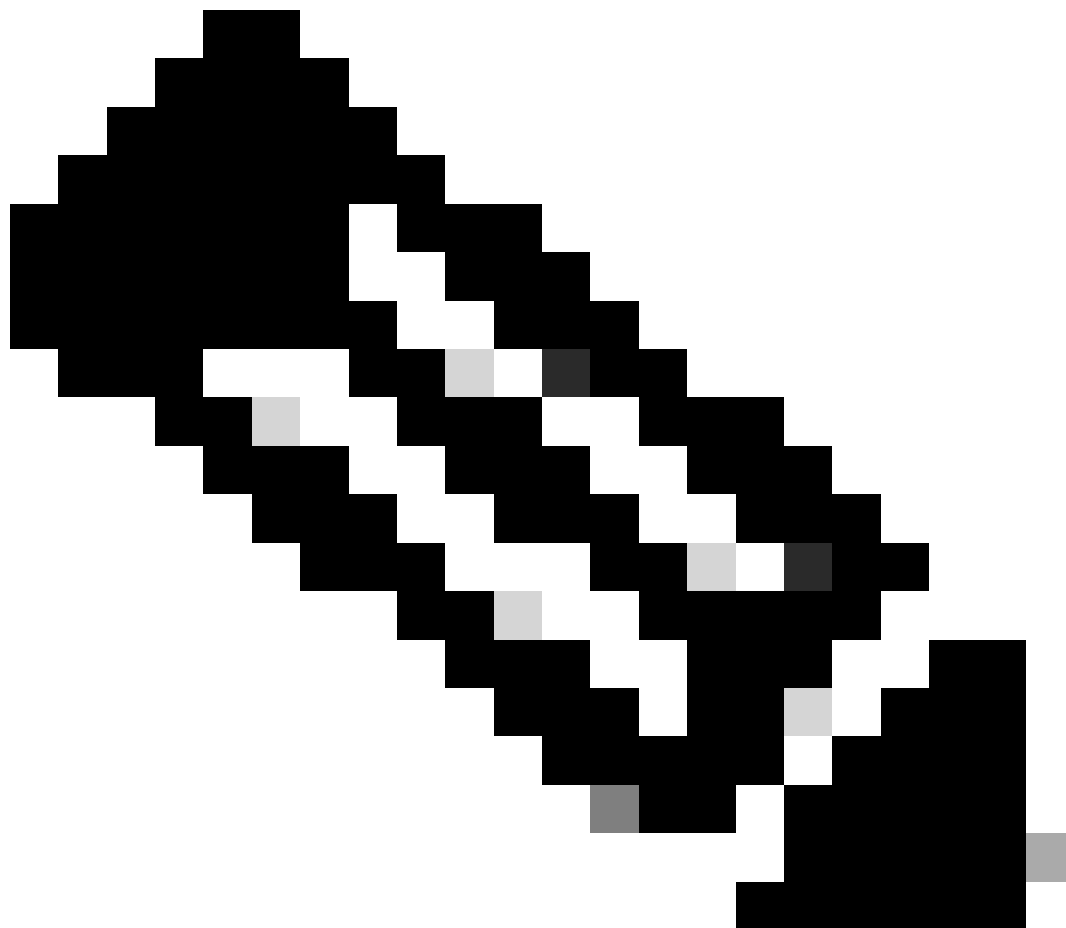
[Done](#)

Configurar o túnel no Firewall Seguro

Configurar a interface do túnel

Para esse cenário, você usa a configuração da Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) no Firewall Seguro para atingir essa meta; lembre-se de que, nesse caso, você tem ISP duplo e queremos ter HA se um de seus ISPs falhar.

INTERFACES	FUNÇÃO
WAN primária	WAN de Internet principal
WAN secundária	WAN de Internet secundária
VTIprimário	Vinculado para enviar o tráfego pelo Principal Internet WAN para acesso seguro
VTIsecundário	Vinculado para enviar o tráfego pelo Secondary Internet WAN para acesso seguro



Note: 1. Você precisa adicionar ou atribuir uma rota estática ao roteador **Primary or Secondary Datacenter IP** para poder ter ambos os túneis ativos.



Note: 2. Se você tiver o ECMP configurado entre as interfaces, não será necessário criar nenhuma rota estática para o Primary or Secondary Datacenter IP para poder ativar ambos os túneis.

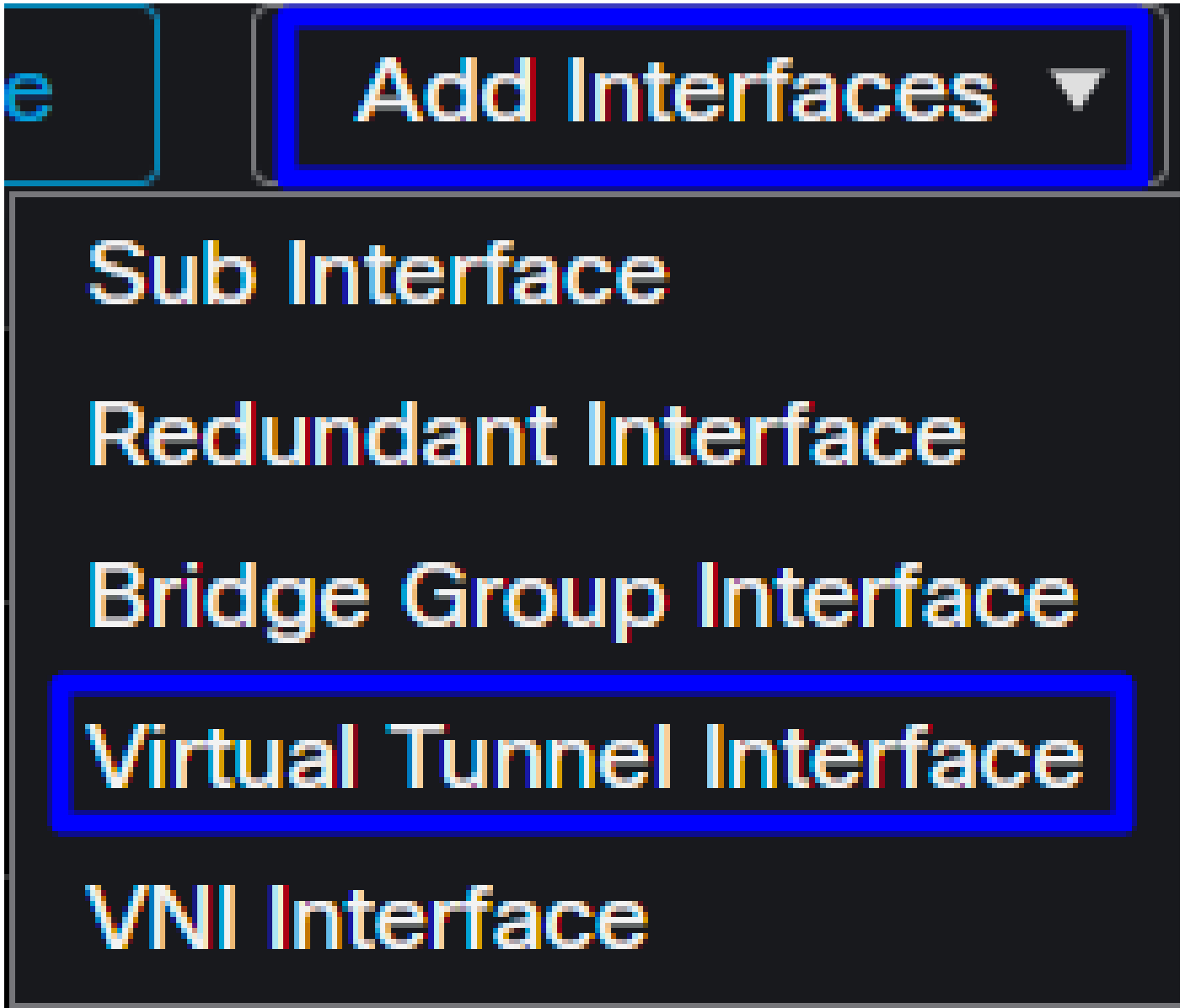
Com base no cenário, temos PrimaryWAN e SecondaryWAN, que devemos usar para criar as interfaces VTI.

Navegue até o Firepower Management Center > Devices.

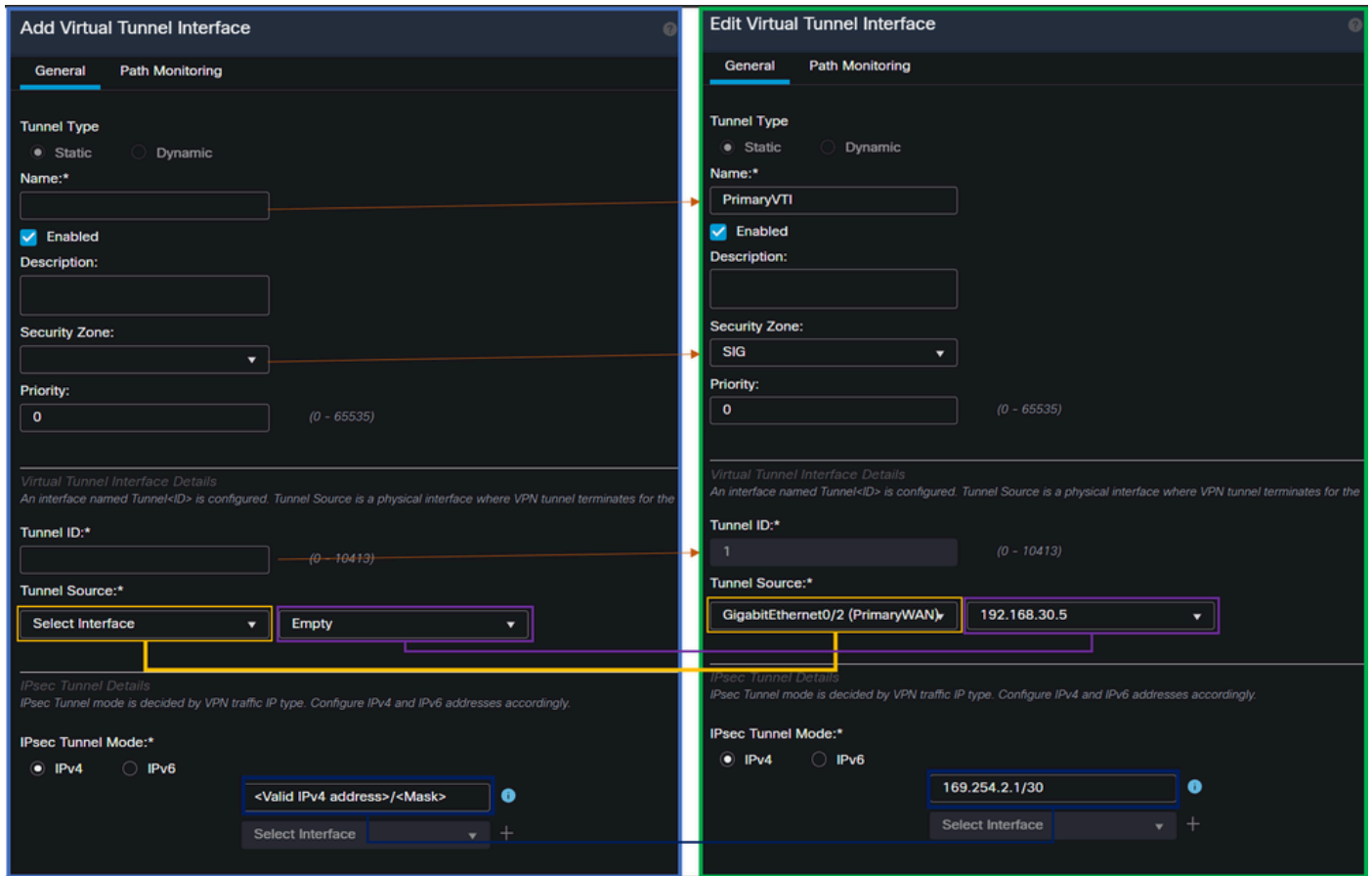
- Escolha seu FTD
- Escolha Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)

- Clique em **Add Interfaces > Virtual Tunnel Interface**



- Configure a interface com base nas próximas informações



- **Name** : Configure um nome que se refira ao **PrimaryWAN** interface
- **Security Zone** : Você pode reutilizar outro **Security Zone**, mas criar um novo para tráfego de acesso seguro é melhor
- **Tunnel ID** : Adicionar um número para a ID do túnel
- **Tunnel Source** : Escolha seu **PrimaryWAN** interface endereço IP e o IP privado ou público da interface
- **IPsec Tunnel Mode** : Escolha **IPv4** e configure um IP não roteável em sua rede com máscara 30



Note: Para a interface VTI, você deve usar um IP não roteável; por exemplo, se você tiver duas interfaces VTI, poderá usar 169.254.2.1/30 para o **PrimaryVTI** e 169.254.3.1/30 para o **SecondaryVTI**.

Depois disso, você precisa fazer o mesmo para o **SecondaryWAN interface**, e você tem tudo configurado para a alta disponibilidade de VTI e, como resultado, você tem o próximo resultado:

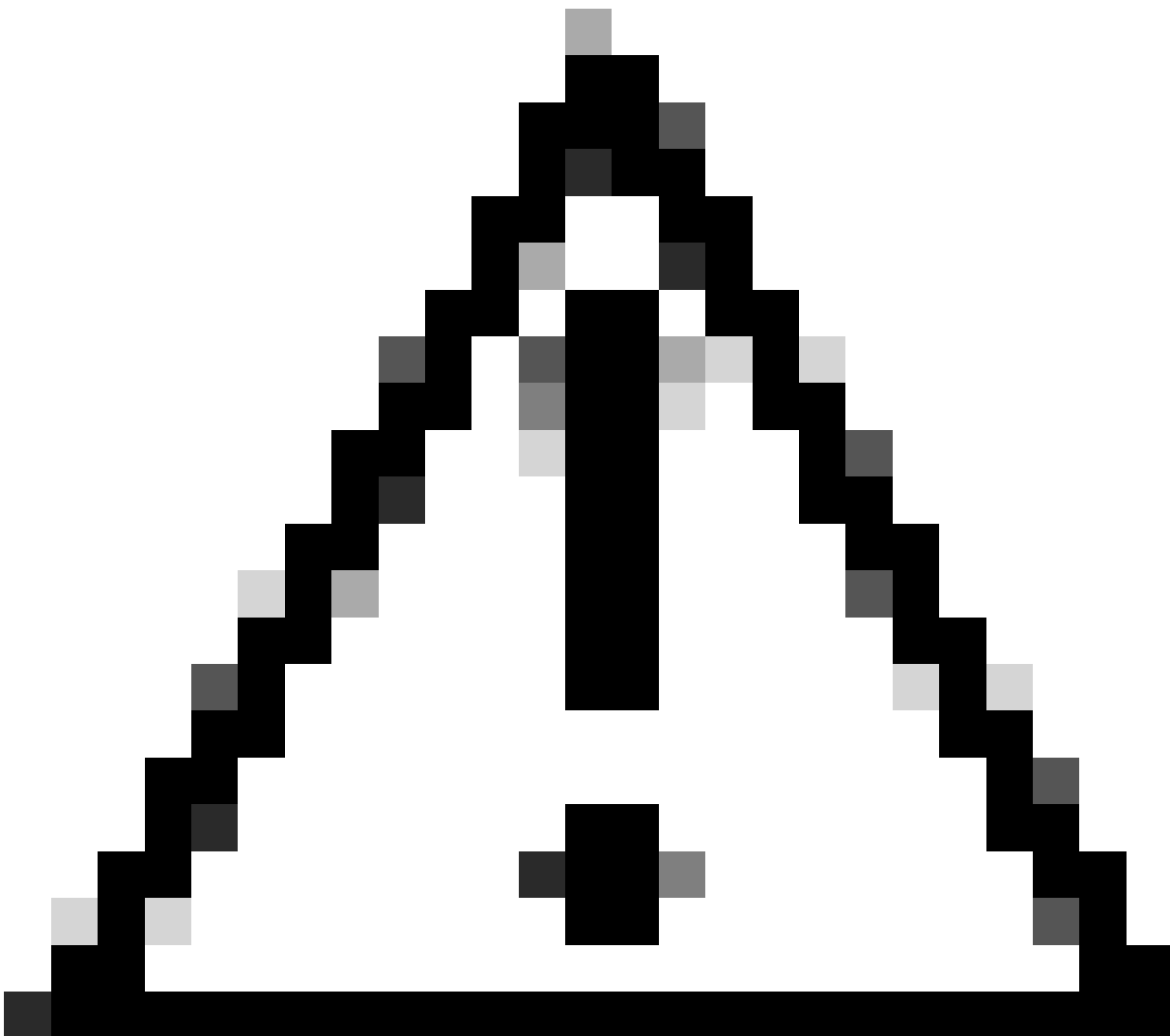
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

Para esse cenário, os IPs usados são:

Configuração IP de VTI		
Nome Lógico	IP	Faixa
VTIprimário	169.254.2.1/30	169.254.2.1-169.254.2.2
VTIsecundário	169.254.3.1/30	169.254.3.1-169.254.3.2

Configurar a rota estática para a interface secundária

Para permitir que o tráfego do **SecondaryWAN interface** **acesse** o **Secondary Datacenter IP Address** **servidor**, você precisa configurar uma rota estática para o IP do datacenter. Você pode configurá-lo com uma métrica de um (1) para torná-lo superior à tabela de roteamento; especifique também o IP como um host.



Caution: Isso só é necessário se você não tiver uma configuração de ECMP entre os canais de WAN; se você tiver o ECMP configurado, poderá ir para a próxima etapa.

Navegue até **Device > Device Management**

- Clique em seu dispositivo FTD
- Clique em **Routing**
- Escolha **Static Route > + Add Route**

Edit Static Route Configuration




Type: IPv4 IPv6

Interface*

SecondaryWAN

Choose the SecondaryWAN interface


(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

Add

Selected Network

SecureAccessTunnel 

Choose the Secondary Datacenter IP

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWWT1

Ensure that egress virtualrouter has route to that destination

Gateway

Outside_GW +

Choose the SecondaryWAN Gateway


Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+ 

Cancel

OK

- Interface: Escolha a interface WAN secundária
- Gateway: Escolha o gateway WAN secundário
- Selected Network: Adicione o IP do datacenter secundário como um host; você pode encontrar as informações fornecidas ao configurar o túnel na etapa Secure Access, [Data for Tunnel Setup](#)

- **Metric:** Use um (1)
- **OK** Clique em **Save** para salvar as informações e, em seguida, implantar.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
SecureAccessTunnel	SecondaryWAN	Global	Outside_GW	false	1	
any-ipv4	PrimaryWAN	Global	ASA_GW	false	1	
▼ IPv6 Routes						

Configurar a VPN para proteger o acesso no modo VTI

Para configurar a VPN, navegue até o firewall:

- Clique em **Devices > Site to Site**
- Clique em **+ Site to Site VPN**

Configuração de endpoints

Para configurar a etapa Endpoints, você precisa usar as informações fornecidas sob a etapa [Data for Tunnel Setup](#).

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

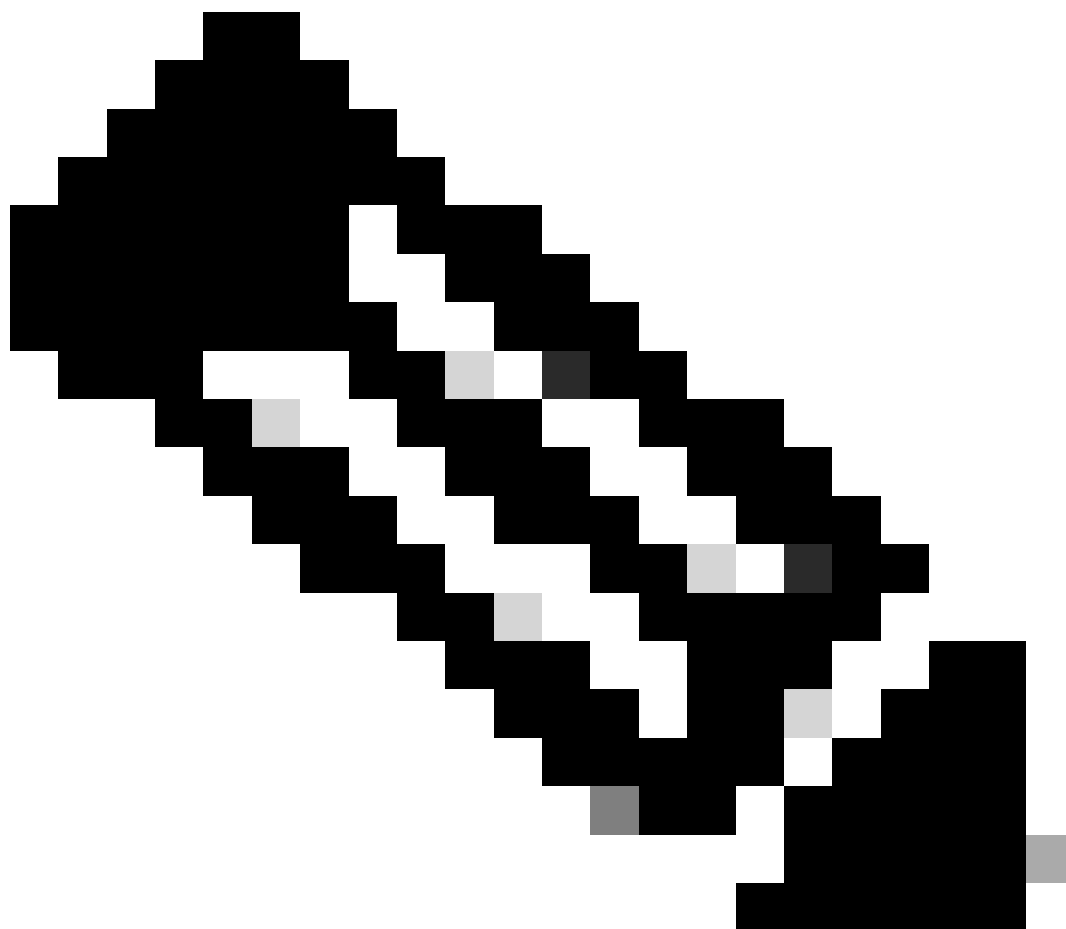
IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A	Node B
Device:* <input type="text" value="FTD_HOME"/>	Device:* <input type="text" value="Extranet"/>
Virtual Tunnel Interface:* <input type="text" value="PrimaryVTI (IP: 169.254.2.1)"/>	Device Name*: <input type="text" value="SecureAccess"/>
Tunnel Source: PrimaryWAN (IP: 192.168.30.5) Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers	Endpoint IP Address*: <input type="text" value="18.156.145.74,3.120.45.23"/>
Local Identity Configuration:* <input type="text" value="Email ID"/> <input type="text" value="jairohome@8195126-615626006-"/>	
Backup VTI: Remove	

- Nome da topologia: Criar um nome relacionado à integração do Secure Access
- Escolha **Routed Based (VTI)**

- Escolha **Point to Point**
 - IKE Version: **Escolher IKEv2**
-



Note: IKEv1 não é suportado para integração com o Secure Access.

Em **Node A**, você precisa configurar os próximos parâmetros:

Node A

Device:*

FTD_HOME

Virtual Tunnel Interface:*

PrimaryVTI (IP: 169.254.2.1)



Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

jairohome@

[+ Add Backup VTI \(optional\)](#)

- Device: Escolha seu dispositivo FTD
- Virtual Tunnel Interface: Escolha o VTI relacionado ao PrimaryWAN Interface.
- Marcar a caixa de seleção para Send Local Identity to Peers
- Local Identity Configuration: Escolha ID de e-mail e preencha as informações com base nas Primary Tunnel ID informações fornecidas na sua configuração na etapa, [Data for Tunnel Setup](#)

Depois de configurar as informações no PrimaryVTI clique em + Add Backup VTI:

Backup VTI:

Remove

Virtual Tunnel Interface:*

SecondaryVTI (IP: 169.254.3.1) ▼

+

Tunnel Source: SecondaryWAN (IP: 192.168.0.202) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@

- **Virtual Tunnel Interface:** Escolha o VTI relacionado ao PrimaryWAN Interface.
- Marcar a caixa de seleção para **Send Local Identity to Peers**
- **Local Identity Configuration:** Escolha ID de e-mail e preencha as informações com base nas **Secondary Tunnel ID** informações fornecidas na sua configuração na etapa, [Data for Tunnel Setup](#)

Em **Node B**, você precisa configurar os próximos parâmetros:

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- **Device:** Extranet
- **Device Name:** Escolha um Nome para reconhecer o Acesso Seguro como o destino.
- **Endpoint IP Address:** A configuração para primário e secundário deve ser primário **Datacenter IP**, **Secondary Datacenter IP**, você pode encontrar essas informações na etapa, [Data for Tunnel Setup](#)

Depois disso, sua configuração para **Endpoints** está concluída e você pode ir para a etapa, **Configuração IKE**.

Configuração de IKE

Para configurar os parâmetros IKE, clique em **IKE**.

Endpoints

IKE

IPsec

Advanced

Em **IKE**, você precisa configurar os próximos parâmetros:

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Umbrella-AES-GCM-256

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

- **Policies:** Você pode usar a configuração padrão do Umbrella `Umbrella-AES-GCM-256` ou configurar parâmetros diferentes com base no [Supported IKEv2 and IPSEC Parameters](#)
- **Authentication Type:** Chave manual pré-compartilhada
- **Key/Confirm Key:** Você pode encontrar as `Passphrase` informações na etapa [Data for Tunnel Setup](#)

Depois disso, sua configuração para **IKE** está concluída e você pode ir para a etapa Configuração de IPSEC.

Configuração de IPSEC

Para configurar os parâmetros IPSEC, clique em IPSEC.

Endpoints

IKE



IPsec

Advanced

Em IPSEC, você precisa configurar os próximos parâmetros:

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha	Umbrella-AES-GCM-256
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

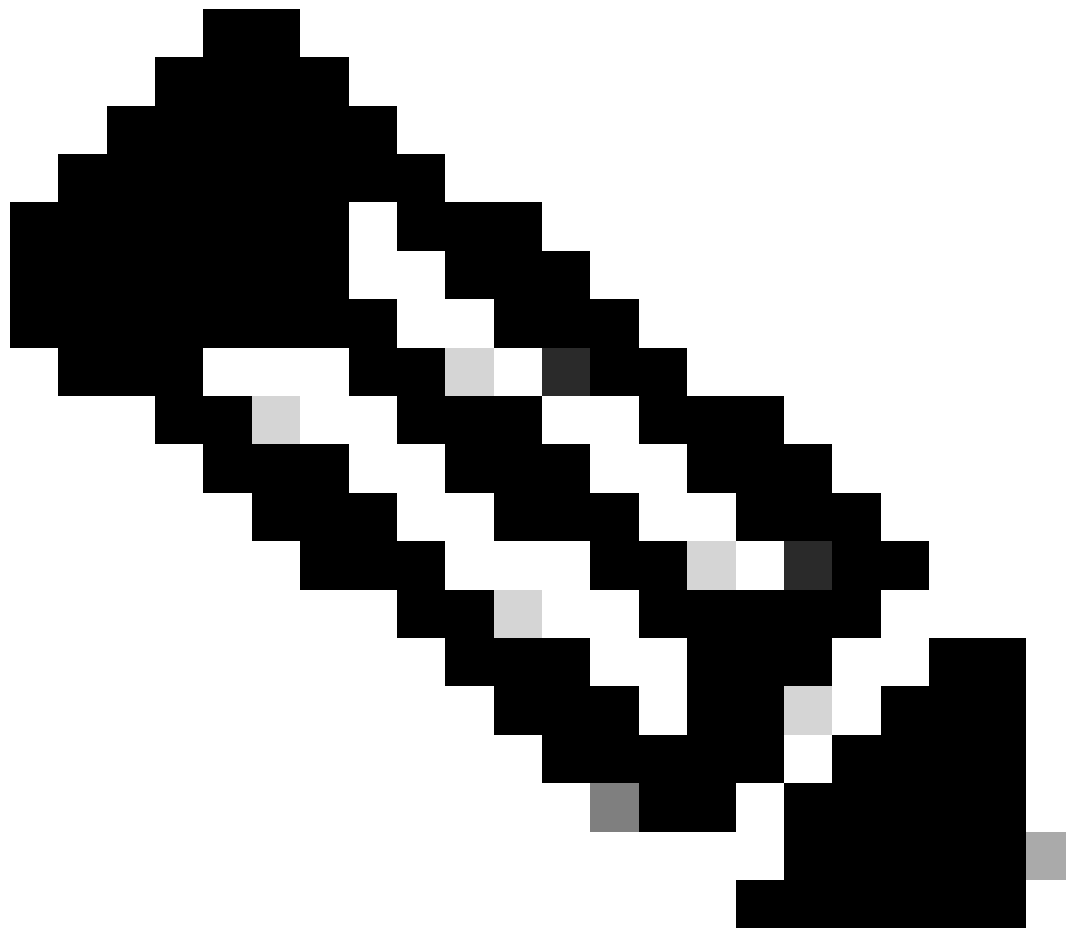
Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: Você pode usar a configuração padrão do Umbrella **Umbrella-AES-GCM-256** ou configurar parâmetros diferentes com base no [Supported IKEv2 and IPSEC Parameters](#)



Note: Nada mais é necessário no IPSEC.

Depois disso, sua configuração para IPSEC será concluída e você poderá ir para a etapa Configuração avançada.

Configuração avançada

Para configurar os parâmetros avançados, clique em Avançado.

Endpoints

IKE

IPsec

Advanced

Em *Advanced*, você precisa configurar os próximos parâmetros:

ISAKMP Settings

IKE Keepalive: Enable

Threshold: 10 Seconds (Range 10 - 3600)

Retry Interval: 2 Seconds (Range 2 - 10)

Identity Sent to Peers: autoOrDN

Peer Identity Validation: Do not check

Enable Aggressive Mode

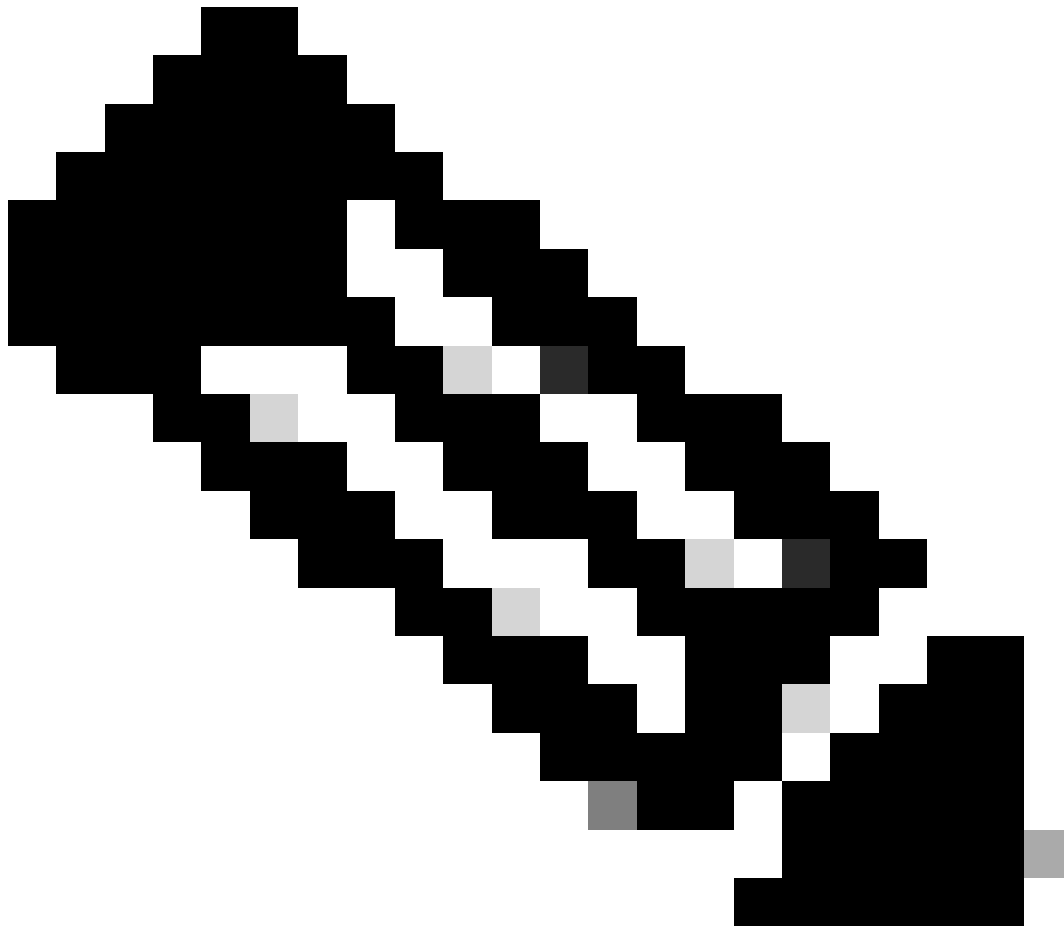
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive: Enable
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: autoOrDN
- Peer Identity Validation: Não verificar

Depois disso, você pode clicar em **Save e Deploy**.



Note: Após alguns minutos, você verá a VPN estabelecida para ambos os nós.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess	Route Based (VTI)	Point to Point	2 - Tunnels	✓	✓
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet	3.120.4... (3.120.45.23)●.....	FTD FTD_HOME	Secon... (192.168.0.202)	Seconda... (169.254.3.1)
EXTRANET Extranet	18.15... (18.156.145.74)●.....	FTD FTD_HOME	Primary... (192.168.30.5)	PrimaryVTI (169.254.2.1)

Depois disso, a configuração do VPN to Secure Access in VTI Mode será concluída e você poderá ir para a etapa **Configure Policy Base Routing**.



aviso: O tráfego para acesso seguro é encaminhado somente para o túnel principal quando ambos os túneis são estabelecidos; se o principal ficar inoperante, o acesso seguro permitirá que o tráfego seja encaminhado através do túnel secundário.

Observação: o failover no site do Secure Access é baseado nos valores de DPD documentados no [guia do usuário](#) para os valores de IPsec suportados.

Cenários de configuração da política de acesso

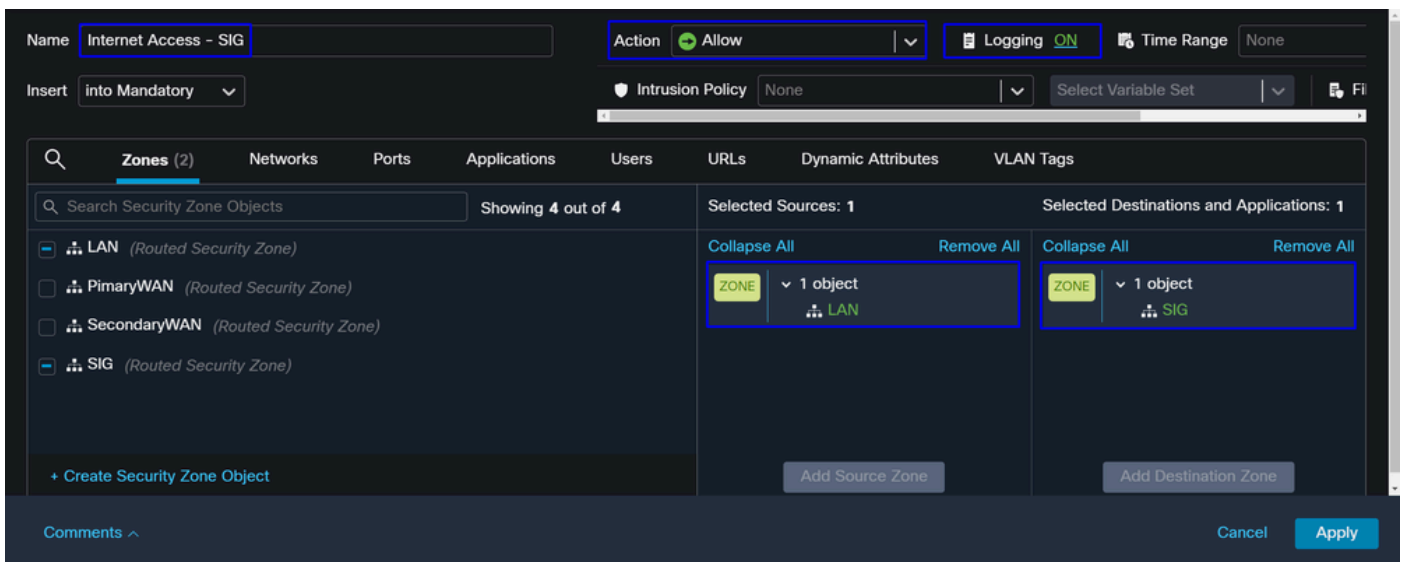
As regras de política de acesso definidas se baseiam em:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
● Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
● GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
● GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
● Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

Interface	Zona
VTIprimário	SIG
VTIsecundário	SIG
LAN	LAN

Cenário de acesso à Internet

Para fornecer acesso à Internet para todos os recursos que você configura no Roteamento de base de política, você precisa configurar algumas regras de acesso e também algumas políticas no acesso seguro, então deixe-me explicar como conseguir isso neste cenário:



Essa regra fornece acesso à Internet e, nesse caso, LAN a Internet está SIGdesativada.

Cenário de RA-VPN

Para fornecer acesso dos usuários do RA-VPN, você precisa configurá-lo com base no intervalo atribuído no pool do RA-VPN.



Note: Para configurar sua política RA-VPNaaS, você pode passar por [Gerenciar redes virtuais privadas](#)

Como você verifica o pool IP de seu VPNaaS?

Navegue até o [Painel do Secure Access](#)

- Clique em **Connect > End User Connectivity**
- Clique em **Virtual Private Network**
- Em **Manage IP Pools**, clique em **Manage**

End User Connectivity

↓ Cisco Secure Client

Manage DNS Servers (2)

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust

Virtual Private Network

Internet Security

Global FQDN

fb57.vpn.sse.cisco.com [Copy](#)

Manage IP Pools

2 Regions mapped

Manage

- Você vê sua piscina sob **Endpoint IP Pools**

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House

- Você precisa permitir esse intervalo em SIG, mas também deve adicioná-lo na ACL configurada em seu PBR.

Configuração de regra de acesso

Se você estiver configurando apenas o Acesso seguro para usá-lo com os recursos para acessar os recursos de aplicativos particulares, sua regra de acesso poderá ter esta aparência:

Name: Private APP, Action: Allow, Logging: ON, Time Range: None, Insert: into Mandatory, Intrusion Policy: None, Select Variable Set: [None]

Search Network and Geolocation Objects: Showing 27 out of 27

Networks	Geolocations
<input type="checkbox"/> 192.168.0.150 (Host Object)	192.168.0.150
<input type="checkbox"/> 192.168.10.153 (Host Object)	192.168.10.153
<input type="checkbox"/> any (Network Group)	0.0.0.0::/0
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0
<input type="checkbox"/> any-ipv6 (Host Object)	::/0

Selected Sources: 2

- ZONE: 1 object (SIG)
- NET: 1 object (192.168.50.0/24)

Selected Destinations and Applications: 1

- ZONE: 1 object (LAN)

Buttons: Add Source Network, Add Destination Network, Comments, Cancel, Apply

Essa regra permite o tráfego do pool de RA-VPN 192.168.50.0/24 para sua LAN; você pode especificar mais, se necessário.

Configuração da ACL

Para permitir o tráfego de roteamento de SIG para sua LAN, você deve adicioná-lo na ACL para fazê-lo funcionar no PBR.

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	192.168.10.0/24	Any	192.168.50.0/24	Any	Any	Any	
2	Block	Any	Any	Any	Any	Any	Any	

Cenário ZTNA CLAP-BAP

Você deve configurar sua rede com base no intervalo CGNAT 100.64.0.0/10 para fornecer acesso à sua rede a partir dos usuários Client Base ZTA ou Browser Base ZTA.

Configuração de regra de acesso

Se você estiver configurando apenas o Acesso seguro para usá-lo com os recursos para acessar os recursos de aplicativos particulares, sua regra de acesso poderá ter esta aparência:

Name: ZTNA Access - IN Action: Allow Logging: ON Time Range: None Rule Enabled: ON

Insert: into Mandatory Intrusion Policy: None Select Variable Set: File Policy: None

Showing 27 out of 27

Selected Sources: 2

- ZONE SIG
- NET 100.64.0.0/10 (CGNAT RANGE)

Selected Destinations and Applications: 1

- ZONE LAN

Essa regra permite o tráfego do intervalo ZTNA CGNAT 100.64.0.0/10 para sua LAN.

Configuração da ACL

Para permitir o tráfego de roteamento de SIG usando CGNAT para sua LAN, você deve adicioná-lo na ACL para fazê-lo funcionar sob o PBR.

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	192.168.10.0/24	Any	100.64.0.0/10	Any	Any	Any	
2	Block	Any	Any	Any	Any	Any	Any	

Configurar o Roteamento Base da Política

Para fornecer acesso a recursos internos e à Internet por meio do Secure Access, você deve criar rotas por meio do Roteamento Base de Política (PBR - Policy Base Routing) que facilitam o roteamento do tráfego da origem para o destino.

- Navegue até **Devices > Device Management**
- Escolha o dispositivo FTD onde você criou a rota

<input type="checkbox"/>	Name	Model	Version
<input type="checkbox"/>	Ungrouped (1)		
<input type="checkbox"/>	FTD_HOME Snort 3 192.168.0.201 - Routed	FTDv for VMware	7.2.5

- Clique em **Routing**
- Escolha **Policy Base Routing**
- Clique em **Add**

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress Interfaces accordingly

[Configure Interface Priority](#) [Add](#)

Neste cenário, você seleciona todas as interfaces que usa como origem para rotear o tráfego para o Secure Access ou para fornecer autenticação de usuário para o Secure Access usando RA-VPN ou acesso ZTA baseado em cliente ou navegador aos recursos internos da rede:

- Em Interface de ingresso, selecione todas as interfaces que enviam tráfego através do Secure Access:

Edit Policy Based Route

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

Ingress Interface*

LAN x

- Em Match Criteria and Egress Interface, você define os próximos parâmetros depois de clicar em **Add**:

Match Criteria and Egress Interface
Specify forward action for chosen match criteria.

[Add](#)

Add Forwarding Actions

Match ACL:* Select... +

Send To:* IP Address

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

Internal Sources

Match ACL:* ACL

Send To:* IP Address

IPv4 Addresses: 169.254.2.2, 169.254.3.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

- **Match ACL:** Para essa ACL, você configura tudo o que é roteado para o Secure Access:

Traffic to the destination 208.67.222.222 or 208.67.220.220 over DNS using TCP or UDP will not be routed to Secure Access

✗ REJECT

Name: SSPT_FTD_ACL

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.222.220	Any
2	Allow	192.168.10.0/24	Any	Any	Any

Traffic from the source 192.168.10.0/24 will be routed to Secure Access

Depends how you play with the ACL, you can define how the traffic must be routed to Secure Access

✓ ACCEPT

- **Send To:** Escolher endereço IP
- **IPv4 Addresses:** Você deve usar o próximo IP sob a máscara 30 configurada em ambos os VTIs; você pode verificar isso na etapa [Config](#) da [interface VTI](#)

Interface	IP	GW
VTIprimário	169.254.2.1/30	169.254.2.2
VTIsecundário	169.254.3.1/30	169.254.3.2

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2 → 169.254.2.2, 169.254.3.2

Depois de configurá-lo dessa forma, você obterá o próximo resultado e poderá continuar clicando

em Save:

The screenshot shows a configuration window for an ACL. The following fields are highlighted with blue boxes:

- Match ACL:* **ACL**
- Send To:* **IP Address**
- IPv4 Addresses: **169.254.2.2, 169.254.3.2**
- IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:
- Don't Fragment: **None**

Below these fields, there is a checkbox for "Default Interface" which is unchecked. There are tabs for "IPv4 settings" (selected) and "IPv6 settings". Under "IPv4 settings", there are fields for "Recursive:" (For example, 192.168.0.1) and "Default:" (For example, 192.168.0.1, 10.10.10.1). There is also a checkbox for "Peer Address" which is unchecked, and a "Verify Availability" button with a "+" icon. At the bottom right, there are "Cancel" and "Save" buttons.

Depois disso, você precisará save fazer isso novamente e configurá-lo da seguinte maneira:

The screenshot shows a configuration window for a policy-based route. At the top, it says "A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces". Below this, there is a dropdown menu for "Ingress Interface*" with "LAN" selected. Underneath, there is a section titled "Match Criteria and Egress Interface" with the instruction "Specify forward action for chosen match criteria." and an "Add" button. A table below shows the configuration:

Match ACL	Forwarding Action
ACL	Send through 169.254.2.2 169.254.3.2 Send the traffic to the PrimaryVTI

There are edit and delete icons to the right of the table row. Below the table, there is a note: "If PrimaryVTI fail it will send the traffic to the SecondaryVTI". At the bottom right, there are "Cancel" and "Save" buttons.

Depois disso, você poderá Implantar e verá o tráfego das máquinas configuradas na ACL que faz o roteamento do tráfego para Acesso seguro:



Note: Por padrão, a Política de acesso seguro padrão permite o tráfego para a Internet. Para fornecer acesso a aplicativos privados, você precisa criar recursos privados e adicioná-los à política de acesso para acesso a recursos privados.

Configurar a Diretiva de Acesso à Internet no Acesso Seguro

Para configurar o acesso para acesso à Internet, você precisa criar a política no [Painel de Acesso Seguro](#):

- Clique em **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Clique em `Add Rule > Internet Access`

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

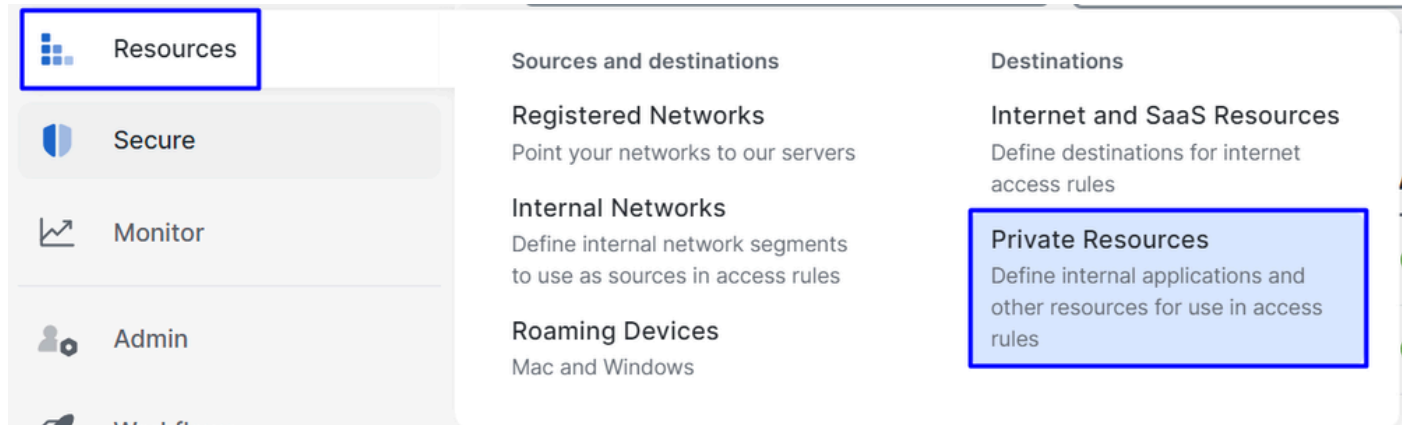
Control and secure access to public destinations from within your network and from managed devices

Nela, você pode especificar a origem como o túnel e, para o destino, você pode escolher qualquer um, dependendo do que deseja configurar na política. Verifique o [Guia do usuário do Secure Access](#).

Configurar o acesso a recursos privados para ZTNA e RA-VPN

Para configurar o acesso para recursos privados, você precisa criar os recursos primeiro no [Painel de Acesso Seguro](#):

Clique em **Resources** > **Private Resources**



- Depois, clique em **ADD**

Na configuração, você encontrará as próximas seções para configurar: **General**, **Communication with Secure Access Cloud and Endpoint Connection Methods**.

General

General

Private Resource Name

Description (optional)

- **Private Resource Name** : Crie um nome para o recurso ao qual você fornece acesso por meio do **Acesso Seguro** à sua rede

Métodos de Conexão de Endpoint

Zero-trust connections
 Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
 Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection
 Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ
 https:// ⓘ

Protocol **Server Name Indication (SNI)** (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections:** Marque a caixa de seleção.
- **Client-based connection:** Se você habilitá-lo, poderá usar o Secure Client - Zero Trust Module para habilitar o acesso por meio do modo baseado no cliente.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** Configurar os recursos IP ou FQDN; se você configurar o FQDN, precisará adicionar o DNS para resolver o nome.
- **Browser-based connection:** Se você habilitá-lo, poderá acessar seus recursos por meio do navegador (somente adicione recursos com comunicação HTTP ou HTTPS)
- **Public URL for this resource:** Configurar o URL público que você usa através do navegador; O acesso seguro protege esse recurso.
- **Protocol:** Selecionar o protocolo (HTTP ou HTTPS)

VPN connections
 Allow endpoints to connect to this resource when connected to the network using VPN.

VPN Connection: Marque a caixa de seleção para habilitar o acesso via RA-VPNaaS.

Depois disso, clique em **Save** e você poderá adicionar esse recurso ao **Access Policy**.

Configurar a política de acesso

Ao criar o recurso, você precisa atribuí-lo a uma das políticas de acesso seguro:

- Clique em **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Clique em **Add > Private Resource**

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

Para essa regra de acesso privado, você configura os valores padrão para fornecer acesso ao recurso. Para saber mais sobre configurações de diretivas, consulte o [Guia do usuário](#).

1 Specify Access

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

Action

<input checked="" type="radio"/> Allow Allow specified traffic if security requirements are met.	<input type="radio"/> Block Block specified traffic.
--	--

From

Specify one or more sources.

Information about sources, including selecting multiple sources. [Help](#)

To

Specify one or more destinations.

Information about destinations, including selecting multiple destinations. [Help](#)

- **Action** : Escolha Permitir para fornecer acesso ao recurso.
- **From** : Especifique o usuário que pode ser usado para fazer logon no recurso.
- **To** : Escolha o recurso que você deseja acessar por meio do Acesso seguro.

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

<input type="checkbox"/> Zero-Trust Client-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is installed. <input type="text" value="System provided (Client-based)"/>
Private Resources: SplunkFTD
<input type="checkbox"/> Zero Trust Browser-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is NOT installed. <input type="text" value="System provided (Browser-based)"/>
Private Resources: SplunkFTD

- **Zero-Trust Client-based Posture Profile**: Escolha o perfil padrão para o acesso da base de clientes
- **Zero-Trust Browser-based Posture Profile**: Escolha o acesso básico do navegador de perfil padrão



Note: Para saber mais sobre a política de postura, consulte o [guia do usuário](#) para obter acesso seguro.

Depois disso, clique em **Next** e **Save** e sua configuração, e você pode tentar acessar seus recursos por meio de RA-VPN e Client Base ZTNA ou Browser Base ZTNA.

Troubleshooting

Para solucionar problemas com base na comunicação entre o Firewall Seguro e o Acesso Seguro, você pode verificar se a Fase 1 (IKEv2) e a Fase 2 (IPSEC) foram estabelecidas entre os dispositivos sem problemas.

Verificar Fase1 (IKEv2)

Para verificar a Fase 1, você precisa executar o próximo comando na CLI do FTD:

```
show crypto isakmp sa
```

Nesse caso, a saída desejada é dois IKEv2 SAs IPs do data center de acesso seguro e o status desejado é **READY**:

```
There are no IKEv1 SAs
```

```
IKEv2 SAs:
```

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
52346451 192.168.0.202/4500 3.120.45.23/4500
  Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/4009 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xfb34754c/0xc27fd2ba
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
52442403 192.168.30.5/4500 18.156.145.74/4500
  Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/3891 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x4af761fd/0xfbca3343
```

Verificar Fase2 (IPSEC)

Para verificar a Fase2, você precisa executar o próximo comando na CLI do FTD:

```
interface: PrimaryVTI
  Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.5

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer: 18.156.145.74

  #pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965
  #pkts decaps: 91325, #pkts decrypt: 91325, #pkts verify: 91325
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.30.5/4500, remote crypto endpt.: 18.156.145.74/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: FBCA3343
current inbound spi : 4AF761FD

inbound esp sas:

spi: 0x4AF761FD (1257726461)

SA State: active

transform: esp-aes-gcm-256 esp-null-hmac no compression

in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }

slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1

sa timing: remaining key lifetime (kB/sec): (3916242/27571)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:

spi: 0xFBCA3343 (4224332611)

SA State: active

transform: esp-aes-gcm-256 esp-null-hmac no compression

in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }

slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1

sa timing: remaining key lifetime (kB/sec): (4239174/27571)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

interface: SecondaryVTI

Crypto map tag: __vti-crypto-map-Tunnel2-0-2, seq num: 65280, local addr: 192.168.0.202

Protected vrf (ivrf): Global

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: 3.120.45.23

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#TFC rcvd: 0, #TFC sent: 0

#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0

#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.0.202/4500, remote crypto endpt.: 3.120.45.23/4500

path mtu 1500, ipsec overhead 63(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: C27FD2BA

current inbound spi : FB34754C

inbound esp sas:

spi: 0xFB34754C (4214519116)

SA State: active

transform: esp-aes-gcm-256 esp-null-hmac no compression

```

in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4101120/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
outbound esp sas:
spi: 0xC27FD2BA (3263156922)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4239360/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

```

Na última saída, você pode ver os dois túneis estabelecidos; o que não é desejado é a próxima saída sob o pacote `encaps` e `decaps`.

```

#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

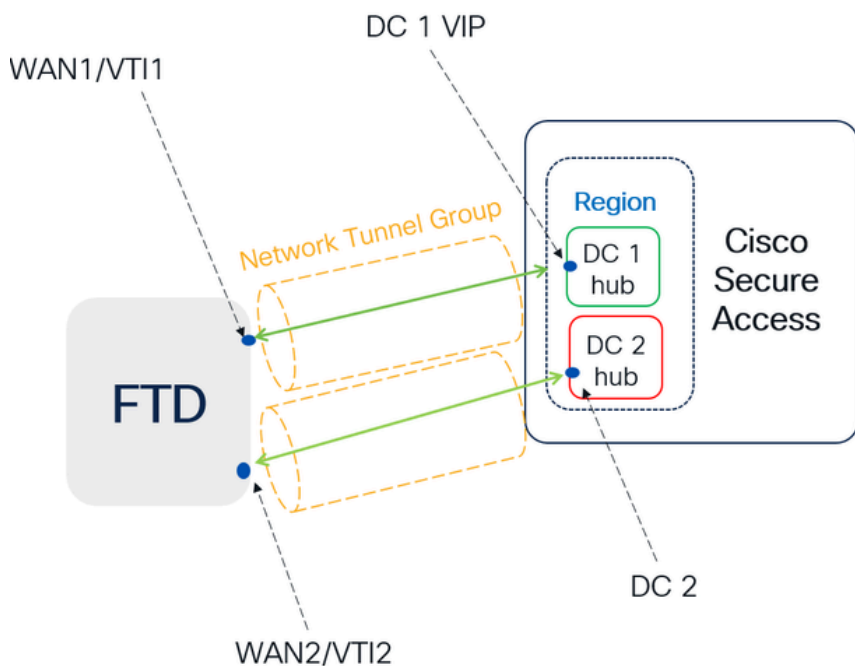
```

Se você tiver esse cenário, abra um caso no TAC.

Função de alta disponibilidade

A função dos túneis com acesso seguro que se comunicam com o data center na nuvem é ativa/passiva, o que significa que apenas a porta para DC 1 estará aberta para receber tráfego; a porta DC 2 fica fechada até que o túnel número 1 se desligue.

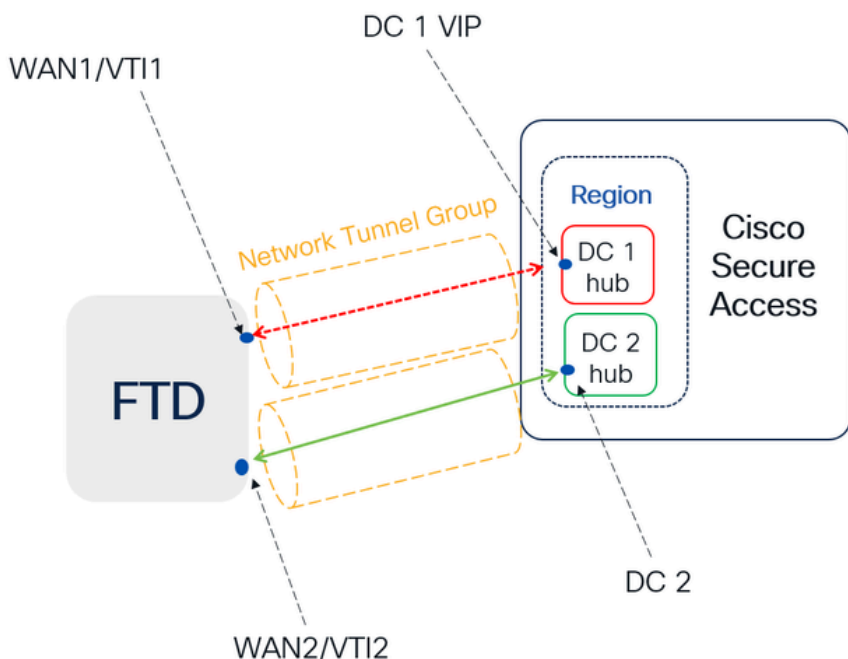
Normal Behavior



Secure Access default behavior

- DC2 is **passive** when DC1 is **active**
- Data Centers operating in High Availability (HA) mode ensure that only one tunnel receives traffic at a time. The other tunnel remains on standby and will drop any packets sent through it while in standby mode.

HA Behavior



Secure Access HA Behavior

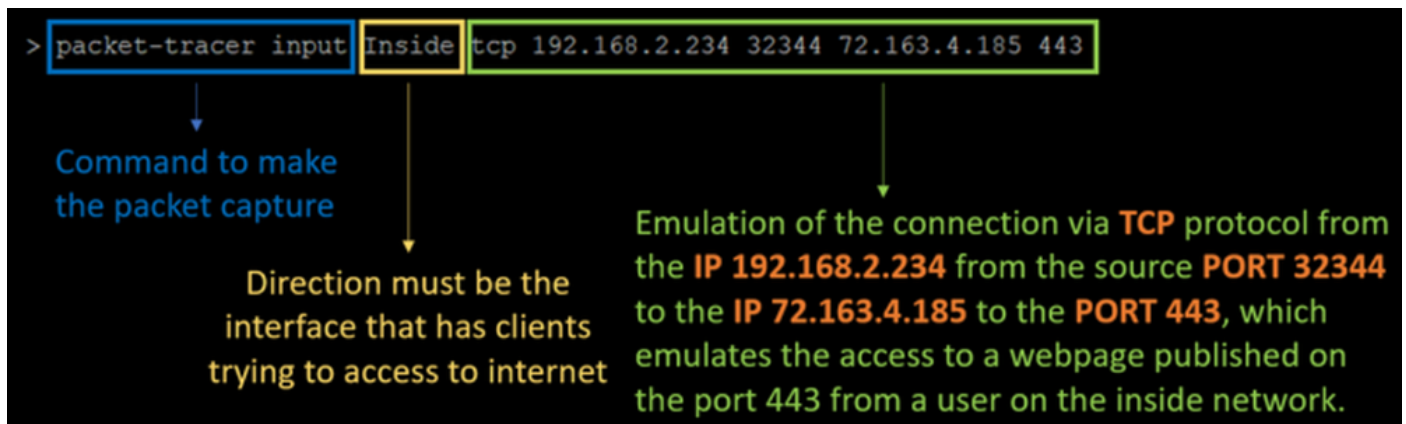
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

Verificar o roteamento de tráfego para proteger o acesso

Neste exemplo, usamos a origem como a máquina na rede de firewall:

- Fonte: 192.168.10.40
- Destino: 146.112.255.40 (IP de monitoramento de acesso seguro)

Exemplo:



Comando:

```
packet-tracer input LAN tcp 192.168.10.40 3422 146.112.255.40 80
```

Saída:

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 14010 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

```
Phase: 3
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:
  Source Object Group Match Count:      0
  Destination Object Group Match Count:  0
```

Object Group Search: 0

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 233 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any ifc PrimaryVTI any rule-id 268434435
access-list CSM_FW_ACL_ remark rule-id 268434435: ACCESS POLICY: HOUSE - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434435: L7 RULE: New-Rule-#3-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
class-map class_map_Any
match access-list Any
policy-map policy_map_LAN
class class_map_Any
set connection decrement-ttl
service-policy policy_map_LAN interface LAN
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Elapsed time: 18680 ns
Config:
Additional Information:

Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Elapsed time: 25218 ns
Config:
Additional Information:

Phase: 10

Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 14944 ns
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 19614 ns
Config:
Additional Information:
New flow created with id 23811, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 27086 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Phase: 15
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 450193 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268434435
Additional Information:
Starting rule matching, zone 1 -> 3, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0,
Matched rule ids 268434435 - Allow

Result:
input-interface: LAN(vrfid:0)
input-status: up
input-line-status: up
output-interface: PrimaryVTI(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 620979 ns

Aqui, muitas coisas podem nos dar contexto sobre a comunicação e saber se tudo está corretamente na configuração de PBR para rotear o tráfego corretamente para o acesso seguro:

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

PrimaryVTI A Fase 2 indica que o tráfego está sendo encaminhado para a interface, o que está correto porque, com base nas configurações neste cenário, o tráfego da Internet deve ser encaminhado para o Secure Access através do VTI.

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information:

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.