

Configure o acesso seguro com o firewall Fortigate

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar a VPN no acesso seguro](#)

[Dados do túnel](#)

[Configure o site VPN para o site no Fortigate](#)

[Rede](#)

[Autenticação](#)

[Fase 1 Proposta](#)

[Fase 2 Proposta](#)

[Configurar a interface do túnel](#)

[Configurar Rota de Política](#)

[Verificar](#)

Introdução

Este documento descreve como configurar o acesso seguro com o Firewall Fortigate.

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:

- Firewall da versão Fortigate 7.4.x
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA sem cliente

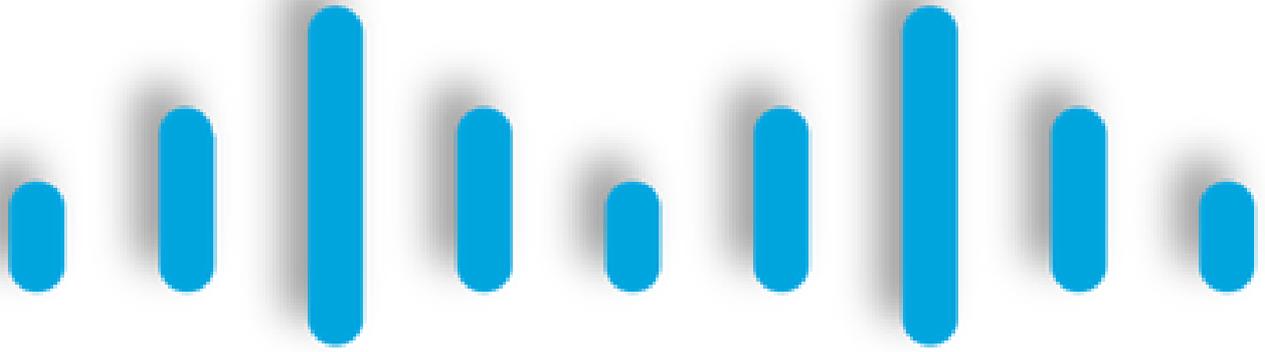
Componentes Utilizados

As informações neste documento são baseadas em:

- Firewall da versão Fortigate 7.4.x
- 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

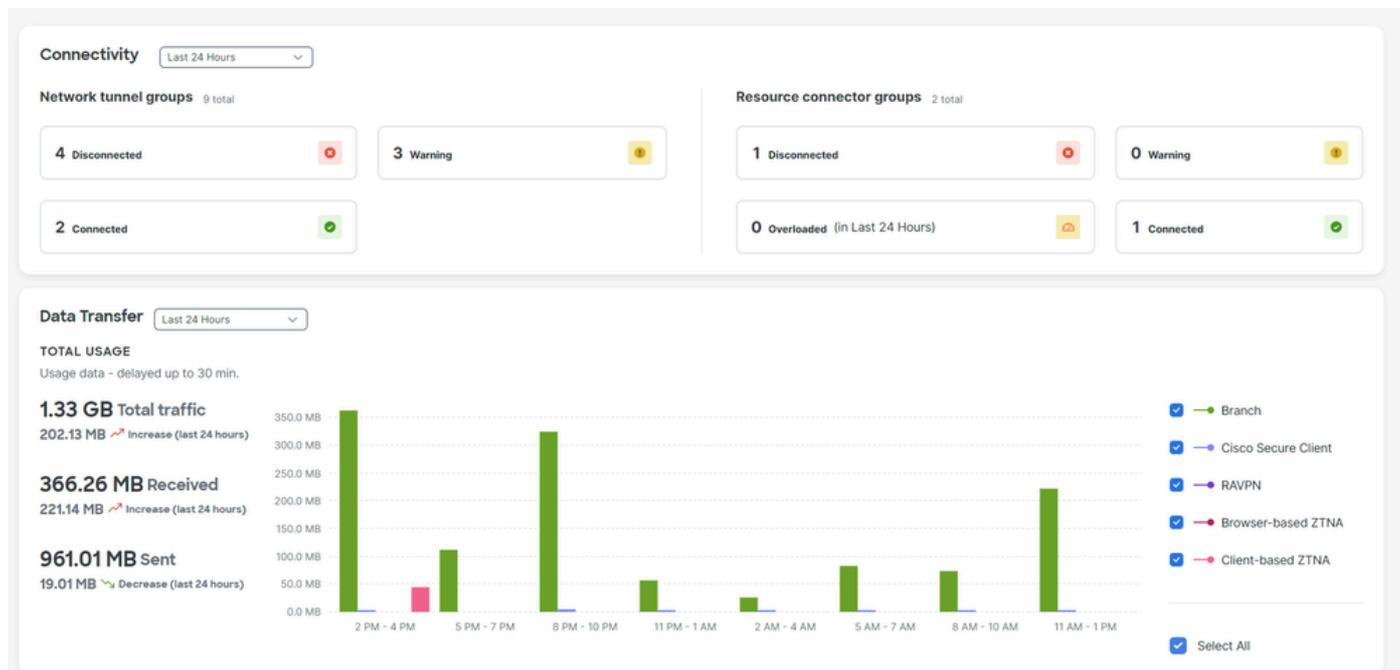
FORTINET®

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.

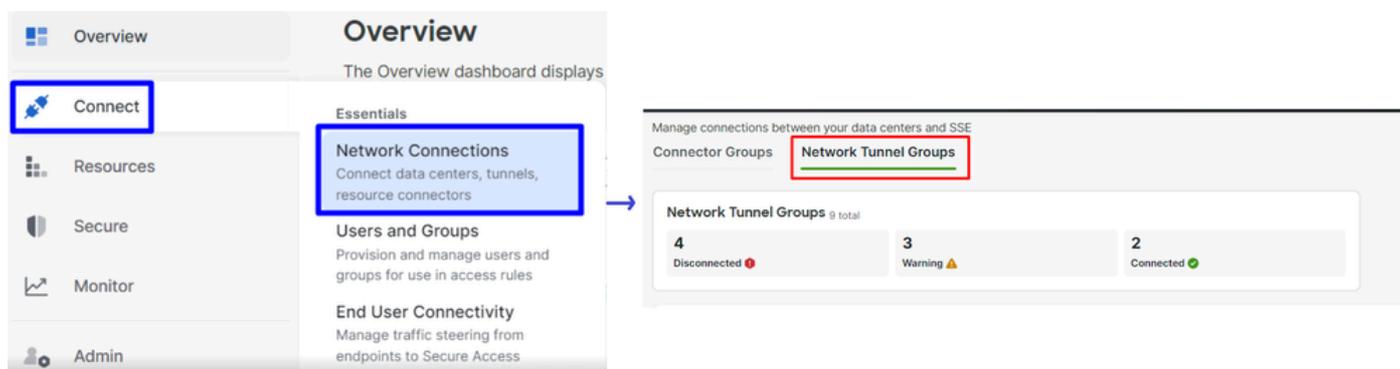
Configurar

Configurar a VPN no acesso seguro

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



- Clique em **Connect > Network Connections > Network Tunnels Groups**



- Em Network Tunnel Groups clique em + Add

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to security control user access to the Internet and private resources. [Help](#)

Search Region Status 9 Tunnel Groups



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

✓ 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 a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

Region

Device Type

Cancel

Next



Observação: escolha a região mais próxima ao local do firewall.

-
- Configure o Tunnel ID Format e Passphrase
 - Clique emNext

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

Email IP Address

Tunnel ID

fortigate @<org>
<hub>.sse.cisco.com

Passphrase

.....

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

.....



Cancel

Back

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**

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

Network subnet overlap

Enable NAT / Outbound only

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

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

192.168.100.0/24

Dynamic routing

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



Cancel

Back

Save

Depois de clicar nas informações sobre **Save** o túnel que são exibidas, salve essas informações para a próxima etapa, **Configure the VPN Site**

to Site on Fortigate.

Dados do túnel

Data for Tunnel Setup

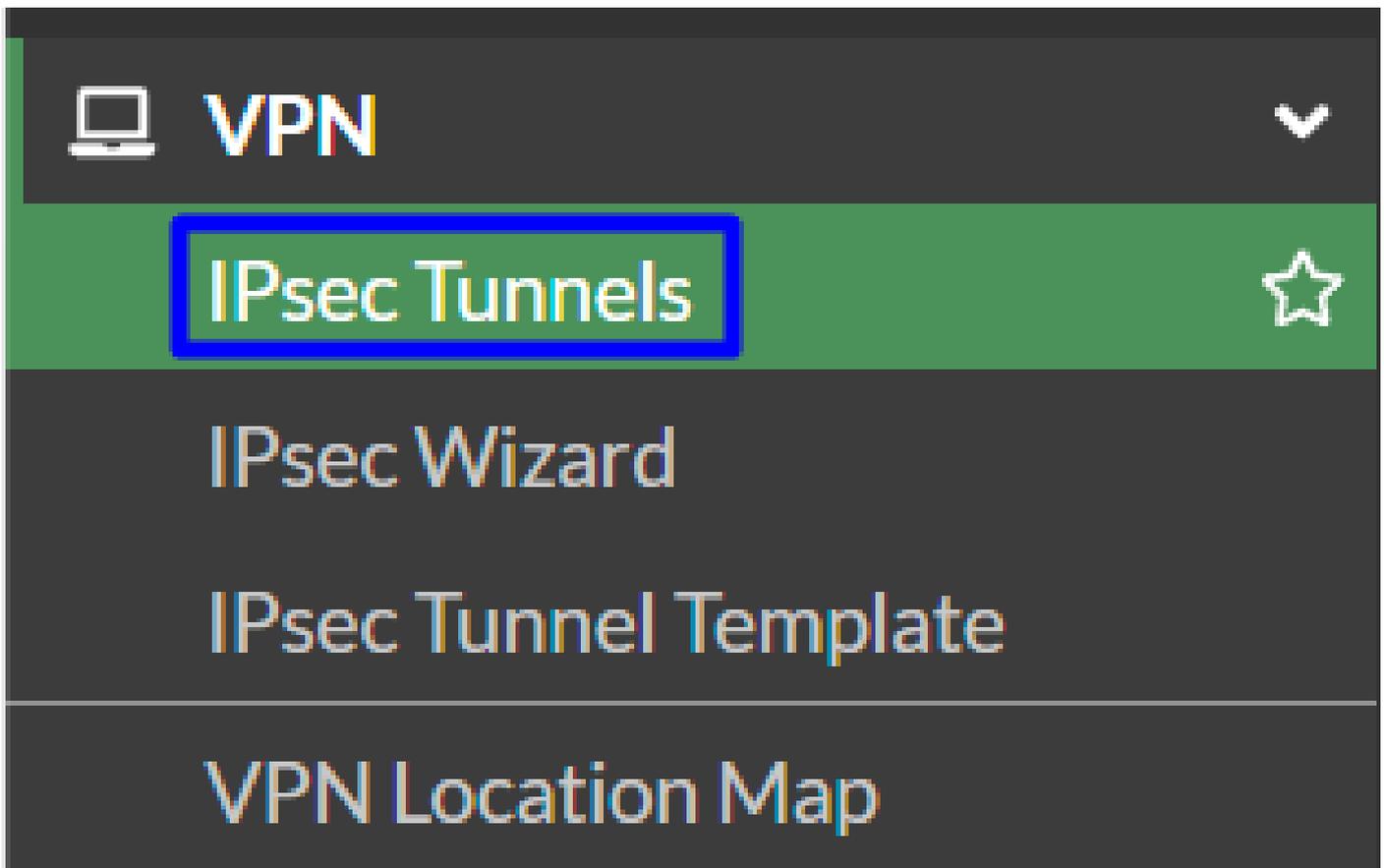
Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	@	-sse.cisco.com	
Primary Data Center IP Address:	18.156.145.74		
Secondary Tunnel ID:	@	-sse.cisco.com	
Secondary Data Center IP Address:	3.120.45.23		
Passphrase:		CP	

Configure o site VPN para o site no Fortigate

Navegue até o painel Fortificar.

- Clique em VPN > IPsec Tunnels



- Clique em Create New > IPsec Tunnels

+ Create new ▾

IPsec Tunnel

IPsec Aggregate

Custom 2

- Clique em Custom , configure um **Name** e clique em Next.

1 VPN Setup

Name 2 Cisco Secure

Template type Site to Site Hub-and-Spoke Remote Access Custom 1

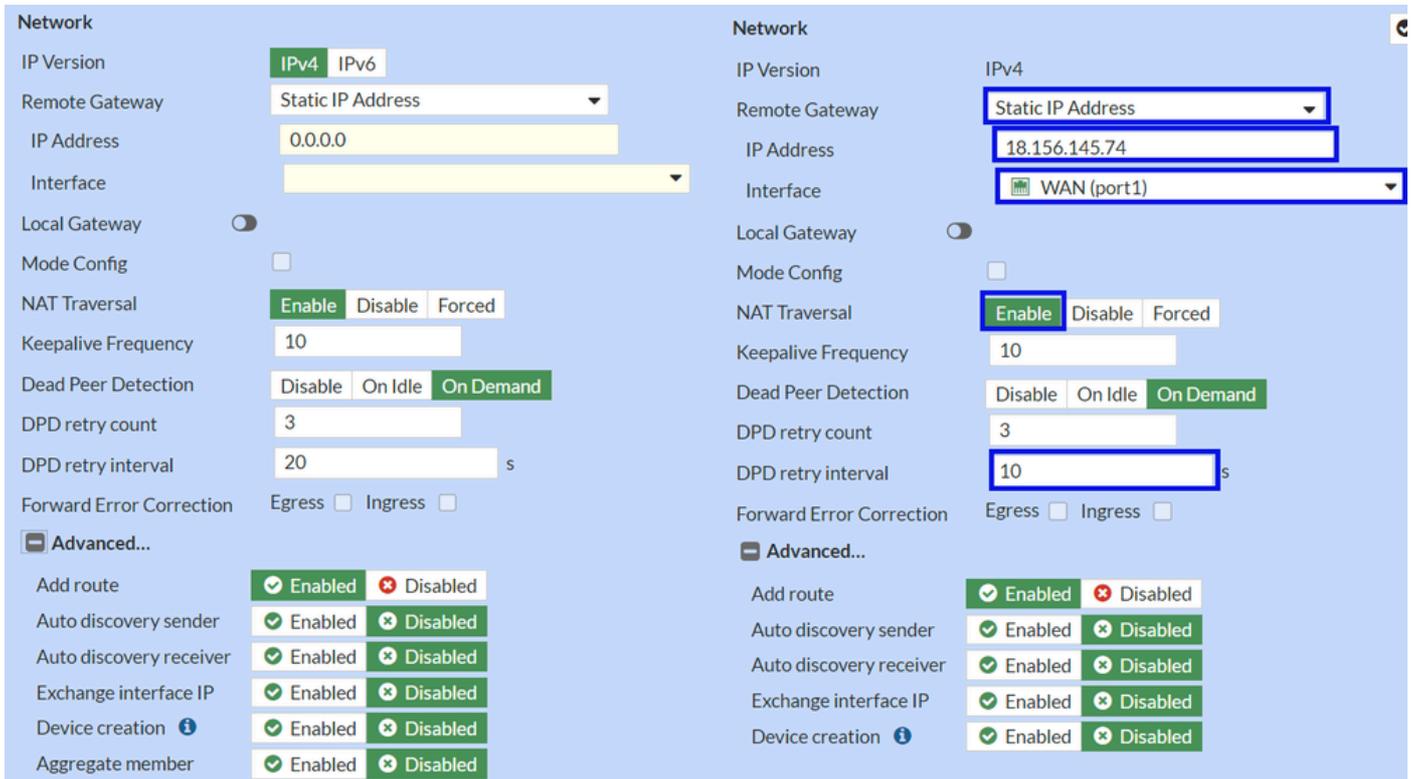
< Back

3 Next >

Cancel

Na próxima imagem, você verá como é necessário definir as configurações da **Network** peça.

Rede



- Network

- IP Version :IPv4

- **Remote Gateway** :Endereço IP estático
- **IP Address**: Use o IP de Primary IP Datacenter IP Address,fornevido na etapa [Dados do túnel](#)
- **Interface** : Escolha a interface WAN que você planejou usar para estabelecer o túnel
- **Local Gateway** : Desabilitar como padrão
- **Mode Config** : Desabilitar como padrão
- **NAT Traversal** :Enable
- **Keepalive Frequency** :10
- **Dead Peer Detection** : sob demanda
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : Não marque nenhuma caixa.
- **Advanced...:** configure-o como a imagem.

Agora configure o IKE **Authentication**.

Autenticação

Authentication		Authentication	
Method	Pre-shared Key	Method	Pre-shared Key
Pre-shared Key		Pre-shared Key	••••••••
IKE		IKE	
Version	1 2	Version	1 2
Mode	Aggressive Main (ID protection)		

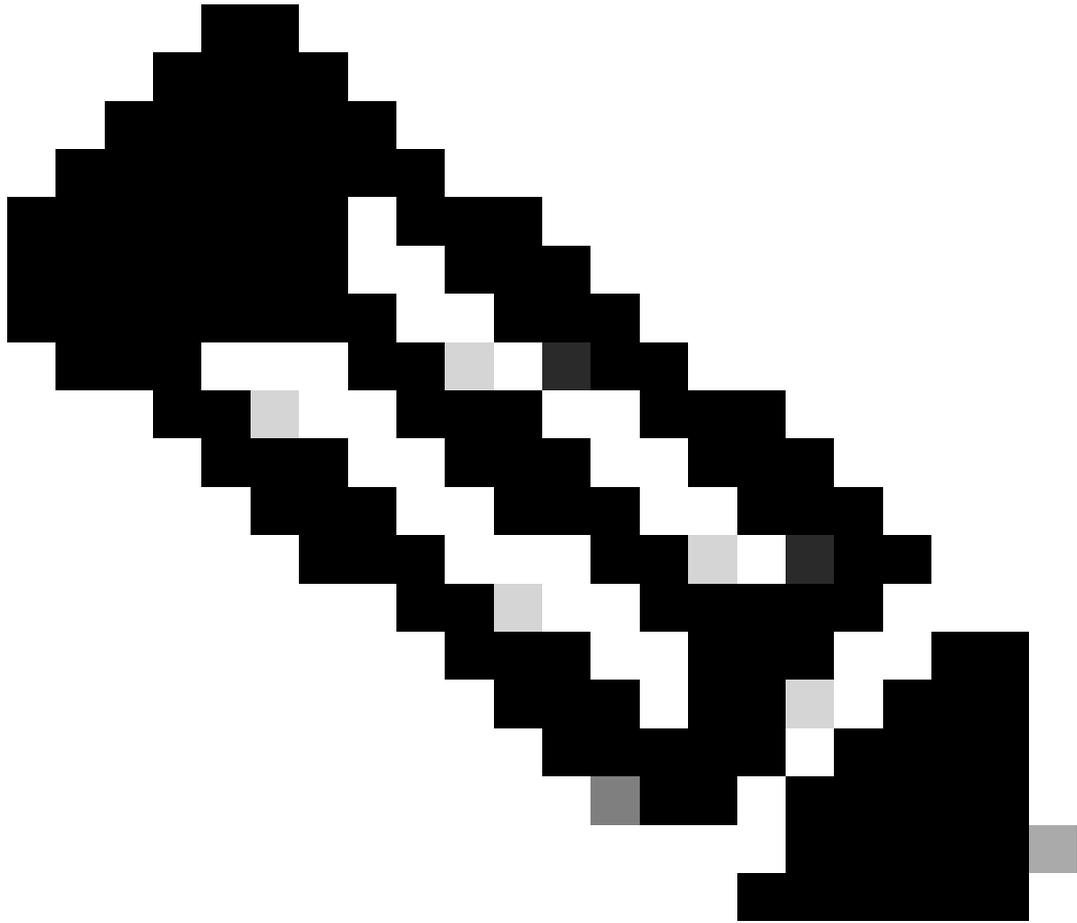
- **Authentication**

- **Method** : Chave pré-compartilhada como padrão

- **Pre-shared Key** : Use o **Passphrase** da etapa [Dados do túnel](#)

- **IKE**

- **Version** : Escolha a versão 2.



Observação: o Secure Access suporta apenas IKEv2

Agora configure o **Phase 1 Proposal**.

Fase 1 Proposta

The image shows two screenshots of a configuration interface for Phase 1 Proposal. The left screenshot shows a list of four proposals with encryption and authentication settings. The right screenshot shows a detailed view of a proposal with encryption set to AES256, authentication set to SHA256, Diffie-Hellman Groups 19 and 20 selected, Key Lifetime set to 86400, and Local ID set to fortigate@8195126-621099508-sse.ci.

- Phase 1 Proposal

- Encryption : Escolha AES256

- Authentication : Escolha SHA256
- Diffie-Hellman Groups : Marque as caixas 19 e 20
- Key Lifetime (seconds) : 86400 como padrão
- Local ID : Use o comando Primary Tunnel ID, fornecido na etapa [Dados do túnel](#)

Agora configure o **Phase 2 Proposal**.

Fase 2 Proposta

New Phase 2

Name: CSA

Comments: Comments

Local Address: addr_subnet 0.0.0.0/0.0.0.0

Remote Address: addr_subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal **Add**

Encryption	AES128	Authentication	SHA1	X
Encryption	AES256	Authentication	SHA1	X
Encryption	AES128	Authentication	SHA256	X
Encryption	AES256	Authentication	SHA256	X
Encryption	AES128GCM			X
Encryption	AES256GCM			X
Encryption	CHACHA20POLY1305			X

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 32 31 30 29 28 27
 21 20 19 18 17 16
 15 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds
43200

New Phase 2

Name: CSA

Comments: Comments

Local Address: addr_subnet 0.0.0.0/0.0.0.0

Remote Address: addr_subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal **Add**

Encryption: AES128 Authentication: SHA256

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds
43200

- New Phase 2
 - **Name** : Deixe como padrão (tirado do nome da sua VPN)
 - **Local Address** : Deixe como padrão (0.0.0.0/0.0.0.0)
 - **Remote Address** : Deixe como padrão (0.0.0.0/0.0.0.0)

- Advanced
 - **Encryption** : Escolha AES128
 - **Authentication** : Escolha SHA256
 - **Enable Replay Detection** : Deixe como padrão (Habilitado)
 - **Enable Perfect Forward Secrecy (PFS)** : Desmarcar a caixa de seleção
 - **Local Port** : Deixe como padrão (Habilitado)

- **Remote Port:** Deixe como padrão (Habilitado)
- **Protocol :** Deixe como padrão (Habilitado)
- **Auto-negotiate :** Deixar como padrão (Desmarcado)
- **Autokey Keep Alive :** Deixar como padrão (Desmarcado)
- **Key Lifetime :** Deixe como padrão (segundos)
- **Seconds :** Deixe como padrão (43200)

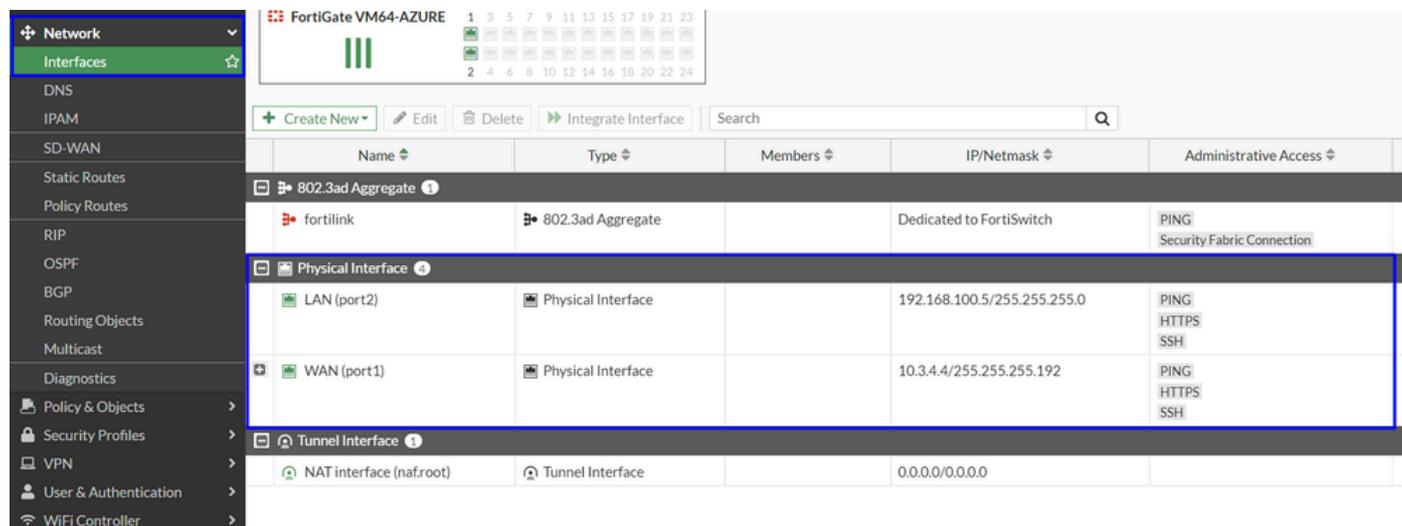
Depois disso, clique em OK. Após alguns minutos, você verá que a VPN foi estabelecida com o Secure Access e poderá continuar com a próxima etapa, **Configure the Tunnel Interface**.



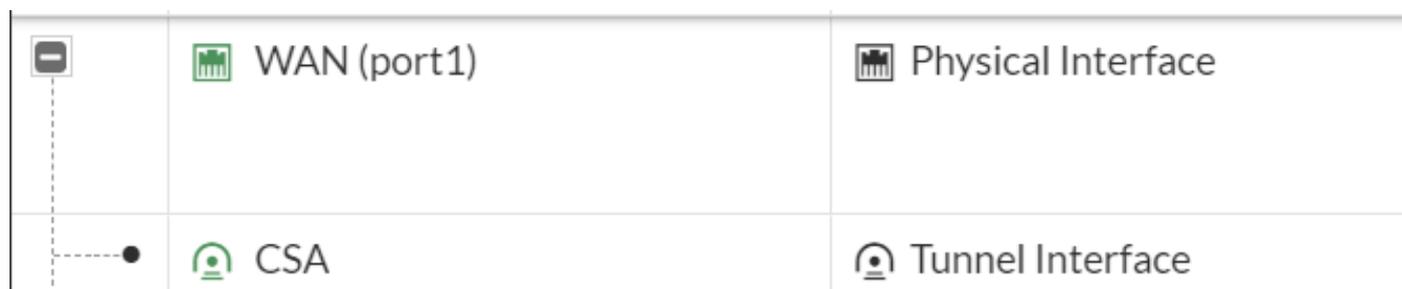
Configurar a interface do túnel

Depois que o túnel for criado, você perceberá que há uma nova interface atrás da porta que está usando como interface WAN para se comunicar com o Secure Access.

Para verificar isso, navegue até **Network > Interfaces**.



Expanda a porta que você usa para se comunicar com o Secure Access; nesse caso, a **WAN** interface.



- Clique no **Tunnel Interface** e em **Edit**

+ Create New Edit Delete Integrate Interface Search	
Name	Type
802.3ad Aggregate 1	
fortilink	802.3ad Aggregate
Physical Interface 4	
LAN (port2)	Physical Interface
WAN (port1)	Physical Interface
CSA	Tunnel Interface

- Você tem a próxima imagem que precisa configurar

Name
 Alias
 Type
 Interface
 VRF ID
 Role

Name
 Alias
 Type
 Interface
 VRF ID
 Role

Address

Addressing mode

IP

Netmask

Remote IP/Netmask

Address

Addressing mode

IP

Netmask

Remote IP/Netmask

- Interface Configuration

- IP : Configure um IP não roteável que você não tenha em sua rede (169.254.0.1)
- Remote IP/Netmask : configure o IP remoto como o próximo IP do IP da interface e com uma máscara de rede de 30 (169.254.0.2 255.255.255.252)

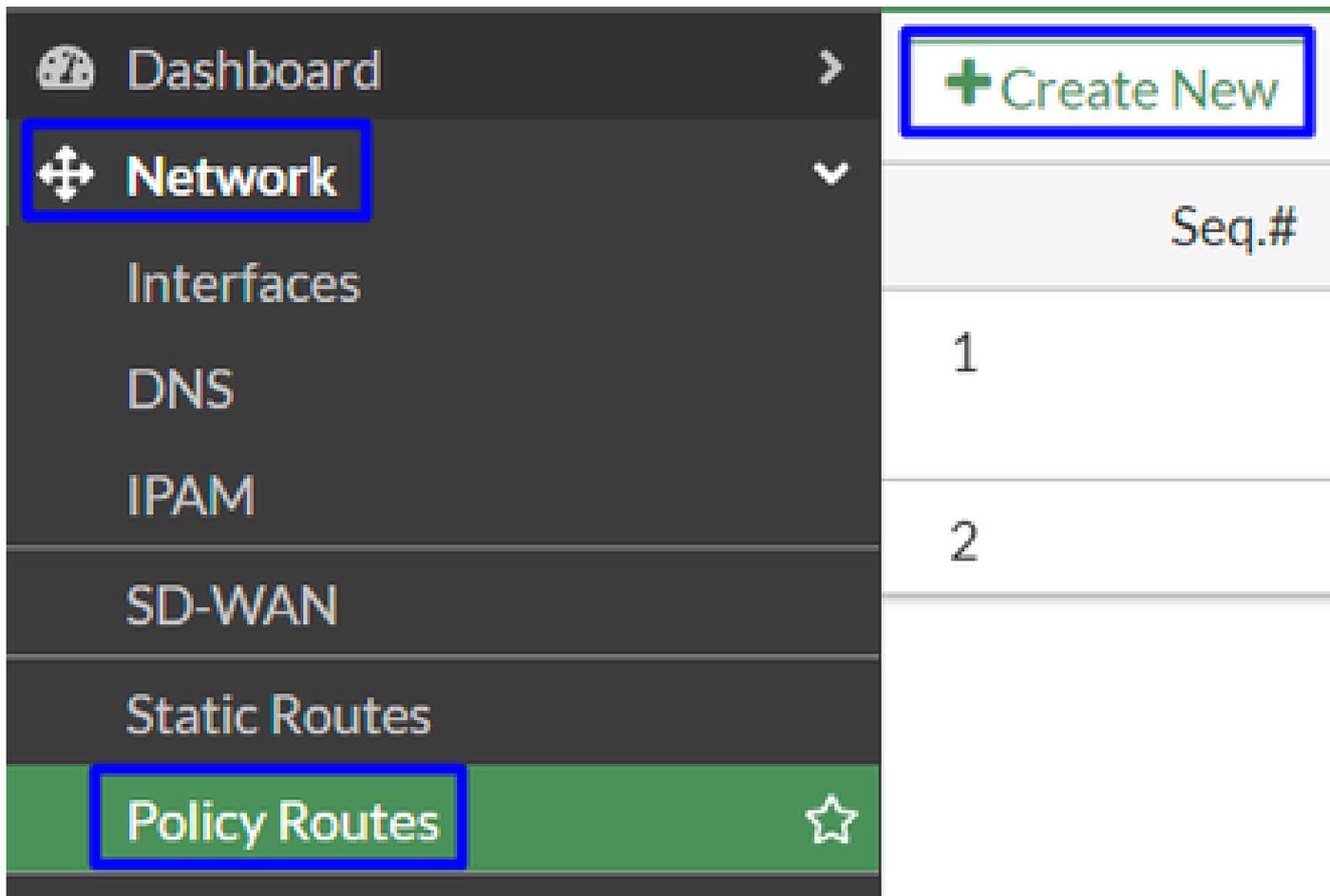
Depois disso, clique **OK** para salvar a configuração e continuar com a próxima etapa, Configure Policy Route (Roteamento baseado na origem).



Aviso: Após esta parte, você deve configurar as Políticas de Firewall em seu FortiGate para permitir ou permitir o tráfego de seu dispositivo para Acesso Seguro e de Acesso Seguro para as redes que você deseja rotear o tráfego.

Neste ponto, você tem sua VPN configurada e estabelecida para acesso seguro; agora, você deve redirecionar o tráfego para acesso seguro para proteger seu tráfego ou acesso a seus aplicativos privados por trás do firewall FortiGate.

- Navegue até Network > Policy Routes



The screenshot shows the FortiGate web interface. On the left is a dark navigation menu with the following items: Dashboard, Network (highlighted with a blue box), Interfaces, DNS, IPAM, SD-WAN, Static Routes, and Policy Routes (highlighted with a blue box and a star icon). On the right, there is a '+ Create New' button (highlighted with a blue box) and a table with a single column labeled 'Seq.#'. The table contains two rows with the values '1' and '2'.

Seq.#
1
2

- Configurar a política

If incoming traffic matches:	If incoming traffic matches:
Incoming interface <input type="text" value="+"/>	Incoming interface <input type="text" value="LAN (port2)"/>
Source Address	Source Address
IP/Netmask <input type="text"/>	IP/Netmask <input type="text" value="192.168.100.0/255.255.255.0"/>
Addresses <input type="text" value="+"/>	Addresses <input type="text" value="+"/>
Destination Address	Destination Address
IP/Netmask <input type="text"/>	IP/Netmask <input type="text"/>
Addresses <input type="text" value="+"/>	Addresses <input type="text" value="all"/>
Internet service <input type="text" value="+"/>	Internet service <input type="text" value="+"/>
Protocol <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="SCTP"/> <input checked="" type="text" value="ANY"/> <input type="text" value="Specify"/>	Protocol <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="SCTP"/> <input checked="" type="text" value="ANY"/> <input type="text" value="Specify"/>
Type of service <input type="text" value="0"/>	Type of service <input type="text" value="0"/>
<input type="text" value="0x00"/> Bit Mask <input type="text" value="0x00"/>	<input type="text" value="0x00"/> Bit Mask <input type="text" value="0x00"/>
Then:	Then:
Action <input checked="" type="text" value="Forward Traffic"/> <input type="text" value="Stop Policy Routing"/>	Action <input checked="" type="text" value="Forward Traffic"/> <input type="text" value="Stop Policy Routing"/>
Outgoing interface <input checked="" type="radio"/> <input type="radio"/> <input type="text" value="CSA"/>	Outgoing interface <input checked="" type="radio"/> <input type="radio"/> <input type="text" value="CSA"/>
Gateway address <input type="text"/>	Gateway address <input type="text" value="169.254.0.2"/>
Comments <input type="text" value="Write a comment..."/>	Comments <input type="text" value="Write a comment..."/>
Status <input checked="" type="text" value="Enabled"/> <input type="text" value="Disabled"/>	Status <input checked="" type="text" value="Enabled"/> <input type="text" value="Disabled"/>

- If Incoming traffic matches
 - Incoming Interface : Escolha a interface de onde você planejou redirecionar o tráfego para o Secure Access (origem do tráfego)

- Source Address
 - IP/Netmask : use esta opção apenas se você rotear uma sub-rede de uma interface
 - Addresses : use esta opção se você tiver o objeto criado e a origem do tráfego vier de várias interfaces e várias sub-redes

- Destination Addresses
 - Addresses: Escolher all

- Protocol: Escolher **ANY**

- Then
 - Action: **Choose Forward Traffic**

 - Outgoing Interface : Escolha a interface de túnel que você modificou na etapa, [Configurar interface de túnel](#)
 - Gateway Address: Configure o IP remoto configurado na etapa, [RemoteIPNetmask](#)
 - Status : Escolher Habilitado

Clique **OK** para salvar a configuração. Agora, você está pronto para verificar se o tráfego de seus dispositivos foi roteado novamente para o Secure Access.

Verificar

Para verificar se o tráfego da sua máquina foi redirecionado para o Secure Access, você tem duas opções: você pode verificar na Internet e seu IP público ou executar o próximo comando com curl:

<#root>

```
C:\Windows\system32>curl ipinfo.io { "ip": "151.186.197.1", "city": "Frankfurt am Main", "region": "Hes
```

O intervalo público de onde você pode ver seu tráfego é de:

Min Host:151.186.176.1

Max Host :151.186.207.254



Observação: esses IPs estão sujeitos a alterações, o que significa que a Cisco provavelmente estenderá esse intervalo no futuro.

Se você vir a alteração de seu IP público, isso significa que você está sendo protegido pelo Secure Access e agora você pode configurar seu aplicativo privado no painel do Secure Access para acessar seus aplicativos de VPNaaS ou ZTNA.

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.