

Configuración del acceso seguro con Fortigate Firewall

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de la VPN en Secure Access](#)

[Datos del túnel](#)

[Configuración del sitio VPN a sitio en Fortigate](#)

[Red](#)

[Autenticación](#)

[Fase 1 Propuesta](#)

[Fase 2 Propuesta](#)

[Configuración de la interfaz de túnel](#)

[Configurar ruta de política](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar Secure Access con Fortigate Firewall.

Prerequisites

- [Configurar aprovisionamiento de usuarios](#)
- [Configuración de Autenticación SSO de ZTNA](#)
- [Configurar acceso seguro VPN de acceso remoto](#)

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall de la versión Fortigate 7.4.x
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA
- ZTNA sin cliente

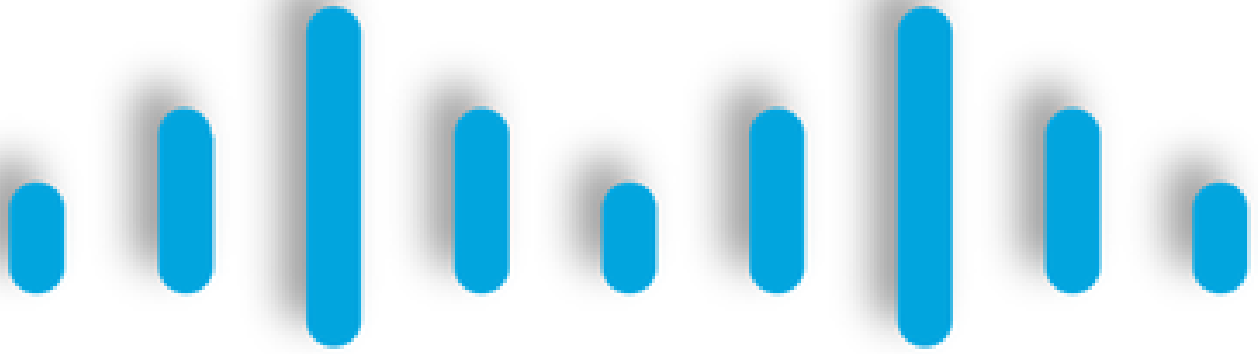
Componentes Utilizados

La información de este documento se basa en:

- Firewall de la versión Fortigate 7.4.x
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes



CISCO

Secure

Access

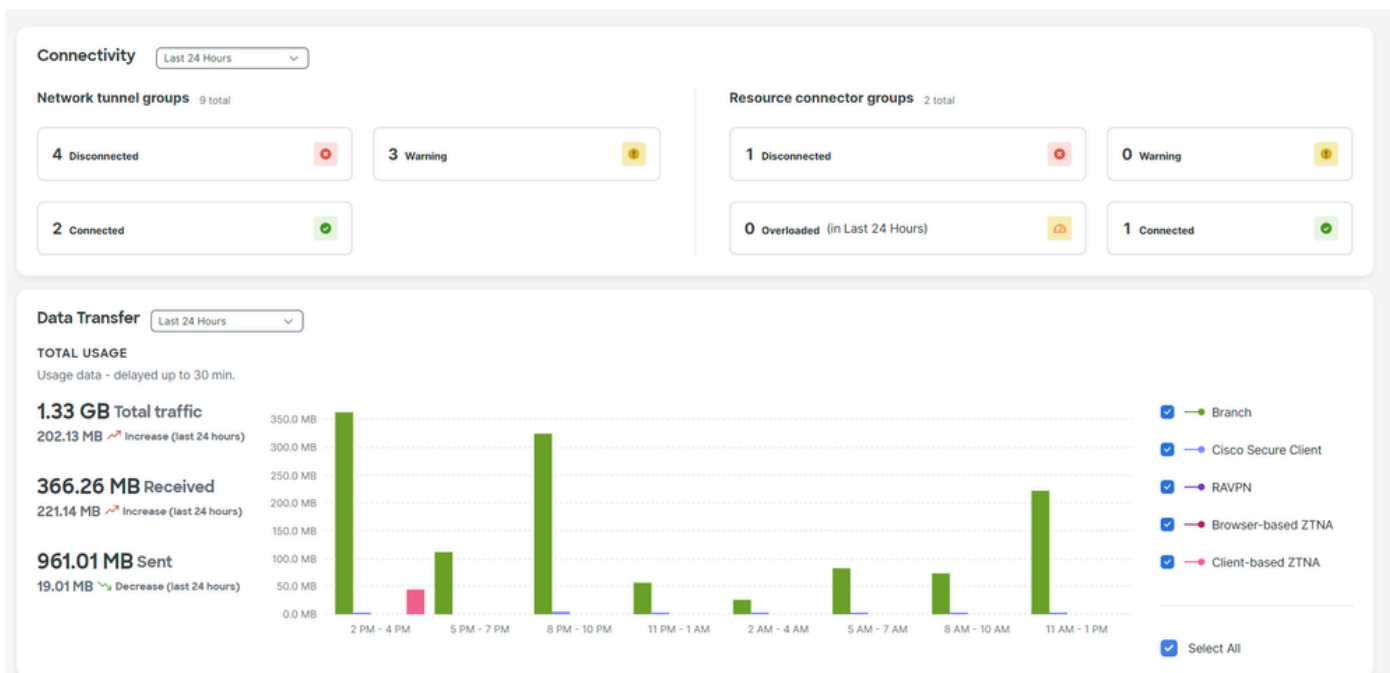
FORTINET®

Cisco ha diseñado Secure Access para proteger y proporcionar acceso a aplicaciones privadas, tanto in situ como basadas en la nube. También protege la conexión de la red a Internet. Esto se consigue mediante la implementación de varios métodos y capas de seguridad, todo ello con el objetivo de preservar la información a medida que acceden a ella a través de la nube.

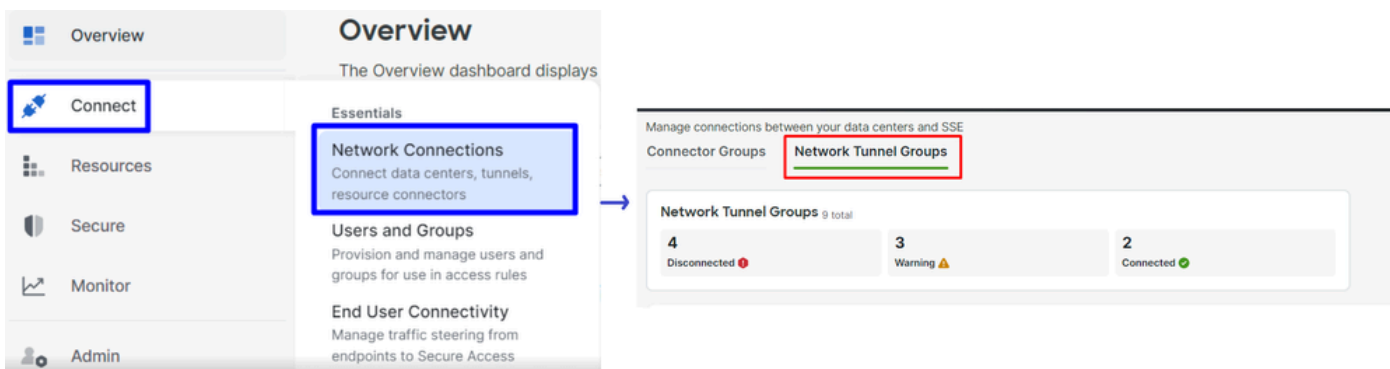
Configurar

Configuración de la VPN en Secure Access

Vaya al panel de administración de [Secure Access](#).



- Haga clic en **Connect > Network Connections > Network Tunnels Groups**



- En Network Tunnel Groups haga clic en **+ 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



- Configurar Tunnel Group Name, Regiony Device Type
- Haga clic en **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



Nota: Seleccione la región más cercana a la ubicación del firewall.

-
- Configure el Tunnel ID Format y Passphrase
 - Haga clic enNext

- ✓ 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 los rangos de direcciones IP o los hosts que ha configurado en la red y que desea que el tráfico pase a través de Secure Access
- Haga clic en **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

Después de hacer clic en **Save** la información sobre el túnel se muestra, guarde esa información para el siguiente paso, **Configure the VPN Site to Site on Fortigate**.

Datos del túnel

Data for Tunnel Setup

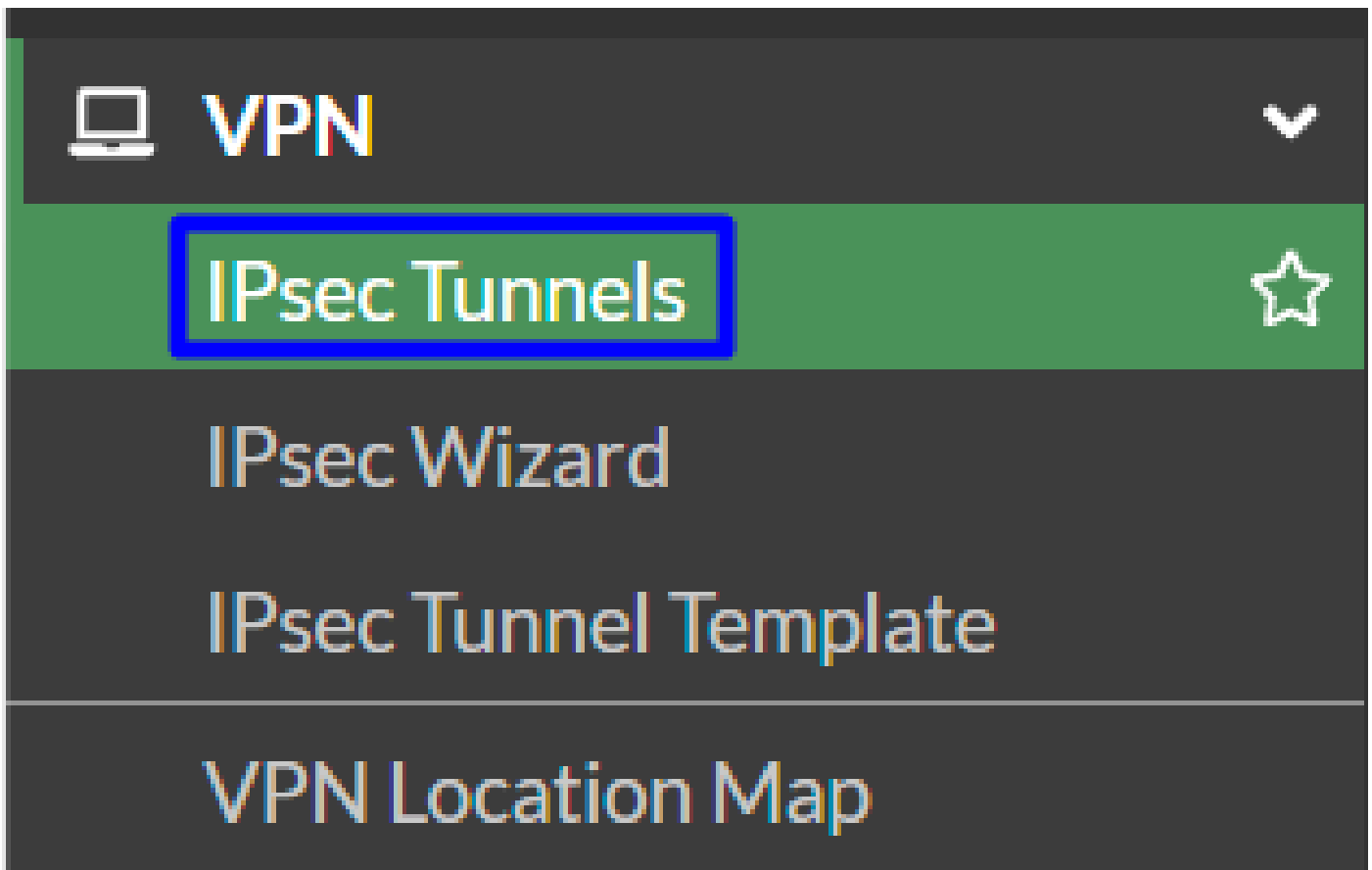
Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

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	

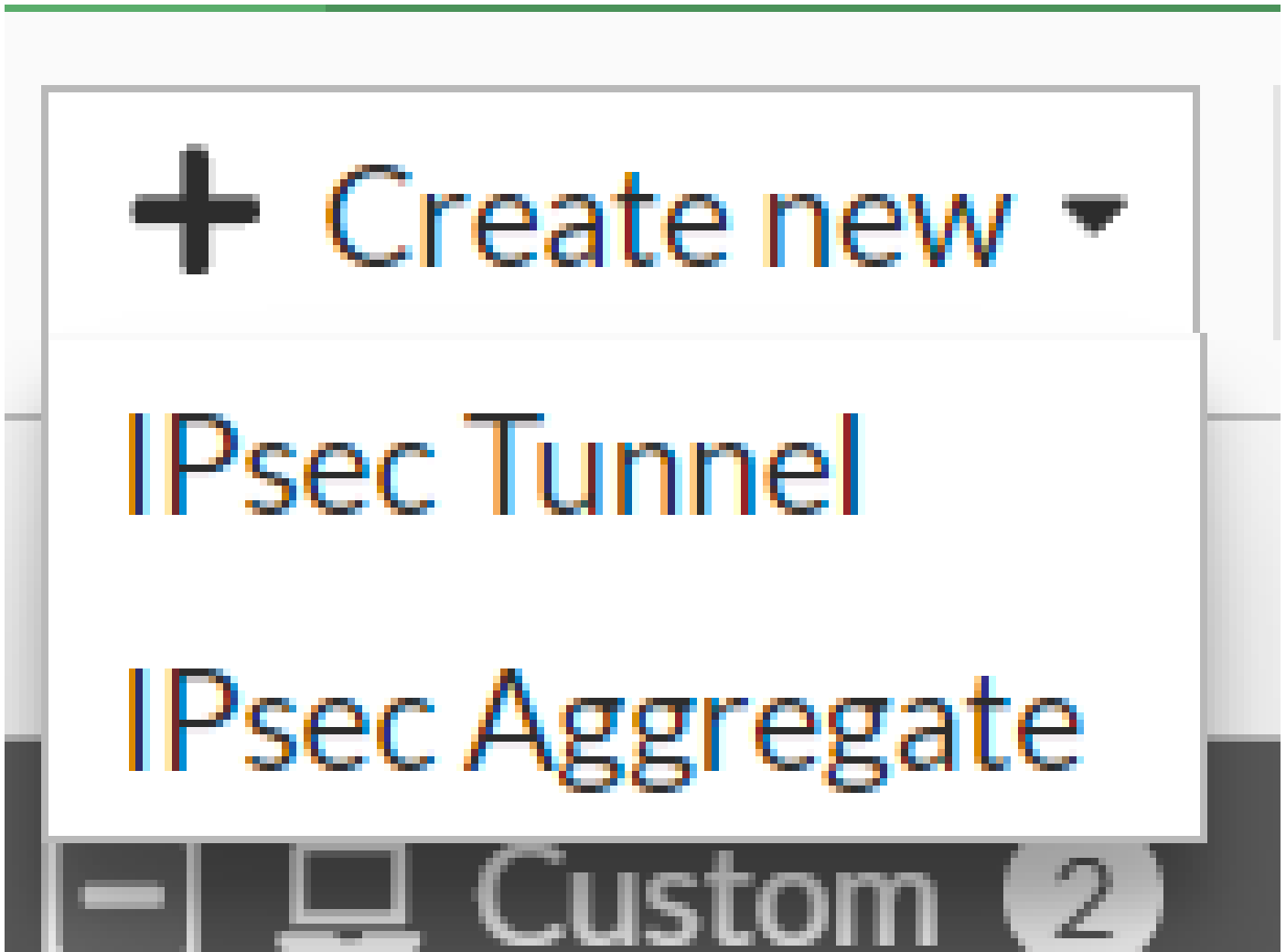
Configuración del sitio VPN a sitio en Fortigate

Desplácese hasta el panel de Fortigate.

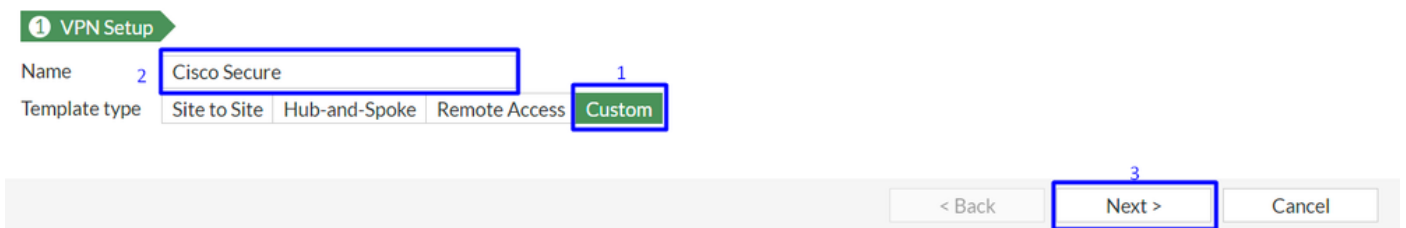
- Haga clic en VPN > IPsec Tunnels



- Haga clic en Create New > IPsec Tunnels

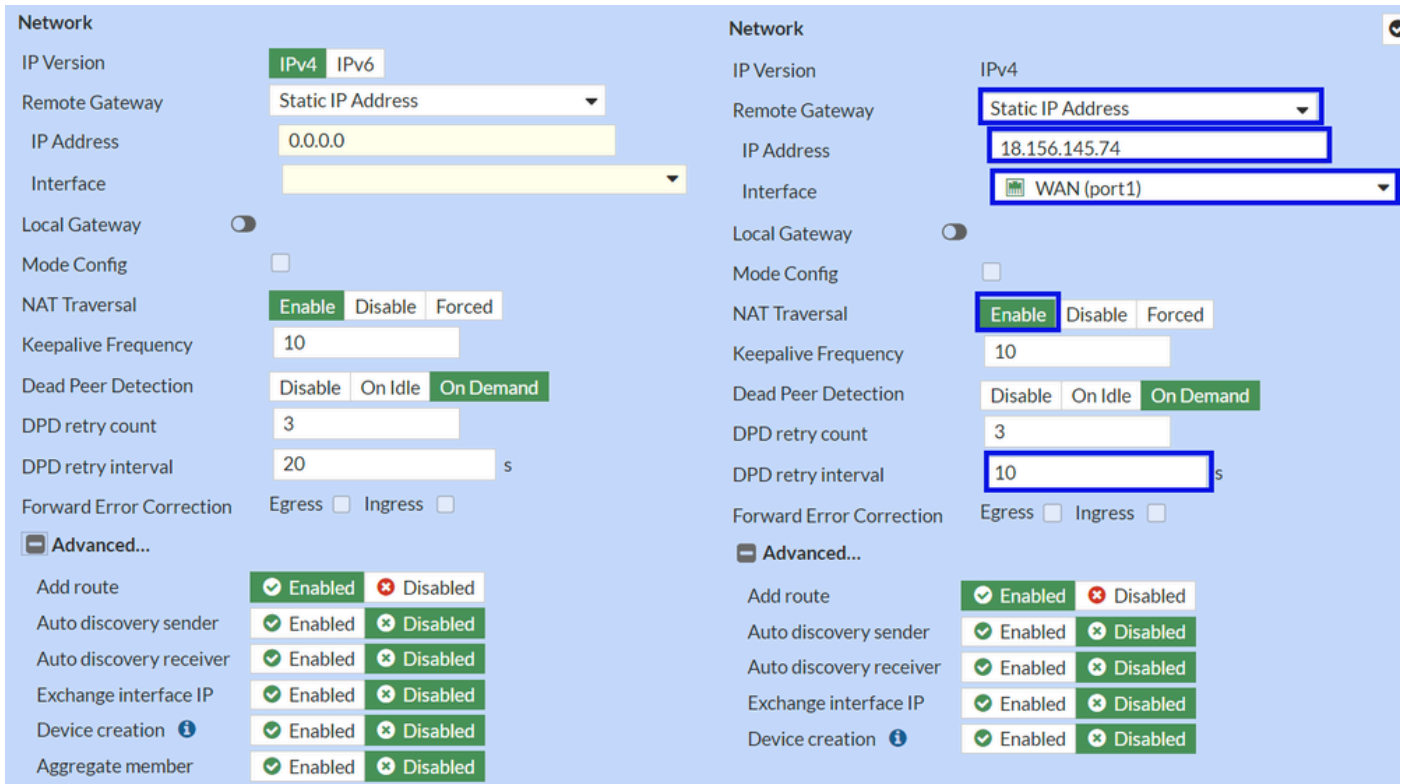


- Haga clic en Custom , configure a **Name** y haga clic en **Next**.



En la siguiente imagen, verá cómo debe configurar los ajustes del **Network** artículo.

Red



- Network

- IP Version :IPv4

- **Remote Gateway** :Dirección IP estática
- **IP Address**: Utilice la dirección IP de Primary IP Datacenter IP Address,dada en el paso [Tunnel Data](#)
- **Interface** : elija la interfaz WAN que tiene previsto utilizar para establecer el túnel
- **Local Gateway** : Desactivar como valor predeterminado
- **Mode Config** : Desactivar como valor predeterminado
- **NAT Traversal** :Habilitar
- **Keepalive Frequency** :10
- **Dead Peer Detection** : a demanda
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : no active ninguna casilla.
- **Advanced...:** configúrelo como la imagen.

Ahora configure el IKE **Authentication**.

Autenticación

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)		

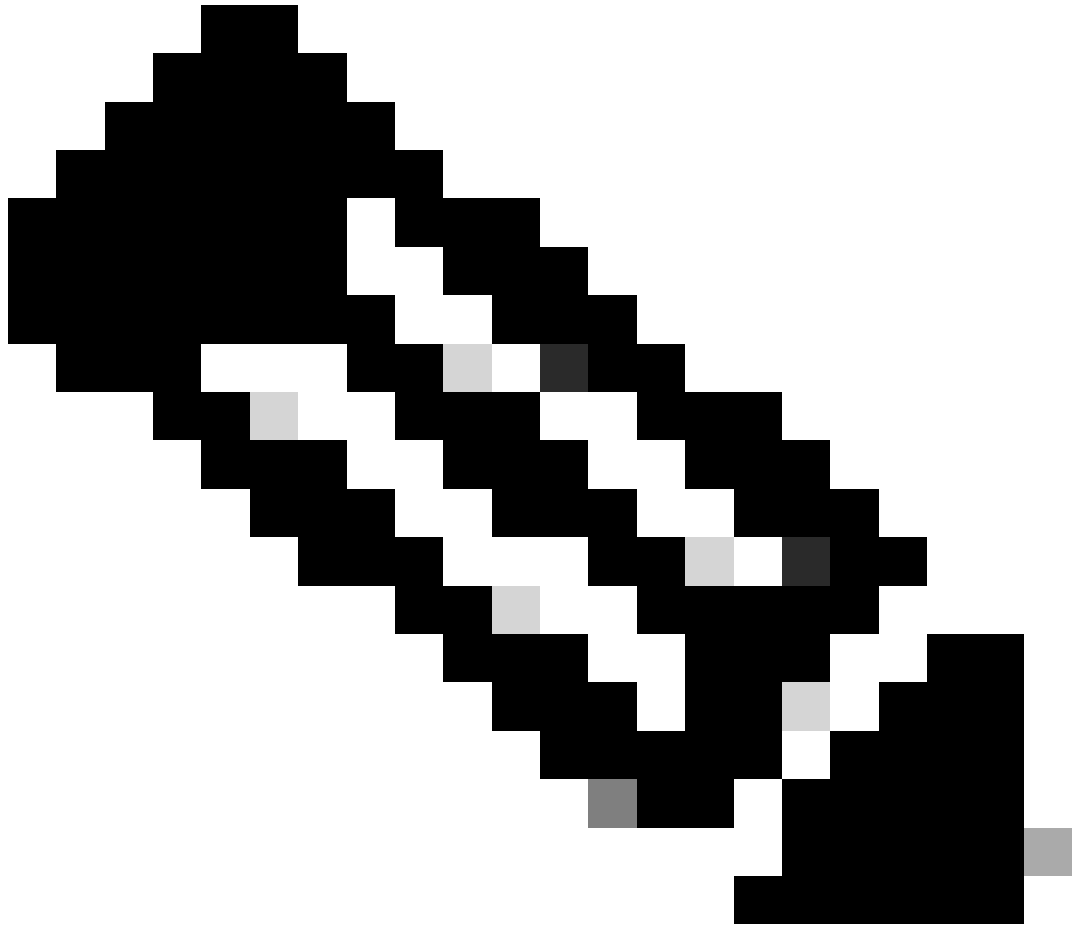
- **Authentication**

- **Method** : Pre-Shared Key (Clave precompartida) como valor predeterminado

- **Pre-shared Key** : Utilice el **Passphrase** dado en el paso [Tunnel Data](#)

- **IKE**

- **Version** : Elija la versión 2.



Nota: Secure Access sólo admite IKEv2

Ahora configure el **Phase 1 Proposal**.

Fase 1 Propuesta

The image shows two instances of the 'Phase 1 Proposal' configuration interface. The left instance shows a list of four proposals with encryption and authentication settings. The right instance shows a detailed view of a proposal with the following settings:

- Encryption: AES256
- Authentication: SHA256
- Diffie-Hellman Groups: 19 and 20 (checked)
- Key Lifetime (seconds): 86400
- Local ID: fortigate@8195126-621099508-sse.ci

- Phase 1 Proposal

- Encryption : Elija AES256

- Authentication : Elija SHA256

- Diffie-Hellman Groups : Marque las casillas 19 y 20

- Key Lifetime (seconds) : 86400 como valor predeterminado

- Local ID : Utilice el Primary Tunnel ID, indicado en el paso [Tunnel Data](#)

Ahora configure el **Phase 2 Proposal**.

Fase 2 Propuesta

The image shows two screenshots of a configuration interface for a VPN Phase 2 proposal. The left screenshot shows the 'Advanced...' options, and the right screenshot shows the main configuration fields.

Left Screenshot (Advanced...):

- Phase 2 Proposal:** Add
- Encryption:** AES128, AES256, AES128, AES256, AES128GCM, AES256GCM, CHACHA20POLY1305
- Authentication:** SHA1, SHA1, SHA256, SHA256
- Enable Replay Detection:**
- Enable Perfect Forward Secrecy (PFS):**
- Diffie-Hellman Group:** 14, 5
- Local Port:** All
- Remote Port:** All
- Protocol:** All
- Auto-negotiate:**
- Autokey Keep Alive:**
- Key Lifetime:** Seconds, 43200

Right Screenshot (New Phase 2):

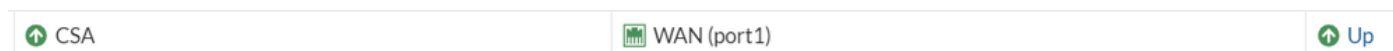
- Name:** CSA
- Comments:** Comments
- Local Address:** addr_subnet, 0.0.0.0/0.0.0.0
- Remote Address:** addr_subnet, 0.0.0.0/0.0.0.0
- Advanced...:**
 - Phase 2 Proposal:** Add
 - Encryption:** AES128
 - Authentication:** SHA256
 - Enable Replay Detection:**
 - Enable Perfect Forward Secrecy (PFS):**
 - Local Port:** All
 - Remote Port:** All
 - Protocol:** All
 - Auto-negotiate:**
 - Autokey Keep Alive:**
 - Key Lifetime:** Seconds, 43200

- New Phase 2
 - **Name** : Dejar como predeterminado (Esto se toma del nombre de su VPN)
 - **Local Address** : Dejar como predeterminado (0.0.0.0/0.0.0.0)
 - **Remote Address** : Dejar como predeterminado (0.0.0.0/0.0.0.0)

- Advanced
 - **Encryption** : Elija AES128
 - **Authentication** : Elija SHA256
 - **Enable Replay Detection** : activada de forma predeterminada (Activado)
 - **Enable Perfect Forward Secrecy (PFS)** : desactive la casilla de verificación
 - **Local Port** : activada de forma predeterminada (Activado)

- **Remote Port**: activada de forma predeterminada (Activado)
- **Protocol** : activada de forma predeterminada (Activado)
- **Auto-negotiate** : dejar como predeterminado (sin marcar)
- **Autokey Keep Alive** : dejar como predeterminado (sin marcar)
- **Key Lifetime** : Dejado como predeterminado (segundos)
- **Seconds** : Dejar como predeterminado (43200)

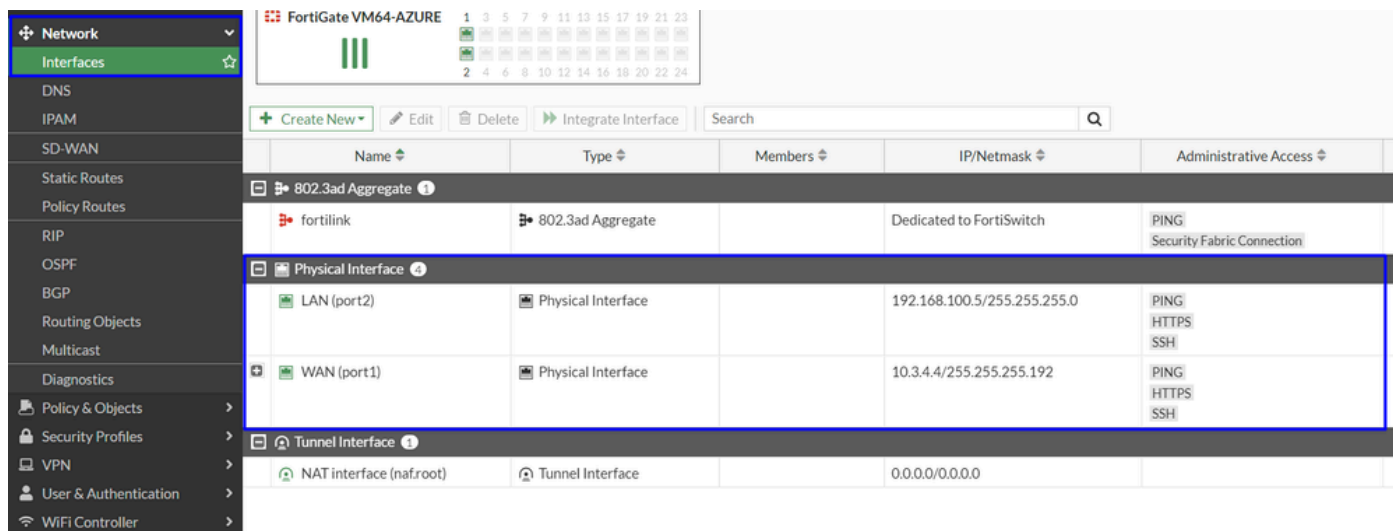
A continuación, haga clic en Aceptar. Después de unos minutos verá que la VPN se estableció con Secure Access, y puede continuar con el siguiente paso, **Configure the Tunnel Interface**.



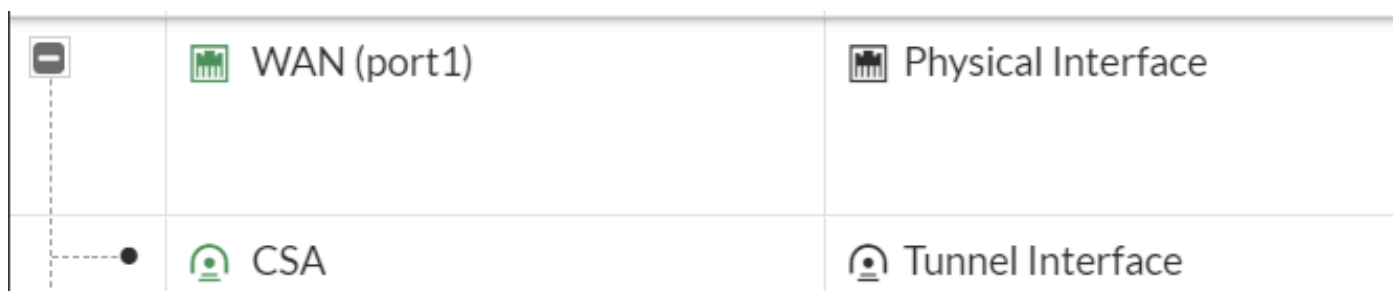
Configuración de la interfaz de túnel

Una vez creado el túnel, se percata de que hay una nueva interfaz detrás del puerto que se utiliza como interfaz WAN para comunicarse con Secure Access.

Para comprobarlo, navegue hasta **Network > Interfaces**.



Amplie el puerto que utiliza para comunicarse con Secure Access; en este caso, la **WAN** interfaz.



- Haga clic en el **Tunnel Interface** y en **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

- Tiene la siguiente imagen que necesita 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 una IP no enrutable que no tenga en su red (169.254.0.1)
- Remote IP/Netmask : configure la IP remota como la siguiente IP de su interfaz IP y con una máscara de red de 30 (169.254.0.255.255.255.252)

A continuación, haga clic **OK** para guardar la configuración y continúe con el siguiente paso Configure Policy Route (Routing basado en el origen).

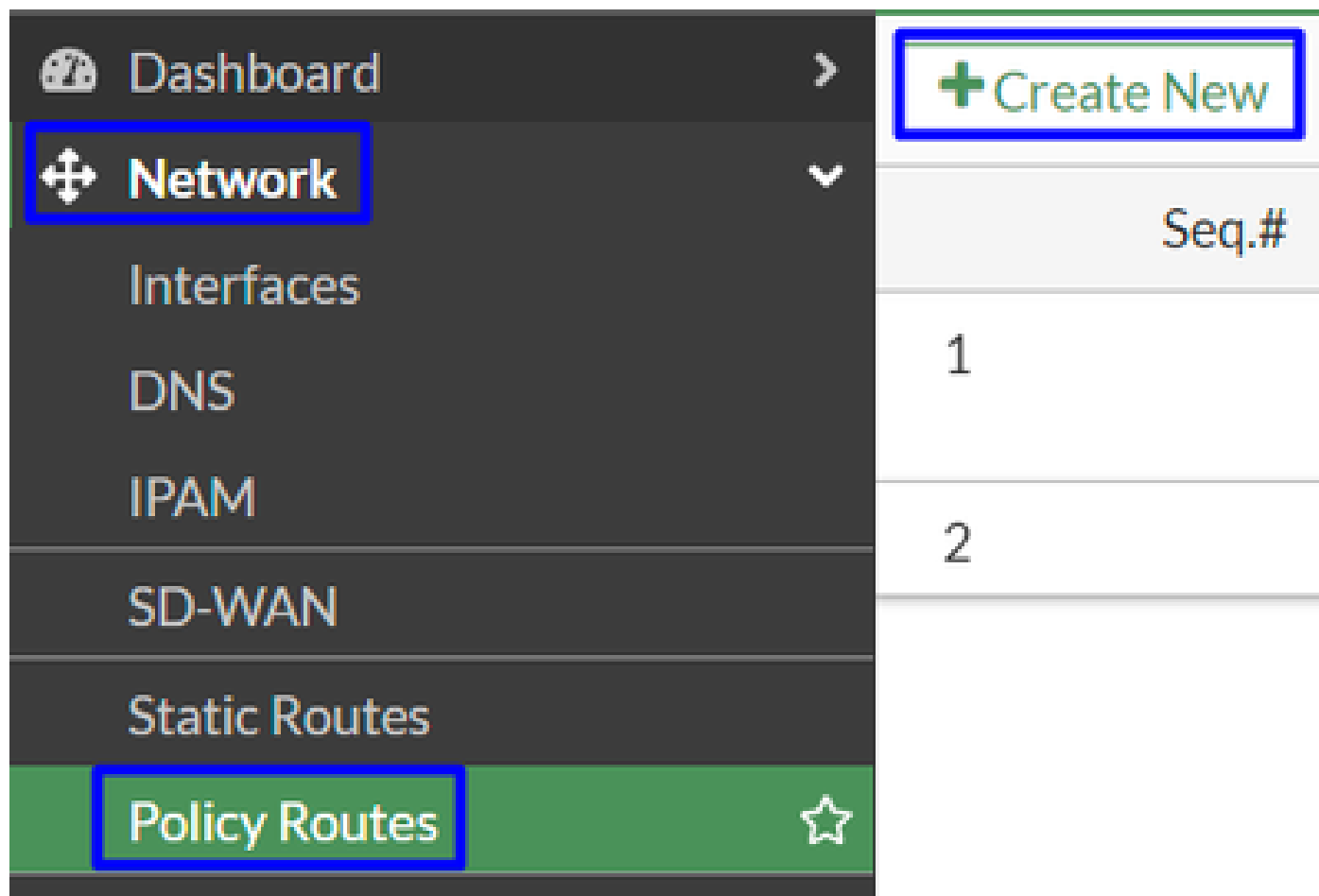


Advertencia: Después de esta parte, debe configurar las políticas de firewall en su FortiGate para permitir o permitir el tráfico desde su dispositivo a Secure Access y desde Secure Access a las redes que desea rutear el tráfico.

Configurar ruta de política

En este momento, tiene su VPN configurada y establecida para Secure Access; ahora, debe volver a enrutar el tráfico a Secure Access para proteger su tráfico o el acceso a sus aplicaciones privadas detrás de su firewall FortiGate.

- Desplácese hasta 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, a table is visible with a header 'Seq.#' and two rows containing the numbers '1' and '2'. Above the table, a green button with a plus sign and the text '+ Create New' is highlighted with a blue box.

- Configurar la directiva

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 : elija la interfaz desde la que planea redirigir el tráfico a Secure Access (Origen del tráfico)

- Source Address
 - IP/Netmask : utilice esta opción si sólo enruta una subred de una interfaz
 - Addresses : utilice esta opción si ha creado el objeto y el origen del tráfico proviene de varias interfaces y varias subredes

- Destination Addresses
 - Addresses: Elegir all

- Protocol: Elegir **ANY**

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

 - Outgoing Interface : Seleccione la interfaz de túnel que ha modificado en el paso [Configurar interfaz de túnel](#)
 - Gateway Address: Configure la IP remota configurada en el paso [RemoteIPNetmask](#)
 - Status : Seleccione Activado

Haga clic **OK** para guardar la configuración; ahora está listo para comprobar si el tráfico de los dispositivos se ha redirigido a Secure Access.

Verificación

Para verificar si el tráfico de su máquina fue re-enrutado a Secure Access, tiene dos opciones; puede verificar en Internet y verificar su IP pública, o puede ejecutar el siguiente comando con curl:

<#root>

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

El rango público desde donde puede ver su tráfico es desde:

Min Host:151.186.176.1

Max Host :151.186.207.254



Nota: Estas direcciones IP están sujetas a cambios, lo que significa que es probable que Cisco amplíe este alcance en el futuro.

Si ve el cambio de su IP pública, significa que está siendo protegido por Secure Access, y ahora puede configurar su aplicación privada en el panel Secure Access para acceder a sus aplicaciones desde VPNaaS o ZTNA.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).