

# Configureer beveiligde toegang met Fortigate Firewall

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[VPN bij beveiligde toegang configureren](#)

[Tunnelgegevens](#)

[Configureer de VPN Site naar Site op Fortigate](#)

[Netwerk](#)

[Verificatie](#)

[Voorstel voor fase 1](#)

[Voorstel voor fase 2](#)

[De tunnelinterface configureren](#)

[Configureren van beleidsroute](#)

[Verifiëren](#)

---

## Inleiding

Dit document beschrijft hoe u Secure Access kunt configureren met Fortigate Firewall.

## Voorwaarden

- [Gebruikersprovisioning configureren](#)
- [Configuratie ZTNA SSO-verificatie](#)
- [Beveiligde toegang tot VPN configureren](#)

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Fortigate 7.4.x versie firewall
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA
- Clientloze ZTNA

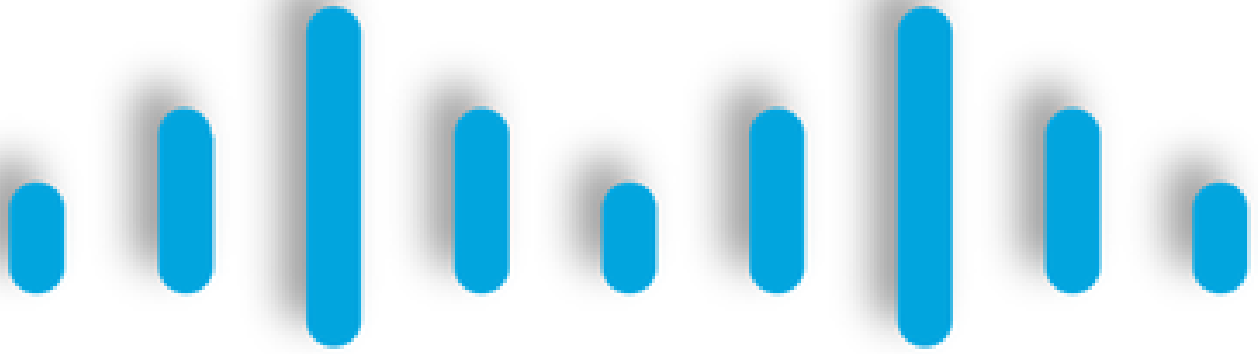
## Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Fortigate 7.4.x versie firewall
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie



# CISCO

## Secure

## Access

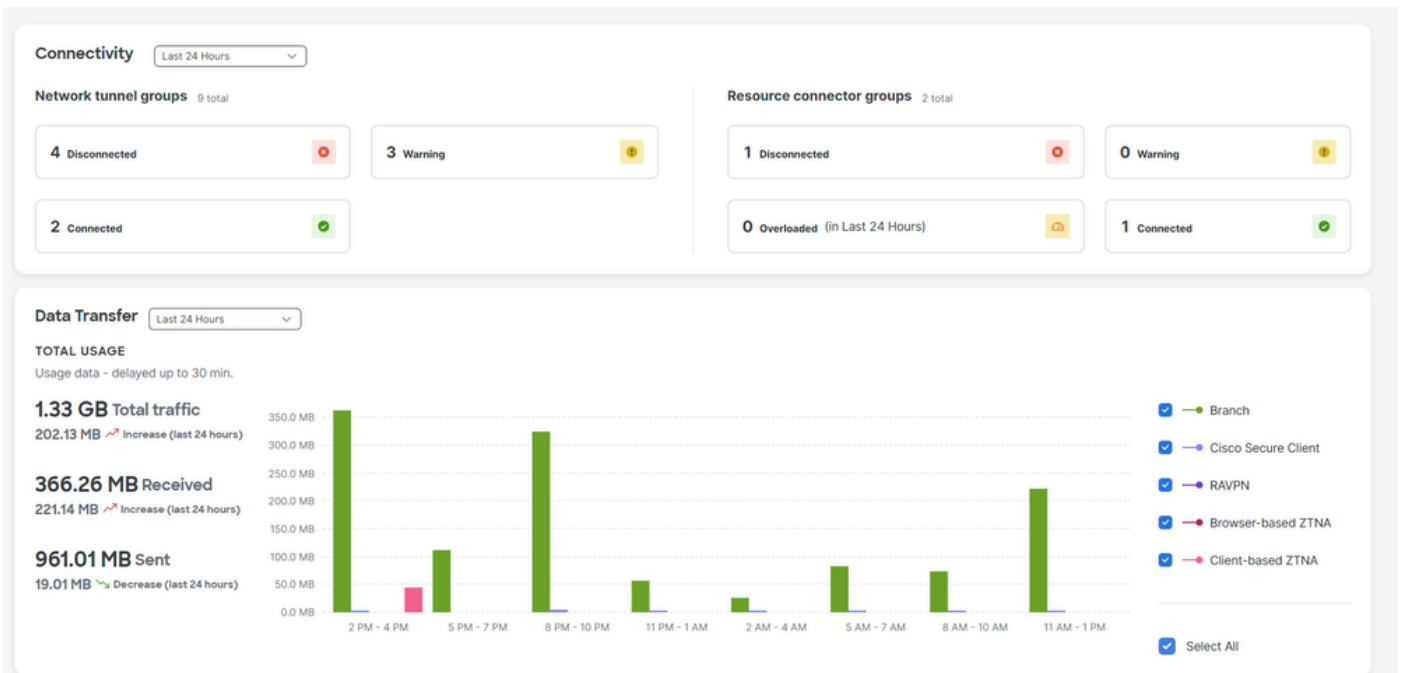
# FORTINET®

Cisco heeft Secure Access ontworpen om toegang tot particuliere toepassingen te beschermen en te bieden, zowel op locatie als in de cloud. Het beschermt ook de verbinding van het netwerk met het internet. Dit wordt bereikt door de implementatie van meerdere beveiligingsmethoden en -lagen, die allemaal gericht zijn op het bewaren van de informatie zoals ze deze via de cloud benaderen.

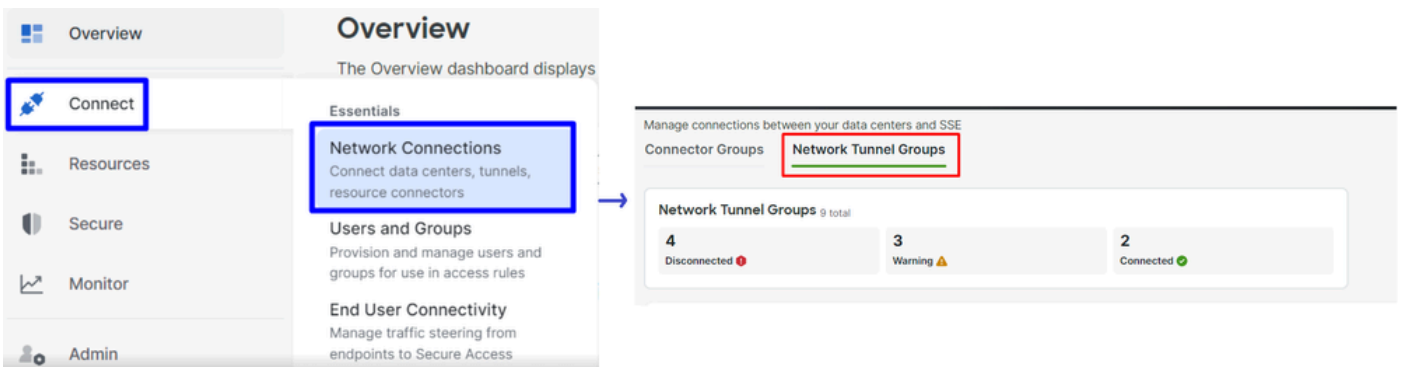
Configureren

# VPN bij beveiligde toegang configureren

Navigeer naar het beheerderspaneel van [Secure Access](#).



- Klik op **Connect > Network Connections > Network Tunnels Groups**



- Onder Network Tunnel Groups klik op + 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



- Configureren Tunnel Group Name, Regionen Device Type
- Klik op de knop **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



**Opmerking:** kies de regio die het dichtst bij de locatie van uw firewall ligt.

- 
- Configureer de Tunnel ID Format en Passphrase
  - Klik op de knop Next

- ✓ 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

- Configureer de IP-adresbereiken of hosts die u op uw netwerk hebt geconfigureerd en u wilt het verkeer via beveiligde toegang doorgeven
- Klik op de knop **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

Nadat u op **Save** de informatie over de tunnel wordt weergegeven, bewaar die informatie voor de volgende stap, **Configure the VPN Site to Site on Fortigate**.

Tunnelgegevens

## 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.

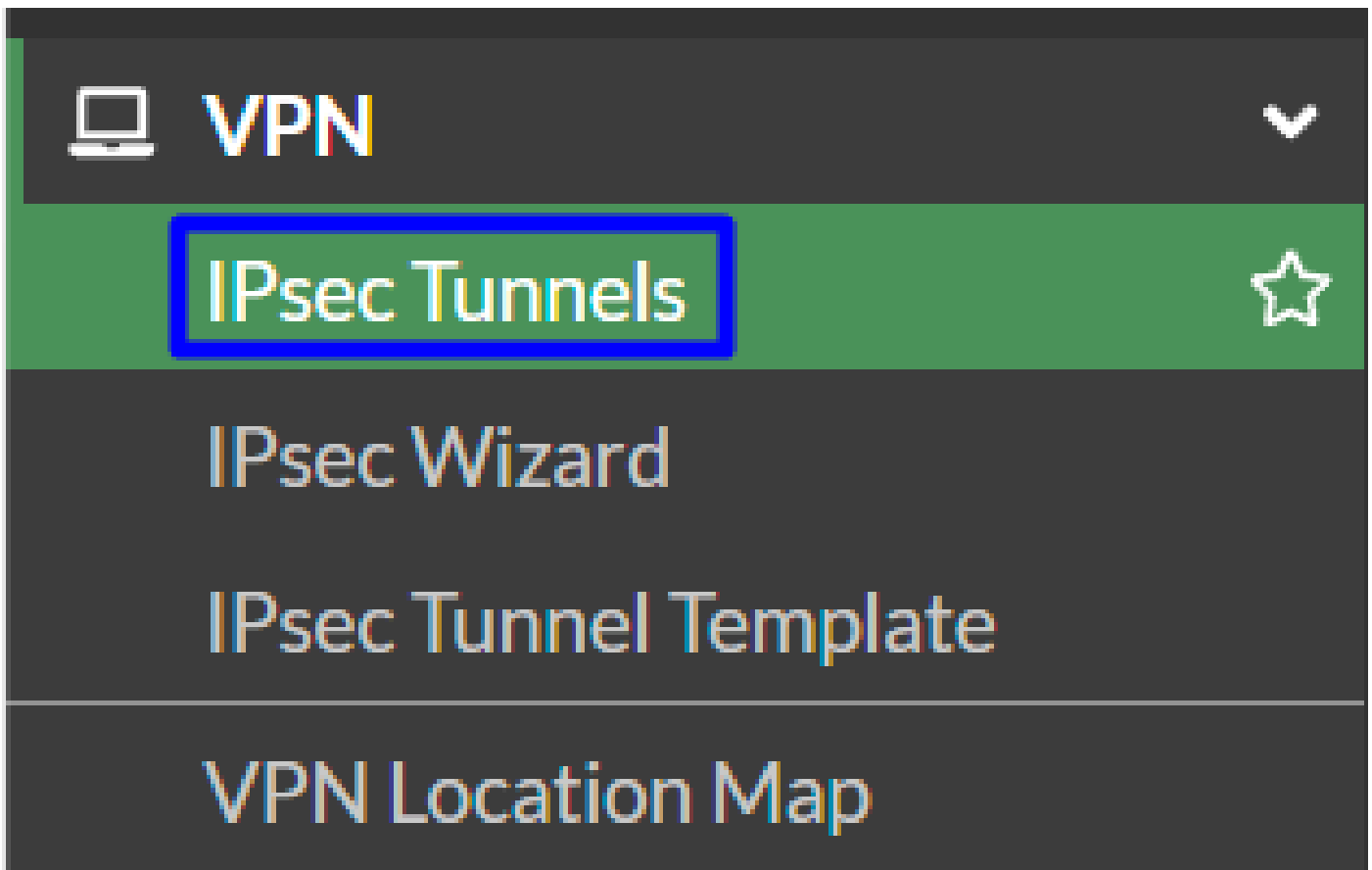
<b>Primary Tunnel ID:</b>	@	-sse.cisco.com	
<b>Primary Data Center IP Address:</b>	18.156.145.74		
<b>Secondary Tunnel ID:</b>	@	-sse.cisco.com	
<b>Secondary Data Center IP Address:</b>	3.120.45.23		
<b>Passphrase:</b>	CP		

Configureer de VPN Site naar Site op Fortigate

Navigeer naar je Fortigate dashboard.

- Klik op de knop VPN > IPsec Tunnels





- Klik op de knop Create New > IPsec Tunnels

+ Create new ▾

IPsec Tunnel

IPsec Aggregate

Custom 2

- Klik op Custom , configureer een bestand **Name** en klik **Next**.

#### 1 VPN Setup

Name 2 Cisco Secure

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

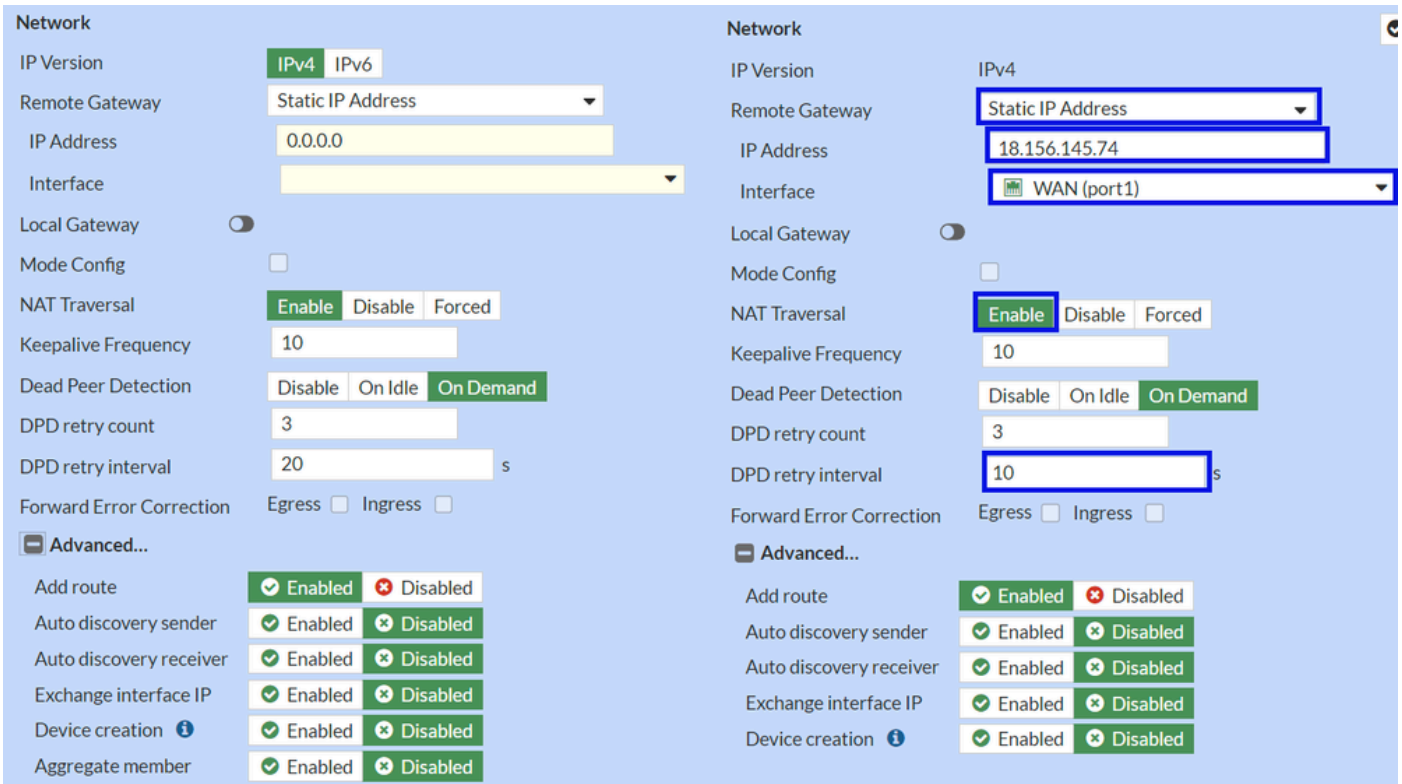
< Back

Next > 3

Cancel

In de volgende afbeelding ziet u hoe u de instellingen voor het **Network** onderdeel moet configureren.

Network



- Network

- IP Version :IPv4

- **Remote Gateway** :Statisch IP-adres
- **IP Address**: Gebruik het IP-adres van de Primary IP Datacenter IP Address,gegevens in de stap [Tunnel](#)
- **Interface** : Kies de WAN-interface die u wilt gebruiken om de tunnel te openen
- **Local Gateway** : Uitschakelen als standaard
- **Mode Config** : Uitschakelen als standaard
- **NAT Traversal** :Inschakelen
- **Keepalive Frequency** :10
- **Dead Peer Detection** : on-demand
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : Vink geen vakje aan.
- **Advanced...:** Configureer het als de afbeelding.

Configureer nu de IKE **Authentication**.

Verificatie

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

- **Authentication**

- **Method** : Vooraf gedeelde sleutel als standaard

- **Pre-shared Key** : Gebruik de **Passphrase**gegeven in de stap [Tunnelgegevens](#)

- **IKE**

- **Version** : Kies versie 2.



**Opmerking:** Secure Access ondersteunt alleen IKEv2

---

Configureer nu de **Phase 1 Proposal**instellingen.

Voorstel voor fase 1

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 to SHA256, and Diffie-Hellman Groups 19 and 20 selected. The key lifetime is set to 86400 seconds and the local ID is fortigate@8195126-621099508-sse.ci.

- Phase 1 Proposal

- Encryption : Kies AES256

- Authentication : Kies SHA256

- Diffie-Hellman Groups : Vak 19 en 20 aanvinken

- Key Lifetime (seconds) : standaard 86400

- Local ID : Gebruik het Primary Tunnel ID formulier dat is aangegeven in de stap [Tunnelgegevens](#)

Configureer nu de **Phase 2 Proposal**instellingen.

Voorstel voor fase 2

The image shows two views of the 'New Phase 2' configuration interface. The left view shows the 'Advanced...' options, and the right view shows the 'New Phase 2' summary with several fields highlighted in blue boxes.

**Left Panel (Advanced...):**

- 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
- Phase 2 Proposal: Add
- Encryption options: AES128, AES256, AES128GCM, AES256GCM, CHACHA20POLY1305
- Authentication options: SHA1, 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

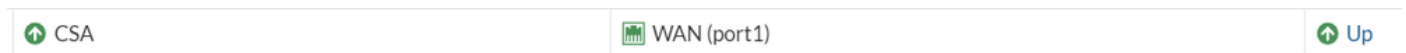
**Right Panel (New Phase 2):**

- 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
- 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** : Laat staan als standaard (dit is afkomstig van de naam van uw VPN)
  - **Local Address** : Laat als standaard (0.0.0.0/0.0.0.0)
  - **Remote Address** : Laat als standaard (0.0.0.0/0.0.0.0)
  
- Advanced
  - **Encryption** : Kies AES128
  - **Authentication** : Kies SHA256
  - **Enable Replay Detection** : Laat als standaard (ingeschakeld)
  - **Enable Perfect Forward Secrecy (PFS)** : Schakel het selectievakje uit
  - **Local Port** : Laat als standaard (ingeschakeld)

- **Remote Port:** Laat als standaard (ingeschakeld)
- **Protocol :** Laat als standaard (ingeschakeld)
- **Auto-negotiate :** Standaard ingeschakeld (niet gemarkeerd)
- **Autokey Keep Alive :** Standaard ingeschakeld (niet gemarkeerd)
- **Key Lifetime :** Standaard ingeschakeld (seconden)
- **Seconds :** Standaard ingeschakeld (43200)

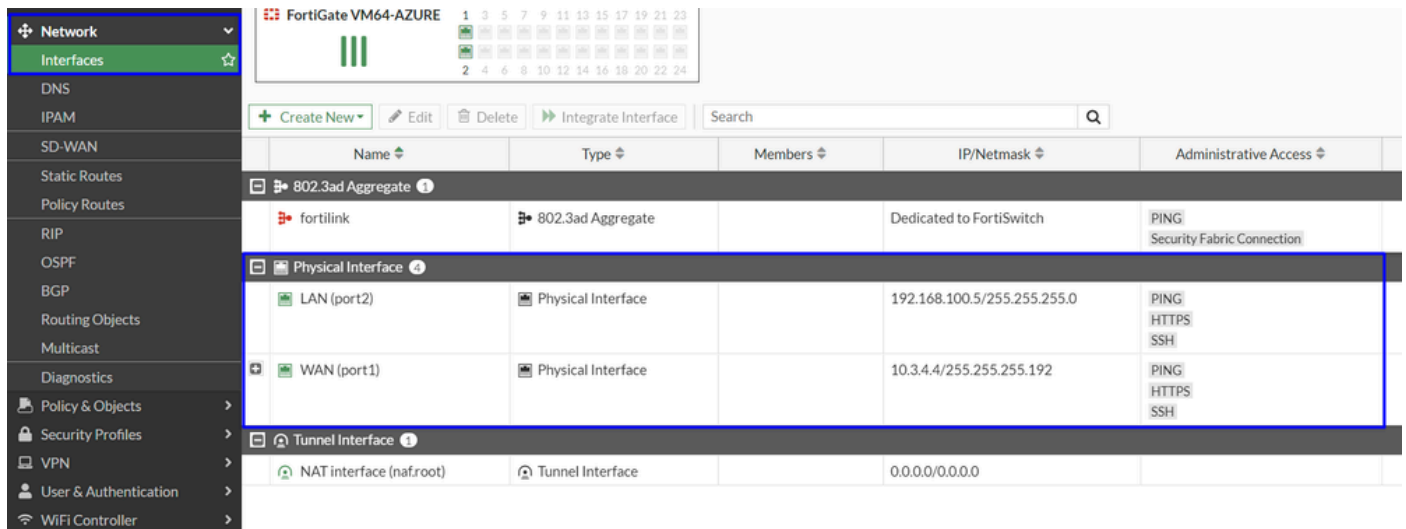
Klik vervolgens op OK. U ziet na enkele minuten dat de VPN is opgezet met Secure Access, en u kunt doorgaan met de volgende stap, **Configure the Tunnel Interface**.



De tunnelinterface configureren

Nadat de tunnel is gemaakt, ziet u dat u een nieuwe interface achter de poort hebt die u als WAN-interface gebruikt om met Secure Access te communiceren.

Om dat te controleren, navigeer dan naar **Network > Interfaces**.



Breed de poort uit die u gebruikt om te communiceren met Secure Access; in dit geval de **WAN** interface.





- Klik op uw **Tunnel Interface** en klik op **Edit**

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

- U hebt het volgende beeld dat u moet configureren

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 : Configureer een niet-routeerbare IP die niet in uw netwerk aanwezig is (169.254.0.1)
- Remote IP/Netmask : Configureer de externe IP als de volgende IP van uw interface-IP en met een Netmasker van 30 (169.254.0.255.255.255.252)

Daarna, klik om de configuratie op **OK** te slaan en met de volgende stap te werk te gaan, Configure Policy Route (op oorsprong gebaseerde routing).

---



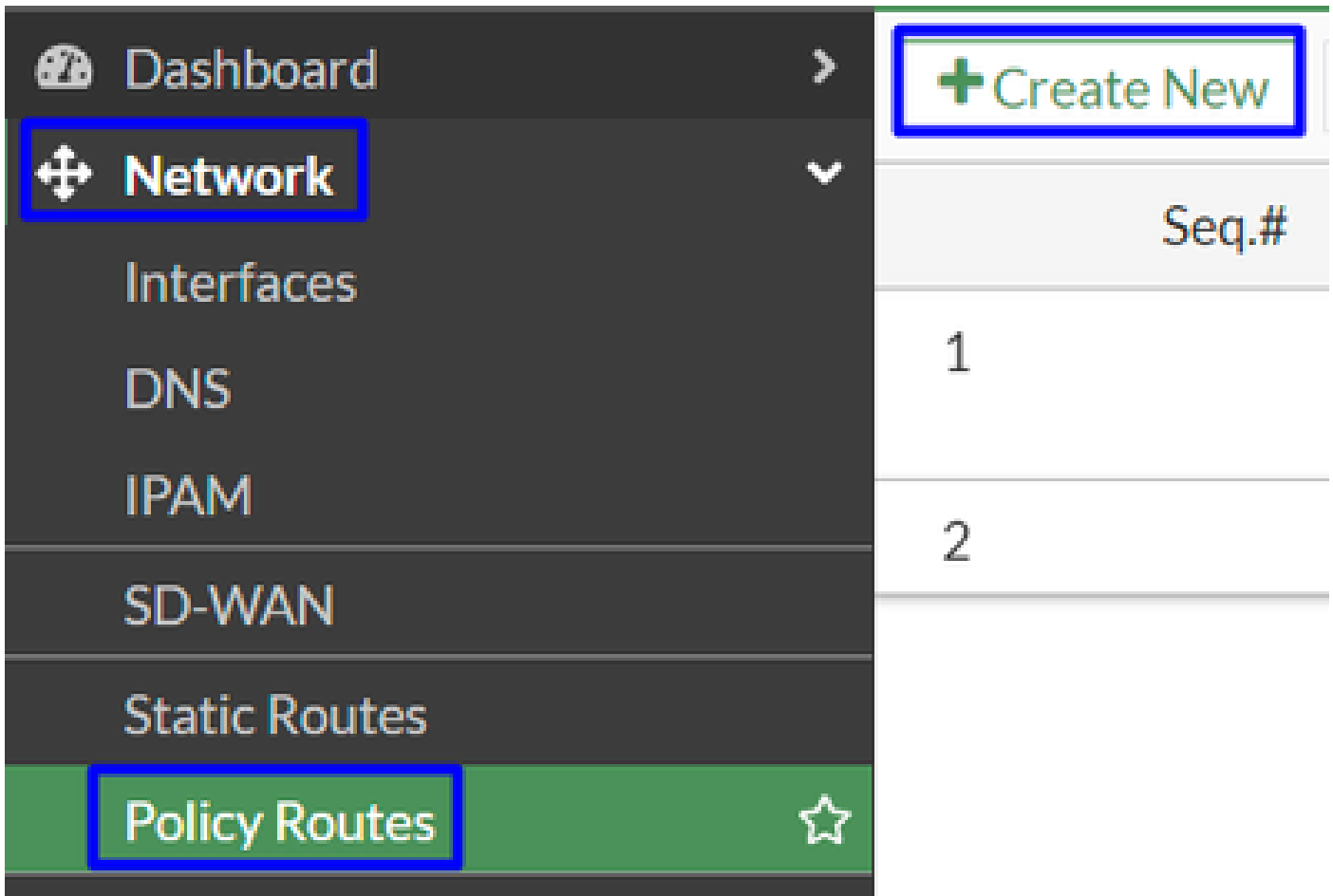
**Waarschuwing:** na dit onderdeel moet u het firewallbeleid op uw FormFiller configureren om verkeer vanaf uw apparaat toe te staan of toe te staan voor beveiligde toegang en van beveiligde toegang tot de netwerken die u wilt leiden.

---

## Configureren van beleidsroute

Op dit punt hebt u uw VPN geconfigureerd en ingesteld om Secure Access te beveiligen; nu moet u het verkeer omleiden naar Secure Access om uw verkeer of toegang tot uw privé-toepassingen achter uw FortiGate firewall te beschermen.

- Naar navigeren 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 green background). On the right, there is a table with a header row containing a '+ Create New' button (highlighted with a blue box) and a 'Seq.#' column. The table contains two rows with sequence numbers 1 and 2.

Seq.#
1
2

- Het beleid configureren

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" value=""/>	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" value=""/>	IP/Netmask <input type="text" value=""/>
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" value=""/>	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 : Kies de interface van waar u het verkeer wilt omleiden naar beveiligde toegang (herkomst van verkeer)
  
- Source Address
  - IP/Netmask : Gebruik deze optie als u alleen een subnetverbinding van een interface routeert
  - Addresses : Gebruik deze optie als u het object hebt gemaakt en de bron van het verkeer afkomstig is van meerdere interfaces en meerdere subnetten
  
- Destination Addresses

- Addresses: Kies all
  
- Protocol: Kies **ANY**
  
  
- Then
  
  
- Action: **Choose Forward Traffic**
  
  
  
- Outgoing Interface : Kies de tunnelinterface die u in de stap hebt aangepast, [Tunnelinterface configureren](#)
- Gateway Address: De configuratie van de externe IP op de stap, [RemoteIPNetmask](#)
- Status : Ingeschakeld kiezen

Klik om de configuratie op **OK** te slaan, u bent nu klaar om te verifiëren of uw apparaatverkeer is omgeleid naar Secure Access.

Verifiëren

Om te controleren of het verkeer van uw machine is omgeleid naar Secure Access, hebt u twee opties; u kunt controleren op het internet en controleren op uw openbare IP, of u kunt de volgende opdracht uitvoeren met krul:

<#root>

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

De openbare waaier van waar u uw verkeer kunt zien is van:

Min Host:151.186.176.1

Max Host :151.186.207.254



**Opmerking:** deze IP's kunnen worden gewijzigd, wat betekent dat Cisco dit bereik in de toekomst waarschijnlijk zal uitbreiden.

---

Als u de wijziging van uw openbare IP ziet, betekent dit dat u wordt beschermd door Secure Access, en nu kunt u uw privé-toepassing configureren op het Secure Access-dashboard om toegang te krijgen tot uw toepassingen via VPNaaS of ZTNA.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.