

Configurer un accès sécurisé avec Fortigate Firewall

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurer le VPN sur un accès sécurisé](#)

[Données du tunnel](#)

[Configurer le site VPN sur le site Fortigate](#)

[Réseau](#)

[Authentification](#)

[Proposition de phase 1](#)

[Proposition de phase 2](#)

[Configuration de l'interface du tunnel](#)

[Configurer le routage de stratégie](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer l'accès sécurisé avec Fortigate Firewall.

Conditions préalables

- [Configurer le provisionnement utilisateur](#)
- [Configuration de l'authentification ZTNA SSO](#)
- [Configuration de l'accès sécurisé VPN à distance](#)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu version Fortigate 7.4.x
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- ZTNA sans client

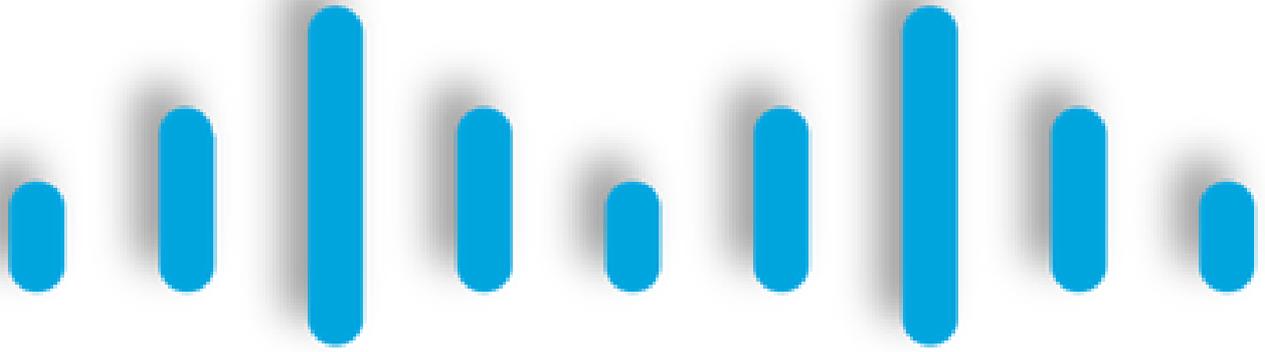
Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Pare-feu version Fortigate 7.4.x
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales



CISCO

Secure

Access

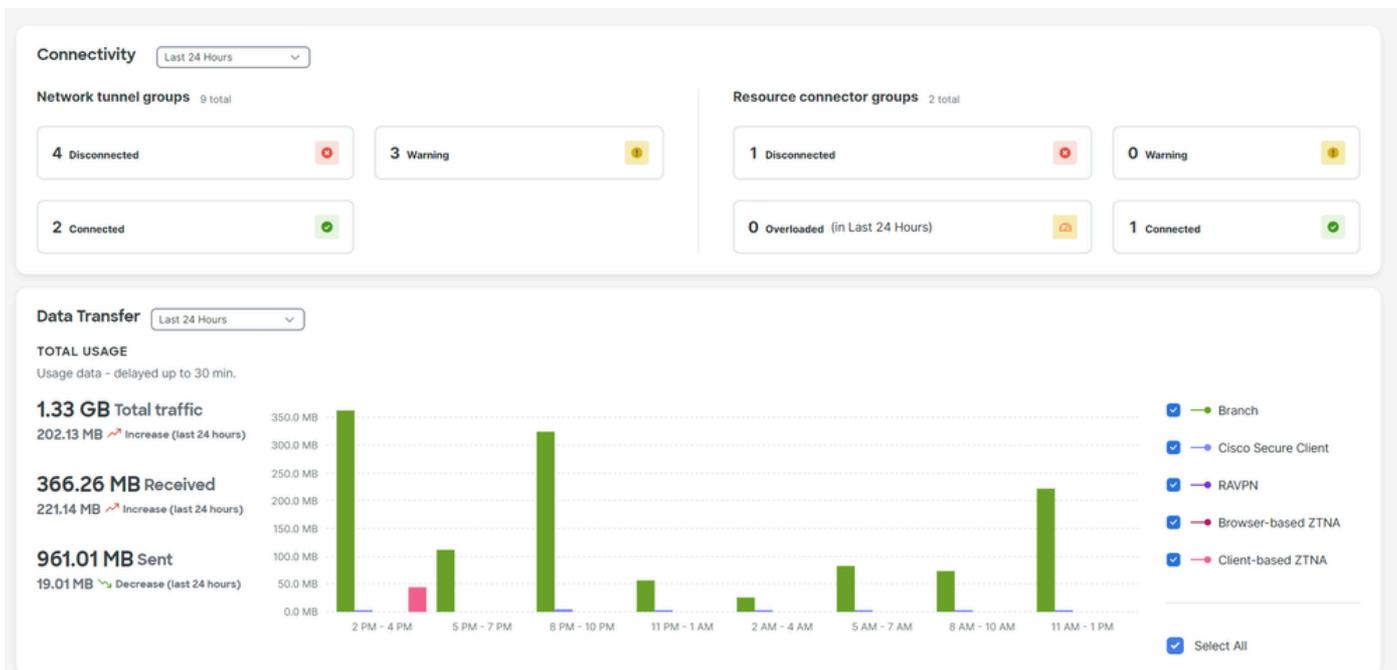
FORTINET®

Cisco a conçu Secure Access pour protéger et fournir un accès aux applications privées, sur site et dans le cloud. Il protège également la connexion du réseau à Internet. Pour ce faire, plusieurs méthodes et couches de sécurité sont mises en oeuvre, toutes visant à préserver les informations lorsqu'elles y accèdent via le cloud.

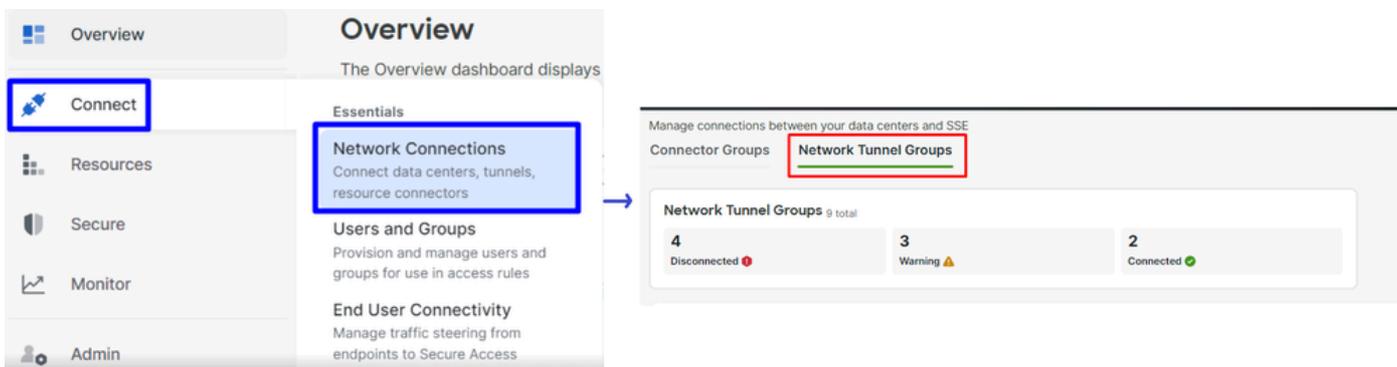
[Configurer](#)

Configurer le VPN sur un accès sécurisé

Accédez au panneau d'administration de [Secure Access](#).



- Cliquez sur **Connect > Network Connections > Network Tunnels Groups**



- Sous **Network Tunnel Groups** cliquez sur **+ 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](#)

Q Search Region Status 9 Tunnel Groups



- Configurer Tunnel Group Name, Region et Device Type
- Cliquer **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



Remarque : choisissez la région la plus proche de l'emplacement de votre pare-feu.

-
- Configurez les Tunnel ID Format et Passphrase
 - CliquerNext

- ✓ 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

- Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez faire passer le trafic par un accès sécurisé
- Cliquer **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

Après avoir cliqué sur **Save** les informations sur le tunnel s'affiche, veuillez enregistrer ces informations pour l'étape suivante, **Configure the VPN Site to Site on Fortigate**.

Données du tunnel

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		

Configurer le site VPN sur le site Fortigate

Accédez à votre tableau de bord Fortigate.

- Cliquer VPN > IPsec Tunnels



VPN



IPsec Tunnels

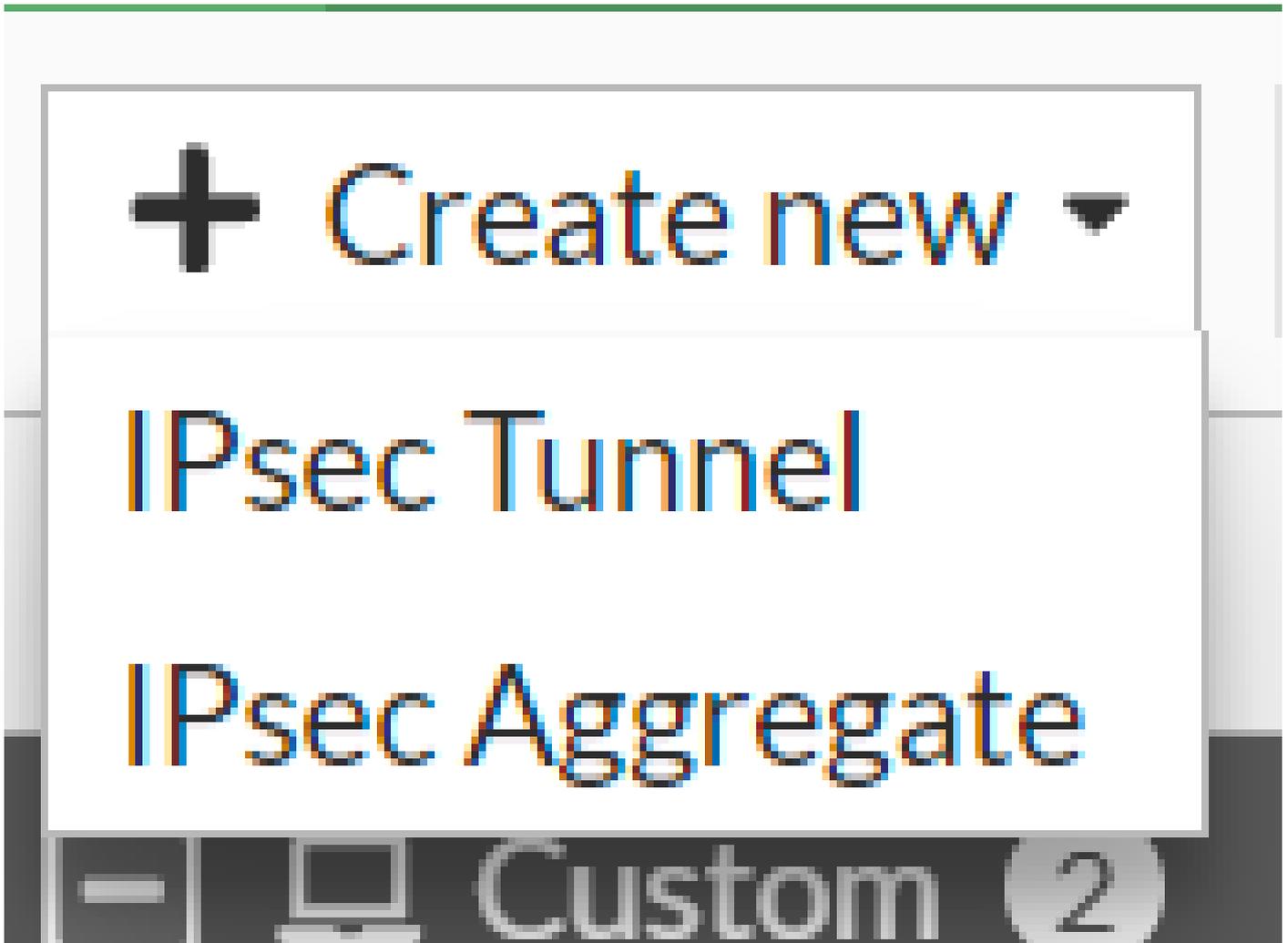


IPsec Wizard

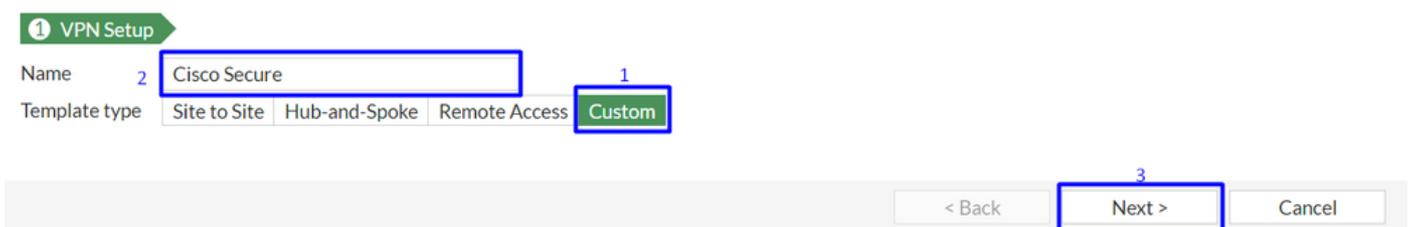
IPsec Tunnel Template

VPN Location Map

- Cliquer Create New > IPsec Tunnels

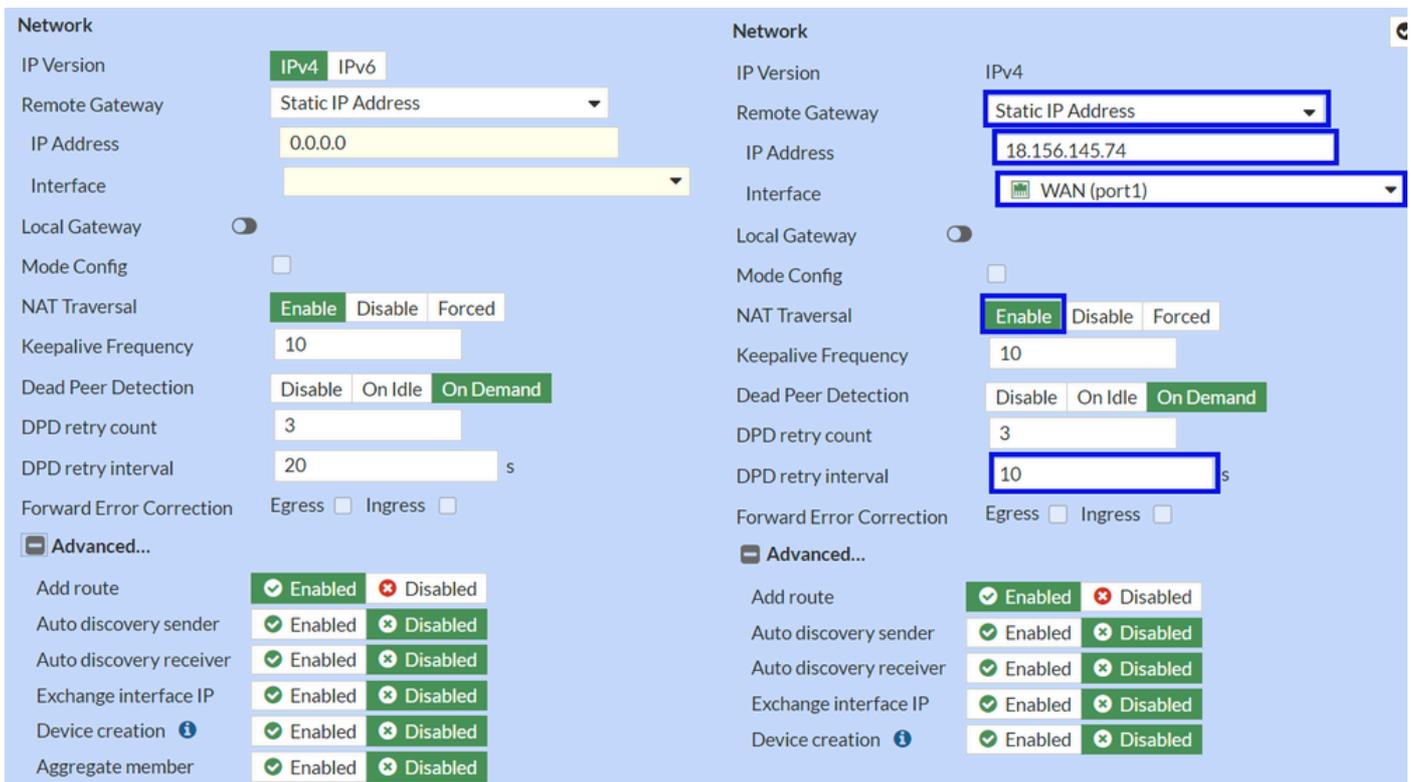


- Cliquez sur Custom , configurez un **Name** et cliquez sur **Next**.



Dans l'image suivante, vous voyez comment vous devez configurer les paramètres de la **Network** pièce.

Réseau



- Network

- IP Version :IPv4

- **Remote Gateway** :Adresse IP statique
- **IP Address**: Utilisez l'IP de Primary IP Datacenter IP Address,donnée dans l'étape [Données de tunnel](#)
- **Interface** : choisissez l'interface WAN que vous avez prévu d'utiliser pour établir le tunnel
- **Local Gateway** : Désactiver par défaut
- **Mode Config** : Désactiver par défaut
- **NAT Traversal** :activer
- **Keepalive Frequency** :10
- **Dead Peer Detection** : à la demande
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : ne cochez aucune case.
- **Advanced...:** configurez-la en tant qu'image.

Configurez maintenant le **Authentication** routeur IKE.

Authentification

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)		

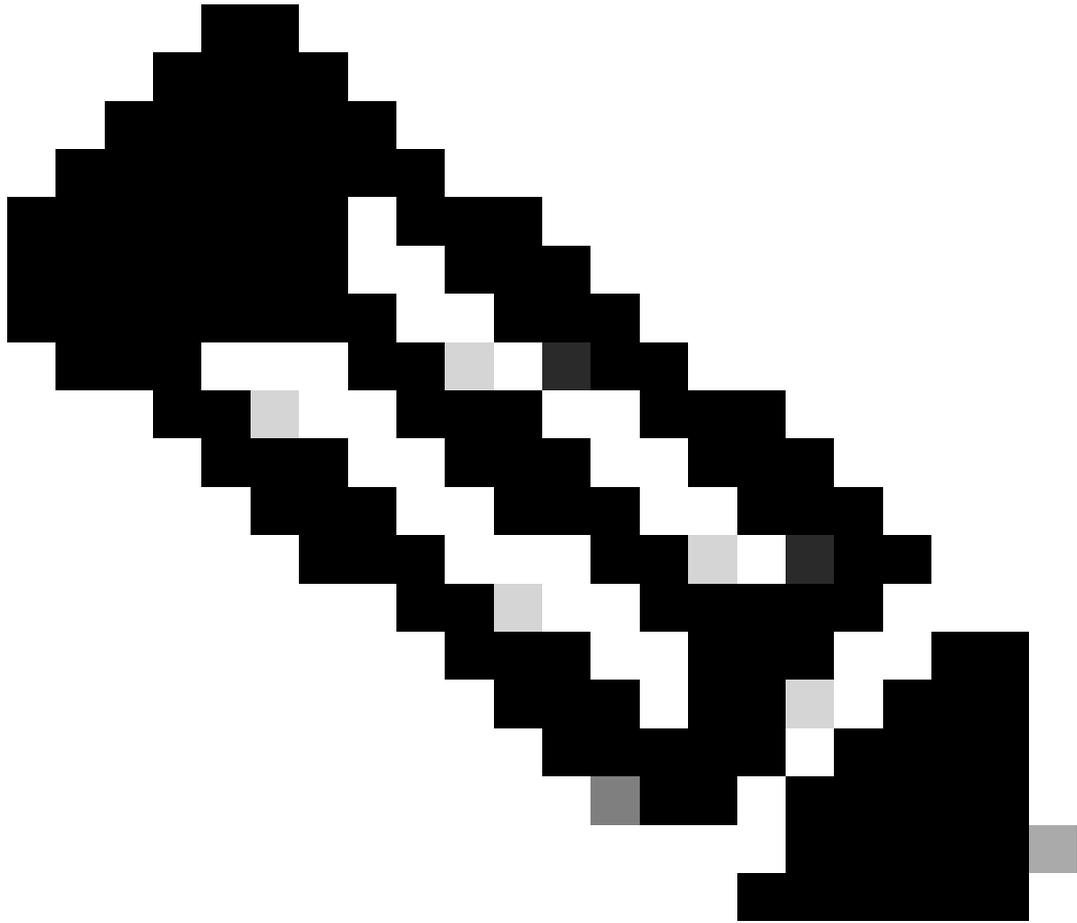
- **Authentication**

- **Method** : clé pré-partagée par défaut

- **Pre-shared Key** : Utilisez la **Passphrase** donnée dans l'étape [Données de tunnel](#)

- **IKE**

- Version : choisissez la version 2.



Remarque : Secure Access prend uniquement en charge IKEv2

Configurez maintenant le **Phase 1 Proposal**.

Proposition de phase 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 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 : sélectionnez AES256

- Authentication : sélectionnez SHA256

- Diffie-Hellman Groups : cochez les cases 19 et 20

- Key Lifetime (seconds) : 86400 par défaut

- Local ID : Utilisez la commande Primary Tunnel ID, donnée à l'étape [Données de tunnel](#)

Configurez maintenant le **Phase 2 Proposal**.

Proposition de phase 2

The image displays two screenshots of the 'New Phase 2' configuration interface. The left screenshot shows the 'Advanced...' section with various encryption and authentication options. The right screenshot shows the 'Advanced...' section with 'AES128' selected for encryption and 'SHA256' for authentication.

Left Screenshot (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, AES128, AES256, AES128GCM, AES256GCM, CHACHA20POLY1305
- Authentication options: 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 (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: 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** : défini par défaut (ce nom provient du nom de votre VPN)
 - **Local Address** : Laisser par défaut (0.0.0.0/0.0.0.0)
 - **Remote Address** : Laisser par défaut (0.0.0.0/0.0.0.0)

- Advanced
 - **Encryption** : sélectionnez AES128
 - **Authentication** : sélectionnez SHA256
 - **Enable Replay Detection** : Laisser par défaut (Activé)
 - **Enable Perfect Forward Secrecy (PFS)** : décochez la case
 - **Local Port** : Laisser par défaut (Activé)

- **Remote Port**: Laisser par défaut (Activé)
- **Protocol** : Laisser par défaut (Activé)
- **Auto-negotiate** : laissé par défaut (non marqué)
- **Autokey Keep Alive** : laissé par défaut (non marqué)
- **Key Lifetime** : Laisser par défaut (secondes)
- **Seconds** : laissé par défaut (43200)

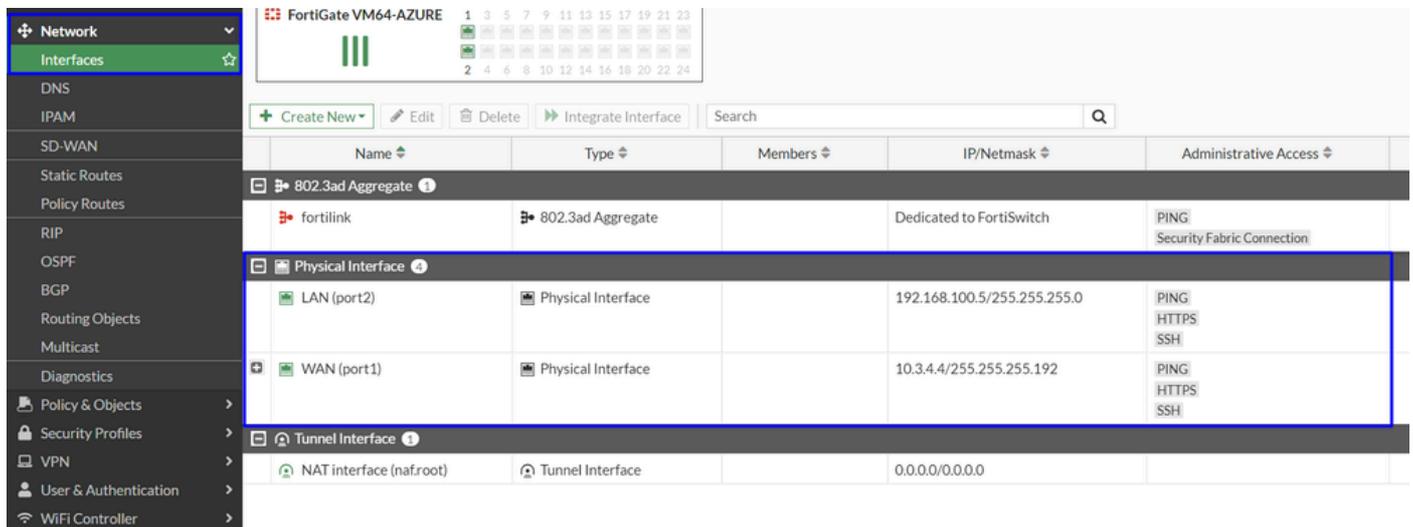
Ensuite, cliquez sur OK. Vous voyez après quelques minutes que le VPN a été établi avec un accès sécurisé, et vous pouvez passer à l'étape suivante, **Configure the Tunnel Interface**.



Configuration de l'interface du tunnel

Une fois le tunnel créé, vous remarquerez qu'une nouvelle interface se trouve derrière le port que vous utilisez comme interface WAN pour communiquer avec Secure Access.

Pour vérifier cela, accédez à **Network > Interfaces**.



Développez le port que vous utilisez pour communiquer avec Secure Access ; dans ce cas, l'**WAN** interface.



- Cliquez sur votre **Tunnel Interface** et sur **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

- Vous devez configurer l'image suivante

Name CSA
 Alias
 Type Tunnel Interface
 Interface WAN (port1)
 VRF ID 0
 Role Undefined

Name CSA
 Alias
 Type Tunnel Interface
 Interface WAN (port1)
 VRF ID 0
 Role Undefined

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

- Interface Configuration

- IP : configurez une adresse IP non routable que vous n'avez pas sur votre réseau (169.254.0.1)
- Remote IP/Netmask : configurez l'adresse IP distante en tant qu'adresse IP suivante de l'interface IP et avec le masque de réseau 30 (169.254.0.2 255.255.255.252)

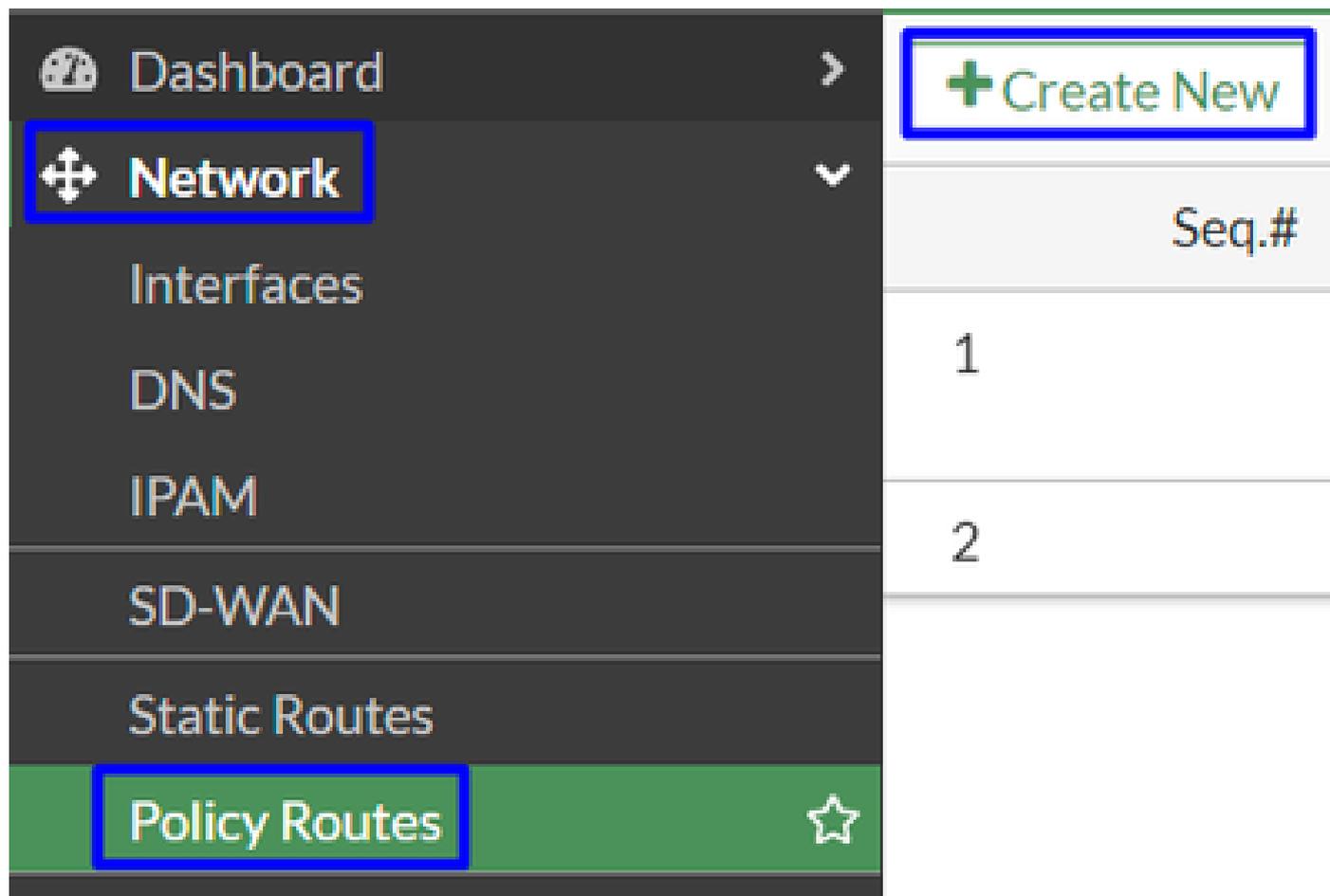
Après cela, cliquez sur **OK** pour enregistrer la configuration et passer à l'étape suivante, Configure Policy Route (routage basé sur l'origine).



Avertissement : Après cette partie, vous devez configurer les stratégies de pare-feu sur votre FortiGate afin d'autoriser ou d'autoriser le trafic de votre périphérique à l'accès sécurisé et de l'accès sécurisé aux réseaux que vous souhaitez acheminer le trafic.

À ce stade, votre VPN est configuré et défini sur Accès sécurisé ; vous devez à présent réacheminer le trafic vers Accès sécurisé pour protéger votre trafic ou l'accès à vos applications privées derrière votre pare-feu FortiGate.

- Naviguez jusqu'à 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

- Configurer la stratégie

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 : choisissez l'interface à partir de laquelle vous prévoyez de réacheminer le trafic vers l'accès sécurisé (origine du trafic)

- Source Address
 - IP/Netmask : utilisez cette option si vous routez uniquement un sous-réseau d'une interface
 - Addresses : utilisez cette option si l'objet est créé et que la source du trafic provient de plusieurs interfaces et sous-réseaux

- Destination Addresses

- Adresses: Choisir all
- Protocol: Choisir **ANY**
- Then
 - Action: **Choose Forward Traffic**
 - Outgoing Interface : Choisissez l'interface de tunnel que vous avez modifiée à l'étape [Configurer l'interface de tunnel](#)
 - Gateway Address: configurez l'adresse IP distante configurée à l'étape [RemoteIPNetmask](#)
 - Status : sélectionnez Activé

Cliquez **OK** pour enregistrer la configuration. Vous êtes maintenant prêt à vérifier si le trafic de vos périphériques a été réacheminé vers Secure Access.

Vérifier

Afin de vérifier si le trafic de votre machine a été réacheminé vers l'accès sécurisé, vous avez deux options : vous pouvez vérifier sur Internet et rechercher votre adresse IP publique, ou vous pouvez exécuter la commande suivante avec curl :

<#root>

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

La plage publique d'où vous pouvez voir votre trafic est :

Min Host:151.186.176.1

Max Host :151.186.207.254



Remarque : ces adresses IP sont sujettes à modification, ce qui signifie que Cisco va probablement étendre cette plage à l'avenir.

Si vous voyez le changement de votre IP publique, cela signifie que vous êtes protégé par un accès sécurisé, et maintenant vous pouvez configurer votre application privée sur le tableau de bord d'accès sécurisé pour accéder à vos applications à partir de VPNaaS ou ZTNA.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.