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
  - 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 d'avoir des connaissances sur les sujets suivants :

- 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

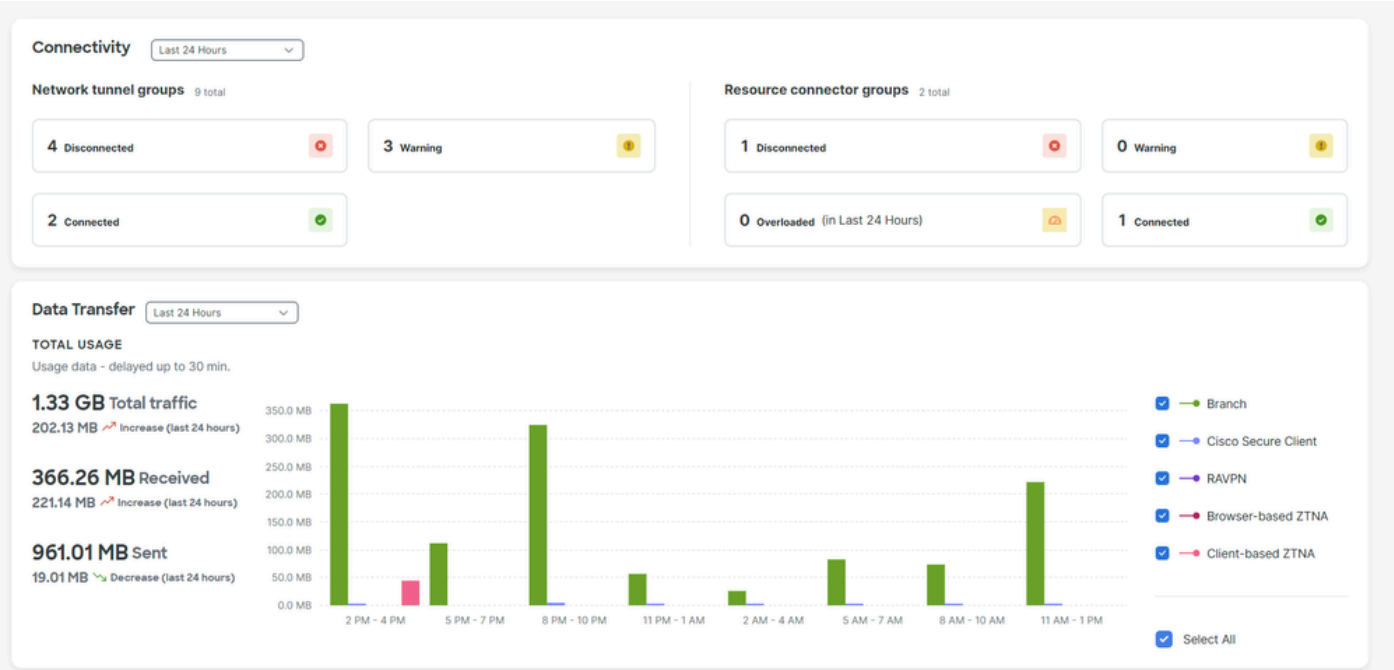


Cisco a conçu Secure Access pour protéger et fournir un accès aux applications privées, sur site et dans le cloud. Il protège également la connexion du réseau à Internet. Pour ce faire, plusieurs méthodes et couches de sécurité sont mises en oeuvre, toutes visant à préserver les informations lorsqu'elles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

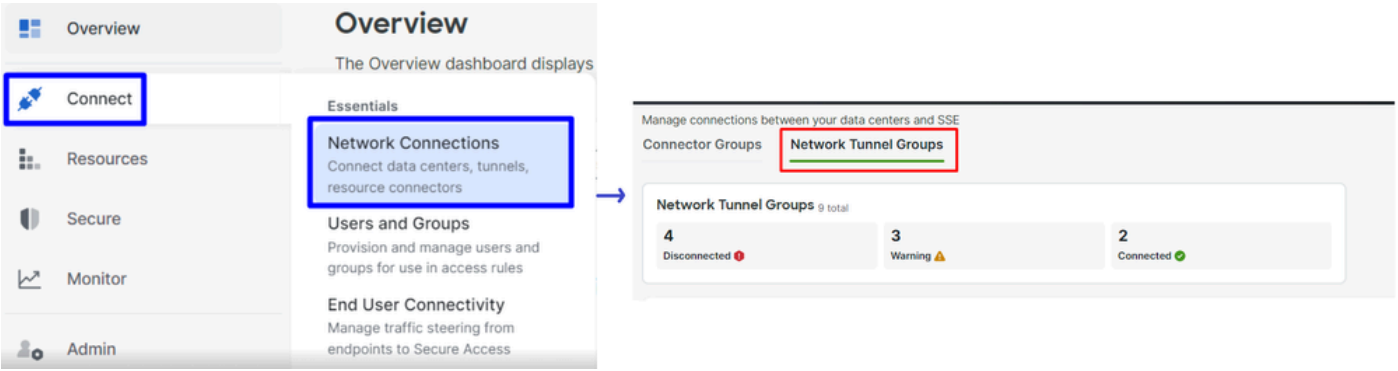
Configurer

Configurer le VPN sur un accès sécurisé

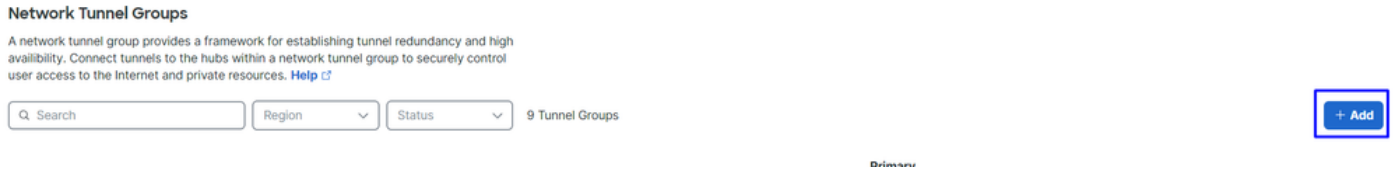
1. Accédez au panneau d'administration de Secure Access.



2. Cliquez sur Connect > Network Connections > Network Tunnels Groups.

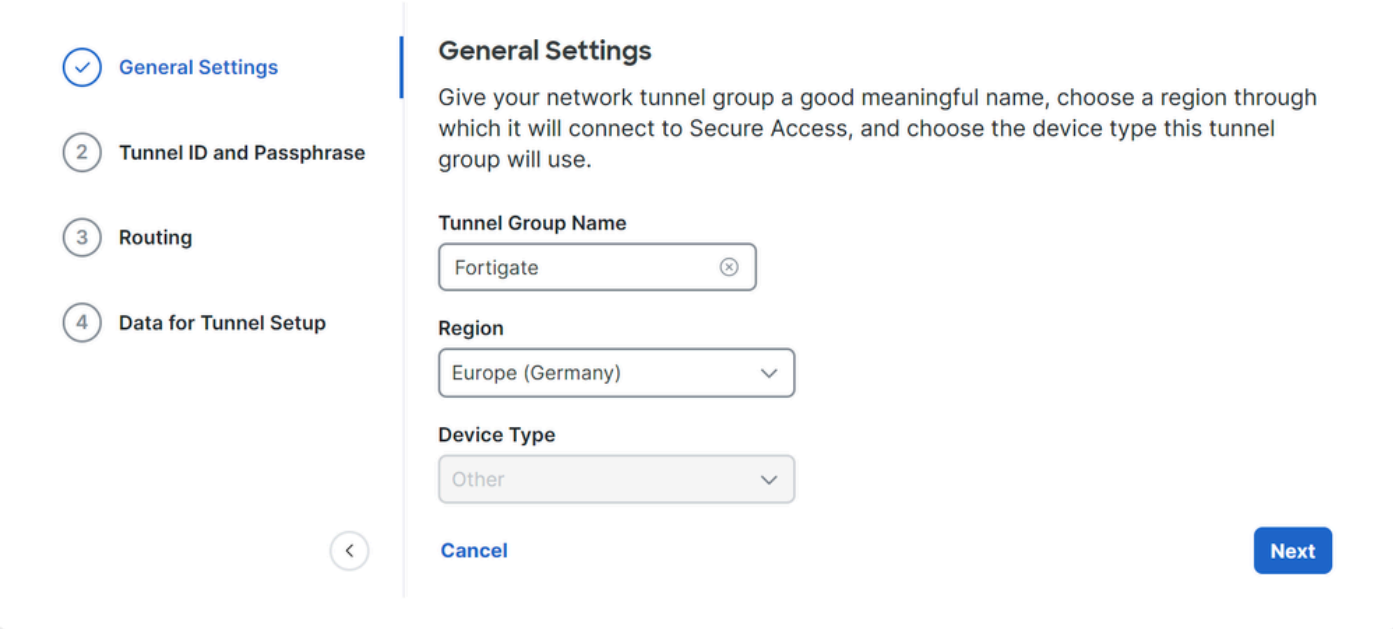


3. Sous Network Tunnel Groups, cliquez sur +Add.



4. Configurez le nom du groupe de tunnels, la région et le type de périphérique.

5. Cliquez sur Suivant.

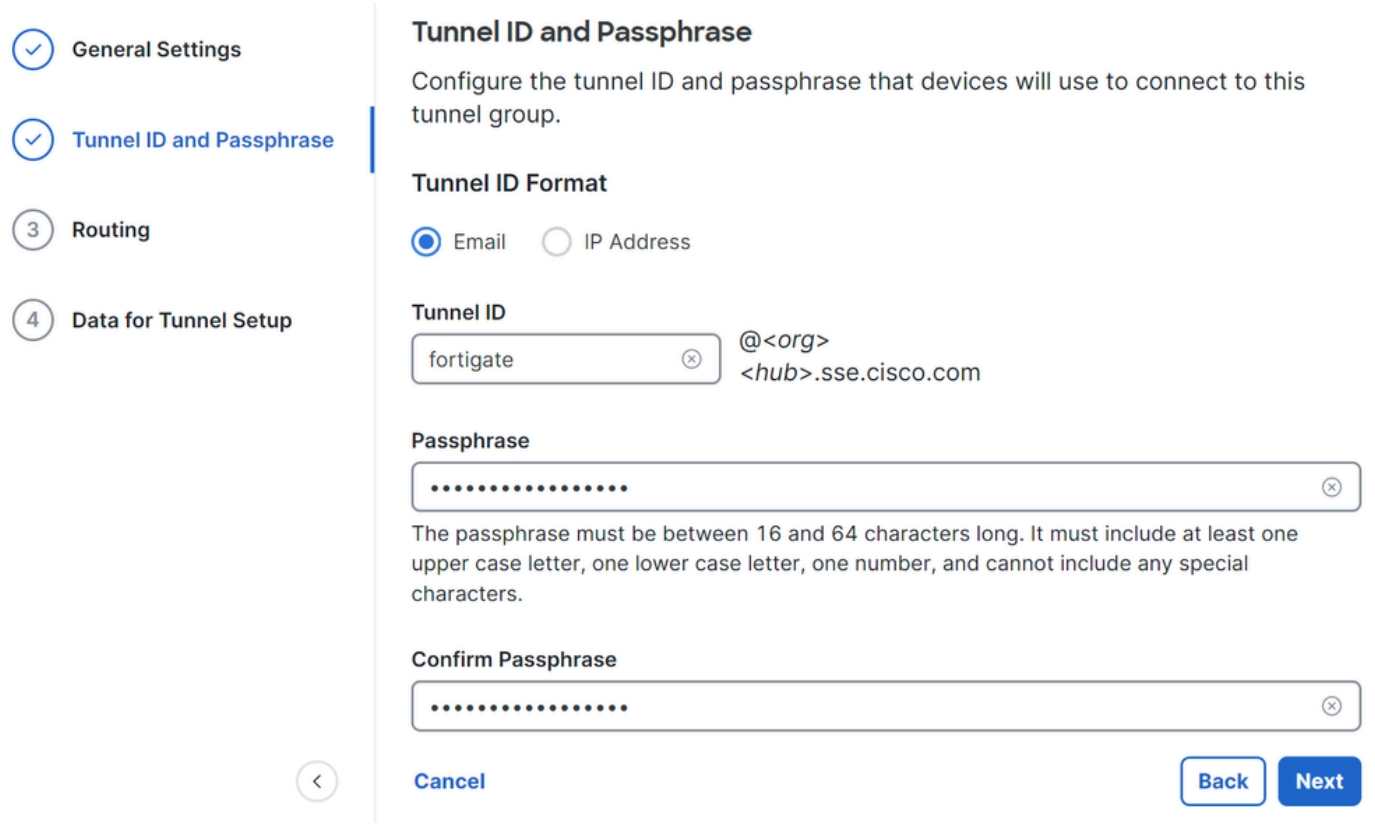


Remarque : Sélectionnez la région la plus proche de l'emplacement de votre pare-feu.

---

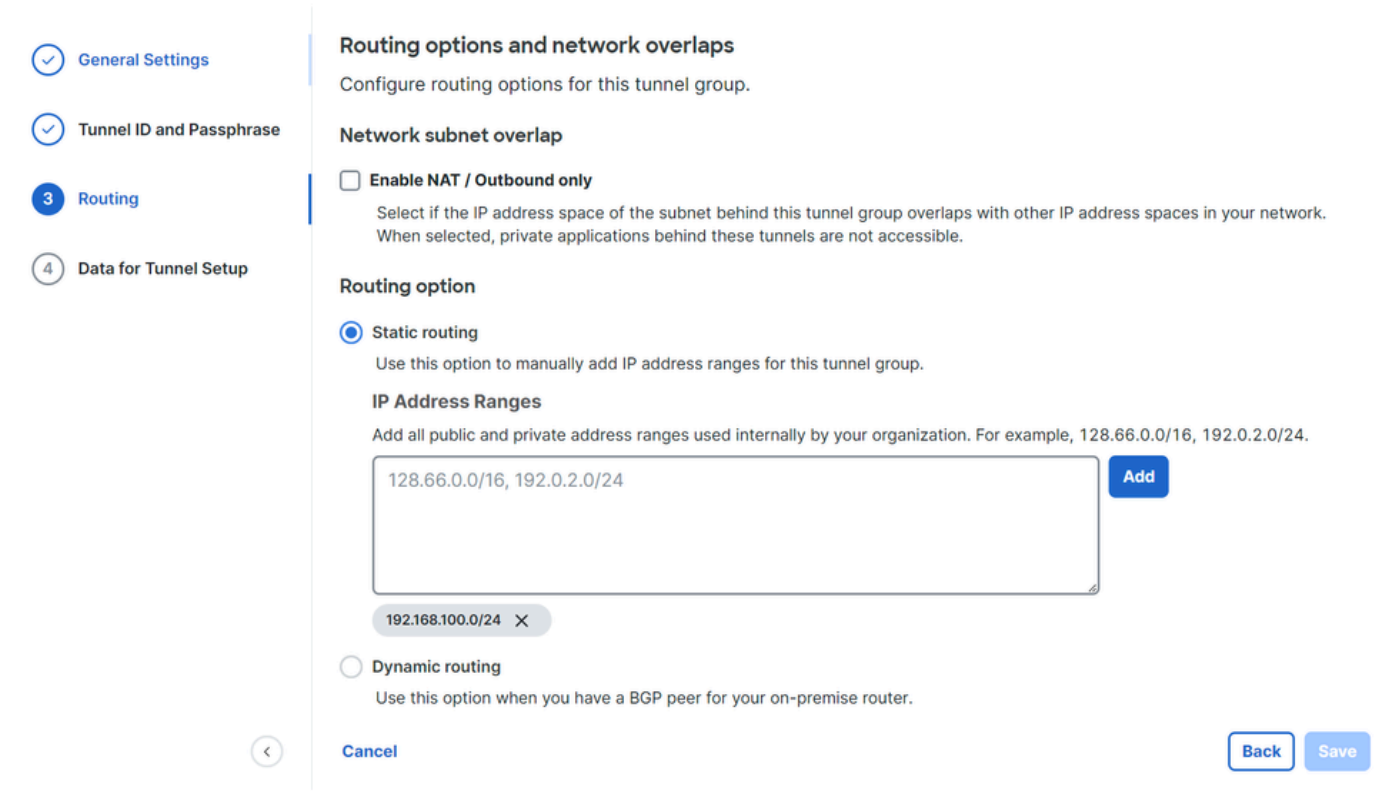
6. Configurez le format d'ID de tunnel et la phrase de passe.

7. Cliquez sur Suivant.



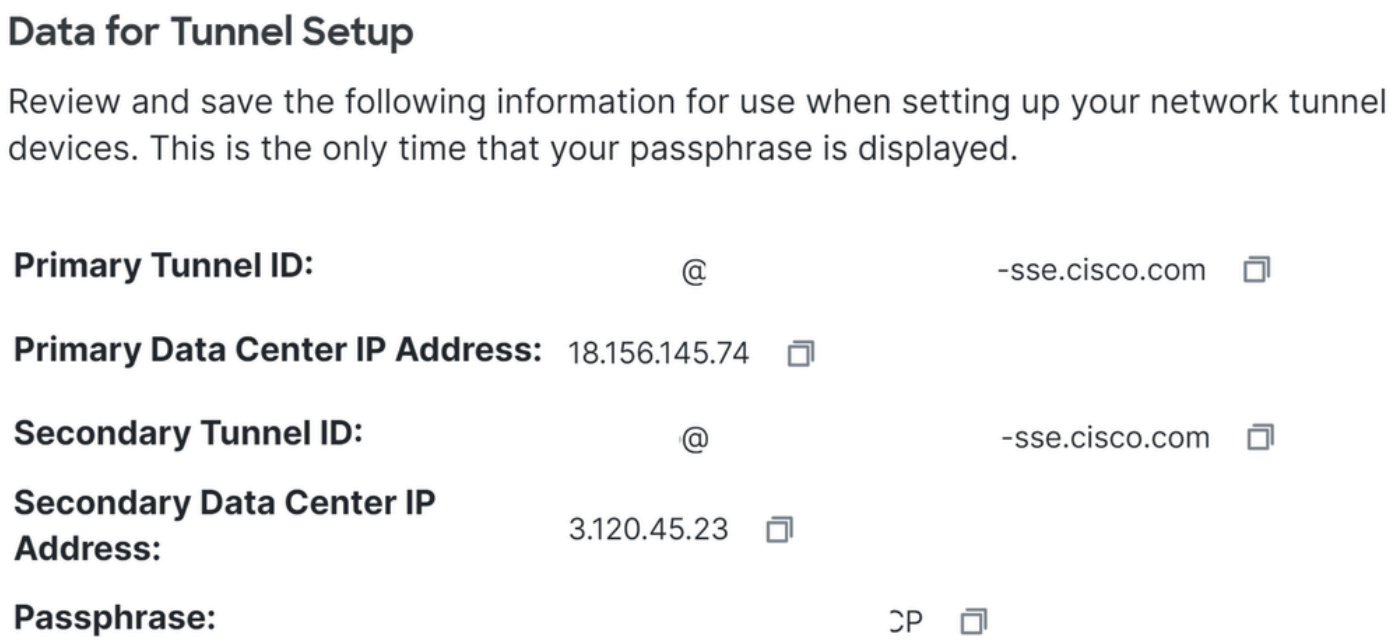
8. Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez faire passer le trafic via l'accès sécurisé.

9. Cliquez sur Enregistrer.



10. Une fois que vous avez enregistré, les informations sur le tunnel s'affichent. Enregistrez ces informations pour l'étape suivante : Configurez le site VPN sur le site Fortigate.

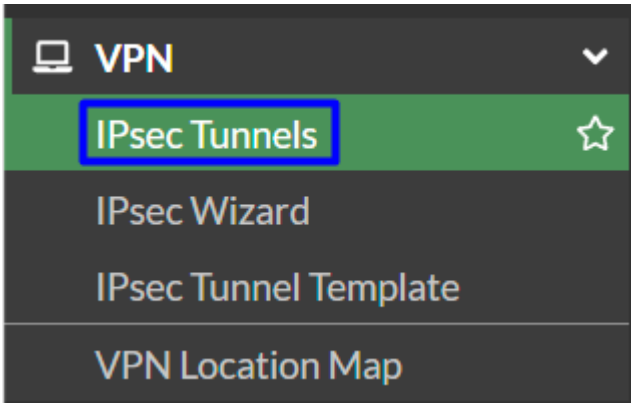
Données du tunnel



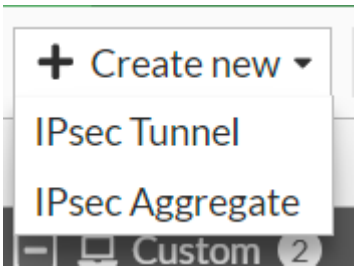
Configurer le site VPN sur le site Fortigate

1. Accédez à votre tableau de bord Fortigate.

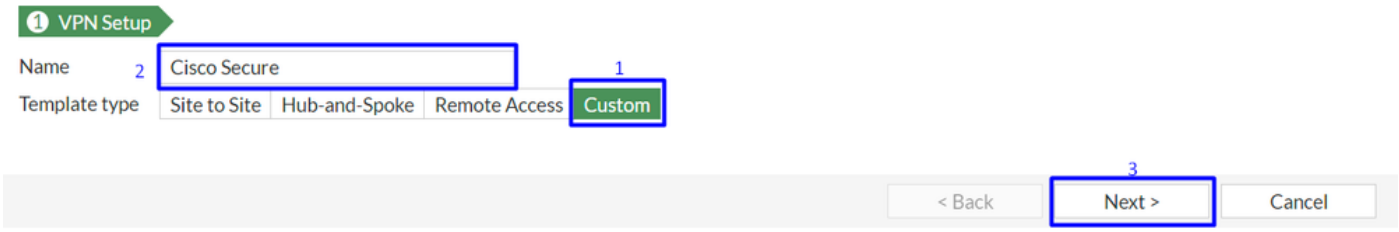
2. Cliquez sur VPN > IPsec Tunnels.



3. Cliquez sur Create New > IPsec **Tunnels**.

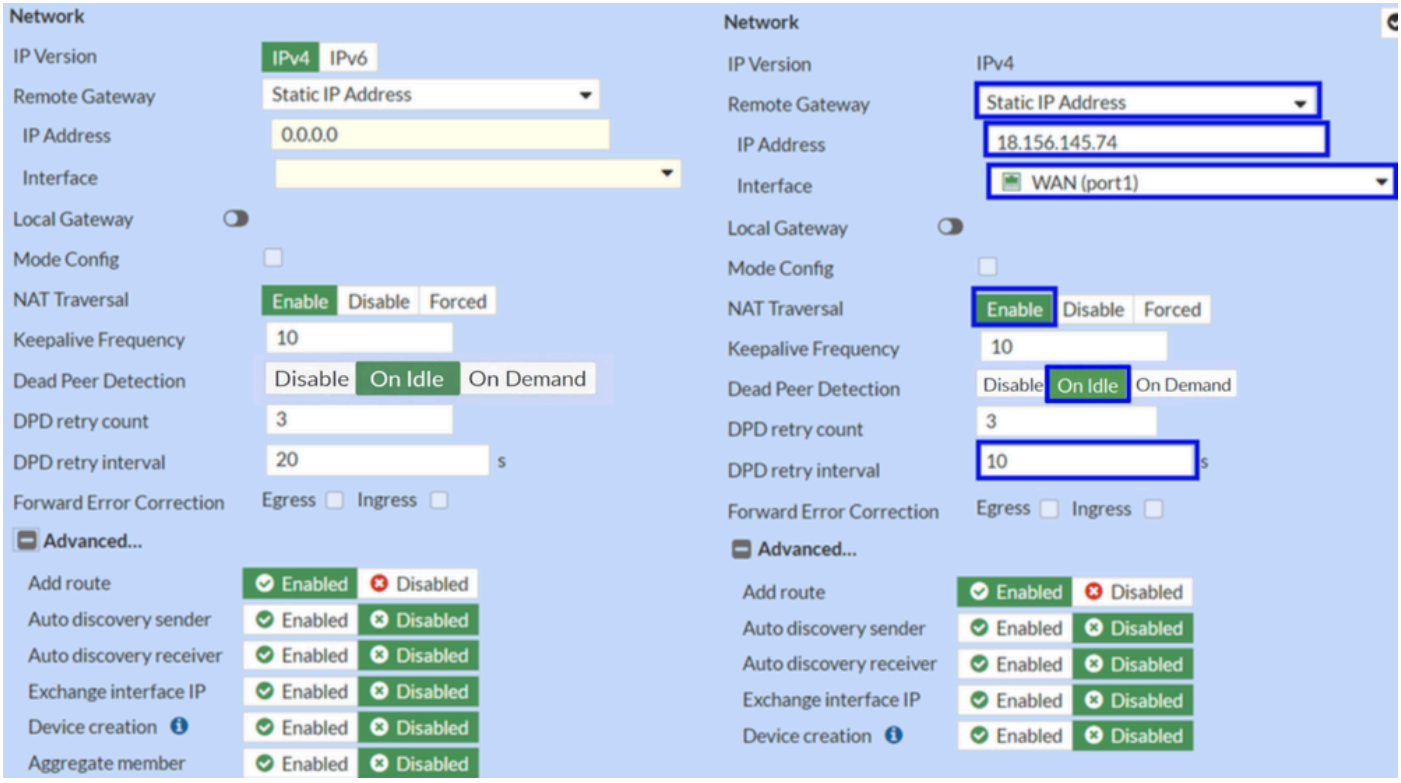


4. Cliquez sur Personnalisé, configurez un nom, puis cliquez sur Suivant.



Dans l'image suivante, vous pouvez voir comment configurer les paramètres du **Network**.

Réseau

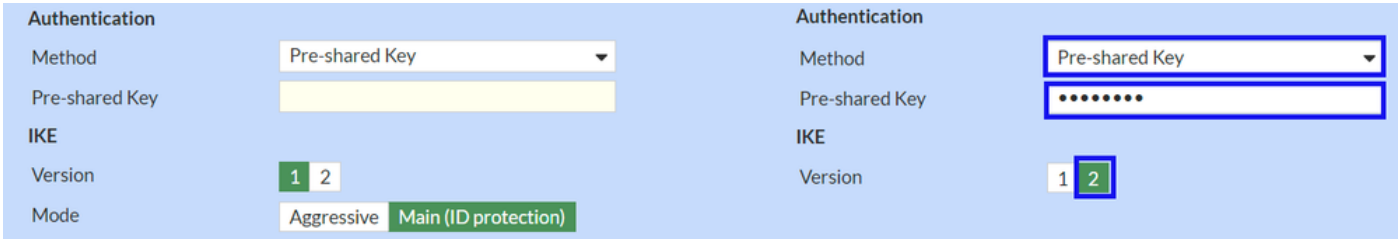


Réseau

- Version IP : IPv4
- Passerelle distante : Adresse IP statique
- Adresse IP: Utilisez l'adresse IP de l'adresse IP principale du data center, fournie dans les données du tunnel
- Interface: Choisissez l'interface WAN que vous prévoyez d'utiliser pour établir le tunnel
- Passerelle locale : Désactiver par défaut
- Configuration du mode : Désactiver par défaut
- Traversée NAT : Activer
- Keepalive Fréquence : 10
- Détection des homologues morts : Au repos
- Nombre de tentatives DPD : 3
- Intervalle entre les tentatives DPD : 10
- Correction des erreurs de transfert : Ne cochez aucune case
- Avancé... : Reportez-vous à la Phase 2 pour les étapes de configuration

À présent, configurez le **Authentication**routeur IKE.

Authentification

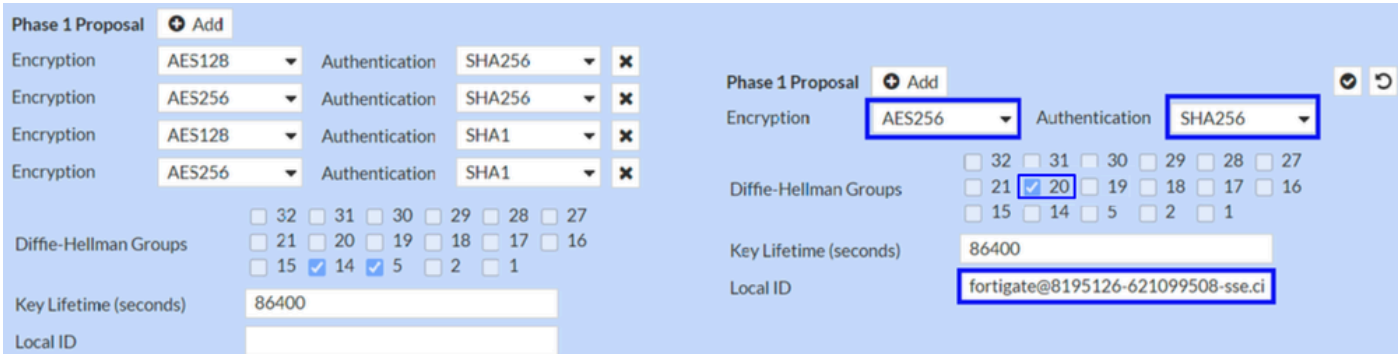


- Authentification
  - Méthode : Clé pré-partagée par défaut
  - Clé pré-partagée : utilisez la phrase de passe fournie à l'étape Données de tunnel
- IKE
  - Version : Choisir la version 2

Remarque : Secure Access prend uniquement en charge IKEv2.

Configurez ensuite le **Phase 1 Proposal**.

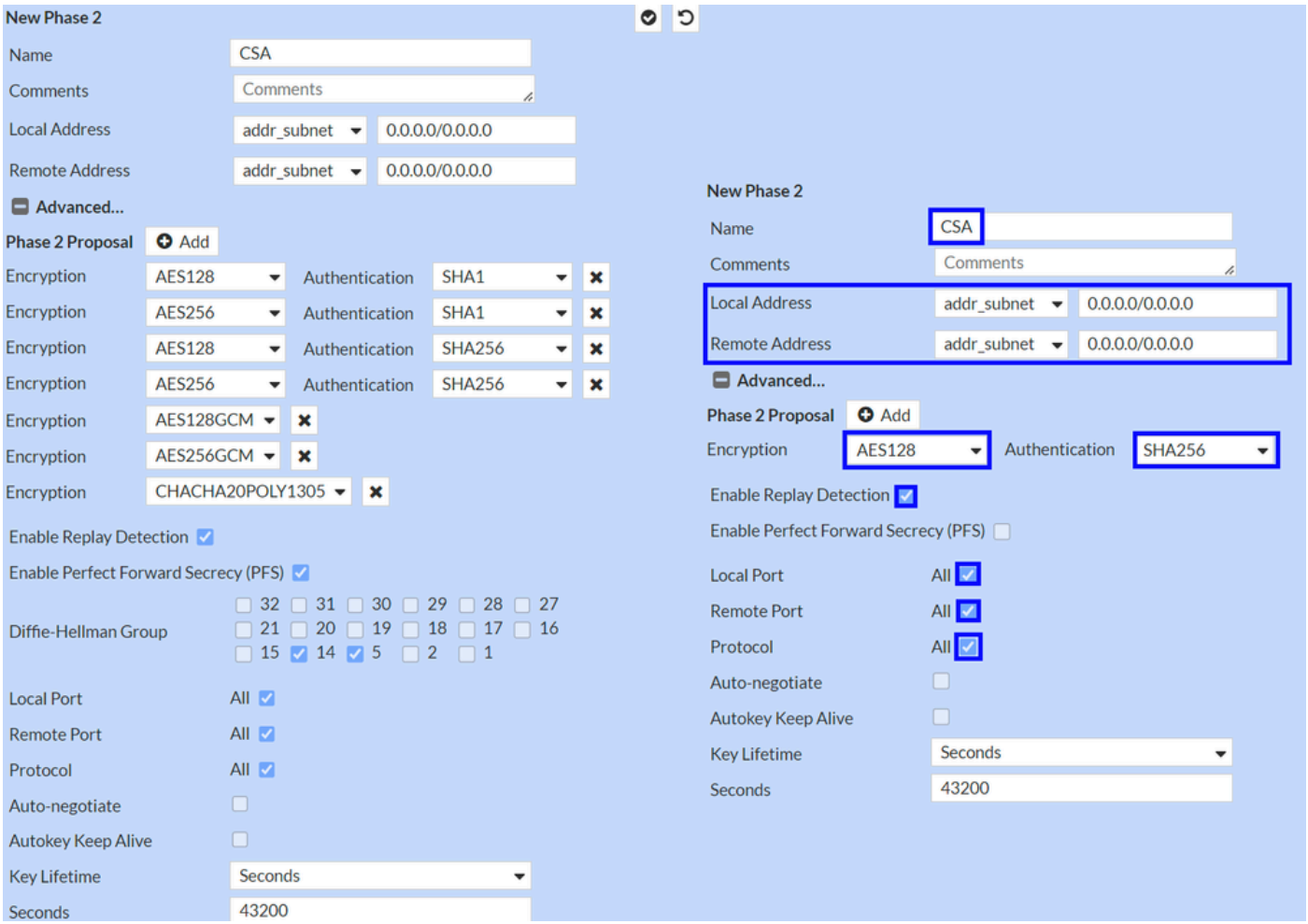
Proposition de phase 1



- Proposition de phase 1
  - Chiffrement : Choisir AES256
  - Authentification: Choisissez SHA256
  - Groupes Diffie-Hellman : Ne choisissez que 20, vous pouvez avoir des problèmes plus tard si vous choisissez des multiples
  - Durée de vie de la clé (secondes) : 86400 par défaut
  - ID local : Utilisez l'ID de tunnel principal, indiqué dans l'étape Données de tunnel

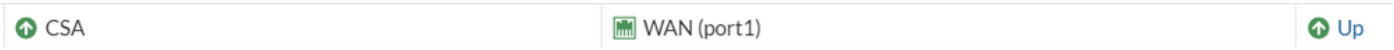
Configurez maintenant la proposition de phase 2.

Proposition de phase 2



- Nouvelle phase 2
  - Name : Laissez comme valeur par défaut (cette valeur correspond au nom de votre connexion VPN)
  - Adresse locale : Laisser par défaut (0.0.0.0/0.0.0.0)
  - Adresse distante : définie par défaut (0.0.0.0/0.0.0.0)
- Avancé
  - Chiffrement : Choisir AES128
  - Authentification: Choisissez SHA256
  - Activer la détection de relecture : Laisser par défaut (Activé)
  - Activer le protocole PFS (Perfect Forward Secrecy) Décochez la case
  - Port local : laisser par défaut (activé)
  - Port distant : Laisser par défaut (Activé)
  - Protocole : conserver par défaut (activé)
  - Négociation automatique : laisser par défaut (non marqué)
  - Clé auto Maintenir la connexion : conserver la connexion par défaut (non marquée)
  - Durée de vie des clés : Laisser par défaut (secondes)
  - Secondes : laisser par défaut (43200)

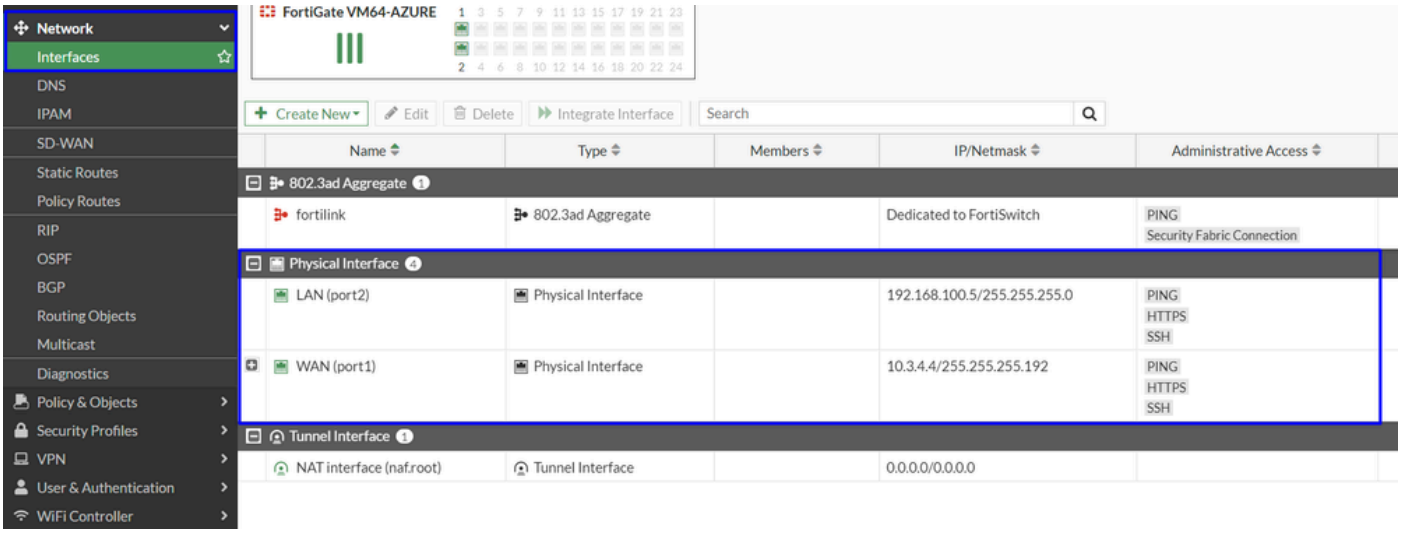
Après cela, cliquez sur OK. Vous verrez que le VPN a été établi avec un accès sécurisé et vous pourrez passer à l'étape suivante ; Configurez l'interface du tunnel.



Configuration de l'interface du tunnel

Une fois le tunnel créé, une nouvelle interface s'affiche derrière le port que vous utilisez comme interface WAN pour communiquer avec Secure Access.

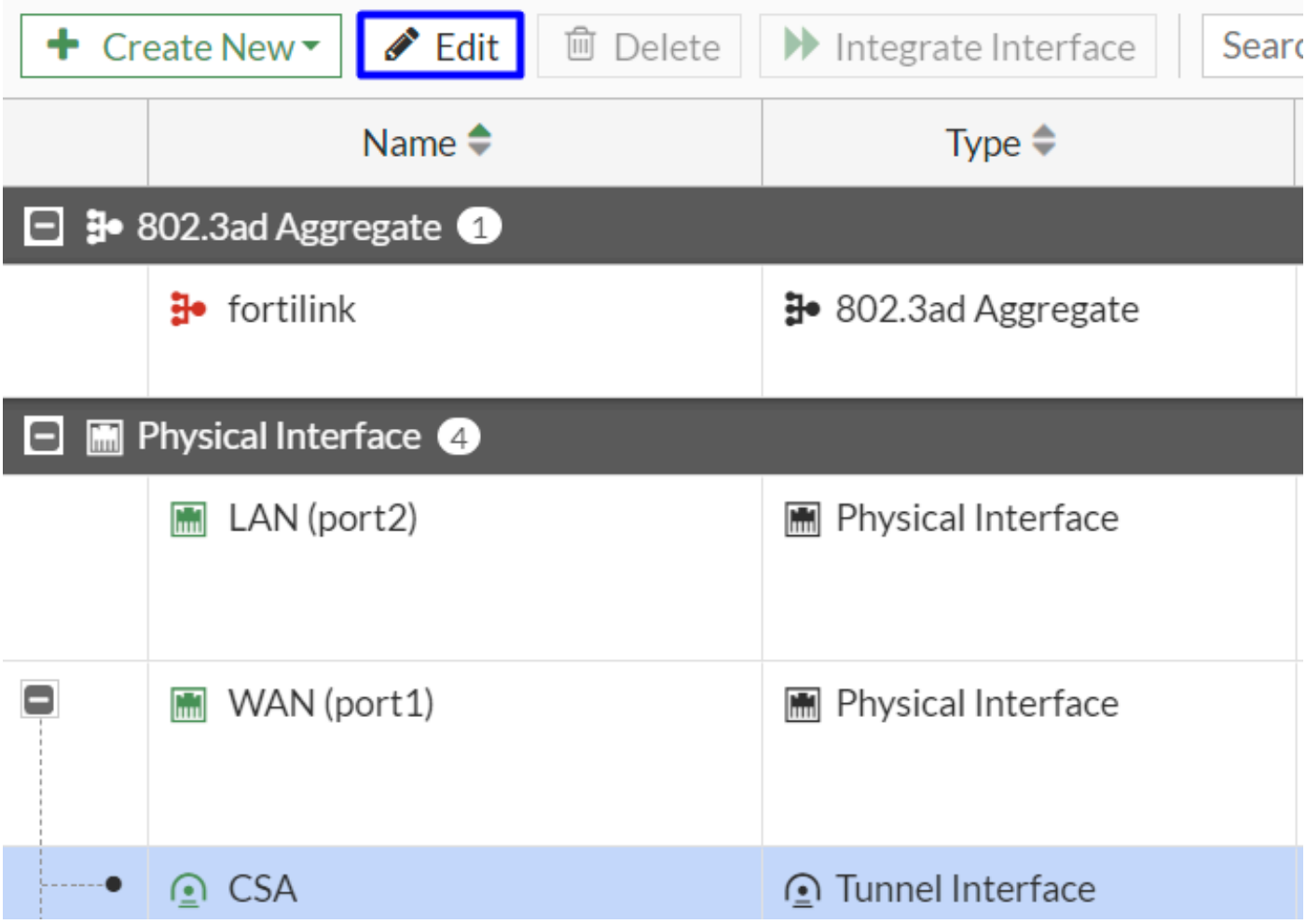
1. Pour le vérifier, accédez à **Network** > **Interfaces**.



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



3. Cliquez sur votre interface de tunnel et cliquez sur Edit.

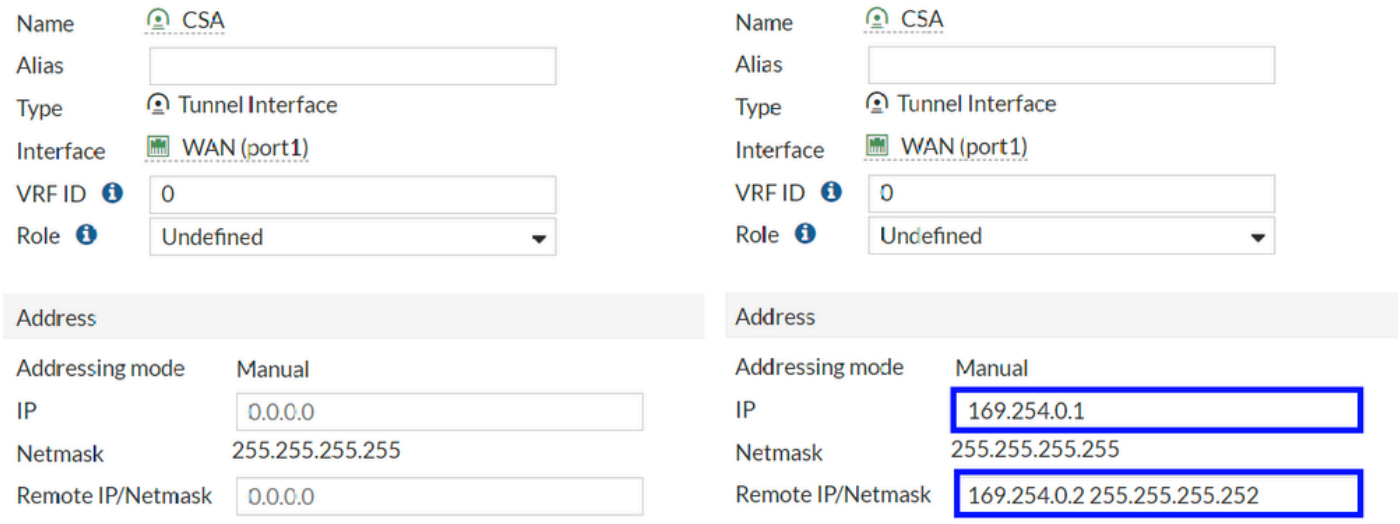


4. Reportez-vous à l'image pour configurer les paramètres.

Configuration de l’interface

- IP : Configurez une adresse IP non routable qui ne se trouve pas sur votre réseau (par exemple, 169.254.0.1).
- IP/masque de réseau distant: Configurez l'adresse IP distante en tant qu'adresse IP suivante pour votre adresse IP d'interface et avec un masque de réseau de 30 (par exemple, 169.254.0.2 255.255.255.252).

5. Cliquez sur ce bouton OK pour enregistrer les paramètres de configuration et passer à l’étape suivante : Configurer le routage de stratégie (routage basé sur l’origine).

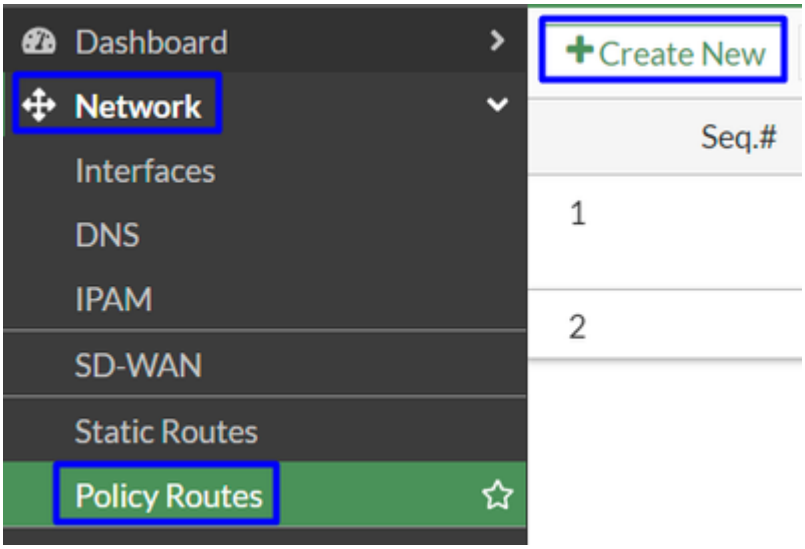


Avertissement : Une fois l'opération terminée, configurez les stratégies de pare-feu FortiGate pour autoriser le trafic de votre périphérique vers l'accès sécurisé et de l'accès sécurisé vers vos réseaux de destination.

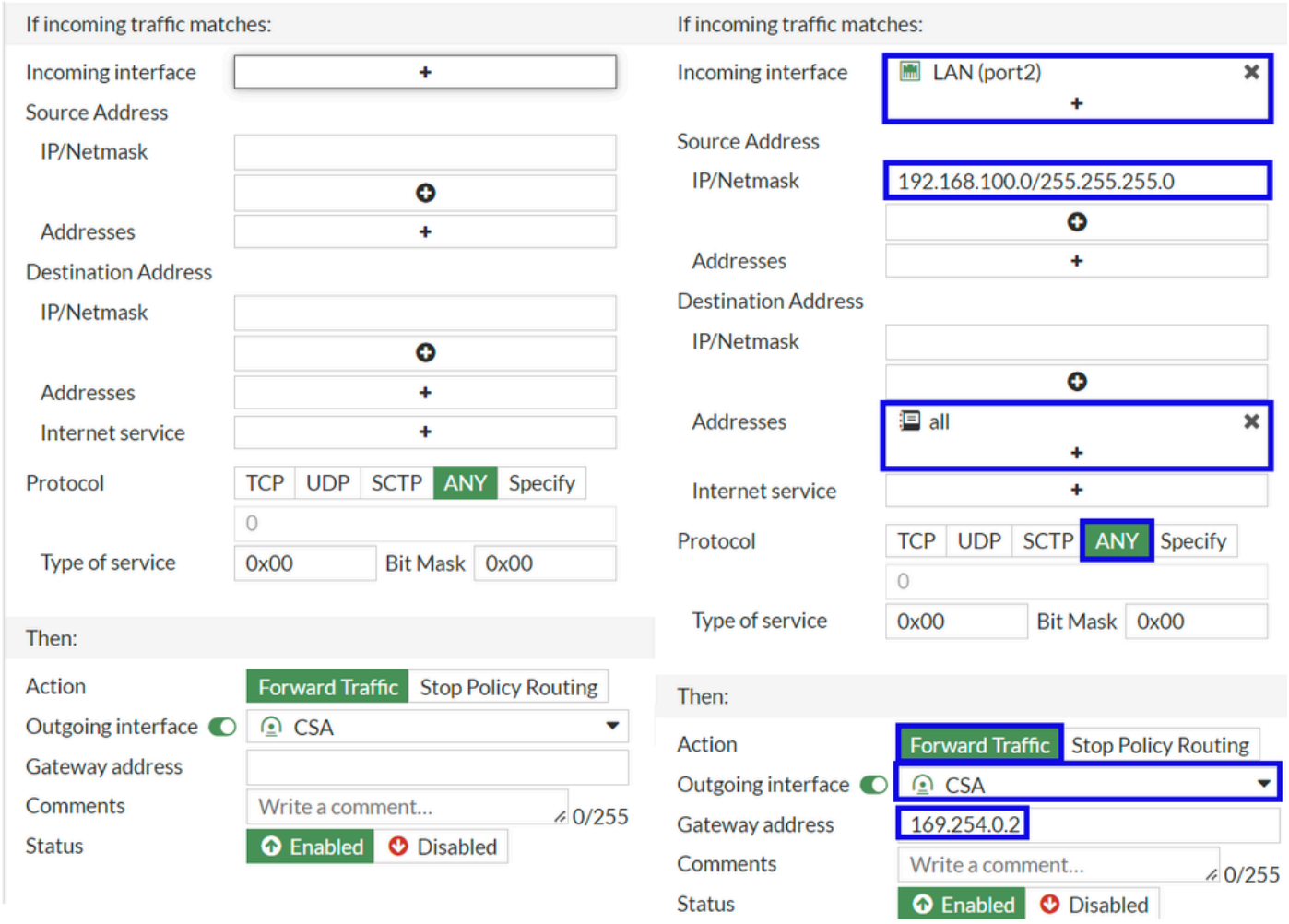
Configurer le routage de stratégie

À ce stade, votre VPN est configuré et configuré pour un accès sécurisé. Maintenant, vous devez réacheminer le trafic vers Secure Access pour protéger votre trafic ou l'accès à vos applications privées derrière votre pare-feu FortiGate.

1. Accédez à Network > Policy **Routes**.



2. Configurez la stratégie.



- Si le trafic entrant correspond :
  - Interface entrante : Choisissez l'interface sur laquelle vous prévoyez de réacheminer le trafic vers Secure Access (origine du trafic).
- Adresse source
  - IP/masque réseau : Utilisez cette option si vous routez uniquement un sous-réseau d'une interface.
  - Adresses : Utilisez cette option si un objet est créé et que la source du trafic provient de plusieurs interfaces et sous-réseaux.
- Adresses de destination
  - Adresses : Choisissez all si vous voulez protéger le trafic Internet. Si vous voulez un accès privé, vous devez ajouter votre pool IP de profil VPN et la plage CGNAT 100.64.0.0/10.
  - Protocole : Sélectionnez ANY.
- Alors
  - Action : Choisir le trafic de transfert
- Interface sortante : Choisissez l'interface de tunnel que vous avez modifiée dans l'étape Configure Tunnel Interface.
- Adresse de la passerelle : Configurez l'adresse IP distante configurée à l'étape RemoteIPNetmask.
- État : Sélectionnez Activé.

3. Cliquez sur OK pour enregistrer les paramètres de configuration. Vérifiez si le trafic vers vos périphériques a été réacheminé vers l'accès sécurisé.

Vérifier

Pour vérifier si le trafic a été réacheminé de 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 avec curl :

```
C:\Windows\system32>curl ipinfo.io
{
  "ip": "151.186.197.1",
  "city": "Frankfurt am Main",
  "region": "Hesse",
  "country": "DE",
  "loc": "50.1112,8.6831",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "60311",
  "timezone": "Europe/Berlin",
  "readme": "https://ipinfo.io/missingauth"
}
```

La plage publique où vous pouvez voir votre trafic est :

- Hôte min : 151.186.176.1
- Hôte max. : 151.186.207.254

Remarque : Ces adresses IP sont sujettes à modification. Cisco peut étendre cette portée à l'avenir.

Si vous constatez un changement dans votre adresse IP publique, cela signifie que vous êtes protégé par un accès sécurisé. Vous pouvez configurer votre application privée sur le tableau de bord Secure Access 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.