Konfigurieren von sicherem Zugriff mit Fortigate Firewall

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit der Fortigate Firewall konfigurieren.

Voraussetzungen

- Konfiguration der Benutzerbereitstellung
- Konfiguration der ZTNA SSO-Authentifizierung
- Konfigurieren des sicheren Remotezugriff-VPN

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Fortigate 7.4.x Version Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Fortigate 7.4.x Version Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

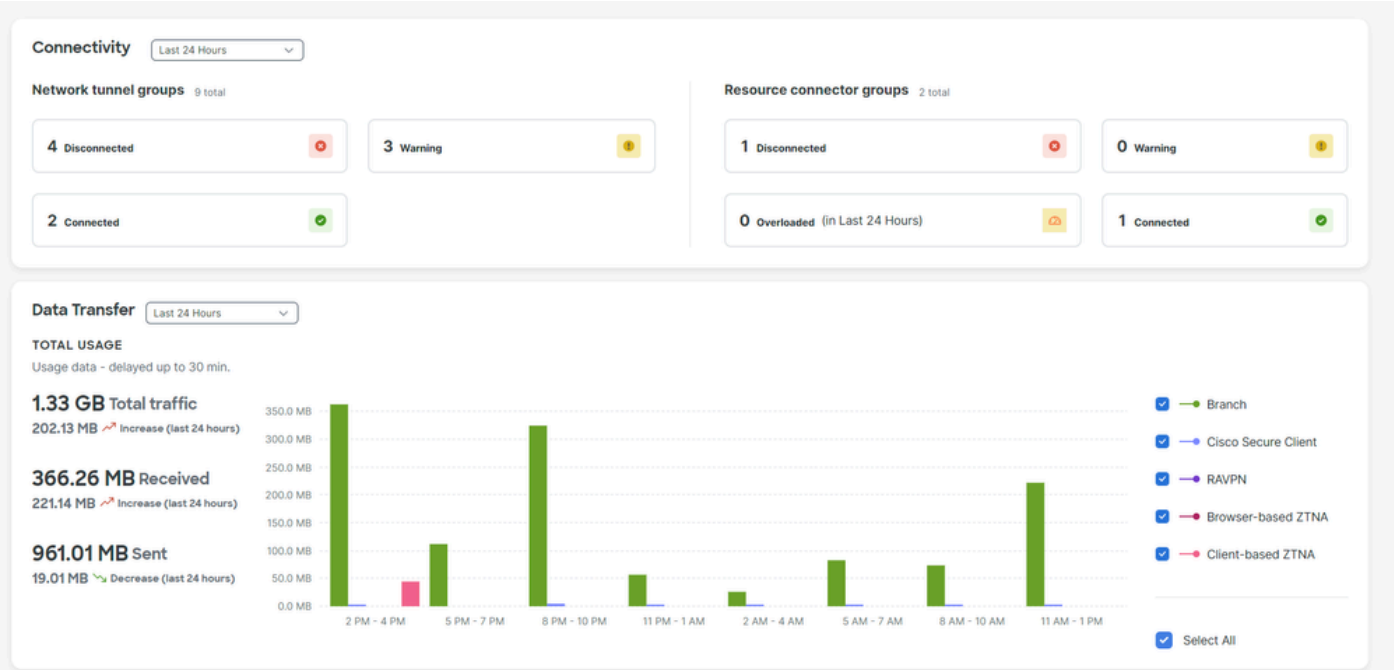
Hintergrundinformationen

Cisco hat Secure Access entwickelt, um den Zugriff auf private Anwendungen vor Ort und in der Cloud zu schützen. Außerdem wird die Verbindung vom Netzwerk zum Internet gesichert. Dies wird durch die Implementierung mehrerer Sicherheitsmethoden und -ebenen erreicht, die alle darauf abzielen, die Informationen beim Zugriff über die Cloud zu erhalten.

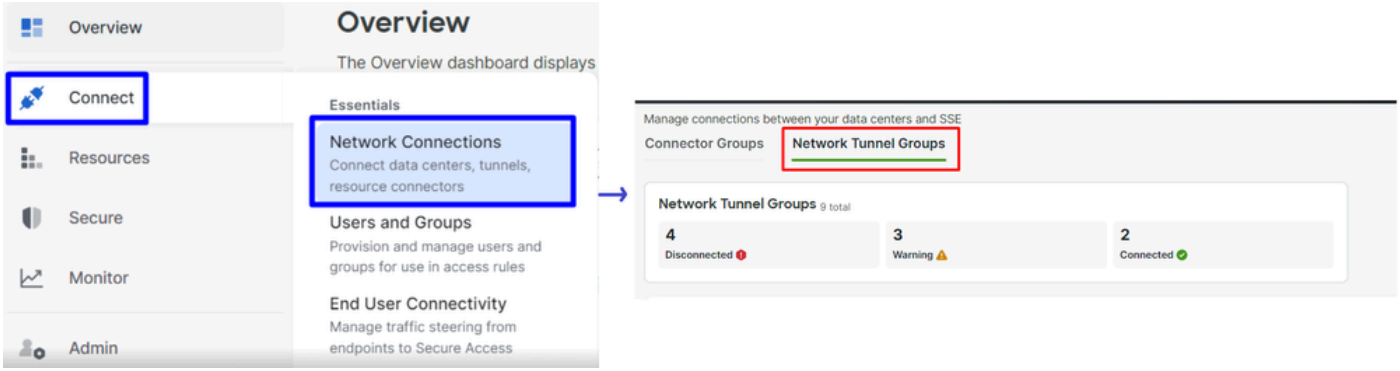
Konfigurieren

Konfigurieren des VPN für sicheren Zugriff

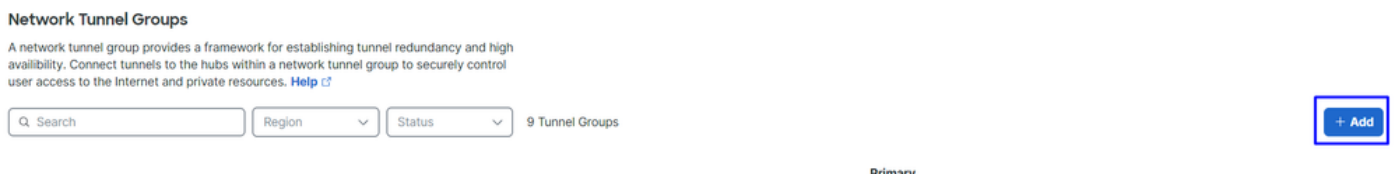
Navigieren Sie zum Admin-Bereich von [Secure Access](#).



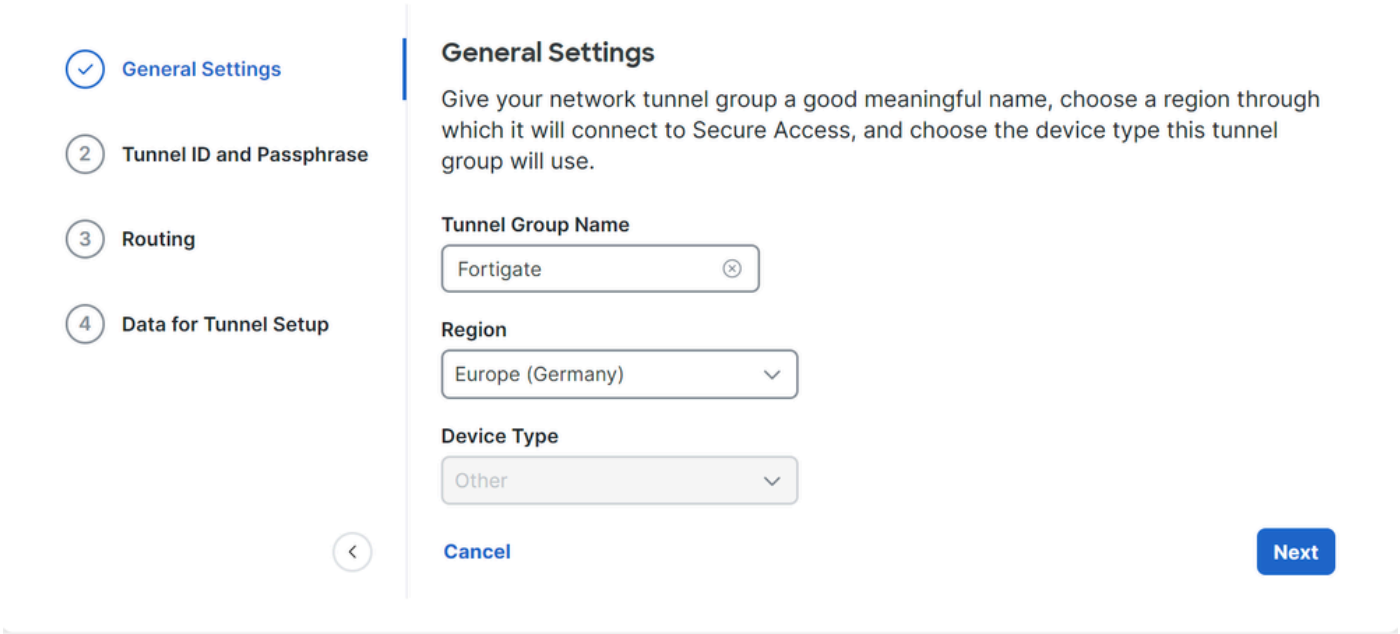
- Klicken Sie Connect > Network Connections > Network Tunnels Groups

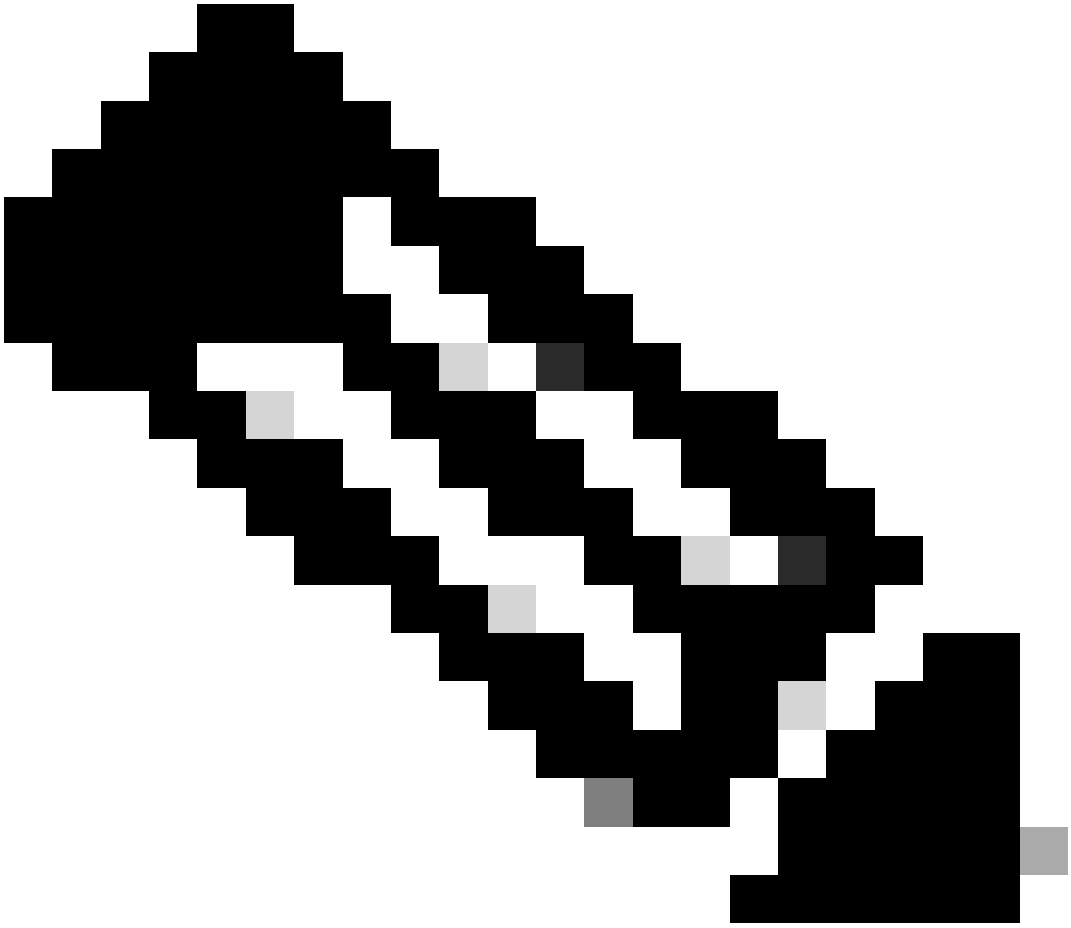


- Klicken Sie unter Network Tunnel Groups auf + Add



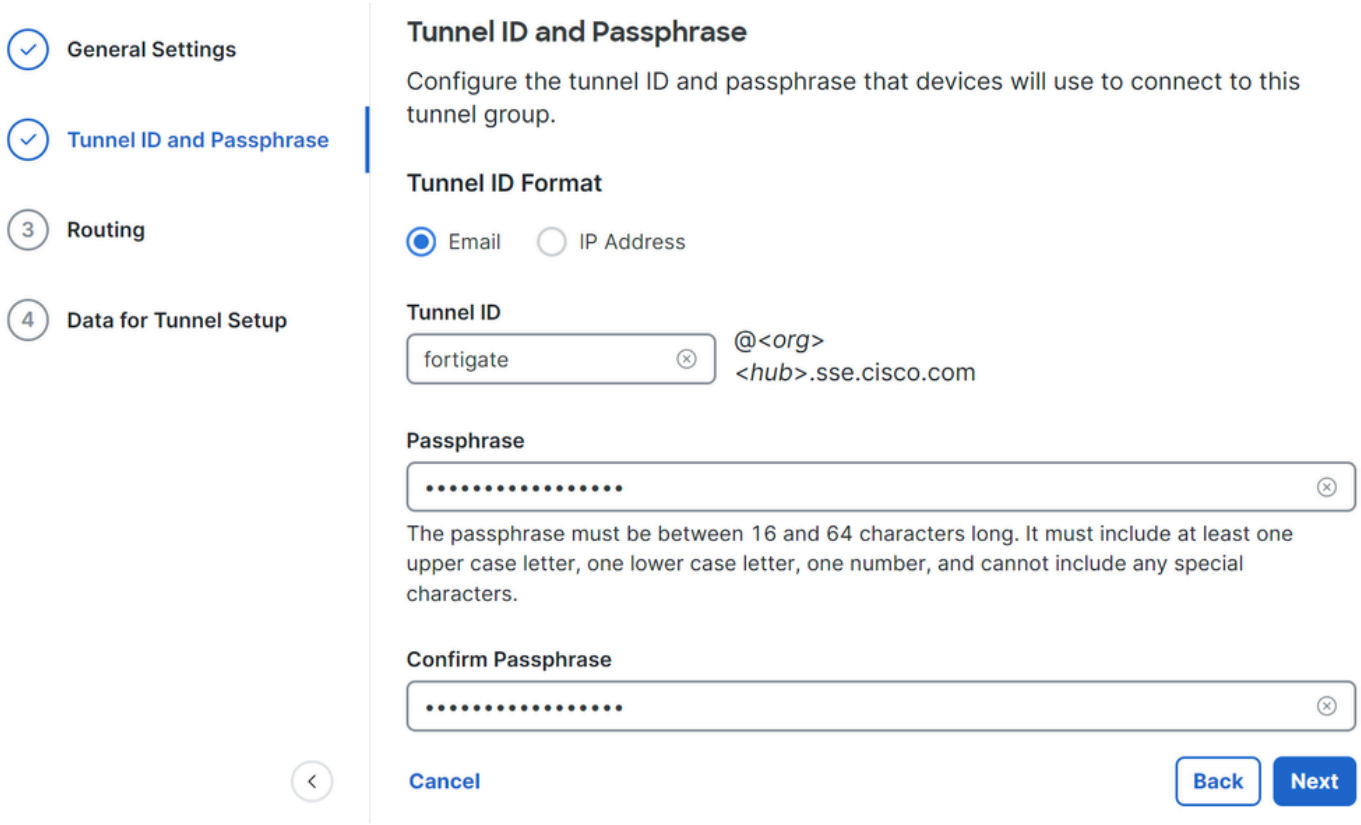
- Konfiguration Tunnel Group Name Region und Device Type
- Klicken Sie auf **Next**


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
Fortigate
Region
Europe (Germany)
Device Type
Other
Cancel
Next



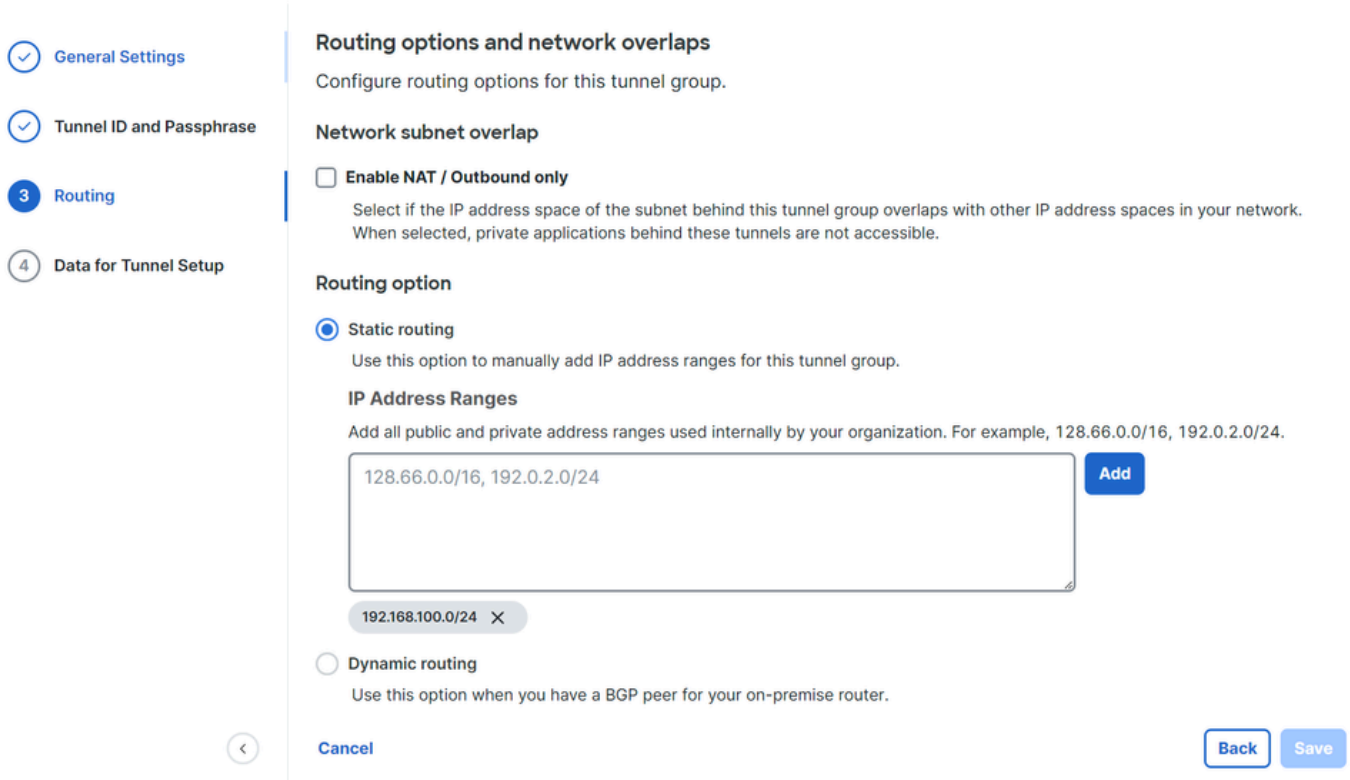
Hinweis: Wählen Sie die Region aus, die dem Standort Ihrer Firewall am nächsten ist.

- Konfigurieren Sie die Tunnel ID Format und Passphrase
- Klicken Sie auf Next



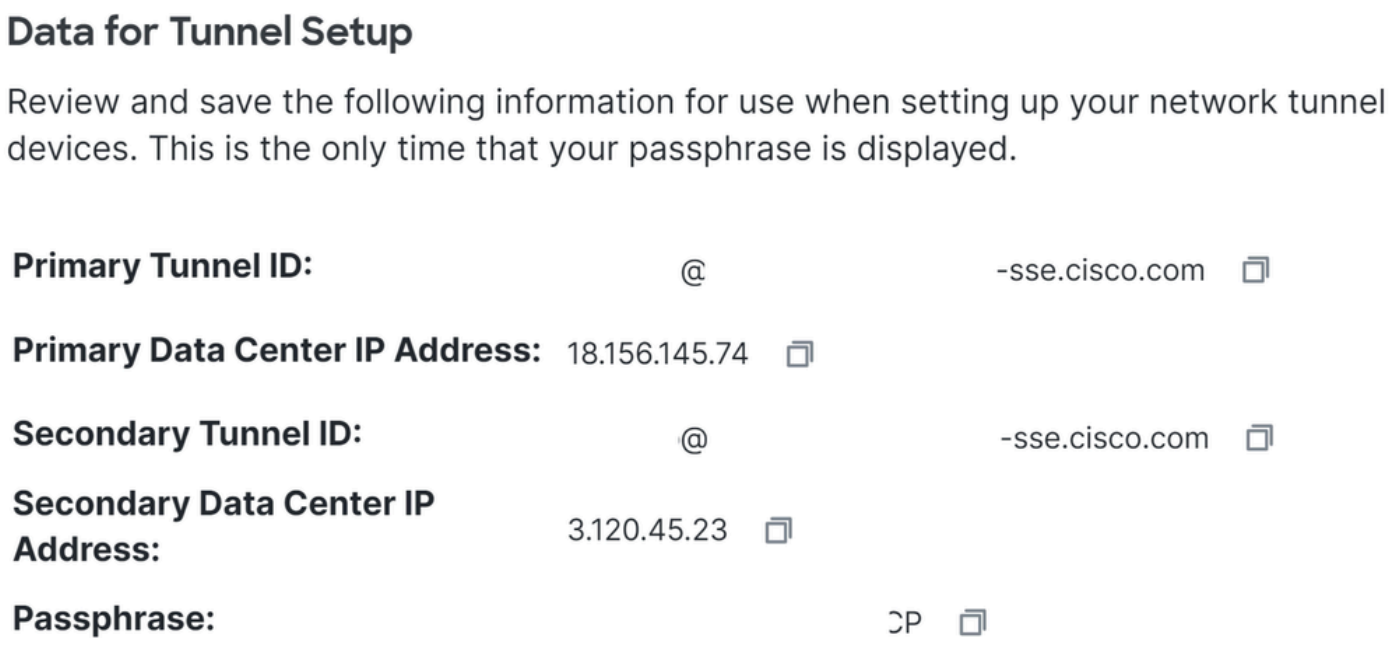
- Konfigurieren Sie die IP-Adressbereiche oder Hosts, die Sie in Ihrem Netzwerk konfiguriert haben, und leiten Sie den Datenverkehr über sicheren Zugriff weiter.

- Klicken Sie auf **Save**



Nachdem Sie auf **Save** die Informationen über den Tunnel geklickt haben, speichern Sie diese Informationen für den nächsten Schritt. **Configure the VPN Site to Site on Fortigate**.

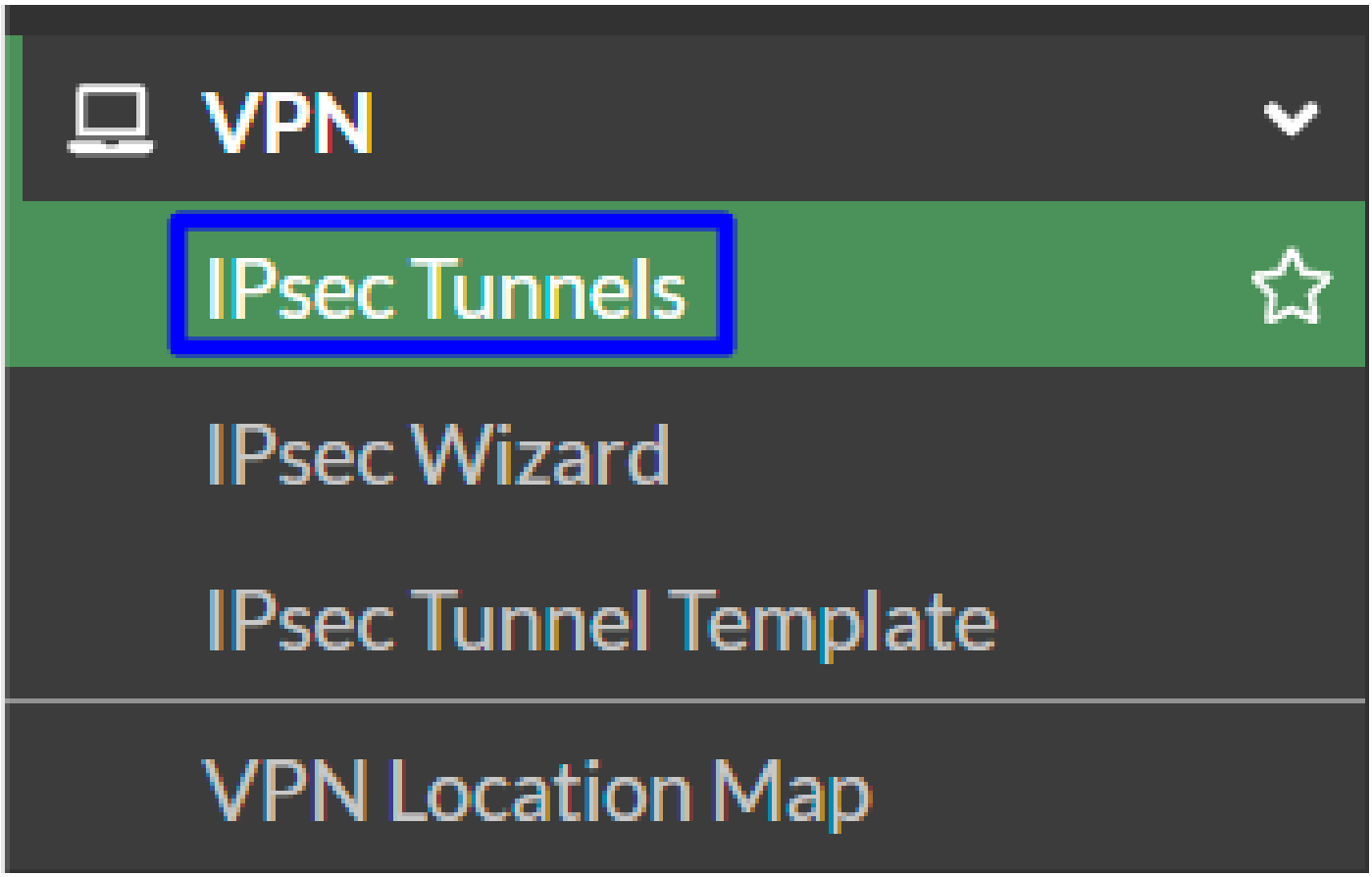
Tunneldaten



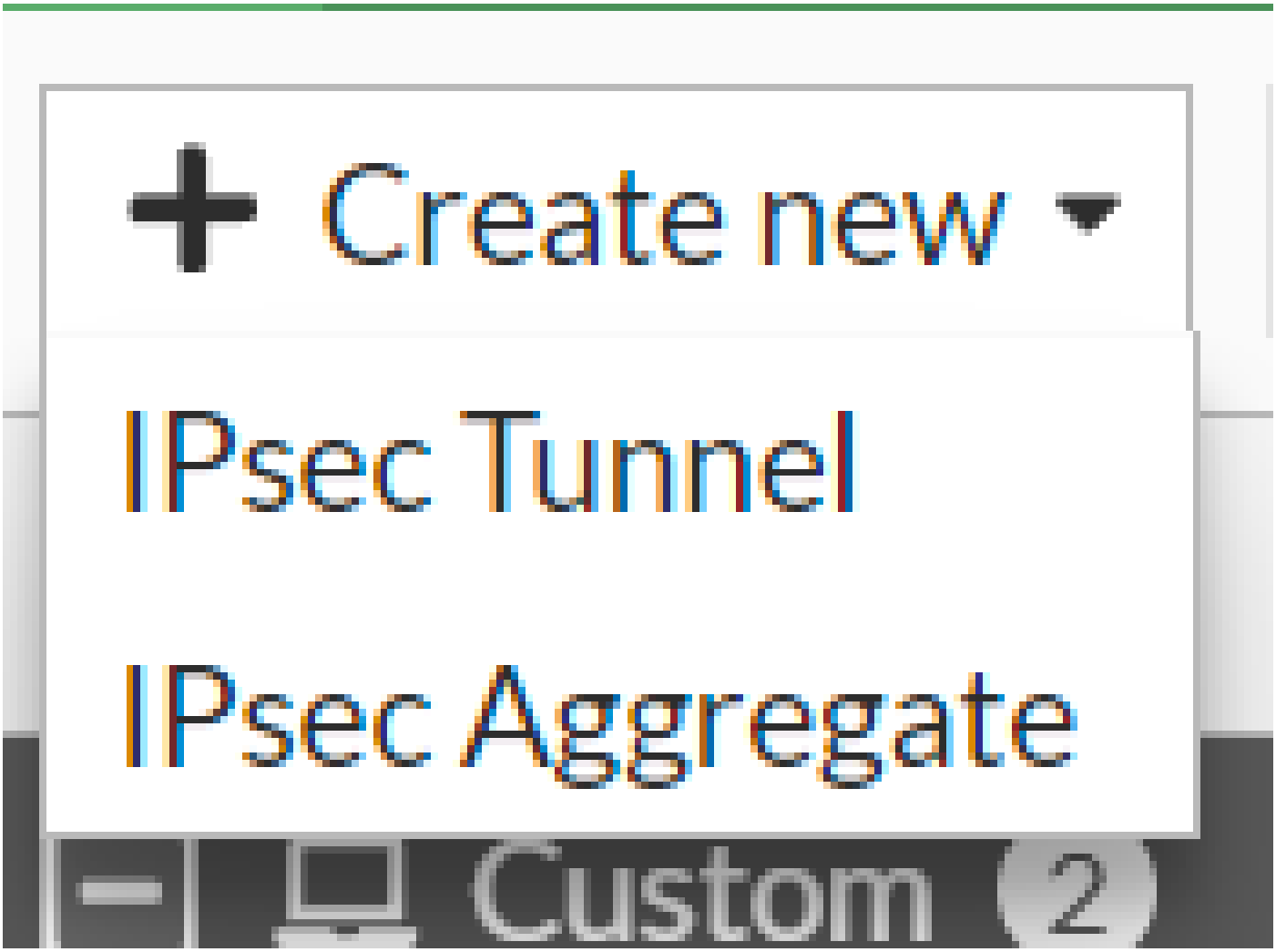
Konfigurieren des VPN-Standorts auf dem Fortigate

Navigieren Sie zu Ihrem Fortigate-Dashboard.

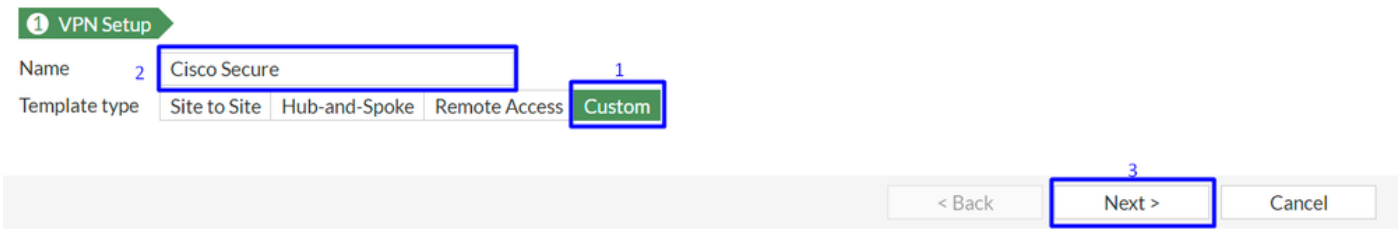
- Klicken Sie auf VPN > IPsec Tunnels



- Klicken Sie auf Create New > IPsec Tunnels

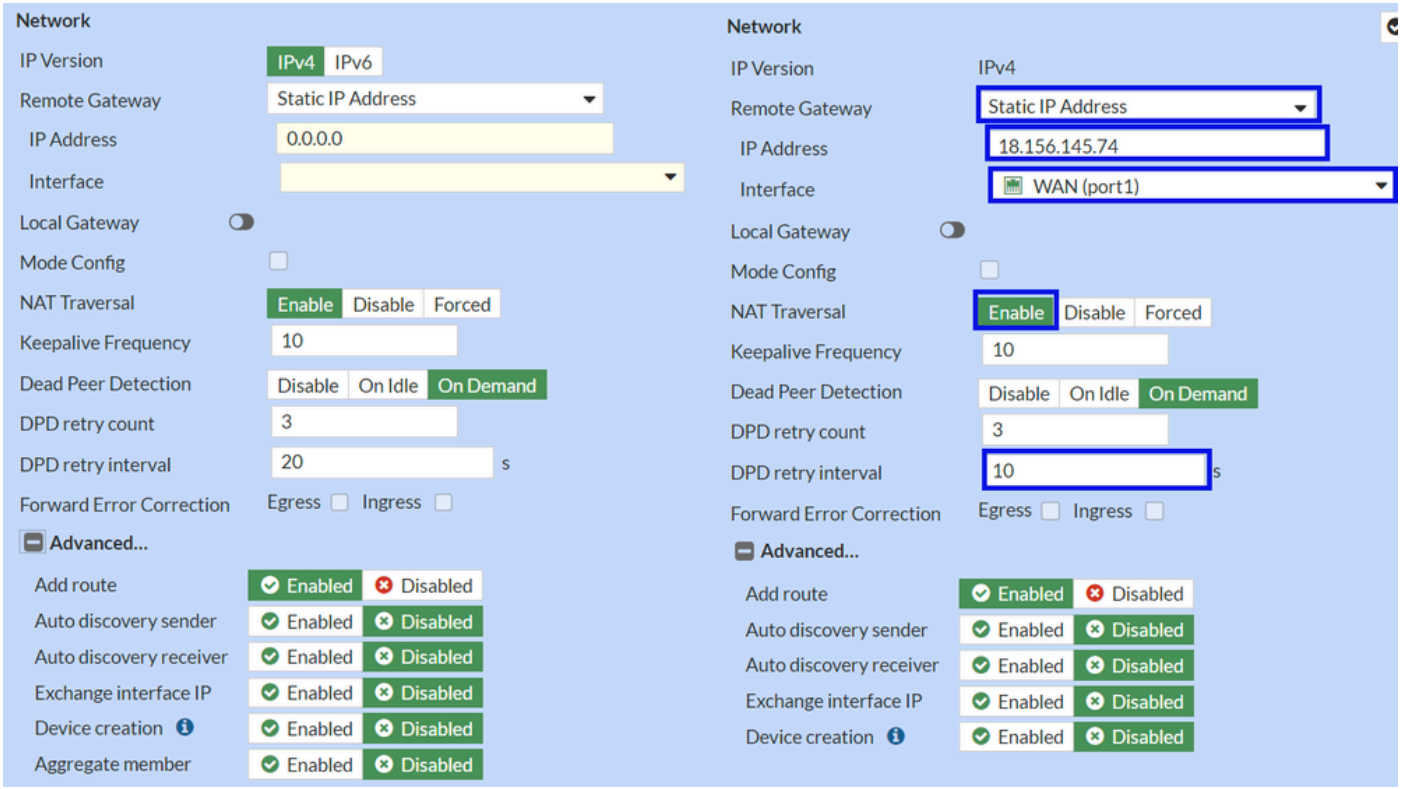


- Klicken Sie auf Custom , konfigurieren **Name** und auf **Next**.



Im nächsten Bild sehen Sie, wie Sie die Einstellungen für das **Network** Teil konfigurieren müssen.

Netzwerk



- Network

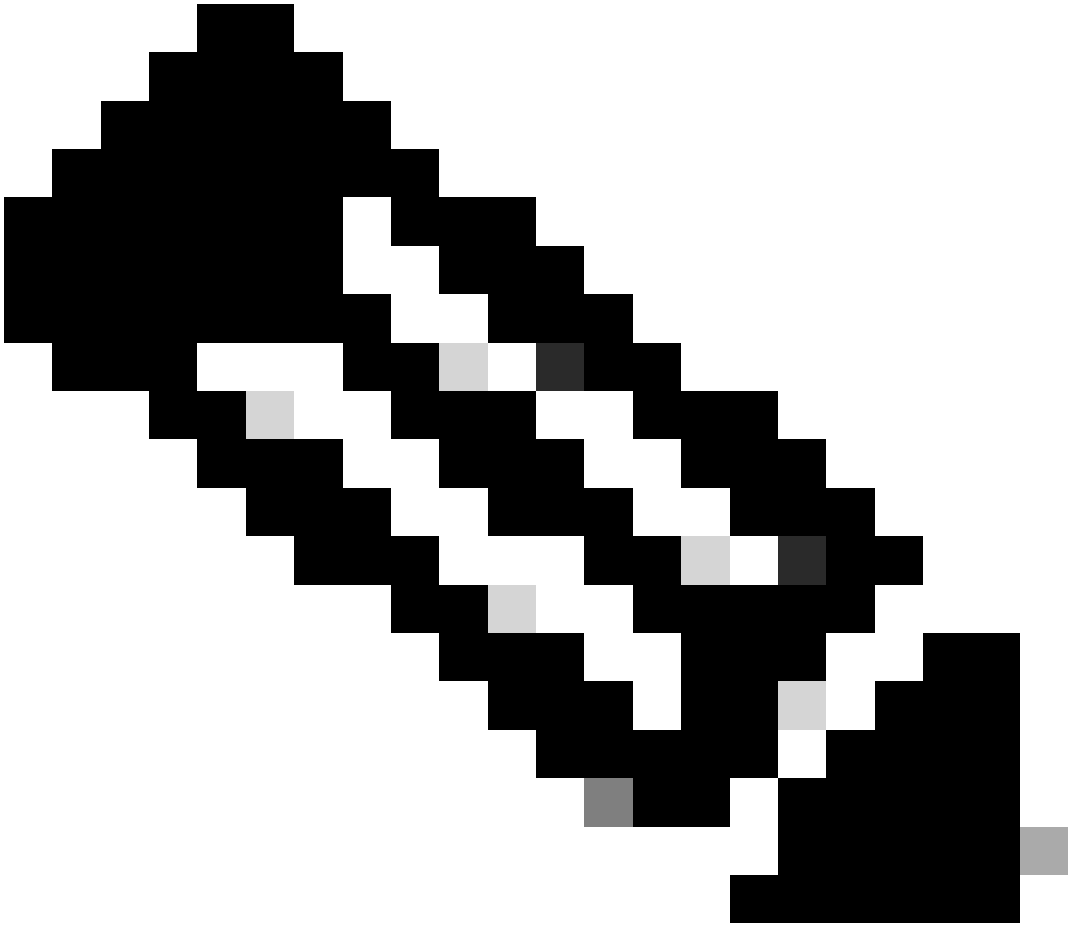
  - IP Version :IPv4

    - **Remote Gateway** :Statische IP-Adresse
    - IP Address: Verwenden Sie die IP-Adresse von Primary IP Datacenter IP Address,angegeben in Schritt Tunneldaten
    - **Interface** : Wählen Sie die WAN-Schnittstelle aus, die Sie für die Einrichtung des Tunnels vorgesehen haben.
    - **Local Gateway** : Als Standard deaktivieren
    - **Mode Config** : Als Standard deaktivieren
    - **NAT Traversal** : Aktivieren
    - **Keepalive Frequency** :10
    - Dead Peer Detection : On-Demand
    - **DPD retry count** :3
    - **DPD retry interval** :10
    - **Forward Error Correction** : Keines der Kontrollkästchen markieren.
    - **Advanced...**: Konfigurieren Sie es als Image.

Konfigurieren Sie jetzt IKE **Authentication**.

Authentifizierung

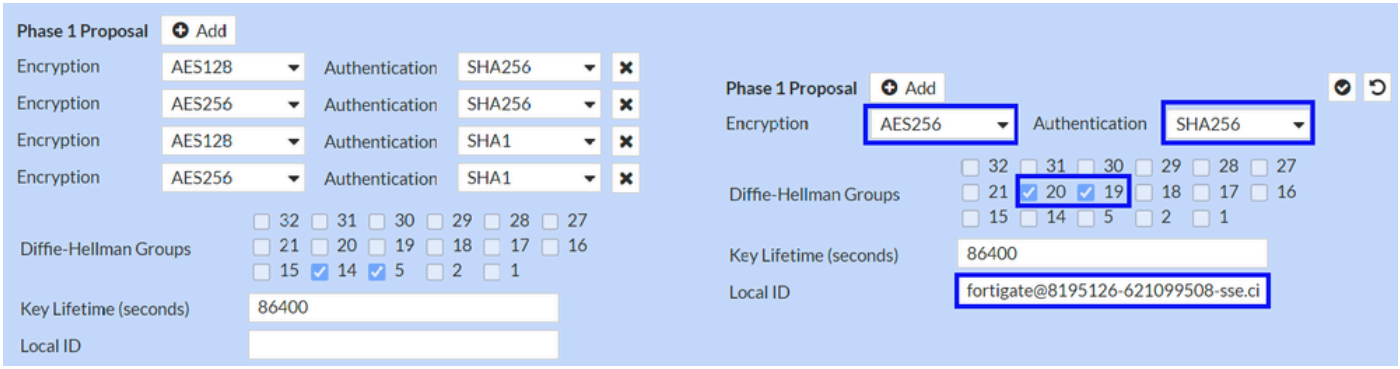
- **Authentication**
  - **Method** : Vorläufiger gemeinsamer Schlüssel als Standard
    - **Pre-shared Key** : Verwenden Sie die **Passphrase**angegebenen Tunneldaten
- **IKE**
  - Version : Wählen Sie Version 2.



Hinweis: Secure Access unterstützt nur IKEv2

Konfigurieren Sie nun die **Phase 1 Proposal**.

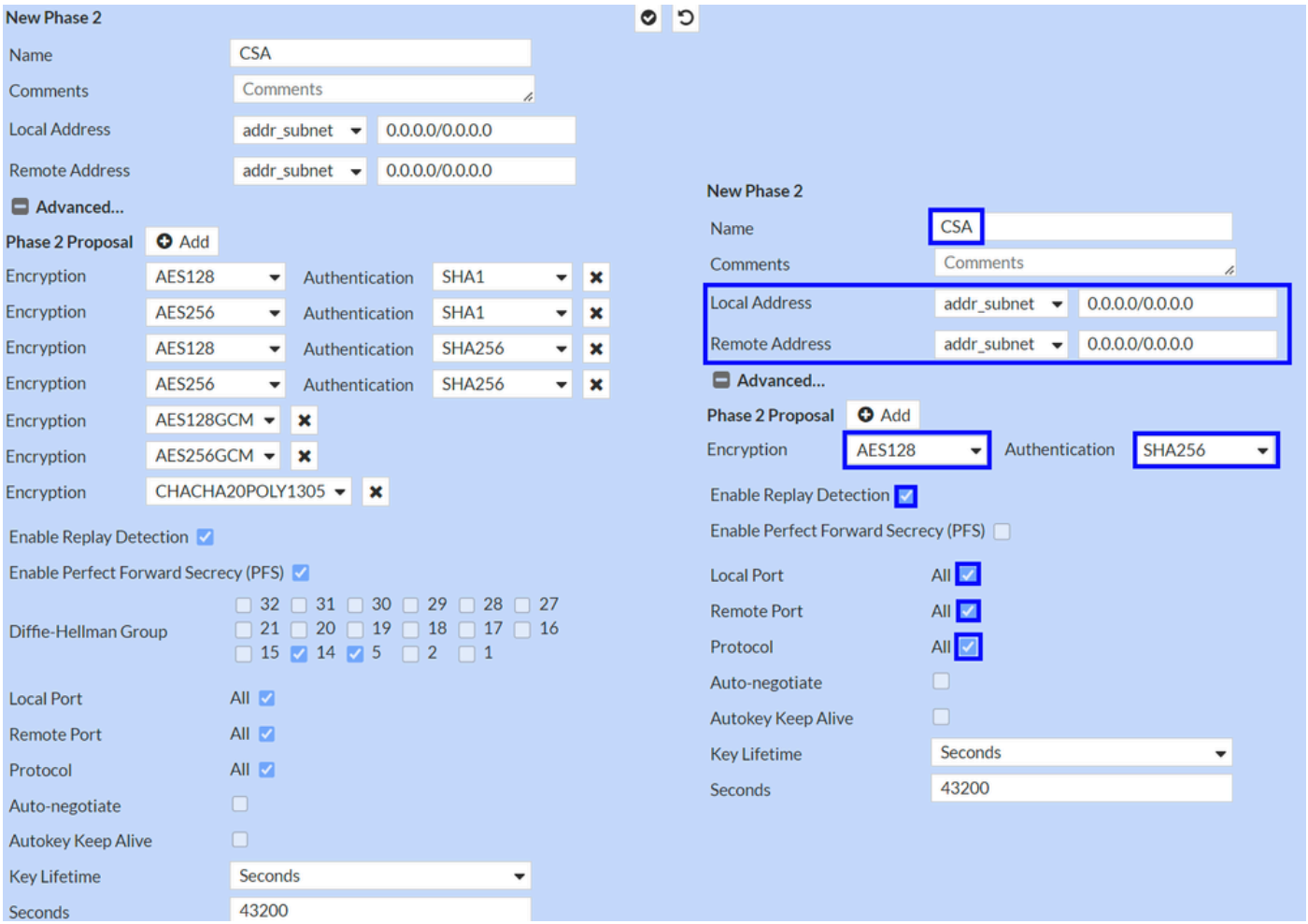
Angebot für Phase 1



- Phase 1 Proposal
    - Encryption : AES256 auswählen
        - Authentication : SHA256 auswählen
        - Diffie-Hellman Groups : Aktivieren Sie die Kontrollkästchen 19 und 20.
        - Key Lifetime (seconds) : 86400 als Standard
        - Local ID : Verwenden Sie die Primary Tunnel ID im Schritt Tunneldaten

Konfigurieren Sie nun die **Phase 2 Proposal**.

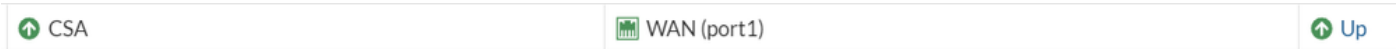
Angebot für Phase 2



- New Phase 2
  - **Name** : Voreingestellt (wird vom Namen Ihres VPNs übernommen)
    - **Local Address** : Let as default (0.0.0.0/0.0.0.0)
    - **Remote Address** : Let as default (0.0.0.0/0.0.0.0)
- Advanced
  - **Encryption** : AES128 auswählen
    - **Authentication** : SHA256 auswählen
    - **Enable Replay Detection** : Als Standard zulassen (Aktiviert)
    - **Enable Perfect Forward Secrecy (PFS)** : Deaktivieren Sie das Kontrollkästchen.
    - **Local Port** : Als Standard zulassen (Aktiviert)

- **Remote Port**: Als Standard zulassen (Aktiviert)
- **Protocol** : Als Standard zulassen (Aktiviert)
- **Auto-negotiate** : Als Standard zulassen (Nicht markiert)
- **Autokey Keep Alive** : Als Standard zulassen (Nicht markiert)
- **Key Lifetime** : Als Standard zulassen (Sekunden)
- **Seconds** : Voreingestellt (43200)

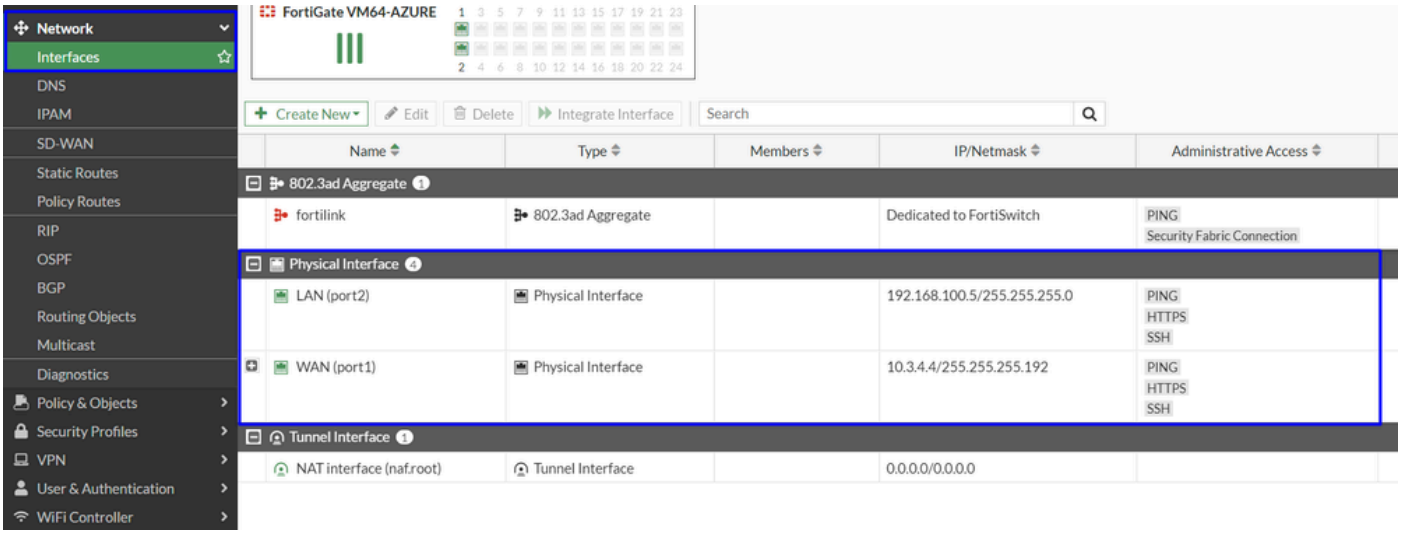
Klicken Sie anschließend auf OK. Nach einigen Minuten sehen Sie, dass das VPN mit Secure Access eingerichtet wurde, und Sie können mit dem nächsten Schritt fortfahren. **Configure the Tunnel Interface.**



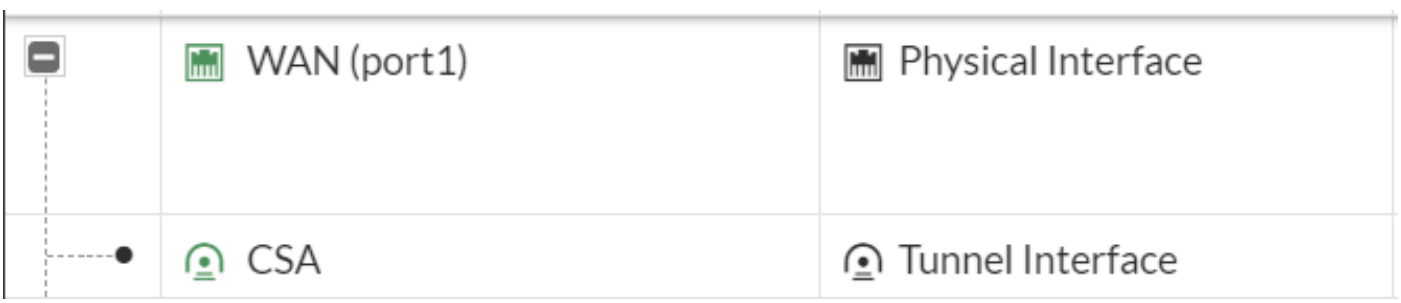
Konfigurieren der Tunnelschnittstelle

Nachdem der Tunnel erstellt wurde, stellen Sie fest, dass sich hinter dem Port eine neue Schnittstelle befindet, die Sie als WAN-Schnittstelle für die Kommunikation mit Secure Access verwenden.

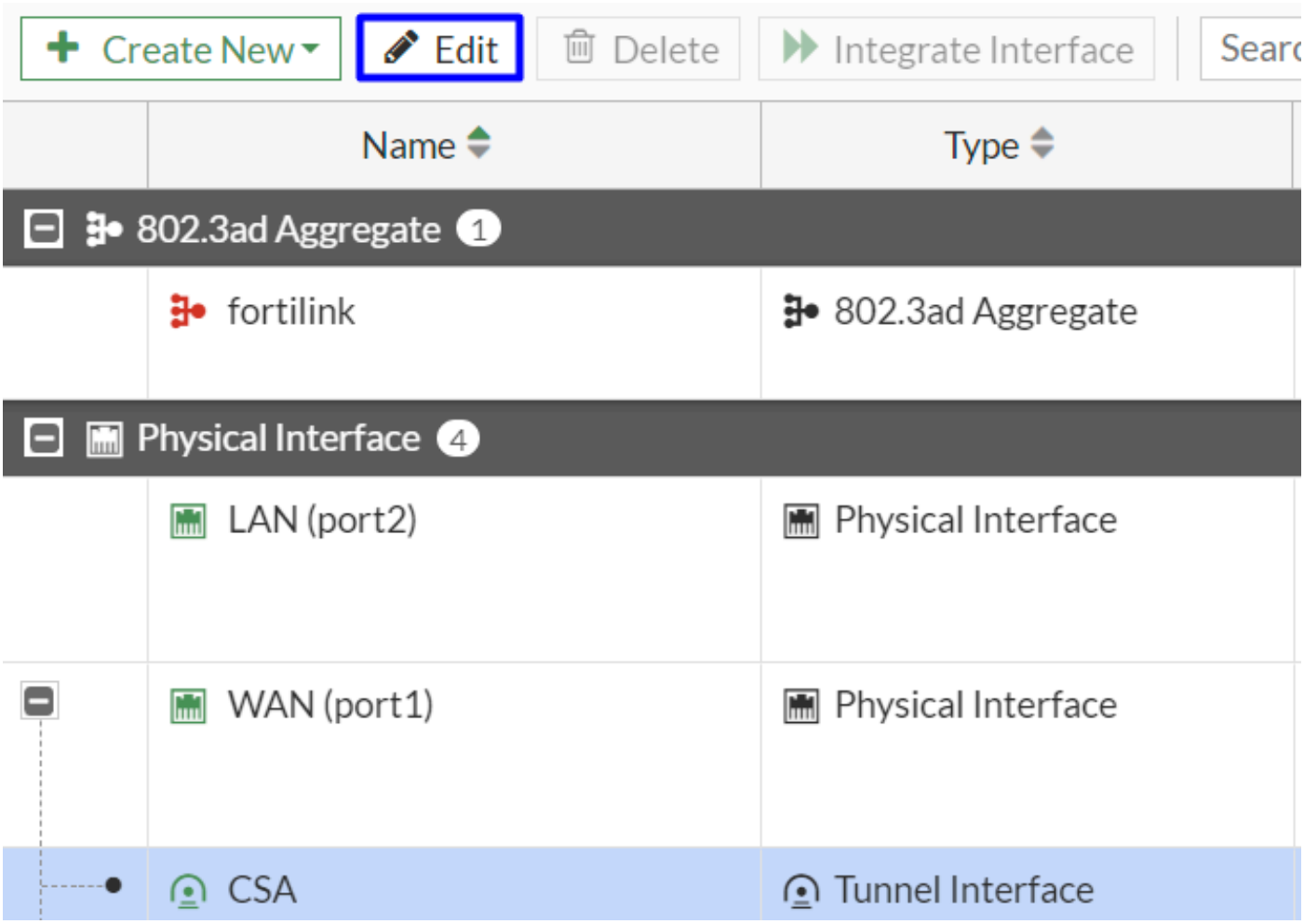
Um dies zu überprüfen, navigieren Sie bitte zu **Network > Interfaces**.



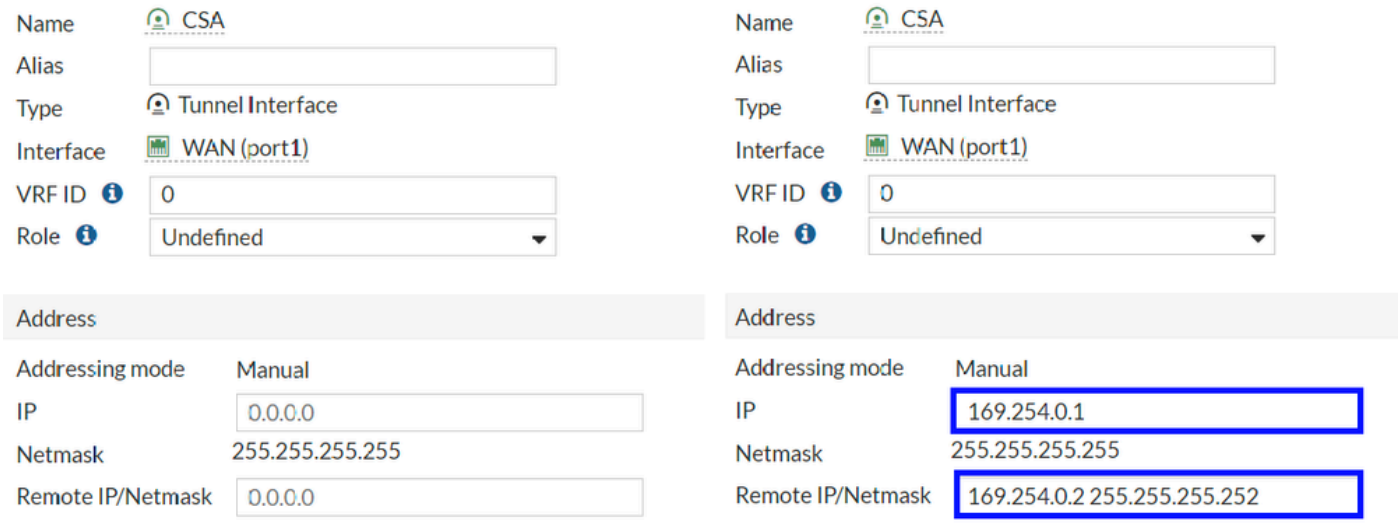
Erweitern Sie den Port, den Sie für die Kommunikation mit Secure Access verwenden, in diesem Fall die **WAN** Schnittstelle.



- Klicken Sie auf Ihre **Tunnel Interface** und anschließend auf **Edit**



- Sie haben das nächste zu konfigurierende Image.

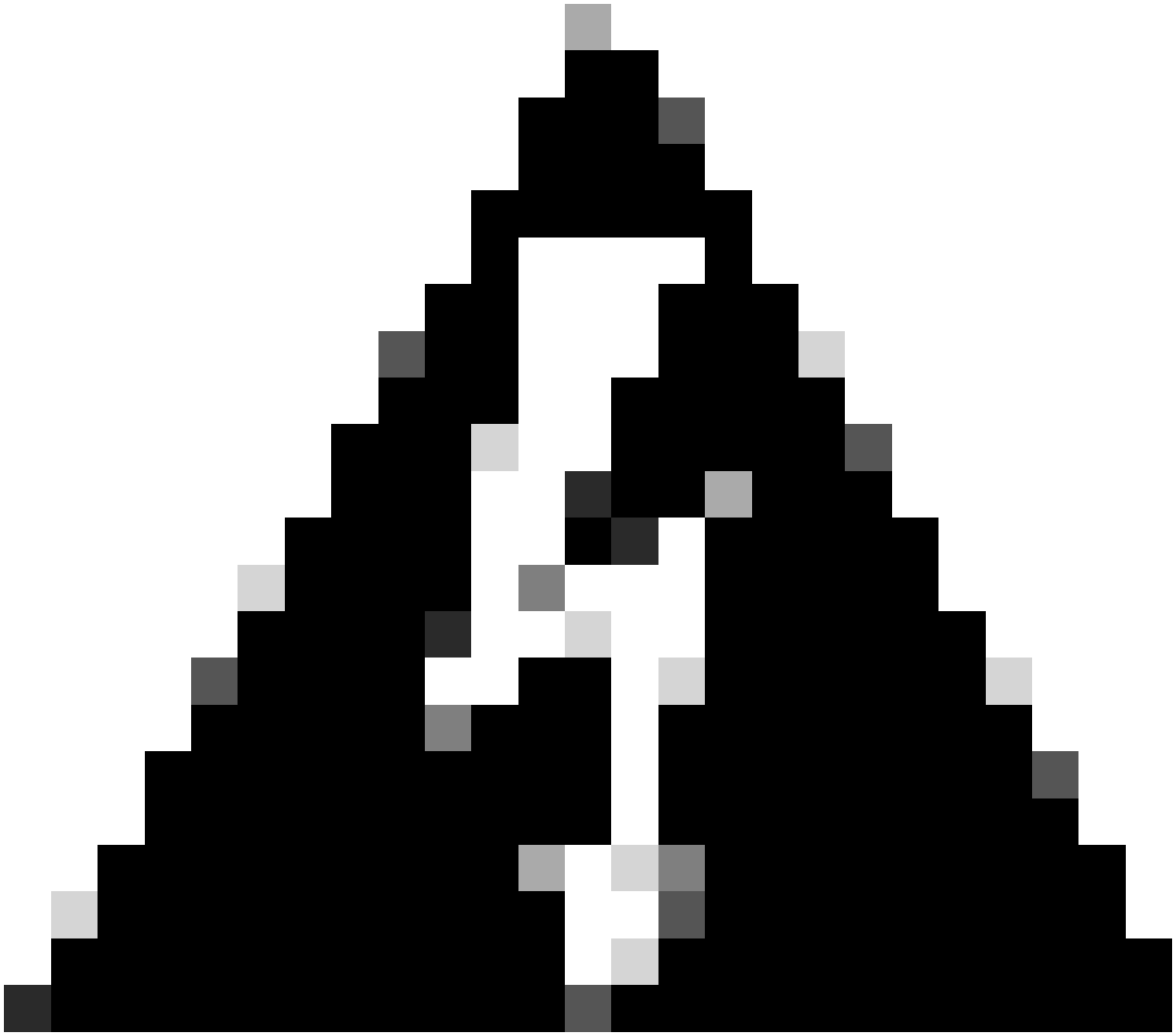


- Interface Configuration

- IP : Konfigurieren Sie eine nicht routbare IP-Adresse, die nicht im Netzwerk vorhanden ist (169.254.0.1).

- Remote IP/Netmask : Konfigurieren Sie die Remote-IP als die nächste IP-Adresse Ihrer Schnittstellen-IP und mit der Netzmaske 30 (169.254.0.2 255.255.255.252).

Speichern Sie **OK** die Konfiguration, und fahren Sie mit dem nächsten Schritt (Configure Policy Route Origin-Based Routing) fort.

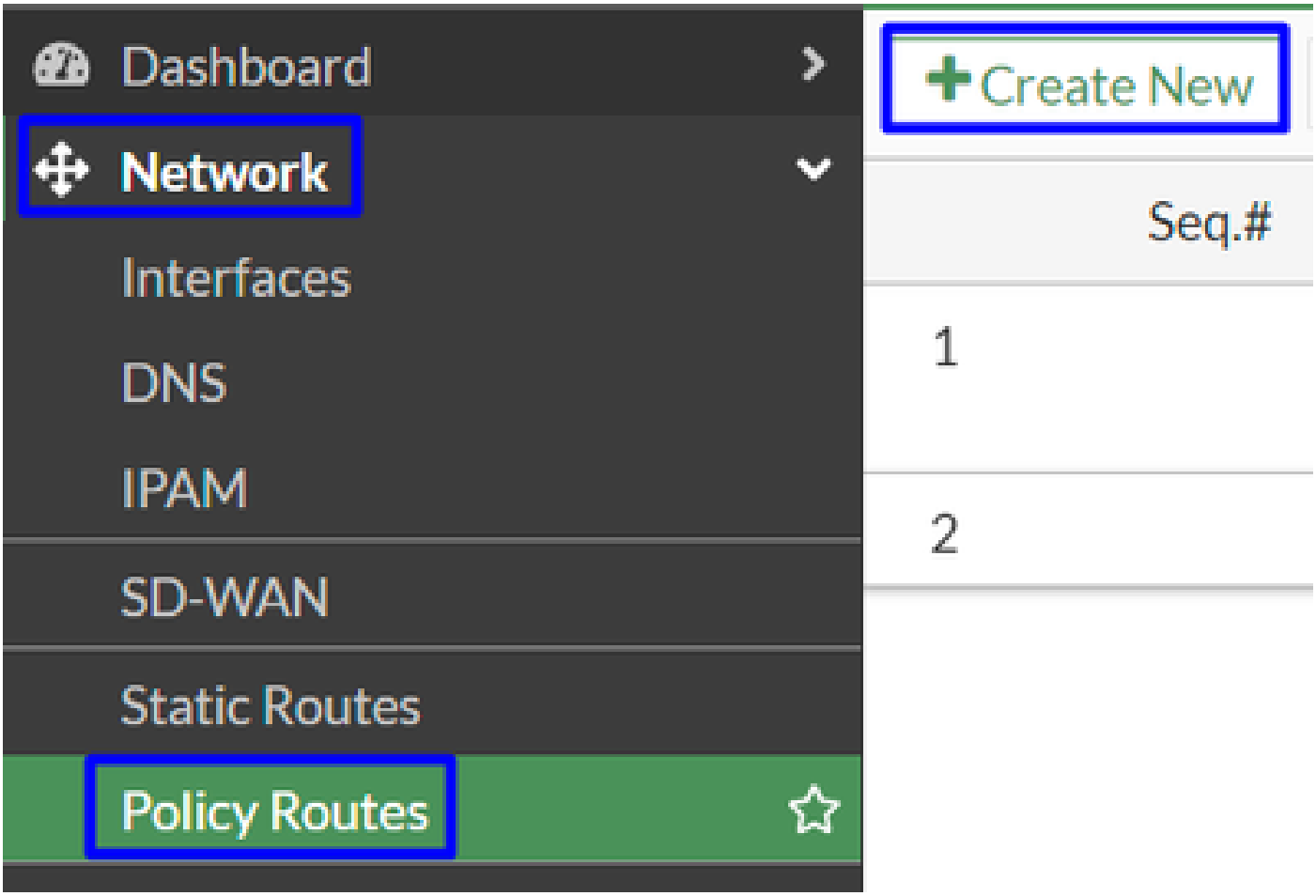


Warnung: Nach diesem Teil müssen Sie die Firewall-Richtlinien auf Ihrem FortiGate konfigurieren, um den Datenverkehr von Ihrem Gerät zu sicherem Zugriff und von sicherem Zugriff zu den Netzwerken, die Sie den Datenverkehr routen möchten, zuzulassen oder zuzulassen.

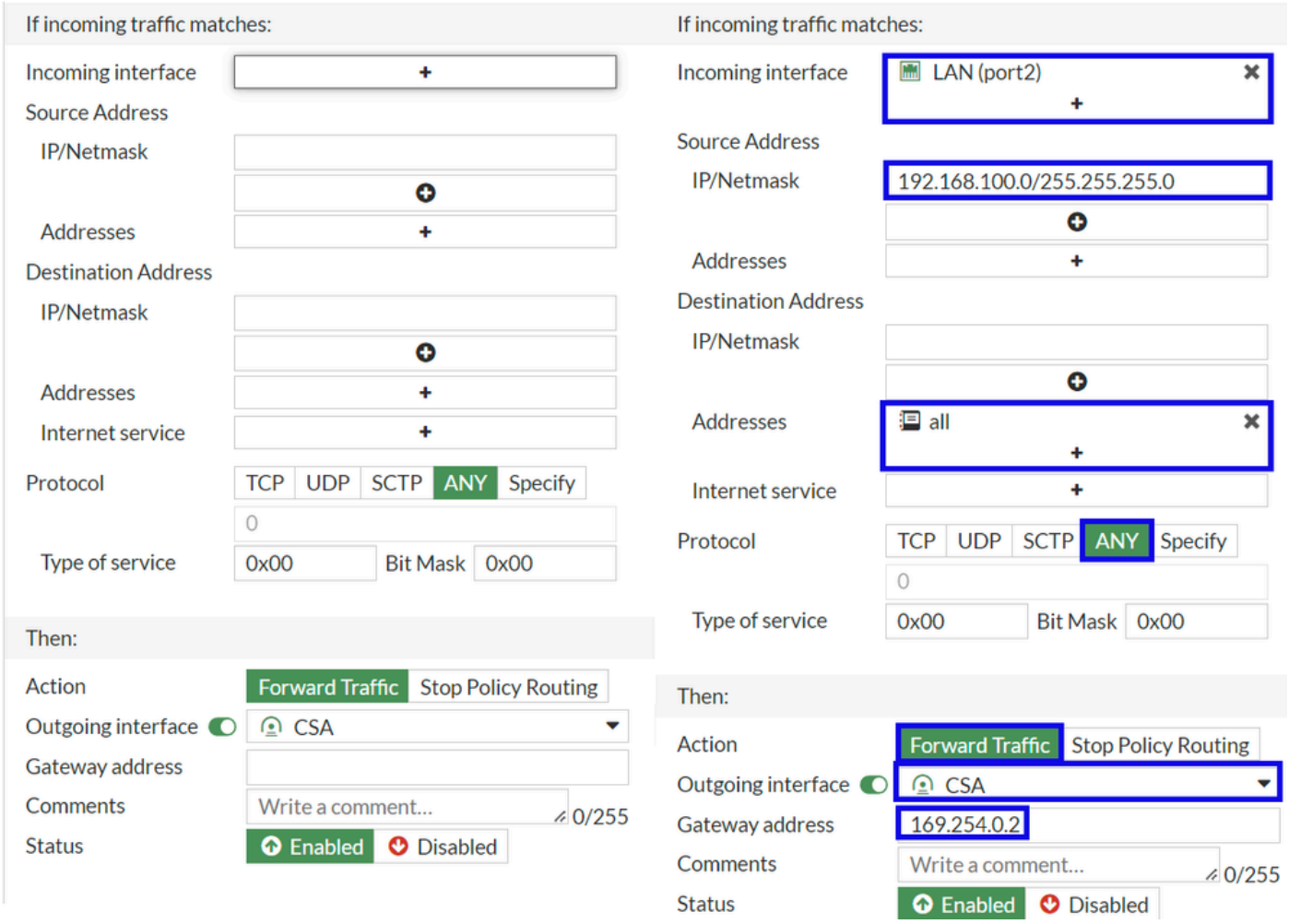
Policy-Route konfigurieren

An diesem Punkt ist Ihr VPN so konfiguriert und eingerichtet, dass Sie sicheren Zugriff haben. Jetzt müssen Sie den Datenverkehr auf sicheren Zugriff umleiten, um Ihren Datenverkehr oder den Zugriff auf Ihre privaten Anwendungen hinter Ihrer FortiGate-Firewall zu schützen.

- Navigieren Sie zu Network > Policy Routes



- Konfigurieren der Richtlinie



- If Incoming traffic matches

  - Incoming Interface : Wählen Sie die Schnittstelle aus, von der aus Sie den Datenverkehr auf den sicheren Zugriff (Ursprung des Datenverkehrs) umleiten möchten.

- Source Address

  - IP/Netmask : Verwenden Sie diese Option, wenn Sie nur ein Subnetz einer Schnittstelle routen

    • Addresses : Verwenden Sie diese Option, wenn das Objekt erstellt wurde und die Quelle des Datenverkehrs von mehreren Schnittstellen und mehreren Subnetzen stammt.

- Destination Addresses

- Addresses: Auswahl all
    - Protocol: Auswahl **ANY**

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

- Outgoing Interface : Wählen Sie die Tunnelschnittstelle aus, die Sie im Schritt Configure Tunnel Interface geändert haben.
- Gateway Address: Konfigurieren Sie die Remote-IP-Adresse, die für den Schritt konfiguriert wurde, RemoteIPNetmask
- Status : Aktivieren auswählen

Klicken Sie hier, **OK** um die Konfiguration zu speichern. Jetzt können Sie überprüfen, ob der Geräteverkehr zu "Sicherer Zugriff" umgeleitet wurde.

Überprüfung

Um zu überprüfen, ob der Datenverkehr Ihres Computers zu Secure Access umgeleitet wurde, haben Sie zwei Möglichkeiten: Sie können im Internet nach Ihrer öffentlichen IP suchen oder den nächsten Befehl mit curl ausführen:

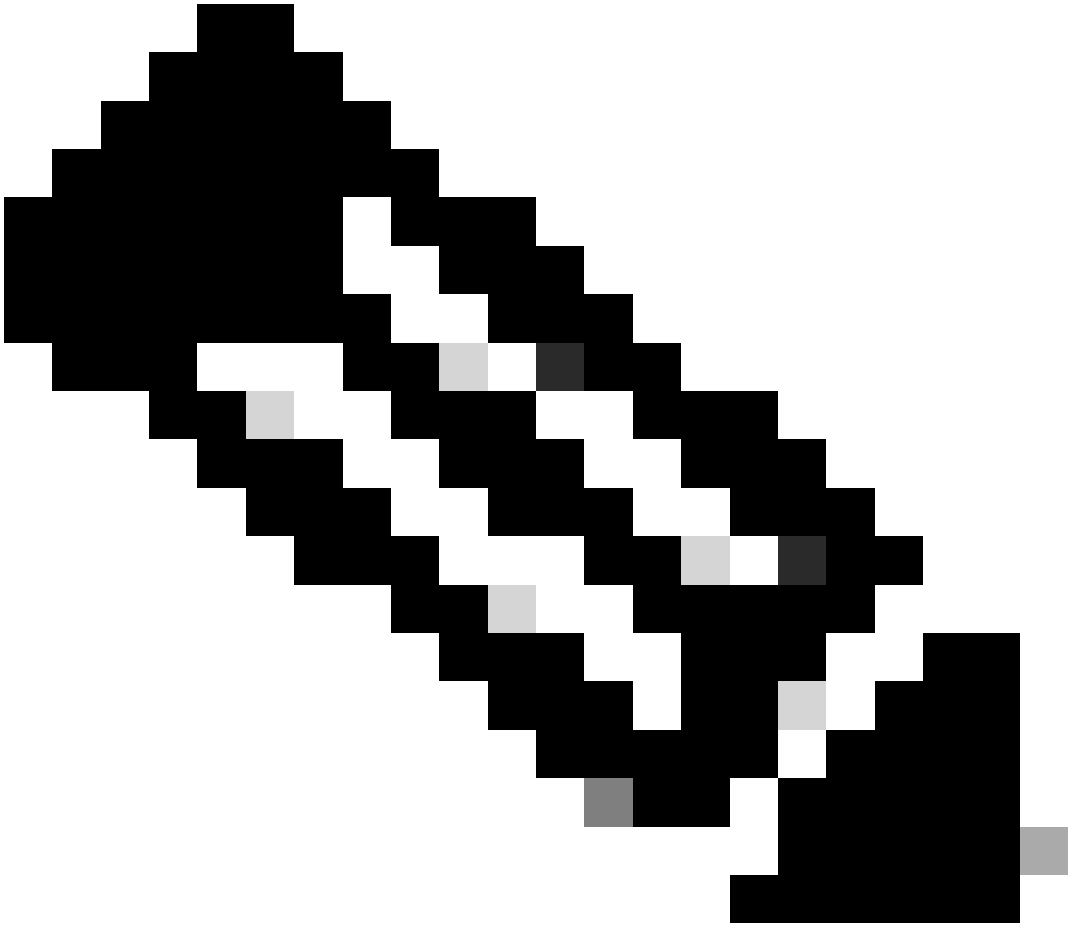
<#root>

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

Der öffentliche Bereich, von dem aus Sie den Datenverkehr sehen können, stammt von:

Min Host:151.186.176.1

Max Host :151.186.207.254



Hinweis: Änderungen an diesen IPs vorbehalten. Cisco wird diesen Bereich demnächst wahrscheinlich erweitern.

Wenn Sie die Änderung Ihrer öffentlichen IP sehen, bedeutet dies, dass Sie durch sicheren Zugriff geschützt sind. Jetzt können Sie Ihre private Anwendung auf dem Dashboard für sicheren Zugriff konfigurieren, um über VPNaaS oder ZTNA auf Ihre Anwendungen zuzugreifen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.