

# Konfigurieren von sicherem Zugriff mit Fortigate Firewall

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren des VPN für sicheren Zugriff](#)

[Tunneldaten](#)

[Konfigurieren des VPN-Standorts auf dem Fortigate](#)

[Netzwerk](#)

[Authentifizierung](#)

[Angebot für Phase 1](#)

[Angebot für Phase 2](#)

[Konfigurieren der Tunnelschnittstelle](#)

[Policy-Route konfigurieren](#)

[Überprüfung](#)

---

## 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

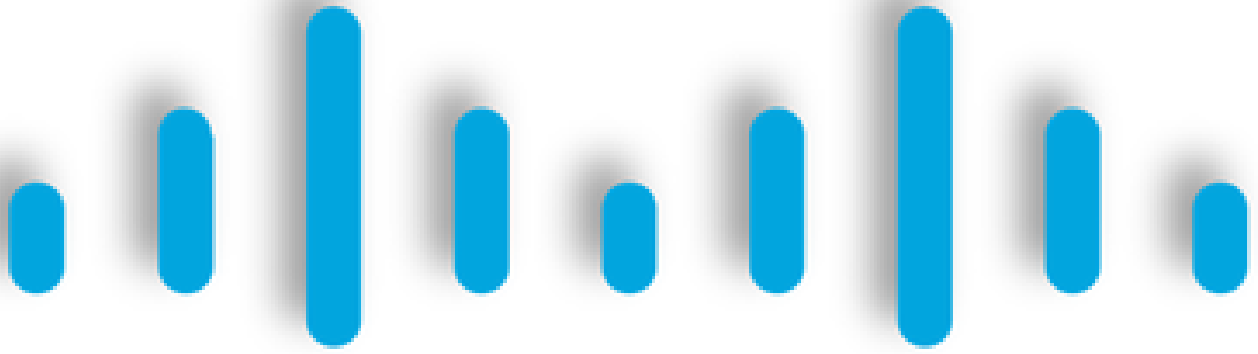
## Verwendete Komponenten

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

## Secure

## Access

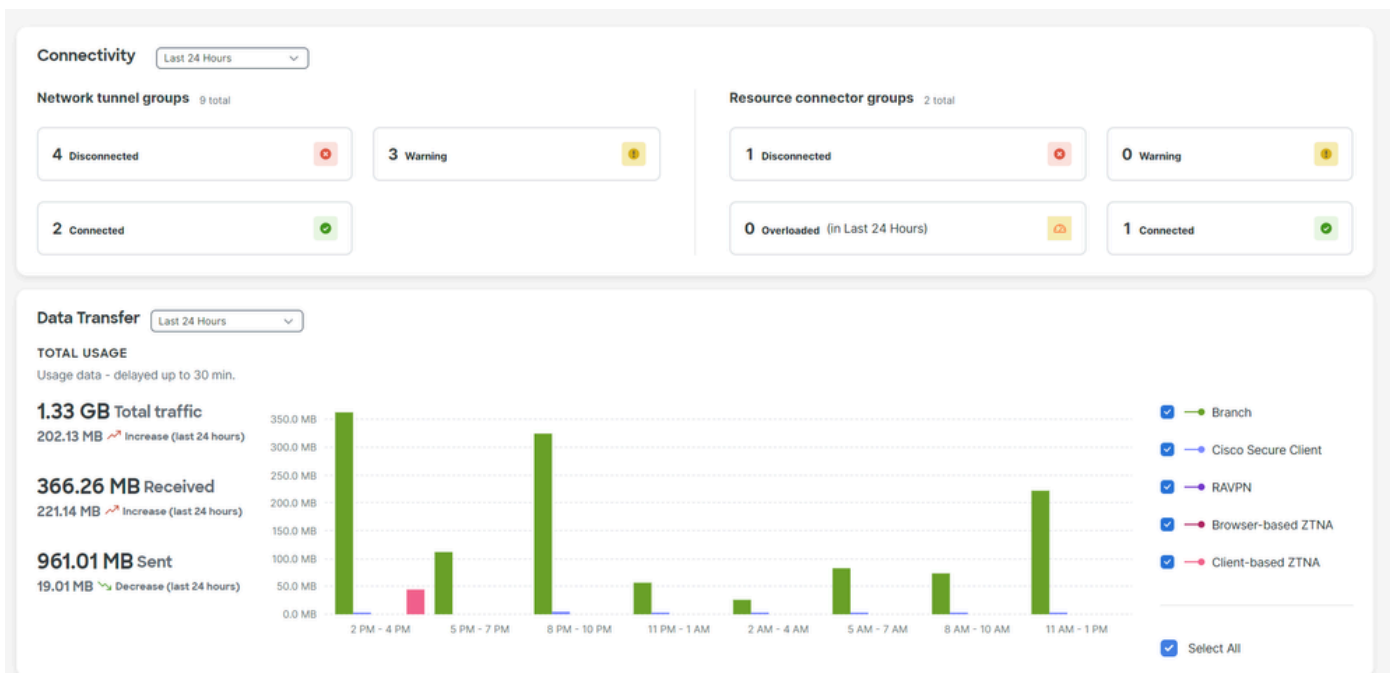
# FORTINET®

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.

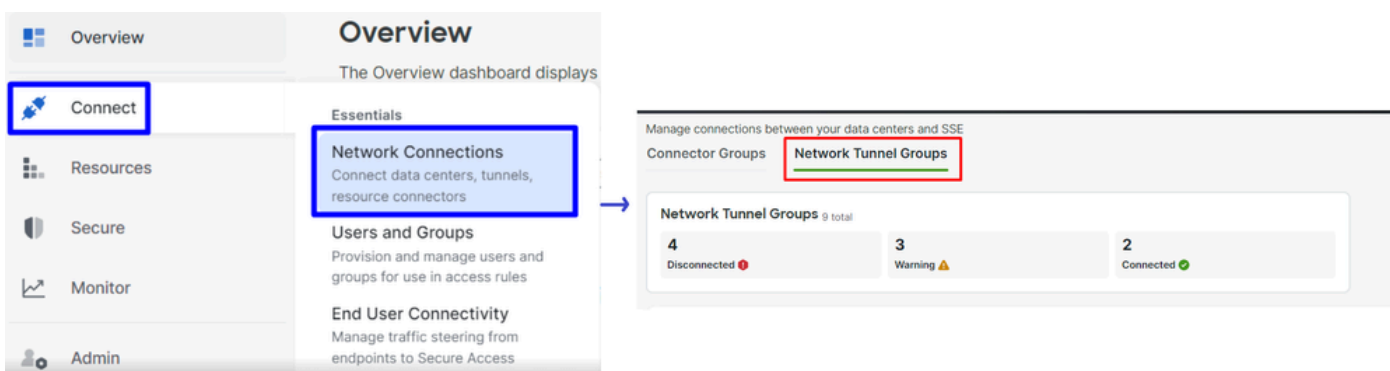
### Konfigurieren

# Konfigurieren des VPN für sicheren Zugriff

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



- Klicken Sie [Connect](#) > [Network Connections](#) > [Network Tunnel Groups](#)



- Klicken Sie unter Network Tunnel Groups auf + 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



- 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

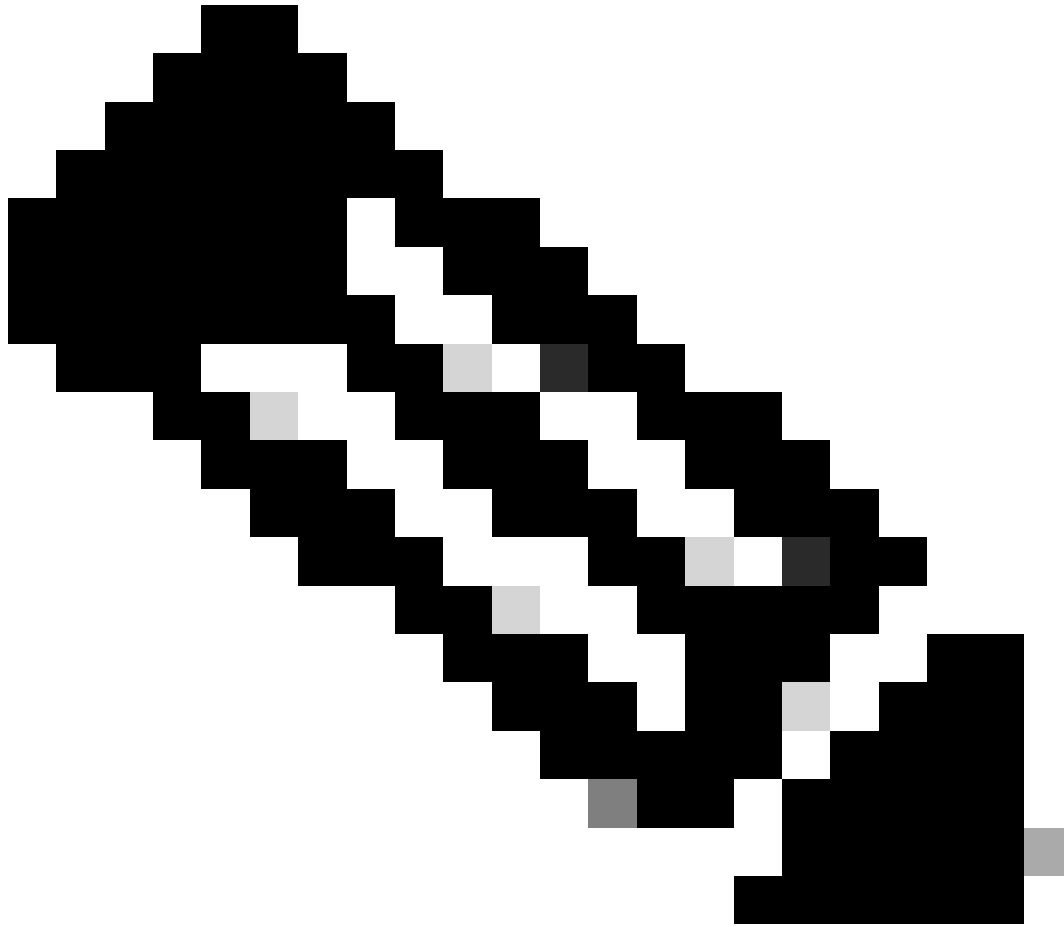
Europe (Germany)

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

- 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

@<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

- 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**

- 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.

Add

192.168.100.0/24 X

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.



Cancel

Back






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.**

Tunneln

## 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.

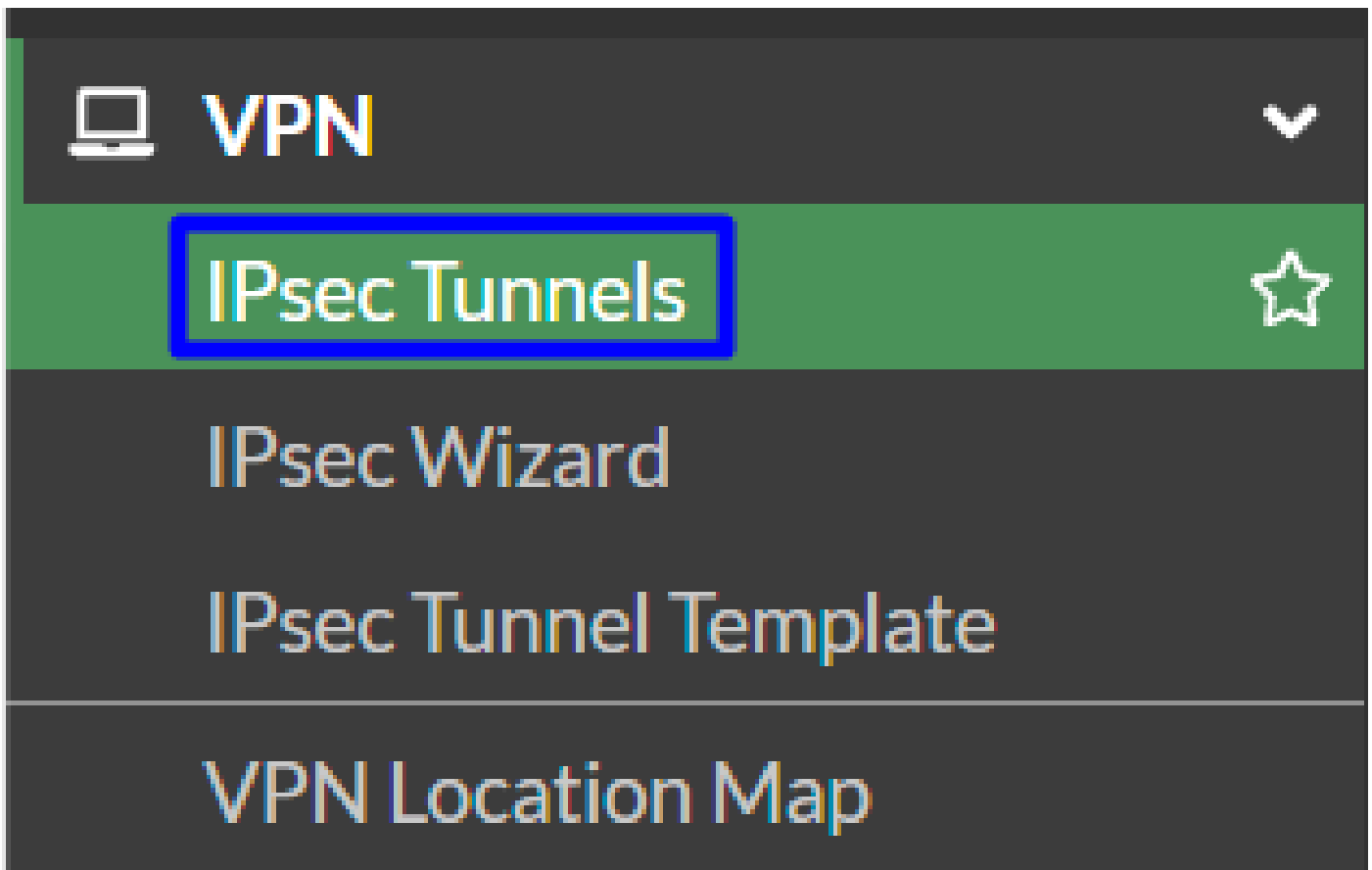
<b>Primary Tunnel ID:</b>	@	-sse.cisco.com	
<b>Primary Data Center IP Address:</b>	18.156.145.74		
<b>Secondary Tunnel ID:</b>	@	-sse.cisco.com	
<b>Secondary Data Center IP Address:</b>	3.120.45.23		
<b>Passphrase:</b>		CP	

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](#)

+ Create new ▾

IPsec Tunnel

IPsec Aggregate

Custom 2

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

#### 1 VPN Setup

Name 2 Cisco Secure 1  
Template type Site to Site Hub-and-Spoke Remote Access Custom

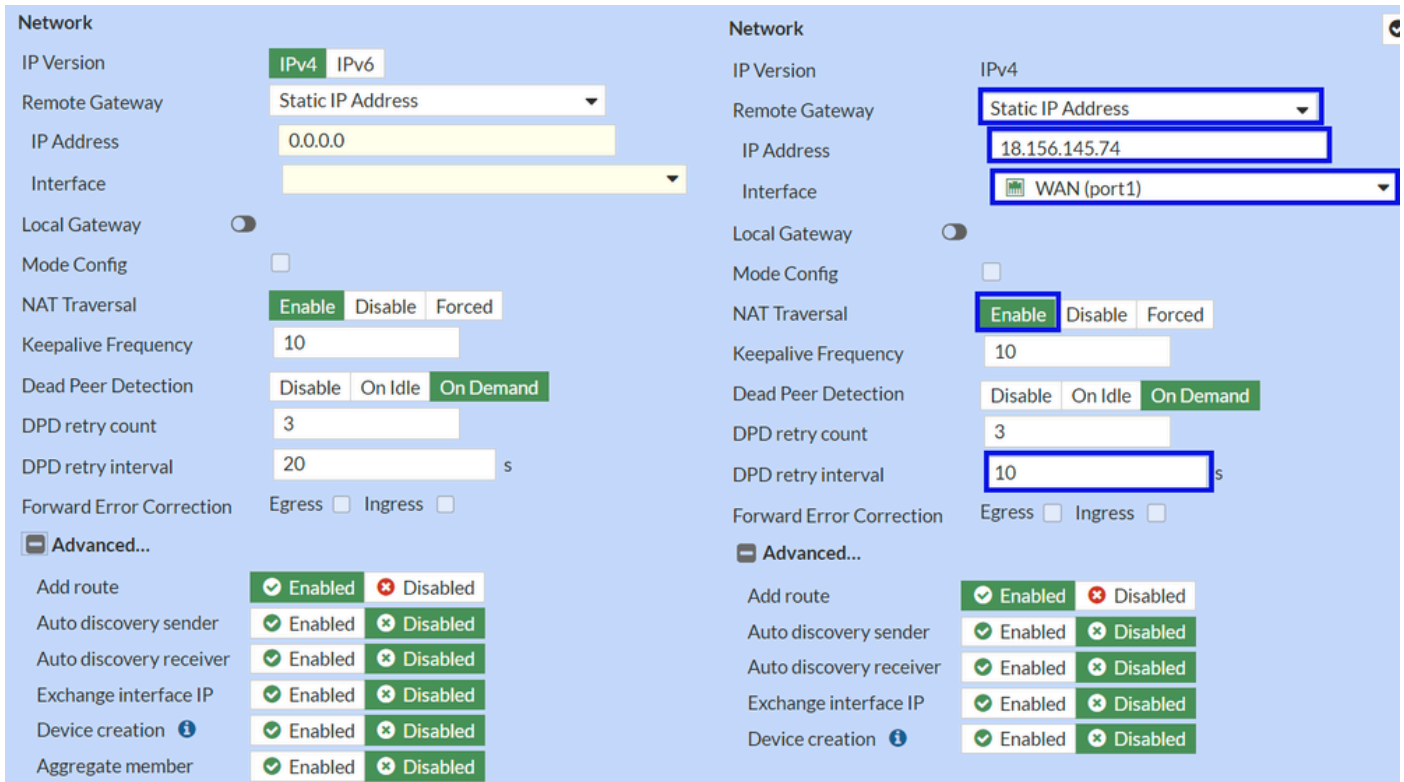
< Back

3  
Next >

Cancel

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

<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)		

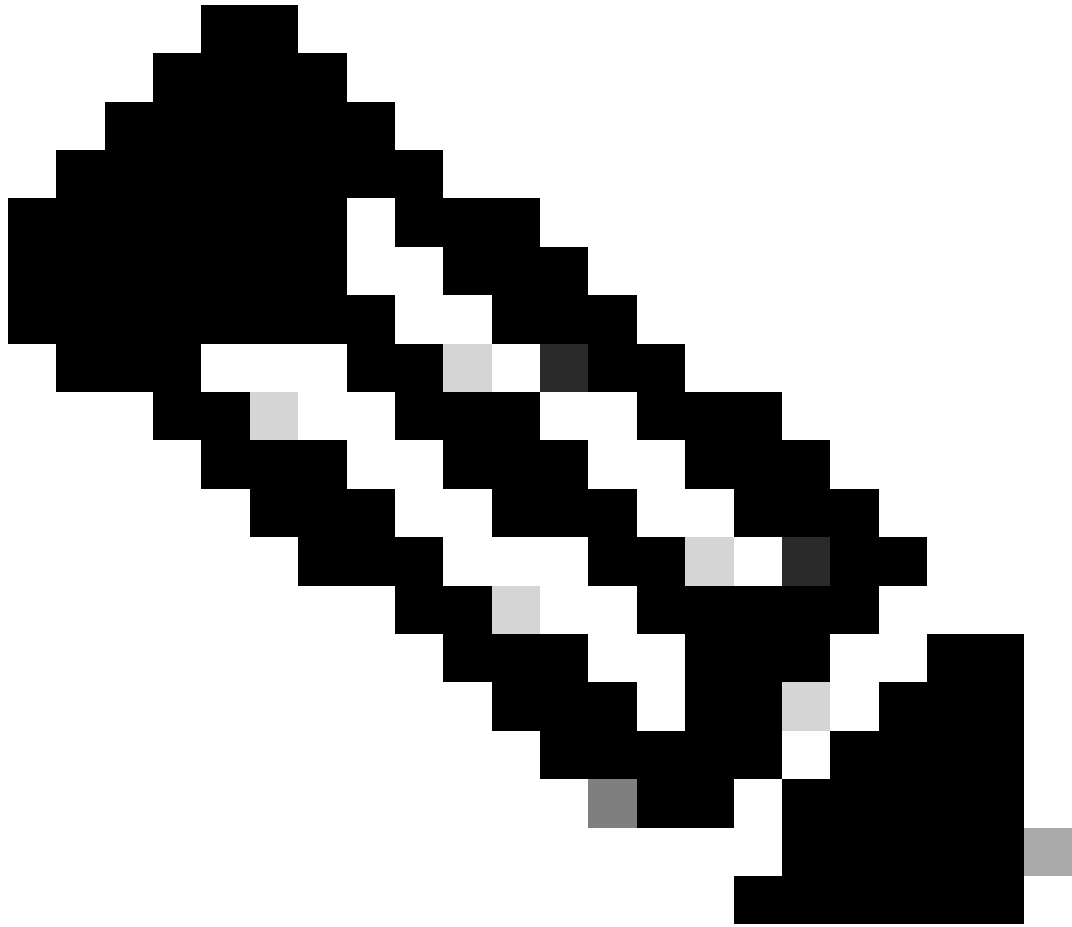
- **Authentication**

- **Method** : 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

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, and Key Lifetime set to 86400 seconds. The Local ID is set to fortigate@8195126-621099508-sse.ci.

- 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: 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	SHA1	X
Encryption	AES256	Authentication	SHA1	X
Encryption	AES128	Authentication	SHA256	X
Encryption	AES256	Authentication	SHA256	X
Encryption	AES128GCM			X
Encryption	AES256GCM			X
Encryption	CHACHA20POLY1305			X

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group:  32  31  30  29  28  27  
 21  20  19  18  17  16  
 15  14  5  2  1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds  
43200

**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:

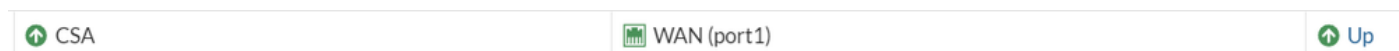
Autokey Keep Alive:

Key Lifetime: Seconds  
43200

- New Phase 2
  - **Name** : 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)

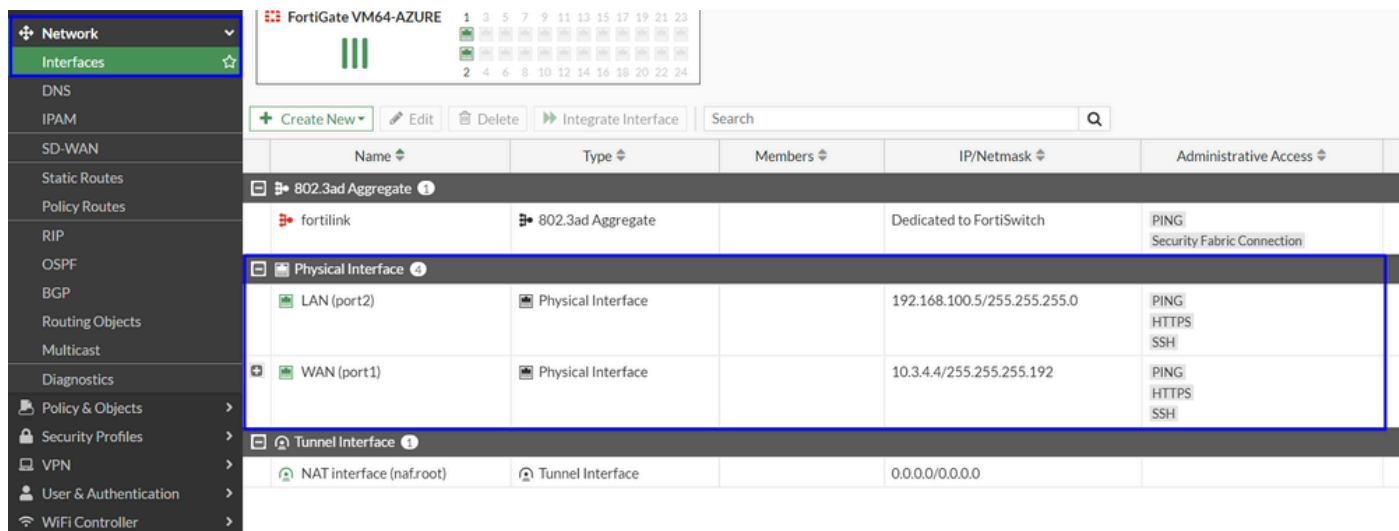
Klicken Sie anschließend auf OK. Nach einigen Minuten sehen Sie, dass das VPN mit Secure Access eingerichtet wurde, und Sie können mit dem nächsten Schritt fortfahren. **Configure the Tunnel Interface.**



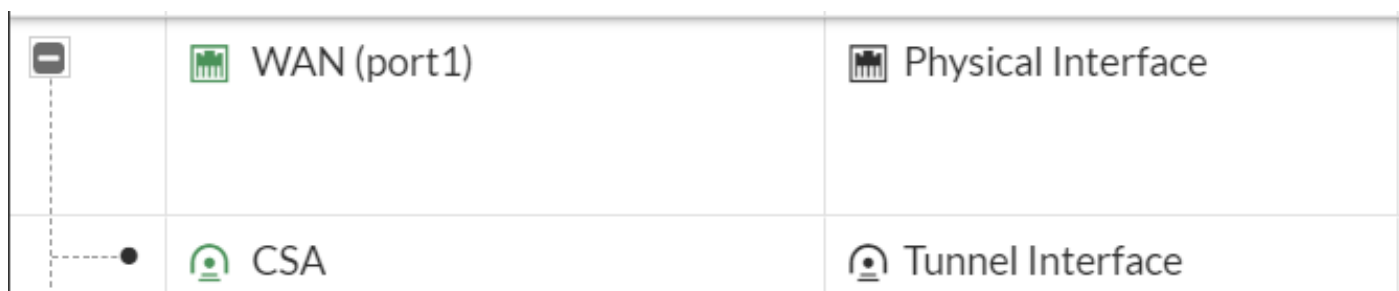
Konfigurieren der Tunnelschnittstelle

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**

+ Create New ▾		<b>Edit</b>	🗑 Delete	▶ Integrate Interface	Search
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			

- Sie haben das nächste zu konfigurierende Image.

Name CSA

Alias

Type Tunnel Interface

Interface WAN (port1)

VRF ID ⓘ

Role ⓘ

Name CSA

Alias

Type Tunnel Interface

Interface WAN (port1)

VRF ID ⓘ

Role ⓘ

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 : 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.

---



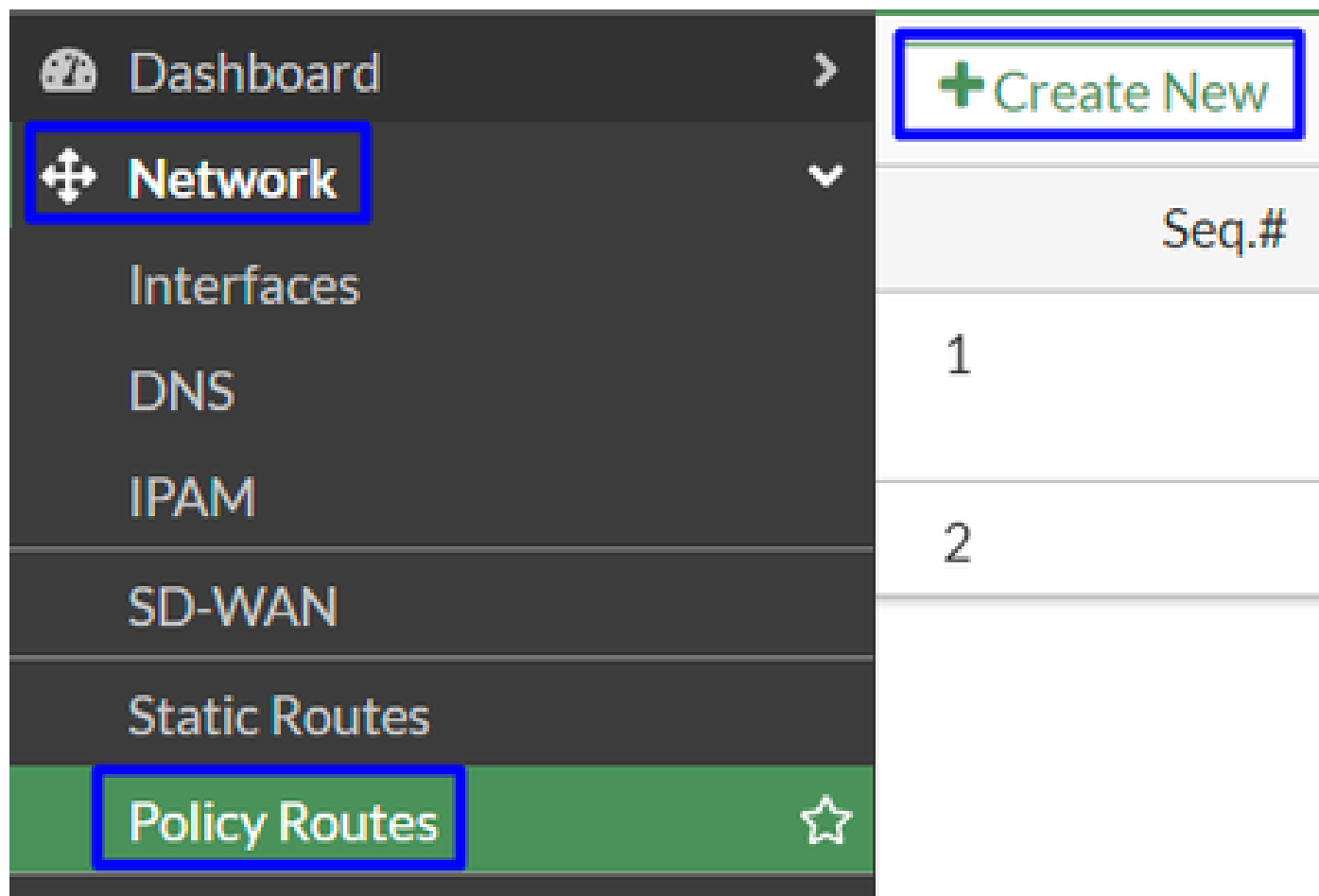
**Warnung:** Nach diesem Teil müssen Sie die Firewall-Richtlinien auf Ihrem FortiGate konfigurieren, um den Datenverkehr von Ihrem Gerät zu sicherem Zugriff und von sicherem Zugriff zu den Netzwerken, die Sie den Datenverkehr routen möchten, zuzulassen oder zuzulassen.

---

## 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



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 table with a header row containing a green '+ Create New' button and a 'Seq.#' column. The table contains two rows with the sequence numbers 1 and 2.

Seq.#
1
2

- Konfigurieren der Richtlinie

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 : 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:

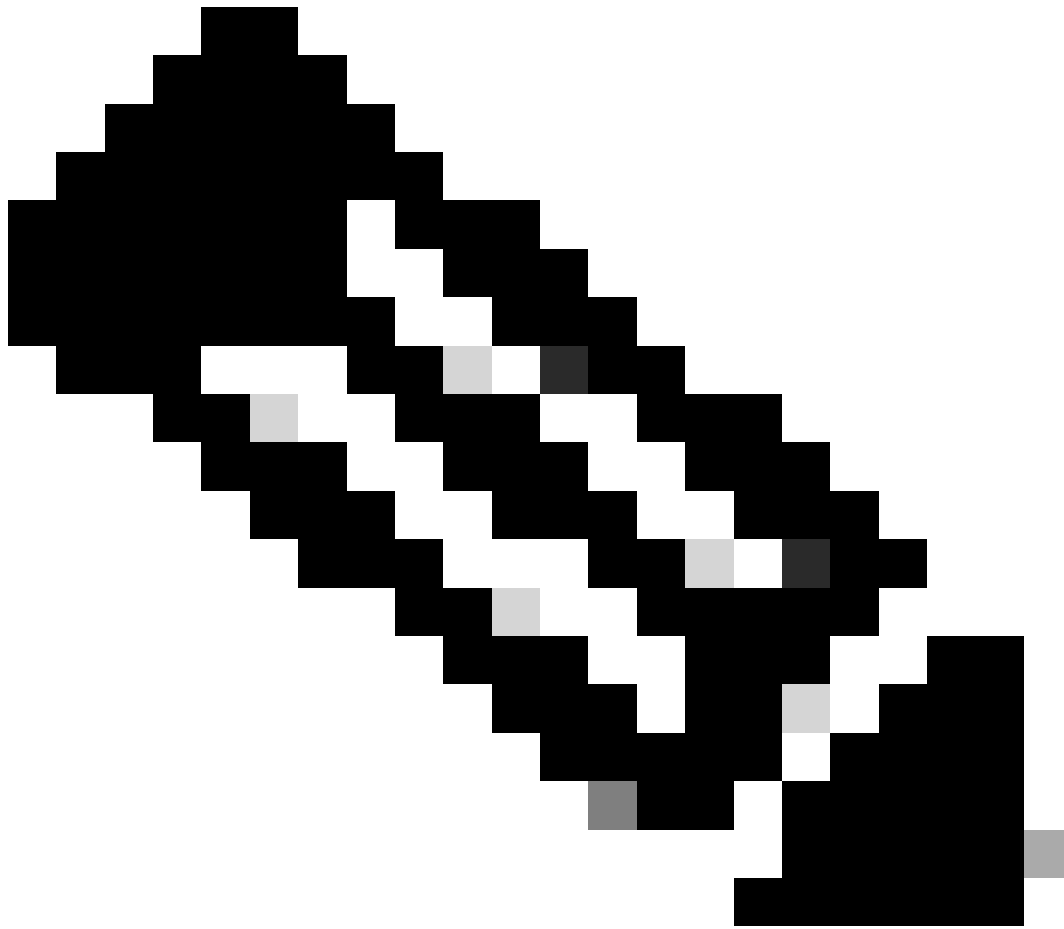
<#root>

```
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.