

Configure Secure Access with Fortigate Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configure the VPN on Secure Access](#)

[Tunnel Data](#)

[Configure the VPN Site to Site on Fortigate](#)

[Network](#)

[Authentication](#)

[Phase 1 Proposal](#)

[Phase 2 Proposal](#)

[Configure the Tunnel Interface](#)

[Configure Policy Route](#)

[Verify](#)

Introduction

This document describes how to configure Secure Access with Fortigate Firewall.

Prerequisites

- [Configure User Provisioning](#)
- [ZTNA SSO Authentication Configuration](#)
- [Configure Remote Access VPN Secure Access](#)

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

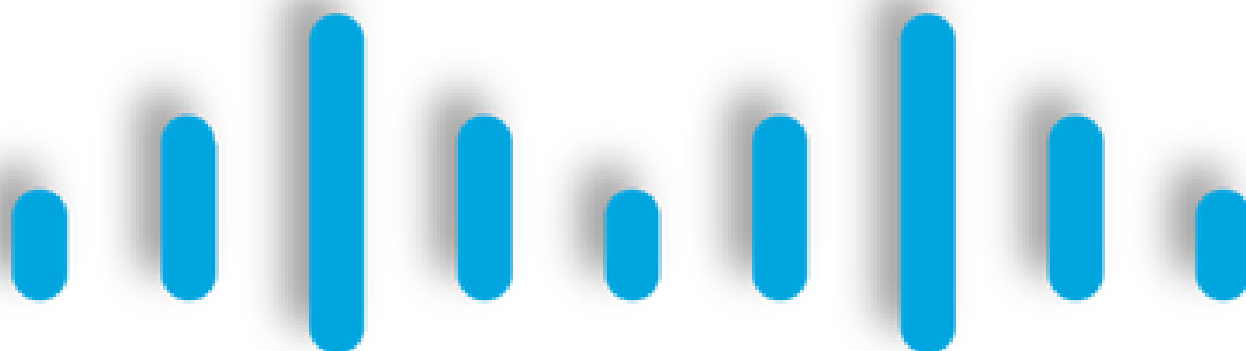
The information in this document is based on:

- Fortigate 7.4.x Version Firewall
- Secure Access

- Cisco Secure Client - VPN
- Cisco Secure Client - 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information



CISCO

Secure

Access

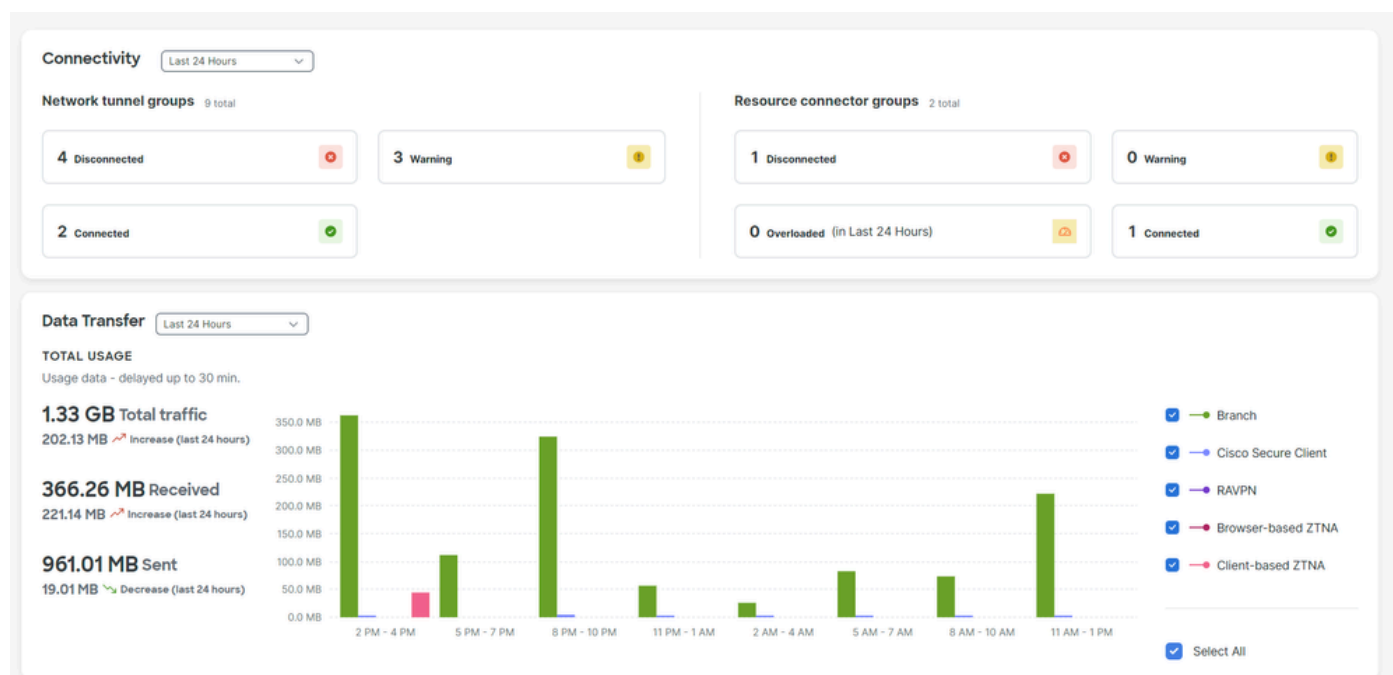
FORTINET®

Cisco has designed Secure Access to protect and provide access to private applications, both on-premise and cloud-based. It also safeguards the connection from the network to the internet. This is achieved through the implementation of multiple security methods and layers, all aimed at preserving the information as they access it via the cloud.

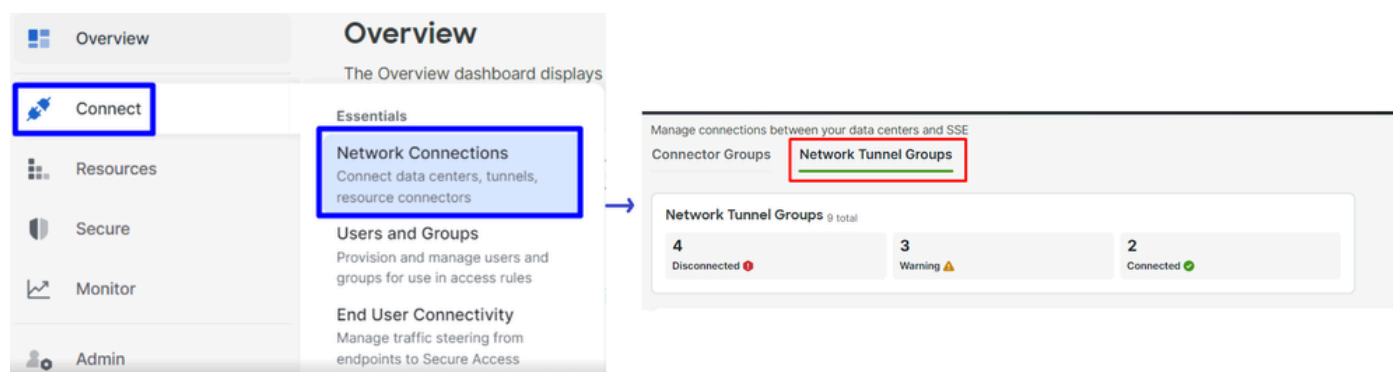
Configure

Configure the VPN on Secure Access

Navigate to the admin panel of [Secure Access](#).



- Click on Connect > Network Connections > Network Tunnels Groups



- Under Network Tunnel Groups click on + 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 securely control user access to the Internet and private resources. [Help](#)

Q Search Region Status 9 Tunnel Groups

+ Add

- Configure Tunnel Group Name, Region and Device Type
- Click 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

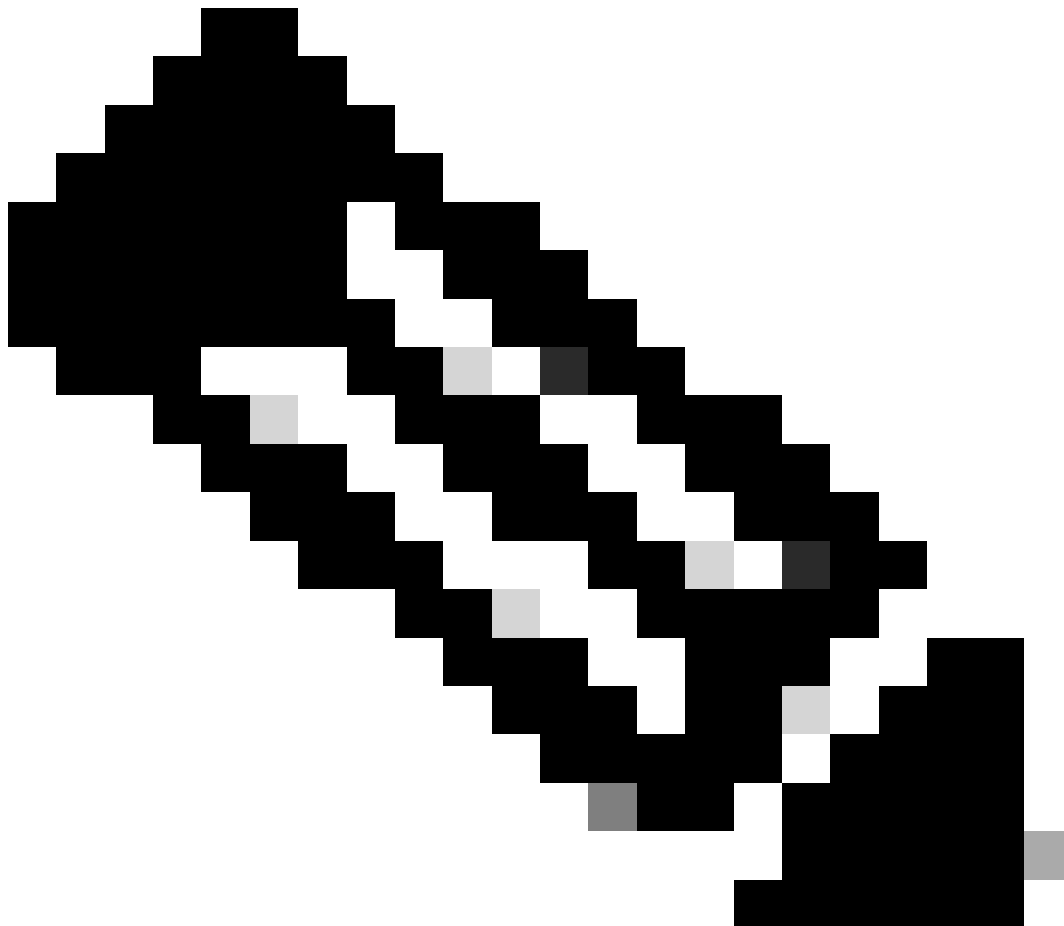
Region

Device Type



Cancel

Next



Note: Choose the region nearest to the location of your firewall.

- Configure the Tunnel ID Format and Passphrase
- ClickNext

✓ 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

- Configure the IP address ranges or hosts that you have configured on your network and want to pass the traffic through Secure Access
- ClickSave

✓ 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

After you click on **save** the information about the tunnel gets displayed, please save that information for the next step, **Configure the VPN Site to Site on Fortigate**.

Tunnel Data

Data for Tunnel Setup

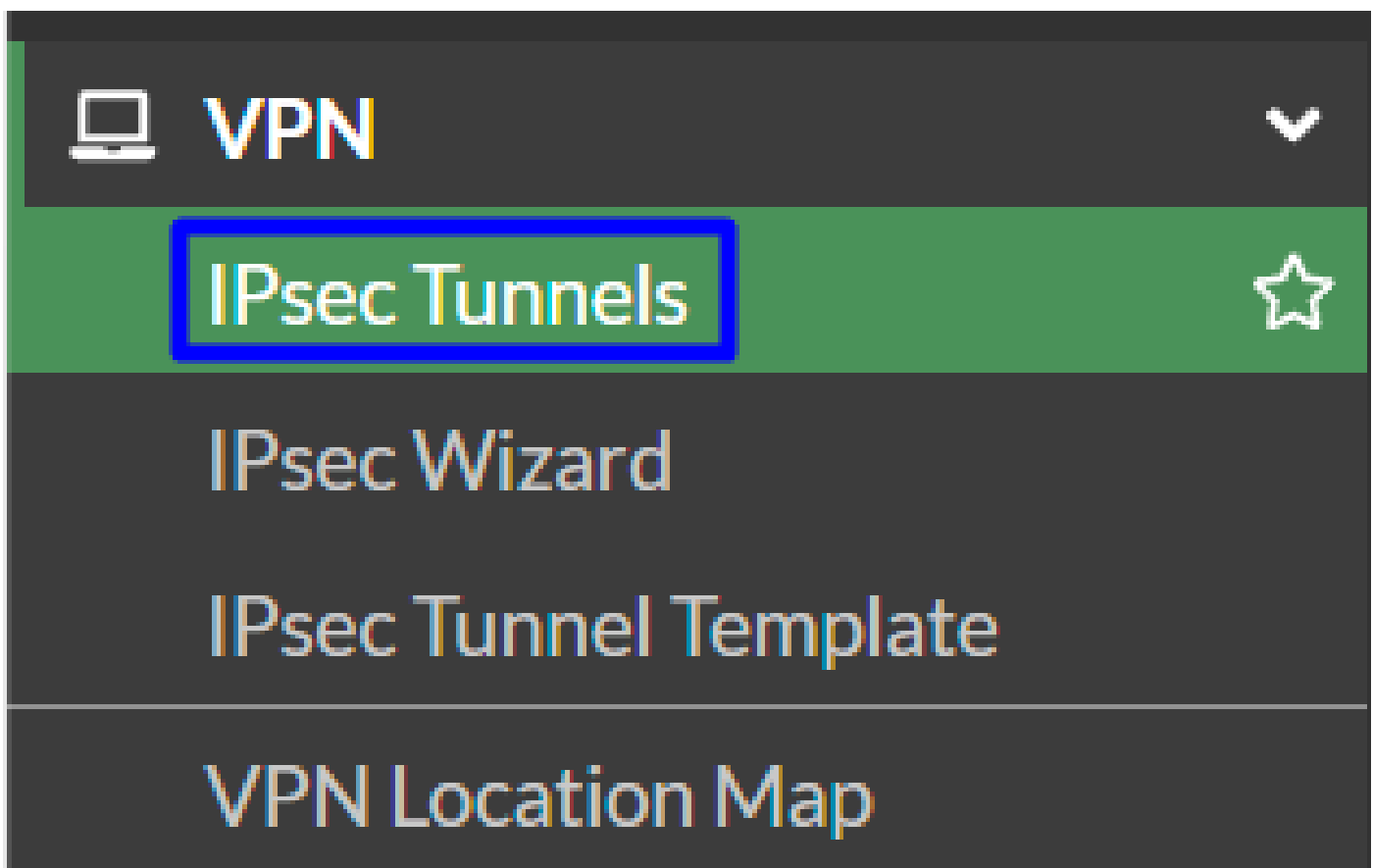
Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

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		

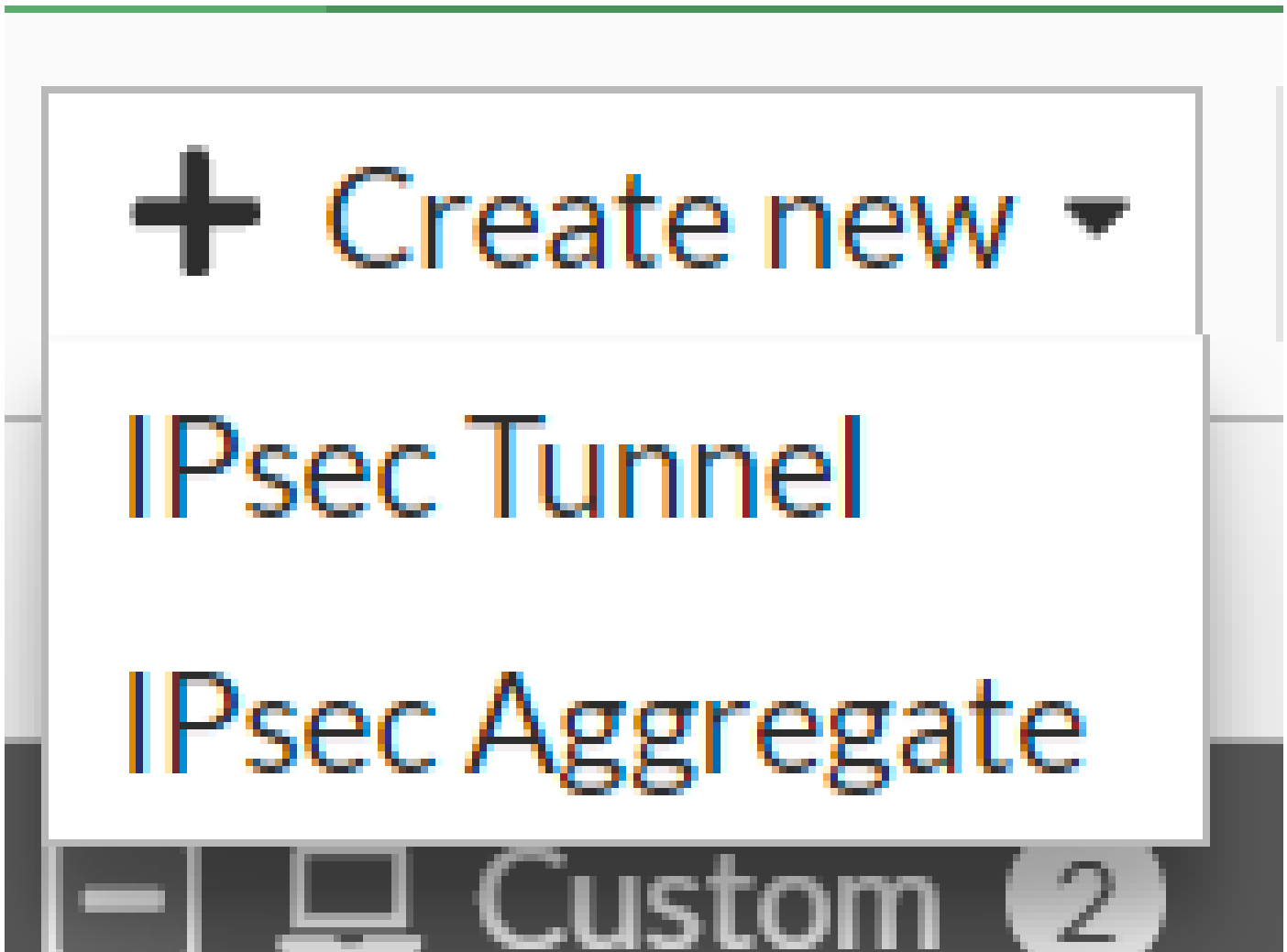
Configure the VPN Site to Site on Fortigate

Navigate to your Fortigate dashboard.

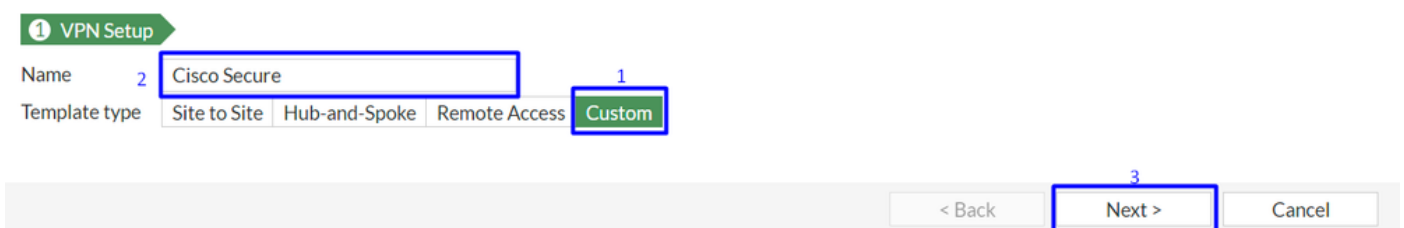
- Click VPN > IPsec Tunnels



- Click Create New > IPsec Tunnels



- Click Custom , configure a **Name** and click Next.



In the next image, you see how you need to configure the settings for the **Network** part.

Network

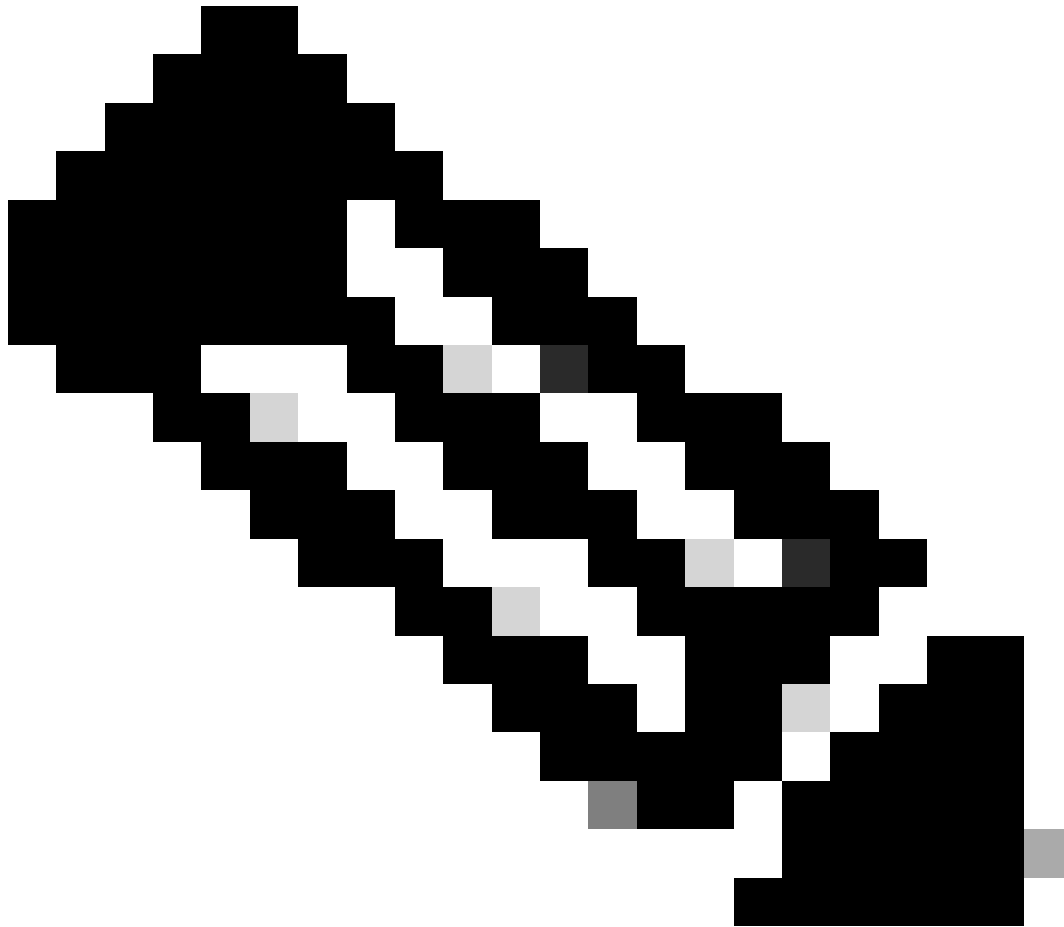
- Network
 - IP Version : IPv4
 - **Remote Gateway** : Static IP Address
 - IP Address: Use the IP of Primary IP Datacenter IP Address,given in the step [Tunnel Data](#)
 - **Interface** : Choose the WAN interface that you have planned to use to establish the tunnel
 - **Local Gateway** : Disable as default
 - **Mode Config** : Disable as default
 - **NAT Traversal** : Enable
 - **Keepalive Frequency** : 10
 - **Dead Peer Detection** : On Idle
 - **DPD retry count** : 3
 - **DPD retry interval** : 10
 - **Forward Error Correction** : Do not check any box.
 - **Advanced...**: Configure it as the image.

Now configure the IKE **Authentication**.

Authentication

- **Authentication**
 - **Method** : Pre-Shared Key as default
 - **Pre-shared Key** : Use the **Passphrase** given in the step [Tunnel Data](#)
- **IKE**
 - Version

: Choose version 2.



Note: Secure Access only supports IKEv2

Now configure the **Phase 1 Proposal**.

Phase 1 Proposal

Phase 1 Proposal ⊕ Add		Phase 1 Proposal ⊕ Add ✓ ↺	
Encryption	AES128	Authentication	SHA256
Encryption	AES256	Authentication	SHA256
Encryption	AES128	Authentication	SHA1
Encryption	AES256	Authentication	SHA1
Diffie-Hellman Groups	☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1		
Key Lifetime (seconds)	86400		
Local ID			

Encryption	AES256	Authentication	SHA256
Diffie-Hellman Groups	☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☒ 20 ☒ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☐ 5 ☐ 2 ☐ 1		
Key Lifetime (seconds)	86400		
Local ID	fortigate@8195126-621099508-sse.ci		

- Phase 1 Proposal
 - Encryption : Choose AES256
 - Authentication : Choose SHA256
 - Diffie-Hellman Groups : Check the box 19 and 20
 - Key Lifetime (seconds) : 86400 as default
 - Local ID : Use the Primary Tunnel ID, given in the step [Tunnel Data](#)

Now configure the **Phase 2 Proposal**.

Phase 2 Proposal

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

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

Seconds: 43200

- New Phase 2
 - **Name** : Let as default (This is taken from the name of your VPN)
 - **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** : Choose AES128
 - **Authentication** : Choose SHA256
 - **Enable Replay Detection** : Let as default (Enabled)
 - **Enable Perfect Forward Secrecy (PFS)** : Unmark the checkbox
 - **Local Port** : Let as default (Enabled)
 - **Remote Port** : Let as default (Enabled)
 - **Protocol** : Let as default (Enabled)
 - **Auto-negotiate** : Let as default (Unmarked)
 - **Autokey Keep Alive** : Let as default (Unmarked)
 - **Key Lifetime** : Let as default (Seconds)

- **Seconds** : Let as default (43200)

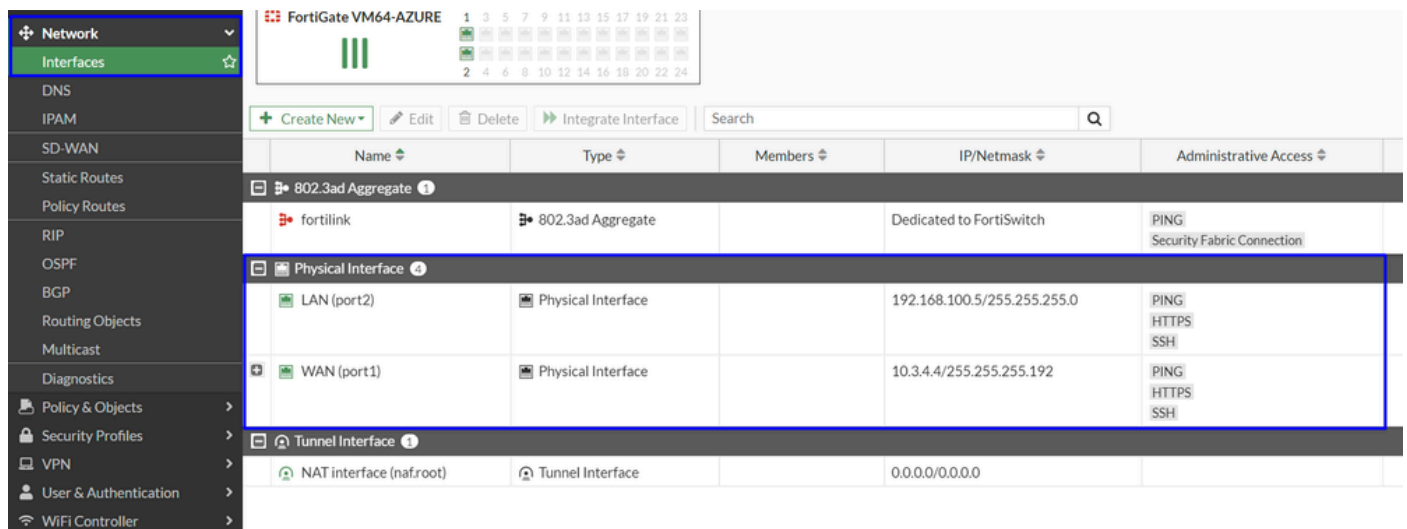
After that, click OK. You see after some minutes that the VPN was established with Secure Access, and you can continue with the next step, **Configure the Tunnel Interface**.



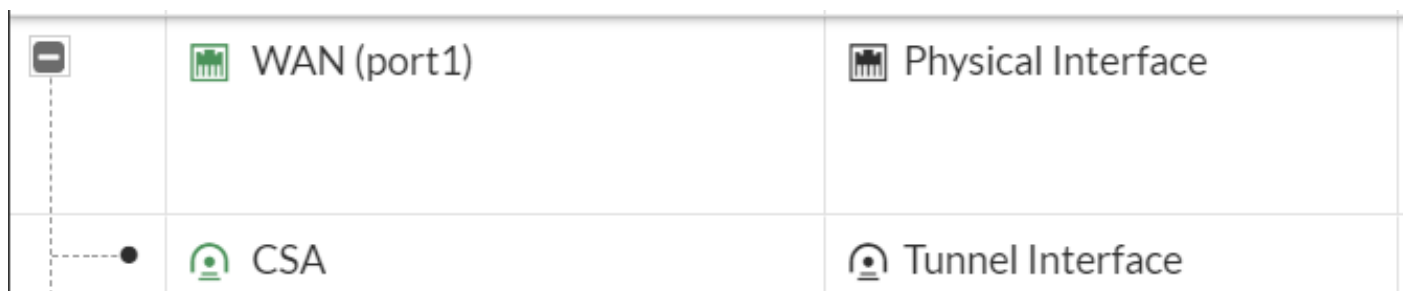
Configure the Tunnel Interface

After the tunnel is created, you notice that you have a new interface behind the port that you are using as a WAN interface to communicate with Secure Acces.

In order to check that, please navigate to **Network > Interfaces**.



Expand the port you use to communicate with Secure Access; in this case, the **WAN** interface.



- Click on your **Tunnel Interface** and click **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

- You have the next image that you need to configure

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 0.0.0.0 Netmask 255.255.255.255 Remote IP/Netmask 0.0.0.0	Address Addressing mode Manual IP 169.254.0.1 Netmask 255.255.255.255 Remote IP/Netmask 169.254.0.2 255.255.255.252
--	--

- Interface Configuration
- IP : Configure a non-routable IP that you do not have in your network (169.254.0.1)
- Remote IP/Netmask : Configure the Remote IP as the next IP of your interface IP and with a Netmask of 30 (169.254.0.2 255.255.255.252)

After that, click **OK** to save the configuration and proceed with the next step, Configure Policy Route (Origin-based routing).



Warning: After this part, you must configure the Firewall Policies on your FortiGate in order to permit or allow the traffic from your device to Secure Access and from Secure Access to the networks that you want to route the traffic.

Configure Policy Route

At this point, you have your VPN configured and established to Secure Access; now, you must re-route the traffic to Secure Access to protect your traffic or access to your private applications behind your FortiGate firewall.

- Navigate to Network > Policy Routes

 Dashboard >

 **Network** v

Interfaces

DNS

IPAM

SD-WAN

Static Routes

Policy Routes ☆

+ Create New

Seq.#

1

2

- Configure the policy

If incoming traffic matches:	If incoming traffic matches:
Incoming interface +	Incoming interface LAN (port2)
Source Address	Source Address
IP/Netmask +	IP/Netmask 192.168.100.0/255.255.255.0
Addresses +	Addresses +
Destination Address	Destination Address
IP/Netmask +	IP/Netmask +
Addresses +	Addresses all
Internet service +	Internet service +
Protocol TCP UDP SCTP <input checked="" type="text" value="ANY"/> Specify	Protocol TCP UDP SCTP <input checked="" type="text" value="ANY"/> Specify
Type of service 0	Type of service 0
0x00 Bit Mask 0x00	0x00 Bit Mask 0x00
Then:	Then:
Action <input checked="" type="text" value="Forward Traffic"/> Stop Policy Routing	Action <input checked="" type="text" value="Forward Traffic"/> Stop Policy Routing
Outgoing interface ☒ CSA	Outgoing interface ☒ CSA
Gateway address	Gateway address 169.254.0.2
Comments Write a comment...	Comments Write a comment...
Status <input checked="" type="text" value="Enabled"/> Disabled	Status <input checked="" type="text" value="Enabled"/> Disabled

- If Incoming traffic matches
 - Incoming Interface : Choose the interface from where you planned to re-route the traffic to Secure Access (Origin of traffic)
- Source Address
 - IP/Netmask : Use this option if you only route a subnet of an interface
 - Addresses : Use this option if you have the object created and the source of the traffic comes from multiple interfaces and multiple subnets
- Destination Addresses
 - Addresses: Choose all
 - Protocol: Choose ANY
- Then
 - Action: Choose Forward Traffic
- Outgoing Interface : Choose the Tunnel Interface that you modified on the step, [Configure Tunnel Interface](#)
- Gateway Address: Configure the Remote IP configured on the step, [RemoteIPNetmask](#)
- Status : Choose Enabled

Click **OK** to save the configuration, you are now ready to verify if your devices traffic was re-routed to Secure Access.

Verify

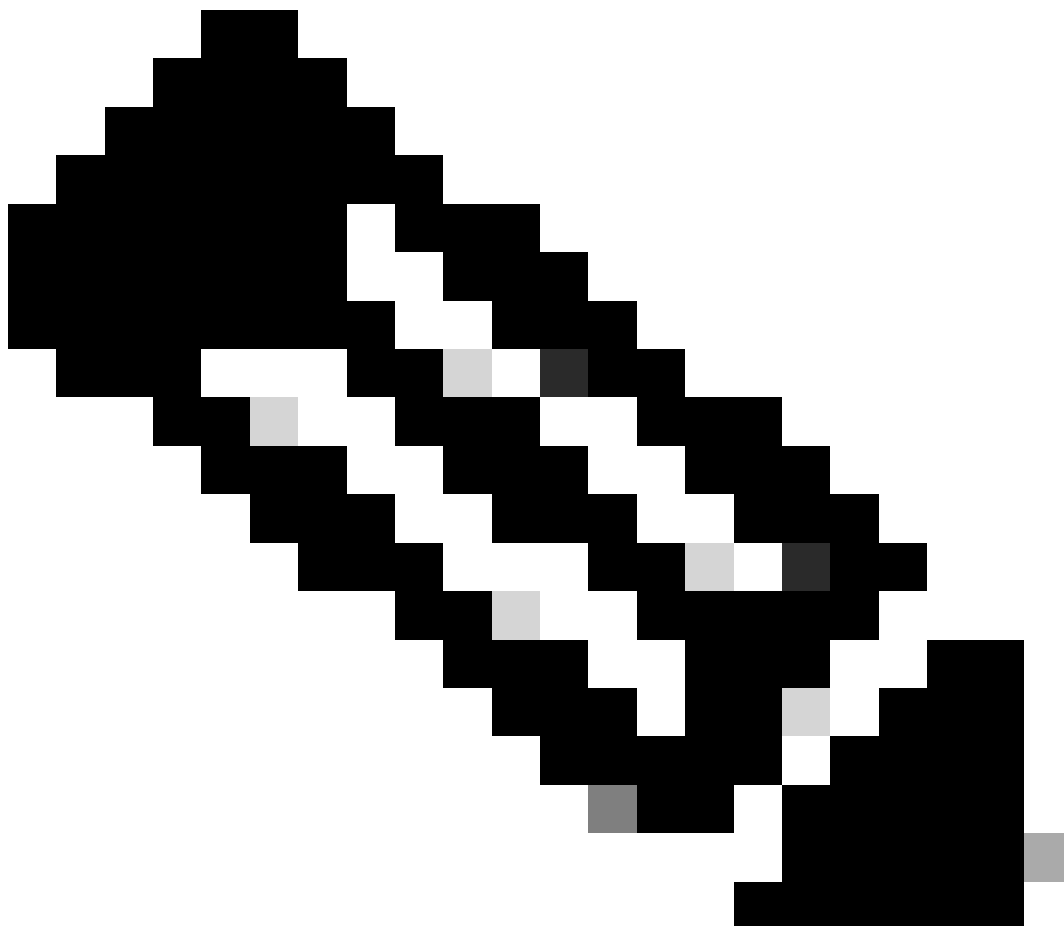
In order to verify if the traffic of your machine was re-routed to Secure Access, you have two options; you can check on the internet and check for your public IP, or you can run the next command with curl:

```
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"
}
```

The public range from where you can see your traffic is from:

Min Host: 151.186.176.1

Max Host : 151.186.207.254



Note: These IPs are subject to change, which means that Cisco probably extend this range in the future.

If you see the change of your public IP, that means you are being protected by Secure Access, and now you can configure your private application on the Secure Access dashboard to access your applications from VPNaaS or ZTNA.