FortiGate
on OCB FE
Configuration Guide

1st February 2020
Version 2.0

document control

date	version no.	author	change/addition
6th December 2018	1.00	Ahmad Samak	Creation
1st February 2020	2.00	Ahmad Samak	Updating the intial configuration and the IPSEC VPN configuration sections

table of contents

1 References

Reference	Description	Link to document
1	FortiOS™ Handbook VM Installation for FortiOS	https://docs.fortinet.com/uploaded/files/1734/fortigate-vm-install-50.pdf#M8.9.51917.Chapter.Title.FortiGate.VM.Deployment
2	FortiOS™ Handbook Troubleshooting for FortiO	https://docs.fortinet.com/uploaded/files/1079/Troubleshooting.pdf
3	Virtual FortiOS -AdminGuide	https://docs.fortinet.com/uploaded/files/2324/fortigate-virtual_fortios-56-1.pdf
4	FortiGate VM Initial Configuration	https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-vm-install-54/vm_FGT-VM_Initial_Configuration.htm

2 Introduction

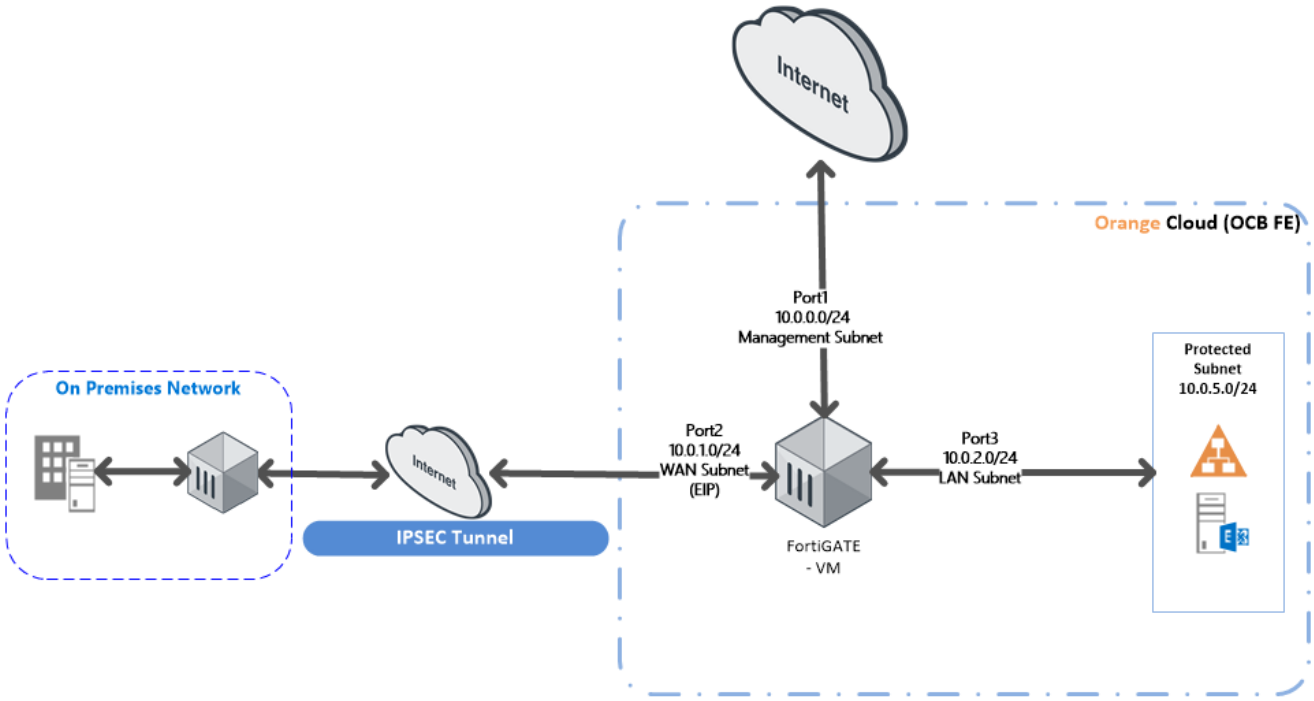
FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

3 Deployment Method

Use the FortiGate VM firewall on OCB FE to secure your network users in the following scenarios:

3.1 Hybrid and VPC to VPC

The FortiGate VM firewall on OCB FE allows you to securely extend your physical data center/private cloud into OCB FE using IPsec tunneling. To improve your data center security, if you have segmented your network and deployed your workloads in separate VPC's, you can secure traffic flowing between VPC's with an IPsec tunnel and application whitelisting policies.

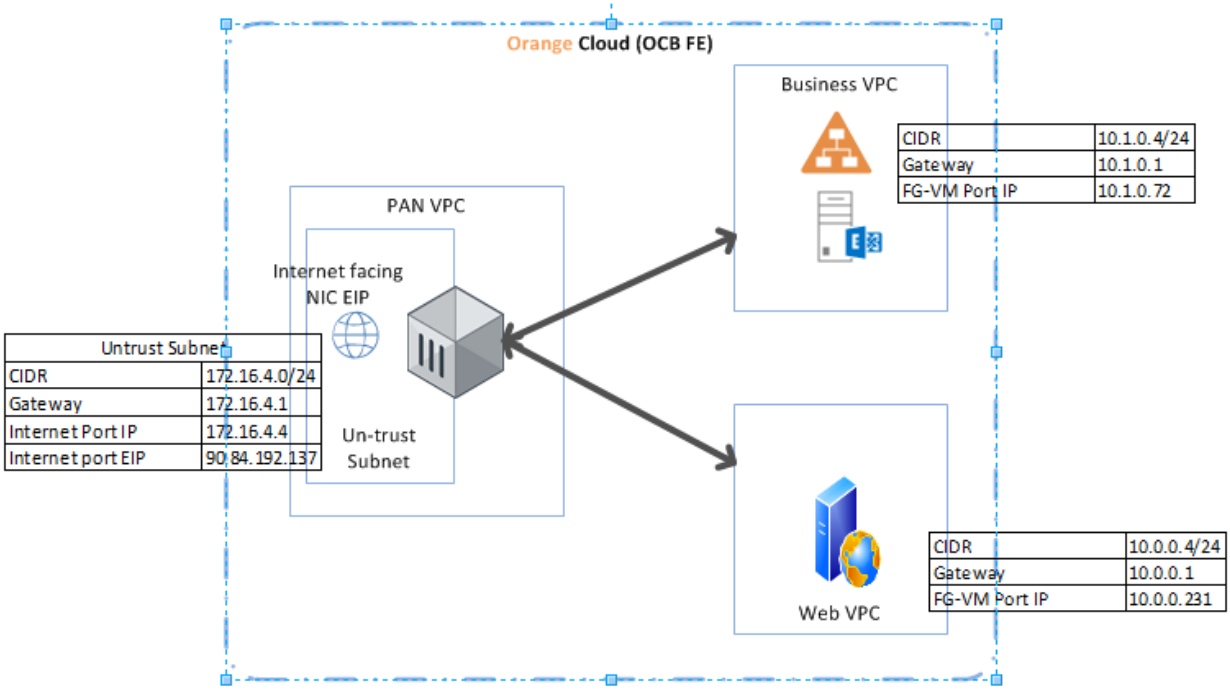


• **Inter-Subnet** —The VM-Series firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.

• **Gateway**—The VM-Series firewall serves as the VPC gateway to protect Internet-facing deployments in the OCB FE (VPC). The FortiGate VM firewall secures traffic destined to the servers in the VPC and it also protects against lateral threats for inter-subnet traffic between applications in a multitier architecture.

• **Remote Access**—Use the OCB FE infrastructure to quickly and easily deploy the FortiGate VM firewall as remote access and extend your gateway security policy to remote users and devices, regardless of location.

3.1.1 VDC Setup on OCB FE



- **FGVM – VPC** hosting one VM Series firewall includes

  Management Subnet
  Internet Facing Subnet

- **Business- VPC** hosting active directory and exchange server and includes

  Business Subnet

  We created a port on the Business VPC and assigned it as a third NIC card to the FortiGate VM firewall on FortiGate VM VPC

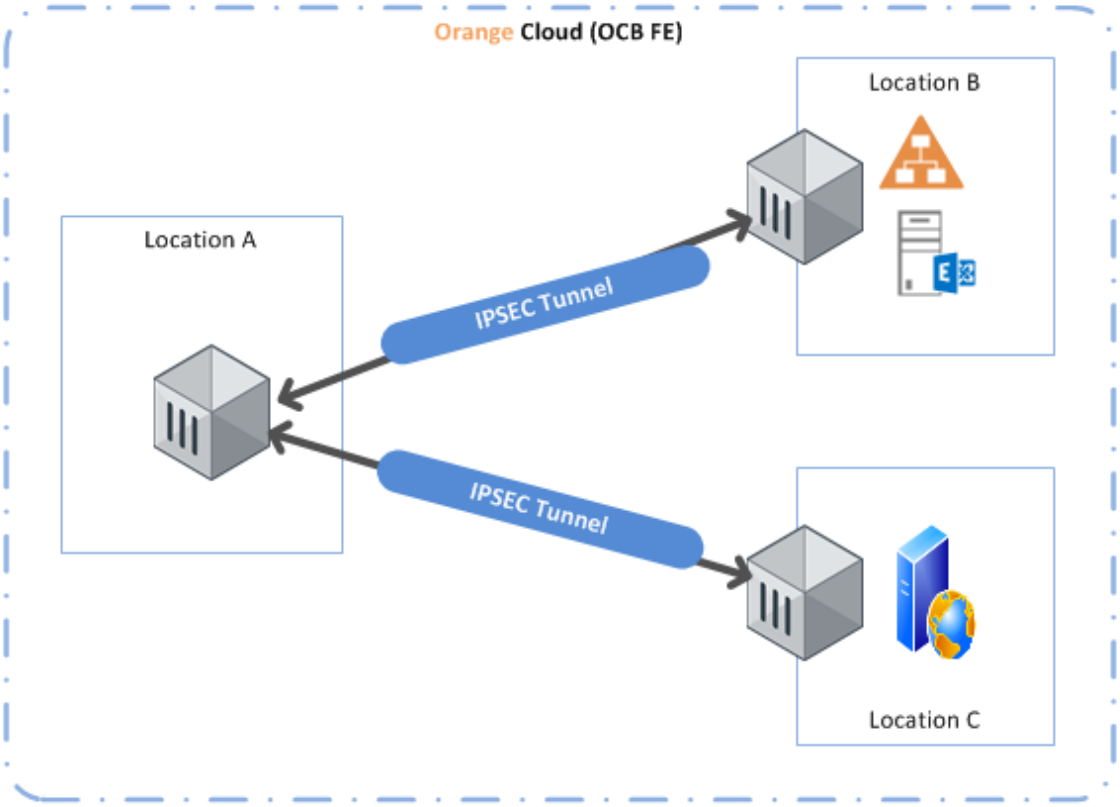
- **Web-VPC** hosting a webserver vm and includes

  Web-Subnet

  We created a port on the Web VPC and assigned it as a third NIC card to the vm-series firewall on FortiGate VM VPC

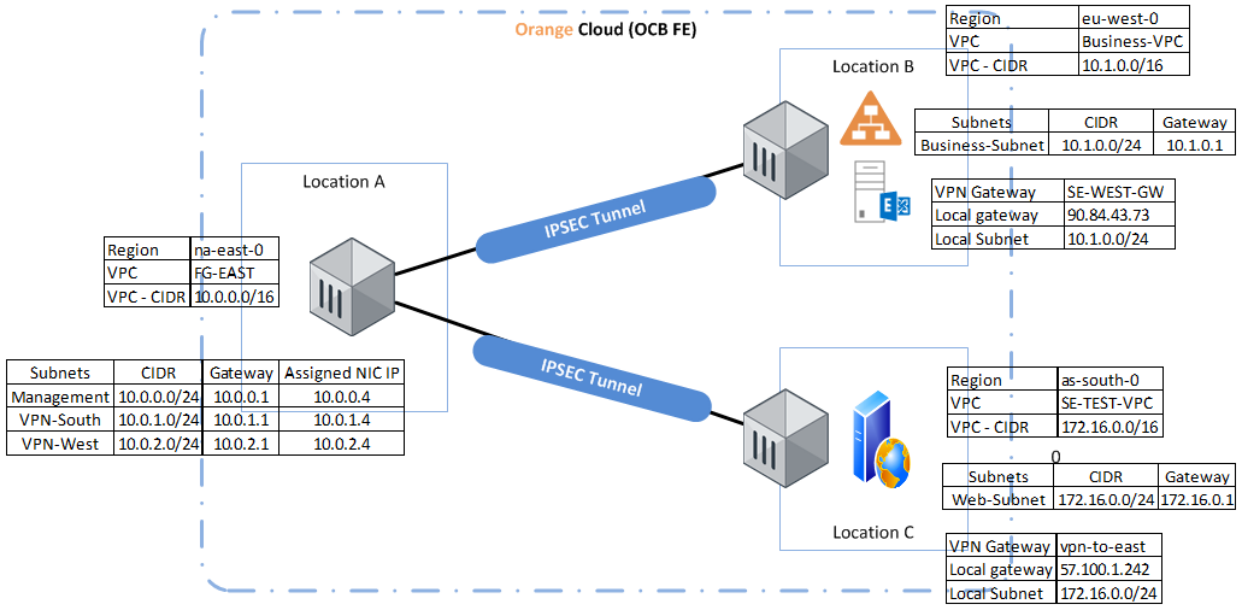
3.2 On Cloud /On Cloud

The FortiGate VM firewall on OCB FE allows you to securely extend your multiple location cloud VPC's into OCB FE using IPsec tunneling.



- **Inter-Subnet** The FortiGate VM firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.
- **VPN Gateway** A Virtual Private Network (VPN) provides an encrypted communication channel that enables users to remotely access VPCs. In this scenario FortiGate VM firewall acts as the VPN gateway of each location
- **Multiple location VPC's** with two subnets in each VPC.

3.2.1 VDC Setup on OCB FE



This scenario connects multiple VPC's in different locations

East Location:

Contains a VPC hosting vm-series firewall that will be the vpn gateway of this VPC.

West Location:

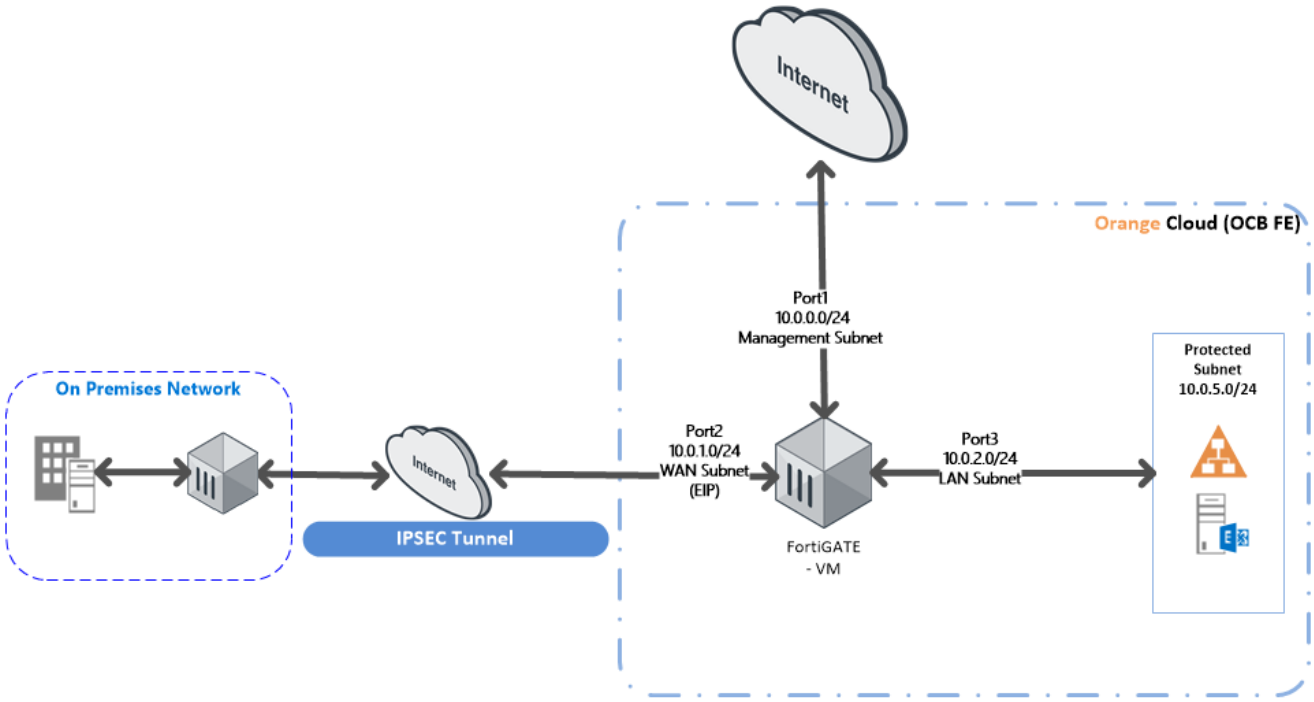
Contains a Business-VPC and a vpn gateway that will initiate the IPsec tunnel for this VPC.

South Location:

Contains a Web-VPC and a vpn Gateway that will initiate the IPsec tunnel for this VPC.

4 Solution Configuration

4.1 Hybrid and VPC to VPC Model



In this model we will configure the following:

1. On Premises ESXI FortiGate VM configuration
2. IPSEC tunnel configuration between on premises Fortigate VM ESXI firewall and OCB FE FortiGate VM
3. Remote VPN configuration.

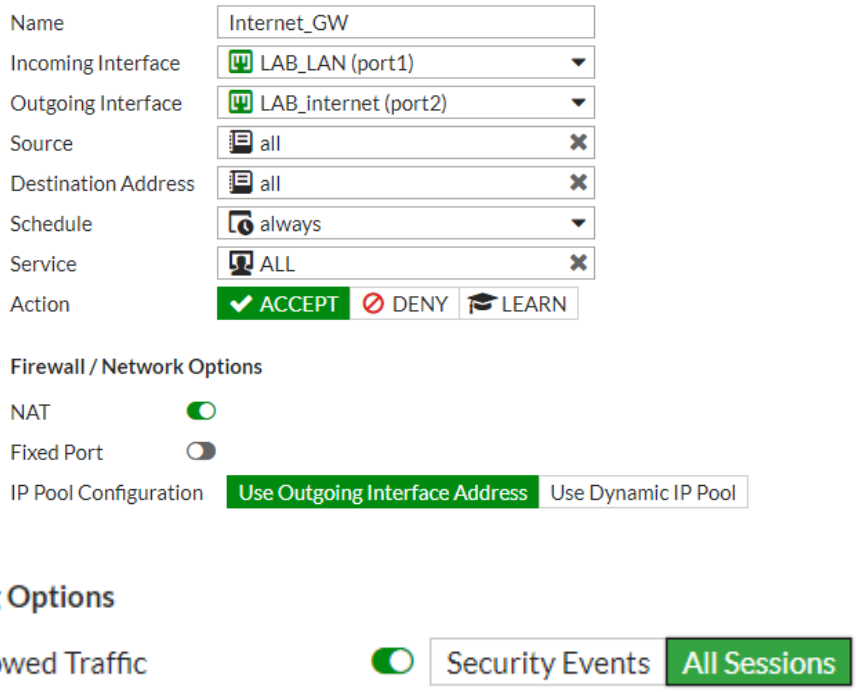
4.1.1 On Premises FortiGate configuration

Creating a policy to allow traffic from the internal network to the Internet

Some FortiGate models include an IPv4 security policy in the default configuration. If you have one of these models, edit it to include the logging options shown below, then proceed to the results section.

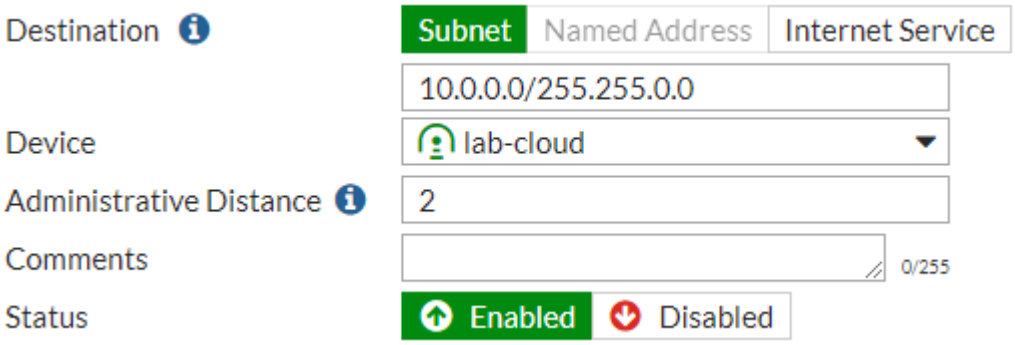
Go to Policy & Objects > IPv4 Policy and create a new policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet. Set the Incoming Interface to the internal interface (called internal on some FortiGate models) and the Outgoing Interface to the Internet facing interface. Set Source, Schedule, and Services as required.

Make sure the Action is set to ACCEPT. Scroll down to view the Logging Options. In order to view the results later, enable Log Allowed Traffic and select All Sessions.



4.1.2 Create a Static Route for the VPN Connection

Add the OCB FE internet Facing Subnet address Range and set the destination to Subnet.

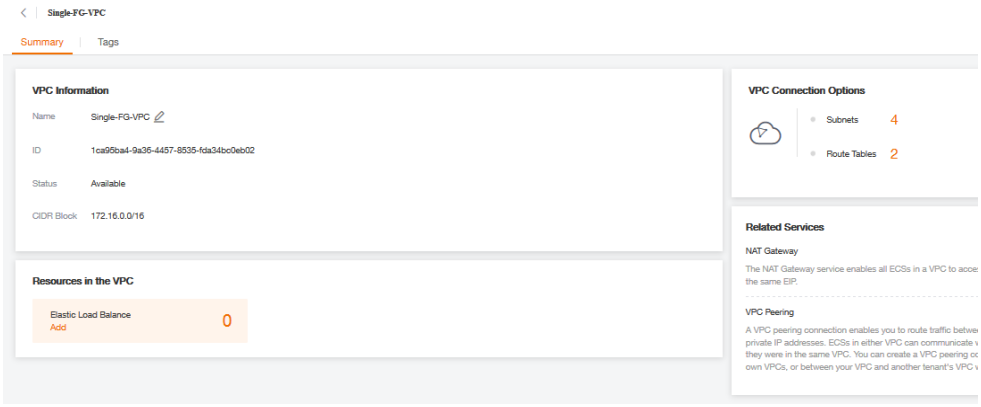


4.1.3 Create user defined routes on OCB FE VPC

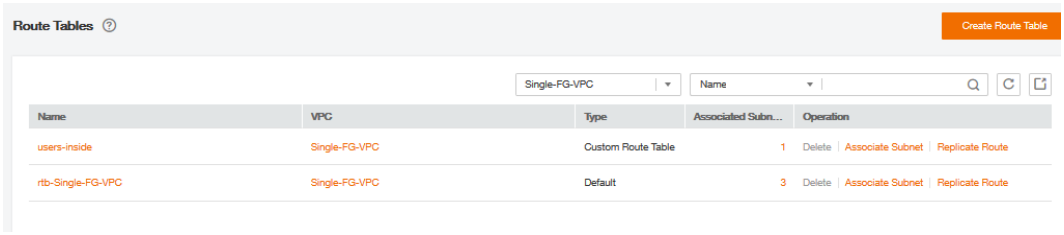
After applying the subnet level routing on OCB FE . We should have to add route table and create routes and associate to the internal (Protected subnet.

1- From Network > Virtual Private Cluod

2- Select your VPC

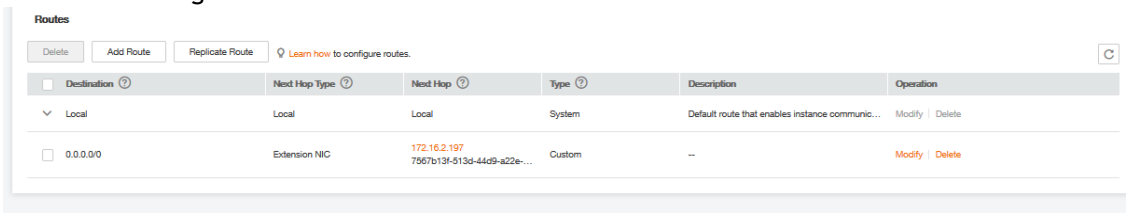


3- Choose route Tables

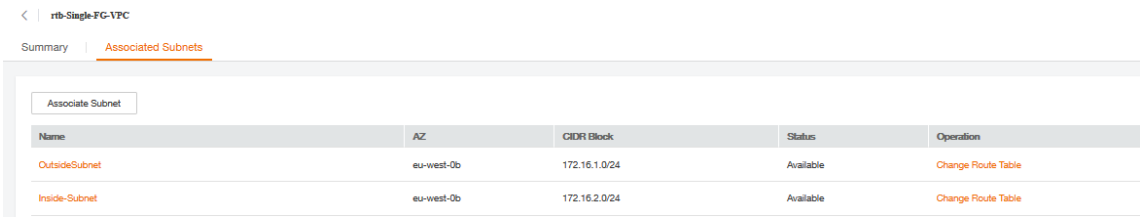


4- Select the route table of type Default

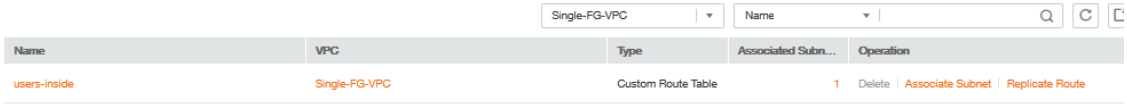
5- Add the following route

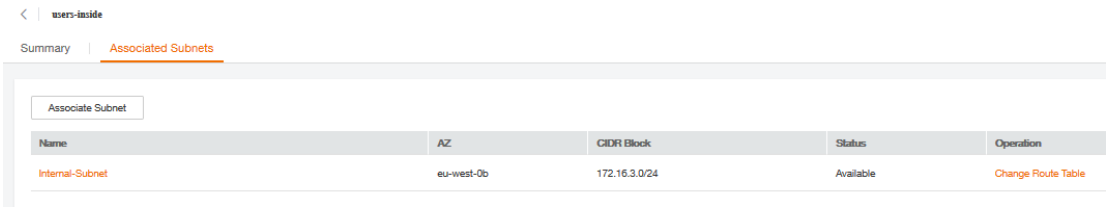


6- Make sure that the Default route table is associated to Internet facing and LAN Subnets.

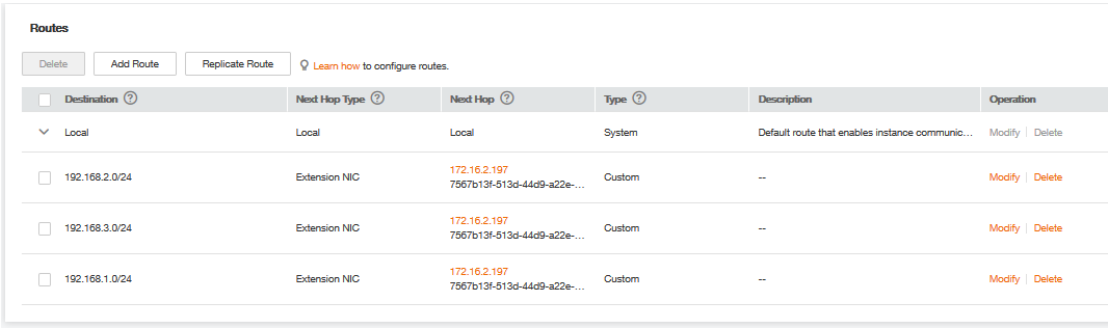


7- Create a new route table and associate to the Internal (Protected) Subnet

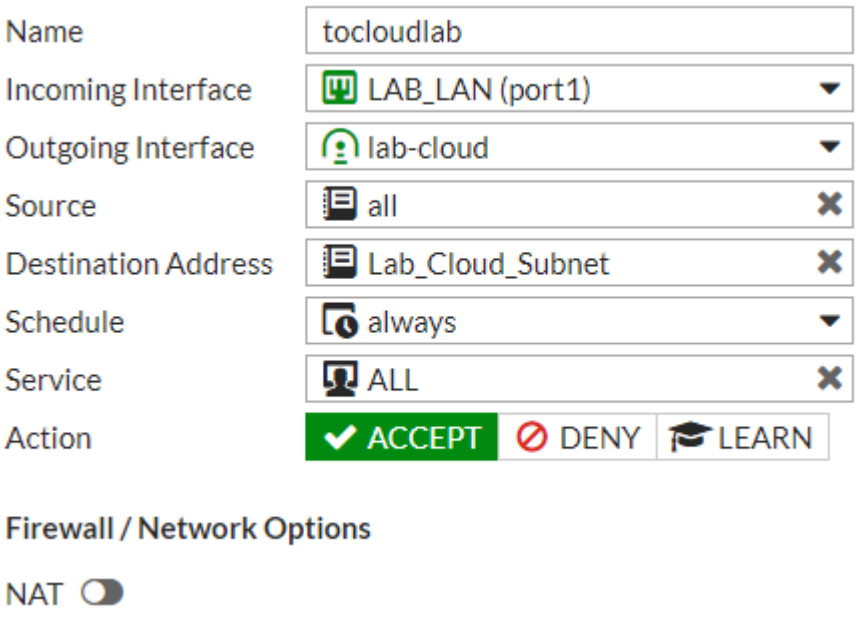


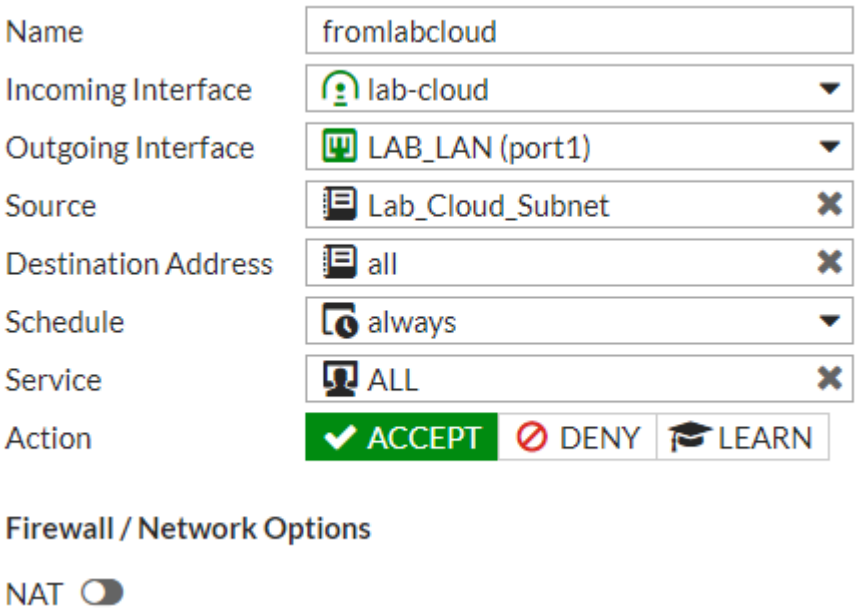


8- Add the following routes to the custom route table to allow traffic to the destination subnets (On premisis Subnets) through the Inside NIC.

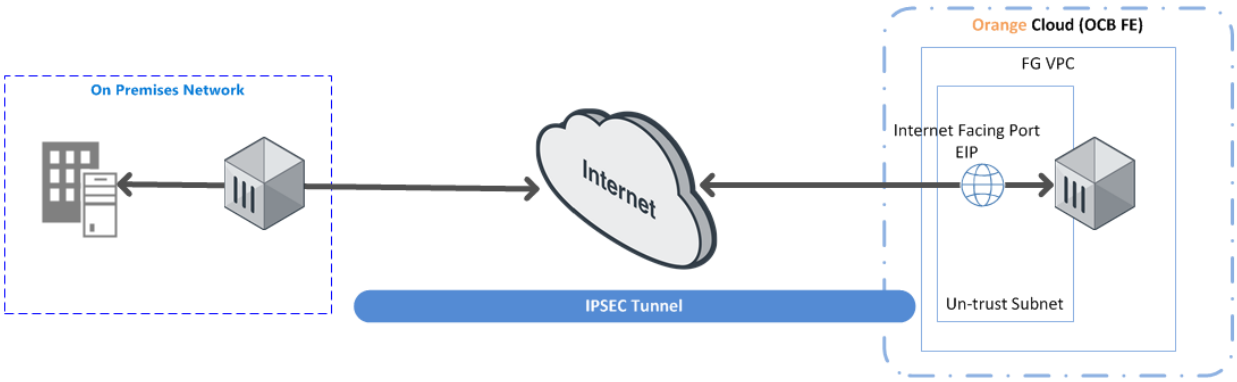


4.1.4 Creating Two policies to allow traffic from the internal network to OCB FE VPC and Vice Versa





4.2 Site-to-Site VPN-IPSEC Tunnel Configuration

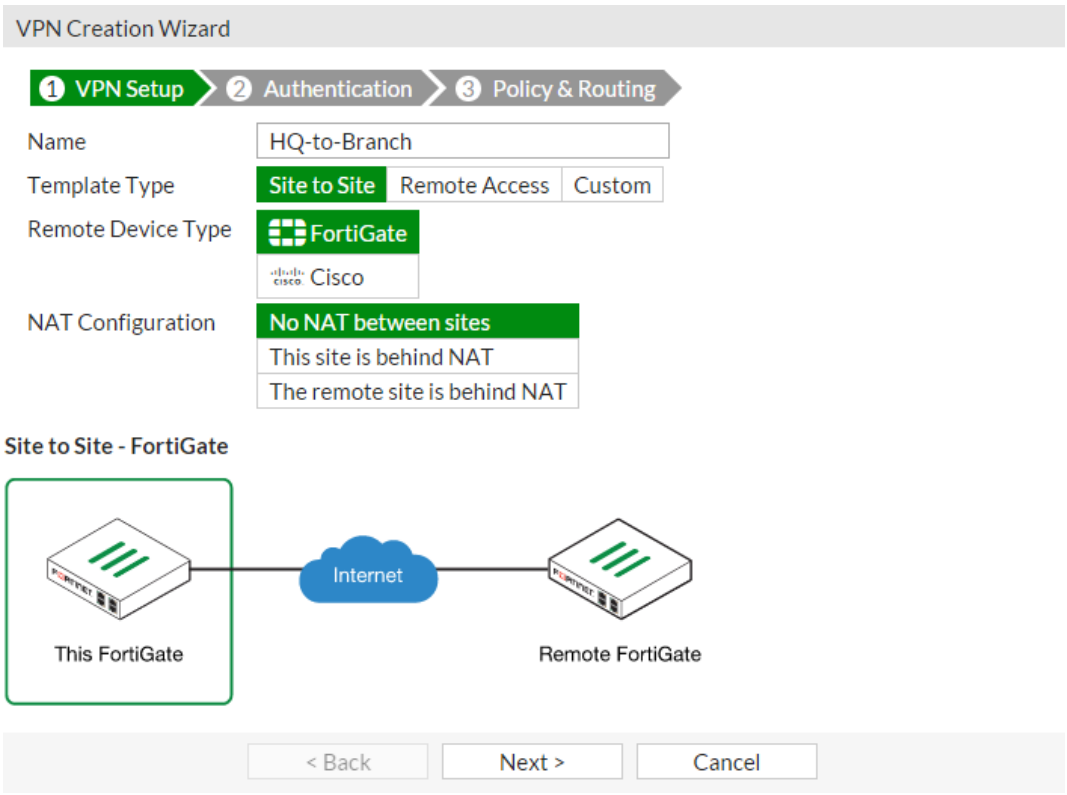


IPSec Tunnel configuration will be performed on Both the firewalls as per the diagram above,

4.2.1 Configuring the onprem. IPsec VPN

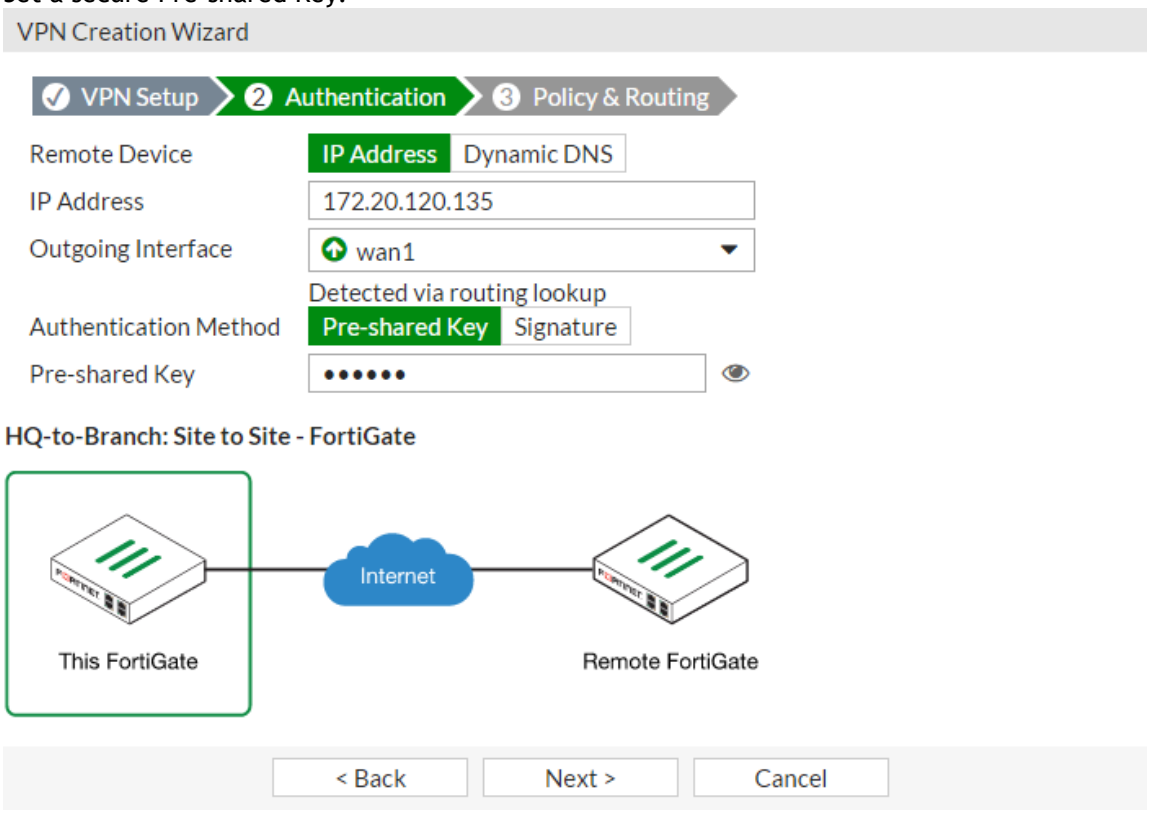
1. From the On premises FortiGate

Go to **VPN > IPSEC Wizard**

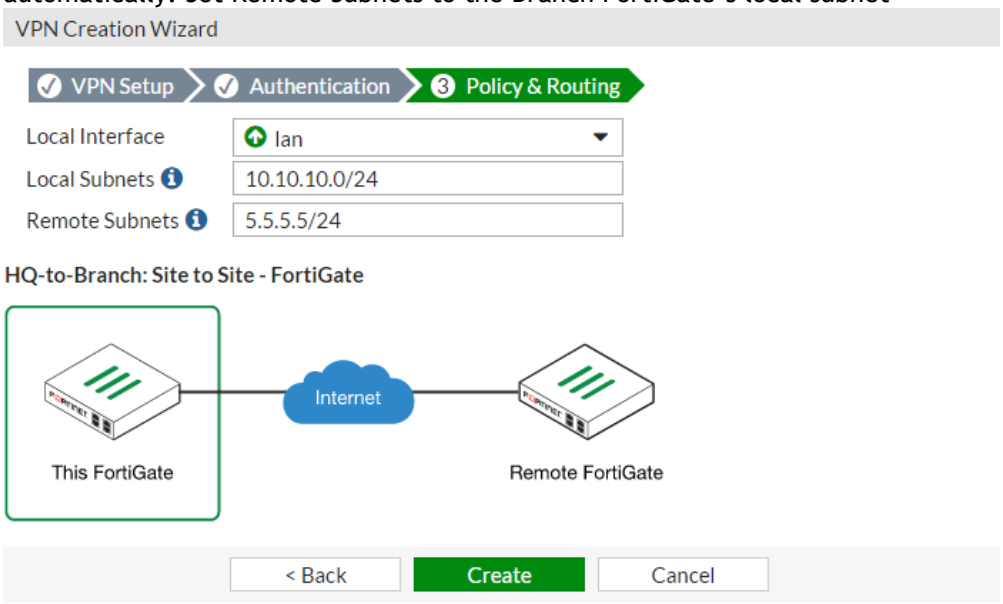


Select the **Site to Site** template, and select **FortiGate**

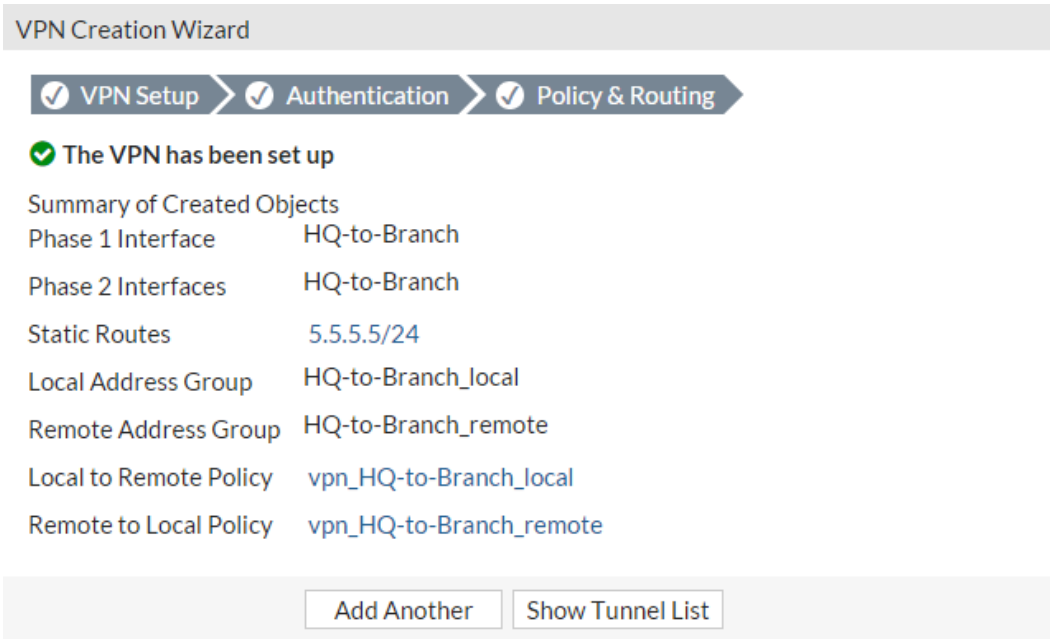
2. In the **Authentication** step, set **IP Address** to the IP of the Branch FortiGate After you enter the gateway, an available interface will be assigned as the Outgoing Interface. If you wish to use a different interface, select it from the drop-down menu.
   Set a secure Pre-shared Key.



3. n the Policy & Routing step, set the Local Interface. The Local Subnets will be added automatically. Set Remote Subnets to the Branch FortiGate's local subnet

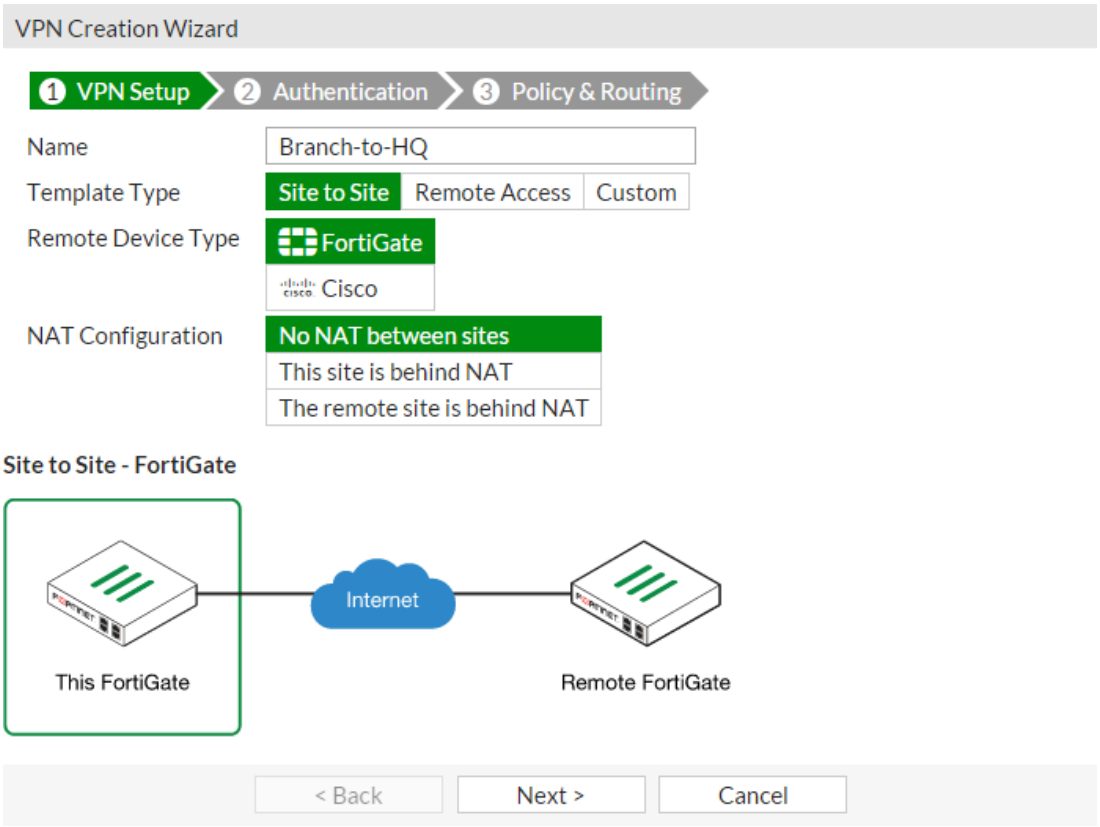


4. A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



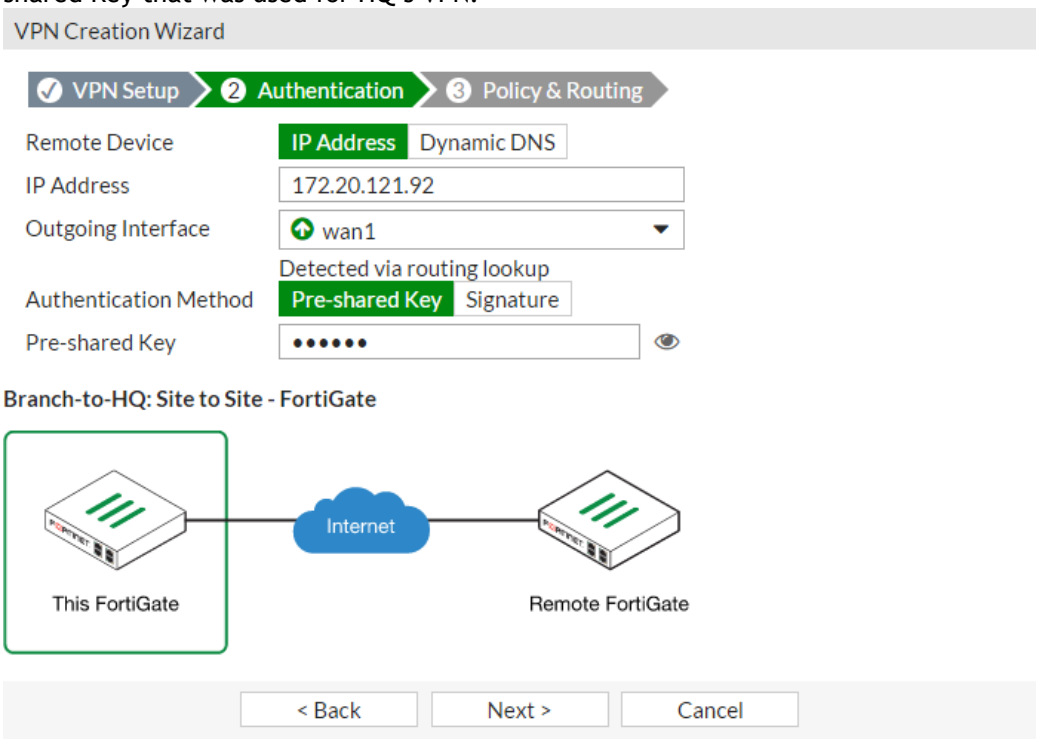
4.2.2 Configuring OCB FE IPSEC VPN

1. On the Branch FortiGate, go to **VPN > IPsec Wizard**. Select the **Site to Site** template, and select **FortiGate**

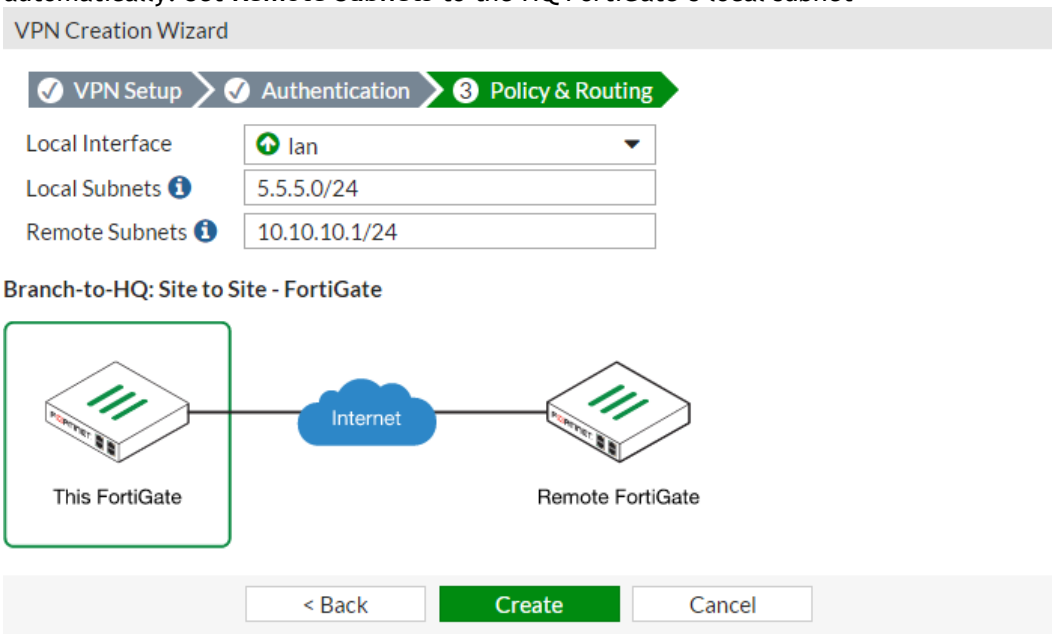


2. In the **Authentication** step, set **IP Address** to the IP of the on prem. FortiGate. After you enter the gateway, an available interface will be assigned as the Outgoing Interface. If you wish to use a different interface, select Change. Set the same Pre-

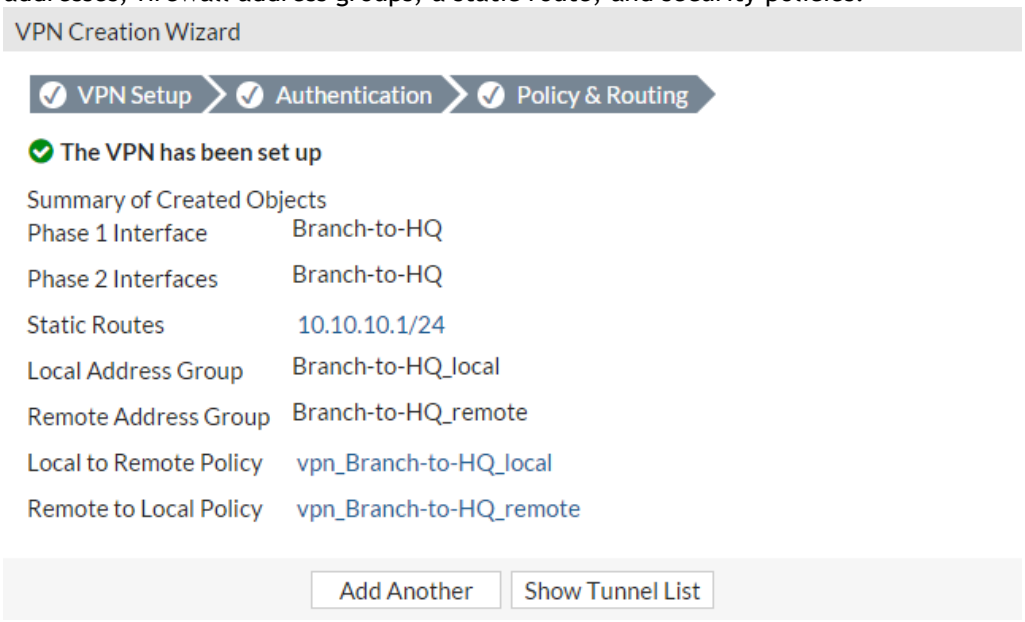
shared Key that was used for HQ's VPN.



3. In the **Policy & Routing** step, set the **Local Interface**. The **Local Subnets** will be added automatically. Set **Remote Subnets** to the HQ FortiGate's local subnet

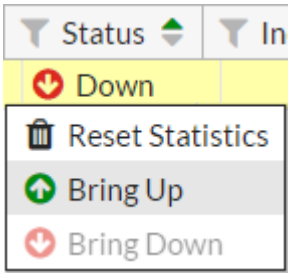


4. A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



4.2.3 Results

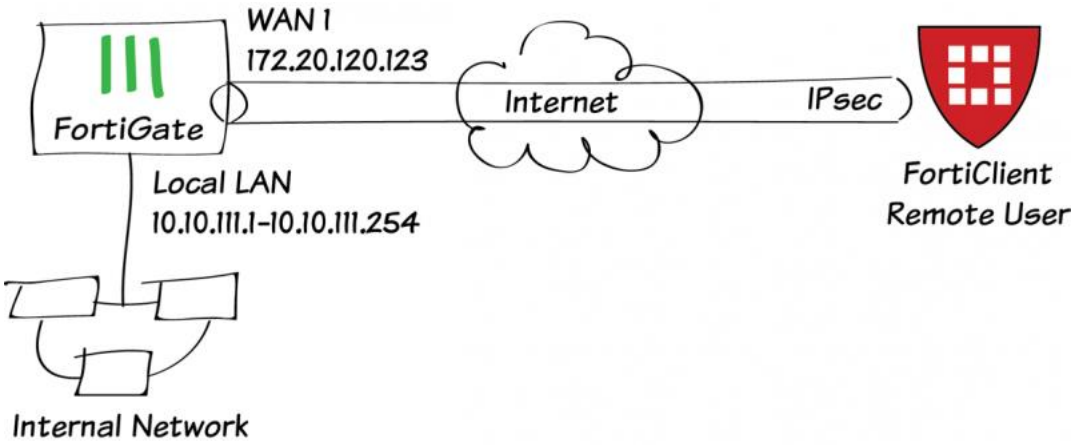
On either FortiGate, go to **Monitor** > **IPsec Monitor** to verify the status of the VPN tunnel. Right-click under **Status** and select **Bring Up**.



4.3 IPsec VPN with FortiClient

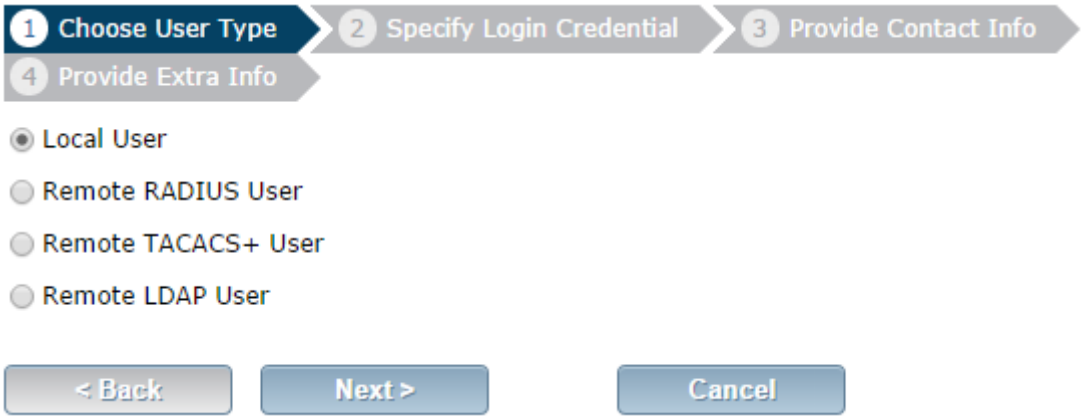
This option uses the IPsec VPN Wizard to provide a group of remote users with secure, encrypted access to the corporate network.

The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet. When the tunnel is configured, you will connect using the FortiClient application.

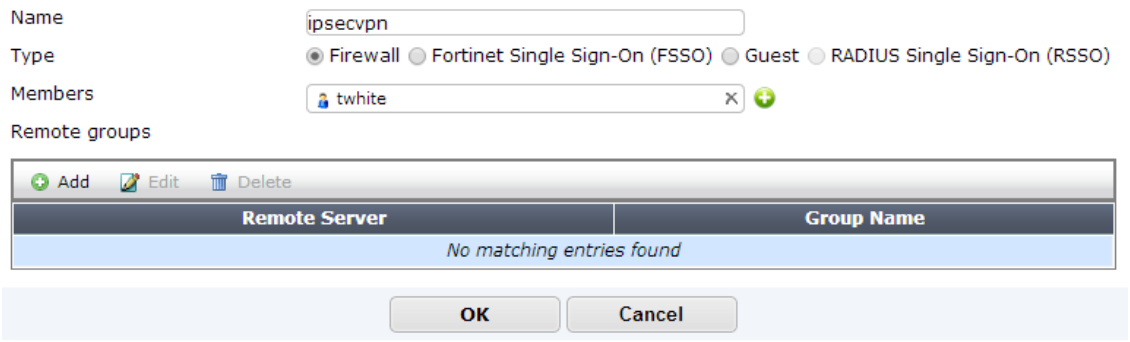


4.3.1 Creating a user group for remote users

1. Go to **User & Device > User > User Definition**.
2. Create a new **Local User** with the **User Creation Wizard**.



3. Proceed through each step of the wizard, carefully entering the appropriate information.
4. Go to User & Device > User > User Groups. Create a user group for remote users and add the user you created.



4.3.2 Adding a firewall address for the local network

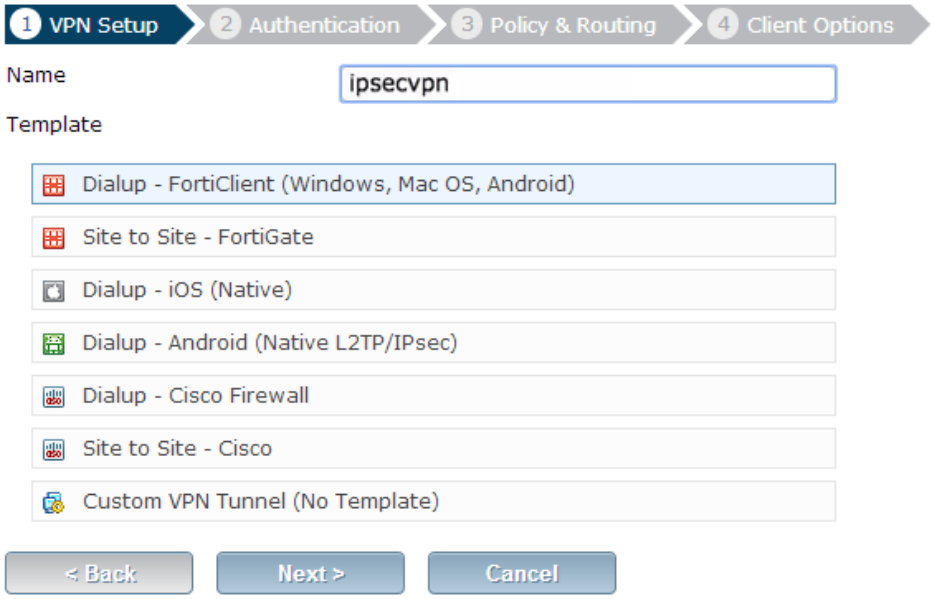
1. Go to Policy & Objects > Objects > Addresses.

2. Add a firewall address for the Local LAN, including the subnet and local interface.

4.3.3 Configuring the IPsec VPN using the IPsec VPN Wizard

1. Go to VPN > IPSec > Wizard.

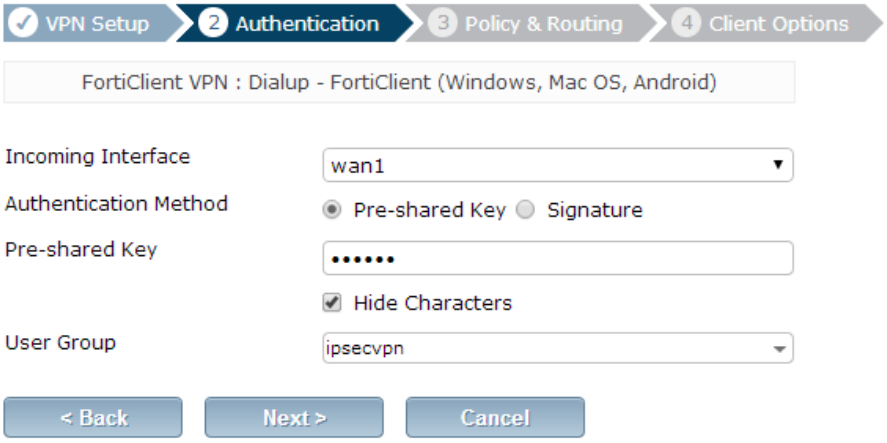
2. Name the VPN connection* and select Dial Up - FortiClient (Windows, Mac OS, Android) and click Next.



3. Set the Incoming Interface to the internet-facing interface.

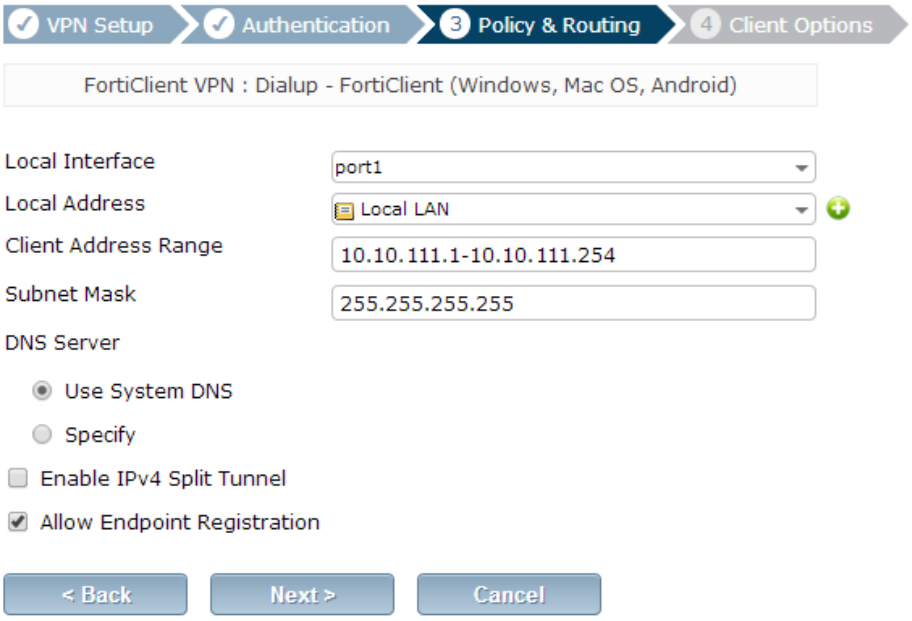
4. Select Pre-shared Key for the Authentication Method.

5. Enter a pre-shared key* and select the new user group, then click Next.

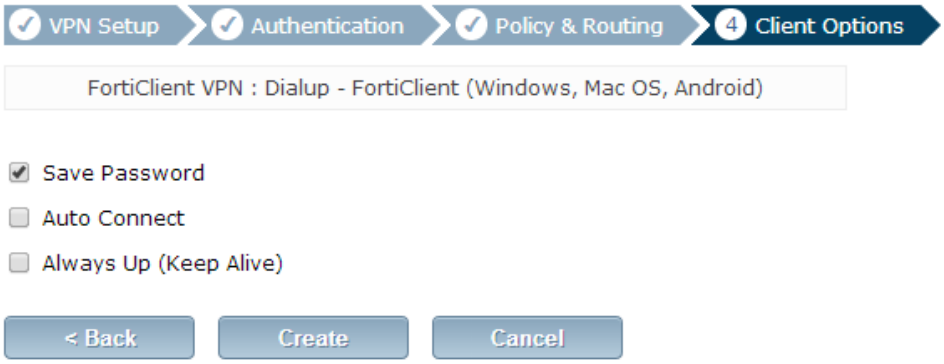


6. Set Local Interface to an internal interface (in the example, port 1) and set Local Address to the local LAN address.

7. Enter an IP range for VPN users in the Client Address Range field.*

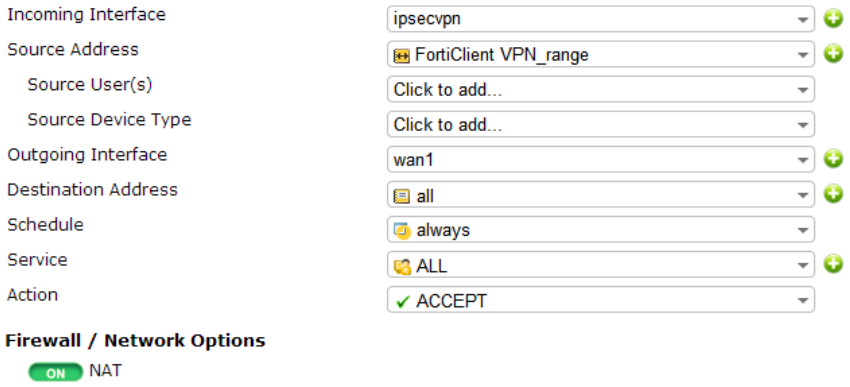


8. Click Next and select Client Options as desired.



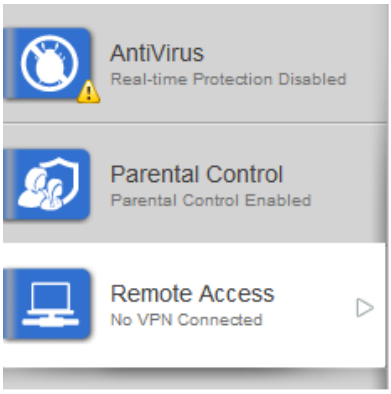
4.3.4 Creating a security policy for access to the Internet

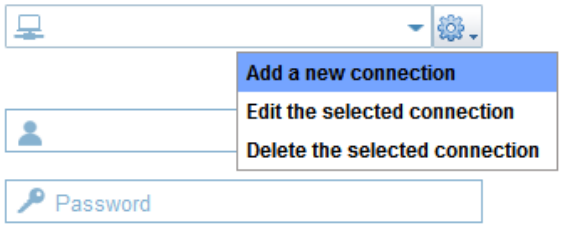
1. Go to Policy & Objects > Policy > IPv4.
2. Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.
3. Set Incoming Interface to the tunnel interface and set Source Address to all.
4. Set Outgoing Interface to wan1 and Destination Address to all.
5. Set Service to ALL and ensure that you enable NAT.



4.3.5 Configuring FortiClient

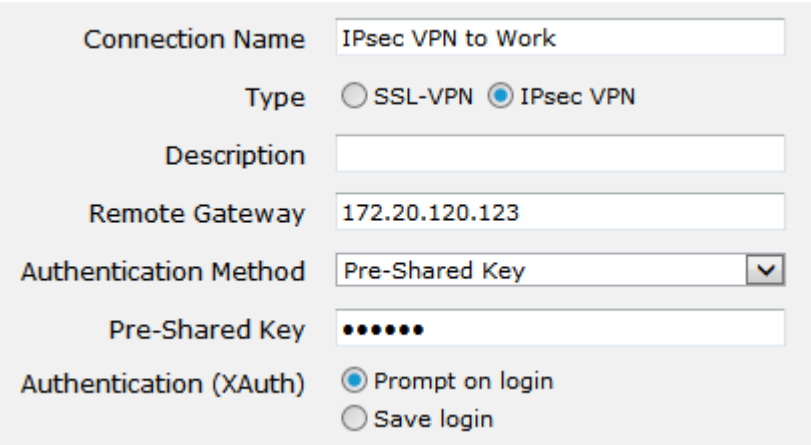
1. Open FortiClient, go to Remote Access and Add a new connection





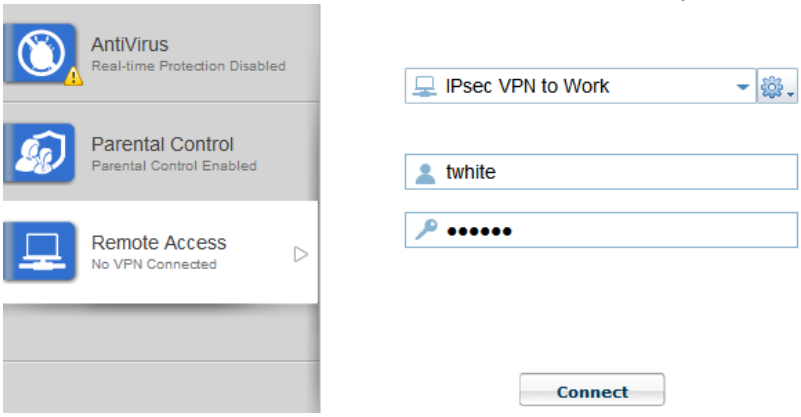
2. Provide a Connection Name and set the Type to IPsec VPN.
3. Set Remote Gateway to the FortiGate IP address.

4. Set Authentication Method to Pre-Shared Key and enter the key below



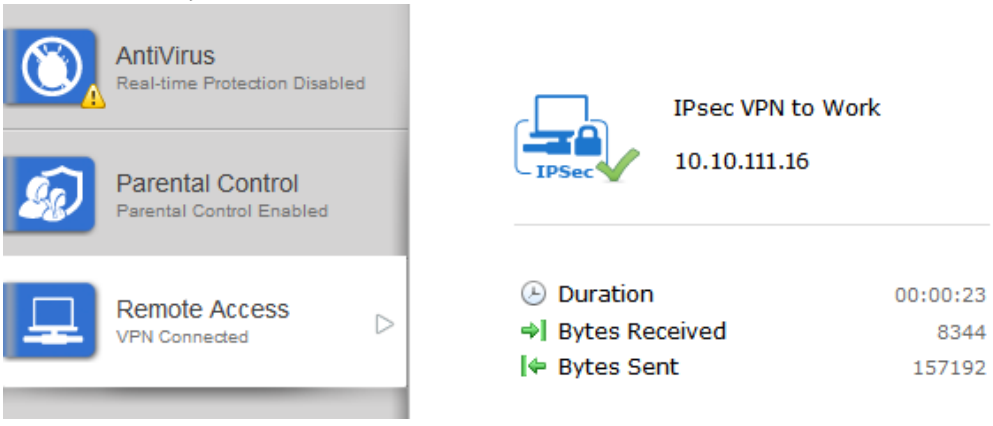
\

5. Select the new connection, enter the username and password, and click Connect.



4.3.6 Results

1. Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received



2. On the FortiGate unit, go to VPN > Monitor > IPsec Monitor and verify that the tunnel Status is Up.

Name	Ty...	Remote Gatew...	Stat...	Incoming D...	Outgoing Data
ipsec_0	Dialup	172.20.120.16	Up	9.22 K	3.48 K

3. Go to Log & Report > Traffic Log > Forward Traffic to view the traffic.

4. Verify that the Sent/Received column displays traffic successfully flowing through the tunnel

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	56 B / 288 B